ローリングパッチのリリースノート

このセクションには、最近のXenMobile® Serverローリングパッチのリリースノートが含まれています。以下のリンクをクリックして、修正された問題と既知の問題、機能の変更、および必要なアクションを表示してください。

最新のローリングパッチには、同じリリースに対する以前のローリングパッチからのすべての修正が含まれています。

現在のリリースへのパッチのリリースノート	公開日	サポート記事
10.16 ローリングパッチ 9	Sep 17, 2026	リリースノート
10.16 ローリングパッチ 8	Jan 27, 2026	リリースノート
10.16 ローリングパッチ 7	Nov 13, 2025	リリースノート
10.16 ローリングパッチ 6	Sep 26, 2025	リリースノート
10.16 ローリングパッチ 5	Apr 22, 2025	CTX692919
10.16 ローリングパッチ 4	Dec 18, 2024	CTX692370
10.16 ローリングパッチ 3	Aug 28, 2024	CTX691503
10.16 ローリングパッチ 2	Jul 02, 2024	CTX678043
10.16 ローリングパッチ 1	Jun 17, 2024	CTX677872

以前のリリースへのパッチのリリースノート	公開日	サポート記事
10.15 ローリングパッチ 14	Jul 02, 2026	リリースノート
10.15 ローリングパッチ 13	Nov 20, 2025	リリースノート
10.15 ローリングパッチ 12	Oct 23, 2025	リリースノート

XENMOBILE®サーバー

以前のリリースへのパッチのリリースノート	公開日	サポート記事
10.15 ローリングパッチ 11	May 13, 2025	CTX693257
10.15 ローリングパッチ 10	Jan 27, 2025	CTX692560
10.15 ローリングパッチ 9	Dec 04, 2024	CTX692268
10.15 ローリングパッチ 8	Jul 11, 2024	CTX691107
10.15 ローリングパッチ 7	Jun 06, 2024	CTX677079
10.15 ローリングパッチ 6	Mar 06, 2024	CTX625010
10.15 ローリングパッチ 5	Nov 13, 2023	CTX583748
10.15 ローリングパッチ 4	Sep 18, 2023	CTX579528
10.15 ローリングパッチ 3	Jul 19, 2023	CTX565649
10.15 ローリングパッチ 2	Apr 26, 2023	CTX546782
10.15 ローリングパッチ 1	Feb 23, 2023	CTX478719
10.14 ローリングパッチ 13	Mar 08, 2024	CTX628921
10.14 ローリングパッチ 12	Oct 19, 2023	CTX582535
10.14 ローリングパッチ 11	May 31, 2023	CTX558678
10.14 ローリングパッチ 10	Mar 23, 2023	CTX491036
10.14 ローリングパッチ 9	Dec 20, 2022	CTX477055
10.14 ローリングパッチ 8	Sep 22, 2022	CTX464099
10.14 ローリングパッチ 7	Aug 18, 2022	CTX463691
10.14 ローリングパッチ 6	May 23, 2022	CTX459871
10.14 ローリングパッチ 5	Mar 30, 2022	CTX399411

以前のリリースへのパッチのリリースノート	公開日	サポート記事
10.14 ローリングパッチ 4	Jan 26, 2022	「CTX339069」(https://support.citrix.com/article/CTX339069)
10.14 ローリングパッチ 3	Dec 22, 2021	「CTX335897」(https://support.citrix.com/article/CTX335897)
10.14 ローリングパッチ 2	Dec 15, 2021	「CTX335763」(https://support.citrix.com/article/CTX335763)
10.14 ローリングパッチ 1	Nov 19, 2021	「CTX335342」(https://support.citrix.com/article/CTX335342)

XenMobile Server 10.16 ローリングパッチ9リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.16 ローリングパッチ9の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ9のソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **Launcher構成デバイスポリシーでのシステム情報有効化のサポート:**

  Android Enterpriseデバイス向けのLauncher構成デバイスポリシーに、新しい設定「**システム情報を有効にする**」が追加されました。この設定により、Citrix Launcherはステータスバーにシステム情報を表示できます。デフォルトは**オフ**で、Secure Hub 26.8以降が必要です。詳しくは、「Launcher構成ポリシー」を参照してください。

- **Launcher構成デバイスポリシーでのアプリの自動起動のサポート:**

  Android Enterpriseデバイス向けのLauncher構成デバイスポリシーに、新しい設定「**アプリの自動起動**」が追加されました。この設定により、管理者はCitrix Launcherの起動時に自動的に開始する**許可されたアプリ**のいずれかを選択できます。デフォルトは**なし（自動起動しな

い）**で、Citrix Launcher 26.8以降が必要です。詳しくは、「Launcher構成ポリシー」を参照してください。

XenMobile Serverには、`afw.launcher.auto_launch`という新しいプロパティがあり、管理者がLauncher構成ポリシーで構成されたAndroid Enterpriseデバイスのアプリの自動起動を設定できるようにします。デフォルト値は**False**です。詳しくは、「サーバープロパティ」を参照してください。

- **デバイスアプリのアプリ検索オプションのサポート:**

  XenMobile Serverコンソールで、**デバイス > デバイスの詳細 > アプリ**ページに新しい**アプリ検索**オプションが追加されました。

- **アプリ設定デバイスポリシーのサポート:**

  構成（宣言型）の下に、新しいデバイスポリシー「**アプリ設定**」が追加されました。このポリシーを使用すると、Appleの宣言型デバイス管理を使用してアプリの許可リストと拒否リストを構成できます。このポリシーは、監視対象のiOS 27以降のデバイスのみをサポートします。詳しくは、「アプリ設定デバイスポリシー」を参照してください。

  XenMobile Serverには、アプリ設定デバイスポリシーを有効にする新しいプロパティ`ios.mdm.ios27.ddm.support`があります。デフォルト値は**True**です。詳しくは、「サーバープロパティ」を参照してください。

- **iOSおよびmacOSの展開ルールでのシリアル番号のサポート:**

  XenMobile Serverは、iOSおよびmacOS向けに新しい展開ルール「**シリアル番号**」をサポートするようになりました。このルールは、**展開ルール > 詳細設定**で追加します。

- **Android 17 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 17 を実行している Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメントを参照してください。

- **iOS 27 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、iOS 27 に対応しました。

- **Secure Hub APNs 証明書の更新:**

  XenMobile Server 10.16 用の Secure Hub Apple Push Notification service (APNs) 証明書は、November 9, 2026 に期限切れになります。この更新プログラムにより、Secure Hub APNs 証明書は、September 18, 2027 まで有効な新しい証明書に自動的に更新されます。

修正された問題

- /api/v1/application/store/{id}/platform/iphone REST API を介した iOS アプリの更新は、エラー 1493 で失敗します。
- トライアルライセンスからライセンスアクティベーションサービス (LAS) ライセンスに移行した後、ライセンスタイプが正しく設定されず、登録プロファイルから iOS オプションがなくなります。

XenMobile Server 10.16.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server の更新プログラムをインストールする

> **重要:**
>
> この更新プログラムをインストールする前に、XenMobile Server バージョン 10.16.0.48 にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。

> クラスターモードで構成されたシステムの場合、次の手順に従って、各ノードを順次更新してください。

1. Citrix® Web サイトでアカウントにサインインし、XenMobile Server 更新プログラム (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、**Settings > Release Management**をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、**Update**をクリックします。「更新」ダイアログボックスが表示されます。
4. Citrix downloads pageからダウンロードした更新 (.bin) ファイルをアップロードするには、**Browse**をクリックします。
5. **Update**をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を確認するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**Settings > Release Management > Updates**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.16 ローリングパッチ9リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.16 ローリングパッチ9の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ9のソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **Launcher構成デバイスポリシーでのシステム情報有効化のサポート:**

  Android Enterpriseデバイス向けのLauncher構成デバイスポリシーに、新しい設定「**システム情報を有効にする**」が追加されました。この設定により、Citrix Launcherはステータスバーにシステム情報を表示できます。デフォルトは**オフ**で、Secure Hub 26.8以降が必要です。詳しくは、「Launcher構成ポリシー」を参照してください。

- **Launcher構成デバイスポリシーでのアプリの自動起動のサポート:**

  Android Enterpriseデバイス向けのLauncher構成デバイスポリシーに、新しい設定「**アプリの自動起動**」が追加されました。この設定により、管理者はCitrix Launcherの起動時に自動的に開始する**許可されたアプリ**のいずれかを選択できます。デフォルトは**なし（自動起動しない）**で、Citrix Launcher 26.8以降が必要です。詳しくは、「Launcher構成ポリシー」を参照してください。

  XenMobile Serverには、`afw.launcher.auto_launch`という新しいプロパティがあり、管理者がLauncher構成ポリシーで構成されたAndroid Enterpriseデバイスのアプリの自動起動を設定できるようにします。デフォルト値は**False**です。詳しくは、「サーバープロパティ」を参照してください。

- **デバイスアプリのアプリ検索オプションのサポート:**

  XenMobile Serverコンソールで、**デバイス > デバイスの詳細 > アプリ**ページに新しい**アプリ検索**オプションが追加されました。

- **アプリ設定デバイスポリシーのサポート:**

構成（宣言型）の下に、新しいデバイスポリシー「**アプリ設定**」が追加されました。このポリシーを使用すると、Appleの宣言型デバイス管理を使用してアプリの許可リストと拒否リストを構成できます。このポリシーは、監視対象のiOS 27以降のデバイスのみをサポートします。詳しくは、「アプリ設定デバイスポリシー」を参照してください。

XenMobile Serverには、アプリ設定デバイスポリシーを有効にする新しいプロパティ`ios.mdm.ios27.ddm.support`があります。デフォルト値は**True**です。詳しくは、「サーバープロパティ」を参照してください。

- **iOSおよびmacOSの展開ルールでのシリアル番号のサポート:**

  XenMobile Serverは、iOSおよびmacOS向けに新しい展開ルール「**シリアル番号**」をサポートするようになりました。このルールは、**展開ルール > 詳細設定**で追加します。

- **Android 17 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 17 を実行している Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメントを参照してください。

- **iOS 27 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、iOS 27 に対応しました。

- **Secure Hub APNs 証明書の更新:**

  XenMobile Server 10.16 用の Secure Hub Apple Push Notification service (APNs) 証明書は、November 9, 2026 に期限切れになります。この更新プログラムにより、Secure Hub APNs 証明書は、September 18, 2027 まで有効な新しい証明書に自動的に更新されます。

修正された問題

- /api/v1/application/store/{id}/platform/iphone REST API を介した iOS アプリの更新は、エラー 1493 で失敗します。
- トライアルライセンスからライセンスアクティベーションサービス (LAS) ライセンスに移行した後、ライセンスタイプが正しく設定されず、登録プロファイルから iOS オプションがなくなります。

XenMobile Server 10.16.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server の更新プログラムをインストールする

> **重要:**
>
> この更新プログラムをインストールする前に、XenMobile Server バージョン 10.16.0.48 にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。
>
> クラスターモードで構成されたシステムの場合、次の手順に従って、各ノードを順次更新してください。

1. Citrix® Web サイトでアカウントにサインインし、XenMobile Server 更新プログラム (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、**Settings > Release Management**をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、**Update**をクリックします。「更新」ダイアログボックスが表示されます。
4. Citrix downloads pageからダウンロードした更新 (.bin) ファイルをアップロードするには、**Browse**をクリックします。
5. **Update**をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を確認するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**Settings > Release Management > Updates**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.16 Rolling Patch 8 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.16 Rolling Patch 8 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 Rolling Patch 8 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **宣言型デバイス管理 (DDM) のサポート:**

XenMobile Server は、iOS 15 以降で Apple の宣言型デバイス管理 (DDM) のサポートを追加します。この機能は、宣言型データモデルを使用することでパフォーマンスとスケーラビリティを向上させ、シリアル化されたコマンドとデバイスポーリングへの依存を減らします。詳細については、「宣言型管理データモデルを活用してデバイスを拡張する」を参照してください。

XenMobile Server には、次の2つの新しいプロパティがあります。

`ios.mdm.declarative.management`: iOS 宣言型デバイス管理 (DDM) を有効にします。

`ios.mdm.software.update.settings`: ソフトウェアアップデート強制デバイスポリシーを有効にします。

両方のプロパティのデフォルト値は **False** です。詳細については、「サーバープロパティ」を参照してください。

DDM 機能を有効にすると、次の宣言型デバイスポリシー がサポートされます。

- Google アカウント
- パスコード
- ソフトウェアアップデート強制
- ソフトウェアアップデート設定
- ステータスサブスクリプション
- ユーザーID(/ja-jp/xenmobile/server/policies/declarative-device-management-policies/user-identity-device-policy.html)

- **iOSデバイスのキャリアネットワーク関連デバイス情報取得のサポート:**

  XenMobile Serverは、iOSデバイスの各SIMに関する追加のキャリアネットワーク関連デバイス情報の取得をサポートするようになりました。これらの詳細は、**デバイスの詳細 > プロパティ > スロットx SIM情報**で確認できます。新しくサポートされるフィールドは次のとおりです。

  - スロットx — キャリア設定バージョン
  - スロットx — 現在のキャリアネットワーク
  - スロットx — 現在のモバイル国コード（以前はネットワーク情報の下に表示）
  - スロットx — 現在のモバイルネットワークコード（以前はネットワーク情報の下に表示）
  - スロットx — データ優先
  - スロットx — ローミング中

- スロットx — 音声優先
- スロットx — ラベルID

- **Microsoft Exchange OnlineのOAuth認証のサポート:**

  Microsoftは、Exchange Onlineが2026年3月にクライアント送信（SMTP AUTH）での基本認証のサポートを完全に削除し、April 30, 2026には100%拒否されるようになると発表しました。詳細については、Exchange Online to retire Basic auth for Client Submission (SMTP AUTH)を参照してください。

  XenMobile Serverは、SMTPサーバーのOAuth認証をサポートしています。この機能を有効にするには、**Microsoft Exchange Online OAuth 2.0**を選択し、必要な**テナントID**、**クライアントID**、および**クライアントシークレット**を指定します。Microsoft Exchange Onlineを使用している場合は、OAuth認証に切り替えることをCitrixは推奨します。設定の詳細については、通知を参照してください。

- **iOSデバイスが近接設定を行うのを防ぐためのサポート:**

  XenMobile Serverは、完全なデバイスワイプ用に新しいオプション **次回の再起動時に近接設定は許可されず、セットアップアシスタントのペインはスキップされます** を追加します。このオプションにより、デバイスセットアップ中にiOSデバイスが近接設定を行うのを防ぎます。この機能はiOS 11.3以降で利用可能です。詳細については、「セキュリティアクション」を参照してください。

- **iOS 26.xアプリサイズの取得をサポートするようにアプリインベントリを強化:**

  XenMobile Serverは、iOS 26.xを実行しているデバイスのアプリサイズ情報の取得をサポートしています。この情報は、**デバイスの詳細 > アプリ** で確認できます。

修正された問題

- 10.16 Rolling Patch 5にアップグレードした後、XenMobile Serverコンソールでのデバイス、アプリ、デリバリーグループの管理などの操作が著しく遅くなり、失敗することがあります。

XenMobile Server 10.16.0の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Serverのアップデートをインストールする

> **重要:**

> このアップデートをインストールする前に、XenMobile Serverバージョン10.16.0.48にアップグレード済みであることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。

> クラスターモードで構成されたシステムの場合、次の手順に従って各ノードを順次アップデートします。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Serverアップデート (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、**設定 > リリース管理** をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードしたアップデート、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、**アップデート** をクリックします。 ダイアログボックスが表示されます。
4. **参照** をクリックして、Citrixダウンロードページからダウンロードしたアップデート (.bin) ファイルをアップロードします。
5. 「**更新**」をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を確認するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**設定 > リリース管理 > 更新**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.16 ローリングパッチ 7 リリースノート

これらのリリースノートでは、XenMobile Server 10.16 ローリングパッチ 7 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ 7 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **Android Enterpriseデバイス向けデュアルSIMおよびeSIMサポートの強化:**

  XenMobile Serverは、iOSとの機能パリティを確保するため、Android Enterpriseデバイス向けに包括的なデュアルSIMサポートを提供するようになりました。この機能強化により、管理者は、2枚の物理SIMカード、1枚のSIMカードと1枚のeSIM、または2枚のeSIMの構成を含む、デバイスプロパティ内のすべてのインストール済みSIMカードとeSIMを表示できるようになります。このアップデートは、デュアルSIM Android Enterpriseデバイスの採用拡大に対応し、以

前にiOSデバイス向けに提供されたeSIM機能と一致する、モバイルデバイスの接続オプションに関する完全な可視性を顧客に提供します。この機能は、以下でのみサポートされます。

- Secure Hub バージョン 25.7.0 以降、および
- Android 13 以降

XenMobile Serverには新しいプロパティ`ae.esim.support`があり、これによりXenMobile ServerはAndroid Enterpriseデバイスからe SIM情報を取得し、eSIM関連のデバイスプロパティをユーザーインターフェイスに表示できます。このプロパティのデフォルト値は**True**です。詳細については、サーバープロパティを参照してください。

- **ライセンスアクティベーションサービス:**

XenMobile Serverは、ライセンスアクティベーションサービス (LAS) ライセンスメカニズムをサポートするようになりました。LASは、Citrix製品スイート全体で従来のファイルベースのライセンスに代わる最新のクラウドベースのライセンスソリューションです。Citrix License ServerをCitrix Cloudに登録して、ライセンスアクティベーションサービスが保持するライセンスと資格を使用してください。詳細については、ライセンスアクティベーションサービスを参照してください。

重要:

Citrixプラットフォーム向けに、業界標準のクラウドベースのライセンスアーキテクチャへの移行を進めています。この移行により、資格とアクティベーションが自動化され、お客様に以下の主要なメリットがもたらされます。

- **ライセンスファイル管理が不要:** ライセンスファイルのダウンロード、割り当て、または管理の必要がなくなり、管理タスクが簡素化されます。
- **資格の自動更新:** 契約更新時に資格がバックグラウンドで自動的に更新され、中断のないサービスが保証されます。
- **回復力の向上:** ライセンスサーバーがユーザーセッションの単一障害点ではなくなり、環境の安定性が向上します。

切り替えまでの期間を利用して、新しいライセンスモデルを「April 15, 2026」までに導入するための移行を計画し、実行することをお勧めします。私たちは、その過程のあらゆる段階で皆様をサポートすることをお約束します。詳細については、「Citrix Modern Licensing Announcement」を参照してください。

- **Secure Hub APNs証明書の更新:**

  XenMobile Server 10.16のSecure Hub Apple Push Notification service (APNs) 証明書は、「January 4, 2026」に期限切れになります。このアップデートにより、Secure Hub APNs証明書は「November 9, 2026」まで有効な新しい証明書に自動的に更新されます。

- **iOS 18.xバージョン向けの新しいiOS制限のサポート:**

  iOSの制限ポリシーに、Apple Intelligence (AI) へのアクセスをブロックしたり、一部の新機能を制限したりするための以下の新しい設定が追加されました。これらの設定は、iOSバージョン18以降に適用されます。デフォルトは**オン**です。詳細については、「Restrictions Policy」を参照してください。

  - 外部インテリジェンス統合を許可する
  - 外部インテリジェンス統合へのサインインを許可する
  - メールスマートリプライを許可する
  - メモの文字起こしを許可する
  - Safariの要約を許可する
  - ビジュアルインテリジェンスの要約を許可する
  - メモの文字起こし要約を許可する
  - Apple Intelligenceレポートを許可する
  - デフォルトの通話アプリの変更を許可する
  - デフォルトのメッセージングアプリの変更を許可する
  - 外部インテリジェンスワークスペースIDを許可
  - デフォルトブラウザの変更
  - FaceTimeリモートコントロールを許可

修正された問題

- XenMobileサーバーでCPUとメモリの使用率が高いためにデバイスの登録が失敗します。

XenMobile Server 10.16.0の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Serverの更新をインストールする

重要:

このアップデートをインストールする前に、XenMobile Serverバージョン10.16.0.48にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。

クラスターモードで構成されたシステムの場合、以下の手順に従って各ノードを順次更新します。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Serverの更新 (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、 **>** をクリックします。

   ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. で、 をクリックします。 ダイアログボックスが表示されます。
4. Citrix downloads page からダウンロードした更新 (.bin) ファイルをアップロードするには、をクリックします。
5. 「**更新**」をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を確認するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、 **> >** に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.16 Rolling Patch 6 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.16 Rolling Patch 6 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 Rolling Patch 6 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **Android 16 のサポート**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 16 を実行している Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメント を参照してください。

- **iOS 26 のサポート**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、iOS 26 と互換性があります。

- **レガシー MDX ポリシーアップグレード通知のサポート**

  XenMobile Server は、レガシーポリシーを使用している既存の Secure Mail および Secure Web MDX アプリがバージョン 25.9.0 に更新されたときに、アップグレードアラートを表示するようになりました。

- **証明書ベースの認証における新しい強力な証明書マッピングのサポート**

  強力なマッピング要件を満たす証明書の発行において、より柔軟性を持たせるための新しいマッピング方法が導入されました。XenMobile Server は、証明書のサブジェクト代替名 (SAN) に `URL=tag:microsoft.com`, `2022-09-14:sid:<user's SID>` を追加するようになりました。

  - 既存のユーザーに対してこの機能を有効にするには、顧客管理者はクライアントプロパティ `MICROSOFT_CERTIFICATE_STRONG_MAPPING` を追加する必要があります。詳細については、「クライアントプロパティ」を参照してください。
  - 強力な証明書マッピングは、**Windows Server 2019 以降**でのみサポートされています。詳細については、「Microsoft Strong Mapping」を参照してください。

- **iOS 17.x バージョン向けの新しい iOS 制限のサポート**

  iOS の制限ポリシーに、iOS バージョン 17.2 以降向けに次の新しい設定が追加されました。デフォルトは **On** です。詳細については、「制限ポリシー」を参照してください。

  - ライブボイスメールを許可する

- **構成ポリシーのテキストボックスを管理する**

  お客様が**Knox Service Plugin**を**Managed Configuration policy**と併用する場合、**Separated Apps Policies**上のすべてのテキストボックスの最大文字長が8,192文字に増加します。

- **Apple Deployment Programsページで新しいiOSセットアップアシスタントオプションをサポート**

  Appleは、Apple Business Management登録用にいくつかの新しいiOSセットアップアシスタントオプション画面を追加しました。以下の新しいオプションが、**Settings > Apple Deployment Programs > iOS Setup Assistant Options**ページに追加されています。XenMobile Serverを構成して、これらの画面をスキップできます。詳しくは、「iOSセットアップアシスタントオプション」を参照してください。

- アクションボタン
- ロックダウンモード
- インテリジェンス
- カメラボタン

- **Apple Business Managerと同期してデバイスの割り当てを管理する**

  XenMobile® Server (XMS) は、Apple Business Manager (ABM) と同期することで、正確なデバイス割り当てを保証するようになりました。この更新により、XMSには正しく割り当てられたデバイスのみが表示され、XMSから削除され、別のベンダー管理ソリューションに割り当てられたデバイスの記録が残ることを防ぎます。たとえば、デバイスが別のソリューションに移動された場合、同期後にはXMSに表示されなくなります。

  XMSには、このサーバーに割り当てられなくなったデバイスをXMSが削除できるようにする新しいプロパティ`remove.unassigned.abm.devices`が含まれるようになりました。デフォルトでは、このプロパティは**False**に設定されています。詳しくは、「サーバープロパティ」を参照してください。

修正された問題

- Legacy MDXアプリケーションがアップロードされていない場合でも、XMSコンソールにLegacy MDXアラートが表示され続ける。
- マウスで右クリックしてパスワードを貼り付けて入力すると、XenMobileポータルのサインインボタンがグレー表示される。
- 「**新しいビューを表示**」機能が有効になっている場合、デバイスリストにフィルターが適用されていても、デバイス数が正しく表示されません。
- iOSユーザーは、Secure Mail/Secure WebからSecure Hubにリダイレクトされると、Secure Mail/Secure Webアプリケーションを起動できず、「開けません」というエラーが発生します。
- Device Enrollment Program (DEP) デバイスは、登録プロファイルが**MDMのみ**として構成されている場合でも、**MDM+MAM**登録を継続して実行します。
- iOSデバイスにアンインストールされたアプリケーションのApp Lockポリシーがある場合、デバイスは「ガイド付きアクセスアプリは利用できません。管理者にお問い合わせください」というエラーでロックされ、強制再起動後でもタッチスクリーンが応答しなくなります。
- XenMobile MDMソリューションでWindowsクライアントを登録すると、デリバリーグループの展開が失敗します。その結果、プッシュされたポリシーを適用するには手動同期操作が必要です。回避策として、単一デバイスへの手動展開が必要です。

XenMobile Server 10.16.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Serverの更新をインストールする

> **重要:**
>
> この更新をインストールする前に、XenMobile Serverバージョン10.16.0.48にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。
>
> クラスターモードで構成されたシステムの場合、各ノードを順次更新するには、次の手順に従います。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Server更新 (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、 **>** をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、 をクリックします。 ダイアログボックスが表示されます。
4. Citrixダウンロードページからダウンロードした更新 (.bin) ファイルをアップロードするには、をクリックします。
5. **更新**をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を検証するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**設定 > リリース管理 > 更新**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.16 Rolling Patch 5 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.16 Rolling Patch 5 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 Rolling Patch 5 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **マネージド構成フィードバックのサポート（テクニカルプレビュー）**

  この機能により、管理者はマネージド構成ポリシーで構成された Android デバイスからアプリの状態に関するフィードバックを取得できます。詳しくは、「マネージド構成フィードバックのサポート（テクニカルプレビュー）」を参照してください。

  XenMobile Server には、新しいプロパティ `afw.app_managed_configurations.feedback` が含まれるようになりました。これにより、管理者はマネージド構成ポリシーで構成された Android デバイスからアプリの状態に関するフィードバックを取得できる機能が有効になります。デフォルトでは、このプロパティは **False** に設定されています。詳しくは、「サーバープロパティ」を参照してください。

- **デバイスページでの永続フィルターのサポート**

  新しいデバイスページでは、すべての**フィルター可能な**オプションでフィルターがサポートされるようになりました。これらのフィルターは、ログインユーザーのセッション間で保存されるため、管理者がデバイスページにアクセスするたびに同じフィルターを再適用する必要がなくなります。対応する列の選択が解除されると、フィルターは自動的に削除されます。

- **iPhone および iPad のデータプラン保持のサポート**

  デバイスの完全ワイプを実行する際に、「ワイプ時にモバイルデータプランを保持」という新しいオプションが利用可能になりました。このオプションを使用すると、ワイプ処理中にデバイス上のモバイルデータプラン（eSIMなど）を保持できます。この機能は、iOS バージョン 11 以降で利用できます。詳しくは、「セキュリティアクション」を参照してください。

- **iOS 向け新しい iOS 18 設定のサポート**

  iOS の制限ポリシーに、Apple Intelligence (AI) へのアクセスをブロックしたり、一部の新機能を制限したりするための以下の新しい設定が追加されました。これらの設定は、iOS バージョン 18 以降に適用されます。デフォルトは **On** です。詳しくは、「制限ポリシー」を参照してください。

  - 通話録音
  - 非表示にするアプリ
  - ロックするアプリ
  - メール概要
  - RCSメッセージング
  - デフォルトブラウザの変更

- **macOS向けに新しいmacOS 15設定をサポート**

  macOSの制限ポリシーでは、Apple Intelligence (AI)へのアクセスをブロックしたり、一部の新機能を制限したりするために、次の新しい設定が追加されました。これらの設定はmacOSバージョン15以降に適用されます。詳細については、制限ポリシーを参照してください。

  - メディア共有の変更を許可
  - スクリーンキャプチャアラートの強制バイパス
  - メール概要

修正された問題

- 「サーバープロパティ」権限がない場合、デバイスページで「新しいビューを表示 (技術プレビュー)」を切り替えると、ロールベースのアクセス制御 (RBAC) 管理者が予期せずログアウトされます。
- アプリケーションが新しいバージョンにアップグレードされても、ボリューム購入プログラム (VPP) アプリのアイコンが更新されません。
- MDM証明書の更新が失敗すると、古い証明書はXenMobile® Serverによって失効済みとしてマークされ、Secure Hub (SH) がサーバーに再接続できなくなります。その結果、SHはまだ期限切れになっていないにもかかわらず、古い証明書を使用してサーバーと通信できません。
- **新しいビューの技術プレビューを表示**機能が有効になっている場合、ロールベースのアクセス制御 (RBAC) 管理者が予期せず検索入力ボックスを表示します。
- 多数のペイロード証明書がAEデバイス用に生成されます。
- **展開スケジュール**で**展開条件**が「以前の展開が失敗した場合のみ」に設定されている場合、再登録時に一部のポリシーがAEデバイスに展開されません。

XenMobile Server 10.16.0 の以前のローリングパッチに関する情報については、「ローリングパッチのリリースノート」(/ja-jp/xenmobile/server/release-notes.html)を参照してください。

XenMobile Server 10.16 ローリングパッチ 4 リリースノート

このリリースノートでは、XenMobile Server 10.16 ローリングパッチ 4 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ 4 のソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **Secure Hub APNs証明書の更新**

XenMobile Server 10.16 用の Secure Hub Apple Push Notification service (APNs) 証明書は、February 9, 2025 に期限切れになります。このアップデートにより、Secure Hub APNs 証明書は、January 4, 2026 まで有効な新しい証明書に自動的に更新されます。

- **macOS 15のサポート**

  XenMobile® ServerおよびCitrix Mobile生産性向上アプリはmacOS 15と互換性がありますが、現在のところmacOS 15のすべての新機能には対応していません。

- **iOS 18のサポート**

  XenMobile ServerおよびCitrix Mobile生産性向上アプリはiOS 18と互換性がありますが、現在のところiOS 18のすべての新機能には対応していません。

- **Android 15のサポート**

  XenMobile ServerおよびCitrix Mobile生産性向上アプリは、Android Enterpriseデバイスの Android 15へのアップデートをサポートするようになりました。セキュリティとプライバシーの利点の詳細については、Android開発者向けドキュメントを参照してください。

- **デバイスの紛失モードAPIを含めるように公開Rest APIドキュメントを更新**

  公開Rest APIドキュメントに紛失モードAPIを追加しました。

- **API呼び出しをURLではなくPOSTボディにするように変更**

  公開Rest APIドキュメントで、API呼び出しがURLではなくリクエストボディにデータを含むように更新しました。

- **iOS向けApple Intelligenceのブロックまたは制限のサポート**

  iOSの制限ポリシーでは、Apple Intelligence (AI)へのアクセスをブロックしたり、一部の新機能を制限したりするために、以下の新しい設定が追加されました。これらの設定はiOSバージョン18以降に適用されます。デフォルトは**オン**です。詳細については、制限ポリシーを参照してください。

  - ジェンモジ
  - イメージプレイグラウンド
  - イメージワンド
  - iPhoneミラーリング
  - パーソナライズされた手書き結果
  - ライティングツール

- **macOS向けApple Intelligenceのブロックまたは制限のサポート**

macOSの制限ポリシーでは、Apple Intelligence (AI)へのアクセスをブロックしたり、一部の新機能を制限したりするために、以下の新しい設定が追加されました。これらの設定はmacOSバージョン15以降に適用されます。デフォルトは**オン**です。詳細については、制限ポリシーを参照してください。

- イメージプレイグラウンド
- iPhoneミラーリング
- ライティングツール

- **iOSデバイスへのOSアップデートの即時インストールをサポート**

  OSアップデート制御デバイスポリシーでは、iOSのOSアップデートオプションに**Install ASAP**という新しいラジオボタンが追加されました。この機能により、以前にダウンロードされたOSアップデートをiOSデバイスに即座にインストールできます。詳細については、iOS向けOSアップデート制御デバイスポリシーを参照してください。

- **システムがデバイスを消去する際にeSIMを保持するサポート**

  新しい設定、**消去時にeSIMを保持**が制限ポリシーに追加されました。この設定により、パスワードの入力に複数回失敗したためシステムがデバイスを消去する場合、または**設定** > **一般** > **リセット**で**すべてのコンテンツと設定を消去**オプションが選択された場合に、eSIMが保持されるようになります。この機能はiOSバージョン17.2以降で利用可能で、デフォルト設定は**オフ**です。詳細については、制限ポリシーを参照してください。

- **Web配布されたサードパーティ製アプリのブロックをサポート**

  制限ポリシーに、iOSデバイス上のWeb配布されたサードパーティ製アプリをブロックするための新しい設定**Web配布**アプリが追加されました。この設定はiOSバージョン17.5以降に適用されます。詳細については、制限ポリシーを参照してください。

- **コピー＆ペースト機能の管理をサポート**

  制限ポリシーに、新しい設定**管理されたペーストボードを要求**が追加されました。これにより、コピー＆ペースト機能が、**管理されていないアプリ内の管理対象アプリからのドキュメント**および**管理対象アプリ内の管理されていないアプリからのドキュメント**に適用するのと同じ制限に従うようになります。デフォルトは**オフ**です。詳細については、制限ポリシーを参照してください。

- **サムスン エンハンスド アッテステーション v3 のサポート**

  Samsung Enhanced Attestation v3は、Samsung KnoxデバイスにおけるXMSセキュリティ機能を向上させます。詳細については、Samsung Knox Enhanced Attestationを参照してください。 XenMobile Serverには、Samsung KnoxデバイスにおけるXMSセキュリティ機能を向上さ

せる機能を有効にする新しいプロパティ`afw.knox.attestation.v3`が追加されました。デフォルトでは、このプロパティは**True**に設定されています。詳細については、サーバープロパティを参照してください。

修正された問題

- SQL Serverがアラートメッセージをトリガーする際に発生するパフォーマンスの問題により、XenMobile Serverは新しいAndroid Enterpriseデバイスを正常に登録できません。
- お客様がFIPS設定を**true**に有効にしているにもかかわらず、ログには引き続き無効と表示されます。さらに、お客様がCLIを通じてデータベース設定を変更しようとすると、XenMobile Serverはデータベースへの接続を確立できず、更新が適用されません。

XenMobile Server 10.16.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.16 ローリングパッチ 3 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.16 ローリングパッチ 3 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ 3 のソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **iPhoneおよびiPad向けサービスへの復帰のサポート**

  サービスへの復帰機能を使用すると、MDMサーバーは、Wi-Fiの詳細とデフォルトのMDM登録プロファイルを含む消去コマンドをユーザーデバイスに送信できます。デバイスは自動的にすべてのユーザーデータを消去し、指定されたWi-Fiネットワークに接続し、提供された登録プロファイルを使用してMDMサーバーに再登録します。詳細については、「セキュリティアクション」を参照してください。

  XenMobile Serverには、iOS 17以降を実行しているiPhoneおよびiPad向けにサービスへの復帰機能を有効にする新しいプロパティ`ios.mdm.return.to.service`が含まれるようになりました。デフォルトでは、このプロパティは**True**に設定されています。詳細については、「サーバープロパティ」を参照してください。

- **自動登録でセットアップを完了するための最小OSバージョンの適用**

  iOS 17では、MDMは自動デバイス登録を通じてデバイスを登録するために必要な最小オペレーティングシステムバージョンを適用できるようになりました。詳細については、「Apple Deployment Programによるデバイスの展開」を参照してください。

XenMobile Serverには、iOS 17以降での自動登録中にセットアップを完了するための最小OSバージョン要件を適用できる新しいプロパティ`ios.mdm.minimum_os_version.enrollment`が含まれるようになりました。デフォルトでは、このプロパティは**True**に設定されています。詳細については、「サーバープロパティ」を参照してください。

- **個人用プロファイルから仕事用プロファイルのメールアプリにアクセスして使用するサポート**

  制限デバイスポリシーのAndroid Enterprise設定に、新しい設定**仕事用プロファイルと個人用プロファイルからメールアプリにアクセス**が追加されました。この設定により、個人用プロファイルから仕事用プロファイルのメールアプリにアクセスして使用できます。詳細については、「制限デバイスポリシー - Android Enterprise設定」を参照してください。

  XenMobile Serverには、Android Enterprise設定で個人用プロファイルから仕事用プロファイルのメールアプリにアクセスして使用できる機能を有効にする新しいプロパティ`afw.mailapp.crossworkprofile`が含まれるようになりました。デフォルトでは、このプロパティは**True**に設定されています。詳細については、「サーバープロパティ」を参照してください。

- **iOS 11.x、12.x、および13.xバージョン向けの新しいiOS制限のサポート**

  iOSの制限ポリシーに新しい設定を追加しました：

  - 共有iPadの一時セッションを許可
  - eSIMの変更を許可する
  - ネットワークドライブ接続を許可する
  - USBデバイス接続を許可する
  - デバイスを探すを許可する
  - 友達を探すを許可する
  - QuickPathキーボードを許可する
  - Wi-Fiを強制的にオンにする
  - 自動入力の前に認証を強制する
  - パーソナルホットスポット設定を変更する

  詳細については、「制限デバイスポリシー - iOS設定」を参照してください。

- **Android Enterpriseマネージド構成ポリシーの機能強化**

  「**マネージド構成**」ポリシーの「**アプリケーション管理ポリシー**」ページにあるすべてのテキストボックスの最大文字長が4096文字に増加しました。

修正された問題

- 新しいバージョンのMAM SDK対応アプリの場合、Secure Hubストアで更新オプションが利用できません。

XenMobile Server 10.16.0の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.16 ローリングパッチ2リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.16 ローリングパッチ2に関する機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 ローリングパッチ2のソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

修正された問題

- XenMobile Server 10.16バージョンにアップグレードした後、XenMobile ServerはSyslogサーバーへのログ送信を停止しました。
- プロキシが構成されている場合、HTTP v1 APIを使用するFirebase Cloud Messagingは正常に機能しません。

XenMobile Server 10.16.0の以前のローリングパッチに関する情報については、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.16 Rolling Patch 1 リリースノート

このリリースノートでは、XenMobile Server 10.16 Rolling Patch 1 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.16 Rolling Patch 1 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **iOS 17.4以降のサードパーティ製アプリのブロックをサポート:** 制限ポリシーに新しい設定 **代替アプリマーケットプレイス** が追加され、Webからの代替マーケットプレイスアプリのインストールを防止し、インストール済みの代替マーケットプレイスアプリがアプリをインストールするのを防止します。詳細については、制限デバイスポリシーを参照してください。
- **レガシーMDXモードで公開されているMDXアプリがある場合にXMSコンソールにアラートを表示:** レガシーMDXモードで公開されているMDXアプリがある場合、XenMobile Serverコンソールにアラートが表示されます。詳細については、サーバープロパティの「**レガシーMDX非推奨アラート**」を参照してください。

- **Firebase Cloud Messagingが新しいhttp v1 APIを使用するように移行をサポート:** HTTP用のFCMレガシーAPIは、Googleにより June 21, 2024 に非推奨になります。FCMが新しいAPIで適切に機能するように、Firebase Cloud Messagingページに新しいフィールド **サービスアカウントキーファイル** が追加され、サービスアカウントキーのJSONファイルをアップロードできるようになりました。詳細については、Firebase Cloud Messagingを参照してください。

  XenMobile Serverには新しいプロパティ `afw.fcm.httpv1.migration` があり、これによりFirebase Cloud Messagingを新しいHTTP v1 APIで使用できます。このプロパティのデフォルト値は **False** です。詳細については、サーバープロパティを参照してください。

  XenMobile Server 10.16 Rolling Patch 1以降でFCM API V1を有効にするには、Knowledge Centerの記事CTX677031を参照してください。

修正された問題

- XenMobile Server 10.16バージョンにアップグレードした後、オプションのWebリンクが継続的に再インストールされます。
- XenMobile Serverを10.16バージョンにアップグレードした後、**クライアントサポート**設定で**デバイスログをITヘルプデスクに送信**を**直接**として選択しても、Secure HubログをITヘルプデスクに送信できません。
- XenMobile® Serverコンソール > **制限** > **Android Enterprise** で、ポリシー設定 **モバイルネットワークの構成** のツールチップの説明がドイツ語で正しくありません。

XenMobile Server 10.16.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.15 Rolling Patch 14 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.15 Rolling Patch 14 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 14 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **Android 17 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 17 を実行する Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメント を参照してください。

- **Microsoft Exchange Online の OAuth 認証のサポート:**

  Microsoft は、Exchange Online が 2026 年 3 月にクライアント送信 (SMTP AUTH) を使用した基本認証のサポートを完全に削除し、April 30, 2026 には 100% の拒否に達すると発表しました。 詳細については、Exchange Online でクライアント送信 (SMTP AUTH) の基本認証を廃止を参照してください。

  XenMobile Server は、SMTP サーバーの OAuth 認証をサポートしています。この機能を有効にするには、**Microsoft Exchange Online OAuth 2.0** を選択し、必要な **テナント ID**、**クライアント ID**、および **クライアントシークレット** を指定します。Microsoft Exchange Online を使用している場合は、OAuth 認証に切り替えることを Citrix は推奨します。構成の詳細については、通知 を参照してください。

- **iOS 26.x アプリサイズの取得をサポートするようにアプリインベントリを強化:**

  XenMobile Server は、iOS 26.x を実行しているデバイスのアプリサイズ情報の取得をサポートしています。この情報は、**デバイスの詳細 > アプリ** で確認できます。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノート を参照してください。

XenMobile Server の更新プログラムをインストールする

> **重要:**
>
> - この更新プログラムをインストールする前に、XenMobile Server バージョン 10.15.0.23 にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。
> - 10.15 RP2 または 10.15 RTM を含むそれ以前のリリースからアップグレードする場合は、クラスター化された XenMobile 展開をアップグレードするには の手順に従って、すべてのクラスターノードをアップグレードしてください。

> クラスターモードで構成されたシステムの場合、次の手順に従って各ノードを順番に更新します。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Server更新 (.bin) ファイルを適切な場所にダウンロードします。

2. ノードのXenMobile Serverコンソールで、**Settings > Release Management**をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、**Update**をクリックします。 ダイアログボックスが表示されます。
4. Citrixダウンロードページからダウンロードした更新 (.bin) ファイルをアップロードするには、**Browse**をクリックします。
5. **Update**をクリックし、プロンプトが表示されたらコマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を検証するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**Settings > Release Management > Updates**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.15 Rolling Patch 14 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.15 Rolling Patch 14 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 14 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **Android 17 のサポート:**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 17 を実行する Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、Android 開発者向けドキュメント を参照してください。

- **Microsoft Exchange Online の OAuth 認証のサポート:**

  Microsoft は、Exchange Online が 2026 年 3 月にクライアント送信 (SMTP AUTH) を使用した基本認証のサポートを完全に削除し、April 30, 2026 には 100% の拒否に達すると発表しました。 詳細については、Exchange Online でクライアント送信 (SMTP AUTH) の基本認証を廃止を参照してください。

  XenMobile Server は、SMTP サーバーの OAuth 認証をサポートしています。この機能を有効にするには、**Microsoft Exchange Online OAuth 2.0** を選択し、必要な **テナント ID**、**クライアント ID**、および **クライアントシークレット** を指定します。Microsoft Exchange Online を使

用している場合は、OAuth 認証に切り替えることを Citrix は推奨します。構成の詳細については、通知 を参照してください。

- **iOS 26.x アプリサイズの取得をサポートするようにアプリインベントリを強化:**

  XenMobile Server は、iOS 26.x を実行しているデバイスのアプリサイズ情報の取得をサポートしています。この情報は、**デバイスの詳細 > アプリ** で確認できます。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノート を参照してください。

XenMobile Server の更新プログラムをインストールする

> **重要:**
>
> - この更新プログラムをインストールする前に、XenMobile Server バージョン 10.15.0.23 にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。
> - 10.15 RP2 または 10.15 RTM を含むそれ以前のリリースからアップグレードする場合は、クラスター化された XenMobile 展開をアップグレードするには の手順に従って、すべてのクラスターノードをアップグレードしてください。

> クラスターモードで構成されたシステムの場合、次の手順に従って各ノードを順番に更新します。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Server更新 (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、**Settings > Release Management**をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードした更新、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、**Update**をクリックします。 ダイアログボックスが表示されます。
4. Citrixダウンロードページからダウンロードした更新 (.bin) ファイルをアップロードするには、**Browse**をクリックします。
5. **Update**をクリックし、プロンプトが表示されたらコマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を検証するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**Settings > Release Management > Updates**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.15 Rolling Patch 13 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.15 Rolling Patch 13 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 13 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **ライセンスアクティベーションサービス:**

  XenMobile Server は、License Activation Service (LAS) ライセンスメカニズムをサポートするようになりました。LAS は、Citrix 製品スイート全体で従来のファイルベースのライセンスに代わる最新のクラウドベースのライセンスソリューションです。License Activation Service が保持するライセンスとエンタイトルメントを使用するには、Citrix License Server を Citrix Cloud に登録してください。詳細については、License Activation Service を参照してください。

  > **重要:**
  >
  > Citrix プラットフォームでは、業界標準のクラウドベースのライセンスアーキテクチャへの移行を進めています。この移行により、エンタイトルメントとアクティベーションが自動化され、お客様に以下の主要なメリットがもたらされます。
  >
  > - **ライセンスファイル管理が不要:** ライセンスファイルのダウンロード、割り当て、管理の必要がなくなり、管理タスクが簡素化されます。
  > - **エンタイトルメントの自動更新:** 契約更新時にエンタイトルメントがバックグラウンドで自動的に更新され、中断のないサービスが保証されます。
  > - **回復力の向上:** ライセンスサーバーがユーザーセッションの単一障害点ではなくなり、環境の安定性が向上します。 April 15, 2026までに新しいライセンスモデルへの移行を計画し、実行するための期間をご活用いただくことをお勧めします。弊社は、

この移行のあらゆる段階でお客様をサポートすることをお約束します。詳細については、Citrix Modern Licensing Announcement を参照してください。

10.15 Rolling Patch 13 以降の Rolling Patch で License Activation Service が有効になっている場合、10.16.0.48 に直接アップグレードすると、License Activation Service の構成がリセットされます。License Activation Service を再構成できるバージョン 10.16 Rolling Patch 7 以降の 10.16 Rolling Patch を引き続き適用してください。既存のデバイスには影響ありません。

修正された問題

- XenMobile Server で CPU とメモリの使用率が高いため、デバイスの登録に失敗します。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノート を参照してください。

XenMobile Server のアップデートをインストールする

重要:

- このアップデートをインストールする前に、XenMobile Server バージョン 10.15.0.23 にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。
- 10.15 RP2 または 10.15 RTM を含むそれ以前のリリースからアップグレードする場合は、すべてのクラスターノードをアップグレードするために、クラスター化されたXenMobile展開をアップグレードするには の手順に従ってください。

クラスターモードで構成されたシステムの場合、以下の手順に従って各ノードを順次アップデートしてください。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Server アップデート (.bin) ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、 **>** の順にクリックします。

   ページには、現在インストールされているソフトウェアバージョンと、アップロードしたすべてのアップデート、パッチ、アップグレードのリストが表示されます。

3. で、 をクリックします。 ダイアログボックスが表示されます。
4. をクリックして、Citrixダウンロードページ からダウンロードしたアップデート (.bin) ファイルをアップロードします。
5. をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を確認するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、 > > の順に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.15 Rolling Patch 12 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.15 Rolling Patch 12 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 12 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **証明書ベースの認証における新しい強力な証明書マッピングのサポート**

  強力なマッピング要件を満たす証明書の発行において、より高い柔軟性を可能にする新しいマッピング方法が導入されました。XenMobile Server は、証明書のサブジェクト代替名 (SAN) に `URL=tag:microsoft.com`、`2022-09-14:sid:<user's SID>` を追加するようになりました。

  - 既存ユーザーに対してこの機能を有効にするには、顧客管理者はクライアントプロパティ `MICROSOFT_CERTIFICATE_STRONG_MAPPING` を追加する必要があります。詳細については、「クライアントプロパティ」を参照してください。
  - 強力な証明書マッピングは、**Windows Server 2019 以降**でのみサポートされています。詳細については、「Microsoft Strong Mapping」を参照してください。

- **iOS 26 のサポート**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、iOS 26 と互換性があります。

- **Android 16 のサポート**

  XenMobile Server および Citrix Mobile 生産性向上アプリは、Android 16 を実行している Android Enterprise デバイスをサポートするようになりました。セキュリティとプライバシーの詳細については、「Android 開発者向けドキュメント」を参照してください。

- **構成ポリシーのテキストボックスの管理**

  お客様が **Knox Service Plugin** を **Managed Configuration policy** とともに使用する場合、**Separated Apps Policies** のすべてのテキストボックスの最大文字長は 8,192 文字に増加します。

- **Secure Hub APNs 証明書の更新**

  XenMobile Server 10.15 用の Secure Hub Apple Push Notification service (APNs) 証明書は、January 4, 2026 に期限切れになります。このアップデートにより、Secure Hub APNs 証明書は、November 9, 2026 まで有効な新しい証明書に自動的に更新されます。

解決済みの問題

- マウスの右クリックと貼り付けでパスワードを入力すると、XenMobileポータルのサインインボタンがグレー表示になります。
- iOSユーザーはSecure Mail/Secure Webアプリケーションを起動できず、Secure Mail/Secure WebからSecure Hubにリダイレクトされると「開けません」というエラーが発生します。
- Device Enrollment Program (DEP) デバイスは、登録プロファイルが**MDM-only**として構成されている場合でも、**MDM+MAM**登録を継続して実行します。
- XenMobile MDMソリューションでWindowsクライアントを登録すると、デリバリーグループの展開が失敗します。その結果、プッシュされたポリシーを適用するには手動同期操作が必要になります。回避策として、単一デバイスへの手動展開が必要になります。
- iOSデバイスにアンインストールされたアプリケーションのApp Lockポリシーがある場合、デバイスは「Guided Access app is Unavailable. Please contact your administrator」というエラーでロックされ、強制再起動後もタッチスクリーンが応答しなくなります。

XenMobile Server 10.15.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Serverのアップデートをインストールする

> **重要：**

> - このアップデートをインストールする前に、XenMobile Serverバージョン10.15.0.23にアップグレードしていることを確認してください。また、現在の設定のスナップショットを取得し、データベースのバックアップを作成してください。

- 10.15 RP2または10.15 RTMを含むそれ以前のリリースからアップグレードする場合は、クラスター化されたXenMobile展開をアップグレードするにはの手順に従って、すべてのクラスターノードをアップグレードしてください。

クラスターモードで構成されたシステムの場合、各ノードを順次更新するには、次の手順に従ってください。

1. Citrix® Webサイトでアカウントにサインインし、XenMobile Serverアップデート（.bin）ファイルを適切な場所にダウンロードします。
2. ノードのXenMobile Serverコンソールで、**Settings > Release Management**をクリックします。

   リリース管理ページには、現在インストールされているソフトウェアバージョンと、アップロードしたすべてのアップデート、パッチ、アップグレードのリストが表示されます。
3. リリース管理で、「**更新**」をクリックします。「更新」ダイアログボックスが表示されます。
4. Citrixダウンロードページからダウンロードした更新 (.bin) ファイルをアップロードするには、「**参照**」をクリックします。
5. 「**更新**」をクリックし、プロンプトが表示されたら、コマンドラインを使用してXenMobile Serverノードを再起動します。

パッチの展開を検証するには

このパッチをインストールした後、管理者としてXenMobile Serverコンソールにサインインし、**設定 > リリース管理 > 更新**に移動します。このページには、最近インストールされたパッチの詳細が表示されます。

XenMobile Server 10.15 ローリングパッチ 11 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.15 ローリングパッチ 11 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 ローリングパッチ 11 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

修正された問題

- 展開スケジュールで展開条件が「以前の展開が失敗した場合のみ」に設定されている場合、再登録時に一部のポリシーがAEデバイスに展開されません。
- 多数のペイロード証明書がAEデバイス用に生成されます。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノート を参照してください。

XenMobile Server 10.15 Rolling Patch 10 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.15 Rolling Patch 10 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 10 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

Secure Hub APNs 証明書の更新: XenMobile Server 10.15 用の Secure Hub Apple Push Notification service (APNs) 証明書は、February 9, 2025 に期限切れになります。このアップデートにより、Secure Hub APNs 証明書は、January 4, 2026 まで有効な新しい証明書に自動的に更新されます。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノート を参照してください。

XenMobile Server 10.15 ローリングパッチ 9 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.15 ローリングパッチ 9 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 ローリングパッチ 9 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **Android 15 のサポート**: XenMobile Server および Citrix Mobile 生産性向上アプリは、Android Enterprise デバイスの Android 15 へのアップデートをサポートするようになりました。セキュリティとプライバシーの利点の詳細については、Android 開発者向けドキュメントを参照してください。
- **iOS 18 のサポート**: XenMobile® Server および Citrix Mobile 生産性向上アプリは iOS 18 と互換性がありますが、現在のところ、iOS 18 のすべての新機能はサポートしていません。
- **macOS 15 のサポート**: XenMobile Server および Citrix Mobile 生産性向上アプリは macOS 15 と互換性がありますが、現在のところ、macOS 15 のすべての新機能はサポートしていません。
- **デバイスの紛失モード API を含めるように公開 REST API ドキュメントを更新**: 公開 REST API ドキュメントに紛失モード API を追加しました。
- **API 呼び出しを URL ではなく POST ボディにするように変更**: 公開 REST API ドキュメントで、API 呼び出しを URL ではなくリクエストボディにデータを含めるように更新しました。

- **構成ポリシーのテキストボックスの管理**: マネージド構成ポリシーの下にある**アプリケーション管理ポリシー**ページのすべてのテキストボックスの最大文字長が 4,096 文字に増加しました。

修正された問題

- Secure Hub ストアで、新しいバージョンの MAM SDK 対応アプリの**更新**オプションが利用できません。
- SQL Server がアラートメッセージをトリガーしたときに発生するパフォーマンスの問題により、XenMobile Server は新しい Android Enterprise デバイスを正常に登録できません。
- お客様が FIPS 設定を **true** に有効にしているにもかかわらず、ログには無効として表示され続けています。さらに、お客様が CLI を介してデータベース設定を変更しようとすると、XenMobile Server はデータベースへの接続を確立できず、更新が適用されません。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.15 Rolling Patch 8 リリース のリリースノート

本リリースノートでは、XenMobile Server 10.15 Rolling Patch 8 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 8 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

修正された問題

- プロキシが構成されている場合、HTTP v1 API を使用する Firebase Cloud Messaging が正常に機能しません。

XenMobile Server 10.15.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.15 ローリングパッチ 7 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.15 ローリングパッチ 7 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 ローリングパッチ 7 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **iOS 17.4 以降でのサードパーティ製アプリのブロックのサポート:** 制限ポリシーに、新しい設定 **代替アプリマーケットプレイス** が追加されました。これにより、Web からの代替マーケッ

トプレイスアプリのインストールを防止し、インストール済みの代替マーケットプレイスアプリがアプリをインストールするのを防止します。詳しくは、「制限デバイスポリシー」を参照してください。

- **レガシー MDX モードで公開されている MDX アプリがある場合に XMS コンソールにアラートを表示:** レガシー MDX モードで公開されている MDX アプリがある場合、XenMobile Server コンソールにアラートが表示されます。詳しくは、「サーバープロパティ」の「**レガシー MDX 非推奨アラート**」を参照してください。
- **Firebase Cloud Messaging が新しい http v1 API を使用するように移行をサポート:** HTTP 用の FCM レガシー API は、Google により June 21, 2024 に非推奨になります。FCM が新しい API で適切に動作するように、サービスアカウントキーの JSON ファイルをアップロードするための新しいフィールド **Service Account Key File** が Firebase Cloud Messaging ページに追加されました。詳細については、「Firebase Cloud Messaging」を参照してください。

  XenMobile Server には新しいプロパティ `afw.fcm.httpv1.migration` があり、Firebase Cloud Messaging を新しい HTTP v1 API で使用できます。このプロパティのデフォルト値は **False** です。詳しくは、「サーバープロパティ」を参照してください。

  XenMobile Server 10.15 ローリングパッチ 7 以降で FCM API V1 を有効にするには、Knowledge Center の記事 CTX677031 を参照してください。

修正された問題

- Apple Business Manager (ABM) 共有 iPad の場合、XenMobile® Server は、登録前にサーバーのデータベースに存在しないログインユーザーを「anonymous」と表示します。
- MacOS と iOS の両プラットフォームをサポートする公開 VPP アプリが XenMobile に同期されると、iOS プラットフォームのみが表示され、MacOS プラットフォームが欠落します。
- XenMobile Server 上の一部の iOS 公開アプリが Apple Store で見つかりません。
- XenMobile Server 10.15 RP6 にアップグレードした後、DEP 設定「構成がセットアップを完了するまで待機」が有効にならず、ポリシーを受信するのを待たずに DEP セットアップアシスタンスページがすぐに表示されます。
- アップグレード後に XenMobile Server コンソールにサインインすると、「管理」タブにエラーメッセージ「**java.util.ConcurrentModificationException**」が表示されます。
- XenMobile Server 10.15 RP6 にアップグレードした後、オプションの Web リンクが継続的に再インストールされます。
- XenMobile Serverコンソール > **制限** > **Android Enterprise** で、ポリシー設定「**モバイルネットワークの構成**」のツールチップの説明がドイツ語で正しくありません。

XenMobile Server 10.15.0 の以前のローリングパッチについては、を参照してください。(/ja-jp/xenmobile/server/release-notes.html).

XenMobile Server 10.15 Rolling Patch 6 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.15 Rolling Patch 6 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 6 ソフトウェアバイナリは、サインインしてダウンロード からダウンロードできます。

新機能

- **Secure Hub APNs 証明書の更新**

  XenMobile Server 10.15 用の Secure Hub Apple Push Notification Service (APNs) 証明書は、March 12, 2024 に期限切れになります。このアップデートにより、Secure Hub APNs 証明書は、February 9, 2025 に期限切れとなる新しい証明書に自動的に更新されます。

- **iOS の Webclip ポリシー設定に新しいフィールド「プロファイルスコープ」を追加**

  iOS デバイスの場合、Webclip デバイスポリシーの**ポリシー設定**に、**プロファイルスコープ**という新しいフィールドが追加されました。この機能により、ポリシーをユーザーに適用するかシステムに適用するかを選択できます。詳細については、「Webclip デバイスポリシー - iOS 設定」を参照してください。

- **REST API を使用したパブリックストアアプリの展開ルールの更新**

  Add New Public Store App および **Update Public Store App** REST API に、**rules** という新しいフィールドが追加されました。この機能により、パブリックストアアプリの展開ルールを更新できます。詳細については、「Public REST API ドキュメント」を参照してください。

- **アプリ属性デバイスポリシーが新しい iOS アプリ属性をサポート**

  iOS デバイスにインストールされているアプリに対して、次の属性を指定できるようになりました。

  - **削除可能なアプリ:** 管理対象アプリである場合に、ユーザーがアプリを削除できるかどうかを指定します。
  - **関連ドメインの直接ダウンロードを有効にする:** アプリがドメインで直接、要求されたサイト関連付け検証を実行できるかどうかを指定します。
  - **関連ドメイン:** アプリに追加する関連ドメインを指定します。

  詳細については、「アプリ属性デバイスポリシー」を参照してください。

- **新しいKnox Platform for Enterprise Keyデバイスポリシーを追加**

Knox Platform for Enterprise Keyという新しいデバイスポリシーが追加されました。このポリシーを使用すると、必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供し、KPEライセンスを使用してSamsungデバイスのセキュリティを強化できます。詳細については、Knox Platform for Enterprise Keyデバイスポリシーを参照してください。

- **共有iPad向けApple Business Managerのサポート**

  XenMobile Server 10.15 RP6以降、共有iPadはXenMobile ServerでApple Business Manager (ABM) をサポートします。この機能により、ABMアカウントを使用して共有iPadにサインインし、それらを使用できます。詳細については、共有iPadの構成を参照してください。

  > **注：**
  >
  > 現在、この機能には制限があり、ログインしたユーザーがXenMobile® Serverコンソールに「Anonymous」と表示される場合があります。その結果、「すべてのユーザーを削除」などの特定のセキュアな操作が、特に共有iPadとして使用されているデバイスで実行できない場合があります。この問題を回避するには、特にABMの共有iPadを使用している場合、DEPユーザー（管理対象Apple ID）をXenMobile Serverコンソールに手動で追加することをお勧めします。恒久的な解決策は今後のリリースに含まれる予定です。

- **共有iPad向けに「すべてのユーザーを削除」という新しいセキュリティアクションを追加**

  XenMobile Server 10.15 RP6以降、XenMobile Serverの共有iPad向けに**すべてのユーザーを削除**という新しいセキュリティアクションが追加されました。この機能により、デバイス上のすべてのユーザーを削除できます。詳細については、共有iPadのセキュリティアクションを参照してください。

- **新しいデリバリーグループのベースとしてデリバリーグループを複製**

  この機能を使用すると、複数のポリシー、アプリ、およびアクションを含む複雑なデリバリーグループをコピーできます。その後、登録プロファイルや新しいActive Directoryユーザーセットの追加など、コピーを編集できます。詳細については、デリバリーグループの複製を参照してください。

- **iOSでのオプションアプリの自動更新のサポート**

  XenMobile Server 10.15 RP6以降、`apple.ios.optional_app_update`という新しいサーバープロパティが追加されました。このプロパティを使用すると、iOSのオプションアプリを自動更新できます。`apple.ios.optional_app_update`のデフォルト値は`False`に設定されています。詳細については、サーバープロパティを参照してください。

オプションのボリューム購入アプリの自動更新の詳細については、アプリの更新を確認するを参照してください。

- **データベースアップグレードメカニズムの最適化**

  データベースのアップグレードプロセスが最適化され、各クラスターが1回だけアップグレードされるようになりました。これにより、HAクラスターでのローリングパッチ更新中のダウンタイムを最小限に抑えることができます。

修正された問題

- ABMまたはASM構成を使用している場合、iOS共有デバイスにWebclipデバイスポリシーを展開できません。

XenMobile Server 10.15.0の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.15 Rolling Patch 5 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.15 Rolling Patch 5 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 5 ソフトウェアバイナリは、サインインしてダウンロードからダウンロードできます。

新機能

- **Android Enterprise の 802.1x 設定に新しい必須フィールド「Domain」を追加**

  Android Enterprise プラットフォームのネットワークポリシー設定ページに、**802.1x EAP** 認証タイプ向けの新しいフィールド **Domain** が追加されました。詳しくは、「Android Enterprise の 802.1x 設定」を参照してください。

  XenMobile Server には新しいプロパティ `afw.network.domain.support` があり、これにより、**Android Enterprise の 802.1x 設定**に *Domain* フィールドが追加されます。このプロパティのデフォルト値は **True** です。詳しくは、「サーバープロパティ」を参照してください。

- **iOS の「OSアップデートの制御」ポリシーに新しいオプション「OS updates version」を追加**

  iOS プラットフォームの「**OSアップデートの制御**」ポリシーで、**OS update frequency** フィールドの後に新しいオプション「**OS updates version**」が追加されました。このオプションを使用すると、監視対象の iOS デバイスを更新するために使用する OS バージョンを指定できます。詳しくは、「iOS 設定」を参照してください。

- **iOS の制限ポリシーとExchangeポリシーに新しい設定を追加**

- iOS の Exchange ポリシーに新しい設定「**Mail Dropを許可**」を追加しました。詳しくは、「Exchangeデバイスポリシー - iOS設定」を参照してください。
- iOS の制限ポリシーに以下の新しい設定を追加しました:
  - ペアリングされていないデバイスによるリカバリへの起動を許可
  - 迅速なセキュリティ対応をインストール
  - 迅速なセキュリティ対応を削除
  - メールプライバシー保護を許可
  - NFC
  - App Clip を許可する
  - Appleパーソナライズド広告を許可する
  - 自動ロック解除

  詳細については、制限デバイスポリシー - iOS設定を参照してください。

- **OSの更新**
  - **Android 14のサポート:** XenMobile ServerおよびCitrix Mobile生産性向上アプリは、Android EnterpriseデバイスのAndroid 14への更新をサポートするようになりました。セキュリティとプライバシーの利点の詳細については、Androidドキュメントを参照してください。
  - **iOS 17のサポート:** XenMobile® ServerおよびCitrix Mobile生産性向上アプリはiOS 17と互換性がありますが、現時点では新しいiOS 17の機能はサポートしていません。
  - **macOS 14のサポート:** XenMobile ServerおよびCitrix Mobile生産性向上アプリはmacOS 14と互換性がありますが、現時点では新しいmacOS 14の機能はサポートしていません。

修正された問題

- XenMobile Server 10.15 RP3または10.15 RP4にアップグレードした後、**構成** > **アプリ**ページの**Android Enterprise** > **管理対象Google Playストアアプリ**で、**アプリの整理**ボタンが利用できません。
- XenMobile Server 10.15 RP3または10.15 RP4にアップグレードした後、**Android Enterprise**プラットフォームのWi-Fiポリシーを構成している間、**CA証明書**ドロップダウンメニューに値が表示されません。**証明書の選択**オプションのみが表示されます。

XenMobile Server 10.15.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.15 ローリングパッチ4リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.15 ローリングパッチ4の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 ローリングパッチ4のソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

- **デバイスとアプリのレポートへのアクセス**

  以前は、**デバイスとアプリ**のレポートページには、ロールベースのアクセス制御 (RBAC) が適用されている場合でも、ユーザーグループに関係なく、すべてのユーザーのすべてのデバイスとアプリに関する情報が表示されていました。

  XenMobile Server 10.15 ローリングパッチ4リリース以降、**デバイスとアプリ**のレポートページには、RBACロールが管理権限を持つ**特定のユーザーグループ**への設定で定義されたユーザーグループに固有のデバイスとアプリが表示されます。RBACを使用したロールの構成について詳しくは、「RBACを使用したロールの構成」を参照してください。

- **OSアップデートの制御デバイスポリシーをシステムデフォルトにリセットするサポート**

  XenMobile Server 10.15 ローリングパッチ4リリース以降、Android Enterprise**のOSアップデートの制御**ページにある**システムアップデートポリシー**ドロップダウンリストに新しい値**デフォルト**が追加されました。この機能により、システムアップデートポリシーをシステムデフォルトにリセットできます。詳しくは、「OSアップデートの制御デバイスポリシー」を参照してください。

- **iOS用Exchangeデバイスポリシー設定にOAuthサインインURLとOAuthトークン要求URLの新しいフィールドを追加**

  XenMobile Server 10.15 ローリングパッチ4リリース以降、**Exchangeポリシー** > **iOS** > **OAuthを使用**ラジオボタンの下に、**OAuthサインインURL**と**OAuthトークン要求URL**フィールドが追加されました。詳しくは、「Exchangeデバイスポリシー」を参照してください。

- **iOS用同期済みExchangeサービスを同期または上書きするサポート**

  XenMobile Server 10.15 ローリングパッチ4リリース以降、関連する設定を有効にすることで、iOS用の以下の同期済みExchangeサービスを同期するか上書きするかを選択できます。

  - カレンダー
  - 連絡先
  - メール

- ノート
- リマインダー

詳細については、Exchangeデバイスポリシーを参照してください。

- **iOSデバイスでのeSIMのサポート**

  XenMobile Serverには新しいプロパティ`ios.esim.support`があり、これによりXenMobile ServerはiOSデバイスからeSIM情報を取得し、eSIM関連のデバイスプロパティをユーザーインターフェイスに表示できます。このプロパティのデフォルト値は**True**です。詳細については、サーバープロパティを参照してください。

XenMobile Server 10.15.0の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

XenMobile Server 10.15 ローリングパッチ 3 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.15 ローリングパッチ 3 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 ローリングパッチ 3 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **XenMobile Serverでの混合ライセンスタイプのサポート。** この機能により、お客様はXenMobile ServerまたはCitrix Licensing Serverを使用して、XenMobileライセンスタイプとエディションの混合をアクティブ化できます。詳細については、「別のライセンスをアクティブ化するには」を参照してください。
- **macOSデバイスでのエンタープライズアプリのサポート。** XenMobile Serverには新しいプロパティ`mac.app.push`があり、macOSを実行しているデバイスでのエンタープライズアプリのサポートを有効にします。このプロパティのデフォルト値は **True** です。詳細については、「サーバープロパティ」を参照してください。

修正された問題

- **管理対象のGoogle Playアカウント**からアプリをダウンロードできません。
- XenMobile® Serverコンソールで、Rapid Security Response (RSR) のバージョンが表示されません。
- Androidデバイスで、ユーザーがレガシーMDX ToolkitからMAM SDKに切り替えると、Secure Mailアプリが Secure Hubストアから削除されます。

- XenMobile Server 10.15 RP2にアップグレードした後、「**制限付きアプリの使用**」を使用する既存のiOS制限デバイスポリシーがiOSデバイスに展開されません。

XenMobile Server 10.15 Rolling Patch 2 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.15 Rolling Patch 2 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 2 ソフトウェアバイナリは、ダウンロードにサインインからダウンロードできます。

新機能

XenMobile Analyzer Tool の廃止。 頻繁かつ安定したリリースサイクルにより、XenMobile Analyzer Tool は不要になりました。Citrix は March 31, 2023 をもってこのサービスを終了しました。Citrix XenMobile コンソールまたは Citrix NetScaler Gateway で利用可能な接続チェックを使用することをお勧めします。詳細については、「接続チェック」を参照してください。

修正された問題

- APK Signature Scheme v2 以降のアルゴリズムを使用して、Android プラットフォームでエンタープライズアプリを構成できません。
- NetScaler で nFactor 認証ポリシーが使用されている場合、Android および iOS デバイスで MAM にアクセスできません。
- XenMobile Server バージョン 10.14 以降で Citrix Gateway 認証の構成スクリプトをエクスポートすると、スクリプトが切り詰められ、機能しません。
- XenMobile Server で、説明に **\b** が含まれる同期済み VPP アプリを再編集できません。
- XenMobile Server バージョン 10.15 以降では、Online Certificate Status Protocol (OCSP) が要求に応答しません。
- XenMobile® Server で、Windows 11 を実行しているデバイスを登録できません。

XenMobile Server 10.15 Rolling Patch 1 リリースノート

これらのリリースノートでは、XenMobile Server 10.15 Rolling Patch 1 の機能強化、修正された問題、および既知の問題について説明します。XenMobile Server 10.15 Rolling Patch 1 ソフトウェアバイナリは、ダウンロードにサインイン からダウンロードできます。

新機能

- **ネットワークアクセスコントロール。** ネットワークアクセスコントロール (NAC) ソリューションを使用して、Android および Apple デバイスの XenMobile デバイスセキュリティ評価を拡張します。NAC ソリューションは、XenMobile セキュリティ評価を使用して認証決定を容易

にし、処理します。NAC アプライアンスを構成すると、XenMobile で構成したデバイスポリシーと NAC フィルターが適用されます。詳しくは、「ネットワークアクセスコントロール」を参照してください。

- **Secure Hub APNs 証明書の更新。** XenMobile Server 10.15 の Secure Hub Apple Push Notification Service (APNs) 証明書は、April 8, 2023 に期限切れになります。この更新プログラムは、March 12, 2024 に期限切れになる Secure Hub APNs 証明書を更新します。

修正された問題

- Android Enterprise デバイスで管理対象構成ポリシーを編集または展開すると、エラーが発生します。
- MAM 専用モードで登録されている iOS デバイスでは、Secure Hub ストアからエンタープライズアプリまたは MDX アプリをインストールできません。
- アプリのトラック ID を構成した後、XenMobile® Server コンソールでアプリの予期されるプレビューバージョンを表示できません。代わりに、アプリの製品版が表示されます。
- XenMobile Server では、プロビジョニングプロファイルデバイスポリシーが保留状態の場合、Secure Hub ストアから MDX ラップアプリをインストールできません。
- MDM プロファイル更新後、ABM 共有 iPad は管理対象外ステータスになります。

XenMobile Server 10.14 Rolling Patch 13 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.14 Rolling Patch 13 の機能強化、修正された問題、および既知の問題について説明します。

新機能

Secure Hub APNs 証明書の更新:

XenMobile Server 10.14 用の Secure Hub Apple Push Notification Service (APNs) 証明書は、March 12, 2024 に期限切れになります。この更新により、Secure Hub APNs 証明書は、February 9, 2025 に期限切れとなる新しい証明書に自動的に更新されます。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.14 Rolling Patch 13 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.14 Rolling Patch 13 の機能強化、修正された問題、および既知の問題について説明します。

新機能

Secure Hub APNs 証明書の更新:

XenMobile Server 10.14 用の Secure Hub Apple Push Notification Service (APNs) 証明書は、March 12, 2024 に期限切れになります。この更新により、Secure Hub APNs 証明書は、February 9, 2025 に期限切れとなる新しい証明書に自動的に更新されます。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.14 Rolling Patch 12 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.14 Rolling Patch 12 の機能強化、修正された問題、および既知の問題について説明します。

修正された問題

- **Managed Google Play Accounts** からアプリをダウンロードできません。
- XenMobile Server 10.14 RP11 にアップグレードした後、既存の iOS 制限ポリシーがデバイスに展開されません。
- モバイルデバイスを Secure Hub に登録すると、Secure Hub ストアと管理対象 Google Play ストアにアプリが表示されません。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「Rolling Patches のリリースノート」を参照してください。

XenMobile Server 10.14 ローリングパッチ 11 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.14 ローリングパッチ 11 の機能強化、修正された問題、および既知の問題について説明します。

修正された問題

- Androidプラットフォームで、アルゴリズムAPK Signature Scheme v2以降を使用してエンタープライズアプリを構成できません。

- XenMobile Serverで、説明に \b が含まれる同期済みVPPアプリを再編集できません。
- XenMobile Serverバージョン10.14 RP9以降で、オンライン証明書状態プロトコル（OCSP）が要求に応答しません。
- XenMobile® Serverで、Windows 11を実行しているデバイスを登録できません。
- XenMobile Serverコンソールで、Rapid Security Response（RSR）バージョンを確認できません。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.14 Rolling Patch 10 リリースに関するリリースノート

このリリースノートでは、XenMobile Server 10.14 Rolling Patch 10 の機能強化、修正された問題、および既知の問題について説明します。

新機能

- **Secure Hub APNs証明書の更新。** XenMobile Server 10.14 の Secure Hub Apple Push Notification Service (APNs) 証明書は、April 8, 2023 に期限切れになります。この更新により、March 12, 2024 に期限切れとなるSecure Hub APNs証明書が更新されます。
- **XenMobile Analyzer Tool の廃止。** 頻繁かつ安定したリリースサイクルにより、XenMobile Analyzer Tool は不要になりました。Citrix は、March 31, 2023 をもってこのサービスを終了することを決定しました。Citrix XenMobile コンソールまたはCitrix NetScaler Gateway で利用可能な接続チェックを使用することをお勧めします。詳細については、「接続チェック」を参照してください。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

修正された問題

- MDMプロファイルの更新後、ABM共有iPadが管理対象外ステータスになります。
- MAM専用モードで登録されているiOSデバイスでは、Secure Hubストアからエンタープライズアプリまたはmdxアプリをインストールできません。
- NetScalerでnFactor認証ポリシーが使用されている場合、AndroidおよびiOSデバイスでMAMにアクセスできません。
- XenMobile Serverバージョン10.14以降でCitrix Gateway認証の構成スクリプトをエクスポートすると、スクリプトが切り詰められ、機能しません。

XenMobile Server 10.14 ローリングパッチ 9 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.14 ローリングパッチ 9 の機能強化、修正された問題、および既知の問題について説明します。

新機能

ネットワークアクセスコントロール。 ネットワークアクセスコントロール (NAC) ソリューションを使用して、Android および Apple デバイスの XenMobile デバイスセキュリティ評価を拡張します。NAC ソリューションは、XenMobile セキュリティ評価を使用して認証決定を容易にし、処理します。NAC アプライアンスを設定すると、XenMobile で設定したデバイスポリシーと NAC フィルターが適用されます。詳しくは、「ネットワークアクセスコントロール」を参照してください。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

修正された問題

- XenMobile Server バージョン 10.14 では、ライセンスの有効期限が通知期間外であっても、ライセンスの有効期限切れ通知が届きます。
- 一部のアプリでは、インストールされているバージョンが最新であっても、Secure Hub アプリストアに「**保留中の更新**」ステータスが表示されます。
- XenMobile® Server では、ドイツ語ロケールで制限デバイスポリシーを作成または編集できません。
- XenMobile Server バージョン 10.14 では、DEP 以外の iOS デバイスの場合、「**所有者**」タブが空白で表示されます。
- **サブジェクトの別名タイプ**が「*なし*」でない場合、SCEP デバイスポリシーが失敗します。
- Android Enterprise デバイスで管理対象構成ポリシーを編集または展開すると、エラーが発生します。
- MAM 専用モードで登録されている iOS デバイスでは、Secure Hub アプリストアからエンタープライズアプリまたは MDX アプリをインストールできません。
- アプリのトラック ID を構成した後、XenMobile Server コンソールでアプリの期待されるプレビューバージョンを表示できません。代わりに、アプリの製品バージョンが表示されます。
- XenMobile Server では、プロビジョニングプロファイルデバイスポリシーが保留状態の場合、Secure Hub ストアから MDX ラップアプリをインストールできません。

XenMobile Server 10.14 ローリングパッチ 8 リリースのリリースノート

このリリースノートでは、XenMobile Server 10.14 ローリングパッチ 8 の機能強化、修正された問題、および既知の問題について説明します。

新機能

Windows Information Protection ポリシーのサポートは非推奨になりました。Windows の発表に従い、XenMobile Server は Windows Information Protection (WIP) のサポートを非推奨にしました。WIP のサポートは、**windows.wip.deprecation** というサーバープロパティを追加することで非推奨になりました。このプロパティの値はデフォルトで **True** に設定されています。詳細については、「サーバープロパティ」を参照してください。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

修正された問題

- XenMobile® Server で、ドイツ語ロケールで **管理対象アプリを自動的に更新** ポリシーを作成または編集できません。

XenMobile Server 10.14 ローリングパッチ 7 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.14 ローリングパッチ 7 の機能強化、修正された問題、および既知の問題について説明します。

新機能

- **OSのアップデート**
  - **iOS 16のサポート。** XenMobile® ServerおよびCitrix Mobile生産性向上アプリはiOS 16と互換性がありますが、現時点ではiOS 16の新機能はサポートしていません。
  - **Android 13のサポート。**XenMobile Serverは、Android EnterpriseデバイスのAndroid 13へのアップデートをサポートするようになりました。セキュリティとプライバシーの利点の概要については、Androidドキュメントを参照してください。
- **非推奨の機能。** 以下の機能のサポートは削除されました。
  - RBACロール - 共有デバイスおよびCOSUデバイスの登録者
  - Android - SonyおよびHTC
  - 高セキュリティ登録モード
  - 派生資格情報

  - SEAMS
  - Windows Phoneデバイス ,
  - 汎用、DigiCert管理、およびEntrustアダプターPKIエンティティ。

  詳細については、非推奨を参照してください。

- **モバイルサービスプロバイダー (MSP) インターフェイスのサポートは非推奨になりました。** MSPのサポートは、コンソールからMSPインターフェイスを削除する新しいサーバープロパティ `deprecate.mobile.service.provider` を追加することで非推奨になりました。このプロパティはデフォルトで**True**に設定されています。詳細については、「サーバープロパティ」を参照してください。
- **Windows 10デバイス向けの*WiFi Sense*ホットスポットへの*自動接続を許可する*制限ポリシーのサポートは削除されました。** 詳細については、「Windowsデスクトップ/タブレット設定」を参照してください。
- **Nexmo SMSゲートウェイのサポートは非推奨になりました。** Nexmo SMSのサポートは、デフォルトで**True**に設定されているサーバープロパティ `deprecate.carrier.sms.gateway` を追加することで非推奨になりました。Nexmo SMSはセルフヘルプポータルでも非推奨になりました。詳細については、「通知」を参照してください。
- **GoogleによるAPIの非推奨化。** Googleは、XenMobile Serverでアプリのカテゴリとライセンスに使用されるいくつかのAPIを非推奨にしています。以下の変更が適用されます。
  - 承認するのではなく、追加するアプリを選択するようになりました。「管理対象アプリストアアプリ」を参照してください。
  - カテゴリではなく、コレクションにアプリを整理するようになりました。「アプリの整理」を参照してください。
  - アプリライセンスをユーザーから関連付け解除することはできなくなりました。「アプリの追加」を参照してください。
- **Android Enterprise管理対象アプリを自動的に更新するための優先度を構成します。** Android Enterprise管理対象アプリが低優先度または高優先度で自動的に更新されるかどうかを指定します。自動更新を延期することもできます。詳細については、「管理対象アプリの自動更新デバイスポリシー」を参照してください。

XenMobile Server 10.14.0の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

修正された問題

- 一部のAndroidデバイスでは、一部の公開アプリがGoogle Playで利用できない場合、Secure Hubにアクセスできません。
- 特定のmacOSデバイスでは、SSL証明書の更新後にインストールされたプロファイルと証明書が自動的に削除されます。
- XenMobile Serverコンソールでは、名前に**/**記号が含まれる制限デバイスポリシーを編集できません。
- リリースされたDEPデバイスがXenMobile Serverコンソールに表示されたままになります。
- Secure Hub Storeにアクセスできません。次のエラーが表示されます: **サインオンの有効期限が切れました。続行するには、もう一度サインオンしてください。**

XenMobile Server 10.14 ローリングパッチ6リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.14 ローリングパッチ6の機能強化、修正された問題、および既知の問題について説明します。

新機能

新しい制限ポリシーを追加しました。 制限ポリシーに、**仕事用プロファイルからのコピーと貼り付けを許可**および**個人用プロファイルからのデータ共有を許可**を追加しました。個人用プロファイルから仕事用プロファイルへのコピー、貼り付け、インポートを制限するには、これらのポリシーを**OFF**に設定します。詳細については、「制限デバイスポリシー」を参照してください。

XenMobile Server 10.14.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

修正された問題

- XenMobile® Serverでは、一部のVPPアプリの正しいバージョンが自動的に更新されません。
- XenMobile Serverバージョン10.14では、特定のActive Directoryユーザーを削除できません。
- iOS 15を実行しているデバイスの新規登録時に、接続タイプが**AlwaysOn IKEv2 Dual Configuration**に設定されている場合、VPNポリシーの展開が失敗します。

XenMobile Server 10.14 ローリングパッチ 5 リリース のリリースノート

このリリースノートでは、XenMobile Server 10.14 ローリングパッチ 5 の機能強化、修正された問題、および既知の問題について説明します。

新機能

- **Google Analytics を有効にする**。XenMobile Server で Google Analytics を有効にするには、サーバープロパティ **xms.ga.enabled** の値を **True** に設定します。デフォルト値は **True** です。
- **Secure Hub APNs 証明書の更新**。XenMobile Server 10.14 の Secure Hub Apple Push Notification Service (APNs) 証明書は May 7, 2022 に期限切れになります。この更新により、April 8, 2023 に期限切れとなる Secure Hub APNs 証明書が更新されます。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「」を参照してください。(/ja-jp/xenmobile/server/release-notes.html).

修正された問題

- XenMobile® Server では、デバイス上の CA 更新後にデバイス証明書発行者 CA が更新されません。
- 一部のデバイスでは、SQL データベースに 2 つの証明書エントリがあり、エラーが発生します。
- XenMobile Server バージョン 10.14 では、プロビジョニングプロファイルのデバイスポリシーを編集できません。
- XenMobile Server で、ShareFile Enterprise からコネクタに変更しても、デリバリーグループの下の GUI が更新されません。

XenMobile Server 10.14 Rolling Patch 4 リリースに関するリリースノート

これらのリリースノートでは、XenMobile Server 10.14 Rolling Patch 4 の機能強化、修正された問題、および既知の問題について説明します。

新機能

WSDLサービスを有効にする。 XenMobile ServerでWSDLサービスを有効にするには、サーバープロパティ`wsdl.service.enabled`の値を**True**に設定します。ActiveSyncゲートウェイコネクタを使用している場合に必要です。デフォルト値は**False**です。

XenMobile Server 10.14.0 の以前のローリングパッチについては、ローリングパッチのリリースノートを参照してください。

修正された問題

- 一部のAndroid Enterpriseデバイスでは、デリバリーグループと割り当てられたポリシーまたはアプリが断続的に適用されません。

- XenMobile Serverバージョン10.13では、ストレージゾーンコネクタのみを使用してストレージゾーンコントローラを接続および構成できません。
- MDMのみモードに登録されているiOSデバイスでは、Secure HubによってApp Storeから開かれたブラウザ経由でアプリを追加できません。次のエラーが表示されます: **サインオンの有効期限が切れました。続行するには、もう一度サインオンしてください。**
- XenMobile Serverバージョン10.13 RP1以降では、SNMP監視のXenMobileノード間接続トラップが機能しません。
- XenMobile® Serverでは、W-SUタイムゾーンで誤った時刻が表示されます。

XenMobile Server 10.14 Rolling Patch 3 リリースのリリースノート

これらのリリースノートでは、XenMobile Server 10.14 Rolling Patch 3 の機能強化、修正済みおよび既知の問題について説明します。

このリリースにはバグ修正が含まれています。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

XenMobile Server 10.14 Rolling Patch 2 リリースノート

このリリースノートでは、XenMobile Server 10.14 Rolling Patch 2 の機能強化、修正された問題、および既知の問題について説明します。

XenMobile Server 10.14.0 の以前のローリングパッチについては、「ローリングパッチのリリースノート」を参照してください。

修正された問題

XenMobile® Server では、ピーク時にサーバーノードで高いCPU使用率が観測されます。

XenMobile Server 10.14 Rolling Patch 1 リリースノート

このリリースノートでは、XenMobile Server 10.14 Rolling Patch 1 の機能強化、修正された問題、および既知の問題について説明します。

新機能

- **Windows 11デバイスのサポート。** XenMobileを使用してWindows 11デバイスを管理できるようになりました。詳細については、オペレーティングシステムのサポートリストを参照してください。

- **macOSの接続モードとネットワーク優先順位を構成する。** Wi-Fiデバイスポリシーで、macOSデバイスの**接続モード**設定を有効にして、ユーザーがネットワークに参加する方法を選択します。デバイスは、システム資格情報またはログインウィンドウで入力された資格情報を使用してユーザーを認証できます。複数のネットワークがある場合は、**優先順位**フィールドに数値を入力して、ネットワーク接続の優先順位を設定します。デバイスは、最も小さい数値のネットワークを選択します。詳細については、Wi-FiデバイスポリシーのmacOS設定を参照してください。
- GoogleによるAndroid Enterpriseデバイスでのグループライセンスのサポート終了に伴い、XenMobile Serverはグループライセンスを Googleに同期できなくなります。詳細については、こちらの記事を参照してください。

既知の問題

macOS 11以前からmacOS 12にアップグレードされた登録済みデバイス、またはmacOS 12に新規登録されたデバイスは、デバイスの**システム環境設定 > プロファイル**の下に「未確認」と表示される場合があります。詳細と回避策については、こちらのサポート記事を参照してください。

修正された問題

- iOS 15またはmacOS 12デバイスを登録した後、MDM構成プロファイルが**未確認**と表示されます。
- XenMobile® Serverコンソールで、アプリの設定を変更してすべてのプラットフォームをクリアして保存すると、そのアプリは**構成 > アプリ**に表示されません。
- Android EnterpriseプラットフォームでCitrix®ランチャーを終了できません。次のエラーが表示されます: **パスワードが正しくありません。**
- XenMobile Serverバージョン10.14では、**iOSおよびmacOSプロファイルのインポート**ポリシーを編集できません。

XenMobile Server 10.16 の新機能

Citrix ADC で非推奨となったクラシックポリシーの継続サポート

Citrix は最近、Citrix ADC 12.0 ビルド 56.20 以降、一部のクラシックポリシーベース機能の非推奨化を発表しました。Citrix ADC の非推奨化に関する通知は、Citrix Gateway との既存の XenMobile Server 統合には影響しません。XenMobile Server は引き続きクラシックポリシーをサポートしており、対応は不要です。

非推奨化のお知らせ

段階的に廃止される Citrix XenMobile 機能の事前通知については、「非推奨」を参照してください。

エンドポイントを iOS 14.5 にアップグレードする前に

いずれかのエンドポイントを iOS 14.5 にアップグレードする前に、Citrix はアプリのクラッシュを軽減するために次のアクションを実行することを推奨します。

- Citrix Secure Mail および Secure Web を 21.2.X 以降にアップグレードします。「MDXまたはエンタープライズアプリのアップグレード」を参照してください。
- MDX Toolkit を使用している場合は、すべてのサードパーティ製 iOS アプリケーションを MDX Toolkit 21.3.X 以降でラップします。最新バージョンについては、MDX Toolkit の「ダウンロードページ」を確認してください。

オンプレミスの Citrix ADC をアップグレードする前に

オンプレミスの Citrix ADC を特定のバージョンにアップグレードすると、シングルサインオンエラーが発生する可能性があります。ブラウザで Citrix Files または ShareFile ドメイン URL に「**会社の従業員としてサインイン**」オプションを使用してシングルサインオンすると、エラーが発生します。ユーザーはサインインできません。

この問題を回避するには：Citrix Gateway の ADC CLI から次のコマンドをまだ実行していない場合は、グローバル SSO を有効にするために実行します。

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

詳細については、以下を参照してください。

- 「Citrix ADC リリース (機能フェーズ) 13.1 ビルド 33.52」
- 「影響を受ける SSO 構成」

回避策を完了すると、ユーザーはブラウザで「会社の従業員サインイン」オプションを使用して、SSO経由でCitrix FilesまたはShareFileドメインURLに認証できます。

XenMobile 10.16 (オンプレミス) へのアップグレード前

システム要件が一部変更されました。詳細については、「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. アップグレードするXenMobile® Serverを実行している仮想マシンのRAMが8 GB未満の場合は、RAMを少なくとも8 GBに増やすことをお勧めします。
2. XenMobile Server 10.16の最新バージョンに更新する前に、Citrix License Serverを11.17.2.0 Build 47000以降に更新してください。

   XenMobileの最新バージョンには、Citrix License Server 11.17（最小バージョン）が必要です。

   注：

   XenMobile 10.16のカスタマーサクセスサービス日（以前のSubscription Advantage date）はNovember 15, 2022です。Citrixライセンスのカスタマーサクセスサービス日は、この日付より後である必要があります。

   License Serverでライセンスの横に日付を表示できます。XenMobileの最新バージョンを古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。

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

License Activation Service (LAS)は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。License Activation Serviceが10.15 Rolling Patch 13以降のRolling Patchで有効になっている場合、10.16.0.48に直接アップグレードすると、License Activation Serviceの構成がリセットされます。License Activation Serviceを再構成できるバージョン10.16 Rolling Patch 7以降の10.16 Rolling Patchを適用し続けてください。既存のデバイスには影響ありません。

3. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。

   - Citrix GatewayがSSL永続性のために構成されている場合、すべてのXenMobile Serverノードでポート80を開く必要があります。

4. 推奨事項：XenMobileの更新をインストールする前に、VMの機能を使用してシステムのスナップショットを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に問題が発生した場合でも、完全なバックアップがあれば回復できます。

アップグレードするには

このリリースにより、XenMobileはVMware ESXi 7.0をサポートします。ESXi 7.0をインストールまたはアップグレードする前に、10.14以降にアップグレードしていることを確認してください。

XenMobile 10.15.xまたは10.14.xからXenMobile 10.16に直接アップグレードできます。アップグレードを行うには、利用可能な最新のバイナリをダウンロードしてください。Citrixダウンロードページにアクセスします。**Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**に移動します。ハイパーバイザー用のXenMobile Serverソフトウェアのタイルで、**Download File**をクリックします。

アップグレードをアップロードするには、XenMobileコンソールの**Release Management**ページを使用します。Release Managementページを使用したアップグレードを参照してください。

アップグレード後

送信接続に関連する機能が動作しなくなり、接続構成を変更していない場合は、XenMobile Serverのログで次のようなエラーを確認してください。「VPPサーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません。」.

- 証明書の検証エラーは、XenMobile Serverでホスト名検証を無効にする必要があることを意味します。
- 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検証が有効になっています。
- ホスト名検証によって展開が中断される場合は、サーバープロパティ`disable.hostname.verification`を`true`に変更してください。このプロパティのデフォルト値は`false`です。

プラットフォームの更新

- **Android 14のサポート:** XenMobile ServerおよびCitrix Mobile生産性向上アプリは、Android EnterpriseデバイスのAndroid 14への更新をサポートするようになりました。セキュリティとプライバシーの利点の詳細については、Androidドキュメントを参照してください。
- **iOS 17のサポート:** XenMobile ServerおよびCitrix Mobile生産性向上アプリはiOS 17と互換性がありますが、現時点では新しいiOS 17の機能はサポートしていません。
- **macOS 14のサポート:** XenMobile ServerおよびCitrix Mobile生産性向上アプリはmacOS 14と互換性がありますが、現時点では新しいmacOS 14の機能はサポートしていません。

デバイスとアプリのレポートへのアクセス

以前は、**デバイスとアプリ**のレポートページには、ロールベースのアクセス制御 (RBAC) が適用されている場合でも、ユーザーグループに関係なく、すべてのユーザーのすべてのデバイスとアプリに関する情報が表示されていました。

XenMobile Server 10.16リリース以降、**デバイスとアプリ**のレポートページには、RBACロールが管理権限を持つ**特定のユーザーグループへ**で定義されたユーザーグループに固有のデバイスとアプリが表示されます。RBACを使用したロールの構成の詳細については、RBACを使用したロールの構成を参照してください。

Android Enterprise の 802.1x 設定に新しい必須フィールド「ドメイン」を追加しました

新しいフィールド**ドメイン**が、**802.1x EAP**認証タイプ向けの Android Enterprise プラットフォームのネットワークポリシー設定ページに追加されました。詳細については、「Android Enterprise の 802.1x 設定」を参照してください。

iOS の制限デバイスポリシーと Exchange デバイスポリシーに新しい設定を追加しました

- iOS の Exchange デバイスポリシーに新しい設定**Mail Dropを許可**を追加しました。詳細については、「Exchangeデバイスポリシー - iOS設定」を参照してください。
- iOS の制限デバイスポリシーに以下の新しい設定を追加しました。
  - ペアリングされていないデバイスによるリカバリへの起動を許可する
  - 迅速なセキュリティ対応をインストールする
  - 迅速なセキュリティ対応を削除する
  - メールプライバシー保護を許可する
  - NFC
  - App Clipを許可する
  - Appleパーソナライズ広告を許可する
  - 自動ロック解除

詳細については、「制限デバイスポリシー - iOS設定」を参照してください。

iOS の Exchange デバイスポリシー設定に新しいフィールド OAuth サインイン URL と OAuth トークン要求 URL を追加しました

XenMobile Server 10.16リリース以降、「**OAuthサインインURL**」と「**OAuthトークン要求URL**」フィールドが「**Exchangeポリシー**」>「**iOS**」>「**OAuthを使用**」ラジオボタンの下に追加されました。詳細については、「Exchangeデバイスポリシー」を参照してください。

新しいKnox Platform for Enterprise Keyデバイスポリシーを追加

「**Knox Platform for Enterprise Key**」という新しいデバイスポリシーが追加されました。このポリシーを使用すると、必要なSamsung Knox Platform for Enterprise（KPE）ライセンス情報を提供し、KPEライセンスを使用してSamsungデバイスのセキュリティを強化できます。詳細については、「Knox Platform for Enterprise Keyデバイスポリシー」を参照してください。

デリバリーグループを複製して新しいデリバリーグループのベースとして使用

この機能を使用すると、複数のポリシー、アプリ、アクションを含む複雑なデリバリーグループをコピーできます。その後、登録プロファイルや新しいActive Directoryユーザーセットの追加など、コピーを編集できます。詳細については、「デリバリーグループの複製」を参照してください。

共有iPad向けApple Business Managerのサポート

XenMobile Server 10.16リリース以降、共有iPadはXenMobile ServerでApple Business Manager（ABM）をサポートします。これにより、ABMアカウントを使用して共有iPadにサインインし、それらを使用できます。詳細については、「共有iPadの構成」を参照してください。

共有iPad向けに「すべてのユーザーを削除」という新しいセキュリティアクションを追加

XenMobile Server 10.16リリース以降、XenMobile Serverの共有iPad向けに「**すべてのユーザーを削除**」という新しいセキュリティアクションが追加されました。これにより、デバイス上のすべてのユーザーを削除できます。詳細については、「共有iPadのセキュリティアクション」を参照してください。

アプリ属性デバイスポリシーが新しいiOSアプリ属性をサポート

iOSデバイスにインストールされているアプリに対して、以下の属性を指定できるようになりました。

- **削除可能なアプリ:** 管理対象アプリである場合に、ユーザーがアプリを削除できるかどうかを指定します。
- **関連ドメインの直接ダウンロードを有効にする:** アプリが主張されたサイト関連付け検証をドメインで直接実行できるかどうかを指定します。
- **関連ドメイン:** アプリに追加する関連ドメインを指定します。

詳細については、「アプリ属性デバイスポリシー」を参照してください。

iOS向け同期済みExchangeサービスの同期または上書きのサポート

XenMobile Server 10.16リリース以降、関連する設定を有効にすることで、iOS向けに以下の同期済みExchangeサービスを同期するか上書きするかを選択できます。

- カレンダー
- 連絡先
- メール
- メモ
- リマインダー

詳細については、「Exchangeデバイスポリシー」を参照してください。

OSアップデート制御デバイスポリシーをシステムデフォルトにリセットするサポート

XenMobile Server 10.16リリース以降、Android Enterprise**OSアップデート制御**の下にある**システムアップデートポリシー**ドロップダウンリストに新しい値**Default**が追加されました。この機能により、システムアップデートポリシーをシステムデフォルトにリセットできます。詳細については、「OSアップデート制御デバイスポリシー」を参照してください。

iOS向けOSアップデートポリシーに新しいオプション「OSアップデートバージョン」を追加

iOSプラットフォームの**OSアップデートポリシー**において、**OSアップデート頻度**フィールドの後に新しいオプション**OSアップデートバージョン**が追加されました。このオプションを使用すると、監視対象のiOSデバイスをアップデートするために使用するOSバージョンを指定できます。詳細については、「iOS設定」を参照してください。

ネットワークアクセスコントロール

ネットワークアクセスコントロール (NAC) ソリューションを使用して、AndroidおよびAppleデバイス向けのXenMobileデバイスセキュリティ評価を拡張します。NACソリューションは、XenMobileセキュリティ評価を利用して認証決定を促進および処理します。NACアプライアンスを構成すると、XenMobileで構成したデバイスポリシーとNACフィルターが適用されます。詳細については、「ネットワークアクセスコントロール」を参照してください。

XenMobile Serverでの混合ライセンスタイプのサポート

この機能により、XenMobile ServerまたはCitrix Licensing Serverのいずれかを使用して、XenMobileライセンスの種類とエディションを組み合わせてアクティブ化できます。詳細については、「別のライセンスをアクティブ化するには」を参照してください。

iOSデバイスでのeSIMのサポート

XenMobile Serverには新しいプロパティ`ios.esim.support`があり、これによりXenMobile ServerはiOSデバイスからeSIM情報を取得し、eSIM関連のデバイスプロパティをユーザーインターフェイスに表示できます。このプロパティのデフォルト値は**True**です。詳細については、「サーバープロパティ」を参照してください。

Android Enterpriseプラットフォーム向けVPNデバイスポリシー

以前は、**XenMobileオプションデバイスポリシー**の**Always-On VPNを有効にする**オプションを有効にすることで、Android Enterpriseで実行されているデバイスのVPNサービスを有効にできました。

XenMobile Server 10.16以降、**VPNデバイスポリシー**の**Always-On VPNを有効にする**オプションを有効にすることで、Android Enterpriseで実行されているデバイスの常時接続VPNサービスを有効にできます。以前のリリースで**XenMobileオプションデバイスポリシー**の**Always-On VPNを有効にする**オプションをすでに有効にしている場合は、新しく登録されたデバイスに対して**VPNデバイスポリシー**で同じオプションを再度有効にしてください。すでに登録されているデバイスについては、変更は必要ありません。詳細については、「Android Enterpriseプラットフォーム向けVPNデバイスポリシー」を参照してください。

iOSのWebクリップポリシー設定に新しいフィールド「プロファイルスコープ」を追加

iOSデバイスの場合、Webクリップデバイスポリシーの**ポリシー設定**の下に、**プロファイルスコープ**という新しいフィールドが追加されました。これにより、ポリシーをユーザーに適用するかシステムに適用するかを選択できます。詳細については、「Webクリップデバイスポリシー - iOS設定」を参照してください。

Secure Hub APNs証明書の更新

このアップデートにより、XenMobile Server 10.16 の Secure Hub Apple Push Notification Service (APNs) 証明書が、February 9, 2025 に期限切れとなる新しい証明書に自動的に更新されます。

REST APIを使用したパブリックストアアプリの展開ルールの更新

新しいパブリックストアアプリの追加および**パブリックストアアプリの更新**REST APIに、**rules**という新しいフィールドが追加されました。これにより、パブリックストアアプリの展開ルールを更新できます。詳細については、「パブリックREST APIドキュメント」を参照してください。

iOSでのオプションアプリの自動更新のサポート

XenMobile Server 10.16以降、`apple.ios.optional_app_update`という新しいサーバープロパティが追加されました。このプロパティを使用すると、iOSのオプションアプリを自動更新できます。`apple.ios.optional_app_update`のデフォルト値は**False**に設定されています。詳細については、「サーバープロパティ」を参照してください。

オプションのボリューム購入アプリの自動更新の詳細については、「アプリの更新を確認する」を参照してください。

macOSデバイスでのエンタープライズアプリのサポート

XenMobile Serverには、macOSを実行しているデバイスでのエンタープライズアプリのサポートを可能にする新しいプロパティ`mac.app.push`があります。このプロパティのデフォルト値は**True**です。詳細については、「サーバープロパティ」を参照してください。

アプリ展開試行回数合計とインストール済みアプリトップ100のデバイスレポートの機能強化

XenMobile Serverコンソールの -> で、に**オペレーティングシステムバージョン**と**デバイスモデル**の2つの新しい列が追加され、各プラットフォームにインストールされている上位100個のアプリを表示する新しいデバイスレポート**インストール済みアプリトップ100**が追加されました。詳細については、「レポート」を参照してください。

XenMobile Serverには、上記の新しいデバイスレポートの機能強化を可能にする新しいプロパティ`device.report.enhancement.enabled`があります。このプロパティのデフォルト値は**True**です。詳細については、「サーバープロパティ」を参照してください。

デバイス登録における並べ替えとフィルタリングの最新化

XenMobile Serverのリストビューは現在、ナビゲートが難しく、ユーザーフレンドリーではありません。フィルタリングと並べ替えのオプションを列ヘッダーに移動することで、ユーザーはこれらの機能を組み合わせて、必要なデータをはるかに簡単かつ直感的に見つけることができます。

非推奨と削除

XenMobile Analyzerツールの非推奨: 頻繁かつ安定したリリースサイクルに従い、XenMobile Analyzerツールは不要になりました。Citrixは、March 31, 2023をもってこのサービスを終了しました。Citrix XenMobileコンソールまたはは Citrix Gateway内で利用可能な接続チェックを使用することをお勧めします。詳細については、「接続チェック」を参照してください。

XenMobile Server 10.15 の新機能

XenMobile Server 10.15 (PDFダウンロード)

Citrix ADC で非推奨になったクラシックポリシーの継続サポート

Citrix は最近、Citrix ADC 12.0 build 56.20 以降、一部のクラシックポリシーベースの機能が非推奨になることを発表しました。Citrix ADC の非推奨通知は、Citrix Gateway との既存の XenMobile Server 統合には影響しません。XenMobile Server は引き続きクラシックポリシーをサポートしており、対応は不要です。

非推奨のお知らせ

段階的に廃止される Citrix XenMobile 機能の事前通知については、非推奨を参照してください。

エンドポイントを iOS 14.5 にアップグレードする前に

いずれかのエンドポイントを iOS 14.5 にアップグレードする前に、Citrix はアプリのクラッシュを軽減するために次のアクションを実行することを推奨します。

- Citrix Secure Mail と Secure Web を 21.2.X 以降にアップグレードします。MDX またはエンタープライズアプリのアップグレードを参照してください。
- MDX Toolkit を使用している場合は、すべてのサードパーティ製 iOS アプリケーションを MDX Toolkit 21.3.X 以降でラップします。最新バージョンについては、MDX Toolkit のダウンロードページを確認してください。

オンプレミスの Citrix ADC をアップグレードする前に

オンプレミスの Citrix ADC を特定のバージョンにアップグレードすると、シングルサインオンエラーが発生する可能性があります。ブラウザで オプションを使用して Citrix Files または ShareFile ドメイン URL にシングルサインオンすると、エラーが発生します。ユーザーはサインインできません。

この問題を回避するには: Citrix Gateway の ADC CLI から次のコマンドをまだ実行していない場合は、グローバル SSO を有効にするために実行します。

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

詳細については、以下を参照してください。

- Citrix ADC リリース (機能フェーズ) 13.1 ビルド 33.52
- 影響を受けるSSO構成

回避策を完了すると、ユーザーはブラウザで「会社の従業員サインイン」オプションを使用してSSOでCitrix FilesまたはShareFileドメインURLに認証できます。

XenMobile 10.15 (オンプレミス) にアップグレードする前に

システム要件が一部変更されました。詳細については、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. アップグレードするXenMobile® Serverを実行している仮想マシンのRAMが8 GB未満の場合、RAMを少なくとも8 GBに増やすことをお勧めします。
2. XenMobile Server 10.15の最新バージョンに更新する前に、Citrix License Serverを11.17以降に更新してください。

   XenMobileの最新バージョンには、Citrix License Server 11.17 (最小バージョン) が必要です。

   > **注:**
   >
   > XenMobile 10.15におけるカスタマーサクセスサービス日 (以前のSubscription Advantage日) は November 15, 2022 です。Citrixライセンスのカスタマーサクセスサービス日は、この日付より後である必要があります。

> License Serverでライセンスの横に日付を表示できます。XenMobileの最新バージョンを古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。

> ライセンスの日付を更新するには、Citrix Portalから最新のライセンスファイルをダウンロードし、そのファイルをライセンスサーバーにアップロードします。カスタマーサクセスサービスを参照してください。

3. クラスター環境の場合: iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL永続性のために構成されている場合、すべてのXenMobile Serverノードでポート80を開く必要があります。
4. 推奨事項: XenMobileの更新をインストールする前に、VMの機能を使用してシステムのスナップショットを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に問題が発生した場合でも、完全なバックアップがあれば回復できます。

アップグレードするには

このリリースでは、XenMobileはVMware ESXi 7.0をサポートしています。ESXi 7.0をインストールまたはアップグレードする前に、10.14以降にアップグレードしていることを確認してください。

XenMobile 10.14.x または 10.13.x から XenMobile 10.15 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、利用可能な最新のバイナリをダウンロードしてください。`<https://www.citrix.com/downloads>` にアクセスします。**Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10** に移動します。ハイパーバイザー用の XenMobile Server ソフトウェアのタイルで、**Download File** をクリックします。

アップグレードをアップロードするには、XenMobile コンソールの **Release Management** ページを使用します。「Release Management ページを使用したアップグレード」を参照してください。

アップグレード後

送信接続を含む機能が動作しなくなり、接続構成を変更していない場合は、XenMobile Server のログで次のようなエラーを確認してください。「VPP Server に接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません。」.

- 証明書の検証エラーは、XenMobile Server でホスト名の検証を無効にする必要があることを意味します。

- 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検証が有効になっています。
- ホスト名の検証によって展開が中断される場合は、サーバープロパティ `disable.hostname.verification` を `true` に変更してください。このプロパティのデフォルト値は `false` です。

プラットフォームの更新

iOS 16 のサポート。 XenMobile Server および Citrix Mobile 生産性向上アプリは iOS 16 と互換性がありますが、現時点では新しい iOS 16 の機能はサポートしていません。

Android 13 のサポート。 XenMobile Server は、Android Enterprise デバイスの Android 13 への更新をサポートしています。セキュリティとプライバシーの利点の概要については、Android ドキュメント を参照してください。

Windows 11 デバイスのサポート。 XenMobile を使用して Windows 11 デバイスを管理できるようになりました。詳細については、「オペレーティングシステムのサポートリスト」を参照してください。

macOS の接続モードとネットワーク優先度を構成する

Wi-Fi デバイスポリシーで、macOS デバイスの **Connection mode** 設定を有効にして、ユーザーがネットワークに参加する方法を選択します。デバイスは、システム資格情報またはログインウィンドウで入力された資格情報を使用してユーザーを認証できます。複数のネットワークがある場合は、*Priority* フィールドに数値を入力して、ネットワーク接続の優先度を設定します。デバイスは最も小さい番号のネットワークを選択します。詳細については、「Wi-Fi デバイスポリシー」の macOS 設定を参照してください。

Android Enterprise 管理対象アプリを自動更新するための優先度を構成する

Android Enterprise 管理対象アプリを低優先度または高優先度で自動的に更新するかどうかを指定します。自動更新を延期することもできます。詳細については、「管理対象アプリの自動更新デバイスポリシー」を参照してください。

Citrix Hypervisor バージョン 8.2 CU1 以降でハードウェア仮想化モード (HVM) イメージを使用する

Citrix Hypervisor バージョン 8.2 CU1 以降では、準仮想化 (PV) VM はサポートされなくなりました。詳細については、累積更新プログラム 1 を参照してください。

XenMobile Server バージョン 10.15 以降では、ハードウェア仮想化モード (HVM) がサポートされています。新規の XenMobile Server インストールの場合、citrix.com から HVM xva イメージをダウンロードしてください。既存の XenMobile Server 環境の場合、PV から HVM ゲストへの移行手順に従ってください。HVM ゲストイメージは、XenMobile Server バージョン 10.15 以降の citrix.com で入手できます。

前提条件

- クラスターが有効になっており、データベースがリモートであることを確認します。
- バックアップとして、古い PV ノードを保持するか、スナップショットを保存します。PV ノードが XenMobile Server バージョン 10.14 または 10.13 の場合、データベースもバックアップしてください。
- 移行前に、新しい HVM ノードに転送されない古い PV ノードからサポートバンドルをダウンロードします。

移行手順

1. XenMobile Server 10.15 HVM xva イメージをダウンロードします。
2. 古い PV ゲストノードをシャットダウンします。
3. Citrix Hypervisor で新しい HVM ノードを起動します。
4. XenMobile Server 10.15 ノードを、古いノードと同じデータベース設定と、既存のクラスターからのサーバーの PKI キーストアパスワードで構成します。
5. 必要に応じて Citrix Gateway の設定を更新します。

> **注：**
>
> 移行中に障害が発生した場合は、同じバージョンのデータベースで古い PV ノードを起動します。

> **重要:**
>
> XenMobile PVゲストに対して`/opt/xensource/bin/pv2hvm`コマンドを実行しないでください。VMの起動に失敗します。

Google Analyticsを有効にする

XenMobile ServerでGoogle Analyticsを有効にするには、サーバープロパティ *xms.ga.enabled* の値を**True**に設定します。デフォルトは**True**です。

新しい制限ポリシーを追加しました

制限ポリシーに、*仕事用プロファイルからのコピーと貼り付けを許可*および*個人用プロファイルからのデータ共有を許可*を追加しました。これらのポリシーを**OFF**に設定すると、個人用プロファイルから仕事用プロファイルへのコピー、貼り付け、インポートが制限されます。詳細については、制限デバイスポリシーを参照してください。

Secure Hub APNs証明書の更新

XenMobile Server の Secure Hub Apple Push Notification Service (APNs) 証明書は、May 7, 2022 に期限切れになりました。このアップデートにより、April 8, 2023 に期限切れとなる Secure Hub APNs 証明書が更新されます。

非推奨と削除

- **GoogleによるAPIの非推奨化。** Googleは、XenMobile Serverでアプリのカテゴリとライセンスに使用されるいくつかのAPIを非推奨にしています。以下の変更が適用されます。
  - アプリを承認するのではなく、追加するアプリを選択するようになりました。管理対象アプリストアアプリを参照してください。
  - アプリをカテゴリではなくコレクションに整理するようになりました。アプリの整理を参照してください。
  - アプリライセンスをユーザーから関連付け解除することはできなくなりました。アプリの追加を参照してください。
- **Windows Information Protectionポリシーのサポートは非推奨になりました。** Windowsの発表に従い、XenMobile ServerはWindows Information Protection (WIP) のサポートを非推奨にしました。WIPのサポートは、*windows.wip.deprecation*というサーバープロパティを追加することで非推奨になりました。このプロパティの値はデフォルトで*True*に設定されています。詳細については、サーバープロパティを参照してください。
- **モバイルサービスプロバイダー (MSP) インターフェイスのサポートは非推奨になりました。** MSPのサポートは、コンソールからMSPインターフェイスを削除する新しいサーバープロパティ *deprecate.mobile.service.provider* を追加することで非推奨になりました。このプロパティはデフォルトで*True*に設定されています。詳細については、サーバープロパティを参照してください。

- **Nexmo SMSゲートウェイのサポートは非推奨になりました。** Nexmo SMSのサポートは、デフォルトで*True*に設定されている*deprecate.carrier.sms.gateway*という新しいサーバープロパティを追加することで非推奨になりました。Nexmo SMSはセルフヘルプポータルでも非推奨になっています。詳細については、通知を参照してください。
- **Windows 10デバイスの*Allow auto-connect to WiFi Sense hotspots*制限ポリシーのサポートは非推奨になりました。** 詳細については、Windowsデスクトップ/タブレット設定を参照してください。
- **登録招待のセットアップ。** デバイスのIMEI、シリアル番号、UDIDを使用して登録招待を作成するサポートは非推奨になりました。登録招待を作成する際は、XenMobile Serverコンソールの**管理 > 登録招待**で利用可能な設定を構成してください。
- **以下の機能のサポートは削除されました。**
  - アンドロイド - アマゾン
  - Android - SonyおよびHTC
  - Zebraデバイス上のカスタムXML
  - 派生資格情報
  - 汎用、DigiCert管理、およびEntrustアダプターPKIエンティティ。
  - 高セキュリティ登録モード
  - RBACロール - 共有およびCOSUデバイス登録者
  - Samsung SAFEおよびKnox
  - SEAMS
  - Windows Phoneデバイス

  詳細については、非推奨を参照してください。

XenMobile Server 10.14の新機能

XenMobile Server 10.14 (PDFダウンロード)

Citrix ADCで非推奨となったクラシックポリシーの継続サポート

Citrixは最近、Citrix ADC 12.0ビルド56.20以降、一部のクラシックポリシーベース機能の非推奨を発表しました。Citrix ADCの非推奨に関する通知は、Citrix Gatewayとの既存のXenMobile Server統合には影響しません。XenMobile Serverは引き続きクラシックポリシーをサポートしており、対応は不要です。

非推奨のお知らせ

段階的に廃止されるCitrix XenMobile機能の事前通知については、非推奨を参照してください。

エンドポイントをiOS 14.5にアップグレードする前に

エンドポイントをiOS 14.5にアップグレードする前に、Citrixはアプリのクラッシュを軽減するために以下の操作を行うことを推奨します。

- Citrix Secure MailおよびSecure Webを21.2.X以降にアップグレードします。MDXまたはエンタープライズアプリのアップグレードを参照してください。
- MDX Toolkitを使用している場合は、すべてのサードパーティ製iOSアプリケーションをMDX Toolkit 21.3.X以降でラップします。最新バージョンについては、MDX Toolkitのダウンロードページを確認してください。

オンプレミスのCitrix ADCをアップグレードする前に

オンプレミスのCitrix ADCを特定のバージョンにアップグレードすると、シングルサインオンエラーが発生する可能性があります。ブラウザでCitrix FilesまたはShareFileドメインURLに**Company Employee Sign in**オプションを使用してシングルサインオンを行うと、エラーが発生します。ユーザーはサインインできません。

この問題を回避するには：Citrix GatewayでADC CLIから以下のコマンドをまだ実行していない場合は、実行してグローバルSSOを有効にします。

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

詳細については、以下を参照してください。

- Citrix ADC リリース（機能フェーズ）13.0 ビルド 67.39/67.43
- 影響を受けるSSO構成(/ja-jp/citrix-adc/current-release/aaa-tm/single-sign-on-types/enable-sso-for-auth-pol.html#impacted-sso-configurations)

回避策を完了すると、ユーザーはブラウザで「Company Employee Sign-in」オプションを使用して、SSOでCitrix FilesまたはShareFileドメインURLに認証できます。

XenMobile 10.14（オンプレミス）にアップグレードする前に

一部のシステム要件が変更されました。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. アップグレードするXenMobile® Serverを実行している仮想マシンのRAMが8GB未満の場合は、RAMを少なくとも8GBに増やすことをお勧めします。
2. XenMobile Server 10.14の最新バージョンに更新する前に、Citrix License Serverを11.16以降に更新してください。

   XenMobileの最新バージョンには、Citrix License Server 11.16（最小バージョン）が必要です。

   > **注：**
   >
   > XenMobile 10.14におけるカスタマーサクセスサービス日付（以前のサブスクリプションアドバンテージ日付）は September 15, 2021 です。Citrixライセンスのカスタマーサクセスサービス日付は、この日付より後である必要があります。
   >
   > 日付はLicense Serverのライセンスの横に表示されます。最新バージョンのXenMobileを古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。
   >
   > ライセンスの日付を更新するには、Citrix Portalから最新のライセンスファイルをダウンロードし、そのファイルをLicensing Serverにアップロードします。「Customer Success Services」(/ja-jp/licensing/current-release/subscription-advantage.html)を参照してください。
3. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL persistence用に構成されている場合、すべてのXenMobile Serverノードでポート80を開く必要があります。
4. 推奨事項：XenMobileの更新をインストールする前に、VMの機能を使用してシステムのsnapshotを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に問題が発生した場合でも、完全なバックアップがあれば回復できます。

アップグレードするには

このリリースでは、XenMobileはVMware ESXi 7.0をサポートしています。ESXi 7.0をインストールまたはアップグレードする前に、10.14にアップグレードしてください。

XenMobile 10.13.xまたは10.12.xからXenMobile 10.14に直接アップグレードできます。アップグレードを行うには、利用可能な最新のバイナリをダウンロードしてください。`<https://www.citrix.com/downloads>`にアクセスします。**Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**に移動します。ハイパーバイザー用のXenMobile Serverソフトウェアのタイルで、**Download File**をクリックします。

アップグレードをアップロードするには、XenMobileコンソールの**Release Management**ページを使用します。「Release Managementページを使用したアップグレード」を参照してください。

アップグレード後

送信接続に関する機能が動作しなくなり、接続構成を変更していない場合は、**XenMobile Serverログ**で次のようなエラーを確認してください。「Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer」（VPPサーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません）。

- 証明書検証エラーは、XenMobile Serverでホスト名検証を無効にする必要があることを意味します。
- デフォルトでは、Microsoft PKIサーバーを除き、送信接続でホスト名検証が有効になっています。
- ホスト名検証によって展開が中断される場合は、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。

プラットフォームサポートの更新

- **iOS 15:** XenMobile ServerおよびCitrix Mobile生産性向上アプリはiOS 15と互換性がありますが、現時点では新しいiOS 15の機能はサポートしていません。
- **Android 12:** XenMobile ServerはAndroid 12をサポートしています。Googleデバイス管理APIの廃止がAndroid 10以降を実行しているデバイスに与える影響については、「デバイス管理からAndroid Enterpriseへの移行」を参照してください。また、このCitrixブログも参照してください。

デバイスポリシー

- Googleの設定にさらに近づけ、構成を簡素化するために、すべてのAndroid Enterprise登録モードに2つの設定を追加しました。
    - **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetooth共有を確立できません。

- **アプリのアンインストールを許可:** ユーザーがManaged Google Playストア内からアプリをアンインストールできるようにします。

また、**無線（OTA）アップグレードを許可**設定を制限ポリシーからOS更新ポリシーに移動しました。

これらの変更の詳細については、「制限デバイスポリシー」および「OS更新デバイスポリシー」を参照してください。

- Android Enterpriseの制限設定は、明確にするために再編成されました。設定名に軽微な変更が加えられている場合があります。再編成の詳細については、「Android Enterprise設定」を参照してください。
- Android Enterpriseデバイスで管理対象アプリを自動的に更新できるようになりました。詳細については、「管理対象アプリの自動更新デバイスポリシー」を参照してください。
- ファイルデバイスポリシーを使用してアップロードできるファイルタイプのリストを構成できます。次のファイルタイプは、この許可リストに追加してもアップロードできません。
  - .キャブ
  - .アップエックス
  - .アイピーエー
  - .エーピーケー
  - .エックスエーピー
  - .エムディーエックス
  - .エグゼ

詳細については、「サーバープロパティ」を参照してください。

デバイス登録

- iOSおよびAndroidデバイス用に異なる登録プロファイルを作成できるようになりました。XenMobile Serverは、さまざまな登録タイプを持つ複数の登録プロファイルをサポートしています。詳細については、「登録プロファイル」を参照してください。
- フルマネージドのAndroid 11以降のデバイスは、企業所有デバイスモードのワークプロファイルに登録されます。この新しいモードでは、デバイス上の個人プロファイルとワークプロファイルがさらに分離されます。この変更により、組織は管理対象プロファイルをより詳細に制御できるようになり、ユーザーは個人プロファイルのプライバシーをより保護できるようになります。詳細については、「Android Enterprise」および「サーバープロパティ」を参照してください。

- ユーザーがiOSまたはmacOSデバイスをセットアップする際にスキップするセットアップ画面をさらに指定できるようになりました。
  - iOS
    - **復元完了:** ユーザーがセットアップ中に復元が完了したかどうかを確認できないようにします。iOS 14.0以降の場合。
    - **アップデート完了:** ユーザーがセットアップ中にソフトウェアアップデートが完了したかどうかを確認できないようにします。iOS 14.0以降の場合。
  - macOS
    - **アクセシビリティ:** ユーザーがVoice Overを自動的に聞くことを防ぎます。デバイスがイーサネットに接続されている場合にのみ利用可能です。macOS 11以降の場合。
    - **生体認証:** ユーザーがTouch IDとFace IDを設定することを防ぎます。macOS 10.12.4以降の場合。
    - **True Tone:** ユーザーがディスプレイのホワイトバランスを動的に調整するために4チャンネルセンサーを設定することを防ぎます。macOS 10.13.6以降の場合。
    - **Apple Pay:** ユーザーがApple Payを設定することを防ぎます。この設定がクリアされている場合、ユーザーはTouch IDとApple IDを設定する必要があります。**Apple ID**と**生体認証**の設定がクリアされていることを確認してください。macOS 10.12.4以降の場合。
    - **スクリーンタイム:** ユーザーがスクリーンタイムを有効にすることを防ぎます。macOS 10.15以降の場合。

  セットアップオプションの構成について詳しくは、「Apple Deployment Program を使用したデバイスの展開」を参照してください。

更新ログファイルの表示

トラブルシューティングメニューの**ログ**コマンドラインインターフェイスに、**更新ログファイルの表示**という新しいオプションが追加されました。このオプションを使用すると、更新ログの内容のリストを確認でき、トラブルシューティングの効率が向上します。コマンドラインインターフェイスツールについて詳しくは、「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。

エラーログファイル

トラブルシューティングとサポート > ログでログを表示する際に、デバッグログからフィルタリングされたエラーを表示するログを確認できるようになりました。詳しくは、「XenMobileでログファイルを表示する」を参照してください。

サーバープロパティ

- レガシーAndroidアプリをAndroid Enterpriseアプリに配信するかどうかは、`afw.allow.legacy.apps`サーバープロパティを構成することで決定できます。詳細については、「サーバープロパティ」を参照してください。
- XenMobile Serverは、ポート443の代替としてポート2197の使用をサポートするようになりました。ポート2197は、`api.push.apple.com`からAPNs通知を送受信するために使用します。このポートは、HTTP/2ベースのAPNsプロバイダーAPIを使用します。サーバープロパティ`apns.http2.alternate.port.enabled`のデフォルト値は`false`です。ポート2197を使用するには、サーバープロパティを更新してからサーバーを再起動してください。
- パスワード検証により、脆弱なパスワードを持つユーザーが防止されます。プロパティ`enable.password.strength.validation`が`true`に設定されている場合、脆弱なパスワードを持つローカルユーザーを作成することはできません。

VPN仮想サーバーリストの機能強化

VPNサーバー名に`_XM_XenMobileGetway`が含まれていない場合、XenMobile Serverはリスト上の利用可能な最初のVPN仮想サーバーを選択します。

Citrix Launcherのサポート

XenMobile Serverは、Android EnterpriseデバイスでのCitrix Launcherをサポートしています。詳細については、「Launcher構成デバイスポリシー」を参照してください。

XenMobile Serverのカラー刷新

XenMobile Serverは、Citrixブランドのカラーアップデートに準拠しています。

XenMobile Server 10.13 の新機能

XenMobile Server 10.13 (PDFダウンロード)

Citrix ADCで非推奨となったクラシックポリシーの継続サポート

Citrixは最近、Citrix ADC 12.0ビルド56.20以降、一部のクラシックポリシーベース機能の非推奨化を発表しました。Citrix ADCの非推奨通知は、Citrix Gatewayとの既存のXenMobile Server統合には影響しません。XenMobile Serverは引き続きクラシックポリシーをサポートしており、対応は不要です。

非推奨のお知らせ

段階的に廃止されるCitrix XenMobile機能の事前通知については、非推奨を参照してください。

エンドポイントをiOS 14.5にアップグレードする前に

Citrixは、エンドポイントをiOS 14.5にアップグレードする前に、アプリのクラッシュを軽減するために以下の操作を行うことを推奨します。

- Citrix Secure MailとSecure Webを21.2.X以降にアップグレードします。MDXまたはエンタープライズアプリのアップグレードを参照してください。
- MDX Toolkitを使用している場合は、すべてのサードパーティ製iOSアプリケーションをMDX Toolkit 21.3.X以降でラップします。最新バージョンについては、MDX Toolkitのダウンロードページを確認してください。

オンプレミスのCitrix ADCをアップグレードする前に

オンプレミスのCitrix ADCを特定のバージョンにアップグレードすると、シングルサインオンエラーが発生する可能性があります。ブラウザでCitrix FilesまたはShareFileドメインURLに**会社従業員サインイン**オプションでシングルサインオンするとエラーが発生し、ユーザーはサインインできません。

この問題を回避するには：Citrix GatewayのADC CLIから以下のコマンドをまだ実行していない場合は、グローバルSSOを有効にするために実行してください。

```
`set vpn parameter SSO ON`

`bind vpn vs <vsName> -portalTheme X1`
```

詳細については、以下を参照してください。

- Citrix ADCリリース (機能フェーズ) 13.0ビルド 67.39/67.43
- 影響を受けるSSO構成(/ja-jp/citrix-adc/current-release/aaa-tm/single-sign-on-types/enable-sso-for-auth-pol.html#impacted-sso-configurations)

回避策を完了すると、ユーザーはブラウザで「会社の従業員サインイン」オプションを使用して、SSO経由でCitrix FilesまたはShareFileドメインURLに認証できるようになります。

XenMobile 10.13 (オンプレミス) にアップグレードする前に

一部のシステム要件が変更されました。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. アップグレードするXenMobile® Serverを実行している仮想マシンのRAMが8 GB未満の場合は、RAMを少なくとも8 GBに増やすことをお勧めします。
2. XenMobile Server 10.13の最新バージョンにアップデートする前に、Citrix License Serverを11.16以降にアップデートしてください。

   XenMobileの最新バージョンには、Citrix License Server 11.16（最小バージョン）が必要です。

   > **注：**
   >
   > XenMobile 10.13のCustomer Success Services日付（以前のSubscription Advantage日付）はSeptember 29, 2020です。CitrixライセンスのCustomer Success Services日付は、この日付より後である必要があります。
   >
   > 日付は、License Serverのライセンスの横に表示されます。XenMobileの最新バージョンを古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。
   >
   > ライセンスの日付を更新するには、Citrix Portalから最新のライセンスファイルをダウンロードし、そのファイルをLicensing Serverにアップロードします。「Customer Success Services」を参照してください。
3. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL永続性のために構成されている場合、すべてのXenMobile Serverノードでポート80を開く必要があります。
4. 推奨事項：XenMobileのアップデートをインストールする前に、VMの機能を使用してシステムのスナップショットを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に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旧できます。

アップグレードするには

このリリースでは、XenMobileはVMware ESXi 7.0をサポートしています。ESXi 7.0をインストールまたはアップグレードする前に、10.13にアップグレードしてください。

XenMobile 10.12.xまたは10.11.xからXenMobile 10.13に直接アップグレードできます。アップグレードを行うには、利用可能な最新のバイナリをダウンロードしてください。`<https://www.citrix.com/downloads>`にアクセスし、**Citrix Endpoint Management (XenMobile) >**

XenMobile Server > Product Software > XenMobile Server 10に移動します。ハイパーバイザー用のXenMobile Serverソフトウェアのタイルで、**Download File**をクリックします。

アップグレードをアップロードするには、XenMobileコンソールの**Release Management**ページを使用します。「」を参照してください(/ja-jp/xenmobile/server/upgrade.html#to-upgrade-using-the-release-management-page)。

アップグレード後

送信接続に関連する機能が動作しなくなり、接続構成を変更していない場合は、**XenMobile Serverログ**で次のようなエラーを確認してください。「VPPサーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません。」.

- 証明書の検証エラーは、XenMobile Serverでホスト名の検証を無効にする必要があることを意味します。
- 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検証が有効になっています。
- ホスト名の検証によって展開が機能しなくなる場合は、サーバープロパティ`disable.hostname.verification`を`true`に変更してください。このプロパティのデフォルト値は`false`です。

プラットフォームサポートの更新

- **iOS 14:** XenMobile ServerおよびCitrix Mobile生産性向上アプリはiOS 14と互換性がありますが、現時点では新しいiOS 14の機能はサポートしていません。MDX Toolkit 20.8.5以降を使用するか、MAM SDKを使用してアプリを準備してください。
- **Android 11:** XenMobile ServerはAndroid 11をサポートしています。Google Device Administration APIの非推奨化がAndroid 10以降を実行しているデバイスに与える影響については、「」を参照してください(/ja-jp/xenmobile/server/provision-devices/migrate-from-device-administration-to-android-enteprise.html)。また、このも参照してください(https://www.citrix.com/blogs/2019/06/26/citrix-endpoint-management-and-android-enterprise-a-season-of-change/)。

単一環境での複数のデバイスおよびアプリ管理モードの構成

1つのXenMobileサイトで複数の登録構成をサポートするように設定できるようになりました。登録プロファイルの役割が拡張され、デバイスおよびアプリ管理の登録設定が含まれるようになりました。

登録プロファイルは、単一のXenMobileコンソール内で複数のユースケースとデバイス移行パスをサポートします。ユースケースには以下が含まれます。

- モバイルデバイス管理 (MDMのみ)
- MDM+モバイルアプリケーション管理 (MAM)
- MAMのみ
- 会社所有の登録
- BYOD登録 (MDM登録をオプトアウトする機能)
- Androidデバイス管理者登録からAndroid Enterprise登録への移行 (完全管理、ワークプロファイル、専用デバイス)

登録プロファイルは、現在非推奨のサーバープロパティ `xms.server.mode` に代わるものです。この変更は、既存のデリバリーグループおよび登録済みデバイスには影響しません。

専用デバイスを登録する必要がない場合は、サーバープロパティ `enable.multimode.xms` を `false` に設定することで、この機能を無効にできます。サーバープロパティを参照してください。

次の表は、既存のサーバープロパティモードから新しい登録プロファイル機能への自動移行パスを示しています。

既存のサーバープロパティ	新しい管理モード
ENTモード (iOS)	Citrix MAMによるAppleデバイス登録
ENTモード (Android)	Citrix MAMによるレガシーデバイス管理者
エントモード (Android Enterprise)	Citrix MAMによる完全管理 (旧COPE) のワークプロファイル
MAMモード (iOSおよびAndroid)	シトリックス MAM
MDMモード (iOS)	Appleデバイス登録
MDMモード (Android)	レガシーデバイス管理者
MDMモード (Androidエンタープライズ)	完全管理対象のワークプロファイル

デリバリーグループを作成する際、登録プロファイルをグループにアタッチできます。登録プロファイルをアタッチしない場合、XenMobileはグローバル登録プロファイルをアタッチします。

登録プロファイルは、以下のデバイス管理機能を提供します。

- **Androidデバイス管理者 (DA) モードからAndroid Enterpriseへの移行がより簡単に。** Android Enterpriseデバイスの場合、設定には、完全管理対象、完全管理対象のワークプロファイル、専用などのデバイス所有者モードが含まれます。「Android Enterprise」を参照してください(/ja-jp/xenmobile/server/provision-devices/android-enterprise.html)。

  Androidの登録プロファイルページ(/en-us/xenmobile/server/media/enrollment-profile-android-mdm-mam-mode.png)

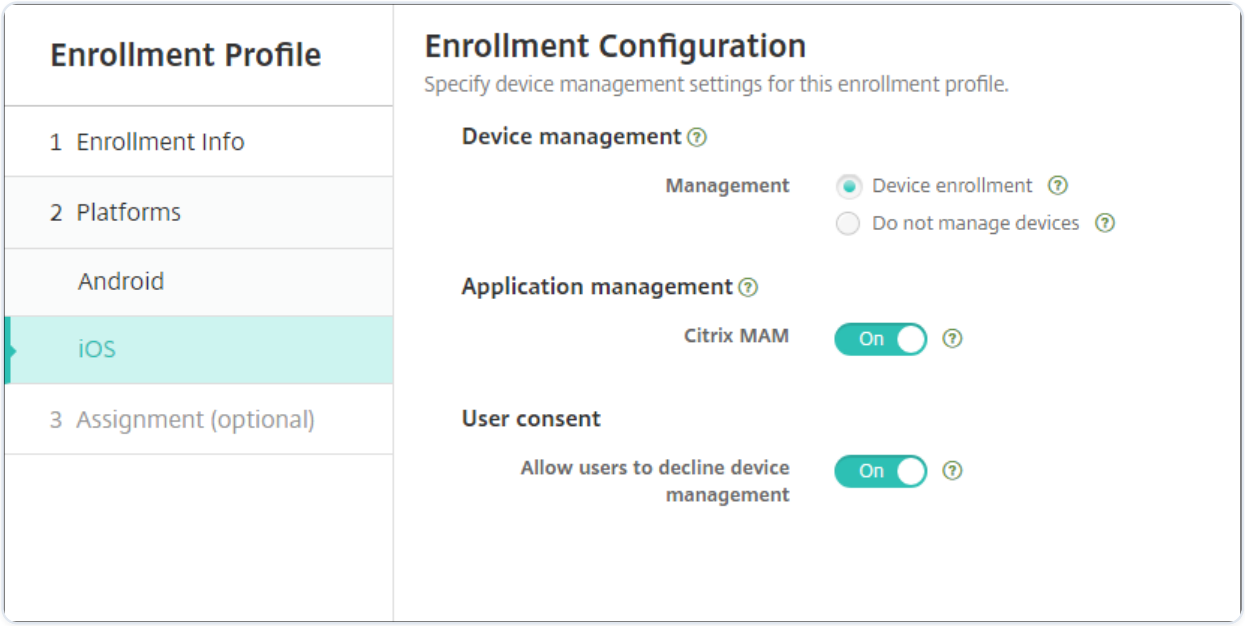
  このアップグレードでは、サーバーモードおよび**設定 > Android Enterprise**に関する現在のXenMobile構成が、新しい登録プロファイル設定に次のようにマッピングされます。

現在の構成	管理設定	デバイス所有者モード設定	CITRIX MAM設定
MDM。マネージド グーグル プレイ (アンドロイド エンタープライズ)	アンドロイド エンタープライズ	完全管理対象の仕事用プロファイル	オフ
MDM。G Suite (レガシーDA)	レガシーDA	該当なし	オフ
MAM	デバイスを管理しない	該当なし	オン
MDM+MAM。マネージド グーグル プレイ (アンドロイド エンタープライズ)	Androidエンタープライズ*	完全に管理されたデバイス上の仕事用プロファイル	オン
MDM+MAM; G Suite (レガシーDA)	レガシーDA*	該当なし	オン

* 登録が必要な場合、**ユーザーによるデバイス管理の拒否を許可**は**オフ**になります。

アップグレード後、現在の登録プロファイルにこれらのマッピングが反映されます。レガシーDAから移行する際に、新しいユースケースに対応するために他の登録プロファイルを作成するかどうかを検討してください。

- **より簡単なiOS管理。** iOSデバイスの場合、設定にはデバイスを管理対象として登録するか、非管理対象として登録するかの選択肢が含まれます。



今回のアップグレードでは、以前の設定が新しい登録プロファイル設定に次のようにマッピングされます。

サーバーモード	管理設定	CITRIX MAM設定
MDM	デバイス登録	オフ
MAM	デバイスを管理しない	オン
MDM+MAM	デバイス登録	オン

登録が必要な場合、**ユーザーがデバイス管理を拒否することを許可する**は**オフ**です。

拡張登録プロファイルには、次の制限があります。

- 拡張登録プロファイル機能は、ワンタイムPINまたは2要素認証の登録招待では利用できません。

登録プロファイルを参照してください。

最新のHTTP/2ベースのAPNsプロバイダーAPIのサポート

Apple Push Notificationサービスレガシーバイナリプロトコルのによるサポートは、March 31, 2021をもって終了します。Appleは、代わりにHTTP/2ベースのAPNsプロバイダーAPIを使用することを推奨しています。XenMobile Serverは現在、HTTP/2ベースのAPIをサポートしています。詳細については、`<https://developer.apple.com/>`のニュース更新「Apple Push Notification

Service Update」を参照してください。APNsへの接続を確認する方法については、接続チェックを参照してください。

以下のバージョンのXenMobile Serverでは、HTTP/2ベースのAPIのサポートがデフォルトで有効になっています。

- XenMobileサーバー 10.13
- XenMobileサーバー 10.12 ローリングパッチ 5以降

以下のバージョンのXenMobile Serverを使用している場合は、サポートを有効にするためにサーバープロパティ **apple.apns.http2** を追加する必要があります。

- XenMobileサーバー 10.12 ローリングパッチ 2〜4以降
- XenMobileサーバー 10.11 ローリングパッチ 5以降

XenMobile Server 10.11のサポートは終了しました。最新バージョンへのアップグレードをお勧めします。

多数のiOSデバイスでデバイス証明書ベースのIPsec VPNを使用する

デバイス証明書ベースのIPsec VPNを必要とする各iOSデバイスに対してVPNデバイスポリシーと資格情報デバイスポリシーを構成する代わりに、プロセスを自動化します。

1. 接続タイプが **Always on IKEv2** のiOS VPNデバイスポリシーを構成します。
2. デバイス認証方法として **Device certificate based on device identity** を選択します。
3. 使用する **Device identity type** を選択します。
4. REST APIを使用してデバイス証明書を一括インポートします。

VPNデバイスポリシーの構成について詳しくは、「VPNデバイスポリシー」を参照してください。証明書の一括インポートについて詳しくは、「REST APIを使用して証明書を一括アップロードする」を参照してください。

Apple Volume Purchaseアプリの自動更新

Volume Purchaseアカウント (**設定 > iOS設定**) を追加すると、すべてのiOSアプリの自動更新を有効にできるようになりました。**App Auto Update**設定については、Apple Volume Purchaseを参照してください。

ローカルユーザーアカウントのパスワード要件

XenMobileコンソールでローカルユーザーアカウントを追加または編集する際は、最新のパスワード要件に従ってください。

詳しくは、ローカルユーザーアカウントを追加するにはを参照してください。

- **パスワード要件:** XenMobile Serverコンソールでローカルユーザーアカウントを追加または編集する際は、最新のパスワード要件に従ってください。ローカルユーザーアカウントを追加するにはを参照してください。
- **ローカルユーザーアカウントのロック:** ユーザーが連続して無効なログイン試行の最大数に達すると、ローカルユーザーアカウントは30分間ロックされます。ロックアウト期間が終了するまで、システムはそれ以降のすべての認証試行を拒否します。XenMobile Serverコンソールでアカウントのロックを解除するには、**管理 > ユーザー**に移動し、ユーザーアカウントを選択して、**ローカルユーザーのロック解除**をクリックします。ローカルユーザーアカウントのロックを解除するにはを参照してください。

デバイスポリシー

Android Enterpriseデバイス向けに、新しいデバイスポリシーとデバイスポリシー設定が追加されました。

Android Enterpriseデバイスでトレイバーアイコンを非表示にする

Android Enterpriseデバイスの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できるようになりました。XenMobileオプションデバイスポリシーを参照してください。

ワークプロファイルモードまたは完全管理モードのAndroid Enterpriseデバイス向け証明書管理機能の追加

管理対象キーストアに証明機関をインストールするだけでなく、以下の機能を管理できるようになりました。

- **特定の管理対象アプリで使用される証明書を構成する。** Android Enterpriseの資格情報デバイスポリシーに、**証明書を使用するアプリ**設定が追加されました。このポリシーで選択された資格情報プロバイダーによって発行されたユーザー証明書を使用するアプリを指定できます。アプリには、実行時にサイレントで証明書へのアクセスが許可されます。すべてのアプリで証明書を使用するには、アプリリストを空白のままにします。資格情報デバイスポリシーを参照してください。
- **管理対象キーストアから証明書をサイレントに削除するか、すべての非システムCA証明書をアンインストールする。** 資格情報デバイスポリシーを参照してください。

- **ユーザーが管理対象キーストアに保存されている資格情報を変更するのを防ぐ。** Android Enterpriseの制限デバイスポリシーに、**ユーザーがユーザー資格情報を構成することを許可する**設定が追加されました。デフォルトでは、この設定は**オン**です。制限デバイスポリシーを参照してください。

マネージド構成での証明書エイリアスのより簡単な使用

新しい**証明書エイリアス**設定を**資格情報**デバイスポリシーで**マネージド構成**デバイスポリシーとともに使用します。これにより、ユーザーの操作なしでアプリがVPNで認証できるようになります。アプリのログで資格情報エイリアスを見つける代わりに、資格情報エイリアスを作成します。**マネージド構成**デバイスポリシーの**証明書エイリアス**フィールドに入力してエイリアスを作成します。次に、**資格情報**デバイスポリシーの**証明書エイリアス**設定に同じ証明書エイリアスを入力します。マネージド構成ポリシーおよび資格情報デバイスポリシーを参照してください。

Android Enterpriseデバイスでの「ロックを1つ使用」設定の制御

パスコードデバイスポリシーの新しい**統合パスコードを有効にする**設定により、デバイスとワークプロファイルに個別のパスコードが必要かどうかを制御できます。この設定が導入される前は、ユーザーはデバイスの**ロックを1つ使用**設定でこの動作を制御していました。**統合パスコードを有効にする**が**オン**の場合、ユーザーはデバイスとワークプロファイルで同じパスコードを使用できます。**統合パスコードを有効にする**が**オフ**の場合、ユーザーはデバイスとワークプロファイルで同じパスコードを使用できません。デフォルトは**オフ**です。**統合ロックを有効にする**設定は、Android 9.0以降を実行しているAndroid Enterpriseデバイスで利用できます。パスコードデバイスポリシーを参照してください。

準拠していないAndroid Enterpriseデバイス上のアプリとショートカットを表示する

Android Enterpriseのパスコードデバイスポリシーには、新しい設定**パスコードが準拠していないときにアプリとショートカットを表示する**があります。この設定を有効にすると、デバイスのパスコードが準拠しなくなったときにアプリとショートカットが表示されたままになります。Citrixは、パスコードが準拠していない場合にデバイスを非準拠としてマークする自動アクションを作成することをお勧めします。パスコードデバイスポリシーを参照してください。

Android Enterpriseワークプロファイルデバイスまたは完全に管理されたデバイスでの印刷機能を無効にする

制限デバイスポリシーの**印刷を許可しない**設定では、ユーザーがAndroid Enterpriseデバイスからアクセス可能なプリンターに印刷できるかどうかを指定できます。Android Enterprise設定を参照してください。

キオスクポリシーにパッケージ名を追加して、専用デバイス上のアプリを許可する

Android Enterpriseプラットフォームで許可するパッケージ名を入力できるようになりました。Android Enterprise設定を参照してください。

Android Enterpriseワークプロファイルおよび完全に管理されたデバイスのキーガード機能を管理する

Androidキーガードは、デバイスとワークチャレンジのロック画面を管理します。キーガード管理デバイスポリシーを使用して、以下を制御します。

- ワークプロファイルデバイスでのキーガード管理。ユーザーがデバイスキーガードとワークチャレンジキーガードを解除する前に利用できる機能を指定できます。たとえば、デフォルトでは、ユーザーは指紋認証によるロック解除を使用し、ロック画面で編集されていない通知を表示できます。また、キーガード管理ポリシーを使用して、Android 9.0以降を実行しているデバイスのすべての生体認証を無効にすることもできます。
- 完全に管理されたデバイスおよび専用デバイスでのキーガード管理。ユーザーがキーガード画面を解除する前に、信頼エージェントやセキュアカメラなどの利用可能な機能を指定できます。または、すべてのキーガード機能を無効にすることもできます。

キーガード管理デバイスポリシーを参照してください。

XenMobileコンソールでAndroid Enterprise向けエンタープライズアプリを公開する

Android Enterpriseプライベートアプリを追加する際に、Google Play開発者アカウントに登録する必要がなくなりました。XenMobileコンソールは、APKファイルをアップロードして公開するためのマネージドGoogle PlayストアUIを開きます。詳細については、「エンタープライズアプリの追加」を参照してください。

XenMobileコンソールでAndroid Enterprise向けWebアプリを公開する

XenMobile向けAndroid Enterprise Webアプリを公開するために、マネージドGoogle PlayまたはGoogle Developerポータルにアクセスする必要がなくなりました。「**Configure > Apps > Web link**」で「**Upload**」をクリックすると、ファイルをアップロードして保存するためのマネージドGoogle PlayストアUIが開きます。アプリの承認と公開には約10分かかる場合があります。詳細については、「Webリンクの追加」を参照してください。

XenMobile Server REST APIを使用してiOSデバイスに証明書を一括アップロードする

証明書を1つずつアップロードするのが実用的でない場合は、XenMobile Server REST APIを使用してiOSデバイスに証明書を一括アップロードしてください。

1. 接続タイプ「**Always on IKEv2**」でiOS VPNデバイスポリシーを構成します。
2. デバイス認証方法として「**Device Certificate Based on Device Identity**」を選択します。
3. 使用する「**Device identity type**」を選択します。
4. REST APIを使用してデバイス証明書を一括インポートします。

VPNデバイスポリシーの構成については、「VPNデバイスポリシー」を参照してください。証明書の一括インポートについては、「REST APIを使用してiOSデバイスに証明書を一括アップロードする」を参照してください。

暗号化キーを更新する

「**Refresh encryption keys**」オプションがXenMobile CLIの「Advanced Settings」に追加されました。このオプションを使用して、暗号化キーを一度に1つのノードで更新できます。「システムオプション」を参照してください。

ESXi 7.0のサポート

このリリースにより、XenMobileはVMware ESXi 7.0をサポートします。ESXi 7.0をインストールまたはアップグレードする前に、10.13にアップグレードしていることを確認してください。

新しいサーバープロパティ

以下のサーバープロパティが利用可能になりました。

- **iOS App Storeリンクのホスト名を許可:** コンソールではなくパブリックAPIを使用してiOS用のパブリックApp Storeアプリを追加するには、必要に応じて許可されたホスト名のリストを構成します。
- **ローカルユーザーアカウントのロックアウト制限:** ローカルユーザーのアカウントがロックされるまでのサインイン試行回数を構成します。
- **ローカルユーザーアカウントのロックアウト時間:** サインイン試行の失敗が多すぎた後、ローカルユーザーがロックアウトされる期間を構成します。
- **ファイルアップロードの最大サイズ制限を有効にする:** アップロードされるファイルの最大ファイルサイズを制限することを有効にします。

- **ファイルアップロードの最大許容サイズ:** アップロードされるファイルの最大ファイルサイズを設定します。

これらのプロパティの詳細については、「サーバープロパティ」を参照してください。

セルフサービスディスククリーンアップ

トラブルシューティングメニューに、**ディスク使用量**という新しいコマンドラインインターフェイスオプションが追加されました。このオプションを使用すると、コアダンプファイルとサポートバンドルファイルのリストを表示できます。リストを表示した後、コマンドラインからそれらのファイルをすべて削除することを選択できます。コマンドラインインターフェイスツールに関する詳細については、「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 Server 10.12の新機能

XenMobile Server 10.12 (PDFダウンロード)

非推奨のお知らせ

廃止されるCitrix XenMobile機能の事前通知については、「非推奨」を参照してください。

今後の変更に備えてAndroidデバイスを準備する

以前発表されたこれらの非推奨事項は、AndroidおよびAndroid Enterpriseデバイスに影響を与えます。

- Android 10のデバイス管理（DA）登録：
  - **July 31, 2020:** Citrix®は、従来のAndroidデバイス管理モードの新規登録を非推奨とします。
  - **November 1, 2020:** Googleは、従来のデバイス管理APIを非推奨とします。従来のデバイス管理モードで実行されているAndroid 10デバイスは動作しなくなります。
- MDX暗号化：
  - **August 1, 2020:** Citrixは、Citrixモバイル生産性アプリおよびサードパーティMDXアプリについて、MDX暗号化からプラットフォーム暗号化への移行を強制し始めます。
  - **September 1, 2020:** MDX暗号化はサポート終了となります。

従来のDAに登録されているデバイスの場合

- MDX暗号化を使用しない場合、操作は不要です。

- MDX暗号化を使用する場合は、July 31, 2020までにAndroidデバイスをAndroid Enterpriseに移行してください。Android 10を実行しているデバイスは、Android Enterpriseを使用して登録または再登録する必要があります。この要件には、MAM専用モードのAndroidデバイスも含まれます。「デバイス管理からAndroid Enterpriseへの移行」を参照してください。

7月31日以降にAndroid Enterpriseに登録済みのデバイスの場合

- Android Enterpriseプラットフォームを使用してアプリを公開した場合、暗号化はすでにAndroid Enterpriseによって処理されています。操作は不要です。
- 従来のAndroidプラットフォームを使用してアプリを公開した場合は、Android Enterpriseを使用してJuly 31, 2020より前にアプリを再公開してください。

XenMobile 10.12（オンプレミス）にアップグレードする前に

システム要件が一部変更されました。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 10.12の最新バージョンにアップデートする前に、Citrix License Serverを11.16以降にアップデートしてください。

   XenMobileの最新バージョンには、Citrix License Server 11.16（最小バージョン）が必要です。

   > **注：**
   >
   > プレビュー版で独自のライセンスを使用する場合は、XenMobile 10.12のCustomer Success Services日付（以前のSubscription Advantage日付）がJanuary 20, 2020であることを認識してください。CitrixライセンスのCustomer Success Services日付は、この日付より後である必要があります。
   >
   > License Serverでライセンスの横に日付を表示できます。最新バージョンのXenMobile®を古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。
   >
   > ライセンスの日付を更新するには、Citrix Portalから最新のライセンスファイルをダウンロードし、そのファイルをライセンスサーバーにアップロードします。詳しくは、「Customer Success Services」を参照してください。

2. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL永続性のために構成されている場合、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を実行している仮想マシンのRAMが4GB未満の場合は、RAMを少なくとも4GBに増やしてください。本番環境での推奨最小RAMは8GBであることに注意してください。
4. 推奨事項：XenMobileのアップデートをインストールする前に、VMの機能を使用してシステムのスナップショットを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に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旧できます。

アップグレードするには

XenMobile 10.11.x または 10.10.x から XenMobile 10.12 に直接アップグレードできます。アップグレードするには、利用可能な最新のバイナリをダウンロードしてください。`<https://www.citrix.com/downloads>` にアクセスします。**Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10** に移動します。ハイパーバイザー用の XenMobile Server ソフトウェアのタイルで、**Download File** をクリックします。

アップグレードをアップロードするには、XenMobile コンソールの **Release Management** ページを使用します。詳細については、「Release Management ページを使用したアップグレード」を参照してください。

アップグレード後

XenMobile 10.12 (オンプレミス) へのアップグレード後:

送信接続を伴う機能が動作しなくなり、接続構成を変更していない場合は、**XenMobile Server ログ**で「Unable to connect to the VPP Server: Host name '192.0.2.0' does not match the certificate subject provided by the peer」のようなエラーがないか確認してください。

証明書の検証エラーは、XenMobile Server でホスト名検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はホスト名検証が有効になっています。ホスト名検証によって展開が中断される場合は、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。

iOS 13 の追加サポート

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ます。このアップグレードは、ユーザーに次のように影響します。

- 登録中に、いくつかの新しい iOS セットアップアシスタントオプション画面が表示されます。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、このバージョンの **Settings > Apple Device Enrollment Program (DEP)** ページに含まれています。XenMobile Server を構成して、これらの画面をスキップできます。これらのページは、iOS 13 デバイスのユーザーに表示されます。
- 以前のバージョンの iOS で監視対象または非監視対象デバイスで利用可能だった一部の制限デバイスポリシー設定は、iOS 13 以降では監視対象デバイスでのみ利用可能です。現在の XenMobile Server コンソールツールヒントは、これらの設定が iOS 13 以降の監視対象デバイス専用であることをまだ示していません。
    - ハードウェアコントロールを許可:
        - FaceTime
        - アプリのインストール
    - アプリを許可:
        - iTunesストア
        - サファリ
        - Safari > 自動入力
    - ネットワーク - iCloudアクションを許可:
        - iCloud書類とデータ
    - 監視対象のみの設定 - 許可:
        - Game Center > 友達を追加
        - Game Center > マルチプレイヤーゲーム
    - メディアコンテンツ - 許可:
        - 露骨な表現を含む音楽、ポッドキャスト、iTunes Uのコンテンツ

これらの制限は次のように適用されます:

- iOS 12 (またはそれ以前) のデバイスがすでにXenMobile Serverに登録されており、その後iOS 13にアップグレードされた場合、前述の制限は非監視対象デバイスと監視対象デバイスの両方に適用されます。
- 非監視対象のiOS 13以降のデバイスがXenMobile Serverに登録された場合、前述の制限は監視対象デバイスにのみ適用されます。
- 監視対象のiOS 13以降のデバイスがXenMobile Serverに登録された場合、前述の制限は監視対象デバイスにのみ適用されます。

Apple ボリューム購入プログラムからApple Business Manager (ABM) およびApple School Manager (ASM) への移行

Apple Volume Purchase Program (VPP) を使用している企業および教育機関は、Apple Business ManagerまたはApple School Managerの「Appとブック」に December 1, 2019 まで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、このAppleサポート記事を参照してください。

組織または学校でVolume Purchase Program (VPP)のみを使用している場合は、ABM/ASMに登録し、既存のVPP購入者を新しいABM/ASMアカウントに招待できます。ASMの場合は`<https://school.apple.com>`に移動します。ABMの場合は`<https://business.apple.com>`に移動します。

XenMobileでVPPアカウントを更新するには：

1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **iOS設定**をクリックします。**Volume Purchase Program**構成ページが表示されます。
3. ABMまたはASMアカウントが、以前のVPPアカウントと同じアプリ構成になっていることを確認してください。
4. ABM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、次の操作を行います。
    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Volume Purchaseアカウントを編集します。
    b. ABMまたはASMの資格情報を編集します。サフィックスは変更しないでください。
    c. **保存**を2回クリックします。

詳しくは、以下を参照してください。

- Apple展開プログラム
- Appleデバイスの一括登録

Android Enterprise COPEデバイスのサポート

XenMobile Server は、以前は COPE (corporate-owned personally enabled) デバイスとして知られていた、ワークプロファイルを持つ Android Enterprise の完全管理対象デバイスをサポートしています。これらのデバイスは、ワークプロファイルも持つ Android Enterprise の完全管理対象デバイスの一種です。デバイスとワークプロファイルに個別のポリシー設定を適用できます。このリリースでは、次のことが可能です。

- これらのデバイスポリシー（資格情報、パスコード、制限）を使用して、デバイスとワークプロファイルに個別の設定を適用できます。
- ロケーションデバイスポリシーのロケーションモード設定は、COPE デバイス自体には適用できますが、COPE デバイスのワークプロファイルには適用できません。ロケーションデバイスポリシーのその他の設定は、COPE デバイスでは利用できません。
- ロックセキュリティアクションは、デバイスまたはワークプロファイルに個別に適用できます。

デバイスポリシー

ワークプロファイルを持つ Android Enterprise の完全管理対象デバイス（COPE デバイス）の場合、一部のデバイスポリシーでは、デバイス全体とワークプロファイルに個別の設定を適用できます。XenMobile Server コンソールでは、一部のデバイスポリシーで個別の設定を適用できます。その他のデバイスポリシーを使用して、デバイス全体にのみ、またはワークプロファイルを持つ完全管理対象デバイスのワークプロファイルにのみ設定を適用できます。

セキュリティアクション

ワークプロファイルを持つ Android Enterprise の完全管理対象デバイス（COPE デバイス）の場合、以下を適用できます。

- ロックセキュリティアクションをデバイスまたはワークプロファイルに個別に適用します。
- その他のすべてのセキュリティアクションをデバイスに適用します。

登録プロファイルによる Android デバイスの登録オプションの制御

XenMobile 展開で Android Enterprise が有効になっている場合、登録プロファイルによって Android デバイスの登録方法が制御されるようになりました。登録プロファイルは、Android デバ

イスがデフォルトの Android Enterprise モード（完全管理対象またはワークプロファイル）で登録されるか、レガシー（デバイス管理者）モードで登録されるかを決定します。

デフォルトでは、グローバル登録プロファイルは、新規および工場出荷時設定にリセットされた Android Enterprise デバイスを完全管理対象デバイスとして登録し、BYOD Android Enterprise デバイスをワークプロファイルデバイスとして登録します。詳細については、「Android Enterprise」を参照してください。

レガシー Android デバイスを Android Enterprise のデフォルト登録として準備する

Google は、デバイス管理のデバイス管理者モードを非推奨とし、すべての Android デバイスを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管理するよう顧客に推奨しています。（Google Android Enterprise 開発者ガイドの「Device admin deprecation」を参照してください。）この変更をサポートするため、Android Enterprise が Android デバイスのデフォルトの登録オプションになりました。

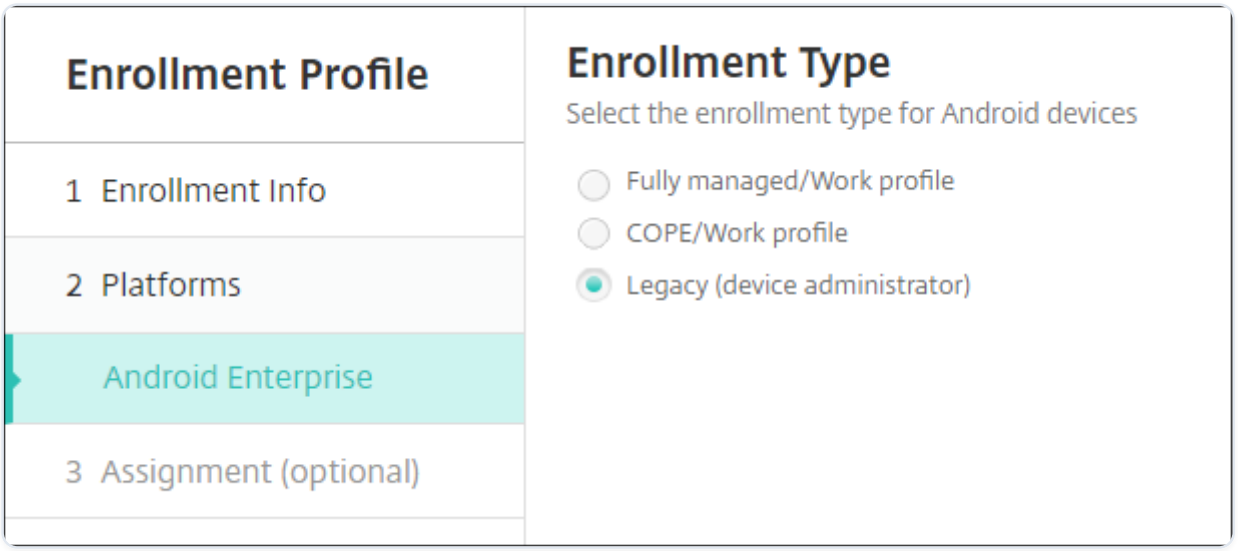
この変更は、XenMobile展開でAndroid Enterpriseが有効になっている場合、新しく登録された、または再登録されたすべてのAndroidデバイスがAndroid Enterpriseデバイスとして登録されることを意味します。

この変更に備えるため、XenMobileでは、Androidデバイスの登録方法を制御する登録プロファイルを作成できるようになりました。

組織によっては、レガシーAndroidデバイスを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管理する準備ができていない場合があります。その場合、デバイス管理者モードで引き続き管理できます。レガシーデバイス用の登録プロファイルを作成し、登録済みのすべてのレガシーデバイスを再登録してください。

レガシーデバイス用の登録プロファイルを作成するには：

1. XenMobileコンソールで、 **>** の順に移動します。
2. 登録プロファイルを追加するには、 をクリックします。ページで、登録プロファイルの名前を入力します。
3. をクリックするか、 の下にある を選択します。ページが表示されます。
4. を に設定します。 をクリックするか、 を選択します。画面が表示されます。



5. 専用デバイスを登録する管理者が属するデリバリーグループを選択します。次に、 をクリックします。

レガシーデバイスをデバイス管理者モードで管理し続けるには、このプロファイルを使用して登録または再登録します。デバイス管理者デバイスは、ユーザーにSecure Hubをダウンロードさせ、登録サーバーURLを提供させることで、ワークプロファイルデバイスと同様に登録します。

Android Enterpriseへの移行に関するEndpoint Managementのサポートの詳細については、ブログ「Citrix Endpoint ManagementサービスにおけるAndroid Enterpriseのデフォルト化」を参照してください。

Android Enterpriseのアプリ管理の簡素化

XenMobile Serverのアプリを承認または公開するために、管理対象のGoogle PlayまたはGoogle Developerポータルにアクセスする必要がなくなりました。その結果、アプリの承認と公開にかかる時間は数時間ではなく約10分になりました。

XenMobile Serverコンソールでパブリックアプリストアの Android Enterpriseアプリを承認します。 XenMobile Serverコンソールを離れることなく、管理対象のGoogle Playストアアプリを承認できるようになりました。検索フィールドにアプリ名を入力すると、管理対象のGoogle PlayストアUIが開き、アプリを承認して保存するための手順が表示されます。その後、アプリが結果に表示され、詳細を構成できるようになります。パブリックアプリストアアプリを追加するを参照してください。

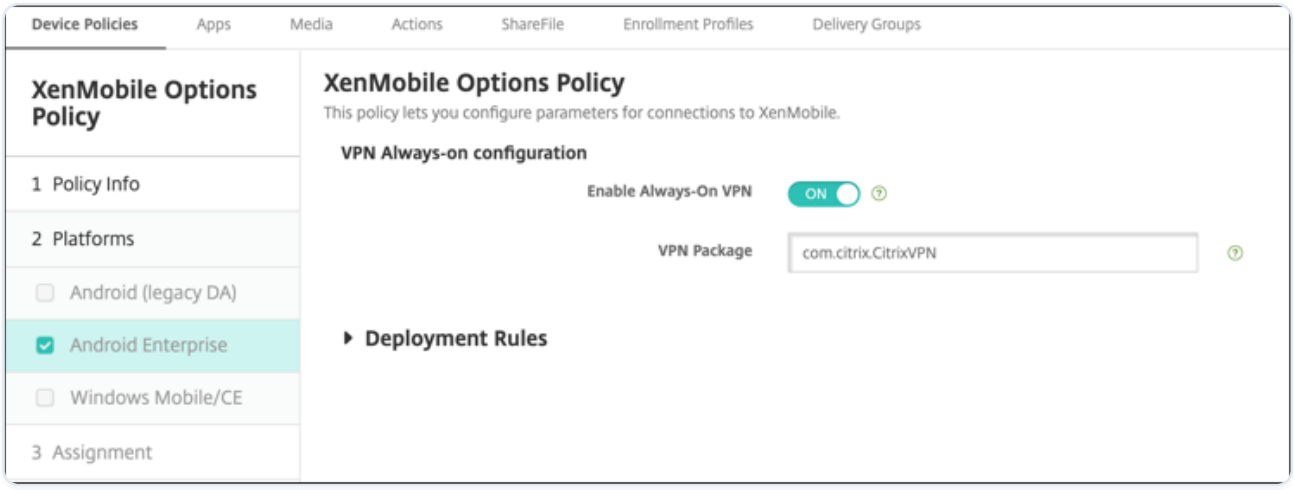
Android Enterprise 用 MDX アプリの追加。 XenMobile Server コンソールは、MDX アプリ展開のプラットフォームとして Android Enterprise をサポートするようになりました。MDX アプリの追加を参照してください。

XenMobile Server コンソールで Android Enterprise 用 MDX アプリを承認する。 XenMobile Server コンソールを離れることなく、Android Enterprise 用の管理対象 Google Play ストアアプリを承認できるようになりました。MDX ファイルをアップロードすると、管理対象 Google Play ストアの UI が開き、アプリを承認して保存するための手順が表示されます。MDX アプリの追加を参照してください。

Android Enterprise の常時接続 VPN のサポート

XenMobile Server のオプションデバイスポリシーで、Android Enterprise の常時接続 VPN を有効にできるようになりました。

Android Enterprise 用の VPN プロファイルを構成するときは、**デフォルトの VPN プロファイル**に VPN プロファイルの名前を入力します。XenMobile は、ユーザーが特定のプロファイルをタップする代わりに、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ときに、このプロファイルを使用します。このフィールドが空の場合、メインプロファイルが接続に使用されます。プロファイルが1つしか構成されていない場合、それはデフォルトプロファイルとしてマークされます。常時接続 VPN の場合、このフィールドには、常時接続 VPN を確立するために使用する VPN プロファイルの名前を設定する必要があります。



Android Enterprise アプリのプロダクトトラックを構成する

Android Enterprise 用のパブリックストアアプリまたは MDX アプリを追加するときは、ユーザーデバイスにプッシュするプロダクトトラックを構成します。たとえば、テスト用に設計されたトラックがある場合、それを選択して特定のデリバリーグループに割り当てることができます。リリースの展開の詳細については、Google Play ヘルプセンターを参照してください。プロダクトトラックの構成については、MDX アプリの追加またはパブリックアプリストアアプリの追加を参照してください。

macOS ユーザーのパスコードリセットを強制する

macOS デバイスがパスコードポリシーを含む構成プロファイルを受信すると、ユーザーはポリシー設定を満たすパスコードを提供する必要があります。ユーザーが次回認証するときに、パスコードのリセットを強制できるようになりました。macOS (10.13 以降) のパスコードデバイスポリシーで、新しい設定**パスコードのリセットを強制**を有効にします。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。

XenMobile Server 10.11 の新機能

XenMobile Server 10.11 (PDFダウンロード)

Apple ボリューム購入プログラムの Apple Business Manager (ABM) および Apple School Manager (ASM) への移行

Apple Volume Purchase Program (VPP) を使用している企業や教育機関は、Apple Business Manager または Apple School Manager の Apps and Books に December 1, 2019 まで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、このAppleサポート記事を参照してください。

組織または学校が Volume Purchase Program (VPP) のみを使用している場合、ABM/ASM に登録し、既存の VPP 購入者を新しい ABM/ASM アカウントに招待できます。ASM の場合は、`<https://school.apple.com>`に移動します。ABM の場合は、`<https://business.apple.com>`に移動します。

XenMobile® で Volume Purchase (旧VPP) アカウントを更新するには：

1. XenMobile コンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **Volume Purchase**をクリックします。**Volume Purchase**構成ページが表示されます。
3. ABM または ASM アカウントが以前の VPP アカウントと同じアプリ構成になっていることを確認してください。
4. ABM 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、次の操作を行います。
    a. その場所の更新されたトークン情報で、既存の Volume Purchase アカウントを編集します。
    b. ABM または ASM の資格情報を編集します。サフィックスは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の追加サポート

重要:

iOS 12以降へのデバイスアップグレードに備えるため: iOS用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VPNデバイスポリシーを作成してください。

VPNデバイスポリシーを削除した後も、以前に展開されたデバイスではCitrix VPN接続は引き続き動作します。新しいVPNデバイスポリシー構成は、ユーザー登録時にXenMobile Server 10.11で有効になります。

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ます。このアップグレードは、ユーザーに次のような影響を与えます。

- 登録中に、いくつかの新しいiOSセットアップアシスタントオプション画面が表示されます。AppleはiOS 13に新しいiOSセットアップアシスタントオプション画面を追加しました。このバージョンでは、新しいオプションは**設定 > Appleデバイス登録プログラム (DEP)**ページに含まれていません。そのため、XenMobile Serverでこれらの画面をスキップするように構成することはできません。これらのページは、iOS 13デバイスのユーザーに表示されます。
- 以前のバージョンのiOSで監視対象または非監視対象デバイスで利用可能だった一部の制限デバイスポリシー設定は、iOS 13以降では監視対象デバイスでのみ利用可能です。現在のXenMobile Serverコンソールのツールヒントは、これらの設定がiOS 13以降の監視対象デバイス専用であることをまだ示していません。
    - ハードウェアコントロールを許可:
        - FaceTime
        - アプリのインストール
    - アプリを許可:
        - iTunes ストア
        - サファリ
        - Safari > 自動入力
    - ネットワーク - iCloudアクションを許可:

        - iCloudの書類とデータ
    - 監視対象のみの設定 - 許可：
        - Game Center > 友達を追加
        - Game Center > マルチプレイヤーゲーム
    - メディアコンテンツ - 許可：
        - 露骨な表現を含む音楽、ポッドキャスト、iTunes Uのコンテンツ

これらの制限は次のように適用されます。

- iOS 12（またはそれ以前）のデバイスがすでにXenMobile Serverに登録されており、その後iOS 13にアップグレードした場合、上記の制限は監視対象外デバイスと監視対象デバイスの両方に適用されます。
- 監視対象外のiOS 13以降のデバイスがXenMobile Serverに登録されると、上記の制限は監視対象デバイスにのみ適用されます。
- 監視対象のiOS 13以降のデバイスがXenMobile Serverに登録されると、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における信頼された証明書の要件

AppleはTLSサーバー証明書に新しい要件を設けています。すべての証明書が新しいAppleの要件に従っていることを確認してください。Appleの公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。証明書の管理については、「XenMobileへ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

April 10, 2018より、GoogleはGoogle Cloud Messaging (GCM) のサポートを終了しました。GoogleはMay 29, 2019にGCMサーバーおよびクライアントAPIを削除しました。

> **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、FCM で利用可能な新機能を利用し始めるために、すぐに Firebase Cloud Messaging (FCM) へのアップグレードを推奨しています。Google からの情報については、`<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サポートを継続するには: XenMobile Server で GCM を使用している場合は、FCM に移行します。その後、Firebase Cloud Messaging Console から入手できる新しい FCM キーで XenMobile Server を更新します。

以下の手順は、信頼された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 からの情報に従って、GCM から FCM にアップグレードします。
2. Firebase Cloud Messaging Console で、新しい FCM キーをコピーします。これは次の手順で必要になります。
3. XenMobile Server コンソールで、 **>** に移動し、設定を構成します。

デバイスは、次回 XenMobile Server にチェックインしてポリシーを更新するときに FCM に切り替わります。Secure Hub にポリシーを強制的に更新させるには: Secure Hub で、 **>** に移動し、をタップします。 FCM の構成の詳細については、Firebase Cloud Messaging を参照してください。

XenMobile 10.11 (オンプレミス) にアップグレードする前に

システム要件の一部が変更されました。詳細については、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更新する前に、Citrix License Server を 11.15 以降に更新してください。

   XenMobile の最新バージョンには、Citrix License Server 11.15 (最小バージョン) が必要です。

   > **注:**
   >
   > プレビュー版で独自のライセンスを使用する場合、XenMobile 10.11のカスタマーサクセスサービス日（旧サブスクリプションアドバンテージ日）はApril 9, 2019です。Citrixライセンスのカスタマーサクセスサービス日は、この日付より後である必要があります。

> ライセンスサーバーで、ライセンスの横に日付が表示されます。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、接続性チェックが失敗し、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、そのファイルをライセンスサーバーに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. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL永続性のために構成されている場合、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を実行している仮想マシンのRAMが4GB未満の場合、RAMを少なくとも4GBに増やしてください。本番環境での推奨最小RAMは8GBであることに留意してください。
4. 推奨事項：XenMobileのアップデートをインストールする前に、VMの機能を使用してシステムのスナップショットを作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に問題が発生した場合でも、完全なバックアップがあれば回復できます。

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。アップグレードを行うには、利用可能な最新のバイナリをダウンロードしてください。`<https://www.citrix.com/downloads>`にアクセスします。**Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10**に移動します。お使いのハイパーバイザー用のXenMobile Serverソフトウェアのタイルで、**Download File**をクリックします。

アップグレードをアップロードするには、XenMobileコンソールの**Release Management**ページを使用します。詳しくは、「Release Managementページを使用してアップグレードするには」(/ja-jp/xenmobile/server/upgrade.html#to-upgrade-using-the-release-management-page)を参照してください。

アップグレード後

XenMobile 10.11 (オンプレミス) にアップグレードした後：

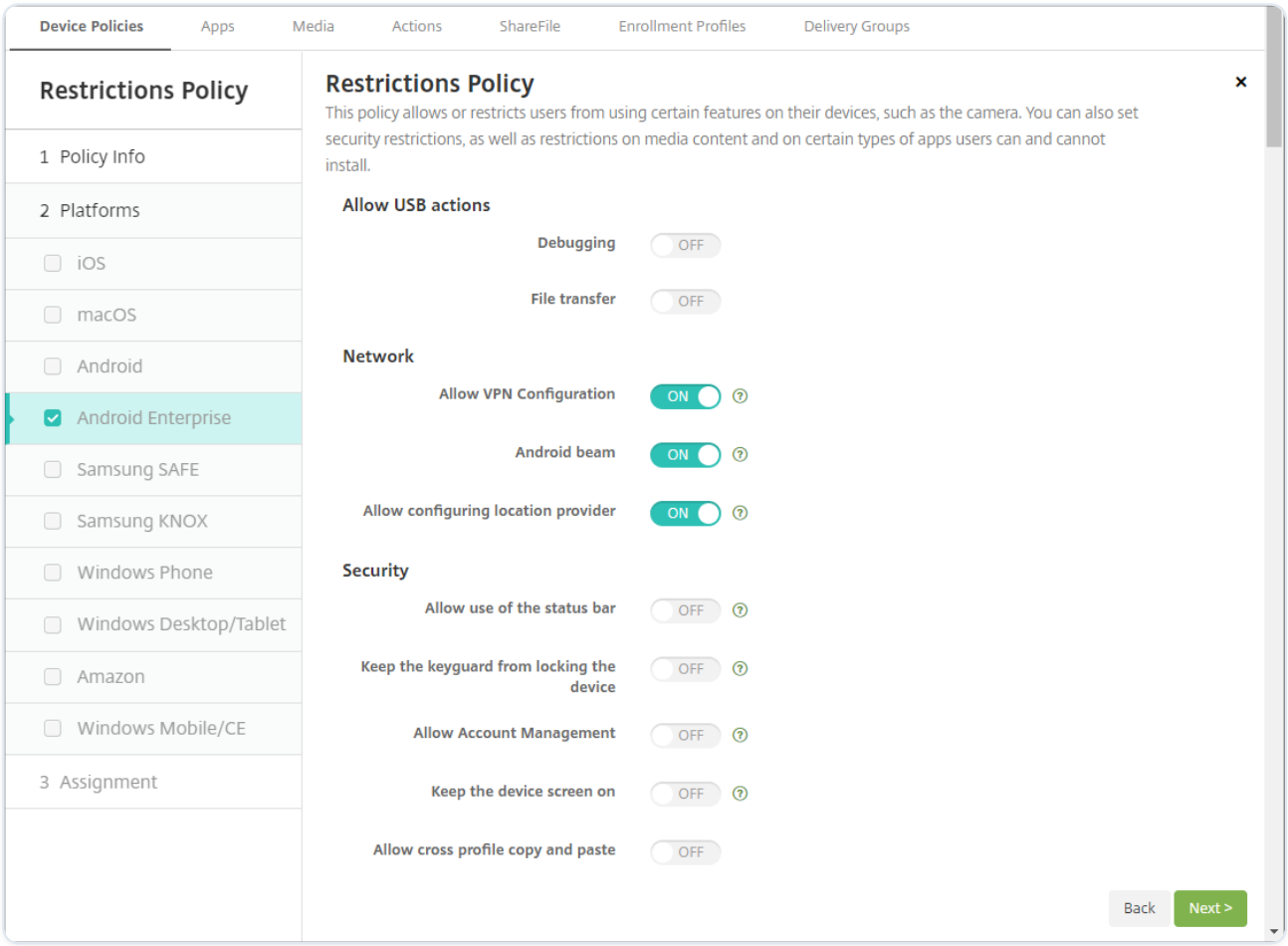
発信接続に関連する機能が動作しなくなり、接続構成を変更していない場合は、XenMobile Serverログで次のようなエラーを確認してください：「VPPサーバーに接続できません：ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません」。

証明書検証エラーは、XenMobile Serverでホスト名検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サーバーを除く発信接続でホスト名検証が有効になっています。ホスト名検証によって展開が機能しなくなる場合は、サーバープロパティ `disable.hostname.verification` を `true` に変更してください。このプロパティのデフォルト値は `false` です。

Android Enterpriseデバイス向け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ポリシーの統合。 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、統合されたデバイスおよびプロファイル管理ソリューションに結合されます。 以下のデバイスポリシーのAndroid EnterpriseページでKnox設定を構成します。

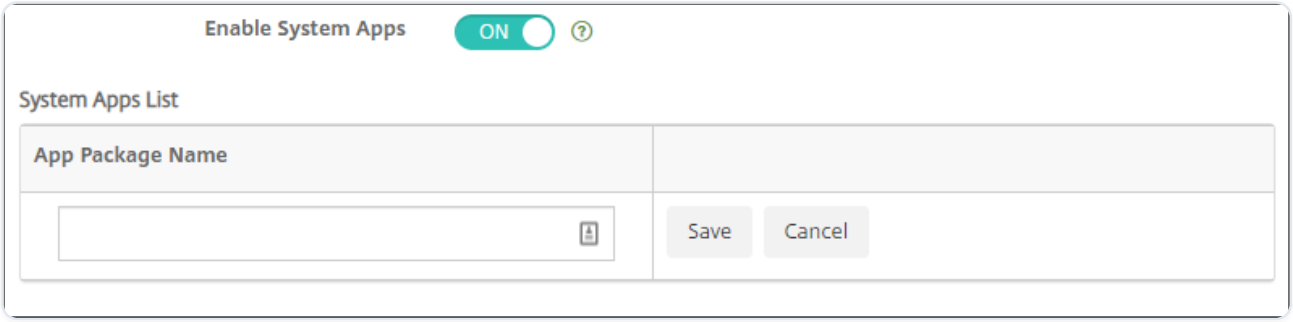
- OSアップデートデバイスポリシー。 Samsung Enterprise FOTAアップデートの設定が含まれます。
- パスコードデバイスポリシー。
- **Samsung MDMライセンスキーデバイスポリシー。** Knoxライセンスキーを構成します。
- 制限デバイスポリシー設定。



Android Enterprise向けアプリインベントリデバイスポリシー。 管理対象デバイス上の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ストア内のすべてのGoogle Playアプリにアクセスする。 管理対象Google Playストア内のすべてのアプリにアクセスするサーバープロパティにより、公開Google Playストアのすべてのアプリが管理対象Google Playストアからアクセス可能になります。このプロパティを**true**に設定すると、すべてのAndroid Enterpriseユーザーが公開Google Playストアアプリを利用できるようになります。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する。 Android Enterpriseの仕事用プロファイルモードまたは完全管理モードで、ユーザーがプリ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るようになります。特定のアプリへのアクセスを制限するには、Android Enterpriseアプリ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、以前は企業所有シングルユース（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を満たすために特化した、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ために必要な1つのアプリまたは少数のアプリに制限されます。また、ユーザーが他のアプリを有効にしたり、デバイスで他の操作を行ったりすることを防ぎます。

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

ポリシー名の変更。 Googleの用語に合わせるため、Android Enterpriseアプリ制限デバイスポリシーは、管理対象構成デバイスポリシーと呼ばれるようになりました。「管理対象構成デバイスポリシー」を参照してください。

Android Enterpriseのロックとパスワードのリセット

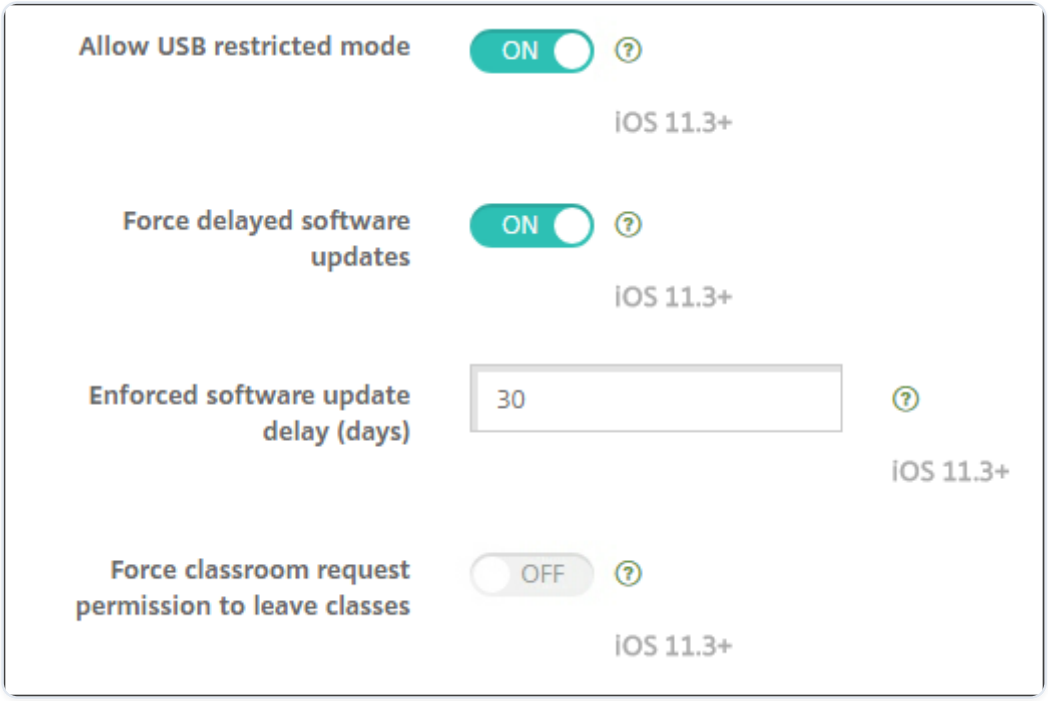
XenMobileは、Android Enterpriseデバイスのロックおよびパスワードのリセットセキュリティアクションをサポートするようになりました。これらのデバイスは、Android 8.0以降を実行する仕事用プロファイルモードで登録されている必要があります。

- 送信されたパスコードはワークプロファイルをロックします。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要件を満たさない場合:
  - ワークプロファイルにパスコードがまだ設定されていない場合、デバイスはロックされます。
  - ワークプロファイルにパスコードがすでに設定されている場合。ワーク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。

ロックおよびパスワードリセットのセキュリティアクションの詳細については、「セキュリティアクション」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

- **管理対象外アプリが管理対象連絡先を読み取る:** オプション。**管理対象外アプリの管理対象アプリからのドキュメント**が無効になっている場合にのみ利用可能です。このポリシーが有効になっている場合、管理対象外アプリは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ます。デフォルトは**オフ**です。iOS 12以降で利用可能です。
- **管理対象アプリが管理対象外連絡先に書き込む:** オプション。有効にすると、管理対象アプリが管理対象外アカウントの連絡先に連絡先を書き込むことを許可します。**管理対象外アプリの管理対象アプリからのドキュメント**が有効になっている場合、この制限は効果がありません。デフォルトは**オフ**です。iOS 12以降で利用可能です。
- **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以降で利用可能です。
- **パスワード近接リクエスト:** 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から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以降で利用可能です。
- **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以降で利用可能です。
- **日付と時刻の自動設定を強制:** 監視対象。有効にすると、ユーザーは**一般 > 日付と時刻 > 自動設定**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以降で利用可能です。
- **USB制限モードを許可:** 監視対象デバイスでのみ利用可能です。オフに設定すると、デバイスはロックされている間でも常にUSBアクセサリに接続できます。デフォルトは**オン**です。iOS 11.3以降で利用可能です。
- **ソフトウェアアップデートの遅延を強制:** 監視対象デバイスでのみ利用可能です。**オン**に設定すると、ユーザーへのソフトウェアアップデートの表示を遅らせます。この制限が有効な場合、ユーザーはソフトウェアアップデートのリリース日から指定された日数が経過するまでソフトウェアアップデートを表示しません。デフォルトは**オフ**です。iOS 11.3およびmacOS 10.13.4以降で利用可能です。
- **強制ソフトウェアアップデート遅延 (日数):** 監視対象デバイスでのみ利用可能です。この制限により、管理者はデバイス上のソフトウェアアップデートを遅延させる期間を設定できます。最大は90日で、デフォルト値は**30**です。iOS 11.3およびmacOS 10.13.4以降で利用可能です。
- **授業を離れるためのClassroomリクエスト許可を強制：** 監視対象デバイスでのみ利用可能です。**On**に設定されている場合、Classroomで管理されていないコースに登録されている生徒は、コースを離れようとするときに教師に許可を求める必要があります。デフォルトは**Off**です。iOS 11.3以降で利用可能です。



「」を参照してください(/ja-jp/xenmobile/server/policies/restrictions-policy.html)。

iOSまたはmacOS向けExchangeデバイスポリシーの更新

iOS 12以降のS/MIME Exchange署名および暗号化設定の追加。 Exchangeデバイスポリシーに、S/MIME署名と暗号化を設定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署名ユーザーによる上書き可能：** **On**に設定されている場合、ユーザーはデバイスの設定でS/MIME署名をオン/オフにできます。デフォルトは**Off**です。
- **S/MIME署名証明書UUIDユーザーによる上書き可能：** **On**に設定されている場合、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。デフォルトは**Off**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切り替えを有効にする：** **On**に設定されている場合、ユーザーが作成する各メッセージに対してS/MIME暗号化をオンまたはオフに切り替えるオプションが表示されます。デフォルトは**Off**です。
- **S/MIMEデフォルト暗号化ユーザーによる上書き可能：** **On**に設定されている場合、ユーザーはデバイスの設定で、S/MIMEをデフォルトでオンにするかどうかを選択できます。デフォルトは**Off**です。

- **S/MIME暗号化証明書UUIDユーザーによる上書き可能： On**に設定されている場合、ユーザーはデバイスの設定でS/MIME暗号化IDと暗号化をオン/オフにできます。デフォルトは**Off**です。

iOS 12以降のExchange OAuth設定。 Exchangeとの接続をOAuth認証を使用するように構成できるようになりました。

macOS 10.14 以降の Exchange OAuth 設定。 認証に OAuth を使用するように Exchange との接続を構成できるようになりました。OAuth を使用した認証の場合、AutoDiscovery 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 向けメールデバイスポリシーの更新

iOS 12 以降の S/MIME Exchange 署名および暗号化設定の追加。 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設定が追加されました。

S/MIME 署名の場合:

- **S/MIME 署名を有効にする:** このアカウントが S/MIME 署名をサポートするかどうかを選択します。デフォルトは **On** です。**On** に設定すると、以下のフィールドが表示されます。
  - **S/MIME 署名ユーザーによる上書き可能: On** に設定すると、ユーザーはデバイスの設定で S/MIME 署名をオン/オフできます。デフォルトは **Off** 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 ユーザーによる上書き可能: On** に設定すると、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。デフォルトは **Off** 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 暗号化を有効にする:** このアカウントが 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 **Off** です。**On** に設定すると、以下のフィールドが表示されます。
  - **メッセージごとの S/MIME 切り替えを有効にする: On** に設定すると、ユーザーが作成する各メッセージで S/MIME 暗号化をオンまたはオフに切り替えるオプションが表示されます。デフォルトは **Off** です。
  - **S/MIME 暗号化のデフォルト設定ユーザーによる上書き可能: On** に設定すると、ユーザーはデバイスの設定で、S/MIME をデフォルトでオンにするかどうかを選択できます。デフォルトは **Off** 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 ユーザーによる上書き可能: On** に設定すると、ユーザーはデバイスの設定で S/MIME 暗号化 ID と暗号化をオン/オフできます。デフォルトは **Off** 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 向けアプリ通知デバイスポリシーの更新

iOS 12以降で、以下のアプリ通知設定が利用可能です。

- **CarPlayで表示: オン**の場合、通知はApple CarPlayに表示されます。デフォルトは**オン**です。
- **重大な通知を有効にする: オン**の場合、アプリは通知を「おやすみモード」や着信音設定を無視する重大な通知としてマークできます。デフォルトは**オフ**です。

「アプリ通知デバイスポリシー」を参照してください。(/ja-jp/xenmobile/server/policies/apps-notifications-policy.html)

Apple Educationで使用される共有iPadのサポート

Apple Education機能とのXenMobile統合が、共有iPadをサポートするようになりました。教室の複数の生徒が、1人または複数の教師が教えるさまざまな科目でiPadを共有できます。

管理者または教師が共有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、生徒は管理対象のApple ID資格情報を提供して共有iPadにサインインします。以前に教育構成ポリシーを生徒に展開していた場合、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がなくなります。

共有iPadの前提条件:

- iPad Pro、iPad（第5世代）、iPad Air 2以降、iPad mini 4以降のいずれか
- 32 GB以上のストレージ
- 監視対象

詳しくは、「共有iPadの構成」(/ja-jp/xenmobile/server/provision-devices/integrate-with-apple-education.html#configure-shared-ipads)を参照してください。

ロールベースのアクセス制御（RBAC）の権限変更

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を使用したロールの構成」(/ja-jp/xenmobile/server/users/rbac-roles-and-permissions.html)を参照してください。

サードパーティ通知

このXenMobile®リリースには、以下のドキュメントに定義されている条件に基づいてライセンス供与されたサードパーティ製ソフトウェアが含まれている場合があります。

XenMobileサードパーティ通知

廃止

この記事でのお知らせは、段階的に廃止されるXenMobile Serverの機能について、事前に通知することを目的としています。この情報を提供することで、お客様がタイムリーなビジネス上の意思決定を行えるようにします。Citrixは、いつ機能が撤回されるかを判断するために、お客様の使用状況とフィードバックを監視しています。お知らせは、その後のリリースで変更される可能性があり、すべての廃止された機能や機能性を含まない場合があります。製品ライフサイクルサポートの詳細については、「製品ライフサイクルサポートポリシー」の記事を参照してください。

廃止と削除

次のリストは、廃止または削除されたXenMobile® Serverの機能を示しています。

*廃止された*項目は、すぐに削除されるわけではありません。Citrix®は、将来のリリースで削除されるまで、廃止された項目をサポートし続けます。

*削除された*項目は、XenMobile Serverから削除されたか、サポートされなくなっています。

サポート終了となったモバイル生産性向上アプリについては、「EOLおよび廃止されたアプリ」を参照してください。

項目	説明	廃止発表	削除済み	代替
ファイルベースのライセンス	ファイルベースのライセンスは、April 15, 2026以降は機能しなくなります。	2025年10月	2026年4月	License Activation Service (LAS) は、Citrix 製品スイート全体で製品アクティベーションを行うための次世代テクノロジーで

項目	説明	廃止発表	削除済み	代替
				す。ファイルベースのライセンスを使用しているお客様は、互換性のあるリリースにアップグレードし、April 15, 2026 までにこのテクノロジー移行を実行する必要があります。April 15, 2026 以降、LAS は Citrix オンプレミスコンポーネントをアクティベートおよびライセンス供与する唯一の方法となります。
ゼンモバイルメールマネージャー (XMM)/ゼンモバイルネットスケーラーコネクター (XNC)	XMM および XNC のサポートは廃止されました。	2025年6月	2025年9月	代替手段はありません。
ハイパーバイザー	Citrix XenServer 8.2 以前、VMware ESXi 6.x 以前、および Hyper-V 2016 のサポートは廃止されました。	2025年3月	2025年5月	システムを次のいずれかのサポートされているバージョンに更新してください: Citrix Hypervisor 8.2 CU1 以降、VMware (ESXi 7.0、ESXi 8.0)、または

項目	説明	廃止発表	削除済み	代替
				Hyper-V (Windows Server 2019 または Windows Server 2022)。
ShareFile との統合	ShareFile (現 Progress) がサポートを終了した場合、ShareFile との統合は廃止されます。	2025年1月		代替手段なし
Zebra 用カスタム XML	Zebra デバイスでのカスタム XML のサポートは非推奨になりました	2022 年 1 月	目標: 2022 年 6 月	Android Enterprise の管理対象構成を使用します。
Windows インフォメーションプロテクション (WIP)	Microsoft からの発表 (https://techcommunity.microsoft.com/t5/windows-it-pro-blog/announcing-the-sunset-of-windows-information-protection-wip/ba-p/3579282) に基づき、Windows Information Protection のサポートは非推奨になりました。	2022 年 8 月	目標: 2022 年 10 月	代替手段なし
XenMobile アナライザー	XenMobile Analyzer ツー	2022 年 7 月	目標: March 31, 2023	代替手段なし

項目	説明	廃止発表	削除済み	代替
	ルのサポートは非推奨になりました。			
PKI ID: 汎用、Symantec PKI、DigiCert、およびEntrustアダプター	汎用、DigiCert管理、およびEntrustアダプターPKIエンティティのサポートは非推奨になりました。	2021年6月	2022年1月	代替手段なし
登録招待のセットアップ	デバイスのIMEI、シリアル番号、およびUDIDを使用して登録招待を作成するサポートは非推奨になりました。	2022年1月	2022年5月	登録招待を作成するときは、XenMobileコンソールの**管理 > 登録招待**で利用可能な設定を構成します。
キャリアSMSゲートウェイ	Nexmo SMSゲートウェイ通知のサポートは非推奨になりました。	2022年1月	2022年4月	SMTP サーバー通知を使用
モバイルサービスプロバイダー (MSP)	Blackberry およびその他のExchange ActiveSync デバイスを照会し、操作を発行するためのMSP インターフェースのサポートを廃止	2022年1月	2022年4月	代替なし
Samsung キオスクモード	Device Admin (DA) モードに基づくレガシーSamsung キオ	2022年1月	2022年3月	Android Enterprise (AE)

項目	説明	廃止発表	削除済み	代替
	スクモードのサポートを廃止.			キオスクモードを使用.
Windows デバイスの Wi-Fi Sense ホットスポットへの自動接続制限を許可	Windows 10 デバイスの Wi-Fi Sense ホットスポットへの自動接続制限のサポートを削除。Windows 10 はこの機能をサポートしなくなりました。詳細については、Microsoft ドキュメントを参照してください。	2021年10月	2022年2月	代替手段なし
Samsung SAFE/Samsung Knoxプラットフォーム	SAFEおよびKnoxプラットフォームのサポートは非推奨になりました。	2022年1月	2022年6月	Android Enterpriseを使用してKnoxポリシーを設定するには、管理対象アプリ構成ポリシーを介してKnox Serviceプラグインを使用します。
高セキュリティ登録モード	**高セキュリティ**登録セキュリティモードでの登録招待状の生成は非推奨になりました。	2021年7月	2022年2月	サポートされている登録セキュリティモードのリストについては、デバイスの登録を参照してください。
RBACロール - 共有デバイス登録者および	共有デバイス登録者とCOSUデバイス登録者の	2021年7月	2021年12月	iOSデバイスはサポートされている登録方法で

項目	説明	廃止発表	削除済み	代替
COSUデバイス登録者	両方に対する事前定義されたロールベースのアクセス制御設定のサポートは非推奨になりました。			構成します。Android COSU (専用) デバイスは登録プロファイルで構成します。
ノックス モバイル エンロールメント (従来のDA)	すべてのAndroidバージョンで、レガシーのデバイス管理者モードにおけるKnox Mobile Enrollment (KME) のサポートは非推奨になりました。	2021年5月	2021年6月	KMEを使用してAndroid Enterpriseモードに登録します。Android 9、10、11はAndroid Enterpriseをサポートしています。
Android 7.xおよびiOS 12.x向けのCitrixモビリティアプリとWorkspaceアプリ	Secure Hub、Secure Mail、Secure Web、およびCitrix WorkspaceアプリのAndroid 7.xおよびiOS 12.xバージョンのサポートは非推奨になりました。	2021年4月	2021年6月	各主要オペレーティングシステムプラットフォームの、少なくとも現在および以前のバージョンを使用してください。古いデバイスは登録されたままになります。ただし、Citrixはレガシーデバイスのテストやサポートは行いません。
派生資格情報	派生資格情報およびCitrix Derived Credentials	2021年3月	2021年12月	iOSでサポートされている認証タイプの一覧については、iOS

項目	説明	廃止発表	削除済み	代替
	Managerアプリのサポートは非推奨になりました。			を参照してください。
インターネットエクスプローラー 11	XenMobile ServerコンソールでのInternet Explorerの使用のサポートを廃止しました。	2021年1月	2021年1月	これらのWebブラウザの最新バージョンを使用してください: Google Chrome、Mozilla Firefox、Microsoft Edge、Apple Safari
Android向けRSAソフトトークンのサポート	Android版Secure HubへのRSAソフトトークンの直接インポートのサポートを廃止しました。	2021年1月	2021年2月	Google Playで入手可能なRSA Secure IDアプリ内でRSAソフトトークンをインポートできます。その後、Citrix Gateway認証にそのトークンを使用できます。
アンドロイド - ソニー	Android Sonyデバイスおよび Sony固有のポリシーのサポートを廃止しました。	2021年1月	2022年2月	Android Enterprise を使用
アンドロイド・エイチティーシー	Android HTC デバイスおよび HTC 固有のポリシーのサポー	2021年1月	2022年2月	Android Enterprise を使用

項目	説明	廃止発表	削除済み	代替
	トは非推奨になりました。			
アンドロイド・アマゾン	Android Amazon デバイスおよび Amazon 固有のポリシーのサポートは非推奨になりました。	2021年1月	2022年2月	Android Enterprise を使用
XenMobile ダッシュボードのサードパーティコンポーネント	XenMobile ダッシュボードの一部として使用されているサードパーティコンポーネントは非推奨になります。	2020年12月	2021年1月	ダッシュボードを引き続き使用するには、XenMobile 10.12以降にアップグレードしてください。
Android Enterpriseデバイス上のレガシーデバイス管理者モード用に公開されたアプリ	レガシーDAプラットフォーム用に公開されたアプリは、Android Enterpriseに登録されているデバイスには配信されなくなりました。	2020年10月	2020年11月	Android Enterpriseデバイスの場合、Android Enterpriseプラットフォーム用にアプリを公開します。DAモードのデバイスにレガシーDAアプリを公開し続けるには、それらのアプリ用に個別のデリバリーグループを作成します。
APNs送信ポート	APNsレガシーバイナリプロトコルに対する	2020年10月	2021年3月	代わりにポート443または2197を使用してくだ

項目	説明	廃止発表	削除済み	代替
	Appleのサポートは、March 31, 2021をもって終了します。Appleは、代わりにHTTP/2ベースのAPNsプロバイダーAPIを使用することを推奨しています。この変更の一環として、`*.push.apple.com`にAPNs通知を送信するために使用されるポート2195および2196のサポートを非推奨とします。			さい。デバイスを管理するためのXenMobileポートを開くを参照してください。
Samsung SEAMSコンテナ	Samsung SEAMSコンテナのサポートを非推奨としました。	2020年6月	2020年8月	Android Enterprise 用の Samsung Knox Service Plug-in (KSP) アプリを使用します。「Knox サービスプラグインアプリの追加」を参照してください。
自己署名型 Secure Sockets Layer (SSL) 証明書	すべてのデバイスプラットフォームにおける自己署名型 SSL 証明書のサポートは非推奨になりました。	2020年5月		既存の自己署名型証明書を、信頼できる認証局 (CA) からの信頼された SSL 証明書に置き換えてください。

XENMOBILE®サーバー

項目	説明	廃止発表	削除済み	代替
証明書ベースの認証署名アルゴリズム (非FIPSおよび脆弱な暗号)	以下の署名アルゴリズムのサポートは非推奨になりました: SHA1withRSA、SHA224withRSA、SHA1withECDSA、SHA224withECDSA、SHA1withDSA、RIPEMD160withRSA、RIPEMD128withRSA、RIPEMD256withRSA。	2020年5月	2021年6月	XenMobile コンソールで資格情報プロバイダーの CSR を作成する際 (**Settings > Credential Providers > Certificate Signing Request**)、より強力な暗号を選択してください。
データベースサーバー	Microsoft SQL Server 2014 以前のサポートは非推奨になりました。	2021年10月	2022年8月	システムを以下のサポート対象バージョンいずれかに更新してください: Microsoft SQL Server 2016 SP2、Microsoft SQL Server 2017 CU 13、または Microsoft SQL Server 2019 CTP 3.2。「システム要件と互換性」でサポート対象サーバーのリストを参照してください。

XENMOBILE®サーバー

項目	説明	廃止発表	削除済み	代替
ハイパーバイザー	Citrix XenServer 6.5.x以前、VMware ESXi 5.5 Update 3以前、およびHyper-V 2012のサポートは非推奨になりました。	2020年5月	2020年8月	システムを以下のサポート対象バージョンいずれかに更新してください: Citrix Hypervisor 8.0以降、Citrix XenServer 7.0以降、VMware (ESXi 6.0、ESXi 6.5.0 Update 3、ESXi 6.7 Update 2 patch 10、またはESXi 7.0)、またはHyper-V (Windows Server 2016またはWindows Server 2019)。
シトリックス ランチャー	レガシーCitrix Launcherアプリのサポートは非推奨になりました。	2020年5月	2020年8月 (アプリストアから削除)	プロビジョニングされたデバイスをキオスク (専用デバイス) として使用し、Android Enterprise向けCitrix Launcherを使用してください。詳細については、Citrix Launcherの代替を参照してください。
Android 6.xおよびiOS 11.x向けCitrixモビリティアプリおよ	Secure Hub、Secure Mail、Secure Web、およびCitrix	2020年4月	2020年6月	各主要オペレーティングシステムプラットフォームの、少

項目	説明	廃止発表	削除済み	代替
びWorkspaceアプリ	WorkspaceアプリのAndroid 6.xおよびiOS 11.xバージョンのサポートは非推奨になりました。			なくとも現在および以前のバージョンを使用してください。
MDX ツールキットとMDXサービス	Mobile App Management (MAM) SDKを優先して、MDX ToolkitとMDX Serviceのサポートを廃止しました。移行期間中は、MDXでラップされたアプリとMAM SDKで開発されたアプリの両方を使用できます。	2020年3月	目標: 2023年7月	エンタープライズアプリケーションの管理を継続するには、MAM SDKを使用してください。
MDX: 代替ゲートウェイサーバー	iOSおよびAndroidデバイスのステップアップ認証を廃止しました。	2020年3月	2021年9月	代替なし
MDX: Micro VPN (フルトンネルモード)	iOSおよびAndroidデバイスのフル仮想プライベートネットワーク (VPN) トンネルを廃止しました。	2020年3月	2021年9月	MAM SDK Web SSOモードを使用するか、Citrix SSO接続タイプでアプリごとのVPNポリシーを作成してください。
MDX: PACファイルサポート	iOSおよびAndroidデバイス向けのフル	2020年3月	2021年9月	内部ネットワークへのアクセスには、Citrix

項目	説明	廃止発表	削除済み	代替
	VPNトンネル展開でのプロキシ自動構成 (PAC) ファイルのサポートを廃止しました。			Gatewayを使用してプロキシサーバー経由で接続します。
MDX共有デバイスサポート	MDXアプリの共有デバイスサポートを廃止しました。	2020年3月	2021年9月	Android Enterpriseの場合、MDMの共有デバイスサポートを使用します。iOSの場合、Apple School ManagerまたはGroundControlを使用します。
Android 10の新しいデバイス管理者登録	Android 10デバイスでのレガシーデバイス管理者モードへの新規登録または再登録のサポートを廃止しました。すでに登録されているデバイスは引き続き機能します。	2020年2月	2020年9月	新しいAndroid 10以降のデバイスをAndroid Enterpriseに登録します。
Android 10デバイス向けのレガシーデバイス管理者モード	Googleは一部のデバイス管理者APIを非推奨にしました。Citrixは、Android APIレベル29をターゲットとするCitrix Secure Hub™へのアッ	2020年2月	2020年11月	Android 10デバイスをAndroid Enterpriseに移行します。

項目	説明	廃止発表	削除済み	代替
	プグレード以降、デバイス管理者モードに登録されたAndroid 10デバイスをサポートしていません。			
MDX暗号化	MDX暗号化およびXenMobileコンソール内のMDX暗号化機能は非推奨になりました。	2019年10月	2020年9月	コンプライアンスチェックが追加された暗号化管理機能を使用して、iOSまたはAndroidプラットフォームの暗号化を有効にします。2020年7月までにMDX暗号化からの移行をテストし、計画していることを確認してください。
パスコードデバイスポリシー：Android Enterpriseの**制限なし**設定	Android 7以降を実行しているAndroid Enterpriseデバイスは、文字制限付きで作成されたパスコードのみをサポートします。以前に**必須文字**を**制限なし**に設定していた場合、この更新によりその値が**数字のみ**に変更されます。	2019年2月	2019年4月	この変更は、現在のユーザーサインインエクスペリエンスには影響しません。

XENMOBILE®サーバー

項目	説明	廃止発表	削除済み	代替
リモートサポート	クラスター化されたオンプレミスXenMobile Server展開用のリモートサポートクライアントは非推奨になりました。	2019年1月	2020年8月	代替手段なし
iOS用Secure Hubネットワーク拡張機能	Secure Hubリリース20.3.0以降、iOSデバイスのネットワーク機能をカスタマイズできるネットワーク拡張フレームワークは非推奨になりました。	2018年10月	2020年3月	代替手段なし
TLSバージョン1.0および1.1	XenMobileのセキュリティを向上させるため、Citrixは現在、Transport Layer Security (TLS) 1.0および1.1を介したすべての通信をブロックしています。セキュリティの弱体化により、PCI CouncilはTLS 1.0およびTLS 1.1を非推奨にしています。	2018年6月	2019年3月	TLS 1.2にアップグレードしてください。
ウィンドウズモバイル/CE	Windows Mobile/CE デバイスのサポート	2018年4月	2020年9月	Windows 10デスクトップおよびノートPCを

項目	説明	廃止発表	削除済み	代替
	は非推奨になりました。			使用してください。
アンドロイドタッチダウン	DigiCertはAndroid TouchDownのサポートを終了しました。Citrixは、ExchangeデバイスポリシーからAndroid TouchDownプラットフォームページを削除します。	2018年7月	2021年	推奨事項: Citrix Secure Mailを使用してください。
フルVPNトンネル - Android	AndroidフルVPNトンネルのサポートは非推奨になりました。	2020年3月	2021年9月	MAM SDK Web SSOモード。
VPNモード切り替えの許可 - Android	AndroidのVPNモード切り替え許可のサポートは非推奨になりました。	2020年3月	2021年9月	代替手段なし
インバウンドドキュメント交換 - Android	Androidのインバウンドドキュメント交換のサポートは非推奨になりました。	2020年3月	2021年9月	代替手段なし

修正された問題

XenMobile 10.16には、以下の修正された問題が含まれています。

- XenMobile Server 10.16バージョンにアップグレードした後、XenMobile ServerはSyslogサーバーへのログ送信を停止しました。
- プロキシが構成されている場合、HTTP v1 APIを使用するFirebase Cloud Messagingが正常に機能しません。
- **MAM専用**モードで登録されたiOSデバイスでは、Secure Hubストアからエンタープライズアプリまたは MDXアプリをインストールできません。
- Android Enterpriseデバイスで**管理対象構成ポリシー**を編集または展開すると、エラーが表示されます。
- アプリのトラックIDを構成した後、XenMobile® Serverコンソールでアプリの期待されるプレビューバージョンが表示されません。代わりに、アプリの製品版が表示されます。
- XenMobile Serverでは、プロビジョニングプロファイルデバイスポリシーが保留状態の場合、Secure HubストアからMDXラップされたアプリをインストールできません。
- MDMプロファイルの更新後、ABM共有iPadは管理対象外の状態になります。
- アルゴリズムAPK署名スキームv2以降を使用している場合、Androidプラットフォームでエンタープライズアプリを構成できません。
- device/filter APIを使用してデバイスをエクスポートできません。
- NetScaler®でnFactor認証ポリシーを使用してAndroidまたはiOSデバイスをMAMとMDMの両方に登録すると、デバイスはMDMのみに登録されます。
- XenMobile Serverバージョン10.14以降でCitrix Gateway認証の構成スクリプトをエクスポートすると、スクリプトが切り詰められ、機能しません。
- XenMobile Serverでは、説明に**\b**が含まれる同期されたVPPアプリを再編集できません。
- XenMobile Serverバージョン10.15以降では、Online Certificate Status Protocol (OCSP)が要求に応答しません。
- XenMobile Server で、Windows 11 を実行しているデバイスを登録できません。
- Android デバイスで、従来の MDX Toolkit から MAM SDK に切り替えると、Secure Mail アプリが Secure Hub Store から削除されます。

- XenMobile Server コンソールで、Rapid Security Response (RSR) のバージョンを確認できません。
- **Managed Google Play Accounts** からアプリをダウンロードできません。
- XenMobile Server 10.16 にアップグレードした後、「Restricted App usage」を使用する既存の iOS 制限デバイスポリシーが iOS デバイスに展開されません。
- ABM または ASM 構成を使用している場合、iOS 共有デバイスに Webclip デバイスポリシーを展開できません。
- **Android Enterprise** > **Managed Google Play Store apps** の **Configure** > **Apps** ページで、**Organize Apps** ボタンが表示されません。
- **Android Enterprise** プラットフォームの Wi-Fi ポリシーを構成する際に、**CA certificate** ドロップダウンメニューに値が表示されません。**Select certificate** オプションのみが表示されます。
- バージョン 10.15.0 ローリングパッチリリースで修正された問題については、以下を参照してください。
  - XenMobile Server 10.15 Rolling Patch 8 のリリースノート
  - XenMobile Server 10.15 Rolling Patch 7 のリリースノート
  - XenMobile Server 10.15 Rolling Patch 6 のリリースノート
  - XenMobile Server 10.15 Rolling Patch 5 のリリースノート
  - XenMobile Server 10.15 Rolling Patch 4 のリリースノート
  - XenMobile Server 10.15 Rolling Patch 3 のリリースノート

関連情報

XenMobileサポート知識センター

既知の問題

XenMobile 10.16には既知の問題はありません。

- モバイル生産性アプリに関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。
- 最新バージョン10.15.0のローリングパッチにおける既知の問題については、XenMobile Server 10.15 Rolling Patch 7のリリースノートを参照してください。

関連情報

XenMobileサポート知識センター

アーキテクチャ

組織のデバイスおよびアプリ管理要件によって、XenMobileアーキテクチャのXenMobile®コンポーネントが決まります。XenMobileのコンポーネントはモジュール式で、相互に連携します。たとえば、展開にはCitrix Gatewayが含まれます。

- Citrix Gatewayは、ユーザーにモバイルアプリへのリモートアクセスを提供し、ユーザーデバイスの種類を追跡します。
- XenMobileは、それらのアプリとデバイスを管理する場所です。

XenMobileコンポーネントの展開：XenMobileを展開して、ユーザーが次の方法で内部ネットワークのリソースに接続できるようにすることができます。

- 内部ネットワークへの接続。ユーザーがリモートの場合、Citrix Gatewayを介したVPNまたはマイクロVPN接続を使用して接続できます。この接続により、内部ネットワーク内のアプリとデスクトップにアクセスできます。
- デバイス登録。ユーザーはモバイルデバイスをXenMobileに登録できるため、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、およびモバイルアプリ。ユーザーは、Secure Hubを介してXenMobileからWeb、SaaS、およびモバイルアプリにアクセスできます。
- Windowsベースのアプリ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、StoreFrontまたはWeb InterfaceからWindowsベースのアプリと仮想デスクトップにアクセスできます。

オンプレミスのXenMobile Serverでこれらの機能を実現するには、CitrixはXenMobileコンポーネントを次の順序で展開することをお勧めします。

- Citrix Gateway。クイック構成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ようにCitrix Gatewayの設定を構成できます。Citrix Gatewayでクイック構成ウィザードを使用する前に、通信を設定するために次のいずれかのコンポーネントをインストールする必要があります：XenMobile、StoreFront、またはWeb Interface。
- XenMobile。XenMobileをインストールした後、ユーザーがモバイルデバイスを登録できるように、XenMobileコンソールでポリシーと設定を構成できます。モバイル、Web、SaaSアプリも構成できます。モバイルアプリには、Apple App StoreまたはGoogle Playのアプリを含める

ことができます。ユーザーは、MDX Toolkitでラップしてコンソールにアップロードしたモバイルアプリにも接続できます。

- MAM SDKまたはMDX Toolkit。MDXラッピングテクノロジーは、2023年7月にサポート終了（EOL）となる予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDKを組み込む必要があります。

  Mobile Application Management（MAM）SDKは、iOSおよびAndroidプラットフォームでカバーされていないMDX機能を提供します。iOSまたはAndroidアプリをMDX対応にして保護できます。これらのアプリは、内部ストアまたは公開アプリストアで利用できるようにします。(/ja-jp/mdx-toolkit/mam-sdk-overview.html)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ベースのアプリと仮想デスクトップへのアクセスを提供できます。
- Citrix Files (オプション)。Citrix Files を展開する場合、XenMobile を介してエンタープライズディレクトリ統合を有効にできます。XenMobile 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の詳細については、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。このセクションでは、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、Citrix はスケーラビリティとサーバー冗長性の両方のために、XenMobile ソリューションをクラスター構成で展開することを推奨しています。また、Citrix ADC の 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、スループットを向上させることができます。Citrix ADC で2つの負荷分散仮想 IP アドレスを構成して XenMobile のクラスタリングを設定する方法の詳細については、「クラスタリング」を参照してください。

災害復旧展開のために XenMobile を構成する方法の詳細については、展開ハンドブックの「災害復旧」の記事を参照してください。この記事にはアーキテクチャ図が含まれています。

以下のセクションでは、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記事「オンプレミス展開のリファレンスアーキテクチャ」および「アーキテクチャ」を参照してください。ポートの完全なリストについては、「ポート要件」(オンプレミス) および「ポート要件」(クラウド) 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 モードを構成し、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 は、ユーザー登録後に認証モードを変更することをサポートしていません。詳細については、「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 はモバイルデバイス管理を提供します。プラットフォームのサポートについては、「サポートされてい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予定がある場合は、XenMobile を MDM モードで展開します。たとえば、次のような場合です。

- デバイスポリシーとアプリを展開する。
- 資産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 Server は DMZ に配置され、オプションで Citrix ADC が前面に配置され、XenMobile の保護を強化します。

モバイルアプリ管理 (MAM) モード

MAM (MAM 専用モードとも呼ばれます) は、モバイルアプリ管理を提供します。プラットフォームのサポートについては、「サポートされてい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予定がある場合は、XenMobile を MAM モードで展開します。たとえば、次のような場合です。

- BYOモバイルデバイス上のアプリとデータを保護する。
- エンタープライズモバイルアプリを配信する。
- アプリをロックし、そのデータをワイプする。

デバイスはMDMに登録できません。

この展開モデルでは、XenMobile ServerはCitrix Gatewayの前に配置され、XenMobileの保護を強化します。

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、およびモバイルデバイスの管理が提供されます。プラットフォームのサポートについては、「サポートされてい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機能を使用する予

定がある場合は、XenMobileをENT（エンタープライズ）モードで展開します。たとえば、次のような場合です。

- MDMを使用して企業支給デバイスを管理する
- デバイスポリシーとアプリを展開する
- 資産インベントリを取得する
- デバイスをワイプする
- エンタープライズモバイルアプリを配信する
- アプリをロックし、デバイス上のデータをワイプする

推奨される展開モデルでは、XenMobile ServerはDMZに配置され、その前にCitrix Gatewayが置かれることで、XenMobileの保護が強化されます。

内部ネットワーク内のXenMobile: もう1つの展開オプションは、オンプレミスのXenMobile ServerをDMZではなく内部ネットワークに配置することです。この展開は、セキュリティポリシーでネットワークアプライアンスのみをDMZに配置する必要がある場合に利用されます。この展開では、XenMobile ServerはDMZにありません。したがって、DMZからSQL ServerおよびPKIサーバーへのアクセスを許可するために、内部ファイアウォールでポートを開く必要はありません。

システム要件と互換性

> **注:**
>
> この記事では、XenMobile Server 10.16 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は、「システム要件」を参照してください。

> その他の要件と互換性情報については、以下の記事を参照してください。

- XenMobile の互換性
- サポートされているデバイスの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 準拠
- 言語サポート

XenMobile 10.16 を実行するには、以下の最小システム要件が必要です。

- 次のいずれか:
  - Citrix Hypervisor 8.2 CU1 および 8.4。詳細については、「XenServer」を参照してください。Citrix Hypervisor バージョン 8.2 CU1 以降では、準仮想化 (PV) VM はサポートされなくなりました。XenServer をアップグレードする前にハードウェア仮想化モード (HVM) に移行してください。詳細については、「Citrix Hypervisor バージョン 8.2 CU1 以降での HVM イメージの使用」を参照してください。XenServer のアップグレードの詳細については、「XenServer のアップ3グレード」を参照してください。
  - VMware (サポートされているバージョン: ESXi 6.0、ESXi 6.5.0 Update 3、または ESXi 6.7 Update 2 patch 10、ESXi 7.0 Update 3g、ESXi 8.0 Update 2)。詳細については、「ESXi 6.7 の回避策」および「VMware」を参照してください。
  - Hyper-V (サポートされているバージョン: Windows Server 2016およびWindows Server 2019)。詳細については、Hyper-Vを参照してください。

- Exchange ActiveSync 10.1.10用のEndpoint Managementコネクタ、またはExchange ActiveSync 8.5.3.19用のCitrix Gatewayコネクタ
- デュアルコアプロセッサ
- 仮想CPU 4基
- 実稼働環境には8 GBのRAM。概念実証およびテスト環境には4 GBのRAM。
- 50 GBのディスク容量
- シトリックス ライセンスサーバー 11.16.

  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てください。

ESXi 6.7の回避策

ESXi 6.7を機能させるには、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ファイルを抽出します。OVFツールはVMwareのページ(https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491)から入手してください。
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. 新しい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 virtual machine**を選択します。
   b. ゲストOSファミリーには、**Linux**を選択します。
   c. ゲストOSのバージョンには、**Other 2.6.x Linux (64-bit)** を選択します。
   d. データストアには、**Default** 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コントローラー、CD/DVDドライブを削除します。
   f. ネットワークで、アダプターの種類として **VMXNET3** を選択します。
   g. ESXiで、ディスクがローカルの場合は **SCSI Controller** と **LSI Logic Parallel** 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の作成を完了します。
4. データストアに移動し、以前にアップロードした.vmdkファイルをコピーします。そのファイルをXenMobile用に作成したVMディレクトリにコピーします。
5. ESXiのWebインターフェイスから、VMを選択し、設定を編集します。

6. **Add Hard disk** をクリックします。
7. 以前にコピーした.vmdkファイルを選択し、VMにアタッチします。
8. **Save** をクリックします。
9. VMの電源をオンにします。

Citrix Gatewayのシステム要件

XenMobile 10.16でCitrix Gatewayを実行するには、以下の最小システム要件が必要です。

- Citrix Gateway (オンプレミス)。サポートされるバージョン: 12.1以降
- Active Directory と通信できる必要もあります。これにはサービスアカウントが必要です。クエリと読み取りアクセスのみが必要です。

XenMobile 10.16 のデータベース要件

XenMobile には、次のいずれかのデータベースが必要です。

- マイクロソフト SQL Server

  XenMobile は、次のサポートされているバージョンのいずれかで実行されている Microsoft SQL Server データベースをサポートしています。Microsoft SQL Server データベースとそのハードウェア要件の詳細については、Microsoft のドキュメントを参照してください。

  - マイクロソフト SQL Server 2016 SP3
  - マイクロソフト SQL Server 2017 CU 31
  - マイクロソフト SQL Server 2019 CU 25
  - マイクロソフト SQL Server 2022 CU 12

  Microsoft SQL Server データベースの要件は、展開の規模によっても異なります。展開規模に応じた Microsoft SQL Server データベースの要件の詳細については、「スケーラビリティ」を参照してください。

  XenMobile は、データベースの高可用性のために SQL Basic Availability Groups (Always On 可用性グループ) および SQL Clustering をサポートしています。

  Citrix は、Microsoft SQL をリモートで使用することを推奨しています。

  Microsoft SQL のアップグレードについては、Microsoft の記事「SQL Server のアップグレード」を参照してください。

- PostgreSQL (テスト環境のみ)。PostgreSQL は XenMobile に含まれています。テスト環境では、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。テスト環境で作成されたデータベースを本番環境に移動することはできません。

  すべての XenMobile エディションは、Windows 用の Remote PostgreSQL 9.5.1 および 9.5.11 をサポートしていますが、以下の制限があります。本番環境には推奨されません。最大 300 台のデバイスをサポートします。300 台を超えるデバイスにはオンプレミスの SQL Server を使用してください。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 で使用する SQL Server のサービスアカウントに `DBcreator` ロールのアクセス許可があることを確認してください。XenMobile Server のインストール時に指定する SQL Server アカウントのパスワードを記録しておいてください。このパスワードは、XenMobile Server のリカバリ中に XenMobile データベースをクローンする必要がある場合に必要になります。

Transparent Data Encryption (TDE) を使用して SQL Server データベースを保護してください。オンプレミス展開のリファレンスアーキテクチャ に示されているように、SQL Server ポートへの外部アクセスを許可しないでください。

SQL Server サービスアカウントの詳細については、Microsoft ドキュメントサイトの以下のページを参照してください。これらのリンクは SQL Server 2014 の情報を示しています。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** リストからサーバーのバージョンを選択してください。

- Windows サービスアカウントとアクセス許可の構成
- サーバーレベルのロール

Virtual Apps and Desktops の互換性

- バーチャルアプリおよびデスクトップ 7.15 LTSR CU3
- バーチャルアプリおよびデスクトップ 7.1811
- 仮想アプリとデスクトップ 7 1906
- 仮想アプリとデスクトップ 7 1909
- バーチャルアプリおよびデスクトップ 7 2006

StoreFront™ の互換性

- StoreFront 3.12.2

- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

その他の互換性

- Exchange ActiveSync 用 エンドポイント管理 コネクタ 10.1.10
  - 以前のバージョンはテストされていません
- Exchange ActiveSync 用 シトリックス ゲートウェイ コネクタ 8.5.3.19
  - 以前のバージョンはテストされていません

XenMobile® 互換性

> **注記:**

> この記事では、XenMobile Server の互換性について説明します。Endpoint Management 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。

> 新機能、修正、およびポリシーの更新を使用するには、Citrix® は、以下の最新バージョンをインストールすることをお勧めします。

- Citrix は、エンタープライズ iOS および Android アプリに Mobile Application Management (MAM) SDK を統合し、MDX 機能をアプリに適用することを推奨します。

  MDX Toolkit は、2023 年 7 月にサポート終了 (EOL) となる予定です。エンタープライズアプリの管理を継続するには、MAM SDK を組み込む必要があります。

この記事では、統合できるサポート対象の XenMobile コンポーネントのバージョンを要約しています。

互換性とアップグレードパス

Secure Hub、MDX Toolkit、およびモバイル生産性向上アプリの最新バージョンは、XenMobile Server の現在および以前のバージョンと互換性があります。

モバイル生産性向上アプリの最新バージョンには、Secure Hub の最新バージョンが必要です。アプリの以前の 2 つのバージョンは、最新の Secure Hub と互換性があります。詳細については、Citrix 製品マトリックスを参照してください。

Citrix は、XenMobile 生産性向上アプリの配布をパブリックアプリストアからのみサポートしています。

XenMobile Server (オンプレミス)

- Citrix は、XenMobile Server の過去 2 つのバージョンからのアップグレードをサポートしています。
- XenMobile Server の最新バージョン: XenMobile Server 10.16
- アップグレード元:
  - XenMobile サーバー 10.15.x
  - XenMobile サーバー 10.14.x

モバイル生産性向上アプリ

ユーザーは、公開アプリストアからモバイル生産性向上アプリにアクセスします。モバイル生産性向上アプリの最新バージョンには、Secure Hubの最新バージョンが必要です。アプリの2つ前のバージョンは、最新のSecure Hubと互換性があります。

モバイル生産性向上アプリの2週間ごとの段階的リリースサイクルについては、リリーススケジュールを参照してください。サポートの詳細については、モバイル生産性向上アプリのサポートを参照してください。

MAM SDK

MAM SDKは、iOSおよびAndroidプラットフォームではカバーされていないMDX機能を提供します。これらのアプリは、社内ストアまたは公開アプリストアで利用可能にできます。MDX App SDKを参照してください。

MDX ツールキット

MDXラッピングテクノロジは、2023年7月にサポート終了 (EOL) となる予定です。エンタープライズアプリケーションの管理を継続するには、MAM SDKを組み込む必要があります。

Citrixは、MDX Toolkitの最新3リリース (n.n.n) をサポートしています。MDX Toolkitの新機能を参照してください。

ブラウザのサポート

XenMobile Serverコンソールには、次のいずれかのサポートされているWebブラウザが必要です。

- Google Chromeの最新バージョン
- Mozilla Firefoxの最新バージョン
- Microsoft Edgeの最新バージョン
- Apple Safari の最新バージョン

サポートされているデバイスのオペレーティングシステム

> **注：**
>
> この記事では、XenMobile Server でサポートされているデバイスの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、「サポートされているデバイスのオペレーティングシステム」を参照してください。

> XenMobile® は、アプリおよびデバイス管理を含むエンタープライズモビリティ管理のために、以下のプラットフォームおよびオペレーティングシステムを実行しているデバイスをサポートしています。プラットフォームの制限とセキュリティ機能のため、XenMobile はすべてのプラットフォームですべての機能をサポートしているわけではありません。

> **注：**
>
> XenMobile Server は、Windows x86 および ARM タイプのデバイスのデバイス管理をサポートしています。

> この記事で説明されているサポート対象デバイスプラットフォームの情報は、Exchange ActiveSync 用 XenMobile コネクタおよび Exchange ActiveSync 用 Citrix Gateway connector™ にも適用されます。

モバイル生産性向上アプリの最新バージョンと MDX 暗号化でサポートされているデバイスについては、「モバイル生産性向上アプリのサポート」を参照してください。

注：

Citrix® は、各主要オペレーティングシステムプラットフォームの現在のバージョンと以前のバージョンを最低限サポートしています。Endpoint Management の新しいバージョンのすべての機能が、古いプラットフォームリリースで動作するわけではありません。

非推奨のお知らせについては、「非推奨」を参照してください。

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ています。

- **アンドロイド:** 10.x、11.x、12.x、13.x、14.x、15.x、16.x、17.x

  Android 10 以降については、「Android の考慮事項」を参照してください。

- **アイオーエス** バージョン： 13.x, 14.x, 15.x, 16.x, 17.x, 18.x, 26.x, 27.x

  XenMobile および Citrix モバイルアプリは、iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x、および iOS 27.x に対応していますが、現在のところ、すべての新しい iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x、および iOS 27.x 機能には対応していません。iOS 14.x、iOS 15.x、iOS 16.x、iOS 17.x、iOS 18.x、iOS 26.x、および iOS 27.x 向けの社内エンタープライズアプリをラップするには、MDX Toolkit 21.8.5 以降を使用するか、MAM SDK を使用してアプリを準備してください。

- **アイパッドオーエス：** 13.x, 14.x, 15.x, 16.x, 17.x, 18.x,26.x, 27.x

  XenMobile および Citrix モバイルアプリは、iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x、および iPadOS 27.x に対応していますが、現在のところ、すべての新しい iPadOS 14.x、iPadOS 15.x、iPadOS 16.x、iPadOS 17.x、iPadOS 18.x、iPadOS 26.x、および iPadOS 27.x 機能には対応していません。

- **macOSのバージョン:** 11.x、12.x、13.x、14.x、15.x

  XenMobile および Citrix モバイルアプリは、macOS 11、macOS 12、macOS 13、macOS 14、および macOS 15 に対応していますが、現在のところ、macOS 11、macOS 12、macOS 13、macOS 14、および macOS 15 のすべての新機能には対応していません。

- **Windows デスクトップおよびタブレット:** (MDM のみ)。Windows 10 および Windows 11

Android に関する考慮事項

重要:

デバイス管理モードはサポートされなくなりました。詳しくは、「デバイス管理から Android Enterprise への移行」を参照してください。

- Citrix では、Android デバイスをレガシーデバイス管理モードで登録しないことを推奨しています。Google はデバイス管理 API を非推奨にしたため、Android 10 以降を実行しているデバイスに影響があります。レガシーデバイス管理モードでの Android デバイスの登録は失敗します。Citrix は、Android 11 デバイスのデバイス管理モードでの登録をサポートしていません。
- Citrix では、Android 10 デバイスに Android Enterprise を使用することを推奨しています。詳しくは、「デバイス管理から Android Enterprise への移行」を参照してください。
- Google API の変更は、MAM 専用モードで登録されたデバイスには影響しません。

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) 拡張機能に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てください。
- ホスト名を検証するには、サーバーは、一致するSANを持つ証明書を提示する必要があります。Citrixは、ホスト名と一致するSANを持つ証明書のみを信頼します。

ポート要件

デバイスとアプリがXenMobile®と通信できるようにするには、ファイアウォールで特定のポートを開きます。以下の表に、開く必要があるポートを示します。

アプリを管理するためのCitrix GatewayとXenMobileのオープンポート

Citrix Secure Hub™、Citrix Receiver、およびCitrix Gatewayプラグインからのユーザー接続をCitrix Gateway経由で以下のコンポーネントに許可するには、以下のポートを開きます。

- XenMobile
- StoreFront™
- シトリックス バーチャルアプリおよびデスクトップ™
- Exchange ActiveSync 用 シトリックス ゲートウェイ コネクタ™
- その他の内部ネットワークリソース（イントラネットWebサイトなど）

Citrix ADCからLaunch Darklyへのトラフィックを有効にするには、このサポート知識センターの記事に記載されているIPアドレスを使用できます。

Citrix Gatewayの詳細については、Citrix Gatewayのドキュメントを参照してください。このドキュメントには、Citrix ADC IP (NSIP)、仮想サーバーIP (VIP)、およびサブネットIP (SNIP) アドレスに関する情報が含まれています。

TCPポート	説明	ソース	宛先
21 または 22	サポートバンドルをFTPまたはSCPサーバーに送信するために使用されます。	XenMobile	FTPまたはSCPサーバー
53 (TCPおよびUDP)	DNS接続に使用されます。	シトリックス ゲートウェイ、ゼノモバイル	DNSサーバー
80	Citrix Gatewayは、VPN接続を2番目のファイアウォールを介して内部ネットワークリソースに渡します。この状況は通常、ユーザーがCitrix Gatewayプラグインでログオンした場合に発生します。	シトリックス ゲートウェイ	イントラネットWebサイト
80または8080; 443	列挙、チケット発行、認証に使用されるXMLおよびSecure Ticket Authority (STA) ポート。Citrixはポート443の使用を推奨しています。	StoreFrontおよびWeb Interface XMLネットワークトラフィック; Citrix Gateway STA	仮想アプリまたはデスクトップ
123 (TCP および UDP)	Network Time Protocol (NTP) サービスに使用されます。	シトリックス ゲートウェイ; ゼノモバイル	NTPサーバー

TCPポート	説明	ソース	宛先
389	安全でないLDAP接続に使用されます	シトリックス ゲートウェイ; ゼノモバイル	LDAP認証サーバーまたはMicrosoft Active Directory
443	Citrix Receiver™ または Receiver for Web から StoreFront を経由して Virtual Apps および Desktops に接続するために使用されます。	インターネット	シトリックス ゲートウェイ
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	シトリックス ゲートウェイ
443	XenMobile Serverへの一般的なデバイス通信に使用されます。	XenMobile	XenMobile
443	モバイルデバイスからXenMobileへの登録用接続に使用されます。	インターネット	XenMobile
443	XenMobileからExchange ActiveSync用Citrix Gatewayコネクタへの接続に使用されます。	XenMobile	Exchange ActiveSync 用 シトリックス ゲートウェイ コネクタ
443	Citrix Gateway connector for Exchange ActiveSync から	Citrix Gateway の Exchange ActiveSync コネクタ	XenMobile

TCPポート	説明	ソース	宛先
	XenMobile への接続に使用されます。		
443	証明書認証を使用しない展開でのコールバック URL に使用されます。	XenMobile	シトリックス ゲートウェイ
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
636	セキュアな LDAP 接続に使用されます。	シトリックス ゲートウェイ; ゼノモバイル	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®接続に使用されます。Citrixは、このポートを開いたままにすることを推奨します。	シトリックス ゲートウェイ	バーチャルアプリまたはデスクトップ
1812	RADIUS接続に使用されます。	シトリックス ゲートウェイ	RADIUS認証サーバー
2598	セッションの信頼性を使用して、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。Citrixは、このポートを開いたままにすることを推奨します。	シトリックス ゲートウェイ	バーチャルアプリまたはデスクトップ
3268	Microsoftグローバルカタログの安全でな	シトリックス ゲートウェイ; ゼノモバイル	LDAP認証サーバーまたはActive Directory

TCPポート	説明	ソース	宛先
	いLDAP接続に使用されます。		
3269	Microsoft Global Catalogのセキュアな LDAP接続に使用されます。	シトリックス ゲートウェイ; ゼノンモバイル	LDAP認証サーバーまたはActive Directory
9080	Citrix ADCと Exchange ActiveSync用Citrix Gatewayコネクタ間のHTTPトラフィックに使用されます。	シトリックス エーディーシー	エクスチェンジ アクティブシンク用シトリックス ゲートウェイ コネクタ
30001	HTTPSサービスの初期ステージング用管理API	内部LAN	ゼノンモバイル サーバー
9443	Citrix ADCと Exchange ActiveSync用Citrix Gatewayコネクタ間のHTTPSトラフィックに使用されます。	シトリックス エーディーシー	Exchange ActiveSync 用 Citrix Gateway コネクタ
45000; 80	クラスターに展開されている場合、2つのXenMobile VM間の通信に使用されます。ポート80は、ノード間通信およびSSLオフロード用です。	XenMobile	XenMobile
8443	登録、XenMobile Store、およびモバイルアプリ管理 (MAM) に使用されます。	XenMobile; Citrix Gateway; デバイス; インターネット	XenMobile

TCPポート	説明	ソース	宛先
4443	管理者がブラウザを介してXenMobileコンソールにアクセスするために使用されます。また、1つのノードからすべてのXenMobileクラスターノードのログとサポートバンドルをダウンロードするためにも使用されます。	アクセスポイント(ブラウザ); XenMobile	XenMobile
27000	外部のCitrix License Serverにアクセスするため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
161	UDPプロトコルを使用した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トラップアラートを送信するために使用されます。送信元はXenMobileで、宛先はSNMP Managerです。	XenMobile	SNMP マネージャー

デバイスを管理するために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、以下のポートを開放してください。

XENMOBILE®サーバー

TCPポート	説明	ソース	宛先
25	XenMobile通知サービスのデフォルトSMTPポート。SMTPサーバーが別のポートを使用している場合は、ファイアウォールがそのポートをブロックしないようにしてください。	XenMobile	SMTPサーバー
80 および 443	Apple iTunes App StoreまたはGoogle Playへのエンタープライズアプリストア接続（80を使用する必要があります）。Appleボリューム購入に使用されます。iOSまたはAndroid用Secure Hubからアプリストアの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 or 443	XenMobile と Nexmo SMS Notification Relay 間の送信接続に使用されます。	XenMobile	Nexmo SMS リレーサーバー
389	安全でない 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 の登録とエージェントのセットアップに使用されます。	インターネット	XenMobile

TCPポート	説明	ソース	宛先
443	Android および Windows デバイス、ならびに MDM リモートサポートクライアントの登録とエージェントのセットアップに使用されます。	インターネット LAN および Wi-Fi	XenMobile
1433	リモートデータベースサーバーへの接続にデフォルトで使用されます（オプション）。	XenMobile	SQLサーバー
443 または 2197	`*.push.apple.com` に APNs 通知を送信するために使用されます。	XenMobile	インターネット (パブリック IP アドレス 17.0.0.0/8 を使用する APNs ホスト
5223	iOS デバイスから `*.push.apple.com` への APNs アウトバウンド接続に使用されます。	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 を使用する APNs ホスト)
8081	オプションの MDM Remote Support Client からのアプリトンネルに使用されます。デフォルトは 8081 です。	リモートサポートクライアント	XenMobile
8443	iOS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

AutoDiscoveryサービス接続のポート要件

このポート構成により、Secure Hub for Androidから接続するAndroidデバイスが、内部ネットワーク内からCitrix AutoDiscovery Service (ADS)にアクセスできるようになります。ADSを通じて提供されるセキュリティ更新プログラムをダウンロードするには、ADSへのアクセスが必要です。

注:

ADS接続はプロキシサーバーをサポートしない場合があります。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できるようにします。

証明書ピンニングを有効にする場合は、次の前提条件を実行してください。

- **XenMobile ServerおよびCitrix ADC証明書を収集します。** 証明書はPEM形式であり、秘密鍵ではなく公開証明書である必要があります。
- **Citrixサポートに連絡し、証明書ピンニングを有効にするようリクエストしてください。** このプロセス中に、証明書の提出を求められます。

証明書ピンニングでは、デバイスが登録される前にADSに接続する必要があります。この要件により、最新のセキュリティ情報がSecure Hubで利用可能になります。Secure Hubがデバイスを登録するには、デバイスがADSに到達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アクセスを開放することは、デバイスの登録を可能にする上で非常に重要です。

Secure Hub for AndroidまたはiOSがADSにアクセスできるようにするには、次のFQDNに対してポート443を開放します。

FQDN	ポート	IPおよびポートの使用状況
`discovery.cem.cloud.us`	443	Secure Hub - CloudFront経由のADS通信

サポートされているIPアドレスについては、AWSのクラウドベースストレージセンターを参照してください。

Android Enterpriseのネットワーク要件

Android Enterpriseのネットワーク環境をセットアップする際に考慮すべきアウトバウンド接続については、Googleサポート記事Android Enterpriseネットワーク要件を参照してください。

XenMobileのポート要件

Managed Google Play Enterpriseを作成し、Managed Google Play iFrameにアクセスするには、以下の宛先ホストがネットワークから到達可能である必要があります。Googleは、アプリの検索と承認を簡素化するために、EMM開発者向けにManaged Play iFrameを提供しました。Managed

Play iFrameを使用するには、XenMobileコンソールにアクセスするブラウザがGoogle Playにアクセスできる必要があります。

宛先ホスト	ポート	説明
`play.google.com`	TCP/443	Google Playストア、Play Enterpriseのサインアップに使用されます
`*.googleapis.com`	TCP/443	Google Mobile Management、Google API、Google PlayストアAPI、FCMに使用されます
`accounts.youtube.com`, `accounts.google.com`	TCP/443	アカウント認証に使用されます
`apis.google.com`	TCP/443	Googleウェブサービスに使用されます
`ogs.google.com`	TCP/443	iFrame UI要素に使用されます
`notifications.google.com`	TCP/443	デスクトップおよびモバイル通知に使用されます
`fonts.googleapis.com`, `*.gstatic.com`, `*.googleusercontent.com`	TCP/443	Google Fontsのユーザー生成コンテンツに使用されます。たとえば、ストア内のアプリアイコンなどです
`cri.pki.goog`, `ocsp.pki.goog`	TCP/443	証明書の検証に使用されます

スケーラビリティとパフォーマンス

XenMobile®インフラストラクチャの規模を理解することは、XenMobileの展開方法と構成方法を決定する上で重要な役割を果たします。この記事には、スケーラビリティテストのデータと、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におけるパフォーマンスとスケーラビリティのインフラストラクチャ要件を決定するためのガイダンスが含まれています。

ここでいうスケーラビリティとは、展開にすでに登録されているデバイスが同時に展開に再接続できる能力のことです。

- *スケーラビリティ*は、展開に登録されている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、既存のデバイスが展開に再接続できる最大レートとして定義されます。

この記事のデータは、10,000台から75,000台のデバイス規模の展開でのテストから得られたものです。テストは、既知のワークロードを使用するモバイルデバイスで構成されました。

すべてのテストは、XenMobile Advanced Edition (オンプレミス) または Citrix Endpoint Management™ (クラウド) で実施されました。

テストはCitrix Gateway 8200を使用して行われました。同等以上の容量を持つCitrix ADCアプライアンスでも、同等以上のスケーラビリティとパフォーマンスが得られると予想されます。

スケーラビリティテスト結果の概要を以下に示します。

最大75,000台のデバイス展開におけるスケーラビリティテスト結果の概要

ログインレート (既存ユーザーの再接続レート) — 1時間あたり最大9,375台のデバイス

使用された構成:

- シトリックス ゲートウェイ
- MPX 8200
- XenMobile Advanced Edition (オンプレミス) または Citrix Endpoint Management (クラウド)
- XenMobile Server 7ノードクラスター
- データベース: Microsoft SQL Server 外部データベース

デバイス数とハードウェア構成別のテスト結果

デバイス数	12,500	30,000	60,000	75,000
既存デバイスの1時間あたりの再接続率	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®サーバー

デバイス数	12,500	30,000	60,000	75,000
XenMobile Server – クラスター	N/A	3	5	7
XenMobile Server – 仮想アプライアンス	メモリ = 8 GB RAM; vCPU = 4	メモリ = 16 GB RAM; vCPU = 6	メモリ = 24 GB RAM; vCPU = 8	メモリ = 24 GB RAM; vCPU = 8
アクティブディレクトリ	メモリ = 4 GB RAM; vCPU = 2	メモリ = 8 GB RAM; vCPU = 4	メモリ = 16 GB RAM; vCPU = 4	メモリ = 16 GB RAM; vCPU = 4
Microsoft SQL Server 外部データベース	メモリ = 8 GB RAM; vCPU = 4	メモリ = 16 GB RAM; vCPU = 8	メモリ = 24 GB RAM; vCPU = 16	メモリ = 24 GB RAM; vCPU = 16

スケーラビリティプロファイル

アクティブディレクトリ構成	使用プロファイル
ユーザー	100,000
グループ	200,000
ネストのレベル	5

XENMOBILE SERVERの構成	合計	ユーザーあたり
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	

XENMOBILE SERVERの構成	合計	ユーザーあたり
デリバリーグループあたりのActive Directoryグループ	10	
SQL		
データベース数	1	

デバイス接続とアプリのアクティビティ

このスケーラビリティテストでは、展開に登録されたデバイスが8時間以内に再接続できる能力に関するデータを収集しました。

このテストでは、再接続間隔をシミュレートしました。この間隔中に、再接続するデバイスはすべての権限のあるセキュリティポリシーを取得し、XenMobile Serverノードは通常よりも高い負荷条件にさらされます。その後の再接続では、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、XenMobile Serverノードの負荷が軽減されます。

これらのテストでは、iOSデバイスとAndroidデバイスをそれぞれ50パーセントずつ組み合わせて使用しました。

これらのテストは、再接続するAndroidデバイスが以前にGCM通知を受信していることを前提としています。

8時間のテスト期間中に、以下のアプリ関連のアクティビティが発生しました。

- Secure Hubが1回開かれ、権限のあるアプリが列挙されました
- 2つのSAML Webアプリが開かれました
- 4つのMAMアプリがダウンロードされました
- Secure Mailで使用するために1つのSTAが生成されました
- マイクロVPNを介したSecure Mailの再接続イベントごとに1つ、合計240回のSTAチケット検証が実行されました。

リファレンスアーキテクチャ

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

注意点と制限事項

この記事のスケーラビリティテスト結果を検討する際は、以下の点に注意してください。

- Windowsプラットフォームはテストされていません。
- ポリシープッシュは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、同時に最大12,000台のデバイスをサポートします。

ライセンス

XenMobile Server は、License Activation Service (LAS) ライセンスメカニズムをサポートするようになりました。LAS は、Citrix 製品スイート全体で従来のファイルベースのライセンスに代わる最新のクラウドベースのライセンスソリューションです。License Activation Service が保持するライセンスとエンタイトルメントを使用するには、Citrix License Server を Citrix Cloud に登録してください。詳細については、「License Activation Service」を参照してください。

> **重要:**
>
> - April 15, 2026までに新しいライセンスモデルを導入してください。詳細については、「Citrix Modern Licensing Announcement」を参照してください。
> - Citrix® ライセンスの返却および変更プロセスは、November 4, 2020から変更されました。詳細については、以下の記事を参照してください。
>   - 「My Account を使用してライセンスを返却する方法」
>   - 「ライセンスファイルを再割り当てする方法」

> XenMobile® は、Citrix Licensing を使用してライセンスを管理します。XenMobile Server と Citrix Gateway にはライセンスが必要です。

Citrix Gateway のライセンスの詳細については、Citrix Gateway のドキュメントを参照してください。Citrix Licensing の詳細については、「Citrix Licensing System」を参照してください。

XenMobile Server を購入すると、ライセンスをアクティベートするための手順が記載された注文確認メールが届きます。新規のお客様は、注文する前にライセンスプログラムに登録する必要があります。XenMobile のライセンスモデルとプログラムの詳細については、「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更新する前に、Citrix License Server を 11.16.x 以降に更新してください。古いライセンスサーバーバージョンは、XenMobile の最新バージョンをサポートしていません。
- XenMobile ライセンスをダウンロードする前に、Citrix Licensing 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 Licensing をインストールしたサーバーの名前が必要です。XenMobile をインストールすると、Citrix Licensing はデフォルトでサーバーにインストールされます。または、既存の Citrix Licensing 展開を使用して XenMobile ライセンスを管理することもできます。Citrix Licensing のインストール、展開、および管理の詳細については、「製品のライセンス」を参照してください。
- XenMobile のノードまたはインスタンスをクラスター化する予定がある場合は、リモートサーバーで Citrix Licensing を使用する必要があります。
- Citrix は、受け取ったすべてのライセンスファイルのローカルコピーを保持することを推奨します。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がバックアップに含まれます。ただし、構成ファイルを最初にバックアップせずに XenMobile を再インストールした場合、元のライセンスファイルが必要になります。

XenMobileのライセンスに関する考慮事項

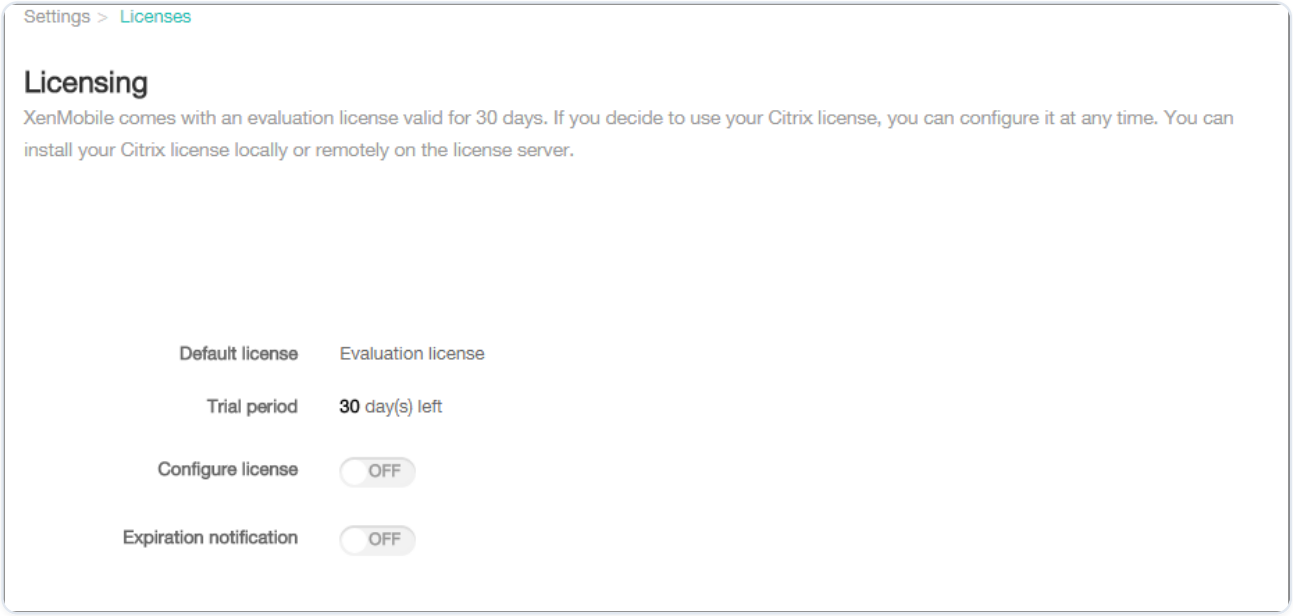
ライセンスがない場合、XenMobileは30日間の猶予期間中、すべての機能を備えたトライアルモードで動作します。このトライアルモードは1回のみ使用でき、30日間の期間はXenMobileをインストールした時点から開始されます。有効なXenMobileライセンスがあるかどうかにかかわらず、XenMobile Webコンソールへのアクセスがブロックされることはありません。XenMobileコンソールで、トライアル期間の残り日数を確認できます。

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

XenMobileライセンスの有効期限が切れると、デバイス管理機能は一切実行できなくなります。たとえば、新しいユーザーやデバイスを登録できなくなり、登録済みのデバイスに展開されたアプリや構成を更新できなくなります。XenMobileのライセンスモデルとプログラムの詳細については、「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見つけるには

XenMobileのインストール後に初めて**ライセンス**ページが表示されると、ライセンスはデフォルトの30日間トライアルモードに設定されており、まだ構成されていません。このページでライセンスを追加および構成できます。



1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **ライセンス**をクリックします。**ライセンス**ページが表示されます。

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、それらはテーブルに表示されます。最初に追加されたライセンスは自動的にアクティブ化されます。Enterpriseやタイプなど、同じカテゴリの複数のライセンスを追加した場合、これらのライセンスはテーブルの1つの行に表示されます。これらの場合、**ライセンスの合計数**と**使用数**は、共通ライセンスの合計数を反映します。**有効期限**の日付は、共通ライセンスの中で最も新しい有効期限を示します。

すべてのローカルライセンスはXenMobileコンソールを通じて管理します。

1. Simple License Service、License Administration Console、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取得します。詳細については、Citrix Licensingのドキュメントを参照してください。
2. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
3. **ライセンス**をクリックします。**ライセンス**ページが表示されます。
4. 「**Configure license**」を「**On**」に設定します。「**License type**」リスト、「**Add**」ボタン、および「**Licensing**」テーブルが表示されます。「**Licensing**」テーブルには、XenMobileで使用したライセンスが表示されます。Citrixライセンスをまだ追加していない場合、テーブルは空です。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/configure-license.png)

5. 「**License type**」が「**Local license**」に設定されていることを確認し、「**Add**」をクリックします。「**Add New License**」ダイアログボックスが表示されます。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/add-license.png)

6. 「**Add New License**」ダイアログボックスで、「**Choose File**」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. 「**Upload**」をクリックします。ライセンスはローカルにアップロードされ、テーブルに表示されます。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/uploaded-local-license.png)

8. 「**Licensing**」ページのテーブルにライセンスが表示されたら、それをアクティブ化します。ライセンスがテーブルの最初の行にある場合、その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している場合は、Citrixライセンスサーバーを使用してすべてのライセンスアクティビティを管理します。詳細については、「Licensing Your Product」を参照してください。

1. ライセンスサーバー証明書をXenMobile Serverにインポートします（**Settings > Certificates**）。
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検証が有効になっています。ホスト名の検証によって展開が中断される場合は、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。

   ホスト名の検証が失敗すると、サーバーログに次のようなエラーが含まれます。「ボリューム購入サーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません」

3. 「**Licensing**」ページで、「**Configure license**」を「**On**」に設定します。「**License type**」リスト、「**Add**」ボタン、および「**Licensing**」テーブルが表示されます。「**Licensing**」テーブルには、XenMobileで使用したライセンスが表示されます。Citrixライセンスをまだ追加していない場合、テーブルは空です。
4. 「**License type**」を「**Remote license**」に設定します。「**License server**」フィールドと「**Port**」フィールド、および「**Test Connection**」ボタンが「**Add**」ボタンに置き換わります。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/add-remote-license.png)

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:** デフォルトのポートを受け入れるか、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. **接続テスト**をクリックします。接続が成功すると、XenMobileはライセンスサーバーに接続し、ライセンステーブルに利用可能なライセンスが入力されます。ライセンスが1つしかない場合は、自動的にアクティブ化されます。

   接続テストをクリックすると、XenMobileは次のことを確認します。

   - XenMobileがライセンスサーバーと通信できること。
   - ライセンスサーバー上のライセンスが有効であること。
   - ライセンスサーバーがXenMobileと互換性があること。

   接続が失敗した場合は、表示されたエラーメッセージを確認し、必要な修正を行ってから、**接続テスト**をクリックします。

   XenMobile接続チェック画面の画像(/en-us/xenmobile/server/media/connectivity-check-license-server.png)

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は、アクティブ化するライセンスを選択できます。

1. **ライセンス**ページの**ライセンステーブル**で、アクティブ化するライセンスを選択します。リスト内の任意の行をクリックすると、**アクティブ化**ダイアログボックスが表示されます。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/activate-mixed-licenses.png)

2. 「**Activate**」をクリックします。
3. ライセンスの「**Active**」行にチェックマークが表示されたら、「**Save**」をクリックします。

> 「**重要:**」:
>
> - **ユーザー**ごとのライセンスと**デバイス**ごとのライセンスは相互に排他的であり、同時にアクティブ化することはできません。

- ADV EditionとENT Editionのライセンスのみを混在させることができます。MDM Editionのライセンスは、ADV EditionまたはENT Editionのライセンスと混在させることはできません。
- 同じエディションのライセンスファイルが同じステータスであることを確認してください。たとえば、1つのADVエディションファイルがアクティブ化されると、残りのADVファイルは自動的にアクティブ化されます。
- XenMobile Server 10.15 Rolling Patch 3より前のバージョンでは、一度に1つのライセンスのみをアクティブにできます。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化されます。

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、XenMobileを設定して、ライセンスの有効期限が近づいたときに、あなたまたは指定された担当者に通知することができます。

1. 「**Licensing**」ページで、「**Expiration notification**」を「**On**」に設定します。新しい通知関連フィールドが表示されます。

   ライセンス構成画面の画像(/en-us/xenmobile/server/media/notification-setup.png)

2. これらの設定を構成します。

   - 「**Notify every:**」タイプ:
   - 通知が送信される頻度。たとえば、**7**日ごと。
   - 通知の送信を開始するタイミング。たとえば、ライセンスの有効期限が切れる60日前。
   - **受信者:** 自分のメールアドレス、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:** 受信者が通知で確認する有効期限通知メッセージを入力します。

3. **保存**をクリックします。設定に基づいて、XenMobileは**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を、**受信者**に入力した受信者に送信し始めます。通知は設定した頻度で送信されます。

ライセンスアクティベーションサービス

重要:

Citrixプラットフォームでは、業界標準のクラウドベースのライセンスアーキテクチャへの移行を進めています。この移行により、エンタイトルメントとアクティベーションが自動化され、お客様に以下の主要なメリットがもたらされます。

- **ライセンスファイル管理が不要:** ライセンスファイルのダウンロード、割り当て、管理の必要がなくなり、管理タスクが簡素化されます。
- **エンタイトルメントの自動更新:** 契約更新時にエンタイトルメントがバックグラウンドで自動的に更新され、中断のないサービスが保証されます。
- **回復力の向上:** ライセンスサーバーがユーザーセッションの単一障害点ではなくなり、環境の安定性が向上します。

切り替えまでの期間を利用して、April 15, 2026までに新しいライセンスモデルへの移行を計画し、実行することをお勧めします。Citrixは、その過程のあらゆる段階でお客様をサポートすることをお約束します。詳細については、「Citrix Modern Licensing Announcement」を参照してください。

ライセンスアクティベーションサービス (LAS) は、従来のCitrixレガシーライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASはアクティベーション用の新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

LASはCitrixライセンスエクスペリエンスを簡素化します。ライセンスサーバーで生成、ダウンロード、またはインストールするライセンスアクセスコードやファイルは不要になりました。ライセンスサーバーをアップグレードし、Citrix Cloudに登録するだけで済みます。互換性のある製品がライセンスサーバーを指すように設定されると、自動的にアクティベートされます。

アクティベーション後、ライセンスサーバーはライセンスアクティベーションサービスと定期的に通信し、アクティベーションを最新の状態に保ちます。LASはクラウドテクノロジーで構築されており、パフォーマンスを向上させ、ダウンタイムがないことを保証します。何らかの理由でライセンスサーバーまたはLASに到達できない場合、システムはライセンスキャッシュモードに入ります。これは、システムのライセンスが失われるのを防ぎ、停止を回避するように設計されています。詳細については、「ライセンスキャッシュモード」を参照してください。

クラウドに接続できないライセンスサーバーの場合、LASはオフラインアクティベーションオプションも提供し、さまざまなネットワーク環境に柔軟性をもたらします。このサービスは、Citrix製品ライセンスを管理するためのシームレスで最新のアプローチを導入します。

LASの詳細については、ライセンスドキュメント「License Activation Service」を参照してください。

LASの互換性

LASと互換性のあるXenMobile Serverの最小要件バージョンは次のとおりです。

- 10.16 ローリングパッチ 7
- 10.15 ローリングパッチ 13

> **注:**
>
> April 15, 2026 に、レガシーファイルベースライセンスは機能しなくなります。レガシーファイルベースライセンスメカニズムを使用する展開は、エンドユーザーに影響を与えます。

前提条件

- ライセンスサーバーをバージョン11.17.2ビルド51000以降にインストールまたは更新します。
- XenMobile Serverのエンタイトルメントに関連付けられているOrgIDを持つCitrix Cloudアカウント。
- オンラインアクティベーション用にライセンスサーバーを構成する。

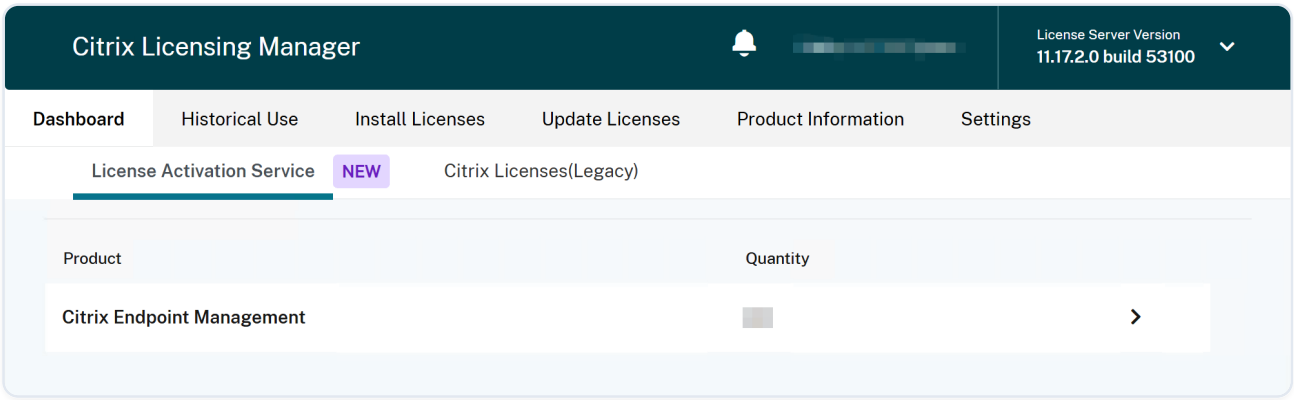
ライセンスアクティベーションサービスを構成する

ステップ1：ライセンスサーバーをインストールまたはアップグレードする

ライセンスサーバーをバージョン11.17.2ビルド51000以降にインストールまたはアップグレードします。Windows用Citrixライセンスサーバーは、Citrix Licensingダウンロードページからダウンロードできます。

ステップ2：LASを構成する

ライセンスアクティベーションサービス用にライセンスサーバーを構成する方法に記載されている手順に従ってLASを構成し、ライセンスサーバーのオンボーディングに使用されたCitrix Cloudの顧客アカウントにXenMobile Serverのエンタイトルメントが含まれていることを確認してください。



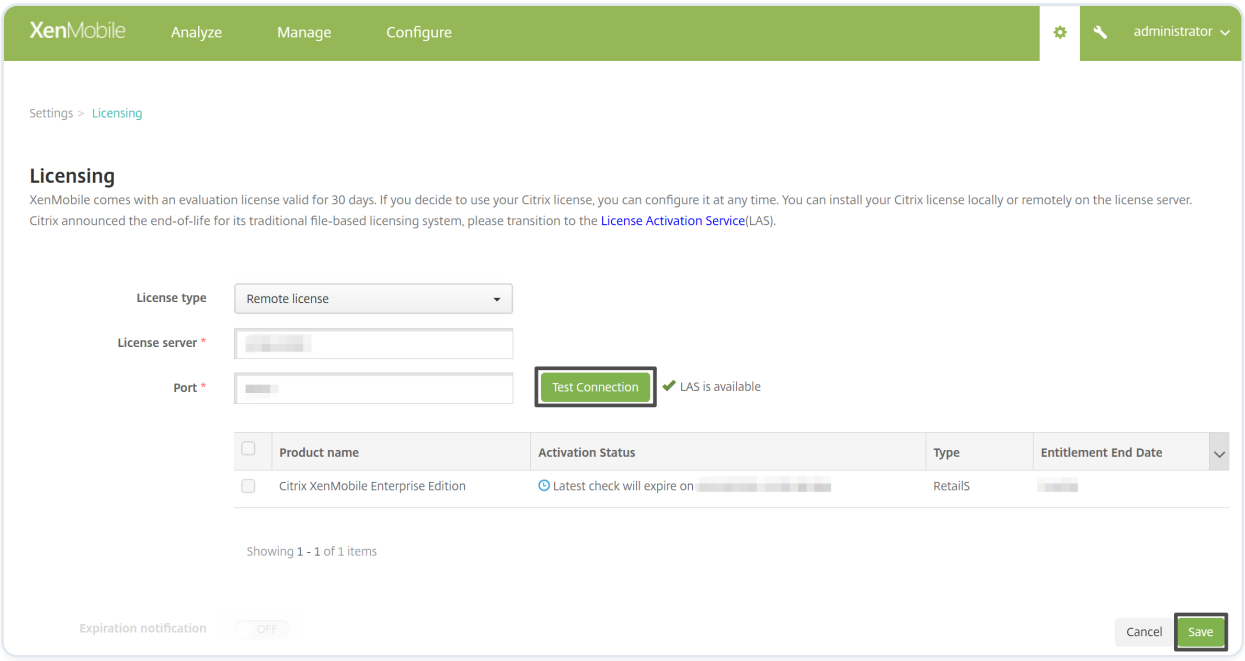
ステップ3：XenMobile Serverをアップグレードする

XenMobile ServerをLAS互換バージョンにアップグレードします。必要な最小XenMobile Serverバージョンは次のとおりです。

- 10.16 ローリングパッチ 7
- 10.15 ローリングパッチ 13

手順4：LASを使用するようにXenMobile Serverを構成する

1. XenMobile Serverコンソールにサインインし、**［Settings］>［Licensing］**の順に移動します。
2. **［License Type］を［Remote License］**に設定します。
3. **［License server］と［Port］**を構成します。
   - **［License server］：**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。
   - **［Port］：**デフォルトポート（LASの場合は8083）を受け入れるか、LASライセンスサーバーとの通信に使用するカスタマイズされたポート番号を入力します。
4. **［Test Connection］**をクリックします。接続が成功すると、LASが利用可能であり、ライセンステーブルに利用可能なライセンスが入力されていることが示されます。アクティベーションステータスにエラーがなく正常であることを確認してください。



5. **［Save］**をクリックします。構成が保存され、XenMobile ServerはLicense Activation Serviceを使用するように切り替わります。

トラブルシューティング

ライセンスサーバーのステータスが緑色でない場合は、次の手順に従ってアクティベーションの詳細を表示し、問題をトラブルシューティングしてください。

Citrix CloudでXenMobile Serverのアクティベーションの詳細を確認するには、次の手順を実行します。

1. **Licensing** > **Licensed Deployments** > **License Servers** の順に移動します。
2. XenMobile Server が使用するライセンスサーバーを見つけ、**詳細の表示**をクリックします。
3. ライセンスサーバーの詳細ページで、**Citrix Endpoint Management**を展開してアクティベーションのリストを表示します。

   各アクティベーションに表示される**ID**は、XenMobile Server のホスト名です。

   CEM の接続成功の画像(/en-us/xenmobile/server/media/cem-successful-connection.png)
4. 必要なアクティベーションについて、**詳細の表示**をクリックします。

   詳細ページには次の情報が表示されます。

   - **XMS ホスト名:** XenMobile Server のホスト名。
   - **XMS IP:** XenMobile Server の IP アドレス。
   - **ホスト名:** XenMobile Server のホスト名。

LAS の詳細表示の画像(/en-us/xenmobile/server/media/xms-view-details.png)

FIPS 140-2 準拠

連邦情報処理標準 (FIPS) は、米国国立標準技術研究所 (NIST) によって発行されています。FIPSは、セキュリティシステムで使用される暗号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、この標準の第2版です。NIST検証済みのFIPS 140モジュールに関する詳細については、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にできます。
- 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、HDX™アプリが使用されていない場合、すべてFIPSに準拠しています。

iOS上のすべての保存データおよび転送データの暗号化操作は、Citrix®およびAppleが提供するFIPS検証済みの暗号モジュールを使用します。Androidでは、すべての保存データの暗号化操作は、デバイスメーカーが提供するプラットフォームの暗号モジュールによって提供されるFIPS検証済みの暗号モジュールを使用します。デバイスメーカーのモジュールに関する詳細については、Citrix担当者にお問い合わせください。

サポートされているWindowsデバイス上のモバイルデバイス管理 (MDM) のすべての保存データおよび転送データの暗号化操作は、FIPS検証済みの暗号モジュールを使用します。

XenMobile MDMのすべての保存データおよび転送データの暗号化操作は、FIPS検証済みの暗号モジュールを使用します。MDMフローのすべての保存データおよび転送データは、エンドツーエンドでFIPS準拠の暗号モジュールを使用します。このセキュリティには、モバイルデバイスについて前述した暗号化操作に加え、モバイルデバイスとCitrix Gateway間の暗号化操作が含まれます。

MDX Vaultは、iOSおよびAndroidデバイス上のMDXでラップされたアプリと関連する保存データを、FIPS検証済みの暗号モジュールを使用して暗号化します。

言語サポート

モバイル生産性アプリとXenMobileコンソールは、英語以外の言語での使用に対応しています。このサポートには、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

の文字やキーボード入力が含まれます。すべてのCitrix製品のグローバリゼーションサポートの詳細については、`<https://support.citrix.com/article/CTX119253>`を参照してください。

この記事では、XenMobileの最新リリースでサポートされている言語を一覧表示します。

XenMobileコンソールとセルフヘルプポータル

- 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

モバイル生産性アプリ

Xは、そのアプリが特定の言語で利用可能であることを示します。

iOSおよびAndroid

言語	セキュアハブ	セキュアメール	セキュアウェブ	QUICKEDIT
日本語	X	X	X	X
簡体字中国語	X	X	X	X
繁体字中国語	X	X	X	X
フランス語	X	X	X	X
ドイツ語	X	X	X	X
スペイン語	X	X	X	X
韓国語	X	X	X	X
ポルトガル語	X	X	X	X
オランダ語	X	X	X	X
イタリア語	X	X	X	X

XENMOBILE®サーバー

言語	セキュアハブ	セキュアメール	セキュアウェブ	QUICKEDIT
デンマーク語	X	X	X	X
スウェーデン語	X	X	X	X
ヘブライ語	X	X	X	iOSのみ
アラビア語	X	X	X	X
ロシア語	X	X	X	X
トルコ語	X	X	Androidのみ	-
ポーランド語	X	X	X	-

Windows

言語	セキュアハブ	セキュアメール	セキュアウェブ
フランス語	X	X	X
ドイツ語	X	X	X
スペイン語	X	X	X
イタリア語	X	X	X
デンマーク語	X	X	X
スウェーデン語	X	X	X

右から左への言語のサポート

次の表は、各アプリにおける中東言語のテキストのサポートをまとめたものです。Xは、そのプラットフォームで機能が利用可能であることを示します。右から左への言語のサポートは、Windowsデバイスでは利用できません。

アプリ	IOS	アンドロイド
セキュアハブ	X	X
セキュアメール	X	X

アプリ	IOS	アンドロイド
セキュアウェブ	X	X
QuickEdit	X	X

インストールと構成

開始する前に

以下のインストール前チェックリストを使用して、オンプレミス版XenMobile®のインストールに必要な前提条件と設定をメモできます。各タスクまたはメモには、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含まれています。

XenMobileの展開を計画するには、多くの考慮事項があります。完全なXenMobile環境に関する推奨事項、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、この記事の後半にある「XenMobileのインストール」セクション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

XenMobileソリューションに必要なネットワーク設定は次のとおりです。

前提条件または設定	コンポーネントまたは機能	設定をメモする	
リモートユーザーが接続する完全修飾ドメイン名 (FQDN) をメモします。	ゼノモバイルとシトリックスゲートウェイ		
パブリックIPアドレスとローカルIPアドレスをメモします。			
これらのIPアドレスは、ネットワークアドレス	ゼノモバイル とシトリックスゲートウェイ		

前提条件または設定	コンポーネントまたは機能	設定をメモする		
変換 (NAT) を設定するためにファイアウォールを構成する際に必要です。				
サブネットマスクをメモします。	ゼノモバイル とシトリックスゲートウェイ			
DNS IPアドレスをメモします。	ゼノモバイル とシトリックスゲートウェイ			
WINSサーバーのIPアドレスを書き留めます(該当する場合)。	シトリックスゲートウェイ			
Citrix Gatewayのホスト名を特定して書き留めます。	シトリックスゲートウェイ	これは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済みサーバー証明書に含まれています。Citrix Gatewayのセットアップウィザードを使用してホスト名を構成できます。	シトリックスゲートウェイ	
XenMobileのIPアドレスをメモします。XenMobileのインスタンスを1	XenMobile			

前提条件または設定	コンポーネントまたは機能	設定をメモする	
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。クラスターを構成する場合は、必要なすべてのIPアドレスをメモします。			
Citrix Gatewayで構成された1つのパブリックIPアドレス	シトリックスゲートウェイ		
Citrix Gateway用の外部 DNS エントリを 1 つ	シトリックスゲートウェイ		
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、管理者ユーザー名、およびパスワードをメモします。これらの設定は、ネットワークにプロキシサーバーを展開する場合（該当する場合）はオプションです。	シトリックスゲートウェイ	Web プロキシのユーザー名を構成する際には、sAMAccountName またはユーザープリンシパル名 (UPN) のいずれかを使用できます。	ゼノモバイルとシトリックスゲートウェイ
デフォルトゲートウェイの IP アドレスをメモします。	ゼノモバイルとシトリックスゲートウェイ		

前提条件または設定	コンポーネントまたは機能	設定をメモする	
システム IP (NSIP) アドレスとサブネットマスクをメモします。	シトリックスゲートウェイ		
サブネット IP (SNIP) アドレスとサブネットマスクをメモします。	シトリックスゲートウェイ		
Citrix Gateway 仮想サーバーの IP アドレスと、証明書からの FQDN をメモします。複数の仮想サーバーを構成するには、すべての仮想 IP アドレスと証明書からの FQDN をメモします。	シトリックスゲートウェイ		
ユーザーが Citrix Gateway を介してアクセスできる内部ネットワークをメモします。例: 10.10.0.0/24。ユーザーが Secure Hub または Citrix Gateway Plug-in を使用して接続し、スプリットトンネリング	シトリックスゲートウェイ		

前提条件または設定	コンポーネントまたは機能	設定をメモする	
がオンに設定されている場合など、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。			
XenMobile Server、Citrix 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到達可能であることを確認してください。	ゼノモバイル とシトリックス ゲートウェイ		

ライセンス

XenMobileでは、Citrix Gatewayと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 Licensingの詳細については、「The Citrix Licensing System」を参照してください。

前提条件	コンポーネント	場所をメモする
Citrix Webサイトからユニバーサルライセンスを取得します。詳細については、Citrix Gatewayドキュメントの「Licensing」を参照してください。	シトリックス ゲートウェイ、ゼノモバイル、およびシトリックス ライセンス サーバー	

証明書

XenMobileとCitrix Gatewayは、他のCitrix製品やアプリ、およびユーザーデバイスからの接続を有効にするために証明書を必要とします。詳細については、XenMobileドキュメントの「Certificates and Authentication」セクションを参照してください。

前提条件	コンポーネント	注
必要な証明書を取得してインストールします。	ゼノモバイル と シトリックス ゲートウェイ	

ポート

XenMobileコンポーネントとの通信を許可するためにポートを開放します。

前提条件	コンポーネント	注
XenMobile用のポートを開放する	XenMobile と シトリックス ゲートウェイ	

データベース

XenMobileにはデータベース接続の構成が必要です。XenMobileリポジトリには、システム要件と互換性に記載されているサポート対象バージョンのいずれかで動作するMicrosoft SQL Serverデータベースが必要です。Citrixは、Microsoft SQLをリモートで使用することを推奨しています。PostgreSQLはXenMobileに含まれています。PostgreSQLは、テスト環境でのみローカルまたはリモートで使用してください。

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では Microsoft JDBCドライバーを使用するには、SQL Serverドライバーを参照してください。

前提条件	コンポーネント	注
Microsoft SQL Server の IP アドレスとポート。 XenMobile で使用する SQL Server のサービスアカウントに DBcreator ロールの権限があることを確認してください。	XenMobile	

Active Directory の設定

前提条件	コンポーネント	注記
プライマリサーバーとセカンダリサーバーの Active Directory IP アドレスとポートをメモします。ポート 636 を使用する場合は、XenMobile に CA からのルート証明書をインストールし、「Use secure connections」オプションを「Yes」に変更します。	XenMobile および Citrix Gateway	
Active Directory ドメイン名をメモします。	XenMobile および Citrix Gateway	
Active Directory サービスアカウントをメモします。これには、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 を照会するために使用するアカウントです。	XenMobile および Citrix Gateway	
ユーザーが配置されているディレクトリレベルであるユーザーベース DN をメモします。例: `cn=users,dc=ace,dc=com` 。Citrix Gateway と XenMobile は、Active Directory を照会するためにユーザーベース DN を使用します。	XenMobile および Citrix Gateway	
グループが配置されているディレクトリレベルであるグループベースDNをメモしま	XenMobile と シトリックスゲートウェイ	

前提条件	コンポーネント	注記
す。Citrix GatewayとXenMobileはこのDNを使用してActive Directoryを照会します。		

XenMobileとCitrix Gateway間の接続

前提条件	コンポーネント	設定をメモします
XenMobileホスト名をメモします。	XenMobile	
XenMobileのFQDNまたはIPアドレスをメモします。	XenMobile	
ユーザーがアクセスできるアプリを特定します。	シトリックス ゲートウェイ	
コールバックURLをメモします。	XenMobile	

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

Citrixは、XenMobileとCitrix Gateway間、およびXenMobileとSecure Hub間の接続設定を構成するために、Citrix ADCのクイック構成ウィザードを使用することを推奨します。Citrix Receiver™およびWebブラウザからのユーザー接続を有効にするために、2つ目の仮想サーバーを作成します。これらの接続は、Virtual Apps and Desktops内の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ものです。Citrixは、これらの設定を構成するためにもCitrix ADCのクイック構成ウィザードを使用することを推奨します。

前提条件	コンポーネント	設定をメモする
Citrix Gatewayのホスト名と外部URLをメモします。外部URLは、ユーザーが接続するWebアドレスです。	XenMobile	
Citrix GatewayのコールバックURLをメモします。	XenMobile	

前提条件	コンポーネント	設定をメモする
仮想サーバーのIPアドレスとサブネットマスクをメモします。	シトリックス ゲートウェイ	
Program Neighborhood AgentまたはVirtual Apps and Desktopsサイトのパスをメモします。	シトリックス ゲートウェイとゼノンモバイル	
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アドレスをメモします（ICA接続のみ）。	シトリックス ゲートウェイ	
XenMobileのパブリックFQDNをメモします。	シトリックス ゲートウェイ	
Secure Hub のパブリックFQDN をメモしてください。	シトリックス ゲートウェイ	

XenMobile展開のフローチャート

このフローチャートは、XenMobileを展開するための主要な手順を案内するのに役立ちます。各手順に関するトピックへのリンクは、図の後に続きます。

1: システム要件と互換性

2: インストールと構成

3および4: インストール前チェックリスト (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 (VM) は、Citrix XenServer、VMware ESXi、またはMicrosoft Hyper-V上で動作します。XenMobileをインストールするには、XenCenter®またはvSphere管理コンソールを使用できます。

> **注:**
>
> ハイパーバイザーが正しい時刻に設定されていることを確認してください。XenMobileはその時刻を使用するため、NTPサーバーを使用するか、手動で設定してください。XenMobileの時刻をハイパーバイザーと同期する際にタイムゾーンの問題が発生した場合は、XenMobileをNTPサーバーに指定することで問題を回避できます。そのためには、コマンドラインインターフェイスオプションで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。XenServerまたはVMware ESXiにXenMobileをインストールする前に、次の操作を行う必要があります。詳細については、XenServerまたはVMwareのドキュメントを参照してください。

- 適切なハードウェアリソースを備えたコンピューターに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をホストするコンピューターは、ネットワーク経由でXenServerまたはVMware ESXiホストに接続します。

Hyper-Vの前提条件。Hyper-VにXenMobileをインストールする前に、次の操作を行う必要があります。詳細については、Hyper-Vのドキュメントを参照してください。

- 適切なシステムリソースを備えたコンピューターに、Hyper-Vが有効化され、役割が有効化されたWindows Server 2016またはWindows Server 2019をインストールします。Hyper-Vの役割をインストールする際は、Hyper-Vが仮想ネットワークを作成するために使用するサーバー上のNICを必ず指定してください。一部のNICはホスト用に予約できます。
- ファイルVirtual Machines/<*build-specific UUID*>.xmlを削除します。
- ファイルLegacy/<*build-specific UUID*>.expをVirtual Machinesに移動します。

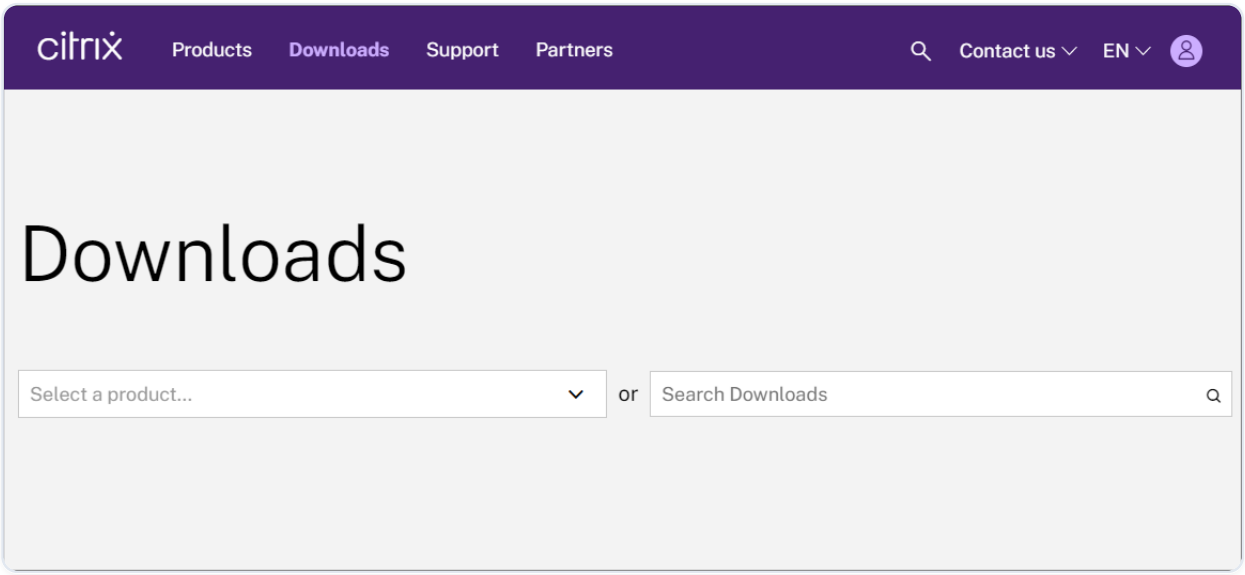
FIPS 140-2モード。FIPSモードでXenMobile Serverをインストールするには、XenMobileでFIPSを構成するで説明されているように、前提条件グループを完了します。

XenMobile製品ソフトウェアをダウンロードする

製品ソフトウェアはCitrix 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、ダウンロードリンクを使用して、ダウンロードしたい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. Citrix Webサイトにアクセスします。
2. 検索ボックスの横にある**Log On**をクリックし、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. ダウンロードページで、「**製品を選択**」リストから「**Citrix Endpoint Management™ (および Citrix XenMobile Server)**」をクリックします。Citrix Endpoint Management (および Citrix XenMobile Server) ページが自動的に表示されます。



5. 「**XenMobile Server (オンプレミス)**」を展開します。
6. 「**製品ソフトウェア**」を展開します。
7. 「**XenMobile Server 10**」をクリックします。
8. 「**ダウンロードにジャンプ**」メニューをクリックし、XenMobile のインストールに使用する適切な仮想イメージを選択します。または、ページを下にスクロールして、インストールするイメージの「**ファイルのダウンロード**」ボタンを見つけます。
9. 画面の指示に従ってソフトウェアをダウンロードします。

Citrix Gateway のソフトウェアをダウンロードするには

この手順を使用して、Citrix Gateway 仮想アプライアンスをダウンロードしたり、既存の Citrix 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したりできます。

1. Citrix Webサイト にアクセスします。

2. Citrix Webサイトにまだログオンしていない場合は、検索ボックスの横にある「**ログオン**」をクリックし、アカウントにログオンします。
3. 「**ダウンロード**」タブをクリックします。
4. ダウンロードページで、製品選択リストから「**Citrix Gateway**」をクリックします。
5. 「**Go**」をクリックします。Citrix Gateway ページが表示されます。
6. Citrix Gateway ページで、実行している Citrix Gateway のバージョンを展開します。
7. 「**ファームウェア**」の下で、ダウンロードしたい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：**」：
>
> 「**Virtual Appliances**」をクリックしてCitrix ADC VPXをダウンロードすることもできます。このオプションを選択すると、各ハイパーバイザーの仮想マシン用ソフトウェアのリストが表示されます。

8. ダウンロードしたい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. ダウンロードしたい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「**Download**」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ます。

XenMobileの初回使用設定

1. XenMobileのIPアドレス、サブネットマスク、デフォルトゲートウェイ、DNSサーバー、その他の設定を行うには、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 template**」ページでOVFテンプレートを展開する際に、ネットワークプロパティを設定しないことをお勧めします。高可用性構成でこれを行うことにより、2番目のXenMobile仮想マシンをクローンして再起動したときに発生するIPアドレスの問題を回避できます。

2. XenMobile管理コンソールには、XenMobile Serverの完全修飾ドメイン名またはノードのIPアドレスを介してのみアクセスしてください。

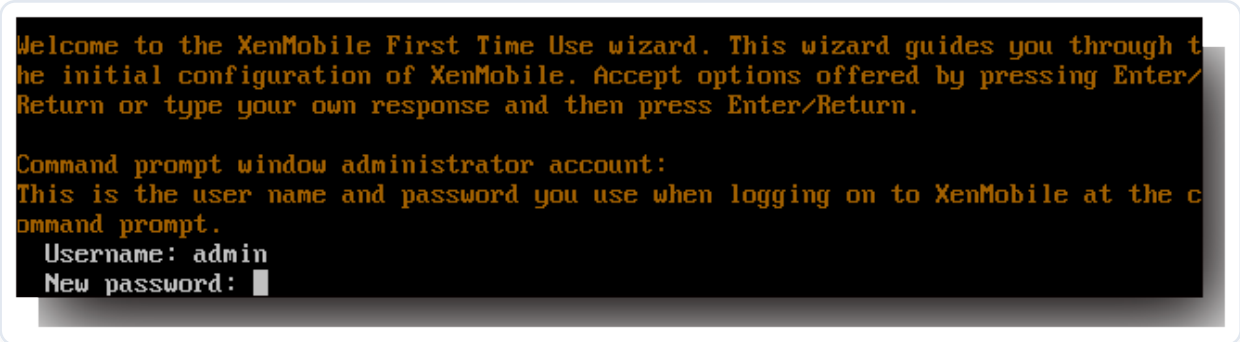
3. ログオンし、初期ログオン画面の指示に従います。

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。詳細については、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、コマンドプロンプトビューを開始します。詳細については、お使いの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管理者ユーザー名とパスワードを入力して、XenMobileの管理者アカウントを作成します。

   コマンドプロンプトの管理者アカウント、公開鍵基盤 (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場合、XenMobileは、XenMobileの外部でパスワードが管理されているActive Directoryユーザーを除くすべてのユーザーに対して、次のルールを適用します。

   - パスワードは8文字以上である必要があります。
   - パスワードは、次の複雑さの基準のうち少なくとも3つ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しても、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、**y**と入力して設定をコミットします。

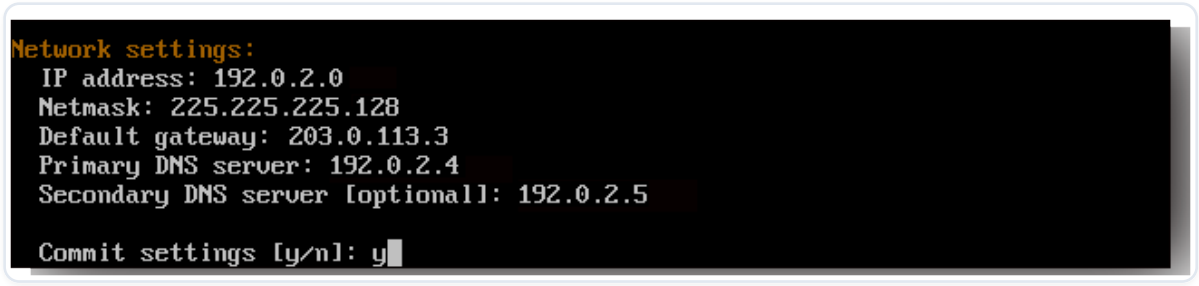
   a. XenMobile ServerのIPアドレス

   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)

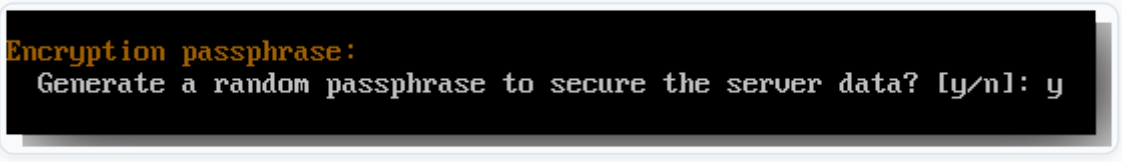
e. セカンダリDNSサーバー (オプション)



> **注:**
>
> この画像および以下の画像に示されているアドレスは機能せず、例としてのみ提供されています。

5. セキュリティを強化するためにランダムな暗号化パスフレーズを生成するには「**y**」と入力するか、独自のパスフレーズを指定するには「**n**」と入力します。Citrixでは、ランダムなパスフレーズを生成するために「**y**」と入力することをお勧めします。

   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の一部として使用されます。サーバーファイルシステムに保存されているパスフレーズのハッシュは、データの暗号化および復号化中にキーを取得するために使用されます。パスフレーズは表示できません。

   > **注:**
   >
   > 環境を拡張してサーバーを追加設定する場合は、独自のパスフレーズを指定してください。ランダムなパスフレーズを選択した場合、それを表示することはできません。
   >
   > 
   >

6. 必要に応じて、連邦情報処理標準 (FIPS) を有効にします。FIPSの詳細については、「FIPS」を参照してください。また、「XenMobileでFIPSを構成する」で説明されているように、前提条件グループを完了していることを確認してください。

```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

7. データベース接続を構成するために、以下の情報を提供します。

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server:        .10
  Port: 5432
  Username: postgres
  Password:
```

- データベースはローカルまたはリモートにできます。ローカルの場合は「**l**」、リモートの場合は「**r**」と入力します。
- データベースの種類を選択します。Microsoft SQLの場合は「**mi**」、PostgreSQLの場合は「**p**」と入力します。

> **重要:**
>
> - CitrixはMicrosoft SQLをリモートで使用することを推奨します。PostgreSQLはXenMobileに同梱されています。PostgreSQLはローカルまたはリモートで、テスト環境で*のみ*使用してください。
> - データベースの移行はサポートされていません。テスト環境で作成されたデータベースを本番環境に移動することはできません。

- 必要に応じて、データベースにSSL認証を使用するには「**y**」と入力します。
- XenMobileをホストするサーバーの完全修飾ドメイン名 (FQDN) を入力します。この単一ホストサーバーは、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、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。
- データベース設定をコミットするには、「**Enter**」キーを押します。

8. 必要に応じて、XenMobileノード（インスタンス）のクラスタリングを有効にするには「**y**」と入力します。

> **重要:**
>
> XenMobileクラスターを有効にする場合、システム構成が完了した後、クラスターメンバー間のリアルタイム通信を有効にするためにポート80を開きます。その設定をすべてのクラスターノードで完了してください。

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



10. 設定をコミットするには、**Enter**キーを押します。
11. 通信ポートを特定します。ポートとその使用方法の詳細については、「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、デフォルトのポートを受け入れます。



12. XenMobileを初めてインストールするため、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はスキップしてください。
13. 各公開鍵インフラストラクチャ（PKI）証明書に同じパスワードを使用する場合は、**y**と入力します。XenMobile PKI機能の詳細については、「証明書のアップロード」を参照してください。

```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

重要：

XenMobileのノードまたはインスタンスをクラスター化する予定がある場合は、後続のノードに同じパスワードを指定してください。

14. 新しいパスワードを入力し、確認のためにもう一度新しいパスワードを入力します。

    新しいパスワードを入力しても、アスタリスクなどの文字は表示されません。

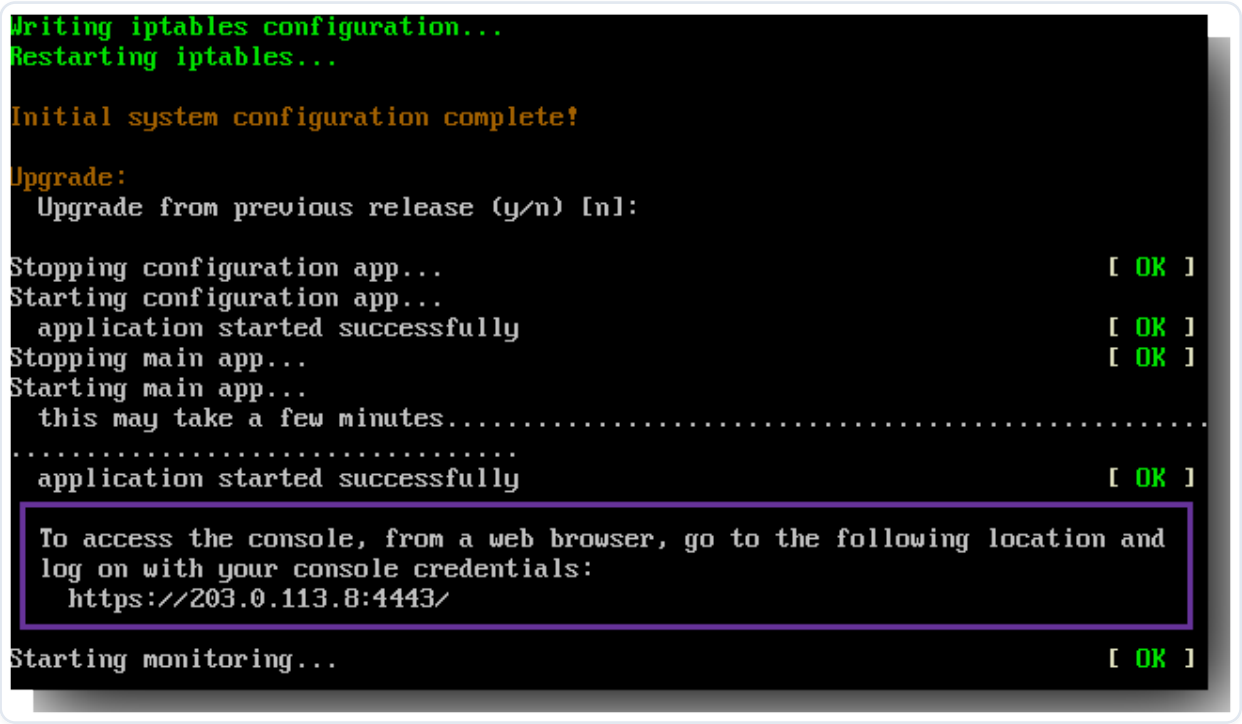
15. 設定をコミットするには、**Enter**キーを押します。
16. WebブラウザでXenMobileコンソールにログオンするための管理者アカウントを作成します。これらの資格情報は、後で使用するために必ず記録しておいてください。

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

注記:

新しいパスワードを入力しても、アスタリスクなどの文字は表示されません。

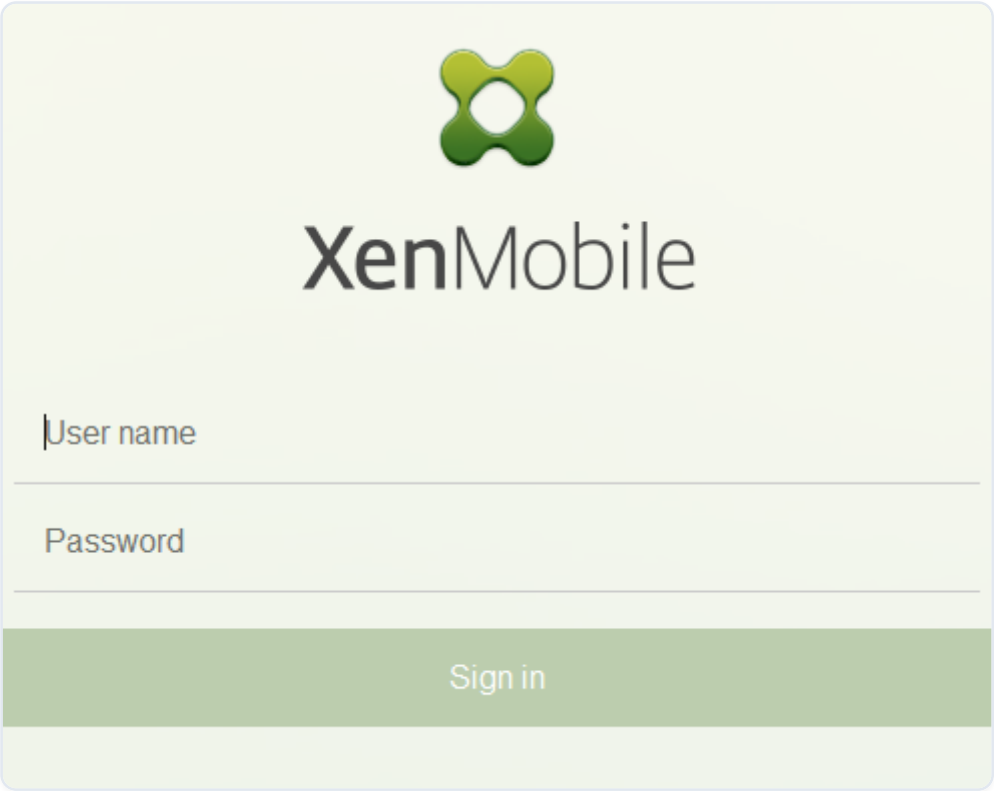
17. **Enter** キーを押して設定をコミットします。初期システム構成が保存されます。
18. アップグレードするかどうかを尋ねられたら、新規インストールであるため「**n**」と入力します。
19. 画面に表示される完全なURLをコピーし、Webブラウザでこの初期XenMobile構成を続行します。



WebブラウザでXenMobileを構成する

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構成の初期部分を完了したら、Webブラウザでプロセスを完了します。

1. Webブラウザで、コマンドプロンプトウィンドウの構成の最後に示された場所に移動します。
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. 「Get Started」ページで、**Start** をクリックします。「**Licensing**」ページが表示されます。
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日間有効な評価ライセンスが使用されます。ライセンスの追加と構成、および有効期限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:**
>
> クラスターノード、つまりXenMobileのインスタンスを追加してXenMobileクラスタリングを使用する予定がある場合は、リモートサーバー上のCitrix Licensing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表示されます。
6. APNsおよびSSLリスナー証明書をインポートします。iOSデバイス管理にはAPNs証明書が必要です。証明書の操作の詳細については、「証明書」を参照してください。

> **注：**
>
> この手順では、サーバーの再起動が必要です。

7. 環境に応じて、Citrix Gatewayを構成します。Citrix Gatewayの構成の詳細については、「Citrix 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：

   - Citrix Gatewayは、内部ネットワーク（またはイントラネット）の境界に展開できます。この展開により、内部ネットワークに存在するサーバー、アプリ、およびその他のネットワークリソースへの安全な単一アクセス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は、内部ネットワーク内のリソースにアクセスする前にCitrix Gatewayに接続する必要があります。
   - Citrix Gatewayはオプション設定ですが、ページにデータを入力した後、ページを離れる前に必須フィールドをクリアまたは完了する必要があります。

8. Active Directoryからユーザーとグループにアクセスするために、LDAP構成を完了します。LDAP接続の構成の詳細については、「LDAP構成」を参照してください。
9. ユーザーにメッセージを送信できるように、通知サーバーを構成します。通知サーバーの構成の詳細については、「通知」を参照してください。

事後要件。証明書をアクティブ化するには、XenMobile Serverを再起動します。

XenMobile® で FIPS を構成する

XenMobile の連邦情報処理標準 (FIPS) モードは、すべての暗号化操作に FIPS 140-2 認定ライブラリのみを使用することで、米国連邦政府の顧客をサポートします。FIPS モードで XenMobile Server をインストールすると、XenMobile クライアントおよびサーバーのすべてのデータが FIPS 140-2 に完全に準拠していることが保証されます。この準拠は、保存データと転送中のデータに適用されます。

FIPS モードで XenMobile Server をインストールする前に、次の前提条件を完了してください。

- XenMobile データベースには外部の SQL Server 2014 を使用します。SQL Server は、セキュアな SSL 通信のために構成されている必要があります。SQL Server へのセキュアな SSL 通信の構成手順については、「データベースエンジンへの暗号化された接続を有効にする (SQL Server 構成マネージャー)」を参照してください。
- セキュアな SSL 通信には、既知の認証局 (CA) からの信頼された SSL 証明書を SQL Server に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入れられません。Citrix® は、SQL Server の FQDN を含む SSL 証明書を要求することを推奨します。

FIPS モードの構成

FIPS モードは、XenMobile Server の初期設定中にのみ有効にできます。インストール完了後に FIPS を有効にすることはできません。したがって、FIPS モードを使用する予定がある場合は、最初から FIPS モードで XenMobile Server をインストールする必要があります。XenMobile クラスターの場合、すべてのクラスターノードで FIPS が有効になっている必要があります。同じクラスター内に FIPS と非 FIPS の XenMobile Server を混在させることはできません。

XenMobile コマンドラインインターフェイスには、**FIPS モードの切り替え**オプションがありますが、これは本番環境での使用を目的としたものではありません。このオプションは、非本番環境での診断目的で使用されるものであり、本番環境の XenMobile Server ではサポートされていません。

1. 初期設定中に、**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 用に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、使用するログオンには DBcreator ロールが必要です。

4. Active Directory アカウントを使用するには、資格情報を domain\\username の形式で入力します。
5. これらの手順が完了したら、XenMobile の初期設定を続行します。

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**」というフレーズが表示されます。

証明書のインポート

次の手順では、証明書をインポートしてXenMobile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インスタンスへの接続は安全である必要があり、SQL Server 2012またはSQL Server 2014である必要があります。接続を保護するには、「Microsoft Management

Consoleを使用してSQL Server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. サービスが正常に再起動しない場合は、以下を確認してください: **Services.msc**を開きます。
   a. SQL Serverサービスに使用されている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**に移動し、証明書項目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**を展開し、インポートされたSSL証明書を見つけます。
   f. インポートされた証明書（SQL Server構成マネージャーで選択されているもの）を右クリックし、**すべてのタスク > プライベートキーの管理**をクリックします。
   g. **グループ名またはユーザー名**の下で、**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はフルコントロールと読み取りの両方の権限を持っていますが、プライベートキーを読み取ることのみが可能である必要があります。
   j. **MMC**を閉じて、SQLサービスを開始します。
3. SQLサービスが正しく開始されていることを確認してください。

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サーバーのデフォルトサイト、C:\\inetpub\\wwwroot にコピーします。
3. デフォルトサイトの**認証**チェックボックスをオンにします。
4. **Anonymous**を**有効**に設定します。
5. **失敗した要求のトレース**ルールチェックボックスを選択します。
6. .cerがブロックされていないことを確認してください。
7. ローカルサーバーからWebブラウザで.cerの場所に移動します `https://localhost/certname.cer`。ルート証明書のテキストがブラウザに表示されます。
8. ルート証明書がWebブラウザに表示されない場合は、IISサーバーでASPが次のように有効になっていることを確認してください。

a. サーバーマネージャーを開きます。
b. **管理 > 役割と機能の追加**でウィザードに移動します。
c. サーバーの役割で、**Webサーバー (IIS)を展開し、Webサーバーを展開し、アプリケーション開発を展開し、次にASP**を選択します。
d. インストールが完了するまで**次へ**をクリックします。

9. `https://localhost/cert.cer`を参照します。

詳細については、Web Server (IIS)を参照してください。

> **注：**
>
> この手順では、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 を構成する手順を完了するときは、ルート証明書をインポートするためにこれらの設定を完了する必要があります。インストール手順の詳細については、Installing XenMobileを参照してください。

- FIPS を有効にする：はい
- ルート証明書をアップロード：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*
- ポート：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：任意の名前。

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**に移動し、**FIPSモードを有効にする**プロパティを編集して、値を**true**に設定します。詳細については、クライアントプロパティを参照してください。

クラスタリングの構成

クラスタリングを構成するには、Citrix ADCで次の2つの負荷分散仮想IPアドレスを構成します。

- **モバイルデバイス管理（MDM）負荷分散仮想IPアドレス:** クラスタで構成されている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。
- **モバイルアプリ管理（MAM）負荷分散仮想IPアドレス:** Citrix Gatewayがクラスタで構成されているXenMobileノードと通信するには、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、Citrix Gatewayからのすべてのトラフィックがポート8443の負荷分散仮想IPアドレスにルーティングされます。

このセクションの手順では、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。これらの手順により、クラスター設定が作成されます。

前提条件

- 必要なXenMobileノードを完全に構成していること。
- すべてのクラスターノードとXenMobileデータベースでNTPを構成します。クラスタリングが正しく機能するためには、すべてのサーバーで同じ時刻が設定されている必要があります。
- MDMロードバランサー用のパブリックIPアドレス1つと、MAM用のプライベートIPアドレス1つ。
- サーバー証明書。
- Citrix Gateway仮想IPアドレス用の空きIPアドレス1つ。
- XenMobileがクラスター設定で、MDM専用モードまたはエンタープライズモード（MDM+MAM）で展開されている場合：すべてのCitrix ADC MDMロードバランサー、つまりポート8443および443用に設定された仮想サーバーに対して、**送信元IP永続性**を使用するようにCitrix ADCロードバランサー構成を変更します。この構成は、ユーザーデバイスがiOS 11にアップグレードする前に完了してください。詳細については、Citrix Knowledge Centerの記事を参照してください: `<https://support.citrix.com/article/CTX227406>`。
- iOS 11デバイスに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。

クラスター構成のXenMobile 10.xの参照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

必要なノード数に基づいて、XenMobile VMを作成します。新しいVMを同じデータベースにポイントし、同じPKI証明書パスワードを提供します。

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。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-admin-password-cli.png)

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。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-ip-address.png)

3. データ保護にデフォルトのパスワードを使用する場合は「**y**」と入力します。それ以外の場合は「**n**」と入力して新しいパスワードを入力します。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-encryption-passphrase.png)

4. FIPSを使用する場合は「**y**」と入力します。それ以外の場合は「**n**」と入力します。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-fips-no.png)

5. 以前に完全に構成されたVMがポイントしていたのと同じデータベースをポイントするようにデータベースを構成します。メッセージ「`Database already exists`」が表示されます。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-same-db-pointed.png)

6. 最初のVMに指定した証明書と同じパスワードを入力します。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-connect-existing-db3.png)

   パスワードを入力すると、2番目のノードの初期構成が完了します。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-initial-config-complete2.png)

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

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

Initial system configuration complete!
Stopping configuration app...                                    [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                            [ OK ]
Stopping main app...                                             [ OK ]
Starting main app...
  this may take a few minutes.........................^[.....................
.....................................
  application started                                            [ OK ]

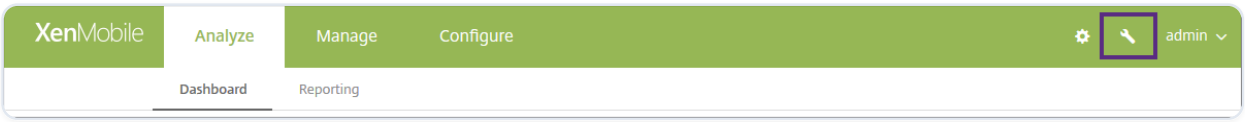
  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                           [ OK ]

xms51.wg.lab login:
```

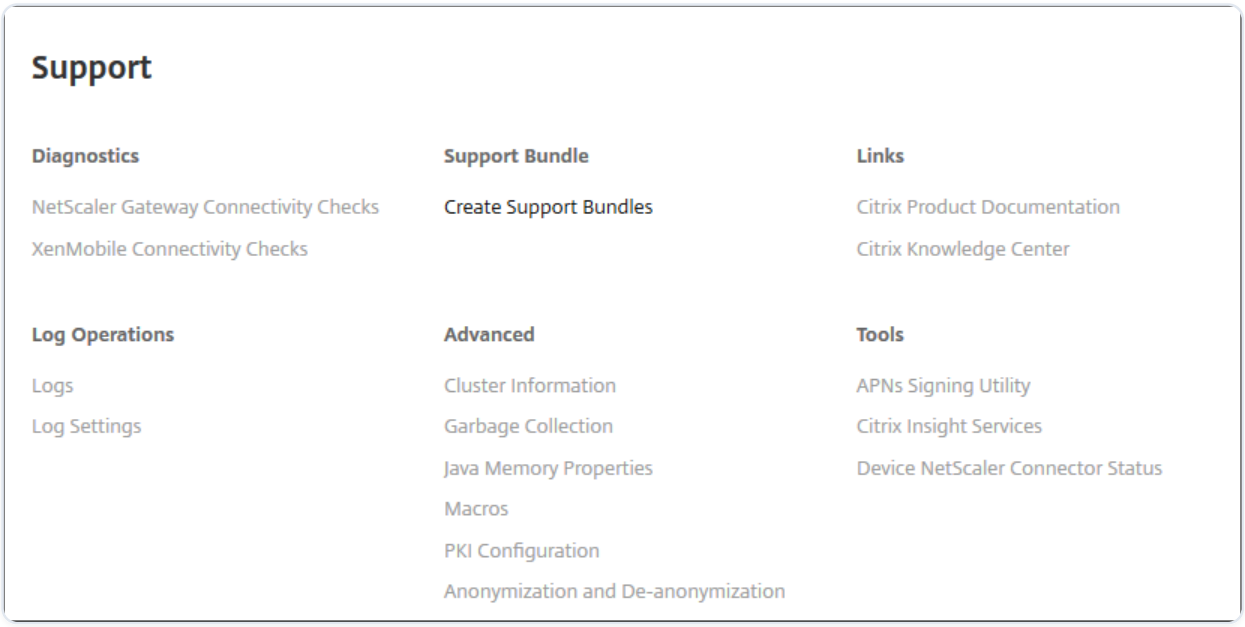
> **注：**
>
> ログオンダイアログボックスは、最初のVMのログオンダイアログボックスと似ています。この一致は、両方のVMが同じデータベースサーバーを使用していることを確認する方法です。

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

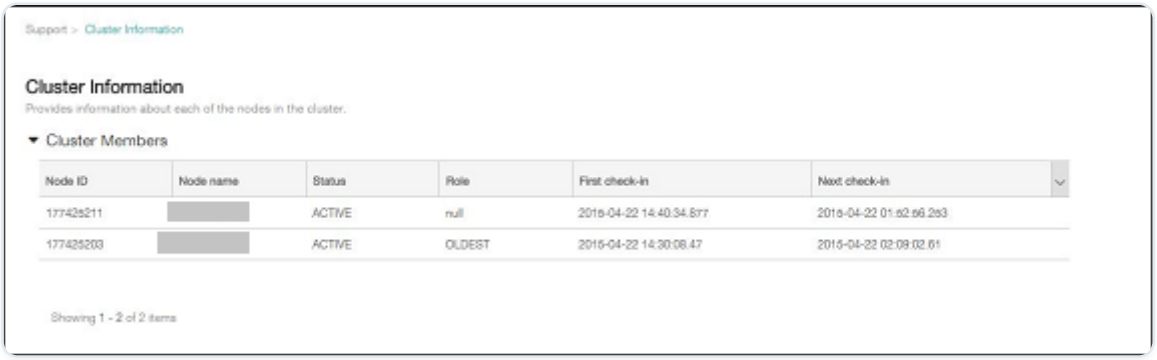


サポートページが開きます。

10. **詳細設定**の下で、**クラスター情報**をクリックします。



クラスターメンバー、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した。

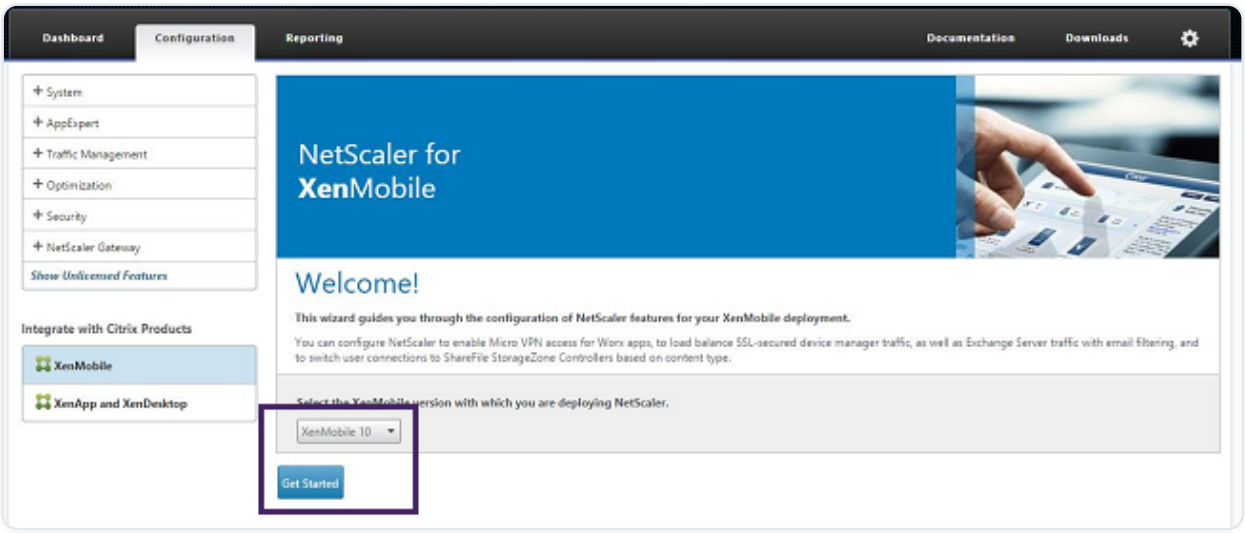


同じ手順に従って、他のノードを追加できます。クラスターに追加された最初のノードの役割は**OLDEST**です。その後に追加されたノードの役割は**NONE**または**null**と表示されます。

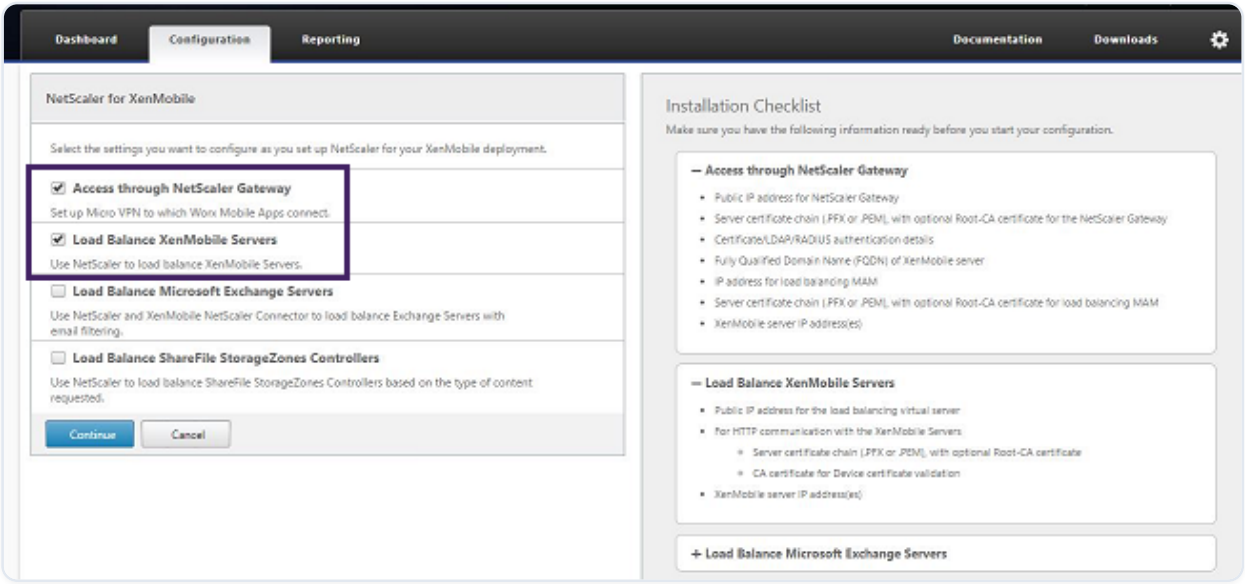
Citrix ADCでXenMobileクラスターの負荷分散を構成するには

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ら、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。負荷分散は、Citrix ADCで利用可能なXenMobileウィザードを実行することによって行われます。次の手順では、ウィザードを実行してXenMobileの負荷分散を行う方法について説明します。

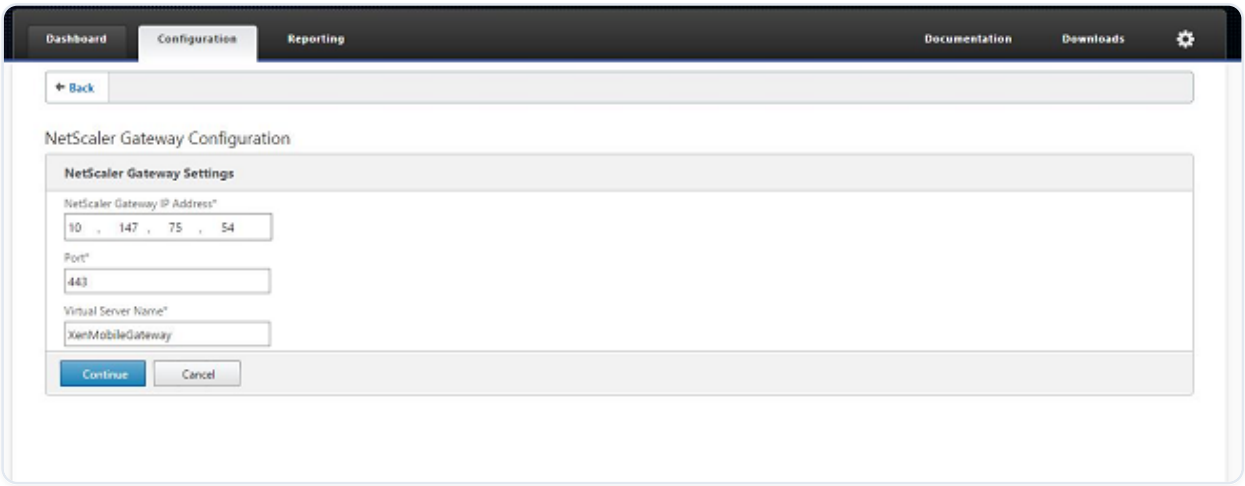
1. Citrix ADC にログオンします。
2. 「Configuration」タブで、「**XenMobile**」をクリックし、次に「**Get Started**」をクリックします。



3. 「**Access through Citrix Gateway**」チェックボックスと「**Load Balance XenMobile Servers**」チェックボックスをオンにして、「**Continue**」をクリックします。



4. Citrix Gateway の IP アドレスを入力し、次に「**Continue**」をクリックします。

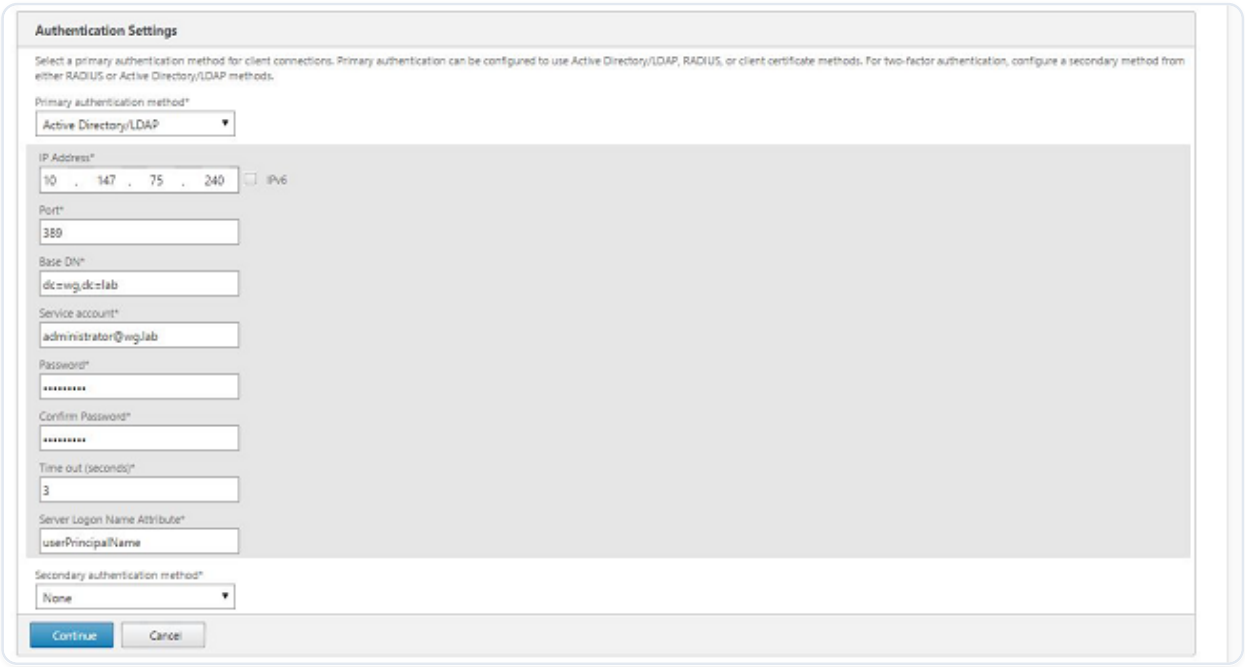


5. サーバー証明書を Citrix Gateway 仮想 IP アドレスにバインドするには、次のいずれかを実行し、次に「**Continue**」をクリックします。

   - 「**Use existing certificate**」で、一覧からサーバー証明書を選択します。
   - 「**Install Certificate**」タブをクリックして、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、次に「**Continue**」をクリックします。



> **注：**
>
> サーバーログオン名属性が、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設定で、MAMの負荷分散FQDNを入力し、「**Continue**」をクリックします。

   クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip.png)

   > **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。

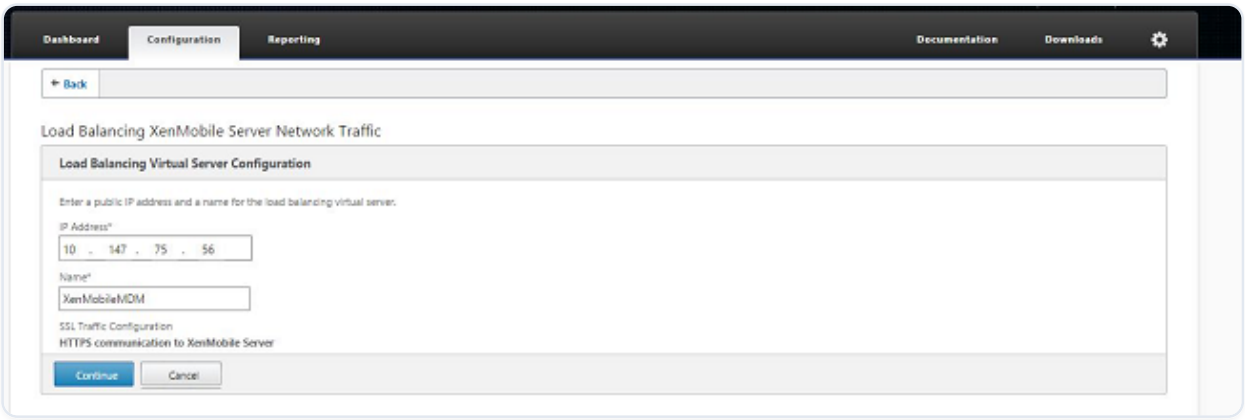
8. SSLブリッジモード (HTTPS) を使用する場合は、「**HTTPS communication to XenMobile Server**」を選択します。ただし、SSLオフロードを使用する場合は、前の図に示すように「**HTTP communication to XenMobile Server**」を選択します。この記事では、SSLブリッジモード (HTTPS) を選択します。
9. MAM負荷分散仮想IPアドレスのサーバー証明書をバインドし、「Continue」をクリックします。 クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-ns-xm-wizard-mam-vip-certbind.png)
10. XenMobile Serversで、「**Add Server**」をクリックしてXenMobileノードを追加します。

    クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip-addnodes.png)
11. XenMobileノードのIPアドレスを入力し、「Add」をクリックします。

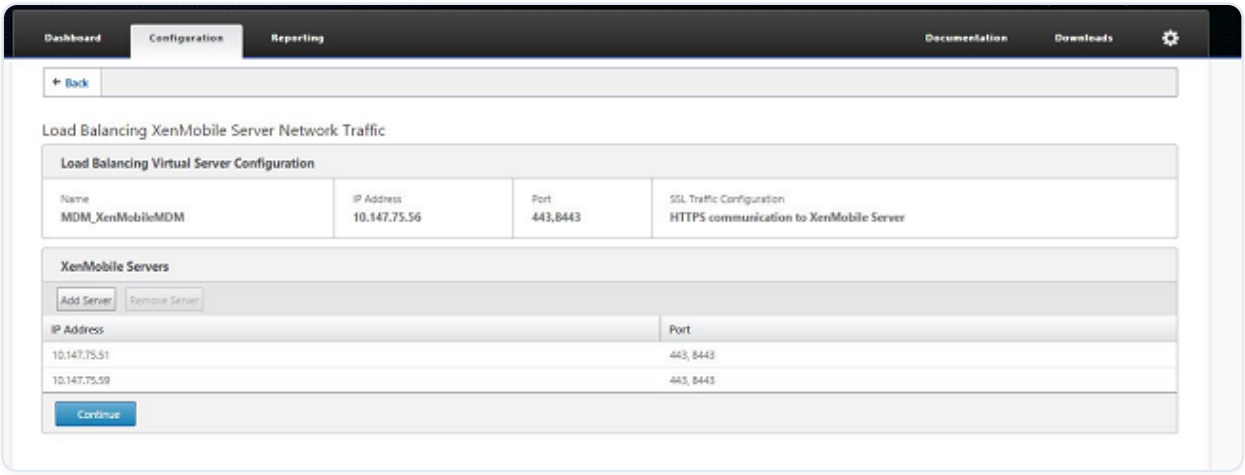
    クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard.mam-vip-addnodes1.png)
12. 手順10と11を繰り返して、XenMobileクラスターの一部であるXenMobileノードを追加します。追加したすべてのXenMobileノードが表示されます。「Continue」をクリックします。

    クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mam-vip-addnodes2.png)
13. 「**Load Balance Device Manager Servers**」をクリックして、MDM負荷分散構成を続行します。

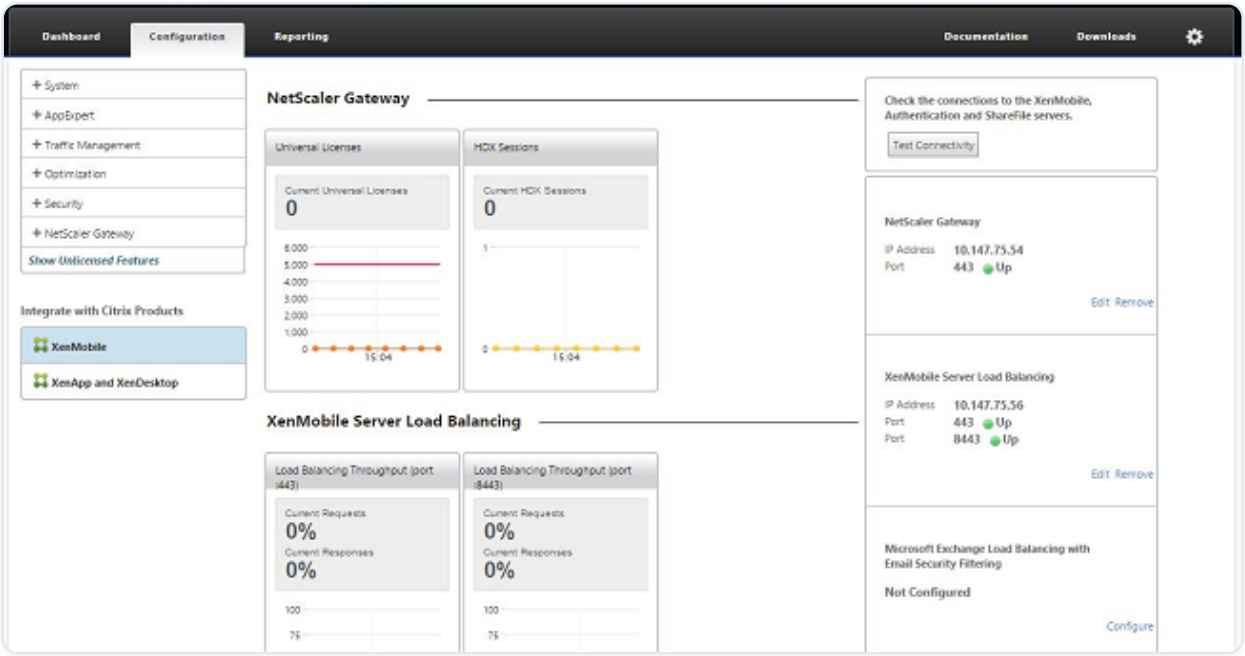
    クラスターノードのセットアップ(/en-us/xenmobile/server/media/xmob-cluster-xm-wizard-mdm-vip.png)
14. MDM負荷分散IPアドレスに使用するIPアドレスを入力し、「**Continue**」をクリックします。



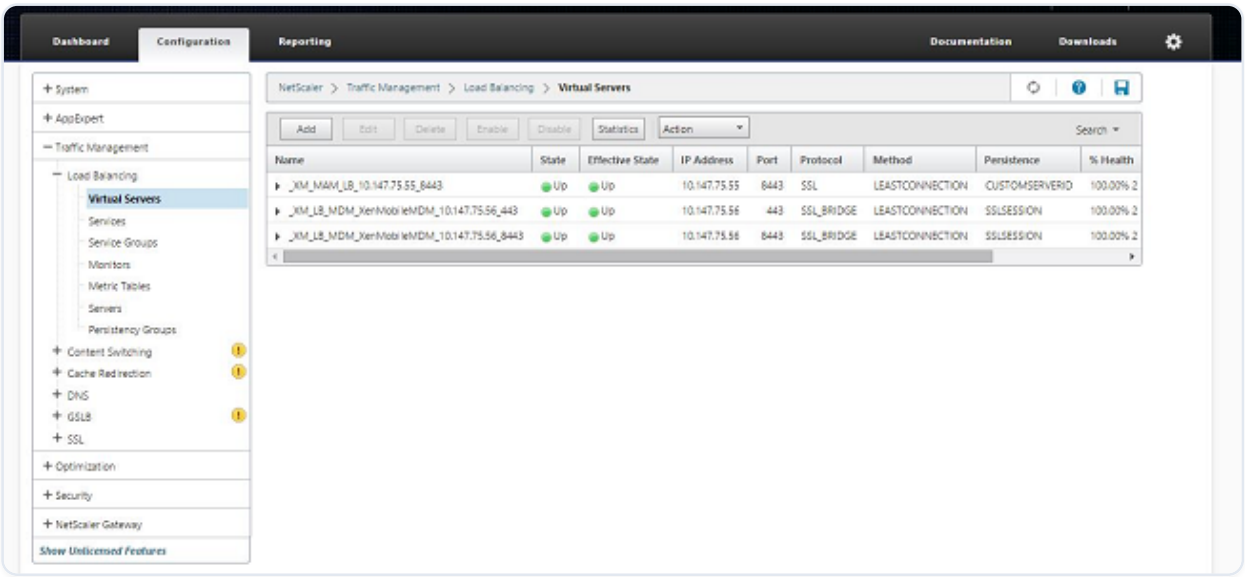
15. リストにXenMobileノードが表示されたら、**続行**をクリックし、次に完了をクリックしてプロセスを終了します。



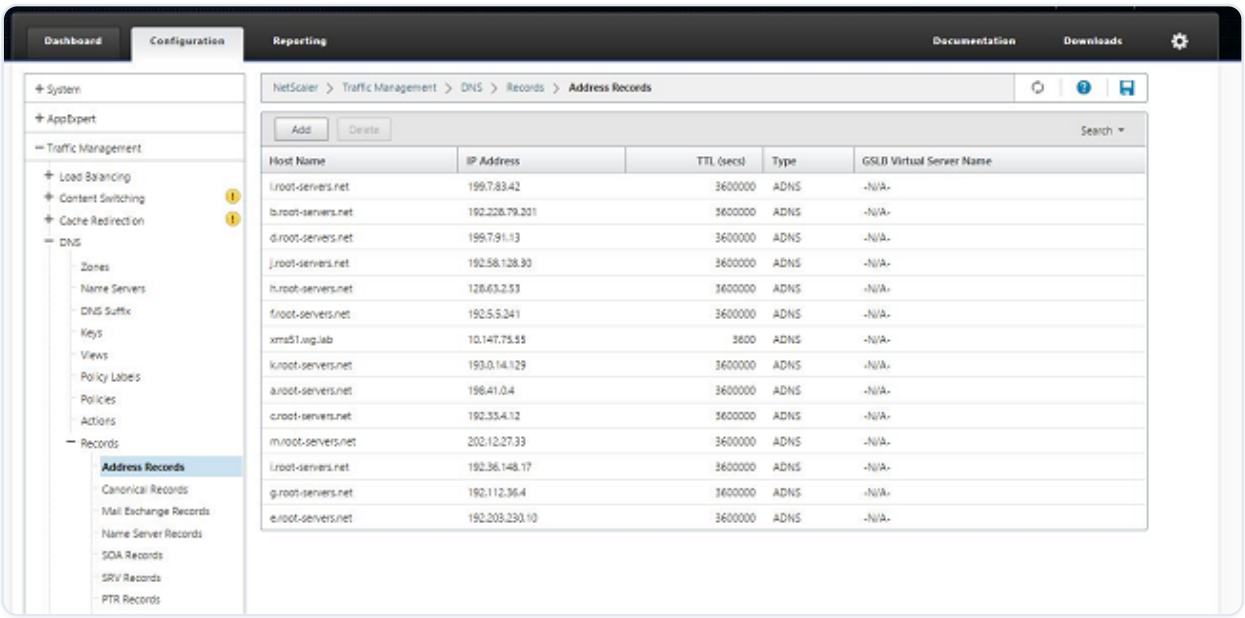
XenMobileページに仮想IPアドレスのステータスが表示されます。



16. 仮想IPアドレスが稼働していることを確認するには、「構成」タブをクリックし、**トラフィック管理 > 負荷分散 > 仮想サーバー**の順に移動します。



Citrix ADCのDNSエントリがMAM負荷分散仮想IPアドレスを指していることも確認できます。



災害復旧ガイド

アクティブ-パッシブフェールオーバーストラテジーを使用して、災害復旧のために複数のサイトを含むXenMobile展開を設計および構成できます。詳細については、XenMobile展開ハンドブックの「災害復旧」(/ja-jp/xenmobile/server/advanced-concepts/xenmobile-deployment/disaster-recovery.html)記事を参照してください。

プロキシサーバーを有効にする

送信インターネットトラフィックを制御するために、XenMobile® でプロキシサーバーをセットアップして、そのトラフィックを処理できます。プロキシサーバーはコマンドラインインターフェ

イス (CLI) を介して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 のメインメニューで、「**2**」と入力してシステムメニューを選択します。
2. システムメニューで、「**6**」と入力してプロキシサーバーメニューを選択します。

   プロキシサーバー設定の画像(/en-us/xenmobile/server/media/proxy-server-setup-1.png)
3. プロキシ構成メニューで、「**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。プロキシは、SOCKS と HTTPS の設定を同じ構成で保存した場合にのみ機能します。

   プロキシサーバー設定の画像(/en-us/xenmobile/server/media/proxy-server-setup-2.png)
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。各プロキシサーバータイプでサポートされているターゲットタイプについては、次の表を参照してください。

プロキシタイプ	**サポートされているターゲット**
SOCKS	APNS
HTTP	APNS, Web, PKI
HTTPS	Web、PKI
認証ありのHTTP	Web、PKI
認証ありのHTTPS	Web、PKI

```
---------------------------------
Proxy Configuration Menu
---------------------------------
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
---------------------------------
Choice: [0 - 6] 1

Enter socks proxy information

Address []: 203.0.113.23

Port[]: 1080

Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]:
```

5. **n**と入力し、次に**2**と入力してHTTPSを選択します。
6. 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。
7. プロキシサーバーで認証用のユーザー名とパスワードを設定する場合は、**y**と入力し、次にユーザー名とパスワードを入力します。

```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
---------------------------------
Choice: [0 - 6] 2

Enter https proxy information

Address []: 203.0.113.23

Port[]: 4443

Configure username & password [y/n]: y

Username: Justaname

Password:

Target - WEB
WEB proxy configured. Override proxy settings?[y/n]:
```

8. **y**と入力して設定を保存します。

SQL Server の構成

オンプレミスの XenMobile® Server から SQL Server への接続には、以下のいずれかのドライバーを使用できます。

- デフォルトドライバー
- jTDS
- Microsoft Javaデータベース接続 (JDBC) ドライバー

jTDS ドライバーは、次の場合にデフォルトドライバーになります。

- XenMobile Server をオンプレミスにインストールする場合。
- jTDS ドライバーを使用するように構成されている XenMobile Server からアップグレードする場合。

どちらのドライバーでも、XenMobile は SQL Server 認証または Windows 認証をサポートします。これらの認証とドライバーの組み合わせでは、SSL はオンまたはオフにできます。

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 を使用した統合認証を使用します。XenMobile は Kerberos に接続して、Kerberos Key Distribution Center (KDC) の詳細を取得します。必要な詳細が利用できない場合、XenMobile CLI は Active Directory サーバーの IP アドレスを要求します。

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 で接続し、XenMobile CLI を使用して構成します。手順は、現在の jTDS ドライバー構成によって次のように異なります。

Microsoft JDBC に切り替える (SQL Server 認証)

これら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 で接続します。
2. XenMobile CLI のメインメニューで、「**2**」と入力して「**System Menu**」を選択します。
3. 「詳細設定」を選択するには「**12**」と入力します。
4. 「JDBCドライバーの切り替え」を選択するには「**7**」と入力し、Microsoftの場合は「**m**」と入力します。

   JDBCドライバーの選択の画像(/en-us/xenmobile/server/media/cli-choose-jdbc-driver.png)
5. プロンプトが表示されたら、「**y**」と入力して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ノードで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オフ、Windows認証）

これら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レルム、およびKDCユーザー名が必要です。

1. すべてのXenMobile Serverノードに SSH接続します。
2. XenMobile CLIのメインメニューで、「**2**」と入力して「**System Menu**」を選択します。
3. 「詳細設定」を選択するには「**12**」と入力します。
4. 「JDBCドライバーの切り替え」を選択するには「**7**」と入力し、「**m**」と入力します。
5. SQL Server認証を使用するかどうかを尋ねられたら、「**n**」と入力します。
6. プロンプトが表示されたら、SQLサーバー用に構成されたActive Directoryのユーザー名とパスワードを入力します。
7. XenMobileがKerberos KDCレルムを自動検出しない場合、SQLサーバーのFQDNを含むKDCの詳細を要求します。
8. SSLを使用するかどうかを尋ねられたら、「**n**」と入力します。XenMobileは構成を保存します。エラーのためにXenMobileが構成を保存できない場合、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データベースパスワードを変更するには

XenMobileデータベースパスワードを変更するには、このガイダンスに従ってください。Citrixサポートからパスワード変更を指示された場合などが該当します。

SQLサーバーがWindows認証を使用している場合、Windows Active Directoryでデータベースパスワードを変更します。その後、データベースサーバー上のデータベース管理者アカウントを更新して、パスワードの変更を同期します。その後、次のようにXenMobileでパスワードを変更できます。

> **重要:**

- XenMobileでデータベースパスワードを変更するためのスケジュールされたメンテナンス期間を計画してください。パスワードの変更はシステムダウンタイム中に実行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を再起動しない場合、XenMobileはリカバリモードになります。その場合、SQLサーバーで古いパスワードに戻し、XenMobileを再起動して、再度パスワードを変更してください。

1. すべてのXenMobile Serverノードが実行されていることを確認します。クラスター環境の場合は、すべてのノードを起動します。
2. 仮想サーバーを無効にすることで、Citrix ADCロードバランサーでの受信デバイストラフィックをブロックします。
3. SQLサーバーでデータベースパスワードを変更するには: XenMobile CLIにログインし、**Configuration > Database**に移動して、プロンプトが表示されたら変更されたパスワードを入力します。

   ```
   Server []: <ipAddress>

   Port [1433]: 1433

   Username [sa]: <userName>

   Password: <****>
   ```

4. サーバーを再起動するには「**Y**」を選択します。
5. クラスター内の他のすべてのノードに対して手順3と4を繰り返します。
6. Citrix ADCロードバランサーで仮想サーバーを有効にすることで、受信デバイスの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

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、多くのサーバープロパティについて説明し、サーバープロパティの追加、編集、削除の方法を詳しく解説します。

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。

通常構成されるプロパティについては、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の定義

常にデバイスを追加

- **true**の場合、XenMobileは登録に失敗した場合でもデバイスをXenMobileコンソールに追加し、どのデバイスが登録を試行したかを確認できるようにします。デフォルトは**false**です。

AGクライアント証明書発行スロットリング間隔

- 証明書生成間の猶予期間です。この間隔により、XenMobileが短期間にデバイスに対して複数の証明書を生成するのを防ぎます。Citrix®は、この値を変更しないことを推奨します。デフォルトは**30**分です。

監査ログクリーンアップ実行時間

- 監査ログのクリーンアップを開始する時刻で、HH:MM AM/PM形式です。例：04:00 AM。デフォルトは**02:00 AM**です。

監査ログクリーンアップ間隔（日数）

- XenMobileが監査ログを保持する日数です。デフォルトは**1**です。

監査ロガー

- **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。デフォルトは**False**です。

監査ログの保持期間 (日数)

- XenMobile が監査ログを保持する日数。デフォルトは **7** です。

auth.ldap.connect.timeout と auth.ldap.read.timeout

- LDAP応答の遅延を補うため、Citrixは以下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推奨します。
    - 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読み取りタイムアウト**

証明書の更新 (秒)

- 証明書の有効期限が切れる何秒前にXenMobileが証明書の更新を開始するか。たとえば、証明書が12月30日に期限切れになり、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）です。

接続タイムアウト

- セッションの非アクティブタイムアウト（分単位）。この時間が経過すると、XenMobileはデバイスへのTCP接続を閉じます。セッション自体は開いたままです。Androidデバイスとリモートサポートに適用されます。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つ秒数。証明書サーバーが遅く、トラフィックが多い場合は、この値を60秒以上に増やしてください。120秒経っても応答しない証明書サーバーはメンテナンスが必要です。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がリソースをデバイスに展開する方法を決定します。ユーザーレベル（**DEFAULT_TO_USER**）またはデバイスレベル。デフォルトは**DEFAULT_TO_DEVICE**です。

展開ログのクリーンアップ（日数）

- XenMobileが展開ログを保持する日数。デフォルトは**7**です。

ホスト名検証の無効化

- デフォルトでは、Microsoft PKIサーバーを除くすべての送信接続でホスト名検証が有効になっています。ホスト名検証が失敗すると、サーバーログに「ボリューム購入サーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません」などのエラーが含まれます。ホスト名検証によって展開が中断される場合は、このプロパティを**true**に変更してください。デフォルトは**false**です。

SSLサーバー検証の無効化

- **True**の場合、以下のすべての条件が満たされたときにSSLサーバー証明書の検証を無効にします。
    - XenMobile Serverで証明書ベースの認証を有効にしていること。
    - Microsoft CAサーバーが証明書の発行元であること。
    - XenMobile Serverがルートを信頼していない内部CAが、証明書に署名しました。

デフォルトは**True**です。

コンソールを有効にする

- **true**の場合、ユーザーはセルフヘルプポータルコンソールにアクセスできます。デフォルトは**true**です。

クラッシュレポートを有効にする

- **true**の場合、CitrixはSecure Hub for iOSおよびAndroidの問題のトラブルシューティングに役立つクラッシュレポートと診断情報を収集します。**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。

診断用のHibernate統計ログを有効/無効にする

- **True**の場合、アプリケーションのパフォーマンス問題のトラブルシューティングを支援するために、Hibernate統計ログが有効になります。Hibernateは、XenMobileがMicrosoft SQL Serverに接続するために使用されるコンポーネントです。デフォルトでは、ログ記録はアプリケーションのパフォーマンスに影響を与えるため無効になっています。巨大なログファイルの作成を避けるため、短期間のみログ記録を有効にしてください。XenMobileはログを/opt/sas/logs/hibernate_stats.logに書き込みます。デフォルトは**False**です。

macOS OTAEを有効にする

- **false**の場合、macOSデバイスの登録リンクの使用が禁止され、macOSユーザーは登録招待状を使用することによってのみ登録できます。デフォルトは**true**です。

通知トリガーを有効にする

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

force.server.push.required.apps

- 次のような状況で、AndroidおよびiOSデバイスへの必須アプリの強制展開を有効にします。
  - 新しいアプリをアップロードし、必須としてマークします。
  - 既存のアプリを必須としてマークします。
  - ユーザーが必須アプリを削除した場合。
  - Secure Hub のアップデートが利用可能です。

必須アプリの強制展開は、デフォルトで **false** です。カスタムキーを作成し、**Value** を **true** に設定して強制展開を有効にします。強制展開中、エンタープライズアプリやパブリックアプリストアアプリを含む、MDX対応の必須アプリは即座にアップグレードされます。このアップグレードは、アプリの更新猶予期間に対して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: **必須アプリの展開を強制する**

ActiveSyncの許可ユーザーと拒否ユーザーの完全なプル

- XenMobileがActiveSyncの許可ユーザーと拒否ユーザーの完全なリスト（ベースライン）をプルする間隔（秒単位）。デフォルトは **28800** 秒です。

hibernate.c3p0.idle_test_period

- このXenMobile Serverプロパティ（カスタムキー）は、接続が自動的に検証されるまでのアイドル時間（秒単位）を決定します。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 アイドルテスト期間**

hibernate.c3p0.max_size

- このカスタムキーは、XenMobile が SQL Server データベースに開くことができる接続の最大数を決定します。XenMobile は、このカスタムキーに指定した値を上限として使用します。接続は、必要な場合にのみ開かれます。設定は、データベースサーバーの容量に基づいてください。詳細については、「XenMobile 操作のチューニング」を参照してください。キーは次のように構成します。デフォルトは **1000** です。
- キー: **hibernate.c3p0.max_size**
- 値: **1000**
- 表示名: **hibernate.c3p0.max_size**
- 説明: **SQL への DB 接続**

hibernate.c3p0.min_size

- このカスタムキーは、XenMobile が SQL Server データベースに開く最小接続数を決定します。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: **SQL への DB 接続**

hibernate.c3p0.timeout

- このカスタムキーは、アイドルタイムアウトを秒単位で決定します。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どうかを識別します

- テレメトリ（カスタマーエクスペリエンス向上プログラム、またはCEIP）が有効になっているかどうかを識別します。XenMobileをインストールまたはアップグレードする際に、CEIPにオ

プトインできます。XenMobileで15回連続してアップロードが失敗した場合、テレメトリは無効になります。デフォルトは **false** です。

非アクティブタイムアウト（分）

- **WebServices timeout type** サーバープロパティが **INACTIVITY_TIMEOUT** の場合: このプロパティは、XenMobileが以下の操作を行った非アクティブな管理者をログアウトするまでの分数を定義します。
  - RESTサービス用のXenMobile Public 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 Public APIを使用してサードパーティアプリにアクセスした。タイムアウトが **0** の場合、非アクティブなユーザーは引き続きログイン状態であることを意味します。

デフォルトは **5** です。

iOSデバイス管理登録の自動インストールが有効

- trueの場合、このプロパティはデバイス登録中に必要なユーザー操作の量を減らします。ユーザーは、必要に応じて**ルートCAのインストール**と**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デバイス管理登録の最初のステップの遅延

- ユーザーがデバイス登録中に資格情報を入力した後、この値はルートCAのプロンプトが表示されるまでの待機時間を指定します。Citrixは、ネットワークの遅延や速度の問題がある場合にのみ、このプロパティを編集することを推奨します。その場合、値を5000ミリ秒（5秒）より大きく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デバイス管理登録の最終ステップの遅延

- デバイス登録中、このプロパティ値は、MDMプロファイルのインストールとデバイス上でのエージェントの起動の間に待機する時間を指定します。Citrixは、ネットワークの遅延や速度の問題がある場合にのみ、このプロパティを編集することを推奨します。その場合、値を5000ミリ秒（5秒）より大きく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配信モード

- XenMobileがMDM証明書をデバイスに配布する方法を、**SCEP**（セキュリティ上の理由から推奨）または**PKCS12**のどちらを使用するかを指定します。PKCS12モードでは、キーペアはサーバー上で生成され、ネゴシエーションは行われません。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、およびXenMobile iOSエージェントIDの秘密鍵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

- XenMobileが証明書の更新を開始する、証明書の有効期限までの日数を指定します。例：証明書が10日後に期限切れになり、このプロパティが**10**日の場合、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**日です。

iOS MDM APNS秘密鍵パスワード

- 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ています。

デバイスが切断されるまでの非アクティブ期間

- XenMobileがデバイスを切断するまでに、最後の認証を含め、デバイスが非アクティブ状態を維持できる期間を指定します。デフォルトは**7**日です。

MAM専用デバイスの最大数

- このカスタムキーは、各ユーザーが登録できるMAM専用デバイスの数を制限します。キーは次のように構成します。**値**を**0**にすると、デバイスの登録が無制限になります。
- キー = **number.of.mam.devices.per.user**
- 値 = **5**
- 表示名 = **MAM Only Device Max**
- 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

- 多数のボリューム購入ライセンスをインポートする際に使用されるスレッド数。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、6などのより多くのスレッドを使用すると、ボリューム購入のインポートでCPU使用率が高くなります。

Citrix ADCシングルサインオン

- **False**の場合、Citrix ADCからXenMobileへのシングルサインオン中にXenMobileコールバック機能を無効にします。Citrix Gateway構成にコールバックURLが含まれている場合、XenMobile

はコールバック機能を使用してCitrix GatewayセッションIDを検証します。デフォルトは**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）のアップロード中に連続して失敗した回数を表示します。アップロードが失敗すると、XenMobileはこの値をインクリメントします。15回のアップロード失敗後、XenMobileはCEIP（テレメトリとも呼ばれます）を無効にします。詳細については、サーバープロパティ**Identifies if telemetry is enabled or not**を参照してください。アップロードが成功すると、XenMobileはこの値を**0**にリセットします。

デバイスあたりのユーザー数

- MDMに同じデバイスを登録できるユーザーの最大数。**0**の値は、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。

許可および拒否されたユーザーの増分変更のプル

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

Microsoft 認証サーバーへの読み取りタイムアウト

- XenMobile が読み取りを行う際に、証明書サーバーからの応答を待機する秒数。証明書サーバーが遅く、トラフィックが多い場合は、この値を 60 秒以上に増やすことができます。120 秒経っても応答しない証明書サーバーはメンテナンスが必要です。デフォルトは **15000** ミリ秒 (15 秒) です。

REST Web サービス

- REST Web サービスを有効にします。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時のマルチスレッド処理に内部的に使用されます。値が高いほど、単一のスレッドがより多くのデバイスを解析します。値が低いほど、より多くのスレッドがデバイスを取得します。値を減らすと、エクスポートとデバイスリスト取得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があります。デフォルトは **1000** です。

セッションログのクリーンアップ (日数)

- XenMobile がセッションログを保持する日数。デフォルトは **7** です。

サーバーモード

- XenMobile が MAM、MDM、または ENT (エンタープライズ) モードで実行されるかどうかを決定します。これらはそれぞれ、アプリ管理、デバイス管理、またはアプリとデバイスの管理に対応します。デバイスを登録する方法に応じて、以下の表に示すようにサーバーモードプロパティを設定します。サーバーモードは、ライセンスの種類に関係なく、デフォルトで **ENT** に設定されます。

XenMobile MDM Edition ライセンスをお持ちの場合、**サーバープロパティ**でサーバーモードをどのように設定しても、有効なサーバーモードは常に MDM になります。MDM Edition ライセンスをお持ちの場合、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することはできません。

お持ちのライセンスエディション	デバイスをこのモードで登録したい場合	サーバーモードプロパティを次のように設定します
エンタープライズ / アドバンスト	MDMモード	MDM
エンタープライズ / アドバンスト	MDM+MAMモード	ENT
MDM	MDMモード	MDM

有効なサーバーモードは、ライセンスの種類とサーバーモードの組み合わせです。MDMライセンスの場合、サーバーモードの設定に関わらず、有効なサーバーモードは常にMDMです。EnterpriseおよびAdvancedライセンスの場合、サーバーモードが**ENT**または**MDM**であれば、有効なサーバーモードはサーバーモードと一致します。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。

XenMobileは、以下の各アクティビティについて、サーバーモードをサーバーログに追加します。ライセンスがアクティブ化されたとき、ライセンスが削除されたとき、および**サーバープロパティ**でサーバーモードを変更したとき。ログファイルの作成と表示については、ログおよびXenMobileでログファイルを表示および分析するを参照してください。

ShareFile構成タイプ

- Citrix Filesのストレージタイプを指定します。**ENTERPRISE**はCitrix Files Enterpriseモードを有効にします。**CONNECTORS**は、XenMobileコンソールを通じて作成するストレージゾーンコネクタへのアクセスのみを提供します。デフォルトは**NONE**で、これは**構成 > ShareFile**画

面の初期ビューを表示し、Citrix Files Enterpriseとコネクタのどちらかを選択します。デフォルトは**NONE**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**の場合: このプロパティは、以下の使用後にXenMobileが管理者をログアウトさせるまでの分数を示します。
  - XenMobileコンソールにアクセスするためのRESTサービス用XenMobileパブリックAPI。
  - サードパーティ製アプリにアクセスするためのRESTサービス用XenMobileパブリックAPI。

デフォルトは**60**です。

トリガーエージェントメッセージ抑制

- Secure Hubクライアントメッセージングを有効または無効にします。値が**false**の場合、メッセージングが有効になります。デフォルトは**true**です。

トリガーエージェントサウンド抑制

- Secure Hubクライアントサウンドを有効または無効にします。値が**false**の場合、サウンドが有効になります。デフォルトは**true**です。

Androidデバイスの非認証アプリダウンロード

- **True**の場合、Android Enterpriseを実行しているAndroidデバイスにセルフホスト型アプリをダウンロードできます。Google PlayストアでダウンロードURLを静的に提供するAndroid Enterpriseオプションが有効になっている場合、XenMobileはこのプロパティを必要とします。その場合、ダウンロードURLには認証トークンを持つワンタイムチケット（**XAM One-Time Ticket server**プロパティで定義）を含めることはできません。デフォルトは**False**です。

Windowsデバイスの非認証アプリダウンロード

- ワンタイムチケットを検証しない古いSecure Hubバージョンでのみ使用されます。**False**の場合、XenMobileからWindowsデバイスに非認証アプリをダウンロードできます。デフォルトは**False**です。

ActiveSync IDを使用してActiveSyncデバイスワイプを実行する

- **true**の場合、Exchange ActiveSync用Endpoint Managementコネクタは、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。

Exchangeからのユーザーのみ

- **true**の場合、ActiveSync Exchangeユーザーのユーザー認証を無効にします。デフォルトは**false**です。

VPベースライン間隔

- XenMobileがAppleからボリューム購入ライセンスを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で、ボリューム購入からインポートされたアプリを手動で削除した場合など、すべての変更がXenMobileに反映されます。デフォルトでは、XenMobileはボリューム購入ライセンスのベースラインを最低**720**分ごとに更新します。

多数のボリューム購入ライセンスがインストールされている場合（例: 50,000以上）、Citrixは、ライセンスのインポート頻度とオーバーヘッドを削減するために、ベースライン間隔を長くすることを推奨します。

Appleからのボリューム購入ライセンスの変更が頻繁に発生すると予想される場合、Citrixは、変更に合わせてXenMobileを最新の状態に保つために、値を小さくすることを推奨します。2つのベースライン間の最小間隔は60分です。また、XenMobileは前回のインポート以降の変更をキャプチャするために、60分ごとに差分インポートを実行します。したがって、ボリューム購入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分遅れる可能性があります。

Webサービスタイムアウトタイプ

- パブリックAPIから取得した認証トークンの有効期限が切れる方法を指定します。**STATIC_TIMEOUT**の場合、XenMobileは、サーバープロパティ**Static Timeout in Minutes**で指定された値の後に認証トークンの有効期限が切れたと見なします。

INACTIVITY_TIMEOUTの場合、XenMobile は、サーバープロパティ **Inactivity Timeout in Minutes** で指定された値の期間、トークンが非アクティブであった場合に、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 WNSチャネル - 更新までの日数

- ChannelURIの更新頻度。デフォルトは**10**日です。

Windows WNSハートビート間隔

- XenMobileがデバイスに3分ごとに5回接続した後、次に接続するまでに待機する時間。デフォルトは**6**時間です。

XAMワンタイムチケット

- ワンタイム認証トークン（OTT）がアプリのダウンロードに有効なミリ秒数。このプロパティと、**Unauthenticated App download for Android**および**Unauthenticated App download for Windows**プロパティは連携して機能します。これらのプロパティは、認証されていない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セルフヘルプポータルコンソールの最大非アクティブ間隔（分）

- XenMobileが非アクティブなユーザーをXenMobileセルフヘルプポータルからログアウトするまでの分数。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の追加、編集、または削除

XenMobileでは、サーバーにプロパティを適用できます。変更を加えた後、変更をコミットしてアクティブ化するために、すべてのノードでXenMobileを再起動してください。

> **注：**
>
> XenMobileを再起動するには、ハイパーバイザーを介してコマンドプロンプトを使用します。

1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**の下にある**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**ページが表示されます。このページから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(/en-us/xenmobile/server/media/settings-server-server-properties.png)

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**ページが表示されます。

   サーバープロパティ(/en-us/xenmobile/server/media/settings-server-server-properties-add.png)
2. 次の設定を構成します。

   - キー：リストから適切なキーを選択します。キーは大文字と小文字を区別します。プロパティ値を編集する前、または特別なキーを要求する前に、Citrixサポートにお問い合わせください。

- 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**テーブル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：必要に応じて、新しいサーバープロパティの説明を入力します。

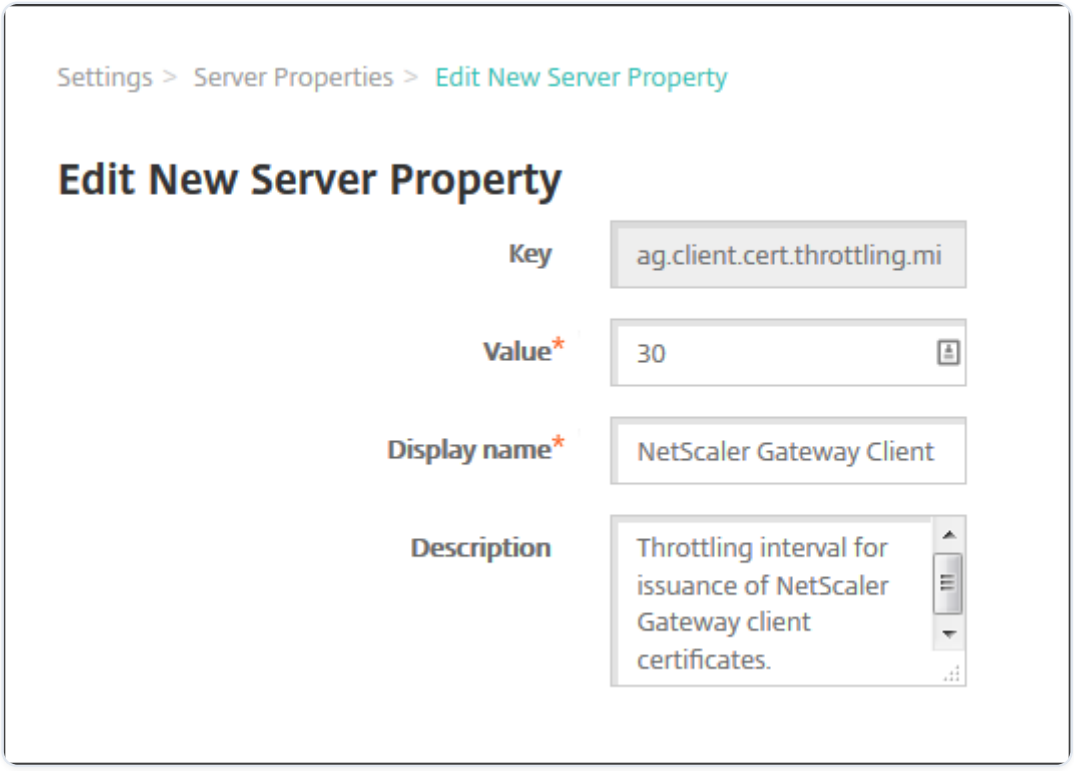
3. **保存**をクリックします。

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**テーブルで、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選択すると、オプションメニューがサーバープロパティリストの上に表示されます。リスト内の他の場所をクリックすると、リストの右側にオプションメニューが開きます。

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**ページが表示されます。



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: プロパティ値。
   - 表示名: プロパティ名。
   - 説明: プロパティの説明。

4. 変更を保存するには**保存**をクリックするか、プロパティを変更しないままにするには**キャンセル**をクリックします。

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**テーブルで、削除するサーバープロパティを選択します。

   複数のプロパティを削除するには、各プロパティの横にあるチェックボックスを選択します。
2. 「**削除**」をクリックします。確認ダイアログボックスが表示されます。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ースオプション

XenMobile® Server のオンプレミスインストールの場合、CLI オプションには次のようにアクセスできます。

- **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、コマンドプロンプトビューを開始して、XenMobile の管理者アカウントにログオンします。詳細については、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 が有効になっている場合、SSH を使用して:** XenMobile の管理者アカウントにログオンします。

CLI を使用して、さまざまな構成およびトラブルシューティングタスクを実行できます。次の図は、CLI のトップレベルメニューを示しています。

コマンドラインオプション(/en-us/xenmobile/server/media/cli-main-menu.png)

構成オプション

以下は、**構成メニュー**の例と、各オプションに表示される設定です。

コマンドラインオプション(/en-us/xenmobile/server/media/cli-configuration-menu.png)

ネットワーク

コマンドラインオプション(/en-us/xenmobile/server/media/cli-configuration-network.png)

ファイアウォール

コマンドラインオプション(/en-us/xenmobile/server/media/cli-configuration-firewall.png)

データベース

コマンドラインオプション(/en-us/xenmobile/server/media/cli-configuration-database.png)

リスナーポート

```
 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]:
```

クラスタリングオプション

以下は、**クラスタリングメニュー**のサンプルと、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
-----------------------------------
```

クラスターの状態を表示

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

クラスターの有効化/無効化

クラスタリングを有効にすることを選択すると、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.`.

クラスタリングを無効にすることを選択すると、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.`.

クラスターメンバーのホワイトリスト

```
Current White List:
 - 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


Please enter hosts or networks to be white listed:
```

SSLオフロードの有効化または無効化

SSLオフロードを有効または無効にすることを選択すると、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.`.

Hazelcastクラスターの表示

Hazelcastクラスターを表示することを選択すると、次のオプションが表示されます。

Hazelcastクラスターメンバー:

> **注:**
>
> 構成済みのノードがクラスターの一部でない場合は、そのノードを再起動してください。

システムオプション

システムメニューから、システムレベルの情報を表示または設定したり、サーバーを再起動またはシャットダウンしたり、**詳細設定**にアクセスしたりできます。

コマンドラインオプション(/en-us/xenmobile/server/media/cli-system-menu.png)

NTPサーバーの設定により、NTPサーバー情報を指定できます。XenMobileの時刻をハイパーバイザーと同期する際にタイムゾーンの問題が発生する場合は、XenMobileをNTPサーバーに指定することで問題を回避できます。このオプションを変更した後は、すべてのクラスターサーバーを再起動してください。

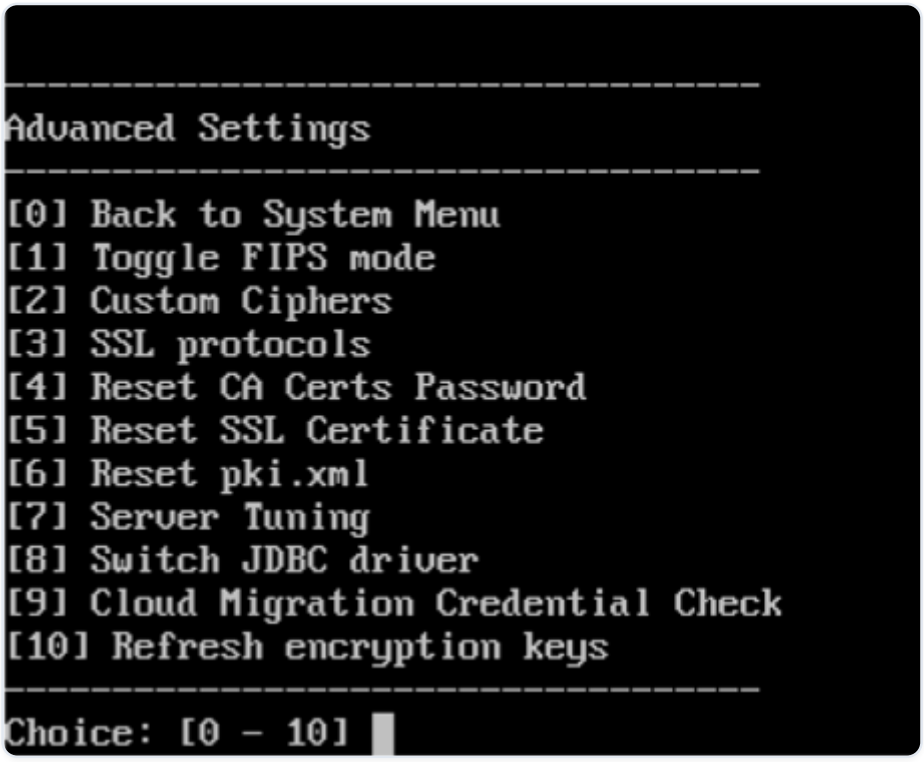
システムディスク使用量の表示メニュー項目を表示して、ディスク容量を確認することもできます。

サーバーノードのシャットダウンについて

クラスター内の単一のサーバーノードをシャットダウンした場合、スケーラビリティとパフォーマンスに記載されている要件を満たしていれば、他のノードが通常はワークロードを処理できます。影響は、同時に停止しているノードの数、ユーザーの総数、およびノードが停止している期間によって異なります。

- ユーザーは引き続きSecure Hubとストアにアクセスできます。
- 利用可能なノードがユーザー数を処理できる場合、ユーザーは展開された管理対象アプリに引き続きアクセスして起動できます。接続が遅くなり、デバイスのチェックインが遅くなる可能性があります。
- すべてのノードがダウンしない限り、デバイスポリシーは引き続き機能します。リソースとデバイスの数によっては、ポリシーの展開が遅くなる場合があります。

高度な設定



SSLプロトコルオプションは、デフォルトですべて許可されたプロトコルに設定されています。プロンプト**有効にする新しいSSLプロトコル**が表示されたら、有効にするプロトコルを入力します。XenMobileは、応答に含まれていないプロトコルを無効にします。例: 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。

サーバーチューニングオプションには、サーバー接続タイムアウト、最大接続数（ポート別）、および最大スレッド数（ポート別）が含まれます。

JDBCドライバーの切り替えオプションは、**jTDS**と**Microsoft** JDBCです。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ドライバーを参照してください。

トラブルシューティングオプション

以下は、**トラブルシューティングメニュー**のサンプルと、各オプションに表示される設定です。

```
-----------------------------------
Troubleshooting Menu
-----------------------------------
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
[4] Disk Usage
-----------------------------------
Choice: [0 - 4] 4
```

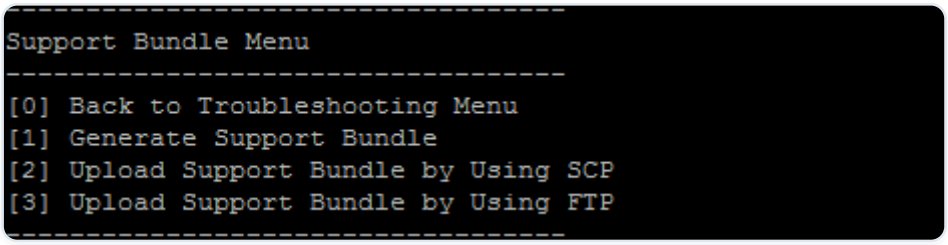
ネットワークユーティリティ

```
---------------------------------
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
---------------------------------
```

ログ

```
-----------------------------------
Logs Menu
-----------------------------------
[0] Back to Troubleshooting Menu
[1] Display debug log file
[2] Display update log file
```

サポートバンドル



ディスク使用量



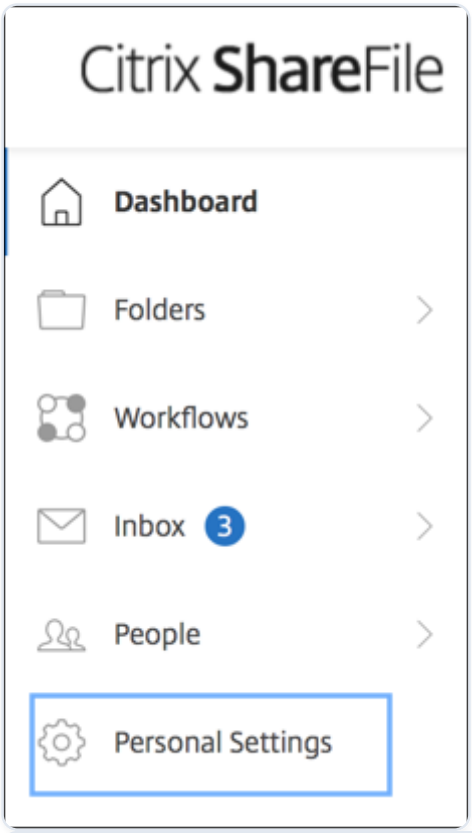
Citrix FilesをFTPサイトとして使用してサポートバンドルをアップロードするには

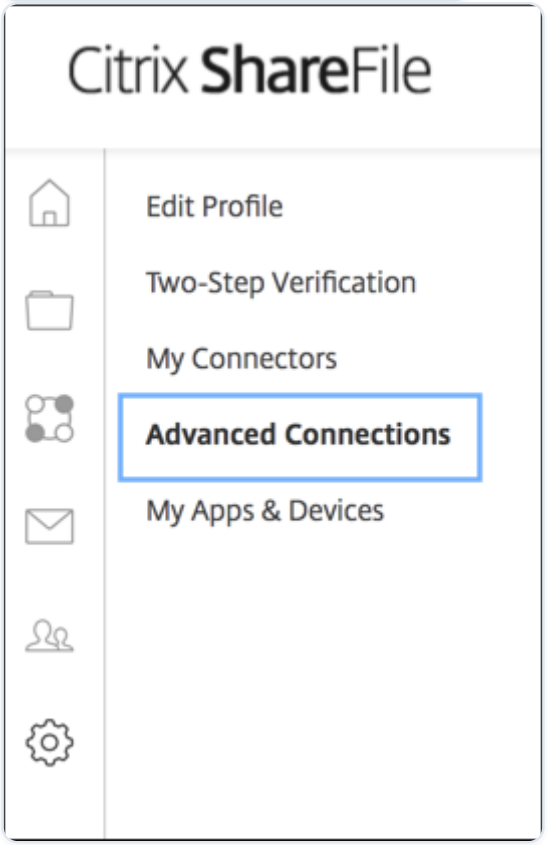
サポートバンドルのアップロードを開始する前に、Citrix Filesで以下の前提条件を構成してください。

1. FTPログオンの詳細を確認します。

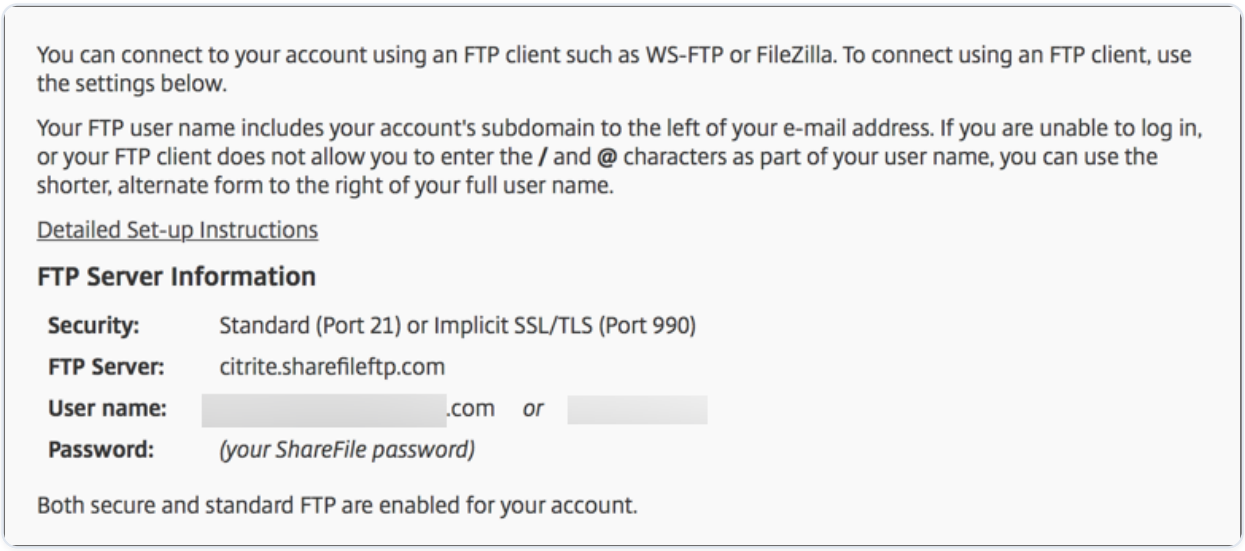
   a. Webブラウザーで`<https://citrix.sharefile.com>`を開きます。

   b. **Personal Settings**をクリックし、次に**Advanced connections**をクリックします。





c. FTPサーバー情報で、ユーザー名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。


You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

Detailed Set-up Instructions

FTP Server Information

Security:	Standard (Port 21) or Implicit SSL/TLS (Port 990)
FTP Server:	citrite.sharefileftp.com
User name:	.com *or*
Password:	*(your ShareFile password)*

Both secure and standard FTP are enabled for your account.

> **注：**
>
> - XenMobileからアップロードするファイルは、Linux CLIベースのFTPクライアントです。そのため、ユーザー名の一部としてバックスラッシュ (\) とアットマーク (@) を入力することはできません。
> - 英数字のユーザーIDが表示されない場合は、ShareFile管理者またはShareFileサポートにこのユーザーIDを要求できます。

2. Citrix Filesサーバーが FTPSとともにFTP通信で有効になっていることを確認してください。理想的には、ShareFile管理者はユーザーアカウントがFTP通信用に開かれることを許可します。ただし、FTPS通信のみが許可される場合もあります。

   管理者権限を持つユーザーは、**Settings** > **Admin Settings** > **Advanced Preferences** > **Enable ShareFile Tools** をクリックして、この設定を確認および有効にできます。**External Apps** > **FTP Access** で、**Enable** チェックボックスが選択されていることを確認してください。

   Citrix Filesの有効化チェックボックス(/en-us/xenmobile/server/media/sharefile-externaltools-ftp.png)

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。**Home** をクリックし、**Folders** をクリックしてから、**Personal Folders** をクリックします。
4. 右端にあるプラス記号（+）アイコンをクリックし、**Create Folder** をクリックしてから、フォルダーの名前を入力します。

Citrix Files共有フォルダーダイアログボックス(/en-us/xenmobile/server/media/sharefile-create-sharedfolder.png)

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

   コマンドラインオプション(/en-us/xenmobile/server/media/sharefile-ftp-cli-options.png)

   > **注:**
   >
   > サポートバンドルが存在する場合、プロンプトが表示されたら、バンドルを上書きするために **y** と入力します。

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。

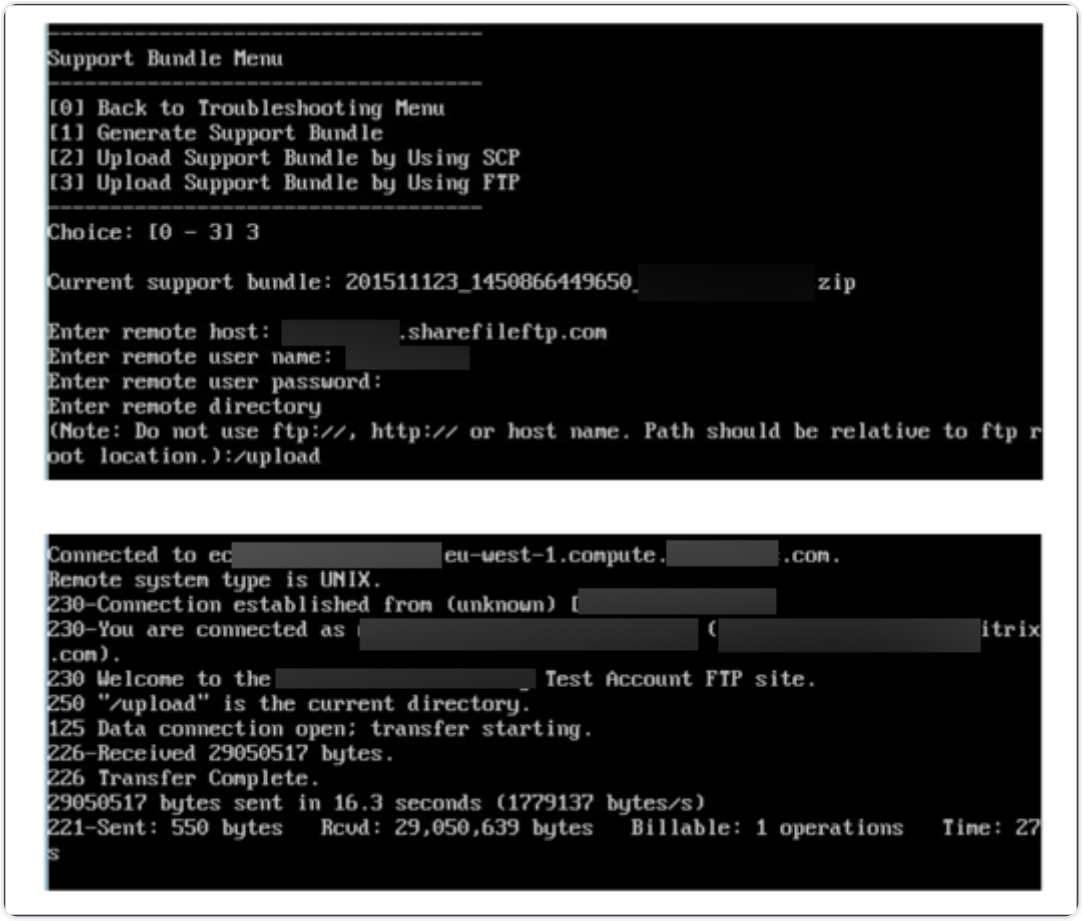
   a. **Upload Support Bundle by using FTP** を選択します。

   b. **リモートホストを入力してください:** プロンプトが表示されたら、FTPサーバー名を入力します。Citrix FilesをFTPサーバーとして使用する場合、会社名に続けてCitrix Files FTPサイト名を入力します。例：citrix.sharefileftp.com。

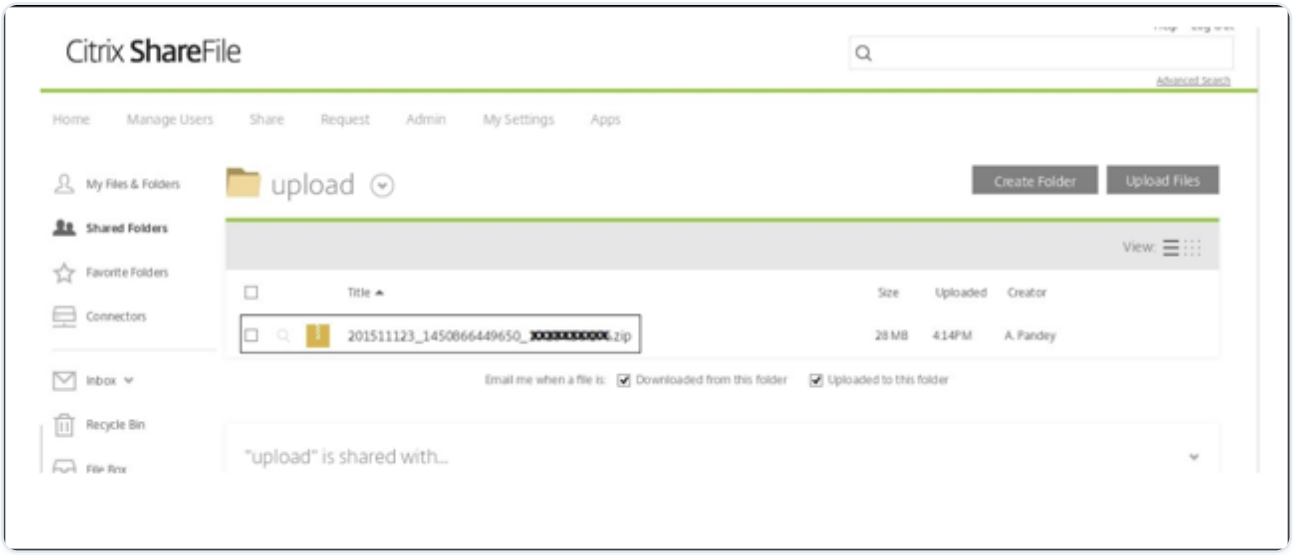
   c. **リモートユーザー名を入力してください:** プロンプトが表示されたら、英数字のユーザーIDを入力します。

   d. **リモートユーザーパスワードを入力:** プロンプトが表示されたら、パスワードを入力します。

   e. **リモートディレクトリを入力:** プロンプトが表示されたら、Citrix Filesで作成した共有フォルダー名を入力し、**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は、Citrix Filesで作成した共有フォルダーで表示できます。



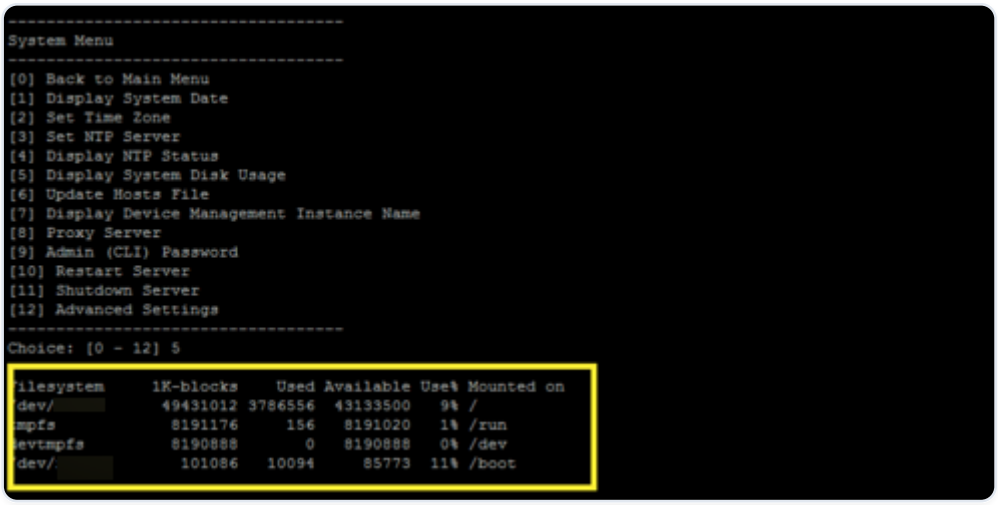
Citrix Files FTPの詳細については、こちらのCitrixサポート技術情報記事を参照してください。

ディスク領域を確認するには

CLIでシステムディスク領域を確認するには、次の手順を実行します。

1. メインメニューで、 メニューを選択します。
2. メニューで、 オプションを選択します。

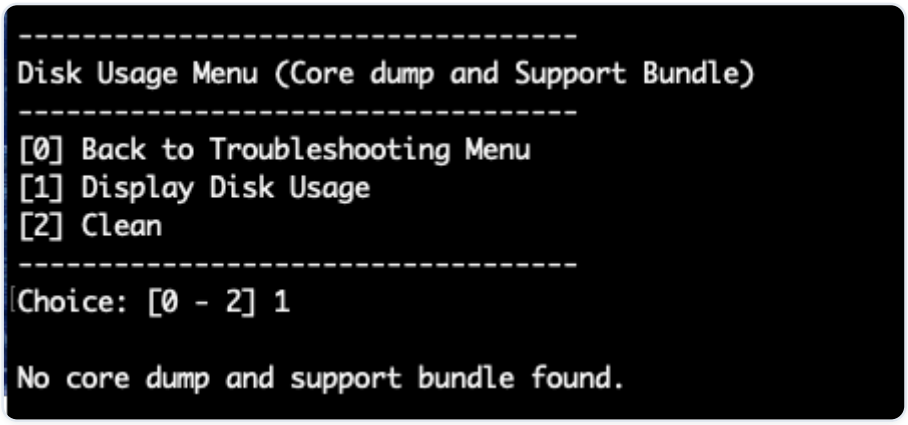
ファイルシステム情報が表示されます。



セルフサービスディスククリーンアップを実行するには

CLIでディスクをクリーンアップするには、次の手順を実行します。

1. メニューで、 を選択します。 リストには、次のオプションがあります。



2. 「1」と入力して、コアダンプファイルとサポートバンドルファイルの種類を一覧表示します。ファイルが存在しない場合は、次のメッセージが表示されます: **コアダンプとサポートバンドルは見つかりませんでした。**
3. 「2」と入力して、スキャンされたコアダンプファイルとサポートバンドルファイルをクリーンアップします。

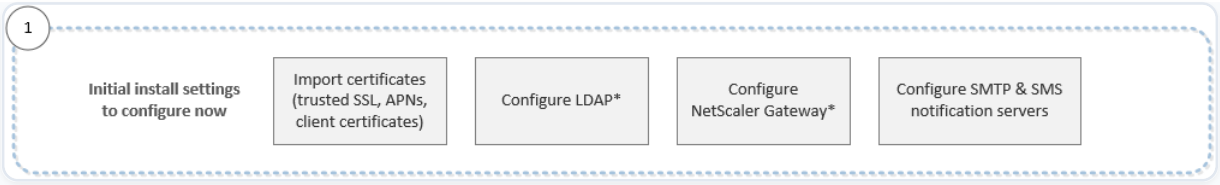
XenMobile® コンソールの開始ワークフロー

XenMobile コンソールは、XenMobile の統合管理ツールです。この記事は、XenMobile をインストール済みで、コンソールで作業する準備ができていることを前提としています。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サポートの詳細については、「XenMobile 互換性」の記事を参照してください。

初期設定ワークフロー

まずコマンドラインコンソールで、次に XenMobile コンソールで XenMobile の構成を完了すると、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。一部のインストール構成をスキップした場合でも、コンソールで次の設定を構成できます。ユーザー、アプリ、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検討してください。開始するには、コンソールの右上隅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。



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

- 認証
- シトリックス ゲートウェイとゼノモバイル
- 通知

Android、iOS、および Windows プラットフォームをサポートするには、次のアカウント関連の設定が必要です。

アンドロイド

- Google Play 資格情報を作成します。詳細については、「Google Play の起動」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。詳細については、「Android Enterprise」を参照してください。
- Google でドメイン名を検証します。詳細については、「Verify your domain for Google Workspace」を参照してください。
- Android Enterprise 用の API を有効にし、サービスアカウントを作成します。詳細については、「Android Enterprise Help」を参照してください。

iOS

- Apple ID と開発者アカウントを作成します。詳細については、Apple Developer Program Web サイトを参照してください。
- Apple Push Notification Service (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予定がある場合は、Apple APNs 証明書が必要です。Secure Mail 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 証明書の取得の詳細については、「Apple Push Certificates Portal」を参照してください。XenMobile と APNs の詳細については、「APNs certificates」および「Push Notifications for Secure Mail for iOS」を参照してください。
- ボリューム購入会社トークンを作成します。詳細については、「Apple Volume Purchasing Program」を参照してください。

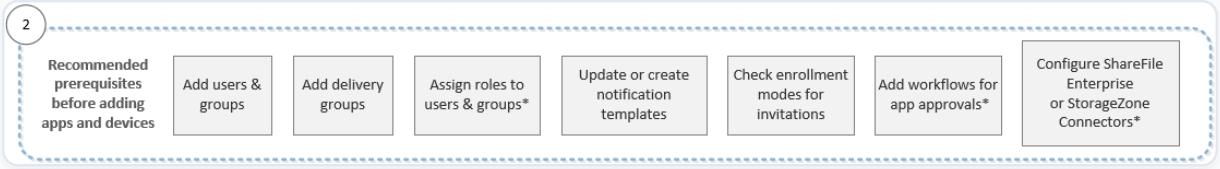
ウィンドウズ

- Microsoft Windows ストア開発者アカウントを作成します。詳細については、「Account types, locations, and fees」を参照してください。
- Microsoft Windows ストア発行元 ID を取得します。詳細については、「Manage account settings and profile info」を参照してください。
- Windows デバイスの登録に XenMobile AutoDiscovery を使用する予定がある場合は、公開 SSL 証明書が利用可能であることを確認してください。詳細については、「XenMobile AutoDiscovery Service」を参照してください。

コンソールの前提条件ワークフロー

このワークフローは、アプリ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。



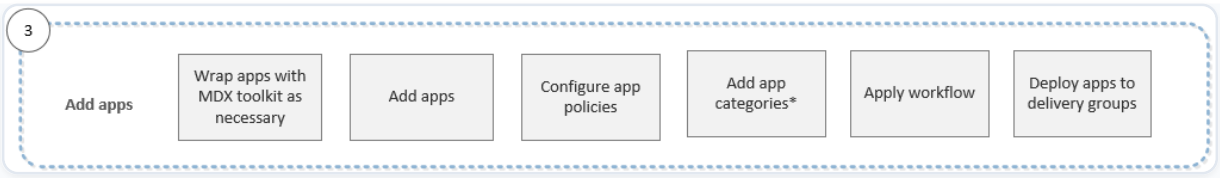
各設定の詳細と手順については、以下のCitrix製品ドキュメントの記事とセクションを参照してください。

- ユーザーアカウント、役割、および登録
- リソースの展開
- RBACによる役割の構成
- 通知
- ワークフローの適用
- ShareFileとXenMobileの併用

アプリ追加ワークフロー

このワークフローは、XenMobileにアプリを追加する際に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。



各設定の詳細と手順については、以下のCitrix製品ドキュメントの記事と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
- ワークフローの適用
- リソースの展開

デバイスの追加ワークフロー

このワークフローは、XenMobileにデバイスを追加および登録する際に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。

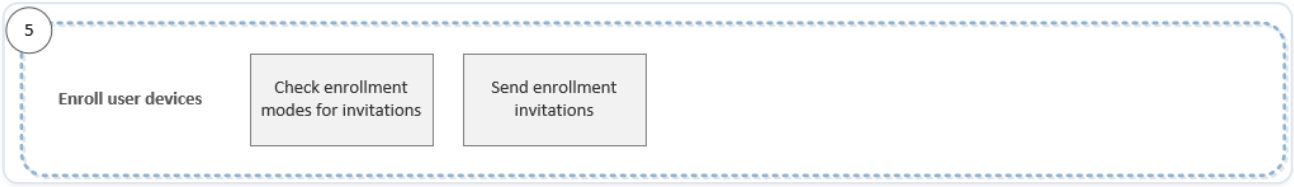


各設定の詳細と、段階的な手順については、以下のCitrix製品ドキュメントの記事とセクションを参照してください。

- デバイス
- 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
- リソースの展開
- 監視とサポート
- 自動化されたアクション

ユーザーデバイスの登録ワークフロー

このワークフローは、XenMobileにユーザーデバイスを登録する際に推奨される順序を示しています。



各設定の詳細と手順については、以下のCitrix製品ドキュメントの記事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

継続的なアプリとデバイスの管理ワークフロー

このワークフローは、コンソールで実行できるアプリとデバイスの管理アクティビティを示しています。

注:

アスタリスクが付いている項目はオプションです。



コンソールの右上隅にある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の詳細については、監視とサポートを参照してください。

証明書と認証

XenMobile® の操作中、認証にはいくつかのコンポーネントが関与します。

- **XenMobile Server:** XenMobile Server は、登録セキュリティと登録エクスペリエンスを定義する場所です。ユーザーをオンボーディングするためのオプションには、次のものがあります。
  - 登録をすべての人に公開するか、招待者のみにするか。
  - 2 要素認証または 3 要素認証を要求するかどうか。XenMobile のクライアントプロパティを通じて、Citrix PIN 認証を有効にし、PIN の複雑さと有効期限を設定できます。
- **Citrix ADC:** Citrix ADC は、マイクロ VPN SSL セッションの終端を提供します。Citrix ADC は、ネットワークの転送中の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ます。
- **Secure Hub:** Secure Hub と XenMobile Server は、登録操作で連携します。Secure Hub は、Citrix ADC と通信するデバイス上のエンティティです。セッションの有効期限が切れると、Secure Hub は Citrix ADC から認証チケットを取得し、そのチケットを MDX アプリに渡します。Citrix は、中間者攻撃を防ぐ証明書ピンニングを推奨しています。詳細については、Secure Hub の記事のこ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 は MDX セキュリティコンテナも促進します。Secure Hub はポリシーをプッシュし、アプリがタイムアウトしたときに Citrix ADC とセッションを作成し、MDX のタイムアウトと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も担当します。
- **MDX ポリシー:** MDX ポリシーは、デバイス上にデータボールトを作成します。MDX ポリシーは、マイクロ VPN 接続を Citrix ADC に戻し、オフラインモードの制限を適用し、タイムアウトなどのクライアントポリシーを適用します。

認証の構成に関する詳細情報（単一要素認証および二要素認証方法の概要を含む）については、展開ハンドブックの記事「認証」を参照してください。

XenMobile では、証明書を使用して安全な接続を作成し、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。その他の構成の詳細については、次の記事を参照してください。

- ドメインまたはドメインと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
- PKI エンティティ
- 資格情報プロバイダー
- APNs証明書
- Citrix FilesでのシングルサインオンSAML
- マイクロソフト アジュール アクティブ ディレクトリ サーバー設定
- Wi-Fiサーバーへの認証のためにデバイスに証明書を送信するには: Wi-Fiデバイスポリシー
- 認証に使用されない一意の証明書（内部ルート証明機関（CA）証明書など）または特定のポリシー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は、サーバーへの通信フローを保護するために、インストール中に自己署名Secure Sockets Layer（SSL）証明書を生成します。SSL証明書は、信頼できる既知のCAからのSSL証明書に置き換える必要があります。

XenMobileは、独自の公開鍵インフラストラクチャ（PKI）サービスを使用するか、クライアント証明書のためにCAから証明書を取得します。すべてのCitrix製品は、ワイルドカード証明書とサブジェクト代替名（SAN）証明書をサポートしています。ほとんどの展開では、2つのワイルドカード証明書またはSAN証明書のみが必要です。

クライアント証明書認証は、モバイルアプリにセキュリティの追加レイヤーを提供し、ユーザーがHDX™アプリにシームレスにアクセスできるようにします。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Citrix PINを入力して、XenMobile対応アプリへのシングルサインオン（SSO）アクセスを行います。Citrix PINは、ユーザー認証エクスペリエンスも簡素化します。Citrix PINは、クライアント証明書を保護したり、Active Directory資格情報をデバイスにローカルに保存したりするために使用されます。

XenMobileでiOSデバイスを登録および管理するには、Appleから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、「APNs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形式と種類を示しています。

XENMOBILE®サーバー

XENMOBILEコンポーネント	証明書形式	必要な証明書の種類
シトリックス ゲートウェイ	PEM (BASE64)、PFX (PKCS #12)	SSL、ルート (Citrix Gateway は PFX を PEM に自動的に変換します。)
XenMobile サーバー	.p12 (Windowsベースのコンピューターでは .pfx)	SSL、SAML、APNs (XenMobile はインストールプロセス中に完全な PKI を生成します。) 重要: XenMobile Server は .pem 拡張子の証明書をサポートしていません。 .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、ビット長が 4096、2048、1024 の SSL リスナー証明書とクライアント証明書をサポートしています。1024ビット証明書は簡単に侵害される可能性があります。

Citrix Gateway および XenMobile Server の場合、Citrix は Verisign、DigiCert、Thawte などの公開 CA からサーバー証明書を取得することを推奨しています。Citrix Gateway または XenMobile 構成ユーティリティから証明書署名要求 (CSR) を作成できます。CSR を作成したら、署名のために CA に提出します。CA が署名済み証明書を返したら、その証明書を Citrix Gateway または XenMobile にインストールできます。

> **重要: iOS、iPadOS、および macOS での信頼された証明書の要件**

> Apple は TLS サーバー証明書に関する新しい要件を設けています。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てください。Apple の公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。

> Apple は TLS サーバー証明書の最大有効期間を短縮しています。この変更は、2020年9月以降に発行されたサーバー証明書にのみ影響します。Apple の公開情報 `<https://support.apple.com/ja-jp/HT211025>` 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、その内容の概要を含め、証明書テーブルにエントリを持ちます。証明書を必要とする PKI 統合コンポーネントを構成する場合、コンテキスト依存の基準を満たすサーバー証明書を選択します。たとえば、XenMobile を Microsoft 証明機関 (CA) と統合するように構成したい場合があります。Microsoft CA への接続は、クライアント証明書を使用して認証する必要があります。

このセクションでは、証明書をアップロードするための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、および構成の詳細については、「クライアント証明書または証明書とドメイン認証」を参照してください。

秘密鍵の要件

XenMobileは、特定の証明書の秘密鍵を所有している場合と所有していない場合があります。同様に、XenMobileは、アップロードされた証明書に秘密鍵を必要とする場合と必要としない場合があります。

証明書のアップロード

証明書をアップロードするには、次の2つのオプションがあります。

- 証明書をコンソールに個別にアップロードします。
- REST APIを使用して、iOSデバイスに証明書を一括アップロードします。

証明書をコンソールに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します。次に、PKCS #12形式をアップロードする場合を除き、インストールするキーストアリポジトリ内のエントリを特定します。
- クリックして証明書をインポートします。

CAが要求の署名に使用するCA証明書（秘密鍵なし）をアップロードできます。また、クライアント認証用のSSLクライアント証明書（秘密鍵あり）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ときに、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リストから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ときに、XenMobileが秘密鍵を所有するすべてのサーバー証明書のリストから選択できます。

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、複数のエントリを含めることができます。したがって、キーストアからロードするときは、ロードするエントリを識別するエントリアリアスを指定するように求められます。エイリアスを指定しない場合、ストアの最初のエ

ントリがロードされます。PKCS #12ファイルには通常1つのエントリしか含まれていないため、キーストアタイプとしてPKCS #12を選択しても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、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **Certificates**をクリックします。**Certificates**ページが表示されます。

   証明書構成ページ(/en-us/xenmobile/server/media/settings-certificates-with-status.png)
3. **Import**をクリックします。**Import**ダイアログボックスが表示されます。
4. 次の設定を構成します。

   - **インポート:** リストで、**Keystore**をクリックします。**Import**ダイアログボックスが、利用可能なキーストアオプションを反映するように変更されます。

   証明書構成ページ(/en-us/xenmobile/server/media/settings-certificates-import-keystore.png)

   - **キーストアの種類:** リストで、**PKCS #12**をクリックします。
   - **用途:** リストで、証明書の使用方法をクリックします。利用可能なオプションは次のとおりです。

     - **サーバー**。サーバー証明書は、XenMobile Serverによって機能的に使用され、XenMobile Webコンソールにアップロードされる証明書です。これには、CA証明書、RA証明書、およびインフラストラクチャの他のコンポーネントとのクライアント認証用の証明書が含まれます。さらに、サーバー証明書を、デバイスに展開する証明書のストレージとして使用できます。この用途は、特にデバイスで信頼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) 認証により、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からのAPNs証明書は、Apple Push Networkを介したモバイルデバイス管理を可能にします。
     - **SSLリスナー**。Secure Sockets Layer (SSL) リスナーは、SSL暗号化アクティビティをXenMobileに通知します。

   - **キーストアファイル:** インポートするキーストアファイル（.p12タイプ、またはWindowsベースのコンピューターでは.pfx）を参照して見つけます。
   - **パスワード:** 証明書に割り当てられているパスワードを入力します。
   - **説明:** オプションで、他のキーストアと区別するために、キーストアの説明を入力します。
5. 「**インポート**」をクリックします。キーストアが証明書テーブルに追加されます。

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、XenMobile は入力から証明書チェーンを構築しようとします。XenMobile は、そのチェーン内のすべての証明書をインポートし、それぞれに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内の証明書がチェーンを形成している場合にのみ機能します。たとえば、チェーン内の後続の各証明書が前の証明書の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の説明を追加できます。説明は、チェーン内の最初の証明書にのみ添付されます。残りの証明書の説明は後で更新できます。

1. XenMobile コンソールで、コンソールの右上隅にある歯車アイコンをクリックし、次に「**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表示されます。
3. 「**インポート**」ダイアログボックスの「**インポート**」で、まだ選択されていない場合は、「**証明書**」をクリックします。
4. 「**インポート**」ダイアログボックスが、利用可能な証明書オプションを反映するように変更されます。「**用途**」で、キーストアの使用方法を選択します。利用可能なオプションは次のとおりです。

    - 「**サーバー**」。サーバー証明書は、XenMobile Server が機能的に使用する証明書で、XenMobile Web コンソールにアップロードされます。これには、CA 証明書、RA 証明書、およびインフラストラクチャの他のコンポーネントとのクライアント認証用の証明書が含まれます。さらに、サーバー証明書をデバイスに展開する証明書のストレージとして使用できます。このオプションは、特にデバイスで信頼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) 認証により、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 (SSO) アクセスを提供できます。
    - 「**SSL リスナー**」。Secure Sockets Layer (SSL) リスナーは、SSL 暗号化アクティビティを XenMobile に通知します。

5. インポートするキーストアを、ファイルの種類が .p12 (Windows ベースのコンピューターでは .pfx) のものから参照して見つけます。
6. 証明書用のオプションの秘密鍵ファイルを参照して見つけます。秘密鍵は、証明書とともに暗号化と復号化に使用されます。
7. 必要に応じて、他の証明書と区別できるように、証明書の説明を入力します。
8. 「**インポート**」をクリックします。証明書が証明書テーブルに追加されます。

REST API を使用して iOS デバイスに証明書を一括アップロードする

証明書を1つずつアップロードするのが実用的でない場合は、REST API を使用して iOS デバイスに一括アップロードできます。この方法では、.p12 形式の証明書がサポートされています。REST API の詳細については、「REST API」を参照してください。

1. 各証明書ファイルを `device_identity_value.p12` の形式で名前変更します。`device_identity_value` は、各デバイスの IMEI、シリアル番号、または MEID にすることができます。

   例として、識別方法としてシリアル番号を使用することを選択したとします。あるデバイスのシリアル番号が `A12BC3D4EFGH` である場合、そのデバイスにインストールする証明書ファイルの名前を `A12BC3D4EFGH.p12` にします。

2. .p12 証明書のパスワードを保存するテキストファイルを作成します。そのファイルに、各デバイスのデバイス識別子とパスワードを新しい行に入力します。`device_identity_value=password` の形式を使用します。以下を参照してください。

   ```
   A12BC3D4EFGH.p12=password1!

