XenMobile Server 10.3.x

Oct 25, 2016

XenMobileサーバー10.3.6について

Oct 25, 2016

XenMobile 10.3.6 Service Packには、XenMobile 10.3.5からのみ直接アップグレードできます。

> **注意**
>
> XenMobileを10.3.6にアップグレードする前に、CitrixライセンスのSubscription Advantage（SA）日付が2016年6月1日以降である必要があります。 SA日付は、ライセンスサーバーのライセンスの隣に表示されています。 SA日付を更新するには、Citrixポータルから最新のライセンスファイルをダウンロードし、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、http://support.citrix.com/article/CTX209580を参照してください。

アップグレードを行うには、xms_10.3.6.310.binを使用します。 XenMobileコンソールで、右上の歯車アイコンをクリックした後、［**Release Management**］をクリックします。 ［**Upgrade**］をクリックしてから、xms_10.3.6.310.binファイルをアップロードします。 コンソールでのアップグレードについて詳しくは、「XenMobileのアップグレード」を参照してください。

XenMobile 10.3.6を新たにインストールする場合は、「XenMobileのインストール」を参照してください。

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

XenMobile 10.3.6の新機能

XenMobile 10.3.6リリースでは、品質とスケーラビリティに重点が置かれています。 バグ修正について詳しくは、「XenMobile 10.3.6の既知の問題および解決された問題」を参照してください。 XenMobile 10.3.6には、次の新機能もあります。

スケーラビリティの改善

XenMobile 10.3.6サーバーで品質が大幅に向上したことにより、XenMobileサーバーとデータベースの通信、XenApp統合、デバイスへの展開の通知、LDAP検索などの領域でのスケールとパフォーマンスも向上しました。

- HDX列挙は、XenMobile 10.3.5と比較して約40%改善されました。
- XenMobile CLIメインメニューで**Server Tuning**コマンド（**Advanced Settings**のオプション**5**）を使用した場合に次の設定に適用されるデフォルトが、以下のように変更されました。

  Maximum connections on port 443：デフォルト値が**10000**から**12000**に変わりました。

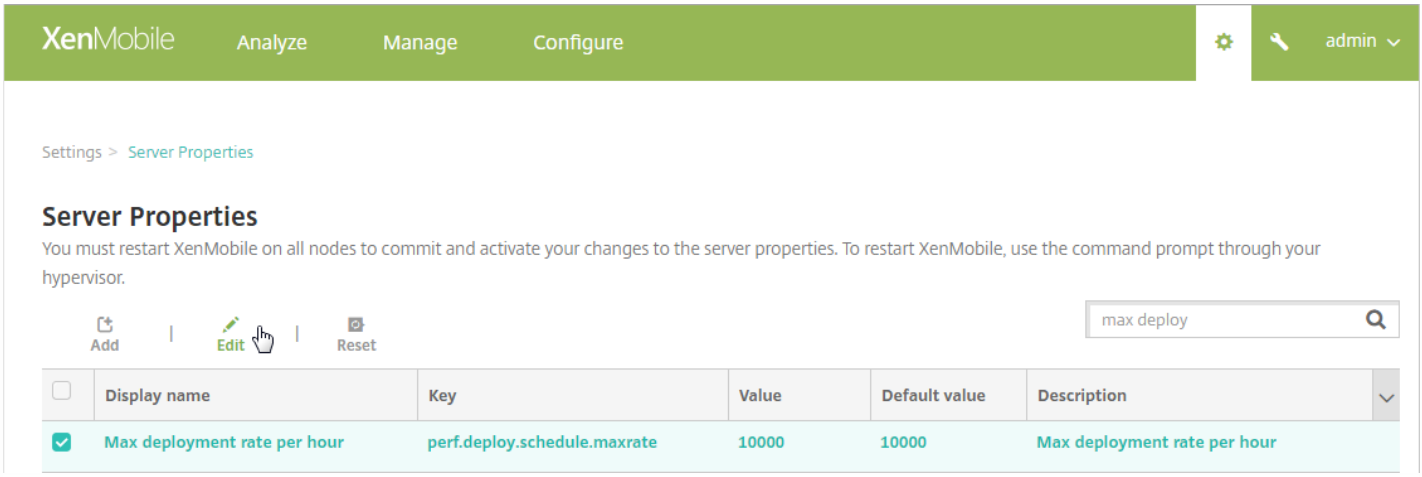
  Maximum connections on port 8443：デフォルト値が**10000**から**12000**に変わりました。