   A12BC3D4EFIJ.p12=password2@

   A12BC3D4EFKL.p12=password3#
   ```

3. 作成したすべての証明書とテキストファイルを .zip ファイルにまとめます。
4. REST API クライアントを起動し、XenMobile にログインして、認証トークンを取得します。
5. メッセージ本文に以下を記述して、証明書をインポートします。

   ```
   {

       "alias": "",

       "useAs": "device",

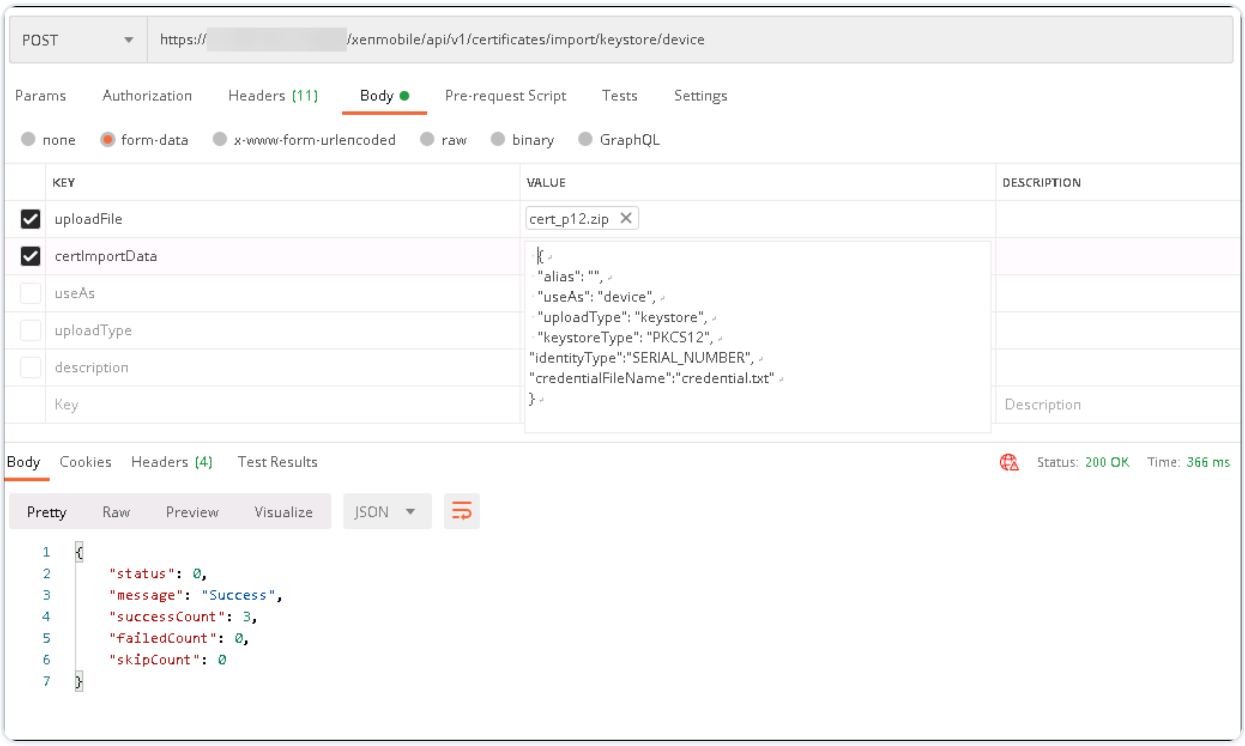
       "uploadType": "keystore",

       "keystoreType": "PKCS12",

       "identityType":"SERIAL_NUMBER",        # identity type can be
   "SERIAL_NUMBER","IMEI","MEID"
   ```

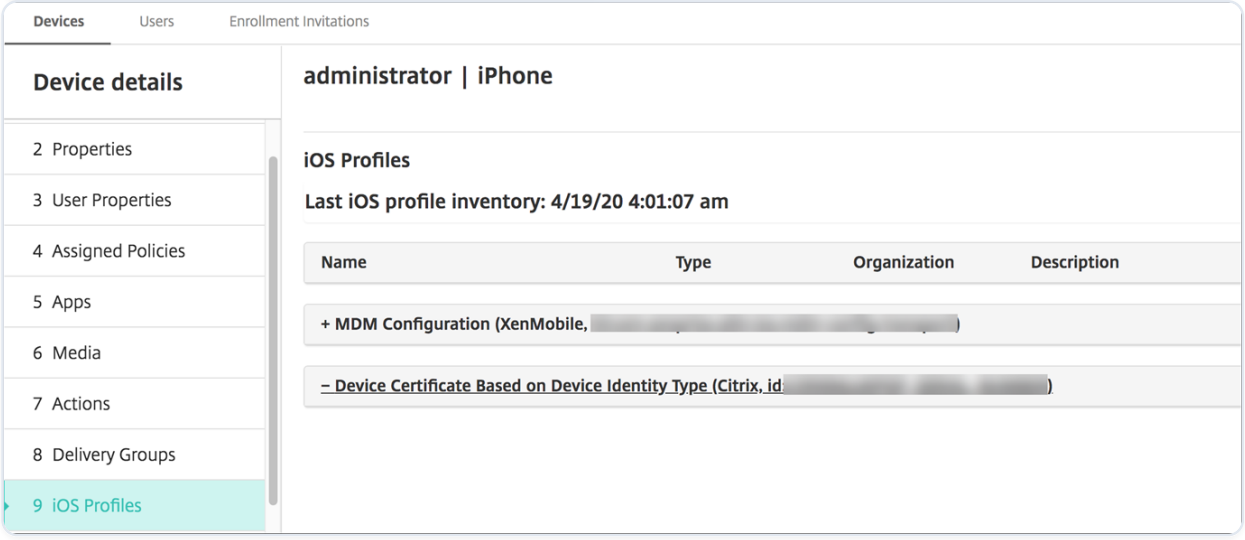
```
    "credentialFileName":"credential.txt"   # The credential file name
in .zip

}
```



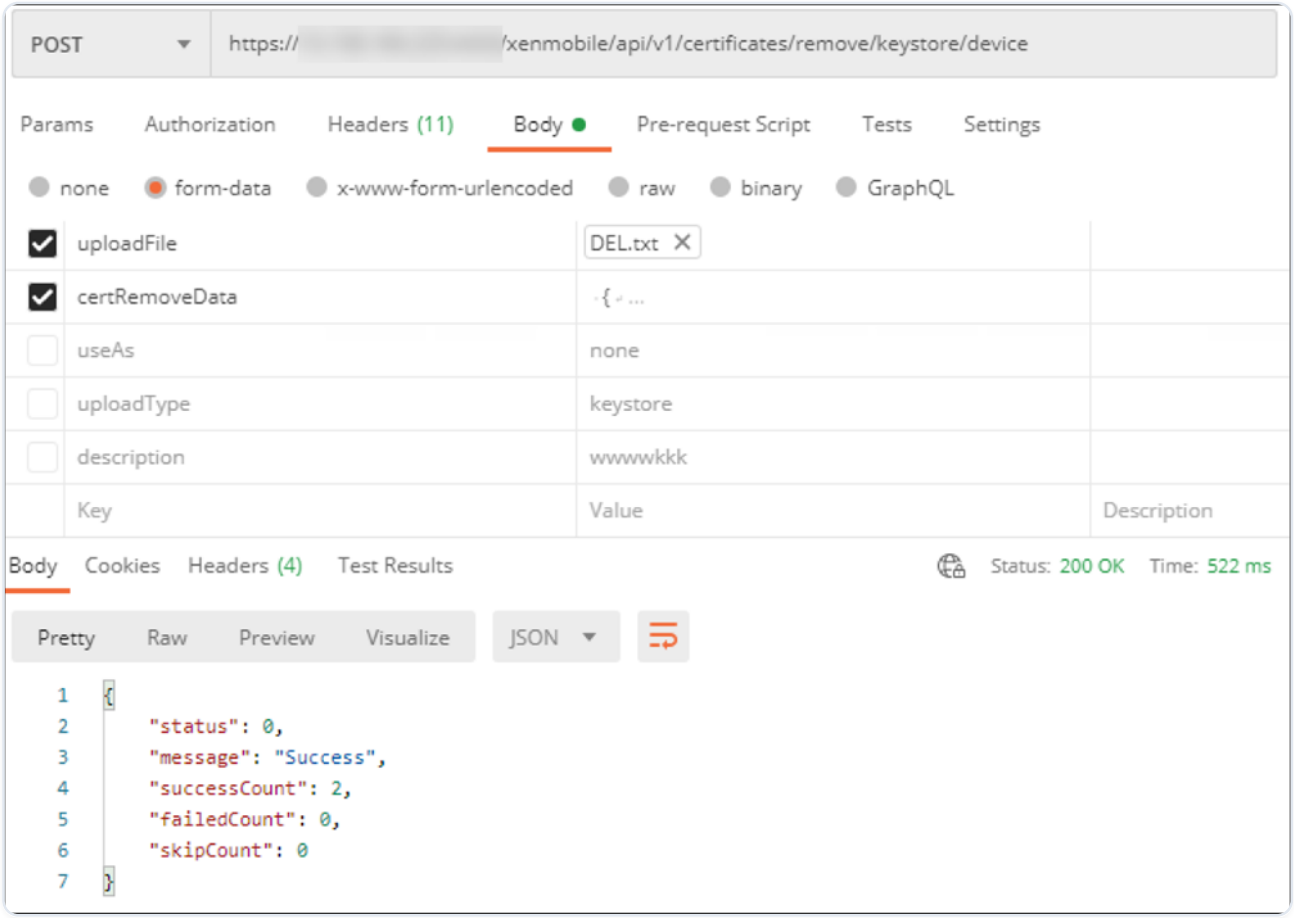
6. 資格情報タイプを **Always on IKEv2**、デバイス認証方法を **Device Certificate Based on Device Identity** に設定して VPN ポリシーを作成します。証明書ファイル名で使用した **Device identity type** を選択します。「VPN デバイスポリシー」を参照してください。
7. iOS デバイスを登録し、VPN ポリシーが展開されるのを待ちます。デバイスの MDM 構成を確認して、証明書のインストールを確認します。XenMobile コンソールでデバイスの詳細を確認することもできます。


12:08
Profile
MDM Configuration
MOBILE DEVICE MANAGEMENT
DEVICE IDENTITY CERTIFICATE
XenMobile MDM
Issued by: Devices Certificate Authority
Expires: April 17, 2022
CERTIFICATES (4)
Root Certificate Authority
Issued by: Root Certificate Authority
Expires: February 18, 2038
DigiCert SHA2 Secure Server CA
Issued by: DigiCert Global Root CA
Expires: March 8, 2023
DigiCert Global Root CA
Issued by: DigiCert Global Root CA
Expires: November 10, 2031
cem user02
Issued by:
Expires: February 25, 2021
SIGNING CERTIFICATE


Devices
Users
Enrollment Invitations
Device details
administrator | iPhone
2 Properties
3 User Properties
4 Assigned Policies
5 Apps
6 Media
7 Actions
8 Delivery Groups
9 iOS Profiles
iOS Profiles
Last iOS profile inventory: 4/19/20 4:01:07 am
Name
Type
Organization
Description
+ MDM Configuration (XenMobile,
– Device Certificate Based on Device Identity Type (Citrix, id

削除する各証明書について `device_identity_value` をリストしたテキストファイルを作成することで、証明書を一括削除することもできます。REST API で、削除 API を呼び出し、`device_identity_value` を適切な識別子に置き換えて、次のリクエストを使用します。

```
{
    "identityType"="device_identity_value"
}
```



証明書の更新

XenMobileでは、システム内に同時に存在する公開キーあたりの証明書は1つのみです。すで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と、既存のエントリを置き換えるか、エントリを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果的に更新するには、次の手順を実行します。コンソールの右上隅にある歯車アイコンをクリックして、 ページを開き、 をクリックします。 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は自動的に新しい証明書を使用するように切り替わります。同様に、デバイスにサーバー証明書を展開している場合、証明書は次回の展開時に自動的に更新されます。

証明書の更新

XenMobile Serverは、PKI用に内部で次の証明機関を使用します: Root CA、device CA、および server CA。これらのCAは論理グループとして分類され、グループ名が提供されます。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、「default」というグループ名が付けられます。

サポートされているiOS、macOS、およびAndroidデバイスのCAは、XenMobile Serverコンソールまたは公開REST APIを使用して更新できます。登録済みのWindowsデバイスの場合、ユーザーは新しいdevice CAを受け取るためにデバイスを再登録する必要があります。

XenMobile Server内の内部PKI CAs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ために、次のAPIが利用可能です。

- グループ証明機関 (CA) を作成します。
- 新しいCAをアクティブ化し、古いCAを非アクティブ化します。
- 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。すでに登録されているデバイスは中断なく動作し続けます。デバイスがサーバーに再接続すると、デバイス証明書が発行されます。
- 古いCAをまだ使用しているデバイスのリストを返します。
- すべてのデバイスが新しいCAを持つようになったら、古いCAを削除します。

詳細については、Public API for REST Services PDFの次のセクションを参照してください。

- セクション 3.16.58、デバイス証明書の更新
- セクション 3.23、内部 PKI CA グループ

デバイスの管理コンソールには、デバイスの登録証明書を更新するために使用されるセキュリティアクション**証明書の更新**が含まれています。

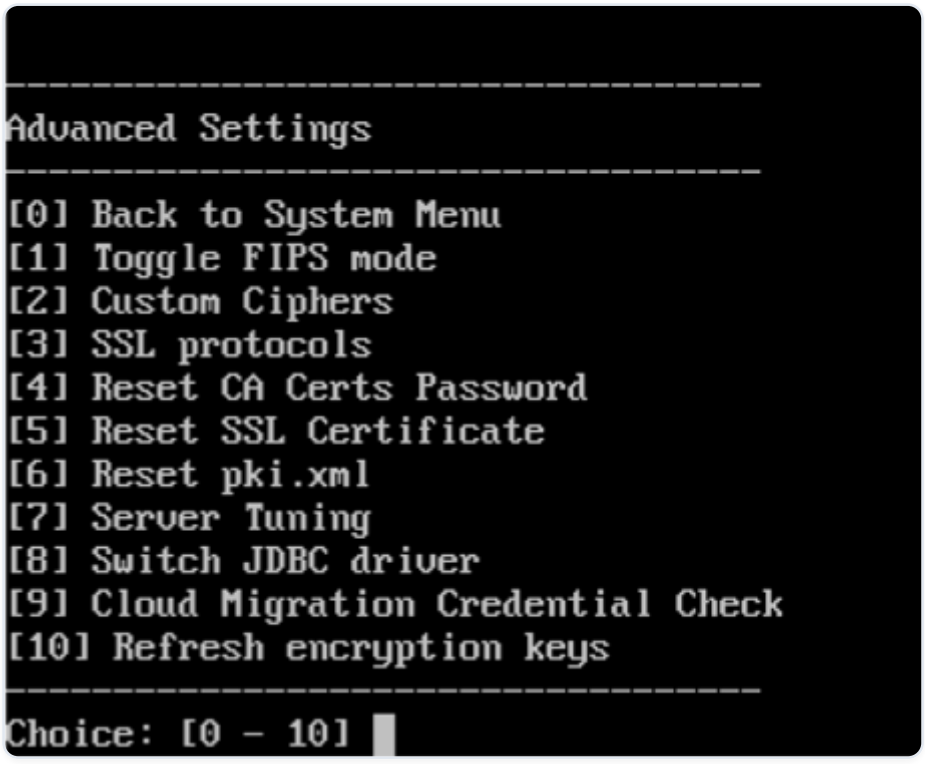
前提条件

- デフォルトでは、この証明書更新機能は無効になっています。証明書更新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:**
>
> Citrix ADCがSSLオフロード用に設定されている場合、新しい証明書を生成する際は、ロードバランサーを新しいcacert.permで更新してください。Citrix Gatewayの設定の詳細については、「NetScaler VIPsでSSLオフロードモードを使用するには」を参照してください。

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

XenMobile Serverノードでサーバー CA証明書を生成した後、XenMobile CLIを使用して他のクラスターノードの証明書パスワードをリセットします。CLIメインメニューから、**System > Advanced Settings > Reset CA certs password**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証明書管理

XenMobile展開で使用する証明書、特にその有効期限と関連するパスワードを一覧表示することをお勧めします。このセクションは、XenMobileでの証明書管理を容易にするためのものです。

お使いの環境には、以下の証明書の一部またはすべてが含まれている場合があります。

- ゼンモバイル サーバー
  - MDM FQDN用SSL証明書
  - SAML証明書 (Citrix Files用)
  - 前述の証明書およびその他の内部リソース (StoreFront/プロキシなど) 用のルートおよび中間CA証明書
  - iOSデバイス管理用APN証明書
  - XenMobile Server Secure Hub通知用内部APNs証明書
  - PKIへの接続用PKIユーザー証明書
- MDX ツールキット
  - Apple開発者証明書
  - 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

  MAM SDKはアプリをラップしないため、証明書は不要です。
- シトリックス エーディーシー
  - MDM FQDN用SSL証明書
  - Gateway FQDN用SSL証明書
  - ShareFile SZC FQDN用SSL証明書
  - Exchange負荷分散用SSL証明書 (オフロード構成)
  - StoreFront ロードバランシング用 SSL 証明書
  - 前述の証明書用のルートおよび中間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、その証明書は無効になります。環境で安全なトランザクションを実行できなくなり、XenMobileリソースにアクセスできなくなります。

> **注：**

> 認証局（CA）は、有効期限が切れる前にSSL証明書を更新するよう促します。

Citrix Secure Mail 用 APNs 証明書

Apple Push Notification Service (APNs) 証明書は毎年期限切れになります。証明書の有効期限が切れる前に、APNs SSL 証明書を作成し、Citrix ポータルで更新してください。証明書の有効期限が切れると、ユーザーはSecure Mailのプッシュ通知に一貫性の問題が生じます。また、アプリのプッシュ通知を送信できなくなります。

iOSデバイス管理用 APNs 証明書

XenMobile で iOS デバイスを登録および管理するには、Apple から APNs 証明書を設定および作成します。証明書の有効期限が切れると、ユーザーは XenMobile に登録できなくなり、iOS デバイスを管理できなくなります。詳細については、「APNs 証明書」を参照してください。

Apple Push Certificates Portal にログオンすると、APNs 証明書のステータスと有効期限を表示できます。証明書を作成したのと同じユーザーとしてログオンしてください。

また、有効期限の30日前と10日前にAppleからメール通知が届きます。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デバイスで実行されるアプリ（Apple App Storeのアプリを除く）には、次の署名要件があります。

- プロビジョニングプロファイルでアプリに署名します。
- アプリに、対応する配布証明書を使用して署名します。

有効なiOS配布証明書があることを確認するには、次の手順を実行します。

1. Apple Enterprise Developerポータルから、MDX Toolkitでラップする予定の各アプリに対して明示的なApp IDを作成します。許容されるApp IDの例は次のとおりです: `com.CompanyName.ProductName`。
2. Apple Enterprise Developerポータルから、**Provisioning Profiles > Distribution**に移動し、社内プロビジョニングプロファイルを作成します。前の手順で作成した各App IDに対して、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。詳細については、「Wrapping iOS Mobile Apps」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、次の手順を実行します。

1. XenMobileコンソールで、**Settings > Certificates**をクリックします。
2. APNs、SSLリスナー、ルート、および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ます。

Androidキーストア

キーストアは、Androidアプリの署名に使用される証明書を含むファイルです。キーの有効期間が期限切れになると、ユーザーは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。

シトリックス エーディーシー

Citrix ADCの証明書の有効期限の処理方法の詳細については、Citrixサポート技術情報センターの「How to handle certificate expiry on NetScaler」を参照してください。

期限切れのCitrix ADC証明書は、ユーザーが登録してStoreにアクセスするのを妨げます。期限切れの証明書は、Secure Mailを使用しているときにユーザーがExchange Serverに接続するのも妨げます。さらに、ユーザーはHDXアプリを列挙して開くことができません（どの証明書が期限切れになったかによります）。

Expiry MonitorとCommand Centerは、Citrix ADC証明書を追跡するのに役立ちます。証明書の有効期限が切れると、センターから通知されます。これらのツールは、次のCitrix ADC証明書を監視するのに役立ちます。

- MDM FQDN用SSL証明書
- ゲートウェイFQDN用SSL証明書
- ShareFile SZC FQDN用SSL証明書
- Exchange負荷分散用SSL証明書 (オフロード構成)
- StoreFront負荷分散用SSL証明書
- 前述の証明書用のルートおよび中間CA証明書

シトリックス ゲートウェイ と XenMobile®

XenMobile を使用して Citrix Gateway を構成すると、内部ネットワークへのリモートデバイスアクセス用の認証メカニズムが確立されます。この機能により、モバイルデバイス上のアプリがイントラネット内の企業サーバーにアクセスできるようになります。XenMobile は、デバイス上のアプリから Citrix Gateway へのマイクロ VPN を作成します。

XenMobile で使用するために Citrix Gateway を構成するには、XenMobile からスクリプトをエクスポートし、そのスクリプトを Citrix Gateway で実行します。

Citrix Gateway 構成スクリプトを使用するための前提条件

Citrix ADC の要件:

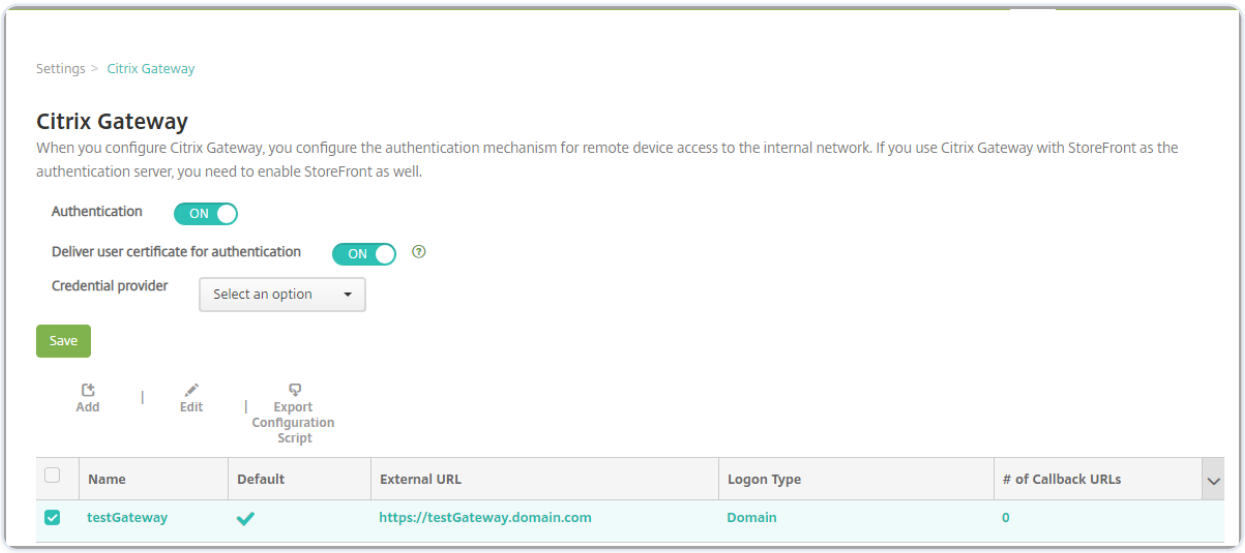
- Citrix ADC (最小バージョン 11.0、ビルド 70.12)。
- Citrix ADC の IP アドレスが構成されており、LDAP サーバーへの接続があること (LDAP がロードバランスされている場合を除く)。
- Citrix ADC サブネット (SNIP) IP アドレスが構成されており、必要なバックエンドサーバーへの接続があり、ポート 8443/TCP 経由でパブリックネットワークアクセスがあること。
- DNS がパブリックドメインを解決できること。
- Citrix ADC が Platform/Universal または Trial ライセンスでライセンスされていること。詳しくは、`<https://support.citrix.com/article/CTX126049>` を参照してください。
- Citrix Gateway SSL 証明書が Citrix ADC にアップロードされ、インストールされていること。詳しくは、`<https://support.citrix.com/article/CTX136023>` を参照してください。

XenMobile の要件:

- XenMobile Server (最小バージョン 10.6)。
- LDAP サーバーが構成されていること。

内部ネットワークへのリモートデバイスアクセス用の認証を構成する

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. 「**サーバー**」の下にある「**Citrix Gateway**」をクリックします。「**Citrix Gateway**」ページが表示されます。次の例では、Citrix Gatewayインスタンスが存在します。



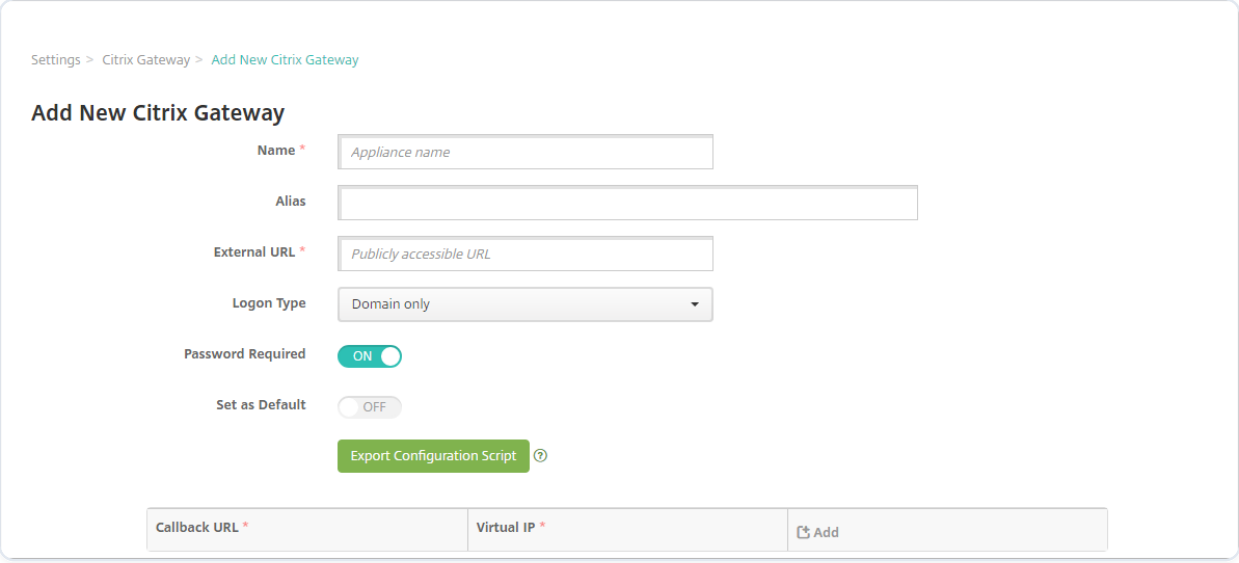
3. これらの設定を構成します。
   - **認証**：認証を有効にするかどうかを選択します。デフォルトは「**ON**」です。
   - **認証用のユーザー証明書を配信**：XenMobileが認証証明書をSecure Hubと共有して、Citrix Gatewayがクライアント証明書認証を処理できるようにするかどうかを選択します。デフォルトは「**OFF**」です。
   - **資格情報プロバイダー**：リストから使用する資格情報プロバイダーをクリックします。詳しくは、「資格情報プロバイダー」を参照してください。
4. 「**保存**」をクリックします。

Citrix Gatewayインスタンスを追加する

認証設定を保存した後、XenMobileにCitrix Gatewayインスタンスを追加します。

1. XenMobileコンソールで、コンソールの右上隅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。

2. 「**サーバー**」の下にある「**Citrix Gateway**」をクリックします。「**Citrix Gateway**」ページが表示されます。
3. 「**追加**」をクリックします。「**新しいCitrix Gatewayの追加**」ページが表示されます。



4. これらの設定を構成します。

   - **名前:** Citrix 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、Citrix Gatewayのエイリアス名を含めます。
   - **外部URL:** Citrix Gatewayの公開アクセス可能なURLを入力します。例: `https://receiver.com`.
   - **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**、**ドメインとセキュリティトークン**、**証明書**、**証明書とドメイン**、**証明書とセキュリティトークン**があります。**ログオンの種類**で選択した内容に基づいて、**パスワード必須**フィールドのデフォルト設定が変更されます。デフォルトは**ドメインのみ**です。

   複数のドメインがある場合は、**証明書とドメイン**を使用します。XenMobileとCitrix Gatewayでの複数ドメイン認証の構成について詳しくは、「複数ドメインの認証を構成する」を参照してください。

   証明書とセキュリティトークンを使用する場合、Secure Hubをサポートするために Citrix Gatewayで追加の構成が必要です。詳しくは、「証明書とセキュリティトークン認証用にXenMobileを構成する」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。

   - **パスワード必須:** パスワード認証を必須にするかどうかを選択します。デフォルトは、選択した**ログオンの種類**によって異なります。

- **デフォルトとして設定:** このCitrix 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:** ボタンをクリックして、Citrix Gatewayにアップロードしてから XenMobile設定で構成する構成バンドルをエクスポートします。詳しくは、これらの手順の後に「オンプレミスのCitrix GatewayをXenMobile Serverで使用するように構成する」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とCitrix Gateway VPN仮想IPを追加する」を参照してください。

5. **保存**をクリックします。

   新しいCitrix Gatewayが追加され、テーブルに表示されます。インスタンスを編集または削除するには、リスト内の名前をクリックします。

XenMobile Serverで使用するためのCitrix Gatewayの構成

オンプレミスのCitrix GatewayをXenMobileで使用するように構成するには、この記事で詳しく説明されている次の一般的な手順を実行します。

1. XenMobile Server からスクリプトと関連ファイルをダウンロードします。スクリプトに付属の readme ファイルで、最新の詳細な手順を確認してください。
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. Citrix ADC でスクリプトを実行します。
5. 構成をテストします。

スクリプトは、XenMobile で必要となる以下の Citrix Gateway 設定を構成します。

- MDM および MAM に必要な Citrix Gateway 仮想サーバー
- Citrix Gateway 仮想サーバーのセッションポリシー
- XenMobile Server の詳細
- Citrix Gateway 仮想サーバーの認証ポリシーとアクション。 スクリプトは LDAP 構成設定について説明します。
- 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
- Citrix ADC の静的ローカル DNS レコード

- その他のバインディング: サービスポリシー、CA 証明書

スクリプトは以下の構成を処理しません。

- Exchange ロードバランシング
- Citrix Files ロードバランシング
- 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. Citrix Gateway を追加する場合は、**Add New Citrix Gateway** ページで **Export Configuration Script** をクリックします。

   Citrix Gateway 構成画面(/en-us/xenmobile/server/media/settings-citrix-gateway-add.png)

   または、Citrix Gateway インスタンスを追加し、スクリプトをエクスポートする前に **Save** をクリックした場合は、**Settings > Citrix Gateway** に戻り、Citrix ADC を選択し、**Export Configuration Script** をクリックしてから、**Download** をクリックします。

   Citrix Gateway 構成画面(/en-us/xenmobile/server/media/settings-citrix-gateway-added.png)

   Export Configuration Script をクリックすると、XenMobile は .tar.gz スクリプトバンドルを作成します。スクリプトバンドルには以下が含まれます。

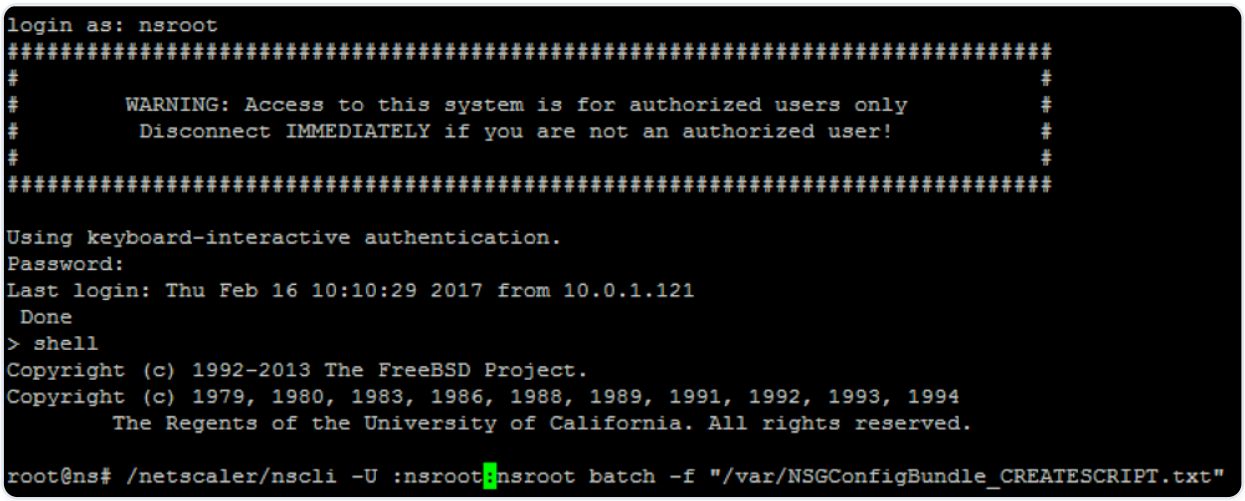
   - 詳細な手順が記載された Readme ファイル
   - Citrix ADC で必要なコンポーネントを構成するために使用される Citrix ADC CLI コマンドを含むスクリプト
   - XenMobile Server のパブリックルートCA証明書および中間CA証明書（これらの証明書はSSLオフロード用であり、現在のリリースでは不要です）
   - Citrix ADC 構成を削除するために使用される Citrix ADC CLI コマンドを含むスクリプト

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詳細に置き換えます。

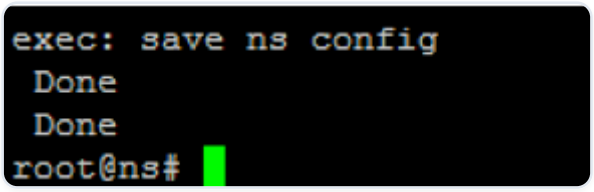
```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard o
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ている readme ファイルの説明に従って、編集したスクリプトを Citrix ADC bash シェルで実行します。例：

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

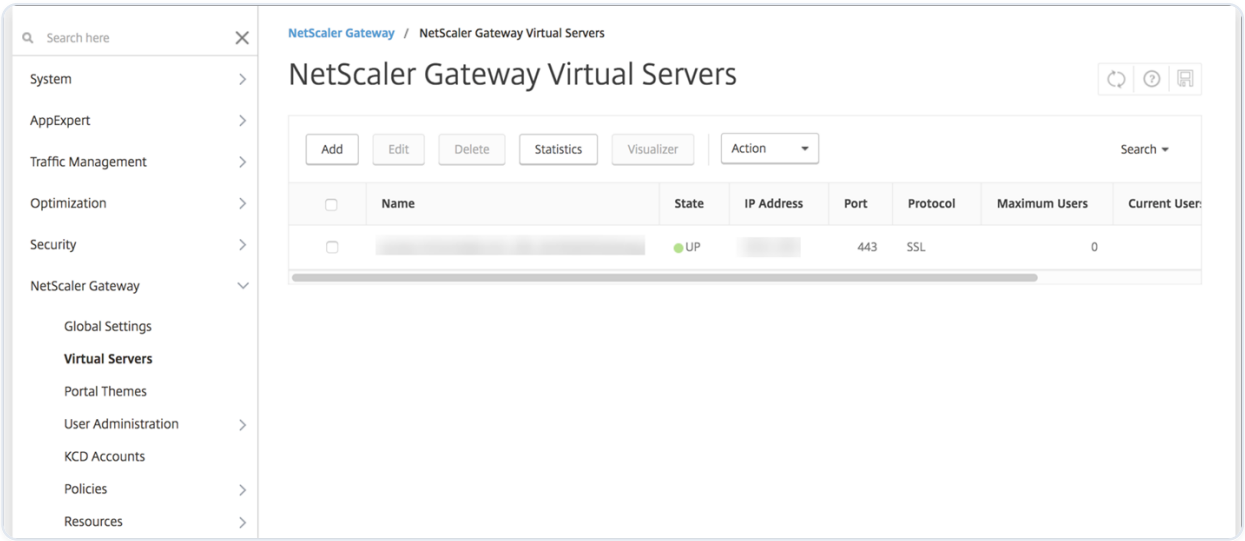


スクリプトが完了すると、次の行が表示されます。

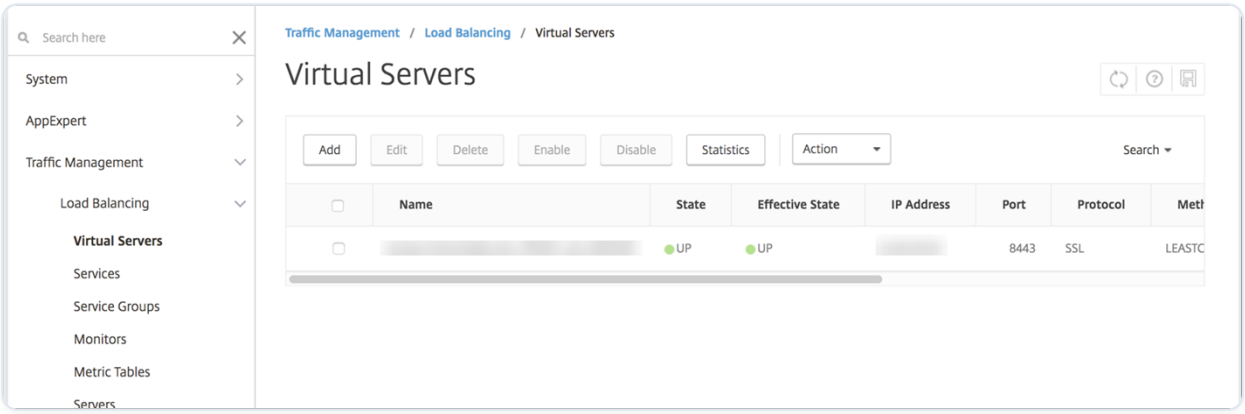


構成をテストする

1. Citrix Gateway Virtual Server の状態が **UP** と表示されていることを確認します。



2. プロキシ負荷分散仮想サーバーの状態が **UP** と表示されていることを確認します。



3. Web ブラウザーを開き、Citrix Gateway URL に接続して、認証を試行します。認証に失敗すると、次のメッセージが表示されます：HTTP Status 404 - Not Found
4. デバイスを登録し、MDM と MAM の両方に登録されていることを確認します。

コールバック URL と Citrix Gateway VPN 仮想 IP を追加する

Citrix Gateway インスタンスを追加した後、コールバック URL を追加し、Citrix Gateway 仮想 IP アドレスを指定できます。これらの設定はオプションですが、特に XenMobile Server が DMZ にある場合に、セキュリティを強化するために構成できます。

1. **設定 > Citrix Gateway**で、Citrix Gatewayを選択し、**編集**をクリックします。
2. テーブルで、**追加**をクリックします。
3. **コールバックURL**には、完全修飾ドメイン名（FQDN）を入力します。コールバックURLは、要求がCitrix Gatewayから発信されたことを検証します。

   コールバックURLがXenMobile Serverから到達可能なIPアドレスに解決されることを確認してください。コールバックURLは、外部のCitrix Gateway URLまたはその他のURLにすることができます。
4. Citrix Gatewayの**仮想IP**アドレスを入力し、**保存**をクリックします。

複数ドメインの認証を構成する

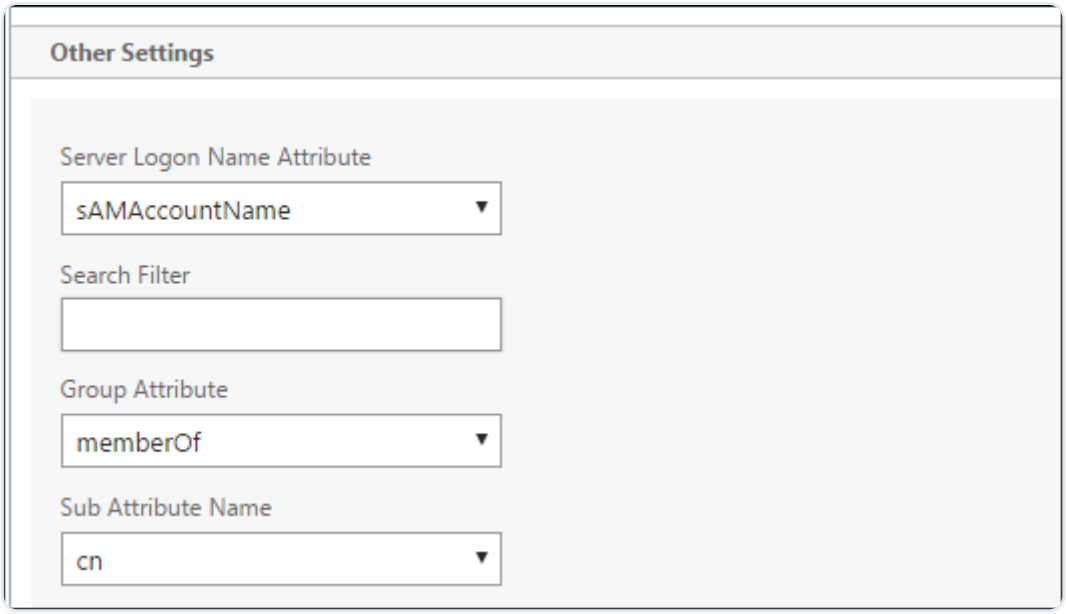
テスト、開発、本番環境など、複数のXenMobile Serverインスタンスがある場合は、追加の環境に対してCitrix Gatewayを手動で構成します（Citrix ADC for XenMobileウィザードは1回しか使用できません）。

Citrix Gatewayの構成

複数ドメイン環境のCitrix 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. Citrix Gateway構成ユーティリティで、**構成**タブの**Citrix 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、**LDAP**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。指定した属性は、XenMobileコンソールでLDAP設定を構成する際に必要となるため、メモしておいてください。



4. 各LDAPポリシーに対してこれらの手順を繰り返します。各ドメインには個別のLDAPポリシーが必要です。
5. Citrix Gateway仮想サーバーにバインドされているセッションポリシーで、**セッションプロファイルの編集 > 公開アプリケーション**に移動します。**シングルサインオンドメイン**が空白であることを確認します。

XenMobile Serverの構成

複数ドメインのXenMobile環境でLDAPを構成するには、次の手順を実行します。

1. XenMobileコンソールで、**［Settings］>［LDAP］**の順に選択し、ディレクトリを追加または編集します。

   XenMobile LDAP設定画面(/en-us/xenmobile/server/media/ldap-settings-multiple-domains1.png)

2. 情報を入力します。

   - **［Domain Alias］**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、ドメイン間にスペースを使用しないでください。例：`domain1.com,domain2.com,domain3.com`
   - **［User search by］フィールドが、Citrix Gateway LDAPポリシーで指定されている［Server Logon Name Attribute］**と一致していることを確認します。

XenMobile LDAP設定画面(/en-us/xenmobile/server/media/ldap-settings-multiple-domains2.png)

特定のURLへの受信接続要求をドロップする

環境内のCitrix GatewayがSSLオフロード用に構成されている場合、特定のURLへの受信接続要求をゲートウェイでドロップするように設定できます。

追加のセキュリティを優先する場合は、Citrix Gatewayで2つのMDMロードバランサー仮想サーバー（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オフロード用に構成されたCitrix Gatewayにのみ適用されます。

1. `XMS_DropURLs`という名前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以下のURLを追加します。必要に応じてこのリスト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. 指定されたサブネットから接続要求が発信されない限り、これらのURLへのすべてのトラフィックを破棄するポリシーを作成します。

```
add responder policy XMS_DROP_pol
“CLIENT.IP.SRC.IN_SUBNET(192.168.0.0/24).NOT &&

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ロードバランサー仮想サーバー（ポート443および8443）にバインドします。

```
bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST


bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName XMS_DROP_pol
-priority 100 -gotoPriorityExpression END -type REQUEST
```

5. ブラウザ経由のMAM URLアクセスをブロックする

   ブラウザからMAM URLに直接アクセスすると、ユーザーはActive Directoryの資格情報を入力するように求められます。これはユーザーが資格情報を検証するためのツールとして機能しますが、一部のユーザーはこれをセキュリティ違反と見なす可能性があります。以下のセクションでは、NetScalerのResponder Policy機能を使用して、MAM URL（NetScaler® Gateway VIP）へのブラウザアクセスを制限する方法について説明します。

   次のいずれかのResponder Policyを作成し、NetScaler Gateway仮想サーバーにバインドします。

   - `add responder policy Resp_Brow_Pol "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"Mozilla\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`

- `add responder policy Resp_Brow_Pol_CR "!HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`
- `add responder policy Resp_Brow_Pol_CR "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT&&HTTP.REQ.URL.PATH_AND_QUERY.EQ(\"/vpn/index.html\")" DROP`

`bind vpn vserver _XM_XenMobileGateway -policy Resp_Brow_Pol_CR -priority 100 -gotoPriorityExpression END -type REQUEST`を使用してNetScaler Gateway仮想サーバーにバインドします

> **注:**
>
> `_XM_XenMobileGateway`は、NetScaler Gateway仮想サーバーの例の名前です。

ドメインまたはドメインとセキュリティトークン認証

XenMobile® は、Lightweight Directory Access Protocol (LDAP) に準拠した1つ以上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1つ以上のディレクトリへの接続を構成し、その LDAP 構成を使用してグループ、ユーザーアカウント、および関連プロパティをインポートできます。

LDAP は、インターネットプロトコル (IP) ネットワーク上で分散ディレクトリ情報サービスにアクセスし、維持するためのオープンソースでベンダーニュートラルなアプリケーションプロトコルです。ディレクトリ情報サービスは、ネットワーク全体で利用可能なユーザー、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 の一般的な使用法は、複数のサービス間で単一のパスワード (ユーザーごと) が共有される、ユーザー向けのシングルサインオン (SSO) を提供することです。シングルサインオンにより、ユーザーは会社のウェブサイトに一度ログオンするだけで、企業イントラネットへの認証済みアクセスが可能になります。

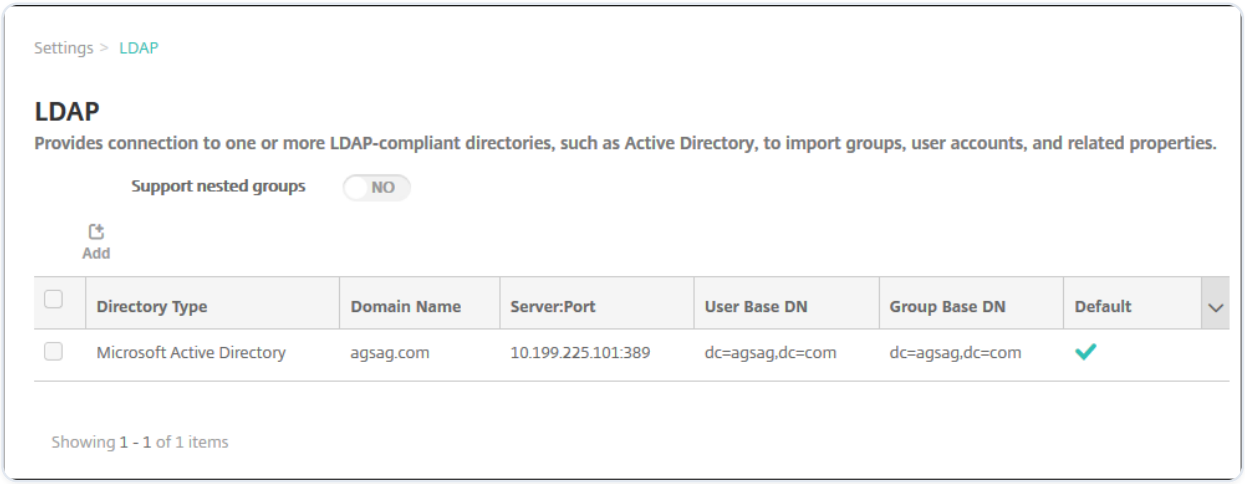
クライアントは、ディレクトリシステムエージェント (DSA) と呼ばれる LDAP サーバーに接続することで LDAP セッションを開始します。その後、クライアントはサーバーに操作リクエストを送信し、サーバーは適切な認証で応答します。

> **重要:**

> XenMobile では、ユーザーがデバイスを XenMobile に登録した後で、認証モードをドメイン認証から別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。

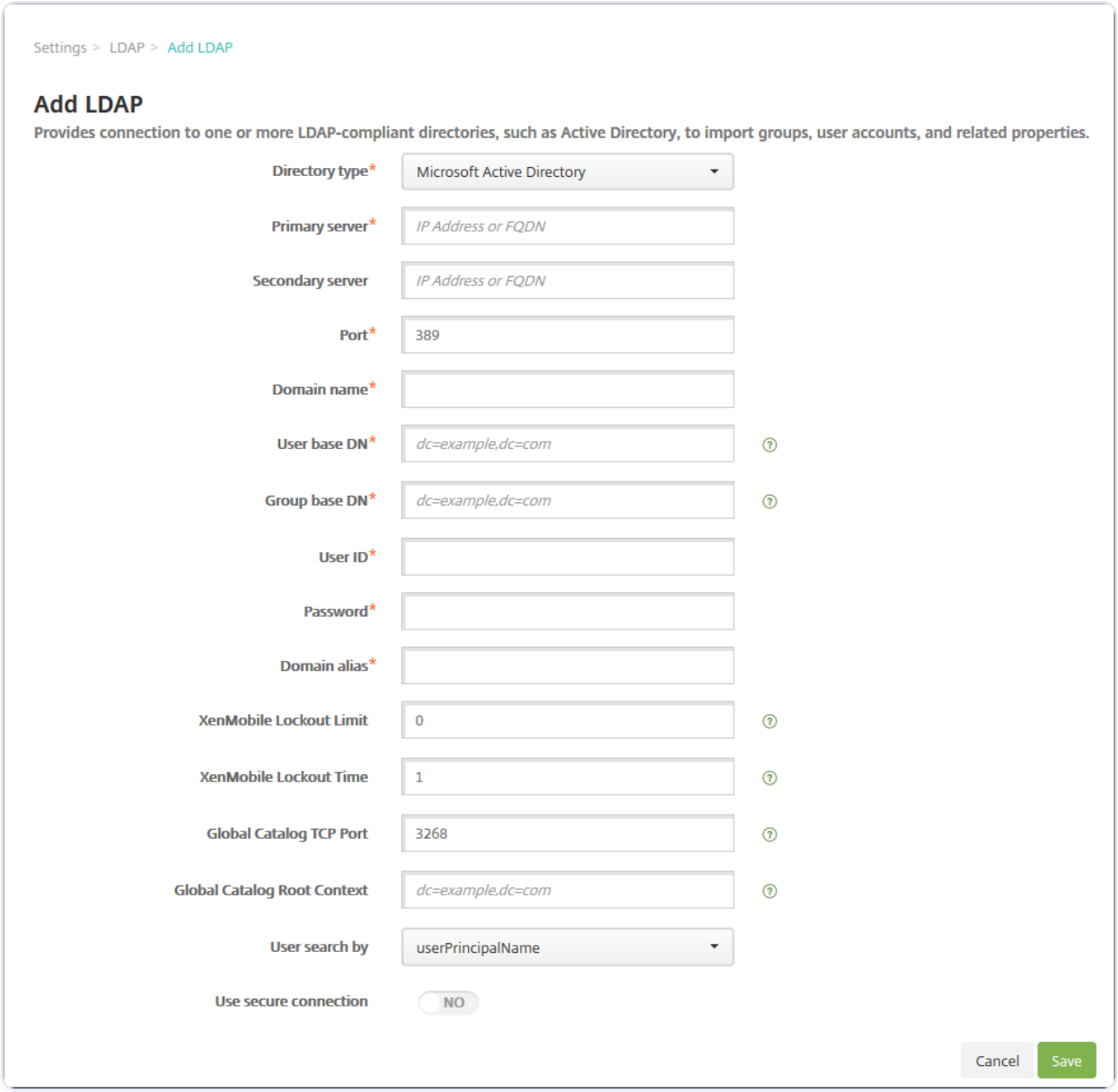
XenMobile で LDAP 接続を追加するには

1. XenMobile コンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**の下で、**LDAP**をクリックします。**LDAP**ページが表示されます。この記事で説明されているように、LDAP 準拠のディレクトリを追加、編集、または削除できます。



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**ページが表示されます。



2. これらの設定を構成します:

- **ディレクトリの種類:** リストで、適切なディレクトリの種類をクリックします。デフォルトは **Microsoft Active Directory** です。
- **プライマリサーバー:** LDAPに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）のいずれかを入力できます。
- **セカンダリサーバー:** オプションで、セカンダリサーバーが構成されている場合は、その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に到達できない場合に使用されるフェールオーバーサーバーです。
- **ポート:** LDAPサーバーが使用するポート番号を入力します。デフォルトでは、保護されていないLDAP接続の場合、ポート番号は **389** に設定されています。保護されたLDAP接続にはポート番号 **636** を使用し、Microsoftの保護されていないLDAP接続には **3268** を、Microsoftの保護されたLDAP接続には **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:** 一意の識別子を使用して、Active Directory内のユーザーの場所を入力します。構文の例には、`ou=users`、`dc=example`、または `dc=com` があります。
- **グループベースDN:** Active Directory内のグループの場所を入力します。たとえば、`cn=users, dc=domain, dc=net` のように入力します。ここで、`cn=users` はグループのコンテナ名を表し、`dc` はActive Directoryのドメインコンポーネントを表します。
- **ユーザーID:** Active Directoryアカウントに関連付けられているユーザーIDを入力します。
- **パスワード:** ユーザーに関連付けられている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。登録後に**ドメインエイリアス**の設定を変更した場合、ユーザーは再登録する必要があります。
- **XenMobileロックアウト制限:** ログオン失敗回数として **0** から **999** までの数値を入力します。値が **0** の場合、XenMobileはログオン失敗に基づいてユーザーをロックアウトすることはありません。
- **XenMobileロックアウト時間:** ロックアウト制限を超過した後、ユーザーが待機する必要がある分数として **0** から **99999** までの数値を入力します。値が **0** の場合、ロックアウト後にユーザーが待機を強制されることはありません。
- **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接続の場合はポート番号 **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:** オプションで、Active Directoryでグローバルカタログ検索を有効にするために使用されるグローバルルートコンテキストの値を入力します。この検索は、実際のドメイン名を指定する必要なく、任意のドメインで標準のLDAP検索に追加して行われます。
- **ユーザー検索基準:** リストで、**userPrincipalName** または **sAMAccountName** のいずれかをクリックします。デフォルトは **userPrincipalName** です。登録後に**ユーザー検索基準**の設定を変更した場合、ユーザーは再登録する必要があります。
- 「**セキュア接続を使用:**」セキュア接続を使用するかどうかを選択します。デフォルトは「**いいえ**」です。

3. 「**保存**」をクリックします。

LDAP準拠ディレクトリを編集するには

1. 「**LDAP**」テーブルで、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選択すると、LDAPリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

2. 「**編集**」をクリックします。「**LDAPの編集**」ページが表示されます。

   LDAP構成画面(/en-us/xenmobile/server/media/edit-ldap.png)

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:**」リストで、適切なディレクトリの種類をクリックします。
   - 「**プライマリサーバー:**」LDAPに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）のいずれかを入力できます。
   - 「**セカンダリサーバー:**」オプションで、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サーバーで使用されるポート番号を入力します。デフォルトでは、保護されていないLDAP接続の場合、ポート番号は「**389**」に設定されています。セキュアなLDAP接続にはポート番号「**636**」を、Microsoftの保護されていないLDAP接続には「**3268**」を、MicrosoftのセキュアなLDAP接続には「**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:**」一意の識別子を介してActive Directory内のユーザーの場所を入力します。構文の例は次のとおりです: `ou=users`、`dc=example`、または`dc=com`。
   - 「**グループベースDN:**」`cn=groupname`として指定されたグループベースDNグループ名を入力します。たとえば、`cn=users`がグループ名である`cn=users, dc=servername, dc=net`のように。`DN`と`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ているユーザーIDを入力します。
   - **パスワード:** ユーザーに関連付けられている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。登録後に**ドメインエイリアス**設定を変更した場合、ユーザーは再登録する必要があります。
   - **XenMobileロックアウト制限:** ログオン失敗回数として**0**から**999**の間の数値を入力します。値が**0**の場合、XenMobileはログオン失敗回数に基づいてユーザーをロックアウトすることはありません。
   - **XenMobileロックアウト時間:** ロックアウト制限を超過した後、ユーザーが待機する必要がある分数として**0**から**99999**の間の数値を入力します。値が**0**の場合、ロックアウト後にユーザーは待機を強制されません。

- **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接続の場合は、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:** オプションで、Active Directoryでグローバルカタログ検索を有効にするために使用されるグローバルルートコンテキスト値を入力します。この検索は、実際のドメイン名を指定することなく、任意のドメインで標準のLDAP検索に追加して行われます。
- **ユーザー検索基準:** リストで、**userPrincipalName**または**sAMAccountName**のいずれかをクリックします。登録後に**ユーザー検索基準**設定を変更した場合、ユーザーは再登録する必要があります。
- **セキュア接続を使用:** セキュア接続を使用するかどうかを選択します。

4. 変更を保存するには**保存**をクリックし、プロパティを変更しないままにするには**キャンセル**をクリックします。

LDAP準拠ディレクトリを削除するには

1. **LDAP**テーブルで、削除するディレクトリを選択します。

   各プロパティの横にあるチェックボックスを選択すると、複数のプロパティを削除できます。

2. **削除**をクリックします。確認ダイアログボックスが表示されます。もう一度**削除**をクリックします。

複数のドメインの認証を構成する

XenMobile ServerをLDAP構成で複数のドメインサフィックスを使用するように構成するには、Citrix Endpoint Managementドキュメントの「複数のドメインの認証を構成する」の手順を参照してください。オンプレミス版のXenMobile ServerとEndpoint Managementクラウドリリースでは、手順は同じです。

ドメインとセキュリティトークン認証を構成する

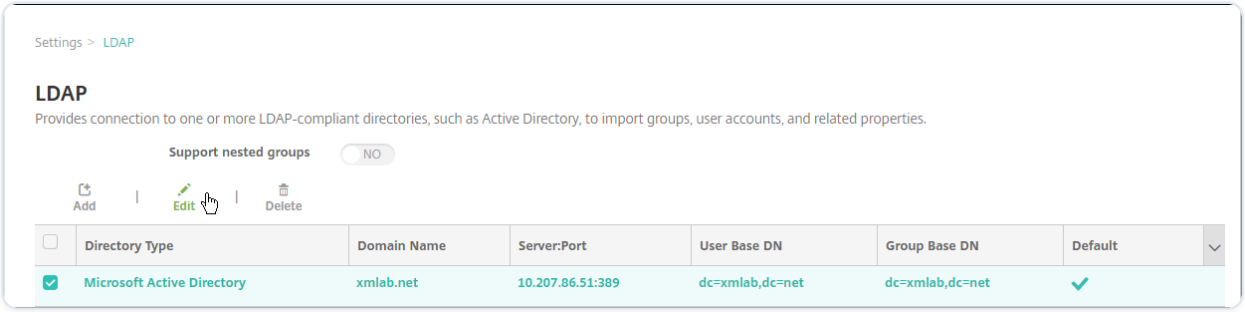
XenMobileを構成して、RADIUSプロトコルを使用して、ユーザーがLDAP資格情報とワンタイムパスワードで認証するように要求できます。

最適な使いやすさのために、この構成をCitrix PINおよびActive Directoryパスワードキャッシュと組み合わせることができます。この構成では、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ありません。ユーザーは、登録、パスワードの有効期限、およびアカウントロックアウトのためにユーザー名とパスワードを入力します。

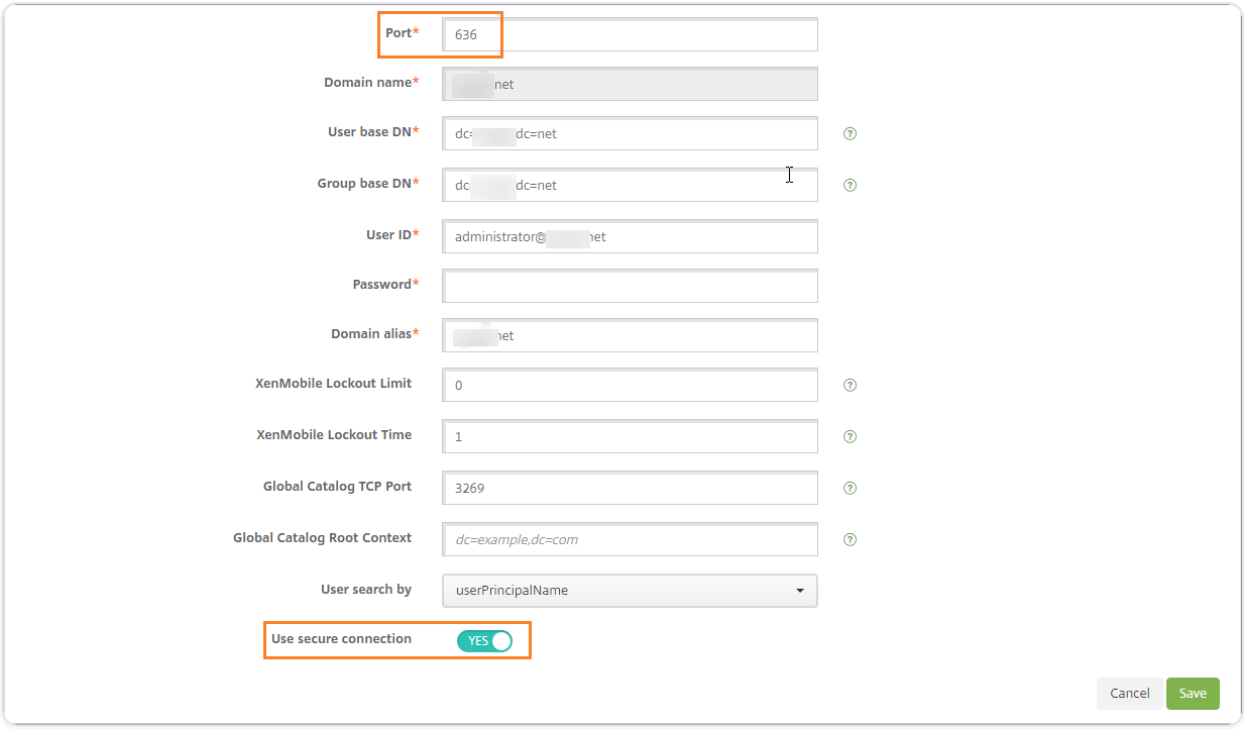
LDAP設定を構成する

認証にLDAPを使用するには、XenMobileに認証局からのSSL証明書をインストールする必要があります。詳細については、「XenMobileでの証明書のアップロード」を参照してください。

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



3. ポートがセキュアなLDAP接続の場合は**636**、Microsoftセキュアなldap接続の場合は**3269**であることを確認します。
4. **［セキュアな接続を使用］を［はい］**に変更します。



Citrix Gateway設定を構成する

次の手順は、Citrix GatewayインスタンスをXenMobileにすでに追加していることを前提としています。Citrix Gatewayインスタンスを追加するには、「Citrix Gatewayインスタンスを追加する」を参照してください。

1. **［設定］で、［Citrix Gateway］**をクリックします。

2. 「**Citrix Gateway**」を選択し、「**編集**」をクリックします。
3. 「**ログオンの種類**」から「**ドメインとセキュリティトークン**」を選択します。

   Citrix Gateway構成画面(/en-us/xenmobile/server/media/logon-type-domain-and-security-token.png)

Citrix PINおよびユーザーパスワードのキャッシュを有効にする

Citrix PINおよびユーザーパスワードのキャッシュを有効にするには、**［設定］>［クライアントプロパティ］**に移動し、次のチェックボックスをオンにします: **［Citrix PIN認証を有効にする］および［ユーザーパスワードのキャッシュを有効にする］**。詳しくは、［クライアントプロパティ］(/ja-jp/xenmobile/server/provision-devices/client-properties.html)を参照してください。

ドメインとセキュリティトークン認証用にCitrix Gatewayを構成する

XenMobileで使用される仮想サーバーのCitrix Gatewayセッションプロファイルとポリシーを構成します。詳しくは、Citrix 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

XenMobile®のデフォルト構成は、ユーザー名とパスワード認証です。XenMobile環境への登録とアクセスに別のセキュリティ層を追加するには、証明書ベースの認証の使用を検討してください。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良の組み合わせです。証明書とドメイン認証は、Citrix ADCでの二要素認証によって提供されるセキュリティと相まって、最高のSSOの可能性を秘めています。

最適な使いやすさのために、証明書とドメイン認証をCitrix PINおよびActive Directory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ありません。ユーザーは、登録、パスワードの有効期限切れ、およびアカウントロックアウトのためにユーザー名とパスワードを入力します。

> **重要:**
>
> XenMobileは、ユーザーがXenMobileにデバイスを登録した後、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をサポートしていません。

> LDAPを許可せず、スマートカードまたは類似の方法を使用する場合、証明書を構成することで、スマートカードをXenMobileに提示できます。その後、ユーザーはXenMobileが生成す

> る一意のPINを使用して登録します。ユーザーがアクセス権を取得すると、XenMobileはXenMobile環境への認証に使用される証明書を作成および展開します。

Citrix ADC証明書のみの認証または証明書とドメイン認証を使用する場合、Citrix ADC for XenMobileウィザードを使用してXenMobileに必要な構成を実行できます。Citrix ADC for XenMobileウィザードは1回のみ実行できます。

高度なセキュリティ環境では、組織外のパブリックネットワークまたは安全でないネットワークでのLDAP資格情報の使用は、組織にとって主要なセキュリティ上の脅威と見なされます。高度なセキュリティ環境では、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二要素認証がオプションです。詳細については、「証明書と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 MAMモード（MAMのみ）およびENTモード（ユーザーがMDMに登録する場合）で利用できます。ユーザーがレガシーMAMモードに登録する場合、XenMobile ENTモードではクライアント証明書認証は利用できません。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サーバー、およびCitrix Gatewayを構成する必要があります。この記事で説明されている一般的な手順に従ってください。

Microsoftサーバーで:

1. Microsoft Management Consoleに証明書スナップインを追加します。
2. 証明機関 (CA) にテンプレートを追加します。
3. CAサーバーからPFX証明書を作成します。

XenMobileサーバーで:

1. 証明書をXenMobileにアップロードします。
2. 証明書ベースの認証用の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. 認証用のユーザー証明書を配信するようにCitrix Gatewayを構成します。

Citrix Gatewayの構成については、Citrix ADCドキュメントの以下の記事を参照してください。

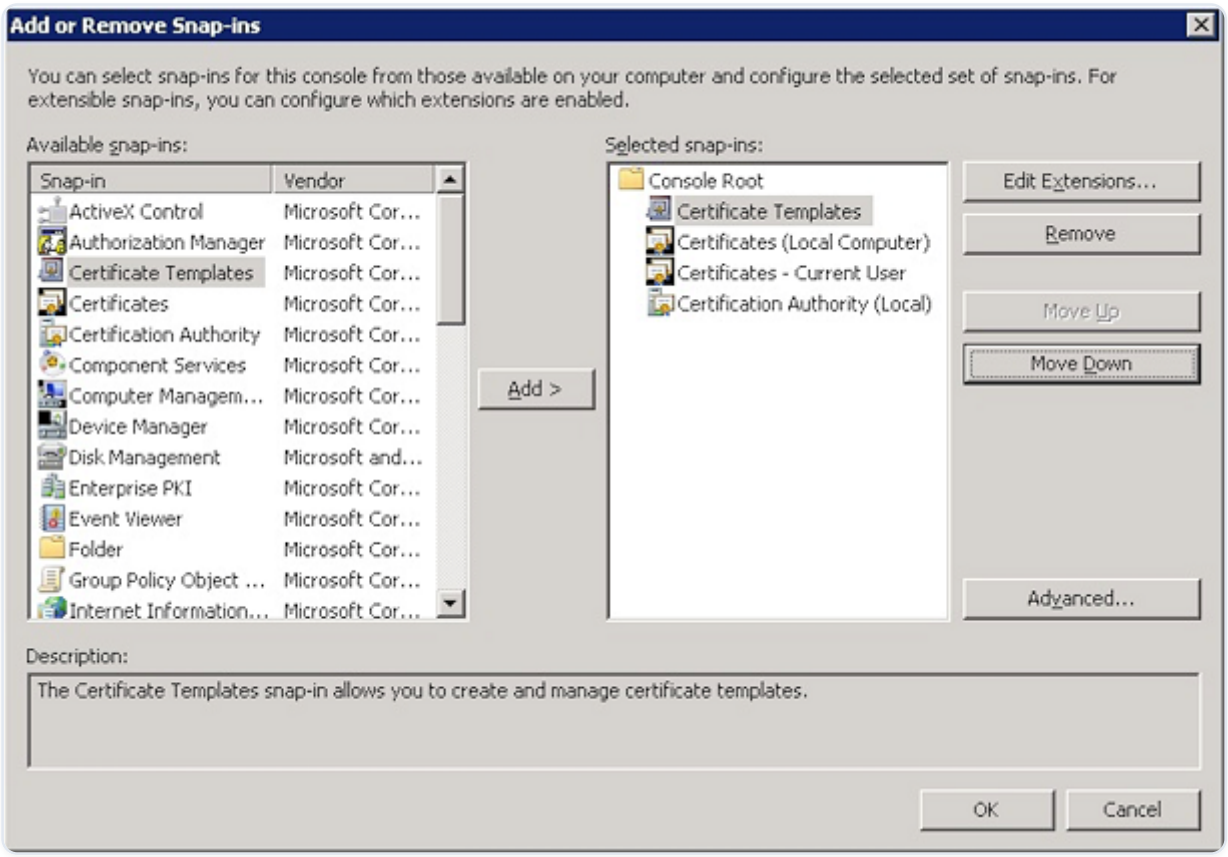
- クライアント認証
- SSLプロファイルインフラストラクチャ
- クライアント証明書認証ポリシーの構成とバインド

前提条件

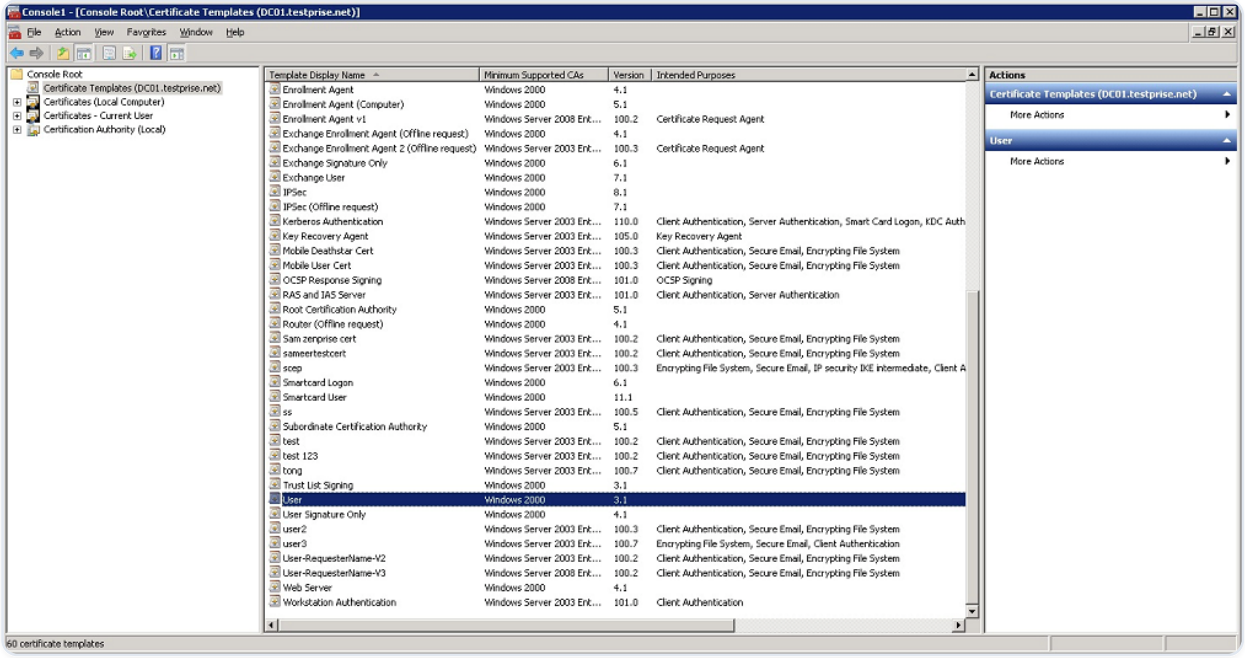
- Microsoft Certificate Servicesエンティティテンプレートを作成する際は、特殊文字を除外して、登録済みデバイスでの認証に関する潜在的な問題を回避してください。たとえば、テンプレート名に次の文字を使用しないでください: `: ! $ ( ) # % + * ~ ? | {} []`
- Exchange ActiveSyncの証明書ベースの認証を構成するには、このMicrosoftブログを参照してください。クライアント証明書を要求するように、Exchange ActiveSync用の証明機関（CA）サーバーサイトを構成します。
- ActiveSyncトラフィックをExchange Serverに保護するためにプライベートサーバー証明書を使用する場合は、モバイルデバイスに必要なすべてのルート/中間証明書があることを確認してください。そうしないと、Secure Mailでのメールボックス設定中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、次の操作を行う必要があります。
  - ExchangeでXenMobileを使用するための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サイトには、「Microsoft-Server-ActiveSync」用と「EWS」用の2つのアプリケーションを追加する必要があります。これらの両方のアプリケーションで、**SSL設定**の下にある**SSLを要求**を選択します。

Microsoft管理コンソールに証明書スナップインを追加する

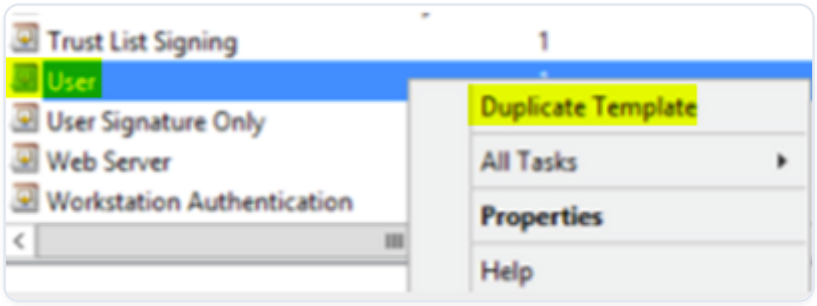
1. コンソールを開き、**スナップインの追加と削除**をクリックします。
2. 次のスナップインを追加します。
   - 証明書テンプレート
   - 証明書 (ローカル コンピューター)
   - 証明書 - 現在のユーザー
   - 証明機関 (ローカル)



3. **証明書テンプレート**を展開します。



4. **ユーザー**テンプレートを選択し、**テンプレートの複製**を選択します。

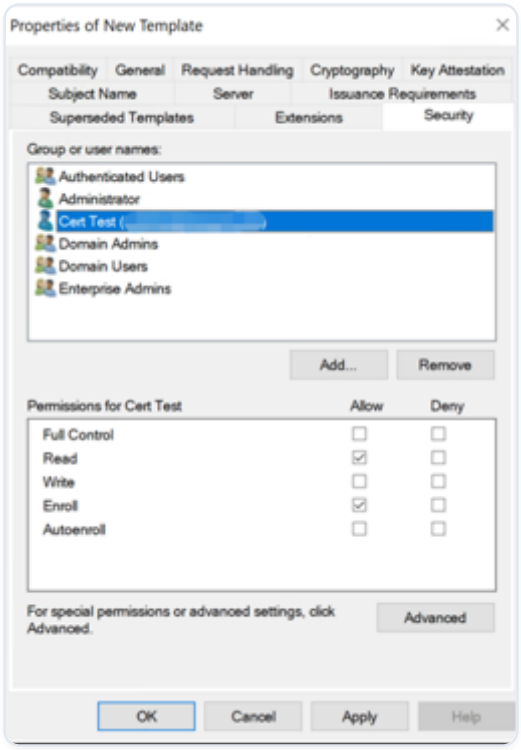


5. テンプレートの表示名を指定します。

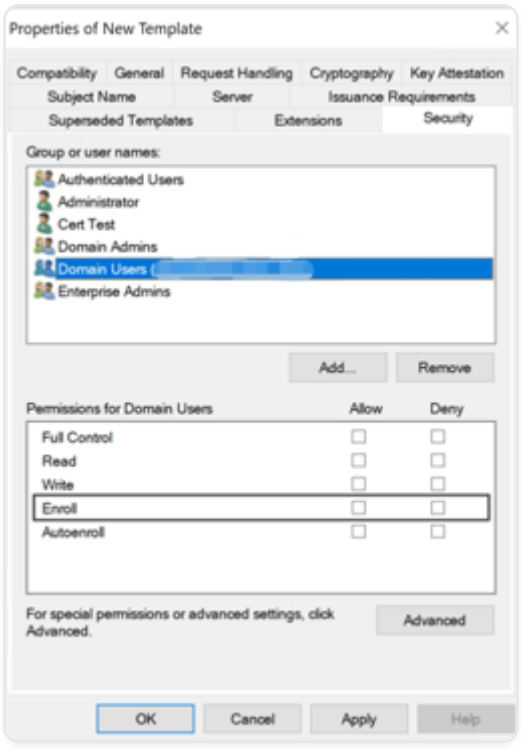
> **重要:**
>
> **Active Directory で証明書を発行する**オプションを選択することはお勧めしません。このオプションを選択すると、Active Directory 内のすべてのユーザーに対してクライアント証明書が作成され、Active Directory データベースが煩雑になる可能性があります。

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 サーバーでは、**互換性**の下で**証明機関**を選択し、受信者を**Windows 2003**に設定します。
7. **セキュリティ**で、以下を構成します:
   a. **追加**をクリックし、次に XenMobile Server が証明書の生成に使用する AD ユーザーアカウントを選択します。

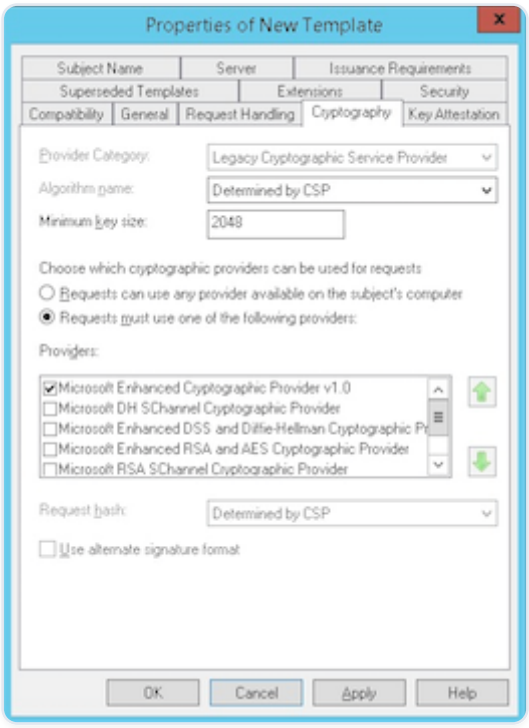
> **重要:**
>
> ここではサービスアカウントユーザーのみを追加します。**登録**権限はこの AD ユーザーアカウントにのみ追加します。
>
> この記事で後述するように、サービスアカウントを使用してユーザー .pfx 証明書を作成します。詳細については、「CA サーバーから PFX 証明書を作成する」を参照してください。



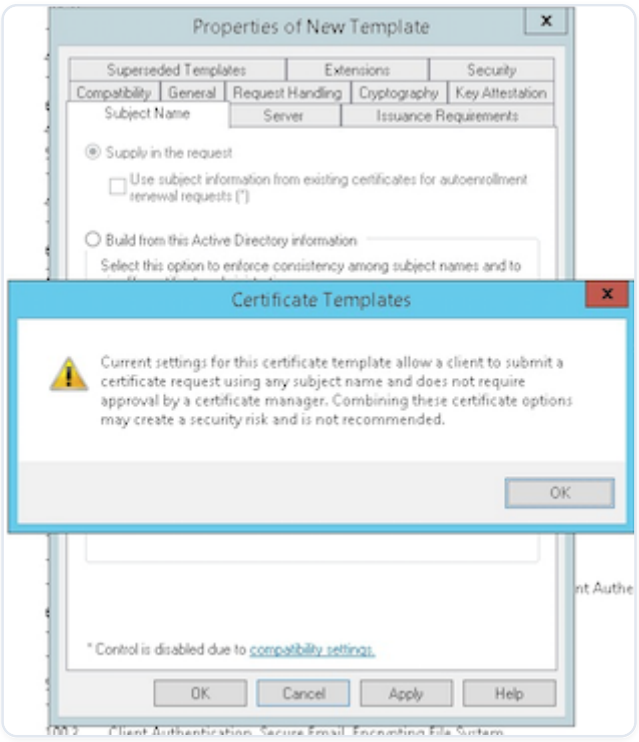
b. **ドメインユーザー**から**登録**権限を取り消します。



8. **暗号化**で、キーサイズを指定していることを確認します。このキーサイズは、後で XenMobile を構成するときに入力します。

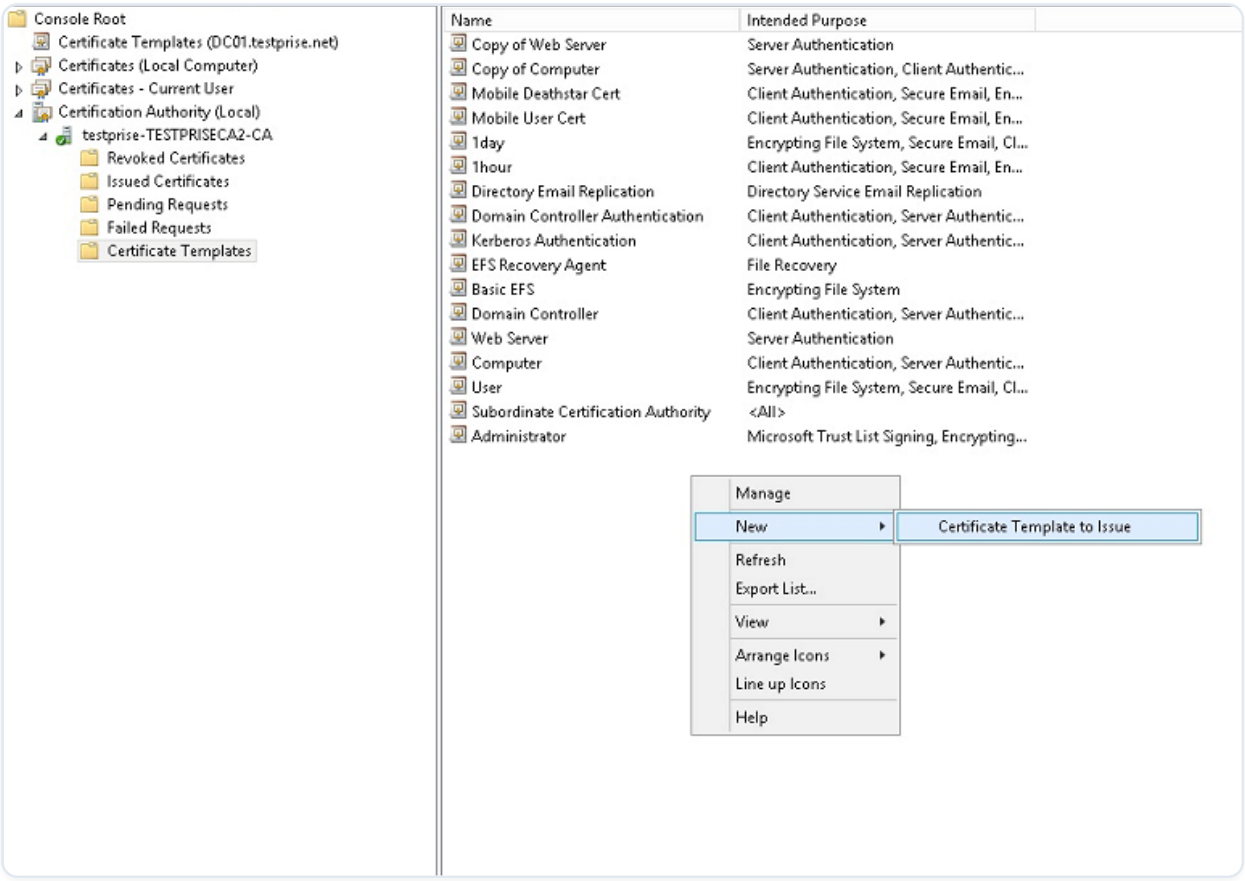


9. **サブジェクト名**で、**要求で指定**を選択します。変更を適用して保存します。

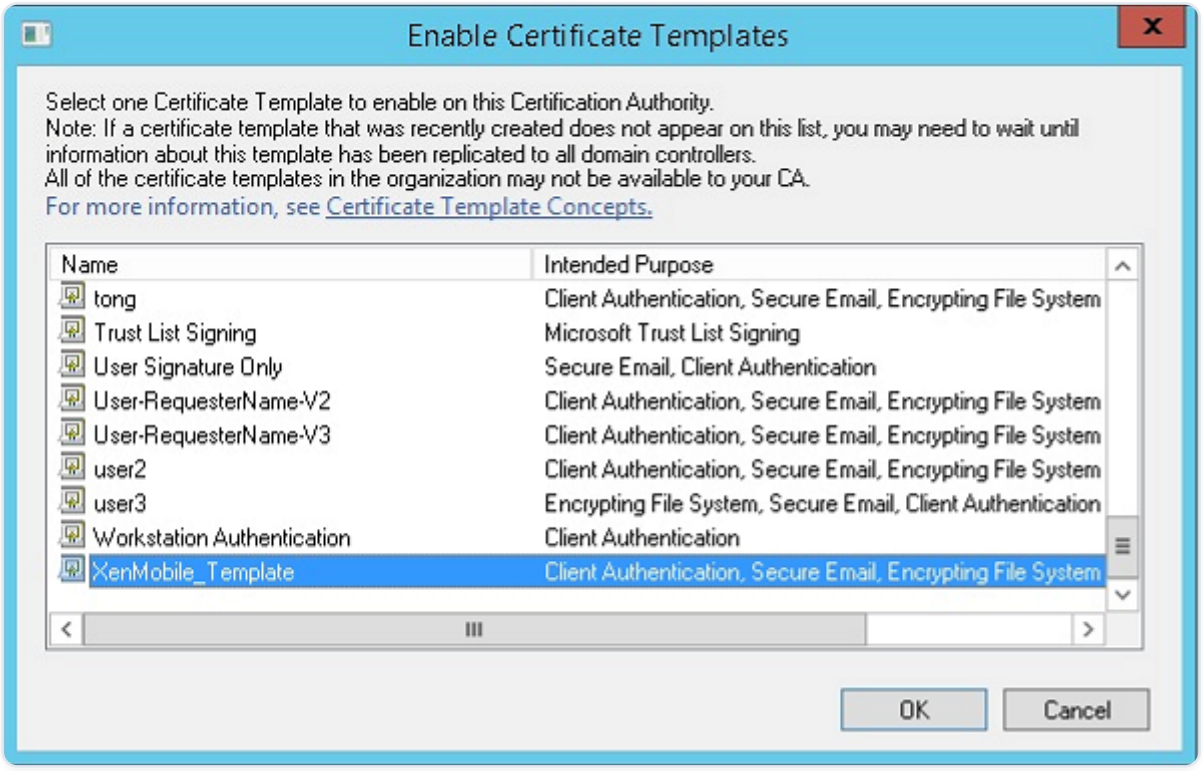


証明機関へのテンプレートの追加

1. **証明機関**に移動し、**証明書テンプレート**を選択します。
2. 右ペインで右クリックし、次に**新規 > 発行する証明書テンプレート**を選択します。

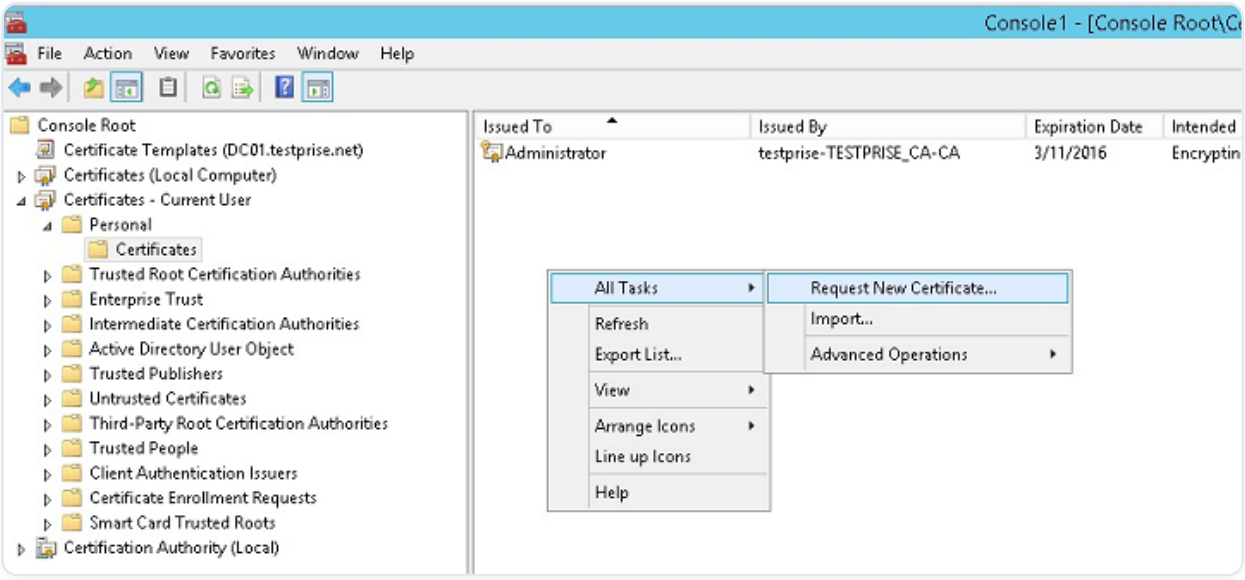


3. 前のステップで作成したテンプレートを選択し、**OK**をクリックして**証明機関**に追加します。

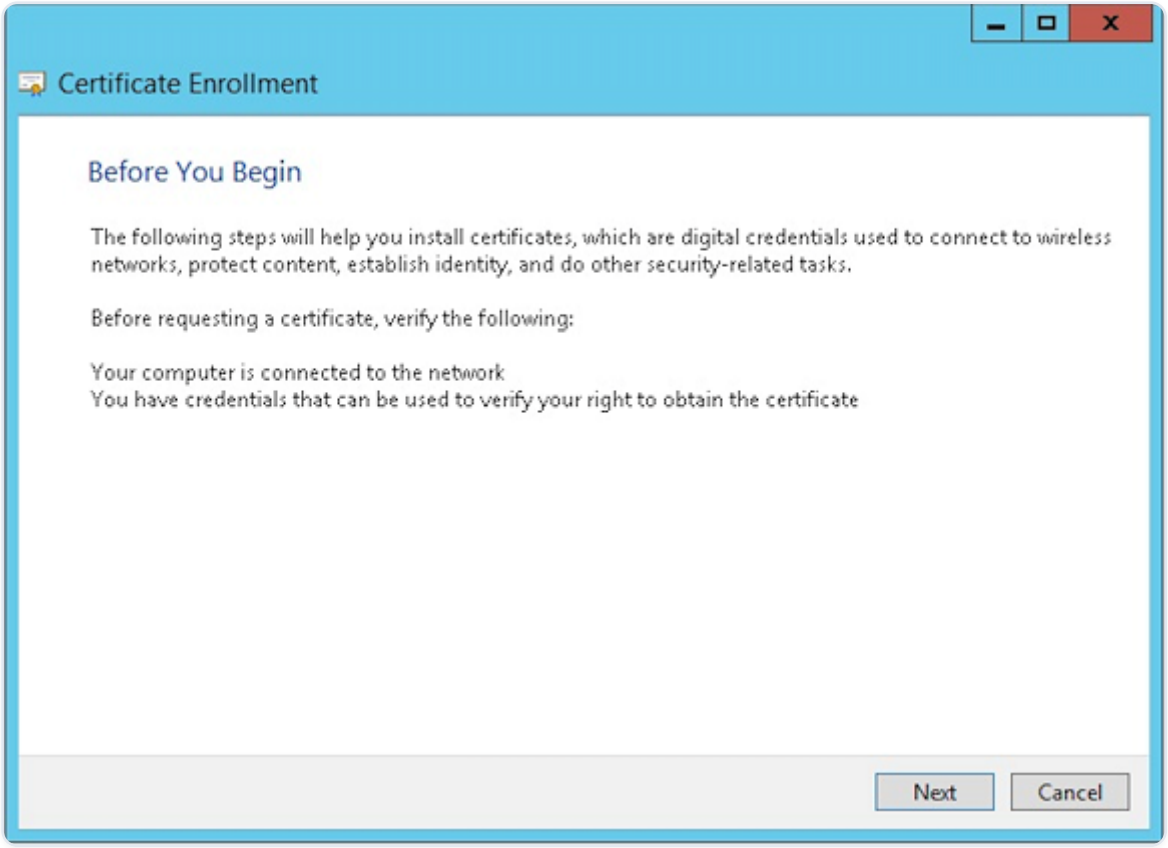


CAサーバーからPFX証明書を作成する

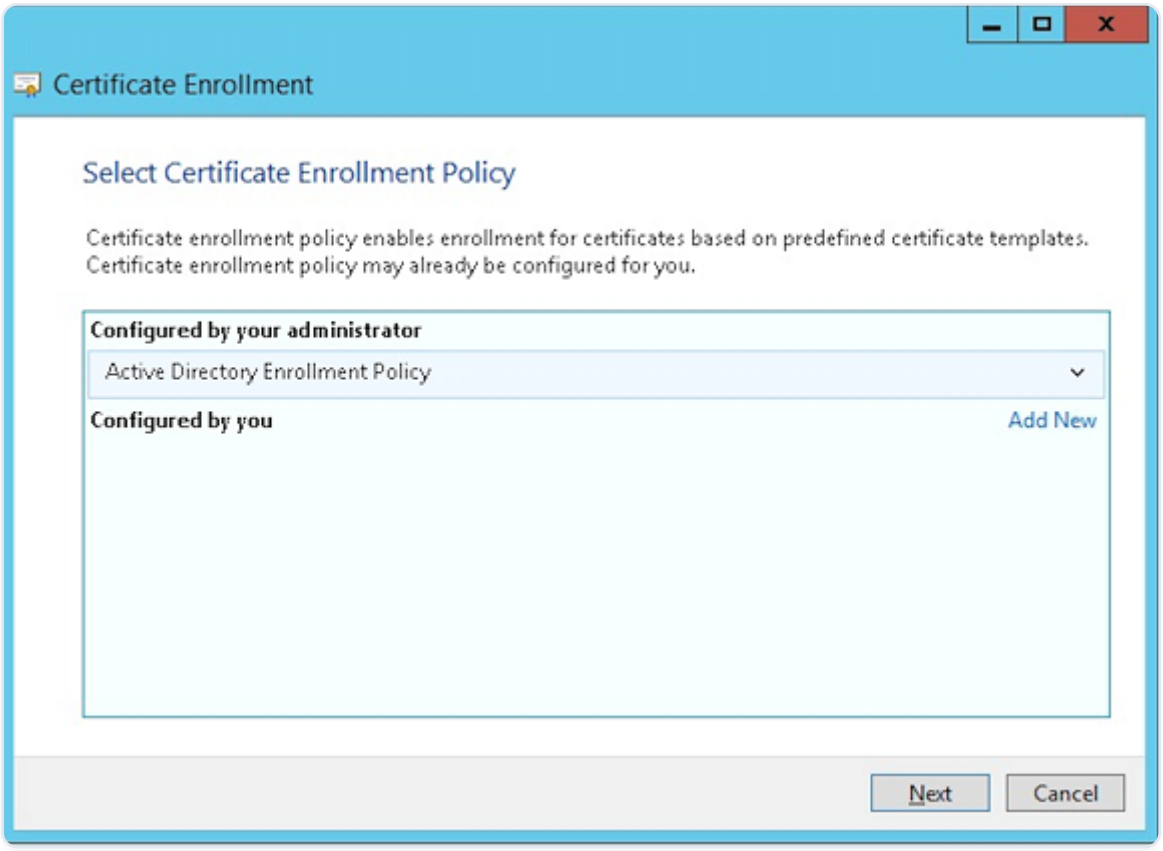
1. ログインしたサービスアカウントを使用して、ユーザーの.pfx証明書を作成します。.pfxはXenMobileにアップロードされ、その後、デバイスを登録するユーザーに代わってユーザー証明書を要求します。
2. **現在のユーザー**の下で、**証明書**を展開します。
3. 右ペインで右クリックし、**新しい証明書を要求**をクリックします。



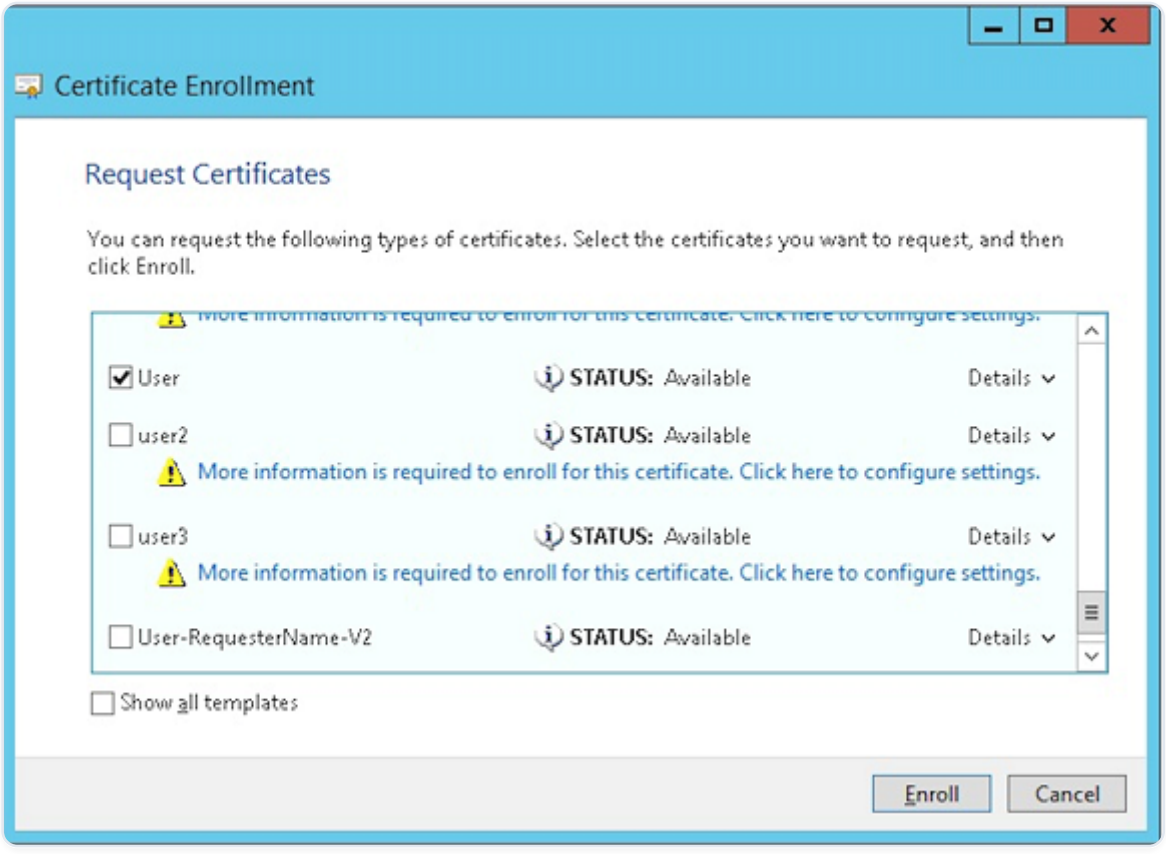
4. **証明書の登録**画面が表示されます。**次へ**をクリックします。



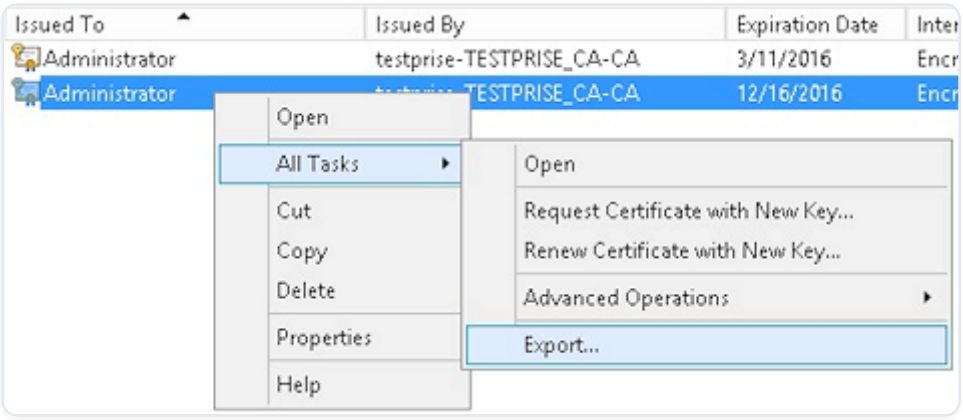
5. **Active Directory登録ポリシー**を選択し、**次へ**をクリックします。



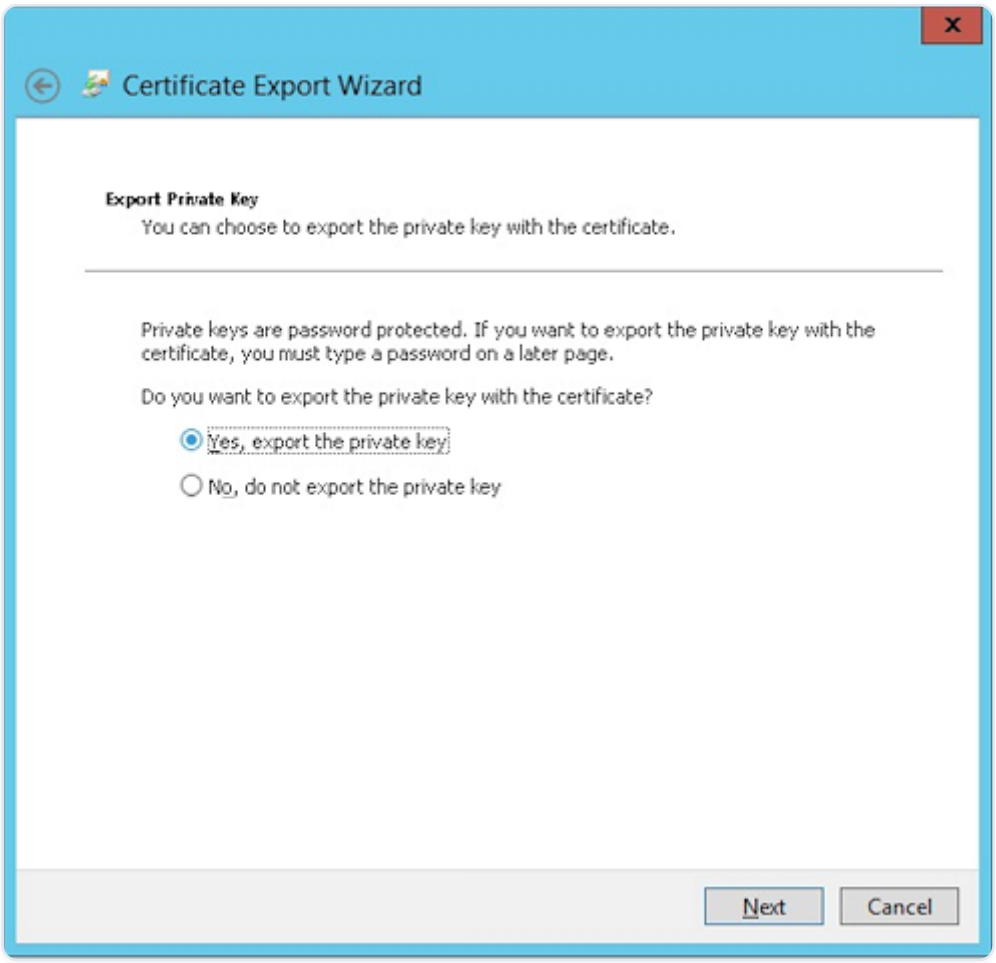
6. **ユーザー**テンプレートを選択し、**登録**をクリックします。



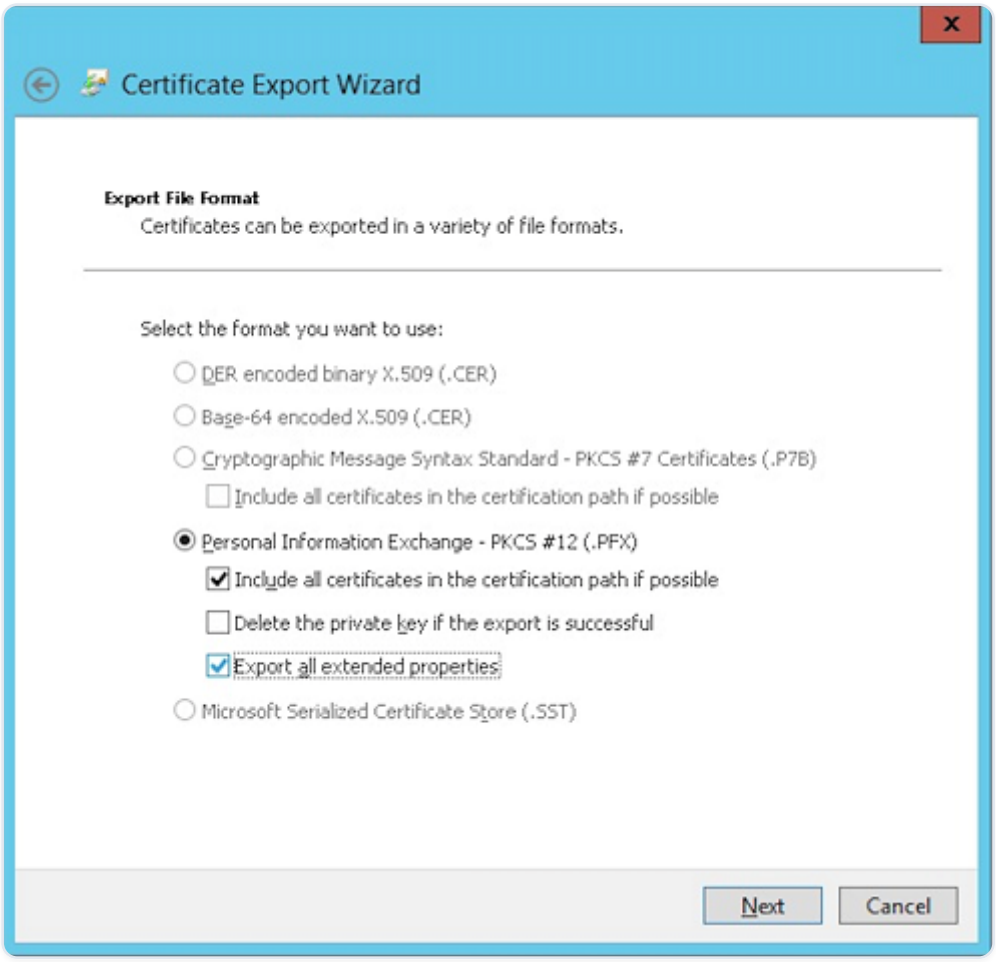
7. 前のステップで作成した.pfxファイルをエクスポートします。



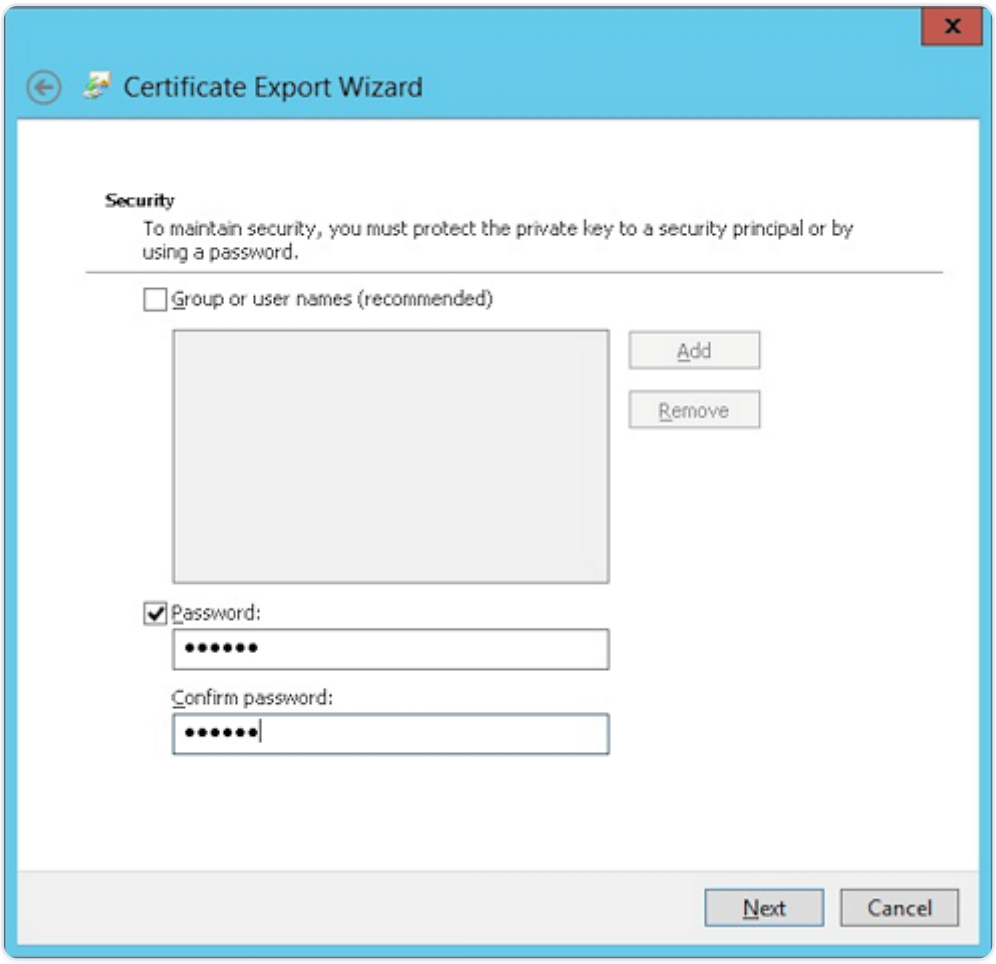
8. 「**はい、秘密キーをエクスポートします**」をクリックします。



9. 「**可能であれば、証明のパスにあるすべての証明書を含める**」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. この証明書をXenMobileに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、右上隅にある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、次に「**インポート**」をクリックします。
3. 次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
    - **用途:** サーバー
    - 「**キーストアファイル**」：「**参照**」をクリックして、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。

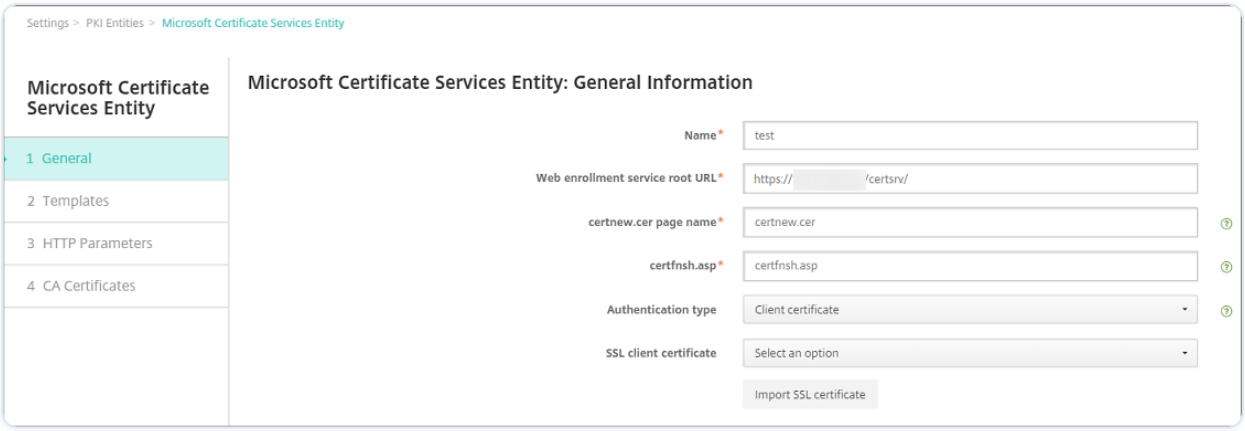
    証明書構成画面のスクリーンショット(/en-us/xenmobile/server/media/import-certificate.png)
4. 「**インポート**」をクリックします。

5. 証明書が正しくインストールされていることを確認します。正しくインストールされた証明書は、ユーザー証明書として表示されます。

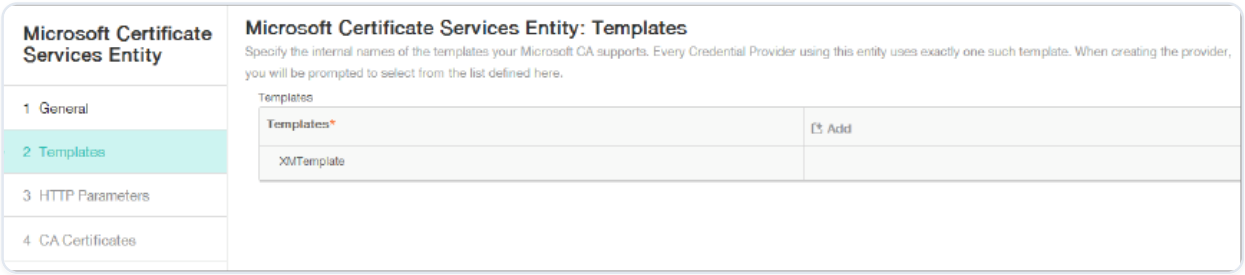
証明書ベースの認証用のPKIエンティティの作成

1. 「**設定**」で、「**その他 > 証明書管理 > PKIエンティティ**」の順に進みます。
2. 「**追加**」をクリックし、その後「**Microsoft Certificate Servicesエンティティ**」をクリックします。「**Microsoft Certificate Servicesエンティティ：一般情報**」画面が表示されます。
3. 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
   - 「**Web登録サービスルートURL**」：`https://RootCA-URL/certsrv/` (URLパスの最後のスラッシュ「/」を必ず追加してください。)
   - 「**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の発行に使用するユーザー証明書を選択します。

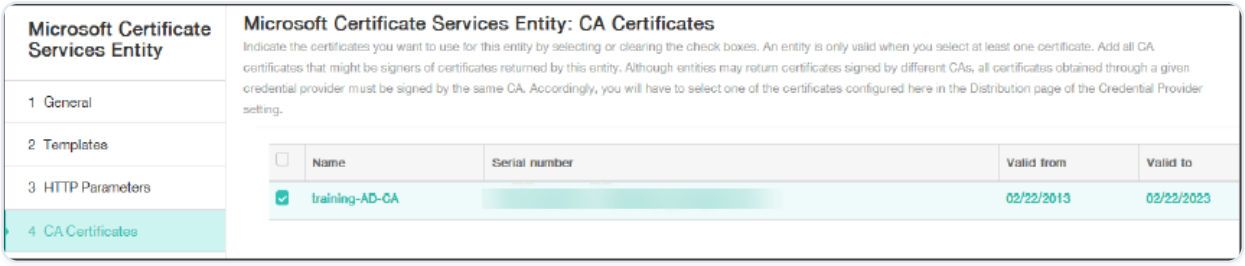


4. 「**テンプレート**」で、Microsoft 証明書を構成したときに作成したテンプレートを追加します。スペースを追加しないでください。



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. 環境に対応するルート CA 名を選択します。このルート CA 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。

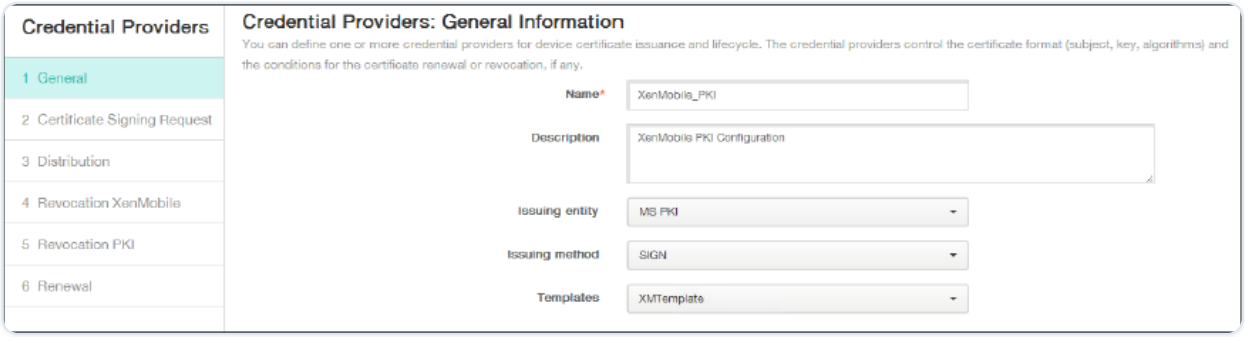


7. **保存**をクリックします。

資格情報プロバイダーの構成

1. 「**設定**」で、**その他 > 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. 「**一般**」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:** 以前に作成した PKI エンティティを選択します。
   - **発行方法:** SIGN
   - **テンプレート:** PKIエンティティの下に追加されたテンプレートを選択します。

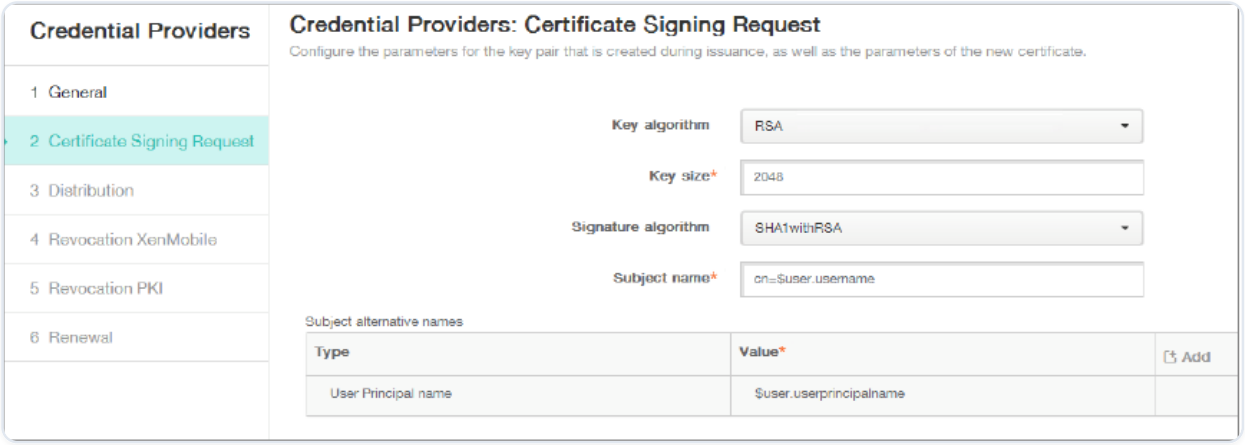


4. **証明書署名要求**をクリックし、次のパラメーターを入力します。

   - **キーアルゴリズム:** RSA
   - **キーサイズ:** 2048
   - **署名アルゴリズム:** SHA256withRSA
   - **サブジェクト名:** `cn=$user.username`

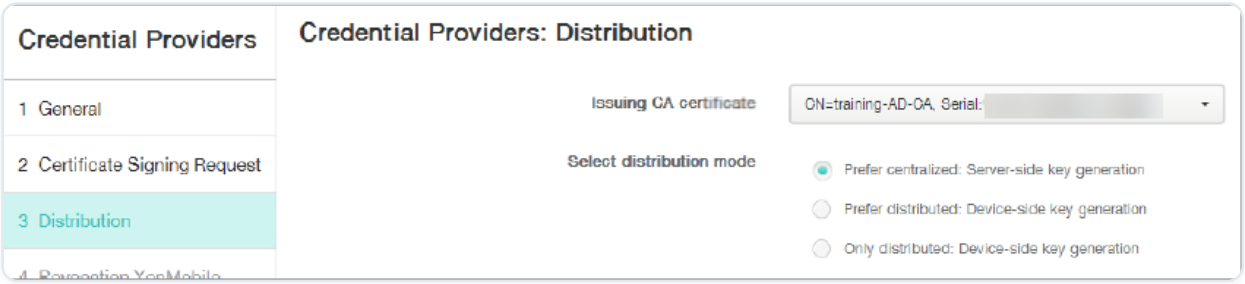
   サブジェクトの別名については、**追加**をクリックし、次のパラメーターを入力します。

- **種類:** ユーザープリンシパル名
- **値:** `$user.userprincipalname`



5. **配布**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:** XenMobileクライアント証明書に署名した発行CAを選択します。
   - **配布モードの選択: 集中型を優先: サーバー側でのキー生成**を選択します。



6. 次の2つのセクション、**Revocation XenMobile** と **Revocation PKI** については、必要に応じてパラメータを設定します。この例では、両方のオプションをスキップします。
7. **更新**をクリックします。
8. **証明書の有効期限が切れたときに更新する**については、**ON**を選択します。
9. その他の設定はすべてデフォルトのままにするか、必要に応じて変更します。

   資格情報プロバイダーの構成画面(/en-us/xenmobile/server/media/configure-credential-providers-4.png)

10. **保存**をクリックします。

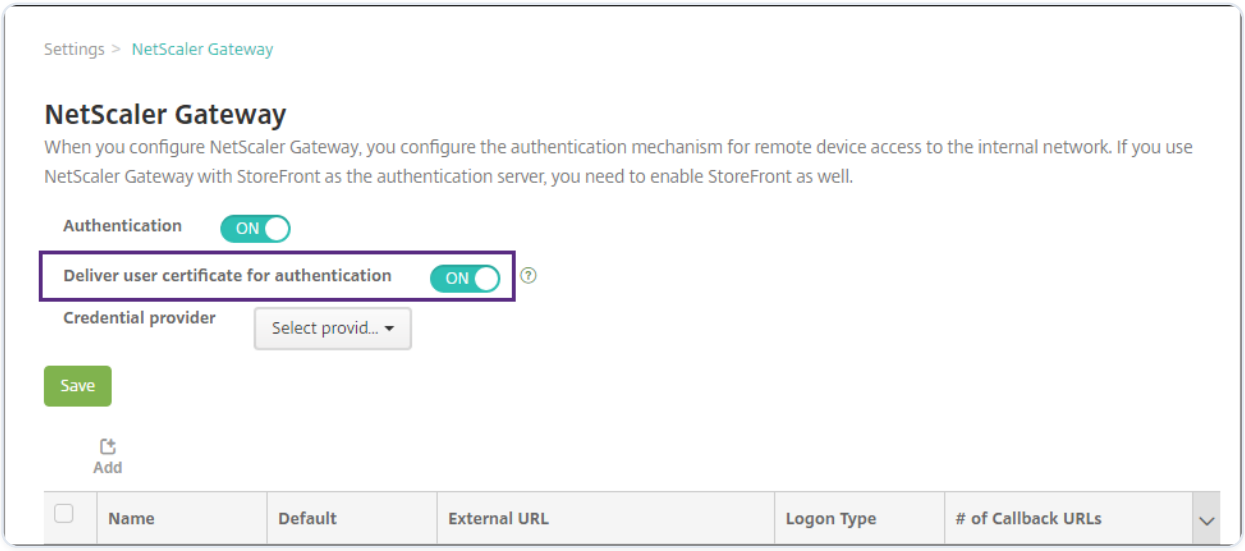
証明書ベースの認証を使用するようにSecure Mailを構成する

Secure MailをXenMobileに追加するときは、**アプリ設定**の下のExchange設定を必ず構成してください。

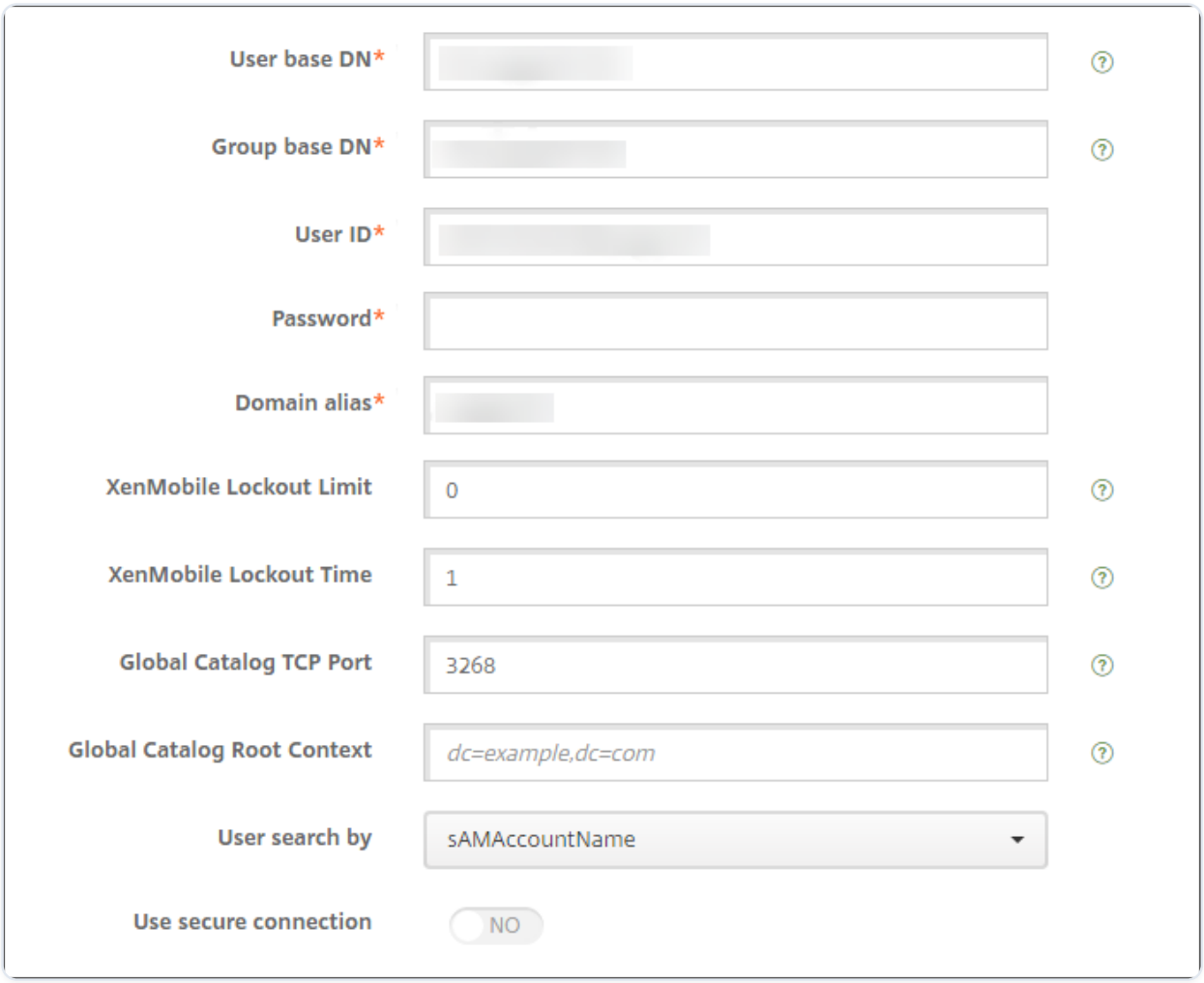
アプリの構成画面(/en-us/xenmobile/server/media/configure-worxmail-certificate-authentication.png)

XenMobileでのCitrix ADC証明書配信の構成

1. XenMobileコンソールにログオンし、右上隅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**の下で、**Citrix Gateway**をクリックします。
3. Citrix Gatewayがまだ追加されていない場合は、**追加**をクリックし、設定を指定します。
   - **外部URL:** `https://YourCitrixGatewayURL`
   - **ログオンの種類:** 証明書とドメイン
   - **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**には、**オン**を選択します。



5. **資格情報プロバイダー**には、プロバイダーを選択し、**保存**をクリックします。
6. ユーザー証明書のsAMAccount属性をユーザープリンシパル名 (UPN) の代替として使用するには、XenMobileで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、**ユーザー検索条件**で**sAMAccountName**を選択します。



Citrix PINとユーザーパスワードのキャッシュを有効にする

Citrix PINとユーザーパスワードのキャッシュを有効にするには、**設定 > クライアントプロパティ**に移動し、**Citrix PIN認証を有効にする**と**ユーザーパスワードのキャッシュを有効にする**のチェックボックスをオンにします。詳しくは、「クライアントプロパティ」を参照してください。

クライアント証明書構成のトラブルシューティング

上記の構成とCitrix Gateway構成が正常に完了すると、ユーザーワークフローは次のようになります。

1. ユーザーはモバイルデバイスを登録します。
2. XenMobileは、Citrix PINの作成をユーザーに促します。
3. その後、ユーザーはXenMobile Storeにリダイレクトされます。
4. ユーザーがSecure Mailを起動しても、XenMobileはメールボックス構成のユーザー資格情報を要求しません。代わりに、Secure MailはSecure Hubから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が資格情報を要求する場合は、構成を確認してください。

ユーザーがSecure Mailをダウンロードしてインストールできるが、メールボックスの構成中にSecure Mailが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/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に選択されている認証タイプが**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。

   Microsoft ActiveSyncのプロパティ画面(/en-us/xenmobile/server/media/activesync-require-client-certs.png)
3. Microsoft Exchange Serverで、**Microsoft-Server-ActiveSync**サイトを確認し、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。このオプションは、**構成エディター > セキュリティ > 認証**の下にあります。

   Microsoft ActiveSyncの構成画面(/en-us/xenmobile/server/media/activesync-enable-cert-mapping.png)

   Trueを選択した後、変更を適用するために**適用**をクリックしてください。
4. XenMobileコンソールでCitrix Gatewayの設定を確認します。**認証用のユーザー証明書を配信**が**オン**になっており、**資格情報プロバイダー**に正しいプロファイルが選択されていることを確認します。

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確認するには

1. XenMobileコンソールで、**管理 > デバイス**に移動し、デバイスを選択します。
2. **編集**または**詳細を表示**をクリックします。
3. **配信グループ**セクションに移動し、次のエントリを検索します。

   Citrix Gateway資格情報: 要求された資格情報, CertId=

クライアント証明書ネゴシエーションが有効になっているかどうかを検証するには

1. IIS Webサイトにバインドされ ているSSL証明書構成を表示するには、この`netsh`コマンドを実行します。

   ```
   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、それを有効にするには、次のコマンドを実行します。

`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`

例:

`netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid={4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable`

PKIエンティティ

XenMobile®の公開鍵インフラストラクチャ (PKI) エンティティ構成は、実際のPKI操作 (発行、失効、ステータス情報) を行う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の内部または外部にあります。内部コンポーネントは裁量的と呼ばれます。外部コンポーネントは、企業のインフラストラクチャの一部です。

XenMobileは、以下の種類のPKIエンティティをサポートしています。

- Microsoft 証明書サービス
- 裁量的な認証局 (CA)

XenMobileは以下のCAサーバーをサポートしています。

- ウィンドウズ サーバー 2019
- ウィンドウズ サーバー 2016

> **注記:**
>
> Windows Server 2012 R2、2012、および2008 R2は、サポート終了に達したため、サポートされなくなりました。詳細については、Microsoft製品のライフサイクルに関するドキュメントを参照してください。

一般的なPKIの概念

種類にかかわらず、すべてのPKIエンティティは以下の機能の一部を備えています。

- **署名:** 証明書署名要求 (CSR) に基づいて新しい証明書を発行します。
- **取得:** 既存の証明書とキーペアを回復します。
- **失効:** クライアント証明書を失効させます。

CA証明書について

PKIエンティティを構成する際、そのエンティティによって発行された（または回復された）証明書の署名者であるCA証明書をXenMobileに示します。そのPKIエンティティは、任意の数の異なるCAによって署名された証明書（取得済みまたは新規署名済み）を返すことができます。

これらの各CA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。そのためには、証明書をXenMobileにアップロードし、PKIエンティティでそれらを参照します。裁量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、証明書を手動で指定する必要があります。

> **重要:**

> Microsoft Certificate Servicesエンティティテンプレートを作成する際、登録済みデバイスでの認証の問題を回避するため、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、`! : $ ( ) # % + * ~ ? | { } [ ]`は使用しないでください。

マイクロソフト証明書サービス

XenMobileは、Web登録インターフェイスを介してMicrosoft Certificate Servicesと連携します。XenMobileは、そのインターフェイスを介した新しい証明書の発行のみをサポートします。Microsoft CAがCitrix Gatewayユーザー証明書を生成する場合、Citrix Gatewayはそ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 Webインターフェイスのベースを指定する必要があります。必要に応じて、SSLクライアント認証を使用して、XenMobileとCertificate Services Webインターフェイス間の接続を保護します。

Microsoft Certificate Servicesエンティティを追加する

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックし、次に**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 Certificate Servicesエンティティ**をクリックします。

   Microsoft Certificate Servicesエンティティ: 一般情報ページが表示されます。

4. **Microsoft Certificate Servicesエンティティ: 一般情報**ページで、これら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である必要があります。
   - **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を入力します。例: `https://192.0.2.13/certsrv/`。URLは、プレーンHTTPまたはHTTP-over-SSLを使用できます。
   - **certnew.cerページ名:** certnew.cerページの名称。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ページの名称。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 Basic:** 接続に必要なユーザー名とパスワードを入力します。
     - **クライアント証明書:** 正しい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、接続に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 Certificate Servicesエンティティ: テンプレートページが表示されます。このページでは、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は、ここで定義されているリストからテンプレートを選択します。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は、そのようなテンプレートを1つだけ使用します。

   Microsoft Certificate Servicesのテンプレート要件については、お使いのMicrosoft Serverバージョンのマイクロソフトドキュメントを参照してください。XenMobileは、証明書に記載されている証明書形式以外に、配布する証明書に関する要件はありません。

7. **Microsoft Certificate Servicesエンティティ: テンプレート**ページで、**追加**をクリックし、テンプレート名を入力してから**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 Certificate Servicesエンティティ: HTTPパラメーターページが表示されます。このページでは、XenMobileがMicrosoft Web登録インターフェイスへのHTTPリクエストに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に対してのみ役立ちます。
9. 「**Microsoft Certificate Services Entity: HTTP parameters**」ページで、「**Add**」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、「**Next**」をクリックします。

   「**Microsoft Certificate Services Entity: CA Certificates**」ページが表示されます。このページで、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 Certificate Services Entity: CA Certificates**」ページで、このエンティティに使用する証明書を選択します。
11. 「**Save**」をクリックします。

    エンティティがPKIエンティティテーブルに表示されます。

Citrix ADC証明書失効リスト (CRL)

XenMobileは、サードパーティの認証局 (CA) に対してのみ証明書失効リスト (CRL) をサポートします。Microsoft CAが構成されている場合、XenMobileはCitrix ADC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際は、Citrix ADCの証明書失効リスト (CRL) 設定「**Enable CRL Auto Refresh**」を構成するかどうかを検討してください。この手順により、MAM専用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いようにします。

XenMobileは、証明書が失効した後でもユーザーがユーザー証明書を生成することを制限しないため、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エンティティをチェックする際に、PKIエンティティのセキュリティを向上させます。

裁量CA

裁量CAは、XenMobileにCA証明書と関連する秘密鍵を提供すると作成されます。XenMobileは、指定されたパラメーターに従って、証明書の発行、失効、およびステータス情報を内部的に処理します。

裁量CAを構成する際、そのCAのオンライン証明書ステータスプロトコル (OCSP) サポートを有効にできます。OCSPサポートを有効にした場合にのみ、CAはCAが発行する証明書に拡張機能 `id-pe-authorityInfoAccess` を追加します。この拡張機能は、次の場所にあるXenMobile内部OCSPレスポンダーを指します。

`https://<server>/<instance>/ocsp`

OCSPサービスを構成する際、該当する裁量エンティティのOCSP署名証明書を指定します。CA証明書自体を署名者として使用できます。CA秘密鍵の不必要な露出を避けるため (推奨): CA証明書によって署名された委任OCSP署名証明書を作成し、この拡張機能 `id-kp-OCSPSigning` `extendedKeyUsage` を含めます。

XenMobile OCSPレスポンダーサービスは、基本的なOCSP応答と、要求における次のハッシュアルゴリズムをサポートしています。

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

応答はSHA-256と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。

裁量CAを追加する

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックし、次に**その他 > 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. **裁量CA**をクリックします。

   裁量CA: 一般情報ページが表示されます。
4. **裁量CA: 一般情報**ページで、次の操作を行います。

- **名前:** 裁量CAのわかりやすい名前を入力します。
- **証明書要求に署名するCA証明書:** 裁量CAが証明書要求に署名するために使用する証明書をクリックします。

  この証明書リストは、XenMobileの** > > **でアップロードした秘密鍵を持つCA証明書から生成されます。

5. をクリックします。

   ページが表示されます。

6. ページで、次の操作を行います。

   - **シリアル番号ジェネレーター:** 裁量CAは、発行する証明書のシリアル番号を生成します。このリストから、 または をクリックして、番号の生成方法を決定します。
   - **次のシリアル番号:** 発行される次の番号を決定する値を入力します。
   - **証明書の有効期間:** 証明書が有効な日数を入力します。
   - **キー使用法:** 裁量CAによって発行される証明書の目的を、適切なキーを****に設定して特定します。設定すると、CAはその目的の証明書の発行に限定されます。
   - **拡張キー使用法:** パラメーターを追加するには、 をクリックし、キー名を入力して、 をクリックします。

7. をクリックします。

   ページが表示されます。

8. ページで、配布モードを選択します。

   - **集中型: サーバー側キー生成**。Citrixは集中型オプションを推奨しています。秘密鍵はサーバー上で生成および保存され、ユーザーデバイスに配布されます。
   - **分散型: デバイス側キー生成**。秘密鍵はユーザーデバイス上で生成されます。この分散モードではSCEPを使用し、`keyUsage keyEncryption` 拡張機能を持つRA暗号化証明書と、`keyUsage digitalSignature` 拡張機能を持つRA署名証明書が必要です。同じ証明書を暗号化と署名の両方に使用できます。

9. をクリックします。

   「**裁量的CA: オンライン証明書ステータスプロトコル (OCSP)**」ページが表示されます。

   「**裁量的CA: オンライン証明書ステータスプロトコル (OCSP)**」ページで、次の操作を行います。

- このCAによって署名された証明書に`AuthorityInfoAccess` (RFC2459) 拡張機能を追加する場合は、「**このCAのOCSPサポートを有効にする**」を「**オン**」に設定します。この拡張機能は、`https://<server>/<instance>/ocsp`にあるCA OCSPレスポンダーを指します。
- OCSPサポートを有効にした場合は、OCSP署名CA証明書を選択します。この証明書リストは、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。

裁量的CAがPKIエンティティテーブルに表示されます。

資格情報プロバイダー

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、スタンドアロンであるか (つまり、そのままデバイスにプッシュされるか) にかかわらず行われます。

デバイスの登録は、証明書のライフサイクルを制約します。つまり、XenMobile は登録前に証明書を発行しませんが、登録の一部として一部の証明書を発行する場合があります。さらに、1つ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、登録が取り消されると失効します。管理関係が終了すると、有効な証明書は残りません。

1つの資格情報プロバイダー構成を複数の場所で使用することで、1つの構成が同時に任意の数の証明書を管理できます。この統合は、展開リソースと展開に基づいています。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に展開される場合、Pの発行設定によってDに展開される証明書が決定されます。同様に、Cが更新されるとDの更新設定が適用されます。また、Cが削除されたりDが取り消されたりすると、Dの失効設定も適用されます。

これらのルールに従って、XenMobile の資格情報プロバイダー構成は以下を決定します。

- 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) するか。
- 発行または回復のパラメーター。たとえば、キーサイズ、キーアルゴリズム、証明書拡張機能などの証明書署名要求 (CSR) パラメーター。
- 証明書がデバイスに配信される方法。
- 失効条件。管理関係が切断されると、XenMobile のすべての証明書は失効しますが、構成によってより早い失効が指定される場合があります。たとえば、関連するデバイス構成が削除さ

れたときに証明書を失効させるように構成で指定できます。さらに、特定の条件下では、XenMobile での関連証明書の失効がバックエンドの公開鍵インフラストラクチャ (PKI) に送信される場合があります。つまり、XenMobile での証明書の失効は、PKI での証明書の失効を引き起こす可能性があります。

- 更新設定。特定の資格情報プロバイダーを通じ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できます。または、それとは別に、有効期限が近づいたときに通知を発行できます。

The availability of configuration options mainly depends on the type of PKI Entity and issuance method that you select for a credential provider.

証明書発行方法

署名によって証明書を取得できます。これは発行方法として知られています。

この方法では、発行には新しい秘密鍵の作成、CSR の作成、および署名のために CSR を認証局 (CA) に提出することが含まれます。XenMobile は、MS Certificate Services エンティティと Discretionary CA エンティティの両方で署名方法をサポートしています。

資格情報プロバイダーは、発行の署名メソッドを使用します。

証明書の配信

XenMobileでは、証明書の配信モードとして、集中型と分散型の2つが利用可能です。分散型モードは、Simple Certificate Enrollment Protocol (SCEP) を使用し、クライアントがプロトコルをサポートしている状況 (iOSのみ) でのみ利用できます。分散型モードは、一部の状況で必須です。

資格情報プロバイダーが分散型 (SCEPアシスト) 配信をサポートするには、特別な構成手順が必要です。それは、登録機関 (RA) 証明書の設定です。RA証明書は必須です。なぜなら、SCEPプロトコルを使用する場合、XenMobileは実際の証明機関に対するデリゲート (登録者) として機能するからです。XenMobileは、そのように機能する権限があ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、前述の証明書をXenMobileにアップロードすることで確立されます。

2つの異なる証明書ロールが必要です (ただし、1つの証明書で両方の要件を満たすことができます): RA署名とRA暗号化。これらのロールの制約は次のとおりです。

- 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、証明書をXenMobileにアップロードし、その後資格情報プロバイダー内でそれらにリンクします。

資格情報プロバイダーは、証明書ロール用に構成された証明書を持っている場合にのみ、分散型配信をサポートすると見なされます。各資格情報プロバイダーを、集中型モードを優先するか、分散型モードを優先するか、または分散型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よって異なります。コンテキストが分散型モードをサポートしていないが、資格情報プロバイダーがこのモードを必須とする場合、展開は失敗します。同様に、コンテキストが分散型モードを必須とするが、資格情報プロバイダーが分散型モードをサポートしていない場合、展開は失敗します。その他のすべての場合において、優先設定が尊重されます。

次の表は、XenMobile全体でのSCEPの配布を示しています。

コンテキスト	SCEP対応	SCEP必須
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構成	いいえ	いいえ
Windowsタブレット登録	いいえ	いいえ
Windowsタブレット構成	いいえ。ただし、Windows 10およびWindows 11でサポートされているWi-Fiデバイスポリシーは除きます。	いいえ

証明書の失効

失効には3つの種類があります。

- **内部失効:** 内部失効は、XenMobileによって維持される証明書ステータスに影響します。XenMobileは、提示された証明書を評価する際、または証明書のOCSPステータス情報を提供する際に、このステータスを考慮します。資格情報プロバイダーの構成は、さまざまな条件下でこのステータスがどのように影響を受けるかを決定します。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、証明書を失効済みとしてフラグ付けするように指定する場合があります。

- **外部伝播失効:** Revocation XenMobileとも呼ばれるこの種類の失効は、外部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の構成で定義された条件の下で、XenMobileが内部的に証明書を失効させると、PKI上で証明書が失効します。
- **外部誘発失効:** Revocation PKIとも呼ばれるこの種類の失効も、外部PKIから取得した証明書にのみ適用されます。XenMobileは、特定の証明書ステータスを評価するたびに、そのステータスについてPKIに照会します。証明書が失効している場合、XenMobileは内部的に証明書を失効させます。このメカニズムはOCSPプロトコルを使用します。

これら3つの種類は排他的ではなく、むしろ組み合わせて適用されます。外部失効または独立した発見が内部失効を引き起こす可能性があります。内部失効は、外部失効に影響を与える可能性があります。

証明書の更新

証明書の更新とは、既存の証明書の失効と、別の証明書の発行を組み合わせたものです。

XenMobileは、発行が失敗した場合のサービス中断を避けるため、以前の証明書を失効させる前に、まず新しい証明書を取得しようとします。分散型（SCEP対応）配信の場合、失効は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発生します。それ以外の場合、失効は新しい証明書がデバイスに送信される前に発生します。この失効は、証明書のインストールの成否とは無関係です。

失効構成では、特定の期間（日数）を指定する必要があります。デバイスが接続すると、サーバーは証明書の`NotAfter`日付が現在の日付から指定された期間を引いた日付よりも後であるかどうかを確認します。証明書がその条件を満たしている場合、XenMobileは証明書の更新を試みます。

資格情報プロバイダーを作成する

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選択する発行エンティティと発行方法によって異なります。内部エンティティまたは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の内部にある裁量エンティティは、内部エンティティです。裁量エンティティの発行方法は常に署名です。署名とは、発行操作ごとにXenMobileがエンティティに選択されたCA証明書で新しいキーペアに署名することを意味します。キーペアがデバイスで生成されるかサーバーで生成されるかは、選択した配布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が含まれます。

1. XenMobileコンソールで、右上隅の歯車アイコンをクリックし、次に **>** をクリックします。
2. ページで、 をクリックします。

ページが表示されます。

3. ページで、次の操作を行います。

   - **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、後でXenMobileコンソールの他の部分で構成を識別するために使用されます。
   - **説明:** 資格情報プロバイダーを説明します。このフィールドはオプションですが、説明によってこの資格情報プロバイダーに関する有用な詳細を提供できます。
   - **発行エンティティ:** 証明書発行エンティティをクリックします。
   - **発行方法:** 構成されたエンティティから証明書を取得するためにシステムが使用する方法として、 または をクリックします。クライアント証明書認証には、 を使用します。
   - リストが利用可能な場合は、資格情報プロバイダーのPKIエンティティの下に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、 **>** でMicrosoft Certificate Servicesエンティティが追加されたときに利用可能になります。

4. をクリックします。

   ページが表示されます。

5. 「**Credential Providers: Certificate Signing Request**」ページで、証明書構成に従っ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:**」キーペアのサイズをビット単位で入力します。このフィールドは必須です。

     許容される値は、キーの種類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。基盤となるハードウェアとソフトウェアに依存する誤検出を避けるため、XenMobileはキーサイズを強制しません。運用環境でアクティブ化する前に、必ずテスト環境で資格情報プロバイダーの構成を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クリックします。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。新しい証明書サブジェクトの識別名 (DN) を入力します。例: `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の場合は、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:**」SHA256withRSA
- 「**サブジェクト名:**」`cn=$user.username`

- 「**Subject alternative names**」テーブルにエントリを追加するには、「**Add**」をクリックします。代替名の種類を選択し、2番目の列に値を入力します。

  クライアント証明書認証の場合は、以下を指定します。

  - 「**種類:**」ユーザープリンシパル名
  - 「**値:**」`$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: 配信ページが表示されます。

7. **資格情報プロバイダー: 配信**ページで、次の操作を行います。

   - **発行CA証明書**リストで、提示されたCA証明書をクリックします。資格情報プロバイダーは裁量的な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自体で構成されたCA証明書になります。CA証明書は、外部エンティティを使用する構成との整合性のためにここに表示されます。
   - **配信モードの選択**で、キーを生成および配布する次のいずれかの方法をクリックします。
     - **集中型を優先: サーバー側でのキー生成:** Citrixはこの集中型オプションを推奨します。これはXenMobileがサポートするすべてのプラットフォームをサポートし、Citrix Gateway認証を使用する場合に必要です。秘密キーはサーバーで生成および保存され、ユーザーデバイスに配布されます。
     - **分散型を優先: デバイス側でのキー生成:** 秘密キーはユーザーデバイスで生成および保存されます。この分散モードではSCEPを使用し、keyUsage keyEncryptionを持つRA暗号化証明書と、KeyUsage digitalSignatureを持つRA署名証明書が必要です。同じ証明書を暗号化と署名の両方に使用できます。
     - **分散型のみ: デバイス側でのキー生成:** このオプションは「分散型を優先: デバイス側でのキー生成」と同じように機能しますが、「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り利用できない場合はオプションがありません。

分散型を優先: デバイス側でのキー生成または**分散型のみ: デバイス側でのキー生成**を選択した場合、RA署名証明書とRA暗号化証明書をクリックします。同じ証明書を両方に使用できます。これらの証明書に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ページが表示されます。このページでは、このプロバイダー構成を通じて発行された証明書をXenMobileが内部的に失効済みとしてフラグ付け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、次の操作を行います。

   - **発行済み証明書の失効**で、証明書を失効させる時期を示すオプションのいずれかを選択します。
   - 証明書が失効したときにXenMobileに通知を送信させるには: **通知の送信**の値を**オン**に設定し、通知テンプレートを選択します。
   - XenMobileから証明書が失効されたときにPKIで証明書を失効させるには: **Revoke certificate on PKI** を **On** に設定し、**Entity list** でテンプレートをクリックします。Entity listには、失効機能を持つすべての利用可能なエンティティが表示されます。XenMobileから証明書が失効されると、Entity listから選択されたPKIに失効呼び出しが送信されます。

10. **Next** をクリックします。

    Credential Providers: Revocation PKI ページが表示されます。このページでは、証明書が失効された場合にPKIで実行するアクションを特定します。通知メッセージを作成するオプションもあります。

11. **Credential Providers: Revocation PKI** ページで、PKIから証明書を失効させたい場合は、次の操作を行います。

    - **Enable external revocation checks** の設定を **On** に変更します。失効PKIに関連する追加フィールドが表示されます。
    - **OCSP responder CA certificate** リストで、証明書のサブジェクトの識別名 (DN) をクリックします。

      DNフィールドの値にはXenMobileマクロを使用できます。例: `CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation`

    - **When certificate is revoked** リストで、証明書が失効されたときにPKIエンティティに対して実行する次のいずれかのアクションをクリックします。

      - 何もしない。

    - 証明書を更新する。
    - デバイスを失効させてワイプする。

- 証明書が失効されたときにXenMobileに通知を送信させるには: **Send notification** の値を **On** に設定します。

  次の2つの通知オプションから選択できます。

- **Select notification template** を選択すると、事前に作成された通知メッセージを選択し、それをカスタマイズできます。これらのテンプレートは、Notification templateリストにあります。
- **Enter notification details** を選択すると、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とメッセージを提供するだけでなく、通知の送信頻度を設定できます。

12. **次へ**をクリックします。

    Credential Providers: Renewalページが表示されます。このページでは、XenMobileを次のように構成できます。

    - 証明書を更新します。オプションで、更新時に通知を送信したり、すでに期限切れの証明書を操作から除外したりできます。
    - 期限切れが近い証明書に対して通知を送信します（更新前の通知）。

13. **Credential Providers: Renewal**ページで、証明書の期限が切れたときに更新する場合は、次の操作を行います。

    証明書の期限切れ時に更新を**オン**に設定します。追加のフィールドが表示されます。

    - **証明書の有効期限が近づいたときに更新**フィールドで、証明書を更新する有効期限までの日数を入力します。
    - オプションで、**すでに期限切れの証明書は更新しない**を選択します。この場合、「すでに期限切れ」とは、`NotAfter`の日付が過去のものであり、失効したわけではないことを意味します。XenMobileは、内部的に失効した証明書を更新しません。

    証明書が更新されたときにXenMobileに通知を送信させるには、**通知を送信**を**オン**に設定します。証明書の期限が近づいたときにXenMobileに通知を送信させるには、**証明書の期限切れが近づいたときに通知**を**オン**に設定します。 いずれかの選択肢について、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:** 事前に作成された通知メッセージを選択し、カスタマイズできます。これらのテンプレートは、通知テンプレートリストにあります。

- **通知の詳細を入力:** 独自の通知メッセージを作成します。受信者のメールアドレス、メッセージ、および通知を送信する頻度を指定します。

証明書の有効期限が近づいたときに通知フィールドで、通知を送信する証明書の有効期限までの日数を入力します。

14. **保存**をクリックします。

資格情報プロバイダーは、資格情報プロバイダーテーブルに表示されます。

APNs証明書

> **重要:**
>
> APNsレガシーバイナリプロトコルに対するAppleのサポートは、March 31, 2021をもって終了します。Appleは、代わりにHTTP/2ベースのAPNsプロバイダーAPIを使用することを推奨しています。リリース10.13.0以降、XenMobile ServerはHTTP/2ベースのAPIをサポートしています。詳細については、`<https://developer.apple.com/>`のニュース更新「Apple Push Notification Service Update」を参照してください。APNsへの接続確認については、Connectivity checksを参照してください。

> XenMobile®でiOSおよびmacOSデバイスを登録および管理するには、AppleからApple Push Notificationサービス（APNs）証明書を設定します。

ワークフローの概要:

- **ステップ1:** 次のいずれかの方法で証明書署名要求 (CSR) を作成します:
  - macOSのキーチェーンアクセスを使用してCSRを作成する(#create-a-csr-by-using-keychain-access-on-macos) (Citrix®推奨)
  - Microsoft IISを使用してCSRを作成する(#create-a-csr-by-using-microsoft-iis)
  - OpenSSLを使用してCSRを作成する(#create-a-csr-by-using-openssl)
- **ステップ2:** XenMobile ToolsでCSRに署名する
- **ステップ3:** 署名済みCSRをAppleに提出してAPNs証明書を取得する
- **ステップ4:** ステップ1で使用したのと同じコンピューターを使用して、CSRを完了し、PKCS #12ファイルをエクスポートする:

- macOSのキーチェーンアクセスを使用してPKCS #12ファイルを作成する(#create-a-pkcs-12-file-by-using-keychain-access-on-macos)
- Microsoft IISを使用してPKCS #12ファイルを作成する(#create-a-pkcs-12-file-by-using-microsoft-iis)
- OpenSSLを使用してPKCS #12ファイルを作成する(#create-a-pkcs-12-file-by-using-openssl)

- **ステップ 5:** APNs証明書をXenMobileにインポートする
- **ステップ 6:** APNs証明書を更新する

証明書署名要求を作成する

macOSのキーチェーンアクセスを使用してCSRを作成することをお勧めします。Microsoft IISまたはOpenSSLを使用してCSRを作成することもできます。

重要:

- 証明書の作成に使用するApple IDについて:
  - Apple IDは、個人用ではなく企業用である必要があります。
  - 証明書の作成に使用するApple IDを記録してください。
  - 証明書を更新するには、同じ組織名とApple IDを使用してください。異なるApple IDを使用して証明書を更新すると、デバイスの再登録が必要になります。
- 誤って、または意図的に証明書を取り消した場合、デバイスを管理する機能が失われます。
- iOS Developer Enterprise Programを使用してモバイルデバイスマネージャープッシュ証明書を作成した場合: 移行された証明書に関するすべてのアクションは、Apple Push Certificates Portalで処理するようにしてください。

macOSのキーチェーンアクセスを使用してCSRを作成する

1. macOSを実行しているコンピューターで、**アプリケーション > ユーティリティ**からキーチェーンアクセスアプリを起動します。
2. **キーチェーンアクセス**メニューを開き、**証明書アシスタント > 認証局に証明書を要求**をクリックします。
3. 証明書アシスタントは、次の情報の入力を求めます:

- **メールアドレス:** 証明書の管理を担当する個人またはロールアカウントのメールアドレス。
- **共通名:** 証明書の管理を担当する個人またはロールアカウントの共通名。
- **CAメールアドレス:** 認証局のメールアドレス。

4. **ディスクに保存**と**キーペア情報を指定する**オプションを選択し、**続行**をクリックします。
5. CSRファイルの名前を入力し、ファイルをコンピューターに保存してから、**保存**をクリックします。
6. キーペア情報を指定します: **キーサイズ**を2048ビット、**RSAアルゴリズム**を選択し、**続行**をクリックします。CSRファイルは、APNs証明書プロセスの一部としてアップロードする準備ができました。
7. 証明書アシスタントがCSRプロセスを完了したら、**完了**をクリックします。
8. 続行するには、CSRに署名します。

Microsoft IISを使用してCSRを作成する

APNs証明書要求を生成するための最初のステップは、証明書署名要求 (CSR) を作成することです。Windowsの場合、Microsoft IISを使用してCSRを生成します。

1. Microsoft IISを開きます。
2. IISのサーバー証明書アイコンをダブルクリックします。
3. **サーバー証明書**ウィンドウで、**証明書要求の作成**をクリックします。
4. 適切な識別名 (DN) 情報を入力し、**次へ**をクリックします。
5. 暗号化サービスプロバイダーには**Microsoft RSA SChannel Cryptographic Provider**を、ビット長には**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、CSRを保存する場所を指定してから、 をクリックします。
7. 続行するには、CSRに署名する。

OpenSSLを使用してCSRを作成する

macOSデバイスまたはMicrosoft IISを使用してCSRを生成できない場合は、OpenSSLを使用します。OpenSSLは、OpenSSL Webサイトからダウンロードしてインストールできます。

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. 証明書の命名情報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。

```
You are about to be asked to enter information that will be
incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a
DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [AU]:US

State or Province Name (full name) [Some-State]:CA

Locality Name (eg, city) []:RWC

Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer

Organizational Unit Name (eg, section) [:Marketing

Common Name (eg, YOUR name) []:John Doe

Email Address []:john.doe@customer.com
```

3. 次のメッセージで、CSR秘密キーのパスワードを入力します。

```
Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

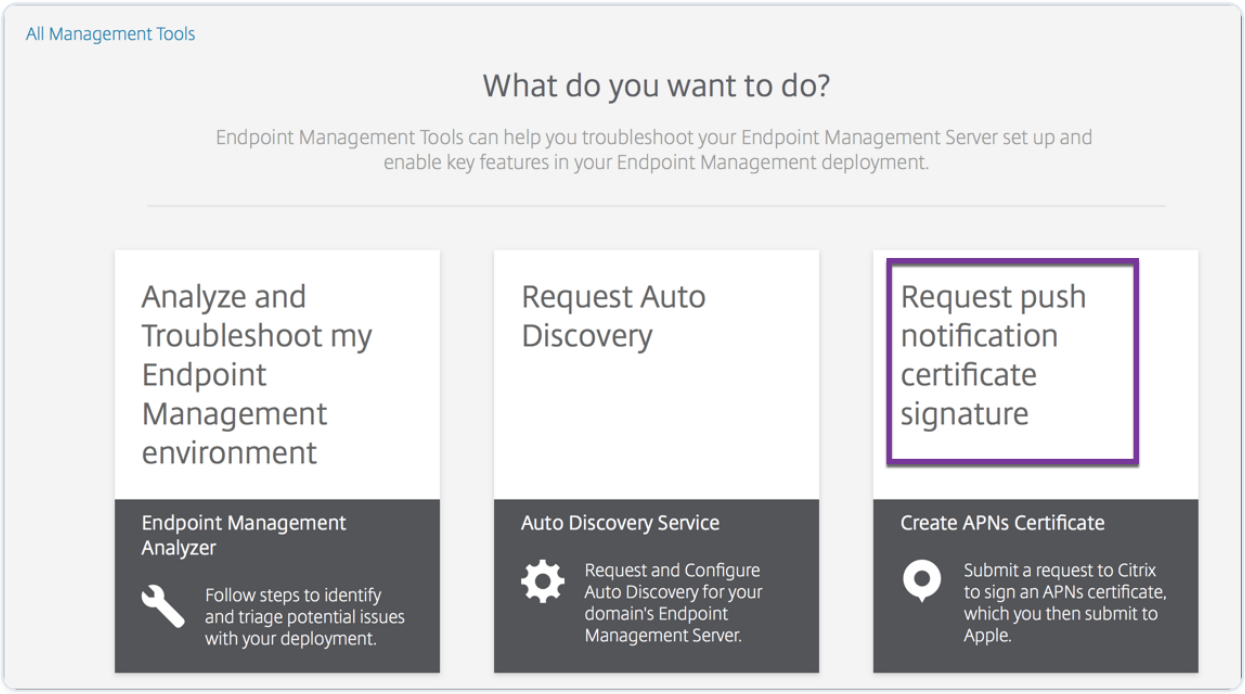
An optional company name []:
```

4. 続行するには、次のセクションで説明されているようにCSRに署名します。

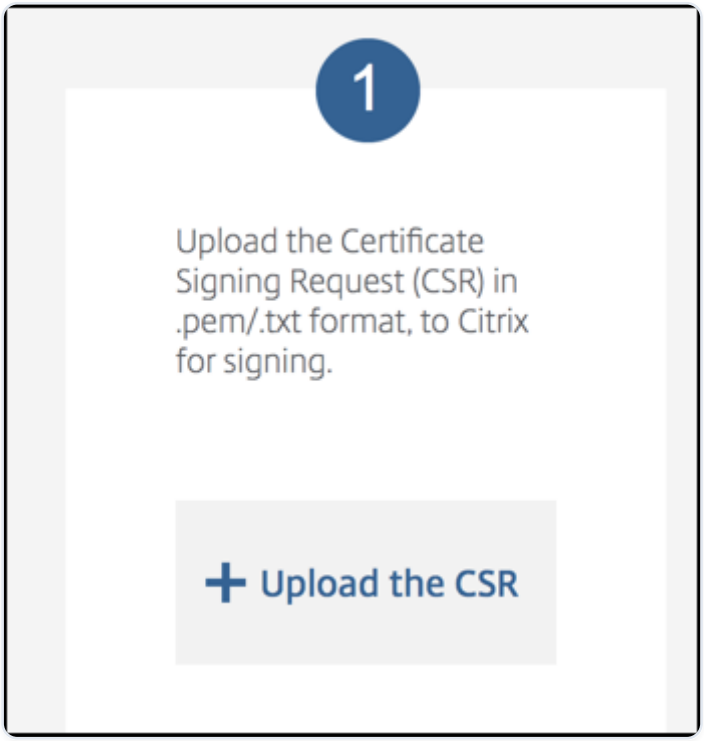
CSRに署名する

XenMobileで証明書を使用するには、署名のためにCitrixに提出します。Citrixは、モバイルデバイス管理署名証明書でCSRに署名し、署名済みファイルを`.plist`形式で返します。

1. ブラウザーで、Endpoint Management Tools Webサイトにアクセスし、 をクリックします。



2. ページで、 をクリックします。



3. 証明書を参照して選択します。

証明書は.pem/.txt形式である必要があります。

4. **Endpoint Management APNs CSR署名**ページで、**署名**をクリックします。CSRが署名され、構成済みのダウンロードフォルダーに自動的に保存されます。
5. 続行するには、次のセクションで説明するように、署名済みCSRを送信します。

署名済みCSRをAppleに提出してAPNs証明書を取得する

Citrixから署名済み証明書署名要求（CSR）を受け取ったら、そのCSRをAppleに提出して、XenMobileにインポートするために必要なAPNs証明書を取得します。

> **注：**
>
> 一部のユーザーから、Apple Push Portalへのログインに関する問題が報告されています。代替策として、Apple Developer Portalにログオンしてから、次の手順に従ってください。

1. ブラウザーで、Apple Push Certificates Portalにアクセスします。
2. **証明書の作成**をクリックします。
3. Appleで初めて証明書を作成する場合：**これらの利用規約を読み、同意します**チェックボックスをオンにしてから、**同意**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済みCSRを参照して、**アップロード**をクリックします。確認メッセージが表示され、アップロードが成功したことが示されます。
5. **ダウンロード**をクリックして、.pem証明書を取得します。
6. 続行するには、次のセクションで説明するように、CSRを完了し、PKCS #12ファイルをエクスポートします。

CSRを完了し、PKCS #12ファイルをエクスポートする

Apple から APNs 証明書を受け取ったら、Keychain Access、Microsoft IIS、または OpenSSL に戻り、証明書を PCKS #12 ファイルにエクスポートします。

PKCS #12 ファイルには、APNS 証明書ファイルと秘密鍵が含まれています。PFX ファイルの拡張子は通常 .pfx または .p12 です。.pfx ファイルと .p12 ファイルは互換性があります。

> **重要:**

Citrix では、個人キーと公開キーをローカルシステムから保存またはエクスポートすることをお勧めします。APNs 証明書を再利用するには、これらのキーが必要です。同じキーがない場合、証明書は無効になり、CSR と APNs のプロセス全体を繰り返す必要があります。

macOS の Keychain Access を使用して PKCS #12 ファイルを作成する

重要:

このタスクには、CSR の生成に使用したのと同じ macOS デバイスを使用してください。

1. デバイスで、Apple から受け取ったプロダクション ID (.pem) 証明書を見つけます。
2. Keychain Access アプリケーションを起動し、**ログイン > マイ証明書**タブに移動します。プロダクト ID 証明書を開いているウィンドウにドラッグアンドドロップします。
3. 証明書をクリックし、左矢印を展開して、証明書に関連付けられた秘密鍵が含まれていることを確認します。
4. 証明書を PCKS #12 (.pfx) 証明書にエクスポートするには、証明書と秘密鍵を選択し、右クリックして**2 項目を書き出す**を選択します。
5. XenMobile で使用するために、証明書ファイルに一意の名前を付けます。名前にスペースを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択し、.pfx ファイル形式を選択して、**保存**をクリックします。
6. 証明書をエクスポートするためのパスワードを入力します。Citrix では、一意の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できるように、証明書とパスワードを安全に保管してください。
7. Keychain Access アプリは、ログインパスワードまたは選択したキーチェーンのパスワードを要求します。パスワードを入力し、**OK**をクリックします。保存された証明書は、XenMobile Server で使用できるようになりました。
8. 続行するには、「XenMobile に APNs 証明書をインポートする」を参照してください。

Microsoft IIS を使用して PKCS #12 ファイルを作成する

重要:

CSR を生成したのと同じ IIS サーバーをこのタスクに使用してください。

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、**証明書要求の完了**をクリックします。
4. Apple からの Certificate.pem ファイルを参照します。次に、フレンドリ名または証明書名を入力し、**OK**をクリックします。名前にスペースを含めないでください。
5. 手順 4 で特定した証明書を選択し、**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、**OK**をクリックします。

   証明書を XenMobile にインポートするには、そのパスワードが必要です。
7. .pfx 証明書を、XenMobile をインストールする予定のサーバーにコピーします。
8. 続行するには、「APNs 証明書を XenMobile にインポートする」を参照してください。

OpenSSL を使用して PKCS #12 ファイルを作成する

OpenSSL を使用して CSR を作成した場合、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 の秘密キーです。`APNs_Certificate.pem` は Apple から受け取ったばかりの証明書です。

   ```
   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度使用するため、覚えておいてください。
3. .pfx 証明書ファイルの場所をメモします。次に、コンソールを使用してファイルをアップロードできるように、ファイルをXenMobile Serverにコピーします。
4. 続行するには、次のセクションで説明されているように、APNs証明書をXenMobileにインポートします。

APNs証明書をXenMobileにインポートする

新しいAPNs証明書を受け取ったら、APNs証明書をXenMobileにインポートして、初めて証明書を追加するか、証明書を置き換えます。

1. XenMobileコンソールで、**設定 > 証明書**に移動します。
2. **インポート > キーストア**をクリックします。
3. **用途**から、**APNs**を選択します。

4. コンピューター上の.pfxまたは.p12ファイルを参照します。
5. パスワードを入力し、**インポート**をクリックします。

XenMobileの証明書の詳細については、証明書と認証を参照してください。

APNs証明書を更新する

> **重要:**
>
> 更新プロセスで別のApple IDを使用する場合、ユーザーデバイスを再登録する必要があります。
>
> APNs証明書を更新するには、証明書を作成する手順を実行し、Apple Push Certificates Portalにアクセスします。そのポータルを使用して新しい証明書をアップロードします。ログイン後、既存の証明書または以前のApple開発者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。

証明書ポータルで証明書を更新する際の唯一の違いは、**Renew**をクリックすることです。サイトにアクセスするには、証明書ポータルで開発者アカウントを持っている必要があります。証明書を更新するには、同じ組織名とApple IDを使用してください。

XenMobileコンソールでAPNs証明書の有効期限を確認するには、**Settings > Certificates**に移動します。証明書の有効期限が切れても、失効させないでください。

1. Microsoft IIS、キーチェーンアクセス (macOS)、またはOpenSSLを使用してCSRを生成します。CSRの生成について詳しくは、「証明書署名要求の作成」を参照してください。
2. ブラウザでEndpoint Management Toolsにアクセスします。次に、**Request push notification certificate signature**をクリックします。
3. **+ Upload the CSR**をクリックします。
4. ダイアログボックスでCSRに移動し、**Open**をクリックして、**Sign**をクリックします。
5. `.plist`ファイルを受信したら、保存します。
6. ステップ3のタイトルで、**Apple Push Certificates Portal**をクリックしてサインオンします。
7. 更新する証明書を選択し、**Renew**をクリックします。
8. `.plist`ファイルをアップロードします。出力として.pemファイルが生成されます。.pemファイルを保存します。

9. その.pemファイルを使用して、CSRを完了します（ステップ1でCSRを作成した方法に従って）。
10. 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、次のように構成を完了します。

1. **Settings > Certificates > Import**に移動します。
2. 「**インポートメニュー**」から「**キーストア**」を選択します。
3. 「**キーストアの種類**」メニューから「**PKCS #12**」を選択します。
4. 「**用途**」から「**APNs**」を選択します。

   「証明書のインポート」ダイアログボックス(/en-us/xenmobile/server/media/import-apns-certificate.png)
5. 「**キーストアファイル**」で「**参照**」をクリックし、ファイルに移動します。
6. 「**パスワード**」に証明書のパスワードを入力します。
7. オプションの「**説明**」を入力します。
8. 「**インポート**」をクリックします。

XenMobileは「**証明書**」ページにリダイレクトします。「**名前**」、「**状態**」、「**有効期間開始**」、「**有効期間終了**」の各フィールドが更新されます。

Citrix FilesでのシングルサインオンのためのSAML

> **免責事項:**

> ShareFile (現 Progress) がサポートを終了した場合、この機能は非推奨となります。

> XenMobile® と ShareFile を構成して、Security Assertion Markup Language (SAML) を使用し、Citrix Files モバイルアプリへのシングルサインオン (SSO) アクセスを提供できます。この機能には以下が含まれます。

- MAM SDK が有効になっている、または MDX Toolkit を使用してラップされた Citrix Files アプリ
- Webサイト、Outlookプラグイン、同期クライアントなどの非ラップ型Citrix Filesクライアント
- **ラップされた Citrix Files アプリの場合**。Citrix Files モバイルアプリを介して Citrix Files にログオンするユーザーは、ユーザー認証と SAML トークンの取得のために Secure Hub にリダイ

レクトされます。認証が成功すると、Citrix Files モバイルアプリは SAML トークンを ShareFile に送信します。最初のログオン後、ユーザーは SSO を介して Citrix Files モバイルアプリにアクセスできます。また、毎回ログオンすることなく、ShareFile から Secure Mail のメールにドキュメントを添付することもできます。

- **非ラップ型 Citrix Files クライアントの場合。**Webブラウザまたはその他の Citrix Files クライアントを使用して Citrix Files 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 はユーザーを認証し、ユーザーは SAML トークンを取得して ShareFile に送信します。最初のログオン後、ユーザーは毎回ログオンすることなく、SSO を介して Citrix Files クライアントにアクセスできます。

XenMobile を ShareFile への SAML ID プロバイダー (IdP) として使用するには、この記事で説明されているように、XenMobile をエンタープライズアカウントで使用するように構成する必要があります。または、XenMobile をストレージゾーンコネクタでのみ動作するように構成することもできます。詳細については、「XenMobile で ShareFile を使用する」を参照してください。

詳細な参照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 と Citrix Files アプリで SSO を構成する前に、以下の前提条件を完了してください。

- MAM SDK または互換性のあるバージョンの MDX Toolkit (Citrix Files モバイルアプリ用)。

  詳細については、「XenMobile の互換性」を参照してください。
- 互換性のあるバージョンの Citrix Files モバイルアプリと Secure Hub。
- ShareFile 管理者アカウント。
- XenMobile と ShareFile 間の接続が確認済みであること。

ShareFile アクセスの構成

ShareFile 用に SAML を設定する前に、次のように ShareFile アクセス情報を提供します。

1. XenMobile Web コンソールで、 **>** の順にクリックします。 構成ページが表示されます。

   ShareFile 構成設定(/en-us/xenmobile/server/media/configure-content-collaboration-saml-for-non-mdx-apps.png)
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る:** ShareFile で SSO を使用できるようにするデリバリーグループを選択または検索します。
- **ShareFile 管理者アカウントのログオン**
- **ユーザー名:** ShareFile 管理者ユーザー名を入力します。このユーザーには管理者権限が必要です。
- **パスワード:** ShareFile 管理者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:** この設定は無効のままにします。ユーザープロビジョニングには ShareFile User Management Tool を使用します。ユーザーアカウントと配布グループのプロビジョニングを参照してください。

3. 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指定された ShareFile アカウントに対して認証されることを確認します。
4. をクリックします。

- XenMobileはShareFileと同期し、ShareFileの設定である**ShareFile Issuer/Entity ID**と**Login URL**を更新します。
- **Configure > ShareFile**ページに**App internal name**が表示されます。その名前は、後述の(#modify-the-citrix-filescom-sso-settings)で説明されている手順を完了するために必要です。

ラップされたCitrix Files MDXアプリのSAMLをセットアップする

ラップされたCitrix Files MDXアプリでのシングルサインオン構成にCitrix Gatewayを使用する必要はありません。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Citrix Filesクライアントのアクセスを構成するには、(/ja-jp/xenmobile/server/authentication/saml-sso-sharefile.html#configure-the-citrix-gateway-for-other-citrix-files-clients)を参照してください。

以下の手順は、iOSおよびAndroidアプリとデバイスに適用されます。ラップされたCitrix Files MDXアプリのSAMLを構成するには、次の手順を実行します。

1. MDX Toolkitを使用して、Citrix Filesモバイルアプリをラップします。MDX Toolkitを使用したアプリのラッピングについて詳しくは、(/ja-jp/mdx-toolkit/10/xmob-mdx-kit-app-wrap-ios.html)を参照してください。
2. XenMobileコンソールで、ラップされたCitrix Filesモバイルアプリをアップロードします。MDXアプリのアップロードについて詳しくは、(/ja-jp/xenmobile/server/apps.html)を参照してください。
3. SAML設定を確認します。以前に構成した管理者ユーザー名とパスワードを使用してShareFileにログオンします。

4. ShareFileとXenMobileが同じタイムゾーンに構成されていることを確認します。XenMobileが構成されたタイムゾーンの正しい時刻を表示し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。

Citrix Filesモバイルアプリを検証する

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Citrix Filesモバイルアプリをダウンロードしてインストールします。
3. Citrix Filesモバイルアプリを起動します。Citrix Filesは、ユーザー名またはパスワードの入力を求めずに起動します。

Secure Mailで検証する

1. ユーザーデバイスで、まだ実行されていない場合は、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、セットアップします。
3. 新しいメールフォームを開き、 をタップします。ユーザー名やパスワードを要求されることなく、メールに添付できるファイルが表示されます。

その他の Citrix Files クライアント向けに Citrix Gateway を構成する

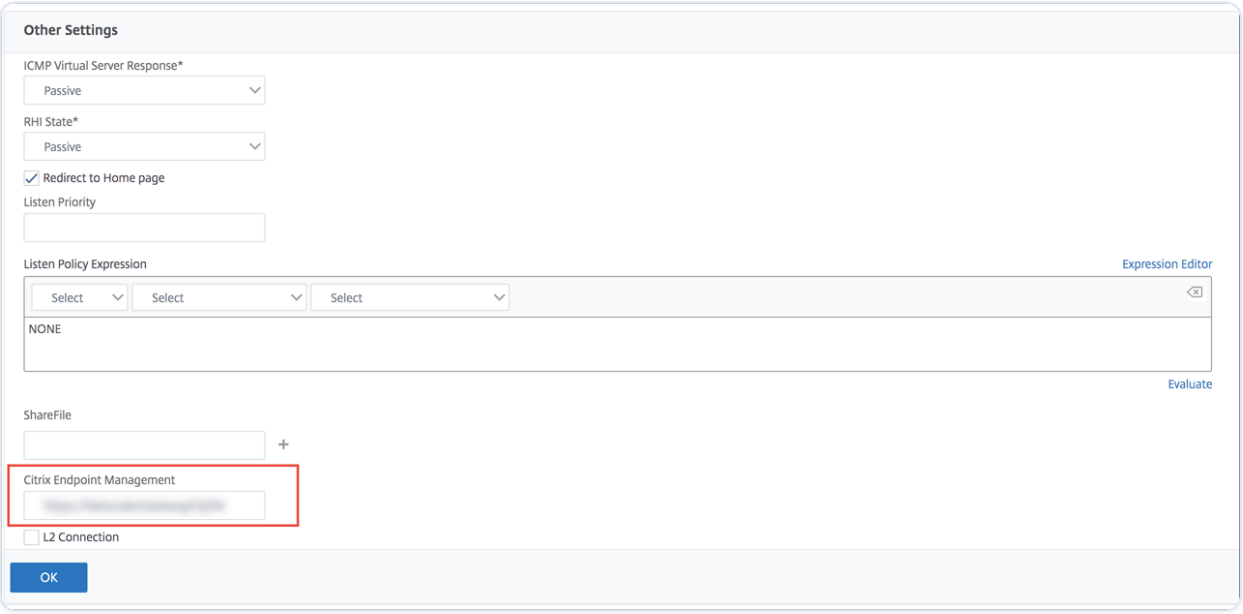
Webサイト、Outlookプラグイン、同期クライアントなどの非ラップ型Citrix Filesクライアントのアクセスを構成するには、Citrix GatewayをSAML IDプロバイダーとしてXenMobileの使用をサポートするように、次のように構成します。

- ホームページのリダイレクトを無効にする。
- Citrix Filesセッションポリシーとプロファイルを作成する。
- Citrix Gateway仮想サーバーで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パスを介して行われる要求のデフォルトの動作を無効にします。このアクションにより、ユーザーは構成されたホームページではなく、元の要求された内部URLを表示できるようになります。

1. XenMobileログオンに使用されるCitrix Gateway仮想サーバーの設定を編集します。Citrix ADCで、 に移動し、 というラベルのチェックボックスをオフにします。



2. (現在はShareFileと呼ばれています) で、XenMobile内部サーバー名とポート番号を入力します。
3. で、XenMobile URLを入力します。お使いのCitrix Gatewayのバージョンでは、古い製品名である**AppController**が参照され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への要求が承認されます。

Citrix Filesセッションポリシーと要求プロファイルを作成する

Citrix Filesセッションポリシーとリクエストプロファイルを作成するには、これらの設定を構成します。

1. Citrix 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、**Citrix Gateway > ポリシー > セッション**をクリックします。
2. セッションポリシーを作成します。**ポリシー**タブで、**追加**をクリックします。
3. **名前**フィールドに「**ShareFile_Policy**」と入力します。
4. **+**ボタンをクリックしてアクションを作成します。**セッションプロファイルの作成**ページが表示されます。

   Citrix Gatewayセッションプロファイル画面(/en-us/xenmobile/server/media/configure-sharefile-ns-session-policy.png)

   これらの設定を構成します。

   - **名前:** 「**ShareFile_Profile**」と入力します。
   - **クライアントエクスペリエンス**タブをクリックし、次にこれらの設定を構成します。

- **ホームページ:** 「**none**」と入力します。
- **セッションタイムアウト（分）:** 「**1**」と入力します。
- **Webアプリケーションへのシングルサインオン:** この設定を選択します。
- **資格情報インデックス: PRIMARY**をクリックします。

- **公開アプリケーション**タブをクリックします。

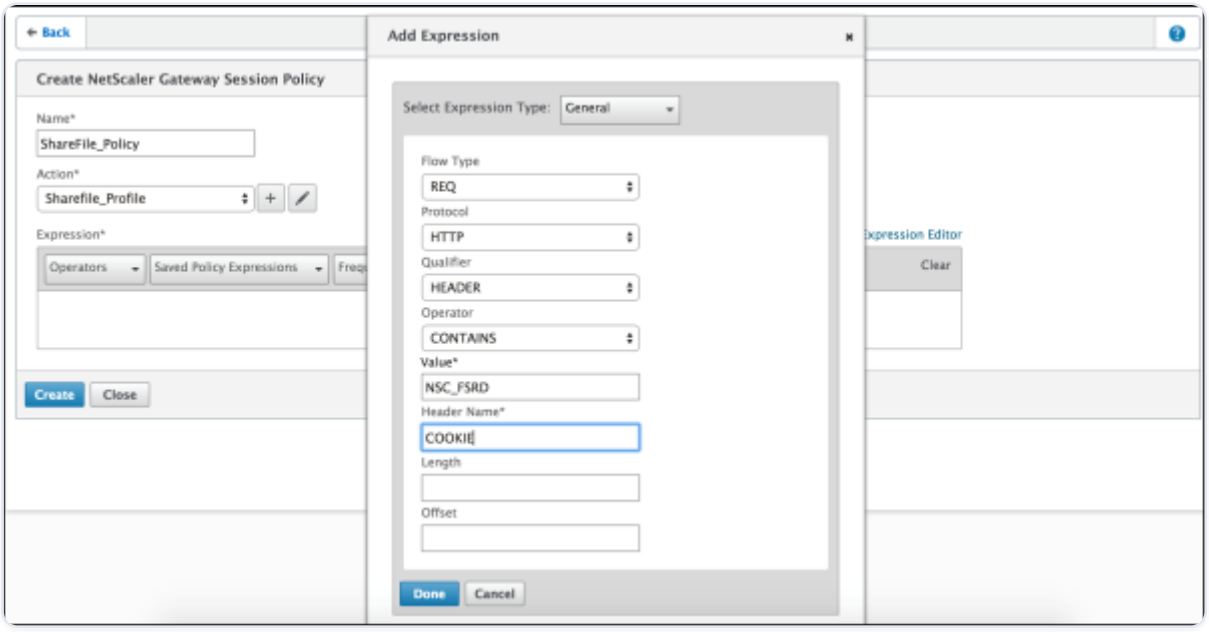
Citrix Gatewayセッションプロファイル画面(/en-us/xenmobile/server/media/configure-sharefile-ns-session-policy-published-apps.png)

これらの設定を構成します。

- **ICA® プロキシ: ON** をクリックします。
- **Webインターフェイスアドレス:** XenMobile ServerのURLを入力します。
- **シングルサインオンドメイン:** Active Directoryのドメイン名を入力します。

  Citrix Gatewayセッションプロファイルを構成する際、**シングルサインオンドメイン**のドメインサフィックスは、LDAPで定義されているXenMobileドメインエイリアスと一致している必要があります。

5. セッションプロファイルを定義するには、**作成**をクリックします。
6. **式エディター**をクリックします。



これらの設定を構成します。

- **値: NSC_FSRD**と入力します。
- **ヘッダー名: COOKIE**と入力します。

7. **作成**をクリックし、次に**閉じる**をクリックします。



Citrix Gateway仮想サーバーでポリシーを構成する

Citrix Gateway仮想サーバーでこれらの設定を構成します。

1. Citrix 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、**Citrix Gateway > 仮想サーバー**をクリックします。
2. **詳細**ペインで、Citrix 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. **構成済みポリシー > セッションポリシー**をクリックし、**バインドの追加**をクリックします。
5. **ShareFile_Policy**を選択します。
6. 選択したポリシーの自動生成された**優先度**番号を編集し、リストされている他のポリシーと比較して最も高い優先度（最小の番号）になるようにします。例:

   VPN仮想サーバーセッションポリシーバインド画面(/en-us/xenmobile/server/media/configure-sharefile-ns-config-policies-on-nsg-vs.png)
7. **完了**をクリックし、実行中のCitrix ADC構成を保存します。

Citrix Files.com SSO設定を変更する

MDXおよび非MDXのCitrix Filesアプリの両方について、以下の変更を行います。

> **重要:**

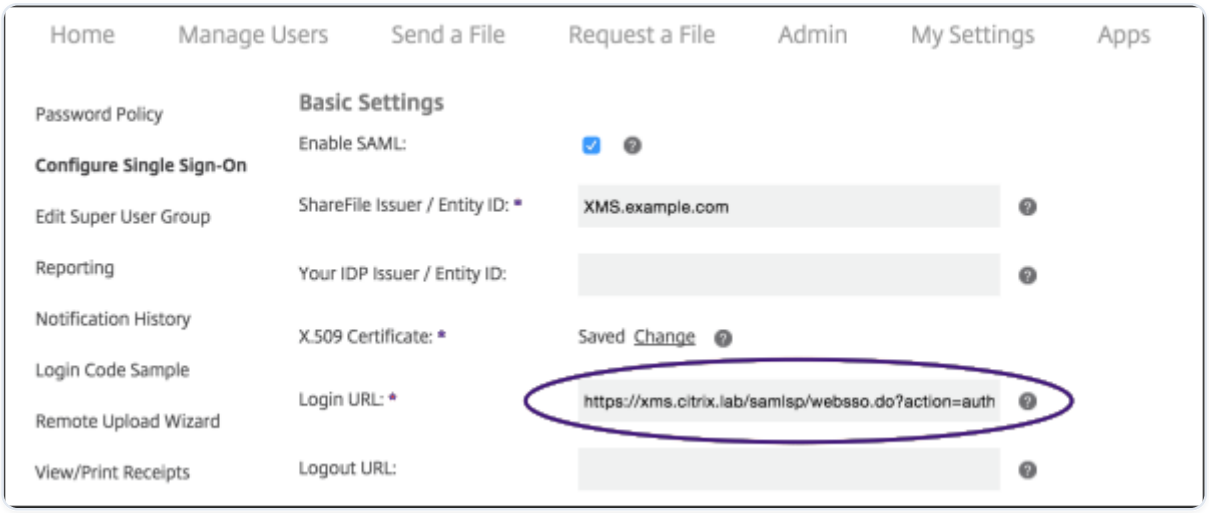
> 内部アプリケーション名に新しい番号が追加されます。

> - Citrix Filesアプリを編集または再作成するたびに
> - XenMobileでShareFile設定を変更するたびに

> その結果、Citrix Files Webサイトのログインurlも更新されたアプリ名を反映するように更新する必要があります。

1. ShareFile管理者として、ShareFileアカウント (`https://<subdomain>.sharefile.com`) にログオンします。
2. ShareFile Webインターフェイスで、**Admin** をクリックし、**Configure Single Sign-on** を選択します。
3. **Login URL** を次のように編集します。

   編集前の**Login URL** の例を次に示します: `https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1`。



   - Citrix Gateway仮想サーバーの外部FQDNと** `/cginfra/https/` ** をXenMobile Server FQDNの前に挿入し、XenMobile FQDNの後に**8443**を追加します。

     編集されたURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=SHareFile_SAML_SP&reqtype=1`

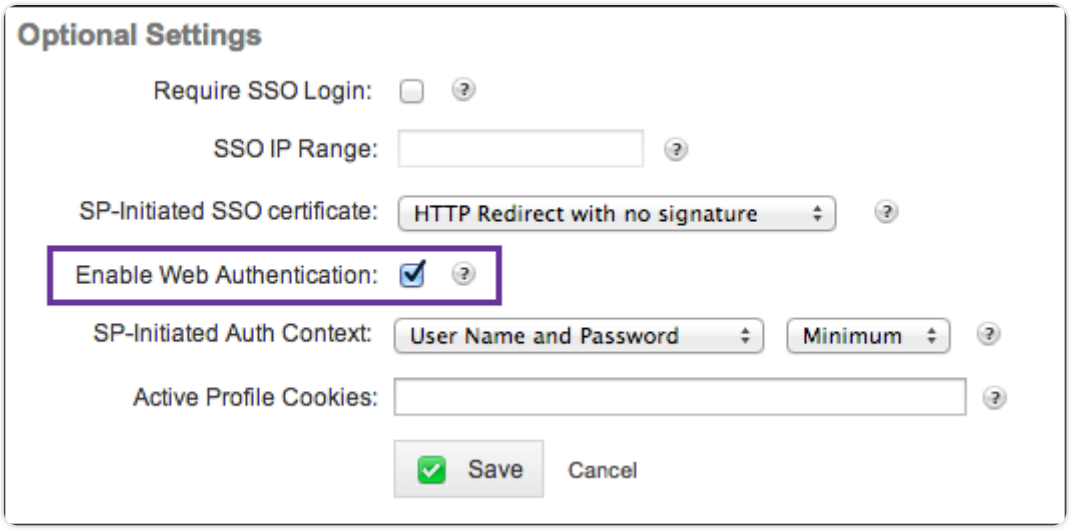
   - パラメーター `&app=ShareFile_SAML_SP` を内部Citrix Filesアプリケーション名に変更します。内部名はデフォルトで `ShareFile_SAML` です。ただし、構成を変更するたびに、内部名に番号が追加されます (`ShareFile_SAML_2`、`ShareFile_SAML_3` など)。**App internal name** は、**Configure > ShareFile** ページで確認できます。

編集されたURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1`

- URLの末尾に `&nssso=true` を追加します。

  最終的なURLの例を次に示します: `https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true`。

4. **Optional Settings** で、**Enable Web Authentication** チェックボックスをオンにします。



構成を検証する

構成を検証するには、次の手順を実行します。

1. ブラウザで `https://<subdomain>sharefile.com/saml/login` にアクセスします。

   Citrix 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、以前の設定を確認してください。

2. 設定したCitrix GatewayおよびXenMobile環境のユーザー名とパスワードを入力します。

   `<subdomain>.sharefile.com` にあるCitrix Filesフォルダーが表示されます。Citrix Filesフォルダーが表示されない場合は、適切なログオン資格情報を入力したことを確認してください。

IDプロバイダーとしてのAzure Active Directory

Azure Active Directory (AAD) をIDプロバイダー (IdP) として構成すると、ユーザーはAzure資格情報を使用してXenMobile®に登録できます。

iOS、Android、Windows 10、およびWindows 11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を介して登録します。この認証方法は、Citrix Secure Hubを介してMDMに登録するユーザーのみが利用できます。MAMに登録するデバイスは、AAD資格情報を使用して認証できません。MDM+MAMでSecure Hubを使用するには、MAM登録にCitrix Gatewayを使用するようにXenMobileを構成します。詳細については、「Citrix GatewayとXenMobile」(/ja-jp/xenmobile/server/authentication/citrix-gateway-and-xenmobile.html)を参照してください。

> > でAzureをIdPとして構成します。 ページは、このバージョンのXenMobileで新しく追加されました。以前のバージョンのXenMobileでは、 **>** でAzureを構成していました。

要件

- バージョンとライセンス
  - iOSまたはAndroidデバイスを登録するには、Secure Hub 10.5.5が必要です。
  - Windows 10およびWindows 11デバイスを登録するには、Microsoft Azure Premiumライセンスが必要です。
- ディレクトリサービスと認証
  - XenMobile Serverは、証明書ベースの認証用に構成されている必要があります。
  - 認証にCitrix ADCを使用している場合、Citrix ADCは証明書ベースの認証用に構成されている必要があります。
  - 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尊重します。
  - XenMobile Server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を介して登録され、XenMobileがAzureをIdPとして使用するように構成されている場合:

1. ユーザーは、Secure Hubに表示されるAzure ADログイン画面で、自分のデバイスにAzure Active Directoryのユーザー名とパスワードを入力します。
2. Azure ADはユーザーを検証し、IDトークンを送信します。
3. Secure HubはIDトークンをXenMobile Serverと共有します。
4. XenMobileはIDトークンと、IDトークンに含まれるユーザー情報を検証します。XenMobileはセッションIDを返します。

Azureアカウントのセットアップ

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、次の変更を行います。

1. カスタムドメインを登録し、ドメインを検証します。詳細については、「Azure Active Directoryにカスタム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、オンプレミスディレクトリをAzure Active Directoryに拡張します。詳細については、「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およびWindows 11デバイスを登録するには、Azureアカウントに次の変更を加えます。

1. MDMをAzure ADの信頼できるパーティにします。これを行うには、**Azure Active Directory > アプリケーション**をクリックし、**追加**をクリックします。
2. ギャラリーから**アプリケーションの追加**を選択します。**モバイルデバイス管理**に移動し、**オンプレミス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クラウドにサインアップした場合でも、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、マルチテナントではないアプリケーションはすべてオンプレミスMDMアプリケーションです。
3. アプリケーションで、XenMobile Serverの検出、利用規約エンドポイント、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。**これらのユーザーのデバイスを管理**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のMDM管理を有効にします。

   Windows 10およびWindows 11デバイスでAzure ADを使用する方法について詳しくは、Microsoftの記事「Azure Active Directory integration with MDM」を参照してください。

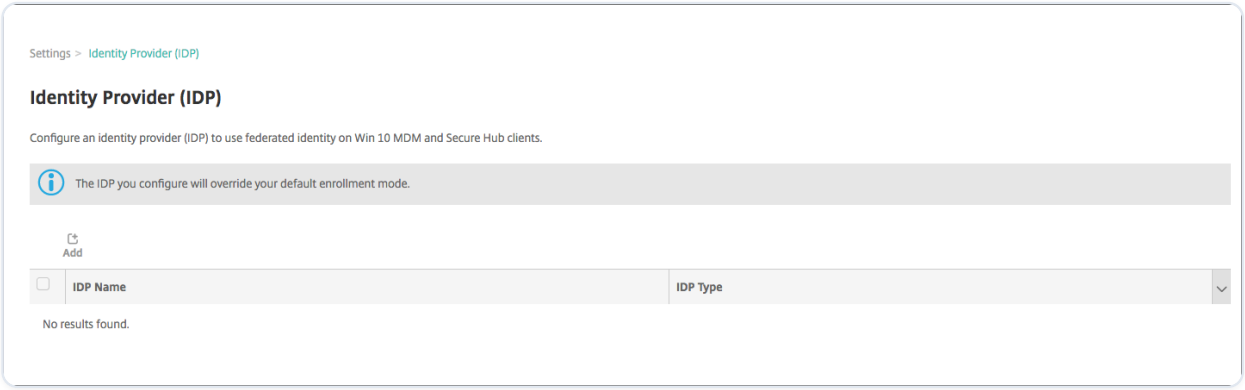
Azure AD を IdP として構成する

1. Azureアカウントから必要な情報を探し出すか、メモしておきます。

   - Azureアプリケーション設定ページからのテナントID。
   - Azure ADを使用してWindows 10およびWindows 11デバイスを登録する場合は、次のものも必要です。

- **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構成ページから取得した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から。

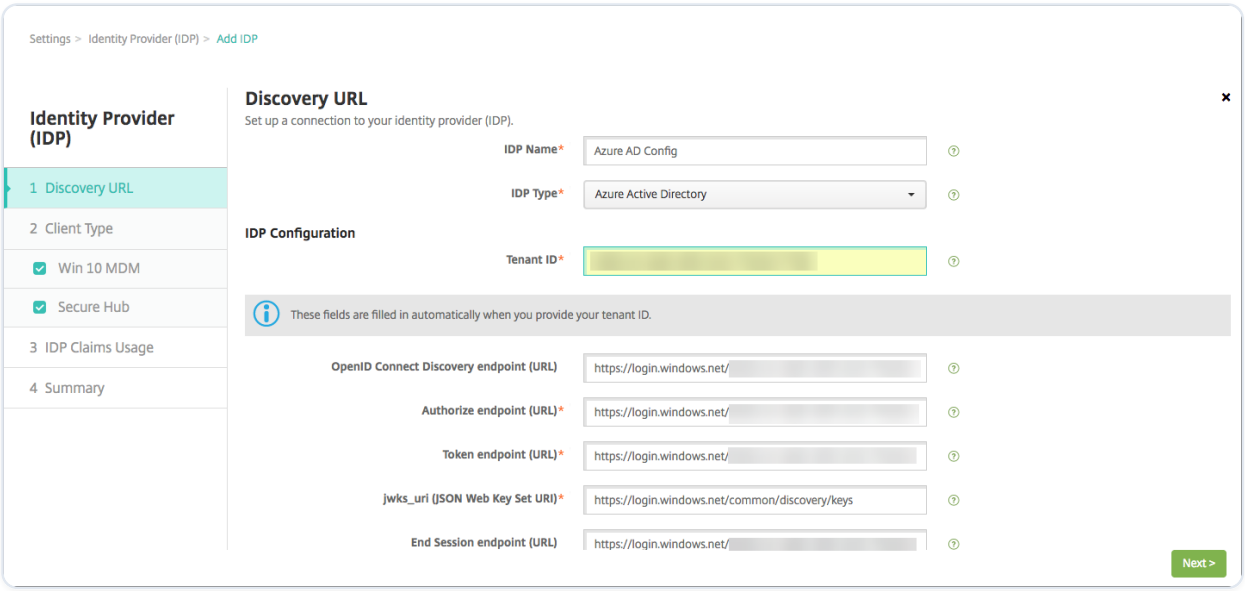
2. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
3. **認証**の下で、**IDプロバイダー (IDP)** をクリックします。**IDプロバイダー**ページが表示されます。



4. **追加**をクリックします。**IDP構成**ページが表示されます。
5. IdPに関する次の情報を構成します。

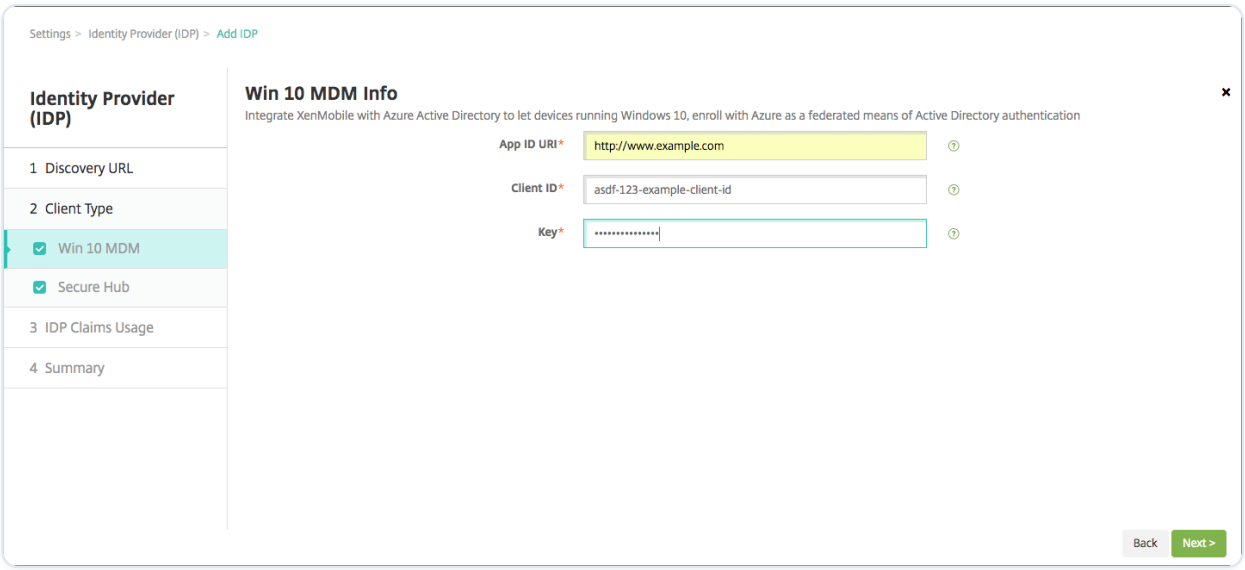
- **IDP 名:** 作成する IdP 接続の名前を入力します。
- **IDP タイプ:** IdP タイプとして Azure Active Directory を選択します。
- **テナント ID:** この値を Azure アプリケーション設定ページからコピーします。ブラウザのアドレスバーで、数字と文字で構成されるセクションをコピーします。

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 `abc123-abc123-abc123` です。



6. 残りのフィールドは自動的に入力されます。入力されたら、**次へ**をクリックします。
7. Azure AD を使用して Windows 10 および Windows 11 デバイスを MDM 登録するために XenMobile を構成するには、次の設定を構成します。このオプションの手順をスキップするには、**Windows MDM** のチェックを外します。

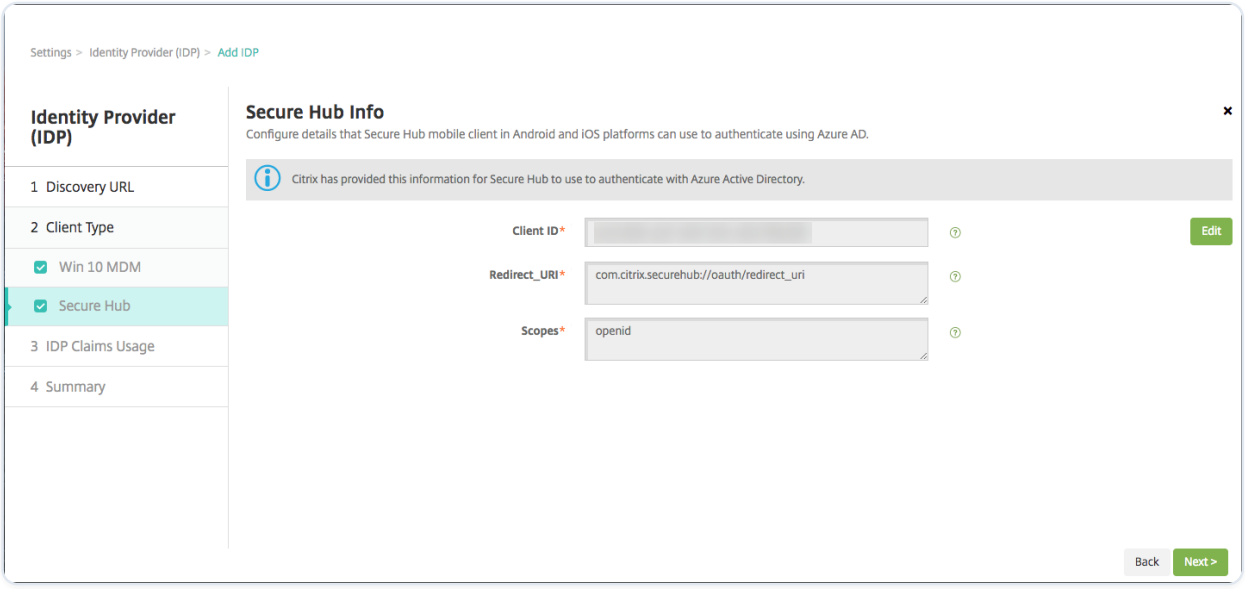
   - **アプリ ID URI:** Azure 設定を構成したときに入力した XenMobile Server の URL を入力します。
   - **クライアント ID:** この値を Azure 構成ページからコピーして貼り付けます。クライアント ID は、アプリの一意の識別子です。
   - **キー:** この値を Azure アプリケーション設定ページからコピーします。キーの下で、リストから期間を選択し、設定を保存します。その後、キーをコピーしてこのフィールドに貼り付けることができます。アプリが Microsoft Azure AD でデータを読み書きする場合、キーが必要です。



8. **次へ**をクリックします。

Citrix は Secure Hub を Microsoft Azure に登録し、情報を維持しています。この画面には、Secure Hub が Azure Active Directory と通信するために使用する詳細が表示されます。このページは、将来この情報に変更が必要になった場合に使用されます。Citrix から指示があった場合にのみ、このページを編集してください。

9. **次へ**をクリックします。



10. IdP が提供するユーザー識別子の種類を構成します。
    - **ユーザー識別子の種類:** リストから **userPrincipalName** を選択します。
    - **ユーザー識別子文字列:** このフィールドは自動的に入力されます。
11. **次へ** をクリックします。

    ID プロバイダー構成画面の画像(/en-us/xenmobile/server/media/add-idp5.png)
12. **概要** ページを確認し、**保存** をクリックします。

    ID プロバイダー構成画面の画像(/en-us/xenmobile/server/media/add-idp6.png)

ユーザーの操作

1. ユーザーは Secure Hub を起動します。次に、XenMobile Server 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。

   Secure Hub 画面の画像(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll1.png)
2. ユーザーは **はい、登録します** をクリックします。

   Secure Hub 画面の画像(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll2.png)
3. ユーザーは Azure AD の資格情報を使用してログオンします。

Secure Hub 画面の画像(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll3.png)

Secure Hub 画面の画像(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll4.png)

Secure Hub画面の画像(/en-us/xenmobile/server/media/secure-hub-ios-idp-enroll5.png)

4. ユーザーは、Secure Hubを介した他の登録と同じ方法で登録手順を完了します。

> **注：**
>
> XenMobileは、登録招待状に対するAzure ADを介した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した場合、ユーザーはAzure ADではなくLDAPを介して認証します。

アップグレード

XenMobile 10.16へのアップグレードの前に

1. XenMobile Server 10.16の最新バージョンにアップデートする前に、Citrix License Serverを11.17.2.0 Build 47000以降にアップデートしてください。

   XenMobileの最新バージョンには、Citrix License Server 11.17（最小バージョン）が必要です。

   XenMobile 10.16におけるCustomer Success Servicesの日付（以前のSubscription Advantageの日付）はNovember 15, 2022です。CitrixライセンスのCustomer Success Servicesの日付は、この日付より後である必要があります。License Serverでライセンスの横に日付を表示できます。XenMobileの最新バージョンを古いLicense Server環境に接続すると、接続チェックが失敗し、License Serverを構成できません。

   ライセンスの有効期限を更新するには、Citrix Portalから最新のライセンスファイルをダウンロードし、そのファイルをライセンスサーバーに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. クラスター環境の場合：iOS 11以降を実行しているデバイスへの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。Citrix GatewayがSSL永続性のために構成されている場合、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. If the virtual machine running the XenMobile Server to be upgraded has less than 8 GB of RAM, we recommend that you increase the RAM to at least 8 GB.
4. Recommendation: Before you install a XenMobile update, use the functionality in your VM to take a snapshot of your system. Also, back up your system configuration database. If you experience issues during an upgrade, complete backups enable you to recover.

アップグレードするには

XenMobile 10.15.xまたは10.14.xからXenMobile 10.16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、利用可能な最新のバイナリをダウンロードします。`<https://www.citrix.com/downloads>`にアクセスします。**Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**に移動します。ハイパーバイザー

用のXenMobile Serverソフトウェアのタイルで、**Download File**をクリックします。アップグレードをアップロードするには、XenMobileコンソールの**Release Management**ページを使用します。

Release Managementページを使用してアップグレードするには

Release Management ページを使用して、XenMobile Server の最新バージョン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。

クラスター展開をお使いの場合は、この記事の最後にある手順を参照してください。

1. 利用可能な最新のバイナリをダウンロードします: `<https://www.citrix.com/downloads>` にアクセスします。**Citrix Endpoint Management (and Citrix XenMobile Server) > XenMobile Server (on-premises) > Product Software > XenMobile Server 10** に移動します。ハイパーバイザー用のXenMobile Serverソフトウェアのタイルで、**Download File** をクリックします。
2. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**Settings** ページが表示されます。
3. **Release Management** をクリックします。**Release Management** ページが表示されます。

   リリース管理の画像(/en-us/xenmobile/server/media/settings-release-management.png)
4. **Updates** の下にある **Update** をクリックします。**Update** ダイアログボックスが表示されます。

   リリース管理の画像(/en-us/xenmobile/server/media/settings-release-management-update.png)
5. **Browse** をクリックしてファイルの場所に移動し、Citrix.comからダウンロードしたXenMobileアップグレードファイルを選択します。
6. **Update** をクリックし、プロンプトが表示されたらXenMobileを再起動します。

   何らかの理由でアップデートが正常に完了できない場合、問題を示すエラーメッセージが表示されます。システムはアップデート試行前の状態に戻されます。

アップグレード後

アップグレード後、XenMobileは再起動が必要です。XenMobile CLIを使用してXenMobile Serverを再起動します。システム再起動後、ブラウザのキャッシュをクリアすることが重要です。

送信接続に関連する機能が動作しなくなり、接続構成を変更していない場合は、**XenMobile Serverログ**で次のようなエラーを確認してください: 「VPPサーバーに接続できません: ホスト名 '192.0.2.0' がピアから提供された証明書のサブジェクトと一致しません」

証明書の検証エラーは、XenMobile Serverでホスト名の検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はホスト名の検証が有効になっています。ホスト名の検証によって展開が機能しなくなる場合は、サーバープロパティ **disable.hostname.verification** を **true** に変更してください。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アップデートをCitrix.comに公開します。同時に、各顧客の登録連絡先に通知が送信されます。

クラスター化されたXenMobile展開をアップグレードするには

> **重要:**
>
> XenMobileのアップデート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作成してください。また、システム構成データベースをバックアップしてください。アップグレード中に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旧できます。

システムがクラスターモードで構成されている場合は、XenMobile 10リリースから各ノードを更新するために、次の手順に従ってください。

1. **Settings > Release Management**から、すべてのノードに.binファイルをアップロードします。
2. CLIの**System Menu**からすべてのノードをシャットダウンします。
3. CLIの**System Menu**から1つのノードを起動し、サービスが実行されていることを確認します。
4. 他のノードを順次起動します。

   XenMobileがアップデートを正常に完了できない場合、問題を示すエラーメッセージが表示されます。その後、XenMobileはシステムをアップデート試行前の状態に戻します。

XenMobile MDM EditionからEnterprise Editionへのアップグレード

XenMobile MDM Editionを、iOSおよびAndroidデバイス向けにXenMobile Advanced Edition (オンプレミス) またはCitrix Endpoint Management™ (クラウド) にアップグレードできます。

前提条件

- 適切なEnterpriseライセンス。
- Citrix Gatewayが構成されていること。

アップグレードするには

1. 「**設定 > ライセンス**」に移動し、正しいEnterprise Editionライセンスタイプ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、「**サーバーモード**」プロパティを「**MDM**」から「**ENT**」に変更します。
3. 「**設定 > Citrix Gateway**」に移動し、Citrix Gatewayの詳細を構成します。認証モードをMDM Editionと同じ、つまりドメイン（Active Directory）認証に設定します。XenMobileは、ユーザー登録後に認証モードを変更すること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。

これらの手順を完了したら、ユーザーはデバイスをEnterpriseモードに切り替えるために、次の手順を実行する必要があります。

iOSユーザー

1. Secure Hubを閉じます：デバイスのホームボタンを2回（素早く）タップし、Secure Hubアプリを上にスライドします。
2. Secure Hubを開きます。

Androidユーザー

1. Secure Hubを開きます。
2. 「**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はユーザーにPINの作成を促します。ユーザーがPINを作成すると、XenMobileはデバイスをEnterpriseモードで構成します。XenMobileコンソールで

は、「**管理 > デバイス**」ページに、そのデバイスのMDMとMAMの両方がアクティブとして表示されます。

ユーザーアカウント、ロール、および登録

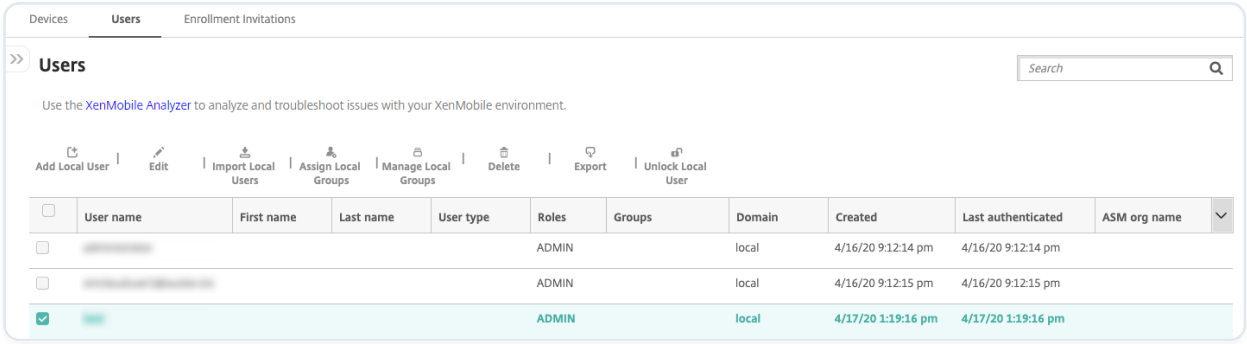
ユーザーアカウント、ロール、および登録は、XenMobile®コンソールの**Manage**タブと**Settings**ページで構成します。特に指定がない限り、以下のタスクの手順はこの記事で説明されています。

- ユーザーアカウントとグループ:
  - **Manage > Users**から、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。
  - **Settings > Workflows**から、ワークフローを使用してユーザーアカウントの作成と削除を管理します。
- ユーザーアカウントとグループのロール
  - **Settings > Role-Based Access Control**から、定義済みのロール（権限のセット）をユーザーとグループに割り当てます。これらの権限は、ユーザーがシステム機能にアクセスできるレベルを制御します。詳細については、「RBACでロールを構成する」を参照してください。
  - **Settings > Notification Templates**から、自動アクション、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または更新します。通知テンプレートは、Secure Hub、SMTP、SMSの3つの異なるチャネルでメッセージを送信するように構成します。詳細については、「通知テンプレートの作成と更新」を参照してください。
- 登録セキュリティモードと招待
  - **Settings > Enrollment**から、最大7つの登録セキュリティモードを構成し、登録招待を送信します。各登録セキュリティモードには、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ために実行する必要がある手順があります。
  - 「ユーザー登録のためにXenMobileでAutoDiscoveryを有効にする」

ローカルユーザーアカウントの追加、編集、ロック解除、または削除

XenMobileにローカルユーザーアカウントを手動で追加することも、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することもできます。プロビジョニングファイルからユーザーアカウント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、**Manage > Users**をクリックします。**Users**ページが表示されます。



2. 「**フィルターの表示**」をクリックして、リスト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**ページが表示されます。

   ユーザー管理の画像(/en-us/xenmobile/server/media/manage-users-add-local.png)

2. 次の設定を構成します。

   - **ユーザー名:** 必須フィールドである名前を入力します。名前には、大文字と小文字のほかにスペースを含めることができます。
   - **パスワード:** オプションのユーザーパスワードを入力します。パスワードは14文字以上で、次のすべての条件を満たす必要があります。
     - 2つ以上の数字を含める
     - 1つ以上の大文字と1つ以上の小文字を含める
     - 1つ以上の特殊文字を含める
     - 辞書に載っている単語や、Citrix®ユーザー名またはメールアドレスなどの制限された単語を含めないでください
     - 1111、1234、asdfなどの3つ以上の連続した繰り返し文字やキーボードパターンを含めないでください

- **役割:** リストでユーザーの役割をクリックします。役割の詳細については、「RBACで役割を構成する」を参照してください。選択可能なオプションは次のとおりです。
  - ADMIN
  - DEVICE_PROVISIONING
  - サポート
  - ユーザー
- **メンバーシップ:** リストで、ユーザーを追加するグループをクリックします。
- **ユーザープロパティ:** オプションの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、次の操作を行います。
  - **ユーザープロパティ:** リストでプロパティをクリックし、その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。
  - ユーザープロパティを保存するには**完了**をクリックするか、**キャンセル**をクリックします。

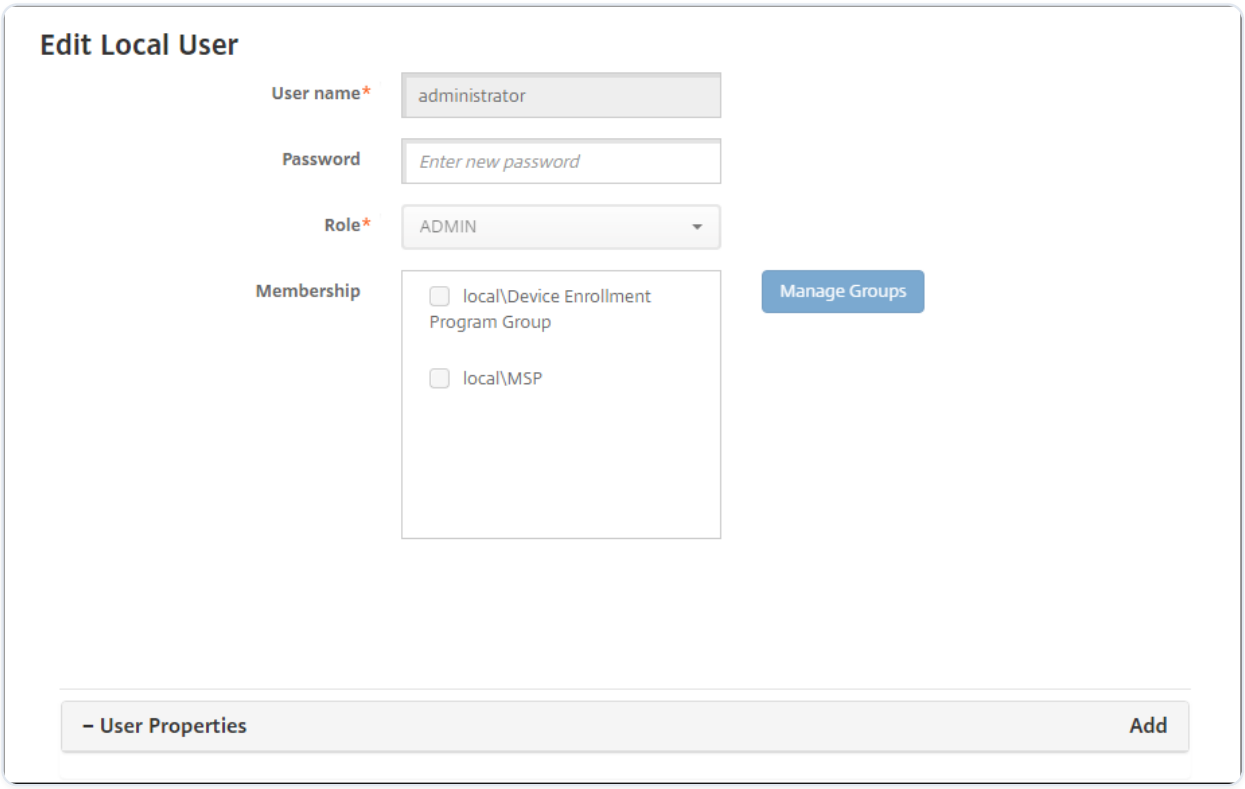
既存のユーザープロパティを削除するには、プロパティを含む行にカーソルを合わせ、右側のXをクリックします。プロパティはすぐに削除されます。

既存のユーザープロパティを編集するには、プロパティをクリックして変更します。変更したリストを保存するには**完了**をクリックするか、リストを変更しないままにするには**キャンセル**をクリックします。

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**ページで、ユーザーのリストからユーザーを選択し、**編集**をクリックします。**ローカルユーザーの編集**ページが表示されます。



2. 必要に応じて、次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:** リストで、ユーザーの役割をクリックします。
- **メンバーシップ:** リストで、ユーザーアカウントを追加または編集するグループをクリックします。グループからユーザーアカウントを削除するには、グループ名の横にあるチェックボックスをオフにします。
- **ユーザープロパティ:** 次のいずれかを実行します。
  - 変更するユーザープロパティごとに、プロパティをクリックして変更を加えます。変更したリストを保存するには「**完了**」をクリックし、リストを変更しないままにするには「**キャンセル**」をクリックします。
  - 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、次の操作を実行します。
    - **ユーザープロパティ:** リストでプロパティをクリックし、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。
    - ユーザープロパティを保存するには「**完了**」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。

- 削除する既存のユーザープロパティごとに、プロパティを含む行にカーソルを合わせ、右側にある「**X**」をクリックします。プロパティはすぐに削除されます。

3. 変更を保存するには「**保存**」をクリックし、ユーザーを変更しないままにするには「**キャンセル**」をクリックします。

ローカルユーザーアカウントのロックを解除するには

1. 「**ユーザー**」ページで、ユーザーアカウントのリストからユーザーアカウントをクリックして選択します。
2. 「**ローカルユーザーのロック解除**」をクリックします。確認ダイアログボックスが表示されます。
3. ユーザーアカウントのロックを解除するには「**ロック解除**」をクリックし、ユーザーを変更しないままにするには「**キャンセル**」をクリックします。

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**」ページで、ユーザーアカウントのリストからユーザーアカウントをクリックして選択します。

削除するユーザーアカウントの横にあるチェックボックスを選択することで、複数のユーザーアカウントを選択できます。

1. **Delete** をクリックします。確認ダイアログボックスが表示されます。
2. ユーザーアカウントを削除するには **Delete** をクリックするか、**Cancel** をクリックします。

Active Directoryユーザーを削除するには

複数のActive Directoryユーザーを一度に削除するには、ユーザーを選択して **Delete** をクリックします。

削除するユーザーが登録済みデバイスを所有しており、それらのデバイスを再登録したい場合は、再登録する前にデバイスを削除してください。デバイスを削除するには、**Manage > Devices** に移動し、デバイスを選択して **Delete** をクリックします。

ユーザーアカウントのインポート

プロビジョニングファイルと呼ばれる.csvファイルから、ローカルユーザーアカウントとプロパティを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

フォーマットの詳細については、「プロビジョニングファイルのフォーマット」を参照してください。

注：

- ローカルユーザーの場合、インポートファイルでは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する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、そのユーザーは対応するLDAP資格情報を使用して登録できません。
- 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、インポートプロセスを高速化するためにデフォルトドメインを無効にします。ドメインを無効にすると登録に影響することに留意し、内部ユーザーのインポートが完了したらデフォルトドメインを再度有効にしてください。
- ローカルユーザーはユーザープリンシパル名（UPN）形式にすることができます。ただし、Citrixは管理対象ドメインを使用しないことを推奨します。たとえば、example.com が管理されている場合、user@example.com のようなUPN形式でローカルユーザーを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ら、次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、**Manage > Users** をクリックします。**Users** ページが表示されます。
2. **Import Local Users** をクリックします。**Import Provisioning File** ダイアログボックスが表示されます。

   ユーザー管理の画像(/en-us/xenmobile/server/media/local-users-and-groups-import-provisioning-file.png)
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、**User** または **Property** のいずれかを選択します。
4. **参照**をクリックしてファイルが保存されている場所に移動し、使用するプロビジョニング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の形式

XenMobile にユーザーアカウントとプロパティをインポートするためのプロビジョニングファイルを手動で作成できます。有効な形式は次のとおりです。

- **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;propertyValue2`

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。フィールドの一部にセミコロンが含まれる場合は、バックスラッシュ文字 (\\) でエスケープします。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内で `propertyV\\;test\\;1\\;2` と入力します。
- **役割**の有効な値は、定義済みの役割である USER、ADMIN、SUPPORT、DEVICE_PROVISIONING、およびユーザーが定義したその他の役割です。
- グループ階層を作成するには、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を使用しないでください。
- 属性プロビジョニングファイルでは、プロパティ属性に小文字を使用してください。データベースでは大文字と小文字が区別されます。

ユーザープロビジョニングコンテンツの例

エントリ `user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` は次のことを意味します。

- **ユーザー:** `user01`
- **パスワード:** `pwd;01`
- **役割:** `USER`
- **グループ:**
  - `myGroup.users01`
  - `myGroup.users02`
  - `myGroup.users.users.users01`

別の例として、`AUser0;1.password;USER;ActiveDirectory.test.net` は次のことを意味します。

- **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コンテンツの例

エントリ `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` は次のことを意味します。

- **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`

登録セキュリティモードを構成する

XenMobile でデバイス登録のセキュリティレベルと通知テンプレートを指定するために、デバイス登録セキュリティモードを構成します。

XenMobile には7つの登録セキュリティモードがあり、それぞれ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ために実行する必要がある手順があります。登録セキュリティモードは、XenMobile Server コンソールの **>** ページで構成します。

一部のモードはセルフヘルプポータルで利用できるように設定できます。ポータルから、ユーザーはデバイスを登録するための登録リンクを生成します。iOS、iPadOS、macOS、Android Enterprise、およびレガシーAndroidのユーザーは、ポータルから登録招待状を自分宛てに送信することを選択できます。Windowsデバイスでは登録招待状は利用できません。

登録招待状は、 **>** ページから送信します。詳細については、「登録招待状を送信する」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がある場合は、登録セキュリティモードを構成する前にテンプレートを設定する必要があります。通知テンプレートの詳細については、「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、コンソールの右上隅にある歯車アイコンをクリックします。 ページが表示されます。
2. をクリックします。使用可能なすべての登録セキュリティモードのテーブルを含む ページが表示されます。デフォルトでは、すべての登録セキュリティモードが有効になっています。
3. リスト内の任意の登録セキュリティモードを選択して編集します。その後、そのモードをデフォルトとして設定するか、モードを無効にするか、またはセルフヘルプポータルを通じてユーザーにアクセスを許可します。

   > **注:**
   >
   > 登録セキュリティモードの横にあるチェックボックスを選択すると、登録セキュリティモードリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

   > 登録設定の画像(/en-us/xenmobile/server/media/settings-enrollment.png)

   次の登録セキュリティモードから選択します。

   - ユーザー名 + パスワード
   - 高セキュリティ
   - 招待URL
   - 招待URL + PIN
   - 招待URL + パスワード
   - 2要素認証
   - ユーザー名 + PIN

   登録招待を使用して、招待状を持つユーザーのみに登録を制限できます。登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードの

みを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはSecure Hubで手動で資格情報を入力する必要があります。

ワンタイムPIN (OTP) 登録招待を2要素認証ソリューションとして使用できます。OTP登録招待は、ユーザーが登録できるデバイスの数を制御します。OTP招待はWindowsデバイスでは利用できません。

登録セキュリティモードを編集するには

1. 「**登録**」リストで、登録セキュリティモードを選択し、「**編集**」をクリックします。「**登録モードの編集**」ページが表示されます。選択したモードによって、表示されるオプションが決まります。

   登録セキュリティモードの編集(/en-us/xenmobile/server/media/settings-enrollment-edit.png)

2. 必要に応じて、次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**」と入力します。

   - **日数:** リストで、「**有効期限**」に入力した有効期限に対応する「**日数**」または「**時間**」をクリックします。
   - **最大試行回数:** ユーザーが登録プロセスからロックアウトされるまでに試行できる登録回数を入力します。この値は、ユーザーおよびグループの登録招待構成ページに表示されます。

     無制限の試行を許可するには、「**0**」と入力します。

   - **PINの長さ:** 生成されるPINの長さを設定する数値を入力します。
   - **数字:** リストで、PINの種類として「**数字**」または「**英数字**」をクリックします。
   - **通知テンプレート:**

     - **登録URLのテンプレート:** リストで、登録URLに使用するテンプレートをクリックします。たとえば、登録招待テンプレートは、ユーザーにメールまたはSMSを送信します。この方法は、ユーザーがXenMobileにデバイスを登録できるようにするテンプレートをどのように構成したかによって異なります。通知テンプレートの詳細については、「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のテンプレート:** リストで、登録PINに使用するテンプレートをクリックします。

- **登録確認のテンプレート:** リストで、ユーザーに登録が成功したことを通知するために使用するテンプレートをクリックします。

3. 「**保存**」をクリックします。

登録セキュリティモードをデフォルトとして設定するには

登録セキュリティモードをデフォルトとして設定すると、別の登録セキュリティ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使用されます。登録セキュリティモードがデフォルトとして設定されていない場合、デバイス登録ごとに登録要求を作成する必要があります。

> **注：**
>
> デフォルトとして使用できる登録セキュリティモードは、**ユーザー名 + パスワードのみ**、**2要素認証**、または**ユーザー名 + PIN**です。

1. デフォルトの登録セキュリティモードとして、**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**のいずれかを選択します。

   モードをデフォルトとして使用するには、まずそれを有効にします。

2. **Default**をクリックします。選択したモードがデフォルトになりました。他の登録セキュリティ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はなくなります。

登録セキュリティモードを無効にするには

登録セキュリティモードを無効にすると、グループ登録招待とセルフヘルプポータルの両方で利用できなくなります。ある登録セキュリティモードを無効にし、別のモードを有効にすることで、ユーザーがデバイスを登録する方法を変更できます。

1. 登録セキュリティモードを選択します。

   デフォルトの登録セキュリティモードを無効にすることはできません。デフォルトの登録セキュリティモードを無効にしたい場合は、まずそのデフォルトステータスを解除する必要があります。

2. **Disable**をクリックします。登録セキュリティモードは有効ではなくなります。

セルフヘルプポータルで登録セキュリティモードを有効にするには

セルフヘルプポータルで登録セキュリティモードを有効にすると、ユーザーは個別にXenMobileにデバイスを登録できるようになります。

> **注：**
>
> - 登録セキュリティモードは、セルフヘルプポータルで利用できるように、有効にして通知テンプレートにバインドする必要があります。
> - セルフヘルプポータルでは、一度に1つの登録セキュリティモードのみを有効にできます。

1. 登録セキュリティモードを選択します。
2. **Self Help Portal**をクリックします。選択した登録セキュリティモードが、セルフヘルプポータルでユーザーに利用可能になります。セルフヘルプポータルで既に有効になっているモードは、ユーザーには利用できなくなります。

グループの追加または削除

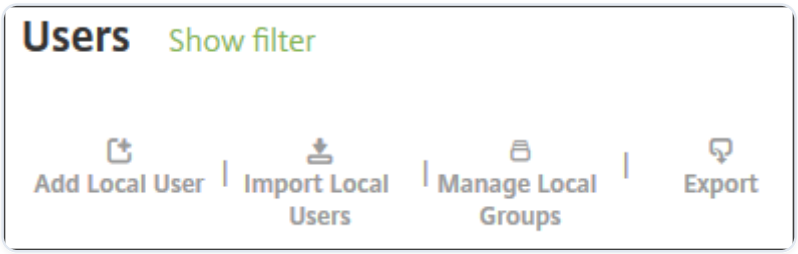
XenMobileコンソールの**ユーザー**、**ローカルユーザーの追加**、または**ローカルユーザーの編集**ページにある**グループの管理**ダイアログボックスでグループを管理します。グループ編集コマンドはありません。

グループを削除する場合、グループの削除はユーザーアカウントに影響を与えないことに注意してください。グループを削除すると、そのグループとのユーザーの関連付けが解除されるだけです。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るアプリやプロファイルへのアクセスも失います。ただし、その他のグループ関連付けはそのまま維持されます。ユーザーが他のローカルグループに関連付けられていない場合、最上位レベルで関連付けられます。

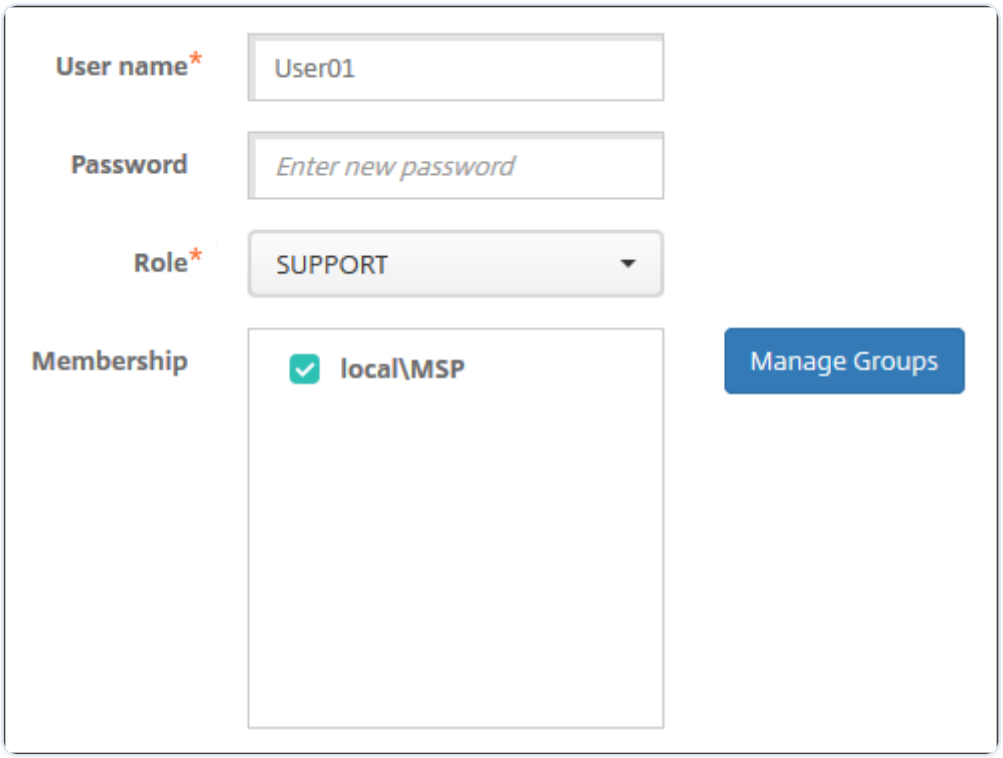
ローカルグループを追加するには

1. 次のいずれかを実行します。

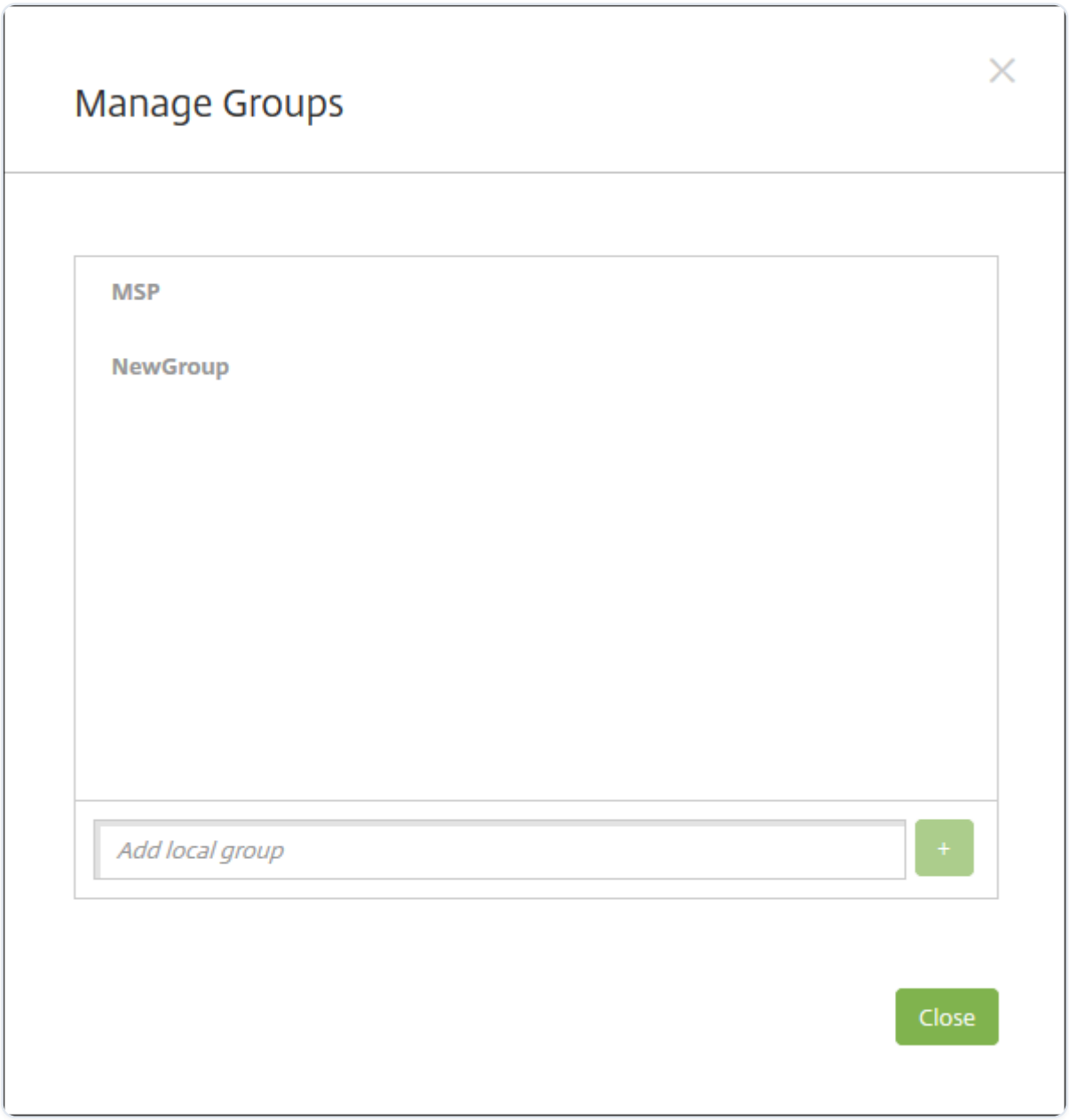
   - **ユーザー**ページで、**ローカルグループの管理**をクリックします。



- **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**ページのいずれかで、**グループの管理**をクリックします。



グループの管理ダイアログボックスが表示されます。



2. グループリストの下に、新しいグループ名を入力し、プラス記号（+）をクリックします。ユーザーグループがリストに追加されます。
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しません。グループを削除すると、そのグループとのユーザーの関連付けが解除されるだけです。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るアプリやプロファイルへのアクセスも失います。ただし、他のグループの関連付けはそのまま残ります。ユーザーが他のローカルグループに関連付けられていない場合、最上位レベルで関連付けられます。

1. 次のいずれかを実行します。

- **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**ページのいずれかで、**グループの管理**をクリックします。

グループの管理ダイアログボックスが表示されます。

ユーザーグループ管理の画像(/en-us/xenmobile/server/media/local-users-and-groups-manage-group-remove.png)

2. **グループの管理**ダイアログボックスで、削除するグループをクリックします。
3. グループ名の右側にあるゴミ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表示されます。
4. **削除**をクリックして操作を確定し、グループを削除します。

> **重要:**
>
> この操作は元に戻せません。

5. **グループの管理**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と管理

ワークフローを使用して、ユーザーアカウントの作成と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個人を特定します。その後、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。

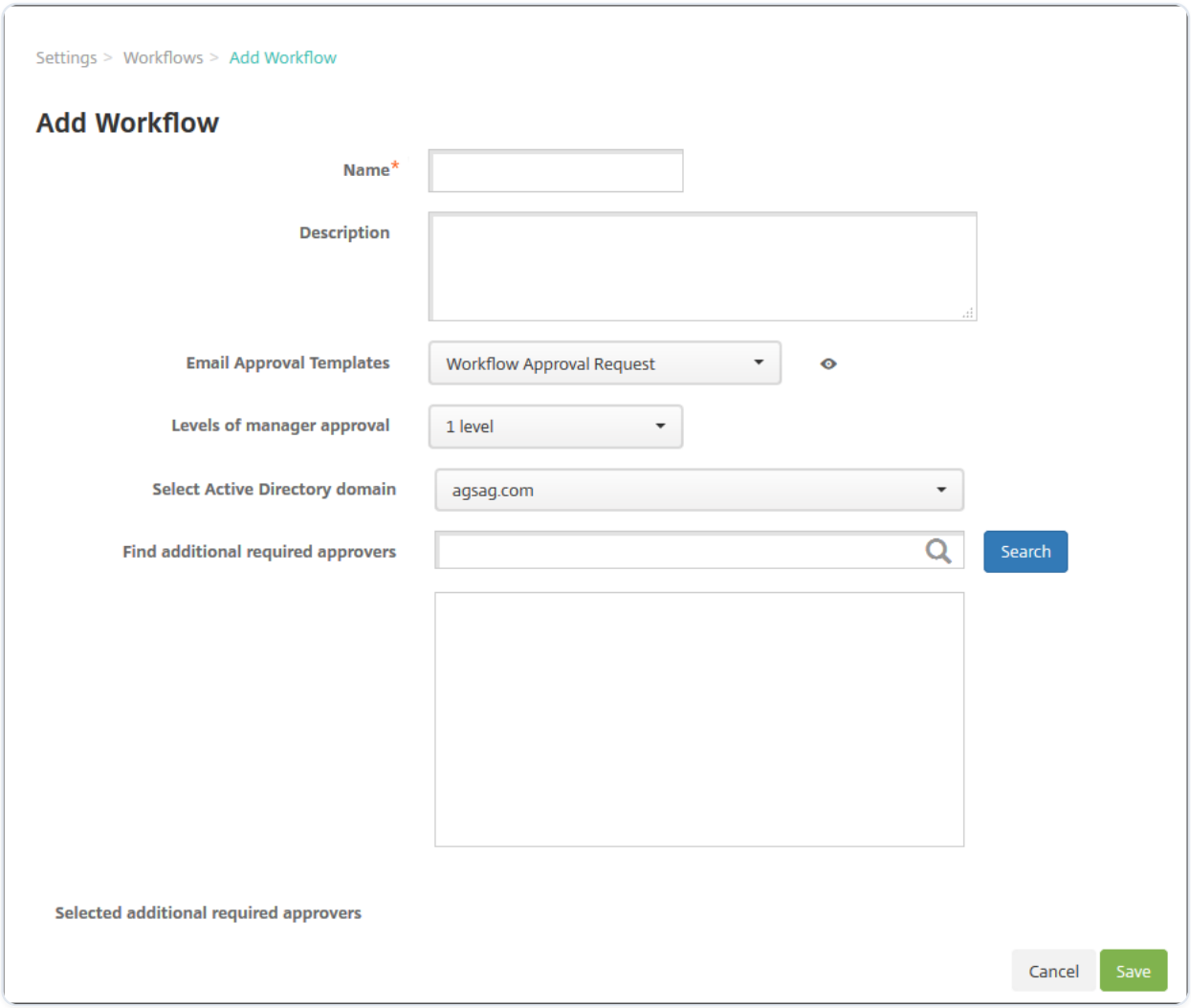
XenMobileを初めてセットアップするときに、ワークフローのメール設定を構成します。これらの設定は、ワークフローを使用する前に設定する必要があります。ワークフローのメール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウント作成要求に承認が必要かどうかが含まれます。

XenMobileでは、ワークフローを次の2か所で構成できます。

- XenMobileコンソールの ページ。 ページでは、アプリ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、アプリを構成するときにそ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アプリで構成するときに、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個人を構成します。「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には、最大3つのレベルを割り当てることができます。他のユーザーにユーザーアカウントの承認を依頼する必要がある場合は、名前またはメールアドレスを使用してそれらのユーザーを検索して選択できます。XenMobileがそのユーザーを見つけると、そのユーザーをワークフローに追加します。ワークフロー内のすべての個人は、新しいユーザーアカウントを承認または拒否するためのメールを受信します。

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。 ページが表示されます。
2. をクリックします。 ページが表示されます。
3. をクリックします。 ページが表示されます。



4. 次の設定を構成します。

- **名前:** ワークフローの一意の名前を入力します。
- **説明:** 必要に応じて、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:** リストから、割り当てるメール承認テンプレートを選択します。メールテンプレートは、XenMobileコンソールの の セクションで作成します。このフィー

ルドの右側にある目のアイコンをクリックすると、構成しているテンプレートのプレビューが表示されます。

- **マネージャー承認レベル:** リストで、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは**1 レベル**です。選択可能なオプションは次のとおりです。
  - 不要
  - 1 レベル
  - 2 レベル
  - 3 レベル
- **Active Directory ドメインの選択:** リストで、ワークフローに使用する適切な Active Directory ドメインを選択します。
- **追加の必須承認者の検索:** 検索フィールドに名前を入力し、**検索**をクリックします。名前は Active Directory に由来します。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスをオンにします。名前とメールアドレスが**選択された追加の必須承認者**リストに表示されます。
  - リストから名前を削除するには、次のいずれかを実行します。
    - **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のリストを表示します。
    - 検索ボックスに名前の全部または一部を入力し、**検索**をクリックして検索結果を絞り込みます。
    - **選択された追加の必須承認者**リストのユーザーは、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除したい各名前の横にある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。作成されたワークフローが**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した後、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ている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は、ワークフローを編集できません。異なる承認レベルまたは承認者を持つ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を表示および削除するには

1. 「**ワークフロー**」ページで、既存のワークフローのリストから特定のワークフローを選択します。そのためには、テーブル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表示されます。もう一度「**削除**」をクリックします。

> 「**重要:**」:

> この操作は元に戻すことはできません。

登録プロファイル

登録プロファイルでは、以下を指定します。

- AndroidおよびiOSデバイスのデバイス管理登録オプション。Androidの場合、MDM+MAM (ENT) サーバーモードで利用可能な登録オプションは、MDMモードのオプションとは異なります。
- AndroidおよびiOSデバイスのアプリ管理登録オプション。
- その他の登録オプション:
  - ユーザーが登録できるデバイスの数を制限するかどうか。

    デバイス制限に達した場合、エラーメッセージによって、ユーザーはデバイス登録制限を超過したことを知らされます。
  - ユーザーがデバイス管理を拒否することを許可するかどうか。

登録プロファイルを使用すると、単一のXenMobile® Serverコンソール内で複数のユースケースとデバイス移行パスを組み合わせることができます。いくつかのユースケースは次のとおりです。

- モバイルデバイス管理 (MDMのみ)
- MDM+モバイルアプリケーション管理 (MAM)
- MAMのみ
- 企業所有の登録
- BYOD登録 (MDM登録をオプトアウトする機能)
- Androidデバイス管理者登録からAndroid Enterprise登録への移行 (完全管理、仕事用プロファイル、専用デバイス)

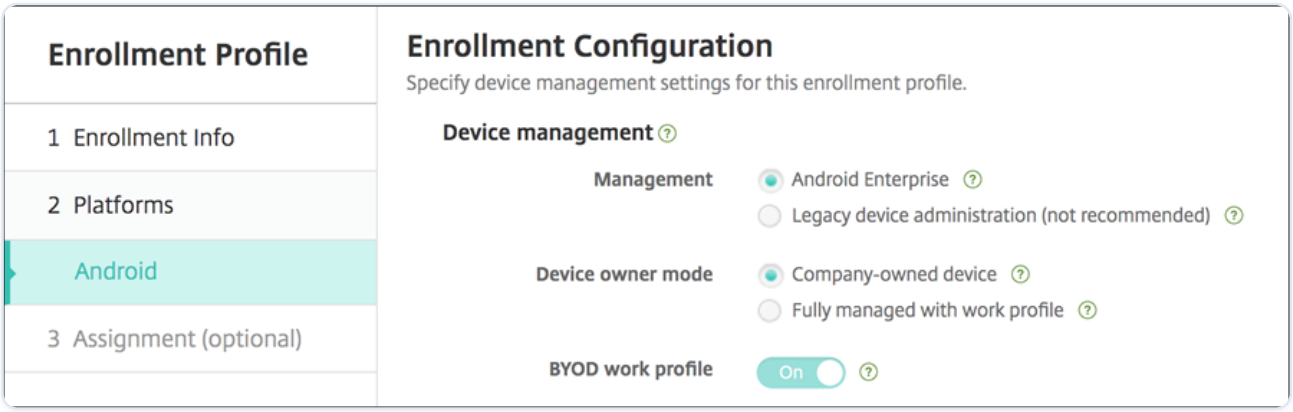
デリバリーグループを作成する際、Globalという名前のデフォルトの登録プロファイルを使用するか、別の登録プロファイルを指定できます。

プラットフォームごとの登録プロファイルの機能は次のとおりです。

- **Androidデバイスの場合:** デバイス所有者モードを指定します。例：完全管理、仕事用プロファイル付き完全管理、BYOD仕事用プロファイル。**専用デバイス**オプションは、XenMobileのEnterpriseまたはAdvancedライセンスをお持ちの場合にのみ表示されます。新しいデバイスは、デフォルトでAndroid Enterpriseおよびアプリ管理に登録されます。登録セキュリティモードの**ユーザー名 + PIN**、**招待URL**、**招待URL + PIN**、**招待URL + パスワード**は、Android Enterpriseでは利用できません。
- **iOSデバイスの場合:** デバイス登録タイプ（デバイス登録またはデバイスを管理しない）を指定します。iOS設定は、XenMobileのEnterpriseまたはAdvancedライセンスをお持ちの場合にのみ表示されます。新しいデバイスは、デフォルトでAppleデバイス管理およびアプリ管理に登録されます。

Androidデバイス用の専用デバイスの登録や、AndroidまたはiOSデバイス用のMAMのみの登録が不要な場合は、サーバープロパティ`enable.multimode.xms`を無効にできます。ただし、このプロパティを有効にしておくと、あらゆる種類の登録プロファイルを処理するために必要なXenMobile Serverは1つだけで済みます。サーバープロパティを参照してください。

`enable.multimode.xms`を無効にすると、このスクリーンショットの設定のみが利用可能になります。

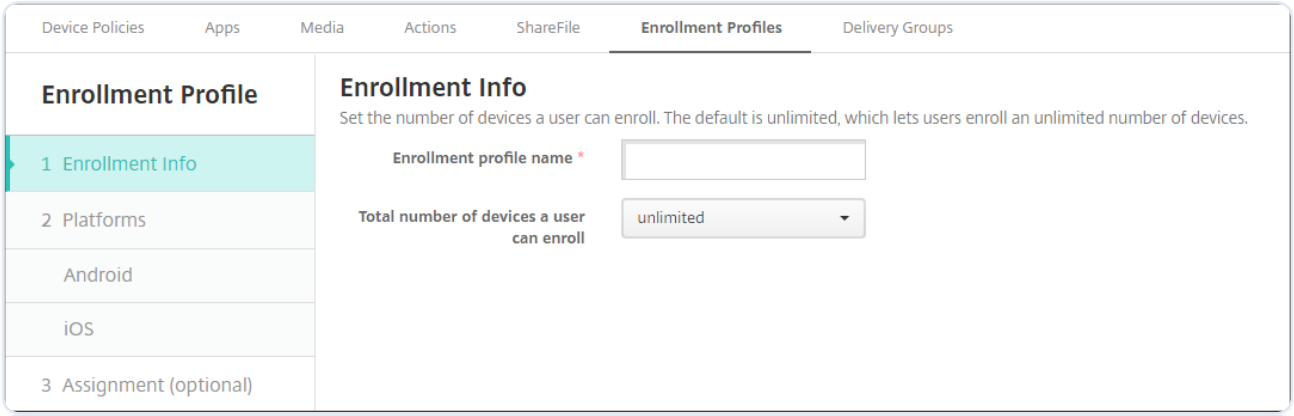


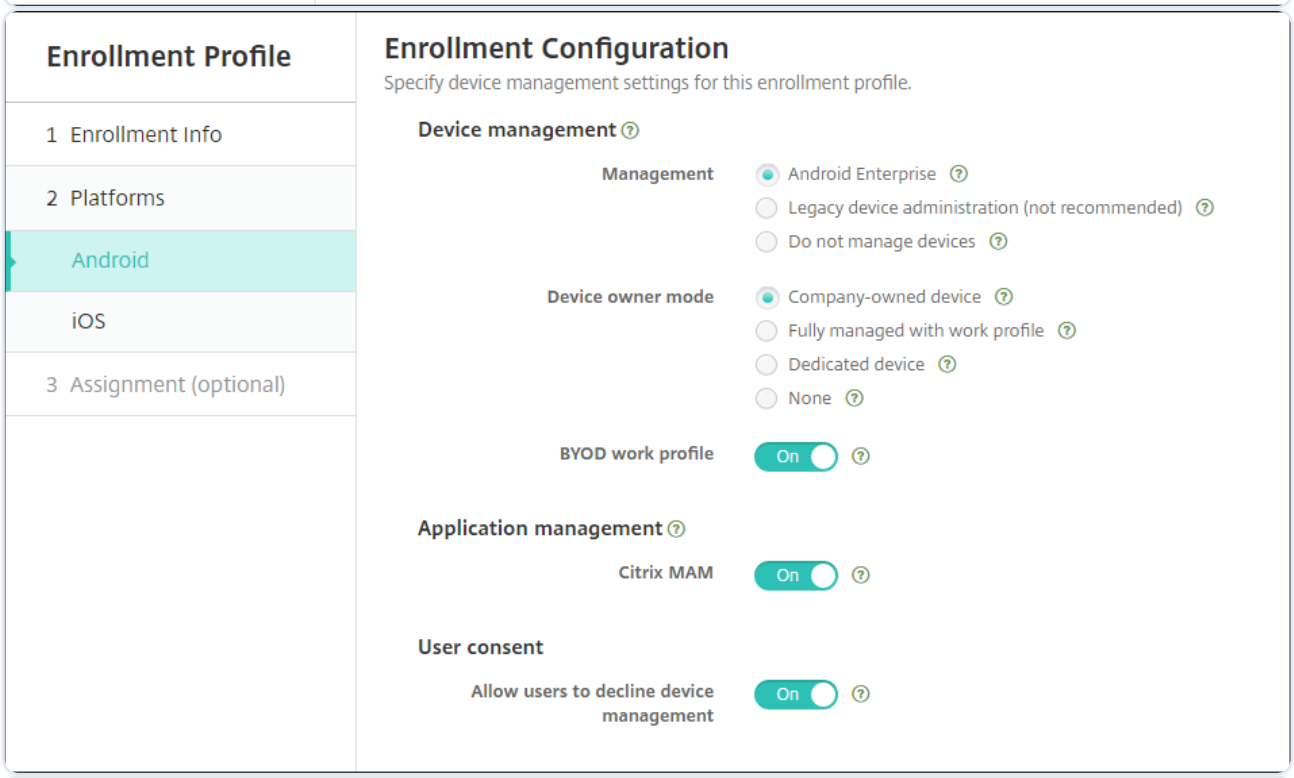
これらの設定の詳細については、Android Enterpriseを参照してください。

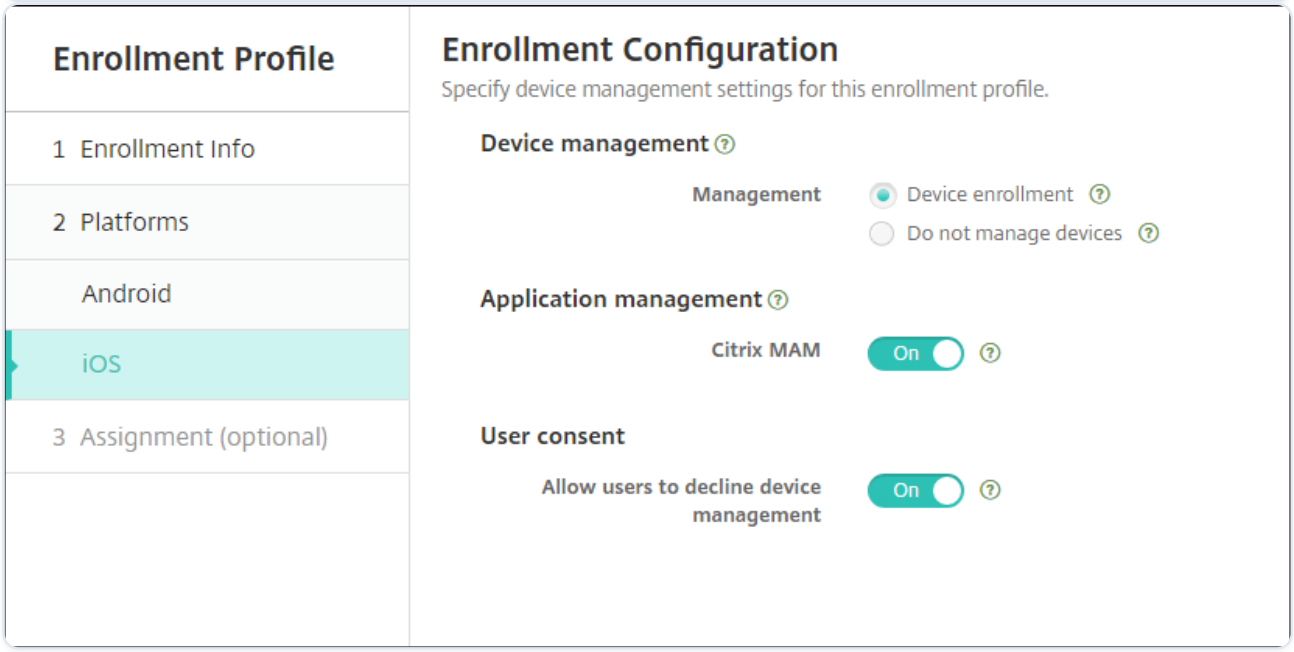
グローバル登録プロファイル

デフォルトの登録プロファイルはGlobalという名前です。Globalプロファイルは、登録プロファイルを作成する機会ができるまでのテストに役立ちます。

次のスクリーンショットは、グローバル登録プロファイルのデフォルト設定を示しています。


Device Policies
Apps
Media
Actions
ShareFile
Enrollment Profiles
Delivery Groups
Enrollment Profile
1 Enrollment Info
2 Platforms
Android
iOS
3 Assignment (optional)
Enrollment Info
Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.
Enrollment profile name *
Total number of devices a user can enroll
unlimited


Enrollment Profile
1 Enrollment Info
2 Platforms
Android
iOS
3 Assignment (optional)
Enrollment Configuration
Specify device management settings for this enrollment profile.
Device management
Management
Android Enterprise
Legacy device administration (not recommended)
Do not manage devices
Device owner mode
Company-owned device
Fully managed with work profile
Dedicated device
None
BYOD work profile
On
Application management
Citrix MAM
On
User consent
Allow users to decline device management
On


Enrollment Profile
1 Enrollment Info
2 Platforms
Android
iOS
3 Assignment (optional)
Enrollment Configuration
Specify device management settings for this enrollment profile.
Device management
Management
Device enrollment
Do not manage devices
Application management
Citrix MAM
On
User consent
Allow users to decline device management
On

登録プロファイル、デリバリーグループ、および登録

登録プロファイルとデリバリーグループは次のように連携します。

- 登録プロファイルを1つ以上のデリバリーグループにアタッチできます。
- ユーザーが異なる登録プロファイルを持つ複数のデリバリーグループに属している場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。XenMobile Serverは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。たとえば、次のような場合を想定します。
  - 「EP1」と「EP2」という名前の2つの登録プロファイル。
  - 「DG1」と「DG2」という名前の2つのデリバリーグループ。
  - 「DG1」は「EP1」に関連付けられています。
  - 「DG2」は「EP2」に関連付けられています。

  登録ユーザーが「DG1」と「DG2」の両方のデリバリーグループに属している場合、XenMobile Serverは「EP2」登録プロファイルを使用して、ユーザーの登録タイプを決定します。
- 展開順序は、MDM (デバイス管理) 用に構成された登録プロファイルを持つデリバリーグループ内のデバイスにのみ適用されます。
- デバイスが登録された後、登録プロファイルに対する一部の変更には再登録が必要です。
  - MDM用に構成された登録プロファイルにMAMを追加する。
  - MDMに登録されているデバイスを、MDM+MAM用に構成されたデリバリーグループに移動する。この変更は新しいデバイス登録にのみ影響します。既存のデバイス登録には影響しません。
  - MAM用に構成された登録プロファイルにMDMを追加する。
- 別の登録プロファイルに切り替えても、既存の登録済みデバイスには影響しません。ただし、変更を有効にするには、ユーザーはそれらのデバイスの登録を解除してから再登録する必要があります。

登録プロファイルを作成するには

1. XenMobile Server コンソールで、 > の順に移動します。
2. ページで、プロファイルの説明的な名前を入力します。デフォルトでは、ユーザーは無制限のデバイスを登録できます。ユーザーあたりのデバイス数を制限する値を選択します。この制限は、ユーザーが登録するMAMまたはMDM管理のAndroidおよびiOSデバイスの合計に適用されます。

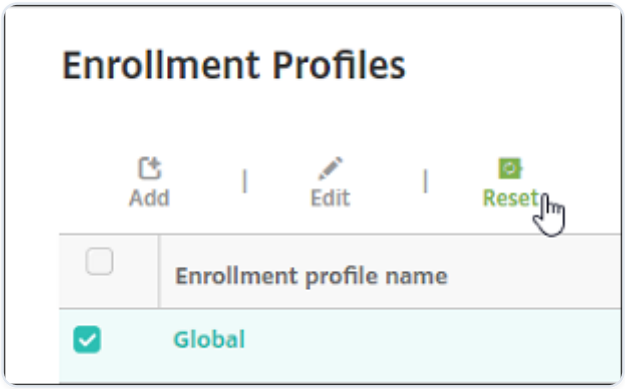
3. プラットフォームページを完了します。プラットフォーム固有の登録設定については、以下を参照してください。

   - Android エンタープライズ
   - iOS: サポートされている登録方法

4. ページで、1つ以上のデリバリーグループを登録プロファイルにアタッチします。

   ユーザーは、異なる登録プロファイルを持つ複数のデリバリーグループに属している場合があります。その場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。XenMobileは、デリバリーグループのアルファベット順リストで最後に表示され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作成するには、 > の順に移動します。

登録プロファイルのリストは、 > ページに表示されます。グローバルプロファイルを編集するか、元のデフォルトにリセットするには、グローバルプロファイルの行を選択し、 をクリックします。グローバルプロファイルを削除することはできません。



RBACで役割を構成する

事前定義された各ロールベースのアクセス制御 (RBAC) ロールには、特定のアクセス権限と機能権限が関連付けられています。この記事では、それらの各権限がどのような機能を持つかについて説明します。各組み込みロールのデフォルト権限の完全なリストについては、ロールベースのアクセス制御のデフォルトをダウンロードしてください。

*権限を適用*する場合、RBACロールが管理する権限を持つユーザーグループを定義することになります。デフォルトの管理者は、適用された権限設定を変更できません。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*を行う場合、RBACロールをグループに割り当て、そのユーザーグループがRBAC管理者権限を所有するようにします。

> **重要:**

> 設定権限の下では、RBAC権限は管理者ユーザーに、自身の権限を割り当てる機能を含む完全なアクセス権を与えます。このアクセス権は、Endpoint Managementシステム内のすべてを操作する能力を与えることを意図しているユーザーにのみ付与してください。

> この記事には、次のセクションがあります。

- 管理者ロール
- サポートロール
- ユーザーロール
- RBACで役割を構成する

管理者ロール

事前定義された管理者ロールを持つユーザーは、XenMobileの次の機能にアクセスできます、またはアクセスできません。デフォルトでは、**承認済みアクセス**（セルフヘルプポータルを除く）、**コンソール機能**、および**権限の適用**が有効になっています。

承認済みアクセス

管理コンソールアクセス	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。
セルフヘルプポータルアクセス	管理者はセルフヘルプポータルにアクセスできません。
共有デバイス登録者	管理者は共有デバイス登録者アクセス権を持ちません。この機能は、共有デバイスを登録する必要があるユーザーを対象としています。
リモートサポートアクセス	管理者はリモートサポートアクセス権を所有しています。*
パブリックAPIアクセス	管理者は、XenMobileコンソールで利用可能なアクションをプログラムで実行するために、パブリックAPIにアクセスできます。これらのアクションには、証明書、アプリ、デバイス、デリバリーグループ、およびローカルユーザーの管理が含まれます。

COSUデバイス登録者	登録プロファイルを使用してこの機能が構成されていない場合、管理者が専用のAndroid Enterpriseデバイス（COSUデバイスとも呼ばれる）を登録する方法を提供します。

* リモートサポートにより、ヘルプデスク担当者は管理対象のAndroidモバイルデバイスをリモートで制御できます。スクリーンキャストはSamsung Knoxデバイスでのみサポートされています。クラスター化されたオンプレミスXenMobile Server展開では、リモートサポートは利用できません。リモートサポートは、January 1, 2019以降の新規顧客には提供されなくなりました。既存の顧客は引き続き製品を使用できますが、Citrixは機能強化や修正を提供しません。

コンソール機能

管理者はXenMobileコンソールへの無制限のアクセス権を持っています。

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最初に表示されるページです。「**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**」ページには、アプリとデバイスの展開を分析できる事前定義されたレポートが用意されています。	
デバイス	「**管理 > デバイス**」ページでは、ユーザーデバイスを管理します。このページで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複数のデバイスを一度に追加したりできます。	
ローカルユーザーとグループ	「**管理 > ユーザー**」ページでは、ローカルユーザーとロー	

	カルユーザーグループを追加、編集、または削除できます。	
登録	「**管理 > 登録招待**」ページでは、ユーザーがXenMobileにデバイスを登録するよう招待される方法を管理します。	
ポリシー	「**構成 > デバイスポリシー**」ページでは、VPNやWi-Fiなどのデバイスポリシーを管理します。	
アプリ	「**構成 > アプリ**」ページでは、ユーザーがデバイスにインストールできるさまざまなアプリを管理します。	
メディア	「**構成 > メディア**」ページでは、ユーザーがデバイスにインストールできるさまざまなメディアを管理します。	
アクション	**Configure > Actions** ページでは、トリガーイベントへの応答を管理します。	
登録プロファイル	**Configure > Enrollment Profiles** ページでは、ユーザーがデバイスを登録できるように登録プロファイル（モード）を構成します。	
デリバリーグループ	**Configure > Delivery Groups** ページでは、デリバリーグループとそれに関連付けられているリソースを管理します。	
設定	**Settings** ページでは、クライアントおよびサーバーのプロパティ、証明書、資格情報プ	

	ロバイダーなどのシステム設定を管理します。**重要:** これらの設定にはRBAC権限が含まれます。RBAC権限は、管理者自身に権限を割り当てる機能を含め、管理者にフルアクセスを付与します。このアクセスは、Endpoint Managementシステム内のすべてを操作する権限を付与する意図のあるユーザーにのみ与えてください。	
サポート	**Troubleshooting and Support** ページでは、診断の実行やログの生成などのトラブルシューティング活動を行います。	

デバイス

管理者は、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などを行うことで、コンソール全体でデバイス機能にアクセスします。

デバイスの完全ワイプ	デバイスからすべてのデータとアプリを消去します。デバイスにメモリカードがある場合はそれらも含まれます。
制限のクリア	1つ以上のデバイス制限を削除します。
デバイスの選択的ワイプ	デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。
位置の表示	デバイスの位置を確認し、地理的制限を設定します。含まれるもの: デバイスの検索、デバイスの位置の確認、デバイスの追跡、デバイスの位置の経時的な追跡。
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、デバイスをリモートでロックします。

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、デバイスをリモートでロック解除します。
コンテナのロック	デバイス上の企業コンテナをリモートでロックします。
コンテナのロック解除	デバイス上の企業コンテナをリモートでロック解除します。
コンテナパスワードのリセット	企業コンテナのパスワードをリセットします。
ASM DEP/アクティベーションロックのバイパスを有効にする	アクティベーションロックが有効になっている場合、監視対象のiOSデバイスにバイパスコードを保存します。デバイスを消去する必要がある場合は、このコードを使用してアクティベーションロックを自動的に解除します。
デバイスを鳴らす	Windowsデバイスをリモートで5分間、最大音量で鳴らします。
デバイスを再起動する	XenMobileコンソールからWindowsデバイスを再起動します。
デバイスに展開する	アプリ、通知、制限などをデバイスに送信します。
デバイスを編集する	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からデバイスを追加または削除します。
デバイスのインポート	ファイルからデバイスのグループをXenMobileにインポートします。
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	デバイスがXenMobileに接続するのを禁止します。

アプリロック	デバイス上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XenMobileにログインできません。iOSでは、ユーザーはログインできますが、アプリにアクセスできません。
アプリワイプ	Androidでは、このアクションによりユーザーのXenMobileアカウントが削除されます。iOSでは、このアクションによりユーザーがXenMobile機能にアクセスするために必要な暗号化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確認します。
AirPlayミラーリングのリクエスト	AirPlayストリーミングの開始をリクエストします。
AirPlayミラーリングの停止	AirPlayストリーミングを停止します。
紛失モードを有効にする	**管理 > デバイス**で、監視対象デバイスを紛失モードに設定して、ロック画面でブロックできます。紛失モードでは、デバイスが紛失または盗難にあった場合に、デバイスを特定することもできます。
紛失モードを無効にする	**管理 > デバイス**で、紛失モードに設定されているデバイスの紛失モードを無効にできます。
デバイスのOSを更新	デバイスにOS更新制御デバイスポリシーを展開できます。
デバイスをシャットダウン	XenMobileコンソールからiOSデバイスをシャットダウンします。
デバイスを再起動	XenMobileコンソールからiOSデバイスを再起動します。

ローカルユーザーとグループ

管理者は、XenMobileの**管理 > ユーザー**ページでローカルユーザーとローカルユーザーグループを管理します。

ローカルユーザーを追加
ローカルユーザーを削除
ローカルユーザーを編集
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
ローカルユーザーロックIDの取得
ローカルユーザーロックの削除

登録

管理者は、登録招待を追加および削除したり、ユーザーに通知を送信したり、登録テーブルを.csvファイルにエクスポートしたりできます。

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を追加または削除します。
ユーザーへの通知	ユーザーまたはユーザーグループに登録招待を送信します。
登録招待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の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の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の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のポリシーをコピーします。
ポリシーの無効化	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	1つ以上のデリバリーグループにデバイスポリシーを割り当てます。

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アプリまたはエンタープライズアプリ (MDX対応ではない) 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アプリまたはエンタープライズアプリ (MDX対応ではない) を変更します。
MDX、Web、およびSaaSアプリの追加/削除	MDX対応アプリ、社内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のアプリ (SaaS) をXenMobileに追加または削除します。
MDX、Web、およびSaaSアプリの編集	MDX対応アプリ、社内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のアプリ (SaaS) をXenMobileに変更します。
カテゴリの追加/削除	XenMobile Storeにアプリが表示され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をデリバリーグループに割り当て	パブリックアプリストアアプリまたはMDX対応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。

MDX/WebLink/SaaSアプリをデリバリーグループに割り当て	MDX対応、シングルサインオンを必要としない (WebLink)、またはパブリックネットワークからのアプリ (SaaS) を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。

注:

コンソール機能 > アプリを選択すると、APIエンドポイント`GET <https://XMS_IP:4443/controlpoint/rest/ad>`は設計上LDAP情報を返します。

メディア

パブリックアプリストアまたはボリューム購入ライセンスを通じ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をデリバリーグループに割り当てる
アプリストアまたはエンタープライズブックの編集

アクション

アクションの追加/削除	トリガー（イベント、デバイスまたはユーザープロパティ、またはインストールされているアプリ名）と関連する応答によって定義されるアクションを追加または削除します。
アクションの編集	トリガー（イベント、デバイスまたはユーザープロパティ、またはインストールされているアプリ名）と関連する応答によって定義されるアクションを変更します。

アクションをデリバリーグループに割り当てる	ユーザーデバイスに展開するために、アクションをデリバリーグループに割り当てます。
アクションのエクスポート	[Actions] ページからアクション情報を収集し、.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、 > 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	指定されたユーザーとオプションのポリシー、アプリ、アクションを追加するデリバリーグループを作成または削除します。
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、ユーザーとオプションのポリシー、アプリ、アクションを修正します。
デリバリーグループの展開	デリバリーグループを使用可能にします。
デリバリーグループのエクスポート	[Delivery group] ページからデリバリーグループ情報を収集し、.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
登録プロファイルを編集
登録プロファイルをデリバリーグループに割り当てる

設定

管理者は、**設定**ページでさまざまな設定を構成します。

RBAC	RBACの割り当て、役割の割り当て。**重要:** この権限は、管理者自身に権限を割り当てる機能を含め、管理者にフルアクセスを許可します。このアクセスは、Endpoint Managementシステム内のすべてを操作する機能を付与する意図のあるユーザーにのみ許可してください。
LDAP	グループ、ユーザーアカウント、および関連プロパティをインポートするために、Active DirectoryなどのLDAP準拠ディレクトリを1つ以上管理します。
ライセンス	オンプレミスXenMobile Serverの場合。Citrix®ライセンスを管理します。
登録	ユーザーおよびセルフヘルプポータルの登録セキュリティ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いるリリースを表示します。含まれるもの: リリース管理の更新
証明書	APNS証明書、証明書SSLリスナーの編集
通知テンプレート	自動アクション、登録、およびユーザーへの標準通知メッセージ配信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	アプリケーション構成で使用するユーザーアカウントの作成、承認、および削除を管理します。
資格情報プロバイダー	デバイス証明書の発行を許可された1つ以上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、証明書の形式と、証明書の更新または失効の条件を制御します。
PKIエンティティ	公開鍵インフラストラクチャエンティティ（汎用、Microsoft Certificate Services、または裁量CA）を管理します。

PKI接続のテスト	サーバーがアクセス可能であることを確認するには、**設定 > PKIエンティティ** ページの **接続テスト** ボタンを使用します。
クライアントプロパティ	パスコードの種類、強度、有効期限など、ユーザーデバイス上のさまざまな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できる方法（メール、電話、またはサポートチケットメール）を設定します。
クライアントブランディング	XenMobile Store のカスタムストア名とデフォルトストアビューを作成します。XenMobile Store または 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ゲートウェイをセットアップして、XenMobile がキャリアSMSゲートウェイ経由で送信する通知を構成します。
通知サーバー	SMTPゲートウェイサーバーをセットアップして、ユーザーにメールを送信します。
ActiveSyncゲートウェイ	ルールとプロパティを通じて、ユーザーとデバイスへのユーザーアクセスを管理します。
Apple展開プログラム	XenMobile に Apple展開プログラムアカウントを追加します。
Apple Configuratorデバイス登録	XenMobile で Apple Configurator の設定を構成します。
iOS/ボリューム購入設定	Appleボリューム購入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インターフェースを使用して、BlackBerryおよびその他のExchange ActiveSyncデバイスを照会し、操作を発行します。

シトリックス ゲートウェイ	オンプレミスのXenMobile Serverの場合。Citrix Gatewayを追加します。認証を有効にするかどうか、および認証用のユーザー証明書をプッシュするかどうかを選択します。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コントロール	デバイスが非準拠であると判断され、ネットワークへのアクセスが拒否される条件を設定します。
サムスン ノックス	XenMobileがSamsung Knoxアテステーションサーバーの REST APIを照会できるように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。
シスログ	オンプレミスのXenMobile Serverの場合。サーバーのホスト名またはIPアドレスを使用して、ログファイルをシステムログ（syslog）サーバーに送信します。
XenAppおよびXenDesktop®	ユーザーがSecure Hubを介して仮想アプリとデスクトップを追加できるようにします。
シトリックス ファイルズ	XenMobileをエンタープライズアカウントで使用する場合：ShareFileアカウントと管理者サービスアカウントに接続してユーザーアカウントを管理するための設定を構成します。既存のCitrix Filesドメインと管理者資格情報が必要です。XenMobileをストレージゾーンコネクタで使用する場合：XenMobileを、ストレージゾーンコネクタで定義されたネットワーク共有およびSharePointの場所にポイントするように構成します。
エクスペリエンス向上プログラム	オンプレミスのXenMobile Serverの場合。匿名の統計情報と使用状況情報をCitrixに送信するかどうかを選択します。

マイクロソフト Azure	オンプレミスのXenMobile Serverの場合。XenMobileをMicrosoft Azureと統合します。
アンドロイド エンタープライズ	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。
XenMobileツール	XenMobileツールのページにアクセスします。
SNMP構成	XenMobile ServerノードでSNMPを有効にします。監視ユーザーの編集または追加、トラップ通知が表示されるSNMPマネージャーの設定、トラップ間隔と閾値の構成を行います。

サポート

管理者はさまざまなサポートタスクを実行できます。

Citrix Gateway接続チェック	IPアドレスでCitrix Gatewayのさまざまな接続チェックを実行します。ユーザー名とパスワードが必要です。
XenMobile接続チェック	データベース、DNS、Google Planなど、選択したXenMobile機能の接続チェックを実行します。
サポートバンドルの作成	オンプレミスXenMobile Serverの場合。トラブルシューティングのためにCitrixサポートに送信するファイルを作成します。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、およびXenMobileまたはCitrix Gatewayの最新の構成情報が含まれます。
Citrix製品ドキュメント	公開されているCitrix XenMobileドキュメントサイトにアクセスします。
シトリックス ナレッジセンター	Citrixサポートサイトにアクセスして、ナレッジベースの記事を検索します。

ログ	デバッグ、管理者監査、ユーザー監査のログファイルの詳細にアクセスして分析します。
クラスター情報	オンプレミスXenMobile Serverの場合。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XenMobile Serverの場合。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メモリプロパティ	オンプレミス版XenMobile Server向け。Javaメモリ使用量、メモリの詳細、メモリプールの詳細のスナップショットにアクセスします。
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入力します。単一のポリシーを構成し、そのポリシーを大規模なユーザーベースに展開し、ターゲットとなる各ユーザーにユーザー固有の値を表示させます。
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 Push Network署名（APNs）証明書のリクエストを送信するか、iOS用のSecure Mail APNs証明書をアップロードします。
シトリックス インサイト サービス	さまざまな問題の解決を支援するため、ログをCitrix Insight Services (CIS)にアップロードします。
Exchange ActiveSyncステータス用デバイスCitrix Gateway connector™	デバイスのActiveSync IDに基づいて、Exchange ActiveSync用Citrix Gateway connectorに送信されたデバイスのステータスをXenMobileに照会します。
匿名化と匿名化解除	オンプレミス版XenMobile Server向け。XenMobileでサポートバンドルを作成すると、機密性の高いユーザー、サーバー、および

	ネットワークデータはデフォルトで匿名化されます。この動作は、**Advanced**の下にある**Support > Anonymization and De-anonymization**で変更できます。
ログ設定	ログレベルをカスタマイズするか、カスタムロガーを追加します。

グループアクセスを制限する

管理者ユーザーは、すべてのユーザーグループに権限を適用できます。

サポートロール

サポートロールを持つユーザーは、リモートサポートにアクセスできます。これらの権限はデフォルトですべてのユーザーに適用され、この設定を編集することはできません。

ユーザーロール

ユーザーロールを持つユーザーは、XenMobileへのアクセスが次のように制限されます。

承認済みアクセス

セルフヘルプポータル	ユーザーはXenMobileのセルフヘルプポータルにのみアクセスできます。

コンソール機能

ユーザーはXenMobileコンソールへのアクセスが次のように制限されます。

デバイス

デバイスの完全ワイプ	デバイスからすべてのデータとアプリを消去します。デバイスにメモリカードがある場合は、それも含まれます。
選択的ワイプデバイス	デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。

位置の表示	デバイスの位置を確認し、地理的制限を設定します。含まれるもの: デバイスの検索、デバイスの位置の確認、デバイスの追跡、デバイスの位置を時系列で追跡
デバイスのロック	デバイスをリモートでロックして、使用できないようにします。
デバイスのロック解除	デバイスをリモートでロック解除して、使用できるようにします。
コンテナのロック	デバイス上の企業コンテナをリモートでロックします。
コンテナのロック解除	デバイス上の企業コンテナをリモートでロック解除します。
コンテナパスワードのリセット	企業コンテナのパスワードをリセットします。
ASM DEP/アクティベーションロックのバイパスを有効にする	監視対象のiOSデバイスでアクティベーションロックが有効になっている場合、バイパスコードを保存します。デバイスを消去する必要がある場合は、このコードを使用してアクティベーションロックを自動的に解除します。
デバイスを鳴らす	Windowsデバイスを5分間、最大音量でリモートで鳴らします。
デバイスを再起動する	Windowsデバイスを再起動します。
ソフトウェアインベントリを表示する	デバイスにインストールされているソフトウェアを確認します。

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を追加または削除します。
ユーザーに通知する	ユーザーまたはユーザーグループに登録招待を送信します。

グループアクセスを制限する

4つのデフォルトロールすべてにおいて、この権限はデフォルトで設定されており、すべてのユーザーグループに適用できます。このロールは編集できません。

RBACでロールを構成する

XenMobileのロールベースアクセス制御 (RBAC) 機能を使用すると、定義済みの役割、つまり一連の権限をユーザーとグループに割り当てることができます。これらの権限は、ユーザーがシステム機能にアクセスできるレベルを制御します。

XenMobileは、システム機能へのアクセスを論理的に分離するために、4つのデフォルトのユーザー役割を実装しています。

- **管理者:** 完全なシステムアクセスを許可します。
- **サポート:** リモートサポートへのアクセスを許可します。
- **ユーザー:** デバイスを登録し、セルフヘルプポータル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、カスタマイズしてユーザー役割を作成するためのテンプレートとして使用することもできます。デフォルトの役割で定義されている機能を超えて、特定のシステム機能にアクセスするための役割権限を割り当てることができます。

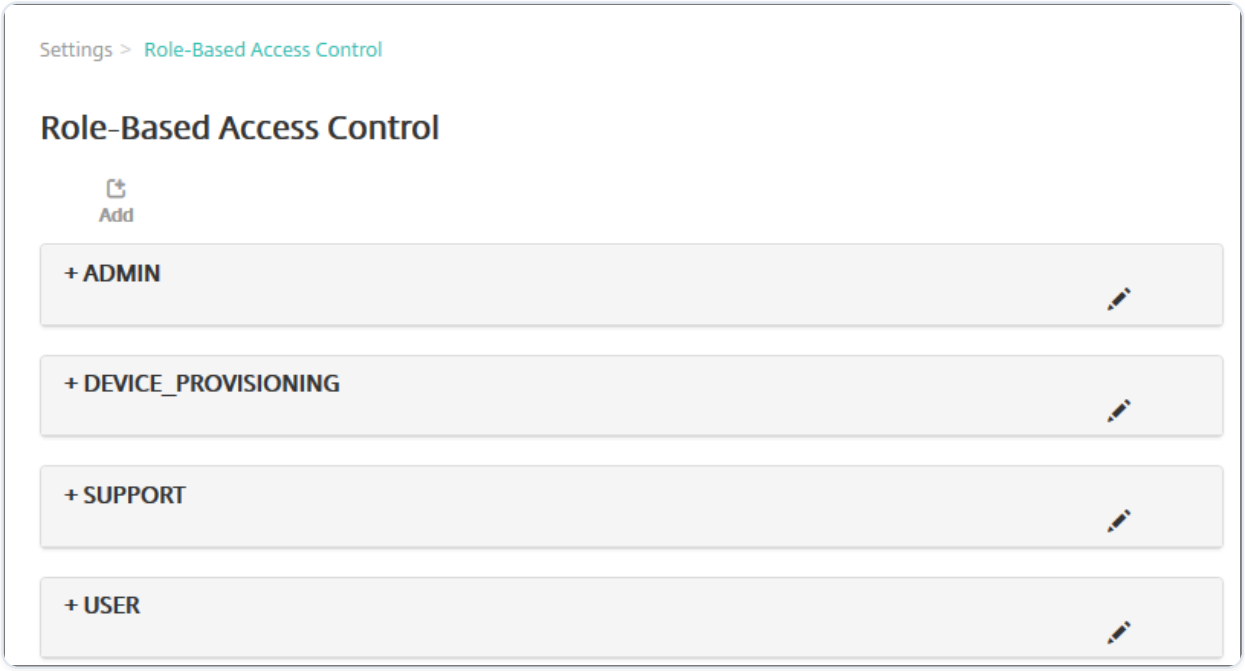
役割は、ローカルユーザー (ユーザーレベル) またはActive Directoryグループ (そのグループ内のすべてのユーザーが同じ権限を持つ) に割り当てることができます。ユーザーが複数のActive Directoryグループに属している場合、すべての権限がマージされ、そのユーザーの権限が定義されます。たとえば、ADGroupAのユーザーが管理者のデバイスを特定でき、ADGroupBのユーザーが従業員のデバイスをワイプできるとします。この場合、両方のグループに属するユーザーは、管理者と従業員の両方のデバイスを特定およびワイプできます。

> **注:**
>
> ローカルユーザーには、1つの役割のみが割り当てられる場合があります。

XenMobileのRBAC機能を使用して、次のことができます。

- 役割を作成します。
- 役割にグループを追加します。
- ローカルユーザーを役割に関連付けます。

1. XenMobileコンソールで、 > の順に移動します。 ページが表示され、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」の横にあるプラス記号（+）をクリックすると、次の図に示すように、その役割のすべての権限が表示されるように展開されます。

XenMobile RBAC構成(/en-us/xenmobile/server/media/rbac-device-provisioning.png)

2. 新しいユーザー役割を追加するには、 をクリックします。役割を編集するには、既存の役割の右側にあるペンアイコンをクリックします。役割を削除するには、役割の右側にあるゴミ箱アイコンをクリックします。デフォルトのユーザー役割は削除できません。

   - またはペンアイコンをクリックすると、 または ページが表示されます。
   - ゴミ箱アイコンをクリックすると、確認ダイアログが表示されます。選択した役割を削除するには、 をクリックします。

3. ユーザー役割を作成または編集するには、次の情報を入力します。

   - **RBAC名:** 新しいユーザー役割のわかりやすい名前を入力します。既存の役割の名前は変更できません。
   - **RBACテンプレート:** オプションで、新しい役割の開始点としてテンプレートをクリックします。既存の役割を編集している場合は、テンプレートを選択できません。

   RBACテンプレートは、デフォルトのユーザー役割です。これらは、その役割に関連付けられたユーザーが持つシステム機能へのアクセスを定義します。RBACテンプレートを選択すると、 および フィールドで、その役割に関連付けられたすべての権限を確認できます。テンプ

レートの使用はオプションです。 および フィールドで、役割に割り当てるオプションを直接選択できます。

XenMobile RBAC構成(/en-us/xenmobile/server/media/select-rbac-template.png)

4. 選択した フィールドの近くにある をクリックして、 および に事前定義されたアクセス権限と機能権限を設定します。

   XenMobile RBAC構成(/en-us/xenmobile/server/media/rbac-add-role.png)

5. 役割をカスタマイズするには、 および のチェックボックスを選択またはクリアします。

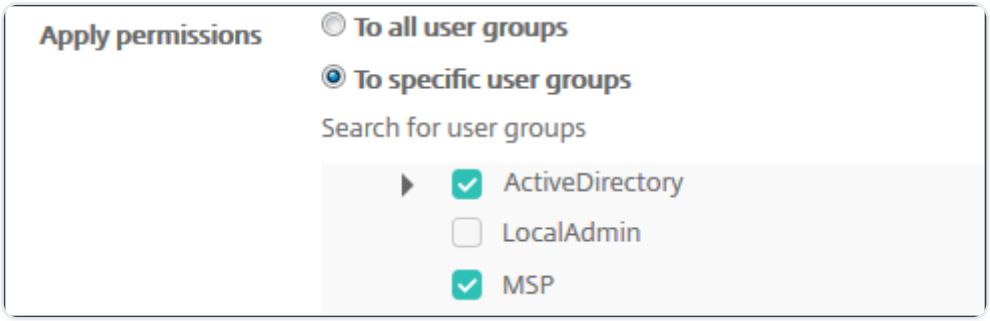
   コンソール機能の横にある三角形をクリックすると、その機能に固有の権限が表示され、選択またはクリアできます。トップレベルのチェックボックスをクリックすると、そのコンソール領域へのアクセスが禁止されます。トップレベルの下にある個々のオプションを選択して、それらのオプションを有効にします。たとえば、次の図では、 および オプションは、役割に割り当てられたユーザーには表示されません。チェックされたオプションは表示されます。

   XenMobile RBAC構成(/en-us/xenmobile/server/media/rbac-console-features.png)

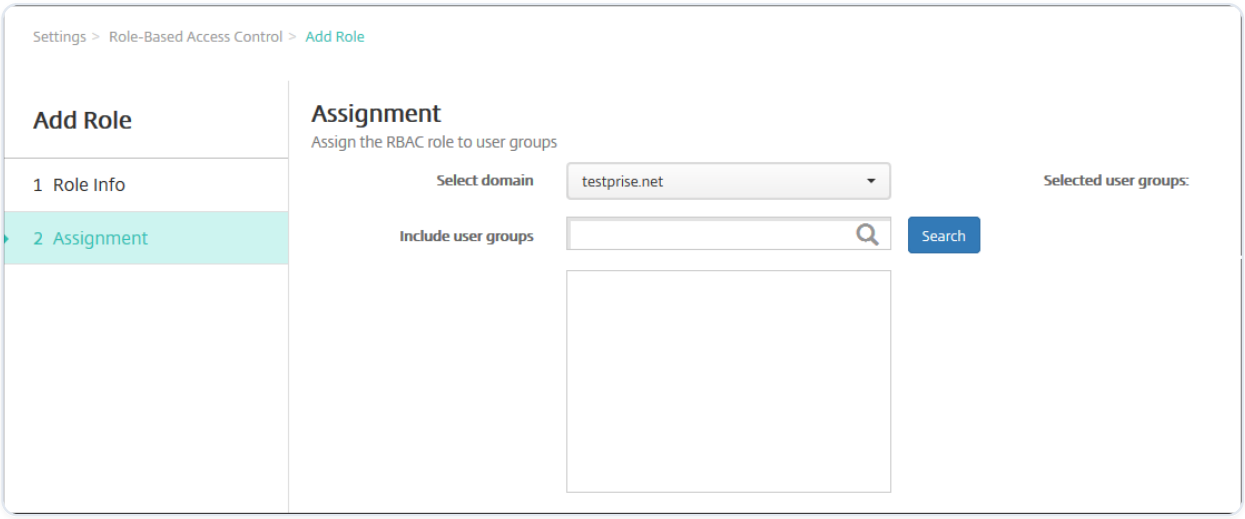
6. **権限の適用:** 管理者が管理できるグループを制限するために、1つ以上のユーザーグループを選択します。「**特定のユーザーグループへ**」をクリックすると、グループのリストが表示され、そこから1つ以上のグループを選択できます。

   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のみにアクセスできます。
   - 管理者は、他のローカルユーザーやADユーザーを表示できません。管理者は、それらのグループのいずれかの子グループのメンバーであるユーザーを表示できます。
   - 管理者は、次の宛先に招待を送信できます:
     - 権限グループとその子グループ
     - 権限グループとその子グループのメンバーであるユーザー

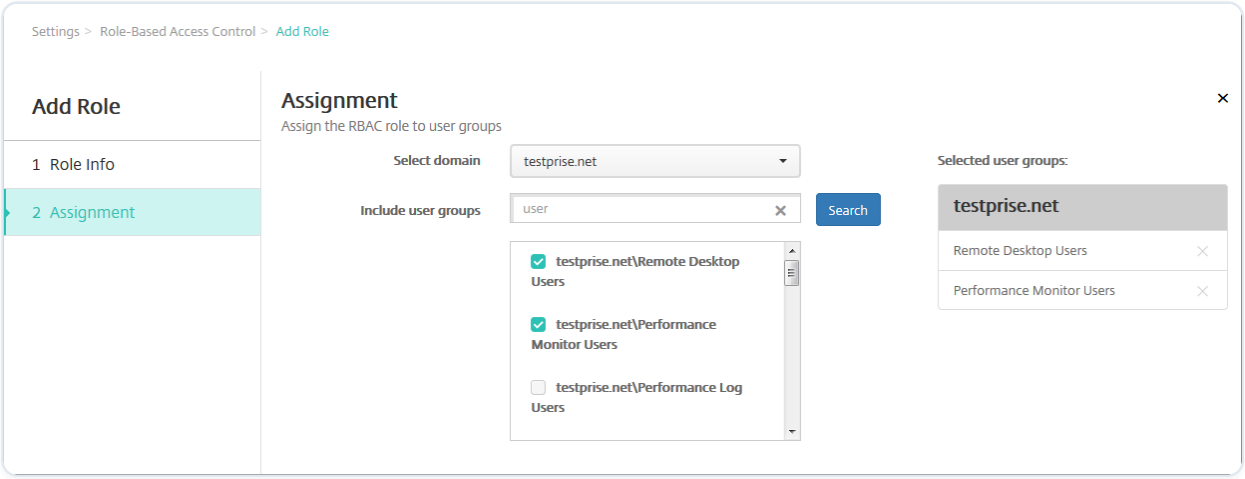


7. 「**次へ**」をクリックします。「**割り当て**」ページが表示されます。



8. 役割をユーザーグループに割り当てるには、次の情報を入力します。

- **ドメインの選択:** ドロップダウンリストからドメインをクリックします。
- **ユーザーグループを含める:** 「検索」をクリックして利用可能なすべてのグループのリストを表示するか、完全または部分的なグループ名を入力して、その名前を持つグループのみにリストを制限します。
- 表示されるリストで、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、そのグループは「**選択されたユーザーグループ**」リストに表示されます。



注：

「**選択されたユーザーグループ**」リスト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。

9. 「**保存**」をクリックします。

通知

XenMobile® の通知は、以下の目的で使用できます。

- 特定のシステム関連機能について、選択したユーザーグループと通信するため。これらの通知は、特定のユーザーを対象と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、コンプライアンス違反のデバイスを持つユーザー、従業員所有のデバイスを持つユーザーなどです。
- ユーザーとそのデバイスを登録するため。
- 特定の条件が満たされたときに、ユーザーに自動的に通知するため（自動アクションを使用）。例：
    - 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場合。
    - デバイスがジェイルブレイクまたはルート化されている場合

自動アクションの詳細については、「自動アクション」を参照してください。

XenMobile で通知を送信するには、ゲートウェイと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、Simple Mail Transfer Protocol (SMTP) および Short Message Service (SMS) ゲートウェイサーバーを構成し、ユーザーにメールおよびテキスト (SMS) 通知を送信できます。通知は、SMTP または SMS の 2 つの異なるチャネルでメッセージを送信するために使用できます。

- SMTP は、接続指向のテキストベースのプロトコルであり、メール送信者がコマンド文字列を発行し、必要なデータ（通常は Transmission Control Protocol (TCP) 接続経由）を提供することで、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（メッセージを送信する人）によって開始されたコマンドと、SMTP サーバーからの対応する応答で構成されます。
- 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ングサービスコンポーネントです。SMS 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デバイスが短いテキストメッセージを交換できるようにします。

XenMobile でキャリア SMS ゲートウェイを設定して、キャリアの SMS ゲートウェイを介して送信される通知を構成することもできます。キャリアは SMS ゲートウェイを使用して、電気通信ネットワークとの間で SMS 送信を送受信します。これらのテキストベースのメッセージは、標準

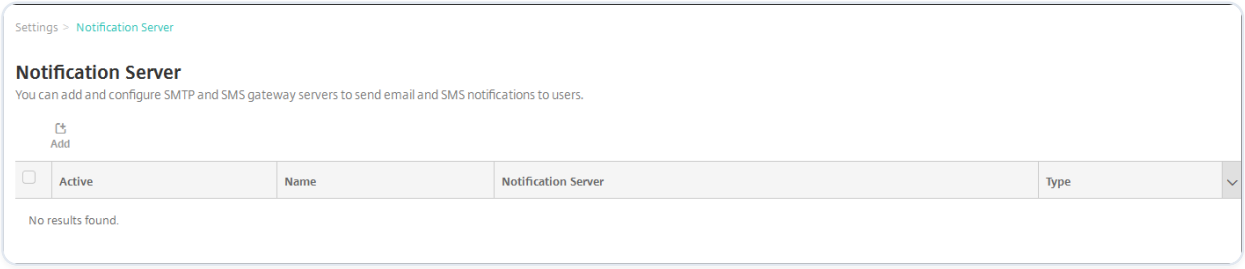
化された通信プロトコルを使用して、固定電話または携帯電話デバイスが短いテキストメッセージを交換できるようにします。

前提条件

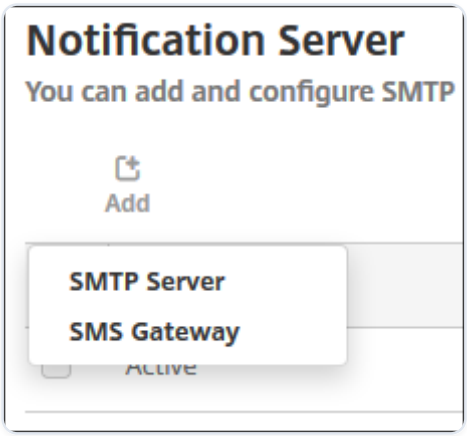
- SMS ゲートウェイを構成する前に、システム管理者に相談してサーバー情報を確認してください。SMS サーバーが社内サーバーでホストされているか、ホスト型メールサービスの一部であるかを知ることが重要です。後者の場合、サービスプロバイダーの Web サイトから情報が必要になります。
- SMTP 通知サーバーを構成して、ユーザーにメッセージを送信します。サーバーが社内サーバーでホストされている場合は、システム管理者に構成情報を問い合わせてください。サーバーがホスト型メールサービスである場合は、サービスプロバイダーの Web サイトで適切な構成情報を見つけてください。
- 1つのアクティブなSMTPサーバーと1つのアクティブなSMSサーバーを同時に使用できます。これらの両方の通信チャネルは、1つのアクティブな構成を許可します。
- ネットワークDMZ内にあるXenMobileからポート25を開放し、内部ネットワーク上のSMTPサーバーを指すようにします。これにより、XenMobileは通知を正常に送信できるようになります。

SMTPサーバーとSMSゲートウェイを構成する

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **通知**の下で、**通知サーバー**をクリックします。**通知サーバー**ページが表示されます。

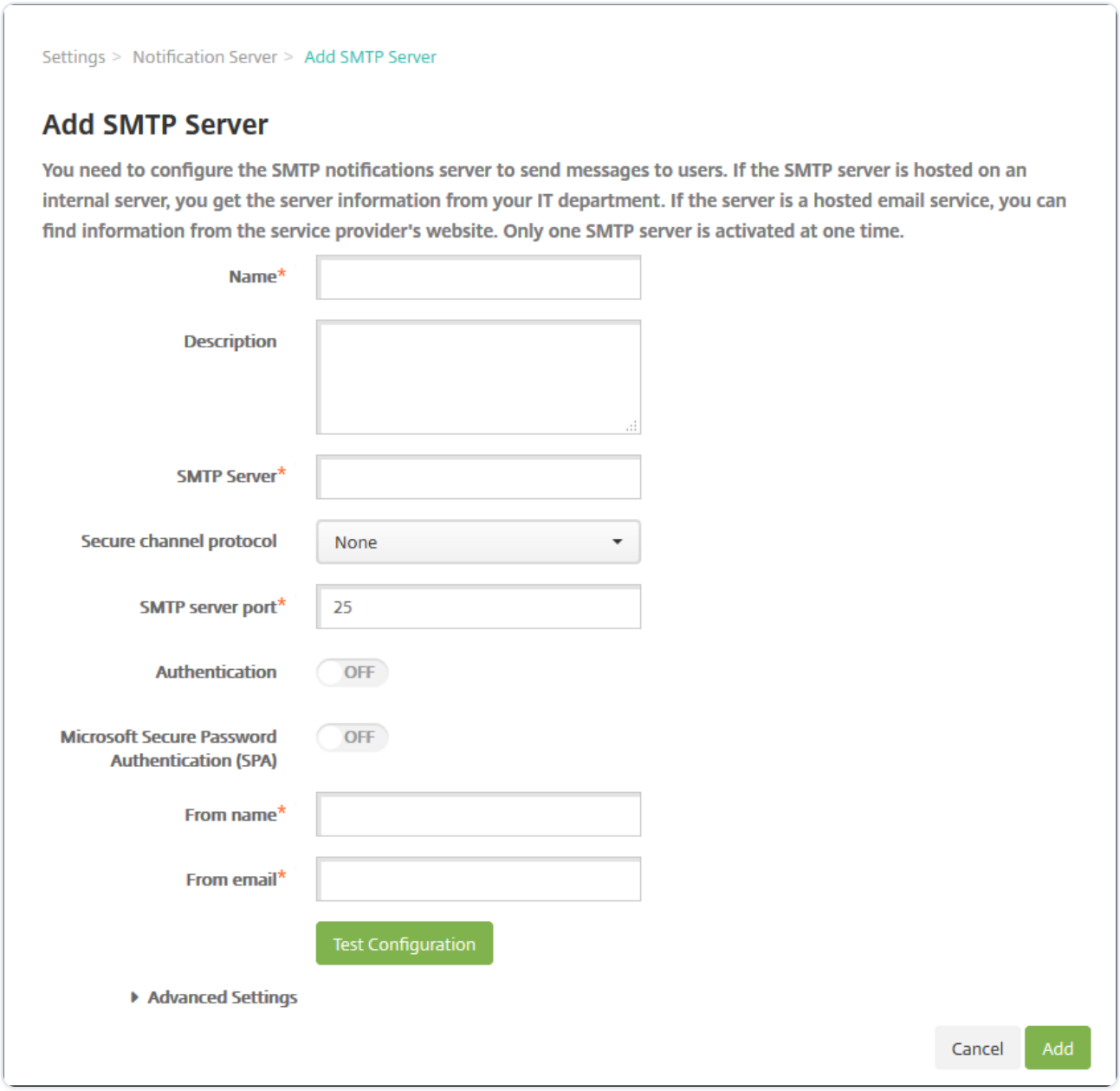


3. **追加**をクリックします。SMTPサーバーまたはSMSゲートウェイを構成するためのオプションを含むメニューが表示されます。



- SMTPサーバーを追加するには、**SMTPサーバー**をクリックし、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**をクリックし、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サーバーを追加する



1. これら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られた名前を入力します。
   - **説明:** 必要に応じて、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。ホスト名は、完全修飾ドメイン名(FQDN) またはIPアドレスである必要があります。
   - **セキュアチャネルプロトコル:** サーバーが使用するセキュアチャネルプロトコル（サーバーがセキュア認証を使用するように構成されている場合）のドロップダウンリストで、**SSL**、**TLS**、または**None**をクリックします。デフォルトは**None**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: ON**または**OFF**を選択します。デフォルトは**OFF**です。
- **認証**を有効にする場合は、次の設定を構成します。
  - **ユーザー名:** 認証用のユーザー名を入力します。
  - **パスワード:** 認証ユーザーのパスワードを入力します。

> **重要:**
>
> Microsoft Exchange OnlineでOAuthを使用するには、まずMicrosoft Entra IDにアプリケーションを登録する必要があります。登録後、**認証**と**Microsoft Exchange Online OAuth 2.0**を有効にします。

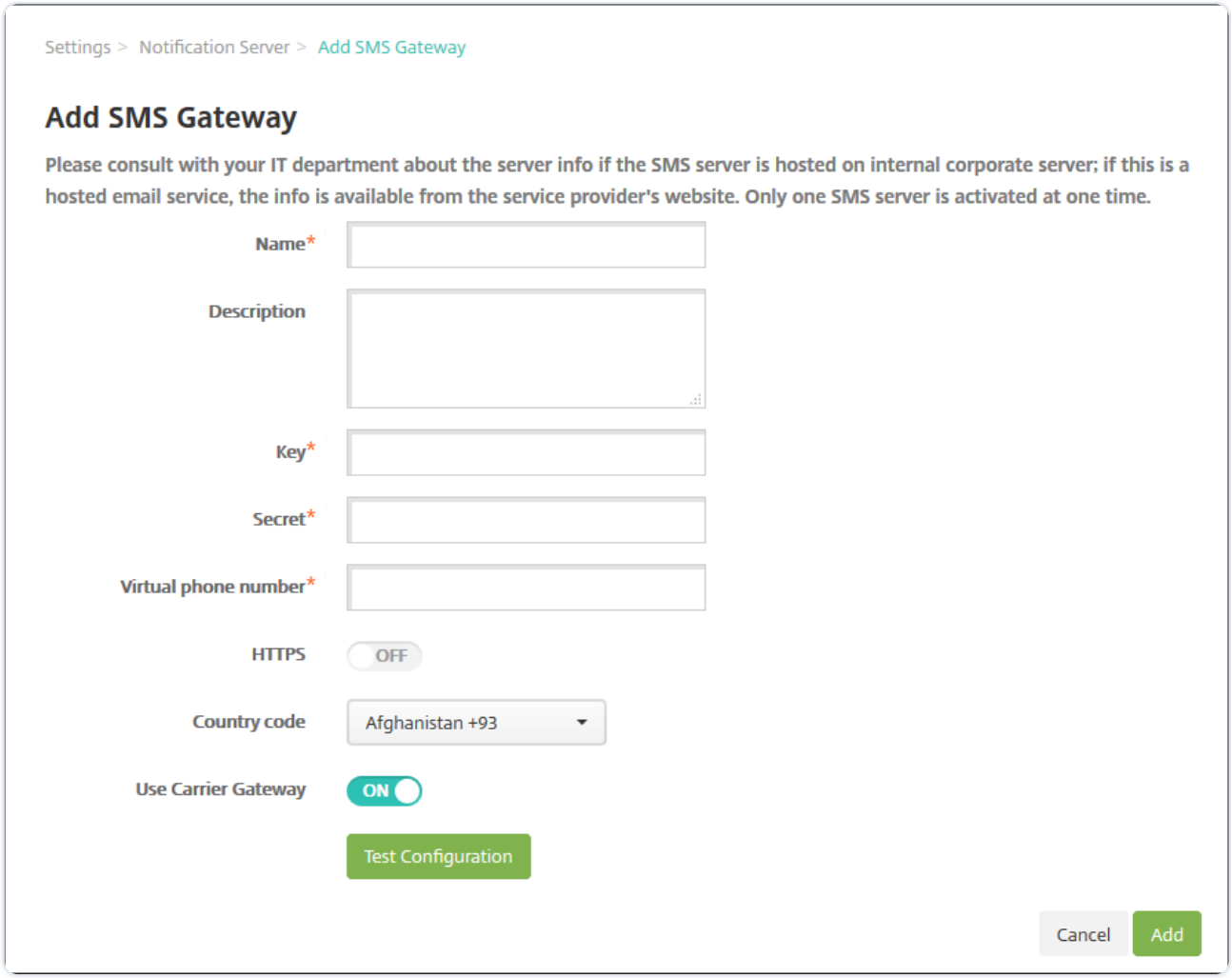
- **認証**と**Microsoft Exchange Online OAuth 2.0**を有効にする場合は、次の設定を構成します。
  - **ユーザー名:** 認証用のユーザー名を入力します。
  - **テナントID:** Microsoft Entra IDディレクトリのテナントIDを入力します。
  - **クライアントID:** 登録済みアプリケーションのクライアント（アプリケーション）IDを入力します。これは、Azure portal > 登録済みアプリケーション > **アプリケーション (クライアント) ID** で確認できます。
  - **クライアントシークレット:** 登録済みアプリケーションのクライアントシークレットを入力します。これは、Azure portal > 登録済みアプリケーション > **証明書とシークレット** で確認できます。
- **Microsoft Secure Password Authentication (SPA):** SMTPサーバーがSPAを使用している場合は、**ON**をクリックします。デフォルトは**OFF**です。
- **差出人名:** 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に、**差出人**ボックスに表示される名前を入力します。例: Corporate IT。
- **差出人メールアドレス:** SMTPサーバーから送信された通知にメール受信者が返信した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、テストメール通知を送信します。
3. **詳細設定**を展開し、次の設定を構成します。

- **SMTP再試行回数:** SMTPサーバーから送信された失敗したメッセージを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リクエストを送信する際に待機する時間（秒単位）を入力します。タイムアウトが原因でメッセージ送信が継続的に失敗する場合は、この値を増やしてください。この値を減らす場合は注意してください。タイムアウトしたメッセージや未配信メッセージの数が増加する可能性があります。デフォルトは30秒です。
- **SMTP受信者の最大数:** SMTPサーバーによって送信されるメールメッセージあたり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ゲートウェイを追加する



注:

> XenMobileはNexmo SMSメッセージングのみをサポートしています。Nexmoメッセージングを使用するためのアカウントをまだお持ちでない場合は、Webサイトにアクセスして作成してください。

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:** オプションで、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際にシステム管理者から提供された数値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:** パスワードを紛失または盗難した場合にアカウントにアクセスするために使用される、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（+1プレフィックス付き）に送信する場合に使用されます。Nexmoの仮想電話番号を入力する必要があり、このフィールドでは数字のみを使用する必要があります。仮想電話番号はNexmoのウェブサイトで購入できます。
   - **HTTPS:** NexmoにSMSリクエストを送信するためにHTTPSを使用するかどうかを選択します。デフォルトは**OFF**です。

   > **重要:**
   >
   > CitrixサポートからOFFにするよう指示がない限り、HTTPSは**ON**のままにしておきます。

   - **国コード:** 組織内の受信者向けのデフォルトのSMS国コードプレフィックスをドロップダウンリストでクリックします。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**をクリックして、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の接続エラーが検出され、すぐに表示されます。メッセージは、携帯電話間で送信されるメッセージと同じ時間枠で受信されます。
3. **追加**をクリックします。

キャリアSMSゲートウェイを追加する

XenMobileでキャリアSMSゲートウェイを設定して、キャリアのSMSゲートウェイを介して送信される通知を構成できます。キャリアは、電気通信ネットワークとの間でSMS送信を送受信するために、ショートメッセージサービス（SMS）ゲートウェイを使用します。これらのテキストベースのメッセージは、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デバイスが短いテキストメッセージを交換できるようにします。

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **通知**の下で、**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。

   通知サーバーSMSゲートウェイの追加(/en-us/xenmobile/server/media/settings-notifications-carrier-sms-gateway.png)
3. 次のいずれかを実行します。

   - 「**検出**」をクリックすると、ゲートウェイが自動的に検出されます。新しいキャリアが検出されなかったこと、または登録済みデバイスの中から検出された新しいキャリアを一覧表示するダイアログボックスが表示されます。
   - 「**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表示されます。

   通知サーバーがSMSゲートウェイを追加(/en-us/xenmobile/server/media/settings-notifications-carrier-sms-gateway-add.png)

   > **注：**
   >
   > XenMobileはNexmo SMSメッセージングのみをサポートしています。Nexmoメッセージングを使用するためのアカウントをまだお持ちでない場合は、Webサイトにアクセスして作成してください。
4. 次の設定を構成します。

   - **キャリア：** キャリア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ているドメインを入力します。
   - **国コード：** ドロップダウンリストで、キャリアの国コードをクリックします。

- **メール送信プレフィックス：** 必要に応じて、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**」をクリックして新しいキャリアを追加しないようにします。

通知テンプレートの作成と更新

XenMobileで通知テンプレートを作成または更新して、自動アクション、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。通知テンプレートは、Secure Hub、SMTP、SMSの3つの異なるチャネルでメッセージを送信するように構成します。

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イベントの異なる種類を反映した、多くの事前定義された通知テンプレートが含まれています。

> **注：**
>
> ユーザーに通知を送信するためにSMTPまたはSMSチャネルを使用する予定がある場合は、それらを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。XenMobileは、通知テンプレートを追加する際に、チャネルがまだ設定されていない場合に、チャネルを設定するように促します。

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
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**ページが表示されます。

   通知テンプレート設定ページの画像(/en-us/xenmobile/server/media/settings-notification-templates.png)

通知テンプレートを追加する

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通知の使用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サーバーの設定を今すぐ行うことを選択した場合、**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。使用したいチャネルを設定した後、**通知テンプレート**ページに戻り、通知テンプレートの追加または変更を続行できます。

   > **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、通知テンプレートを追加または編集する際にそれらのチャネルをアクティブ化できず、ユーザー通知の送信にそれらのチャネルが利用できなくなります。

2. これらの設定を構成します。

   - **名前:** テンプレートのわかりやすい名前を入力します。
   - **説明:** テンプレートの説明を入力します。
   - **種類:** ドロップダウンリストで通知の種類をクリックします。選択した種類でサポートされているチャネルのみが表示されます。APNS証明書有効期限テンプレートは1つのみ許可されており、これは事前定義されたテンプレートです。つまり、この種類の新しいテンプレートを追加することはできません。

> **注:**
>
> 一部のテンプレートタイプでは、タイプの下に「手動送信対応」というフレーズが表示されます。これは、**ダッシュボード**の**通知**リストおよび**デバイス**ページでテンプレートが利用可能であり、ユーザーに手動で通知を送信できることを意味します。手動送信は、いずれかのチャネルの件名またはメッセージフィールドで次のマクロを使用するテンプレートでは利用できません。
>
> - ${outofcompliance.reason(allowlist_blocklist_apps_name)}
> - ${outofcompliance.reason(smg_block)}

3. で、この通知で使用する各チャネルの情報を構成します。すべてのチャネルを選択することも、一部のチャネルを選択することもできます。選択するチャネルは、通知の送信方法によって異なります。

   - **Secure Hub** を選択した場合、iOS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で登録しているため、メッセージを受信します。
   - **SMS** を選択した場合、SIMカードを搭載したデバイスを使用しているユーザーのみが通知を受信します。

セキュアハブ:

- **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:** ユーザーに送信するメッセージを入力します。Secure Hubを使用している場合、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は、「マクロ」を参照してください。
- **サウンドファイル:** 通知を受信したときにユーザーが聞く通知サウンドをドロップダウンリストからクリックします。

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サーバーを設定した後にのみ、SMTP通知をアクティブ化できます。
- **送信者:** 通知のオプションの送信者を入力します。これは、名前、メールアドレス、またはその両方です。
- **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に対して、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事前構築済みマクロがあります。Citrixでは、テンプレート内のマクロを変更しないことをお勧めします。ユーザーに加えて、受信者（たとえば、企業管理者）をセミコロン（;）で区切ってアドレス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、このページで特定の受信者を入力するか、 **>** ページからデバイスを選択してそこから通知を送信できます。詳細については、「デバイス」を参照してください。
- **件名:** 通知のわかりやすい件名を入力します。このフィールドは必須です。
- **メッセージ:** ユーザーに送信す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サーバーを設定した後にのみ、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に対して、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、事前構築済みのマクロが含まれています。Citrixでは、テンプレート内のマクロを変更しないことをお勧めします。アドホック通知を送信するには、特定の受信者を指定するか、**［管理］>［デバイス］**ページからデバイスを選択できます。
- **メッセージ:** ユーザーに送信す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ると、［通知テンプレート］**ページにSMTP、SMS、Secure Hubの順で表示されます。正しく構成されていないチャネルは、正しく構成されたチャネルの後に表示されます。

通知テンプレートを編集する

1. 通知テンプレートを選択します。そのテンプレートに固有の編集ページが表示され、**［種類］**フィールドを除くすべての項目を変更したり、チャネルをアクティブ化または非アクティブ化したりできます。
2. **［保存］**をクリックします。

通知テンプレートを削除する

追加した通知テンプレートのみを削除できます。事前定義された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表示されます。
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キャンセルします。

デバイス

Citrix XenMobile® は、単一の管理コンソール内で、幅広い種類のデバイスをプロビジョニング、管理、保護、およびインベントリできます。

XenMobile Serverデータベースには、モバイルデバイスのリストが保存されます。各モバイルデバイスは、固有のシリアル番号または国際移動体装置識別番号 (IMEI)/モバイル機器識別子 (MEID) によって一意に定義されます。XenMobileコンソールにデバイスを登録するには、デバイスを手動で追加するか、ファイルからデバイスのリストをインポートできます。デバイスプロビジョニングファイル形式の詳細については、この記事の後半にある「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**」ページには、各デバイスと以下の情報が一覧表示されます。

- **ステータス:** アイコンは、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が利用可能か、および展開状態を示します。
- **モード:** デバイスモードがMDM、MAM、またはその両方であるかどうか。
- デバイスに関するその他の情報（例：**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**、**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**」テーブルをカスタマイズするには、最後見出しのドロップダウン矢印をクリックします。次に、テーブルに表示したい追加の見出しを選択するか、削除したい見出しの選択を解除します。

デバイステーブルのカスタマイズオプションの画像(/en-us/xenmobile/server/media/manage-devices-headings-menu.png)

デバイスの手動追加、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、デバイス詳細の編集、セキュリティアクションの実行、デバイスへの通知送信が可能です。また、すべてのデバイステーブルデータを.csvファイルにエクスポートして、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た場合、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。

デバイスを手動で追加する

1. XenMobileコンソールで、「**管理 > デバイス**」をクリックします。「**デバイス**」ページが表示されます。

   デバイスページの画像(/en-us/xenmobile/server/media/manage-devices-columns.png)

2. 「**追加**」をクリックします。「**デバイスの追加**」ページが表示されます。

   デバイスの追加ページの画像(/en-us/xenmobile/server/media/manage-devices-add-device.png)

3. これらの設定を構成します:

   - **プラットフォームの選択: iOS** または **Android** のいずれかをクリックします。
   - **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:** オプションで、Android デバイスの場合のみ、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** テーブルが表示され、デバイスがリストの下部に追加されます。追加したデバイスを選択し、表示されるメニューで **編集** をクリックして、デバイスの詳細を表示および確認します。

   > **注:**
   >
   > デバイスの横にあるチェックボックスを選択すると、オプションメニューがデバイスリストの上に表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

   - Enterprise (XME) または MDM モードで構成された XenMobile Server
   - LDAP が構成されている
   - ローカルグループとローカルユーザーを使用している場合:
     - 1つ以上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に関連付けられています。
   - Active Directory を使用している場合:
     - デリバリーグループは Active Directory グループに関連付けられています。

「デバイスの詳細」リストの画像(/en-us/xenmobile/server/media/manage-devices-details-general.png)

5. 「**一般**」ページには、シリアル番号、ActiveSync ID、およびプラットフォームタイプに関するその他の情報など、デバイスの「**識別子**」が一覧表示されます。「**デバイスの所有権**」には、「**会社所有**」または「**BYOD**」を選択します。

   「**一般**」ページには、強力なID、デバイスのロック、アクティベーションロックのバイパス、およびプラットフォームタイプに関するその他の情報など、デバイスの「**セキュリティ**」プロパティも一覧表示されます。「**デバイスの完全ワイプ**」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、ユーザーはそ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、ここで調べることができます。

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プロパティが一覧表示されます。このリストには、デバイスの追加に使用されたプロビジョニングファイルに含まれるすべてのデバイスプロパティが表示されます。プロパティを追加するには、「**追加**」をクリックし、リスト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ついては、PDF「デバイスプロパティ名と値」を参照してください。

   プロパティを追加すると、最初は追加したカテゴリの下に表示されます。「**次へ**」をクリックして「**プロパティ**」ページに戻ると、そのプロパティは適切なリストに表示されます。

   プロパティを削除するには、リストにカーソルを合わせ、右側の「**X**」をクリックします。XenMobileはすぐにその項目を削除します。

7. 残りの「**デバイスの詳細**」セクションには、デバイスの概要情報が含まれています。

   - 「**ユーザープロパティ**」：RBACロール、グループメンバーシップ、ボリューム購入アカウント、およびユーザーのプロパティを表示します。このページからボリューム購入アカウントを廃止できます。
   - 「**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を表示します。各ポリシーのポリシー名、種類、最終展開情報を提供します。
   - 「**アプリ**」：最後のインベントリについて、インストール済み、保留中、失敗したアプリ展開の数を表示します。アプリ名、識別子、種類、およびその他の情報を提供します。
   - 「**メディア**」：最後のインベントリについて、展開済み、保留中、失敗したメディア展開の数を表示します。
   - 「**アクション**」：展開済み、保留中、失敗したアクションの数を表示します。アクション名と最終展開時刻を提供します。

- 「**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を表示します。各展開について、デリバリーグループ名と展開時刻を提供します。デリバリーグループを選択すると、ステータス、アクション、チャネルまたはユーザーを含む詳細情報が表示されます。
- 「**iOSプロファイル**」：名前、種類、組織、説明を含む、最後のiOSプロファイルインベントリを表示します。
- 「**iOSプロビジョニングプロファイル**」：UUID、有効期限、管理されているかどうかなど、エンタープライズ配布プロビジョニングプロファイル情報を表示します。
- **証明書:** 有効、期限切れ、または失効した証明書について、種類、プロバイダー、発行者、シリアル番号、有効期限までの残り日数などの情報を表示します。
- **接続:** 最初の接続ステータスと最後の接続ステータスを表示します。各接続について、ユーザー名、最後から2番目の認証時刻、および最後の認証時刻を提供します。
- **MDMステータス:** MDMステータス、最終プッシュ時刻、最終デバイス応答時刻などの情報を表示します。

プロビジョニングファイルからデバイスをインポートする

モバイルオペレーターまたはデバイスメーカーから提供されたファイルをインポートすることも、独自のデバイスプロビジョニングファイルを作成することもできます。詳細については、この記事の後半にある「デバイスプロビジョニングファイルの形式」を参照してください。

1. **管理 > デバイス**に移動し、**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表示されます。

   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の画像(/en-us/xenmobile/server/media/manage-devices-import-provisioning-file.png)
2. **ファイルの選択**をクリックし、インポートするファイルに移動します。
3. **インポート**をクリックします。**デバイス**テーブルにインポートされたファイルが一覧表示されます。
4. デバイス情報を編集するには、デバイスを選択して**編集**をクリックします。**デバイスの詳細**ページについては、「デバイスを手動で追加する」を参照してください。

デバイスに通知を送信する

デバイスページからデバイスに通知を送信できます。通知の詳細については、「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表示されます。**受信者**フィールドには、通知を受信するすべてのデバイスが一覧表示されます。

   通知ダイアログボックスの画像(/en-us/xenmobile/server/media/manage-devices-notification.png)
3. これらの設定を構成します。

   - **テンプレート:** リストで、送信したい通知の種類をクリックします。**アドホック**を除く各テンプレートでは、**件名**フィールドと**メッセージ**フィールドに、選択したテンプレートに設定されているテキストが表示されます。
   - **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**と**SMS**です。各チャネルのメッセージ形式を確認するには、タブをクリックします。
   - **送信者:** オプションの送信者を入力します。
   - **件名: アドホック**メッセージの件名を入力します。
   - **メッセージ: アドホック**メッセージのメッセージを入力します。
4. **通知**をクリックします。

デバイステーブルをエクスポートする

1. エクスポートファイルに表示したい内容に応じて、**デバイス**テーブルをフィルターします。
2. **デバイス**テーブルの上にある**エクスポート**ボタンをクリックします。XenMobileは、フィルターされた**デバイス**テーブルの情報を抽出し、.csvファイルに変換します。
3. プロンプトが表示されたら、.csvファイルを開くか保存します。

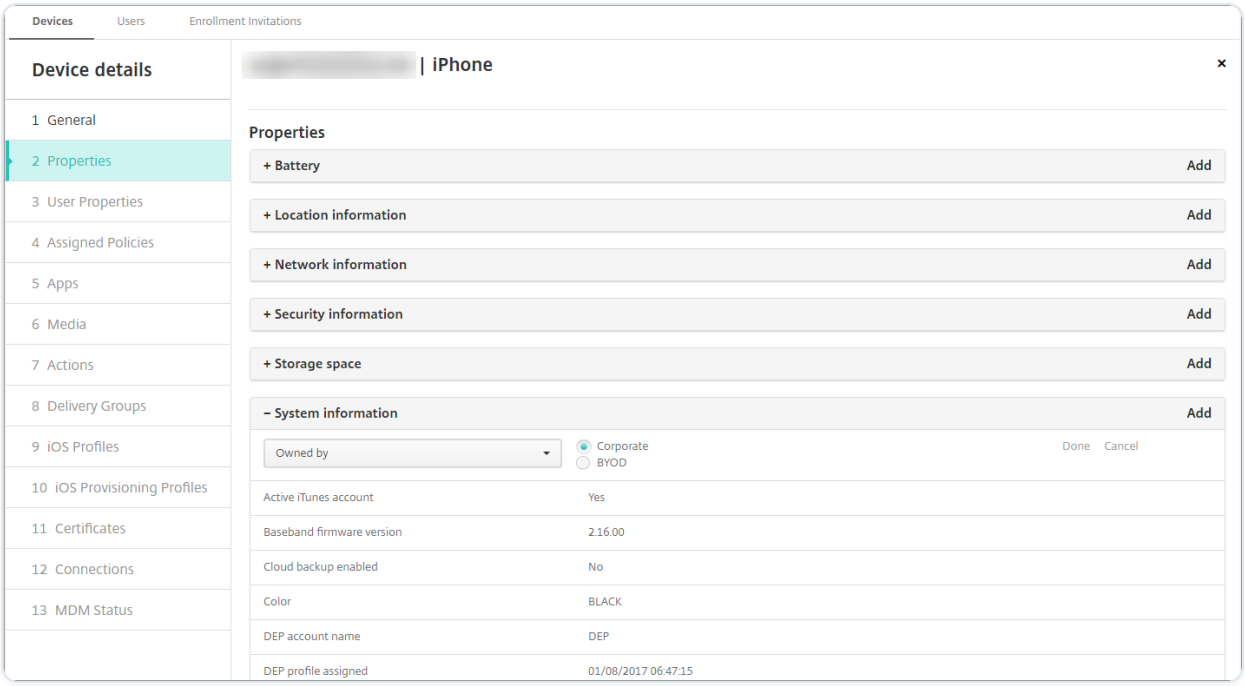
ユーザーデバイスを手動でタグ付けする

XenMobileでデバイスを手動でタグ付けするには、次の方法があります。

- 招待ベースの登録プロセス中。
- セルフヘルプポータル登録プロセス中。
- 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

デバイスを企業所有または従業員所有としてタグ付けするオプションがあります。セルフヘルプポータルを使用してデバイスを自己登録する場合、デバイスを企業所有または従業員所有としてタグ付けできます。デバイスを手動でタグ付けすることもできます。その方法は次のとおりです。

1. XenMobileコンソールの**デバイス**タブからデバイスにプロパティを追加します。
2. **Owned by**という名前のプロパティを追加し、**Corporate**または**BYOD** (従業員所有) 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の形式

多くのモバイルオペレーターまたはデバイスメーカーは、承認されたモバイルデバイスのリストを提供しています。これらのリストを使用すると、多数のモバイルデバイスを手動で入力する手間を省くことができます。XenMobileは、サポートされている3つのデバイスタイプ（Android、iOS、Windows）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、デバイスをXenMobileにインポートするため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

次の点に注意してください。

- 各プロパティの有効な値については、PDF デバイスプロパティ名と値を参照してください。
- UTF-8文字セットを使用してください。
- プロビジョニングファイル内のフィールドを区切るには、セミコロン (;) を使用します。フィールドの一部にセミコロンが含まれている場合は、バックスラッシュ文字 (\\) でエスケープします。

たとえば、このプロパティの場合：

`propertyV;test;1;2`

次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要です。
- その他のデバイスプラットフォームでは、シリアル番号またはIMEIのいずれかを含める必要があります。
- **OperatingSystemFamily** の有効な値は、**WINDOWS**、**ANDROID**、または **iOS** です。

デバイスプロビジョニングファイルの例：

```
`1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;prop
ertyV\;test\;1\;2;prop 2

2050BF3F51730108161006551059039l;25244201625379902;ANDROID;propertyN;prope
rtyV$*&&éééétest

3050BF3F51730108161006551059039l;35244201625379903;iOS;test;

4050BF3F51730108161006551059039l;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;`
```

ファイル内の各行はデバイスを表します。上記のサンプルの最初の項目は次のことを意味します。

- シリアル番号: `1050BF3F51730108161006551059039l`
- IMEI: `15244201625379901`
- OperatingSystemFamily: `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

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とデスクトップ（またはラップトップ）コンピューター間でデータを同期します。

XenMobile で ActiveSync Gateway ルールを構成できます。これらのルールに基づいて、デバイスの ActiveSync データへのアクセスを許可または拒否できます。たとえば、「必須アプリの不足」ルールをアクティブ化すると、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。各ルールについて、**「許可」**または**「拒否」**のいずれかを選択できます。デフォルト設定は**「許可」**です。

アプリアクセスデバイ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 は、次のルールをサポートしています。

匿名デバイス： デバイスが匿名モードであるかどうかを確認します。このチェックは、デバイスが再接続しようとしたときに XenMobile がユーザーを再認証できない場合に利用できます。

Samsung KNOX 認証の失敗： デバイスが Samsung KNOX 認証サーバーへのクエリに失敗したかどうかを確認します。

禁止アプリ： アプリアクセスポリシーで定義されている禁止アプリがデバイスにあるかどうかを確認します。

暗黙的な許可と拒否： このアクションは、ActiveSync Gateway のデフォルトです。ゲートウェイは、他のフィルタールール条件を満たさないすべてのデバイスのデバイスリストを作成し、そのリストに基づいて接続を許可または拒否します。ルールが一致しない場合、デフォルトは暗黙的な許可です。

非アクティブなデバイス： サーバープロパティの**デバイス非アクティブ日数しきい値**設定で定義されているように、デバイスが非アクティブであるかどうかを確認します。

必須アプリの不足： アプリアクセスポリシーで定義されている必須アプリがデバイスに不足しているかどうかを確認します。

推奨されないアプリ： アプリアクセスポリシーで定義されている推奨されないアプリがデバイスにあるかどうかを確認します。

非準拠パスワード： ユーザーパスワードが準拠しているかどうかを確認します。iOS および Android デバイスでは、XenMobile は、デバイス上の現在のパスワードがデバイスに送信されたパスコードポリシーに準拠しているかどうかを判断できます。たとえば、iOS では、XenMobile がパスコードポリシーをデバイスに送信した場合、ユーザーはパスワードを設定するために 60 分間与えられます。ユーザーがパスワードを設定する前は、パスコードが非準拠である可能性があります。

非準拠デバイス： 非準拠デバイスプロパティに基づいて、デバイスが非準拠であるかどうかを確認します。このプロパティは通常、自動アクションまたは XenMobile API を利用するサードパーティによって変更されます。

失効ステータス： デバイス証明書が失効したかどうかを確認します。失効したデバイスは、再度承認されるまで再登録できません。

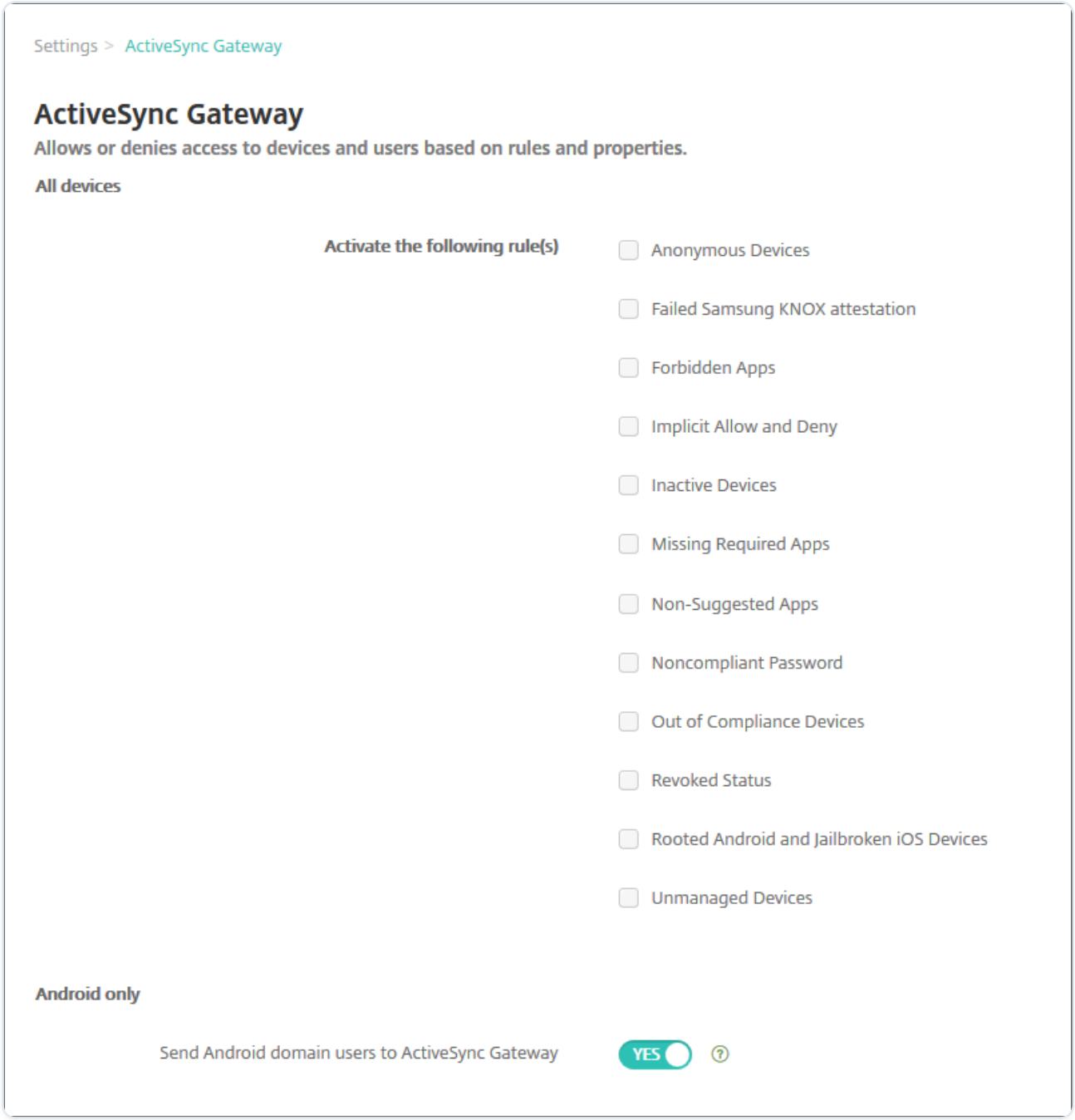
Rooted Android and Jailbroken iOS Devices: AndroidまたはiOSデバイスがジェイルブレイクされているかどうかを確認します。

Unmanaged Devices: デバイスがXenMobileの制御下で管理された状態にあるかどうかを確認します。たとえば、MAMに登録されているデバイスや登録解除されたデバイスは管理されていません。

Send Android domain users to ActiveSync Gateway: はいをクリックして、XenMobileがAndroidデバイス情報をActiveSync Gatewayに送信するようにします。

ActiveSync Gateway設定を構成するには

1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**の下にある**ActiveSync Gateway**をクリックします。**ActiveSync Gateway**ページが表示されます。



1. **次のルールをアクティブ化**で、アクティブ化するルールを1つ以上選択します。
2. **AndroidのみのAndroidドメインユーザーをActiveSync Gatewayに送信**で、**はい**をクリックして、XenMobileがAndroidデバイス情報をActiveSync Gatewayに送信するようにします。
3. **保存**をクリックします。

デバイス管理からAndroid Enterpriseへの移行

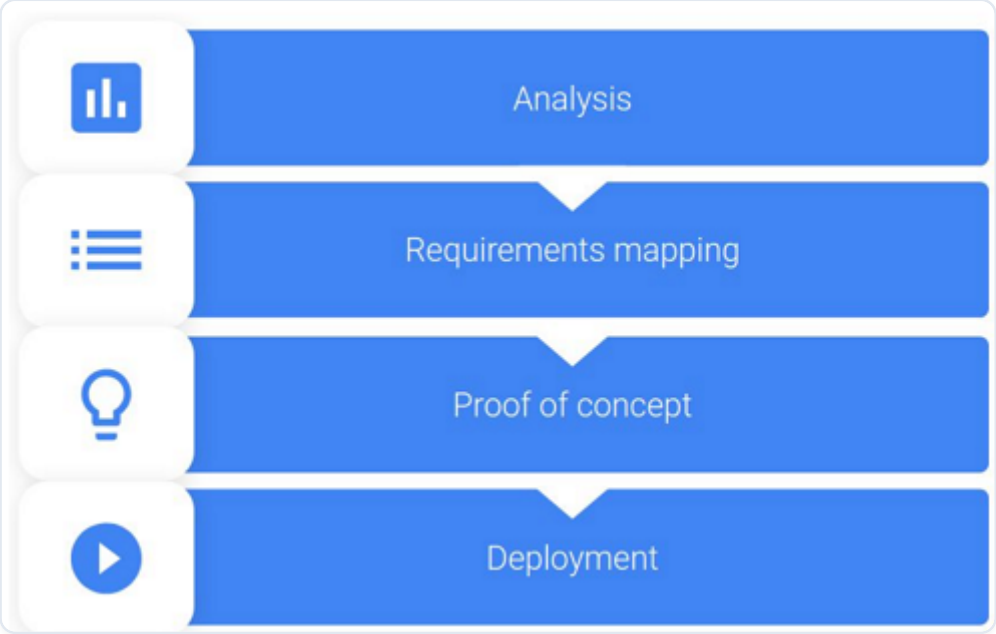
この記事では、従来のAndroidデバイス管理からAndroid Enterpriseへの移行に関する考慮事項と推奨事項について説明します。GoogleはAndroid Device Administration APIを非推奨にしています。

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デバイスのデフォルトの登録方法としてAndroid Enterpriseに移行しています。GoogleがAPIを非推奨にした後、デバイス管理モードのAndroid Qデバイスでは登録が失敗します。

Android Enterpriseには、完全管理モードと仕事用プロファイルデバイスモードのサポートが含まれています。Googleの出版物であるAndroid Enterprise Migration Bluebookでは、従来のデバイス管理とAndroid Enterpriseがどのように異なるかについて詳しく説明しています。Googleからの移行情報を読むことをお勧めします。

その出版物では、デバイス管理移行の4つのフェーズについても説明しており、以下の図が含まれています。この記事には、移行フェーズに関するXenMobile固有の推奨事項が含まれています。



> Android Enterprise Migration Bluebookからの図。 Googleの許可を得て再公開。

デバイス管理の非推奨化の影響

Googleは以下のデバイス管理APIを非推奨にしています。Secure HubをAndroid Q APIレベルをターゲットにするようにアップグレードした後、これらのAPIはAndroid Qを実行しているデバイスでは動作しません。

- カメラの無効化: デバイスカメラへのアクセスを制御します。
- パスワードの有効期限: 設定可能な期間が経過した後、ユーザーにパスワードの変更を強制します。

- パスワードの制限: 制限的なパスワード要件を設定します。

非推奨のAPIは、Citrix MAM専用モードで登録されたデバイスには影響しません。

推奨事項

以下の推奨事項は、すでにAndroidレガシーデバイス管理モード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専用モードに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	推奨されるアクション
既存のデバイスがデバイス管理モードに登録されており、Android Qにアップグレード可能です。	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に移行してください。
既存のデバイスがデバイス管理モードに登録されています。このデバイスはAndroid Qにアップグレードできません。	デバイスはデバイス管理モードのままで構いません。ただし、デバイスを更新する際には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に登録されており、Android Qにアップグレードされています。	GoogleがAPIを非推奨にする前に、デバイス管理モードからAndroid Enterpriseに移行してください。これらのデバイスに関する警告メッセージがXenMobileコンソールに表示されます。
Android Qを搭載して提供され、デバイス管理モードに登録された新しいデバイス。	GoogleがAPIを非推奨にする前に、デバイス管理モードからAndroid Enterpriseに移行してください。これらのデバイスに関する警告メッセージがXenMobileコンソールに表示されます。
Android Qを搭載して提供される、またはAndroid Qにアップグレード可能な新しいデバイス。このデバイスは登録されていません。	新しいデバイスにはAndroid Enterpriseを使用してください。
GoogleがAPIを非推奨にした後、Android Qを搭載した新規または既存のデバイスがデバイス管理モードに登録されます。	非推奨となるGoogle APIの影響を避けるため、CitrixはGoogleがAPIを非推奨にする前にAndroid Enterpriseへの移行を推奨します。その日付以降、これらのデバイスの登録は失敗します。

デバイス登録ステータス	推奨されるアクション
Citrix MAM専用モードに登録されている新規または既存のデバイス	アクションは不要です。非推奨のGoogle APIは、MAM専用モードのデバイスには影響しません。

分析

移行の分析フェーズは以下で構成されます。

- レガシーAndroidセットアップの理解
- レガシー機能をAndroid Enterprise機能にマッピングできるように、レガシーセットアップを文書化する

推奨される分析

1. XenMobileでのAndroid Enterpriseの評価: フルマネージド、ワークプロファイル付きフルマネージド、専用デバイス、ワークプロファイル (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、次の手順を実行します。

1. スプレッドシートを作成し、XenMobileコンソール内の現在のポリシーグループをリストアップします。
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. 各ユースケースについて、以下を文書化します。
    - 名前
    - ビジネスオーナー
    - ユーザーIDモデル
    - デバイス要件
        - セキュリティ
        - 管理
        - 使いやすさ
    - デバイスインベントリ

    - メーカーとモデル
    - OSバージョン
  - アプリ

4. 各アプリについて、以下をリストアップします。
   - 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
   - アプリが必須であるかどうか (true/false)

要件マッピング

完了した分析に基づいて、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。
   - ワークプロファイル (BYOD): 再登録が必要です。工場出荷時設定へのリセットは不要です。
   - フルマネージド: 工場出荷時設定への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) 識別子、ゼロタッチを使用してデバイスを登録します。
2. アプリケーション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。各デバイス要件について、その要件に最も近い機能と、それに対応するAndroidバージョンを文書化します。
4. 機能要件に基づいて、最小のAndroid OS (7.0、8.0、9.0) を決定します。
5. IDモデルを選択します。
   - 推奨: マネージドGoogle Playアカウント
   - Google Cloud Identityのお客様である場合にのみ、Google G-Suiteアカウントを使用してください。
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: デバイスがサポートされている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

要件マッピングを完了したら、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動します。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

  a. 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。

  b. デリバリーグループを選択します。アプリが必須の場合は、そのアプリをデリバリーグループの**必須アプリ**リストに移動します。

  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、社内またはサードパーティの開発者によって開発されます。プライベートアプリはGoogle Playを使用して公開することをお勧めします。

  a. 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。

  b. APKファイルをアップロードし、アプリ設定を構成します。

  c. アプリを必要なデリバリーグループに公開します。

- MDXアプリ

  a. 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。

  b. 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。

  c. MDXポリシーを選択します。

  Enterprise MDXアプリについては、MDX SDKモードでラップされたアプリに変更することをお勧めします。

  - オプション1：組織にプライベートに割り当てられた開発者アカウントを使用して、Google PlayでAPKをホストします。XenMobileでMDXファイルを公開します。

    - オプション2：XenMobileからアプリをエンタープライズアプリとして公開します。XenMobileでAPKを公開し、MDXファイルのプラットフォームとして**Android Enterprise**を選択します。

Citrixデバイスポリシーの移行

AndroidおよびAndroid Enterpriseプラットフォームの両方で利用可能なポリシーの場合：ポリシーを編集し、プラットフォームとして**Android Enterprise**を選択します。

Android Enterpriseの場合、登録モードを考慮してください。一部のポリシーオプションは、ワーク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利用可能です。

概念実証

アプリをAndroid Enterpriseに移行した後、移行テストを設定して、機能が意図どおりに動作していることを確認できます。

推奨される概念実証のセットアップ

1. 展開インフラストラクチャをセットアップします。
    - 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. ユーザーアプリをセットアップします。
3. Android Enterprise機能を構成します。
4. Android Enterpriseデリバリーグループにポリシーを割り当てます。
5. 機能をテストして確認します。
6. 各ユースケースのデバイスセットアップウォークスルーを完了します。
7. ユーザーセットアップ手順を文書化します。

展開

これで、Android Enterpriseのセットアップを展開し、ユーザーを移行に備えることができます。

推奨される展開戦略

Citrixが推奨する展開戦略は、すべての本番システムでAndroid Enterpriseをテストし、その後でデバイスの移行を完了することです。

- このシナリオでは、ユーザーは現在の構成でレガシーデバイスを使い続けます。Android Enterprise管理用に新しいデバイスをセットアップします。

- 既存のデバイスは、アップグレードまたは交換が必要な場合にのみ移行します。
- 既存のデバイスは、通常のライフサイクルの終わりに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それらのデバイスを移行します。

アンドロイド エンタープライズ

Android Enterpriseは、Androidデバイス向けのエンタープライズ管理ソリューションとしてGoogleが提供するツールとサービスのセットです。Android Enterpriseを使用すると、次のことができます。

- XenMobile®を使用して、会社所有のAndroidデバイスと個人所有のデバイス (BYOD) のAndroidデバイスを管理します。
- デバイス全体、またはデバイス上の個別のプロファイルを管理できます。個別のプロファイルは、ビジネスアカウント、アプリ、データを個人アカウント、アプリ、データから分離します。
- 在庫管理など、単一の用途に特化したデバイスを管理することもできます。GoogleのAndroid Enterprise機能の概要については、「Android Enterprise Management」を参照してください。

リソース:

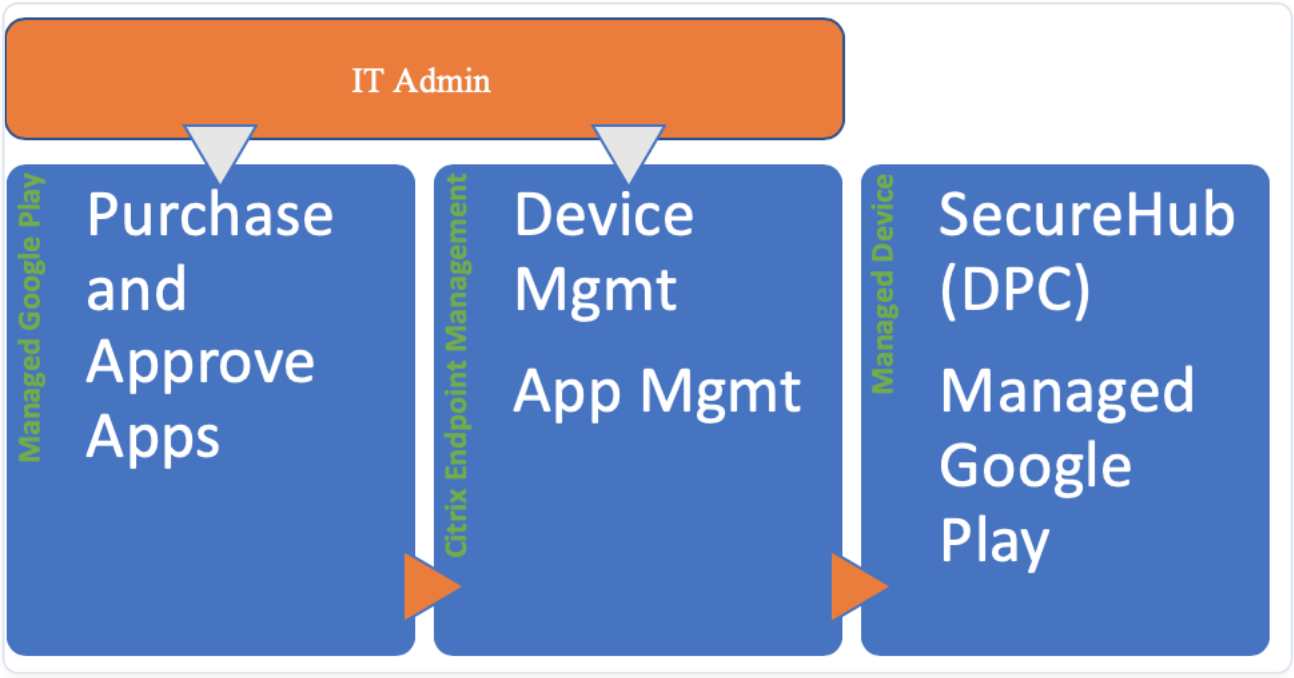
- Android Enterpriseに関連する用語と定義のリストについては、Google Android Enterprise開発者ガイドの「Android Enterprise terminology」を参照してください。Googleはこれらの用語を頻繁に更新します。
- XenMobileでサポートされているAndroidオペレーティングシステムについては、「Supported device operating systems」を参照してください。
- Android Enterpriseのネットワーク環境をセットアップする際に考慮すべきアウトバウンド接続については、Googleサポート記事「Android Enterprise Network Requirements」を参照してください。

XenMobileをManaged Google Playと統合してAndroid Enterpriseを使用すると、エンタープライズが作成されます。Googleは、エンタープライズを組織とエンタープライズモビリティ管理 (EMM) ソリューション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じ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、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、完全な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、セキュアなデジタルワークスペースのための統合されたXenMobile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ための手段を提供します。
- **Citrix Secure Hub™:** Citrix DPCアプリ。Secure HubはXenMobileの起動パッドです。Secure Hubはデバイスにポリシーを適用します。
- **Managed Google Play:** XenMobileと統合されるGoogleエンタープライズアプリプラットフォーム。Google Play EMM APIは、アプリポリシーを設定し、アプリを配布します。

この図は、管理者がこれらのコンポーネントとどのようにやり取りし、コンポーネントが互いにどのようにやり取りするかを示しています。



XenMobile で管理対象の Google Play を使用する

> **注記:**
>
> Citrix を EMM プロバイダーとして登録するには、管理対象の Google Play または Google Workspace のいずれかを使用できます。この記事では、管理対象の Google Play で Android Enterprise を使用する方法について説明します。組織が Google Workspace を使用してアプリへのアクセスを提供している場合は、Android Enterprise でそれを使用できます。「Google Workspace (旧 G-Suite) のお客様向けのレガシー Android Enterprise」を参照してください。

> 管理対象の Google Play を使用する場合、デバイスとエンドユーザー向けに管理対象の Google Play アカウントをプロビジョニングします。管理対象の Google Play アカウントは、管理対象の Google Play へのアクセスを提供し、ユーザーが利用可能なアプリをインストールして使用できるようにします。組織がサードパーティの ID サービスを使用している場合、管理対象の Google Play アカウントを既存の ID アカウントとリンクできます。

このタイプのエンタープライズはドメインに縛られないため、単一の組織に対して複数のエンタープライズを作成できます。たとえば、組織内の各部門または地域は、異なるエンタープライズとして登録し、個別のデバイスとアプリのセットを管理できます。

XenMobile 管理者にとって、管理対象の Google Play は、Google Play のユーザーエクスペリエンスとアプリストア機能を、エンタープライズ向けに設計された一連の管理機能と組み合わせています。管理対象の Google Play を使用して、デバイス上の Android Enterprise ワークスペースに展開するアプリを追加、購入、承認します。Google Play を使用して、公開アプリ、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にとって、管理対象の Google Play はエンタープライズアプリストアです。ユーザーはアプリを閲覧し、アプリの詳細を表示し、インストールできます。公開版の Google Play とは異なり、ユーザーは管理対象の Google Play から、利用可能にしたアプリのみをインストールできます。

デバイス展開シナリオと動作モード

デバイス展開シナリオとは、展開するデバイスの所有者と、それらをどのように管理するかを指します。デバイスプロファイルとは、DPC がデバイス上のポリシーをどのように管理し、適用するかを指します。

仕事用プロファイルは、ビジネスアカウント、アプリ、データを個人アカウント、アプリ、データから分離します。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。

> **重要:**

> Android Enterprise デバイスが Android 11 にアップデートされると、Google は「仕事用プロファイルを持つ完全管理」として管理されているデバイスを、新しいセキュリティ強化された仕事用プロファイルエクスペリエンスに移行します。詳細については、「Android Enterprise の仕事用プロファイルを持つ完全管理の今後の変更点」を参照してください。

デバイス管理	ユースケース	仕事用プロファイル	個人用プロファイル	備考
会社所有デバイス (完全管理)	仕事でのみ使用することを目的とした会社所有デバイス	いいえ	はい。DPC は、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、デバイス全体のアクションを実行できます。	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み。
仕事用プロファイルで完全に管理	仕事と個人利用の両方を目的とした会社所有デバイス	はい	はい。これらのデバイスでは、DPC のコピーが 2 つ実行されます。1 つはデバイスオーナーモードでデバイスを管理し、もう 1 つはプロファイルオーナーモードで仕事用プロファイルを管理します。デバイスと仕事用プロファイルに個別のポリシーを適用できます。	以前は企業所有個人利用可能 (COPE) デバイスとして知られていました。
専用デバイス*	デジタルサイネージやチケット印刷など、単一のユースケース	いいえ	はい。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	以前は企業所有シングルユース (COSU) デバイスとして知

デバイス管理	ユースケース	仕事用プロファイル	個人用プロファイル	備考
	向けに構成された会社所有デバイス		きないようにします。	られていました。
BYODワークプロファイル **	ワークプロファイルモード (プロファイル所有者モードとも呼ばれる) に登録された個人デバイス	はい	はい。DPCはデバイス全体ではなく、ワークプロファイルのみを管理します。	これらのデバイスは新品である必要も、工場出荷時設定にリセットされている必要もありません。

* ユーザーは専用デバイスを共有できます。ユーザーが専用デバイス上のアプリにサインオンすると、その作業の状態はデバイスではなくアプリに紐付けられます。

** XenMobileは、BYODワークプロファイルモードでのZebraデバイスをサポートしていません。XenMobileは、完全に管理されたデバイスとして、またデバイスレガシーモード (デバイス管理者モードとも呼ばれる) でのZebraデバイスをサポートしています。

レガシー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については、「デバイス管理からAndroid Enterpriseへの移行」を参照してください。

認証方法

登録プロファイルは、Androidデバイスが MAM、MDM、またはMDM+MAMのいずれに登録されるかを決定し、ユーザーはMDMをオプトアウトするオプションを選択できます。

セキュリティレベルと必要な登録手順の指定については、「登録セキュリティモードの構成」を参照してください。

XenMobileは、MDM+MAMに登録されたAndroidデバイスに対して以下の認証方法をサポートしています。詳細については、「証明書と認証」の記事を参照してください。

- ドメイン
- ドメインと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とドメイン

- IDプロバイダー:
  - アジュール アクティブ ディレクトリ
  - Citrix Identityプロバイダー

ほとんど使用されない別の認証方法として、クライアント証明書とセキュリティトークンがあります。詳細については、`<https://support.citrix.com/article/CTX215200>`を参照してください。

要件

Android Enterpriseの使用を開始する前に、以下が必要です。

- アカウントと資格情報:
  - マネージドGoogle PlayでAndroid Enterpriseをセットアップするための企業Googleアカウント
  - 最新のMDXファイルをダウンロードするための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）のGoogle開発者アカウント
- XenMobile用に構成されたFirebase Cloud Messaging (FCM)。手順については、Firebase Cloud Messagingを参照してください。
- Samsung Knox Mobile Enrollment (オプション) の場合、Knox プレミアムライセンス。

XenMobile を Google Play に接続する

組織向けに Android Enterprise を設定するには、マネージド Google Play を介して Citrix を EMM プロバイダーとして登録します。この設定により、マネージド Google Play が XenMobile に接続され、XenMobile に Android Enterprise 用のエンタープライズが作成されます。

Google Play にサインインするには、企業の Google アカウントが必要です。

1. XenMobile コンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. **設定 > Android Enterprise** に移動します。

Android Enterprise が強調表示された設定ページ(/en-us/xenmobile/server/media/android-enterprise-setup1.png)

1. **接続**をクリックします。Google Play が開きます。

Android Enterprise が Google Play に接続します(/en-us/xenmobile/server/media/android-enterprise-setup-connect-1.png)

1. 企業の Google アカウントの資格情報を使用して Google Play にサインインします。組織名を入力し、Citrix が EMM プロバイダーであることを確認します。
2. Android Enterprise のエンタープライズ ID が追加されます。Android Enterprise を有効にするには、「**Android Enterprise を有効にする**」を「**はい**」にスライドします。

   Android Enterprise を有効にするオプション(/en-us/xenmobile/server/media/android-enterprise-setup-enable.png)

エンタープライズ ID が XenMobile コンソールに表示されます。

画像(/en-us/xenmobile/server/media/android-enterprise-id.png)

環境が Google に接続され、デバイスを管理する準備ができました。これでユーザーにアプリを提供できます。

XenMobile は、Citrix モバイル生産性向上アプリ、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 リンクをユーザーに提供するために使用できます。これらのアプリの種類とユーザーへの提供方法の詳細については、「アプリの追加」を参照してください。

次のセクションでは、モバイル生産性向上アプリを提供する方法について説明します。

Android Enterprise ユーザーに Citrix モバイル生産性向上アプリを提供する

Android Enterprise ユーザーに Citrix モバイル生産性向上アプリを提供するには、次の手順が必要です。

1. アプリを MDX アプリとして公開します。「MDX アプリとしてアプリを構成する」を参照してください。
2. ユーザーがデバイス上のワーク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チャレンジのルールを構成します。「セキュリティチャレンジポリシーを構成する」を参照してください。

公開したアプリは、Android Enterprise に登録されているデバイスで利用できます。

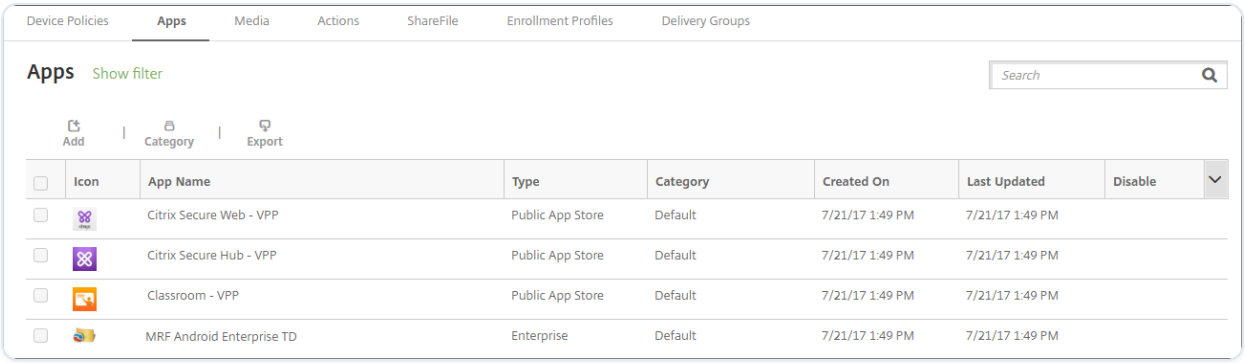
> **注：**

> Android Enterprise のパブリックアプリストアアプリを Android ユーザーに展開すると、そのユーザーは自動的に Android Enterprise に登録されます。

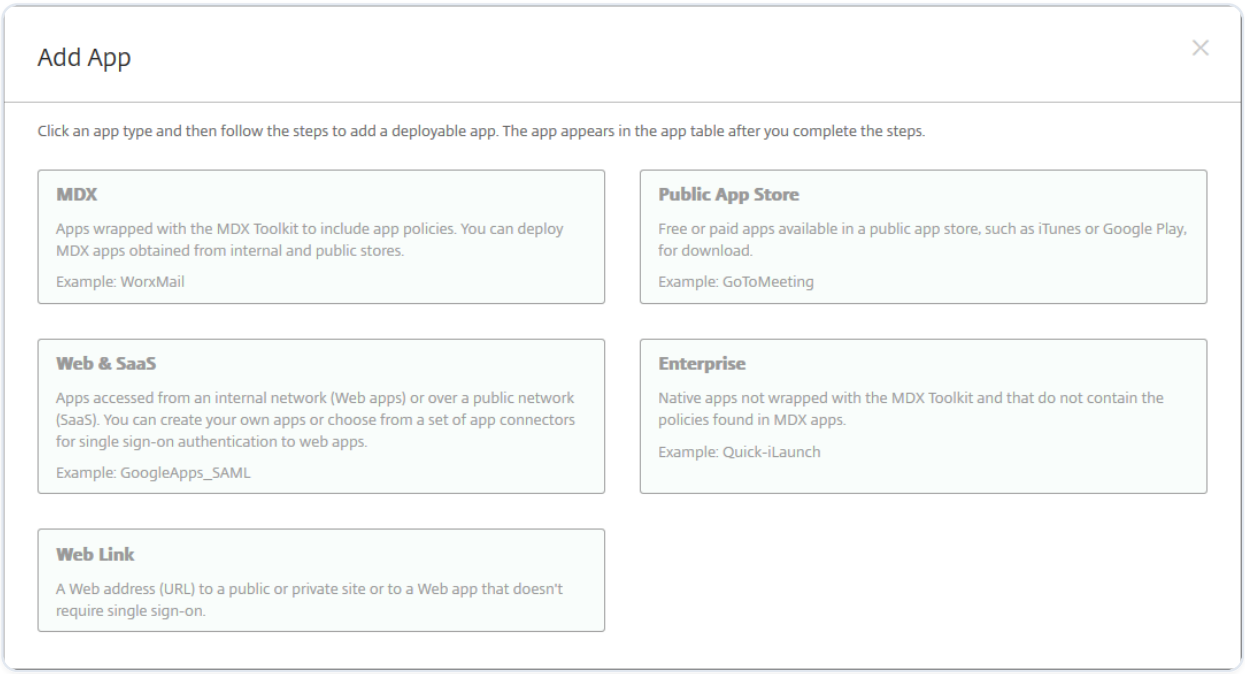
アプリを MDX アプリとして構成する

Citrix 生産性向上アプリを Android Enterprise 用の MDX アプリとして構成するには：

1. XenMobile コンソールで、 > をクリックします。 ページが表示されます。



2. をクリックします。 ダイアログボックスが表示されます。

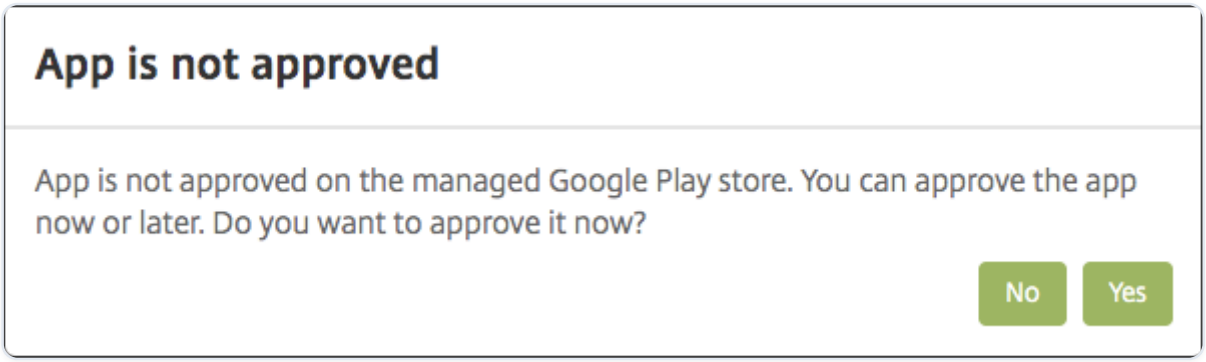


3. 「**MDX**」をクリックします。「**アプリ情報**」ページが表示されます。
4. ページの左側で、プラットフォームとして「**Android Enterprise**」を選択します。
5. 「**アプリ情報**」ページで、次の情報を入力します。

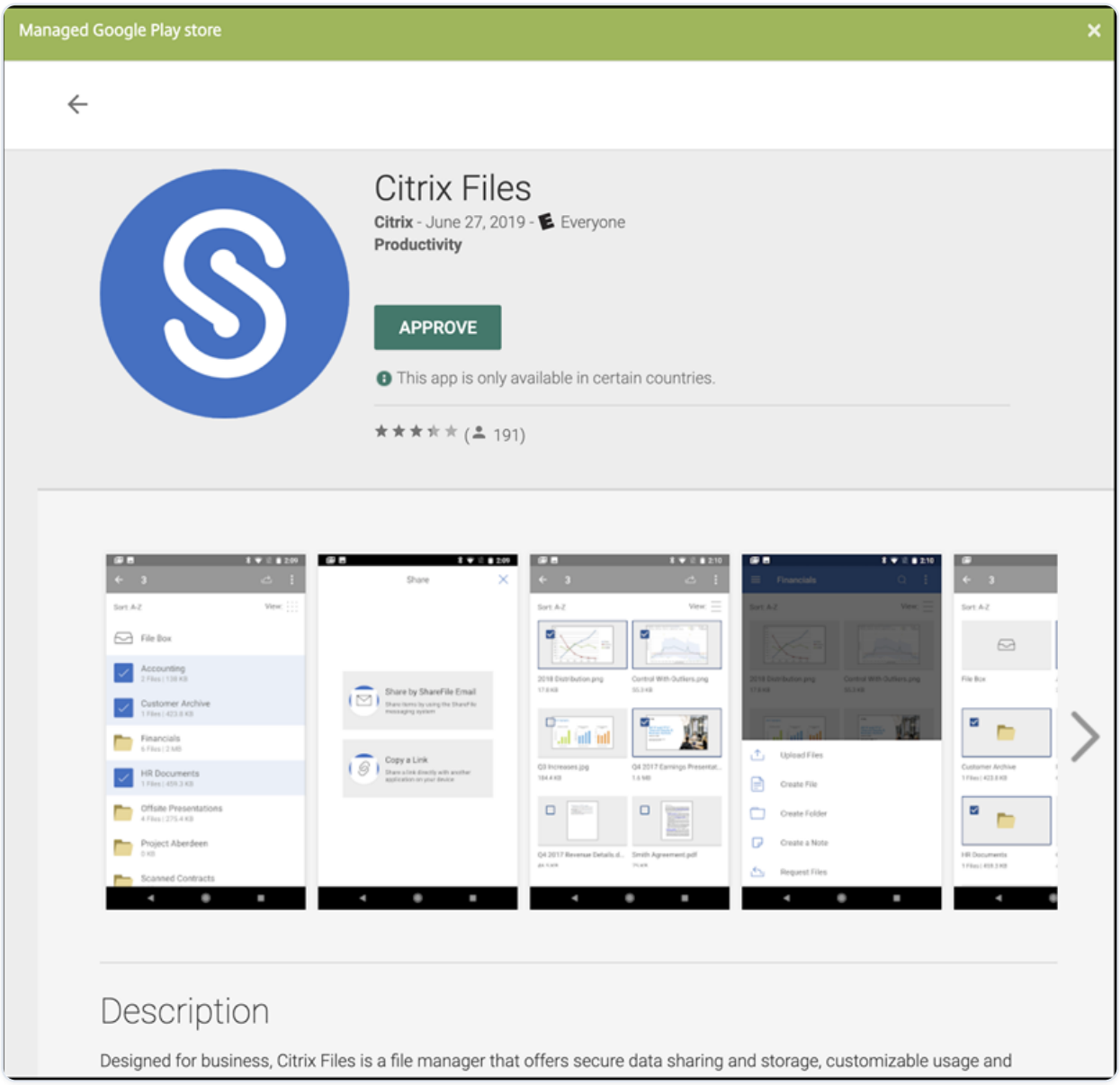
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、「**アプリ**」テーブルの「**アプリ名**」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。

- **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

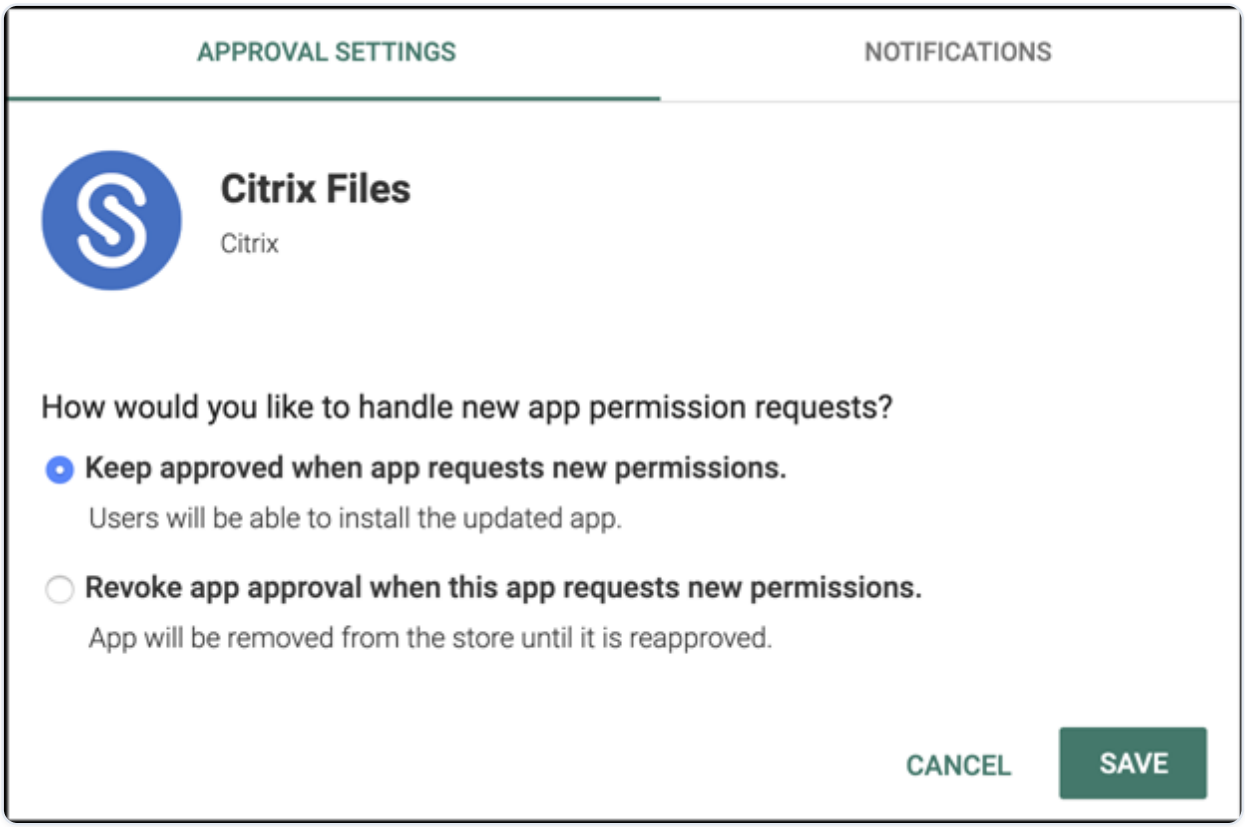
6. 「**次へ**」をクリックします。「**Android Enterprise MDXアプリ**」ページが表示されます。
7. 「**アップロード**」をクリックし、アプリの.mdxファイルの場所を参照します。ファイルを選択して「**開く**」をクリックします。
8. 添付されたアプリケーションが管理対象Google Playストアからの承認を必要とする場合、UIが通知します。XenMobileコンソールを離れることなくアプリケーションを承認するには、「**はい**」をクリックします。



9. 管理対象Google Playストアページが開いたら、「**承認**」をクリックします。



10. もう一度「**承認**」をクリックします。
11. 「**アプリが新しい権限を要求した場合でも承認を維持する**」を選択します。「**保存**」をクリックします。

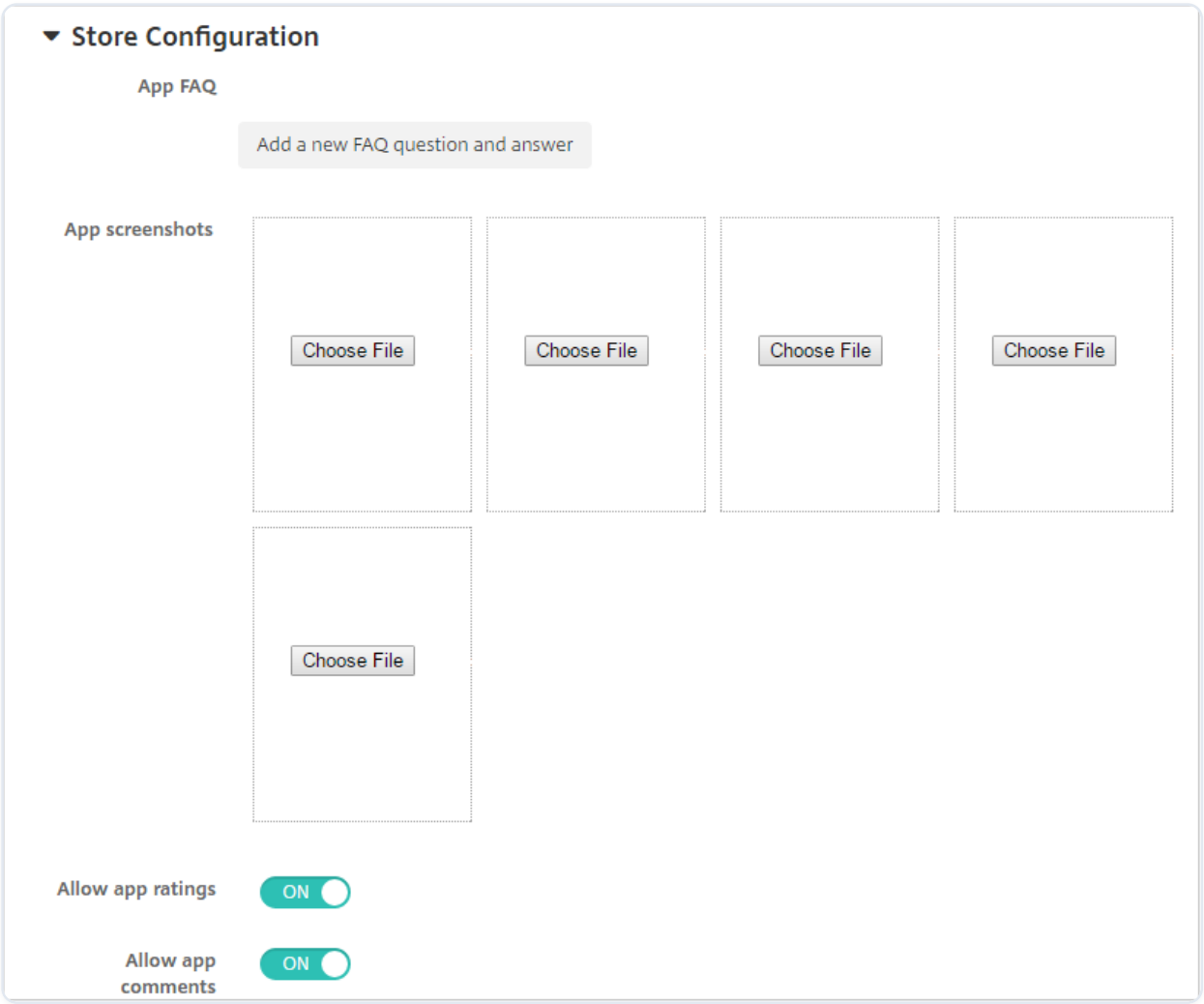


12. アプリが承認され保存されると、ページにさらに設定が表示されます。これらの設定を構成します。

    - **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。
    - **製品トラック:** ユーザーデバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトはProductionです。
    - **アプリのバージョン:** 必要に応じて、アプリのバージョン番号を入力します。
    - **パッケージID:** Google PlayストアにあるアプリのURL。
    - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
    - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
    - **除外されたデバイス:** 必要に応じて、アプリを実行できないデバイスのメーカーまたはモデルを入力します。

13. **MDXポリシー**を構成します。MDXアプリのアプリポリシーの詳細については、「MDXポリシーの概要」および「MAM SDKの概要」を参照してください。
14. 展開ルールを構成します。詳細については、「リソースの展開」を参照してください。

15. **ストア構成**を展開します。この設定は、管理対象のGoogle Playにのみ表示されるAndroid Enterpriseアプリには適用されません。



必要に応じて、アプリのFAQやアプリストアに表示されるスクリーンショットを追加できます。また、ユーザーがアプリを評価したりコメントしたりできるかどうかを設定することもできます。

- これらの設定を構成します。
  - **アプリのFAQ:** アプリのFAQの質問と回答を追加します。
  - **アプリのスクリーンショット:** アプリストアでアプリを分類するのに役立つスクリーン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またはJPEG画像はアップロードできません。
  - **アプリの評価を許可:** ユーザーがアプリを評価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**ON**です。 **アプリのコメントを許可:** ユーザーが選択したアプリについてコメント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**ON**です。

16. **次へ**をクリックします。**承認**ページが表示されます。

アプリ構成画面(/en-us/xenmobile/server/media/configure-apps-approvals-workflow.png)

ユーザーアカウントを作成する際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しない場合は、手順15に進むことができます。

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:** リストで既存のワークフローをクリックするか、**新しいワークフローを作成**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を作成**を選択した場合は、これらの設定を構成します。詳細については、「ワークフローの適用」を参照してください。
- **名前:** ワークフローの一意の名前を入力します。
- **説明:** 必要に応じて、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:** リストで、割り当てる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側にある目のアイコンをクリックすると、テンプレートをプレビューできるダイアログボックスが表示されます。
- **マネージャー承認レベル:** リストで、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは1レベルです。可能なオプションは次のとおりです。
    - 不要
    - 1レベル
    - 2レベル
    - 3レベル
- **Active Directoryドメインの選択:** リストから、ワークフローに使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を見つける:** 検索フィールドに追加の必須承認者の名前を入力し、「**検索**」をクリックします。名前はActive Directoryから取得されます。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスをオンにします。名前とメールアドレスは、「**選択された追加の必須承認者**」リストに表示されます。
    - 「**選択された追加の必須承認者**」リストからユーザーを削除するには、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リストを表示します。
        - 検索ボックスに氏名または部分的な名前を入力し、「**検索**」をクリックして検索結果を絞り込みます。

- 「**選択された追加の必須承認者**」リストのユーザーには、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除したい各名前の横にあるチェックボックスをオフにします。

17. 「**次へ**」をクリックします。「**デリバリーグループの割り当て**」ページが表示されます。

アプリ構成画面(/en-us/xenmobile/server/media/configure-apps-delivery-groups.png)

18. 「**デリバリーグループの選択**」の横で、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、「**アプリの割り当てを受け取るデリバリーグループ**」リストに表示されます。
19. 「**展開スケジュール**」を展開し、次の設定を構成します。

- 「**展開**」の横で、展開をスケジュールするには「**ON**」をクリックし、展開を防止するには「**OFF**」をクリックします。デフォルトのオプションは「**ON**」に設定されています。
- 展開スケジュールの横で、「**今すぐ**」または「**後で**」をクリックします。デフォルトのオプションは「**今すぐ**」に設定されています。
- 「**後で**」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、展開の日時を選択します。
- 「**展開条件**」の横で、「**すべての接続時**」をクリックするか、「**前回の展開が失敗した場合のみ**」をクリックします。デフォルトオプションは「**すべての接続時**」に設定されています。
- 「**常時接続の展開**」の横で、「**OFF**」が選択されていることを確認します。デフォルトオプションは「**OFF**」に設定されています。XenMobileをバージョン10.18.19以降で使い始めた場合、Android Enterpriseでは常時接続は利用できません。バージョン10.18.19より前にXenMobileを使い始めたお客様には、この接続は推奨されません。

  このオプションは、「**設定 > サーバープロパティ**」でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

  構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、「**常時接続の展開**」を除き、すべてのプラットフォームに適用されます。

20. 「**保存**」をクリックします。

各モバイル生産性向上アプリのMDXアプリを構成する手順を繰り返します。

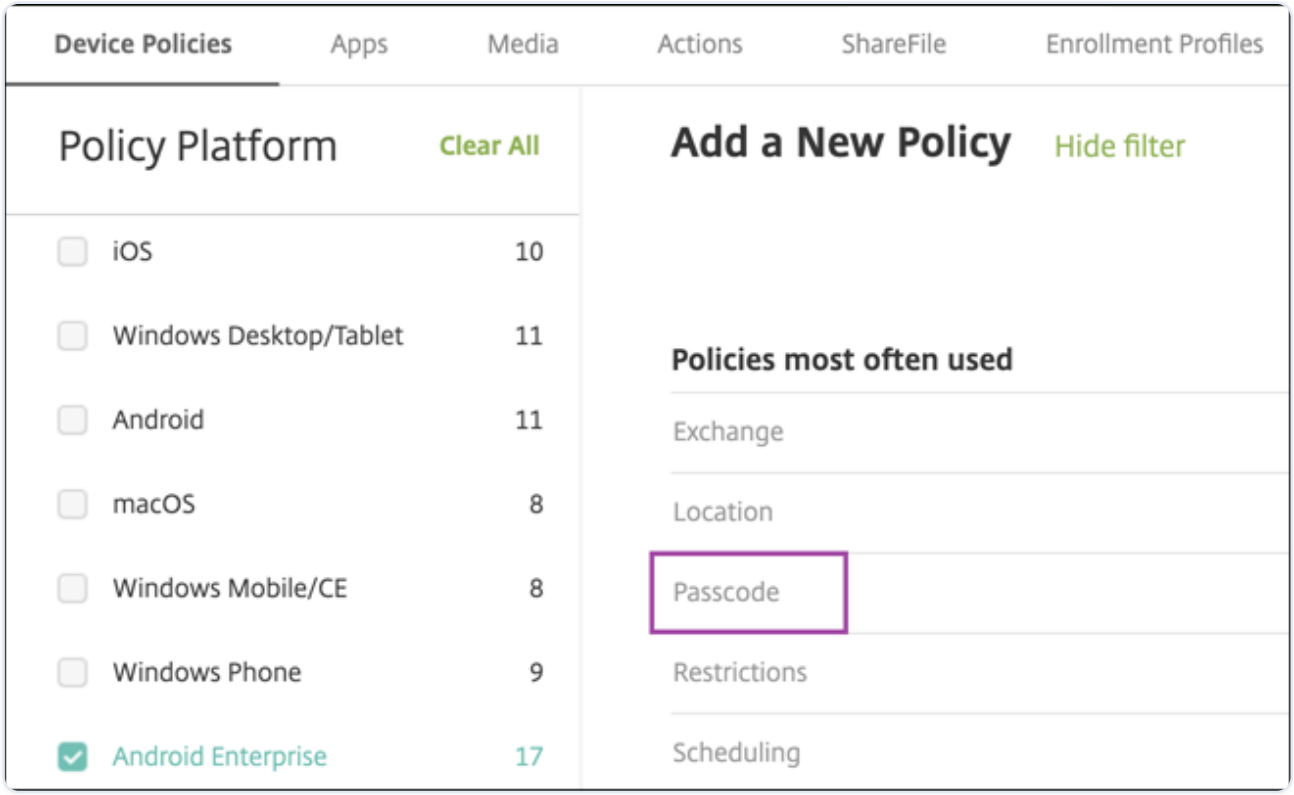
セキュリティチャレンジポリシーを構成する

XenMobileのパスコードデバイスポリシーは、ユーザーがデバイスまたはデバイス上のAndroid Enterpriseワークプロファイルにアクセスするためのセキュリティチャレンジのルールセットを構成します。セキュリティチャレンジには、パスコードまたは生体認証を使用できます。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。

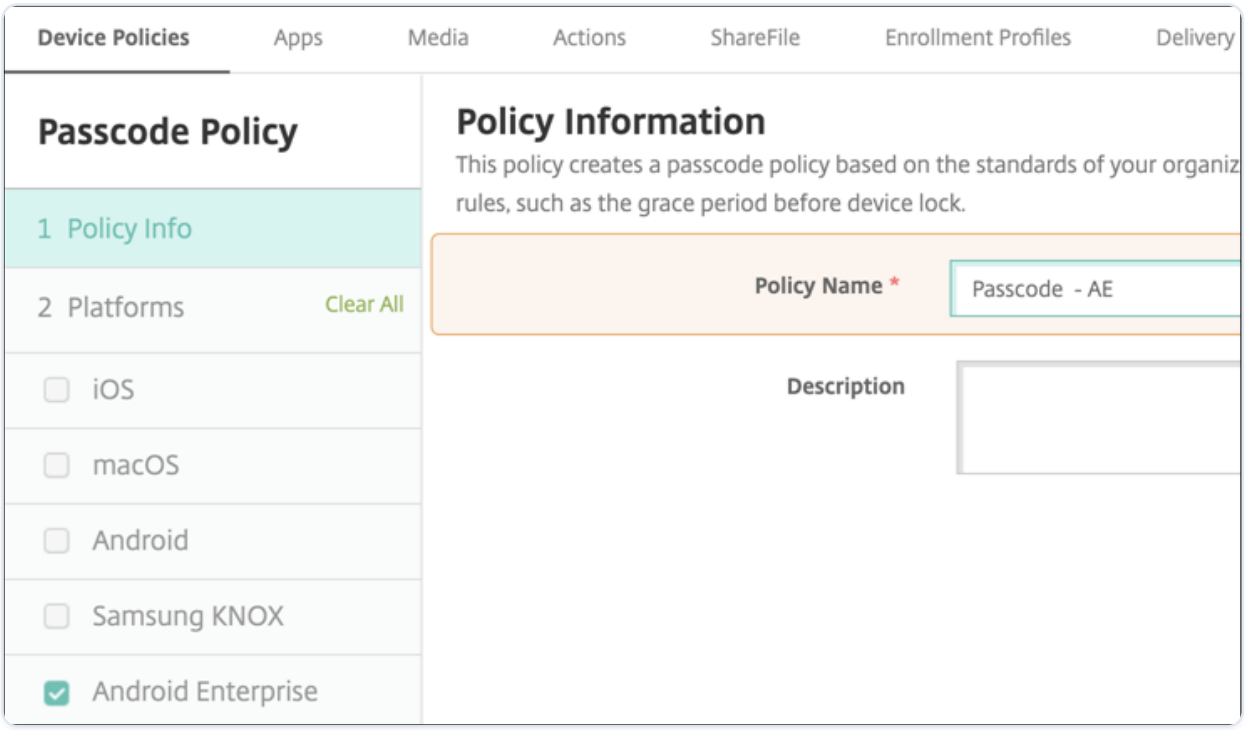
- Android Enterprise展開にBYODデバイスが含まれている場合は、ワークプロファイル用のパスコードポリシーを構成します。
- 展開に会社所有の完全に管理されたデバイスが含まれている場合は、デバイス自体のパスコードポリシーを構成します。
- 展開に両方の種類のデバイスが含まれている場合は、両方の種類のパスコードポリシーを構成します。

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. 「**フィルターの表示**」をクリックして「**ポリシープラットフォーム**」ペインを表示します。「**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. 右側のペインで「**パスコード**」をクリックします。



1. 「**ポリシー名**」を入力します。「**次へ**」をクリックします。



2. 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チャレンジで利用可能な設定を表示するには、「**デバイスのパスコードが必要**」を「**オン**」に設定します。
   - ワークプロファイルのセキュリティチャレンジで利用可能な設定を表示するには、「**ワークプロファイルのセキュリティチャレンジ**」を「**オン**」に設定します。
3. 「**次へ**」をクリックします。
4. 1つ以上のデリバリーグループにポリシーを割り当てます。
5. 「**保存**」をクリックします。

登録プロファイルの作成

登録プロファイルは、XenMobile展開でAndroid Enterpriseが有効になっている場合に、Androidデバイスがどのように登録されるかを制御します。Android Enterpriseデバイスを登録するための登録プロファイルを作成する際、新規デバイスおよび工場出荷時設定にリセットされたデバイスを次のように登録するように登録プロファイルを構成できます。

- 完全管理対象デバイス
- 専用デバイス（COSUデバイス）
- ワークプロファイルを持つ完全に管理されたデバイス (COPEデバイス)

これらの各Android Enterprise登録プロファイルを、BYOD Androidデバイスをワークプロファイルデバイスとして登録するように構成することもできます。

XenMobile展開でAndroid Enterpriseが有効になっている場合、新しく登録された、または再登録されたすべてのAndroidデバイスはAndroid Enterpriseデバイスとして登録されます。デフォルトでは、グローバル登録プロファイルは、新規および工場出荷時設定にリセットされたAndroidデバイスを完全に管理されたデバイスとして登録し、BYOD Androidデバイスをワークプロファイルデバイスとして登録します。

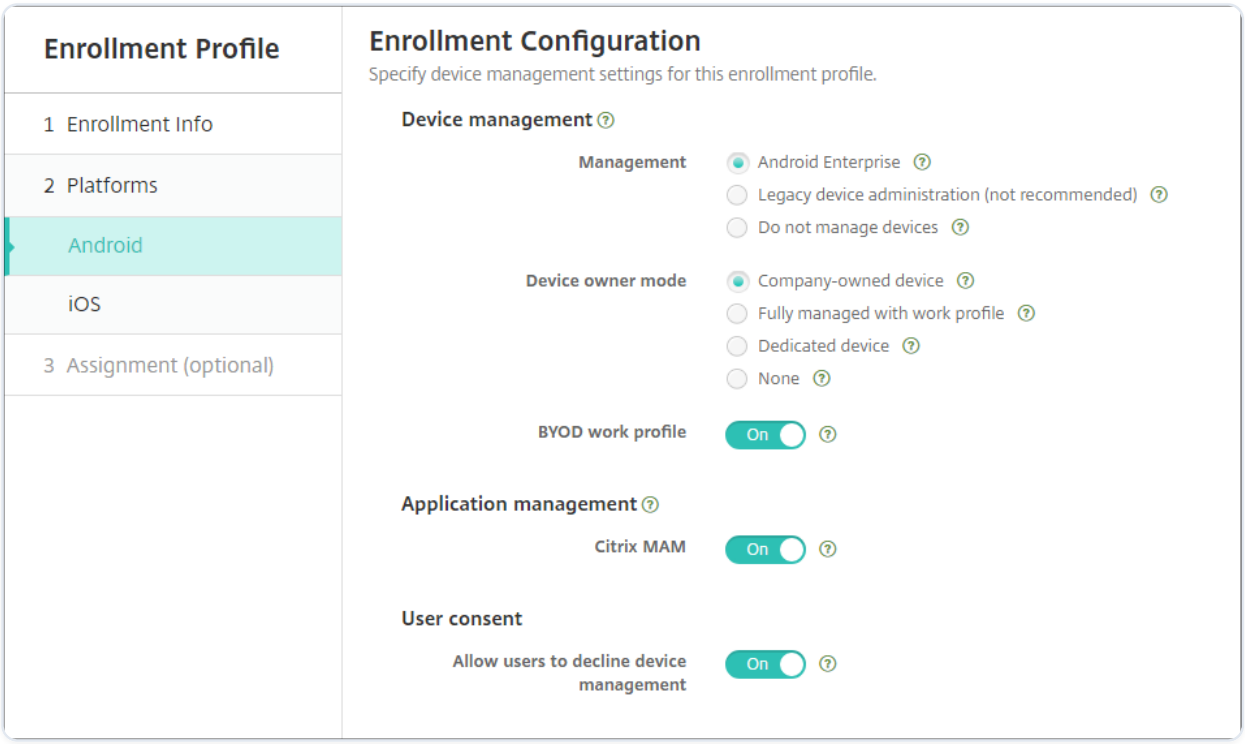
登録プロファイルを作成するときは、それらにデリバリーグループを割り当てます。ユーザーが異なる登録プロファイルを持つ複数のデリバリーグループに属している場合、使用される登録プロファイルはデリバリーグループの名前によって決定されます。XenMobileは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。詳細については、登録プロファイルを参照してください。

登録プロファイルを使用して、MDMのみ、MDM+MAM、MAMのみなど、複数のユースケースを組み合わせることができます。サーバープロパティ`xms.server.mode`に反映されるXenMobile Serverライセンスタイプによって、**構成 > 登録プロファイル**で利用可能な設定が決まります。

完全に管理されたデバイスの登録プロファイルを追加する

グローバル登録プロファイルはデフォルトで完全に管理されたデバイスを登録しますが、完全に管理されたデバイスを登録するための登録プロファイルをさらに作成できます。

1. XenMobileコンソールで、**構成 > 登録プロファイル**に移動します。
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。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。
4. **プラットフォーム**の下で**Android**を選択するか、**次へ**をクリックします。登録構成ページが表示されます。
5. **管理**を**Android Enterprise**に設定します。
6. **デバイス所有者モード**を**会社所有デバイス**に設定します。



7. **BYODワークプロファイル**を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するように登録プロファイルを構成できます。新規および工場出荷時設定にリセットされたデバイスは、完全に管理されたデバイスとして登録されます。

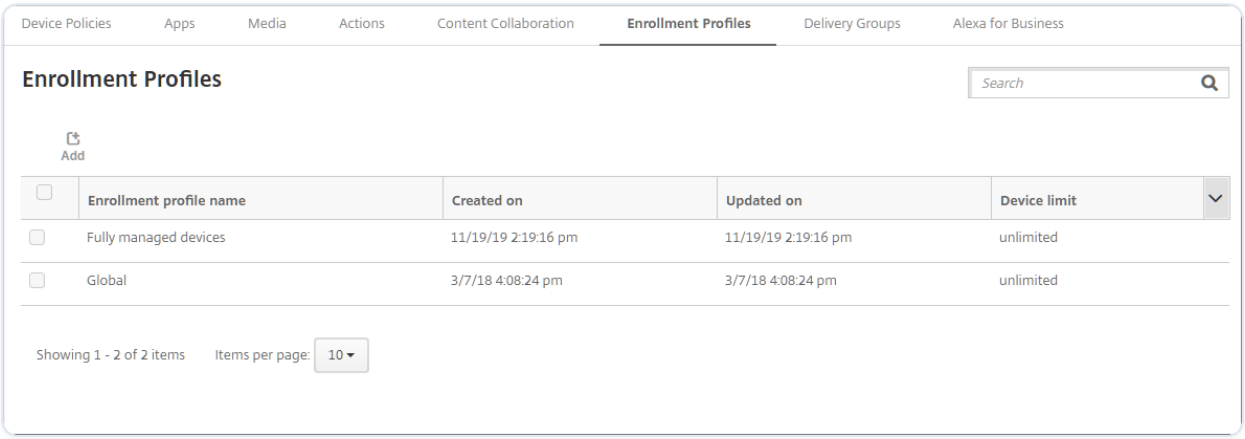
   - **BYODワークプロファイル**を**オン**に設定して、BYODデバイスをワークプロファイルデバイスとして登録できるようにします。デフォルトは**オン**です。
   - **BYODワークプロファイル**を**オフ**に設定して、登録を完全に管理されたデバイスに制限します。

8. Citrix MAMにデバイスを登録するかどうかを選択します。
9. **BYODワークプロファイル**を**オン**に設定した場合は、ユーザーの同意を設定します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、**ユーザーがデバイス管理を拒否することを許可する**を**オン**に設定します。

   BYODワークプロファイルが**オン**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**のデフォルト値は**オン**です。**BYODワークプロファイル**が**オフ**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可する**は無効になります。

10. **割り当て (オプション)** を選択します。デリバリーグループの割り当て画面が表示されます。
11. 完全に管理されたデバイスを登録する管理者が含まれている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。

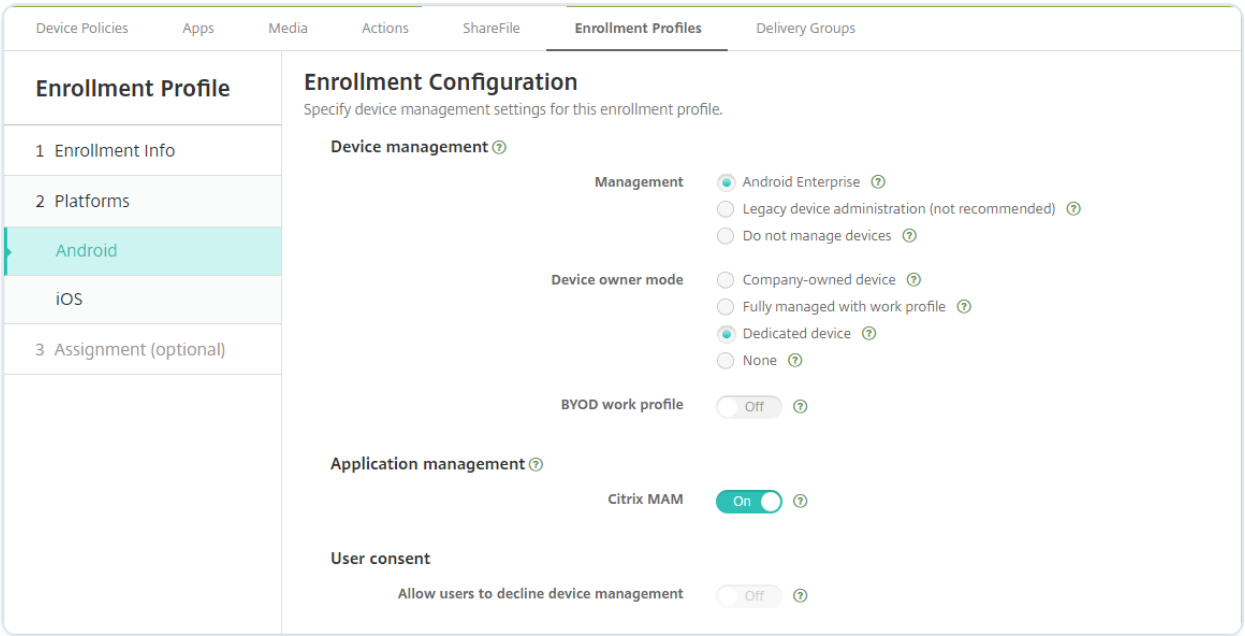
    追加したプロファイルとともに登録プロファイルページが表示されます。



専用デバイスの登録プロファイルを追加する

XenMobile展開に専用デバイスが含まれている場合、1人のXenMobile管理者または少数の管理者が多数の専用デバイスを登録します。これらの管理者がすべての必要なデバイスを登録できるようにするには、ユーザーあたりのデバイス数を無制限に許可する登録プロファイルを作成します。

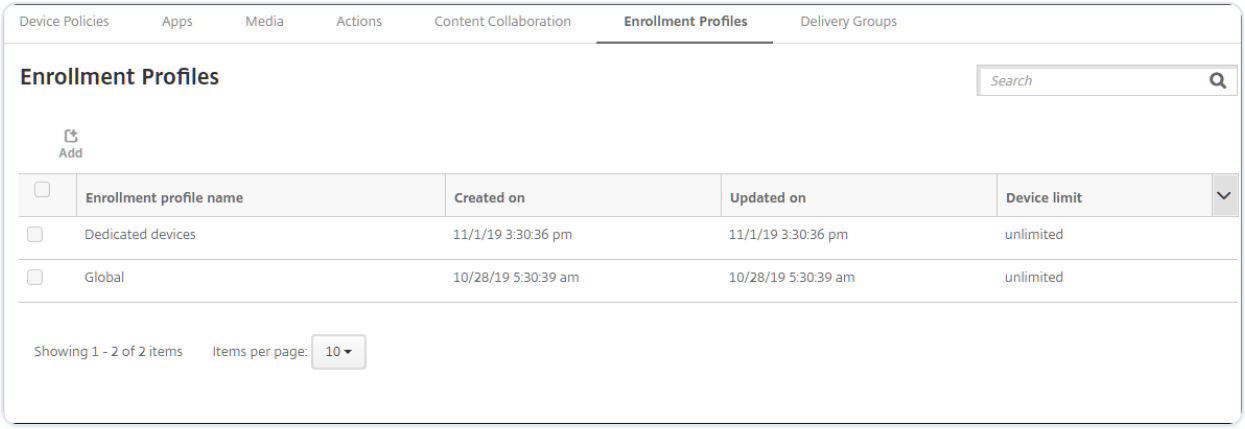
1. XenMobileコンソールで、**構成 > 登録プロファイル**の順に移動します。
2. 登録プロファイルを追加するには、**追加**をクリックします。登録情報ページで、登録プロファイルの名前を入力します。このプロファイルを持つメンバーが登録できるデバイスの数が無制限に設定されていることを確認してください。
3. **プラットフォーム**の下にある**Android**を選択するか、**次へ**をクリックします。登録構成ページが表示されます。
4. **管理**を**Android Enterprise**に設定します。
5. 「**デバイス所有者モード**」を「**専用デバイス**」に設定します。



6. 「**BYODワークプロファイル**」を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するための登録プロファイルを構成できます。新規デバイスおよび工場出荷時設定にリセットされたデバイスは、専用デバイスとして登録されます。BYODデバイスをワークプロファイルデバイスとして登録できるようにするには、**BYODワークプロファイル**を**オン**に設定します。登録を会社所有のデバイスに制限するには、**BYODワークプロファイル**を**オフ**に設定します。デフォルトは**オン**です。
7. Citrix MAMにデバイスを登録するかどうかを選択します。
8. 「**BYODワークプロファイル**」を「**オン**」に設定した場合、ユーザーの同意を構成します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、「**ユーザーがデバイス管理を拒否することを許可する**」を「**オン**」に設定します。

   「**BYODワークプロファイル**」が「**オン**」に設定されている場合、「**ユーザーがデバイス管理を拒否することを許可する**」のデフォルト値は「**オン**」です。「**BYODワークプロファイル**」が「**オフ**」に設定されている場合、「**ユーザーがデバイス管理を拒否することを許可する**」は無効になります。
9. 「**割り当て（オプション）**」を選択します。デリバリーグループ割り当て画面が表示されます。
10. 専用デバイスを登録する管理者が所属する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。

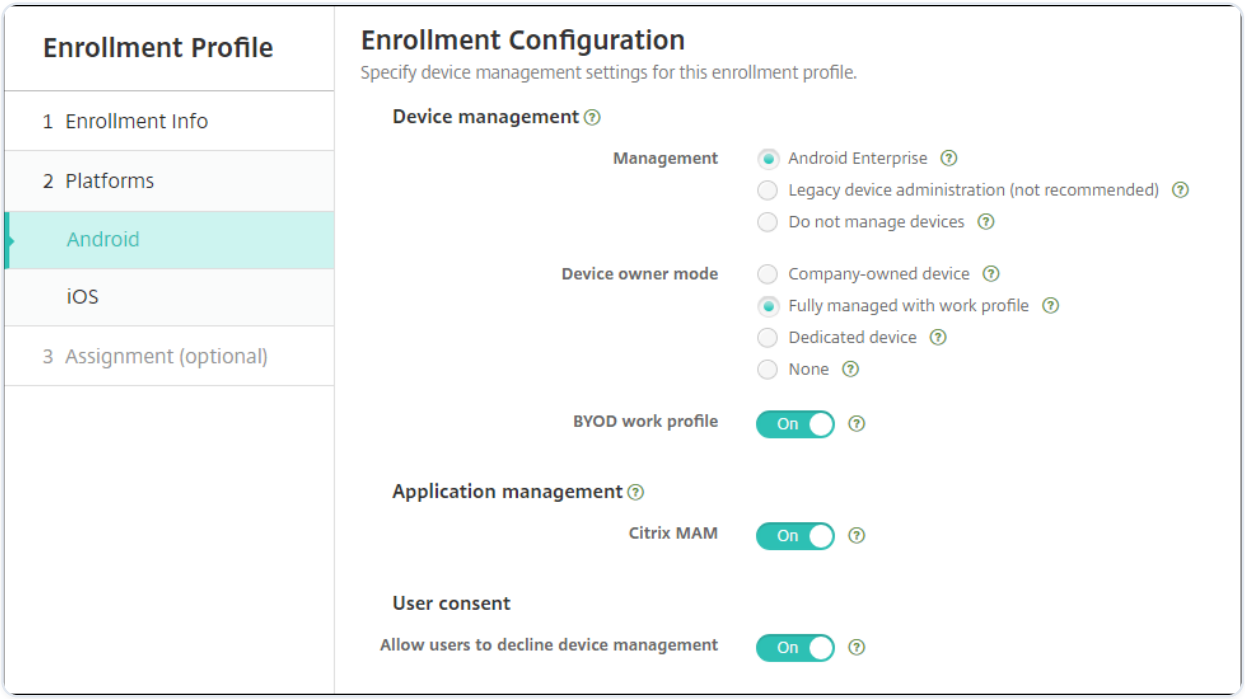
    追加したプロファイルとともに登録プロファイルページが表示されます。



ワークプロファイルを持つ完全に管理されたデバイスの登録プロファイルを追加する

1. XenMobileコンソールで、**構成 > 登録プロファイル**に移動します。
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。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。

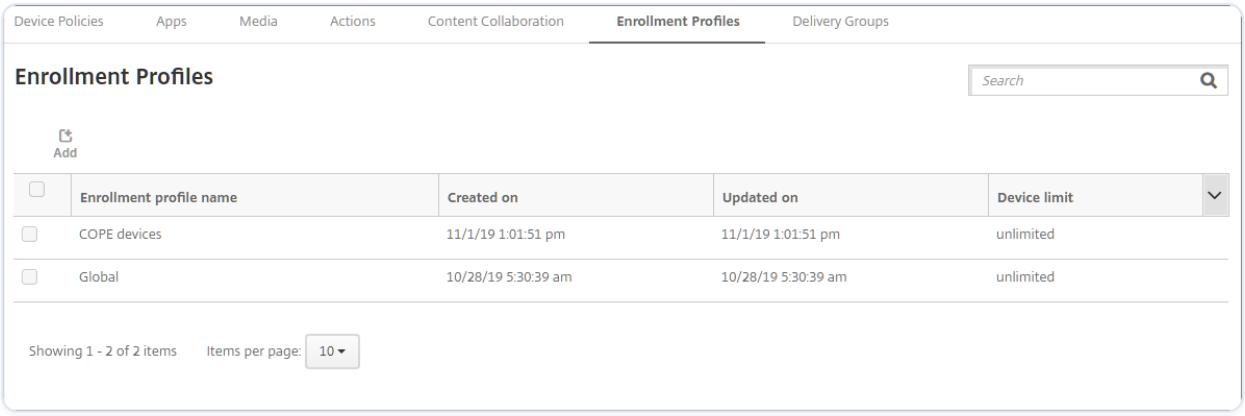
4. 「**プラットフォーム**」の下にある「**Android**」を選択するか、「**次へ**」をクリックします。登録構成ページが表示されます。
5. **管理**を**Android Enterprise**に設定します。**デバイス所有者モード**を**ワークプロファイルで完全に管理**に設定します。



6. **BYODワークプロファイル**を使用すると、BYODデバイスをワークプロファイルデバイスとして登録するように登録プロファイルを構成できます。新規デバイスおよび工場出荷時設定にリセットされたデバイスは、ワークプロファイルを持つ完全に管理されたデバイスとして登録されます。BYODデバイスをワークプロファイルデバイスとして登録できるようにするには、**BYODワークプロファイル**を**オン**に設定します。登録を専用デバイスに制限するには、**BYODワークプロファイル**を**オフ**に設定します。デフォルトは**オフ**です。
7. Citrix MAMにデバイスを登録するかどうかを選択します。
8. **BYODワークプロファイル**を**オン**に設定した場合、ユーザーの同意を構成します。BYODワークプロファイルデバイスのユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、**ユーザーがデバイス管理を拒否することを許可**を**オン**に設定します。

   BYODワークプロファイルが**オン**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可**のデフォルト値は**オン**です。**BYODワークプロファイル**が**オフ**に設定されている場合、**ユーザーがデバイス管理を拒否することを許可**は無効になります。
9. **割り当て（オプション）**を選択します。デリバリーグループ割り当て画面が表示されます。
10. ワークプロファイルを持つ完全に管理されたデバイスを登録する管理者が属する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。

追加したプロファイルを含む登録プロファイルページが表示されます。



レガシーデバイスの登録プロファイルの追加

Googleは、デバイス管理のデバイス管理者モードを非推奨にしています。Googleは、すべてのAndroidデバイスを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管理することを推奨しています。（Google Android Enterprise開発者ガイドのデバイス管理者モードの非推奨化を参照してください。）

この変更をサポートするために：

- Citrixは、Androidデバイスのデフォルトの登録オプションとしてAndroid Enterpriseを設定します。
- XenMobile展開でAndroid Enterpriseが有効になっている場合、新しく登録された、または再登録されたすべてのAndroidデバイスは、Android Enterpriseデバイスとして登録されます。

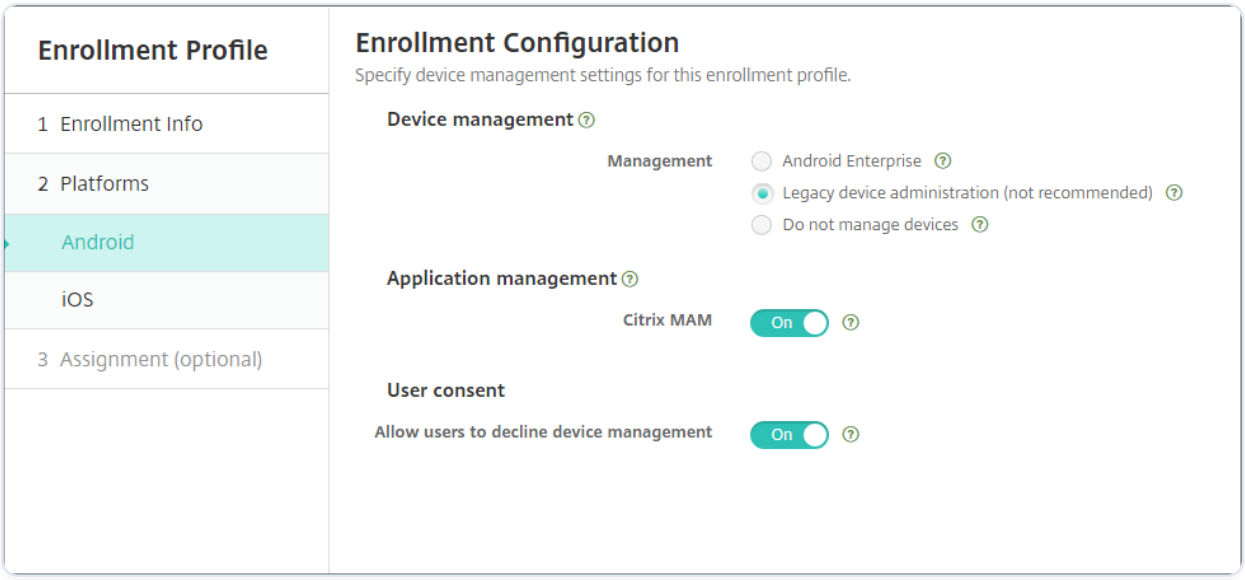
組織は、Android Enterprise を使用してレガシー Android デバイスの管理を開始する準備ができていない場合があります。その場合、デバイス管理者モードで管理を続行できます。すでにデバイス管理者モードで登録されているデバイスについては、XenMobile は引き続きデバイス管理者モードで管理します。

新しい Android デバイスの登録でデバイス管理者モードを使用できるように、レガシーデバイス用の登録プロファイルを作成します。

レガシーデバイス用の登録プロファイルを作成するには:

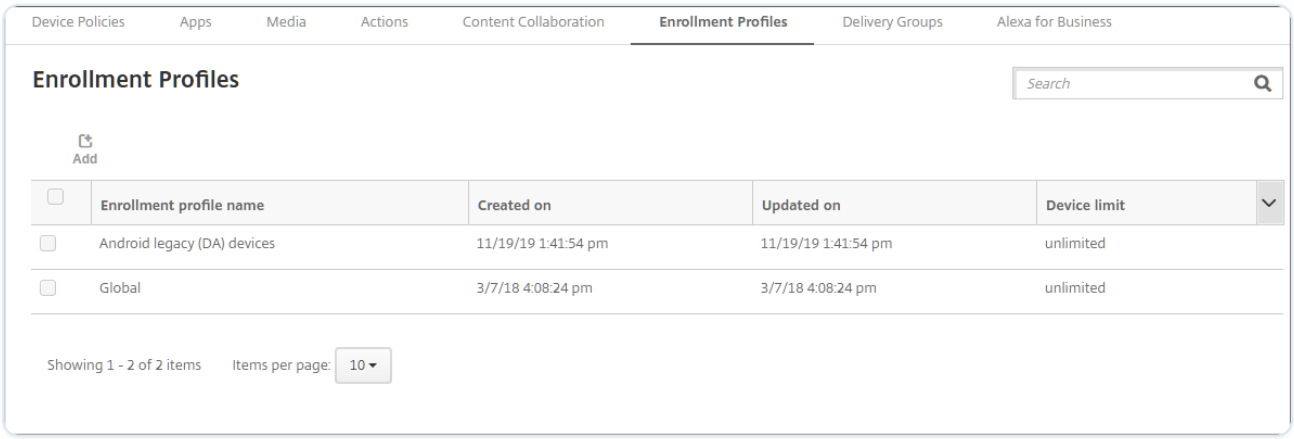
1. XenMobile コンソールで、 **>** の順に移動します。
2. 登録プロファイルを追加するには、 をクリックします。 ページで、登録プロファイルの名前を入力します。
3. このプロファイルを持つメンバーが登録できるデバイスの数を設定します。
4. で を選択するか、 をクリックします。 ページが表示されます。

5. を に設定します。 をクリックします。



6. Citrix MAM にデバイスを登録するかどうかを選択します。
7. ユーザーがデバイスを登録する際にデバイス管理を拒否できるようにするには、 を に設定します。デフォルトは です。
8. を選択します。 画面が表示されます。
9. 専用デバイスを登録する管理者が所属するデリバリーグループを選択します。次に、 をクリックします。

追加したプロファイルを含む ページが表示されます。



デバイス管理者モードでレガシーデバイスの管理を継続するには、このプロファイルを使用してデバイスを登録または再登録します。デバイス管理者デバイスの登録は、ユーザーにSecure Hubをダウンロードさせ、登録サーバーURLを提供することで、ワークプロファイルデバイスと同様に行います。

Android Enterpriseワークプロファイルデバイスのプロビジョニング

Android Enterpriseワーク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、新規または工場出荷時設定にリセットされている必要はありません。BYODデバイスはワークプロファイルデバイスとして登録されます。登録エクスペリエンスは、XenMobileでのAndroid登録に似ています。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。

デフォルトでは、Android Enterpriseにワークプロファイルデバイスとして登録されたデバイスでは、**USBデバッグと不明なソース**の設定が無効になります。

Android Enterpriseにワークプロファイルデバイスとしてデバイスを登録する場合は、常にGoogle Playにアクセスしてください。そこから、Secure Hubがユーザーの個人プロファイルに表示されるように有効にします。

Android Enterpriseの完全管理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、完全管理デバイスを登録できます。完全管理デバイスは会社所有のデバイスであり、デバイス所有者モードで登録されます。新規または工場出荷時設定にリセットされたデバイスのみがデバイス所有者モードで登録できます。

次のいずれかの登録方法を使用して、デバイスをデバイス所有者モードで登録できます。

- **DPC識別子トークン:** この登録方法では、ユーザーはデバイスのセットアップ時に `afw#xenmobile` の文字を入力します。 `afw#xenmobile` はCitrix DPC識別子トークンです。このトークンは、デバイスがXenMobileによって管理されていることを識別し、Google PlayストアからSecure Hubをダウンロードします。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。新規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、およびその他の通信モードは無効になっています。この状態では、NFCがデバイスが使用できる唯一の通信プロトコルです。NFCバンプを使用したデバイスの登録を参照してください。
- **QRコード:** QRコード登録は、NFCをサポートしないタブレットなどの分散型デバイス群を登録するために使用できます。QRコード登録方法では、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で、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コードを使用したデバイスの登録を参照してください。
- **ゼロタッチ:** ゼロタッチ登録を使用すると、デバイスの電源が初めてオンになったときに自動的に登録されるように構成できます。ゼロタッチ登録は、Android 9.0以降を実行している一部の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、Google Workspaceを使用している企業向けです。

Citrix DPC識別子トークンを使用したデバイスの登録

新規または工場出荷時設定にリセットされたデバイスの初期セットアップのために電源をオンにした後、Googleアカウントの入力を求められたときに、ユーザーは`afw#xenmobile`を入力します。この操作によりSecure Hubがダウンロードおよびインストールされます。その後、ユーザーはSecure Hubのセットアッププロンプトに従って登録を完了します。

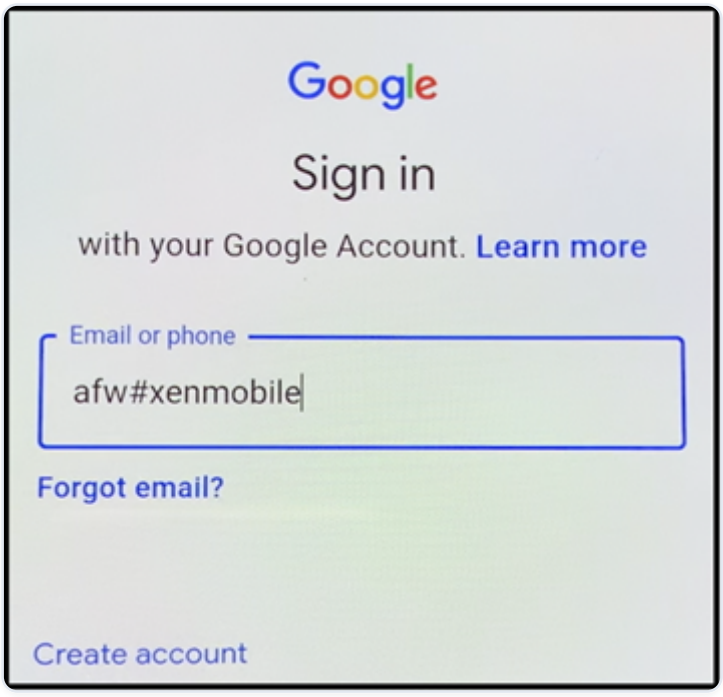
この登録方法は、Secure Hub の最新バージョンが Google Play ストアからダウンロードされるため、ほとんどのお客様に推奨されます。他の登録方法とは異なり、XenMobile Server から Secure Hub をダウンロード用に提供する必要はありません。

システム要件

- Android OS を実行しているすべての Android デバイスでサポートされています。

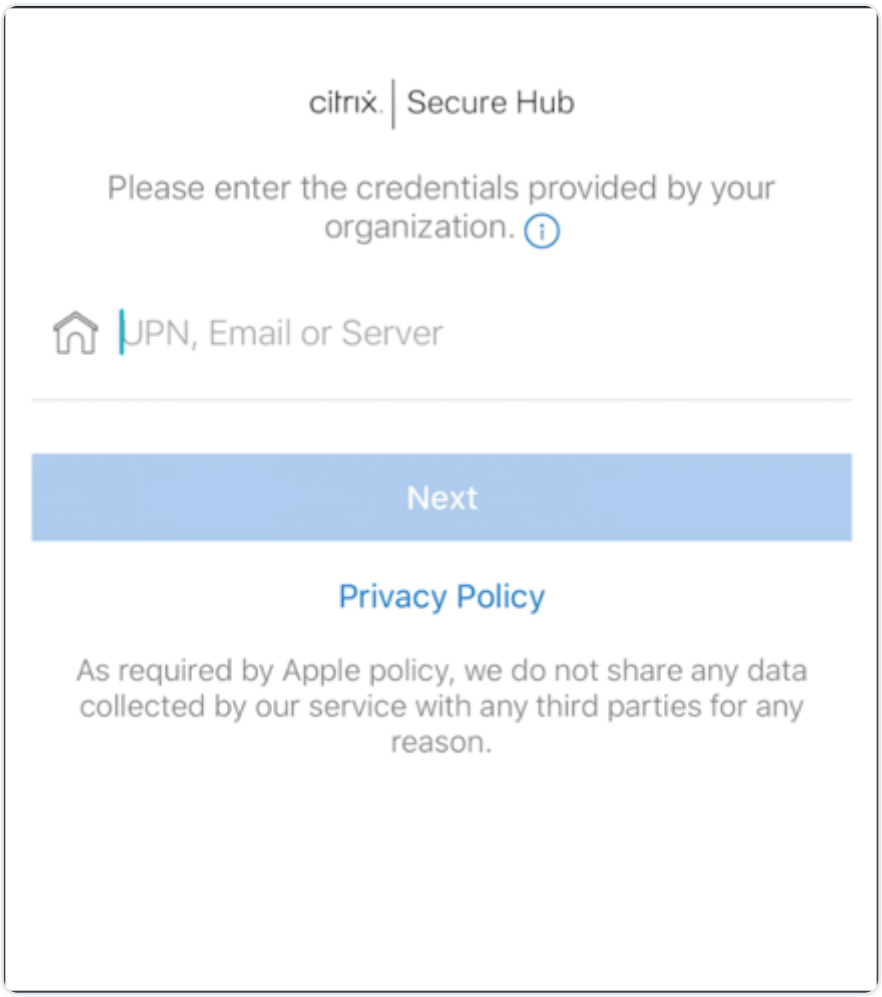
デバイスを登録するには

1. 新しいデバイスまたは工場出荷時設定にリセットされたデバイスの電源を入れます。
2. 初期デバイスセットアップがロードされ、Google アカウントの入力を求められます。デバイスのホーム画面がロードされた場合は、通知バーに「**セットアップを完了**」通知がないか確認します。
3. **メールアドレスまたは電話番号**フィールドに `afw#xenmobile` と入力します。



4. Secure Hub のインストールを促す 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. すべてのアプリのアクセス許可要求に対して、**許可**をタップします。
7. Secure Hub をインストールし、デバイスを管理することを許可するには、**同意して続行**をタップします。
8. Secure Hub がインストールされ、デフォルトの登録画面が表示されます。この例では、AutoDiscovery は設定されていません。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すると、サーバーが自動的に検出されます。代わりに、環境の登録 URL を入力し、**次へ**をタップします。



9. XenMobile のデフォルト設定では、ユーザーは MAM または MDM+MAM のどちら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場合は、**はい、登録**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求められます。**設定**をタップし、パスコードを入力します。
12. ユーザーはワーク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**をタップし、**PIN**をタップしてPINを入力します。

パスコードオプション(/en-us/xenmobile/server/media/passcode-options.png)

13. デバイスはSecure Hubの**マイアプリ**ランディング画面に表示されます。**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。

    Secure Hubストア(/en-us/xenmobile/server/media/secure-hub-store.png)
15. **追加**をタップします。
16. Secure Hubは、Secure Webをインストールするためにユーザーをを Google Playストアに誘導します。**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。画面共有またはリモートデバッグの開発者オプションもブロックされています。

    アカウントの変更(/en-us/xenmobile/server/media/account-modification-not-allowed.png)

NFCバンプによるデバイスの登録

NFCバンプを使用してデバイスを完全に管理されたデバイスとして登録するには、2つのデバイスが必要です。1つは工場出荷時の設定にリセットされたデバイス、もう1つはXenMobile Provisioning Toolを実行しているデバイスです。

システム要件と前提条件

- サポートされているAndroidデバイス。
- Android Enterpriseの完全管理デバイスとしてプロビジョニングされた、新品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ための手順は、この記事の後半で確認できます。
- NFC機能を備え、構成済みのプロビジョニングツールを実行している別のデバイス。プロビジョニングツールは、Secure HubまたはCitrixダウンロードページで入手できます。

各デバイスには、Secure Hubで管理されるAndroid Enterpriseプロファイルを1つだけ持つことができます。各デバイスで許可されるプロファイルは1つだけです。2つ目のDPCアプリを追加しようとすると、インストールされているSecure Hubが削除されます。

NFCバンプで転送されるデータ

工場出荷時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、Android Enterpriseを初期化するために、NFCバンプを介して次のデータを送信する必要があります。

- デバイス所有者として機能するDPCアプリのパッケージ名（この場合はSecure Hub）。
- 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/インターネットの場所。
- ダウンロードが成功したかどうかを確認するためのDPCアプリのSHA1ハッシュ。
- 工場出荷時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ためのWi-Fi接続の詳細。注：Androidは現在、この手順で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）。
- デバイスの地理的位置（オプション）。

2つのデバイスがバンプされると、プロビジョニングツールからのデータが工場出荷時設定にリセットされたデバイスに送信されます。そのデータは、管理者設定でSecure Hubをダウンロードするために使用されます。タイムゾーンと位置情報を入力しない場合、Androidは新しいデバイスで値を自動的に構成します。

XenMobileプロビジョニングツールの構成

NFCバンプを行う前に、プロビジョニングツールを構成する必要があります。この構成は、NFCバンプ中に工場出荷時設定にリセットされたデバイスに転送されます。

プロビジョニングツールの構成(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

必須フィールドにデータを入力するか、テキストファイルを使用して入力できます。次の手順では、テキストファイルの設定方法と各フィールドの説明について説明します。アプリは入力後に情報を保存しないため、将来の使用のために情報を保持するテキストファイルを作成することをお勧めします。

テキストファイルを使用してプロビジョニングツールを構成するには

ファイル名を nfcprovisioning.txt にし、そのファイルをデバイスのSDカードにある`/sdcard/`フォルダーに配置します。その後、アプリはテキストファイルを読み取り、値を入力できます。

テキストファイルには、次のデータが必要です。

```
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/インターネット上の場所です。NFCバンプ後に工場出荷時設定にリセットされたデバイスがWi-Fiに接続した後、デバイスはこの場所にアクセスしてダウンロードできる必要があります。URLは通常のURLであり、特別な書式設定は必要ありません。

```
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ことを確認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、この記事の後半で説明します。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

この行は、プロビジョニングツールが実行されているデバイスの接続済みWi-Fi SSIDです。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

サポートされている値はWEPと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2文字の小文字の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2文字の大文字のISO国コード（USなど）です。たとえば、米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ているタイムゾーン。Olson形式の地域/場所の名前を入力します。たとえば、太平洋時間の場合は「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、値がSecure Hubとしてアプリにハードコードされているため、必須ではありません。ここでは、完全を期す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がある場合、完成したnfcprovisioning.txtファイルは次のようになります。

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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がある場合、完成したnfcprovisioning.txtファイルは次のようになります。

`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=ga50TwdCmfdJ72LGRFkke4CrbAk\u`

`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`

Citrix Secure Hubのチェックサムを取得するには

Secure Hubのチェックサムは定数値です: `qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM`。Secure HubのAPKファイルをダウンロードするには、次のGoogle Playストアリンクを使用してください: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

アプリのチェックサムを取得するには

前提条件:

- Android SDK ビルドツール の **apksigner** ツール
- OpenSSLコマンドライン

任意のアプリのチェックサムを取得するには、次の手順に従います。

1. アプリのAPKファイルをGoogle Playストアからダウンロードします。
2. OpenSSLコマンドラインで、**apksigner**ツールに移動し: `android-sdk/build-tools/<version>/apksigner`、次のように入力します。

```
apksigner verify -print-certs <apk_path> | perl -nle 'print $& if m{(?<=SHA-256 digest:) .*}'  | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
```

コマンドは有効なチェックサムを返します。

3. QRコードを生成するには、`PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`フィールドにチェックサムを入力します。例:

```
{

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.zenprise/com.zenprise.configuration.AdminFunction",


"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"qn7oZUth
eu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",

  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://play.google.com/managed/downloadManagingApp?
identifier=xenmobile",

  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {

      "serverURL": "https://supportablility.xm.cloud.com"

   }

}
```

使用されているライブラリ

プロビジョニングツールは、そのソースコードで以下のライブラリを使用しています:

- GoogleによるApacheライセンス2.0のもとでのv7 `appcompat`ライブラリ、デザインサポートライブラリ、およびv7パレットライブラリ

  詳細については、Support Library Features Guideを参照してください。

- Jake WhartonによるApacheライセンス2.0のもとでのButter Knife

QRコードを使用したデバイスの登録

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、そのJSONをQRコードに変換することでQRコードを生成します。デバイスのカメラはQRコードをスキャンしてデバイスを登録します。

システム要件

- Android 9.0以降を実行しているすべてのAndroidデバイスでサポートされています。

JSONからQRコードを作成する

以下のフィールドを使用してJSONを作成します。

これらのフィールドは必須です:

Key: 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2文字の小文字の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2文字の大文字のISO国コード (USなど) です。たとえば、米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:** デバイスが実行されているタイムゾーン。

  Olson形式の地域/場所名 を入力します。たとえば、太平洋時間の場合は America/Los_Angeles です。入力しない場合、タイムゾーンは自動的に設定されます。

- **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、POSIX時間、Unixタイムスタンプ）は、January 1, 1970（UTC/GMTの深夜）から経過した秒数です。この時間にはうるう秒は含まれません（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。プロファイル作成時に暗号化を強制するには **false** に設定します。

一般的なJSONは次のようになります:

```
{
  "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。そのJSON文字列を、https://www.qr-code-generator.com などのオンラインQRコードジェネレーターを使用してQRコードに変換します。

このQRコードは、初期化されたデバイスによってスキャンされ、デバイスを完全管理デバイスとして登録します。

デバイスを登録するには

新しいデバイスまたは初期化されたデバイスの電源を入れた後：

1. ようこそ画面で画面を6回タップし、QRコード登録フローを起動します。
2. プロンプトが表示されたら、Wi-Fiに接続します。QRコード（JSONにエンコードされています）内のSecure Hubのダウンロード場所は、このWi-Fiネットワーク経由でアクセス可能です。

   デバイスがWi-Fiに正常に接続すると、GoogleからQRコードリーダーをダウンロードし、カメラを起動します。
3. カメラをQRコードに向けてコードをスキャンします。

   Androidは、QRコード内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をインストールしてデバイス所有者として設定します。

詳細については、Android EMM開発者向けのこのGoogleガイドを参照してください: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`。

ゼロタッチ登録

ゼロタッチ登録を使用すると、デバイスが初めて電源オンになったときに、それ自体を完全管理デバイスとしてプロビジョニングするように設定できます。

デバイス販売店は、デバイスに構成を適用できるオンラインツールであるAndroidゼロタッチポータルでアカウントを作成します。Androidゼロタッチポータルを使用して、1つ以上のゼロタッチ登録構成を作成し、それらの構成をアカウントに割り当てられたデバイスに適用します。ユーザーがこれらのデバイスの電源を入れると、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、その自動登録プロセスが定義されます。

システム要件

- ゼロタッチ登録のサポートはAndroid 9.0から開始されます。

販売店からのデバイスとアカウント情報

- 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されます。Android Enterpriseゼロタッチパートナーのリストについては、Androidウェブ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ゼロタッチポータルアカウント。
- リセラーによって提供されたAndroid Enterpriseゼロタッチポータルアカウントのログイン情報。

ゼロタッチ構成を作成する

ゼロタッチ構成を作成する際は、構成の詳細を指定するためにカスタムJSONを含めます。

このJSONを使用して、指定したXenMobile Serverにデバイスを登録するように構成します。この例の「URL」をサーバーのURLに置き換えてください。

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

  {

        "serverURL":"URL",

   }

}
```

より多くのパラメーターを含むオプションの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サーバーにログオンするために使用するユーザー名およびパスワードを指定しています。

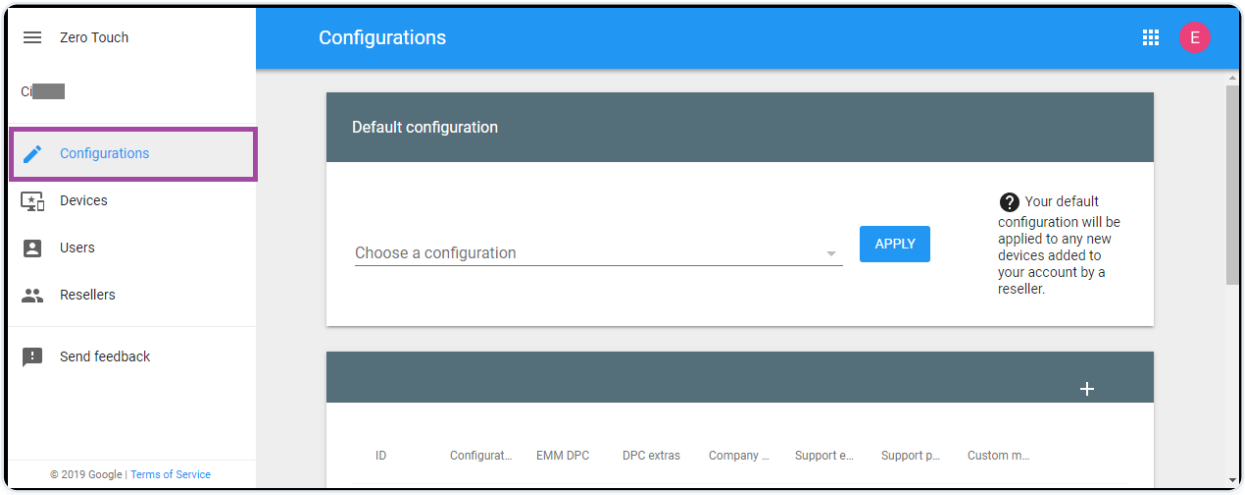
```
{

   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

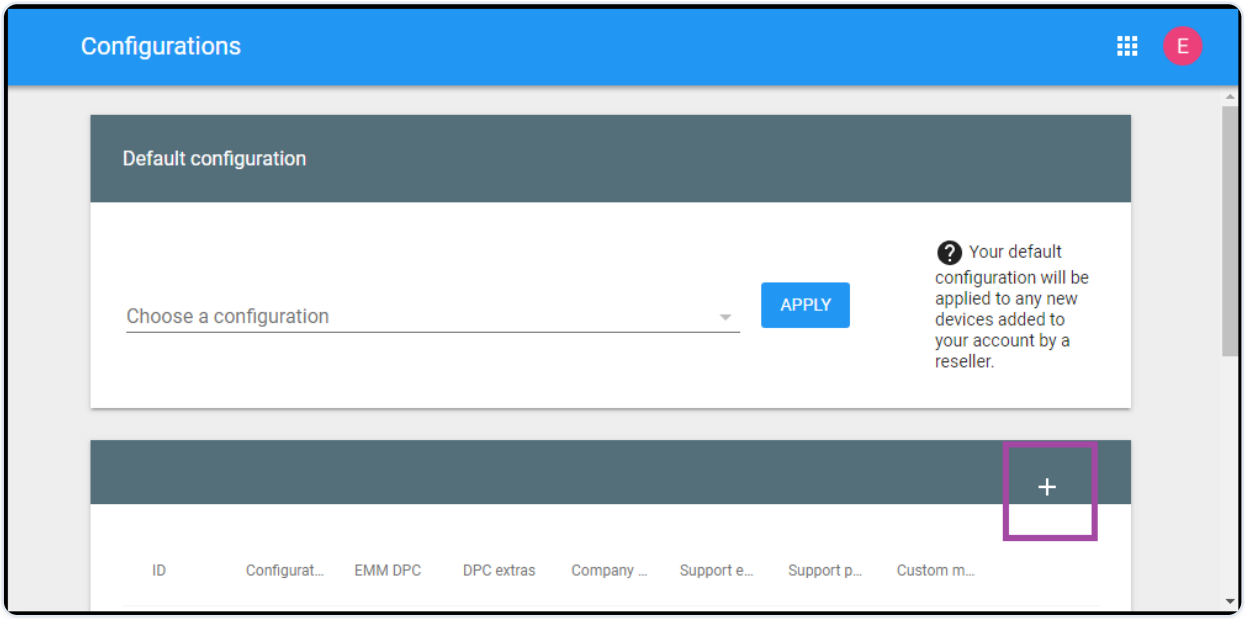
     {
```

```
        "serverURL":"URL",
        "xm_username":"username",
        "xm_password":"password"
    }
      }
```

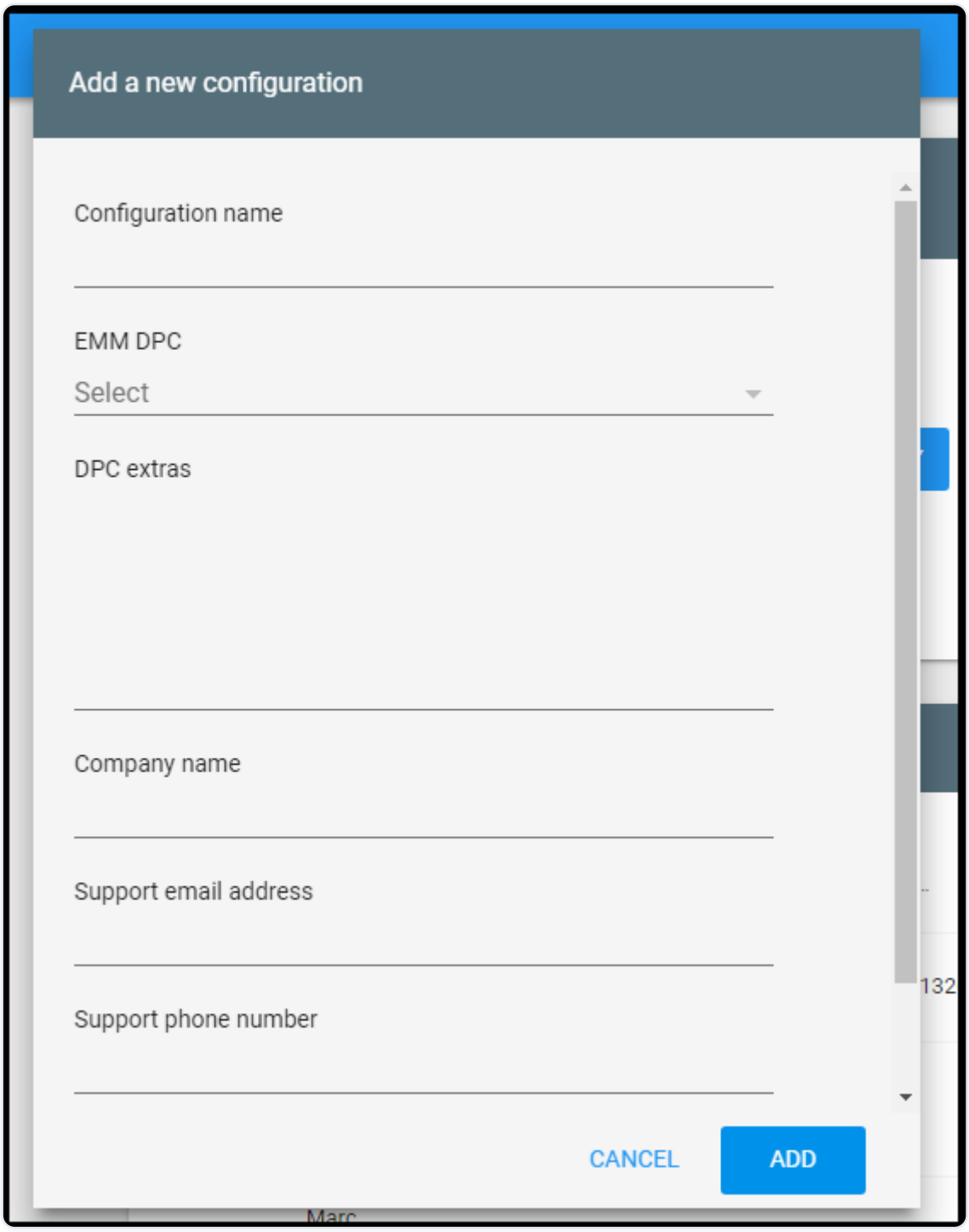
1. https://partner.android.com/zerotouchでAndroidゼロタッチポータルにアクセスします。ゼロタッチデバイスリセラーから提供されたアカウント情報でログインします。
2. **構成**をクリックします。



3. 構成テーブルの上にある**+**をクリックします。



4. 表示される構成ウィンドウに構成情報を入力します。



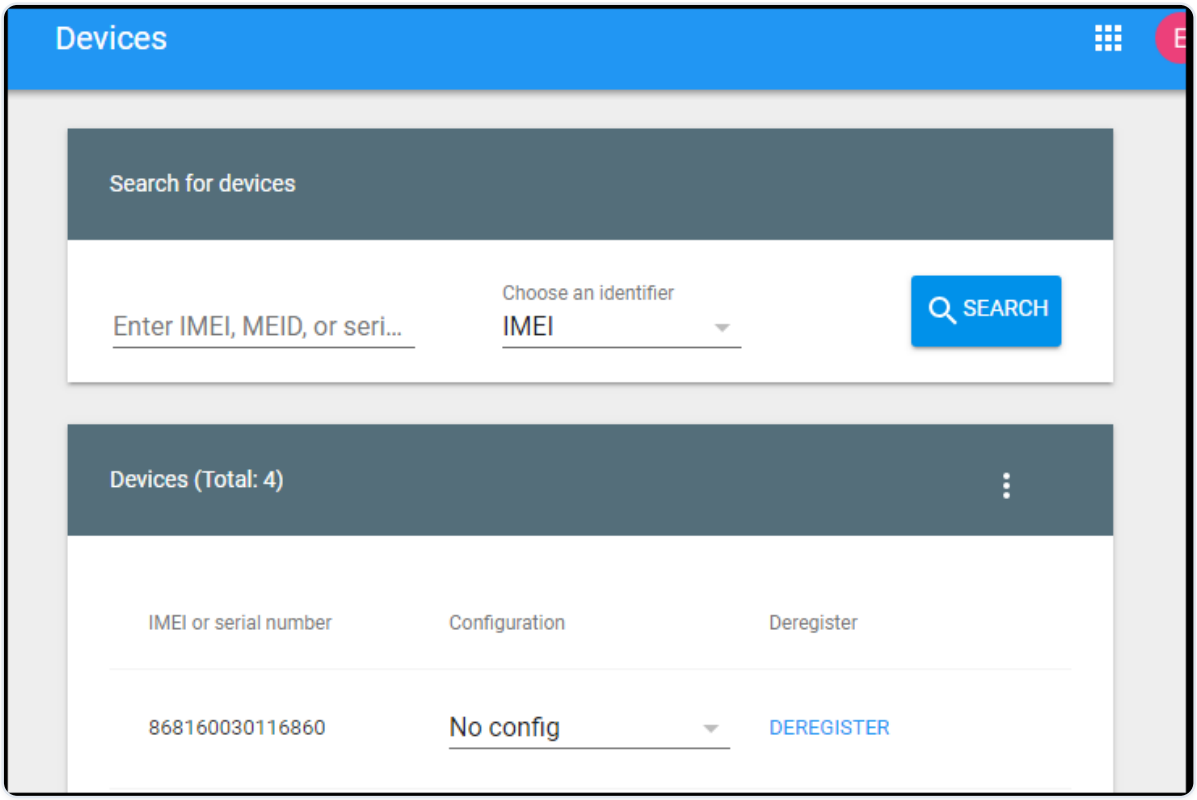
- **構成名:** この構成に選択した名前を入力します。
- **EMM DPC: Citrix Secure Hub** を選択します。
- **DPC追加情報:** このフィールドにカスタムJSONテキストを貼り付けます。
- **会社名:** デバイスプロビジョニング中にAndroid Enterpriseゼロタッチデバイスに表示する名前を入力します。

- **サポートメールアドレス:** ユーザーがヘルプを求める際に連絡でき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ゼロタッチデバイスに表示されます。
- **サポート電話番号:** ユーザーがヘルプを求める際に連絡でき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ゼロタッチデバイスに表示されます。
- **カスタムメッセージ:** 必要に応じて、ユーザーが連絡を取りやすくしたり、デバイスで何が起こっているかについて詳細を伝えたりするための1、2文を追加します。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から4を繰り返します。
7. デバイスに構成を適用するには：

   a. Androidゼロタッチポータルで、**デバイス**をクリックします。

   b. デバイスのリストからデバイスを見つけ、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、複数のデバイスに構成を適用できます。

複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「IT管理者向けのゼロタッチ登録」を参照してください。このAndroid Enterpriseヘルプトピックには、構成を管理し、デバイスに適用する方法に関する詳細情報が記載されています。

専用のAndroid Enterpriseデバイスのプロビジョニング

専用のAndroid Enterpriseデバイスは、単一のユースケースを満たすために特化した完全に管理されたデバイスです。専用デバイスは、企業所有単一用途（COSU）デバイスとも呼ばれます。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ために必要な1つのアプリまたは少数のアプリセットに制限されます。また、ユーザーが他のアプリを有効にしたり、デバイスで他の操作を行ったりすることを防ぎます。

Android Enterpriseの完全に管理されたデバイスのプロビジョニングで説明されているように、他の完全に管理されたデバイスに使用される登録方法のいずれかを使用して専用デバイスを登録します。専用デバイスのプロビジョニングには、登録前により多くのセットアップが必要です。

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、登録プロファイルを追加します。「登録プロファイルの作成」を参照してください。(#creating-enrollment-profiles).
- 専用デバイスがアクセスできるようにするアプリを許可します。
- オプションで、許可された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の場合、ユーザーがアプリを開くと、アプリはデバイス画面に固定されます。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、サインアウトなどのアプリにプログラムされたアクションを使用してアプリを終了します。
- 追加した登録プロファイルに各デバイスを登録します。

システム要件

- 専用デバイスの登録のサポートはAndroid 6.0から開始されます。

アプリを許可し、ロックタスクモードを設定する

キオスクデバイスポリシーを使用すると、アプリを許可し、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サービスが許可されています。

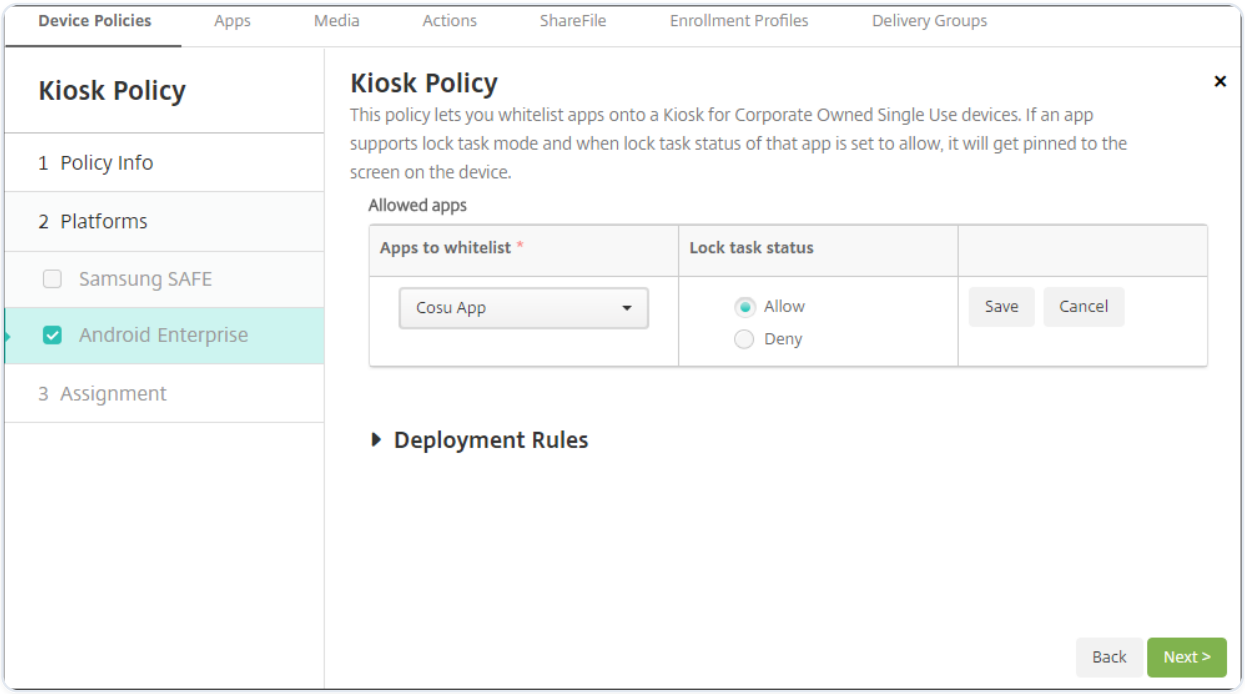
キオスクポリシーを追加するには：

1. XenMobileコンソールで、 **>** をクリックします。 ページが表示されます。
2. をクリックします。 ダイアログボックスが表示されます。

3. を展開し、 の下にある をクリックします。 ページが表示されます。
4. で、 を選択します。他のプラットフォームの選択を解除します。
5. ペインで、 とオプションの を入力します。
6. をクリックし、次に をクリックします。
7. アプリを許可し、そのアプリのロックタスクモードを許可または拒否するには:

   リストから許可するアプリを選択します。

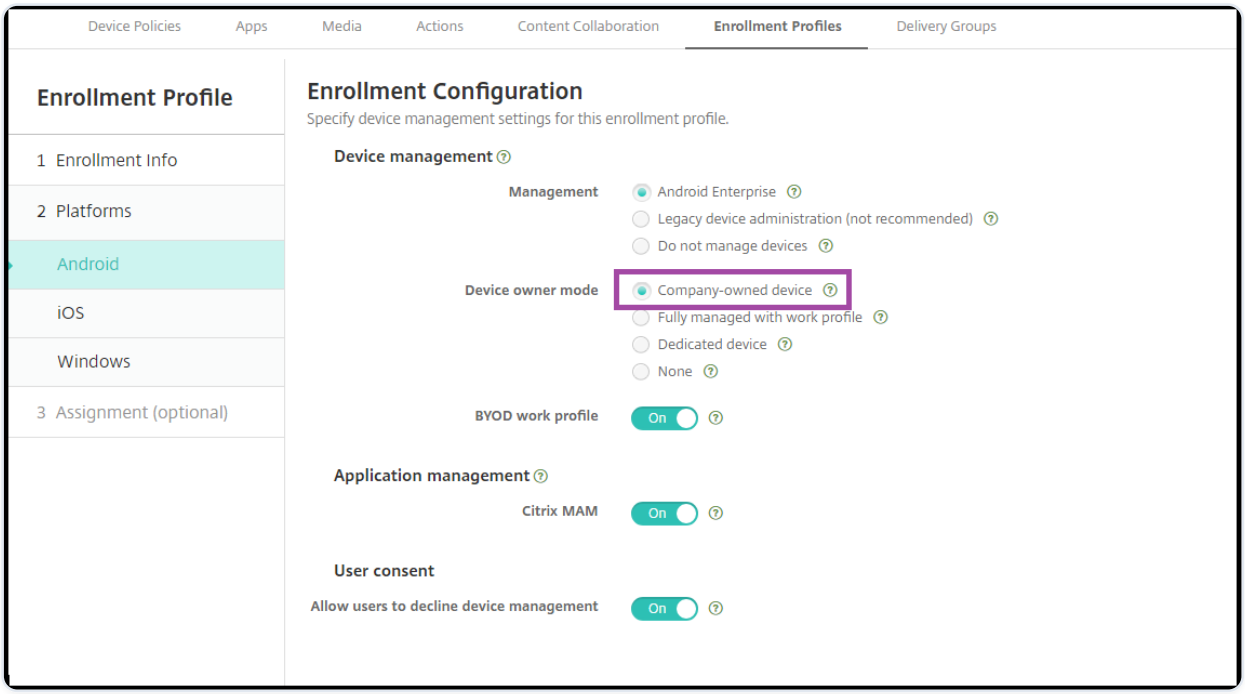
   ユーザーがアプリを起動したときに、アプリをデバイス画面に固定するように設定するには、**許可**を選択します。アプリを固定しないように設定するには、**拒否**を選択します。デフォルトは**許可**です。



8. **保存**をクリックします。
9. 別のアプリを許可し、そのアプリのロックタスクモードを許可または拒否するには、**追加**をクリックします。
10. 展開ルールを構成し、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. **次へ**をクリックするか、**プラットフォーム**の下にある**Android**を選択します。登録構成ページが表示されます。
2. **管理**を**Android Enterprise**に設定します。
3. **デバイス所有者モード**を**会社所有デバイス**に設定します。



4. **割り当て（オプション）**を選択します。デリバリーグループ割り当て画面が表示されます。
5. 専用デバイスを登録する管理者が所属する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。

登録プロファイルで**BYODワークプロファイル**を有効にした場合、新規または工場出荷時設定にリセットされていないデバイスは、ワークプロファイルデバイスとして登録されます。「Android Enterpriseワークプロファイルデバイスのプロビジョニング」を参照してください。

Android Enterpriseのワークプロファイル付き完全管理対象デバイス（COPEデバイス）をプロビジョニングする

ワークプロファイル付き完全管理対象デバイス（以前はCOPEデバイスと呼ばれていました）は、仕事と個人の両方の目的で使用される会社所有のデバイスです。組織はデバイス全体を管理します。デバイスには1つのポリシーセットを適用し、ワークプロファイルには別のポリシーセットを適用できます。

XenMobileコンソールでは、ワークプロファイル付き完全管理対象デバイスは次の用語で表示されます。

- デバイスの所有権は「Corporate」です。
- デバイスのAndroid Enterpriseインストールタイプは「Corporate Owner Personally Enabled」です。

システム要件

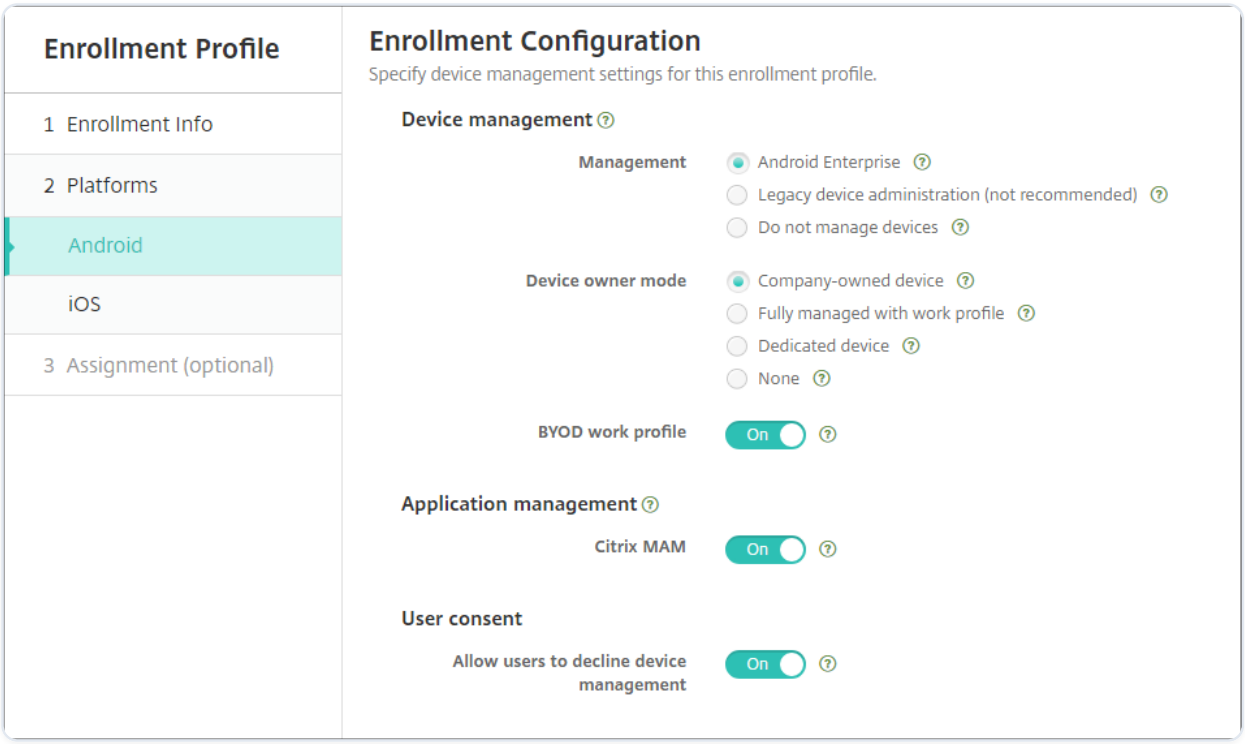
- ワークプロファイル付き完全管理対象デバイスの登録は、Android 9.0からAndroid 10.xまでサポートされています。

ワークプロファイル付き完全管理対象デバイスの登録プロファイルを追加する

ワークプロファイル付き完全管理対象デバイスを登録するための登録プロファイルを作成します。この登録プロファイルに割り当てられたデリバリーグループの管理者は、ワークプロファイル付き完全管理対象デバイスを登録できます。これらの管理者が必要なすべてのデバイスを登録できるように、ユーザーごとに許可されるデバイス数が無制限の登録プロファイルを作成します。このプロファイルを、ワークプロファイル付き完全管理対象デバイスを登録する管理者が含まれるデリバリーグループに割り当てます。

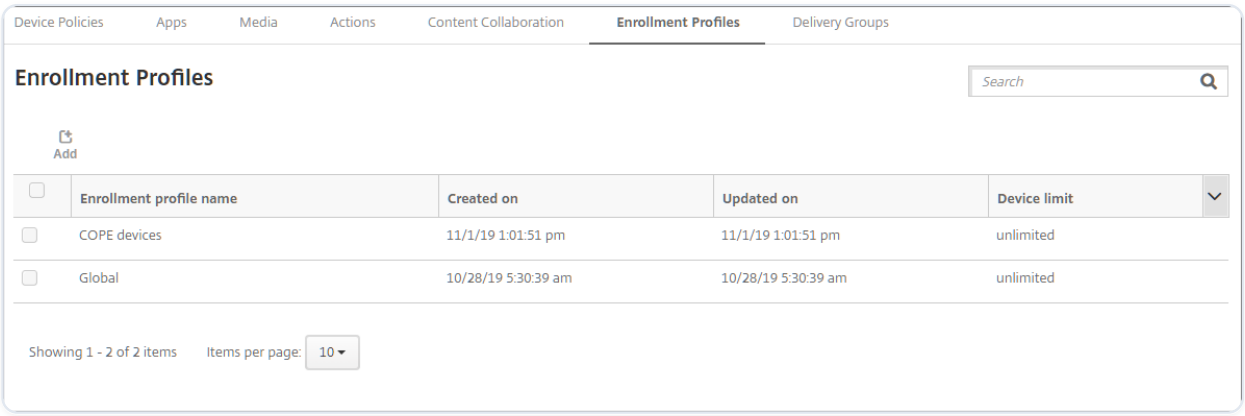
1. XenMobileコンソールで、**Configure > Enrollment Profiles**に移動します。
2. 登録プロファイルを追加するには、**Add**をクリックします。Enrollment Infoページで、登録プロファイルの名前を入力します。このプロファイルを持つメンバーが登録できるデバイスの数が無制限に設定されていることを確認します。
3. **Next**をクリックするか、**Platforms**の下にある**Android Enterprise**を選択します。Enrollment Configurationページが表示されます。
4. **Enrollment Type**を次のいずれかに設定します。

    - **Fully managed/Work profile:** 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は、完全管理対象として登録されます。BYODデバイスは、ユーザーが管理するワークプロファイルのみで登録されます。
    - **COPE/Work profile:** 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は、ワークプロファイル付き完全管理対象として登録されます。BYODデバイスは、ユーザーが管理するワークプロファイルのみで登録されます。



5. **割り当て (オプション)** を選択するか、**次へ** をクリックします。デリバリーグループの割り当て画面が表示されます。
6. 専用デバイスを登録する管理者が属する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。

   追加したプロファイルを含む登録プロファイルページが表示されます。



ユーザーが異なる登録プロファイルを持つ複数のデリバリーグループに属している場合、デリバリーグループの名前によって使用される登録プロファイルが決定されます。XenMobileは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。

デバイスを登録するには

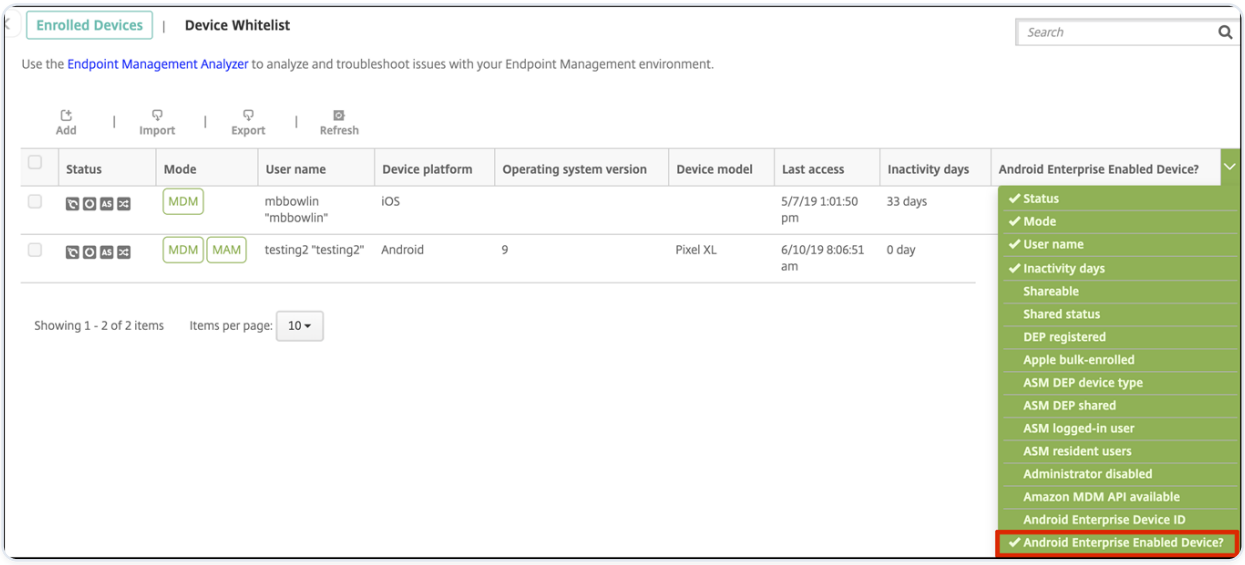
新規デバイスおよび工場出荷時設定にリセットされたデバイスは、DPC識別子トークン、近距離無線通信 (NFC) バンプ、またはQRコード方式を使用して、ワークプロファイルを持つ完全管理デ

バイスとして登録されます。Citrix DPC識別子トークンを使用したデバイスの登録、NFCバンプを使用したデバイスの登録、またはQRコードを使用したデバイスの登録を参照してください。

新規デバイスまたは工場出荷時設定にリセットされていないデバイスは、Android Enterpriseワークプロファイルデバイスのプロビジョニングで説明されているように、ワークプロファイルデバイスとして登録されます。

XenMobileコンソールでのAndroid Enterpriseデバイスの表示

1. XenMobileコンソールで、**管理 > デバイス** に移動します。
2. このページのテーブル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？** 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、完全管理デバイスを選択し、**セキュリティ保護** をクリックします。デバイスが完全管理されている場合、**完全ワイプ** アクションは利用可能ですが、**選択的ワイプ** は利用できません。この違いは、デバイスが管理対象のGoogle Playストアからのアプリのみを許可するためです。ユーザーが公開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。組織が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デバイスおよびアプリポリシーの構成

デバイスレベルとアプリレベルの両方で制御されるポリシーの概要については、(/ja-jp/mdx-toolkit/policies-platform/android-enterprise-supported-device-and-mdx-policies.html)を参照してください。

ポリシーについて知っておくべきこと:

- **データ損失防止:** XenMobile MAMコンテナテクノロジーは、暗号化やその他のモバイルデータ損失防止（DLP）テクノロジーを使用してアプリを保護します。Citrix MAM SDKまたはMDX Toolkitを使用して、アプリをMDX対応にします。
- **デバイス制限:** 数十種類のデバイス制限により、次のような機能を制御できます。
  - デバイスカメラの使用
  - 仕事用プロファイルと個人用プロファイル間のコピー＆ペーストの使用
- **アプリごとのVPN:** マネージド構成デバイスポリシーを使用して、Android EnterpriseのVPNプロファイルを構成します。
- **メールポリシー:** アプリの構成には、マネージド構成デバイスポリシーを使用することをお勧めします。

この表は、Android Enterpriseデバイスで利用可能なすべてのデバイスポリシーを一覧表示します。

> **重要:**

Android Enterpriseに登録し、MDXアプリを使用するデバイスの場合: MDXとAndroid Enterpriseを通じて一部の設定を制御できます。MDXには最も制限の少ないポリシー設定を使用し、Android Enterpriseを通じてポリシーを制御してください。

Android Enterpriseアプリの権限	マネージド構成	アプリインベントリ
アプリのアンインストール	管理対象アプリを自動更新(/ja-jp/xenmobile/server/policies/app-auto-update-policy.html)	OSアップデートの制御(/ja-jp/xenmobile/server/policies/control-os-updates.html#android-enterprise-settings)
資格情報(/ja-jp/xenmobile/server/policies/credentials-policy.html#android-enterprise-settings)	カスタムXML(/ja-jp/xenmobile/server/policies/custom-xml-policy.html)	エクスチェンジ
ファイル(/ja-jp/xenmobile/server/policies/files-policy.html#android-enterprise-settings)	キーガード管理(/ja-jp/xenmobile/server/policies/android-enterprise-keyguard-management-policy.html)	キオスク(/ja-jp/xenmobile/server/policies/kiosk-policy.html#android-enterprise-settings)
位置情報(/ja-jp/xenmobile/server/policies/location-policy.html#android-enterprise-settings)	パスコード(/ja-jp/xenmobile/server/policies/passcode-policy.html#android-enterprise-settings)	制限(/ja-jp/xenmobile/server/policies/restrictions-policy.html#android-enterprise-settings)
Samsung MDMライセンスキー(/ja-jp/xenmobile/server/policies/samsung-mdm-license-key-policy.html#samsung-safe-settings)	スケジュール設定(/ja-jp/xenmobile/server/policies/connection-scheduling-policy.html)	ワイファイ
XenMobileオプション(/ja-jp/xenmobile/server/policies/options-		

policy.html#android-enterprise-settings)		

ワークプロファイルを持つ完全管理対象デバイス (COPEデバイス) のデバイスポリシー

ワークプロファイルを持つ完全管理対象デバイス (COPEデバイス) の場合、一部のデバイスポリシーを使用して、デバイス全体とワークプロファイルに個別の設定を適用できます。他のデバイスポリシーを使用して、デバイス全体にのみ、またはワークプロファイルを持つ完全管理対象デバイスのワークプロファイルにのみ設定を適用できます。

ポリシー	適用対象
Android Enterpriseアプリの権限	ワークプロファイル
管理対象構成	ワークプロファイル
アプリインベントリ	ワークプロファイル
アプリのアンインストール	ワークプロファイル
管理対象アプリを自動的に更新	ワークプロファイル
OSアップデートの制御	該当なし
資格情報	仕事用プロファイル
カスタムXML	該当なし
エクスチェンジ	該当なし
ファイル	仕事用プロファイル
キーガード管理	デバイスと仕事用プロファイル
キオスク	該当なし
位置情報	デバイス (位置情報モードのみ)
パスコード	デバイスとワークプロファイル
制限	デバイスとワークプロファイル (デバイスとワークプロファイルで個別のポリシーを作成)

ポリシー	適用対象
Samsung MDMライセンスキー	N/A
スケジュール	ワークプロファイル
ワイファイ	デバイス
XenMobileオプション	ワークプロファイル

以下も参照してください: Android Enterpriseでサポートされているデバイスポリシーと MDXポリシー および MAM SDKの概要。

セキュリティアクション

Android Enterpriseは、次のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、セキュリティアクションを参照してください。

セキュリティアクション	仕事用プロファイル	完全管理
証明書の更新	はい	はい
完全ワイプ	いいえ	はい
検索	はい	はい
ロック	はい	はい
ロックとパスワードのリセット	いいえ	はい
通知（着信音）	はい	はい
取り消し	はい	はい
選択的ワイプ	はい	いいえ

セキュリティアクションに関する注意事項

- 位置情報デバイスポリシーがデバイスの位置情報モードを**高精度**または**バッテリー節約**に設定していない限り、位置情報セキュリティアクションは失敗します。「位置情報デバイスポリシー」を参照してください(/ja-jp/xenmobile/server/policies/location-policy.html#android-enterprise-settings)。

- Android 9.0より前のバージョンのAndroidを実行しているワークプロファイルデバイスの場合：
  - ロックとパスワードのリセットアクションはサポートされていません。
- Android 9.0以降のワークプロファイルデバイスの場合:
  - 送信されたパスコードはワークプロファイルをロックします。デバイス自体はロックされません。
  - ワークプロファイルにパスコードが設定されていない場合:
    - 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要件を満たさない場合: デバイスはロックされます。
  - ワークプロファイルにパスコードが設定されている場合:
    - 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要件を満たさない場合: ワークプロファイルはロックされますが、デバイス自体はロックされません。
- ワークプロファイルを持つ完全に管理されたデバイス (COPEデバイス) の場合:
  - ロックセキュリティアクションをデバイスまたはワークプロファイルに個別に適用できます。

Android Enterpriseエンタープライズの登録解除

Android Enterpriseエンタープライズの使用を中止する場合は、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、そのエンタープライズを通じてすでに登録されているデバイス上のAndroid Enterpriseアプリはデフォルトの状態にリセットされます。Googleはデバイスを管理しなくなります。新しいAndroid Enterpriseエンタープライズに登録する場合は、管理対象Google Playから新しい組織のアプリを承認する必要があります。その後、XenMobileコンソールからアプリを更新できます。

Android Enterpriseエンタープライズの登録が解除された後:

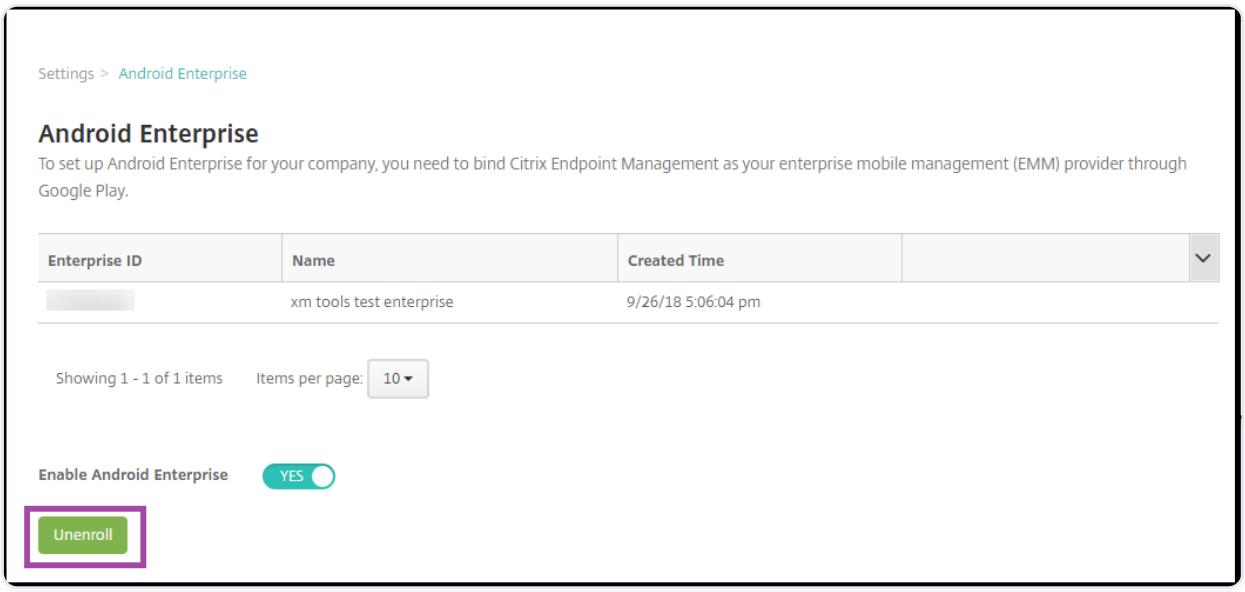
- エンタープライズを通じて登録されたデバイスとユーザーは、Android Enterpriseアプリがデフォルトの状態にリセットされます。以前に適用された管理対象構成ポリシーは、操作に影響を与えなくなります。
- XenMobileは、エンタープライズを通じて登録されたデバイスを管理します。Googleの観点からは、これらのデバイスは管理されていません。新しいAndroid Enterpriseアプリを追加することはできません。マネージド構成ポリシーを適用することはできません。スケジュール、パスワード、制限などの他のポリシーをこれらのデバイスに適用できます。
- Android Enterpriseにデバイスを登録しようとすると、それらは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エンタープライズの登録を解除します。

このタスクを実行すると、XenMobileはXenMobile Toolsのポップアップウィンドウを開きます。開始する前に、使用しているブラウザでXenMobileがポップアップウィンドウを開く権限を持っていることを確認してください。Google Chromeなどの一部のブラウザでは、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許可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、右上隅にある歯車アイコンをクリックします。ページが表示されます。
2. 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。



Android Enterpriseアプリの配布

XenMobile®は、デバイスに展開されたアプリを管理します。次の種類のAndroid Enterpriseアプリを整理して展開できます。

- **管理対象アプリストアアプリ:** これには、管理対象のGoogle Playストアで利用できる無料アプリが含まれます。例: GoToMeeting。
- **MDX:** MAM SDKで準備された、またはMDX Toolkitでラップされたアプリ。これらのアプリにはMDXポリシーが含まれます。MDXアプリは、社内ソースおよびパブリックストアから入手します。Citrix®モバイル生産性向上アプリをMDXアプリとして展開します。
- **エンタープライズ:** 開発した、または別のソースから入手したプライベートアプリ。これらのアプリは、管理対象のGoogle Playストアを通じてユーザーに提供します。管理対象のGoogle Playストアは、Googleのエンタープライズアプリストアです。
- **MDX対応プライベートアプリ:** MAM SDKで準備された、またはMDX Toolkitでラップされたエンタープライズアプリ。

エンタープライズアプリとMDX対応プライベートアプリは、2つの異なる方法で追加できます。

- この記事のエンタープライズアプリおよびMDX対応プライベートアプリのセクションで説明されているように、アプリをエンタープライズアプリとしてXenMobileコンソールに追加します。
- Google開発者アカウントを使用して、アプリを管理対象のGoogle Playストアに直接公開します。次に、アプリを管理対象アプリストアアプリとしてXenMobileコンソールに追加します。管理対象アプリストアアプリを参照してください。

Google開発者アカウントを使用してアプリを公開し、その後XenMobileコンソールを使用するように切り替えた場合、アプリの所有権が異なります。この場合、両方の場所でアプリを管理してください。Citrixでは、いずれかの方法でアプリを追加することをお勧めします。

管理対象のGoogle Playストアから自己管理アプリを削除する必要がある場合は、Googleにチケットをオープンしてください。開発者は、管理対象のGoogle Playストアからアプリを無効にすることはできますが、削除することはできません。

以下のセクションでは、Android Enterpriseアプリの構成に関する詳細情報を提供します。アプリの配布については、アプリの追加を参照してください。この記事には以下が含まれます。

- WebアプリとSaaSアプリ、またはWebリンクを追加するための一般的なワークフロー
- エンタープライズアプリとパブリックストアアプリに必要なアプリワークフロー
- Citrix Content Delivery Network (CDN) for Enterprise Appsからエンタープライズアプリを配信する方法

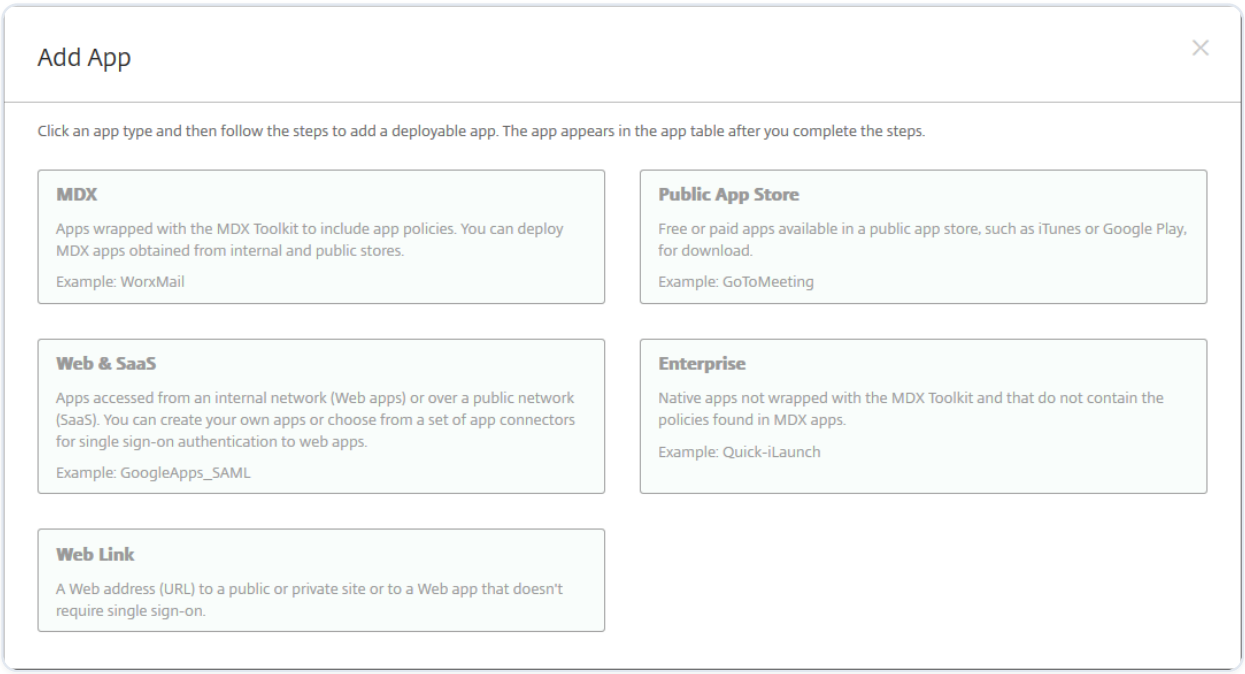
管理対象アプリストアアプリ

管理対象のGoogle Playストアで利用可能な無料アプリをXenMobileに追加できます。

> **注:**
>
> 管理対象のGoogle PlayからGoogle Playストアのすべてのアプリにアクセスできるようにするには、**Access all apps in the managed Google Play store** サーバープロパティを使用します。(/ja-jp/xenmobile/server/advanced-concepts/xenmobile-deployment/server-properties.html)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ユーザーが公開Google Playストアアプリにアクセスできるようになります。その後、(/ja-jp/xenmobile/server/policies/restrictions-policy.html#android-enterprise-settings)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。

ステップ1：アプリの追加と構成

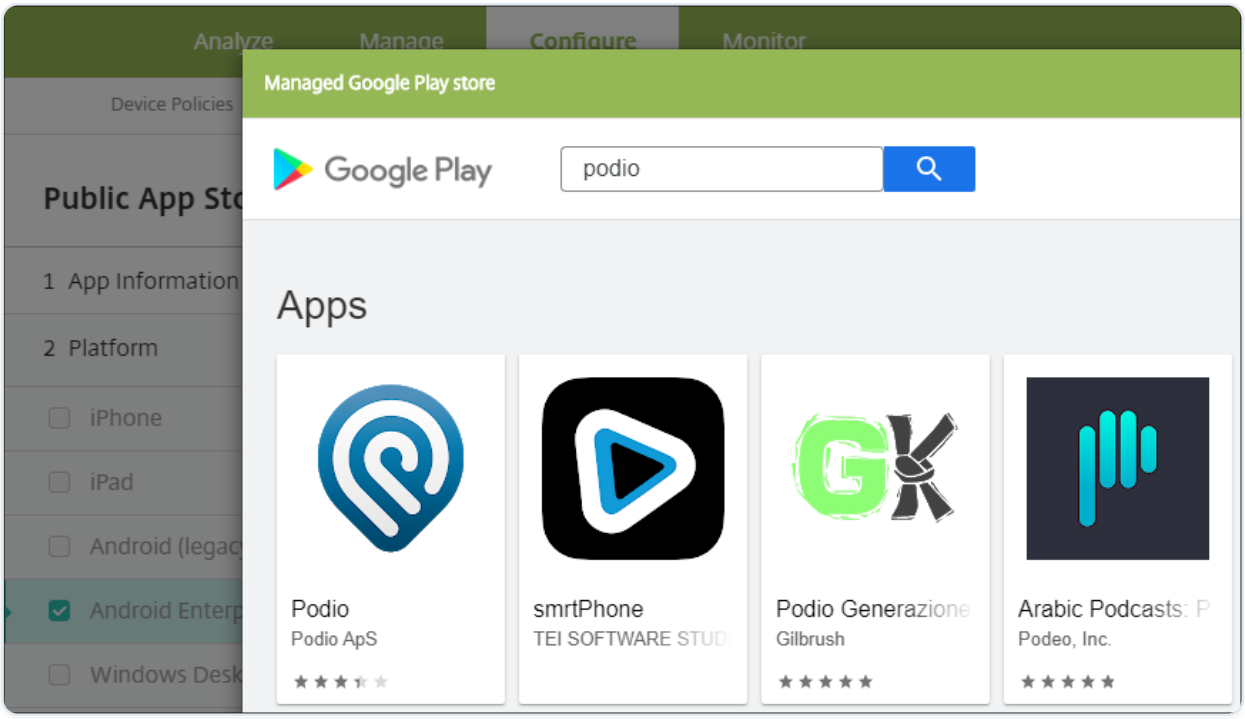
1. XenMobileコンソールで、**Configure > Apps**に移動します。**Add**をクリックします。
2. **Public App Store**をクリックします。



3. **App Information**ペインで、次の情報を入力します。
   - **Name:** アプリのわかりやすい名前を入力します。この名前は、**Apps**テーブルの**App Name**の下に表示されます。
   - **Description:** アプリのオプションの説明を入力します。

- **App category:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、(/ja-jp/xenmobile/server/apps.html#about-app-categories)を参照してください。

4. プラットフォームとして**Android Enterprise**を選択します。
5. 検索ボックスにアプリ名またはパッケージIDを入力し、**Search**をクリックします。パッケージIDはGoogle Playストアで確認できます。IDはアプリのURLに含まれています。たとえば、`com.Slack`は`https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`のパッケージIDです。



6. 検索条件に一致するアプリが表示されます。目的のアプリをクリックし、**承認**をクリックします。

   Android Enterpriseアプリの承認(/en-us/xenmobile/server/media/android-enterprise-public-app-approve.png)

7. もう一度**承認**をクリックします。
8. **アプリが新しい権限を要求した場合でも承認を維持する**を選択します。**保存**をクリックします。

   Google Playの承認設定(/en-us/xenmobile/server/media/google-play-approval-settings.png)

9. アプリアイコンをクリックし、アプリの**名前**と**説明**を設定します。

   Android Enterpriseアプリの構成(/en-us/xenmobile/server/media/android-enterprise-public-app-configure.png)

10. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳細については、「リソースの展開」を参照してください。

ステップ2：アプリの展開を構成する

1. **構成 > デリバリーグループ**に移動し、構成したデリバリーグループを選択します。**編集**をクリックします。
2. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。 アプリを必須としてマークする(/en-us/xenmobile/server/media/required-app-delivery-group.png)
3. **概要**ページで、**保存**をクリックします。
4. **デリバリーグループ**ページで、デリバリーグループを選択し、**展開**をクリックします。

MDXアプリ

MDXファイルをXenMobileに追加し、アプリの詳細とポリシー設定を構成します。Android Enterprise向けにCitrixモバイル生産性向上アプリを構成するには、MDXアプリとして追加します。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。

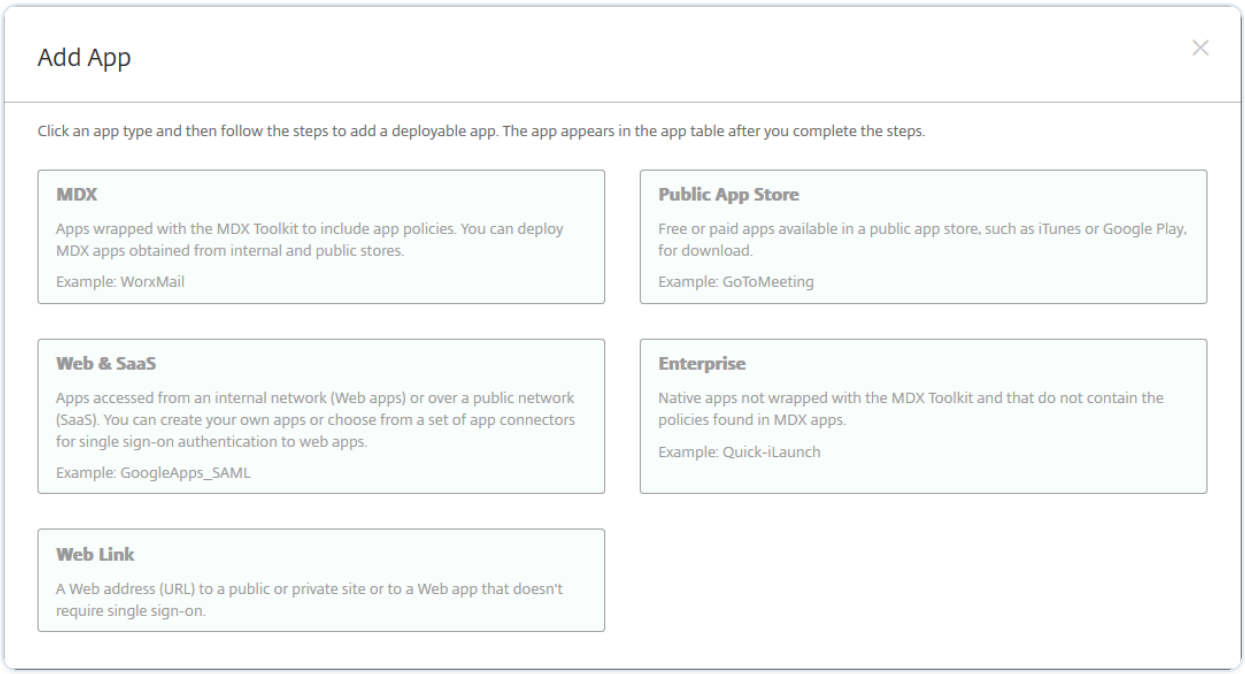
- MAM SDKの概要
- MDXポリシーの概要

手順1：アプリを追加して構成する

1. Citrixモバイル生産性向上アプリの場合は、パブリックストアのMDXファイルをダウンロードします。`<https://www.citrix.com/downloads>`に移動します。**Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**の順に移動します。

   その他の種類のMDXアプリの場合は、MDXファイルを入手します。

2. XenMobileコンソールで、**［構成］>［アプリ］の順にクリックします。［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表示されます。

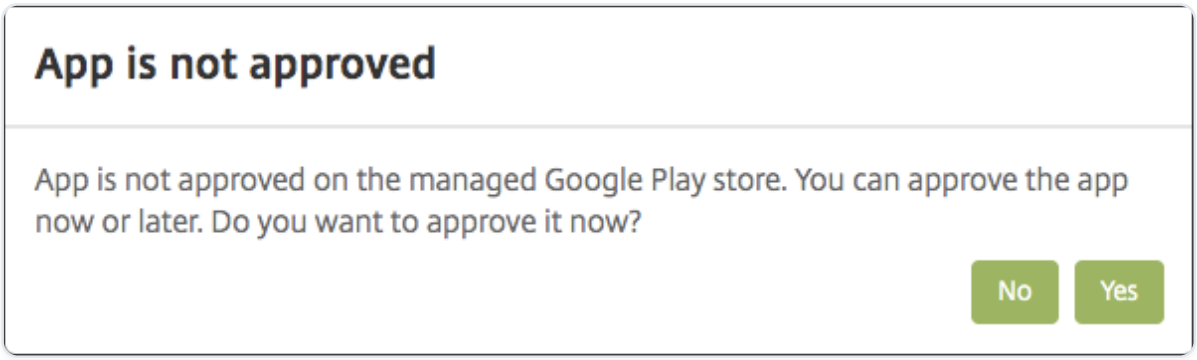


3. **［MDX］をクリックします。［MDXアプリ情報］ページが表示されます。［アプリ情報］**ペインで、次の情報を入力します。

   - **名前：** アプリのわかりやすい名前を入力します。この名前は、**［アプリ］テーブルの［アプリ名］**の下に表示されます。
   - **説明：** アプリのオプションの説明を入力します。
   - **アプリカテゴリ：** 必要に応じて、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリについて詳しくは、「アプリカテゴリについて」を参照してください。

4. プラットフォームとして**［Android Enterprise］**を選択します。
5. **［アップロード］**をクリックして、MDXファイルに移動します。Android Enterpriseは、MAM SDKまたはMDX Toolkitで準備されたアプリのみをサポートします。

   - 添付されたアプリケーションが管理対象のGoogle Playストアからの承認を必要とする場合、UIはそれを通知します。XenMobileコンソールを離れることなくアプリケーションを承認するには、**［はい］**をクリックします。



マネージドGoogle Playストアが開いたら、指示に従ってアプリを承認し、保存します。

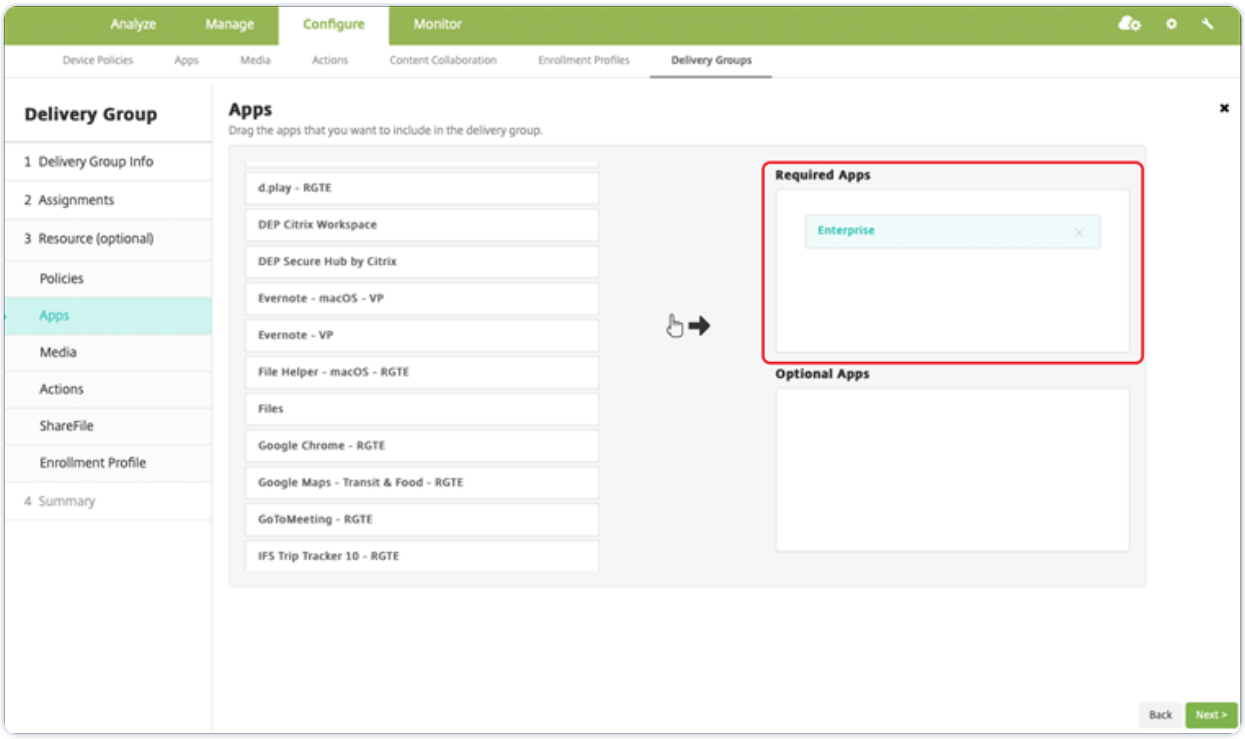
MDXアプリを承認する(/en-us/xenmobile/server/media/mdx-approve-app.png)

アプリの追加に成功すると、**アプリの詳細**ページが表示されます。

6. 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:** 必要に応じて、アプリのバージョン番号を入力します。
   - **パッケージID:** マネージドGoogle Playストアから取得した、アプリのパッケージIDを入力します。
   - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** 必要に応じて、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。
7. **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、アプリの制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールチップがあります。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。
   - MAM SDKの概要
   - MDXポリシーの概要
8. 展開ルールとストア構成を構成します。
9. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳しくは、リソースの展開を参照してください。

ステップ2：アプリの展開を構成する

1. **構成 > デリバリーグループ**に移動し、構成したデリバリーグループを選択します。**編集**をクリックします。
2. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。



3. **概要**ページで、**保存**をクリックします。
4. **デリバリーグループ**ページで、デリバリーグループを選択し、**展開**をクリックします。

エンタープライズアプリ

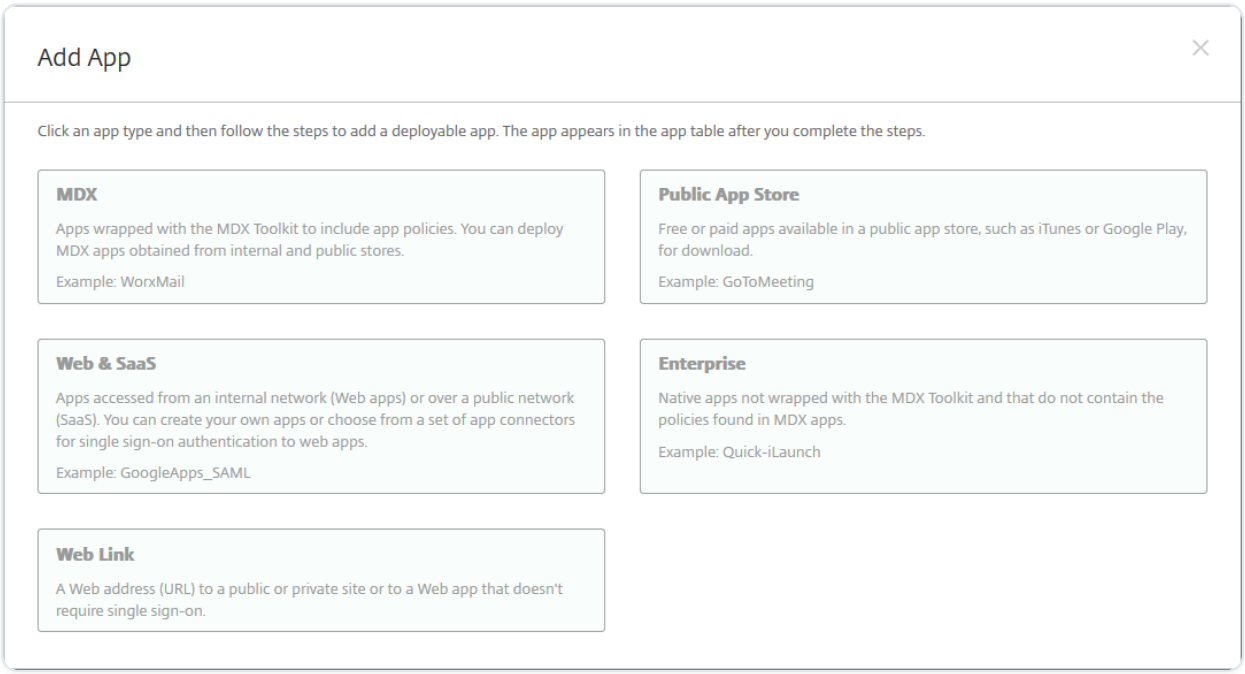
エンタープライズアプリは、MAM SDKまたはMDX Toolkitで準備されていないプライベートアプリを表します。これらのアプリは、自分で開発するか、他のソースから直接入手します。エンタープライズアプリを追加するには、アプリに関連付けられたAPKファイルが必要です。Googleのプライベートアプリのベストプラクティスに従っていることを確認してください。

ステップ1：アプリを追加して構成する

アプリを次の2つのいずれかの方法で追加します。

- アプリを管理対象のGoogle Playストアに直接公開し、管理対象Playストアアプリとして XenMobileコンソールに追加します。Googleのプライベートアプリの公開に関するドキュメントに従い、次に管理対象アプリストアアプリセクションの手順に従います。
- アプリをエンタープライズアプリとしてXenMobileコンソールに追加します。次の手順を実行します。

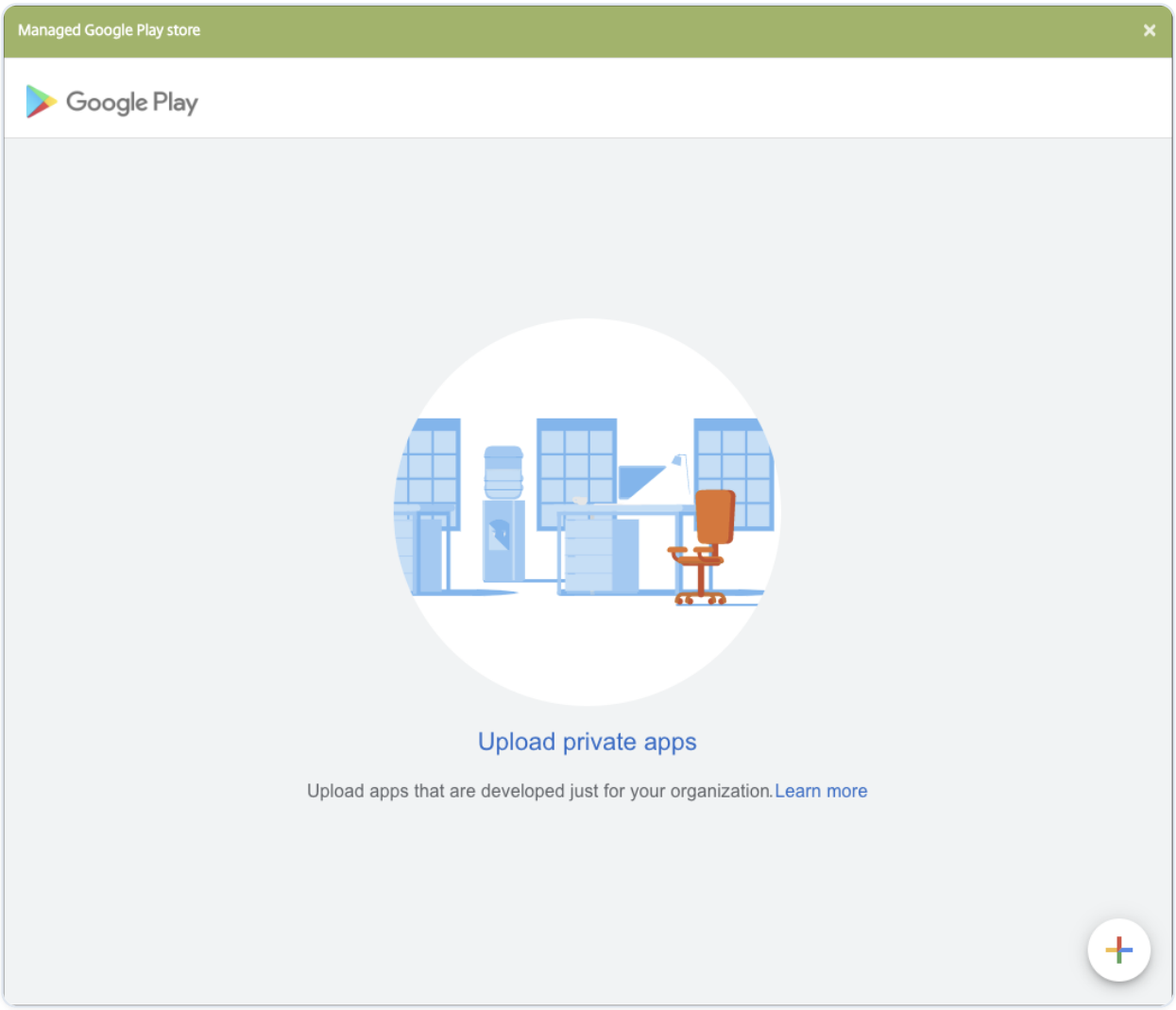
1. XenMobileコンソールで、**構成 > アプリ**をクリックします。**追加**をクリックします。**アプリの追加**ダイアログボックスが表示されます。



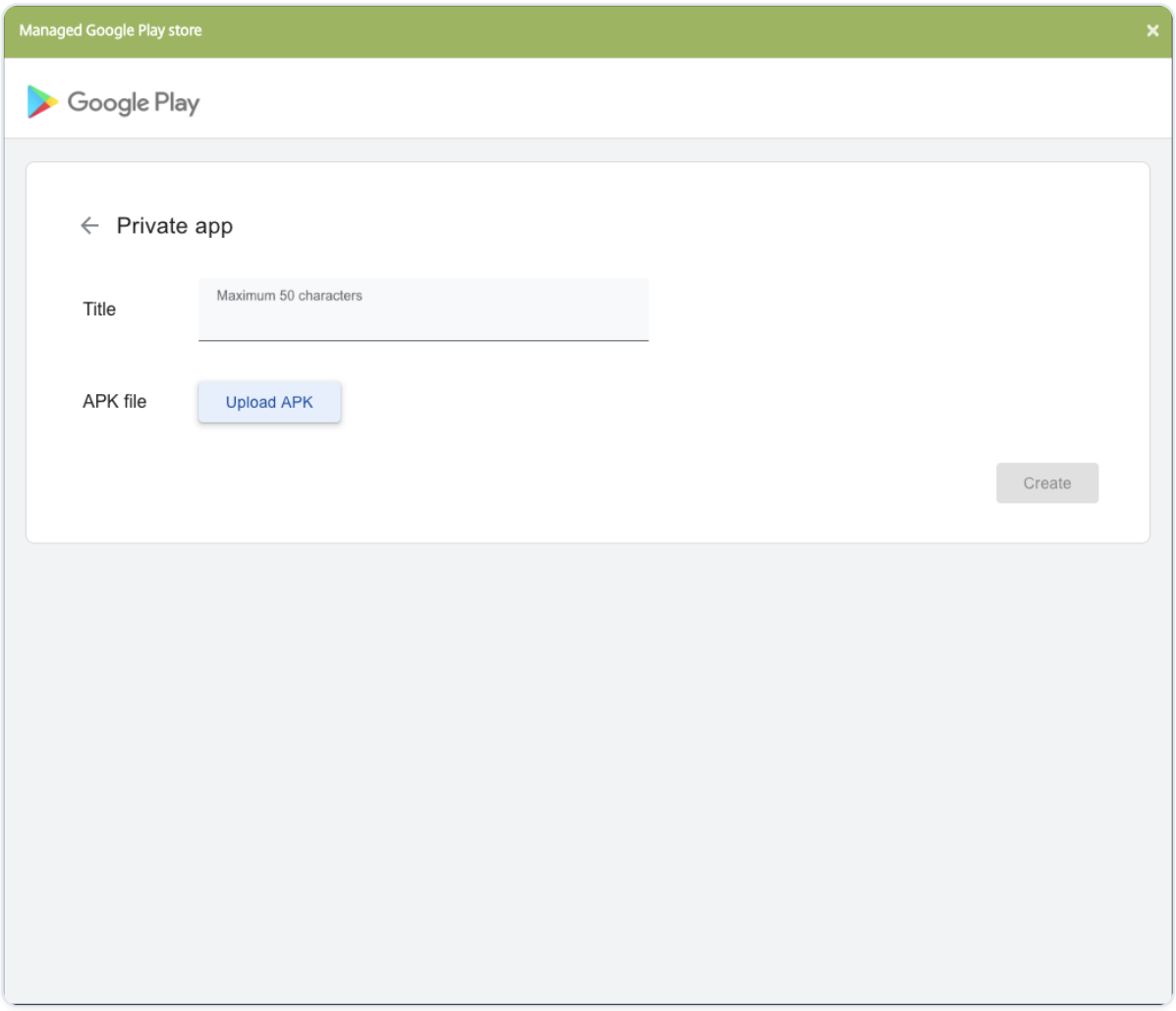
2. 「**Enterprise**」をクリックします。「**App Information**」ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加したいカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

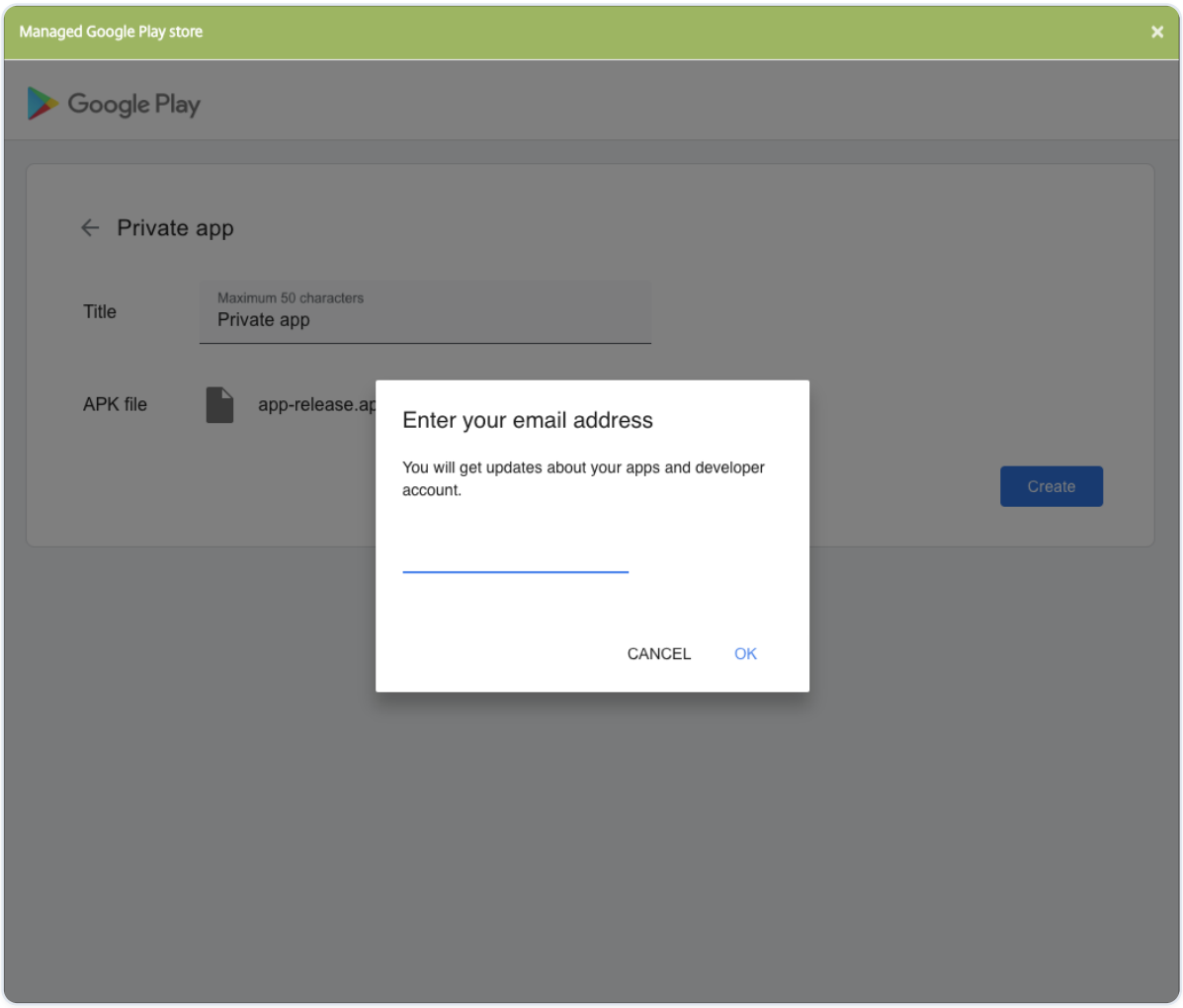
3. プラットフォームとして「**Android Enterprise**」を選択します。
4. 「**アップロード**」ボタンをクリックすると、管理対象のGoogle Playストアが開きます。プライベートアプリを公開するために、開発者アカウントを登録する必要はありません。続行するには、右下隅にある「**プラス**」アイコンをクリックします。



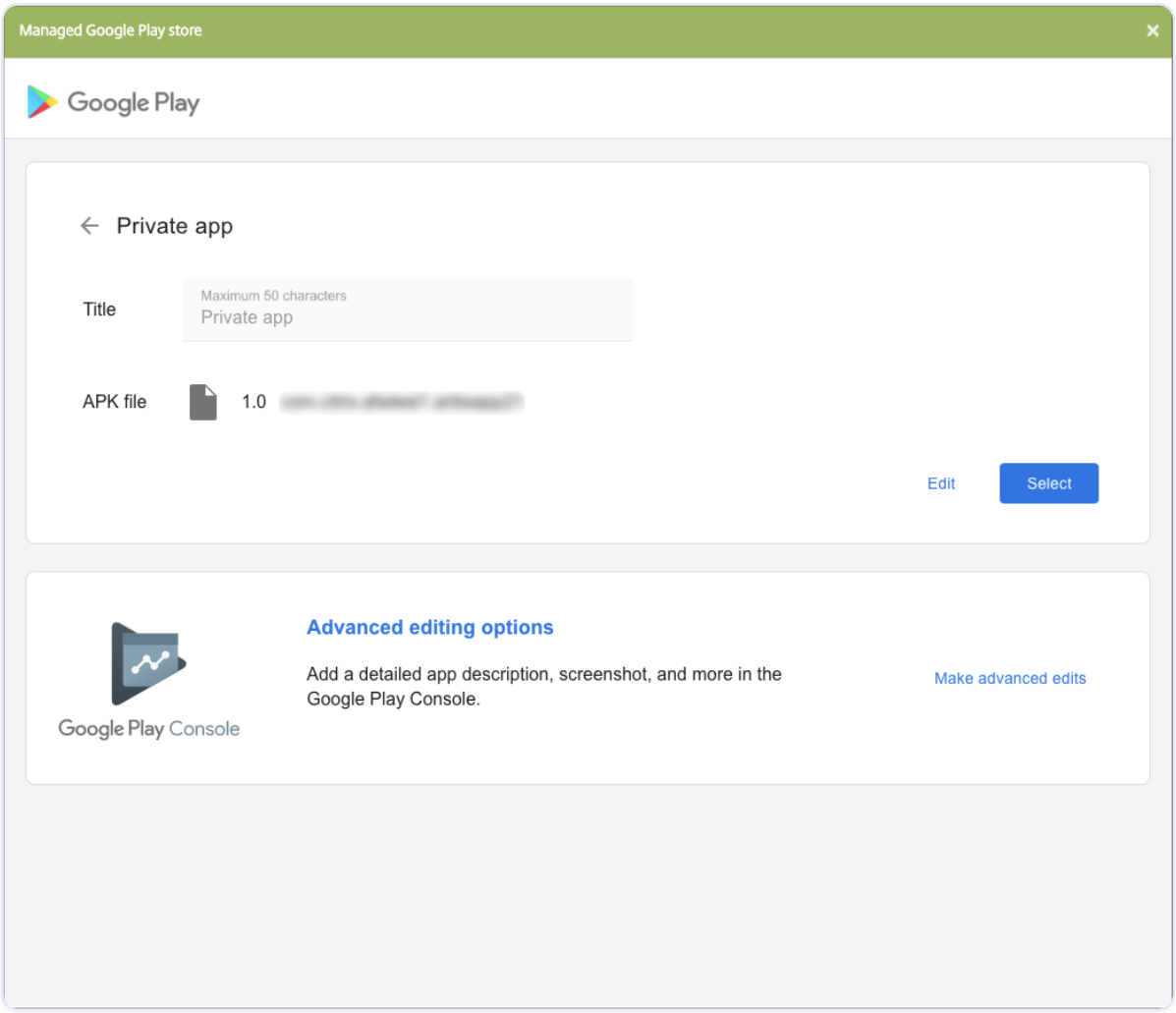
a. アプリの名前を入力し、.apkファイルをアップロードします。完了したら、「**作成**」をクリックします。プライベートアプリが公開されるまでに最大10分かかる場合があります。



b. アプリに関する更新情報を受け取るためのメールアドレスを入力します。



c. アプリケーションが公開されたら、プライベートアプリのアイコンをクリックします。アプリの説明を追加したり、アプリのアイコンを変更したり、その他の操作を行いたい場合は、「**高度な編集を行う**」をクリックします。それ以外の場合は、「**選択**」をクリックしてアプリ情報ページを開きます。



5. 「**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表示されます。
6. プラットフォームの種類の設定を構成します。例:

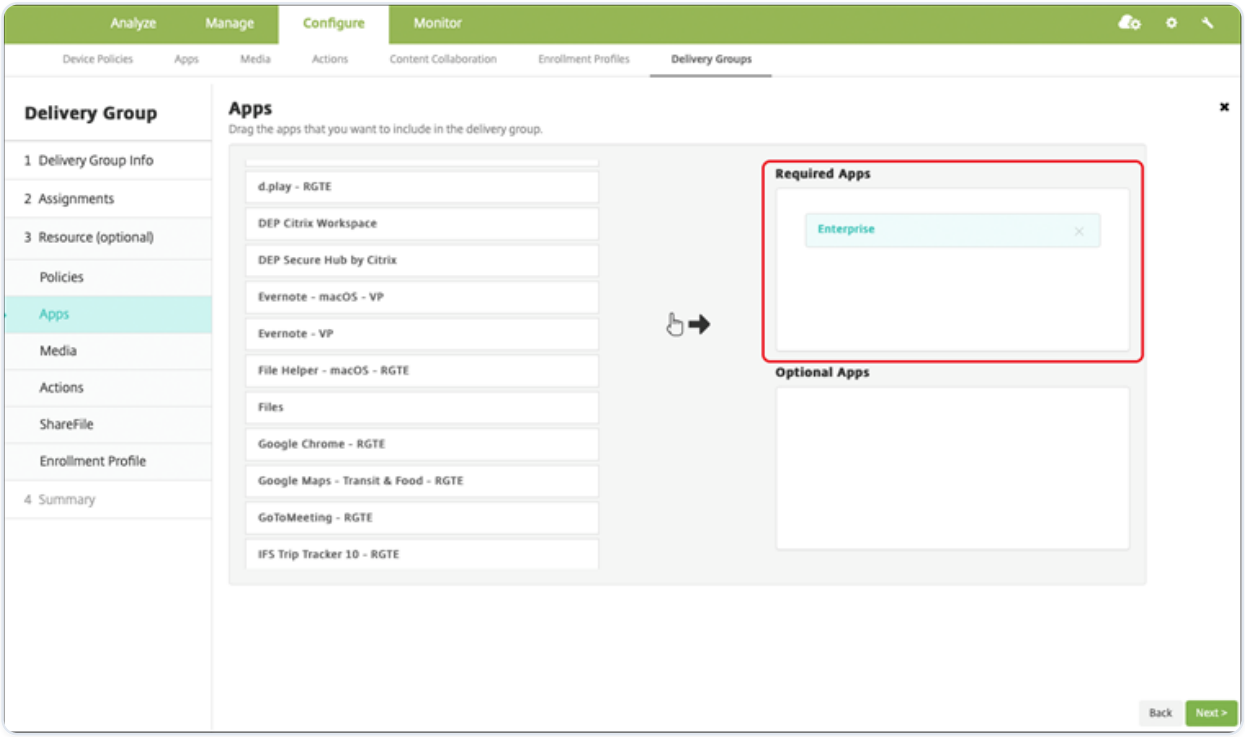
   - **ファイル名:** 必要に応じて、アプリの新しい名前を入力します。
   - **アプリの説明:** 必要に応じて、アプリの新しい説明を入力します。
   - **アプリのバージョン:** このフィールドは変更できません。
   - **パッケージID:** アプリの一意の識別子。
   - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** 必要に応じて、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。

7. 展開ルールとストア構成を構成します。

8. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳細については、「リソースの展開」を参照してください。

ステップ2：アプリの展開を構成する

1. **構成 > デリバリーグループ**に移動し、構成したデリバリーグループを選択します。**編集**をクリックします。
2. **アプリ**セクションで、目的のアプリを**必須アプリ**ボックスにドラッグします。



3. **概要**ページで、**保存**をクリックします。
4. **デリバリーグループ**ページで、デリバリーグループを選択し、**展開**をクリックします。

MDX対応のプライベートアプリ

Android EnterpriseアプリをMDX対応のエンタープライズアプリとして追加するには：

1. プライベートなAndroid Enterpriseアプリを作成し、そのアプリをMDX対応にします。
2. アプリをXenMobileコンソールに追加します。
   - 管理対象のGoogle Playストアでアプリをホストおよび公開します。
   - アプリをエンタープライズアプリとしてXenMobileコンソールに追加します。
3. MDXファイルをXenMobileに追加します。

Google Playストアを通じてアプリをホストおよび公開する場合、Google証明書署名を選択しないでください。アプリをMDX対応にするために使用したのと同じ証明書でアプリに署名します。アプリの公開に関する詳細については、Googleドキュメントのアプリの公開およびアプリへの署名を参照してください。MAM SDKはアプリをラップしないため、アプリの開発に使用された証明書以外の証明書は必要ありません。

Google Play Consoleを通じてプライベートアプリを公開する方法の詳細については、Googleドキュメントの Play Consoleからプライベートアプリを公開するを参照してください。

XenMobileを通じてアプリを公開するには、以下のセクションを参照してください。

プライベートなAndroid Enterpriseアプリを準備する

プライベートなAndroid Enterpriseアプリを作成する際は、Googleのプライベートアプリのベストプラクティスに従ってください。

プライベートなAndroid Enterpriseアプリを作成したら、MAM SDKをアプリと統合するか、MDX Toolkitを使用してアプリをラップします。その後、結果のファイルをXenMobileに追加します。

更新された.apkファイルをアップロードすることで、アプリを更新できます。以下の手順では、MDX Toolkitを使用したアプリのラッピングについて説明します。

1. プライベートなAndroid Enterpriseアプリを作成し、署名済みの.apkファイルを生成します。
2. 以下のサンプルファイルには、既知のすべてのポリシーが含まれていますが、その一部は環境に適用できない場合があります。使用できない設定は無視されます。次のパラメーターを使用してXMLファイルを作成します。

```
<?xml version="1.0" encoding="UTF-8"?>

<MobileAppPolicies>

    <PolicySchemaVersion>

        1.0

    </PolicySchemaVersion>

    <Policies>

        <DevicePasscode>false</DevicePasscode>

        <AppPasscode>false</AppPasscode>
```

```
        <MaxOfflinePeriod>72</MaxOfflinePeriod>

        <StepupAuthAddress/>

        <RequireUserEntropy>false</RequireUserEntropy>

        <BlockRootedDevices>true</BlockRootedDevices>

        <BlockDebuggerAccess>false</BlockDebuggerAccess>

        <RequireDeviceLock>false</RequireDeviceLock>

        <NonCompliantDeviceBehavior>AllowAppAfterWarning</
NonCompliantDeviceBehavior>

        <WifiOnly>false</WifiOnly>

        <RequireInternalNetwork>false</RequireInternalNetwork>

        <InternalWifiNetworks/>

        <AllowedWifiNetworks/>

        <UpgradeGracePeriod>168</UpgradeGracePeriod>

        <WipeDataOnAppLock>false</WipeDataOnAppLock>

        <ActivePollPeriod>60</ActivePollPeriod>

        <PublicFileAccessLimitsList/>

        <CutAndCopy>Unrestricted</CutAndCopy>

        <Paste>Unrestricted</Paste>

        <DocumentExchange>Unrestricted</DocumentExchange>

        <OpenInExclusionList/>

        <InboundDocumentExchange>Unrestricted</InboundDocumentExchange>

        <InboundDocumentExchangeWhitelist/>
```

```
        <connectionSecurityLevel>TLS</connectionSecurityLevel>

        <DisableCamera>false</DisableCamera>

        <DisableGallery>false</DisableGallery>

        <DisableMicrophone>false</DisableMicrophone>

        <DisableLocation>false</DisableLocation>

        <DisableSms>false</DisableSms>

        <DisableScreenCapture>false</DisableScreenCapture>

        <DisableSensor>false</DisableSensor>

        <DisableNFC>false</DisableNFC>

        <BlockLogs>false</BlockLogs>

        <DisablePrinting>false</DisablePrinting>

        <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
MvpnNetworkAccess>

        <MvpnSessionRequired>False</MvpnSessionRequired>

        <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>

        <DisableLocalhostConnections>false</
DisableLocalhostConnections>

        <CertificateLabel/>

        <DefaultLoggerOutput>file,console</DefaultLoggerOutput>

        <DefaultLoggerLevel>15</DefaultLoggerLevel>

        <MaxLogFiles>2</MaxLogFiles>

        <MaxLogFileSize>2</MaxLogFileSize>

        <RedirectSystemLogs>false</RedirectSystemLogs>
```

```
        <EncryptLogs>false</EncryptLogs>

        <GeofenceLongitude>0</GeofenceLongitude>

        <GeofenceLatitude>0</GeofenceLatitude>

        <GeofenceRadius>0</GeofenceRadius>

        <EnableGoogleAnalytics>false</EnableGoogleAnalytics>

        <Authentication>OfflineAccessOnly</Authentication>

        <ReauthenticationPeriod>480</ReauthenticationPeriod>

        <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>

    </Policies>

</MobileAppPolicies>
```

3. MDX Toolkitを使用してアプリをラップします。MDX Toolkitの使用方法については、「Androidモバイルアプリのラッピング」を参照してください。

   apptypeパラメーターを**Premium**に設定します。次のコマンドで、前の手順で作成したXMLファイルを使用します。

   アプリのストアURLがわかっている場合は、**storeURL**パラメーターをストアURLに設定します。アプリを公開すると、ユーザーはストアURLからアプリをダウンロードします。

   SampleAEappというアプリをラップするために使用されるMDX Toolkitコマンドの例を次に示します。

```
```

 java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en
-Duser.variant

 -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap

 -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk

 -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
```
```

```
 -MinPlatform 5.0

 -keystore /MyKeystore

 -storepass mystorepwd123

 -keyalias key0

 -keypass mykeypwd123

 -storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"

 -appType Premium

 -premiumMdxPolicies <Path to Premium policy XML>

```

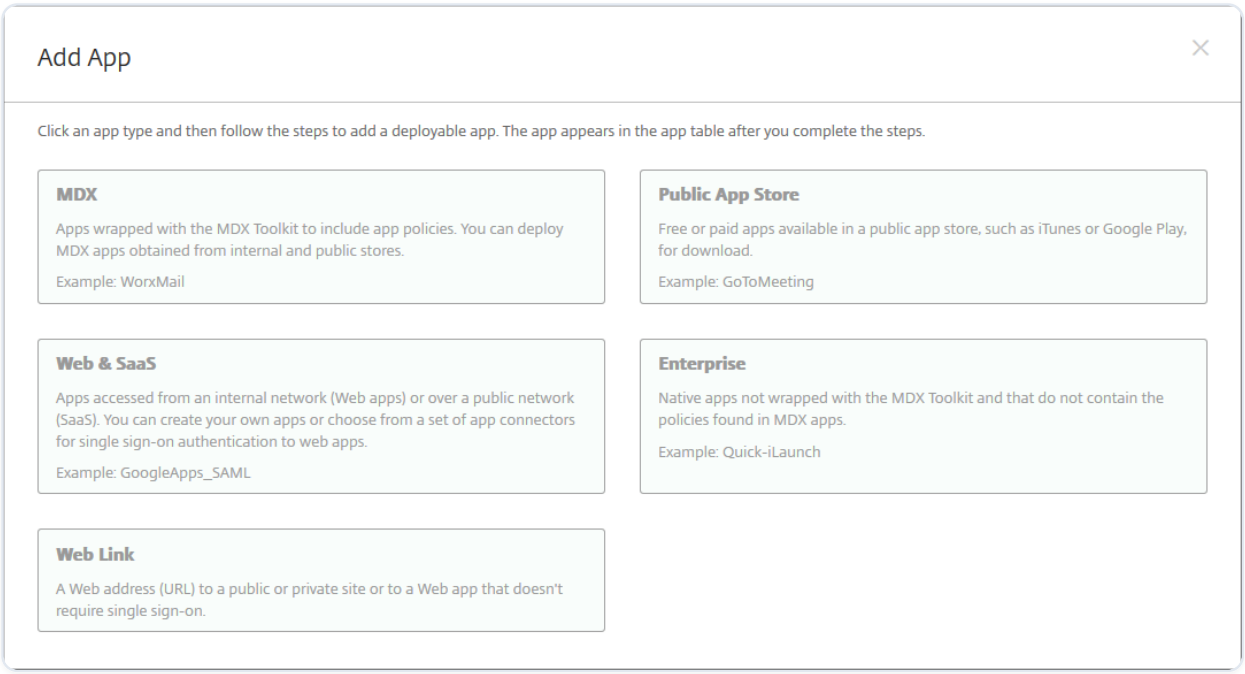
アプリをラップすると、ラップされた.apkファイルと.mdxファイルが生成されます。

ラップされた.apkファイルを追加する

アプリを次の2つの方法のいずれかで追加します。

- アプリを管理対象Google Playストアに直接公開し、管理対象Playストアアプリとして XenMobileコンソールに追加します。Googleのドキュメントに従ってプライベートアプリを公開し、管理対象アプリストアアプリセクションの手順に従います。
- アプリをエンタープライズアプリとしてXenMobileコンソールに追加します。次の手順を実行します。

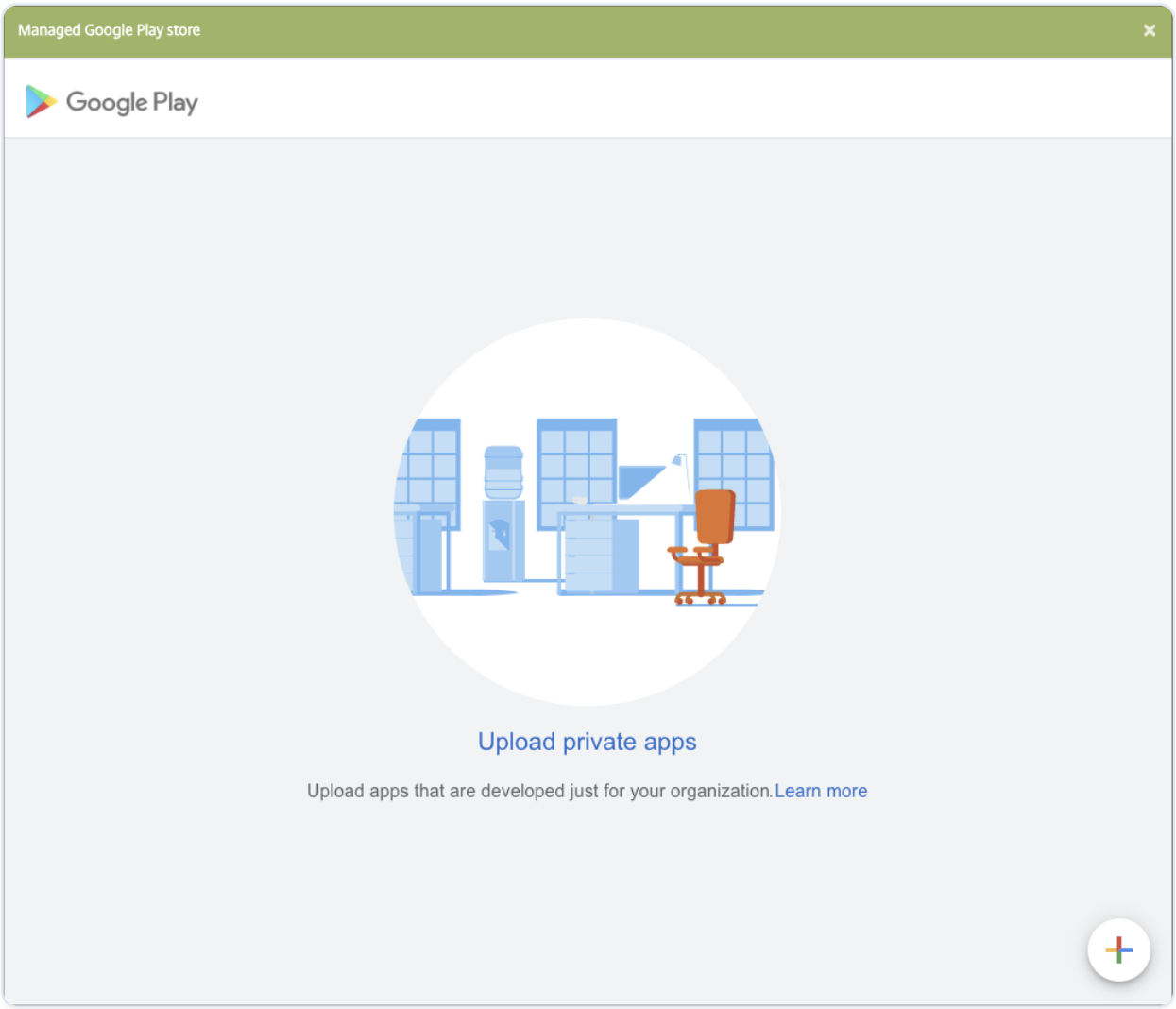
1. XenMobileコンソールで、**［構成］>［アプリ］**の順にクリックします。［アプリ］**ページが開きます。
2. **［追加］**をクリックします。［アプリの追加］**ダイアログボックスが表示されます。



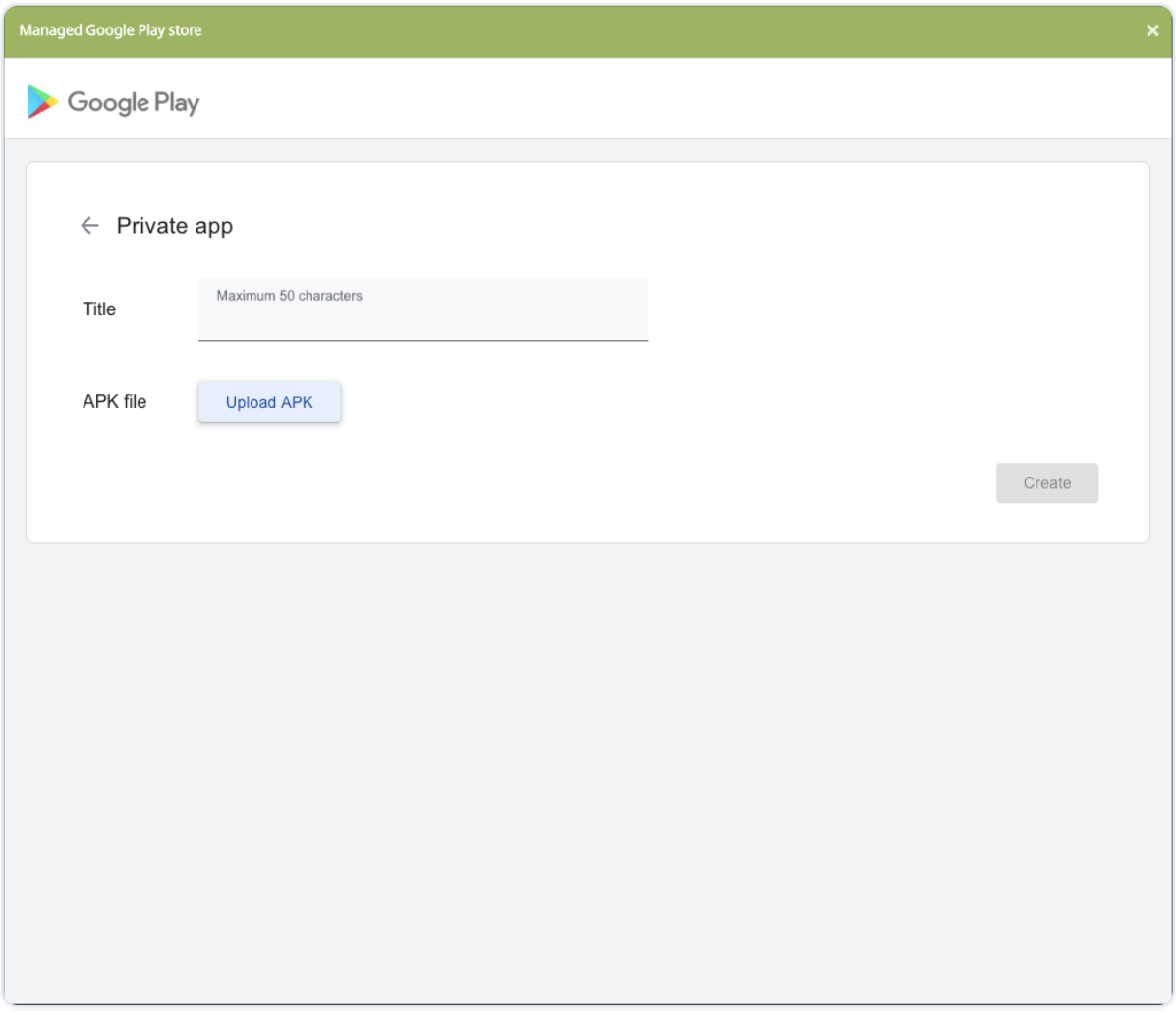
3. **［エンタープライズ］**をクリックします。［アプリ情報］**ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルのアプリ名の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリのカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリのカテゴリの詳細については、「アプリのカテゴリについて」を参照してください。

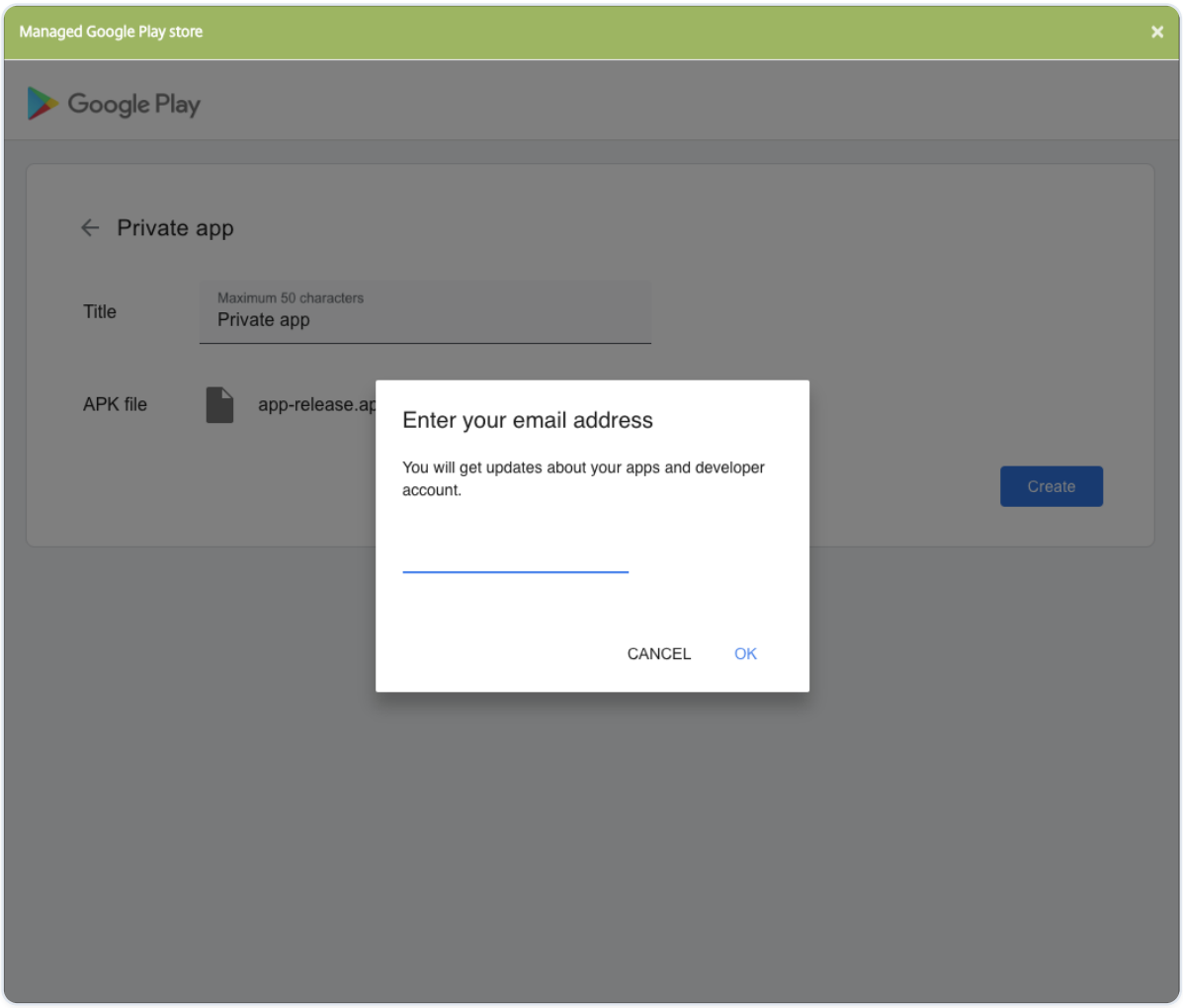
4. プラットフォームとして **Android Enterprise** を選択します。
5. **アップロード**ボタンをクリックすると、管理対象のGoogle Playストアが開きます。プライベートアプリを公開するために開発者アカウントを登録する必要はありません。続行するには、右下隅にある**プラス**アイコンをクリックします。



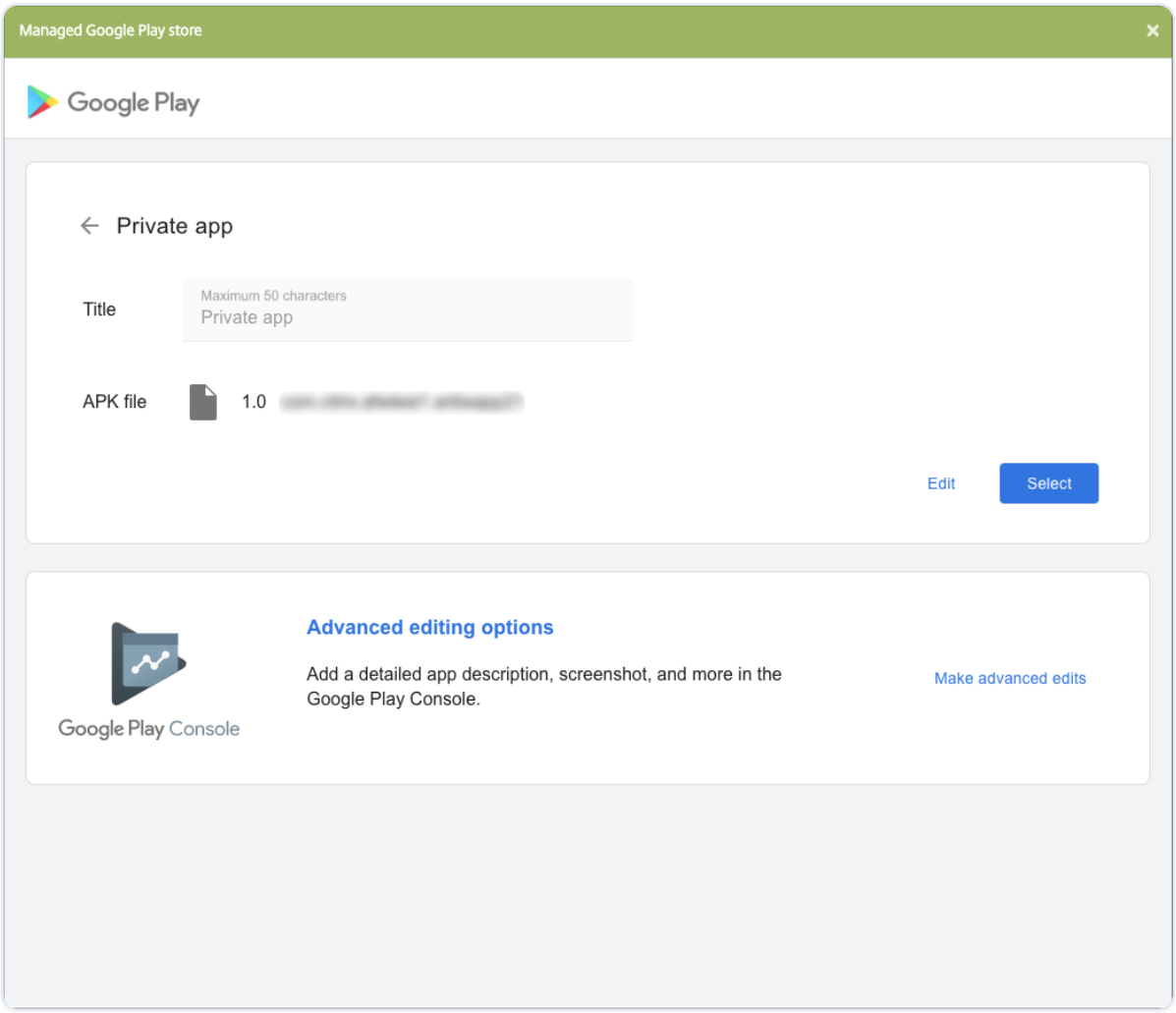
a. アプリの名前を入力し、.apkファイルをアップロードします。完了したら、**作成**をクリックします。プライベートアプリが公開されるまでに最大10分かかる場合があります。



b. アプリに関する更新情報を受け取るためのメールアドレスを入力します。



c. アプリケーションが公開されたら、プライベートアプリのアイコンをクリックし、**選択**をクリックしてアプリ情報ページを開きます。



6. **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表示されます。
7. プラットフォームタイプの次の設定を構成します。

   - **ファイル名:** オプションで、アプリの新しい名前を入力します。
   - **アプリの説明:** オプションで、アプリの新しい説明を入力します。
   - **アプリのバージョン:** このフィールドは変更できません。
   - **パッケージID:** アプリの一意の識別子です。
   - **最小OSバージョン:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムのバージョンを入力します。
   - **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** オプションで、アプリを実行できないデバイスのメーカーまたはモデルを入力します。

8. 展開ルールとストア構成を構成します。

9. **Android Enterprise Enterprise App**ページで、**次へ**をクリックします。**承認**ページが表示されます。

   ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、ワークフローの適用を参照してください。承認ワークフローが必要ない場合は、手順13に進むことができます。

10. **次へ**をクリックします。
11. **デリバリーグループの割り当て**ページが表示されます。このページでは何も操作する必要はありません。.mdxファイルを追加するときに、このアプリのデリバリーグループと展開スケジュールを構成します。**保存**をクリックします。

オプション: ストアURLを追加または変更する

アプリをラップしたときにストアURLがわからなかった場合は、今すぐストアURLを追加してください。

1. 管理対象のGoogle Playストアでアプリを表示します。アプリを選択すると、ブラウザのアドレスバーにストアURLが表示されます。URL形式からアプリのパッケージ名をコピーします。例: `https://play.google.com/store/apps/details?id=SampleAEappPackage`。コピーしたURLは`https://play.google.com/work/`で始まる場合があります。`work`を`store`に変更してください。
2. MDX Toolkitを使用して、ストアURLを.mdxファイルに追加します。

```
java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \

setinfo \

-in ~/Desktop/SampleApps/Sample.mdx \

-out ~/Desktop/SampleApps/wrapped/Sample.mdx \

-storeURL "https://play.google.com/store/apps/details?
id=SampleAEappPackage"
```

.mdxファイルを追加する

1. XenMobileコンソールで、**Configure > Apps**をクリックします。**Add**をクリックします。**Add App**ダイアログボックスが表示されます。

   アプリ構成画面(/en-us/xenmobile/server/media/configure-apps-add.png)

2. **MDX**をクリックします。**MDX App Information**ページが表示されます。**App Information**ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**Apps**テーブルの**App Name**の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加したいカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

3. プラットフォームとして**Android Enterprise**を選択します。
4. **Upload**をクリックして、MDXファイルに移動します。Android Enterpriseは、MDX Toolkitでラップされたアプリのみをサポートしています。

   - 添付されたアプリケーションが管理対象Google Playストアからの承認を必要とする場合、UIが通知します。XenMobileコンソールを離れることなくアプリケーションを承認するには、**Yes**をクリックします。

     MDXアプリを追加(/en-us/xenmobile/server/media/mdx-app-not-approved.png)

     管理対象Google Playストアが開いたら、指示に従ってアプリを承認して保存します。

     MDXアプリを承認(/en-us/xenmobile/server/media/mdx-approve-app.png)

     アプリが正常に追加されると、**App details**ページが表示されます。

5. 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:** 必要に応じて、アプリのバージョン番号を入力します。
   - **パッケージID:** マネージドGoogle Playストアから取得したアプリのパッケージIDを入力します。
   - **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
   - **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
   - **除外デバイス:** 必要に応じて、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。

6. **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、アプリ制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールチップがあります。各デバイスプラットフォームタイプで利用可能なアプリポリシーについては、以下を参照してください。

   - MAM SDKの概要
   - MDXサードパーティアプリポリシーの概要

7. 展開ルールとストア構成を構成します。

   常時接続の展開は、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

   常時接続オプションは次のとおりです。

   - バージョン10.18.19以降でEndpoint Managementの使用を開始したAndroid Enterpriseのお客様は利用できません
   - バージョン10.18.19より前にEndpoint Managementの使用を開始したAndroid Enterpriseのお客様には推奨されません

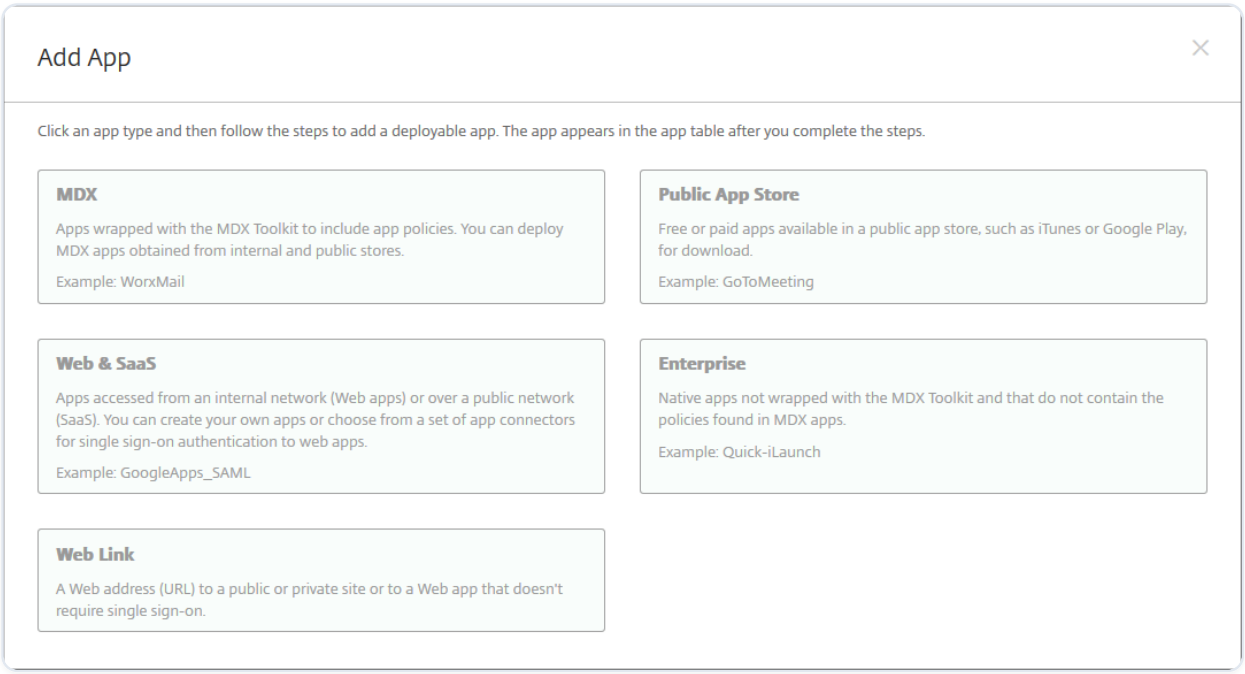
   構成する展開スケジュールは、すべてのプラットフォームで同じです。**常時接続の展開**を除き、行った変更はすべてのプラットフォームに適用されます。

8. アプリにデリバリーグループを割り当て、**保存**をクリックします。詳細については、「リソースの展開」を参照してください。

アプリを更新する

Android Enterpriseアプリを更新するには、更新された.apkファイルをラップしてアップロードします。

1. MAM SDKまたはMDX Toolkitを使用して、更新されたアプリの.apkファイルをラップします。
2. 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。



3. **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表示されます。
4. **エンタープライズ**をクリックします。**アプリ情報**ペインで、次の情報を入力します。

   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

5. プラットフォームとして**Android Enterprise**を選択します。
6. **次へ**をクリックします。**Android Enterpriseエンタープライズアプリ**ページが表示されます。
7. **アップロード**をクリックします。
8. 管理対象Google Playストアページで、更新するアプリを選択します。
9. アプリ情報ページで、.apkファイル名の横にある**編集**をクリックします。

   アプリを編集(/en-us/xenmobile/server/media/publish-enterprise-app.png)
10. 新しい.apkファイルに移動し、アップロードします。
11. 管理対象Google Playストアページで、**保存**をクリックします。

Google Workspace (旧 G Suite) のお客様向けレガシー Android Enterprise

Google Workspace (旧 G Suite) のお客様は、レガシー Android Enterprise を構成するために、レガシー Android Enterprise の設定を使用する必要があります。

レガシー Android Enterprise の要件:

- 公開アクセス可能なドメイン
- Google 管理者アカウント
- 管理プロファイルのサポートがあり、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
- デバイスに設定された仕事用プロファイル

レガシー Android Enterprise の構成を開始するには、XenMobile® 設定の **Android Enterprise** ページで **legacy Android Enterprise** をクリックします。

レガシー Android Enterprise オプションの画像(/en-us/xenmobile/server/media/android-for-work-legacy-1.png)

Android Enterprise アカウントの作成

Android Enterprise アカウントを設定する前に、Google でドメイン名を検証する必要があります。

ドメイン名をすでに Google で検証している場合は、この手順にスキップできます: Android Enterprise サービスアカウントを設定し、Android Enterprise 証明書をダウンロードする。

1. `<https://gsuite.google.com/signup/basic/welcome>` に移動します。

   管理者情報と会社情報を入力する以下のページが表示されます。

   アカウント設定ページの画像(/en-us/xenmobile/server/media/afw-account-setup-redirect.png)
2. 管理者ユーザー情報を入力します。

   管理者ユーザー情報の画像(/en-us/xenmobile/server/media/afw-enter-admin-user-info.png)
3. 管理者アカウント情報に加えて、会社情報を入力します。

   会社情報画面の画像(/en-us/xenmobile/server/media/afw-enter-company-info.png)

   プロセスの最初のステップが完了し、次のページが表示されます。

   確認ページの画像。(/en-us/xenmobile/server/media/afw-dns-verification-1.png)

ドメイン所有権の確認

Googleが次のいずれかの方法でドメインを確認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は最初の方法を推奨しています。この記事ではドメイン所有権を確認する手順については説明していませんが、必要な情報は次の場所で確認できます: https://support.google.com/a/answer/6248925。

1. ドメインの確認を開始するには、**Start**をクリックします。

   Verify domain ownershipページが表示されます。ページの手順に従ってドメインを確認します。

2. **Verify**をクリックします。

   確認ボタンの画像(/en-us/xenmobile/server/media/afw-verify-domain-ownership.png)

   確認画面の画像(/en-us/xenmobile/server/media/afw-domain-verified.png)

3. Googleがドメインの所有権を確認します。

   ドメイン所有権の確認の画像(/en-us/xenmobile/server/media/afw-google-verification.png)

4. 確認が正常に完了すると、次のページが表示されます。**続行**をクリックします。

   成功確認ページの画像(/en-us/xenmobile/server/media/afw-dns-verification-9.png)

5. Googleは、Citrix®に提供し、Android Enterprise設定を構成する際に使用するEMMバインディングトークンを作成します。トークンをコピーして保存します。このトークンは、セットアップ手順の後半で必要になります。

   バインディングトークンの画像(/en-us/xenmobile/server/media/afw-obtain-token.png)

6. Android Enterpriseのセットアップを完了するには、**完了**をクリックします。ドメインが正常に確認され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後、Google管理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をセットアップし、Android Enterprise証明書をダウンロードする

XenMobileがGoogle Playおよびディレクトリサービスに接続できるようにするには、開発者向けのGoogle Project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用Googleサービス間のサーバー間通信に使用されます。使用されている認証プロトコルの詳細については、`<https://developers.google.com/identity/protocols/OAuth2ServiceAccount>`にアクセスしてください。

1. Webブラウザで`<https://console.cloud.google.com/project>`にアクセスし、Google管理者資格情報でサインインします
2. **プロジェクト**リストで、**プロジェクトを作成**をクリックします。

   プロジェクトを作成オプションの画像(/en-us/xenmobile/server/media/google-config-api-1.png)
3. 「**プロジェクト名**」に、プロジェクトの名前を入力します。

   プロジェクト名オプションの画像(/en-us/xenmobile/server/media/google-config-api-2.png)
4. ダッシュボードで、**Google API を使用**をクリックします。

   Google API を使用オプションの画像(/en-us/xenmobile/server/media/google-config-api-6.png)
5. **ライブラリ**をクリックし、**検索**に「**EMM**」と入力して、検索結果をクリックします。

   EMM 検索オプションの画像(/en-us/xenmobile/server/media/afw-emm-search.png)
6. **概要**ページで、**有効にする**をクリックします。

   有効にするオプションの画像(/en-us/xenmobile/server/media/afw-emm-enable.png)
7. **Google Play EMM API**の横にある**資格情報に移動**をクリックします。

   資格情報に移動オプションの画像(/en-us/xenmobile/server/media/google-config-api-13.png)
8. **プロジェクトに資格情報を追加**リストのステップ1で、**サービスアカウント**をクリックします。

   サービスアカウントオプションの画像(/en-us/xenmobile/server/media/google-config-api-1b.png)
9. **サービスアカウント**ページで、**サービスアカウントを作成**をクリックします。

   サービスアカウントを作成オプションの画像(/en-us/xenmobile/server/media/google-config-api-1e.png)
10. 「**サービスアカウントを作成**」でアカウントに名前を付け、「**新しい秘密鍵を提供する**」チェックボックスをオンにします。「**P12**」をクリックし、「**Google Apps ドメイン全体の委任を有効にする**」チェックボックスをオンにしてから、「**作成**」をクリックします。

    サービスアカウント作成オプションの画像(/en-us/xenmobile/server/media/google-config-api-1f.png)

    証明書（P12ファイル）がお使いのコンピューターにダウンロードされます。証明書は安全な場所に保存してください。
11. 「**サービスアカウントが作成されました**」確認ページで、**閉じる**をクリックします。

確認ページの画像(/en-us/xenmobile/server/media/google-config-api-20.png)

12. **権限**で、**サービスアカウント**をクリックし、サービスアカウントの**オプション**の下にある**クライアントIDを表示**をクリックします。

    クライアントID表示オプションの画像(/en-us/xenmobile/server/media/google-config-api-1g.png)

13. Google管理コンソールでのアカウント認証に必要な詳細が表示されます。**クライアントID**と**サービスアカウントID**を、後で情報を取得できる場所にコピーします。この情報とドメイン名をCitrixサポートに送信して許可を得る必要があります。

    アカウント認証の詳細の画像(/en-us/xenmobile/server/media/google-config-api-1h.png)

14. 「**ライブラリ**」ページで、**Admin SDK**を検索し、検索結果をクリックします。

    Admin SDK検索の画像(/en-us/xenmobile/server/media/afw-admin-sdk-search.png)

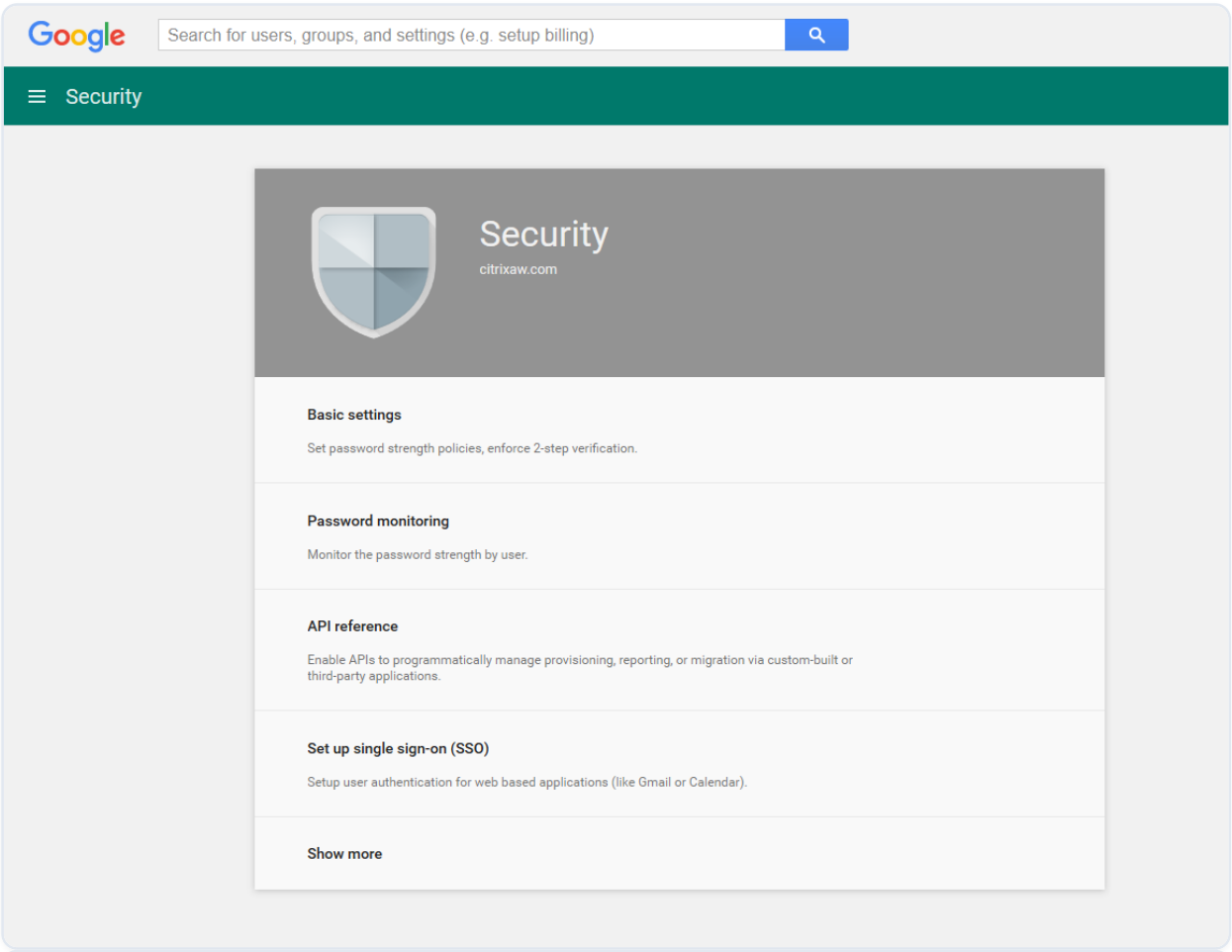
15. 「**概要**」ページで、**有効にする**をクリックします。

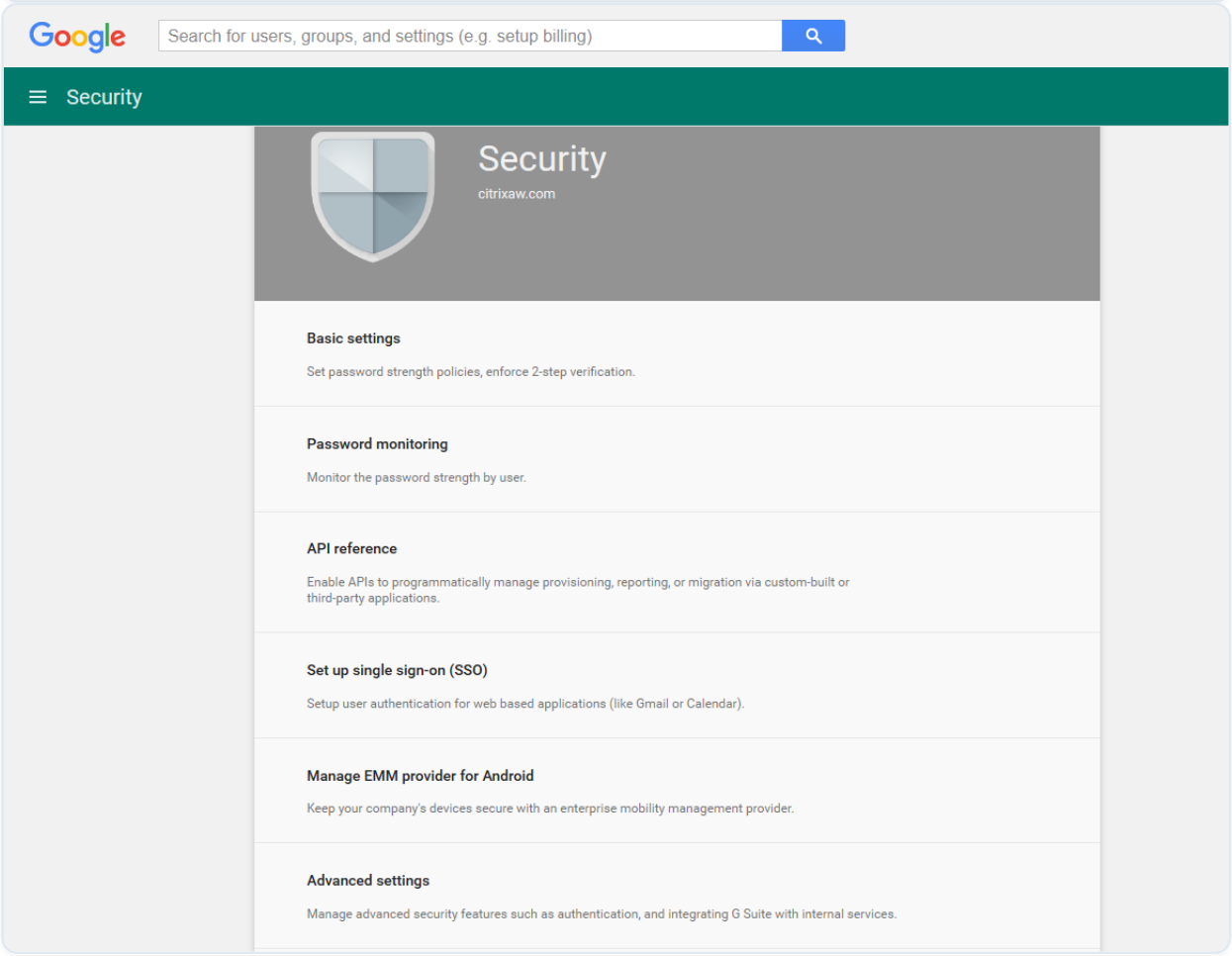
    有効にするボタンの画像(/en-us/xenmobile/server/media/afw-admin-sdk-enable.png)

16. お使いのドメインのGoogle管理コンソールを開き、**セキュリティ**をクリックします。

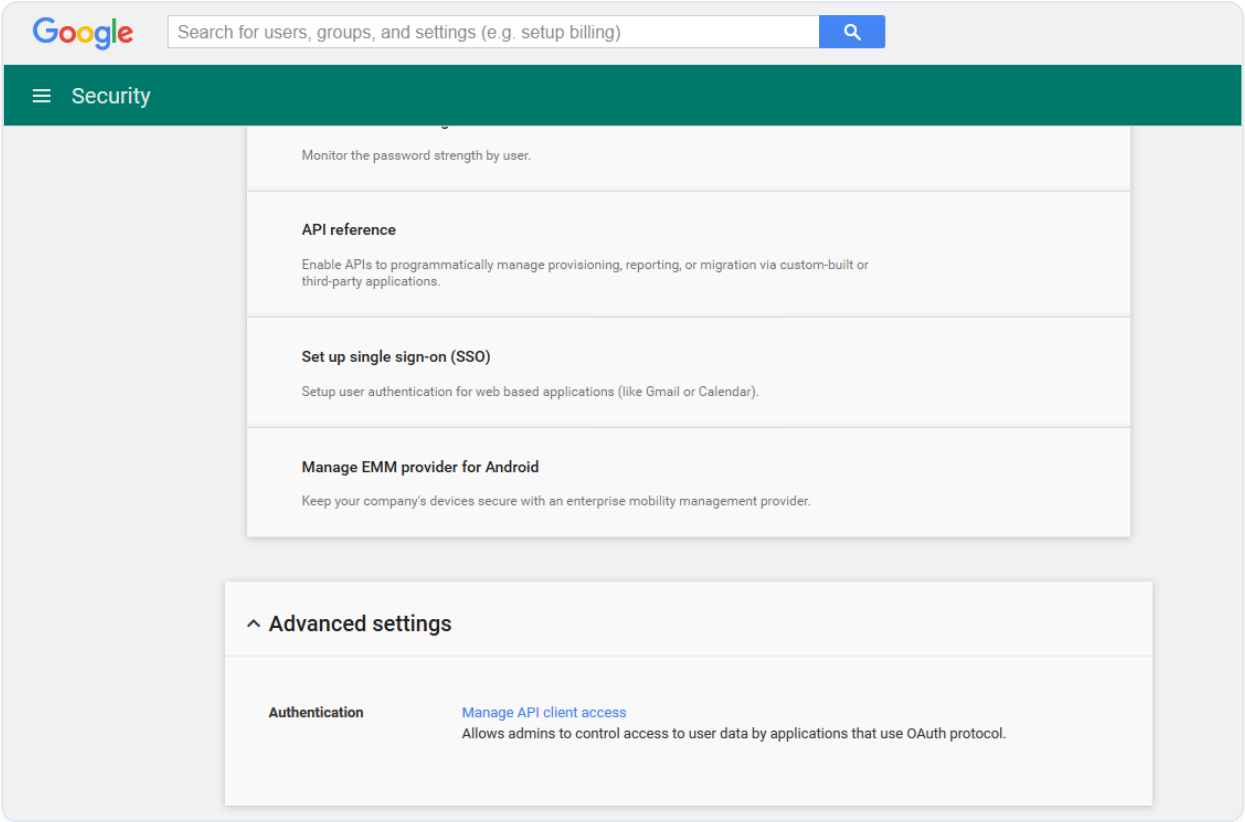
    セキュリティオプションの画像(/en-us/xenmobile/server/media/afw-admin-console-security-1.png)

17. 「**設定**」ページで、**詳細を表示**をクリックし、**詳細設定**をクリックします。

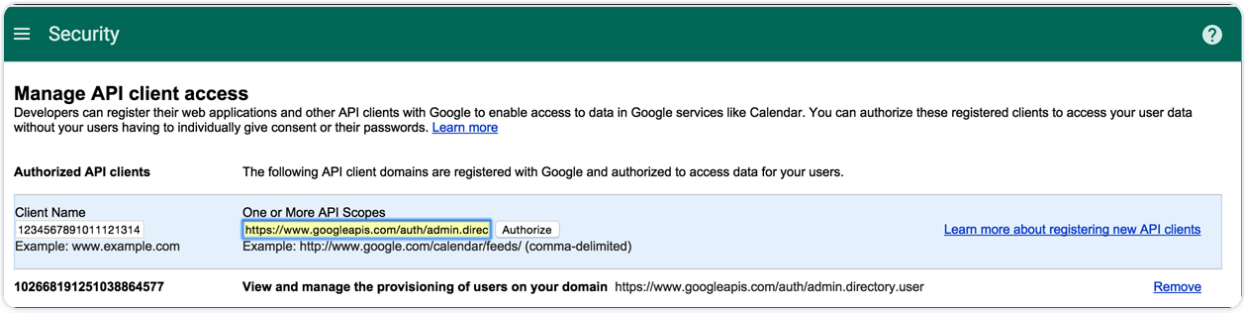

Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Show more


Google
Search for users, groups, and settings (e.g. setup billing)
Security
Security
citrixaw.com
Basic settings
Set password strength policies, enforce 2-step verification.
Password monitoring
Monitor the password strength by user.
API reference
Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.
Set up single sign-on (SSO)
Setup user authentication for web based applications (like Gmail or Calendar).
Manage EMM provider for Android
Keep your company's devices secure with an enterprise mobility management provider.
Advanced settings
Manage advanced security features such as authentication, and integrating G Suite with internal services.

18. **API クライアント アクセスの管理**をクリックします。



19. **クライアント名**に以前保存したクライアント ID を入力し、**1 つ以上の API スコープ**に `https://www.googleapis.com/auth/admin.directory.user` と入力してから、**承認**をクリックします。



EMM へのバインド

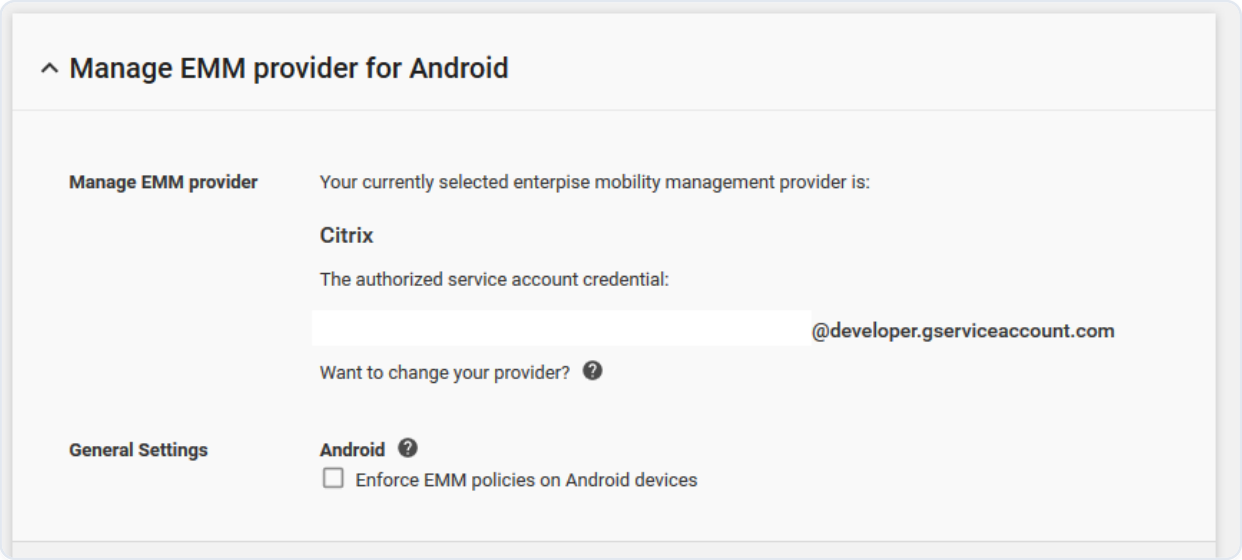
XenMobile を使用して Android デバイスを管理する前に、Citrix テクニカルサポートに連絡し、ドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。Citrix は、お客様のエンタープライズモビリティ管理 (EMM) プロバイダーとして、トークンを XenMobile にバインドします。Citrix テクニカルサポートの連絡先については、「Citrix テクニカルサポート」を参照してください。

1. バインドを確認するには、Google 管理ポータルにサインインし、**セキュリティ**をクリックします。

2. **Android 用 EMM プロバイダーの管理**をクリックします。

   Google Android Enterprise アカウントが EMM プロバイダーとして Citrix にバインドされていることがわかります。

   トークンのバインドを確認したら、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 (SSO) を有効にし、少なくとも 1 つの Android Enterprise デバイスポリシーを定義します。



P12 証明書をインポートする

Android Enterprise P12 証明書をインポートするには、次の手順に従います。

1. XenMobileコンソールにサインインします。
2. コンソールの右上隅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**ページが表示されます。

   証明書ページの画像(/en-us/xenmobile/server/media/afw-certificates-page.png)

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表示されます。

   インポートダイアログボックスの画像(/en-us/xenmobile/server/media/afw-import-certificate-detail.png)

   次の設定を構成します。

   - **インポート:** リストで、**キーストア**をクリックします。
   - **キーストアの種類:** リストで、**PKCS#12**をクリックします。
   - **用途:** リストで、**サーバー**をクリックします。

- **キーストアファイル: 参照**をクリックし、P12証明書に移動します。
- **パスワード:** キーストアのパスワードを入力します。
- **説明:** 必要に応じて、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サーバー設定をセットアップする

1. XenMobileコンソールで、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. 「**サーバー**」の下で、「**Android Enterprise**」をクリックします。「**Android Enterprise**」ページが表示されます。

   Android Enterpriseページの画像(/en-us/xenmobile/server/media/settings-server-legacy-android-for-work.png)

   次の設定を構成し、「**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。
   - **ドメイン管理者アカウント:** ドメイン管理者のユーザー名を入力します。例: Google Developer Portalで使用したメールアカウント。
   - **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サービスアカウントに関連付けられているメールアドレス (`serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com`)。
   - **クライアントID:** Googleサービスアカウントの数値クライアントIDを入力します。
   - **Android Enterpriseを有効にする:** Android Enterpriseを有効または無効にするには、これを選択します。

SAMLベースのシングルサインオンを有効にする

1. XenMobileコンソールにサインインします。
2. コンソールの右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
3. 「**証明書**」をクリックします。「**証明書**」ページが表示されます。

   証明書ページの画像(/en-us/xenmobile/server/media/afw-certificates-export-saml.png)

4. 証明書の一覧で、SAML証明書をクリックします。
5. 「**エクスポート**」をクリックし、証明書をコンピューターに保存します。

6. Android Enterprise管理者認証情報を使用してGoogle管理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は、Google管理ポータルを参照してください。
7. **セキュリティ**をクリックします。

   セキュリティオプションの画像(/en-us/xenmobile/server/media/afw-admin-console-security-1.png)
8. **セキュリティ**の下にある**シングルサインオン (SSO) の設定**をクリックし、次の設定を構成します。

   SSO設定の画像(/en-us/xenmobile/server/media/afw-sso-settings.png)

   - **サインインページURL:** システムおよびGoogle Appsにサインインするユーザーの URLを入力します。例: `https://<Xenmobile-FQDN>/aw/saml/signin`。
   - **サインアウトページURL:** ユーザーがサインアウトしたときにリダイレクトされるURLを入力します。例: `https://<Xenmobile-FQDN>/aw/saml/signout`。
   - **パスワード変更URL:** ユーザーがシステムでパスワードを変更できるようにする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ている場合、SSOが利用できない場合でも、ユーザーはこのプロンプトを表示されます。
   - **検証証明書: ファイルを選択**をクリックし、XenMobileからエクスポートされたSAML証明書に移動します。
9. **変更を保存**をクリックします。

Android Enterpriseデバイスポリシーを設定する

ユーザーが最初に登録するときにデバイスにパスコードを設定する必要があるように、パスコードポリシーを設定します。

パスコードポリシーページの画像(/en-us/xenmobile/server/media/configure-device-policy-passcode-android-for-work.png)

デバイスポリシーを設定するための基本的な手順は次のとおりです。

1. XenMobileコンソールにサインオンします。
2. 「**Configure**」をクリックし、「**Device Policies**」をクリックします。
3. 「**Add**」をクリックし、「**Add a New Policy**」ダイアログボックスで、追加するポリシーを選択します。この例では、「**Passcode**」をクリックします。
4. 「**Policy Information**」ページを完了します。

5. 「**Android Enterprise**」をクリックし、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。

Android Enterpriseアカウント設定を構成する

デバイスでAndroidアプリとポリシーの管理を開始する前に、XenMobileでAndroid Enterpriseドメインと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のセットアップタスクを完了し、ドメイン管理者を設定して、サービスアカウントIDとバインディングトークンを取得します。

1. XenMobile Webコンソールで、右上隅にある歯車アイコンをクリックします。「**Settings**」ページが表示されます。
2. 「**Server**」の下にある「**Android Enterprise**」をクリックします。「**Android Enterprise**」構成ページが表示されます。

Android Enterprise構成ページの画像(/en-us/xenmobile/server/media/settings-server-legacy-android-for-work-1.png)

1. 「**Android Enterprise**」ページで、次の設定を構成します。
   - **Domain Name:** ドメイン名を入力します。
   - **Domain Admin Account:** ドメイン管理者ユーザー名を入力します。
   - **Service Account ID:** GoogleサービスアカウントIDを入力します。
   - **Client ID::** Googleサービスアカウントのクライアントを入力します。
   - **Android Enterpriseを有効にする:** Android Enterpriseを有効にするかどうかを選択します。
2. をクリックします。

XenMobileのGoogle Workspaceパートナーアクセスを設定する

Chromeの一部のエンドポイント管理機能は、GoogleパートナーAPIを使用してXenMobileとGoogle Workspaceドメイン間で通信します。たとえば、XenMobile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を必要とします。

パートナーAPIを有効にするには、XenMobileコンソールでGoogle Workspaceドメインを設定し、Google Workspaceアカウントを構成します。

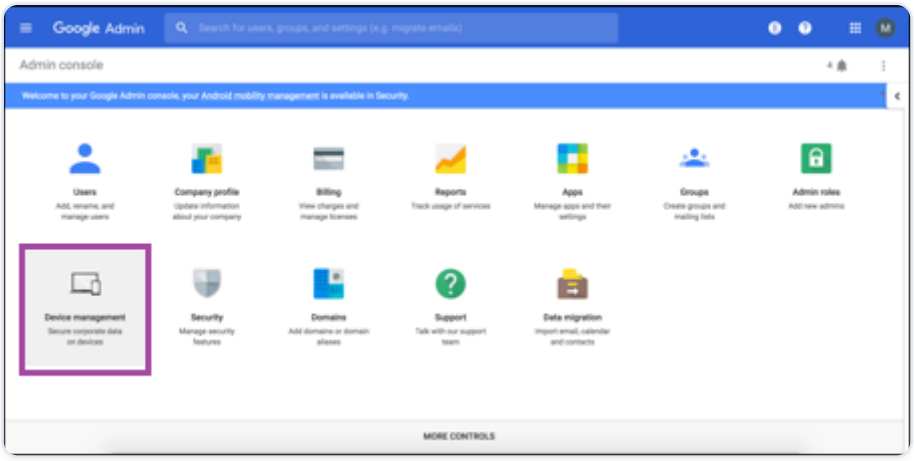
XenMobileでGoogle Workspace（旧G Suite）ドメインを設定する

XenMobileがGoogle Workspaceドメイン内のAPIと通信できるようにするには、 > に移動して設定を構成します。

- **G Suiteドメイン:** XenMobileが必要とするAPIをホストするGoogle Workspace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:** CitrixのクライアントID。この値を使用して、Google Workspaceドメインのパートナーアクセスを構成します。
- **G Suiteエンタープライズ ID:** Googleエンタープライズアカウントから入力された、アカウントのエンタープライズID。

Google Workspace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. をクリックします。



3. 「**Chrome management**」をクリックします。

   Google 管理コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access2.png)

4. 「**User settings**」をクリックします。

   Google 管理コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access3.png)

5. 「**Chrome Management - Partner Access**」を検索します。

   Google 管理コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access4.png)

6. 「**Enable Chrome Management - Partner Access**」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を有効にすることを理解し、同意します。「**Save**」をクリックします。
8. Chrome management ページで、「**Device Settings**」をクリックします。

Google 管理コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access5.png)

9. 「**Chrome Management - Partner Access**」を検索します。

   Google 管理コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access6.png)

10. 「**Enable Chrome Management - Partner Access**」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を有効にすることを理解し、同意します。「**Save**」をクリックします。
12. 「**Security**」ページに移動し、「**Advanced Settings**」をクリックします。

    Google 管理者コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access7.png)

13. **Manage API client Access** をクリックします。
14. XenMobile コンソールで、**Settings > Google Chrome Configuration** に移動し、Google Workspace Client ID の値をコピーします。次に、**Manage API client Access** ページに戻り、コピーした値を **Client Name** フィールドに貼り付けます。
15. **One or More API Scopes** で、URL を追加します: `https://www.googleapis.com/auth/chromedevicemanagementapi`

    Google 管理者コンソールの画像(/en-us/xenmobile/server/media/google-admin-partner-access8.png)

16. **Authorize** をクリックします。

    「Your settings have been saved」というメッセージが表示されます。

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/restrictions-device-policy-ios113.png)

Android Enterprise デバイスの登録

デバイスの登録プロセスでユーザーがユーザー名またはユーザー ID の入力を求められる場合、受け入れられる形式は、XenMobile Server がユーザーをユーザープリンシパル名 (UPN) または SAM アカウント名で検索するように構成されている方法によって異なります。

XenMobile Server が UPN でユーザーを検索するように構成されている場合、ユーザーは次の形式で UPN を入力する必要があります。

- *ユーザー名@ ドメイン*

XenMobile Server が SAM でユーザーを検索するように構成されている場合、ユーザーは次のいずれかの形式で SAM を入力する必要があります。

- *ユーザー名@ ドメイン*
- *domain\username*

XenMobile Serverがどの種類のユーザー名に設定されているかを確認するには：

1. XenMobile Serverコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **LDAP**をクリックして、LDAP接続の構成を表示します。
3. ページの下部にある**ユーザー検索基準**フィールドを確認します。
    - **userPrincipalName**に設定されている場合、XenMobile ServerはUPN用に設定されています。
    - **sAMAccountName**に設定されている場合、XenMobile ServerはSAM用に設定されています。

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エンタープライズの登録を解除できます。

このタスクを実行すると、XenMobile ServerはXenMobile Toolsのポップアップウィンドウを開きます。開始する前に、使用しているブラウザでXenMobile Serverがポップアップウィンドウを開く権限を持っていることを確認してください。Google Chromeなどの一部のブラウザでは、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許可リストに追加する必要があります。

> **警告：**

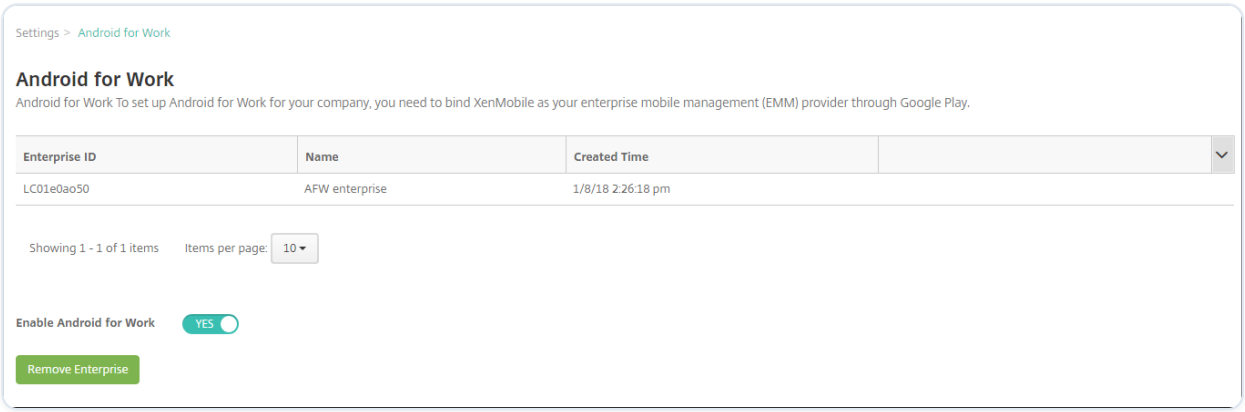
> エンタープライズの登録が解除されると、そのエンタープライズを通じてすでに登録されているデバイス上のAndroid Enterpriseアプリは、デフォルトの状態にリセットされます。デバイスはGoogleによって管理されなくなります。Android Enterpriseエンタープライズに再登録しても、追加の構成なしでは以前の機能が復元されない場合があります。

> Android Enterpriseエンタープライズの登録が解除された後：

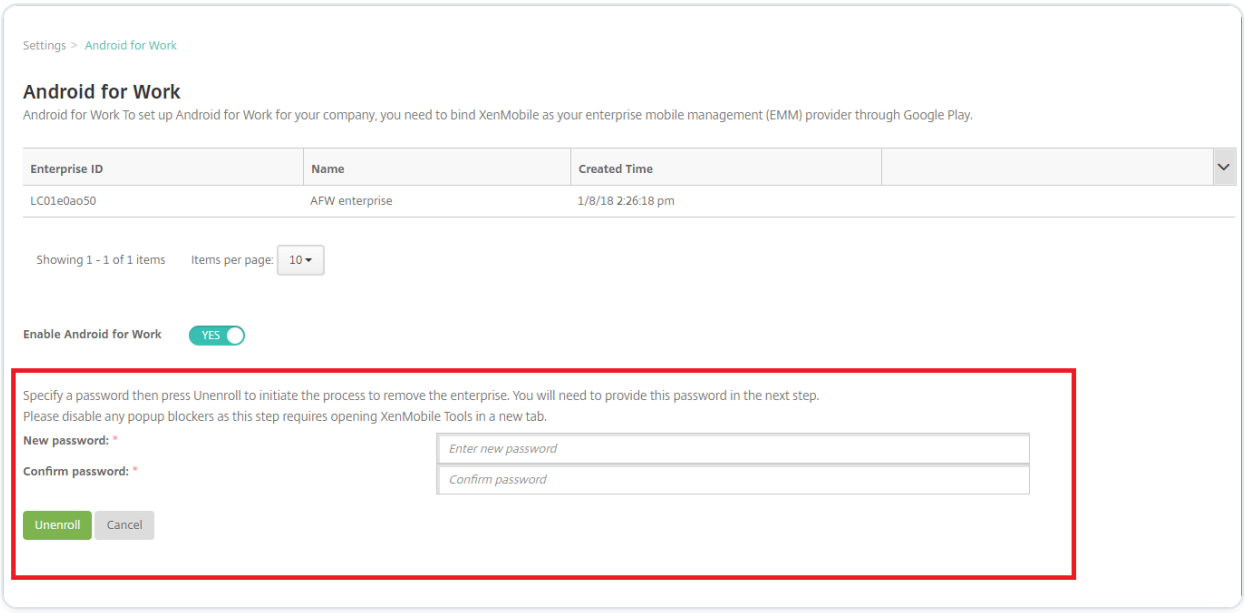
- エンタープライズを通じて登録されたデバイスとユーザーは、Android Enterpriseアプリがデフォルトの状態にリセットされます。以前適用されていたAndroid Enterpriseアプリの権限とAndroid Enterpriseアプリの制限ポリシーは、もはや効果がありません。
- エンタープライズを通じて登録されたデバイスはXenMobileによって管理されますが、Googleの観点からは管理対象外となります。新しいAndroid Enterpriseアプリを追加することはできません。Android Enterpriseアプリの権限またはAndroid Enterpriseアプリの制限ポリシーを適用することはできません。スケジューリング、パスワード、制限などの他のポリシーは、これらのデバイスに引き続き適用できます。
- Android Enterpriseにデバイスを登録しようとすると、それらは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：

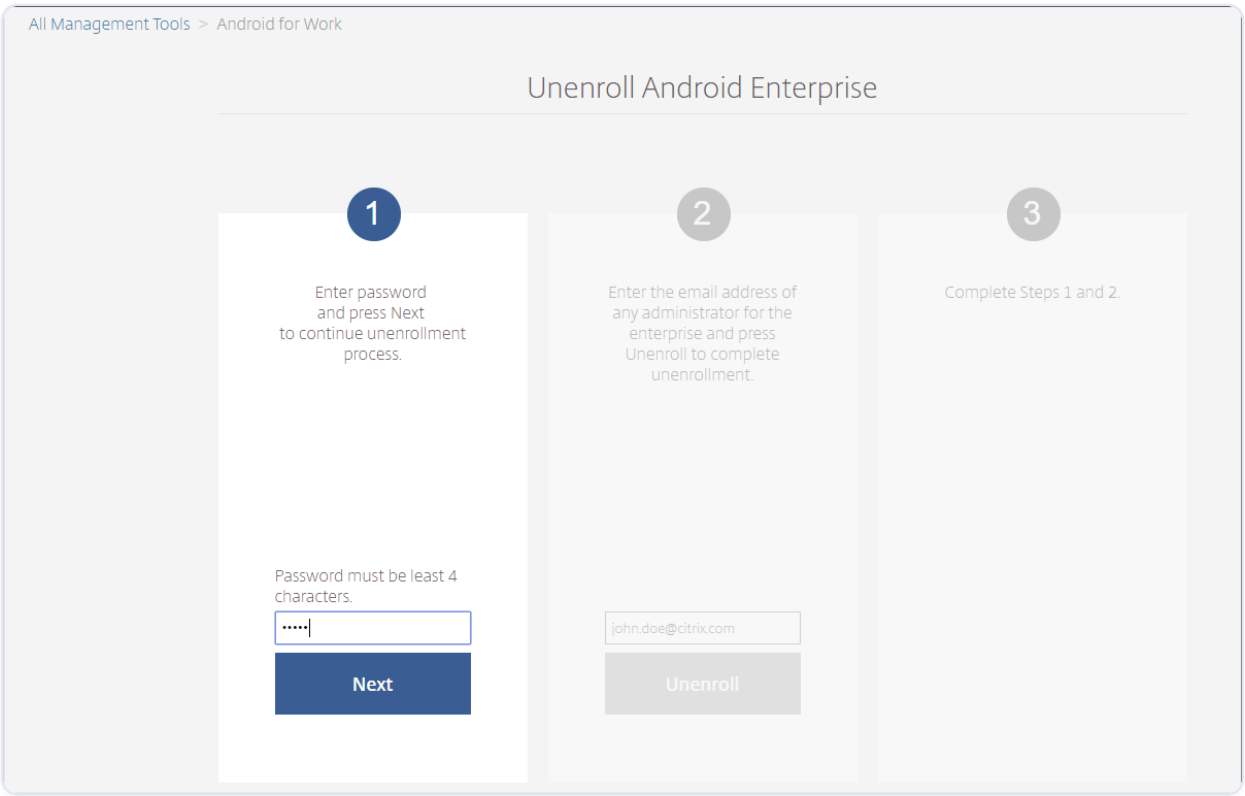
1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。「設定」ページが表示されます。
2. 「設定」ページで、**Android Enterprise**をクリックします。
3. をクリックします。



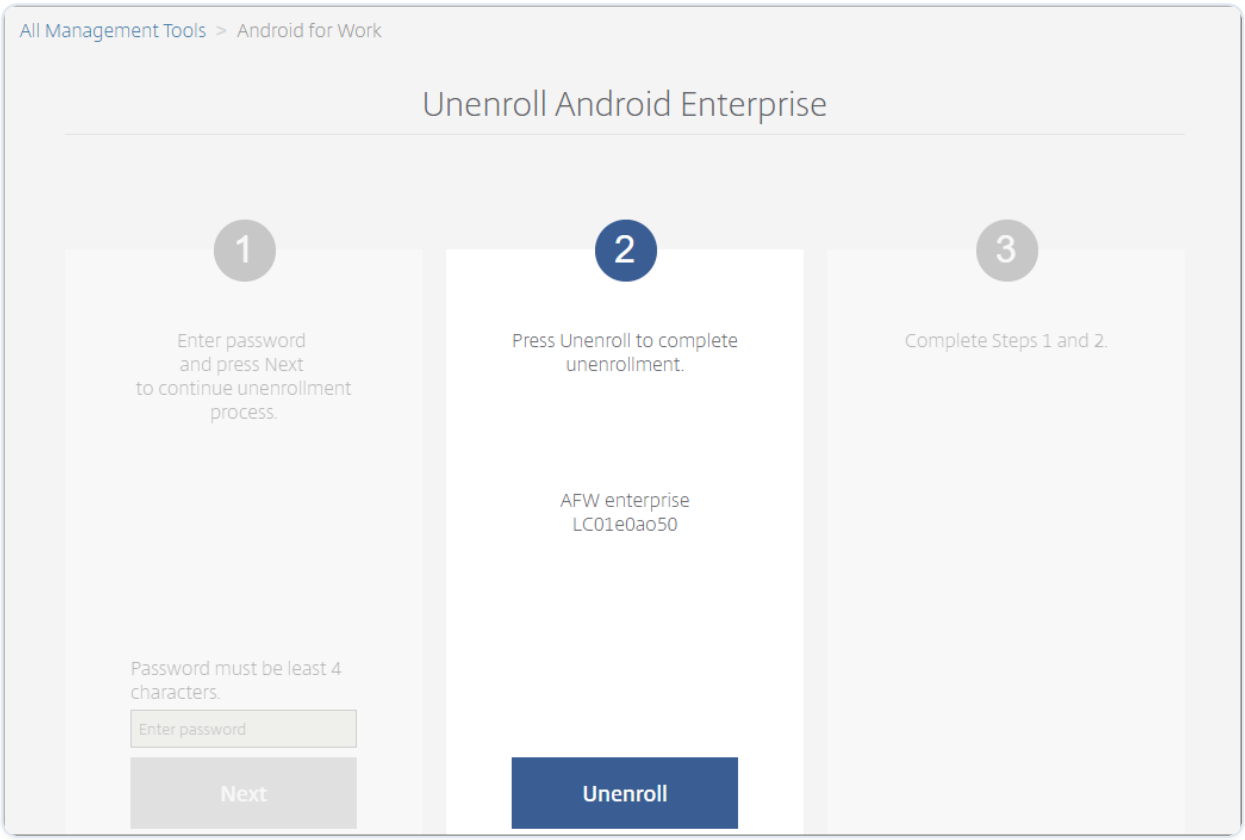
4. パスワードを指定します。登録解除を完了するための次の手順でこのパスワードが必要になります。次に、 をクリックします。



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. をクリックします。



Android Enterpriseでの完全管理対象デバイスのプロビジョニング

会社所有のデバイスのみが、Android Enterpriseの完全管理対象デバイスとなることができます。完全管理対象デバイスでは、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制御されます。完全管理対象デバイスは、仕事用管理対象デバイスとも呼ばれます。

XenMobileは、完全管理対象デバイスの登録に次の方法をサポートしています。

- **afw#xenmobile:** この登録方法では、ユーザーはデバイスのセットアップ時に「afw#xenmobile」という文字を入力します。このトークンは、デバイスがXenMobileによって管理されていることを識別し、Secure Hubをダウンロードします。
- **QRコード:** QRコードプロビジョニングは、タブレットなどNFCをサポートしない分散型デバイス群をプロビジョニングする簡単な方法です。QRコード登録方法は、工場出荷時の設定にリセットされたデバイス群で使用できます。QRコード登録方法は、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で、完全に管理されたデバイスをセットアップおよび構成します。
- **近距離無線通信 (NFC) バンプ:** NFCバンプ登録方法は、工場出荷時の設定にリセットされたデバイス群で使用できます。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。工場出荷時の状態にリセットされたデバイスでは、Bluetooth、Wi-Fi、その他の通信モードは無効になっています。NFCは、この状態でデバイスが使用できる唯一の通信プロトコルです。

afw#ゼノモバイル

この登録方法は、新規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オンにした後、初期設定のために使用されます。ユーザーはGoogleアカウントの入力を求められたときに「afw#xenmobile」と入力します。この操作により、Secure Hubがダウンロードおよびインストールされます。その後、ユーザーはSecure Hubのセットアッププロンプトに従って登録を完了します。

この登録方法は、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 Serverからダウンロードするためにに Secure Hubを提供する必要はありません。

前提条件:

- Android 5.0以降を実行しているすべてのAndroidデバイスでサポートされています。

QRコード

QRコードを使用してデバイスをデバイスモードで登録するには、JSONを作成し、そのJSONをQRコードに変換することでQRコードを生成します。デバイスのカメラがQRコードをスキャンしてデバイスを登録します。

前提条件:

- Android 7.0以降を実行しているすべてのAndroidデバイスでサポートされています。

JSONからQRコードを作成する

以下のフィールドを含むJSONを作成します。

これらのフィールドは必須です:

Key: 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

Value: qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM

キー: android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION

値: `https://path/to/securehub.apk`

> **注:**

> Secure Hubがエンタープライズアプリとしてcitrix XenMobile Serverにアップロードされている場合、`https://<fqdn>:4443/*instanceName*/worxhome.apk`からダウンロードできます。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するWi-Fi接続経由でアクセス可能である必要があります。

> 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2文字の小文字の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2文字の大文字のISO国コード（USなど）です。たとえば、米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:** デバイスが実行されているタイムゾーン。

  Olson形式の地域/場所名を入力します。たとえば、太平洋時間の場合はAmerica/Los_Angelesです。入力しない場合、タイムゾーンは自動的に設定されます。

- **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、POSIX時間、またはUnixタイムスタンプ）とは、January 1, 1970（UTC/GMTの深夜）から経過した秒数です。この時間には閏秒は含まれません（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。プロファイル作成時に暗号化を強制するには**false**に設定します。

典型的なJSONは次のようになります。

典型的なJSONの画像(/en-us/xenmobile/server/media/afw-qr-code-json.png)

作成されたJSONは、https://jsonlint.comなどのJSON検証ツールを使用して検証します。そのJSON文字列を、https://goqr.meなどのオンラインQRコードジェネレーターを使用してQRコードに変換します。

このQRコードは、工場出荷時設定にリセットされたデバイスによってスキャンされ、デバイスをワークマネージドデバイスモードに登録します。

デバイスを登録するには

デバイスを完全管理デバイスとして登録するには、デバイスが工場出荷時設定にリセットされた状態である必要があります。

1. ウェルカム画面で画面を6回タップして、QRコード登録フローを起動します。
2. プロンプトが表示されたら、Wi-Fiに接続します。QRコード（JSONにエンコードされている）内のSecure Hubのダウンロード場所は、このWi-Fiネットワーク経由でアクセスできます。

   デバイスがWi-Fiに正常に接続すると、GoogleからQRコードリーダーをダウンロードし、カメラを起動します。
3. カメラをQRコードに向けてコードをスキャンします。

   Androidは、QRコード内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をインストールして、デバイス所有者として設定します。

詳細については、Android EMM開発者向けのGoogleガイドを参照してください: `<https://developers.google.com/android/work/prov-devices#qr_code_method>`。

NFCバンプ

NFCバンプを使用してデバイスを完全管理デバイスとして登録するには、2つのデバイスが必要です。1つは工場出荷時設定にリセットされたデバイス、もう1つはXenMobile Provisioning Toolを実行しているデバイスです。

前提条件:

- Android 5.0、Android 5.1、Android 6.0以降を実行しているすべてのAndroidデバイスでサポートされています。
- Android Enterpriseが有効になっているXenMobile Serverバージョン10.4。
- Android Enterprise向けに完全に管理されたデバイスとして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ための手順は、この記事の後半で確認できます。
- 構成済みのプロビジョニングツールを実行している、NFC対応の別のデバイス。プロビジョニングツールは、Secure Hub 10.4またはCitrixダウンロードページで入手できます。

各デバイスには、エンタープライズモビリティ管理（EMM）アプリによって管理されるAndroid Enterpriseプロファイルを1つだけ持つことができます。XenMobileでは、Secure HubがEMMアプリです。各デバイスで許可されるプロファイルは1つだけです。2つ目のEMMアプリを追加しようとすると、最初の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、Android Enterpriseを初期化するために、NFCバンプを介して次のデータを送信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のパッケージ名（この場合はSecure Hub）。
- 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/インターネットの場所。
- ダウンロードが成功したかどうかを確認するためのEMMプロバイダーアプリのSHA1ハッシュ。
- 工場出荷時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ためのWi-Fi接続の詳細。注：Androidは現在、この手順で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）。
- デバイスの地理的位置（オプション）。

2つのデバイスがバンプされると、プロビジョニングツールからのデータが工場出荷時設定にリセットされたデバイスに送信されます。そのデータは、管理者設定でSecure Hubをダウンロードするために使用されます。タイムゾーンと場所の値を入力しない場合、Androidは新しいデバイスで値を自動的に構成します。

XENMOBILEプロビジョニングツールの構成

NFCバンプを行う前に、プロビジョニングツールを構成する必要があります。この構成は、NFCバンプ中に工場出荷時設定にリセットされたデバイスに転送されます。

プロビジョニングツールの構成の画像(/en-us/xenmobile/server/media/nfc-provisioning-secure-hub.png)

必要なフィールドにデータを入力するか、テキストファイルを通じてデータを入力できます。次の手順では、テキストファイルの構成方法と各フィールドの説明について説明します。アプリは入力後に情報を保存しないため、将来の使用のために情報を保持するためにテキストファイルを作成することをお勧めします。
テキストファイルを使用してプロビジョニングツールを構成するには
ファイルをnfcprovisioning.txtという名前にし、デバイスのSDカードの/sdcard/フォルダーに配置します。そうすると、アプリはテキストファイルを読み取り、値を入力できます。

テキストファイルには次のデータが必要です。

```
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/インターネット上の場所です。NFCバンプ後に工場出荷時設定にリセットされたデバイスがWi-Fiに接続した後、ダウンロードのためにこの

場所にアクセスできる必要があります。URLは通常のURLであり、特別な書式設定は必要ありません。

`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ことを確認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、この記事の後半で説明します。

`android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>`

この行は、プロビジョニングツールが実行されているデバイスの接続済みWi-Fi SSIDです。

`android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>`

サポートされている値はWEPと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である必要があります。

`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2文字の小文字の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2文字の大文字のISO国コード（USなど）です。たとえば、米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ているタイムゾーン。Olson name of the form area/locationの形式で入力します。たとえば、太平洋時間の場合は「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ているため、必須ではありません。ここでは、完全を期すためにのみ記載しています。

WPA2を使用して保護されたWi-Fiがある場合、完成したnfcprovisioning.txtファイルは次のようになります。

```
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=ga50TwdCmfdJ72LGRFkke4CrbAk\u
```

```
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がある場合、完成したnfcprovisioning.txtファイルは次のようになります。

```
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=ga50TwdCmfdJ72LGRFkke4CrbAk\u
```

```
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のチェックサムを取得するには

任意の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、**Configure > Apps** に移動し、**Add** をクリックします。

   Add Apps ウィンドウが表示されます。
2. **Enterprise** をクリックします。

   App information ページが表示されます。

   App Informationページの画像(/en-us/xenmobile/server/media/nfc-provisioning-add-app-enterprise.png)
3. 次の構成を選択し、**Next** をクリックします。

   Android Enterprise Enterprise App ページが表示されます。

Android Enterpriseアプリの画像(/en-us/xenmobile/server/media/configure-apps-android-for-work-1.png)

4. .apkへのパスを指定し、**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。

   ファイルアップロードページの画像(/en-us/xenmobile/server/media/configure-apps-android-for-work-2.png)

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開きます。このファイルはGoogle Playにアップロードするために使用します。Secure Hubの場合、Google Playへのアップロードは不要ですが、JSONファイルからSHA1値を読み取る必要があります。

   JSONファイルダウンロードページの画像(/en-us/xenmobile/server/media/nfc-provisioning-android-for-work-json.png)

   一般的なJSONファイルは次のようになります。

   一般的なJSONファイルの画像(/en-us/xenmobile/server/media/nfc-provisioning-typical-json-file.png)

6. **file_sha1_base64値**をコピーし、プロビジョニングツールの**Hash**フィールドで使用します。

   > **注：**
   >
   > ハッシュはURLセーフである必要があります。

   - **+**記号を**-**に変換します
   - **/**記号を**_**に変換します
   - 末尾の**\\u003d**を**=**に置き換えます

   ハッシュをデバイスのSDカードにあるnfcprovisioning.txtファイルに保存すると、アプリが安全変換を行います。ただし、ハッシュを手動で入力することを選択した場合、そのURLの安全性を確保するのはお客様の責任です。

使用されているライブラリ

プロビジョニングツールは、そのソースコードで以下のライブラリを使用しています。

- GoogleによるApache License 2.0のv7 appcompatライブラリ、Design supportライブラリ、およびv7 Paletteライブラリ

詳細については、「Support Library Features Guide」を参照してください。

- Butter Knife、Jake Wharton作、Apache License 2.0ライセンスのもとで

Android Enterpriseでのワークプロファイルデバイスのプロビジョニング

Android Enterpriseのワークプロファイルデバイスでは、デバイス上の企業領域と個人領域を安全に分離します。たとえば、BYODデバイスはワークプロファイルデバイスにすることができます。ワークプロファイルデバイスの登録エクスペリエンスは、XenMobileでのAndroid登録と似ています。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。

デフォルトでは、Android Enterpriseにワークプロファイルデバイスとして登録されているデバイスでは、USBデバッグと不明なソースの設定は無効になっています。

ヒント:

Android Enterpriseにワークプロファイルデバイスとしてデバイスを登録する際は、常にGoogle Playにアクセスしてください。そこから、Secure Hubがユーザーの個人プロファイルに表示されるように有効にします。

マネージド構成フィードバックのサポート (テクニカルプレビュー)

注:

テクニカルプレビューの機能は、非本番環境または限定的な本番環境で使用でき、お客様にフィードバックを共有する機会を提供します。Citrix® は、テクニカルプレビューの機能に関するサポートケースを受け付けていませんが、それらの改善のためのフィードバックを歓迎します。この機能に関するフィードバックは、 をクリックして提供できます。Citrix は、フィードバックの重大度、重要度、および優先度に基づいて対応する場合があります。

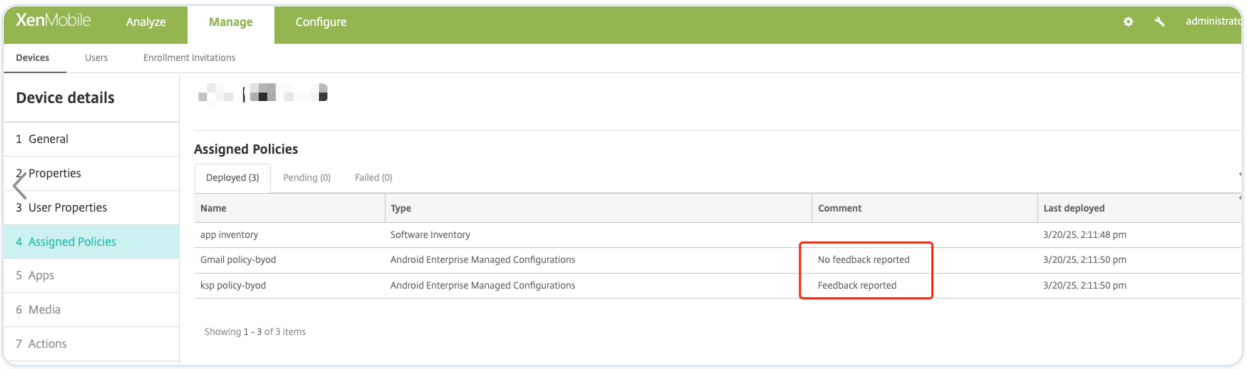
マネージド構成フィードバック機能を使用すると、管理者はマネージド構成ポリシーで構成された Android デバイスからアプリの状態に関するフィードバックを取得できます。このフィードバックは、これらのポリシーの有効性とステータスを監視するために使用できます。

前提条件

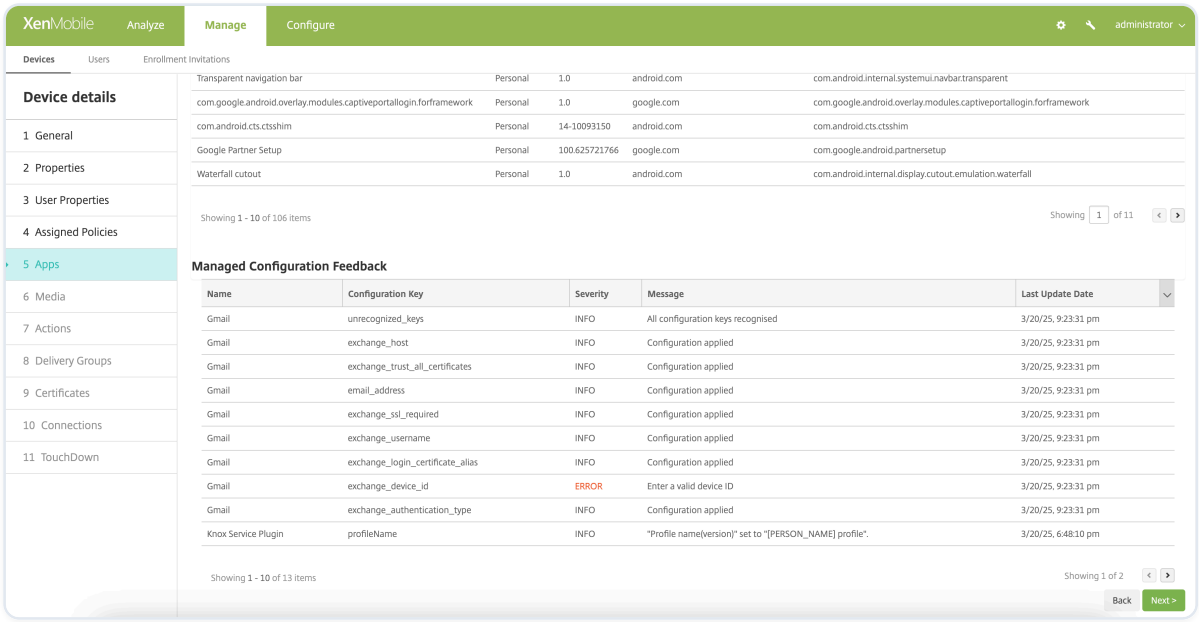
1. `App Support`: アプリケーションはマネージド構成ポリシーをサポートしている必要があります。
2. `Keyed App States`: アプリはキー付きアプリの状態もサポートしている必要があります。アプリのフィードバックがどのように機能するかについての詳細は、「EMM にアプリのフィードバックを送信する」を参照してください。

構成フィードバックを管理および利用する手順

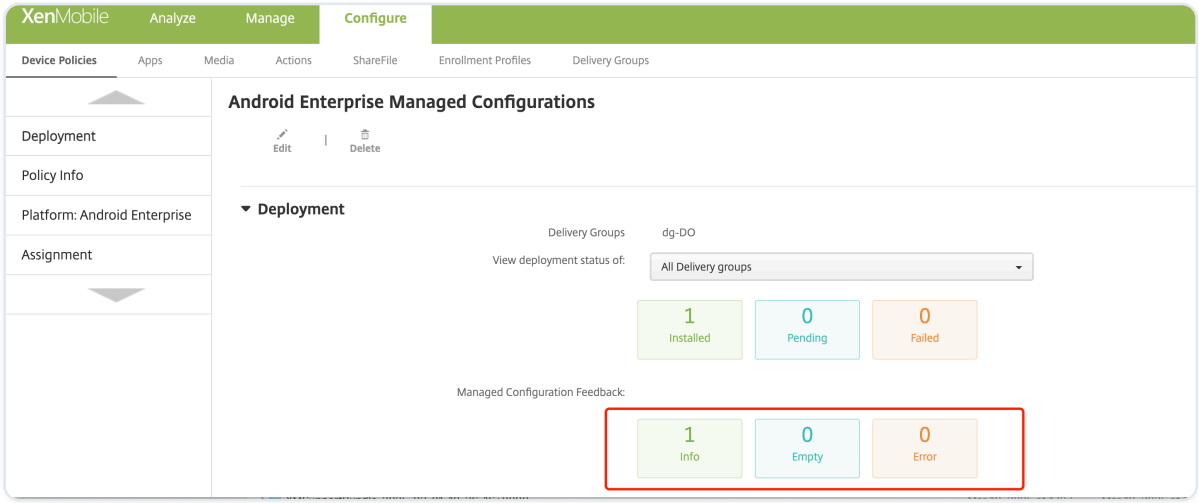
1. 指定された XenMobile Server のサーバープロパティ `afw.app_managed_configurations.feedback` を有効にします。
2. マネージド構成ポリシーを確認します。
   - Android デバイスが登録されており、マネージド構成ポリシーが正常に適用されていることを確認します。
   - に移動し、 をクリックします。マネージド構成ポリシーに関連するコメントが表示されます。
     - **フィードバックが報告されました**: このポリシー関連アプリにフィードバックが利用可能であることを示します。
     - **フィードバックは報告されていません**: このポリシー関連アプリにフィードバックが報告されていないことを示します。



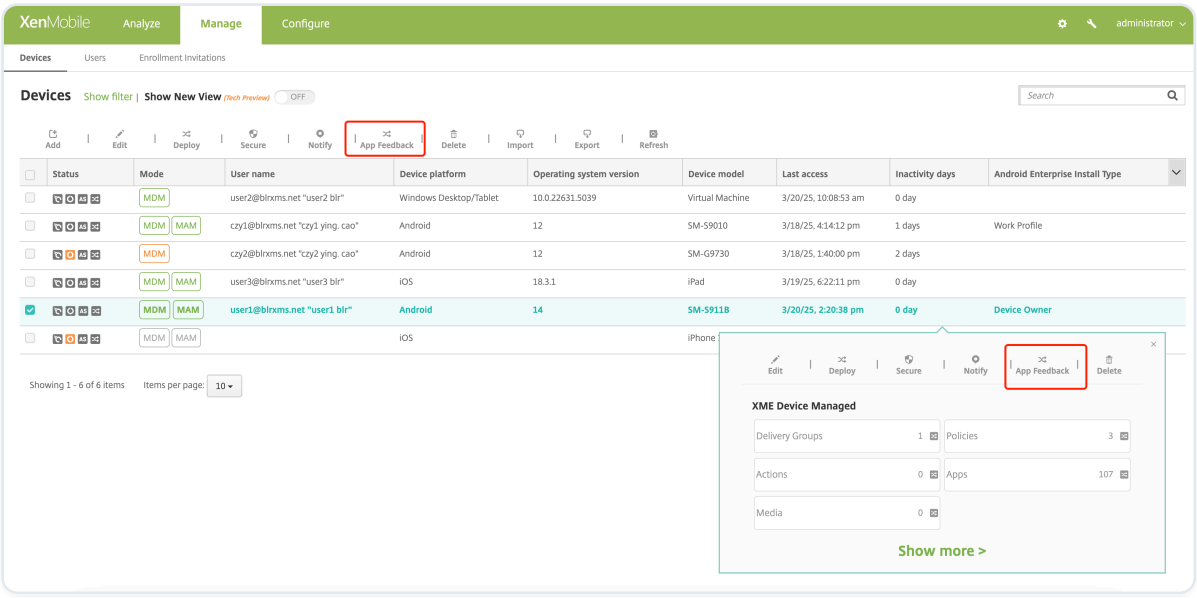
   - 「**デバイスの詳細**」に移動し、「**アプリ**」をクリックします。詳細なフィードバックは、すべてのアプリデータを含む「**管理対象構成フィードバック**」テーブルの下に表示されます。



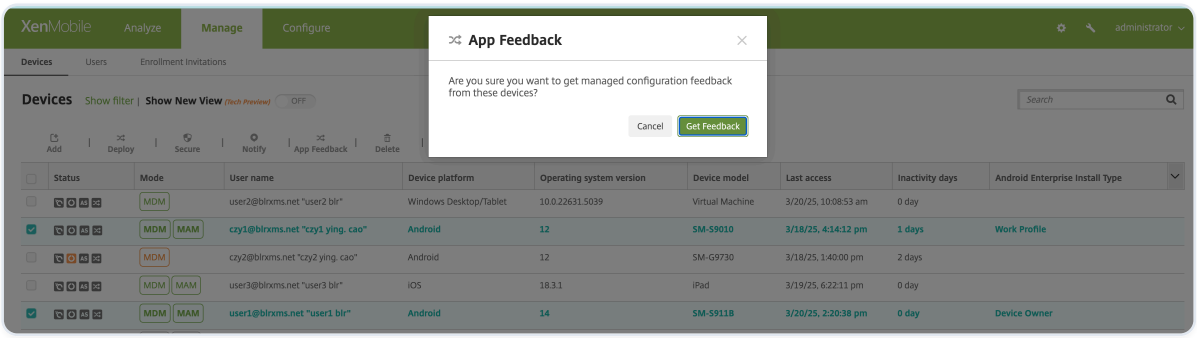
- 単一の管理対象構成ポリシーの場合、割り当てられたすべてのデバイスのフィードバックの詳細を確認できます。
  - **情報**: エラーを含まないフィードバックデータが報告されたすべてのデバイス。
  - **エラー**: エラーを含むフィードバックデータが報告されたすべてのデバイス。
  - **空**: フィードバックデータが報告されていないすべてのデバイス。



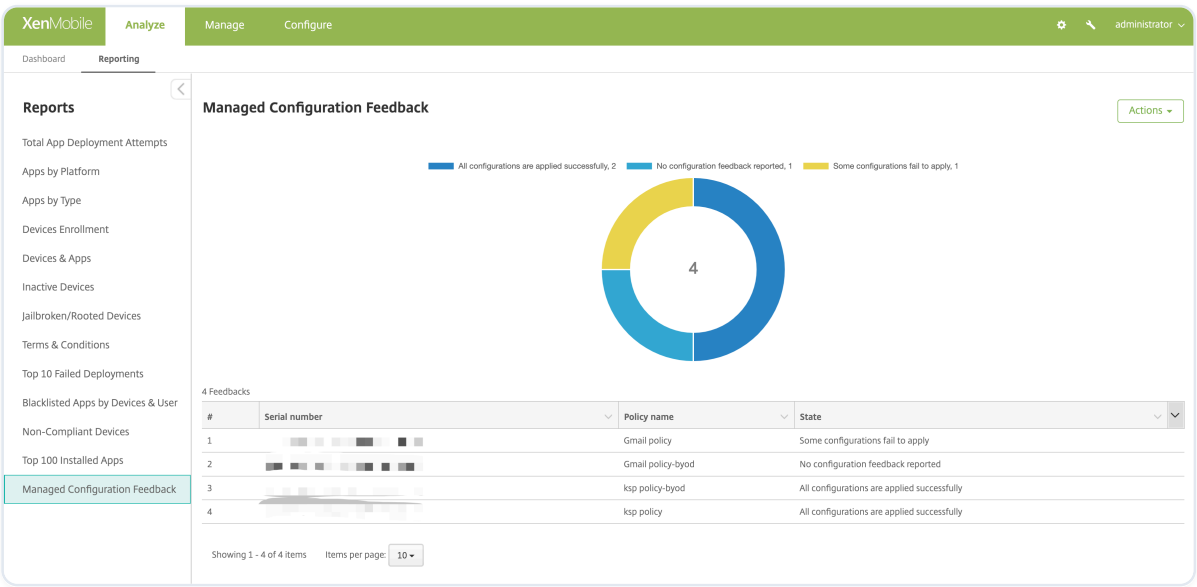
- フィードバックを手動で取得するには、「**管理**」をクリックし、対応するデバイスを見つけるためのチェックボックスを選択します。たとえば、対応するチェックボックスを選択し、「**アプリフィードバック**」をクリックします。



- 「**フィードバックを取得**」をクリックして、選択したデバイスから管理対象構成フィードバックを取得します。



- 管理対象構成フィードバックレポートから、「**分析**」を選択し、「**レポート**」をクリックして全体的なフィードバックを取得します。すべてのデバイス、構成ポリシーの管理、および関連する構成障害に関するレポートを確認できます。



3. フィードバックのスケジュールを調整するために、2つのサーバープロパティが導入されました。サーバープロパティを使用してコンソールで値を変更し、フィードバックデータがデータベースに保存されるタイミングを制御します。

   a. Android Enterprise管理対象構成フィードバックデータベースを更新するバッチサイズ:

      - キー: `android.managed.configuration.feedback.db.update.batch.size`
      - レポートをDBに保存するバッチサイズを定義できます。DBに保存されたデータのみがUIに表示されます。デフォルト値は100で、最大値は1000です。

   b. Android Enterprise マネージド構成フィードバック DB更新時間間隔:

      - キー: `android.managed.configuration.feedback.db.update.time.interval`
      - サイズがバッチ制限に達しない場合でも、レポートがデータベースに保存される期間を指定できます。デフォルト値は6時間です。

トラブルシューティング

デフォルトでは、フィードバックレポートは各デバイスのチェックイン時（Secure Hubがサーバーに接続するとき）に取得されます。ただし、「アプリフィードバック」ボタンを使用して、特定のデバイスのレポートを手動で取得できます。

iOS

XenMobile ServerでiOSデバイスを管理するには、AppleからApple Push Notificationサービス (APNs) 証明書を設定します。詳しくは、APNs証明書を参照してください。

登録プロファイルは、iOSデバイスがMDM+MAMに登録するかどうかを決定し、ユーザーがMDMからオプトアウトするオプションを提供します。XenMobile Serverは、MDM+MAMにおけるiOSデバイスに対して、以下の認証タイプをサポートしています。詳しくは、証明書と認証の項目を参照してください。

- ドメイン
- ドメインと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とドメイン

> **iOS 13における信頼された証明書の要件:**

> AppleはTLSサーバー証明書に関する新しい要件を設けています。すべての証明書がAppleの新しい要件に準拠していることを確認してください。Appleの公開情報 `<https://support.apple.com/ja-jp/HT210176>` を参照してください。証明書の管理については、XenMobile Serverでの証明書のアップロードを参照してください。

> 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、サポートされてい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。

iOS 14の互換性

XenMobile® ServerおよびCitrix®モバイルアプリはiOS 14と互換性がありますが、現在、新しいiOS 14の機能はサポートしていません。

監視対象のiOSデバイスでは、ソフトウェアアップグレードを最大90日間遅延させることができます。iOSの制限デバイスポリシーで、以下の設定を使用します。

- **ソフトウェアアップデートの遅延を強制する**
- **強制的なソフトウェアアップデートの遅延**

「iOS設定」(/ja-jp/xenmobile/server/policies/restrictions-policy.html#ios-settings)を参照してください。これらの設定は、ユーザー登録モードまたは非監視（完全MDM）モードのデバイスでは利用できません。

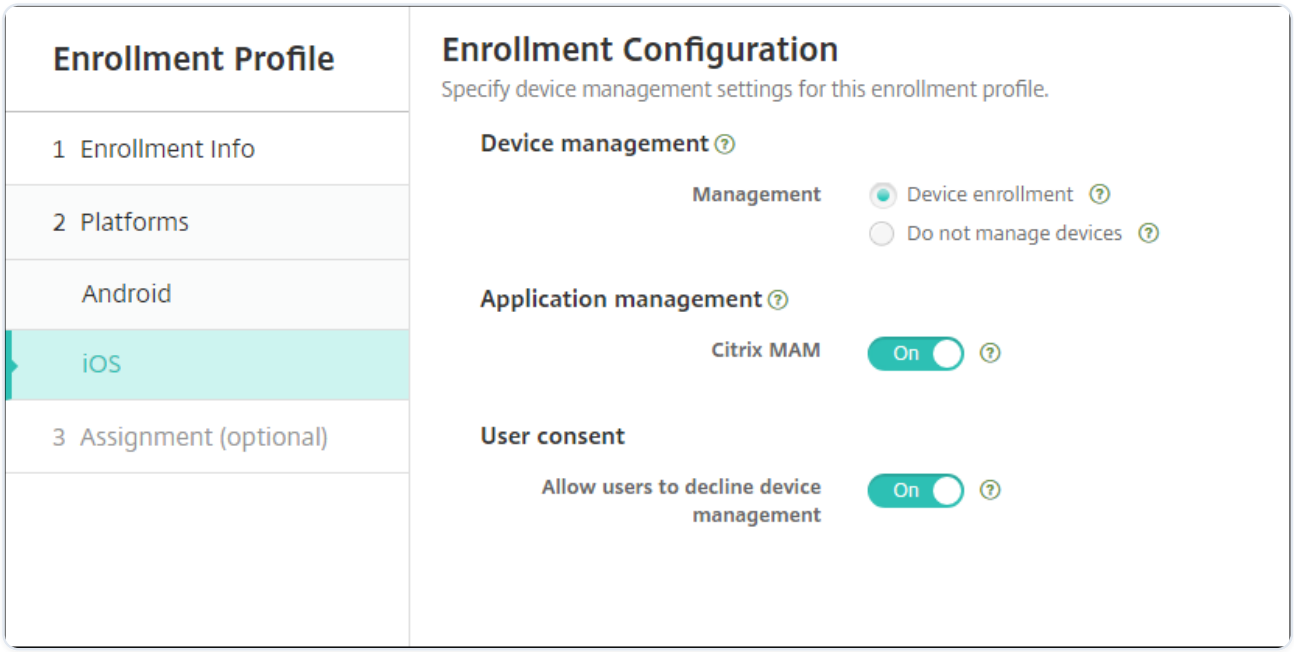
開放しておく必要があるAppleホスト名

iOS、macOS、およびApple App Storeが適切に動作するように、一部のAppleホスト名を開放しておく必要があります。これらのホスト名をブロックすると、iOS、iOSアプリ、MDMの操作、デバイスおよびアプリの登録のインストール、更新、および適切な動作に影響を与える可能性があります。詳細については、`<https://support.apple.com/ja-jp/HT201999>`を参照してください。

サポートされている登録方法

登録プロファイルでiOSデバイスの管理方法を指定します。デバイス登録またはMDM登録なしを選択できます。

iOSデバイスの登録設定を構成するには、**構成 > 登録プロファイル > iOS**に移動します。



次の表に、XenMobile ServerがiOSデバイスでサポートする登録方法を示します。

方法	サポート
Apple展開プログラム	はい
アップル スクール マネージャー	はい
アップルコンフィギュレータ	はい
手動登録	はい
登録招待	はい

Appleは、ビジネスおよび教育アカウント向けのデバイス登録プログラムを提供しています。ビジネスアカウントの場合、XenMobile Serverでのデバイス登録と管理にApple Deployment Programを使用するために、Apple Deployment Programに登録します。このプログラムは、iOSおよびmacOSデバイス用です。Apple Deployment Programを介したデバイスの展開を参照してください。

教育アカウントの場合、Apple School Managerアカウントを作成します。Apple School Managerは、Deployment Programとボリューム購入を統合します。Apple School Managerは、教育機関向けのApple Deployment Programの一種です。Apple Education機能との統合を参照してください。

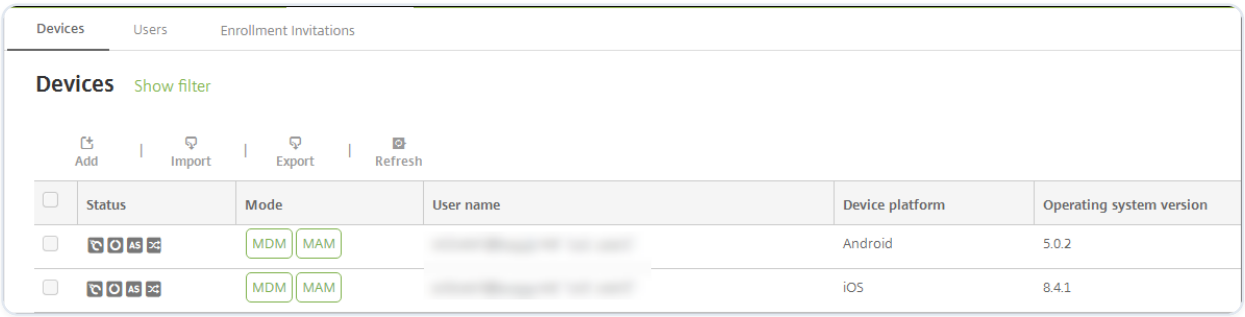
Apple Deployment Programを使用して、iOSおよびmacOSデバイスを一括登録できます。これらのデバイスは、Apple、参加しているApple正規販売店、または通信事業者から直接購入できま

す。iOSデバイスをAppleから直接購入するかどうかにかかわらず、Apple Configuratorを使用してこれらのデバイスを登録できます。Appleデバイスの一括登録を参照してください。

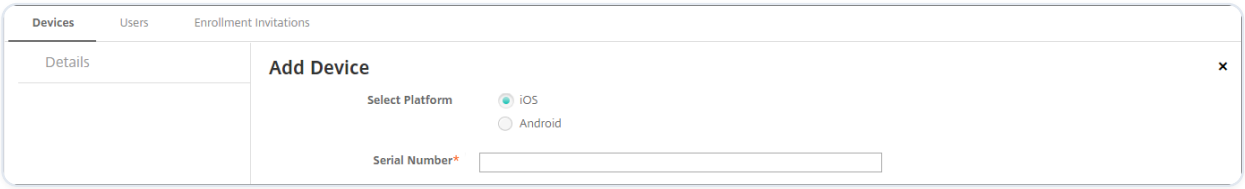
iOSデバイスを手動で追加する

テスト目的などでiOSデバイスを手動で追加する場合は、次の手順に従います。

1. XenMobile Serverコンソールで、 > の順にクリックします。 ページが表示されます。



2. をクリックします。 ページが表示されます。



3. 次の設定を構成します。

   - **プラットフォームの選択:** 「**iOS**」をクリックします。
   - **シリアル番号:** デバイスのシリアル番号を入力します。

4. 「**追加**」をクリックします。**デバイス**テーブルが表示され、リストの一番下にデバイスが追加されます。デバイスの詳細を表示して確認するには、追加したデバイスを選択し、表示されるメニューで「**編集**」をクリックします。

> **注:**
>
> デバイスの横にあるチェックボックスを選択すると、デバイスリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

   - LDAPが構成済み
   - ローカルグループとローカルユーザーを使用している場合:

- 1つ以上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に関連付けられています。

- Active Directoryを使用している場合:
  - デリバリーグループはActive Directoryグループに関連付けられています。

デバイスの詳細リスト(/en-us/xenmobile/server/media/manage-devices-details-general.png)

5. 「**全般**」ページには、シリアル番号やプラットフォームタイプに関するその他の情報など、デバイスの**識別子**が一覧表示されます。「**デバイスの所有権**」には、「**企業**」または「**BYOD**」を選択します。

   「**全般**」ページには、強力なID、デバイスのロック、アクティベーションロックのバイパスなど、デバイスの**セキュリティ**プロパティやプラットフォームタイプに関するその他の情報も一覧表示されます。「**デバイスの完全ワイプ**」フィールドには、ユーザーのPINコードが含まれています。ユーザーはデバイスがワイプされた後、そ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、ここで調べることができます。

6. 「**プロパティ**」ページには、XenMobile Serverがプロビジョニングするデバイスプロパティが一覧表示されます。このリストには、デバイスの追加に使用されたプロビジョニングファイルに含まれるすべてのデバイスプロパティが表示されます。プロパティを追加するには、「**追加**」をクリックし、リスト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ついては、PDF「デバイスプロパティ名と値」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の下に表示されます。「**次へ**」をクリックして「**プロパティ**」ページに戻ると、そのプロパティは適切なリストに表示されます。

   プロパティを削除するには、リストにカーソルを合わせ、右側の「**X**」をクリックします。XenMobile Serverはすぐにその項目を削除します。

7. 残りの「**デバイスの詳細**」セクションには、デバイスの概要情報が表示されます。

   - **ユーザープロパティ:** RBACロール、グループメンバーシップ、ボリューム購入アカウント、およびユーザーのプロパティを表示します。このページからボリューム購入アカウントを廃止できます。
   - **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を表示します。各ポリシーのポリシー名、種類、および最終展開情報を提供します。

- **アプリ:** 最後のインベントリについて、インストール済み、保留中、失敗したアプリ展開の数を表示します。アプリ名、識別子、種類、およびその他の情報を提供します。**HasUpdateAvailable**などのiOSおよびmacOSインベントリキーの説明については、「モバイルデバイス管理 (MDM) プロトコル」を参照してください。
- **メディア:** 最後のインベントリについて、展開済み、保留中、失敗したメディア展開の数を表示します。
- **アクション:** 展開済み、保留中、失敗したアクションの数を表示します。アクション名と最終展開時刻を提供します。
- **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を表示します。各展開について、デリバリーグループ名と展開時刻を提供します。デリバリーグループを選択すると、ステータス、アクション、チャネルまたはユーザーを含む詳細情報が表示されます。
- **iOSプロファイル:** 名前、種類、組織、説明を含む、最後のiOSプロファイルインベントリを表示します。
- **iOSプロビジョニングプロファイル:** UUID、有効期限、管理ステータスなどのエンタープライズ配布プロビジョニングプロファイル情報を表示します。
- **証明書:** 有効、期限切れ、または失効した証明書について、種類、プロバイダー、発行者、シリアル番号、有効期限までの残り日数などの情報を表示します。
- **接続:** 最初の接続ステータスと最後の接続ステータスを表示します。各接続について、ユーザー名、最後から2番目の認証時刻、および最終認証時刻を提供します。
- **MDMステータス:** MDMステータス、最終プッシュ時刻、最終デバイス応答時刻などの情報を表示します。

iOSデバイスポリシーを構成する

これらのポリシーを使用して、XenMobile ServerがiOSを実行しているデバイスとどのようにやり取りするかを構成します。この表は、iOSデバイスで利用可能なすべてのデバイスポリシーを一覧表示します。

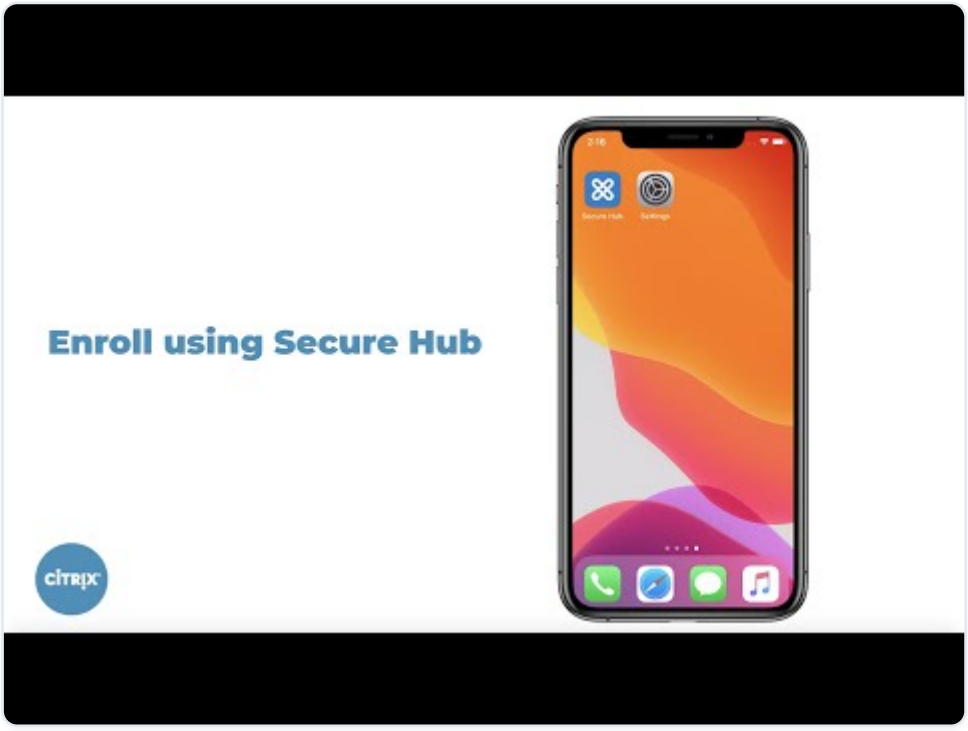
AirPlayミラーリング	AirPrint	APN
アプリのアクセス	アプリの属性	アプリの構成
アプリのインベントリ	アプリのロック	アプリのネットワーク使用状況

アプリのアンインストール	アプリの通知	カレンダー (CalDAV)
モバイルデータ通信	連絡先 (CardDAV)(/ja-jp/xenmobile/server/policies/contacts-carddav-ios-policy.html)	OSアップデートの制御(/ja-jp/xenmobile/server/policies/control-os-updates.html#ios-settings)
資格情報(/ja-jp/xenmobile/server/policies/credentials-policy.html#ios-settings)	デバイス名(/ja-jp/xenmobile/server/policies/device-name-policy.html)	教育構成(/ja-jp/xenmobile/server/policies/education-configuration-policy.html)
エクスチェンジ	フォント(/ja-jp/xenmobile/server/policies/font-policy.html)	ホーム画面のレイアウト(/ja-jp/xenmobile/server/policies/home-screen-layout-policy.html)
iOSおよびmacOSプロファイルのインポート(/ja-jp/xenmobile/server/policies/import-ios-mac-os-x-profile-policy.html)	LDAP(/ja-jp/xenmobile/server/policies/ldap-policy.html)	場所(/ja-jp/xenmobile/server/policies/location-policy.html)
メール(/ja-jp/xenmobile/server/policies/mail-policy.html)	管理対象ドメイン(/ja-jp/xenmobile/server/policies/managed-domains-policy.html)	MDMオプション(/ja-jp/xenmobile/server/policies/mdm-options-policy.html)
組織情報(/ja-jp/xenmobile/server/policies/organization-info-policy.html)	パスコード(/ja-jp/xenmobile/server/policies/passcode-policy.html#ios-settings)	インターネット共有(/ja-jp/xenmobile/server/policies/personal-hotspot-policy.html)
プロファイルの削除(/ja-jp/xenmobile/server/policies/profile-removal-policy.html)	プロビジョニングプロファイル(/ja-jp/xenmobile/server/policies/provisioning-profile-policy.html)	プロビジョニングプロファイルの削除(/ja-jp/xenmobile/server/policies/provisioning-profile-removal-policy.html)
プロキシ(/ja-jp/xenmobile/server/policies/proxy-policy.html)	機能制限(/ja-jp/xenmobile/server/policies/restrictions-policy.html#ios-settings)	ローミング(/ja-jp/xenmobile/server/policies/roaming-policy.html)

SCEP(/ja-jp/xenmobile/server/policies/scep-policy.html)	共有iPad - 最大常駐ユーザー数(/ja-jp/xenmobile/server/provision-devices/integrate-with-apple-education.html#configure-shared-ipads)	共有iPad - パスコードロック猶予期間(/ja-jp/xenmobile/server/provision-devices/integrate-with-apple-education.html#configure-shared-ipads)
SSOアカウント(/ja-jp/xenmobile/server/policies/sso-account-policy.html)	ストア(/ja-jp/xenmobile/server/policies/store-policy.html)	登録済みカレンダー(/ja-jp/xenmobile/server/policies/subscribed-calendars-policy.html)
利用規約(/ja-jp/xenmobile/server/policies/terms-and-conditions-policy.html)	VPN	壁紙
Webコンテンツフィルター	ウェブクリップ	ワイファイ

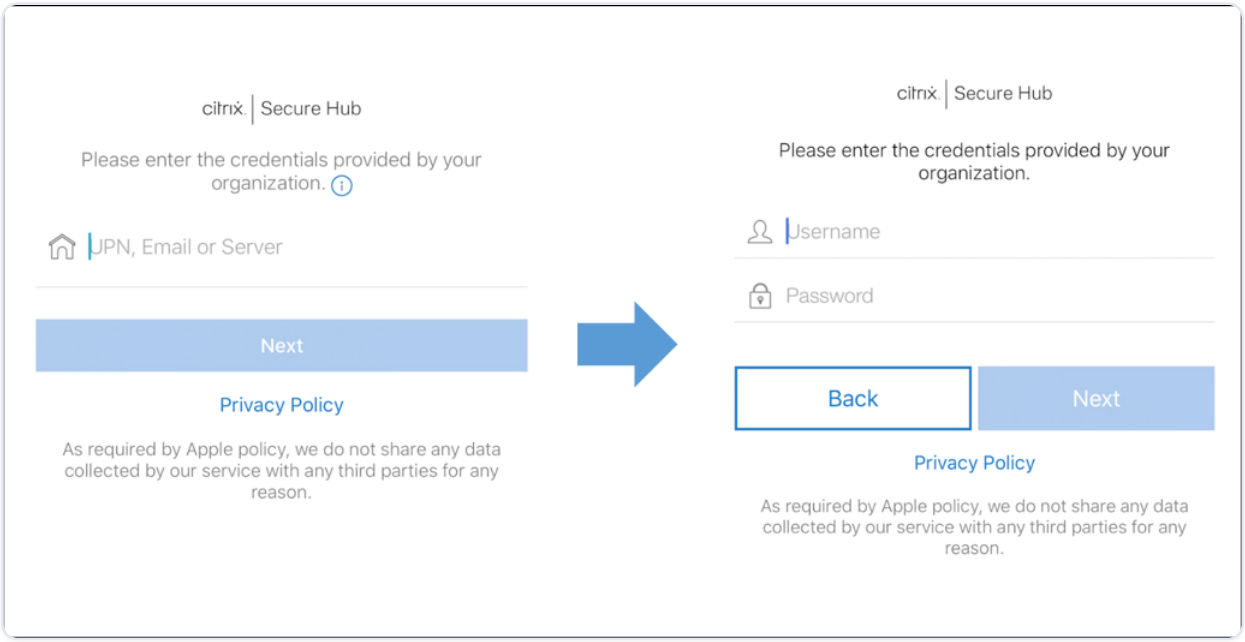
iOSデバイスを登録する

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に登録する方法を示します。iOS登録の詳細については、次のビデオを開いてください。

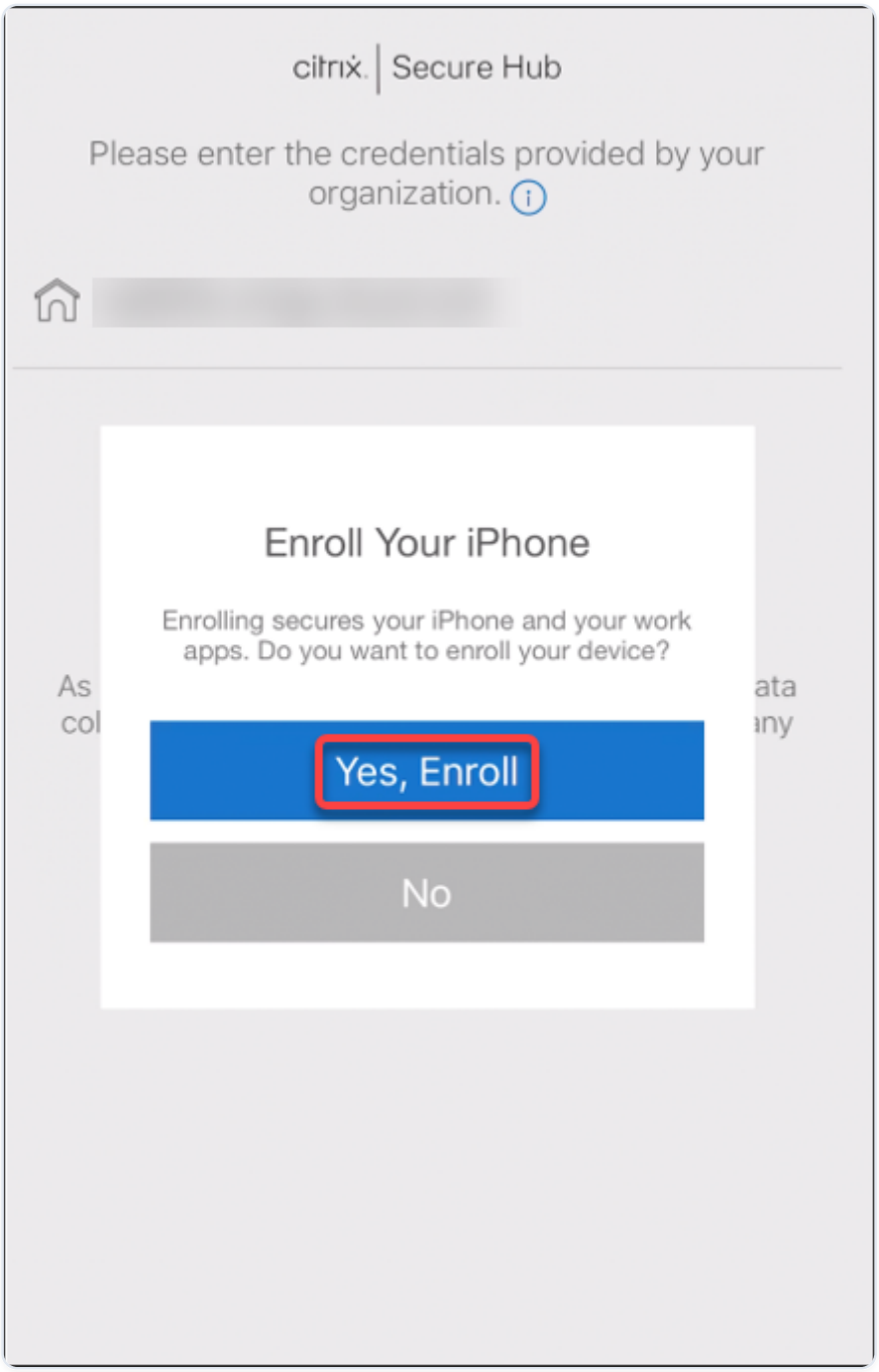


1. iOSデバイスでApple Storeにアクセスし、Citrix Secure Hub™アプリをダウンロードして、アプリをタップします。

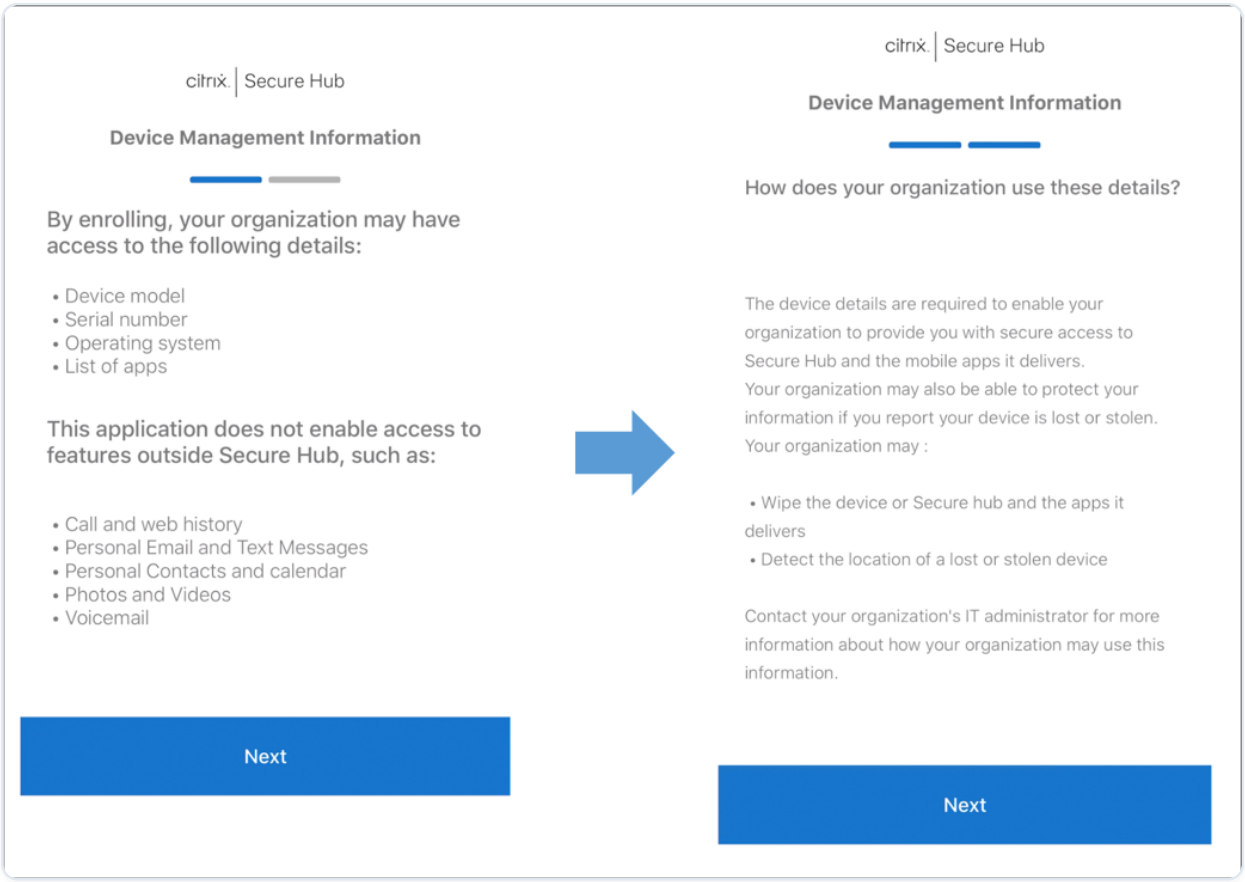
2. アプリのインストールを求められたら、**次へ**をタップし、次に**インストール**をタップします。
3. Secure Hubのインストール後、**開く**をタップします。
4. XenMobile Serverのサーバー名、ユーザープリンシパル名（UPN）、またはメールアドレスなどの企業資格情報を入力します。次に、**次へ**をクリックします。



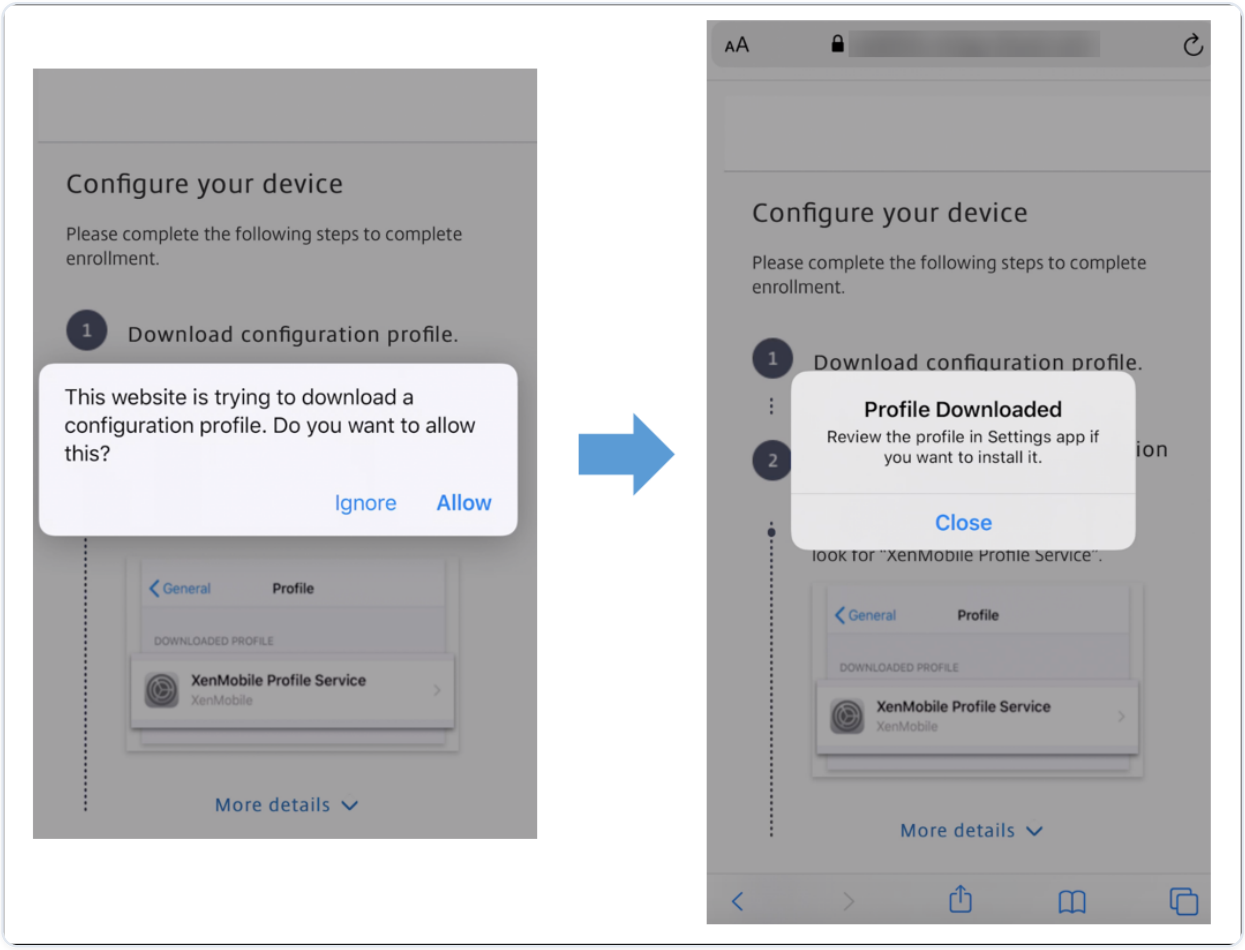
5. iOSデバイスを登録するには、**はい、登録**をタップします。



6. XenMobile Serverが収集するデータの一覧が表示されます。**次へ**をクリックします。組織がそのデータをどのように使用するかについての説明が表示されます。**次へ**をクリックします。



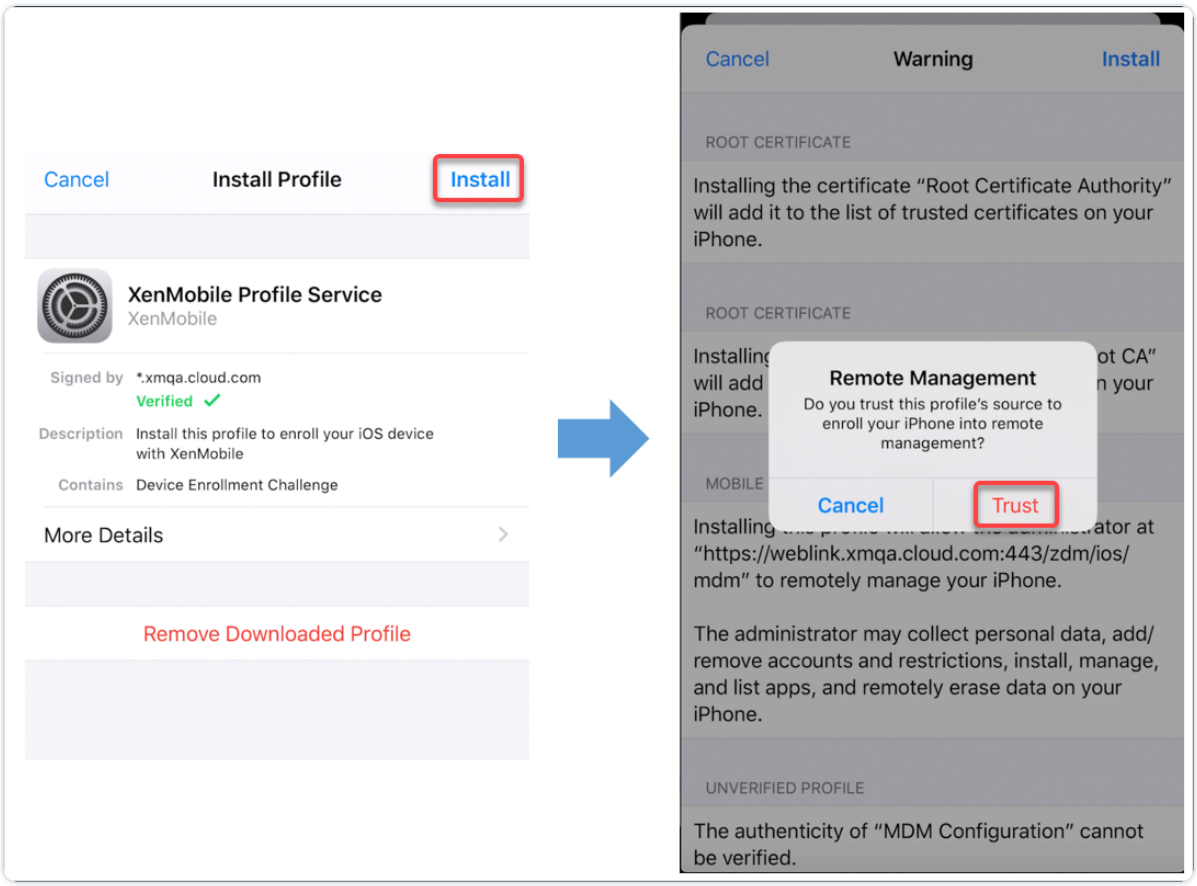
7. 資格情報を入力した後、プロンプトが表示されたら**許可**をタップして構成プロファイルをダウンロードします。構成プロファイルのダウンロード後、**閉じる**をタップします。



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リストに追加します。

   - **設定 > 一般 > 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**」をタップしてデバイスをリモート管理に登録します。



9. 登録が成功したら、Secure Hubを開きます。MDM+MAMに登録する場合：資格情報が検証された後、プロンプトが表示されたらCitrix PINを作成して確認します。
10. ワークフローが完了すると、デバイスは登録されます。その後、App Storeにアクセスして、iOSデバイスにインストールできるアプリを表示できます。

セキュリティアクション

iOSは以下のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、セキュリティアクションを参照してください。

アクティベーションロックバイパス	アプリロック	アプリワイプ
ASMアクティベーションロック	証明書の更新	制限のクリア
紛失モードの有効化/無効化	追跡の有効化/無効化	完全ワイプ
検索	ロック	着信音を鳴らす

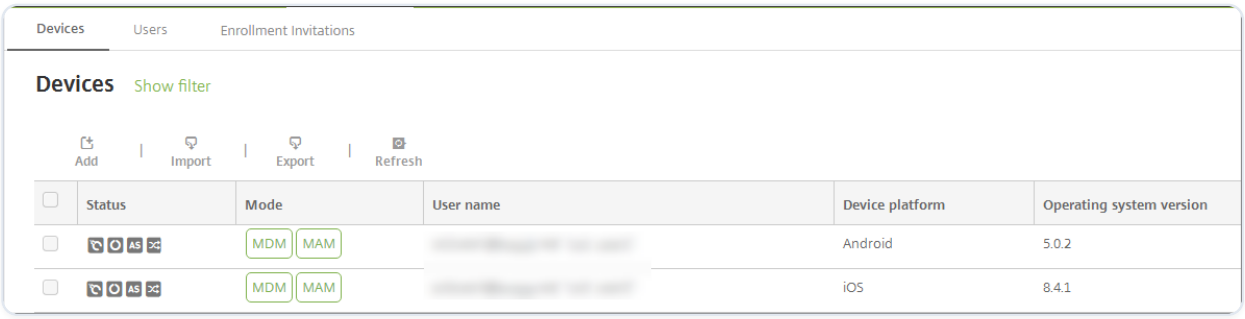
AirPlayミラーリングの要求/停止	再起動/シャットダウン	取り消し/承認
選択的ワイプ	ロック解除	

iOSデバイスをロックする

紛失した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させることができます。

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、XenMobile Serverコンソールでパスコードポリシーを**true**に設定します。または、ユーザーがデバイスで手動でパスコードを有効にすることもできます。

1. **>** をクリックします。 ページが表示されます。



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選択すると、デバイスリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、リストの右側にオプションメニューが表示されます。

   オプションメニュー(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

   オプションメニュー(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. オプションメニューで、**Secure**をクリックします。**Security Actions**ダイアログボックスが表示されます。

   Security Actionsダイアログボックス(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. **Lock**をクリックします。**Security Actions**確認ダイアログボックスが表示されます。

Security Actionsの確認(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. オプションで、デバイスのロック画面に表示されるメッセージと電話番号を入力します。

   iOSは、**Message**フィールドに入力した内容に「Lost iPad」という単語を追加します。

   Messageフィールドを空のままにして電話番号を入力すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

6. **Lock Device**をクリックします。

iOSデバイスを紛失モードにする

XenMobile Serverの紛失モードデバイスプロパティは、iOSデバイスを紛失モードにします。Apple Managed Lost Modeとは異なり、XenMobile Serverの紛失モードでは、ユーザーがデバイスを特定できるようにするために、次のいずれかのアクションを実行する必要はありません。**iPhone/iPadを探す**設定を構成するか、Citrix Secure Hubのロケーションサービスを有効にするかです。

XenMobile Serverの紛失モードでは、XenMobile Serverのみがデバイスのロックを解除できます。（対照的に、XenMobile Serverのデバイスロック機能を使用する場合、ユーザーは提供されたPINコードを使用してデバイスのロックを直接解除できます。

紛失モードを有効または無効にするには、**Manage > Devices**に移動し、監視対象のiOSデバイスを選択して、**Secure**をクリックします。次に、**Enable Lost Mode**または**Disable Lost Mode**をクリックします。

「紛失モード」のオプション(/en-us/xenmobile/server/media/manage-devices-enable-lost-mode-button.png)

「**紛失モードを有効にする**」をクリックすると、デバイスが紛失モードのときに表示される情報を入力します。

デバイスに表示される情報(/en-us/xenmobile/server/media/enable-lost-mode-dialog.png)

紛失モードのステータスを確認するには、次のいずれかの方法を使用します。

- **セキュリティアクション**ウィンドウで、ボタンが「**紛失モードを無効にする**」に設定されていることを確認します。
- **管理 > デバイス**から、**セキュリティ**の下にある**全般**タブで、最後の「紛失モードを有効にする」または「紛失モードを無効にする」アクションを確認します。

全般タブ(/en-us/xenmobile/server/media/manage-devices-ios-lost-mode.png)

- **管理 > デバイス**から、**プロパティ**タブで、**MDM紛失モードが有効**設定の値が正しいことを確認します。

MDM紛失モードが有効設定(/en-us/xenmobile/server/media/manage-devices-details-properties.png)

iOSデバイスでXenMobile Serverの紛失モードを有効にすると、XenMobile Serverコンソールも次のように変更されます。

- **構成 > アクション**では、**アクション**リストに次の自動アクションは含まれません: **デバイスの取り消し**、**デバイスの選択的ワイプ**、**デバイスの完全ワイプ**。
- **管理 > デバイス**では、**セキュリティアクション**リストに**取り消し**および**選択的ワイプ**デバイスアクションは含まれなくなります。必要に応じて、セキュリティアクションを使用して**完全ワイプ**アクションを実行することは引き続き可能です。

iOSは、**セキュリティアクション**画面の**メッセージ**に入力した内容に「Lost iPad」という単語を追加します。

メッセージを空のままにして電話番号を提供すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

iOSアクティベーションロックをバイパスする

アクティベーションロックは、「iPhone/iPadを探す」の機能であり、紛失または盗難された監視対象デバイスの再アクティベーションを防止します。アクティベーションロックでは、ユーザーのApple IDとパスワードがないと、誰も「iPhone/iPadを探す」をオフにする、デバイスを消去する、またはデバイスを再アクティベートするなどの操作を行うことができません。組織が所有するデバイスの場合、たとえばデバイスをリセットまたは再割り当てするために、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 Server MDMオプションデバイスポリシーを構成して展開します。その後、ユーザーのApple資格情報なしでXenMobile Serverコンソールからデバイスを管理できます。アクティベーションロックのApple資格情報要件をバイパスするには、XenMobile Serverコンソールからアクティベーションロックバイパスセキュリティアクションを発行します。

たとえば、ユーザーが紛失した電話を返却した場合、または完全ワイプの前後にデバイスをセットアップする場合：電話がApple App Storeアカウントの資格情報を要求したときに、XenMobile Serverコンソールからアクティベーションロックバイパスセキュリティアクションを発行することで、その手順をバイパスできます。

アクティベーションロックバイパスのデバイス要件

- Apple ConfiguratorまたはApple Deployment Programによって監視されている
- iCloudアカウントで構成されている
- 「iPhone/iPadを探す」が有効になっている
- XenMobile Serverに登録されている
- アクティベーションロックが有効になっているMDMオプションデバイスポリシーがデバイスに展開されている

デバイスの完全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：

1. > に移動し、デバイスを選択し、 をクリックし、次に をクリックします。
2. デバイスをワイプします。デバイスのセットアップ中にアクティベーションロック画面は表示されません。

デバイスの完全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：

1. デバイスをリセットまたはワイプします。デバイスのセットアップ中にアクティベーションロック画面が表示されます。
2. > に移動し、デバイスを選択し、 をクリックし、次に をクリックします。
3. デバイスの戻るボタンをタップします。ホーム画面が表示されます。

次の点に注意してください。

- ユーザーには、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。デバイスから完全ワイプを実行しないでください。どちらの場合も、ユーザーはiCloudアカウントのパスワードの入力を求められます。アカウントの検証後、すべてのコンテンツと設定を消去しても、ユーザーはiPhone/iPadをアクティベート画面を見ることがありません。
- 生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：完全ワイプ後にiPhone/iPadをアクティベートページをバイパスできない場合でも、XenMobile Server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サポートに直接連絡して、デバイスのブロックを解除できます。
- ハードウェアインベントリ中に、XenMobile Serverはデバイスにアクティベーションロックバイパスコードを照会します。バイパスコードが利用可能な場合、デバイスはそれをXenMobile Serverに送信します。その後、デバイスからバイパスコードを削除するには、XenMobile Serverコンソールからアクティベーションロックバイパスセキュリティアクションを送信します。その時点で、XenMobile ServerとAppleはデバイスのブロックを解除するために必要なバイパスコードを保持しています。

- アクティベーションロックバイパスセキュリティアクションは、Appleサービスの可用性に依存します。アクションが機能しない場合、次のように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を空のままにして、パスワードフィールドにバイパスコードを入力します。バイパスコードを検索するには、**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、**プロパティ**をクリックします。**アクティベーションロックバイパスコード**は**セキュリティ情報**の下にあります。

macOS

XenMobileでmacOSデバイスを管理するには、AppleからApple Push Notification service (APNs)証明書を設定します。詳細については、APNs証明書を参照してください。

XenMobile®はmacOSデバイスをMDMに登録します。XenMobileは、MDMにおけるmacOSデバイスの以下の登録認証タイプをサポートしています。

- ドメイン
- ドメインとワンタイムパスワード
- 招待URLとワンタイムパスワード

> **macOS 15における信頼された証明書の要件:**

> AppleはTLSサーバー証明書に新しい要件を設けています。すべての証明書がAppleの新しい要件に準拠していることを確認してください。Appleの公開情報 `<https://support.apple.com/ja-jp/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。

> macOSデバイス管理を開始するための一般的なワークフローは次のとおりです。

1. macOSデバイスポリシーの構成。
2. macOSデバイスの登録。
3. デバイスおよびアプリのセキュリティアクションを設定します。セキュリティアクションを参照してください。

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、サポートされてい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。

開いたままにする必要があるAppleホスト名

iOS、macOS、およびApple App Storeが適切に動作するように、一部のAppleホスト名は開いたままにする必要があります。これらのホスト名をブロックすると、iOS、iOSアプリ、MDMの動作、デバイスおよびアプリの登録のインストール、更新、および適切な動作に影響を与える可能性があります。詳細については、`<https://support.apple.com/ja-jp/HT201999>`を参照してください。

サポートされている登録方法

次の表に、XenMobileがmacOSデバイスでサポートする登録方法を示します。

方法	サポート
Apple Deployment Program (アップル デプロイメント プログラム)	はい
Apple School Manager (アップル スクール マネージャー)	はい
Apple Configurator (アップル コンフィギュレータ)	いいえ
手動登録	はい
登録招待	はい

Appleは、ビジネスアカウントと教育アカウント向けのデバイス登録プログラムを提供しています。ビジネスアカウントの場合、XenMobileでのデバイス登録と管理にApple Deployment Programを使用するには、Apple Deployment Programに登録します。このプログラムは、iOSおよびmacOSデバイス用です。「Apple Deployment Programによるデバイスの展開」を参照してください。

教育機関向けアカウントの場合、Apple School Managerアカウントを作成します。Apple School Managerは、導入プログラムとボリューム購入を統合します。Apple School Managerは、教育機関向けApple導入プログラムの一種です。「Apple Education機能との統合」(/ja-jp/xenmobile/server/provision-devices/integrate-with-apple-education.html)を参照してください。

Apple Deployment Programを使用して、iOSおよびmacOSデバイスを一括登録できます。これらのデバイスは、Apple、参加しているApple正規販売店、または通信事業者から直接購入できます。

macOSデバイスポリシーの構成

これらのポリシーを使用して、XenMobileがmacOSを実行しているデバイスとどのように連携するかを構成します。この表は、macOSデバイスで利用可能なすべてのデバイスポリシーを一覧表示します。

AirPlayミラーリング	アプリインベントリ	カレンダー (CalDAV)
連絡先 (CardDAV)	OSアップデートの制御	資格情報

ファイアウォール	フォント	iOSおよびmacOSプロファイルのインポート
LDAP	メール	パスコード
プロファイルの削除	制限	SCEP
VPN	Webクリップ	ワイファイ

macOSデバイスの登録

XenMobileは、macOSを実行しているデバイスを登録するための2つの方法を提供します。どちらの方法でも、macOSユーザーはデバイスから直接、ワイヤレスで登録できます。

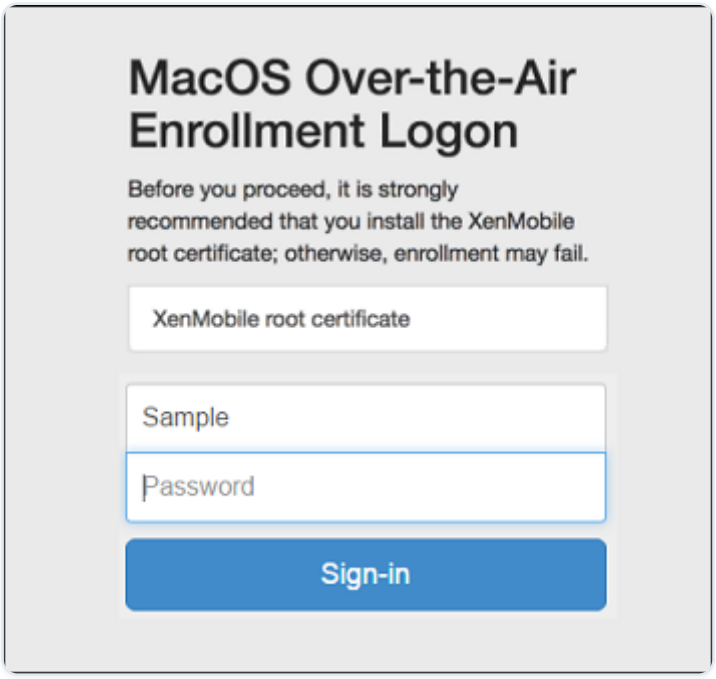
- **ユーザーに登録招待を送信する:** この登録方法では、macOSデバイスに対して以下のいずれかの登録セキュリティモードを設定できます。
  - ユーザー名 + パスワード
  - ユーザー名 + PIN
  - 二要素認証

  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。
- **ユーザーに登録リンクを送信する:** macOSデバイス向けのこの登録方法では、ユーザーに登録リンクが送信され、ユーザーはそれをSafariまたはChromeブラウザで開くことができます。その後、ユーザーはユーザー名とパスワードを入力して登録します。

  macOSデバイスの登録リンクの使用を防止するには、サーバープロパティ **Enable macOS OTAE** を **false** に設定します。その結果、macOSユーザーは登録招待を使用することによってのみ登録できます。

macOSユーザーに登録招待を送信する

1. macOSユーザー登録の招待を追加します。登録招待を作成するを参照してください。
2. ユーザーが招待を受け取り、リンクをクリックすると、Safariブラウザに次の画面が表示されます。XenMobileはユーザー名を入力します。登録セキュリティモードで **Two Factor** を選択した場合、別のフィールドが表示されます。



3. ユーザーは必要に応じて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促すプロンプトが表示されるかどうかは、macOS用に以下を設定したかどうかによって異なります: 公開的に信頼されたSSL証明書と公開的に信頼されたデジタル署名証明書。証明書に関する情報については、証明書と認証を参照してください。
4. ユーザーは要求された資格情報を提供します。

   Mac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macOSデバイスの管理を開始できます。

macOSユーザーにインストールリンクを送信する

1. ユーザーがSafariまたはChromeブラウザで開くことができる登録リンク `https://serverFQDN:8443/instanceName/macos/otae` を送信します。
   - **serverFQDN** は、XenMobileを実行してい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。別のポートを設定した場合は、8443の代わりにそのポートを使用してください。

- **instanceName** は、`zdm` と表示されることが多いですが、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関する詳細については、登録招待の送信 を参照してください。

2. ユーザーは必要に応じて証明書をインストールします。iOS および macOS 用に公開信頼された SSL 証明書とデジタル署名証明書を構成した場合、ユーザーは証明書をインストールするよう促されます。証明書に関する情報については、証明書と認証 を参照してください。
3. ユーザーは Mac にサインオンします。

   Mac 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 macOS デバイスの管理を開始できます。

セキュリティアクション

macOS は次のセキュリティアクションをサポートしています。各セキュリティアクションの説明については、セキュリティアクション を参照してください。

取り消し	ロック	選択的ワイプ
完全ワイプ	証明書の更新	

macOS デバイスのロック

紛失した macOS デバイスをリモートでロックできます。XenMobile はデバイスをロックします。その後、PIN コードを生成し、デバイスに設定します。デバイスにアクセスするには、ユーザーは 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、 を使用します。

PIN コードに関連付けられた追加設定を構成するには、パスコード デバイスポリシーを使用できます。詳細については、macOS 設定 を参照してください。

1. 「**管理 > デバイス**」をクリックします。「**デバイス**」ページが表示されます。

   「デバイスページ」(/en-us/xenmobile/server/media/manage-devices-macos.png)
2. ロックするmacOS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選択すると、デバイスリストの上にオプションメニューが表示されます。リスト内の項目をどこでもクリックすると、リストの右側にオプションメニューが表示されます。

   「オプションメニュー」(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos.png)

「オプションメニュー」(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-macos-2.png)

3. オプションメニューで、「**セキュリティ保護**」をクリックします。「**セキュリティアクション**」ダイアログボックスが表示されます。

   「セキュリティアクション」ダイアログボックス(/en-us/xenmobile/server/media/manage-devices-secure-lock-macos.png)

4. 「**ロック**」をクリックします。「**セキュリティアクション**」確認ダイアログボックスが表示されます。

   「セキュリティアクション」確認(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm-macos.png)

5. 「**デバイスのロック**」をクリックします。

> **重要:**
>
> XenMobileが生成するコードを使用する代わりに、パスコードを指定することもできます。指定されたコードがデバイスまたは既存のワークプロファイルのコード要件を満たしていない場合、ロックアクションは失敗します。

Appleデバイスの一括登録

XenMobile®に多数のiOS、iPadOS、およびmacOSデバイスを登録するには、2つの方法があります。

- Apple Deployment Programを使用して、Appleから直接、または参加しているApple正規販売店や通信事業者から購入したiOS、iPadOS、およびmacOSデバイスを登録します。このサポートには、共有iPadが含まれます。XenMobileは、教育機関向けのApple Business Manager (ABM) およびApple School Manager (ASM) のApple Deployment Programをサポートしています。この記事では、複数のデバイスをABMアカウントと統合する方法について説明します。ABMへの登録およびABMアカウントとXenMobileの接続については、「Deploy devices through Apple Deployment Program」を参照してください。Apple School Managerアカウントについては、「Integrate with Apple Education features」を参照してください。

  macOSデバイスの登録には、macOS 10.10以降が実行されている必要があります。

- Appleから直接購入したかどうかにかかわらず、Apple Configurator 2を使用してiOSデバイスを登録することもできます。

ABMを使用する場合：

- デバイスに触れたり準備したりする必要はありません。代わりに、ABMを通じてデバイスのシリアル番号または発注番号を送信して、デバイスを構成および登録します。
- XenMobileがデバイスを登録した後、すぐに使用を開始できるユーザーにデバイスを渡すことができます。ABMでデバイスをセットアップすると、ユーザーがデバイスを初めて起動するときに完了する必要があるセットアップアシスタントの手順の一部を省略できます。
- ABMのセットアップの詳細については、「Apple Business Manager」から入手できるドキュメントを参照してください。

Apple Configurator 2を使用する場合：

- iOSデバイスを、macOS 10.7.2以降とApple Configurator 2アプリが実行されているAppleコンピューターに接続します。Apple Configurator 2を通じてiOSデバイスを準備し、ポリシーを構成します。
- 必要なポリシーでデバイスをプロビジョニングした後、デバイスが初めてXenMobileに接続すると、XenMobileからポリシーを受信します。その後、デバイスの管理を開始できます。
- Apple Configurator 2の使用方法の詳細については、「Apple Configurator Help」を参照してください。

前提条件

XenMobileとApple間の接続に必要なポートを開きます。詳細については、「Port requirements」を参照してください。

Apple Business ManagerアカウントをXenMobileと統合する

XenMobileでABMアカウントが設定されていない場合は、Deploy devices through Apple Deployment Programで次の手順を完了してください。

- Apple Business Managerに登録する。
- Apple Business ManagerアカウントをXenMobileに接続する。
- Deployment Program対応デバイスを注文する。
- Deployment Program対応デバイスを管理する。

一括登録のデフォルトサーバーを設定する

大量のiOS、iPadOS、およびmacOSデバイスをMDMサーバーに割り当てるには、XenMobileをデフォルトサーバーとして設定できます。

1. 管理者またはデバイス登録マネージャーアカウントを使用して、Apple Business Managerにサインインします。
2. サイドバーで、 > をクリックします。
3. 既存のMDMサーバーを選択します。 で をクリックします。各デバイスタイプのデフォルトのXenMobileサーバーを選択します。 をクリックします。

ABMアカウントのデバイスポリシーとアプリの展開ルールを構成する

> および > の下の セクションを使用して、ABMアカウントをさまざまなデバイスポリシーや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が次のいずれかであることを指定できます。

- 特定のABMアカウントにのみ展開される。
- 選択したアカウントを除くすべてのABMアカウントに展開される。

ABMアカウントのリストには、有効または無効のステータスを持つアカウントのみが含まれます。ABMアカウントが無効になっている場合、ABMデバイスはこのアカウントに属しません。そのため、XenMobileはアプリやポリシーをデバイスに展開しません。

次の例では、デバイスポリシーは「ABM Account NR」というABMアカウント名を持つデバイスにのみ展開されます。

Appleデバイスプログラム設定画面(/en-us/xenmobile/server/media/apple-dep-deployment-rule-policy-example.png)

Apple Deployment Program対応デバイスを登録する際のユーザーエクスペリエンス

ユーザーがApple Deployment Program対応デバイスを登録すると、そのエクスペリエンスは次のようになります。

1. ユーザーはApple Deployment Program対応デバイスを起動します。
2. XenMobileは、XenMobileコンソールで構成したApple Deployment Program構成を、Apple Deployment Program対応デバイスに配信します。
3. ユーザーはデバイスの初期設定を行います。
4. デバイスは自動的にXenMobileデバイス登録プロセスを開始します。
5. ユーザーはデバイスのその他の初期設定を続行します。
6. ホーム画面で、ユーザーはCitrix Secure Hubをダウンロードするために Apple App Storeにサインインするよう求められる場合があります。