  Maximum threads on port 443：デフォルト値が**750**から**2000**に変わりました。

  Maximum threads on port 8443：デフォルト値が**750**から**2000**に変わりました。

- iOSとWindows Phoneデバイス、およびGoogle Cloud Messaging用に構成されたAndroidデバイスからの再接続要求の急増を防ぐため、XenMobileは段階的展開で通知を送信するようになりました。 展開のレートのデフォルトは毎時10,000デバ

イスです。 展開のレートを変更するには、 **[Max deployment rate]** サーバープロパティ（perf.deploy.schedule.maxrate）を編集します。



- XenMobile展開の対象は、ターゲットデリバリーグループに含まれるデバイスのみになりました。 これまでは、役割に関係なくすべてのデバイスが展開されていました。

Worxアプリの更新

Worx Home

- **WorxMailによるログの送信**：ユーザーが問題の報告時にログを送信する場合、デフォルトでWorxMailが開くようになりました。 これにより、ユーザーはサイズの大きいファイルを送信できます。 Worx Homeの以前のバージョンでは、サイズの大きいファイルの送信が失敗することがありました。

WorxMail

- **Exchange Server 2016のサポート**： WorxMailをExchange Server 2016と統合できるようになりました。 Active Sync 14がサポートされますが、WorxMailにはActive Sync 16との互換性も必要です。
- **ShareFileからのファイルの添付（Android）**： **[Attach from ShareFile]** をタップすると、電子メールまたはカレンダーイベントにファイルを添付できます。
- **ShareFileの制限付きStorageZoneおよびコネクタからのファイルの添付（iOS）**。 電子メールまたはカレンダーイベントで **[Attach from ShareFile]** をタップすると、電子メールやカレンダーイベントに、ShareFileからだけでなく、制限付きStorageZonesおよびコネクタ（SharePointやネットワーク共有など）からもファイルを添付できます。
- **.vcardファイルによる連絡先データの共有**：ユーザーは、.vcardファイルとして送信された添付ファイルから連絡先情報をインポートできます。
- **新しいネットワークアクセスのデフォルト**：MDX Toolkitの**ネットワークアクセス**ポリシーのデフォルトは **[Tunneled to the internal network]** になりました。 この変更により、構成エラーが軽減されます。

WorxWeb

- **デフォルトでのポップアップのブロック**：Safariのポップアップをデフォルトでブロックするには、XenMobileコンソールを使用して**制限**デバイスポリシーの **[Block pop-ups]** オプションを **[On]** に設定します。 バージョン10.3.6にアップグレードする前に **[Block pop-ups]** を **[Off]** に設定した場合、この設定はオフのままとなります。 そうでない場合は、設定は **[On]** になり、Safariのポップアップはブロックされます。
- **ShareFileでのリンクの開き方**：ShareFile 4.0では、リンクをブラウザで開くか、ShareFileで直接開くかを選択できます。

WorxChatのテクニカルプレビュー

- **Androidのサポート：** WorxChatをAndroidで使用できるようになりました。
- **Lync 2013およびSkype for Business 2015のサポート：** WorxChatを同じプールにあるLync 2013およびSkype for Business 2015と統合できるようになりました。

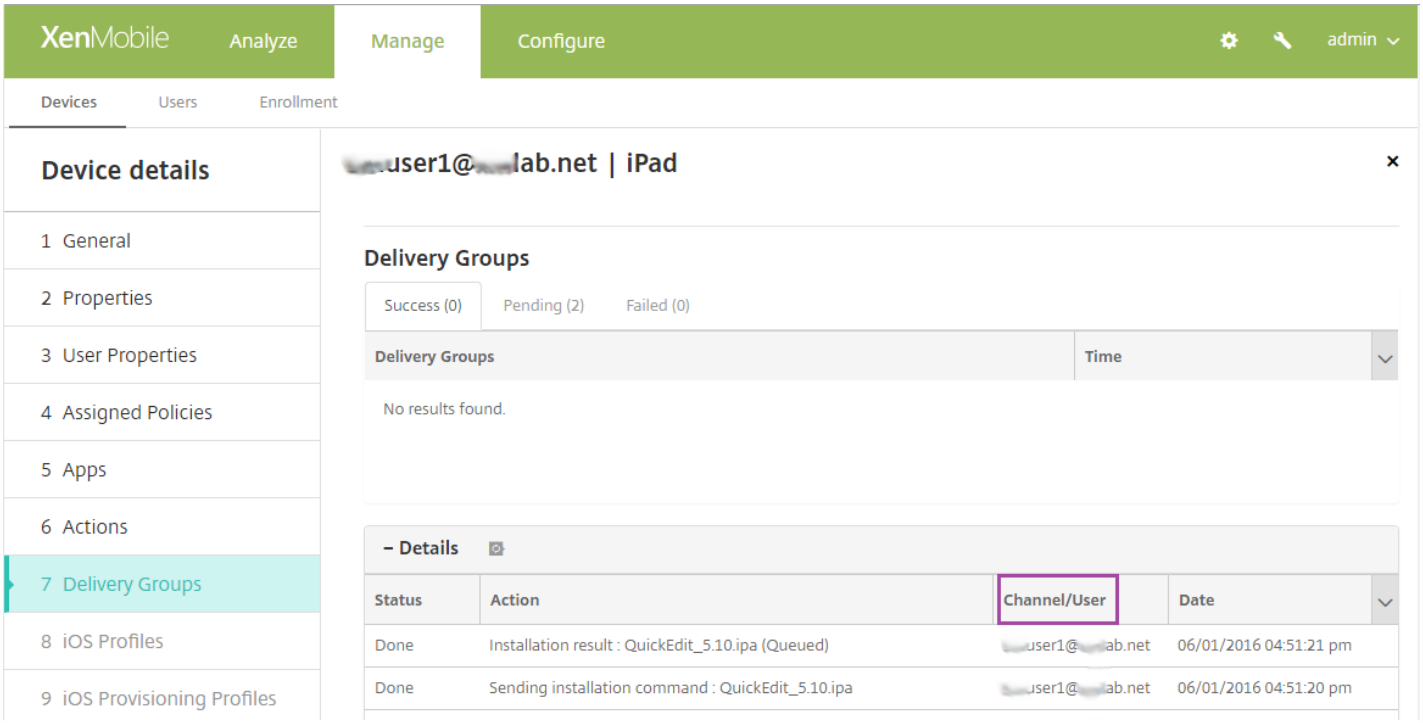
Secure Forms

- **ShareFileの制限付きゾーンのサポート：** Secure FormsをShareFileの制限付きゾーンで構成できるようになりました。 設定手順については、「Secure FormsとShareFileの統合」を参照してください。
- **iBeacon機能：** iBeacon技術を使用して、モバイルアプリ上のフォームに自動入力できるビーコンを構成および追跡できます。 ビーコン情報は、ユーザーがフォームを送信するときに含められます。 ビーコンの設定について詳しくは、「ビーコン」を参照してください。
- **作成者名：** Secure Forms Composerに、フォームを作成したユーザーの名前が表示されるようになりました。 この機能により、Composerに複数のユーザーがアクセスする場合に追跡を行いやすくなりました。
- **番号の範囲：** Composerの［**Number**］フィールドで、ユーザーがフォームの入力時に入力可能な番号の範囲を指定できます。
- **新規ファイル名形式：** モバイルアプリで送信したフォームおよび添付ファイルが送信者名とタイムスタンプ付きで保存されるようになり、ファイル名の確認と整理がしやすくなりました。