> **注:**
>
> デバイスベースのボリューム購入アプリ割り当てを使用してSecure Hubアプリを展開するようにXenMobileを構成した場合、この手順はオプションです。この場合、Apple App Storeアカウントを作成したり、既存のアカウントを使用したりする必要はありません。

> Apple Deployment Programセットアップ(/en-us/xenmobile/server/media/ios-dep-54.png)

7. ユーザーはSecure Hubを開き、資格情報を入力します。ポリシーで必要とされる場合、ユーザーはCitrix PINを作成して確認するよう求められる場合があります。

   XenMobile は、残りの必要なアプリをデバイスに展開します。

Apple Configurator 2 の設定を構成するには

Apple Business Manager の代わりに Apple Configurator 2 を使用して、iPhone および iPad デバイスを一括で構成および展開できます。

ステップ 1: XenMobile で設定を構成する

1. XenMobile コンソールで、 > の順に移動します。

   Apple 展開プログラム設定画面(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-8.png)

2. を に設定します。
3. は読み取り専用フィールドです。この設定は、Apple と通信する XenMobile Server の URL を提供します。Apple Configurator 2 で設定を構成するときに、この URL をコピーして貼り付けます。登録 URL は、`mdm.server.url.com` のような XenMobile Server の完全修飾ドメイン名 (FQDN) または IP アドレスです。
4. 不明なデバイスの登録を防ぐには、 を に設定します。注: この設定が の場合、登録する前に、構成済みのデバイスを XenMobile の > に手動で、または CSV ファイルを介して追加する必要があります。
5. iOS デバイスのユーザーが登録時に資格情報を入力するように要求するには、 を に設定します。デフォルトでは、登録に資格情報は要求されません。
6. 注: XenMobile Server が信頼された SSL 証明書を使用している場合は、この手順をスキップしてください。 をクリックし、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。

Apple 展開プログラム設定画面(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-9.png)

ステップ 2: Apple Configurator 2 で設定を構成する

1. App Store から Apple Configurator 2 をインストールします。
2. Dock Connector-to-USB ケーブルを使用して、Apple Configurator 2 を実行している Mac にデバイスを接続します。最大 30 台の接続されたデバイスを同時に構成できます。Dock Connector がない場合は、1 つ以上の電源付き USB 2.0 高速ハブを使用してデバイスを接続します。
3. Apple Configurator 2 を起動します。コンフィギュレータには、監視用に準備できるすべてのデバイスが表示されます。
4. デバイスを監視用に準備するには:

   - 構成を定期的に再適用してデバイスの制御を維持する場合は、**Supervise devices** を選択します。**Next** をクリックします。

     > **重要:**
     >
     > デバイスを監視モードにすると、選択したバージョンの iOS がデバイスにインストールされ、以前に保存されていたユーザーデータやアプリはすべて完全に消去されます。

   - iOS で、インストールする最新バージョンの iOS の **Latest** をクリックします。

5. **Enroll in MDM Server** で、MDM サーバーを選択します。新しいサーバーを追加するには、**Next** をクリックします。
6. **Define an MDM server** で、サーバーの名前を指定し、XenMobile コンソールから MDM サーバーの URL を貼り付けます。
7. **Assign to organization** で、デバイスを監視する組織を選択します。

   Apple Configurator 2 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「デバイスの準備」を参照してください。
8. 各デバイスの準備が完了したら、電源を入れて iOS 設定アシスタントを起動し、デバイスを初回使用に備えて準備します。

Apple Configurator 2 から Apple Business Manager にデバイスを割り当てるには

Apple Configurator 2 からの iPhone および iPad デバイスを Apple Business Manager アカウントに関連付けることができます。デバイスを追加すると、**Devices** セクションに表示されます。これらのデバイスには、Apple Configurator 2 を介して割り当てられた登録設定は含まれなくなります。詳しくは、「Apple Configurator 2 から追加されたデバイスを Apple Business Manager に割り当てる」を参照してください。

Apple Deployment Program を使用する際の証明書の更新

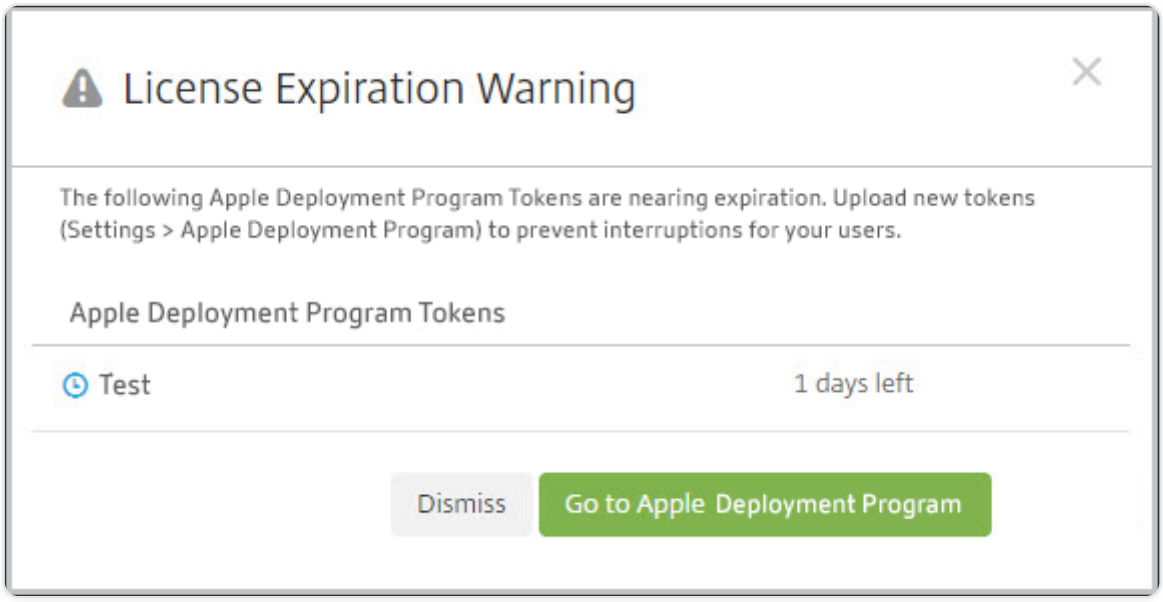
XenMobile の Secure Sockets Layer (SSL) 証明書が更新されたら、XenMobile コンソールの **Settings > Certificates** で新しい証明書をアップロードします。**Import** ダイアログボックスの **Use as** で、証明書が SSL に使用されるように **SSL Listener** をクリックします。サーバーを再起動すると、XenMobile は新しい SSL 証明書を使用します。XenMobile の証明書について詳しくは、「XenMobile での証明書のアップロード」を参照してください。

SSL証明書を更新またはアップデートしても、Apple Deployment ProgramとXenMobile間の信頼関係を再構築する必要はありません。ただし、この記事の前の手順に従って、いつでも**Apple Deployment Program**の設定を再構成できます。

Apple Deployment Programの詳細については、Appleのドキュメントを参照してください。

Apple Deployment ProgramとXenMobile間の接続を更新する

Automated Device Enrollmentサーバーのトークンの有効期限が切れると、XenMobileはライセンス有効期限切れ警告を表示します。



Apple School Manager/Apple Business Managerからトークンを置き換えます。

ステップ1：XenMobile Serverから公開キーをダウンロードする

1. XenMobileコンソールで、**設定 > Apple Deployment Program**に移動し、新しい公開キーをダウンロードします。

ステップ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する

1. Apple Business Managerにサインインして、トークンをダウンロードします。
2. **設定**を開き、トークンが必要なサーバーを選択します。**編集**をクリックします。
3. **MDMサーバー設定**で、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、変更を保存します。
4. **トークンをダウンロード**をクリックして、新しいトークンをダウンロードします。

ステップ3：XenMobileでサーバートークンファイルをアップロードする

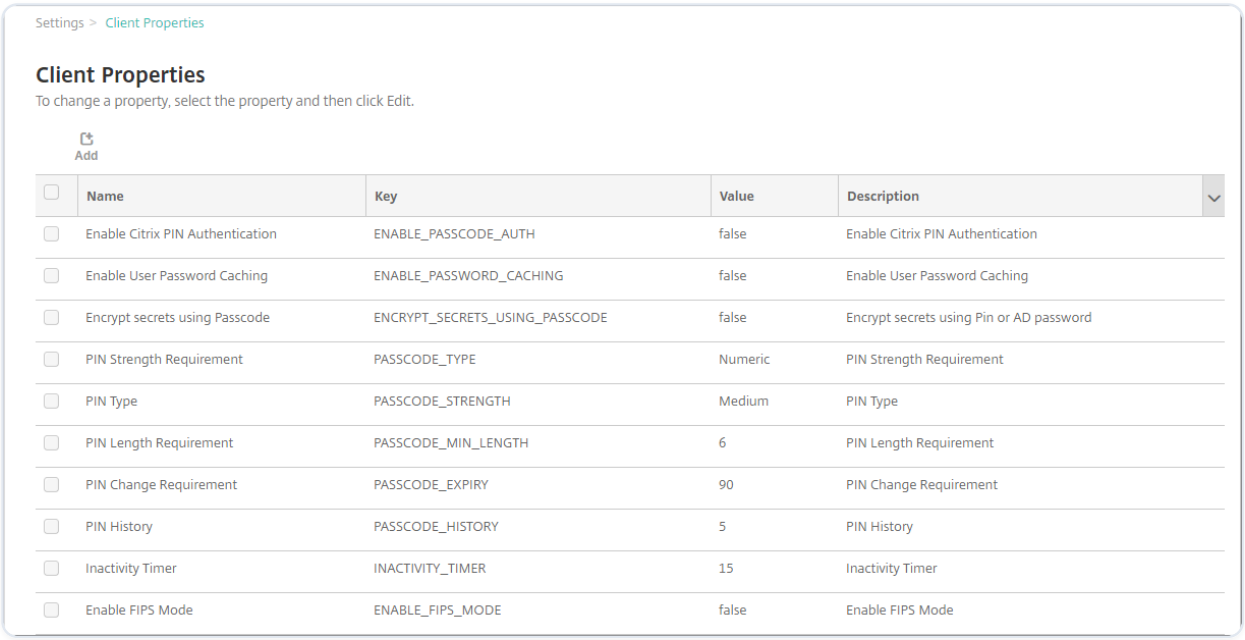
1. Citrix XenMobileで、**設定 > Apple Deployment Program**に移動します。
2. 展開プログラムアカウントを選択し、**編集**をクリックして、サーバートークンファイルをアップロードします。
3. **次へ**をクリックし、変更を保存します。

クライアントプロパティ

クライアントプロパティには、ユーザーデバイス上の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などの高度な設定を構成できます。クライアントプロパティはCitrixサポートから入手します。

クライアントプロパティは、Secure Hubのリリースごと、およびクライアントアプリによっては変更される場合があります。より一般的に構成されるクライアントプロパティの詳細については、この記事の後半にある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。

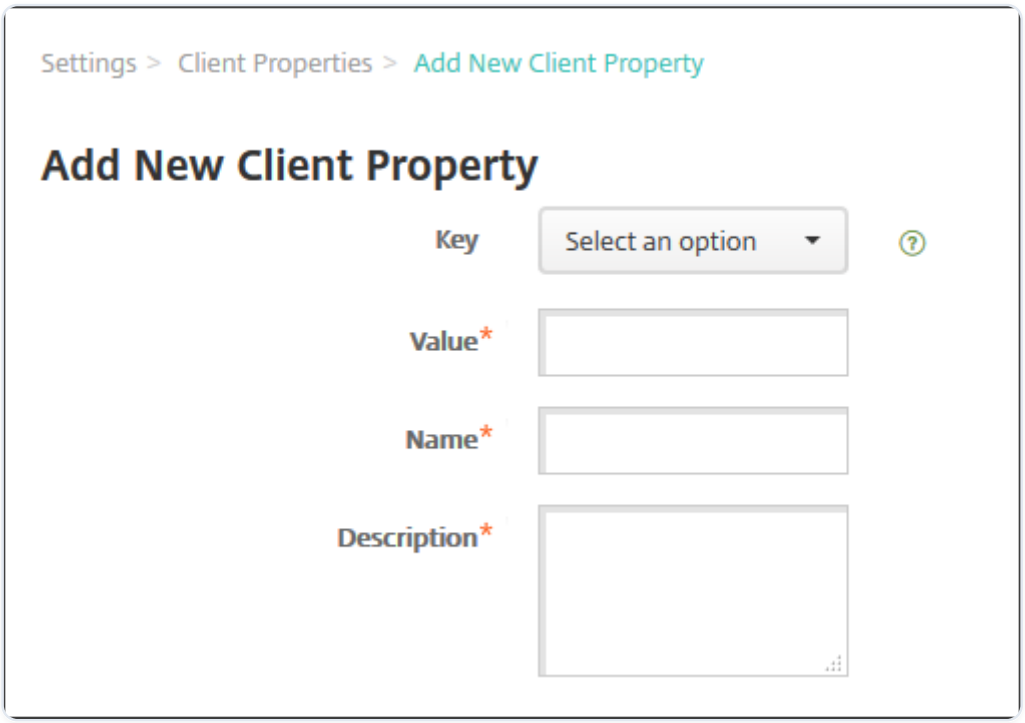
1. XenMobile®コンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **クライアント**の下にある**クライアントプロパティ**をクリックします。**クライアントプロパティ**ページが表示されます。このページからクライアントプロパティを追加、編集、削除できます。



Name	Key	Value	Description
Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
PIN History	PASSCODE_HISTORY	5	PIN History
Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

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**ページが表示されます。



2. 次の設定を構成します。

- **キー:** リストで、追加するプロパティキーをクリックします。重要: 設定を更新する前にCitrixサポートに連絡してください。特別なキーを要求できます。
- **値:** 選択したプロパティの値。
- **名前:** プロパティの名前。
- **説明:** プロパティの説明。

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**テーブルで、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選択すると、オプションメニューがクライアントプロパティリストの上に表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

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**ページが表示されます。



3. 必要に応じて、次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。
   - **名前:** プロパティ名。
   - **説明:** プロパティの説明。

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に終了します。

クライアントプロパティを削除するには

1. **クライアントプロパティ**テーブルで、削除するクライアントプロパティを選択します。

   各プロパティの横にあるチェックボックスを選択すると、複数のプロパティを選択して削除できます。

2. **削除**をクリックします。確認ダイアログボックスが表示されます。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のリファレンス

XenMobileの事前定義されたクライアントプロパティとそのデフォルト設定は次のとおりです。

- **CONTAINER_SELF_DESTRUCT_PERIOD**
  - 表示名: MDXコンテナの自己破壊期間
  - 自己破壊は、指定された日数にわたる非アクティブ状態の後、Secure Hubおよび管理対象アプリへのアクセスを防止します。期限が過ぎると、アプリは使用できなくなります。データのワイプには、アプリキャッシュとユーザーデータを含む、インストールされている各アプリのアプリデータのクリアが含まれます。

    非アクティブ時間とは、サーバーが特定の期間にわたってユーザーを検証するための認証要求を受信しない期間を指します。たとえば、このプロパティが30日に設定されており、ユーザーが30日以上アプリを使用しない場合、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、iOSおよびAndroidプラットフォームに適用され、既存のアプリロックおよびワイプポリシーの機能強化です。
  - このグローバルポリシーを構成するには、 **>** に移動し、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: デバイスログをITヘルプデスクに送信
  - このプロパティは、ITヘルプデスクにログを送信する機能を有効または無効にします。
  - 指定可能な値: **true** または **false**
  - デフォルト値: **false**
- **DISABLE_LOGGING**
  - 表示名: ログ記録の無効化
  - このプロパティを使用すると、ユーザーがデバイスからログを収集およびアップロードするのを防ぐことができます。このプロパティは、Secure Hubおよびインストールされているすべてのアプリのログ記録を無効にします。ユーザーはサポートページからどのアプリのログも送信できません。メール作成ダイアログボックスが表示されても、ログは添付されません。ログ記録が無効になっていることを示すメッセージが表示されます。この設定により、XenMobileコンソールでSecure HubおよびMDXアプリのログ設定を更新することもできなくなります。

    このプロパティが**true**に設定されている場合、Secure Hubは**アプリケーションログのブロック**を**true**に設定します。その結果、新しいポリシーが適用されるとMDXアプリはログ記録を停止します。

- 設定可能な値: **true**または**false**
- デフォルト値: **false** (ログ記録は無効になっていません)

- **ENABLE_CRASH_REPORTING**
  - 表示名: クラッシュレポートの有効化
  - **true**の場合、Citrixは、iOSおよびAndroid版Secure Hubの問題のトラブルシューティングに役立つクラッシュレポートと診断情報を収集します。**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: 資格情報ストアの有効化
  - 資格情報ストアを有効にすると、AndroidまたはiOSユーザーはモバイル生産性アプリにアクセスする際にパスワードを1回入力するだけで済みます。Citrix PINを有効にするかどうかにかかわらず、資格情報ストアを使用できます。Citrix PINを有効にしない場合、ユーザーはActive Directoryパスワードを入力します。XenMobileは、Secure Hubおよびパブリックストアアプリでのみ、資格情報ストアとActive Directoryパスワードの使用をサポートしています。資格情報ストアでActive Directoryパスワードを使用する場合、XenMobileはPKI認証をサポートしません。
  - Secure Mailでの自動登録には、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**に移動し、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が次回のオンライン認証を行うときに、Secure Hubは新しい値をデバイスに渡します。
  - 指定可能な値: **true** または **false**
  - デフォルト値: **false**
- **ENABLE_PASSCODE_AUTH**

- 表示名: Citrix PIN認証を有効にする
- 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。Citrix PINまたはパスコードを使用すると、ユーザーはActive Directoryパスワードの代わりにPINを定義するように求められます。この設定は、ENABLE_PASSWORD_CACHINGが有効になっている場合、またはXenMobileが証明書認証を使用している場合に自動的に有効になります。

  オフライン認証の場合、Citrix PINはローカルで検証され、ユーザーは要求したアプリまたはコンテンツにアクセスできます。オンライン認証の場合、Citrix PINまたはパスコードはActive Directoryパスワードまたは証明書のロックを解除し、その後、XenMobileでの認証の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がパスワードを保存しないため、オンライン認証では常にパスワードが求められます。
- 指定可能な値: **true** または **false**
- デフォルト値: **false**

- **ENABLE_PASSWORD_CACHING**
  - 表示名: ユーザーパスワードのキャッシュを有効にする
  - このプロパティにより、Active Directoryパスワードをモバイルデバイスにローカルでキャッシュできます。このプロパティを**true**に設定すると、**ENABLE_PASSCODE_AUTH**プロパティも**true**に設定する必要があります。ユーザーパスワードキャッシュが有効になっている場合、XenMobileはユーザーにCitrix PINまたはパスコードの設定を求めます。
  - 指定可能な値: **true** または **false**
  - デフォルト値: **false**
- **ENABLE_TOUCH_ID_AUTH**
  - 表示名: Touch ID認証を有効にする
  - Touch ID認証をサポートするデバイスの場合、このプロパティは、デバイスでの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が有効になっている必要があります。LDAP認証が無効になっている場合（たとえば、証明書ベースの認証のみが使用されているため）、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**ENABLE_PASSCODE_AUTH**が**false**であっても、XenMobileはCitrix PINを要求します。

ENABLE_PASSCODE_AUTHを**false**に設定すると、ユーザーがアプリを起動したときに、Touch IDを使用するためのプロンプトに応答する必要があります。

- 指定可能な値: **true** または **false**
- デフォルト値: **false**

- **ENABLE_WORXHOME_CEIP**
  - 表示名: Enable Worx Home CEIP
  - このプロパティは、カスタマーエクスペリエンス向上プログラムを有効にします。この機能は、匿名の構成データと使用状況データを定期的にCitrixに送信します。このデータは、CitrixがXenMobileの品質、信頼性、およびパフォーマンスを向上させるのに役立ちます。
  - 値: **true** または **false**
  - デフォルト値: **false**
- **ENCRYPT_SECRETS_USING_PASSCODE**
  - 表示名: パスコードを使用してシークレットを暗号化
  - このプロパティは、iOSキーチェーンなどのプラットフォームベースのネイティブストアではなく、シークレットボールトに機密データをデバイスに保存します。このプロパティにより、主要なアーティファクトの強力な暗号化が可能になり、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とは、ユーザーのみが知っている、ユーザーが生成したランダムなPINコードです。

    Citrixは、ユーザーデバイスのセキュリティを向上させるために、このプロパティを有効にすることを推奨します。その結果、ユーザーはCitrix PINの認証プロンプトをより多く経験することになります。
  - 設定可能な値: **true** または **false**
  - デフォルト値: **false**
- **INACTIVITY_TIMER**
  - 表示名: 非アクティブタイマー
  - このプロパティは、ユーザーがデバイスを非アクティブな状態にしてから、Citrix PINまたはパスコードのプロンプトなしでアプリにアクセスできる期間を定義します。MDXアプリでこの設定を有効にするには、 設定を にします。 設定が の場合、ユーザーはSecure Hubにリダイレクトされ、完全な認証を行います。この設定を変更すると、ユーザーが認証を求められる次回のタイミングで値が有効になります。

iOSでは、非アクティブタイマーはMDXアプリと非MDXアプリの両方でSecure Hubへのアクセスも管理します。

- 設定可能な値: 任意の正の整数
- デフォルト値: **15** (分)

- **ON_FAILURE_USE_EMAIL**
  - 表示名: 失敗時にメールを使用してデバイスログをITヘルプデスクに送信
  - このプロパティは、メールを使用してデバイスログをIT部門に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**
  - 既定値: **true**
- **PASSCODE_EXPIRY**
  - 表示名: PIN変更要件
  - このプロパティは、Citrix PINまたはパスコードが有効な期間を定義します。この期間が過ぎると、ユーザーはCitrix PINまたはパスコードの変更を強制されます。この設定を変更した場合、新しい値は現在のCitrix PINまたはパスコードの有効期限が切れたときにのみ設定されます。
  - 指定可能な値: **1**～**99**を推奨します。PINのリセットをなくすには、値を大きな数値（例: 100,000,000,000）に設定します。有効期限を最初に1～99日の間に設定し、その期間中に大きな数値に変更した場合、PINは最初の期間の終わりに期限切れになりますが、その後は期限切れになりません。
  - 既定値: **90** (日)
- **PASSCODE_HISTORY**
  - 表示名: PIN履歴
  - このプロパティは、ユーザーがCitrix PINまたはパスコードを変更する際に再利用できない、以前使用したCitrix PINまたはパスコードの数を定義します。この設定を変更した場合、新しい値はユーザーが次回Citrix PINまたはパスコードをリセットするときに設定されます。
  - 指定可能な値: **1**～**99**
  - 既定値: **5**
- **PASSCODE_MAX_ATTEMPTS**

- 表示名: PIN試行回数
- このプロパティは、ユーザーが完全認証を求められるまでに、Citrix PINまたはパスコードを誤って入力できる回数を定義します。ユーザーが完全認証に成功すると、Citrix PINまたはパスコードの作成を求められます。
- 指定可能な値: 任意の正の整数
- 既定値: **15**

- **PASSCODE_MIN_LENGTH**
  - 表示名: PINの長さ要件
  - このプロパティは、Citrix PINの最小の長さを定義します。
  - 指定可能な値: **4〜10**
  - 既定値: **6**
- **PASSCODE_STRENGTH**
  - 表示名: PINの強度要件
  - このプロパティは、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、Citrix PINまたはパスコードを作成するよう求められます。
  - 指定可能な値: **低**、**中**、**高**、または**強**
  - 既定値: **中**
  - PASSCODE_TYPE設定に基づいた各強度設定に対するパスワードの規則は次のとおりです。

数値パスコードの規則:

パスコードの強度	数値パスコードの種類の規則	許可	許可されていません
低	すべての数字、任意の順序が許可されます	444444, 123456, 654321	
中 (デフォルト設定)	すべての数字を同じにしたり、連続させたりすることはできません。	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321

パスコードの強度	数値パスコードの種類の規則	許可	許可されていません
高	隣接する数字を同じにすることはできません。	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
強	同じ数字を3回以上使用しないでください。3つ以上の連続した数字を続けて使用しないでください。3つ以上の連続した数字を逆順で使用しないでください。	102983, 085085, 824673, 132312	132132, 131313, 902030

英数字パスコードのルール:

パスコードの強度	英数字パスコードの種類のルール	許可	不許可
低	少なくとも1つの数字と1つの文字を含める必要があります	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef
中 (デフォルト設定)	低パスコード強度のルールに加え、文字とすべての数字を同じにすることはできません。文字を連続させたり、数字を連続させたりすることはできません。	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	少なくとも1つの大文字と1つの小文字を含める。	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12、DFGH2 など
強	少なくとも1つの数字、1つの特殊記号、1つの大文字、	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

パスコードの強度	英数字パスコードの種類のルール	許可	不許可
	および1つの小文字を含める。		

- **PASSCODE_TYPE**
  - 表示名: PINの種類
  - このプロパティは、ユーザーが数値のCitrix PINを定義できるか、英数字のパスコードを定義できるかを決定します。**数値**を選択すると、ユーザーは数字のみを使用できます (Citrix PIN)。**英数字**を選択すると、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)。

    この設定を変更した場合、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。
  - 指定可能な値: **数値**または**英数字**
  - デフォルト値: **数値**
- **REFRESHINTERVAL**
  - 表示名: REFRESHINTERVAL
  - 既定では、XenMobileは、3日ごとにAuto Discovery Server (ADS)にpingを送信して、ピン留めされた証明書を確認します。更新間隔を変更するには、 **>** に移動し、カスタムキー **REFRESHINTERVAL** を追加して、 を時間数に設定します。
  - 既定値: **72** 時間 (3 日)
- **SEND_LDAP_ATTRIBUTES**
  - Android、iOS、またはmacOSデバイスのMAM専用展開の場合: XenMobileを構成すると、メール資格情報でSecure Hubに登録したユーザーは、Secure Mailに自動的に登録されます。その結果、ユーザーはSecure Mailに登録するために追加情報を提供したり、追加の手順を実行したりする必要がありません。
  - このグローバルクライアントポリシーを構成するには、 **>** に移動し、カスタムキー **SEND_LDAP_ATTRIBUTES** を追加して、 を次のように設定します。
  - 値: `userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}`
  - 属性値は、MDMポリシーと同様にマクロとして指定されます。

- このプロパティのサンプルアカウントサービス応答を次に示します。

  ```
  <property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,em
  name="SEND_LDAP_ATTRIBUTES"/>
  ```

- このプロパティの場合、XenMobileはコンマ文字を文字列ターミネータとして扱います。したがって、属性値にコンマが含まれる場合は、その前にバックスラッシュを付けます。バックスラッシュは、クライアントが埋め込まれたコンマを属性値の終わりとして解釈するのを防ぎます。バックスラッシュ文字は `"\\"` で表します。

- **HIDE_THREE_FINGER_TAP_MENU**

  - このプロパティが設定されていないか、**false** に設定されている場合、ユーザーはデバイスで3本指タップを行うことで、非表示機能メニューにアクセスできます。非表示機能メニューでは、ユーザーがアプリケーションデータをリセットできました。このプロパティを **true** に設定すると、ユーザーは非表示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、 **>** に移動し、カスタムキー **HIDE_THREE_FINGER_TAP_MENU** を追加して、 を設定します。

- **TUNNEL_EXCLUDE_DOMAINS**

  - 表示名: トンネル除外ドメイン
  - デフォルトでは、MDXは、XenMobile SDKおよびアプリがさまざまな機能に使用する一部のサービスエンドポイントをマイクロVPNトンネリングから除外します。たとえば、これらのエンドポイントには、Google Analytics、Citrix Cloud™サービス、Active Directoryサービスなど、エンタープライズネットワークを介したルーティングを必要としない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、除外されるドメインのデフォルトリストを上書きします。
  - このグローバルクライアントポリシーを構成するには、 **>** に移動し、カスタムキー **TUNNEL_EXCLUDE_DOMAINS** を追加して、 を設定します。
  - 値: デフォルトのリストを、トンネリングから除外するドメインに置き換えるには、ドメインサフィックスのコンマ区切りリストを入力します。すべてのドメインをトンネリングに含めるには、**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
    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
    ```

XenMobile Serverのカスタムクライアントプロパティは次のとおりです。

- **ENABLE_MAM_NFACTOR_SSO**
  - このプロパティを使用すると、NetScaler® Gatewayで高度な認証ポリシーを使用しているときに、Secure HubのMAM登録またはログイン中にMAM nFactor SSOを有効または無効にできます。値が **true** に設定されている場合、Secure HubのMAM登録またはログイン中にMAM nFactor SSOが有効になります。
  - このプロパティを構成するには、 **>** に移動し、 をクリックします。 ドロップダウンメニューで を選択し、必要に応じて次の情報を更新します。
    - キー - ENABLE_MAM_NFACTOR_SSO
    - 値 - true または false
    - 名前 - ENABLE_MAM_NFACTOR_SSO
    - 説明 - 関連する説明を追加します
- **MICROSOFT_CERTIFICATE_STRONG_MAPPING**
  - このプロパティは、Microsoft公開鍵インフラストラクチャ (PKI) を使用してSecure Mailを使用する場合に、既存のクライアント証明書が、Subject Alternative Name (SAN) にセキュリティ識別子 (SID) を追加することで証明書の強力なマッピング機能をサポートするように更新されるかどうかを制御します。値が **true** に設定されている場合、既存のクライアント証明書はSAN SIDを含むように更新されます。
  - このプロパティはMicrosoft PKIにのみ適用されます。
  - このプロパティを設定するには、 **>** に移動し、 をクリックします。 ドロップダウンメニューで を選択し、必要に応じて以下の情報を更新します。
    - キー - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 値 - true または false
    - 名前 - MICROSOFT_CERTIFICATE_STRONG_MAPPING
    - 説明 - SAN SIDを含めるようにクライアント証明書を更新します

Apple Deployment Program を介してデバイスを展開する

Apple には、ビジネスアカウントと教育機関アカウント向けのデバイス登録プログラムがあります。ビジネスアカウントの場合、XenMobile でのデバイス登録と管理のために Apple Business

Manager (ABM) または Apple School Manager (ASM) を使用するには、Apple Deployment Program に登録します。このプログラムは、iOS、iPadOS、および macOS デバイス向けです。

Apple Deployment Program は、個人ではなく組織向けに提供されています。Apple Deployment Program アカウントを作成するには、かなりの数の企業詳細情報を提供する必要があります。そのため、アカウントの申請と承認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、Apple School Manager アカウントを作成します。ASM は Apple Deployment Program と Apple ボリューム購入を統合します。Apple School Manager アカウントを作成するには、Apple School サイトにアクセスしてください。

Apple Deployment Program に登録する

Apple Business Manager に登録するには、business.apple.comにアクセスします。**Enroll now** をクリックして、新しいアカウントを申請します。ベストプラクティスは、`deployment@company.com` のような組織のメールアドレスを使用することです。登録プロセスには数日かかる場合があります。ログオン資格情報を受け取ったら、Apple Business Manager に記載されている手順に従ってアカウントを作成します。

> **注:**
>
> 教育機関アカウントについては、Apple Education 機能との統合を参照してください。

Apple Business Manager アカウントを XenMobile に接続する

Apple Business Manager アカウントを XenMobile 展開に接続するには、XenMobile コンソールと Apple Business Manager に情報を入力します。次の手順に従います。

ステップ 1: XenMobile Server から公開キーをダウンロードする

1. XenMobile コンソールで、**Settings > Apple Deployment Program** に移動します。



2. **Download Public Key** の下にある **Download** をクリックします。

ステップ 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する

1. 管理者またはデバイス登録マネージャーアカウントを使用して、Apple Business Managerにサインインします。
2. サイドバーの下部にある**Settings**をクリックし、**Device Management Settings > Add MDM Server**をクリックします。

   Apple Deployment Program設定画面](/en-us/xenmobile/server/media/asm-add-mdm-server.png)
3. **MDM Server Name**設定で、XenMobile Serverの名前を入力します。入力するサーバー名は参照用です。サーバーのURLや名前ではありません。
4. **Upload Public Key**の下で、**Choose File**をクリックします。XenMobileからダウンロードした公開キーをアップロードし、変更を保存します。
5. **Download Token**をクリックして、サーバートークンファイルをコンピューターにダウンロードします。

   ABMアカウントをXenMobileに追加する際に、サーバートークンファイルをアップロードする必要があります。トークンファイルをインポートすると、ABMトークン情報がXenMobileコンソールに表示されます。
6. **Default Device Assignment**の下で、**Change**をクリックします。デバイスの割り当て方法を選択し、要求された情報を提供します。詳細については、ABM User Guideを参照してください。

ステップ3：XenMobileにABMアカウントを追加する

XenMobileには複数のABMアカウントを追加できます。この機能により、国や部署などに応じて異なる登録設定やセットアップアシスタントオプションを使用できます。その後、ABMアカウントを異なるデバイスポリシーに関連付けます。

たとえば、異なる国からのすべてのABMアカウントを同じXenMobile Serverに一元化して、すべてのABMデバイスをインポートおよび監視することができます。部署、組織階層、またはその他の構造ごとに登録設定とセットアップアシスタントオプションをカスタマイズすることで、ポリシーは組織全体で適切な機能を提供し、ユーザーは適切な支援を受けることができます。

1. XenMobileコンソールで、**Settings > Apple Deployment Program**に移動し、**Add Apple Deployment Program Account**の下にある**Add**をクリックします。

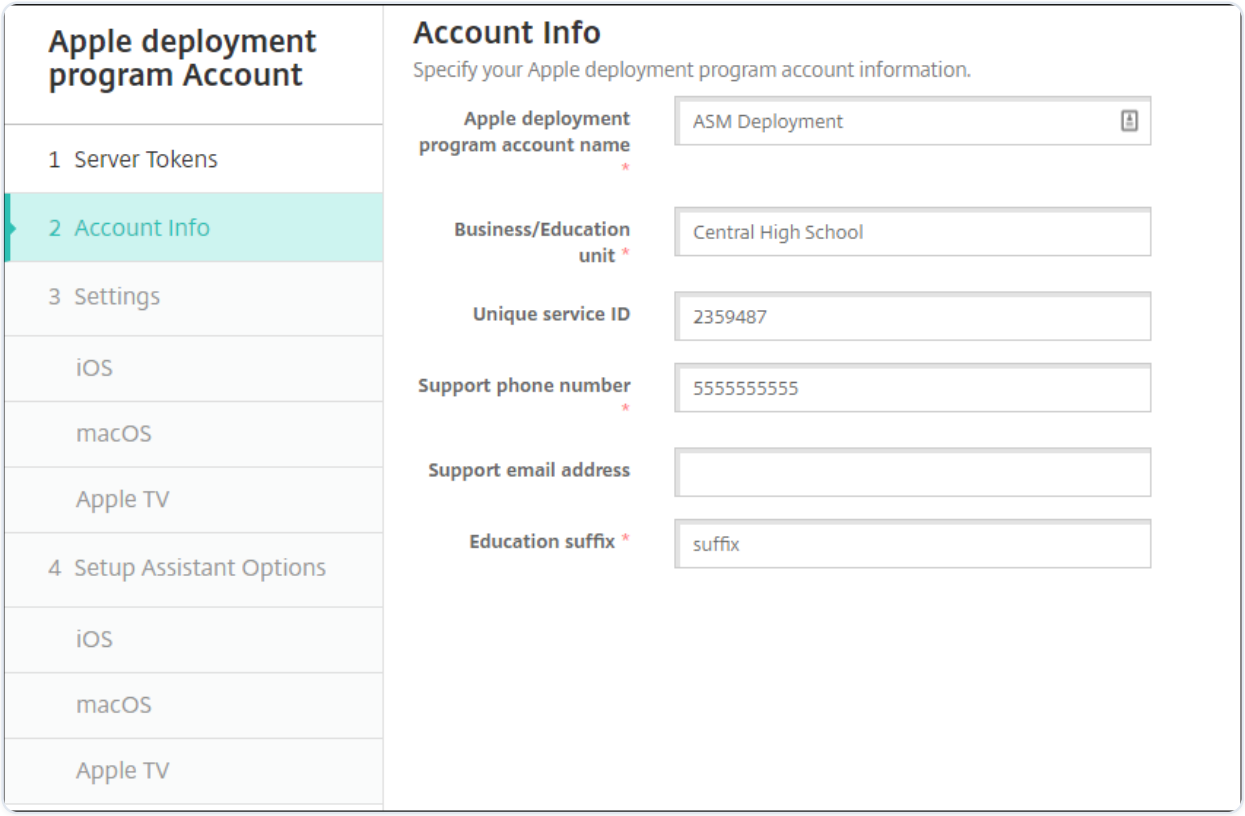
Apple Deployment Program設定画面](/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-1.png)

2. **Server Tokens**ページで、サーバートークンファイルを指定し、**Upload**をクリックします。

   Apple Deployment Program設定画面](/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-2.png)

   サーバーのトークン情報が表示されます。

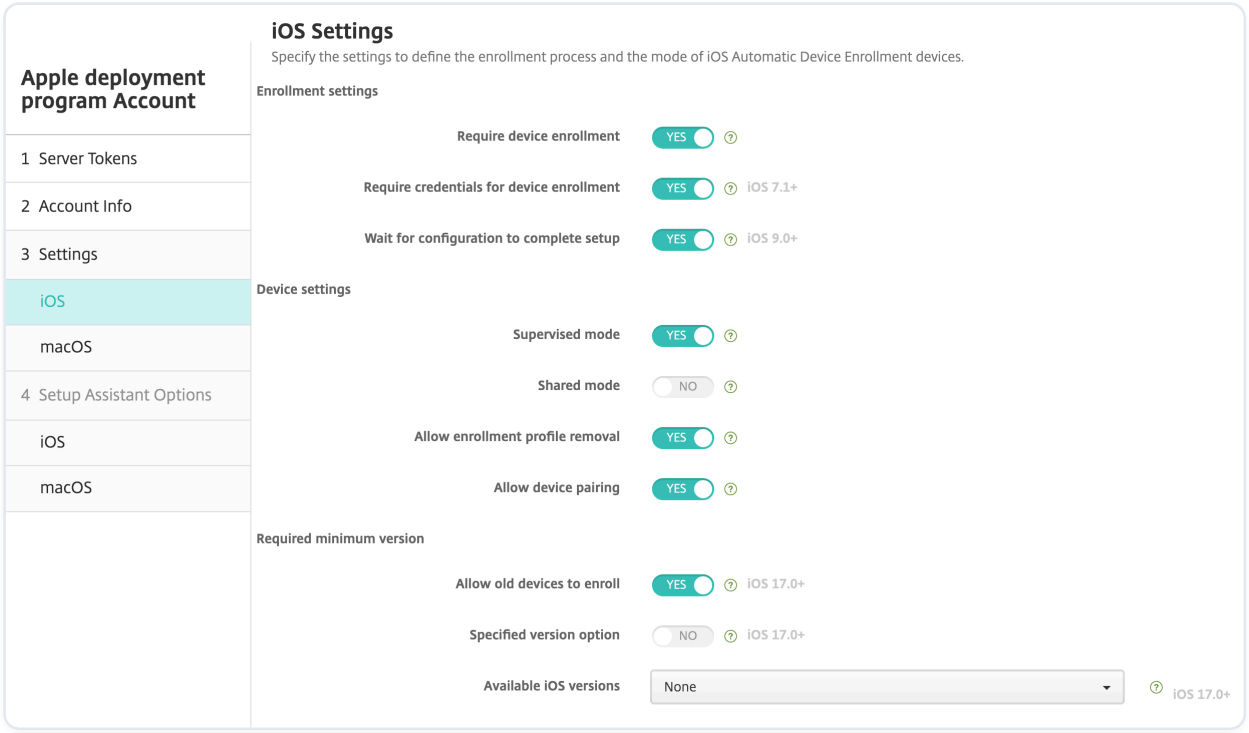
3. ページで、次の設定を指定します。



- **Apple Deployment Programアカウント名:** このApple Deployment Programアカウントの一意の名前。国や組織階層など、Apple Deployment Programアカウントをどのように整理しているかを反映する名前を使用します。
- **ビジネス/教育ユニット:** デバイスが割り当てられるビジネスユニットまたは部門。このフィールドは必須です。
- **一意のサービスID:** アカウントをさらに識別するのに役立つオプションの一意のID。
- **サポート電話番号:** セットアップ中にユーザーがヘルプを求めるために電話するサポート電話番号。このフィールドは必須です。
- **サポートメールアドレス:** エンドユーザーが利用できるオプションのサポートメールアドレス。

- **教育サフィックス**: ASMアカウントの場合。このアカウントを通じて登録されたデバイスに割り当てられたサフィックスを入力します。

4. で、次の設定を指定します。



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するかどうか。デフォルトは****です。
- **デバイス登録に資格情報を要求する:** ABMセットアップ中にユーザーに資格情報の入力を要求するかどうか。Citrix®は、すべてのユーザーにデバイス登録中に資格情報の入力を要求し、承認されたユーザーのみがデバイスを登録できるようにすることを推奨します。デフォルトは****です。

  初回セットアップの前にABMを有効にし、このオプションを選択しない場合、XenMobileはABMコンポーネントを作成します。この作成には、ABMユーザー、Secure Hub、ソフトウェアインベントリ、ABM展開グループなどのコンポーネントが含まれます。このオプションを選択した場合、XenMobileはコンポーネントを作成しません。その結果、後でこのオプションをクリアしても、資格情報を入力していないユーザーは、これらのABMコンポーネントが存在しないため、ABMに登録できません。その場合、ABMコンポーネントを追加するには、ABMアカウントを無効にしてから再度有効にします。
- **構成のセットアップ完了を待機:** すべてのMDMリソースがデバイスに展開されるまで、ユーザーのデバイスをセットアップアシスタントモードに維持する必要があるかどうか。この設定は、監視モードのデバイスで利用できます。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場合、以下のコマンドは機能しない可能性があります。
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

デバイス設定

- **監視モード:** Apple Configuratorを使用してABM登録済みデバイスを管理する場合、または**構成のセットアップ完了を待機**が有効になっている場合は、**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デバイスを監視モードにする方法の詳細については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」を参照してください。
- **登録プロファイルの削除を許可:** デバイスがリモートで削除できるプロファイルを使用することを許可するかどうか。デフォルトは**いいえ**です。
- **デバイスのペアリングを許可:** ABMを通じて登録されたデバイスについて、Apple MusicおよびApple Configuratorを通じて管理できるかどうか。デフォルトは**いいえ**です。

必須最小バージョン

- **古いデバイスの登録を許可**: 有効にすると、現在の必須最小バージョンにアップグレードできなかったデバイスでも登録できます。デフォルトはオンです。このオプションはiOS 17.0以降でのみ利用可能です。
- **指定バージョンオプション**: 管理者が指定バージョンを手動で入力することを許可するかどうか。デフォルトは**オフ**です。このオプションはiOS 17.0以降でのみ利用可能です。
- **利用可能なiOSバージョン**: リストから利用可能なiOSバージョンを選択できます。デバイスのiOSバージョンが現在のバージョンより低い場合、デバイスで更新プロセスが開始されます。将来的にバージョンが期限切れになった場合、利用可能なバージョンリストの最小バージョンが使用されます。デフォルトは**なし**で、**なし**に設定しても効果はありません。このオプションはiOS 17.0以降でのみ利用可能です。
- **指定されたバージョン**: デバイスのiOSバージョンが現在のバージョンより低い場合、デバイスで更新プロセスが開始されます。将来的にバージョンが期限切れになった場合、利用

可能なバージョンリストの最小バージョンが使用されます。予期せぬエラーを防ぐため、正しいバージョン番号を入力してください。

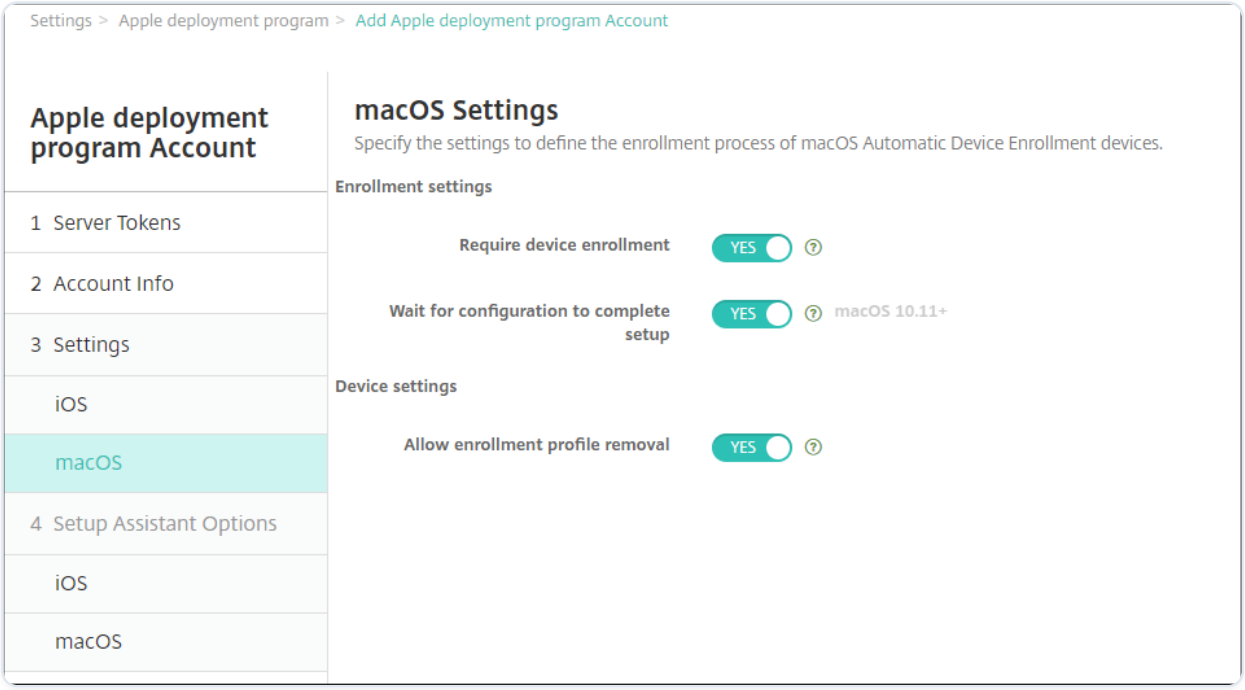
監視ID

GroundControlツールを使用している場合、以下の目的で証明書を追加できます。

- ペアリング制限を上書きして、「このホストを信頼しますか」というプロンプトを回避する。
- ユーザーの操作なしでプロファイルのインストールなどのアクティビティを行うために、USB経由で管理対象デバイスのアクションをエスカレートする。これにより、GroundControlはチェックアウトのためにシングルアプリモードとデバイスロックを有効にできます。
- ABMデバイスにバックアップを復元する。

GroundControlの詳細については、The GroundControl websiteを参照してください。

5. **macOS設定**で、以下の設定を指定します。



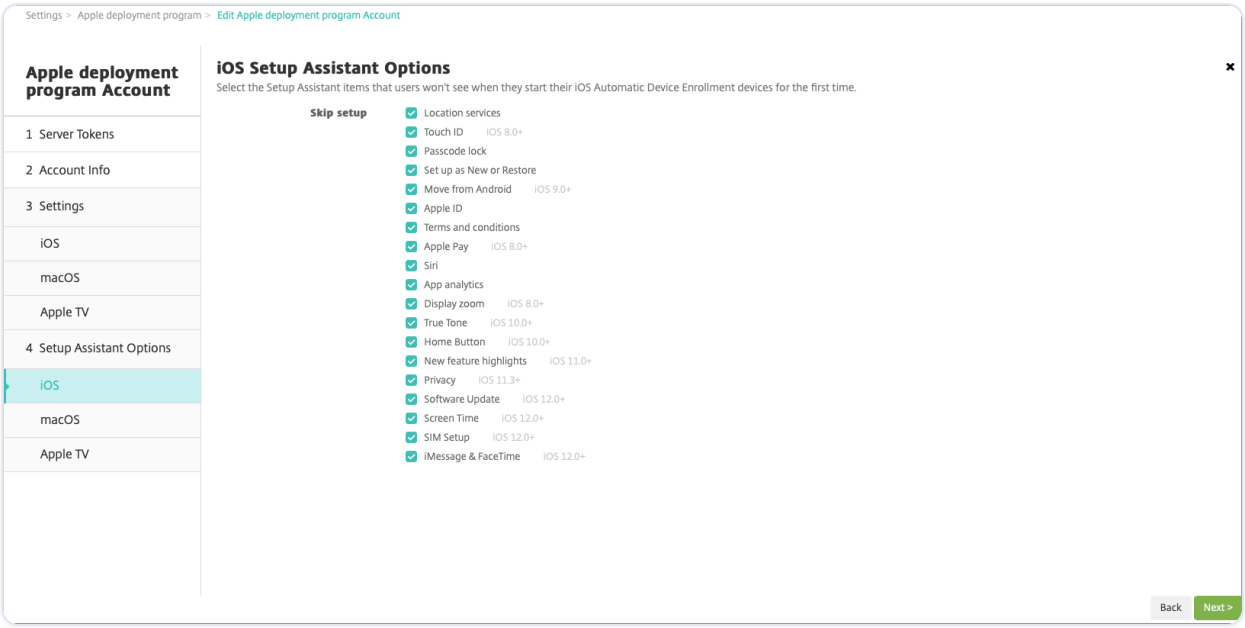
登録設定

- **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するかどうか。デフォルトは**はい**です。
- **構成がセットアップを完了するまで待機する: はい**の場合、MDMリソースの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。この展開は、ローカルアカウントの作成前に行われます。この設定はmacOS 10.11以降のデバイスで利用可能です。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する:** リモートで削除できるプロファイルをデバイスが使用することを許可するかどうか。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、ユーザーがデバイスを初めて起動するときにiOSセットアップアシスタントがスキップする手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。アクセスを完全に制限しない限り、ユーザーはセットアップ完了後にスキップされた機能を構成できます。機能へのアクセスを制限する方法の詳細については、「制限デバイスポリシー」を参照してください。すべての項目のデフォルトはクリアされています。以下の説明は、設定が選択された場合に何が起こるかを示しています。



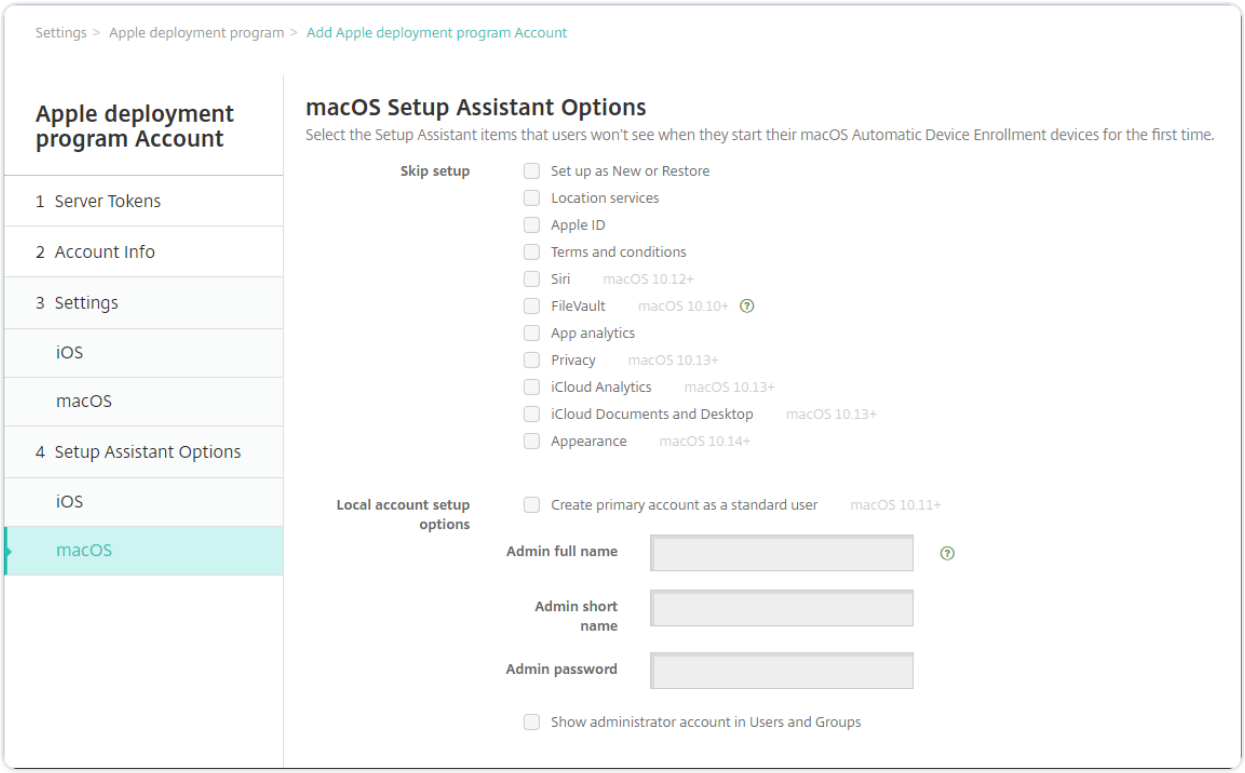
- **位置情報サービス:** ユーザーがデバイスで位置情報サービスを設定するのを防ぎます。
- **Touch ID:** ユーザーがiOSデバイスでTouch IDまたはFace IDを設定するのを防ぎます。iOS 15で非推奨になりました。
- **パスコードロック:** ユーザーがデバイスのパスコードを設定するのを防ぎます。パスコードが存在しない場合、ユーザーはTouch IDまたはApple Payを使用できません。
- **新規として設定または復元:** ユーザーがデバイスを新規として設定したり、iCloudまたはApple App Storeのバックアップから復元したりするのを防ぎます。
- **Androidから移行:** ユーザーがAndroidデバイスからiOSデバイスにデータを転送するのを防ぎます。このオプションは、**新規として設定または復元**が選択されている場合（つまり、手順がスキップされている場合）にのみ利用可能です。
- **Apple ID:** ユーザーがデバイスの管理対象Apple IDアカウントを設定するのを防ぎます。
- **利用規約:** ユーザーがデバイスの使用に関する利用規約を読み、同意するのを防ぎます。

- **Apple Pay:** ユーザーがApple Payを設定するのを防ぎます。この設定がクリアされている場合、ユーザーはTouch IDとApple IDを設定する必要があります。これらの設定がクリアされていることを確認してください。
- **Siri:** ユーザーがSiriを構成するのを防ぎます。
- **App解析:** ユーザーがクラッシュデータと使用状況統計をAppleと共有するかどうかを設定するのを防ぎます。
- **画面表示の拡大/縮小:** ユーザーがiOSデバイスで画面解像度（標準または拡大）を設定するのを防ぎます。iOS 17で非推奨になりました。
- **True Tone:** ユーザーが4チャンネルセンサーを設定してディスプレイのホワイトバランスを動的に調整するのを防ぎます。
- **ホームボタン:** ユーザーがホームボタンのフィードバックスタイルを設定するのを防ぎます。iOS 15で非推奨になりました。
- **新機能のハイライト:** ユーザーがAppleソフトウェアの新機能に関する情報を表示する画面を見るのを防ぎます。
- **プライバシー:** ユーザーがデータとプライバシーのペインを見るのを防ぎます。iOS 11.3以降の場合。
- **ソフトウェアアップデート:** ユーザーがiOSを最新バージョンにアップデートするのを防ぎます。iOS 12.0以降の場合。
- **スクリーンタイム:** ユーザーがスクリーンタイムを有効にするのを防ぎます。iOS 12.0以降の場合。
- **SIM設定:** ユーザーがモバイル通信プランを設定するのを防ぎます。iOS 12.0以降の場合。
- **iMessageとFaceTime:** ユーザーがiMessageとFaceTimeを有効にするのを防ぎます。iOS 12.0以降の場合。
- **外観:** ユーザーが外観モードを選択するのを防ぎます。iOS 13.0以降の場合。
- **ようこそ:** ユーザーが**開始**画面を見るのを防ぎます。iOS 13.0以降の場合。
- **復元完了:** ユーザーがセットアップ中に復元が完了したかどうかを見るのを防ぎます。iOS 14.0以降の場合。
- **アップデート完了:** ユーザーがセットアップ中にソフトウェアアップデートが完了したかどうかを見るのを防ぎます。iOS 14.0以降の場合。
- **アクションボタン:** ユーザーがアクションボタンの構成ペインを見るのを防ぎます。iOS 17.0以降の場合。
- **ロックダウンモード:** Appleアカウントが設定されている場合、ユーザーがロックダウンモードのペインを見るのを防ぎます。iOS 17.1以降の場合。

- **インテリジェンス:** ユーザーがインテリジェンスのペインを見るのを防ぎます。iOS 18.0以降の場合。
- **カメラボタン:** ユーザーがカメラボタンのペインを見るのを防ぎます。iOS 18.0以降の場合。

ABMアカウントは**設定 > Apple Deployment Program**に表示されます。

7. 「**macOS設定アシスタントオプション**」で、ユーザーがデバイスを初めて起動するときにmacOS設定アシスタントがスキップする手順を選択します。画面がスキップされると、関連する機能はデフォルト設定を使用します。それらの機能へのアクセスを完全に制限しない限り、ユーザーはセットアップ完了後にスキップされた機能を構成できます。機能へのアクセスを制限する方法の詳細については、「制限デバイスポリシー」を参照してください。すべての項目のデフォルトはクリアされています。以下の説明は、設定が選択された場合に何が起こるかを説明しています。



- **新規として設定または復元:** ユーザーがデバイスを新規として設定したり、Time Machineバックアップから復元したり、システム移行を行ったりするのを防ぎます。
- **位置情報サービス:** ユーザーがデバイスで位置情報サービスを設定するのを防ぎます。macOS 10.11以降の場合。
- **Apple ID:** ユーザーがデバイス用の管理対象Apple IDアカウントを設定するのを防ぎます。
- **利用規約:** ユーザーがデバイスの使用に関する利用規約を読み、同意するのを防ぎます。
- **Siri:** ユーザーがSiriを構成するのを防ぎます。macOS 10.12以降の場合。

- **FileVault:** FileVaultを使用して起動ディスクを暗号化します。XenMobileは、システムに単一のローカルユーザーアカウントがあり、そのアカウントがiCloudにサインインしている場合にのみFileVault設定を適用します。

  macOS FileVaultディスク暗号化機能を使用して、システムボリュームの内容を暗号化することで保護できます(https://support.apple.com/ja-jp/HT204837)。FileVaultがオンになっていない後期モデルのポータブルMacで設定アシスタントを実行すると、この機能をオンにするよう求められる場合があります。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、システムに単一のローカル管理者アカウントがあり、そのアカウントがiCloudにサインインしている場合に限ります。
- **App解析:** ユーザーがクラッシュデータと使用状況統計をAppleと共有するかどうかを設定するのを防ぎます。
- **プライバシー:** ユーザーが「データとプライバシー」ペインを見るのを防ぎます。macOS 10.13以降の場合。
- **iCloud解析:** ユーザーが診断用iCloudデータをAppleに送信するかどうかを選択するのを防ぎます。macOS 10.13以降の場合。
- **iCloud書類とデスクトップ:** ユーザーがiCloudデスクトップと書類を設定するのを防ぎます。macOS 10.13以降の場合。
- **外観:** ユーザーが外観モードを選択するのを防ぎます。macOS 10.14以降の場合。
- **アクセシビリティ:** ユーザーがVoice Overを自動的に聞くのを防ぎます。デバイスがイーサネットに接続されている場合にのみ利用可能です。macOS 11以降の場合。
- **生体認証:** ユーザーがTouch IDとFace IDを設定するのを防ぎます。macOS 10.12.4以降の場合。
- **True Tone:** ユーザーが4チャンネルセンサーを設定して、ディスプレイのホワイトバランスを動的に調整するのを防ぎます。macOS 10.13.6以降の場合。
- **Apple Pay:** ユーザーがApple Payを設定するのを防ぎます。この設定がオフの場合、ユーザーはTouch IDとApple IDを設定する必要があります。**Apple ID**と**生体認証**の設定がオフになっていることを確認してください。macOS 10.12.4以降の場合。
- **スクリーンタイム:** ユーザーがスクリーンタイムを有効にするのを防ぎます。macOS 10.15以降の場合。
- **ローカルアカウント設定オプション:** デバイスに管理者アカウントを作成するための設定を指定します。ユーザーはこの情報を使用してmacOSデバイスにログインします。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。

- **プライマリアカウントを標準ユーザーとして作成:** このユーザーにデバイスの管理者権限を付与する代わりに、XenMobileは標準権限を持つユーザーを作成します。macOSは管理者アカウントを必要とするため、XenMobileはまず管理者アカウントを作成し、次に新しい標準アカウントを作成してそれをプライマリとして設定します。
- **管理者名 (フルネーム):** システムが管理者アカウントに表示する名前を入力します。
- **管理者名 (ショートネーム):** デバイスがホームフォルダおよびシェルに表示する名前を入力します。
- **管理者パスワード:** 管理者アカウントの安全なパスワードを入力します。
- **ユーザーとグループに管理者アカウントを表示:** オフの場合、管理者アカウントはmacOS設定の**ユーザーとグループ**に表示されません。プライマリアカウントを標準ユーザーとして作成する場合、この設定を有効にして、XenMobileが最初に作成する管理者アカウントを非表示にします。

Deployment Program対応デバイスの注文

Deployment Program対応デバイスは、Appleから直接、またはDeployment Program対応の正規販売店や通信事業者から注文できます。Appleから注文するには、Apple Deployment ProgramポータルでAppleカスタマーIDを提供します。カスタマーIDにより、Appleは購入したデバイスをApple Deployment Programアカウントに関連付けることができます。

販売店または通信事業者から注文するには、Appleの販売店または通信事業者に連絡して、Apple Deployment Programに参加しているかどうかを確認してください。デバイスを購入する際に、販売店のApple Deployment Program IDを尋ねてください。Apple Deployment Programアカウントに Apple Deployment Program販売店を追加する際、Appleはその情報を必要とします。販売店の Apple Deployment Program IDを追加すると、Deployment Programカスタマーが発行されます。このDeployment ProgramカスタマーIDを販売店に提供すると、販売店はそのIDを使用してデバイス購入に関する情報をAppleに送信します。詳細については、このApple Use Device Enrollmentサイトを参照してください。

Deployment Program対応デバイスの管理

注文が出荷された後、iOS、iPadOS、およびmacOSデバイスをXenMobile Serverに関連付けることができます。

1. 管理者またはデバイス登録マネージャーのアカウントを使用して、Apple Business Managerにサインインします。

2. サイドバーで、 をクリックします。Appleから直接購入したデバイスは自動的に表示されます。Apple Configurator 2からApple Business Managerにデバイスを割り当てるには、「Apple Business Managerユーザーガイド」を参照してください。
3. リストでデバイスまたはデバイスの総数を選択し、 をクリックします。2つのオプションがあります。

    - MDMサーバーにデバイスを割り当てるには、 でXenMobile Serverの名前を選択します。 をクリックします。

      新しいデバイスをApple Business Managerに一括で割り当てるには、展開用のデフォルトのXenMobile Serverを設定します。詳しくは、「一括登録のデフォルトサーバーを設定する」を参照してください。
    - XenMobile Serverからデバイスの割り当てを解除するには、 を選択します。

Apple Deployment Programデバイスが、選択したXenMobile Serverに関連付けられました。

iOS、iPadOS、またはmacOSデバイスを修理に出す場合、Apple Business Managerからデバイスを削除する必要があります。修理済みのデバイスが返却されたら、そのデバイスをXenMobile Serverに再割り当てする必要があります。デバイスを交換する場合は、注文番号を使用して新しいデバイスをXenMobile Serverに割り当てることができます。

割り当てられたデバイスの履歴を確認するには：

1. 管理者またはデバイス登録マネージャーのアカウントを使用して、Apple Business Manager にサインインします。
2. サイドバーで、 をクリックします。次に、割り当てを選択して詳細情報を表示します。
3. をクリックして、割り当て済みおよび未割り当てのすべてのデバイスのシリアル番号を含むCSVファイルをダウンロードします。

デバイスが販売された、盗難された、または修理できない場合は、Apple Business ManagerからiOS、iPadOS、およびmacOSデバイスを削除できます。

1. 管理者またはデバイス登録マネージャーのアカウントを使用して、Apple Business Manager にサインインします。
2. サイドバーで、 をクリックし、デバイスを検索します。
3. デバイスを選択し、**Release Device** をクリックします。ダイアログボックスで、プログラムからデバイスを削除するための変更を確定します。iOSおよびiPadOSデバイスを再度追加するには、Apple Configurator 2を使用します。macOSデバイスはApple Configurator 2で再度追加することはできません。

デバイスを登録する

ユーザーデバイスをリモートで安全に管理するには、XenMobileにユーザーデバイスを登録します。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IDが認証されます。その後、XenMobileとユーザープロファイルがインストールされます。次に、XenMobileコンソールでデバイス管理タスクを実行できます。ポリシーを適用したり、アプリを展開したり、デバイスにデータをプッシュしたり、紛失または盗難されたデバイスをロック、ワイプ、および検索したりできます。

Azure Active Directoryへの登録は、iOS、Android、Windows 10、およびWindows 11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の詳細については、「XenMobile Integration with Azure Active Directory as IdP」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。詳細については、「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**ページに移動します。詳細については、この記事の「登録招待を送信する」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、Citrix Secure Hub™アプリをダウンロードして、アプリをタップします。
2. アプリのインストールを求められたら、**次へ**をクリックし、**インストール**をクリックします。
3. Secure Hubのインストール後、**開く**をタップします。
4. XenMobile Server名、ユーザープリンシパル名（UPN）、またはメールアドレスなどの企業資格情報を入力します。次に、**次へ**をクリックします。
5. **デバイス管理者権限を有効にする**画面で、**有効にする**をタップします。

6. 企業パスワードを入力し、**サインオン**をタップします。
7. XenMobile の構成方法によっては、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 や Secure Mail、Citrix Files などの XenMobile 対応アプリにサインオンできます。Citrix PIN を 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 にアクセスして、Android デバイスにインストールできるアプリを表示できます。
9. XenMobile を構成して、登録後にアプリをデバイスに自動的にプッシュするように設定している場合、ユーザーはアプリのインストールを求められます。また、XenMobile で構成したポリシーがデバイスに展開されます。アプリをインストールするには、**［インストール］**をタップします。

Android デバイスの登録解除と再登録

ユーザーは Secure Hub 内から登録解除できます。ユーザーが以下の手順を使用して登録解除しても、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たままになります。ただし、デバイスに対してアクションを実行することはできません。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 アプリを開くにはタップします。
2. スマートフォンまたはタブレットのどちらを使用しているかに応じて、次の操作を行います。

   スマートフォンの場合：

   - 画面の左端からスワイプして、設定ペインを開きます。
   - **［設定］をタップし、［アカウント］をタップしてから、［アカウントの削除］**をタップします。

   タブレットの場合：

   - 右上隅にあるメールアドレスの横の矢印をタップします。
   - **［設定］をタップし、［アカウント］をタップしてから、［アカウントの削除］**をタップします。

3. **［再登録］**をタップします。デバイスを再登録すること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。

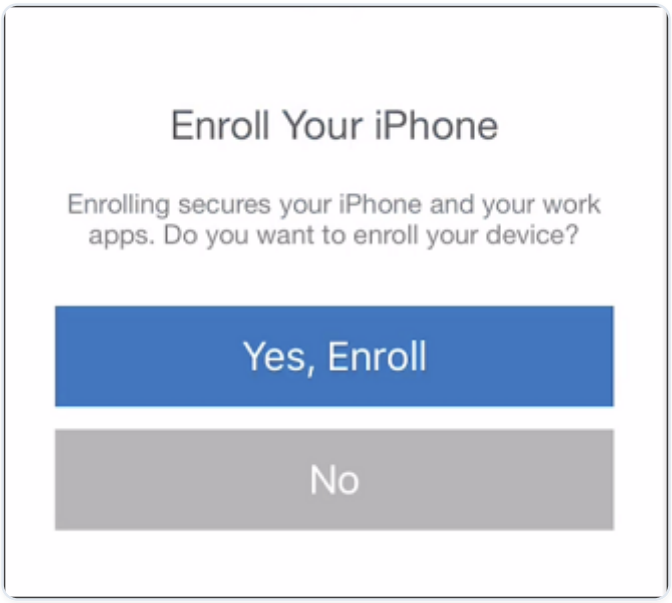
   デバイスの登録が解除されました。
5. 画面の指示に従って、デバイスを再登録してください。

iOSデバイスを登録する

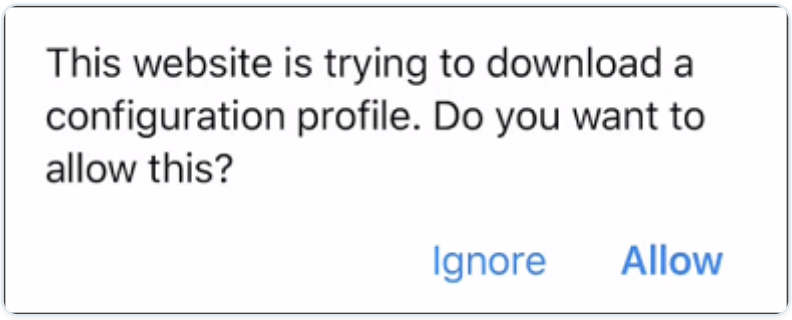
このセクションでは、ユーザーがiOSデバイス（12.2以降）をXenMobile Serverに登録する方法について説明します。iOS登録の詳細については、次のビデオを開いてください。



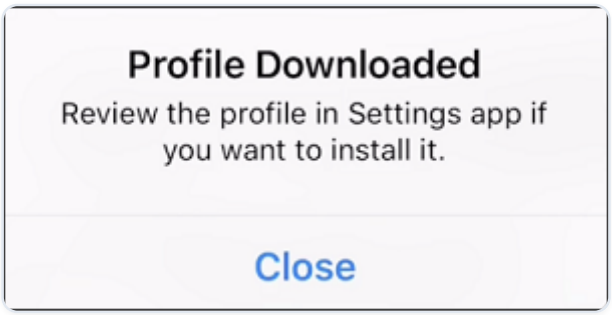
1. iOSデバイスでApple Storeにアクセスし、Citrix Secure Hubアプリをダウンロードして、アプリをタップします。
2. アプリのインストールを求められたら、**次へ**をタップし、**インストール**をタップします。
3. Secure Hubのインストール後、**開く**をタップします。
4. XenMobile Server名、ユーザープリンシパル名（UPN）、またはメールアドレスなどの企業資格情報を入力します。次に、**次へ**をクリックします。
5. iOSデバイスを登録するには、**はい、登録**をタップします。



6. 資格情報を入力した後、プロンプトが表示されたら**許可**をタップして、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リストに追加します。

   - **設定 > 一般 > 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。

     プロファイルを追加(/en-us/xenmobile/server/media/simpler-enrollment-ios-4.png)

   - 通知ウィンドウで、**信頼** をタップしてデバイスをリモート管理に登録します。

     信頼設定(/en-us/xenmobile/server/media/simpler-enrollment-ios-5.png)

9. Secure Hubにサインインします。MDM+MAMに登録する場合：資格情報が検証された後、プロンプトが表示されたらCitrix PINを作成して確認します。
10. ワークフローが完了すると、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て、iOSデバイスにインストールできるアプリを表示できます。

iOSデバイス

1. デバイスのApple iTunes App StoreからSecure Hubアプリをダウンロードし、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アプリが開いたら、ヘルプデスクから提供されたサーバーアドレスを入力します。

   表示される画面は、XenMobileの構成方法によって、これらの例とは異なる場合があります。
4. プロンプトが表示されたら、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. 登録を促されたら、**はい、登録** をクリックし、プロンプトが表示されたら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 Servicesをインストールします。

   Citrix Profile Services画面の画像(/en-us/xenmobile/server/media/worxhome-enroll-5.png)
7. **信頼**をタップします。

   リモート管理の信頼画面の画像(/en-us/xenmobile/server/media/worxhome-enroll-8.png)
8. **開く**をタップし、資格情報を入力します。

macOSデバイス

XenMobileは、macOSを実行しているデバイスを登録するための2つの方法を提供します。どちらの方法でも、macOSユーザーはデバイスから直接、ワイヤレスで登録できます。

- **ユーザーに登録招待状を送信する:** この登録方法では、macOSデバイスに対して以下のいずれかの登録セキュリティモードを設定できます。
  - ユーザー名 + パスワード
  - ユーザー名 + PIN
  - 2要素認証

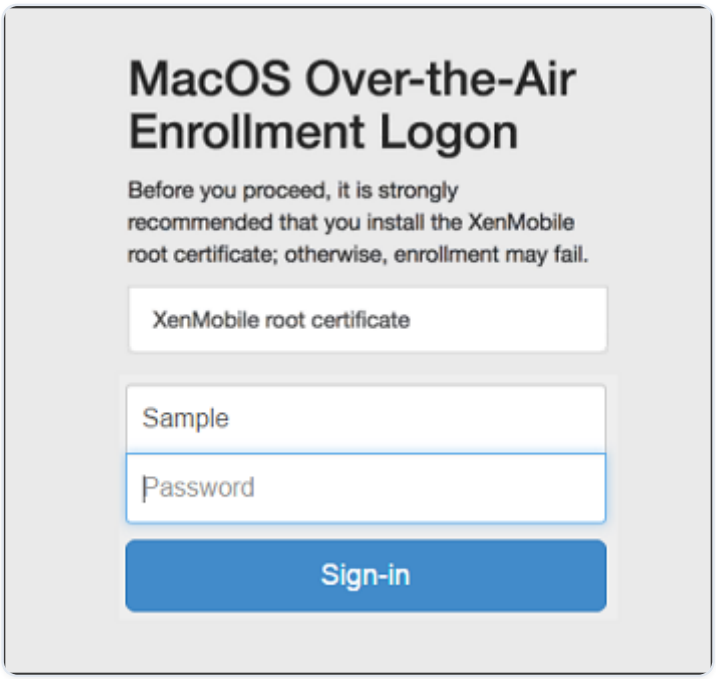
  ユーザーが登録招待状の指示に従うと、ユーザー名が入力済みのサインオン画面が表示されます。

- **ユーザーにインストールリンクを送信する:** macOSデバイス向けのこの登録方法では、ユーザーに登録リンクが送信され、ユーザーはそのリンクをSafariまたはChromeブラウザで開くことができます。その後、ユーザーはユーザー名とパスワードを入力して登録します。

  macOSデバイスで登録リンクの使用を防止するには、サーバープロパティ**Enable macOS OTAE**を**false**に設定します。その結果、macOSユーザーは登録招待状を使用することによってのみ登録できます。

ユーザーに登録招待状を送信する

1. 必要に応じて、XenMobileコンソールでmacOSデバイスポリシーを設定します。デバイスポリシーの詳細については、「デバイスポリシー」を参照してください。
2. macOSユーザー登録の招待を追加します。詳細については、この記事の「登録招待を送信する」を参照してください。
3. ユーザーが招待を受け取り、リンクをクリックすると、Safariブラウザに次の画面が表示されます。XenMobileはユーザー名を入力します。登録セキュリティモードで**Two Factor**を選択した場合、別のフィールドが表示されます。



4. ユーザーは必要に応じて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促すプロンプトが表示されるかどうかは、macOS用に次のものを構成したかどうかによって異なります。公開信頼されたSSL証明書と公開信頼されたデジタル署名証明書。証明書の詳細については、「証明書と認証」を参照してください。
5. ユーザーは要求された資格情報を提供します。

Mac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の管理を開始できます。

ユーザーにインストールリンクを送信する

1. 必要に応じて、XenMobileコンソールでmacOSデバイスポリシーを設定します。デバイスポリシーの詳細については、「デバイスポリシー」を参照してください。
2. ユーザーがSafariまたはChromeブラウザで開くことができる登録リンク`https://serverFQDN:8443/instanceName/macos/otae`を送信します。

   - **serverFQDN**は、XenMobileを実行してい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た場合は、8443の代わりにそのポートを使用してください。
   - **instanceName**は、zdmとして表示されることが多く、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の詳細については、「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. ユーザーは必要に応じて証明書をインストールします。iOSおよびmacOS用に公開信頼されたSSL証明書とデジタル署名証明書を構成した場合、ユーザーには証明書のインストールを促すプロンプトが表示されます。証明書の詳細については、「証明書と認証」を参照してください。
4. ユーザーはMacにサインオンします。

   Macデバイスの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の管理を開始できます。

Windowsデバイス

Windows 10およびWindows 11デバイスは、Active Directory認証のフェデレーション手段としてAzureに登録されます。Windows 10およびWindows 11デバイスをMicrosoft Azure ADに参加させるには、次のいずれかの方法があります。

- デバイスの電源を初めてオンにしたときに、Azure AD Joinの一部としてMDMに登録する。
- デバイスの構成後、Windowsの設定ページからAzure AD Joinの一部としてMDMに登録する。

次のWindowsオペレーティングシステムを実行しているデバイスをXenMobileに登録できます。

- ウィンドウズ 10

- ウィンドウズ 11

ユーザーは自分のデバイスから直接登録できます。

> **注：**
>
> Windows 10 RS2 PhoneおよびTabletの場合、再登録時にユーザーはサーバーURLの入力を求められません。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、**サービスに接続中**の横にあるXをタップして、サーバーURLページに移動します。これはサードパーティの問題です。

> サポートされているWindowsデバイスの管理を有効にするには、ユーザー登録のためにAutoDiscoveryとWindows検出サービスを構成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、XenMobileでMicrosoft Azureサーバー設定を構成する必要があります。詳細については、「Microsoft Azure Active Directoryサーバー設定」を参照してください。

自己検出で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 ServiceとWindows検出サービスを構成することをお勧めします。詳細については、「XenMobile AutoDiscovery Service」を参照してください。

1. デバイスで、利用可能なすべてのWindows Updateを確認してインストールします。
2. チャームメニューで、**設定**をタップし、次に**アカウント > 職場または学校にアクセス > 職場または学校に接続**をタップします。
3. Windows 10およびWindows 11の場合: 会社のメールアドレスを入力し、**続行**をタップします。Windows 8.1の場合: **デバイス管理をオンにする**をタップします。ローカルユーザーとして登録するには、正しいドメイン名を持つ存在しないメールアドレス（例: `foo@mydomain.com`）を入力します。これにより、Windowsの組み込みデバイス管理によって登録が行われるという既知のMicrosoftの制限を回避できます。**サービスに接続中**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ているユーザー名とパスワードを入力します。デバイスは自動的にXenMobile Serverを検出し、登録プロセスを開始します。
4. パスワードを入力します。XenMobileのユーザーグループに属するアカウントに関連付けられているパスワードを使用します。
5. Windows 10およびWindows 11の場合: **利用規約**ダイアログボックスで、デバイスの管理に同意することを示し、**同意する**をタップします。Windows 8.1の場合: **IT管理者からのアプリと**

サービスを許可ダイアログボックスで、デバイスの管理に同意することを示し、**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

AutoDiscoveryなしでWindowsデバイスを登録することは可能です。ただし、CitrixはAutoDiscoveryを構成することを推奨します。AutoDiscoveryなしでの登録は、目的のURLに接続する前にポート80への呼び出しが発生するため、本番環境での展開にはベストプラクティスとは見なされません。Citrixは、このプロセスをテスト環境および概念実証の展開でのみ使用することを推奨します。

1. デバイスで、利用可能なすべてのWindows Updateを確認してインストールします。
2. Windows 10およびWindows 11の場合: チャームメニューで、**設定**をタップし、次に**アカウント > 職場または学校にアクセス > 職場または学校に接続**をタップします。Windows 8.1の場合: **PC設定 > ネットワーク > 職場**をタップします。
3. 会社のメールアドレスを入力します。
4. Windows 10およびWindows 11の場合: AutoDiscovery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的に検出**が**オン**に設定されている場合は、タップしてオプションを**オフ**にします。
5. Windows 10およびWindows 11の場合、**サーバーアドレスを入力**フィールドに、アドレス: `https://serverfqdn:8443/serverInstance/wpe`を入力します。

   認証されていないSSL接続に8443以外のポートが使用されている場合は、このアドレスの8443の代わりにそのポート番号を使用します。

   Windows 8.1の場合: 次の形式でサーバーアドレスを入力します: `https://serverfqdn:8443/serverInstance/Discovery.svc`。

   認証されていないSSL接続に8443以外のポートが使用されている場合は、このアドレスの8443の代わりにそのポート番号を使用します。
6. パスワードを入力します。
7. Windows 10およびWindows 11の場合: **Terms of use**ダイアログボックスで、デバイスの管理に同意することを示し、**Accept**をタップします。Windows 8.1の場合: **Allow apps and services from IT admin**ダイアログボックスで、デバイスの管理に同意することを示し、**Turn on**をタップします。

登録招待状を送信する

XenMobileコンソールでは、iOS、macOS、Android Enterprise、およびレガシーAndroidデバイスを使用しているユーザーに登録招待状を送信できます。また、iOS、Android Enterprise、またはレガシー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。

登録招待状は次のように送信されます。

- 登録招待状がローカルユーザーまたはActive Directoryユーザー1名宛ての場合: ユーザーは、指定した電話番号と通信事業者名でSMSから招待状を受け取ります。
- 登録招待状がグループ宛ての場合: ユーザーはSMSから招待状を受け取ります。Active DirectoryユーザーがActive Directoryにメールアドレスと携帯電話番号を登録している場合、招待状を受け取ります。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状を受け取ります。

ユーザーが登録すると、デバイスは**管理 > デバイス**に管理対象として表示されます。招待URLのステータスは**引き換え済み**と表示されます。

前提条件

- Enterprise (XME) またはMDMモードで構成されたXenMobile Server
- LDAPが構成されていること
- ローカルグループとローカルユーザーを使用する場合:
  - 1つ以上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がローカルグループに関連付けられていること。
- Active Directoryを使用する場合：
  - デリバリーグループはActive Directoryグループに関連付けられています。

登録招待を作成する

1. XenMobileコンソールで、 **>** をクリックします。 ページが表示されます。

   XenMobileコンソールの登録招待ページの画像(/en-us/xenmobile/server/media/manage-enrollment-invitations.png)
2. 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。

招待の追加メニューの画像(/en-us/xenmobile/server/media//manage-enrollment-invitations-add-menu.png)

- ユーザーまたはグループに登録招待を送信するには、 をクリックします。
- SMTPまたはSMS経由で受信者リストに登録インストールリンクを送信するには、 をクリックします。

登録招待とインストールリンクの送信については、これらの手順の後に説明します。

3. をクリックします。 画面が表示されます。

登録招待画面の画像(/en-us/xenmobile/server/media/manage-enrollment-invitation-new.png)

4. 次の設定を構成します。

- **受信者:** または を選択します。
- **プラットフォームの選択:** が の場合、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を変更できます。 が の場合、プラットフォームは選択されません。プラットフォームを選択します。

  Android Enterpriseデバイスの登録招待を作成するには、**Android > Android Enterprise**を選択します。
- **デバイスの所有権: 企業**または**従業員**を選択します。

ユーザーまたはグループの設定が、以下のセクションで説明されているように表示されます。

ユーザーに登録招待を送信するには

登録招待設定の画像(/en-us/xenmobile/server/media/manage-enrollment-invitation-user.png)

1. 次の**ユーザー**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にローカルユーザーとして、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。ユーザーがローカルの場合、そのユーザーに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てください。ユーザーがActive Directoryにいる場合は、LDAPが構成されていることを確認してください。
- **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、デバイスの対応する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。必要に応じて、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:** ユーザーの登録セキュリティモードを選択します。デフォルトは**ユーザー名 + パスワード**です。以下のオプションの一部は、すべてのプラットフォームで利用できるわけではありません。
  - ユーザー名 + パスワード
  - 高セキュリティ
  - 招待URL
  - 招待URL + PIN
  - 招待URL + パスワード
  - 2要素
  - ユーザー名 + PIN

登録招待を送信するには、「**招待URL**」、「**招待URL + PIN**」、または「**招待URL + パスワード**」の登録セキュリティモードのみを使用できます。「**ユーザー名 + パスワード**」、「**2要素**」、または「**ユーザー名 + PIN**」で登録するデバイスの場合、ユーザーはSecure Hubで手動で資格情報を入力する必要があります。

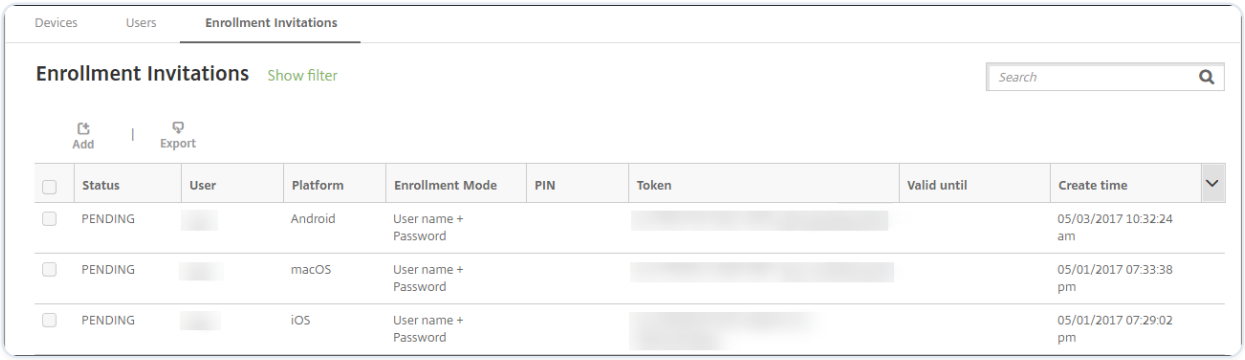
登録用PINはワンタイムPINとも呼ばれます。このようなPINは、ユーザーが登録するときにのみ有効です。

> **注：**
>
> PINを含む登録セキュリティモードを選択すると、「**登録PINのテンプレート**」フィールドが表示され、そこで「**登録PIN**」をクリックします。

- **エージェントダウンロードのテンプレート：** 「**ダウンロードリンク**」という名前のダウンロードリンク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に対応しています。
- **登録URLのテンプレート：** 「**登録招待**」を選択します。
- **登録確認のテンプレート：** 「**登録確認**」を選択します。

- **有効期限：** このフィールドは、登録モードを構成するときに設定され、登録の有効期限を示します。登録セキュリティモードの構成の詳細については、「登録セキュリティモードの構成」を参照してください。
- **最大試行回数：** このフィールドは、**登録モード**を構成するときに設定され、登録プロセスが実行される最大回数を示します。登録セキュリティモードの構成の詳細については、「登録セキュリティモードの構成」を参照してください。
- **招待を送信：** 招待をすぐに送信するには「**ON**」を選択します。招待を「**登録招待**」ページのテーブルに追加するが送信しない場合は「**OFF**」を選択します。

2. 「**招待を送信**」を有効にした場合は、「**保存して送信**」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。招待は「**登録招待**」ページのテーブルに表示されます。



グループに登録招待を送信するには

次の図は、グループへの登録招待を設定するための設定を示しています。

グループへの登録招待ページを示す画像(/en-us/xenmobile/server/media/manage-enrollment-invitation-group.png)

1. 次の設定を構成します。

- **ドメイン:** 招待を受け取るグループのドメインを選択します。
- **グループ:** 招待を受け取るグループを選択します。
- **登録モード:** グループ内のユーザーをどのように登録するかを選択します。デフォルトは**ユーザー名 + パスワード**です。以下のオプションの一部は、すべてのプラットフォームで利用できるわけではありません。
  - ユーザー名 + パスワード
  - 高セキュリティ
  - 招待URL
  - 招待URL + PIN

- 招待URL + パスワード
- 2要素認証
- ユーザー名 + PIN

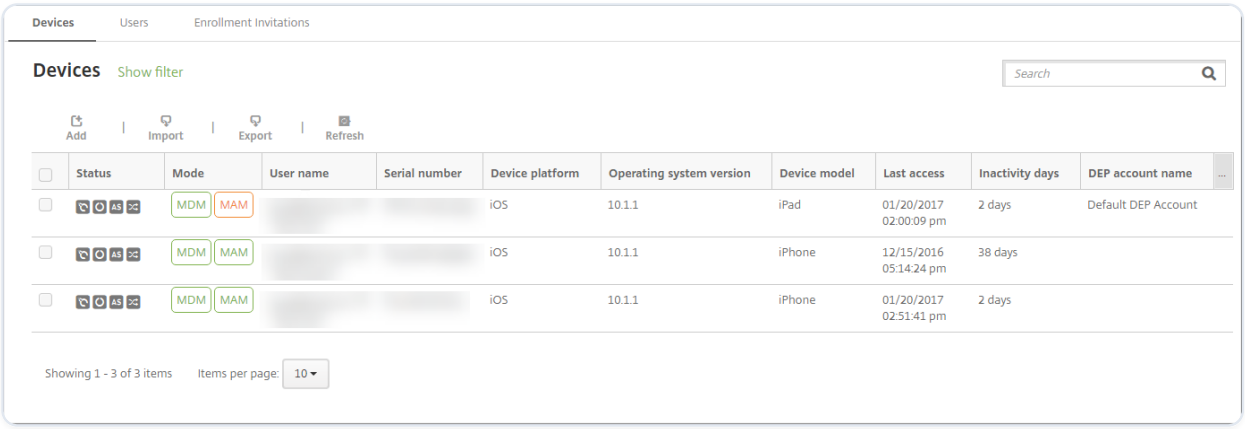
登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードのみを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはSecure Hubで資格情報を手動で入力する必要があります。

選択した各プラットフォームに有効な登録セキュリティモードのみが表示されます。

> **注：**
>
> PINを含む登録セキュリティモードを選択すると、**登録PIN**をクリックした場所に**登録PINのテンプレート**フィールドが表示されます。

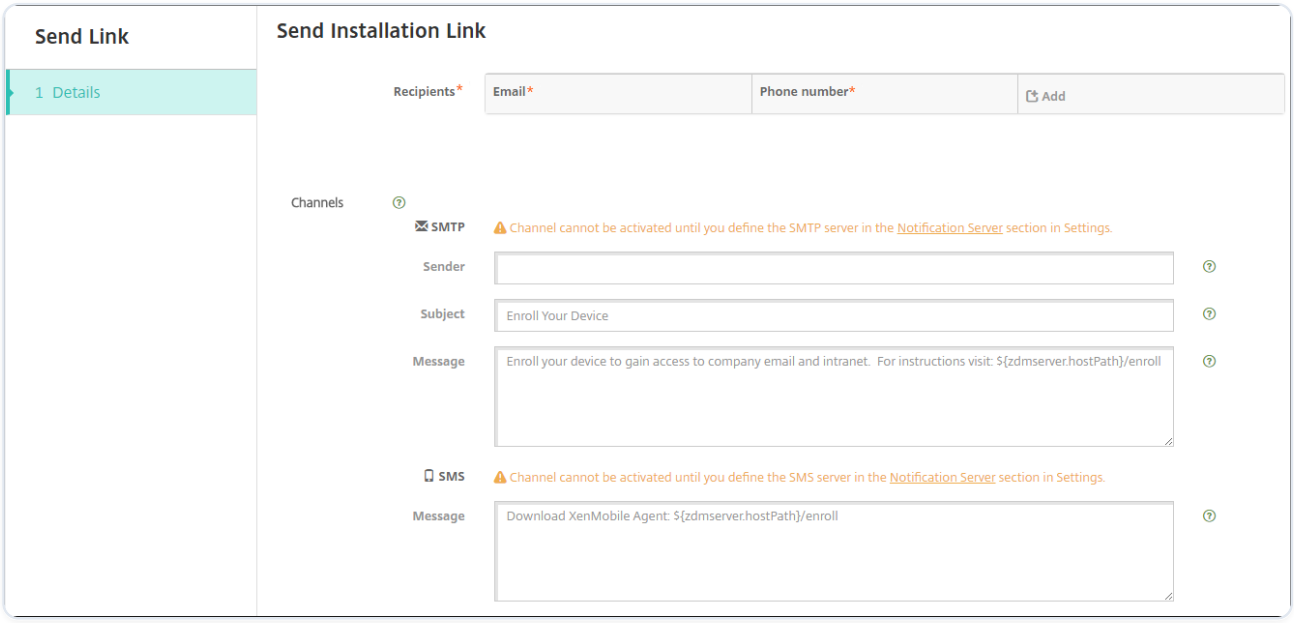
- **エージェントダウンロードのテンプレート：** 「**ダウンロードリンク：**」という名前のダウンロードリンクトテンプレートを選択します。このテンプレートは、サポートされているすべてのプラットフォーム用です。
- **登録URLのテンプレート：** 「**登録招待**」を選択します。
- **登録確認のテンプレート：** 「**登録確認**」を選択します。
- **有効期限：** このフィールドは、登録モードを構成するときに設定され、登録の有効期限を示します。登録セキュリティモードの構成について詳しくは、「登録セキュリティモードの構成」を参照してください。
- **最大試行回数：** このフィールドは、登録モードを構成するときに設定され、登録プロセスが実行される最大回数を示します。登録セキュリティモードの構成について詳しくは、「登録セキュリティモードの構成」を参照してください。
- **招待状を送信：** 招待状をすぐに送信するには、**ON**を選択します。招待状を**登録招待**ページのテーブルに追加するが、送信しない場合は、**OFF**を選択します。

2. **招待状を送信**を有効にした場合は、**保存して送信**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。招待状は、**登録招待**ページのテーブルに表示されます。



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**ページから通知サーバーでチャネル（SMTPまたはSMS）を構成する必要があります。詳細については、「通知」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。

   - **受信者:** 追加する受信者ごとに、**追加**をクリックし、次の操作を行います。
     - **メール:** 受信者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:** 受信者の電話番号を入力します。このフィールドは必須です。

> **注:**
>
> 既存の受信者を削除するには、リストがある行にカーソルを合わせ、右側にあるゴミ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表示されます。リストを削

> 除するには**削除**をクリックするか、リストを保持するには**キャンセル**をクリックします。

> 既存の受信者を編集するには、リストがある行にカーソルを合わせ、右側にあるペンアイコンをクリックします。リストを更新し、変更されたリストを保存するには**保存**をクリックするか、リストを変更しないままにするには**キャンセル**をクリックします。

- **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。**SMTP**または**SMS**で通知を送信できます。これらのチャネルは、**Notification Server**の**設定**ページでサーバー設定を構成するまでアクティブ化できません。詳細については、「通知」を参照してください。
- **SMTP:** これらのオプション設定を構成します。これらのフィールドに何も入力しない場合、選択したプラットフォーム用に構成された通知テンプレートで指定されたデフォルト値が使用されます。
  - **送信者:** オプションの送信者を入力します。
  - **件名:** メッセージのオプションの件名を入力します。例: 「デバイスを登録してください」
  - **メッセージ:** 受信者に送信するオプションのメッセージを入力します。例: 「組織のアプリとメールにアクセスするには、デバイスを登録してください」
- **SMS:** こ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、選択したプラットフォーム用に構成された通知テンプレートで指定されたデフォルト値が使用されます。
  - **メッセージ:** 受信者に送信するメッセージを入力します。このフィールドはSMSベースの通知に必須です。

> **注:** 北米では、160文字を超えるSMSメッセージは、複数のメッセージに分割して配信されます。

2. **送信**をクリックします。

> **注：**

> 環境でsAMAccountNameを使用している場合：ユーザーが招待を受け取り、リンクをクリックした後、認証を完了するためにユーザー名を編集する必要があります。ユーザー名は`sAMAccountName@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。

プラットフォーム別の登録セキュリティモード

以下の表は、ユーザーデバイスの登録に使用できるセキュリティモードを示しています。表中の**はい**は、特定の登録および管理モードを異なる登録プロファイルでサポートするデバイスプラットフォームを示します。

MDM登録セキュリティモード	CITRIX GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルのサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
Citrix Cloud™を介したIDプロバイダーとしてのAzure ADおよびOkta	クライアント証明書	MDM+MAM またはMDM	はい	はい	はい	はい	はい	いいえ	いいえ
ユーザー	LDAP、	MDM+MA	はい	はい	はい	はい	はい	はい	はい

MDM登録セキュリティモード	CITRIX GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルのサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
名 + パスワード	LDAP + クライアント証明書、およびクライアント証明書のみ	M、MDM、またはMAM (MAM専用モードはCitrix Gatewayでクライアント証明書をサポートしていません)							
招待URL	クライアント証明書	MDM+MAM またはMDM	はい	はい	はい	いいえ	はい	いいえ	いいえ

MDM登録セキュリティモード	CITRIX GATEWAY上のMAM登録セキュリティモード	管理モード	異なる登録プロファイルのサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
招待URL + PIN	クライアント証明書	MDM+MAM またはMDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
招待URL + パスワード	LDAP、LDAP + クライアント証明書、およびクライアント証明書のみ	MDM+MAM またはMDM	はい	はい	はい	いいえ	はい	いいえ	いいえ
2要素認証 (ユーザー名 + パスワー	LDAP、LDAP + クライアント	MDM+MAM またはMDM	はい	はい	はい	いいえ	はい	はい	いいえ

MDM 登録セキュリティモード	CITRIX GATEWAY上の MAM 登録セキュリティモード	管理モード	異なる登録プロファイルのサポート	ANDROID (レガシー)	アンドロイドエンタープライズ	IOS (ユーザー登録モード)	IOS	MACOS	ウィンドウズ
ド + PIN)	証明書、およびクライアント証明書のみ								
ユーザー名 + PIN	クライアント証明書	MDM +MAM または MDM	はい	はい	はい	いいえ	はい	はい	いいえ

iOS、Android、および Android Enterprise デバイスでの登録セキュリティモードの動作を以下に示します。

- **ユーザー名 + パスワード** (デフォルト)
  - ユーザーに登録 URL を含む単一の通知を送信します。ユーザーがその URL をクリックすると、Secure Hub が開きます。その後、ユーザーはユーザー名とパスワードを入力して、デバイスを XenMobile に登録します。
- **招待 URL**
  - ユーザーに登録 URL を含む単一の通知を送信します。ユーザーがその URL をクリックすると、Secure Hub が開きます。XenMobile Server の名前と **はい、登録** ボタンが表示されます。ユーザーは **はい、登録** をタップして、デバイスを XenMobile に登録します。

- **招待 URL + PIN**
  - ユーザーに以下のメールを送信します。
    - ユーザーがSecure Hubを介してXenMobileにデバイスを登録できる登録URLを含むメール。
    - ユーザーがデバイスを登録する際に、ユーザーのActive Directory（またはローカル）パスワードとともに、入力する必要があるワンタイムPINを含むメール。
  - このモードでは、ユーザーは通知内の登録URLを使用するだけで登録します。ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待を送信することはできます。
- **招待URL + パスワード**
  - 登録URLを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Secure Hubが開きます。XenMobileサーバー名が表示され、ユーザーがパスワードを入力できるフィールドも表示されます。
- **2要素認証**
  - 登録URLとワンタイムPINを含む単一の通知をユーザーに送信します。ユーザーがURLをクリックすると、Secure Hubが開きます。XenMobileサーバー名が表示され、ユーザーがパスワードとPIN番号を入力できる2つのフィールドも表示されます。
- **ユーザー名 + PIN**
  - ユーザーに以下のメールを送信します。
    - ユーザーがSecure Hubをダウンロードしてインストールできる登録URLを含むメール。Secure Hubが開いた後、ユーザーはXenMobileにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。
    - ユーザーがデバイスを登録する際に、ユーザーのActive Directory（またはローカル）パスワードとともに、入力する必要があるワンタイムPINを含むメール。
  - ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待を送信することはできます。

以下に、macOSデバイスでの登録セキュリティモードの動作について説明します。

- **ユーザー名 + パスワード**

    - ユーザーに登録URLを含む単一の通知を送信します。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーはXenMobileにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。

- **2要素認証**
    - ユーザーに登録URLとワンタイムPINを含む単一の通知を送信します。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーはパスワードとPIN番号を入力できる2つのフィールドが表示されます。
- **ユーザー名 + PIN**
    - ユーザーに以下のメールを送信します:
        - 登録URLを含むメール。ユーザーがURLをクリックすると、Safariブラウザが開きます。サインインページが表示され、ユーザーはXenMobileにデバイスを登録するためにユーザー名とパスワードを入力するよう求められます。
        - デバイスを登録する際にユーザーが入力する必要があるワンタイムPINと、ユーザーのActive Directory（またはローカル）パスワードを含むメール。
    - ユーザーが通知招待を紛失した場合、登録できません。ただし、別の招待を送信することはできます。

Windowsデバイスに登録招待を送信することはできません。Windowsユーザーはデバイスから直接登録します。

Firebase Cloud Messaging

> **注記:**
>
> Firebase Cloud Messaging (FCM) は、以前は Google Cloud Messaging (GCM) と呼ばれていました。XenMobile® コンソールの一部のラベルやメッセージでは、GCM の用語が使用されています。

> Citrix® は、Android デバイスが XenMobile に接続する方法とタイミングを制御するために、Firebase Cloud Messaging (FCM) を使用することを推奨しています。XenMobile は、FCM 用に構成されている場合、FCM が有効になっている Android デバイスに接続通知を送信しま

> す。セキュリティアクションまたは展開コマンドは、プッシュ通知をトリガーして、ユーザーに XenMobile Server への再接続を促します。

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 の FCM サービスに登録されます。この接続により、FCM を使用して XenMobile Service からデバイスへのほぼリアルタイムの通信が可能になります。FCM 登録は、新規デバイス登録と以前に登録されたデバイスの両方で機能します。

XenMobile がデバイスへの接続を開始する必要がある場合、FCM サービスに接続します。その後、FCM サービスはデバイスに接続するよう通知します。この種の接続は、Apple がプッシュ通知サービスに使用しているものと似ています。

前提条件

- 最新のSecure Hubクライアント
- Google 開発者アカウントの資格情報
- FCM が有効な Android デバイスに Google Play サービスがインストールされていること

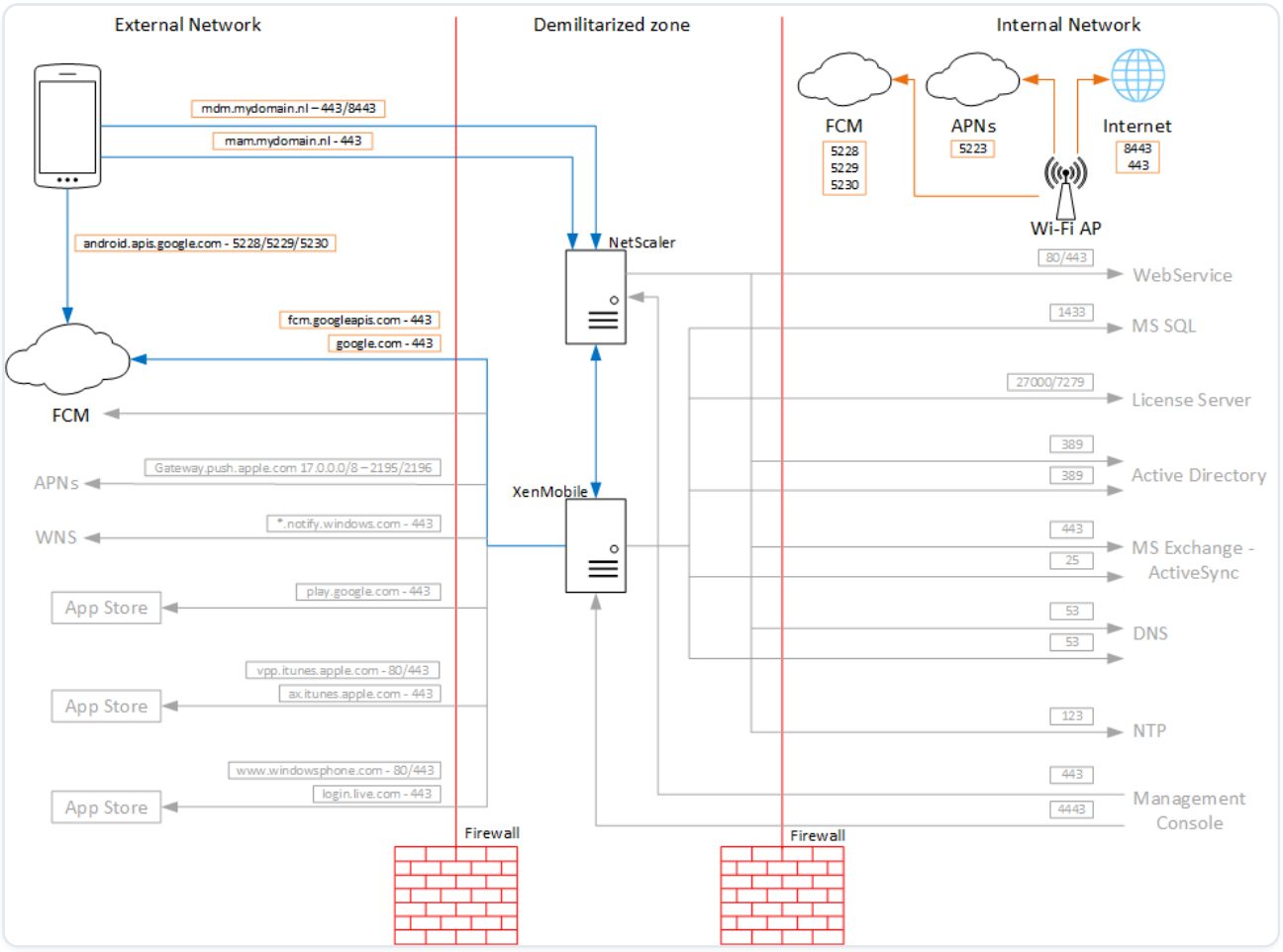
ファイアウォールポート

- XenMobile でポート 443 を `fcm.googleapis.com` および `Google.com` に開きます。
- デバイスの Wi-Fi の発信インターネット通信をポート 5228、5229、および 5230 で開きます。
- 発信接続を許可するには、FCM は IP 制限なしでポート 5228 から 5230 を許可することを推奨しています。ただし、IP 制限が必要な場合は、FCM は IPv4 および IPv6 ブロック内のすべての IP アドレスを許可することを推奨しています。これらのブロックは、Google の ASN of 15169 に記載されています。そのリストは毎月更新してください。FCM ポートの詳細については、Google の FCM ports に関するドキュメントを参照してください。

詳細については、ポート要件 を参照してください。

アーキテクチャ

この図は、外部ネットワークと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。

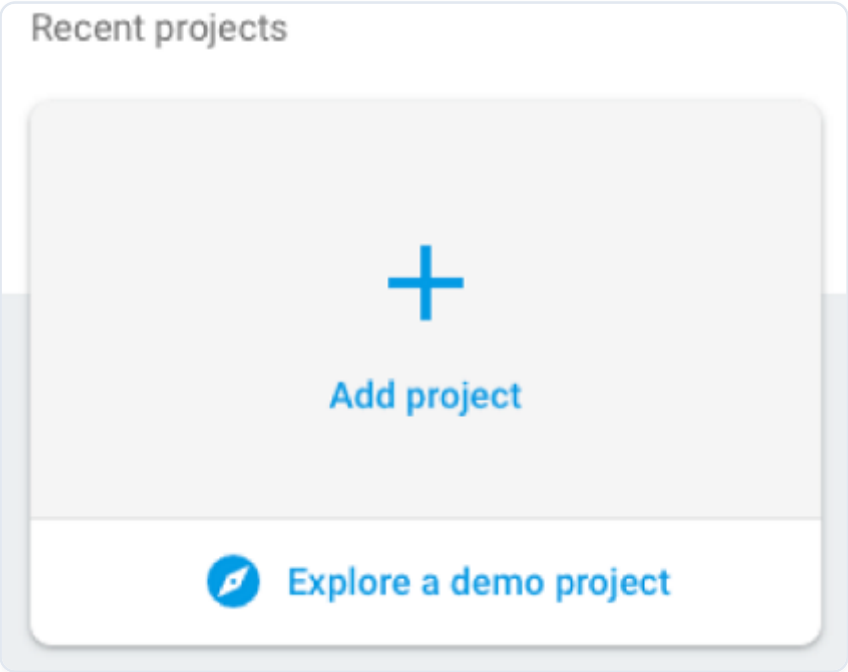


FCM用にGoogleアカウントを構成するには

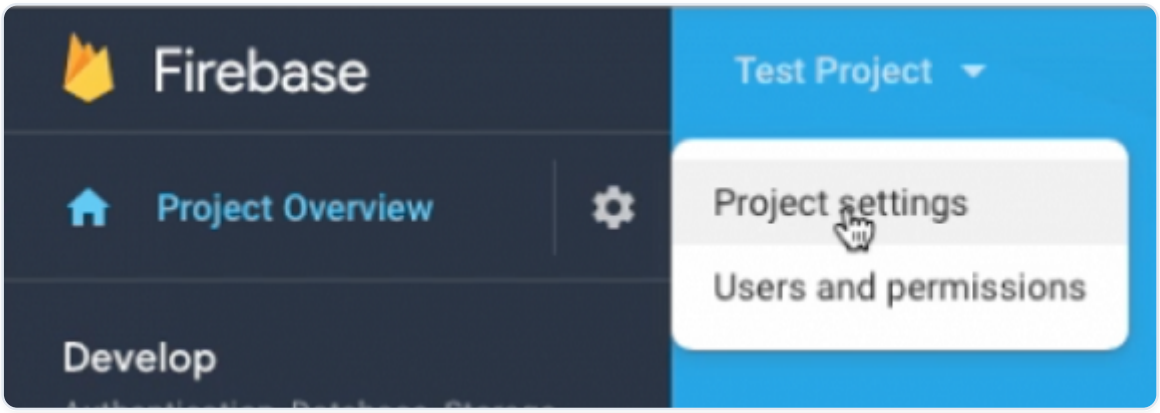
1. Google開発者アカウントの資格情報を使用して、次のURLにサインインします。

   `<https://console.firebase.google.com/>`

2. **プロジェクトを追加**をクリックします。



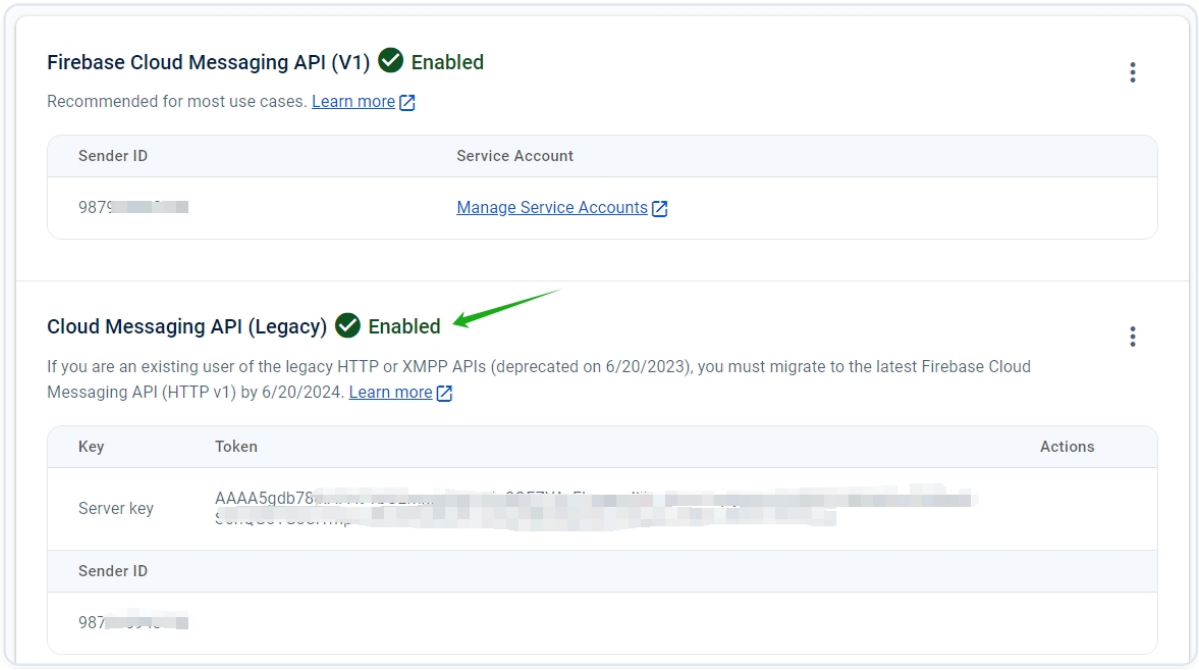
3. プロジェクトを作成したら、**プロジェクト設定**をクリックします。



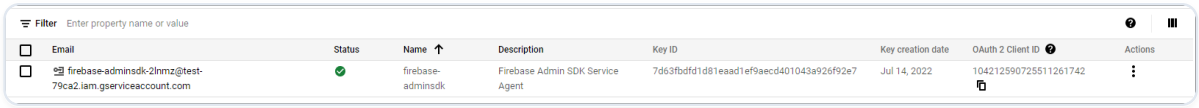
> **注：**
>
> Googleは、現在FCMの実装で使用されているHTTP用のFCMレガシーAPIを非推奨にする予定です。移行期限はJune 21, 2024です。FCMをレガシーFCM APIからHTTP v1 APIに移行する必要があります。詳細については、レガシーFCM APIからHTTP v1に移行するを参照してください。

4. **Cloud Messaging**タブをクリックします。Firebase Cloud Messaging APIが有効になっていることを確認し、**サービスアカウントの管理**をクリックします。

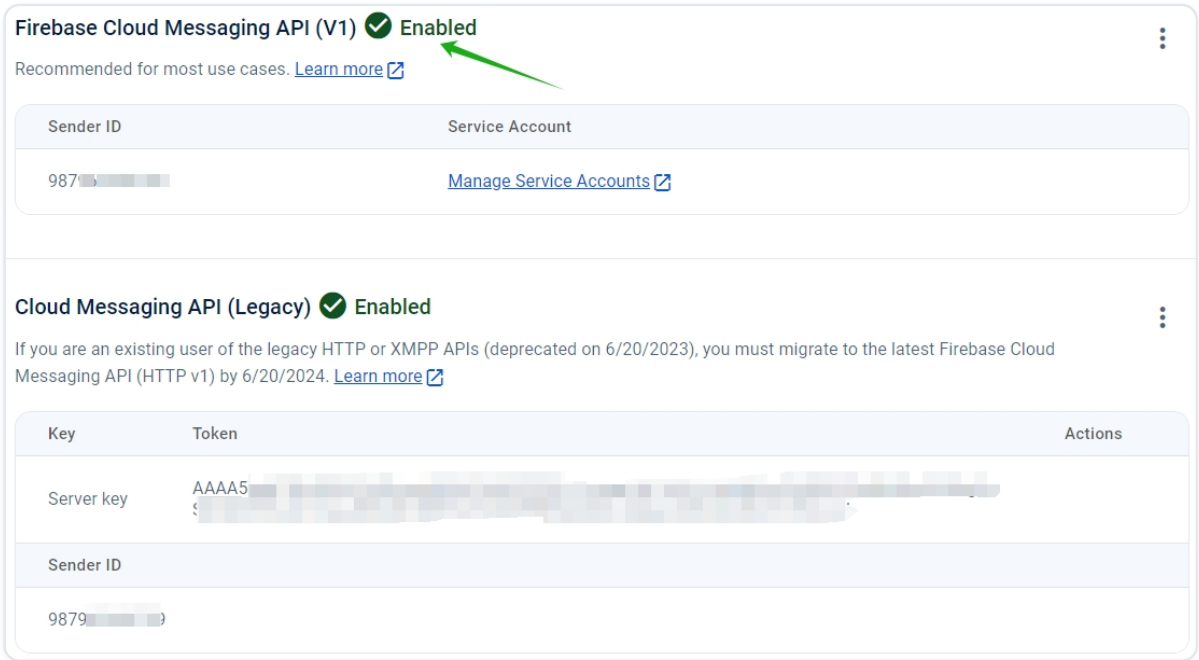
   a. 移行前はレガシーAPIを使用できたため、Cloud Messaging API（レガシー）が有効になっていることを確認してください。**キー**フィールドと**送信者ID**フィールドから値をコピーします。



キーがリストされていない場合は、**Actions** の下の省略記号をクリックしてキーを追加します。

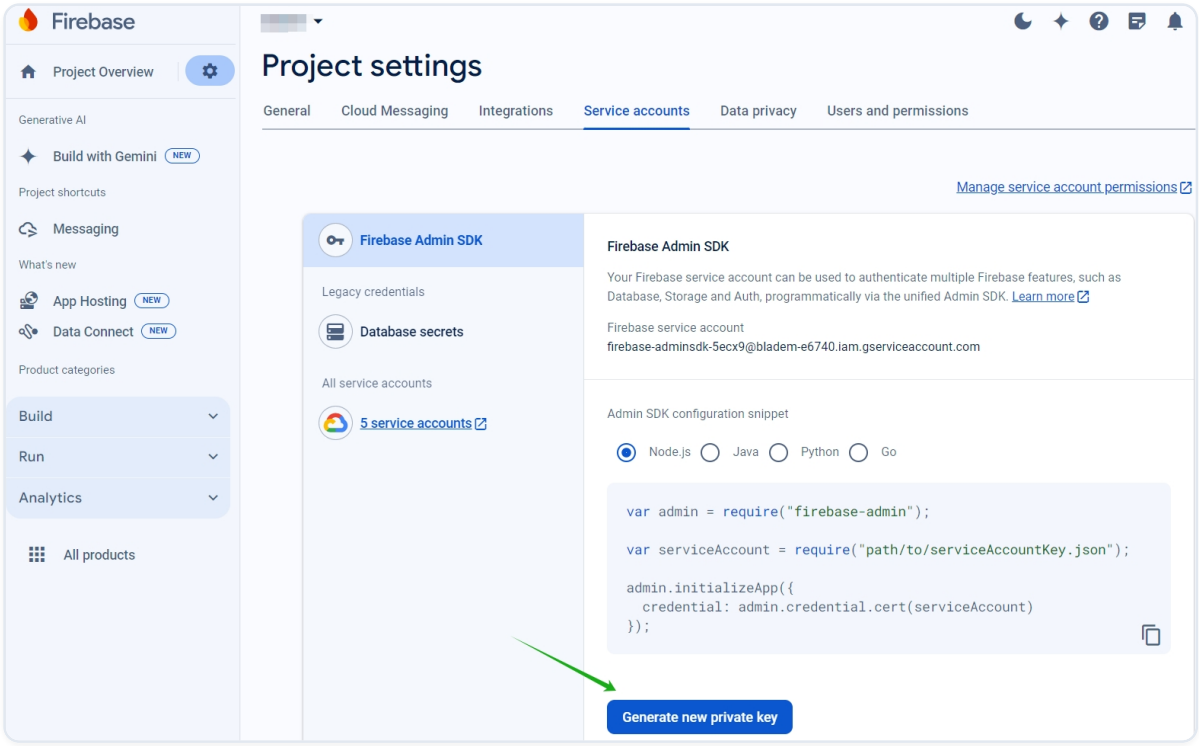


b. 移行後、レガシーAPIはGoogleから非推奨になりました。Firebase Cloud Messaging API(V1)を有効にする必要があります。詳細については、レガシーFCM APIからHTTP v1への移行を参照してください。



Project settings の下の **Service accounts** からサービスアカウントのJSONファイルをダウンロードします。サービスアカウントの秘密鍵ファイルを生成するには、手動で資格情

報を提供するセクションを参照してください。**Generate new private key** をクリックして、サービスアカウントキーのJSONファイルをダウンロードします。



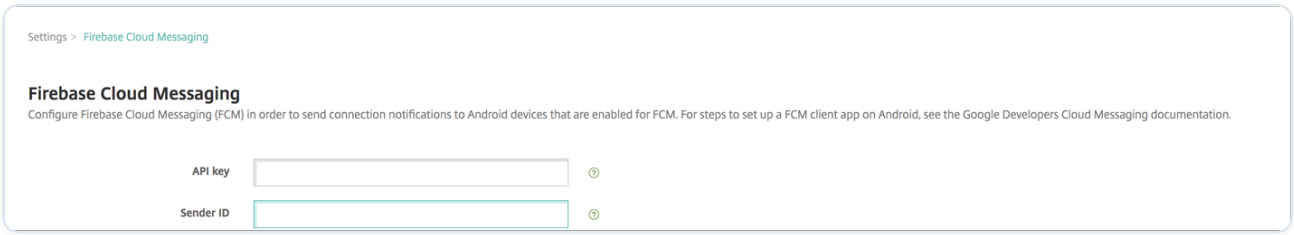
AndroidでFCMクライアントアプリをセットアップする手順については、Google Developers Cloud Messagingのこの記事を参照してください: `<https://firebase.google.com/docs/cloud-messaging/android/client>`。

FCM用にXenMobileを構成するには

XenMobileコンソールで、**Settings > Firebase Cloud Messaging** に移動します。

Cloud Messaging API (レガシー)の場合

1. Firebase Cloud Messaging構成の最後のステップで取得したFirebase Cloud Messaging**Key**を、**API key**フィールドに入力します。
2. 前の手順で取得した**Sender ID**の値を入力します。

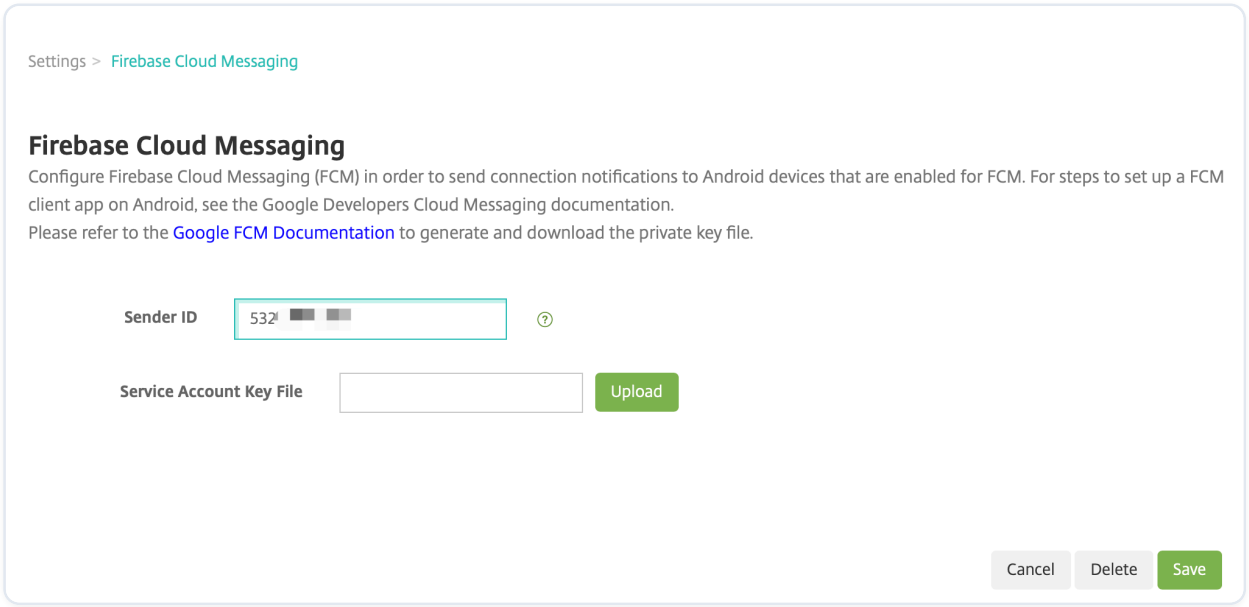


ファイアベース クラウド メッセージング エーピーアイ (V1) 向け

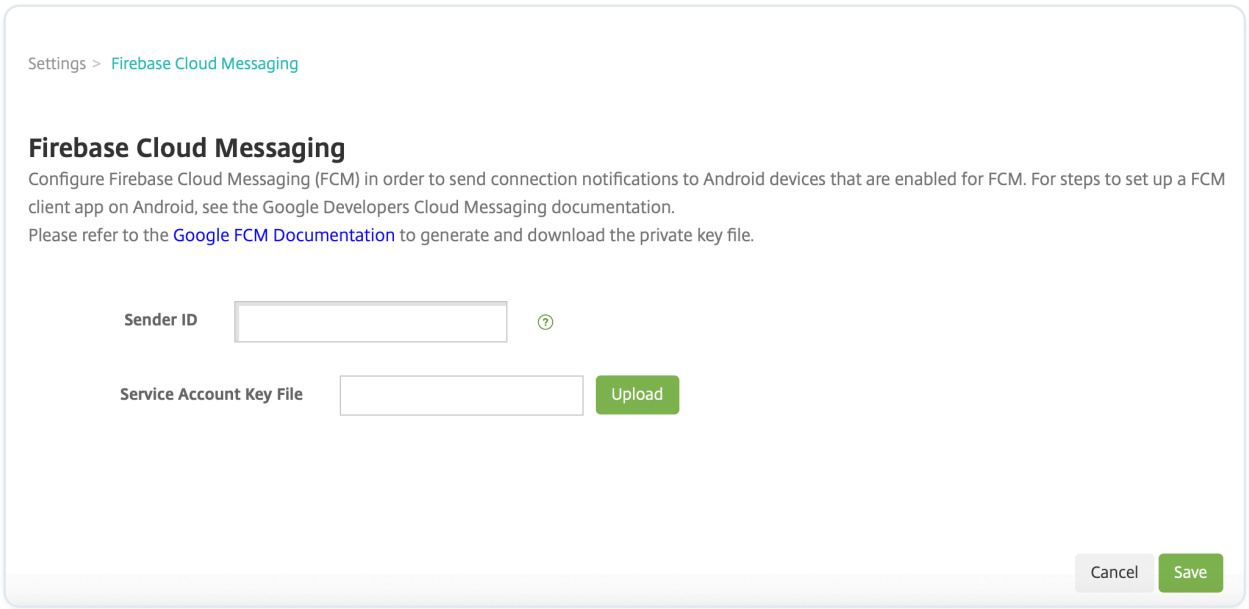
注:

- XenMobile Server バージョン 10.15 Rolling Patch 7 以降で FCM API V1 を有効にするには、Knowledge Center の記事 CTX677031 を参照してください。
- 新規の FCM ユーザーの場合は、手順 1 をスキップして手順 2 から進んでください。

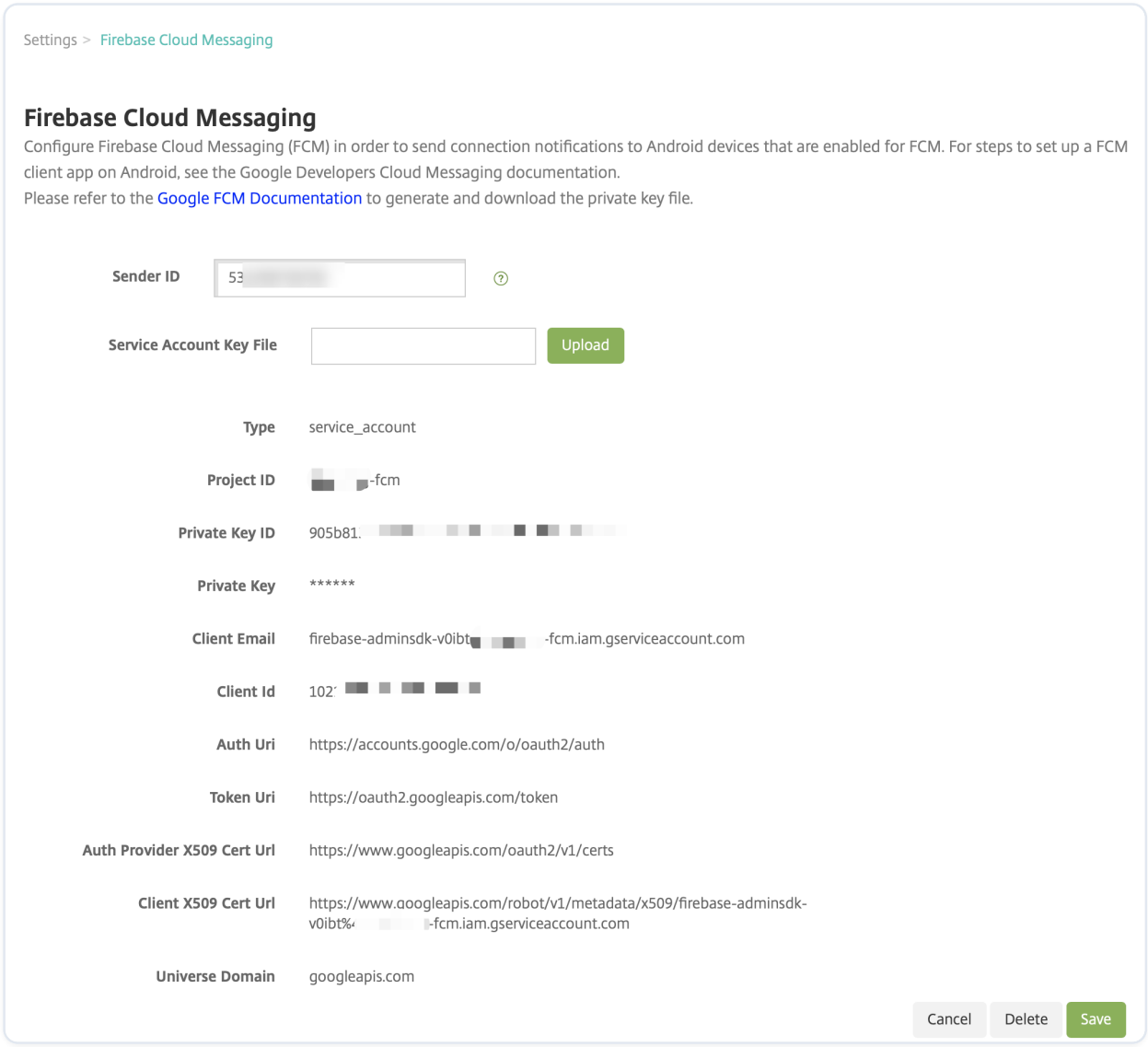
1. 既に FCM を使用している場合は、送信者 ID が現在の FCM プロジェクトで自動入力され、**サービスアカウントキーファイル**をアップロードする新しいオプションが表示されます。



2. 新規の FCM ユーザーの場合は、前の手順で取得した**送信者 ID** を入力し、**サービスアカウントキーファイル**をアップロードします。



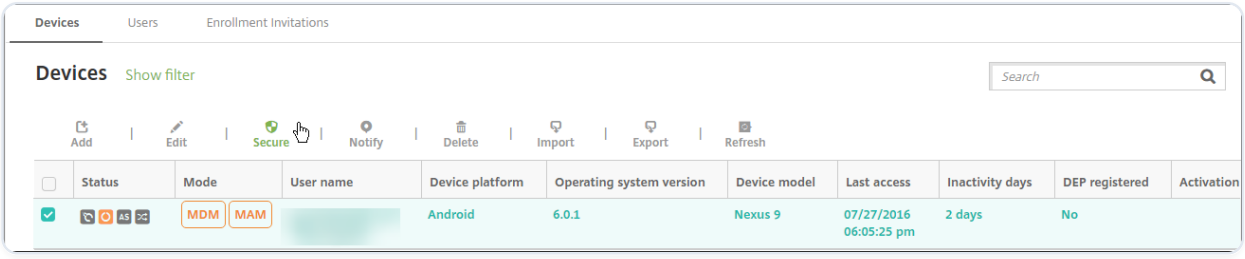
3. アップロードされたファイルは解析され、対応するフィールドが自動生成されます。



4. 情報を確認し、**保存**をクリックします。

構成をテストするには

1. Android デバイスを登録します。
2. デバイスをしばらくアイドル状態にして、XenMobile から切断されるようにします。
3. XenMobile コンソールにサインインし、**管理**をクリックして Android デバイスを選択し、**セキュリティ保護**をクリックします。



4. **デバイスアクション**で、**選択的ワイプ**をクリックします。

「選択的ワイプ」オプション(/en-us/xenmobile/server/media/security-action-selective-wipe.png)

構成が成功すると、デバイス上で選択的ワイプが実行されます。

Apple Education機能との統合

Apple Educationを使用する環境で、XenMobile®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は、Apple School Manager（ASM）とiPad用Classroomアプリをサポートしています。XenMobile Education Configurationデバイスポリシーは、Apple Educationで使用するための教師および生徒のデバイスを構成します。

事前構成され、監視対象のiPadを教師と生徒に提供します。この構成には、XenMobileへのASM登録、新しいパスワードで構成されたManaged Apple IDアカウント、および必要なボリューム購入アプリとiBooksが含まれます。

XenMobileのApple Education機能サポートの主な点を以下に示します。

Apple School Manager (アップルスクールマネージャー)

ASMは、教育機関で使用されるiOS（iPadOS）デバイスおよびmacOSラップトップのセットアップ、展開、管理を可能にするサービスです。ASMには、IT管理者が次のことを行えるWebベースのポータルが含まれています。

- Apple Deployment Programデバイスを異なるMDMサーバーに割り当てる。
- アプリとiBooksのボリューム購入ライセンスを購入する
- **Managed Apple ID**を一括作成します。これらのカスタマイズされたApple IDは、iCloud Driveへのドキュメントの保存やApple App Storeコースへの登録など、Appleサービスへのアクセスを提供します。

複数のASMアカウントをXenMobileに追加できます。たとえば、この機能を使用すると、教育部門または部署ごとに異なる登録設定とセットアップアシスタントオプションを使用できます。その後、ASMアカウントを異なるデバイスポリシーに関連付けます。

XenMobileコンソールにASMアカウントを追加すると、XenMobileはクラスと名簿の情報を取得します。デバイスのセットアップ中に、XenMobileは次のことを行います。

- デバイスを登録します。
- デバイスポリシー（Education Configuration、ホーム画面レイアウトなど）など、展開用に構成したリソースをインストールします。

- ボリューム購入を通じて購入したアプリとiBooksの両方もインストールします。

その後、事前構成されたデバイスを教師と生徒に提供します。デバイスが紛失または盗難された場合、MDM紛失モード機能を使用してデバイスをロックおよび検索できます。

iPad用Classroomアプリ

iPad用Classroomアプリを使用すると、教師は生徒のデバイスに接続して管理できます。デバイス画面の表示、iPadでのアプリの起動、Webリンクの共有と開くことができます。

ClassroomはApp Storeで無料で入手できます。アプリをXenMobileコンソールにアップロードします。その後、教育構成デバイスポリシーを使用してClassroomアプリを構成し、教師のデバイスに展開します。

Apple Education機能の詳細については、AppleのEducationサイトおよび同サイトのApple Education Deployment Guideを参照してください。

前提条件

- シトリックス ゲートウェイ
- MDM+MAM用に構成された登録プロファイル。
- Apple iPad第3世代（最小バージョン）またはiPad Mini、iOS 9.3（最小バージョン）

> **注：**

> XenMobileは、ASMユーザーアカウントをLDAPまたはActive Directoryに対して検証しません。ただし、ASMの教師や生徒に関係のないユーザーやデバイスの管理のために、XenMobileをLDAPまたはActive Directoryに接続することはできます。たとえば、Active Directoryを使用して、IT管理者やマネージャーなどの他のASMメンバーにSecure MailおよびSecure Webを提供できます。

> ASMの教師と生徒はローカルユーザーであるため、Citrix Secure Hub™をデバイスに展開する必要はありません。

> Citrix Gateway認証を含むMAM登録は、ローカルユーザー（Active Directoryユーザーのみ）をサポートしていません。そのため、XenMobileは、必要なボリューム購入アプリとiBooksのみを教師と生徒のデバイスに展開します。

アップル スクール マネージャーとゼンモバイルの構成

AppleまたはApple正規販売店や通信事業者からiPadを購入した後：このセクションのワークフローに従って、ASMアカウントとデバイスを設定します。このワークフローには、ASMポータルとXenMobileコンソールで行う手順が含まれています。

1対1モデル（生徒1人につきiPad 1台）で使用するiPad、または教師用iPad（共有なし）の統合を構成するには、これらの手順に従ってください。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。

ステップ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予定がある場合は、Appleサポート記事のUpgrade your institution to ASMを参照してください。ASMアカウントを作成するには、`<https://school.apple.com/>`にアクセスし、登録手順に従ってください。ASMに初めてログインすると、セットアップアシスタントが開きます。

- ASM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は、Apple School Managerユーザーガイドを参照してください。
- ASMを設定する際は、Active Directoryのドメイン名とは異なるドメイン名を使用してください。たとえば、ASMのドメイン名には`appleid`のようなプレフィックスを付けてください。
- ASMを名簿データに接続すると、ASMは教員と生徒のためにManaged Apple IDを作成します。名簿データには、教員、生徒、クラスが含まれます。ASMに名簿データを追加する方法については、前述のASMユーザーガイドを参照してください。
- 前述のASMユーザーガイドに記載されているように、組織のManaged Apple ID形式をカスタマイズできます。

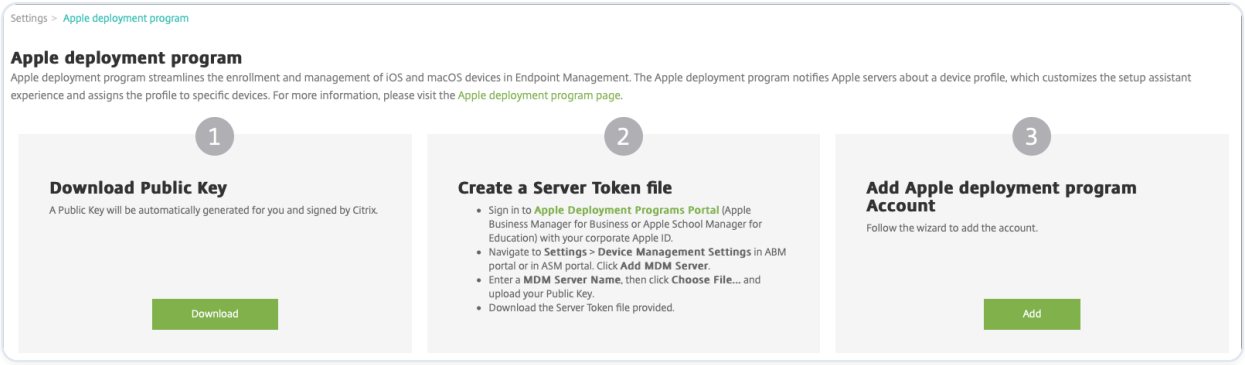
> **重要：**
>
> ASM情報をXenMobileにインポートした後で、Managed Apple IDを変更しないでください。

- 再販業者または通信事業者を通じてデバイスを購入した場合は、それらのデバイスをASMにリンクしてください。詳細については、前述のASMユーザーガイドを参照してください。

ステップ2：XenMobileをApple School ManagerのMDMサーバーとして構成し、デバイスの割り当てを構成する

ASMポータルには**MDMサーバー**タブがあります。このセットアップを完了するには、XenMobileからの公開鍵ファイルが必要です。

1. XenMobileの公開鍵をローカルコンピューターにダウンロードします。XenMobileコンソールで、**［設定］>［Apple Deployment Program］**の順に移動します。



2. **［公開鍵のダウンロード］の下で、［ダウンロード］**をクリックし、PEMファイルを保存します。
3. **Apple School Managerポータルで、［設定］、次に**［デバイス管理設定］**をクリックします。**［MDMサーバーの追加］**をクリックします。

「ASMポータル」(/en-us/xenmobile/server/media/asm-add-mdm-server.png)

4. XenMobileの名前を入力します。入力するサーバー名は参照用であり、サーバーのURLや名前ではありません。「**公開キーのアップロード**」の下にある「**ファイルの選択**」をクリックします。

「ASMポータル」(/en-us/xenmobile/server/media/ios-dep-30.png)

5. XenMobileからダウンロードした公開キーをアップロードし、「**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。「**トークンのダウンロード**」をクリックして、サーバートークンファイルをコンピューターにダウンロードします。

「ASMポータル」(/en-us/xenmobile/server/media/asm-add-mdm-server-get-token.png)

7. 「**デフォルトのデバイス割り当て**」の下にある「**変更**」をクリックします。デバイスの割り当て方法を選択し、要求された情報を提供します。詳細については、ASMユーザーガイドを参照してください。

ステップ3：Apple School ManagerアカウントをXenMobileに追加する

1. XenMobileコンソールで、「**設定 > Apple Deployment Program**」に移動し、「**Apple Deployment Programアカウントの追加**」の下にある「**追加**」をクリックします。

   「Apple Deployment Program設定画面」(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-1.png)

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、ASM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。トークン情報が表示されます。

   「Apple Deployment Program設定画面」(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-2.png)

   注：

   - 「**組織ID**」は、Apple Deployment Programの顧客IDです。
   - ASMアカウントの「**組織タイプ**」は「**教育**」であり、「**組織バージョン**」は「**v2**」です。

3. 「**アカウント情報**」ページで、次の設定を指定します。

   Apple Deployment Program設定画面(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-3.png)

   - **Apple Deployment Programアカウント名:** このApple Deployment Programアカウントの一意の名前。国や組織階層など、Apple Deployment Programアカウントをどのように整理しているかを反映する名前を使用します。
   - **ビジネス/教育ユニット:** デバイス割り当てのための教育ユニットまたは部門。このフィールドは必須です。
   - **一意のサービスID:** アカウントをさらに識別するのに役立つオプションの一意のID。
   - **サポート電話番号:** セットアップ中にユーザーがヘルプを求めることができるサポート電話番号。このフィールドは必須です。
   - **サポートメールアドレス:** エンドユーザーが利用できるオプションのサポートメールアドレス。
   - **教育サフィックス:** 特定のASM Deployment Programアカウントのクラスにフラグを付けます。（ボリューム購入サフィックスは、特定のボリューム購入アカウントのアプリとiBooksにフラグを付けます。）ASM Deployment ProgramとASMボリューム購入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、次の設定を指定します。

Apple設定画面(/en-us/xenmobile/server/media/settings-apple-dep-enrollment-asm-4.png)

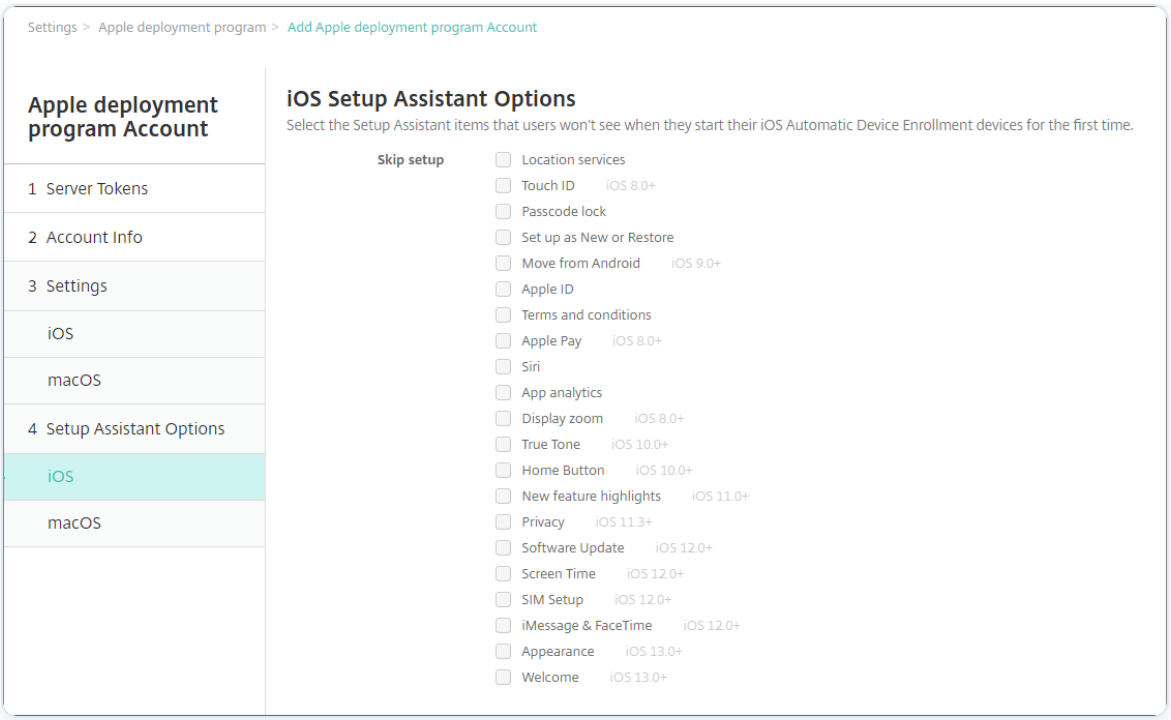
- **登録設定**
  - **デバイス登録を必須にする:** ユーザーにデバイスの登録を要求します。この設定を**いいえ**に変更します。
  - **デバイス登録に資格情報を要求する:** Apple Deployment Programのセットアップ中に、ユーザーに資格情報の入力を要求します。XenMobileとのASM統合の場合、この設定はデフォルトで**はい**であり、変更できません。Apple Deployment Programは、デバイス登録に資格情報を要求します。
  - **構成がセットアップを完了するまで待機する:** すべてのMDMリソースがデバイスに展開されるまで、ユーザーデバイスがセットアップアシスタントモードのままであることを要求するかどうか。XenMobileとのASM統合の場合、この設定はデフォルトで**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場合、次のコマンドは機能しない可能性があります。
    - InviteToProgram
    - アプリケーションのインストール
    - メディアのインストール
    - 引き換えコードの適用
- **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**は変更しないでください。iOSデバイスを監視モードにする方法の詳細については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」を参照してください。
  - **共有モード:** iPadで共有モードを有効にします。最小要件を満たさないデバイスは共有できません。
  - **登録プロファイルの削除を許可:** ASM統合の場合、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:** ASM統合の場合、Apple App StoreおよびApple Configuratorを介してデバイスを管理できるように、デバイスのペアリングを許可します。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、ユーザーがデバイスを初めて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ることを考慮してください。

重要:

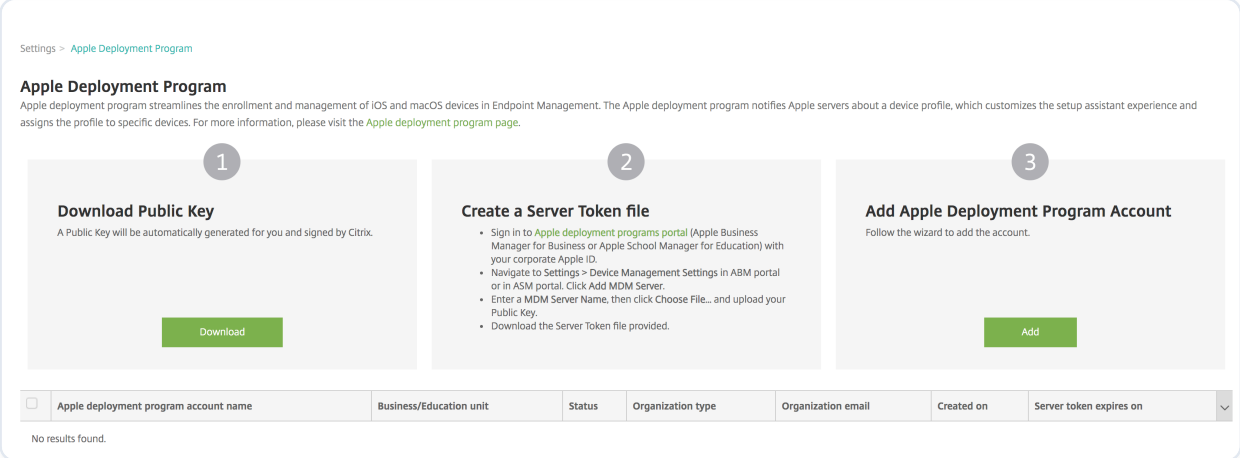
Citrixは、**Apple ID**と**利用規約**の手順を含めることを強く推奨します。これらの手順により、教員と生徒は新しい管理対象Apple IDパスワードを提供し、必要な利用規約に同意できます。



- **位置情報サービス:** デバイスで位置情報サービスを設定します。
- **Touch ID:** iOSデバイスで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。
- **新規として設定または復元:** デバイスを新規として、またはiCloudまたはApple App Storeのバックアップから設定します。
- **Androidから移行:** AndroidデバイスからiOS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、「**新規として設定または復元**」が選択されている場合（つまり、この手順がスキップされている場合）にのみ利用可能です。
- **Apple ID:** デバイスのApple IDアカウントを設定します。Citrixでは、この手順を含めるためにチェックボックスを選択することをお勧めします。
- **利用規約:** ユーザーにデバイスの使用に関する利用規約への同意を求めます。Citrixでは、この手順を含めるためにチェックボックスを選択することをお勧めします。

- **Apple Pay:** iOSデバイスで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設定します。
- **App解析:** クラッシュデータと使用状況統計をAppleと共有するかどうかを設定します。
- **画面表示の拡大:** iOSデバイスの画面解像度（標準または拡大）を設定します。
- **True Tone:** iOSデバイスでTrue Toneディスプレイを設定します。
- **ホームボタン:** ホームボタンの画面感度を設定します。
- **新機能のハイライト:** iOS 11.0デバイス（最小バージョン）で、オンボーディング情報画面、「どこからでもDockにアクセス」、「最近使ったAppを切り替える」を設定します。
- **プライバシー:** Apple Deployment Programデバイスのセットアップ中に、ユーザーがデータとプライバシーのペインを表示するのを防ぎます。iOS 11.3以降の場合。
- **ソフトウェアアップデート:** Apple Deployment Programデバイスのセットアップ中に、ユーザーが必須のソフトウェアアップデート画面を表示するのを防ぎます。iOS 12.0以降の場合。
- **スクリーンタイム:** Apple Deployment Programデバイスのセットアップ中に、ユーザーがスクリーンタイム画面を表示するのを防ぎます。iOS 12.0以降の場合。
- **SIM設定:** Apple Deployment Programデバイスのセットアップ中に、ユーザーが「モバイル通信プランを追加」画面を表示するのを防ぎます。iOS 12.0以降の場合。
- **iMessageとFaceTime:** Apple Deployment Programデバイスのセットアップ中に、ユーザーがiMessageとFaceTimeの画面を見るのを防ぎます。iOS 12.0以降の場合。

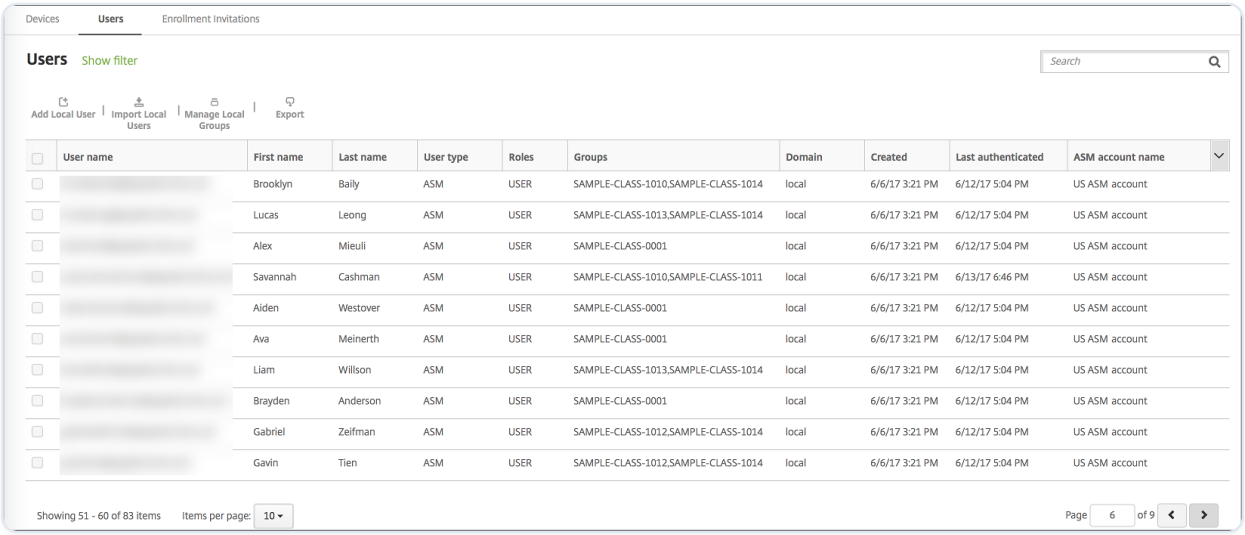
6. アカウントは**設定 > Apple Deployment Program**に表示されます。XenMobileとASMアカウント間の接続をテストするには、アカウントを選択し、**接続テスト**をクリックします。



ステータスメッセージが表示されます。



数分後、ASMから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を作成します。以下の例では、ユーザーアカウントのカスタマイズされたApple IDのドメイン名プレフィックスは`appleid`です。

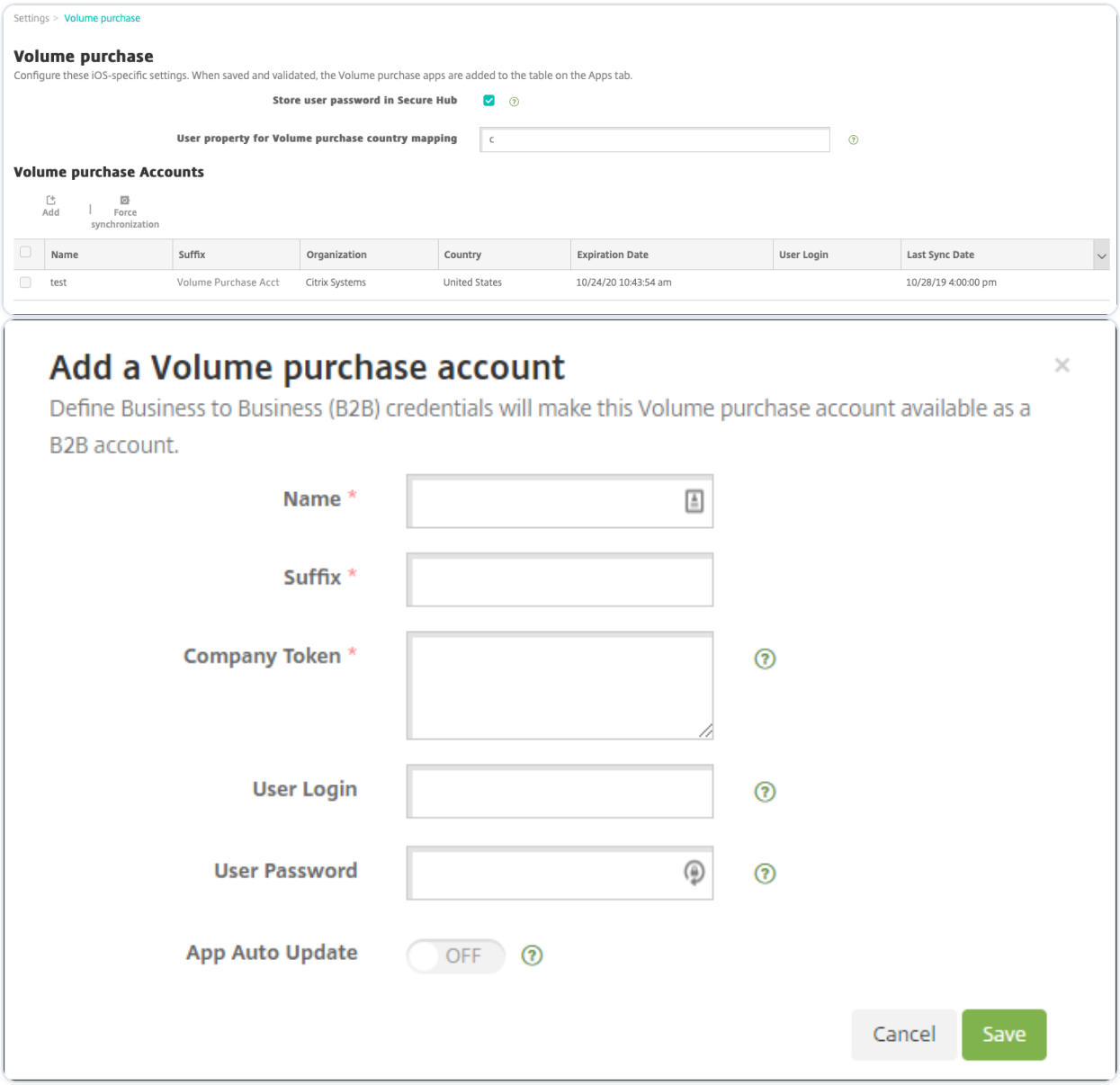


特定のASMアカウントのすべてのユーザーを見つけるには、ユーザー検索フィルターにアカウント名を入力します。

ステップ4：Apple School Managerの教育機関向けボリューム購入アカウントを構成する

このセクションでは、アプリやiBooksのボリューム購入ライセンスを購入するために使用するボリューム購入アカウントをXenMobileに指定します。

1. ASMの教育機関向けボリューム購入アカウントを構成するには、Apple Volume Purchaseの手順に従ってください。ボリューム購入アカウントの追加画面では、会社トークンを提供する必要があります。教育機関向けボリューム購入アカウントから直接トークンをダウンロードし、**ボリューム購入アカウントの追加**画面に貼り付けます。



2. ボリューム購入ライセンスがXenMobileにインポートされるまで数分待ちます。

ステップ5：Apple School Managerユーザーのパスワードを追加する

ASMアカウントを追加すると、XenMobileはASM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、コンソールでは「グループ」という用語を使用します。クラスにASMでグループ名が設定されている場合、XenMobileはそのグループ名をクラスに割り当てます。そうでない場合、XenMobileはソースシステムIDをグループ名として使用します。ASMのコース名は一意ではないため、XenMobileはコース名をクラス名として使用しません。

XenMobileは、管理対象Apple IDを使用して、ユーザータイプが**ASM**のローカルユーザーを作成します。ASMはすべての外部データソースとは独立して資格情報を作成するため、ユーザーはローカルです。その結果、XenMobileはこれらの新しいユーザーを認証するためにディレクトリサーバーを使用しません。

ASMは一時的なユーザーパスワードをXenMobileに送信しません。CSVファイルからインポートするか、手動で追加できます。一時的なユーザーパスワードをインポートするには：

1. 管理対象Apple IDの一時パスワードを作成する際にASM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、一時パスワードを、ユーザーがXenMobileに登録するために提供する新しいパスワードに置き換えます。この目的のためのパスワードタイプに制約はありません。

   CSVファイルのエントリの形式は次のとおりです。
   `user@appleid.citrix.com,Firstname,Middle,Lastname,Password123!`!

   ここで：

   ユーザー: `user@appleid.citrix.com`

   名: `Firstname`

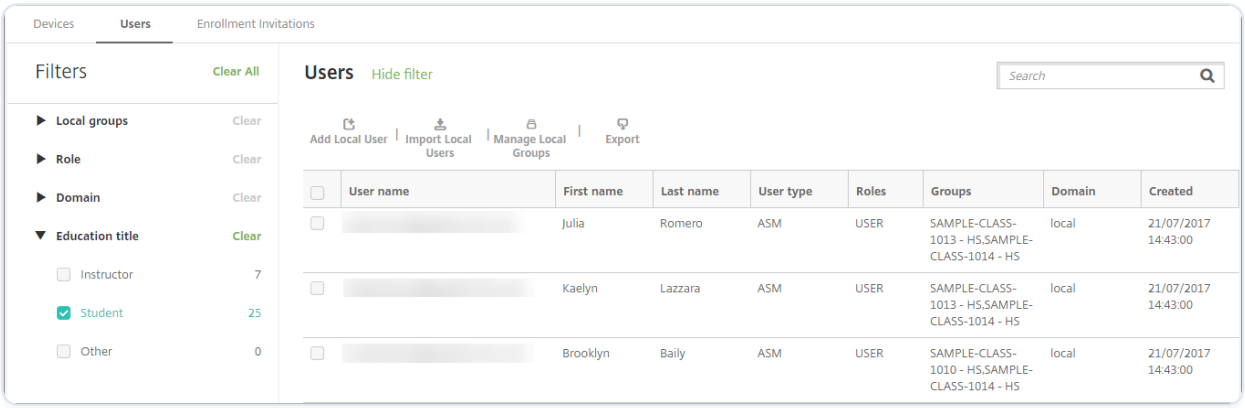
   ミドルネーム: `Middle`

   姓: `Lastname`

   パスワード: `Password123!`!
3. XenMobileコンソールで、 **>** をクリックします。 ページが表示されます。

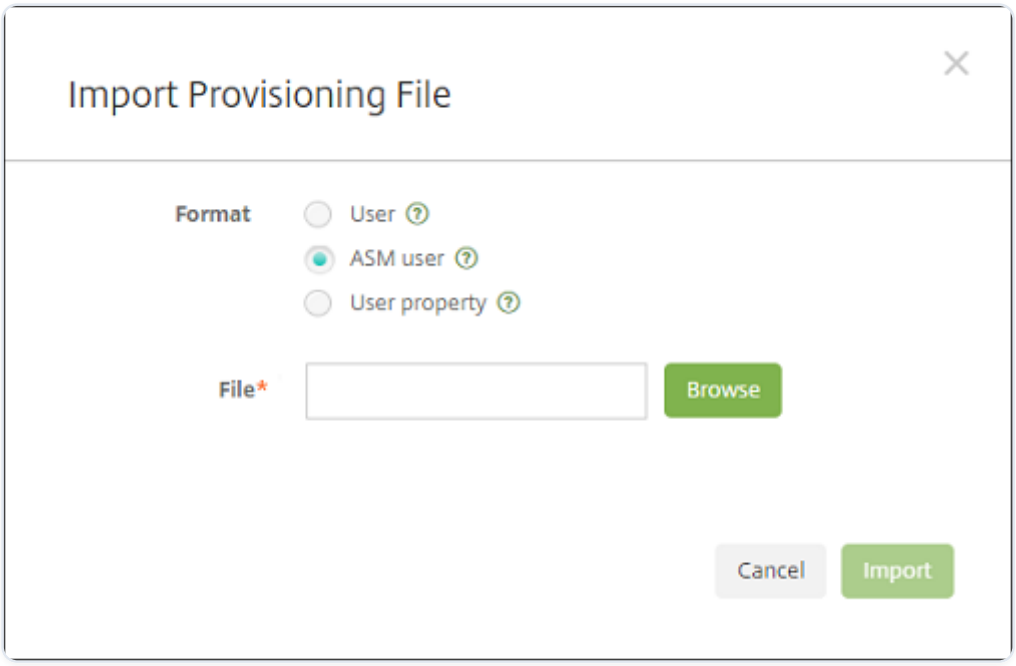
   次の** > ** 画面のサンプルは、ASMからインポートされたユーザーのリストを示しています。リストでは：

   - には、管理対象Apple IDが表示されます。
   - ユーザータイプは **ASM** で、アカウントがASMから作成されたことを示します。
   - **グループ** はクラスを表示します。

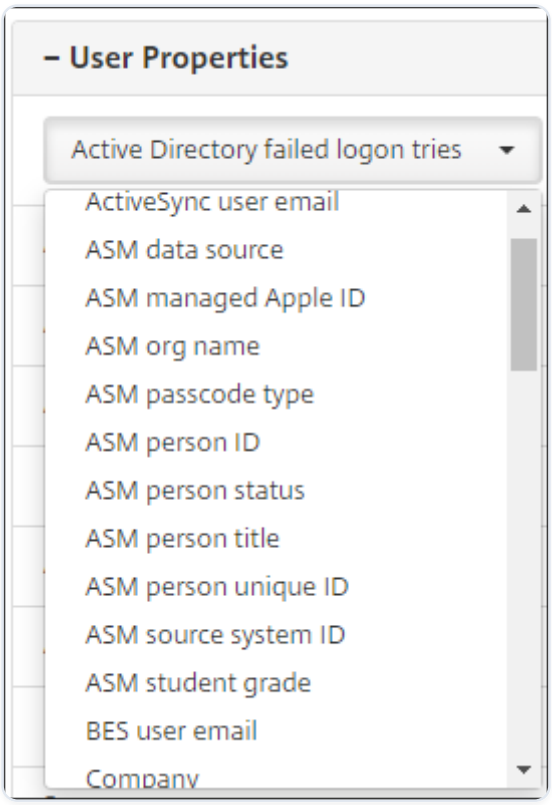


4. **ローカルユーザーのインポート** をクリックします。**プロビジョニングファイルのインポート** ダイアログボックスが表示されます。

5. 形式には **ASMユーザー** を選択し、ステップ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、ユーザーを選択して **編集** をクリックします。



名前のプロパティに加えて、次のASMプロパティが利用可能です。

- **ASMデータソース:** クラスのデータソース（例: **CSV** または **SFTP**）。

- **ASM管理対象Apple ID:** 管理対象Apple IDには、組織名と `appleid` が含まれる場合があります。たとえば、IDは `johnappleseed@appleid.myschool.edu` のようになることがあります。XenMobileでは、認証に管理対象Apple IDが必要です。
- **ASM組織名:** XenMobileでアカウントに付けた名前。
- **ASMパスコードタイプ:** 個人のパスワードポリシー: **複雑**（8文字以上の数字と文字で構成される学生以外のパスワード）、**4桁**（数字）、または **6桁**（数字）。
- **ASM個人一意ID:** ユーザーの識別子。
- **ASM個人ステータス:** 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。このステータスは、ユーザーが管理対象Apple IDアカウントの新しいパスワードを提供した後にアクティブになります。
- **ASM担当者の役職:** 教員、生徒、またはその他。
- **ASM担当者の一意のID:** ユーザーの一意の識別子。
- **ASMソースシステムID:** システムソースの識別子。
- **ASM生徒の学年:** 生徒の学年情報（教員は使用しません）。

手順6：オプションで生徒の写真を追加する

各生徒の写真を追加できます。教員がApple Classroomアプリを使用している場合、写真はこのアプリに表示されます。

写真の推奨事項:

- 解像度: 256 x 256ピクセル（2倍デバイスでは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**に移動し、ユーザーを選択して**編集**をクリックし、**画像を選択**をクリックします。

ユーザー画面(/en-us/xenmobile/server/media/manage-users-asm-user-image.png)

手順7：リソースとデリバリーグループを計画してXenMobileに追加する

デリバリーグループは、ユーザーのカテゴリに展開するリソースを指定します。たとえば、教員と生徒用に1つのデリバリーグループを作成できます。あるいは、複数のデリバリーグループを作成して、さまざまな教員や生徒に送信されるアプリ、メディア、ポリシーをカスタマイズすることもできます。クラスごとに1つ以上のデリバリーグループを作成できます。また、管理者（教育機関の他のスタッフ）用に1つ以上のデリバリーグループを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、ボリューム購入アプリ、iBooksが含まれます。

- デバイスポリシー:

  インストラクターがClassroomアプリを使用する場合、教育構成デバイスポリシーが必要です。インストラクターと生徒のiPadをどのように構成し、制限するかを決定するために、他のデバイスポリシーを確認してください。

- ボリューム購入アプリ:

  XenMobileでは、教育ユーザー向けにボリューム購入アプリを必須アプリとして展開する必要があります。XenMobileは、このようなボリューム購入アプリをオプションとして展開することをサポートしていません。

  Apple Classroomアプリを使用する場合は、インストラクターデバイスにのみ展開してください。

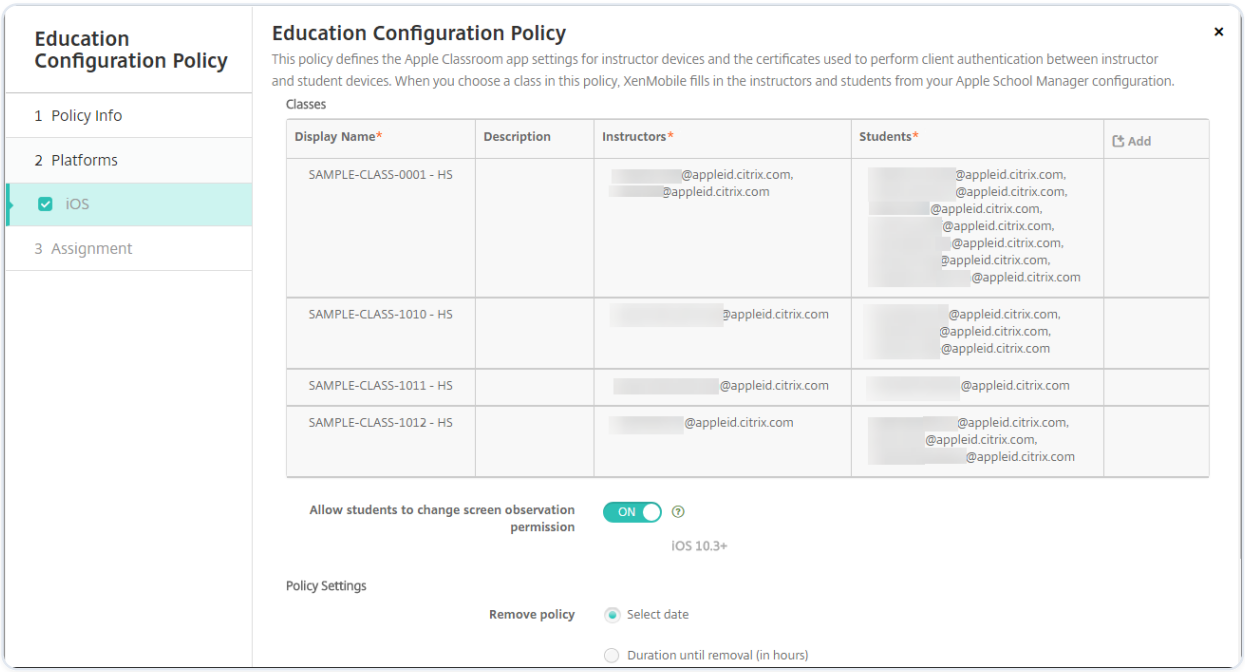
  インストラクターまたは生徒に提供したい他のアプリを展開します。このソリューションはCitrix Secure Hubアプリを使用しないため、インストラクターまたは生徒に展開する必要はありません。

- ボリューム購入iBooks:

  XenMobileがASMアカウントに接続すると、購入したiBooksがXenMobileコンソールの**構成 > メディア**に表示されます。そのページにリストされているiBooksは、デリバリーグループに追加できます。XenMobileは、iBooksを必須メディアとしてのみ追加することをサポートしています。

インストラクターと生徒向けのリソースとデリバリーグループを計画したら、XenMobileコンソールでそれらのアイテムを作成できます。

1. インストラクターまたは生徒のデバイスに展開したいデバイスポリシーを作成します。教育構成デバイスポリシーの詳細については、教育構成デバイスポリシーを参照してください。

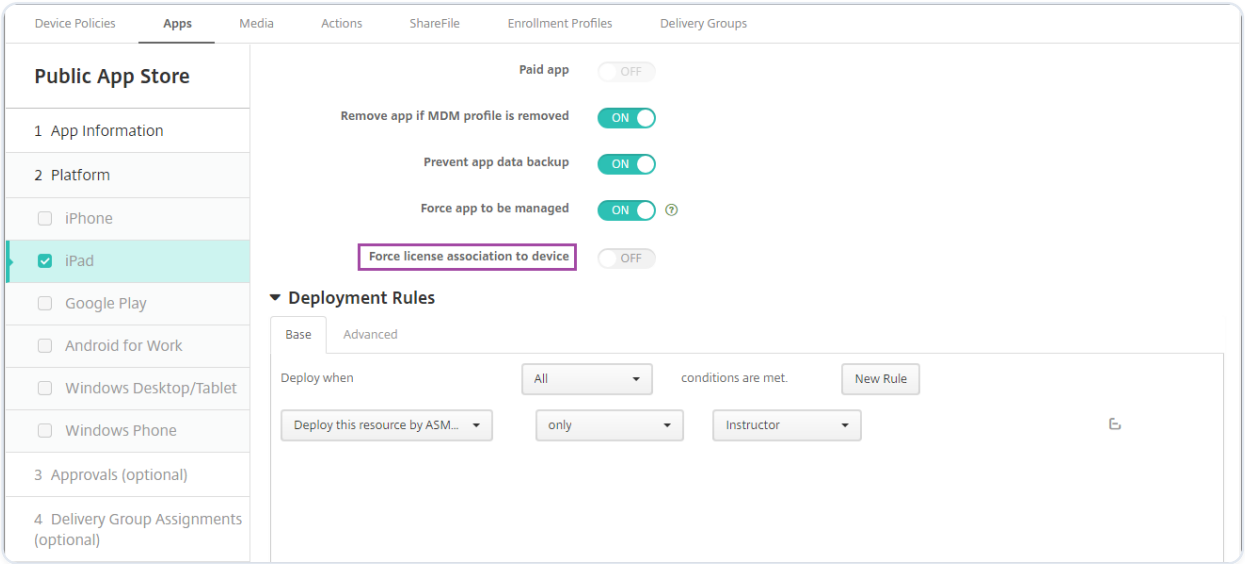


デバイスポリシーの詳細については、デバイスポリシーおよび個々のポリシー記事を参照してください。

2. アプリの構成 (**構成 > アプリ**) とiBooks (**構成 > メディア**):

   - デフォルトでは、XenMobileはアプリとiBooksをユーザーレベルで割り当てます。初回展開時に、インストラクターと生徒はASMに登録するようプロンプトを受け取ります。招待を承諾すると、ユーザーは次回の展開時（6時間以内）にASMアプリとiBooksを受け取ります。Citrixは、新しいASMユーザーにアプリとiBooksの展開を強制することをお勧めします。これを行うには、デリバリーグループを選択し、**展開**をクリックします。

     アプリ（iBooksは除く）をデバイスレベルで割り当てることもできます。これを行うには、設定**デバイスへのライセンス関連付けを強制**を**オン**に変更します。アプリをデバイスレベルで割り当てると、ユーザーはAppleボリューム購入への招待を受け取りません。

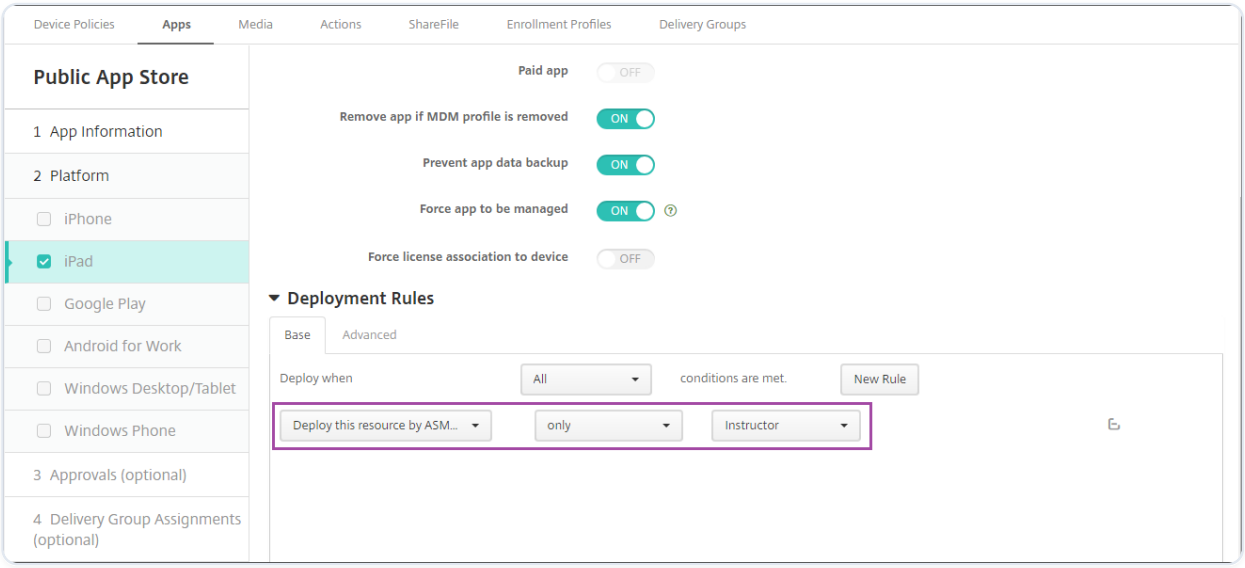


- アプリを教員のみに展開するには、教員のみを含むデリバリーグループを選択するか、次の展開ルールを使用します。

```
Deploy this resource by ASM device type

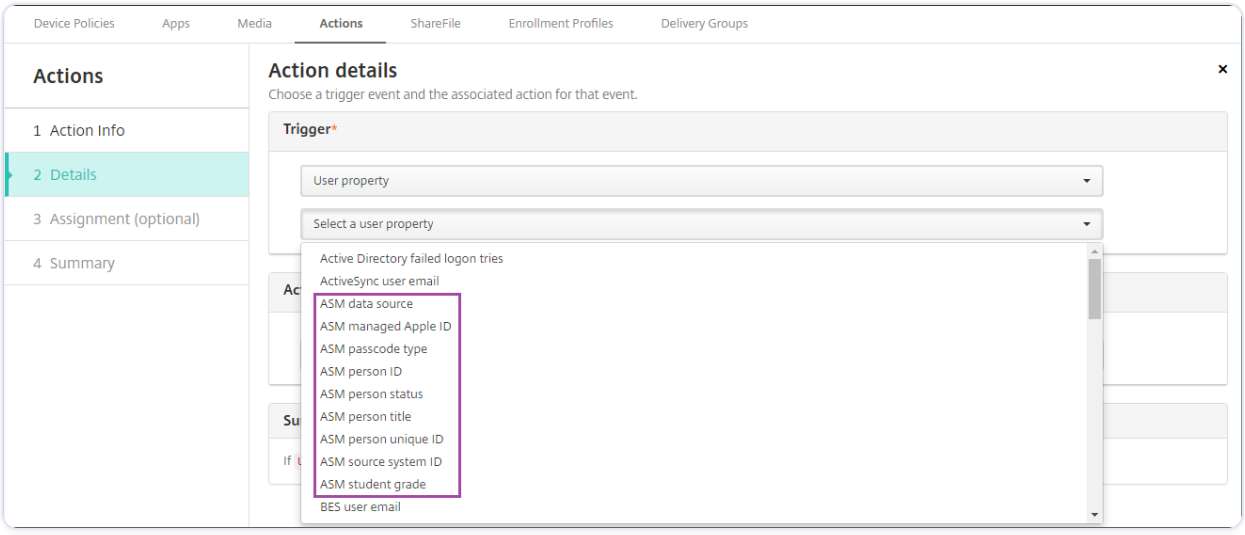
only

Instructor
```



- ボリューム購入アプリの追加については、「パブリックApp Storeアプリの追加」を参照してください。

3. オプション。ASM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、新しいアプリがインストールされたときに学生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がトリガーするアクションを作成することもできます。



アクションを作成するには、 > に移動します。アクションの構成については、「自動アクション」を参照してください。

4. > で、教員用と学生用のデリバリーグループを作成します。ASMからインポートされたクラスを選択します。また、教員と学生の展開ルールを作成します。

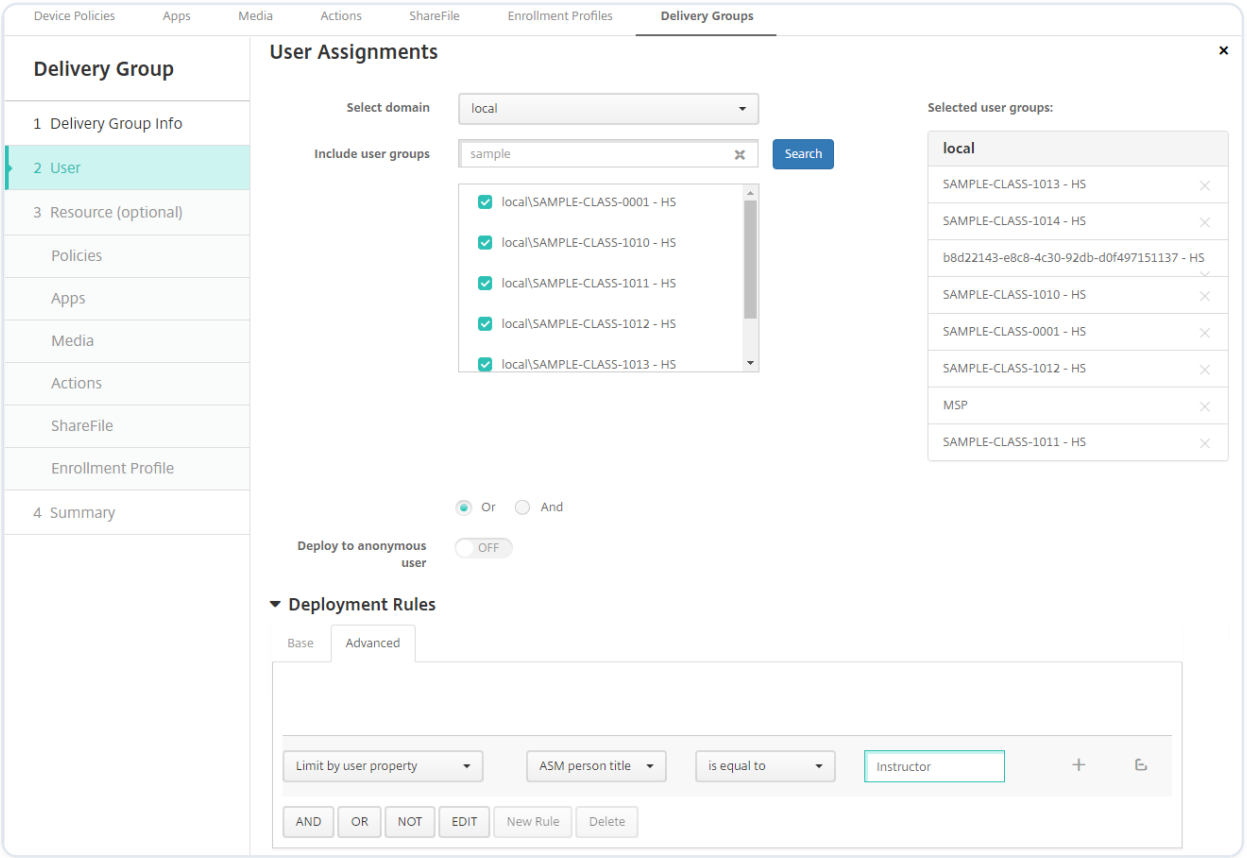
   たとえば、次のユーザー割り当ては教員用です。展開ルールは次のとおりです。

```
Limit by user property

ASM person title

is equal to

Instructor
```



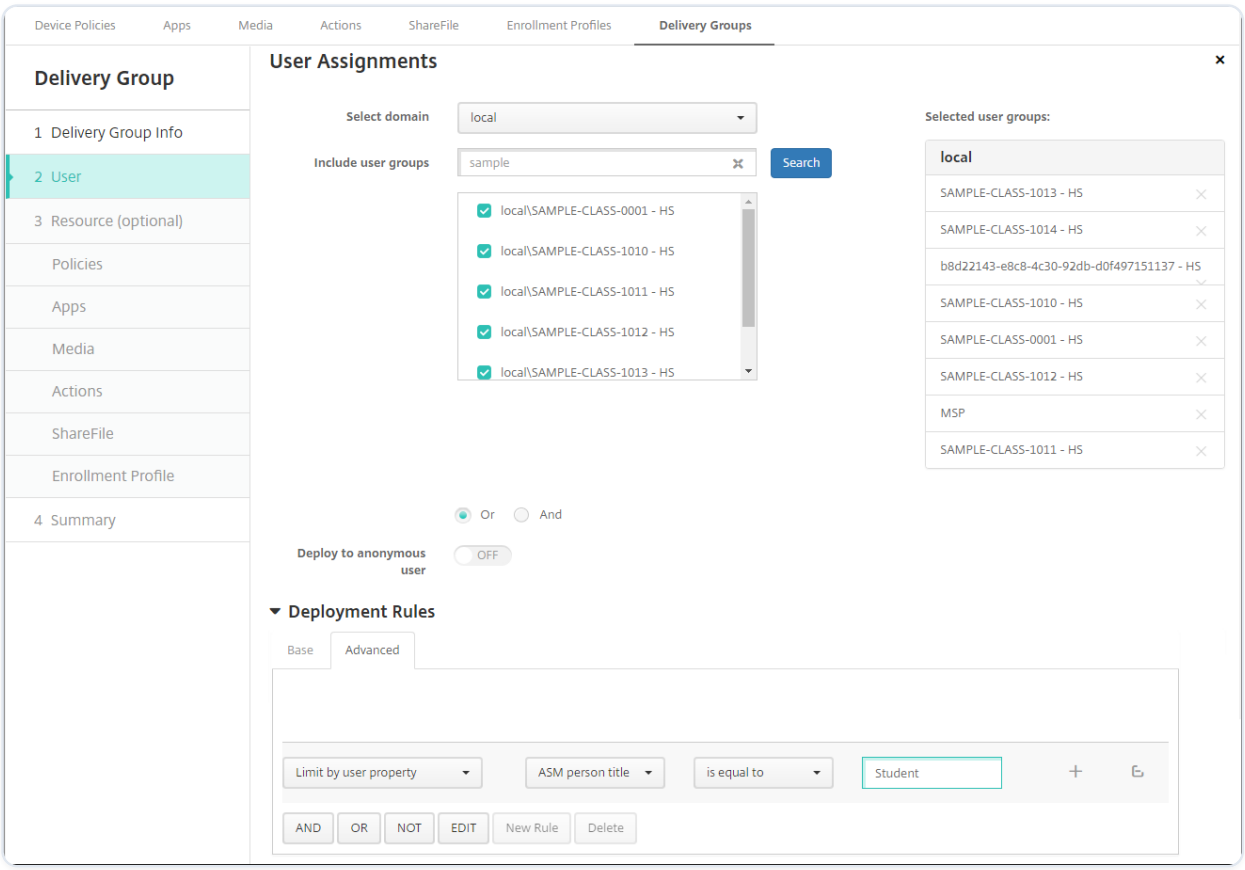
次のユーザー割り当ては学生用です。展開ルールは次のとおりです。

```
Limit by user property

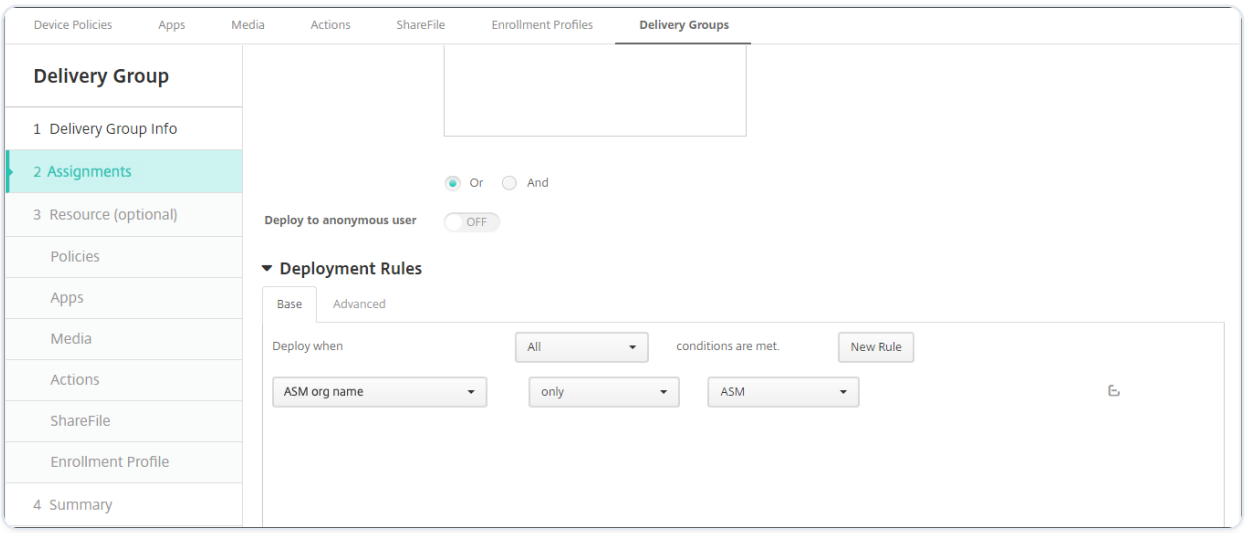
ASM person title

is equal to
```

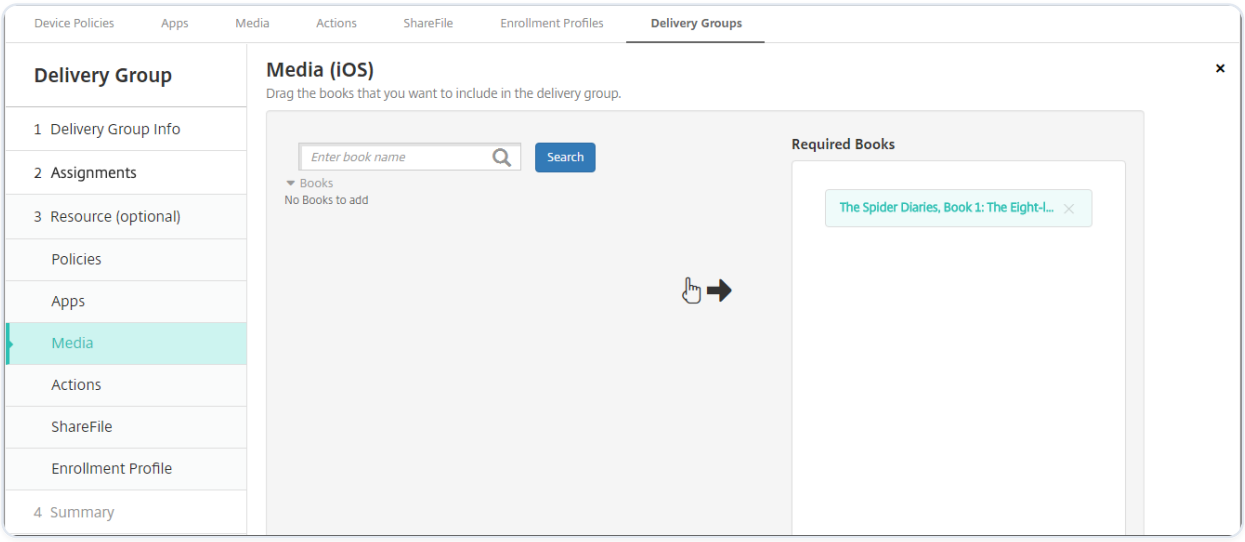
```
Student
```



ASM組織名に基づいた展開ルールを使用して、デリバリーグループをフィルタリング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。



デリバリーグループを選択して**展開**をクリックしたときに表示される確認ダイアログの例を次に示します。

デリバリーグループ構成画面(/en-us/xenmobile/server/media/deploy-delivery-group.png)

詳細については、(/ja-jp/xenmobile/server/deploy-resources.html)の「デリバリーグループを編集するには」および「デリバリーグループに展開するには」を参照してください。

ステップ8：教員および生徒のデバイス登録をテストする

デバイスは、次のいずれかの方法で登録できます。

- 学校管理者は、XenMobileコンソールで設定できるユーザーパスワードを使用して、教員および生徒のデバイスを登録できます。その結果、アプリとメディアがすでにセットアップされているデバイスをユーザーに提供できます。
- ユーザーがデバイスを受け取ると、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はデバイスポリシー、アプリ、およびメディアをデバイスに送信します。

登録をテストするには、ASMにリンクされているApple Deployment Programデバイスを使用します。

1. デバイスがASMにリンクされていない場合は、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. ASMデバイスを教員に登録します。次に、ASMデバイスを生徒に登録します。
3. **管理 > デバイス**ページで、両方のASMデバイスがMDMのみに登録されていることを確認します。

   デバイスページは、ASMデバイスのステータス（**ASM登録済み**、**ASM共有**、**教員**、**生徒**）でフィルタリングできます。

デバイス構成画面(/en-us/xenmobile/server/media/manage-devices-asm-filtered.png)

4. 各デバイスにMDMリソースが正しく展開されている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、さまざまなページを確認します。

   デバイス構成画面(/en-us/xenmobile/server/media/manage-devices-asm-details.png)

ステップ 9: デバイスを配布する

Apple は、インストラクターや学生にデバイスを配布するためのイベントを主催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は、以下の情報もこれらのユーザーに提供してください。

- 登録用の XenMobile パスワード
- 管理対象 Apple ID 用の ASM 一時パスワード。

初回ユーザーエクスペリエンスは次のとおりです。

1. ユーザーがハードリセット後にデバイスを初めて起動すると、XenMobile は登録画面でデバイスの登録を促します。
2. ユーザーは、XenMobile への認証に使用する管理対象 Apple ID と XenMobile パスワードを入力します。
3. Apple ID の設定手順で、デバイスはユーザーに Managed Apple ID と ASM の一時パスワードの入力を求めます。これらの項目は、ユーザーを Apple サービスに認証します。
4. デバイスは、iCloud のデータを保護するために使用する Managed Apple ID のパスワードを作成するようユーザーに促します。
5. セットアップアシスタントの最後に、XenMobile はポリシー、アプリ、メディアのデバイスへのインストールを開始します。ユーザーレベルで割り当てられたアプリと iBooks については、アシスタントがインストラクターと学生にボリューム購入への登録を促します。招待を承諾すると、ユーザーは次回の展開時（6 時間以内）にボリューム購入アプリと iBooks を受け取ります。

インストラクター、学生、クラスデータを管理する

インストラクター、学生、クラスデータを管理する際は、次の点に注意してください。

- XenMobile に ASM 情報をインポートした後で、Managed Apple ID を変更しないでください。XenMobile は、ユーザーを識別するために ASM ユーザー識別子も使用します。

- 1 つ以上の教育構成デバイスポリシーを作成した後に ASM でクラスデータを追加または変更した場合は、ポリシーを編集してから再展開してください。
- クラスのインストラクターがEducation Configurationデバイスポリシーの展開後に変更された場合: ポリシーを確認してXenMobileコンソールで更新されていることを確認し、ポリシーを再展開します。
- ASMポータルでユーザープロパティを更新すると、XenMobileもコンソールでそれらのプロパティを更新します。ただし、XenMobileは、他のプロパティを受信するのと同じ方法でASMの人物の役職プロパティ（インストラクター、学生、その他）を受信しません。したがって、ASMでASMの人物の役職を変更した場合は、その変更をXenMobileに反映させるために、次の手順を実行します。

データを管理するには:

1. ASMポータルで、学生の学年を更新し、インストラクターの学年をクリアします。
2. 学生アカウントをインストラクターアカウントに変更した場合は、クラスの学生リストからユーザーを削除します。その後、同じクラスまたは別のクラスのインストラクターリストにユーザーを追加します。

   インストラクターアカウントを学生アカウントに変更した場合は、クラスからユーザーを削除します。その後、同じクラスまたは別のクラスの学生リストにユーザーを追加します。更新は、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. Education Configurationデバイスポリシーを編集して変更を適用し、再展開します。

   - ASMポータルからユーザーを削除すると、フェッチ後にXenMobileもそのユーザーをXenMobileコンソールから削除します。

     このサーバープロパティ値 **bulk.enrollment.fetchRosterInfoDelay** （デフォルトは **1440** 分）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。
   - リソースを展開した後: 学生がクラスに参加した場合、その学生のみを含むデリバリーグループを作成し、その学生にリソースを展開します。
   - 学生またはインストラクターが一時パスワードを紛失した場合は、ASM管理者に連絡するよう伝えてください。管理者は一時パスワードを提供するか、新しいパスワードを生成できます。

Apple School ManagerのApple Deployment Programに登録されている紛失または盗難されたデバイスを管理する

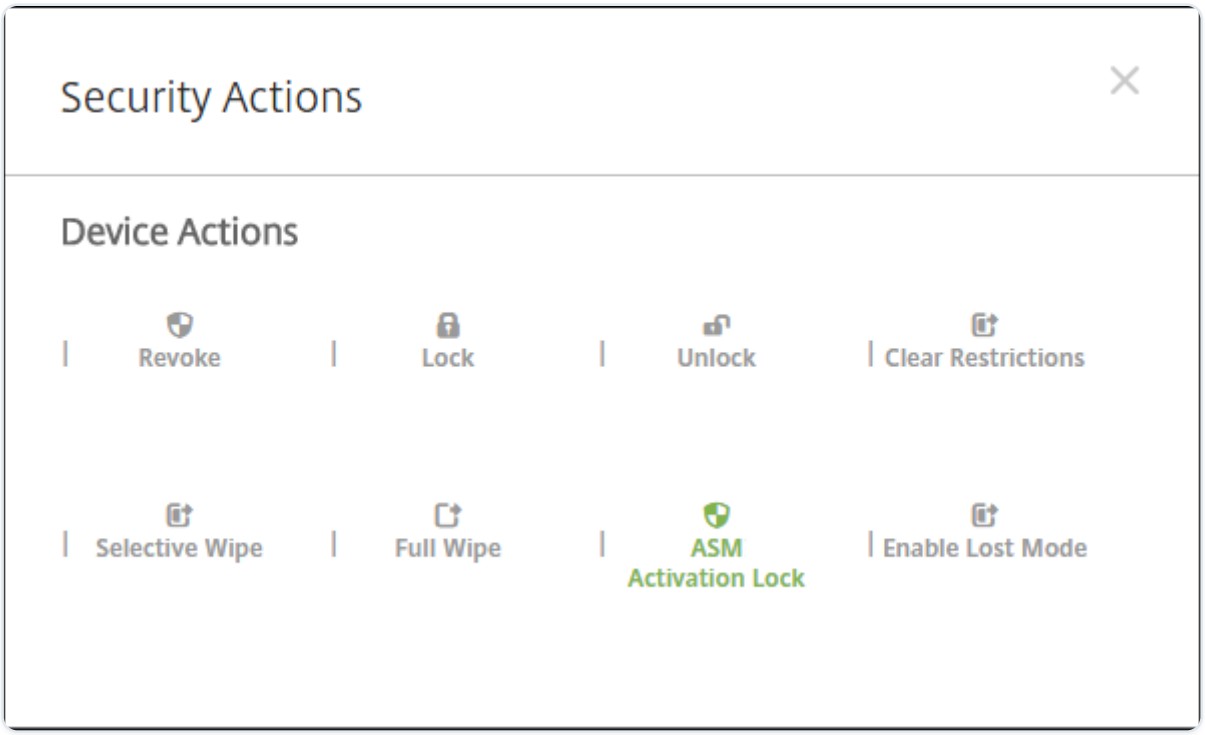
Appleの「iPhone/iPadを探す」サービスには、アクティベーションロック機能が含まれています。アクティベーションロックは、Apple Deployment Programに登録されている紛失または盗難されたデバイスを、不正なユーザーが使用したり転売したりするのを防ぎます。

XenMobileには、ASM Apple Deployment Programに登録されているデバイスにロックコードを送信できる **ASM Activation Lock** セキュリティアクションが含まれています。

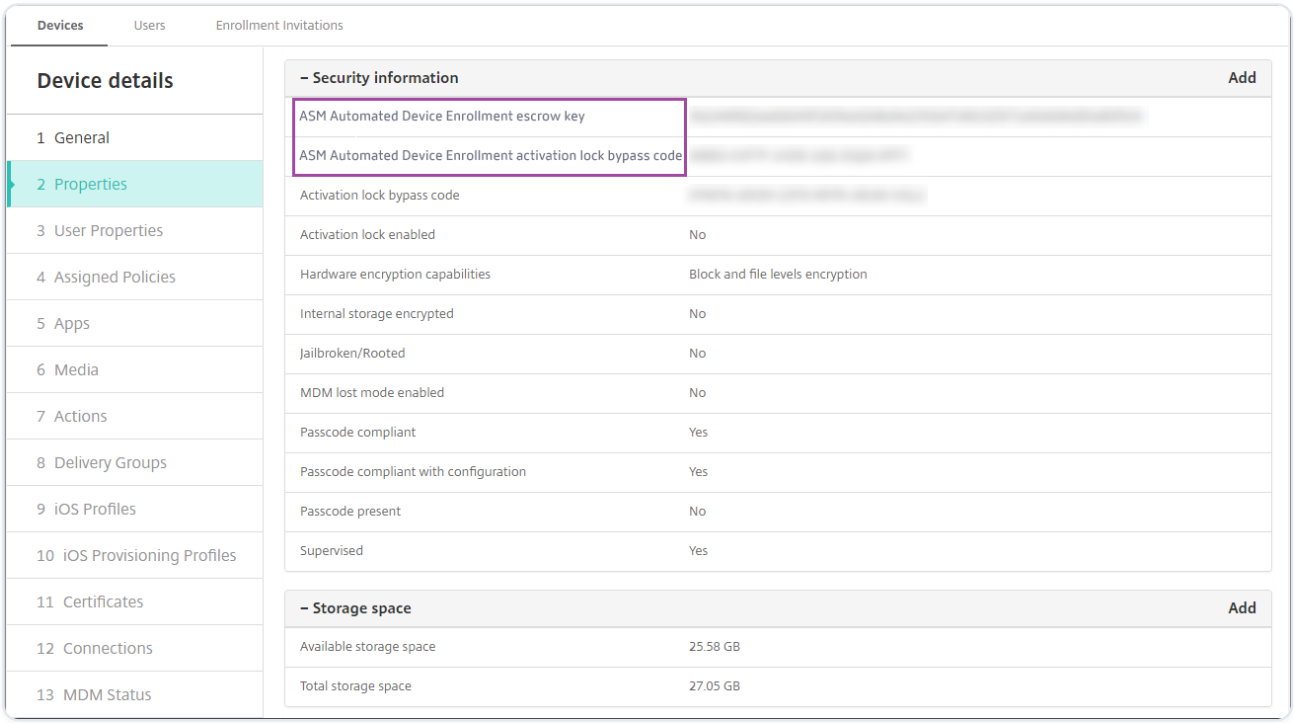
ASM Activation Lock セキュリティアクションを使用すると、XenMobileはユーザーが「iPhone/iPadを探す」サービスを有効にする必要なくデバイスを特定できます。ASMデバイスがハードリセットまたは完全にワイプされた場合、ユーザーは管理対象Apple IDとパスワードを提供してデバイスのロックを解除します。

コンソールからロックを解除するには、セキュリティアクションの をクリックします。アクティベーションロックのバイパスについては、「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。ユーザーはログインを空白のままにして、パスワードとして **ASM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、 の タブで確認できます。

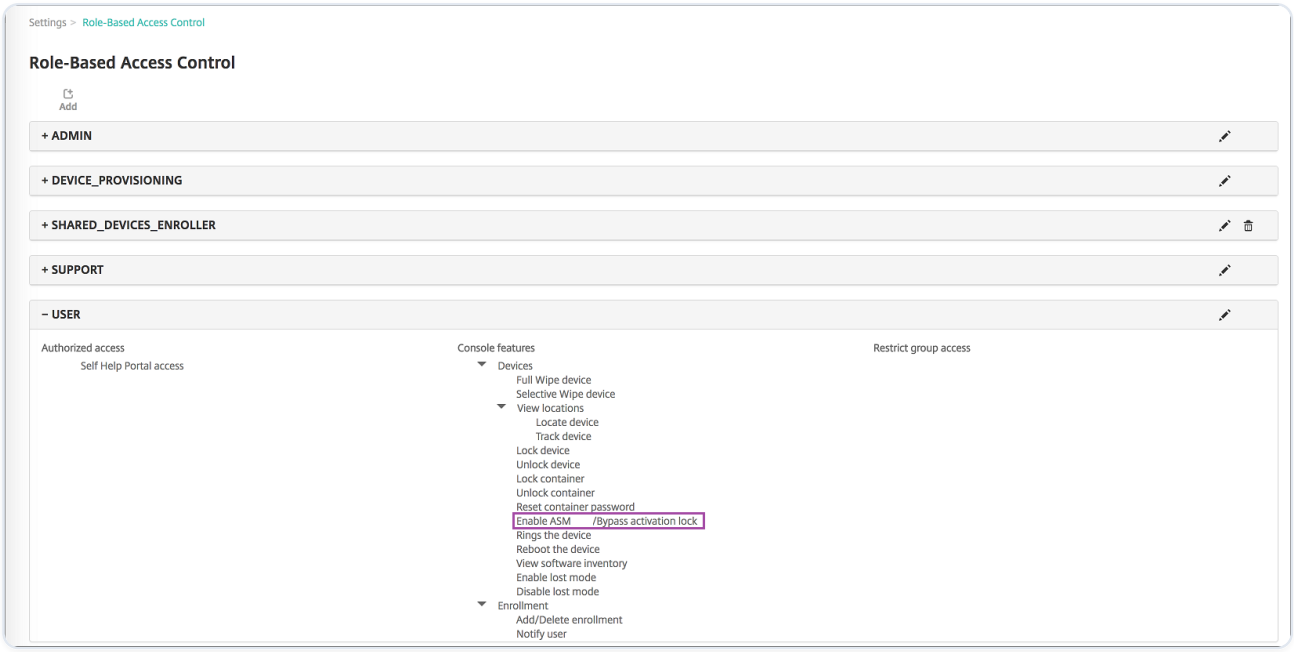
アクティベーションロックを設定するには、 **>** に移動し、デバイスを選択して をクリックし、 をクリックします。



プロパティの **ASMエスクローキー** と **ASMアクティベーションロックバイパスコード** は、 に表示されます。



ASMアクティベーションロックのRBAC権限は、 **>** です。



共有iPad

共有iPad機能を使用すると、複数のユーザーが1台のiPadを使用できます。デバイスが共有されていても、ユーザーエクスペリエンスをパーソナライズできます。共有iPadは、教育またはビジネス目的で使用できます。Apple School Manager (ASM) は、Apple Business Manager (ABM) がサポートする役割に加えて、インストラクターと生徒の役割をサポートします。

前提条件

- アップルスクールマネージャーまたはアップルビジネスマネージャー
- ゼノモバイル® サーバー
- iPad Pro、iPad 第5世代、iPad Air 2以降、iPad mini 4以降のいずれか
- 32 GB以上のストレージ
- 監視対象

共有iPadの構成

教室の複数の生徒が、1人または複数のインストラクターが教えるさまざまな科目のためにiPadを共有できます。

管理者またはインストラクターが共有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、生徒は管理対象Apple IDの資格情報を提供して共有iPadにサインインします。以前に教育構成ポリシーを生徒に展開している場合、生徒は共有デバイスに「Other User」としてサインインする必要がなくなります。

XenMobileは、共有iPad用に2つの通信チャネルを使用します。デバイス所有者（インストラクター）用のシステムチャネルと、現在の常駐ユーザー（生徒）用のユーザーチャネルです。XenMobileはこれらのチャネルを使用して、Appleがサポートするリソースに対して適切なMDMコマンドを送信します。

システムチャネル経由で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：教育構成、最大常駐ユーザー、およびパスコードロック猶予期間
- デバイスベースのボリューム購入アプリ

  Appleは、共有iPadでのエンタープライズアプリやユーザーベースのボリューム購入アプリをサポートしていません。共有iPadにインストールされたアプリは、デバイス全体でグローバルであり、ユーザーごとではありません。
- ユーザーベースのボリューム購入iBooks

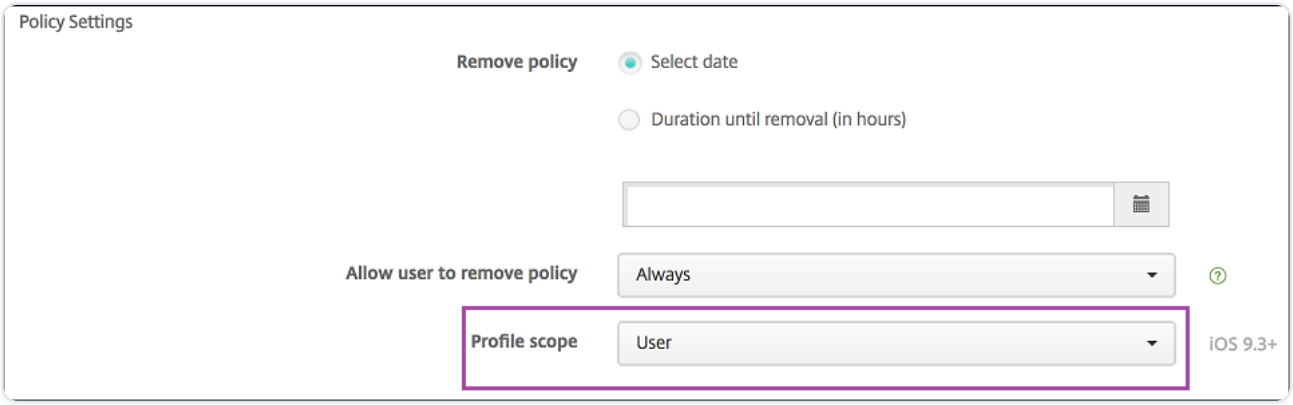
  Appleは、共有iPadでのユーザーベースのボリューム購入iBooksの割り当てをサポートしています。

ユーザーチャネルを介して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、Webクリップ

XenMobileは、ユーザーチャネルを介したこれら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際は、ポリシー設定の**Profile scope**で展開チャネルを指定します。



ユーザーチャネルを介して展開したデバイスポリシーを削除するには、プロファイル削除ポリシーの**Deployment scope**で**User**を選択していることを確認してください。

一般的なワークフロー

通常、事前構成済みで監視対象の共有iPadをインストラクターに提供します。インストラクターは、それらのデバイスを生徒に配布します。事前登録済みの共有iPadをインストラクターに配布しない場合は、インストラクターがデバイスを登録できるように、XenMobile Serverのパスワードを提供していることを確認してください。

共有iPadを構成および登録するための一般的なワークフローは次のとおりです。

1. XenMobile Serverコンソールを使用して、**Shared mode**が有効になっているASMまたはABMアカウント（**Settings** > **Apple Deployment Program**）を追加します。詳しくは、「共有iPadのASMまたはABM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されているように、必要なデバイスポリシー、アプリ、メディアをXenMobileに追加します。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. インストラクターに共有iPadのハードリセットを実行してもらいます。登録用のリモート管理画面が表示されます。
4. 教員が共有iPadを登録します。

   XenMobileは、構成されたリソースを登録済みの各共有iPadに展開します。自動再起動後、教員はデバイスを生徒と共有できます。iPadにサインインページが表示されます。
5. 生徒はクラスを選択し、管理対象Apple IDと一時的なASMまたはABMパスワードを入力します。

共有iPadはASMまたはABMで認証し、生徒にASMまたはABMパスワードの作成を促します。次回の共有iPadへのサインインでは、生徒は新しいパスワードを入力する必要があります。

6. iPadを共有している別の生徒は、前の手順を繰り返してサインインできます。

共有iPadのApple School ManagerまたはApple Business Managerアカウントを管理する

Apple EducationでXenMobileを既に使用している場合：教員が使用するデバイスなど、共有されていないデバイス用にXenMobileで構成された既存のASMまたはABMアカウントがあります。共有デバイスと非共有デバイスの両方に、同じASMまたはABMとXenMobile Serverを使用できます。

XenMobileは、次の展開シナリオをサポートしています。

- クラスごとの共有iPadのグループ

  このシナリオでは、共有iPadを生徒のクラスに割り当てます。iPadは教室に置かれたままになります。そのクラスで異なる科目を教える教員は、同じiPadのセットを使用します。

- 教員ごとの共有iPadのグループ

  このシナリオでは、共有iPadを教員に割り当て、その教員が担当するさまざまなクラスでそれらのiPadを使用します。

共有iPadをデバイスグループに整理する

ASMまたはABMを使用すると、複数のMDMサーバーを作成してデバイスをグループに整理できます。共有iPadをMDMサーバーに割り当てるときは、クラスごとまたは教員ごとに、共有iPadの各グループに対してデバイスグループを作成します。

- 共有iPadのグループ1 > デバイスグループ1 MDMサーバー
- Shared iPads のグループ 2 > デバイスグループ 2 MDM サーバー
- Shared iPads 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の ASM または ABM アカウントを追加する

XenMobile Server コンソールから複数の ASM または ABM アカウントを作成すると、Shared iPads のグループ (各クラスまたはインストラクターにつき 1 つ) が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 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 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 アカウント

Shared iPads に固有の要件は次のとおりです。

- 各デバイスグループに 1 つの ASM または ABM アカウント。以下の設定が有効になっている必要があります。
  - **デバイス登録を必須にする**
  - **監視モード**
  - **共有モード**
- 特定の教育機関の場合、すべての ASM または ABM アカウントで同じ **Education suffix** を使用していることを確認してください。

アカウントを追加するには、**設定** > **Apple Deployment Program** に移動します。

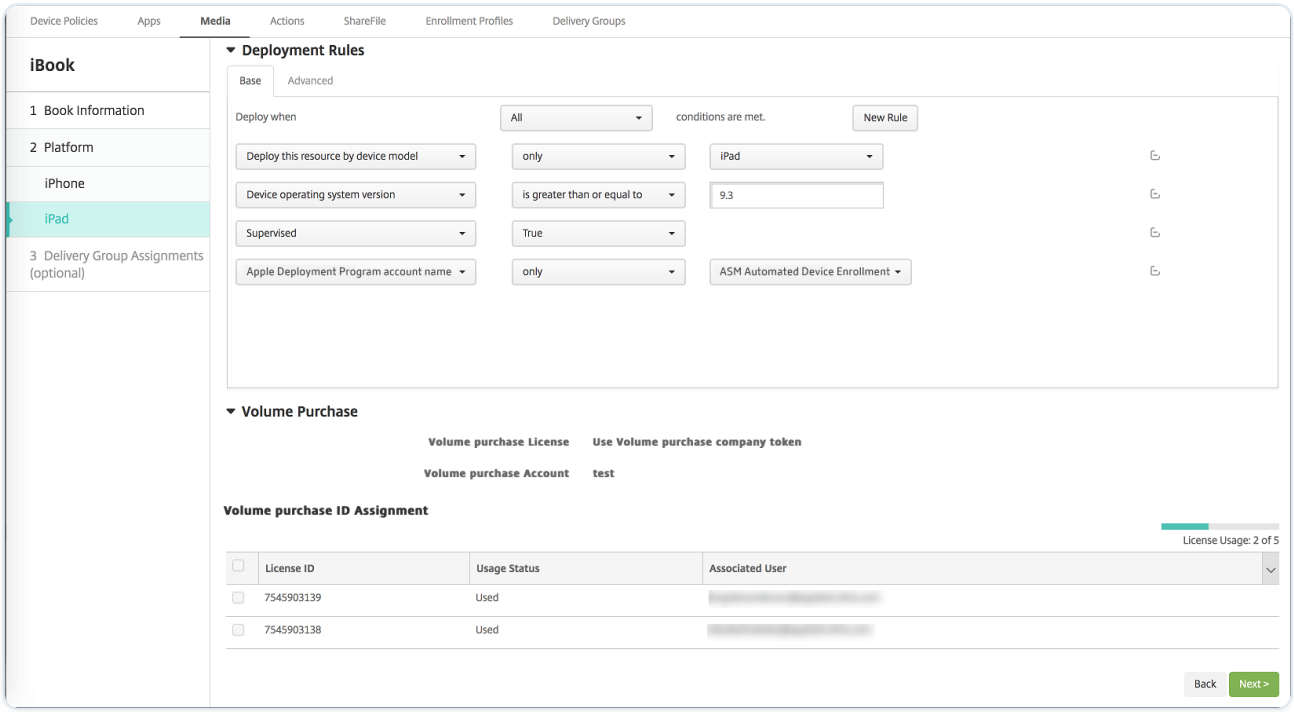
Apple Deployment Program 設定構成画面のスクリーンショット(/en-us/xenmobile/server/media/settings-dep-account-ios-shared.png)

共有iPad用アプリ

共有iPadは、デバイスベースのボリューム購入アプリの割り当てをサポートします。共有iPadにアプリを展開する前に、XenMobileはAppleボリューム購入サーバーにリクエストを送信し、ボリューム購入ライセンスをデバイスに割り当てます。ボリューム購入の割り当てを確認するには、 > > に移動し、 を展開します。

共有iPad用メディア

共有iPadは、ユーザーベースのボリューム購入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、XenMobileはAppleボリューム購入サーバーにリクエストを送信し、ボリューム購入ライセンスを学生に割り当てます。ボリューム購入の割り当てを確認するには、 > > に移動し、 を展開します。



共有iPadの展開ルール

共有iPadの展開では、デリバリーグループレベルのルールはユーザープロパティに関連するため適用されません。デバイスの各グループのポリシー、アプリ、およびメディアをフィルタリングするには、アカウント名に基づいてリソースの展開ルールを追加します。例:

- デバイスグループ1アカウントの場合、この展開ルールを設定します。

```
Apple Deployment Program account name

Only

Device Group 1 account
```

- デバイスグループ2アカウントの場合、この展開ルールを設定します。

```
Apple Deployment Program account name

Only

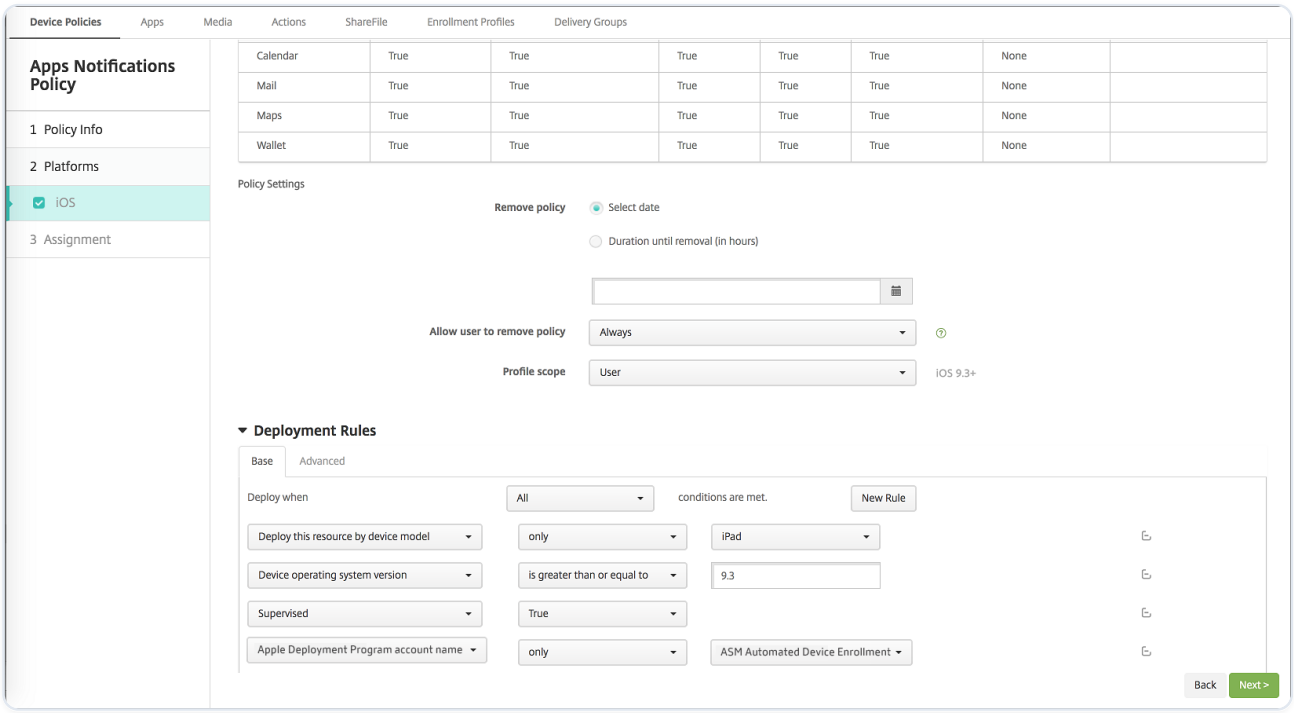
Device Group 2 account
```

- デバイスグループNアカウントの場合、この展開ルールを設定します。

```
Apple Deployment Program account name

Only

Device Group N account
```



Apple Classroomアプリをインストラクター（共有されていないiPadを使用）にのみ展開するには、これらの展開ルールを使用して、ASMまたはABMの共有ステータスでリソースをフィルタリングします。

```
Deploy this resource regarding ASM or ABM shared mode

only

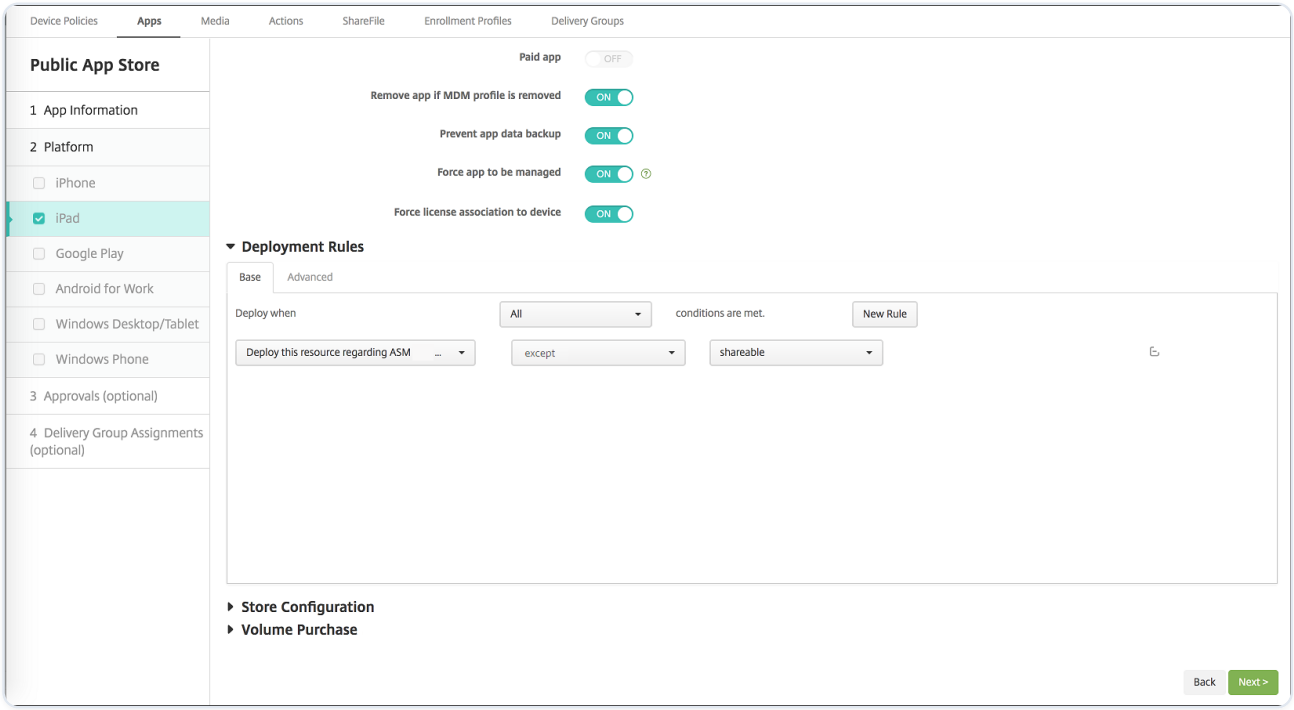
unshared
```

または:

```
Deploy this resource regarding ASM or ABM shared mode

except

shareable
```



共有iPad用デリバリーグループ

各インストラクターのデバイスグループの場合:

- 1つのデリバリーグループを構成します。インストラクターには、教育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。

デリバリーグループ構成画面(/en-us/xenmobile/server/media/configure-delivery-group-user-assignment.png)

- そのデリバリーグループには、以下のMDMリソースを含める必要があります:
    - デバイスポリシー:
        - 教育構成

    - アプリ通知
    - ホーム画面レイアウト
    - 制限
    - 最大常駐ユーザー数
    - パスコードロック猶予期間
  - 必須のボリューム購入アプリ
  - 必須のボリューム購入iBooks

デリバリーグループ構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-summary.png)

共有iPadのセキュリティアクション

既存のセキュリティアクションに加えて、Shared iPadには以下のセキュリティアクションを使用できます。

- **常駐ユーザーの取得:** 現在のデバイスでアクティブなアカウントを持つユーザーを一覧表示します。このアクションにより、デバイスとXenMobile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:** 特定のユーザーの現在のセッションを削除します。ユーザーは再度サインインできます。
- **すべてのユーザーを削除:** デバイス上のすべてのユーザーを削除します。

セキュリティアクション画面(/en-us/xenmobile/server/media/security-actions-shared-ipads.png)

常駐ユーザーの削除をクリックした後、ユーザー名を指定できます。

セキュリティアクション画面(/en-us/xenmobile/server/media/force-delete-resident-user-shared-ipad.png)

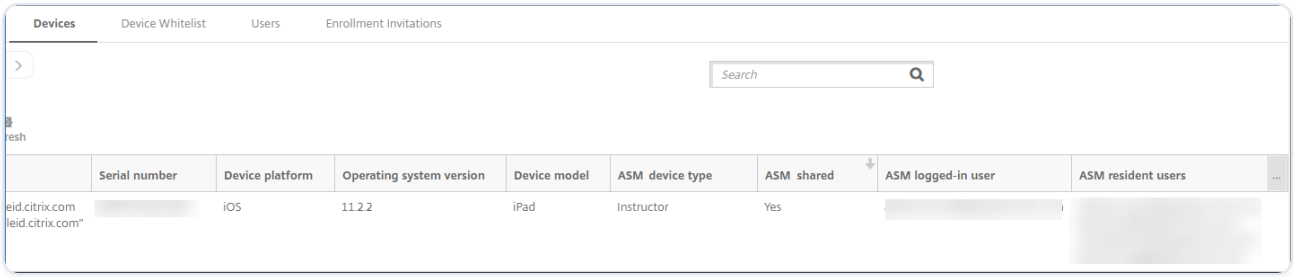
セキュリティアクションの結果は、**管理** > **デバイス** > **一般**および**管理** > **デバイス** > **デリバリーグループ**のページに表示されます。

Shared iPadに関する情報の取得

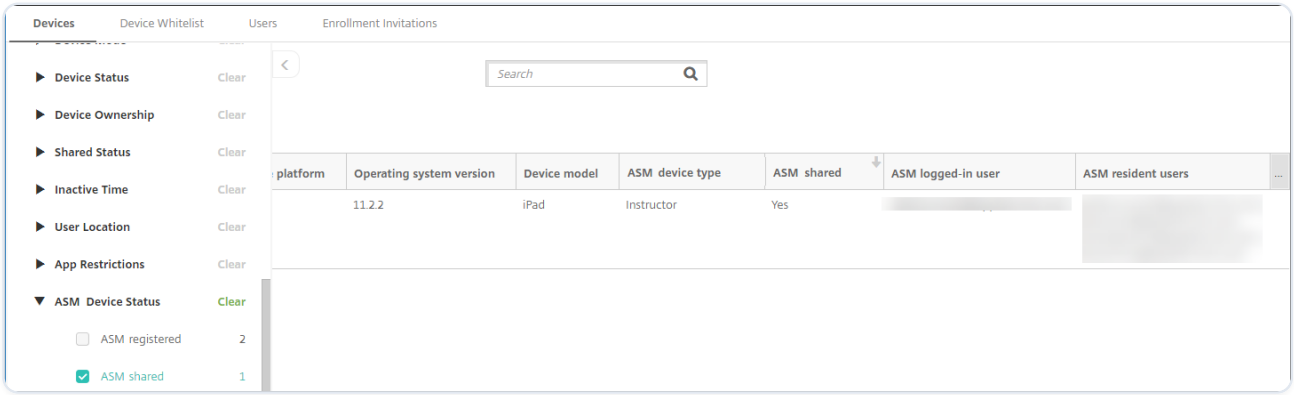
管理 > **デバイス**ページで、Shared iPadに固有の情報を確認します。

- 検索対象:
  - デバイスが共有されているかどうか（**ASMまたはABM共有**）

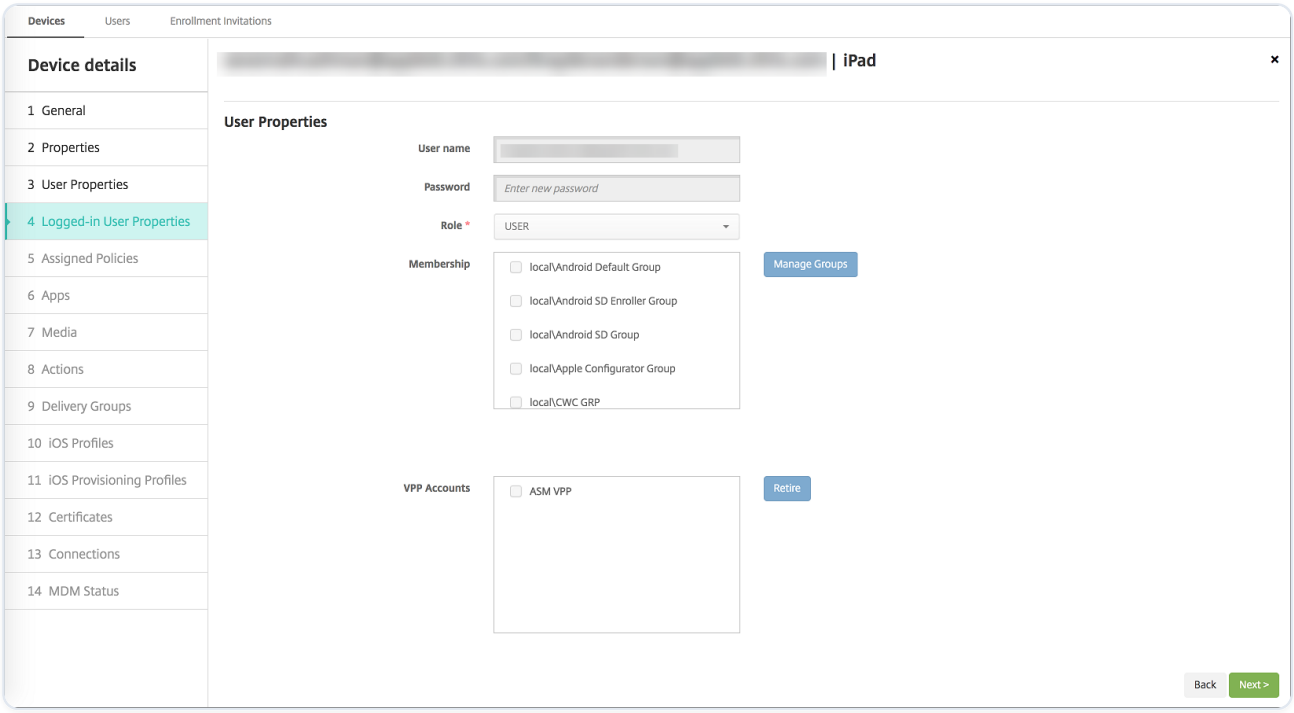
- 共有デバイスにログインしているユーザー（**ASMまたはABMログインユーザー**）
- 共有デバイスに割り当てられているすべてのユーザー（**ASMまたはABM常駐ユーザー**）

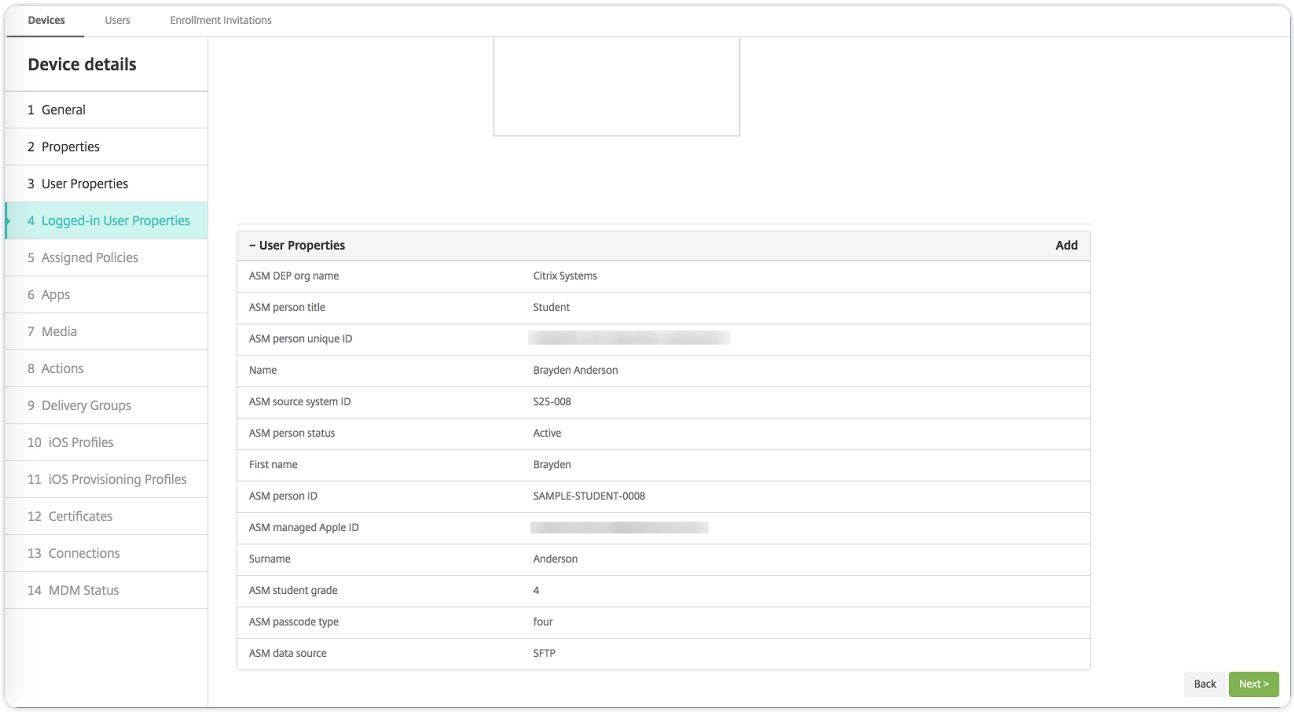


- デバイスリストを**ASMまたはABMデバイスステータス**でフィルタリングします。

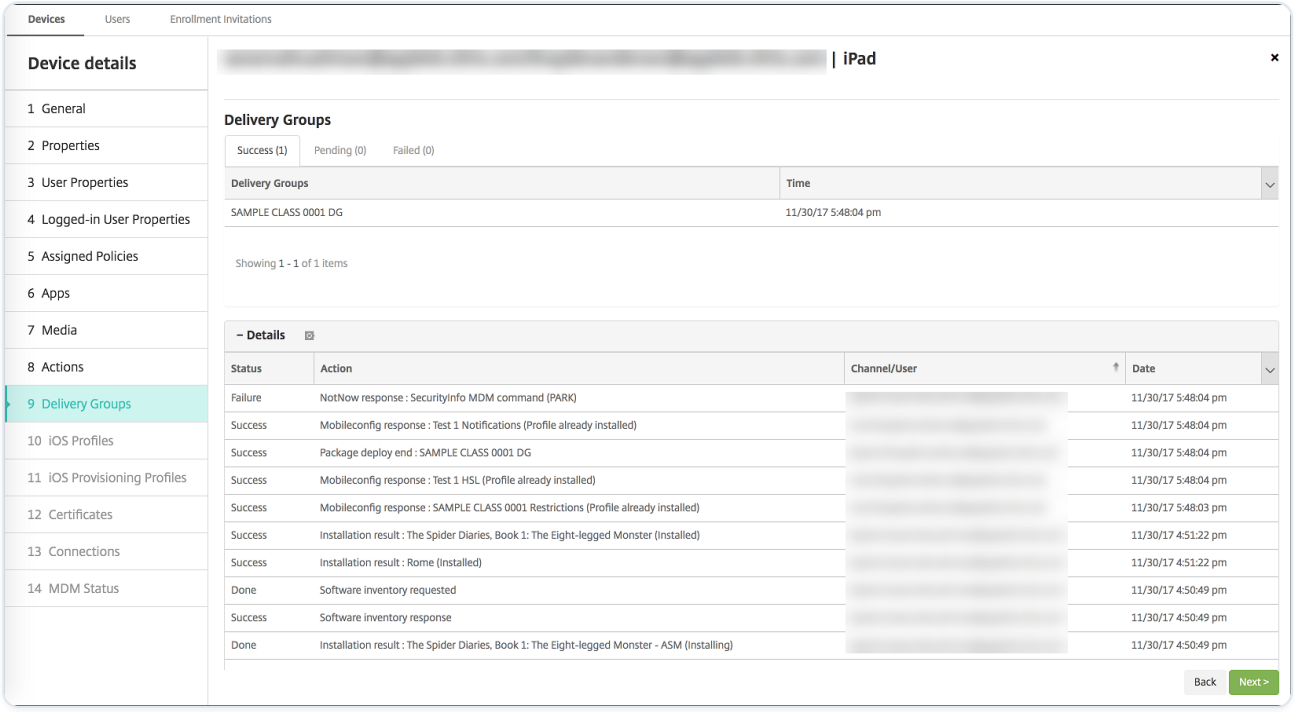


- **Manage** > **Devices** > **Logged-in User Properties**ページで、共有iPadにログインしているユーザーの詳細を表示します。



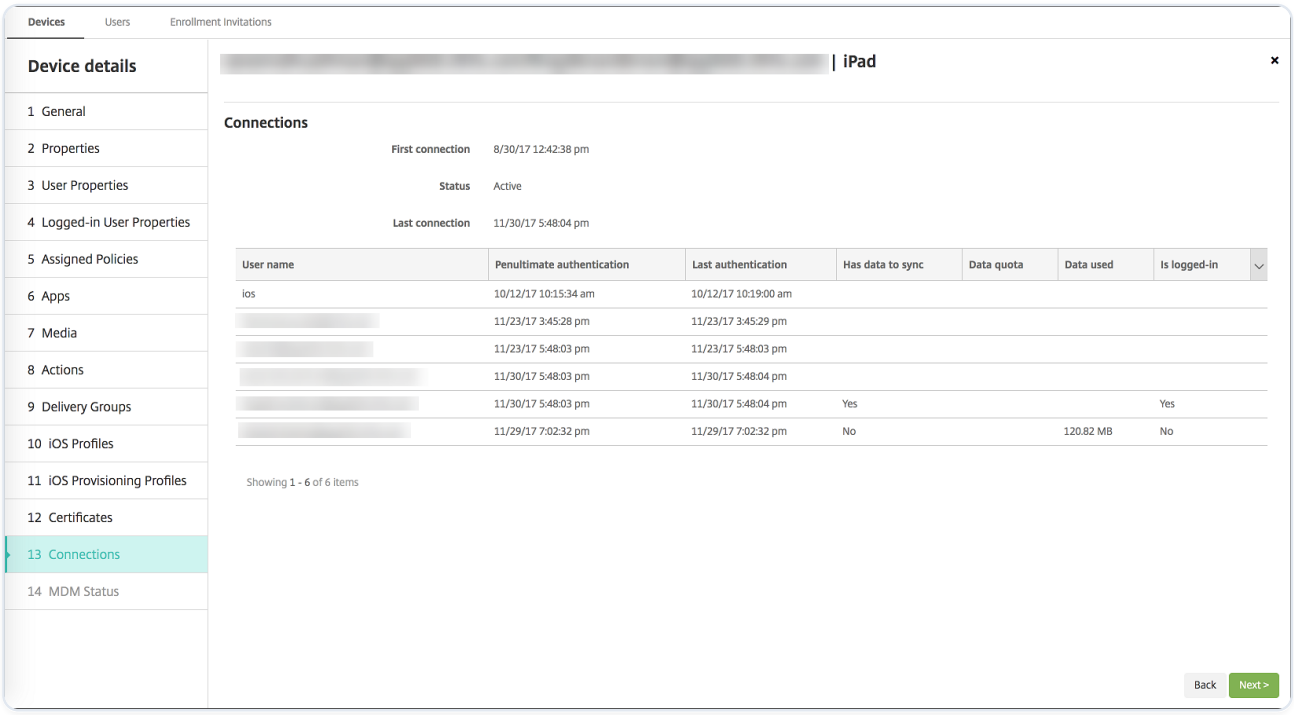


- 「**Manage** > **Devices** > **Delivery Groups**」ページで、デリバリーグループ内のインストラクターとユーザーにリソースを展開するために使用されるチャネルを確認します。「**Channel/ User**」列には、タイプ（**System** または **User**）および受信者（インストラクターまたは学生）が表示されます。

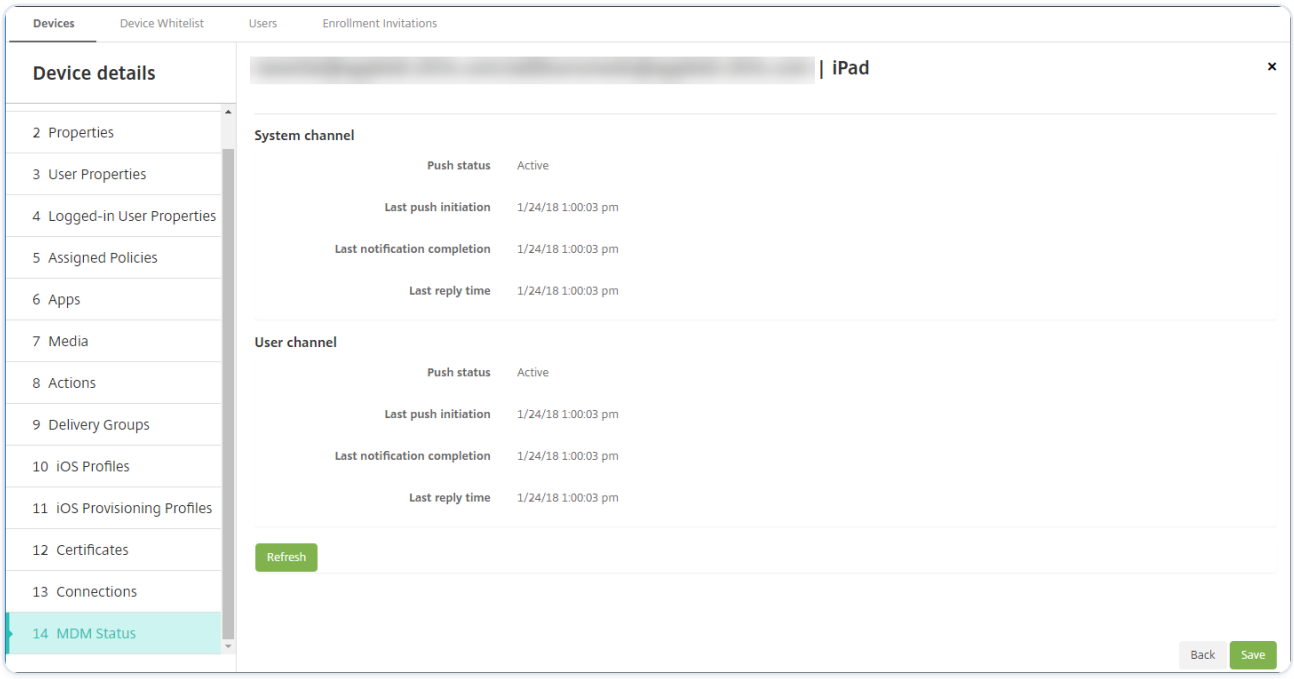


- 常駐ユーザーに関する情報を取得します。
  - **同期するデータがあるか:** ユーザーがクラウドに同期するデータを持っているかどうか。

- **データクォータ:** ユーザーに設定されたデータクォータ（バイト単位）。ユーザーのクォータが一時的にオフになっている場合や、ユーザーに適用されていない場合は、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）。システムが情報を収集する際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。
- **ログイン済み:** ユーザーがデバイスにログイ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表示します。



Appleアプリの配布

XenMobileは、デバイスに展開されたアプリを管理します。以下の種類のiOS/iPadOSおよびmacOSアプリを整理して展開できます。

- **パブリックApp Store (iOS/iPadOSのみ):** これらのアプリには、Apple App StoreやGoogle Playなどのパブリックアプリストアで入手できる無料または有料のアプリが含まれます。例: GoToMeeting。
- **エンタープライズ (iOS/iPadOS/macOS):** MDXが有効になっておらず、MDXアプリに関連付けられたポリシーを持たないネイティブアプリ。
- **MDX (iOS/iPadOSのみ):** MAM SDKで準備された、またはMDX Toolkitでラップされたアプリ。これらのアプリにはMDXポリシーが含まれます。MDXアプリは、内部ソースおよびパブリックストアから入手できます。
- **ボリューム購入 (iOS/iPadOS/macOS):** Appleボリューム購入プログラムを通じてライセンスが管理されるアプリ。
- **iOSカスタムアプリ (iOS/iPadOSのみ):** 社内またはサードパーティによって開発された独自の企業間アプリ。

さまざまな種類のアプリの詳細については、アプリの追加を参照してください。

一部の展開では、Apple Business Management (ABM) またはApple School Management (ASM) アカウントが必要です。詳細については、以下のセクションを参照してください。

Citrixは、アプリの種類と配布方法ごとに、一連の構成プラクティスを推奨しています。他のプラットフォームへのアプリの配布については、アプリの追加を参照してください。以下のセクションでは、iOSアプリの構成に関する詳細情報を提供します。

アプリ配布の一般的な手順

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
(#public-app-store-apps) (Citrix®モビリティアプリを含む)	該当なし	**XenMobile®の場合:** **[構成] > [アプリ]** で、iPhoneまたはiPad用の**パブリックアプリストア**アプリを追加します。アプリを構成し、デリバ	**XenMobileの場合:** デリバリーグループを使用してアプリを構成および展開します。

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
		リーグループに割り当てます。	
(#public-app-store-apps-delivered-with-apple-volume-purchase) (Citrixモビリティアプリを含む)	Apple展開プログラムに登録します。**XenMobileの場合:** **[設定] > [ボリューム購入]** に移動して、ボリューム購入アカウントを追加します。	**ABMまたはASMの場合:** [アプリとブック]からアプリを購入して追加します。**XenMobileの場合:** **[構成] > [アプリ]** に移動し、アプリを構成してデリバリーグループに割り当てます。	**XenMobileの場合:** デリバリーグループを使用してアプリを構成および展開します。
(#enterprise-apps)	該当なし	**XenMobileの場合:** **[構成] > [アプリ]** に移動します。**[追加]** をクリックし、次に **[エンタープライズ]** をクリックします。IPAファイルをアップロードします。アプリを構成し、デリバリーグループに割り当てます。	**XenMobileの場合:** デリバリーグループを使用してアプリを構成および展開します。
(#mdx-apps)	該当なし	**XenMobileの場合:** **[構成] > [アプリ]** に移動します。**[追加]** をクリックし、次に **[MDX]** をクリックします。プラットフォームとして**iPad/iPhone**を選択していることを確認してください。MDXファイルをアップロードします。アプリを構成し、デリバリーグ	**XenMobileで:** デリバリーグループを使用してアプリを構成および展開します。

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
		ループに割り当てます。	
Appleボリューム購入を使用して配布されるMDXアプリ	Apple展開プログラムに登録します。**XenMobileで: 設定 > ボリューム購入**に移動して、ボリューム購入アカウントを追加します。	**ABMで:** 「Appとブック」からMDXアプリを購入して追加します。アプリをABMアカウントにリンクします。**XenMobileで: 構成 > アプリ**に移動し、アプリを構成してデリバリーグループに割り当てます。	**XenMobileで:** デリバリーグループを使用してアプリを構成および展開します。
カスタムアプリ	Apple展開プログラムに登録します。**XenMobileで: 設定 > ボリューム購入**に移動して、ボリューム購入アカウントを追加します。	**ABMで:** アプリをプライベートアプリとしてApp Storeに追加します。アプリをABMアカウントにリンクします。**XenMobileで: 構成 > アプリ**に移動し、アプリを構成してデリバリーグループに割り当てます。	**XenMobileで:** デリバリーグループを使用してアプリを構成および展開します。
MDX対応カスタムアプリ	Apple展開プログラムに登録します。**XenMobileで: 設定 > ボリューム購入**に移動して、ボリューム購入アカウントを追加します。	**ABMで:** アプリをプライベートアプリとしてApp Storeに追加します。アプリをABMアカウントにリンクします。**XenMobileで: 構成 > アプリ**に移動してMDXファイルをアップロードします。アプリを構成してデリ	**XenMobileで:** デリバリーグループを使用してアプリを構成および展開します。

シナリオ	ステップ1: アカウントのリンク	ステップ2: アプリの追加と構成	ステップ3: デリバリーグループの構成とアプリの展開
		バリーグループに割り当てます。	

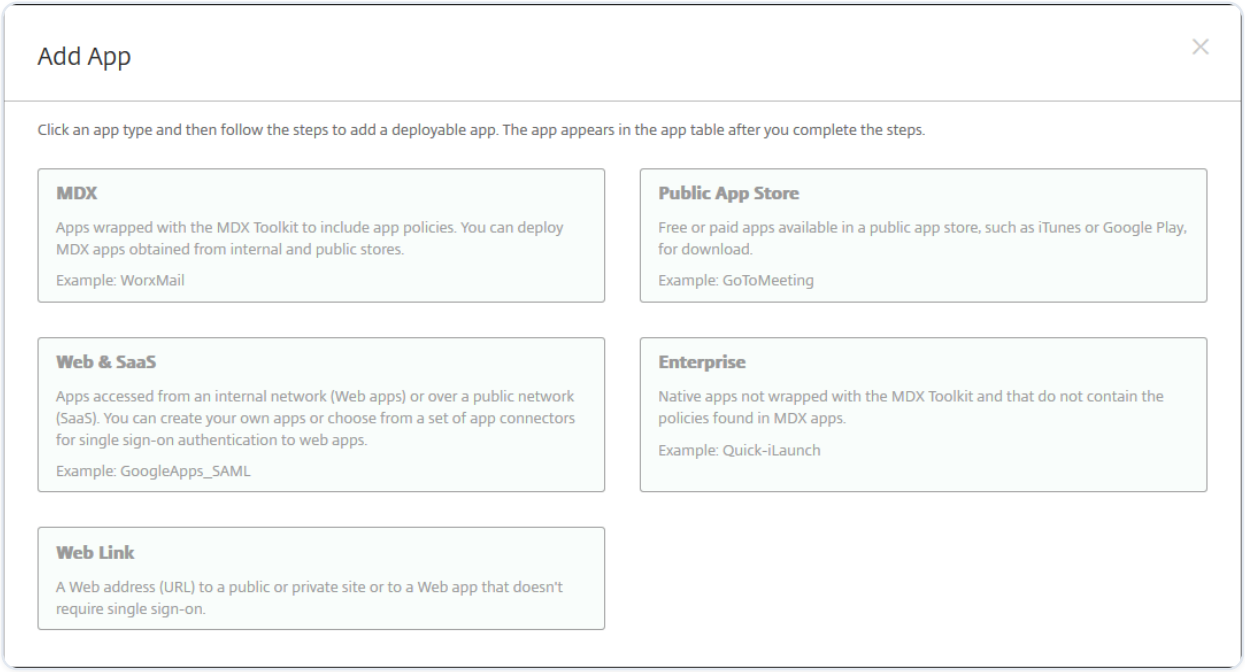
パブリックApp Storeアプリ

App Storeで利用可能な無料アプリと有料アプリをXenMobileに追加できます。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	いいえ
利用可能	iOS/iPadOS

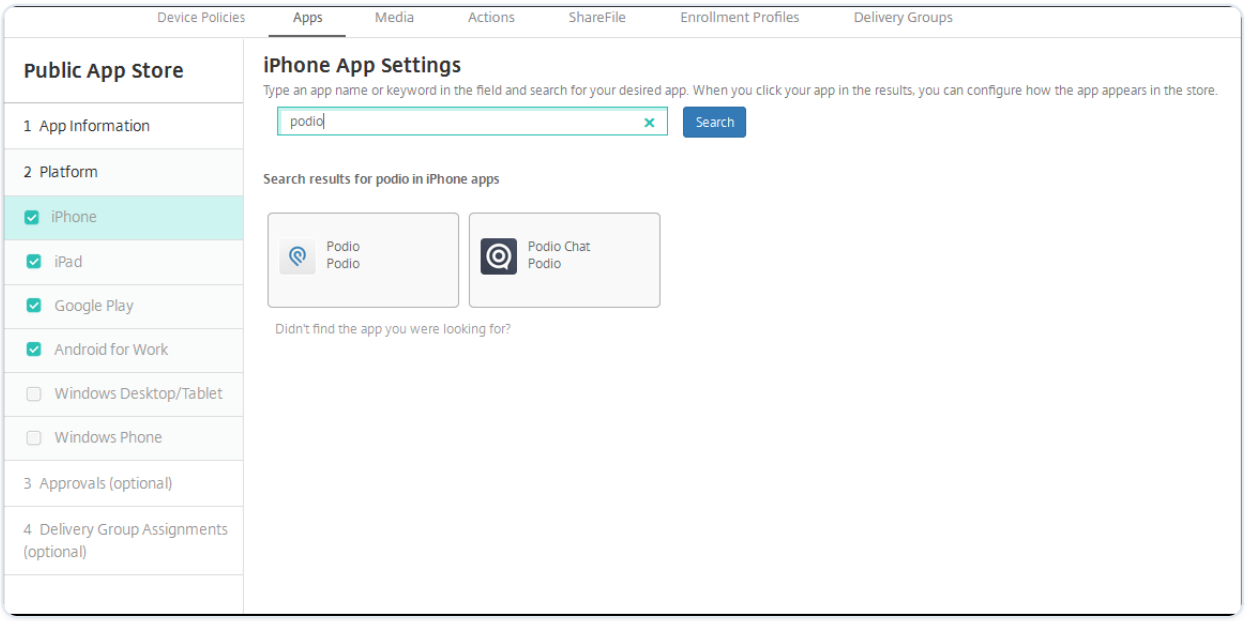
ステップ1：アプリの追加と構成

1. XenMobileコンソールで、**構成 > アプリ**に移動します。**追加**をクリックします。
2. **パブリックアプリストア**をクリックします。



3. プラットフォームとして**iPhone**または**iPad**を選択します。

4. 検索ボックスにアプリ名を入力し、**検索**をクリックします。

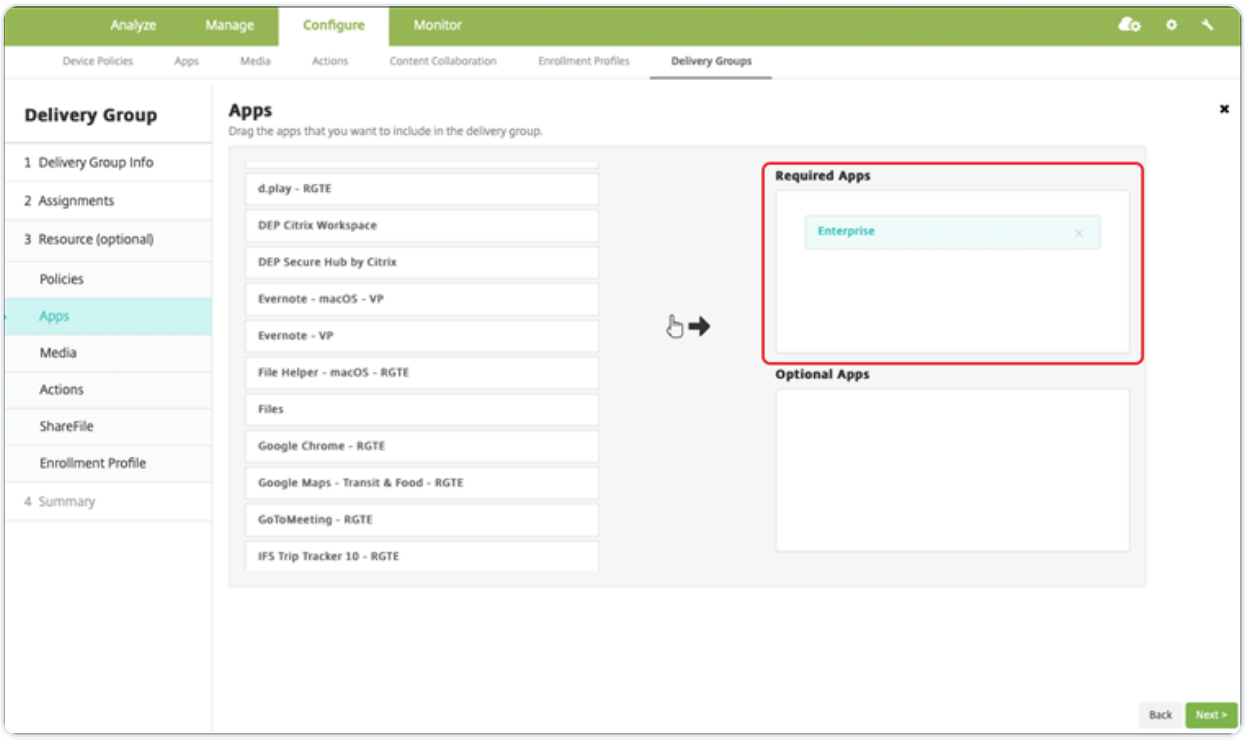


5. 検索条件に一致するアプリが表示されます。目的のアプリをクリックします。
6. アプリにデリバリーグループを割り当て、**保存**をクリックします。

ステップ2：アプリの展開を構成する

1. XenMobileコンソールで、**構成 > アプリ**に移動します。
2. 構成するアプリを選択し、**編集**をクリックします。
3. Citrixは、**アプリの管理を強制**機能を有効にすることを推奨します。
4. 配信グループを割り当てて、**保存**をクリックします。
5. **構成 > 配信グループ > アプリ**に移動します。

6. 目的のアプリを**必須**としてマークします。



7. **構成 > 配信グループ**に戻ります。
8. 配信グループを選択し、**展開**をクリックします。
9. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。



Appleボリューム購入で配信されるパブリックアプリストアアプリ

Appleボリューム購入プログラムを通じてiOS/iPadOSアプリライセンスを管理できます。XenMobileにボリューム購入アプリを追加するには、次の手順に従います。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS/macOS

ステップ 1: アカウントをリンクする

1. Apple Business Manager (ABM) または Apple School Manager (ASM) を設定して登録します。これらのプログラムの詳細については、Apple ドキュメントを参照してください。
2. ABM/ASM アカウントを XenMobile にリンクします。ボリューム購入アカウントのリンクの詳細については、Apple ボリューム購入を参照してください。
3. ボリューム購入アカウントを追加するときに、**App Auto Update** を有効にします。この設定により、Apple Store でアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的にアップデートされるようになります。

ステップ 2: Apple からアプリとライセンスを取得する

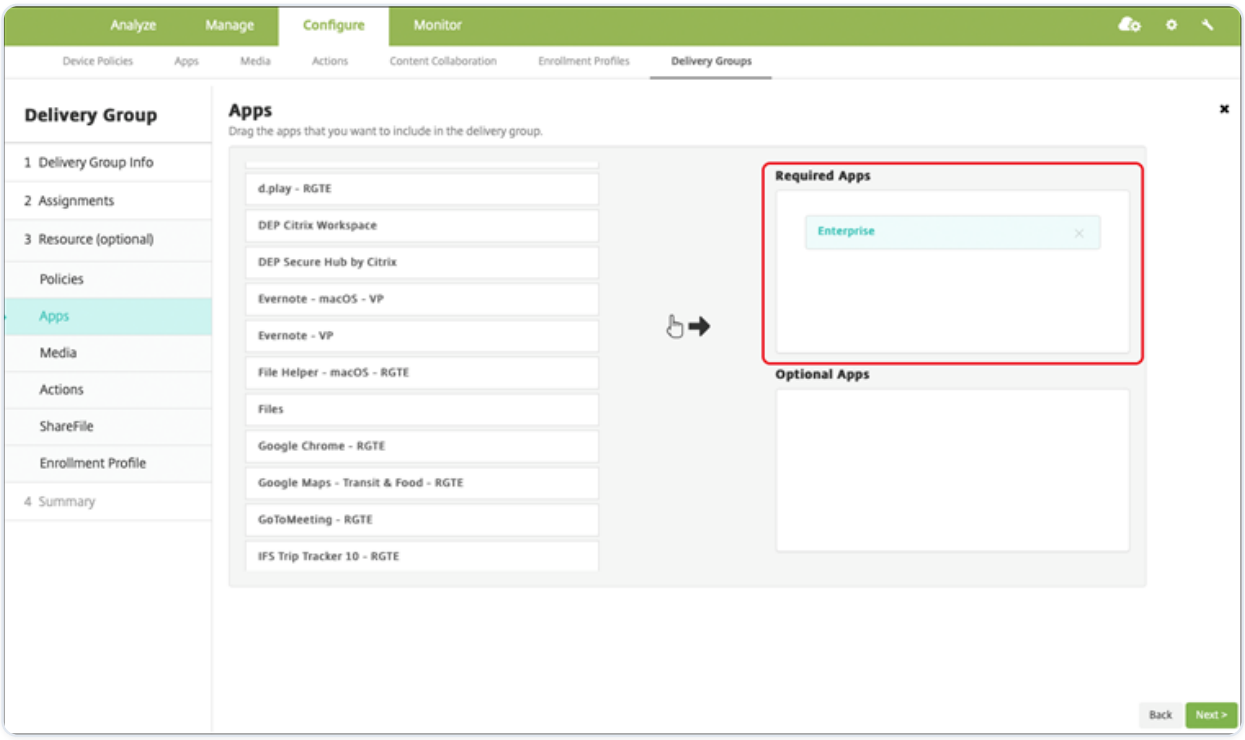
ABM/ASM アカウントにアプリを追加します。Apple App Store または Apple Books (iOS/iPadOS のみ) から購入を追加できます。無料のアプリであっても、すべてのアプリを購入する必要があることに注意してください。

ビジネスでアプリを利用可能にする方法については、Apple ドキュメントを参照してください。

ステップ 3: アプリの展開を構成する

1. XenMobile コンソールで、**Configure > Apps** に移動します。
2. 構成するボリューム購入アプリを選択し、**Edit** をクリックします。
3. プラットフォームを選択します: **iPhone**、**iPad**、または **macOS**。
4. Citrix は、**Force app to be managed** 機能 (iOS/iPadOS のみ) を有効にすることをお勧めします。
5. 配信グループを割り当てて、**保存**をクリックします。
6. **構成 > 配信グループ > アプリ**に移動します。

7. 目的のアプリを**必須**としてマークします。



8. **構成 > 配信グループ**に戻ります。
9. 配信グループを選択し、**展開**をクリックします。
10. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。



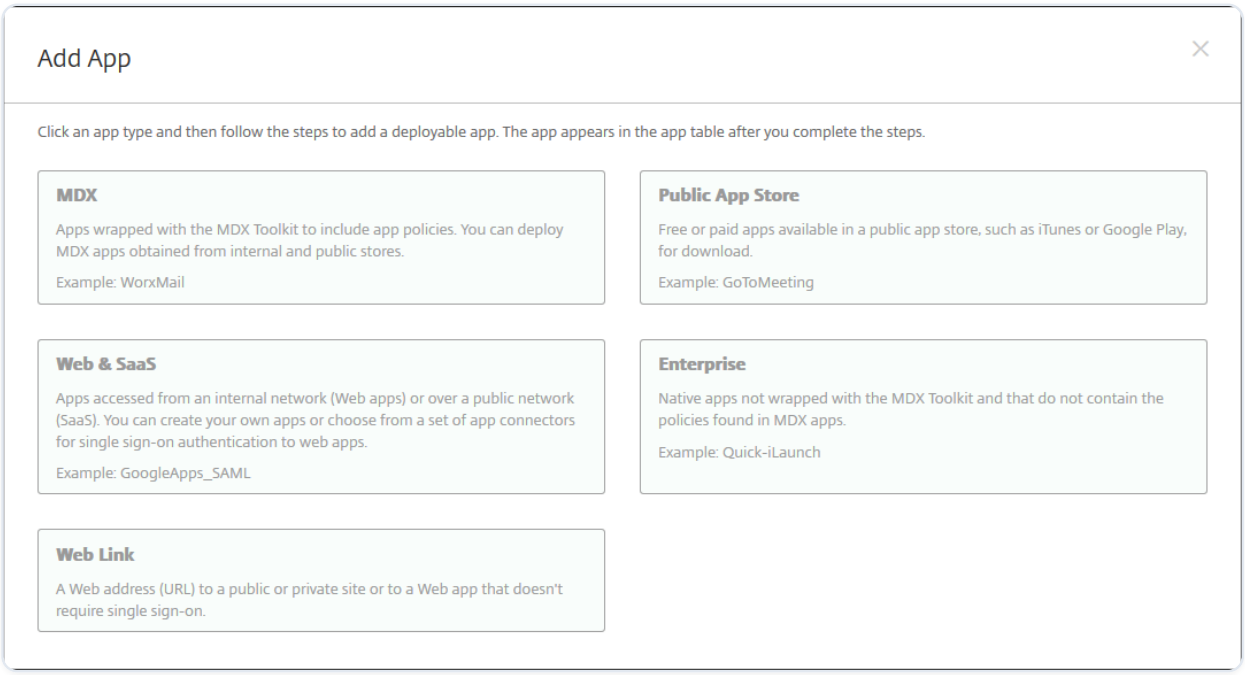
エンタープライズアプリ

MDXポリシーが関連付けられていないネイティブアプリを追加することもできます。App Storeにないアプリを追加するには、次の手順に従います。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
OS	iOS/iPadOS/macOS

ステップ 1: アプリの追加と構成

1. XenMobileコンソールで、**Configure > Apps**に移動します。**Add**をクリックします。
2. **Enterprise**をクリックします。

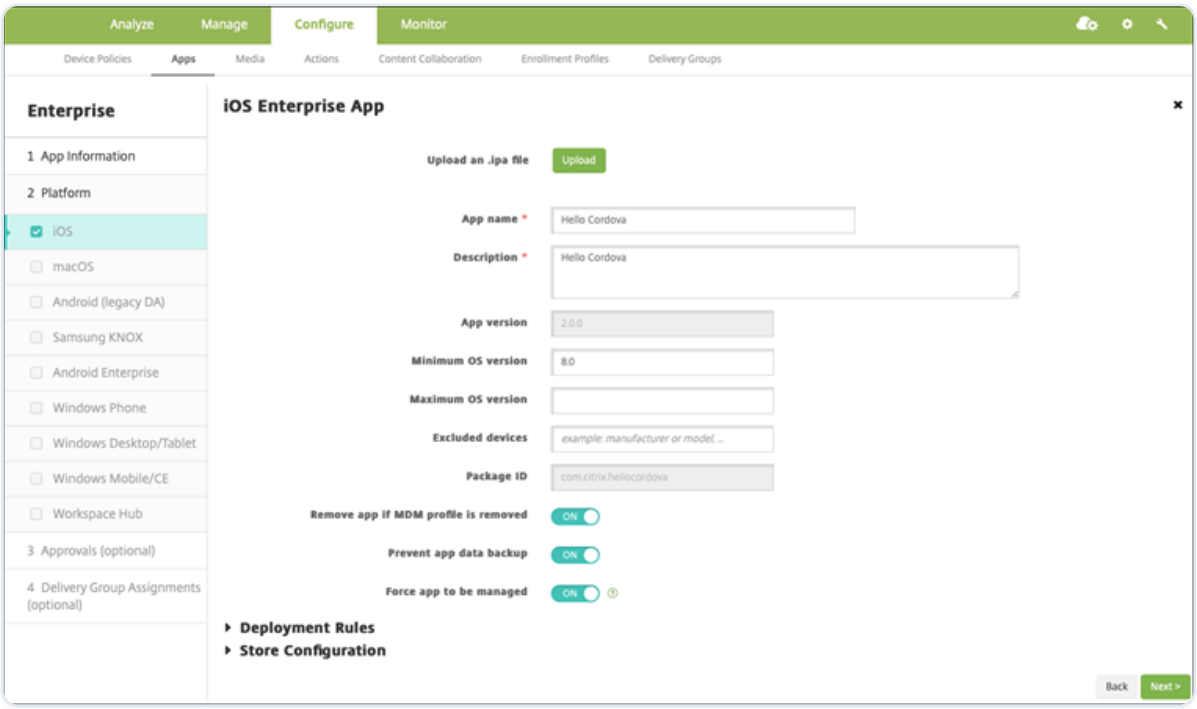


3. **App information**ページで、以下を構成します。
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルのの下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。
4. **Next**をクリックします。**App Platforms**ページが表示されます。
5. プラットフォームを選択します: **iPhone**、**iPad**、または**macOS**。

6. IPAファイル (iOS/iPadOS) をアップロードするか、PKGファイル (macOS) をアップロードします
7. **Next**をクリックします。**App details**ページが表示されます。
8. これらの設定を構成します。

    - **ファイル名:** オプションで、アプリの新しい名前を入力します。
    - **アプリの説明:** オプションで、アプリの新しい説明を入力します。
    - **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:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
    - **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
    - **除外デバイス:** オプションで、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場合にアプリを削除:** MDMプロファイルが削除されたとき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ONです。(iOS/iPadOSのみ)
    - **アプリのデータバックアップを防止:** アプリがデータをバックアップするのを防止するかどうかを選択します。デフォルトはONです。(iOS/iPadOSのみ)
    - **アプリの管理を強制:** 管理されていないアプリをインストールする場合、監視されていないデバイスのユーザーにアプリの管理を許可するプロンプトを表示させたい場合は、**ON**を選択します。ユーザーがプロンプトを受け入れると、アプリは管理されます。(iOS/iPadOSの

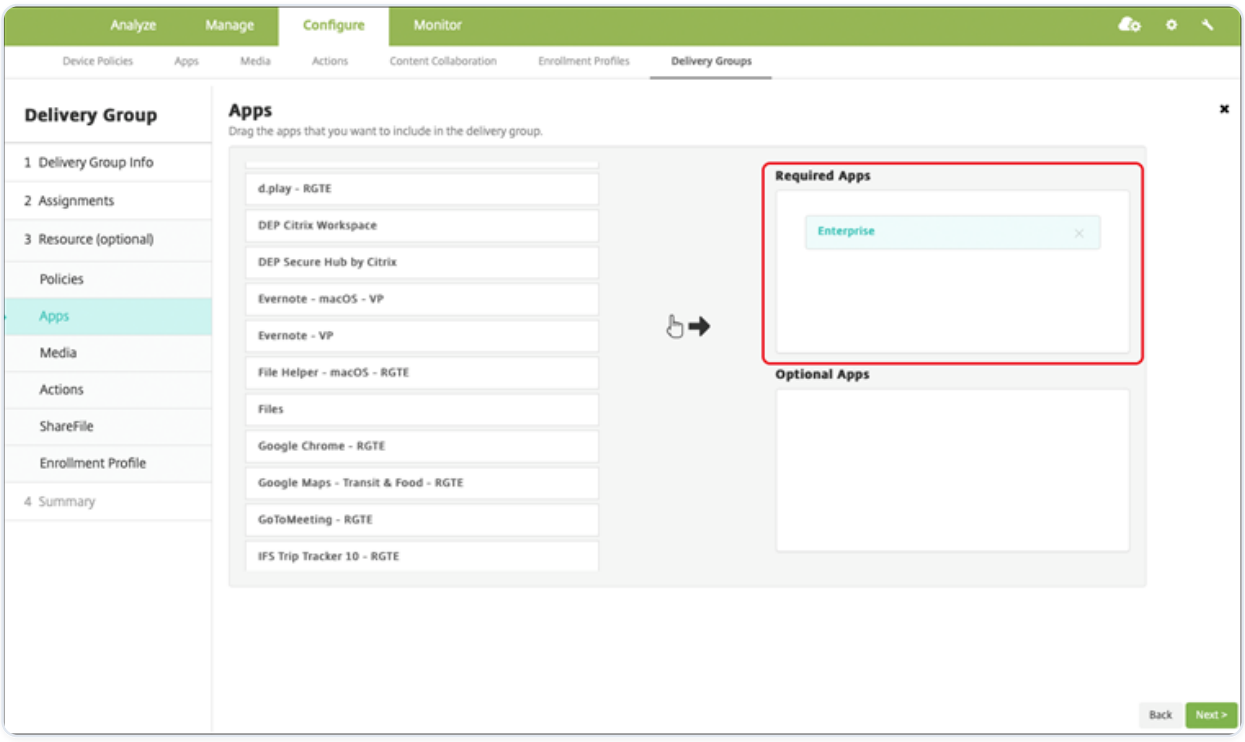
み)



9. アプリにデリバリーグループを割り当て、**保存**をクリックします。

ステップ2：アプリの展開を構成する

1. XenMobileコンソールで、**構成 > デリバリーグループ**に移動します。構成するデリバリーグループを選択し、**アプリ**ページをクリックします。
2. 必要なアプリを**必須**としてマークします。



3. **構成 > デリバリーグループ**に移動します。

4. デリバリーグループを選択し、**展開**をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。



MDXアプリ

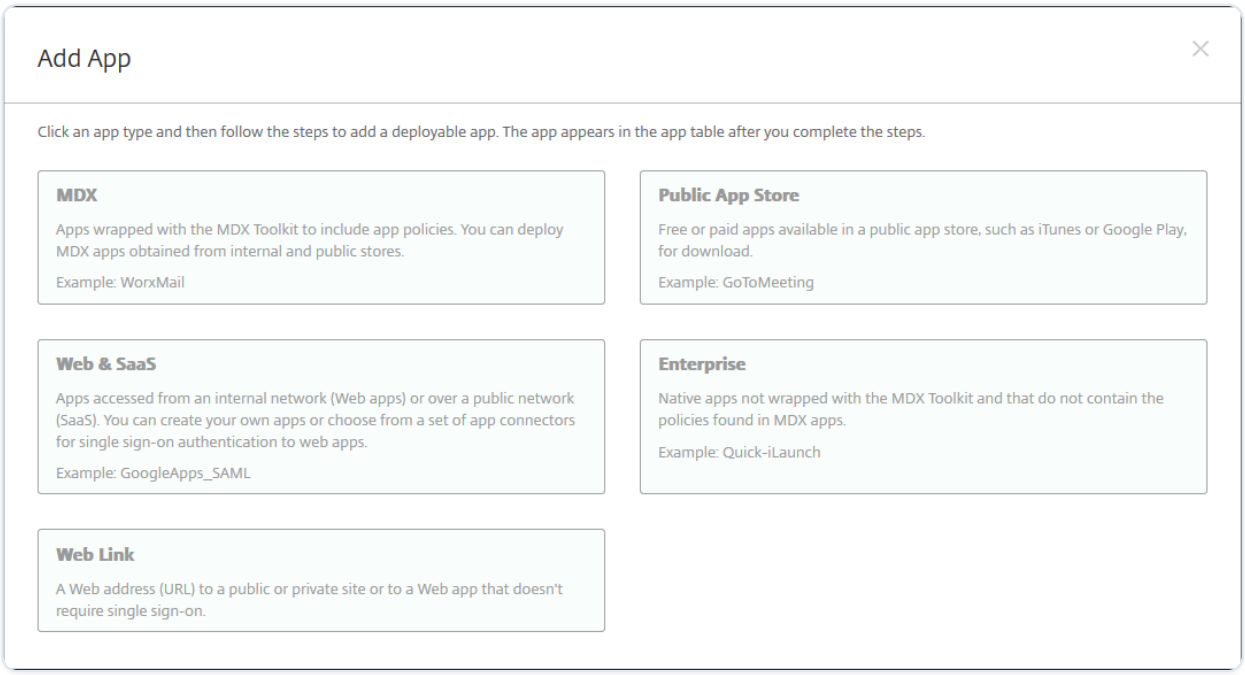
MDXポリシーとセキュリティ機能を使用するには、MAM SDKが有効になっているか、MDXでラップされたアプリを追加します。MDXアプリは、ボリューム購入を使用しても使用しなくても展開できます。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能なOS	iOS/iPadOS

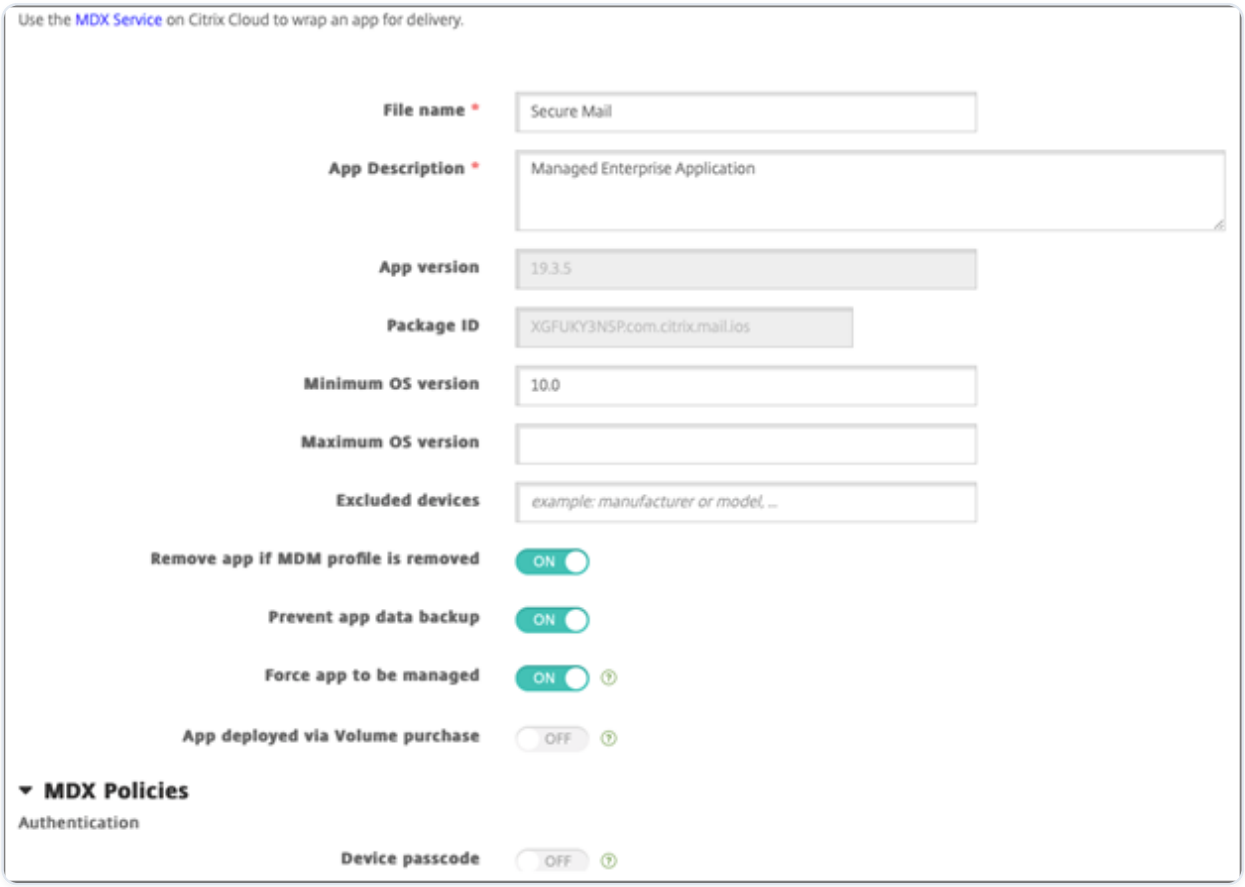
ステップ1：アプリの追加と構成

1. XenMobileコンソールで、 > に移動します。 をクリックします。

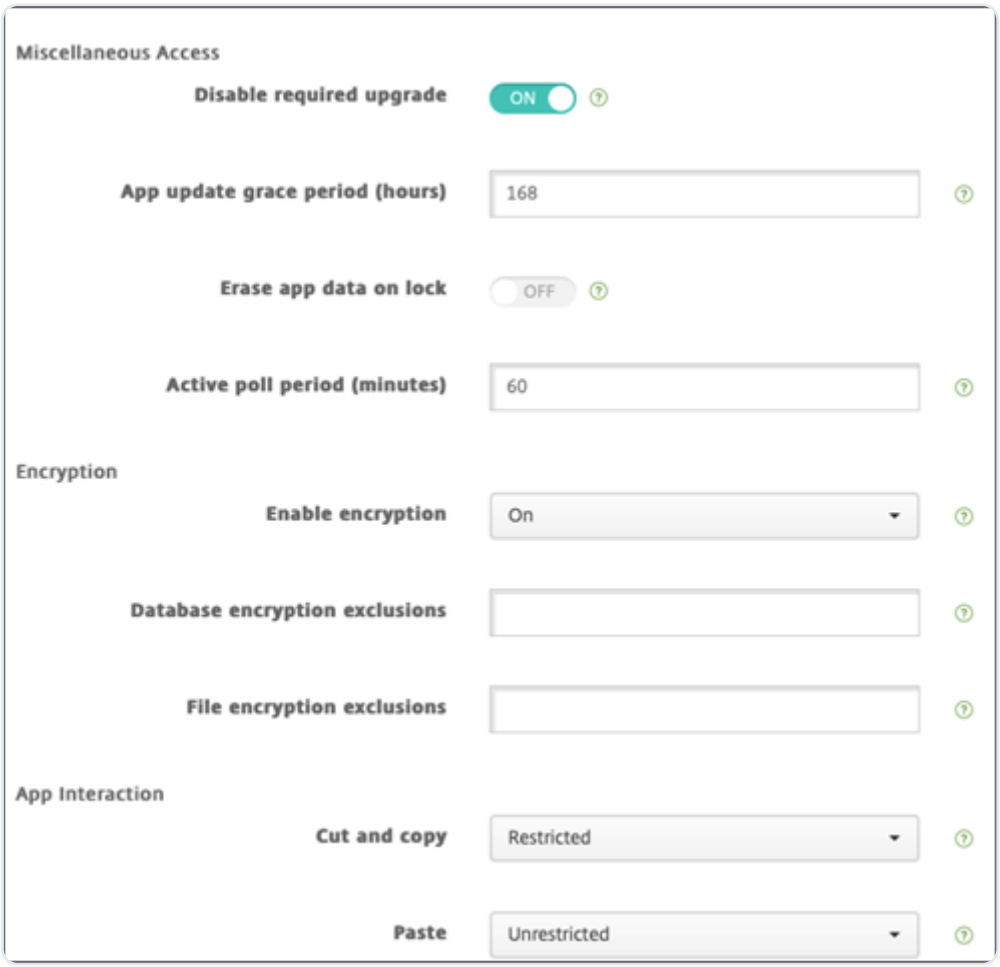
2. をクリックします。



3. プラットフォームとして または を選択します。
4. MDXファイルをアップロードします。
5. アプリの詳細を構成します。 を に設定します。Citrixは、 機能を有効にすることも推奨しています。



6. MDXポリシーを構成します。 を に設定します。

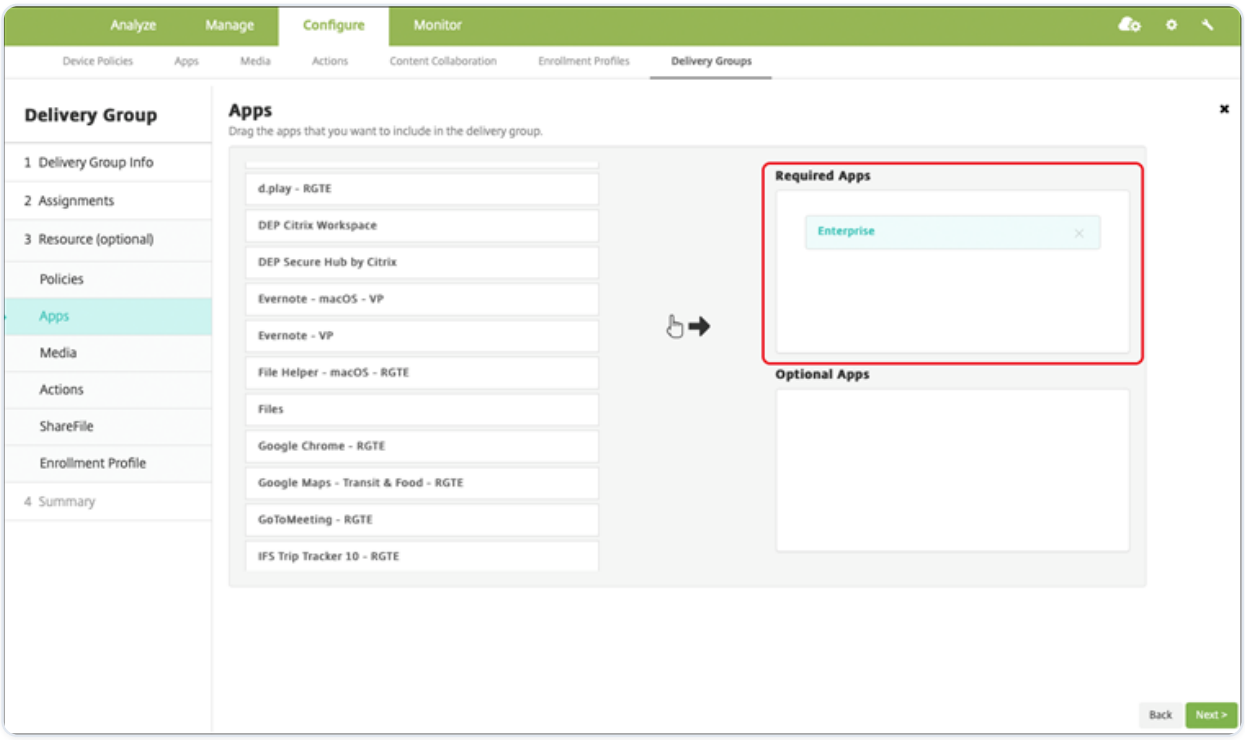


7. アプリにデリバリーグループを割り当て、 をクリックします。

ステップ 2: アプリの展開を構成する

1. XenMobile コンソールで、 **［構成］ > ［デリバリーグループ］ > ［アプリ］** の順に移動します。

2. 目的のアプリを ［**必須**］ としてマークします。



3. ［**構成**］ > ［**デリバリーグループ**］ の順に移動します。
4. デリバリーグループを選択し、 ［**展開**］ をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承諾するとアプリはバックグラウンドでインストールされます。



Apple ボリューム購入を使用して配布される MDX アプリ

MDX ポリシーとセキュリティ機能を使用するには、MAM SDK が有効になっているアプリまたは MDX でラップされたアプリを追加します。ボリューム購入を使用してアプリを展開するには、アプリがアプリストアに存在している必要があります。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能なプラットフォーム	iOS/iPadOS

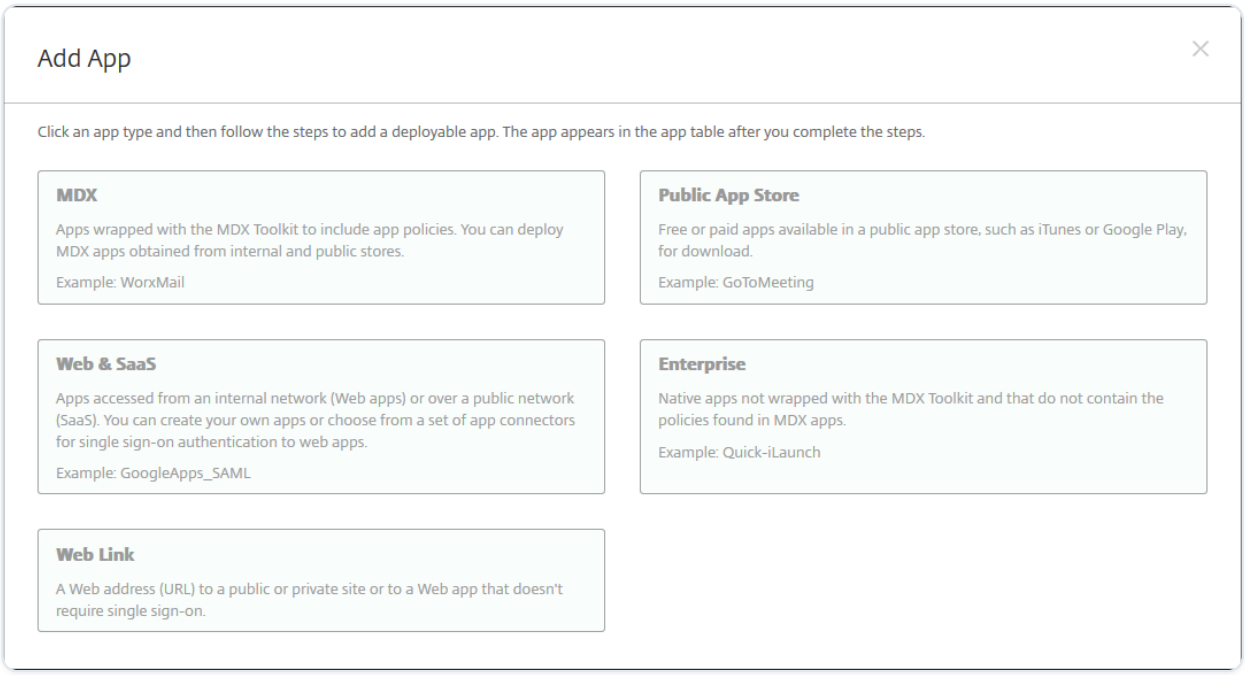
ステップ 1: アカウントをリンクする

1. Apple Business Manager (ABM) または Apple School Manager (ASM) を設定して登録します。これらのプログラムの詳細については、Appleのドキュメントを参照してください。
2. XenMobile に ABM/ASM アカウントをリンクします。ボリューム購入アカウントのリンクの詳細については、Appleボリューム購入を参照してください。
3. ボリューム購入アカウントを追加するときは、**アプリの自動更新**を有効にします。この設定により、Apple Store でアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。

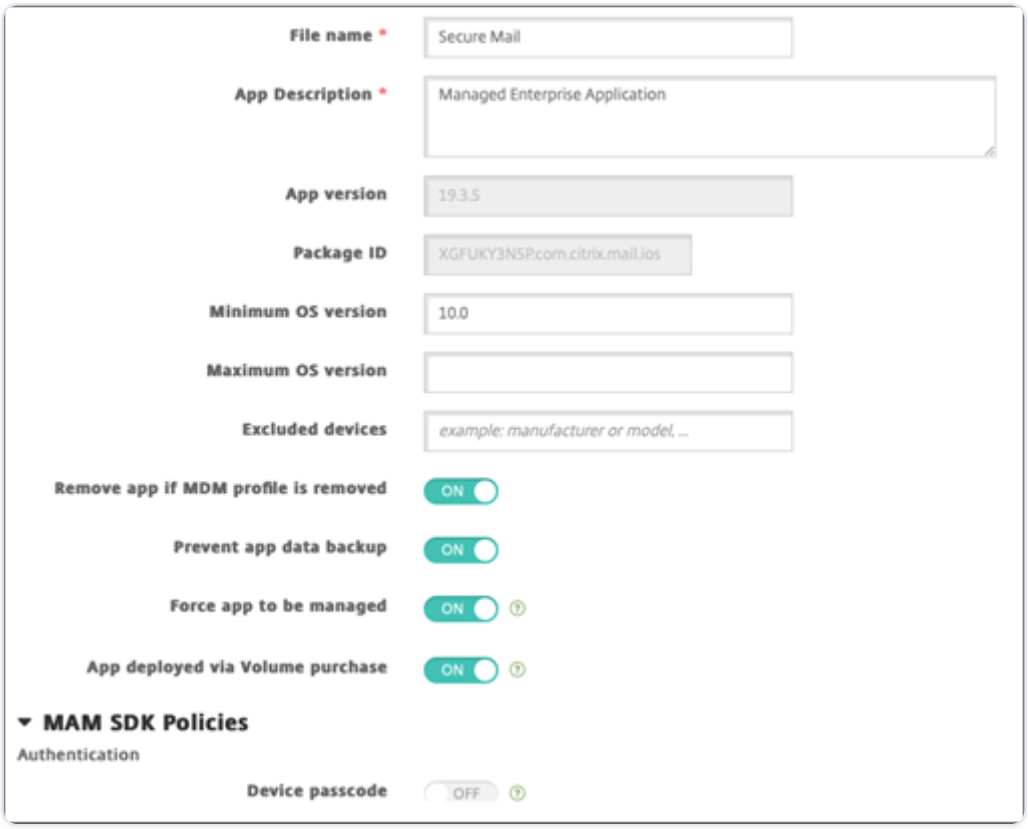
ステップ 2: アプリを追加して構成する

1. XenMobile コンソールで、**Configure > Apps** に移動します。**追加**をクリックします。

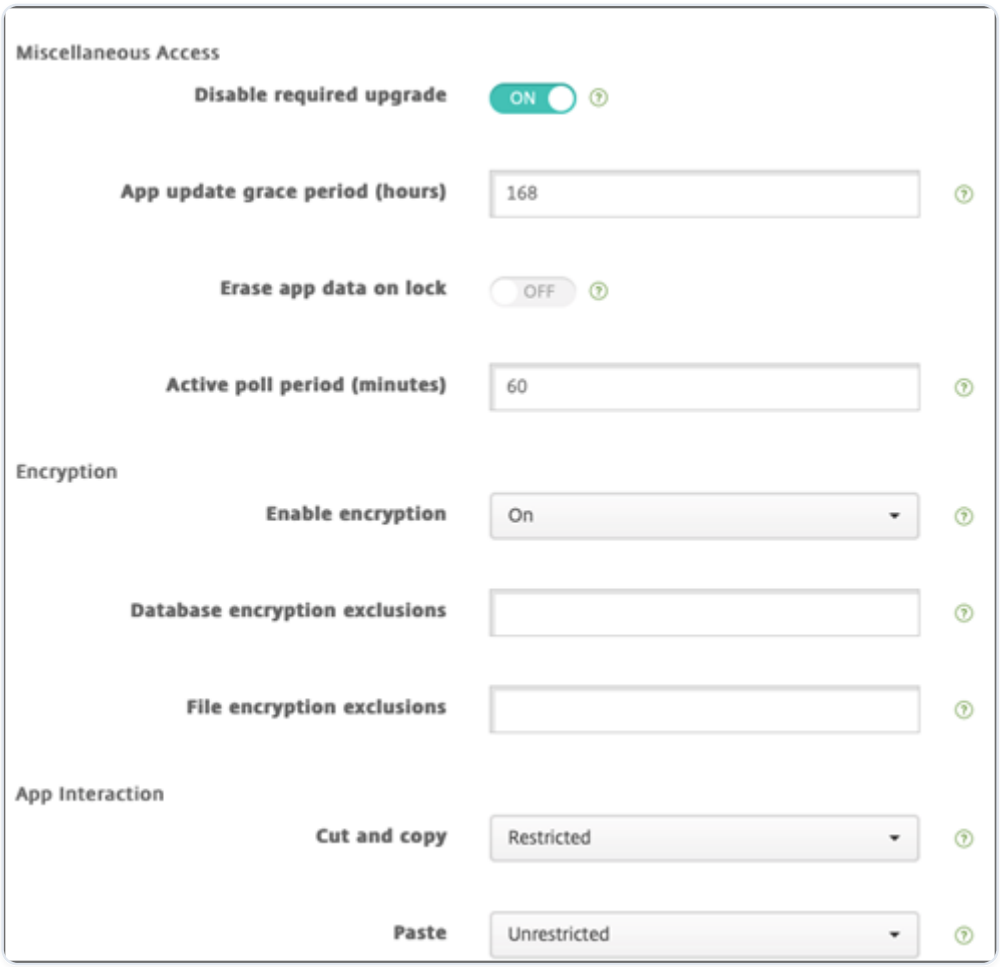
2. **MDX**をクリックします。



3. プラットフォームとして**iPhone**または**iPad**を選択します。
4. MDXファイルをアップロードします。
5. アプリの詳細を構成します。**ボリューム購入経由で展開されたアプリ**を**オン**に設定します。Citrix は、**アプリの管理を強制**機能を有効にすることも推奨しています。



6. MDXポリシーを構成します。**必須アップグレードを無効にする**を**オン**に設定します。



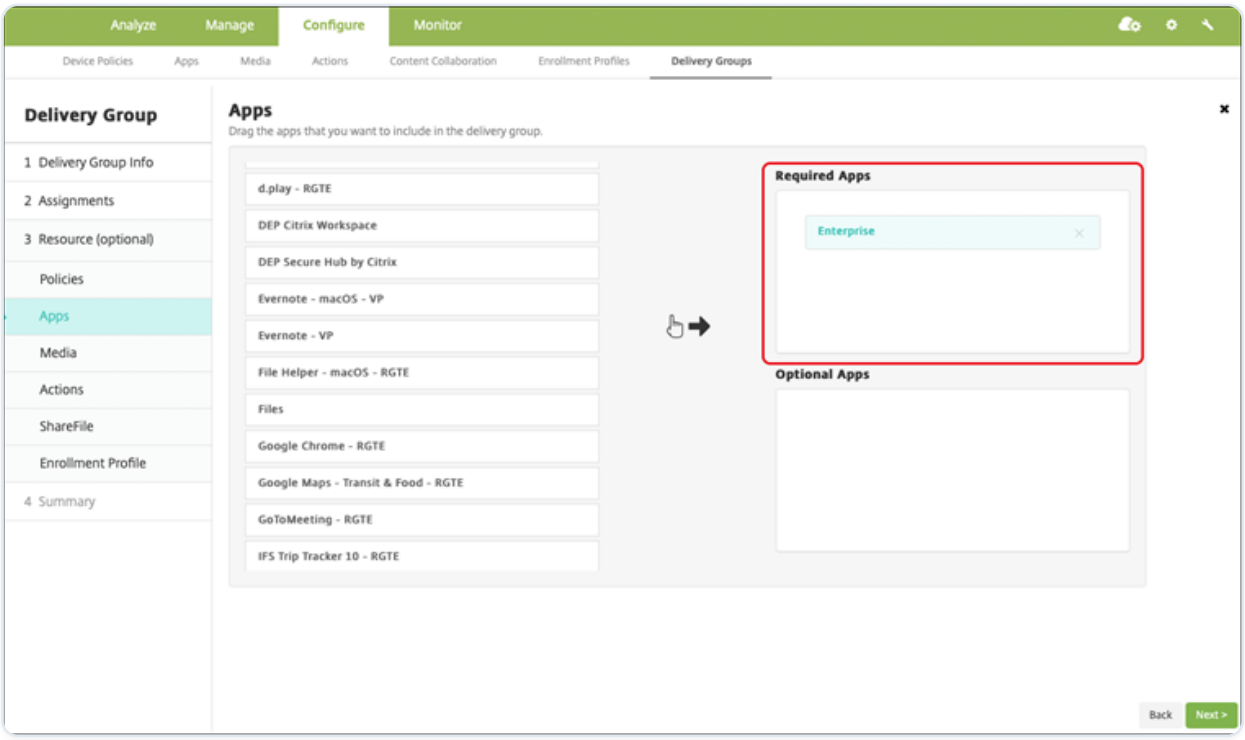
7. 各プラットフォームのアプリにデリバリーグループを割り当て、**保存**をクリックします。

この構成により、アプリリストにこのアプリの2つのエントリが表示されます。構成するアプリを選択するときは、**種類**が**MDX**のアプリを選択します。

ステップ 3: アプリの展開を構成する

1. XenMobile コンソールで、**Configure > Delivery Groups > Apps** に移動します。

2. 目的のボリューム購入アプリを**必須**としてマークします。



3. **構成 > 配信グループ**に移動します。
4. 配信グループを選択し、**展開**をクリックします。
5. ユーザーはアプリのインストール要求を受け取り、承諾すると、アプリはバックグラウンドでインストールされます。



カスタムアプリ

カスタムアプリは、独自の企業間アプリです。XenMobileとAppleボリューム購入を使用して、独自のアプリをプライベートかつ安全に配布できます。特定のパートナー、クライアント、フランチャイズ加盟店、および社内従業員にアプリを配布できます。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能OS	iOS/iPadOS

カスタムアプリの要件

- Apple Business ManagerまたはApple School Managerアカウント
- Appleボリューム購入アカウント（iOS 7以降のデバイスが必要）
- 以下のいずれかのApple登録モードを使用して、デバイスをXenMobileに登録します。
  - 自動デバイス登録
  - デバイス登録
  - ユーザー登録

ステップ1：アカウントのリンク

ボリューム購入を使用してカスタムアプリを展開するには、ボリューム購入アカウントをXenMobileにリンクします。

1. Apple Business Manager (ABM) を設定して登録します。これらのプログラムの詳細については、Appleのドキュメントを参照してください。
2. ABMアカウントをXenMobileにリンクします。ボリューム購入アカウントのリンクの詳細については、Appleボリューム購入を参照してください。
3. ボリューム購入アカウントを追加するときに、**App Auto Update** を有効にします。この設定により、Apple Storeでアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。

ステップ2：ABMでアプリを構成する

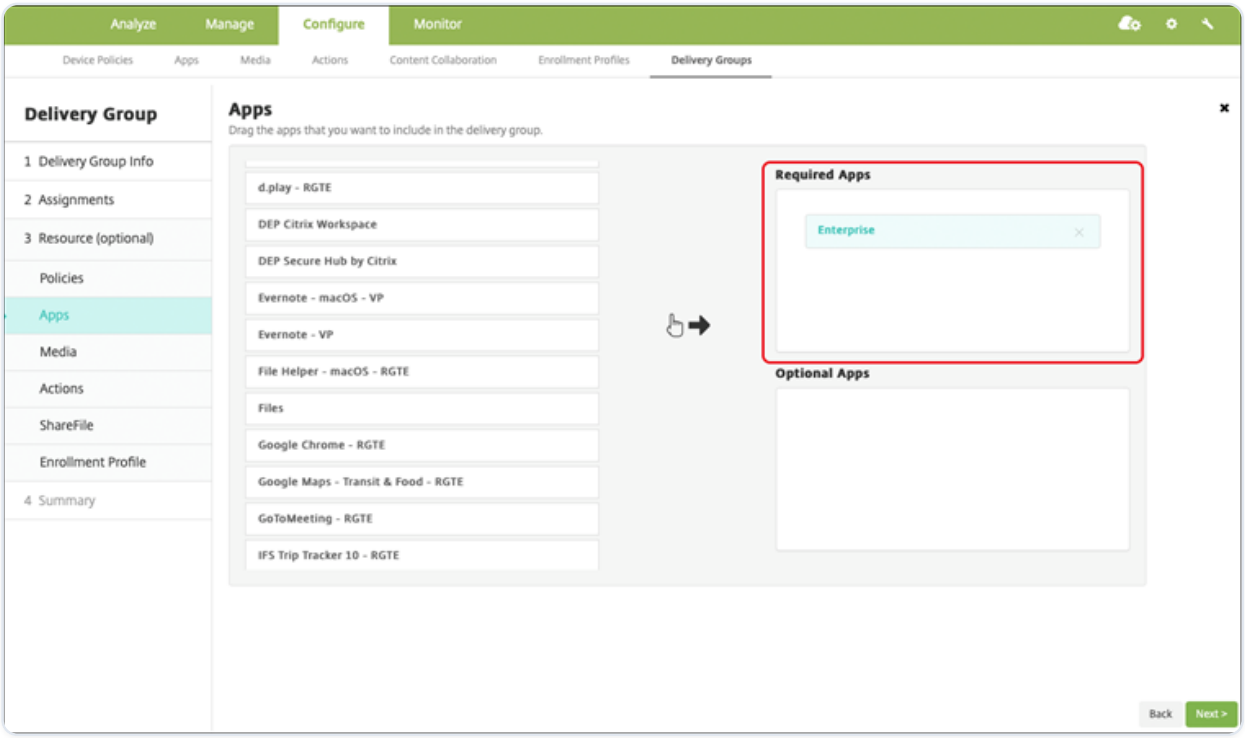
ABMアカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布したり、他の組織からカスタムアプリのライセンスを購入したりできます。ABMでのカスタムアプリの追加と有効化の詳細については、Appleのドキュメントを参照してください。

ステップ3：XenMobileでアプリを追加および構成する

1. XenMobileコンソールで、**Configure > Apps** に移動します。ボリューム購入アプリがアプリのリストに表示されます。
2. 構成するアプリを選択します。**Edit** をクリックします。
3. プラットフォームを選択します: **iPhone**、**iPad**、または **macOS**。
4. アプリを配布するデリバリーグループを選択します。**Save** をクリックします。

ステップ 4: アプリの展開を構成する

1. XenMobile コンソールで、**Configure > Delivery Groups > Apps** に移動します。
2. 配布するアプリを **Required** としてマークします。



3. **Configure > Delivery Groups** に戻ります。
4. 展開するデリバリーグループを選択し、**Deploy** をクリックします。

5. ユーザーはアプリを展開する要求を受け取ります。ユーザーが承認すると、アプリはバックグラウンドでインストールされます。



MDX対応のカスタムアプリ

MDXポリシーとセキュリティ機能を使用するには、MAM SDK対応またはMDXでラップされたカスタムアプリを追加します。

機能の可用性	
デバイスの監視が必要	いいえ
ユーザー登録モードで利用可能	はい
利用可能	iOS/iPadOS

ステップ1：アカウントのリンク

ボリューム購入を使用してカスタムアプリを展開するには、ボリューム購入アカウントをXenMobileにリンクします。

1. Apple Business Manager (ABM) を設定し、登録します。これらのプログラムの詳細については、Appleのドキュメントを参照してください。

2. ABMアカウントをXenMobileにリンクします。ボリューム購入アカウントのリンクの詳細については、(/ja-jp/xenmobile/server/apps/apple-volume-purchase.html)を参照してください。
3. ボリューム購入アカウントを追加する際に、**App Auto Update**を有効にします。この設定により、Apple Storeでアップデートが利用可能になったときに、ユーザーデバイス上のアプリが自動的に更新されるようになります。

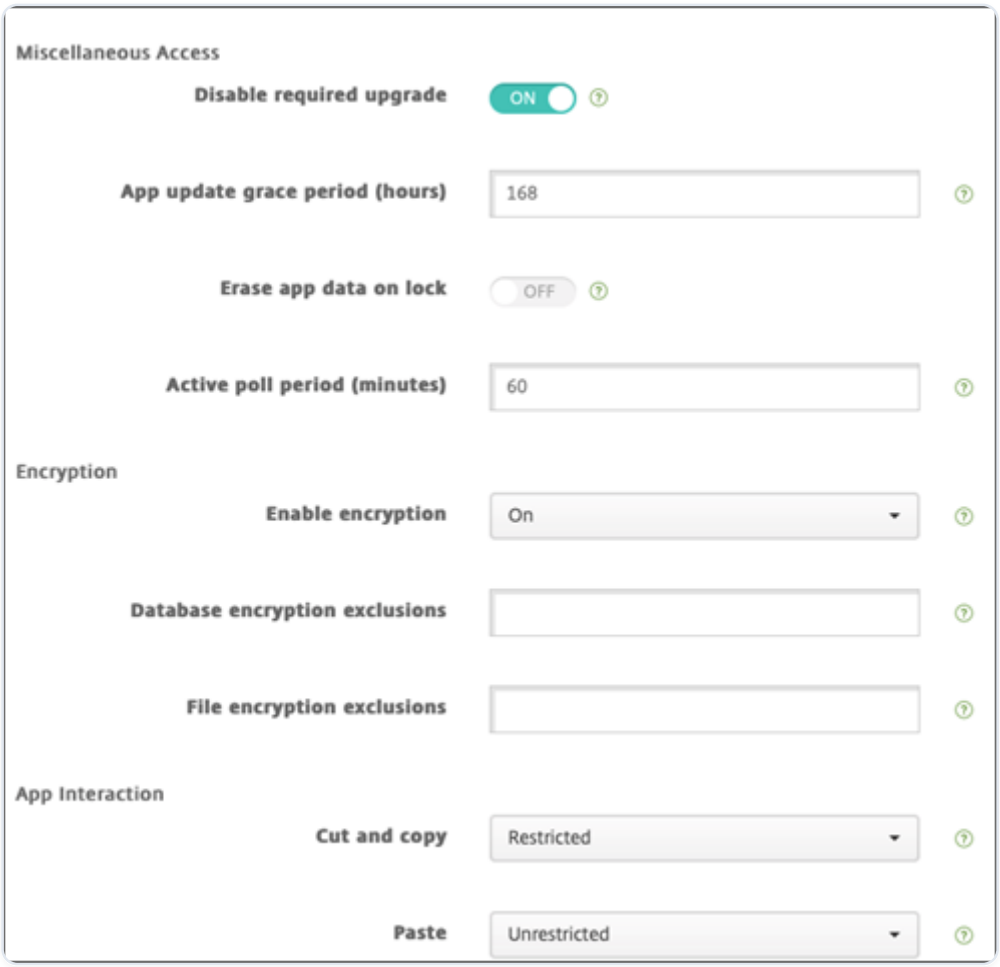
ステップ2：ABMでアプリを構成する

ABMアカウントにアプリを追加します。独自のカスタムアプリをアップロードして配布したり、他の組織からカスタムアプリのライセンスを購入したりできます。ABMでのカスタムアプリの追加と有効化の詳細については、Appleのドキュメントを参照してください。

ステップ3：XenMobileでアプリを追加および構成する

1. XenMobileコンソールで、**Configure > Apps**に移動します。**Add**をクリックします。
2. **MDX**をクリックします。 (/en-us/xenmobile/server/media/configure-apps-add.png)
3. **iPhone**または**iPad**プラットフォームを選択します。
4. 追加するアプリのMDXファイルをアップロードします。
5. アプリの詳細を構成します。**App deployed via Volume purchase**を**On**に設定します。Citrixは、**Force app to be managed**機能の有効化も推奨しています。 (/en-us/xenmobile/server/media/mdx-app-volume-purchase-on.png)

6. MDXポリシーを構成します。「**必須アップグレードを無効にする**」を「**オン**」に設定します。



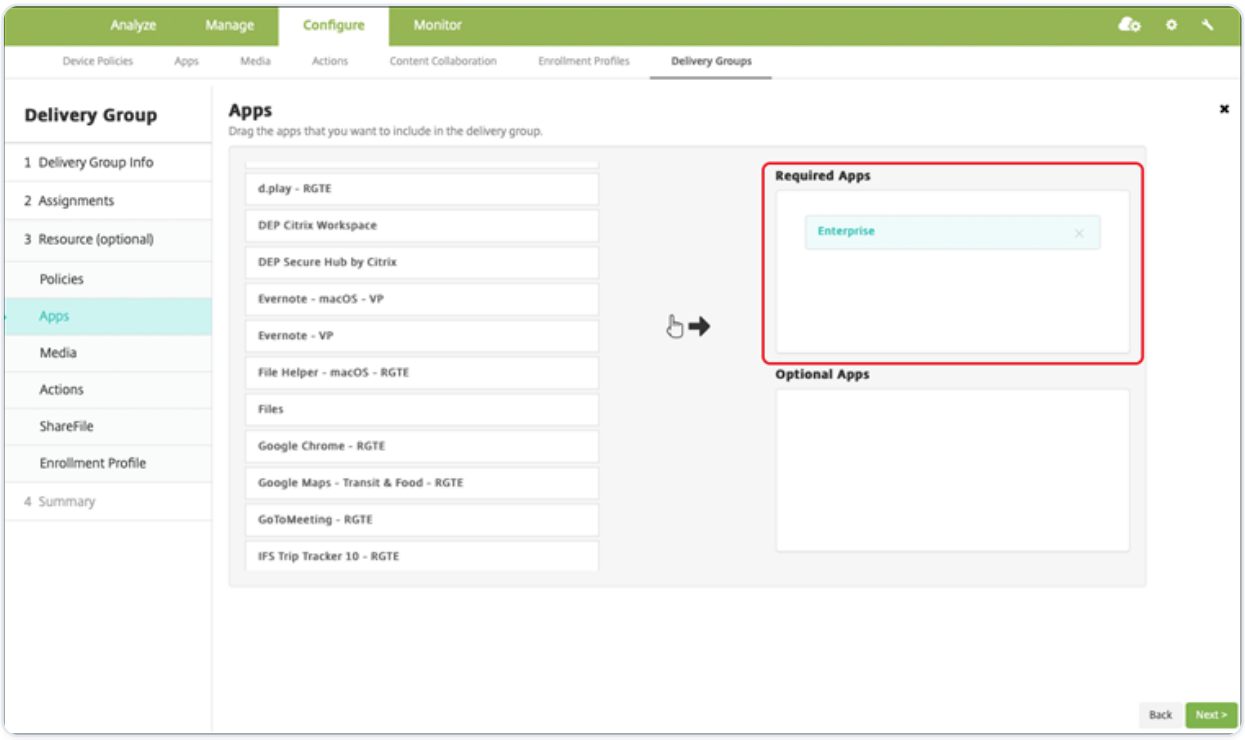
7. アプリにデリバリーグループを割り当て、「**保存**」をクリックします。

この構成により、アプリ一覧にこのアプリの2つのエントリが表示されます。構成するアプリを選択するときは、**種類**が**MDX**のアプリを選択してください。

ステップ4：アプリの展開を構成する

1. XenMobileコンソールで、**構成 > アプリ**に移動します。ボリューム購入アプリがアプリの一覧に表示されます。
2. 構成するアプリを選択します。「**編集**」をクリックします。
3. 各プラットフォームでアプリを配布するデリバリーグループを選択します。「**保存**」をクリックします。
4. **構成 > デリバリーグループ > アプリ**に戻ります。

5. 配布するアプリを「**必須**」としてマークします。



6. **構成 > デリバリーグループ**に戻ります。
7. 展開するデリバリーグループを選択し、「**展開**」をクリックします。
8. ユーザーはアプリを展開する要求を受け取ります。ユーザーが承諾すると、アプリはバックグラウンドでインストールされます。

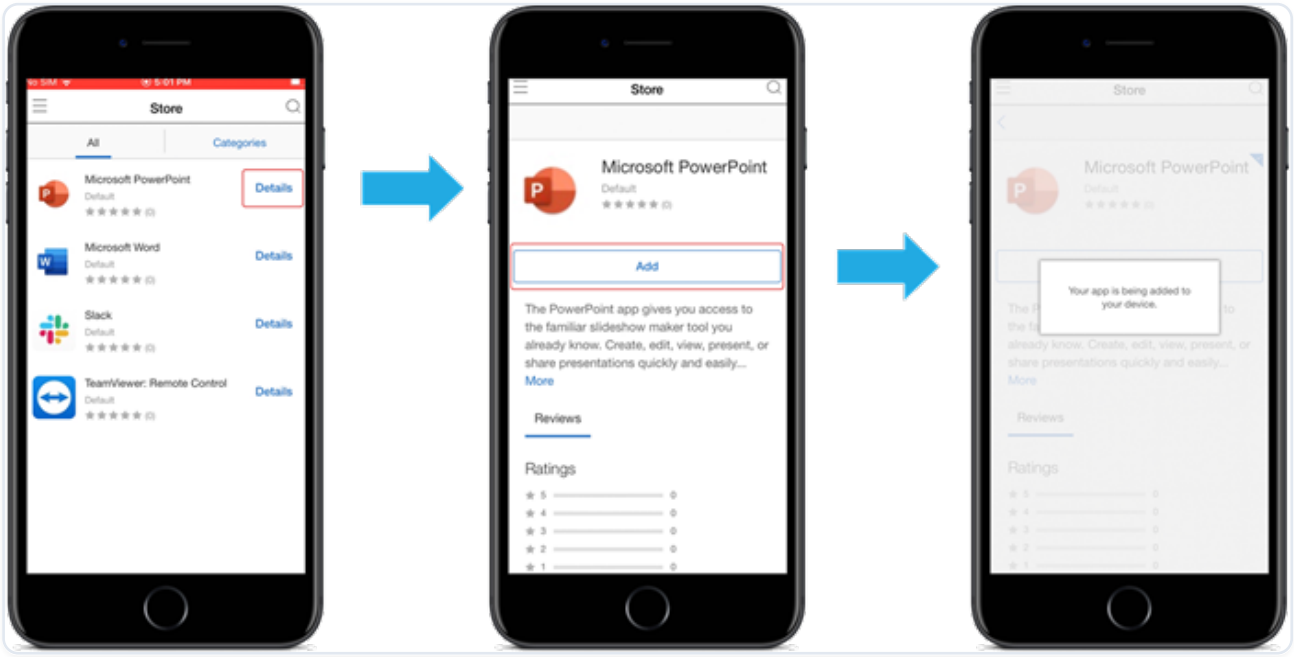


オプションアプリ (iOS/iPadOSのみ)

Citrixでは、アプリを**必須**として展開することをお勧めします。必須アプリはユーザーデバイスにサイレントインストールされ、操作を最小限に抑えます。この機能を有効にすると、アプリが自動的に更新されるようにもなります。

オプションアプリでは、ユーザーがインストールするアプリを選択できますが、ユーザーはSecure Hubを介して手動でインストールを開始する必要があります。

オプションアプリをインストールするには、ユーザーはSecure Hubを起動し、**ストア**に移動して、目的のアプリの**詳細**を選択し、**追加**をクリックする必要があります。



ネットワークアクセス制御

ネットワークアクセス制御 (NAC) ソリューションを使用して、Android および Apple デバイスの XenMobile® デバイスセキュリティ評価を拡張できます。NAC ソリューションは、XenMobile セキュリティ評価を使用して認証の決定を容易にし、処理します。NAC アプライアンスを構成すると、XenMobile で構成したデバイスポリシーと NAC フィルターが適用されます。

NAC ソリューションと XenMobile を使用すると、QoS と、ネットワーク内部のデバイスに対するよりきめ細かな制御が追加されます。NAC と XenMobile を統合する利点の概要については、「アクセス制御」を参照してください。

Citrix® は、XenMobile との統合のために以下のソリューションをサポートしています。

- シトリックス ゲートウェイ
- シスコ アイデンティティ サービス エンジン (ISE)

- ForeScout

Citrix は、他の NAC ソリューションとの統合を保証しません。

ネットワークに NAC アプライアンスがある場合:

- XenMobile は、iOS、Android Enterprise、および Android デバイスのエンドポイントセキュリティ機能として NAC をサポートしています。
- XenMobile でフィルターを有効にして、ルールまたはプロパティに基づいて、NAC のデバイスを準拠または非準拠として設定できます。例:
  - XenMobile の管理対象デバイスが指定された基準を満たさない場合、XenMobile はそのデバイスを非準拠としてマークします。NAC アプライアンスは、ネットワーク上の非準拠デバイスをブロックします。
  - XenMobile の管理対象デバイスに非準拠アプリがインストールされている場合、NAC フィルターが VPN 接続をブロックできます。その結果、非準拠のユーザーデバイスは VPN 経由でアプリや Web サイトにアクセスできません。
  - NAC に Citrix Gateway を使用している場合、スプリットトンネリングを有効にして、Citrix Gateway プラグインが不要なネットワークトラフィックを Citrix Gateway に送信するのを防ぐことができます。スプリットトンネリングの詳細については、「スプリットトンネリングの構成」を参照してください。

サポートされている NAC コンプライアンスフィルター

XenMobile Server は、次の NAC コンプライアンスフィルターをサポートしています。

匿名デバイス: デバイスが匿名モードであるかどうかを確認します。このチェックは、デバイスが再接続しようとしたときに XenMobile がユーザーを再認証できない場合に利用できます。

Samsung Knox アテステーションの失敗: デバイスが Samsung Knox アテステーションサーバーへのクエリに失敗したかどうかを確認します。

禁止アプリ: デバイスに、アプリアクセスデバイスポリシーで定義されている禁止アプリがあるかどうかを確認します。このポリシーの詳細については、「アプリアクセスデバイスポリシー」を参照してください。

非アクティブなデバイス: デバイスが、**サーバープロパティ**の**デバイス非アクティブ日数しきい値**設定で定義されているように非アクティブであるかどうかを確認します。詳細については、「サーバープロパティ」を参照してください。

必須アプリの欠落: デバイスに、アプリアクセスポリシーで定義されている必須アプリが欠落しているかどうかを確認します。

推奨されないアプリ: デバイスに、アプリアクセスポリシーで定義されている推奨されないアプリがあるかどうかを確認します。

非準拠パスワード: ユーザーパスワードが準拠しているかどうかを確認します。iOS および Android デバイスでは、XenMobile は、デバイス上の現在のパスワードがデバイスに送信されたパスコードポリシーに準拠しているかどうかを判断できます。たとえば、iOS では、XenMobile がパスコードポリシーをデバイスに送信した場合、ユーザーはパスワードを設定するために 60 分間与えられます。ユーザーがパスワードを設定する前は、パスコードが非準拠である可能性があります。

コンプライアンス違反デバイス: デバイスが、コンプライアンス違反デバイスプロパティに基づいてコンプライアンス違反であるかどうかを確認します。通常、自動化されたアクションまたは XenMobile API を使用するサードパーティが、そのデバイスプロパティを変更します。

失効ステータス: デバイス証明書が失効しているかどうかを確認します。失効したデバイスは、再度承認されるまで再登録できません。

Root化された Android および Jailbreakされた iOS デバイス: Android または iOS デバイスが Jailbreakされているかどうかを確認します。

管理対象外デバイス: デバイスが XenMobile の制御下で管理状態にあるかどうかを確認します。たとえば、MAM に登録されているデバイスや未登録のデバイスは管理対象外です。

> **注:**
>
> 暗黙的な準拠/非準拠フィルターは、XenMobile が管理しているデバイスにのみデフォルト値を設定します。たとえば、ブロックされたアプリ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ます。NAC アプライアンスは、これらのデバイスをネットワークからブロックします。

構成の概要

記載されている順序でNACコンポーネントを構成することをお勧めします。

1. NACをサポートするようにデバイスポリシーを構成します。

iOSデバイスの場合: NACをサポートするようにVPNデバイスポリシーを構成するを参照してください。

Android Enterpriseデバイスの場合: Citrix SSOのAndroid Enterprise管理対象構成を作成するを参照してください。

Androidデバイスの場合: Android向けCitrix SSOプロトコルを構成するを参照してください。

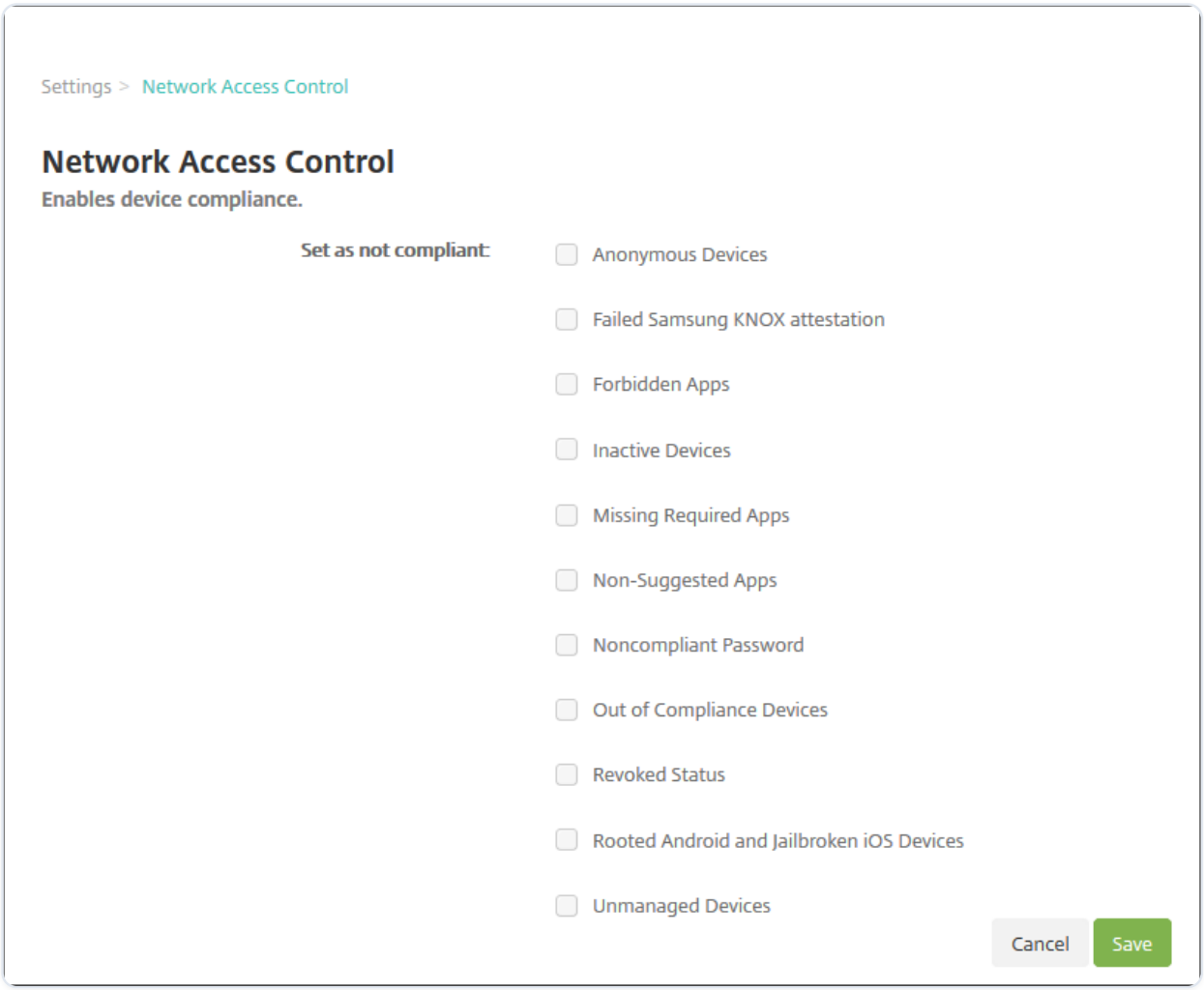
2. XenMobileでNACフィルターを有効にする。
3. NACソリューションを構成します。

   - Citrix Gateway、詳細はNACをサポートするようにCitrix Gatewayポリシーを更新するを参照してください。

     デバイスにCitrix SSOをインストールする必要があります。Citrix Gatewayクライアントを参照してください。
   - Cisco ISE: Ciscoドキュメントを参照してください。
   - ForeScout: ForeScoutドキュメントを参照してください。

XenMobileでNACフィルターを有効にする

1. XenMobileコンソールで、**「設定」>「ネットワークアクセスコントロール」**に移動します。



2. 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。
3. 「**保存**」をクリックします。

NACをサポートするようにCitrix Gatewayポリシーを更新する

VPN仮想サーバーで、高度な（従来のポリシーではない）認証およびVPNセッションポリシーを構成する必要があります。

これらの手順は、次のいずれかの特性を持つCitrix Gatewayを更新します。

- XenMobile Server環境と統合されている。
- または、VPN用に設定されており、XenMobile Server環境の一部ではないが、XenMobileに到達できる。

仮想VPNサーバーで、コンソールウィンドウから次の操作を行います。コマンドと例のIPアドレスは架空のものです。

1. VPN仮想サーバーで従来のポリシーを使用している場合は、すべての従来のポリシーを削除してバインドを解除します。確認するには、次のように入力します。

`show vpn vserver <VPN_VServer>`

Classicという単語を含む結果を削除します。例: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

ポリシーを削除するには、次のように入力します。

`unbind vpn vserver <VPN_VServer> -policy <policy_name>`

2. 対応する高度なセッションポリシーを作成するには、次のように入力します。

   `add vpn sessionPolicy <policy_name> <rule> <session action>`

   例: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. ポリシーをVPN仮想サーバーにバインドするには、次のように入力します。

   `bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100`

4. 認証仮想サーバーを作成するには、次のように入力します。

   `add authentication vserver <authentication vserver name> <service type> <ip address>`

   例: `add authentication vserver authvs SSL 0.0.0.0` この例では、`0.0.0.0` は認証仮想サーバーが公開されていないことを意味します。

5. 仮想サーバーにSSL証明書をバインドするには、次のように入力します。

   `bind ssl vserver <authentication vserver name> -certkeyName <Webserver certificate>`

   例: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. VPN仮想サーバーから認証仮想サーバーに認証プロファイルを関連付けます。まず、次のように入力して認証プロファイルを作成します。

   `add authentication authnProfile <profile name> -authnVsName <authentication vserver name>`

   例:

   `add authentication authnProfile xm_nac_prof -authnVsName authvs`

7. 認証プロファイルをVPN仮想サーバーに関連付けるには、次のように入力します。

   `set vpn vserver <vpn vserver name> -authnProfile <authn profile name>`

例:

```
set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
```

8. Citrix Gatewayからデバイスへの接続を、次のように入力して確認します。

   ```
   curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
   ```

   たとえば、このクエリは、環境に登録されている最初のデバイス (`deviceid_1`) のコンプライアンスステータスを取得することで、接続性を検証します。

   ```
   curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
   ```

   成功した結果は、次の例のようになります。

   ```
   HTTP/1.1 200 OK

   < Server: Apache-Coyote/1.1

   < X-Citrix-Device-State: Non Compliant

   < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
   ```

9. 前のステップが成功したら、XenMobileへのWeb認証アクションを作成します。まず、iOS VPNプラグインからデバイスIDを抽出するポリシー式を作成します。次のように入力します。

   ```
   add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\'=\', \'&\').VALUE(\"deviceidvalue\")"
   ```

10. 次のように入力して、XenMobileにリクエストを送信します。この例では、XenMobile ServerのIPは `10.207.87.82` で、FQDNは `example.em.server.com:4443` です。

    ```
    add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{"GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host: example.em.server.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " + xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\"200\") &&HTTP.RES.HEADER(\"X-Citrix-Device-State\").EQ(\"Compliant\")"
    ```

XenMobile NACの成功した出力は`HTTP status 200 OK`です。`X-Citrix-Device-State`ヘッダーの値は`Compliant`である必要があります。

11. 次のように入力して、アクションを関連付ける認証ポリシーを作成します。

    `add authentication Policy <policy name> -rule <rule> -action <web authentication action>`

    例: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NAC\")" -action xm_nac`

12. 既存のLDAPポリシーを次のように入力して、高度なポリシーに変換します。

    `add authentication Policy <policy_name> -rule <rule> -action <LDAP action name>`

    例: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. 以下を入力して、LDAPポリシーを関連付けるポリシーラベルを追加します。

    `add authentication policylabel <policy_label_name>`

    例: `add authentication policylabel ldap_pol_label`

14. 以下を入力して、LDAPポリシーをポリシーラベルに関連付けます。

    `bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol -priority 100 -gotoPriorityExpression NEXT`

15. 準拠デバイスを接続してNACテストを実行し、LDAP認証が成功したことを確認します。以下を入力します。

    `bind authentication vserver <authentication vserver> -policy <web authentication policy> -priority 100 -nextFactor <ldap policy label> -gotoPriorityExpression END`

16. 認証仮想サーバーに関連付けるUIを追加します。デバイスIDを取得するには、以下のコマンドを入力します。

    `add authentication loginSchemaPolicy <schema policy>-rule <rule> -action lschema_single_factor_deviceid`

17. 以下を入力して、認証仮想サーバーをバインドします。

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority 100
-gotoPriorityExpression END
```

18. LDAP高度認証ポリシーを作成してSecure Hub接続を有効にします。以下を入力します。

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\"User-
Agent\").CONTAINS(\"NAC\").NOT" -action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority 110
-gotoPriorityExpression NEXT
```

サムスン Knox

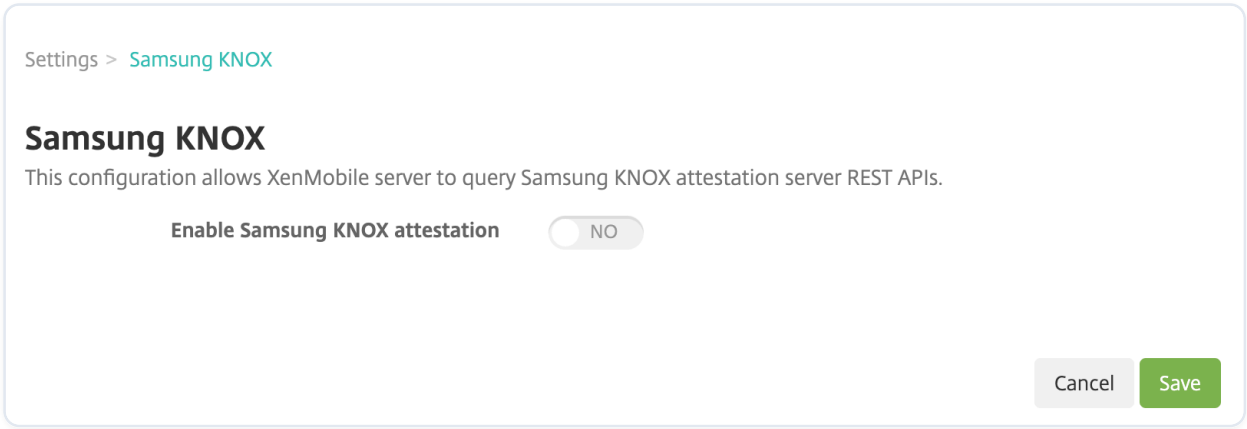
Samsung は、XenMobile® Server と互換性のあるいくつかのソリューションを提供しています。

- XenMobile は、互換性のある Samsung デバイスで Samsung Knox ポリシーをサポートし、拡張します。
- Knox Service プラグイン (KSP) は、Knox Platform for Enterprise (KPE) 機能のサブセットをサポートするアプリです。KPE に関する Samsung からの情報については、「Configure Knox Platform for Enterprise」および「Overview」を参照してください。

XenMobile を構成して、Samsung Knox アテステーションサーバーの REST API を照会できます。

Samsung Knox は、オペレーティングシステムとアプリケーションに複数のレベルの保護を提供するハードウェアセキュリティ機能を使用します。このセキュリティの 1 つのレベルは、アテステーションを介したプラットフォームにあります。アテステーションサーバーは、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、信頼できるブート中に収集された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、右上隅の歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. 「**プラットフォーム**」の下で、「**Samsung KNOX**」をクリックします。「**Samsung KNOX**」ページが表示されます。



3. 「**Samsung KNOX アテステーションを有効にする**」で、Samsung Knox アテステー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「**いいえ**」です。
4. 「**保存**」をクリックします。

> **注:**
>
> Samsung Knox Mobile Enrollment を使用すると、各デバイスを手動で構成することなく、複数の Samsung Knox デバイスを XenMobile (または任意のモバイルデバイスマネージャー) に登録できます。詳細については、「Samsung Knox の一括登録」を参照してください。

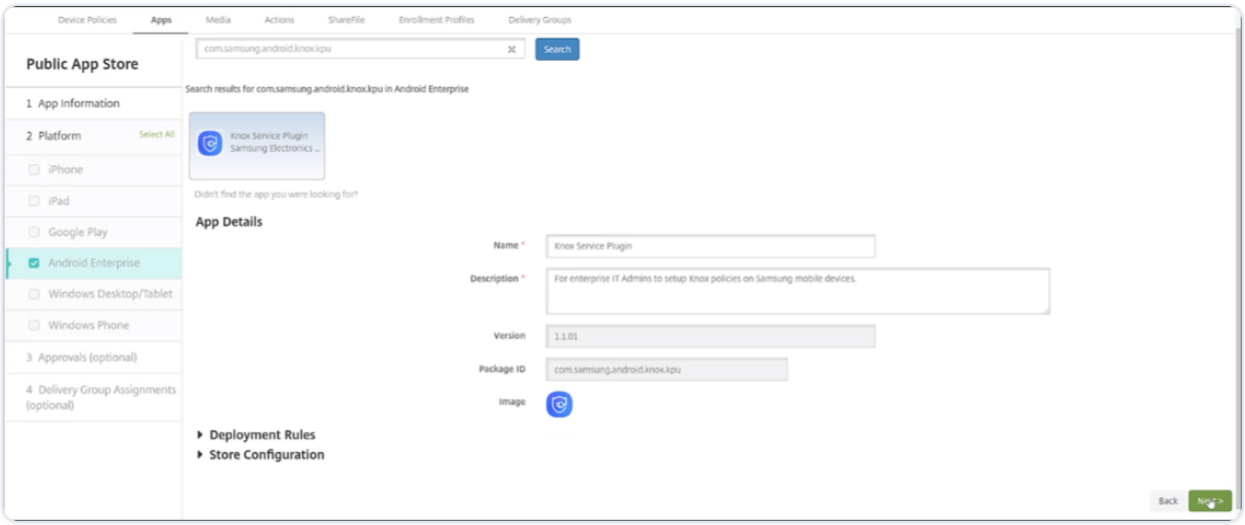
Knox サービスプラグインアプリを追加する

Knox で Android Enterprise を使用する予定がある場合は、Knox サービスプラグイン (KSP) を XenMobile に追加します。KSP アプリは AndroidOEMConfig を使用して、セキュリティポリシー、柔軟な VPN 構成、生体認証制御などの機能をサポートします。AndroidOEMConfig は、OEM とエンドポイントモビリティマネージャー (EMM) がカスタム OEM API をサポートできるようにします。これらの API は、Android Enterprise ではサポートされていないユースケースをカバーします。

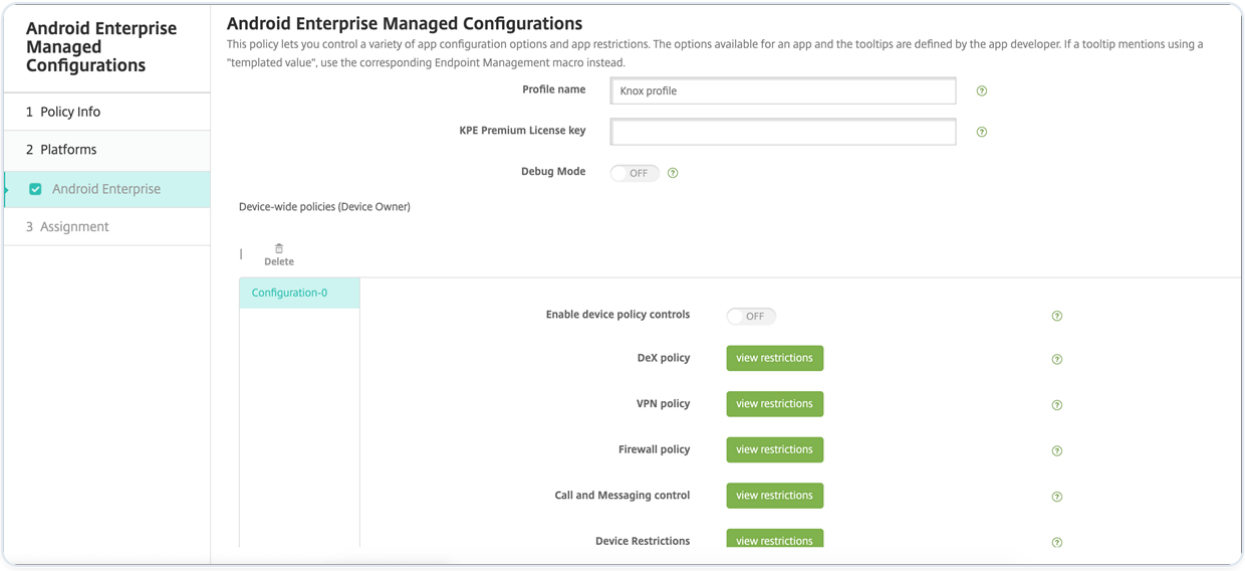
KSPの詳細については、Knox Service Plugin Guideを参照してください。

1. Googleアカウントにサインインし、`https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu`に移動します。Knox Service Plug-inアプリを承認します。
2. XenMobileコンソールにサインインし、Knoxサービスプラグインをパブリックアプリストアアプリとして追加します。パブリックアプリストアアプリの追加の詳細については、パブリック

アプリストアアプリの追加を参照してください。

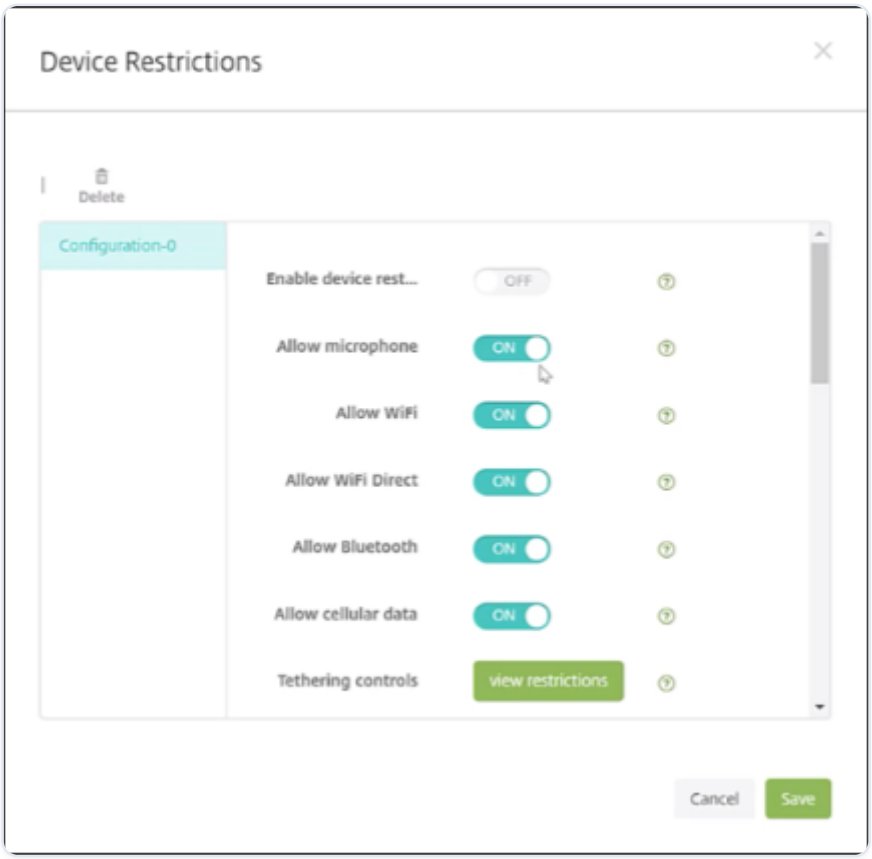


3. XenMobileコンソールで、**構成 > デバイスポリシー**に移動します。**追加**をクリックします。
4. **管理対象構成**をクリックします。表示されるダイアログで、メニューから**Knox Service Plugin**を選択します。管理対象構成ポリシーの詳細については、管理対象構成ポリシーを参照してください。
5. ポリシーの名前を入力し、プラットフォームページに進みます。



6. プラットフォームページで、Knoxプロファイルの**プロファイル名**を入力し、Samsungから提供された**KPE Premium License key**を入力します。これらのフィールドの下に表示されるポリシーは、Knox展開から取得されます。Knoxポリシーの詳細については、このセクションで

前述したKnox Service Admin Plug-in Guideを参照してください。



7. **次へ**をクリックし、ポリシーの展開ルールを構成します。
8. **保存**をクリックします。

Samsung Knoxの一括登録

複数のSamsung KnoxデバイスをXenMobile®（または任意のモバイルデバイスマネージャー）に、各デバイスを手動で設定することなく登録するには、Knox Mobile Enrollmentを使用します。登録は初回使用時または工場出荷時設定へのリセット後に実行されます。管理者はユーザー名とパスワードをデバイスに直接渡すこともできるため、ユーザーは登録時に情報を入力する必要がありません。

> **注：**
>
> Knox Mobile Enrollmentのセットアップは、XenMobile Knoxコンテナとは関係ありません。Knox Mobile Enrollmentの詳細については、Knox Mobile Enrollment管理者ガイドを参照してください。

Knox Mobile Enrollmentの前提条件

- XenMobileが構成され（ライセンスと証明書を含む）、実行されていること。
- Secure Hub APKファイル。Knox Mobile Enrollmentを設定する際にファイルをアップロードします。
- KMEの要件のリストについては、Knox Mobile Enrollmentの概要を参照してください。
- デバイスポリシーを適用するために必要なSamsung Knox Platform for Enterprise (PKE) ライセンス。XenMobileデバイスポリシーのKnox Platform for Enterpriseでライセンスキーを提供します。

Secure Hub APKファイルをダウンロードするには

Google Playストアにアクセスして、Android用Citrix Secure Hub™ファイルをダウンロードします。

ファイアウォール例外を構成する

Knox Mobile Enrollmentにアクセスするには、以下のファイアウォール例外を構成します。これらのファイアウォール例外の一部はすべてのデバイスに必要であり、一部はデバイスの地理的地域に固有のものです。

デバイスの地域	URL	ポート	宛先
すべて	`https://gslb.secb2b.com`	443	Knox Mobile Enrollment の開始用グローバルロードバランサー
すべて	`https://gslb.secb2b.com`	80	一部の限定されたレガシーデバイスでの Knox Mobile Enrollment 開始用グローバルロードバランサー
すべて	`umc-cdn.secb2b.com`	443	Samsung エージェント更新サーバー
すべて	`bulkenrollment.s3.amazonaws.com`	80	Knox Mobile Enrollment 顧客向け使用許諾契約

XENMOBILE®サーバー

デバイスの地域	URL	ポート	宛先
すべて	`eula.secb2b.com`	443	Knox Mobile Enrollment 顧客向け使用許諾契約
すべて	`us-be-api-mssl.samsungknox.com`	443	IMEI検証用Samsungサーバー
米国	`https://us-segd-api.secb2b.com`	443	米国地域向けSamsung Enterprise Gateway
ヨーロッパ	`https://eu-segd-api.secb2b.com`	443	ヨーロッパ地域向けSamsung Enterprise Gateway
中国	`https://china-segd-api.secb2b.com`	443	中国地域向けSamsung Enterprise Gateway

注：

Knox Mobile Enrollment 管理ガイドで、ファイアウォール例外の完全なリストを確認できます。

Knox Mobile Enrollment へのアクセス

Samsung のドキュメントに従って、KME の使用を開始するで Knox Mobile Enrollment にアクセスしてください。

ノックス モバイル エンロールメント の設定

Knox Mobile Enrollment にアクセスしたら、Knox ポータルにログインします。

登録プロセスは、次の一般的な手順に従います。

1. MDMコンソール情報と設定を使用してMDMプロファイルを作成します。

   MDMプロファイルは、デバイスがMDMに接続する方法を示します。

2. デバイスをMDMプロファイルに追加します。

   デバイス情報を含むCSVファイルをアップロードするか、Google PlayからKnox展開アプリをインストールして使用できます。

3. デバイスの所有権が確認されると、Samsungから通知されます。
4. ユーザーにMDM資格情報を提供します。Wi-Fiを使用してインターネットに接続し、デバイスを登録するためのプロンプトを受け入れるように指示します。

MDMプロファイルを作成するには

プロファイル構成に関するSamsungドキュメントに記載されている手順に従ってください。

以下のフィールドまたは手順が表示されたら、記載されているとおりに構成してください。

- **MDMを選択:** メニューから**Citrix®**を選択します。デバイス所有者プロファイルのみ。
- **MDMエージェントAPK:** デバイス所有者プロファイルのみ。Secure Hub APKダウンロードURLを入力します: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`。

  APKファイルは、登録中にデバイスがアクセスできる任意のサーバーに置くことができます。登録中、デバイスは次のことを行います。

  - APKダウンロードURLからSecure Hubをダウンロードします
  - Secure Hubをインストールします
  - その後、次に説明するカスタムJSONデータでSecure Hubを開きます。

  .apk ファイル名の大文字/小文字は、入力する URL と一致している必要があります。たとえば、ファイル名がすべて小文字の場合、URL 内でもすべて小文字である必要があります。

- **MDMサーバーURI:** MDMサーバーURIは指定しないでください。XenMobileはSamsung MDMプロトコルを使用しません。
- **カスタムJSONデータ:** Secure Hubは、登録のためにXenMobile Serverのアドレスとユーザー名、パスワードを必要とします。Secure Hubがユーザーにそれらを要求しないように、そのデータをJSONで提供できます。Secure Hubは、JSONからフィールドが省略されている場合にのみ、サーバーアドレス、ユーザー名、またはパスワードをユーザーに要求します。

  カスタムJSONデータの形式は次のとおりです。

  ```
  {"serverURL": "URL", "xm_username":"Username", "xm_password":"Password"}
  ```

この例は一括登録に典型的なもので、Secure Hubは登録中にサーバーアドレスや資格情報をユーザーに要求しません。

`{"serverURL":"https://example.com/zdm", "xm_username":"userN", "xm_password":"password1234"}` `{"serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2", "xm_password":"password7890"}`

この例はキオスクベースのデバイスに典型的なもので、Secure Hubはユーザーに資格情報を要求します。

`{"serverURL":"https://example.com/zdm"}`

Android Enterpriseのゼロタッチ登録用にカスタムJSONを入力することもできます。

```
{

    "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

    {


"serverURL":"URL","xm_username":"username","xm_password":"password"

    }

}
```

デバイスが登録を開始すると、指定されたURLからSecure Hubをダウンロードし、Secure Hubをインストールして開きます。

追加の構成

構成の詳細については、以下のSamsungドキュメントページを参照してください。

- デバイス構成: デバイスを一括で追加します。
- Samsung Knox Deployment App: Bluetooth、NFC、またはWi-Fi Direct登録を介してデバイスを登録します。
- Knox Mobile Enrollment: Samsung Knoxの詳細については、Samsungのドキュメントを参照してください。

Knox APIバージョン2.4より前のデバイスを登録するには

Knox APIバージョン2.4より前のデバイスでは、初期デバイスセットアップ中に一括登録は開始されません。代わりに、ユーザーが登録を開始する必要があります。そのためには、ユーザーはSamsungのサイトにアクセスして新しいモバイル登録クライアントをダウンロードし、登録を開始します。

ダウンロードされた登録クライアントは、Knox 2.4/2.4.1デバイス向けにKnox一括登録ポータルで構成されたものと同じMDMプロファイルとAPKを使用します。

ユーザーは通常、次の手順に従います。

1. デバイスの電源を入れ、Wi-Fiに接続します。モバイル登録が開始されない場合、またはWi-Fiが利用できない場合は、次の操作を行います。
    a. Samsung Knox Mobile Enrollmentにアクセスします。
    b. **次へ**ボタンをタップして、モバイルデータでデバイスを登録します。
2. **Knoxで登録**のプロンプトが表示されたら、**続行**をタップします。
3. EULA（利用可能な場合）を読みます。**次へ**をタップします。
4. プロンプトが表示されたら、IT管理者が提供した**ユーザーID**と**パスワード**を入力します。

この時点で、ユーザー資格情報が検証され、デバイスが組織のエンタープライズIT環境に登録されます。

Samsungデバイスの生体認証を有効/無効にする

XenMobileは、生体認証とも呼ばれる指紋認証と虹彩スキャン認証をサポートしています。ユーザーからの操作を必要とせずに、Samsungデバイスの生体認証を有効または無効にできます。XenMobileで生体認証を無効にすると、ユーザーおよびサードパーティ製アプリはその機能を有効にできません。

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**ページが表示されます。
2. 「**追加**」をクリックします。「**新しいポリシーの追加**」ページが表示されます。
3. 「**パスコード**」をクリックします。「**パスコードポリシー情報**」ページが表示されます。
4. 「**ポリシー情報**」ペインで、次の情報を入力します。
    - **ポリシー名:** ポリシーのわかりやすい名前を入力します。
    - **説明:** 必要に応じて、ポリシーの説明を入力します。

5. 「**次へ**」をクリックします。「**プラットフォーム**」ページが表示されます。
6. 「**プラットフォーム**」で、「**Android**」または「**Samsung Knox**」を選択します。
7. 「**生体認証の構成**」を「**ON**」に設定します。
8. 「**Android**」を選択した場合は、「**Samsung SAFE**」で「**指紋を許可**」、「**虹彩を許可**」、またはその両方を選択します。

   「生体認証の構成」オプション (/en-us/xenmobile/server/media/samsung-knox-biometric-auth.png)

セキュリティアクション

デバイスとアプリのセキュリティアクションは、 > ページから実行します。デバイスアクションには、取り消し、ロック、ロック解除、ワイプが含まれます。アプリのセキュリティアクションには、アプリのロックと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:** デバイスのアクティベーション前に、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、ユーザーの個人のApple IDやパスワードは必要ありません。
- **アプリのロック:** デバイス上のすべてのアプリへのアクセスを拒否します。Androidでは、アプリのロック後、ユーザーはXenMobileにサインインできません。iOSでは、ユーザーはサインインできますが、どのアプリにもアクセスできません。
- **アプリのワイプ:** Secure Hubからユーザーアカウントを削除し、デバイスの登録を解除します。**アプリのワイプ解除**アクションを実行するまで、ユーザーは再登録できません。
- **ASM展開プログラムの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。
- **制限のクリア:** 監視対象のiOSデバイスでは、このコマンドによりXenMobileは、ユーザーが構成した制限パスワードと制限設定をクリアできます。
- **紛失モードの有効化/無効化:** 監視対象のiOSデバイスを紛失モードにし、デバイスに表示するメッセージ、電話番号、および脚注を送信します。このコマンドを2回目に送信すると、デバイスは紛失モードを解除されます。
- **追跡の有効化:** AndroidまたはiOSデバイスでは、このコマンドによりXenMobileは、指定した頻度で特定のデバイスの位置をポーリングできます。デバイスの座標と地図上の位置を表示するには、 **>** に移動し、デバイスを選択して、 をクリックします。デバイス情報は、 の下の タブにあります。デバイスを継続的に追跡するには、 を使用します。Secure Hubは、デバイスの実行中に定期的に位置を報告します。

- **完全ワイプ:** メモリカードを含む、デバイス上のすべてのデータとアプリを即座に消去します。
    - Androidデバイスの場合、この要求にはメモリカードをワイプするオプションも含まれます。
    - 仕事用プロファイルを持つAndroid Enterpriseの完全管理デバイス（COPEデバイス）の場合、選択的ワイプで仕事用プロファイルを削除した後、完全ワイプを実行できます。
    - iOSおよびmacOSデバイスの場合、デバイスがロックされていても、ワイプは即座に実行されます。
        - iOS 11デバイス（最小バージョン）の場合: 完全ワイプを確定する際に、デバイス上のモバイルデータプランを保持するかどうかを選択できます。
        - iOS 11.3デバイス（最小バージョン）の場合: 完全ワイプを確定する際に、iOSデバイスが近接設定を行うのを防ぐことができます。新しいiOSデバイスを設定する際、ユーザーは通常、すでに構成済みのiOSデバイスを使用して自分のデバイスを設定できます。XenMobile Serverで管理され、ワイプされたデバイスでは、近接設定をブロックできます。
        - iOS 17デバイス（最小バージョン）の場合: 完全ワイプを確定すると、デバイスはすべてのユーザーデータを自動的にワイプし、指定されたWi-Fiネットワークに接続し、提供された登録プロファイルを使用してMDMサーバーに再登録されます。
    - メモリカードのコンテンツが削除される前にデバイスユーザーがデバイスの電源を切った場合、ユーザーはデバイスデータにアクセスできる可能性があります。
    - ワイプリクエストは、リクエストがデバイスに送信されるまでキャンセルできます。
- **位置特定:** デバイスを特定し、マップを含め、**管理 > デバイス**ページの**デバイスの詳細 > 一般**の下にデバイスの位置を報告します。位置特定は1回限りのアクションです。アクションを実行した時点での現在のデバイスの位置を表示するには、**位置特定**を使用します。一定期間デバイスを継続的に追跡するには、**追跡を有効にする**を使用します。
    - このアクションをAndroid (Android Enterpriseを除く) デバイス、またはAndroid Enterprise (企業所有またはBYOD) デバイスに適用する場合、以下の動作に注意してください。
        - **位置特定**では、登録中にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録中に権限を付与しない場合、XenMobileは**位置特定**コマンドを送信する際に再度位置情報権限を要求します。

    - この機能をiOSまたはAndroid Enterpriseデバイスに適用する場合、以下の制限に注意してください。

        - Android Enterpriseデバイスの場合、位置情報デバイスポリシーがデバイスの位置情報モードを**高精度**または**バッテリー節約**に設定していない限り、このリクエストは失敗します。
        - iOSデバイスの場合、このコマンドは、デバイスがMDM紛失モードの場合にのみ成功します。

- **ロック:** デバイスをリモートでロックします。このアクションは、デバイスを紛失し、盗難されたかどうかわからない場合に役立ちます。XenMobileはPINコードを生成し、デバイスに設定します。デバイスにアクセスするには、ユーザーは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、**ロック解除**を使用します。
- **ロックしてパスワードをリセット:** デバイスをリモートでロックし、パスコードをリセットします。

    - Android 8.0より前のAndroidバージョンを実行している、ワーク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以降を実行している、ワーク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はワークプロファイルをロックします。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要件を満たさない場合、およびワークプロファイルにパスコードがすでに設定されていない場合: 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要件を満たさないが、ワークプロファイルにパスコードが既に設定されている場合: ワーク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 (着信音):** Android デバイスでサウンドを再生します。
- **再起動:** Windows 10 および Windows 11 デバイスを再起動します。Windows タブレットおよび PC の場合、「システムはまもなく再起動します」というメッセージが表示され、5 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:** デバイスが接続することを禁止します。
- **取り消し/承認 (iOS、macOS):** 選択的ワイプと同じアクションを実行します。取り消し後、デバイスを再承認して再登録できます。
- **着信音:** デバイスが紛失モードの場合、監視対象の iOS デバイスで着信音が鳴ります。この音は、デバイスを紛失モードから解除するか、ユーザーが音を無効にするまで鳴り続けます。
- **選択的ワイプ:** デバイスからすべての企業データとアプリを消去し、個人データとアプリはそのまま残します。選択的ワイプ後、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、デバイスが Device Manager および企業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 にアクセスできないようにするには、デバイス証明書も取り消す必要があります。
    - Android デバイスを選択的にワイプすると、そのデバイスも取り消されます。デバイスを再承認するか、コンソールから削除した後にのみ、デバイスを再登録できます。
    - ワークプロファイルを持つ Android Enterprise の完全管理デバイス (COPE デバイス) の場合、選択的ワイプでワークプロファイルを削除した後、完全ワイプを実行できます。または、同じユーザー名でデバイスを再登録することもできます。デバイスを再登録すると、ワークプロファイルが再作成されます。
    - Samsung Knox API が有効になっている場合、デバイスを選択的にワイプすると、Samsung Knox コンテナも削除されます。
    - iOS および macOS デバイスの場合、このコマンドは MDM を介してインストールされたすべてのプロファイルを削除します。
    - Windows デバイスでの選択的ワイプは、現在サインオンしているユーザーのプロファイルフォルダーの内容も削除します。選択的ワイプでは、構成を通じてユーザーに配信する 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、ユーザーが手動でデバイスの登録を解除する必要があります。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。
- **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。このコマンドではデバイスのロックは解除されません。

「**管理 > デバイス**」で、**デバイスの詳細**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、強力な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タイプに関するその他の情報が含まれます。**デバイスの完全ワイプ**フィールドにはユーザーPINコードが含まれています。ユーザーはデバイスがワイプされた後にそ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、ここで調べることができます。

Androidデバイスのセキュリティアクション

セキュリティアクション	ANDROID (ANDROID ENTERPRISEデバイスを除く)	アンドロイド エンタープライズ (BYOD)	ANDROID ENTERPRISE (企業所有)
アプリロック	はい	いいえ	いいえ
アプリワイプ	はい	いいえ	いいえ
完全ワイプ	はい	いいえ	はい
検索	はい: Android 6.0以降を実行しているデバイスの場合、検索には、登録中にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録中に権限を付与しない場合、XenMobileは検索コマンドの送信時に再度位置情報権限を要求します。	はい: Android 6.0以降を実行しているデバイスの場合、検索には、登録中にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録中に権限を付与しない場合、XenMobileは検索コマンドの送信時に再度位置情報権限を要求します。	はい: Android 6.0以降を実行しているデバイスの場合、検索には、登録中にユーザーが位置情報権限を付与する必要があります。ユーザーは位置情報権限を付与しないことを選択できます。ユーザーが登録中に権限を付与しない場合、XenMobileは検索コマンドの送信時に再度位置情報権限を要求します。
ロック	はい	はい	はい
ロックしてパスワードをリセット	はい	いいえ	はい
通知 (着信音)	はい	はい	はい
取り消し	はい	はい	はい
選択的ワイプ	はい	はい	いいえ

iOSおよびmacOSデバイスのセキュリティアクション

セキュリティアクション	IOS	MACOS
アクティベーションロックバイパス	はい	いいえ
アプリロック	はい	いいえ
アプリワイプ	はい	いいえ
ASM展開プログラムのアクティベーションロック	はい	いいえ
制限をクリア	はい	いいえ
紛失モードの有効化/無効化	はい	いいえ
追跡の有効化/無効化	はい	いいえ
完全ワイプ	はい	はい
検索	はい	いいえ
ロック	はい	はい
着信音を鳴らす	はい	はい
AirPlayミラーリングを要求/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アクション

セキュリティアクション	WINDOWS タブレット 10
位置特定	はい

セキュリティアクション	WINDOWS タブレット 10
ロック	はい
ロックしてパスワードをリセット	いいえ
再起動	はい
取り消し	はい
鳴動	いいえ
選択的ワイプ	はい
ワイプ	はい

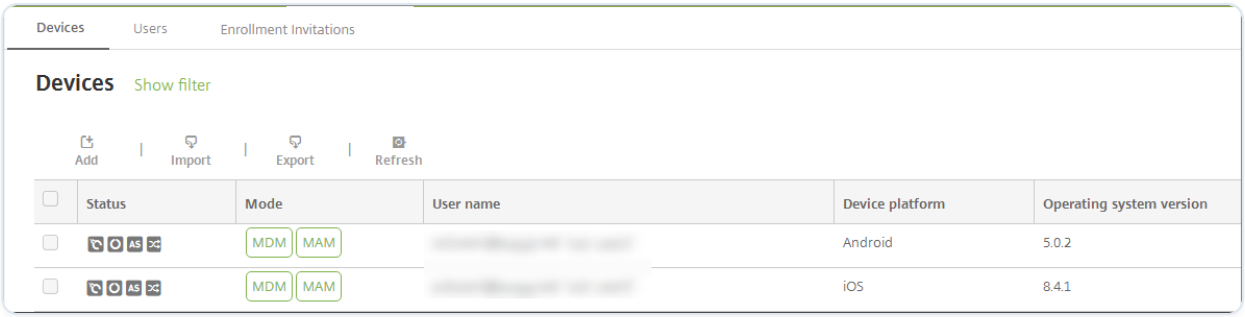
このドキュメントの残りの部分では、さまざまなセキュリティアクションを実行する手順について説明します。一部のアクションは自動化することもできます。詳細については、「自動化されたアクション」を参照してください。

iOSデバイスをロックする

紛失した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ています。

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、XenMobileコンソールでパスコードポリシーを**true**に設定します。または、ユーザーがデバイスでパスコードを手動で有効にすることもできます。

1. **管理 > デバイス**をクリックします。**デバイス**ページが表示されます。



2. ロックしたい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選択すると、デバイスリストの上にオプションメニューが表示されます。リスト内の他の場所をクリックすると、オプションメニューがリストの右側に表示されます。

オプションメニューの画像(/en-us/xenmobile/server/media/manage-devices-with-commands-secure.png)

オプションメニューの画像(/en-us/xenmobile/server/media/manage-devices-with-commands-secure-2.png)

3. オプションメニューで、**Secure**をクリックします。**Security Actions**ダイアログボックスが表示されます。

   Security Actionsダイアログボックスの画像(/en-us/xenmobile/server/media/manage-devices-secure-lock.png)

4. **Lock**をクリックします。**Security Actions**確認ダイアログボックスが表示されます。

   Security Actions確認の画像(/en-us/xenmobile/server/media/manage-devices-ios-secure-device-confirm.png)

5. 必要に応じて、デバイスのロック画面に表示され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の場合：iOSは、**Message**フィールドに入力した内容に「Lost iPad」という単語を追加します。

   iOS 7以降を実行しているiPhoneの場合：**Message**フィールドを空のままにして電話番号を提供すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

6. **Lock Device**をクリックします。

XenMobileコンソールからデバイスを削除する

> **重要：**
>
> XenMobileコンソールからデバイスを削除しても、管理対象アプリとデータはデバイスに残ります。デバイスから管理対象アプリとデータを削除するには、この記事の後半にある「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** に移動し、管理対象デバイスを選択して、**削除** をクリックします。

削除オプションの画像(/en-us/xenmobile/server/media/manage-devices-delete.png)

デバイスを選択的にワイプする

1. **管理 > デバイス** に移動し、管理対象デバイスを選択して、**保護** をクリックします。

2. **セキュリティアクション** で、**選択的ワイプ** をクリックします。
3. Android デバイスの場合のみ、デバイスを企業ネットワークから切断します。デバイスがワイプされた後、**セキュリティアクション** で **取り消し** をクリックします。

   ワイプが実行される前に選択的ワイプ要求を取り消すには、**セキュリティアクション** で **選択的ワイプのキャンセル** をクリックします。

デバイスを削除する

この手順により、管理対象アプリとデータがデバイスから削除され、XenMobile コンソールのデバイスリストからデバイスが削除されます。Endpoint Management Public REST API を使用して、デバイスを一括削除できます。

1. **管理 > デバイス** に移動し、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** 列の MDM および MAM の琥珀色は、ワイプコマンドが成功したことを示します。

   ワイプコマンドが成功したことを示す画像(/en-us/xenmobile/server/media/manage-devices-check-wipe-status.png)
4. **管理 > デバイス** で、デバイスを選択し、**削除** をクリックします。プロンプトが表示されたら、もう一度 **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、またはワイプ解除

1. 「**管理 > デバイス**」に移動し、管理対象デバイスを選択して、「**セキュリティ**」をクリックします。
2. 「**セキュリティアクション**」で、アプリのアクションをクリックします。

   セキュリティアクションボックスを使用して、Active Directoryからアカウントが無効化または削除されたユーザーのデバイスステータスを確認することもできます。アプリのロック解除またはアプリのワイプ解除アクションの存在は、ロックまたはワイプされたアプリを示します。

アプリのワイプとワイプ解除

1. 「**管理 > デバイス**」に移動します。デバイスを選択します。
2. アプリのワイプ

- 「**セキュリティ > アプリのワイプ**」をクリックします。次のメッセージが表示されたダイアログボックスが表示されます: 「**このデバイスをアプリワイプしてもよろしいですか？**」「**アプリのワイプ**」をクリックします。

3. アプリのワイプ解除

- 「**セキュリティ > アプリのワイプ解除**」をクリックします。次のメッセージが表示されたダイアログボックスが表示されます: 「**このデバイスをアプリワイプ解除してもよろしいですか？**」「**デバイスのアプリワイプ解除**」をクリックします。

4. デバイスでSecure Hubを開き、「**ストア**」をクリックします。
5. Secure Hubを起動します。

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は、iOSデバイスを紛失モードにします。Apple Managed Lost Modeとは異なり、XenMobileの紛失モードでは、ユーザーがデバイスを特定できるようにするために、次のいずれかのアクションを実行する必要はありません: 「**iPhone/iPadを探す**」設定を構成するか、Citrix Secure Hubのロケーションサービスを有効にする。

XenMobileの紛失モードでは、管理者のみがデバイスのロックを解除できます。（対照的に、XenMobileのデバイスロック機能を使用する場合、ユーザーは提供されたPINコードを使用してデバイスのロックを直接解除できます。

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、監視対象のiOSデバイスを選択して、「**セキュリティ**」をクリックします。次に、「**紛失モードを有効にする**」または「**紛失モードを無効にする**」をクリックします。

紛失モードオプションの画像(/en-us/xenmobile/server/media/manage-devices-enable-lost-mode-button.png)

「**紛失モードを有効にする**」をクリックすると、紛失モード時にデバイスに表示される情報を入力します。

デバイスに表示される情報の画像(/en-us/xenmobile/server/media/enable-lost-mode-dialog.png)

紛失モードのステータスを確認するには、以下のいずれかの方法を使用します。

- 「**セキュリティアクション**」ウィンドウで、ボタンが「**紛失モードを無効にする**」になっているか確認します。
- 「**管理 > デバイス**」から、「**セキュリティ**」の下にある「**一般**」タブで、最後に実行された「紛失モードを有効にする」または「紛失モードを無効にする」アクションを確認します。

「一般」タブの画像(/en-us/xenmobile/server/media/manage-devices-ios-lost-mode.png)

- 「**管理 > デバイス**」から、「**プロパティ**」タブで、「**MDM紛失モード有効**」設定の値が正しいことを確認します。

「MDM紛失モード有効」設定の画像(/en-us/xenmobile/server/media/manage-devices-details-properties.png)

iOSデバイスでXenMobile紛失モードを有効にすると、XenMobileコンソールも次のように変更されます。

- 「**構成 > アクション**」では、「**アクション**」リストに、次の自動アクションは含まれません。「**デバイスの取り消し**」、「**デバイスの選択的ワイプ**」、「**デバイスの完全ワイプ**」。
- 「**管理 > デバイス**」では、「**セキュリティアクション**」リストに、「**取り消し**」および「**選択的ワイプ**」デバイスアクションは含まれなくなります。必要に応じて、セキュリティアクションを使用して「**完全ワイプ**」アクション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の場合：iOSは、「**セキュリティアクション**」画面の「**メッセージ**」に入力した内容に「Lost iPad」という単語を追加します。

iOS 7以降を実行しているiPhoneの場合：「**メッセージ**」を空のままにして電話番号を提供すると、Appleはデバイスのロック画面に「Call owner」というメッセージを表示します。

iOSアクティベーションロックをバイパスする

アクティベーションロックは、紛失または盗難された監視対象デバイスの再アクティベーションを防止する「iPhone/iPadを探す」の機能です。アクティベーションロックでは、誰かが「iPhone/iPadを探す」を無効にしたり、デバイスを消去したり、デバイスを再アクティベートしたりする前に、ユーザーのApple IDとパスワードが必要です。組織が所有するデバイスの場合、たとえばデバイスをリセットまたは再割り当てするために、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オプションデバイスポリシーを構成して展開します。これにより、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できます。アクティベーションロックのApple資格情報要件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セキュリティアクションを発行します。

たとえば、ユーザーが紛失した電話を返却した場合や、完全ワイプの前後にデバイスをセットアップする場合：電話がiTunesアカウントの資格情報を要求したときに、XenMobileコンソールか

らアクティベーションロックバイパスセキュリティアクションを発行することで、その手順をバイパスできます。

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を介して監視されている
- iCloudアカウントで構成されている
- 「iPhone/iPadを探す」が有効になっている
- XenMobileに登録されている
- アクティベーションロックが有効になっているMDMオプションデバイスポリシーがデバイスに展開されている

デバイスの完全ワイプを実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：

1. **［管理］>［デバイス］** に移動し、デバイスを選択して **［セキュリティ］** をクリックし、**［アクティベーションロックバイパス］** をクリックします。
2. デバイスをワイプします。デバイスのセットアップ中にアクティベーションロック画面は表示されません。

デバイスの完全ワイプを実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：

1. デバイスをリセットまたはワイプします。デバイスのセットアップ中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**」に移動し、デバイスを選択し、「**セキュリティ**」をクリックし、その後、「**アクティベーションロックバイパス**」をクリックします。
3. デバイスの「戻る」ボタンをタップします。ホーム画面が表示されます。

次の点に注意してください。

- ユーザーに「iPhone/iPadを探す」を無効にしないようアドバイスしてください。デバイスから完全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の入力を求められます。アカウントの検証後、すべてのコンテンツと設定を消去しても、ユーザーは「iPhone/iPadをアクティベート」画面を見なくなります。
- アクティベーションロックバイパスコードが生成され、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：完全ワイプ後に「iPhone/iPadをアクティベート」ページをバイパスできない場合でも、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サポートに直接連絡して、デバイスのブロックを解除できます。

- ハードウェアインベントリ中に、XenMobileはデバイスにアクティベーションロックバイパスコードを照会します。バイパスコードが利用可能な場合、デバイスはそれをXenMobileに送信します。その後、デバイスからバイパスコードを削除するには、XenMobileコンソールからアクティベーションロックバイパスセキュリティアクションを送信します。その時点で、そしてAppleはデバイスのブロックを解除するために必要なバイパスコードを持っています。
- アクティベーションロックバイパスセキュリティアクションは、Appleサービスの可用性に依存します。アクションが機能しない場合は、次のように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を空のままにし、パスワードフィールドにバイパスコードを入力します。バイパスコードを検索するには、「**管理 > デバイス**」に移動し、デバイスを選択し、「**編集**」をクリックし、「**プロパティ**」をクリックします。「**アクティベーションロックバイパスコード**」は「**セキュリティ情報**」の下にあります。

XenMobile® AutoDiscoveryサービス

AutoDiscoveryサービスは、メールベースのURL検出を通じてユーザーの登録プロセスを簡素化します。AutoDiscoveryサービスは、登録検証、証明書ピン留め、およびCitrix Workspace™のお客様向けのその他の利点などの機能も提供します。Citrix Cloud™でホストされているこのサービスは、多くのXenMobile展開において重要な部分です。

AutoDiscoveryサービスを使用すると、ユーザーは次のことができます。

- 会社のネットワーク資格情報を使用してデバイスを登録できます。
- XenMobile Serverのアドレスに関する詳細を入力する必要がありません。
- ユーザープリンシパル名 (UPN) 形式でユーザー名を入力します。例: `user@mycompany.com`。

高セキュリティ環境ではAutoDiscoveryサービスを使用することをお勧めします。AutoDiscoveryサービスは公開鍵証明書ピン留めをサポートしており、これにより中間者攻撃を防ぎます。証明書ピン留めにより、CitrixクライアントがXenMobileと通信する際に、企業によって署名された証明書が使用されることが保証されます。XenMobileサイトの証明書ピン留めを構成するには、Citrixサポートにお問い合わせください。証明書ピン留めの詳細については、「証明書ピン留め」を参照してください。

AutoDiscoveryサービスにアクセスするには、`<https://adsui.cloud.com>` (商用) または `<https://adsui.cem.cloud.us>` (政府機関向け) に移動します。

前提条件

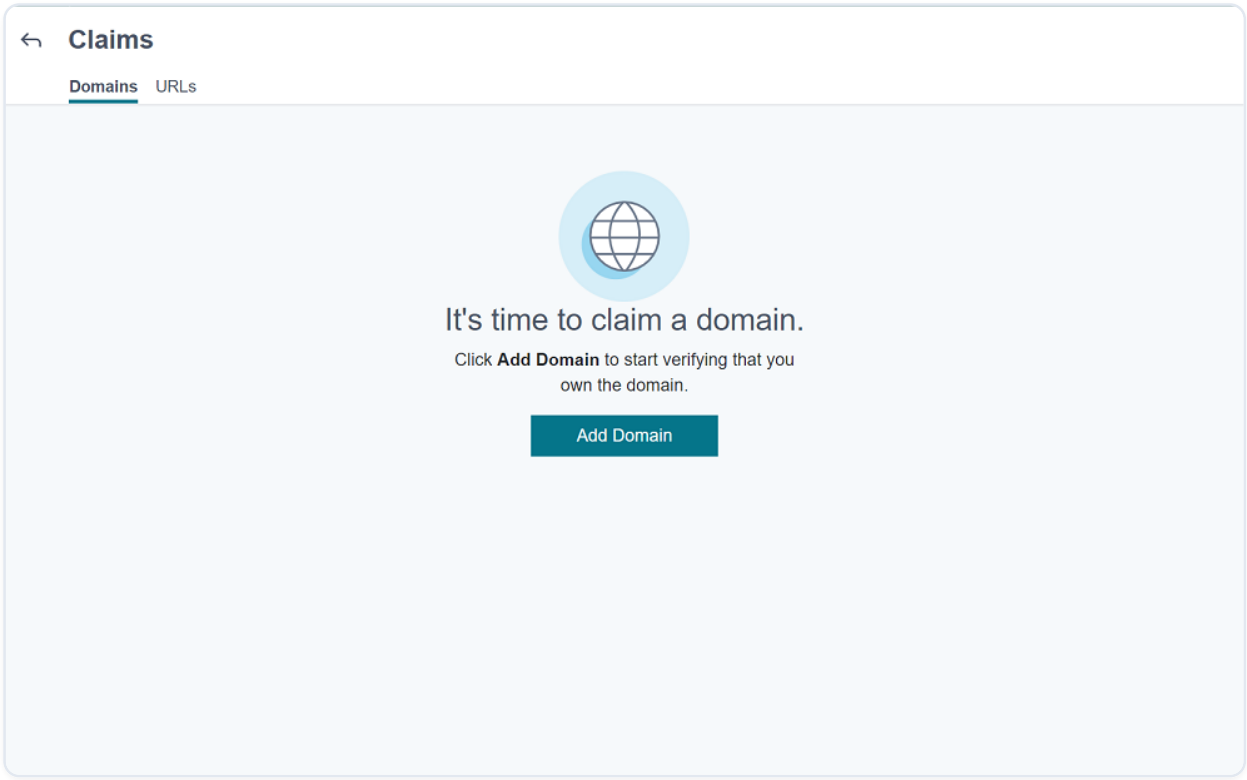
- Citrix Cloudの新しいAutoDiscoveryサービスには、Secure Hubの最新バージョンが必要です。
  - iOSの場合、Secure Hubバージョン21.6.0以降
  - Androidの場合、Secure Hubバージョン21.8.5以降

    以前のバージョンのSecure Hubで実行されているデバイスでは、サービスの中断が発生する可能性があります。
- 新しいAutoDiscoveryサービスにアクセスするには、フルアクセス権を持つCitrix Cloud管理者アカウントが必要です。AutoDiscoveryサービスは、カスタムアクセス権を持つ管理者アカウントをサポートしていません。アカウントをお持ちでない場合は、「Citrix Cloudへのサインアップ」を参照してください。

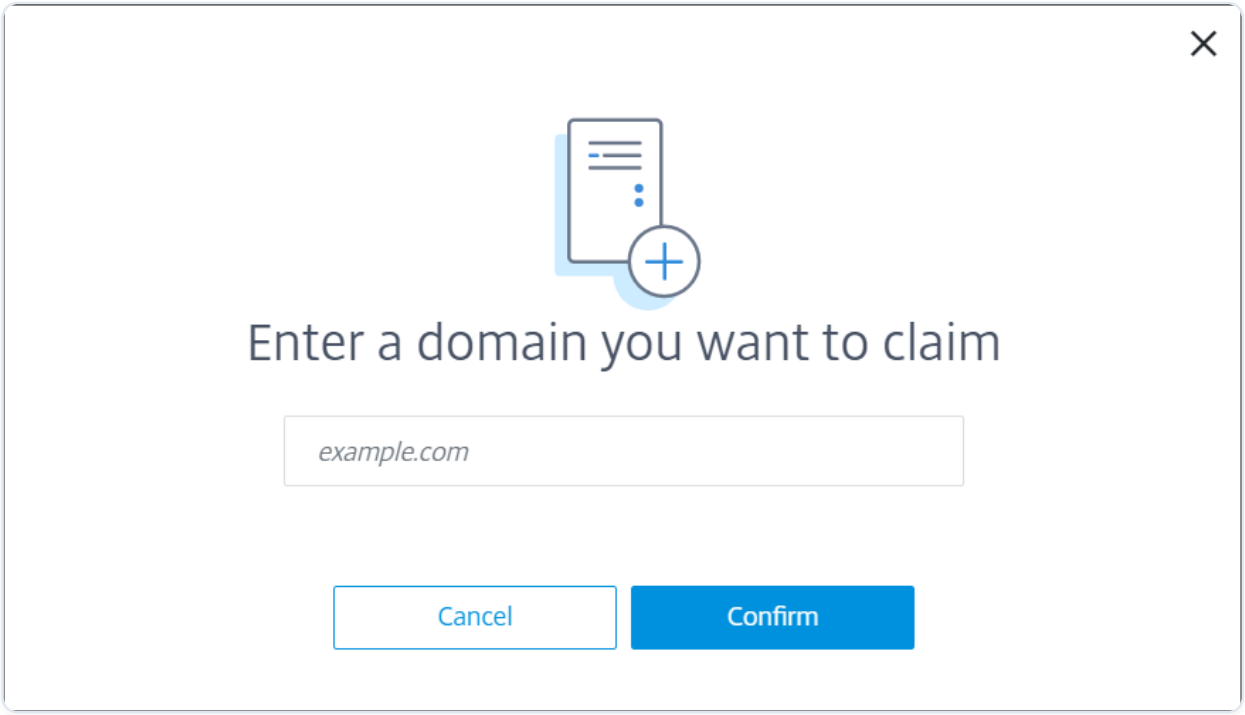
  Citrixは、既存のすべてのAutoDiscoveryレコードをサービス中断なしにCitrix Cloudに移行しました。移行されたレコードは、新しいコンソールに自動的に表示されません。所有権を証明するには、新しいAutoDiscoveryサービスでドメインを再要求する必要があります。詳細については、「CTX312339」を参照してください。
- Endpoint ManagementデプロイメントでAutoDiscoveryサービスを使用開始する前に、ドメインを検証して要求します。最大10個のドメインを要求できます。要求により、検証済みドメインがAutoDiscoveryサービスに関連付けられます。10個を超えるドメインを要求するには、SREチケットを開くか、Citrixテクニカルサポートにお問い合わせください。
- MAMトラフィックをデータセンターに誘導するには、Citrix Gateway FQDNの代わりにMAMポート設定を使用します。Citrix Gatewayのポートとともに完全修飾ドメイン名を入力すると、クライアントデバイスは**MAM Port**設定の構成を使用します。
- 広告ブロッカーによってサイトが開かない場合は、ウェブサイト全体で広告ブロッカーを無効にしてください。

ドメインを要求する

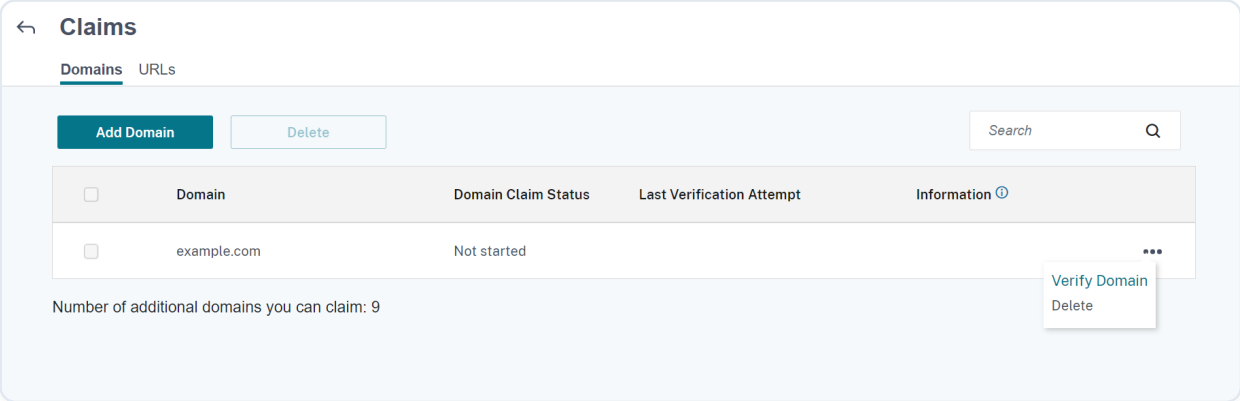
1. **Claims > Domains**タブで、**Add Domain**をクリックします。



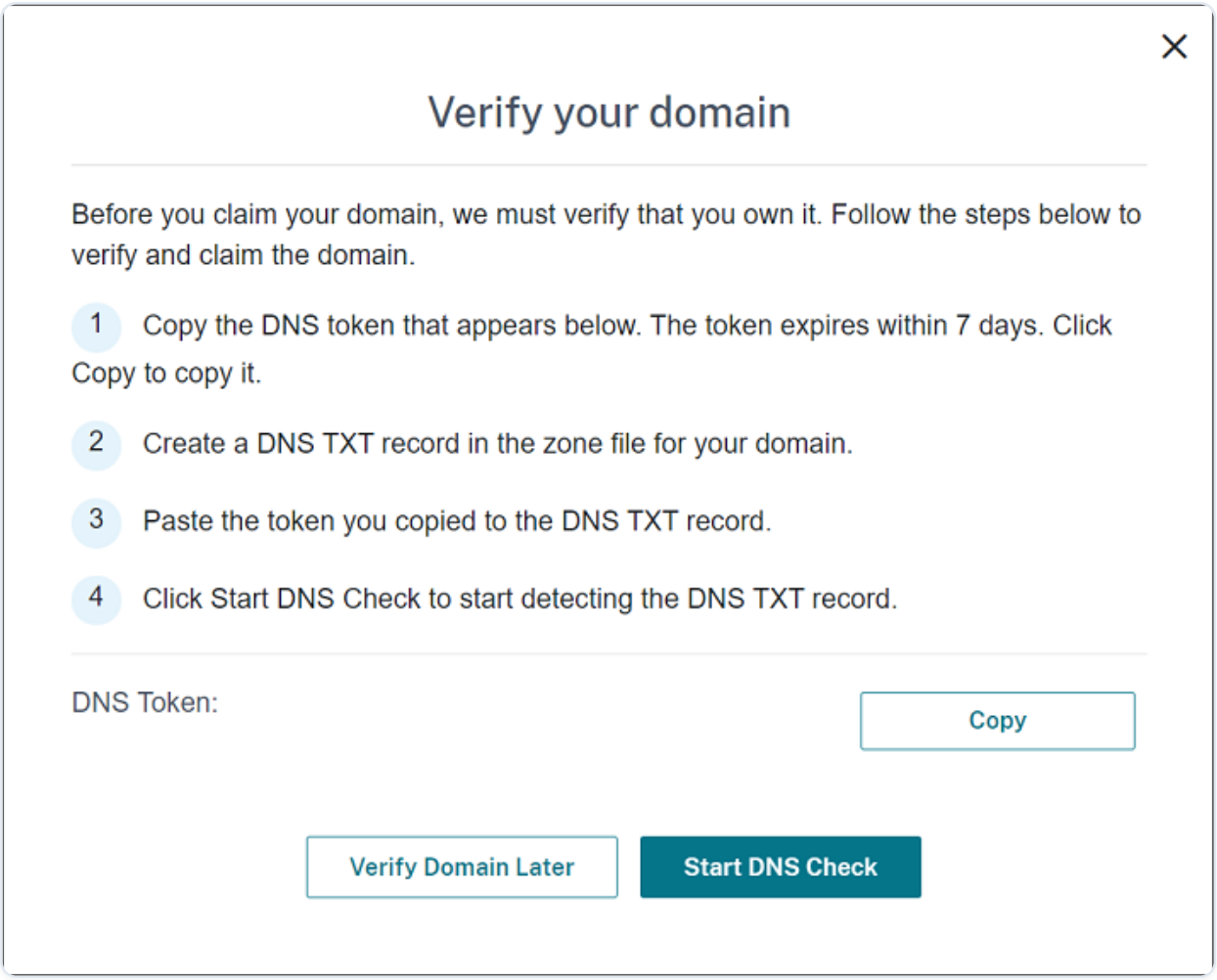
2. 表示されるダイアログボックスで、XenMobile環境のドメイン名を入力し、**Confirm**をクリックします。ドメインが**Claims > Domains**に表示されます。



3. 追加したドメインで、省略記号メニューをクリックし、**Verify Domain**を選択して検証プロセスを開始します。**Verify your domain**ページが表示されます。



4. **Verify your domain**ページで、指示に従ってドメインを所有していることを確認します。



a. **Copy**をクリックして、DNSトークンをクリップボードにコピーします。

b. 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。これを行うには、ドメインホスティングプロバイダーポータルにアクセスし、コピーしたDNSトークンを追加します。

   次のスクリーンショットは、ドメインホスティングプロバイダーポータルを示しています。お使いのポータルは異なる場合があります。

   ドメインを確認(/en-us/xenmobile/server/media/domain-hosting-provider.png)

c. Citrix Cloudで、**ドメインを確認**ページで、**DNSチェックを開始**をクリックしてDNS TXTレコードの検出を開始します。後でドメインを確認する場合は、**後でドメインを確認**をクリックします。

検証プロセスは通常約1時間かかります。ただし、応答が返されるまでに最大2日かかる場合があります。ステータスチェック中にログアウトして再度ログインしても問題ありません。

構成が完了すると、ドメインのステータスが**保留中**から**確認済み**に変わります。

5. ドメインを要求した後、AutoDiscoveryサービスに関する情報を提供します。追加したドメインの省略記号メニューをクリックし、次に**Endpoint Management情報の追加**をクリックします。**AutoDiscoveryサービス情報**ページが表示されます。
6. 次の情報を入力し、次に**保存**をクリックします。

- **Endpoint Management Server FQDN:** XenMobile Serverの完全修飾ドメイン名を入力します。例: `example.xm.cloud.com`。この設定は、MDMおよびMAM制御トラフィックに使用されます。
- **Citrix Gateway FQDN:** Citrix Gatewayの完全修飾ドメイン名（FQDNまたはFQDN:ポートの形式）を入力します。例: `example.com`。この設定は、MAMトラフィックをデータセンターにルーティングするために使用されます。MDMのみの展開の場合、このフィールドは空白のままにします。

> **注：**
>
> Citrixでは、MAMトラフィックを制御するために、**Citrix Gateway FQDN**ではなく**MAMポート**設定を使用することをお勧めします。Citrix Gatewayのポートとともに完全修飾ドメイン名を入力した場合、クライアントデバイスは**MAMポート**設定の構成を使用します。

- **インスタンス名：** 以前に構成したXenMobile Serverのインスタンス名を入力します。インスタンス名が不明な場合は、デフォルト値の**zdm**のままにします。
- **MDMポート：** MDM制御トラフィックおよびMDM登録に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは443です。
- **MAMポート：** MAM制御トラフィック、MAM登録、iOS登録、およびアプリ列挙に使用されるポートを入力します。クラウドベースのサービスの場合、デフォルトは8443です。

WindowsデバイスのAutoDiscoveryを要求する

Windowsデバイスを登録する予定がある場合は、次の手順を実行します。

1. Citrixサポートに連絡し、Windows AutoDiscoveryを有効にするためのサポートリクエストを作成します。
2. `enterpriseenrollment.mycompany.com` 用の、公開署名されたワイルドカードではないSSL証明書を取得します。`mycompany.com` の部分は、ユーザーが登録に使用するアカウントを持つドメインです。前の手順で作成したサポートリクエストに、.pfx形式のSSL証明書とそのパスワードを添付します。

   複数のドメインを使用してWindowsデバイスを登録するには、以下の構造を持つマルチドメイン証明書を使用することもできます。

   - サービスを提供するプライマリドメインを指定するCNを持つSubjectDN（例: enterpriseenrollment.mycompany1.com）。
   - 残りのドメインに対する適切なSAN（例: enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.comなど）。
3. DNSに正規名 (CNAME) レコードを作成し、SSL証明書のアドレス (enterpriseenrollment.mycompany.com) をautodisc.xm.cloud.comにマッピングします。

   WindowsデバイスのユーザーがUPNを使用して登録すると、Citrix登録サーバーは次の処理を行います。

   - XenMobile Serverの詳細を提供します。
   - デバイスにXenMobileから有効な証明書を要求するよう指示します。

この時点で、サポートされているすべてのデバイスを登録できます。次のセクションに進み、デバイスにリソースを配信する準備をします。

デバイスポリシー

ポリシーを作成することで、XenMobile® がデバイスとどのように連携するかを構成できます。多くのポリシーはすべてのデバイスに共通ですが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。そのため、プラットフォーム間、さらにはAndroidデバイスの異なるメーカー間でも違いが見られる場合があります。

各デバイスポリシーの概要については、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およびWindows 11デバイス向けにXenMobileデバイスポリシーを構成する際は、以下の規則に留意してください。1つ以上の登録済みデバイスでポリシーが競合する場合、GPOに準拠した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については、「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。

デバイスポリシーを追加する

デバイスポリシーを作成する基本的な手順は次のとおりです。

1. ポリシーに名前を付け、説明します。
2. 1つ以上のプラットフォーム向けにポリシーを構成します。
3. 展開ルールを作成します (オプション)。

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 (オプション)。

デバイスポリシーを作成および管理するには、 > に移動します。

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/configure-device-policies-unfiltered.png)

ポリシーを追加するには:

1. ページで、 をクリックします。 ページが表示されます。

   デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/configure-device-policies-add.png)
2. 1つ以上のプラットフォームをクリックして、選択したプラットフォームのデバイスポリシーのリストを表示します。ポリシー名をクリックして、ポリシーの追加を続行します。

   デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/configure-device-policies-add-filtered.png)

   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、一致する可能性のある項目が表示されます。ポリシーがリストにある場合は、それをクリックします。選択したポリシーのみが結果に残ります。それをクリックして、そのポリシーの****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は、手順5に表示されます。
4. ページを完了し、 をクリックします。 ページでは、ポリシー名などの情報を収集して、ポリシーの識別と追跡に役立てます。このページは、すべてのポリシーで同様です。
5. プラットフォームページを完了します。プラットフォームページは、手順3で選択した各プラットフォームに表示されます。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場合があります。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わけではありません。

   一部のページには項目のテーブルが含まれています。既存の項目を削除するには、リストを含む行にカーソルを合わせ、右側にあるゴミ箱アイコンをクリックします。確認ダイアログで、 をクリックします。

   既存の項目を編集するには、リストを含む行にカーソルを合わせ、右側にあるペンアイコンをクリックします。

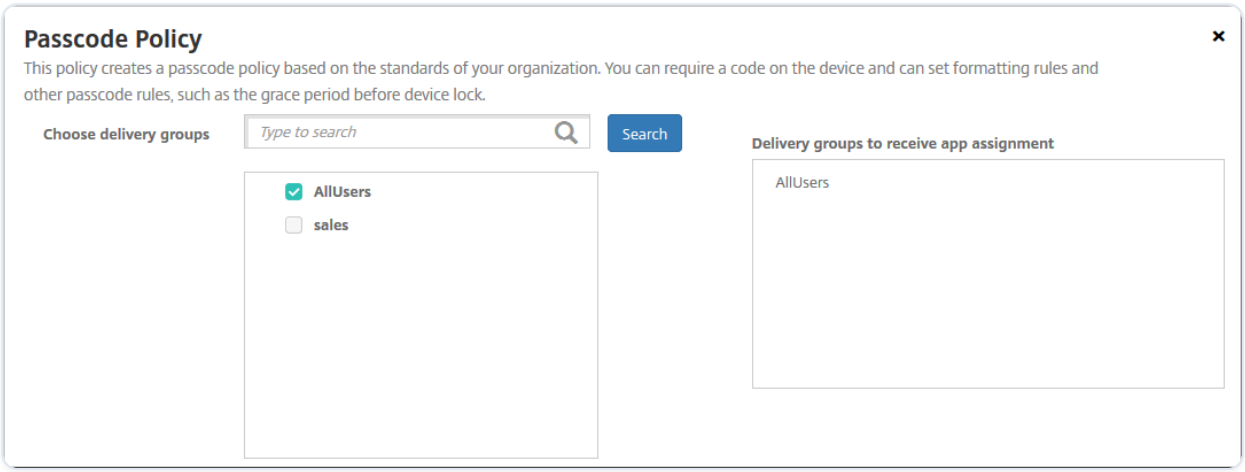
展開ルール、割り当て、およびスケジュールを構成するには

展開ルール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. プラットフォームページで、**展開ルール**を展開し、次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。
   - リストでオプションをクリックし、ポリシーを展開するタイミングを決定します。すべての条件が満たされたとき、または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ことを選択できます。デフォルトのオプションは**すべて**に設定されています。
   - **新規ルール**をクリックして条件を定義します。
   - リストで、**デバイスの所有権**や**BYOD**などの条件をクリックします。
   - さらに条件を追加する場合は、もう一度**新規ルール**をクリックします。条件はいくつでも追加できます。
2. **詳細**タブをクリックして、ルールをブールオプションと組み合わせます。**基本**タブで選択した条件が表示されます。
3. より高度なブール論理を使用して、ルールを結合、編集、または追加できます。
   - **AND**、**OR**、または**NOT**をクリックします。
   - リストで、ルールに追加する条件を選択します。次に、右側にあるプラス記号（**+**）をクリックして、条件をルールに追加します。

     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するか、**削除**をクリックして条件を削除できます。
   - **新規ルール**をクリックして、別の条件を追加します。
4. **次へ**をクリックして次のプラットフォームページに移動するか、すべてのプラットフォームページが完了したら**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、そのグループが**アプリの割り当てを受け取るデリバリーグループ**ボックスに表示されます。

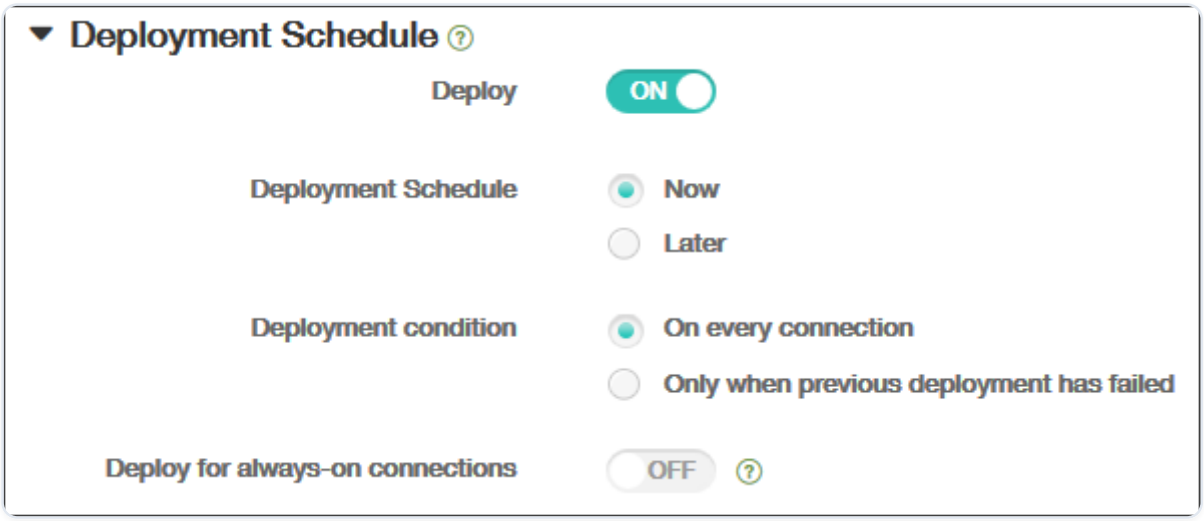
   アプリの割り当てを受け取るデリバリーグループは、デリバリーグループを選択するまで表示されません。



6. **割り当て**ページで、**展開スケジュール**を展開し、次の設定を構成します。

   - **展開**の横にある**オン**をクリックして展開をスケジュールするか、**オフ**をクリックして展開を防止します。デフォルトのオプションは**オン**に設定されています。
   - **展開スケジュール**の横にある**今すぐ**または**後で**をクリックします。デフォルトのオプションは**今すぐ**に設定されています。
   - **後で**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、展開の日付と時刻を選択します。
   - **展開条件**の横にある**すべての接続時**をクリックするか、**前回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**すべての接続時**に設定されています。
   - **常時接続の展開**の横にある**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**に設定されています。

   > **注:**
   >
   > このオプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キー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デバイスでは利用できません。
   >
   > 構成する展開スケジュールは、すべてのプラットフォームで同じです。加えた変更はすべてのプラットフォームに適用されますが、iOSには適用されない**常時接続の展開**は除きます。



7. **保存**をクリックします。

   ポリシーは**デバイスポリシー**テーブルに表示されます。

デバイスからデバイスポリシーを削除する

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。

- アンドロイド

  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。詳細については、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および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、削除したいポリシーのみのプロファイル削除デバイスポリシーを作成できます。残りのポリシーとプロファイルはデバイスに残ります。詳細については、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およびWindows 11

  Windowsデスクトップまたはタブレットデバイスからデバイスポリシーを直接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。ユーザーは続行するために再登録します。
  - 特定のデバイスを選択的にワイプするセキュリティアクションをプッシュします。このアクションにより、すべての企業アプリとデータがデバイスから削除されます。その後、そ

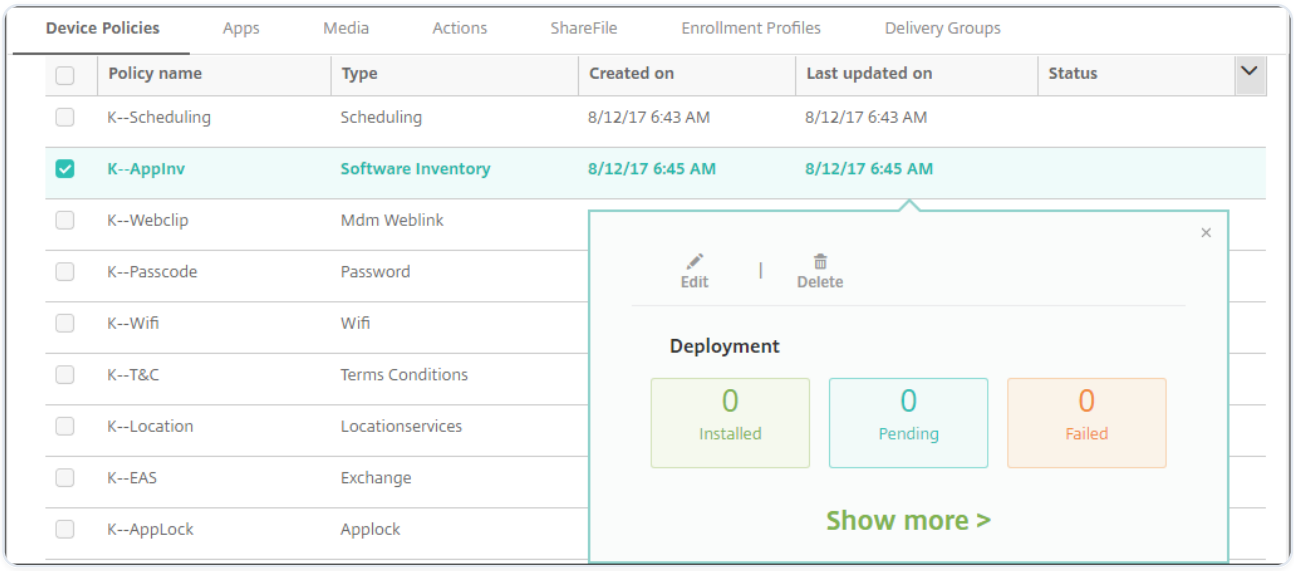
のデバイスのみを含むデリバリーグループからデバイスポリシーを削除し、そのデリバリーグループをデバイスにプッシュします。ユーザーは続行するために再登録します。

- クローム OS

  Chrome OSデバイスからデバイスポリシーを削除するには、そのデバイスのみ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、そのデリバリーグループをデバイスにプッシュします。

デバイスポリシーを編集する

ポリシーを編集するには、ポリシーの横にあるチェックボックスを選択して、ポリシーリストの上にあるオプションメニューを表示します。または、リスト内のポリシーをクリックして、リストの右側にあるオプションメニューを表示します。



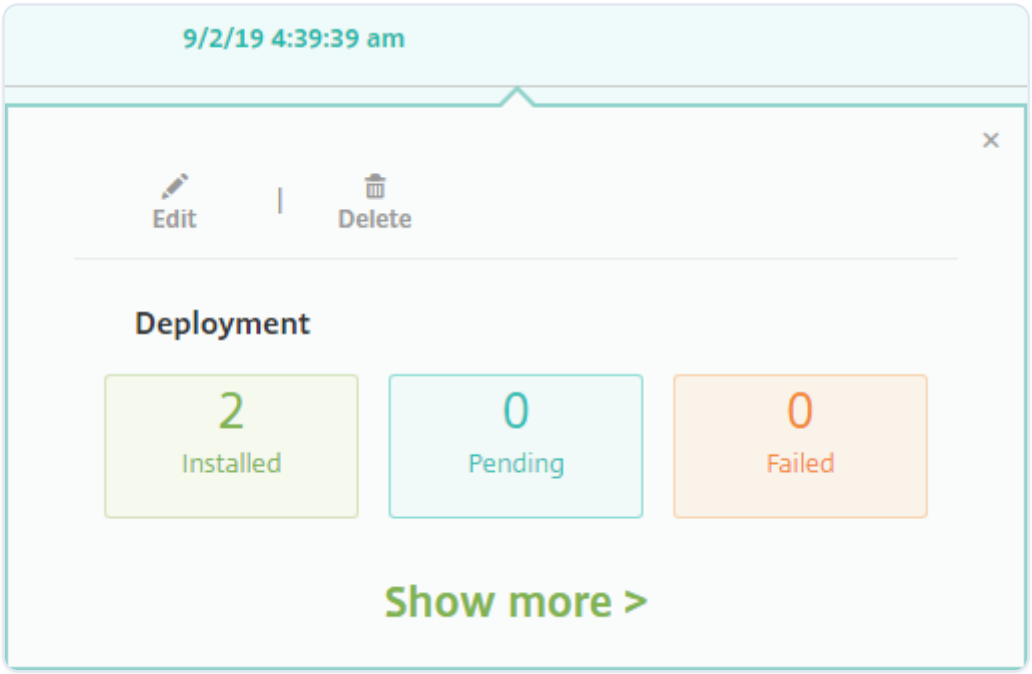
ポリシーの詳細を表示するには、 をクリックします。

デバイスポリシーのすべての設定を編集するには、 をクリックします。

をクリックすると、確認ダイアログボックスが表示されます。ポリシーを削除するには、もう一度をクリックします。

ポリシー展開ステータスの確認

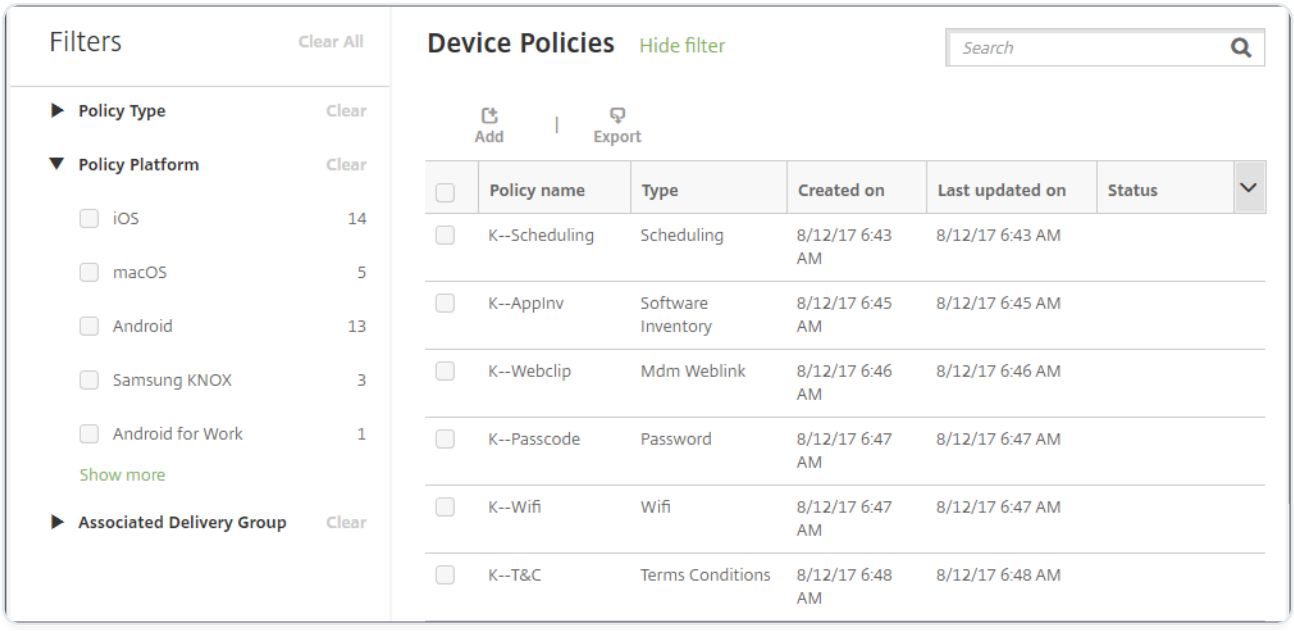
展開ステータスを確認するには、 > ページでポリシーの行をクリックします。



ポリシーの展開が保留中の場合、ユーザーはSecure Hubで > > をタップしてポリシーを更新できます。

追加されたデバイスポリシーのリストをフィルターする

追加されたポリシーのリストは、ポリシーの種類、プラットフォーム、および関連付けられたデリバリーグループでフィルターできます。 > ページで、 をクリックします。リストで、表示する項目のチェックボックスをオンにします。



フィルターを保存するには、 をクリックします。フィルターの名前は、 ボタンの下にボタンとして表示されます。

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（別の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許可リストにデバイスを追加するオプションもあります。このオプションでは、ユーザーは許可リストにあるAirPlayデバイスのみに制限されます。
AirPrint	iOSデバイスのAirPrintプリンターリストにAirPrintプリンターを追加します。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上にある環境をサポートしやすくなります。
Android Enterpriseアプリの権限	ワークプロファイル内のAndroid Enterpriseアプリへの要求が、Googleが「危険な」権限と呼ぶものをどのように処理するかを構成します。
Android Enterpriseアプリの制限	Androidアプリに関連付けられている制限を更新します。
APN	デバイスを特定の電話会社のGeneral Packet Radio Service (GPRS) に接続するために使用される設定を決定します。この設定は、ほとんどの新しい電話で既に定義されています。組織がモバイルデバイスからインターネットに接続するためにコンシューマーAPNを使用しない場合は、このポリシーを使用します。
アプリのアクセス	デバイス上で必須、オプション、または禁止されているアプリのリストを定義します。その後、そのアプリのリストに対するデバイスのコンプライアンスに対応する自動アクションを作成できます。
アプリの属性	iOSデバイスの管理対象アプリバンドルIDやアプリごとのVPN識別子などの属性を指定します。

デバイスポリシー名	デバイスポリシーの説明
アプリの構成	管理対象構成をサポートするアプリのさまざまな設定と動作をリモートで構成します。そのためには、XML構成ファイル（プロパティリスト、またはplistと呼ばれます）をiOSデバイスに展開します。または、キー/値のペアをWindows 10 Phone、またはWindows 10またはWindows 11を実行しているデスクトップまたはタブレットデバイスに展開します。
アプリのインベントリ	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、そのインベントリをそれらのデバイスに展開されているアプリアクセスポリシーと比較します。これにより、アプリアクセス許可リストまたはブロックリストにあるアプリを検出し、適切に対応できます。
アプリロック	ユーザーが iOS または特定の Android デバイスで実行できる、または実行できないアプリのリストを定義します。
アプリのネットワーク使用状況	iOS デバイスで、管理対象アプリが携帯電話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かを指定するネットワーク使用ルールを設定します。このルールは管理対象アプリにのみ適用されます。管理対象アプリとは、XenMobile を介してユーザーデバイスに展開するアプリのことです。
アプリのアンインストール	ユーザーデバイスからアプリを削除します。
アプリの通知	iOS ユーザーが指定されたアプリから通知を受け取る方法を制御します。
管理対象アプリを自動的に更新する	Android Enterprise デバイスにインストールされている管理対象アプリがどのように更新されるかを制御します。
BitLocker	Windows 10 および Windows 11 デバイスの BitLocker インターフェイスで利用可能な設定を構成します。

デバイスポリシー名	デバイスポリシーの説明
カレンダー (CalDAV)	iOS または macOS デバイスにカレンダー (CalDAV) アカウントを追加します。CalDAV アカウントを使用すると、ユーザーは CalDAV をサポートする任意のサーバーとスケジュールデータを同期できます。
セルラー	セルラーネットワーク設定を構成します。
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でのみ利用可能です。
連絡先 (CardDAV)	iOSまたはmacOSデバイスにiOS連絡先 (CardDAV) アカウントを追加します。CardDAVアカウントを使用すると、ユーザーはCardDAVをサポートする任意のサーバーと連絡先データを同期できます。
OSアップデートの制御	サポート対象の監視対象デバイスに最新のOSアップデートを展開します。
資格情報	XenMobileのPKI構成との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、またはサーバー証明書を使用します。
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、デバイス構成、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	Windows 10およびWindows 11のデスクトップおよびタブレット向けにWindows Defender設定を構成します。
デバイス正常性構成証明	Windows 10およびWindows 11デバイスがその健全性の状態を報告することを要求します。そのためには、分析のために特定のデータとランタイム情報をHealth Attestation Service (HAS)に送信します。HASは、デバイスがXenMobileに送信するHealth Attestation

デバイスポリシー名	デバイスポリシーの説明
	Certificateを作成して返します。XenMobileがHealth Attestation Certificateを受信すると、その証明書の内容に基づいて、構成した自動アクションを展開できます。
デバイス名	iOSおよびmacOSデバイスに名前を設定し、デバイスを識別できるようにします。マクロ、テキスト、またはその両方の組み合わせを使用して、デバイス名を定義できます。
教育構成	Apple Educationで使用するために、教員および生徒のデバイスを構成します。教員がClassroomアプリを使用する場合、Education Configurationデバイスポリシーが必要です。
エクスチェンジ	デバイス上のネイティブメールクライアントでActiveSyncメールを有効にします。
ファイル	ユーザーのために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自分のデバイスでアクセスできるようにしたいドキュメントファイルを追加できます。ファイルを追加する際に、デバイスにファイルを保存するディレクトリも指定できます。
FileVault	このポリシーにより、登録済みのmacOSデバイスでFileVaultデバイス暗号化を有効にできます。また、ユーザーがログイン中に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以降で利用可能です。
フォント	iOS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)フォント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。

デバイスポリシー名	デバイスポリシーの説明
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で、iOSホーム画面の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。このファイルには、Apple Configuratorを使用して準備するデバイスセキュリティポリシーと制限が含まれています。
キーガード管理	ユーザーがデバイスのキーガードとワークチャレンジのキーガードを解除する前に利用できる機能を制御します。また、完全に管理された専用デバイスのデバイスキーガード機能を制御することもできます。たとえば、指紋認証によるロック解除、信頼エージェント、通知などのロック画面機能を無効にできます。
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または複数のアプリに制限できます。このポリシーは、特定の種類のアプリのみを実行することを目的とした企業デバイスに役立ちます。このポリシーでは、キオスクモードのデバイスのホーム画面とロック画面の壁紙にカスタム画像を選択することもできます。
ノックス プラットフォーム フォー エンタープライズ キー	必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供できます。
ランチャー構成	Androidデバイス上のCitrix Launcherの設定（許可されるアプリやLauncherアイコンのカスタムロゴ画像など）を指定します。
LDAP	iOSデバイスで使用するLDAPサーバーに関する情報（LDAPサーバーのホスト名などの必要なアカウント情報を含む）を提供します。このポリシーは、LDAPサーバーをクエリするときに使用する一連のLDAP検索ポリシーも提供します。

デバイスポリシー名	デバイスポリシーの説明
位置情報	Secure HubでGPSが有効になっていることを前提として、マップ上でデバイスの地理的位置を特定できます。このポリシーをデバイスに展開した後、XenMobile Serverから位置特定コマンドを送信できます。デバイスは位置座標で応答します。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ています。
メール	iOSまたはmacOSデバイスでメールアカウントを設定します。
管理対象ドメイン	メールおよびSafariブラウザに適用される管理対象ドメインを定義します。管理対象ドメインは、Safariを使用してドメインからダウンロードされたドキュメントをどのアプリが開くことができるかを制御することで、企業データを保護するのに役立ちます。iOS 8以降の監視対象デバイスでは、ユーザーがブラウザからドキュメント、添付ファイル、ダウンロードを開く方法を制御するために、URLまたはサブドメインを指定できます。
MDMオプション	監視対象のiOS 7.0以降の電話デバイスで、iPhoneを探す機能とiPad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強制します。デバイスのパスコードの複雑さとタイムアウトを設定できます。
インターネット共有	ユーザーがWi-Fiネットワークの範囲外にいるときにインターネットに接続できるようにします。ユーザーは、インターネット共有機能を使用して、iOSデバイスのモバイルデータ通信接続を介して接続します。
プロファイルの削除	iOSまたはmacOSデバイスからアプリプロファイルを削除します。

デバイスポリシー名	デバイスポリシーの説明
プロビジョニングプロファイル	デバイスに送信す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指定します。iOSエンタープライズアプリを開発してコード署名する場合、通常はプロビジョニングプロファイルを含めます。Appleは、アプリがiOSデバイスで実行されるためにこのプロファイルを必要とします。プロビジョニングプロファイルが見つからないか期限切れの場合、ユーザーがアプリを開こうとタップ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	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。デバイスごとに展開できるグローバルHTTPプロキシポリシーは1つだけです。
制限	管理対象デバイスの機能と機能をロックダウンおよび制御するための何百ものオプションを提供します。制限オプションの例：カメラまたはマイクを無効にする、ローミングルールを適用する、アプリストアなどのサードパーティサービスへのアクセスを適用する。
ローミング	iOSデバイスで音声およびデータローミングを許可するかどうかを設定します。音声ローミングが無効になっている場合、データローミングは自動的に無効になります。
スケジューリング	MDM管理、アプリプッシュ、およびポリシー展開のために、AndroidデバイスがXenMobile Serverに接続し直すために必要です。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し直すことができません。
SCEP	外部SCEPサーバーから証明書を取得するようにiOSおよびmacOSデバイスを設定します。XenMobileに接続されているPKIからSCEPを

デバイスポリシー名	デバイスポリシーの説明
	使用してデバイスに証明書を配信することもできます。そのためには、分散モードでPKIエンティティとPKIプロバイダーを作成します。
SSOアカウント	ユーザーがXenMobileおよび社内リソースにアクセスするために一度だけサインオンするシングルサインオン（SSO）アカウントを作成します。ユーザーはデバイスに資格情報を保存する必要はありません。XenMobileは、App Storeのアプリを含む、アプリ全体でSSOアカウントのエンタープライズユーザー資格情報を使用します。このポリシーはKerberos認証と互換性があります。iOSで利用可能です。
購読済みカレンダー	iOSデバイスの予定表リストに購読済みの予定表を追加します。ユーザーデバイスの購読済み予定表リストに追加する前に、予定表を購読していることを確認してください。
利用規約	企業ネットワークへの接続を管理する会社の特定のポリシーをユーザーが承諾することを要求します。ユーザーがXenMobileにデバイスを登録する際、デバイスを登録するには利用規約に同意する必要があります。利用規約を拒否すると、登録プロセスはキャンセルされます。
トンネル	リモートサポートでのみ使用されます。リモートサポートにより、ヘルプデスク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。クラスター化されたオンプレミスXenMobile Server展開では、リモートサポートは利用できません。Remote Supportは、January 1, 2019以降、新規顧客には提供されなくなりました。既存の顧客は引き続き製品を使用できますが、Citrixは機能強化や修正を提供しません。
VPN	従来のVPNゲートウェイテクノロジー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

デバイスポリシー名	デバイスポリシーの説明
	す。XenMobileは、Cisco AnyConnect、Juniper、Citrix VPNなど、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	iOSデバイスのロック画面、ホーム画面、またはその両方に壁紙を設定するために、.pngまたは.jpgファイルを追加します。iPadとiPhoneで異なる壁紙を使用するには、異なる壁紙ポリシーを作成し、適切なユーザーに展開します。
Webコンテンツフィルター	iOSデバイスのWebコンテンツをフィルタリングします。XenMobileは、Appleの自動フィルター機能と、許可リストおよびブロックリストに追加したサイトを使用します。iOS監視対象デバイスでのみ利用可能です。
Webクリップ	Webサイトへのショートカット（Webクリップ）を配置し、ユーザーデバイス上のアプリと並んで表示されるようにします。iOS、macOS、および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タブレットでは、ラベルとURLのみが必要です。
ワイファイ	管理者がWi-Fiルーターの詳細を管理対象デバイスに展開できるようにします。ルーターの詳細には、SSID、認証データ、および構成データが含まれます。
Windows 情報保護	ポリシーに設定した適用レベルで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およびWindows 11の監視対象デバイス用です。
XenMobile ストア	XenMobile Storeの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。

デバイスポリシー名	デバイスポリシーの説明
XenMobileオプション	AndroidデバイスからXenMobileに接続する際のSecure Hubの動作を構成します。
XenMobileアンインストール	AndroidおよびWindow Mobile/CEデバイスからXenMobileをアンインストールします。展開されると、このポリシーは展開グループ内のすべてのデバイスからXenMobileを削除します。

プラットフォーム別のデバイスポリシー

プラットフォームごとに利用可能なポリシーを表示するには、次の手順に従います。

1. XenMobile®コンソールで、 > の順に移動します。
2. をクリックします。
3. 各デバイスプラットフォームは、 ペインのリストに表示されます。このペインが開いていない場合は、 をクリックします。
4. プラットフォームで利用可能なすべてのポリシーのリストを表示するには、そ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利用可能なポリシーのリストを表示するには、それらのプラットフォームをそれぞれ選択します。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リストに表示されます。

デバイスポリシー構成画面のフィルター処理された画像(/en-us/xenmobile/server/media/policies-list-filtered.png)

XenMobileの最新バージョンは、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。

- アマゾン
- アンドロイド
- アンドロイド エンタープライズ
- アンドロイド ゼブラ
- iOS
- macOS
- サムスン SAFE
- サムスン ノックス

- Windows 10およびWindows 11デスクトップ/タブレット

XenMobileの最新バージョンでサポートされているデバイスの詳細については、サポートされている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およびWindows 11向けにXenMobileデバイスポリシーを構成する際は、以下の規則に留意してください。1つ以上の登録済みデバイスでポリシーが競合する場合、GPOに準拠した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

AppleのAirPlay機能を使用すると、デバイスのディスプレイに表示されている内容を別のMacコンピュータに正確にミラーリングできます。

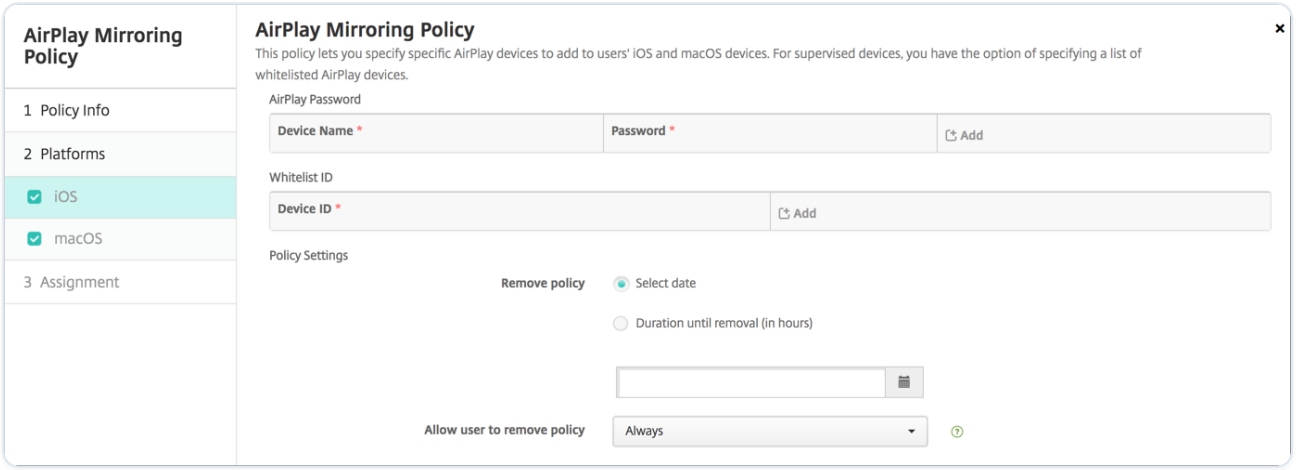
XenMobileでデバイスポリシーを追加して、特定のAirPlayデバイス（別のMacコンピュータなど）をiOSデバイスに追加できます。また、監視対象デバイスの許可リストにデバイスを追加するオプションもあり、これによりユーザーは許可リスト上のAirPlayデバイスのみに制限されます。デバイスを監視モードにする方法については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」(/ja-jp/xenmobile/server/provision-devices/ios-bulk-enrollment.html#to-configure-apple-configurator-2-settings)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とパスワードを準備してください。

> このポリシーを追加または構成するには、**Configure > Device Policies**に移動します。詳細については、「デバイスポリシー」(/ja-jp/xenmobile/server/policies.html)を参照してください。

iOS設定



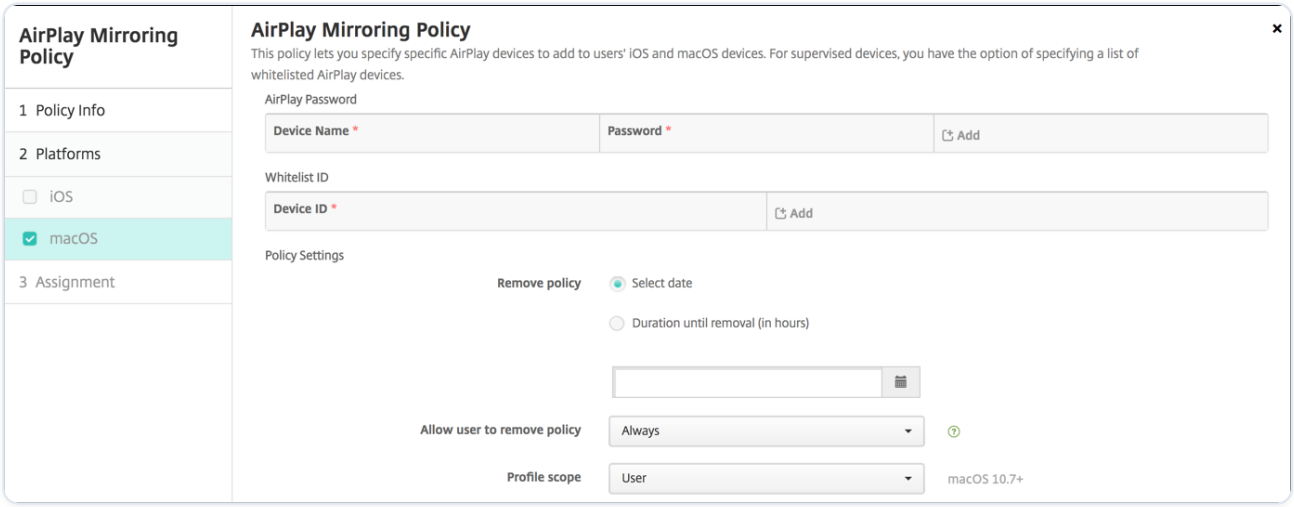
- **AirPlayパスワード:** 追加する各デバイスについて、**追加**をクリックし、次の操作を行います。
  - **デバイスID:** ハードウェアアドレス（MACアドレス）をxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - **パスワード:** デバイスのオプションのパスワードを入力します。
  - デバイスを追加するには**追加**をクリックし、デバイスの追加をキャンセルするには**キャンセル**をクリックします。
- **ホワイトリストID:** このリストは、監視対象外のデバイスでは無視されます。このリストのデバイスIDは、ユーザーのデバイスで利用可能な唯一のAirPlayデバイスです。リストに追加する各AirPlayデバイスについて、**追加**をクリックし、次の操作を行います。

> **注:**
>
> XenMobile® Serverコンソールには、「ブラックリスト」と「ホワイトリスト」という用語が含まれています。今後のリリースで、これらの用語は「ブロックリスト」と「許可リスト」に変更されます。

  - **デバイスID:** デバイスIDをxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - デバイスを追加するには**追加**をクリックし、デバイスの追加をキャンセルするには**キャンセル**をクリックします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。

- **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
- **削除までの期間（時間）:** ポリシーが削除されるまでの時間を入力します。

macOS設定



- **AirPlayパスワード:** 追加する各デバイスについて、**追加**をクリックし、次の操作を行います。
  - **デバイスID:** ハードウェアアドレス（MACアドレス）をxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - **パスワード:** デバイスのオプションのパスワードを入力します。
  - デバイスを追加するには**追加**をクリックし、デバイスの追加をキャンセルするには**キャンセル**をクリックします。
- **ホワイトリストID:** このリストは、監視対象外のデバイスでは無視されます。このリストのデバイスIDは、ユーザーデバイスで利用可能な唯一のAirPlayデバイスです。リストに追加する各AirPlayデバイスについて、**追加**をクリックし、次の操作を行います。
  - **デバイスID:** デバイスIDをxx:xx:xx:xx:xx:xx形式で入力します。このフィールドでは大文字と小文字は区別されません。
  - デバイスを追加するには**追加**をクリックし、デバイスの追加をキャンセルするには**キャンセル**をクリックします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択** および **削除までの期間 (時間)** です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。

- **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから **常に**、**パスコードが必要**、または **しない** を選択します。**パスコードが必要** を選択した場合は、**削除パスコード** フィールドにパスコードを入力します。
- **プロファイルスコープ:** このポリシーを **ユーザー** に適用するか、**システム** 全体に適用するかを選択します。デフォルトは **ユーザー** です。このオプションは macOS 10.7 以降でのみ利用可能です。

AirPrint デバイスポリシー

XenMobile® でデバイスポリシーを追加して、iOS デバイスの AirPrint プリンターリストに AirPrint プリンターを追加できます。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ある環境をサポートしやすくなります。

このポリシーは iOS 7.0 以降に適用されます。

> **注記:**
>
> 各プリンターの IP アドレスとリソースパスを必ず用意してください。

> このポリシーを追加または構成するには、 > に移動します。詳細については、デバイスポリシーを参照してください。

iOS 設定

- **AirPrint 宛先:** 追加する AirPrint 宛先ごとに、 をクリックし、次の操作を行います。
  - **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。例: printers/Canon_MG5300_series または printers/Xerox_Phaser_7600。
  - をクリックしてプリンターを追加するか、 をクリックしてプリンターの追加をキャンセルします。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、 と です。

- **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
- **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0 以降でのみ利用可能です。

Android Enterpriseアプリの権限

ワークプロファイル内のAndroid Enterpriseアプリに対するリクエストが、Googleが「危険」と呼ぶ権限をどのように処理するかを設定できます。ユーザーに権限リクエストの許可または拒否を求めるかどうかを制御します。この機能は、Android 7.0以降を実行しているデバイスに適用されます。

Googleは、危険な権限を、ユーザーの個人情報に関わるデータやリソースへのアプリのアクセスを許可したり、ユーザーの保存データや他のアプリの操作に潜在的に影響を与えたりする権限と定義しています。たとえば、ユーザーの連絡先を読み取る機能は危険な権限です。

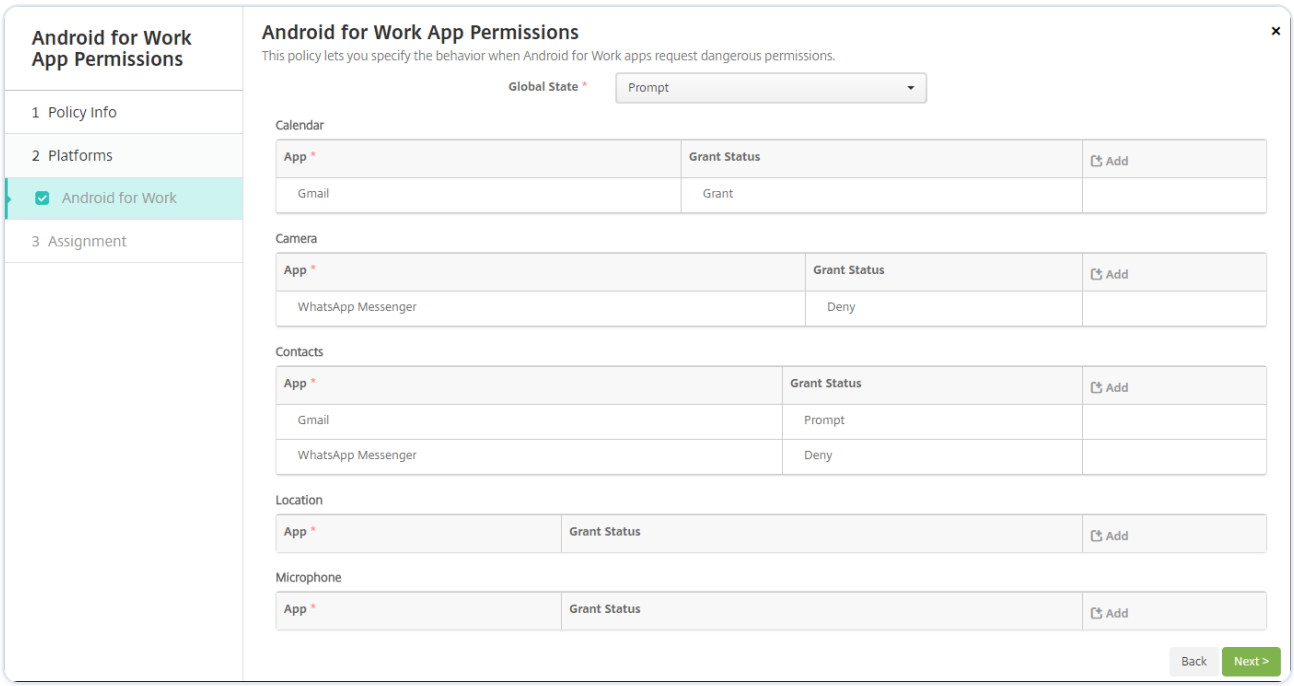
ワークプロファイル内のAndroid Enterpriseアプリに対するすべての危険な権限リクエストの動作を制御するグローバル状態を設定できます。また、Googleによって定義された個々の権限グループについて、アプリごとに危険な権限リクエストの動作を制御することもできます。これらの個別の設定は、グローバル状態を上書きします。

Googleが権限グループをどのように定義しているかについては、このAndroid開発者ガイドの「権限グループ」を参照してください。

デフォルトでは、ユーザーは危険な権限リクエストの許可または拒否を求められます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

Android Enterpriseの設定



- **グローバル状態:** すべての危険な権限リクエストの動作を制御します。リストで、、、または**** をクリックします。
  - **プロンプト:** ユーザーは危険な権限リクエストの許可または拒否を求められます。
  - **許可:** すべての危険な権限リクエストが許可されます。ユーザーにプロンプトは表示されません。
  - **拒否:** すべての危険な権限リクエストが拒否されます。ユーザーにプロンプトは表示されません。

  デフォルトは****です。
- アプリごとに、権限グループごと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、 をクリックします。 で、リスト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は、 をクリックし、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。 で、、、または**** を選択します。この許可状態はグローバル状態を上書きします。
  - **プロンプト:** ユーザーは、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ように求められます。
  - **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は許可されます。ユーザーにプロンプトは表示されません。

> **注:**

> **プロファイル所有者**モードで登録されているデバイスの場合、デバイスがAndroid 12以降で実行されている場合、カメラ、位置情報、マイク、センサーには**許可**権限は適用されません。

- **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は拒否されます。ユーザーに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。

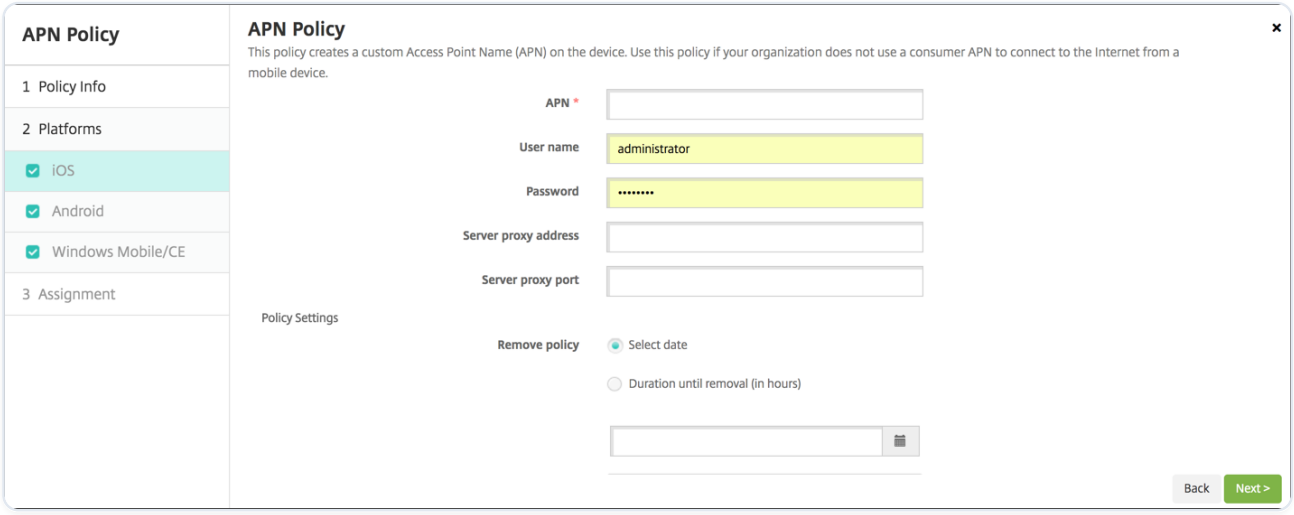
- アプリと許可状態の横にある**保存**をクリックします。
- 権限グループにアプリを追加するには、もう一度**追加**をクリックし、これらの手順を繰り返します。
- 必要なすべての権限グループの許可状態の設定が完了したら、**次へ**をクリックします。

APNデバイスポリシー

iOSおよびAndroidデバイス用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、組織がモバイルデバイスからインターネットに接続するために消費者向けAPNを使用しない場合に使用します。APNポリシーは、デバイスを特定の電話会社のGPRS（General Packet Radio Service）に接続するために使用される設定を決定します。この設定は、ほとんどの新しい電話で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、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

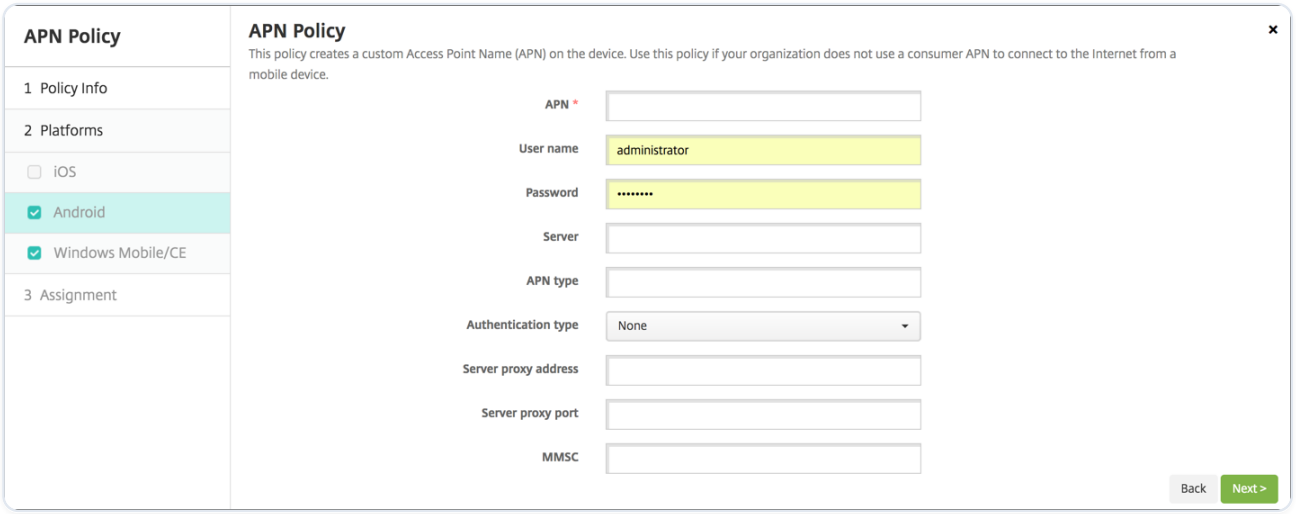
iOS設定



- **APN:** アクセスポイントの名前を入力します。このAPN名は、承認されたiOS APNと一致している必要があります。一致しない場合、ポリシーは失敗します。

- **ユーザー名:** この文字列は、このAPNのユーザー名を指定します。ユーザー名が指定されていない場合、プロファイルのインストール中にデバイスが文字列の入力を求めます。
- **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、プロファイルのインストール中にデバイスがパスワードの入力を求めます。
- **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。
- **サーバープロキシポート:** APNプロキシのポート番号。サーバープロキシアドレスを入力した場合、このサーバープロキシポート番号は必須です。
- で、 の横にある または のいずれかをクリックします。
  - をクリックした場合は、カレンダーをクリックして削除する特定の日付を選択します。
  - リストで、、、または をクリックします。
  - をクリックした場合は、 の横に必要なパスワードを入力します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択** と **削除までの期間 (時間)** です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

Android設定



- **APN:** アクセスポイントの名前を入力します。このAPN名は、承認されたAndroid APNと一致している必要があります。一致しない場合、ポリシーは失敗します。

- **ユーザー名:** この文字列は、このAPNのユーザー名を指定します。ユーザー名が指定されていない場合、プロファイルのインストール中にデバイスが文字列の入力を求めます。
- **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、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、プロファイルのインストール中にデバイスがパスワードの入力を求めます。
- **サーバー:** スマートフォンが登場する以前の設定であり、通常は空です。標準的なウェブサイトにアクセスできない可能性のある電話機向けに、Wireless Application Protocol (WAP) ゲートウェイサーバーを参照します。
- **APNタイプ:** この設定は、アクセスポイントに対するキャリアの意図する用途と一致している必要があります。これはAPNサービス指定子のコンマ区切り文字列であり、ワイヤレスキャリアが公開している定義と一致している必要があります。例を次に示します。
  - *: すべてのトラフィックがこのアクセスポイントを通過します。
  - 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通過します。
  - default: マルチメディアを含むすべてのトラフィックがこのアクセスポイントを通過します。
  - supl: セキュアユーザープレーンロケーションは、アシスト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キングは古く、めったに使用されません。
  - hipri" 高優先度ネットワーク。
  - fota: ファームウェア無線更新は、ファームウェアの更新を受信するために使用されます。
- **認証タイプ:** ドロップダウンリストで使用する認証タイプをクリックします。デフォルトは「なし」です。
- **サーバープロキシアドレス:** キャリアのAPN HTTPプロキシのIPアドレスまたはURL。
- **サーバープロキシポート:** APNプロキシのポート番号。サーバープロキシアドレスを入力した場合、このサーバープロキシポート番号は必須です。
- **MMSC:** キャリアによって提供されるMMSゲートウェイサーバーアドレス。
- **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、画像や動画などのマルチメディアコンテンツを含むより大きなメッセージを送信するためにSMSの後継となりました。これらのサーバーには、特定のプロトコル (MM1、... MM11など) が必要です。
- **MMSポート:** MMSプロキシに使用されるポート。

アプリケーションアクセスデバイスポリシー

XenMobile® のアプリケーションアクセスデバイスポリシーでは、以下を定義できます。

- デバイスにインストールする必要があるアプリのリスト。
- デバイスにインストールできるアプリのリスト。
- デバイスにインストールしてはならないアプリのリスト。

その後、アプリのリストに対するデバイスのコンプライアンスに対応する自動アクションを作成できます。iOS および Android デバイス用のアプリケーションアクセスポリシーを作成できます。

一度に構成できるアクセスポリシーは1種類のみです。必須アプリ、推奨アプリ、または許可されていないアプリのいずれかのリストに対してポリシーを追加できますが、同じアプリケーションアクセスポリシー内でこれらを混在させることはできません。各リストタイプに対してポリシーを作成する場合は、各ポリシーに慎重に名前を付けることをお勧めします。各ポリシーに慎重に名前を付けることで、XenMobile のどのポリシーがどのアプリのリストに適用されるかを把握できます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「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

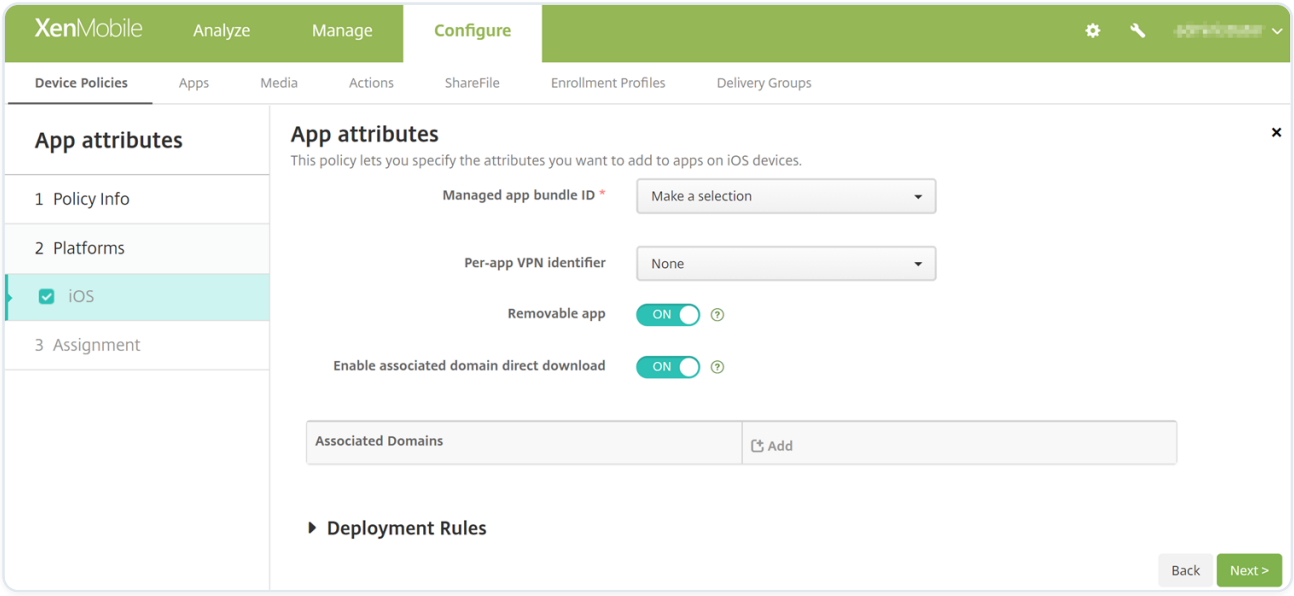
- **アクセスポリシー:** 、、または をクリックします。デフォルトは です。
- リストに1つ以上のアプリを追加するには、 をクリックし、次の操作を行います。
  - **アプリ名:** アプリ名を入力します。
  - **アプリ識別子:** オプションのアプリ識別子を入力します。
  - または をクリックします。
  - 追加するアプリごとにこれらの手順を繰り返します。

アプリ属性デバイスポリシー

アプリ属性デバイスポリシーを使用すると、iOSデバイスの管理対象アプリバンドルIDやアプリごとのVPN識別子などの属性を指定できます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **管理対象アプリバンドルID:** 次のいずれかの方法でアプリを指定します。
  - アプリバンドルIDを選択します。このオプションは、管理対象デバイス上のアプリのインベントリを収集する**アプリインベントリ**デバイスポリシーを有効にした後にのみ使用できます。
  - を選択し、アプリバンドルIDを入力します。 アプリバンドルIDを見つけるには、「App Storeでアプリのバンドルを見つける」を参照してください。
- **アプリごとのVPN識別子:** (オプション) このアプリのアプリごとのVPNを選択します。オプションには、**デバイスポリシー** > **VPNポリシー** ページで構成したアプリごとのVPN接続が含まれます。詳細については、「アプリごとのVPNを構成する」を参照してください。
- **削除可能なアプリ:** (オプション) 管理対象アプリである場合に、ユーザーがアプリを削除できるかどうかを指定します。ユーザーがアプリをアンインストールできないようにするには、このオプションを**に設定します。デフォルト値は**に設定されています。iOS 14以降で利用可能です。
- **関連ドメインの直接ダウンロードを有効にする:** (オプション) アプリがAppleのサーバーではなく、ドメインで直接、主張されたサイト関連付け検証を実行できるかどうかを指定します。このオプションは、インターネットにアクセスできないドメインに対してのみ**に設定します。デフォルト値は**に設定されています。iOS 14以降で利用可能です。
- **関連ドメイン:** (オプション) このアプリに関連ドメインを追加するには、 をクリックし、完全修飾ドメイン名 (FQDN) を入力します。iOS 13以降で利用可能です。

App Storeでアプリのバンドルを見つける

1. App Storeでアプリを見つけ、URLの末尾にある番号をコピーします。たとえば、363501921はCitrix Workspaceアプリのアプリです。
2. `https://itunes.apple.com/lookup?id=`にアクセスし、そのURLの後に番号を貼り付けます。TXTファイルが自動的にコンピューターにダウンロードされます。
3. TXTファイルで、`bundleId`を検索し、アプリのバンドルを取得します。例えば、Citrix Workspaceアプリのバンドルは`com.citrix.ReceiveriPad`です。

アプリ構成デバイスポリシー

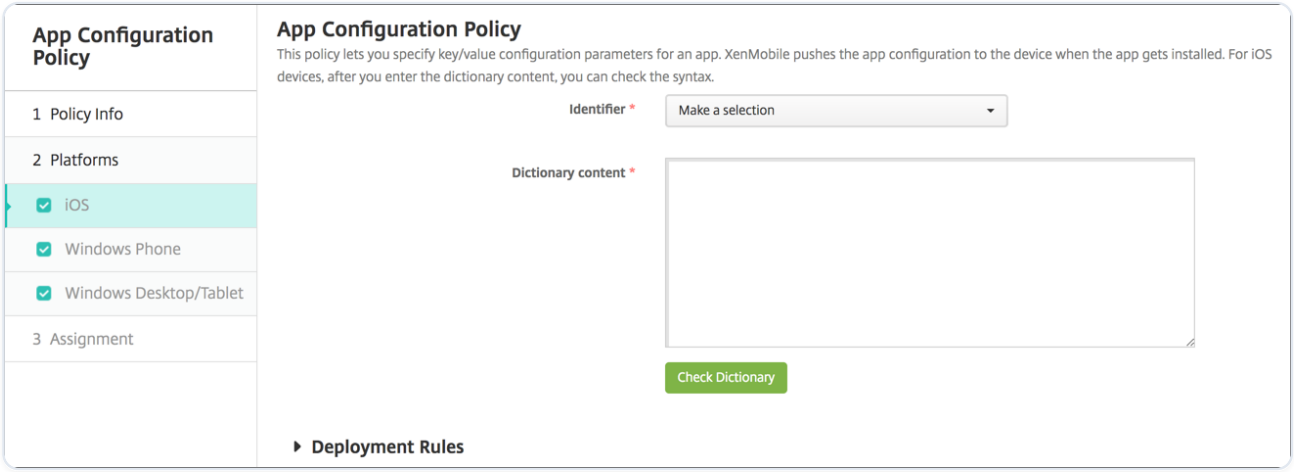
管理対象構成をサポートするアプリは、以下をデプロイすることでリモートから構成できます。

- iOSデバイスへのXML構成ファイル（プロパティリスト、またはplistと呼ばれる）
- または、Windows 10またはWindows 11を実行しているWindows 10の電話、タブレット、またはデスクトップデバイス用のキー/値ペア。

この構成では、アプリ内のさまざまな設定と動作を指定します。XenMobile®は、ユーザーがアプリをインストールするときに、構成をデバイスにプッシュします。構成できる実際の設定と動作はアプリによって異なり、この記事の範囲外です。

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。

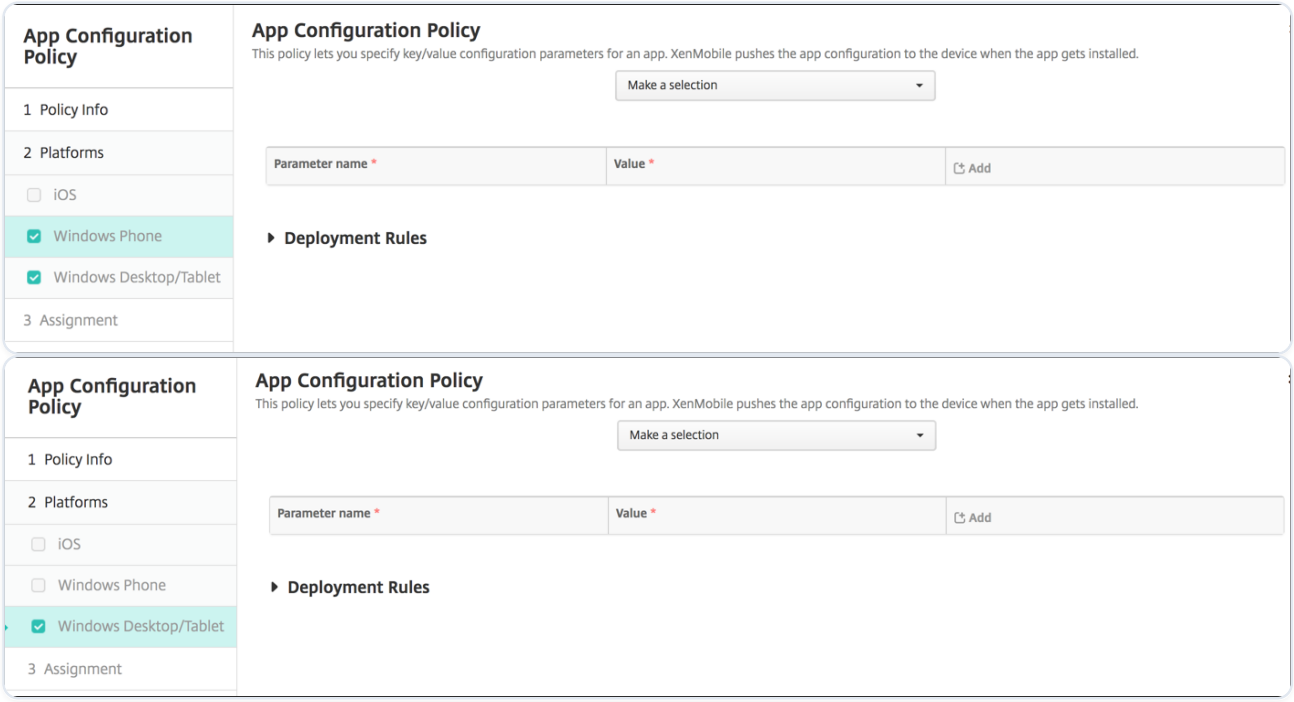
iOS設定



- **［識別子］**：構成するアプリをドロップダウンリストからクリックするか、**［新規追加］**をクリックしてアプリをリストに追加します。
  - **［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の識別子を入力します。

- **［辞書コンテンツ］**：XMLプロパティリスト（plist）の構成情報を入力するか、コピーして貼り付けます。
- **［辞書をチェック］をクリックします。XenMobileがXMLを検証します。エラーがない場合は、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構文エラーが表示された場合は、続行する前にそれらを修正する必要があります。

Windowsデスクトップ/タブレット設定



- 「**選択**」リストで、構成したいアプリをクリックするか、「**新規追加**」をクリックしてリストにアプリを追加します。
  - 「**新規追加**」をクリックした場合、表示されるフィールドにパッケージファミリー名を入力します。
- 追加したい構成パラメータごとに「**追加**」をクリックし、次の操作を行います。
  - 「**パラメータ名:**」 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のドキュメントを参照してください。
  - 「**値:**」 指定したパラメータの値を入力します。
  - パラメータを追加するには「**追加**」をクリックするか、パラメータの追加をキャンセルするには「**キャンセル**」をクリックします。

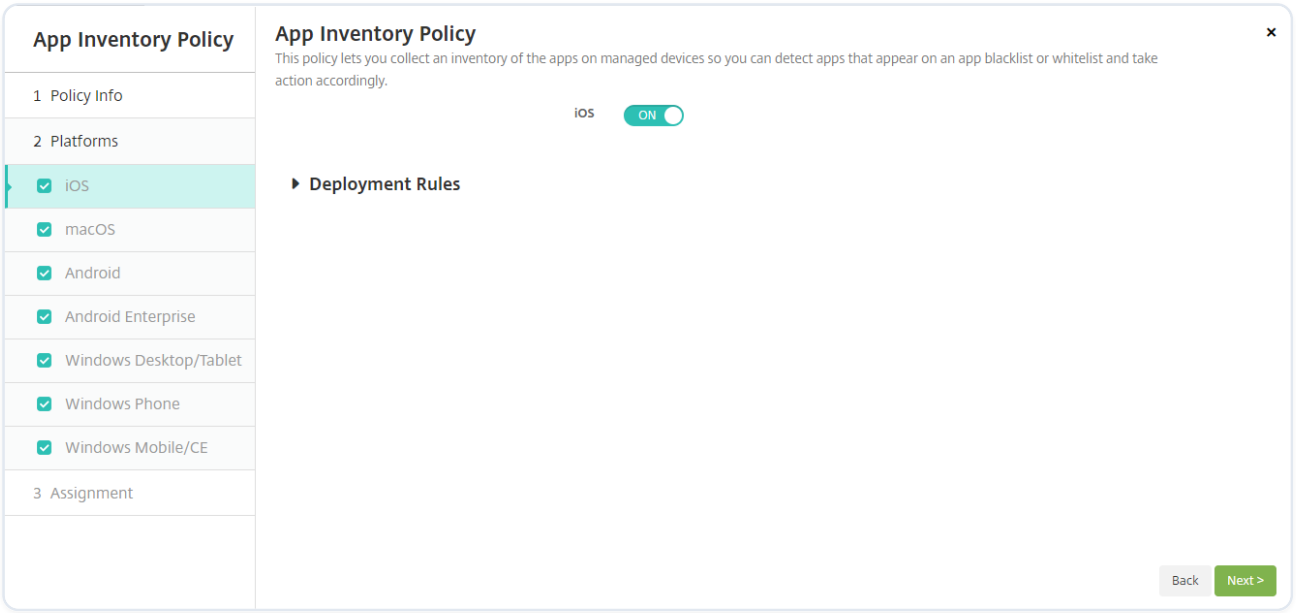
アプリインベントリデバイスポリシー

アプリインベントリポリシーを使用すると、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、そのインベントリをそれらのデバイスに展開されているアプリアクセスポリシーと比較できます。これにより、アプリの許可リストまたはブロックリストに表示されるアプリを検出し、適切に対処できます。

iOS、macOS、Android、Android Enterprise、または Windows のデスクトップおよびタブレット端末向けに、アプリケーションのアクセス制御ポリシーを作成できます。

このポリシーを追加または構成するには、 > に移動します。詳細については、「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



- 選択した各プラットフォームについて、デフォルト設定のままにするか、設定を に変更します。デフォルトは です。

アプリロックデバイスポリシー

アプリロックデバイスポリシーは、デバイスで実行を許可するアプリのリスト、またはデバイスでの実行をブロックするアプリのリストを定義します。このポリシーはiOSデバイスとAndroidデバイスの両方で構成できますが、ポリシーの動作方法はプラットフォームごとに異なります。たとえば、iOSデバイスで複数のアプリをブロックすることはできません。

同様に、iOSデバイスの場合、ポリシーごとに1つのiOSアプリしか選択できません。これは、ユーザーがデバイスを使用して単一のアプリのみを実行できることを意味します。アプリロックポリ

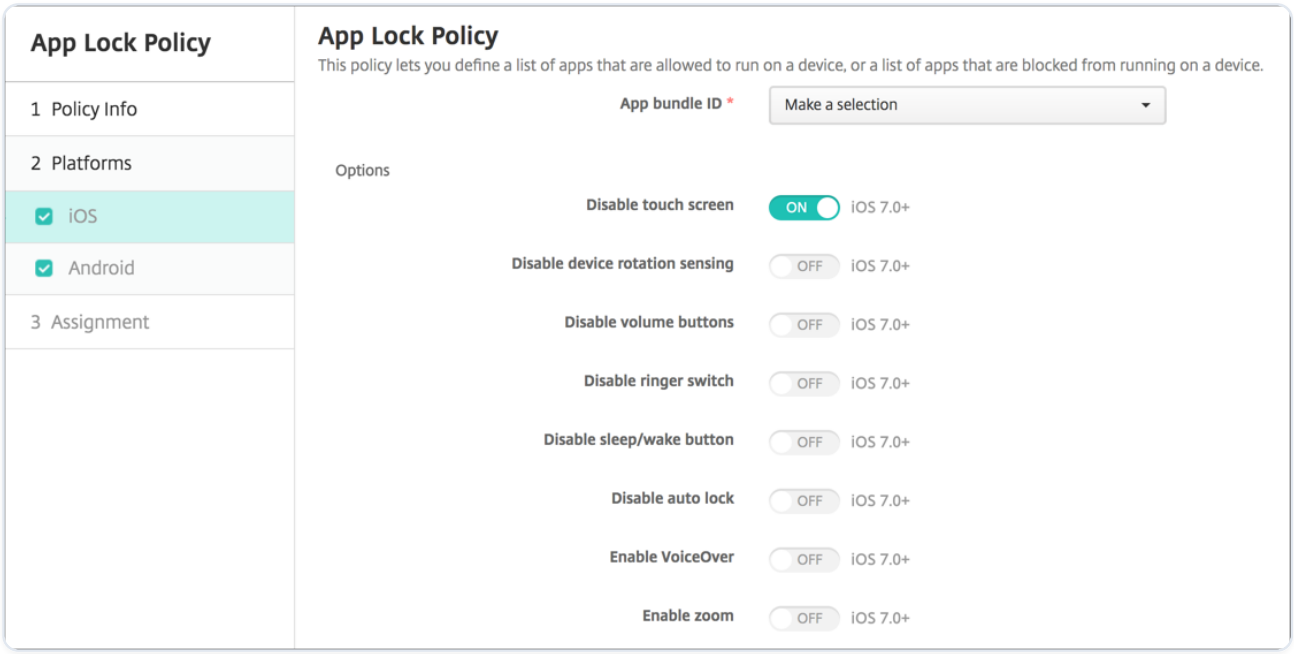
シーが適用されている間は、明示的に許可したオプションを除いて、デバイスで他のアクティビティを行うことはできません。

また、アプリロックポリシーをプッシュするには、iOSデバイスが監視されている必要があります。

このデバイスポリシーはほとんどのAndroid LおよびMデバイスで機能しますが、Googleが必要なAPIを非推奨にしたため、Android N以降のデバイスではアプリロックは機能しません。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS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ドロップダウンリストからクリックするか、 をクリックしてリストにアプリを追加します。 を選択した場合は、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。各オプションのデフォルトは**オフ**ですが、タッチスクリーンを無効にするオプションのみデフォルトが**オン**です。
  - タッチスクリーンを無効にする
  - デバイスの回転感知を無効にする
  - 音量ボタンを無効にする
  - 着信/サイレントスイッチを無効にする

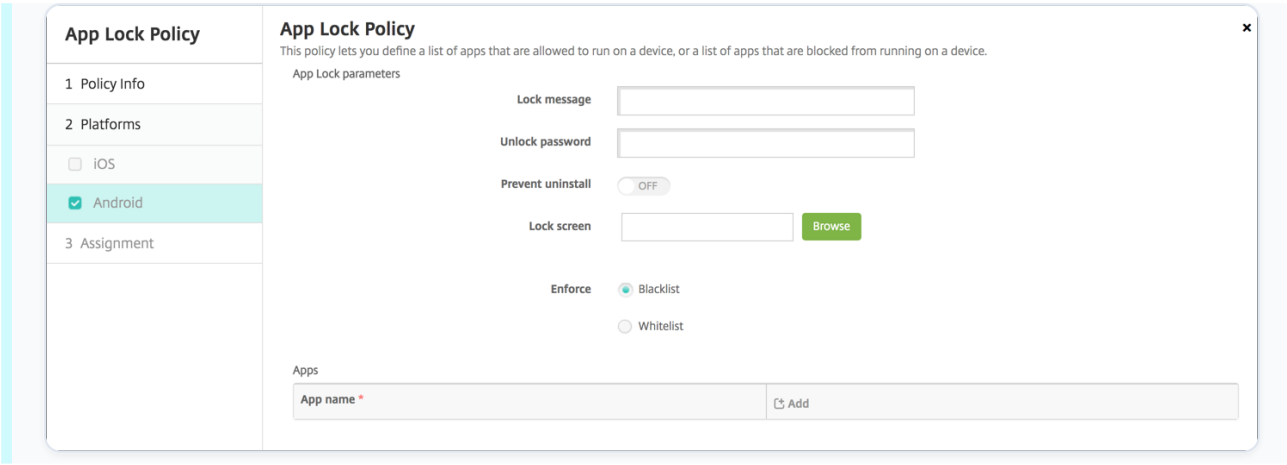
着信/サイレントスイッチを無効にするオプションが**オン**の場合、着信音の動作は、最初に無効になったときにスイッチがどの位置にあったかによって異なります。

- スリープ/スリープ解除ボタンを無効にする
- 自動ロックを無効にする
- VoiceOverを無効にする
- ズームを有効にする
- 色の反転を有効にする
- AssistiveTouchを有効にする
- 選択項目の読み上げを有効にする
- モノラルオーディオを有効にする

- **ユーザー有効オプション:** 以下の各オプションは、iOS 7.0以降にのみ適用されます。各オプションのデフォルトは**オフ**です。
  - VoiceOverの調整を許可する
  - ズーム調整を許可する
  - 色の反転調整を許可する
  - AssistiveTouchの調整を許可する
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

Android設定

> **注:**
>
> App Lockデバイスポリシーを使用して、Android設定アプリをブロックすることはできません。



- **App Lockパラメーター**
  - **ロックメッセージ:** ロックされたアプリを開こうとしたときにユーザーに表示されるメッセージを入力します。
  - **ロック解除パスワード:** アプリのロックを解除するためのパスワードを入力します。
  - **アンインストールを防止:** ユーザーがアプリをアンインストール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。
  - **ロック画面:** 参照をクリックしてファイルの場所に移動し、デバイスのロック画面に表示される画像を選択します。
  - **適用:** デバイスで実行が許可されないアプリのリストを作成するには**ブラックリスト**を、デバイスで実行が許可されるアプリのリストを作成するには**ホワイトリスト**をクリックします。

    > **注:**
    >
    > XenMobile® Serverコンソールには、「blacklist」および「whitelist」という用語が含まれています。今後のバージョンでは、これらの用語を「block list」および「allow list」に変更する予定です。

- **アプリ: 追加**をクリックし、次の操作を行います。
  - **アプリ名:** ドロップダウンリストからアプリ名をクリックして、許可リストまたはブロックリストに追加します。または、**新規追加**をクリックして、利用可能なアプリのリストにアプリを追加します。
  - **新規追加**を選択した場合、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。

- 許可リストまたはブロックリストに追加する各アプリについて、これらの手順を繰り返します。

アプリのネットワーク使用状況デバイスポリシー

iOSデバイスで、管理対象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かを指定するネットワーク使用状況ルールを設定できます。このルールは管理対象アプリにのみ適用されます。管理対象アプリとは、XenMobileを介してユーザーのデバイスに展開するアプリのことです。XenMobileを介さずにユーザーがデバイスに直接ダウンロードしたアプリや、デバイスがXenMobileに登録されたときにすでにデバイスにインストールされていたアプリは含まれません。

このポリシーを追加または構成するには、 > の順に進みます。詳しくは、「デバイスポリシー」を参照してください。

iOS設定

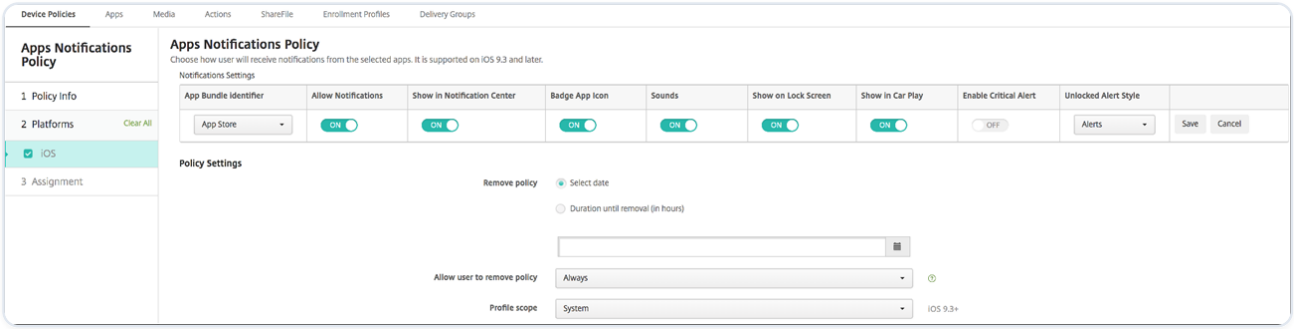
- : 指定したアプリがローミング中に携帯データ通信接続を使用できるかどうかを選択します。デフォルトは です。
- : 指定したアプリが携帯データ通信接続を使用できるかどうかを選択します。デフォルトは です。
- : リストに追加する各アプリについて、 をクリックしてから、次の操作を行います。
  - : アプリ識別子を入力します。
  - アプリをリストに保存するには をクリックし、保存しない場合は をクリックします。

アプリ通知デバイスポリシー

アプリ通知ポリシーを使用すると、iOSユーザーが指定され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、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **アプリバンドル識別子:** 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、 を選択します。
- **通知センターに表示:** ユーザーデバイスの通知センターに通知を表示するには、 を選択します。
- **バッジアプリアイコン:** 通知とともにバッジアプリアイコンを表示するには、 を選択します。
- **サウンド:** 通知にサウンドを含めるには、 を選択します。
- **ロック画面に表示:** ユーザーデバイスのロック画面に通知を表示するには、 を選択します。
- **CarPlayに表示:** の場合、通知はApple CarPlayに表示されます。iOS 12以降で利用可能です。デフォルトは****です。
- **重大なアラートを有効にする:** の場合、アプリは通知を「おやすみモード」や着信音設定を無視する重大な通知としてマークできます。iOS 12以降で利用可能です。デフォルトは****です。
- **ロック解除時のアラートスタイル:** リストから**、、**または**を選択して、ロック解除時のアラートの外観を構成します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**システム**です。このオプションはiOS 9.3以降でのみ利用可能です。

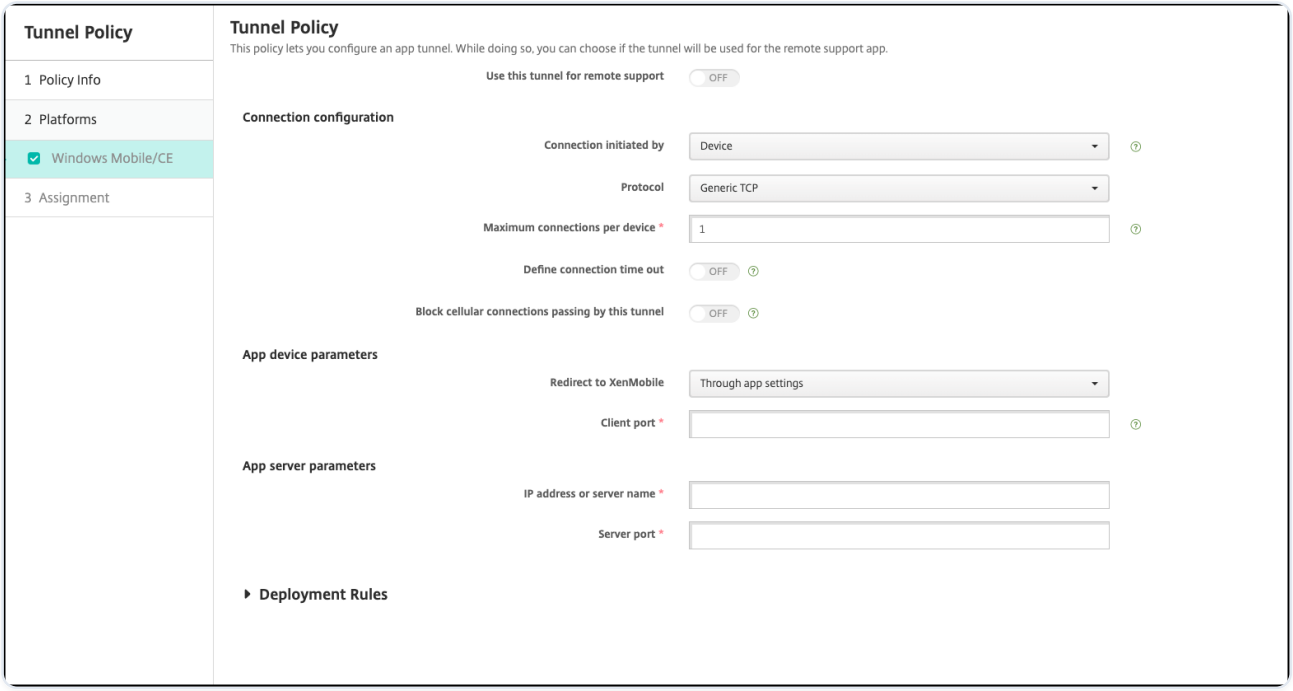
トンネルデバイスポリシー

アプリケーショントンネル（アプリトンネル）は、モバイルアプリのサービス継続性と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。Androidデバイスのトンネルポリシーを構成できます。

このポリシーで定義したトンネルを介して送信されるアプリトラフィックはすべて、アプリを実行しているサーバーにリダイレクトされる前にXenMobile®を通過します。

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



- **接続の開始元：** 接続を開始するソースを指定するには、**［デバイス］または［サーバー］**をクリックします。
- **デバイスあたりの最大接続数：** アプリが確立できる同時TCP接続の数を指定する数値を入力します。このフィールドは、デバイスが開始する接続にのみ適用されます。
- **接続タイムアウトの定義：** トンネルが閉じられるまでにアプリがアイドル状態になる時間を設定するかどうかを選択します。
    - **接続タイムアウト：** **［接続タイムアウトの定義］を［オン］**に設定した場合、トンネルが閉じられるまでにアプリがアイドル状態になる時間を秒単位で入力します。

- **このトンネルを通過する携帯電話接続をブロック：** ローミング中にこのトンネルをブロックするかどうかを選択します。Wi-FiおよびUSB接続はブロックされません。
- **XenMobileにリダイレクト：** **［アプリ設定経由］**を選択します。
- **クライアントポート：** クライアントポート番号を入力します。通常、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、デバイスが開始する接続にのみ適用されます。
- **サーバーポート：** サーバーポート番号を入力します。

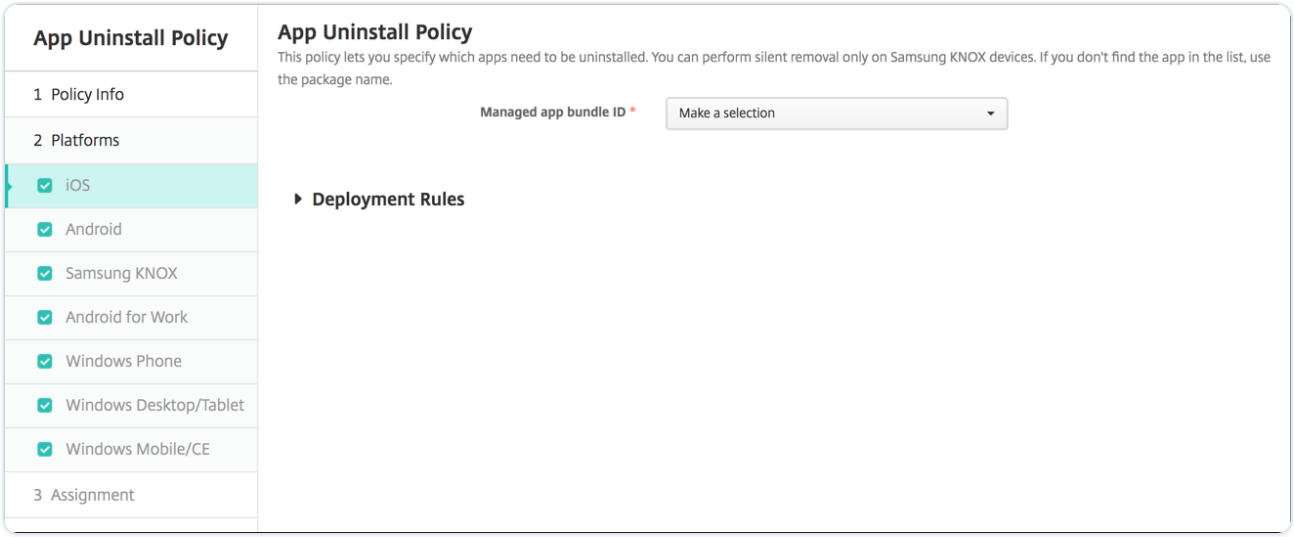
アプリのアンインストールデバイスポリシー

iOS、Android、Samsung Knox、Android Enterprise、Windowsデスクトップ/タブレットプラットフォーム向けに、アプリのアンインストールポリシーを作成できます。アプリのアンインストールポリシーを使用すると、さまざまな理由でユーザーデバイスからアプリを削除できます。例えば、特定のアプリのサポートを終了したい場合や、会社が既存のアプリを異なるベンダーの類似アプリに置き換えたい場合など、さまざまな理由が考えられます。

このポリシーがユーザーデバイスに展開されると、アプリが削除されます。Samsung Knoxデバイスを除き、ユーザーにはアプリをアンインストールするよう求めるプロンプトが表示されます。Samsung Knoxデバイスのユーザーには、アプリをアンインストールするよう求めるプロンプトは表示されません。

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設定



- **管理対象アプリのバンドルID：** ドロップダウンリストから既存のアプリをクリックするか、**［新規追加］**をクリックします。このプラットフォーム用に構成されたアプリがない場合、リストは空になり、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。

その他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：** 追加するアプリごとに、**［追加］**をクリックしてから、次の操作を行います。
    - **アプリ名：** ドロップダウンリストから既存のアプリをクリックするか、**［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用に構成されたアプリがない場合、リストは空になり、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キャンセルします。

対応するパブリックアプリストアアプリのインストール後にエンタープライズアプリを自動的にアンインストールする

パブリックアプリストア版のCitrix®アプリがインストールされたときに、XenMobile®がエンタープライズ版を削除するように構成できます。この機能により、パブリックアプリストア版がインストールされた後、ユーザーデバイスに2つの同じアプリアイコンが表示されるのを防ぎます。

アプリのアンインストールデバイスポリシーの展開条件により、新しいバージョンがインストールされたときに、XenMobileがユーザーデバイスから古いアプリを削除するようトリガーされます。この機能は、エンタープライズモード（XME）のXenMobile Serverに接続されている管理対象iOSデバイスでのみ利用できます。

「インストール済みアプリ名」条件で展開ルールを構成するには：

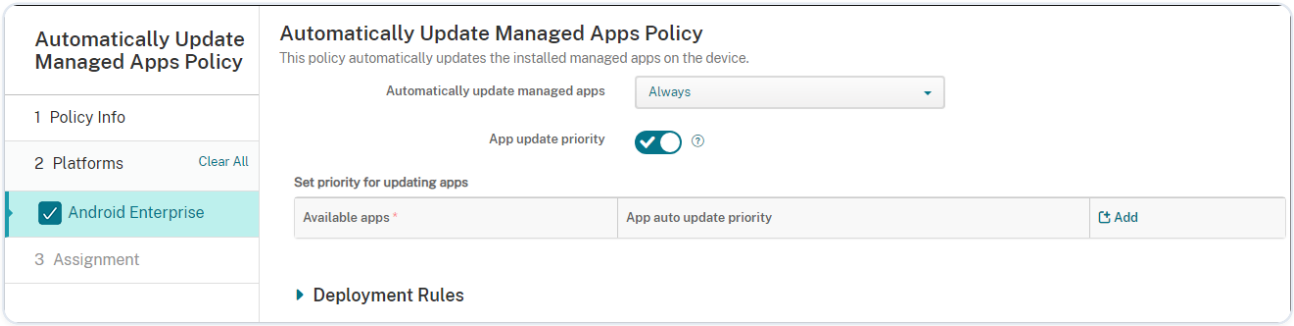
- Enterpriseアプリの**管理対象アプリバンドルID**を指定します。
- ルールを追加します。**新規ルール**をクリックし、サンプルに示すように、**インストール済みアプリ名**と**次と等しい**を選択します。パブリックアプリストアアプリのアプリバンドルIDを入力します。

この例では、指定されたデリバリーグループ内のデバイスにパブリックアプリストアアプリ (com.citrix.mail.ios) がインストールされると、XenMobileはEnterpriseバージョン (com.citrix.mail) を削除します。

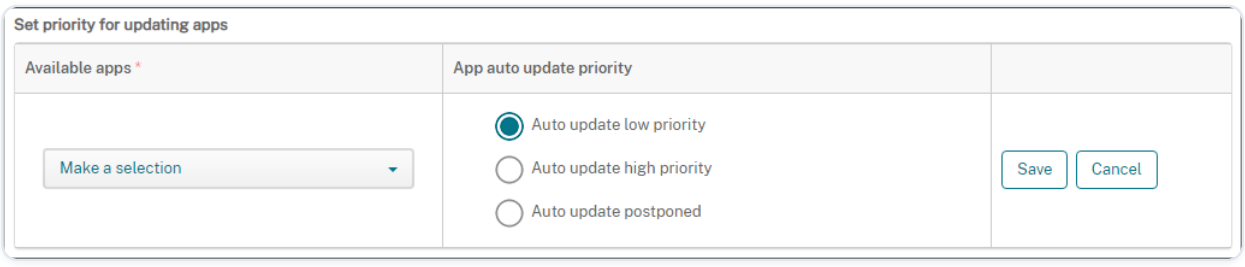
管理対象アプリの自動更新デバイスポリシー

このポリシーは、Android Enterpriseデバイスにインストールされている管理対象アプリがどのように更新されるかを制御します。ユーザーがデバイス上のアプリの自動更新を許可する機能を制限できます。ユーザーがデバイス上のアプリの自動更新を制御できるようにする場合、ユーザーは管理対象のGoogle Playストアで自動アプリ更新ポリシーを設定します。

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**に移動します。詳細については、デバイスポリシーを参照してください。



- **管理対象アプリを自動更新**
  - **常に:** アプリの自動更新を有効にします。**常に**がデフォルトです。
  - **ユーザーにポリシーの構成を許可:** ユーザーが管理対象のGoogle Playストアでデバイスの自動アプリ更新ポリシーを構成できるようにします。
  - **しない:** アプリの自動更新を無効にします。
  - **デバイスがWi-Fiに接続されている場合のみ:** デバイスがWi-Fiに接続されている場合にのみ、アプリの自動更新を許可します。
- **アプリの更新優先度: オン**の場合、各管理対象アプリの更新優先度レベルを構成できます。
- **アプリの更新優先度を設定: 追加**をクリックして、アプリの更新優先度を構成します。



- **利用可能なアプリ:** メニューからアプリを選択して、更新優先度を構成します。
- **アプリの自動更新優先度:** 次の中から更新優先度を選択します。
  - **自動更新低優先度:** デバイスが充電中で、アクティブに使用されておらず、従量制ではないネットワークに接続されている場合にアプリを更新します。

- **自動更新（高優先度）：**アプリは制約なしに、できるだけ早く更新されます。
- **自動更新（延期）：**新しいバージョンが利用可能になってから最大90日間、アプリは自動的に更新されません。90日後、アプリは低優先度で自動的に更新されます。アプリが更新された後、さらに90日間は自動的に更新されません。ユーザーはいつでも手動でアプリを更新できます。

- 完了したら、**保存**をクリックします。鉛筆アイコンをクリックして構成を編集できます。ゴミ箱アイコンをクリックして構成を削除します。

BitLocker デバイスポリシー

Windows 10およびWindows 11には、BitLockerと呼ばれるディスク暗号化機能が含まれており、紛失または盗難されたWindowsデバイスへの不正アクセスからファイルとシステムを保護します。さらに保護を強化するには、BitLockerをTrusted Platform Module (TPM) チップバージョン1.2以降と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、暗号化キーを生成、保存、および使用を制限します。

Windows 10ビルド1703以降、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およびWindows 11デバイスのBitLockerウィザードで利用可能な設定を構成します。たとえば、BitLockerが有効になっているデバイスでは、BitLockerは起動時にドライブのロックを解除する方法、回復キーをバックアップする方法、固定ドライブのロックを解除する方法をユーザーに尋ねることができます。BitLockerデバイスポリシー設定では、以下の項目も構成します。

- TPMチップのないデバイスでBitLockerを有効にする。
- BitLockerインターフェイスで回復オプションを表示する。
- BitLockerが有効になっていない場合に、固定ドライブまたはリムーバブルドライブへの書き込みアクセスを拒否する。

> **注：**

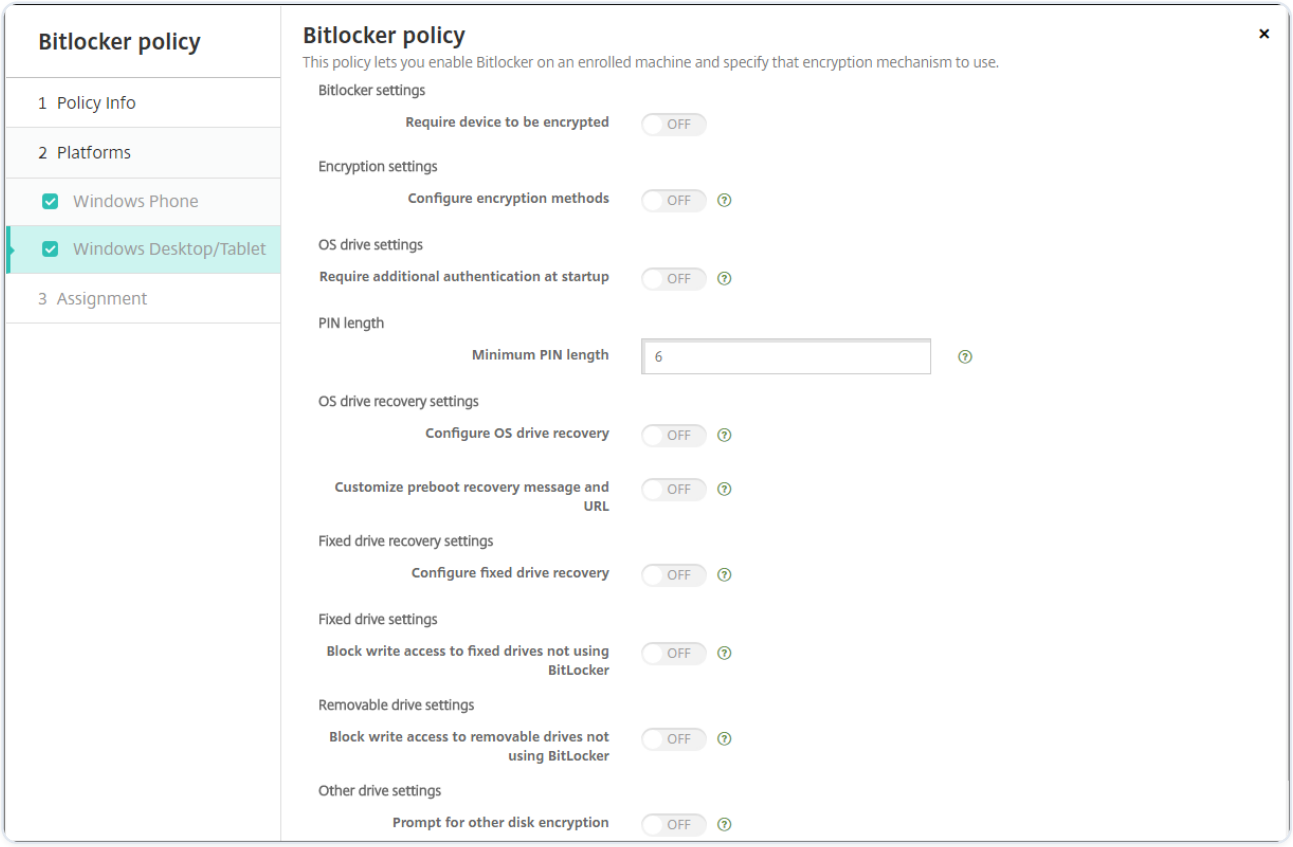
> デバイスでBitLocker暗号化が開始された後、更新されたBitLockerデバイスポリシーを展開しても、後からデバイスのBitLocker設定を変更することはできません。

> 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。

要件

- BitLockerデバイスポリシーには、Windows 10またはWindows 11 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を使用するための環境を準備してください。BitLockerのシステム要件やセットアップなど、Microsoftからの詳細情報については、「BitLocker」とそのノード配下の記事を参照してください。

Windowsデスクトップおよびタブレットの設定



- **デバイスの暗号化を必須にする：** Windowsデスクトップまたはタブレットで**BitLocker**暗号化を有効にするようユーザーに促すかどうかを決定します。**［オン］の場合、登録完了後にデバイスに、企業がデバイスの暗号化を要求していることを示すメッセージが表示されます。［オフ］の場合、ユーザーにプロンプトは表示されず、BitLockerはポリシー設定を使用します。デフォルトは**［オフ］**です。
- **暗号化方法の構成:** 特定のドライブタイプに使用する暗号化方法を決定します。**オフ**の場合、BitLockerウィザードは、ドライブタイプに使用する暗号化方法をユーザーに求めます。すべてのドライブの暗号化方法はデフォルトでXTS-AES 128ビットになります。リムーバブルドライブの暗号化方法はデフォルトでAES-CBC 128ビットになります。**オン**の場合、BitLockerはポリシーで指定された暗号化方法を使用します。**オン**の場合、**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**の追加設定が表示されます。各ドライブタイプのデフォルトの暗号化方法を選択します。デフォルトは**オフ**です。

- **起動時に追加認証を要求:** デバイスの起動時に必要な追加認証を指定します。また、TPMチップを搭載し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を搭載していないデバイスはBitLocker暗号化を使用できません。TPMの詳細については、Microsoftの記事「Trusted Platform Module Technology Overview」を参照してください。**オン**の場合、以下の追加設定が表示されます。デフォルトは**オフ**です。
  - **TPMチップなしのデバイスでBitLockerをブロック:** TPMチップのないデバイスでは、BitLockerはユーザーにロック解除パスワードまたはスタートアップキーの作成を要求します。スタートアップキーはUSBドライブに保存され、ユーザーは起動前にデバイスに接続する必要があります。ロック解除パスワードは最低8文字です。デフォルトは**オフ**です。
  - **TPMスタートアップ:** TPMを搭載したデバイスには、TPMのみ、TPM + PIN、TPM + キー、TPM + PIN + 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TPMのみのモードで、暗号化キーはTPMチップに保存されます。このモードでは、ユーザーが追加のロック解除データを提供する必要はありません。ユーザーデバイスは、TPMチップからの暗号化キーを使用して、再起動時に自動的にロック解除されます。デフォルトは**TPMを許可**です。
  - **TPMスタートアップPIN:** この設定はTPM + PINロック解除モードです。PINは最大20桁まで設定できます。**最小PIN長**設定を使用して、最小PIN長を指定します。ユーザーはBitLockerセットアップ中にPINを設定し、デバイス起動時にPINを提供します。
  - **TPMスタートアップキー:** この設定はTPM + キーロック解除モードです。スタートアップキーはUSBまたはその他のリムーバブルドライブに保存され、ユーザーは起動前に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 + PIN + キーロック解除モードです。

    ロック解除が成功すると、オペレーティングシステムがロードを開始します。ロック解除が失敗すると、デバイスは回復モードに入ります。
- **最小PIN長:** TPMスタートアップPINの最小長。デフォルトは**6**です。
- **OSドライブ回復の構成:** ロック解除手順が失敗した場合、BitLockerは構成された回復キーをユーザーに求めます。この設定は、ロック解除パスワードまたはUSBスタートアップキーを持っていない場合にユーザーが利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。
  - **証明書ベースのデータ回復エージェントを許可:** 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にある公開キーポリシーから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の詳細については、Microsoftの記事「BitLocker Group Policy settings」を参照してください。デフォルトは**オフ**です。

- **OSドライブ回復用に48ビット回復パスワードを作成:** ユーザーが回復パスワードを使用することを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**です。
- **256ビット回復キーを作成:** ユーザーが回復キーを使用することを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ビット回復キーを許可**です。
- **OSドライブ回復オプションを非表示:** BitLockerインターフェイスで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**の場合、BitLockerインターフェイスには回復オプションが表示されません。その場合、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、**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 Domain Services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に保存される回復情報を構成する:** BitLocker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 Domain Services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データを回復できます。デフォルトは**回復パスワードのバックアップ**です。
- **AD DSに回復情報を保存した後にBitLockerを有効にする:** デバイスがドメインに接続されており、BitLocker回復情報のActive Directoryへのバックアップが成功しない限り、ユーザーがBitLockerを有効にできないようにするかどうかを指定します。**オン**の場合、BitLockerを開始する前にデバイスがドメインに参加している必要があります。デフォルトは**オフ**です。

- **プレブート回復メッセージとURLをカスタマイズする:** BitLockerが回復画面に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**の場合、次の追加設定が表示されます: **デフォルトの回復メッセージとURLを使用する、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。オフ**の場合、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のユーザーへ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。起動中にドライブのロックを解除するには、ユーザーはパスワードまたはスマートカードを提供します。このポリシーには含まれていない起動時のロック解除設定は、ユーザーが固定ドライブでBitLocker暗号化を有効にしたときにBitLockerインターフェイスに表示されます。関連設定については、このリストの前の**OSドライブの回復を構成する**を参照してください。デフォルトは**オフ**です。

- **BitLockerを使用してい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**の場合、ユーザーはBitLockerで暗号化されている場合にのみ固定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を使用してい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**の場合、ユーザーはBitLockerで暗号化されている場合にのみリムーバブルドライブに書き込むことができます。この設定は、組織が他の組織のリムーバブルドライブへの書き込みアクセスを許可するかどうかに応じて構成してください。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:** デバイス上の他のディスク暗号化に関する警告プロンプトを無効にできます。デフォルトは**オフ**です。

カレンダー (CalDAV) デバイスポリシー

XenMobile® でデバイスポリシーを追加すると、ユーザーの iOS または macOS デバイスにカレンダー (CalDAV) アカウントを追加して、CalDAV をサポートする任意のサーバーとスケジュールデータを同期できるようになります。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS 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 サーバーに接続する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へのベース 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:** オプションのユーザーパスワードを入力します。
- **SSL の使用:** CalDAV サーバーへの 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。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。

    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0 以降でのみ利用可能です。

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サーバーに接続する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へのベース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:** オプションのユーザーパスワードを入力します。
- **SSLを使用:** CalDAVサーバーへの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。
- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
        - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
        - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。
    - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
    - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

携帯デバイスポリシー

このポリシーを使用すると、iOSデバイスで携帯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設定

- **APNをアタッチ**
  - **名前：** この構成の名前。
  - **認証の種類：** ドロップダウンリストで、Challenge Handshake Authentication Protocol（**CHAP**）またはPassword Authentication Protocol（**PAP**）をクリックします。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。
- **APN**
  - **名前：** アクセスポイント名（APN）構成の名前。
  - **認証の種類：** ドロップダウンリストで**CHAP**または**PAP**をクリックします。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。
  - **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。
  - **プロキシサーバーポート：** プロキシサーバーのポート。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

接続スケジューリングデバイスポリシー

> **重要:**

> Citrixでは、Android、Android Enterprise、およびChrome OSデバイスからXenMobile Serverへの接続を制御するために、Firebase Cloud Messaging (FCM)を使用することをお勧めします。FCMの使用方法については、「Firebase Cloud Messaging」を参照してください。

> FCMを使用しないことを選択した場合、ユーザーデバイスがXenMobile® Serverに接続する方法とタイミングを制御する接続スケジューリングポリシーを作成できます。

ユーザーがデバイスを手動で接続するか、デバイスが定義された時間枠内で接続するように指定できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「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

- **デバイスの接続を要求:** このスケジュールに設定するオプションをクリックします。
    - **常時:** 接続を永続的に維持します。ユーザーデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobile Serverへの再接続を試み、定期的に制御パケットを送信して接続を監視します。Citrix®は、セキュリティを最適化するためにこのオプションを推奨します。**常時**を選択する場合は、デバイスの**トンネルポリシー**で**接続タイムアウトの定義**設定も使用して、接続がバッテリーを消耗しないようにしてください。接続を維持することで、ワイプやロックなどのセキュリティコマンドをオンデマンドでデバイスにプッシュできます。また、デバイスに展開される各ポリシーで、**展開スケジュール**オプションの**常時接続用に展開**を選択する必要があります。
    - **しない:** 手動で接続します。ユーザーはデバイス上のXenMobileから接続を開始する必要があります。このオプションは、デバイスへのセキュリティポリシーの展開を妨げ、ユーザーが新しいアプリやポリシーを受け取ることができなくなるため、Citrixは本番環境での展開には推奨しません。
    - **毎回:** 指定された間隔で接続します。このオプションが有効なときに、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、デバイスが次回接続するときにXenMobileがデバイス上でそのアクションを処理します。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、デバイスが再接続するまでの分数（N）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、ユーザーデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobile Serverへの再接続を試み、定義した時間枠内で定期的に制御パケットを送信して接続を監視します。接続時間枠の定義方法については、次の「接続時間枠の定義」を参照してください。
        - **これらの時間帯は永続的な接続を維持:** ユーザーのデバイスは、定義された時間枠内で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:** ユーザーのデバイスは、定義された時間枠のいずれかで少なくとも1回接続されている必要があります。
        - **UTCではなくローカルデバイス時間を使用:** 定義された時間枠を協定世界時 (UTC) ではなく、ローカルデバイス時間に同期します。

接続時間枠の定義

以下のオプションを有効にすると、希望する時間枠を定義できるタイムラインが表示されます。特定の時間帯に永続的な接続を要求するため、または特定の時間枠内で接続を要求するために、いずれかまたは両方のオプションを有効にできます。タイムラインの各マスは30分なので、平日の午前8時から午前9時の間に接続したい場合は、タイムライン上の平日の午前8時から午前9時の間の2つのマスをクリックします。

たとえば、次の図の2つのタイムラインでは、平日の午前8時から午前9時の間の永続的な接続、土曜日の午前0時から日曜日の午前1時の間の永続的な接続、および平日の午前5時から午前8時の間または午前10時から午後11時の間の少なくとも1つの接続が必要です。

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-scheduling-define-schedule.png)

連絡先 (CardDAV) デバイスポリシー

XenMobile® でデバイスポリシーを追加して、ユーザーの iOS または macOS デバイスに iOS 連絡先 (CardDAV) アカウントを追加し、CardDAV をサポートする任意のサーバーと連絡先データを同期できるようにします。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS 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 サーバーに接続する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へのベース 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:** オプションのユーザーパスワードを入力します。
- **SSL を使用:** CardDAV サーバーへの 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。
- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。

    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0 以降でのみ利用可能です。

macOS 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 サーバーに接続する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へのベース 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:** オプションのユーザーパスワードを入力します。
- **SSL を使用:** CardDAV サーバーへの 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。
- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択** と **削除までの期間 (時間)** です。
        - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
        - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
    - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから **常に**、**パスコードが必要**、または **なし** を選択します。**パスコードが必要** を選択した場合は、**削除パスコード** フィールドにパスコードを入力します。
    - **プロファイルスコープ:** このポリシーを **ユーザー** に適用するか、**システム** 全体に適用するかを選択します。デフォルトは **ユーザー** です。このオプションは macOS 10.7 以降でのみ利用可能です。

OSアップデート制御デバイスポリシー

OSアップデート制御デバイスポリシーでは、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アップデート。

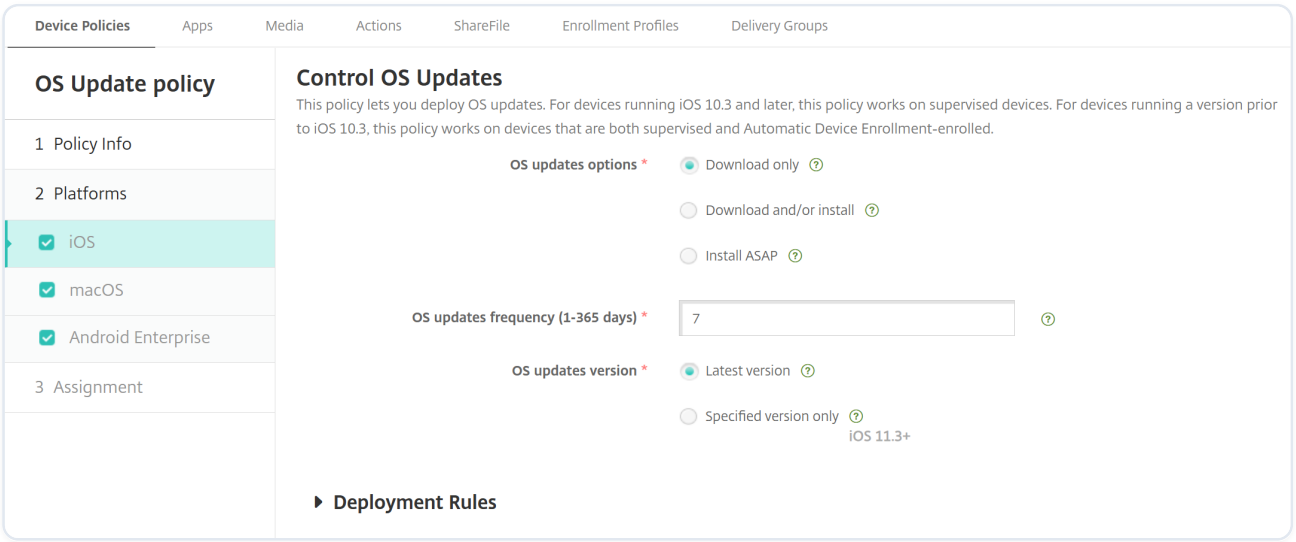
OSアップデートデバイスポリシーは、Apple Deployment Programに登録されている監視対象デバイスでのみ機能します。

- 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およびアプリのアップデート。
- Android Enterprise Work Managedデバイスへの最新のOSアップデート。

  Android Enterprise Work Managedデバイスの場合、XenMobile®はOSアップデート制御ポリシーをSecure Hubに送信し、Secure Hubがその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がポリシーを送信した日時と、デバイスがポリシーを受信した日時が表示されます。

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**に移動します。詳細については、「デバイスポリシー」を参照してください。

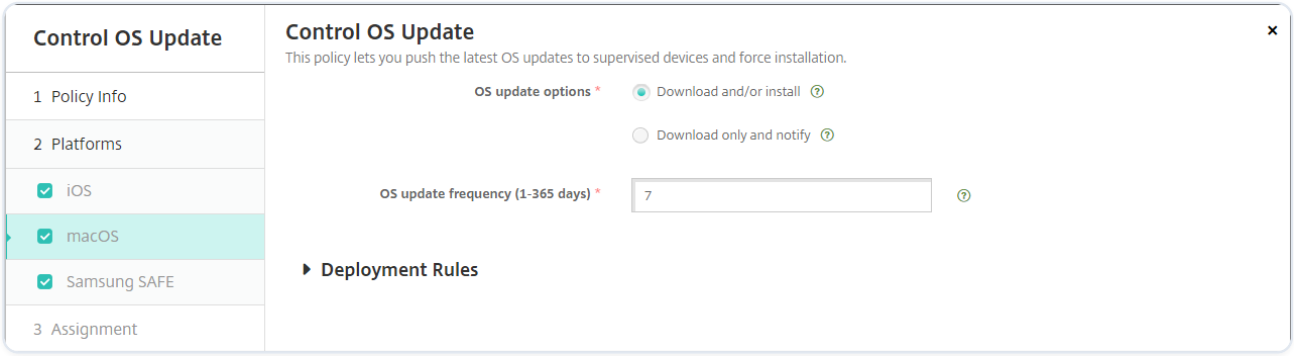
iOS設定



- **OSアップデートオプション:**
  - **ダウンロードのみ:** OSアップデートの頻度に従って、最新のOSアップデートを監視対象デバイスにダウンロードしますが、インストールはしません。
  - **ダウンロードおよび/またはインストール:** OSアップデートの頻度に従って、最新のOSアップデートを監視対象デバイスにダウンロードします。デバイスはアップデートのインストールを促します。プロンプトはデバイスのロックを解除した後に表示されます。
  - **できるだけ早くインストール:** 以前にダウンロードしたOSアップデートをすぐにインストールできます。
- **OSアップデートの頻度:** XenMobileがデバイスOSをチェックおよびアップデートする頻度を決定します。デフォルトは**7**日です。

- **OS updates version:** 監視対象のiOSデバイスを更新するために使用するOSバージョンを指定します。デフォルトは**最新バージョン**です。
  - **最新バージョン:** 最新のOSバージョンに更新するには、これを選択します。
  - **特定のバージョンのみ:** 特定のOSバージョンに更新するには、これを選択し、バージョン番号を入力します。このオプションはiOS 11.3以降に適用されます。

macOS設定



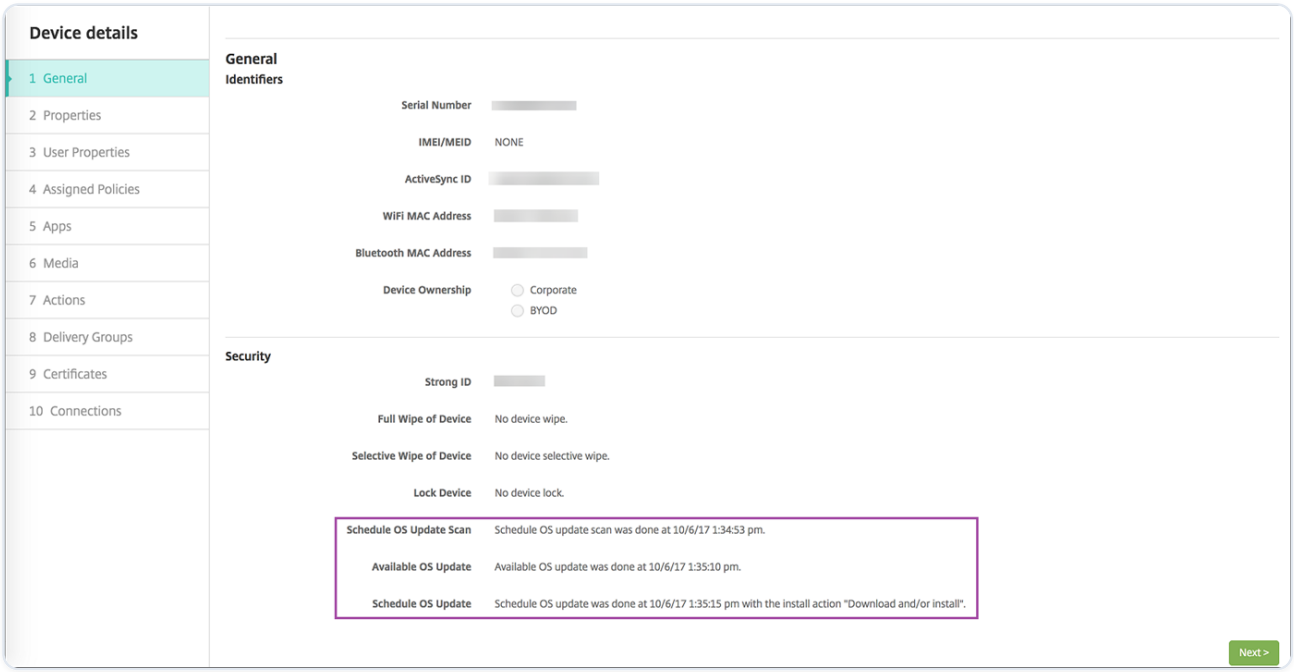
- **OS update options:** どちらのオプションも、**OS update frequency**に従って最新のmacOSアップデートをダウンロードします。アップデートをインストールするか、App Storeを通じてユーザーにアップデートが利用可能であることを通知するかを選択できます。
- **OS update frequency:** XenMobileがデバイスOSをチェックして更新する頻度を決定します。デフォルトは**7**日です。

iOSおよびmacOSの更新アクションのステータスを取得する

iOSおよびmacOSの場合、XenMobileはControl OS Updatesポリシーをデバイスに展開しません。代わりに、XenMobileは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。

- Schedule OS Update Scan: デバイスがOSアップデートのバックグラウンドスキャンを実行するよう要求します。(iOSではオプション)
- Available OS Updates: デバイスに利用可能なOSアップデートのリストを照会します。
- Schedule OS Update: デバイスがmacOSアップデート、アプリのアップデート、またはその両方を行うよう要求します。そのため、デバイスOSがOSおよびアプリのアップデート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。

Manage > Devices > Device details (General) ページには、スケジュールされた利用可能なOSアップデートスキャン、およびスケジュールされたmacOSとアプリのアップデートのステータスが表示されます。



更新アクションのステータスの詳細については、**Manage > Devices > Device details (Delivery Groups)** ページに移動してください。

デバイス詳細画面の画像(/en-us/xenmobile/server/media/control-os-update-delivery-group.png)

利用可能なOSアップデートや最終インストール試行などの詳細については、**管理 > デバイス > デバイスの詳細 (プロパティ)** ページに移動します。

デバイス詳細画面の画像(/en-us/xenmobile/server/media/control-os-update-system-properties.png)

デバイス詳細画面の画像(/en-us/xenmobile/server/media/control-os-update-custom-properties.png)

Android Enterpriseの設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policies-control-os-updates-android-enterprise.png)

- **システム更新ポリシー:** システムアップデートがいつ行われるかを決定します。**Control Enterprise FOTA** 設定を有効にすると、この設定の構成に関係なく、アップデートは自動的に行われます。
    - **自動:** アップデートが利用可能になったときにインストールします。
    - **時間枠指定: 開始時刻**と**終了時刻**で指定された日次メンテナンス時間枠内で、アップデートを自動的にインストールします。
        - **開始時刻:** デバイスの現地時間で深夜0時からの分数 (**0**～**1440**) で測定されるメンテナンス時間枠の開始時刻。デフォルトは**0**です。

    - **終了時刻:** デバイスの現地時間で深夜0時からの分数 (**0**～**1440**) で測定されるメンテナンス時間枠の終了時刻。デフォルトは**120**です。
  - **延期:** ユーザーがアップデートを最大30日間延期できるようにします。
  - **デフォルト:** 更新ポリシーをシステムデフォルトに設定します。
- **無線アップグレードを許可:** 無効にすると、ユーザーデバイスはワイヤレスでソフトウェアアップデートを受信できません。デフォルトは**オン**です。

資格情報デバイスポリシー

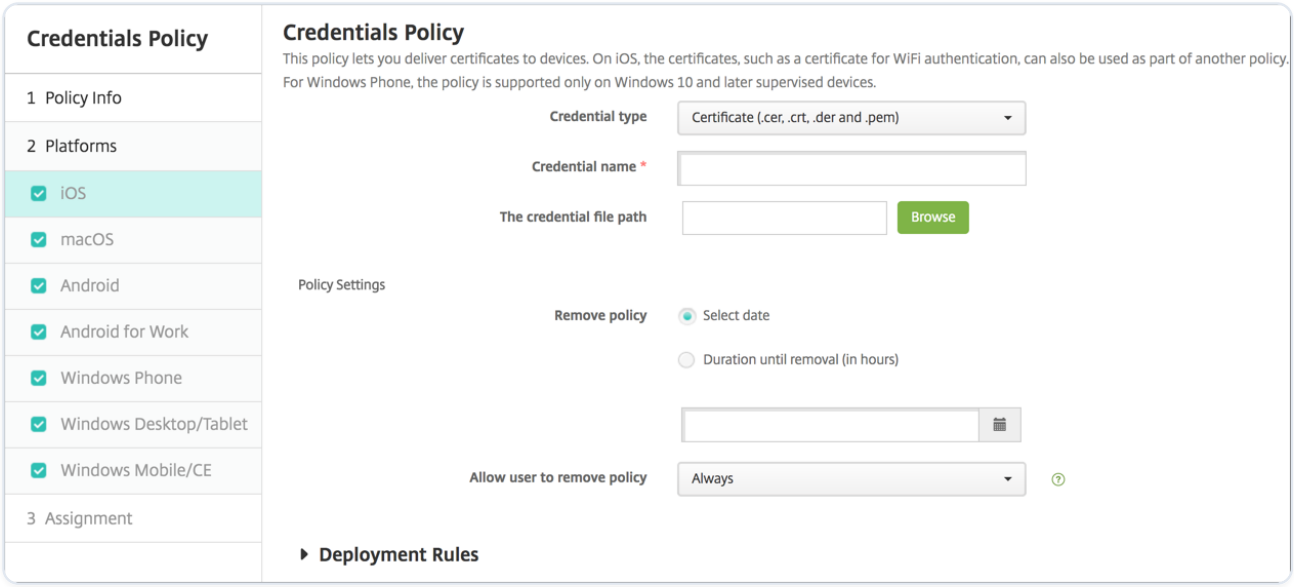
資格情報デバイスポリシーは、XenMobileで構成されたPKIを指します。たとえば、PKI構成には、PKIエンティティ、キーストア、資格情報プロバイダー、またはサーバー証明書が含まれる場合があります。資格情報の詳細については、「証明書と認証」を参照してください。

サポートされている各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で説明されています。

> **注:**
>
> このポリシーを作成する前に、各プラットフォームで使用する予定の資格情報、および証明書と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**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

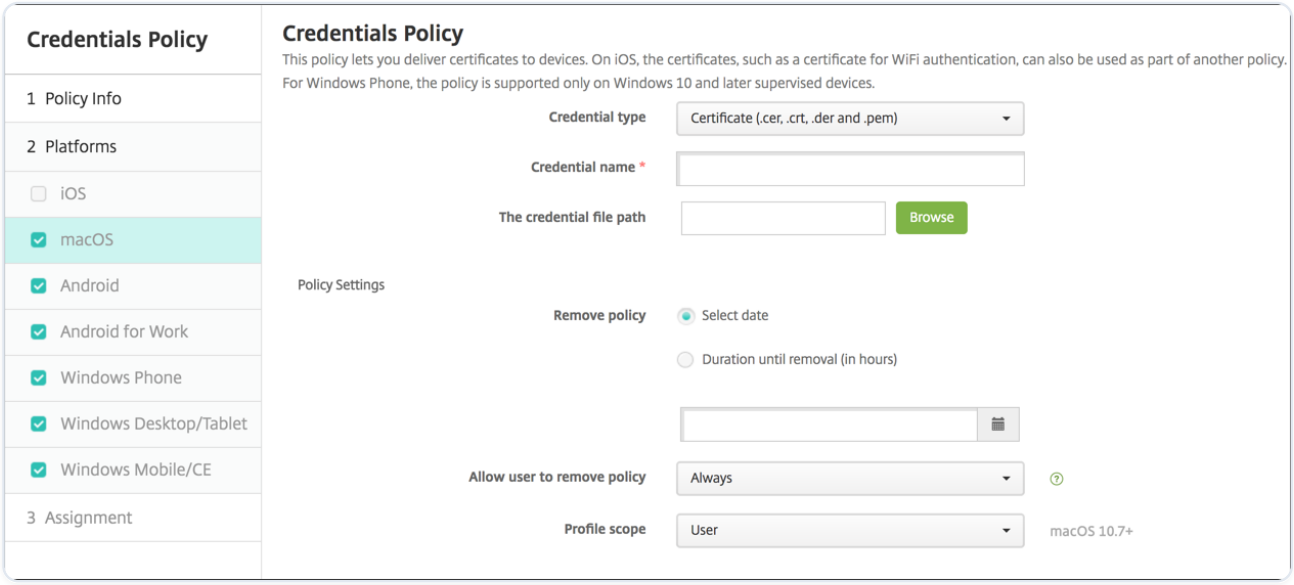


次の設定を構成します。

- **資格情報タイプ:** このポリシーで使用する資格情報の種類をドロップダウンリストでクリックし、選択した資格情報について次の情報を入力します。
  - **証明書**
    - **資格情報名:** 資格情報の一意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を選択し、ファイルの場所へ移動します。
  - **キーストア**
    - **資格情報名:** 資格情報の一意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ファイルの場所に移動し、資格情報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:** ドロップダウンリストから使用する証明書をクリックします。
  - **資格情報プロバイダー**
    - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。
- **ポリシー設定**

- **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)** です。
  - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
  - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

macOS設定



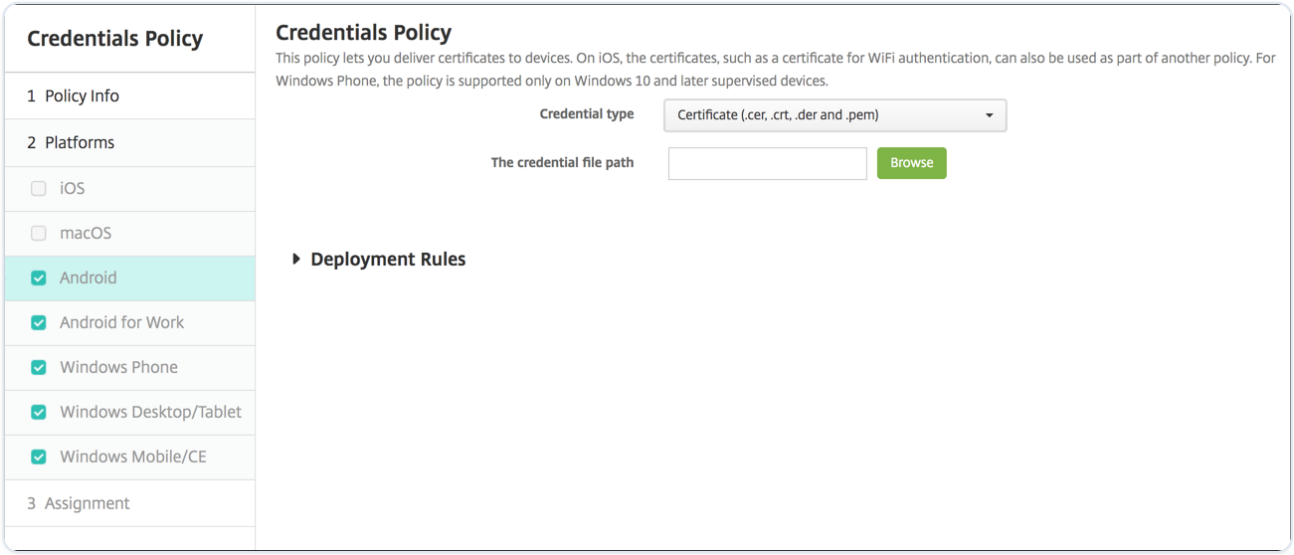
次の設定を構成します。

- **資格情報タイプ:** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、選択した資格情報について次の情報を入力します。
  - **証明書**
    - **資格情報名:** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス: 参照**をクリックしてファイルの場所へ移動し、資格情報ファイルを選択します。
  - **キーストア**
    - **資格情報名:** 資格情報の一意の名前を入力します。
    - **資格情報ファイルのパス: 参照**をクリックしてファイルの場所へ移動し、資格情報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:** ドロップダウンリストから使用する証明書をクリックします。
  - **資格情報プロバイダー**
    - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

Android設定

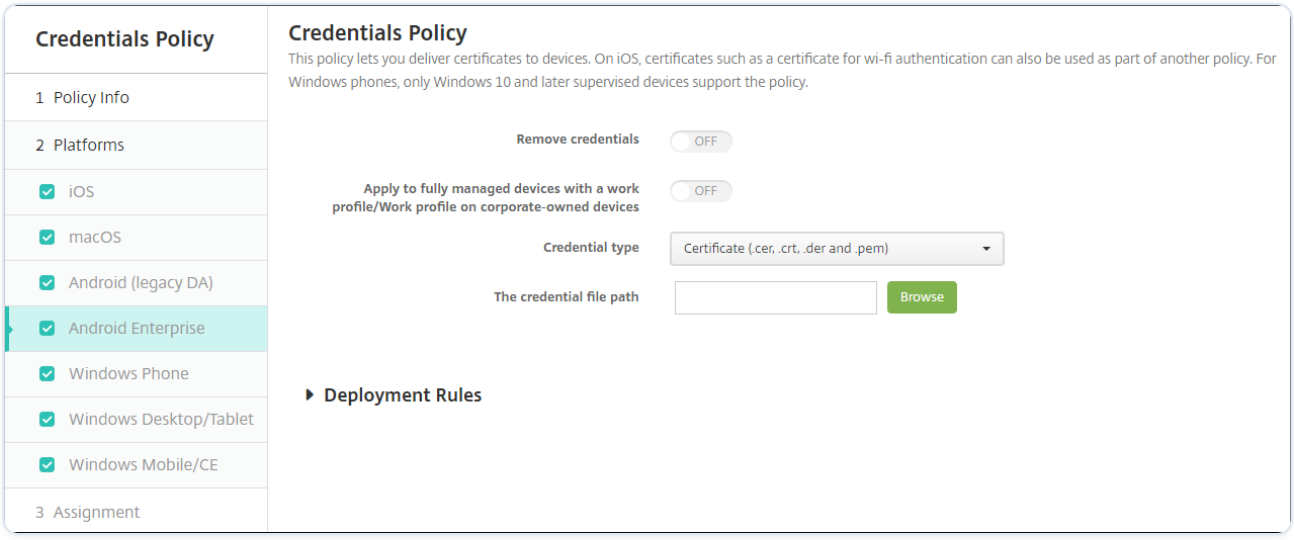


次の設定を構成します。

- **資格情報タイプ:** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、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**
  - **資格情報名:** 資格情報の一意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を選択し、ファイルの場所へ移動します。
- **キーストア**
  - **資格情報名:** 資格情報の一意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を選択し、ファイルの場所へ移動します。
  - **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:** 使用する証明書をドロップダウンリストからクリックします。
- **資格情報プロバイダー**
  - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

Android エンタープライズ設定



XenMobile®が資格情報設定を適用する方法を決定するために、これらの設定を構成します。

- **資格情報の削除:** 以下の設定を構成するには、「**オン**」に設定します。デフォルトは「**オフ**」です。
  - **ユーザー資格情報の削除:** 管理対象キーストアから証明書を削除します。デフォルトは「**オフ**」です。

    - **信頼されたルート証明書の削除:** すべての非システムCA証明書をアンインストールします。デフォルトは「**オフ**」です。

- **仕事用プロファイルを持つ完全に管理されたデバイス/会社所有デバイス上の仕事用プロファイルに適用:** 仕事用プロファイルを持つ完全に管理されたデバイスの資格情報ポリシー設定を構成できます。この設定が「**オン**」の場合、構成した資格情報設定は仕事用プロファイルにのみ適用されます。この設定が「**オフ**」の場合、構成した資格情報設定はデバイスにのみ適用されます。デフォルトは「**オフ**」です。

資格情報設定を構成します。

- **資格情報タイプ:** このポリシーで使用する資格情報の種類をドロップダウンリストからクリックし、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**

        - **資格情報ファイルのパス:** 「**参照**」をクリックして資格情報ファイルを選択し、ファイルの場所に移動します。

    - **キーストア**

        - **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を選択し、ファイルの場所に移動します。
        - **証明書エイリアス:** 証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。管理対象構成デバイスポリシーで証明書エイリアスを構成します。次に、資格情報デバイスポリシーの「**証明書エイリアス**」フィールドにエイリアスを入力します。アプリは、ユーザーによる操作なしで証明書を取得し、VPNを認証します。
        - **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**

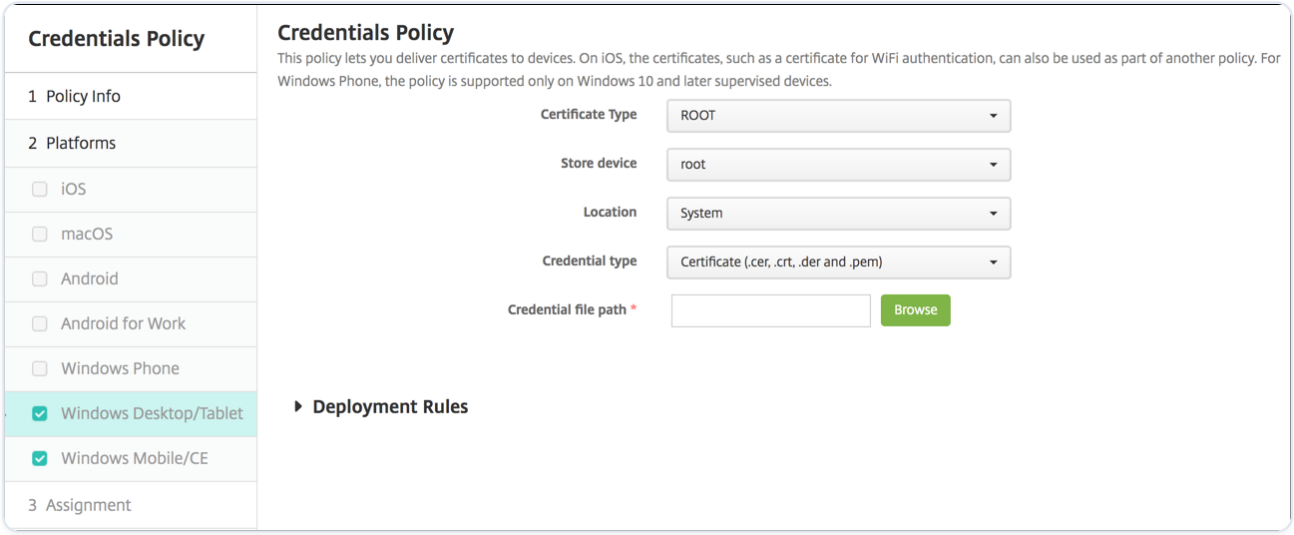
        - **サーバー証明書:** ドロップダウンリストから使用する証明書をクリックします。

    - **資格情報プロバイダー**

        - **証明書エイリアス:** 証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。管理対象構成デバイスポリシーで証明書エイリアスを構成します。次に、資格情報デバイスポリシーの**証明書エイリアス**フィールドにエイリアスを入力します。アプリは証明書を取得し、ユーザーによる操作なしでVPNを認証します。
        - **資格情報プロバイダー:** ドロップダウンリストから資格情報プロバイダーの名前をクリックします。

- **証明書を使用するアプリ:** このプロバイダーからの資格情報にサイレントアクセスできるアプリを指定するには、**追加**をクリックし、アプリを選択して、**保存**をクリックします。

Windowsデスクトップ/タブレットの設定



- **証明書の種類:** ドロップダウンリストで**ROOT**または**CLIENT**をクリックします。
- **ROOT**をクリックした場合は、次の設定を構成します。
  - **デバイスの保存先:** 資格情報の証明書ストアの場所として、ドロップダウンリストで**root**、**My**、または**CA**をクリックします。**My**は、証明書をユーザーの証明書ストアに保存します。
  - **場所:** Windows 10およびWindows 11タブレットの場合、**システム**が唯一の場所です。
  - **資格情報の種類:** Windows 10およびWindows 11タブレットの場合、**証明書**が唯一の資格情報の種類です。
  - **資格情報ファイルパス: 参照**をクリックしてファイルの場所に移動し、証明書ファイルを選択します。
- 「**CLIENT**」をクリックした場合、以下の設定を構成します。
- **場所:** Windows 10およびWindows 11タブレットの場合、**システム**が唯一の場所です。
- **資格情報タイプ:** Windows 10およびWindows 11タブレットの場合、**キーストア**が唯一の資格情報タイプです。
- **資格情報名:** 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。
- **資格情報ファイルパス:** 「**参照**」をクリックしてファイルの場所に移動し、証明書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ている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

XenMobile®では、サポートされているWindowsデバイスで以下の機能をカスタマイズするために、カスタムXMLポリシーを作成できます。

- プロビジョニング（デバイスの構成、機能の有効化または無効化を含む）
- デバイス構成（ユーザーが設定やデバイスパラメータを変更できるようにすることを含む）
- ソフトウェアアップグレード（アプリやシステムソフトウェアを含む、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を含む）
- 障害管理（デバイスからのエラーおよびステータスレポートの受信を含む）

> **注：**
>
> XMLコンテンツを作成する際は、\%文字の使用には注意してください。\%文字はXMLの予約文字であり、XMLの特殊文字をエスケープするためにのみ使用されます。名前に\%を使用するには、\%25としてエンコードしてください。

> Windowsデバイスの場合：Windowsの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の作成は、このトピックの範囲外です。OMA DM APIの使用に関する詳細については、Microsoft Developer NetworkサイトのOMA Device Managementを参照してください。

> **注：**
>
> Windows 10 RS2 Phoneの場合：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が電話に展開された後も、ブラウザは有効なままです。この問題を回避するには、電話を再起動してください。この問題はサードパーティの問題です。

> 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**に移動します。詳細については、デバイスポリシーを参照してください。

Windowsデスクトップ/タブレット設定

- **XMLコンテンツ：** ポリシーに追加するカスタムXMLコードを入力またはコピー＆ペーストします。

  次へをクリックすると、XenMobileはXMLコンテンツの構文をチェックします。構文エラーはコンテンツボックスの下に表示されます。続行する前に、すべてのエラーを修正してください。

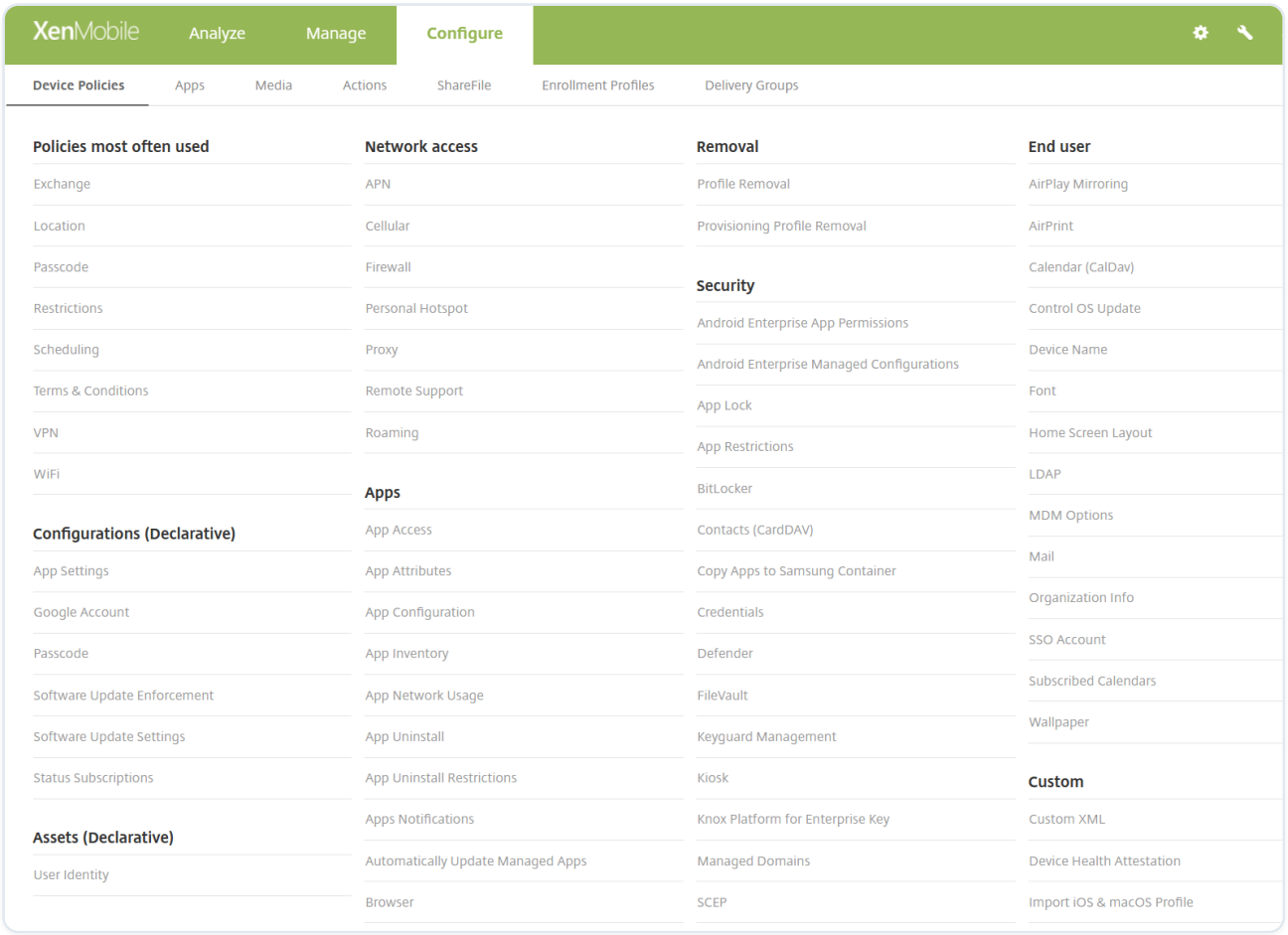
  構文エラーがない場合、**カスタムXMLポリシー**の割り当てページが表示されます。

宣言型デバイス管理ポリシー

AppleはiOS 15で、宣言型データモデルパラダイムを使用した宣言型デバイス管理 (DDM) を発表しました。このパラダイムにより、サーバーは、コマンドのシリアル化やMDMを介したデバイスのポーリングに通常関連する一般的なパフォーマンスおよびスケーラビリティの問題を回避できます。詳細については、「デバイスを拡張するための宣言型管理データモデルの活用」を参照してください。

DDM機能を有効にすると、次の宣言型デバイスポリシーがサポートされます。

- アプリ設定
- Googleアカウント
- パスコード
- ソフトウェアアップデートの適用
- ソフトウェアアップデート設定
- ステータスサブスクリプション
- ユーザーID



アプリ設定デバイスポリシー

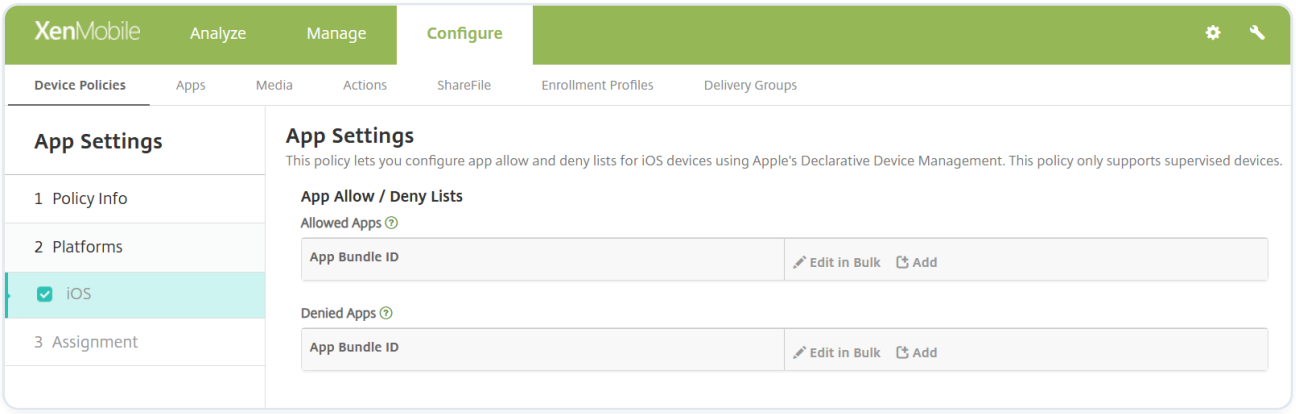
アプリ設定デバイスポリシーを使用すると、Appleの宣言型デバイス管理を使用して、アプリの許可リストと拒否リストを構成できます。これは、非推奨の`allowListedAppBundleIDs`および`blockedAppBundleIDs`制限キーを置き換えるものです。このポリシーは、監視対象デバイスのみをサポートします。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、 デバイスポリシーを参照してください。

前提条件

- XenMobile Server 10.16 ローリングパッチ 9以降。
- サーバープロパティ`ios.mdm.ios27.ddm.support`が**True**に設定されていること。
- iOS 27以降およびiPadOS 27以降で利用可能です。監視対象デバイスのみをサポートします。

iOS設定



- **アプリの許可/拒否リスト:**
  - **許可されたアプリ:** 存在する場合、デバイスはリスト内のバンドルIDを持つアプリのみを表示または起動します。すべてのWebクリップを許可するには、値`com.apple.webapp`を含めます。これは、App Storeアプリ、マーケットプレイスアプリ、およびローカルにインストールされたアプリ（Configurator、Xcodeなどを使用）に適用されます。
    - **アプリバンドルID:** アプリバンドルIDを追加するには、 をクリックし、アプリバンドルIDを入力して、 をクリックします。追加したいアプリバンドルIDごとにこのプロセスを繰り返します。または、 をクリックし、アプリバンドルIDを1行に1つずつ、またはコンマで区切って入力または貼り付け、 をクリックすることもできます。
  - **拒否されたアプリ:** 存在する場合、デバイスはリスト内のバンドルIDを持つアプリの表示または起動を禁止します。すべてのWebクリップを制限するには、値`com.apple.webapp`を含めます。これは、App Storeアプリ、マーケットプレイスアプリ、およびローカルにインストールされたアプリ（Configurator、Xcodeなどを使用）に適用されます。

注:

- システムアプリを拒否すると、他の機能が無効になる場合があります。たとえば、App Storeアプリを拒否すると、ユーザーがユーザーベースのボリューム購入プログラム (VPP) の利用規約に同意できなくなる可能性があります。
- アプリ許可リストまたはアプリ拒否リストのいずれかを構成することをお勧めしますが、両方は構成しないでください。

Googleアカウントデバイスポリシー

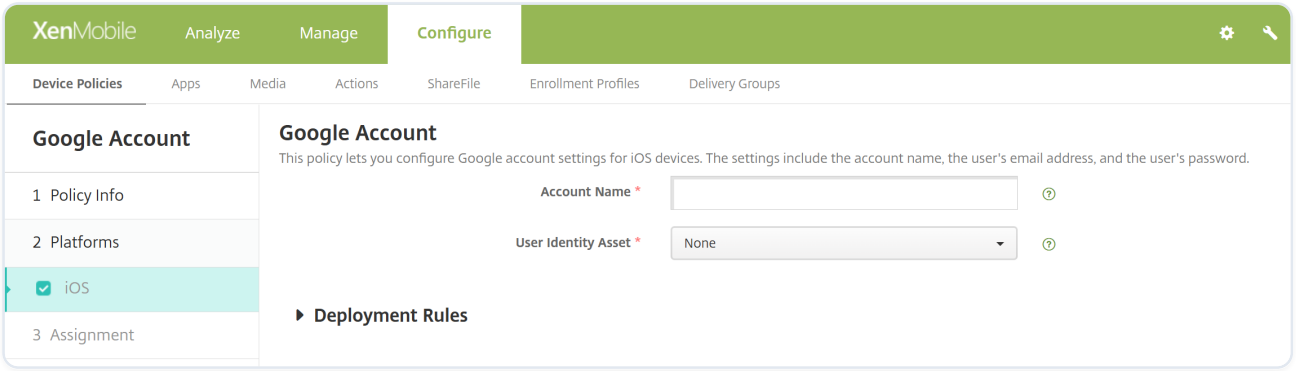
Googleアカウントデバイスポリシーを使用すると、iOSデバイスのGoogleアカウント設定を構成できます。設定には、アカウント名と、メールアドレスおよびユーザーのフルネームを構成するユーザーIDアセットが含まれます。

このポリシーを追加または構成するには、 > に移動します。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

- ゼノモバイルサーバー 10.16 ローリングパッチ 8 以降。
- サーバープロパティ `ios.mdm.declarative.management` が **True** に設定されていること。
- ユーザーIDポリシーが構成されていること。「ユーザーIDデバイスポリシー」を参照してください。

iOS設定



- **アカウント名:** Googleアカウントの名前を入力します。
- **ユーザーIDアセット:** リストから、ユーザーのメールアドレスとフルネームを含む、ユーザーIDポリシーによって作成されたユーザーIDアセットを選択します。デフォルトは です。

パスコードデバイスポリシー

パスコードデバイスポリシーは、組織の標準に基づいてパスコード要件を作成します。デバイスにコードを要求したり、書式設定ルールや、デバイスロックまでの猶予期間などの他のパスコードルールを設定したりできます。

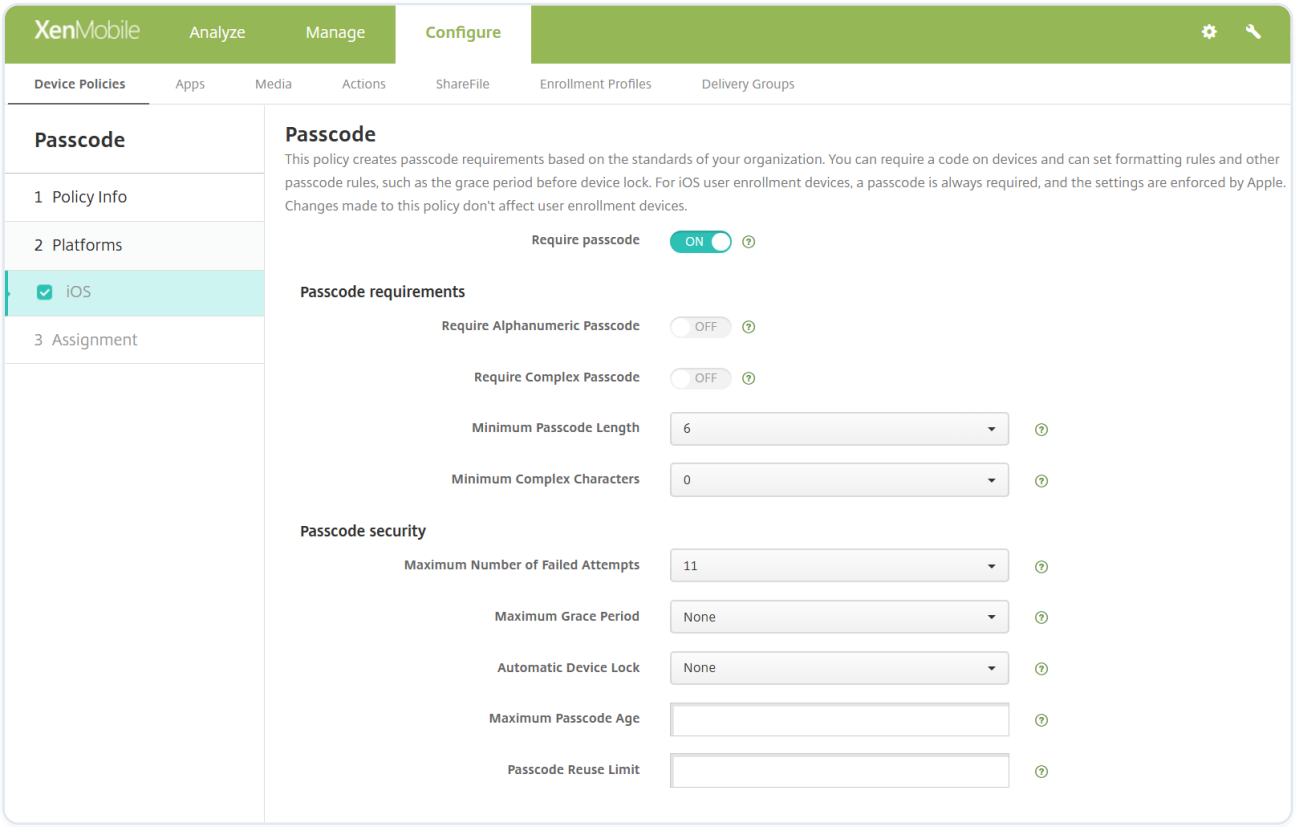
このポリシーを追加または構成するには、 > に移動します。 詳細については、デバイスポリシーを参照してください。

前提条件

- XenMobile Server 10.16 ローリングパッチ 8 以降。

- サーバープロパティ `ios.mdm.declarative.management` が **True** に設定されています。

iOS設定



- **パスコードを要求:** このオプションを選択すると、パスコードが要求され、iOS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。**オン**の場合、パスコードの長さや品質に関する要件なしに、ユーザーにパスコードの設定を要求し、パスコード要件とパスコードセキュリティの設定を構成できるようにページが展開されます。デフォルトは**オン**です。
- **パスコード要件**
  - **英数字パスコードを要求:** パスコードに少なくとも1つの英字と少なくとも1つの数字を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。
  - **複雑なパスコードを要求:** 複雑なパスコードを要求するかどうかを選択します。複雑なパスコードとは、繰り返し文字や増加/減少文字（123やCBAなど）を含まず、少なくとも1つの非数字および非英字文字を含むパスコードです。デフォルトは**オフ**です。
  - **最小パスコード長:** パスコードに含めることができる最小文字数を選択します。デフォルトは**6**です。
  - **最小複雑文字数:** パスワード内の複雑な文字の最小数を選択します。複雑な文字とは、数字や文字以外の文字（&、%、$、#など）です。デフォルトは**0**です。
- **パスコードセキュリティ**

- **失敗試行の最大回数:** iOSがデバイスを消去するまでにシステムがユーザーに許可するパスコード失敗試行回数を選択します。この設定を変更しない場合、6回の失敗試行後、デバイスはユーザーが再度パスコードを入力できるようになるまでに時間遅延を課します。時間遅延は失敗試行ごとに増加します。最後の失敗試行後、システムはiOSデバイスからすべてのデータと設定を安全に消去します。パスコードの時間遅延は6回目の試行後に開始されるため、この値が6以下の場合、システムは時間遅延なしで、ユーザーが制限を超えるとすぐに消去またはロックをトリガーします。デフォルトは**11**です。
- **最大猶予期間:** ユーザーがパスコードなしでデバイスのロックを解除できる最大期間を選択します。猶予期間なしの場合は**すぐに**を選択すると、デバイスはすぐにパスコードを要求します。デフォルトは**なし**で、ユーザーは任意の期間を選択できます。
- **自動デバイスロック:** システムがデバイスを自動的にロックするまでの、デバイスがアイドル状態であることができる最大期間を選択します。デバイスがこの制限に達すると、デバイスはロックされ、ユーザーはロックを解除するためにパスコードを入力する必要があります。デフォルトは**なし**で、ユーザーは任意の期間を選択できます。
- **パスコードの最大有効期間:** パスコードが変更されずに維持できる最大日数を選択します。この日数が経過すると、システムはデバイスのロックを解除する前にユーザーにパスコードの変更を強制します。有効な値は0～730です。**0**の値は、即時のパスコード変更を強制します。デフォルトは空で、パスコードの有効期間制限がないことを意味します。
- **パスコード再利用制限:** 新しいパスコードを検証する際にシステムがチェックする過去のパスコードエントリの数を選択します。指定されたパスコード履歴範囲内で以前使用されたパスコードと一致する場合、デバイスは新しいパスコードを拒否します。有効な値は1～50です。デフォルトは空で、システムが履歴チェックを実行しないことを意味します。

> **注:**
>
> 同じ設定がMDMプロファイルおよび宣言型構成としてデバイスに送信された場合、設定が複数のプロファイルによって配信された場合と同じルールが適用されます。たとえば、パスコードポリシーがプロファイル（パスコードポリシー経由）と構成（宣言型パスコードポリシー経由）によって構成されている場合、ポリシーはマージされ、最も厳格な設定が適用されます。

ソフトウェアアップデート強制デバイスポリシー

特定のOSリリース向けのソフトウェアアップデート強制デバイスポリシーを使用すると、IT管理者はiOSデバイスのアップデートを管理し、どのアップデートを適用するかを制御したり、すべてのアップデートを完了するための期限を設定したりできます。これらの設定は、Appleの宣言型デ

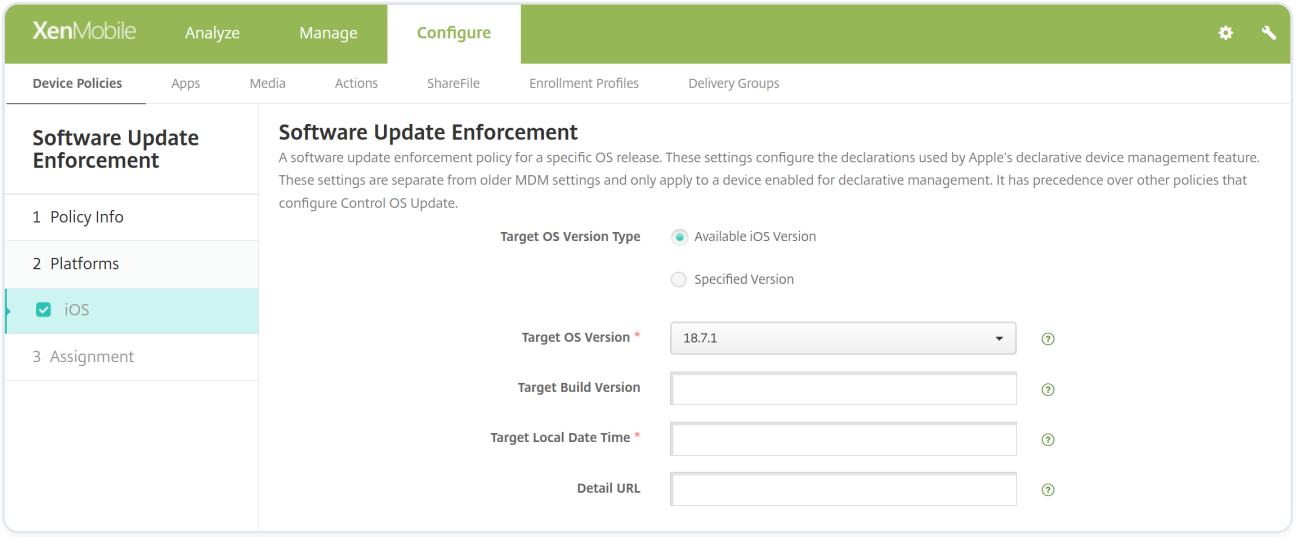
バイス管理機能で使用される宣言を構成します。これらの設定は、以前のMDM設定とは別のものであり、宣言型管理が有効になっているデバイスにのみ適用されます。同じ設定の場合、OSアップデート制御ポリシーよりも優先されます。

このポリシーを追加または構成するには、 **>** に移動します。 詳細については、デバイスポリシーを参照してください。

前提条件

- XenMobile Server 10.16 ローリングパッチ 8 以降。
- サーバープロパティ `ios.mdm.declarative.management` が **True** に設定されています。
- **iOS 17.0**以降および**iPadOS 17.0**以降で利用可能です。

iOS設定



- **ターゲットOSバージョンタイプ:** ターゲットOSバージョンを構成する方法を指定します。デフォルトは**利用可能なiOSバージョン**です。
  - **利用可能なiOSバージョン: オン**の場合、**ターゲットOSバージョン**で利用可能なターゲットOSバージョンを一覧表示します。
  - **指定されたバージョン: オン**の場合、推奨される形式でOSバージョンを手動で入力します。
- **ターゲットOSバージョン: (必須)** 適切な時期までにデバイスをアップデートするターゲットOSバージョンを選択または入力します。これはOSのバージョン番号であり、たとえば17.7です。補足的なバージョン識別子（たとえば17.7.2）を含む場合もあります。
- **ターゲットビルドバージョン:** 適切な時期までにデバイスをアップデートするターゲットビルドバージョンを入力します（例: 20A242）。システムは、シード期間中のテストにビルドバージョンを使用します。ビルドバージョンには、補足的なバージョン識別子（例: 20A242a）を

含めることができます。ビルドバージョンがTargetOSVersionキーで指定されたターゲットOSバージョンと一致しない場合、ターゲットOSバージョンが優先されます。

- **ターゲットローカル日時: (必須)** ソフトウェアアップデートを強制的にインストールする日時を指定するローカル日時値を入力します。RFC3339から派生していますが、タイムゾーンオフセットを含まないyyyy-mm-ddThh:mm:ss形式を使用します。ユーザーがこの時間までにソフトウェアアップデートをトリガーしない場合、デバイスは強制的にインストールします。
- **詳細URL:** 組織が提供する強制アップデートに関する詳細を示すWebページのURLを入力します。

注:

ソフトウェアアップデート強制ポリシーとOSアップデート制御ポリシーの両方で、デバイスのOSアップデートを管理できます。ただし、ソフトウェアアップデート強制ポリシーはOSアップデート制御ポリシーよりも優先されます。両方のポリシーが同じ設定で展開されている場合、OSアップデート制御ポリシーの設定は上書きされ、適用されません。詳細については、「宣言型デバイス管理への移行」を参照してください。

また、ソフトウェアアップデート強制ポリシーとOSアップデート制御ポリシーにはいくつかの違いがあります。

ポリシーの種類	ソフトウェアアップデート強制	OSアップデート制御
デバイスの種類	監視対象または非監視対象デバイス	監視対象デバイス
アップデート期限の強制	✓	✗
ヘルプURLの入力	✓	✗
ビルドバージョン番号を指定	✓	✗
最新の更新を自動展開	✗	✓
サポートされる最小バージョン	iOS 17.0	iOS 10.3 (監視対象)

ソフトウェアアップデート設定デバイスポリシー

ソフトウェアアップデート設定デバイスポリシーを使用すると、OSアップデートを延期し、ユーザーがシステム設定でソフトウェアアップデートを手動で操作する方法を制御できます。このポリシーは、監視対象デバイスのみをサポートします。

このポリシーを追加または構成するには、 **>** に移動します。 詳細については、デバイスポリシーを参照してください。

前提条件

- XenMobile Server 10.16 ローリングパッチ 8 以降。
- サーバープロパティ`ios.mdm.declarative.management`と`ios.mdm.software.update.settings`が**True**に設定されています。
- **iOS 18.0**以降および**iPadOS 18.0**以降で利用可能で、監視対象デバイスのみをサポートします。

iOS設定

ソフトウェアアップデート設定デバイスポリシー](/en-us/xenmobile/server/media/software-update-setting-ios-settings1.png)

- **自動アクション**
  - **ダウンロード:** ユーザーが利用可能なアップデートの自動ダウンロードを制御できるかどうかを指定します。デフォルトは**許可**です。
    - **許可** - ユーザーは自動ダウンロードを有効または無効にできます。
    - **常にオン** - 自動ダウンロードは常に有効になります。
    - **常にオフ** - 自動ダウンロードは常に無効になります。
  - **OSアップデートのインストール:** ユーザーが利用可能なアップデートの自動インストールを制御できるかどうかを指定します。デフォルトは**許可**です。
    - **許可** - ユーザーは自動インストールを有効または無効にできます。
    - **常にオン** - 自動インストールは常に有効になります。
    - **常にオフ** - 自動インストールは常に無効になります。
- **延期**
  - **合計期間 (日数):** デバイス上のメジャーまたはマイナーOSソフトウェアアップデートを延期する日数を指定します。設定すると、ソフトウェアアップデートは、ソフトウェアアッ

プデートのリリース後、指定された遅延期間が経過した後にのみ表示されます。iOS 18以降で利用可能です。有効な値は0〜90です。デフォルトは**0**で、遅延は発生しません。

- **推奨される頻度**
  - **推奨される頻度:** デバイスがユーザーにソフトウェアアップデートを表示する方法を指定します。複数のアップデートが利用可能な場合、デバイスは次のように動作します。デフォルトは**すべて**です。
    - **すべて** - すべてのソフトウェアアップデートバージョンを表示します。
    - **最も古い** - 最も古い（番号の小さい）ソフトウェアアップデートバージョンのみを表示します。
    - **最新** - 最新の（番号の大きい）ソフトウェアアップデートバージョンのみを表示します。
- **通知**
  - **通知: オン**の場合、デバイスはすべてのソフトウェアアップデート強制通知を表示します。**オフ**の場合、デバイスは強制期限の1時間前にトリガーされる通知と、再起動カウントダウン通知のみを表示します。デフォルトは**オン**です。
- **緊急セキュリティ対応**
  - **有効化: オフ**の場合、緊急セキュリティ対応はユーザーによるインストールに提供されません。システムは`com.apple.configuration.softwareupdate.enforcement.specific`構成で緊急セキュリティ対応をインストールできます。**オン**の場合、システムはユーザーに緊急セキュリティ対応を提供します。デフォルトは**オン**です。
  - **ロールバックを有効にする: オフ**の場合、システムはユーザーに緊急セキュリティ対応のロールバックを提供しません。**オン**の場合、システムはユーザーに緊急セキュリティ対応のロールバックを提供します。デフォルトは**オン**です。

ステータスサブスクリプションデバイスポリシー

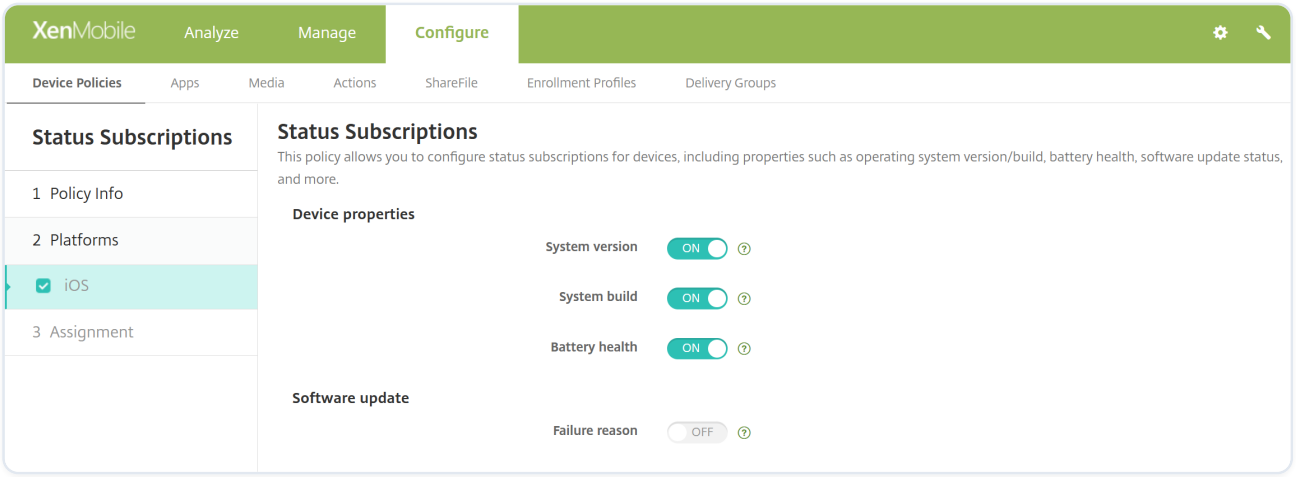
ステータスサブスクリプションデバイスポリシーを使用すると、オペレーティングシステムのバージョン/ビルド、バッテリーの状態、ソフトウェアアップデートのステータスなどのプロパティを含む、デバイスのステータスサブスクリプションを構成できます。

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**に移動します。 詳細については、デバイスポリシーを参照してください。

前提条件

- XenMobile サーバー 10.16 ローリングパッチ 8 以降。
- サーバープロパティ`ios.mdm.declarative.management`が**True**に設定されています。

iOS設定



- **デバイスプロパティ**
  - **システムバージョン: オン**の場合、デバイスはオペレーティングシステムのバージョン（例：18.0）を報告し、これはデバイスプロパティのシステム情報セクションに表示されます。バージョンアップグレードが発生したときにデバイスが自動的に報告するため、これは便利です。デフォルトは**オン**です。iOS 15以降で利用可能です。
  - **システムビルド: オン**の場合、デバイスはオペレーティングシステムのビルドバージョン（例：18F132）を報告し、これはデバイスプロパティのシステム情報セクションに表示されます。バージョンアップグレードが発生したときにデバイスが自動的に報告するため、これは便利です。デフォルトは**オン**です。iOS 15以降で利用可能です。
  - **バッテリーの状態: オン**の場合、新しい設定**バッテリーの状態**がデバイスプロパティに追加されます。この設定により、管理者は**管理 > デバイス > プロパティ > バッテリー > バッテリーの状態**に移動して、登録済みiOSデバイスのバッテリーの状態を表示できます。デフォルトは**オン**です。iOS 17以降で利用可能です。
- **ソフトウェアアップデート**
  - **失敗理由: オン**の場合、デバイスは失敗したOSアップデートの理由を報告し、これはデバイスプロパティのソフトウェアアップデート情報セクションに表示されます。デフォルトは**オフ**です。iOS 17以降で利用可能です。

ユーザーIDデバイスポリシー

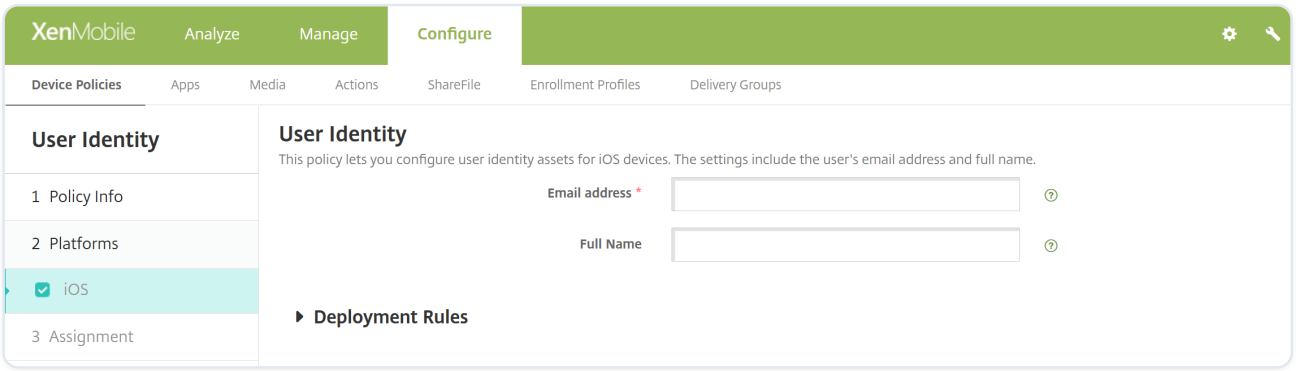
ユーザーIDデバイスポリシーを使用すると、iOSデバイスのユーザーIDアセットを構成できます。設定には、ユーザーのメールアドレスと氏名が含まれます。

このポリシーを追加または構成するには、 > に移動します。 詳細については、デバイスポリシーを参照してください。

前提条件

- XenMobile Server 10.16 Rolling Patch 8 またはそれ以降。
- サーバープロパティ `ios.mdm.declarative.management` が**True**に設定されています。

iOS設定



- **メールアドレス:** ユーザー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。
- **氏名:** ユーザーの氏名を入力します。

Defenderデバイスポリシー

Windows Defenderは、Windows 10およびWindows 11に搭載されているマルウェア対策機能です。XenMobile®デバイスポリシーであるDefenderを使用して、デスクトップおよびタブレット向けのWindows 10およびWindows 11用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、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

Windowsデスクトップおよびタブレットの設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-defender.png)

- **アーカイブのスキャンを許可:** 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 です。

- **クラウド保護を許可:** Defenderがマルウェア活動に関する情報をMicrosoftに送信することを許可または禁止します。デフォルトは です。
- **リムーバブルドライブのフルスキャンを許可:** 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 です。
- **Windows Defenderリアルタイム監視機能を許可:** デフォルトは です。
- **ネットワークファイルのスキャンを許可:** 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 です。
- **Windows Defender UIへのユーザーアクセスを許可:** 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、ユーザーデバイスが次回起動したときに有効になります。この設定が 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 です。
- **除外する拡張子:** リアルタイムスキャンまたはスケジュール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。例: 「lib\|obj」。
- **除外するパス:** リアルタイムスキャンまたはスケジュール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。例: 「C:\\Example\|C:\\Example1」。
- **除外するプロセス:** リアルタイムスキャンまたはスケジュールスキャンから除外するプロセス。プロセスを区切るには、**\|** 文字を使用します。例: 「C:\\Example.exe\|C:\\Example1.exe」。
- **サンプルの送信の同意:** 悪意のあるファイルで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: 、、、。デフォルトは です。

デバイスヘルス構成証明デバイスポリシー

XenMobile®では、Windows 10およびWindows 11デバイスに、特定のデータとランタイム情報をHealth Attestation Service (HAS)に送信させて分析させることで、デバイスのヘルス状態を報告させることができます。HASは、デバイスがXenMobileに送信するHealth Attestation Certificateを作成して返します。XenMobileはHealth Attestation Certificateを受信すると、その内容に基づいて、以前に設定した自動アクションを展開できます。

HASによって検証されるデータは次のとおりです。

- AIKの存在
- BitLockerのステータス
- ブートデバッグが有効
- ブートマネージャー改訂リストバージョン

- コード整合性が有効
- コード整合性改訂リストバージョン
- Apple展開プログラムポリシー
- ELAMドライバーがロード済み
- 発行日時
- カーネルデバッグが有効
- PCR
- リセット回数
- 再起動回数
- セーフモード有効
- SBCPハッシュ
- セキュアブート有効
- テスト署名有効
- VSM有効
- WinPE有効

詳細については、MicrosoftのDevice 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、 **>** に移動します。詳細については、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で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、オンプレミスのDHAサービスを有効にするXenMobile Serverポリシーを作成します。

1. DHAサーバーを構成するには、Windows Server 2016 Technical Preview 5以降を実行しているマシンに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サーバーを構成する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、これらの設定を構成します:

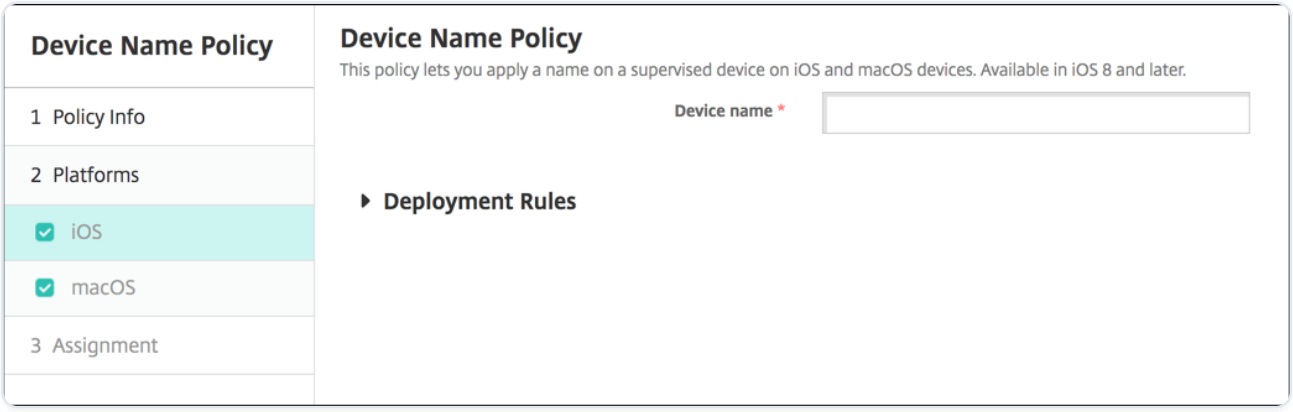
   - **デバイス正常性構成証明を有効にする: オン**に設定します。
   - **オンプレミス正常性構成証明サービスを構成する: オン**に設定します。
   - **オンプレミス DHA サービス FQDN:** 設定した DHA サーバーの完全修飾ドメイン名を入力します。
   - **オンプレミス DHA API バージョン:** DHA サーバーにインストールされている DHA サービスのバージョンを選択します。

デバイス名デバイスポリシー

監視対象のiOSおよびmacOSデバイスに名前を設定して、デバイスを簡単に識別できるようにすることができます。デバイス名を定義するには、マクロ、テキスト、またはその両方の組み合わせを使用できます。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、${device.serialnumber}を使用する必要があります。デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.comを使用する必要があります。マクロの詳細については、「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、 > に移動します。詳細については、「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:** 各デバイスに一意の名前を付けるには、マクロ、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ます。たとえば、${device.serialnumber}を使用してデバイス名を各デバイスのシリアル番号に設定したり、${device.serialnumber} ${ user.username } を使用してデバイス名にユーザー名を含めたりします。

教育構成デバイスポリシー

教育構成デバイスポリシーは以下を定義します。

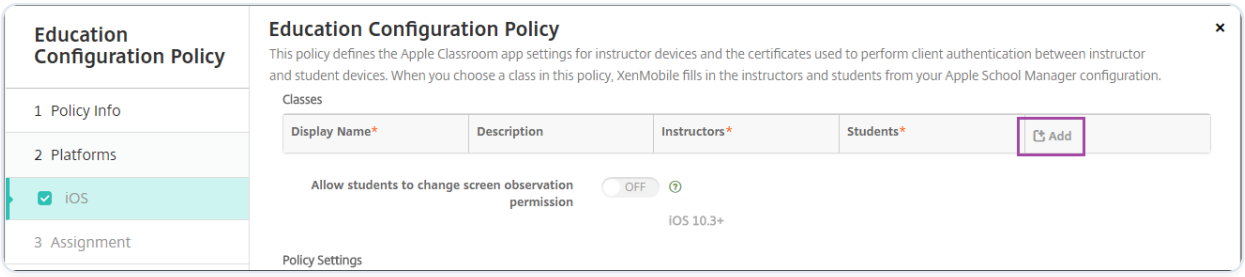
- 教師用デバイスのApple Classroomアプリ設定。
- 教師と生徒のデバイス間でクライアント認証を行うために使用される証明書。

このポリシーでクラスを選択すると、XenMobile®コンソールはApple School Manager構成から教師と生徒を自動入力します。このポリシーのApple Classroomアプリ設定がすべてのクラスで同じである場合は、1つのポリシーを作成します。

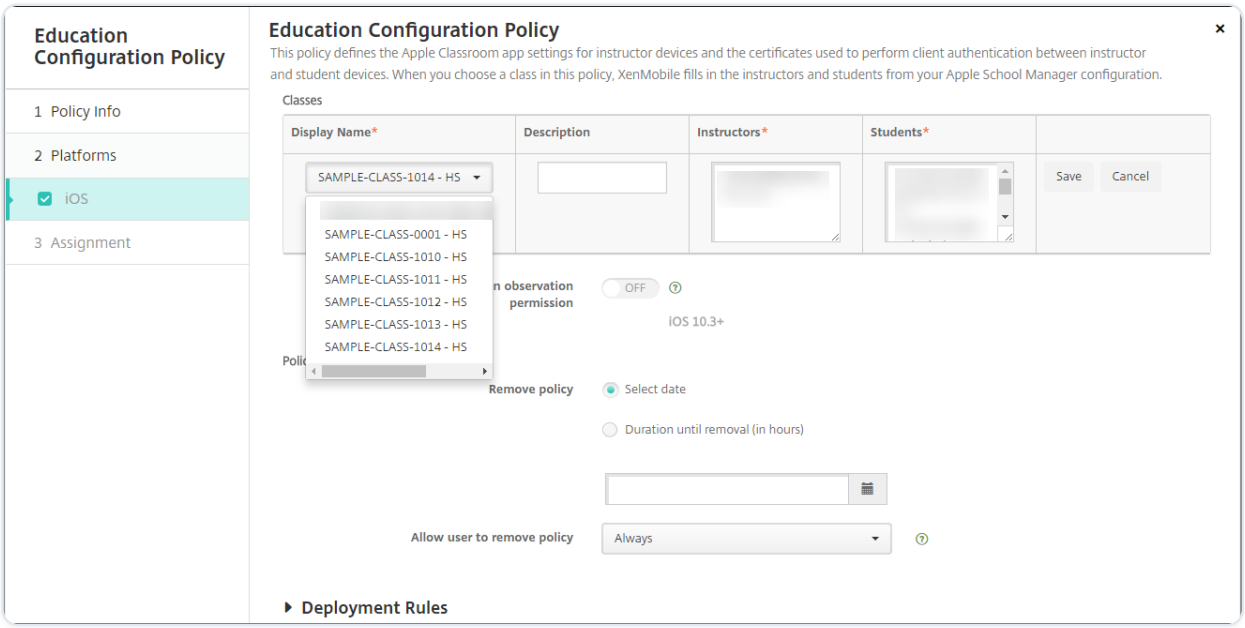
このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

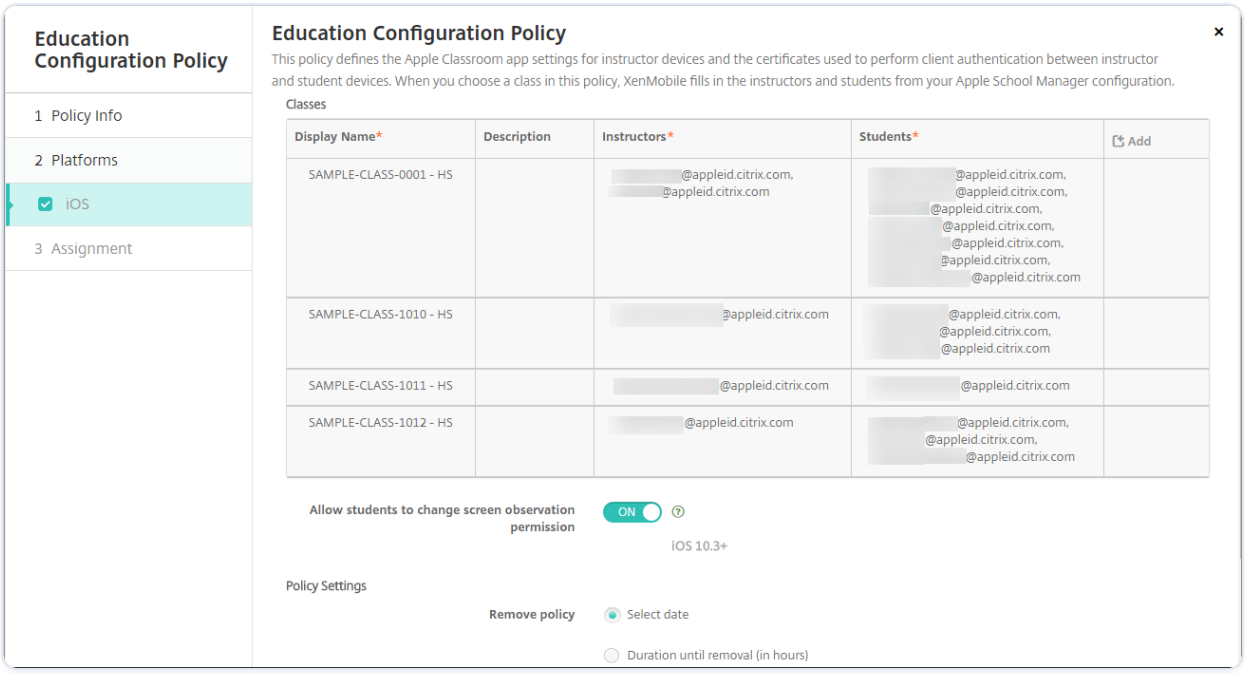
- **クラス:** クラスを追加するには、 をクリックします。



次に、 リストをクリックします。接続されているApple School Managerアカウントから取得されたクラスのリストが表示されます。



からクラスを選択すると、XenMobileは教師と生徒を自動入力します。引き続きクラスを追加します。

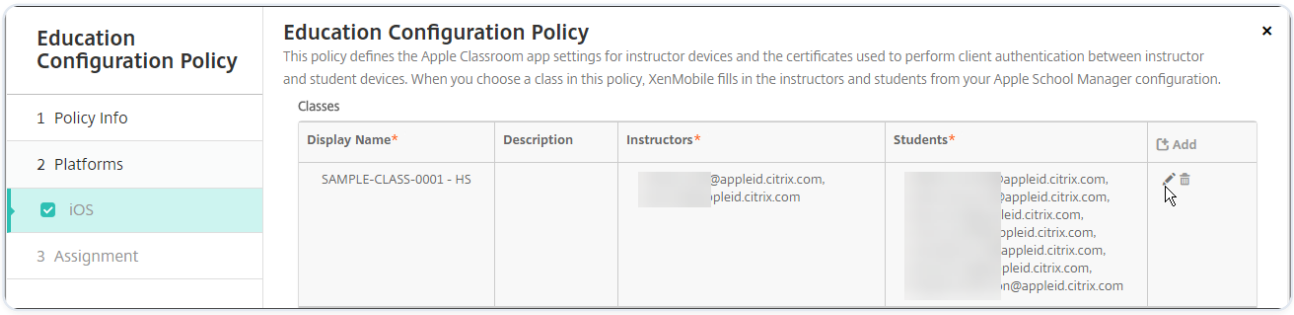


- **生徒に画面監視の許可変更を許可する:** の場合、管理対象クラスに登録されている生徒は、教師が自分のデバイス画面を監視することを許可するかどうかを選択できます。デフォルトは**オン**です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーを削除するスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。

ポリシー内のクラス情報を編集するには

クラスに説明を追加できます (Classroomアプリの「表示名」)。また、インストラクターや生徒を追加または削除することもできます。XenMobileは、これらの変更をApple School Managerアカウントに保存しません。詳細については、「Apple Education機能との統合」の「インストラクター、生徒、およびクラスデータの管理」を参照してください。

編集したいクラスの**追加**列にマウスカーソルを合わせ、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、削除したいクラスの**追加**列にマウスカーソルを合わせ、ゴミ箱アイコンをクリックします。

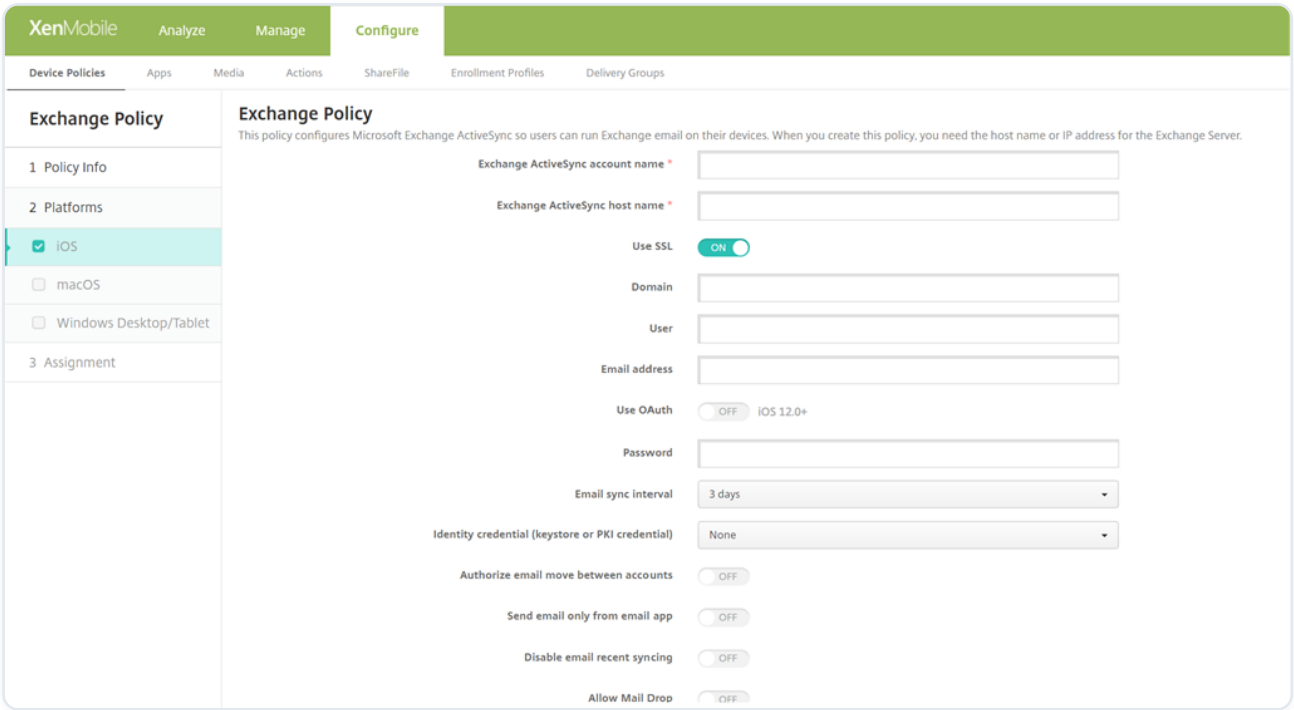
Exchange デバイスポリシー

Exchange ActiveSync デバイスポリシーを使用して、ユーザーデバイス上のメールクライアントを構成し、Exchange でホストされている企業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 Enterprise、Samsung SAFE、Samsung Knox、Windows Tablet 用のポリシーを作成できます。各プラットフォームには異なる値のセットが必要であり、これについては以下のセクションで詳しく説明します。

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 の設定については、Microsoft の記事「ActiveSync CSP」を参照してください。

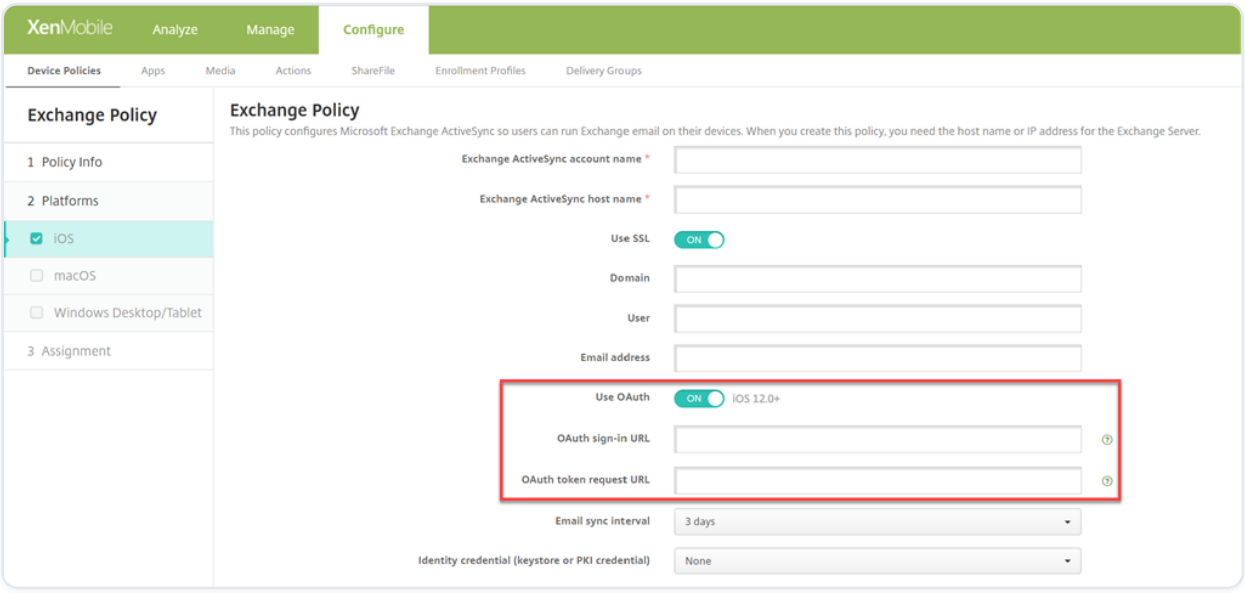
このポリシーを追加または構成するには、**［構成］>［デバイスポリシー］** の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

iOS の設定



- **Exchange ActiveSync アカウント名:** ユーザー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 ホスト名:** メールサーバーのアドレスを入力します。
- **SSL の使用:** ユーザーデバイスと Exchange Server 間の接続を保護するかどうかを選択します。デフォルトは **オン** です。

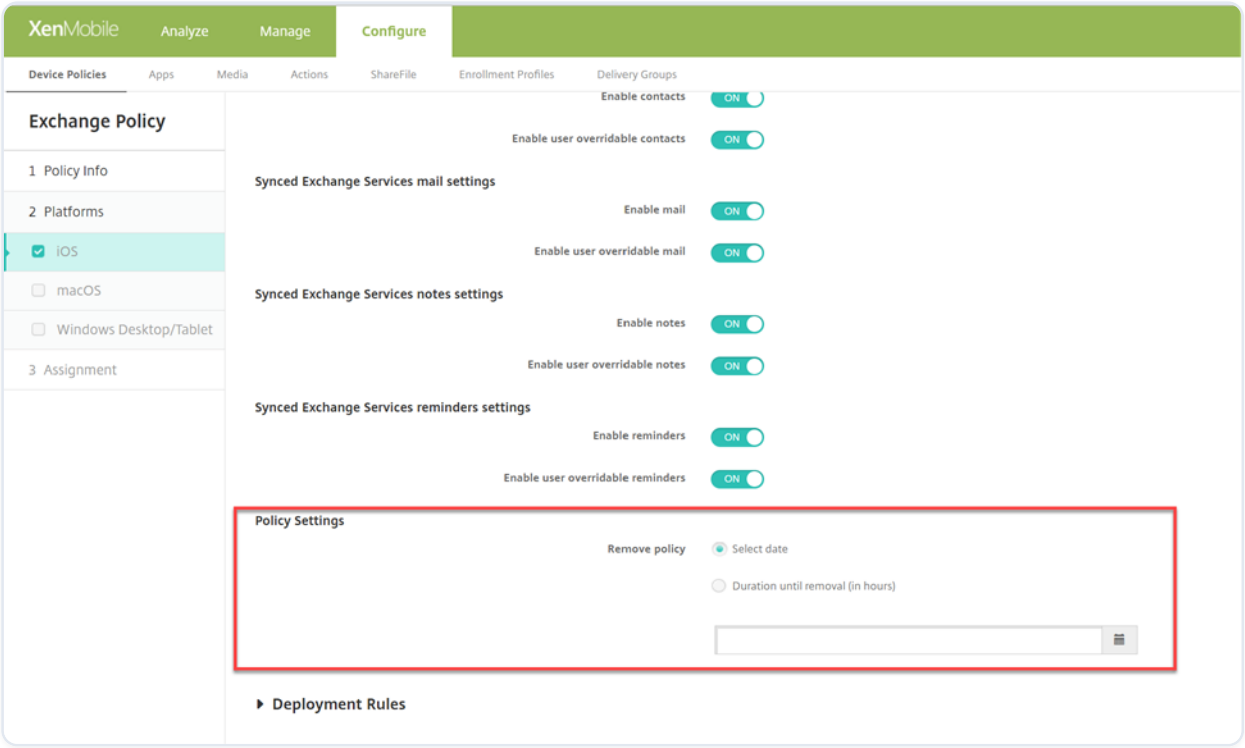
- **ドメイン:** Exchange Server が存在するドメインを入力します。このフィールドでシステムマクロ $user.domainname を使用すると、ユーザーのドメイン名を自動的に検索できます。
- **ユーザー:** Exchange ユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ $user.username を使用すると、ユーザー名を自動的に検索できます。
- **メールアドレス:** 完全なメールアドレスを指定します。このフィールドでシステムマクロ $user.mail を使用すると、ユーザーのメールアカウントを自動的に検索できます。
- **OAuth の使用: オン** に設定すると、接続は認証に OAuth を使用します。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。
    - **OAuth サインイン URL**: AutoDiscovery Service が使用されていない場合に、OAuth を使用して認証するために Webview に読み込む URL を指定します。このフィールドは、**OAuth の使用** が **オン** に設定されている場合にのみ表示されます。
    - **OAuth トークン要求 URL**: アカウントが OAuth トークン要求に使用できる URL を指定します。このフィールドは、**OAuth の使用** が **オン** に設定されている場合にのみ表示されます。



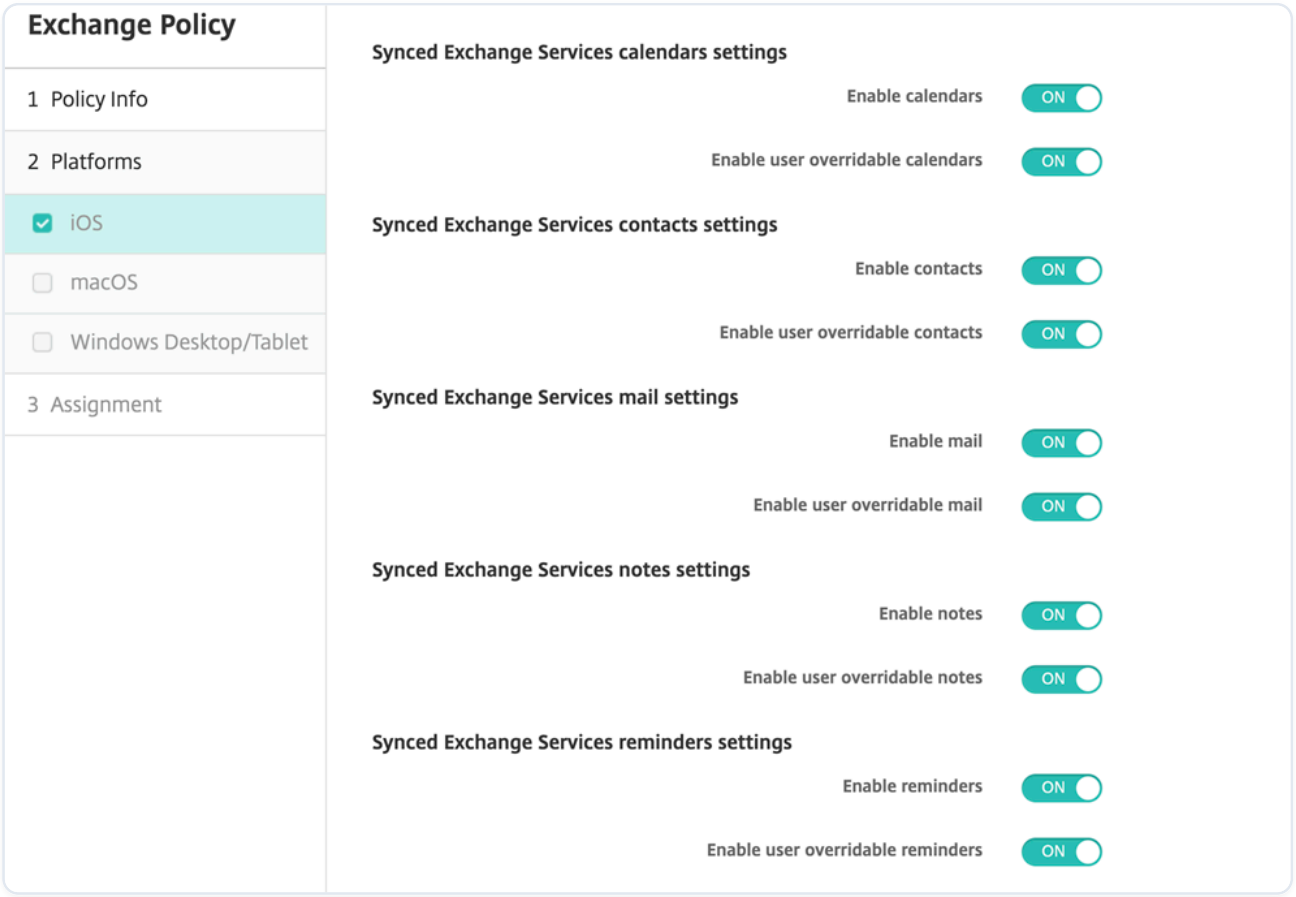
- **パスワード:** Exchangeユーザーアカウントのオプションのパスワードを入力します。**OAuthの使用**が**オン**の場合、この設定は表示されません。
- **メール同期間隔:** リストから、Exchange Serverとメールを同期する頻度を選択します。デフォルトは**3日間**です。
- **ID資格情報 (キーストアまたはPKI):** XenMobileのIDプロバイダーを構成している場合は、ドロップダウンリストでオプションのID資格情報をクリックします。このフィールドは、Exchangeがクライアント証明書認証を必要とする場合にのみ必須です。デフォルトは**なし**です。

- **アカウント間のメール移動を許可:** ユーザーがこのアカウントから別のメールアカウントにメールを移動したり、別のアカウントから転送および返信したり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。
- **メールアプリからのみメールを送信:** ユーザーがメール送信にiOSメールアプリのみを使用するよう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にする:** ユーザーが最近のアドレスを同期するのを防ぐ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。
- **Mail Dropを許可:** アカウントで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署名を有効にする:** このアカウントがS/MIME署名をサポートするかどうかを選択します。デフォルトは**オン**です。**オン**に設定すると、次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。
  - **S/MIME署名ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定でS/MIME署名をオン/オフにできます。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署名証明書UUIDユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。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暗号化を有効にする:** このアカウントが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**に設定すると、次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切り替えを有効にする: オン**に設定すると、ユーザーが作成する各メッセージに対してS/MIME暗号化をオンまたはオフに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。
  - **S/MIME 暗号化のデフォルト設定をユーザーが上書き可能: オン**に設定されている場合、ユーザーはデバイスの設定でS/MIMEをデフォルトでオン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 をユーザーが上書き可能: オン**に設定されている場合、ユーザーはデバイスの設定でS/MIME暗号化IDと暗号化をオン/オフできます。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。
- **ポリシー設定**

- **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間単位)**です。
  - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
  - **削除までの期間 (時間単位):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。



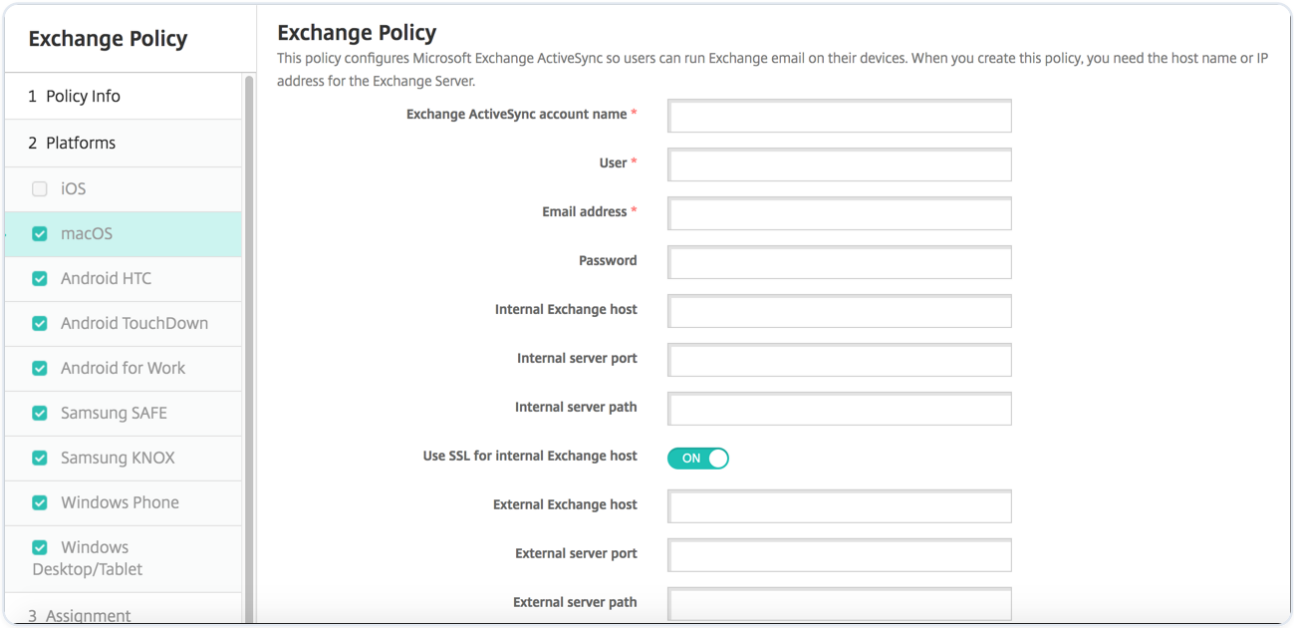
同期されたExchangeサービス



- **同期されたExchangeサービスのカレンダー設定**
  - **カレンダーを有効にする**: アカウントの*カレンダー*サービスを有効または無効にできます。デフォルト値は**オン**です。 **オフ**に設定されている場合、アカウントの*カレンダー*サービスは無効になります。*カレンダー*サービスは、**ユーザーがカレンダーを上書き可能にする**ボタンが**オン**に設定されている場合にのみ、設定で再度有効にできます。
  - **ユーザーがカレンダーを上書き可能にする**: 設定でアカウントの*カレンダー*サービスの状態を変更できます。デフォルト値は**オン**です。 **オフ**に設定されている場合、*カレンダー*サービスの状態を変更することはできません。
- **同期されたExchangeサービスの連絡先設定**
  - **連絡先を有効にする**: アカウントの*連絡先*サービスを有効または無効にできます。デフォルト値は**オン**です。 **オフ**に設定されている場合、アカウントの*連絡先*サービスは無効になります。*連絡先*サービスは、**ユーザーが連絡先を上書き可能にする**ボタンが**オン**に設定されている場合にのみ、設定で再度有効にできます。
  - **ユーザーが連絡先を上書き可能にする**: 設定でアカウントの*連絡先*サービスの状態を変更できます。デフォルト値は**オン**です。 **オフ**に設定されている場合、*カレンダー*サービスの状態を変更することはできません。

- **同期されたExchangeサービスメール設定**
  - **メールを有効にする**: アカウントの*メール*サービスを有効または無効にできます。デフォルト値は**ON**です。 **OFF**に設定されている場合、アカウントの*メール*サービスは無効になります。*メール*サービスは、**ユーザーが上書き可能なメールを有効にする**ボタンが**ON**に設定されている場合にのみ、設定で再度有効にできます。
  - **ユーザーが上書き可能なメールを有効にする**: 設定でアカウントの*メール*サービスの状態を変更できます。デフォルト値は**ON**です。 **OFF**に設定されている場合、*メール*サービスの状態を変更できません。
- **同期されたExchangeサービスノート設定**
  - **ノートを有効にする**: アカウントの*ノート*サービスを有効または無効にできます。デフォルト値は**ON**です。 **OFF**に設定されている場合、アカウントの*ノート*サービスは無効になります。*ノート*サービスは、**ユーザーが上書き可能なノートを有効にする**ボタンが**ON**に設定されている場合にのみ、設定で再度有効にできます。
  - **ユーザーが上書き可能なノートを有効にする**: 設定でアカウントの*ノート*サービスの状態を変更できます。デフォルト値は**ON**です。 **OFF**に設定されている場合、*ノート*サービスの状態を変更できません。
- **同期されたExchangeサービスリマインダー設定**
  - **リマインダーを有効にする**: アカウントの*リマインダー*サービスを有効または無効にできます。デフォルト値は**ON**です。 **OFF**に設定されている場合、アカウントの*リマインダー*サービスは無効になります。*リマインダー*サービスは、**ユーザーが上書き可能なリマインダーを有効にする**ボタンが**ON**に設定されている場合にのみ、設定で再度有効にできます。
  - **ユーザーが上書き可能なリマインダーを有効にする**: 設定でアカウントの*リマインダー*サービスの状態を変更できます。デフォルト値は**ON**です。 **OFF**に設定されている場合、*リマインダー*サービスの状態を変更できません。

macOS設定



- **Exchange ActiveSyncアカウント名:** ユーザー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$user.usernameを使用すると、ユーザー名を自動的に検索できます。
- **メールアドレス:** 完全なメールアドレスを指定します。このフィールドでシステムマクロ$user.mailを使用すると、ユーザーのメールアカウントを自動的に検索できます。
- **OAuthを使用:** **On**に設定されている場合、接続は認証にOAuthを使用します。デフォルトは**Off**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サービスが使用されていない場合に、OAuthを使用して認証するためにウェブビューにロードするURLを指定します。このフィールドは、**OAuthを使用**が**オン**に設定されている場合に表示されます。
- **パスワード:** Exchangeユーザーアカウントのオプション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:** 内部と外部のExchangeホスト名を異なるものにしたい場合は、オプションの内部Exchangeホスト名を入力します。
- **内部サーバーポート:** 内部と外部のExchangeサーバーポートを異なるものにしたい場合は、オプションの内部Exchangeサーバーポート番号を入力します。
- **内部サーバーパス:** 内部と外部のExchangeサーバーパスを異なるものにしたい場合は、オプションの内部Exchangeサーバーパスを入力します。
- **内部ExchangeホストにSSLを使用:** ユーザーデバイスと内部Exchangeホスト間の接続を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:** 内部と外部のExchangeホスト名を異なるものにしたい場合は、オプションの外部Exchangeホスト名を入力します。
- **外部サーバーポート:** 内部と外部のExchangeサーバーポートを異なるものにしたい場合は、オプションの外部Exchangeサーバーポート番号を入力します。
- **外部サーバーパス:** 内部と外部のExchangeサーバーパスを異なるものにしたい場合は、オプションの外部Exchangeサーバーパスを入力します。
- **外部ExchangeホストにSSLを使用:** ユーザーデバイスと内部Exchangeホスト間の接続を保護するかどうかを選択します。デフォルトは**オン**です。
- **Mail Dropを許可:** 既存のネットワークに接続することなく、ユーザーが2台のMac間でファイルをワイヤレスで共有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。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除の特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから、**常に**、**パスコードが必要**、または**許可しない**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

Windowsデスクトップ/タブレット設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-exchange-windowsdesktop.png)

> **注：**
>
> このポリシーでは、ユーザーパスワードを設定できません。ポリシーをプッシュした後、ユーザーは自分のデバイスからその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が存在す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$user.domainnameを使用すると、ユーザーのドメイン名を自動的に検索できます。
- **ユーザーIDまたはユーザー名:** Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ$user.usernameを使用すると、ユーザー名を自動的に検索できます。
- **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を使用すると、ユーザーのメールアカウントを自動的に検索できます。
- **SSL接続を使用:** ユーザーデバイスとExchange Server間の接続を保護するかどうかを選択します。デフォルトは**オフ**です。
- **同期する過去の日数:** リストで、デバイス上のすべてのコンテンツをExchange Serverと同期する過去の日数をクリックします。デフォルトは**すべてのコンテンツ**です。
- **頻度:** リストで、Exchange Serverからデバイスに送信されるデータを同期する際に使用するスケジュールをクリックします。デフォルトは**到着時**です。
- **ログレベル:** ドロップダウンリストで、Exchangeアクティビティをログに記録する際の詳細レベルを指定するために、**無効**、**基本**、または**詳細**をクリックします。デフォルトは**無効**です。

ファイルデバイスポリシー

ユーザーがAndroidおよびAndroid Enterpriseデバイスでアクセスできるようにファイルを追加および展開できます。ファイルをデバイスに保存するディレクトリを指定します。たとえば、ユーザーに会社のドキュメントまたは.pdfファイルを受け取らせたい場合などです。ファイルをデバイスに展開し、ユーザーにファイルの場所を知らせます。

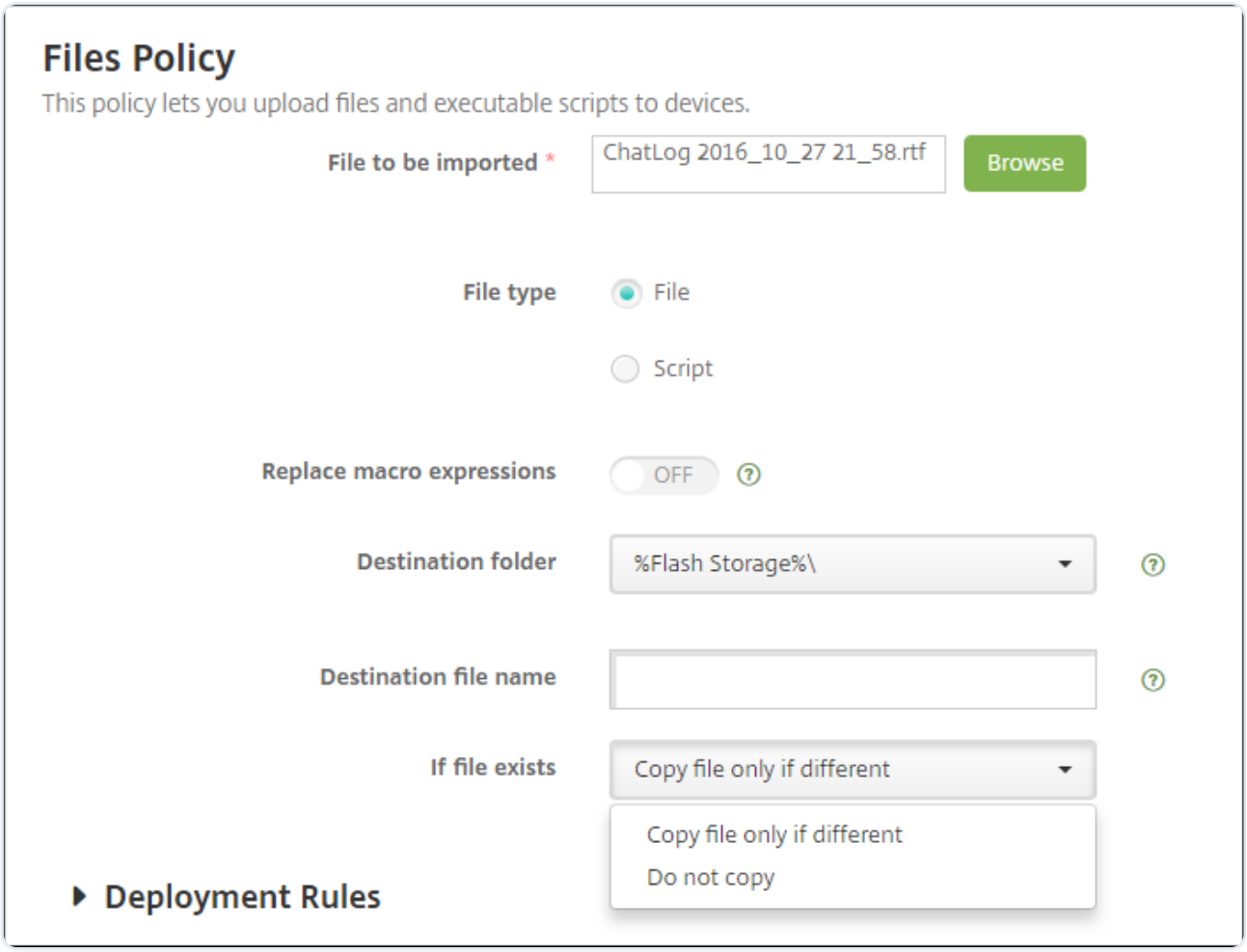
Androidデバイスはスクリプトのネイティブ実行をサポートしていません。ユーザーはスクリプトを実行するためにサードパーティ製ソフトウェアを必要とします。

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）
- その他のファイル（ドキュメント、画像、スプレッドシート、プレゼンテーションなど）

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

アンドロイド エンタープライズ 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、 をクリックしてファイルの場所に移動します。
- **ファイルの種類:** を選択します。
- **保存先フォルダー:** リストからアップロードしたファイルを保存する場所を選択するか、 をクリックしてリストにないファイルの場所を選択します。任意のパス識別子の先頭にマクロ %XenMobile Folder%\ または %Flash Storage%\ を使用できます。
- **保存先ファイル名:** オプション。ファイルを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:** リストから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 です。

Android設定

- **インポートするファイル: 参照**をクリックしてファイルの場所に移動し、インポートするファイルを選択します。
- **ファイルの種類: ファイル**を選択します。

- **保存先フォルダー:** リストからアップロードしたファイルを保存する場所を選択するか、**新規追加**をクリックしてリストにないファイルの場所を選択します。また、パス識別子の先頭として、マクロ %XenMobile Folder%\\ または %Flash Storage%\\ を使用できます。
- **保存先ファイル名:** 必要に応じて、デバイスに展開する前に変更する必要がある場合は、ファイルに別の名前を入力します。
- **異なる場合のみファイルをコピー:** リストで、既存のファイルと異なる場合にファイルをコピーするかどうかを選択します。デフォルトでは、ファイルが異なる場合にのみコピーされます。

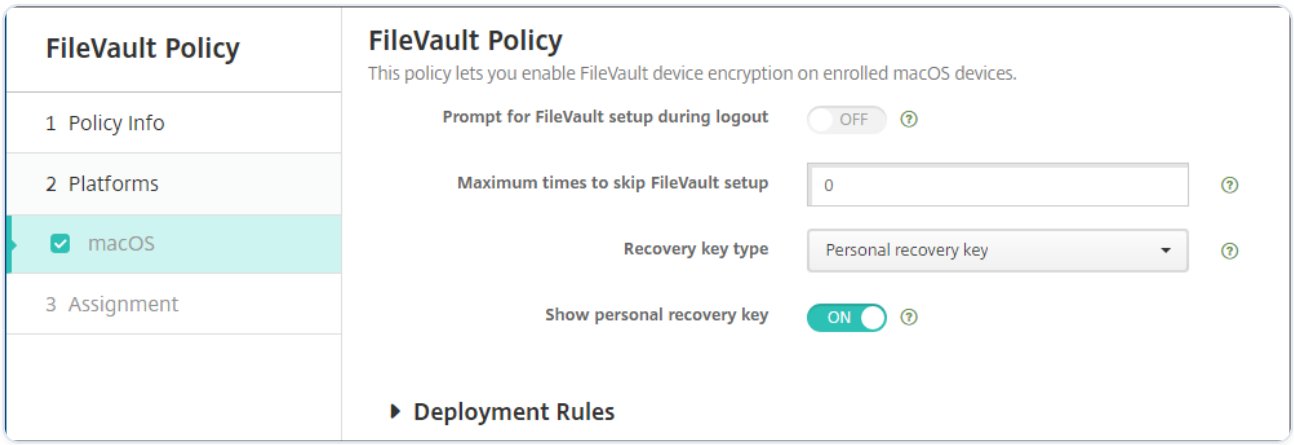
FileVaultデバイスポリシー

macOSのFileVaultディスク暗号化機能は、システムボリュームの内容を暗号化することで保護します。macOSデバイスでFileVaultが有効になっている場合、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紛失した場合、リカバリキーを使用すると、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デバイスポリシーのFileVaultは、FileVaultのユーザー設定画面を有効にし、リカバリキーなどの設定を構成します。FileVaultの詳細については、Appleサポートサイト`<https://support.apple.com>`を参照してください。

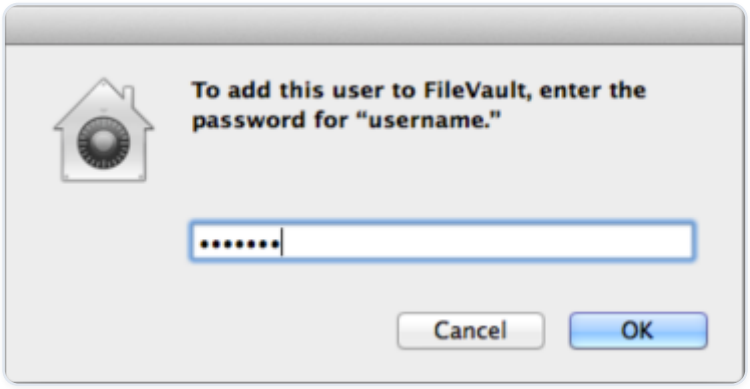
FileVaultポリシーを追加するには、 **>** に移動します。

macOSの設定

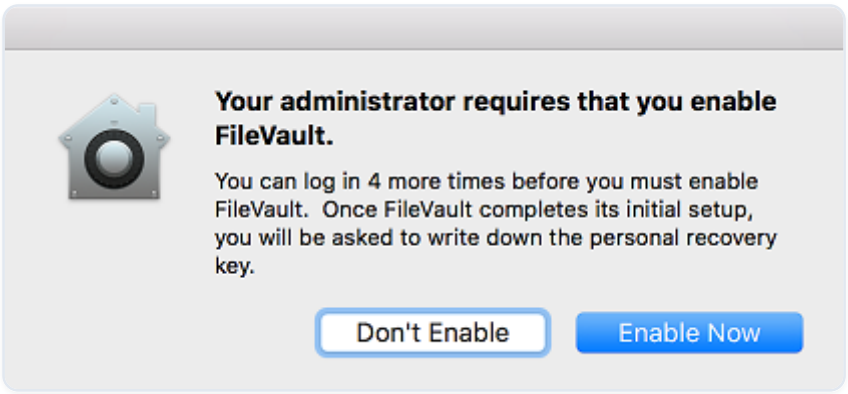


- **ログアウト時にFileVaultセットアップを促す: オン**の場合、**FileVaultセットアップをスキップする最大回数**オプションで指定された次のN回のログアウト時に、ユーザーにFileVaultを有効にするよう促します。**オフ**の場合、FileVaultのパスワードプロンプトは表示されません。

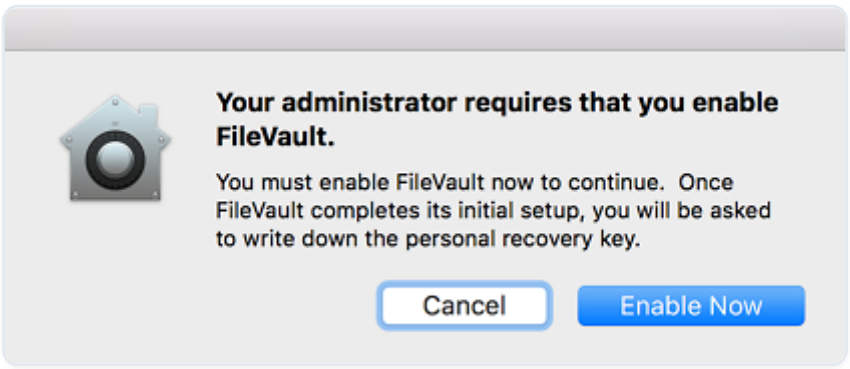
この設定を有効にしてFileVaultポリシーを展開すると、ユーザーがデバイスからサインオフするときに次の画面が表示されます。この画面では、サインオフする前にFileVaultを有効にするオプションがユーザーに提供されます。

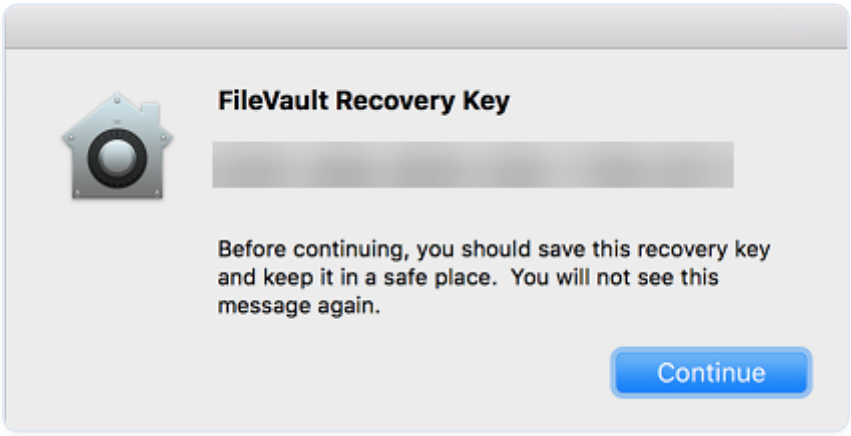


FileVaultセットアップをスキップする最大回数の値が0でない場合: この設定を無効にしてFileVaultポリシーを展開し、その後ユーザーがサインオンすると、次の画面が表示されます。



FileVault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、次の画面が表示されます。





フォントデバイスポリシー

XenMobile® でデバイスポリシーを追加して、iOS および macOS デバイスにフォントを追加できます。フォントは TrueType (`.ttf`) または OpenType (`.oft`) フォント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`) はサポートされていません。

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、 > の順に選択します。詳細については、「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リストに表示される名前を入力します。
- **フォントファイル:** をクリックしてファイルの場所に移動し、ユーザーのデバイスに追加するフォントファイルを選択します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0 以降でのみ利用可能です。

macOS の設定

- **ユーザーに表示される名前:** ユーザーのフォントリストに表示される名前を入力します。
- **フォントファイル:** をクリックしてファイルの場所に移動し、ユーザーのデバイスに追加するフォントファイルを選択します。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

ホーム画面レイアウトデバイスポリシー

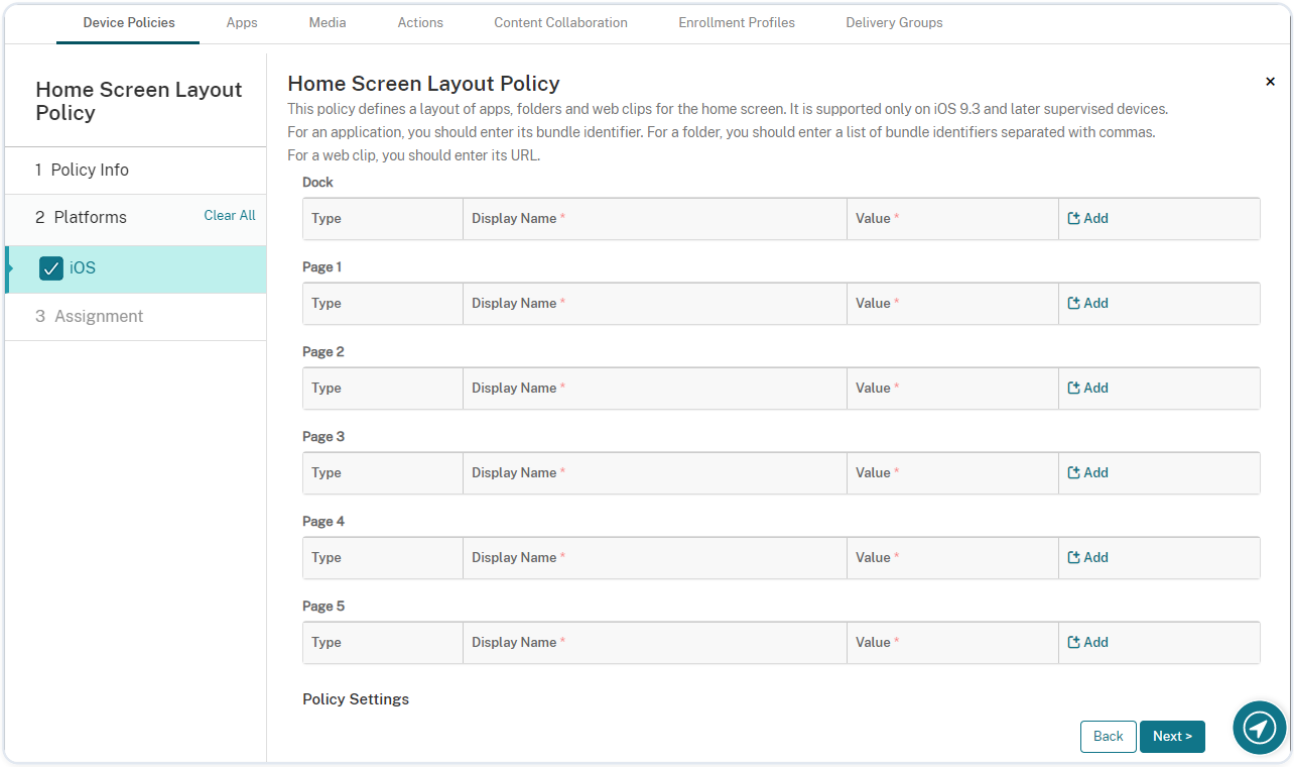
iOSホーム画面のアプリとフォルダのレイアウトを指定できます。**ホーム画面レイアウト**デバイスポリシーは、iOS 9.3以降の監視対象デバイス用です。

重要:

複数のホーム画面レイアウトポリシーを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のいずれかを通じてホーム画面を定義する場合に適用されます。

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**に移動します。詳細については、「デバイスポリシー」を参照してください。

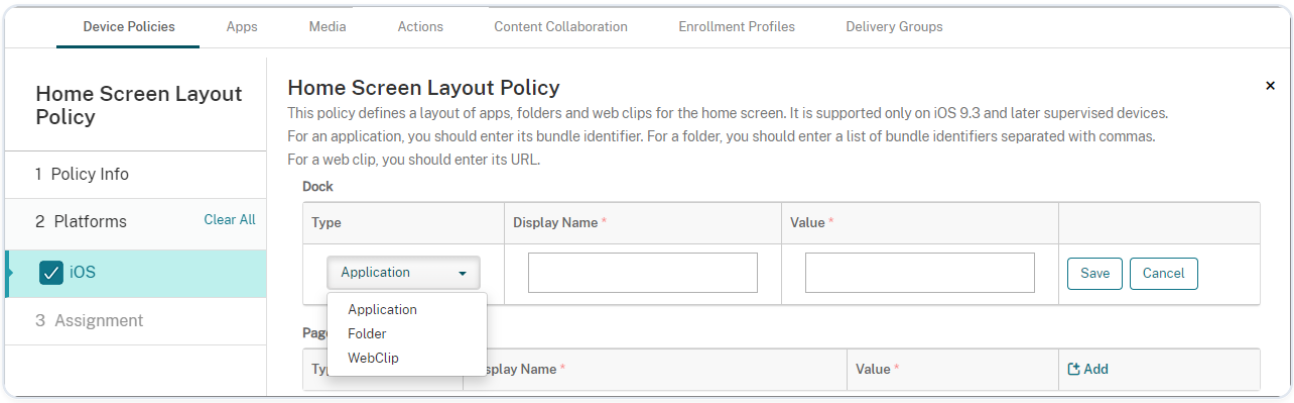
iOS設定



- 構成する画面領域（**Dock**や**ページ1**など）ごとに、**追加**をクリックします。
- **種類: アプリケーション**、**フォルダ**、または**Webクリップ**のいずれかを選択します。

  制限デバイスポリシーの**制限付きアプリの使用 > 一部のアプリのみを許可**設定により、Webクリップがホーム画面に正しく表示されない場合があります。Webクリップを正しく表示するには、次のいずれかを実行します。

  - **制限付きアプリの使用**を**すべてのアプリを許可**または**一部のアプリを許可しない**に設定します。
  - **制限付きアプリの使用**が**一部のアプリのみを許可**に設定されている場合、Webクリップを許可するには、バンドルID `com.apple.webapp` のアプリを追加します。



- **表示名:** アプリまたはフォルダのホーム画面に表示される名前。

- **値:** アプリの場合、バンドル識別子を入力します。フォルダの場合、コンマで区切られたバンドル識別子のリストを入力します。Webクリップの場合、バンドルID `com.apple.webClip.managed` を入力し、WebクリップポリシーでWebクリップのURLを構成します。同じURLを持つWebクリップ値が複数存在する場合、iOS 11.3以降のデバイスでは動作が未定義になります。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはiOS 9.3以降でのみ利用可能です。

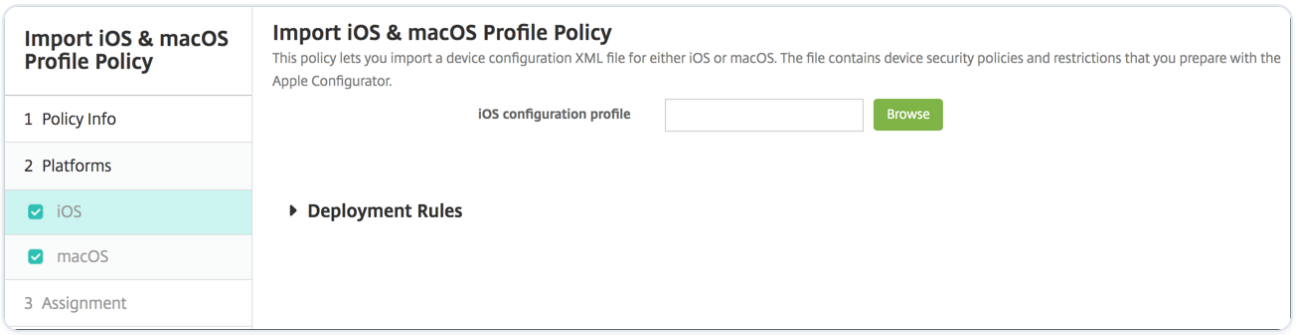
iOSおよびmacOSプロファイルデバイスポリシーのインポート

iOSおよびmacOSデバイス用のデバイス構成XMLファイルをXenMobileにインポートできます。このファイルには、Apple Configuratorで準備したデバイスセキュリティポリシーと制限が含まれています。

この記事の後半で説明するように、Apple Configuratorを使用してiOSデバイスを監視モードにすることができます。Apple Configuratorを使用して構成ファイルを作成する方法の詳細については、AppleのConfigurator Support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、 > に移動します。詳細については、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:** インポートする構成ファイルを選択するには、 をクリックしてファイルの場所に移動します。

Apple Configuratorを使用してiOSデバイスを監視モードにする

Apple Configuratorを使用するには、macOS 10.7.2以降を実行しているAppleコンピュータが必要です。

> **重要:**
>
> デバイスを監視モードにすると、選択したバージョンのiOSがデバイスにインストールされ、以前に保存されていたユーザーデータやアプリはすべて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コンピュータに接続します。
3. Apple Configuratorを起動します。Configuratorは、監視用に準備するデバイスがあることを示します。
4. デバイスを監視用に準備するには:
    a. 「**Supervision**」コントロールを「**On**」に切り替えます。Citrix®では、構成を定期的に再適用することで、デバイスの制御を継続的に維持する予定がある場合に、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. iOSで、インストールする最新バージョンのiOSの「**Latest**」をクリックします。
5. デバイスを監視用に準備する準備ができたら、「**Prepare**」をクリックします。

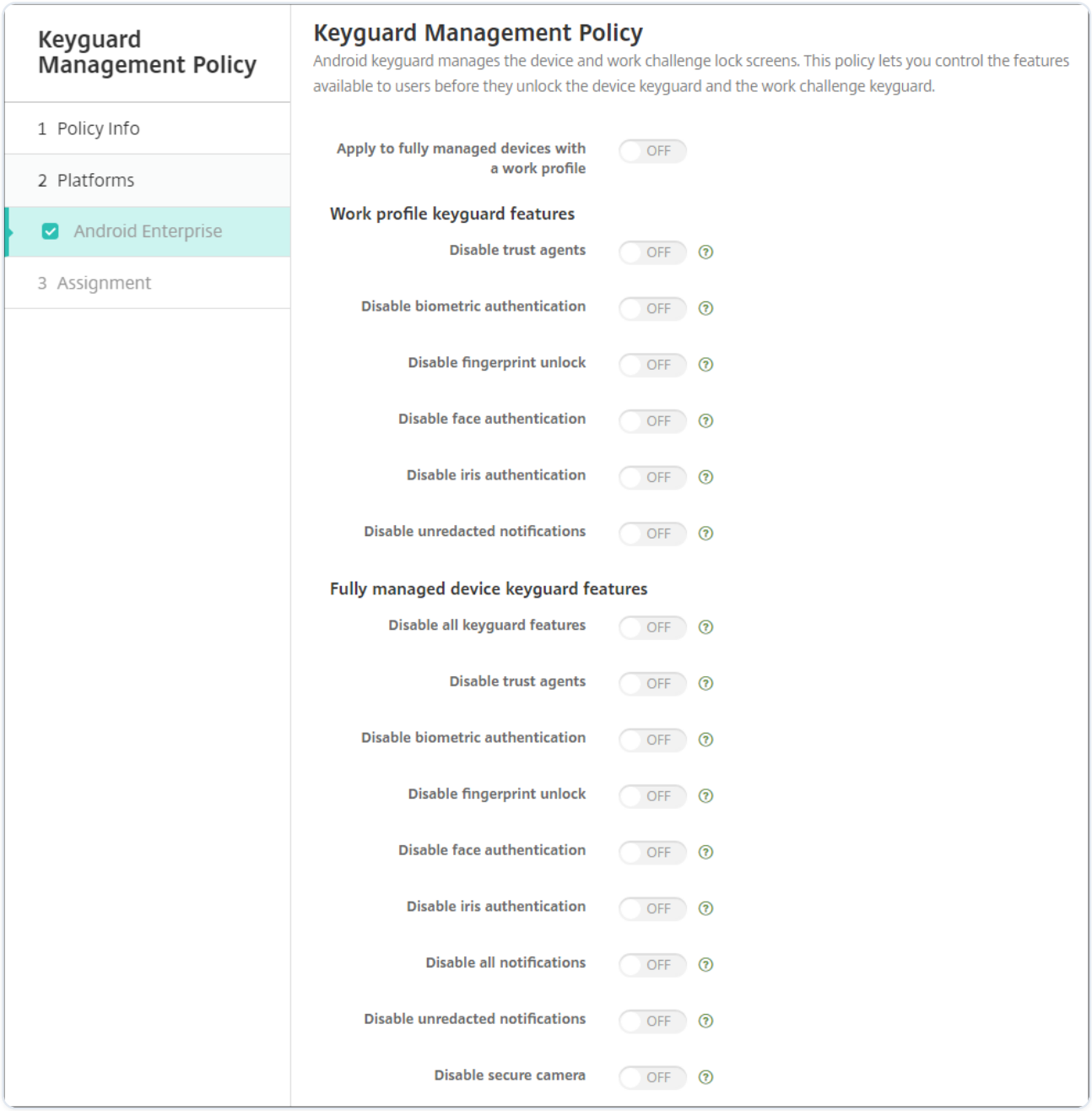
キーガード管理デバイスポリシー

Androidのキーガードは、デバイスと仕事用チャレンジのロック画面を管理します。このポリシーを使用すると、Android Enterpriseの仕事用プロファイルキーガードと高度なデバイスキーガードの機能を管理できます。次の項目を制御できます。

- 仕事用プロファイルデバイスでのキーガード管理。ユーザーがデバイスキーガードと仕事用チャレンジキーガードを解除する前に利用できる機能を指定できます。たとえば、デフォルトでは、ユーザーは指紋認証によるロック解除を使用したり、ロック画面で編集されていない通知を表示したりできます。
- フルマネージドデバイスおよび専用デバイスでのキーガード管理。ユーザーがキーガード画面を解除する前に、信頼エージェントやセキュアカメラなどの利用可能な機能を指定できます。または、すべてのキーガード機能を無効にすることもできます。
- 仕事用プロファイルを持つフルマネージドデバイスでのキーガード管理。1つのキーガード管理ポリシーを使用して、デバイスと仕事用プロファイルに個別の設定を適用できます。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

Android Enterpriseの設定



- **仕事用プロファイルを持つフルマネージドデバイスに適用:** 仕事用プロファイルを持つフルマネージドデバイスのキーガード管理デバイスポリシー設定を構成できます。

  この設定が**オン**の場合、仕事用プロファイルを持つフルマネージドデバイスのデバイスと仕事用プロファイルに個別の設定を適用できます。

  この設定が**オフ**の場合、仕事用プロファイルデバイスまたはフルマネージドデバイスに設定を適用できます。仕事用プロファイル用に構成した設定は、仕事用プロファイルデバイスにのみ適用されます。フルマネージドデバイス用に構成した設定は、フルマネージドデバイスにのみ適用されます。

デフォルトは**オフ**です。

- **仕事用プロファイルのキーガード機能:** ユーザーが仕事用プロファイルのキーガード（ロック画面）を解除する前に、次の機能が利用可能かどうかを制御します。
  - **信頼エージェントを無効にする: オフ**の場合、仕事用プロファイルにチャレンジが設定されているときに、信頼エージェントはセキュアなキーガード画面で動作できます。仕事用プロファイルのすべての信頼エージェントを無効にするには、**オン**に設定します。デフォルトは**オフ**です。
  - **生体認証を無効にする: オフ**の場合、仕事用プロファイルにチャレンジが設定されているときに、セキュアなキーガード画面で生体認証が利用できます。仕事用プロファイルで生体認証を無効にするには、**オン**に設定します。この設定は、指紋認証によるロック解除、顔認証、虹彩認証を無効にします。デフォルトは**オフ**です。Android 9.0以降の場合。
  - **指紋認証ロック解除を無効にする: オン**の場合、ワークプロファイルでチャレンジが設定されている場合、セキュアキーガード画面で指紋認証ロック解除は利用できません。ワークプロファイルで指紋認証ロック解除を有効にするには、**オフ**に設定します。デフォルトは**オフ**です。
  - **顔認証を無効にする: オフ**の場合、ワークプロファイルでチャレンジが設定されている場合、セキュアキーガード画面で顔認証が利用可能です。ワークプロファイルで顔認証を無効にするには、**オン**に設定します。デフォルトは**オフ**です。Android 9.0以降の場合。
  - **虹彩認証を無効にする: オフ**の場合、ワークプロファイルでチャレンジが設定されている場合、セキュアキーガード画面で虹彩認証が利用可能です。ワークプロファイルで虹彩認証を無効にするには、**オン**に設定します。デフォルトは**オフ**です。Android 9.0以降の場合。
  - **編集されていない通知を無効にする: オフ**の場合、編集済みおよび編集されていない通知の両方がセキュアキーガード画面に表示されます。編集されていない通知を無効にし、編集済みの通知のみを表示するには、**オン**に設定します。デフォルトは**オフ**です。
- **フルマネージドデバイスのキーガード機能:** ユーザーがデバイスのキーガード（ロック画面）を解除する前に、以下の機能が利用可能かどうかを制御します。これらの機能は、フルマネージドデバイスまたは専用デバイスに適用されます。
  - **すべてのキーガード機能を無効にする: オフ**の場合、現在および将来のすべてのキーガードカスタマイズがセキュアキーガード画面で利用可能です。すべてのキーガードカスタマイズを無効にするには、**オン**に設定します。デフォルトは**オフ**です。
  - **信頼エージェントを無効にする: オフ**の場合、信頼エージェントはセキュアキーガード画面で動作できます。信頼エージェントを無効にするには、**オン**に設定します。デフォルトは**オフ**です。

- **生体認証を無効にする: オフ**の場合、デバイスでチャレンジが設定されている場合、セキュアキーガード画面で生体認証が利用可能です。デバイスで生体認証を無効にするには、**オン**に設定します。これにより、指紋認証ロック解除、顔認証、および虹彩認証が無効になります。デフォルトは**オフ**です。Android 9.0以降の場合。
- **指紋認証ロック解除を無効にする: オフ**の場合、デバイスでチャレンジが設定されている場合、セキュアキーガード画面で指紋認証ロック解除が利用可能です。デバイスで指紋認証ロック解除を無効にするには、**オン**に設定します。デフォルトは**オフ**です。
- **顔認証を無効にする: オフ**の場合、デバイスでチャレンジが設定されている場合、セキュアキーガード画面で顔認証が利用可能です。デバイスで顔認証を無効にするには、**オン**に設定します。デフォルトは**オフ**です。Android 9.0以降の場合。
- **虹彩認証を無効にする: オフ**の場合、デバイスでチャレンジが設定されている場合、セキュアキーガード画面で虹彩認証が利用可能です。デバイスで虹彩認証を無効にするには、**オン**に設定します。デフォルトは**オフ**です。Android 9.0以降の場合。
- **すべての通知を無効にする: オフ**の場合、すべての通知がセキュアキーガード画面に表示されます。すべての通知を表示するには、**オン**に設定します。デフォルトは**オフ**です。
- **編集されていない通知を無効にする: オフ**の場合、編集済みおよび編集されていない通知の両方がセキュアキーガード画面に表示されます。編集されていない通知を無効にし、編集済みの通知のみを表示するには、**オン**に設定します。デフォルトは**オフ**です。
- **セキュアカメラを無効にする: オフ**の場合、セキュアカメラはセキュアキーガード画面で利用可能です。セキュアカメラを無効にするには、**オン**に設定します。デフォルトは**オフ**です。

キオスクデバイスポリシー

キオスクポリシーを使用すると、実行できる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。XenMobile® は、デバイスのどの部分がキオスクモードでロックされるかを制御しません。ポリシーを展開した後、デバイスが**キオスクモード**の設定を管理します。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

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するすべてのアプリは、ユーザーデバイスにすで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 Mobile Device Management (MDM) API 4.0 以降にのみ適用されます。

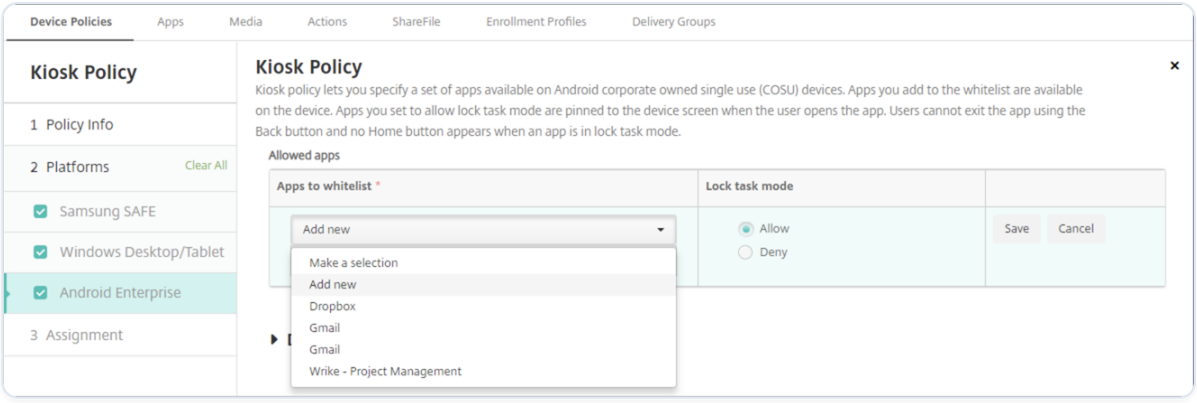
Android Enterprise の設定

専用の Android Enterprise デバイス (企業所有のシングルユース (COSU) デバイスとも呼ばれます) のアプリを許可し、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 サービスは許可リストに含まれています。

アプリを許可するには、 をクリックします。複数のアプリを許可できます。詳細については、「Android Enterprise」を参照してください。

> **注：**
>
> XenMobile Server コンソールには、「ブラックリスト」と「ホワイトリスト」という用語が含まれています。今後のリリースで、これらの用語を「ブロックリスト」と「許可リスト」に変更します。

- **ホワイトリストに登録するアプリ：** ホワイトリストに登録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。
  - をクリックして、リストに表示が承認されている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 Server 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ときに、アプリをデバイス画面に固定するように設定するには、 を選択します。アプリを固定しないように設定するには、 を選択します。デフォルトでは、Secure Hub と Google Play サービスは許可されています。デフォルトは****です。

アプリがロックタスクモードの場合、ユーザーがアプリを開くと、そのアプリはデバイス画面に固定されます。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、サインアウトなどのアプリにプログラムされたアクションを使用してアプリを終了します。

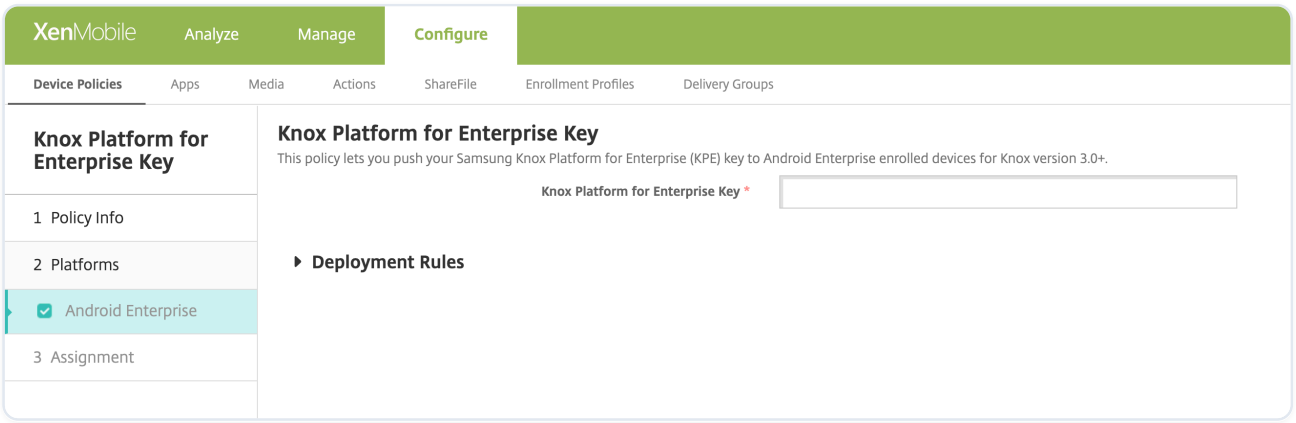
Knox Platform for Enterpriseキーデバイスポリシー

このポリシーを使用すると、必要なSamsung Knox Platform for Enterprise (KPE) ライセンス情報を提供できます。

このポリシーを追加または構成するには、 > 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

このポリシーを使用すると、Samsung Knoxバージョン3.0以降のAndroid Enterpriseプラットフォームに登録されているデバイスに、Samsung Knox Platform for Enterprise (KPE) ライセンスキーをプッシュできます。



Knox Platform for Enterpriseキー: Android EnterpriseデバイスにプッシュするSamsung Knox Platform for Enterprise (KPE) キーを入力します。KPEライセンスキーはSamsung Knox Platform for Enterprise (KPE) キーで申請してください。

ランチャー構成デバイスポリシー

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。

ランチャー構成ポリシーを追加して、以下のCitrix Launcher機能を制御できます。

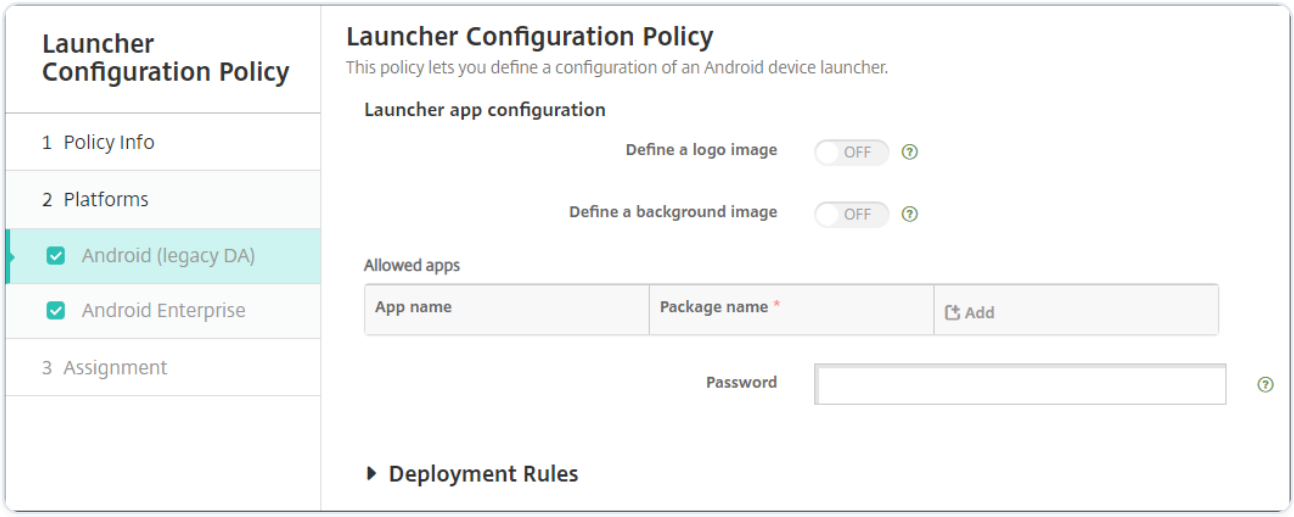
- ユーザーが指定したアプリのみにアクセスできるようにAndroidデバイスを管理します。
- オプションで、Citrix Launcherアイコンのカスタムロゴ画像と、Citrix Launcherのカスタム背景画像を指定します。
- ユーザーがランチャーを終了するために必要なパスワードを指定します。

Citrix Launcherを使用すると、デバイスレベルの制限を適用できますが、ランチャーは、Wi-Fi設定、Bluetooth設定、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アクセスを通じて、ユーザーが必要とする操作上の柔軟性を提供します。Citrix Launcherは、デバイスプラットフォームがすでに提供しているセキュリティの上に、追加のセキュリティ層として意図されたものではありません。

Citrix Launcherを展開すると、XenMobileはそれをインストールし、デフォルトのAndroidランチャーを置き換えます。

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設定



- **ロゴ画像を定義する：** 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：** **［ロゴ画像を定義する］** を有効にすると、**［参照］** をクリックしてファイルの場所を参照し、画像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、GIFです。
- **背景画像を定義する：** 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：** **［背景画像を定義する］** を有効にすると、**［参照］** をクリックしてファイルの場所を参照し、画像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、GIFです。
- **許可されたアプリ:** Citrix Launcherで許可する各アプリについて、**追加**をクリックし、以下を実行します。

  - **追加する新しいアプリ:** 追加するアプリの完全な名前を入力します。例: Androidカレンダーアプリの場合はcom.android.calendar。
  - アプリを追加するには**保存**をクリックするか、アプリの追加をキャンセルするには**キャンセル**をクリックします。

- **パスワード:** ユーザーがCitrix Launcherを終了するために必要なパスワード。

アンドロイド エンタープライズ 設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-launcherconfig-android-enterprise.png)

- **システム情報を有効にする:** Citrix Launcherのステータスバーにシステム情報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。Secure Hub 26.8以降が必要です。
- **ロゴ画像を定義する:** 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: ロゴ画像を定義する**を有効にすると、**参照**をクリックしてファイルの場所に移動し、画像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、GIFです。
- **背景画像を定義する:** 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: 背景画像を定義する**を有効にすると、**参照**をクリックしてファイルの場所に移動し、画像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、GIFです。
- **許可されたアプリ:** Citrix Launcherで許可する各アプリについて、**追加**をクリックし、以下を実行します。
  - **追加する新しいアプリ:** 追加するアプリの完全な名前を入力します。例: Androidカレンダーアプリの場合はcom.android.calendar。
  - アプリを追加するには**保存**をクリックするか、アプリの追加をキャンセルするには**キャンセル**をクリックします。
- **自動起動アプリ:** Citrix Launcherの起動時に自動的に開始する**許可されたアプリ**のいずれかを選択します。デフォルトは**なし** (自動起動しない) です。Citrix Launcher 26.8以降が必要です。
- **パスワード:** ユーザーが Citrix Launcher を終了するために必要なパスワード。

LDAPデバイスポリシー

XenMobile®でiOSデバイス用のLDAPポリシーを作成し、必要なアカウント情報を含む使用するLDAPサーバーに関する情報を提供します。このポリシーは、LDAPサーバーをクエリする際に使用するLDAP検索ポリシーのセットも提供します。

このポリシーを構成する前に、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**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **アカウントの説明:** オプションのアカウントの説明を入力します。
- **アカウントのユーザー名:** オプションのユーザー名を入力します。
- **アカウントのパスワード:** オプションの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でのみ使用してください。
- **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サーバーへの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サーバーをクエリする際に使用する検索設定を追加します。検索設定はいくつでも入力できますが、アカウントを有効にするには少なくとも1つの検索設定を追加する必要があります。**追加**をクリックして、以下を実行します。
  - **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:** LDAPツリーをどこまで深く検索するかを定義するために、**ベース**、**1レベル**、または**サブツリー**を選択します。デフォルトは**ベース**です。
    - **ベース**は、検索ベースが指すノードを検索します。
    - **1レベル**は、ベースノードとその下の1レベルを検索します。
    - **サブツリー**は、深さに関係なく、ベースノードとそのすべての子を検索します。
  - **検索ベース:** 検索を開始するノードへのパスを入力します。例: ou=people または 0=example corp。このフィールドは必須です。
  - 検索設定を追加するには**保存**をクリックし、検索設定の追加をキャンセルするには**キャンセル**をクリックします。
  - 追加する検索設定ごとに、これらの手順を繰り返します。
- **ポリシー設定**

- **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
  - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
  - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

macOS設定

- **アカウントの説明:** オプションのアカウントの説明を入力します。
- **アカウントのユーザー名:** オプションのユーザー名を入力します。
- **アカウントのパスワード:** オプションの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でのみ使用します。
- **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サーバーへの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サーバーをクエリする際に使用する検索設定を追加します。必要なだけ検索設定を入力できますが、アカウントを機能させるには少なくとも1つの検索設定を追加する必要があります。**追加**をクリックし、次の操作を行います。
  - **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:** LDAPツリーをどの深さまで検索するかを定義するために、**Base**、**One level**、または**Subtree**を選択します。デフォルトは**Base**です。
    - **Base**は、検索ベースによって指定されたノードを検索します。
    - **One level**は、Baseノードとその1つ下のレベルを検索します。
    - **Subtree**は、Baseノードとそのすべての子を、深さに関係なく検索します。
  - **検索ベース:** 検索を開始するノードへのパスを入力します。例: ou=people または 0=example corp。このフィールドは必須です。
  - 検索設定を追加するには**保存**をクリックし、検索設定の追加をキャンセルするには**キャンセル**をクリックします。
  - 追加する検索設定ごとに、これらの手順を繰り返します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。

- **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
- **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。

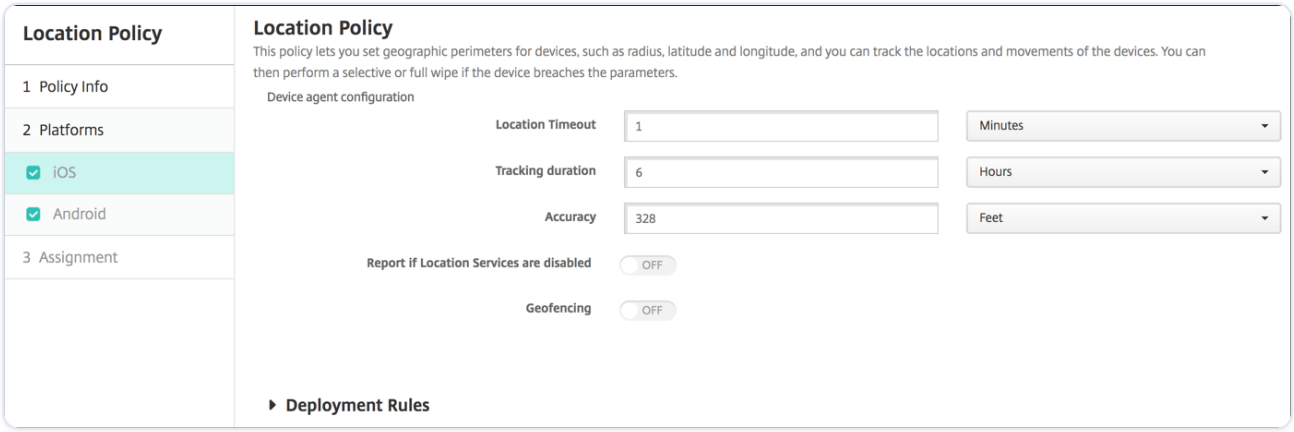
- **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
- **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

位置情報デバイスポリシー

XenMobileで地理的境界を適用するために、位置情報デバイスポリシーを作成します。ユーザーが定義された境界（*ジオフェンス*とも呼ばれます）を越えた場合、XenMobileは特定のアクションを実行できます。たとえば、定義された境界を越えたときにユーザーに警告メッセージを発行するようにポリシーを設定できます。また、境界を越えたときに、すぐに、または遅延後に、ユーザーの企業データをワイプするようにポリシーを設定することもできます。デバイスの追跡や位置特定などのセキュリティアクションについては、「セキュリティアクション」(/ja-jp/xenmobile/server/provision-devices/security-actions.html)を参照してください。

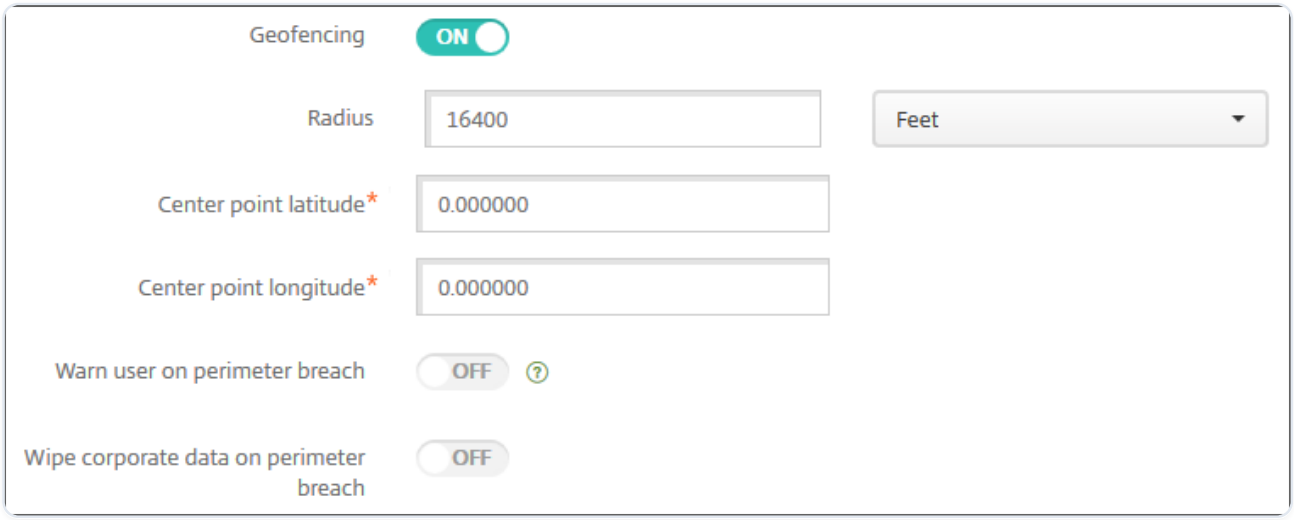
このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」(/ja-jp/xenmobile/server/policies.html)を参照してください。

iOS設定



- **位置情報タイムアウト:** 数値を入力し、リストから または をクリックして、XenMobile®がデバイスの位置情報を取得しようと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、リストから または をクリックして、XenMobileがデバイスを追跡する期間を設定します。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、リストから 、、または をクリックして、XenMobileがデバイスを追跡する際のデバイスへの近接度を設定します。有効な値は10～5000ヤードまたはメートル、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な場合のレポート:** GPSが無効になっている場合に、デバイスが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 です。
- **ジオフェンシング**

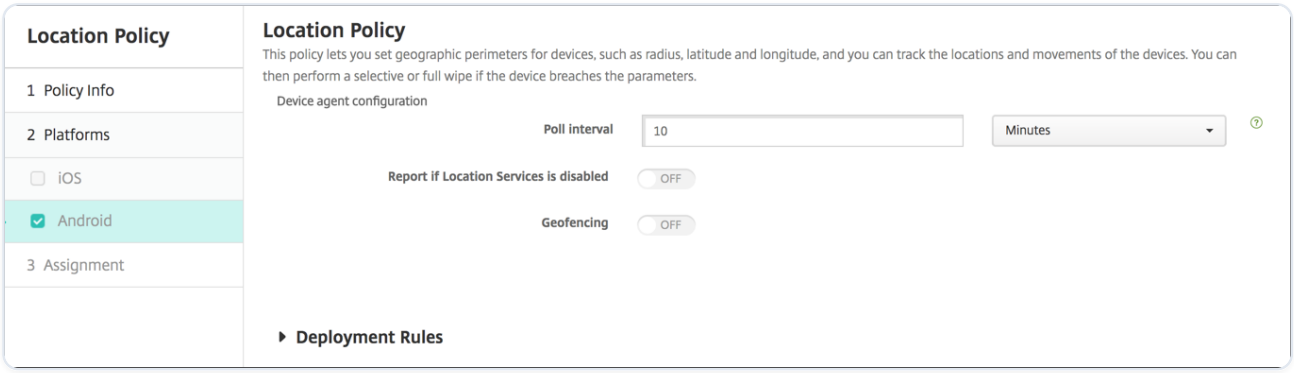


ジオフェンシングを有効にすると、次の設定を構成します。

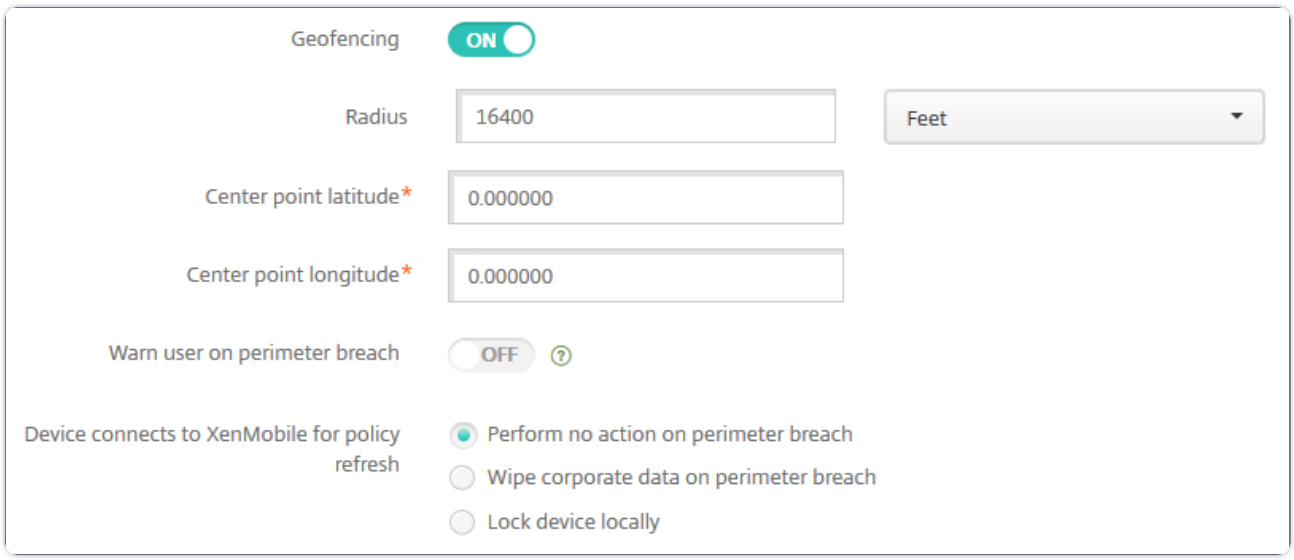
- **半径:** 数値を入力し、リストから半径の測定に使用する単位をクリックします。デフォルトは16,400フィートです。半径の有効な値は次のとおりです。
  - 164～164000フィート
  - 50～50000メートル
  - 54～54680ヤード
  - 1～31マイル
- **中心点の緯度:** 37.787454などの緯度を入力して、ジオフェンスの中心点の緯度を定義します。
- **中心点の経度:** 122.402952などの経度を入力して、ジオフェンスの中心点の経度を定義します。
- **境界侵害時にユーザーに警告:** ユーザーが定義された境界を侵害したときに警告メッセージを発行するかどうかを選択します。デフォルトは**オフ**です。警告メッセージを表示するためにXenMobileへの接続は必要ありません。

- **境界侵害時に企業データをワイプ:** ユーザーが境界を侵害したときにデバイスを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、**ローカルワイプの遅延フィールド**が表示されます。
    - 数値を入力し、リストで**秒**または**分**をクリックして、ユーザーのデバイスから企業データをワイプするまでの遅延時間を設定します。この設定により、XenMobileがデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは0秒です。

Android設定



- **ポーリング間隔:** 数値を入力し、リストで**分**、**時間**、または**日**をクリックして、XenMobileがデバイスの位置を特定しようと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な場合に報告:** GPSが無効な場合にデバイスが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有効にすると、次の設定を構成します。

- **半径:** 数値を入力し、リストで半径の測定に使用する単位をクリックします。デフォルトは16,400フィートです。半径の有効な値は次のとおりです。
    - 164〜164000 フィート
    - 1〜50 キロメートル
    - 50〜50000 メートル
    - 54〜54680 ヤード
    - 1〜31 マイル
- **中心点の緯度:** 37.787454 のような緯度を入力して、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:** 122.402952 のような経度を入力して、ジオフェンスの中心点の経度を定義します。
- **境界侵犯時にユーザーに警告:** ユーザーが定義された境界を侵犯したときに警告メッセージを発行するかどうかを選択します。デフォルトは **オフ** です。警告メッセージを表示するために XenMobile への接続は必要ありません。
- **デバイスがポリシー更新のために XenMobile に接続:** ユーザーが境界を侵犯したときの次のオプションのいずれかを選択します。
    - **境界侵犯時にアクションを実行しない:** 何もしません。この設定がデフォルトです。
    - **境界侵犯時に企業データをワイプ:** 指定された期間の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、**ローカルワイプの遅延** フィールドが表示されます。
        - 数値を入力し、リストで または をクリックして、ユーザーのデバイスから企業データをワイプするまでの遅延時間を設定します。この設定により、XenMobile がデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは 0 秒です。
    - **ロックの遅延:** 指定された期間の後にユーザーのデバイスをロックします。このオプションを有効にすると、**ロックの遅延** フィールドが表示されます。
        - 数値を入力し、リストで または をクリックして、ユーザーのデバイスをロックするまでの遅延時間を設定します。この設定により、XenMobile がデバイスをロックする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは 0 秒です。

アンドロイド エンタープライズ 設定

Androidの位置追跡が機能するためには、以下の要件が満たされていることを確認してください。

- Android 8.5以降
- Android Enterpriseの制限デバイスポリシーで**位置情報共有を許可**設定が有効になっていること
- 接続スケジューリング（Firebase Cloud Messagingを推奨）

デバイスポリシー設定画面(/en-us/xenmobile/server/media/device-policy-location-android-enterprise.png)

ワークプロファイルを持つ完全に管理されたデバイスに適用

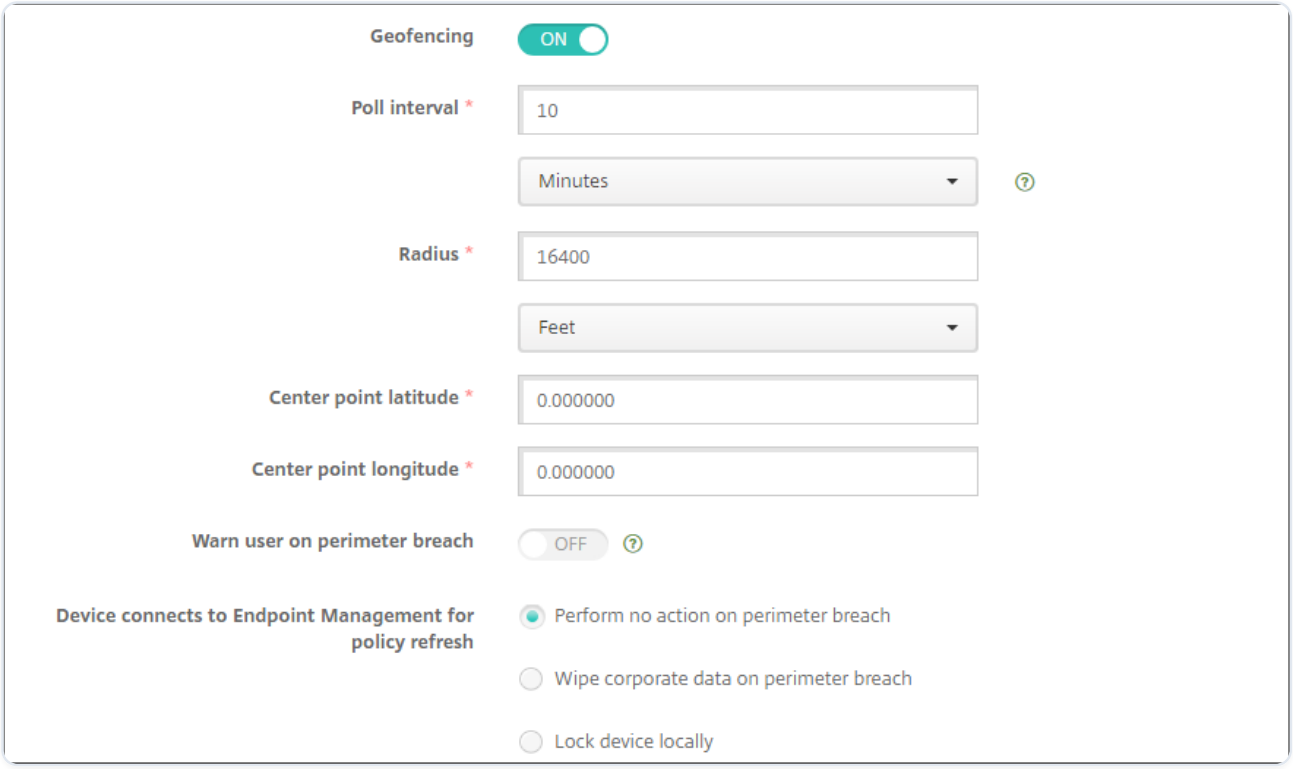
ワークプロファイルを持つ完全に管理されたデバイスでは、位置情報モード設定のみが利用可能です。

- **ワークプロファイルを持つ完全に管理されたデバイスに適用/企業所有デバイス上のワークプロファイル:** ワークプロファイルを持つ完全に管理されたデバイスの位置情報モードを構成できます。この設定がオンの場合、ワークプロファイルの位置情報モード設定を構成します。
  - **位置情報サービスが無効になっている場合に報告:** ユーザーがGPSをオフにしたときに、デバイスが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:** この記事の管理対象デバイスの下にある設定を参照してください。

ワークプロファイルを持つ完全に管理されたデバイスに適用/企業所有デバイス上のワークプロファイルがオフの場合、設定は以下のセクションに示すように、管理対象デバイスとワークプロファイルに適用されます。デフォルトは**オフ**です。

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程度を指定します。**検索**セキュリティアクションは、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にのみ使用できます。デフォルトは「高精度」です。
  - **高精度:** GPS、ネットワーク、その他のセンサーを含むすべての位置情報検出方法を有効にします。
  - **センサーのみ:** GPSとその他のセンサーのみを有効にします。
  - **バッテリー節約:** ネットワークロケーションプロバイダーのみを有効にします。
  - **オフ:** 位置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有効にすると、次の設定を構成します。

- **ポーリング間隔:** 数値を入力し、**分**、**時間**、または**日**をクリックして、XenMobile Serverがデバイスの位置を特定しようと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与える可能性があります。
- **半径:** 数値を入力し、半径の測定に使用する単位をクリックします。デフォルトは**16400フィート** (**5000メートル**) です。半径の有効な値は次のとおりです。
  - 164～164000フィート
  - 1～50キロメートル
  - 50～50000メートル
  - 54～54680ヤード
  - 1～31マイル
- **中心点の緯度:** 37.787454などの緯度を入力して、ジオフェンスの中心点の緯度を定義します。値を確認するには、 **>** に移動し、デバイスを選択して、 をクリックし、 をクリックします。デバイスを検索した後、XenMobile Serverは**** の下の** > ** ページにデバイスの位置を報告します。
- **中心点の経度:** 122.402952などの経度を入力して、ジオフェンスの中心点の経度を定義します。

- **境界侵害時にユーザーに警告:** ユーザーが定義された境界を侵害したときに警告メッセージを発行するかどうかを選択します。デフォルトは**オフ**です。警告メッセージを表示するためにXenMobile Serverへの接続は必要ありません。
- **ポリシー更新のためにXenMobile Serverにデバイスが接続する:** ユーザーが境界を越えた場合のオプションを以下から選択します。
  - **境界侵害時にアクションを実行しない:** 何もしません。この設定がデフォルトです。
  - **境界侵害時に企業データをワイプする:** 指定された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、**ローカルワイプの遅延**フィールドが表示されます。
    - 数値を入力し、**秒**または**分**をクリックして、ユーザーデバイスから企業データをワイプするまでの遅延時間を設定します。この遅延により、XenMobile Serverがデバイスを選択的にワイプする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは**0秒**です。
  - **デバイスをローカルでロックする:** 指定された時間後にユーザーのデバイスをロックします。このオプションを有効にすると、**ロックの遅延**フィールドが表示されます。
    - 数値を入力し、**秒**または**分**をクリックして、ユーザーデバイスをロックするまでの遅延時間を設定します。この遅延により、XenMobile Serverがデバイスをロックする前に、ユーザーは許可された場所に戻る機会を得られます。デフォルトは**0秒**です。

管理対象プロファイル

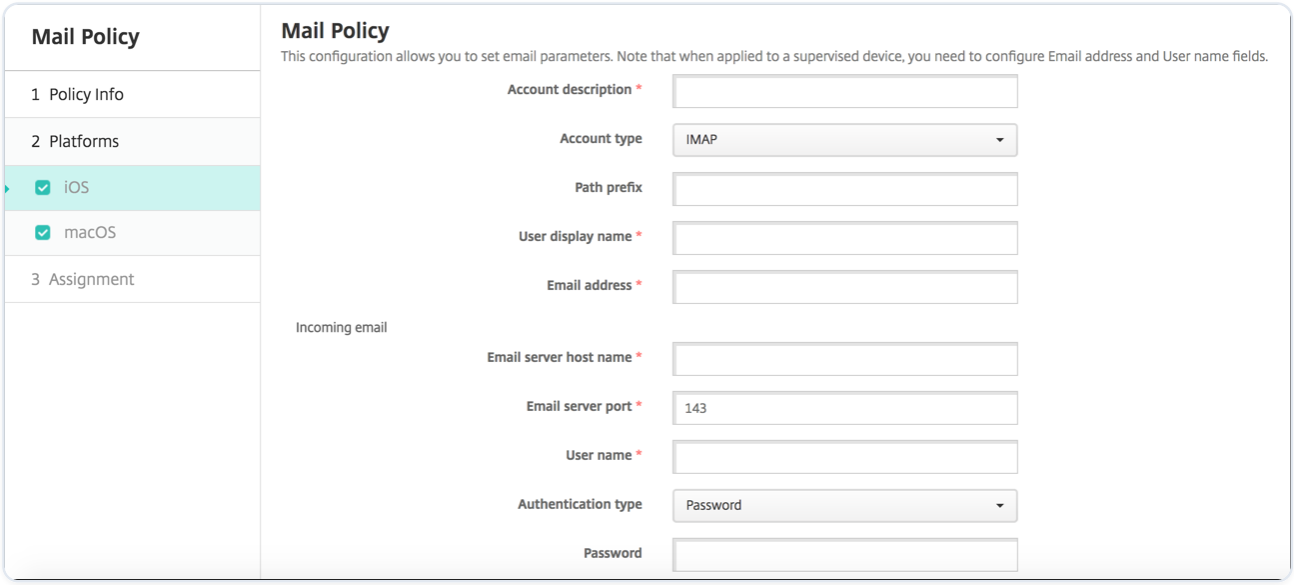
- **位置情報サービスが無効になっている場合に報告する:** ユーザーがGPSをオフにしたときに、デバイスがXenMobile Serverにレポートを送信するかどうかを選択します。デフォルトは**オフ**です。
- **ジオフェンシング:** この記事の管理対象デバイスにある設定を参照してください。

メールデバイスポリシー

XenMobile®でメールデバイスポリシーを追加して、iOSまたはmacOSデバイスでメールアカウントを構成できます。

このポリシーを追加または構成するには、 **>** に移動します。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:** メールアプリと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:** ユーザーアカウントに使用するプロトコルとして、**IMAP**または**POP**のいずれかを選択します。デフォルトは**IMAP**です。**POP**を選択すると、以下の**パス**プレフィックスオプションは表示されなくなります。
- **パスプレフィックス: INBOX**またはIMAPメールアカウントのパス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に使用するフル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。この名前は通常、@記号までのメールアドレスと同じです。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**を選択すると、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:** 受信メールサーバーのオプション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が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い場合、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。この名前は通常、@文字までのメールアドレスと同じです。このフィールドは必須です。
  - **認証タイプ:** 使用する認証タイプを選択します。デフォルトは**パスワード**です。
  - **パスワード:** 送信メールサーバーのオプションのパスワードを入力します。
  - **送信パスワードを受信パスワードと同じにする:** 受信パスワードと送信パスワードが同じ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が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**
  - **アカウント間のメール移動を許可:** ユーザーがこのアカウントから別のメールアカウントにメールを移動したり、別のメールアカウントから転送および返信したり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。
  - **メールアプリからのみメールを送信:** ユーザーがメールの送信にiOSメールアプリのみを使用するよう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にする:** ユーザーが最近のアドレスを同期するのを防ぐ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。
  - **Mail Dropを許可:** iOS 9.2以降を実行しているデバイスで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署名を有効にする:** このアカウントがS/MIME署名をサポートするかどうかを選択します。デフォルトは**オン**です。**オン**に設定すると、以下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。
    - **S/MIME署名ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定でS/MIME署名をオン/オフできます。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署名証明書UUIDユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定で、使用する署名資格情報を選択できます。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暗号化を有効にする:** このアカウントが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**に設定すると、以下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切り替えを有効にする: オン**に設定すると、ユーザーが作成する各メッセージに対してS/MIME暗号化をオンまたはオフに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。
    - **S/MIMEデフォルト暗号化ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定で、S/MIMEをデフォルトでオン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ユーザーによる上書き可能: オン**に設定すると、ユーザーはデバイスの設定でS/MIME暗号化IDと暗号化をオン/オフできます。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。

- **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、この設定を構成して、**日付を選択**してポリシーを削除するか、**削除までの期間（時間）**でポリシーを削除できます。
    - **ユーザーによるポリシーの削除を許可:** ユーザーがメールポリシーを**常に**削除できるようにするか、**パスコードが必要**な場合のみ削除できるようにするか、**許可しない**かを設定します。
    - **プロファイルスコープ:** 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**に適用するかを選択します。

管理対象構成ポリシー

管理対象構成デバイスポリシーは、さまざまなアプリ構成オプションとアプリ制限を制御します。アプリ開発者は、アプリで利用可能なオプションとツールヒントを定義します。ツールヒントに「テンプレート値」の使用が記載されている場合は、対応するXenMobileマクロを使用してください。詳細については、リモート構成の概要 (Android開発者サイト上) およびマクロを参照してください。

アプリ構成設定には、次のような項目を含めることができます。

- アプリのメール設定
- WebブラウザのURLを許可またはブロックする
- モバイルデータ通信またはWi-Fi接続のみによるアプリコンテンツ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は、アプリ開発者にお問い合わせください。

前提条件

- GoogleでAndroid Enterpriseのセットアップタスクを完了し、Android Enterpriseを管理対象Google Playに接続します。詳細については、Android Enterpriseを参照してください。
- Android EnterpriseアプリをXenMobileに追加します。詳細については、XenMobileへのアプリ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、 > に移動します。詳細については、デバイスポリシーを参照してください。

アプリごとのVPNの要件

AE用のアプリごとのVPNを作成するには、管理対象構成ポリシーの構成に加えて、追加の手順を実行する必要があります。また、次の前提条件が満たされていることを確認する必要があります。

- オンプレミスCitrix Gateway
- デバイスに次のアプリケーションがインストールされています。
  - シトリックス SSO
  - シトリックス セキュアハブ™

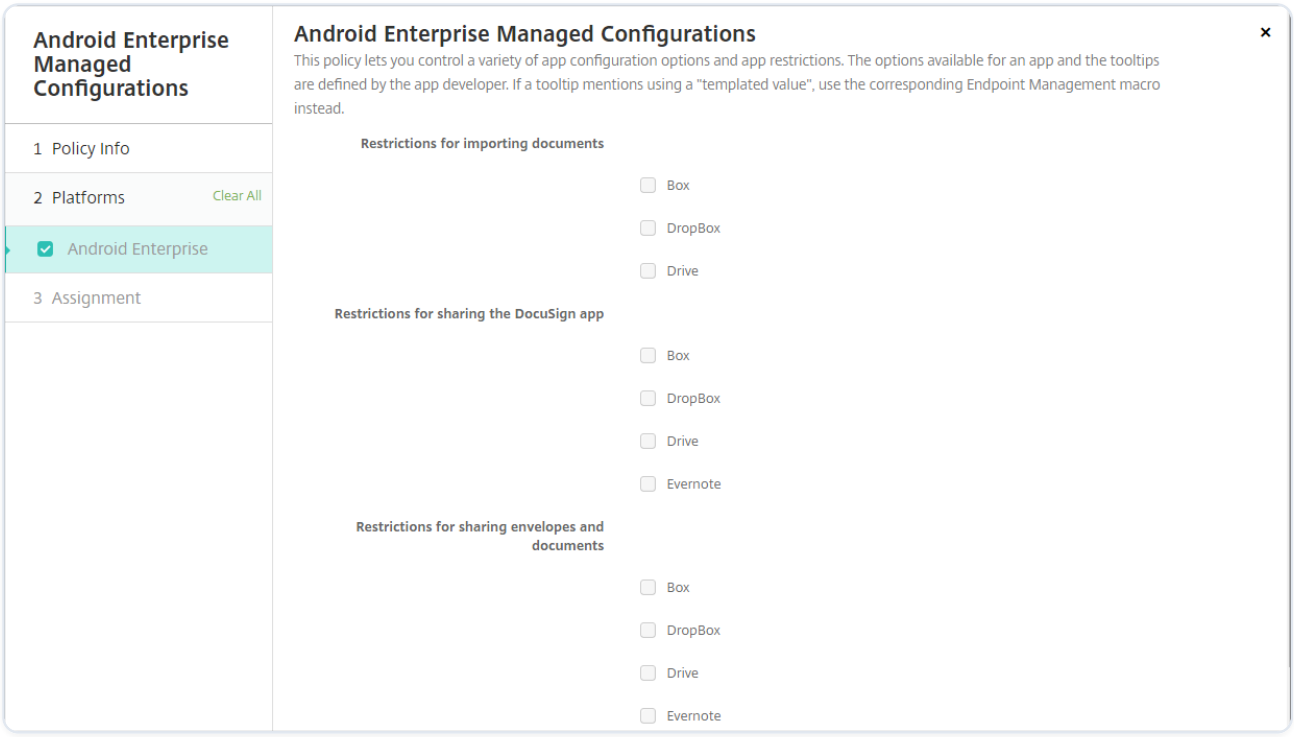
AEデバイスのアプリごとのVPNを構成するための一般的なワークフローは次のとおりです。

1. この記事で説明されているように、VPNプロファイルを構成します。
2. アプリごとのVPNからのトラフィックを受け入れるようにCitrix ADCを構成します。詳細については、Citrix Gatewayでの完全なVPNセットアップを参照してください。

Android Enterpriseの設定

管理対象構成デバイスポリシーの追加を選択すると、アプリを選択するためのプロンプトが表示されます。XenMobile®にAndroid Enterpriseアプリが追加されていない場合、続行できません。

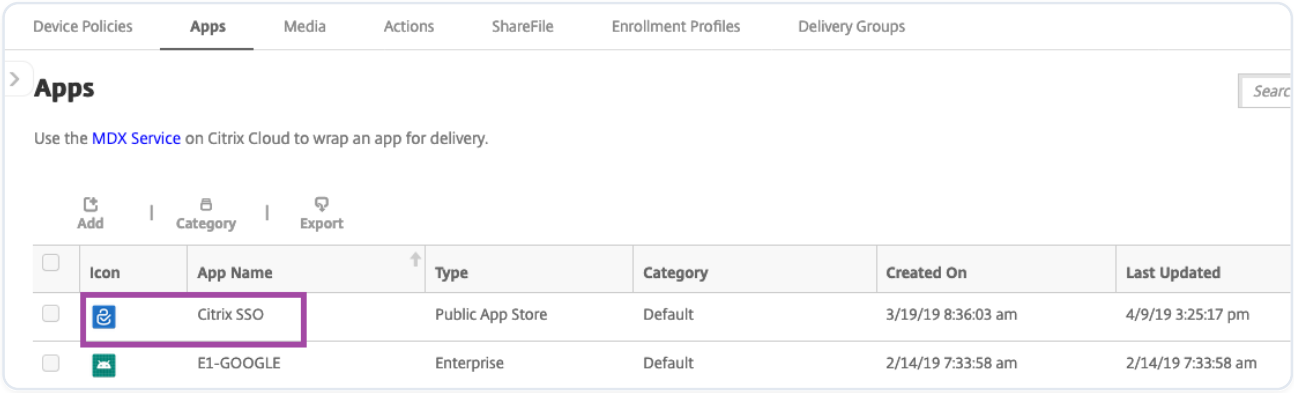
アプリを選択したら、ポリシー設定を構成します。設定は各アプリに固有です。



Android EnterpriseのVPNプロファイルを構成する

管理対象構成デバイスポリシーを使用してCitrix SSOアプリで、Android Enterpriseデバイスに VPNプロファイルを利用可能にします。

まず、Citrix SSOをGoogle PlayストアアプリとしてXenMobileコンソールに追加します。パブリックアプリストアアプリの追加を参照してください。



Citrix SSO用のAndroid Enterprise管理対象構成を作成する

VPNプロファイルを作成するために、Citrix SSOの管理対象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、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 FQDN とポートが必要です。

1. XenMobile コンソールで、 > をクリックします。 をクリックします。

2. を選択します。 をクリックします。

   Android Enterprise ポリシーの選択の画像 (/en-us/xenmobile/server/media/select-ae-managed-configuration-policy.png)

3. ウィンドウが表示されたら、リストから を選択し、 をクリックします。

   アプリケーション ID の選択ウィンドウの画像 (/en-us/xenmobile/server/media/citrix-sso-select-app-id.png)

4. Citrix SSO VPN 構成の名前と説明を入力します。 をクリックします。

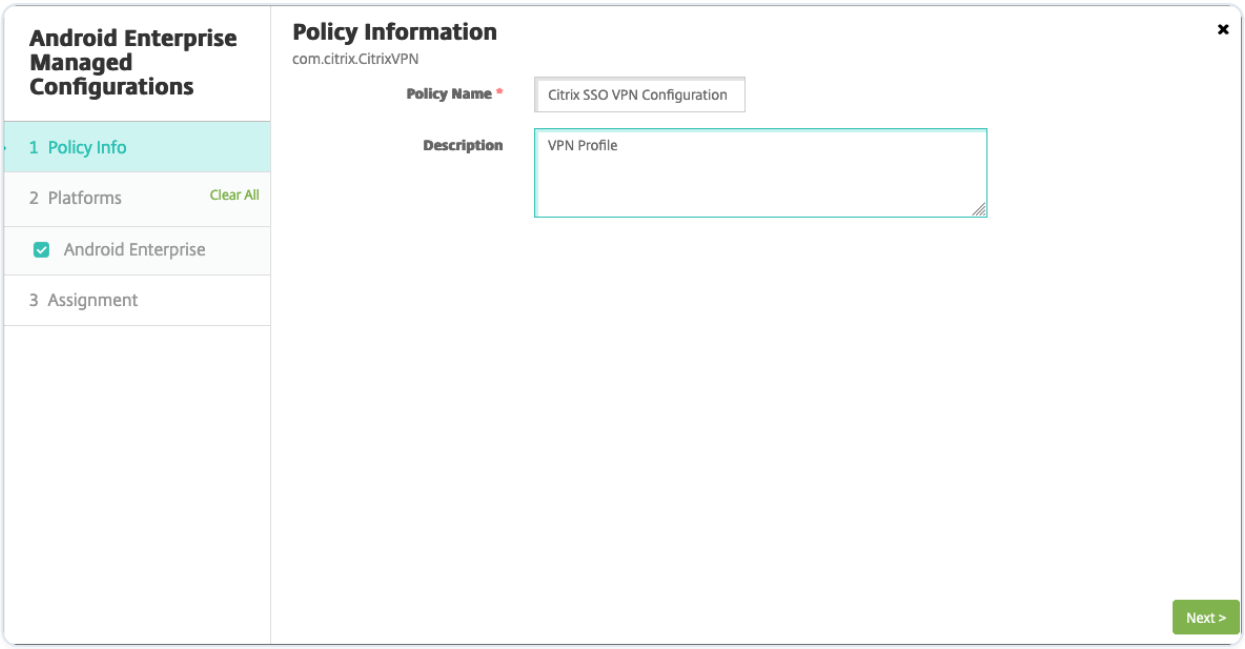
   Android Enterprise 管理対象構成ウィザードの画像 (/en-us/xenmobile/server/media/citrix-sso-ae-managed-config-1.png)

5. VPN プロファイルパラメータを構成します。

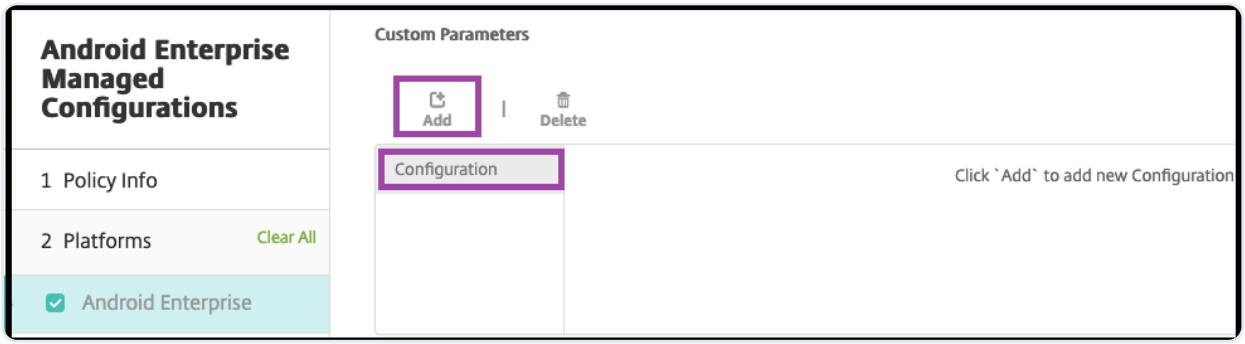
   - **VPN プロファイル名。** VPN プロファイルの名前を入力します。複数の VPN プロファイルを作成する場合は、それぞれに一意の名前を使用します。名前を指定しない場合、 フィールドに入力したアドレスが VPN プロファイル名として使用されます。
   - **サーバーアドレス(*)。** Citrix Gateway FQDN を入力します。Citrix Gateway のポートが 443 でない場合は、ポートも入力します。URL 形式を使用します。例: `https://gateway.mycompany.com:8443`。
   - **ユーザー名 (オプション)。** エンドユーザーが Citrix Gateway へ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）。ユーザー名を指定しない場合、ユーザーは Citrix Gateway に接続する際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 への認証に使用するパスワードを入力します。パスワードを指定しない場合、ユーザーは Citrix Gateway に接続する際に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)。** 証明書エイリアスを入力します。証明書エイリアスを使用すると、アプリが証明書にアクセスしやすくなります。同じ証明書エイリアスが資格情報デバイスポリシーとともに使用される場合、アプリは証明書を取得し、ユーザーによる操作なしで VPN を認証します。
   - **アプリごとの VPN タイプ (オプション)。** この VPN を使用するアプリを制限するためにアプリごとの VPN を使用している場合は、この設定を構成できます。 を選択すると、 にリストされているアプリパッケージ名のネットワークトラフィックは VPN を介してルーティングされます。他のすべてのアプリのネットワークトラフィックは VPN の外部にルーティングされます。 を選択すると、 にリストされているアプリパッケージ名のネットワークト

ラフィックは VPN の外部にルーティングされます。他のすべてのアプリのネットワークトラフィックは VPN を介してルーティングされます。デフォルトは です。

- **PerAppVPNアプリリスト。** VPN上でトラフィックが許可またはブロックされるアプリのリストです。「**Per-App VPN Type**」の値によって異なります。アプリのパッケージ名をコンマまたはセミコロンで区切ってリストします。アプリのパッケージ名は大文字と小文字を区別し、Google Playストアに表示されているとおりにこのリストに正確に記載する必要があります。このリストはオプションです。デバイス全体のVPNをプロビジョニングする場合は、このリストを空のままにします。
- **デフォルト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代わりに、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ときに使用するVPNプロファイルの名前を入力します。このフィールドが空の場合、メインプロファイルが接続に使用されます。プロファイルが1つしか構成されていない場合、それはデフォルトプロファイルとしてマークされます。常時接続VPNの場合、このフィールドには常時接続VPNを確立するために使用されるVPNプロファイルの名前を設定する必要があります。
- **ユーザープロファイルを無効にする。** この設定がON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OFF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OFFです。
- **信頼できないサーバーをブロックする。** Citrix Gatewayに自己署名証明書を使用している場合、またはCitrix Gateway証明書を発行するCAのルート証明書がシステムCAリストにない場合、この設定はOFFになります。この設定がONの場合、Androidオペレーティングシステムは Citrix Gateway証明書を検証します。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ONです。

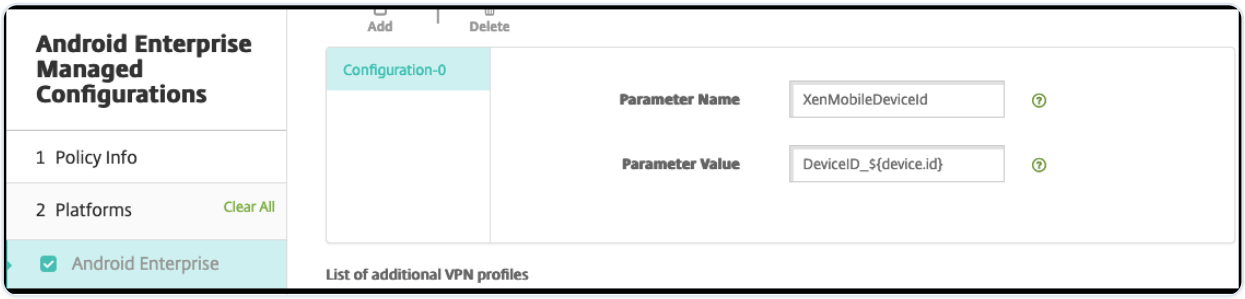


6. オプションで、カスタムパラメータを作成します。カスタムパラメータ「**XenMobileDeviceId**」と「**UserAgent**」がサポートされています。現在のVPN構成を選択し、「**追加**」をクリックします。



a. カスタムパラメータを作成します。

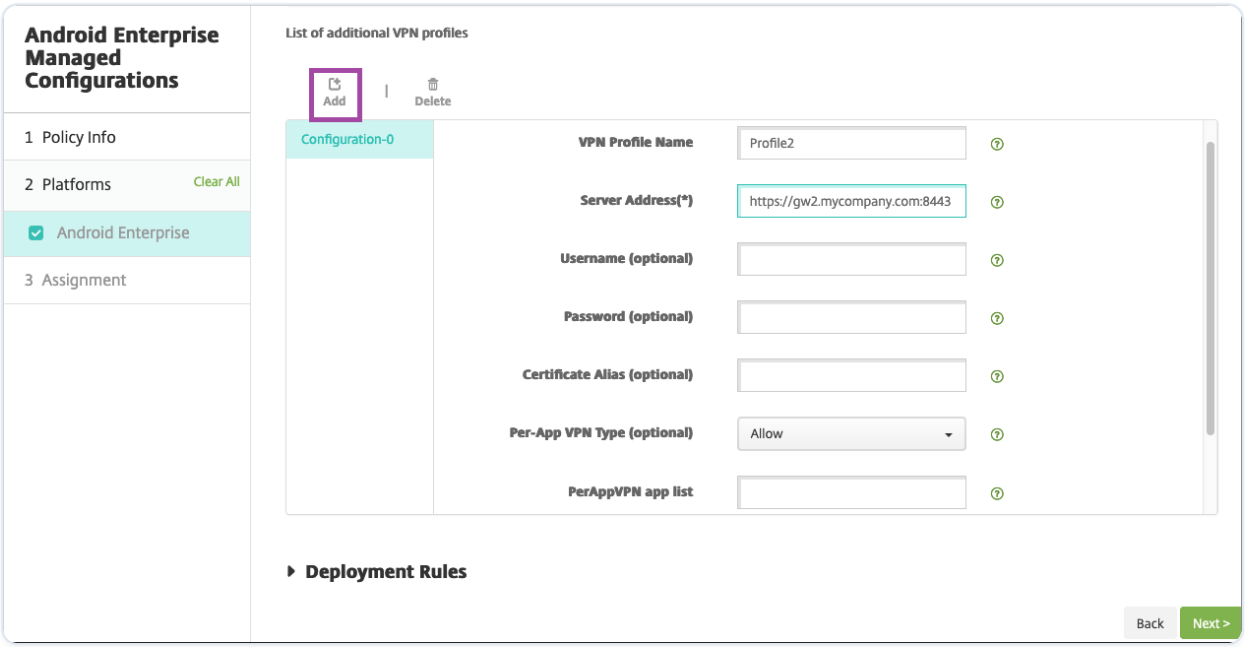
- **パラメータ名。**「**XenMobileDeviceId**」と入力します。このフィールドは、XenMobileでのデバイス登録に基づいてネットワークアクセスチェックに使用するデバイスIDです。XenMobileがデバイスを登録および管理している場合、VPN接続は許可されます。それ以外の場合、VPN確立時に認証が拒否されます。
- **パラメータ値** XenMobileがデバイスの登録および管理状態を判断するには、XenMobileDeviceIDの値を `DeviceID_${device.id}` に設定します。



a. 別のカスタムパラメータを作成するには、もう一度「**追加**」をクリックします。このカスタムパラメータを作成します。

- **パラメータ名。**「**UserAgent**」と入力します。このテキストは、Citrix Gatewayで追加のチェックを行うためにUser-Agent HTTPヘッダーに追加されます。このテキストの値は、Citrix SSOアプリがCitrix Gatewayと通信する際に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テキストを入力します。このテキストはHTTP User-Agentの仕様に準拠している必要があります。

7. オプションで、さらにVPNプロファイル構成を作成します。構成リストの下にある「**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を繰り返し、オプションで手順6も繰り返します。



8. 必要なすべてのVPNプロファイルを作成したら、**次へ**をクリックします。
9. Citrix SSO のこのマネージド構成の展開ルールを構成します。
10. **保存**をクリックします。

このCitrix SSOのマネージド構成が、構成済みデバイスポリシーのリストに表示されます。

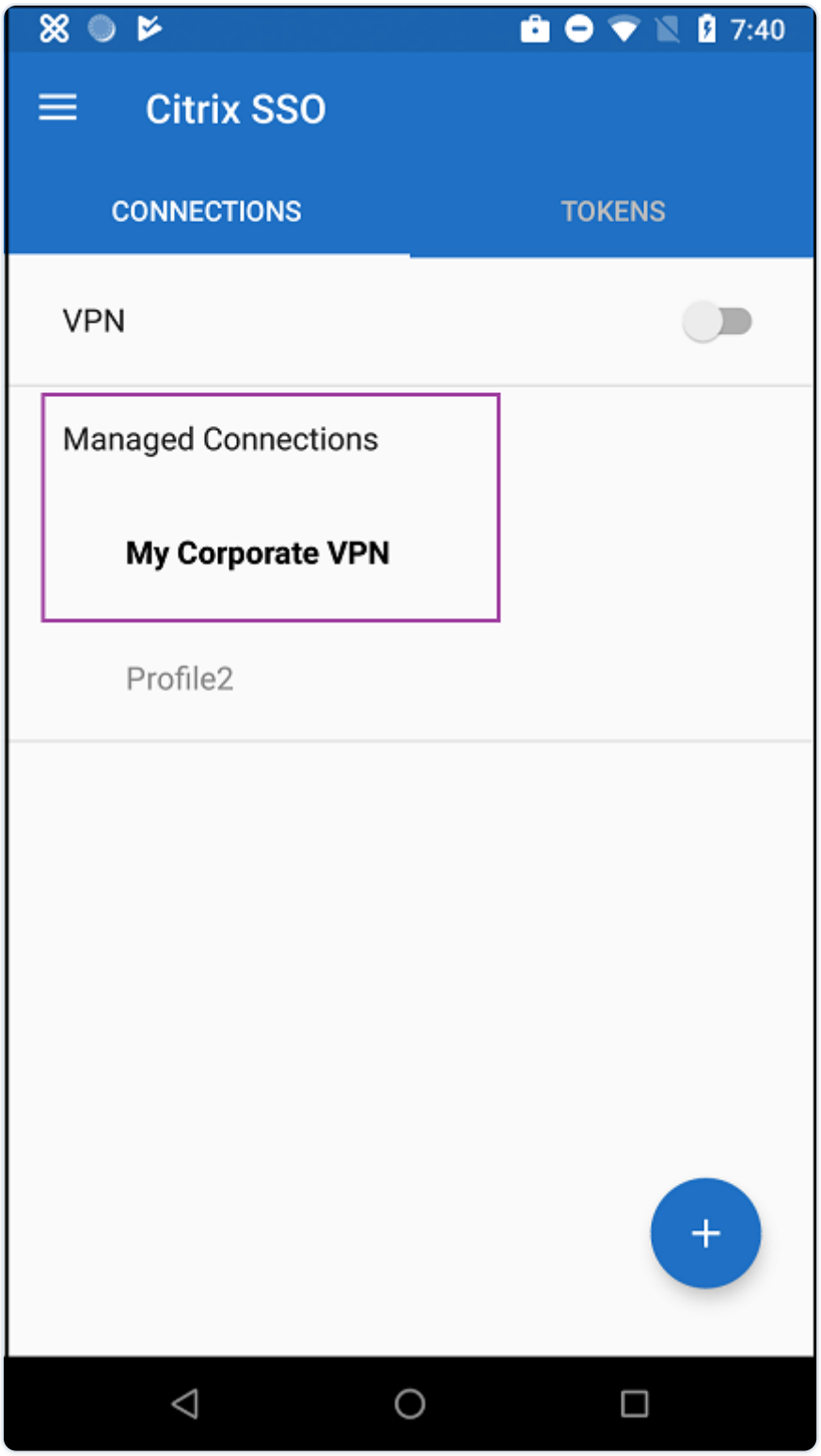
構成したVPNプロファイルの常時接続を有効にするには、XenMobileオプションデバイスポリシーを設定します。

> **注：** Android Enterpriseの常時接続VPNには、Citrix Secure Hub 19.5.5以降が必要です。

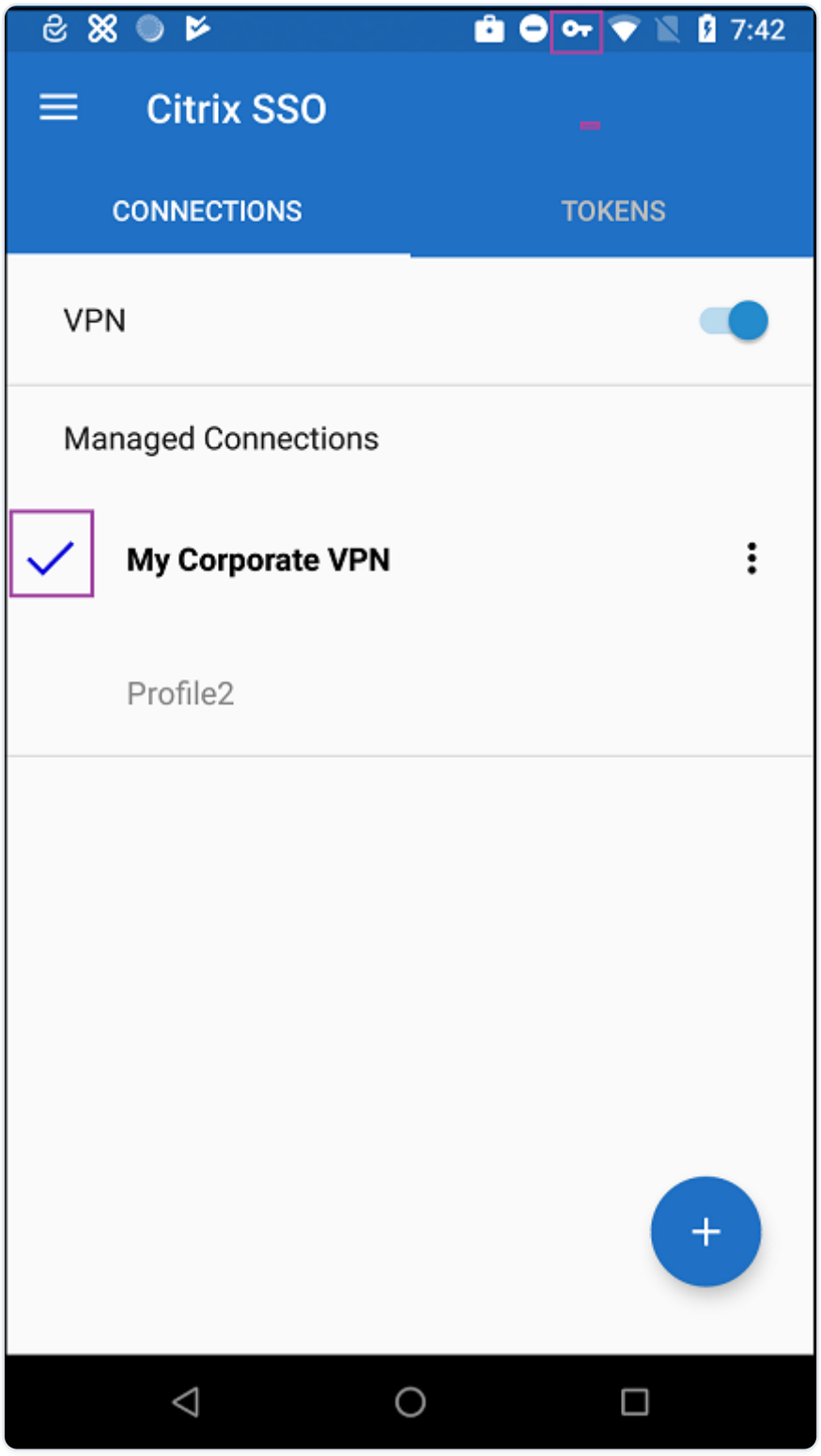
デバイスからのVPNプロファイルへのアクセス

作成したVPNプロファイルにアクセスするには、Android EnterpriseユーザーはGoogle PlayストアからCitrix SSOをインストールします。

構成したVPNプロファイルは、アプリの**Managed Connections**領域に表示されます。ユーザーはVPNプロファイルをタップして、そのVPNプロファイルを使用して接続します。



ユーザーが認証して接続すると、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が接続されていることを示します。



Zebra OEMConfigを使用したZebra Androidデバイスの管理

Zebra Technologies OEMConfig管理ツールを使用して、Zebra Androidデバイスを管理します。Zebra OEMConfigアプリの詳細については、Zebra TechnologiesのWebサイトを参照してください。

XenMobileはZebra OEMConfigバージョン9.2以降をサポートしています。デバイスへのZebra OEMConfigのインストールに関するシステム要件については、Zebra TechnologiesのWebサイトでOEMConfig Setupを参照してください。

まず、Zebra OEMConfigアプリをGoogle PlayストアアプリとしてXenMobileコンソールに追加します。Add a public app store appを参照してください。

Zebra OEMConfigアプリのAndroid Enterprise管理対象構成を作成する

Zebra OEMConfigアプリの管理対象構成デバイスポリシーを構成します。このポリシーは、Zebra OEMConfigアプリがインストールされ、ポリシーが展開されているZebraデバイスに適用されます。

1. XenMobileコンソールで、 > をクリックします。 をクリックします。
2. を選択します。 をクリックします。



3. ウィンドウが表示されたら、リストから を選択し、 をクリックします。
4. Zebra OEMConfig構成の名前と説明を入力します。 をクリックします。
5. Zebra OEMConfig構成の名前を入力します。
6. 利用可能なパラメータを構成します。例:
   - デバイスの前面カメラを無効にするには、 を選択し、 を に設定します。
   - デバイスの時刻形式を変更するには、 を選択し、 を12時間形式の場合は に、24時間形式の場合は に設定します。

利用可能なすべての構成のリストと説明については、Zebra TechnologiesのWebサイトでZebra Managed Configurationsを参照してください。

1. 必要に応じて、さらにZebra OEMConfig構成を作成します。構成のリストの下にある 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、パラメータを構成します。
2. 必要なZebra OEMConfig構成をすべて作成したら、「**次へ**」をクリックします。
3. Zebra OEMConfig 用のこの管理対象構成の展開ルールを構成します。
4. 「**保存**」をクリックします。

管理対象ドメインデバイスポリシー

メールとSafariブラウザに適用される管理対象ドメインを定義できます。管理対象ドメインは、Safariを使用してドメインからダウンロードされたドキュメントをどのアプリが開けるかを制御することで、企業データの保護に役立ちます。

iOS 8以降の監視対象デバイスでは、ユーザーがブラウザからドキュメント、添付ファイル、ダウンロードを開く方法を制御するために、URLまたはサブドメインを指定します。iOS 9.3以降の監視対象デバイスでは、ユーザーがSafariでパスワードを保存できるURLを指定できます。

iOSデバイスを監視モードに設定する手順については、「Apple Configuratorを使用してiOSデバイスを監視モードにする」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 リストにないドメインの受信者にメールを送信すると、そのメッセージはユーザーのデバイスにフラグが立てられ、企業ドメイン外の相手にメッセージを送信していることを警告します。

ドキュメント、添付ファイル、ダウンロードなどの項目について: ユーザーが管理対象Webドメインリストにあ るWebドメインからSafariを使用して項目を開くと、適切な企業アプリがその項目を開きます。項目が管理対象Webドメインリストにない Webドメインからのものである場合、ユーザーは企業アプリでその項目を開くことはできません。個人用の管理対象外アプリを使用する必要があります。

監視対象デバイスの場合、Safariのパスワード自動入力ドメインを指定しない場合でも、デバイスが一時的な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、デバイスが一時的な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、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

ドメインを指定するには:

形式	説明
`example.com`	`example.com` 以下のすべてのパスを管理対象として扱いますが、 `site.example.com/` は管理対象としません。

形式	説明
`foo.example.com`	`foo.example.com`以下のすべてのパスを管理対象としますが、`example.com/`または`bar.example.com/`は管理対象としません。
`*.example.com`	`foo.example.com`または`bar.example.com`以下のすべてのパスを管理対象としますが、`example.com/`は管理対象としません。
`example.com/sub`	`example.com/sub`およびその下のすべてのパスを管理対象としますが、`example.com/`は管理対象としません。
`foo.example.com/sub`	`foo.example.com/sub`以下のすべてのパスを管理対象としますが、`example.com`、`example.com/sub`、`foo.example.com/`、または`bar.example.com/sub`は管理対象としません。
`*.example.com/sub`	`foo.example.com/sub`または`bar.example.com/sub`以下のすべてのパスを管理対象としますが、`example.com`または`foo.example.com/`は管理対象としません。

ルール:

- ドメインを比較する際、URLの先頭の「www.」と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ある場合、そのポート番号を指定するアドレスのみが管理対象と見なされます。それ以外の場合、標準ポートのみ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、パターン`*.example.com:8080`は`https://site.example.com:8080/page.html`に一致しますが、`https://site.example.com/page.html`には一致しません。しかし、パターン`*.example.com`は`https://site.example.com/page.html`と`https://site.example.com/page.html`に一致しますが、`https://site.example.com:8080/page.html`には一致しません。
- 管理対象のSafari Webドメイン定義は累積的です。すべての管理対象Safari Webドメインペイロードによって定義されたパターンは、URLリクエストを照合するために使用されます。

設定:

- **管理対象ドメイン**

- **マークなしのメール ドメイン:** リストに含める各メール ドメインについて、**追加**をクリックし、次の操作を行います。
  - **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**をクリックしてメール ドメインを保存しないようにします。
- **管理対象の Safari Web ドメイン:** リストに含める各 Web ドメインについて、**追加**をクリックし、次の操作を行います。
  - **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 Web ドメインを保存しないようにします。
- **Safari パスワード自動入力ドメイン:** リストに含める各自動入力ドメインについて、**追加**をクリックし、次の操作を行います。
  - **Safari パスワード自動入力ドメイン:** 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保存しないようにします。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間 (時間)**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0 以降でのみ利用可能です。

最大常駐ユーザーデバイスポリシー

最大常駐ユーザーデバイスポリシーは、iOS (iPadOS) を実行している共有デバイス向けです。共有iPadの詳細については、「Apple Education機能との統合」を参照してください。

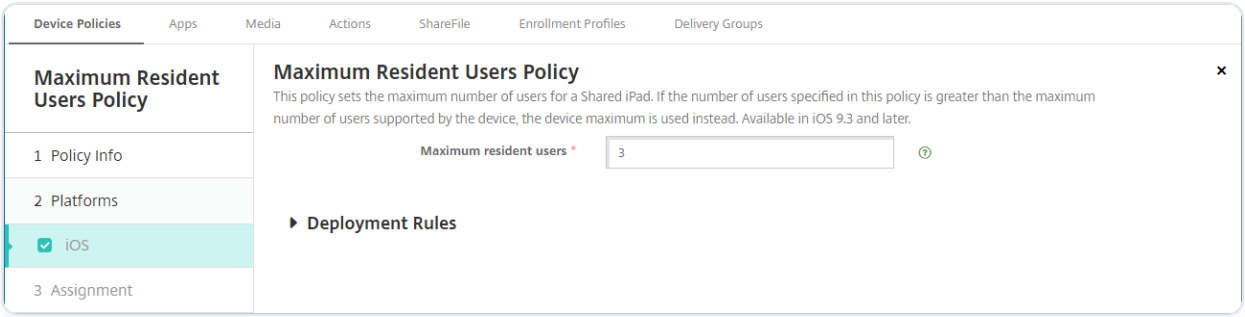
このポリシーは、iPadがセットアップアシスタント中の「構成待ち」フェーズにあるときに展開される必要があります。Appleは、共有iPadが登録された後にこのポリシーを展開することを許可していません。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **最大常駐ユーザー数:** 共有iPadの最大ユーザー数。このポリシーで指定されたユーザー数がデバイスでサポートされる最大ユーザー数よりも多い場合、Citrix Endpoint Managementは代わりにデバイスの最大値を使用します。デフォルトは**5**ユーザーです。

  Appleは、最大常駐ユーザーの値を可能な限り低く保つことを推奨しています。値が低いと、各ユーザーのiPadストレージ容量が最大化されます。また、値が低いとiCloudとの通信が最小限に抑えられ、より高速なサインインエクスペリエンスが提供されます。AppleがiPad上の共有ストレージをどのように処理するかについては、`<https://developer.apple.com/education/shared-ipad/>`を参照してください。



MDMオプションデバイスポリシー

XenMobileでデバイスポリシーを作成して、監視対象のiOS 7.0以降の電話デバイスで「iPhone/iPadを探す」のアクティベーションロックを管理できます。iOSデバイスを監視モードに設定する手順については、「Apple Configuratorを使用してiOSデバイスを監視モードにする」を参照してください。

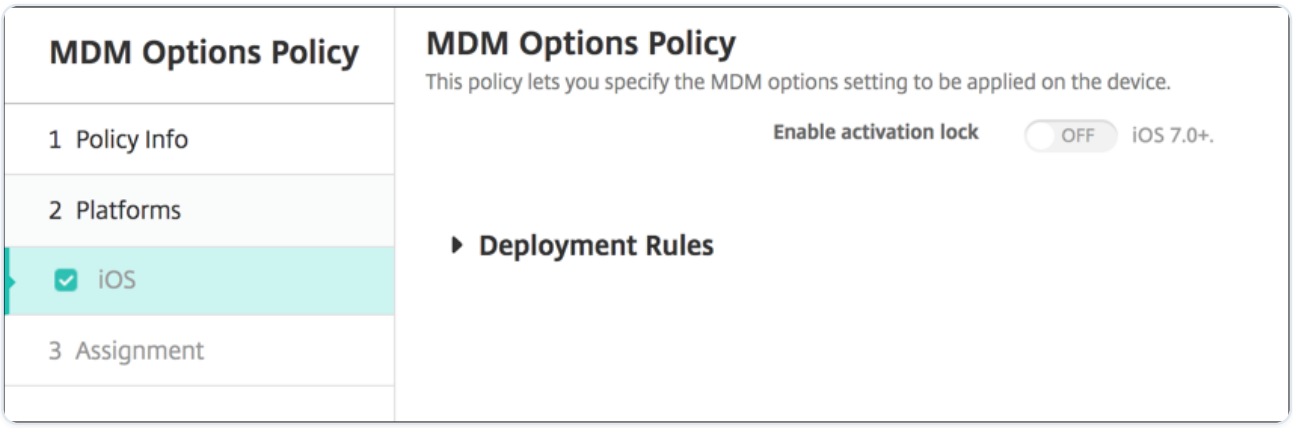
アクティベーションロックは「iPhone/iPadを探す」の機能で、紛失または盗難された監視対象デバイスの再アクティベーションを防止します。アクティベーションロックでは、誰かが「iPhone/iPadを探す」をオフにしたり、デバイスを消去したり、デバイスを再アクティベートしたりする前に、ユーザーのApple IDとパスワードが必要です。組織が所有するデバイスの場合、アクティベーションロックをバイパスすることは、たとえばデバイスをリセットまたは再割り当てするために必要です。

アクティベーションロックを有効にするには、XenMobile® MDMオプションデバイスポリシーを構成して展開します。その後、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できます。アクティベーションロックのApple資格情報要件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」セキュリティアクションを発行します。

たとえば、ユーザーが紛失した電話を返却した場合、または完全ワイプの前後にデバイスをセットアップする場合：電話がiTunesアカウントの資格情報を要求したときに、XenMobileコンソールから「アクティベーションロックバイパス」セキュリティアクションを発行することで、その手順をバイパスできます。

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］** に移動します。詳しくは、「デバイスポリシー」を参照してください。

iOS設定



- **アクティベーションロックを有効にする：** 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すると、**［管理］>［デバイス］** ページでそれらのデバイスを選択し、**［セキュリティ］** をクリックすると、セキュリティアクション**［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とパスワードを知らなくても、デバイスのアクティベーション前に監視対象デバイスからアクティベーションロックを解除できます。完全ワイプの前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。詳しくは、セキュリティアクションの記事の「iOSアクティベーションロックをバイパスする」を参照してください。

組織情報デバイスポリシー

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。このポリシーはiOS 7以降のデバイスで利用可能です。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

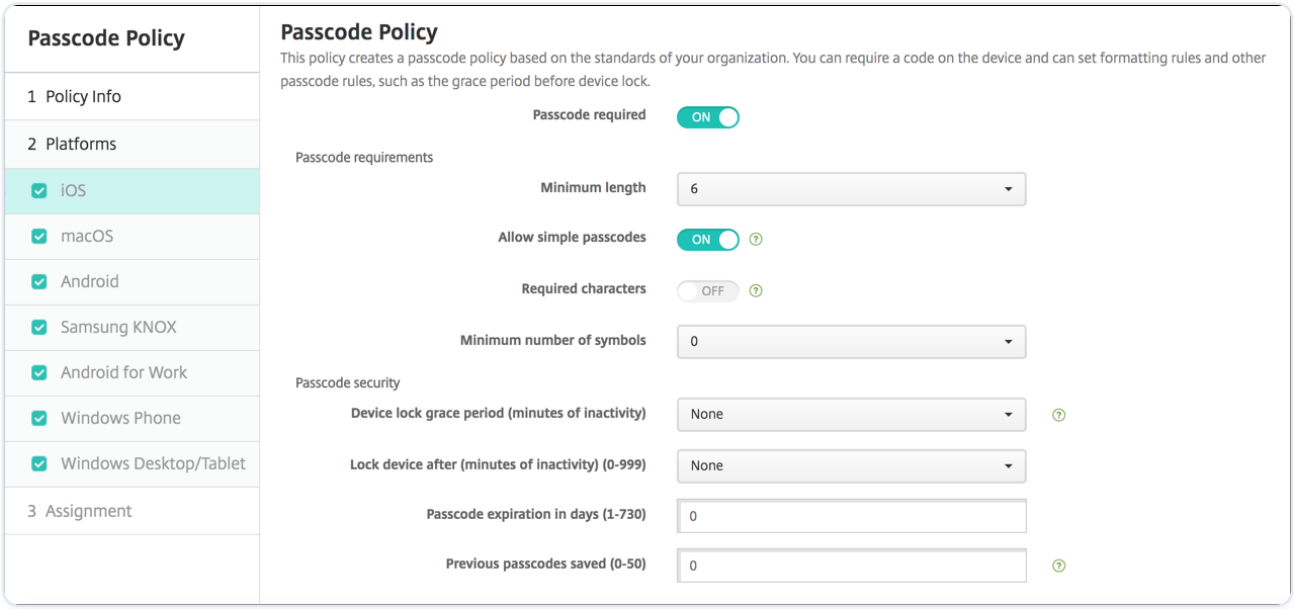
- **名前:** XenMobileを実行している組織の名前を入力します。
- **住所:** 組織の住所を入力します。
- **電話:** 組織のサポート電話番号を入力します。
- **メール:** サポートのメールアドレスを入力します。
- **マジック:** 組織が管理するサービスを説明する単語またはフレーズを入力します。

パスコードデバイスポリシー

XenMobileで、組織の標準に基づいてパスコードポリシーを作成します。ユーザーのデバイスにパスコードを要求し、さまざまな書式設定とパスコードルールを設定できます。iOS、macOS、Android、Samsung Knox、Android Enterprise、Windowsデスクトップ/タブレット用のポリシーを作成できます。各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で説明します。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **パスコードが必要:** このオプションを選択すると、パスコードが必須になり、iOS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、およびポリシー設定を構成できるようになります。
- **パスコード要件**

- **最小の長さ:** ドロップダウンリストで、パスコードの最小の長さをクリックします。デフォルトは**6**です。
- **簡易パスコードを許可:** 簡易パスコードを許可するかどうかを選択します。簡易パスコードとは、繰り返しまたは連続した文字のセットです。デフォルトは**オン**です。
- **必須文字:** パスコードに少なくとも1つの文字を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:** リストで、パスコードに含める必要がある記号の数をクリックします。デフォルトは**0**です。

- **パスコードセキュリティ**
  - **デバイスロック猶予期間 (非アクティブな時間 (分)):** リストで、ロックされたデバイスのロックを解除するためにユーザーがパスコードを入力する必要があるまでの時間をクリックします。デフォルトは**なし**です。
  - **デバイスをロックするまでの時間 (非アクティブな時間 (分)):** リストで、デバイスがロックされるまでに非アクティブでいられる時間をクリックします。デフォルトはなしです。
  - **パスコードの有効期限 (日数) (1〜730):** パスコードの有効期限が切れ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、これはパスコードが期限切れにならないことを意味します。
  - **以前に保存されたパスワード (0-50):** 保存する使用済みパスワードの数を入力します。ユーザーはこのリスト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、これはユーザーがパスワードを再利用できることを意味します。
  - **サインオン失敗の最大試行回数:** リストで、ユーザーがサインイン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、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。

macOS設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-passcode-macos.png)

- **パスコードが必要:** パスコードを要求し、iOSパスコードデバイスポリシーの構成オプションを表示するには、このオプションを選択します。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、およびポリシー設定を構成できるようになります。
- **パスコードが必要**を有効にしない場合、**サインオン失敗後の遅延時間 (分)** の横に、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遅延時間（分）を入力します。
- **パスコードが必要**を有効にする場合、次の設定を構成します。

- **パスコード要件**
  - **最小の長さ:** リストで、最小パスコードの長さをクリックします。デフォルトは**6**です。
  - **簡単なパスコードを許可する:** 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、繰り返しまたは連続した文字のセットです。デフォルトは**オン**です。
  - **必須文字:** パスコードに少なくとも1つの文字を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:** リストで、パスコードに含める必要がある記号の数をクリックします。デフォルトは**0**です。
- **パスコードセキュリティ**
  - **デバイスロック猶予期間 (非アクティブな時間 (分)):** リストで、ロックされたデバイスのロックを解除するためにユーザーがパスコードを入力する必要があるまでの時間をクリックします。デフォルトは**なし**です。
  - **デバイスをロックするまでの時間 (非アクティブな時間 (分)):** リストで、デバイスがロックされるまでに非アクティブでいられる時間をクリックします。デフォルトは**なし**です。
  - **パスコードの有効期限（日数）（1〜730）：** パスコードの有効期限が切れ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。
  - **以前使用した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。ユーザーはこのリスト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利用できることを意味します。
  - **最大サインオン失敗回数：** リストで、ユーザーがサインイン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デバイスがロックされます。デフォルトは**未定義**です。
  - **サインオン失敗後の遅延時間（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遅延時間（分）を入力します。
  - **パスコードのリセットを強制：** ユーザーが次回認証するときに、パスコードをリセットする必要があります。
- **ポリシー設定**
  - **プロファイルスコープ：** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