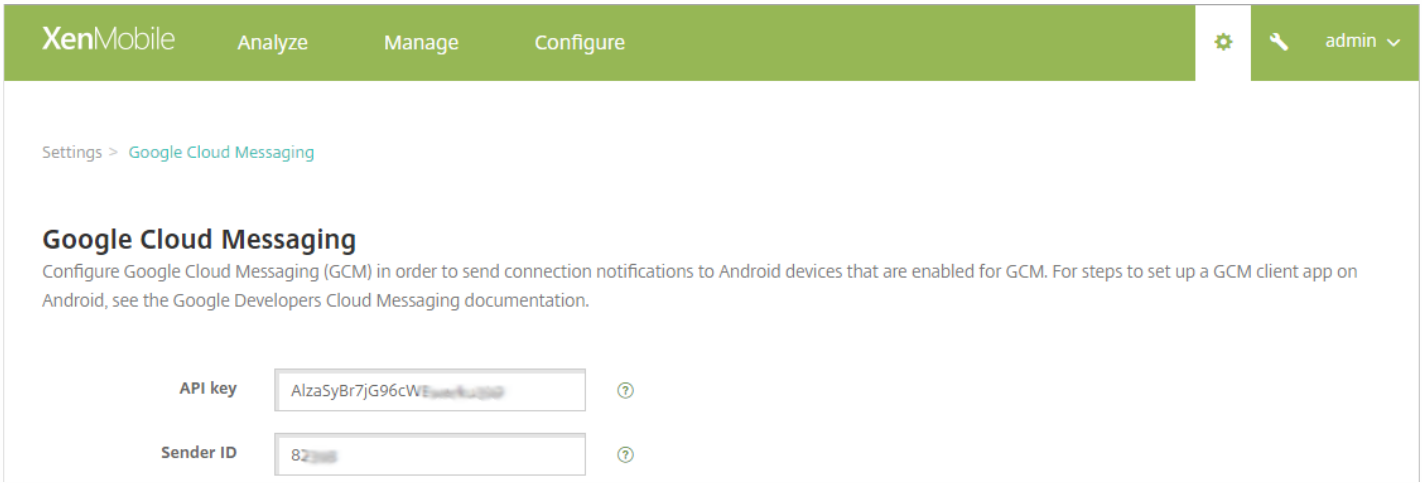
詳しくは、「Worxモバイルアプリの新機能」を参照してください。

その他の更新

- **追加のCitrixコンポーネントバージョンのサポート：**
  - NetScaler Gateway 10.5.x、11.0.x、11.1.x（XenMobileオンプレミス）
  - NetScaler Gateway 10.5.57.7（XenMobile Cloud）
  - XenAppおよびXenDesktop 7.9と7.8
  - StoreFront 3.6
  - ライセンスサーバー11.13.1.2
- **WiFiネットワークのホワイトリストへの追加：**Whitelisted WiFi networksポリシーを使用すると、許可されるネットワークを指定できます。 アプリは、ホワイトリストに含まれているいずれかのネットワークに接続されているときのみ動作します。 この機能は、MDM+MAMモードでのみ使用できます。
- **ShareFileでの共有デバイスのサポート：**ShareFile Mobileアプリのバージョン4.4では、MDM+MAMモードの共有デバイスがサポートされるようになりました。これにより、複数のユーザーが再登録せずにデバイスを共有できます。 詳しくは、「XenMobileの共有デバイス」を参照してください。
- **アイコンの制御（iOS）：**アプリ開発者は、info.plistの代わりに、アプリバンドルのルートフォルダーにアイコンファイルを含めることができるようになりました。 ツールキットがアイコンファイルを見つけられるように、アイコンファイルの名前は次のいずれかの形式にする必要があります。
  - icon.png
  - icon-60x2.pn
  - icon-72.png
  - icon-76.png
- **メール同期の改善（iOS）：**メール同期およびShareFile統合が更新され、メール同期の信頼性が向上しました。
- **デバイス情報の追加：**XenMobileコンソールの［**Device details**］ページに、デバイス上の展開操作の対象が表示される［**Channel/User**］列が追加されました。 対象には、デバイスを登録したユーザー、共有デバイスにチェックインしたユーザー、または特定のユーザーに関連付けられていないシステムレベルの設定や展開操作が表示されます。 この情報を使用すると、特にMac OS Xなどの特定のプラットフォームで1つのデバイスを複数のユーザーが制御している場合や、このプラットフォーム上に多数のコンテナがある場合に、展開プロセスを追跡しやすくなります。

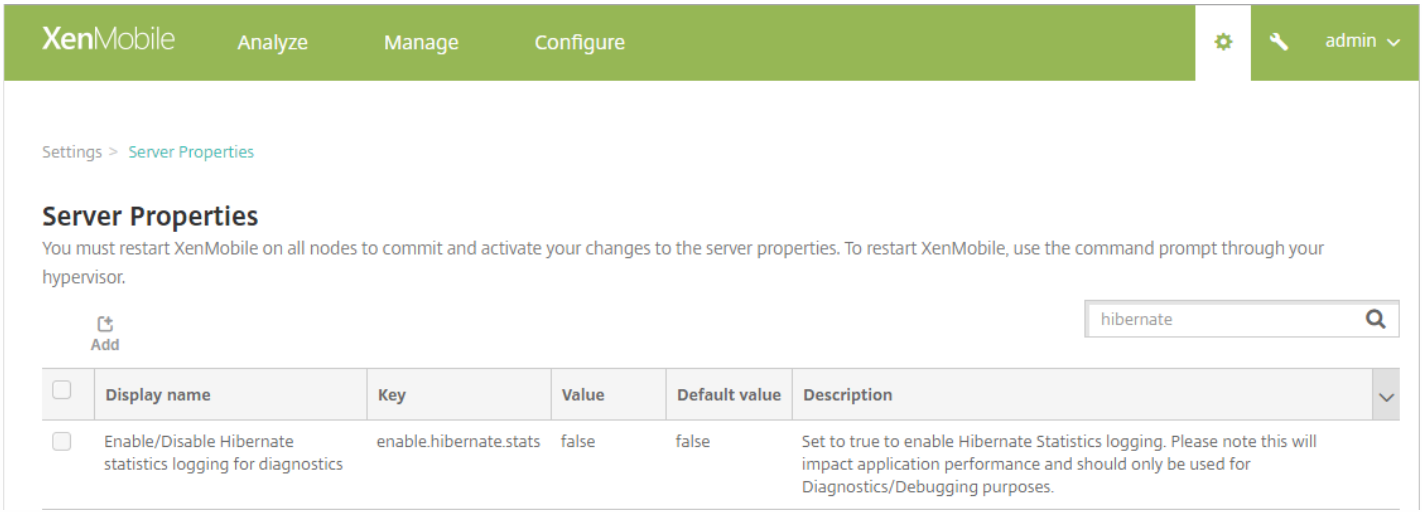


- **新しいXenMobileコンソールページ：**XenMobileコンソールには、新しいページである［**Settings**］＞［**Google Cloud Messaging**］が含まれます。このページでは、GCMの**API key**および**Sender ID**を指定できます。 これらの項目は、以前は［**Server Properties**］にのみ表示されていました。



- **Hibernateによる診断統計ログ：**アプリケーションのパフォーマンスに関する問題のトラブルシューティングを支援するために、XenMobileでは、XenMobileとMicrosoft SQL Serverとの接続に使用されるコンポーネントであるHibernateについての統計ログレポートを利用できるようになりました。

  Hibernate統計ログを有効にするには、［**Enable/Disable Hibernate statistics logging for diagnostics**］サーバープロパティ（enable.hibernate.stats）を［**true**］に変更します。 ログはアプリケーションのパフォーマンスに影響を及ぼすため、デフォルトでは無効になっています。 膨大なログファイルが作成されるのを避けるため、ログを有効にするのは短期間だけにしてください。 XenMobileは、/opt/sas/logs/hibernate_stats.logにログを書き込みます。