Android設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-passcode-android.png)

> **注：**
>
> Androidのデフォルト設定は**オフ**です。

- **パスコード必須：** このオプションを選択すると、パスコードが必須になり、Android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、およびSamsung SAFEの設定を構成できます。
- **パスコード要件**
  - **最小の長さ：** ドロップダウンリストで、パスコードの最小の長さを選択します。デフォルトは6です。
  - **生体認証：** 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すると、「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:** ドロップダウンリストで、パスコードの構成方法を設定するために、**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。デフォルトは「制限なし」です。
  - **詳細ルール:** 詳細なパスコードルール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以降で利用可能です。デフォルトは「**オフ**」です。
  - **詳細ルール**を有効にすると、次の各リストから、パスコードに含める必要のある各文字タイプの最小数をクリックします。
    - **記号:** 記号の最小数。
    - **文字:** 文字の最小数。
    - **小文字:** 小文字の最小数。
    - **大文字:** 大文字の最小数。
    - **数字または記号:** 数字または記号の最小数。
    - **数字:** 数字の最小数。
- **パスコードのセキュリティ**

- **デバイスをロックするまでの時間（非アクティブな分数）:** リストで、デバイスがロックされるまでに非アクティブでいられる時間を選択します。デフォルトは「**なし**」です。
- **パスコードの有効期限（日数、1〜730）:** パスコードの有効期限が切れ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。
- **保存された以前のパスワード（0〜50）:** 保存する使用済みパスワードの数を入力します。ユーザーはこのリスト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利用できることを意味します。
- **サインオン失敗の最大試行回数:** リストで、ユーザーがサインイン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デバイスがワイプされます。デフォルトは「**未定義**」です。

- **暗号化**
  - **暗号化を有効にする**：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以降で利用可能です。このオプションは、**パスコードが必要**の設定に関わらず利用できます。

    デバイスを暗号化するには、ユーザーはバッテリーが充電された状態で開始し、暗号化にかかる1時間以上デバイスを接続したままにする必要があります。暗号化プロセスを中断すると、デバイス上の一部のデータまたはすべてのデータが失われる可能性があります。デバイスが暗号化された後、工場出荷時設定にリセットしてデバイス上のすべてのデータを消去する以外に、プロセスを元に戻すことはできません。

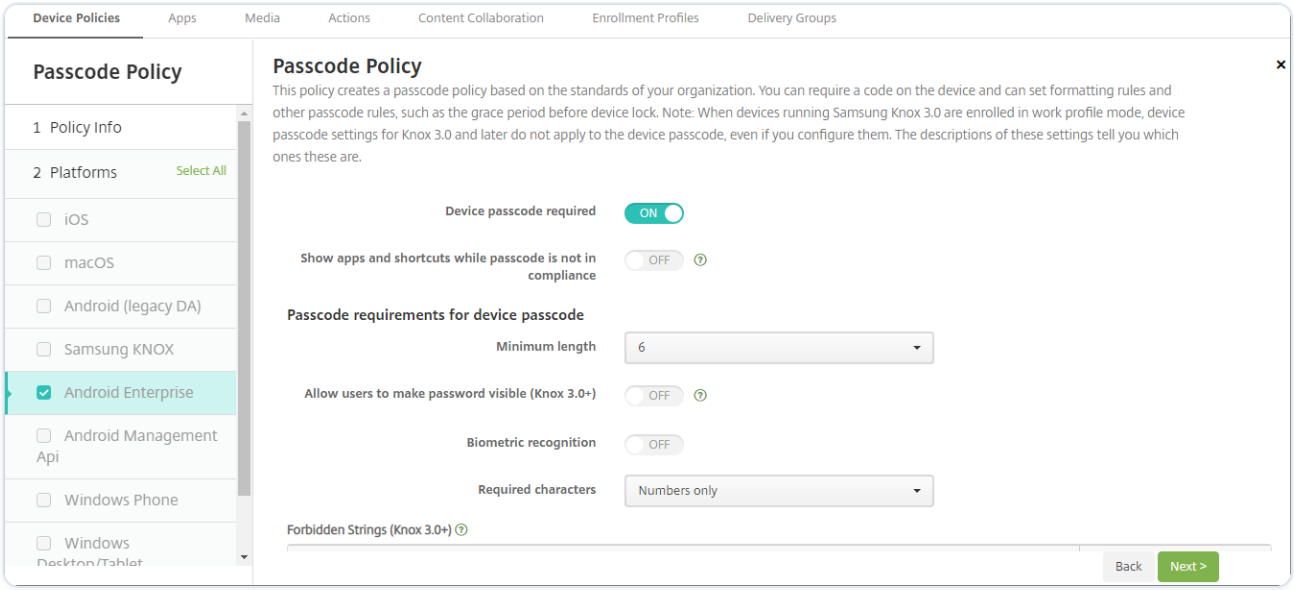
- **サムスン セーフ**

> **注：**
>
> Samsung SAFEデバイスで顔認証または虹彩認証を無効にするための回避策として：Samsung SAFE用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、`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。

  - **すべてのユーザーで同じパスコードを使用する**：すべてのユーザーで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、**パスコードが必要**の設定に関わらず利用できます。

- **すべてのユーザーで同じパスコードを使用する**を有効にすると、**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。
- **パスコードが必要**を有効にすると、以下のSamsung SAFE設定を構成します。
  - **変更された文字数**：ユーザーが以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。
  - **文字の出現回数**：パスコード内で文字が出現できる最大回数を入力します。デフォルトは**0**です。
  - **英字シーケンスの長さ**：パスコード内の英字シーケンスの最大長を入力します。デフォルトは**0**です。
  - **数字シーケンスの長さ**：パスコード内の数字シーケンスの最大長を入力します。デフォルトは**0**です。
  - **ユーザーがパスワードを表示できるようにする**：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。
  - **生体認証を構成する**。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、以下のオプションを設定できます。
    - **指紋を許可する**。ユーザーが指紋を使用して認証できるように選択します。
    - **虹彩を許可する**。ユーザーが虹彩を使用して認証できるようにするには、これを選択します。
  - **禁止文字列:** ユーザーが「password」、「pwd」、「welcome」、「123456」、「111111」のような推測されやすい安全でない文字列を使用するのを防ぐために、禁止文字列を作成します。拒否したい文字列ごとに、**追加**をクリックし、次の操作を行います。
    - **禁止文字列:** ユーザーが使用しない可能性のあ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キャンセルします。

Android Enterpriseの設定



Android Enterpriseデバイスの場合、デバイスのパスコード、Android Enterpriseワークプロファイルのセキュリティチャレンジ、またはその両方を要求できます。

Android 9.0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、**Android Enterprise**ページでSamsung Knoxの設定を構成します。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**ページを使用します。

> **注：**
>
> Samsung Knox 3.0を実行しているデバイスがワーク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は、構成してもデバイスパスコードには適用されません。

- **デバイスパスコード必須:** デバイスにパスコードを要求します。この設定が**オン**の場合、**デバイスパスコードのパスコード要件**と**デバイスパスコードのパスコードセキュリティ**の設定を構成します。デフォルトは**オフ**です。
- **パスコードが準拠していないときにアプリとショートカットを表示:** この設定が**オン**の場合、パスコードが準拠していなくても、デバイス上のアプリとショートカットは非表示になりません。この設定が**オフ**の場合、パスコードが準拠していないときにアプリとショートカットは非表示になります。この設定を有効にする場合、Citrix®は、パスコードが準拠していないときにデバイスを非準拠としてマークする自動アクションを作成することを推奨します。デフォルトは**オフ**です。
- **デバイスパスコードのパスコード要件:**

- **最小長:** パスコードの最小長を指定します。デフォルトは6です。
- **ユーザーがパスワードを表示できるようにする:** 有効なKnoxライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイスの場合。完全に管理されているデバイスのみに適用されます。この設定は、ワーク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。ユーザーがパスワードを表示できるようにします。デフォルトは**オフ**です。
- **生体認証:** 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。リストから、**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でのみ使用してください。Android 7.1以降では、**制限なし**の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ライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイス向けです。完全に管理されているデバイスのみに適用されます。この設定は、ワーク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として使用できない文字列を指定します。ユーザーが「password」、「pwd」、「welcome」、「123456」、「111111」のような推測しやすい安全でない文字列を使用するのを防ぐために、禁止文字列を作成します。拒否したい各文字列について、**追加**をクリックします。ユーザーに使用させたくない文字列を入力し、**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キャンセルします。
- **詳細ルール:** パスコードで使用できる文字の種類に関する詳細ルールを適用します。この設定が**オン**の場合、**最小数**と**最大数**の下の設定を構成します。この設定は、Android 5.0より前のAndroidデバイスでは利用できません。デフォルトは**オフ**です。
- **最小数:**
  - **記号:** 記号の最小数を指定します。デフォルトは**0**です。
  - **文字:** 文字の最小数を指定します。デフォルトは**0**です。
  - **小文字:** 小文字の最小数を指定します。デフォルトは**0**です。
  - **大文字:** 大文字の最小数を指定します。デフォルトは**0**です。
  - **数字または記号:** 数字または記号の最小数を指定します。デフォルトは**0**です。
  - **数字:** 数字の最小数を指定します。デフォルトは**0**です。
  - **変更された文字:** 有効なKnoxライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイス向けです。完全に管理されているデバイスのみに適用されます。この設定は、ワーク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。ユーザーが以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ライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイス向けです。完全に管理されているデバイスのみに適用されます。この設定は、ワーク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。
  - **文字の出現回数:** パスコード内で文字が出現できる最大回数を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **アルファベット順の長さ:** パスコード内のアルファベット順の最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **数値シーケンスの長さ:** パスコード内の数値シーケンスの最大長を指定します。デフォルトは**0**で、最大制限がないことを意味します。

- **デバイスパスコードのパスコードセキュリティ:**
  - **デバイスをワイプするまでの失敗したサインオン試行回数:** 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。
  - **デバイスをロックするまでの非アクティブ時間 (分) (0-999):** デバイスがロックされるまでの非アクティブな時間を分単位で指定します。デフォルトは**なし**です。
  - **パスコードの有効期限 (日数) (1-730):** パスコードが期限切れにな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、パスコードが期限切れにならないことを意味します。
  - **保存された以前のパスワード (0-50):** 保存する使用済みパスワードの数を指定します。ユーザーはこのリスト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利用できることを意味します。
  - **デバイスをロックするまでの失敗したサインオン試行回数** 有効なKnoxライセンスキーが構成されているSamsung Knox 3.0以降を実行しているデバイスの場合。完全に管理されたデバイスのみに適用されます。この設定は、ワークプロファイルデバイスとして登録された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はロックされます。デフォルトは**未定義**です。

- **ワークプロファイルのセキュリティチャレンジ:** Android Enterpriseワークプロファイルで実行されているアプリへのアクセスに、ユーザーがセキュリティチャレンジを完了することを要求します。Android 7.0以降を実行しているデバイスの場合。この設定が**オン**の場合、「**ワークプロファイルのセキュリティチャレンジのパスコード要件**」および「**ワークプロファイルのセ**

キュリティチャレンジのパスコードセキュリティ」の下の設定を構成します。デフォルトは**オフ**です。

- **ワークプロファイルのセキュリティチャレンジのパスコード要件:**
  - **最小の長さ:** 最小パスコード長を指定します。デフォルトは6です。
  - **ユーザーにパスワードの表示を許可する:** 有効なKnoxライセンスキーが構成されているKnox 3.0以降を実行しているデバイスの場合。ユーザーがパスワードを表示できるようにします。デフォルトは**オフ**です。
  - **生体認証:** 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。リストから、**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でのみ使用してください。Android 7.1以降では**制限なし**の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ライセンスキーが構成されているKnox 3.0以降を実行しているデバイスの場合。ユーザーがパスコードとして使用できない文字列を指定します。ユーザーが「password」、「pwd」、「welcome」、「123456」、「111111」のような推測しやすい安全でない文字列を使用するのを防ぐために、禁止文字列を作成します。拒否したい各文字列について、**追加**をクリックします。ユーザーに使用させたくない文字列を入力し、**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キャンセルします。
  - **詳細ルール:** パスコードに含めることができる文字の種類に関する詳細ルールを適用します。この設定が**オン**の場合、「**最小数**」および「**最大数**」の下の設定を構成します。この設定はAndroid 5.0より前のAndroidデバイスでは利用できません。デフォルトは**オフ**です。
  - **最小数:**
    - **記号:** 記号の最小数を指定します。デフォルトは**0**です。
    - **文字:** 文字の最小数を指定します。デフォルトは**0**です。
    - **小文字:** 小文字の最小数を指定します。デフォルトは**0**です。
    - **大文字:** 大文字の最小数を指定します。デフォルトは**0**です。
    - **数字または記号:** 数字または記号の最小数を指定します。デフォルトは**0**です。
    - **数字:** 数字の最小数を指定します。デフォルトは**0**です。
    - **変更された文字数:** Knox 3.0以降を実行し、有効なKnoxライセンスキーが構成されているデバイスの場合。ユーザーが以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:** Knox 3.0以降を実行し、有効なKnoxライセンスキーが構成されているデバイスの場合。
  - **文字の出現回数:** パスコード内で文字が出現できる最大回数を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **アルファベット順の長さ:** パスコード内のアルファベット順の最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
  - **数字順の長さ:** パスコード内の数字順の最大長を指定します。デフォルトは**0**で、これは最大制限がないことを意味します。
- **統合パスコードを有効にする: オン**の場合、ユーザーはデバイスと仕事用プロファイルに1つのパスコードを使用します。**オフ**の場合:
  - ユーザーはデバイスと仕事用プロファイルに異なるパスコードを使用する必要があります。
  - ユーザーがデバイスと仕事用プロファイルに1つのパスコードを使用したい場合に設定する、デバイス上の**1つのロックを使用**設定は無効になります。ユーザーはそれを有効にできません。
  - 仕事用プロファイルのセキュリティチャレンジのパスコード要件がデバイスのパスコードよりも複雑な場合: **Use one lock** 設定が有効になっているユーザーは、仕事用プロファイルのパスコードを変更するよう求められます。

  デフォルトは**オフ**です。Android 9.0以降で利用可能です。

- **仕事用プロファイルのセキュリティチャレンジのパスコードセキュリティ**
  - **コンテナをワイプするまでの失敗したサインオン試行回数:** 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。ワイプ後、ユーザーは仕事用プロファイルを再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非アクティブ時間 (分):** 仕事用プロファイルがロックされるまでにデバイスが非アクティブでいられる分数を指定します。デフォルトは**なし**です。
  - **パスコードの有効期限 (日数) (1-730):** パスコードが期限切れにな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、パスコードは期限切れになりません。
  - **保存された以前のパスワード (0-50):** 保存する使用済みパスワードの数を指定します。ユーザーはこのリスト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、ユーザーはパスワードを再利用できます。

- **コンテナをロックするまでの失敗したサインオン試行回数:** 有効なKnoxライセンスキーが構成されているKnox 3.0以降を実行しているデバイスの場合。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、デバイスがロックされます。デフォルトは**未定義**です。

Windowsデスクトップ/タブレット設定

デバイスポリシー設定画面の画像(/en-us/xenmobile/server/media/device-policy-passcode-windowsdesktop.png)

- **簡易ログオンを許可しない:** ユーザーが画像パスワードまたは生体認証ログオンでデバイスにアクセス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。
- **最小パスコード長:** ドロップダウンリストで最小パスコード長を選択します。デフォルトは**6**です。
- **ワイプ前の最大パスコード試行回数:** リストで、ユーザーが正常にサインイン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、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 (日数) (0-730):** パスコードが期限切れになるまでの日数を入力します。有効な値は0～730です。デフォルトは**0**で、パスコードは期限切れになりません。
- **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。ユーザーはこのリスト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から24まで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非アクティブ時間（分）（1-999）：** デバイスがロックされるまでの非アクティブな時間を分単位で入力します。有効な値は1～999です。このフィールドには1から999までの数値を入力する必要があります。デフォルトは**0**です。

パーソナルホットスポットデバイスポリシー

ユーザーがWi-Fiネットワークの範囲外にいる場合でも、iOSデバイスのパーソナルホットスポット機能を通じてセルラーデータ接続を使用することで、インターネットに接続できるようにします。iOS 7.0以降で利用可能です。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

パーソナルホットスポットを無効にする: ユーザーデバイスでパーソナル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、ユーザーデバイスのパーソナルホットス

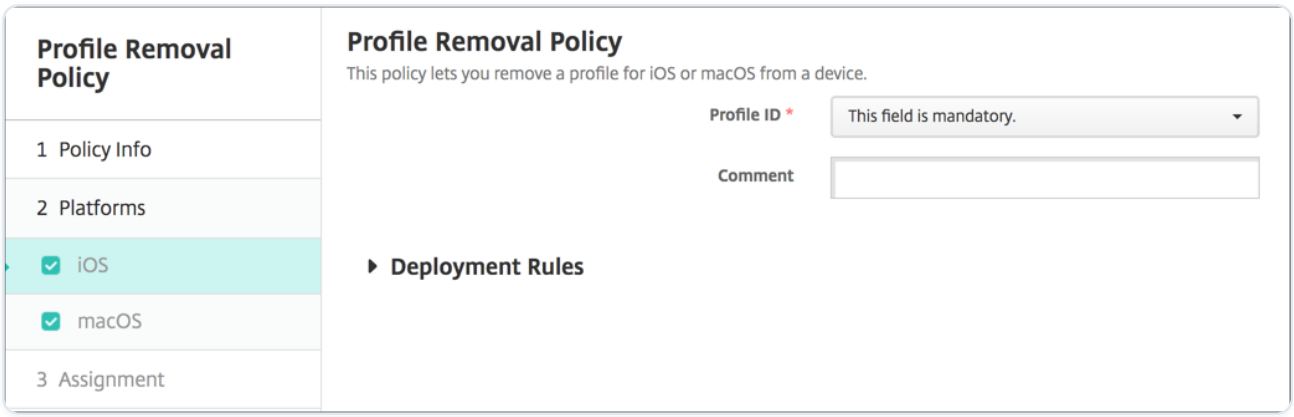
ポットをオフにします。このポリシーは機能を無効にするものではありません。ユーザーは引き続きデバイスでパーソナルホットスポットを使用できます。ただし、ポリシーが展開されると、パーソナルホットスポットはデフォルトでオンのままにならないようにオフになります。

プロファイル削除デバイスポリシー

XenMobileでアプリプロファイル削除デバイスポリシーを作成できます。このポリシーは、展開されると、ユーザーのiOSまたはmacOSデバイスからアプリプロファイルを削除します。

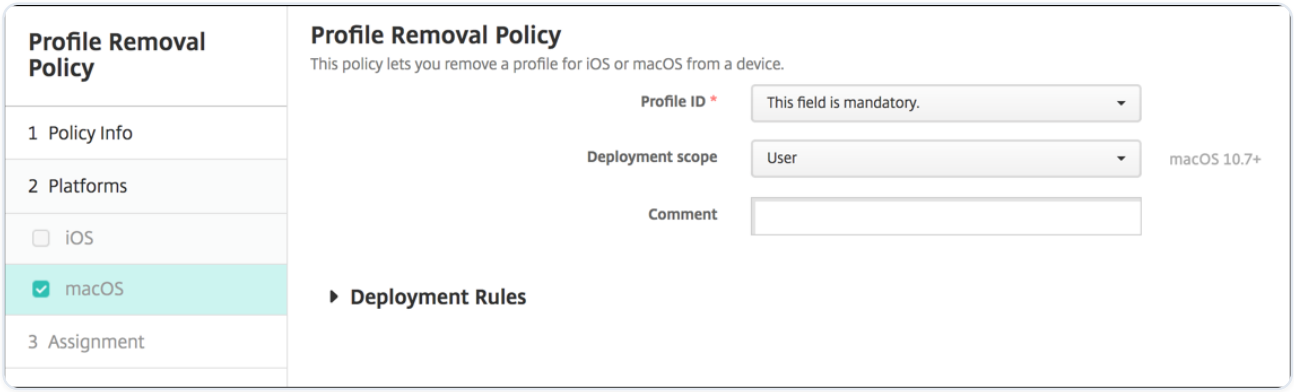
このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



- **プロファイルID:** ドロップダウンリスト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:** オプションのコメントを入力します。

macOS設定



- **プロファイルID:** ドロップダウンリスト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。

- **展開スコープ:** ドロップダウンリストから**** または を選択します。デフォルトは**** です。このオプションはmacOS 10.7以降でのみ利用可能です。
- **コメント:** オプションの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

iOSエンタープライズアプリを開発してコード署名する場合、通常、AppleがiOSデバイスでアプリを実行するために必要とす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か期限切れの場合、ユーザーがタップして開こうとするとアプリがクラッシュします。

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年後に期限切れになることです。ユーザーが登録したすべてのiOSデバイス上のすべてのプロビジョニングプロファイルの有効期限を追跡する必要があります。有効期限の追跡には、実際の有効期限を把握するだけでなく、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を把握することも含まれます。2つの解決策として、プロビジョニングプロファイルをユーザーにメールで送信するか、ダウンロードしてインストールできるようにWebポータルに配置する方法があります。これらの解決策は機能しますが、ユーザーがメールの指示に反応したり、Webポータルにアクセスして正しいプロファイルをダウンロードしてインストールしたりする必要があるため、エラーが発生しやすいです。

このプロセスをユーザーにとって透過的にするために、XenMobile®ではデバイスポリシーを使用して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。不足しているプロファイルや期限切れの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ため、アプリをタップするだけで使用できるようになります。

プロビジョニングプロファイルポリシーを作成する前に、プロビジョニングプロファイルファイルを作成する必要があります。詳細については、Apple Developerサイトで開発プロビジョニングプロファイルを作成する方法に関するAppleの記事を参照してください。

iOS設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/info-provisioning-profile.png)

- **iOSプロビジョニングプロファイル: 参照**をクリックしてファイルが保存されている場所に移動し、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を選択します。

プロビジョニングプロファイルの削除デバイスポリシー

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の詳細は、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、 > に移動します。詳細については、デバイスポリシーを参照してください。

iOS設定

- **iOSプロビジョニングプロファイル:** 削除するプロビジョニングプロファイルをドロップダウンリストでクリックします。
- **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

XenMobileでデバイスポリシーを追加して、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。デバイスごとに展開できるグローバルHTTPプロキシポリシーは1つだけです。

このポリシーを追加または構成するには、 > の順に移動します。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

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デバイスを監視モードにする」または「Apple Deployment Programを介してデバイスを展開する」を参照してください。

プロキシポリシーをデバイスに送信する前に、デバイスを登録するための展開ルールを設定します。

iOS設定

- **プロキシ構成:** ユーザーのデバイスでプロキシを構成する方法として、 または をクリックします。
    - をクリックした場合は、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:** プロキシサーバーへの認証に使用するオプションのユーザー名を入力します。
- **パスワード:** プロキシサーバーへの認証に使用するオプションのパスワードを入力します。

◦ をクリックした場合は、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が到達不能な場合に直接接続を許可する:** PACファイルが到達不能な場合に、ユーザーが宛先に直接接続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**オン**です。このオプションはiOS 7.0以降でのみ利用可能です。

- **キャプティブネットワークにアクセスするためにプロキシをバイパスすることを許可する:** キャプティブネットワークにアクセスするためにプロキシをバイパス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。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除の特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を入力します。iOS 6.0以降でのみ利用可能です。

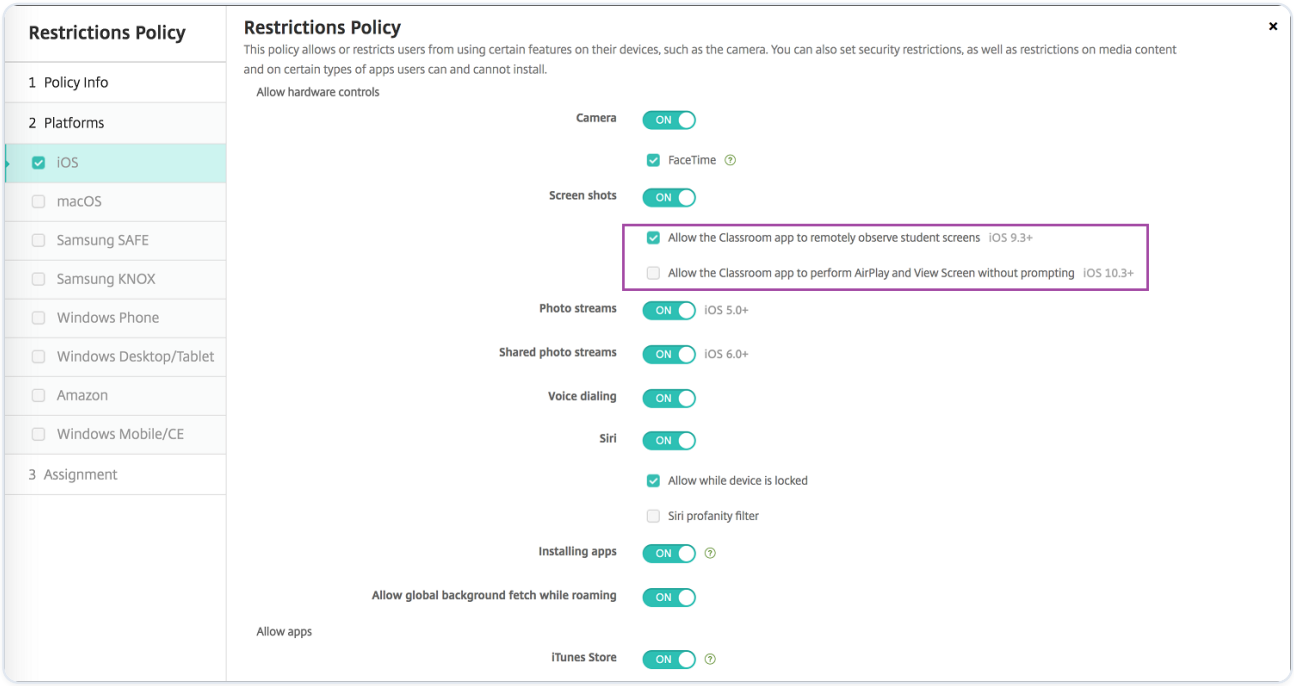
制限デバイスポリシー

制限デバイスポリシーでは、カメラなどのユーザーデバイス上の特定の機能や機能を許可または制限します。メディアコンテンツの制限や、ユーザーがインストールできるアプリの種類とできないアプリの種類の制限に加えて、セキュリティ制限も設定できます。ほとんどの制限設定はデフォルトで**オン**（*許可*）になっています。主な例外は、iOSセキュリティ - 強制機能とすべてのWindowsタブレット機能で、これらはデフォルトで**オフ**（*制限*）になっています。

Windows 10 RS2 Phoneの場合：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が電話に展開された後も、ブラウザは有効のままです。この問題を回避するには、電話を再起動してください。この問題はサードパーティの問題です。

> ヒント：
>
> **オン**を選択したオプションはすべて、ユーザーがその操作を実行したり、その機能を使用したりできることを意味します。例：
>
> **カメラ**。**オン**の場合、ユーザーはデバイスのカメラを使用できます。**オフ**の場合、ユーザーはデバイスの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撮ることができます。**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撮ることができません。
>
> 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**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定



一部のiOS制限ポリシー設定は、ここに記載されているとおり、またXenMobile®コンソールの制限ポリシーページに記載されているとおり、特定のiOSバージョンにのみ適用されます。

iOS制限ポリシー設定は、デバイスがユーザー登録モード、非監視（フルMDM）モード、または監視モードで登録されている場合に適用できます。次の表は、iOS 13以降の各制限ポリシー設定で利用可能な登録モードを示しています。

表に記載されているように、以前は非監視モードと監視モードで利用可能だった一部の設定は、iOS 13以降、監視モードでのみ利用可能です。次のルールが適用されます。

- 監視対象のiOS 13以降のデバイスがXenMobileに登録されている場合、設定がデバイスに適用されます。
- 非監視対象のiOS 13以降のデバイスがXenMobileに登録されている場合、設定はデバイスに適用されません。
- XenMobileに登録済みのiOS 12（またはそれ以前）デバイスがiOS 13にアップグレードしても、変更はありません。設定はアップグレード前と同様にデバイスに適用されます。

iOSデバイスを監視モードに設定する方法については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」(/ja-jp/xenmobile/server/provision-devices/ios-bulk-enrollment.html#to-configure-apple-configurator-2-settings)を参照してください。

設定	ユーザー登録	非監視	監視
ハードウェア制御を許可			
カメラ	いいえ	はい	はい
FaceTime	いいえ	いいえ（iOS 13で新規）	はい
FaceTimeリモートコントロールを許可	いいえ	いいえ	はい
スクリーンショット	はい	いいえ	はい
Classroomアプリによる生徒の画面のリモート監視を許可	いいえ	いいえ	はい
ClassroomアプリによるAirPlayと画面表示のプロンプトなしでの実行を許可	いいえ	いいえ	はい
写真ストリーム	いいえ	はい	はい
共有写真ストリーム	いいえ	はい	はい

設定	ユーザー登録	非監視	監視
共有iPadの一時セッションを許可	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
デバイスがロックされている間も許可	はい	はい	はい
Siriの不適切表現フィルター	いいえ	いいえ	はい
アプリのインストール	不可	不可 (iOS 13で新規)	可
代替アプリマーケットプレイス	不可	不可	可
Web配布アプリ	不可	不可	可
ローミング中のグローバルバックグラウンドフェッチを許可	不可	可	可
アプリを許可			
アイチューンズストア	いいえ	いいえ (iOS 13で新規)	はい
アプリ内課金	いいえ	はい	はい
購入に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で新規）	はい
自動入力	いいえ	いいえ（iOS 13で新規）	はい

設定	ユーザー登録	非監視	監視
詐欺警告を強制	はい	はい	はい
JavaScriptを有効にする	いいえ	はい	はい
ポップアップをブロック	不可	可	可
Cookieを許可	不可	可	可
ネットワーク - iCloudアクションを許可			
iCloudの書類とデータ	不可	不可 (iOS 13で新規)	可
iCloudバックアップ	不可	可	はい
iCloud写真キーチェーン	いいえ	はい	はい
iCloud写真ライブラリ	いいえ	はい	はい
セキュリティ - 強制			
暗号化されたバックアップ	はい	はい	はい
広告追跡の制限	いいえ	はい	はい
最初のAirPlayペアリング時のパスコード	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を使用した管理対象ドキュメントの共有	はい	はい	はい

設定	ユーザー登録	非監視	監視
セキュリティ - 許可			
信頼できない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
管理対象ペーストボードを要求	はい	はい	はい
管理対象外アプリでの管理対象アプリからのドキュメント	はい	はい	はい
管理対象外のアプリが管理対象の連絡先を読み取る	いいえ	いいえ	はい
管理対象のアプリが管理対象外の連絡先に書き込む	いいえ	いいえ	はい
管理対象外のアプリからのドキュメントを管理対象のアプリで	はい	はい	はい
Appleへの診断情報の送信	はい	はい	はい
Touch IDでデバイスのロックを解除	いいえ	はい	はい
自動ロック解除	いいえ	はい	はい
ロック時のPassbook通知	いいえ	はい	はい
ハンドオフ	いいえ	はい	はい

設定	ユーザー登録	非監視	監視
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でのインターネット検索結果	いいえ	はい	はい
エンタープライズアプリの信頼	いいえ	はい	はい
Appleパーソナライズ広告を許可	いいえ	はい	はい
監視対象デバイスのみの設定 - 許可			
eSIMの変更を許可	いいえ	いいえ	はい
消去時にeSIMを保持	いいえ	いいえ	はい
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
指紋の変更	いいえ	いいえ	はい
デバイスからのアプリのインストール	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
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
アプリの自動ダウンロード	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のユーザー生成コンテンツ	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で新規)	はい
友達を追加	いいえ	いいえ	はい
マルチプレイヤーゲーム	いいえ	いいえ (iOS 13で新規)	はい
アカウント設定の変更	いいえ	いいえ	はい
アプリのモバイルデータ設定の変更	いいえ	いいえ	はい
ネットワークドライブ接続を許可	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
USBデバイス接続を許可	いいえ	いいえ	はい
デバイスを探すを許可	いいえ	いいえ	はい
「友達を探す」を許可	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
キーボードの自動修正	いいえ	いいえ	はい
キーボードのスペルチェック	いいえ	いいえ	はい
QuickPathキーボードを許可	いいえ	いいえ	はい
定義の検索	いいえ	いいえ	はい
シングルアプリバンドルID	いいえ	いいえ	はい
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
制限付きアプリの使用	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
診断提出の変更	いいえ	いいえ	はい
Bluetoothの変更	いいえ	いいえ	はい
音声入力を許可	いいえ	いいえ	はい
Wi-Fiを強制的にオンにする	いいえ	いいえ	はい
Wi-Fiポリシーによってインストールされたネットワークのみに参加する	いいえ	いいえ	はい
Classroomアプリがプロンプトなしで 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
Classroomアプリがプロンプトなしでアプリにロックし、デバイスをロックできるようにする	いいえ	いいえ	はい
プロンプトなしでClassroom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の資格情報をキーチェーンに保存することを許可	いいえ	いいえ	はい
iBeaconを使用してAirPrintプリンターの検出を許可	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
信頼された証明書を持つ宛先にのみAirPrintを許可	いいえ	いいえ	はい
VPN構成の追加	いいえ	いいえ	はい
モバイルデータ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のセットアップ	いいえ	いいえ	はい
USB制限モードを許可する	いいえ	いいえ	はい
ソフトウェアアップデートの遅延を強制する	いいえ	いいえ	はい
強制的なソフトウェアアップデートの遅延	いいえ	いいえ	はい
クラスを離れるための教室リクエストの許可を強制する	いいえ	いいえ	はい
自動入力の前に認証を強制する	いいえ	いいえ	はい
日付と時刻の自動設定を強制する	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
パスワードの近接要求	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
パスワード共有	いいえ	いいえ	はい
インターネット共有設定の変更	いいえ	いいえ	はい
ペアリングされていないデバイスによるリカバリへの起動を許可	いいえ	いいえ	はい
迅速なセキュリティ対応をインストール	いいえ	いいえ	はい
迅速なセキュリティ対応を削除	いいえ	いいえ	はい
メールプライバシー保護を許可	いいえ	いいえ	はい
NFC	いいえ	いいえ	はい
App Clipを許可	いいえ	いいえ	はい
ゲン文字	いいえ	いいえ	はい
イメージプレイグラウンド	いいえ	いいえ	はい
イメージワンド	いいえ	いいえ	はい
iPhoneミラーリング	いいえ	いいえ	はい
パーソナライズされた手書き入力結果	いいえ	いいえ	はい
書き込みツール	いいえ	いいえ	はい
通話録音	いいえ	いいえ	はい
非表示にするアプリ	いいえ	いいえ	はい
ロックするアプリ	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
メール概要	いいえ	いいえ	はい
RCSメッセージング	いいえ	いいえ	はい
外部インテリジェンス統合を許可する	いいえ	いいえ	はい
外部インテリジェンス統合へのサインインを許可する	いいえ	いいえ	はい
メールのスマートリプライを許可する	いいえ	いいえ	はい
メモの文字起こしを許可	いいえ	いいえ	はい
Safariの要約を許可	いいえ	いいえ	はい
ビジュアルインテリジェンスの要約を許可	いいえ	いいえ	はい
メモの文字起こし要約を許可	いいえ	いいえ	はい
Apple Intelligence レポートを許可	いいえ	いいえ	はい
デフォルトの通話アプリの変更を許可	いいえ	いいえ	はい
デフォルトのメッセージングアプリの変更を許可	いいえ	いいえ	はい
外部インテリジェンスワークスペースIDを許可	いいえ	いいえ	はい
デフォルトブラウザの変更	いいえ	いいえ	はい

設定	ユーザー登録	非監視	監視
ライブボイスメールを許可	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
今日のビュー	はい	はい	はい
メディアコンテンツ - 許可			
露骨な表現の音楽、ポッドキャスト、iTunes Uのコンテンツ	いいえ	いいえ (iOS 13で新規)	はい
iBooks内の露骨な性的コンテンツ	いいえ	はい	はい
評価地域	いいえ	はい	はい
映画	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デバイスの場合。
    - **FaceTimeリモートコントロールを許可:** リモートFaceTimeセッションがデバイスの制御を要求できるようにします。監視対象のiOSデバイスの場合。iOS 18.4以降で利用可能です。

- **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。
  - **Classroomアプリによる生徒の画面のリモート監視を許可:** この制限が選択されていない場合、インストラクターはClassroomアプリを使用して生徒の画面をリモートで監視できません。デフォルト設定は選択されており、インストラクターはClassroomアプリを使用して生徒の画面を監視できます。**ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可**の設定により、生徒がインストラクターに許可を与えるプロンプトを受け取るかどうかが決まります。監視対象のiOSデバイスの場合。
  - **ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可:** この制限が選択されている場合、インストラクターは許可を求めるプロンプトなしで、生徒のデバイスでAirPlayと画面表示を実行できます。デフォルト設定は選択されていません。監視対象のiOSデバイスの場合。
- **フォトストリーム:** ユーザーがMyPhotoStreamを使用して、iCloud経由で写真をすべてのiOSデバイスと共有できるようにします。
- **共有フォトストリーム:** ユーザーがiCloud写真共有を使用して、同僚、友人、家族と写真を共有できるようにします。
- **共有iPadの一時セッションを許可:** 設定が**オフ**の場合、共有iPadの一時セッションへのアクセスを防止します。デフォルトは**オン**です。
- **音声ダイヤル:** ユーザーデバイスでの音声ダイヤルを有効にします。
- **Siri:** ユーザーがSiriを使用できるようにします。
  - **デバイスロック中の許可:** デバイスがロックされている間でも、ユーザーがSiriを使用できるようにします。
  - **Siriの不適切表現フィルター:** Siriの不適切表現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、不適切表現のフィルタリングは行われません。

    Siriとセキュリティの詳細については、Siriと音声入力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デバイスの場合。
- **代替アプリマーケットプレイス:** Webからの代替マーケットプレイスアプリのインストールを防止し、インストール済みの代替マーケットプレイスアプリがアプリをインストールするのを防止します。この機能はiOS 17.4以降のバージョンで利用可能です。デフォルトは**オン**です。監視対象のiOSデバイスの場合。
- **Web配布アプリ:** 顧客管理者がiOSデバイス上のWeb配布されたサードパーティアプリをブロックできるようにします。これはiOSバージョン17.5以降に適用されます。詳細については、制限を参照してください。

- **ローミング中のグローバルバックグラウンドフェッチを許可:** デバイスがローミング中に、メールアカウントをiCloudに自動的に同期できるようにします。**オフ**の場合、iOSフォンがローミング中のグローバルバックグラウンドフェッチアクティビティを無効にします。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にアクセスできるようにします。監視対象のiOSデバイスの場合。
  - **アプリ内課金:** ユーザーがアプリ内課金を行えるようにします。
    - **購入にiTunesパスワードを要求:** アプリ内課金にパスワードを要求します。デフォルトではこの機能は制限されており、アプリ内課金に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デバイスの場合。
    - **自動入力:** ユーザーがSafariでユーザー名とパスワードの自動入力を設定できるようにします。
    - **詐欺警告を強制する**：この設定が有効で、ユーザーが疑わしいフィッシング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、警告は発行されません。
    - **JavaScriptを有効にする**：SafariでJavaScriptの実行を許可します。
    - **ポップアップをブロックする**：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**：Cookieが受け入れられる範囲を設定します。リストから、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「**常に**」で、すべてのWebサイトがSafariにCookieを保存することを許可します。その他のオプションは「**現在のWebサイトのみ**」、「**しない**」、「**訪問済みのサイトからのみ**」です。

- **ネットワーク - iCloudアクションを許可する**
  - **iCloudの書類とデータ**：ユーザーが書類とデータをiCloudに同期できるようにします。監視対象のiOSデバイス向け。
  - **iCloudバックアップ**：ユーザーがデバイスをiCloudにバックアップできるようにします。
  - **iCloudキーチェーン**：ユーザーがパスワード、Wi-Fiネットワーク、クレジットカード、その他の情報をiCloudキーチェーンに保存できるようにします。
  - **iCloud写真ライブラリ**：ユーザーがiCloud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**

  デフォルトでは以下の機能は制限されており、セキュリティ機能は有効になっていません。

  - **暗号化されたバックアップ**：iCloudへのバックアップを強制的に暗号化します。
  - **広告追跡の制限**：ターゲット広告の追跡をブロックします。
  - **初回AirPlayペアリング時のパスコード**：AirPlay対応デバイスがAirPlayを使用する前に、1回限りの画面上のコードで認証されることを要求します。
  - **ペアリングされたApple Watchで手首検出を使用する**：ペアリングされたApple Watchが「**手首検出**」を使用することを要求します。
  - **AirDropを使用した管理対象ドキュメントの共有:** このオプションを**オン**に設定すると、AirDropが管理対象外のドロップターゲットとして表示されます。

- **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:** ユーザーがWebサイトの信頼されていないSSL証明書を受け入れることを許可します。
  - **証明書信頼設定の自動更新:** 信頼された証明書が自動的に更新されることを許可します。
  - **管理対象ペーストボードを必須にする:** オンにすると、コピー＆ペースト機能は、**管理対象アプリから管理対象外アプリへのドキュメント**および**管理対象外アプリから管理対象アプリへのドキュメント**に適用するのと同じ制限に従うようになります。デフォルトは**オフ**です。 たとえば、次のように構成します。

    - **管理対象ペーストボードを必須にする**: オン
    - **管理対象アプリから管理対象外アプリへのドキュメント**: オフ
    - **管理対象外アプリから管理対象アプリへのドキュメント**: オン

    > **注:**
    >
    > ポリシーをiOSデバイスに展開した後、ユーザーは管理対象アプリから管理対象外アプリへデータをコピー＆ペーストすることはできませんが、管理対象外アプリから管理対象アプリへデータをコピー＆ペーストすることはできます。

  - **管理対象アプリから管理対象外アプリへのドキュメント:** ユーザーが管理対象（企業）アプリから管理対象外（個人）アプリへデータを移動することを許可します。

- **管理対象外アプリから管理対象アプリへのドキュメント:** ユーザーが管理対象外（個人）アプリから管理対象（企業）アプリへデータを移動することを許可します。
- **Appleへの診断情報の送信:** ユーザーのデバイスに関する匿名診断データがAppleに送信されることを許可します。
- **Touch IDによるデバイスのロック解除:** ユーザーが指紋を使用してデバイスのロックを解除することを許可します。
- **自動ロック解除: オフ**の場合、ユーザーはApple Watchを使用してペアリングされたiPhoneのロックを解除できません。デフォルトは**オン**です。iOS 14.5以降で利用可能です。
- **ロック時のPassbook通知:** ロック画面にPassbook通知を表示することを許可します。
- **Handoff:** ユーザーがアクティビティをあるiOSデバイスから近くの別のiOSデバイスに転送することを許可します。
- **管理対象アプリのiCloud同期:** ユーザーが管理対象アプリをiCloudに同期することを許可します。
- **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をiCloudにバックアップすることを許可します。
- **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とハイライトをiCloudに同期することを許可します。
- **エンタープライズアプリの信頼:** エンタープライズアプリケーションを信頼することを許可します。エンタープライズアプリとは、組織向けにカスタム作成されたアプリのことです。これらは社内で作成することも、外部ベンダーから開発・購入することもできます。詳細については、「iOSにカスタムエンタープライズアプリをインストールする」を参照してください。
- **Spotlightでのインターネット検索結果:** Spotlightがデバイスに加えてインターネットからの検索結果を表示することを許可します。
- **非管理対象アプリによる管理対象連絡先の読み取り:** オプション。**非管理対象アプリ内の管理対象アプリからのドキュメント**が無効になっている場合にのみ利用可能です。このポリシーが有効な場合、非管理対象アプリは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ます。デフォルトは**オフ**です。iOS 12以降で利用可能です。
- **管理対象アプリによる非管理対象連絡先への書き込み:** オプション。有効な場合、管理対象アプリが非管理対象アカウントの連絡先に連絡先を書き込むことを許可します。**非管理対象アプリ内の管理対象アプリからのドキュメント**が有効な場合、この制限は影響しません。デフォルトは**オフ**です。iOS 12以降で利用可能です。

- **Appleパーソナライズド広告を許可: オフ**の場合、ユーザーのデータはApple広告プラットフォームによってパーソナライズド広告の配信に使用されません。デフォルトは**オン**です。iOS 14.0以降で利用可能です。

- **監視対象デバイスのみの設定 - 許可**

これらの設定は、監視対象デバイスにのみ適用されます。iOSデバイスを監視モードに設定する手順については、「Apple Configuratorを使用してiOSデバイスを監視モードにする」を参照してください。

- **eSIMの変更を許可:** ユーザーがデバイスのeSIM設定を変更することを許可します。
- **消去時にeSIMを保持: オン**の場合、パスワード入力の失敗回数が多すぎるか、**設定** > **一般** > **リセット**の「すべてのコンテンツと設定を消去」オプションによりデバイスが消去される際に、システムはeSIMを保持します。デフォルトは**オフ**です。

> **注:**
>
> **探す**がデバイスの消去を開始した場合、システムはeSIMを保持しません。

- **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ペアレンタルコントロールを設定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:** ユーザーが、あなたが展開した以外の構成プロファイルをインストールできるようにします。
- **指紋の変更:** ユーザーがTouch IDの指紋を変更または削除できるようにします。
- **デバイスからの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。この設定を無効にすると、エンドユーザーは新しいアプリをインストールできなくなります。App Storeは無効になり、そのアイコンはホーム画面から削除されます。
- **キーボードショートカット:** ユーザーが頻繁に使用する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:** ユーザーが監視対象デバイスにApple Watch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の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。
- **アプリの自動ダウンロード:** アプリをダウンロードできるようにします。
- **AirDrop:** ユーザーが近くのiOSデバイスと写真、ビデオ、Webサイト、位置情報などを共有できるようにします。
- **iMessage:** ユーザーがiMessageでWi-Fi経由でテキストメッセージを送信できるようにします。
- **Siriユーザー生成コンテンツ:** SiriがWebからユーザー生成コンテンツを照会できるようにします。従来のジャーナリストではなく、消費者がユーザー生成コンテンツを作成します。たとえば、TwitterやFacebookで見つか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で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:** ユーザーが友達にゲームをプレイするための通知を送信できるようにします。
  - **マルチプレイヤーゲーム:** ユーザーがデバイスでマルチプレイヤーゲームを開始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。
- **アプリのモバイルデータ設定の変更:** ユーザーがアプリによるモバイルデータの使用方法を変更できるようにします。
- **ネットワークドライブ接続を許可:** 設定が**オフ**の場合、ファイルアプリでネットワークドライブへの接続を防止します。デフォルトは**オン**です。
- **USBデバイス接続を許可:** 設定が**オフ**の場合、ファイルアプリで接続されているUSBデバイスへの接続を防止します。デフォルトは**オン**です。
- **デバイスを探すを許可:** 設定が**オフ**の場合、探すアプリの**デバイスを探す**オプションを無効にします。デフォルトは**オン**です。
- **友達を探すを許可:** 設定が**オフ**の場合、探すアプリの**友達を探す**オプションを無効にします。デフォルトは**オン**です。
- **友達を探す設定の変更:** ユーザーが友達を探す設定を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:** 管理者がユーザーデバイスをどのデバイスとペアリングできるかを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ホストとのペアリングを除き、ペアリングが防止されます。監視ホスト証明書が構成されていない場合、すべてのペアリングが無効になります。

- **予測キーボード:** ユーザーデバイスが入力時に単語を提案するために予測キーボードを使用できるようにします。ユーザーに候補の単語へのアクセスを許可したくない標準テストの実施などの状況では、このオプションを無効にします。
- **キーボードの自動修正:** ユーザーデバイスが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へのアクセスを許可したくない、標準化されたテストの実施などの状況では、このオプションを無効にします。
- **キーボードのスペルチェック:** ユーザーデバイスが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のアクセスを許可したくない、標準化されたテストの実施などの状況では、このオプションを無効にします。
- **QuickPathキーボードを許可:** 設定が**オフ**の場合、QuickPathキーボードを無効にします。デフォルトは**オン**です。
- **辞書検索:** ユーザーデバイスが入力中に辞書検索を使用できるようにします。ユーザーが入力中に辞書検索を使用することを許可したくない、標準化されたテストの実施などの状況では、このオプションを無効にします。
- **シングルアプリバンドルID:** デバイスの制御を維持し、他のアプリや機能とのやり取りを防止できるアプリのリストを作成します。 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。追加したいアプリごとにこのプロセスを繰り返します。
- **ニュース:** ユーザーがニュース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、ミュージックアプリはクラシックモードで実行されます。
- **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。
- **制限付きアプリの使用:** 提供するバンドルIDに基づいて、ユーザーがすべてのアプリを使用できるようにするか、アプリを使用または使用しないようにします。監視対象デバイスにのみ適用されます。**一部のアプリのみを許可**を選択した場合、Webクリップを許可するには、バンドルID `com.apple.webapp` のアプリを追加します。

> **注：**

> iOS 11以降、Appleはアプリの制限に利用できるポリシーに変更を加えました。Appleは、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を許可しなくなりました。

> 一部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、そのポリシーを展開した後：後でそれらのアプリの一部またはすべてを許可したい場合でも、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。この場合、iOSは変更をiOSプロファイルに適用しません。続行するには、プロファイル削除ポリシーを使用してiOSプロファイルを削除し、更新された制限デバイスポリシーを展開します。

この設定を**一部のアプリのみを許可**に変更した場合：このポリシーを展開する前に、Apple Deployment Programを使用して登録されたデバイスのユーザーに対し、設定アシスタントからAppleアカウントにサインインするよう助言してください。そうしないと、ユーザーは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ために、デバイスで2要素認証を無効にする必要がある場合があります。

- **診断提出の変更:** ユーザーが**設定 > 診断と使用状況**ペインで診断提出とアプリ分析の設定を変更できるようにします。
- **Bluetoothの変更:** ユーザーがBluetooth設定を変更できるようにします。
- **音声入力を許可:** 監視対象のみ。この制限が**オフ**に設定されている場合、音声認識を含む音声入力は許可されません。既定の設定は**オン**です。
- **Wi-Fiを強制的にオンにする:** 設定またはコントロールセンターでWi-Fiがオンまたはオフになるのを防ぎます。機内モードを有効にしても、この制限には影響しません。この制限は、接続するWi-Fiネットワークを選択することを妨げるものではありません。既定は**オフ**です。
- **Wi-Fiポリシーによってインストールされた Wi-Fiネットワークのみに参加:** オプション。監視対象のみ。この制限が**オン**に設定されている場合、デバイスは構成プロファイルを通じて設定されたWi-Fiネットワークにのみ参加できます。既定の設定は**オフ**です。
- **ClassroomアプリがプロンプトなしでAirPlayと画面表示を実行することを許可:** この制限が選択されている場合、インストラクターは許可を求めるプロンプトなしで、学生のデバイスでAirPlayと画面表示を実行できます。既定の設定は選択されていません。監視対象のiOSデバイスの場合。
- **Classroomアプリがプロンプトなしでアプリにロックし、デバイスをロックすることを許可:** この制限が**オン**に設定されている場合、Classroomアプリはユーザーにプロンプトを表示することなく、ユーザーデバイスを自動的にアプリにロックし、デバイスをロックしま

す。既定の設定は**オフ**です。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。

- **Classroomアプリのクラスにプロンプトなしで自動的に参加:** この制限が**オン**に設定されている場合、Classroomアプリはユーザーにプロンプトを表示することなく、ユーザーを自動的にクラスに参加させます。既定の設定は**オフ**です。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。既定の設定は**オン**です。この制限が**オン**の場合、これらの追加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の資格情報をキーチェーンに保存することを許可:** 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。既定の設定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。
  - **iBeaconを使用してAirPrintプリンターの検出を許可:** この制限が選択されていない場合、iBeaconによるAirPrintプリンターの検出は無効になります。これにより、偽のAirPrint Bluetoothビーコンがネットワークトラフィックをフィッシングするのを防ぎます。既定の設定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。
  - **信頼された証明書を持つ宛先にのみAirPrintを許可:** この制限が選択されている場合、ユーザーはAirPrintを使用して、信頼された証明書を持つ宛先にのみ印刷できます。既定の設定は選択されていません。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。既定の設定は**オン**です。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。
- **携帯電話プラン設定の変更:** この制限が**オフ**に設定されている場合、ユーザーは携帯電話プラン設定を変更できません。既定の設定は**オン**です。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。
- **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。既定の設定は**オン**です。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。
- **新しい近くのデバイスのセットアップ:** この制限がオフに設定されている場合、ユーザーは新しい近くのデバイスをセットアップできません。既定の設定はオンです。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、デバイスはロック中でも常にUSBアクセサリに接続できます。デフォルトは**オン**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **ソフトウェアアップデートの遅延を強制: オン**の場合、ユーザーがソフトウェアアップデートを確認できるタイミングを遅らせます。この制限が有効な場合、ユーザーはソフトウェアアップデートのリリース日から指定された日数が経過するまで、ソフトウェアアップデートを確認できません。デフォルトは**オフ**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **強制ソフトウェアアップデート遅延 (日数):** デバイス上のソフトウェアアップデートを遅延させる日数を指定できます。最大遅延日数は**90**日です。デフォルトは**30**日です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **クラスを離れるためのClassroomリクエスト許可を強制: オン**の場合、Classroomで管理されていないコースに登録している生徒は、コースを離れようとするときに教師に許可を求める必要があります。デフォルトは**オフ**です。監視対象のiOS 11.3以降のデバイスでのみ利用可能です。
- **自動入力前の認証を強制: オン**の場合、Safariやアプリでシステムがパスワードやクレジットカード情報を自動入力する前に、ユーザーは認証を行う必要があります。Face IDまたはTouch IDを搭載したデバイスでのみサポートされます。デフォルトは**オフ**です。
- **日付と時刻の自動設定を強制:** 監視対象デバイスで日付と時刻を自動的に設定できます。**オン**の場合、デバイスユーザーは**一般 > 日付と時刻**の下にある**自動設定**をオフにできません。デバイスのタイムゾーンは、デバイスがその位置を特定できる場合にのみ更新されます。つまり、デバイスがモバイルデータ通信接続または位置情報サービスが有効なWi-Fi接続を持っている場合です。デフォルトは**オフ**です。監視対象のiOS 12以降のデバイスでのみ利用可能です。
- **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機能や強力なパスワードの自動生成機能を使用できません。デフォルトは**オン**です。iOS 12以降で利用可能です。
- **パスワードの近接リクエスト:** 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からパスワードを要求しません。デフォルトは**オン**です。iOS 12以降で利用可能です。
- **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以降で利用可能です。
- **インターネット共有設定の変更: オフ**にすると、インターネット共有設定の変更を無効にします。デフォルトは**オン**です。

- **ペアリングされていないデバイスによるリカバリへの起動を許可: オン**の場合、ペアリングされていないデバイスによるリカバリモードでのデバイス起動を許可します。デフォルトは**オフ**です。iOS 14.5以降で利用可能です。
- **緊急セキュリティ対応のインストール: オフ**の場合、緊急セキュリティ対応のインストールを禁止します。デフォルトは**オン**です。
- **緊急セキュリティ対応の削除: オフ**の場合、緊急セキュリティ対応の削除を禁止します。デフォルトは**オン**です。
- **メールプライバシー保護を許可: オフ**の場合、デバイスのメールプライバシー保護を無効にします。デフォルトは**オン**です。iOS 15.2以降で利用可能です。
- **NFC: オフ**の場合、NFCを無効にします。デフォルトは**オン**です。iOS 14.2以降で利用可能です。
- **App Clipを許可**: **オフ**の場合、ユーザーがApp Clipを追加するのを防ぎ、デバイス上の既存のApp Clipをすべて削除します。デフォルトは**オン**です。iOS 14.0以降で利用可能です。
- **Genmoji: オフ**の場合、新しいGenmojiの作成を禁止します。iOS 18以降で利用可能です。
- **Image Playground: オフ**の場合、画像生成の使用を禁止します。iOS 18以降で利用可能です。
- **Image Wand: オフ**の場合、Image Wandの使用を禁止します。iOS 18以降で利用可能です。
- **iPhoneミラーリング: オフ**の場合、iPhoneミラーリングの使用を禁止します。iOSで使用する場合、これによりiPhoneがMacにミラーリングされるのを防ぎます。iOS 18以降で利用可能です。
- **パーソナライズされた手書き結果: オフ**の場合、システムがユーザーの手書きでテキストを生成するのを防ぎます。iOS 18以降で利用可能です。
- **ライティングツール: オフ**の場合、Apple Intelligenceのライティングツールを無効にします。iOS 18以降で利用可能です。
- **通話録音: オフ**の場合、通話録音を無効にします。監視対象デバイスが必要です。iOS 18.1以降で利用可能です。
- **非表示にするアプリ: オフ**の場合、ユーザーがアプリを非表示にする機能を禁止します。iOSで使用する場合、これによりユーザーがアプリを非表示にするのを防ぎますが、ホーム画面から削除しながらAppライブラリにアプリを残すことは引き続き許可されます。監視対象デバイスが必要です。iOS 18以降で利用可能です。
- **ロックするアプリ: オフ**の場合、ユーザーがアプリをロックする機能を禁止します。iOSで使用する場合、これによりユーザーがアプリをロックするのを防ぎ、結果としてアプリを

非表示にすることも防ぎます。監視対象デバイスが必要です。iOS 18以降で利用可能です。

- **メールの要約: オフ**の場合、メールメッセージの手動での要約作成機能を禁止します。iOSで使用する場合、これは自動要約生成には影響しません。監視対象デバイスが必要です。iOS 18.1以降で利用可能です。
- **RCSメッセージング: オフ**の場合、RCSメッセージングの使用を防ぎます。監視対象デバイスが必要です。iOS 18.1以降で利用可能です。
- **外部インテリジェンス統合を許可: オフ**の場合、Siriでの外部クラウドベースのインテリジェンスサービスの使用を無効にします。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **外部インテリジェンス統合へのサインインを許可: オフ**の場合、外部インテリジェンスプロバイダーを匿名モードに強制します。ユーザーがすでに外部インテリジェンスプロバイダーにサインインしている場合、この制限を適用すると、次回の要求が試行されたときにサインアウトされます。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **メールのスマートリプライを許可: オフ**の場合、メールのスマートリプライを無効にします。デフォルトは**オン**です。iOS 18.2以降で利用可能です。
- **メモの文字起こしを許可:** 「**オフ**」の場合、メモでの文字起こしを無効にします。デフォルトは「**オン**」です。iOS 18.2以降で利用可能です。
- **Safariの要約を許可:** 「**オフ**」の場合、システムはSafariでコンテンツを要約する機能を無効にします。デフォルトは「**オン**」です。iOS 18.4以降で利用可能です。
- **ビジュアルインテリジェンスの要約を許可:** 「**オフ**」の場合、システムはビジュアルインテリジェンスの要約を無効にします。デフォルトは「**オン**」です。iOS 18.3以降で利用可能です。
- **メモの文字起こし要約を許可:** 「**オフ**」の場合、メモでの文字起こし要約を無効にします。デフォルトは「**オン**」です。iOS 18.3以降で利用可能です。
- **Apple Intelligenceレポートを許可:** 「**オフ**」の場合、システムはApple Intelligenceレポートを無効にします。デフォルトは「**オン**」です。iOS 18.4以降で利用可能です。
- **デフォルトの通話アプリの変更を許可:** 「**オフ**」の場合、デフォルトの通話アプリ設定の変更を無効にします。この設定が適用されている場合でも、デフォルトの通話アプリ設定を行うMDM設定コマンドは引き続き機能します。デフォルトは「**オン**」です。iOS 18.4以降で利用可能です。
- **デフォルトのメッセージングアプリの変更を許可:** 「**オフ**」の場合、デフォルトのメッセージングアプリ設定の変更を無効にします。この設定が適用されている場合でも、デ

フォルトのメッセージングアプリ設定を行うMDM設定コマンドは引き続き機能します。デフォルトは「**オン**」です。iOS 18.4以降で利用可能です。

- **外部インテリジェンスワークスペースIDを許可:** 文字列の配列ですが、現在は単一の要素に制限されています。存在する場合、Apple Intelligenceは指定された外部統合ワークスペースIDのみの使用を許可し、リクエストを行うにはサインインが必要です。ユーザーはサインインをサポートする統合にサインインする必要があります。複数のペイロードは交差演算を使用して結合されます。これは、複数のペイロードで競合する値が指定された場合、許可されるワークスペースIDのセットが空になる可能性があることを意味します。iOS 18.3以降で利用可能です。
  - **外部インテリジェンスワークスペースID:** 外部インテリジェンスワークスペースIDを追加するには、「**追加**」をクリックし、「**外部インテリジェンスワークスペースID**」を入力して、「**保存**」をクリックします。追加したいワークスペースIDごとにこのプロセスを繰り返します。
- **デフォルトブラウザの変更:** 「**オフ**」の場合、デフォルトブラウザ設定の変更を禁止します。iOSで使用する場合、これはMDM設定コマンドによるデフォルトブラウザ設定を依然として許可します。監視対象デバイスが必要です。iOS 18.2以降で利用可能です。
- **ライブボイスメールを許可:** 「**オフ**」の場合、システムはデバイス上のライブボイスメールを無効にします。デフォルトは「**オン**」です。iOS 17.2以降で利用可能です。

- **セキュリティ - ロック画面に表示**
  - **コントロールセンター:** ロック画面でコントロールセンターへのアクセスを許可します。コントロールセンターを使用すると、ユーザーは機内モード、Wi-Fi、Bluetooth、おやすみモード、画面回転ロックの設定を簡単に変更できます。
  - **通知:** ロック画面での通知を許可します。
  - **今日の表示:** 天気や今日のカレンダー項目などの情報を集約する「今日の表示」をロック画面で許可します。
- **メディアコンテンツ - 許可**
  - **露骨な表現を含む音楽、ポッドキャスト、iTunes Uのコンテンツ:** ユーザーのデバイスで露骨な表現を含むコンテンツを許可します。
  - **iBooksの露骨な性的コンテンツ:** iBooksから露骨な表現を含むコンテンツをダウンロードすることを許可します。
  - **レーティング地域:** 保護者による制限のレーティングを取得する地域を設定します。リストから国をクリックして、レーティング地域を設定します。デフォルトは**米国**です。

- **映画:** ユーザーのデバイスで映画を許可するかどうかを設定します。映画が許可されている場合、オプションで映画のレーティングレベルを設定します。リストからオプションをクリックして、デバイスでの映画を許可または制限します。デフォルトは「すべての映画を許可」です。
- **テレビ番組:** ユーザーのデバイスでテレビ番組を許可するかどうかを設定します。テレビ番組が許可されている場合、オプションでテレビ番組のレーティングレベルを設定します。リストからオプションをクリックして、デバイスでのテレビ番組を許可または制限します。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許可するかどうかを設定します。アプリが許可されている場合、オプションでアプリのレーティングレベルを設定します。リストからオプションをクリックして、デバイスでのアプリを許可または制限します。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:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは「**日付を選択**」と「**削除までの期間 (時間)**」です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはiOS 9.3以降でのみ利用可能です。

macOS設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-restrictions-macos.png)

- **環境設定**
  - **システム環境設定の項目を制限:** システム環境設定へのユーザーアクセスを許可または制限します。デフォルトは**オフ**で、ユーザーはシステム環境設定に完全にアクセスできます。有効にした場合は、次の設定を構成します。
    - **システム環境設定パネル:** 選択した設定を有効にするか無効にするかを選択します。デフォルトではすべての設定が有効になっており、既定で**オン**です。
      - ユーザーとグループ

- 一般
- アクセシビリティ
- アップストア
- ソフトウェア・アップデート
- ブルートゥース
- CD と DVD
- 日付と時刻
- デスクトップとスクリーンセーバ
- ディスプレイ
- ドック
- 省エネルギー
- 機能拡張
- 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
- ミッションコントロール
- マウス
- ネットワーク
- 通知
- ペアレンタルコントロール
- プリンタとスキャナ
- 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
- 発音とスピーチ
- スポットライト

    - 起動ディスク
    - タイムマシン
    - トラックパッド
    - エックスサン

- **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の友達追加を許可:** ユーザーが友達にゲームをプレイするための通知を送信できるようにします。デフォルトは**オン**です。
    - **マルチプレイヤーゲームを許可:** ユーザーがマルチプレイ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アカウントの変更を許可:** ユーザーが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での採用を許可:** App StoreがOS Xに既存のアプリを採用すること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が保存しているパスワード、住所、その他の基本情報でウェブサイトのフィールドを自動的に入力できるようにします。デフォルトは**オン**です。
    - **アプリのインストールまたは更新に管理者パスワードを要求:** アプリのインストールまたは更新に管理者パスワードを要求します。デフォルトは**オフ**です。これは管理者パスワードが不要であることを意味します。
    - **App Storeをソフトウェアアップデートのみに制限:** App Storeをアップデートのみに制限し、App Storeの「アップデート」以外のすべてのタブを無効にします。デフォルトは**オフ**で、App Storeへのフルアクセスを許可します。
    - **起動を許可するアプリを制限:** 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を許可します。有効にした場合、次の設定を構成します。
        - **許可されたアプリ: 追加**をクリックし、起動を許可するアプリの名前とバンドルIDを入力して、**保存**をクリックします。起動を許可する各アプリについて、この手順を繰り返します。
        - **許可されていないフォルダー: 追加**をクリックし、ユーザーアクセスを制限したいフォルダーのファイルパス（例: /Applications/Utilities）を入力して、**保存**をクリックします。ユーザーにアクセスさせたくないすべてのフォルダーについて、この手順を繰り返します。

    - **許可されたフォルダー: 追加**をクリックし、ユーザーアクセスを許可したいフォルダーのファイルパスを入力して、**保存**をクリックします。ユーザーにアクセスさせたい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**
    - **次のDashboardウィジェットのみ実行を許可:** ユーザーが実行できるDashboardウィジェット（世界時計や計算機など）を許可または制限します。デフォルトは**オフ**で、すべてのウィジェットの実行を許可します。有効にした場合、次の設定を構成します。
        - **許可されたウィジェット: 追加**をクリックし、実行を許可するウィジェットの名前とIDを入力して、**保存**をクリックします。Dashboardで実行したい各ウィジェットについて、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、位置情報などを近くのiOSデバイスと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的に有効にする:** 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への共有追加を許可するかどうかを選択します。
    - **Sina Weibo:** 共有Sina Weiboマイクロブログ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への共有追加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共有追加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**

- **デスクトップピクチャをロック:** ユーザーがデスクトップピクチャ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、ユーザーはデスクトップピクチャを変更できます。
- **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、ユーザーはカメラを使用できません。
- **Apple Musicを許可:** 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、ミュージックアプリはクラシックモードで実行されます。監視対象デバイスにのみ適用されます。デフォルトは**オン**です。
- **Spotlightの提案を許可:** ユーザーがSpotlightの提案を使用してMacを検索したり、インターネット、iTunes、App StoreからSpotlightの提案を提供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の提案を使用できません。
- **調べるを許可:** 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調べられ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で調べる機能を使用できません。
- **ローカルアカウントにiCloudパスワードの使用を許可:** ユーザーがApple IDと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。このポリシーを有効にすると、ユーザーはMacの *すべて*のログイン画面で1つのIDとパスワードのみを使用することになります。デフォルトは**オン**で、ユーザーはApple IDとiCloudパスワードを使用してMacにアクセスできます。
- **iCloud書類とデータを許可:** ユーザーがMacでiCloudに保存されている書類とデータにアクセス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iCloud書類とデータを使用できません。
    - **iCloudデスクトップと書類を許可:** (macOS 10.12.4以降) デフォルトは選択済みです。
- **iCloudキーチェーン同期を許可:** iCloudキーチェーン同期を許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudメールを許可:** ユーザーがiCloudメールを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloud連絡先を許可:** ユーザーがiCloud連絡先を使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudカレンダーを許可:** ユーザーがiCloudカレンダーを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudリマインダーを許可:** ユーザーがiCloudリマインダーを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。

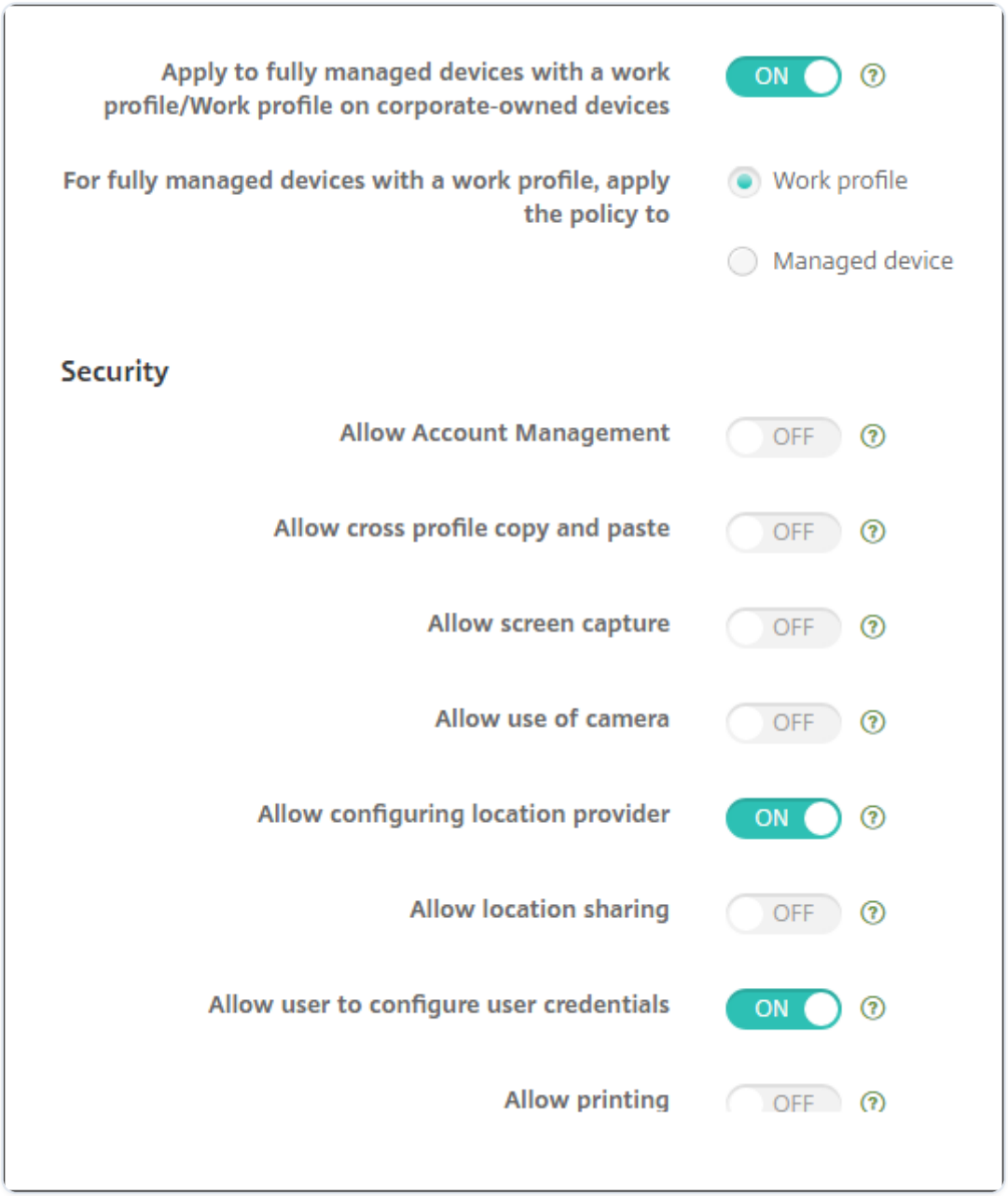
- **iCloudブックマークを許可:** ユーザーがiCloudブックマークと同期することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloudメモを許可:** ユーザーがiCloudメモを使用することを許可します (macOS 10.12以降)。デフォルトは**オン**です。
- **iCloud写真を許可:** この設定を**オフ**に変更すると、iCloud写真ライブラリから完全にダウンロードされていない写真は、ローカルデバイスストレージから削除されます (macOS 10.12以降)。デフォルトは**オン**です。
- **自動ロック解除を許可:** このオプションとApple Watchの詳細については、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。
- **Touch IDによるMacのロック解除を許可:** (macOS 10.12.4以降)。デフォルトは**オン**です。
- **ソフトウェアアップデートの遅延を強制: オン**の場合、この設定はユーザーへのソフトウェアアップデートの表示を遅らせます。ユーザーは、ソフトウェアアップデートのリリース日から指定された日数が経過するまで、ソフトウェアアップデートを確認できません。デフォルトは**オフ**です。macOS 10.13.4以降を実行している監視対象デバイスでのみ利用可能です。
- **ソフトウェアアップデートの遅延を強制 (日数):** デバイスでのソフトウェアアップデートを遅延させる日数を指定します。最大は90日です。デフォルトは**30**です。macOS 10.13.4以降を実行している監視対象デバイスでのみ利用可能です。
- **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以降で利用可能です。
- **パスワードの近接リクエスト:** 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から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以降で利用可能です。
- **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以降で利用可能です。
- **画像プレイグラウンド: オフ**の場合、画像生成の使用を禁止します。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。
- **iPhoneミラーリング: オフ**の場合、iPhoneミラーリングの使用を禁止します。macOSで使用する場合、MacがiPhoneをミラーリングするのを防ぎます。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。

- **ライティングツール: オフ**の場合、Apple Intelligenceライティングツールを無効にします。デフォルトは**オン**です。macOS 15以降を実行している監視対象デバイスでのみ利用可能です。
- **メディア共有の変更を許可: オフ**の場合、メディア共有設定の変更を禁止します。デフォルトは**オン**です。macOS 15.1以降で利用可能です。
- **スクリーンキャプチャアラートの強制バイパス: オン**の場合、スクリーンキャプチャアラートの表示をバイパスします。デフォルトは**オフ**です。macOS 15.1以降で利用可能です。
- **メールの要約: オフ**の場合、メールメッセージの要約を手動で作成する機能を無効にします。これは自動要約生成には影響しません。デフォルトは**オン**です。macOS 15.1以降で利用可能です。

Android設定

- **カメラ:** 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。**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。

アンドロイド エンタープライズ 設定



新規または工場出荷時設定にリセットされたAndroidデバイスがワークプロファイルモードで登録されると、Android 9.0-10.xを実行しているデバイスはワークプロファイルを持つ完全に管理されたデバイスとして登録されます。Android 11以降を実行しているデバイスは、企業所有デバイス上のワークプロファイルとして登録されます。制限ポリシーは、デバイス上のワークプロファイルまたは管理対象デバイスのいずれかに適用できます。

企業所有デバイスモードでワークプロファイルに登録されたデバイスでは、以下の制限がワークプロファイルでのみ利用可能です。

- バックアップサービスを許可
- システムアプリを有効にする

- キーガードがデバイスをロックしないようにする
- ステータスバーの使用を許可する
- デバイスの画面をオンのままにする
- アプリケーション設定のユーザー制御を許可する
- ユーザーがユーザー資格情報を構成できるようにする
- VPN構成を許可する
- USB大容量ストレージを許可する
- 出荷時設定へのリセットを許可する
- アプリのアンインストールを許可する
- 仕事用プロファイルと個人用プロファイルからメールアプリにアクセスする
- Google Play以外のアプリを許可する
- プロファイル間のコピー＆ペーストを許可する
- アプリの検証を有効にする
- アカウント管理を許可する
- 印刷を許可する
- NFCを許可
- ユーザーの追加を許可

デフォルトでは、デバイスがAndroid Enterpriseのワークプロファイルモードに登録されている場合、**USBデバッグと不明なソース**の設定は無効になります。

Android 9.0～10.xおよびSamsung Knox 3.0以降を実行しているデバイスの場合、**Android Enterprise**ページでSamsung KnoxとSamsung SAFEの設定を構成します。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**および**Samsung SAFE**ページを使用します。

Samsungの制限は、企業所有デバイスモードのワークプロファイルに登録されているデバイスには適用されません。これらのデバイスにSamsungの制限を適用するには、Knox Service Plugin (KSP) を使用します。詳細については、Samsungのドキュメントを参照してください。

最新のSamsung Knox管理機能を使用するには、Samsung Knox 3.4以降を使用することをお勧めします。

- **ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用:** ワークプロファイルを持つ完全に管理されたデバイスの制限ポリシー設定を構成できます。この設定が**オン**の場合、次のいずれかの設定を選択します。
  - **ワークプロファイル:** 構成する制限設定は、デバイス上のワークプロファイルにのみ適用されます。
  - **デバイスの管理:** 構成する制限設定は、デバイスにのみ適用されます。

  この設定が**オフ**の場合、構成する資格情報設定は、ワークプロファイルに明示的に適用される設定を除き、デバイスに適用されます。デフォルトは**オフ**です。

ワークプロファイルを持つ完全に管理されたデバイス/企業所有デバイス上のワークプロファイルに適用がオフの場合、次の設定を構成します。

- **セキュリティ**
  - **アカウント管理を許可:** ワークプロファイルおよび管理対象デバイスに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。
  - **プロファイル間のコピーと貼り付けを許可: オン**の場合、ユーザーはAndroid Enterpriseプロファイルのアプリと個人領域のアプリの間でコピーと貼り付けを行うことができます。デフォルトは**オフ**です。
  - **画面キャプチャを許可:** ユーザーがデバイス画面を録画またはスクリーンキャプチャできるようにします。デフォルトは**オフ**です。
  - **カメラの使用を許可する:** ユーザーがデバイスのカメラで写真やビデオを撮影できるようにします。デフォルトは**オフ**です。
  - **VPN構成を許可する:** ユーザーがVPN構成を作成できるようにします。Android 6以降を実行しているワーク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の場合。デフォルトは**オン**です。
  - **バックアップサービスを許可する:** ユーザーがデバイス上のアプリケーションデータと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。
  - **NFCを許可する:** ユーザーがNFC（近距離無線通信）を使用して、Webページ、写真、ビデオ、またはその他のコンテンツを自分のデバイスから別のデバイスに送信できるようにします。MDM 4.0以降の場合。デフォルトは**オン**です。
  - **位置情報プロバイダーの構成を許可する:** 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以降の場合。デフォルトは**オン**です。
  - **位置情報の共有を許可する:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

> **ヒント:**
>
> XenMobileで位置情報デバイスポリシーを作成して、地理的境界を適用できます。「位置情報デバイスポリシー」(/ja-jp/xenmobile/server/policies/location-policy.html#android-enterprise-settings)を参照してください。

- **ユーザーがユーザー資格情報を構成することを許可する:** ユーザーが管理対象キーストアで資格情報を構成できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可する: オン**の場合、ユーザーはユーザーデバイスからアクセス可能な任意のプリンターに印刷できます。デフォルトは**オフ**です。利用可能: Android 9以降。
- **USBデバッグを許可する:** デフォルトは**オフ**です。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされているデバイスアプリを実行できるようにします。デフォルトは**オフ**です。特定のアプリを有効にするには、「**システムアプリリスト**」テーブルで「**追加**」をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリストです。「**システムアプリを有効にする**」を「**オン**」に設定し、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`) コマンドを呼び出すことができます。たとえば、`adb shell "pm list packages -f name"` のように、「name」はパッケージ名の一部です。詳細については、`<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アプリのアクセス許可」(/ja-jp/xenmobile/server/policies/android-enterprise-app-permissions.html#android-enterprise-settings)ポリシーを使用してアプリのアクセス許可を制限できます。
  - **アプリケーションを無効にする:** 指定されたアプリのリストがデバイスで実行されないようにブロックします。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、「**アプリケーションリスト**」テーブルで「**追加**」をクリックします。
    - **アプリケーションリスト:** ブロックするアプリのリストです。**アプリケーションの無効化**を**オン**に設定し、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストは上書きされます。例:

com.example1とcom.example2を無効にし、その後リストをcom.example1とcom.example3に変更した場合、XenMobileはcom.example.2を有効にします。

- **アプリの検証を有効にする:** 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アプリを有効にする:** ユーザーがGoogle Mobile Services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。
- **Google Play以外のアプリを許可する:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
- **アプリケーション設定のユーザー制御を許可する:** ユーザーがアプリのアンインストール、アプリの無効化、キャッシュとデータのクリア、任意のアプリの強制停止、デフォルトのクリアを行えるようにします。ユーザーはこれらの操作をアプリから行います。デフォルトは**オフ**です。
- **アプリのアンインストールを許可する:** ユーザーがManaged Google Playストア内からアプリをアン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。この設定を表示するには、サーバープロパティ `afw.restriction.policy.v2` を有効にします。サーバープロパティの詳細については、サーバープロパティを参照してください。
- **仕事用プロファイルと個人用プロファイルからメールアプリにアクセスする**: 設定が**オン**の場合、ユーザーが個人用プロファイルから仕事用プロファイルのメールアプリにアクセスして使用できるようにします。デフォルトは**オフ**です。

- **BYOD仕事用プロファイル**
  - **ホーム画面に仕事用プロファイルアプリウィジェットを許可する:** この設定が**オン**の場合、ユーザーはデバイスのホーム画面に仕事用プロファイルアプリウィジェットを配置できます。この設定が**オフ**の場合、ユーザーはデバイスのホーム画面に仕事用プロファイルアプリウィジェットを配置できません。デフォルトは**オフ**です。
    - **ウィジェットが許可されているアプリ:** ホーム画面で許可するアプリのリストです。**ホーム画面に仕事用プロファイルアプリウィジェットを許可する**を**オン**に設定し、アプリを追加します。**追加**をクリックし、ホーム画面でウィジェットを許可するアプリをリストから選択します。**保存**をクリックします。このプロセスを繰り返して、さらにアプリウィジェットを許可します。
  - **デバイスの連絡先に仕事用プロファイルの連絡先を許可する:** 親プロファイルで、着信通話のために管理対象のAndroid Enterpriseプロファイルからの連絡先を表示します (Android 7.0以降)。デフォルトは**オフ**です。
- **完全に管理されたデバイスのみ**

- **ユーザーの追加を許可する:** ユーザーがデバイスに新しいユーザーを追加できるようにします。デフォルトは**オン**です。
- **データローミングを許可する:** ユーザーがローミング中にセルラー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のローミングを無効にします。デフォルトは**オフ**です。
- **SMSを許可する:** 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。
- **ステータスバーの使用を許可: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）でステータスバーを有効にします。この設定は、通知、クイック設定、および全画面モードからの脱出を可能にするその他の画面オーバーレイを無効にします。ユーザーはシステム設定に移動して通知を確認できます。Android 6.0以降の場合。デフォルトは**オフ**です。
- **Bluetoothを許可:** 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。
  - **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetoothによる送信共有を確立できません。デフォルトは選択されています。この設定を表示するには、サーバープロパティ`afw.restriction.policy.v2`を有効にします。サーバープロパティの詳細については、「サーバープロパティ」を参照してください。
- **日付と時刻の設定を許可:** 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。
- **出荷時設定へのリセットを許可:** ユーザーがデバイスを出荷時設定にリセットできるようにします。デフォルトは**オン**です。
- **デバイス画面をオンのままにする:** この設定が**オン**の場合、デバイスが接続されている間、デバイス画面はオンのままになります。デフォルトは**オフ**です。
- **USB大容量ストレージを許可:** ユーザーのデバイスとコンピューター間でUSB接続を介して大容量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。
- **マイクを許可:** ユーザーがデバイスの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。
- **テザリングを許可:** ユーザーがポータブルホットスポットを設定し、データをテザリングできるようにします。デフォルトは**オフ**です。
- **キーガードによるデバイスのロックを防止: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）のロック画面でキーガードを無効にします。デフォルトは**オフ**です。

- **Wi-Fiの変更を許可: オン**の場合、ユーザーはWi-Fiをオンまたはオフにしたり、Wi-Fiネットワークに接続したりできます。デフォルトは**オン**です。
- **ファイル転送を許可:** USB経由でのファイル転送を許可します。デフォルトは**オフ**です。

- **サムスン**
  - **TIMAキーストアを有効にする:** TIMAキーストアは、対称鍵用のTrustZoneベースのセキュアな鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可:** ユーザーが「共有」リスト内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。
  - **監査ログを有効にする:** デバイスのフォレンジック分析のためにイベント監査ログの作成を有効にします。デフォルトは**オフ**です。
- **Samsung: 完全管理対象デバイスのみ**
  - **ODEトラステッドブート検証を有効にする:** ODEトラステッドブート検証を使用して、ブートローダーからシステムイメージへの信頼の連鎖を確立します。デフォルトは**オン**です。
  - **緊急通話のみを許可する:** ユーザーがデバイスで緊急通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。
  - **ファームウェアの回復を許可する:** ユーザーがデバイスのファームウェアを回復できるようにします。デフォルトは**オン**です。
  - **高速暗号化を許可する:** 使用中のメモリ領域のみの暗号化を許可します。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは異なります。そのデータには、設定、アプリケーションデータ、ダウンロードされたファイルとアプリケーション、メディア、その他のファイルが含まれます。デフォルトは**オン**です。
  - **コモンクライテリアモードを有効にする:** デバイスをコモンクライテリアモードにします。コモンクライテリア構成は、厳格なセキュリティプロセスを強制します。デフォルトは**オン**です。
  - **再起動バナーを有効にする:** ユーザーのデバイスが再起動されたときに、DoD承認の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。
  - **設定変更を許可する:** ユーザーが完全管理対象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。
  - **バックグラウンドデータ使用を有効にする:** 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。完全管理対象デバイスの場合。デフォルトは**オン**です。

- **クリップボードを許可する:** ユーザーがデバイスのクリップボードにデータをコピーできるようにします。
  - **クリップボード共有を許可する:** ユーザーがデバイスとコンピューター間でクリップボードコンテンツを共有できるようにします (MDM 4.0以降)。
- **ホームキーを許可する:** ユーザーが完全管理対象デバイスで**ホーム**キーを使用できるようにします。デフォルトは**オン**です。
- **モックロケーションを許可する:** ユーザーがGPS位置情報を偽装できるようにします。完全管理対象デバイスの場合。デフォルトは**オフ**です。
- **NFC:** ユーザーが完全管理対象デバイスでNFCを使用できるようにします (MDM 3.0以降)。デフォルトは**オン**です。
- **電源オフを許可:** ユーザーが完全に管理されているデバイス (MDM 3.0 以降) の電源をオフにすることを許可します。デフォルトは**オン**です。
- **Wi-Fi Direct を許可:** ユーザーが Wi-Fi 接続を介して別のデバイスに直接接続することを許可します。デフォルトは**オン**です。**オン**の場合、**Wi-Fi 変更を許可**設定を有効にする必要があります。
- **SD カードを許可:** ユーザーが利用可能な場合、デバイスで SD カードを使用することを許可します。デフォルトは**オン**です。
- **USB ホストストレージを許可:** ユーザーのデバイスが、USB デバイスが接続されたときに USB ホストとして機能することを許可します。その後、ユーザーのデバイスは USB デバイスに電力を供給します。デフォルトは**オン**です。
- **音声ダイヤラーを許可:** ユーザーがデバイスで音声ダイヤラーを使用することを許可します (MDM 4.0 以降)。デフォルトは**オン**です。
- **Sビームを許可:** ユーザーが NFC および Wi-Fi Direct を使用して他のユーザーとコンテンツを共有することを許可します (MDM 4.0 以降)。デフォルトは**オン**です。
- **Sボイスを許可:** 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知識ナビゲーターを使用することを許可します (MDM 4.0 以降)。デフォルトは**オン**です。
- **USB テザリングを許可:** ユーザーが USB 接続を使用してモバイルデータ接続を別のデバイスと共有することを許可します。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **Bluetooth テザリングを許可:** ユーザーが Bluetooth 接続を使用してモバイルデータ接続を別のデバイスと共有することを許可します。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。

    - **Bluetooth 共有を許可:** 選択されていない場合、ユーザーはデバイスで Bluetooth 共有を確立できません。デフォルトは選択されています。この設定を表示するには、サーバープロパティ `afw.restriction.policy.v2` を有効にします。サーバープロパティの詳細については、「サーバープロパティ」を参照してください。

- **Wi-Fi テザリングを許可:** ユーザーが Wi-Fi 接続を使用してモバイルデータ接続を別のデバイスと共有することを許可します。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **受信 MMS を許可:** ユーザーが MMS メッセージを受信することを許可します。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **送信 MMS を許可:** ユーザーが MMS メッセージを送信することを許可します。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **受信 SMS を許可:** ユーザーが SMS メッセージを受信することを許可します。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **送信 SMS を許可:** ユーザーが SMS メッセージを送信することを許可します。デフォルトは**オフ**です。**オン**の場合、**SMS を許可**設定をオンにする必要があります。
- **モバイルネットワークの構成:** ユーザーが携帯データ接続を使用できるようにします。デフォルトは**オフ**です。
- **1日あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **1週間あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **1か月あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **セキュアなVPN接続のみを許可:** ユーザーがセキュアな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。
- **音声録音を許可:** ユーザーがデバイスで音声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。**オン**の場合、**マイクを許可**設定をオンにする必要があります。
- **ビデオ録画を許可:** 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**オフ**です。**オン**の場合、**カメラの使用を許可**設定をオンにする必要があります。
- **ローミング時のプッシュメッセージを許可:** ユーザーがプッシュのために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。

- **ローミング時の自動同期を許可:** ユーザーが同期のために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング時の音声通話を許可:** ユーザーが音声通話のために携帯データを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。

- **サムスン: Knox コンテナ/フルマネージド デバイス**
  - **失効チェックを有効にする:** 失効した証明書のチェックを有効にします。デフォルトは**オフ**です。

- **Samsung: Knoxコンテナのみ**
  - **アプリをコンテナに移動:** ユーザーがKnoxコンテナとデバイスの個人領域の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に、指紋とパスワードまたはPINなどの別の認証方法を使用する必要があります。デフォルトは**オン**です。
  - **コンテナの認証を強制する:** KNOXコンテナを開くために、デバイスのロック解除に使用される方法とは異なる認証方法を使用します。デフォルトは**オン**です。
  - **セキュアキーパッドを有効にする:** Knoxコンテナ内でセキュアキーボードの使用をユーザーに強制します。デフォルトは**オン**です。

- **サムスン: DeX**
  - **Samsung DeXを有効にする:** サポートされているKnox対応デバイスがSamsung DeXモードで実行できるようにします。Samsung Knox 3.1 (最小バージョン) が必要です。デフォルトは**オン**です。Samsung DeXのデバイス要件と設定については、Samsung Developersのドキュメントを参照してください。
    - **DeXモードでのみイーサネットを許可する:** Samsung DeXモードでのイーサネットの使用を有効にします。DeXモードでは、モバイルデータ、Wi-Fi、およびテザリング (Wi-Fi、Bluetooth、USB) が制限されます。デフォルトは選択されていません。
    - **DeXロゴ画像をアップロードする:** Samsung DeXのアイコンとして使用する.png画像を指定するには、この設定を選択します。
    - **DeX画面のタイムアウト (秒):** DeX画面がオフになるまでのアイドル時間 (秒単位) を指定します。タイムアウトを無効にするには、「**0**」と入力します。デフォルトは**1200**秒 (20分) です。

- **Samsung DeXにアプリのショートカットを追加する:** アプリのショートカットをDeXに追加するには、アプリのパッケージ名を指定します。アプリのパッケージ名を調べるには、Google Playにアクセスしてアプリを選択します。URLにはパッケージ名が含まれています: `https://play.google.com/store/apps/details?id=<package.name>`。
- **Samsung DeXからアプリのショートカットを削除する:** DeXからショートカットを削除するには、アプリのパッケージ名を指定します。アプリのパッケージ名を調べるには、Google Playにアクセスしてください。
- **Samsung DeXで無効にするアプリパッケージ:** Samsung DeXモードでブロックするアプリパッケージのコンマ区切りリストを指定します。例: `"com.android.chrome", "com.google.android.gm"`。

「ワークプロファイルを持つ完全に管理されたデバイスに適用」がオンで、**「ワークプロファイルを持つ完全に管理されたデバイスの場合、ポリシーを適用する対象」**が**「ワークプロファイル」**に設定されている場合、次の設定を構成します。

- **セキュリティ**
  - **アカウント管理を許可する:** ワークプロファイルと管理対象デバイスに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。
  - **プロファイル間のコピーと貼り付けを許可する: オン**の場合、ユーザーはAndroid Enterpriseプロファイルのアプリと個人領域のアプリの間でコピー＆ペーストできます。デフォルトは**オフ**です。
  - **画面キャプチャを許可する:** ユーザーがデバイス画面を録画またはスクリーンキャプチャできるようにします。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影できるようにします。デフォルトは**オフ**です。
  - **位置情報プロバイダーの設定を許可:** 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以降の場合。デフォルトは**オン**です。
  - **位置情報の共有を許可:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

> **ヒント:**
>
> XenMobileで位置情報デバイスポリシーを作成して、地理的境界を適用できます。位置情報デバイスポリシーを参照してください。

- **ユーザー資格情報の設定を許可:** ユーザーが管理対象キーストアで資格情報を設定できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可:** **オン**の場合、ユーザーはユーザーデバイスからアクセス可能な任意のプリンターに印刷できます。デフォルトは**オフ**です。対象: Android 9以降。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされたデバイスアプリを実行できるようにします。デフォルトは**オフ**です。特定のアプリを有効にするには、**システムアプリリスト**テーブルで**追加**をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリストです。**システムアプリを有効にする**を**オン**に設定し、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調べるには、Android Debug Bridge (`adb`) を使用してAndroidパッケージマネージャー (`pm`) コマンドを呼び出すことができます。たとえば、`adb shell "pm list packages -f name"` のように、「name」はパッケージ名の一部です。詳細については、`<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アプリの権限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にする:** 指定されたアプリのリストがデバイスで実行されないようにブロックします。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、**アプリケーションリスト**テーブルで**追加**をクリックします。
    - **アプリケーションリスト:** 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、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストが上書きされます。例: com.example1とcom.example2を無効にし、後でリストをcom.example1とcom.example3に変更した場合、XenMobileはcom.example.2を有効にします。
  - **アプリの検証を有効にする:** 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アプリを有効にする:** ユーザーがGoogle Mobile Services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。
  - **Google Play以外のアプリを許可:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
  - **アプリケーション設定のユーザー制御を許可:** ユーザーがアプリのアンインストール、アプリの無効化、キャッシュとデータのクリア、任意のアプリの強制停止、およびデフォルト

のクリアを実行できるようにします。ユーザーはこれらの操作をアプリから実行します。デフォルトは**オフ**です。

- **アプリのアンインストールを許可:** ユーザーがManaged Google Playストア内からアプリをアン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。この設定を表示するには、サーバープロパティ`afw.restriction.policy.v2`を有効にします。サーバープロパティの詳細については、サーバープロパティを参照してください。
- **仕事用プロファイルと個人用プロファイルからのメールアプリへのアクセス:** 設定が**オン**の場合、ユーザーは個人用プロファイルから仕事用プロファイルのメールアプリにアクセスして使用できます。デフォルトは**オフ**です。

- **BYOD仕事用プロファイル**
  - **ホーム画面での仕事用プロファイルアプリ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ァイルアプリウィジェットをデバイス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ァイルアプリウィジェットをデバイスのホーム画面に配置できません。デフォルトは**オフ**です。
    - **ウィジェットが許可されているアプリ:** ホーム画面で許可するアプリのリストです。「**ホーム画面での仕事用プロファイルアプリウィジェットを許可**」を**オン**に設定し、アプリを追加します。「**追加**」をクリックし、ホーム画面でウィジェットを許可するアプリをリストから選択します。「**保存**」をクリックします。このプロセスを繰り返して、さらに多くのアプリウィジェットを許可します。
  - **デバイスの連絡先に仕事用プロファイルの連絡先を許可:** 管理対象のAndroid Enterpriseプロファイルからの連絡先を、着信時に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。

- **サムスン**
  - **TIMAキーストアを有効にする:** TIMAキーストアは、対称鍵用のTrustZoneベースのセキュアな鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可:** ユーザーが「共有」リスト内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。
  - **監査ログを有効にする:** デバイスのフォレンジック分析のためのイベント監査ログの作成を有効にします。デフォルトは**オフ**です。

- **サムスン: Knoxコンテナ/完全に管理されたデバイス**

- **失効チェックを有効にする:** 失効した証明書のチェックを有効にします。デフォルトは**オフ**です。

- **Samsung: Knoxコンテナのみ**
  - **アプリをコンテナに移動:** ユーザーがKnoxコンテナとデバイスの個人領域の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。
  - **多要素認証を強制する:** ユーザーは、デバイスを開くために、指紋とパスワードまたはPINなどの別の認証方法を使用する必要があります。デフォルトは**オン**です。
  - **コンテナの認証を強制する:** KNOXコンテナを開くには、デバイスのロック解除に使用した方法とは異なる認証方法を使用します。デフォルトは**オン**です。
  - **セキュアキーパッドを有効にする:** Knoxコンテナ内でセキュアキーボードを使用するようユーザーに強制します。デフォルトは**オン**です。

ワークプロファイルを持つ完全に管理されたデバイスに適用がオンで、**ワークプロファイルを持つ完全に管理されたデバイスの場合、ポリシーを適用する対象**が**管理対象デバイス**に設定されている場合、以下の設定を構成します。

- **セキュリティ**
  - **アカウント管理を許可する:** ワークプロファイルおよび管理対象デバイスに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。
  - **プロファイル間のコピー＆ペーストを許可する: オン**の場合、ユーザーはAndroid Enterpriseプロファイルのアプリと個人領域のアプリの間でコピー＆ペーストできます。デフォルトは**オフ**です。
  - **スクリーンキャプチャを許可する:** ユーザーがデバイス画面を録画またはスクリーンキャプチャできるようにします。デフォルトは**オフ**です。
  - **カメラの使用を許可する:** ユーザーがデバイスのカメラで写真やビデオを撮影できるようにします。デフォルトは**オフ**です。
  - **VPN構成を許可する:** ユーザーがVPN構成を作成できるようにします。Android 6以降を実行しているワークプロファイルデバイスおよび完全に管理されたデバイスの場合。デフォルトは**オン**です。
  - **バックアップサービスを許可する:** ユーザーがデバイス上のアプリケーションデータと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。
  - **NFCを許可する:** ユーザーがNFC（近距離無線通信）を使用して、デバイスから別のデバイスにウェブページ、写真、ビデオ、またはその他のコンテンツを送信できるようにします。MDM 4.0以降の場合。デフォルトは**オン**です。

- **位置情報プロバイダーの設定を許可する:** 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以降の場合。デフォルトは**オン**です。
- **位置情報共有を許可する:** 管理対象プロファイルの場合、デバイス所有者がこの設定を上書きできます。デフォルトは**オフ**です。

> **ヒント:**
>
> XenMobileでロケーションデバイスポリシーを作成して、地理的境界を適用できます。ロケーションデバイスポリシーを参照してください。

- **ユーザーがユーザー資格情報を構成することを許可する:** ユーザーが管理対象キーストアで資格情報を構成できるかどうかを指定します。デフォルトは**オン**です。
- **印刷を許可する: オン**の場合、ユーザーはユーザーデバイスからアクセス可能な任意のプリンターに印刷できます。デフォルトは**オフ**です。対象: Android 9以降。
- **USBデバッグを許可する:** デフォルトは**オフ**です。

- **アプリ**
  - **システムアプリを有効にする:** ユーザーがプリインストールされたデバイスアプリを実行できるようにします。デフォルトは**オフ**です。特定のアプリを有効にするには、**システムアプリリスト**テーブルで**追加**をクリックします。
    - **システムアプリリスト:** デバイスで有効にするシステムアプリのリストです。**システムアプリを有効にする**を**オン**に設定し、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`) コマンドを呼び出すことができます。例: `adb shell "pm list packages -f name"` （「name」はパッケージ名の一部です）。詳細については、`<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アプリの権限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にする:** 指定されたアプリのリストがデバイス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、**アプリケーションリスト**テーブルで**追加**をクリックします。
    - **アプリケーションリスト:** 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、アプリを追加します。アプリのパッケージ名を入力します。アプリリストを変更して展開すると、以前のアプリリストは上書きされます。例:

com.example1とcom.example2を無効にし、その後リストをcom.example1とcom.example3に変更した場合、XenMobileはcom.example.2を有効にします。

- **アプリの検証を有効にする:** 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アプリを有効にする:** ユーザーがGoogle Mobile Services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。
- **Google Play以外のアプリを許可する:** Google Play以外のストアからのアプリのインストールを許可します。デフォルトは**オフ**です。
- **ユーザーによるアプリケーション設定の制御を許可する:** ユーザーがアプリのアンインストール、アプリの無効化、キャッシュとデータのクリア、任意のアプリの強制停止、およびデフォルトのクリアを行えるようにします。ユーザーはこれらのアクションを「設定」アプリから実行します。デフォルトは**オフ**です。
- **アプリのアンインストールを許可する:** ユーザーがManaged Google Playストア内からアプリをアン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。この設定を表示するには、サーバープロパティ `afw.restriction.policy.v2` を有効にします。サーバープロパティの詳細については、サーバープロパティを参照してください。

- **完全に管理されたデバイスのみ**
  - **ユーザーの追加を許可:** ユーザーがデバイスに新しいユーザーを追加することを許可します。デフォルトは**オン**です。
  - **データローミングを許可:** ユーザーがローミング中にモバイルデータを使用することを許可します。デフォルトはオフで、ユーザーのデバイスでのローミングを無効にします。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することを許可します。デフォルトは**オフ**です。
  - **ステータスバーの使用を許可: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）でステータスバーを有効にします。この設定は、通知、クイック設定、およびフルスクリーンモードからの脱出を可能にするその他の画面オーバーレイを無効にします。ユーザーはシステム設定に移動して通知を確認できます。Android 6.0以降の場合。デフォルトは**オフ**です。
  - **Bluetoothを許可:** ユーザーがBluetoothを使用することを許可します。デフォルトは**オン**です。
    - **Bluetooth共有を許可:** 選択されていない場合、ユーザーはデバイスでBluetoothによる発信共有を確立できません。デフォルトは選択されています。この設定を表示するに

は、サーバープロパティ`afw.restriction.policy.v2`を有効にします。サーバープロパティの詳細については、「サーバープロパティ」を参照してください。

- **日付と時刻の設定を許可:** ユーザーがデバイスの日付と時刻を変更することを許可します。デフォルトは**オン**です。
- **工場出荷時設定へのリセットを許可:** ユーザーがデバイスを工場出荷時設定にリセットすることを許可します。デフォルトは**オン**です。
- **デバイス画面をオンのままにする:** この設定が**オン**の場合、デバイスが接続されている間、デバイス画面はオンのままになります。デフォルトは**オフ**です。
- **USB大容量ストレージを許可:** ユーザーのデバイスとコンピューター間でUSB接続を介して大容量データファイルを転送することを許可します。デフォルトは**オン**です。
- **マイクを許可:** ユーザーがデバイスのマイクを使用することを許可します。デフォルトは**オン**です。
- **テザリングを許可:** ユーザーがポータブルホットスポットを設定し、データをテザリングすることを許可します。デフォルトは**オフ**です。この設定がオンの場合、Samsungデバイスでは次の設定が利用可能です。
- **キーガードによるデバイスのロックを防止: オン**の場合、この設定は管理対象デバイスおよび専用デバイス（COSUデバイスとも呼ばれる）のロック画面でキーガードを無効にします。デフォルトは**オフ**です。
- **Wi-Fiの変更を許可: オン**の場合、ユーザーはWi-Fiをオンまたはオフにしたり、Wi-Fiネットワークに接続したりできます。デフォルトは**オン**です。
- **ファイル転送を許可:** USB経由でのファイル転送を許可します。デフォルトは**オフ**です。

- **サムスン**
  - **TIMAキーストアを有効にする:** TIMAキーストアは、対称鍵用のTrustZoneベースの安全な鍵ストレージを提供します。RSA鍵ペアと証明書は、ストレージのためにデフォルトのキーストアプロバイダーにルーティングされます。デフォルトは**オフ**です。
  - **共有リストを許可する:** ユーザーがリスト内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。
  - **監査ログを有効にする:** デバイスのフォレンジック分析のためのイベント監査ログの作成を有効にします。デフォルトは**オフ**です。
- **Samsung: 完全管理対象デバイスのみ**

- **ODEトラステッドブート検証を有効にする:** ブートローダーからシステムイメージへの信頼の連鎖を確立するために、ODEトラステッドブート検証を使用します。デフォルトは**オン**です。
- **緊急通話のみを許可する:** ユーザーがデバイスで緊急通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。
- **ファームウェアの回復を許可する:** ユーザーがデバイスのファームウェアを回復できるようにします。デフォルトは**オン**です。
- **高速暗号化を許可する:** 使用済みメモリ領域のみの暗号化を許可します。この暗号化は、すべてのデータを暗号化するフルディスク暗号化とは異なります。そのデータには、設定、アプリケーションデータ、ダウンロードされたファイルとアプリケーション、メディア、その他のファイルが含まれます。デフォルトは**オン**です。
- **コモンクライテリアモードを有効にする:** デバイスをコモンクライテリアモードにします。コモンクライテリア構成は、厳格なセキュリティプロセスを強制します。デフォルトは**オン**です。
- **再起動バナーを有効にする:** ユーザーのデバイスが再起動されたときに、DoD承認の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。
- **設定変更を許可する:** ユーザーが完全管理対象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。
- **バックグラウンドデータ使用を有効にする:** 完全管理対象デバイスの場合、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。デフォルトは**オン**です。
- **クリップボードを許可する:** ユーザーがデバイスのクリップボードにデータをコピーできるようにします。デフォルトは**オン**です。
  - **クリップボード共有を許可する:** ユーザーがデバイスとコンピューター間でクリップボードコンテンツを共有できるようにします（MDM 4.0以降）。
- **ホームキーを許可:** ユーザーが完全に管理されたデバイスで**ホーム**キーを使用できるようにします。デフォルトは**オン**です。
- **擬似ロケーションを許可:** ユーザーがGPS位置情報を偽装できるようにします。完全に管理されたデバイスの場合。デフォルトは**オフ**です。
- **NFC:** ユーザーが完全に管理されたデバイスでNFCを使用できるようにします (MDM 3.0以降)。デフォルトは**オン**です。
- **電源オフを許可:** ユーザーが完全に管理されたデバイスの電源をオフにできるようにします (MDM 3.0以降)。デフォルトは**オン**です。

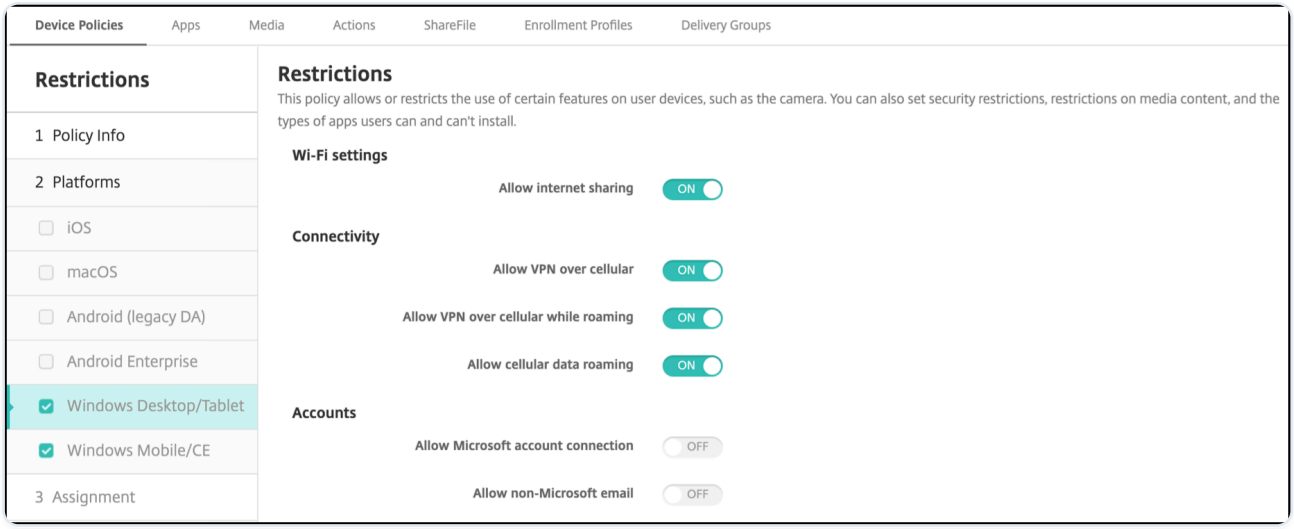
- **Wi-Fi Directを許可:** ユーザーがWi-Fi接続を介して別のデバイスに直接接続できるようにします。デフォルトは**オン**です。**オン**の場合、**Wi-Fi変更を許可**設定を有効にする必要があります。
- **SDカードを許可:** ユーザーが利用可能なSDカードをデバイスで使用できるようにします。デフォルトは**オン**です。
- **USBホストストレージを許可:** ユーザーのデバイスが、USBデバイスが接続されたときにUSBホストとして機能できるようにします。その後、ユーザーのデバイスはUSBデバイスに電力を供給します。デフォルトは**オン**です。
- **音声ダイヤラーを許可:** 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。
- **Sビームを許可:** ユーザーがNFCとWi-Fi Directを使用して他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。
- **Sボイスを許可:** 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知識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。
- **USBテザリングを許可:** ユーザーがUSB接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **Bluetoothテザリングを許可:** ユーザーがBluetooth接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **Wi-Fiテザリングを許可:** ユーザーがWi-Fi接続を使用してモバイルデータ接続を別のデバイスと共有できるようにします。デフォルトは**オフ**です。**オン**の場合、**テザリングを許可**設定も**オン**にする必要があります。
- **受信MMSを許可:** 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**オフ**です。**オン**の場合、**SMSを許可**設定をオンにする必要があります。
- **送信MMSを許可:** 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**オフ**です。**オン**の場合、**SMSを許可**設定をオンにする必要があります。
- **受信SMSを許可:** ユーザーがSMSメッセージを受信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMSを許可**設定をオンにする必要があります。
- **送信SMSを許可:** ユーザーがSMSメッセージを送信できるようにします。デフォルトは**オフ**です。**オン**の場合、**SMSを許可**設定をオンにする必要があります。
- **モバイルネットワークを構成:** ユーザーがモバイルデータ接続を使用できるようにします。デフォルトは**オフ**です。

- **1日あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **1週間あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **1か月あたりの制限 (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、この機能は無効になります (MDM 4.0以降)。
- **セキュアなVPN接続のみを許可:** ユーザーがセキュアな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。
- **音声録音を許可:** ユーザーがデバイスで音声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。**オン**の場合、**マイクを許可**設定をオンにする必要があります。
- **ビデオ録画を許可:** 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**オフ**です。**オン**の場合、**カメラの使用を許可**設定をオンにする必要があります。
- **ローミング時のプッシュメッセージを許可:** ユーザーがプッシュのためにモバイルデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング時の自動同期を許可:** ユーザーが同期のためにモバイルデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。
- **ローミング時の音声通話を許可:** ユーザーが音声通話のためにモバイルデータを使用できるようにします。デフォルトは**オフ**です。**オン**の場合、**データローミングを許可**設定を有効にする必要があります。

- **サムスン: ノックス コンテナ/フルマネージドデバイス**
  - **失効チェックを有効にする:** 失効した証明書のチェックを有効にします。デフォルトは**オフ**です。
- **Samsung: Knoxコンテナのみ**
  - **アプリをコンテナに移動:** ユーザーがKnoxコンテナとデバイスの個人領域の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に、指紋とパスワードまたはPINなどの別の認証方法を使用する必要があります。デフォルトは**オン**です。
  - **コンテナの認証を強制:** デバイスのロック解除に使用される方法とは異なる認証方法を使用して、KNOXコンテナを開きます。デフォルトは**オン**です。

- **セキュアキーパッドを有効にする:** ユーザーにKnoxコンテナ内でセキュアキーボードの使用を強制します。デフォルトは**オン**です。

Windowsデスクトップ/タブレットの設定



- **Wi-Fi設定**
  - **インターネット共有を許可:** デバイスをWi-Fiホットスポットに変えることで、他のデバイスとインターネット接続を共有できるようにします。
- **接続**
  - **携帯電話ネットワーク経由のVPNを許可:** デバイスがVPN経由で携帯電話ネットワークに接続できるようにします。
  - **ローミング中の携帯電話ネットワーク経由のVPNを許可:** デバイスが携帯電話ネットワーク上でローミングしているときに、VPN経由で接続できるようにします。
  - **携帯電話データローミングを許可:** ユーザーがローミング中に携帯電話データを使用できるようにします。
- **アカウント**
  - **Microsoftアカウント接続を許可:** デバイスが、メール以外の接続認証およびサービスに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。
- **システム**
  - **ストレージカードを許可:** デバイスがストレージカードを使用することを許可します。

- **テレメトリ:** ドロップダウンリストからオプションを選択して、デバイスがテレメトリ情報を送信することを許可または制限します。デフォルトは**許可**です。その他のオプションは、**許可しない**および**セカンダリデータ要求を除く許可**です。
- **位置情報サービスを許可:** 位置情報サービスを許可します。
- **内部ビルドのプレビューを許可:** ユーザーがMicrosoftの内部ビルドをプレビューすることを許可します。

- **カメラ:**
  - **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することを許可します。
- **ブルートゥース:**
  - **検出モードを許可:** Bluetoothデバイスがローカルデバイスを検出することを許可します。
  - **ローカルデバイス名:** ローカルデバイスの名前。
- **エクスペリエンス:**
  - **Cortanaを許可:** ユーザーがインテリジェントパーソナルアシスタントおよび知識ナビゲーターであるCortanaにアクセスすることを許可します。
  - **デバイスの検出を許可:** デバイスのネットワーク検出を許可します。
  - **手動MDM登録解除を許可:** ユーザーがXenMobile MDMからデバイスを手動で登録解除することを許可します。
  - **デバイス設定の同期を許可:** ユーザーがローミング中にWindows 10デバイスとWindows 11デバイス間で設定を同期することを許可します。
- **ロック画面より上:**
  - **トーストを許可:** ロック画面でのトースト通知を許可します。
- **アプリ**
  - **アプリストアの自動更新を許可:** アプリストアからのアプリの自動更新を許可します。
- **プライバシー:**
  - **入力のパーソナライズを許可:** ユーザーが入力した内容に基づいて、ペンやタッチキーボードなどの予測入力を改善するために、入力パーソナライズサービスを実行することを許可します。
- **設定:**

- **自動再生を許可:** ユーザーが自動再生設定を変更することを許可します。
- **データ使用状況を許可:** ユーザーがデータ使用状況の設定を変更することを許可します。
- **日付と時刻を許可:** ユーザーが日付と時刻の設定を変更することを許可します。
- **言語を許可:** ユーザーが言語設定を変更することを許可します。
- **電源とスリープを許可:** ユーザーが電源とスリープの設定を変更することを許可します。
- **地域を許可:** ユーザーが地域設定を変更することを許可します。
- **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することを許可します。
- **職場を許可:** ユーザーが職場設定を変更することを許可します。
- **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。

ローミングデバイスポリシー

XenMobileでデバイスポリシーを追加して、ユーザーのiOSデバイスで音声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。音声ローミングが無効になっている場合、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利用可能です。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

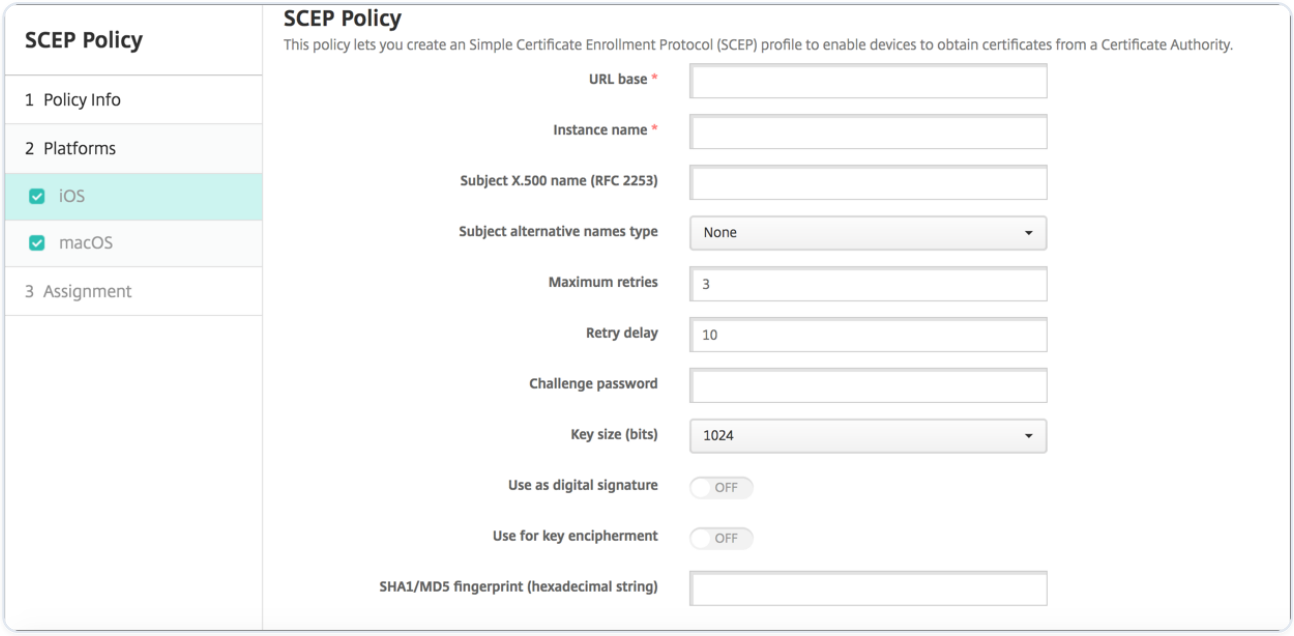
- **音声ローミングを無効にする:** 音声ローミングを無効にするかどうかを選択します。このオプションが有効になっている場合、データローミングは自動的に無効になります。デフォルトは**オフ**で、音声ローミングが許可されます。
- **データローミングを無効にする:** データローミングを無効にするかどうかを選択します。このオプションは、音声ローミングが有効になっている場合にのみ利用可能です。デフォルトは**オフ**で、データローミングが許可されます。

SCEPデバイスポリシー

このポリシーを使用すると、iOSおよびmacOSデバイスを構成して、外部のSCEPサーバーからSimple Certificate Enrollment Protocol (SCEP) を使用して証明書を取得できます。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信する場合は、分散モードでPKIエンティティとPKIプロバイダーを作成する必要があります。詳細については、「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、 > 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設定



- **URLベース:** SCEP要求がHTTPまたはHTTPS経由で送信される場所を定義するために、SCEPサーバーのアドレスを入力します。秘密鍵は証明書署名要求 (CSR) と一緒に送信されないため、要求を暗号化せずに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を使用する必要があります。この手順は必須です。
- **インスタンス名:** SCEPサーバーが認識する任意の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も構いません。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。この手順は必須です。
- **サブジェクトX.500名 (RFC 2253):** オブジェクト識別子 (OID) と値の配列として表現されるX.500名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 は、次のように変換される場合があります: \[\[\["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \]。OIDは、国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) のショートカットを使用して、ドット区切りの数値として表現できます。
- **サブジェクトの別名タイプ:** ドロップダウンリストで別名タイプをクリックします。SCEPポリシーでは、証明書の発行にCAが必要とする値を提供するオプションの別名タイプを指定できます。、、、または**** を指定できます。
- **最大再試行回数:** SCEPサーバーがPENDING応答を送信したときに、デバイスが再試行できる回数を入力します。デフォルトは**3**です。

- **再試行遅延:** 後続の再試行の間に待機する秒数を入力します。最初の再試行は遅延なしで試行されます。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):** キーサイズをビット単位で**2048**以上に選択します。
- **デジタル署名として使用:** 証明書をデジタル署名として使用するかどうかを指定します。誰かがデジタル署名を検証するために証明書を使用している場合 (たとえば、証明書がCAによって発行されたかどうかを検証する場合)、SCEPサーバーは、公開鍵を使用してハッシュを復号化する前に、証明書がこの方法で使用できることを検証します。
- **キー暗号化に使用:** 証明書をキー暗号化に使用するかどうかを指定します。サーバーがクライアントから提供された証明書の公開鍵を使用して、データが秘密鍵で暗号化されたことを検証する場合、サーバーはまず証明書がキー暗号化に使用できるかどうかを確認します。使用できない場合、操作は失敗します。
- **SHA1/MD5フィンガープリント (16進数文字列):** CAがHTTPを使用している場合、このフィールドを使用してCA証明書のフィンガープリントを指定します。デバイスは登録中にCA応答の信頼性を確認するためにこれを使用します。SHA1またはMD5フィンガープリントを入力するか、証明書を選択してその署名をインポートできます。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

macOS設定

デバイスポリシー設定画面の画像(/en-us/xenmobile/server/media/device-policy-scep-macos.png)

- **URLベース:** SCEPリクエストがHTTPまたはHTTPS経由でどこに送信されるかを定義するために、SCEPサーバーのアドレスを入力します。秘密鍵は証明書署名要求 (CSR) と一緒に送信されないため、暗号化されていないリクエストを送信しても安全です。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を使用する必要があります。この手順は必須です。
- **インスタンス名:** SCEPサーバーが認識する任意の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も構いません。CAが複数のCA証明書を持っている場合、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。この手順は必須です。

- **サブジェクトX.500名 (RFC 2253):** オブジェクト識別子 (OID) と値の配列として表現されるX.500名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 は、\[\[\ ["C", "US"\] \], \[\["O", "Apple Inc."\] \], ..., \[\["1.2.5.3", "bar" \] \] \] となります。OIDは、国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) のショートカットを持つドット区切りの数値として表現できます。
- **サブジェクト代替名タイプ:** ドロップダウンリストから代替名タイプをクリックします。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タイプを指定できます。**なし**、**RFC 822名**、**DNS名**、または**URI**を指定できます。
- **最大再試行回数:** SCEPサーバーがPENDING応答を送信したときに、デバイスが再試行できる回数を入力します。デフォルトは**3**です。
- **再試行遅延:** その後の再試行の間に待機する秒数を入力します。最初の再試行は遅延なしで試行されます。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):** キーサイズをビット単位で**2048**以上に選択します。
- **デジタル署名として使用:** 証明書をデジタル署名として使用するかどうかを指定します。誰かがデジタル署名を検証するために証明書を使用している場合（例えば、証明書がCAによって発行されたかどうかを検証する場合など）、SCEPサーバーは、公開鍵を使用してハッシュを復号化する前に、証明書がこの方法で使用できることを検証します。
- **鍵の暗号化に使用:** 証明書を鍵の暗号化に使用するかどうかを指定します。サーバーがクライアントから提供された証明書の公開鍵を使用して、データが秘密鍵で暗号化されたことを検証する場合、サーバーはまず証明書が鍵の暗号化に使用できるかどうかを確認します。使用できない場合、操作は失敗します。
- **SHA1/MD5フィンガープリント (16進数文字列):** CAがHTTPを使用している場合、このフィールドを使用してCA証明書のフィンガープリントを指定します。これは、デバイスが登録中にCA応答の信頼性を確認するために使用します。SHA1またはMD5フィンガープリントを入力するか、証明書を選択してその署名をインポートできます。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間 (時間)**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間 (時間):** ポリシーが削除されるまでの時間を時間単位で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**なし**を選択しま

す。**パスコードが必要**を選択した場合、**削除パスコード**フィールドにパスコードを入力します。

- **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションはmacOS 10.7以降でのみ利用可能です。

Siriと音声入力のポリシー

ユーザーが管理対象のiOSデバイスでSiriに何かを尋ねたり、テキストを音声入力したりすると、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経由するため、安全なXenMobile®コンテナの外部に存在します。ただし、音声入力の結果として生成されたテキストはコンテナ内に残ります。

XenMobileでは、セキュリティ要件に応じてSiriおよび音声入力サービスをブロックできます。

MAM展開では、各アプリの**音声入力をブロック**ポリシーは、デフォルトで**オン**になっています。これにより、デバイスのマイクが無効になります。音声入力を許可する場合は、**オフ**に設定します。このポリシーは、XenMobileコンソールの**構成 > アプリ**で確認できます。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。

アプリ構成画面の画像(/en-us/xenmobile/server/media/device-policy-siri-dictation-off.png)

MDM展開では、**構成 > デバイスポリシー**にあるSiriポリシーを使用して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。

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-siri-restrictions-on.png)

Siriと音声入力を許可するかどうかを決定する際に留意すべき点がいくつかあります。

- Appleが公開した情報によると、AppleはSiriと音声入力の音声クリップデータを最大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。詳細については、Wiredの記事「Apple reveals how long Siri keeps your data」を参照してください。
- Appleのプライバシーポリシーは、任意のiOSデバイスで**設定 > 一般 > キーボード**に移動し、**音声入力を有効にする**の下にあるリンクをタップすることで確認できます。

SSOアカウントデバイスポリシー

XenMobile®でシングルサインオン (SSO) アカウントを作成すると、ユーザーはさまざまなアプリからXenMobileおよび社内リソースに1回だけサインオンしてアクセスできるようになります。ユーザーはデバイスに資格情報を保存する必要はありません。SSOアカウントのエンタープライズユーザー資格情報は、App Storeのアプリを含む、すべてのアプリで使用されます。このポリシーは、Kerberos認証バックエンドと連携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設定

- **アカウント名：**ユーザーのデバイスに表示される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）：**ユーザーの操作なしでKerberos資格情報を更新するために使用できる、ドロップダウンリストのオプションのID資格情報をクリックします。
- **Kerberosレルム：**このポリシーのKerberosレルムを入力します。この設定値は通常、すべて大文字のドメイン名です（例：EXAMPLE.COM）。このフィールドは必須です。
- **許可されたURL：**__SSOを必須にする各URLについて、__［追加］**をクリックし、次の操作を行います。
    - **許可されたURL：**ユーザーがiOSデバイスからURLにアクセスしたときにSSOを必須にするURLを入力します。

      たとえば、ユーザーがサイトを閲覧しようとして、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リストにない場合、iOSデバイスは、以前のKerberosログオンからデバイスにキャッシュされている可能性のあるKerberosトークンを提供してSSOを試行しません。一致はURLのホスト部分で正確である必要があります。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、ホストの一致に基づいてKerberosがアクティブ化されていない場合でも、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がKerberosを使用したSSOの

みに構成されている場合、標準のパスワードチャレンジやHTTPエラーなど、ほぼ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の追加をキャンセルします。

- **アプリ識別子：**このログインの使用が許可されている各アプリについて、［追加］**をクリックし、次の操作を行います。
  - **アプリケーション識別子:** このログインの使用が許可されているアプリのアプリケーション識別子を入力します。アプリケーション識別子を追加しない場合、このログインは**すべて**のアプリケーション識別子に一致します。
  - アプリケーション識別子を追加するには、**追加**をクリックするか、アプリケーション識別子の追加をキャンセルするには、**キャンセル**をクリックします。

- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

ストアデバイスポリシー

XenMobile®でポリシーを作成し、iOS、Android、またはWindowsタブレットデバイスがXenMobileストアのWebクリップをデバイスのホーム画面に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、 > に移動します。詳細については、「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

構成する各プラットフォームについて、XenMobileストアのWebクリップをユーザーデバイスに表示するかどうかを選択します。デフォルトは****です。

購読済みカレンダーデバイスポリシー

XenMobileでデバイスポリシーを追加して、iOSデバイスのカレンダーリストに購読済みカレンダーを追加できます。購読できる公開カレンダーのリストは、www.apple.com/downloads/macosx/calendarsで入手できます。

このポリシーを追加または構成するには、 > に移動します。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

ユーザーデバイスの購読済みカレンダーリストに追加する前に、カレンダーを購読しておく必要があります。

iOS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。`webcal://` URLまたはiCalendarファイル（.ics）への `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:** オプションのユーザーパスワードを入力します。
- **SSLを使用:** カレンダーへの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。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

利用規約デバイスポリシー

ユーザーに企業ネットワークへの接続を管理する会社の特定のポリシーを受け入れてもらいたい場合、XenMobile® で利用規約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際、利用規約が表示され、デバイスを登録するにはそれらを受け入れる必要があります。利用規約を拒否すると、登録プロセスはキャンセルされます。

会社に海外のユーザーがいて、彼らが母国語で利用規約を受け入れることを望む場合、異なる言語で利用規約の異なるポリシーを作成できます。展開を計画しているプラットフォームと言語の組み合わせごとにファイルを提供する必要があります。Android および iOS デバイスの場合、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、テキスト (.txt) ファイルと付随する画像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、 > に移動します。詳細については、「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:** をクリックしてファイルの場所に移動し、インポートする利用規約ファイルを選択します。
- **デフォルトの利用規約:** このファイルが、異なる利用規約を持つ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ドキュメントであるかどうかを選択します。デフォルトは です。

Windows タブレットの設定

- **インポートするファイル:** をクリックしてファイルの場所に移動し、インポートする利用規約ファイルを選択します。
- **画像:** をクリックしてファイルの場所に移動し、インポートする画像ファイルを選択します。
- **デフォルトの利用規約:** このファイルが、異なる利用規約を持つ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ドキュメントであるかどうかを選択します。デフォルトは です。

VPNデバイスポリシー

VPNデバイスポリシーは、ユーザーデバイスが企業リソースに安全に接続できるようにする仮想プライベートネットワーク (VPN) 設定を構成します。VPNデバイスポリシーは、以下のプラットフォーム用に構成できます。各プラットフォームには異なる値のセットが必要であり、それらについてはこの記事で詳しく説明します。

このポリシーを追加または構成するには、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

アプリごとのVPNの要件

アプリごとのVPN機能は、VPNポリシーを介して以下のプラットフォーム用に構成します。

- iOS
- macOS
- Android (レガシーDA)
- サムスン セーフ
- サムスン ノックス

Android Enterpriseデバイスの VPNを構成するには、Citrix SSOアプリの管理対象構成デバイスポリシーを作成します。「Android Enterprise向けVPNプロファイルの構成」を参照してください。

アプリごとのVPNオプションは、特定の接続タイプで利用できます。次の表は、アプリごとのVPNオプションが利用可能な場合を示しています。

プラットフォーム	接続タイプ	備考
iOS	Cisco レガシー AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix SSO、またはカスタム SSL。	
macOS	Cisco AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、またはカスタムSSL。	
Android (レガシーDA)	シトリックス SSO	
サムスン SAFE	IPSEC、SSL	VPNの種類を**Generic**に設定
サムスン Knox	IPSEC、SSL	VPNの種類を**Generic**に設定

Citrix SSOアプリを使用してiOSおよびAndroid (レガシーDA) デバイス用のアプリごとのVPNを作成するには、VPNポリシー構成に加えて、追加の手順を実行する必要があります。また、以下の前提条件が満たされていることを確認する必要があります。

- オンプレミスのCitrix Gateway
- デバイスに以下のアプリケーションがインストールされていること:
  - シトリックス SSO
  - シトリックス セキュアハブ™

iOSおよびAndroidデバイス向けにCitrix SSOアプリを使用してアプリごとのVPNを構成する一般的なワークフローは次のとおりです。

1. この記事で説明されているように、VPNデバイスポリシーを構成します。

- *iOS* の場合は、iOS向けCitrix SSOプロトコルの構成を参照してください。VPNデバイスポリシーを介してiOS向けCitrix SSOプロトコルを構成した後、アプリをアプリごとのVPNポリシーに関連付けるために、アプリ属性ポリシーも作成する必要があります。詳細については、アプリごとのVPNの構成を参照してください。
    - **接続の認証タイプ**フィールドで**証明書**を選択した場合、まずEndpoint Managementの証明書ベースの認証を構成する必要があります。クライアント証明書または証明書とドメイン認証を参照してください。
- *Android (レガシーDA)* の場合は、Android向けCitrix SSOプロトコルの構成を参照してください。
    - **接続の認証タイプ**フィールドで**証明書**または**パスワードと証明書**を選択した場合、まずEndpoint Managementの証明書ベースの認証を構成する必要があります。クライアント証明書または証明書とドメイン認証を参照してください。

2. アプリごとのVPNからのトラフィックを受け入れるようにCitrix ADCを構成します。詳細については、Citrix Gatewayでの完全なVPNセットアップを参照してください。

iOS設定

iOS 12へのデバイスアップグレードの準備:

iOS向け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。既存のVPNデバイスポリシーを削除し、Citrix SSO接続タイプでVPNデバイスポリシーを作成するには、次の手順を実行します。

1. iOS向けVPNデバイスポリシーを削除します。
2. iOS向けVPNデバイスポリシーを追加します。重要な設定:
    - **接続タイプ** = **Citrix SSO**
    - **アプリごとのVPNを有効にする** = **オン**
    - **プロバイダーの種類** = **パケットトンネル**
3. iOS用のアプリ属性デバイスポリシーを追加します。**アプリごとのVPN識別子**には、**iOS_VPN**を選択します。

> デバイスポリシー構成画面(/en-us/xenmobile/server/media/vpn-policy-ios.png)

- **接続名:** 接続の名前を入力します。
- **接続の種類:** リストから、この接続に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:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。
  - **PPTP:** ポイントツーポイントトンネリング。
  - **IPSec:** 会社のVPN接続。
  - **Cisco Legacy AnyConnect:** この接続の種類では、ユーザーデバイスにCisco Legacy AnyConnect VPNクライアントがインストールされている必要があります。シスコは、現在非推奨となっているVPNフレームワークに基づいていたCisco Legacy AnyConnectクライアントを段階的に廃止しています。詳細については、サポート記事`<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**として**Custom 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:** アリバネットワークス 仮想インターネットアクセス クライアント。
  - **IKEv2 (iOSのみ):** iOSのみのInternet Key Exchangeバージョン2。
  - **AlwaysOn IKEv2:** IKEv2を使用した常時接続アクセス。
  - **AlwaysOn IKEv2デュアル構成:** IKEv2デュアル構成を使用した常時接続アクセス。
  - **Citrix SSO:** iOS 12以降向けのCitrix SSOクライアント。
  - **Custom SSL:** カスタムSecure Socket Layer。この接続タイプは、バンドルIDが**com.cisco.anyconnect**であるCisco AnyConnectクライアントに必要です。**接続名**として**Cisco AnyConnect**を指定します。VPNポリシーを展開し、iOSデバイス向けにネットワークアクセスコントロール (NAC) フィルターを有効にすることもできます。このフィルターは、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接続をブロックします。この構成には、以下のiOSセクションで説明されているiOS VPNポリシーの特定の構成が必要です。NACフィルターを有効にするために必要なその他の設定については、「ネットワークアクセスコントロール」を参照してください。

以下のセクションでは、上記の各接続タイプの構成オプションを一覧表示します。

iOS向けL2TP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:** オプションの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**のいずれかを選択します。
- **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:** すべてのトラフィックをVPN経由で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:** オプションの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**のいずれかを選択します。
- **暗号化レベル:** リスト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用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:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**共有シークレット**または**証明書**のいずれかを選択します。デフォルトは**共有シークレット**です。
- **共有シークレット**を有効にする場合、これらの設定を構成します。
  - **グループ名:** オプションのグループ名を入力します。
  - **共有シークレット:** オプションの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、サーバーが最初にクライアントに対して認証を行い、次にクライアントがサーバーに対して認証を行います。デフォルトは**オフ**です。

- **パスワードの入力を求める:** ユーザーがネットワークに接続するとき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**」を有効にする場合、これらの設定を構成します。
  - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
  - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を要求するかどうかを選択します。デフォルトは**オフ**です。
  - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。「**VPNオンデマンドを有効にする**」が**オン**の場合の設定の構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** 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。
- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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接続を自動的にトリガー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。

iOS向けCiscoレガシーAnyConnectプロトコルの構成

Ciscoレガシー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。

- **プロバイダーバンドル識別子:** レガシー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:** オプションのユーザーアカウントを入力します。
- **グループ:** オプションのグループ名を入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - 「**証明書**」を有効にする場合は、次の設定を構成します。
    - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。

    - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときに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。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。「**VPNオンデマンドを有効にする**」が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。

    - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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接続を自動的にトリガー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:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次の操作を行います。

        - **ドメイン:** 追加するドメインを入力します。
        - ドメインを保存するには**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。

iOS向けJuniper SSLプロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **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:** オプションのユーザーアカウントを入力します。
- **レルム:** オプションのレルム名を入力します。
- **役割:** オプションの役割名を入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。

    - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
    - **証明書**を有効にする場合は、次の設定を構成します。

- **ID資格情報:** リストから、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。
- **接続時にPINを要求:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
- **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときに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。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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。
  - **プロバイダータイプ:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

iOS向けF5 SSLプロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じタイプの複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **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:** オプションのユーザーアカウントを入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。
    - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。

    - **接続時にPINを要求する:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときに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。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。

    - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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かどうかを選択します。
    - **プロバイダーの種類:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次の操作を行います。

        - **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**をクリックしてドメインを保存しないようにします。

iOS向けSonicWALLプロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとのVPNプロファイルに、同じ種類の複数のVPNプロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **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:** オプションの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:** オプションの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:** この接続の認証の種類として、リストから**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。

    - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
    - **証明書**を有効にする場合は、次の設定を構成します。

- **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
- **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときに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。
- **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「iOS向けVPNオンデマンド設定の構成」を参照してください。

- **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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かどうかを選択します。
  - **プロバイダーの種類:** アプリごとのVPNが**アプリプロキシ**として提供されるか、**パケットトンネル**として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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次を実行します。
    - **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**」をクリックしてドメインを保存しないようにします。

iOS 用 Ariba VIA プロトコルの構成

- **プロバイダーバンドル識別子:** アプリごとの VPN プロファイルに、同じ種類の複数の VPN プロバイダーを持つアプリのバンドル識別子がある場合は、ここで使用するプロバイダーを指定します。
- **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:** オプションのユーザーアカウントを入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから「**パスワード**」または「**証明書**」を選択します。デフォルトは「**パスワード**」です。
  - 「**パスワード**」を有効にする場合は、「**認証パスワード**」フィールドにオプションの認証パスワードを入力します。
  - 「**証明書**」を有効にする場合は、次の設定を構成します。

- **ID 資格情報:** リストから使用する ID 資格情報を選択します。デフォルトは「**なし**」です。
- **接続時に PIN の入力を求める:** ユーザーがネットワークに接続するときに 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。
- **VPN オンデマンドを有効にする:** ユーザーがネットワークに接続したときに 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。「**VPN オンデマンドを有効にする**」が「**オン**」の場合の設定の構成については、「iOS 用 VPN オンデマンド設定の構成」を参照してください。

- **アプリごとの VPN を有効にする:** 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する場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとの VPN サービスにリンクされた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:** 含めるアプリごとの VPN 接続をトリガーできる各 Safari ドメインについて、「**追加**」をクリックして次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

iOS 用 IKEv2 プロトコルの構成

このセクションには、IKEv2、AlwaysOn IKEv2、およびAlwaysOn IKEv2 Dual Configurationプロトコルで使用される設定が含まれています。AlwaysOn IKEv2 Dual Configurationプロトコルの場合、これらの設定はすべて、セルラーネットワークとWi-Fiネットワークの両方に対して構成します。

- **ユーザーによる自動接続の無効化を許可する:** AlwaysOnプロトコル用。ユーザーが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。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。このフィールドは必須です。
- **デバイス認証:** この接続の認証タイプとして、**共有シークレット**、**証明書**、または**デバイス識別子に基づくデバイス証明書**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**を選択した場合は、オプションの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、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。
- **デバイス識別子に基づくデバイス証明書**を選択した場合は、使用する**デバイスIDタイプ**を選択します。デフォルトは**IMEI**です。このオプションを使用するには、REST APIを使用して証明書を一括インポートします。「REST API を使用して iOS デバイスに証明書を一括アップロードする」を参照してください。**Always On IKEv2**を選択した場合にのみ利用可能です。

- **拡張認証を有効にする:** 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。
- **デッドピア検出間隔:** ピアデバイスが到達可能であることを確認するために、ピアデバイスに連絡する頻度を選択します。デフォルトは**なし**です。オプションは次のとおりです。
  - **なし:** デッドピア検出を無効にします。
  - **低:** 30分ごとにピアに連絡します。
  - **中:** ピアに10分ごとに接続します。
  - **高:** ピアに1分ごとに接続します。
- **モビリティとマルチホーミングを無効にする:** 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を使用する:** 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にする:** リダイレクトを無効にするかどうかを選択します。
- **デバイスがスリープ状態のときにNATキープアライブを有効にする:** AlwaysOnプロトコル用です。キープアライブパケットは、IKEv2接続のNATマッピングを維持します。デバイスが起動しているとき、チップはこれらのパケットを定期的に送信します。この設定がオンの場合、デバイスがスリープ状態であっても、チップはキープアライブパケットを送信します。デフォルトの間隔は、Wi-Fi経由で20秒、セルラー経由で110秒です。NATキープアライブ間隔パラメーターを使用して、間隔を変更できます。
- **NATキープアライブ間隔（秒）:** デフォルトは20秒です。
- **Perfect Forward Secrecyを有効にする:** 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IPアドレス:** オプション。DNSサーバーIPアドレス文字列のリストです。これらのIPアドレスには、IPv4アドレスとIPv6アドレスが混在している場合があります。アドレスを入力するには、**追加**をクリックします。
- **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。シングルラベルホスト名を完全に修飾するために使用されるドメイン文字列のリストです。

- **補足一致ドメインをリゾルバーのリストに追加する:** オプション。補足一致ドメインリストをリゾルバーの検索ドメインリスト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。
- **補足一致ドメイン:** オプション。DNSサーバーアドレスのDNSリゾルバー設定を使用するDNSクエリを決定するために使用されるドメイン文字列のリストです。このキーは、特定のドメイン内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スプリットDNS構成を作成します。このリストのドメインのいずれかにないホストは、システムのデフォルトリゾルバーを使用して解決されます。

このパラメーターが空の文字列の場合、その文字列がデフォルトドメインになります。これにより、スプリットトンネル構成は、プライマリDNSサーバーの前にすべてのDNSクエリをVPN DNSサーバーに転送できます。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、リストされているDNSサーバーがデフォルトのリゾルバーになります。その場合、補足一致ドメインリストは無視されます。

- **IKE SAパラメーターと子SAパラメーター。**各セキュリティアソシエーション（SA）パラメーターオプションについて、これらの設定を構成します。
  - **暗号化アルゴリズム:** リストから、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:** リストから、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:** リストから、Diffie Hellmanグループ番号を選択します。デフォルトは **2** です。
  - **IKEライフタイム (分):** SAライフタイム (再キー間隔) を表す10から1440までの整数を入力します。デフォルトは **1440** 分です。
- **サービス例外:** AlwaysOnプロトコル用。サービス例外は、AlwaysOn VPNの対象外となるシステムサービスです。これらのサービス例外設定を構成します。
  - **ボイスメール:** リストから、ボイスメール例外の処理方法を選択します。デフォルトは **トンネル経由でトラフィックを許可** です。
  - **AirPrint:** リストから、AirPrint例外の処理方法を選択します。デフォルトは **トンネル経由で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トンネル外のパブリックホットスポットに接続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。

- **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トンネル外のすべてのホットスポットネットワーク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識別子:** ユーザーがアクセスを許可されている各ホットスポットネットワークアプリのバンドル識別子について、**追加** をクリックし、ホットスポットネットワークアプリの **バンドル識別子** を入力します。**保存** をクリックしてアプリのバンドル識別子を保存します。

- **アプリごとのVPN**。IKEv2接続タイプに対してこれらの設定を構成します。
  - **アプリごとのVPNを有効にする:** 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。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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:** VPN接続がプロキシサーバー経由でルーティングされる方法を選択します。デフォルトは **なし** です。

iOS 用 Citrix SSO プロトコルの構成

Citrix SSO クライアントは、Apple Store の `<https://apps.apple.com/us/app/citrix-sso/id1333396910>` で入手できます。

- **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:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして **Password** または **Certificate** を選択します。デフォルトは **Password** です。
  - **Password** を有効にする場合は、**Auth password** フィールドにオプションの認証パスワードを入力します。
  - **Certificate** を有効にする場合は、次の設定を構成します。
    - **ID 資格情報:** リストから、使用する ID 資格情報を選択します。デフォルトは **None** です。
    - **接続時に PIN を要求:** ユーザーがネットワークに接続するときに PIN を要求するかどうかを選択します。デフォルトは **OFF** です。

    - **VPN オンデマンドを有効にする:** ユーザーがネットワークに接続したときに VPN 接続をトリガーするかどうかを選択します。デフォルトは **OFF** です。**VPN オンデマンドを有効にする** が **On** の場合の設定については、「iOS 用 VPN オンデマンド設定を構成する」を参照してください。

- **アプリごとの VPN を有効にする:** 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 **Off** です。このオプションを ON に設定する場合は、次の設定を構成します。

    - **オンデマンド一致アプリを有効にする:** アプリごとの VPN サービスにリンクされた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かどうかを選択します。
    - **プロバイダータイプ:** アプリごとの VPN が **App proxy** として提供されるか、**Packet tunnel** として提供されるかを選択します。デフォルトは **App proxy** です。
    - **プロバイダータイプ: Packet tunnel** に設定します。
    - **Safari ドメイン:** 含めるアプリごとの VPN 接続をトリガーできる各 Safari ドメインについて、**追加** をクリックして以下を実行します。

        - **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**をクリックしてドメインを保存しないようにします。

- **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。利用可能なパラメーターは次のとおりです。

    - **disableL3：** システムレベルのVPNを無効にします。アプリごとのVPNのみを許可します。**値**は不要です。
    - **useragent：** このデバイスポリシーを、VPNプラグインクライアントを対象とするCitrix Gatewayポリシーに関連付けます。プラグインによって開始された要求の場合、このキーの**値**は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

Cisco Legacy 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プロトコルでVPNデバイスポリシーを構成します。ポリシーをiOSデバイスに展開します。
2. `<https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>`からCisco AnyConnectクライアントをアップロードし、XenMobileにアプリを追加し、その後、アプリをiOSデバイスに展開します。

3. 古いVPNデバイスポリシーをiOSデバイスから削除します。

設定：

- **カスタムSSL識別子（逆引きDNS形式）：** バンドル識別子に設定します。Cisco AnyConnectクライアントの場合は、**com.cisco.anyconnect**を使用します。
- **プロバイダーバンドル識別子： カスタムSSL識別子**で指定されたアプリに、同じタイプ（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ある場合は、このバンドル識別子を指定します。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：** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**Password**または**Certificate**を選択します。デフォルトは**Password**です。
  - **Password**を有効にする場合は、**Auth password**フィールドにオプションの認証パスワードを入力します。
  - **Certificate**を有効にする場合は、これらの設定を構成します。
    - **識別情報資格情報:** リストから使用する識別情報資格情報を選択します。デフォルトは**None**です。
    - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときにPINの入力を求めるかどうかを選択します。デフォルトは**OFF**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**OFF**です。**VPNオンデマンドを有効にする**が**On**の場合の設定の構成については、「iOS向けVPNオンデマンド設定の構成」を参照してください。
- **アプリごとのVPNを有効にする:** 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**Off**です。このオプションをONに設定する場合は、次の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** 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は、プロバイダーがVPNサービスであるかプロキシサービスであるかを示します。VPNサービスの場合は、**Packet tunnel**を選択します。プロキシサービスの場合は、**App proxy**を選択します。Cisco AnyConnectクライアントの場合は、**Packet tunnel**を選択します。

    - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**Add**をクリックして、次の操作を行います。
        - **ドメイン:** 追加するドメインを入力します。
        - ドメインを保存するには**Save**をクリックし、ドメインを保存しない場合は**Cancel**をクリックします。

- **カスタムXML:** 追加するカスタムXMLパラメーターごとに、**Add**をクリックして、次の操作を行います。
    - **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**に関連付けられた値を入力します。
    - 「**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**」をクリックしてパラメーターを保存しません。

NACをサポートするようにVPNデバイスポリシーを構成する

1. NACフィルターを構成するには、**接続タイプ**として**カスタムSSL**が必要です。
2. **接続名**として**VPN**を指定します。
3. **カスタムSSL識別子**には、「**com.citrix.NetScalerGateway.ios.app**」と入力します。
4. **プロバイダーバンドル識別子**には、「**com.citrix.NetScalerGateway.ios.app.vpnplugin**」と入力します。

ステップ3と4の値は、NACフィルタリングに必要なCitrix SSOのインストールから取得されます。認証パスワードは構成しません。NAC機能の使用について詳しくは、「ネットワークアクセス制御」を参照してください。

iOSのVPNオンデマンドオプションを有効にするように構成する

- **オンデマンドドメイン:** ユーザーが接続したときに実行する各ドメインと関連付けられたアクションについて、「**追加**」をクリックして、次の操作を行います。
- **ドメイン:** 追加するドメインを入力します。
- **アクション:** リストから可能な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。
    - **必要に応じて確立:** ドメイン名解決に失敗した場合、ドメインはVPN接続の試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。

- 「**保存**」をクリックしてドメインを保存するか、「**キャンセル**」をクリックしてドメインを保存しません。

- **オンデマンドルール**
  - **アクション:** リスト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。可能なアクションは次のとおりです。
    - **許可:** トリガーされたときにオンデマンドVPNの接続を許可します。
    - **接続:** 無条件にVPN接続を開始します。
    - **切断:** VPN接続を削除し、ルールが一致する限りオンデマンドで再接続しません。
    - **接続の評価:** 各接続のActionParameters配列を評価します。
    - **無視:** 既存のVPN接続を維持しますが、ルールが一致する限りオンデマンドで再接続しません。
  - **DNSドメイン一致:** デバイスの検索ドメインリストが一致する可能性のあるドメインで、追加したいものごとに、**追加**をクリックして以下を実行します。
    - **DNSドメイン:** ドメイン名を入力します。複数のドメインに一致させるには、ワイルドカード「*」プレフィックスを使用できます。たとえば、*.example.com は mydomain.example.com、yourdomain.example.com、herdomain.example.com に一致します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。
  - **DNSサーバーアドレス一致:** ネットワークの指定されたDNSサーバーのいずれかが一致する可能性のあるIPアドレスで、追加したいものごとに、**追加**をクリックして以下を実行します。
    - **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。DNSサーバーに一致させるには、ワイルドカード「*」サフィックスを使用できます。たとえば、17.* はクラスAサブネット内の任意のDNSサーバーに一致します。
    - DNSサーバーアドレスを保存するには**保存**をクリックし、DNSサーバーアドレスを保存しない場合は**キャンセル**をクリックします。
  - **インターフェースタイプ一致:** リストから、使用中のプライマリネットワークインターフェースハードウェアのタイプを選択します。デフォルトは **Unspecified** です。可能な値は次のとおりです。

- **指定なし:** 任意のネットワークインターフェースハードウェアに一致します。このオプションがデフォルトです。
- **Ethernet:** イーサネットネットワークインターフェースハードウェアのみに一致します。
- **WiFi:** Wi-Fiネットワークインターフェースハードウェアのみに一致します。
- **Cellular:** セルラーネットワークインターフェースハードウェアのみに一致します。

◦ **SSIDMatch:** 追加する現在のネットワークと一致させる各SSIDについて、**追加**をクリックし、以下を実行します。

- **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、一致は失敗します。任意のSSIDに一致させるには、このリストを空のままにします。
- SSIDを保存するには**保存**をクリックし、SSIDを保存しない場合は**キャンセル**をクリックします。

◦ **URLStringProbe:** フェッチするURLを入力します。このURLがリダイレクトなしで正常にフェッチされた場合、このルールは一致します。

◦ **ActionParameters : Domains:** 追加するEvaluateConnectionがチェックする各ドメインについて、**追加**をクリックし、以下を実行します。

- **Domain:** 追加するドメインを入力します。
- ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

◦ **ActionParameters : DomainAction:** リストから、指定された**ActionParameters : Domains**ドメインの**VPN動作**を選択します。デフォルトは**ConnectIfNeeded**です。可能なアクションは次のとおりです。

- **ConnectIfNeeded:** ドメイン名解決が失敗した場合、ドメインはVPN接続試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
- **NeverConnect:** ドメインはVPN接続をトリガーしません。

◦ **Action Parameters: RequiredDNSServers:** 指定されたドメインの解決に使用する各DNSサーバーIPアドレスについて、**追加**をクリックし、以下を実行します。

- **DNS Server: ActionParameters** : **DomainAction** = **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

トワーク構成の一部である必要はありません。DNSサーバーに到達できない場合、応答として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サーバーのいずれかである必要があります。

- DNSサーバーを保存するには**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。

- **ActionParameters : RequiredURLStringProbe:** オプションで、GETリクエストを使用してプローブするHTTPまたはHTTPS（推奨）URLを入力します。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は、VPN接続が確立されます。**ActionParameters** : **DomainAction** = **ConnectIfNeeded**の場合にのみ有効です。
- **OnDemandRules : XML content:** オンデマンドルールでXML構成を入力またはコピー＆ペーストします。

  - **Check Dictionary**をクリックしてXMLコードを検証します。XMLが有効な場合、**XML content**テキストボックスの下に緑色のテキストで「Valid XML」と表示されます。有効でない場合は、エラーを説明するオレンジ色のテキストでエラーメッセージが表示されます。

- **プロキシ**

  - **プロキシ構成:** リストから、VPN接続がプロキシサーバーを介してルーティングされる方法を選択します。デフォルトは**なし**です。

    - **手動**を有効にする場合は、以下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:** オプションのプロキシサーバーユーザー名を入力します。
      - **パスワード:** オプションのプロキシサーバーパスワードを入力します。

    - **自動**を構成する場合は、こ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**の下にある**ポリシーの削除**の横で、**日付を選択**または**削除までの期間（時間）**のいずれかを選択します。
- 「**日付を選択**」を選択した場合、カレンダーをクリックして削除する特定の日付を選択します。
- 「**ユーザーによるポリシーの削除を許可**」リストで、「**常に許可**」、「**パスワードが必要**」、または「**許可しない**」を選択します。
- 「**パスワードが必要**」を選択した場合、「**削除パスワード**」の横に必要なパスワードを入力します。

アプリごとのVPNを構成する

iOS用のアプリごとのVPNオプションは、以下の接続タイプで利用できます: Cisco Legacy AnyConnect、Juniper SSL、F5 SSL、SonicWALL Mobile Connect、Ariba VIA、Citrix VPN、Citrix SSO、およびCustom SSL。

アプリごとのVPNを構成するには：

1. 「**構成 > デバイスポリシー**」で、VPNポリシーを作成します。例：

   デバイスポリシー構成画面(/en-us/xenmobile/server/media/configure-device-policies-vpn-per-app-ios-example.png)

   デバイスポリシー構成画面(/en-us/xenmobile/server/media/configure-device-policies-vpn-per-app-ios-example2.png)

2. 「**構成 > デバイスポリシー**」で、アプリをアプリごとのVPNポリシーに関連付けるためのアプリ属性ポリシーを作成します。「**アプリごとのVPN識別子**」には、手順1で作成したVPNポリシーの名前を選択します。「**管理対象アプリバンドルID**」には、アプリリストから選択するか、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、アプリリストにアプリが表示されます。）

   デバイスポリシー構成画面(/en-us/xenmobile/server/media/configure-device-policies-app-attributes-per-app.png)

- **ポリシー設定**
  - **ポリシーの削除：** ポリシーの削除をスケジュールする方法を選択します。利用可能なオプションは「**日付を選択**」と「**削除までの期間（時間）**」です。
    - **日付を選択：** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）：** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

macOS設定

デバイスポリシー構成画面(/en-us/xenmobile/server/media/configure-device-policies-vpn-macos-example.png)

- **接続名:** 接続の名前を入力します。
- **接続タイプ:** リストから、この接続に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:** 事前共有キー認証を使用するレイヤー2トンネリングプロトコル。
  - **PPTP:** ポイントツーポイントトンネリング。
  - **IPSec:** 会社の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:** アリバ・ネットワークス バーチャル・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Secure Socket Layer。

以下のセクションでは、上記の各接続タイプの構成オプションを一覧表示します。

macOS 用 L2TP プロトコルを構成する

- **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:** オプションの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、**または**CryptoCard認証**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 用 PPTP プロトコルを構成する

- **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:** オプションの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、またはCryptoCard認証**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:** 目的の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 用 IPsec プロトコルを構成する

- **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:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして **共有シークレット** または **証明書** のいずれかを選択します。デフォルトは **共有シークレット** です。
  - **共有シークレット** 認証を有効にする場合は、次の設定を構成します。
    - **グループ名:** オプションのグループ名を入力します。
    - **共有シークレット:** オプションの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、サーバーが最初にクライアントに対して自身を認証し、次にクライアントがサーバーに対して自身を認証します。デフォルトは **オフ** です。
    - **パスワードのプロンプト:** ユーザーがネットワークに接続するとき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** 認証を有効にする場合は、次の設定を構成します。
    - **ID 資格情報:** リストから、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。
    - **接続時に PIN のプロンプト:** ユーザーがネットワークに接続するときに PIN の入力を要求するかどうかを選択します。デフォルトは **オフ** です。
    - **VPN オンデマンドを有効にする:** ユーザーがネットワークに接続したときに VPN 接続をトリガーするかどうかを選択します。デフォルトは **オフ** です。**VPN オンデマンドを有効にする** が **オン** の場合の設定の構成については、「VPN オンデマンドオプションの有効化を構成する」を参照してください。

macOS 用 Cisco AnyConnect プロトコルを構成する

- **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:** オプションのユーザーアカウントを入力します。
- **グループ:** オプションのグループ名を入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。
    - **ID資格情報:** リストから、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。
    - **接続時にPINを要求:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「VPNオンデマンドオプションの有効化を構成する」を参照してください。
  - **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。
    - **オンデマンド一致アプリを有効にする:** 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:** 含めるアプリごとのVPN接続をトリガーできるSafariドメインごとに、**追加**をクリックして次の操作を行います。
      - **ドメイン:** 追加するドメインを入力します。
      - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。

macOS 用のJuniper SSLプロトコルを構成する

- **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:** オプションのユーザーアカウントを入力します。
- **レルム:** オプションのレルム名を入力します。

- **ロール:** オプションのロール名を入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、以下の設定を構成します。
    - **ID資格情報:** 使用するID資格情報をリストから選択します。デフォルトは**なし**です。
    - **接続時にPINを要求:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンド設定の有効化を構成する」を参照してください。
- **アプリごとのVPNを有効にする:** 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する場合は、以下の設定を構成します。
  - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**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。

macOS用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:** オプションのユーザーアカウントを入力します。
- **接続の認証の種類:** この接続の認証の種類として、リストから**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、次の設定を構成します。

    - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは**なし**です。
    - **接続時にPINの入力を求める:** ユーザーがネットワークに接続するときに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。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定の構成については、「VPNオンデマンド設定の有効化を構成する」を参照してください。

- **アプリごとのVPNを有効にする:** 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する場合は、次の設定を構成します。
    - **オンデマンド一致アプリを有効にする:** 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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして次の操作を行います。
        - **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**をクリックしてドメインを保存しないようにします。

macOS 用の SonicWALL Mobile Connect プロトコルを構成する

- **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:** オプションの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:** オプションのログオングループまたはドメインを入力します。
- **接続の認証タイプ:** この接続の認証タイプとして、リストから **Password** または **Certificate** を選択します。デフォルトは **Password** です。
    - **Password** を有効にする場合は、**Auth password** フィールドにオプションの認証パスワードを入力します。
    - **Certificate** を有効にする場合は、以下の設定を構成します。
        - **ID資格情報:** リストから使用するID資格情報を選択します。デフォルトは **None** です。
        - **接続時にPINを要求:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは **Off** です。

    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは **Off** です。**VPNオンデマンドを有効にする** が **On** の場合の設定については、「VPNオンデマンドを有効にする設定を構成する」を参照してください。

- **アプリごとのVPNを有効にする:** 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 **Off** です。このオプションを有効にする場合は、以下の設定を構成します。
    - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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 **Off** です。
    - **Safariドメイン:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**Add** をクリックして以下を実行します。
        - **ドメイン:** 追加するドメインを入力します。
        - ドメインを保存するには **Save** をクリックし、保存しない場合は **Cancel** をクリックします。

macOS 用の Ariba VIA プロトコルを構成する

- **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:** オプションのユーザーアカウントを入力します。
- **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**のいずれかを選択します。デフォルトは**パスワード**です。
    - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
    - **証明書**を有効にする場合は、以下の設定を構成します。
        - **ID資格情報:** リストから、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。
        - **接続時にPINを要求:** ユーザーがネットワークに接続するときにPINを要求するかどうかを選択します。デフォルトは**オフ**です。
        - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときに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。**VPNオンデマンドを有効にする**が**オン**の場合の設定構成については、「VPNオンデマンド設定の有効化を構成する」を参照してください。
- **アプリごとのVPNを有効にする:** 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する場合は、以下の設定を構成します。

- **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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:** 含めるアプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
  - **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**をクリックしてドメインを保存しないようにします。

macOS用のカスタムSSLプロトコルを構成する

- **カスタムSSL識別子 (逆引き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:** オプションのユーザーアカウントを入力します。
  - **接続の認証タイプ:** リストから、この接続の認証タイプとして**パスワード**または**証明書**を選択します。デフォルトは**パスワード**です。
  - **パスワード**を有効にする場合は、**認証パスワード**フィールドにオプションの認証パスワードを入力します。
  - **証明書**を有効にする場合は、以下の設定を構成します。
    - **ID資格情報:** リストから、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。
    - **接続時にPINを要求:** ユーザーがネットワークに接続する際にPINを要求するかどうかを選択します。デフォルトは**オフ**です。
    - **VPNオンデマンドを有効にする:** ユーザーがネットワークに接続したときにVPN接続をトリガーするかどうかを選択します。デフォルトは**オフ**です。**VPNオンデマンドを有効にする**が**オン**の場合の設定については、「VPNオンデマンドを有効にする設定を構成する」を参照してください。
  - **アプリごとの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する場合は、以下の設定を構成します。
    - **オンデマンド一致アプリを有効にする:** アプリごとのVPNサービスにリンクされた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:** 含めたい、アプリごとのVPN接続をトリガーできる各Safariドメインについて、**追加**をクリックして以下を実行します。
        - **ドメイン:** 追加するドメインを入力します。
        - ドメインを保存するには**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。

- **カスタムXML:** 追加したい各カスタムXMLパラメーターについて、**追加**をクリックして以下を実行します。
    - **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**に関連付けられた値を入力します。
    - 「**保存**」をクリックしてドメインを保存するか、「**キャンセル**」をクリックしてドメインを保存しないようにします。

VPNオンデマンドオプションの有効化を構成する

- **オンデマンドドメイン:** 追加する各ドメインと、ユーザーがそれらに接続したときに実行される関連アクションについて、「**追加**」をクリックして、次の操作を行います。
    - **ドメイン:** 追加するドメインを入力します。
    - **アクション:** リストから可能な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。
        - **決して確立しない:** ドメインはVPN接続をトリガーしません。
        - **必要に応じて確立:** ドメイン名解決が失敗した場合、ドメインはVPN接続の試行をトリガーします。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
    - 「**保存**」をクリックしてドメインを保存するか、「**キャンセル**」をクリックしてドメインを保存しないようにします。

- **オンデマンドルール**
    - **アクション:** リスト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。可能なアクションは次のとおりです。
        - **許可:** トリガーされたときにVPNオンデマンドが接続することを許可します。
        - **接続:** 無条件にVPN接続を開始します。
        - **切断:** VPN接続を削除し、ルールが一致する限りオンデマンドで再接続しません。

- **EvaluateConnection:** 各接続の**ActionParameters**配列を評価します。
- **無視:** 既存のVPN接続を維持しますが、ルールが一致する限り、オンデマンドで再接続しません。

- **DNSDomainMatch:** ユーザーデバイスの検索ドメインリストが一致する可能性のあるドメインで、追加したいものごとに、**追加**をクリックして、以下を実行します。
  - **DNSドメイン:** ドメイン名を入力します。複数のドメインに一致させるには、ワイルドカード「*」プレフィックスを使用できます。たとえば、*.example.com は mydomain.example.com、yourdomain.example.com、および herdomain.example.com に一致します。
  - ドメインを保存するには**保存**をクリックするか、ドメインを保存しない場合は**キャンセル**をクリックします。
- **DNSServerAddressMatch:** ネットワークの指定されたDNSサーバーのいずれかが一致する可能性のあるIPアドレスで、追加したいものごとに、**追加**をクリックして、以下を実行します。
  - **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。DNSサーバーに一致させるには、ワイルドカード「*」サフィックスを使用できます。たとえば、17.* はクラスAサブネット内の任意のDNSサーバーに一致します。
  - DNSサーバーアドレスを保存するには**保存**をクリックするか、DNSサーバーアドレスを保存しない場合は**キャンセル**をクリックします。
- **InterfaceTypeMatch:** リストで、使用中のプライマリネットワークインターフェースハードウェアの種類をクリックします。デフォルトは**指定なし**です。可能な値は次のとおりです。
  - **指定なし:** 任意のネットワークインターフェースハードウェアに一致します。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ースハードウェアのみに一致します。
  - **Wi-Fi:** Wi-Fiネットワークインターフェースハードウェアのみに一致します。
  - **セルラー:** セルラーネットワークインターフェースハードウェアのみに一致します。
- **SSIDMatch:** 現在のネットワークと一致させたいSSIDごとに、**追加**をクリックして、以下を実行します。

- **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、一致は失敗します。任意のSSIDに一致させるには、このリストを空のままにします。
- SSIDを保存するには**保存**をクリックするか、SSIDを保存しない場合は**キャンセル**をクリックします。

- **URLStringProbe:** 取得するURLを入力します。このURLがリダイレクトなしで正常に取得された場合、このルールが一致します。
- **ActionParameters : Domains:** EvaluateConnectionがチェックするドメインのうち、追加したいドメインごとに**追加**をクリックして、以下を実行します。
  - **ドメイン:** 追加するドメインを入力します。
  - ドメインを保存するには**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。
- **ActionParameters : DomainAction:** リストから、指定された**ActionParameters : Domains**ドメインの**VPN動作**を選択します。デフォルトは**ConnectIfNeeded**です。可能なアクションは次のとおりです。
  - **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。失敗は、DNSサーバーがドメインを解決できない場合、別のサーバーにリダイレクトされる場合、またはタイムアウトした場合に発生します。
  - **NeverConnect:** ドメインはVPN接続をトリガーしません。
- **Action Parameters: RequiredDNSServers:** 指定されたドメインの解決に使用するDNSサーバーIPアドレスごとに**追加**をクリックして、以下を実行します。
  - **DNSサーバー: ActionParameters** : **DomainAction** = **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の一部である必要はありません。DNSサーバーに到達できない場合、応答として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サーバーのいずれかである必要があります。
  - DNSサーバーを保存するには**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。
- **ActionParameters : RequiredURLStringProbe:** オプションで、GETリクエストを使用してプローブするHTTPまたはHTTPS（推奨）URLを入力します。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、VPN接続

が確立されます。**ActionParameters** : **DomainAction** = **ConnectIfNeeded**の場合にのみ有効です。

- **OnDemandRules : XML content:** XMLオンデマンドルールを入力またはコピー＆ペーストします。
  - XMLコードを検証するには**辞書をチェック**をクリックします。XMLが有効な場合、**XML content**テキストボックスの下に緑色のテキストで「Valid XML」と表示されます。有効でない場合、エラーを説明するオレンジ色のテキストでエラーメッセージが表示されます。

- **プロキシ**
  - **プロキシ構成:** リストから、VPN接続がプロキシサーバーを介してルーティングされる方法を選択します。デフォルトは**なし**です。
    - 「**手動**」を有効にする場合は、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:** オプションのプロキシサーバーユーザー名を入力します。
      - **パスワード:** オプションのプロキシサーバーパスワードを入力します。
    - 「**自動**」を構成する場合は、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

デバイスポリシー構成画面(/en-us/xenmobile/server/media/configure-device-policies-vpn-android-example.png)

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:** リストから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:** VPNが信頼されたネットワークと信頼されていないネットワークにどのように反応するかを設定するには、このオプションを有効または無効にします。有効にした場合は、以下の設定を構成します。
    - **信頼されたネットワークポリシー:** リスト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。選択可能なオプションは次のとおりです。
      - **切断:** クライアントは信頼されたネットワークでVPN接続を終了します。この設定がデフォルトです。
      - **接続:** クライアントは信頼されたネットワークでVPN接続を開始します。
      - **何もしない:** クライアントは何もアクションを実行しません。
      - **一時停止:** ユーザーが信頼されたネットワーク外でVPNセッションを確立し、その後信頼されたネットワークとして構成されたネットワークに入ると、VPNセッションは一時停止されます。ユーザーが再び信頼されたネットワークを離れると、セッションは再開されます。この設定により、信頼された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必要がなくなります。
    - **信頼されていないネットワークポリシー:** リスト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。選択可能なオプションは次のとおりです。
      - **接続:** クライアントは信頼されていないネットワークでVPN接続を開始します。
      - **何もしない:** クライアントは信頼されていないネットワークでVPN接続を開始します。このオプションは常時接続VPNを無効にします。
  - **信頼されたドメイン:** クライアントが信頼されたネットワークにいるときにネットワークインターフェイスが持つ各ドメインサフィックスについて、**追加**をクリックして以下を実行します。
    - **ドメイン:** 追加するドメインを入力します。
    - ドメインを保存するには**保存**をクリックし、ドメインを保存しない場合は**キャンセル**をクリックします。
  - **信頼されたサーバー:** クライアントが信頼されたネットワークにいるときにネットワークインターフェイスが持つ各サーバーアドレスについて、**追加**をクリックして以下を実行します。

- **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**」をクリックしてサーバーを保存しないようにします。

Android 用 Citrix SSO プロトコルの構成

- **接続名:** 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:** Citrix Gateway の FQDN または IP アドレスを入力します。
- **接続の認証タイプ:** 認証タイプを選択し、そのタイプに表示されるフィールドに入力します。
  - **ユーザー名**と**パスワード: 認証タイプ**が**パスワード**または**パスワードと証明書**の場合、VPN 資格情報を入力します。オプションです。VPN 資格情報を提供しない場合、Citrix VPN アプリはユーザー名とパスワードの入力を求めます。
  - **ID 資格情報: 認証タイプ**が**証明書**または**パスワードと証明書**の場合に表示されます。リストから ID 資格情報を選択します。
- **アプリごとの VPN を有効にする:** アプリごとの VPN を有効にするかどうかを選択します。アプリごとの VPN を有効にしない場合、すべてのトラフィックは Citrix VPN トンネルを通過します。アプリごとの VPN を有効にする場合は、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、許可されているすべてのアプリがこの VPN を介してトンネル接続します。**ブラックリスト**の場合、ブロックリストにあるアプリを除くすべてのアプリがこの VPN を介してトンネル接続します。

    > **注:**
    >
    > XenMobile® Server コンソールには、「ブラックリスト」と「ホワイトリスト」という用語が含まれています。今後のリリースで、これらの用語を「ブロックリスト」と「許可リスト」に変更する予定です。

  - **アプリケーションリスト:** 許可またはブロックするアプリを指定します。「**追加**」をクリックし、アプリパッケージ名をコンマ区切りで入力します。
- **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 は Citrix VPN で次のパラメーターをサポートしています。
  - **DisableUserProfiles:** オプション。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。有効にすると、XenMobile はユーザーが追加した VPN 接続を表示せず、ユー

ザーは接続を追加できません。この設定はグローバルな制限であり、すべての VPN プロファイルに適用されます。

- **userAgent:** 文字列値。各 HTTP リクエストで送信するカスタムユーザーエージェント文字列を指定できます。指定されたユーザーエージェント文字列は、既存の Citrix VPN ユーザーエージェントに追加されます。

NACをサポートするようにVPNを構成する

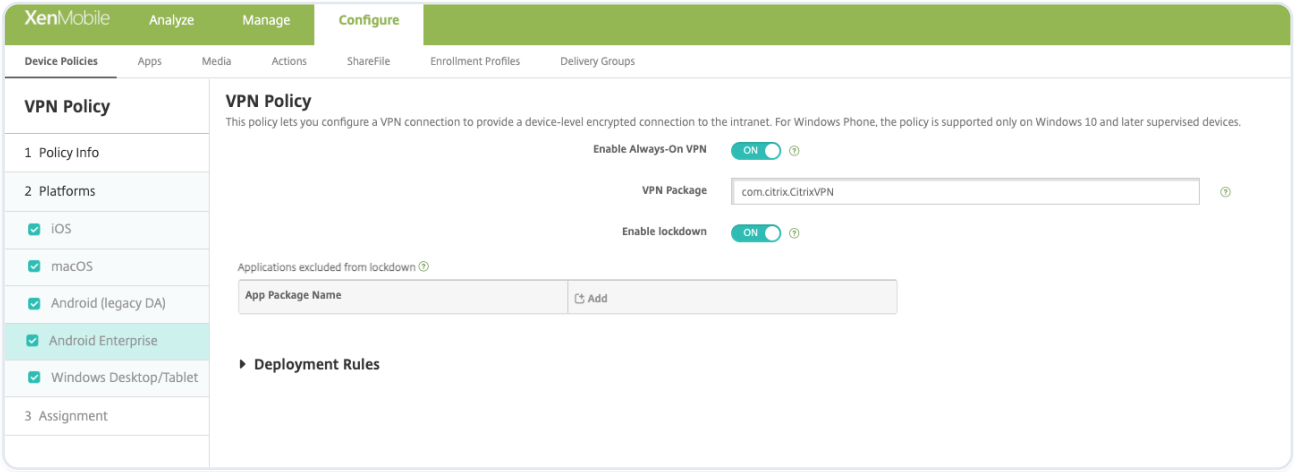
1. NACフィルターを構成するには、**接続の種類**で**カスタムSSL**を使用します。
2. **接続名**に**VPN**を指定します。
3. **カスタムXML**の場合は、**追加**をクリックして、次の操作を行います。

   - **パラメーター名: XenMobileDeviceId**と入力します。このフィールドは、XenMobileへのデバイス登録に基づいてNACチェックに使用するデバイスIDです。XenMobileがデバイスを登録および管理している場合、VPN接続は許可されます。それ以外の場合、VPN確立時に認証が拒否されます。
   - **値:** パラメーター**XenMobileDeviceId**の値である**DeviceID_${device.id}**と入力します。
   - **保存**をクリックしてパラメーターを保存します。

Android Enterprise向けVPNの構成

Android Enterpriseデバイス向けVPNを構成するには、Citrix SSOアプリの管理対象構成デバイスポリシーを作成します。「Android Enterprise向けVPNプロファイルの構成」を参照してください。

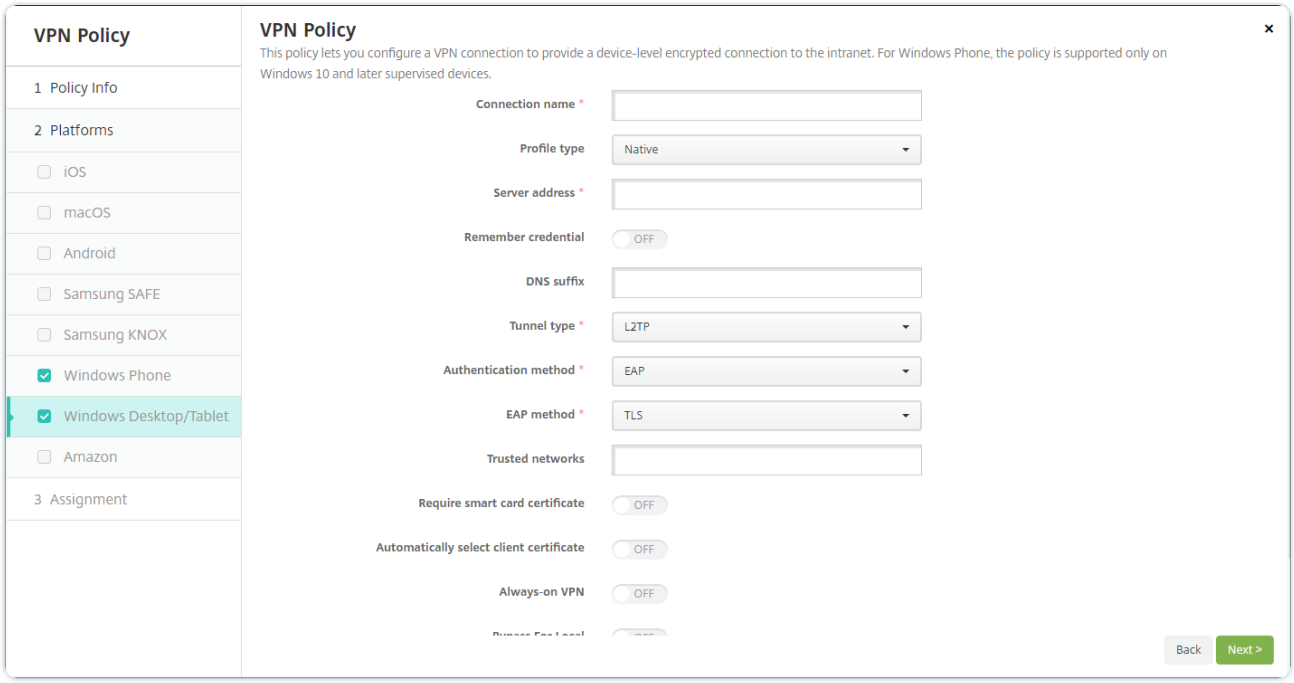
Android Enterpriseの設定



- **常時接続VPNを有効にする:** VPNを常時接続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接続はオンのままになります。

- **VPNパッケージ:** デバイスが使用するVPNアプリのパッケージ名を入力します。
- **ロックダウンを有効にする:** 無効にすると、VPN接続が存在しない場合、どのアプリもネットワークにアクセスできません。有効にすると、VPN接続が存在しない場合でも、以下の設定で構成したアプリはネットワークにアクセスできます。Android 10以降のデバイスで利用可能です。
- **ロックダウンから除外されるアプリケーション: 追加**をクリックして、ロックダウン設定をバイパスするアプリのパッケージ名を入力します。

Windows デスクトップおよびタブレットの設定



- **接続名:** 接続の名前を入力します。このフィールドは必須です。
- **プロファイルの種類:** リストから、**Native** または **Plugin** を選択します。デフォルトは **Native** です。
- **Native プロファイルの種類を構成:** これらの設定は、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 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。
  - **資格情報を記憶:** 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 **Off** です。有効にすると、可能な限り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。
  - **トンネルの種類:** リストから、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。選択可能なオプションは次のとおりです。

    - **L2TP:** 事前共有キー認証を使用したレイヤー2トンネリングプロトコル。
    - **PPTP:** ポイントツーポイントトンネリング。
    - **IKEv2:** インターネットキー交換バージョン2。
  - **認証方法:** リストから、使用する認証方法を選択します。デフォルトは **EAP** です。選択可能なオプションは次のとおりです。
    - **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。このオプションは、トンネルの種類に **IKEv2** を選択した場合は使用できません。
  - **EAPメソッド:** リストから使用するEAPメソッドを選択します。デフォルトは**TLS**です。MSChapV2認証が有効な場合、このフィールドは使用できません。選択可能なオプションは次のとおりです。
    - **TLS:** トランスポート層セキュリティ
    - **PEAP:** 保護された拡張認証プロトコル
  - **信頼されたネットワーク:** VPN接続を必要としないネットワークのリストをコンマで区切って入力します。たとえば、ユーザーが社内ワイヤレスネットワークに接続している場合、保護されたリソースに直接アクセスできます。
  - **スマートカード証明書を要求:** スマートカード証明書を要求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を自動的に選択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**を有効にすると、このオプションは使用できません。
  - **常時接続VPN:** VPNを常時接続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接続は維持されます。
  - **ローカルのバイパス:** ローカルリソースがプロキシサーバーをバイパスできるように、アドレスと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を構成:** これらの設定は、Windowsストアから入手し、ユーザーのデバイスにインストールされた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。
  - **資格情報を記憶:** 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、可能な限り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: 参照**をクリックしてファイルの場所に移動し、使用するカスタムVPNプラグインプロファイルを選択します。形式と詳細については、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:** VPN接続を必要としないネットワークのリストをコンマで区切って入力します。たとえば、ユーザーが社内ワイヤレスネットワークに接続している場合、保護されたリソースに直接アクセスできます。
- **常時接続VPN**：VPNを常時接続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接続は維持されます。
- **ローカルのバイパス**：ローカルリソースがプロキシサーバーをバイパスできるように、アドレスとポート番号を入力します。

壁紙デバイスポリシー

iOSデバイスのロック画面、ホーム画面、またはその両方に壁紙を設定するために、.pngまたは.jpgファイルを追加できます。iOS 7.1.2以降の監視対象デバイスでのみ利用可能です。iPadとiPhoneで異なる壁紙を使用するには、異なる壁紙ポリシーを作成し、適切なユーザーに展開する必要があります。

次の表は、Appleが推奨するiOSデバイスの画像寸法を示しています。

iPhone

デバイス	ピクセル単位の画像寸法
アイフォーン 12 Pro Max	2778 x 1284
iPhone 12 & iPhone 12 Pro	2532 x 1170
アイフォーン 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
アイフォン XS マックス	2688 x 1242

デバイス	ピクセル単位の画像寸法
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
アイフォン SE 第2世代	1334 x 750
アイフォン 7 プラス、8 プラス	2208 x 1242
iPhone 7, 8	1334 x 750
アイフォーン 8 PLus	1334 x 750
iPhone 8	1334 x 750

iPad

デバイス	画像サイズ（ピクセル）
iPad Pro (第1世代、第2世代、第3世代 12.9インチ)	2732 x 2048
iPad Pro 10.5インチ	2224 x 1668
iPad Pro (9.7インチ)	1536 x 2048
iPad Air 2	2048 x 1536

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**に移動します。詳細については、デバイスポリシーを参照してください。

iOS設定

- **適用先:** リストから、**ロック画面、ホーム（アイコンリスト）画面、**または**ロック画面とホーム画面**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**をクリックしてファイルの場所へ移動し、壁紙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

XenMobileでデバイスポリシーを追加して、許可リストとブロックリストに追加する特定のサイトでAppleの自動フィルター機能を使用して、iOSデバイスのWebコンテンツをフィルターできます。このポリシーは、監視モードのiOS 7.0以降のデバイスでのみ利用可能です。iOSデバイスを監視モードにする方法については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」を参照してください。

> **注記:**
>
> - AndroidデバイスはWebコンテンツフィルタリングをサポートしていません。
> - iOSバージョン16.5以降では、Webコンテンツフィルターデバイスポリシーが許可リスト内の`https://localhost`を認識しなくなります。この問題により、一部のアプリが応答しなくなります。また、`http://localhost:`、`http://localhost:*`などのURLの派生を許可リストに追加しても、この問題は解決されません。

> 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**に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **フィルターの種類:** ドロップダウンリストで**組み込み**または**プラグイン**をクリックし、選択したオプションについて以下の手順に従います。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**
  - **自動フィルターを有効にする:** 不適切なコンテンツについてWebサイトを分析するためにAppleの自動フィルター機能を使用するかどうか。デフォルトは**オフ**です。
  - **許可されたURL: 自動フィルターを有効にする**が**オフ**に設定されている場合、このリストは無視されます。**自動フィルターを有効にする**が**オン**に設定されている場合、自動フィルターがアクセスを許可するかどうかにかかわらず、このリストの項目は常にアクセス可能です。許可リストに追加する各URLについて、**追加**をクリックして以下を実行します。
    - 許可するWebサイトのURLを入力します。Webアドレスの前に`http://`または`https://`を追加する必要があります。

    - **保存**をクリックしてWebサイトを許可リストに保存するか、**キャンセル**をクリックして保存しないようにします。
  - **ブラックリストに登録されたURL:** このリストの項目は常にブロックされます。ブロックリストに追加する各URLについて、**追加**をクリックして以下を実行します。
    - 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`http://`または`https://`を追加する必要があります。
    - Webサイトをブロックリストに保存するには、**保存**をクリックするか、保存しない場合は**キャンセル**をクリックします。

      > **注:**
      >
      > XenMobile® Serverコンソールには、「ブラックリスト」と「ホワイトリスト」という用語が含まれています。今後のリリースで、これらの用語を「ブロックリスト」と「許可リスト」に変更する予定です。

- **ブックマークホワイトリスト**
  - **ブックマークホワイトリスト:** 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、その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ストアへのアクセスを有効にするには、XenMobile ServerのURLを**URL**リストに追加します。Webアドレスの前に`http://`または`https://`を追加する必要があります。このフィールドは必須です。
    - **ブックマークフォルダー:** オプションの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サイトのわかりやすいタイトルを入力します。たとえば、URL`https://google.com`には「Google」と入力します。
    - Webサイトを許可リストに保存するには、**保存**をクリックするか、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:** フィルターの一意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:** オプションの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:** サービス用のオプションのユーザー名を入力します。
- **パスワード:** サービス用のオプションのパスワードを入力します。
- **証明書:** ドロップダウンリストから、サービスへのユーザー認証に使用するオプションのID証明書をクリックします。デフォルトは**なし**です。
- **WebKitトラフィックのフィルタリング:** 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のフィルタリング:** 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、次の操作を行います。
    - **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には**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。
- **ポリシー設定**
    - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
        - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
        - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。iOS 6.0以降でのみ利用可能です。

Webクリップデバイスポリシー

ユーザーのデバイス上のアプリと並んで表示されるように、Webサイトへのショートカット（Webクリップ）を配置できます。iOS、iPadOS、macOS、および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タブレットでは、ラベルとURLのみが必要です。iOSおよびiPadOSデバイスの場合、作成したWebクリップを整理するには、ホーム画面レイアウトデバイスポリシーを構成します。iOSでアプリへのアクセスを制限する場合は、Webクリップを許可するように制限デバイスポリシーを構成してください。これらのポリシーの構成に

ついては、「ホーム画面レイアウトデバイスポリシー」および「制限デバイスポリシー」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、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

iOS設定

- **ラベル:** Webクリップとともに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。URLはプロトコルで始まる必要があります（例: `https://server`）。
- **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。このオプションは共有iPadではサポートされていません。
- **更新するアイコン:** をクリックしてファイルの場所へ移動し、Webクリップに使用するアイコンを選択します。
- **プリコンポーズアイコン:** アイコンに効果（角丸、ドロップシャドウ、反射光沢）が適用されているかどうかを選択します。デフォルトは**オフ**で、効果が追加されます。
- **全画面表示:** リンクされたWebページが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。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、 と です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。
  - **プロファイルスコープ:** ポリシーをユーザーに適用するか、システム全体に適用するかを選択します。デフォルト値は**システム**です。iOS 9.3以降でのみ利用可能です。

macOS 設定

- **ラベル:** Webクリップとともに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。URLはプロトコルで始まる必要があります（例: `https://server`）。
- **更新するアイコン:** 参照をクリックしてファイルの場所へ移動し、Webクリップに使用するアイコンを選択します。

Android 設定

- **ルール:** このポリシーがWebクリップを追加するか削除するかを選択します。デフォルトは**追加**です。
- **ラベル:** Webクリップとともに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられている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、**参照**をクリックしてファイルの場所へ移動し、使用するアイコンファイルを選択します。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付の選択**と**削除までの期間（時間）**です。
    - **日付の選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を数値で入力します。
  - **ユーザーによるポリシーの削除を許可:** ユーザーがデバイスからポリシーを削除できるタイミングを選択できます。メニューから**常に**、**パスコードが必要**、または**しない**を選択します。**パスコードが必要**を選択した場合は、**削除パスコード**フィールドにパスコードを入力します。
  - **プロファイルスコープ:** このポリシーを**ユーザー**に適用するか、**システム**全体に適用するかを選択します。デフォルトは**ユーザー**です。このオプションは、macOS 10.7以降でのみ利用可能です。

Windowsデスクトップ/タブレットの設定

- **名前:** Webクリップとともに表示されるラベルを入力します。
- **URL:** Webクリップに関連付けられているURLを入力します。

Wi-Fiデバイスポリシー

XenMobile®で新しいWi-Fiデバイスポリシーを作成したり、既存のポリシーを編集したりするには、**Configure > Device Policies**ページを使用します。Wi-Fiポリシーを使用すると、以下の項目を定義することで、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、**Configure > Device Policies**に移動します。詳細については、「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いることを確認してください。

- 使用する予定のデリバリーグループを作成します。
- ネットワーク名と種類を把握します。
- 使用する予定の認証またはセキュリティの種類を把握します。
- 必要となる可能性のあるプロキシサーバー情報を把握します。
- 必要なCA証明書をインストールします。
- 必要な共有キーを用意します。
- 証明書ベースの認証用の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。

詳細については、認証とそのサブ記事を参照してください。

iOS設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-wifi-ios.png)

- **ネットワークの種類:** リストから、使用するネットワークの種類を設定するために、**Standard**、**Legacy Hotspot**、または**Hotspot 2.0**を選択します。
- **ネットワーク名:** デバイスで利用可能なネットワークのリストに表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **非表示ネットワーク (ネットワークがオープンまたはオフの場合に有効にする):** ネットワークを非表示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する):** 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、このネットワークには参加しません。デバイスが自動的に接続する前に、ユーザーは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。

- **静的MACアドレスを使用:** MACアドレスは、デバイスがネットワーク内で送信する一意の識別子です。プライバシーを向上させるため、iOSおよびiPadOSデバイスは、ネットワークに接続するたびに異なるMACアドレスを使用できます。**オン**の場合、デバイスはこのネットワークに接続するときに常に同じMACアドレスを使用します。**オフ**の場合、デバイスはこのネットワークに接続するたびに異なるMACアドレスを使用します。デフォルトは**オフ**です。
- **セキュリティの種類:** リストから、使用する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 - それ以上の構成は不要です。
  - 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 Enterprise: WPA-2 Enterpriseを使用するには、Simple Certificate Enrollment Protocol (SCEP) を構成する必要があります。その後、XenMobileは証明書をデバイスに送信して、Wi-Fiサーバーへの認証を行うことができます。SCEPを構成するには、**設定 > 資格情報プロバイダー**の配布ページに移動します。詳細については、「資格情報プロバイダー」を参照してください。
  - 任意 (Enterprise)

以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

iOSのWPA、WPA Personal、任意 (Personal) の設定

パスワード: オプションの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、ユーザーはログオン時にパスワードの入力を求められる場合があります。

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 iOS 設定

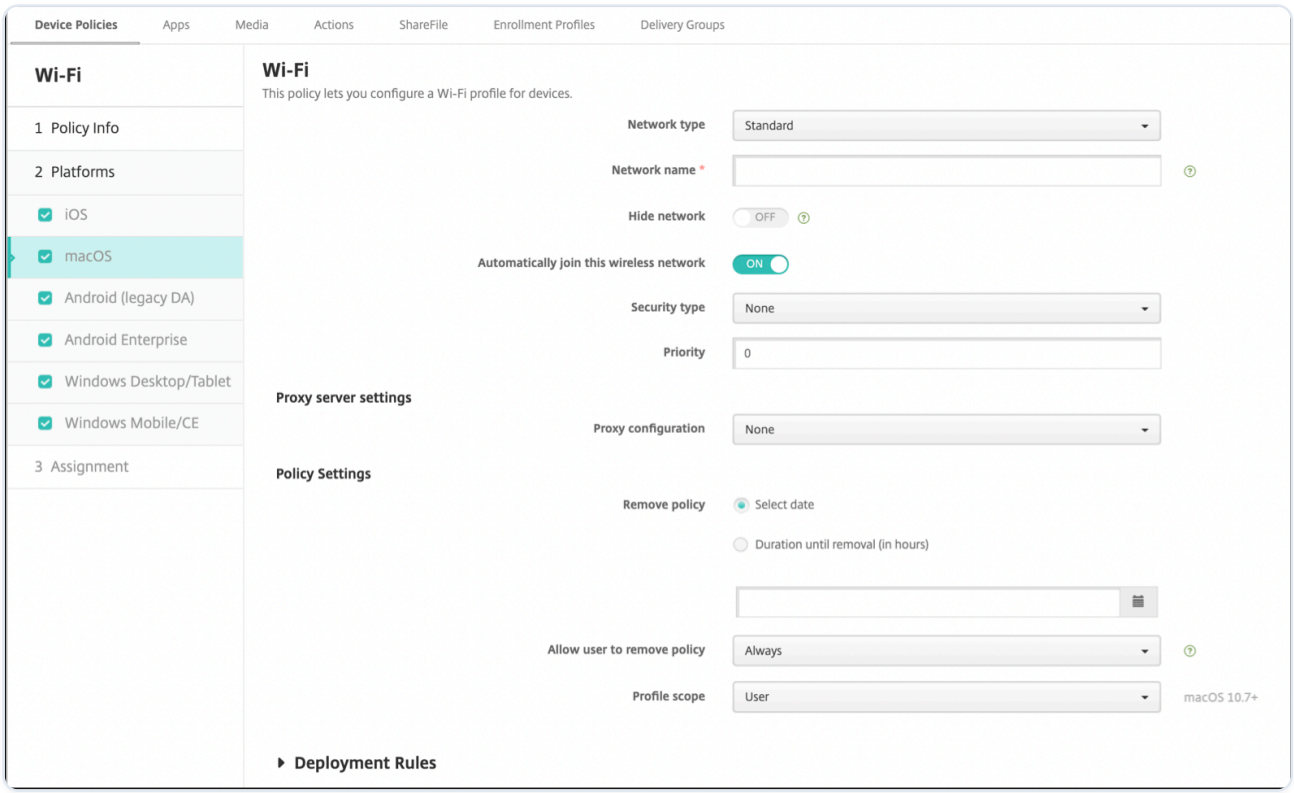
これらの設定のいずれかを選択すると、その設定は**プロキシサーバー設定**の後に一覧表示されます。

- **プロトコル、許可されるEAPタイプ:** サポートするEAPタイプを有効にし、関連する設定を構成します。使用可能な各EAPタイプのデフォルトは**オフ**です。
- **内部認証 (TTLS):** *TTLSを有効にした場合にのみ必要です。*リストから、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、プロビジョニングPACを使用するかどうかを選択します。
    - **プロビジョニングPAC**を選択した場合、エンドユーザークライアントと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:** オプションの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、ユーザーはログオン時にパスワードの入力を求められる場合があります。
  - **ID資格情報 (キーストアまたはPKI資格情報):** リストから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** *を有効にする場合にのみ必要です。*外部から見えるユーザー名を入力します。「anonymous」などの一般的な用語を入力してユーザー名が表示されないようにすることで、セキュリティを強化できます。
  - **TLS証明書を要求する:** TLS証明書を要求するかどうかを選択します。
- **信頼**
  - **信頼された証明書:** 信頼された証明書を追加するには、**追加**をクリックし、追加する各証明書について、次の操作を行います。
    - **アプリケーション:** リストから追加するアプリケーションを選択します。
    - 証明書を保存するには**保存**をクリックするか、**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名:** 信頼されたサーバー証明書の共通名を追加するには、**追加**をクリックし、追加する各名前について、次の操作を行います。
    - **証明書:** サーバー証明書の名前を入力します。wpa.*.example.com のようにワイルドカードを使用して名前を指定できます。
    - 証明書名を保存するには**保存**をクリックするか、**キャンセル**をクリックします。

- **信頼例外を許可する:** 証明書が信頼されていない場合に、証明書の信頼ダイアログがユーザーデバイスに表示されるかどうかを選択します。デフォルトは**オン**です。
- **プロキシサーバー設定**
  - **プロキシ構成:** リストから、**なし**、**手動**、または**自動**を選択して、VPN接続がプロキシサーバー経由でルーティングされる方法を設定し、その他のオプションを構成します。デフォルトは**なし**で、それ以上の構成は不要です。
  - **手動**を選択した場合、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:** プロキシサーバーへの認証に使用するオプションのユーザー名を入力します。
    - **パスワード:** プロキシサーバーへの認証に使用するオプションのパスワードを入力します。
  - **自動**を選択した場合、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に到達できない場合に直接接続を許可する:** PACファイルに到達できない場合に、ユーザーが宛先に直接接続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**オン**です。このオプションはiOS 7.0以降でのみ利用可能です。
- **ポリシー設定**
  - **ポリシーの削除:** ポリシー削除のスケジュール方法を選択します。利用可能なオプションは、**日付を選択**と**削除までの期間（時間）**です。
    - **日付を選択:** カレンダーをクリックして、削除する特定の日付を選択します。
    - **削除までの期間（時間）:** ポリシーが削除されるまでの時間を時間単位で入力します。iOS 6.0以降でのみ利用可能です。

macOS設定



- **ネットワークの種類:** リストから、使用するネットワークの種類として、**Standard**、**Legacy Hotspot**、または **Hotspot 2.0** を選択します。
- **ネットワーク名:** デバイスで利用可能なネットワークのリストに表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **ネットワークを非表示にする:** ネットワークを非表示にするかどうかを選択します。
- **このワイヤレスネットワークに自動的に参加する:** 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、このネットワークには参加しません。デバイスが自動的に接続する前に、ユーザーは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:** リストから、使用する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 - それ以上の設定は不要です。
    - 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)

- **優先度:** 複数のネットワークがある場合、**優先度**フィールドに数値を入力して、ネットワーク接続の優先度を設定します。デバイスは最も小さい番号のネットワークを選択します。

以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

WPA、WPA Personal、WPA 2 Personal、任意 (パーソナル) のmacOS設定

- **パスワード:** オプションの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、ユーザーはログオン時にパスワードの入力を求められる場合があります。

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、任意の (エンタープライズ) の macOS 設定

これらの設定のいずれかを選択すると、その設定は**プロキシサーバー設定**の後にリストされます。

- **プロトコル、許可されるEAPタイプ:** サポートするEAPタイプを有効にし、関連する設定を構成します。デフォルトでは、利用可能な各EAPタイプは**オフ**です。
- **内部認証 (TTLS):** *TTLSを有効にした場合にのみ必要です。*リストから、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、プロビジョニングPACを使用するかどうかを選択します。
        - **プロビジョニングPAC**を選択した場合、エンドユーザークライアントと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:** オプションの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、ユーザーはログオン時にパスワードの入力を求められる場合があります。

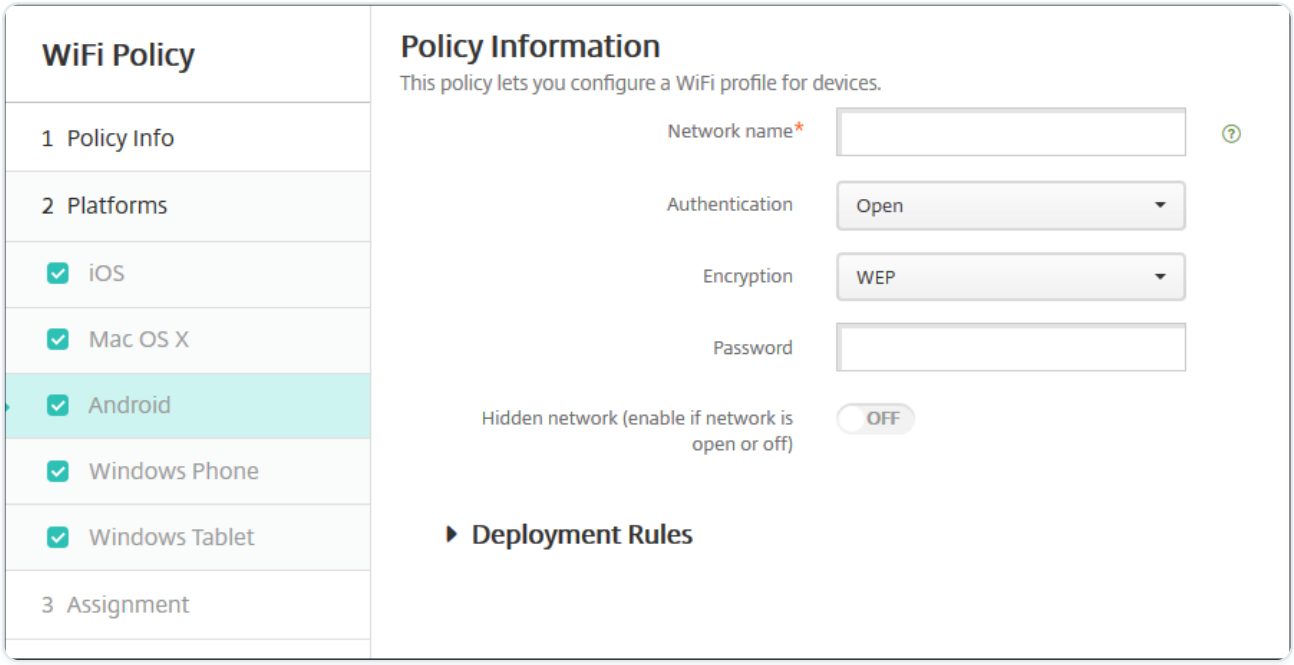
- **ID資格情報 (キーストアまたはPKI資格情報):** リストから、ID資格情報の種類を選択します。デフォルトは**なし**です。
- **外部ID: PEAP**、**TTLS**、*または* **EAP-FAST***を有効にした場合にのみ必要です*。外部から見えるユーザー名を入力します。「anonymous」のような一般的な用語を入力することで、ユーザー名が見えないようにしてセキュリティを強化できます。
- **TLS証明書を要求する**：TLS証明書を要求するかどうかを選択します。

- **信頼**
  - **信頼された証明書**：信頼された証明書を追加するには、**追加**をクリックし、追加する各証明書について以下を実行します。
    - **アプリケーション**：リストから、追加するアプリケーションを選択します。
    - 証明書を保存するには**保存**をクリックするか、**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名**：信頼されたサーバー証明書の共通名を追加するには、**追加**をクリックし、追加する各名前について以下を実行します。
    - **証明書**：追加するサーバー証明書の名前を入力します。wpa.*.example.com のようにワイルドカードを使用して名前を指定できます。
    - 証明書名を保存するには**保存**をクリックするか、**キャンセル**をクリックします。
- **信頼例外を許可**：証明書が信頼されていない場合に、ユーザーデバイスに証明書の信頼ダイアログが表示され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**：ログインウィンドウで入力された同じ資格情報を使用してユーザーを認証するかどうかを選択します。
- **プロキシサーバー設定**
  - **プロキシ構成**：リストから、**なし**、**手動**、または**自動**を選択して、VPN接続がプロキシサーバーを介してルーティングされる方法を設定し、追加のオプションを構成します。デフォルトは**なし**で、それ以上の構成は不要です。
  - **手動**を選択した場合は、以下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:** プロキシサーバーで認証するためのオプションのユーザー名を入力します。

- **パスワード:** プロキシサーバーで認証するためのオプションのパスワードを入力します。

- **自動**を選択した場合、以下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に到達できない場合に直接接続を許可する:** PACファイルに到達できない場合に、ユーザーが直接宛先に接続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**オン**です。このオプションはiOS 7.0以降でのみ利用可能です。

Androidの設定



- **ネットワーク名:** ユーザーデバイスで利用可能なネットワークのリストにあるSSIDを入力します。
- **認証:** リストから、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

以下のセクションでは、前述の各接続タイプについて構成するオプションを一覧表示します。

Androidのオープン、共有設定

- **暗号化:** リストから、**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:** オプションのパスワードを入力します。

AndroidのWPA、WPA-PSK、WPA2、WPA2-PSK設定

- **暗号化:** リストから、**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:** オプションのパスワードを入力します。

Androidの802.1x設定

- **EAPタイプ:** リストから、**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:** オプションのパスワードを入力します。
- **認証フェーズ2:** リストから、**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とドメインを入力します。
- **匿名:** オプションの、外部から見えるユーザー名を入力します。ユーザー名が表示されないように、「anonymous」のような一般的な用語を入力することで、セキュリティを強化できます。
- **CA証明書:** リストから、使用する証明書を選択します。
- **ID資格情報:** リストから、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。
- **非表示ネットワーク (ネットワークがオープンまたはオフの場合に有効):** ネットワークを非表示にするかどうかを選択します。

Android Enterpriseの設定

Wi-Fiポリシー Android Enterpriseの画像(/en-us/xenmobile/server/media/device-policy-wifi-android-enterprise.png)

- **ネットワーク名:** ユーザーデバイスで利用可能なネットワークのリストにあるSSIDを入力します。
- **認証:** リストから、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

以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

Android Enterpriseのオープン、共有設定

- **暗号化:** リストから**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:** オプションのパスワードを入力します。

WPA、WPA-PSK、WPA2、WPA2-PSK の Android Enterprise 設定

- **暗号化:** リストから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:** オプションのパスワードを入力します。

Android Enterprise 向けの 802.1x 設定

- **EAPタイプ:** リストから**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:** オプションのパスワードを入力します。
- **認証フェーズ2:** リストから**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とドメインを入力します。
- **匿名:** オプションの、外部から見えるユーザー名を入力します。ユーザー名が見えないように、「anonymous」のような一般的な用語を入力することで、セキュリティを強化できます。
- **CA証明書:** リストから使用する証明書を選択します。
- **ドメイン:** 必須のドメイン名を入力します。詳細については、「ドメイン」を参照してください。

> **注:**
>
> Android 13以降を実行しているデバイスでWi-Fiポリシーを構成する場合、**CA証明書**と**ドメイン**のフィールドは必須で更新する必要があります。更新されない場合、構成は失敗します。

- **ID資格情報:** リストから、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。

- **非表示ネットワーク (ネットワークがオープンまたはオフの場合に有効にする):** ネットワークを非表示にするかどうかを選択します。

Windows 10およびWindows 11の設定

デバイスポリシー構成画面の画像(/en-us/xenmobile/server/media/device-policy-wifi-windesktop.png)

- **認証:** ドロップダウンリストから、Wi-Fi接続で使用するセキュリティの種類をクリックします。
  - 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: 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構成により、XenMobileはWi-Fiサーバーへの認証のために証明書をデバイスに送信できます。SCEPを構成するには、**設定 > 資格情報プロバイダー**の**配信**ページに移動します。詳細については、「資格情報プロバイダー」を参照してください。

以下のセクションでは、上記の各接続タイプに対して構成するオプションを一覧表示します。

Windows 10およびWindows 11のオープン設定

- **非表示ネットワーク (ネットワークがオープンまたはオフの場合に有効にする):** ネットワークを非表示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およびWindows 11のWPAパーソナル、WPA-2パーソナル設定

- **暗号化:** リストから、暗号化の種類を設定するために**AES**または**TKIP**のいずれかを選択します。デフォルトは**AES**です。
- **非表示ネットワーク (ネットワークがオープンまたはオフの場合に有効にする):** ネットワークが非表示であるかどうかを選択します。
- **自動接続:** 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およびWindows 11用のWPA-2 Enterprise設定

- **暗号化:** リストから、暗号化の種類を設定するために**AES**または**TKIP**のいずれかを選択します。デフォルトは**AES**です。

- **EAPタイプ:** リストから、EAPタイプを設定するために**PEAP-MSCHAPv2**または**TLS**のいずれかを選択します。デフォルトは**PEAP-MSCHAPv2**です。
- **非表示の場合に接続:** ネットワークが非表示であるかどうかを選択します。
- **自動接続:** 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:** リストから、SCEPの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 Information Protection デバイスポリシー

Windows Information Protection (WIP) は、以前は enterprise data protection (EDP) と呼ばれていましたが、企業データの潜在的な漏洩から保護する Windows テクノロジーです。データ漏洩は、企業データを企業保護されていないアプリに共有したり、アプリ間で共有したり、組織ネットワーク外に共有したりすることで発生する可能性があります。詳細については、「Windows Information Protection (WIP) を使用して企業データを保護する」を参照してください。

XenMobile® でデバイスポリシーを作成し、設定した適用レベルで Windows Information Protection を必要とするアプリを指定できます。Windows Information Protection ポリシーは、Windows 10 または Windows 11 を実行している監視対象のタブレットおよびデスクトップ向けです。

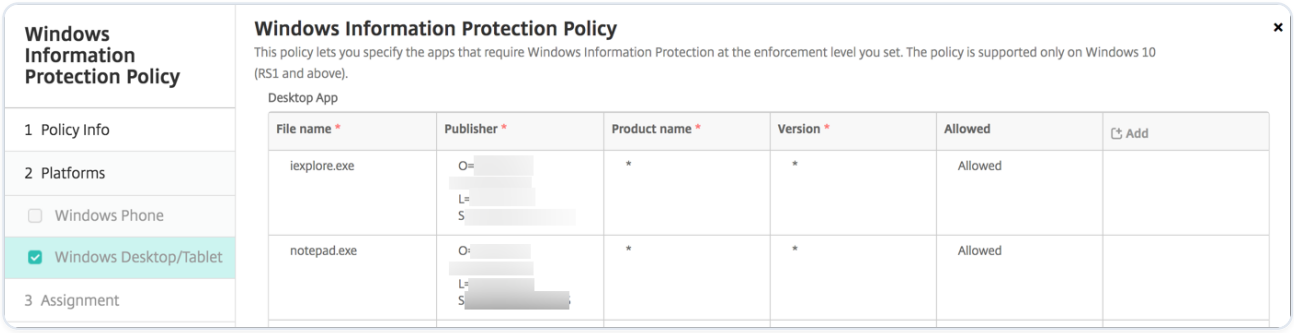
XenMobile には一般的なアプリがいくつか含まれており、他のアプリを追加することもできます。ポリシーには、ユーザーエクスペリエンスに影響を与える適用レベルを指定します。たとえば、次のことができます。

- 不適切なデータ共有をブロックする。
- 不適切なデータ共有について警告し、ユーザーがポリシーを上書きできるようにする。
- 不適切なデータ共有をログに記録し、許可しながら、WIP をサイレントで実行する。

Windows Information Protection からアプリを除外するには、Microsoft AppLocker XML ファイルでアプリを定義し、それらのファイルを 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、 > に移動します。詳細については、「デバイスポリシー」を参照してください。

Windows 10 および Windows 11 の設定



- **Desktop App** (Windows 10 または Windows 11 デスクトップ)、**Store App** (Windows 10 または Windows 11 タブレット): XenMobile には、上記のサンプルに示すように、いくつかの一般的なアプリが含まれています。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。

  他のアプリを追加するには、 または テーブルで をクリックし、アプリ情報を提供します。

  Allowed アプリは企業データを読み取り、作成、更新できます。**Denied** アプリは企業データにアクセスできません。**Exempt** アプリは企業データを読み取ることができますが、データを作成または変更することはできません。

  - **AppLocker XML:** Microsoft は、WIP との互換性の問題が知られている Microsoft アプリのリストを提供しています。WIP からこれらのアプリを除外するには、**Browse** をクリックしてリストをアップロードします。XenMobile は、アップロードされた AppLocker XML と、構成されたデスクトップアプリおよびストアアプリをデバイスに送信されるポリシーに結合します。詳細については、「Windows Information Protection の推奨ブロックリスト」を参照してください。
  - **適用レベル:** Windows Information Protection でデータ共有を保護および管理する方法を指定するオプションを選択します。既定値は **Off** です。
    - **0-Off:** WIP はオフになり、データを保護または監査しません。
    - **1-Silent:** WIP はサイレントで実行され、不適切なデータ共有をログに記録し、何もブロックしません。ログは Reporting CSP を介してアクセスできます。
    - **2-Override:** WIP は、安全でない可能性のあるデータ共有についてユーザーに警告します。ユーザーは警告を上書きしてデータを共有できます。このモードでは、ユーザーによる上書きを含むアクションが監査ログに記録されます。
    - **3-Block:** WIP は、ユーザーが安全でない可能性のあるデータ共有を完了するのを防ぎます。
  - **保護されたドメイン名:** 企業がユーザーIDに使用するドメイン。この管理されたIDドメインのリストは、プライマリドメインとともに、管理対象企業のIDを構成します。リストの最

初のドメインは、Windows UIで使用される主要な企業IDです。リスト項目を区切るには「|」を使用します。例: `domain1.com | domain2.com`

- **データ回復証明書: 参照**をクリックし、暗号化された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、暗号化ファイルシステム (EFS) のデータ回復エージェント (DRA) 証明書と同じですが、グループポリシーではなく MDM を介して配信されます。回復証明書が利用できない場合は、作成します。詳細については、このセクションの「データ回復証明書を作成する」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リスト。WIP は、このリスト内の完全修飾ドメインへのすべてのトラフィックを保護します。この設定は、**IP範囲**設定と合わせて、プライベートネットワーク上のネットワークエンドポイントが企業のものか個人用かを検出します。リスト項目を区切るにはコンマを使用します。例: corp.example.com,region.example.com
- **IP範囲:** 企業ネットワーク内のコンピューターを定義する企業 IPv4 および IPv6 範囲のリスト。WIP は、これらの場所を企業データ共有の安全な宛先と見なします。リスト項目を区切るにはコンマを使用します。例:

  `10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **IP範囲リストは信頼できる:** Windows による IP 範囲の自動検出を防ぐには、この設定を **On** に変更します。既定値は **Off** です。
- **プロキシサーバー:** 企業が企業リソースに使用できるプロキシサーバーのリスト。ネットワークでプロキシを使用する場合、この設定が必要です。プロキシサーバーがない場合、クライアントがプロキシの背後にあるときに企業リソースが利用できない可能性があります。たとえば、ホテルやレストランの特定の Wi-Fi ホットスポットからリソースが利用できない場合があります。リスト項目を区切るにはコンマを使用します。例:

  `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 リソースにアクセスするために経由するプロキシ サーバーのリスト。このサーバー タイプを使用すると、接続しているクラウド リソースが企業リソースであることが示されます。WIP で保護されていないトラフィックに使用される **プロキシ サーバー** 設定のサーバーは、このリストに含めないでください。リスト項目を区切るにはコンマを使用します。例:

  `example.internalproxy1.com;10.147.80.50`
- **クラウド リソース:** WIP によって保護されているクラウド リソースのリスト。各クラウド リソースについて、オプションで**プロキシ サーバー**リストにプロキシ サーバーを指定して、このクラウド リソースのトラフィックをルーティングすることもできます。**プロキシ**

サーバーを介してルーティングされるすべてのトラフィックは、エンタープライズ トラフィックとして扱われます。リスト項目を区切るにはコンマを使用します。例:

```
domain1.com:InternalProxy.domain1.com,domain2.com:InternalProxy.domain2.com
```

- **登録解除時に WIP 証明書を失効させる:** Windows Information Protection から登録解除されたときに、ユーザーデバイスからローカル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企業データにアクセスできなくなります。**オフ**の場合、キーは失効せず、ユーザーは登録解除後も保護されたファイルにアクセスできます。既定値は**オン**です。
- **オーバーレイ アイコンを表示:** エクスプローラーの企業ファイルおよびスタートメニューのエンタープライズ専用アプリタイルに、Windows Information Protection アイコンのオーバーレイを含めるかどうかを指定します。既定値は**オフ**です。

データ回復証明書を作成する

Windows Information Protectionポリシーを有効にするには、データ回復証明書が必要です。

1. XenMobile コンソールが実行されているマシンで、コマンドプロンプトを開き、証明書を作成するフォルダー（Windows\\System32 以外）に移動します。
2. 次のコマンドを実行します。

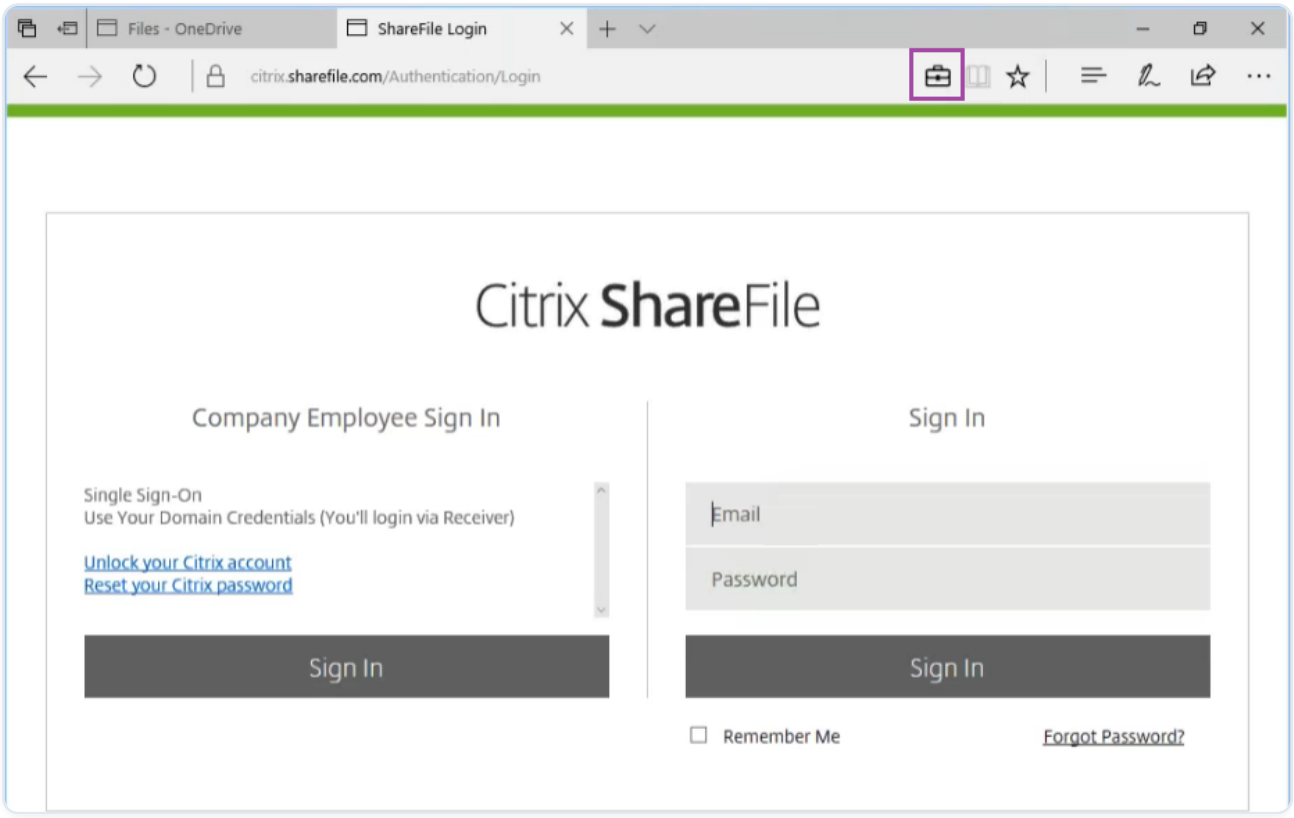
   ```
   cipher /r:ESFDRA
   ```

3. プロンプトが表示されたら、秘密キーファイルを保護するためのパスワードを入力します。

   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、Windows 10 および Windows 11 タブレットに適用される .cer ファイルをインポートします。

ユーザーエクスペリエンス

Windows Information Protection が有効な場合、アプリとファイルにはアイコンが含まれます。



Windows Information Protection アイコンの例(/en-us/xenmobile/server/media/wip-file-overlay.png)

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した場合、構成されている適用レベルに応じて、以下の通知が表示されます。

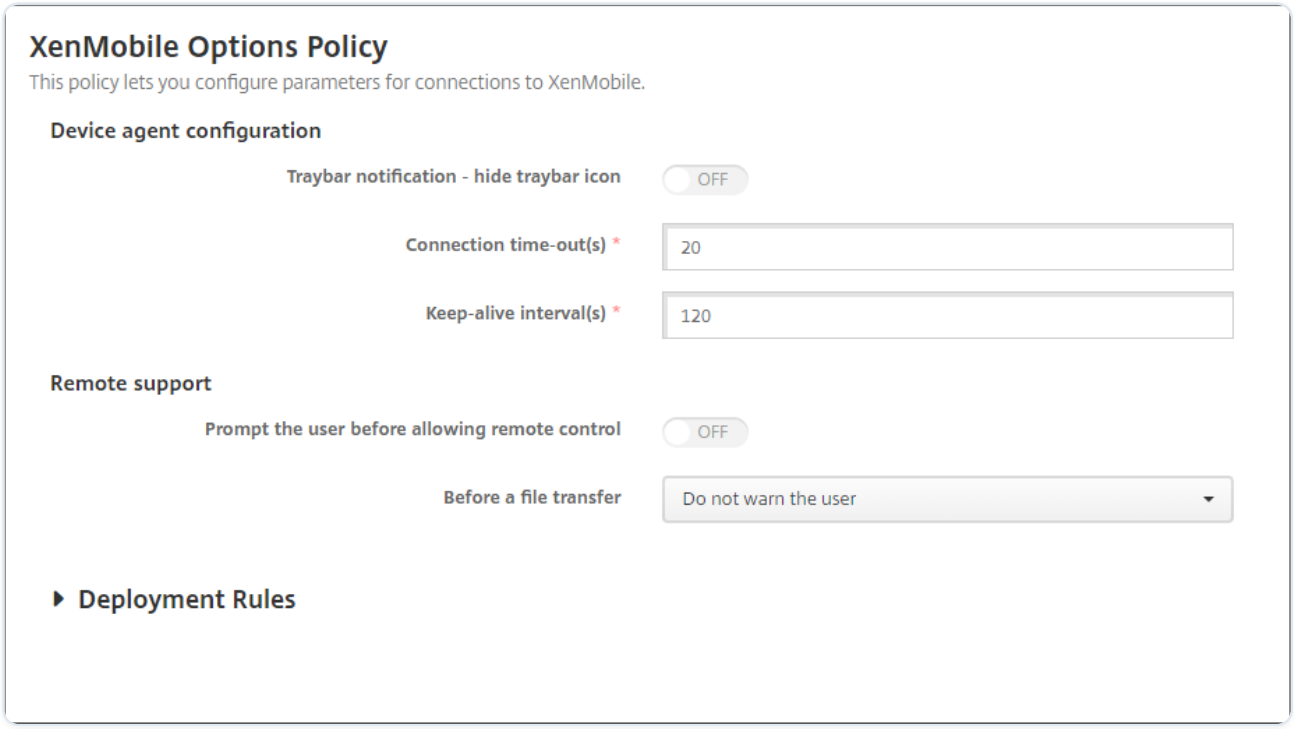
通知の例(/en-us/xenmobile/server/media/wip-protected-content-message.png)

XenMobile® オプションデバイスポリシー

AndroidデバイスからXenMobileに接続する際のSecure Hubの動作を構成するために、XenMobileオプションポリシーを追加します。

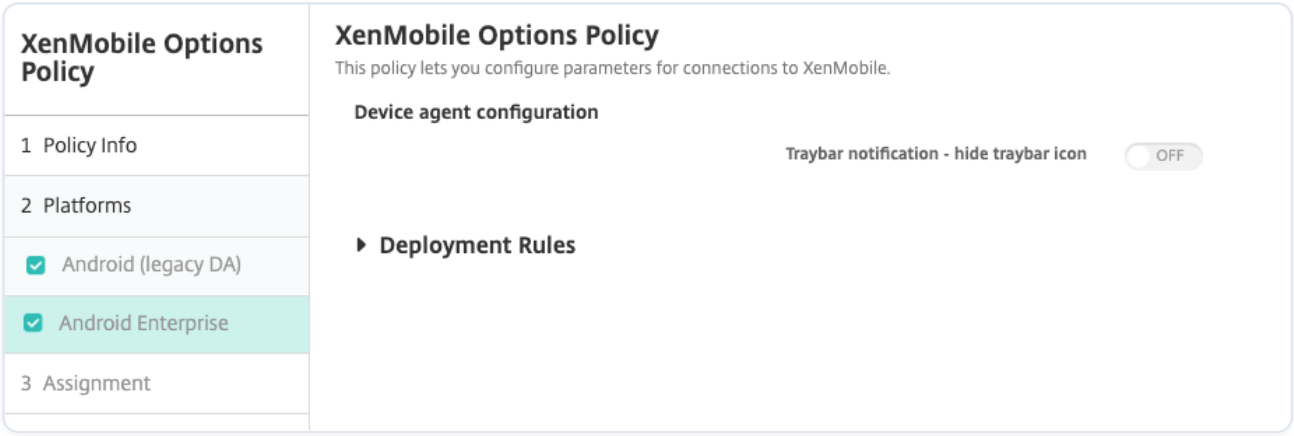
このポリシーを追加または構成するには、 > の順に選択します。詳しくは、「デバイスポリシー」を参照してください。

Android設定



- **トレイバー通知 - トレイバーアイコンを非表示にする:** 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 です。
- **接続: タイムアウト(秒):** 接続がタイムアウトするまでにアイドル状態を維持できる時間を秒単位で入力します。デフォルトは20秒です。
- **キープアライブ間隔(秒):** 接続を開いたままにする時間を秒単位で入力します。デフォルトは120秒です。

アンドロイド エンタープライズ 設定



Androidバージョン7以降でサポートされています。

トレイバー通知 - トレイバーアイコンを非表示にする: 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 です。

注:

Android Enterpriseで実行されているデバイスのVPNサービスを有効にする場合は、**VPNデバイスポリシー**で**オプションを有効にできます。以前のリリースで**XenMobileオプションデバイスポリシー**の**オプションをすでに有効にしている場合は、**VPNデバイスポリシー**で再度同じオプションを有効にしてください。VPNデバイスポリシーについて詳しくは、「VPNデバイスポリシー - Android Enterprise設定」を参照してください。

XenMobile® デバイスアンインストールポリシー

XenMobileで、AndroidデバイスからXenMobileをアンインストールするためのデバイスポリシーを追加できます。展開されると、このポリシーは展開グループ内のすべてのデバイスからXenMobileを削除します。

このポリシーを追加または構成するには、 **>** に移動します。詳細については、デバイスポリシーを参照してください。

Android設定の構成

- **デバイスからXenMobileをアンインストール:** 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。

アプリを追加

XenMobile®にアプリを追加すると、モバイルアプリケーション管理 (MAM) 機能が提供されます。XenMobileは、アプリケーションの配信、ソフトウェアライセンス、構成、およびアプリケーションライフサイクル管理を支援します。

アプリをMDX対応にすることは、ほとんどの種類のアプリをユーザーデバイスに配布するための準備の重要な部分です。MDXの概要については、「MDX Toolkitについて」および「MAM SDKの概要」を参照してください。

- Citrixは、アプリをMDX対応にするためにMAM SDKを使用することを推奨しています。または、MDX Toolkitが非推奨になるまで、アプリのMDXラッピングを継続することもできます。「非推奨」を参照してください。
- MDX Toolkitを使用してCitrix®モバイル生産性向上アプリをラップすることはできません。モバイル生産性向上アプリのMDXファイルは、Citrixダウンロードから入手してください。

XenMobileコンソールにアプリを追加すると、次のことができます。

- アプリ設定を構成する
- 必要に応じて、Secure Hubでアプリを整理するためにカテゴリに配置する
- 必要に応じて、ユーザーがアプリにアクセスする前に承認を要求するワークフローを定義する
- ユーザーにアプリを展開する

この記事では、アプリを追加するための一般的なワークフローについて説明します。プラットフォーム固有の詳細については、以下の記事を参照してください。

- Android Enterpriseアプリを配布する
- Appleアプリを配布する

アプリの種類と機能

次の表は、XenMobileで展開できるアプリの種類をまとめたものです。

アプリの種類	ソース	注記	参照
MDX	ユーザー向けに開発するiOSおよびAndroidアプリ。Citrixモバイル生産性向上アプリ。	MAM SDKを使用してiOSまたはAndroidアプリを開発するか、MDX Toolkitでラップします。モバイル生産性向上アプリの場合は、Citrixダウンロード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。その後、アプリをXenMobileに追加します。	MDXアプリを追加する
パブリックアプリストア	Google PlayやApple App Storeなどのパブリックアプリストアから入手できる無料または有料のアプリ。	アプリをアップロードし、MDXを有効にしてから、XenMobileにアプリを追加します。	パブリックアプリストアアプリを追加する
WebおよびSaaS	社内ネットワーク（Webアプリ）またはパブリックネットワーク（SaaS）。	Citrix Workspace™は、MDMに登録されているiOSおよびAndroidデバイスからネイティブSaaSアプリへのモバイルシングルサインオンを提供します。または、Security Assertion Markup Language (SAML) アプリケーションコネクタを使用します。	WebアプリまたはSaaSアプリを追加する
エンタープライズ	MDXが有効になっていないWin 32アプリを含むプライベートアプリ。MDXが有効になっているプライ	アプリをXenMobileに追加します。	エンタープライズアプリを追加する

アプリの種類	ソース	注記	参照
	ベートAndroid Enterpriseアプリ。エンタープライズアプリは、コンテンツデリバリーネットワークの場所またはXenMobileサーバーに存在します。		
Webリンク	インターネットのWebアドレス、イントラネットのWebアドレス、またはシングルサインオンを必要としないWebアプリ。	XenMobileでWebリンクを構成します。	Webリンクを追加する

アプリの配布を計画する際は、次の機能を考慮してください。

- サイレントインストールについて
- 必須アプリとオプションアプリについて
- アプリのカテゴリについて
- Microsoft 365アプリを有効にする
- ワークフローを適用する
- App StoreとCitrix Secure Hub™のブランディング

サイレントインストールについて

Citrixは、iOS、Android Enterprise、およびSamsungアプリのサイレントインストールとアップグレードをサポートしています。サイレントインストールとは、デバイスに展開するアプリのインストールをユーザーに促すことなく、アプリがバックグラウンドで自動的にインストールされることを意味します。

サイレントインストールを実装するための前提条件:

- iOSの場合、管理対象のiOSデバイスを監視モードにします。詳細については、「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 Enterpriseの場合、アプリはデバイスのAndroidワークプロファイルにインストールされます。詳細については、「Android Enterprise」を参照してください。
- Samsungデバイスの場合、デバイスでSamsung Knoxを有効にします。

  そのためには、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。詳細については、「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。

必須アプリとオプションアプリについて

デリバリーグループにアプリを追加するときに、オプションにするか必須にするかを選択します。Citrixは、アプリを**必須**として展開することを推奨しています。

- 必須アプリはユーザーデバイスにサイレントインストールされ、ユーザーの操作を最小限に抑えます。この機能を有効にすると、アプリが自動的に更新されるようにもなります。
- オプションアプリでは、ユーザーがインストールするアプリを選択できますが、ユーザーはSecure Hubを介して手動でインストールを開始する必要があります。

必須としてマークされたアプリの場合、ユーザーは次のような状況で迅速に更新を受け取ることができます。

- 新しいアプリをアップロードし、必須としてマークする。
- 既存のアプリを必須としてマークする。
- ユーザーが必須アプリを削除します。
- Secure Hub のアップデートが利用可能です。

必須アプリの強制展開の要件

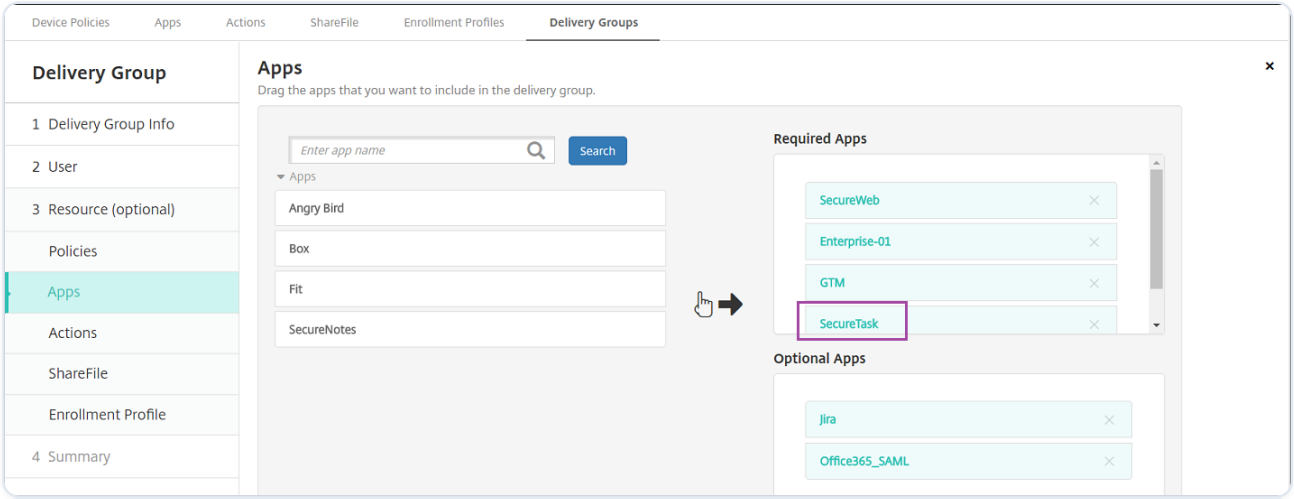
- XenMobile Server 10.6 (最小バージョン)
- iOS 用 Secure Hub 10.5.15 および Android 用 10.5.20 (最小バージョン)
- MAM SDK または MDX Toolkit 10.6 (最小バージョン)
- カスタムサーバープロパティ、force.server.push.required.apps

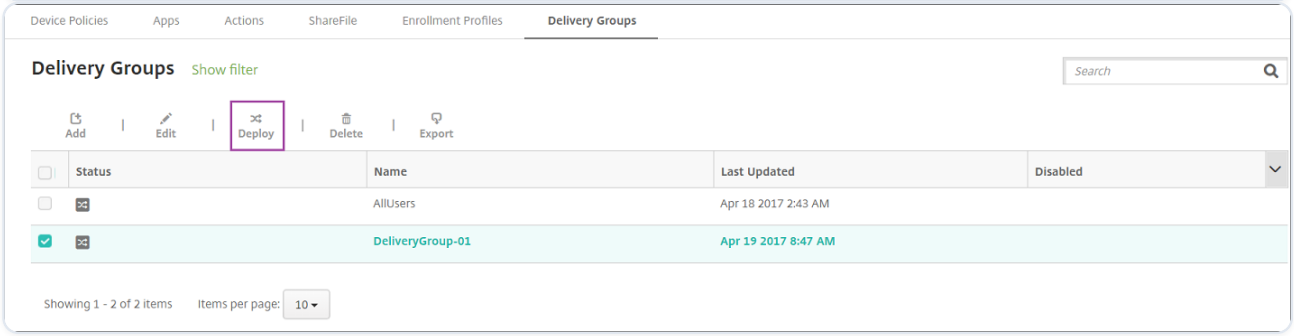
  必須アプリの強制展開は、デフォルトで無効になっています。この機能を有効にするには、カスタムキーサーバープロパティを作成します。**Key** と **Display name** を **force.server.push.required.apps** に設定し、**Value** を **true** に設定します。

- XenMobile Server と Secure Hub をアップグレードした後: 登録済みデバイスのユーザーは、必須アプリの展開アップデートを取得するために、一度 Secure Hub からサインオフしてからサインインする必要があります。

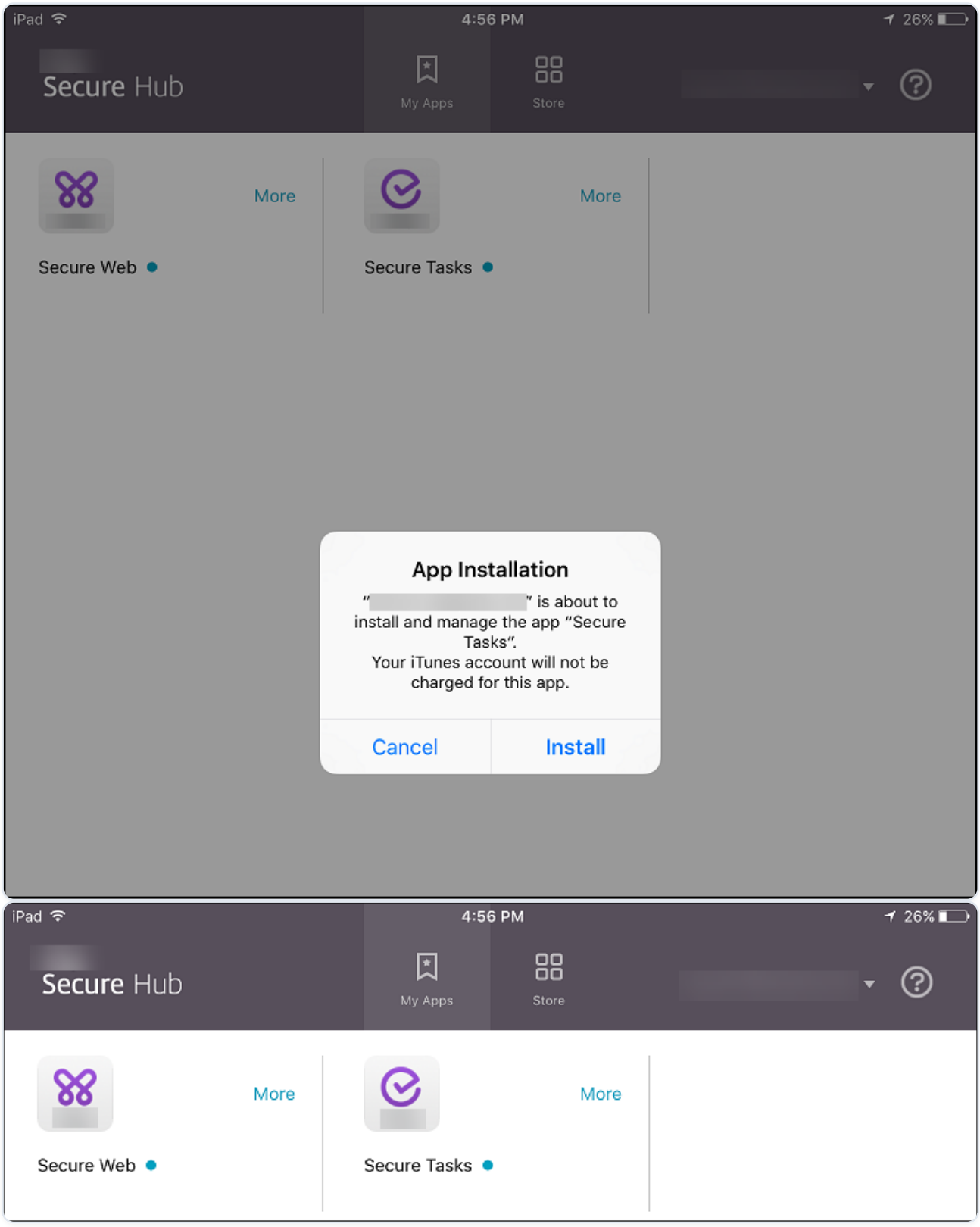
例

次の例は、Citrix Secure Tasks という名前の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手順を示しています。





サンプルアプリの Citrix Secure Tasks がユーザーデバイスに展開されると、Secure Hub はユーザーにアプリのインストールを促します。



重要:

MDX対応の必須アプリ（エンタープライズアプリやパブリックアプリストアアプリを含む）は、直ちにアップグレードされます。アプリの更新猶予期間に対して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、アップグレードは実行されます。

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向けのiOS必須アプリのワークフロー

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コンソールで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、アップグレードは自動的に開始されます。ユーザーに更新を促すプロンプトは表示されません。
5. ユーザーはホーム画面からアプリを開きます。アプリの更新猶予期間を設定し、ユーザーが後でアプリをアップグレードするようにタップした場合でも、アプリは直ちにアップグレードされます。

エンタープライズアプリ向けのAndroid必須アプリのワークフロー

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されます。(Nexusデバイスでは更新のインストールを促すプロンプトが表示されますが、Samsungデバイスではサイレントインストールが実行されます。)
4. ユーザーはホーム画面からアプリを開きます。アプリの更新猶予期間を設定し、ユーザーが後でアプリをアップグレードするようにタップした場合でも、アプリは直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実行されます。)

パブリックストアアプリ向けのAndroid必須アプリのワークフロー

1. 初期登録時にXenMobileアプリを展開します。必要なアプリがデバイスにインストールされます。
2. XenMobileコンソールでアプリを更新します。
3. XenMobileコンソールを使用して、必要なアプリを展開します。または、デバイスでSecure Hubストアを開きます。ストアに更新アイコンが表示されます。
4. アプリのアップグレードが自動的に開始されます。（Nexusデバイスでは、ユーザーに更新のインストールを促すプロンプトが表示されます。）

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されます。ユーザーに猶予期間のプロンプトは表示されません。（Samsungデバイスではサイレントインストールが実行されます。）

必須として構成されているアプリをアンインストールする

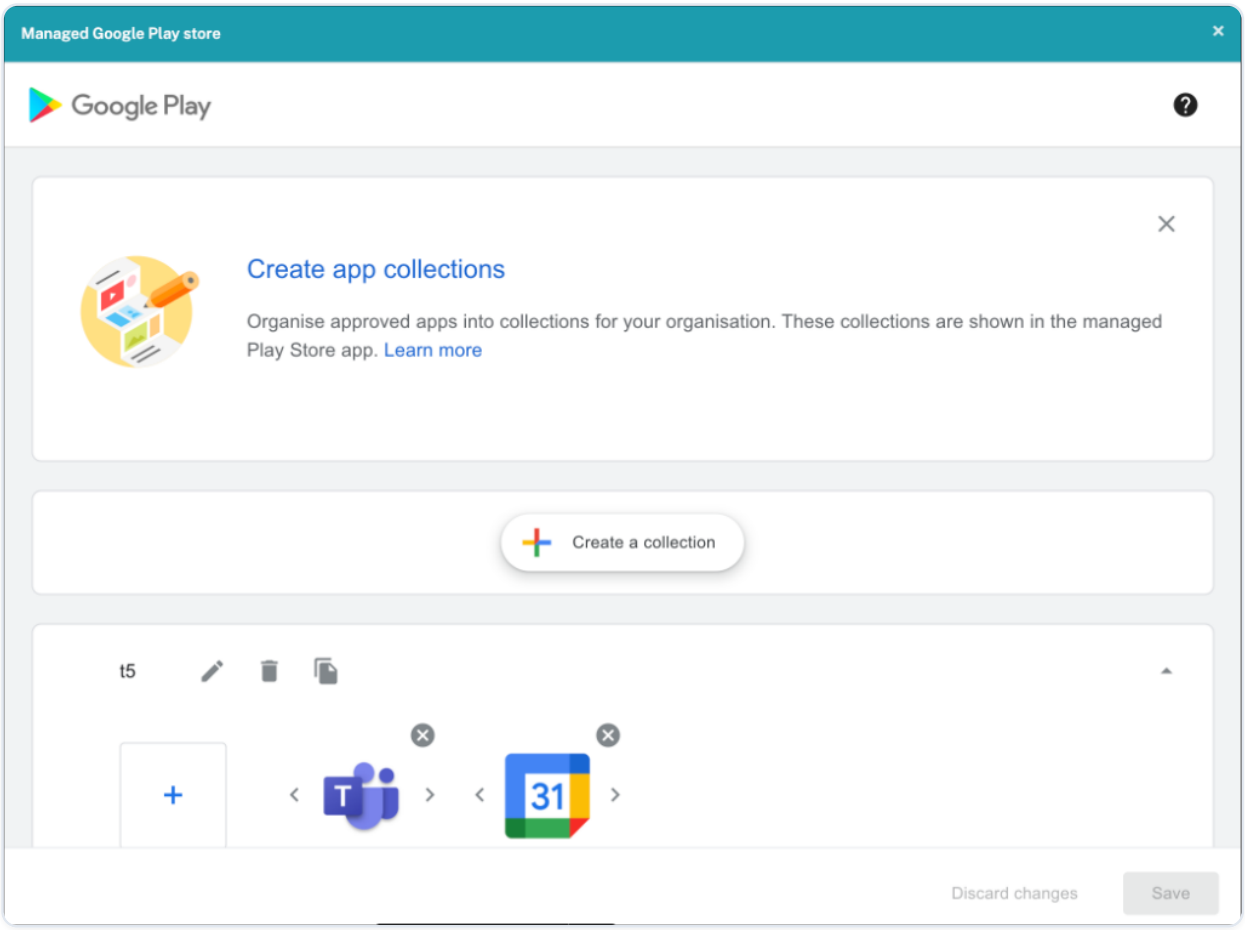
必須として構成されているアプリをユーザーがアンインストールできるようにすることができます。**［構成］>［デリバリーグループ］**の順に選択し、アプリを**［必須アプリ］**から**［オプションアプリ］**に移動します。

推奨： 特定のユーザーがアプリをアンインストールできるように、特別なデリバリーグループを使用してアプリを一時的にオプションに変更します。既存の必須アプリをオプションに変更し、そのデリバリーグループにアプリを展開してから、それらのデバイスからアプリをアンインストールできます。その後、そのデリバリーグループの今後の登録でアプリを必須にする場合は、アプリを必須に戻すことができます。

アプリの整理（Android Enterprise）

ユーザーがSecure Hubにログオンすると、XenMobile Serverで設定したアプリ、Webリンク、ストアのリストが表示されます。Android Enterpriseでは、これらのアプリをコレクションに整理して、ユーザーが特定のアプリ、ストア、またはWebリンクのみにアクセスできるようにすることができます。たとえば、財務コレクションを作成し、財務に関連するアプリのみをそのコレクションに追加します。または、営業アプリを割り当てる営業コレクションを構成することもできます。

1. XenMobile Serverコンソールで、**［構成］>［アプリ］>［アプリの整理］の順にクリックします。**［管理対象Google Playストア］**ウィンドウが表示されます。



2. **［コレクションの作成］**をクリックし、そのコレクションに追加するアプリを選択します。
3. コレクションの追加が完了したら、**［保存］**をクリックします。

> **注：**
>
> IT管理者は、Managed Google Playウィンドウのコレクションにアプリを追加する前に、そのアプリを承認する必要があります。IT管理者は、`<https://play.google.com/work>`にアクセスしてアプリを承認できます。今後のリリースでは、コレクションにアプリを追加する前に承認する必要はなくなります。

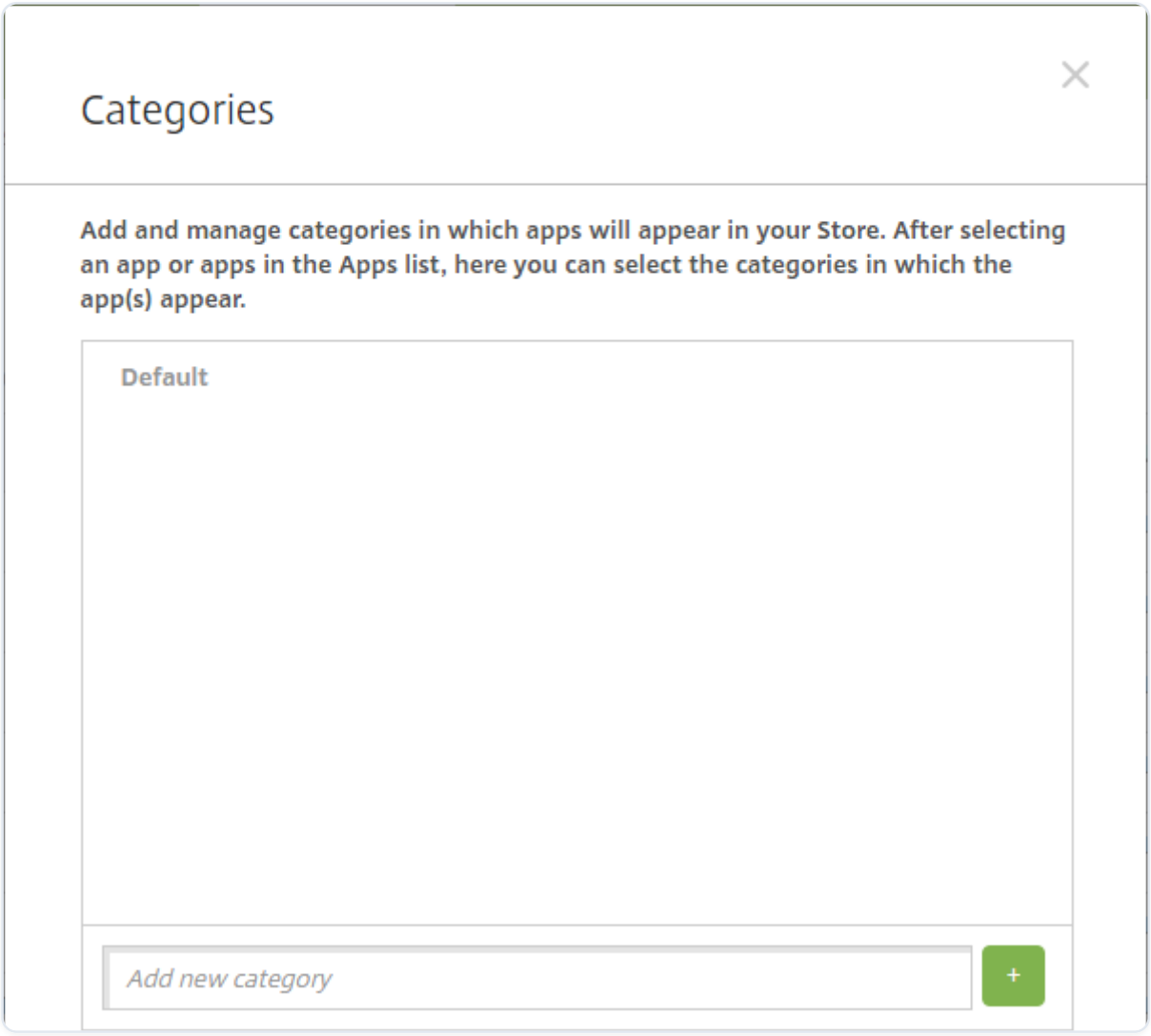
アプリカテゴリについて

ユーザーがSecure Hubにログオンすると、XenMobileで設定したアプリ、Webリンク、ストアのリストが表示されます。アプリカテゴリを使用すると、ユーザーが特定のアプリ、ストア、またはWebリンクのみにアクセスできるようにすることができます。たとえば、財務カテゴリを作成

し、財務にのみ関連するアプリをそのカテゴリに追加できます。または、営業アプリを割り当てる営業カテゴリを設定することもできます。

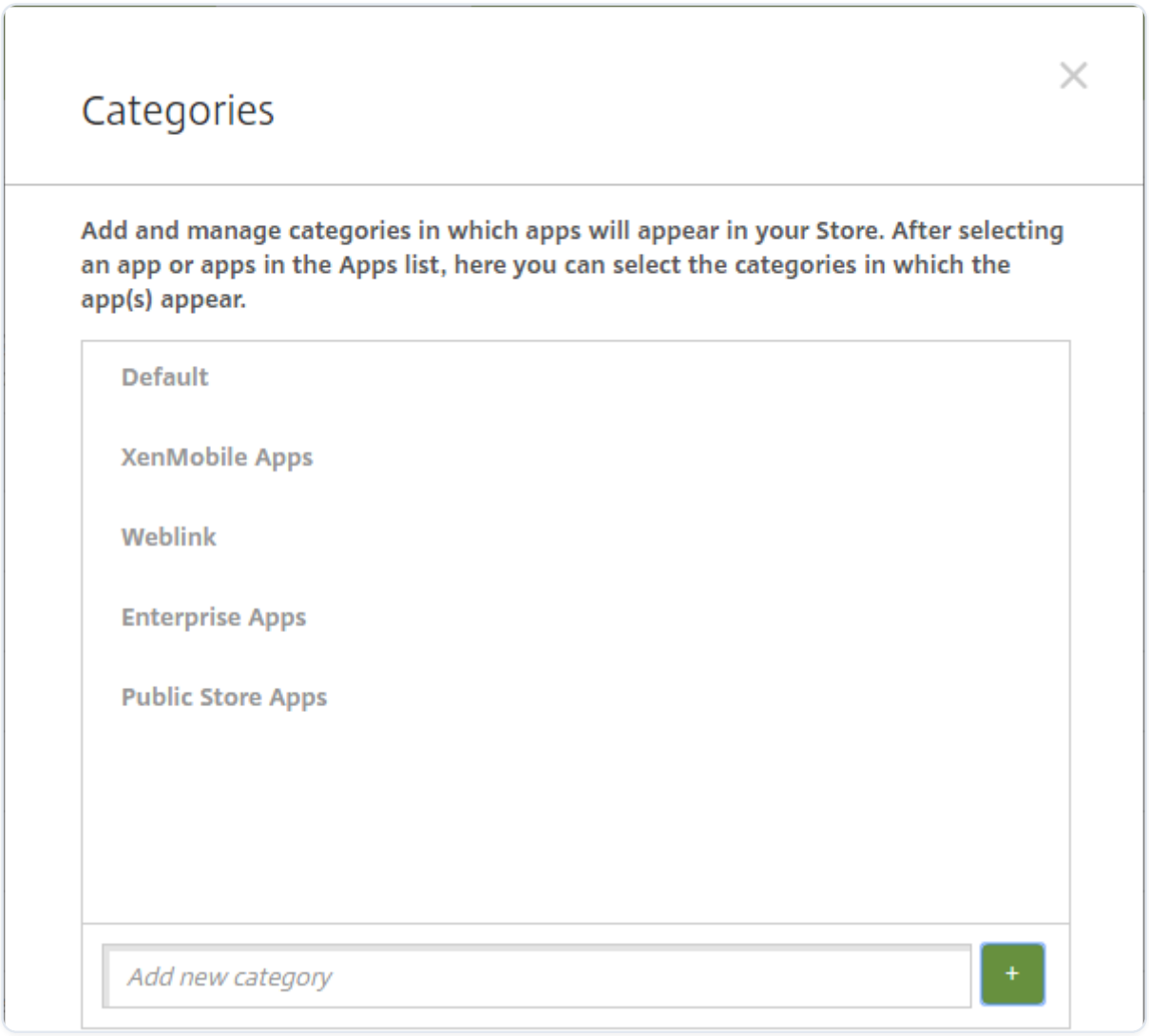
アプリ、Webリンク、またはストアを追加または編集するときに、構成済みのカテゴリの1つ以上にアプリを追加できます。

1. XenMobileコンソールで、 **> >** の順にクリックします。 ダイアログボックスが表示されます。



2. 追加するカテゴリごとに、次の操作を行います。

   - ダイアログボックスの下部にある**** 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、エンタープライズアプリのカテゴリを作成するには、「エンタープライズアプリ」と入力します。
   - プラス記号（+）をクリックしてカテゴリを追加します。新しく作成されたカテゴリが追加され、 ダイアログボックスに表示されます。



3. カテゴリの追加が完了したら、 ダイアログボックスを閉じます。
4. ページで、既存のアプリを新しいカテゴリに配置できます。

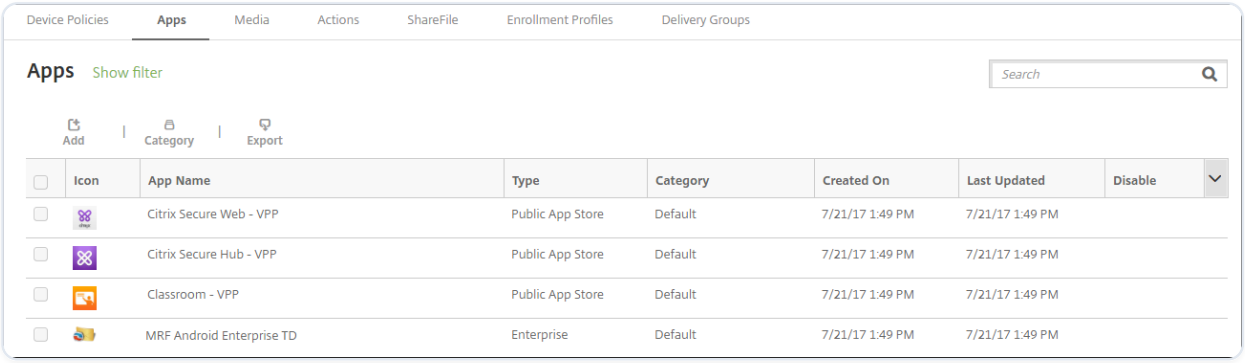
   - 分類するアプリを選択します。
   - をクリックします。 ページが表示されます。
   - リストで、カテゴリのチェックボックスをオンにして新しいカテゴリを適用します。アプリに適用したくない既存のカテゴリのチェックボックスはオフにします。
   - 「**配信グループの割り当て**」タブをクリックするか、以降の各ページで「**次へ**」をクリックして、残りのアプリセットアップページに進みます。
   - 「**配信グループの割り当て**」ページで「**保存**」をクリックして、新しいカテゴリを適用します。新しいカテゴリがアプリに適用され、「**アプリ**」テーブルに表示されます。

MDXアプリを追加する

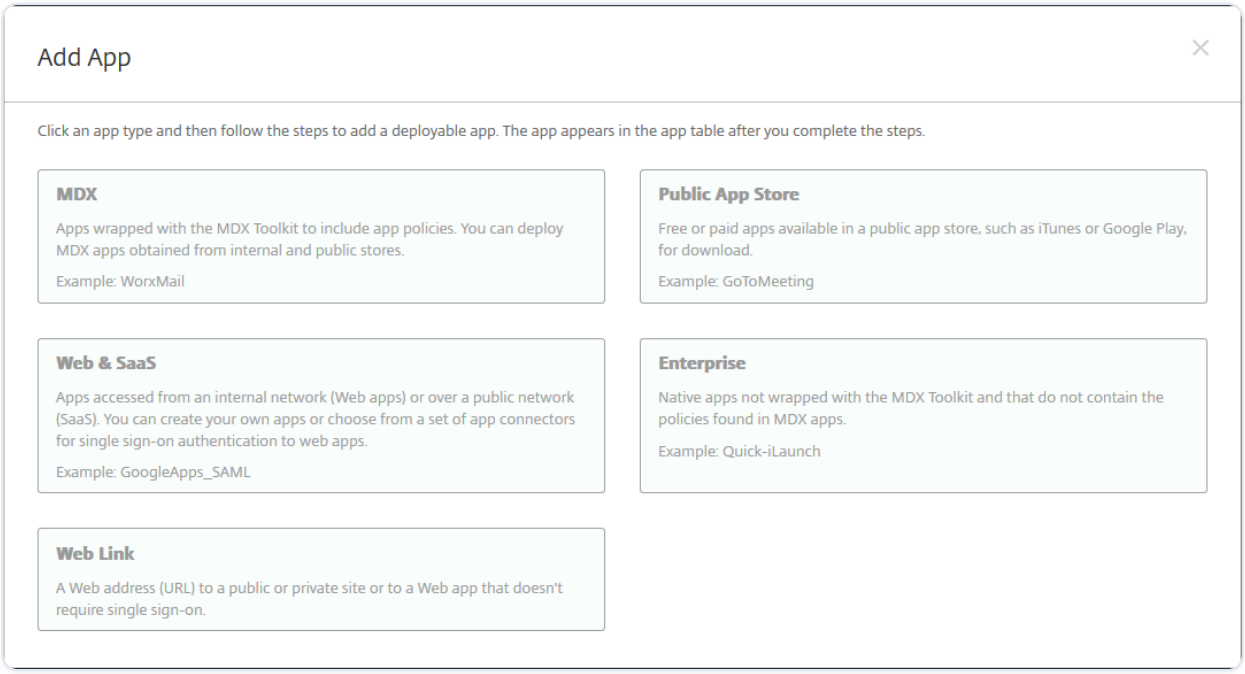
iOSまたはAndroidアプリ用のMDXファイルを受け取ったら、そのアプリをXenMobileにアップロードできます。アプリをアップロードした後、アプリの詳細とポリシー設定を構成できます。各デバイスプラットフォームタイプで利用可能なアプリポリシーについて詳しくは、以下を参照してください。

- MAM SDKの概要
- MDXポリシーの概要

1. XenMobileコンソールで、「**構成 > アプリ**」をクリックします。「**アプリ**」ページが表示されます。



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表示されます。



3. 「**MDX**」をクリックします。「**MDXアプリ情報**」ページが表示されます。
4. 「**アプリ情報**」ペインで、次の情報を入力します。

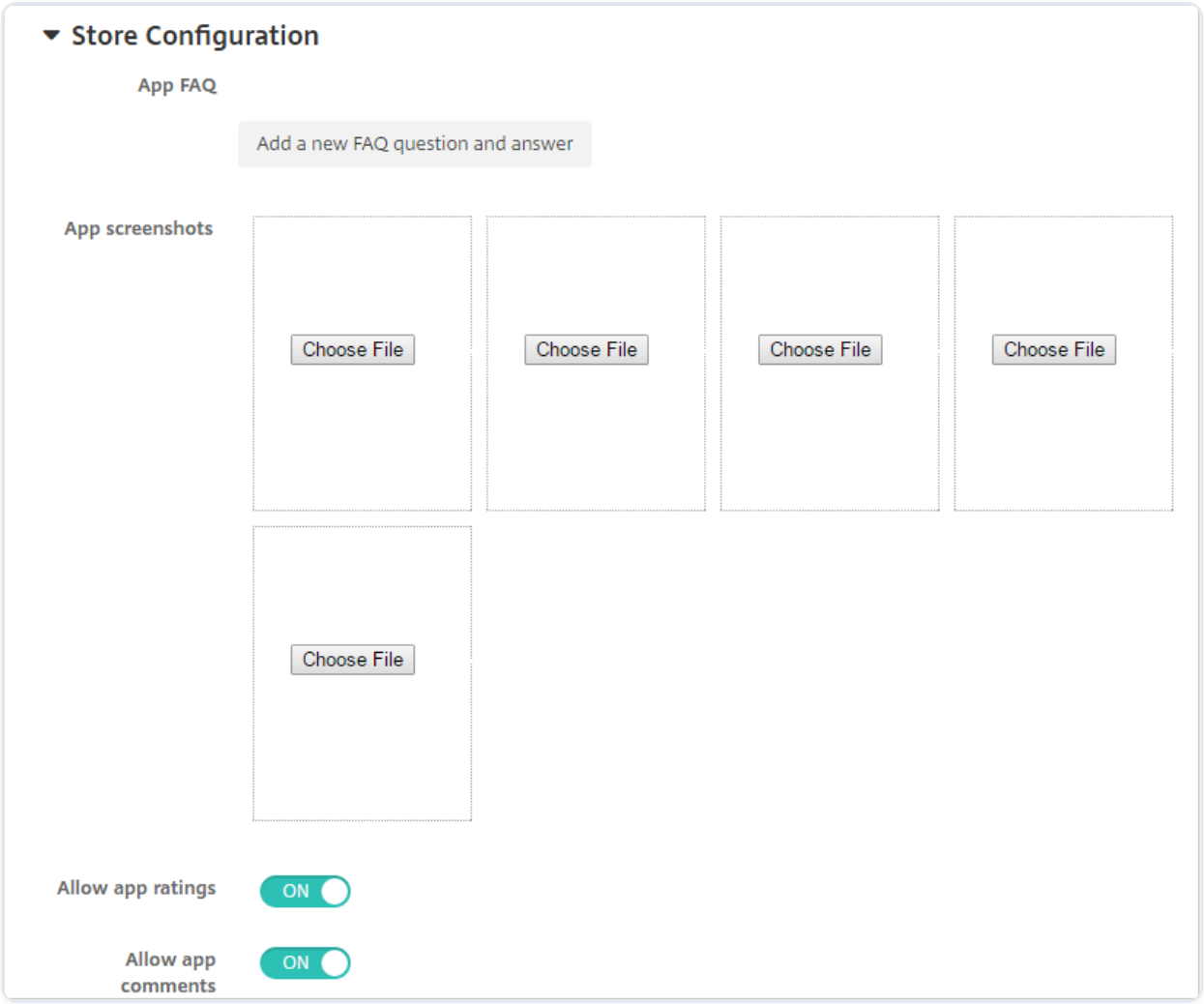
- **名前:** アプリのわかりやすい名前を入力します。この名前は、「**アプリ**」テーブルの「**アプリ名**」の下に表示されます。
- **説明:** アプリのオプションの説明を入力します。
- **アプリカテゴリ:** 必要に応じて、リストでアプリを追加するカテゴリをクリックします。アプリカテゴリについて詳しくは、「アプリカテゴリについて」を参照してください。

5. **次へ**をクリックします。**アプリプラットフォーム**ページが表示されます。
6. **プラットフォーム**で、追加するプラットフォームを選択します。1つのプラットフォームのみを構成する場合は、他のプラットフォームの選択を解除します。
7. アップロードするMDXファイルを選択するには、**アップロード**をクリックして、ファイルの場所に移動します。
8. **アプリの詳細**ページで、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:** 必要に応じて、アプリのバージョン番号を入力します。
- **パッケージID:** 管理対象のGoogle Playストアから取得した、アプリのパッケージIDを入力します。
- **最小OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
- **最大OSバージョン:** 必要に応じて、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
- **除外デバイス:** 必要に応じて、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場合にアプリを削除:** MDMプロファイルが削除されたときに、iOS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防止:** ユーザーがiOSデバイスでアプリデータをバックアップするのを防止するかどうかを選択します。デフォルトは**オン**です。
- **製品トラック:** iOSデバイスにプッシュする製品トラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトは**本番**です。
- **アプリの管理を強制:** 管理対象外としてインストールされるアプリの場合、監視対象外のiOSデバイスでアプリの管理を許可するようにユーザーにプロンプト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。

- **ボリューム購入で展開されたアプリ:** Appleボリューム購入を使用してアプリを展開するかどうかを選択します。**オン**に設定し、アプリのMDXバージョンを展開してボリューム購入を使用してアプリを展開する場合、Secure Hubはボリューム購入インスタンスのみを表示します。デフォルトは**オフ**です。

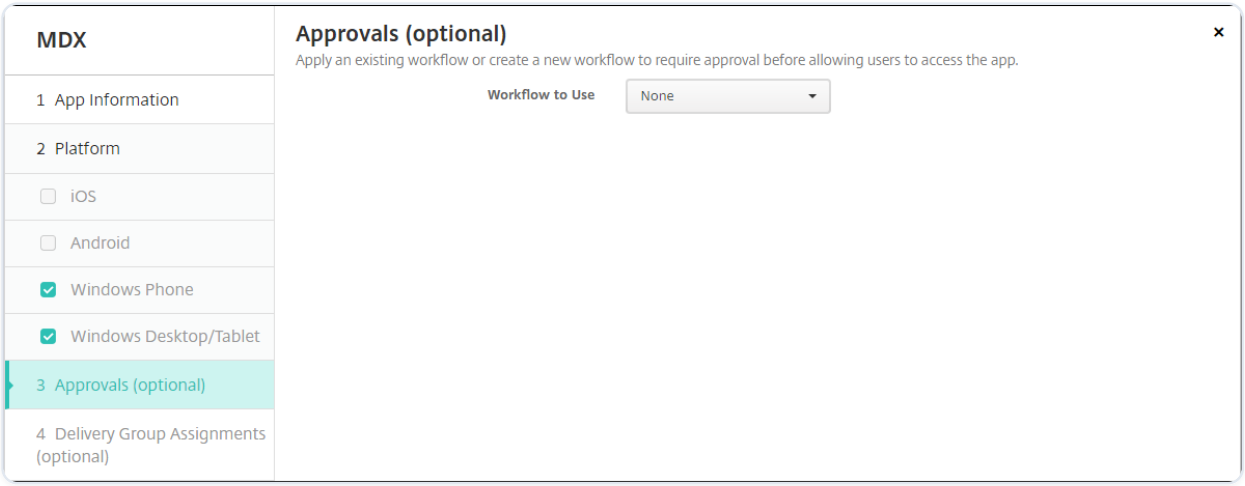
9. **MDXポリシー**を構成します。MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、アプリ制限などのポリシー領域のオプションが含まれます。コンソールでは、各ポリシーにポリシーを説明するツールチップがあります。
10. 展開ルールを構成します。詳細については、展開ルールを参照してください。
11. **ストア構成**を展開します。



- **アプリFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。

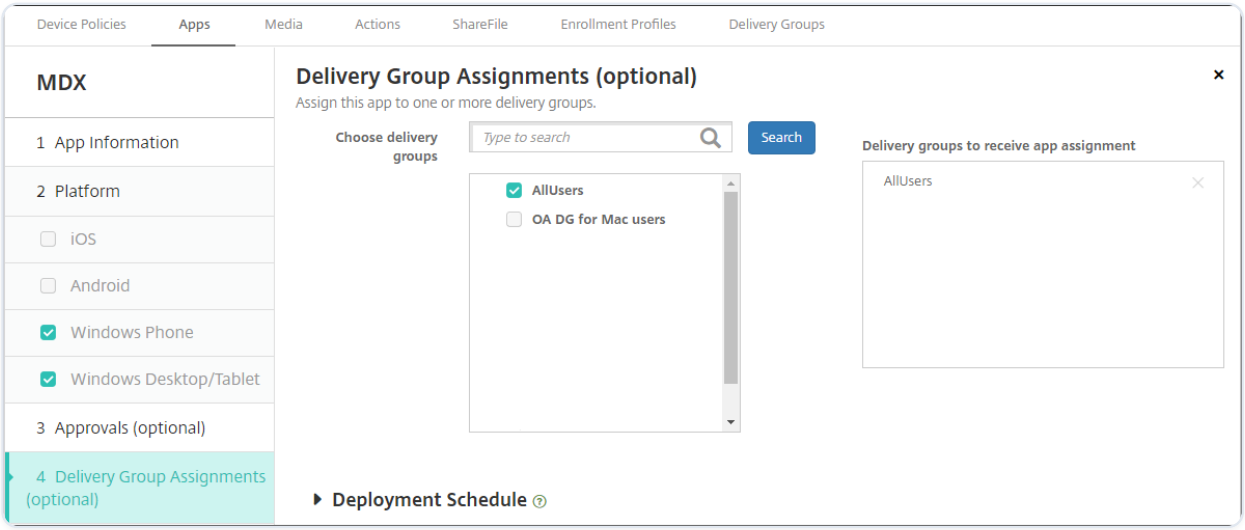
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

12. **次へ**をクリックします。**承認**ページが表示されます。



ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、ワークフローの適用を参照してください。承認ワークフローを設定しない場合は、次のステップに進みます。

13. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。



14. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリ割り当てを受け取るデリバリーグループ**リストに表示されます。
15. 「**展開スケジュール**」を展開し、次の設定を構成します:

- **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
- **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日付と時刻を構成します。デフォルトは**今すぐ**です。

- **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。以前にデバイスがアプリを受信できなかった場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

常時接続に展開オプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

構成する展開スケジュールは、すべてのプラットフォームで同じです。**常時接続に展開**を除き、加えた変更はすべてのプラットフォームに適用されます。

16. **保存**をクリックします。

パブリックアプリストアアプリを追加する

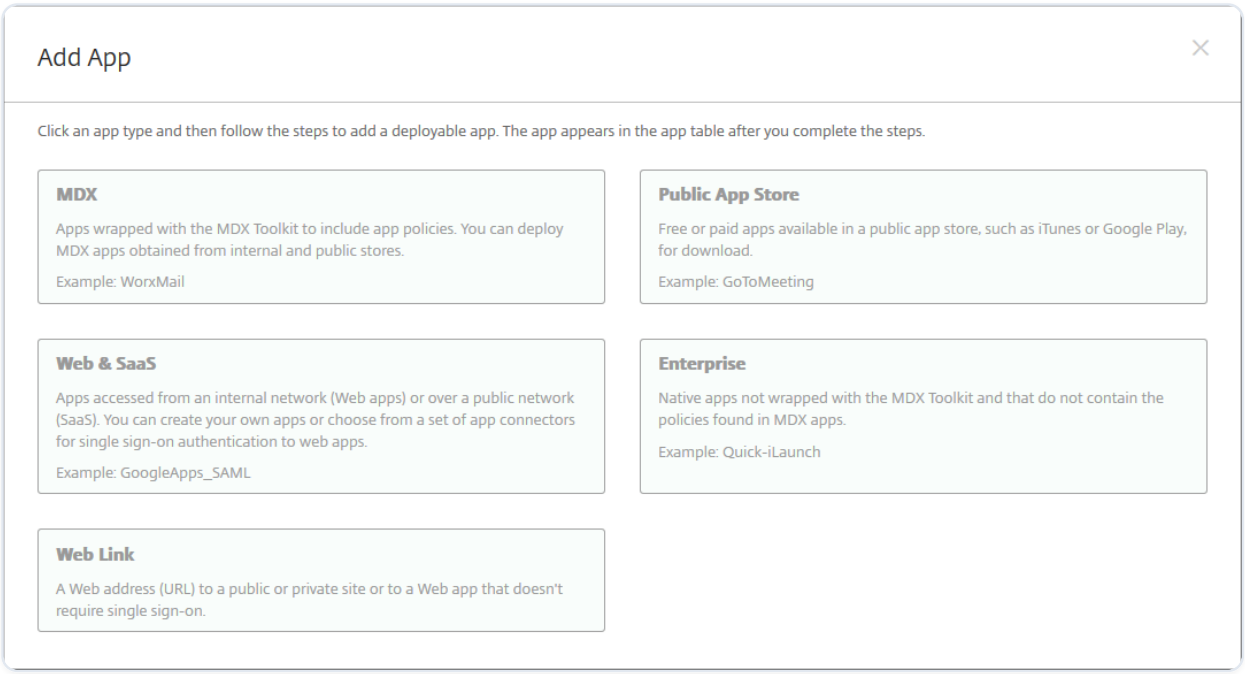
Apple App StoreやGoogle Playなどのパブリックアプリストアで入手できる無料または有料のアプリをXenMobileに追加できます。

Apple App Storeからアプリ名と説明を取得するように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は既存の名前と説明を上書きします。Google Playストアのアプリ情報は手動で構成してください。

Android Enterprise用の有料パブリックアプリストアアプリを追加すると、一括購入ライセンスのステータスを確認できます。このステータスには、利用可能なライセンスの総数、現在使用中の数、および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が含まれます。Android Enterpriseの一括購入プランは、組織向けにアプリやその他のデータを一括で検索、購入、配布するプロセスを簡素化します。

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 > 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表示されます。



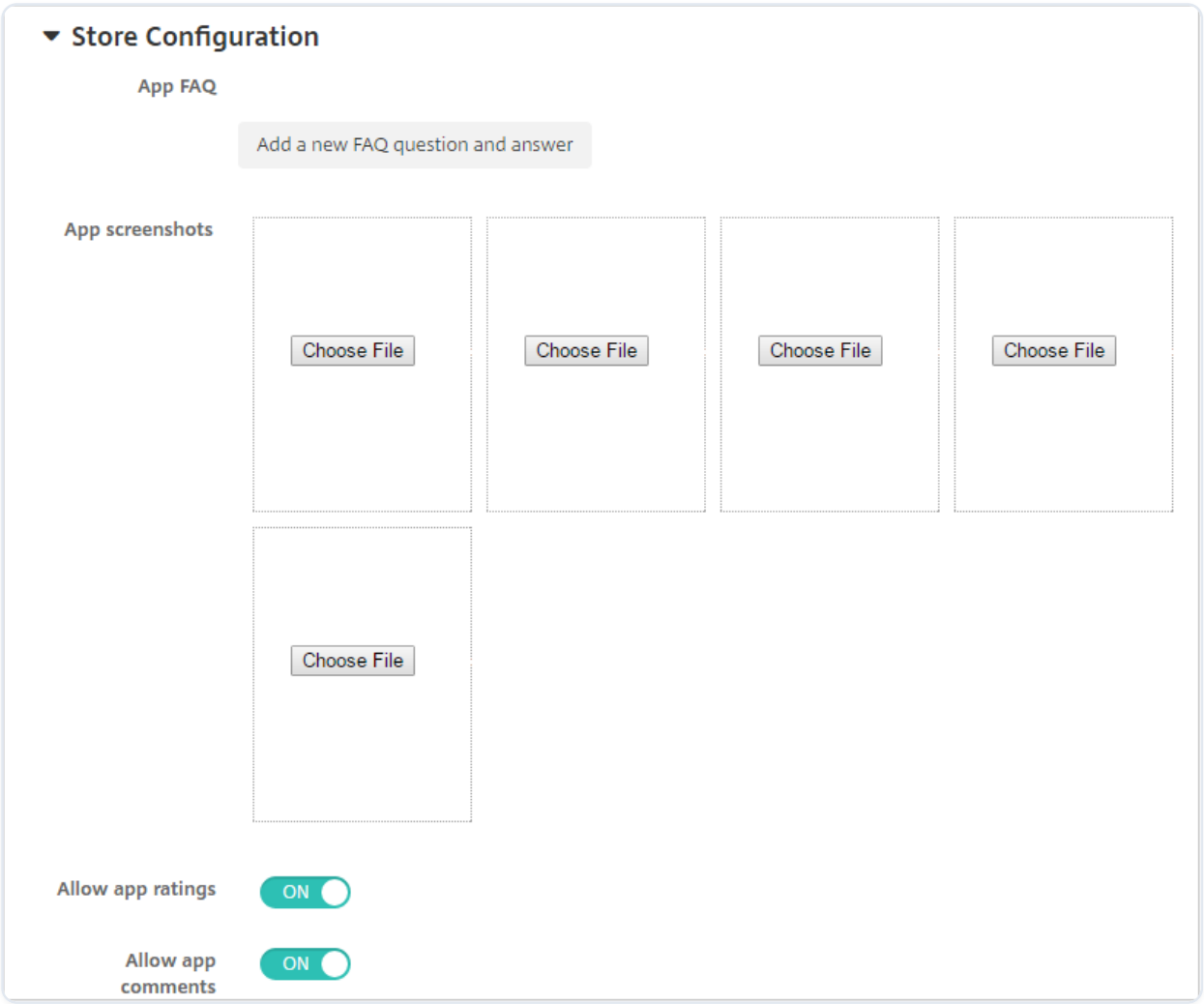
2. **パブリックアプリストア**をクリックします。**アプリ情報**ページが表示されます。
3. 「**アプリ情報**」ペインで、次の情報を入力します。
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、**アプリ**テーブルの**アプリ名**の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。
4. **次へ**をクリックします。**アプリプラットフォーム**ページが表示されます。
5. **プラットフォーム**で、追加するプラットフォームを選択します。1つのプラットフォームのみを構成する場合は、他のプラットフォームの選択を解除します。

次に、各プラットフォームのアプリ設定を構成します。参照:

- Google Playアプリのアプリ設定を構成する
- 管理対象アプリストアアプリ
- iOSアプリのアプリ設定を構成する

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アプリストア構成を設定します。

1. 展開規則を構成します。詳細については、「展開規則」を参照してください。
2. **ストア構成**を展開します。



- **アプリFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

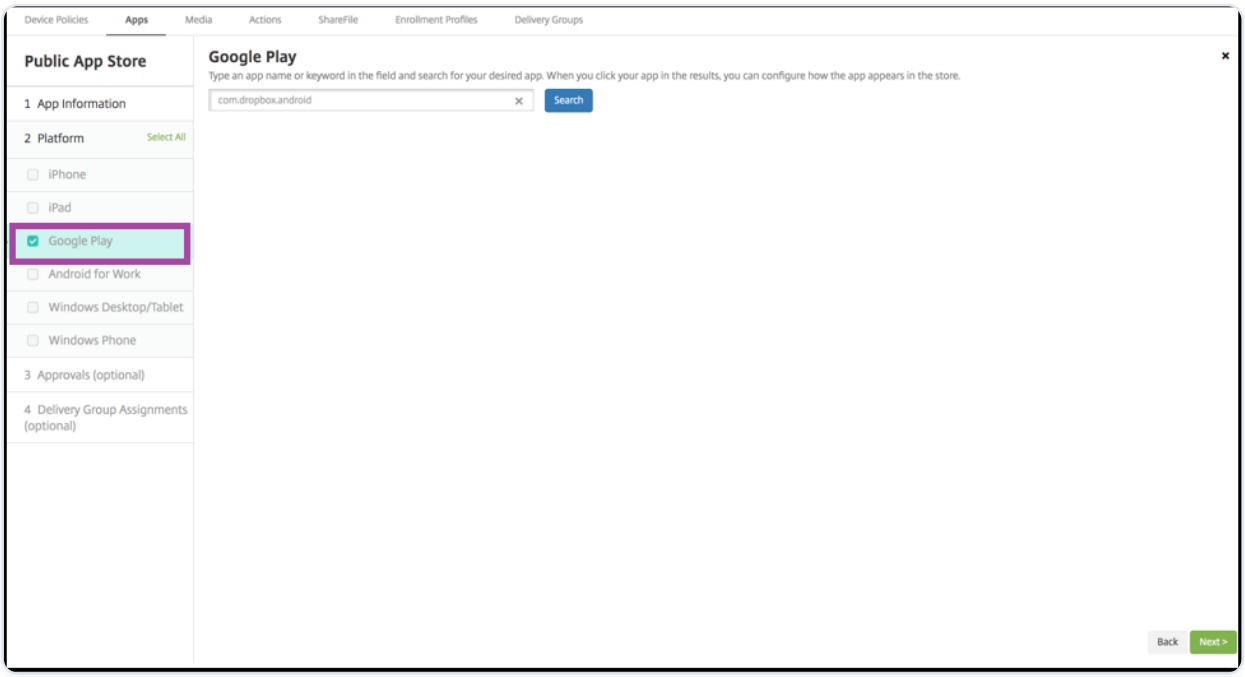
Google Playアプリのアプリ設定を構成する

> **注:**
>
> 管理対象Google PlayからGoogle Playストアのすべてのアプリにアクセスできるようにするには、XenMobile Serverのプロパティ**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ユーザーが公開Google Playストアアプリを利用できるよう

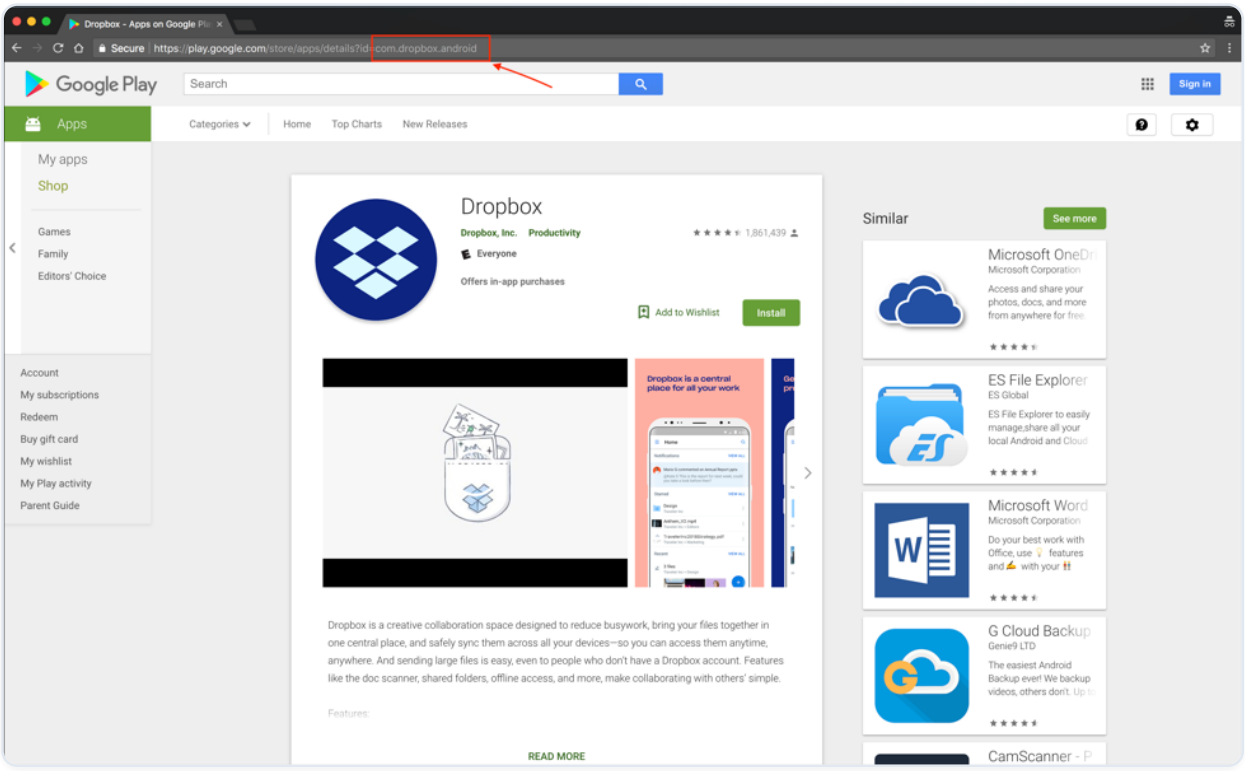
になります。その後、制限デバイスポリシーを使用して、これらのアプリへのアクセスを制御できます。

Google Playストアアプリの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ストアアプリの情報を手動で構成する必要があります。

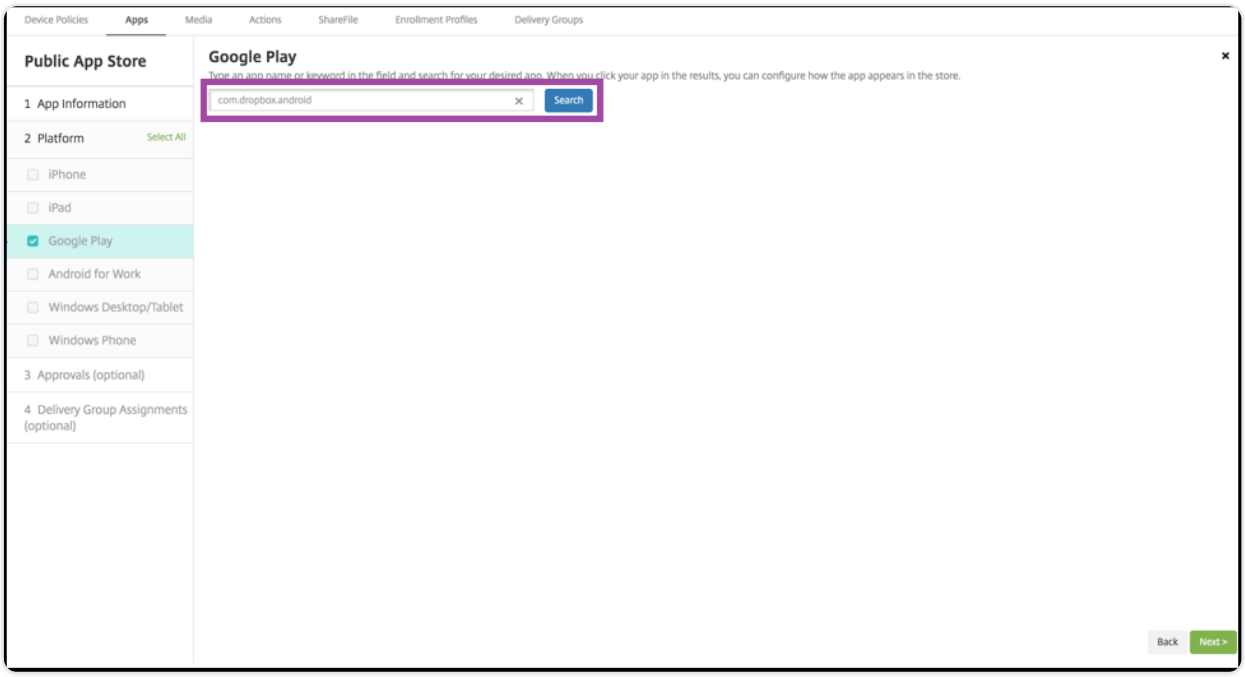
1. **プラットフォーム**で**Google Play**が選択されていることを確認します。



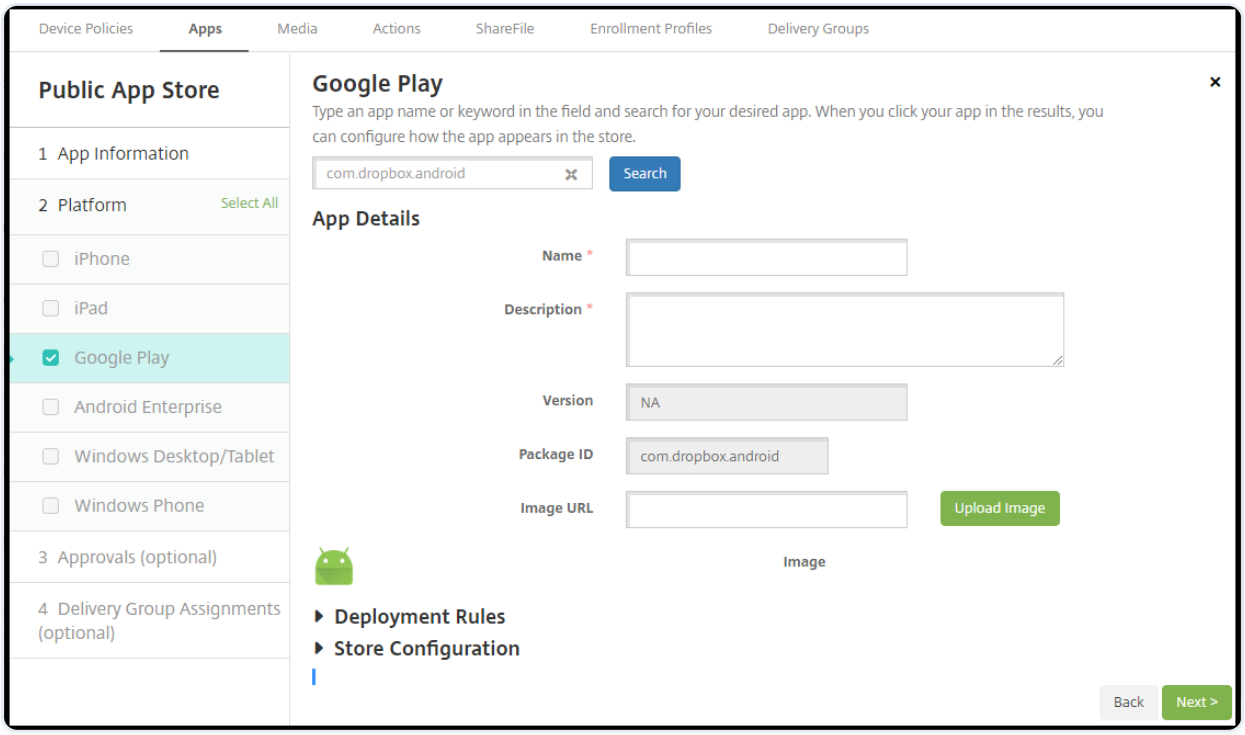
2. Google Playストアに移動します。Google Playストアからパッケージ IDをコピーします。IDはアプリのURLに記載されています。



3. XenMobile Serverコンソールでパブリックストアアプリを追加する際に、検索バーにパッケージ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、アプリの詳細を入力できるUIが表示されます。



5. ストアに表示されるアプリの画像のURLを設定できます。Google Playストアの画像を使用するには：

   a. Google Playストアにアクセスします。アプリの画像を右クリックし、画像アドレスをコピーします。

   b. 画像アドレスを**Image URL**フィールドに貼り付けます。

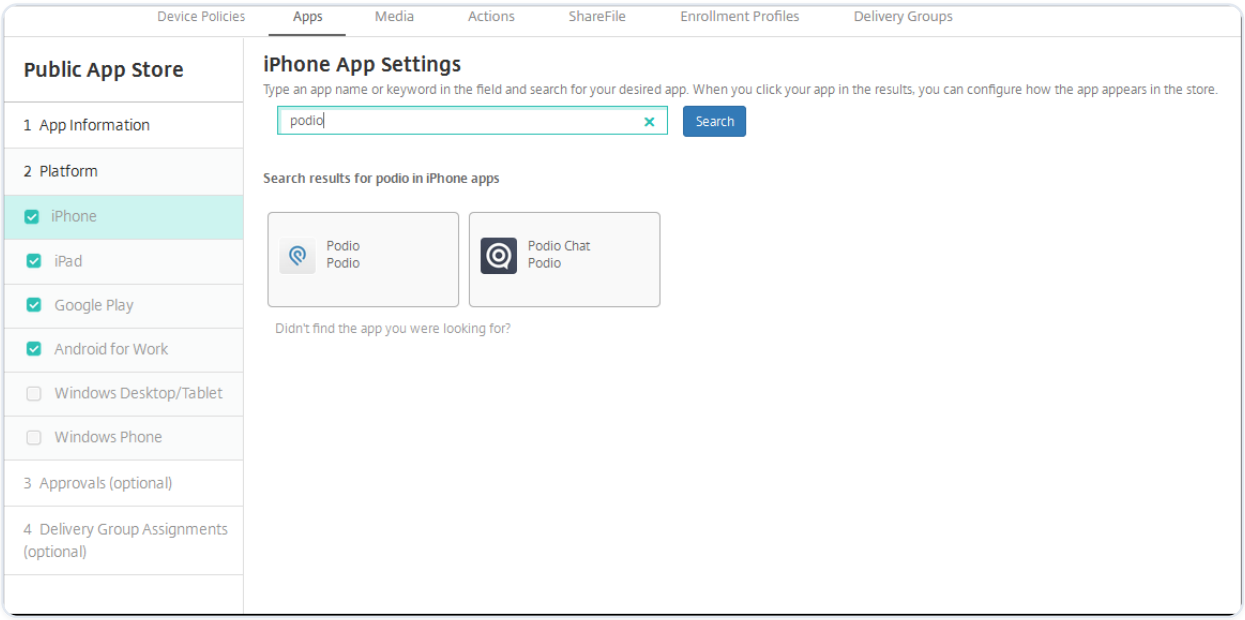
   c. **Upload image**をクリックします。画像が**Image**の横に表示されます。

画像を構成しない場合、汎用Android画像がアプリとともに表示されます。

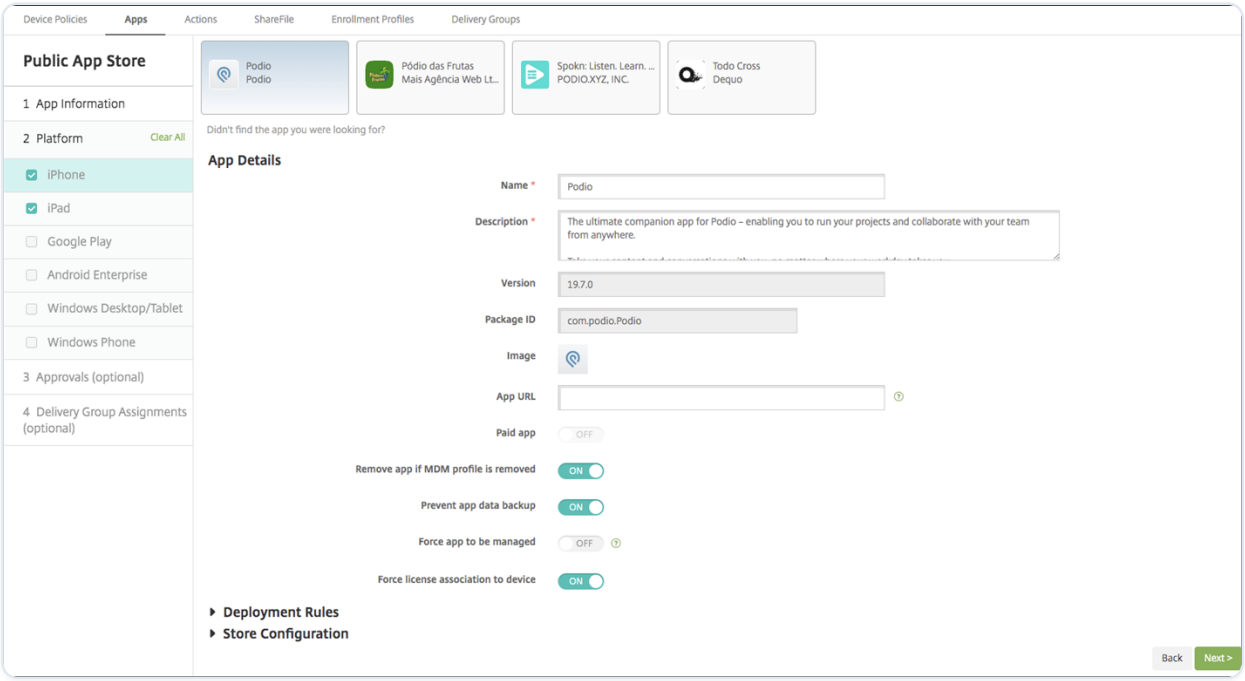
iOSアプリのアプリ設定を構成する

1. 検索ボックスにアプリ名を入力し、**Search**をクリックします。検索条件に一致するアプリが表示されます。検索条件に一致するアプリが表示されます。

   次の図は、iPhoneのアプリで**podio**を検索した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。
3. 選択したアプリに関連する情報（名前、説明、バージョン番号、関連画像など）が**App Details**フィールドに事前入力されます。

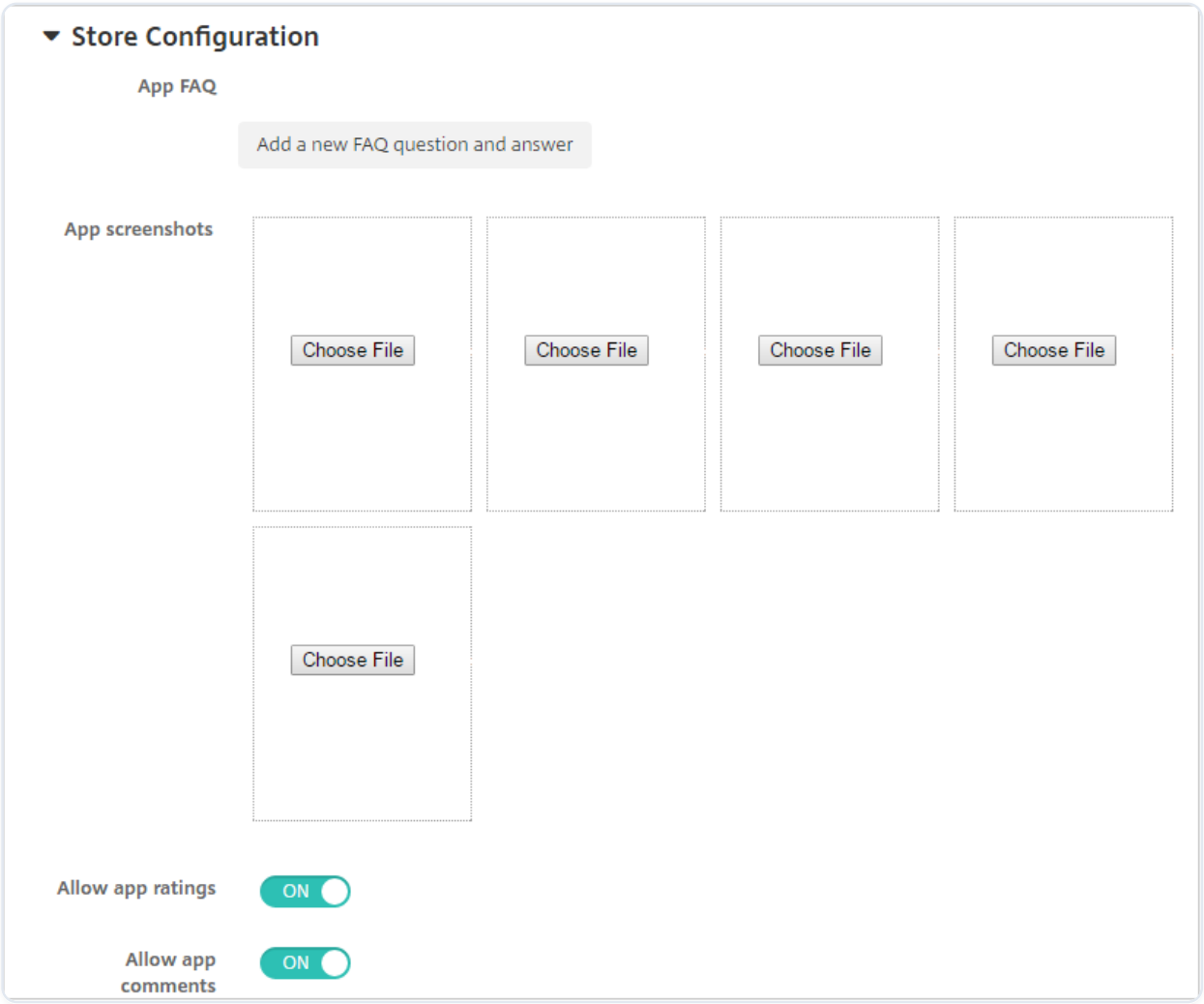


4. 設定を構成します。

- 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場合にアプリを削除する:** 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。

- **アプリのデータバックアップを防止する:** アプリがデータをバックアップするのを防ぐかどうかを選択します。デフォルトは**オン**です。
- **プロダクトトラック:** ユーザーデバイスにプッシュするプロダクトトラックを指定します。テスト用に設計されたトラックがある場合は、それを選択してユーザーに割り当てることができます。デフォルトは**Production**です。
- **アプリの管理を強制する:** アプリが管理されていない状態でインストールされたときに、監視されていないデバイスでアプリの管理を許可するようにユーザーに促すかどうかを選択します。デフォルトは**オフ**です。iOS 9.0以降で利用可能です。
- **ライセンスをデバイスに関連付けることを強制する:** デバイス関連付けが有効になっている状態で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以降で利用可能です。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。

5. 展開ルールを構成します。詳細については、「展開ルール」を参照してください。
6. **ストア構成**を展開します。



- **アプリのFAQ: 新しいFAQの質問と回答を追加**をクリックして、アプリのFAQを作成します。
- **電話/タブレットのスクリーンショットを追加する:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可する:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可する:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

7. iPhoneまたはiPadの場合は、**ボリューム購入**を展開します。

   a. XenMobileがアプリのボリューム購入ライセンスを適用できるようにするには、**ボリューム購入ライセンス**リストで**ボリューム購入ライセンスをアップロード**をクリックします。

   b. 表示されるダイアログボックスで、ライセンスをインポートします。

      「ライセンス割り当て」テーブルには、利用可能なライセンスの総数のうち、アプリで使用されているライセンスの数が表示されます。

      個々のユーザーのボリューム購入ライセンスの関連付けを解除できます。これにより、ライセンス割り当てが終了し、ライセンスが解放されます。

8. Android Enterprise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」テーブルには、利用可能なライセンスの総数のうち、アプリで使用されているライセンスの数が表示されます。

   ユーザーを選択し、**関連付けを解除**をクリックすると、そのユーザーのライセンス割り当てが終了し、別のユーザーのためにライセンスが解放されます。ただし、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のみ、ライセンスの関連付けを解除できます。

   アプリ構成画面(/en-us/xenmobile/server/media/afw-bulk-purchase-license.png)

9. **ボリューム購入**または**一括購入**の設定が完了したら、**次へ**をクリックします。**承認**ページが表示されます。

   ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、「ワークフローの適用」を参照してください。承認ワークフローが必要ない場合は、次の手順に進みます。

10. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。

11. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
12. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日付と時刻を構成します。デフォルトは**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。デバイスが以前にアプリの受信に失敗した場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

    常時接続の展開は、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

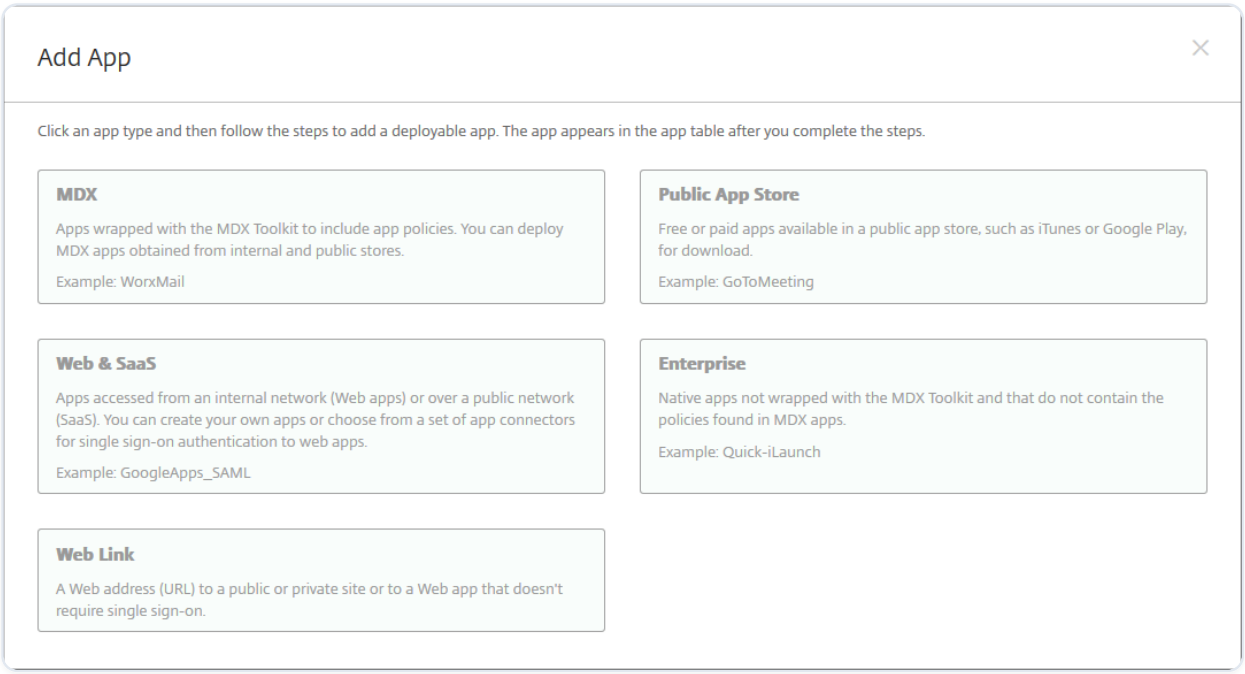
    構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、**Deploy for always-on connection** を除き、すべてのプラットフォームに適用されます。
13. **保存** をクリックします。

WebアプリまたはSaaSアプリを追加する

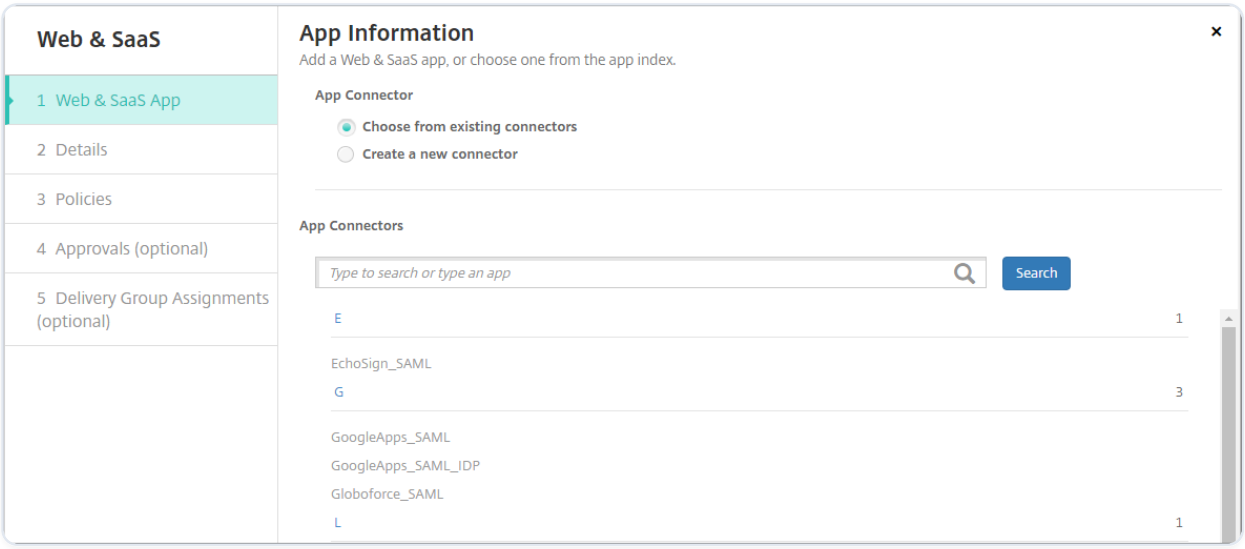
XenMobileコンソールを使用して、モバイル、エンタープライズ、Web、およびSaaSアプリへのシングルサインオン (SSO) 認証をユーザーに付与できます。アプリケーションコネクタテンプレートを使用して、SSO用にアプリを有効にできます。XenMobileで利用可能なコネクタの種類の一覧については、「アプリケーションコネクタの種類」を参照してください。WebアプリまたはSaaSアプリを追加する際に、XenMobileで独自のコネクタを構築することもできます。

アプリがSSOでのみ利用可能な場合: 設定を保存すると、アプリは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 > 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表示されます。



2. **Web & SaaS** をクリックします。**アプリ情報** ページが表示されます。



3. 既存または新規のアプリコネクタを次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** ページで、前述のように **既存のコネクタから選択** がすでに選択されています。**アプリコネクタ** リストで、使用するコネクタをクリックします。アプリコネクタ情報が表示されます。
2. 次の設定を構成します。

   - **アプリ名:** 事前入力された名前を受け入れるか、新しい名前を入力します。
   - **アプリの説明:** 事前入力された説明を受け入れるか、独自の説明を入力します。

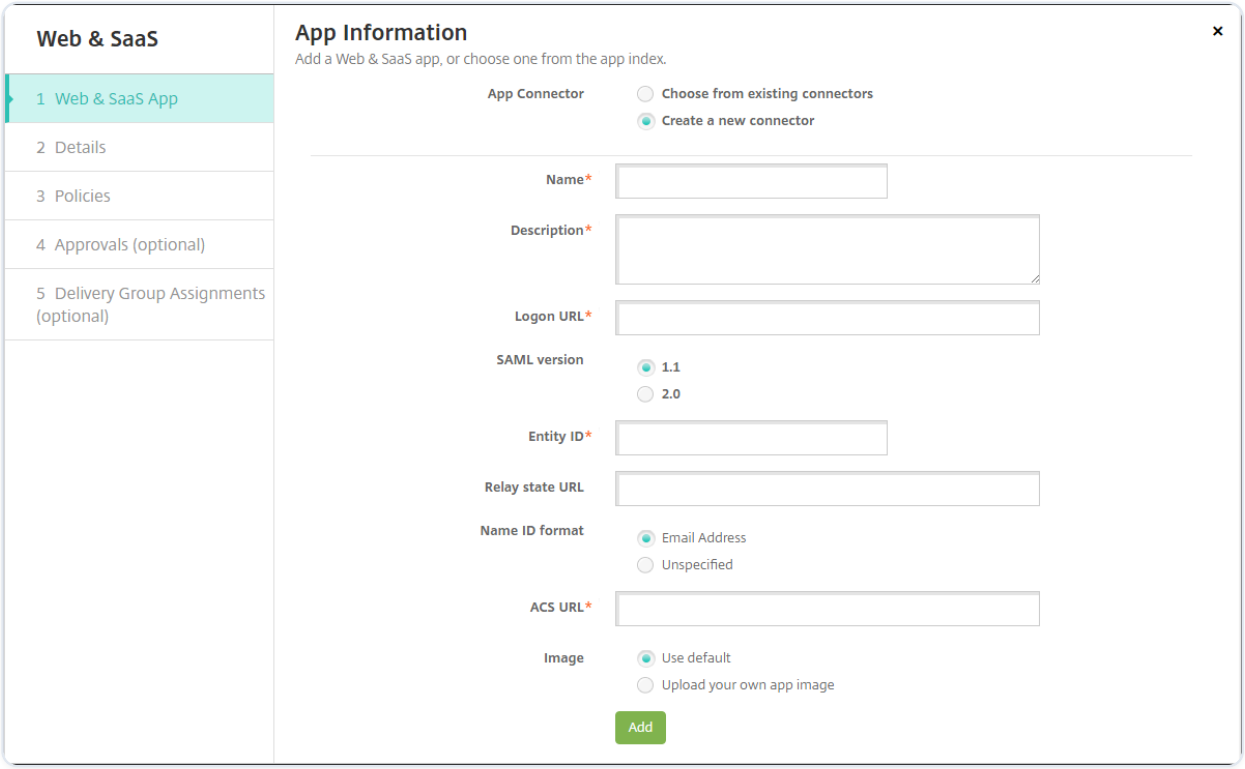
- **URL:** 事前に入力されたURLを受け入れるか、アプリのWebアドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれている場合があり、次のページに進む前にそれを置き換える必要があります。
- **ドメイン名:** 該当する場合は、アプリのドメイン名を入力します。このフィールドは必須です。
- **アプリは内部ネットワークでホストされています:** アプリが内部ネットワーク内のサーバーで実行されているかどうかを選択します。ユーザーがリモートの場所から内部アプリに接続する場合、Citrix Gatewayを介して接続する必要があります。このオプションを**ON**に設定すると、アプリにVPNキーワードが追加され、ユーザーはCitrix Gatewayを介して接続できるようになります。デフォルトは**OFF**です。
- **アプリカテゴリ:** リストから、アプリに適用するオプションのカテゴリをクリックします。
- **ユーザーアカウントプロビジョニング:** 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。Globoforce_SAMLコネクタを使用する場合は、シームレスなSSO統合を確実にするために、このオプションを有効にする必要があります。
- **ユーザーアカウントプロビジョニング**を有効にする場合は、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**
    - **ユーザーエンタイトルメントの終了時:** リストから、ユーザーがアプリへのアクセスを許可されなくなったときに実行するアクションをクリックします。デフォルトは**アカウントを無効にする**です。
  - **ユーザー名ルール**
    - 追加するユーザー名ルールごとに、次の操作を行います。
      - **ユーザー属性:** リストから、ルールに追加するユーザー属性をクリックします。
      - **長さ（文字数）:** リストから、ユーザー名ルールで使用するユーザー属性の文字数をクリックします。デフォルトは**すべて**です。
      - **ルール:** 追加する各ユーザー属性は、ユーザー名ルール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長を入力します。デフォルトは**8**です。

- **パスワードの有効期限**
  - **有効期間 (日数):** パスワードが有効な日数を入力します。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する:** パスワードの有効期限が切れたときに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**OFF**です。このフィールドを有効にしない場合、ユーザーはパスワードの有効期限が切れた後にアプリを開くことができません。

新しいアプリコネクタを構成するには

1. In the **App Information**ページで、**Create a new connector**を選択します。アプリコネクタ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URLを入力または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ブラウザを開き、そのアプリのログオンページに移動します。たとえば、`https://www.example.com/logon`のようになる場合があります。このフィールドは必須です。

- **SAMLバージョン: 1.1**または**2.0**のいずれかを選択します。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アプリケーションのWebアドレスを入力します。リレー状態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**のいずれかを選択します。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を入力します。ACS URLは、ユーザーにSSO機能を提供します。
- **画像:** デフォルトのCitrix画像を使用するか、独自のアプリ画像をアップロードするかを選択します。デフォルトは「デフォルトを使用」です。
    - 独自の画像をアップロードするには、**参照**をクリックしてファイルの場所に移動します。ファイルは.PNGファイルである必要があります。JPEGまたは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すると、後で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**ページが表示されます。
4. **次へ**をクリックします。**アプリポリシー**ページが表示されます。

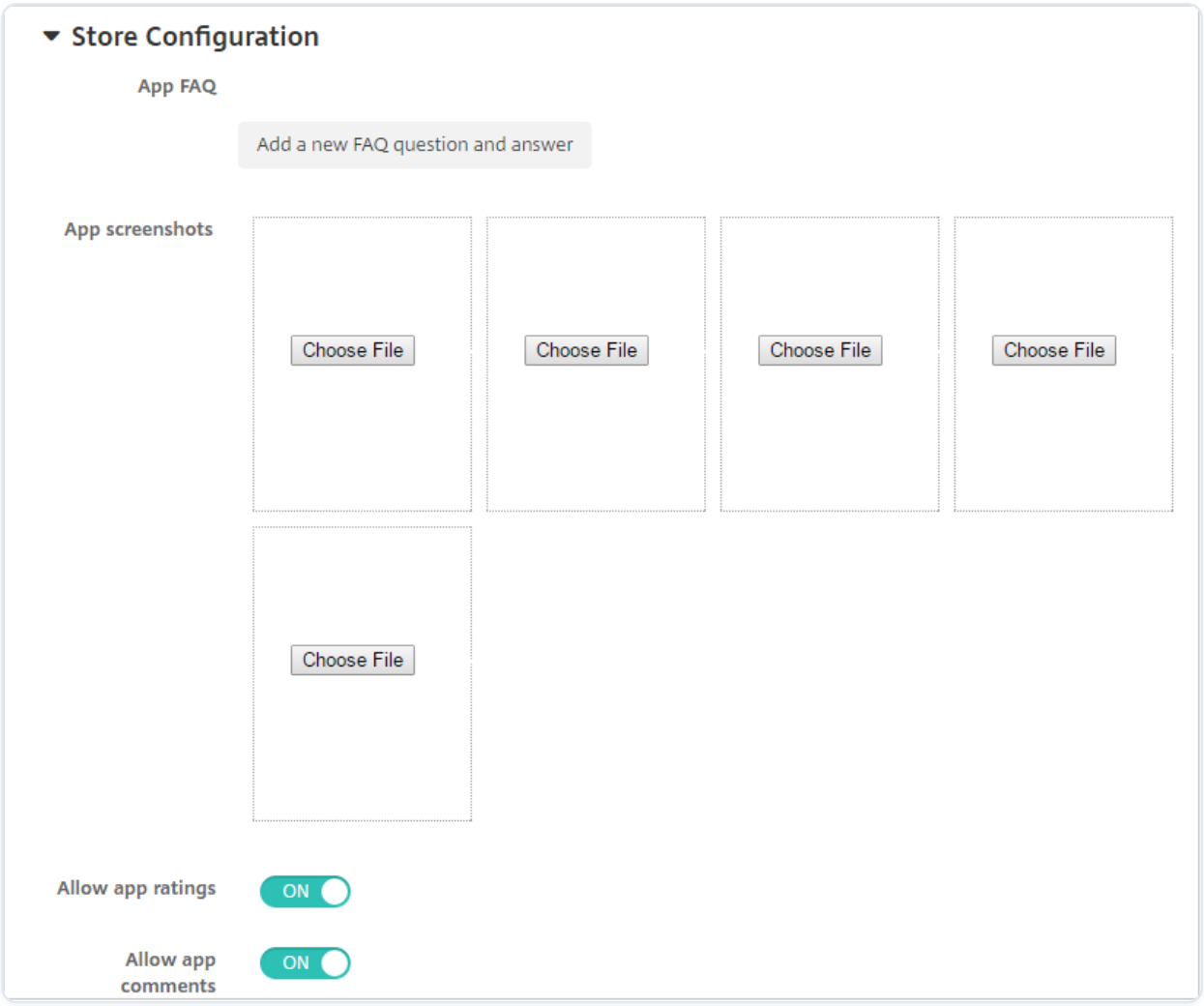
   アプリ構成画面のスクリーンショットです。(/en-us/xenmobile/server/media/configure-apps-web-saas-add-policies.png)

5. 次の設定を構成します:

   - **デバイスセキュリティ**
   - **ジェイルブレイクまたはルート化されたデバイスをブロック:** ジェイルブレイクまたはルート化されたデバイスがアプリにアクセスするのをブロックするかどうかを選択します。デフォルトは**ON**です。
   - **ネットワーク要件**
   - **Wi-Fi必須:** アプリを実行するためにWi-Fi接続が必要かどうかを選択します。デフォルトは**OFF**です。
   - **内部ネットワーク必須:** アプリを実行するために内部ネットワークが必要かどうかを選択します。デフォルトは**OFF**です。
   - **内部Wi-Fiネットワーク: Wi-Fi必須**を有効にした場合、使用する内部Wi-Fiネットワークを入力します。

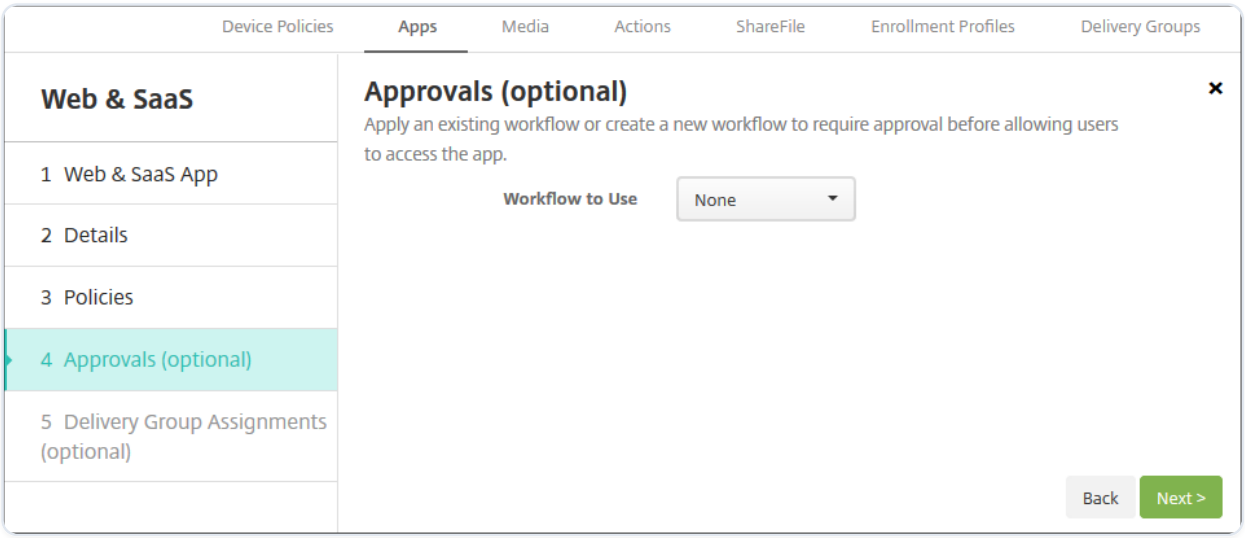
6. 展開ルールを設定します。詳細については、展開ルールを参照してください。

7. **Store Configuration**を展開します。



- **アプリFAQ:** アプリのFAQを作成するには、**新しいFAQの質問と回答を追加**をクリックします。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

8. **次へ**をクリックします。**承認**ページが表示されます。



ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、ワークフローの適用を参照してください。

9. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。
10. **デリバリーグループの選択**の横で、デリバリーグループを検索するためにタイプするか、1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
11. **展開スケジュール**を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日時を構成します。デフォルトは**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。デバイスが以前にアプリを受信できなかった場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

    常時接続展開は、**設定 > サーバープロパティ**でスケジュールされたバックグラウンド展開キーを構成している場合に適用されます。

    構成する展開スケジュールは、すべてのプラットフォームで同じです。加えた変更はすべてプラットフォームに適用されますが、**常時接続展開**は例外です。
12. **保存**をクリックします。

エンタープライズアプリを追加する

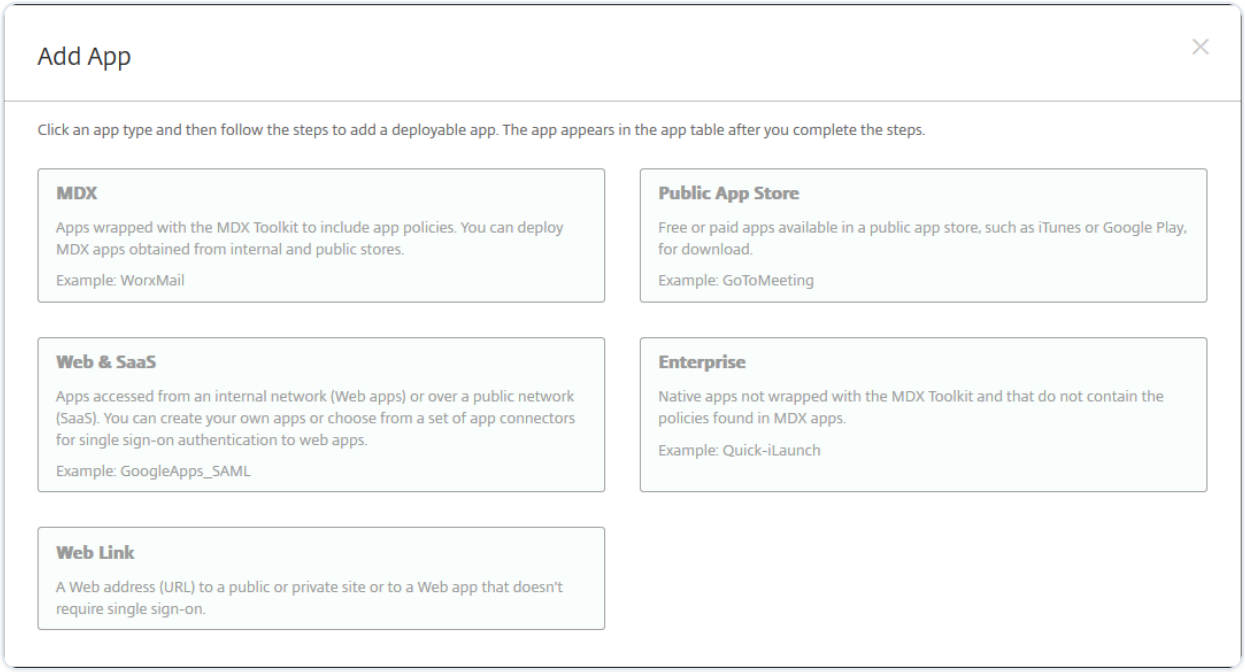
XenMobileのエンタープライズアプリは、MAM SDKまたはMDX Toolkitで準備されていないネイティブアプリを表します。これらのアプリには、MDXアプリに関連付けられたポリシーは含まれていません。XenMobileコンソールの**アプリ**タブでエンタープライズアプリをアップロードできま

す。エンタープライズアプリは、次のプラットフォーム（および対応するファイルタイプ）をサポートしています。

- 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)
- 参照: MDX対応プライベートアプリ

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、Google Playストアのアプリをパブリックアプリストアアプリとして追加してください。パブリックアプリストアアプリを追加するを参照してください。

1. XenMobileコンソールで、**構成 > アプリ > 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表示されます。

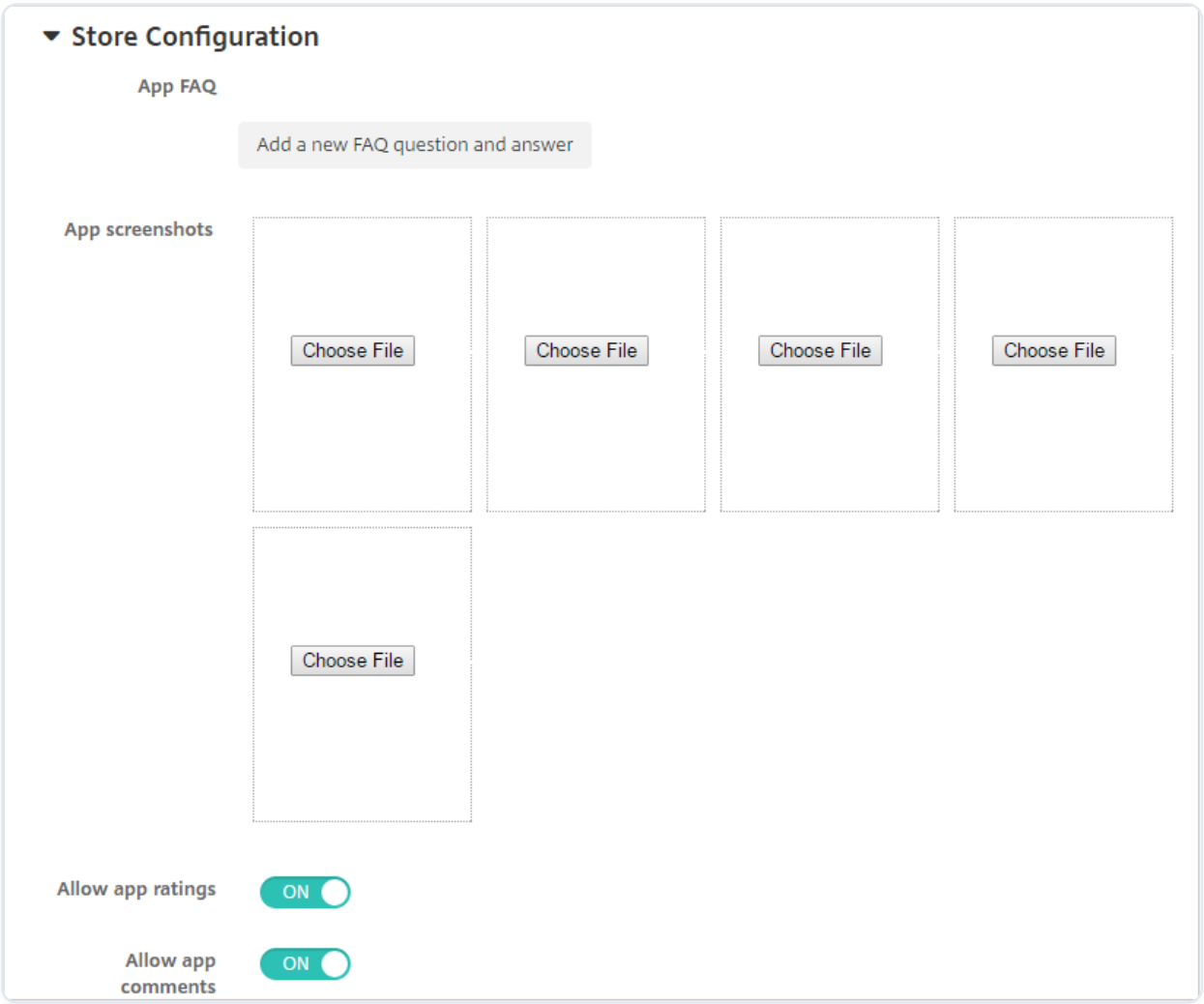


2. **エンタープライズ**をクリックします。**アプリ情報**ページが表示されます。
3. 「**アプリ情報**」ペインで、次の情報を入力します。
   - **名前:** アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの「アプリ名」の下に表示されます。
   - **説明:** アプリのオプションの説明を入力します。
   - **アプリカテゴリ:** オプションで、リストからアプリを追加するカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

4. **次へ**をクリックします。「**アプリプラットフォーム**」ページが表示されます。
5. **プラットフォーム**で、追加するプラットフォームを選択します。1つのプラットフォームのみを構成する場合は、他のプラットフォームの選択を解除します。
6. 選択した各プラットフォームについて、**アップロード**をクリックしてファイルの場所に移動し、アップロードするファイルを選択します。
7. **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表示されます。
8. プラットフォームの種類の設定を構成します。例:

    - **ファイル名:** オプションで、アプリの新しい名前を入力します。
    - **アプリの説明:** オプションで、アプリの新しい説明を入力します。
    - **アプリバージョン:** このフィールドは変更できません。
    - **最小OSバージョン:** オプションで、デバイスがアプリを使用するために実行できる最も古いオペレーティングシステムバージョンを入力します。
    - **最大OSバージョン:** オプションで、デバイスがアプリを使用するために実行する必要がある最新のオペレーティングシステムを入力します。
    - **除外デバイス:** オプションで、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。
    - **パッケージID:** アプリの一意の識別子。
    - **MDMプロファイルが削除された場合にアプリを削除:** MDMプロファイルが削除されたとき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。
    - **アプリのデータバックアップを防止:** アプリがデータをバックアップするのを防止するかどうかを選択します。デフォルトは**オン**です。
    - **アプリの管理を強制:** 管理されていないアプリをインストールする場合、監視されていない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プロンプトを表示するには、**オン**を選択します。ユーザーがプロンプトを承諾すると、アプリは管理されます。

9. 展開ルールを構成します。詳しくは、「展開ルール」を参照してください。
10. **ストア構成**を展開します。



- **アプリFAQ:** アプリのFAQを作成するには、**新しいFAQの質問と回答を追加**をクリックします。
- **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
- **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
- **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

11. **次へ**をクリックします。**承認**ページが表示されます。

    ユーザーがアプリにアクセスする前に承認を要求するワークフローを使用するには、「ワークフローの適用」を参照してください。承認ワークフローが不要な場合は、次の手順に進みます。

12. **次へ**をクリックします。**デリバリーグループの割り当て**ページが表示されます。

13. **デリバリーグループの選択**の横に、デリバリーグループを検索するための文字を入力するか、リストから1つまたは複数のグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
14. 「**展開スケジュール**」を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは**オン**です。
    - **展開スケジュール:** アプリを**今すぐ**展開するか、**後で**展開するかを選択します。**後で**を選択した場合は、アプリを展開する日時を構成します。デフォルトは**今すぐ**です。
    - **展開条件:** デバイスが接続するたびにアプリを展開するには、**接続ごとに**を選択します。デバイスが以前にアプリの受信に失敗した場合にアプリを展開するには、**以前の展開が失敗した場合のみ**を選択します。デフォルトは**接続ごとに**です。

    常時接続の展開は、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

    構成する展開スケジュールは、すべてのプラットフォームで同じです。**常時接続の展開**を除き、行った変更はすべてのプラットフォームに適用されます。
15. **保存**をクリックします。

Webリンクを追加する

Webリンクとは、インターネットまたはイントラネットサイトへのWebアドレスです。Webリンクは、SSOを必要としないWebアプリケーションを指すこともできます。Webリンクの構成が完了すると、そのリンクはアプリストアにアイコンとして表示されます。ユーザーがSecure Hubでログオンすると、そのリンクは利用可能なアプリとデスクトップのリストとともに表示されます。

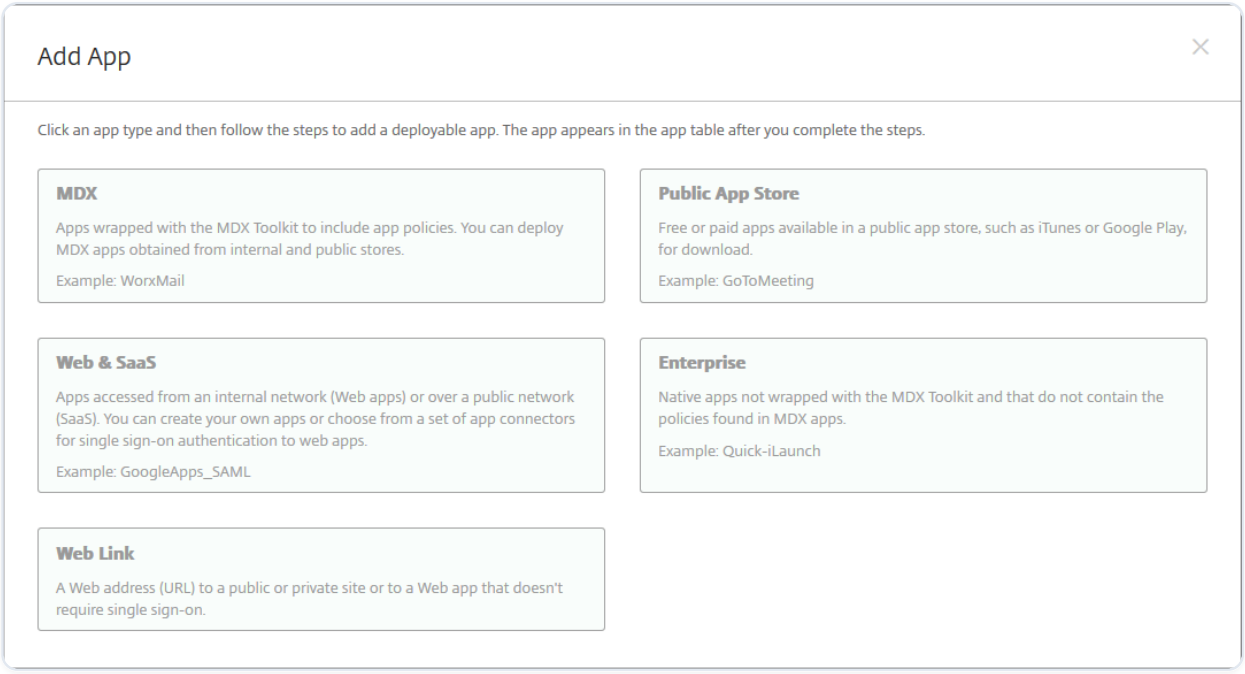
XenMobileコンソールの**アプリ**タブからWebリンクを構成できます。Webリンクの構成が完了すると、そのリンクは**アプリ**テーブルのリストにリンクアイコンとして表示されます。ユーザーがSecure Hubでログオンすると、そのリンクは利用可能なアプリとデスクトップのリストとともに表示されます。

リンクを追加するには、次の情報を提供します。

- 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、**Configure > Apps > Add** をクリックします。**Add App** ダイアログボックスが表示されます。

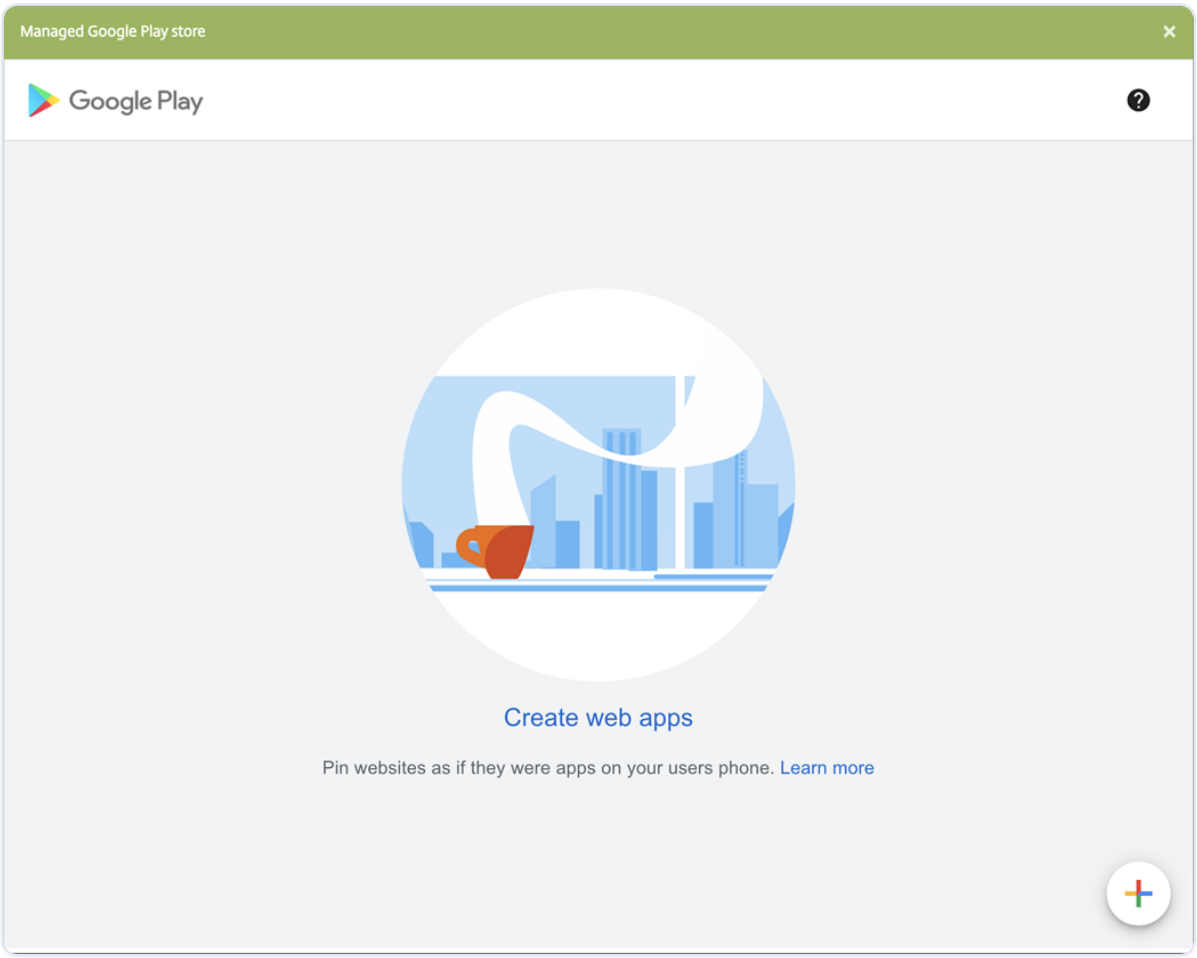


2. **Web Link** をクリックします。**App Information** ページが表示されます。
3. **App Information** ペインで、次の情報を入力します。

   名前: アプリのわかりやすい名前を入力します。この名前は、アプリテーブルの の下に表示されます。 **説明:** アプリのオプションの説明を入力します。 **アプリカテゴリ:** オプションで、リストからアプリを追加したいカテゴリをクリックします。アプリカテゴリの詳細については、「アプリカテゴリについて」を参照してください。

4. **Next** をクリックします。**App Platforms** ページが表示されます。
5. **Platforms** で、iOSおよびAndroid (レガシーDA) 用のWebアプリを追加するには **Other platforms** を選択するか、**Android Enterprise** を選択します。追加したくないチェックボックスはオフにします。

   - **Other platforms** を選択した場合は、次の手順に進んで設定を構成します。
   - **Android Enterprise** を選択した場合は、**Upload** ボタンをクリックして管理対象のGoogle Playストアを開きます。Webアプリを公開するために開発者アカウントを登録する必要はありません。続行するには、右下隅にある **Plus** アイコンをクリックします。



これらの設定を構成します:

- **タイトル:** Webアプリの名前を入力します。
- **URL:** アプリのWebアドレスを入力します。
- **表示:** ユーザーデバイスにWebアプリを表示する方法を選択します。利用可能なオプションは、**全画面表示**、**スタンドアロン**、**最小限のUI**です。
- **アイコン:** Webアプリを表す独自の画像をアップロードします。

Webアプリ構成画面(/en-us/xenmobile/server/media/create-new-web-app.png)

完了したら、**作成**をクリックします。Webアプリが公開されるまでに最大10分かかる場合があります。

6. Android Enterprise以外のプラットフォームでは、以下の設定を構成します。

- **アプリ名:** 事前に入力された名前を受け入れるか、新しい名前を入力します。
- **アプリの説明:** 事前に入力された説明を受け入れるか、独自のものを入力します。
- **URL:** 事前に入力されたURLを受け入れるか、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ている場合があり、次のページに進む前にそれを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ています:** アプリが内部ネットワーク内のサーバーで実行されているかどうかを選択します。ユーザーがリモートロケーションから内部アプリに接続する場合、Citrix Gatewayを介して接続する必要があります。このオプションを**ON**に設定すると、アプリにVPNキーワードが追加され、ユーザーはCitrix Gatewayを介して接続できるようになります。デフォルトは**OFF**です。
- **アプリカテゴリ:** リストで、アプリに適用するオプションのカテゴリをクリックします。
- **画像:** デフォルトのCitrix画像を使用するか、独自のアプリ画像をアップロードするかを選択します。デフォルトは「デフォルトを使用」です。
    - 独自の画像をアップロードするには、**参照**をクリックしてファイルの場所に移動します。ファイルは.PNGファイルである必要があります。JPEGまたは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すると、後で変更することはできません。

7. 展開ルールを構成します。詳細については、展開ルールを参照してください。
8. **ストア構成**を展開します。

   アプリ構成画面(/en-us/xenmobile/server/media/configure-apps-store-configuration.png)

   - **アプリのFAQ:** 「**新しいFAQの質問と回答を追加**」をクリックして、アプリのFAQを作成します。
   - **電話/タブレットのスクリーンショットを追加:** アプリストアに表示されるスクリーンショットを追加します。
   - **アプリの評価を許可:** ユーザーがアプリストアでアプリを評価できるようにします。
   - **アプリのコメントを許可:** ユーザーがアプリストアでアプリにコメントを残せるようにします。

9. 「**次へ**」をクリックします。「**デリバリーグループの割り当て**」ページが表示されます。
10. 「**デリバリーグループの選択**」の横に、デリバリーグループを検索するためにタイプするか、リストから1つまたは複数のグループを選択します。選択したグループは、「**アプリの割り当てを受け取るデリバリーグループ**」リストに表示されます。
11. 「**展開スケジュール**」を展開し、次の設定を構成します。

    - **展開:** アプリをデバイスに展開するかどうかを選択します。デフォルトは「**オン**」です。
    - **展開スケジュール:** アプリを「**今すぐ**」展開するか、「**後で**」展開するかを選択します。「**後で**」を選択した場合は、アプリを展開する日付と時刻を構成します。デフォルトは「**今すぐ**」です。

- **展開条件:** デバイスが接続するたびにアプリを展開するには、「**接続ごとに**」を選択します。以前にデバイスがアプリの受信に失敗した場合にアプリを展開するには、「**以前の展開が失敗した場合のみ**」を選択します。デフォルトは「**接続ごとに**」です。

「**常時接続の展開**」は、「**設定 > サーバープロパティ**」でスケジューリングバックグラウンド展開キーを構成した場合に適用されます。

構成する展開スケジュールは、すべてのプラットフォームで同じです。「**常時接続の展開**」を除き、行った変更はすべてのプラットフォームに適用されます。

12. 「**保存**」をクリックします。

Microsoft 365アプリを有効にする

Secure Mail、Secure Web、およびCitrix Filesがドキュメントとデータを Microsoft Office 365アプリに転送できるように、MDXコンテナを開くことができます。詳細については、「Office 365アプリとの安全な対話を許可する」を参照してください。

ワークフローを適用

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:** リストで既存のワークフローをクリックするか、**新しいワークフローを作成**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を作成を選択した場合は、次の設定を構成します。

  - **名前:** ワークフローの一意の名前を入力します。
  - **説明:** 必要に応じて、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:** リストで、割り当てる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側にある目のアイコンをクリックすると、テンプレートをプレビューできるダイアログボックスが表示されます。
  - **マネージャー承認レベル:** リストで、このワークフローに必要なマネージャー承認レベルの数を選択します。デフォルトは1レベルです。選択可能なオプションは次のとおりです。
    - 不要
    - 1レベル
    - 2レベル
    - 3レベル

- **Active Directoryドメインの選択:** リストで、ワークフローに使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を見つける:** 検索フィールドに追加の必須承認者の名前を入力し、**検索**をクリックします。名前はActive Directoryから取得されます。
- フィールドに名前が表示されたら、名前の横にあるチェックボックスをオンにします。名前とメールアドレスは、**選択された追加の必須承認者**リストに表示されます。

  「**選択された追加の必須承認者**」リストからユーザーを削除するには、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リストを表示します。
  - 検索ボックスに氏名または部分的な名前を入力し、**検索**をクリックして検索結果を絞り込みます。
  - 「**選択された追加の必須承認者**」リストのユーザーには、検索結果リストの名前の横にチェックマークが付いています。リストをスクロールし、削除する各名前の横にあるチェックボックスをオフにします。

アプリストアとCitrix Secure Hubのブランディング

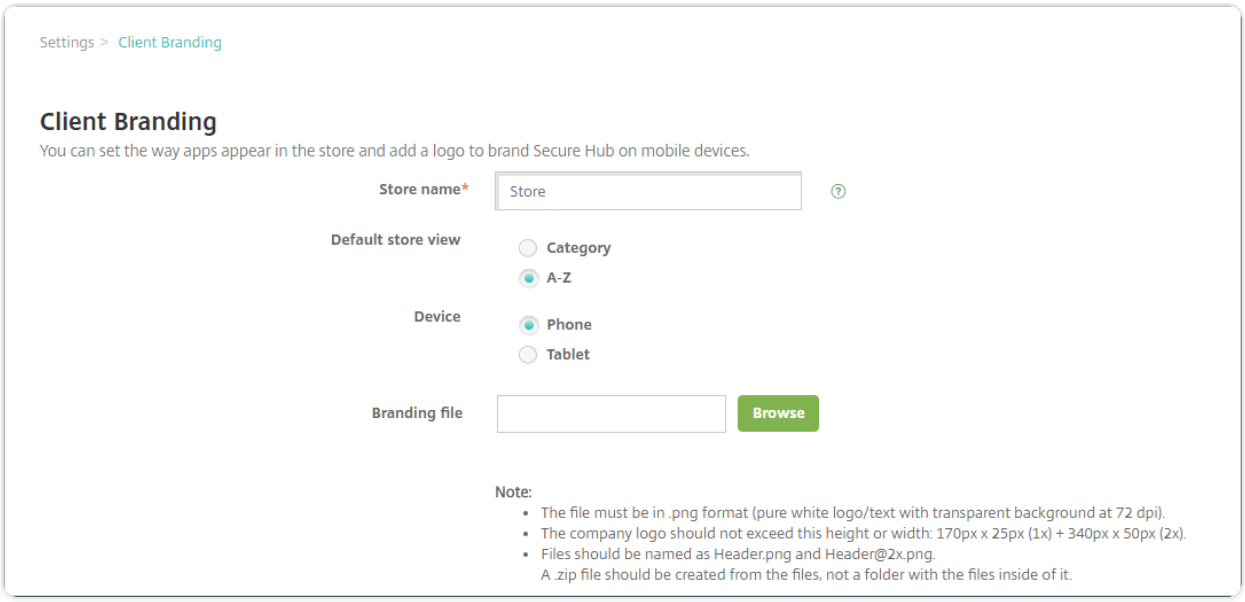
ストアでのアプリの表示方法を設定し、Secure Hubとアプリストアをブランド化するためのロゴを追加できます。これらのブランディング機能は、iOSおよびAndroidデバイスで利用できます。

開始する前に、カスタム画像が準備され、アクセス可能であることを確認してください。

カスタム画像は、次の要件を満たしている必要があります。

- ファイルは.png形式である必要があります
- 72 dpiで、透明な背景を持つ純粋な白のロゴまたはテキストを使用してください。
- 会社のロゴは、高さまたは幅が170 px x 25 px (1x) および 340 px x 50 px (2x) を超えないようにしてください。
- ファイル名をHeader.pngと`Header@2x.png`にしてください。
- ファイルを含むフォルダではなく、ファイルから.zipファイルを作成してください。

1. XenMobile Serverコンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. **クライアント**の下にある**クライアントブランディング**をクリックします。「**クライアントブランディング**」ページが表示されます。



次の設定を構成します。

- **ストア名:** ストア名は、ユーザーのアカウント情報に表示されます。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変更する必要はありません。

  > **重要:**
  >
  > ストア名には英数字のみを含めることができます。

- **デフォルトのストアビュー: カテゴリ**または**A-Z**のいずれかを選択します。デフォルトは**A-Z**です。
- **デバイスオプション: 電話**または**タブレット**のいずれかを選択します。デフォルトは**電話**です。
- **ブランディングファイル: 参照**をクリックしてファイルの場所に移動し、ブランディングに使用する画像または画像の.zipファイルを選択します。

3. **保存**をクリックします。

アプリコネクタの種類

次の表に、WebまたはSaaSアプリを追加する際にXenMobile®で利用できるコネクタとその種類を示します。WebまたはSaaSアプリを追加する際に、XenMobileに新しいコネクタを追加することもできます。

この表は、コネクタがユーザーアカウント管理をサポートしているかどうかを示しています。これにより、新しいアカウントを自動的に、またはワークフローを使用して作成できます。

コネクタ名	SSO SAML	ユーザーアカウント管理をサポート
EchoSign_SAML	Y	Y
Globoforce_SAML		**注:** このコネクタを使用する場合、シームレスなSSO統合のために、プロビジョニングのユーザー管理を有効にする必要があります。
GoogleApps_SAML	Y	Y
GoogleApps_SAML_IDP	Y	Y
Lynda_SAML	Y	Y
Office365_SAML	Y	Y
Salesforce_SAML	Y	Y
Salesforce_SAML_SP	Y	Y
SandBox_SAML	はい	
SuccessFactors_SAML	はい	
ShareFile_SAML	はい	
ShareFile_SAML_SP	はい	
WebEx_SAML_SP	はい	はい

MDXまたはエンタープライズアプリをアップグレードする

XenMobileでMDXまたはエンタープライズアプリをアップグレードするには、XenMobileコンソールでアプリを無効にしてから、新しいバージョンのアプリをアップロードします。Citrix Secure Mailのような公開アプリストアのアプリを無効にする必要はありません。

1. XenMobile®コンソールで、 **［構成］ > ［アプリ］** の順にクリックします。 **［アプリ］** ページが表示されます。
2. 管理対象デバイス（モバイルデバイス管理のためにXenMobileに登録されているデバイス）の場合は、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管理目的でのみXenMobileに登録されているデバイス）の場合は、次の操作を行います。

   a. **［アプリ］** テーブルで、アプリの横にあるチェックボックスをオンにするか、更新するアプリがある行をクリックします。

   b. 表示されるメニューで **［無効化］** をクリックします。

   アプリメニュー(/en-us/xenmobile/server/media/configure-apps-disable-app.png)

   c. 確認ダイアログボックスで **［無効化］** をクリックします。アプリの **［無効化］** 列に *無効* と表示されます。

   無効化されたアプリ(/en-us/xenmobile/server/media/configure-apps-disable-app-disabled.png)

   > **注：**
   >
   > アプリが無効になっている間、ユーザーはログオフ後にアプリに再接続できません。アプリの無効化は任意ですが、アプリの機能に関する問題を回避するために、アプリを無効にすることをお勧めします。たとえば、新しいバージョンをアップロードしているときにユーザーがアプリのダウンロードを要求すると、問題が発生する可能性があります。

3. **［アプリ］** テーブルで、アプリの横にあるチェックボックスをクリックするか、更新するアプリがある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。 **［アプリ情報］** ページが表示され、アプリ用に最初に選択したプラットフォームが選択されています。
5. 次の設定を構成します。

   - **名前：** 必要に応じて、アプリ名を変更します。
   - **説明:** 必要に応じて、アプリの説明を変更します。
   - **アプリカテゴリ:** 必要に応じて、アプリ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表示されます。選択した各プラットフォームについて、以下を実行します。

a. **アップロード**をクリックしてファイルの場所に移動し、アップロードする置換ファイルを選択します。アプリがXenMobileにアップロードされます。

   Android Enterprise用アプリをアップロードする場合、管理対象のGoogle Playウィンドウが表示されます。ここでアプリの新しいバージョンをアップロードします。詳細については、「Android Enterpriseアプリの配布」を参照してください。

b. 必要に応じて、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。

c. 必要に応じて、展開ルールとXenMobile Storeの構成を設定します。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**ページが表示されます。
8. 手順2でアプリを無効にした場合は、以下を実行します。

a. **アプリ**テーブルで、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。

b. 表示される確認ダイアログボックスで、**有効にする**をクリックします。これでユーザーはアプリにアクセスできるようになり、アプリをアップグレードするよう促す通知を受け取ります。

シトリックス ランチャー

Citrix Launcherの代替

Citrixは2020年8月にCitrix Launcherをアプリストアから削除しました。Citrix Launcherの代わりに、既存の機能を使用できます。

デバイスをキオスク (専用デバイス) としてプロビジョニングするには:

1. XenMobile管理者が専用デバイスをXenMobile展開に登録できるようにするRBACロールを追加します。詳細については、「専用Android Enterpriseデバイスのプロビジョニング」を参照してください。
2. **登録タイプ**が**完全管理/仕事用プロファイル**の登録プロファイルを作成します。詳細については、「登録プロファイルを作成するには」を参照してください。
3. **タスクロックモード**設定を有効にして、アプリをデバイス画面に固定するように構成するキオスクデバイスポリシーを作成します。詳細については、「Android Enterprise設定」を参照してください。

Citrix Launcherについて

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Launcher Configurationデバイスポリシーは、Android Enterpriseと互換性がありません。

Launcher Configurationポリシーを追加して、次のCitrix Launcher機能を制御できます。

- ユーザーが指定したアプリのみにアクセスできるようにAndroidデバイスを管理します。
- オプションで、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指定します。
- ユーザーがランチャーを終了するために必要なパスワードを指定します。

Citrix Launcherを使用するとデバイスレベルの制限を適用できますが、ランチャーはWi-Fi設定、Bluetooth設定、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アクセスをユーザーに許可します。Citrix Launcherは、デバイスプラットフォームがすでに提供しているセキュリティの上に、追加のセキュリティ層として意図されたものではありません。

AndroidデバイスにCitrix Launcherを提供するには、次の一般的な手順に従います。

1. Citrix Launcherアプリをダウンロードするには、`<https://www.citrix.com/downloads>`にアクセスします。**Citrix Launcher**を検索します。ファイル名はCitrixLauncher.apkです。このファイルはXenMobileにアップロードする準備ができており、ラッピングは不要です。
2. デバイスポリシー**Launcher Configuration Policy**を追加します。**Configure > Device Policies**に移動し、**Add**をクリックして、**Add a New Policy**ダイアログボックスで「**Launcher**」と入力し始めます。詳しくは、「Launcher Configuration Policy」を参照してください。

   ランチャー構成の画像(/en-us/xenmobile/server/media/configure-device-policies-android-launcher-information.png)
3. Citrix Launcherアプリをエンタープライズアプリとして XenMobileに追加します。**Configure > Apps**で、**Add**をクリックし、次に**Enterprise**をクリックします。詳しくは、「Add an enterprise app」を参照してください。

   エンタープライズアプリの追加の画像(/en-us/xenmobile/server/media/add-enterprise-app.png)
4. **Configure > Delivery groups**で、以下の構成でCitrix Launcherのデリバリーグループを作成します。

   - **Policies**ページで、**Launcher Configuration Policy**を追加します。

- **Apps**ページで、**Citrix Launcher**を**Required Apps**にドラッグします。
- **Summary**ページで、**Deployment Order**をクリックし、**Citrix Launcher**アプリが**Launcher Configuration**ポリシーより前に配置されていることを確認します。

起動展開順序の画像(/en-us/xenmobile/server/media/launcher-app-policy-deployment-order.png)

詳しくは、「Deploy resources」を参照してください。

Apple ボリューム購入

Apple iOSボリューム購入を使用すると、iOSアプリのライセンスを管理できます。ボリューム購入ソリューションは、組織向けにアプリやその他のデータを一括で検索、購入、配布するプロセスを簡素化します。

ボリューム購入を使用すると、XenMobile® を使用して公開アプリストアのアプリを配布できます。

- ボリューム購入はMAM登録ではサポートされていません。ボリューム購入デバイスは、MDMまたはMDM+MAMに登録する必要があります。
- ボリューム購入は、Citrix® モバイル生産性向上アプリではサポートされていません。
- ボリューム購入でXenMobile公開ストアアプリを配布することはできますが、展開は最適ではありません。制限に対処するには、XenMobileおよびSecure Hubストアの機能強化が必要です。
- ボリューム購入を通じてXenMobile公開ストアアプリを配布する際の既知の問題のリストについては、Citrix Knowledge CenterのCTX222633を参照してください。

ボリューム購入を使用すると、該当するアプリをデバイスに直接配布できます。または、引き換えコードを使用してユーザーにコンテンツを割り当てます。XenMobileでiOSボリューム購入に固有の設定を構成します。

XenMobileは、ライセンスがすべての変更を反映していることを確認するために、Appleからボリューム購入ライセンスを定期的に再インポートします。このような変更には、ボリューム購入からインポートされたアプリを手動で削除した場合が含まれます。デフォルトでは、XenMobileはボリューム購入ライセンスのベースラインを最低1440分（24時間）ごとに更新します。サーバープロパティ`VPP.baseline`を通じて、ボリューム購入ベースライン間隔を変更できます。サーバープロパティを参照してください。

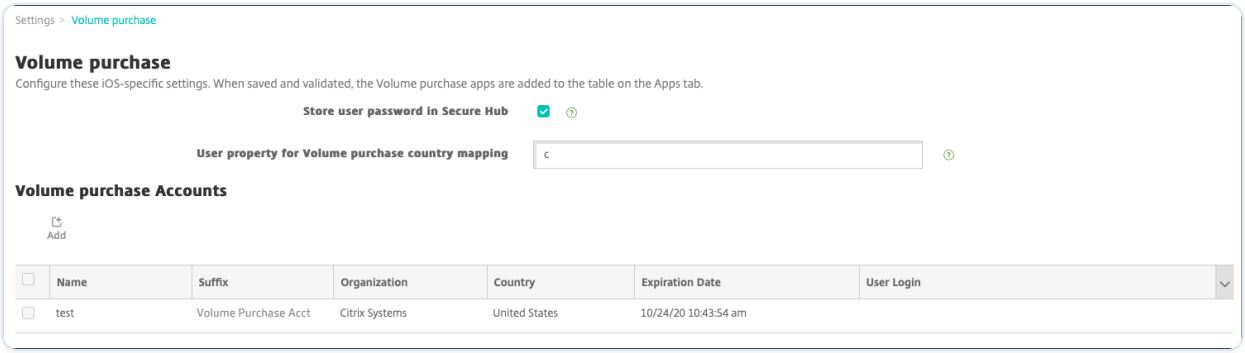
アプリの自動更新設定も`VPP.baseline`サーバープロパティに依存しており、アプリはそのプロパティで設定された同じスケジュールで更新されます。

この記事では、XenMobileを使用してアプリを配布できる、管理対象ライセンスでのボリューム購入の使用に焦点を当てています。現在引き換えコードを使用しており、管理対象配布に変更したい場合は、このAppleサポートドキュメントボリューム購入で引き換えコードから管理対象配布に移行するを参照してください。

iOSボリューム購入の詳細については、`<https://volume.itunes.apple.com/us/store>`を参照してください。ボリューム購入に登録するには、`<https://deploy.apple.com/qforms/open/register/index/avs>`にアクセスしてください。iTunesでボリューム購入ストアにアクセスするには、`<https://volume.itunes.apple.com/?l=en>`にアクセスしてください。

XenMobileでこれらのiOSボリューム購入設定を保存すると、購入したアプリが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、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **ボリューム購入**をクリックします。**ボリューム購入**構成ページが表示されます。



3. 次の設定を構成します。

   - **Secure Hubにユーザーパスワードを保存:** XenMobile認証のためにSecure Hubにユーザー名とパスワードを保存するかどうかを選択します。デフォルトでは、この安全な方法を使用して情報が保存されます。
   - **ボリューム購入の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。

   XenMobileは、このマッピングを使用してボリューム購入のプロパティプールを選択します。たとえば、ユーザープロパティが米国である場合、ボリューム購入コードが英国のものであれば、そのユーザーはアプリをダウンロードできません。国マッピングコードの詳細については、ボリューム購入プランの管理者にお問い合わせください。

4. 追加するボリューム購入アカウントごとに、**追加**をクリックします。**ボリューム購入アカウントの追加**ダイアログボックスが表示されます。



5. 追加する各アカウントについて、次の設定を構成します。

> **注:**
>
> Apple Configurator 1を使用している場合は、ライセンスファイルをアップロードします。**構成 > アプリ**に移動し、プラットフォームページに移動して、**ボリューム購入**を展開します。

- **名前:** ボリューム購入アカウント名を入力します。
- **サフィックス:** ボリューム購入アカウントを通じて取得したアプリ名に表示するサフィックスを入力します。たとえば、**VP**と入力すると、Secure Mailアプリはアプリリストに**Secure Mail - VP**と表示されます。
- **会社トークン:** Appleから取得したボリューム購入サービストークンをコピーして貼り付けます。トークンを取得するには、Appleボリューム購入ポータルの**アカウント概要**ページで、**ダウンロード**ボタンをクリックしてボリューム購入ファイルを生成およびダウンロードします。このファイルには、サービストークンと、国コードや有効期限などのその他の情報が含まれています。ファイルを安全な場所に保存します。
- **ユーザーログイン:** カスタムB2Bアプリのインポートに使用する、オプションの承認済みボリューム購入アカウント管理者名を入力します。
- **ユーザーパスワード:** ボリューム購入アカウントの管理者パスワードを入力します。
- **App Auto Update:** 「**On**」の場合、Apple Storeでアップデートが利用可能になると、ボリューム購入アプリは自動的に更新されます。デフォルトは「**Off**」です。

6. ダイアログボックスを閉じるには、**Save**をクリックします。
7. ボリューム購入構成を保存するには、**Save**をクリックします。

   XenMobileがアプリを**Configure > Apps**ページのリストに追加したことを示すメッセージが表示されます。このページで、ボリューム購入アカウントからのアプリ名に、前の構成で指定したサフィックスが含まれていることに注意してください。

これで、ボリューム購入アプリの設定を構成し、ボリューム購入アプリのデリバリーグループとデバイスポリシー設定を調整できます。これらの構成が完了すると、ユーザーはデバイスを登録できます。以下の注意事項は、これらのプロセスに関する考慮事項を提供します。

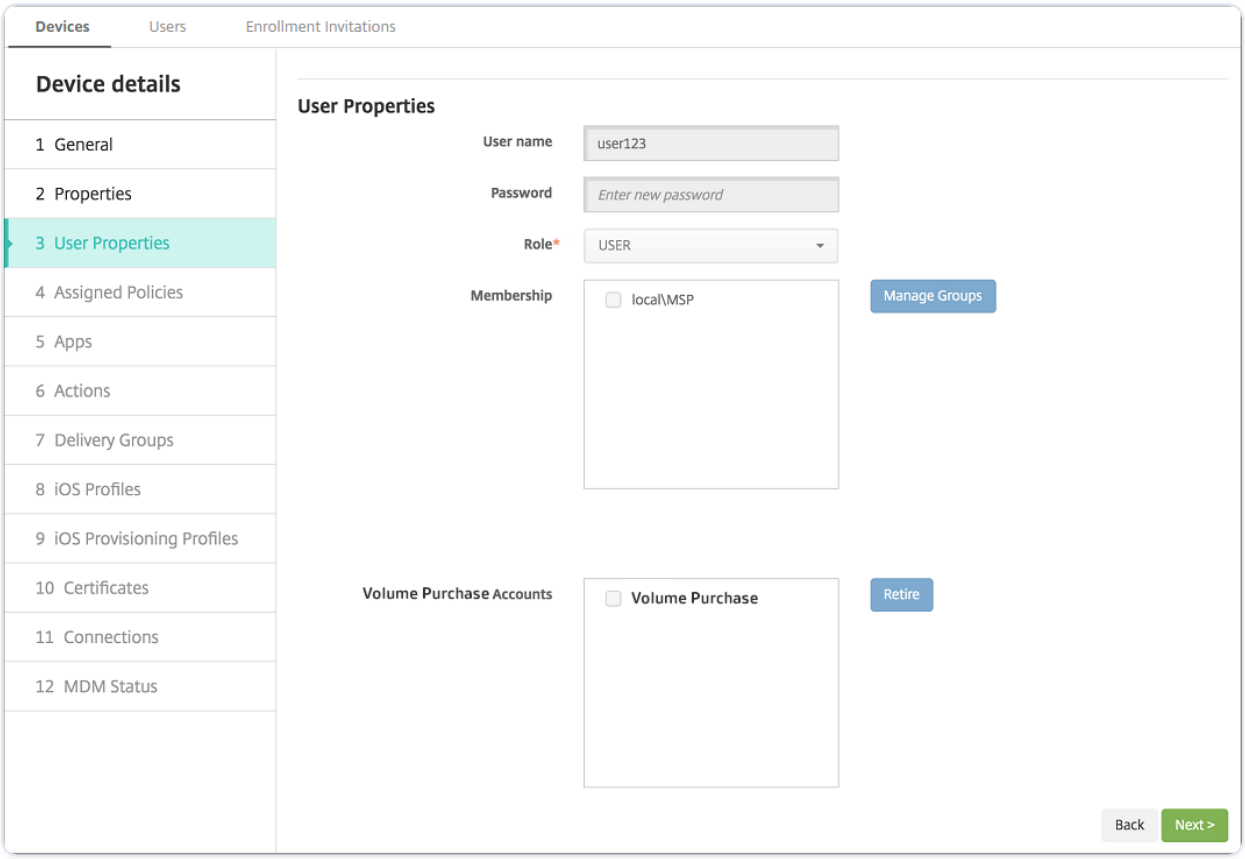
- ボリューム購入アプリの設定（**Configure > Apps**）を構成する際は、**Force license association to device**を有効にします。

  Appleボリューム購入および監視対象デバイスでのDeployment Programを使用する利点：XenMobileを使用して、アプリをユーザーレベルではなくデバイスレベルで割り当てることができます。その結果、Apple IDデバイスを使用する必要がありません。また、ユーザーはAppleボリューム購入への招待を受け取りません。ユーザーはiTunesアカウントにサインインしなくてもアプリをダウンロードできます。

  そのアプリのボリューム購入情報を表示するには、**Volume purchase**を展開します。**Volume purchase License Keys**テーブルで、ライセンスがデバイスに関連付けられていることに注意してください。ユーザーがトークンを削除して再度インポートすると、Appleのプライバシー制限により、シリアル番号の代わりに「**Hidden**」という単語が表示されます。

  ライセンスの関連付けを解除するには、ライセンスの行をクリックし、**Disassociate**をクリックします。

  ボリューム購入ライセンスをユーザーに関連付けると、XenMobileはユーザーをボリューム購入アカウントに統合します。また、ユーザーのiTunes IDをボリューム購入アカウントに関連付けます。ユーザーのiTunes IDは、会社やXenMobile Serverには決して表示されません。Appleはユーザーのプライバシーを保護するために、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ために、Appleボリューム購入からユーザーを引退させることができます。ユーザーを引退させるには、**Manage > Devices**に移動します。



- アプリをデリバリーグループに割り当てると、デフォルトでXenMobileはアプリをオプションアプリとして識別します。XenMobileがアプリをデバイスに展開するようにするには、**Configure** > **Delivery Groups**に移動します。**Apps**ページで、アプリを**Required Apps**リストに移動します。
- アプリのアップデートが利用可能になると、ボリューム購入によってアプリにアップデートがプッシュされ、デバイス上のアプリが自動的にアップデートされます。詳細については、「アプリのアップデートを確認する」を参照してください。

Appleボリューム購入の有効期限が切れると、XenMobileはライセンス有効期限警告を表示します。

アプリのアップデートを確認する

ボリューム購入アカウントを追加する際に**App Auto Update**設定をオンにすると、XenMobile Serverはボリューム購入済みアプリ（必須アプリ）およびCitrix Secure Hubストアからサブスクライブされたオプションアプリの新しいバージョンを定期的にチェックし、それらをアップデートします。XenMobile Serverが必須アプリの新しいバージョンを受信すると、手動でアップデートを促すことなく、新しいバージョンを自動的にデバイスにプッシュしてインストールします。ただし、オプションアプリを自動アップデートするには、プロパティ

`apple.ios.optional_app_update`を**True**に設定する必要があります。そうしないと、オプションアプリを手動でアップデートする必要があります。詳細については、「サーバープロパティ」を参照してください。

任意のアプリの新しいバージョンを手動で確認してアップデートするには、次の手順を実行します。

1. **Configure** > **Apps**の順にクリックします。

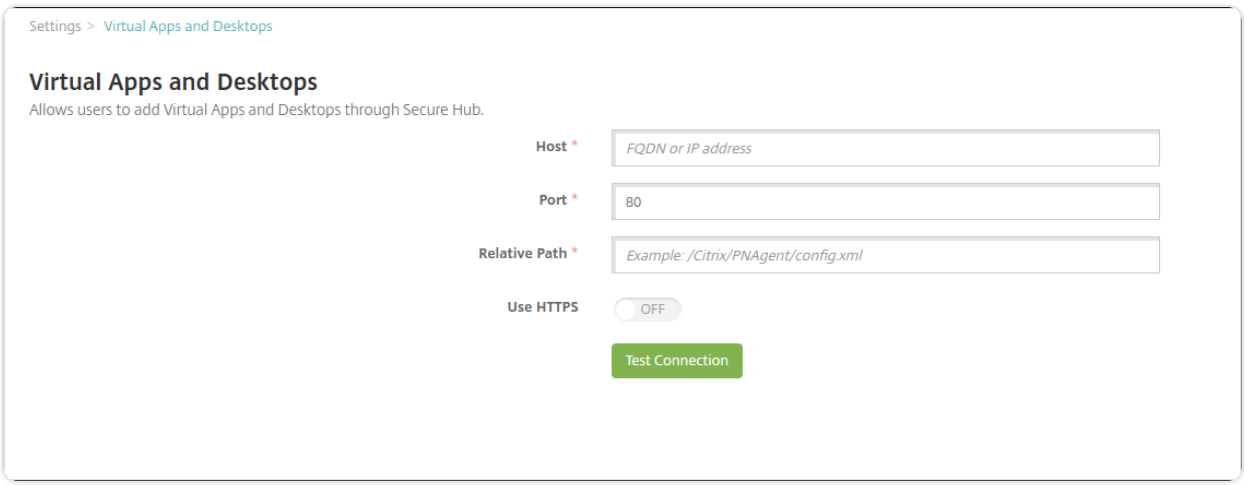
   Appsページが表示されます。
2. アプリを選択し、**Edit**をクリックします。
3. **Platform**ページに移動し、**Version**の横にある**Check for Updates**ボタンをクリックします。
4. **Update**ダイアログボックスで、新しいバージョンが利用可能な場合はアップデートを適用します。

Citrix Secure Hub™ を介した仮想アプリおよびデスクトップ

XenMobileは、Virtual Apps and Desktopsからアプリを収集し、XenMobile Storeでモバイルデバイスユーザーが利用できるようにします。ユーザーはXenMobile Store内で直接アプリを購読し、Secure Hubから起動します。アプリを起動するには、ユーザーデバイスにCitrix Receiver™がインストールされている必要がありますが、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 (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、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **Virtual Apps and Desktops**をクリックします。**Virtual Apps and Desktops**ページが表示されます。



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。例: /Citrix/PNAgent/config.xml
    - **HTTPSを使用:** Web InterfaceサイトまたはStoreFrontとクライアントデバイス間のセキュア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. **接続テスト**をクリックして、XenMobileが指定されたVirtual Apps and Desktopsサーバーに接続できることを確認します。
5. **保存**をクリックします。

XenMobile®でShareFileを使用する

> **免責事項:**

> ShareFile (現 Progress) がサポートを終了した場合、この機能は非推奨となります。

> XenMobileには、ShareFileと統合するための2つのオプションがあります。Citrix Filesとストレージゾーンコネクタです。Citrix Filesまたはストレージゾーンコネクタとの統合には、XenMobile Advanced Edition (オンプレミス) またはCitrix Endpoint Management™ (クラウド) が必要です。

シトリックス ファイルズ

XenMobile Advanced Edition (オンプレミス) またはCitrix Endpoint Management (クラウド) をお持ちの場合、XenMobileを構成してCitrix Filesアカウントへのアクセスを提供できます。その構成では、次のことが可能です。

- ファイル共有、ファイル同期、ストレージゾーンコネクタなどの完全なEnterprise機能セットにモバイルユーザーがアクセスできるようにします。
- Citrix Filesに、XenMobile Appユーザーのシングルサインオン認証と包括的なアクセス制御ポリシーを提供できます。
- XenMobileコンソールを通じて、Citrix Filesの構成、サービスレベル監視、およびライセンス使用状況監視を提供します。

Citrix Files向けXenMobileの構成の詳細については、「Citrix FilesでのシングルサインオンのためのSAML」を参照してください。

ストレージゾーンコネクタ

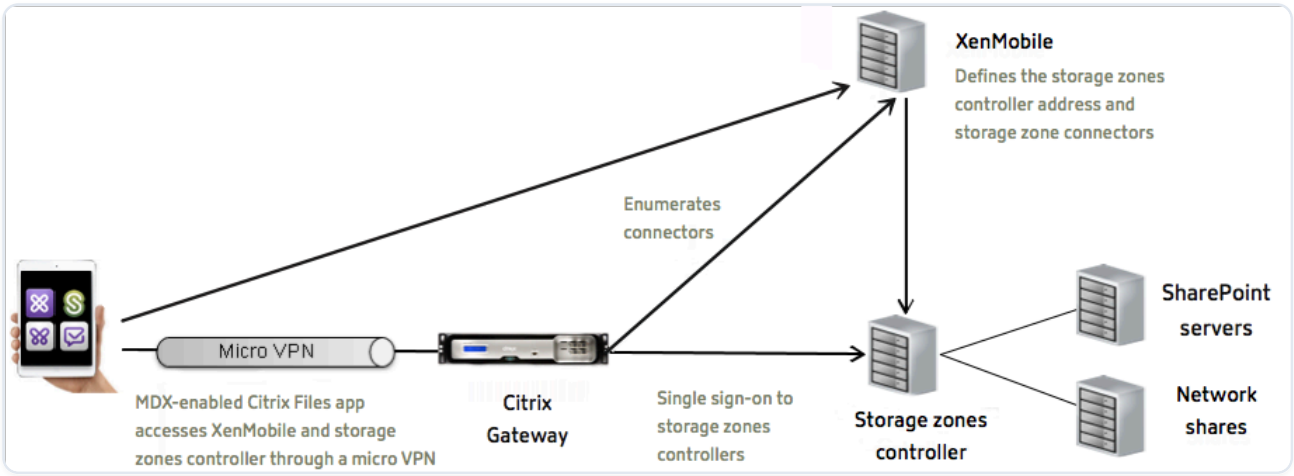
XenMobileコンソールを通じて作成したストレージゾーンコネクタにのみアクセスを提供するようにXenMobileを構成できます。その構成では、次のことが可能です。

- 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ストレージリポジトリへの安全なモバイルアクセスを提供します。
- ShareFileサブドメインを設定したり、Citrix Filesデータをホストしたりする必要はありません。
- iOSおよびAndroid向けのCitrix Filesモバイル生産性向上アプリを通じて、データへのモバイルアクセスを提供します。Microsoft Officeドキュメントを編集できます。また、モバイルデバイスからAdobe PDFファイルをプレビューおよび注釈付けできます。
- 企業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制限に準拠します。
- XenMobileコンソールを介したストレージゾーンコネクタの簡単なセットアップを提供します。後でXenMobileでCitrix Filesの全機能を使用することにした場合、XenMobileコンソールで構成を変更できます。
- XenMobile Advanced Edition (オンプレミス) またはCitrix Endpoint Management (クラウド) が必要です。

ストレージゾーンコネクタのみを使用するXenMobile統合の場合：

- ShareFileは、シングルサインオン構成を使用してCitrix Gateway経由でストレージゾーンコントローラと認証します。
- Citrix Filesコントロールプレーンが使用されないため、XenMobileはSAMLを介して認証しません。

次の図は、ストレージゾーンコネクタを使用するXenMobileのハイレベルアーキテクチャを示しています。



要件

- 最小コンポーネントバージョン：
  - XenMobile Server 10.5 (オンプレミス)
  - iOS版 ShareFile (MDX) 5.3
  - アンドロイド版 シェアファイル (MDX) 5.3
  - ストレージゾーンコントローラー 5.0

    この記事では、Storage zones controller 5.0を構成する方法について説明します。
- ストレージゾーンコントローラー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。要件については、「システム要件」を参照してください。

Citrix Files Data 用ストレージゾーンおよび制限付きストレージゾーンの要件は、ストレージゾーンコネクタのみを使用するXenMobile統合には適用されません。

XenMobileはDocumentumコネクタをサポートしていません。

- PowerShellスクリプトを実行するには：
  - PowerShellの32ビット (x86) バージョンでスクリプトを実行します。

インストールタスク

ストレージゾーンコントローラーをインストールしてセットアップするには、以下のタスクを提示された順序で完了してください。これらの手順は、ストレージゾーンコネクタのみを使用するXenMobile統合に特化したものです。これらの記事の一部は、ストレージゾーンコントローラーのドキュメントに記載されています。

1. ストレージゾーンコントローラー用にCitrix ADCを構成する

Citrix ADCをストレージゾーンコントローラーのDMZプロキシとして使用できます。

2. SSL証明書をインストールする

   標準ゾーンをホストするストレージゾーンコントローラーにはSSL証明書が必要です。制限付きゾーンをホストし、内部アドレスを使用するストレージゾーンコントローラーにはSSL証明書は必要ありません。

3. サーバーを準備する

   ストレージゾーンコネクタには、IISおよびASP.NETのセットアップが必要です。

4. ストレージゾーンコントローラーをインストールする
5. ストレージゾーンコネクタ専用のストレージゾーンコントローラーを準備する
6. ストレージゾーンのプロキシサーバーを指定する(/ja-jp/storagezones-controller/5-0/install/specify-proxy.html)

   ストレージゾーンコントローラーコンソールを使用すると、ストレージゾーンコントローラーのプロキシサーバーを指定できます。他の方法を使用してプロキシサーバーを指定することもできます。

7. 委任のためにストレージゾーンコントローラーを信頼するようにドメインコントローラーを構成する(/ja-jp/storagezones-controller/5-0/install/configure-domain-controller.html)

   ネットワーク共有またはSharePointサイトでNTLMまたは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. セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる(#join-a-secondary-storage-zones-controller-to-a-storage-zone)

   高可用性用にストレージゾーンを構成するには、少なくとも2つのストレージゾーンコントローラーを接続します。

ストレージゾーンコントローラーのインストール

1. ストレージゾーンコントローラー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. `<https://www.citrix.com/downloads>`にアクセスします。**ShareFile**を検索し、最新のストレージゾーンコントローラーインストーラーをダウンロードします。

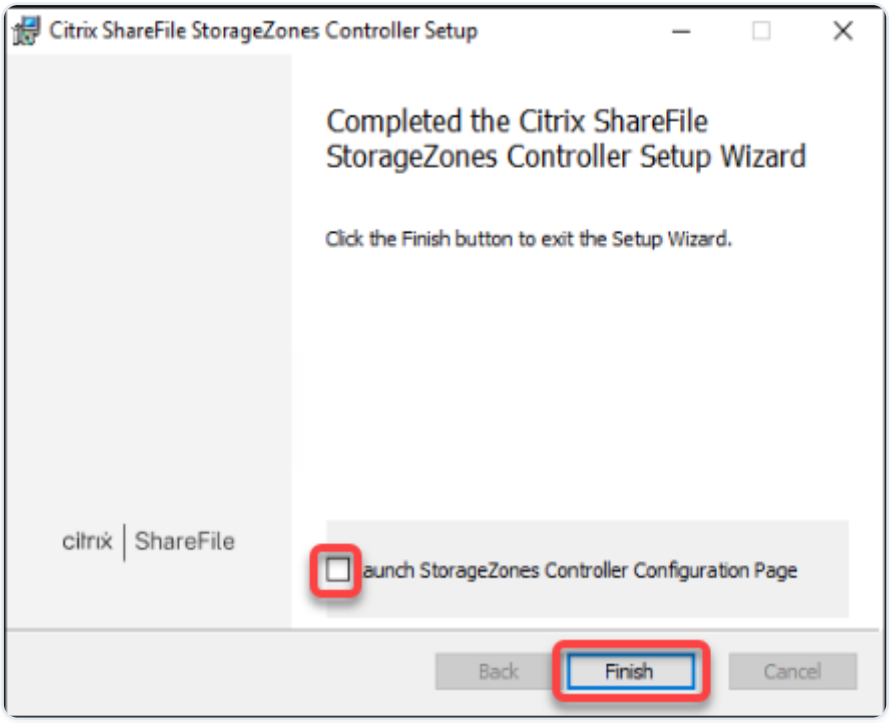
   b. ストレージゾーンコントローラーをインストールすると、サーバー上のデフォルトのWebサイトがコントローラーのインストールパスに変更されます。デフォルトのWebサイトで**匿名認証**を有効にします。

2. ストレージゾーンコントローラーをインストールするサーバーで、StorageCenter.msiを実行します。

   ストレージゾーンコントローラーのセットアップウィザードが起動します。

3. プロンプトに応答します。

   - **Destination Folder**ページで、Internet Information Services (IIS) がデフォルトの場所にインストールされている場合は、デフォルトのままにします。そうでない場合は、IISのインストール場所に移動します。
   - インストールが完了したら、**Launch Storage Zones Controller Configuration Page**のチェックボックスをオフにして、**Finish**をクリックします。



4. プロンプトが表示されたら、ストレージゾーンコントローラーを再起動します。
5. インストールが成功したことをテストするには、`https://localhost/`に移動します。インストールが成功すると、Citrix Filesのロゴが表示されます。

   Citrix Filesのロゴが表示されない場合は、ブラウザのキャッシュをクリアしてもう一度試してください。

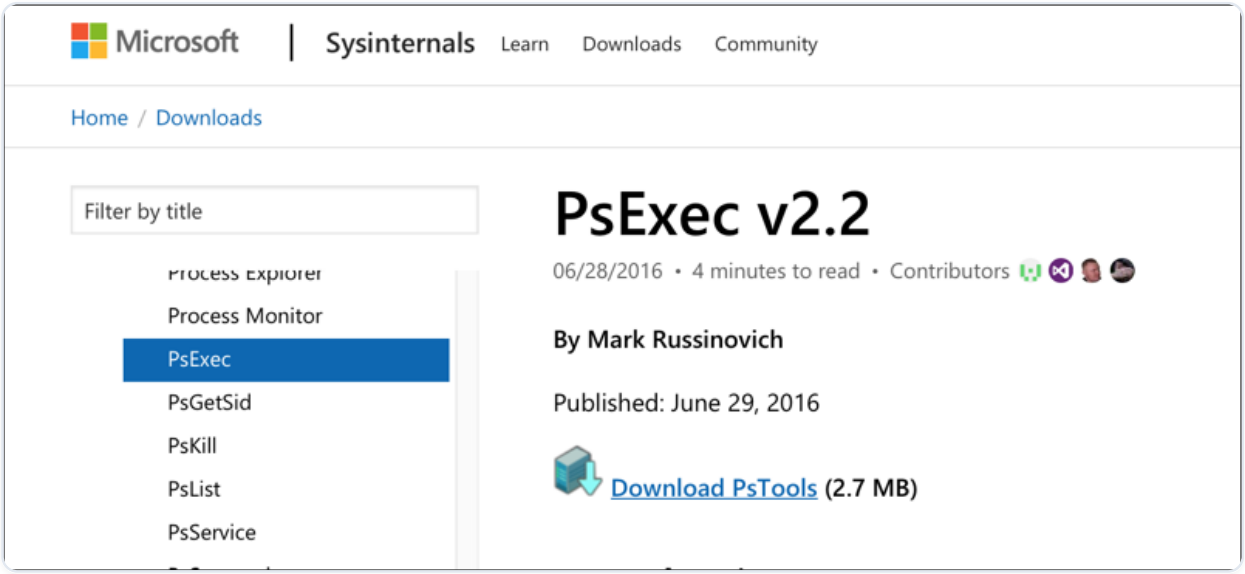
> **重要:**
>
> ストレージゾーンコントローラーをクローンする予定がある場合は、ストレージゾーンコントローラーの構成を続行する前にディスクイメージをキャプチャします。

ストレージゾーンコネクタのみで使用するためのストレージゾーンコントローラーの準備

ストレージゾーンコネクタのみとの統合の場合、ストレージゾーンコントローラーの管理コンソールは使用しません。そのインターフェイスにはCitrix Files管理者アカウントが必要ですが、このソリューションでは不要です。そのため、PowerShellスクリプトを実行して、Citrix Filesコントロールプレーンなしで使用できるようにストレージゾーンコントローラーを準備します。スクリプトは次の処理を実行します。

- 現在のストレージゾーンコントローラーをプライマリストレージゾーンコントローラーとして登録します。後でセカンダリストレージゾーンコントローラーをプライマリコントローラーに参加させることができます。
- ゾーンを作成し、そのパスフレーズを設定します。

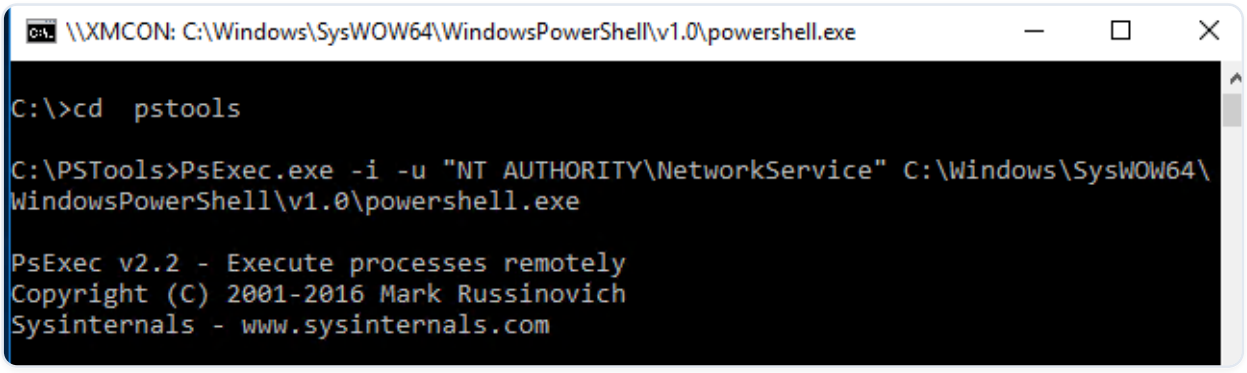
1. ストレージゾーンコントローラーサーバーからPsExecツールをダウンロードします。Microsoft Windows Sysinternalsに移動し、**Download PsTools**をクリックします。ツールをCドライブのルートに抽出します。



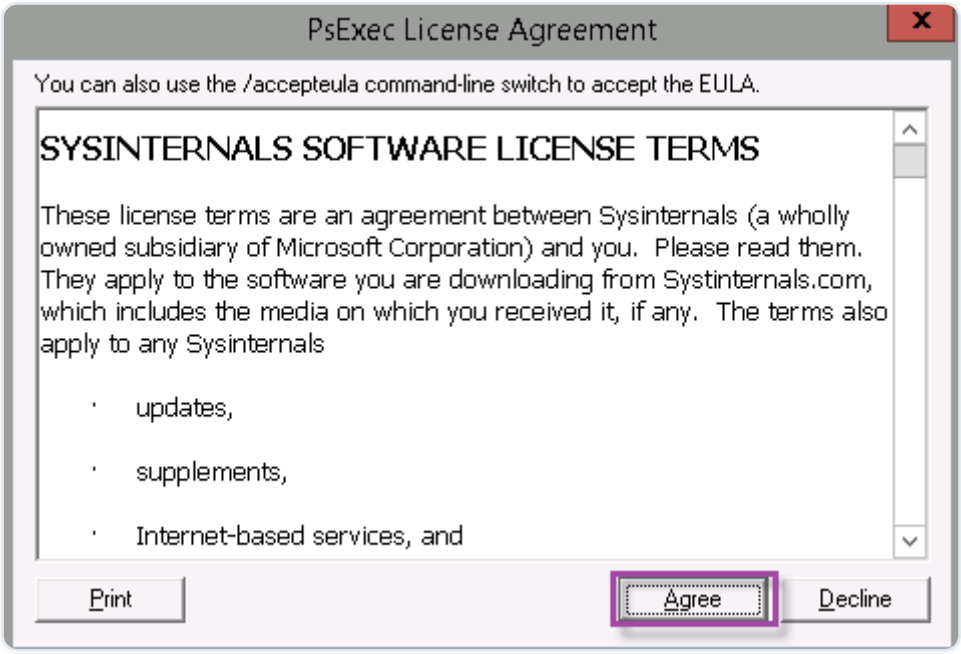
2. PsExecツールを実行します。管理者ユーザーとしてコマンドプロンプトを開き、次のように入力します。

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:
\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. プロンプトが表示されたら、**Agree**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、次のように入力します。

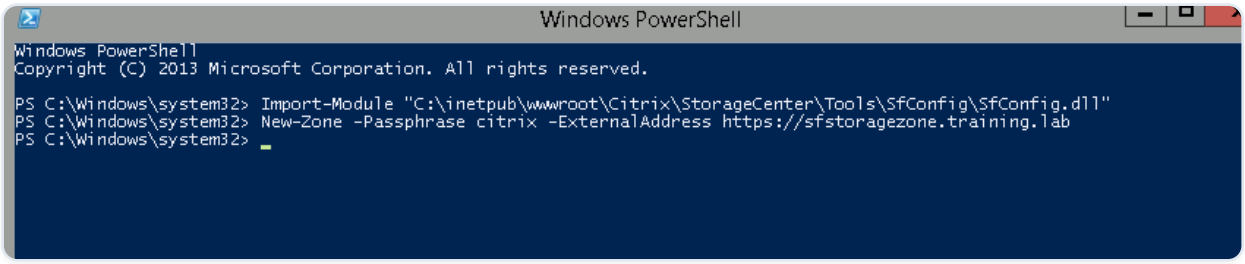
```
Import-Module "C:
\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

説明:

Passphrase: は、サイトに割り当てるパスフレーズです。コントローラーからパスフレーズを回復できないため、メモしておいてください。パスフレーズを紛失した場合、ストレージゾーンコントローラーを再インストールすることはできません。サーバーに障害が発生した場合、ストレージゾーンにさらにストレージゾーンコントローラーを参加させるか、ストレージゾーンを回復してください。

ExternalAddress: は、ストレージゾーンコントローラーサーバーの外部完全修飾ドメイン名です。



プライマリストレージゾーンコントローラーの準備が整いました。

ストレージゾーンコネクタを作成するためにXenMobileにログインする前に、該当する場合は以下の構成を完了してください。

ストレージゾーンのプロキシサーバーを指定する

委任のためにドメインコントローラーがストレージゾーンコントローラーを信頼するように構成する

セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる

ストレージゾーンコネクタを作成するには、XenMobileでストレージゾーンコントローラー接続を定義するを参照してください。

セカンダリストレージゾーンコントローラーをストレージゾーンに参加させる

高可用性のためにストレージゾーンを構成するには、少なくとも2つのストレージゾーンコントローラーを接続します。セカンダリストレージゾーンコントローラーをゾーンに参加させるには、2番目のサーバーにストレージゾーンコントローラーをインストールします。その後、そのコントローラーをプライマリコントローラーのゾーンに参加させます。

1. プライマリサーバーに参加させたいストレージゾーンコントローラーサーバーでPowerShellウィンドウを開きます。
2. PowerShellウィンドウで、次のように入力します。

```
Join-Zone -Passphrase \<passphrase\> -PrimaryController \<HostnameOrIP>
```

例:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

XenMobileでストレージゾーンコントローラー接続を定義する

ストレージゾーンコネクタを追加する前に、ストレージゾーンコネクタが有効になっている各ストレージゾーンコントローラーの接続情報を構成します。ストレージゾーンコントローラーは、このセクションで説明されているように、またはコネクタを追加するときに定義できます。

> ページに初めてアクセスすると、エンタープライズアカウントにXenMobileを使用する場合とストレージゾーンコネクタを使用する場合の違いがページに要約されます。

ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-first-time-use.png)

この記事の構成手順を続行するには、 をクリックします。

ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-no-list.png)

1. **>** で、 をクリックします。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-empty.png)
2. で、接続情報を追加します。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-manage-storagezones-add-new.png)

   - **名前:** StorageZoneを識別するためにXenMobileで使用される、StorageZoneの記述的な名前。名前にスペースや特殊文字を含めないでください。
   - **FQDNとポート:** XenMobile Serverから到達可能なストレージゾーンコントローラーの完全修飾ドメイン名とポート番号。
   - **セキュア接続:** ストレージゾーンコントローラーへの接続にSSLを使用する場合は、デフォルト設定のONを使用します。接続にSSLを使用しない場合は、この設定をOFF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の形式）とパスワード。または、ストレージゾーンコントローラーに対する読み取りおよび書き込み権限を持つユーザーアカウント。
3. **保存**をクリックします。
4. 接続をテストするには、XenMobile Serverがポート443でストレージゾーンコントローラーの完全修飾ドメイン名に到達できることを確認します。

5. 別のストレージゾーンコントローラー接続を定義するには、**Manage StorageZones**で**追加**ボタンをクリックします。

   ストレージゾーンコントローラー接続の情報を編集または削除するには、**Manage StorageZones**で接続名を選択します。次に、**編集**または**削除**をクリックします。

XenMobileでストレージゾーン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。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-no-list.png)

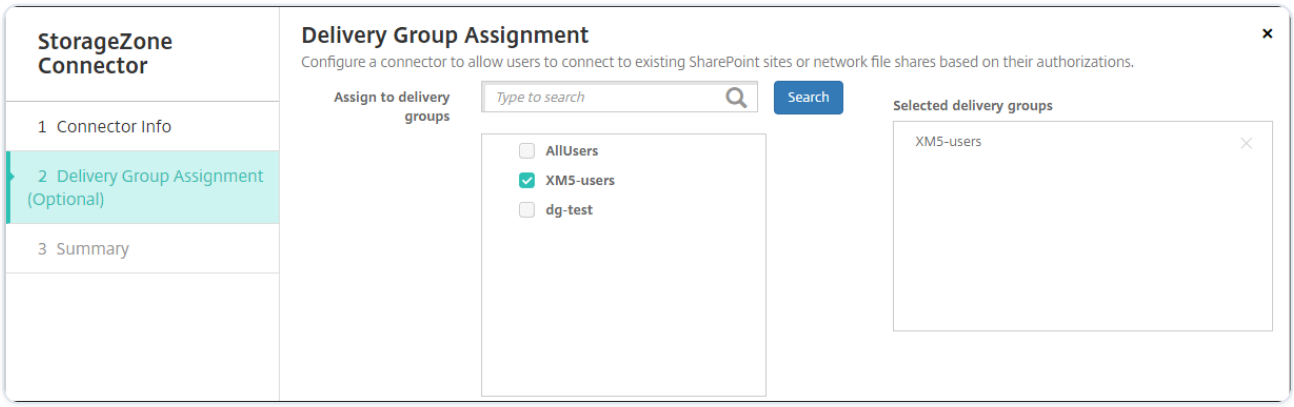
2. **コネクタ情報**ページで、これらの設定を構成します。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-add-storagezone-connector.png)

   - **コネクタ名:** XenMobileでストレージゾーン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 **Network** のいずれかを選択します。」.
   - 「**StorageZone:** コネクタに関連付けられているストレージゾーンを選択します。ストレージゾーンが一覧にない場合は、**Manage StorageZones** をクリックしてストレージゾーンコントローラーを定義します。」.
   - 「**場所:** SharePoint の場合、SharePoint のルートレベルサイト、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、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. 「**Delivery Group Assignment** ページで、必要に応じてコネクタをデリバリーグループに割り当てます。または、**Configure > Delivery Groups** を使用してコネクタをデリバリーグループに関連付けることもできます。」.

「



」

1. 「**Summary** 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、**Back** をクリックします。」.
2. 「**Save** 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. 「Citrix Files クライアントをラップするときは、次の操作を行います。」:

    - 「ネットワークアクセスポリシーを **内部ネットワークにトンネル接続** に設定します。」.

    「この動作モードでは、XenMobile MDX フレームワークが Citrix Files クライアントからのすべてのネットワークトラフィックを傍受します。トラフィックは、アプリ固有のマイクロ VPN を使用して Citrix 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 **トンネル接続 - Web SSO** に設定します。」.

    「このトンネル接続モードでは、MDX フレームワークが MDX アプリからの SSL/HTTP トラフィックを終了します。その後、MDX はユーザーに代わって内部接続への新しい接続を開始します。このポリシー設定により、MDX フレームワークは Web サーバーによって発行された認証チャレンジを検出して応答できます。」.

    b. 「Citrix Files クライアントを XenMobile に追加します。詳細については、「Endpoint Management クライアント向け Citrix Files の統合と配信」を参照してください。」.

    c. 「サポートされているデバイスから、Citrix Files およびコネクタへのシングルサインオンを確認します。」.

以下のサンプルでは、SharefileDevはコネクタの名前です。

ShareFile構成(/en-us/xenmobile/server/media/connector-app-1.png)

ShareFile構成(/en-us/xenmobile/server/media/connector-app-2.png)

ストレージゾーンコネクタリストをフィルタリングする

コネクタの種類、割り当てられたデリバリーグループ、およびストレージゾーンで、ストレージゾーンコネクタのリストをフィルタリングできます。

1. **Configure > ShareFile** に移動し、**Show filter** をクリックします。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-storagezone-connectors-show-filter.png)

2. フィルタの見出しを展開して選択を行います。フィルタを保存するには、**Save This View** をクリックし、フィルタ名を入力して **Save** をクリックします。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-filter-storagezone-connectors.png)

3. フィルタの名前を変更または削除するには、フィルタ名の横にある矢印アイコンをクリックします。

   ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-save-filter.png)

Citrix Filesに切り替える

ストレージゾーンコネクタをXenMobileと統合した後、後で完全なEnterprise機能セットに切り替えることができます。Citrix Files機能セットを使用するには、XenMobile Advanced Edition (オンプレミス) またはCitrix Endpoint Management (クラウド) が必要です。XenMobileは、既存のストレージゾーンコネクタ統合設定を保持します。

Configure > ShareFile に移動し、**StorageZone Connectors** ドロップダウンメニューをクリックして、**Configure ShareFile Enterprise** をクリックします。

ShareFile構成(/en-us/xenmobile/server/media/configure-sharefile-switch-to-enterprise.png)

Citrix Files の構成に関する情報については、「SAML for single sign-on with Citrix Files」(/ja-jp/xenmobile/server/authentication/saml-sso-sharefile.html) を参照してください。

HDX™アプリ用SmartAccess

この機能を使用すると、デバイスのプロパティ、デバイスのユーザープロパティ、またはデバイスにインストールされている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。この機能は、自動アクションを設定してデバイスを非準拠としてマークし、そのデバイスへのアクセスを拒否することで使用します。この機能で使用されるHDXアプリは、非準拠デバイスへのアクセスを拒否するSmartAccessポリシーを使用して、Virtual Apps and Desktopsで構成されます。XenMobileは、署名され暗号化されたタグを使用して、デバイスのステータスをStoreFront™

に伝達します。その後、StoreFrontはアプリのアクセスコントロール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、展開環境で次のものが必要です。

- バーチャルアプリおよびデスクトップ 7.6
- StoreFront 3.7または3.8
- StoreFrontサーバーからHDXアプリを集約するように構成されたXenMobile® Server
- タグの署名と暗号化に使用されるSAML証明書で構成されたXenMobile Server。秘密鍵なしの同じ証明書がStoreFrontサーバーにアップロードされます。

この機能の使用を開始するには：

- XenMobile Server証明書をStoreFrontストアに構成する
- 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する
- XenMobileで自動アクションを設定する

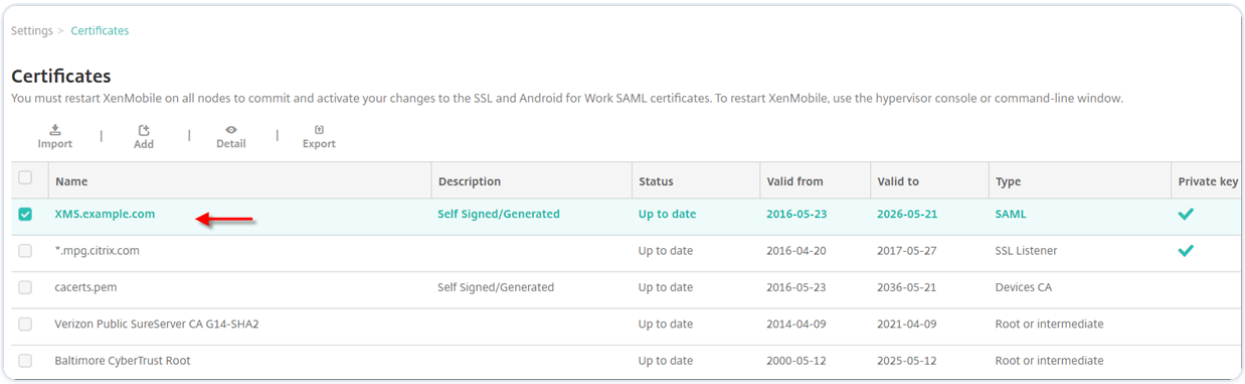
XenMobile Server証明書をエクスポートして構成し、StoreFrontストアにアップロードする

SmartAccessは、署名され暗号化されたタグを使用して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 Server証明書をStoreFrontストアに追加します。

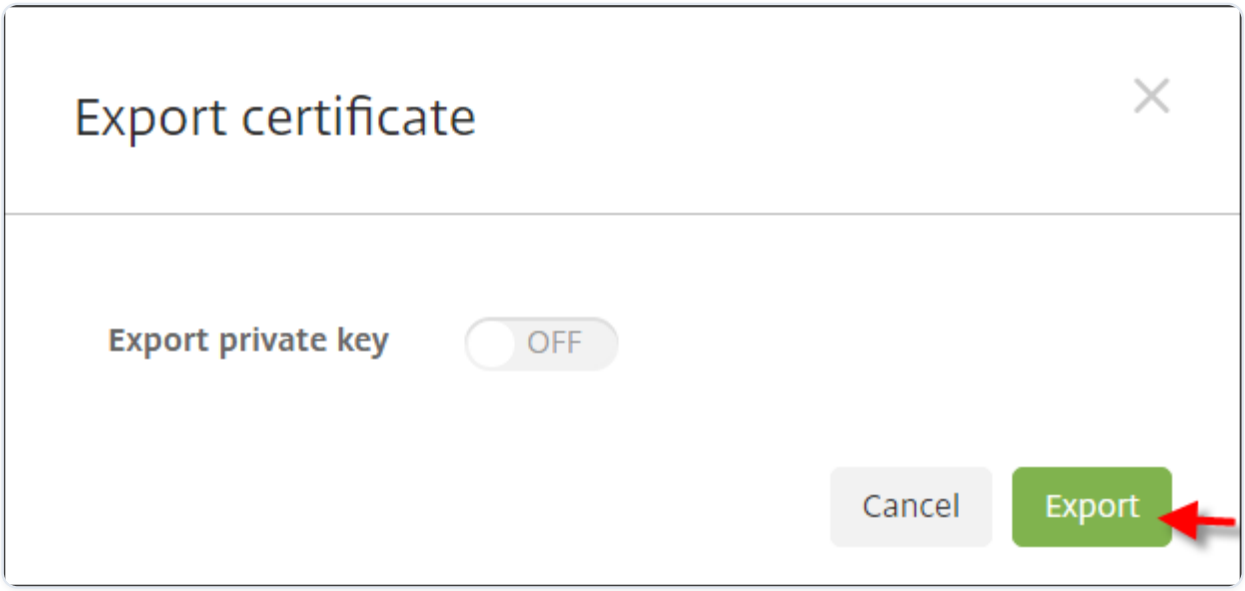
XenMobileでドメインおよび証明書ベースの認証が有効になっている場合のStoreFrontとXenMobileの統合の詳細については、サポート技術情報センターを参照してください。

XenMobile ServerからSAML証明書をエクスポートする

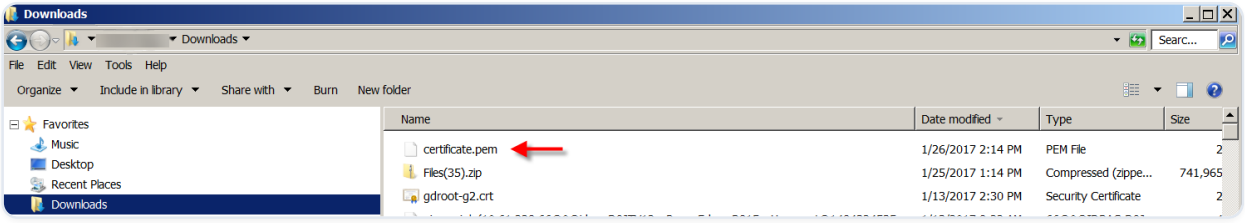
1. XenMobileコンソールで、右上隅の歯車アイコンをクリックします。**設定**ページが表示されます。**証明書**をクリックします。
2. XenMobile ServerのSAML証明書を見つけます。



3. **秘密キーのエクスポート**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。

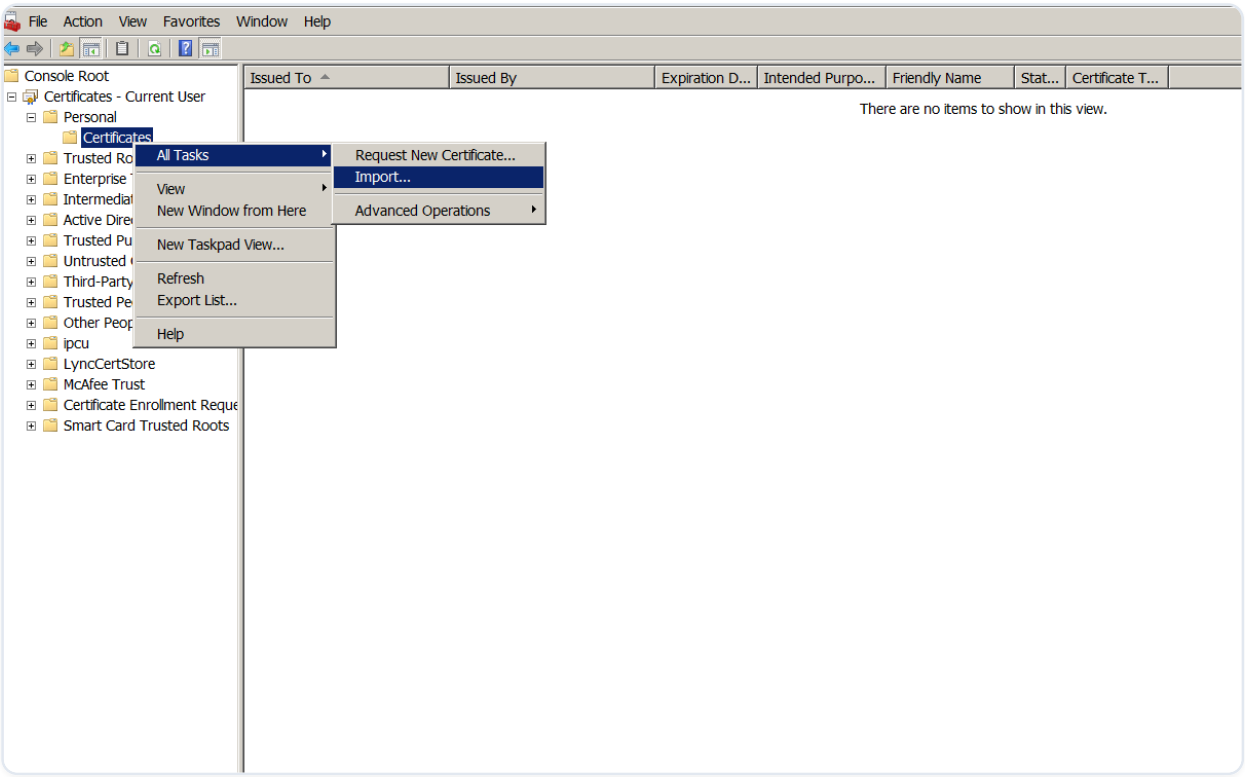


4. ダウンロードディレクトリにある証明書を見つけます。証明書はPEM形式です。



証明書をPEMからCERに変換する

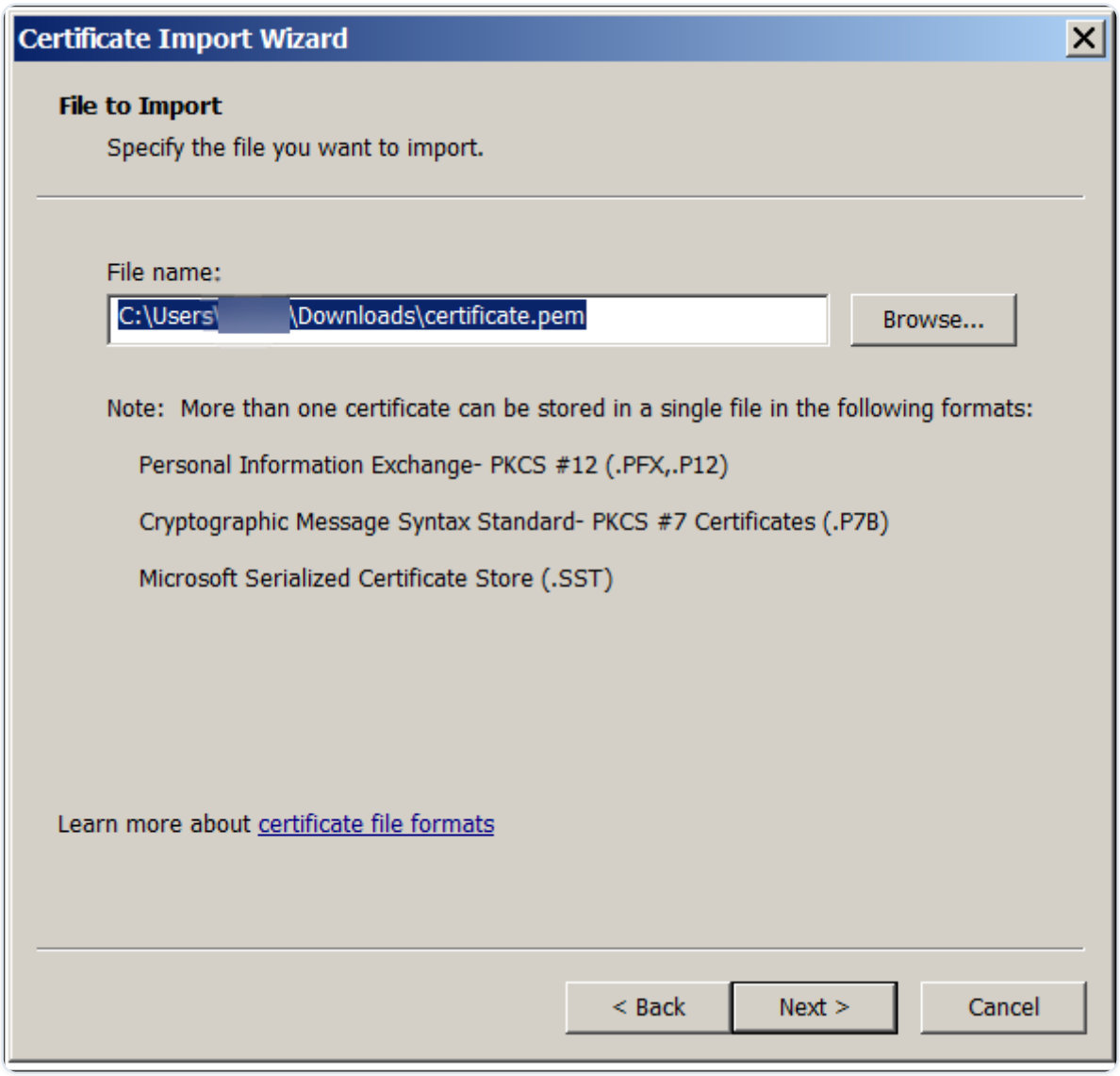
1. Microsoft管理コンソール (MMC) を開き、**証明書 > すべてのタスク > インポート**を右クリックします。



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にある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**を選択し、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。

   「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-import-certificate-store.png)

5. 選択内容を確認し、**完了**をクリックします。確認ウィンドウを閉じるには、**OK**をクリックします。
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**を選択します。

   「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-export-certificate.png)

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。

   「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-export-certificate-wizard.png)

8. 形式として**DER encoded binary X.509 (.CER)**を選択します。**次へ**をクリックします。

   「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-convert-certificate.png)

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。

「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-export-certificate-browse.png)

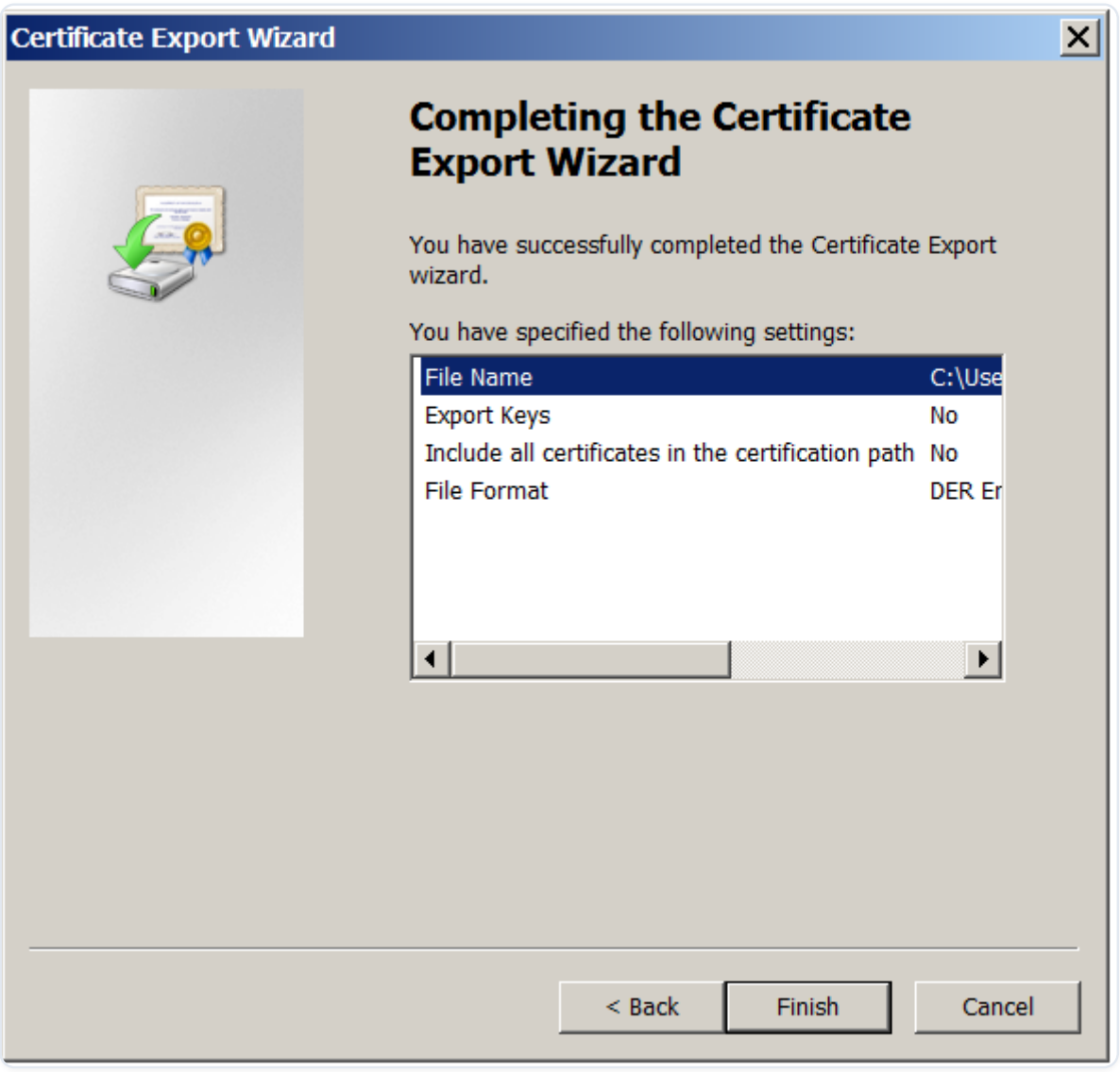
10. 証明書を保存します。

「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-export-certificate-save.png)

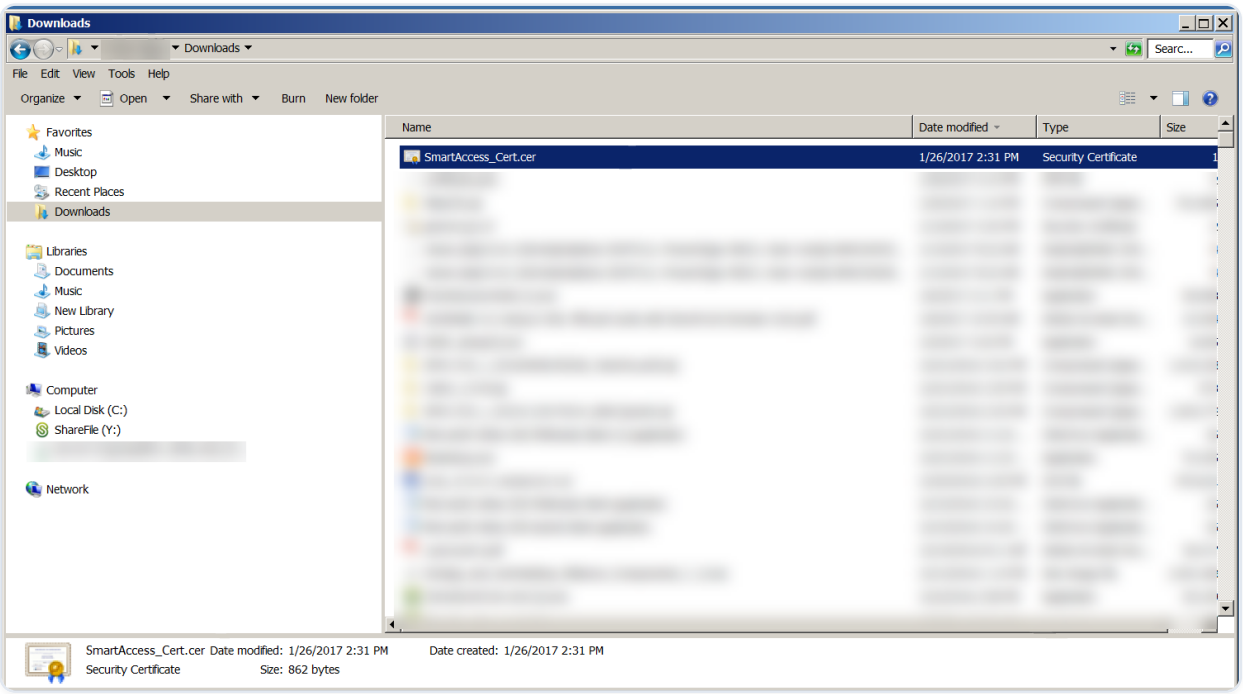
11. 証明書を参照し、**次へ**をクリックします。

「SmartAccess構成」(/en-us/xenmobile/server/media/mmc-export-certificate-browse.png)

12. 選択内容を確認し、**完了**をクリックします。確認ウィンドウを閉じるには、**OK**をクリックします。

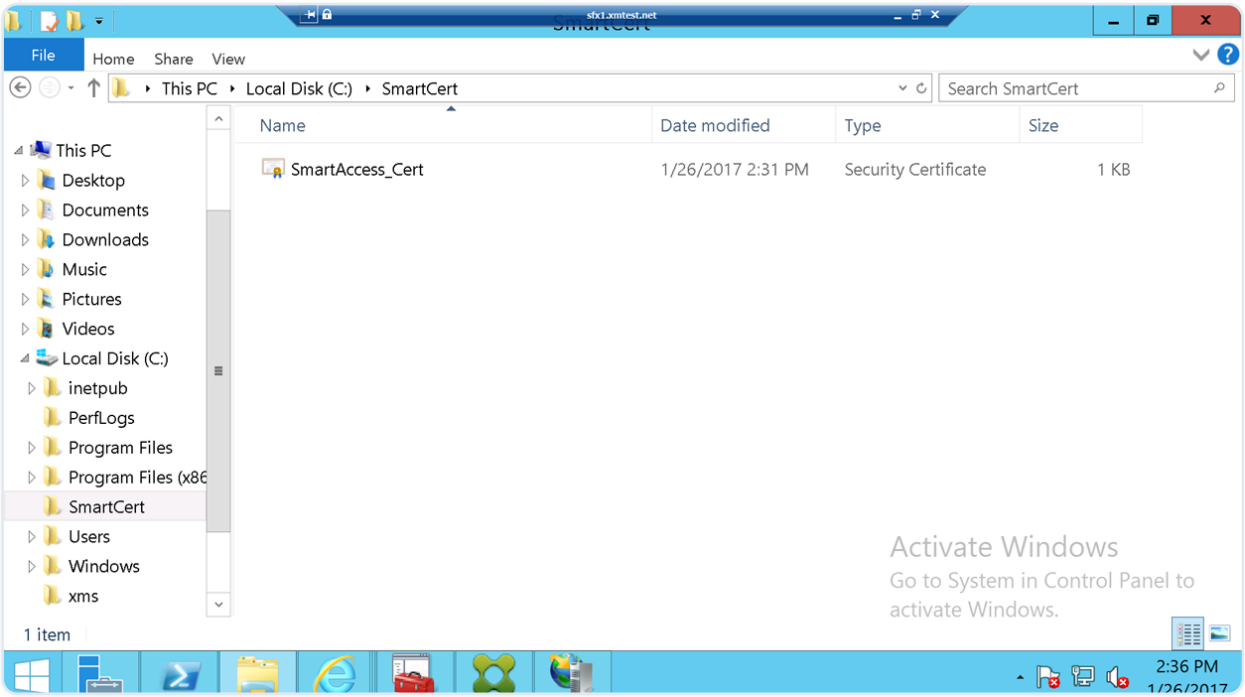


13. ダウンロードディレクトリで証明書を見つけます。証明書はCER形式です。



証明書をStoreFrontサーバーにコピーする

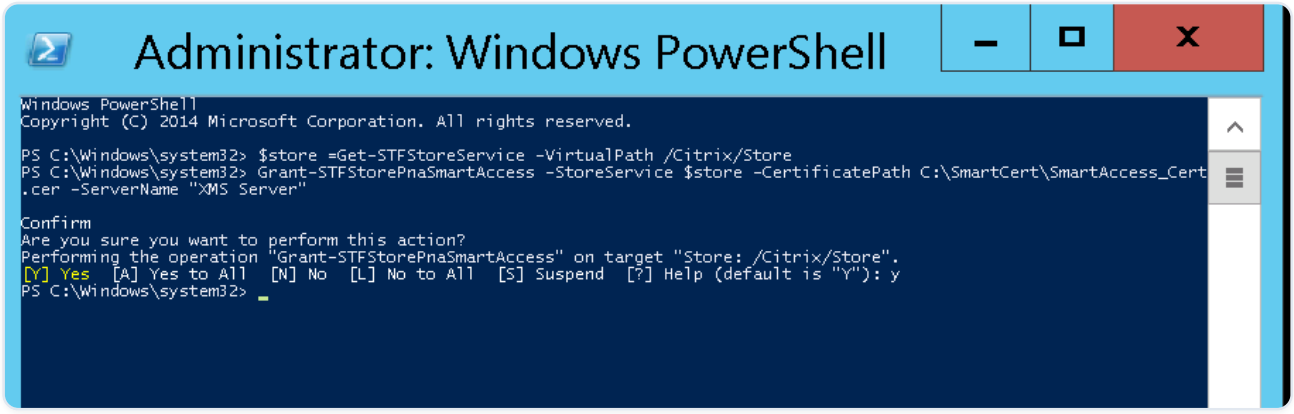
1. StoreFrontサーバーで、**SmartCert**という名前のフォルダーを作成します。
2. 証明書を**SmartCert**フォルダーにコピーします。



StoreFrontストアで証明書を構成する

StoreFrontサーバーで、このPowerShellコマンドを実行して、変換されたXenMobile Server証明書をストアに構成します。

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath  “C:\xms\xms.cer” –ServerName “XMS server”
```



StoreFrontストアに既存の証明書がある場合は、このPowerShellコマンドを実行してそれらを失効させます。

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```



または、StoreFrontサーバーで次のいずれかのPowerShellコマンドを実行して、StoreFrontストアの既存の証明書を失効させることもできます。

- 名前で失効:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server"
```

- サムプリントで失効:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store
```

```
    Revoke-STFStorePnaSmartAccess –StoreService $store –
CertificateThumbprint “ReplaceWithThumbprint”
```

- サーバーオブジェクトによる失効:

```
    $store = Get-STFStoreService –VirtualPath /Citrix/Store



    $access = Get-STFStorePnaSmartAccess –StoreService $store



    Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess
$access.AccessConditionsTrusts[0]
```

Virtual Apps and Desktops の SmartAccess ポリシーを構成する

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:

1. Virtual Apps and Desktops サーバーで、Citrix Studio を開きます。
2. Studio ナビゲーションペインで、**Delivery Groups** を選択します。
3. アクセスを制御するアプリを配信しているグループを選択します。次に、**Actions** ペインで **Edit Delivery Group** を選択します。
4. 「**アクセスポリシー**」ページで、「**NetScaler® Gateway 経由の接続**」と「**次のいずれかの条件を満たす接続**」を選択します。
5. **Add** をクリックします。
6. **Farm** が **XM** で、**Filter** が **XMCompliantDevice** であるアクセスポリシーを追加します。

   SmartAccess の構成(/en-us/xenmobile/server/media/delivery-group-app-desktop-access-policy.png)
7. 行った変更を適用してウィンドウを開いたままにするには **Apply** をクリックし、変更を適用してウィンドウを閉じるには **OK** をクリックします。

XenMobile で自動アクションを設定する

HDX アプリのデリバリーグループで設定した SmartAccess ポリシーは、デバイスが非準拠の場合、そのデバイスへのアクセスを拒否します。自動アクションを使用して、デバイスを非準拠としてマークします。

SmartAccess の構成(/en-us/xenmobile/server/media/actions-out-of-compliance.png)

1. XenMobile コンソールで、**Configure > Actions** をクリックします。**Actions** ページが表示されます。
2. アクションを追加するには、「**追加**」をクリックします。「**アクション情報**」ページが表示されます。
3. 「**アクション情報**」ページで、アクション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**」ページが表示されます。次の例では、ユーザープロパティ名が**eng5**または**eng6**であるデバイスを、即座に非準拠としてマークするトリガーが作成されます。

   SmartAccess構成(/en-us/xenmobile/server/media/configure-actions-trigger-example.png)
5. 「**トリガー**」リストで、「**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**」リストで:
   - 「**デバイスを非準拠としてマークする**」を選択します。
   - 「**次と等しい**」を選択します。
   - 「**True**」を選択します。
   - トリガー条件が満たされたときにデバイスを即座に非準拠としてマークするアクションを設定するには、時間枠を「**0**」に設定します。
7. このアクションを適用するXenMobileデリバリーグループを選択します。
8. アクションの概要を確認します。
9. 「**次へ**」をクリックし、その後「**保存**」をクリックします。

デバイスが非準拠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。ユーザーはアプリのサブスクライブを解除されます。デバイスに通知は送信されず、Secure Hubストアには、HDXアプリが以前利用可能であったことを示すものは何もありません。

デバイスが非準拠としてマークされたときにユーザーに通知したい場合は、通知を作成し、その通知を送信する自動アクションを作成します。

この例では、デバイスがコンプライアンス違反とマークされたときに、次の通知を作成して送信します: 「デバイスのシリアル番号または電話番号がデバイスポリシーに準拠しなくなり、HDXアプリケーションがブロックされました。」

SmartAccess構成(/en-us/xenmobile/server/media/secure-hub-notification-out-of-compliance.png)

デバイスがコンプライアンス違反と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、コンソールの右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
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**ページが表示されます。
3. **通知テンプレート**ページで、**追加**をクリックします。
4. 最初にSMSサーバーを設定するよう求められたら、**いいえ、後で設定します**をクリックします。

   SmartAccess構成(/en-us/xenmobile/server/media/notification-template-set-up-sms-server-later.png)
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の場合のエージェント通知
   - **種類:** アドホック通知
   - **Secure Hub:** アクティブ化済み
   - **メッセージ:** デバイス ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} はデバイスポリシーに準拠しなくなり、HDXアプリケーションはブロックされました。

   SmartAccess構成(/en-us/xenmobile/server/media/notification-template-settings.png)
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マークされたときに通知を送信するアクションを作成します

1. XenMobileコンソールから、「**構成 > アクション**」をクリックします。「**アクション**」ページが表示されます。
2. 「**追加**」をクリックしてアクションを追加します。「**アクション情報**」ページが表示されます。
3. 「**アクション情報**」ページで、アクション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ため、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**」ページが表示されます。
5. 「**トリガー**」リストで、次のようにします。
   - 「**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。
   - 「**である**」を選択します。
   - 「**True**」を選択します。

   SmartAccess構成(/en-us/xenmobile/server/media/configure-actions-details-example.png)
6. 「**アクション**」リストで、トリガーが満たされたときに発生するアクションを指定します。
   - 「**通知を送信**」を選択します。
   - 「**HDXアプリケーションブロック、作成した通知**」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たときに通知が送信されます。
7. このアクションを適用するXenMobileデリバリーグループを選択します。この例では、「**AllUsers**」を選択します。
8. アクションの概要を確認します。
9. 「**次へ**」をクリックし、次に「**保存**」をクリックします。

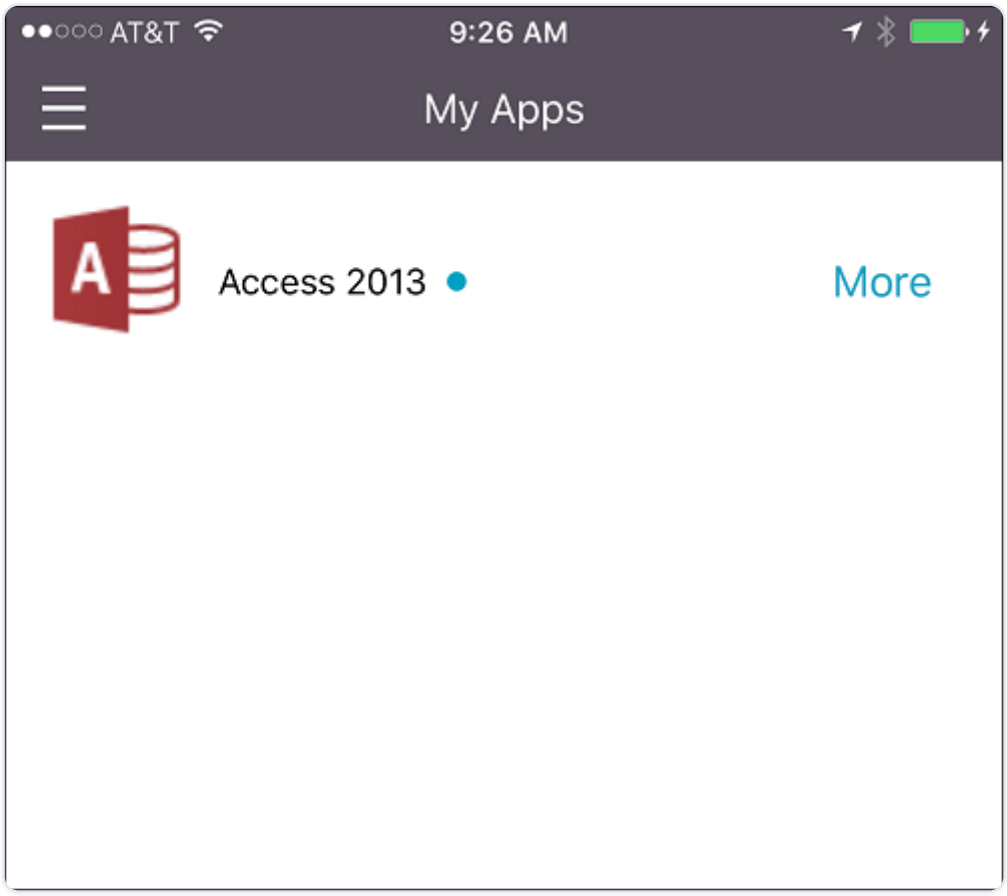
自動アクションの設定の詳細については、自動アクションを参照してください。

ユーザーがHDXアプリへのアクセスを回復する方法

デバイスがコンプライアンスに準拠した状態に戻った後、ユーザーはHDXアプリに再度アクセスできるようになります。

1. デバイスでSecure Hubストアに移動し、ストア内のアプリを更新します。
2. アプリに移動し、アプリに「**追加**」をタップします。

アプリが追加されると、新しくインストールされたアプリであるため、マイアプリに青い点が付いて表示されます。


AT&T
9:26 AM
My Apps
Access 2013
More

メディアを追加

ユーザーデバイスにメディアを展開できるように、XenMobile®にメディアを追加します。Appleボリューム購入を通じて入手したApple Booksを展開するためにXenMobileを使用できます。

XenMobileでボリューム購入アカウントを設定すると、購入済みおよび無料のブックが**Configure > Media**に表示されます。**Media**ページから、デリバリーグループを選択し、展開ルールを指定することで、iOSデバイスに展開するブックを設定します。

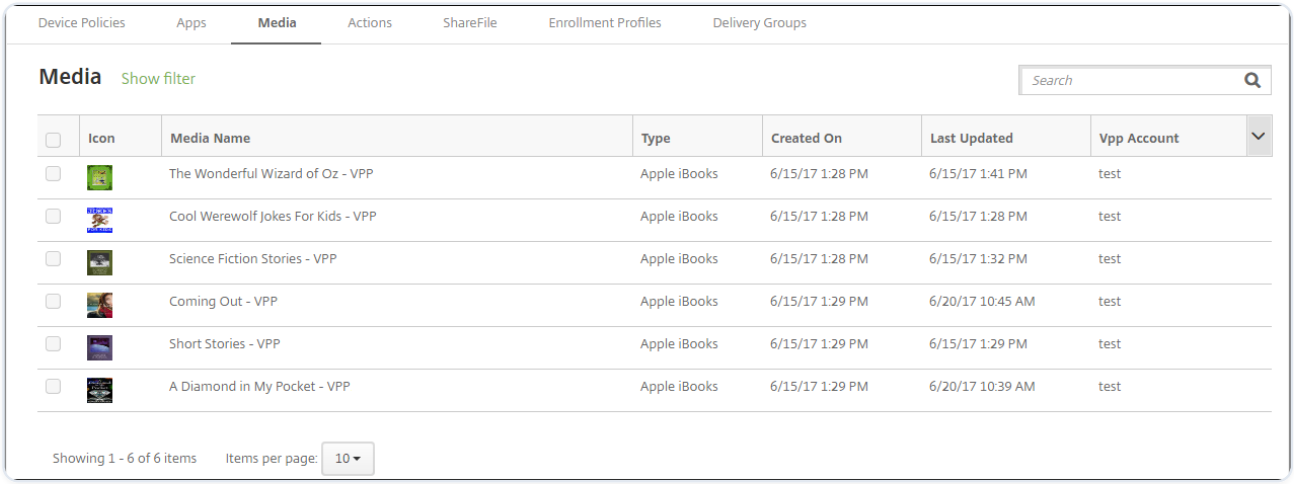
ユーザーが初めてブックを受け取り、ボリューム購入ライセンスを承諾すると、展開されたブックがデバイスにインストールされます。ブックはApple Bookアプリに表示されます。ブックライセンスをユーザーから関連付け解除したり、デバイスからブックを削除したりすることはできません。XenMobileは、必須メディアとしてブックをインストールします。ユーザーがデバイスからインストール済みのブックを削除しても、ブックはApple Bookアプリに残っており、ダウンロード可能です。

前提条件

- iOSデバイス
- Apple Volume Purchaseで説明されているように、XenMobileでAppleボリューム購入を設定します。

ブックの構成

ボリューム購入を通じて入手したApple Booksは、**Configure > Media**ページに表示されます。



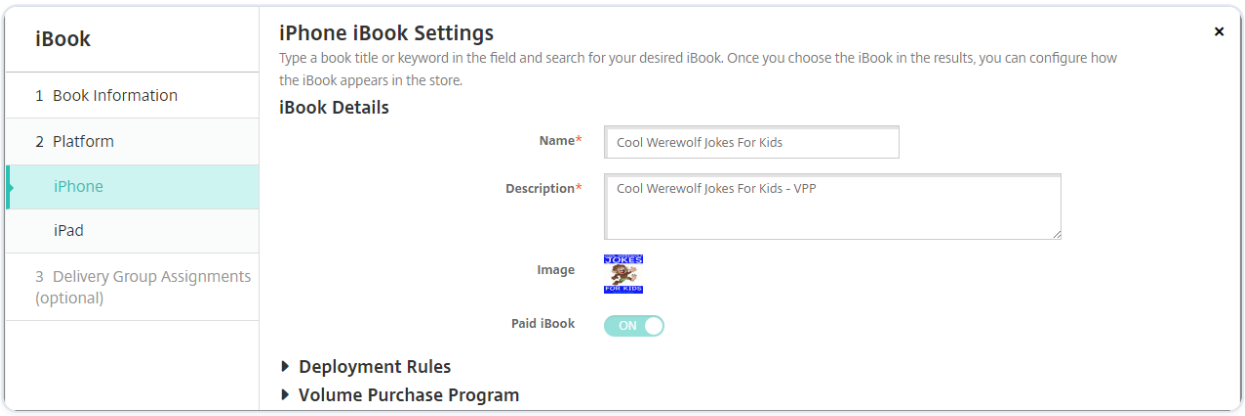
展開するApple Bookを構成するには

1. **Configure > Media**で、ブックを選択し、**Edit**をクリックします。**Book Information**ページが表示されます。

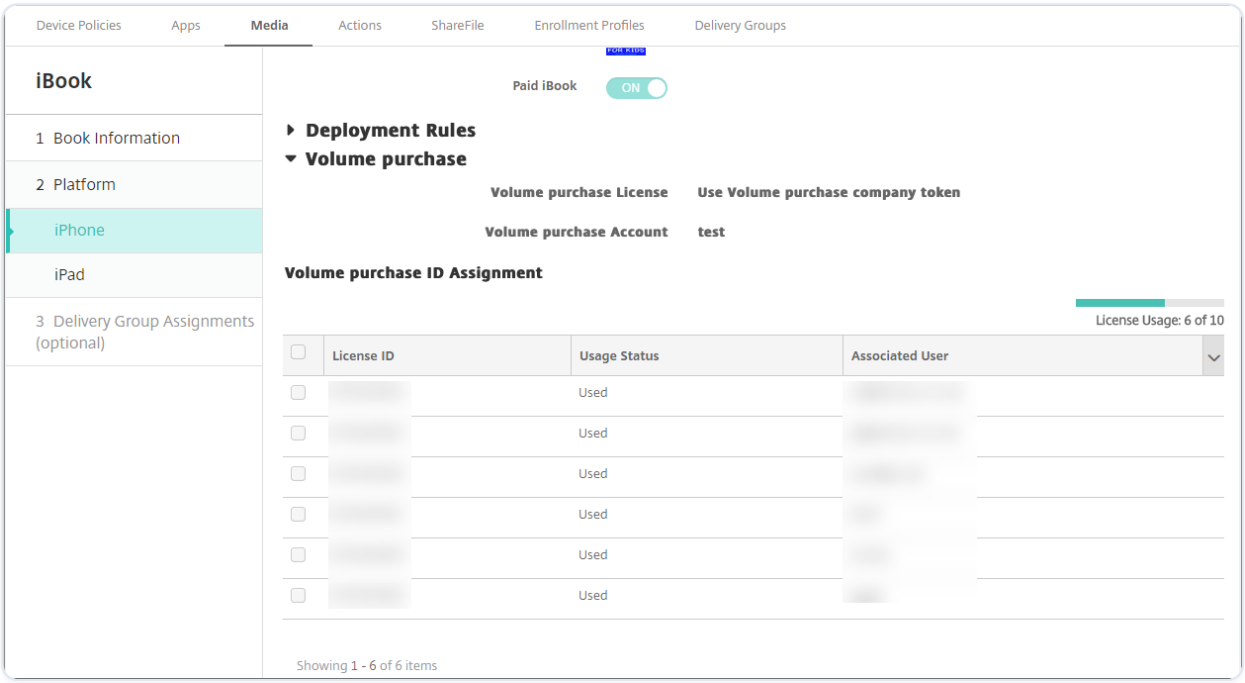


Nameと**Description**は、XenMobileコンソールとログにのみ表示されます。

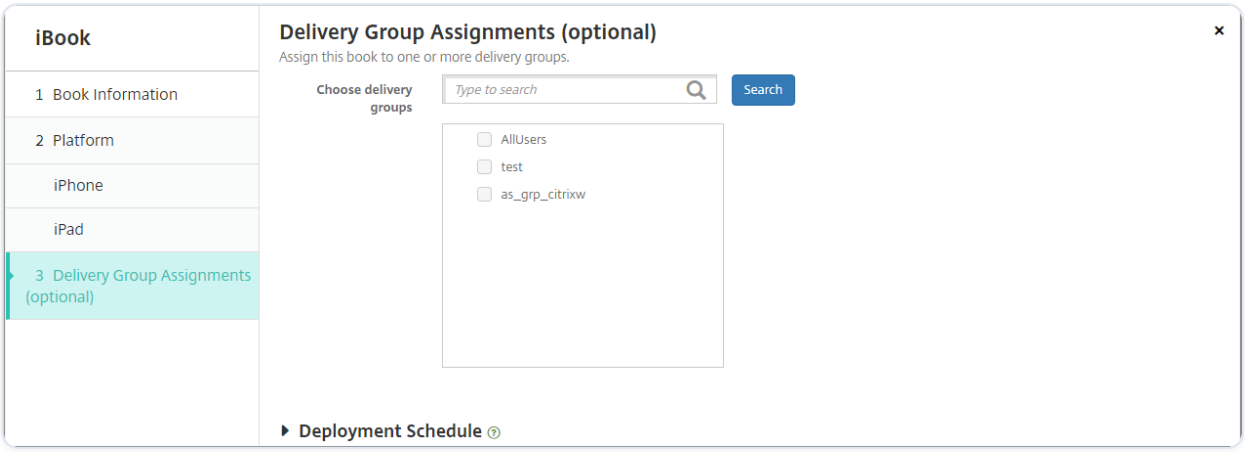
2. **iPhone iBook Settings**および**iPad iBook Settings**ページで: ブックの名前と説明は任意で変更できますが、Citrix®はこれらの設定を変更しないことを推奨します。画像は情報提供のみを目的としており、編集できません。**Paid iBook**は、ブックがAppleボリューム購入を通じて購入されたことを示します。



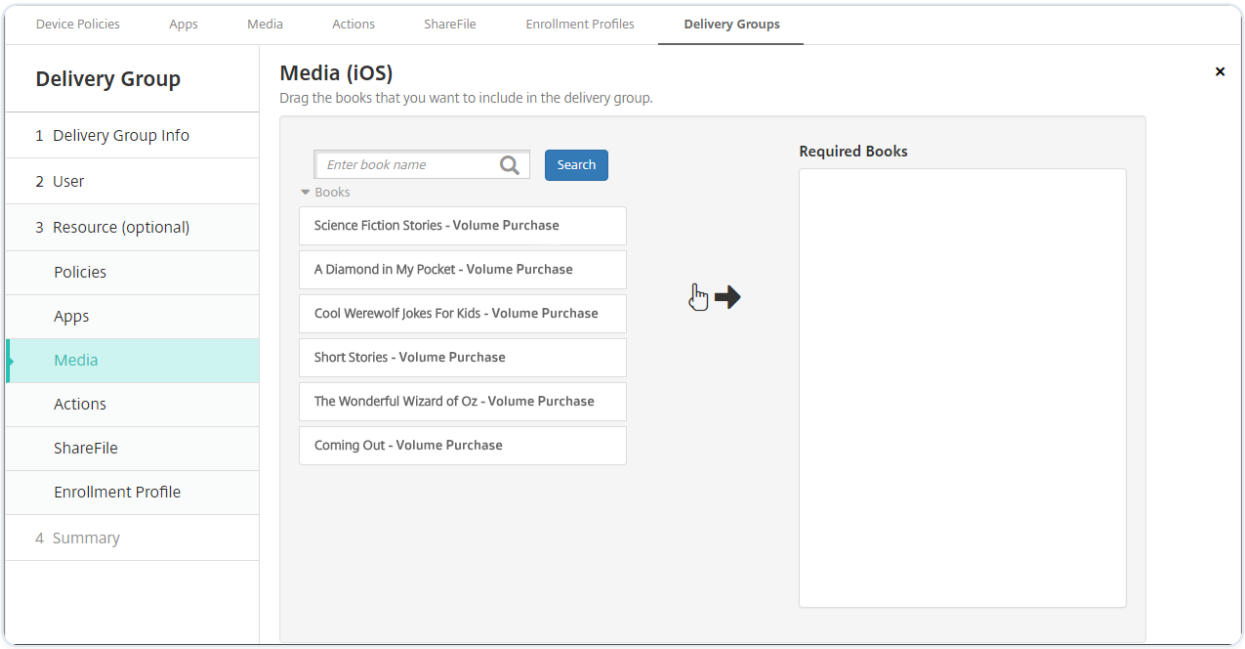
展開ルールを指定したり、ボリューム購入情報を表示したりすることもできます。



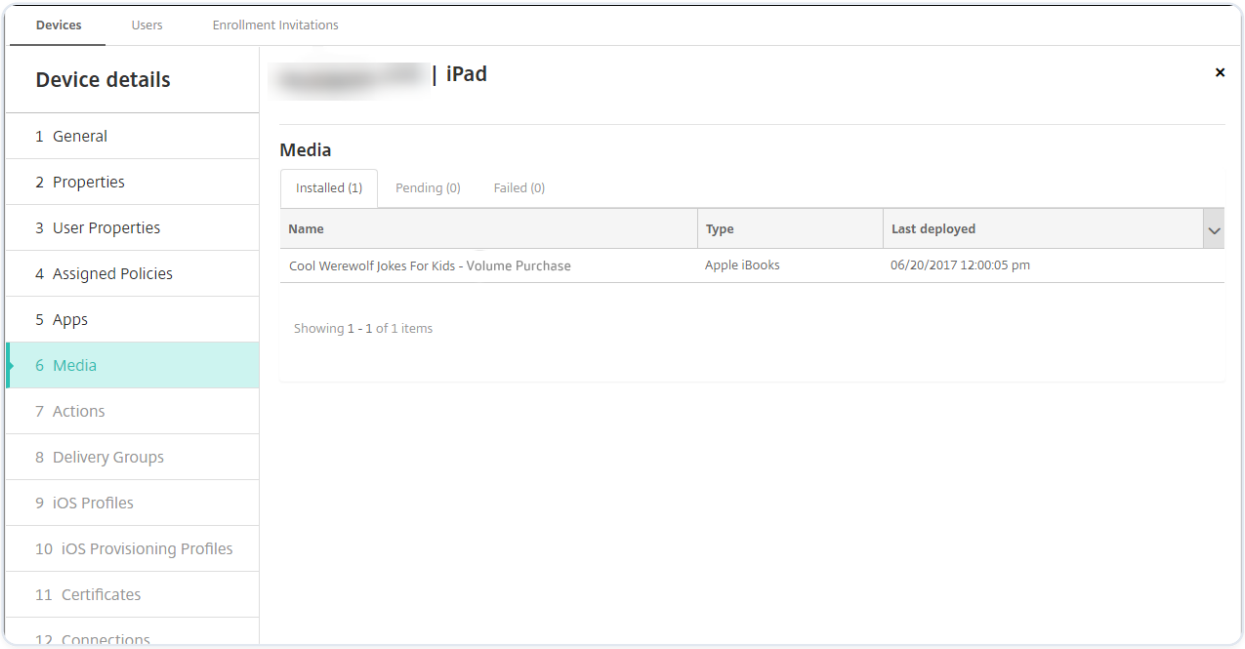
3. 必要に応じて、ブックを配信グループに割り当て、展開スケジュールを設定します。



Configure > Delivery Groups の **メディア** タブから、ブックを配信グループに割り当てることもできます。XenMobile は、必須のブック展開のみをサポートしています。



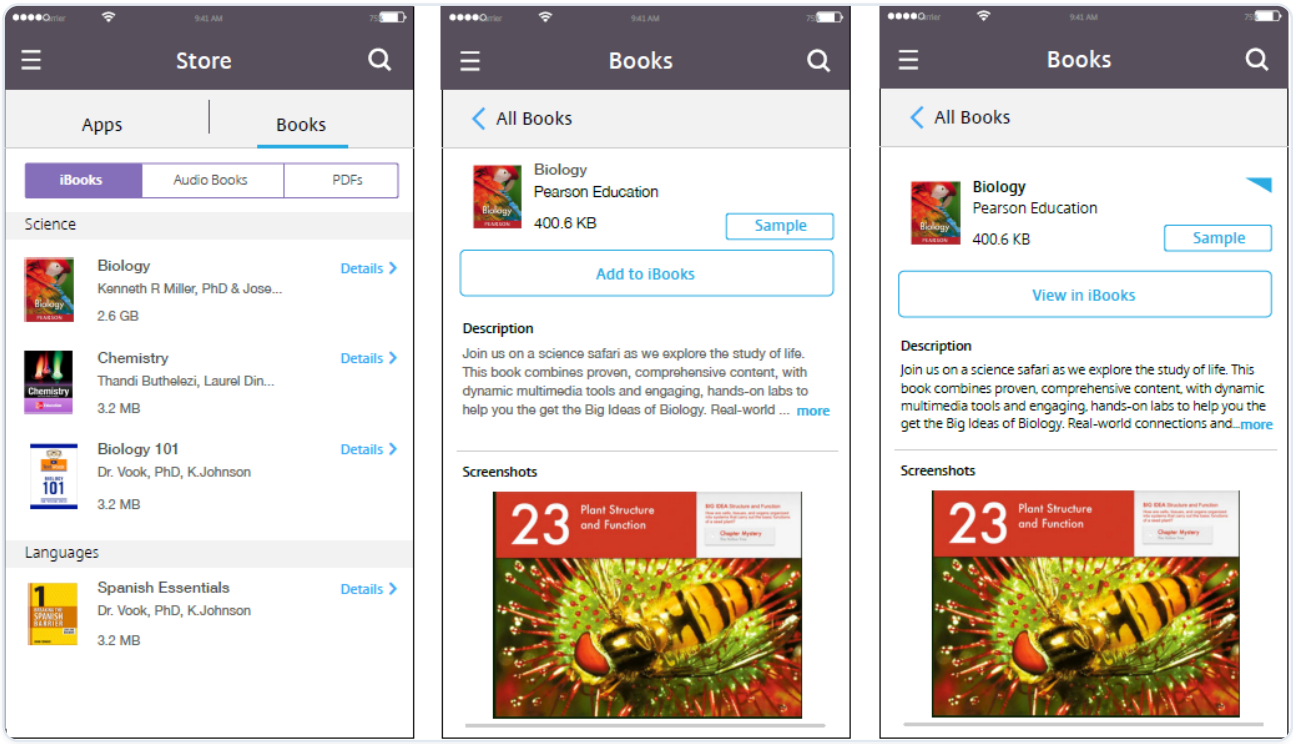
4. **Manage > Devices** の **メディア** タブを使用して、展開ステータスを表示します。



注：

Configure > Media ページで、ブックを選択して **削除** をクリックすると、XenMobile はリストからブックを削除します。ただし、XenMobile が次回 Apple ボリューム購入と同期するときに、Apple ボリューム購入から削除されていない限り、ブックはリストに再表示されます。リストからブックを削除しても、デバイスからブックは削除されません。

ブックは、次の例に示すようにユーザーデバイスに表示されます。


Store
Apps
Books
iBooks
Audio Books
PDFs
Science
Biology
Kenneth R Miller, PhD & Jose...
2.6 GB
Details
Chemistry
Thandi Buthelezi, Laurel Din...
3.2 MB
Details
Biology 101
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Languages
Spanish Essentials
Dr. Vook, PhD, K.Johnson
3.2 MB
Details
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
Add to iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world ... more
Screenshots
23
Plant Structure and Function
Books
All Books
Biology
Pearson Education
400.6 KB
Sample
View in iBooks
Description
Join us on a science safari as we explore the study of life. This book combines proven, comprehensive content, with dynamic multimedia tools and engaging, hands-on labs to help you the get the Big Ideas of Biology. Real-world connections and...more
Screenshots
23
Plant Structure and Function

リソースの展開

デバイスの構成と管理には通常、XenMobile® コンソールでリソース（ポリシー、アプリ、メディア）とアクションを作成し、デリバリーグループを使用してそれらをパッケージ化する作業が含まれます。XenMobileがデリバリーグループ内のリソースとアクションをデバイスにプッシュする順序は、展開順序と呼ばれます。この記事では、次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、展開する方法
- デリバリーグループ内のリソースとアクションの展開順序を変更する方法
- ユーザーが重複または競合するポリシーを持つ複数のデリバリーグループに属している場合に、XenMobileが展開順序を決定する方法.

デリバリーグループは、ポリシー、アプリ、メディア、およびアクションの組み合わせを展開するデバイスを持つユーザーのカテゴリを指定します。デリバリーグループへの組み込みは、通常、会社、国、部署、勤務先住所、役職などのユーザー特性に基づいています。デリバリーグループを使用すると、誰がどのリソースをいつ取得するかをより詳細に制御できます。デリバリーグループを全員に展開することも、より限定されたユーザーグループに展開することもできます。

デリバリーグループへの展開とは、サポートされているiOS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です。これらのユーザーは、XenMobileに再接続するために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、およびアクションを展開できます。

Androidデバイスを使用しているユーザーの場合：すでに接続されている場合は、すぐにリソースを受け取ります。そうでない場合は、スケジューリングポリシーに基づいて、次回接続時にリソースを受け取ります。

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。これには、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グループを削除することはできませんが、すべてのユーザーにリソースをプッシュしたくない場合は、グループを無効にすることができます。

展開順序

展開順序とは、XenMobileがリソースをデバイスにプッシュする順序のことです。展開順序は、デバイス管理（MDM）用に構成された登録プロファイルを持つデリバリーグループ内のデバイスにのみ適用されます。

展開順序を決定する際、XenMobileは展開ルールや展開スケジュールなどのフィルターと制御基準をリソースに適用します。リソースには、ポリシー、アプリ、アクション、デリバリーグループが含まれます。デリバリーグループを追加する前に、このセクションの情報が展開目標にどのように関連するかを検討してください。

展開順序に関連する主要な概念の概要を以下に示します。

- **展開順序：** XenMobileがリソース（ポリシー、アプリ、メディア）とアクションをデバイスにプッシュする順序。利用規約やソフトウェアインベントリなどの一部のポリシーの展開順序は、他のリソースには影響しません。アクションが展開される順序は、他のリソースには影響しません。したがって、XenMobileがリソースを展開する際には、それらの位置は無視されます。
- **展開ルール：** XenMobileは、デバイスプロパティに指定した展開ルールを使用して、ポリシー、アプリ、メディア、アクション、およびデリバリーグループをフィルター処理します。たとえば、展開ルールでは、ドメイン名が特定の値と一致する場合に展開パッケージをプッシュするように指定できます。
- **展開スケジュール:** XenMobileは、ポリシー、アプリ、メディア、およびアクションに指定した展開スケジュールを使用して、それらのアイテムの展開を制御します。展開は即時、特定の日時、または展開条件に従って行われるように指定できます。

次の表は、さまざまなオブジェクトおよびリソースタイプのフィルターと制御基準を示しています。展開ルールはデバイスのプロパティに基づいています。

オブジェクト/リソース	デバイスプラットフォーム	展開ルール	展開スケジュール	ユーザー/グループ
デバイスポリシー	Y	Y	Y	-
アプリ	Y	Y	Y	-
メディア	Y	Y	Y	-
アクション	-	Y	Y	-

オブジェクト/リソース	デバイスプラットフォーム	展開ルール	展開スケジュール	ユーザー/グループ
デリバリーグループ	-	Y	-	Y

一般的な環境では、複数のデリバリーグループが1人のユーザーに割り当てられる可能性が高く、その結果として以下の状況が考えられます。

- デリバリーグループ内に重複するオブジェクトが存在する。
- 特定のポリシーが、ユーザーに割り当てられている複数のデリバリーグループで異なる設定になっている。

これらの状況のいずれかが発生した場合、XenMobileはデバイスに配信または適用する必要があるすべてのオブジェクトの展開順序を計算します。計算手順はデバイスプラットフォームに依存しません。

計算手順

1. ユーザー、グループ、および展開ルールのフィルターに基づいて、特定のユーザーに対するすべてのデリバリーグループを決定します。
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、アクション）の順序付きリストを作成します。このリストは、デバイスプラットフォーム、展開ルール、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。順序付け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序を持つデリバリーグループのリソースを、ユーザー定義の展開順序を持たないデリバリーグループのリソースよりも前に配置します。この配置の根拠は、これらの手順の後に説明します。

    b. デリバリーグループ間のタイブレーカーとして、デリバリーグループ名でデリバリーグループの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のリソースよりも前に配置します。

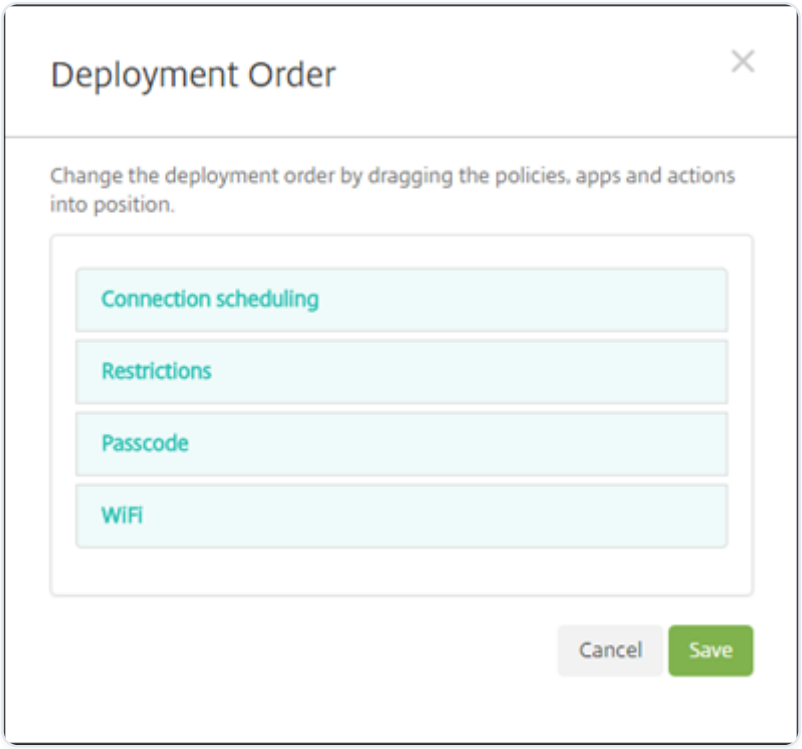
    c. ソート中に、デリバリーグループのリソースに対してユーザー定義の展開順序が指定されている場合は、その順序を維持します。それ以外の場合は、そのデリバリーグループ内のリソースをリソース名でソートします。

    d. 同じリソースが複数回出現する場合は、重複するリソースを削除します。

ユーザー定義の順序が関連付けられているリソースは、ユーザー定義の順序がないリソースよりも先に展開されます。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できます。上記の手順で示されているように、計算アルゴリズムは冗長なリソースを削除し、このリストの最初のリソースのみを配信します。このように重複するリソースを削除することで、XenMobileはXenMobile管理者が定義した順序を適用します。

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、アカウントマネージャー 1: リソースの順序が**指定されていない**。ポリシーの**WiFi**と**パスコード**が含まれています。
- デリバリーグループ、アカウントマネージャー 2: リソースの順序が**指定されている**。ポリシーの**接続スケジューリング**、**制限**、**パスコード**、および**WiFi**が含まれています。この場合、**パスコード**ポリシーを**WiFi**ポリシーより先に配信する必要があります。



計算アルゴリズムが展開グループを名前のみで順序付けした場合、XenMobileは、デリバリーグループ「アカウントマネージャー 1」から開始して、**WiFi**、**パスコード**、**接続スケジューリング**、および**制限**の順序で展開を実行します。XenMobileは、アカウントマネージャー 2デリバリーグループからの重複する**パスコード**と**WiFi**の両方を無視します。

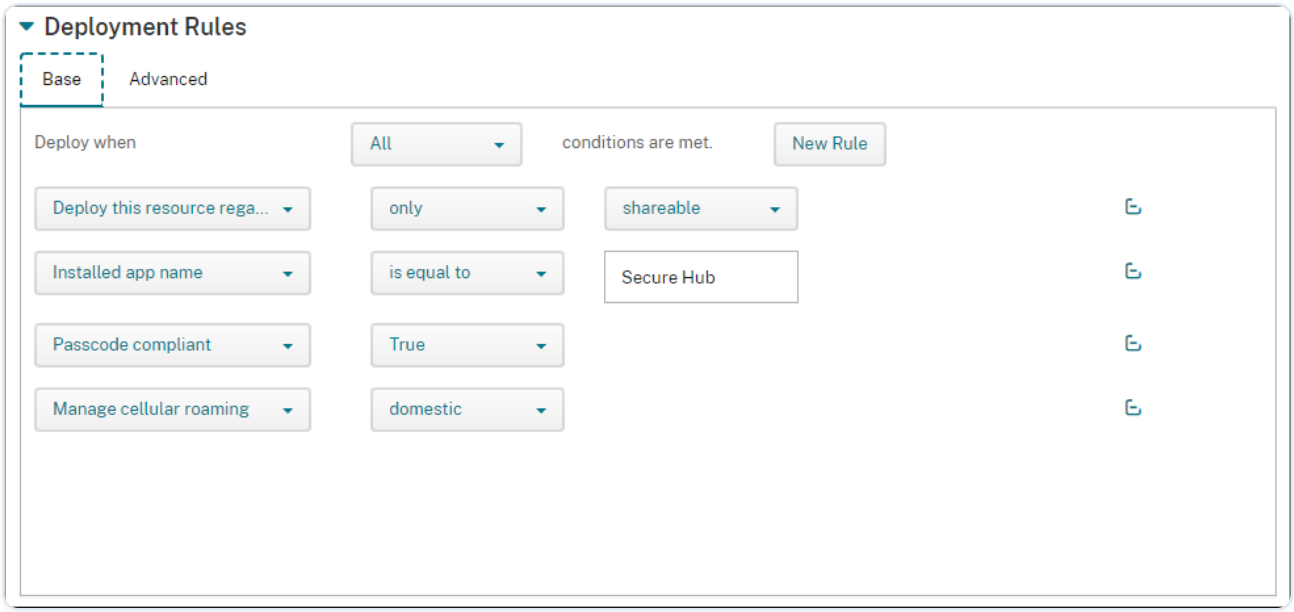
ただし、アカウントマネージャー 2グループには管理者が指定した展開順序があります。したがって、計算アルゴリズムは、アカウントマネージャー 2デリバリーグループのリソースを、他のデリバリーグループのリソースよりもリストの上位に配置します。その結果、XenMobileはポリシーを**接続スケジューリング**、**制限**、**パスコード**、および**WiFi**の順序で展開します。XenMobileは、アカ

ウントマネージャー 1デリバリーグループからの**WiFi**と**パスコード**のポリシーを、重複しているため無視します。そのため、このアルゴリズムはXenMobile管理者が指定した順序を尊重します。

展開ルール

特定の条件が存在する場合にのみリソースを配信するように展開ルールを構成します。基本または高度な展開ルールを構成できます。

基本エディターを使用して展開ルールを追加する場合、まず、リソースを展開するタイミングを選択します。



- **すべて:** ユーザーまたはデバイスが構成したすべての条件を満たした場合にリソースを配信します。
- **いずれか:** ユーザーまたはデバイスが構成した条件の少なくとも1つを満たした場合にリソースを配信します。

新しいルールをクリックして条件を追加します。ルールは、展開されるリソースと、リソースを構成するプラットフォームによって異なります。いくつかの種類のルールが存在します。リソースを展開するように選択できます。

- 選択したプロパティが存在する場合のみ、または選択したプロパティが存在する場合を除く。
- プロパティが入力したテキストと完全に一致する場合、プロパティが入力したテキストを含む場合、またはプロパティが入力したテキストと一致しない場合。
- デバイスまたはユーザーが選択したプロパティに準拠している場合、または選択したプロパティに準拠していない場合。
- デバイスまたはユーザーのプロパティが、定義済みリストから選択した条件と一致する場合。

より複雑な展開ルールを作成するには、詳細エディターを使用します。選択できるルールはさらに多く、詳細ルールを作成する際にさまざまなブール論理演算子を組み合わせることができます。

展開ルールの詳細構成(/en-us/xenmobile/server//media/deployment-rules-advanced.png)

デリバリーグループを追加するには

Citrix®では、デバイスポリシーと登録プロファイルを作成する前に、デリバリーグループを作成することをお勧めします。

1. コンソールで、 > の順にクリックします。
2. ページで、 をクリックします。
3. ページで、デリバリーグループの名前と説明を入力し、 をクリックします。

   ユーザーが異なる登録プロファイルを持つ複数のデリバリーグループに属している場合、デリバリーグループの名前によって使用される登録プロファイルが決まります。XenMobileは、デリバリーグループのアルファベット順リストで最後に表示されるデリバリーグループを選択します。詳しくは、「登録プロファイル」を参照してください。
4. ページで、デリバリーグループのユーザー割り当てを管理する方法を指定します。

   デリバリーグループ構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-assignments.png)

   > **重要：**
   >
   > ユーザーグループの作成後、 設定を変更することはできません。

   - **ドメインの選択：** リストから、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：** 次のいずれかを実行します。
     - ユーザーグループのリストで、追加するグループをクリックします。選択したグループは、**選択されたユーザーグループ**のリストに表示されます。
     - 選択したドメイン内のすべてのユーザーグループのリストを表示するには、**検索**をクリックします。
     - 検索ボックスにグループ名の全部または一部を入力し、**検索**をクリックしてユーザーグループのリストを絞り込みます。

選択されたユーザーグループのリストからユーザーグループを削除するには、次のいずれかを実行します。

- **選択されたユーザーグループ**のリストで、削除する各グループの横にある**X**をクリックします。
- 選択したドメイン内のすべてのユーザーグループのリストを表示するには、**検索**をクリックします。リストをスクロールし、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。
- 検索ボックスにグループ名の全部または一部を入力し、**検索**をクリックしてユーザーグループのリストを絞り込みます。リストをスクロールし、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:** リソースがユーザーに展開されるために、ユーザーがいずれかのグループに属している必要があるか (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されていないユーザーに展開するかどうかを選択します。認証されていないユーザーとは、認証できなかったものの、デバイスのXenMobileへの接続を許可したユーザーです。

5. 展開ルールを構成します。
6. **次へ**をクリックします。**デリバリーグループリソース**ページが表示されます。ここでは、オプションでデリバリーグループのポリシー、アプリ、またはアクションを追加できます。この手順をスキップするには、**デリバリーグループ**の下にある**概要**をクリックして、デリバリーグループの構成の概要を表示します。

   リソースをスキップするには、**リソース (オプション)** の下で、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. 追加する各ポリシーについて、次の操作を行います。

   - 利用可能なポリシーのリストをスクロールして、追加するポリシーを見つけます。
   - または、ポリシーのリストを制限するには、検索ボックスにポリシーの完全な名前または部分的な名前を入力し、次に、**検索**をクリックします。
   - 追加するポリシーをクリックし、右側のボックスにドラッグします。

   ポリシーを削除するには、右側のボックスでポリシー名の横にある**X**をクリックします。

デリバリーグループ構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-policies.png)

2. **次へ**をクリックします。**アプリ**ページが表示されます。

アプリを追加するには

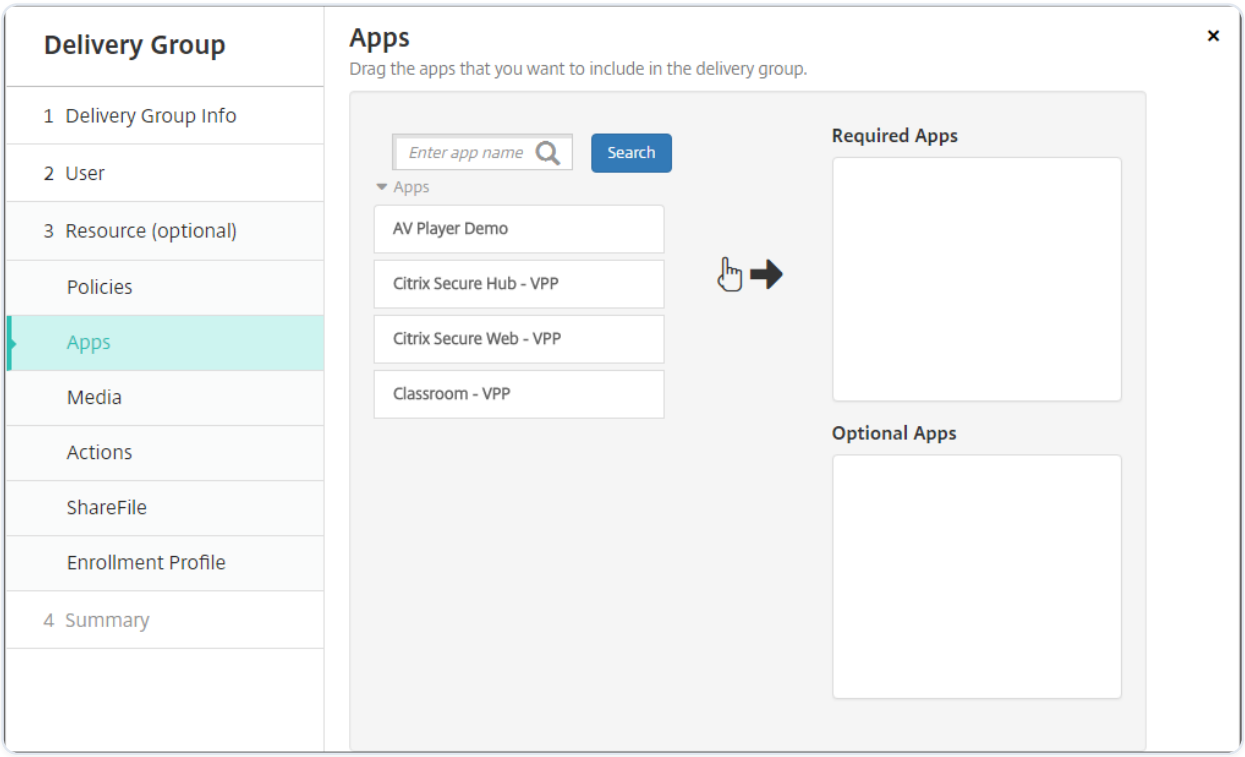
1. 追加する各アプリについて、次の操作を行います。

   - 利用可能なアプリのリストをスクロールして、追加するアプリを見つけます。
   - または、アプリのリストを制限するには、検索ボックスにアプリの完全な名前または部分的な名前を入力し、次に、**検索**をクリックします。
   - 追加するアプリをクリックし、**必須アプリ**ボックスまたは**オプションアプリ**ボックスのいずれかにドラッグします。

   必須としてマークされたアプリの場合、ユーザーは次のような状況で迅速に更新を受け取ることができます。

   - 新しいアプリをアップロードし、必須としてマークします。
   - 既存のアプリを必須としてマークします。
   - ユーザーが必須アプリを削除した場合。
   - Secure Hubの更新が利用可能です。

   必須アプリの強制展開に関する情報（機能の有効化方法を含む）については、「必須アプリとオプションアプリについて」を参照してください。



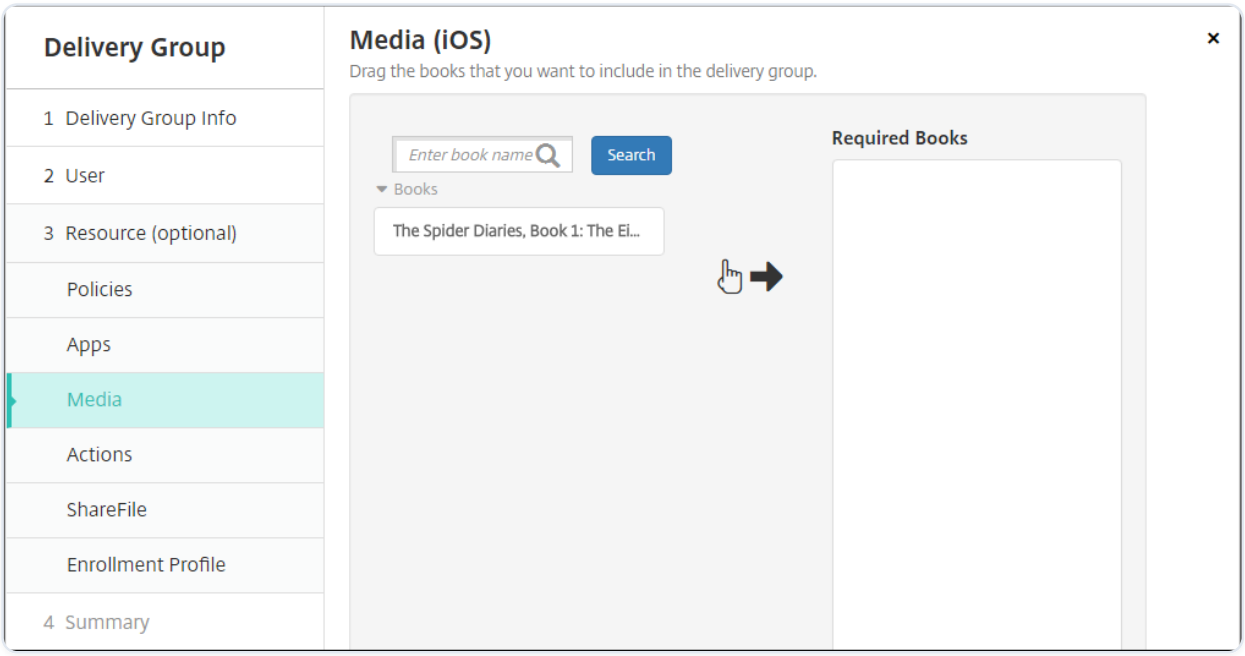
アプリを削除するには、右側のボックスでアプリ名の横にある**X**をクリックします。

2. **次へ**をクリックします。**メディア**ページが表示されます。

メディアを追加するには

1. 追加する各ブックについて、次の操作を行います。

   - 利用可能なブックのリストをスクロールして、追加するブックを見つけます。
   - または、ブックのリストを制限するには、検索ボックスにブックの完全な名前または部分的な名前を入力し、**検索**をクリックします。
   - 追加するブックをクリックし、**必須ブック**ボックスにドラッグします。



必須としてマークされたブックの場合、ユーザーは次のような状況で速やかに更新を受け取ります。

- 新しいブックをアップロードし、必須としてマークする。
- 既存のブックを必須としてマークする。
- ユーザーが必須ブックを削除した場合。
- Secure Hubのアップデートが利用可能になった場合。

本を削除するには、右側のボックスにある本名の横の**X**をクリックします。

2. **次へ**をクリックします。**アクション**ページが表示されます。

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、次の操作を行います。

   - 利用可能なアクションのリストをスクロールして、追加したいアクションを見つけます。
   - または、アクションのリストを絞り込むには、検索ボックスにアクションの完全な名前または部分的な名前を入力し、**検索**をクリックします。
   - 追加したいアクションをクリックし、右側のボックスにドラッグします。

   アクションを削除するには、右側のボックスにあるアクション名の横の**X**をクリックします。

   配信グループ構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-actions.png)

2. **次へ**をクリックします。**ShareFile**ページが表示されます。

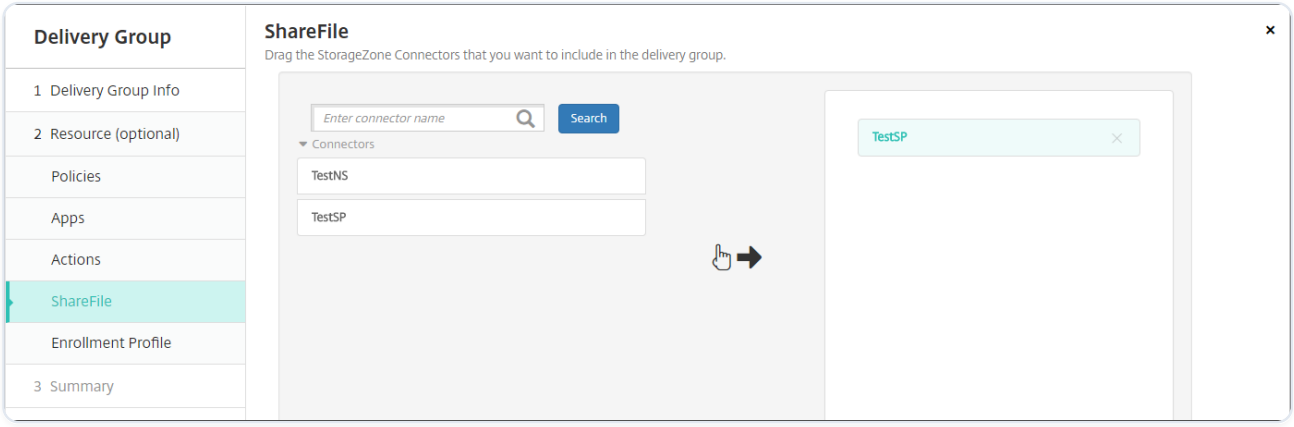
ShareFile構成を適用するには

ShareFileページは、XenMobile (**構成 > ShareFile**) をエンタープライズアカウント用に構成したか、ストレージゾーンコネクタ用に構成したかによって異なります。

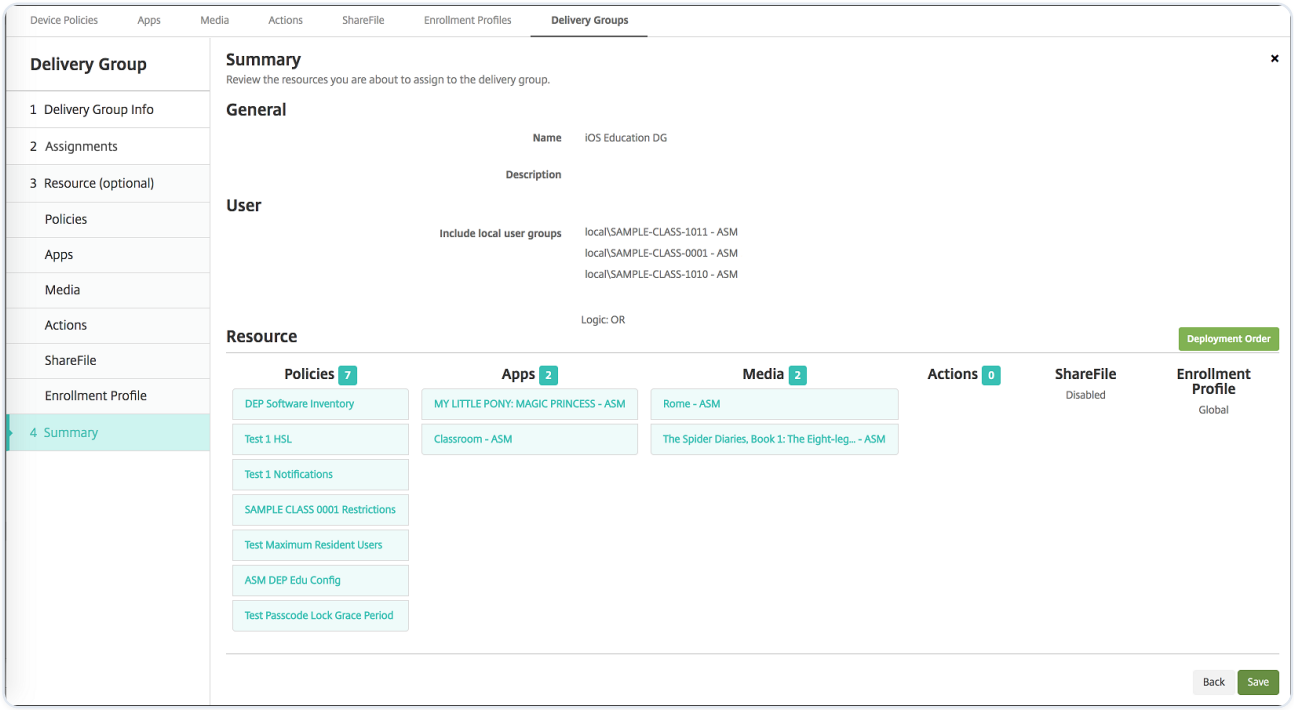
XenMobileで使用するエンタープライズアカウントを構成した場合: **ShareFileを有効にする**を**ON**に設定して、配信グループにShareFileコンテンツおよびデータへのシングルサインオンアクセスを提供します。

配信グループ構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-sharefile.png)

XenMobileで使用するストレージゾーンコネクタを構成した場合は、配信グループに含めるストレージゾーンコネクタを選択します。

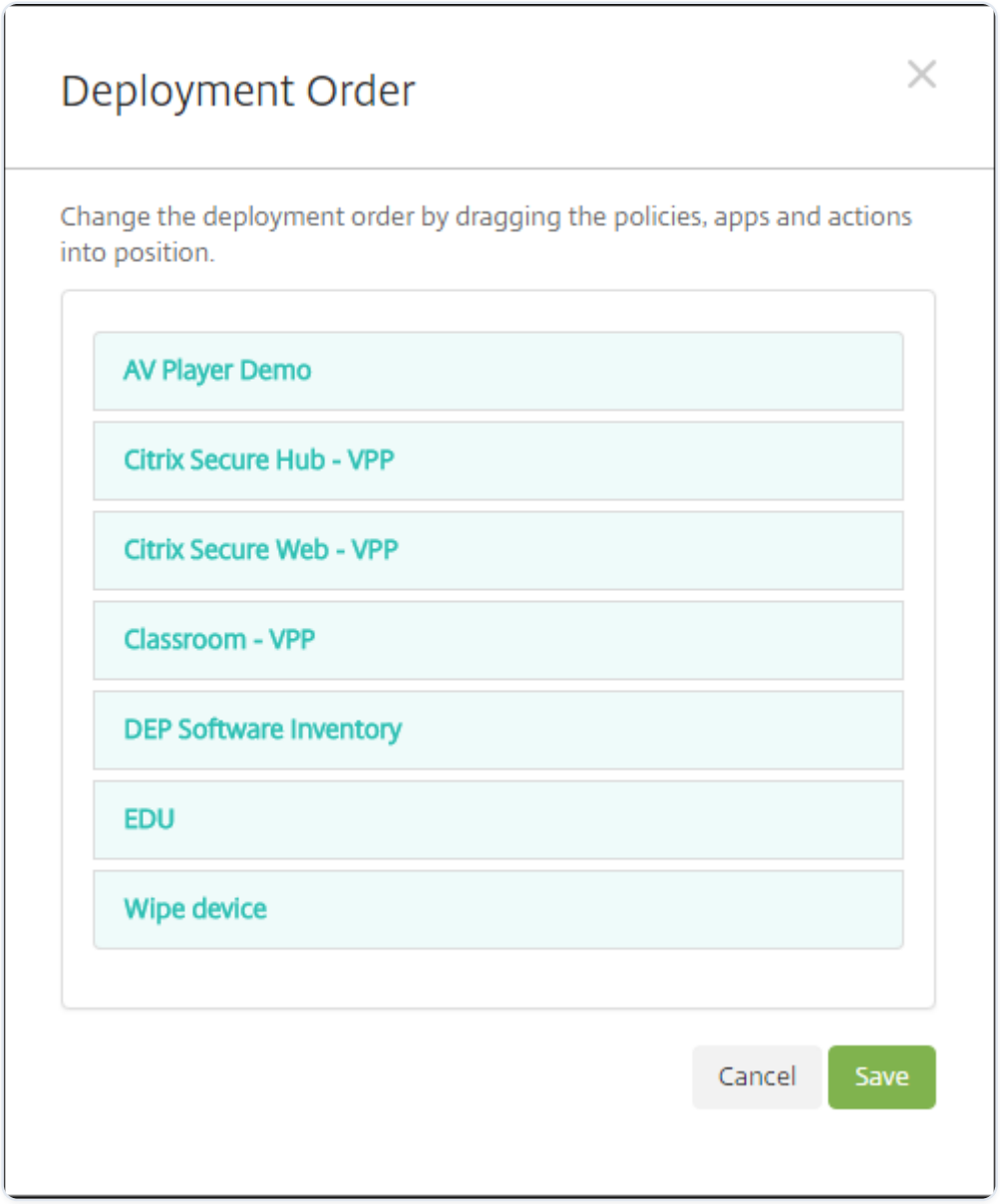


構成済みのオプションを確認し、展開順序を変更するには



概要ページでは、デリバリーグループに構成したオプションを確認し、リソースの展開順序を変更できます。概要ページには、リソースがカテゴリ別に表示されます。概要ページには展開順序は反映されません。

1. 構成に必要な調整を行うために、**戻る**をクリックして前のページに戻ります。
2. 展開順序を表示または並べ替えるには、**展開順序**をクリックします。**展開順序**ダイアログボックスが表示されます。



3. リソースをクリックして、展開したい場所にドラッグします。展開順序を変更すると、XenMobileはリスト内のリソースを上から下へ展開します。
4. 展開順序を保存するには、**保存**をクリックします。
5. デリバリーグループを保存するには、**保存**をクリックします。

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。その他の設定を更新するには、**構成 > デリバリーグループ**に移動し、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、有効または無効に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、次のいずれかを実行します。

- **Disable** をクリックして、AllUsers デリバリーグループを無効にします。このコマンドは、AllUsers が有効になっている場合（デフォルト）にのみ使用できます。デリバリーグループテーブルの **Disabled** 見出しの下に **Disabled** と表示されます。
- **Enable** をクリックして、AllUsers デリバリーグループを有効にします。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テーブルの **Disabled** 見出しの下から **Disabled** 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 および 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。これらのユーザーは、XenMobile に再接続するためにデリバリーグループに属している必要があります。これにより、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ます。

その他のプラットフォームデバイスのユーザーの場合：これらのデバイスがすでにXenMobileに接続されている場合、すぐにリソースを受け取ります。そうでない場合、スケジューリングポリシーに基づいて、次回接続時にリソースを受け取ります。Android Enterpriseプラットフォームのユーザーは、Firebase Cloud Messaging通知システムから通知を受け取り、XenMobile Serverに接続してリソースを取得します。

更新されたアプリをAndroidデバイスのXenMobile Storeの「更新可能なアプリ」リストに表示するには、まずApp Inventoryポリシーをユーザーデバイスに展開します。

1. **Delivery Groups** ページで、次のいずれかを実行します。
    - 一度に複数のデリバリーグループに展開するには、展開したいグループの横にあるチェックボックスを選択します。

- 単一のデリバリーグループに展開するには、その名前の横にあるチェックボックスを選択するか、その名前を含む行をクリックします。

2. **Deploy** をクリックします。

   単一のデリバリーグループを選択する方法に応じて、**Deploy** コマンドはデリバリーグループの上または右に表示されます。

   アプリ、ポリシー、アクションを展開したいグループがリストされていることを確認し、**Deploy** をクリックします。アプリ、ポリシー、アクションは、デバイスプラットフォームとスケジューリングポリシーに基づいて、選択されたグループに展開されます。

   Delivery Groups ページで、次のいずれかの方法で展開ステータスを確認できます。

   - デリバリーグループの **Status** 見出しの下にある展開アイコンを見て、展開の失敗を確認します。
   - デリバリーグループを含む行をクリックして、**Installed**、**Pending**、**Failed** 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構成画面(/en-us/xenmobile/server/media/configure-delivery-groups-check-deployment.png)

デリバリーグループを複製するには

既存のデリバリーグループと類似したデリバリーグループを作成する場合は、デリバリーグループを複製します。複製したものを新しいデリバリーグループの開始点として使用します。その後、登録プロファイルの追加や新しいADユーザーセットの追加など、複製に変更を加えます。

1. XenMobile Serverコンソールで、**Configure**をクリックし、**Delivery Groups**タブを選択します。
2. デリバリーグループの一覧から、新しいグループのベースとして使用するものを選択します。
3. **Clone**を選択します。
4. **Clone a Delivery Group**ダイアログボックスで、新しいグループの名前と説明（オプション）を入力します。
5. **Clone**を選択します。

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、すべてのユーザーにリソースをプッシュしたくない場合は、そのグループを無効にできます。

1. **Delivery Groups**ページで、次のいずれかを実行します。
   - 複数のデリバリーグループを一度に削除するには、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。
   - 単一のデリバリーグループを削除するには、その名前の横にあるチェックボックスをオンにするか、その名前を含む行をクリックします。
2. **Delete**をクリックします。**Delete**ダイアログボックスが表示されます。

   単一のデリバリーグループを選択する方法に応じて、**Delete**コマンドはデリバリーグループの上または右に表示されます。

   > **重要:**
   >
   > 削除を取り消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テーブルをエクスポートするには

1. **デリバリーグループ**テーブルの上にある**エクスポート**ボタンをクリックします。XenMobileは、**デリバリーグループ**テーブルの情報を抽出し、.csvファイルに変換します。
2. ブラウザーの通常の手順に従って、.csvファイルを開くか保存します。操作をキャンセルすることもできます。

マクロ

XenMobile® は、以下の項目のテキストフィールドにユーザーまたはデバイスのプロパティデータを入力する方法としてマクロを提供します。

- ポリシー
- 通知
- 登録テンプレート
- 自動アクション
- 資格情報プロバイダーの証明書署名要求

XenMobile は、マクロを対応するユーザーまたはシステムの値に置き換えます。たとえば、数千人のユーザーにわたる単一のExchangeプロファイルで、ユーザーのメールボックス値を事前に入力できます。

マクロ構文

マクロは次の形式をとることができます。

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]}`

ドル記号 ($) に続くすべての構文を中括弧 ({ }) で囲みます。

- 修飾プロパティ名は、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参照します。
- 修飾プロパティ名は、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は `${user.[PROPERTYNAME] (prefix="user.")}` の形式を取ります。
- デバイスプロパティは `${device.[PROPERTYNAME] (prefix="device.")}` の形式を取ります。
- プロパティ名は大文字と小文字を区別します。
- 関数は、限定されたリスト、または関数を定義するサードパーティのリファレンスへのリンクにすることができます。通知メッセージの次のマクロには、**firstnotnull**関数が含まれています。

  デバイス `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` はブロックされました…
- カスタムマクロ (定義するプロパティ) の場合、プレフィックスは `${custom}` です。プレフィックスを省略できます。

ポリシーのテキストフィールドにユーザー名の値を入力する、一般的に使用されるマクロ `${user.username}` の例を次に示します。このマクロは、Exchange ActiveSyncプロファイルや、多くのユーザーが使用するその他のプロファイルを構成するのに役立ちます。次の例は、Exchangeポリシーでマクロを使用する方法を示しています。**ユーザー**のマクロは** `${user.username}` **です。メールアドレスのマクロは** `${user.mail}` **です。

デバイスポリシー構成画面のマクロの画像(/en-us/xenmobile/server/media/macro-example-exchange-policy.png)

次の例は、証明書署名要求にマクロを使用する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。

資格情報プロバイダー構成画面のマクロの画像(/en-us/xenmobile/server/media/macro-example-credential-providers-certificate-signing-request.png)

次の例は、通知テンプレートでマクロを使用する方法を示しています。このテンプレートの例では、非準拠デバイスのためにHDX™アプリケーションがブロックされたときにユーザーに送信されるメッセージを定義しています。**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)}` はデバイスポリシーに準拠しなくなり、HDXアプリケーションはブロックされます。

通知テンプレート構成画面のマクロの画像(/en-us/xenmobile/server/media/macro-example-notification-template.png)

通知で使用されるマクロのその他の例については、**設定 > 通知テンプレート**に移動し、定義済みの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、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ることができます。たとえば、 `${device.serialnumber}` を使用して、デバイス名を各デバイスのシリアル番号に設定します。 `${device.serialnumber} ${ user.username }` を使用して、デバイス名にユーザー名を含めます。デバイス名デバイスポリシーは、監視対象のiOSおよびmacOSデバイスで機能します。

デバイスポリシー構成画面のマクロの画像(/en-us/xenmobile/server/media/macro-example-device-name-policy.png)

デフォルト通知テンプレートのマクロ

デフォルト通知テンプレートでは、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)}`

> **注:**
>
> XenMobile Serverコンソールには「ブラックリスト」と「ホワイトリスト」という用語が含まれています。これらの用語は、今後のリリースで「ブロックリスト」と「許可リスト」に変更されます。

- `${vpp.account}`
- `${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およびmacOSの場合) では、**デバイス名**にこれら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、**URL**にこのマクロを使用できます。

- `${webeas-url}`

Samsung MDMライセンスキーデバイスポリシーの場合、**ELMライセンスキー**にこのマクロを使用できます。

- `${elm.license.key}`

組み込みデバイスプロパティを取得するマクロ

表示名	マクロ
デバイスID	`$device.id`
デバイスGUID	`$device.uniqueid`
デバイスIMEI	`$device.imei`
OSファミリー	`$device.OSFamily`
シリアル番号	`$device.serialNumber`

すべてのデバイスプロパティのマクロ

以下の一覧は、表示名、Web要素、およびマクロを示しています。

アカウントは停止されていますか？

- 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

- 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によって認識されている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

- ADMIN_DISABLED
- ${device.ADMIN_DISABLED}

AIK が存在しますか？

- WINDOWS_HAS_AIK_PRESENT
- ${device.WINDOWS_HAS_AIK_PRESENT}

Amazon MDM API が利用可能

- 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 インストールタイプ

- GOOGLE_AW_INSTALL_TYPE
- ${device.GOOGLE_AW_INSTALL_TYPE}

アンチスパイウェア署名ステータス

- ANTI_SPYWARE_SIGNATURE_STATUS
- ${device.ANTI_SPYWARE_SIGNATURE_STATUS}

アンチスパイウェアステータス

- ANTI_SPYWARE_STATUS
- ${device.ANTI_SPYWARE_STATUS}

アンチウイルス署名ステータス

- ANTI_VIRUS_SIGNATURE_STATUS
- ${device.ANTI_VIRUS_SIGNATURE_STATUS}

アンチウイルスステータス

- 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}

資産タグ

- ASSET_TAG
- ${device.ASSET_TAG}

ソフトウェアアップデートを自動的に確認

- AutoCheckEnabled
- ${device.AutoCheckEnabled}

バックグラウンドでソフトウェアアップデートを自動的にダウンロード

- BackgroundDownloadEnabled
- ${device.BackgroundDownloadEnabled}

アプリのアップデートを自動的にインストール

- AutomaticAppInstallationEnabled
- ${device.AutomaticAppInstallationEnabled}

OSアップデートを自動的にインストール

- AutomaticOSInstallationEnabled
- ${device.AutomaticOSInstallationEnabled}

セキュリティアップデートを自動的にインストール

- AutomaticSecurityUpdatesEnabled
- ${device.AutomaticSecurityUpdatesEnabled}

自動更新ステータス

- AUTOUPDATE_STATUS
- ${device.AUTOUPDATE_STATUS}

利用可能なRAM

- MEMORY_AVAILABLE
- ${device.MEMORY_AVAILABLE}

利用可能なソフトウェアアップデート

- AVAILABLE_OS_UPDATE_HUMAN_READABLE
- ${device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}

利用可能なストレージ容量

- 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}

バッテリー稼働時間

- BATTERY_RUNTIME
- ${device.BATTERY_RUNTIME}

バッテリーステータス

- BATTERY_STATUS
- ${device.BATTERY_STATUS}

MSによって認識されている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サーバーバージョン

- BES_VERSION
- ${device.BES_VERSION}

BIOS情報

- BIOS_INFO
- ${device.BIOS_INFO}

BitLockerステータス

- 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改訂リストバージョン

- 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URL

- CatalogURL
- ${device.CatalogURL}

セルラー高度

- GPS_ALTITUDE_FROM_CELLULAR
- ${device.GPS_ALTITUDE_FROM_CELLULAR}

セルラーコース

- GPS_COURSE_FROM_CELLULAR
- ${device.GPS_COURSE_FROM_CELLULAR}

セルラー水平精度

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}

セルラー緯度

- GPS_LATITUDE_FROM_CELLULAR
- ${device.GPS_LATITUDE_FROM_CELLULAR}

携帯電話の経度

- GPS_LONGITUDE_FROM_CELLULAR
- ${device.GPS_LONGITUDE_FROM_CELLULAR}

携帯電話の速度

- GPS_SPEED_FROM_CELLULAR
- ${device.GPS_SPEED_FROM_CELLULAR}

携帯電話の技術

- CELLULAR_TECHNOLOGY

- ${device.CELLULAR_TECHNOLOGY}

携帯電話のタイムスタンプ

- GPS_TIMESTAMP_FROM_CELLULAR
- ${device.GPS_TIMESTAMP_FROM_CELLULAR}

携帯電話の垂直精度

- GPS_VERTICAL_ACCURACY_FROM_CELLULAR
- ${device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR}

次回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

- CLOUD_BACKUP_ENABLED
- ${device.CLOUD_BACKUP_ENABLED}

コード整合性が有効ですか？

- WINDOWS_HAS_CODE_INTEGRITY_ENABLED
- ${device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED}

コード整合性失効リストバージョン

- 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タイプ

- CPU_TYPE
- ${device.CPU_TYPE}

作成時間

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- ${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}

重要なソフトウェアアップデート

- 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有効

- DATA_ROAMING_ENABLED
- ${device.DATA_ROAMING_ENABLED}

最後のiCloudバックアップの日付

- 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}

DEPプロファイル割り当て済み

- PROFILE_ASSIGN_TIME
- ${device.PROFILE_ASSIGN_TIME}

DEPプロファイルプッシュ済み

- PROFILE_PUSH_TIME
- ${device.PROFILE_PUSH_TIME}

DEPプロファイルが削除されました

- 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

- DESCRIPTION

- ${device.DESCRIPTION}

デバイス識別子

- アクティブシンクID
- ${device.activesyncid}

デバイスモデル

- 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}

おやすみモードが有効

- DO_NOT_DISTURB
- ${device.DO_NOT_DISTURB}

ELAMドライバーはロードされていますか？

- WINDOWS_HAS_ELAM_DRIVER_LOADED
- ${device.WINDOWS_HAS_ELAM_DRIVER_LOADED}

暗号化コンプライアンス

- 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: 空き容量

- 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: 合計容量

- EXTERNAL_STORAGE1_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE1_TOTAL_SPACE}

外部ストレージ 2: 利用可能容量

- 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: 合計容量

- EXTERNAL_STORAGE2_TOTAL_SPACE
- ${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

外部ストレージ暗号化済み

- EXTERNAL_ENCRYPTION
- ${device.EXTERNAL_ENCRYPTION}

FileVault 有効

- IS_FILEVAULT_ENABLED
- ${device.IS_FILEVAULT_ENABLED}

ファイアウォールステータス

- DEVICE_FIREWALL_STATUS
- ${device.DEVICE_FIREWALL_STATUS}

ファイアウォールステータス

- FIREWALL_STATUS
- ${device.FIREWALL_STATUS}

ファームウェアバージョン

- FIRMWARE_VERSION
- ${device.FIRMWARE_VERSION}

初回同期

- ZMSP_FIRST_SYNC
- ${device.ZMSP_FIRST_SYNC}

Google ディレクトリ エイリアス

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- ${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Google ディレクトリ 姓

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- ${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Google ディレクトリ 名前

- GOOGLE_AW_DIRECTORY_NAME
- ${device.GOOGLE_AW_DIRECTORY_NAME}

Google ディレクトリ 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 標高

- GPS_ALTITUDE_FROM_GPS
- ${device.GPS_ALTITUDE_FROM_GPS}

GPS コース

- GPS_COURSE_FROM_GPS
- ${device.GPS_COURSE_FROM_GPS}

GPS 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}

現在ログインしているiTunes Store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}

ICCID

- ICCID
- ${device.ICCID}

ID

- AS_DEVICE_IDENTITY
- ${device.AS_DEVICE_IDENTITY}

IMEI/MEID 番号

- IMEI
- ${device.IMEI}

IMSI

- SIM_ID
- ${device.SIM_ID}

内部ストレージの暗号化

- LOCAL_ENCRYPTION
- ${device.LOCAL_ENCRYPTION}

IPロケーション

- 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}

発行日時

- WINDOWS_HAS_ISSUED_AT
- ${device.WINDOWS_HAS_ISSUED_AT}

ジェイルブレイク/ルート化

- ROOT_ACCESS
- ${device.ROOT_ACCESS}

カーネルデバッグが有効ですか？

- 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}

最後に確認されたIPアドレス

- LAST_IP_ADDR
- ${device.LAST_IP_ADDR}

最終ポリシー更新時刻

- LAST_POLICY_UPDATE_TIME
- ${device.LAST_POLICY_UPDATE_TIME}

最終スキャン日

- PreviousScanDate
- ${device.PreviousScanDate}

最終スキャン結果

- PreviousScanResult
- ${device.PreviousScanResult}

最後のスケジュールされたソフトウェア更新

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- ${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

最後のスケジュールされたソフトウェア更新の失敗メッセージ

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- ${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

最後のスケジュールされたソフトウェア更新のステータス

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- ${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

最終同期

- ZMSP_LAST_SYNC
- ${device.ZMSP_LAST_SYNC}

ロケーターサービスが有効

- 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アドレスタイプ

- MAC_ADDRESS_TYPE
- ${device.MAC_ADDRESS_TYPE}

メールボックス設定

- 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紛失モードが有効

- 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}

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}

組織のメールアドレス

- 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}

パスコードが存在する

- PASSCODE_PRESENT
- ${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- ${device.WINDOWS_HAS_PCR0}

境界侵害

- GPS_PERIMETER_BREACH
- ${device.GPS_PERIMETER_BREACH}

定期チェック

- PerformPeriodicCheck
- ${device.PerformPeriodicCheck}

パーソナルホットスポットがアクティブ化されました

- 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}

主要電話番号

- IDENTITY1_PHONENUMBER
- ${device.IDENTITY1_PHONENUMBER}

主要SIMキャリアオペレーター

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- ${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

主要SIM ICCID

- IDENTITY1_ICCID
- ${device.IDENTITY1_ICCID}

主要SIM IMEI

- IDENTITY1_IMEI
- ${device.IDENTITY1_IMEI}

主要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ローミングコンプライアンス

- IDENTITY1_ROAMING_COMPLIANCE
- ${device.IDENTITY1_ROAMING_COMPLIANCE}

製品名

- PRODUCT_NAME

- ${device.PRODUCT_NAME}

パブリッシャーデバイス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}

セーフモードが有効ですか？

- WINDOWS_HAS_SAFE_MODE
- ${device.WINDOWS_HAS_SAFE_MODE}

Samsung KNOX APIが利用可能

- SAMSUNG_KNOX
- ${device.SAMSUNG_KNOX}

Samsung KNOX APIバージョン

- SAMSUNG_KNOX_VERSION
- ${device.SAMSUNG_KNOX_VERSION}

Samsung KNOXアテステーション

- SAMSUNG_KNOX_ATTESTED
- ${device.SAMSUNG_KNOX_ATTESTED}

Samsung KNOX 認証更新日

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- ${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}

Samsung SAFE API 利用可能

- 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キャリアオペレーター

- 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}

セキュアブートステータス

- SECURE_BOOT_STATE

- ${device.SECURE_BOOT_STATE}

セキュアコンテナ有効

- 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対応

- IS_SMS_CAPABLE
- ${device.IS_SMS_CAPABLE}

監視対象

- SUPERVISED
- ${device.SUPERVISED}

サスペンド理由

- GOOGLE_AW_DIRECTORY_SUSPENTION_REASON
- ${device.GOOGLE_AW_DIRECTORY_SUSPENTION_REASON}

改ざんステータス

- TAMPERED_STATUS
- ${device.TAMPERED_STATUS}

利用規約

- TERMS_AND_CONDITIONS
- ${device.TERMS_AND_CONDITIONS}

利用規約に同意済みか？

- GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS
- ${device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS}

テスト署名が有効か？

- WINDOWS_HAS_TEST_SIGNING_ENABLED
- ${device.WINDOWS_HAS_TEST_SIGNING_ENABLED}

合計RAM

- MEMORY
- ${device.MEMORY}

総ストレージ容量

- 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ステータス

- 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}

音声通話対応

- IS_VOICE_CAPABLE
- ${device.IS_VOICE_CAPABLE}

音声ローミング許可

- VOICE_ROAMING_ENABLED
- ${device.VOICE_ROAMING_ENABLED}

VSM有効?

- WINDOWS_HAS_VSM_ENABLED
- ${device.WINDOWS_HAS_VSM_ENABLED}

WiFi MACアドレス

- WIFI_MAC
- ${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY

- ${device.WINDOWS_ENROLLMENT_KEY}

WinPE 有効ですか？

- WINDOWS_HAS_WINPE
- ${device.WINDOWS_HAS_WINPE}

WNS 通知ステータス

- 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の有効期限

- 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 の利用可否

- ZEBRA_MDM
- ${device.ZEBRA_MDM}

Zebra MXMF バージョン

- ZEBRA_MDM_VERSION
- ${device.ZEBRA_MDM_VERSION}

Zebra パッチ バージョン

- ZEBRA_PATCH_VERSION
- ${device.ZEBRA_PATCH_VERSION}

組み込みユーザー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 (ドメインを除くログイン名、存在する場合)	`${user.username}`

すべてのユーザープロパティのマクロ

表示名	WEB要素	マクロ
Active Directoryのログオン失敗試行回数	バッドパスワードカウント	`${user.badpwdcount}`
ActiveSyncユーザーメール	アズユーザーEメール	`${user.asuseremail}`
ASMデータソース	アズエムパーソンソース	`${user.ampersonsource}`
ASM DEPアカウント名	アズエムディーイーピーアカウント	`${user.asmdepaccount}`
ASM管理対象Apple ID	アズエムパーソンマネージドアップルID	`${user.ampersonmanagedappleid}`
ASMパスコードタイプ	アズエムパーソンパスコードタイプ	`${user.ampersonpasscodetype}`

表示名	WEB要素	マクロ
ASM 個人 ID	ASM個人ID	`${user.aspersonid}`
ASM 個人のステータス	ASM個人ステータス	`${user.aspersonstatus}`
ASM 個人の役職	ASM個人タイトル	`${user.aspersontitle}`
ASM 個人の一意の ID	ASM個人一意ID	`${user.aspersonuniqueid}`
ASM ソースシステム ID	ASM個人ソースシステムID	`${user.aspersonsourcesystemid}`
ASM 学生の成績	ASMユーザーグレード	`${user.aspersongrade}`
BES ユーザーのメールアドレス	BESユーザーメール	`${user.besuseremail}`
会社	会社	`${user.company}`
会社名	会社名	`${user.companyname}`
国	c	`${user.c}`
部署	部署	`${user.department}`
説明	説明	`${user.description}`
無効なユーザー	無効なユーザー	`${user.disableduser}`
表示名	表示名	`${user.displayname}`
識別名	識別名	`${user.distinguishedname}`
ドメイン名	ドメイン名	`${user.domainname}`
メール	メール	`${user.mail}`
名	名	`${user.givenname}`

XENMOBILE®サーバー

表示名	WEB要素	マクロ
自宅住所	自宅住所	`${user.homestreetaddress}`
自宅市	自宅都市	`${user.homecity}`
居住国	居住国	`${user.homecountry}`
自宅FAX	自宅FAX	`${user.homefax}`
自宅電話	自宅電話	`${user.homephone}`
居住地の都道府県/地域	居住州	`${user.homestate}`
自宅の郵便番号	自宅郵便番号	`${user.homezip}`
IP電話	IP電話	`${user.ipphone}`
ミドルイニシャル	ミドルイニシャル	`${user.middleinitial}`
ミドルネーム	ミドルネーム	`${user.middlename}`
モバイル	モバイル	`${user.mobile}`
名前	cn	`${user.cn}`
勤務先住所	物理的配送オフィス名	`${user.physicaldeliveryofficename}`
勤務先都市	l	`${user.l}`
勤務先FAX番号	ファクシミリ電話番号	`${user.facsimiletelephonenumber}`
勤務先都道府県	st	`${user.st}`
勤務先番地	オフィス番地	`${user.officestreetaddress}`

表示名	WEB要素	マクロ
会社の電話番号	電話番号	`${user.telephonenumber}`
会社の郵便番号	郵便番号	`${user.postalcode}`
私書箱	私書箱	`${user.postofficebox}`
ポケットベル	ページャー	`${user.pager}`
プライマリグループID	プライマリグループID	`${user.primarygroupid}`
SAM アカウント	サムアカウント名	`${user.samaccountname}`
住所	住所	`${user.streetaddress}`
姓	sn	`${user.sn}`
役職	役職	`${user.title}`
ユーザーログオン名	ユーザープリンシパル名	`${user.userprincipalname}`

自動アクション

XenMobile®では、イベント、ユーザーまたはデバイスのプロパティ、あるいはユーザーデバイス上のアプリの存在に対する反応をプログラムするために、自動アクションを作成します。自動アクションを作成すると、そのアクションに定義されたトリガーによって、ユーザーデバイスがXenMobileに接続されたときに何が起こるかが決定されます。イベントがトリガーされた場合、より深刻なアクションが実行される前に、問題を修正するようユーザーに通知を送信できます。

自動的に実行されるように設定する効果には、次のようなものがあります。

- デバイスの完全または選択的ワイプ。
- デバイスを非準拠に設定する。
- デバイスの取り消し。
- より深刻なアクションが実行される前に、問題を修正するようユーザーに通知を送信する。

MAM専用モードの場合、アプリロックおよびアプリワイプアクションを構成できます。

> **注：**
>
> ユーザーに通知する前に、XenMobileがメッセージを送信できるように、XenMobile設定でSMTPおよびSMSの通知サーバーを構成する必要があります。詳細については、「通知」を参照してください。また、続行する前に、使用する予定の通知テンプレートを設定してください。詳細については、「通知テンプレートの作成と更新」を参照してください。

アクションの例

自動アクションの使用例をいくつか示します。

例1

- 以前にブロックしたアプリ（例：「Words with Friends」）を検出したいとします。「Words with Friends」アプリを検出した後、ユーザーデバイスを非準拠に設定するトリガーを指定できます。その後、このアクションは、デバイスを準拠状態に戻すためにアプリを削除する必要があることをユーザーに通知します。また、ユーザーが準拠するまで待機する時間制限を設定

することもできます。その時間制限が過ぎると、デバイスを選択的にワイプするなどの定義されたアクションが実行されます。

例2

- 顧客が最新のファームウェアを使用しているか確認し、ユーザーがデバイスを更新する必要がある場合にリソースへのアクセスをブロックしたいとします。ユーザーデバイスが最新バージョンでない場合に、ユーザーデバイスを非準拠状態にするトリガーを指定できます。自動アクションを使用して、リソースをブロックし、顧客に通知します。

例3

- ユーザーデバイスが非準拠状態になり、その後ユーザーがデバイスを修正した場合。デバイスを準拠状態にリセットするパッケージを展開するポリシーを構成できます。

例4

- 特定の期間非アクティブだったユーザーデバイスを非準拠としてマークしたいとします。非アクティブなデバイスに対して、次のように自動アクションを作成できます。

  a. XenMobileコンソールで、**Settings > Network Access Control** に移動し、**Inactive Devices** を選択します。**Inactive Devices** 設定の詳細については、Network Access Control を参照してください。

  b. アクションの追加と管理 で概説されているアクションを追加する手順に従います。唯一の違いは、**Action details** ページで次のように設定を構成することです。

     ◦ **Trigger**。**Device property**、**Out of compliance**、および **True** を選択します。

     ◦ **Action**。**Send notification** を選択し、**Settings** の **Notification Template** を使用して作成したテンプレートを選択します。次に、アクションを実行するまでの遅延を日、時間、または分で設定します。ユーザーがトリガーとなる問題に対処するまでアクションが繰り返される間隔を設定します。

> **ヒント:**
>
> 非アクティブなデバイスを一括削除するには、Public API for REST Services を使用します。まず、削除したい非アクティブなデバイスのデバイスIDを手動で取得し、その後削除APIを実行して一括削除します。

アクションの追加と管理

自動アクションを追加、編集、フィルタリングするには：

1. XenMobileコンソールから、**Configure > Actions** をクリックします。**Actions** ページが表示されます。
2. **Actions** ページで、次のいずれかを実行します。
   - 「**追加**」をクリックしてアクションを追加します。
   - 既存のアクションを選択して編集または削除します。使用したいオプションをクリックします。
3. 「**アクション情報**」ページが表示されます。
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:** アクションを識別するための名前を入力します。このフィールドは必須です。
   - **説明:** アクションが実行する内容を記述します。
5. 「**次へ**」をクリックします。「**アクションの詳細**」ページが表示されます。

   次の例は、**イベント**トリガーを設定する方法を示しています。別のトリガーを選択した場合、表示されるオプションはここに示されているものとは異なります。

   アクション設定画面の画像(/en-us/xenmobile/server/media/configure-actions.png)
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。

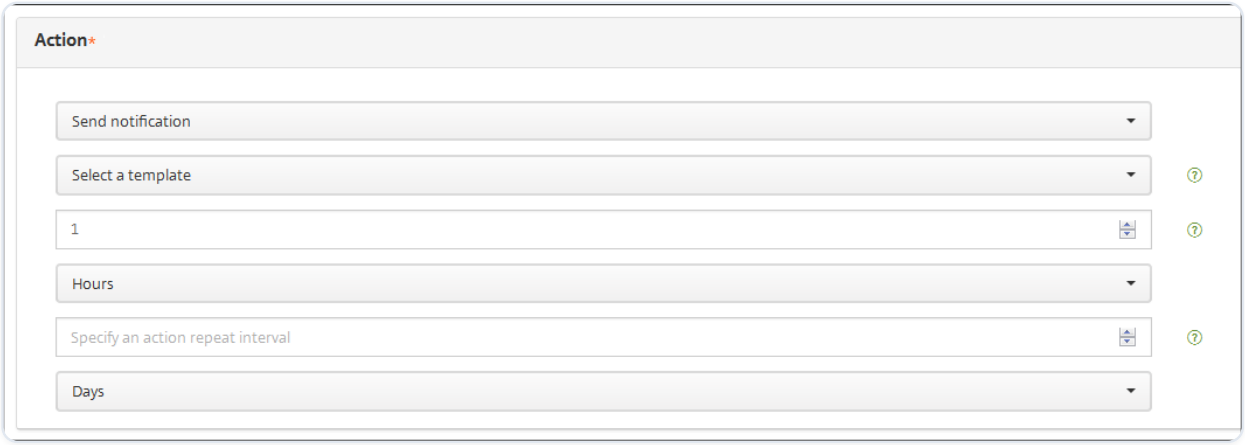
   「**トリガー**」リストで、このアクションのイベントトリガータイプをクリックします。各トリガーの意味は次のとおりです。
   - **イベント:** 事前定義されたイベントに反応します。
   - **デバイスプロパティ:** MDM管理対象デバイスのデバイス属性をチェックし、それに反応します。詳細については、「デバイスプロパティ名と値」を参照してください。
   - **ユーザープロパティ:** 通常、Active Directoryからのユーザー属性に反応します。
   - **インストール済みアプリ名:** アプリのインストールに反応します。MAM専用モードには適用されません。デバイスでアプリインベントリポリシーが有効になっている必要があります。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デフォルトで有効になっています。詳細については、「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. 次のリストで、トリガーへの応答をクリックします。

8. **［アクション］** リストで、トリガー条件が満たされたときに実行するアクションをクリックします。 **［通知の送信］** を除き、ユーザーがトリガーの原因となった問題を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、選択したアクションが実行されます。アクションの定義については、「セキュリティアクション」を参照してください。

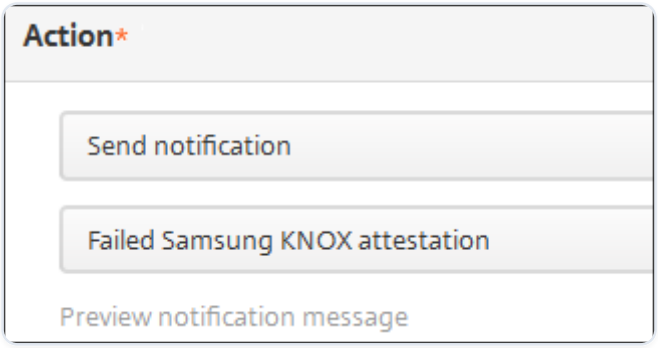
   ［通知の送信］ を選択した場合は、次の手順で通知アクションを送信します。

9. 次のリストで、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する通知テンプレートが表示されます。ただし、通知の種類に対してテンプレートがまだ存在しない場合は、次のメッセージが表示され、テンプレートを構成するように求められます：このイベントタイプにはテンプレートがありません。 **［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てください。

   ユーザーに通知する前に、XenMobileがメッセージを送信できるように、SMTPおよびSMSの設定で通知サーバーを構成しておく必要があります。通知を参照してください。また、続行する前に、使用する予定の通知テンプレートを設定してください。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と更新を参照してください。



   テンプレートを選択したら、 **［通知メッセージのプレビュー］** をクリックして通知をプレビューできます。



10. 次のフィールドで、アクションを実行するまでの遅延を日、時間、または分で設定します。ユーザーがトリガーの問題に対処するまで、アクション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アクションが作成されていることを確認します。



12. アクションの詳細を構成したら、各プラットフォームの展開規則を個別に構成できます。これを行うには、選択した各プラットフォームについて手順13を完了します。
13. 展開規則を構成します。展開規則の構成に関する一般的な情報については、「リソースの展開」を参照してください。

    この例では、次のようになります。

    - デバイスの所有権は**BYOD**である必要があります。
    - デバイスのローカル暗号化は**True**である必要があります。
    - 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はアンドラのみにすることはできません。

14. アクションのプラットフォーム展開ルール構成が完了したら、**次へ**をクリックします。**アクションの割り当て**ページが表示され、そこでアクションを1つまたは複数の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の選択**の横で、デリバリーグループを検索するか、リストからグループを選択します。選択したグループは、**アプリの割り当てを受け取るデリバリーグループ**リストに表示されます。
16. 展開スケジュールを展開し、次の設定を構成します。

    - **展開**の横で、**ON**をクリックして展開をスケジュールするか、**OFF**をクリックして展開を防止します。デフォルトのオプションは**ON**に設定されています。**OFF**を選択した場合、他のオプションは不要です。
    - **展開スケジュール**の横で、**今すぐ**または**後で**をクリックします。デフォルトのオプションは**今すぐ**に設定されています。

- **後で**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、展開の日付と時刻を選択します。
- **展開条件**の横で、**接続ごとに**をクリックするか、**前回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**接続ごとに**に設定されています。
- **常時接続の展開**の横で、**ON**または**OFF**をクリックします。デフォルトのオプションは**OFF**に設定されています。

  このオプションは、**設定 > サーバープロパティ**でスケジューリングバックグラウンド展開キー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デバイスでは利用できません。

構成する展開スケジュールは、すべてのプラットフォームで同じです。行った変更は、iOSには適用されない**常時接続の展開**を除き、すべてのプラットフォームに適用されます。

17. **次へ**をクリックします。**概要**ページが表示され、アクションの構成を確認できます。
18. アクションを保存するには、「**保存**」をクリックします。

MAM専用モードでのアプリロックおよびアプリワイプアクション

XenMobileコンソールにリストされている4つのトリガーカテゴリ（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）すべてに応じて、デバイス上のアプリをワイプまたはロックできます。

自動アプリワイプまたはアプリロックを構成するには

1. XenMobileコンソールで、「**構成 > 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、アクションの名前とオプションの説明を入力します。
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。

   この手順では、次の条件に留意してください。

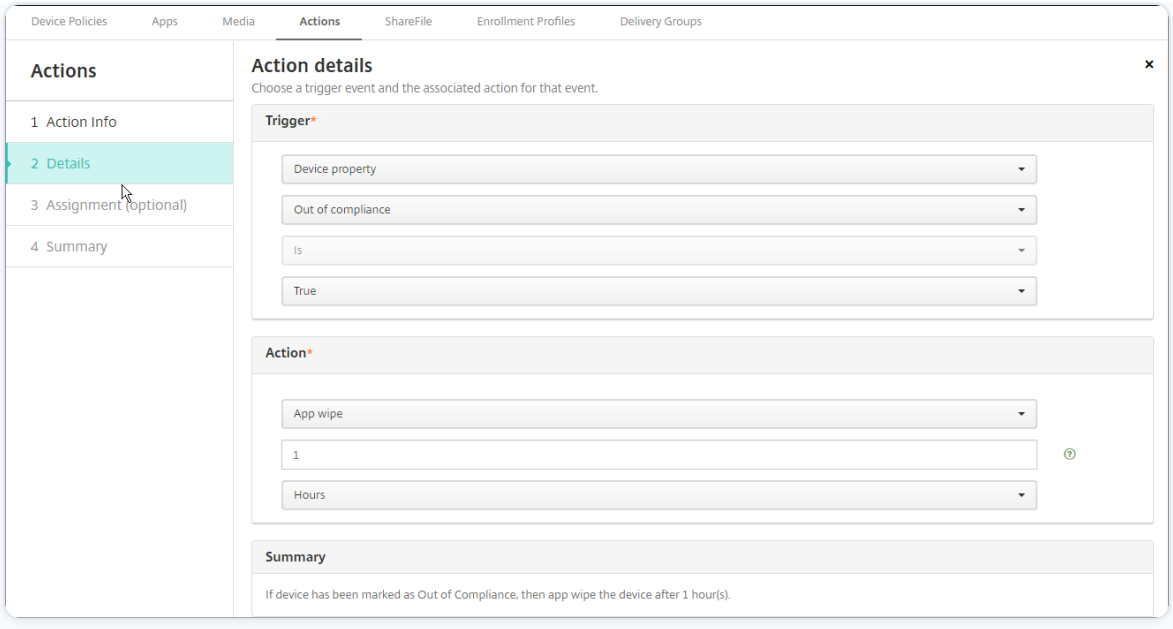
   トリガーの種類が「**イベント**」に設定されており、値が「**Active Directory無効ユーザー**」ではない場合、「**アプリワイプ**」および「**アプリロック**」アクションは表示されません。

   トリガーの種類が「**デバイスプロパティ**」に設定されており、値が「**MDM紛失モードが有効**」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する
- デバイスを完全にワイプする
- デバイスを取り消す

各オプションについて、1時間の遅延が自動的に設定されますが、遅延期間は分、時間、または日で選択できます。遅延の目的は、アクションが実行される前にユーザーが問題を解決する時間を与えることです。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、「セキュリティアクション」を参照してください。

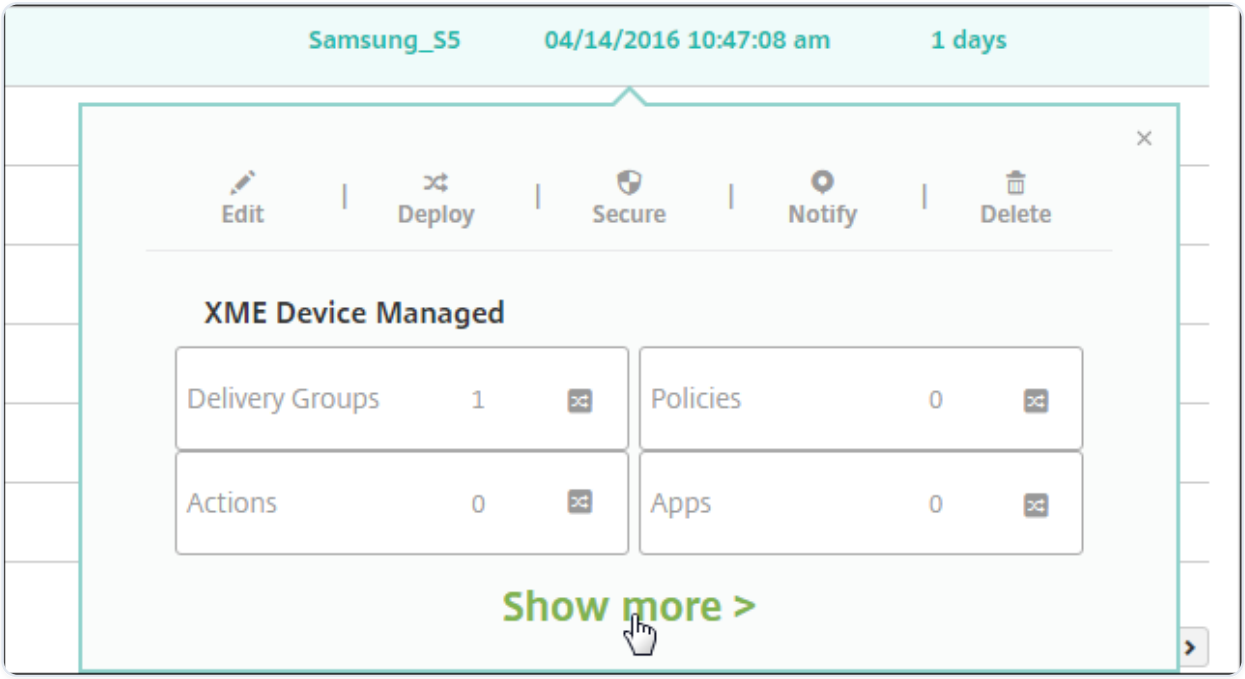
> **注：**
>
> トリガーを**イベント**に設定した場合、繰り返し間隔は自動的に最低1時間になります。通知を受信するには、デバイスがサーバーと同期するためにポリシーの更新を実行する必要があります。通常、デバイスはユーザーがサインオンしたとき、またはSecure Hubを介してポリシーを手動で更新したときにサーバーと同期します。
>
> Active Directoryデータベースが XenMobileと同期できるように、アクションが実行される前に約1時間の追加遅延が発生する場合があります。



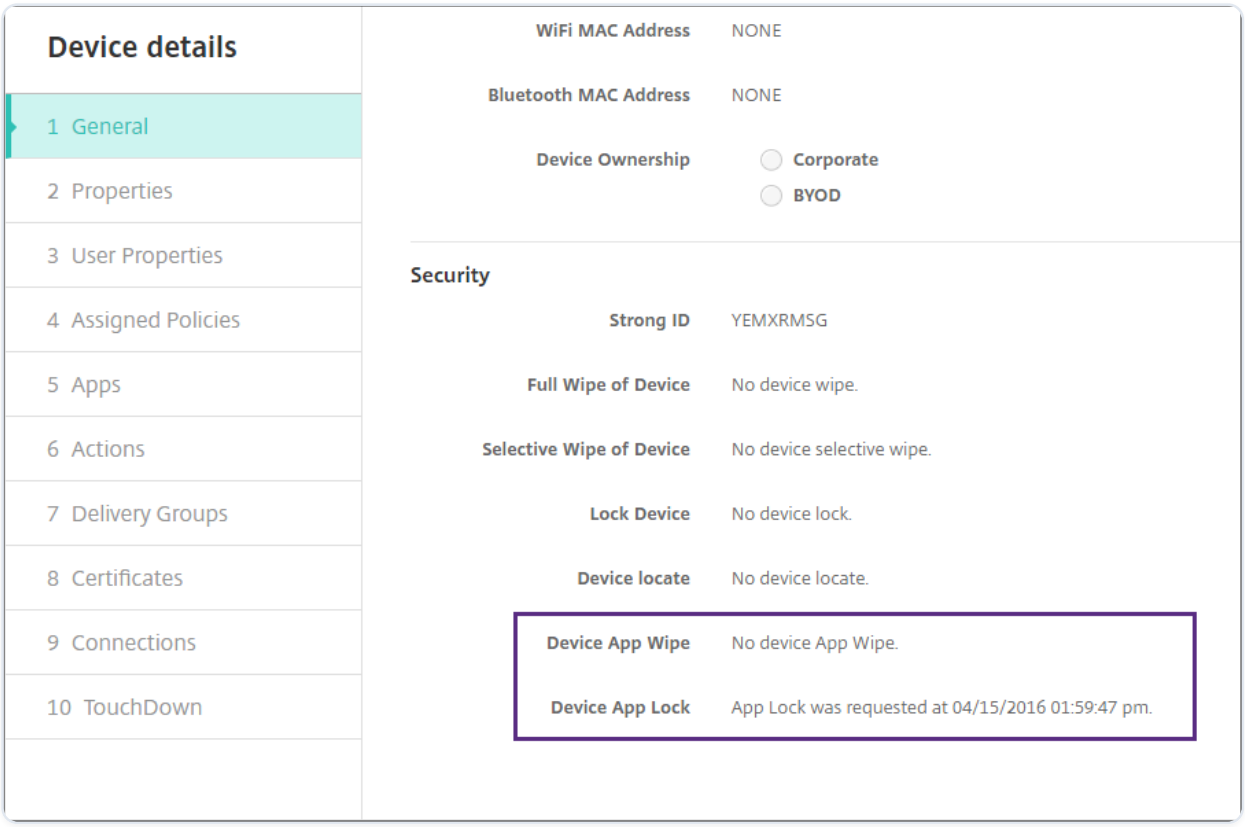
6. 展開ルールを構成し、**次へ**をクリックします。
7. 配信グループの割り当てと展開スケジュールを構成し、**次へ**をクリックします。
8. **保存**をクリックします。

アプリのロックまたはアプリのワイプステータスを確認するには

1. **管理 > デバイス**に移動し、デバイスをクリックして、**詳細を表示**をクリックします。



2. **デバイスアプリのワイプ**と**デバイスアプリのロック**までスクロールします。



デバイスがワイプされると、ユーザーはPINコードの入力を求められます。ユーザーがコードを忘れた場合は、デバイスの詳細で確認できます。

監視とサポート

XenMobile® Dashboard と XenMobile Support ページを使用して、XenMobile Server を監視およびトラブルシューティングできます。XenMobile Support ページを使用して、サポート関連の情報やツールにアクセスできます。

オンプレミスの XenMobile Server の場合、XenMobile CLI からアクションを実行することもできます。詳細については、「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、右上隅にあるレンチアイコンをクリックします。

サポートアイコンの画像(/en-us/xenmobile/server/media/select-support-wrench.png)

トラブルシューティングとサポートのページが表示されます。

XenMobile の ページを使用して、次の操作を実行します。

- 診断にアクセスします。
- サポートバンドルを作成します (オンプレミスインストールのみ)。
- Citrix 製品ドキュメントとナレッジセンターへのリンクにアクセスします。
- ログ操作にアクセスします。
- 高度な構成オプションを使用します。
- 一連のツールとユーティリティにアクセスします。

XenMobile コンソール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もできます。この情報を使用すると、ウィジェットを使用して問題や成功をすばやく確認できます。

分析ダッシュボードの画像(/en-us/xenmobile/server/media/analyze-dashboard.png)

ダッシュボードは通常、XenMobileコンソールにサインオンしたときに最初に表示されるページです。コンソールの他の場所からダッシュボードにアクセスするには、 をクリックします。ダッシュボードで をクリックして、ページのレイアウトと表示されるウィジェットを編集します。

- **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。これらのダッシュボードは個別に編集でき、保存したダッシュボードを選択してそれぞれを表示できます。

- **レイアウトスタイル:** この行では、ダッシュボードに表示されるウィジェットの数と、ウィジェットのレイアウト方法を選択できます。
- **ウィジェットの選択:** ダッシュボードに表示する情報を選択できます。
  - **通知:** 左側の数字の上にあるチェックボックスをオンにすると、ウィジェットの上に通知バーが追加されます。このバーには、準拠デバイス、非アクティブデバイス、および過去24時間以内にワイプまたは登録されたデバイスの数が表示されます。
  - **プラットフォーム別デバイス:** プラットフォームごとの管理対象デバイスと非管理対象デバイスの数を表示します。
  - **キャリア別デバイス:** キャリアごとの管理対象デバイスと非管理対象デバイスの数を表示します。各バーをクリックすると、プラットフォーム別の内訳が表示されます。
  - **プラットフォーム別管理対象デバイス:** プラットフォームごとの管理対象デバイスの数を表示します。
  - **プラットフォーム別非管理対象デバイス:** プラットフォームごとの非管理対象デバイスの数を表示します。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、権限が取り消されているか、ワイプされています。
  - **ActiveSync Gatewayステータス別デバイス:** ActiveSync Gatewayステータス別にグループ化されたデバイスの数を表示します。情報には、ブロック済み、許可済み、または不明のステータスが表示されます。各バーをクリックすると、プラットフォーム別にデータを内訳できます。
  - **所有権別デバイス:** 所有権ステータス別にグループ化されたデバイスの数を表示します。情報には、企業所有、従業員所有、または不明の所有権ステータスが表示されます。
  - **失敗したデリバリーグループ展開:** パッケージごとの失敗した展開の合計数を表示します。失敗した展開があるパッケージのみが表示されます。
  - **ブロック理由別デバイス:** ActiveSyncによってブロックされたデバイスの数を表示します。
  - **インストール済みアプリ:** アプリ情報をグラフで表示するには、アプリ名を入力します。
  - **ボリューム購入アプリのライセンス使用状況:** Appleボリューム購入アプリのライセンス使用状況統計を表示します。

各ウィジェットで、個々の部分をクリックして詳細情報をドリルダウンできます。

分析ダッシュボードのドリルダウンの画像(/en-us/xenmobile/server/media/analyze-dashboard-drill-down.png)

また、**アクション**メニューをクリックして、情報を.csvファイルとしてエクスポートできます。

分析ダッシュボードメニューの画像(/en-us/xenmobile/server/media/analyze-dashboard-actions-menu.png)

サポートバンドル内のデータを匿名化する

XenMobile®でサポートバンドルを作成すると、機密性の高いユーザー、サーバー、およびネットワークデータはデフォルトで匿名化されます。ページでこの動作を変更できます。また、XenMobileがデータを匿名化するときに保存する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。Citrix®サポートは、データを非匿名化し、特定のユーザーまたはデバイスの問題を特定するために、このファイルを要求できます。

1. XenMobileコンソールで、右上隅にあるレンチアイコンをクリックします。**サポート**ページが表示されます。
2. **サポート**ページで、**詳細設定**の下にある**匿名化と非匿名化**をクリックします。**匿名化と非匿名化**ページが表示されます。

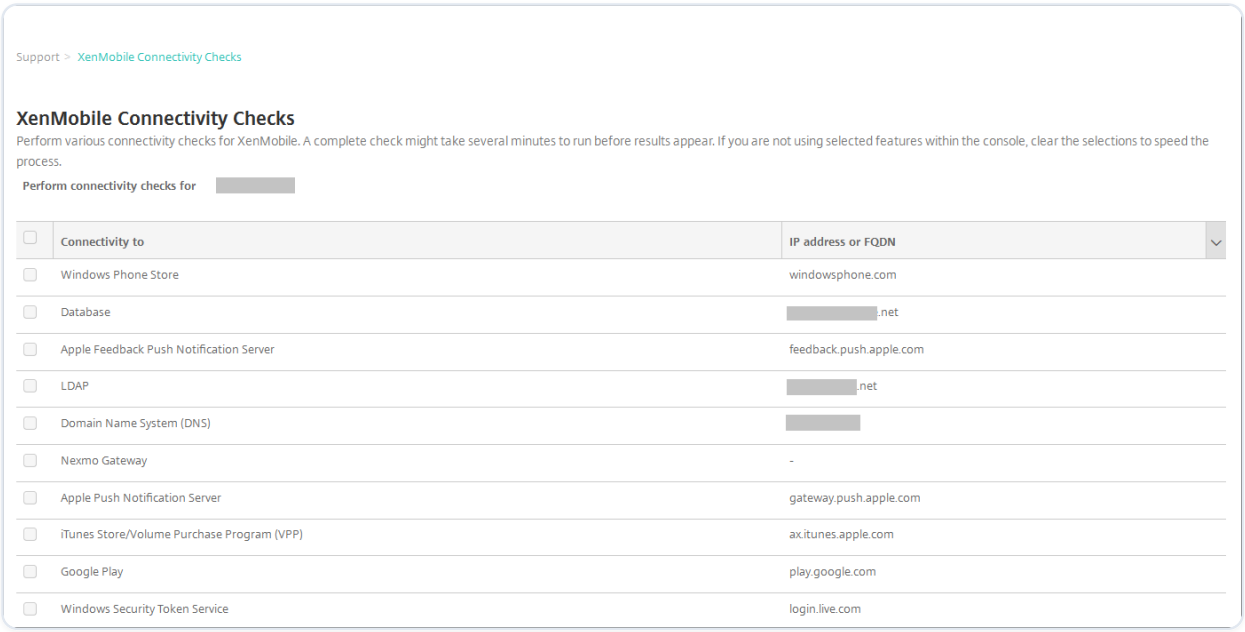
   データ匿名化構成の画像(/en-us/xenmobile/server/media/anonymize-data-screen.png)
3. **サポートバンドルの匿名化**で、データが匿名化されるかどうかを選択します。デフォルトは**ON**です。
4. **非匿名化**の横にある**非匿名化ファイルをダウンロード**をクリックして、問題の診断に特定のデバイスまたはユーザー情報が必要な場合にCitrixサポートに送信するマッピングファイルをダウンロードします。

接続チェック

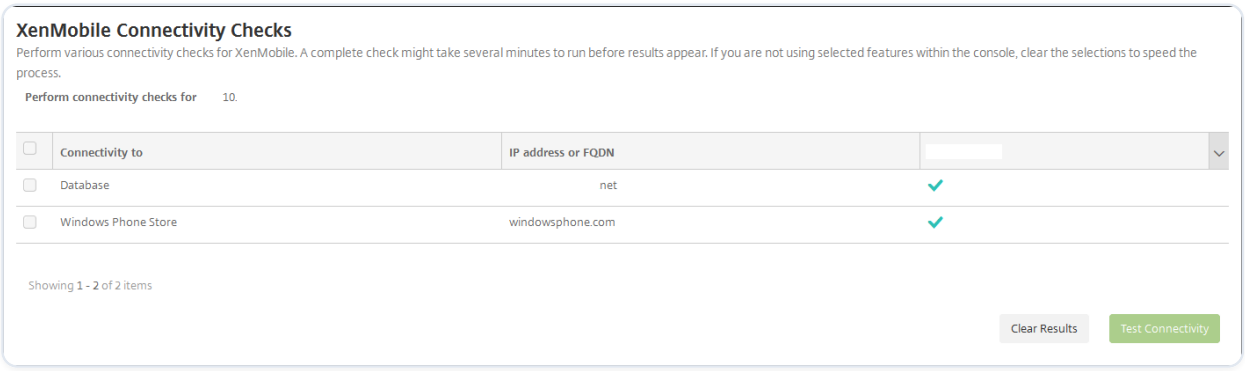
XenMobile® の ページから、Citrix Gateway およびその他のサーバーや場所への XenMobile 接続を確認できます。

XenMobile 接続チェックの実行

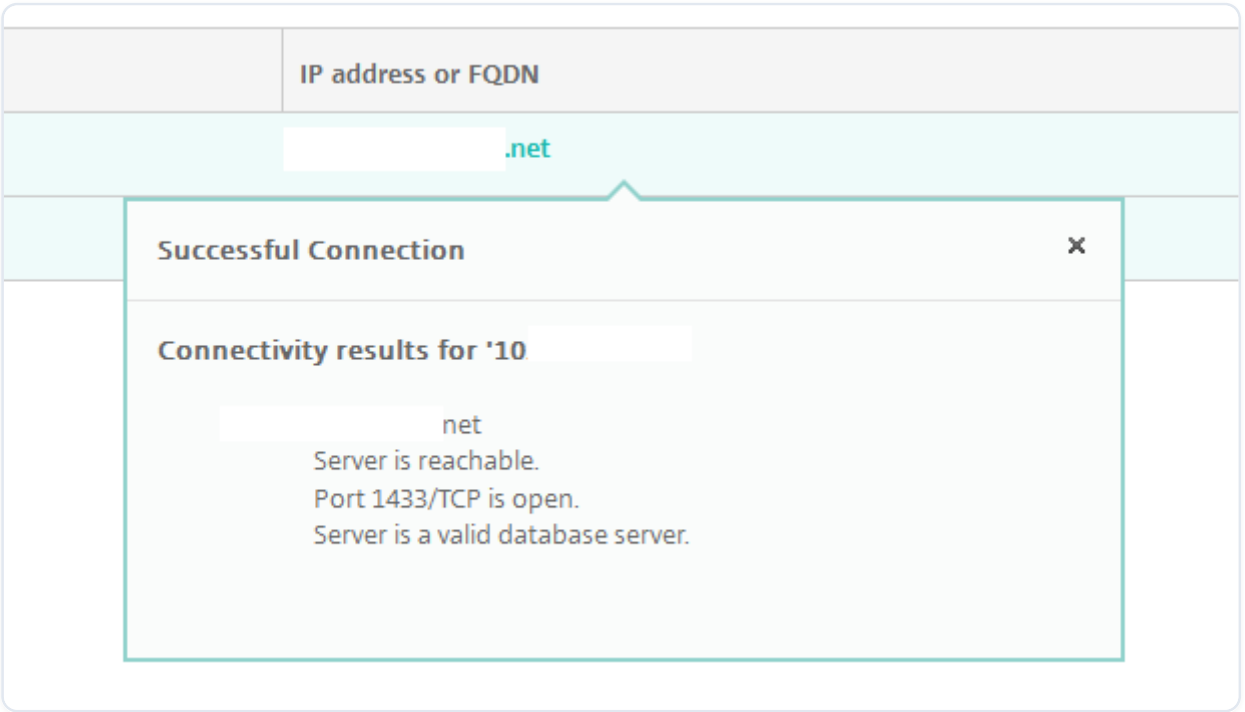
1. XenMobile コンソールで、コンソールの右上隅にあるレンチアイコンをクリックします。 ページが表示されます。
2. の下で、 をクリックします。 ページが表示されます。XenMobile 環境にクラスター化されたノードがある場合、すべてのノードが表示されます。



3. 接続テストに含めるサーバーを選択し、 をクリックします。テスト結果ページが表示されます。

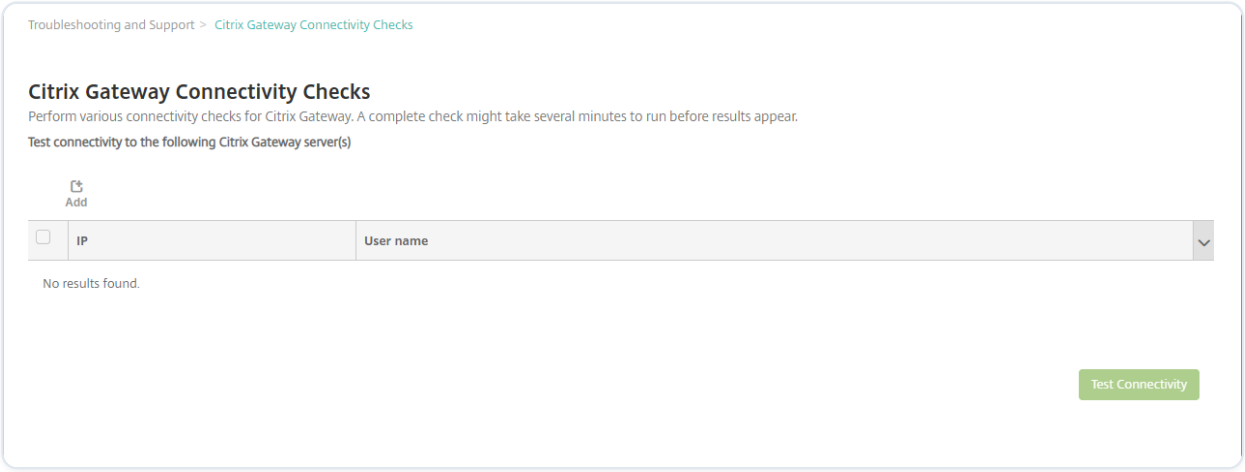


4. テスト結果テーブルでサーバーを選択して、そのサーバーの詳細な結果を表示します。

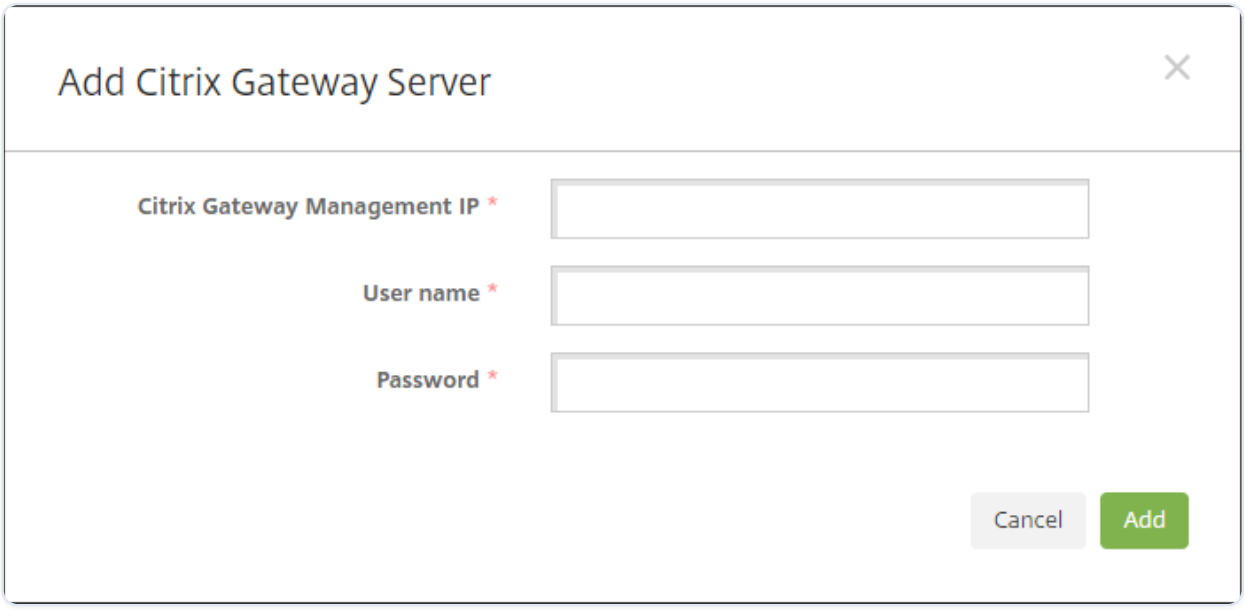


Citrix Gateway 接続チェックの実行

1. ページで、 の下にある をクリックします。 ページが表示されます。Citrix Gateway サーバーを追加していない場合、テーブルは空です。



2. をクリックします。 ダイアログボックスが表示されます。



3. 「**Citrix Gateway Management IP**」に、テストするCitrix 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：**
>
> 以前に追加されたCitrix Gatewayサーバーの接続チェックを実行している場合、IPアドレスは入力されています。

4. このCitrix Gatewayの管理者資格情報を入力します。

> **注：**
>
> 以前に追加されたCitrix Gatewayサーバーの接続チェックを実行している場合、ユーザー名は入力されています。

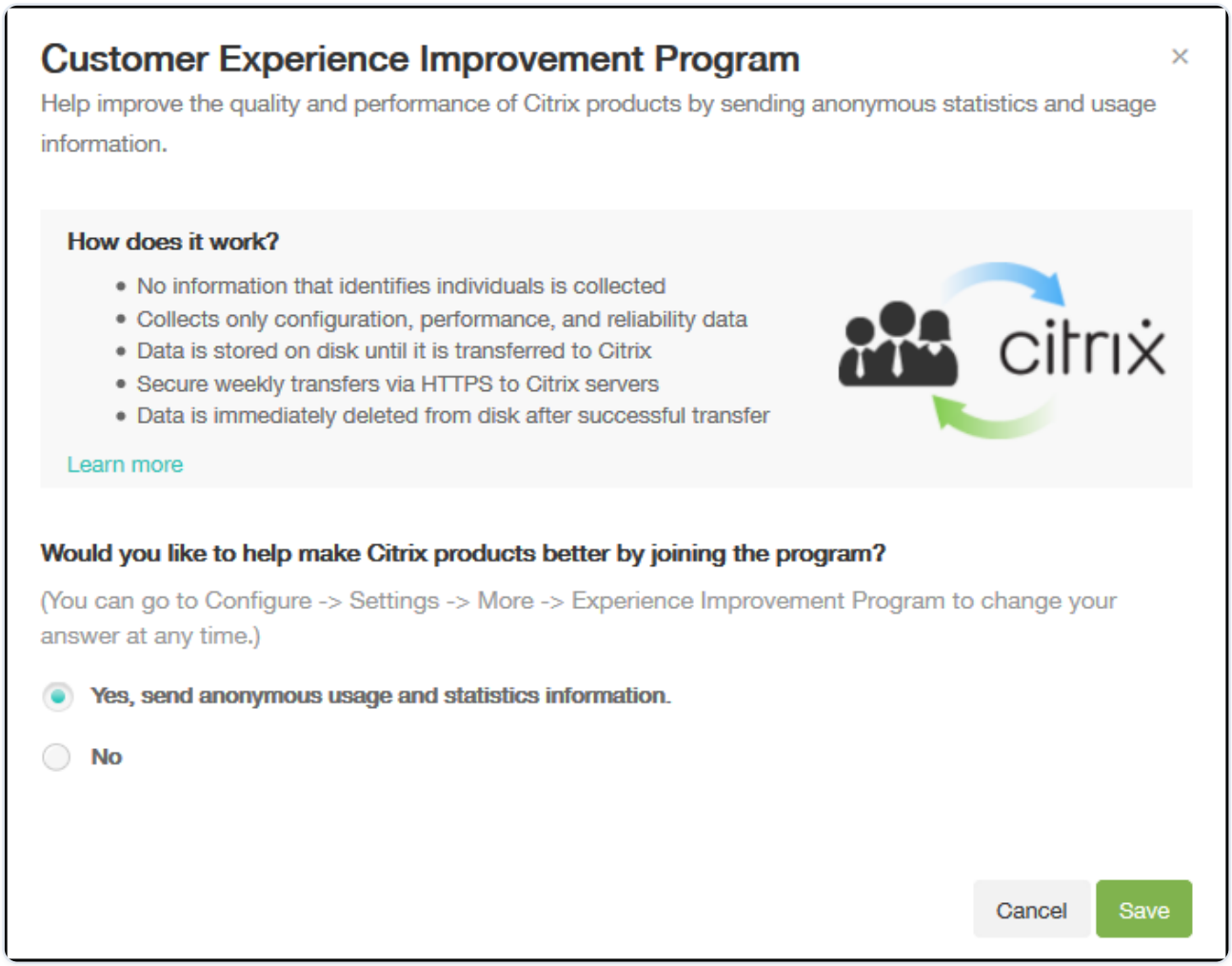
5. 「**追加**」をクリックします。Citrix Gatewayが「**Citrix Gateway Connectivity Checks**」ページのテーブルに追加されます。
6. Citrix Gatewayサーバーを選択し、「**接続テスト**」をクリックします。結果はテスト結果テーブルに表示されます。
7. テスト結果テーブルでサーバーを選択して、そのサーバーの詳細な結果を表示します。

カスタマーエクスペリエンス向上プログラム

Citrixカスタマーエクスペリエンス向上プログラム (CEIP) は、XenMobileから匿名の構成データと使用状況データを収集し、Citrixに自動的に送信します。このデータは、CitrixがXenMobileの品質、信頼性、およびパフォーマンスを向上させるのに役立ちます。CEIPへの参加は任意です。XenMobileを初めてインストールするとき、またはアップデートをインストールするときに、CEIPに参加できます。オプトインすると、データは通常週単位で収集され、パフォーマンスデータと使用状況データは時間単位で収集されます。データはディスクに保存され、毎週HTTPS経由でCitrixに安全に転送されます。XenMobileコンソールでCEIPへの参加の有無を変更できます。CEIPの詳細については、「Citrix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。

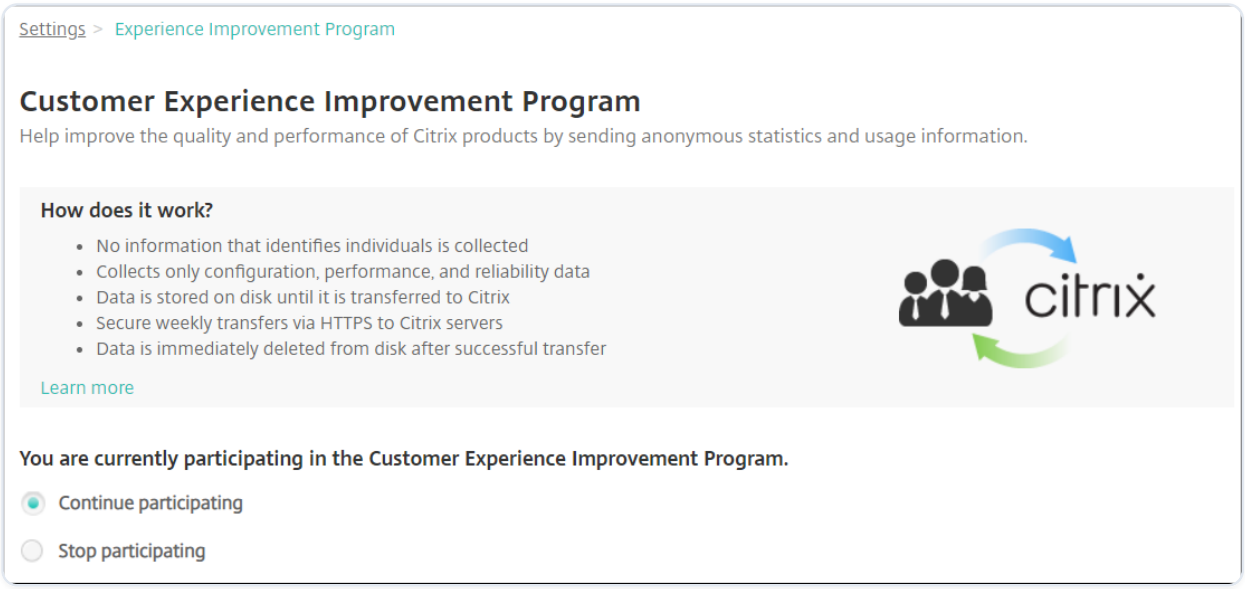
CEIPへの参加を選択する

XenMobile®を初めてインストールするとき、またはアップデートを行うときに、参加を促す次のダイアログボックスが表示されます。



CEIP参加設定の変更

1. XenMobileコンソールでCEIP参加設定を変更するには、コンソールの右上隅にある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**ページが表示されます。表示される正確なページは、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、停止したい場合は、**参加を停止**をクリックします。
4. 現在CEIPに参加しておらず、開始したい場合は、**参加を開始**をクリックします。
5. **保存**をクリックします。

ログ

XenMobile® が生成するログの出力をカスタマイズするために、ログ設定を構成できます。XenMobileコンソールでログ設定を構成する際に、クラスター化されたXenMobileサーバーがある場合、それらの設定はクラスター内の他のすべてのサーバーと共有されます。

1. XenMobileコンソールで、コンソールの右上隅にあるレンチアイコンをクリックします。**サポート**ページが表示されます。
2. **ログ操作**の下で、**ログ設定**をクリックします。**ログ設定**ページが表示されます。

   ログ構成の画像(/en-us/xenmobile/server/media/support-log-settings.png)

   ログ設定ページでは、次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、データベースに保持されるログバックアップファイルの最大数を制御します。ログサイズは、XenMobileがサポートする各ログ（デバッグログ、管理者アクティビティログ、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、設定を永続化したりします。
   - **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。

   ログ構成の画像(/en-us/xenmobile/server/media/support-log-settings-log-size.png)

2. これらの設定を構成します。

   - **デバッグログファイルのサイズ (MB):** リストで、5 MBから20 MBの間のサイズをクリックして、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:** リストで、サーバーによって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、XenMobileはサーバー上に50個のバックアップファイルを保持します。
   - **管理者アクティビティログファイルサイズ (MB):** リストで、管理者アクティビティファイルの最大サイズを変更するために、5 MBから20 MBの間のサイズをクリックします。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:** リストで、サーバーによって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、XenMobileはサーバー上に300個のバックアップファイルを保持します。
   - **ユーザーアクティビティログファイルサイズ (MB):** リストで、ユーザーアクティビティファイルの最大サイズを変更するために、5 MBから20 MBの間のサイズをクリックします。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:** リストで、サーバーによって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、XenMobileはサーバー上に300個のバックアップファイルを保持します。

ログレベルオプションを構成するには

ログレベルでは、XenMobileがログに収集す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、個々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テーブルが表示されます。

   ロギング構成の画像(/en-us/xenmobile/server/media/support-log-settings-log-level.png)

2. 次のいずれかを実行します。

   - 1つのクラスの横にあるチェックボックスをクリックし、**レベル設定**をクリックして、こ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、テーブル内のすべてのクラスにログレベルの変更を適用します。

ログレベル設定ダイアログボックスが表示され、ログレベルを設定し、XenMobile Serverを再起動したときにログレベル設定を保持するかどうかを選択できます。

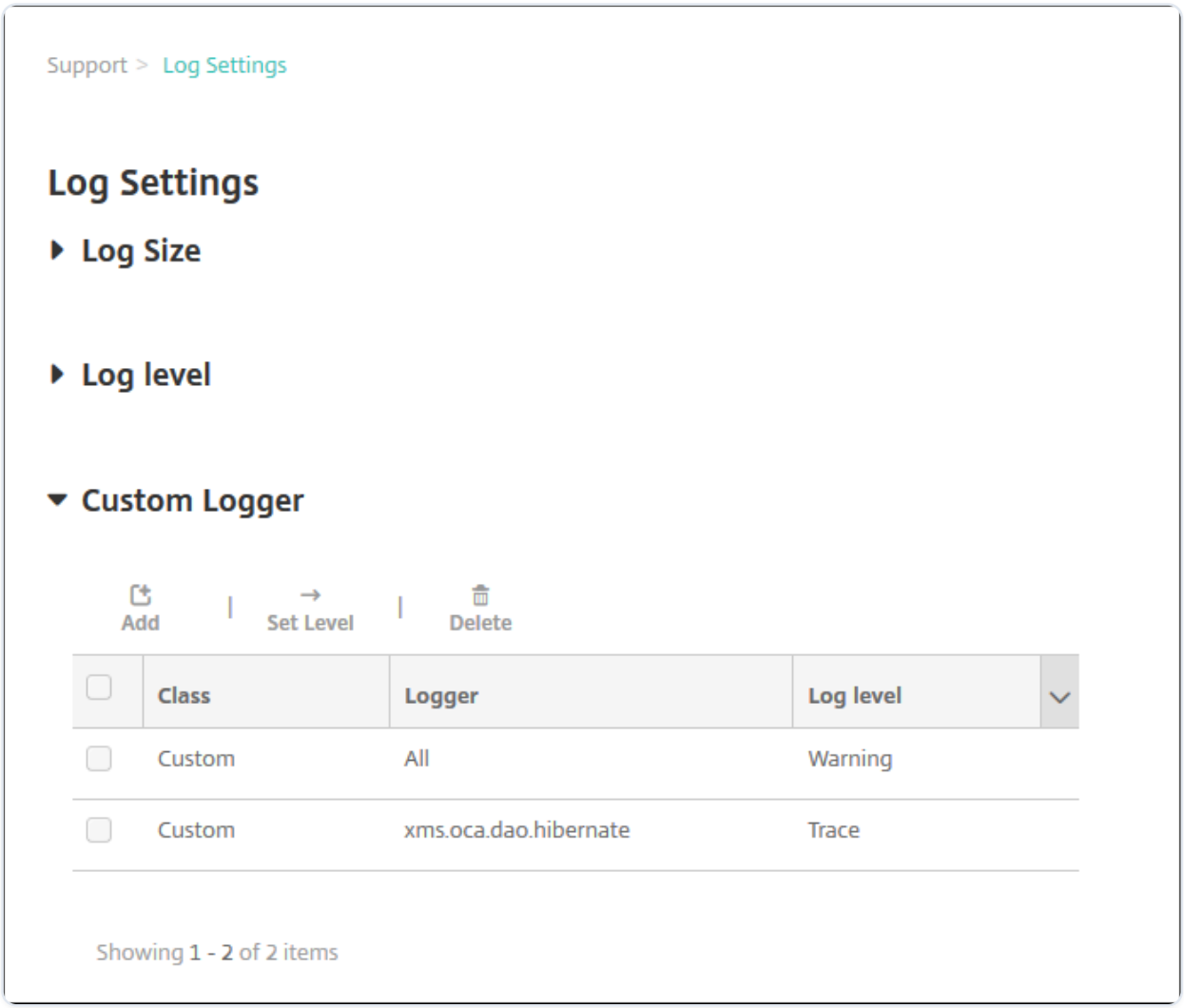
ロギング構成の画像(/en-us/xenmobile/server/media/support-log-settings-log-level-set-level.png)

- **クラス名**: このフィールドには、すべてのクラスのログレベルを変更している場合は**すべて**と表示され、個々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**: このフィールドには、すべてのクラスのログレベルを変更している場合は**すべて**と表示され、個々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**: リストからログレベルをクリックします。サポートされているログレベルは次のとおりです。
  - 致命的
  - エラー
  - 警告
  - 情報
  - デバッグ
  - トレース
  - オフ
- **含まれるロガー**: すべてのクラスのログレベルを変更している場合、このフィールドは空白になります。または、個々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。
- **設定を保持**: サーバーを再起動してもログレベル設定を保持したい場合は、このチェックボックスを選択します。このチェックボックスを選択しない場合、サーバーの再起動時にログレベル設定はデフォルトに戻ります。

3. 変更をコミットするには、**設定**をクリックします。

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**テーブルが表示されます。カスタムロガーを追加していない場合、テーブルは最初は空です。



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表示されます。

   ログ構成の画像(/en-us/xenmobile/server/media/support-log-settings-custom-logger-add.png)

3. 以下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:** リストからログレベルをクリックします。サポートされているログレベルは次のとおりです:
     - 致命的
     - エラー
     - 警告
     - 情報
     - デバッグ
     - トレース
     - オフ

- **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、すべてのロガーを含める場合はフィールドを空白のままにします。

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**テーブルに追加されます。

ログ構成の画像(/en-us/xenmobile/server/media/support-log-settings-custom-logger-table.png)

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表示されます。「**OK**」をクリックします。

> **重要:**
>
> この操作は元に戻せません。

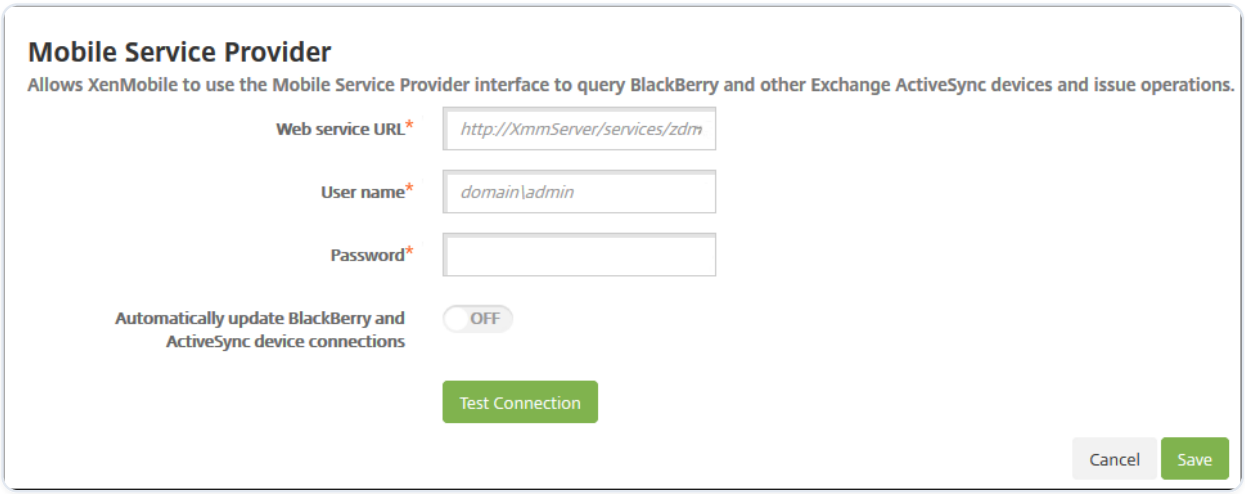
モバイルサービスプロバイダー

XenMobile®で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、BlackBerryおよびExchange ActiveSyncデバイスを照会し、操作を発行できます。

たとえば、組織に1,000人のユーザーがいて、各ユーザーが1つ以上のデバイスを使用しているとします。すべてのユーザーに、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伝えた後、XenMobileコンソールには、ユーザーが登録したデバイスの数が表示されます。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特定できます。この方法で、次のことができます。

- ユーザーがまだデバイスを登録する必要があるかどうかを判断します。
- Exchange Serverに接続しているユーザーデバイスに、データワイプなどのコマンドを発行します。

1. XenMobileコンソールで、右上隅の歯車アイコンをクリックします。**設定**ページが表示されます。
2. **サーバー**の下で、**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**ページが表示されます。



3. これらの設定を構成します:

   - **WebサービスURL:** WebサービスのURLを入力します。例: `https://<XmmServer>/services/xdmservice`
   - **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、接続を確認します。

4. **保存**をクリックします。

レポート

XenMobile® は、アプリとデバイスの展開を分析できる以下の事前定義レポートを提供します。各レポートはテーブルとグラフとして表示されます。テーブルは列で並べ替えたり、フィルターしたりできます。グラフの要素を選択すると、より詳細な情報を表示できます。

- **アプリ展開試行の合計:** ユーザーがデバイスにインストールしようとした展開済みアプリを一覧表示します。
- **プラットフォーム別アプリ:** デバイスのプラットフォームとバージョン別にアプリとアプリのバージョンを一覧表示します。
- **種類別アプリ:** バージョン、種類、カテゴリ別にアプリを一覧表示します。
- **デバイス登録:** 登録されているすべてのデバイスを一覧表示します。
- **デバイスとアプリ:** 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。
- **非アクティブなデバイス:** XenMobile Server のプロパティ device.inactivity.days.threshold で指定された日数、アクティビティがないデバイスのリスト。

- **ジェイルブレイク/ルート化されたデバイス:** ジェイルブレイクされた iOS デバイスとルート化された Android デバイスを一覧表示します。
- **利用規約:** 利用規約に同意したユーザーと拒否したユーザーを一覧表示します。グラフの領域を選択すると、詳細を表示できます。
- **上位 10 アプリ:** 展開失敗 - 展開に失敗したアプリを最大 10 個一覧表示します。
- **デバイスとユーザー別のブラックリスト登録済みアプリ:** ユーザーがデバイスに持っているブロックされたアプリを一覧表示します。

> **注:**
>
> XenMobile Server コンソールには、「ブラックリスト」と「ホワイトリスト」という用語が含まれています。今後のリリースでは、これらの用語を「ブロックリスト」と「許可リスト」に変更する予定です。

- **非準拠デバイス:** デバイスがジェイルブレイクされているか、実行中の OS バージョン、パスコードがあるかなど、コンプライアンス基準を満たしていないデバイスを一覧表示します。

各テーブルのデータは.csv形式でエクスポートでき、Microsoft Excelなどのプログラムで開くことができます。各レポートのチャートはPDF形式でエクスポートできます。

- **インストール済みアプリトップ100:** 各プラットフォームにインストールされているアプリの上位100個までを一覧表示します。詳細については、「サーバープロパティ」を参照してください。

レポートを生成するには

1. XenMobileコンソールで、 **>** をクリックします。 ページが表示されます。
2. 生成したいレポートをクリックします。

   レポート生成の画像(/en-us/xenmobile/server/media/reporting-total-apps.png)

レポートの詳細を表示するには

1. チャートの領域をクリックしてドリルダウンし、詳細情報を表示します。

   レポート詳細の画像(/en-us/xenmobile/server/media/reporting-total-apps-drilldown.png)

テーブルの列を並べ替え、フィルター、または検索するには、列見出しをクリックします

レポート列の並べ替え、フィルター、検索の画像(/en-us/xenmobile/server/media/reporting-click-column-heading.png)

日付でレポートをフィルターするには

1. 列見出しをクリックしてフィルター設定を表示します。

   日付によるレポートフィルターの画像(/en-us/xenmobile/server/media/analyze-reporting-date-filter.png)

2. から、報告される日付をどのように制限するかを選択します。

   レポートフィルターの日付の画像(/en-us/xenmobile/server/media/analyze-reporting-date-filter-condition.png)

3. 日付選択ツールを使用して日付を指定します。

   レポートフィルターの日付の画像(/en-us/xenmobile/server/media/analyze-reporting-date-filter-choose-date.png)

4. 日付フィルターのある列は、次の例に示すように表示されます。

   レポートフィルターの日付の画像(/en-us/xenmobile/server/media/analyze-reporting-date-filter-indicator.png)

5. フィルターを削除するには、列見出しをクリックし、**Remove Filter** をクリックします。

   フィルターを削除する画像(/en-us/xenmobile/server/media/analyze-reporting-date-filter-remove.png)

グラフまたはテーブル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、**Actions** をクリックし、**Export graph as PDF** をクリックします。
- テーブルデータをCSV形式でエクスポートするには、**Actions** をクリックし、**Export data as CVS** をクリックします。

グラフまたはテーブルをエクスポートする画像(/en-us/xenmobile/server/media/reporting-export-snip.png)

> **重要:**

> SQL Serverを使用してカスタムレポートを作成することは可能ですが、Citrix®はこの方法を推奨していません。Citrixはスキーマを公開しておらず、通知なしにスキーマを変更する可能性があります。このレポート作成方法を追求する場合は、SQLクエリが読み取り専用アカウントを使用して実行されることを確認してください。実行に時間がかかる複数のJOINを含むクエリは、その間XenMobile Serverのパフォーマンスに影響を与えます。

SNMP監視

XenMobile ServerでSNMP監視を有効にすると、監視システムがXenMobileノードに関する情報を照会および取得できるようになります。クエリでは、プロセッサ負荷、ロードアベレージ、メモリ使用量、接続性などのパラメータが使用されます。認証および暗号化の仕様など、SNMP v3の詳細については、公式SNMPドキュメントのRFC 3414を参照してください。

> **注：**
>
> SNMP v3監視は、XenMobile Server 10.8以降でサポートされています。

> SCOMなど、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の構成の詳細については、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プロトコルを使用したSNMPトラフィックに使用されます。ソースはSNMPマネージャーで、宛先はXenMobileです。
- **ポート162 (UDP):** XenMobileからSNMPマネージャーにSNMPトラップアラートを送信するために使用されます。ソースはXenMobileで、宛先はSNMPマネージャーです。

XenMobileのポート構成の詳細については、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展開のアーキテクチャ図を確認するには、オンプレミス展開のリファレンスアーキテクチャを参照してください。

SNMPを設定するための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、トラップを受信し、XenMobile Serverを監視する権限を継承します。

2. **トラップを受信するSNMPマネージャーの追加:** トラップは、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が生成するアラートです。
3. **SNMPマネージャーをXenMobileと連携するように構成する:** XenMobile Serverは、特定の管理情報ベース (MIB) を使用して操作を実行します。MIBは、XenMobileコンソールの**設定 > SNMP構成**ページからダウンロードします。その後、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:**
   >
   > 各SNMPマネージャーには、独自のMIBインポーターがあります。

4. **トラップを有効にする:** XenMobileコンソール内でトラップを有効にし、環境に基づいて間隔と閾値を定義します。
5. **サードパーティSNMPマネージャー内でトラップを表示する:** トラップを表示するには、SNMPマネージャーを確認します。ただし、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を構成できます。たとえば、通知がメールに表示されるように構成できます。

XenMobileから以下のトラップを生成できます。

トラップ名: プロセッサー負荷

- **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。負荷がカスタム閾値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: 1分間の平均負荷

- **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。平均負荷がカスタム閾値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: 5分間の平均負荷

- **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。平均負荷がカスタム閾値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: 15分間の平均負荷

- **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ごとに、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と、XenMobileはSNMPトラップを生成します。

トラップ名: 利用可能な合計メモリ

- **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ごとに利用可能なメモリを監視します。利用可能なメモリがカスタムしきい値を下回ると、XenMobileはSNMPトラップを生成します。注: 利用可能な合計メモリには、RAMとスワップメモリ（仮想メモリ）の両方が含まれます。合計スワップメモリを取得するには、SNMP OID .1.3.6.1.4.1.2021.4.3を使用してクエリを実行できます。利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を使用してクエリを実行できます。

トラップ名: 使用済みディスクストレージの合計

- **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ごとにシステムディスクストレージを監視します。ディスクストレージがカスタムしきい値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: Javaヒープメモリ使用量

- **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ごとにXenMobileのJava仮想マシン (JVM) ヒープメモリ使用量を監視します。使用量がカスタムしきい値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: Javaメタスペース使用量

- **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ごとにXenMobileのJavaメタスペース使用量を監視します。使用量がしきい値を超えると、XenMobileはSNMPトラップを生成します。

トラップ名: LDAP接続

- **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:** LDAPサーバーとXenMobileノード間の接続を、ユーザー定義の間隔ごとに監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: DNS接続

- **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:** DNSサーバーとXenMobileノード間の接続を、ユーザー定義の間隔ごとに監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Googleストアサーバー接続

- **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:** GoogleストアサーバーとXenMobileノード間の接続を、ユーザー定義の間隔ごとに監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Windowsタブストア接続

- **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:** タブストアサーバーとXenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Windowsセキュリティトークンサーバー接続

- **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:** Windowsセキュリティトークンサーバーと XenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Windows通知サーバー接続

- **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:** Windows NotificationサーバーとXenMobileノード間の接続性を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Apple Push Notificationサーバー (APNs) 接続

- **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:** APNsとXenMobileノード間の接続性を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Apple Feedbackサーバー接続

- **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:** Apple FeedbackサーバーとXenMobileノード間の接続性を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Apple Storeサーバー接続

- **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:** Apple StoreサーバーとXenMobileノード間の接続性を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: XenMobileデータベース接続

- **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:** XenMobileデータベースとXenMobileノード間の接続性を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Firebase Cloud Messagingサーバー接続

- **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:** Firebase Cloud MessagingサーバーとXenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Citrix License Server接続

- **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:** Citrix License ServerとXenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: Citrix Gateway接続

- **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:** Citrix GatewayとXenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: XenMobileノード間接続

- **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:** XenMobileクラスターノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

トラップ名: XenMobile Tomcatノードサービス接続

- **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:** XenMobile Tomcatノードサービスと XenMobileノード間の接続を、ユーザー定義の間隔で監視します。接続に失敗した場合、XenMobileはSNMPトラップを生成します。

SNMPしきい値を構成する際の最適なサーバーパフォーマンスのために、以下の要素を考慮してください。

- 呼び出しの頻度
- 収集するトラップデータと閾値チェック
- ノード間通信メカニズム
- 接続チェックの頻度
- チェック中の障害発生時のタイムアウト

SNMPユーザーを追加するには

SNMPユーザーはSNMPマネージャーと対話し、トラップを受信します。

1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。「**設定**」ページが表示されます。
2. 「**監視**」の下にある「**SNMP構成**」をクリックします。「**SNMP構成**」ページが表示されます。

   SNMP構成の画像(/en-us/xenmobile/server/media/snmp-configuration-page.png)
3. 「**SNMP監視ユーザー**」の下にある「**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。

   SNMP構成の画像(/en-us/xenmobile/server/media/add-snmp-user.png)

   ユーザー名: SNMPマネージャーにログオンするために使用するユーザー名。英数字、アンダースコア、ハイフンを使用できますが、スペースやその他の特殊文字をユーザー名に使用することはできません。

   > **注:**
   >
   > XenMobileが内部使用のために名前を予約しているため、ユーザー名「xmsmonitor」を追加できません。

   > **認証プロトコル:**

   - **SHA** (推奨)
   - **MD5**

認証パスワード: 8文字から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。

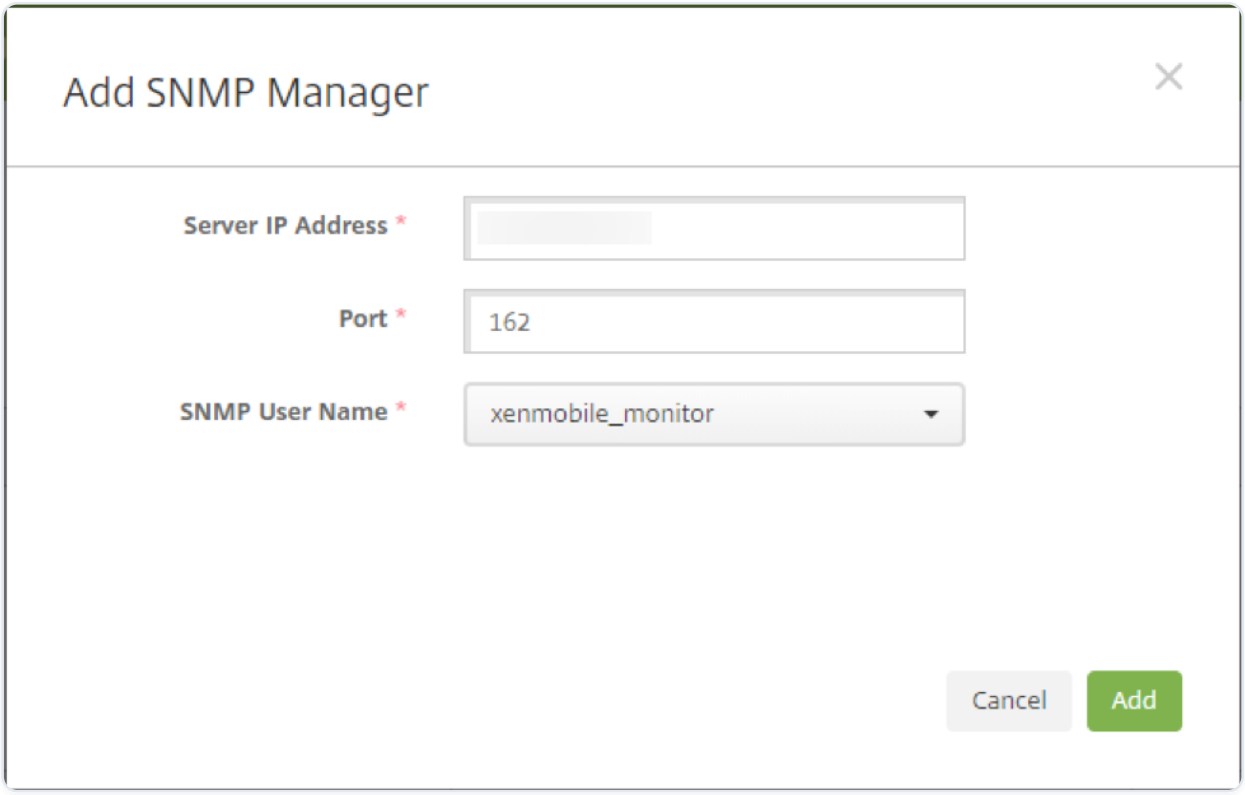
プライバシープロトコル:

- **DES**
- **AES 128** (推奨)

プライバシーパスワード: 8文字から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**で、**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。

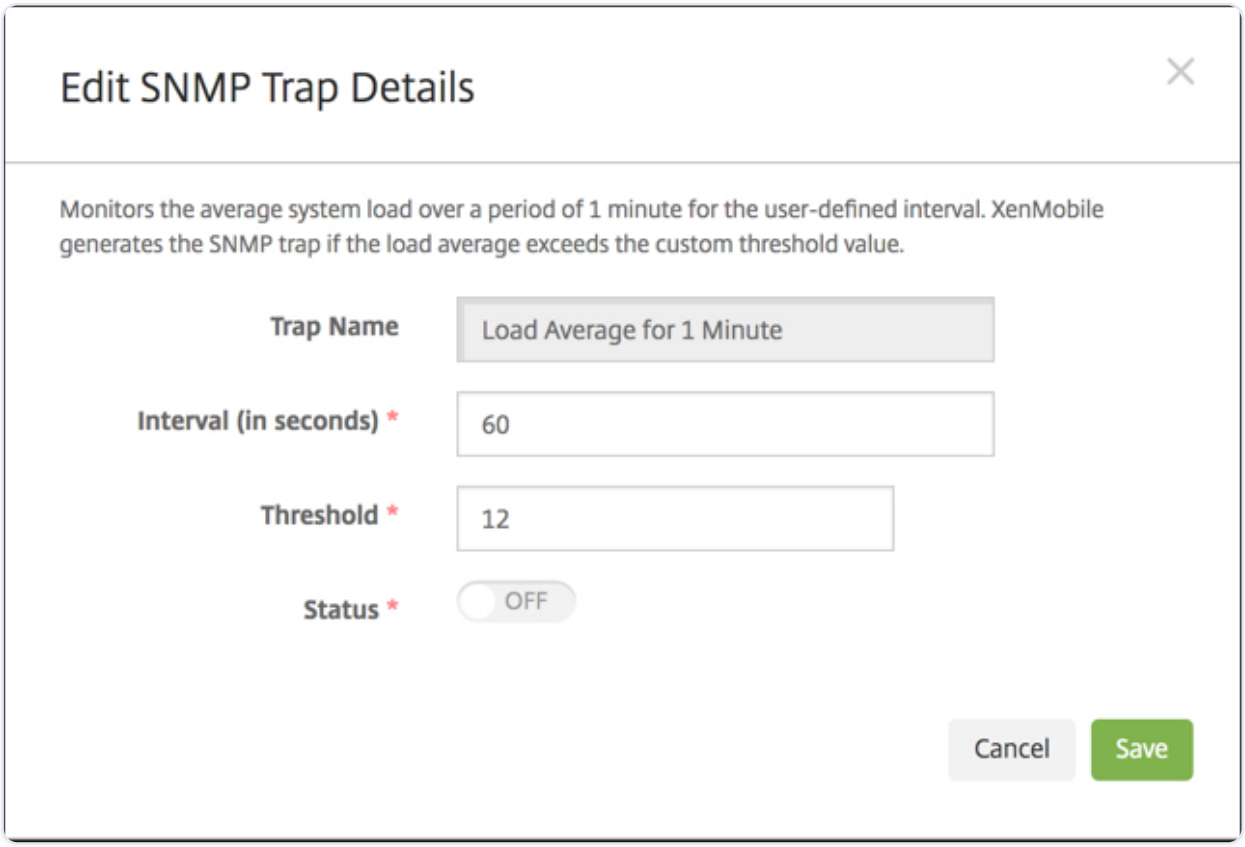
ポート: 必要に応じてポート番号を変更します。デフォルトは162です。

SNMPユーザー名: マネージャーへのアクセス権を持つ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1分間のロードアベレージを監視するには、1分間のロードアベレージを有効にしてしきい値を指定します。XenMobile Serverの1分間のロードアベレージが指定されたしきい値を超えると、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て、**［有効にする］**をクリックします。
   - リスト内のすべてのトラップを有効にするには、上部にあるチェックボックスをオンにして、**［有効にする］**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、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（秒単位）: 許容範囲は60～86400（24時間）です。

しきい値: 次のトラップにしきい値を変更できます。

- プロセッサ負荷
- 1分間のロードアベレージ
- 5分間のロードアベレージ
- 15分間のロードアベレージ
- 利用可能な合計メモリ
- 使用済みディスクストレージの合計
- Javaヒープメモリ使用量
- Javaメタスペース使用量

状態: トラップのSNMP監視を有効にするには、**ON**を選択します。監視を無効にするには、**OFF**を選択します。

SNMPを使用したXenMobileの監視に関する詳細情報については、こちらのブログ投稿を参照してください。

サポートバンドル

Citrix に問題を報告したり、問題をトラブルシューティングしたりするには、サポートバンドルを作成します。その後、サポートバンドルを Citrix Insight Services (CIS) に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以下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。これらのファイルのデフォルトのファイルサイズは 10 MB です。

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

サポートバンドルに各カテゴリのログアーカイブファイルが 100 個含まれると、ログファイルはロールオーバーします。ログファイルの最大数を少なく設定した場合、XenMobile® はそのノードの余分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、 > に移動します。

サポートバンドルを作成するには：

1. XenMobile コンソールで、右上隅にあるレンチアイコンをクリックします。 ページが表示されます。

2. ページで、 をクリックします。 ページが表示されます。XenMobile 環境にクラスターノードがある場合、すべてのノードが表示されます。

   サポートバンドル(/en-us/xenmobile/server/media/create-support-bundle.png)

3. チェックボックスが選択されていることを確認します。
4. XenMobile 環境にクラスターノードがある場合、 で、すべてのノードまたはデータの取得元となるノードの任意の組み合わせを選択できます。
5. 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は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が含まれます。
     - **デリバリーグループデータ:** アプリの種類とアプリ配信ポリシーの詳細を含むアプリデリバリーグループ情報が含まれます。
     - **デバイスとユーザー情報:** デバイスポリシー、アプリ、アクション、およびデリバリーグループが含まれます。
   - 「**すべてのデータ**」をクリックします。

   > **注:**
   >
   > 「**デバイスとユーザー情報**」または「**すべてのデータ**」を選択し、これが初めて作成するサポートバンドルである場合、「**機密情報に関する免責事項**」ダイアログボックスが表示されます。免責事項を読み、「**同意する**」または「**キャンセル**」をクリックします。「**キャンセル**」をクリックすると、サポートバンドルをCitrixにアップロードできません。「**同意する**」をクリックすると、サポートバンドルをCitrixにアップロードでき、次回デバイスまたはユーザーデータを含むサポートバンドルを作成する際には、この免責事項は表示されません。

   > サポートバンドルの法的通知(/en-us/xenmobile/server/media/support-bundle-legal-notice.png)

6. オプション「**サポートデータの匿名化がオンになっています**」は、デフォルト設定がデータの匿名化であることを示します。データ匿名化とは、機密性の高いユーザー、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内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、「**匿名化と匿名化解除**」をクリックします。データ匿名化の詳細については、「サポートバンドルでのデータ匿名化」を参照してください。

7. Citrix Gatewayからのサポートバンドルを含めるには、「**Citrix Gatewayのサポートバンドル**」チェックボックスをオンにして、次の操作を行います。

   a. 「**追加**」をクリックします。「**Citrix Gatewayサーバーの追加**」ダイアログボックスが表示されます。

   Citrix Gatewayサポートバンドル(/en-us/xenmobile/server/media/add-nsg-support-bundle.png)

   b. 「**Citrix Gateway管理IP**」に、サポートバンドルデータを取得したいCitrix GatewayのCitrix ADC管理IPアドレスを入力します。

   > **注記:**
   >
   > 既に追加されているCitrix Gatewayサーバーからバンドルを作成する場合、IPアドレスが提供されます。

   c. 「**ユーザー名**」と「**パスワード**」に、Citrix Gatewayを実行しているサーバーにアクセスするために必要なユーザー資格情報を入力します。

   > **注記:**
   >
   > 既に追加されているCitrix Gatewayサーバーからバンドルを作成する場合、ユーザー名が提供されます。

8. 「**追加**」をクリックします。新しいCitrix Gatewayサポートバンドルがテーブルに追加されます。
9. 手順7を繰り返して、さらにCitrix 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にアップロード**」と「**クライアントにダウンロード**」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、バンドルをCitrix Insight Services (CIS) にアップロードするか、コンピューターにダウンロードできます。

XenMobileからCISへのアップロードは、SSLアウトバウンド接続を介して行われます。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を開放してください。HTTPSトラフィックにプロキシを使用している場合は、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てください。

これらの手順は、バンドルをCISに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 IDと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にアップロード**」をクリックします。「**Citrix Insight Services (CIS) にアップロード**」ダイアログボックスが表示されます。
2. 「**ユーザー名**」に、My Citrix IDを入力します。
3. 「**パスワード**」に、My Citrixパスワードを入力します。
4. 既存のサービスリクエスト番号にこのバンドルを関連付ける場合は、**SR#に関連付ける**チェックボックスをオンにし、表示される2つの新しいフィールドで次の操作を行います。
   - **SR#** に、このバンドルを関連付けたい8桁のサービスリクエスト番号を入力します。
   - **SRの説明** 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が初めてで、他の製品を通じてCISでアカウントを作成しておらず、データ収集とプライバシーに関する契約に同意していない場合、次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、契約に同意する必要があります。CISにアカウントがあり、以前に契約に同意している場合は、サポートバンドルはすぐにアップロードされます。

   サポートバンドルの法的契約(/en-us/xenmobile/server/media/cis-legal-agreement.png)
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。

サポートバンドルをコンピューターにダウンロードする

サポートバンドルを作成した後、そのバンドルをCISにアップロードするか、コンピューターにダウンロードできます。自分で問題をトラブルシューティングしたい場合は、サポートバンドルをコンピューターにダウンロードしてください。

サポートバンドルの作成 ページで、**クライアントにダウンロード** 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。

サポートバンドルには、分析価値が異なるファイルが含まれています。ファイルとその分析価値のリストについては、次の表を参照してください。

ファイル名	種類	説明	値
DbDump.json	JSONデータベースダンプ	ユーザー/デバイス/アプリケーション情報	高
Garbage.html	HTMLファイル	Javaガベージコレクター	低
MemoryInfo.html	HTMLファイル	メモリ使用量 - Java関連のメモリ使用量	高
MultiNodeClusterInfo.html	HTMLファイル	クラスター構成	高
Patches.html	HTMLファイル	パッチ情報。xmspatches.txt の方が良い	高
pg_dump0.sql	PGダンプ	デフォルトのPostgreSQLインスタンスダンプ	中
rt_db/*	DBコピー (冗長、これはpg_dump0.sqlのバイナリ表現です)		該当なし
sas_config/c3p0.properties	プロパティファイル	C3P0 DB構成プロパティ	中
sas_config/catalina.policy	ポリシーファイル	Webサーバー Catalinaポリシー - ファイルは変更されません	低
sas_config/catalina.properties	プロパティファイル	Webサーバー Catalinaプロパティ - ファイルは変更されません	低

XENMOBILE®サーバー

ファイル名	種類	説明	値
sas_config/ew-config.properties	プロパティファイル	XMサーバーの構成に関する情報	高
sas_config/ew-config-reloadable.properties	プロパティファイル	セキュリティモデル情報	高
sas_config/hazelcast.xml	XMLファイル	Hazelcastログ - あまり役に立たないと思われます。	低
sas_config/pki.xml	XMLファイル	サードパーティのPKIサーバーが使用されているかどうかを判断するために使用できます。	高
sas_config/push_services.xml	XMLファイル	プッシュサービス - ファイルは変更されません	低
sas_config/server.xml	XMLファイル	ここに暗号情報 - セキュリティ関連	高
sas_config/sftu_config/AppC.properties	プロパティファイル	AppCプロパティ - ファイルは変更されません	低
sas_config/sftu_config/catalina.policy	ポリシーファイル	Catalinaポリシー - ファイルは変更されません	低
sas_config/sftu_config/catalina.properties	プロパティファイル	Catalinaプロパティ - ファイルは変更されません	低
sas_config/sftu_config/logging.properties	プロパティファイル	ログプロパティ - ファイルは変更されません	低

ファイル名	種類	説明	値
sas_config/sftu_config/server.xml	XMLファイル	ここに暗号情報 - セキュリティ関連	高
sas_config/sftu_config/server_migration.xml	XMLファイル	移行情報	高
sas_config/sftu_config/server_sftu.xml	XMLファイル	初回ユーザー設定	高
sas_config/sftu_config/tomcat-users.xml	XMLファイル	TomCat Users - ファイルは変更されません	低
sas_config/sftu_config/web.xml	XMLファイル	Web - ファイルは変更されません	低
sas_config/sftu.properties	プロパティファイル	SFTU構成プロパティ	高
sas_config/variables.xml	XMLファイル	変数 - ファイルは変更されません	低
sas_config/web.xml	XMLファイル	Webサーバー関連情報	中
sas_log/AdminAuditLogFile.log	Linuxログファイル	すべての構成変更	高
sas_log/create_sb_output.sh	Linuxログファイル	サポート生成コマンド出力	低
sas_log/DebugLogFile.log	Linuxログファイル	すべての機能ログ	高
sas_log/HibernateStats.log	Linuxログファイル	Hibernate統計ログ	低

ファイル名	種類	説明	値
sas_log/kafka-consumer.log	Linuxログファイル	Kafkaログ	低
sas_log/kafka-server.log	Linuxログファイル	Kafkaログ	低
sas_log/kafka-topics.log	Linuxログファイル	Kafkaログ	低
sas_log/LPE.log	Linuxログファイル	LPEログ	低
sas_log/migration.log	Linuxログファイル	移行プロセスの出力	中
sas_log/PlatformAuditLogFile.log	Linuxログファイル	バックエンド監査レベル情報	高
sas_log/PlatformDebugLogFile.txt	テキストファイル	バックエンドサーバー関連ログ	高
sas_log/postgres.log	Linuxログファイル	PostgreSQLログ	中
sas_log/SFTU.log	Linuxログファイル	SFTUログ	中
sas_log/tc1/catalina.log	Linuxログファイル	Catalina ログ	低
sas_log/tc1/console	Linux ログファイル	コンソール	低
sas_log/tc1/host-manager.log	Linux ログファイル	ホストマネージャー	低
sas_log/tc1/localhost.log	Linux ログファイル	ローカルホスト	低
sas_log/updates.log	Linuxログファイル	パッチ適用プロセスの出力	中
sas_log/UserAuditLogFile.log	Linuxログファイル	ユーザーアクション	高

ファイル名	種類	説明	値
sas_log/zookeeper.txt	テキストファイル	Zookeeperログ	低
snmp/snmpd_etc_netsnmp.conf	プロパティファイル	SNMP構成プロパティ	低
snmp/snmpd_privileges.conf	プロパティファイル	SNMP構成プロパティ	低
sys_info/arp_entries.txt	テキストファイル	XMSサーバーのARPエントリ	中
sys_info/chrony.txt	テキストファイル	Chronyログ	低
sys_info/diskspace_usage.txt	テキストファイル	ディスク領域の使用状況	高
sys_info/firewall_rules.txt	テキストファイル	XMSで定義されたファイアウォールルール	中
sys_info/interface_config.txt	テキストファイル	システムコマンド出力	中
sys_info/net_connections.txt	テキストファイル	システムコマンド出力	中
sys_info/root_account_info.txt	テキストファイル	システムコマンド出力	中
sys_info/routing_table.txt	テキストファイル	高い値	高
sys_info/running_process.txt	テキストファイル	高い値	高
sys_info/top.txt	テキストファイル	システムコマンド出力	中

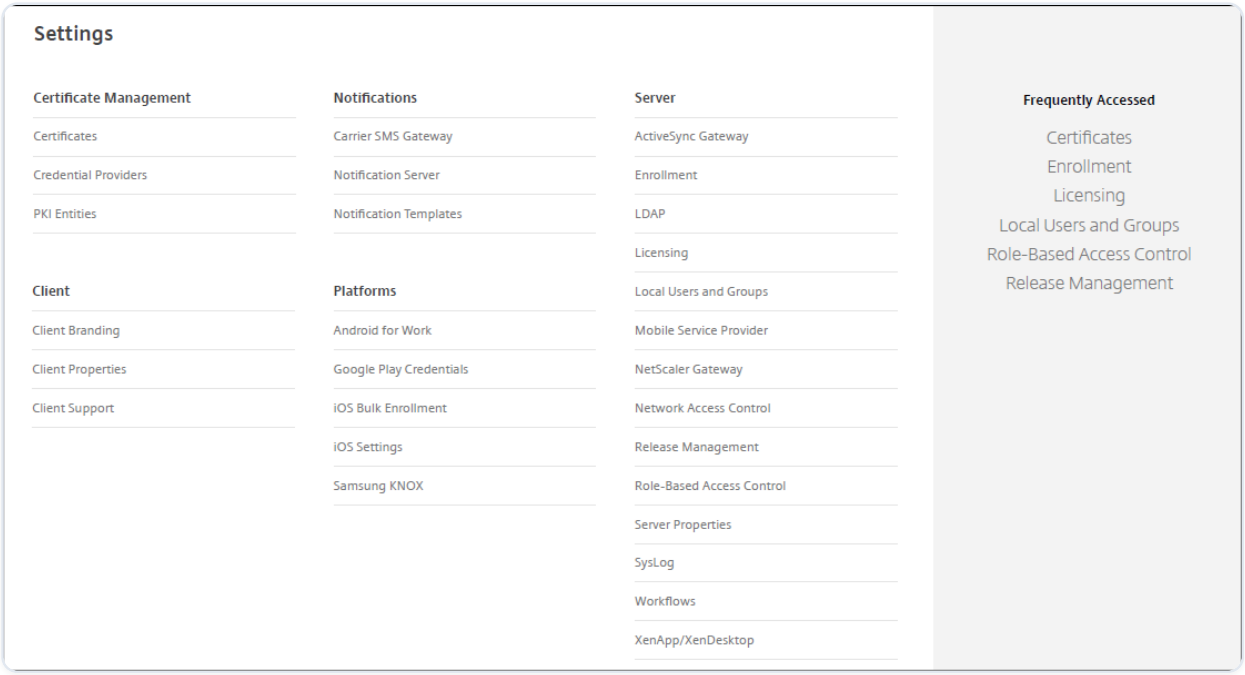
ファイル名	種類	説明	値
ThreadDump.html	HTMLファイル	使用されなくなりました。	低
ThreadDumpV2.html	HTMLファイル	スレッドスタックトレースなど	中
var_log/auth.log	Linuxログファイル	OSレベルのログ	中
var_log/boot.log	Linuxログファイル	OSレベルのログ	中
var_log/btmp	Linuxログファイル	OSレベルログ	中
var_log/daemon.log	Linuxログファイル	OSレベルログ	中
var_log/kern.log	Linuxログファイル	OSレベルログ	中
var_log/lastlog	Linuxログファイル	OSレベルログ	中
var_log/mail.log	Linuxログファイル	OSレベルログ	中
var_log/sys.log	Linuxログファイル	OSレベルログ	中
var_log/user.log	Linuxログファイル	OSレベルログ	中
var_log/wtmp	Linuxログファイル	OSレベルログ	中
version.txt	テキストファイル	XMサーバーのバージョン	中
XENMOBILE-`<IP Address>`-ConnectivityCheckResults.xml	XMLファイル	XMSサーバーでの接続チェック結果	中
xmspatches.txt	テキストファイル	パッチ情報。	高

サポートオプションとリモートサポート

ユーザーがサポート担当者に連絡するためのメールアドレスを提供できます。ユーザーがデバイスから支援を要求すると、そ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。ログを直接送信するか、メールで送信するかを設定できます。

1. XenMobile®コンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。



2. **クライアント**の下にある**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**ページが表示されます。
3. 次の設定を構成します。

   - **サポートメール (ITヘルプデスク):** ITヘルプデスクの連絡先メールアドレスを入力します。
   - **デバイスログをITヘルプデスクに送信:** デバイスログを**直接**送信するか、**メールで**送信するかを選択します。デフォルトは**メールで**です。

     - **直接**を有効にすると、ShareFile (現在はCitrix Files) にログを保存する設定が表示されます。ShareFileにログを保存する設定を有効にすると、ログはCitrix Filesに直接送信されます。そうでない場合、ログはXenMobileに送信され、その後ヘルプデスクにメールで送信されます。また、デフォルトで有効になっている**直接送信が失敗した場合、メールを使用する**オプションが表示されます。サーバーの問題のためにクライアントメールを使用してログを送信したくない場合は、このオプションを無効にできます。ただし、このオプションを無効にしてサーバーの問題が発生した場合、ログは送信されません。
     - **メールで**を有効にすると、ログの送信には常にクライアント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:**
>
> リモートサポートは、January 1, 2019 以降、新規のお客様には提供されなくなりました。既存のお客様は引き続き製品を使用できますが、Citrix は機能強化や修正を提供しません。

> オンプレミスのXenMobile Server展開の場合: リモートサポートにより、ヘルプデスク担当者は管理対象のAndroidモバイルデバイスをリモート制御できます。スクリーンキャストはSamsung Knoxデバイスでのみサポートされています。

クラスター化されたオンプレミスのXenMobile Server展開では、リモートサポートは利用できません。

リモート制御セッション中:

- ユーザーは、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をモバイルデバイスで確認できます。
- リモートサポートユーザーには、リモートサポートアプリケーションウィンドウと、制御対象デバイスのレンダリングを表示するリモート制御ウィンドウが表示されます。

リモートサポート(/en-us/xenmobile/server/media/remote-support-with-rendered-device.png)

リモートサポートを使用すると、次のことができます。

- ユーザーデバイスにリモートでサインオンし、画面を制御します。ユーザーは、あなたが画面を操作する様子を見ることができ、これはトレーニング目的にも役立ちます。
- リモートデバイスをリアルタイムで操作および修復します。構成を変更したり、オペレーティングシステムの問題をトラブルシューティングしたり、問題のあるアプリやプロセスを無効にしたり停止したりできます。
- ネットワークアクセスをリモートで無効にし、不正なプロセスを停止し、アプリやマルウェアを削除することで、脅威が他のモバイルデバイスに広がる前に隔離および封じ込めます。
- デバイスの着信音をリモートで有効にして電話をかけ、ユーザーがデバイスを見つけられるようにします。ユーザーがデバイスを見つけられない場合、機密データが侵害されないようにデバイスをワイプできます。

リモートサポートは、サポート担当者が次のことを行うことも可能にします。

- 1つ以上のXenMobileインスタンス内のすべての接続済みデバイスのリストを表示します。

- デバイスモデル、オペレーティングシステムレベル、国際移動体装置識別番号 (IMEI)、シリアル番号、メモリとバッテリーの状態、接続性などのシステム情報を表示します。
- XenMobileのユーザーとグループを表示します。
- デバイスのタスクマネージャーを実行し、アクティブなプロセスを表示、終了し、モバイルデバイスを再起動できます。
- モバイルデバイスと中央ファイルサーバー間の双方向ファイル転送を含むリモートファイル転送を実行します。
- 1つまたは複数のモバイルデバイスにソフトウェアプログラムを一括でダウンロードしてインストールします。
- デバイスのリモートレジストリキー設定を構成します。
- リアルタイムのデバイス画面リモートコントロールを使用して、低帯域幅のセルラーネットワークでの応答時間を最適化します。
- ほとんどのモバイルデバイスのブランドとモデルのデバイススキンを表示します。スキンエディターを表示して、新しいデバイスモデルを追加し、物理キーをマッピングします。
- デバイスでの一連の操作をキャプチャしてビデオAVIファイルを作成する機能により、デバイスの画面キャプチャ、記録、再生を有効にします。
- 共有ホワイトボード、VoIPベースの音声通信、モバイルユーザーとサポート担当者間のチャットを使用して、ライブ会議を実施します。

リモートサポートのシステム要件

リモートサポートソフトウェアは、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されます。ポート要件については、「ポート要件」を参照してください。

サポートされているプラットフォーム:

- Intel Xeon/Pentium 4 - 1 GHz以上 ワークステーションクラス
- 512 MB RAM以上
- 100 MB以上の空きディスク容量

サポートされているオペレーティングシステム:

- Microsoft Windows 2003 Server スタンダード エディション または エンタープライズ エディション SP1 以降
- Microsoft Windows 2000 プロフェッショナル SP4
- マイクロソフト ウィンドウズ XP SP2 以降

- マイクロソフト ウィンドウズ Vista SP1 以降
- Microsoft Windows 10 または Windows 11
- Microsoft Windows 8
- マイクロソフト Windows 7

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 はインストールプログラムの名前です。例:

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

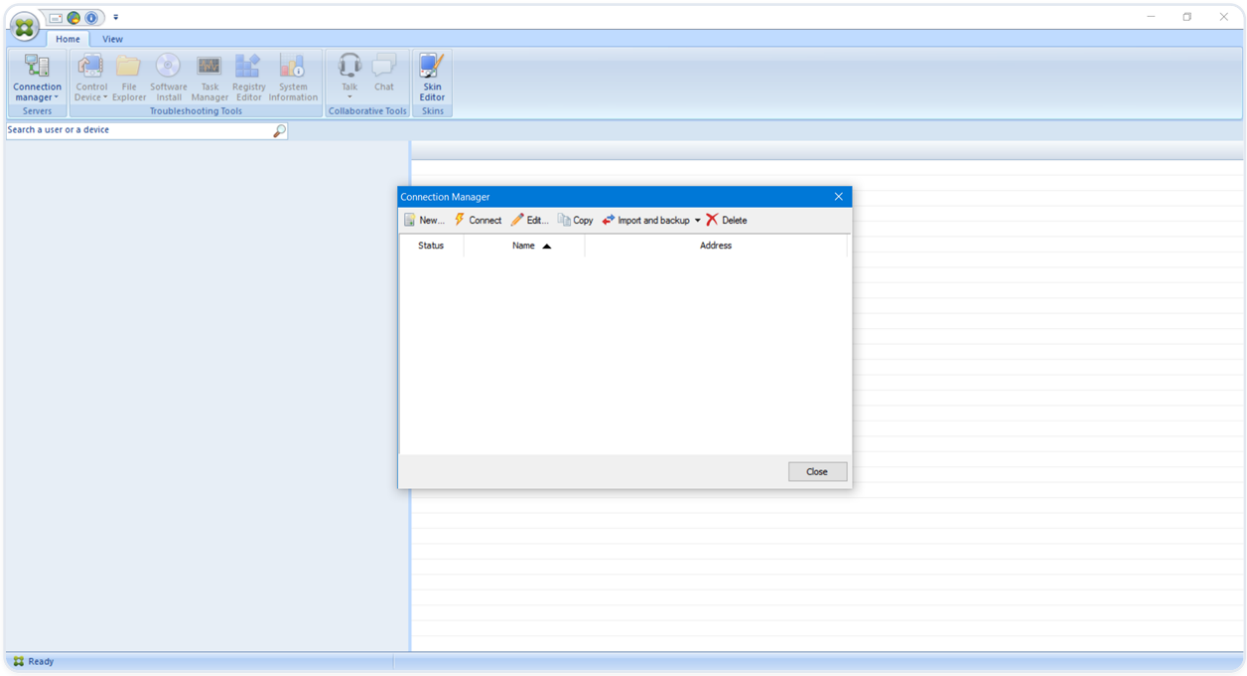
Remote Supportソフトウェアのインストール時に、次の変数を使用できます。

- /S: デフォルトパラメーターでRemote Supportソフトウェアをサイレントインストールします。
- /D=dir: カスタム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、デバイスを管理する1つ以上のXenMobile Serverへの接続を追加する必要があります。この接続は、AndroidデバイスのデバイスポリシーであるトンネルMDMポリシーで定義するアプリトンネルを介して実行されます。Remote SupportをXenMobileに接続する前に、アプリトンネルを定義してください。詳しくは、「アプリトンネリングデバイスポリシー」を参照してください。

1. リモートサポート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. **接続マネージャー**で、**新規**をクリックします。



3. **接続構成**ダイアログボックスの**サーバー**タブで、次の値を入力します。

   a. **構成名**に、構成エントリの名前を入力します。

   b. **サーバーIPアドレスまたは名前**に、XenMobileサーバーのIPアドレスまたはDNS名を入力します。

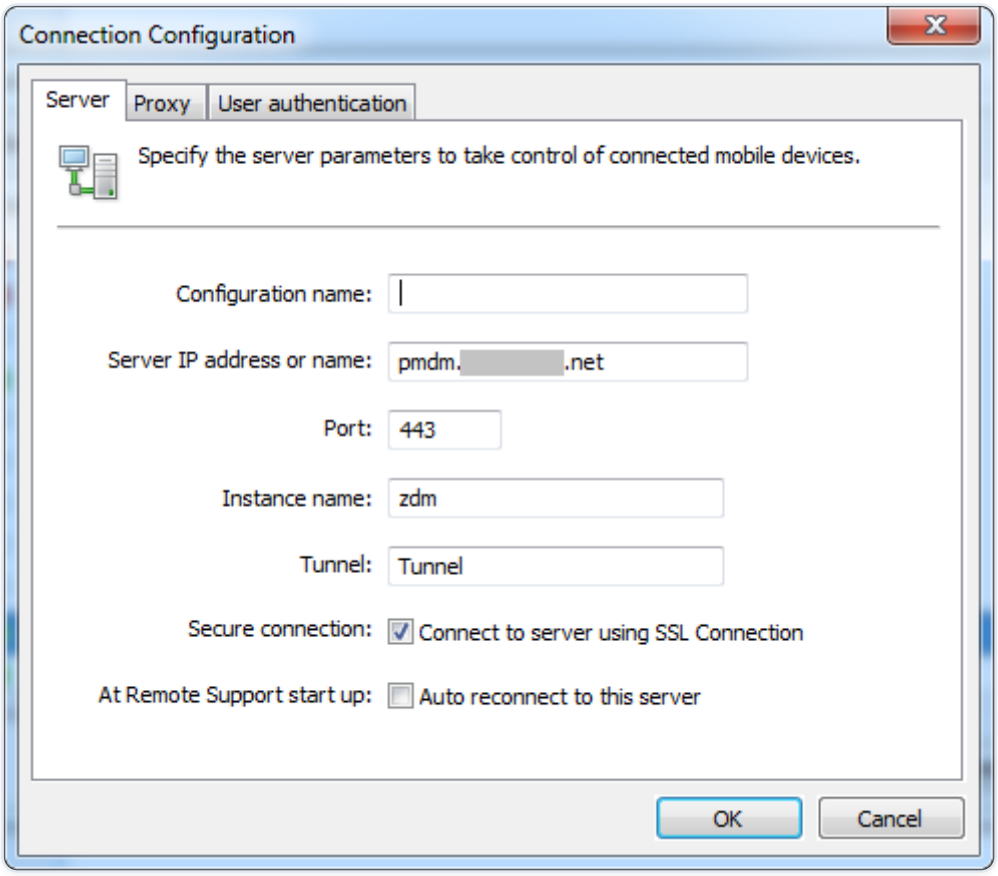
   c. **ポート**に、XenMobileサーバー構成で定義されているTCPポート番号を入力します。

   d. XenMobileがマルチテナント展開の一部である場合は、**インスタンス名**にインスタンス名を入力します。

   e. **トンネル**に、トンネルポリシーの名前を入力します。

   f. **SSL接続を使用してサーバーに接続**チェックボックスをオンにします。

   g. リモートサポートアプリケーションが起動するたびに構成済みのXenMobileサーバーに接続するには、**このサーバーに自動再接続**チェックボックスをオンにします。



4. **プロキシ**タブで、**HTTPプロキシサーバーを使用**を選択し、次の情報を入力します。

   a. **プロキシIPアドレス**に、プロキシサーバーのIPアドレスを入力します。

   b. **ポート**に、プロキシで使用されるTCPポート番号を入力します。

   c. プロキシサーバーがトラフィックを許可するために認証を必要とする場合は、**マイプロキシサーバーは認証を必要とします**チェックボックスをオンにします。

   d. **ユーザー名**に、プロキシサーバーで認証されるユーザー名を入力します。

   e. **パスワード**に、プロキシサーバーで認証されるパスワードを入力します。

   リモートサポートのセットアップ(/en-us/xenmobile/server/media/remote-support-connection-config-proxy.png)

5. **ユーザー認証**タブで、**ログインとパスワードを記憶する**チェックボックスをオンにし、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、そ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デバイスのリモートサポートを有効にするには

XenMobileでリモートサポートポリシーを作成すると、Samsung Knoxデバイスへのリモートアクセスが可能になります。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（メモリとCPUの使用状況）、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、ウィンドウの色を制御したり、ヘルプデスクとユーザー間でVoIPセッションを確立したり、ヘルプデスクとユーザー間でチャットセッションを確立したりできます。

  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ときは、**Samsung KNOX**プラットフォームのみを選択してください。Samsung SAFEプラットフォームの場合、ELMキーは、SamsungデバイスがXenMobileに登録されると自動的に展開されます。したがって、このポリシーではSamsung SAFEプラットフォームを選択しないでください。詳細については、「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構成については、「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

リモートサポートを開始すると、リモートサポート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、現在接続しているユーザーがいるグループのみが表示されます。各ユーザーのエントリの横に、その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、左側の列から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、緑色のアイコンで示されます。
2. 現在接続されていないユーザーを含むすべてのユーザーを表示するには、**表示**をクリックし、**未接続デバイス**を選択します。 未接続のユーザーは、小さな緑色のアイコンなしで表示されます。

XenMobile Serverに接続されているが、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。(リストに**匿名**という文字列が表示されます。)これらのデバイスは、ログインしているユーザーのデバイスと同様に制御できます。

デバイスを制御するには、その行をクリックしてデバイスを選択し、**デバイスの制御**をクリックします。デバイスのレンダリングがリモートコントロールウィンドウに表示されます。制御されたデバイスとは、次の方法で対話できます。

- メインウィンドウまたは別のフローティングウィンドウで、色付きの制御を含め、デバイスの画面を制御します。
- ヘルプデスクとユーザー間でVoIPセッションを確立します。VoIP設定を構成します。
- ユーザーとチャットセッションを確立します。
- デバイスのタスクマネージャーにアクセスし、メモリ使用量、CPU使用量、実行中のアプリなどの項目を管理します。
- モバイルデバイスのローカルディレクトリを探索します。ファイルを転送します。
- デバイスのシステム情報とインストールされているすべてのソフトウェアを表示します。
- XenMobile Serverとのモバイルデバイスの接続ステータスを更新します。

システムログ

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、2つのコンポーネントを持つ標準的なログプロトコルです。監査モジュール (アプライアンス上で実行されます) と、リモートシステム上で実行できるサーバーです。Syslogプロトコルは、データ転送に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、次の種類の情報を収集できます。

- XenMobileによって実行されたアクションの記録を持つシステムログ。
- XenMobileのシステムアクティビティの時系列記録を持つ監査ログ。

syslogサーバーがアプライアンスから収集するログ情報は、メッセージの形式でログファイルに保存されます。これらのメッセージには通常、次の情報が含まれます。

- 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 (Critical、Error、Notice、Warning、Informational、Debug、Alert、またはEmergency)

- メッセージ情報

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メッセージデータは、特定の形式を持たないプレーンテキストです。

この情報を使用して、アラートの原因を分析し、必要に応じて是正措置を講じることができます。

1. XenMobileコンソールで、右上隅にある歯車アイコンをクリックします。**設定**ページが表示されます。
2. **Syslog**をクリックします。**Syslog**ページが表示されます。
3. 以下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。デフォルトでは、ポートは514に設定されています。
    - **ログに記録する情報: システムログ**と**監査**を選択またはクリアします。
        - システムログには、XenMobileによって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記録が含まれます。
        - XenMobileのデバッグログ。
4. **保存**をクリックします。

XenMobile® でログファイルを表示する

XenMobile の管理に役立つログの表示、操作、ダウンロードを行います。

1. XenMobile コンソールで、コンソールの右上隅にある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. **ログ操作**の下にある**ログ**をクリックします。**ログ**ページが表示されます。個々のログがテーブルに表示されます。

    サポートログの画像(/en-us/xenmobile/server/media/support-logs.png)
3. 表示したいログを選択します。
    - 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 Support に役立つ情報が含まれています。
    - 管理者監査ログファイルには、XenMobile コンソールでのアクティビティに関する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、構成されたユーザーに関連する情報が含まれています。

- エラーログファイルには、デバッグログからフィルタリングされたエラーメッセージのみが含まれています。

4. テーブルの上部にあるアクションを使用して、すべてダウンロード、表示、ローテーション、単一ログのダウンロード、または選択したログの削除を行います。

   サポートログの分析画像(/en-us/xenmobile/server/media/analyze-logs.png)

   > **注:**
   >
   > - 複数のログファイルを選択した場合、**すべてダウンロード**と**ローテーション**のみが利用可能です。
   > - クラスター化された XenMobile サーバーを使用している場合、接続しているサーバーのログのみを表示できます。他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. 以下のいずれかを実行します。

   - **すべてダウンロード:** コンソールは、システムに存在するすべてのログ (デバッグ、管理者監査、ユーザー監査、サーバーログなど) をダウンロードします。
   - **表示:** 選択したログの内容をテーブルの下に表示します。
   - **ローテーション:** 現在のログファイルをアーカイブし、ログエントリをキャプチャするためのファイルを作成します。ログファイルをアーカイブするとダイアログボックスが表示されます。「ローテーション」をクリックして続行します。
   - **ダウンロード:** コンソールは、選択した単一のログファイルタイプのみをダウンロードします。また、その同じタイプのアーカイブされたログもダウンロードします。
   - **削除:** 選択したログファイルを完全に削除します。

   デバッグログの例の画像(/en-us/xenmobile/server/media/debug-log-file-example.png)

XenMobile® Server テレメトリーデータ要素

XenMobile Server 構成

イベントヘッダー

キー	説明	例
バージョン	ヘッダーのバージョンを示します。	1
id	一意のイベント ID (GUID) を示します。	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
タイプ	イベントの種類名を示します。	SYSTEM_CONFIGURATION
st	UTC形式のタイムスタンプを示します。	2011-08-12T20:17:46.384Z
本番	製品名を示します。	XenMobile.OnPrem
prodVer	製品バージョンを示します。	10.16.0.10123

イベントペイロード

キー	説明	例
バージョン	XenMobile Server構成ペイロードのバージョン番号を示します。	1.1
xmsVer	XenMobile Serverのバージョン番号を示します。	10.16.0.48
xmsrpVer	XenMobile Serverのローリングパッチバージョン番号を示します。	10.16.0.10323

キー	説明	例
dbType	XenMobile Serverのデータベースの種類を示します。	MSSQL
dbVer	XenMobile Serverのデータベースのバージョン番号を示します。	Microsoft SQL Server 2019 (RTM-CU8) (KB4577194) - 15.0.4073.23 (X64) Sep 23 2020 16:03:08 著作権 (C) 2019 Microsoft Corporation 標準エディション (64ビット) Windows Server 2016 Standard 10.0 X64 (Build 14393:) 上 (ハイパーバイザー)
hostType	XenMobile Serverのハイパーバイザーの種類を示します。	オンプレミス - XenServer®
instanceName	XenMobile Serverのインスタンス名を示します。	/ゼットディーエム
licenseType	XenMobile Serverでアクティベートされたライセンスの種類を示します。	CXM_ENTU_UD
sp	収集されるすべてのサーバープロパティを示します。	sp: {afw_restriction_v2: 真 device_page_enhancement_new: はい multimode: 有効

キー	説明	例
		http2_alternate_port: 無効 playemmapi_update: 有効 afw_efota: 有効 password_strength: 有効 モード: ENT wsdl: いいえ afw_restriction_cope: はい playemmapi: はい mac_app_push: 有効 ga: はい zdm_pki: はい tiffany: いいえ ios_mdm: はい nac_mail: いいえ console_ceip: 有効 ssl_sign: 有効 wip: 有効 zebra: 有効 apple_apns_http2: 有効

キー	説明	例
		afw_hide_vpn_always_on: 真 force_push_apps: 真 ftu: 偽 afw_vpn_always_on_lockdown: 真 mfa: 真 mobile_service_provider: 真 afw_network_domain: 真 deprecate_sms: 真 cert_self_signed: 真 ios_http2_pushtype_bg: 偽 device_update_awapppushtask: 有効 android.deprecate.policy: 有効 device_page_enhancement: 有効 macos_http2_pushtype_bg: 偽 edu_shared_ipad: 真 sync_license: 無効

キー	説明	例
		force_push_apps_flag: 有効 shp: 無効 wsapi: 無効 aw_dg_performance: 有効 apple_profile_renew: 真 afw_priority_update_apps: 真 esim: 真 wpcod: 真 knox: 真 device_report: 有効 ios_app_update: 有効 mspki_revert: トゥルー}

キー	説明	例	
cp	収集されるすべてのクライアントプロパティを示します。	cp: {PASSCODE_STRENGTH: 中 ENABLE_WORXHOME_CEIP: フォルス ENABLE_FIPS_MODE: 無効 DEVICE_LOGS_TO_IT_HELP_DESK: 無効 ENABLE_WORXHOME_GA: 有効 ENCRYPT_SECRETS_USING_PASSCODE: 無効 ENABLE_PASSCODE_AUTH: 無効 ON_FAILURE_USE_EMAIL: 真 PASSCODE_TYPE: 数値 CONTAINER_SELF_DESTRUCT_PERIOD: 0 PASSCODE_MIN_LENGTH: 6	

キー	説明	例
		ENABLE_CRASH_REPORTING: 真 PASSCODE_EXPIRY: 90 INACTIVITY_TIMER: 15 ENABLE_PASSWORD_CACHING: 無効 PASSCODE_MAX_ATTEMPTS: 15 PASSCODE_HISTORY: 5 ロギング無効化: false Touch ID認証有効化: false ビーコンチェック有効化: false}
enrolledDevices	登録済みデバイスの数を示します。	enrolledDevices: {ANDROID:1,iOS:2, MACOSX:1}
完全修飾ドメイン名	顧客のパブリックFQDNを示します。	zl225.xmqa.cloud.com
ladpAuthType	LDAP認証タイプを示します。	ドメイン
nodeCount	クラスター内のノードの数を示します。	4

キー	説明	例
managedApps	XenMobile Serverによって管理されているアプリケーションの数を示します。	1000
usersUsingMicroVPN	MicroVPNユーザーの数を示します。	9999
isIntuneIntegrated	IntuneがXenMobile Serverと統合されているかどうかを示します。	はい
configuratedPolicies	XenMobile Serverによって構成されたポリシーの数を示します。	7777

XenMobile Server の使用状況

イベントヘッダー

キー	説明	例
バージョン	ヘッダーのバージョンを示します。	1
id	一意のイベントID (GUID) を示します。	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
タイプ	イベントタイプ名を示します。	DEVICE_CHECKIN
st	UTC形式のタイムスタンプを示します。	2011-08-12T20:17:46.384Z
プロダクト	製品名を示します。	XenMobile.OnPrem
prodVer	製品バージョンを示します。	10.16.0.10123

キー	説明	例
ユーザー	ユーザー情報を示します。ローカルユーザーの場合、ペイロードにSIDはありません。**値はスクランブルされています。**	**ADユーザー** ユーザー: { upn: C982F651A44B3F7 **(常にスクランブルされます)** domain: C982F651A44B3F7 **(常にスクランブルされます)** email: C982F651A44B3F7 **(常にスクランブルされます)** sid: C982F651A44B3F7 **(常にスクランブルされます)}** **ローカルユーザー**
		ユーザー: { upn: C982F651A44B3F7 **(常にスクランブル化されています)** sAMAccountName: C982F651A44B3F7 **(常にスクランブル化されています)**}

イベントペイロード

キー	説明	例
バージョン	XenMobile Serverの使用状況ペイロードのバージョン番号を示します。	1.1
deviceType	デバイスの種類を示します。	iPhone
hostName	オンプレミス展開のお客様のFQDNを示します。	test.xmqa.cloud.com
platformInfo	デバイスプラットフォームを示します。	iPhone - iPhone
jailBroken	このキーは、デバイスが**JAILBROKEN**または**ROOT**の場合にのみ使用できます。タグがない場合、デバイスはJailbrokenまたはrootedではありません。	はい、またはいいえ
serialNum	デバイスのシリアル番号を示します（デフォルトでハッシュ化されています）。	KsPRhShj0h9IhbVkFEU7ZQ==
os	デバイスのOSタイプを示します。	iOS
managementMode	デバイスの管理モードを示しました。	MDM または MAM または XME または管理対象外
deviceId	内部デバイスの一意のIDを示します。	41CC018E-7CC0-4697-B07E-1E8CCEF7F592
監視対象	デバイスが監視対象であるかどうかを示します。	はい、またはいいえ
osVersion	デバイスのOSバージョン番号を示します。	16.4.1 (a)
イメーイ	利用可能な場合、デバイスのIMEI番号を示します。デフォ	6M6iBmcsokQxPQyeVwiaQQ==

キー	説明	例
	ルトでハッシュ化されています。	
deviceModel	デバイスのモデルを示します。	iPhone
lastActivity	デバイスの最終アクティビティのタイムスタンプを示します。	2024-03-29 14:17:14.277
corporateOwned	デバイスが企業所有であるかどうかを示します。	いいえ
enabledFeatures	複数の機能の有効化を示します。	1
エルピーイーアイディー	一意のXMSサイトを識別するために使用できる一意の環境IDを示します。	95ba4968cfaf069c20949d76473ecd4f3994f556d0fef7f2fa11912731d720bf または、LASが利用できない場合は空白

REST API

> **注:**
>
> この記事では、XenMobile Server の REST API について説明します。Endpoint Management の REST API については、「REST API」を参照してください。

> XenMobile® REST API を使用すると、XenMobile コンソールを通じて公開されているサービスを呼び出すことができます。任意の 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 は、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ことを要求しません。

利用可能な API の完全な最新セットについては、「REST サービス用パブリック API」PDF をダウンロードしてください。

REST API にアクセスするために必要な権限

REST API へのアクセスには、次のいずれかの権限が必要です。

- ロール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。詳細については、「RBAC を使用したロールの構成」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、Chrome 用の Advanced REST クライアントを使用しています。

> **注:**
>
> 以下の例では、ホスト名とポート番号を環境に合わせて変更してください。

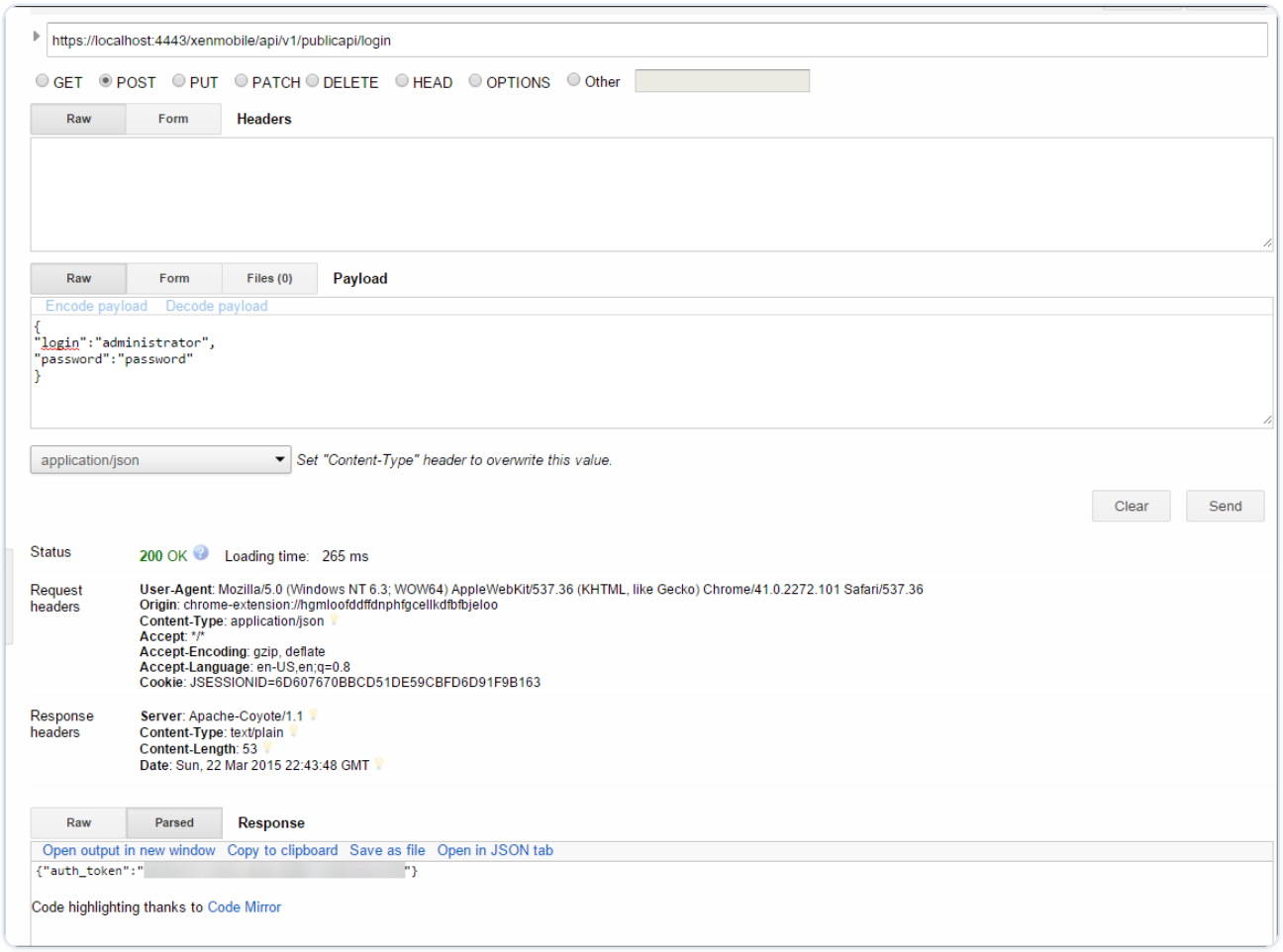
ログイン

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

リクエスト: `{ "login":"administrator", "password":"password" }`

メソッドタイプ: POST

コンテンツタイプ: application/json



関連情報

- XenMobile REST API

Exchange ActiveSync 用 Endpoint Management コネクタ

XenMobile Mail Manager は、Exchange ActiveSync 用 Endpoint Management コネクタになりました。Citrix の統合ポートフォリオの詳細については、Citrix 製品ガイドを参照してください。

このコネクタは、XenMobile® の機能を次の方法で拡張します。

- Exchange Active Sync（EAS）デバイスの動的アクセス制御。EAS デバイスは、Exchange サービスへのアクセスを自動的に許可またはブロックできます。
- XenMobile が Exchange によって提供される EAS デバイスのパートナーシップ情報にアクセスする機能。
- XenMobile が EAS ステータスに基づいてモバイルデバイスをワイプする機能。
- XenMobile が Blackberry デバイスに関する情報にアクセスし、ワイプやパスワードのリセットなどの制御操作を実行する機能。

EAS ステータスに基づいてデバイスをワイプするには、ActiveSync トリガーを使用して自動アクションを構成します。自動アクションを参照してください。

Exchange ActiveSync 用 Endpoint Management コネクタをダウンロードするには：

1. `<https://www.citrix.com/downloads>` にアクセスします。
2. **Citrix Endpoint Management™ (および Citrix XenMobile Server) > XenMobile Server (オンプレミス) > 製品ソフトウェア > XenMobile Server 10 > サーバーコンポーネント** に移動します。
3. **Citrix Endpoint Management connector for Exchange ActiveSync** タイルで、**Download File** をクリックします。

> **重要：**

> 2022年10月以降、Microsoft がこちらで発表した認証変更に伴い、Exchange ActiveSync 用 Endpoint Management および Citrix Gateway コネクタは Exchange Online をサポートしな

> くなります。Exchange 用 Endpoint Management コネクタは、Microsoft Exchange Server（オンプレミス）で引き続き動作します。

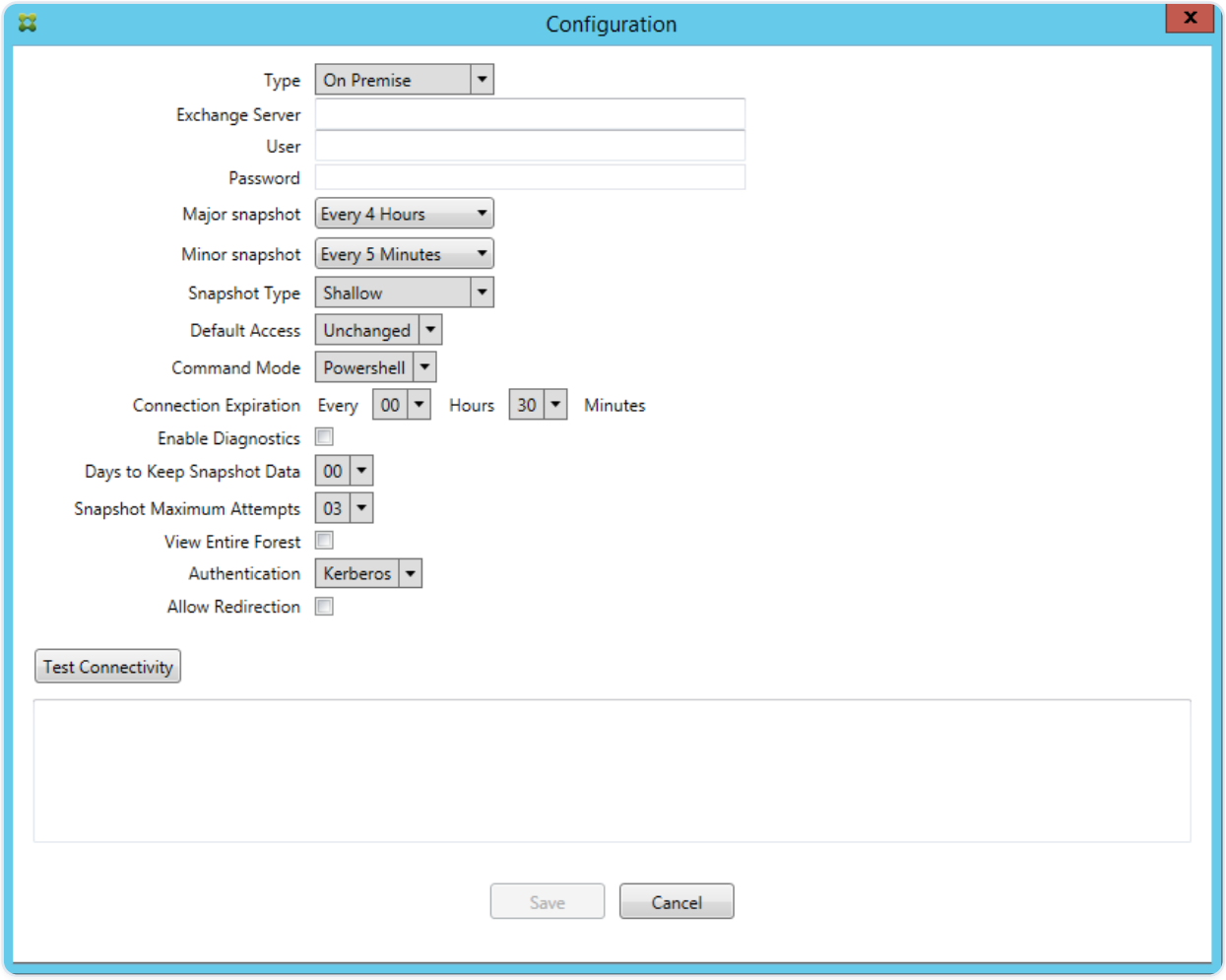
新機能

以下のセクションでは、以前はXenMobile Mail Managerと呼ばれていたExchange ActiveSync用Endpoint Managementコネクタの新機能について説明します。

バージョン10.1.10の新機能

バージョン10.1.10では、以下の問題が修正されています。

- 頻繁にネットワークの問題が発生するお客様は、以前提供されていた3回の試行回数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、管理者が最大試行回数（1〜10回）を設定できます。この修正により、スナップショットプロセスを完全に中断することなく、通信の中断が複数回発生してもスナップショットを続行できるようになります。



- 以前のバージョンでは、スナップショットタイプがExchange構成のリストに表示されませんでした。今回のバージョンでは、スナップショットタイプが表示されるようになりました。

- PowerShellによって報告されるPSRemotingTransport例外は、Exchangeへのセッションがもはや有効ではないことを示します。このステータスは、デフォルトで構成ファイルの「重大なエラー」リストに追加されます。これにより、PSRemotingTransportExceptionが検出されると、接続は後で破棄するためにエラー状態としてマークされます。次回の通信では、有効な接続が使用されるか、新しい接続が作成されます。
- 構成の変更が保存される際、新しい構成をロードする前に、以前に構成されたすべての内部コンポーネントが適切に破棄されない可能性があります。この問題は、予測不能な動作につながる可能性があります。動作は、特定の変更と、その変更が以前の構成と競合したかどうかに依存します。このリリースでは、新しい構成をロードする前にすべての内部コンポーネントが破棄されます。

以前のバージョンの新機能

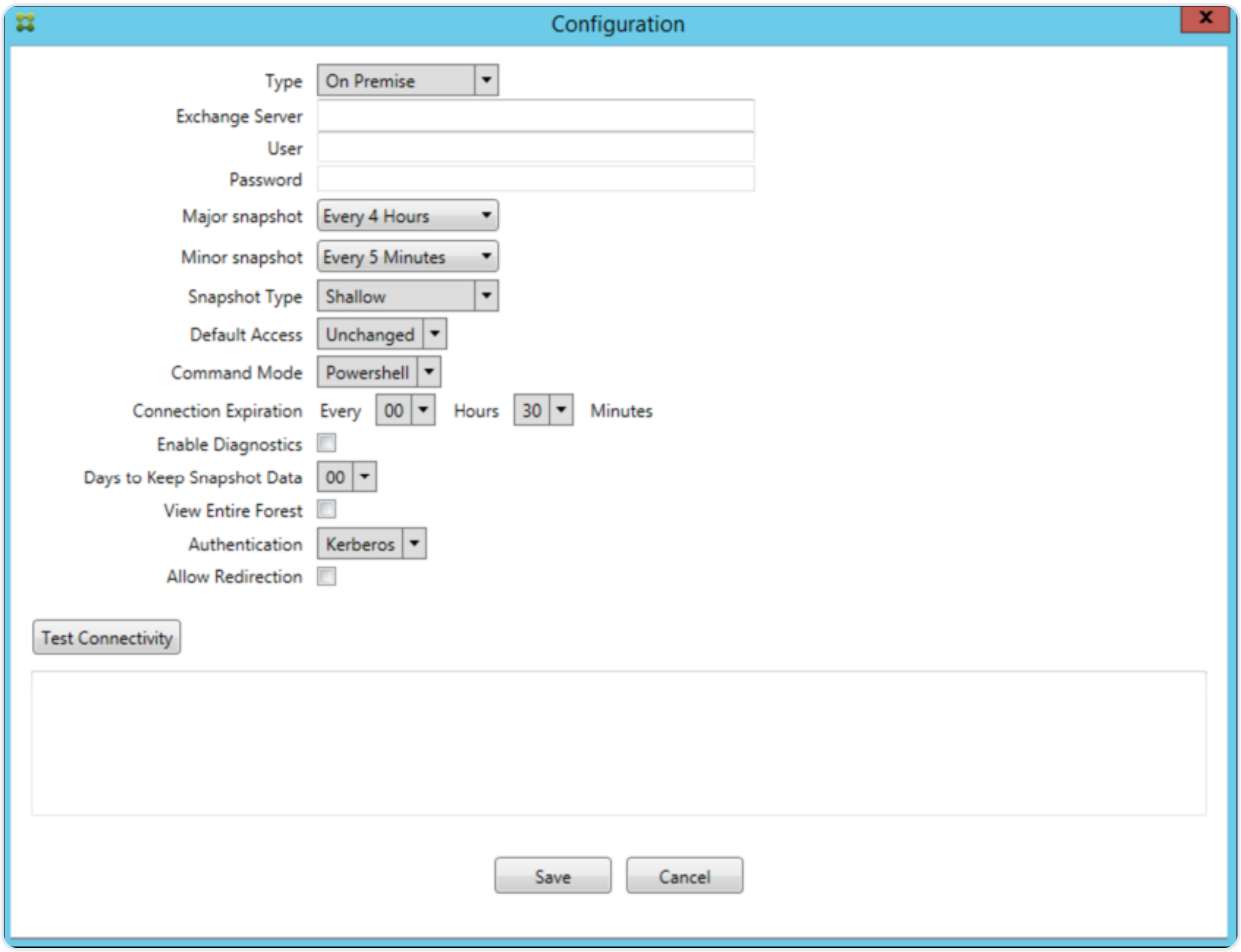
以下のセクションでは、Exchange ActiveSync用Endpoint Managementコネクタの以前のバージョンの機能と修正された問題について説明します。

バージョン10.1.9の新機能

バージョン10.1.9では、以下の問題が修正されています。

- 構成の変更がより一貫した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され、アクティブまたはスケジュールされた処理が中断されます。次に、新しい構成がロードされ、サブシステムが再起動されます。これにより、すべてのスケジュールおよびその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。この問題は、バージョン10.1.8の既知の問題を修正します。
- 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。データベース構成は、アップグレードされた構成ファイルにマージされるようになりました。
- スナップショット関連の診断ファイルで、列ヘッダーが欠落していました。ヘッダーが復元されました。
- 以前のバージョンからアップグレードする際、構成ファイルのデフォルトセクションが、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デフォルトセクションへの追加や改善がサービスによってロードされませんでした。このバージョン以降、デフォルトセクションは常に最新の構成を反映します。
- アプリケーションの実行中にShiftキーを押しても、管理者は特定のオプションにアクセスできなくなりました。これらのオプションは以前、Citrixの許可があれば利用可能でした。「リダイレクトの許可 (Allow Redirection)」などの一部のオプションは完全に利用可能になり、「ハ

ング検出 (Hang Detection)」や「カウント修正 (Count Correction)」などの他のオプションは非推奨になりました。



バージョン10.1.8の新機能

バージョン10.1.8で修正された問題は次のとおりです。

- Exchangeは、Exchange ActiveSyncサービス用のCitrix Endpoint Managementコネクタがコマンドを頻繁に発行しすぎないようにスロットリングする可能性があります。これはOffice 365への接続でよく見られます。スロットリングの影響により、サービスは次のコマンドを送信する前に指定された期間一時停止する必要があります。Configureコンソールに、一時停止の残り時間が表示されるようになりました。
- 構成ファイル (config.xml) の「Watchdog」または「SpecialistsDefaults」セクションに変更が加えられた場合、アップグレード後にその変更が構成ファイルに反映されません。このリリースでは、変更が新しい構成ファイルに正しくマージされます。
- Google Analyticsに送信される分析情報に、特にスナップショットに関する詳細が追加されました。
- Exchangeの接続テスト機能は、接続の初期化を1回だけ試行していました。Office 365接続はスロットリングされる可能性があるため、スロットリング時に接続テストが失敗したように見

えることがありました。Exchange ActiveSync用Citrix Endpoint Managementコネクタは、接続を最大3回試行するようになりました。

- Exchangeでポリシーを適用するには、Exchange ActiveSync用Citrix Endpoint Managementコネクタが、各メールボックスに関連するすべてのデバイスを許可リストとブロックリストの2つのリストに含める**Set-CASMailbox**コマンドをコンパイルする必要があります。デバイスがどちらのリスト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戻ります。そのデフォルトのアクセス状態がデバイスの望ましい状態と異なる場合、そのデバイスはコンプライアンス違反になります。その結果、Exchangeのデフォルトのアクセス状態がブロックされており、許可されるべきである場合に、ユーザーがメールへのアクセスを失う可能性があります。あるいは、メールへのアクセスがブロックされるべきユーザーにアクセスが許可される可能性もあります。Exchange ActiveSync用Citrix Endpoint Managementコネクタは、有効な望ましい状態を持つすべてのデバイスが各**Set-CasMailbox**コマンドに含まれるようにします。

バージョン10.1.8で確認されている問題は次のとおりです。

管理者がConfigureアプリケーションで構成データを変更する際に、サービスがスナップショットやポリシー評価などの長時間かかる操作を実行している場合、サービスが不定の状態になる可能性があります。起こりうる症状としては、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が考えられます。サービスを動作状態に戻すには、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を使用してサービスプロセスを終了する必要がある場合があります。

バージョン10.1.7の新機能

- XenMobile Mail Managerは、Exchange ActiveSync用Endpoint Managementコネクタになりました。
- Exchange構成ダイアログボックスの**Disable Pipelining**オプションは非推奨になりました。config.xmlファイルで各コマンドに複数のステップを構成することで、同じ機能を実現できます。

バージョン10.1.7で修正された問題は次のとおりです。

- スナップショット履歴ウィンドウでは、エラーメッセージがほとんどコンテキストなしで表示される場合があります。現在、エラーメッセージには、発生した場所のコンテキストがプレフィックスとして付けられます。
- 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。

- 診断を改善するため、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されるデバイスIDのリストの文字列形式を最近変更しました。しかし、あまりにも多くのデバイスを指定すると、最大文字列サイズを超えてしまいました。現在、内部配列データ構造を使用しています。この構造にはサイズ制限がなく、診断目的でデータを適切にフォーマットします。
- Exchangeと同期していないデバイスポリシーが検出された場合、そのコマンドには関連するメールボックスに属さないデバイスが含まれる可能性があります。Endpoint Management connector for Exchange ActiveSync は、Exchangeへのコマンドがそれぞれのメールボックスに属するデバイスのみを表すようにします。
- 一部の環境では、Microsoftアセンブリが利用できません。必要なアセンブリは、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。
- デバイスまたはメールボックスの識別名に、属性名と等号の間にスペースがある場合、および/または等号の後と値の前にスペースがある場合、Endpoint Management connector for Exchange ActiveSync はデバイスをそのメールボックスと適切に照合できない可能性があり、その逆も同様です。その結果、スナップショットの調整中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。

> **注:**
>
> 以下のセクションでは、Endpoint Management connector for Exchange ActiveSync を旧称のXenMobile Mail Managerで参照しています。名称はバージョン10.1.7から変更されました。

バージョン10.1.6.20での更新

10.1.6への更新には、バージョン10.1.6.20の以下の修正が含まれています。

- Exchangeと同期していないデバイスポリシーが検出された場合、そのコマンドには関連するメールボックスに属さないデバイスが含まれる可能性があります。XenMobile Mail Managerは、Exchangeへのコマンドがそれぞれのメールボックスに属するデバイスのみを表すようにします。

バージョン10.1.6の新機能

XenMobile Mail Manager バージョン10.1.6には、以下の修正された問題と機能強化が含まれています。

- スナップショット履歴ウィンドウが、更新されなくなる状態になることがあります。ウィンドウの更新メカニズムが改善され、より確実に更新されるようになりました。

- パーティション化された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は、2つの異なるモードと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「*」パーティションを使用する構成のパーティション化されたスナップショットと同等であるため、パーティション化されていないスナップショットモードは廃止されました。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）を持つ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。
- スナップショット履歴ウィンドウでは、エラーメッセージがステータスメッセージによって上書きされていました。現在、XenMobile Mail Managerは2つの別々のフィールドを提供し、ユーザーがステータスとエラーを同時に表示できるようにしています。
- Exchange Online (Office 365) に接続する際、スナップショット関連のクエリがデータセットの切り捨てを引き起こす可能性があります。この問題は、XenMobile Mail Managerが複数コマンドのパイプラインスクリプトを実行する際に発生する可能性があります。アップストリームコマンドがダウンストリームコマンドにデータを十分に速く渡せず、ダウンストリームコマンドが prematurely に処理を完了してしまうためです。その結果、不完全なデータが発生します。XenMobile Mail Managerは、パイプライン自体を模倣し、アップストリームコマンドが完了するまで待ってからダウンストリームコマンドを呼び出すことができ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、キャプチャされるはずです。
- Exchangeへのポリシー更新コマンドで解決不可能なエラーが発生した場合、同じコマンドが長期間にわたって繰り返しワークキューに戻されていました。この状況により、コマンドがExchangeに何度も送信されていました。このバージョンのXenMobile Mail Managerでは、エラーが発生したコマンドは、ワークキューに特定の回数だけ戻されるようになりました。
- 特定のメールボックスに対するポリシー更新で、すべてのデバイスの許可またはブロックが含まれる場合: 発行された **Set-CASMailbox** コマンドは、空のリストが **NULL** ではなく空の文字列に変換されるため、失敗していました。適切なデータが送信されるようになりました。
- 新しいデバイスを処理する際、Exchangeはしばらくの間（通常15分間）状態を「DeviceDiscovery」として返すことがあります。XenMobile Mail Managerはこの状態を具体的に処理していませんでした。XenMobile Mail Managerは現在この状態を処理します。UIの「監視」タブで、ユーザーはこの状態のデバイスをフィルタリングできます。
- XenMobile Mail Managerは、XenMobile Mail Managerデータベースへの書き込み権限をチェックしていませんでした。その結果、権限が制限されている場合、動作を予測できませんでした。XenMobile Mail Managerは現在、データベースから必要な権限をキャプチャして検証します。XenMobile Mail Managerは、接続テスト時（メッセージが表示されます）またはメインの「構成」ウィンドウの下部にあるデータベースインジケーター（メッセージを表示するにはホバーします）で、権限が削減されていることを示します。
- 現在のワークロードによっては、指示されたときにXenMobile Mail Managerサービスがすぐに停止しない場合があります。そのため、サービスが応答しない状態にあるように見えます。改

善により、進行中のタスクを中断できるようになり、より正常なシャットダウンが可能になります。

バージョン10.1.5の新機能

XenMobile Mail Managerバージョン10.1.5には、以下の修正された問題が含まれています。

- ExchangeがXenMobile Mail Managerのアクティビティにスロットリングを適用している場合、スロットリングが発生していることを示す表示（ログ以外）がありませんでした。このリリースでは、ユーザーがアクティブなスナップショットにカーソルを合わせると、「スロットリング」状態が表示されます。また、XenMobile Mail Managerがスロットリングされている間は、Exchangeがスロットリングの禁止を解除するまで、メジャースナップショットの開始が禁止されます。
- メジャースナップショット中にXenMobile Mail ManagerがExchangeによってスロットリングされている場合: 次のスナップショット試行を実行する前に、十分な時間が経過しない可能性があります。この問題は、さらなるスロットリングとスナップショットの失敗につながります。XenMobile Mail Managerは現在、Exchangeがスナップショット試行間に待機するよう指定した時間の最小値を待機します。
- 診断が有効になっている場合、コマンドファイルには、各プロパティ名の前にハイフンが欠落している **Set-CasMailbox** コマンドが表示されます。この問題は、診断ファイルのフォーマットのみで発生し、Exchangeへの実際のコマンドでは発生しません。ハイフンが欠落しているため、ユーザーはコマンドを切り取ってPowerShellプロンプトに直接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。ハイフンが追加されました。
- メールボックスのIDが「lastname, firstname」の形式である場合、Exchangeはクエリからデータを返す際にコンマの前にバックスラッシュを追加します。XenMobile Mail ManagerがそのIDを使用してさらにデータをクエリする場合、このバックスラッシュを削除する必要があります。

既知の制限事項

> **注:**

> 以下の制限はバージョン10.1.6で解決されています。

> XenMobile Mail Managerには、Exchangeへのコマンドが失敗する原因となる既知の制限があります。Exchangeにポリシー変更を適用するために、XenMobile Mail Managerによって**Set_CASMailbox**コマンドが発行されます。このコマンドは、許可するデバイスとブロック

> するデバイスの2つのリストを受け取ることができます。このコマンドは、メールボックスと提携しているデバイスに適用されます。

これらのリストは、Microsoft APIによってそれぞれ256文字に制限されています。いずれかのリストがこの制限を超えると、コマンド全体が失敗し、そのメールボックスのデバイスに対するすべてのポリシーが設定されなくなります。XenMobile Mail Managerのログに表示されるエラーは、次のようになります。この例はブロックされたリストに関するものです。

「メッセージ: 'ActiveSyncBlockedDeviceIDs' パラメーターをターゲットにバインドできません。"ActiveSyncBlockedDeviceIDs" の設定中に例外が発生しました: "プロパティの長さが長すぎます。最大長は256ですが、指定された値の長さは…"」

デバイスIDの長さは様々ですが、約10台以上のデバイスが同時に許可またはブロックされると、制限を超える可能性があるという目安があります。特定のメールボックスに関連付けられているデバイスがそれほど多くなることは稀ですが、可能性はあります。XenMobile Mail Managerがこのようなシナリオを処理できるように改善されるまで、ユーザーとメールボックスに関連付けられるデバイスの数を10以下に制限することをお勧めします。

バージョン10.1.4の新機能

XenMobile Mail Managerバージョン10.1.4には、以下の修正された問題が含まれています。

- セキュリティの脆弱化のため、PCI協議会によってTLS 1.0は非推奨とされています。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。
- XenMobile Mail Managerには新しい診断ファイルが含まれています。Exchangeの仕様で**Enable Diagnostics**が選択されている場合、新しいスナップショット履歴ファイルが生成されます。スナップショットの試行ごとに、スナップショットの結果を示す行がファイルに追加されます。
- コマンド診断ファイルでは、**Set-CASMailbox**コマンドに対して許可またはブロックされたデバイスのリストが表示されませんでした。代わりに、関連する引数に対して内部クラス名がファイルに表示されていました。XenMobile Mail Managerは、デバイスIDのリストをカンマ区切りのリストとして表示するようになりました。
- 不正な仕様が原因でExchangeへの接続の取得に失敗した場合、エラーメッセージが「すべての接続が使用中です」という誤ったメッセージで上書きされていました。現在では、「すべての接続が動作不能です」、「接続プールが空です」、「すべての接続がスロットリングされています」、「利用可能な接続がありません」などの、より詳細なメッセージが表示されます。
- XenMobile Mail Managerの内部キャッシュに、許可/ブロック/ワイプコマンドが複数回キューに入れられることがありました。この問題により、Exchangeへのコマンド送信が遅延してい

ました。XenMobile Mail Managerは、各コマンドのインスタンスを1つだけキューに入れるようになりました。

バージョン10.1.3の新機能

- **Google Analyticsのサポート:** お客様がXenMobile Mail Managerをどのように使用しているかを知ることで、製品をより良くするための改善点に注力できます。
- **診断を有効にする設定: 構成**ダイアログボックスの構成コンソールに、**診断を有効にする**チェックボックスが表示されます。

エンドポイント マネジメント コネクタ for エクスチェンジ アクティブシンク コンソールの画像(/en-us/xenmobile/server/media/mail-manager-diagnostics-checkbox.png)

バージョン10.1.3で修正された問題

- 「**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ヒントが実際の状態を反映していません。 まれに、XenMobile Mail ManagerがCommands診断ファイルに書き込めないことがあります。この場合、コマンド履歴が完全にログに記録されません。
- 接続でエラーが発生した場合、その接続が「エラー状態」としてマークされないことがあります。その結果、後続のコマンドがその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。
- Exchange Serverからのスロットリングが発生すると、Check Healthルーチンで例外がスローされることがあります。その結果、エラーが発生した接続や期限切れの接続がパージされない可能性があります。また、スロットリング時間が経過するまで、XenMobile Mail Managerが接続を作成しない可能性があります。
- Exchangeの最大セッション数を超過すると、XenMobile Mail Managerは「Device Capture Failed」というエラーを報告しますが、これは正確なメッセージではありません。代わりに、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であるべきです。

バージョン10.1.2の新機能

- **Exchangeへの接続の改善**: XenMobile Mail ManagerはPowerShellセッションを使用してExchangeと通信します。PowerShellセッションは、特にOffice 365を扱う場合、しばらくすると不安定になり、後続のコマンドの成功を妨げることがあります。XenMobile Mail Managerは、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セッションを正常にシャットダウンし、新しい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。

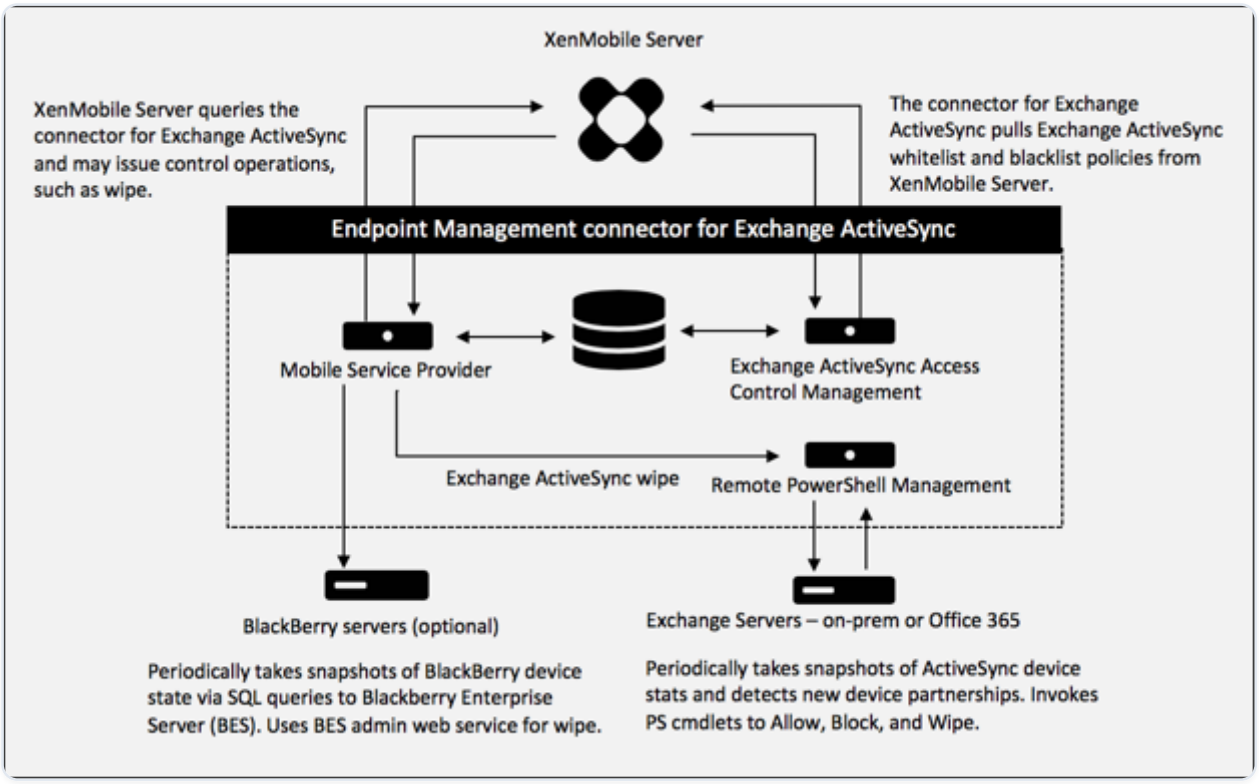
- **スナップショットワークフローの改善**: メジャースナップショットは時間とプロセスを大量に消費する操作です。スナップショット中にエラーが発生した場合、XenMobile Mail Managerはスナップショットを完了するために複数回（最大3回）試行するようになりました。後続の試行は最初から開始されません。XenMobile Mail Managerは中断したところから続行します。この機能強化により、スナップショットが進行中でも一時的なエラーを通過させることで、スナップショットの成功率が全体的に向上します。
- **診断機能の改善**: スナップショット操作のトラブルシューティングが、スナップショット中にオプションで生成される3つの新しい診断ファイルによって容易になりました。これらのファイルは、PowerShellコマンドの問題、情報が不足しているメールボックス、メールボックスに関連付けられないデバイスの特定に役立ちます。管理者はこれらのファイルを使用して、Exchangeで正しくない可能性のあるデータを特定できます。
- **メモリ使用量の改善**: XenMobile Mail Managerは、メモリ使用においてより効率的になりました。管理者は、システムをクリーンな状態にするために、XenMobile Mail Managerを自動的に再起動す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。

修正された問題

- 資格情報のプロンプトエラー: Office 365セッションの不安定性がこのエラーの主な原因でした。「Exchangeへの接続の改善」機能強化により、この問題が解決されます。(XMHELP-293, XMHELP-311, XMHELP-801)
- メールボックスとデバイス数の不正確さ: XenMobile Mail Managerは、メールボックスとデバイスの関連付けアルゴリズムを改善しました。「診断機能の改善」機能は、XenMobile Mail Managerがその責任範囲外と見なすメールボックスとデバイスの特定に役立ちます。(XMHELP-623)
- 許可/ブロック/ワイプ コマンドが認識されない: XenMobile Mail Managerの許可/ブロック/ワイプ コマンドが認識されない場合があるバグが修正されました。(XMHELP-489)
- メモリ管理: メモリ管理と軽減策が改善されました。(XMHELP-419)

アーキテクチャ

次の図は、Exchange ActiveSync用Endpoint Managementコネクタの主要コンポーネントを示しています。詳細な参照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。



主な3つのコンポーネントは次のとおりです。

- **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、このポリシーをローカルで定義されたポリシーとマージして、Exchangeへのアクセスを許可または拒否すべき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グループ、ユーザー、デバイスタイプ、またはデバイスユーザーエージェント（通常はモバイルプラットフォームのバージョン）によるアクセス制御を許可するようにポリシー規則を拡張できます。
- **リモートPowerShell管理:** Exchange ActiveSyncアクセス制御管理によってコンパイルされたポリシーを実行するために、リモートPowerShellコマンドのスケジュール設定と呼び出しを担当します。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がExchange ActiveSyncのクエリ、Blackberryデバイスのクエリ、およびActiveSyncデバイスとBlackberryデバイスに対するワイプなどの制御操作を発行できるように、Webサービスインターフェイスを提供します。

システム要件と前提条件

Exchange ActiveSync用Endpoint Managementコネクタを使用するには、以下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である必要があります。Windows Server 2008 R2 Service

Pack 1のサポートはJanuary 14, 2020に終了し、Windows Server 2012 R2のサポートはOctober 10, 2023に終了します。

- Microsoft SQL Server 2016 サービスパック 2 または SQL Server 2014 サービスパック 3。
- Microsoft .NET フレームワーク 4.6。
- Blackberry Enterprise Service、バージョン5（オプション）。

Microsoft Exchange Server の最小サポートバージョン:

- マイクロソフト オフィス 365
- エクスチェンジ サーバー 2016
- エクスチェンジ サーバー 2013 (サポート終了 April 11, 2023)
- エクスチェンジ サーバー 2010 サービス パック 3 (サポート終了 January 14, 2020)

前提条件

- Windows Management Framework がインストールされている必要があります。
  - PowerShell V5、V4、および V3
- PowerShell の実行ポリシーは、Set-ExecutionPolicy RemoteSigned を使用して RemoteSigned に設定する必要があります。
- Endpoint Management connector for Exchange ActiveSync 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 が開いている必要があります。
- **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対して常に同じ ActiveSync ID を返すわけではありません。Endpoint Management connector for Exchange ActiveSync は各デバイスに対して一意の ActiveSync ID を期待するため、各デバイスに対して常に同じ一意の ActiveSync ID を生成するメールクライアントのみがサポートされます。以下のメールクライアントはCitrixによってテストされ、エラーなしで動作しました:
  - Samsung ネイティブメールクライアント
  - iOS ネイティブメールクライアント
- **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次のとおりです。

  Exchange 構成UIで指定された資格情報は、Exchange Serverに接続でき、以下の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権が付与されている必要があります。

  - **Exchange Server 2010 SP2 の場合:**

- ゲット-CASメールボックス
- セット-CASメールボックス
- ゲット-メールボックス
- Get-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- クリア-アクティブシンクデバイス
- Get-ExchangeServer
- Get-ManagementRole
- Get-ManagementRoleAssignment

- **Exchange Server 2013 および Exchange Server 2016 の場合:**
  - ゲット-CASメールボックス
  - セット-CASメールボックス
  - ゲット-メールボックス
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - クリア-モバイルデバイス
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- Endpoint Management connector for Exchange ActiveSync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、**Set-AdServerSettings -ViewEntireForest $true**を実行する権限が付与されている必要があります。
- 提供された資格情報には、リモートシェル経由でExchange Serverに接続する権限が付与さ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っています。
- リモート接続を確立し、リモートコマンドを実行するには、資格情報はリモートマシン上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、そのコマンドに関する説明はこのドキュメントの範囲外です。詳細については、Microsoftの記事「セッション構成について」を参照してください。

- Exchange Serverは、HTTP経由のリモートPowerShellリクエスト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がいれば十分です: WinRM QuickConfig。
- Exchangeには多くのスロットリングポリシーがあります。そのポリシーの1つは、ユーザーごとに許可される同時PowerShell接続の数を制御します。Exchange 2010では、ユーザーに許可される同時接続のデフォルト数は18です。接続制限に達すると、Endpoint Management connector for Exchange ActiveSyncはExchange Serverに接続できません。PowerShell経由で許可される同時接続の最大数を変更する方法がありますが、それらはこのドキュメントの範囲外です。興味がある場合は、PowerShellによるリモート管理に関連するExchangeのスロットリングポリシーを調べてください。

Office 365 Exchangeの要件

- **権限:** Exchange構成UIで指定された資格情報は、Office 365に接続でき、以下の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権が付与されている必要があります。
  - ゲット-CASメールボックス
  - セット-CASメールボックス
  - ゲット-メールボックス
  - 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付与さ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が必要な特権を持っています。
- **スロットリングポリシー:** Exchangeには多くのスロットリングポリシーがあります。そのポリシーの1つは、ユーザーごとに許可されるPowerShellの同時接続数を制御します。Office 365では、ユーザーに許可される同時接続のデフォルト数は3です。接続制限に達すると、Exchange ActiveSync用Endpoint ManagementコネクタはExchange Serverに接続できません。PowerShellを介して許可される同時接続の最大数を変更する方法がありますが、これはこのド

キュメントの範囲外です。興味がある場合は、PowerShellによるリモート管理に関連するExchangeのスロットリングポリシーを調べてください。

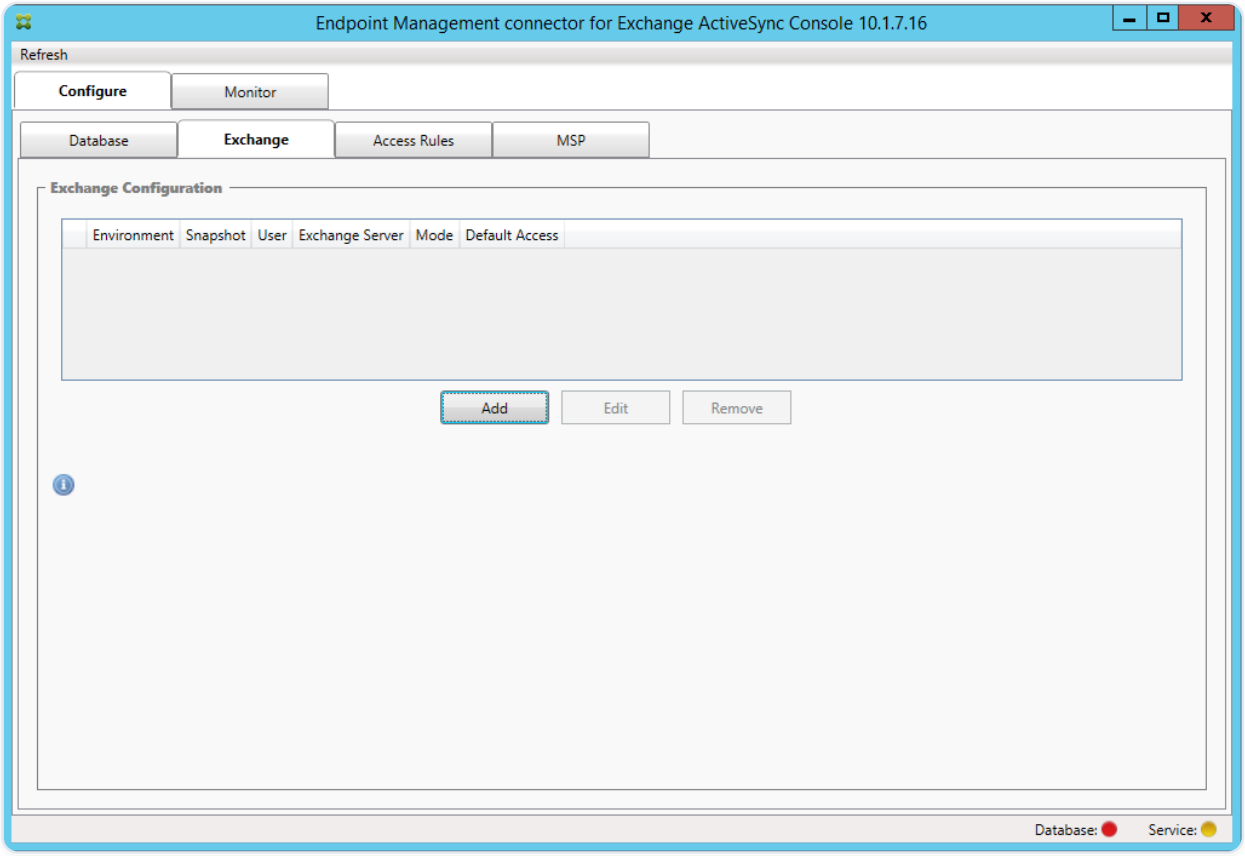
インストールと構成

1. XmmSetup.msiファイルをクリックし、インストーラーの指示に従ってExchange ActiveSync用Endpoint Managementコネクタ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を起動**が選択されたままにします。または、**スタート**メニューからExchange ActiveSync用Endpoint Managementコネクタを開きます。
3. 次のデータベースプロパティを構成します。
   - **構成 > データベース**タブを選択します。
   - SQL Serverの名前を入力します（デフォルトはlocalhost）。
   - データベースはデフォルトの**CitrixXmm**のままにします。
4. SQLで使用する以下の認証モードのいずれかを選択します。
   - **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 Integrated:** このオプションを選択した場合、Endpoint Management connector for Exchange ActiveSync Serviceのログオン資格情報を、SQL Serverにアクセスする権限を持つ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**を開き、Endpoint Management connector for Exchange ActiveSync Serviceのエントリを右クリックして、**ログオン**タブをクリックします。

   BlackBerryデータベース接続にもWindows Integratedが選択されている場合、ここで指定されたWindowsアカウントにもBlackBerryデータベースへのアクセス権を付与する必要があります。
5. **Test Connectivity**をクリックしてSQL Serverへの接続が可能であることを確認し、**Save**をクリックします。
6. サービスを再起動するようメッセージが表示されます。**Yes**をクリックします。

   Endpoint Management connector for Exchange ActiveSyncセットアップ画面の画像(/en-us/xenmobile/server/media/xmm-install-2.png)
7. 1つ以上のExchange Serverを構成します。

- 単一のExchange環境を管理している場合は、単一のサーバーのみを指定します。複数のExchange環境を管理している場合は、各Exchange環境に対して単一のExchange Serverを指定します。
- **Configure > Exchange**タブをクリックし、**Add**をクリックします。



8. Exchange Server環境のタイプを選択します: **On Premise**または**Office 365**。

- **On Premise**を選択した場合は、Remote PowerShellコマンドに使用するExchange Serverの名前を入力します。
- 「要件」セクションで指定されているように、Exchange Server上で適切な権限を持つWindows IDの**ユーザー名**を入力し、そのユーザーの**パスワード**を入力します。
- メジャーな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。メジャーなスナップショットは、すべてのExchange ActiveSyncパートナーシップを検出します。
- 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は、新しく作成されたExchange ActiveSyncパートナーシップを検出します。
- スナップショットの種類を、**ディープ**または**シャロー**から選択します。シャロー スナップショットは通常はるかに高速で、Endpoint Management connector for Exchange ActiveSync のすべての Exchange ActiveSync アクセス制御機能を実行するのに十分です。ディープ スナップショットは時間がかかる場合があり、ActiveSync でモバイルサービスプ

ロバイダーが有効になっている場合にのみ必要です。このオプションにより、XenMobileは管理対象外のデバイスを照会できます。

- デフォルトアクセスを、**許可**、**ブロック**、または**変更なし**から選択します。この設定は、明示的なXenMobileまたはローカルルールによって識別されたデバイス以外のすべてのデバイスがどのように扱われるかを制御します。**許可**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。**ブロック**を選択すると、アクセスが拒否されます。**変更なし**を選択すると、変更は行われません。
- ActiveSyncコマンドモードを、**PowerShell**または**シミュレーション**から選択します。
- **PowerShell**モードでは、Endpoint Management connector for Exchange ActiveSync は、目的のアクセス制御を実行するためにPowerShellコマンドを発行します。シミュレーションモードでは、Endpoint Management connector for Exchange ActiveSync はPowerShellコマンドを発行しませんが、意図されたコマンドと意図された結果をデータベースにログ記録します。シミュレーションモードでは、ユーザーは**監視**タブを使用して、PowerShellモードが有効になっていた場合に何が起こったかを確認できます。
- **接続の有効期限**で、接続の有効期間を時間と分で設定します。接続が指定された期間に達すると、その接続は期限切れとしてマークされ、二度と使用されなくなります。期限切れの接続が使用されなくなると、Endpoint Management connector for Exchange ActiveSyncはその接続を正常にシャットダウンします。接続が再度必要になった場合、利用可能な接続がない場合は新しい接続が初期化されます。指定がない場合、デフォルトの30分が使用されます。
- **フォレスト全体を表示**を選択して、Exchange環境内のActive Directoryフォレスト全体を表示するようにEndpoint Management connector for Exchange ActiveSync を構成します。
- 認証プロトコルを、**Kerberos**または**基本**から選択します。Endpoint Management connector for Exchange ActiveSync は、オンプレミス展開の基本認証をサポートしています。これにより、Endpoint Management connector for Exchange ActiveSync サーバーがExchangeサーバーが存在するドメインのメンバーではない場合でも、Endpoint Management connector for Exchange ActiveSync を使用できます。
- **接続テスト**をクリックしてExchange Serverへの接続が可能であることを確認し、**保存**をクリックします。
- サービスを再起動するようメッセージが表示されます。**はい**をクリックします。

9. アクセスルールを構成します。**構成 > アクセスルール**タブを選択し、**XMSルール**タブをクリックして、**追加**をクリックします。

   Exchange ActiveSync 用 Endpoint Management コネクタのルールの画像(/en-us/xenmobile/server/media/connector-access-rules.png)

10. **XenMobileサーバーサービスプロパティ**ページで、URL文字列をXenMobileサーバーを指すように変更します。たとえば、インスタンス名が**zdm**の場合、`https://<XdmHostName>/zdm/services/MagConfigService`と入力します。この例では、**XdmHostName**をXenMobileサーバーのIPアドレスまたはDNSアドレスに置き換えます。

    Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/xmm-install-7.png)

    - サーバーの認証済みユーザーを入力します。
    - ユーザーのパスワードを入力します。
    - **Baseline Interval**、**Delta Interval**、および**Timeout**の値はデフォルトのままにします。
    - **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選択されている場合、XenMobile Mail ServiceはXenMobileからポリシーを収集しません。

11. **Local Rules**タブをクリックします。

    Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/connector-access-rules-local.png)

    - ActiveSyncデバイスID、デバイスの種類、ADグループ、ユーザー、またはデバイスのUserAgentに基づいてローカルルールを追加できます。リストから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。

    グループ以外のすべての種類について、システムはスナップショットで検出されたデバイスに依存します。したがって、開始したばかりでスナップショットを完了していない場合、利用可能なエンティティはありません。

    - 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、ルールの順序を変更したり、削除したりできます。特定のユーザーとデバイスの場合、ルールは表示されている順序で評価され、上位のルール（上部に近い）に一致すると、それ以降のルールは無効になるため、順序は重要です。たとえば、すべてのiPadデバイスを許可するルールがあり、その後にユーザーMattをブロックするルールがある場合、iPadルールがMattルールよりも高い実効優先度を持つため、MattのiPadは引き続き許可されます。
    - ルールリスト内のルールを分析して、潜在的なオーバーライド、競合、または補足的な構成を見つけるには、**Analyze**をクリックし、**Save**をクリックします。

12. Active Directoryグループに対して機能するローカルルールを構築する場合は、**Configure LDAP**をクリックし、LDAP接続プロパティを構成します。

    Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/xmm-install-8.png)

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、XenMobileが管理対象外のデバイスを照会するために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するように構成されている場合にのみ必要です。

    - 「**Configure > MSP**」タブをクリックします。

    Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/connector_msp.png)

    - モバイルサービスプロバイダーサービスに対して、サービストランスポートタイプを**HTTP**または**HTTPS**に設定します。
    - モバイルサービスプロバイダーサービスに対して、**サービスポート**（通常は80または443）を設定します。ポート443を使用する場合、そのポートにはIISでバインドされたSSL証明書が必要です。
    - **承認グループ**または**ユーザー**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に接続できるユーザーまたはユーザーのセットが設定されます。
    - ActiveSyncクエリを有効にするかどうかを設定します。XenMobile ServerでActiveSyncクエリが有効になっている場合、1つ以上のExchange Serverのスナップショットタイプを**Deep**に設定する必要があります。この設定は、スナップショットの取得に大きなパフォーマンスコストがかかる可能性があります。
    - 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**ActiveSyncのフィルター**フィールドを変更します。 空白の場合、すべてのデバイスがXenMobileに転送されます。
    - 「**保存**」をクリックします。

14. オプションで、BlackBerry Enterprise Server (BES) のインスタンスを1つ以上構成します。「**追加**」をクリックし、BES SQL Serverのサーバー名を入力します。

    Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/xmm-install-10.png)

    - 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。Windows統合認証を選択した場合、Endpoint Management connector for Exchange ActiveSyncサービスのユーザーアカウントが、BES SQL Serverへの接続に使用されるアカウントになります。Endpoint Management connector for Exchange ActiveSyncデータベース接続にもWindows統合を選択した場合、ここで指定されたWindowsアカウントにもEndpoint Management connector for Exchange ActiveSyncデータベースへのアクセス権を付与する必要があります。
- **SQL認証**を選択した場合は、ユーザー名とパスワードを入力します。
- **同期スケジュール**を設定します。これは、BES SQL Serverに接続し、デバイスの更新を確認するために使用されるスケジュールです。
- 「**接続テスト**」をクリックして、SQL Serverへの接続を確認します。Windows統合を選択した場合、このテストは現在ログオンしているユーザーを使用し、Endpoint Management connector for Exchange ActiveSyncサービスユーザーは使用しないため、SQL認証を正確にテストするものではありません。
- XenMobileからBlackBerryデバイスのリモートワイプとパスワードリセットをサポートするには、**Enabled**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 (FQDN) を入力します。
- 管理Webサービスに使用される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とパスワードを入力します。
- BESへの接続をテストするには、**Test Connectivity**をクリックします。
- **Save**をクリックします。

ActiveSync IDでメールポリシーを適用する

企業のメールポリシーによっては、特定のデバイスが企業メールの使用を承認されていない場合があります。このポリシーに従うために、従業員がそのようなデバイスから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 connector for Exchange ActiveSync と XenMobile は連携して、このようなメールポリシーを適用します。XenMobile は企業メールアクセスに関するポリシーを設定し、未承認のデバイスが XenMobile に登録されると、Endpoint Management connector for Exchange ActiveSync 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、デバイスの識別に使用されるデバイスID（ActiveSync IDとも呼ばれる）を使用して、Exchange Server（またはOffice 365）に自身を通知します。Secure Hubは同様の識別子を取得し、デバイスが登録されるとXenMobileにその識別子を送信します。2つのデバイスIDを比較することで、Exchange ActiveSync用Endpoint Managementコネクタは、特

定のデバイスが企業メールアクセスを持つべきかどうかを判断できます。次の図はこの概念を示しています。

ActiveSync ID検出ワークフローの図(/en-us/xenmobile/server/media/enforce-email-policies-figure.png)

XenMobileが、デバイスがExchangeに公開するIDとは異なるActiveSync IDをEndpoint Management connector for Exchange ActiveSyncに送信した場合、Endpoint Management connector for Exchange ActiveSyncはExchangeにそのデバイスをどうすべきかを指示できません。

ActiveSync IDの一致は、ほとんどのプラットフォームで確実に機能します。しかし、Citrixは一部のAndroid実装において、デバイスからのActiveSync IDがメールクライアントがExchangeに通知するIDと異なることを発見しました。この問題を軽減するために、次のことができます。

- Samsung SAFEプラットフォームでは、XenMobileからデバイスのActiveSync構成をプッシュします。

企業メールアクセス ポリシーが適切に適用されることを保証するために、防御的なセキュリティ体制を採用し、Endpoint Management connector for Exchange ActiveSync を構成して、静的ポリシーをデフォルトで拒否に設定することでメールをブロックできます。これは、従業員が Android デバイスでメール クライアントを構成し、ActiveSync ID 検出が適切に機能しない場合、その従業員は企業メールアクセスを拒否されることを意味します。

アクセス制御ルール

Endpoint Management connector for Exchange ActiveSync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ルールベースのアプローチを提供します。Endpoint Management connector for Exchange ActiveSyncのアクセス制御ルールは、一致式と目的のアクセス状態（許可またはブロック）の2つの部分で構成されます。特定のExchange ActiveSyncデバイスに対してルールが適用されるか、デバイスと一致するかを判断するために、ルールが評価される場合があります。一致式には複数の種類があります。たとえば、特定のデバイスタイプ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などにルールが一致する場合があります。

ルールリスト内のルールの追加、削除、再配置のどの時点でも、**キャンセル**ボタンをクリックすると、ルールリストは最初に開いたときの状態に戻ります。**保存**をクリックしない限り、このウィンドウで行われた変更は、構成ツールを閉じると失われます。

Endpoint Management connector for Exchange ActiveSyncには、ローカルルール、XenMobile Serverルール（XDMルールとも呼ばれます）、およびデフォルトアクセスルールの3種類のルールがあります。

ローカルルール: ローカルルールは最も高い優先順位を持ちます。デバイスがローカルルールに一致した場合、ルール評価は停止します。XenMobile Serverルールもデフォルトアクセスルールも参照されません。ローカルルールは、**構成 > アクセスルール > ローカルルール**タブを介して、Endpoint Management connector for Exchange ActiveSyncにローカルで構成されます。サポートの一致は、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いています。サポートの一致は、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デバイスタイプ
- ユーザープリンシパル名（UPN）
- ActiveSyncユーザーエージェント（通常はデバイスプラットフォームまたはメールクライアント）

メジャーな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、通常ルールまたは正規表現ルールのいずれかを追加できます。メジャーなスナップショットが完了していない場合は、正規表現ルールのみを追加できます。

XenMobileサーバールール: XenMobile Serverルールは、管理対象デバイスに関するルールを提供する外部XenMobile Serverへの参照です。XenMobile Serverは、デバイスがジェイルブレイクされているか、禁止されたアプリが含まれているかなど、XenMobileに既知のプロパティに基づいて許可またはブロックするデバイスを識別する独自の高レベルルールで構成できます。XenMobileは高レベルルールを評価し、許可またはブロックされたActiveSyncデバイスIDのセットを生成し、それらはEndpoint Management connector for Exchange ActiveSyncに配信されます。

デフォルトアクセスルール: デフォルトアクセスルールは、すべてのデバイスに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ユニークです。このルールはキャッチオールルールであり、特定のデバイスがローカルルールまたはXenMobile Serverルールに一致しない場合、デバイスの目的のアクセス状態はデフォルトアクセスルールの目的のアクセス状態によって決定されることを意味します。

- **デフォルトアクセス – 許可:** ローカルルールまたはXenMobile Serverルールのいずれにも一致しないデバイスはすべて許可されます。
- **デフォルトアクセス – ブロック:** ローカルルールまたはXenMobile Serverルールのいずれにも一致しないデバイスはすべてブロックされます。

- **デフォルトアクセス - 変更なし:** ローカルルールまたはXenMobile Serverルールのいずれにも一致しないデバイスは、Endpoint Management connector for Exchange ActiveSyncによってアクセス状態が変更されることはありません。デバイスがExchangeによって検疫モードに置かれている場合、アクションは実行されません。たとえば、検疫モードからデバイスを削除する唯一の方法は、明示的なローカルルールまたはXDMルールで検疫を上書きすることです。

ルール評価について

ExchangeがEndpoint Management connector for Exchange ActiveSyncに報告する各デバイスについて、ルールは優先度の高いものから低いものへと、次の順序で評価されます。

- ローカルルール
- XenMobile Serverルール
- デフォルトアクセスルール

一致が見つかると、評価は停止します。たとえば、ローカルルールが特定のデバイスに一致する場合、そのデバイスはXenMobile Serverルールやデフォルトアクセスルールのいずれに対しても評価されません。これは、特定のルールタイプ内でも同様です。たとえば、ローカルルールリスト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った時点で評価は停止します。

Endpoint Management connector for Exchange ActiveSyncは、デバイスのプロパティが変更された場合、デバイスが追加または削除された場合、あるいはルール自体が変更された場合に、現在定義されているルールセットを再評価します。メジャースナップショットは、構成可能な間隔でデバイスのプロパティの変更と削除を検出します。マイナースナップショットは、構成可能な間隔で新しいデバイスを検出します。

Exchange ActiveSyncにもアクセスを管理するルールがあります。これらのルールがEndpoint Management connector for Exchange ActiveSyncのコンテキスト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、個人免除、デバイスルール、組織設定の3つのレベルのルールで構成されている場合があります。Endpoint Management connector for Exchange ActiveSyncは、Remote PowerShellリクエストをプログラムで発行して個人免除リストに影響を与えることにより、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付けられた許可またはブロックされたExchange ActiveSyncデバイスIDのリストです。展開されると、Endpoint Management connector for Exchange ActiveSyncは、Exchange内の免除リスト機能の管理を効果的に引き継ぎます。詳細については、Microsoftの記事「Controlling Device Access」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ルールが定義されている状況で役立ちます。ルール間の関係をトラブルシューティングできます。ルール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デバイスタイプ、ユーザー、ユーザーエージェントなど、一致するフィールドに基づいてルールがグループで分析されます。

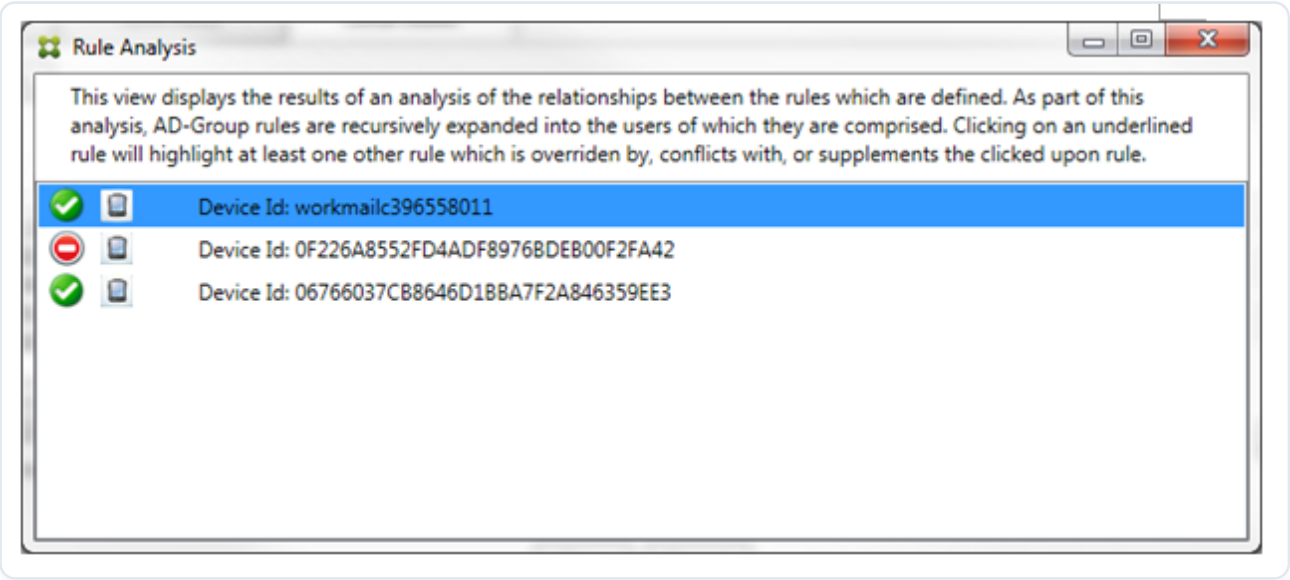
ルールの用語

- **上書きルール:** 1つのデバイスに複数のルールが適用できる場合に上書きが発生します。ルールはリスト内の優先度によって評価されるため、後から適用される可能性のあるルールインスタンスは評価されない場合があります。
- **競合ルール:** 1つのデバイスに複数のルールが適用される可能性があるが、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。競合するルールが正規表現ルールでない場合、競合は常に暗黙的に上書きを意味します。
- **補足ルール:** 複数のルールが正規表現ルールであり、2つ（またはそれ以上）の正規表現を単一の正規表現ルールに結合できるか、または機能が重複していないことを確認する必要がある場合に補足が発生します。補足ルールは、そのアクセス（許可/ブロック）において競合する可能性もあります。
- **プライマリルール:** プライマリルールは、ダイアログボックス内でクリックされたルールです。このルールは、周囲を囲む実線の境界線によって視覚的に示されます。また、上向きまたは下向きの緑色の矢印が1つまたは2つ表示されます。矢印が上を指している場合、それはプライマリルールの前に補助ルールがあることを示します。矢印が下を指している場合、これはプライマリルールの後に補助ルールがあることを示します。一度にアクティブにできるプライマリルールは1つだけです。
- **補助ルール:** 補助ルールは、上書き、競合、または補足関係を通じて、何らかの形でプライマリルールに関連しています。これらのルールは、周囲を囲む破線の境界線によって視覚的に示されます。各プライマリルールには、1つから多数の補助ルールが存在する可能性があります。下線付きのエントリをクリックすると、強調表示される補助ルールは常にプライマリルールの観点からのものです。たとえば、補助ルールはプライマリルールによって上書きされるか、および/または補助ルールはプライマリルールとのアクセスで競合するか、および/または補助ルールはプライマリルールを補足します。

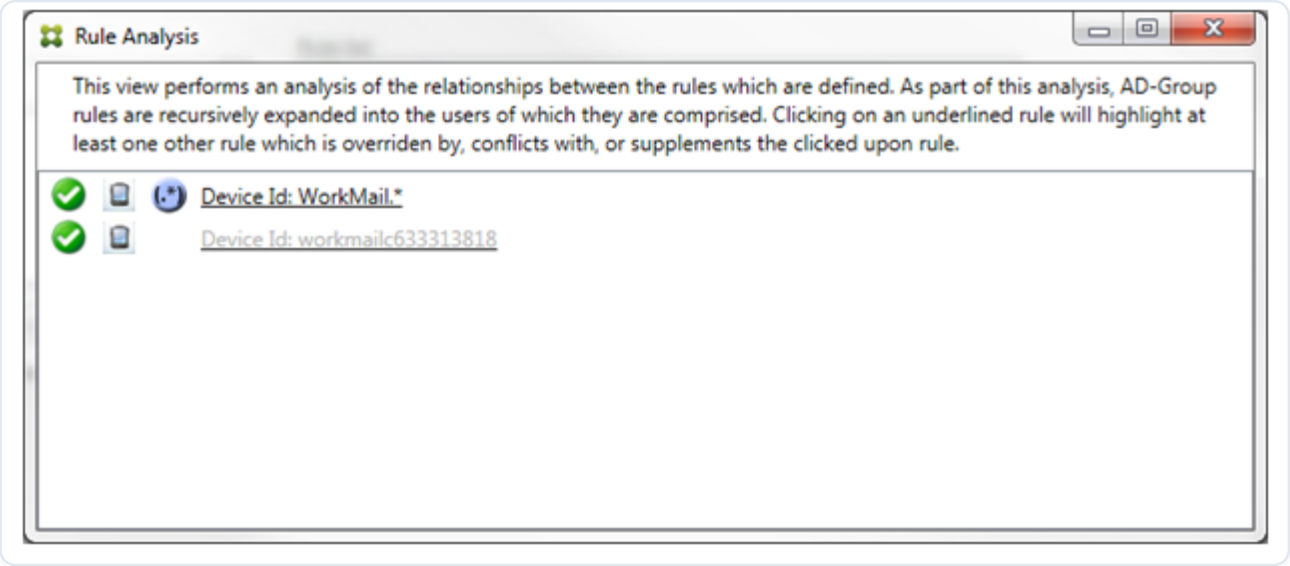
ルール分析ダイアログボックスでのルールの種類の表示方法

競合、オーバーライド、または補足がない場合、 ダイアログボックスには下線付きのエントリはありません。いずれかの項目をクリックしても影響はありません。たとえば、通常選択された項目の視覚効果が表示されます。

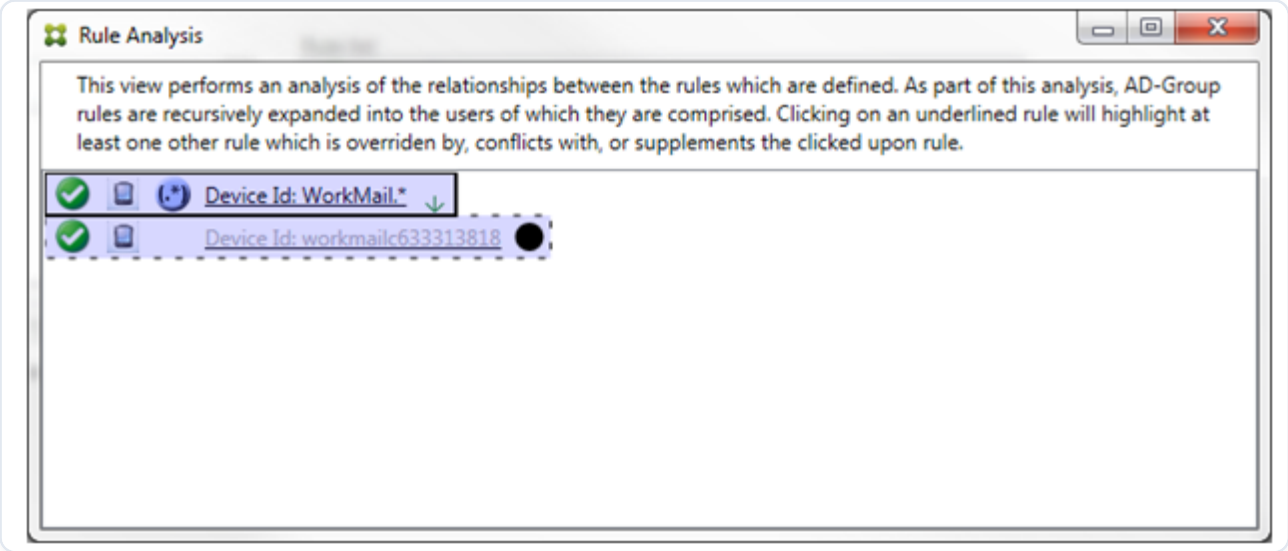
ウィンドウにはチェックボックスがあり、これを選択すると、競合、オーバーライド、冗長、または補足であるルールのみが表示されます。



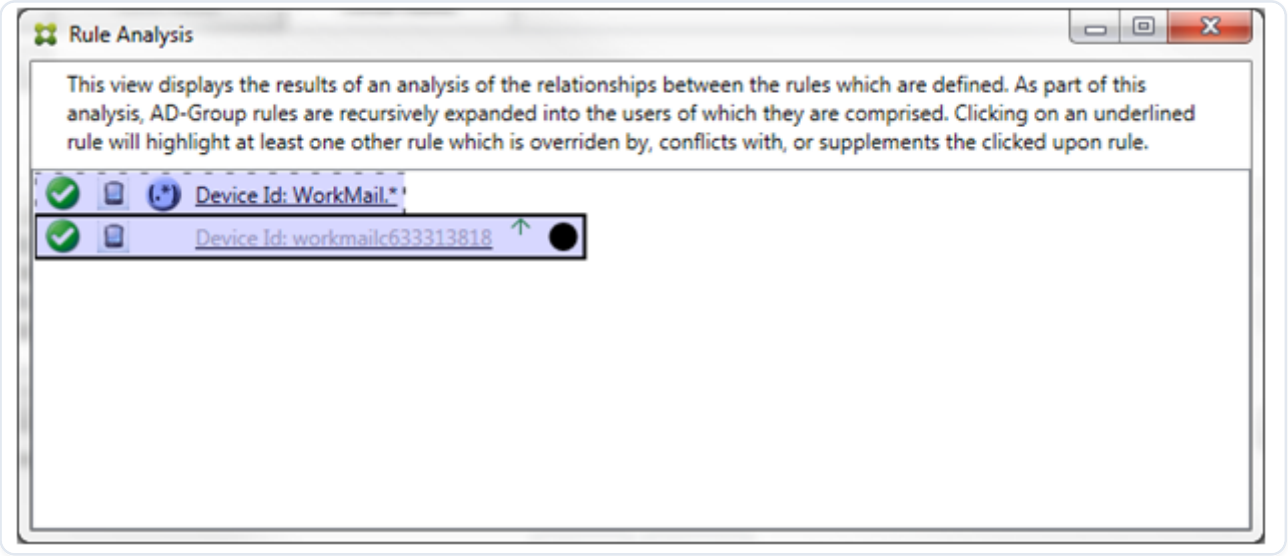
オーバーライドが発生すると、少なくとも2つのルール（プライマリルールと補助ルールまたは複数のルール）に下線が引かれます。少なくとも1つの補助ルールは、より薄いフォントで表示され、そのルールがより優先度の高いルールによってオーバーライドされていることを示します。オーバーライドされたルールをクリックすると、どのルールがそのルールをオーバーライドしたかを確認できます。オーバーライドされたルールが、プライマリルールまたは補助ルールであるために強調表示されている場合、その横に黒い丸が表示され、そのルールが非アクティブであることをさらに視覚的に示します。たとえば、ルールをクリックする前は、ダイアログボックスは次のように表示されます。



最も優先度の高いルールをクリックすると、ダイアログボックスは次のように表示されます。



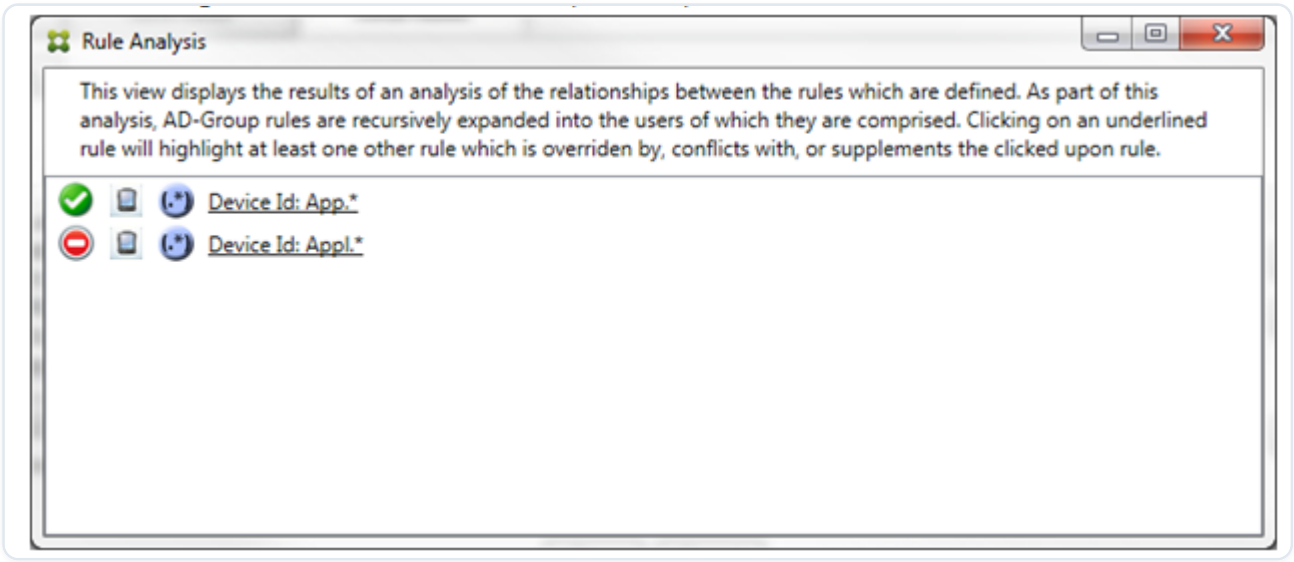
この例では、正規表現ルール `WorkMail.*` がプライマリルール（実線で示される）であり、通常のルール `workmailc633313818` が補助ルール（破線で示される）です。補助ルールの横にある黒い点は、そのルールが先行するより優先度の高い正規表現ルールによって非アクティブ（評価されることはない）であることをさらに示す視覚的な合図です。オーバーライドされたルールをクリックすると、ダイアログボックスは次のように表示されます。



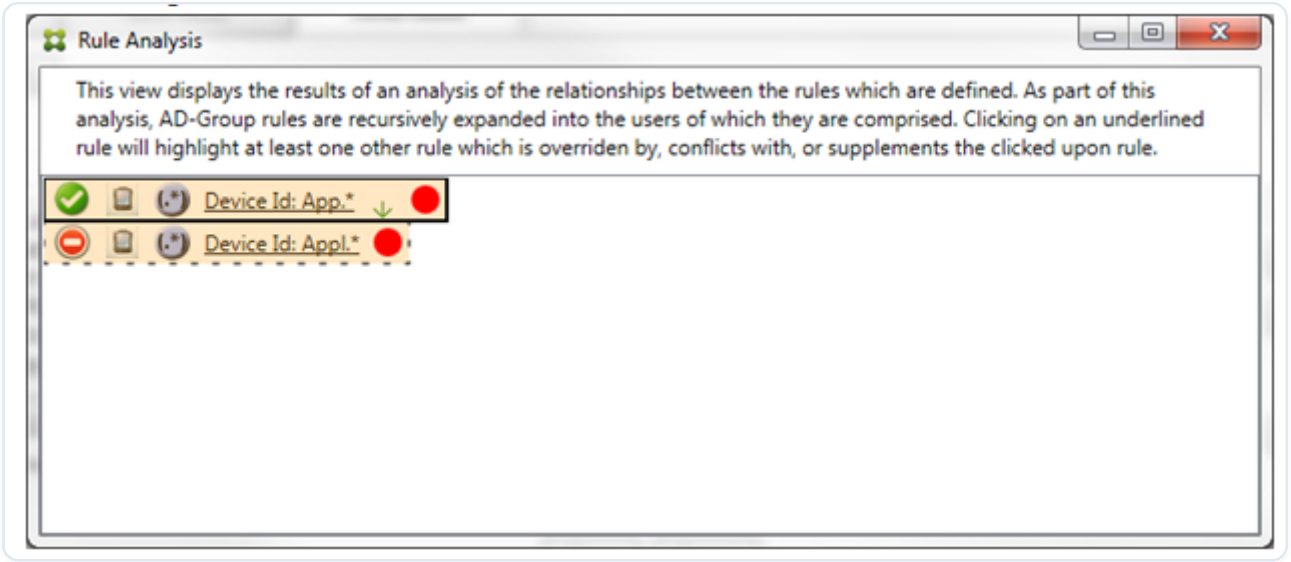
前の例では、正規表現ルール `WorkMail.*` が補助ルール（破線で示される）であり、通常のルール `workmailc633313818` がプライマリルール（実線で示される）です。この単純な例では、大きな違いはありません。より複雑な例については、このトピックの後半にある複雑な式の例を参照してください。多くのルールが定義されているシナリオでは、オーバーライドされたルールをクリックすることで、どのルールがそれをオーバーライドしたかを迅速に特定できます。

競合が発生すると、少なくとも2つのルール（プライマリルールと補助ルールまたは複数のルール）に下線が引かれます。競合しているルールは赤い点で示されます。互いにのみ競合するルールは、2つ以上の正規表現ルールが定義されている場合にのみ可能です。他のすべての競合シナリオ

では、競合だけでなく、オーバーライドも発生します。単純な例でいずれかのルールをクリックする前は、ダイアログボックスは次のように表示されます。



2つの正規表現ルールを検査すると、最初のルールが「App」を含むデバイスIDを持つすべてのデバイスを許可し、2番目のルールが「Appl」を含むデバイスIDを持つすべてのデバイスを拒否することが明らかです。さらに、2番目のルールが「Appl」を含むデバイスIDを持つすべてのデバイスを拒否するにもかかわらず、許可ルールの優先度が高いため、その条件に一致するデバイスが拒否されることはありません。最初のルールをクリックすると、ダイアログボックスは次のように表示されます。



前のシナリオでは、プライマリルール（正規表現ルール `App.*`）と補助ルール（正規表現ルール `Appl.*`）の両方が黄色で強調表示されています。これは、単一の一致可能なフィールドに複数の正規表現ルールを適用していることを警告する単なる視覚的な警告であり、冗長性の問題やより深刻な問題を示している可能性があります。

競合と上書きの両方があるシナリオでは、プライマリールール（正規表現ルール `App.*`）と補助ルール（正規表現ルール `Appl.*`）の両方が黄色で強調表示されます。これは、単一の一致可能なフィールドに複数の正規表現ルールを適用したという事実を警告するための視覚的な警告であり、冗長性の問題、またはより深刻な問題を示している可能性があります。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像 (/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules18.png)

前の例では、最初のルール（正規表現ルール `SAMSUNG.*`）が次のルール（通常のルール `SAMSUNG-SM-G900A/101.40402`）を上書きするだけでなく、2つのルールでアクセスが異なること（プライマリは許可、補助はブロックを指定）が容易にわかります。2番目のルール（通常のルール `SAMSUNG-SM-G900A/101.40402`）は、上書きされて非アクティブになっていることを示すために、薄いテキストで表示されます。

正規表現ルールをクリックすると、ダイアログボックスは次のように表示されます。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像 (/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules19.png)

プライマリールール（正規表現ルール `SAMSUNG.*`）には赤い点が付いており、そのアクセス状態が1つ以上の補助ルールと競合していることを示します。補助ルール（通常のルール `SAMSUNG-SM-G900A/101.40402`）には赤い点が付いており、そのアクセス状態がプライマリールールと競合していることを示します。そのルールには黒い点も付いており、上書きされて非アクティブになっていることを示します。

少なくとも2つのルール、つまりプライマリールールと補助ルールが下線で示されます。互いに補完し合うだけのルールには、正規表現ルールのみが関係します。ルールが互いに補完し合う場合、それらは黄色のオーバーレイで示されます。いずれかのルールをクリックする前の簡単な例では、ダイアログボックスは次のように表示されます。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像 (/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules20.png)

目視検査により、両方のルールが正規表現ルールであり、Endpoint Management connector for Exchange ActiveSync のActiveSyncデバイスIDフィールドに両方とも適用されていることが容易に明らかになります。最初のルールをクリックすると、ダイアログボックスは次のように表示されます。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像 (/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules21.png)

プライマリールール（正規表現ルール `WorkMail.*`）は、少なくともう1つの正規表現である補助ルールが存在することを示すために、黄色のオーバーレイで強調表示されます。補助ルール（正規表現ルール `SAMSUNG.*`）は、それとプライマリールールの両方が、Endpoint Management connector for Exchange ActiveSync 内の同じフィールドに適用されている正規表現ルールであることを示すために、黄色のオーバーレイで強調表示されます。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を判断するのはあなた次第です。

複雑な式の例

多くの潜在的な上書き、競合、または補足が発生する可能性があり、すべての可能なシナリオの例を示すことは不可能です。次の例では、すべきでないことについて説明するとともに、ルール分析の視覚的構成の全能力を示す役割も果たします。次の図では、ほとんどの項目に下線が引かれています。多くの項目が薄いフォントで表示されますが、これは、問題のルールが何らかの方法でより優先度の高いルールによって上書きされていることを示します。さまざまな正規表現ルールも、(.*) アイコンで示されているように、リストに含まれています。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像 (/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules22.png)

上書きを分析する方法

特定のルールを上書きしたルールを確認するには、そのルールをクリックします。

例1: この例では、`zentrain01@zenprise.com` が上書きされた理由を調べます。

Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules23.png)

プライマリルール（ADグループルール `zenprise/TRAINING/ZenTraining B`、`zentrain01@zenprise.com` はそのメンバー）には、次の特徴があります。

- 青色で強調表示され、実線で囲まれています。
- 上向きの緑色の矢印があります（補助ルールがすべてその上にあることを示します）。
- 赤い丸と黒い丸の両方が続き、それぞれ1つ以上の補助ルールがそのアクセスと競合していること、およびプライマリルールが上書きされて非アクティブになっていることを示します。

上にスクロールすると、次の内容が表示されます。

Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules24.png)

この場合、プライマリルールを上書きする2つの補助ルールがあります。正規表現ルール`zen.*`と通常ルール`zentrain01@zenprise.com`（`zenprise/TRAINING/ZenTraining A`の）です。後者の補助ルールの場合、Active Directoryグループルール`ZenTraining A`にユーザー`zentrain01@zenprise.com`が含まれており、Active Directoryグループルール`ZenTraining B`にもユーザー`zentrain01@zenprise.com`が含まれています。しかし、補助ルールはプライマリルールよりも優先順位が高いため、プライマリルールは上書きされています。プライマリルールのアクセスは「許可」ですが、両方の補助ルールのアクセスは「ブロック」であるため、すべて赤い丸が続き、アクセス競合がさらに示されます。

例2: この例では、ActiveSyncデバイスIDが`069026593E0C4AEAB8DE7DD589ACED33`のデバイスが上書きされた理由を示します。

Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules25.png)

プライマリルール（通常のデバイスIDルール`069026593E0C4AEAB8DE7DD589ACED33`）には、次の特徴があります。

- 青色で強調表示され、実線で囲まれています。
- 上向きの緑色の矢印があります（補助ルールがその上にあることを示します）。
- 補助ルールがプライマリルールを上書きし、その結果非アクティブになっていることを示す黒い丸がその後に続きます。

Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules26.png)

この場合、単一の補助ルールがプライマリルールを上書きします。正規表現のActiveSyncデバイスIDルールは`3E.*`です。正規表現`3E.*`が`069026593E0C4AEAB8DE7DD589ACED33`に一致するため、プライマリルールは評価されません。

補足と競合を分析する方法

この場合、プライマリルールは正規表現のActiveSyncデバイスタイプルール`touch.*`です。特徴は次のとおりです。

- 特定のルールフィールド（この場合はActiveSyncデバイスタイプ）に対して複数の正規表現ルールが動作していることを警告する、黄色のオーバーレイが付いた実線の境界線で示されます。
- それぞれ上向きと下向きの2つの矢印は、優先度の高い補助ルールが少なくとも1つと、優先度の低い補助ルールが少なくとも1つ存在することを示しています。

- その隣の赤い丸は、少なくとも1つの補助ルールがアクセスを「許可」に設定しており、それがプライマリルールの「ブロック」アクセスと競合していることを示しています。
- 2つの補助ルールがあります。正規表現のActiveSyncデバイスタイプルール`SAM.*`と、正規表現のActiveSyncデバイスタイプルール`Andro.*`です。
- 両方の補助ルールは、補助であることを示すために破線で囲まれています。
- 両方の補助ルールは、ActiveSyncデバイスタイプのルールフィールドにも適用されることを示すために、黄色でオーバーレイされています。
- このようなシナリオでは、正規表現ルールが冗長でないことを確認する必要があります。

  Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules27.png)

ルールをさらに分析する方法

この例では、ルール間の関係が常にプライマリルールの視点からどのように見られるかを探ります。前の例では、値が`touch.*`のデバイスタイプのルールフィールドに適用される正規表現ルールをクリックする方法を示しました。補助ルール`Andro.*`をクリックすると、異なる一連の補助ルールが強調表示されます。

「Endpoint Management connector for Exchange ActiveSync コンソールページ」の画像(/en-us/xenmobile/server/media/xenmobilemailmanager-accessrules28.png)

この例は、ルール関係に含まれる上書きされたルールを示しています。このルールは、通常のActiveSyncデバイスタイプルール`Android`であり、上書きされており（薄くなったフォントと隣の黒い丸で示されています）、プライマリルールの正規表現ActiveSyncデバイスタイプルール`Andro.*`とのアクセスで競合もしています。このルールは、クリックされる前は補助ルールでした。前の例では、通常のActiveSyncデバイスタイプルール`Android`は、その時点でのプライマリルール（正規表現ActiveSyncデバイスタイプルール`touch.*`）の観点から、関連性がなかったため、補助ルールとして表示されませんでした。

通常の式ローカルルールを構成するには

1. 「**アクセスルール**」タブをクリックします。

   「Endpoint Management connector for Exchange ActiveSync コンソールページ」の画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)
2. 「**デバイスID**」リストで、ローカルルール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の一意の一致をすべて表示します。この例では、「**デバイスの種類**」フィールドが選択されており、選択肢は以下のリストボックスに表示されています。

   「Endpoint Management connector for Exchange ActiveSync コンソールページ」の画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-localrules-unique.png)

4. 結果リストボックスの項目を1つクリックし、次のいずれかのオプションをクリックします。

   - **許可**は、一致するすべてのデバイスに対してActiveSyncトラフィックを許可するようにExchangeが構成されることを意味します。
   - **拒否**は、一致するすべてのデバイスに対してActiveSyncトラフィックを拒否するようにExchangeが構成されることを意味します。

   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がアクセスを拒否されます。

   「Endpoint Management connector for Exchange ActiveSync コンソールページ」の画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-deny-samsung.png)

正規表現を追加するには

正規表現ローカルルールは、その横に表示されるアイコン - アイコンの画像(/en-us/xenmobile/server/media/xenmobilemailmanager-regexpression-icon.png) - で区別できます。

正規表現ルールを追加するには、特定のフィールドの結果リストから既存の値を使用して正規表現ルールを作成するか（主要なスナップショットが完了している限り）、または単に目的の正規表現を入力することができます。

既存のフィールド値から正規表現を作成するには

1. **アクセスルール**タブをクリックします。

   Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)

2. **デバイスID**リストで、正規表現ローカルルールを作成したい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の一意の一致をすべて表示します。この例では、**デバイスタイプ**フィールドが選択されており、選択肢は以下のリストボックスに表示されています。

   Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-magnifier.png)

4. 結果リストのいずれかの項目をクリックします。この例では、**SAMSUNGSPHL720**が選択され、**デバイスタイプ**の横のテキストボックスに表示されています。

   Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-localrules-samsung-regex.png)

5. デバイスタイプ値に「Samsung」を含むすべてのデバイスタイプを許可するには、以下の手順に従って正規表現ルールを追加します。

   a. 選択した項目テキストボックス内をクリックします。
   b. テキストを**SAMSUNGSPHL720**から**SAMSUNG.***に変更します。
   c. 正規表現チェックボックスが選択されていることを確認します。
   d. **許可**をクリックします。

   Endpoint Management connector for Exchange ActiveSync コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-allow-samsung.png)

アクセスルールを作成するには

1. タブをクリックします。
2. 正規表現を入力するには、デバイスIDリストと選択した項目テキストボックスの両方を使用する必要があります。

   Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-local-rule.png)

3. 照合するフィールドを選択します。この例では、デバイスの種類を使用します。
4. 正規表現を入力します。この例では、`samsung.*`を使用します。
5. 正規表現チェックボックスが選択されていることを確認し、 または をクリックします。この例では、 を選択します。最終結果は次のとおりです。

   Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-samsung-asterisk.png)

デバイスを検索するには

正規表現チェックボックスを選択すると、指定された表現に一致する特定のデバイスを検索できます。この機能は、メジャースナップショットが正常に完了した場合にのみ利用できます。正規表現ルールを使用する予定がない場合でも、この機能を使用できます。たとえば、ActiveSyncデバイ

スIDに「workmail」というテキストが含まれるすべてのデバイスを検索したいとします。これを行うには、次の手順に従います。

1. タブをクリックします。
2. デバイス一致フィールドセレクターがデバイスID（デフォルト）に設定されていることを確認します。

   Endpoint Management connector for Exchange ActiveSyncコンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-tab.png)
3. 選択した項目テキストボックス内（前の図で青色で示されている部分）をクリックし、`workmail.*` と入力します。
4. 正規表現チェックボックスが選択されていることを確認し、虫眼鏡アイコンをクリックして、次の図に示すように一致するものを表示します。

   「Endpoint Management connector for Exchange ActiveSync」コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-accessrules-localrules-regex.png)

個々のユーザー、デバイス、またはデバイスタイプを静的ルールに追加するには

ActiveSync Devicesタブで、ユーザー、デバイスID、またはデバイスタイプに基づいて静的ルールを追加できます。

1. **ActiveSync Devices**タブをクリックします。
2. リストで、ユーザー、デバイス、またはデバイスタイプを右クリックし、選択を許可するか拒否するかを選択します。

   次の画像は、user1が選択されたときの許可/拒否オプションを示しています。

   「Endpoint Management connector for Exchange ActiveSync」コンソールページの画像(/en-us/xenmobile/server/media/connector-exchangeactivesync-devices-allowdeny.png)

デバイス監視

Endpoint Management connector for Exchange ActiveSyncの**Monitor**タブでは、検出されたExchange ActiveSyncおよびBlackBerryデバイスと、発行された自動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 デバイス**:

- **Export**ボタンをクリックして、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、適切な許可またはブロックルールタイプを選択することで、ローカル（静的）ルールを追加できます。
- 展開された行を折りたたむには、展開された行をCtrlキーを押しながらクリックします。

- **Blackberry デバイス**
- **自動化履歴**

「**構成**」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。スナップショット履歴には、スナップショットがいつ実行されたか、かかった時間、検出されたデバイスの数、および発生した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**タブの下で、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と診断

Exchange ActiveSync用Endpoint Managementコネクタは、エラーやその他の運用情報をログファイル（*インストールフォルダー*\log\XmmWindowsService.log）に記録します。Exchange ActiveSync用Endpoint Managementコネクタは、重要なイベントもWindowsイベントログに記録します。

ログレベルを変更するには

Exchange ActiveSync用Endpoint Managementコネクタには、次のログレベルが含まれています：Error、Info、Warn、Debug、Trace。

> **注：**

> 各レベルは、次のレベルに進むにつれてより詳細な情報（より多くのデータ）を生成します。たとえば、Errorレベルは最も詳細度が低く、Traceレベルは最も詳細度が高くなります。

> 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で、nlog.configファイルを開きます。

2. `<rules>`セクションで、*minilevel*パラメーターを希望のログレベルに変更します。例：

```
    <rules>



    <logger name="*" writeTo="file" minlevel="Debug" />



    </rules>
```

3. ファイルを保存します。

   変更はすぐに有効になります。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

以下に一般的なエラーを示します。

- Endpoint Management connector for Exchange ActiveSyncサービスが起動しない

  ログファイルとWindowsイベントログでエラーを確認してください。一般的な原因は次のとおりです。

  - Exchange ActiveSyncサービス用Endpoint ManagementコネクタがSQL Serverにアクセスできません。これは以下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ません。
    - 認証の失敗。

    Windows統合認証が構成されている場合、Exchange ActiveSyncサービス用Endpoint Managementコネクタのユーザーアカウントは、許可されたSQLログオンである必要があります。Exchange ActiveSyncサービス用Endpoint Managementコネクタのアカウントは、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ログオンはSQLで適切に構成されている必要があります。
  - モバイルサービスプロバイダー（MSP）用に構成されたポートが利用できません。システム上の他のプロセスで使用されていないリスニングポートを選択する必要があります。

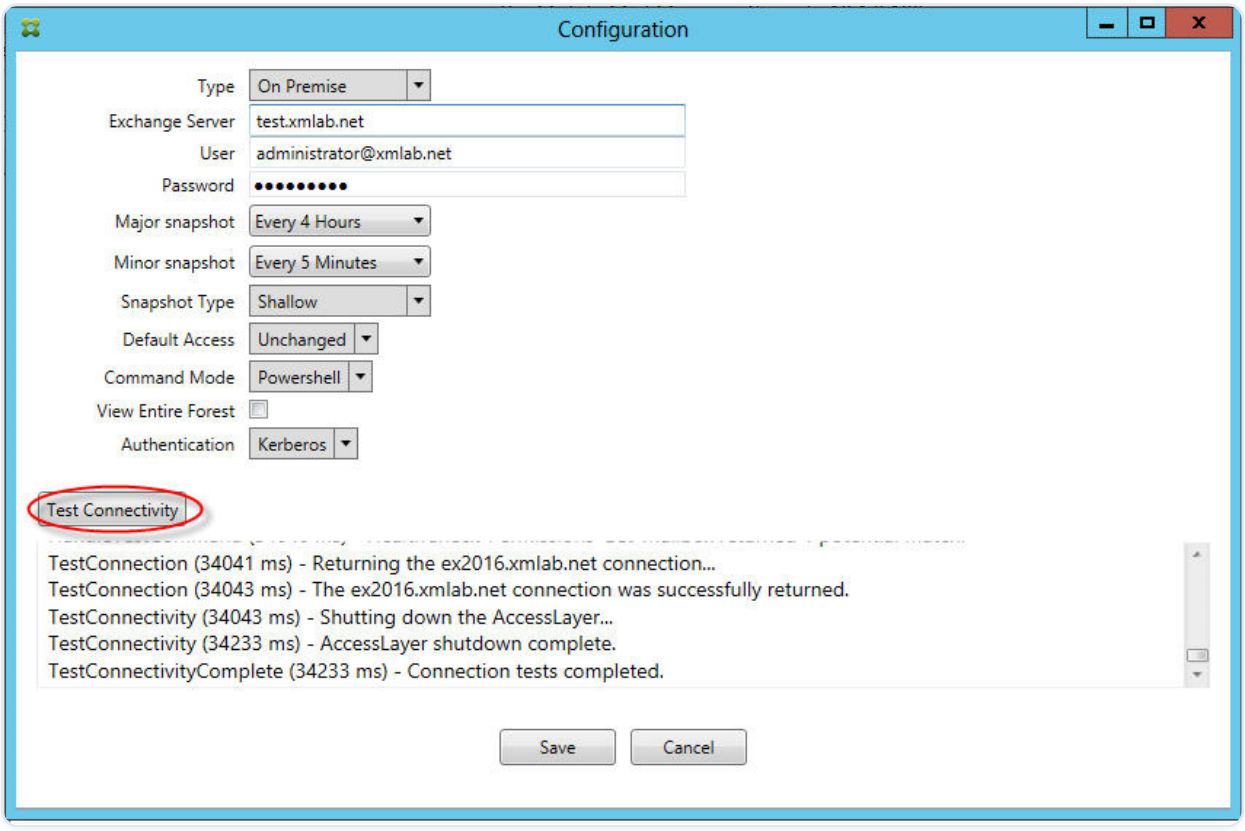
- XenMobileがMSPに接続できません

Endpoint Management connector for Exchange ActiveSync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てください。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てください。

HTTPSが構成されている場合、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、IISマネージャーを使用して証明書をインストールできます。IISがインストールされていない場合は、証明書のインストール方法の詳細について「SSL証明書を使用してポートを構成する方法」を参照してください。

Endpoint Management connector for Exchange ActiveSync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、URLと資格情報をXenMobileで構成されているURLと資格情報に設定し、**Test Connectivity**をクリックします。これにより、XenMobile Serverが発行するWebサービスリクエストがシミュレートされます。HTTPSが構成されている場合、サーバーの実際のホスト名（SSL証明書で指定されている名前）を指定する必要があります。

Test Connectivityを使用する際は、少なくとも1つのActiveSyncDeviceレコードがあることを確認してください。そうし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

トラブルシューティング用のPowerShellユーティリティのセットは、**Support\PowerShell**フォルダーにあります。

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とデバイスの詳細な分析を実行し、エラー状態や潜在的な障害領域を検出し、ユーザーの詳細なRBAC分析を行います。すべてのコマンドレットの生出力をテキストファイルに保存できます。

エクスチェンジ アクティブシンク 用 シトリックス ゲートウェイ コネクタ™

XenMobile Citrix ADC Connector は、Exchange ActiveSync 用 Citrix Gateway connector になりました。Citrix の統合ポートフォリオの詳細については、Citrix 製品ガイドを参照してください。

Exchange ActiveSync 用コネクタは、Exchange ActiveSync プロトコルのリバースプロキシとして機能する Citrix ADC に対し、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® 内で定義するポリシーと、Exchange ActiveSync 用 Citrix Gateway connector によってローカルで定義されるルールの組み合わせによって制御されます。

詳細については、ActiveSync Gateway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 Citrix Gateway connector の現在のリリースはバージョン 8.5.2 です。

> **重要:**

> 2022 年 10 月以降、Endpoint Management および Exchange ActiveSync 用 Citrix Gateway connector は、Microsoft がこちらで発表した認証変更のため、Exchange Online をサポートしなくなりました。Exchange 用 Endpoint Management connector は、Microsoft Exchange Server (オンプレミス) で引き続き動作します。

新機能

以下のセクションでは、以前は XenMobile Citrix ADC Connector と呼ばれていた Exchange ActiveSync 用 Citrix Gateway connector の現在および以前のバージョンの新機能について説明します。

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ました。

- Google Analytics に送信される分析情報に、特にスナップショットに関する詳細が追加されました。

バージョン 8.5.2 の新機能

- XenMobile Citrix ADC Connector は、Exchange ActiveSync 用 Citrix Gateway connector になりました。

このリリースでは、以下の問題が修正されています。

- ポリシールールの定義で複数の条件が使用され、その条件の1つにユーザーIDが含まれる場合、次の問題が発生する可能性があります。ユーザーが複数のエイリアスを持っている場合、ルール適用時にエイリアスもチェックされません。

> **注：**
>
> 以下の「新機能」セクションでは、Exchange ActiveSync 用 Citrix Gateway コネクタを、以前の名称である XenMobile Citrix ADC Connector で参照しています。名称はバージョン 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 Citrix ADC Connector には、Microsoft .NET Framework 4.5 が必要です。
- **Google Analytics のサポート：** XenMobile Citrix ADC Connector の使用状況を把握し、製品を改善できる点に注力したいと考えています。
- **TLS 1.1 および 1.2 のサポート：** セキュリティの脆弱化のため、TLS 1.0 は PCI Council によって非推奨とされています。XenMobile Citrix ADC Connector に TLS 1.1 および 1.2 のサポートが追加されました。

Exchange ActiveSync 用 Citrix Gateway コネクタの監視

Exchange ActiveSync 用 Citrix Gateway コネクタの構成ユーティリティは、Secure Mobile Gateway によって許可またはブロックされた、Exchange Server を通過する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を提供します。

ログタブを使用して、Citrix ADC によって認証のために Exchange ActiveSync 用コネクタに転送された ActiveSync リクエストの履歴を表示します。

また、Exchange ActiveSync Web サービス用 Citrix Gateway コネクタ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に次の URL を読み込みます `https://<host:port>/services/ActiveSync/Version`。URL が製品バージョンを文字列として返した場合、Web サービスは応答しています。

Exchange ActiveSync 用 Citrix Gateway コネクタで ActiveSync トラフィックをシミュレートするには

Exchange ActiveSync 用 Citrix Gateway コネクタを使用して、ポリシーが適用された場合の ActiveSync トラフィックがどのように見えるかをシミュレートできます。コネクタ構成ユーティリティで、**シミュレーター**タブを選択します。結果には、構成したルールに従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。

Exchange ActiveSync 用 Citrix Gateway コネクタのフィルターの選択

Citrix Gateway connector for Exchange ActiveSync フィルターは、特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分析することで機能します。デバイスが基準を満たしている場合、そのデバイスはデバイスリストに配置されます。このデバイスリストは、許可リストでもブロックリストでもありません。これは、定義された基準を満たすデバイスのリストです。XenMobile 内のコネクタで利用できるフィルターは次のとおりです。各フィルターの2つのオプションは、**許可**または**拒否**です。

- **匿名デバイス:** XenMobile に登録されているが、ユーザーのIDが不明なデバイスを許可または拒否します。たとえば、登録済みだがActive Directoryパスワードの有効期限が切れているユーザー、または不明な資格情報で登録したユーザーなどが該当します。
- **Samsung KNOX 認証の失敗:** Samsung デバイスには、セキュリティおよび診断機能があります。このフィルターは、デバイスが KNOX 用に設定されていることを確認します。詳細については、「Samsung Knox」を参照してください。
- **禁止アプリ:** ブロックリストポリシーによって定義されたデバイスリストと、ブロックされたアプリの存在に基づいてデバイスを許可または拒否します。
- **Implicit Allow/Deny:** Creates a Device List of all devices that do not meet any of the other filter rule criteria and allows or denies based on that list. The Implicit Allow/Deny option ensures that the Citrix Gateway connector for Exchange ActiveSync status in the Devices tab is enabled and shows the connector status for your devices. The Implicit Allow/Deny option also controls all of the other connector filters that have not been selected. For example, the connector denies blocked apps yet allows all other filters because the Implicit Allow/Deny option is set to **Allow**.