- **Android Appアプリストアの更新：**Androidアプリストアでは、Androidデバイスにインストールされているバージョンがアプリストアのバージョンよりも古い場合に限り、更新されたアプリのバージョンが表示されるようになりました。
- **XenMobile Analyzerツール。** XenMobile環境に問題がある場合、Citrixサポートに問い合わせると、時間と費用がかかることがあります。 XenMobile Analyzerを使用すると、サポートに問い合わせる前に、一般的な問題を自身で選別できます。 XenMobile Analyzerツールは、多数のユースケースと、MDM、MDM+MAM、およびMAM-onlyなどの展開オプション、5つの異なる認証シナリオ、iOSおよびAndroidのモバイル環境をサポートします。

  XenMobile Analyzerでは、以下のことができます。
  - お使いの環境での問題のチェックとソリューションの推奨。 XenMobile Analyzerの環境チェックは、デバイスの問題、ユーザー登録の問題、および認証の問題を識別できます。
  - 高度な診断を受けるための手順の確認。
  - WorxMail対応やサーバー接続性チェックを確認するためのツール操作。
  - 他の手段がすべて失敗すると、ツールにCitrixサポートへの直接リンクが表示されます。

  詳しくは、「XenMobile Analyzerツール」を参照してください。

- **XenMobile AutoDiscoveryサービス。** これまで、自動検出をアクティブ化するには、サポートチケットを作成する必要がありました。 AutoDiscoveryサービスポータルを使用すると、自身で自動検出を設定できます。 サービスでは、ドメインを指定して自動検出レコードを作成する手順が案内されます。 詳しくは、「XenMobile AutoDiscoveryサービス」を参照してください。

XenMobile 10.3.6の既知の問題および解決された問題

Aug 02, 2016

XenMobile 10.3.6の既知の問題および解決された問題は次のとおりです。

既知の問題

ユーザーがMicrosoftワークアカウントを使用して個人デバイスを登録しようとすると、登録に失敗します。 [#597037]

ユーザーがAzure Active DirectoryアカウントでXenMobileに登録すると、デバイスをワイプまたは失効しても、認証なしに再度登録できます。 これはサードパーティ製品の問題です。 [#628865]

XenMobileを10.3.6に更新した後、クラスタ構成で、iOSデバイス登録が失敗する場合があります。 回避策として、このKnowledge Articleを参照してください。 [#650061]

解決された問題

XenMobile管理者がXenMobileコンソールにアクセスしようとすると、代わりにXenMobile Self-Help Portalに移動することがありました。 この問題は、XenMobile管理者グループが役割ベースのアクセス制御を設定して作成されており、グループをあるActive Directory OUから別のActive Directory OUに移動した場合に起きることがあります。 [#585032]

この修正により、ユーザーがログファイルサイズとバックアップログファイルの最大数を設定した場合に、これらの値がXenMobileで正しく構成され、ファイルが適切にロールオーバーされるようになります。 ただし、既知の問題#551199で記述されているとおり、更新された値がXenMobileコンソールに反映されないことがあります。 [#597772]

統合MDMおよびMAMが含まれるXenMobileのエディションで、iOSデバイスが正しく登録されないことがありました。 デバイスは、MDMには登録されるがMAMに登録されないか、またはMAMには登録されるがMDMに登録されないことがありました。 [#610847]

WindowsのExchange ActiveSyncデバイスポリシーを構成し、展開規則で [**Only when previous deployment has failed**] オプションを設定すると、次の問題が起きることがありました：Windows PhoneユーザーがExchange Serverメールの同期時間を変更した後、次にXenMobileによってExchange ActiveSyncポリシーがWindowsデバイスにプッシュされるときに、ユーザーによる変更が上書きされます。 [#616725]