- **非アクティブなデバイス:** 指定された時間内に XenMobile と通信していないデバイスのデバイスリストを作成します。これらのデバイスは非アクティブと見なされます。フィルターは、それに応じてデバイスを許可または拒否します。
- **必須アプリの不足:** ユーザーが登録すると、インストールする必要がある必須アプリのリストを受け取ります。必須アプリの不足フィルターは、1つ以上のアプリが存在しなくなったことを示します。たとえば、ユーザーが1つ以上のアプリを削除した場合などです。
- **推奨されないアプリ:** ユーザーが登録すると、インストールする必要があるアプリのリストを受け取ります。推奨されないアプリフィルターは、そのリストにないアプリをデバイスでチェックします。
- **非準拠パスワード:** デバイスにパスコードが設定されていないすべてのデバイスのデバイスリストを作成します。
- **コンプライアンス違反デバイス:** 独自の社内ITコンプライアンス基準を満たすデバイスを拒否または許可できます。コンプライアンスは、デバイスプロパティ「Out of Compliance」によって定義される任意のオプションであり、**True**または**False**のいずれかになるブール値フラグです。(このプロパティを手動で作成して値を設定することも、デバイスが特定の基準を満たすかどうかに応じて、自動アクションを使用してデバイス上にこのプロパティを作成することもできます。)
  - **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を満たしていない場合、そのデバイスはコンプライアンス違反です。
  - **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を満たしている場合、そのデバイスは準拠しています。
- **失効ステータス:** すべての失効済みデバイスのデバイスリストを作成し、失効ステータスに基づいて許可または拒否します。
- **Root化されたAndroid/ジェイルブレイクされたiOSデバイス**。Root化済みとしてフラグ付けされたすべてのデバイスのデバイスリストを作成し、Root化ステータスに基づいて許可または拒否します。
- **管理対象外デバイス**。XenMobile データベース内のすべてのデバイスのデバイスリストを作成します。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 connector for Exchange ActiveSync への接続を構成するには

Citrix Gateway connector for Exchange ActiveSync は、セキュアなWebサービスを介してXenMobileおよびその他のリモート構成プロバイダーと通信します。

1. コネクタ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、管理者権限を持ち、XenMobile Server との基本的なHTTP認証に使用されるユーザー名を入力します。
3. **Url** に、XenMobile GCS のWebアドレスを入力します。通常、形式は `https://<FQDN>/<instanceName>/services/<MagConfigService>` です。*MagConfigService* の名前は大文字と小文字を区別します。
4. **Password** に、XenMobile Server との基本的なHTTP認証に使用されるパスワードを入力します。
5. **Managing Host** に、コネクタサーバー名を入力します。
6. **Baseline Interval** に、Device Manager から新しい更新された動的ルールセットがプルされる期間を指定します。
7. **Delta interval** に、動的ルールの更新がプルされる期間を指定します。
8. **Request Timeout** に、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、構成プロバイダーサーバーインスタンスが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がXenMobileに通知するようにする場合は、このオプションを有効にします。XenMobileの自動アクションでコネクタルールを使用している場合、このオプションは必須です。
11. **Save** をクリックし、次に **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は、ローカルファイアウォール設定が接続を許可していることを確認するか、管理者に連絡してください。
12. 接続が成功したら、**Disabled** チェックボックスをオフにして、**Save** をクリックします。

新しい構成プロバイダーを追加すると、Citrix Gateway connector for Exchange ActiveSync は、そのプロバイダーに関連付けられた1つ以上のポリシーを自動的に作成します。これらのポリシーは、NewPolicyTemplate セクションの `config\policyTemplates.xml` に含まれ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ている各 Policy 要素に対して、新しいポリシーが作成されます。

以下の条件が満たされている場合、オペレーターは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準拠しており、標準の置換文字列（中括弧で囲まれている）が変更されていないこと。次に、プロバイダーの新しいグループを追加し、新しいグループを含めるようにポリシーを更新します。

XenMobileからポリシーをインポートするには

1. Exchange ActiveSync構成ユーティリティ用のCitrix Gatewayコネクタで、 タブをクリックし、をクリックします。
2. ダイアログボックスの に、XenMobile Serverとの基本的なHTTP認証に使用され、管理者権限を持つユーザー名を入力します。
3. に、XenMobile Gateway Configuration Service (GCS) のWebアドレスを入力します。通常、形式は `https://<xdmHost>/xdm/services/<MagConfigService>` です。MagConfigService名は、大文字と小文字が区別されます。
4. に、XenMobile Serverとの基本的なHTTP認証に使用されるパスワードを入力します。
5. をクリックして、ゲートウェイと構成プロバイダー間の接続をテストします。接続に失敗した場合は、ローカルファイアウォール設定で接続が許可されているかを確認するか、管理者に確認してください。
6. 接続が正常に確立されたら、 チェックボックスをオフにして、 をクリックします。
7. では、ローカルホストコンピューターのデフォルトのDNS名をそのまま使用します。この設定は、複数のForefront Threat Management Gateway (TMG) サーバーがアレイで構成されている場合に、XenMobileとの通信を調整するために使用されます。

   設定を保存した後、GCSを開きます。

Exchange ActiveSyncポリシーモード用のCitrix Gatewayコネクタの構成

Exchange ActiveSync用のCitrix Gatewayコネクタは、次の6つのモードで実行できます。

- 。このポリシーモードは、コネクタを通過するすべてのトラフィックにアクセスを許可します。他のフィルタリングルールは使用されません。
- 。このポリシーモードは、コネクタを通過するすべてのトラフィックのアクセスをブロックします。他のフィルタリングルールは使用されません。
- 。このポリシーモードは、最後に暗黙的な拒否またはブロックステートメントを持つ静的ルールを実行します。コネクタは、他のフィルタールールによって許可または許可されていないデバイスをブロックします。
- **静的ルール: 許可モード**。このポリシーモードは、最後に暗黙的な許可または許可ステートメントを持つ静的ルールを実行します。他のフィルタールールによってブロックまたは拒否されていないデバイスは、コネクタを通過することが許可されます。

- **静的 + ZDM ルール**: ブロックモード。このポリシーモードは、最初に静的ルールを実行し、次に XenMobile からの動的ルールを実行し、最後に暗黙的な拒否またはブロックステートメントを持ちます。デバイスは、定義されたフィルターとデバイスマネージャールールに基づいて許可または拒否されます。定義されたフィルターとルールに一致しないデバイスはすべてブロックされます。
- **静的 + ZDM ルール**: 許可モード。このポリシーモードは、最初に静的ルールを実行し、次に XenMobile からの動的ルールを実行し、最後に暗黙的な許可または許可ステートメントを持ちます。デバイスは、定義されたフィルターとXenMobileルールに基づいて許可または拒否されます。定義されたフィルターとルールに一致しないデバイスはすべて許可されます。

Exchange ActiveSync 用 Citrix Gateway コネクタは、XenMobile から受信した iOS および Windows ベースのモバイルデバイスの一意の ActiveSync ID に基づいて、動的ルールの許可またはブロックを処理します。Android デバイスは製造元によって動作が異なり、一意の ActiveSync ID を容易に公開しないものもあります。これを補うため、XenMobile は Android デバイスのユーザー ID 情報を送信して、許可またはブロックの決定を行います。その結果、ユーザーが Android デバイスを 1 台しか持っていない場合、許可とブロックは正常に機能します。ユーザーが複数の Android デバイスを持っている場合、Android デバイスは区別できないため、すべてのデバイスが許可されます。既知の場合、ActiveSyncID によってこれらのデバイスを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、デバイスタイプ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、次の操作を行います。

1. **パスフィルター**タブをクリックし、次に**追加**をクリックします。
2. **パスプロパティ**ダイアログボックスで、**ポリシー**リストからポリシーモードを選択し、**保存**をクリックします。

構成ユーティリティの**ポリシー**タブでルールを確認できます。ルールは、Exchange ActiveSync 用 Citrix Gateway コネクタで上から下へ処理されます。許可ポリシーは緑色のチェックマークで表示されます。拒否ポリシーは、線が引かれた赤い丸で表示されます。画面を更新して最新のルールを表示するには、**更新**をクリックします。config.xml ファイルでルールの順序を変更することもできます。

ルールをテストするには、**シミュレーター**タブをクリックします。フィールドに値を指定します。これらはログからも取得できます。許可またはブロックを指定する結果メッセージが表示されます。

静的ルールを構成するには

ActiveSync 接続 HTTP リクエストの ISAPI フィルタリングが読み取る値を持つ静的ルールを入力します。静的ルールにより、Exchange ActiveSync 用 Citrix Gateway コネクタは、次の基準でトラフィックを許可またはブロックできます。

- **ユーザー:** Exchange ActiveSync 用 Citrix Gateway コネクタは、デバイス登録中に取得された認証済みユーザーの値と名前構造を使用します。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 として見つかります。コネクタ構成ユーティリティ内の**ログ**タブには、コネクタを介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、または異なる場合に値が渡されます。
- **デバイス ID (ActiveSyncID):** 接続されているデバイスの 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にあります。この値は、コネクタ構成ユーティリティのログタブから確認することもできます。
- **デバイスタイプ:** コネクタは、デバイスが iPhone、iPad、またはその他のデバイスタイプであるかどうかを判断し、その基準に基づいて許可またはブロックできます。他の値と同様に、コネクタ構成ユーティリティは、ActiveSync 接続で処理されているすべての接続済みデバイスタイプを明らかにできます。
- **ユーザーエージェント:** 使用されている ActiveSync クライアントに関する情報が含まれています。通常、指定された値は、モバイルデバイスプラットフォームの特定のオペレーティングシステムビルドとバージョンに対応します。

サーバー上で実行されているコネクタ構成ユーティリティは、常に静的ルールを管理します。

1. SMGコントローラー構成ユーティリティで、**［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（AllowedUserなど）を入力してアクセスを許可するユーザーを入力し、［Disabled］**チェックボックスをオフにすることができます。
3. **［Save］**をクリックします。

   静的ルールが有効になりました。また、正規表現を使用して値を定義することもできますが、その場合はconfig.xmlファイルでルール処理モードを有効にする必要があります。

動的ルールを構成するには

XenMobileのデバイスポリシーとプロパティは、動的ルールを定義し、Exchange ActiveSyncフィルター用の動的Citrix Gatewayコネクタ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。コネクタフィルターは、特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分析することで機能します。デバイスが基準を満たしている場合、そのデバイスはデバイスリストに配置されます。このデバイスリストは、許可リストでもブロックリストでもありません。定義された基準を満たすデバイスのリストです。以下の構成オプションを使用すると、コネクタを使用してデバイスリスト内のデバイスを許可するか拒否するかを定義できます。

> **注：**
>
> 動的ルールを構成するには、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、右上隅にある歯車アイコンをクリックします。**［Settings］**ページが表示されます。
2. **［Server］の下で、［ActiveSync Gateway］**をクリックします。ActiveSync Gatewayページが表示されます。
3. **［Activate the following rules］**で、アクティブ化するルールを1つ以上選択します。
4. Androidのみの場合、**［Send Android domain users to ActiveSync Gateway］で［YES］**をクリックして、XenMobileがAndroidデバイス情報をSecure Mobile Gatewayに送信するようにします。

   このオプションが有効になっている場合、XenMobileがAndroidデバイスユーザーのActiveSync識別子を持っていないときに、XenMobileはAndroidデバイス情報をExchange ActiveSync用Citrix Gatewayコネクタに送信します。

Exchange ActiveSync XMLファイル用のCitrix Gatewayコネクタを編集してカスタムポリシーを構成するには

Citrix Gateway connector for Exchange ActiveSync 設定ユーティリティの「**Policies**」タブで、デフォルト構成の基本ポリシーを表示できます。カスタムポリシーを作成する場合は、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** セクションを見つけ、新しい **Policy** 要素を追加します。
2. 新しいグループ（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）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で、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 connector for Exchange ActiveSync XMLファイルの構成

Citrix Gateway connector for Exchange ActiveSync は、コネクタの動作を指示するためにXML構成ファイルを使用します。このファイルには、他のエントリの中でも、HTTPリクエストを評価する際にフィルターが実行するグループファイルと関連アクションが指定されています。デフォルトでは、ファイル名はconfig.xmlで、次の場所にあります: ..\Program Files\Citrix\XenMobile Citrix ADC Connector\config\.

GroupRefノード

GroupRefノードは論理グループ名を定義します。デフォルトは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値は、特定のユーザーアカウントまたはデバイスを照合するために使用される論理コンテナまたはメンバーのコレクションを識別します。アクション属性は、コレクション内のルールに一致するメンバーをフィルターがどのように処理するかを指定します。たとえば、AllowGroupセット内のルールに一致するユーザーアカウントまたはデバイスは「通過」します。「通過」とは、Exchange CASへのアクセスが許可されることを意味します。DenyGroupセット内のルール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」とは、Exchange CASへのアクセスが許可されないことを意味します。

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ルールに合致する場合、リクエストの結果を指示するために優先順位の規則が使用されます。優先順位は、config.xmlファイル内のGroupRefノードの順序（上から下へ）によって具現化されます。GroupRefノードは優先順位順にランク付けされます。Allowグループ内の特定の条件に対するルールは、常にDenyグループ内の同じ条件に対するルールよりも優先されます。

グループノード

さらに、config.xmlはGroupノードを定義します。これらのノードは、論理コンテナであるAllowGroupとDenyGroupを外部XMLファイルにリンクします。外部ファイルに保存されたエントリは、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allow.xmlとdeny.xmlの2つのXMLファイルが実装されます。

Exchange ActiveSync用Citrix Gatewayコネクタの構成

Exchange ActiveSync用Citrix Gatewayコネクタを構成して、次の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できます。**Active Sync Service ID**、**デバイスの種類**、**ユーザーエージェント** (デバイスのオペレーティングシステム)、**承認済みユーザー**、および**ActiveSyncコマンド**。

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ます。静的グループは、SMG Controller Configurationユーティリティを使用して管理します。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、既知のデバイスカテゴリで構成される場合があります。

Gateway Configuration Providerと呼ばれる外部ソースが動的グループを維持します。Exchange ActiveSync用Citrix Gatewayコネクタは、定期的にグループを接続します。XenMobileは、許可されたデバイスとブロックされたデバイスおよび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、Gateway Configuration Providerと呼ばれる外部ソースによって維持され、Exchange ActiveSync用Citrix Gatewayコネクタによって定期的に収集されます。XenMobileは、許可されたデバイスとブロックされたデバイスおよび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。

ポリシーは、各グループに関連付けられたアクション（許可またはブロック）とグループメンバーのリストを持つ、順序付けられたグループのリストです。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。一致が見つかるとそのグループのアクションが実行され、後続のグループは評価されないためです。

メンバーは、要求のプロパティを照合する方法を定義します。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やユーザーエージェントなどの複数のプロパティを照合できます。

Exchange ActiveSync用Citrix Gatewayコネクタのセキュリティモデルの選択

セキュリティモデルを確立することは、あらゆる規模の組織にとってモバイルデバイスの展開を成功させるために不可欠です。デフォルトでユーザー、コンピューター、またはデバイスへのアクセスを許可するために、保護されたネットワーク制御または隔離されたネットワーク制御を使用するのが一般的です。この方法は常に理想的であるとは限りません。ITセキュリティを管理するすべての組織は、モバイルデバイスのセキュリティに対してわずかに異なる、またはカスタマイズされたアプローチを持っている場合があります。

同じロジックがモバイルデバイスのセキュリティにも適用されます。多数のモバイルデバイスと種類、ユーザーあたりのモバイルデバイス、および利用可能なオペレーティングシステムプラットフォームとアプリがあるため、許可モデルを使用することは弱い選択です。ほとんどの組織では、制限モデルが最も論理的な選択です。

CitrixがExchange ActiveSync用Citrix GatewayコネクタとXenMobileを統合するために許可する構成シナリオは次のとおりです。

許可モデル（許可モード）

許可セキュリティモデルは、すべてがデフォルトで許可またはアクセスが許可されるという前提で動作します。ルールとフィルタリングによってのみ、何かがブロックされ、制限が適用されます。許可セキュリティモデルは、モバイルデバイスに関するセキュリティ上の懸念が比較的緩い組織に適しています。このモデルは、適切な場合（ポリシー規則が失敗した場合）にのみアクセスを拒否する制限的な制御を適用します。

制限モデル (ブロックモード)

制限的なセキュリティモデルは、デフォルトでは何も許可されず、アクセスも付与されないという前提に基づいています。セキュリティチェックポイントを通過するすべてのものはフィルタリングおよび検査され、アクセスを許可するルールが通過しない限り、アクセスは拒否されます。制限的なセキュリティモデルは、モバイルデバイスに関する比較的厳格なセキュリティ基準を持つ組織に適しています。このモードは、アクセスを許可するすべてのルールが通過した場合にのみ、ネットワークサービスでの使用と機能へのアクセスを許可します。

Exchange ActiveSync 用 Citrix Gateway コネクタの管理

Citrix Gateway connector for Exchange ActiveSync を使用して、アクセス制御ルールを作成できます。これらのルールは、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、デバイスの状態、アプリの許可/ブロックリスト、およびその他のコンプライアンス条件に基づいています。

Exchange ActiveSync 構成ユーティリティ用 Citrix Gateway コネクタを使用すると、企業のメールポリシーを適用する動的および静的ルールを作成でき、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できます。また、メール添付ファイルの暗号化を設定することもでき、Exchange Server を介して管理対象デバイスに渡されるすべての添付ファイルが暗号化され、承認されたユーザーのみが管理対象デバイスで表示できるようになります。

Exchange ActiveSync 用 Citrix Gateway コネクタ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。

Exchange ActiveSync 用 Citrix Gateway コネクタをインストール、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、既存のコネクタのアップグレードまたは削除を許可します。
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 構成サービスと通知サービスを手動で再起動する必要があります。

Exchange ActiveSync 用 Citrix Gateway コネクタのインストール

Exchange ActiveSync 用 Citrix Gateway コネクタは、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かける 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 を超える) の場合、クラスター環境がない場合は、複数のコアをプロビジョニングする必要がある場合があります。コネクタのメモリフットプリントは、より多くのメモリを必要とするほど重要ではありません。

Citrix Gateway connector for Exchange ActiveSync のシステム要件

Citrix Gateway connector for Exchange ActiveSync は、Citrix ADC アプライアンスで構成された SSL ブリッジを介して Citrix ADC と通信します。このブリッジにより、アプライアンスはすべてのセキュアなトラフィックを XenMobile に直接ブリッジできます。このコネクタには、以下の最小システム構成が必要です。

コンポーネント	要件
コンピューターとプロセッサー	733 MHz Pentium III 733 MHz 以上のプロセッサー。2.0 GHz Pentium III 以上のプロセッサー (推奨)
シトリックス ADC	ソフトウェアバージョン 10 の Citrix ADC アプライアンス
メモリ	1 GB
ハードディスク	150 MB の空きハードディスク容量を持つ NTFS 形式の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である必要があります。Windows Server 2008 R2 Service Pack 1 のサポートは January 14, 2020 に終了し、Windows Server 2012 R2 のサポートは October 10, 2023 に終了します。
その他のデバイス	内部ネットワークとの通信のためにホストオペレーティングシステムと互換性のあるネットワークアダプター
マイクロソフト .NET フレームワーク	バージョン 8.5.1.11 には Microsoft .NET Framework 4.5 が必要です。
ディスプレイ	VGA またはそれ以上の解像度のモニター

Exchange ActiveSync 用 Citrix Gateway コネクタのホストコンピューターには、以下の最小空きハードディスク容量が必要です。

- **アプリケーション:** 10〜15 MB (100 MB 推奨)

- **ログ記録:** 1 GB (20 GB 推奨)

Exchange ActiveSync 用 Citrix Gateway コネクタのプラットフォームサポートについては、「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」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、デバイスに対して常に同じ ActiveSync ID を返すわけではありません。Exchange ActiveSync 用 Citrix Gateway コネクタは、各デバイスに対して一意の ActiveSync ID を期待するため、以下のことが当てはまります。各デバイスに対して常に同じ一意の ActiveSync ID を生成するメールクライアントのみがサポートされます。Citrix はこれらのメールクライアントをテストし、クライアントはエラーなしで動作しました。

- Samsung ネイティブメールクライアント
- iOS ネイティブメールクライアント

Exchange ActiveSync 用 Citrix Gateway コネクタの展開

Exchange ActiveSync 用 Citrix Gateway コネクタを使用すると、Citrix ADC を使用して、XenMobile 管理対象デバイスとの XenMobile Server 通信をプロキシおよびロードバランスできます。コネクタは定期的に XenMobile と通信してポリシーを同期します。コネクタと XenMobile は、一緒に、または個別にクラスター化でき、Citrix ADC によってロードバランスできます。

Citrix Gateway connector for Exchange ActiveSync のコンポーネント

- **Citrix Gateway connector for Exchange ActiveSync サービス:** このサービスは、Citrix ADCがデバイスからのActiveSync要求が承認されているかどうかを判断するために呼び出すことができるREST Webサービスインターフェイスを提供します。
- **XenMobile 構成サービス:** このサービスは、XenMobileと通信して、XenMobileのポリシー変更をコネクタと同期します。
- **XenMobile 通知サービス:** このサービスは、不正なデバイスアクセスに関する通知をXenMobileに送信します。これにより、XenMobile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、適切な措置を講じることができます。
- **Citrix Gateway connector for Exchange ActiveSync 構成ユーティリティ:** このアプリケーションを使用すると、管理者はコネクタを構成および監視できます。

Citrix Gateway connector for Exchange ActiveSync のリスニングアドレスを設定するには

Citrix Gateway connector for Exchange ActiveSync がCitrix ADCからのActiveSyncトラフィックを承認する要求を受信するには、次の手順を実行します。コネクタがCitrix ADC 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**メニューから、Exchange ActiveSync 構成ユーティリティ用のCitrix Gateway connectorを選択します。
2. **Web Service**タブをクリックし、コネクタWebサービスのリスニングアドレスを入力します。**HTTP**または**HTTPS**、あるいはその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）は、XenMobileと競合しないポート値を選択してください。
3. 値が構成されたら、**Save**をクリックし、**Start Service**をクリックしてWebサービスを開始します。

Citrix Gateway connector for Exchange ActiveSync でデバイスアクセスコントロール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コントロールポリシーを構成するには、次の手順を実行します。

1. Exchange ActiveSync 構成ユーティリティ用のCitrix Gateway connectorで、**Path Filters**タブをクリックします。
2. 最初の行「**Microsoft-Server-ActiveSync is for ActiveSync**」を選択し、**Edit**をクリックします。
3. **ポリシー**リストから、目的のポリシーを選択します。XenMobileポリシーを含むポリシーの場合は、**Static + ZDM: Permit Mode または Static + ZDM: Block Mode** を選択します。これらのポリシーは、ローカル（または静的）ルールとXenMobileからのルールを組み合わせたものです。Permit Mode は、ルールによって明示的に識別されていないすべてのデバイスがActiveSyncへのアクセスを許可されることを意味します。Block Mode は、そのようなデバイスがブロックされることを意味します。
4. ポリシーを設定したら、 をクリックします。

XenMobile との通信を構成するには

Citrix Gateway connector for Exchange ActiveSync および Citrix ADC で使用する XenMobile Server (Config Provider とも呼ばれます) の名前とプロパティを指定します。

> **注:**
>
> このタスクは、XenMobile がすでにインストールおよび構成されていることを前提としています。

1. Citrix Gateway connector for Exchange ActiveSync 構成ユーティリティで、 タブをクリックし、 をクリックします。
2. この展開で使用している XenMobile Server の名前と URL を入力します。マルチテナント展開で複数の XenMobile Server を展開している場合、この名前は各サーバーインスタンスで一意である必要があります。たとえば、 に「**XMS**」と入力できます。
3. に、XenMobile GlobalConfig Provider (GCP) の Web アドレスを入力します。通常、形式は `https://<FQDN>/<instanceName>/services/<MagConfigService>` です。*MagConfigService* の名前では大文字と小文字が区別されます。
4. に、XenMobile Web サーバーでの基本 HTTP 認証に使用されるパスワードを入力します。
5. に、Citrix Gateway connector for Exchange ActiveSync をインストールしたサーバー名を入力します。
6. で、XenMobile から新しい更新された動的ルールセットがプルされる期間を指定します。
7. で、サーバー要求のタイムアウト間隔を指定します。
8. で、構成プロバイダーサーバーインスタンスがポリシー構成を提供するかどうかを選択します。
9. で、デバイスがブロックされたときに Secure Mobile Gateway が XenMobile に通知するようにする場合は、このオプションを有効にします。このオプションは、Device Manager の自動アクションで Secure Mobile Gateway ルールを使用している場合に必要です。
10. サーバーを構成したら、 をクリックして XenMobile への接続をテストします。
11. 接続が確立されたら、**保存**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 connector for Exchange ActiveSyncの展開

Citrix Gateway connector for Exchange ActiveSyncおよびXenMobileの展開をスケーリングしたい場合、複数のWindows Serverにコネクタのインスタンスをインストールし、すべて同じXenMobileインスタンスを指すようにして、Citrix ADCを使用してサーバーの負荷分散を行うことができます。

Citrix Gateway connector for Exchange ActiveSyncの構成には2つのモードがあります。

- 非共有モードでは、各Citrix Gateway connector for Exchange ActiveSyncインスタンスはXenMobile Serverと通信し、結果として得ら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、各XenMobile Serverでコネクタインスタンスを実行でき、コネクタはローカルのXenMobileインスタンスからポリシーを取得します。
- 共有モードでは、1つのコネクタノードがプライマリノードとして選択され、XenMobileと通信します。結果として得られる構成は、Windowsネットワーク共有またはWindows（あるいはサードパーティ）レプリケーションのいずれかによって、他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（いくつかのXMLファイルで構成）にあります。コネクタプロセスは、このフォルダー内のファイルの変更を検出し、自動的に構成を再ロードします。共有モードでは、プライマリノードのフェイルオーバーはありません。しかし、最後に認識された正常な構成がコネクタプロセスにキャッシュされているため、システムはプライマリサーバーが数分間（たとえば、再起動のため）ダウンしても許容できます。

高度な概念

> **注:**
>
> この記事では、XenMobile Server の高度な概念について説明します。Citrix Endpoint Management の高度な情報については、高度な概念を参照してください。

> XenMobile® の高度な概念に関する記事では、XenMobile の製品ドキュメントをより深く掘り下げて説明しています。その目的は、専門的な手法を通じて展開時間を短縮することです。これらの記事では、コンテンツを作成した技術専門家を引用している場合があります。

エンドツーエンドの XenMobile 環境における意思決定ポイント、推奨事項、よくある質問、ユースケースについては、このセクションの XenMobile 展開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® と Active Directory の連携

この記事では、XenMobile Server と Active Directory の連携について説明します。XenMobile Server は、インラインおよびバックグラウンドの両方で Active Directory と連携します。以下のセクションでは、Active Directory との連携を伴うインライン操作とバックグラウンド操作について詳しく説明します。

> **注：**
>
> この記事は連携の概要であり、詳細な内容には触れていません。XenMobile コンソールでの Active Directory および LDAP の構成について詳しくは、「ドメインまたはドメインとセキュリティトークン認証」を参照してください。

インライン連携

XenMobile Server は、管理者が構成する LDAP 設定を使用して Active Directory と通信します。これらの設定は、ユーザーとグループに関する情報を取得します。以下は、XenMobile Server と Active Directory の連携につながる操作です。

1. **LDAP 構成。**Active Directory 自体の構成により、Active Directory との連携が発生します。XenMobile Server は、Active Directory で情報を認証することにより、その情報の検証を試みます。サーバーは、指定されたインターネットプロトコル、ポート、およびサービスアカウントの資格情報を使用してこれを行います。バインドが成功すると、接続が正しく構成されていることを示します。
2. **グループベースの連携。**

   a. ロールベースのアクセス制御（RBAC）およびデリバリーグループ定義の作成中に、1つ以上のグループを検索します。XenMobile Server 管理者は、XenMobile コンソールで検索テキスト文字列を入力します。XenMobile Server は、指定されたサブストリングを持つすべてのグループについて、選択されたドメインを検索します。その後、XenMobile Server は、検索で識別されたグループの objectGUID、sAMAccountName、および Distinguished Name 属性を取得します。

   > **注：**
   >
   > この情報は XenMobile Server データベースには保存されません。

   b. RBAC および展開グループ定義の追加または更新。XenMobile Server 管理者は、以前の検索に基づいて対象の Active Directory グループを選択し、それらを展開グループ定義に含めます。XenMobile Server は、Active Directory 内で特定のグループを一度に1つずつ検索します。XenMobile Server は objectGUID 属性を検索し、メンバーシップ情報を含む選択された属性を取得します。グループメンバーシップ情報は、取得されたグループと XenMobile Server データベース内の既存のユーザーまたはグループとの間のメンバーシップを判断するのに役立ちます。グループメンバーシップの変更は、影響を受けるユーザーメンバーの RBAC および展開グループの派生につながり、ユーザーの資格を決定します。

   > **注：**
   >
   > 展開グループ定義の変更は、影響を受けるユーザーのアプリまたはポリシーの資格の変更につながる可能性があります。

c. **ワンタイム PIN（OTP）招待。**XenMobile Server 管理者は、XenMobile Server データベースに存在する Active Directory グループのリストからグループを選択します。このグループの場合、直接的および間接的なすべてのユーザーが Active Directory から取得されます。OTP 招待は、前の手順で識別されたユーザーに送信されます。

> **注記:**
>
> 前述の3つのやり取りは、グループベースのやり取りがXenMobile Serverの構成変更に基づいてトリガーされることを意味します。構成に変更がない場合、これらのやり取りはActive Directoryとのやり取りがないことを意味します。また、定期的にグループ側の変更を捕捉するためのバックグラウンドジョブの要件がないことも意味します。

3. **ユーザーベースのやり取り**

a. **ユーザー認証:** ユーザー認証ワークフローは、Active Directoryとの2つのやり取りをもたらします。

- 提供された資格情報でユーザーを認証するために使用されます。
- objectGUID、識別名、sAMAccountName、およびグループへの直接メンバーシップを含む、選択されたユーザー属性をXenMobile Serverデータベースに追加または更新します。グループメンバーシップの変更により、アプリ、ポリシー、およびアクセス権限が再評価されます。

ユーザーは、デバイスから、またはXenMobile Serverコンソールから認証できます。どちらのシナリオでも、Active Directoryとのやり取りは同じ動作に従います。

b. **App Storeへのアクセスと更新:** ストアの更新により、直接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。このアクションにより、ユーザーの権限が再評価されます。

c. **デバイスのチェックイン:** 管理者は、XenMobileコンソールでデバイスの定期的なチェックインを設定できます。デバイスがチェックインされるたびに、直接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。これらのチェックインにより、ユーザーの権限が再評価されます。

d. **グループによるOTP招待:** XenMobile Server管理者は、XenMobile Serverデータベースに存在するActive Directoryグループのリストからグループを選択します。直接的および間接的（ネストのため）なユーザーメンバーは、Active Directoryから取得され、XenMobile

Serverデータベースに保存されます。OTP招待は、前述のステップで特定されたユーザーメンバーに送信されます。

e. **ユーザーによるOTP招待:** 管理者はXenMobileコンソール内で検索テキスト文字列を入力します。XenMobile ServerはActive Directoryを照会し、入力されたテキスト文字列に一致するユーザーレコードを返します。その後、管理者はOTP招待を送信するユーザーを選択します。XenMobile ServerはActive Directoryからユーザーの詳細を取得し、ユーザーに招待を送信する前に同じ詳細をデータベースで更新します。

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から得られる結論の1つは、グループベースのやり取りがXenMobile Server構成の選択された変更に基づいてトリガーされるということです。構成に変更がない場合、グループに対するActive Directoryとのやり取りがないことを意味します。

このやり取りには、Active Directoryと定期的に同期し、関連する変更を対象グループに更新するバックグラウンドジョブが必要です。

以下は、Active Directoryとやり取りするバックグラウンドジョブです。

1. **グループ同期ジョブ**。このジョブの目的は、関心のあるグループについて、Active Directoryに対し、識別名またはsAMAccountName属性の変更をグループごとに照会することです。Active Directoryへの検索クエリは、関心のあるグループのobjectGUIDを使用して、識別名とsAMAccountName属性の現在の値を取得します。関心のあるグループの識別名またはsAMAccountName値の変更は、データベースに更新されます。

   > **注：**
   >
   > このジョブは、ユーザーからグループへのメンバーシップ情報を更新しません。

2. **ネストされたグループ同期ジョブ**。このジョブは、関心のあるグループのネスト階層の変更を更新します。XenMobile Serverは、関心のあるグループの直接メンバーと間接メンバーの両方がエンタイトルメントを取得できるようにします。ユーザーの直接メンバーシップは、ユーザーベースのインラインインタラクション中に更新されます。バックグラウンドで実行されるこのジョブは、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、ユーザーが、関心のあるグループのメンバーであるグループのメンバーである場合を指します。

   このジョブは、XenMobile ServerデータベースからActive Directoryグループのリストを収集します。これらのグループは、展開グループまたはRBAC定義の一部です。このリストの各グ

ループについて、XenMobile Serverは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のリストです。

XenMobile Serverは、関心のあるグループのユーザーメンバーのみを取得するために、Active Directoryに別のクエリを実行します。2つのリストの差は、関心のあるグループのグループメンバーのみを示します。メンバーグループの変更はデータベースに更新されます。階層内のすべてのグループに対して同じプロセスが繰り返されます。

ネストの変更により、影響を受けるユーザーのエンタイトルメント変更が処理されます。

3. **無効なユーザーの確認**。このジョブは、XenMobile管理者が無効なユーザーを確認するアクションを作成した場合にのみ実行されます。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。このジョブは、Active Directoryにクエリを実行して、関心のあるユーザーの無効なステータスをユーザーごとに確認します。

よくある質問

バックグラウンドジョブの実行頻度は、デフォルトでどのくらいですか？

- グループ同期ジョブは、現地時間の午前2時から5時間ごとに実行されます。
- ネストされたグループ同期ジョブは、現地時間の深夜に1日1回実行されます。

グループ同期ジョブが必要なのはなぜですか？

- Active Directoryのユーザーレコードの**memberOf**属性は、ユーザーが直接メンバーであるグループのリストを提供します。グループが1つのOUから別のOUに移動すると、**memberOf**属性は識別名の最新の値を反映します。XenMobile Serverデータベースにも、最後に更新された値があります。グループの識別名に不一致があると、ユーザーが展開グループへのアクセスを失う可能性があります。ユーザーは、その展開グループに関連付けられているアプリとポリシーも失う可能性があります。
- バックグラウンドジョブは、ユーザーがエンタイトルメントにアクセスできるように、XenMobile Serverデータベースのグループ識別名属性を最新の状態に保ちます。
- 同期ジョブは5時間ごとにスケジュールされます。これは、Active Directory内のグループ変更がまれであると想定されているためです。

グループ同期ジョブをオフにできますか？

- 対象のグループが1つのOUから別のOUに変更されないことがわかっている場合、ジョブをオフにできます。

ネストされたグループ処理のバックグラウンドジョブが必要なのはなぜですか？

- Active Directoryにおけるグループのネストの変更は日常的に発生するものではありません。対象グループのネスト階層の変更は、影響を受けるユーザーのエンタイトルメントの変更につながります。グループが階層に追加されると、そのメンバーユーザーはそれぞれの役割に対するエンタイトルメントが付与されます。グループがネストから外れると、そのグループのメンバーユーザーはロールベースのエンタイトルメントへのアクセスを失う可能性があります。
- ネストの変更はユーザーのリフレッシュ中に捕捉されません。ネストの変更はオンデマンドではできないため、変更はバックグラウンドジョブを通じて捕捉されます。
- ネストの変更はまれであると想定されているため、バックグラウンドジョブは1日1回実行され、変更がないか確認します。

ネストされたグループ処理ジョブをオフにできますか？

- 対象のグループにネストの変更が発生しないことがわかっている場合、ジョブをオフにできます。

XenMobile® の展開

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。

- どのデバイスを選択するか？
- デバイスを管理する方法は？
- 優れたユーザーエクスペリエンスを提供しながら、ネットワークのセキュリティを維持するにはどうすればよいか？
- どのようなハードウェアが必要で、そのトラブルシューティングをどのように行うか？

このセクションの記事は、このような疑問に答えることを目的としています。展開に関する懸念事項を網羅するトピックについて、ユースケースと推奨事項が含まれています。

ガイドラインや推奨事項がすべての環境やユースケースに適用されるとは限らないことに留意してください。XenMobile の展開を本稼働させる前に、必ずテスト環境をセットアップしてください。

このセクションの記事では、以下の領域について説明します。

- **評価:** 展開を計画する際に考慮すべき一般的な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
- **運用と監視:** 稼働中の環境が円滑に動作していることを確認する。

評価

他の展開と同様に、ニーズの評価が最優先事項です。XenMobile の主なニーズは何ですか？環境内のすべてのデバイスを管理する必要がありますか、それともアプリだけですか？両方を管理する必要があるかもしれません。XenMobile 環境はどの程度のセキュリティが必要ですか？展開を計画する際に考慮すべき一般的なユースケースと質問を見てみましょう。

- 管理モード
- デバイス要件
- 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の統合
- マルチサイト要件

設計と構成

展開のニーズの評価が完了したら、環境の設計と構成を決定できます。計画する必要がある事項をいくつか示します。

- サーバーのハードウェアの選択
- アプリとデバイスのポリシーの設定
- ユーザーの登録

このセクションでは、これらの各シナリオなどに関するユースケースと推奨事項について説明します。

- Citrix ADCおよびCitrix Gatewayとの統合
- MDXアプリのSSOとプロキシに関する考慮事項
- 認証
- オンプレミス展開の参照アーキテクチャ
- サーバープロパティ
- デバイスとアプリのポリシー
- ユーザー登録オプション
- XenMobile操作のチューニング

運用と監視

XenMobile環境が稼働したら、スムーズな運用を確保するために監視したくなるでしょう。監視セクションでは、以下について説明します。

- 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を見つける場所
- それらのログの読み方

このセクションには、カスタマーサポートのフィードバック時間を短縮するために従うことができる、さまざまな一般的なトラブルシューティング手順も含まれています。

- 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
- ロールベースのアクセス制御とXenMobileサポート
- システム監視
- 災害復旧
- Citrix サポートプロセス

管理モード

各XenMobile®インスタンス（単一サーバーまたはノードクラスター）について、デバイス、アプリ、あるいはその両方を管理するかどうかを選択できます。XenMobileは、デバイスおよびアプリの管理モードに以下の用語を使用します。

- モバイルデバイス管理モード（MDMモード）
- モバイルアプリ管理モード（MAMモード）
- MDM+MAMモード（エンタープライズモード）

モバイルデバイス管理（MDMモード）

> **重要:**

> MDMモードを構成し、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は、ユーザー登録後に認証モードを変更することをサポートしていません。詳細については、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構成、保護、およびサポートできます。MDMにより、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構成できます。たとえば、デバイスが紛失、盗難、またはコンプライアンス違反の場合、デバイスを選択的にワイプできます。MDMモードではアプリ管理は利用できませんが、このモードで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。MDMモードの一般的なユースケースは次のとおりです。

- MDMは、完全ワイプ、選択的ワイプ、地理位置情報などのデバイスレベルの管理ポリシーまたは制限が必要な、企業所有デバイスの検討事項です。
- 顧客が実際のデバイスの管理を必要とするが、アプリのコンテナ化、アプリデータ共有の制御、マイクロVPNなどのMDXポリシーを必要としない場合。
- ユーザーがモバイルデバイス上のネイティブメールクライアントにメールを配信するだけでよく、Exchange ActiveSyncまたはClient Access Serverが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を使用してメール配信を構成できます。
- 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る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データ漏洩を防げない可能性があることに注意してください。Office 365アプリでのコピー＆ペーストや名前を付けて保存の操作でデータ漏洩が発生する可能性があります。

モバイルアプリ管理（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ます。MAMはまた、個人データとは別に企業データとリソースの管理を可能にします。MAMモード用に構成されたXenMobileを使用すると、MDX対応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モードという用語は、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モードと区別します。

MDXポリシーを使用することで、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インタラクション、データ暗号化、アプリアクセスに対するアプリレベルの制御を提供します。

MAMは、デバイスが管理されていなくても企業データが保護されるため、BYO（個人所有）デバイスに適していることがよくあります。MDXには、MDM制御を必要としないMAM専用ポリシーが多数あります。

MAMは、モバイル生産性アプリもサポートしています。このサポートには、Citrix Secure Mailへのセキュアなメール配信、保護されたモバイル生産性アプリ間のデータ共有、Citrix Filesでのセキュアなデータストレージが含まれます。詳細については、モバイル生産性アプリを参照してください。

MAMは、以下の例に適していることがよくあります。

- アプリレベルで管理されるMDXアプリなどのモバイルアプリを配信する場合。
- システムレベルでデバイスを管理する必要がない場合。

MDM+MAM（エンタープライズモード）

MDM+MAMは、エンタープライズモードとも呼ばれるハイブリッドモードで、XenMobile Enterprise Mobility Management (EMM) ソリューションで利用可能なすべての機能セットを有効にします。XenMobileをMDM+MAMモードで構成すると、MDM機能とMAM機能の両方が有効になります。

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どうか、またはデバイス管理を必須とするかどうかを指定できます。この柔軟性は、さまざまな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リソースにアクセスするためにMDMポリシーによるデバイス管理が必要な場合とそうでない場合があります。

MDM+MAMは、以下の例に適しています。

- MDMとMAMの両方が必要な単一のユースケースがある場合。MAMリソースにアクセスするにはMDMが必要です。
- 一部のユースケースではMDMが必要ですが、そうでないユースケースもあります。
- 一部のユースケースではMAMが必要ですが、そうでないユースケースもあります。

XenMobile Serverの管理モードは、**Server Mode**プロパティで指定します。この設定はXenMobileコンソールで構成します。モードは、MDM、MAM、またはENT（MDM+MAMの場合）のいずれかです。

ライセンスを持つXenMobileエディションによって、以下の表に示すように、利用可能な管理モードやその他の機能が決まります。

XenMobile MDM エディション	**XenMobile Advanced エディション**
MDM 機能	MDM 機能

-	MAM 機能
-	MAM SDK
セキュアハブ	セキュアハブ
-	セキュアメール
-	セキュアウェブ

管理モードと登録プロファイル

管理モードと登録プロファイルは連携して動作します。登録プロファイルを使用して、Android および iOS デバイスのデバイス管理およびアプリ管理の登録オプションを構成します。Android の場合、MDM+MAM サーバーモードで利用可能な登録オプションは、MDM モードのオプションとは異なります。詳細については、登録プロファイルを参照してください。

デバイス管理と MDM 登録

XenMobile Enterprise 環境には、さまざまなユースケースが含まれる場合があります。その中には、MAM リソースへのアクセスを許可するために MDM ポリシーによるデバイス管理を必要とするものもあります。モバイル生産性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 登録を必須とするかどうかを決定してください。後で MDM 登録の要件を変更することにした場合、ユーザーはデバイスを再登録する必要がある可能性が高いです。

> **注:**
>
> ユーザーに MDM 登録を要求するかどうかを指定するには、XenMobile コンソール (**設定 > サーバープロパティ**) で XenMobile Server プロパティ **Enrollment Required** を使用します。こ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。

以下は、XenMobile Enterprise モード展開で MDM 登録を必須とする場合の利点と欠点（およびその軽減策）の概要です。

MDM 登録がオプションの場合

利点:

- 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ます。このオプションは、ユーザーの採用を増やすことができます。
- 企業データを保護するために、MAM リソースへのアクセスを保護する機能。
- **App Passcode** などの MDX ポリシーは、各 MDX アプリのアプリアクセスを制御できます。
- Citrix ADC、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 とともに構成することで、追加の保護層が提供されます。
- MDM アクションはデバイスに適用されませんが、MAM アクセスを拒否するための MDX ポリシーがいくつか利用可能です。拒否は、ジェイルブレイクされたデバイスやルート化されたデバイスなどのシステム設定に基づきます。
- ユーザーは、初回使用時にデバイスを MDM に登録するかどうかを選択できます。

欠点:

- MAMリソースは、MDMに登録されていないデバイスでも利用できます。
- MDMポリシーとアクションは、MDMに登録されているデバイスでのみ利用できます。

軽減策のオプション:

- ユーザーに、コンプライアンス違反を選択した場合に責任を負うことを定めた会社の利用規約に同意させる。管理者に、管理されていないデバイスを監視させる。
- アプリケーションタイマーを使用して、アプリケーションのアクセスとセキュリティを管理します。タイムアウト値を短縮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を与える可能性があります。
- MDM登録が必要な2つ目のXenMobile環境も選択肢の1つです。このオプションを検討する際は、2つの環境を管理するための追加のオーバーヘッドと、必要な追加リソースを考慮してください。

MDM登録が必要な場合

利点:

- MAMリソースへのアクセスをMDM管理デバイスのみに制限する機能。
- MDMポリシーとアクションは、必要に応じて環境内のすべてのデバイスに適用できます。
- ユーザーはデバイスの登録を拒否できません。

欠点:

- すべてのユーザーがMDMに登録する必要があります。
- 個人デバイスの企業管理に反対するユーザーの導入を減少させる可能性があります。

軽減策のオプション:

- ユーザーに、XenMobileがデバイス上で実際に何を管理しているのか、管理者がどのような情報にアクセスできるのかを教育します。
- MDM管理を必要としないデバイスには、MAMのサーバーモード（MAM専用モードとも呼ばれます）を持つ2つ目のXenMobile環境を使用できます。このオプションを検討する際は、2つの環境を管理するための追加のオーバーヘッドと、追加で必要となるリソースを考慮してください。

MAMおよびレガシーMAMモードについて

XenMobile 10.3.5では、新しいMAM専用サーバーモードが導入されました。以前のMAMモードと新しいMAMモードを区別するために、ドキュメントではこれらの用語を使用しています。新しいモードはMAM専用またはMAと呼ばれ、以前のMAMモードはレガシーMAMモードと呼ばれます。

XenMobileの**サーバーモード**プロパティがMAMの場合、MAM専用モードが有効になります。デバイスはMAMモードで登録されます。

XenMobileの**サーバーモード**プロパティがENTで、ユーザーがデバイス管理をオプトアウトすることを選択した場合、レガシーMAM機能が有効になります。その場合、デバイスはMAMモードで登録されます。MDM管理をオプトアウトしたユーザーは、引き続きレガシーMAM機能を受け取ります。

> **注：**
>
> 以前は、サーバーモードプロパティをMAMに設定することは、ENTに設定することと同じ効果がありました。MDM管理をオプトアウトしたユーザーは、レガシーMAM機能を受け取っていました。

> 次の表は、特定のライセンスタイプと目的のデバイスモードで使用する**サーバーモード**設定をまとめたものです。

お使いのライセンスは次のエディション用です	**デバイスをこのモードで登録したい場合**	**サーバーモードプロパティを次のように設定します**
Enterprise/ Advanced/MDM	MDMモード	MDM

エンタープライズ/アドバンスト	MAMモード（MAM専用モードとも呼ばれます）	MAM
エンタープライズ/アドバンスト	MDM+MAMモード	ENT（デバイス管理をオプトアウトしたユーザーは、レガシーMAMモードで動作します。）

MAM専用モードは、以前はENTでのみ利用可能だった次の機能をサポートしています。

- **証明書ベースの認証:** MAM専用モードは証明書ベースの認証をサポートしています。ユーザーは、Active Directoryのパスワードが期限切れになっても、アプリへの継続的なアクセスを体験できます。MAMデバイスで証明書ベースの認証を使用する場合は、Citrix Gatewayを構成する必要があります。デフォルトでは、**XenMobile Settings > Citrix Gateway**で、が**オフ**に設定されており、これはユーザー名とパスワードによる認証が使用されることを意味します。その設定を**オン**に変更して、証明書認証を有効にします。
- **セルフヘルプポータル:** ユーザーが自分でアプリのロックとアプリのワイプを実行できるようにします。これらのアクションは、デバイス上のすべてのアプリに適用されます。アプリのロックとアプリのワイプのアクションは、**Configure > Actions**で構成できます。
- **すべての登録セキュリティモード:** 高セキュリティ、招待URL、2要素認証を含み、**Manage > Enrollment Invitations**を通じて構成されます。
- **AndroidおよびiOSデバイスのデバイス登録制限:** サーバープロパティ**Number of Devices Per User**は**Configure > Enrollment Profiles**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専用API:** MAM専用デバイスの場合、任意のRESTクライアントとXenMobile REST APIを使用して、XenMobileコンソールが公開するサービスを呼び出すことができます。
- MAM専用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。
    - デバイスでアプリのロックとワイプを発行する。

以下の表は、レガシーMAMとMAM専用機能の違いをまとめたものです。

登録シナリオとその他の機能	**レガシーMAM (サーバーモードはENT)**	**MAM専用モード (サーバーモードはMAM)**

証明書認証	サポートされていません。	サポートされています。証明書認証には、Citrix Gatewayが必要です。
展開要件	XenMobile Serverは、デバイスから直接アクセスできる必要はありません。	XenMobile Serverは、デバイスから直接アクセスできる必要はありません。
登録オプション	Citrix 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ます。	XenMobile Server FQDNを使用します。
登録方法*	ユーザー名 + パスワード	ユーザー名 + パスワード、高セキュリティ、招待URL、招待URL+PIN、招待URL + パスワード、2要素認証、ユーザー名 + PIN
アプリのロックとワイプ	サポートされています。	サポートされています。
アプリのロックとワイプのセルフヘルプポータルオプション	サポートされていません。	サポートされています。
アプリのワイプ動作	アプリはデバイスに残りますが、使用できません。XenMobileはクライアント上のアカウントのみを削除します。	アプリはデバイスに残りますが、使用できません。XenMobileはクライアント上のアカウントのみを削除します。
MAM専用ユーザー向けの自動化されたアクション。	イベント、デバイスプロパティ、ユーザープロパティのアクションはサポートされています。インストールされているアプリベースの自動化されたアクションはサポートしていません。	イベント、デバイスプロパティ、ユーザープロパティ、およびアプリのワイプとアプリのロックを含む一部のアプリベースのアクションをサポートします。
Active Directoryユーザーが削除された場合の組み込みアクション	アプリのワイプをサポートします。	アプリのワイプをサポートします。

登録制限	サポートされています。登録プロファイルを通じて構成されます。	サポートされています。登録プロファイルを通じて構成されます。
ソフトウェアインベントリ	サポートされています。XenMobileはデバイスにインストールされているアプリを一覧表示します。	サポートされていません。

***通知について:** SMTPは、登録招待を送信するための唯一のサポートされている方法です。

> **重要:**
>
> MAM専用モードの場合、以前に登録されたユーザーはデバイスを再登録する必要があります。ユーザーに登録に必要なXenMobile Server FQDNを提供してください。MAM専用モードでは、ENTモードと同様に、デバイスはXenMobile Server FQDNを使用して登録します。（レガシーMAMモードでは、デバイスはCitrix Gateway FQDNを使用して登録します。）

デバイス要件

あらゆる展開において考慮すべき重要な点は、展開を計画しているデバイスです。iOS、Android、Windowsプラットフォームでは、多くの選択肢があります。XenMobileがサポートするデバイスのリストについては、「サポートされているデバイスプラットフォーム」(/ja-jp/xenmobile/server/system-requirements/supported-device-platforms.html)を参照してください。

BYOD (Bring Your Own Device) 環境では、サポートされている複数のプラットフォームが混在する可能性があります。ただし、ユーザーが登録できるデバイスについて通知する際は、「サポートされているデバイスプラットフォーム」の記事にある制限事項を考慮してください。環境内で1つまたは2つのデバイスのみを許可している場合でも、XenMobile®はiOS、Android、Windowsデバイスでわずかに異なる動作をします。各プラットフォームで異なる機能セットが利用可能です。

また、すべてのアプリデザインがタブレットと電話の両方のフォームファクターを対象としているわけではありません。広範囲な変更を行う前に、展開したいデバイスの画面にアプリが適合するかどうかをテストしてください。

登録要素も考慮できます。AppleとGoogleは、企業向け登録プログラムを提供しています。Apple Deployment ProgramとGoogle Android Enterpriseを通じて、従業員がすぐに使用できる事前設定済みのデバイスを購入できます。

登録の詳細については、「ユーザー登録オプション」(/ja-jp/xenmobile/server/advanced-concepts/xenmobile-deployment/user-enrollment-options.html)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

セキュリティはどの組織にとっても重要ですが、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取る必要があります。たとえば、ユーザーが使いにくい、非常に安全な環境になっている場合があります。あるいは、環境が非常にユーザーフレンドリーであるため、アクセス制御がそれほど厳しくない場合もあります。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。この記事の目的は、一般的なセキュリティ上の懸念事項と、XenMobileで利用できるセキュリティオプションの概要を説明することです。

各ユースケースで留意すべき重要な考慮事項を以下に示します。

- 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？
- ユーザーにどのようにIDを認証させたいですか？LDAP、証明書ベースの認証、またはその両方の組み合わせを使用する予定ですか？
- ユーザーセッションのタイムアウトをどのように処理しますか？バックグラウンドサービス、Citrix ADC、およびオフライン中にアプリにアクセスできる場合のタイムアウト値は異なることに注意してください。
- ユーザーにデバイスレベルのパスコード、アプリレベルのパスコード、またはその両方を設定させたいですか？ユーザーに何回のログオン試行を許可しますか？MAMで実装された追加のアプリごとの認証要件がユーザーエクスペリエンスにどのように影響するかを考慮してください。
- ユーザーにどのような他の制限を課したいですか？ユーザーにSiriなどのクラウドサービスへのアクセスを許可しますか？提供する各アプリで、ユーザーは何ができて何ができませんか？オフィス内で携帯電話のデータプランが消費されるのを防ぐために、企業Wi-Fiポリシーを展開しますか？

アプリとデバイス

最初に考慮すべきことの1つは、モバイルアプリ管理（MAM）を使用して特定のアプリのみを保護するかどうかです。あるいは、モバイルデバイス管理（MDM）を使用してデバイス全体も管理したいかどうかです。一般的に、デバイスレベルの制御が必要ない場合は、特に組織がBring Your Own Device（BYOD）をサポートしている場合、モバイルアプリのみを管理します。

XenMobileが管理しないデバイスを持つユーザーは、アプリストアを通じてアプリをインストールできます。選択的または完全なワイプなどのデバイスレベルの制御の代わりに、アプリポリシーを通じてアプリへのアクセスを制御します。設定した値に応じて、ポリシーはデバイスが定期的に

XenMobileをチェックし、アプリが引き続き実行を許可されていることを確認することを要求します。

MDMを使用すると、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する機能を含め、デバイス全体を保護できます。デバイスがジェイルブレイクされている、ルート化されている、または安全でないソフトウェアがインストールされている場合、登録を防止できます。しかし、このレベルの制御を行うと、ユーザーは自分の個人デバイスに対するそのような多くの権限を許可することに警戒心を抱き、登録率が低下する可能性があります。

認証

認証は、ユーザーエクスペリエンスの大部分が行われる場所です。組織がすでにActive Directoryを実行している場合、Active Directoryを使用することが、ユーザーがシステムにアクセスするための最も簡単な方法です。

認証ユーザーエクスペリエンスのもう1つの重要な部分はタイムアウトです。高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ことができますが、そのオプションはすべての組織にとって理想的ではありません。たとえば、ユーザーがメールにアクセスするたびに資格情報を入力させることは、ユーザーエクスペリエンスに大きな影響を与える可能性があります。

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できます。Citrix Secure Hub™やその他のいくつかのアプリは、すべてが適切に機能するように、パスワード、PIN、証明書などの共通データを共有することがよくあります。この情報は、Secure Hub内の汎用ボールトに保存されます。**Encrypt Secrets**オプションを通じてユーザーエントロピーを有効にすると、XenMobileはUserEntropyという新しいボールトを作成します。XenMobileは、汎用ボールトから新しいボールトに情報を移動します。Secure Hubまたは別のアプリが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、複数の場所で認証レイヤーが追加されます。その結果、アプリがUserEntropyボールト内の証明書を含む共有データへのアクセスを要求するたびに、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の詳細については、XenMobileドキュメントの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有効にするには、関連設定をクライアントプロパティで確認できます。

ポリシー

MDXポリシーとMDMポリシーはどちらも組織に大きな柔軟性をもたらしますが、ユーザーを制限することもできます。たとえば、機密データをさまざまな場所に送信する可能性のある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ブロックしたい場合があります。これらのサービスへのアクセスをブロックするポリシーを設定できますが、そのようなポリシーには意図しない結果が生じる可能性があることに留意してください。iOSキーボードマイクもクラウドアクセスに依存しており、その機能へのアクセスもブロックする可能性があります。

アプリ

エンタープライズモビリティ管理 (EMM) は、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) に分かれます。MDMが組織によるモバイルデバイスのセキュリティ保護と制御を可能にする一方、MAMはアプリケーションの配信と管理を容易にします。BYODの採用が増加するにつれて、通常、アプリケーションの配信、ソフトウェアライセンス、構成、およびアプリケーションライフサイクル管理を支援するためにMAMソリューションを実装できます。

XenMobileを使用すると、特定のMAMポリシーとVPN設定を構成して、データ漏洩やその他のセキュリティ脅威を防ぐことで、これらのアプリをさらに保護できます。XenMobileは、組織に以下のいずれかのソリューションを展開する柔軟性を提供します。

- MAM専用環境
- MDM専用環境
- MDMとMAMの両方の機能を同じプラットフォームで提供する統合XenMobile Enterprise環境

モバイルデバイスにアプリを配信する機能に加えて、XenMobileはMDXテクノロジーを介したアプリのコンテナ化を提供します。MDXは、プラットフォームによって提供される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。アプリをワイプまたはロックでき、アプリはきめ細かなポリシーベースの制御の対象となります。独立系ソフトウェアベンダー (ISV) は、Mobile Apps SDKを使用してこれらの制御を適用できます。

企業環境では、ユーザーは職務を支援するためにさまざまなモバイルアプリを使用します。アプリには、パブリックアプリストアのアプリ、社内開発アプリ、ネイティブアプリが含まれます。XenMobileはこれらのアプリを次のように分類します。

パブリックアプリ: これらのアプリには、Apple App StoreやGoogle Playなどのパブリックアプリストアで利用可能な無料または有料のアプリが含まれます。組織外のベンダーは、多くの場合、パブリックアプリストアでアプリを提供しています。このオプションにより、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応じて、組織内で多数のパブリッ

クアプリを使用する場合があります。このようなアプリの例には、GoToMeeting、Salesforce、EpicCareアプリなどがあります。

Citrix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し、それをMDX Toolkitでラップしてエンタープライズ配布することをサポートしていません。サードパーティ製アプリケーションをMDX対応にするには、アプリベンダーに連絡してアプリバイナリを入手してください。バイナリはMDX Toolkitを使用してラップするか、MAM SDKをバイナリと統合することができます。

社内アプリ: 多くの組織には、特定の機能を提供し、組織内で独自に開発および配布されるアプリを作成する社内開発者がいます。特定のケースでは、一部の組織はISVが提供するアプリも持っている場合があります。そのようなアプリはネイティブアプリとして展開することも、XenMobileなどのMAMソリューションを使用してコンテナ化することもできます。たとえば、医療機関は、医師がモバイルデバイスで患者情報を表示できる社内アプリを作成できます。組織は、患者情報を保護し、バックエンドの患者データベースサーバーへのVPNアクセスを可能にするために、そのアプリをMAM SDK対応にするか、MDMでラップすることができます。

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（Webアプリ）またはパブリックネットワーク（SaaS）からアクセスするアプリが含まれます。XenMobileでは、アプリコネクタのリスト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は、既存のWebアプリへのシングルサインオン（SSO）を容易にすることができます。詳細については、「アプリコネクタの種類」を参照してください。たとえば、Security Assertion Markup Language (SAML) に基づくSSOのために、Google Apps SAMLをGoogle Appsに使用できます。

モバイル生産性アプリ: XenMobileライセンスに含まれるCitrix開発のアプリ。詳細については、「モバイル生産性アプリについて」を参照してください。Citrixは、ISVがMobile Apps SDKを使用して開発するその他のビジネス対応アプリも提供しています。

HDXアプリ: StoreFrontで公開するWindowsホスト型アプリ。Citrix Virtual Apps and Desktops™環境がある場合、アプリをXenMobileと統合して、登録済みユーザーがアプリを利用できるようにすることができます。

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、基盤となる構成とアーキテクチャは異なります。たとえば、異なる権限レベルを持つ複数のユーザーグループが単一のアプリを使用する場合、アプリの2つのバージョンを展開するために個別のデリバリーグループが必要になることがあります。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に、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があります。

Appleボリューム購入を使用してiOSアプリケーションのライセンスを管理することもできます。このオプションでは、Appleボリューム購入に登録し、XenMobileコンソールでXenMobileボリューム購入設定を構成して、ボリューム購入ライセンスでアプリを配布する必要があります。このようなさまざまなユースケースがあるため、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。次の項目を定義することからMAM戦略の計画を開始できます。

アプリの種類: サポートする予定のさまざまな種類のアプリをリストアップし、分類します。例：パブリック、ネイティブ、モバイル生産性アプリ、Web、社内、ISVアプリなど。また、iOSやAndroidなどの異なるデバイスプラットフォーム向けにアプリを分類します。この分類は、各種類のアプリに必要なXenMobile設定を調整するのに役立ちます。たとえば、特定のアプリはラッピングの対象とならない場合や、他のアプリとの対話のために特別なAPIを有効にするためにMobile Apps SDKを必要とする場合があります。

ネットワーク要件: 特定のネットワークアクセス要件を持つアプリを、適切な設定で構成します。たとえば、特定のアプリはVPNを介して内部ネットワークへのアクセスを必要とする場合があります。一部のアプリは、DMZを介して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を必要とする場合があります。そのような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、それに応じてさまざまな設定を構成する必要があります。アプリごとのネットワーク要件を定義することは、アーキテクチャ上の決定を早期に確定するのに役立ち、全体的な実装プロセスを合理化します。

セキュリティ要件: 個々のアプリ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が重要です。その計画により、XenMobile Serverをインストールする際に適切な構成を作成できます。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、セッションおよび認証設定はすべてのアプリに適用されます。一部のアプリには、展開を簡素化するために事前に概説できる特定の暗号化、コンテナ化、ラッピング、暗号化、認証、ジオフェンシング、パスコード、またはデータ共有の要件がある場合があります。

展開要件: 公開されたアプリを準拠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したい場合があります。たとえば、特定のアプリで次のいずれかを要求したい場合があります。

- デバイスプラットフォームベースの暗号化が有効になっている
- デバイスが管理されている
- デバイスが最小オペレーティングシステムバージョンを満たしている
- 特定のアプリは企業ユーザーのみが利用できる

企業ユーザーのみが利用できる特定のアプリが必要な場合もあります。適切な展開ルールやアクションを設定できるよう、そのような要件を事前に明確にしてください。

ライセンス要件: アプリ関連のライセンス要件を記録しておきます。これらの記録は、ライセンスの使用状況を効果的に管理し、ライセンスを容易にするためにXenMobileで特定の機能を構成するかどうかを決定するのに役立ちます。たとえば、無料または有料のiOSアプリを展開する場合、AppleはユーザーにiTunesアカウントへのサインインを要求することで、アプリにライセンス要件を適用します。これらのアプリをXenMobile経由で配布および管理するには、Appleのボリューム購入に登録できます。ボリューム購入により、ユーザーは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ます。また、Samsung SAFEやSamsung Knoxなどのツールには特別なライセンス要件があり、これらの機能を展開する前に完了する必要があります。

許可リストとブロックリストの要件: ユーザーが一部のアプリをインストールしたり使用したりするのを防ぎたいと思うでしょう。デバイスを非準拠にするアプリの許可リストを作成します。次に、デバイスが非準拠になったときにトリガーされるポリシーを設定します。一方、あるアプリは使用が許容されるものの、何らかの理由でブロックリストに該当する場合があります。その場合、そのアプリを許可リストに追加し、使用は許容されるが必須ではないことを示すことができます。また、新しいデバイスにプリインストールされているアプリには、オペレーティングシステムの一部ではない一般的なアプリが含まれている場合があることにも注意してください。これらのアプリは、ブロックリスト戦略と競合する可能性があります。

アプリのユースケース

ある医療機関は、モバイルアプリのMAMソリューションとしてXenMobileを展開する予定です。モバイルアプリは、企業ユーザーとBYODユーザーに提供されます。IT部門は、以下のアプリを提供および管理することを決定しました。

- **モバイル生産性アプリ:** Citrixが提供するiOS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:** インターネットおよび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。
- **Citrix Files:** 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がXenMobileと通信するために使用するクライアント。IT部門は、Secure Hubクライアントを介して、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およびiOSデバイスは、Secure Hubを介してXenMobileに登録します。
- **Citrix Receiver™:** ユーザーがモバイルデバイスでVirtual Apps and Desktopsによってホストされているアプリケーションを開くことを可能にするモバイルアプリ。

- **GoToMeeting:** ユーザーがインターネットを介して他のコンピューターユーザー、顧客、クライアント、または同僚とリアルタイムで会議を行うことを可能にする、オンライン会議、デスクトップ共有、ビデオ会議クライアント。
- **Salesforce1:** Salesforce1は、ユーザーがモバイルデバイスからSalesforceにアクセスできるようにし、すべてのChatter、CRM、カスタムアプリ、およびビジネスプロセスを、あらゆるSalesforceユーザーにとって統一されたエクスペリエンスにまとめます。
- **RSA SecurID:** 2要素認証用のソフトウェアベースのトークン。
- **EpicCareアプリ:** これらのアプリは、医療従事者に患者のカルテ、患者リスト、スケジュール、メッセージングへの安全でポータブルなアクセスを提供します。
    - **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向けのモバイルアプリ
    - **Rover:** iPhoneおよびiPad向けのモバイルアプリ。

HDX: これらのアプリは、Citrix Virtual Apps™およびDesktopsを介して配信されます。

- **Epic Hyperspace:** 電子カルテ管理用のEpicクライアントアプリケーション。

ISV

- **Vocera:** HIPAA準拠のVoIPおよびメッセージングモバイルアプリで、iPhoneおよびAndroidスマートフォンを介して、いつでもどこでもVocera音声テクノロジーの利点を拡張します。

社内アプリ

- **HCMail:** 暗号化されたメッセージの作成、社内メールサーバーのアドレス帳の検索、および電子メールクライアントを使用して連絡先に暗号化されたメッセージを送信するのに役立つアプリ。

社内WEBアプリ

- **PatientRounding:** さまざまな部署が患者の健康情報を記録するために使用するWebアプリケーション。
- **Outlook Web Access:** Webブラウザを介した電子メールへのアクセスを可能にします。
- **SharePoint:** 組織全体のファイルおよびデータ共有に使用されます。

次の表に、MAM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ラッピング**	**iOS**	**アンドロイド**

セキュアメール	XenMobileアプリ	バージョン10.4.1以降はいいえ	はい	はい
セキュアウェブ	XenMobileアプリ	バージョン10.4.1以降はいいえ	はい	はい
シトリックス ファイルズ	XenMobile App	バージョン10.4.1以降ではいいえ	はい	はい
セキュア ハブ	公開アプリ	NA	はい	はい
シトリックス レシーバー	公開アプリ	NA	はい	はい
GoToMeeting	パブリックアプリ	NA	はい	はい
セールスフォース1	パブリックアプリ	NA	はい	はい
RSA SecurID	パブリックアプリ	NA	はい	はい
エピック ハイク	パブリックアプリ	NA	はい	はい
エピック カント	パブリックアプリ	NA	はい	いいえ
エピック ローバー	パブリックアプリ	NA	はい	いいえ
エピック ハイパースペース	HDX™ アプリ	該当なし	はい	はい
ボセラ	ISV アプリ	はい	はい	はい
エイチシーメール	社内アプリ	はい	はい	はい

PatientRounding	Webアプリ	N/A	はい	はい
アウトルック ウェブ アクセス	Webアプリ	N/A	はい	はい
SharePoint	Webアプリ	N/A	はい	はい

以下の表は、XenMobileでMAMポリシーを構成する際に参照できる特定の要件を示しています。

アプリ名	VPN必須	インタラクション	インタラクション	デバイスプラットフォームベースの暗号化
		(コンテナ外のアプリとの連携)	(コンテナ外のアプリから)	
セキュアメール	Y	選択的に許可	許可	不要
セキュアウェブ	Y	許可	許可	不要
シトリックス ファイルズ	Y	許可	許可	不要
セキュアハブ	Y	N/A	N/A	N/A
シトリックス レシーバー	Y	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
セールスフォース1	N	N/A	N/A	N/A
RSA SecurID	N	該当なし	該当なし	該当なし
エピック ハイク	Y	該当なし	該当なし	該当なし
エピック カント	Y	該当なし	該当なし	該当なし

XENMOBILE®サーバー

アプリ名	VPN必須	インタラクション	インタラクション	デバイスプラットフォームベースの暗号化
		(コンテナ外のアプリとの連携)	(コンテナ外のアプリから)	
エピック ローバー	Y	該当なし	該当なし	該当なし
エピック ハイパースペース	はい	該当なし	該当なし	該当なし
ボセラ	はい	ブロック済み	ブロック済み	不要
HCメール	はい	ブロック済み	ブロック済み	必須
PatientRounding	Y	N/A	N/A	必須
アウトルック ウェブ アクセス	Y	N/A	N/A	不要
SharePoint	Y	N/A	N/A	不要

アプリ名	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
セキュアメール	必須	N/A	選択的に必須	N/A	適用済み
セキュアウェブ	必須	N/A	不要	N/A	適用済み
シトリックス ファイル	必須	N/A	不要	N/A	適用済み
セキュアハブ	不要	ボリューム購入	不要	該当なし	適用されません

XENMOBILE®サーバー

アプリ名	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
シトリックス レシーバー	不要	ボリューム購入	不要	該当なし	適用されません
GoToMeeting	不要	ボリューム購入	不要	該当なし	適用されません
セールスフォース1	不要	ボリューム購入	不要	該当なし	適用されません
RSA SecurID	不要	ボリューム購入	不要	該当なし	適用されません
エピック ハイク	不要	ボリューム購入	不要	該当なし	適用されません
エピック カント	不要	ボリューム購入	不要	該当なし	適用されません
エピック ローバー	不要	ボリューム購入	不要	該当なし	適用されません
エピック ハイパースペース	不要	N/A	不要	N/A	強制なし
ボセラ	必須	N/A	必須	必須	強制
エイチシーメール	必須	N/A	必須	必須	適用済み
PatientRound-ing	必須	該当なし	不要	該当なし	適用なし
Outlook Web アクセス	必須	該当なし	不要	該当なし	適用なし
SharePoint	必須	N/A	不要	N/A	適用外

ユーザーコミュニティ

各組織は、さまざまな機能的役割を担う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じて提供されるさまざまなリソースを使用して、異なるタスクやオフィス機能を実行します。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遠隔地のオフィスで作業する場合があります。あるいは、ユーザーは個人のモバイルデバイスを使用する場合があります。これにより、特定のセキュリティコンプライアンス規則の対象となるツールにアクセスできます。

より多くのユーザーコミュニティがモバイルデバイスを使用するにつれて、データ漏洩を防ぎ、セキュリティ制限を適用するために、Enterprise Mobility Management (EMM) が不可欠になります。効率的でより高度なモバイルデバイス管理のために、ユーザーコミュニティを分類できます。そうすることで、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が適切なユーザーに適用されるようになります。

次の例は、医療機関のユーザーコミュニティがEMM向けにどのように分類されているかを示しています。

ユーザーコミュニティのユースケース

この医療機関の例では、ネットワークおよび関連会社の従業員やボランティアを含む複数のユーザーにテクノロジーリソースとアクセスを提供しています。この組織は、EMMソリューションを非管理職ユーザーにのみ展開することを選択しました。

この組織のユーザーの役割と機能は、臨床、非臨床、契約社員などのサブグループに分類できます。一部のユーザーは会社のモバイルデバイスを受け取り、他のユーザーは個人のデバイスから限られた会社の情報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適用し、データ漏洩を防ぐために、組織は、企業支給またはBYODのいずれであっても、登録された各デバイスを企業ITが管理することを決定しました。また、ユーザーは1つのデバイスしか登録できません。

次のセクションでは、各サブグループの役割と機能の概要を説明します。

臨床

- 看護師
- 医師 (内科医、外科医など)
- 専門医 (栄養士、麻酔科医、放射線科医、循環器科医、腫瘍科医など)
- 外部医師 (遠隔オフィスで勤務する非従業員の医師および事務員)
- 在宅医療サービス (患者宅への訪問診療を行う事務員およびモバイルワーカー)
- 研究専門家 (6つの研究機関で医学的問題の解決策を見つけるための臨床研究を行うナレッジワーカーおよびパワーユーザー)

- 教育および研修 (教育および研修に携わる看護師、医師、専門家)

非臨床

- 共有サービス (人事、給与、買掛金、サプライチェーンサービスなど、さまざまなバックオフィス業務を行う事務員)
- 医師サービス (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、マネージドケア管理、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、プロバイダーにさまざまな医療管理、管理サービス、およびビジネスプロセスソリューションを提供する事務員)
- サポートサービス (福利厚生管理、臨床統合、コミュニケーション、報酬および業績管理、施設および資産サービス、人事テクノロジーシステム、情報サービス、内部監査およびプロセス改善など、さまざまな非臨床業務を行う事務員)
- 慈善プログラム (慈善プログラムを支援するためにさまざまな業務を行う事務員およびモバイルワーカー)

請負業者

- 製造元およびベンダーパートナー (サイト間VPNを介してオンサイトおよびリモートで接続し、さまざまな非臨床サポート機能を提供)

上記の情報に基づいて、組織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) およびグループ

OU = XenMobile Resources の場合:

- OU = 臨床; グループ =
    - XM-看護師
    - XM-医師
    - XM-専門家
    - XM-外部医師
    - XM-在宅医療サービス
    - XM-研究専門家
    - XM-教育およびトレーニング
- OU = 非臨床; グループ =
    - XM-共有サービス

- XM-医師サービス
- XM-サポートサービス
- XM-慈善プログラム

XENMOBILE ローカルユーザーとグループ

グループ = 契約者、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

- 臨床 - 看護師
- 臨床 - 医師
- 臨床 - 専門家
- 臨床 - 外部医師
- 臨床 - 在宅医療サービス
- 臨床 - 研究専門家
- 臨床 - 教育および研修
- 非臨床 - 共有サービス
- 非臨床医師サービス
- 非臨床サポートサービス
- 非臨床慈善プログラム

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	臨床看護師
XM-医師	臨床医師
XM-専門医	臨床専門医
XM-外部医師	臨床外部医師

XM-在宅医療サービス	臨床 - 在宅医療サービス
XM - 研究スペシャリスト	臨床 - 研究スペシャリスト
XM - 教育およびトレーニング	臨床 - 教育およびトレーニング
XM - 共有サービス	非臨床 - 共有サービス
XM - 医師サービス	非臨床 - 医師サービス
XM - サポートサービス	非臨床 - サポートサービス
XM - 慈善プログラム	非臨床 - 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、このユースケースで各デリバリーグループに割り当てられている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、2番目の表はパブリックアプリ、HDXアプリ、および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**
臨床 - 看護師	X		
臨床 - 医師			
臨床 - 専門医			
臨床 - 外部医師	X		
臨床 - 在宅医療サービス	X		
臨床 - 研究専門家	X		
臨床 - 教育およびトレーニング		X	X
非臨床 - 共有サービス		X	X

非臨床 - 医師サービス		X	X
非臨床 - サポートサービス	X	X	X
非臨床 - 慈善プログラム	X	X	X
契約社員	X	X	X

XenMobile デリバリーグループ	**公開アプリ: RSA SecurID**	**公開アプリ: EpicCare Haiku**	**HDX アプリ: Epic Hyperspace**	**パスコードポリシー**	**デバイス制限**	**自動アクション**	**Wi-Fi ポリシー**
臨床看護師							X
臨床 - 医師					X		
臨床 - 専門医							
臨床 - 外部医師							
臨床 - 在宅医療サービス							
臨床 - 研究専門家							

臨床 - 教育および研修		X	X				
非臨床 - 共有サービス		X	X				
非臨床 - 医師サービス		X	X				
非臨床サポートサービス		X	X				

注意事項と考慮事項

- XenMobileは、初期設定時に「All Users」という名前の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場合、すべてのActive Directoryユーザーは XenMobileに登録する権利を持ちます。
- XenMobileは、LDAPサーバーへの動的接続を使用して、Active Directory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にマッピング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はそのユーザーをXenMobileにマッピングされたグループにのみ分類します。
- MDM登録を必須にするには、XenMobileコンソールのサーバープロパティで「登録必須」オプションをTrueに設定する必要があります。詳細については、「サーバープロパティ」を参照してください。
- SQL Serverデータベースのdbo.userlistgrpsにあるエントリを削除することで、XenMobileデリバリーグループからユーザーグループを削除できます。 **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におけるデバイスの所有権について

ユーザーのデバイスの所有者に基づい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、企業所有デバイスと、個人所有デバイス (BYOD) としても知られるユーザー所有デバイスが含まれます。BYODデバイスがネットワークに接続する方法は、XenMobileコンソールの2つの場所で制御できます。各リソースタイプの展開ルールと、**設定**ページのサーバープロパティです。展開ルールの詳細については、XenMobileドキュメントの「展開ルールの構成」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、「サーバープロパティ」を参照してください。

すべてのBYODユーザーに、アプリにアクセスする前にデバイスの企業管理を受け入れるよう要求できます。または、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を許可することもできます。

サーバー設定 **wsapi.mdm.required.flag** を **true** に設定すると、XenMobileはすべての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を拒否されます。企業ITチームが、XenMobileにユーザーデバイスを登録する際に、高いセキュリティと良好な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 をデフォルト設定である **false** のままにすると、ユーザーは登録を拒否できますが、XenMobile Storeを通じてデバイス上のアプリにアクセスできる場合があります。プライバシー、法的、または規制上の制約により、デバイス管理は不要で、企業アプリ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を通じてアプリをインストールできます。選択的ワイプや完全ワイプなどのデバイスレベルの制御ではなく、アプリポリシーを通じてアプリへのアクセスを制御します。設定した値に応じて、ポリシーはデバイスが定期的にXenMobileサーバーをチェックし、アプリが引き続き実行を許可されていることを確認するよう要求します。

セキュリティ要件

XenMobile環境を展開する際のセキュリティに関する考慮事項は、すぐに圧倒されるほど多くなります。多くの相互に関連する要素と設定があります。Citrixは、開始を支援し、許容可能な保護レベルを選択するために、次の表に示すように、高、より高、最高のセキュリティに関する推奨事項を提供しています。

展開モードの選択は、セキュリティ上の懸念だけではありません。ユースケースの要件も確認し、展開モードを選択する前にセキュリティ上の懸念を軽減できるかどうかを判断することが重要です。

高: これらの設定を使用すると、ほとんどの組織で許容される基本的なセキュリティレベルを維持しながら、最適なユーザーエクスペリエンスが提供されます。

より高: これらの設定は、セキュリティとユーザビリティのより強力なバランスを生み出します。

最高: これらの推奨事項に従うと、ユーザビリティとユーザーの採用を犠牲にして、高いレベルのセキュリティが提供されます。

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またはMDM	MDM+MAM	MDM+MAM; およびFIPS

注記:

- ユースケースに応じて、MDMのみまたはMAMのみ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、MDMはデバイスの管理と保護に十分です。
- アプリのコンテナ化だけでビジネスおよびセキュリティ要件をすべて満たせるBYODのようなユースケースでは、CitrixはMAMのみのモードを推奨します。
- 高セキュリティ環境（および企業支給デバイス）の場合、Citrixは利用可能なすべてのセキュリティ機能を活用するためにMDM+MAMを推奨します。MDM登録を必ず適用してください。
- 連邦政府など、最高のセキュリティニーズを持つ環境向けのFIPSオプション。

FIPSモードを有効にする場合、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。

Citrix ADCおよびCitrix 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におけるCitrix ADCおよびCitrix 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**
Citrix ADCを推奨します。Citrix GatewayはMAMおよび	XenMobileがDMZにある場合は、SSLブリッジを使用した	エンドツーエンド暗号化によるSSLオフロード

ENTに必須であり、MDMに推奨されます。	XenMobileウィザード構成用の標準Citrix ADC。または、XenMobile Serverが内部ネットワークにある場合にセキュリティ標準を満たすために必要な場合は、SSLオフロード。	

注：

- XenMobile ServerをNATまたは既存のサードパーティ製プロキシおよびロードバランサーを介してインターネットに公開することは、MDMのオプションとなり得ます。ただし、この設定ではSSLトラフィックがXenMobile Serverで終端される必要があり、潜在的なセキュリティリスクをもたらします。
- 高セキュリティ環境では、デフォルトのXenMobile構成のCitrix ADCは通常、セキュリティ要件を満たすか、それを上回ります。
- 最高のセキュリティニーズを持つMDM環境では、Citrix ADCでのSSL終端により、境界でのトラフィック検査が可能になり、エンドツーエンドのSSL暗号化が維持されます。
- SSL/TLS暗号を定義するオプション。
- SSL FIPS Citrix ADCハードウェアも利用可能です。
- 詳細については、「Citrix GatewayおよびCitrix ADCとの統合」を参照してください。

登録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におけるCitrix ADCおよびCitrix 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。すべてのユーザーのデリバリーグループは無効。	招待制の登録セキュリティモード。Active Directoryグループメンバーシップのみ。すべてのユーザーのデリバリーグループは無効。	デバイスIDに紐付けられた登録セキュリティモード。Active Directoryグループメンバーシップのみ。すべてのユーザーのデリバリーグループは無効。

注：

- Citrix は、登録を事前定義された Active Directory グループのユーザーのみに制限することを一般的に推奨しています。この設定では、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。
- 登録招待を使用して、招待されたユーザーのみに登録を制限できます。登録招待は Windows デバイスでは利用できません。
- ワンタイムPIN (OTP) 登録招待を二要素認証ソリューションとして使用し、ユーザーが登録できるデバイスの数を制御できます。OTP招待は Windows デバイスでは利用できません。

デバイスパスコ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におけるデバイスパスコード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**	**最高セキュリティ**
推奨。デバイスレベルの暗号化には高セキュリティが必要です。MDMを使用して適用されます。MDXポリシー「非準拠デバイスの動作」を使用して、MAM専用として高セキュリティを必須に設定できます。	MDM、MDXポリシー、またはその両方を使用して適用されます。	MDMと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:

- Citrix はデバイスパスコードの使用を推奨しています。
- MDMポリシーを介してデバイスパスコードを適用できます。
- MDXポリシーを使用して、管理対象アプリを使用するためのデバイスパスコードを必須にすることができます。たとえば、BYODのユースケースなどです。
- Citrixは、MDM+MAM環境におけるセキュリティ強化のため、MDMおよびMDXポリシーオプションを組み合わせることを推奨します。
- 最高のセキュリティ要件を持つ環境では、複雑なパスコードポリシーを設定し、MDMでそれらを強制できます。デバイスがパスコードポリシーに準拠しない場合、管理者に通知したり、デバイスの選択的/完全ワイプを実行したりする自動アクションを設定できます。

アプリ

エンタープライズモビリティ管理 (EMM) は、モバイルデバイス管理 (MDM) とモバイルアプリケーション管理 (MAM) に分かれます。MDM は組織がモバイルデバイスを保護および制御できるようにする一方、MAM はアプリケーションの配信と管理を容易にします。BYOD の導入をサポートするために、XenMobile® のような MAM ソリューションを実装して、次のことを支援できます。

- 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

ユーザーに MDM 管理へのオプトインを要求または許可することもできます。

XenMobile を使用すると、特定の MAM ポリシーと VPN 設定を構成して、データ漏洩やその他のセキュリティ脅威を防ぐことで、これらのアプリをさらに保護できます。XenMobile は、組織がソリューションを次のように展開するための柔軟性を提供します。

- MAM 専用環境
- MDM 専用環境
- MDM と MAM の両方の機能を提供する統合 XenMobile Enterprise 環境

モバイルデバイスにアプリを配信する機能に加えて、XenMobile は MDX テクノロジーを介したアプリのコンテナ化を提供します。アプリは、きめ細かなポリシーベースの制御の対象となります。独立系ソフトウェアベンダー (ISV) は、Mobile Apps SDK を使用してこれらの制御を適用できます。

企業環境では、ユーザーは職務を支援するためにさまざまなモバイルアプリを使用します。アプリには、パブリックアプリストアのアプリ、社内で開発されたアプリ、またはネイティブアプリが含まれます。XenMobile はこれらのアプリを次のように分類します。

- **パブリックアプリ:** これらのアプリには、Apple App Store や Google Play などのパブリックアプリストアで入手できる無料または有料のアプリが含まれます。組織外のベンダーは、多くの場合、パブリックアプリストアでアプリを提供しています。このオプションにより、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応じて、組織内で多数のパブリックアプリを使用する場合があります。このようなアプリの例には、GoToMeeting、Salesforce、EpicCare アプリなどがあります。

  - **MAM SDK を使用する場合:** アプリベンダーからアプリバイナリを入手します。次に、MAM SDK をアプリに統合します。
  - **MDX Toolkitを使用する場合:** Citrix®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し、それをMDX Toolkitでラップしてエンタープライズ配布することをサポートしていません。サードパーティ製アプリケーションをラップするには、アプリベンダーと協力してアプリバイナリを入手してください。その後、MDX Toolkitを使用してバイナリをラップできます。

- **社内アプリ:** 多くの組織には、特定の機能を提供し、組織内で独自に開発および配布されるアプリを作成する社内開発者がいます。特定のケースでは、一部の組織はISVが提供するアプリも持っている場合があります。そのようなアプリはネイティブアプリとして展開することも、XenMobileなどのMAMソリューションを使用してアプリをコンテナ化することもできます。

  たとえば、医療機関は、医師がモバイルデバイスで患者情報を表示できる社内アプリを作成する場合があります。組織は、次のいずれかを使用して、患者情報を保護し、患者データベースへのVPNアクセスを有効にできます。

  - MAM SDK
  - MDXツールキット

- **Webアプリと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。XenMobileでは、アプリコネクタのリストを使用してカスタムのWebアプリと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は、既存のWebアプリへのシングルサインオン（SSO）を容易にします。詳細については、「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へのSecurity Assertion Markup Language (SAML) に基づくSSOにGoogle Apps SAMLを使用できます。
- **モバイル生産性アプリ:** モバイル生産性アプリは、XenMobileライセンスに含まれるCitrix開発のアプリです。詳細については、「モバイル生産性アプリについて」を参照してください。Citrixは、ISVがMobile Apps SDKを使用して開発するその他のビジネス対応アプリも提供しています。
- **HDXアプリ:** HDXアプリは、StoreFrontで公開するWindowsホスト型アプリです。Citrix Virtual Apps and Desktops™とCitrix Workspace™を使用している場合、HDXアプリは登録ユーザーが利用できます。

XenMobileで展開および管理するモバイルアプリの種類に応じて、基になる構成が異なる場合があります。たとえば、異なるレベルの権限を持つ複数のユーザーグループが1つのアプリを使用する場合があります。その場合、同じアプリの2つの異なるバージョンを展開するために、個別のデリ

バリーグループを作成できます。さらに、ユーザーのデバイスでのポリシーの不一致を避けるために、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があります。

Appleボリューム購入を使用してiOSアプリケーションのライセンスを管理することもできます。このオプションでは、ボリューム購入プログラムに登録し、XenMobileコンソールでボリューム購入設定を構成する必要があります。この構成により、ボリューム購入ライセンスでアプリを配布できます。さまざまなユースケースがあるため、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。次の項目を定義することで、MAM戦略の計画を開始できます。

- **Types of apps:** List the different types of apps that you plan to support and categorize them, such as public, native, Web, in-house, or ISV apps. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization helps with aligning the various XenMobile settings that are required for each type of app. For example, a few apps might require use of the Mobile Apps SDK to enable special APIs for interaction with other apps.
- **Network requirements:** Configure the settings of apps that have specific network access requirements. For example, certain apps might need access to your internal network through the VPN. Some apps might require Internet access to route access via the DMZ. To allow such apps to connect to the required network, you must configure various settings accordingly. Defining per-app network requirements help in finalizing your architectural decisions early on, which streamlines the overall implementation process.
- **セキュリティ要件:** 個々のアプリまたはすべてのアプリに適用するセキュリティ要件を定義できます。

  - Settings, such as the MDX policies, apply to individual apps
  - セッションおよび認証設定は、すべてのアプリに適用されます。
  - 一部のアプリには、特定のコンテナ化、MDX、認証、ジオフェンシング、パスコード、またはデータ共有の要件がある場合があります。

  展開を簡素化するために、これらの要件を事前に概説してください。Endpoint Management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。
- **展開要件** - 準拠しているユーザーのみが公開されたアプリを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したい場合があります。たとえば、特定のアプリでは、デバイスが管理されていること、またはデバイスが最小オペレーティングシステムバージョンを満たしていることが必要になる場合があります。また、特定のアプリを企業ユーザーのみが利用できるようにしたい場合もあります。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、このような要件を事前に概説してください。

- **ライセンス要件:** アプリ関連のライセンス要件を記録しておいてください。メモは、ライセンスの使用状況を効果的に管理し、ライセンスを容易にするためにXenMobileで特定の機能を構成するかどうかを決定するのに役立ちます。たとえば、無料または有料のiOSアプリを展開する場合、Appleはそのアプリにライセンス要件を適用します。その結果、ユーザーはApple App Storeアカウントにサインインする必要があります。

  ただし、Appleボリューム購入に登録することで、XenMobileを使用してこれらのアプリを配布および管理できます。ボリューム購入により、ユーザーはApple App Store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ます。

  Samsung SAFEやSamsung Knoxなどの一部のプラットフォームでは、これらの機能を展開する前に完了する必要がある特別なライセンス要件があります。

- **許可リストとブロックリストの要件:** ユーザーにインストールまたは使用させたくないアプリを特定する場合があります。ブロ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が定義されます。その後、イベントが発生したときにトリガーされるポリシーを設定できます。一方、アプリは使用が許容されるものの、何らかの理由でブロックリストに該当する場合があります。その場合、アプリを許可リストに追加し、そのアプリは使用が許容されるが必須ではないことを示すことができます。また、新しいデバイスにプリインストールされているアプリには、オペレーティングシステムの一部ではない一般的なアプリが含まれている場合があることに注意してください。このようなアプリは、ブロックリスト戦略と競合する可能性があります。

ユースケース

ある医療機関は、モバイルアプリのMAMソリューションとしてXenMobileを展開する予定です。モバイルアプリは、企業ユーザーとBYODユーザーに提供されます。IT部門は、以下のアプリを提供および管理することを決定しました。

モバイル生産性アプリ: Citrixが提供するiOSおよびAndroidアプリ。詳細については、「モバイル生産性アプリ」を参照してください。

Citrix Secure Hub™: すべてのモバイルデバイスがXenMobileと通信するために使用するクライアント。Secure Hubを使用して、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およびiOSデバイスは、Secure Hubを介してXenMobileに登録します。

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を可能にするモバイルアプリ。

GoToMeeting: オンライン会議、デスクトップ共有、ビデオ会議クライアントであり、ユーザーがインターネットを介して他のコンピューターユーザー、顧客、クライアント、または同僚とリアルタイムで会議を行うことができます。

SalesForce1: Salesforce1は、ユーザーがモバイルデバイスからSalesforceにアクセスできるようにし、すべてのChatter、CRM、カスタムアプリ、およびビジネスプロセスを、あらゆるSalesforceユーザーにとって統一されたエクスペリエンスにまとめます。

RSA SecurID: 2要素認証用のソフトウェアベースのトークン。

EpicCareアプリ: これらのアプリは、医療従事者に患者のカルテ、患者リスト、スケジュール、メッセージングへの安全でポータブルなアクセスを提供します。

Haiku: iPhoneおよびAndroidフォン向けのモバイルアプリ。

Canto: iPad向けのモバイルアプリ。

Rover: iPhoneおよびiPad向けのモバイルアプリ。

HDX™: Citrix Virtual AppsはHDXアプリを提供します。

- **Epic Hyperspace:** 電子カルテ管理用のEpicクライアントアプリケーション。

ISV:

- **Vocera:** HIPAA準拠のボイスオーバーIPおよびメッセージングモバイルアプリで、iPhoneおよびAndroidスマートフォンを介して、いつでもどこでもVocera音声テクノロジーの利点を拡張します。

社内アプリ:

- **HCMail:** 暗号化されたメッセージを作成し、社内メールサーバーのアドレス帳を検索し、電子メールクライアントを使用して暗号化されたメッセージを連絡先に送信するのに役立つアプリ。

社内Webアプリ:

- **PatientRounding:** さまざまな部門が患者の健康情報を記録するために使用するWebアプリケーション。
- **Outlook Web Access:** Webブラウザを介した電子メールへのアクセスを可能にします。
- **SharePoint:** 組織全体のファイルおよびデータ共有に使用されます。

次の表に、MAM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	MAM SDK統合またはMDXラッピング	iOS	アンドロイド
セキュアメール	XenMobileアプリ	バージョン10.4.1以降は不要	はい	はい
セキュアウェブ	XenMobileアプリ	バージョン10.4.1以降は不要	はい	はい
シトリックスファイル	XenMobileアプリ	バージョン10.4.1以降はいいえ	はい	はい
セキュア ハブ	公開アプリ	該当なし	はい	はい
シトリックス レシーバー	公開アプリ	該当なし	はい	はい
GoToMeeting	公開アプリ	N/A	はい	はい
SalesForce1	公開アプリ	N/A	はい	はい
RSA SecurID	公開アプリ	N/A	はい	はい
エピック ハイク	パブリックアプリ	N/A	はい	はい
エピック カント	パブリックアプリ	N/A	はい	いいえ
エピック ローバー	パブリックアプリ	N/A	はい	いいえ
エピック ハイパースペース	HDXアプリ	該当なし	はい	はい
ボセラ	ISVアプリ	はい	はい	はい
エイチシーメール	社内アプリ	はい	はい	はい

PatientRounding	Webアプリ	該当なし	はい	はい
Outlook Web アクセス	Webアプリ	該当なし	はい	はい
SharePoint	Webアプリ	該当なし	はい	はい

以下の表に、XenMobileでMAMポリシーを設定する際に参照できる特定の要件を記載しています。

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
セキュアメール	はい	選択的に許可	許可	必須	N/A	選択的に必須	N/A	強制
セキュアウェブ	Y	許可	許可	必須	N/A	不要	N/A	強制
シトリックスファイル	Y	許可	許可	必須	該当なし	不要	該当なし	適用済み
セキュアハブ	Y	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	適用されません
シトリックス レシーバー	Y	N/A	N/A	不要	ボリューム購入	不要	N/A	適用されません

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
GoTo Meeting	N	N/A	N/A	不要	ボリューム購入	不要	該当なし	適用されません
Sales Force 1	N	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	適用されません
RSA SecurID	N	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	強制されない
エピック ハイク	はい	該当なし	該当なし	不要	ボリューム購入	不要	該当なし	適用されません
エピック カント	Y	N/A	N/A	不要	ボリューム購入	不要	N/A	適用されません
エピック ローバー	Y	N/A	N/A	不要	ボリューム購入	不要	N/A	適用されません
エピック ハイパースペース	Y	N/A	N/A	不要	N/A	不要	N/A	適用されません
ボセーラ	Y	ブロック済み	ブロック済み	必須	該当なし	必須	必須	強制

アプリ名	VPNが必要	相互作用 (コンテナ外のアプリとの)	相互作用 (コンテナ外のアプリからの)	プロキシフィルタリング	ライセンス	ジオフェンシング	モバイルアプリSDK	最小オペレーティングシステムバージョン
エイチシーメール	Y	ブロック済み	ブロック済み	必須	該当なし	必須	必須	強制
患者回診	Y	N/A	N/A	必須	N/A	不要	N/A	強制なし
アウトルックウェブアクセス	Y	N/A	N/A	必須	N/A	不要	N/A	適用されません
SharePoint	はい	N/A	N/A	必須	N/A	不要	N/A	適用されません

ユーザーコミュニティ

すべての組織は、さまざまな機能的役割で活動する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介して提供されるさまざまなリソースを使用して、さまざまなタスクやオフィス機能を実行します。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ことも、個人用モバイルデバイスを使用して、特定のセキュリティコンプライアンス規則に従うツールにアクセスすることもできます。

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て、データ漏洩を防ぎ、組織のセキュリティ制限を適用するために、エンタープライズモビリティ管理 (EMM) が重要になります。効率的でより高度なモバイルデバイス管理のために、ユーザーコミュニティを分類できます。そうすることで、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が適切なユーザーに適用されるようになります。

ユーザーコミュニティの分類には、以下のコンポーネントの使用が含まれます。

- Active Directory組織単位 (OU) およびグループ

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、ポリシーや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、以前に許可されていたXenMobile®リソースへのアクセスが削除されます。

- XenMobileローカルユーザーおよびグループ

  Active Directoryにアカウントを持たないユーザーの場合、ローカルXenMobileユーザーとして作成できます。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

  異なるレベルの権限を持つ複数のユーザーグループが単一のアプリを使用する場合、個別のデリバリーグループを作成する必要があるかもしれません。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からActive Directoryグループへのマッピングは、1対1または1対多のいずれかになります。1対多のデリバリーグループマッピングには、基本ポリシーとアプリを割り当てます。1対1のデリバリーグループマッピングには、機能固有のポリシーとアプリを割り当てます。

- アプリのデリバリーグループとリソースのマッピング

  各デリバリーグループに特定のアプリを割り当てます。

- 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

  各デリバリーグループにアプリと特定のデバイス管理リソースを割り当てます。たとえば、デリバリーグループを次の任意の組み合わせで構成します。アプリの種類（パブリック、HDX™など）、アプリの種類ごとの特定のアプリ、およびデバイスポリシーや自動アクションなどのリソース。

次の例は、医療機関のユーザーコミュニティがEMM向けにどのように分類されているかを示しています。

ユースケース

この医療機関の例では、ネットワークおよび関連会社の従業員やボランティアを含む複数のユーザーにテクノロジーリソースとアクセスを提供しています。この組織は、EMMソリューションを非役員ユーザーのみに展開することを選択しました。

この組織のユーザーの役割と機能は、臨床、非臨床、契約社員などのサブグループに分けることができます。一部のユーザーは会社のモバイルデバイスを受け取り、他のユーザーは個人のデバイ

ス（BYOD）から限られた会社の情報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適用し、データ漏洩を防ぐため、組織は登録された各デバイスを企業ITが管理することを決定しました。また、ユーザーは1台のデバイスしか登録できません。

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を説明します。

臨床

- 看護師
- 医師（内科医、外科医など）
- 専門家（栄養士、採血技師、麻酔科医、放射線科医、心臓病専門医、腫瘍専門医など）
- 外部医師（遠隔地のオフィスで働く非従業員の医師および事務員）
- 在宅医療サービス（患者宅への訪問診療を行う事務員およびモバイルワーカー）
- 研究専門家（医学の問題に対する答えを見つけるために臨床研究を行う6つの研究機関のナレッジワーカーおよびパワーユーザー）
- 教育および研修（教育および研修に携わる看護師、医師、専門家）

非臨床

- 共有サービス（人事、給与、買掛金、サプライチェーンサービスなど、さまざまなバックオフィス業務を行うオフィスワーカー）
- 医師サービス（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、マネージドケア管理、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、プロバイダーに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、臨床統合、コミュニケーション、報酬およびパフォーマンス管理、施設および不動産サービス、人事テクノロジーシステム、情報サービス、内部監査およびプロセス改善など、さまざまな非臨床業務を行うオフィスワーカー）
- 慈善プログラム（慈善プログラムを支援するさまざまな業務を行うオフィスワーカーおよびモバイルワーカー）

請負業者

- 製造元およびベンダーパートナー（サイト間VPNを介してオンサイトおよびリモートで接続し、さまざまな非臨床サポート機能を提供）

上記の情報に基づき、組織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 = 臨床; グループ =
    - XM-看護師
    - XM-医師
    - XM-専門医
    - XM-外部医師
    - XM-在宅医療サービス
    - XM-研究スペシャリスト
    - XM-教育およびトレーニング
- OU = 非臨床; グループ =
    - XM-共有サービス
    - XM-医師サービス
    - XM-サポートサービス
    - XM-慈善プログラム

XenMobileローカルユーザーおよびグループ

グループ=請負業者、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

- 臨床-看護師
- 臨床 - 医師
- 臨床 - 専門医
- 臨床 - 外部医師
- 臨床 - 在宅医療サービス
- 臨床 - 研究専門家

- 臨床 - 教育およびトレーニング
- 非臨床 - 共有サービス
- 非臨床 - 医師サービス
- 非臨床 - サポートサービス
- 非臨床 - 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	臨床 - 看護師
XM-医師	臨床-医師
XM-専門家	臨床-専門家
XM-外部医師	臨床-外部医師
XM-在宅医療サービス	臨床-在宅医療サービス
XM-研究専門家	臨床-研究専門家
XM-教育および研修	臨床-教育および研修
XM-共有サービス	非臨床-共有サービス
XM-医師サービス	非臨床医師サービス
XM-サポートサービス	非臨床サポートサービス
XM-慈善プログラム	非臨床慈善プログラム

デリバリーグループとアプリのリソースマッピング

	セキュアメール	**セキュアウェブ**	**ShareFile**	**レシーバー**	**SalesForce 1**	**RSA SecurID**	**エピックケアハイク**	**エピック ハイパースペース**

臨床看護師	X	X	X					
臨床医								
臨床専門医								
臨床-外部医師	X		X					
臨床-在宅医療サービス	X		X					
臨床-研究専門家	X		X					
臨床-教育およびトレーニング							X	X
非臨床 - 共有サービス							X	X
非臨床 - 医師サービス							X	X
非臨床 - サポートサービス	X		X				X	X

非臨床 - 慈善プログラム	X		X				X	X
契約社員	X		X	X	X		X	X

デリバリーグループとMDMリソースのリソースマッピング

	MDM: パスコードポリシー	**MDM: デバイス制限**	**MDM: 自動アクション**	**MDM: Wi-Fiポリシー**
臨床 - 看護師				X
臨床 - 医師		X		
臨床 - 専門医				
臨床 - 外部医師				
臨床 - 在宅医療サービス				
臨床 - 研究専門家				
臨床 - 教育および研修				
非臨床 - 共有サービス				
非臨床 - 医師サービス				
非臨床 - サポートサービス				
非臨床 - 慈善プログラム				

契約者				X

注意事項

- XenMobileは、初期構成時に「All Users」という名前の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場合、すべてのActive DirectoryユーザーはXenMobileに登録する権利を持ちます。
- XenMobileは、LDAPサーバーへの動的接続を使用して、Active Directory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にマッピング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、XenMobileにマッピングされているグループにのみユーザーを分類します。
- MDM登録を必須にするには、XenMobileコンソールの**でオプションを**に設定します。詳細については、「Server Properties」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、SQL Serverデータベースのdbo.userlistgrpsにあるエントリを削除します。

> **注意:**
>
> この操作を行う前に、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における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基づい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、企業所有デバイスとユーザー所有デバイス（BYODとしても知られる）が含まれます。BYODデバイスがネットワークに接続する方法は、XenMobileコンソールの2つの場所で制御できます。展開規則と、****ページのXenMobile Serverプロパティです。展開規則の詳細については、XenMobileドキュメントの「Deploy resources」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「Server Properties」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、アプリにアクセスする前にデバイスの企業管理を受け入れるよう要求できます。または、デバイスを管理せずに企業アプリへのアクセスをユーザーに許可することもできます。

wsapi.mdm.required.flagサーバープロパティを**true**に設定すると、XenMobileはすべての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を拒否されます。エンタープラ

イズITチームが高いセキュリティと登録中の良好な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。

デフォルト設定である**wsapi.mdm.required.flag**を**false**のままにすると、ユーザーは登録を拒否できます。ただし、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、法的、または規制上の制約により、デバイス管理ではなくエンタープライズアプリ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を通じてアプリをインストールできます。選択的ワイプや完全ワイプなどのデバイスレベルの制御の代わりに、アプリポリシーを通じ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、アプリが引き続き実行を許可されていることを確認するために、デバイスが定期的にXenMobile Serverをチェックする必要があります。

メール戦略

モバイルデバイスからのメールへのセキュアなアクセスは、あらゆる組織のモビリティ管理イニシアチブの主要な推進要因の1つです。適切なメール戦略を決定することは、XenMobile®の設計において重要な要素となることがよくあります。XenMobileは、セキュリティ、ユーザーエクスペリエンス、統合要件に基づいて、さまざまなユースケースに対応するためのいくつかのオプションを提供します。この記事では、クライアントの選択からメールトラフィックフローまで、適切なソリューションを選択するための一般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

クライアントの選択は、通常、全体的なメール戦略設計において最優先事項です。Citrix Secure Mail™、特定のモバイルプラットフォームオペレーティングシステムに付属するネイティブメール、または公開アプリストアを通じて利用可能なその他のサードパーティクライアントなど、いくつかのクライアントから選択できます。ニーズに応じて、単一の（標準）クライアントでユーザーコミュニティをサポートすることも、複数のクライアントを組み合わせて使用する必要がある場合もあります。

以下の表は、利用可能なさまざまなクライアントオプションに関する設計上の考慮事項をまとめたものです。

トピック	**セキュアメール**	**ネイティブ (例: iOS メール)**	**サードパーティメール**
最小XenMobileエディション	高度な	MDM	MDM

構成	MDXポリシーを介して構成されたExchangeアカウントプロファイル。	MDMポリシーを介して構成されたExchangeアカウントプロファイル。Androidのサポートは、SAFE/KNOXおよびAndroid Enterpriseに限定されます。その他のすべてのクライアントはサードパーティクライアントと見なされます。	通常、ユーザーによる手動設定が必要です。
セキュリティ	設計上安全で、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追加されたMDXポリシーを使用します。Secure Mailは、MDXポリシーを介して完全に管理されるアプリです。Citrix PINによる認証レイヤーが追加されています。	ベンダー/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にはデバイスレベルの認証に依存します。	ベンダー/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）アプリとの連携を許可します。Citrix Secure WebでWeb URLを開きます。Citrix Filesにファイルを保存したり、Citrix Filesからファイルを添付したりできます。GoToMeetingに直接参加したり、ダイヤルインしたりできます。	デフォルトでは、他の非管理対象（非MDX）アプリとのみ連携できます。	デフォルトでは、他の非管理対象（非MDX）アプリとのみ連携できます。

展開/ライセンス	MDMを介して、または公開アプリストアから直接Secure Mailをプッシュできます。XenMobile AdvancedおよびEnterpriseライセンスに含まれています。	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クライアントアプリ。追加のライセンス要件はありません。	MDMを介して、エンタープライズアプリとして、または公開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く関連ライセンスモデル/費用。
サポート	クライアントとEMMソリューション（Citrix）に対する単一ベンダーサポート。Secure Hub/アプリのデバッグログ機能に埋め込まれたサポート連絡先情報。サポートするクライアントは1つ。	ベンダー定義のサポート（Apple/Google）。デバイス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。	ベンダー定義のサポート。サードパーティ製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と仮定した場合、サポートするクライアントは1つ。

メール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

このセクションでは、XenMobileにおけるメール（ActiveSync）トラフィックのフローに関する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：公開された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公開されています。モバイルActiveSyncクライアントは、リバースプロキシ（Citrix ADCなど）またはエッジサーバーを介して、この外部に面したパス経由で接続します。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ために必要であり、これらのクライアントがこのシナリオで一般的な選択肢となっています。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。そうすることで、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恩恵を受けることができます。

シナリオ2：Citrix ADC経由のトンネル（マイクロVPNおよびSTA）

このシナリオは、Secure Mailクライアントのマイクロ VPN機能により、Secure Mailクライアントを使用する場合のデフォルトです。この場合、Secure MailクライアントはCitrix Gatewayを介してActiveSyncへのセキュアな接続を確立します。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見なすことができます。Citrixのお客様は、モバイルActiveSyncクライアントとしてSecure Mailを標準化することがよくあります。この決定は、最初のシナリオで説明したように、公開されたExchange Server上でActiveSyncサービスをインターネットに公開することを避けるための取り組みの一部です。

MAM SDKが有効になっているアプリ、またはMDXでラップされたアプリのみがマイクロVPN機能を使用できます。MDXラッピングを使用する場合、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製クライアントをラップすることは可能かもしれませんが、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製クライアントのトンネル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証明されています。

シナリオ3：クラウドホスト型Exchangeサービス

Microsoft Office 365などのクラウドホスト型Exchangeサービスは、ますます普及しています。XenMobileのコンテキストでは、ActiveSyncサービスもインターネットに公開されているため、このシナリオは最初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肢が決まります。選択肢には通常、Secure Mailやその他のネイティブまたはサードパーティ製クライアントなど、ほとんどのActiveSyncクライアントのサポートが含まれます。

このシナリオにおいて、XenMobileは次の3つの領域で価値を付加できます。

- MDXポリシーとSecure Mailによるアプリ管理を備えたクライアント
- サポートされているネイティブメールクライアントでのMDMポリシーを使用したクライアント構成
- Endpoint Management connector for Exchange ActiveSync を使用した ActiveSync フィルタリングオプション

メールトラフィックフィルタリングに関する考慮事項

ほとんどのインターネットに公開されているサービスと同様に、パスを保護し、認証されたアクセスに対してフィルタリング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およびサードパーティクライアントに ActiveSync 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が含まれています。Citrix Gateway connector™ for Exchange ActiveSync と Endpoint Management connector for Exchange ActiveSync です。

Citrix Gateway 用 Exchange ActiveSync コネクタ

Citrix Gateway connector for Exchange ActiveSync は、ActiveSync トラフィックのプロキシとして Citrix ADC 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に配置され、メールが環境に出入りする際に傍受します。Citrix Gateway connector for Exchange ActiveSync は、Citrix ADC と XenMobile Server の間の仲介役として機能します。デバイスが Citrix ADC 上の ActiveSync 仮想サーバーを介して Exchange と通信すると、Citrix ADC は Exchange ActiveSync サービス用のコネクタに HTTP コールアウトを実行します。その後、そのサービスは XenMobile でデバイスの状態を確認します。デバイスの状態に基づいて、Exchange ActiveSync 用コネクタは Citrix ADC に接続を許可または拒否するよう応答します。ユーザー、エージェント、デバイスの種類または ID に基づいてアクセスをフィルタリングするための静的ルールを設定することもできます。

この設定により、Exchange ActiveSync サービスをインターネットに公開し、不正アクセスを防ぐためのセキュリティ層を追加できます。設計上の考慮事項は次のとおりです。

- Windows Server: Exchange ActiveSync コンポーネント用のコネクタには Windows Server が必要です。
- フィルタリングルールセット: 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リングするように設計されています。ユーザー ID でフィルタリングするための静的ルールを設定できますが、たとえば Active Directory グループメンバーシップに基づいてフィルタリングするオプションはありません。Active Directory グループフィルタリングが必要な場合は、代わりに Endpoint Management connector for Exchange ActiveSync を使用できます。
- Citrix ADC のスケーラビリティ: Citrix ADC を介して ActiveSync トラフィックをプロキシする必要があるため、すべての ActiveSync SSL 接続の追加ワークロードをサポートするには、Citrix ADC インスタンスの適切なサイジングが重要です。
- Citrix ADC の統合キャッシュ: Citrix ADC 上の Exchange ActiveSync 用コネクタの構成は、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。この構成の結果、Citrix ADC 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 connector for Exchange ActiveSync に要求を発行する必要がありません。この構成は、適切なパフォーマンスと拡張性にとっても重要です。統合キャッシュは Citrix ADC Platinum Edition で利用可能であり、Enterprise Edition では個別にライセンスを取得できます。
- カスタムフィルタリングポリシー: 標準のネイティブモバイルクライアント以外の特定の ActiveSync クライアントを制限するために、カスタムの Citrix ADC ポリシーを作成する必要がある場合があります。この構成には、ActiveSync HTTP 要求と Citrix ADC レスポンダーポリシー作成に関する知識が必要です。
- Secure Mail クライアント: Secure Mail にはマイクロ VPN 機能があり、境界でのフィルタリングの必要がありません。Secure Mail クライアントは、Citrix Gateway を介して接続されている場合、通常は内部 (信頼された) ActiveSync クライアントとして扱われます。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 (Exchange ActiveSync 用コネクタを使用) の両方、および Secure Mail クライアントのサポートが必要な場合、Citrix は Secure Mail トラフィックが Exchange ActiveSync 用コネクタに使用される Citrix ADC 仮想サーバーを介して流れないようにすることを推奨します。このトラフィックフローは DNS を介して実現でき、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できます。

XenMobile 展開における Citrix Gateway connector for Exchange ActiveSync の図については、「オンプレミス展開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 用 Exchange ActiveSync コネクタ

Endpoint Management connector for Exchange ActiveSync は、Exchange サービスレベルで ActiveSync フィルタリングを提供する XenMobile コンポーネントです。その結果、フィルタリングはメールが XenMobile 環境に入る時ではなく、Exchange サービスに到達した後にのみ行われます。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を照会し、デバイス隔離アクション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 connector for Exchange ActiveSync のルール基準に基づいてデバイスを隔離に出し入れします。Citrix Gateway connector for Exchange ActiveSync と同様に、Endpoint Management connector for Exchange ActiveSync は XenMobile で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リングします。デバイスの種類または ID、エージェントバージョン、および Active Directory グループメンバーシップに基づいてアクセスをフィルタリングするための静的ルールを設定することもできます。

このソリューションでは、Citrix ADC の使用は必要ありません。既存のActiveSyncトラフィックのルーティングを変更することなく、Exchange ActiveSync 用のEndpoint Managementコネクタを展開できます。設計上の考慮事項は次のとおりです。

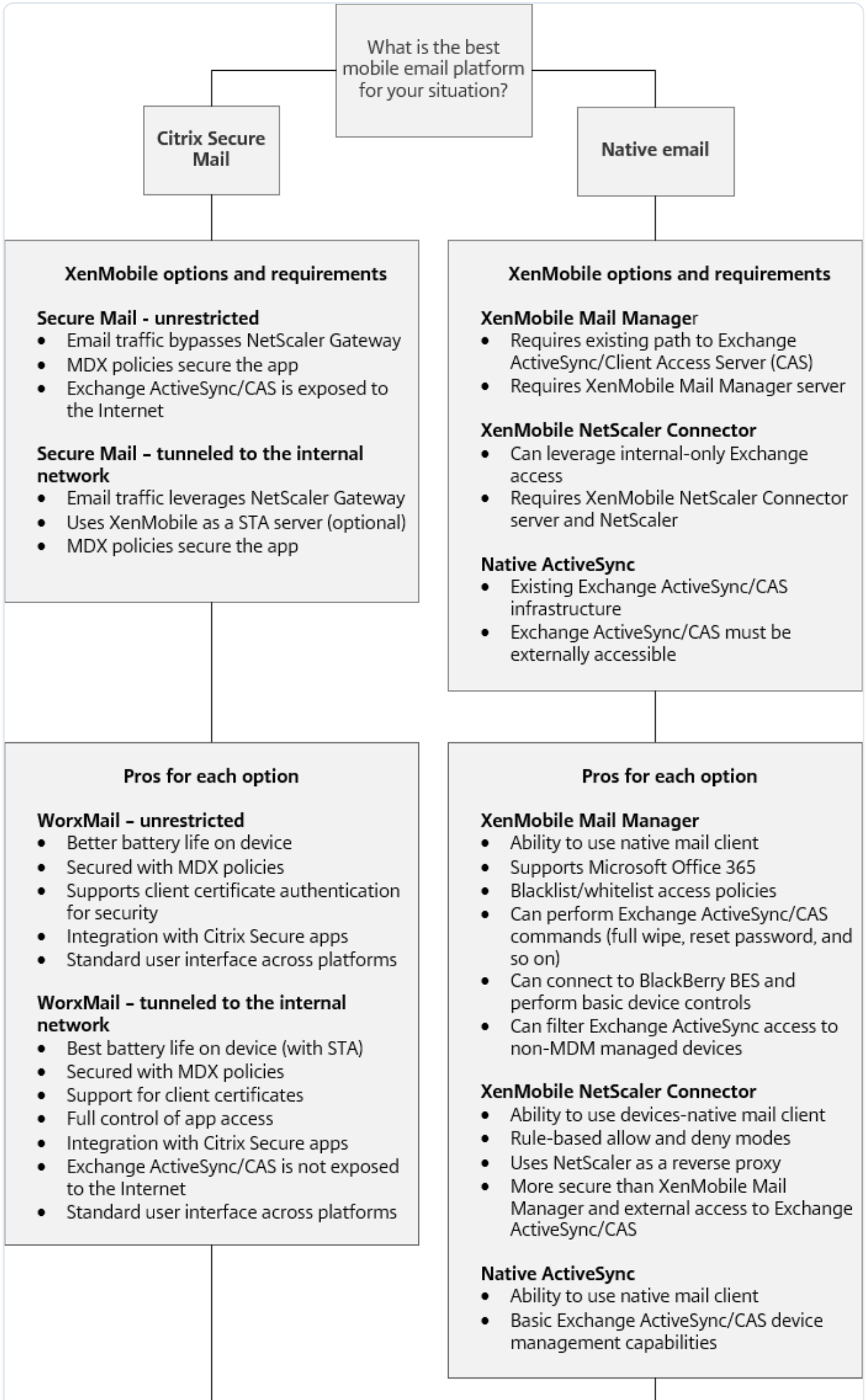
- Windows Server: Exchange ActiveSync コンポーネント用のEndpoint Managementコネクタを展開するには、Windows Server を展開する必要があります。
- フィルタリングルールセット: Exchange ActiveSync 用のCitrix Gatewayコネクタと同様に、Exchange ActiveSync 用のEndpoint Managementコネクタには、デバイスの状態を評価するためのフィルタリングルールが含まれています。また、Exchange ActiveSync 用のEndpoint Managementコネクタは、Active Directory グループメンバーシップに基づいてフィルタリングするための静的ルールもサポートしています。
- Exchange の統合: Exchange ActiveSync 用のEndpoint Managementコネクタは、ActiveSyncロールをホストするExchange Client Access Server (CAS) への直接アクセスと、デバイスの隔離アクションの制御を必要とします。この要件は、環境のアーキテクチャとセキュリティ体制によっては課題となる可能性があります。この技術要件を事前に評価することが重要です。

- その他のActiveSyncクライアント: Exchange ActiveSync 用のEndpoint Managementコネクタ はActiveSyncサービスレベルでフィルタリングを行うため、XenMobile環境外の他の ActiveSyncクライアントを考慮してください。他のActiveSyncクライアントへの意図しない影響を避けるために、Exchange ActiveSync 用のEndpoint Managementコネクタの静的ルールを構成できます。
- 拡張されたExchange機能: Exchange ActiveSync との直接統合により、Exchange ActiveSync 用のEndpoint Managementコネクタは、XenMobile がモバイルデバイスでExchange ActiveSync ワイプを実行する機能を提供します。Exchange ActiveSync 用のEndpoint Managementコネクタは、XenMobile がBlackberryデバイスに関する情報にアクセスし、その他の制御操作を実行することも可能にします。

XenMobile展開におけるExchange ActiveSync 用のEndpoint Managementコネクタの図については、オンプレミス展開の参照アーキテクチャを参照してください。

メールプラットフォームの意思決定ツリー

次の図は、XenMobile展開でネイティブメールソリューションとSecure Mailソリューションのどちらを使用するかの長所と短所を区別するのに役立ちます。各選択肢には、サーバー、ネットワーク、データベースへのアクセスを可能にする関連するXenMobileオプションと要件があります。長所と短所には、セキュリティ、ポリシー、ユーザーインターフェイスに関する考慮事項が含まれます。


What is the best mobile email platform for your situation?
Citrix Secure Mail
Native email
XenMobile options and requirements
Secure Mail - unrestricted
• Email traffic bypasses NetScaler Gateway
• MDX policies secure the app
• Exchange ActiveSync/CAS is exposed to the Internet
Secure Mail – tunneled to the internal network
• Email traffic leverages NetScaler Gateway
• Uses XenMobile as a STA server (optional)
• MDX policies secure the app
XenMobile options and requirements
XenMobile Mail Manager
• Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
• Requires XenMobile Mail Manager server
XenMobile NetScaler Connector
• Can leverage internal-only Exchange access
• Requires XenMobile NetScaler Connector server and NetScaler
Native ActiveSync
• Existing Exchange ActiveSync/CAS infrastructure
• Exchange ActiveSync/CAS must be externally accessible
Pros for each option
WorxMail – unrestricted
• Better battery life on device
• Secured with MDX policies
• Supports client certificate authentication for security
• Integration with Citrix Secure apps
• Standard user interface across platforms
WorxMail – tunneled to the internal network
• Best battery life on device (with STA)
• Secured with MDX policies
• Support for client certificates
• Full control of app access
• Integration with Citrix Secure apps
• Exchange ActiveSync/CAS is not exposed to the Internet
• Standard user interface across platforms
Pros for each option
XenMobile Mail Manager
• Ability to use native mail client
• Supports Microsoft Office 365
• Blacklist/whitelist access policies
• Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
• Can connect to BlackBerry BES and perform basic device controls
• Can filter Exchange ActiveSync access to non-MDM managed devices
XenMobile NetScaler Connector
• Ability to use devices-native mail client
• Rule-based allow and deny modes
• Uses NetScaler as a reverse proxy
• More secure than XenMobile Mail Manager and external access to Exchange ActiveSync/CAS
Native ActiveSync
• Ability to use native mail client
• Basic Exchange ActiveSync/CAS device management capabilities

XenMobile® 統合

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際に考慮すべき事項について説明します。たとえば、Virtual Apps and Desktops に Citrix ADC をすでに使用している場合:

- 既存の Citrix ADC インスタンスを使用しますか、それとも新しい専用インスタンスを使用しますか？
- 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 Citrix Files を使用する予定ですか？
- XenMobile に統合したいネットワークアクセスコントロールソリューションをお持ちですか？
- 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？

シトリックス ADC と シトリックス ゲートウェイ

Citrix Gateway は、XenMobile ENT および MAM モードで必須です。Citrix Gateway は、すべての企業リソースへのアクセスにマイクロ VPN パスを提供し、強力な多要素認証をサポートします。Citrix ADC の負荷分散は、すべての XenMobile Server デバイスモードで必要です。

- 複数の XenMobile Server をお持ちの場合
- または、XenMobile Server が DMZ または内部ネットワーク内にある場合（したがって、トラフィックはデバイスから Citrix ADC を経由して XenMobile に流れる場合）

既存の Citrix ADC 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セットアップ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 Citrix ADC インスタンスを使用する利点と欠点について説明します。

XenMobile 用に作成された Citrix Gateway VIP を備えた共有 Citrix ADC MPX

利点:

- すべての Citrix リモート接続（Citrix Virtual Apps and Desktops™、フル VPN、クライアントレス VPN）に共通の Citrix ADC インスタンスを使用します。
- 既存のCitrix ADC構成（証明書認証やDNS、LDAP、NTPなどのサービスへのアクセスなど）を使用します。
- 単一のCitrix ADCプラットフォームライセンスを使用します。

デメリット:

- 同じCitrix ADCで2つの異なるユースケースを処理する場合、拡張性の計画がより困難になります。
- Citrix Virtual Apps™ and Desktopsのユースケースでは、特定のCitrix ADCバージョンが必要になる場合があります。その同じバージョンがXenMobileで既知の問題を抱えている可能性や、XenMobileがそのCitrix ADCバージョンで既知の問題を抱えている可能性があります。
- Citrix Gatewayが存在する場合、XenMobile用のCitrix ADC構成を作成するために、Citrix ADC for XenMobileウィザードを再度実行することはできません。
- Citrix 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、Citrix ADCにインストールされ、VPN接続に必要となる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Citrix ADC仮想サーバーで利用可能であるため、XenMobile以外のサービスがそれらを消費する可能性があります。

専用のCitrix ADC VPX/MPXインスタンス

メリット:

Citrixは、Citrix ADCの専用インスタンスを使用することを推奨しています。

- 拡張性の計画が容易になり、XenMobileのトラフィックを、すでにリソースが制約されている可能性のあるCitrix ADCインスタンスから分離します。
- XenMobileとCitrix Virtual Apps and Desktopsが異なるCitrix ADCソフトウェアバージョンを必要とする場合に発生する問題を回避します。一般的に、XenMobileには最新の互換性のあるCitrix ADCバージョンとビルドを使用することが推奨されます。
- 組み込みのCitrix ADC for XenMobileウィザードを介して、Citrix ADCのXenMobile構成を可能にします。
- サービスの仮想的および物理的な分離。
- Citrix 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、XenMobileに必要なユーザーアクセスライセンスは、Citrix ADC上のXenMobileサービスでのみ利用可能です。

デメリット:

- XenMobileの構成をサポートするために、Citrix ADC上で追加サービスのセットアップが必要です。
- 別のCitrix ADCプラットフォームライセンスが必要です。Citrix Gateway用に各Citrix ADCインスタンスにライセンスを付与します。

Citrix ADCとCitrix Gatewayを各XenMobile Serverモードと統合する際に考慮すべき事項については、Citrix ADCとCitrix Gatewayとの統合を参照してください。

StoreFront

Citrix Virtual Apps and Desktops環境をお持ちの場合、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、次のようになります。

- アプリは、XenMobileに登録されているユーザーが利用できます。
- アプリは、他のモバイルアプリとともにXenMobile Storeに表示されます。
- XenMobileは、StoreFront上のレガシー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ている場合、HDXアプリはReceiverを使用して起動します。

StoreFrontには、StoreFrontインスタンスごとに1つのサービスサイトという制限があります。複数のストアがあり、それを他の本番環境での使用から分離したいとします。その場合、Citrixは通常、XenMobile用に新しい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に異なる認証要件はありますか？StoreFrontサービスサイトでは、ログオンにActive Directoryの資格情報が必要です。証明書ベースの認証のみを使用しているお客様は、同じCitrix 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、Receiverとモバイル生産性アプリに個別のストアフロントを使用する場合と、結合されたストアフロントを使用する場合の長所と短所について説明します。

既存のStoreFrontインスタンスをXenMobile Serverと統合する

長所:

- 同じストア: HDXアクセスに同じCitrix ADC VIPを使用している場合、XenMobileに追加のStoreFront構成は不要です。同じストアを使用し、Receiverアクセスを新しいCitrix ADC VIPに誘導したい場合は、適切なCitrix Gateway構成をStoreFrontに追加します。
- 同じStoreFrontサーバー: 既存のStoreFront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ための StoreFrontの再構成は、XenMobileにも悪影響を及ぼす可能性があります。

- 同じStoreFrontサーバー: 大規模な環境では、アプリの列挙と起動のためにXenMobileがPNAgentを使用することによる追加の負荷を考慮してください。

XenMobile Server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用のStoreFrontストアの構成変更は、既存のVirtual Apps and Desktopsワークロードに影響を与えてはなりません。
- 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を与えてはなりません。また、アプリの列挙と起動のためにXenMobileがPNAgentを使用すること以外の負荷は、スケーラビリティに影響を与えてはなりません。

短所:

- 新しいストア: StoreFrontストアの構成。
- 新しいStoreFrontサーバー: 新しいStoreFrontのインストールと構成が必要です。

詳細については、XenMobileドキュメントの「Virtual Apps and Desktops through Citrix Secure Hub」を参照してください。

シェアファイルとシトリックスファイル

> **免責事項:**

> ShareFile (現Progress) がサポートを終了した場合、この機能は非推奨になります。

> Citrix Filesを使用すると、ユーザーはあらゆるデバイスからすべてのデータにアクセスして同期できます。Citrix Filesを使用すると、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はCitrix Filesに以下を提供できます。

- XenMobileアプリユーザー向け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。
- 包括的なアクセス制御ポリシー。

モバイルユーザーは、Enterpriseアカウントの全機能セットを利用できます。

あるいは、XenMobileをストレージゾーンコネクタとのみ統合するように構成することもできます。ストレージゾーンコネクタを介して、Citrix Files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サイト内: サイトコレクションとドキュメントライブラリ。

接続されたファイル共有には、Citrix Virtual Apps and Desktops環境で使用されるものと同じネットワーク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、Citrix Filesまたはストレージゾーンコネクタとの統合を構成します。詳細については、「Citrix Files use with XenMobile」を参照してください。

以下のセクションでは、Citrix Filesの設計上の決定を行う際に考慮すべき質問について説明します。

Citrix Files またはストレージゾーンコネクタのみと統合する

検討事項:

- Citrix が管理するストレージゾーンにデータを保存しますか？
- ユーザーにファイル共有および同期機能を提供しますか？
- ユーザーが Citrix Files Web サイト上のファイルに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 のコンテンツやパーソナルクラウドコネクタにアクセスできるようにしますか？

設計上の決定事項:

- これらの質問のいずれかに対する回答が「はい」である場合は、Citrix Files と統合します。
- ストレージゾーンコネクタのみとの統合により、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 サブドメインを設定したり、Citrix Files にユーザーをプロビジョニングしたり、Citrix Files データをホストしたりすることはありません。XenMobile でストレージゾーンコネクタを使用すると、企業ネットワーク外へのユーザー情報の漏洩に対するセキュリティ制限に準拠します。

ストレージゾーンコントローラーサーバーの場所

検討事項:

- オンプレミスストレージまたはストレージゾーンコネクタなどの機能が必要ですか？
- Citrix Files のオンプレミス機能を使用する場合、ストレージゾーンコントローラーはネットワークのどこに配置されますか？

設計上の決定事項:

- ストレージゾーンコントローラーサーバーを Citrix Files クラウド、オンプレミスのシングル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のどこに配置するかを決定します。
- ストレージゾーンコントローラーは、Citrix Files Control Plane と通信するためにインターネットアクセスを必要とします。直接アクセス、NAT/PAT 構成、プロキシ構成など、いくつかの方法で接続できます。

ストレージゾーンコネクタ

質問事項:

- CIFS共有パスは何ですか？
- SharePointのURLは何ですか？

設計上の決定事項:

- それらの場所にアクセスするために、オンプレミスのストレージゾーンコントローラが必要かどうかを判断します。
- ファイルリポジトリ、CIFS共有、SharePointなどの内部リソースとのストレージゾーンコネクタ通信のため、CitrixはストレージゾーンコントローラがDMZファイアウォールの背後にある内部ネットワークに配置され、Citrix ADCによって前面に配置されることを推奨します。

XenMobile EnterpriseとのSAML統合

質問事項:

- Citrix FilesにActive Directory認証は必要ですか？
- XenMobile用Citrix Filesアプリの初回使用時にSSOが必要ですか？
- 現在の環境に標準のIdPはありますか？
- SAMLを使用するために必要なドメイン数はいくつですか？
- Active Directoryユーザーに複数のメールエイリアスがありますか？
- 進行中または近日中に予定されているActive Directoryドメイン移行はありますか？

設計上の決定事項:

XenMobile Enterprise環境では、Citrix Filesの認証メカニズムとしてSAMLを使用することを選択できます。認証オプションは次のとおりです。

- XenMobile ServerをSAMLのIDプロバイダー (IdP) として使用する

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、Citrix Filesアカウントの作成を自動化し、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はこのプロセス向けに強化されています。Active Directoryの同期は必要ありません。
- ユーザープロビジョニングにCitrix Filesユーザー管理ツールを使用する.
- サポートされているサードパーティベンダーをSAMLのIdPとして使用する

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機能を必要としない場合、このオプションが最適である可能性があります。このオプションでは、アカウントプロビジョニングのためにCitrix Filesユーザー管理ツールの使用も必要です。

ADFSなどのサードパーティIdPソリューションを使用すると、Windowsクライアント側でSSO機能を提供することもできます。Citrix Files SAML IdPを選択する前に、ユースケースを評価してください。

また、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として構成することができます。

モバイルアプリ

質問事項:

- どのCitrix Filesモバイルアプリを使用する予定ですか (public、MDM、MDX)？

設計上の決定事項:

- Apple App StoreおよびGoogle Play Storeからモバイル生産性アプリを配布します。この公開アプリストア配布により、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。
- セキュリティが低く、コンテナ化が不要な場合、公開されているCitrix Filesアプリケーションは適切ではない可能性があります。MDMのみの環境では、XenMobileをMDMモードで使用して、Citrix FilesアプリのMDMバージョンを配信できます。
- 詳細については、(/ja-jp/xenmobile/server/advanced-concepts/xenmobile-deployment/apps.html)および(/ja-jp/mobile-productivity-apps/sharefile.html)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

質問事項:

- デスクトップ、Web、モバイルユーザーに対してどのような制限が必要ですか？
- ユーザーに対してどのような標準アクセス制御設定を希望しますか？
- 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？

設計上の決定事項:

- Citrix Files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。詳細については、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Citrix Files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。これらの場合、XenMobileポリシーが優先され、その後にCitrix Filesデバイスセキュリティ設定が適用されます。例: Citrix Filesで外部アプリを無効にしても、XenMobileで有効にした場合、外部アプリはCitrix Filesで無効になります。XenMobileがPIN/パスコードを要求しないようにアプリを設定できますが、Citrix FilesアプリはPIN/パスコードを要求します。

標準ストレージゾーンと制限付きストレージゾーン

質問事項:

- 制限付きストレージゾーンが必要ですか？

設計上の決定事項:

- 標準ストレージゾーンは、機密性の低いデータ向けであり、従業員が非従業員とデータを共有できるようにします。このオプションは、ドメイン外でのデータ共有を伴うワークフローをサポートします。
- 制限付きストレージゾーンは機密データを保護します。認証されたドメインユーザーのみがゾーンに保存されている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可能性の高いシナリオは次のとおりです。XenMobile Serverが存在するサブネットが、必要なApple、Google、またはMicrosoftのIPアドレスへのアウトバウンドインターネットアクセスを持っていない場合です。XenMobileでプロキシサーバー設定を指定して、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。詳細については、「プロキシサーバーを有効にする」を参照してください。

次の表は、XenMobileで最も一般的に使用されるプロキシの利点と欠点について説明しています。

オプション	利点	欠点
XenMobile ServerでHTTP(S)/SOCKSプロキシを使用する。	ポリシーによってXenMobile Serverサブネットからのアウトバウンドインターネット接続が許可されていない場合：	プロキシサーバーが故障すると、APNs (iOS) または Firebase Cloud Messaging (Android) の接続が切断され

	HTTP(S)またはSOCKSプロキシを構成してインターネット接続を提供できます。	ます。その結果、すべてのiOSおよびAndroidデバイスでデバイス通知が失敗します。
Secure WebでHTTP(S)プロキシを使用する。	HTTP/HTTPSトラフィックを監視して、インターネットアクティビティ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インターネットトラフィックがインターネットに送信される前に企業ネットワークにトンネルバックする必要があります。インターネット接続がブラウジングを制限する場合、この構成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を与える可能性があります。

スプリットトンネリングのCitrix ADCセッションプロファイル構成は、トラフィックに次のように影響します。

Citrix ADCスプリットトンネリングが**オフ**の場合：

- MDXの**ネットワークアクセス**ポリシーが**内部ネットワークへのトンネル**に設定されている場合：すべてのトラフィックは、マイクロVPNまたはクライアントレスVPN (cVPN) トンネルを使用してCitrix Gatewayに戻るように強制されます。
- プロキシサーバー用のCitrix ADCトラフィックポリシー/プロファイルを構成し、それらをCitrix Gateway VIPにバインドします。

> **重要：**
>
> Secure Hub cVPNトラフィックをプロキシから除外するようにしてください。

- 詳細については、XenMobile Secure Hub のセキュアブラウズモードにおけるプロキシサーバー経由のトラフィックを参照してください。

Citrix ADCスプリットトンネリングが**オン**の場合：

- アプリがMDXの**ネットワークアクセス**ポリシーを**内部ネットワークへのトンネル**に設定して構成されている場合：アプリはまず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、それらのアプリはCitrix Gatewayにフォールバックします。

- プロキシサーバー用のCitrix ADCトラフィックポリシーとプロファイルを構成します。次に、それらのポリシーとプロファイルをCitrix Gateway VIPにバインドします。

> **重要：**

> Secure Hub cVPNトラフィックをプロキシから除外するようにしてください。

> **スプリットDNS**（**クライアントエクスペリエンス**の下）のCitrix ADCセッションプロファイル構成は、スプリットトンネリングと同様に機能します。

スプリットDNSが有効で**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ようとし、失敗した場合はCitrix ADCにフォールバックしてDNS解決を行います。

スプリットDNSが**リモート**に設定されている場合：

- DNS解決はCitrix ADCでのみ行われます。

Split DNSが**Local**に設定されている場合：

- クライアントはFQDNをローカルで解決しようとします。Citrix ADCはDNS解決には使用されません。

アクセス制御

企業は、ネットワークの内外でモバイルデバイスを管理できます。XenMobileのような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のに優れています。しかし、それらをネットワークアクセスコントロール (NAC) ソリューションと組み合わせると、ネットワーク内部のデバイスにQoSとよりきめ細かな制御を追加できます。この組み合わせにより、NACソリューションを通じてXenMobileデバイスのセキュリティ評価を拡張できます。その後、NACソリューションはXenMobileセキュリティ評価を使用して、認証の決定を容易にし、処理できます。

NACポリシーを適用するために、以下のいずれかのソリューションを使用できます。

- シトリックス ゲートウェイ
- シスコ アイデンティティ サービス エンジン (ISE)
- ForeScout

Citrixは、他のNACソリューションとの統合を保証しません。

XenMobileとのNACソリューション統合の利点は次のとおりです。

- エンタープライズネットワーク上のすべてのエンドポイントに対する、より優れたセキュリティ、コンプライアンス、および制御。
- NACソリューションは次のことができます。
  - デバイスがネットワークに接続しようとした瞬間に検出します。
  - デバイス属性についてXenMobileにクエリを実行します。
  - そのデバイス情報を使用して、それらのデバイスを許可、ブロック、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、適用することを選択したセキュリティポリシーによって異なります。
- NACソリューションは、IT管理者に管理対象外および非準拠デバイスのビューを提供します。

XenMobileがサポートするNACコンプライアンスフィルターの説明と構成の概要については、「ネットワークアクセス制御」を参照してください。

マルチサイト要件

高可用性と災害復旧のために複数のサイトを含むXenMobile®展開を設計および構成できます。この記事では、XenMobile展開で使用される高可用性および災害復旧モデルの概要を説明します。

高可用性

- XenMobileクラスターノードの場合、Citrix ADCがロードバランシングを処理します。詳細については、「クラスタリングの構成」を参照してください。
- XenMobile Serverノードはアクティブ/アクティブ構成で動作します。
- 容量が必要に応じて、XenMobile Serverノードが高可用性クラスターに追加されます。1つのノードで約8,500台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」を参照してください）。
- Citrix®は、「n+1」のXenMobile Serverを構成することを推奨しています。これは、8,500台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台の追加サーバーを意味します。
- Citrixは、構成を2番目のCitrix ADCと同期できるように、可能な限りすべてのCitrix ADCインスタンスに対して高可用性を推奨しています。
- 標準のCitrix ADC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展開には、通常以下が含まれます。

- 2つのCitrix ADCインスタンス（VPXまたはMPX）。Citrix ADC 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つ以上のXenMobile Server。

災害復旧

XenMobileは、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間で災害復旧のために構成できます。Citrix ADCとグローバルサーバーロードバランシング（GSLB）を使用してアクティブ/アクティブな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/アクティブなセットアップと同じになるようにします。

災害復旧の場合、XenMobile展開には以下が含まれます。

- 2つのデータセンター - それぞれに1つまたは複数のCitrix ADC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ます。
- データセンターにトラフィックを誘導するためのGSLBサーバー。GSLBサーバーは、XenMobile登録URLと、サイトへのトラフィックを処理するCitrix Gateway URLの両方に対して構成されます。
- Citrix ADC for XenMobileウィザードを使用してCitrix Gatewayを構成する場合、デフォルトでは、MAMロードバランシングサーバーへの経路で、XenMobile登録サーバーへのトラフィックとCitrix Gatewayへのトラフィックを解決するためにGSLBは有効になっていません。その結果、追加の手順が必要です。これらの手順の準備と実装の詳細については、「災害復旧」を参照してください。
- Always On可用性グループのクラスター化されたSQL Server。
- XenMobileサーバーとSQL Server間の遅延は5ミリ秒未満である必要があります。

> **注：**
>
> このハンドブックで説明されている災害復旧方法は、アクセス層の自動災害復旧のみを提供します。デバイスがXenMobileサーバーに接続できるようになる前に、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。

Citrix GatewayおよびCitrix ADCとの統合

XenMobile®と統合すると、Citrix Gatewayは、MAMデバイスが内部ネットワークにリモートデバイスアクセスするための認証メカニズムを提供します。この統合により、モバイル生産性アプリはマイクロVPNを介してイントラネット内の企業サーバーに接続できます。マイクロVPNは、モバ

イルデバイス上のアプリからCitrix Gatewayに作成されます。Citrix Gatewayは、すべての企業リソースへのアクセスにマイクロVPNパスを提供し、強力な多要素認証をサポートします。

Citrix ADCの負荷分散は、以下のケースで、すべてのXenMobile Serverデバイスモードに必要です。

- 複数のXenMobile Serverがある場合
- または、XenMobile ServerがDMZまたは内部ネットワーク内にある場合（そのため、トラフィックはデバイスからCitrix ADC、XenMobileへと流れます）

XenMobile Serverモードの統合要件

Citrix GatewayとCitrix ADCの統合要件は、XenMobile Serverのモード（MAM、MDM、ENT）によって異なります。

MAM

MAMモードのXenMobile Serverの場合：

- **Citrix Gateway**が必要です。Citrix Gatewayは、すべての企業リソースへのアクセスにマイクロVPNパスを提供し、強力な多要素認証をサポートします。
- **Citrix ADC**は負荷分散に推奨されます。

  Citrixでは、高可用性構成でXenMobileを展開することを推奨しています。これには、XenMobileの前にロードバランサーが必要です。詳細については、「MAMおよびレガシーMAMモードについて」を参照してください。

MDM

MDMモードのXenMobile Serverの場合：

- Citrix Gatewayは必須ではありません。MDM展開の場合、CitrixはモバイルデバイスVPNにCitrix Gatewayを推奨しています。
- Citrix ADC はセキュリティと負荷分散に推奨されます。

  Citrix は、セキュリティと負荷分散のために、XenMobile Server の前に Citrix ADC アプライアンスを展開することを推奨します。DMZ に XenMobile を配置する標準的な展開では、Citrix は Citrix ADC for XenMobile ウィザードと、SSL Bridge モードでの XenMobile Server の負荷分散を推奨します。以下の展開では、SSL オフロードも検討できます。

  - XenMobile Server が DMZ ではなく内部ネットワークに配置されている。
  - または、セキュリティチームが SSL Bridge 構成を要求している。

Citrix は、MDM のために NAT または既存のサードパーティ製プロキシやロードバランサーを介して XenMobile Server をインターネットに公開することを推奨しません。これらの構成は、SSL トラフィックが XenMobile Server (SSL Bridge) で終端される場合でも、潜在的なセキュリティリスクをもたらします。

高セキュリティ環境では、デフォルトの XenMobile 構成を持つ Citrix ADC は、セキュリティ要件を満たすか、それを上回ります。

最高のセキュリティ要件を持つ MDM 環境では、Citrix ADC での SSL 終端により、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。詳細については、「セキュリティ要件」を参照してください。Citrix ADC は、SSL/TLS 暗号と SSL FIPS Citrix ADC ハードウェアを定義するオプションを提供します。

ENT (MAM+MDM)

XenMobile Server が ENT モードの場合:

- Citrix Gateway が必要です。Citrix Gateway は、すべての企業リソースへのアクセスにマイクロ VPN パスを提供し、強力な多要素認証をサポートします。

  XenMobile Server モードが ENT で、ユーザーが MDM 登録をオプトアウトした場合、デバイスはレガシー MAM モードで動作します。レガシー MAM モードでは、デバイスは Citrix Gateway FQDN を使用して登録します。詳細については、「MAM とレガシー MAM モードについて」を参照してください。
- Citrix ADC は負荷分散に推奨されます。詳細については、この記事の「MDM」の項にある Citrix ADC の説明を参照してください。

> **重要:**
>
> 初期登録の場合、負荷分散仮想サーバーを SSL オフロードまたは SSL ブリッジのどちらに構成しても、ユーザーデバイスからのトラフィックは XenMobile Server で認証されます。

設計上の決定事項

以下のセクションでは、XenMobile との Citrix Gateway 統合を計画する際に考慮すべき多くの設計上の決定事項をまとめます。

ライセンスとエディション

決定の詳細:

- どのエディションの Citrix ADC を使用する予定ですか？
- Citrix ADC にプラットフォームライセンスを適用しましたか？
- MAM 機能が必要な場合、Citrix ADC ユニバーサルアクセスライセンスを適用しましたか？

設計ガイダンス:

Citrix Gateway に適切なライセンスを適用していることを確認してください。Exchange ActiveSync 用の Citrix Gateway connector™ を使用している場合、統合キャッシュが必要になることがあります。そのため、適切な Citrix ADC Edition が導入されていることを確認する必要があります。

Citrix ADC 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 の負荷分散には、最低でも Citrix ADC Standard プラットフォームライセンスが必要です。
- ストレージゾーンコントローラーを使用した ShareFile の負荷分散には、最低でも Citrix ADC Standard プラットフォームライセンスが必要です。
- XenMobile Advanced Edition (オンプレミス) または Citrix Endpoint Management™ (クラウド) には、MAM に必要な Citrix Gateway ユニバーサルライセンスが含まれています。
- Exchange の負荷分散には、Citrix ADC Platinum プラットフォームライセンス、または統合キャッシュライセンスを追加した Citrix ADC Enterprise プラットフォームライセンスが必要です。

XenMobile 用 Citrix ADC バージョン

決定の詳細:

- XenMobile環境で実行されているCitrix ADCのバージョンは何ですか？
- 個別のインスタンスが必要ですか？

設計ガイダンス:

Citrixでは、Citrix Gateway仮想サーバーにCitrix ADCの専用インスタンスを使用することをお勧めします。XenMobile環境で、Citrix ADCの最小要件バージョンとビルドが使用されていることを確認してください。通常、XenMobileには最新の互換性のあるCitrix ADCバージョンとビルドを使用するのが最適です。Citrix Gatewayのアップグレードが既存の環境に影響を与える場合は、XenMobile用に2つ目の専用インスタンスが適切である可能性があります。

XenMobileとVPN接続を使用する他のアプリでCitrix ADCインスタンスを共有する予定がある場合は、両方に十分なVPNライセンスがあることを確認してください。XenMobileのテスト環境と本番環境は、Citrix ADCインスタンスを共有できないことに注意してください。

証明書

決定の詳細:

- XenMobile環境への登録とアクセスに、より高度なセキュリティが必要ですか？
- LDAPは選択肢ではありませんか？

設計ガイダンス:

XenMobileのデフォルト設定は、ユーザー名とパスワード認証です。XenMobile環境への登録とアクセスに別のセキュリティ層を追加するには、証明書ベースの認証の使用を検討してください。LDAPと証明書を組み合わせて2要素認証を行うことで、RSAサーバーを必要とせずに、より高度なセキュリティを提供できます。

LDAPを許可せず、スマートカードまたは類似の方法を使用する場合、証明書を構成することで、スマートカードをXenMobileに認識させることができます。ユーザーは、XenMobileが生成する一意のPINを使用して登録します。ユーザーがアクセス権を取得すると、XenMobileはXenMobile環境への認証に使用される証明書を作成して展開します。

XenMobileは、サードパーティの証明機関に対してのみ証明書失効リスト (CRL) をサポートしています。Microsoft CAが構成されている場合、XenMobileはCitrix ADC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際は、Citrix ADCの証明書失効リスト (CRL) 設定 **Enable CRL Auto Refresh** を構成する必要があるかどうかを検討してください。この手順により、MAMのみに登録された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いようにします。XenMobileは新しい証明書を再発行します。これは、証明書が失効した場合でも、ユーザーがユーザー証明書を生成することを制限しないためです。この設定は、CRLが期限切れのPKIエンティティをチェックする際に、PKIエンティティのセキュリティを向上させます。

ネットワークトポロジ

決定の詳細:

- どのようなCitrix ADCトポロジが必要ですか？

設計ガイダンス:

CitrixはXenMobileにCitrix ADCインスタンスを使用することを推奨しています。ただし、内部ネットワークからDMZへのトラフィックを望まない場合があるかもしれません。その場合は、Citrix ADCの追加インスタンスをセットアップすることを検討してください。内部ユーザー用に1つのCitrix ADCインスタンスを、外部ユーザー用に1つのCitrix ADCインスタンスを使用します。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際、DNSレコードのキャッシュにより、Secure Hubのログオンプロンプトが増加する可能性があります。

XenMobileはCitrix 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Citrix Gateway VIP

決定の詳細:

- 現在、Virtual Apps and DesktopsにCitrix Gatewayを使用していますか？
- XenMobileでVirtual Apps and Desktopsと同じCitrix Gatewayを使用する予定ですか？
- 両方のトラフィックフローの認証要件は何ですか？

設計ガイダンス:

Citrix環境にXenMobileとVirtual Apps and Desktopsが含まれている場合、両方に同じCitrix ADCインスタンスとCitrix Gateway仮想サーバーを使用できます。バージョン競合の可能性や環境の分離のため、各XenMobile環境には専用のCitrix ADCインスタンスとCitrix Gatewayを推奨します。ただし、専用のCitrix ADCインスタンスが選択肢にない場合、CitrixはSecure Hubのトラフィックフローを分離するために専用のCitrix Gateway仮想サーバーを使用することを推奨します。この構成は、XenMobileとVirtual Apps and Desktops間で共有される仮想サーバーの代わりとなります。

LDAP認証を使用する場合、ReceiverとSecure Hubは問題なく同じCitrix Gatewayに認証できます。証明書ベースの認証を使用する場合、XenMobileはMDXコンテナに証明書をプッシュし、Secure Hubはその証明書を使用してCitrix Gatewayで認証します。ReceiverはSecure Hubとは別であり、Secure Hubと同じ証明書を使用して同じCitrix Gatewayに認証することはできません。

2つのCitrix Gateway VIPに同じFQDNを使用できる、以下の回避策を検討してください。

- 同じIPアドレスを持つ2つのCitrix Gateway VIPを作成します。Secure Hub用のVIPは標準の443ポートを使用し、Virtual Apps and Desktops（Receiverを展開する）用のVIPはポート444を使用します。
- その結果、1つのFQDNが同じIPアドレスに解決されます。
- この回避策では、StoreFront™ を構成して、デフォルトのポート 443 の代わりにポート 444 の ICA ファイルを返すようにすることができます。この回避策では、ユーザーがポート番号を入力する必要はありません。

Citrix Gateway のタイムアウト

決定の詳細:

- XenMobile トラフィックの Citrix Gateway タイムアウトをどのように構成しますか？

設計ガイダンス:

Citrix 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含まれています。詳細については、推奨される構成 を参照してください。バックグラウンドサービス、Citrix ADC、およびオフライン時のアプリケーションアクセスには、異なるタイムアウト値があることに注意してください。

MAM 用 XenMobile ロードバランサー IP アドレス

決定の詳細:

- VIP には内部 IP アドレスと外部 IP アドレスのどちらを使用していますか？

設計ガイダンス:

Citrix Gateway VIP にパブリック IP アドレスを使用できる環境では、XenMobile ロードバランシング VIP とアドレスをこの方法で割り当てると、登録エラーが発生します。

このシナリオでの登録エラーを回避するために、ロードバランシング VIP が内部 IP を使用していることを確認してください。この仮想 IP アドレスは、プライベート IP アドレスの RFC 1918 標準に従う必要があります。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、認証プロセス中に Citrix ADC が XenMobile Server に正常に接続できません。詳細については、`<https://support.citrix.com/article/CTX200430>` を参照してください。

MDM ロードバランシングメカニズム

決定の詳細:

- Citrix Gateway は XenMobile Server のロードバランスをどのように行いますか？

設計ガイダンス:

XenMobileがDMZにある場合はSSLブリッジを使用します。セキュリティ標準を満たすために必要な場合は、XenMobileが内部ネットワークにあるときにSSLオフロードを使用します。

- SSLブリッジモードでCitrix ADC VIPを使用してXenMobile Serverの負荷分散を行う場合、インターネットトラフィックはXenMobile Serverに直接流れ、そこで接続が終了します。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。
- SSLオフロードモードでCitrix ADC VIPを使用してXenMobile Serverの負荷分散を行う場合、インターネットトラフィックはCitrix ADCに直接流れ、そこで接続が終了します。その後、Citrix ADCはCitrix ADCからXenMobile Serverへの新しいセッションを確立します。SSLオフロードモードでは、セットアップとトラブルシューティングに追加の複雑さが伴います。

SSLオフロードによるMDM負荷分散のサービスポート

決定の詳細:

- 負荷分散にSSLオフロードモードを使用する予定の場合、バックエンドサービスはどのポートを使用しますか？

設計ガイダンス:

SSLオフロードの場合、ポート80または8443を次のように選択します。

- 真のオフロードのために、XenMobile Serverへのバックエンドにポート80を使用します。
- エンドツーエンド暗号化、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サポート記事「Supported Architectures Between NetScaler and XenMobile Server」を参照してください。

登録FQDN

決定の詳細:

- 登録用FQDNおよびXenMobileインスタンス/負荷分散VIPとして何を使用する予定ですか？

設計ガイダンス:

クラスター内の最初のXenMobile Serverの初期構成では、XenMobile Server FQDNを指定する必要があります。そのFQDNは、MDM VIP URLおよび内部MAM LB VIP URLと一致している必要があります。（内部Citrix ADCアドレスレコードがMAM LB VIPを解決します。）詳細については、この記事の後半にある「各管理モードの登録FQDN」を参照してください。

さらに、以下の証明書と同じものを使用する必要があります。

- XenMobile SSLリスナー証明書
- 内部MAM LB VIP証明書
- MDM VIP証明書（MDM VIPにSSLオフロードを使用している場合）

> **重要:**
>
> 登録FQDNを構成した後、変更することはできません。新しい登録FQDNには、新しいSQL ServerデータベースとXenMobile Serverの再構築が必要です。

Secure Webトラフィック

決定の詳細:

- Secure Webを内部Webブラウジングのみに制限する予定ですか？

- Secure Webを内部および外部Webブラウジングの両方で有効にする予定ですか？

設計ガイダンス:

Secure Webを内部Webブラウジングのみに使用する予定の場合、Citrix Gatewayの構成は簡単です。Secure Webは、デフォルトですべての内部サイトに到達できる必要があります。ファイアウォールとプロキシサーバーを構成する必要がある場合があります。

Secure Webを内部および外部ブラウジングの両方で使用する予定の場合、SNIPがアウトバウンドインターネットアクセスを持つように有効にする必要があります。IT部門は通常、登録済みデバイス（MDXコンテナを使用）を企業ネットワークの拡張と見なします。そのため、IT部門は通常、Secure Web接続がCitrix ADCに戻り、プロキシサーバーを経由してインターネットに出ることを望んでいます。デフォルトでは、Secure Webはすべてのネットワークアクセスに対して、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ります。Citrix ADCはスプリットトンネル設定を使用します。

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

決定の詳細:

- プッシュ通知を使用する予定はありますか？

iOS の設計ガイダンス:

Citrix Gateway の構成には、スプリットトンネリングがオフの Secure Ticket Authority (STA) が含まれる場合があります。Citrix Gateway は、iOS 用 Secure Mail の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 Secure Mail からのトラフィックを許可する必要があります。

Android の設計ガイダンス:

Firebase Cloud Messaging (FCM) を使用して、Android デバイスが XenMobile に接続する必要がある方法とタイミングを制御します。FCM が構成されている場合、セキュリティアクションまたは展開コマンドは、ユーザーに XenMobile Server への再接続を促すプッシュ通知を Secure Hub にトリガーします。

HDX™ STA

決定の詳細:

- HDX アプリケーションアクセスを統合する予定がある場合、どの STA を使用しますか？

設計ガイダンス:

HDX STA は StoreFront の STA と一致している必要があり、Virtual Apps and Desktops ファームに対して有効である必要があります。

Citrix Files および ShareFile

決定の詳細:

- 環境でストレージゾーンコントローラーを使用する予定はありますか？
- どのCitrix Files VIP URLを使用する予定ですか？

設計ガイダンス:

環境にストレージゾーンコントローラーを含める場合は、以下を正しく構成してください:

- Citrix Files Switch VIP (Citrix Files Control Planeがストレージゾーンコントローラーサーバーと通信するために使用)
- Citrix Filesロードバランシング VIP
- 必要なすべてのポリシーとプロファイル

詳細については、ストレージゾーンコントローラーのドキュメントを参照してください。

SAML IdP

決定の詳細:

- Citrix FilesでSAMLが必要な場合、XenMobileをSAML IdPとして使用しますか？

設計ガイダンス:

推奨されるベストプラクティスは、Citrix FilesをXenMobile Advanced Edition、XenMobile Advanced Edition (オンプレミス)、またはCitrix Endpoint Management (クラウド) と統合することです。これは、SAMLベースのフェデレーションを構成するよりも簡単な代替手段です。これらのXenMobileエディションで Citrix Filesを使用する場合、XenMobileはCitrix Filesに以下を提供します:

- モバイル生産性アプリユーザーのシングルサインオン (SSO) 認証
- Active Directoryに基づくユーザーアカウントプロビジョニング
- 包括的なアクセス制御ポリシー

XenMobileコンソールを使用すると、Citrix Filesの構成を実行し、サービスレベルとライセンス使用状況を監視できます。

Citrix Filesクライアントには、Citrix Files for XenMobileクライアント（ラップされたCitrix Filesとも呼ばれる）とCitrix Filesモバイルクライアント（ラップされていないCitrix Filesとも呼ばれる）の2種類があります。違いを理解するには、「Citrix Files for XenMobileクライアントとCitrix Filesモバイルクライアントの違い」を参照してください。

XenMobileとShareFileをSAMLを使用するように構成して、以下のSSOアクセスを提供できます。

- Citrix Filesモバイルアプリ
- ラップされていないCitrix Filesクライアント（Webサイト、Outlookプラグイン、同期クライアントなど）

XenMobileをCitrix FilesのSAML IdPとして使用するには、適切な構成が設定されていることを確認してください。詳細については、「Citrix FilesでのSSOのためのSAML」を参照してください。

ShareConnectダイレクト接続

決定の詳細:

- ユーザーは、ShareConnectを実行しているコンピューターまたはモバイルデバイスから、ダイレクト接続を使用してホストコンピューターにアクセスする必要がありますか？

設計ガイダンス:

ShareConnectを使用すると、ユーザーはiPad、Androidタブレット、Androidフォンを介してコンピューターに安全に接続し、ファイルやアプリケーションにアクセスできます。ダイレクト接続の場合、XenMobileはCitrix Gatewayを使用して、ローカルネットワーク外の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。

各管理モードの登録FQDN

管理モード	**登録FQDN**
必須MDM登録を伴うエンタープライズ（MDM+MAM）	XenMobile Server エフキューディーエヌ
エンタープライズ (MDM+MAM)、オプションのMDM登録あり	XenMobile Server エフキューディーエヌ または Citrix Gateway エフキューディーエヌ
MDMのみ	XenMobile Server エフキューディーエヌ
MAMのみ (レガシー)	Citrix Gateway エフキューディーエヌ
MAMのみ	XenMobile Server エフキューディーエヌ

展開の概要

Citrixでは、適切な構成を確実にするために、XenMobileウィザード用のCitrix ADCを使用することをお勧めします。このウィザードは1回しか使用できません。テスト、開発、および本番環境など、複数のXenMobileインスタンスがある場合は、追加の環境用にCitrix ADCを手動で構成する必要があります。動作する環境がある場合は、XenMobile用にCitrix ADCを手動で構成する前に、設定をメモしておいてください。

ウィザードを使用する際の重要な決定事項は、XenMobile Serverへの通信にHTTPSを使用するかHTTPを使用するかです。HTTPSは、Citrix ADCとXenMobile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を提供します。再暗号化はXenMobile Serverのパフォーマンスに影響を与えます。HTTPはXenMobile Serverのパフォーマンスを向上させます。Citrix ADCとXenMobile間のトラフィックは暗号化されません。次の表は、Citrix ADCとXenMobile ServerのHTTPおよびHTTPSポート要件を示しています。

HTTPS

Citrixは通常、Citrix ADC MDM仮想サーバー構成にはSSLブリッジを推奨しています。MDM仮想サーバーでのCitrix ADC SSLオフロードの使用の場合、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。

管理モード	Citrix ADC ロードバランシング方式	SSL再暗号化	XenMobileサーバーポート
MDM	SSLブリッジ	N/A	443, 8443
MAM	SSLオフロード	有効	8443
エンタープライズ	MDM: SSLブリッジ	N/A	443, 8443
エンタープライズ	MAM: SSLオフロード	有効	8443

HTTP

管理モード	Citrix ADCの負荷分散方法	SSL再暗号化	XenMobileサーバーポート
MDM	SSLオフロード	サポートされていません	80

MAM	SSLオフロード	有効	8443
エンタープライズ	MDM: SSLオフロード	サポートされていません	80
エンタープライズ	MAM: SSLオフロード	有効	8443

XenMobile展開におけるCitrix Gatewayの図については、オンプレミス展開の参照アーキテクチャを参照してください。

MDXアプリのSSOとプロキシに関する考慮事項

Citrix ADCとXenMobileを統合することで、ユーザーはすべてのバックエンドHTTP/HTTPSリソースに対してシングルサインオン (SSO) を利用できるようになります。SSO認証の要件に応じて、MDXアプリのユーザー接続を以下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。

- セキュアブラウズ（クライアントレスVPNの一種）
- フルVPNトンネル

環境内でCitrix ADCがSSOを提供する最適な方法でない場合、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およびプロキシオプションについて説明します。これらの概念は他の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。

SSOとユーザー接続の決定フローの図(/en-us/xenmobile/server/media/sso-proxy-decision-flow.png)

Citrix ADC認証方法

このセクションでは、Citrix ADCでサポートされている認証方法に関する一般的な情報を提供します。

SAML認証

Citrix ADCをSecurity Assertion Markup Language (SAML) 用に構成すると、ユーザーはSAMLプロトコルをサポートするWebアプリにシングルサインオンで接続できます。Citrix Gatewayは、SAML WebアプリのIDプロバイダー (IdP) シングルサインオンをサポートしています。

必要な構成:

- Citrix ADC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に対して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、Citrix ADCはNTLM認証を自動的に実行します。

必要な構成:

- Citrix ADC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インパーソネーション

XenMobile®はSecure WebでのみKerberosをサポートします。Citrix ADCでKerberos SSOを構成すると、ユーザーパスワードがCitrix ADCで利用可能な場合にCitrix ADCはインパーソネーションを使用します。インパーソネーションとは、Citrix ADCがユーザー資格情報を使用して、Secure Webなどのサービスへのアクセスに必要なチケットを取得することを意味します。

必要な構成:

- Citrix ADC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。
- Citrix ADCでKerberos Constrained Delegation (KCD) アカウントを構成します。そ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。
- これらの構成およびその他の詳細については、Citrixブログ「WorxWeb and Kerberos Impersonation SSO」を参照してください。

Kerberos の制約付き委任

XenMobileはSecure WebでのみKerberosをサポートします。Citrix ADCでKerberos SSOを構成すると、ユーザーパスワードがCitrix ADCで利用できない場合にCitrix ADCは制約付き委任を使用します。

制約付き委任では、Citrix ADCは指定された管理者アカウントを使用して、ユーザーおよびサービスに代わってチケットを取得します。

必要な構成:

- 必要な権限を持つKCDアカウントをActive Directoryで構成し、Citrix ADCでKCDアカウントを構成します。
- Citrix ADCトラフィックプロファイルでSSOを有効にします。

- Kerberos認証用にバックエンドWebサイトを構成します。

フォーム入力認証

Citrix ADCをフォームベースのシングルサインオン用に構成すると、ユーザーは一度ログオンするだけで、ネットワーク内のすべての保護されたアプリにアクセスできます。この認証方法は、Secure BrowseまたはFull VPNモードを使用するアプリに適用されます。

必要な構成:

- Citrix ADC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を有効にすると、Citrix ADC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、Secure BrowseまたはFull VPNモードを使用するアプリに適用されます。

必要な構成:

- Citrix ADCセッションまたはトラフィックプロファイルでSSOを有効にします。

基本HTTP認証

セッションプロファイルでWebアプリへのSSOを有効にすると、Citrix ADCは基本HTTP認証を自動的に実行します。この認証方法は、Secure BrowseまたはFull VPNモードを使用するアプリに適用されます。

必要な構成:

- Citrix ADCセッションまたはトラフィックプロファイルでSSOを有効にします。

Secure Browse、Full VPNトンネル、またはPAC付きFull VPNトンネル

以下のセクションでは、Secure Webのユーザー接続タイプについて説明します。詳細については、CitrixドキュメントのSecure Webに関する記事「ユーザー接続の構成」を参照してください。

フルVPNトンネル

内部ネットワークにトンネル接続する際に、フルVPNトンネルを使用できます。フル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。Citrixは、クライアント証明書または内部ネットワーク内のリソースへのエンドツーエンドSSLを使用する接続には、フルVPNトンネルを推奨します。フルVPNトンネルは、TCP上のあらゆるプロトコルを処理します。フルVPNトンネルは、Windows、Mac、iOS、Androidデバイスで使用できます。

フルVPNトンネルモードでは、Citrix ADCはHTTPSセッションの内部を可視化できません。

セキュアブラウズ

内部ネットワークにトンネル接続する際に、Secure Browseと呼ばれるクライアントレスVPNのバリエーションを使用できます。Secure Browseは、Secure Webの**優先VPNモード**ポリシーに指定されているデフォルト構成です。Citrixは、シングルサインオン (SSO) を必要とする接続にはSecure Browseを推奨します。

Secure Browseモードでは、Citrix ADCはHTTPSセッションを2つの部分に分割します。

- クライアントからCitrix ADCへ
- Citrix ADCからバックエンドリソースサーバーへ。

このようにして、Citrix ADCは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完全に可視化し、SSOを提供できるようになります。

Secure Browseモードで使用する場合、Secure Webのプロキシサーバーを構成することもできます。詳細については、ブログ「XenMobile WorxWebのSecure Browseモードでのプロキシサーバーを介したトラフィック」を参照してください。

PACを使用したフルVPNトンネル

iOSおよびAndroidデバイス上のSecure WebのフルVPNトンネル展開で、プロキシ自動構成 (PAC) ファイルを使用できます。XenMobileは、Citrix ADCが提供するプロキシ認証をサポートしています。PACファイルには、Webブラウザーが特定のURLにアクセスするためにプロキシを選択する方法を定義するルールが含まれています。PACファイルのルールは、内部サイトと外部サイトの両方の処理を指定できます。Secure WebはPACファイルのルールを解析し、プロキシサーバー情報をCitrix Gatewayに送信します。Citrix 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 MDXポリシーの**Webパスワードキャッシュを有効にする**により、Secure WebはMDXを介してプロキシサーバーへの認証とSSOを提供できます。

Citrix ADCスプリットトンネリング

SSOおよびプロキシ構成を計画する際には、Citrix ADCスプリットトンネリングを使用するかどうかも決定する必要があります。Citrixは、必要な場合にのみCitrix ADCスプリットトンネリングを使用することを推奨します。このセクションでは、スプリットトンネリングの仕組みについて概要を説明します。Citrix ADCは、ルーティングテーブルに基づいてトラフィックパスを決定します。Citrix ADCスプリットトンネリングがオンの場合、Secure Hubは内部 (保護された) ネットワークトラフィックとインターネット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その判断を行います。その後、Secure Hubは内部

ネットワークトラフィックのみをVPNトンネル経由でトンネル化します。Citrix ADCスプリットトンネリングがオフの場合、すべてのトラフィックはVPNトンネルを通過します。

- 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したい場合は、Citrix ADCの分割トンネリングを無効にします。その結果、すべてのトラフィックはVPNトンネルを通過します。
- PACでフルVPNトンネルを使用する場合は、Citrix 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ファイルを構成した場合、PACファイルのルールがCitrix ADCの分割トンネリングルールを上書きします。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、Citrix ADCの分割トンネリングルールを上書きしません。

デフォルトでは、Secure Webの**ネットワークアクセス**ポリシーは**内部ネットワークへのトンネル**に設定されています。この構成では、MDXアプリはCitrix ADCの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は、他のモバイル生産性アプリでは異なります。

Citrix Gatewayには、マイクロVPNリバース分割トンネルモードもあります。この構成は、Citrix ADCにトンネルされないIPアドレスの除外リストをサポートします。代わりに、これらのアドレスは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の詳細については、Citrix 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除外リスト**が含まれています。特定のWebサイトがCitrix Gatewayを介してトンネリングされるのを防ぐには、代わりに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リストを追加します。このリストは、リバース分割トンネリング用にCitrix Gatewayが構成されているSecure Browseモードにのみ適用されます。

認証

XenMobile®展開では、認証を構成する方法を決定する際にいくつかの考慮事項が関係してきます。このセクションでは、以下について説明することで、認証に影響を与えるさまざまな要因を理解するのに役立ちます。

- 認証に関わる主要なMDXポリシー、XenMobileクライアントプロパティ、およびCitrix Gateway設定。
- これらのポリシー、クライアントプロパティ、および設定がどのように相互作用するか。
- 各選択肢のトレードオフ。

この記事には、セキュリティレベルの向上に対応する推奨される構成の3つの例も含まれています。

概して言えば、セキュリティが強化されると、ユーザーはより頻繁に認証する必要があるため、ユーザーエクスペリエンスは最適ではなくなります。これらの懸念事項をどのようにバランスさせるかは、組織のニーズと優先順位に依存します。3つの推奨構成を確認することで、利用可能な認証手段の相互作用と、独自のXenMobile環境を最適に展開する方法について、より深く理解する必要があります。

認証モード

オンライン認証: ユーザーをXenMobileネットワークに許可します。インターネット接続が必要です。

オフライン認証: デバイス上で実行されます。ユーザーはセキュアボールトをロック解除し、ダウンロードされたメール、キャッシュされたWebサイト、メモなどの項目にオフラインでアクセスできます。

認証方法

シングルファクター

LDAP: XenMobileで、Lightweight Directory Access Protocol (LDAP) に準拠したActive Directoryなどの1つ以上のディレクトリへの接続を構成できます。これは、企業環境でシングルサインオン (SSO) を提供するためによく使用される方法です。LDAPでのユーザーエクスペリエンスを向上させつつ、登録時の複雑なパスワード、パスワードの有効期限、およびアカウントロックアウトのセキュリティを維持するために、Active Directoryパスワードキャッシュを使用したCitrix PINを選択することもできます。

詳細については、ドメインまたはドメインとSTAを参照してください。

クライアント証明書: XenMobileは業界標準の証明機関と統合して、証明書をオンライン認証の唯一の方法として使用できます。XenMobileは、ユーザー登録後にこの証明書を提供します。これには、ワンタイムパスワード、招待URL、またはLDAP資格情報のいずれかが必要です。クライアント証明書を主要な認証方法として使用する場合、デバイス上の証明書を保護するために、クライアント証明書のみの環境ではCitrix PINが必要です。

XenMobileは、サードパーティの証明機関に対してのみ証明書失効リスト (CRL) をサポートしています。Microsoft CAが構成されている場合、XenMobileはCitrix ADC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際は、Citrix ADCの証明書失効リスト (CRL) 設定である「CRL自動更新を有効にする」を構成する必要があるかどうかを検討してください。この手順により、MAM専用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いようにします。XenMobileは新しい証明書を再発行します。これは、証明書が失効した場合

でも、ユーザーがユーザー証明書を生成することを制限しないためです。この設定は、CRLが期限切れのPKIエンティティをチェックする際に、PKIエンティティのセキュリティを向上させます。

ユーザーに証明書ベースの認証を使用する予定がある場合、またはデバイス証明書の発行にエンタープライズ証明機関 (CA) を使用する必要がある場合に必要となる展開を示す図については、「オンプレミス展開の参照アーキテクチャ」を参照してください。

二要素認証

LDAP + クライアント証明書: 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あり、Citrix ADCでの二要素認証によって提供されるセキュリティと相まって、最高のSSOの可能性を提供します。LDAPとクライアント証明書の両方を使用することで、ユーザーが知っているもの (Active Directoryパスワード) と、ユーザーが持っているもの (デバイス上のクライアント証明書) の両方でセキュリティが提供されます。Secure Mail (およびその他のモバイル生産性向上アプリ) は、適切に構成されたExchangeクライアントアクセスサーバー環境で、クライアント証明書認証によるシームレスな初回ユーザーエクスペリエンスを自動的に構成および提供できます。最適な使いやすさのために、このオプションをCitrix PINとActive Directory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。最適な使いやすさのために、このオプションをCitrix PINとActive Directoryパスワードキャッシュと組み合わせることができます。

認証に関連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

以下のポリシー、設定、およびクライアントプロパティは、以下の3つの推奨構成で適用されます。

MDXポリシー

アプリのパスコード: オンの場合、アプリの起動時または一定期間の非アクティブ状態からの再開時に、Citrix PINまたはパスコードでアプリのロックを解除する必要があります。デフォルトは**オン**です。

すべてのアプリの非アクティブタイマーを構成するには、XenMobileコンソールの**設定**タブにある**クライアントプロパティ**で、INACTIVITY_TIMERの値を分単位で設定します。デフォルトは15分です。非アクティブタイマーを無効にして、アプリの起動時にのみPINまたはパスコードのプロンプトが表示されるようにするには、値をゼロに設定します。

> **注:**

暗号化キーポリシーで「オフラインを保護」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が必要: オンの場合、ユーザーはエンタープライズネットワークへの接続とアクティブなセッションを持っている必要があります。**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は必要ありません。デフォルトは**オフ**です。

最大オフライン期間 (時間): アプリの資格を再確認したり、XenMobileからポリシーを更新したりすることなく、アプリが実行できる最大期間を定義します。最大オフライン期間を設定すると、iOS用Secure Hubが有効なCitrix Gatewayトークンを持っている場合、アプリはユーザーに中断を与えることなく、XenMobileからMDXアプリの新しいポリシーを取得します。Secure Hubが有効なCitrix ADCトークンを持っていない場合、ユーザーはアプリポリシーを更新するためにSecure Hubを介して認証する必要があります。Citrix ADCトークンは、Citrix Gatewayセッションの非アクティブまたは強制セッションタイムアウトポリシーのために無効になる可能性があります。ユーザーがSecure Hubに再度サインオンすると、アプリの実行を継続できます。

期間が終了する30分前、15分前、5分前に、ユーザーにサインオンするよう通知されます。期限切れ後、ユーザーがサインオ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日間)**です。最小期間は1時間です。

注：

ユーザーが頻繁に移動し、国際ローミングを使用できるシナリオでは、デフォルトの72時間（3日間）では短すぎる可能性があることに留意してください。

バックグラウンドサービスチケットの有効期限： バックグラウンドネットワークサービスチケットが有効な期間。Secure MailがCitrix Gatewayを介してActiveSyncを実行しているExchange Serverに接続すると、XenMobileはSecure Mailが内部Exchange Serverに接続するために使用するトークンを発行します。このプロパティ設定は、Secure Mailが認証とExchange Serverへの接続のために新しいトークンを必要とせずにトークンを使用できる期間を決定します。制限時間が経過すると、ユーザーは新しいトークンを生成するために再度ログオンする必要があります。デフォルトは**168時間（7日間）**です。このタイムアウトが期限切れになると、メール通知は停止します。

オンラインセッション必須の猶予期間： オンラインセッション必須ポリシーによってそれ以上使用できなくなるまで（オンラインセッションが検証されるまで）、ユーザーがアプリをオフラインで使用できる分数。デフォルトは0（猶予期間なし）です。

認証ポリシーについては、以下を参照してください。

- MAM SDKを使用している場合：MAM SDKの概要
- MDX Toolkitを使用している場合：iOS用MDXポリシーおよびAndroid用MDXポリシー

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：** シンプルなサインオンエクスペリエンスのために、Citrix PINを有効にすることを選択できます。PINを使用すると、ユーザーはActive Directoryのユーザー名やパスワードなどの他の資格情報を繰り返し入力する必要がありません。Citrix PINは、スタンドアロンのオフライン認証としてのみ構成することも、PINとActive Directoryパスワードキャッシュを組み合わせて、最適な使いやすさのために認証を効率化することもできます。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Citrix PINを構成します。

以下は、いくつかの重要なプロパティの概要です。詳細については、「クライアントプロパティ」を参照してください。

ENABLE_PASSCODE_AUTH

表示名：Citrix PIN認証を有効にする

このキーを使用すると、Citrix PIN機能を有効にできます。Citrix PINまたはパスコードを使用すると、ユーザーはActive Directoryパスワードの代わりに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場合、またはXenMobileが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。

指定可能な値: true または **false**

既定値: false

ENABLE_PASSWORD_CACHING

表示名: ユーザーパスワードのキャッシュを有効にする

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にローカルで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、**ENABLE_PASSCODE_AUTH**キーもtrueに設定する必要があります。

指定可能な値: true または **false**

既定値: false

PASSCODE_STRENGTH

表示名: PINの強度要件

このキーは、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。

指定可能な値: Low、**Medium**、または **Strong**

既定値: Medium

INACTIVITY_TIMER

表示名: 非アクティブタイマー

このキーは、ユーザーがデバイスを非アクティブなままにしておき、Citrix PINまたはパスコードの入力を求められることなくアプリにアクセスできる時間を分単位で定義します。MDXアプリでこの設定を有効にするには、**App Passcode**設定を**On**にする必要があります。**App Passcode**設定が**Off**になっている場合、ユーザーはSecure Hubにリダイレクトされ、完全な認証を実行します。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適用されます。既定値は15分です。

ENABLE_TOUCH_ID_AUTH

表示名: Touch ID認証を有効にする

オフライン認証に指紋リーダー（iOSのみ）の使用を許可します。オンライン認証には、引き続きプライマリ認証方法が必要です。

ENCRYPT_SECRETS_USING_PASSCODE

表示名: パスコードを使用してシークレットを暗号化する

このキーを使用すると、機密データをiOSキーチェーンなどのプラットフォームベースのネイティブストアではなく、秘密の保管庫にモバイルデバイスに保存できます。この構成キーは、主要なアーティファクトの強力な暗号化を可能にするだけでなく、ユーザーエントロピー（ユーザーのみが知っているユーザー生成のランダムなPINコード）も追加します。

設定可能な値: true または **false**

デフォルト値: false

Citrix ADCの設定

セッションタイムアウト: この設定を有効にすると、Citrix ADCが指定された間隔でネットワークアクティビティを検出しない場合、Citrix Gatewayはセッションを切断します。この設定は、Citrix Gateway Plug-in、Citrix Receiver™、Secure Hub、またはWebブラウザ経由で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。この値をゼロに設定すると、この設定は無効になります。

強制タイムアウト: この設定を有効にすると、ユーザーが何をしていても、タイムアウト間隔が経過するとCitrix Gatewayはセッションを切断します。タイムアウト間隔が経過すると、ユーザーが切断を防ぐためにできるアクションはありません。この設定は、Citrix Gateway Plug-in、Citrix Receiver、Secure Hub、またはWebブラウザ経由で接続するユーザーに適用されます。Secure Mailが特別なCitrix ADCモードであるSTAを使用している場合、**強制タイムアウト**設定はSecure Mailセッションには適用されません。デフォルトは**1440分**です。この値を空白のままにすると、この設定は無効になります。

Citrix Gatewayのタイムアウト設定の詳細については、Citrix ADCのドキュメントを参照してください。

ユーザーがデバイスに資格情報を入力してXenMobileで認証するよう促されるシナリオの詳細については、「認証プロンプトのシナリオ」を参照してください。

デフォルトの構成設定

これらの設定は、以下によって提供されるデフォルトです。

- NetScaler® for XenMobile ウィザード
- MAM SDK または MDX Toolkit
- XenMobile コンソール

設定	設定の場所	既定の設定
セッションタイムアウト	シトリックス ゲートウェイ	1440 分
強制タイムアウト	シトリックス ゲートウェイ	1440 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限	MDXポリシー	168時間 (7日間)
オンラインセッションが必要	MDXポリシー	オフ
オンラインセッションが必要な猶予期間	MDXポリシー	0
アプリのパスコード	MDXポリシー	オン
パスコードを使用してシークレットを暗号化	XenMobileクライアントプロパティ	フォールス
Citrix PIN認証を有効にする	XenMobileクライアントプロパティ	偽
PINの強度要件	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	数字
ユーザーパスワードのキャッシュを有効にする	XenMobileクライアントプロパティ	偽
非アクティブタイマー	XenMobileクライアントプロパティ	15
Touch ID認証を有効にする	XenMobileクライアントプロパティ	偽

推奨される構成

このセクションでは、最低限のセキュリティと最適なユーザーエクスペリエンスから、最高のセキュリティとより介入的なユーザーエクスペリエンスまで、3つのXenMobile構成の例を挙げます。これらの例は、ご自身の構成をどのレベルに設定するかを決定するための役立つ参考情報と

なるはずです。これらの設定を変更すると、他の設定も変更する必要がある場合があります。たとえば、最大オフライン期間は常にセッションタイムアウトよりも短くする必要があります。

最高のセキュリティ

この構成は最高のセキュリティレベルを提供しますが、使いやすさにおいて大きなトレードオフを伴います。

設定	設定の場所	推奨設定	動作への影響
セッションタイムアウト	シトリックス ゲートウェイ	1440	ユーザーは、オンライン認証が必要な場合（24時間ごと）にのみSecure Hubの資格情報を入力します。
強制タイムアウト	シトリックス ゲートウェイ	1440	24時間ごとにオンライン認証が厳密に要求されます。アクティビティによって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	毎日ポリシーの更新が必要です。
バックグラウンドサービスチケットの有効期限	MDXポリシー	72時間	Citrix Gatewayセッショントークンなしで長期間のセッションを可能にするSTAのタイムアウト。Secure Mailの場合、STAタイムアウトをセッションタイムアウトよりも長く設定することで、セッションの有効期限が切れる前にユーザーがアプリを開かなかった場合に、ユーザーにプロンプトを

			表示せずにメール通知が停止するのを防ぎます。
オンラインセッションが必要	MDXポリシー	オフ	アプリを使用するための有効なネットワーク接続とCitrix Gatewayセッションを確保します。
オンラインセッション必須の猶予期間	MDXポリシー	0	猶予期間なし（オンラインセッション必須を有効にした場合）。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求します。
パスコードを使用してシークレットを暗号化する	XenMobileクライアントプロパティ	はい	ユーザーエントロピーから派生したキーがボールトを保護します。
Citrix PIN認証を有効にする	XenMobileクライアントプロパティ	はい	Citrix PINを有効にして、認証エクスペリエンスを簡素化します。
PINの強度要件	XenMobileクライアントプロパティ	強	高いパスワードの複雑さの要件。
PINタイプ	XenMobileクライアントプロパティ	英数字	PINは英数字のシーケンスです。
パスワードキャッシュを有効にする	XenMobileクライアントプロパティ	いいえ	Active Directoryパスワードはキャッシュされず、Citrix PINがオフライン認証に使用されます。

非アクティブタイマー	XenMobile クライアントプロパティ	15	ユーザーがこの期間中にMDXアプリまたはSecure Hubを使用しない場合、オフライン認証を要求します。
Touch ID認証を有効にする	XenMobile クライアントプロパティ	いいえ	iOSでのオフライン認証のユースケースに対してTouch IDを無効にします。

より高いセキュリティ

より中道的なアプローチとして、この構成では、ユーザーは（7日ごとではなく）最大3日ごとに認証を行う必要があり、より強力なセキュリティが求められます。認証回数が増えることで、コンテナがより頻繁にロックされ、デバイスが使用されていないときのデータセキュリティが確保されます。

設定	設定の場所	推奨設定	動作への影響
セッションタイムアウト	シトリックス ゲートウェイ	4320	ユーザーは、オンライン認証が必要な場合（3日ごと）にのみSecure Hubの資格情報を入力します。
強制タイムアウト	シトリックス ゲートウェイ	値なし	アクティビティがある場合、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日ごとにポリシーの更新が必要です。時間の差は、セッションタイムアウト前に更新を許可するためです。

バックグラウンドサービスチケットの有効期限	MDXポリシー	168時間	STAのタイムアウト。これにより、Citrix Gatewayセッショントークンなしで長期間のセッションが可能になります。Secure Mailの場合、STAのタイムアウトをセッションタイムアウトよりも長くすることで、セッションの有効期限が切れる前にユーザーがアプリを開かなかったとしても、ユーザーにプロンプトを表示せずにメール通知が停止するのを防ぎます。
オンラインセッションが必要	MDXポリシー	オフ	アプリを使用するために、有効なネットワーク接続とCitrix Gatewayセッションを確保します。
オンラインセッション必須の猶予期間	MDXポリシー	0	猶予期間なし (オンラインセッション必須を有効にした場合)。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求します。
パスコードを使用してシークレットを暗号化する	XenMobileクライアントプロパティ	フォールス	ボールトを暗号化するためにユーザーエントロピーを要求しません。
Citrix PIN認証を有効にする	XenMobileクライアントプロパティ	真	認証エクスペリエンスを簡素化するため

			にCitrix PINを有効にします。
PINの強度要件	XenMobileクライアントプロパティ	中	中程度のパスワード複雑性ルールを適用します。
PINの種類	XenMobileクライアントプロパティ	数字	PINは数字のシーケンスです。
パスワードキャッシュを有効にする	XenMobileクライアントプロパティ	真	ユーザーPINはActive Directoryパスワードをキャッシュし、保護します。
非アクティブタイマー	XenMobileクライアントプロパティ	30	ユーザーがこの期間中にMDXアプリまたはSecure Hubを使用しない場合、オフライン認証を要求します。
Touch ID認証を有効にする	XenMobileクライアントプロパティ	真	iOSでのオフライン認証ユースケースに対してTouch IDを有効にします。

高セキュリティ

この構成は、ユーザーにとって最も便利であり、ベースレベルのセキュリティを提供します。

設定	設定の場所	推奨設定	動作への影響
セッションタイムアウト	シトリックス ゲートウェイ	10080	ユーザーは、オンライン認証が必要な場合（7日ごと）にのみSecure Hubの資格情報を入力します。

強制タイムアウト	シトリックス ゲートウェイ	値なし	アクティビティがある場合、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）ポリシーの更新が必要です。時間の差は、セッションタイムアウトより前に更新を許可するためです。
バックグラウンドサービスチケットの有効期限	MDXポリシー	240	STAのタイムアウト。これにより、Citrix Gatewayセッショントークンなしで長期間のセッションが可能になります。Secure Mailの場合、STAのタイムアウトをセッションのタイムアウトよりも長く設定することで、セッションの有効期限が切れる前にユーザーがアプリを開かなかった場合に、ユーザーにプロンプトを表示することなくメール通知が停止するのを防ぎます。
オンラインセッションが必要	MDXポリシー	オフ	アプリを使用するための有効なネットワーク接続とCitrix Gatewayセッションを保証します。
オンラインセッションが必要な猶予期間	MDXポリシー	0	猶予期間なし（オンラインセッションが

			必要を有効にした場合）。
アプリのパスコード	MDXポリシー	オン	アプリケーションにパスコードを要求します。
パスコードを使用してシークレットを暗号化	XenMobileクライアントプロパティ	いいえ	ボールトを暗号化するためにユーザーエントロピーを要求しない。
Citrix PIN認証を有効にする	XenMobileクライアントプロパティ	はい	簡素化された認証エクスペリエンスのためにCitrix PINを有効にする。
PINの強度要件	XenMobileクライアントプロパティ	低	パスワードの複雑さの要件なし
PINタイプ	XenMobileクライアントプロパティ	数値	PINは数値シーケンスです。
パスワードキャッシュを有効にする	XenMobileクライアントプロパティ	はい	ユーザーPINはActive Directoryパスワードをキャッシュし、保護します。
非アクティブタイマー	XenMobileクライアントプロパティ	90	ユーザーがこの期間中にMDXアプリまたはSecure Hubを使用しない場合、オフライン認証を要求します。
Touch ID認証を有効にする	XenMobileクライアントプロパティ	はい	iOSでのオフライン認証ユースケースに対してTouch IDを有効にします。

ステップアップ認証の使用

一部のアプリでは、強化された認証（たとえば、トークンや積極的なセッションタイムアウトなどの二次認証要素）が必要になる場合があります。この認証方法はMDXポリシーを通じて制御します。この方法では、認証方法を制御するための個別の仮想サーバー（同じCitrix ADCアプライアンス上または別のアプライアンス上）も必要です。

設定	設定の場所	推奨設定	動作への影響
代替シトリックスゲートウェイ	MDXポリシー	セカンダリCitrix ADCアプライアンスのFQDNとポートが必要です。	セカンダリCitrix ADCアプライアンスの認証ポリシーとセッションポリシーによって制御される、強化された認証を可能にします。

ユーザーが代替Citrix Gatewayインスタンスにログオンするアプリを開くと、他のすべてのアプリはそのCitrix Gatewayインスタンスを使用して内部ネットワークと通信します。セッションは、強化されたセキュリティを持つCitrix Gatewayインスタンスからのセッションがタイムアウトした場合にのみ、セキュリティレベルの低いCitrix Gatewayインスタンスに切り替わります。

オンラインセッション必須の使用

Secure Webなどの特定のアプリケーションでは、ユーザーが認証済みセッションを持ち、デバイスがネットワークに接続されている場合にのみアプリを実行するようにしたい場合があります。このポリシーはそのオプションを強制し、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	設定の場所	推奨設定	動作への影響
オンラインセッション必須	MDXポリシー	オン	デバイスがオンラインであり、有効な認証トークンを持っていることを確認します。
オンラインセッション必須の猶予期間	MDXポリシー	15	ユーザーがアプリを使用できなくなる前に、15分間の猶予期間を許可します。

オンプレミス展開の参照アーキテクチャ

この記事の図は、オンプレミスでのXenMobile展開の参照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のみ、MAMのみ、MDM+MAMが含まれ、SNMP Manager、Exchange ActiveSync用Citrix Gateway connector™、Exchange ActiveSync用Endpoint Management connector、Virtual Apps and Desktopsなどのコンポーネントを含むものも含まれます。これらの図は、XenMobileに必要な最小限のコンポーネントを示しています。

この図を、展開の決定を行う際の一般的なガイドとして使用してください。

展開決定の図(/en-us/xenmobile/server/media/ra-decision-tree.png)

図中のコネクタ上の数字は、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ドキュメントのポート要件を参照してください。

コアMDMのみの参照アーキテクチャ

XenMobileのMDM機能のみを使用する予定がある場合は、このアーキテクチャを展開します。たとえば、MDMを介して企業支給デバイスを管理し、デバイスポリシーやアプリを展開し、資産インベントリを取得し、デバイスワイプなどのデバイスに対するアクションを実行できるようにする必要がある場合です。

コアMDMのみの参照アーキテクチャの図(/en-us/xenmobile/server/media/architecture-mdm-only.png)

コアMAMのみの参照アーキテクチャ

デバイスをMDMに登録せずにXenMobileのMAM機能のみを使用する予定がある場合は、このアーキテクチャを展開します。たとえば、BYOモバイルデバイス上のアプリとデータを保護したい場合、エンタープライズモバイルアプリを配信し、アプリをロックしてデータをワイプしたい場合などです。これらのデバイスはMDMに登録できません。

コアMAMのみの参照アーキテクチャの図(/en-us/xenmobile/server/media/architecture-mam-only.png)

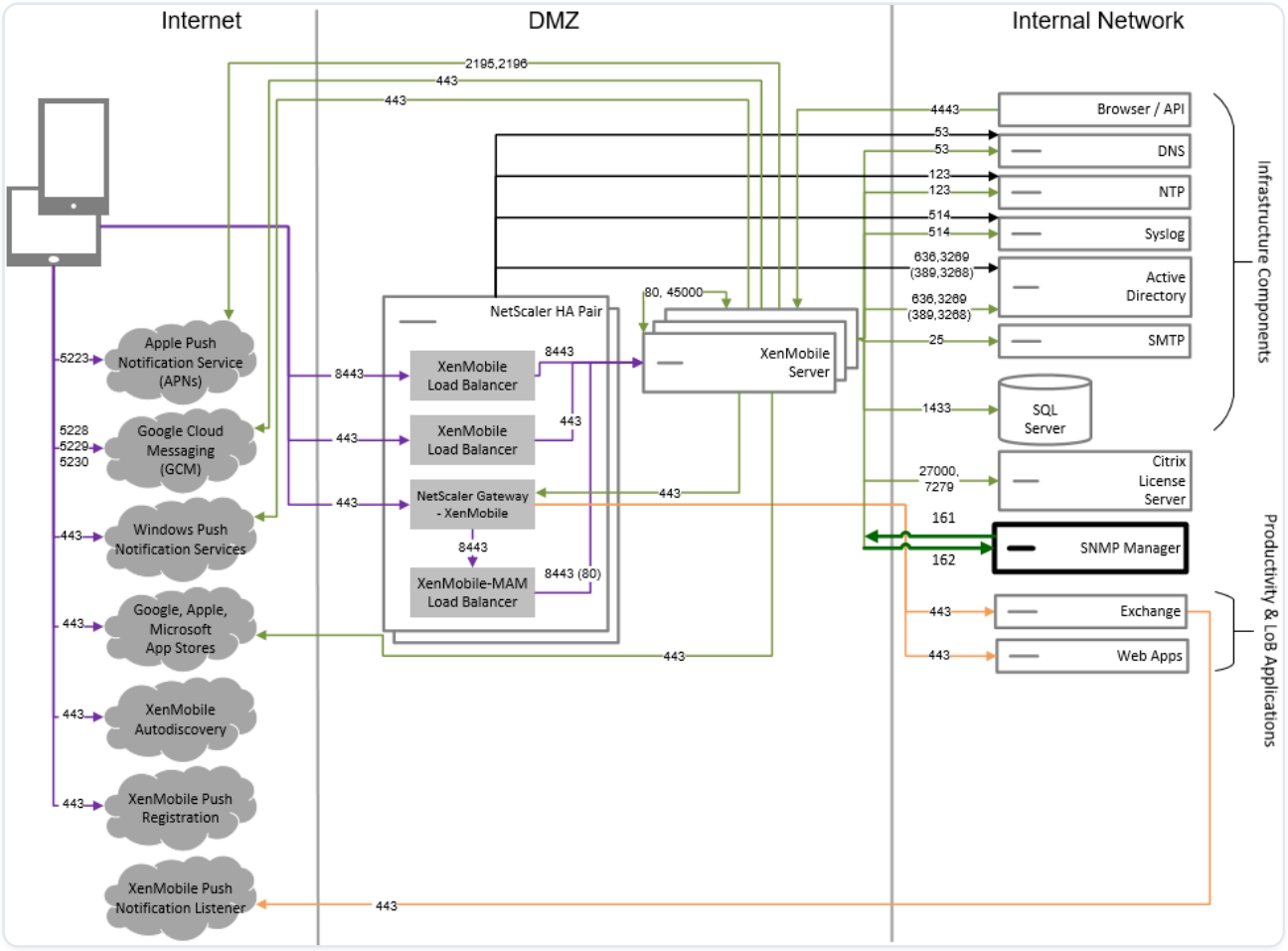
コアMAM+MDM参照アーキテクチャ

XenMobileのMDM+MAM機能を使用する予定がある場合は、このアーキテクチャを展開します。たとえば、MDMを介して企業支給デバイスを管理したい場合、デバイスポリシーやアプリを展開し、資産インベントリを取得し、デバイスをワイプしたい場合などです。また、エンタープライズモバイルアプリを配信し、アプリをロックしてデバイス上のデータをワイプしたい場合も含まれます。

コアMAM+MDM参照アーキテクチャの図(/en-us/xenmobile/server/media/architecture-mdm-mam.png)

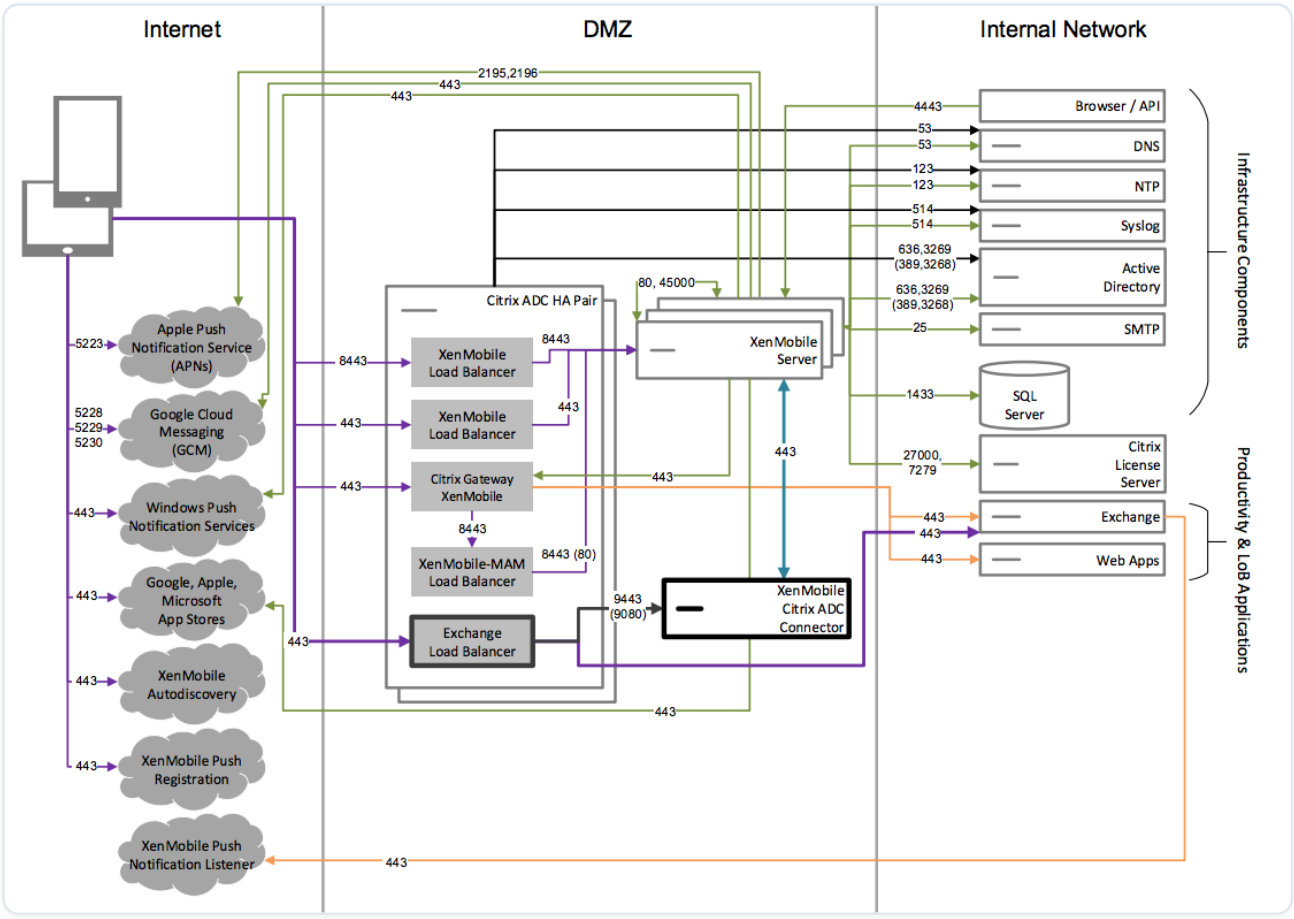
SNMPを含む参照アーキテクチャ

XenMobileでSNMP監視を有効にする予定がある場合は、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ノードに関する情報を照会および取得できるようにしたい場合などです。詳細については、SNMP監視を参照してください。



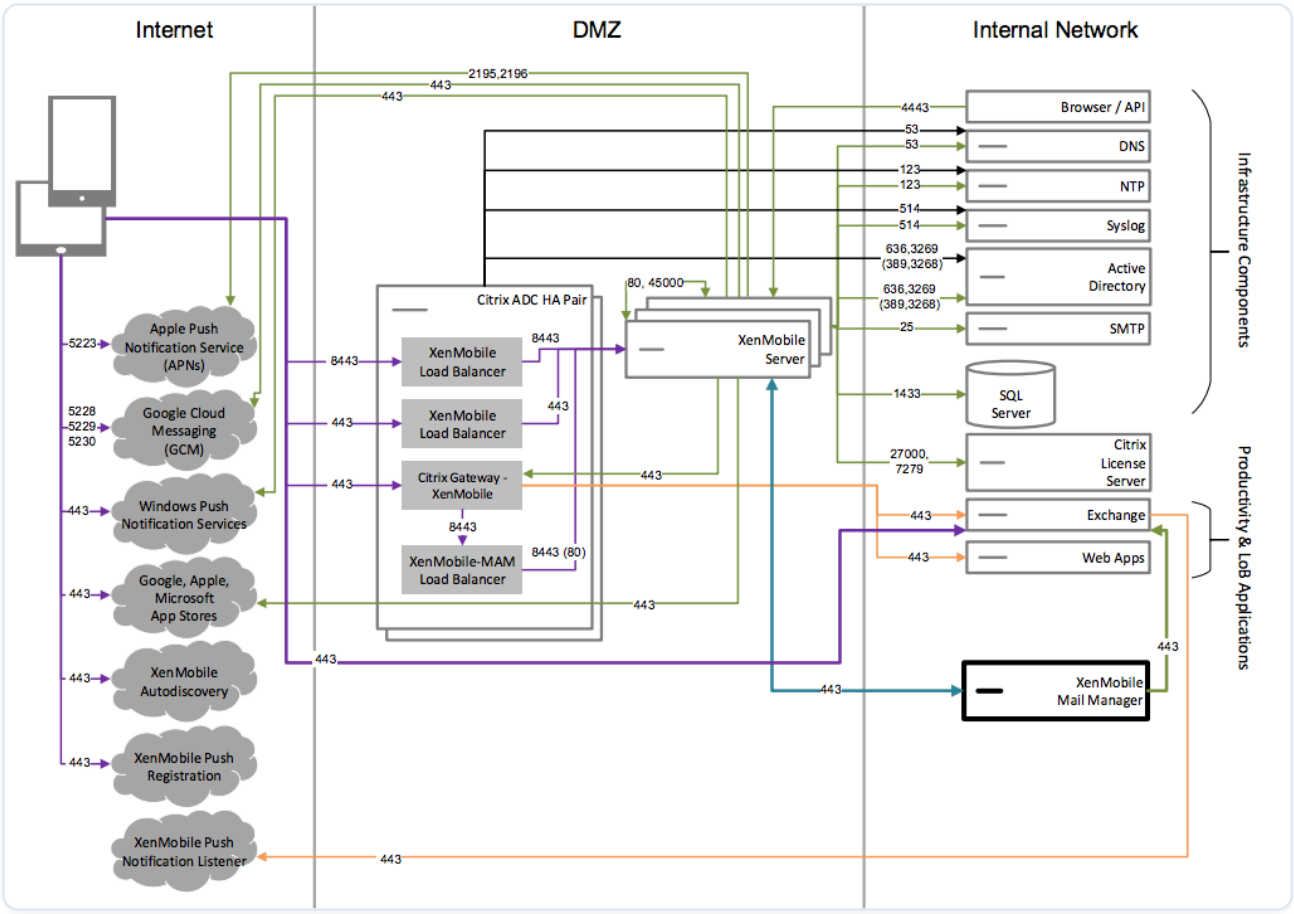
Exchange ActiveSync用Citrix Gatewayコネクタを使用したリファレンスアーキテクチャ

XenMobileでExchange ActiveSync用Citrix Gatewayコネクタを使用する予定がある場合は、このアーキテクチャを展開します。たとえば、ネイティブのモバイルメールアプリを使用するユーザーに安全なメールアクセスを提供する必要がある場合などです。これらのユーザーは引き続きネイティブアプリを介してメールにアクセスするか、時間をかけてCitrix Secure Mailに移行させることができます。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。図ではExchange ActiveSync用コネクタがMDMおよびMAMアーキテクチャに展開されていることを示していますが、MDMのみのアーキテクチャの一部としてExchange ActiveSync用コネクタを同様の方法で展開することもできます。



Exchange ActiveSync用Endpoint Managementコネクタを使用したリファレンスアーキテクチャ

XenMobileでExchange ActiveSync用Endpoint Managementコネクタを使用する予定がある場合は、このアーキテクチャを展開します。たとえば、ネイティブのモバイルメールアプリを使用するユーザーに安全なメールアクセスを提供したい場合などです。これらのユーザーは引き続きネイティブアプリを介してメールにアクセスするか、時間をかけてSecure Mailに移行させることができます。Exchange ActiveSyncサーバーでアクセス制御を実現できます。図ではExchange ActiveSync用Endpoint ManagementコネクタがMDMおよびMAMアーキテクチャに展開されていることを示していますが、MDMのみのアーキテクチャの一部としてExchange ActiveSync用Endpoint Managementコネクタを同様の方法で展開することもできます。

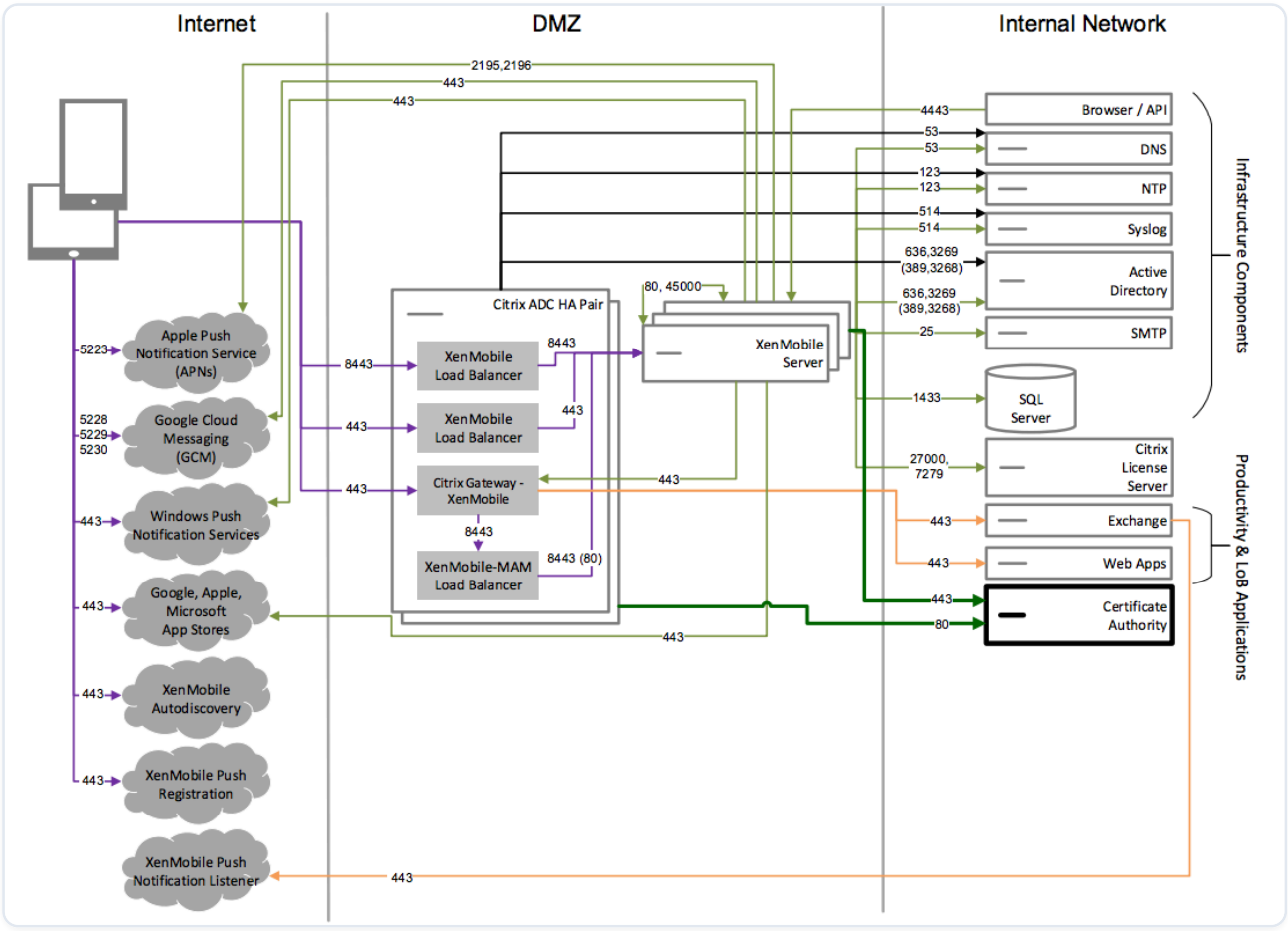


外部証明機関を使用したリファレンスアーキテクチャ

外部証明機関を含む展開は、以下の要件の1つ以上を満たすために推奨されます。

- Citrix Gatewayへのユーザー認証（イントラネットアクセス用）にユーザー証明書が必要です。
- Secure Mailユーザーがユーザー証明書を使用してExchange Serverに認証することを要求します。
- たとえば、Wi-Fiアクセス用に、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する必要があります。

図では外部証明機関がMDM+MAMアーキテクチャに展開されていることを示していますが、MDMのみまたはMAMのみのアーキテクチャの一部として、外部証明機関を同様の方法で展開することもできます。



Virtual Apps and Desktops を使用したリファレンスアーキテクチャ

Virtual Apps and Desktops を XenMobile と統合する予定がある場合は、このアーキテクチャを展開します。たとえば、あらゆる種類のアプリケーション (モバイル、SaaS、Windows) の統合アプリストアをモバイルユーザーに提供する必要がある場合などです。図では、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、MAM 専用アーキテクチャの一部として、同じ方法でこれらのデスクトップを展開することもできます。

Virtual Apps and Desktops を使用したリファレンスアーキテクチャの図(/en-us/xenmobile/server/media/architecture-xenapp-xendesktop.png)

内部ネットワークに XenMobile を配置したリファレンスアーキテクチャ

以下の要件のいずれかまたは複数を満たすために、内部ネットワークに XenMobile を配置したアーキテクチャを展開できます。

- DMZ にハイパーバイザーがない、または配置が許可されていない。
- DMZ にはネットワークアプライアンスのみを含めることができる。
- セキュリティ要件により、SSL オフロードの使用が必要である。

内部ネットワークに XenMobile を配置したリファレンスアーキテクチャの図(/en-us/xenmobile/server/media/architecture-internal-network.png)

ShareFile を使用したリファレンスアーキテクチャ

Citrix Files またはストレージゾーンコネクタのみを XenMobile と統合する場合は、このアーキテクチャを展開します。Citrix Files 統合により、以下の要件のいずれかまたは複数を満たすことができます。

- ユーザーに ShareFile.com へのシングルサインオン (SSO) を提供するために 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。

ストレージゾーンコネクタのみとの統合により、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 サブドメインを設定したり、ユーザーを Citrix Files にプロビジョニングしたり、Citrix Files データをホストしたりする必要はありません。

図ではCitrix FilesがMDM+MAMアーキテクチャに展開されていると示されていますが、MAM専用アーキテクチャの一部として、Citrix Filesを同じ方法で展開することもできます。

Citrix Filesを使用したリファレンスアーキテクチャの図(/en-us/xenmobile/server/media/reference-architecture-sharefile-storagezones.png)

サーバープロパティ

サーバープロパティは、XenMobile®インスタンス全体にわたる操作、ユーザー、デバイスに適用されるグローバルプロパティです。Citrix®は、この記事で説明されているサーバープロパティを環境に合わせて評価することを推奨します。他のサーバープロパティを変更する前に、必ずCitrixに相談してください。

一部のサーバープロパティを変更すると、各ノードの再起動が必要になります。XenMobileは、再起動が必要な場合に通知します。

一部のサーバープロパティは、パフォーマンスと安定性の向上に役立ちます。詳細については、「XenMobile操作のチューニング」を参照してください。

レガシーAndroidアプリをAndroid Enterpriseデバイスに配信する: `afw.allow.legacy.apps` が `true` に設定されている場合、Android EnterpriseデバイスはレガシーAndroidアプリとAndroid

Enterpriseアプリの両方を受け取ります。`false`の場合、Android EnterpriseデバイスはAndroid Enterpriseアプリのみを受け取ります。デフォルトは`true`です。

ファイルポリシーのファイル拡張子を許可する: 管理者がファイルデバイスポリシーを使用してアップロードできるファイルタイプのコンマ区切りリストで`file.extension.allowlist`を構成します。次のファイルタイプは、この許可リストに追加してもアップロードできません。

- .キャブ
- .アップエックス
- .アイピーエー
- .エーピーケー
- .エックスエーピー
- .エムディーエックス
- .イーエックスイー

デフォルト値は
`7z,rar,zip,csv,xls,xlsx,jad,jar,pdf,bmp,gif,jpg,png,pps,ppt,pptx,bsh,js,lua,mscr,pl,py,rb,`
です。

管理対象Google Playストア内のすべてのアプリにアクセスする: `true`の場合、XenMobileは公開Google Playストアのすべてのアプリを管理対象Google Playストアからアクセス可能にします。このプロパティを`true`に設定すると、すべてのAndroid Enterpriseユーザーが公開Google Playストアアプリを利用できるようになります。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。

企業所有デバイスのAndroid Enterpriseワークプロファイル登録:
`afw.work_profile_for_corporate_owned_device.enrollment_mode.enabled`が`true`に設定されている場合、Android 11以降を実行しているデバイスは、企業所有デバイスのワークプロファイル (WPCOD) モードに登録できます。コンソールには、この登録モードの変更が反映されます。`false`に設定されている場合、WPCOD設定は利用できません。デフォルト値は`true`です。

追加のAndroid Enterprise制限設定: プロパティ`afw.restriction.policy.v2`が`true`に設定されている場合、Android Enterpriseデバイスで次の制限設定が利用可能です。

- アプリのアンインストールを許可する
- Bluetooth共有を許可する

これらの設定の詳細については、「制限デバイスポリシー」を参照してください。

COPEデバイスのAndroid Enterprise制限: 制限デバイスポリシーで「**ワークプロファイルを持つ完全に管理されたデバイスに適用/企業所有デバイスのワークプロファイル**」設定を有効にするには、`afw.restriction.cope` を `true` に設定します。デフォルトは `true` です。この設定の詳細については、「制限デバイスポリシー」を参照してください。

iOS App Storeリンクのホスト名を許可: プロパティ `ios.app.store.allowed.hostnames` は、公開APIを使用して公開App Storeアプリをサーバーにアップロードする際に使用される許可されたホスト名のリストです。サーバーを介してアプリをアップロードするのではなく、公開APIを使用して公開App Storeアプリをアップロードする予定がある場合は、このプロパティを構成してください。デフォルト値は `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com` です。

代替APNsポート: `api.push.apple.com` からAPNs通知を送受信するために、ポート443の代わりにポート2197を使用できます。このポートはHTTP/2ベースのAPNsプロバイダーAPIを使用します。ポート2197を使用するには、プロパティ `apns.http2.alternate.port.enabled` を `true` に設定します。サーバープロパティ `apns.http2.alternate.port.enabled` のデフォルト値は `false` です。

弱いパスワードを持つローカルユーザーを防止するためのパスワード検証を有効にする: `enable.password.strength.validation` が `true` に設定されている場合、弱いパスワードを持つローカルユーザーを追加することはできません。`false` に設定されている場合、弱いパスワードを持つローカルユーザーを作成できます。デフォルトは `true` です。

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: 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。デフォルトは `true` です。すべてのセキュリティレベルで推奨される設定は `true` です。

登録が必要: `wsapi.mdm.required.flag` は、モードがENTの場合にのみ適用され、ユーザーにMDMへの登録を要求す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。登録を要求すると、より高いレベルのセキュリティが提供されます。ただし、その決定はMDMを要求するかどうかによって異なります。デフォルトでは、登録は必須ではありません。

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、XenMobile Storeを通じてデバイス上のアプリに引き続きアクセスできます。このプロパティが `true` の場合、登録を拒否したユーザーはすべてのアプリへのアクセスを拒否されます。

ユーザーが登録した後にこのプロパティを変更した場合、ユーザーは再登録する必要があります。

MDM登録を要求するかどうかについての議論は、「デバイス管理とMDM登録」を参照してください。

マルチモード登録を有効にする: プロパティ `enable.multimode.xms` を使用すると、1つのXenMobile Serverで、AndroidおよびiOSデバイスのデバイス管理とアプリ管理の両方の登録設定を制御する登録プロファイルを作成できます。また、新しい拡張登録プロファイル機能により、Androidの専用デバイスの登録と、AndroidおよびiOSデバイスのMAMのみの登録が可能になります。このプロパティが `false` の場合、登録プロファイルを設定する際にこれらの登録オプションは利用できません。デフォルト値は `true` です。このプロパティが `true` のときに登録されたデバイスは、プロパティを `false` に変更しても引き続き機能します。

セルフヘルプポータルを有効にする: `shp.console.enable` が `false` の場合、セルフヘルプポータルへのアクセスが禁止されます。ポート443でセルフヘルプポータルにアクセスするユーザーは404エラーを受け取ります。ポート4443でポータルにアクセスするユーザーは「アクセス拒否」メッセージを受け取ります。`true` の場合、ポート443経由でセルフヘルプポータルへのアクセスを提供します。デフォルトは `false` です。

ローカルユーザーアカウントのロックアウト制限: 制限ポリシーを使用すると、Active Directoryユーザーのサインイン試行回数に制限を設定できます。ローカルユーザーアカウントに対しても同様に、キー `local.user.account.lockout.limit` を使用します。ユーザーが指定した回数サインインを試行すると、一定の時間が経過するまで再試行できなくなります。その時間は、**ローカルユーザーアカウントのロックアウト時間**プロパティで設定します。デフォルト値は `6` です。

ローカルユーザーアカウントのロックアウト時間: プロパティ `local.user.account.lockout.time` を使用すると、ロックアウトされたローカルユーザーアカウントが再度サインインを試行できるようになるまでに経過する必要がある分数を設定できます。デフォルト値は `30` 分です。

ファイルアップロード制限の最大サイズを有効にする: アップロードの最大ファイルサイズを制限するには、設定 `max.file.size.upload.restriction` を `true` に設定して有効にします。この制限を有効にする場合、`max.file.size.upload.allowed` を使用して最大ファイルサイズを設定します。このプロパティのデフォルト値は `true` です。

許可されるファイルアップロードの最大サイズ: `max.file.size.upload.allowed` を使用すると、すべてのアップロードの最大ファイルサイズを指定できます。例としては、`500 B`、`1 KB`、`1 MB`、`1 MiB`、`1 G`、または `1 GiB` があります。デフォルト値は `5 MB` です。

非アクティブタイムアウト（分）: XenMobile Server Public APIを使用してXenMobileコンソールまたはサードパーティ製アプリにアクセスした非アクティブなユーザーをXenMobileがログアウトするまでの分数です。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製アプリの場合、ログイン状態を維持することが通常必要です。デフォルトは`5`です。

iOSデバイス管理登録で必要に応じてルートCAをインストール: Appleの最新の登録ワークフローでは、ユーザーがMDMプロファイルを手動で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への手動登録中、iOSデバイスユーザーは登録中にMDMデバイス証明書のプロンプトのみを受け取ります。

手動登録中のユーザーエクスペリエンスを向上させるため、Citrixはサーバープロパティ`ios.mdm.enrollment.installRootCaIfRequired`を**False**に変更することを推奨します。デフォルト値は**True**です。この変更により、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インストールが簡素化されます。

VPPベースライン間隔: プロパティ`vpp.baseline`は、XenMobileがAppleからボリューム購入ライセンスを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で、インポートされたアプリをボリューム購入から手動で削除した場合など、すべての変更がXenMobileに反映されるようになります。デフォルトでは、XenMobileはボリューム購入ライセンスのベースラインを最低でも`1440`分ごとに更新します。

多数のボリューム購入ライセンス（例えば50,000以上）がインストールされている場合、Citrixはライセンスのインポートのオーバーヘッドを減らすためにベースライン間隔を増やすことを推奨します。Appleからのボリューム購入ライセンスの変更が頻繁に予想される場合、CitrixはXenMobileを最新の状態に保つために値を下げることを推奨します。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60分ごとに実行されるため、ボリューム購入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分遅れる可能性があります。

XenMobile MDMセルフヘルプポータルコンソールの最大非アクティブ間隔（分）: このプロパティ名は、以前のXenMobileバージョンを反映しています。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、XenMobileが非アクティブなユーザーをXenMobileコンソールからログアウトするまでの分数です。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。

Nexmo SMSゲートウェイのサポート廃止: プロパティ`deprecate.carrier.sms.gateway`は、デフォルトで**True**に設定されているNexmo SMSゲートウェイのサポートを削除します。Nexmo SMSはセルフヘルプポータルでも廃止されています。

モバイルサービスプロバイダー（MSP）インターフェイスのサポート廃止: プロパティ`deprecate.mobile.service.provider`は、デフォルトで**True**に設定されているMSPインターフェイスをコンソールから削除します。

Windows Information Protectionポリシーのサポート廃止: Windowsの発表に従い、Windows Information Protection (WIP) のサポートは廃止されました。サーバープロパティ `windows.wip.deprecation` は、デフォルトで**True**に設定されているWIPのサポートを削除します。

Android EnterpriseのOS更新制御ポリシーにおける「Control Enterprise FOTA」フィールドのサポート廃止: プロパティ `afw.disable.osupdate.efota` が**True**に設定されている場合、Android EnterpriseのOS更新制御ポリシーにおける**Control Enterprise FOTA**フィールドは廃止されます。デフォルト値は**True**に設定されています。

macOSデバイス上のエンタープライズアプリのサポート: プロパティ `mac.app.push` が**True**に設定されている場合、macOSを実行しているデバイスにダウンロードされると、エンタープライズアプリが自動的にインストールされます。デフォルト値は**True**に設定されています。

iOSデバイスでのeSIMのサポート: プロパティ `ios.esim.support` が**True**に設定されている場合、XenMobile ServerはiOSデバイスからeSIM情報を取得し、eSIM関連のデバイスプロパティをユーザーインターフェイスに表示します。

Android Enterpriseの802.1x設定におけるWi-Fiポリシーの「ドメイン」フィールドのサポート: プロパティ `afw.network.domain.support` が**True**に設定されている場合、**Android Enterpriseの802.1x設定**に***ドメイン***フィールドが追加されます。

iOSにおけるオプションアプリの自動更新のサポート: `apple.ios.optional_app_update` プロパティが**True**に設定されている場合、Citrix Secure Hubストアからサブスクライブされたi OSのオプションアプリも自動的に更新されます。デフォルト値は**False**に設定されています。

アプリ展開試行回数合計とインストール済みアプリ上位100件のデバイスレポートの機能強化: プロパティ `device.report.enhancement.enabled` が**True**に設定されている場合、**アプリ展開試行回数合計**に**オペレーティングシステムバージョン**と**デバイスモデル**の2つの新しい列が追加され、各プラットフォームにインストールされている上位100個のアプリを表示する新しいデバイスレポート**インストール済みアプリ上位100件**が追加されます。

iPhoneおよびiPadのReturn to Serviceのサポート: プロパティ `ios.mdm.return.to.service` が**True**に設定されている場合、iOS 17以降を実行しているiPhoneおよびiPadでReturn to Service機能を使用できます。このプロパティのデフォルト設定は**True**です。

Android EnterpriseのVPNポリシーにおける常時接続VPNオプションのサポート: プロパティ `afw.policy.vpn_always_on_lockdown` が**True**に設定されている場合、Android Enterpriseプラットフォームの**VPN**ポリシーに**常時接続VPNを有効にする**と**ロックダウンを有効にする**オプションが追加されます。デフォルト値は**True**です。

Android Enterpriseのオプションポリシーにおける常時接続VPNオプションのサポートの廃止: プロパティ`afw.policy.hide_vpn_always_on`は、Android Enterpriseプラットフォームの**XenMobileオプション**ポリシーから**常時接続VPN**オプションを削除します。デフォルト値は**True**です。

レガシーMDX廃止アラート: プロパティ`legacy.mdx.deprecation.alert`が**True**に設定されている場合、レガシーMDXモードのMDXアプリが公開されていると、XenMobile Serverコンソールにアラートが表示されます。デフォルト値は**True**です。

新しいHTTP v1 APIを使用するように移行されたFirebase Cloud Messagingのサポート: プロパティ`afw.fcm.httpv1.migration`が**True**に設定されている場合、新しいHTTP v1 APIでFirebase Cloud Messagingを使用できます。デフォルト値は**False**です。

iPhoneおよびiPadのReturn to Serviceのサポート: プロパティ`ios.mdm.return.to.service`が**True**に設定されている場合、iOS 17以降を実行しているiPhoneおよびiPadでReturn to Service機能を使用できます。このプロパティのデフォルト設定は**True**です。

個人プロファイルから仕事用プロファイルのメールアプリにアクセスして使用するサポート: `afw.mailapp.crossworkprofile`プロパティが**True**に設定されている場合、Android Enterprise設定で個人プロファイルから仕事用プロファイルのメールアプリにアクセスして使用できる機能が有効になります。デフォルトは**True**です。

自動登録でのセットアップを完了するための最小OSバージョンの強制のサポート: `ios.mdm.minimum_os_version.enrollment`プロパティが**True**に設定されている場合、iOS 17以降の自動登録中にセットアップを完了するための最小OSバージョン要件を強制できます。デフォルトは**True**です。

Samsung Knox Enhanced Attestation v3のサポート: `afw.knox.attestation.v3`プロパティが**True**に設定されている場合、Samsung Knoxデバイスのセキュリティ機能を向上させることができます。デフォルトは**True**です。

Android Enterpriseで管理対象構成フィードバックを有効にする: `afw.app_managed_configurations.feedback`が**True**に設定されている場合、管理者は管理対象構成ポリシーで構成されたAndroidデバイスからアプリの状態に関するフィードバックを取得できます。**False**の場合、管理者はフィードバックを受け取りません。デフォルトは**False**です。

Android Enterprise管理対象構成フィードバックDBを更新するためのバッチサイズ: `android.managed.configuration.feedback.db.update.batch.size`が設定されている場合、Android Enterprise管理対象構成フィードバックDBを更新するためのバッチサイズを定義します。サイズはDBの機能に基づいて構成できます。デフォルト値は**100**で、最大値は**1000**です。

Android Enterprise管理対象構成フィードバックDBの更新時間間隔: `android.managed.configuration.feedback.db.update.time.interval`が設定されている場合、Android Enterprise管理対象構成フィードバックDBを更新するための時間間隔を定義します。デフォルトは**6**時間です。

Android Enterpriseポリシーのコンプライアンスを適用する: `afw.policy.compliance`プロパティが**True**に設定されている場合、デバイス所有者モードで登録されたAndroidデバイスは、管理者がデバイスのコンプライアンスを管理できるようにします。デフォルトは**False**です。

ABM MDMサーバーから割り当て解除されたときにXMSからABMデバイスを削除する: `remove.unassigned.abm.devices`が**true**の場合、XMSはこのサーバーに割り当てられなくなったデバイスを削除します。デフォルトは**false**です。

証明書ベースの認証のための新しい強力な証明書マッピングをサポートする: `all_platforms.certificate.strong.mapping`プロパティが**True**に設定されている場合、XenMobile ServerはMicrosoftからの新しい強力な証明書マッピングをサポートします。デフォルトは**True**です。

Android Enterpriseデバイスでの eSIMのサポート: `ae.esim.support`プロパティが**True**に設定されている場合、XenMobile ServerはAndroid Enterpriseデバイスから eSIM情報を取得し、eSIM関連のデバイスプロパティをユーザーインターフェイスに表示します。デフォルトは**True**です。

宣言型デバイス管理 (DDM) のサポート: `ios.mdm.declarative.management`プロパティが**True**に設定されている場合、XenMobile Serverコンソールで iOS宣言型管理ポリシーを構成できます。デフォルトは**False**です。

iOSソフトウェアアップデート強制のサポート: `ios.mdm.software.update.settings`プロパティが**True**に設定されている場合、XenMobile Serverコンソールでソフトウェアアップデート強制デバイスポリシーを構成できます。デフォルトは**False**です。

Android Enterpriseデバイスでのアプリの自動起動のサポート: `afw.launcher.auto_launch`プロパティが**True**に設定されている場合、ランチャー構成デバイスポリシーのAndroid Enterpriseデバイスで**アプリの自動起動**設定が利用可能になります。デフォルトは**False**です。

iOS 27 DDMポリシーのサポート: `ios.mdm.ios27.ddm.support`プロパティが**True**に設定されている場合、XenMobile Serverコンソールで iOS 27で導入されたiOS宣言型管理ポリシーを構成できます。デフォルトは**True**です。

デバイスおよびアプリのポリシー

XenMobile® のデバイスおよびアプリのポリシーを使用すると、次のような要素間のバランスを最適化できます。

- エンタープライズセキュリティ
- 企業データおよび資産の保護
- ユーザーのプライバシー
- 生産的で良好な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異なる場合があります。たとえば、金融などの規制の厳しい組織では、ユーザーの生産性が主な考慮事項となる教育や小売などの他の業界よりも、より厳格なセキュリティ制御が必要です。

ユーザーのID、デバイス、場所、接続タイプに基づいてポリシーを一元的に制御および構成し、企業コンテンツの悪意のある使用を制限できます。デバイスが紛失または盗難にあった場合、ビジネスアプリケーションとデータをリモートで無効化、ロック、またはワイプできます。全体的な結果として、セキュリティと管理制御を確保しながら、従業員の満足度と生産性を向上させるソリューションが実現します。

この記事の主な焦点は、セキュリティに関連する多くのデバイスおよびアプリのポリシーです。

セキュリティリスクに対処するポリシー

XenMobile のデバイスおよびアプリのポリシーは、次のようなセキュリティリスクをもたらす可能性のある多くの状況に対処します。

- ユーザーが信頼できないデバイスや予測不能な場所からアプリやデータにアクセスしようとする場合。
- ユーザーがデバイス間でデータを渡す場合。
- 許可されていないユーザーがデータにアクセスしようとする場合。
- 退職したユーザーが自身のデバイス (BYOD) を使用した場合。
- ユーザーがデバイスを紛失した場合。
- ユーザーが常に安全にネットワークにアクセスする必要がある場合。
- ユーザーが自分のデバイスを管理しており、仕事のデータと個人のデータを分離する必要がある場合。
- デバイスがアイドル状態であり、ユーザー資格情報の再検証が必要な場合。

- ユーザーが機密性の高いコンテンツを保護されていないメールシステムにコピー＆ペーストする場合。
- ユーザーが個人アカウントと会社アカウントの両方を持つデバイスで、機密データを含むメール添付ファイルやWebリンクを受信する場合。

これらの状況は、企業データを保護する際の2つの主要な懸念事項に関連しています。それは、データが次の状態にある場合です。

- 保存されている状態
- 転送中の状態

XenMobileが保存されているデータを保護する方法

モバイルデバイスに保存されているデータは、保存データ（data at rest）と呼ばれます。XenMobileは、iOSおよびAndroidプラットフォームが提供するデバイス暗号化を使用します。XenMobileは、Citrix MAM SDKを通じて利用できるコンプライアンスチェックなどの機能で、プラットフォームベースの暗号化を補完します。

XenMobileのモバイルアプリケーション管理（MAM）機能により、モバイル生産性アプリ、MDX対応アプリ、およびそれらに関連するデータの完全な管理、セキュリティ、制御が可能になります。

The Mobile Apps SDK enables apps for XenMobile deployment through use of the Citrix MDX app container technology. The container technology separates corporate apps and data from personal apps and data on a user device. The data separation allows you to secure any custom-developed, third-party, or BYO mobile app with comprehensive policy-based controls.

XenMobile also includes app-level encryption. XenMobile separately encrypts data stored within any MDX-enabled app without requiring a device passcode and without requiring that you manage the device to enforce the policy.

ポリシーとモバイルアプリSDKを使用すると、次のことが可能になります。

- ビジネスアプリと個人アプリ、およびデータを安全なモバイルコンテナに分離します。
- 暗号化やその他のモバイルデータ損失防止 (DLP) テクノロジーでアプリを保護します。

MDXポリシーは、多くの運用制御を提供します。MAM SDKが有効なアプリまたはMDXでラップされたアプリ間でシームレスな統合を可能にし、すべての通信を制御することもできます。このようにして、データがMAM SDKが有効なアプリまたはMDXでラップされたアプリのみによってアクセス可能であることを保証するなどのポリシーを適用できます。

デバイスおよびアプリのポリシー制御を超えて、保存データを保護する最善の方法は暗号化です。XenMobileは、MDX対応アプリに保存されているデータに暗号化レイヤーを追加し、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、暗号化除外などの機能に対するポリシー制御を提供します。Mobile Apps SDKは、保護されたCitrix Secret Vaultにキーが保存されたFIPS 140-2準拠のAES 256ビット暗号化を使用します。

XenMobileが転送中のデータを保護する方法

ユーザーのモバイルデバイスと社内ネットワーク間を移動するデータは、転送中のデータと呼ばれます。MDXアプリコンテナテクノロジーは、Citrix Gatewayを介して社内ネットワークへのアプリケーション固有のVPNアクセスを提供します。

従業員がモバイルデバイスから安全なエンタープライズネットワーク内にある以下のリソースにアクセスしたい状況を考えてみましょう。

- 会社のメールサーバー
- 企業イントラネットでホストされているSSL対応のWebアプリケーション
- ファイルサーバーまたはMicrosoft SharePointに保存されているドキュメント

MDXは、アプリケーション固有のマイクロVPNを介して、モバイルデバイスからこれらすべてのエンタープライズリソースへのアクセスを可能にします。各デバイスには、独自の専用マイクロVPNトンネルがあります。

マイクロVPN機能は、信頼できないモバイルデバイスのセキュリティを危険にさらす可能性のあるデバイス全体のVPNを必要としません。その結果、社内ネットワークは、企業システム全体に感染する可能性のあるマルウェアや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のモバイルアプリは、1つのデバイス上で共存できます。

さらに強力なレベルのセキュリティを提供するために、認証およびアプリとのマイクロVPNセッションに使用される代替Citrix GatewayポリシーでMDX対応アプリを構成できます。オンラインセッション必須ポリシーで代替Citrix Gatewayを使用して、アプリを特定のゲートウェイに再認証させることができます。このようなゲートウェイは通常、異なる（より高い保証の）認証要件とトラフィック管理ポリシーを持っています。

セキュリティ機能に加えて、マイクロVPN機能は、圧縮アルゴリズムを含むデータ最適化技術も提供します。圧縮アルゴリズムは、以下を保証します。

- 最小限のデータのみが転送されます
- 転送は可能な限り最速で行われます。速度はユーザーエクスペリエンスを向上させ、これはモバイルデバイス導入における主要な成功要因です。

次のような状況で、デバイスポリシーを定期的に再評価してください。

- デバイスのオペレーティングシステムアップデートのリリースにより、XenMobileの新しいバージョンに新規または更新されたポリシーが含まれる場合
- 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していますが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。その結果、iOS、Android、Windowsデバイス間、さらには異なるメーカーのAndroidデバイス間でも違いが見られる場合があります。
- 新しい企業セキュリティポリシーやコンプライアンス規制など、企業または業界の変化に合わせてXenMobileの運用を同期させるため
- MAM SDKの新しいバージョンに新規または更新されたポリシーが含まれる場合
- アプリを追加または更新する場合
- 新しいアプリや新しい要件の結果として、ユーザー向けの新しいワークフローを統合するため

アプリポリシーとユースケースシナリオ

Secure Hubを通じて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とどのように連携するかを定義したい場合もあるでしょう。アプリポリシーを使用してください：

- 一定期間が経過した後にユーザーに認証を要求する場合。
- ユーザーに情報へのオフラインアクセスを提供したい場合。

以下のセクションでは、いくつかのポリシーと使用例について説明します。

- MAM SDKを使用してiOSおよびAndroidアプリに統合できるサードパーティポリシーのリストについては、MAM SDKの概要を参照してください。
- 各プラットフォームのすべてのMDXポリシーのリストについては、「MDX Policies at a Glance」を参照してください。

認証ポリシー

- **デバイスパスコード**

  このポリシーを使用する理由: デバイスパスコードポリシーを有効にすると、デバイスでデバイスパスコード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なります。この機能により、デバイスレベルでのiOS暗号化の使用が保証されます。

  ユーザーの例: このポリシーを有効にすると、ユーザーはMDXアプリにアクセスする前に、iOSデバイスにパスコードを設定する必要があります。

- **アプリパスコード**

  このポリシーを使用する理由: アプリパスコードポリシーを有効にすると、Secure Hubは、ユーザーがアプリを開いてデータにアクセスする前に、管理対象アプリへの認証を求めるプロンプトを表示します。ユーザーは、XenMobile Serverの設定ので構成した内容に応じて、Active Directoryパスワード、Citrix PIN、またはiOS TouchIDで認証できます。クライアントプロパティで非アクティブタイマーを設定すると、継続して使用している場合でも、タイマーが期限切れになるまでSecure Hubが管理対象アプリへの認証を再度求めることはありません。

  アプリパスコードはデバイスパスコードとは異なります。デバイスにデバイスパスコードポリシーがプッシュされると、Secure Hubはユーザーにパスコードまたは PINの設定を促します。ユーザーは、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期限切れになったときに、デバイスにアクセスする前にそのパスコードまたはPINを解除する必要があります。詳細については、「Authentication in XenMobile」を参照してください。

  ユーザーの例: デバイスでCitrix Secure Web™アプリケーションを開く際、非アクティブ期間が期限切れになっている場合、ユーザーはWebサイトを閲覧する前にCitrix PINを入力する必要があります。

- **オンラインセッションが必要**

  このポリシーを使用する理由: アプリケーションの実行にWebアプリ（Webサービス）へのアクセスが必要な場合、このポリシーを有効にすると、XenMobileは、アプリを使用する前にエンタープライズネットワークに接続するか、アクティブなセッションを持つようにユーザーに促します。

  ユーザーの例: オンラインセッション必須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するまで、そのアプリを使用できません。

- **最大オフライン期間**

  このポリシーを使用する理由: このポリシーは、ユーザーがアプリの資格を再確認したり、XenMobileからポリシーを更新したりすることなく、長期間オフラインでアプリを実行できないようにするための追加のセキュリティオプションとして使用します。

  ユーザーの例: 最大オフライン期間を設定したMDXアプリを構成した場合、ユーザーはオフラインタイマー期間が終了するまでアプリをオフラインで開いて使用できます。その時点で、ユーザーは携帯電話またはWi-Fiサービスを介してネットワークに再接続し、プロンプトが表示された場合は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 で新しいバージョンがリリースされたアプリをユーザーが更新しなければならないまでの期間です。猶予期間が終了すると、ユーザーはアプリ内のデータにアクセスする前にアプリを更新する必要があります。この値を設定する際は、モバイルワーカー、特に海外旅行中に長期間オフラインになる可能性のあるワーカーのニーズを考慮してください。

  ユーザーの例: XenMobile Store に Secure Mail の新しいバージョンをロードし、アプリ更新猶予期間を 6 時間に設定します。すべての Secure Mail ユーザーは、6 時間が経過するまで Secure Mail アプリを更新するよう求めるメッセージを受け取ります。6 時間が経過すると、Secure Hub はユーザーを XenMobile Store に誘導します。

- **アクティブポーリング期間 (分)**

  このポリシーを使用する理由: アクティブポーリング期間とは、XenMobile がアプリのセキュリティアクション (アプリロックやアプリワイプなど) を実行するタイミングを確認する間隔です。

  ユーザーの例: アクティブポーリング期間ポリシーを 60 分に設定した場合、XenMobile からデバイスにアプリロック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 分以内にロックが実行されます。

非準拠デバイスの動作ポリシー

デバイスが最小限のコンプライアンス要件を下回った場合、非準拠デバイスの動作ポリシーにより、実行するアクションを選択できます。詳細については、「非準拠デバイスの動作」を参照してください。

アプリインタラクションポリシー

これらのポリシーを使用する理由: アプリインタラクション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とデータのフローを制御します。たとえば、ユーザーがコンテナ外の個人用アプリにデータを移動したり、コンテナ外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のを防ぐことができます。

ユーザーの例: アプリインタラクションポリシーを「制限付き」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、コンテナ外にある個人用の Safari または Chrome ブラウザにそのデータをコピーすることはできません。さらに、ユーザーは Secure Mail から添付されたドキュメントを Citrix Files または Quick Edit で開くことができます

が、コンテナ外にある個人用のファイル表示アプリで添付されたドキュメントを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を使用して、MDX アプリが開いている間にユーザーがアクセスできる機能を制御します。これにより、アプリの実行中に悪意のあるアクティビティ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 で若干異なります。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 NFC の使用を停止できます。

ユーザーの例: MDX アプリで iOS の音声入力をブロックするアプリ制限ポリシーを有効にすると、MDX アプリの実行中にユーザーは iOS キーボードの音声入力機能を使用できません。これにより、ユーザーが音声入力したデータは、安全で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ません。ユーザーがコンテナ外の個人用アプリを開くと、個人間の通信のために音声入力オプションが引き続き利用できます。

アプリ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: デバイス上のコンテナ内のMDXアプリから社内ネットワーク内のデータへのアクセスを提供するには、アプリネットワークアクセス ポリシーを使用します。ネットワークアクセス ポリシーでは、**内部ネットワークにトンネル接続**オプションを設定して、MDXアプリからCitrix ADCを介してバックエンドの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: ユーザーがトンネリングが有効になっているSecure WebなどのMDXアプリを開くと、ユーザーがVPNを開始する必要なく、ブラウザが開き、イントラネットサイトが起動します。Secure Webアプリは、マイクロVPNテクノロジー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と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とジオフェンシングを制御するポリシーには、中心点の経度、中心点の緯度、および半径が含まれます。これらのポリシーは、MDXアプリ内のデータへのアクセスを特定の地理的領域に制限します。これらのポリシーは、緯度と経度の座標の半径によって地理的領域を定義します。ユーザーが定義された半径の外でアプリを使用しようとすると、アプリはロックされたままで、ユーザーはアプリデータにアクセスできません。

ユーザーの例: ユーザーはオフィスにいる間、合併・買収データにアクセスできます。オフィスから移動すると、この機密データには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、Citrix Gatewayを介して接続するために、実質的にSOCKS5プロキシであるSecure Ticket Authority (STA) を使用します。STAは長期間の接続をサポートし、マイクロVPNと比較してバッテリー寿命を向上させます。したがって、STAは常に接続するメールに最適です。Citrixは、Secure Mailにこれらの設定を構成することを推奨します。XenMobile用Citrix ADCウィザードは、Secure Mail用にSTAを自動的にセットアップします。

  ユーザーの例: STAが有効になっていない状態でAndroidユーザーがSecure Mailを開くと、VPNを開くように求められ、そのVPNはデバイス上で開いたままになります。STAが有効になっている状態でAndroidユーザーがSecure Mailを開くと、Secure MailはVPNを必要とせずにシームレスに接続します。

- **デフォルトの同期間隔**

  このポリシーを使用する理由: この設定は、ユーザーがSecure Mailに初めてアクセスしたときにSecure Mailに同期されるメールのデフォルトの日数を指定します。2週間分のメールは3日分よりも同期に時間がかかり、ユーザーのセットアッププロセスを長引かせます。

  ユーザーの例: ユーザーがSecure Mailを初めてセットアップするときにデフォルトの同期間隔が3日に設定されている場合、受信トレイで現在から過去3日間に受信したメールを見ることができます。ユーザーが3日より古いメールを見たい場合は、検索を実行できます。Secure Mailは、サーバーに保存されている古いメールを表示します。Secure Mailのインストール後、各ユーザーは自分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

デバイスポリシーは、MDMポリシーとも呼ばれ、XenMobileがデバイスとどのように連携するかを決定します。多くのポリシーはすべてのデバイスに共通ですが、各デバイスにはそのオペレーティングシステムに固有のポリシーセットがあります。以下のリストには、いくつかのデバイスポリシーが含まれており、それらをどのように使用できるかについて説明しています。すべてのデバイスポリシーのリストについては、デバイスポリシー の記事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確認する必要がある場合は、デバイスにアプリインベントリポリシーを展開します。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

人でインストールしたアプリケーションは表示されません。企業デバイスで特定のアプリの実行をブロックしたい場合は、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管理対象デバイスのユーザーは、この機能を無効にできません。ユーザーが個人でインストールしたアプリケーションは、XenMobile管理者から見ることができます。

- **アプリロックポリシー**

  このポリシーを使用する理由: Androidの場合、アプリロックポリシーを使用すると、アプリをブロックまたは許可できます。たとえば、アプリを許可することで、キオスクデバイスを構成できます。通常、アプリロックポリシーは、ユーザーがインストールできるアプリを制限するため、企業所有デバイスにのみ展開します。ブロックされたアプリへのユーザーアクセスを提供するために、上書きパスワードを設定できます。

  ユーザーの例: Angry Birdsアプリをブロックするアプリロックポリシーを展開したとします。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ことを通知するメッセージが表示されます。

- **接続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、アプリプッシュ、およびポリシー展開のためにXenMobile Serverに接続できるように、接続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、XenMobile Serverへの接続を制御するには、このポリシーの代わりにGoogle Firebase Cloud Messaging (FCM)を使用します。スケジューリングオプションは次のとおりです。

  - **常時:** 接続を永続的に維持します。Citrixは、セキュリティを最適化するためにこのオプションを推奨します。**常時**を選択する場合は、接続がバッテリーを消耗しないように、接続タイマーポリシーも使用してください。接続を維持することで、ワイプやロックなどのセキュリティコマンドをオンデマンドでデバイスにプッシュできます。また、デバイスに展開する各ポリシーで、展開スケジュールオプションの**常時接続用に展開**を選択する必要があります。
  - **なし:** 手動で接続します。Citrixは、**なし**オプションではデバイスにセキュリティポリシーを展開できないため、本番環境での展開にはこのオプションを推奨しません。そのため、ユーザーは新しいアプリやポリシーを受け取ることがありません。
  - **毎回:** 指定された間隔で接続します。このオプションが有効なときに、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、XenMobileはデバイスが次回接続したときにそのポリシーを処理します。

- **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、ユーザーのデバイスをXenMobile Serverに再接続しようとし、定義した時間枠内で定期的に制御パケットを送信して接続を監視します。

ユーザーの例: 登録済みデバイスにパスコードポリシーを展開したいとします。スケジューリングポリシーにより、デバイスは定期的にサーバーに接続して新しいポリシーを収集します。

- **資格情報ポリシー**

このポリシーを使用する理由: Wi-Fiポリシーと組み合わせて使用されることが多い資格情報ポリシーを使用すると、証明書認証を必要とする内部リソースへの認証のために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ネットワークは認証のために証明書を必要とします。資格情報ポリシーは、オペレーティングシステムのキーストアに保存される証明書を展開します。ユーザーは、内部リソースに接続したときにその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では、Microsoft Exchange ActiveSyncメールを配信するための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メールを有効にします。ネイティブメール用のExchangeポリシーを使用すると、マクロを使用して、Active Directory属性からユーザーデータを入力できます。たとえば、${user.username}でユーザー名を入力し、${user.domain}でユーザーのドメインを入力します。

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。その後、Secure Hubはユーザーに認証を求め、メールの同期が開始されます。

- **位置情報ポリシー**

このポリシーを使用する理由: 位置情報ポリシーを使用すると、Secure HubでGPSが有効になっている場合、マップ上でデバイスの地理的位置を特定できます。このポリシーを展開し、XenMobile Serverから位置特定コマンドを送信すると、デバイスは位置座標を返します。

ユーザーの例: 位置情報ポリシーを展開し、デバイスでGPSが有効になっている場合、ユーザーがデバイスを紛失したときに、XenMobileセルフヘルプポータルにログオンして、位置特定オプションを選択すると、マップ上でデバイスの位置を確認できます。ユーザーはSecure

Hubが位置情報サービスを使用することを許可するかどうかを選択します。ユーザーが自分でデバイスを登録する場合、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際のもう1つの考慮事項は、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強制できます。このパスコードポリシーを使用すると、デバイスのパスコードの複雑さとタイムアウトを設定できます。

  ユーザーの例: 管理対象デバイスにパスコードポリシーを展開すると、Secure Hubはユーザーにパスコードまたは PINの設定を求めます。ユーザーは、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期限切れになったときにデバイスにアクセスする前に、それを解除する必要があります。

- **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: ユーザーグループにポリシーを展開し、後でそのポリシーを一部のユーザーから削除する必要があるとします。プロファイル削除ポリシーを作成し、展開ルールを使用して指定されたユーザー名にのみプロファイル削除ポリシーを展開することで、選択したユーザーのポリシーを削除できます。

  ユーザーの例: ユーザーデバイスにプロファイル削除ポリシーを展開しても、ユーザーはその変更に気づかない場合があります。たとえば、プロファイル削除ポリシーがデバイスカメラを無効にする制限を削除した場合、ユーザーはカメラの使用が許可されたことを知りません。変更がユーザーエクスペリエンスに影響を与える場合は、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: 制限ポリシーを使用すると、管理対象デバイスの機能や動作をロックダウンおよび制御するための多くのオプションを利用できます。サポートされているデバイスに対して、デバイスのカメラやマイクの無効化から、ローミングルールの適用、アプリストアなどのサードパーティサービスへのアクセス制限まで、何百もの制限オプションを有効にできます。

  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やApple App Storeにアクセスできなくなる場合があります。

- **利用規約ポリシー**

  このポリシーを使用する理由: デバイスが管理されることによる法的影響について、ユーザーに通知する必要がある場合があります。さらに、企業データがデバイスにプッシュされる際の

セキュリティリスクについて、ユーザーが認識していることを確認したい場合もあります。カスタムの利用規約ドキュメントを使用すると、ユーザーが登録する前にルールや通知を公開できます。

ユーザーの例: ユーザーは登録プロセス中に利用規約情報を確認します。提示された条件の受け入れを拒否した場合、登録プロセスは終了し、企業データにアクセスできません。誰が規約を受け入れたか、または拒否したかを示すレポートを生成し、人事/法務/コンプライアンスチームに提供できます。

- **VPNポリシー**

  このポリシーを使用する理由: VPNポリシーを使用して、古いVPNゲートウェイテクノロジー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。このポリシーは、Cisco AnyConnect、Juniper、Citrix VPNなど、さまざまな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、オンデマンドVPNを有効にすることも可能です。

  ユーザーの例: VPNポリシーが有効になっている場合、ユーザーが内部ドメインにアクセスすると、ユーザーのデバイスは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サイトに直接開くアイコンをデバイスにプッシュしたい場合は、Webクリップポリシーを使用します。WebクリップにはWebサイトへのリンクが含まれ、カスタムアイコンを含めることができます。デバイス上では、Webクリップはアプリアイコンのように見えます。

  ユーザーの例: ユーザーはWebクリップアイコンをクリックして、アクセスする必要があるサービスを提供するインターネットサイトを開くことができます。Webリンクを使用する方が、ブラウザ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、構成データなどの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、デバイスは自動的にWi-Fiネットワークに接続し、ユーザーを認証してネットワークにアクセスできるようにします。

- **ウィンドウズ インフォメーション プロテクション ポリシー**

  このポリシーを使用する理由: Windows Information Protection (WIP) ポリシーを使用して、企業データの潜在的な漏洩から保護します。設定した適用レベルでWindows Information Protectionを必要とするアプリを指定できます。たとえば、不適切なデータ共有をブロックし

たり、不適切なデータ共有について警告し、ユーザーがポリシーを上書きできるようにしたりできます。不適切なデータ共有をログに記録し、許可しながらWIPをサイレントで実行できます。

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ポリシーを構成したとします。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、次のようなメッセージが表示されます: 「仕事で保護されたコンテンツをこの場所に配置することはできません。」.

- **XenMobile Storeポリシー**

  このポリシーを使用する理由: XenMobile Storeは、管理者がユーザーに必要なすべての企業アプリとデータリソースを公開できる統合アプリストアです。管理者は以下を追加できます。

  - Webアプリ、SaaSアプリ、MAM SDK対応アプリ、またはMDXラップアプリ
  - Citrixモバイル生産性向上アプリ
  - .ipaまたは.apkファイルなどのネイティブモバイルアプリ
  - Apple App StoreおよびGoogle Playアプリ
  - Webリンク
  - Citrix StoreFrontを使用して公開されたCitrix Virtual Apps™

  ユーザーの例: ユーザーがデバイスをXenMobileに登録すると、Citrix Secure Hub™アプリを介してXenMobile Storeにアクセスします。ユーザーは、利用可能なすべての企業アプリとサービスを確認できます。ユーザーはアプリをクリックしてインストールしたり、データにアクセスしたり、アプリを評価およびレビューしたり、XenMobile Storeからアプリの更新をダウンロードしたりできます。

ユーザー登録オプション

ユーザーはさまざまな方法でデバイスをXenMobileに登録できます。詳細を検討する前に、MDM+MAM、MDM、またはMAMのいずれに登録するかを決定してください。これらの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。

最上位レベルでは、4つの登録オプションがあります。

- **登録招待:** ユーザーに登録招待または招待URLを送信します。登録招待およびURLは、Windowsデバイスでは利用できません。
- **セルフヘルプポータル:** ユーザーがSecure Hubをダウンロードしてデバイスを登録したり、登録招待を自分自身に送信したりできるポータルを設定します。

- **手動登録:** メール、ハンドブック、またはその他の連絡手段を送信して、システムが登録可能であることをユーザーに知らせます。その後、ユーザーはSecure Hubをダウンロードし、手動でデバイスを登録します。
- **エンタープライズ:** デバイス登録のもう1つのオプションは、Apple Deployment ProgramとGoogle Android Enterpriseを介することです。これらの各プログラムを通じて、従業員がすぐに使用できる事前構成済みのデバイスを購入できます。詳細については、「Appleサポート」のApple Deployment Programの記事と、「Android Enterpriseウェブサイト」のGoogle Android Enterpriseのドキュメントを参照してください。

登録招待

iOS、macOS、Android Enterprise、およびレガシーAndroidデバイスのユーザーに登録招待をメールで送信できます。登録招待およびURLは、Windowsデバイスでは利用できません。

また、SMTPまたはSMSを介して、iOS、macOS、Android、またはWindowsデバイスの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。詳細については、「デバイスの登録」を参照してください。

登録招待方法を使用することを選択した場合、次のことができます。

- **招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードを選択します。
- モードの任意の組み合わせを使用します。
- **設定**ページからモードを有効または無効にします。

各登録セキュリティモードの詳細については、「登録セキュリティモードの構成」を参照してください。

招待は多くの目的に役立ちます。招待の最も一般的な用途は、システムが利用可能であり、ユーザーが登録できることを通知することです。招待URLは一意です。ユーザーが招待URLを使用すると、そのURLは利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またはデバイスを制限できます。

登録プロファイルを構成する際、Active Directoryグループに基づいて、特定のユーザーが登録できるデバイスの数を制御できます。たとえば、財務部門にはユーザーあたり1台のデバイスのみを許可することができます。

特定の登録オプションには、追加のコストと落とし穴があることに注意してください。たとえば、SMSを使用して招待を送信するには、追加のインフラストラクチャが必要です。このオプションの詳細については、「通知」を参照してください。

メールで招待を送信するだけでなく、ユーザーがSecure Hub以外でメールにアクセスできる方法があることを確認してください。MDM登録のActive Directoryパスワードの代替として、ワンタイムパスワード（OTP）登録セキュリティモードを使用できます。

セルフヘルプポータル

セルフヘルプポータルを通じて登録招待をリクエストできます。セルフヘルプポータルの設定については、「登録セキュリティモードの構成」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を介して、またはサーバー情報を入力してXenMobileに接続します。AutoDiscoveryを使用する場合、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資格情報のみでログオンします。AutoDiscoveryを使用しない場合、サーバーアドレスとActive Directory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 Service」を参照してください。

手動登録はいくつかの方法で促進できます。ガイドを作成してユーザーに配布し、ユーザー自身で登録させることができます。IT部門が特定の時間帯にユーザーグループを手動で登録することもできます。ユーザーが資格情報、サーバー情報、またはその両方を入力する必要がある、同様の任意の方法を使用できます。

ユーザーオンボーディング

環境をセットアップしたら、ユーザーを環境に取り込む方法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は、ユーザー登録セキュリティモードの詳細について説明しました。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

ユーザーをオンボーディングする際、次の2つの基本的な方法で登録を許可できます。

- オープン登録。デフォルトでは、LDAP資格情報とXenMobile®環境情報を持つすべてのユーザーが登録できます。
- 制限付き登録。招待を持つユーザーのみが登録できるようにすることで、ユーザー数を制限できます。また、Active Directoryグループによってオープン登録を制限することもできます。

招待方式では、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、オープン登録は許容されますが、いくつか考慮すべき点があります。

- MAM登録の場合、Active Directoryグループメンバーシップを通じてオープン登録を簡単に制限できます。

- MDM登録の場合、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できます。環境内で企業デバイスのみを許可している場合、通常、その制限は問題になりません。ただし、BYOD環境でデバイスの数を制限したい場合は、この方法を検討することをお勧めします。

選択的招待は、オープン登録よりも手間がかかるため、通常はあまり行われません。ユーザーがデバイスを環境に登録するには、各ユーザー固有の招待状を送信する必要があります。登録招待状の送信方法については、「登録招待状の送信」を参照してください。

Active Directoryグループを使用して招待状を一括作成することはできますが、このアプローチは段階的に実行する必要があります。

ユーザーとの最初の接触

オープン登録と選択的招待のどちらにするかを決定し、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。

選択的招待方式を使用する場合、メールとSMSメッセージはプロセスの一部です。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。詳細については、「登録招待状の送信」を参照してください。

いずれの場合も、メールにはSMTPサーバーが必要であり、テキストメッセージにはSMSサーバーが必要であることに留意してください。これらのサーバーは、決定を下す際に考慮すべき追加費用となる可能性があります。方法を選択する前に、新規ユーザーがメールなどの情報にどのようにアクセスすることを期待するかを検討してください。すべてのユーザーがXenMobileを通じてメールにアクセスすることを望む場合、招待メールを送信することは問題となるでしょう。

オープン登録環境の場合、XenMobile以外の別の手段で連絡を送信することもできます。そのオプションを選択する場合は、関連するすべての情報を含めるようにしてください。ユーザーにSecure Hubアプリの入手先と登録方法を知らせてください。検出をオフにしている場合は、XenMobile Serverのアドレスもユーザーに提供してください。AutoDiscoveryの詳細については、「XenMobile AutoDiscovery Service」を参照してください。

XenMobile®運用のチューニング

XenMobileの運用における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係し、Citrix ADCおよびSQL Serverデータベースの構成に依存します。この記事では、XenMobileのチューニングと最適化に関連して、管理者が最も頻繁に構成する設定に焦点を当てています。Citrixは、XenMobileを展開する前に、この記事の各設定を評価することを推奨します。

> **重要:**

> これらのガイドラインは、XenMobile ServerのCPUとRAMがデバイス数に対して十分であることを前提としています。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運用、ユーザー、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、各XenMobile Serverノードの再起動が必要です。XenMobileは、再起動が必要な場合に通知します。

これらのチューニングガイドラインは、クラスター環境と非クラスター環境の両方に適用されます。

hibernate.c3p0.idle_test_period

このXenMobile Serverプロパティ（カスタムキー）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決定します。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アイドルテスト期間**

hibernate.c3p0.max_size

このカスタムキーは、XenMobileがSQL Serverデータベースに開くことができる最大接続数を決定します。XenMobileは、このカスタムキーに指定した値を上限として使用します。接続は、必要な場合にのみ開かれます。設定は、データベースサーバーの容量に基づいてください。

クラスター構成における以下の式に注意してください。c3p0接続数にノード数を乗算した値が、XenMobileがSQL Serverデータベースに開くことができる実際の最大接続数になります。

クラスター構成および非クラスター構成において、SQL Serverのサイズが小さいにもかかわらず値を高く設定しすぎると、ピーク負荷時にSQL側でリソースの問題が発生する可能性があります。値を低く設定しすぎると、利用可能なSQLリソースを活用できない可能性があります。

キーを次のように構成します。デフォルトは **1000** です。

- キー: **hibernate.c3p0.max_size**
- 値: **1000**

- 表示名: **hibernate.c3p0.max_size**
- 説明: SQLへのDB接続

hibernate.c3p0.min_size

このカスタムキーは、XenMobileがSQL Serverデータベースに開く最小接続数を決定します。キーを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: SQLへのDB接続

hibernate.c3p0.timeout

このカスタムキーはアイドルタイムアウトを決定します。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、Citrixではこのカスタムキーを追加し、アイドルタイムアウトを短縮す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: データベースアイドルタイムアウト

プッシュサービスハートビート間隔

この設定は、iOSデバイスがAPNs通知がその間に配信されなかったかどうかをチェックする頻度を決定します。APNsハートビートの頻度を増やすと、データベース通信を最適化できます。値が大きすぎると、不要な負荷が増加する可能性があります。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。

環境内に多数のiOSデバイスがある場合、ハートビート間隔は必要以上の負荷を引き起こす可能性があります。選択的ワイプ、ロック、完全ワイプなどのセキュリティアクションは、このハートビートに依存しません。その理由は、これらのアクションが実行されると、APNs通知がデバイスに送信されるためです。

この値は、Active Directoryグループメンバーシップの変更後にポリシーが更新される速度を制御します。そのため、負荷を軽減するために、この値を12時間から20時間の間で増やすことがよく適切です。

iOS MDM APNS接続プールサイズ

APNs接続プールが小さすぎると、100台を超えるデバイスがある場合にAPNsアクティビティのパフォーマンスに悪影響を及ぼす可能性があります。パフォーマンスの問題には、デバイスへのアプリとポリシーの展開の遅延、およびデバイス登録の遅延が含まれます。デフォルトは**1**です。約400台のデバイスごとにこの値を1ずつ増やすことをお勧めします。

auth.ldap.connect.timeout

LDAP応答の遅延を補うために、Citrixでは、以下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接続タイムアウト**

auth.ldap.read.timeout

低速なLDAP応答を補うため、Citrixは、以下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推奨します。

- 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読み取りタイムアウト**

その他のサーバー最適化

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展開の頻度（分単位）。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。推奨設定は **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（分単位）。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。推奨設定は **1440**（24時間）です。
削除されたActive Directoryユーザーの確認間隔	15 分	Active Directoryの標準同期時間は **15** 分です。値 **0** は、XenMobileが削除されたActive Directoryユーザーを確認するのを防ぎます。推奨設定は **15** 分です。
MaxNumberOfWorker	3	多数のボリューム購入ライセンスをインポートする際に使用されるスレッドの数。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、6などのより多くのスレッドを使用すると、ボリューム購入のインポートでCPU使用率が高くなります。

SQL DBでデッドロックを確認し、履歴データを削除する方法

デッドロックが発生した場合は、以下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. 履歴データを確認するには、次のクエリを実行します。

```
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. 前述の3つのテーブルからデータを削除します。

   注:

   テーブルに履歴データが表示されない場合があります。その場合は、その特定のテーブルのtruncateクエリの実行をスキップしてください。

   ```
   truncate TABLE dbo.EWDEPLOY_HISTO;

   truncate TABLE dbo.EWSESS;

   truncate TABLE dbo.EWAUDIT;
   ```

3. デッドロックが原因でブロックされていたSELECTクエリのブロックを解除します。この手順により、それ以上のデッドロックが処理されます。

   ```
   ALTER DATABASE <database_name> SET       READ_COMMITTED_SNAPSHOT ON
   WITH ROLLBACK IMMEDIATE
   ```

4. デフォルトでは、データベースのクリーンアップはセッション保持データと監査保持データを7日間保持するように設定されており、これは多くのユーザーにとって長すぎます。クリーンアップ値を1日または2日に変更してください。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エントリをクリーンアップする

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確認してください。XenMobile Serverは、登録証明書をENROLLMENT_CERTIFICATEテーブルと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、ENROLLMENT_CERTIFICATEテーブルの証明書は削除されます。KEYSTOREテーブルのエントリは残るため、パフォーマンスの問題を引き起こす可能性があります。KEYSTOREテーブルから孤立したエントリをクリーンアップするには、次の手順を実行します。

> **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. 履歴データを確認するには、次のクエリを実行します。

```
select COUNT(*) from KEYSTORE
```

2. 次のクエリを使用して、KEYSTOREテーブル内の孤立したエントリを確認します。

```
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、孤立したエントリをクリアします。

```
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

        FROM SERVER_CERTIFICATE)

    DELETE FROM keystore

    WHERE id IN
```

```
    (
        SELECT keystore.id
        FROM keystore
            LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
        WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
    );
```

4. 検索効率を向上させるために、KEYSTOREテーブルにインデックスを追加します。

```
DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";

ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;

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

アプリケーションのプロビジョニングは、モバイルアプリのライフサイクル管理を中心に展開されます。XenMobile®環境内でのモバイルアプリの準備、構成、配信、および管理です。場合によっては、アプリケーションコードの開発または変更もプロビジョニングプロセスの一部となることがあります。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備わっています。

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、以下の記事を読むことをお勧めします。

- アプリ - ユーザーコミュニティ

組織がユーザーに配信するアプリの種類を確定したら、アプリのライフサイクル全体にわたる管理プロセスを概説できます。

アプリのプロビジョニングプロセスを定義する際には、以下の点を考慮してください。

- **アプリのプロファイリング:** 組織は限られた数のアプリから始めることができます。しかし、ユーザーの採用率が増加し、環境が拡大するにつれて、管理するアプリの数は急速に増加する可能性があります。アプリのプロビジョニングを管理しやすくするために、最初から特定のアプリプロファイルを定義してください。アプリのプロファイリングは、非技術的な観点からアプリを論理的なグループに分類するのに役立ちます。たとえば、以下の要素に基づいてアプリプロファイルを作成できます。
    - バージョン: 追跡用のアプリバージョン
    - インスタンス: 異なるユーザーセットに展開される複数のインスタンス（たとえば、異なるアクセスレベルを持つもの）
    - プラットフォーム: iOS、Android、またはWindows
    - ターゲットオーディエンス: 標準ユーザー、部門、Cレベルの役員
    - 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: アプリがアップグレードされる頻度
    - ライセンス: ライセンス要件と所有権
    - MAM SDK または MDX ポリシー: モバイルアプリに MDX 機能適用するため
    - ネットワークアクセス: Secure Browse やフル VPN などのアクセスタイプ

> **注:**
>
> Tunneled Web SSO は、MDX 設定における Secure Browse の名称です。動作は同じです。

例:

要素	セキュアメール	メール	社内	エピックローバー
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

要素	セキュアメール	メール	社内	エピックローバー
ターゲットユーザー	VIPユーザー	医師	臨床ユーザー	臨床ユーザー
所有	IT	IT	IT	IT
タイプ	MDX	MDX	ネイティブ	パブリック
アップグレードサイクル	四半期ごと	四半期ごと	年ごと	該当なし
ライセンス	該当なし	該当なし	該当なし	ボリューム購入
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を維持および追跡することは、プロビジョニングプロセスにおいて非常に重要です。バージョン管理はユーザーには透過的です。ユーザーは、新しいバージョンのアプリがダウンロード可能になったときにのみ通知を受け取ります。あなたの視点から見ると、本番環境への影響を避けるために、各アプリのバージョンを非本番環境でレビューおよびテストすることも重要です。

  特定のアップグレードが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つの種類があります。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す。もう1つは、アプリに大幅な変更と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を評価するために、アプリのリリースノートを注意深く確認してください。

- **アプリ開発:** 開発するモバイルアプリにMAM SDKを統合すると、それらのアプリにMDX機能が適用されます。MAM SDKの概要を参照してください。

  MAM SDKは、2023年7月に廃止予定のMDX Toolkitに代わるものです。アプリラッピングの詳細については、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、標準の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部として、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またはMAMポリシーにマッピングできます。この計画により、アプリの展開が簡素化され、迅速化されます。例:

  - 特定のアプリを異なる方法で展開する場合があります。
  - XenMobile環境にアーキテクチャ上の変更を加える必要がある場合があります。変更は、アプリが必要とするセキュリティコンプライアンスの種類によって異なります。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い場合があります。または、特定のアプリがエンドツーエンドのSSL暗号化やジオフェンシングを必要とする場合があります。

- **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 Storeに表示されます。このストアを使用すると、パブリックアプリまたはネイティブアプリをユーザーに便利に配信できます。管理する唯一のMDMアプリ制御は、デバイスレベルの制限を適用することです。ただし、MAMを使用してアプリを配信すると、アプリの配信とアプリ自体を完全に制御できます。通常、MAMを介してアプリを配信する方が適しています。
- **アプリケーションのメンテナンス:**
  - 初期監査の実施: 本番環境でのアプリのバージョンと、前回のアップグレードサイクルを追跡します。アップグレードが必要となった特定の機能やバグ修正を記録します。
  - ベースラインの確立: 各アプリの最新の安定版リリースのリストを維持します。このアプリバージョンは、アップグレード後に予期せぬ問題が発生した場合のフォールバックとなります。また、ロールバック計画も策定します。本番展開の前に、テスト環境でアプリのアップグレードをテストします。可能であれば、最初に本番ユーザーの一部にアップグレードを展開し、その後、全ユーザーベースに展開します。
  - Citrix®ソフトウェア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ー通知の購読: アプリの最新リリースを常に把握しておくことは非常に重要です。早期アクセスリリース (EAR) ビルドがテスト用に利用可能になる場合があります。
  - ユーザーに通知する戦略を考案する: アプリのアップグレードが利用可能になったときにユーザーに通知する戦略を定義します。展開前にトレーニングでユーザーを準備します。アプリを更新する前に複数の通知を送信できます。アプリによっては、最適な通知方法は電子メール通知またはウェブサイトである場合があります。

アプリのライフサイクル管理は、アプリの初期展開から廃止までの完全なライフサイクルを表します。アプリのライフサイクルには、次のフェーズがあります。

1. 仕様の要件: ビジネスケースとユーザー要件から始めます。
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: アプリを本番ユーザーに展開します。
5. メンテナンス: アプリのバージョンを更新します。本番環境でアプリを更新する前に、テスト環境でアプリを展開します。

Secure Mail を使用したアプリケーションライフサイクルの例

1. 仕様の要件: セキュリティ要件として、コンテナ化され、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。アプリにMDXポリシーコントロールを適用できる必要があります。
3. テスト: Secure Mail をテストユーザーグループに割り当て、対応するMDXファイルをXenMobile Serverから展開します。テストユーザーは、メールの送受信、カレンダーおよび連絡先へのアクセスが正常にできることを検証します。テストユーザーは問題やバグも報告します。テストユーザーのフィードバックに基づいて、本番環境での使用のためにSecure Mailの設定を最適化します。
4. 展開: テストフェーズが完了したら、Secure Mail を本番ユーザーに割り当て、XenMobile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 の新しいアップデートが利用可能です。Citrixダウンロードから新しいMDXファイルをダウンロードし、XenMobile Server上の既存のMDXファイルを置き換えます。ユーザーにアップデートを実行するよう指示します。注: Citrixは、このプロセスをテスト環境で完了し、テストすることを推奨します。その後、アプリをXenMobile本番環境にアップロードし、ユーザーに展開します。

詳細については、「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

XenMobile®コンソールのダッシュボードにアクセスすると、情報を一目で確認できます。この情報を使用して、ウィジェットを利用することで問題や成功をすばやく把握できます。

ダッシュボードは通常、XenMobileコンソールに初めてサインオンしたときに表示される画面です。コンソールの他の場所からダッシュボードにアクセスするには、 をクリックします。ダッシュボードで をクリックすると、ページのレイアウトや表示されるウィジェットを編集できます。

- **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。これらのダッシュボードは個別に編集でき、保存したダッシュボードを選択してそれぞれを表示できます。

- **レイアウトスタイル:** この行では、ダッシュボードに表示されるウィジェットの数と、ウィジェットのレイアウト方法を選択できます。
- **ウィジェットの選択:** ダッシュボードに表示する情報を選択できます。
    - **通知:** 左側の数字の上にあるチェックボックスをオンにすると、ウィジェットの上に通知バーを追加できます。このバーには、準拠デバイス、非アクティブデバイス、および過去24時間以内にワイプまたは登録されたデバイスの数が表示されます。
    - **プラットフォーム別デバイス:** プラットフォームごとの管理対象デバイスと非管理対象デバイスの数を表示します。
    - **キャリア別デバイス:** キャリアごとの管理対象デバイスと非管理対象デバイスの数を表示します。各バーをクリックすると、プラットフォーム別の内訳が表示されます。
    - **プラットフォーム別管理対象デバイス:** プラットフォームごとの管理対象デバイスの数を表示します。
    - **プラットフォーム別非管理対象デバイス:** プラットフォームごとの非管理対象デバイスの数を表示します。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、その特権が取り消されているか、ワイプされている可能性があります。
    - **ActiveSync Gatewayステータス別デバイス:** ActiveSync Gatewayステータス別にグループ化されたデバイスの数を表示します。情報には、ブロック済み、許可済み、または不明のステータスが表示されます。各バーをクリックすると、プラットフォーム別にデータを内訳表示できます。
    - **所有権別デバイス:** 所有権ステータス別にグループ化されたデバイスの数を表示します。情報には、会社所有、従業員所有、または不明の所有権ステータスが表示されます。
    - **失敗したデリバリーグループの展開:** パッケージごとの失敗した展開の総数を表示します。展開が失敗したパッケージのみが表示されます。
    - **ブロック理由別デバイス:** ActiveSyncによってブロックされたデバイスの数を表示します。
    - **インストール済みアプリ:** このウィジェットを使用すると、アプリ名を入力でき、そのアプリに関する情報がグラフに表示されます。
    - **ボリューム購入アプリのライセンス使用状況:** Appleボリューム購入アプリのライセンス使用状況統計を表示します。

ユースケース

環境を監視するためにダッシュボードウィジェットを使用できる多くの方法の例を以下に示します。

- モバイル生産性向上アプリを展開しており、デバイスへのモバイル生産性向上アプリのインストール失敗に関するサポートチケットを受け取っています。**非準拠デバイス**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、モバイル生産性向上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監視して、環境からデバイスを削除し、ライセンスを再利用したいと考えています。この統計を追跡するには、**非アクティブなデバイス**ウィジェットを使用します。
- データが適切に同期されないことに関するサポートチケットを受け取っています。問題がActiveSyncに関連しているかどうかを判断するために、**ActiveSyncゲートウェイステータス別のデバイス**および**ブロック理由別のデバイス**ウィジェットを使用することをお勧めします。

レポート

環境がセットアップされ、ユーザーが登録された後、レポートを実行して展開について学習できます。XenMobileには、環境で実行されているデバイスの全体像を把握するのに役立つさまざまなレポートが組み込まれています。詳細については、「レポート」を参照してください。

> **重要:**
>
> SQL Serverを使用してカスタムレポートを作成することは可能ですが、Citrix®はこの方法を推奨していません。この方法でSQL Serverデータベースを使用すると、XenMobile展開に予期せぬ結果をもたらす可能性があります。このレポート方法を追求する場合は、SQLクエリが読み取り専用アカウントを使用して実行されることを確認してください。

ロールベースのアクセス制御とXenMobile®のサポート

XenMobileは、XenMobileコンソール、リモートサポート、パブリックAPIなどのXenMobileシステム機能へのユーザーおよびグループアクセスを制限するために、ロールベースのアクセス制御（RBAC）を使用します。この記事では、XenMobileに組み込まれているロールについて説明し、RBACを使用するXenMobileのサポートモデルを決定する際の考慮事項を含みます。

> **注:**
>
> リモートサポートは、January 1, 2019以降、新規のお客様には提供されなくなりました。既存のお客様は引き続き製品を使用できますが、Citrix®は機能強化や修正を提供しません。

組み込みロール

以下の組み込みロールに付与されているアクセスを変更したり、ロールを追加したりできます。各ロールに関連付けられているアクセス権と機能権限の完全なセットおよびそのデフォルト設定については、XenMobileドキュメントからロールベースのアクセス制御のデフォルト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ドキュメントのRBACでロールを構成するを参照してください。

管理者ロール

付与されるデフォルトのアクセス権:

- リモートサポートを除くシステムへのフルアクセス。
- 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、一部のサポートタスクを実行できます。

考慮事項:

- 管理者の一部または全員がリモートサポートへのアクセスを必要としますか？その場合は、管理者ロールを編集するか、管理者ロールを追加できます。
- 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ロールを追加し、権限を編集します。

サポート

付与されるデフォルトのアクセス権:

- リモートサポートへのアクセス。

考慮事項:

- オンプレミスのXenMobile Server展開の場合: リモートサポートにより、ヘルプデスク担当者は管理対象のAndroidモバイルデバイスをリモートで制御できます。スクリーンキャストはSamsung Knoxデバイスでのみサポートされています。
- クラスター化されたオンプレミスのXenMobile Server展開では、リモートサポートは利用できません。

ユーザー

付与されるデフォルトのアクセス権:

- XenMobileコンソールへの制限付きアクセス: デバイス機能 (ワイプ、デバイスのロック/ロック解除、コンテナのロック/ロック解除、場所の表示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)。登録招待の追加、削除、送信。

考慮事項:

- ユーザーロールを使用すると、ユーザーが自分で問題を解決できるようにすることができます。
- 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ロールを作成します。

XenMobileサポートモデルの考慮事項

採用できるサポートモデルは多岐にわたり、レベル1および2のサポートをサードパーティが担当し、従業員がレベル3および4のサポートを担当する場合があります。サポートの負荷をどのように分散するかに関わらず、このセクションで説明するXenMobile展開とユーザーベースに固有の考慮事項を念頭に置いてください。

ユーザーは会社所有のデバイスを使用していますか、それともBYOデバイスを使用していますか？ サポートに影響を与える主な質問は、XenMobile環境でユーザーデバイスを誰が所有しているかです。ユーザーが会社所有のデバイスを使用している場合、デバイスをロックダウンする方法として、より低いレベルのサポートを提供する場合があります。その場合、デバイスの問題やデバイスの使用方法についてユーザーを支援するヘルプデスクを提供する場合があります。サポートする必要があるデバイスの種類に応じて、ヘルプデスクでRBACデバイスプロビジョニングおよびサポートロールをどのように使用できるかを検討してください。

ユーザーがBYOデバイスを使用している場合、組織はユーザーがデバイスサポートの独自のソースを見つけることを期待する場合があります。その場合、組織が提供するサポートは、XenMobile固有の問題に焦点を当てた管理的な役割になります。

デスクトップのサポートモデルは何ですか？ デスクトップのサポートモデルが他の会社所有のデバイスに適しているかどうかを検討してください。同じサポート組織を使用できますか？どのような追加トレーニングが必要ですか？

ユーザーにXenMobileセルフヘルプポータルへのアクセスを許可しますか？ 設定 > 登録 を使用して、登録セキュリティモードのセルフヘルプポータルを有効にします。セルフヘルプポータルから、ユーザーはデバイスを登録するための登録リンクを生成したり、登録招待を自分自身に送信したりできます。登録セキュリティモードの構成を参照してください。

システム監視

アプリのアクセスと接続の最適な稼働時間を確保するには、XenMobile®環境で次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にログを生成および保存します。これらのログは、システムログ（syslog）サーバーにエクスポートすることもできます。ログ設定を構成して、サイズ制約やログレベルを指定したり、特定のイベントをフィルタリングするためのカスタムロガーを作成したりできます。XenMobileコンソールからいつでもXenMobile Serverログを確認できます。また、syslogサーバーを介してログ内の情報を本番Splunkロギングサーバーにエクスポートすることもできます。

XenMobileで利用可能なログファイルの種類を以下に示します。

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を含む、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>
```

- ここで、`<id>` は sessionID のような一意の識別子です。
- ここで、`<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。

管理者監査ログファイル: XenMobileコンソールでのアクティビティに関する監査情報が含まれています。

> **注:**
>
> 管理者監査ログとユーザー監査ログの両方に同じ形式が使用されます。
>
> メッセージ形式:

必須のDateとTimestampの値を除き、他のすべての属性はオプションです。オプションフィールドはメッセージ内で「」で表されます。

`<date> <timestamp> "<username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>" "<application name>" "<app user id>" "<user agent>" "<details>"`

以下の表に、利用可能な管理者監査ログイベントを示します。

イベントの管理者監査ログメッセージ	ステータス
ログイン	成功/失敗
ログアウト	成功/失敗
管理者を取得	成功/失敗
管理者を更新	成功/失敗
アプリケーションを取得	成功/失敗
アプリケーションを追加	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
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

イベントの管理者監査ログメッセージ	ステータス
アクティブな証明書	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
証明書チェーンを削除	成功/失敗
証明書チェーンを追加	成功/失敗
コネクタを取得	成功/失敗
コネクタを追加	成功/失敗
コネクタを削除	成功/失敗
コネクタを更新	成功/失敗
デバイスを取得	成功/失敗
デバイスをロック	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
ロールの取得	成功/失敗
ロールの追加	成功/失敗
ロールの更新	成功/失敗
ロールの削除	成功/失敗
ロールのバインド	成功/失敗
ロールのバインド解除	成功/失敗

イベントの管理者監査ログメッセージ	ステータス
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
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 を追加	成功/失敗
Active Directory を更新	成功/失敗
masteruserlist を追加	成功/失敗
masteruserlist を更新	成功/失敗
DNS を更新	成功/失敗
ネットワークを更新	成功/失敗
ログサーバーを更新	成功/失敗
ログサーバーからログを転送	成功/失敗
syslogを更新	成功/失敗
レシーバーの更新を更新	成功/失敗
タイムサーバーを更新	成功/失敗
信頼を更新	成功/失敗
サービスレコードを追加	成功/失敗
サービスレコードを更新	成功/失敗
レシーバーのメールを更新	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

イベントの管理者監査ログメッセージ	ステータス
アプリストアのアプリ詳細の取得	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
ブランドを追加	成功/失敗
ブランドを削除	成功/失敗
SSLオフロードを更新	成功/失敗
アカウントプロパティを追加	成功/失敗
アカウントプロパティを削除	成功/失敗
アカウントプロパティを更新	成功/失敗
ビーコンを追加	成功/失敗

ユーザー監査ログファイル: 登録済みデバイスからのユーザーアクティビティに関連する情報が含まれています。

> **注:**
>
> ユーザー監査ログと管理者監査ログの両方に同じ形式が使用されます。
>
> メッセージ形式:

必須のDateおよびTimestamp値を除き、他のすべての属性はオプションです。オプションフィールドはメッセージ内で「」で表されます。例:

`<date> <timestamp> " <username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>" " <application name>" "<app user id>" "<user agent>" "<details>"`

次の表に、利用可能なユーザー監査ログ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
ログイン	成功/失敗
セッションタイムアウト	成功/失敗
購読	成功/失敗
購読解除	成功/失敗
プレ起動	成功/失敗
AGEE SSO	成功/失敗
Citrix Files 用 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
トークン更新	成功/失敗
シークレットが保存されました	成功/失敗
シークレットが取得されました	成功/失敗
ユーザーがパスワード変更を開始しました	成功/失敗
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
ディスカバリサービス	成功/失敗
エンドポイントサービス	成功/失敗

XENMOBILE®サーバー	
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フォルダー作成	成功/失敗
Cabファイル取得	成功/失敗
ファイルのフォルダー作成	成功/失敗
ファイルの取得	成功/失敗
ファイルの送信	成功/失敗
スクリプトのフォルダー作成	成功/失敗
スクリプトの取得	成功/失敗
スクリプトの送信	成功/失敗
スクリプトのシェル実行	成功/失敗
スクリプトの自動実行	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フォルダ作成	成功/失敗
APKファイル取得	成功/失敗

XENMOBILE®サーバー

MDM機能	ステータス
APKアプリ	成功/失敗
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
デバイスの検索	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
アンマネージドアプリケーションの削除	成功/失敗
アンマネージド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カードのワイプ	成功/失敗
暗号化されたメール添付ファイル	成功/失敗

MDM機能	ステータス
ブランド設定	成功/失敗
セキュアブラウザ	成功/失敗
コンテナブラウザ	成功/失敗
コンテナのロック解除	成功/失敗
コンテナパスワードのリセット	成功/失敗
AGクライアント認証資格情報	成功/失敗

Citrix ADCは、XenMobile Webサービスの状態も監視します。これは、各XenMobile Serverクラスターノードへの HTTPリクエストをシミュレートするようにインテリジェントな監視プローブで構成されています。プローブはサービスがオンラインであるかどうかを判断し、受信した応答に基づいて応答します。ノードが期待どおりに応答しない場合、Citrix ADCはそのサーバーをダウンとしてマークします。また、Citrix ADCはノードをロードバランシングプールから外し、Citrix ADC監視ソリューションを介してアラートを生成するためにイベントをログに記録します。

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、CPU、メモリ、ストレージの使用率メトリックに関する関連アラートを提供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インスタンスは常にデータベースへのアクセスを必要とし、SQLインフラストラクチャに障害が発生した場合はオフラインになります（たとえば、応答を停止します）。SQL Serverのディスク容量の問題が発生した後も、XenMobileコンソールはしばらく機能し続ける可能性があります。XenMobileワークロードのデータベースの稼働時間を最大化し、適切なパフォーマンスを確保するには、SQL Serverの状態を積極的に監視する必要があります。SQL Serverの監視の詳細については、「パフォーマンスの監視とチューニングの概要」を参照してください。また、XenMobile環境が成長し続けるにつれて、サービスレベル契約を保証するために、CPU、メモリ、ストレージのリソース割り当てを調整する必要があります。

シトリックス エーディーシー

Citrix ADCは、メトリックを内部ストレージにログ記録したり、外部ログサーバーにログを送信したりする機能を提供します。syslogサーバーを構成して、Citrix ADCログを本番環境のSplunkログサーバーにエクスポートできます。Citrix ADCで利用可能なログレベルは次のとおりです。

- 緊急
- アラート
- クリティカル
- エラー
- 警告
- 情報

ログファイルは、Citrix ADCストレージの/var/log/ns.logディレクトリにも保存され、newnslogという名前が付けられています。Citrix ADC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、xxは連番を表します。

Citrix ADCは、監視オプションとしてSNMPトラップと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は、SNMP監視を参照してください。

災害復旧

アクティブ/パッシブフェールオーバー戦略を使用して、災害復旧のために複数のサイトを含むXenMobile®展開を設計および構成できます。

この記事で説明する推奨される災害復旧戦略は、次の要素で構成されます。

- プライマリサイトとして知られる、単一の地理的場所のデータセンターにある単一のXenMobileアクティブサイトで、すべてのエンタープライズユーザーにグローバルにサービスを提供します。
- 災害復旧サイトとして知られる、2番目の地理的場所のデータセンターにある2番目のXenMobileサイト。この災害復旧サイトは、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、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障害が発生した場合にユーザーがXenMobileにアクセスできるようにするためのXenMobile、SQLデータベース、およびCitrix ADCインフラストラクチャが含まれています。

災害復旧サイトのXenMobileサーバーは、通常の運用中はオフラインのままであり、プライマリサイトから災害復旧サイトへの完全なサイトフェールオーバーが必要な災害復旧シナリオの場合にのみオンラインになります。災害復旧サイトのXenMobileサーバーを起動する前に、災害復旧サイトのSQLサーバーがアクティブであり、接続を受け入れる準備ができている必要があります。

この災害復旧戦略は、停止時にMDMおよびMAM接続を災害復旧サイトにルーティングするためのDNS変更によるCitrix ADCアクセス層の手動フェールオーバーに依存します。

> **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何らかの方法を確立しておく必要があります。

災害復旧フェールオーバープロセス

1. 災害復旧フェールオーバープロセスをテストしている場合は、サイト障害をシミュレートするためにプライマリサイトのXenMobileサーバーをシャットダウンします。
2. XenMobileサーバーのパブリックDNSレコードを、災害復旧サイトの外部IPアドレスを指すように変更します。
3. SQL Serverの内部DNSレコードを、災害復旧サイトのSQL Server IPアドレスを指すように変更します。
4. 災害復旧サイトで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あり、サイトローカルのXenMobileサーバーからの接続を受け入れる準備ができていることを確認します。
5. 災害復旧サイトでXenMobileサーバーをオンにします。

XenMobile Server 更新プロセス

プライマリサーバーとディザスタリカバリサーバーのコードを統一するために、XenMobile をパッチやリリースで更新する際はいつでも、以下の手順に従ってください。

1. プライマリサイトの XenMobile Server 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. ディザスタリカバリサイトの XenMobile Server をオンラインにします。サーバーは、アップグレードプロセス中のみ、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. すべてのディザスタリカバリサイトの XenMobile Server に必要なパッチと更新を適用します。
5. XenMobile Server 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。

ディザスタリカバリのリファレンスアーキテクチャ図

次の図は、XenMobile のディザスタリカバリ展開における高レベルのアーキテクチャを示しています。

ディザスタリカバリのリファレンスアーキテクチャ図(/en-us/xenmobile/server/media/disaster-recovery-diagram.png)

ディザスタリカバリのための GSLB

このアーキテクチャの重要な要素は、トラフィックを適切なデータセンターに誘導するためのグローバルサーバー負荷分散 (GSLB) の使用です。

デフォルトでは、XenMobile ウィザード用の Citrix ADC は、ディザスタリカバリのための GSLB の使用を有効にしない方法で Citrix Gateway を構成します。したがって、追加の手順を実行する必要があります。

GSLB の仕組み

GSLB はその核となる部分で DNS の一種です。参加している Citrix ADC アプライアンスは、権威 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。Citrix ADC アプライアンスは、そのシステムにトラフィックを誘導する DNS クエリに応答する前に、システムの状態をチェックします。

レコードが解決されると、トラフィックの解決におけるGSLBの役割は完了します。クライアントはターゲットの仮想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、レコードの有効期限がいつどのように切れるかを制御する上で重要な役割を果たします。これはCitrix ADCシステムの範囲を大きく超えています。そのため、GSLBはDNS名前解決と同じ制限を受けます。クライアントは応答をキャッシュするため、この方法での負荷分散は従来の負荷分散ほどリアルタイムではありません。

サイト、サービス、モニターを含むCitrix ADC上のGSLB構成は、正しいDNS名前解決を提供するために存在します。

公開サーバーの実際の構成（このシナリオでは、Citrix ADC for XenMobileウィザードが作成する構成）は、GSLBの影響を受けません。GSLBはCitrix ADC上の独立したサービスです。

XenMobileでGSLBを使用する場合のドメイン委任に関する課題

Citrix ADC for XenMobileウィザードは、Citrix Gateway for XenMobileを構成します。このウィザードは、3つの負荷分散仮想サーバーと1つのCitrix Gateway仮想サーバーを生成します。

2つの負荷分散仮想サーバーは、ポート443と8443でMDMトラフィックを処理します。Citrix GatewayはMAMトラフィックを受信し、ポート8443で3番目のサーバー、つまりMAM負荷分散仮想サーバーに転送します。MAM負荷分散仮想サーバーへのすべてのトラフィックはCitrix Gatewayを介して渡されます。

MAM負荷分散仮想サーバーには、XenMobile Serverと同じSSL証明書が必要であり、デバイスの登録に使用されるものと同じFQDNを使用します。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できるようにするため、Citrix ADC for XenMobileウィザードはCitrix Gateway上にローカルDNSレコードを作成します。このDNSレコードは、デバイスの登録に使用されるFQDNと一致します。

この構成は、XenMobile Server URLがGSLBドメインURLではない場合に有効です。災害復旧に必要とされるように、GSLBドメインURLがXenMobile Server URLとして使用される場合、ローカルDNSレコードはCitrix GatewayがMDM負荷分散サーバーへのトラフィックを解決するのを妨げます。

GSLB災害復旧にCNAME方式を使用する

Citrix ADC for XenMobileウィザードによって作成されるデフォルト構成が提示する課題に対処するには、親ドメイン (`company.com`) にXenMobile Server FQDNのCNAMEレコードを作成し、Citrix ADCが権限を持つ委任されたサブゾーン (`gslb.company.com`) のレコードを指すようにします。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アドレスの静的DNS Aレコードを作成できます。

1. 外部DNSで、Citrix ADC GSLB上のGSLBドメインFQDNを指すXenMobile Server FQDNのCNAMEを作成します。MDMトラフィック用とMAM (Citrix Gateway) トラフィック用に2つのGSLBドメインが必要です。

   例:

   ```
   CNAME = xms.company.com IN CNAME xms.gslb.comany.com
   ```

2. 各サイトのCitrix Gatewayインスタンスで、CNAMEレコードが指す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
   ```

   Citrix ADC for XenMobileウィザードを使用してCitrix Gatewayを展開する場合、MAMロードバランシングサーバーを構成する際にXenMobile Server URLを使用します。これにより、XenMobile Server URLの静的DNS Aレコードが作成されます。

3. XenMobile Server URL (`xms.company.com`) を使用してSecure Hubに登録するクライアントでテストします。

   この例では、以下のFQDNを使用します。

- `xms.company.com` は、MDMトラフィックで使用され、デバイスの登録に使用されるURLであり、この例ではCitrix ADC for XenMobileウィザードを使用して構成されます。
- `xms.gslb.company.com` は、XenMobile ServerのGSLBドメインFQDNです。

Citrixサポートプロセス

Citrix製品に関連する問題については、Citrix Technical Support Servicesを利用できます。このグループは回避策と解決策を提供し、開発チームと協力してソリューションを提供します。

Citrix ConsultingSM ServicesまたはCitrix Education Servicesは、製品トレーニングに関する支援を提供し、製品の使用法、構成、インストール、または環境の設計とアーキテクチャについてアドバイスします。

Citrix Consultingは、概念実証、経済的影響評価、インフラストラクチャの健全性チェック、設計要件分析、アーキテクチャ設計検証、統合、運用プロセス開発など、Citrix製品関連のプロジェクトを支援します。

Citrix EducationSMは、Citrix Virtualization、Cloud、およびネットワークテクノロジーに関する最高クラスのITトレーニングと認定を提供します。

Citrixは、サポートケースを作成する前に、Citrixのセルフヘルプリソースと推奨事項を最大限に活用することをお勧めします。たとえば、Citrixの技術専門家が執筆した記事や速報にアクセスしたり、Citrixソリューションとテクノロジーの製品ドキュメントを参照したり、Citrixの役員、製品チーム、技術専門家からの直接的な意見を読んだりできる場所がいくつかあります。それぞれ、Knowledge Center、Product documentation、Blogsのページを参照してください。

よりインタラクティブな支援が必要な場合は、ディスカッションフォーラムに参加して、他の顧客から質問したり、実際の回答を得たりできます。ユーザーグループや関心のある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、Citrix Supportソーシャルネットワーキングサイトを監視しているCitrix Supportエンジニアと交流したりできます。それぞれ、Support ForumsおよびCitrix Communityのページを参照してください。

スキルを向上させるためのトレーニングコースや認定コースも利用できます。Citrix Educationを参照してください。

Citrix Insight Servicesは、Citrix環境向けのシンプルでオンラインのトラブルシューティングプラットフォームおよびヘルスチェッカーを提供します。XenMobile、Citrix Virtual Apps and Desktops、Citrix Hypervisor、およびCitrix Gatewayで利用可能です。Analysis Toolを参照してください。

テクニカルサポートを求めるには、電話またはWeb経由でサポートケースを作成できます。低および中程度の重大度の問題にはWebを使用し、重大度の高い問題には電話オプションを使用できます。XenMobileの問題に関するサポートに連絡するには、Citrix Support Servicesを参照してください。

Citrixソリューションの提供において豊富な経験を持つ、高度な訓練を受けた単一の連絡窓口を求める場合は、Citrix Servicesがテクニカルリレーションシップマネージャーを提供します。Citrixサービスの内容と利点の詳細については、Citrix Worldwide Servicesを参照してください。

XenMobile® でグループ登録招待を送信する

XenMobile Server で、グループおよびネストされたグループに登録招待を送信できます。登録招待は Windows デバイスでは利用できません。

グループ招待を設定する際に、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。また、デバイスにタグを付けて、例えば会社所有のデバイスと従業員所有のデバイスを区別することもできます。その後、ユーザーデバイスの認証タイプを設定します。

> **注:**
>
> カスタム通知テンプレートを使用する予定がある場合は、登録セキュリティモードを構成する前にテンプレートを設定する必要があります。通知テンプレートの詳細については、「通知テンプレートの作成と更新」を参照してください。
>
> ユーザーアカウント、役割、登録セキュリティモード、および招待に関する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、 > の順に移動します。
2. 画面左上にある をクリックし、次に をクリックします。
3. メニューから をクリックします。

   この手順では、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しているユーザーがいないと確信できる場合にのみ、プラットフォームの選択を解除してください。
4. 招待プロセス中にデバイスにタグを付けることができます。 または を選択します。

タグ付けにより、会社所有のデバイスと従業員所有のデバイスを簡単に区別できます。

5. リストで、グループが存在するドメインを選択します。
6. リストで、招待を送信する Active Directory グループを選択します。
7. 「**登録モード**」では、ユーザーが希望する認証セキュリティの種類を設定できます。

   - ユーザー名 + パスワード
   - 高セキュリティ
   - 招待URL
   - 招待URL + PIN
   - 招待URL + パスワード
   - 2要素認証
   - ユーザー名 + PIN

   > **注:**
   >
   > 登録招待を送信するには、**招待URL**、**招待URL + PIN**、または**招待URL + パスワード**の登録セキュリティモードのみを使用できます。**ユーザー名 + パスワード**、**2要素認証**、または**ユーザー名 + PIN**で登録するデバイスの場合、ユーザーはSecure Hubで資格情報を手動で入力する必要があります。

8. **エージェントのダウンロード**、**登録URL**、**登録PIN**、および**登録確認**テンプレートについては、以前に作成したカスタム通知テンプレートを選択するか、リスト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がある場合は、登録セキュリティモードを構成する前にテンプレートを設定する必要があります。通知テンプレートの詳細については、「通知」を参照してください。

   これらの通知テンプレートには、XenMobile内で構成された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**と**最大試行回数**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。これらのオプションは変更できません。

9. 「**招待状を送信**」を「ON」に選択し、「**保存して送信**」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、類似の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のサポート**」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グループから削除されたユーザーにも招待状が送信されています。

「**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伝播するまでに最大6時間かかる場合があります。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でも、XenMobileはそれらのユーザーをグループの一部と見なす可能性があります。

そのため、グループに別のグループ招待状を送信する前に、最大6時間待つのが最善です。

オンプレミスの Device Health Attestation サーバーの構成

オンプレミスの Windows サーバーを介して、Windows 10 および Windows 11 モバイルデバイス向けに Device Health Attestation (DHA) を有効にできます。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、オンプレミスの DHA サービスを有効にするために XenMobile Server ポリシーを作成します。このポリシーの作成については、「Device Health Attestation 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 Technical Preview 5 以降を実行し、デスクトップエクスペリエンスインストールオプションを使用してインストールされたサーバー。
- 1 台以上の Windows 10 および Windows 11 クライアントデバイス。これらのデバイスは、最新バージョンの Windows を実行している TPM 1.2 または 2.0 を搭載している必要があります。
- 次の証明書:

- **DHA SSL 証明書:** エクスポート可能な秘密キーを持つエンタープライズ信頼ルートにチェーンする x.509 SSL 証明書。この証明書は、以下の通信を含む、転送中の DHA データ通信を保護します。
  - サーバー間 (DHA サービスと MDM サーバー)
  - サーバーからクライアント (DHA サービスと Windows 10 または Windows 11 デバイス)
- **DHA 署名証明書:** エクスポート可能な秘密キーを持つエンタープライズ信頼ルートにチェーンする x.509 証明書。DHA サービスはこの証明書をデジタル署名に使用します。
- **DHA 暗号化証明書:** エクスポート可能な秘密キーを持つエンタープライズ信頼ルートにチェーンする x.509 証明書。DHA サービス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内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デバイスは、インターネットに直接アクセスできません。
  - **AIKCert:** AIKCert 検証モードは、インターネットにアクセスできる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デバイスは、インターネットに直接アクセスできる必要があり、Microsoft から AIK 証明書を取得できます。

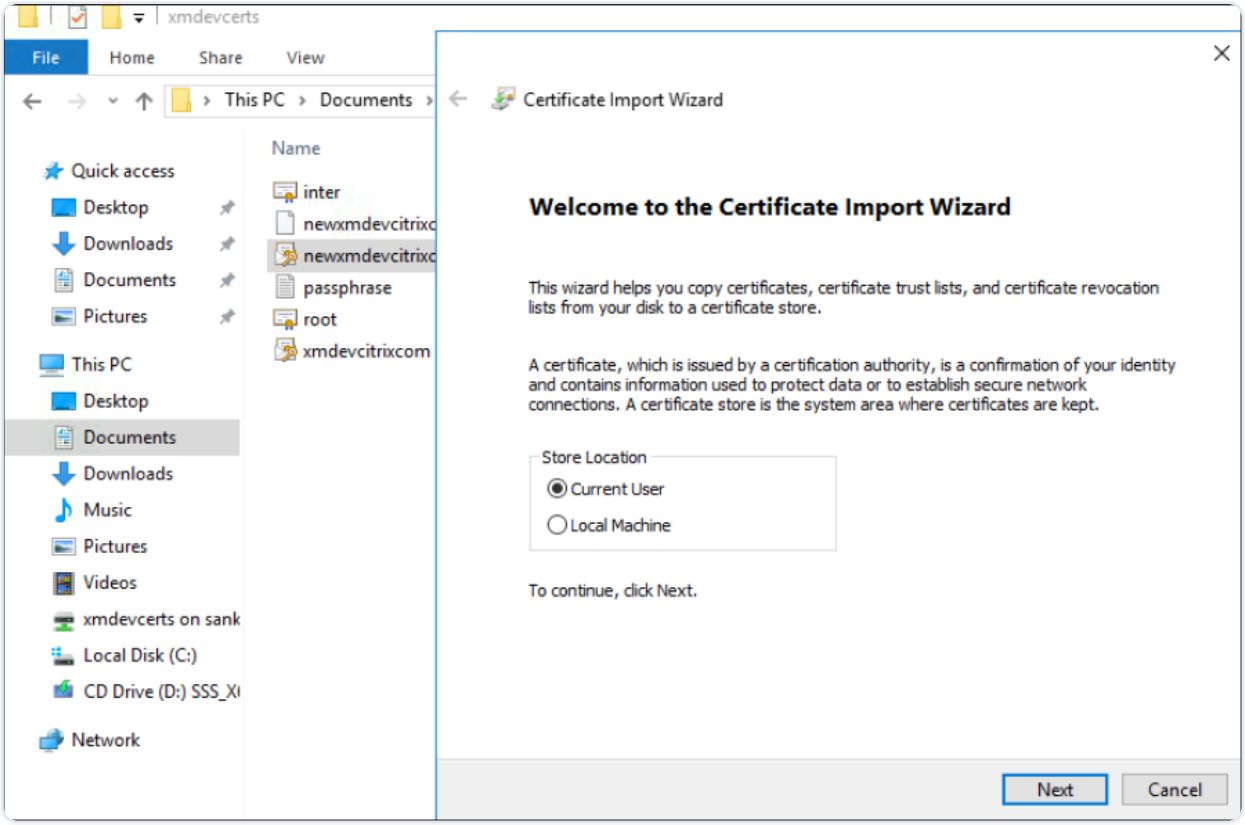
WindowsサーバーにDHAサーバーの役割を追加する

1. Windowsサーバーで、サーバーマネージャーがまだ開いていない場合は、**スタート**をクリックし、次に**サーバーマネージャー**をクリックします。
2. **役割と機能の追加**をクリックします。
3. **開始する前に**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、次に**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、サーバーを選択してから、**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、Device Health Attestation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。

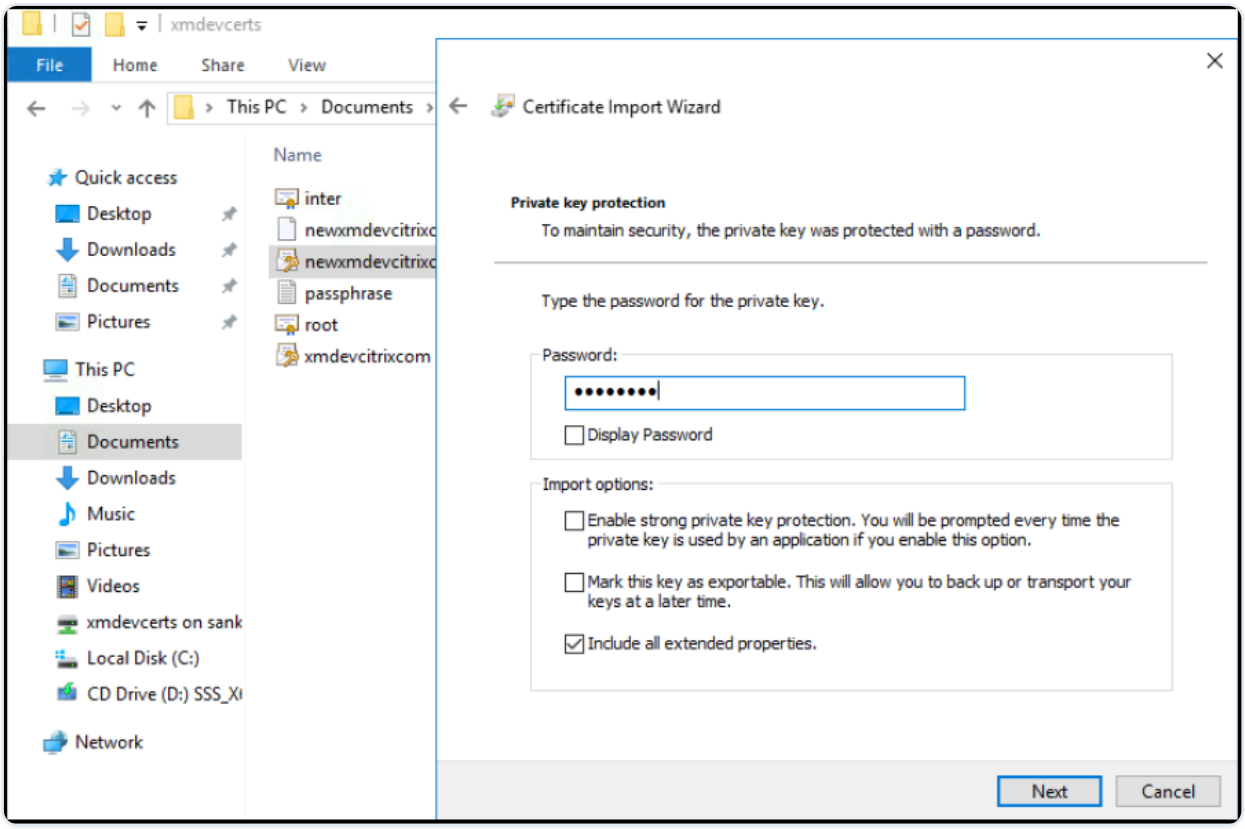
9. **機能の選択**ページで、**次へ**をクリックします。
10. **Webサーバーの役割 (IIS)** ページで、**次へ**をクリックします。
11. **役割サービスの選択**ページで、**次へ**をクリックします。
12. **Device Health Attestationサービス**ページで、**次へ**をクリックします。
13. **インストール選択の確認**ページで、**インストール**をクリックします。
14. インストールが完了したら、**閉じる**をクリックします。

サーバーの証明書ストアにSSL証明書を追加する

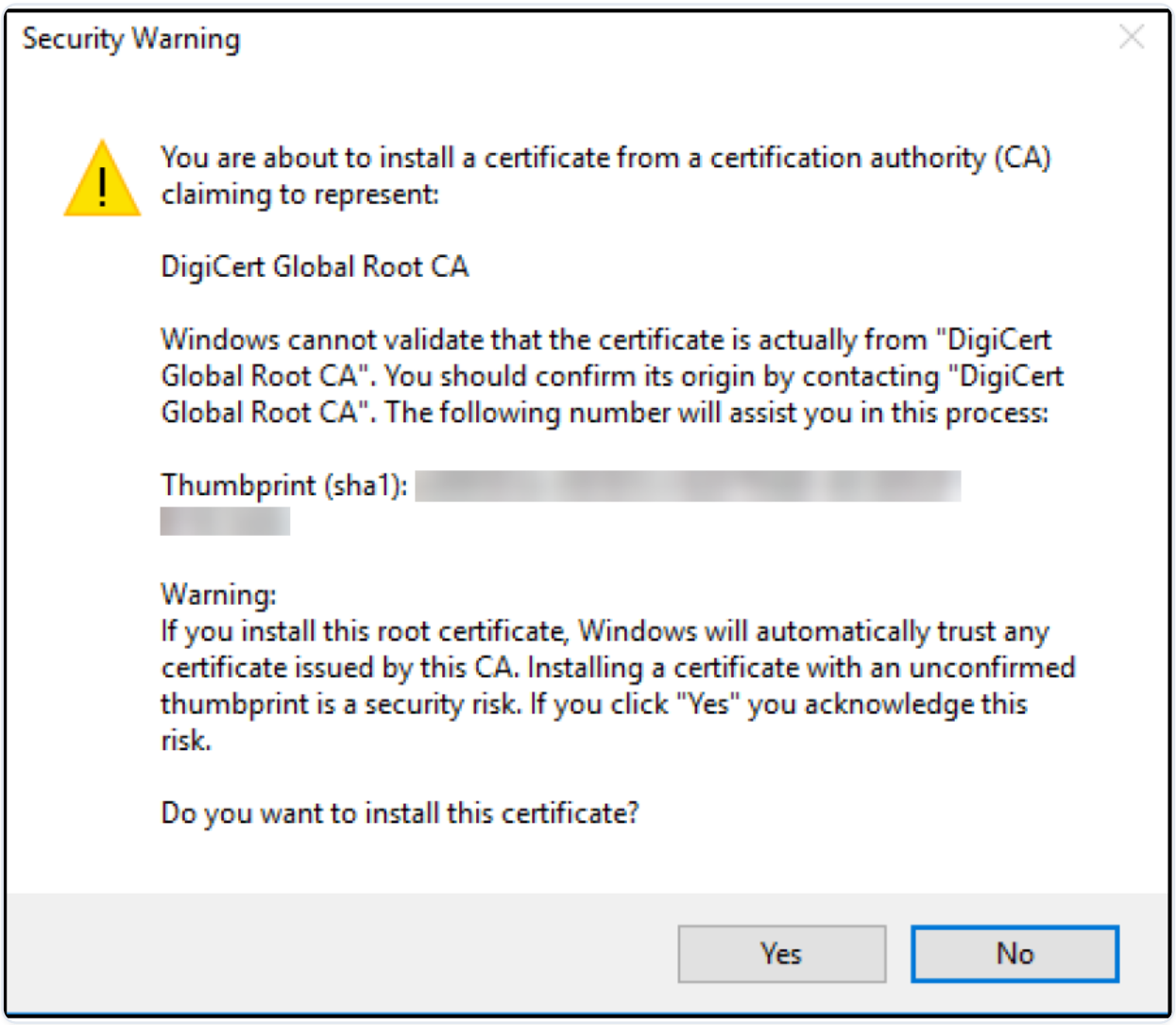
1. SSL証明書ファイルに移動して選択します。
2. ストアの場所として**現在のユーザー**を選択し、**次へ**をクリックします。



3. 秘密キーのパスワードを入力します。
4. インポートオプション**すべての拡張プロパティを含める**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. こ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ていることを確認します。

   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、Enterキーを押します。ローカルコンピューターのストアで証明書を表示するには、管理者ロールである必要があります。

   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、「**マイユーザーアカウント**」を選択します。(サービスアカウントホルダーとしてサイン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. 「コンピューターの選択」ダイアログボックスで、「**完了**」をクリックします。

ウィンドウズ サーバー マネージャー の画像(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. **サーバーマネージャー > IIS** に移動し、アイコンのリストから「**サーバー証明書**」を選択します。

   ウィンドウズ サーバー マネージャー の画像(/en-us/xenmobile/server/media/configure-dha-addcert5.png)

8. 「操作」メニューから「**インポート...**」を選択して、SSL証明書をインポートします。

   ウィンドウズ サーバー マネージャー の画像(/en-us/xenmobile/server/media/configure-dha-addcert6.png)

証明書のサムプリント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...**」をクリックします。

   Windowsファイルエクスプローラーの画像(/en-us/xenmobile/server/media/configure-dha-thumbprint1.png)

3. 利用可能なスナップインから証明書を選択し、選択したスナップインに追加します。

   Windowsスナップインの追加と削除の画像(/en-us/xenmobile/server/media/configure-dha-thumbprint2.png)

4. 「**マイユーザーアカウント**」を選択します。

   「Windows のスナップインの追加と削除」の画像(/en-us/xenmobile/server/media/configure-dha-thumbprint3.png)

5. 証明書を選択し、**OK** をクリックします。

   「Windows のスナップインの追加と削除」の画像(/en-us/xenmobile/server/media/configure-dha-thumbprint4.png)

6. 証明書をダブルクリックし、**詳細** タブを選択します。スクロールして証明書のサムプリントを確認します。

   「Windows のスナップインの追加と削除」の画像(/en-us/xenmobile/server/media/configure-dha-thumbprint5.png)

7. サムプリントをファイルにコピーします。PowerShell コマンドでサムプリントを使用する場合は、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

Windows サーバーでこれらの PowerShell コマンドを実行して、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、示されているように二重引用符で囲んで置き換えます。

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.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、信頼された証明書パッケージをインストールする

Windows サーバーで次のコマンドを実行します。

```
mkdir .\TrustedTpm



expand -F:\* .\TrustedTpm.cab .\TrustedTpm



cd .\TrustedTpm



.\setup.cmd
```

DHA サービスを構成する

Windows サーバーでこ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。

```
Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
ReplaceWithThumbprint



-SigningCertificateThumbprint ReplaceWithThumbprint



-SslCertificateStoreName My -SslCertificateThumbprint
ReplaceWithThumbprint



-SupportedAuthenticationSchema "AikCertificate"
```

Windows サーバーでこれらのコマンドを実行して、DHA サービスの証明書チェーンポリシーを設定します。

```
$policy = Get-DHASCertificateChainPolicy



$policy.RevocationMode = "NoCheck"



Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
```

これらのプロンプトには次のように応答します。

```
  Confirm



    Are you sure you want to perform this action?
```

```
    Performing the operation "Install-DeviceHealthAttestation" on target
"WIN-N27D1FKCEBT".



    [Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help
(default is "Y"): A



    Adding SSL binding to website 'Default Web Site'.



    Add SSL binding?



    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y



    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.



    Add application pool?



    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y



    Adding web application 'DeviceHealthAttestation' to website 'Default
Web Site'.



    Add web application?
```

```
    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Adding firewall rule 'Device Health Attestation Service' to allow
inbound connections on port(s) '443'.


    Add firewall rule?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Setting initial configuration for Device Health Attestation Service.


    Set initial configuration?


    [Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): Y


    Registering User Access Logging.


    Register User Access Logging?


    [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) とサムプリントが表示されます。

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、示されている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、サムプリントが表示されます。

最終確認を行うには、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、「Method not allowed」と表示されます。

DHA サービスチェックの画像(/en-us/xenmobile/server/media/configure-dha-finalcheck.png)

Secure Mail プッシュ通知用の EWS を使用した証明書ベース認証の構成

寄稿者: ヴィジャイ・クマール・クンチャクリ

Secure Mail プッシュ通知が機能するように、Exchange Server を証明書ベース認証用に構成する必要があります。これは、Secure Hub が証明書ベース認証で XenMobile® に登録されている場合に必要です。

Exchange メールサーバー上の Active Sync および Exchange Web Services (EWS) 仮想ディレクトリを証明書ベース認証で構成する必要があります。

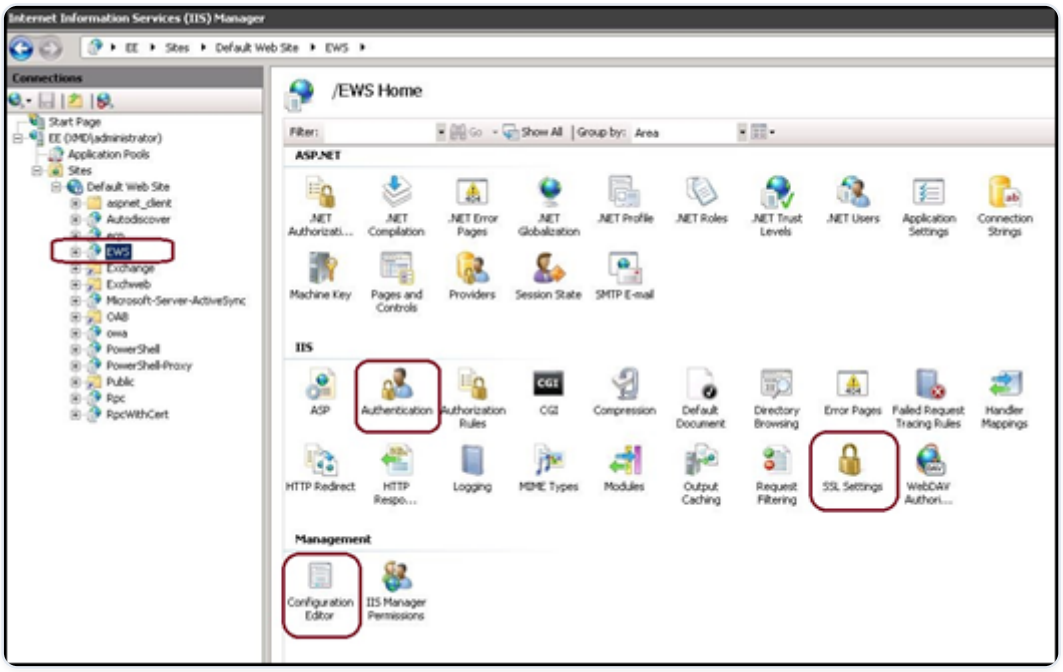
これらの構成を完了しない限り、Secure Mail プッシュ通知のサブスクリプションは失敗し、Secure Mail でバッジの更新は行われません。

この記事では、証明書ベース認証を構成する手順について説明します。これらの構成は、特に Exchange Server 上の EWS 仮想ディレクトリに対して行われます。

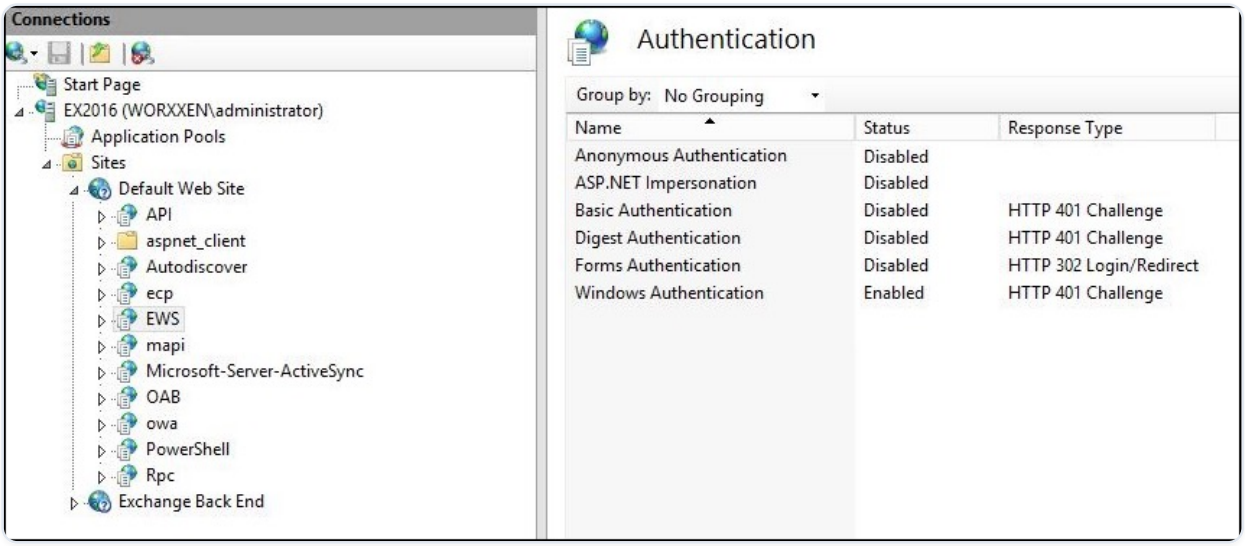
構成を開始するには、次の手順を実行します。

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. **Default Web Site** の下にある 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。



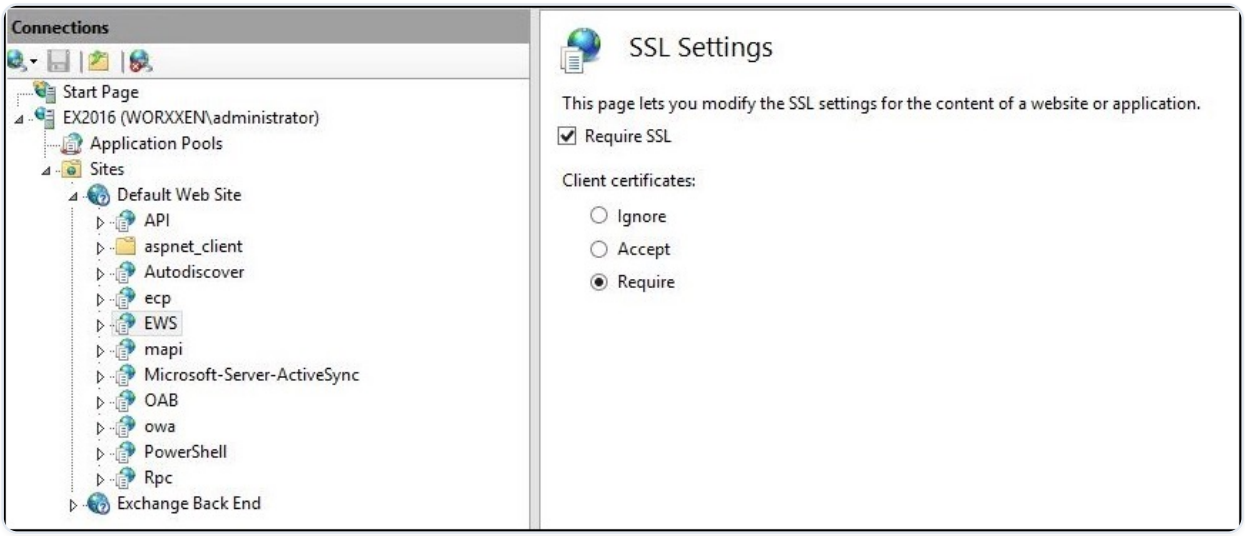
4. EWS の **認証** 設定が次の図に示すように構成されていることを確認します。



5. EWS 仮想ディレクトリの **SSL 設定** を構成します。

   a. **Require SSL**チェックボックスをオンにします。

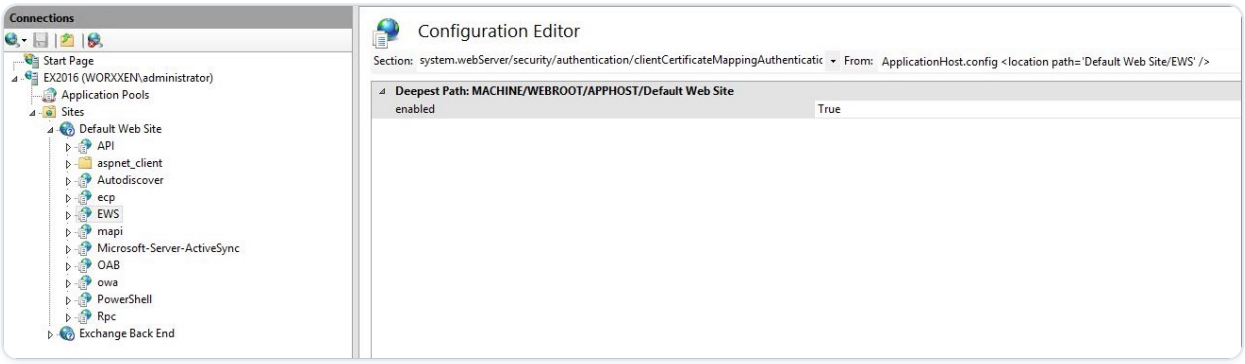
   b. **Client Certificates**の下で、**Require**をクリックします。他のEWSメールクライアントがユーザー名とパスワードを認証情報として使用してExchange Serverに接続する場合、このオプションを**Accept**に設定できます。



6. **Configuration Editor**をクリックします。**Section**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. **enabled**の値を**True**に設定します。



8. **Configuration Editor**をクリックします。**Section**ドロップダウンリストで、次のセクションに移動します。

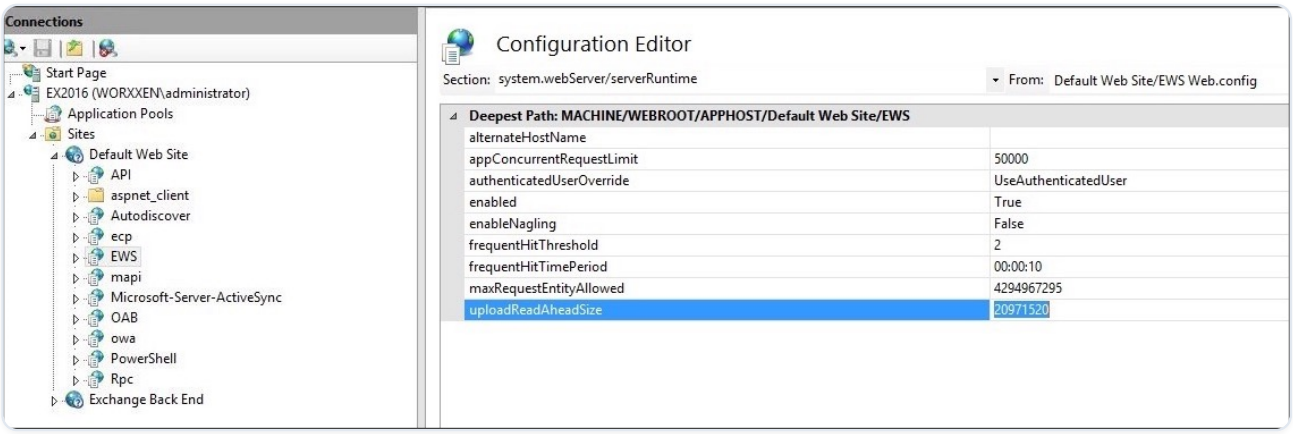
   - **system.webServer/serverRuntime**

9. **uploadReadAheadSize**の値を**10485760** (10 MB) または**20971520** (20 MB)、または組織の要件に応じて設定します。

> **重要：**
>
> この値を正しく設定しないと、EWSプッシュ通知の購読時に証明書ベースの認証がエラーコード413で失敗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。

詳細については、以下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プッシュ通知でのSecure Mailの問題のトラブルシューティングに関する詳細については、この Citrix Support Knowledge Centerの記事を参照してください。

関連情報

iOS版Secure Mailのプッシュ通知

XenMobile® モバイルデバイス管理 (MDM) と Cisco Identity Services Engine (ISE) の統合

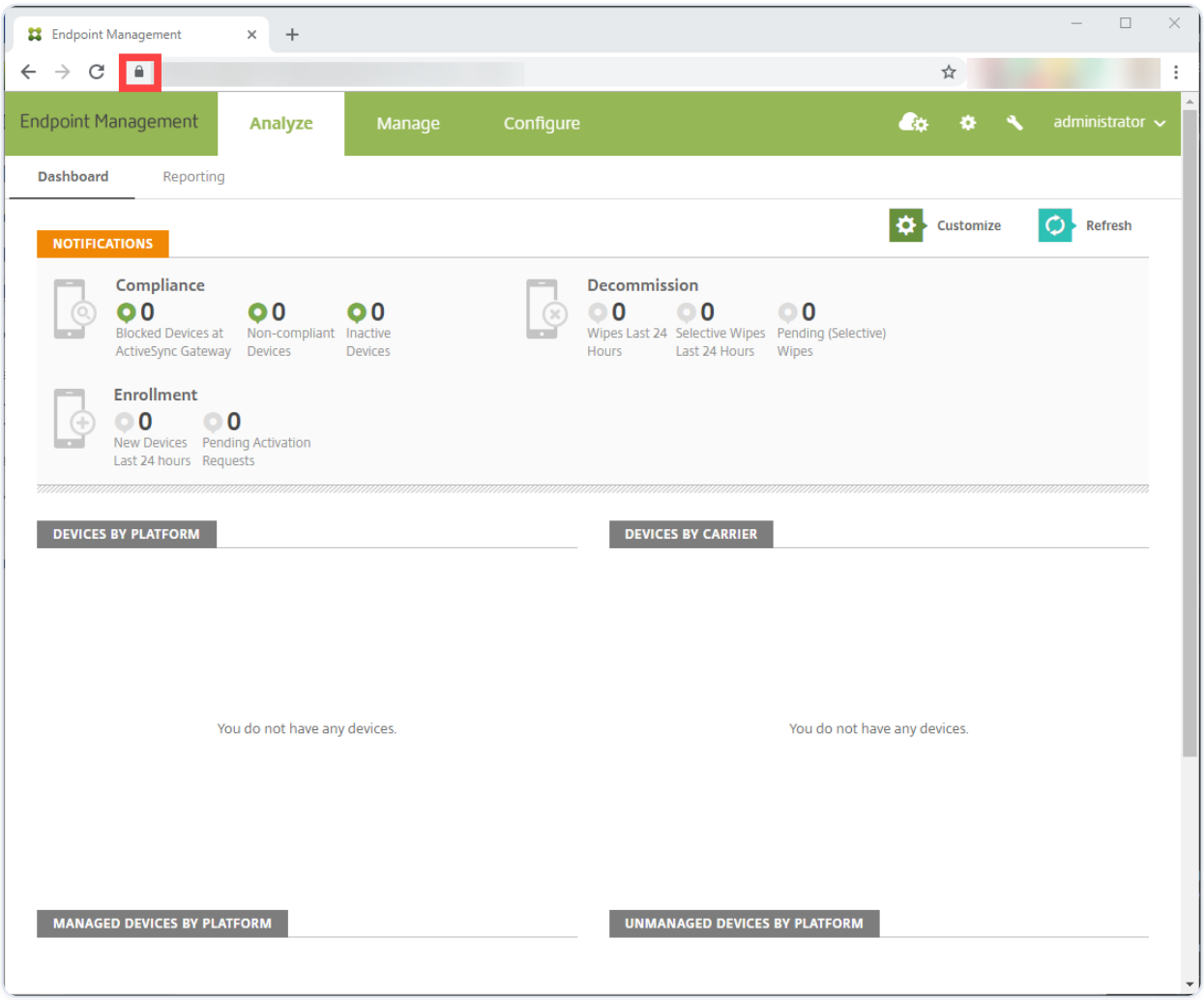
Cisco ISE は、職場におけるモバイルデバイスの展開、セキュリティ保護、監視、統合、および管理に使用されます。モバイルデバイスにダウンロードされたソフトウェアは、以下を制御します。

- アプリケーションとパッチの配布
- エンドポイント上のデータと構成

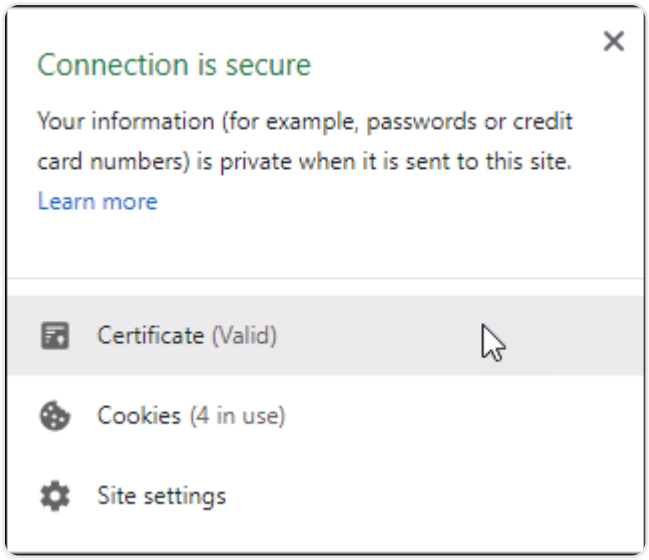
XenMobile は Cisco ISE と統合して、Cisco ISE コンソールで非準拠デバイスや未管理デバイスを管理できます。XenMobile を使用すると、企業サービスへのアクセスを選択的に許可、拒否、または隔離することもできます。

XenMobile との統合を設定するには、XenMobile Server 上に管理者 RBAC ロールが割り当てられたローカルサービスアカウントを作成します。このロールにより、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。

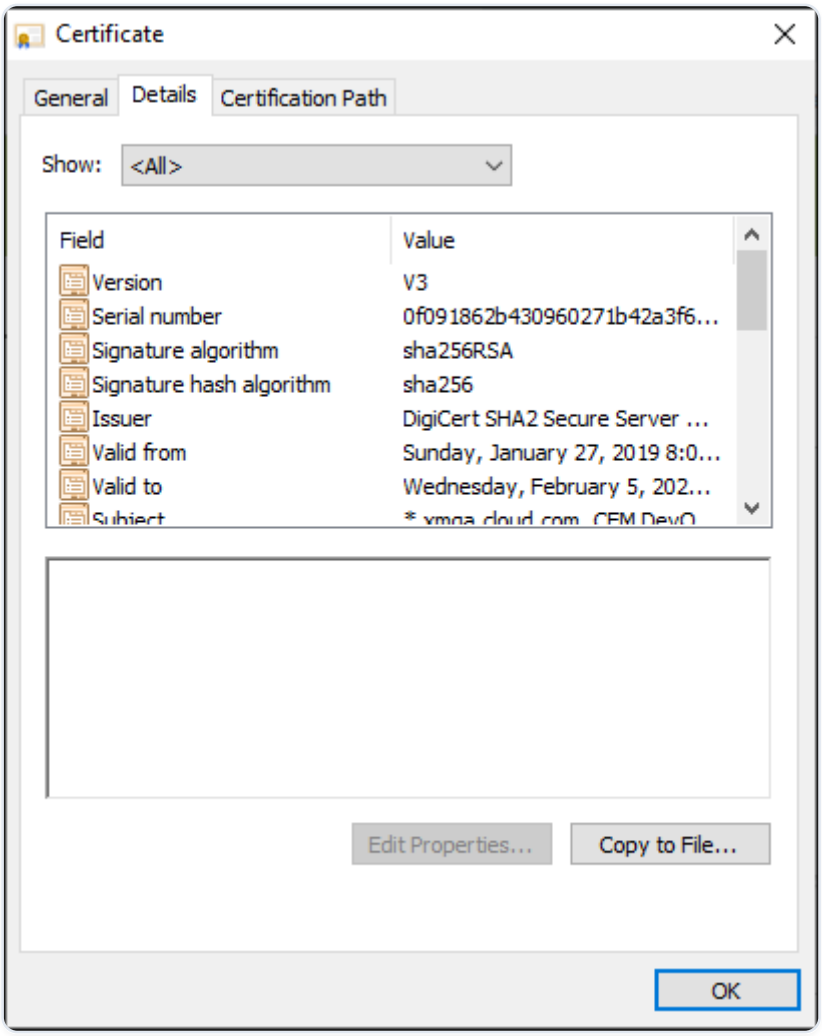
1. ログイン後、アドレスバーの URL の横にあるロックをクリックします。



2. をクリックします。



3. タブを選択し、 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。証明書を Cisco ISE の信頼済み証明書ストアにインポートします。これは、Cisco ISE が XenMobile Server との通信を信頼するために必要です。

   a. **> > > >** の順に移動します。 をクリックします。

   b. 証明書に名前を付け、 と のチェックボックスをオンにします。

6. Cisco ISE 内で XenMobile を外部 MDM として追加します。

   a. **> >** の順に移動します。 をクリックして、以下を入力します。

      - **サーバーホスト:** XenMobile FQDN
      - **ポート:** 443
      - **インスタンス名:** XenMobile Server のインスタンス名です。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管理者アカウントである必要があります。
- **パスワード:** 追加したユーザーのパスワード。
- **有効**と表示されている箇所をオンにします。

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。

> **注:**
>
> ISE 統合は、ホスト型 Endpoint Management ではサポートされていません。

Citrix XenMobile® Server ドキュメント履歴

以下の表は、XenMobile Server製品ドキュメントの重要な変更点について説明しています。これらの更新に関する通知を受け取るには、RSSフィードを購読してください。

日付	変更点	説明
27 Jan 2026	XenMobile Server 10.16 ローリングパッチ 8 のリリースノート	
20 Nov 2025	XenMobile Server 10.15 ローリングパッチ 13 のリリースノート	
13 Nov 2025	XenMobile Server 10.16 ローリングパッチ 7 のリリースノート	
23 Oct 2025	XenMobile Server 10.15 ローリングパッチ 12 のリリースノート	
26 Sep 2025	XenMobile Server 10.16 ローリングパッチ 6 のリリースノート	
13 May 2025	XenMobile Server 10.15 ローリングパッチ 11 のリリースノート	サポート記事 CTX693257 を参照してください。
15 Apr 2025	XenMobile Server 10.16 ローリングパッチ 5 のリリースノート	サポート記事 CTX692919 を参照してください。

日付	変更点	説明
27 Jan 2025	XenMobile Server 10.15 ローリングパッチ 10 のリリースノート	サポート記事 CTX692560 を参照してください。
18 Dec 2024	XenMobile Server 10.16 ローリングパッチ 4 のリリースノート	サポート記事 CTX692370 を参照してください。
04 Dec 2024	XenMobile Server 10.15 ローリングパッチ 9 のリリースノート	サポート記事 CTX692268 を参照してください。
28 Aug 2024	XenMobile Server 10.16 ローリングパッチ 3 のリリースノート	サポート記事 CTX691503 を参照してください。
11 Jul 2024	XenMobile Server 10.15 ローリングパッチ 8 のリリースノート	サポート記事 CTX691107 を参照してください。
02 Jul 2024	XenMobile Server 10.16 ローリングパッチ 2 のリリースノート	サポート記事 CTX678043 を参照してください。
17 Jun 2024	XenMobile Server 10.16 ローリングパッチ 1 のリリースノート	サポート記事 CTX677872 を参照してください。
06 Jun 2024	XenMobile Server 10.15 ローリングパッチ 7 のリリースノート	サポート記事 CTX677079 を参照してください。
08 Mar 2024	XenMobile Server 10.14 ローリングパッチ 13 のリリースノート	サポート記事 CTX628921 を参照してください。
06 Mar 2024	XenMobile Server 10.15 ローリングパッチ 6 のリリースノート	サポート記事 CTX625010 を参照してください。

日付	変更点	説明
13 Nov 2023	XenMobile Server 10.15 ローリングパッチ 5 のリリースノート	サポート記事 CTX583748 を参照してください。
19 Oct 2023	XenMobile Server 10.14 ローリングパッチ 12 のリリースノート	サポート記事 CTX582535 を参照してください。
18 Sep 2023	XenMobile Server 10.15 ローリングパッチ 4 のリリースノート	サポート記事 CTX579528 を参照してください。
19 Jul 2023	XenMobile Server 10.15 ローリングパッチ 3 のリリースノート	サポート記事 CTX565649 を参照してください。
31 May 2023	XenMobile Server 10.14 ローリングパッチ 11 のリリースノート	サポート記事 CTX558678 を参照してください。
26 Apr 2023	XenMobile Server 10.15 ローリングパッチ 2 のリリースノート	サポート記事 CTX546782 を参照してください。
11 Apr 2023	XenMobile Server 10.14 ローリングパッチ 10 のリリースノートに修正された問題を追加	修正された問題を参照してください。
23 Mar 2023	XenMobile Server 10.14 ローリングパッチ 10 のリリースノート	サポート記事 CTX491036 を参照してください。
23 Feb 2023	XenMobile Server 10.15 ローリングパッチ 1 のリリースノート	サポート記事 CTX478719 を参照してください。
20 Dec 2022	XenMobile Server 10.14 ローリングパッチ 9 のリリースノート	サポート記事 CTX477055 を参照してください。

日付	変更点	説明
16 Nov 2022	XenMobile Server 10.15 リリースに関する記事を更新	新機能および変更された機能の概要については、XenMobile Server 10.15 の新機能を参照してください。
22 Sep 2022	XenMobile Server 10.14 ローリングパッチ 8 のリリースノート	サポート記事 CTX464099 を参照してください。
08 Sep 2022	XenMobile Server 10.13 ローリングパッチ 10 のリリースノート	サポート記事 CTX463922 を参照してください。
18 Aug 2022	XenMobile Server 10.14 ローリングパッチ 7 のリリースノート	サポート記事 CTX463691 を参照してください。
14 Jun 2022	XenMobile Server 10.13 ローリングパッチ 9 のリリースノート	サポート記事 CTX460128 を参照してください。
23 May 2022	XenMobile Server 10.14 ローリングパッチ 6 のリリースノート	サポート記事 CTX459871 を参照してください。
12 Apr 2022	XenMobile Server 10.13 ローリングパッチ 8 のリリースノート	サポート記事 CTX447596 を参照してください。
30 Mar 2022	XenMobile Server 10.14 ローリングパッチ 5 のリリースノート	サポート記事 CTX399411 を参照してください。
01 Mar 2022	XenMobile Server 10.13 ローリングパッチ 7 のリリースノート	サポート記事 CTX341602 を参照してください。
26 Jan 2022	XenMobile Server 10.14 ローリングパッチ 4 のリリースノート	サポート記事 CTX339069 を参照してください。

日付	変更点	説明
22 Dec 2021	XenMobile Server 10.14 ローリングパッチ 3 のリリースノート	サポート記事 CTX335897 を参照してください。
21 Dec 2021	XenMobile Server 10.13 ローリングパッチ 6 のリリースノート	サポート記事 CTX335875 を参照してください。
21 Dec 2021	XenMobile Server 10.12 ローリングパッチ 11 のリリースノート	サポート記事 CTX335861 を参照してください。
16 Dec 2021	XenMobile Server 10.12 ローリングパッチ 10 のリリースノート	サポート記事 CTX335785 を参照してください。
15 Dec 2021	XenMobile Server 10.14 ローリングパッチ 2 のリリースノート	サポート記事 CTX335763 を参照してください。
15 Dec 2021	XenMobile Server 10.13 ローリングパッチ 5 のリリースノート	サポート記事 CTX335753 を参照してください。
19 Nov 2021	XenMobile Server 10.14 ローリングパッチ 1 のリリースノート	サポート記事 CTX335342 を参照してください。
08 Oct 2021	XenMobile Server 10.12 ローリングパッチ 9 のリリースノート	サポート記事 CTX331040 を参照してください。
15 Sep 2021	XenMobile Server 10.14 リリースに関する記事を更新	新機能および変更された機能の概要については、XenMobile Server 10.14 の新機能を参照してください。
11 Aug 2021	XenMobile Server 10.13 ローリングパッチ 4 のリリースノート	サポート記事 CTX324159 を参照してください。

日付	変更点	説明
02 Jun 2021	XenMobile Server 10.12 ローリングパッチ 8 のリリースノート	サポート記事 CTX316910 を参照してください。
13 May 2021	XenMobile Server 10.13 ローリングパッチ 3 のリリースノート	サポート記事 CTX315034 を参照してください。
27 Apr 2021	[場所の特定] セキュリティアクションの説明を更新	セキュリティアクションを参照してください。
23 Apr 2021	アクションの例を追加	自動化されたアクションを参照してください。
01 Apr 2021	アプリごとのVPN要件の説明を追加	VPNデバイスポリシーを参照してください。
24 Feb 2021	エンドポイントをiOS 14.5にアップグレードする前に必要な準備に関する発表を追加	エンドポイントをiOS 14.5にアップグレードする前にを参照してください。
17 Dec 2020	Android Enterpriseでインストール済みの管理対象アプリが更新される方法を制御する新しいデバイスポリシー	管理対象アプリの自動更新デバイスポリシーを参照してください。
18 Nov 2020	オンプレミスCitrix ADCに関連するシングルサインオンの問題の回避策を追加	オンプレミスCitrix ADCをアップグレードする前にを参照してください。
26 Oct 2020	XenMobile Server 10.13 リリースに関する記事を更新	新機能および変更された機能の概要については、XenMobile Server 10.13 の新機能を参照してください。
02 Jul 2020	MDX暗号化の廃止に関するタイムラインとアクションプランを追加	今後の変更に備えてAndroidデバイスを準備するを参照してください。
19 Jun 2020	ドキュメント内の「ブラックリスト」と「ホワイトリスト」という用語に対応。「ブ	Endpoint Managementコンソールには現在、「ブラックリスト」と「ホワイトリス

日付	変更点	説明
	ロックリスト」と「許可リスト」に変更。	ト」という用語が含まれています。ドキュメントを更新しました。今後のリリースに向けて、製品コンソール内の用語を変更する作業を進めています。
04 May 2020	iOS、iPadOS、およびmacOSの信頼された証明書に関する新しいTLS証明書要件についての注記を追加。	証明書を参照してください。
18 Feb 2020	用語を更新	ドキュメント全体で、NetScaler®、NetScaler Gateway、ShareFile、およびストレージゾーンコントローラーの用語を更新しました。一部のコンソールコンポーネントには、古い名前が表示されている場合があります。
06 Feb 2020	XenMobile Server 10.12 リリースに関する記事を更新	新機能および変更された機能の概要については、XenMobile Server 10.12 の新機能を参照してください。
06 Nov 2019	Apple VPPからABMまたはASMへの移行に関するセクションを追加	Apple Volume Purchase ProgramからApple Business Manager (ABM) およびApple School Manager (ASM) への移行を参照してください。
04 Sep 2019	XenMobile Server 10.11 リリースに関する記事を更新	新機能および変更された機能の概要については、XenMobile Server 10.11 の新機能を参照してください。
15 May 2019	iOSデバイス登録セクションを更新	iOS 12デバイス登録のビデオと手順を更新しました。iOSデバイスの登録を参照してください。

日付	変更点	説明
10 May 2019	Entrust PKIに関する新しいセクション	「PKIエンティティ」の記事にセクションを追加しました:PKIエンティティ。
03 Apr 2019	Apple DEP更新手順の新しいセクション	「Apple DEPによるデバイスの展開」にセクションを追加しました:Apple Deployment Programへの登録を更新。
02 Apr 2019	Exchange ActiveSync 8.5.3リリース用Gatewayコネクタに関する記事を更新	新機能および変更された機能の概要については、バージョン8.5.3の新機能を参照してください。
26 Mar 2019	Secure Hubストア名の構文を更新	アプリストアとCitrix Secure Hubのブランド設定で、ストア名の英数字要件に関する注記を追加しました。
06 Mar 2019	Exchange ActiveSync 10.1.9リリース用Endpoint Managementコネクタに関する記事を更新	新機能および変更された機能の概要については、バージョン10.1.9の新機能を参照してください。
01 Feb 2019	Exchange ActiveSync 10.1.8リリース用Endpoint Managementコネクタに関する記事を更新	新機能および変更された機能の概要については、バージョン10.1.8の新機能を参照してください。
23 Jan 2019	Secure Browseの用語を更新	ドキュメント全体で、MDX設定の「Secure Browse」を「Tunneled Web SSO」に名称変更しました。詳細については、iOSの場合はアプリネットワークアクセス、Androidの場合はアプリネットワークアクセスを参照してください。