データベースに大量のデータが存在していると、XenMobile内でデバイスやユーザーを検索するときにSQL ServerのCPU使用率が急増して、検索に1分以上かかることがありました。 [#618371]

iOSデバイスのユーザーがWorx Homeに登録すると、ユーザーにWorx PINの作成を求められるまでWorx Homeが最大2分間応答しなくなることがありました。 この問題が発生した後でユーザーがWorxStoreを開くと、Worx Homeが再び応答しなくなります。 [#619945]

Windows 10が実行されているデバイスにXenMobileサーバーからSMS通知を送信できないことがありました。 [#621229]

子Active Directoryグループを1,500人を超えるメンバーが含まれる親グループに追加すると、XenMobileコンソールで実行するアクション（デリバリーグループ割り当てなど）が、追加した子グループのユーザーに適用されないことがありました。 [#622523]

ユーザーがiOSデバイスを登録した後、WorkStoreを開くかアプリを手動で追加しようとするまで、必要なアプリケーションのインストールを求められないという問題がありました。 [#622789]

XenMobile 9.0からXenMobile 10.1にアップグレードして、LDAPの［User search by］オプションをsamAccountNameに設定し、その後XenMobile 10.3.xにアップグレードすると、ユーザーがWorx Homeへの認証を行うことができなくなるという問題がありました。 [#624340]

明示的なUPNがユーザーの暗黙的なUPNと一致しない場合、ポリシーの展開およびRBACの役割の割り当てが失敗することがありました。 [#624612]

クラスター化されているサーバー展開で、Hazelcastの分散マップおよびSQLサーバーへの接続に関連する問題に起因して、XenMobileサーバーが断続的に応答不能になり、ログインできなくなり登録に失敗することがありました。 [#624931]

Androidデバイスを初めてXenMobileサーバーに接続したとき、または再接続したときに、Androidアプリのダウンロード速度が遅くなるかダウンロードが失敗するという問題がありました。 [#625199]

名前または説明にASCII文字16（データリンク拡張文字）が含まれているパブリックアプリケーションがXenMobileコンソールに追加されると、WorxHome 10.3でアプリ一覧が表示されないという問題がありました。 [#627059]

Hazelcastの分散マップが実装されている場合、クラスター化されたサーバーが断続的に応答不能になることがありました。 [#627114]

2つのサーバーインスタンスをXenMobile 10.3にアップグレードして、しばらく実行すると、最初のサーバーが応答不能になるという問題がありました。 [#628270]

iOSデバイスを正常に登録した後で、WorxStoreにログインできず「Unable to fetch the required assets to continue. Please try again.」というメッセージが表示されることがありました。この問題の原因は、XenMobileサーバーがMAMデバイスIDでデバイスを見つけられないことでした。 [#629900]

XenMobileコンソールからデバイスを削除しても、このデバイスでMAMリソースへのアクセスが引き続き許可されるという問題がありました。 [#630137]

iOSユーザーに対して選択的なワイプが行われることがありました。 [#630466]

XenMobile 10.3.xで、Worx Homeのカテゴリビューで HDXアプリが表示されないことがありました。 デフォルトでは、前のXenMobileバージョンのカテゴリビューにあるHDXアプリが含まれる「その他」フォルダーが表示されないことがありました。 [#631439]

ユーザーがデバイスを登録すると、MDM登録は成功しても、MAM登録が失敗してエラーが表示され、アプリがロックされることがありました。 [#632073]

Android SDK Version 22以降を使用してコンパイルされたか、またはDexguardで暗号化されたAndroidアプリが、XenMobileにアップロードされないという問題がありました。 [#632146]

ユーザーがWorx Homeに登録した後、断続的にWorx Homeのアンインストールと再インストールを求められるという問題がありました。 [#633095]

XenMobileコンソールで選択的なワイプ、フルワイプ、またはアカウントやデバイスの削除を実行すると、そのデバイスで構成されたアプリに対して、関連するVPPライセンスが解放されないことがありました。 [#633366]

マイナスのID（例：-123441212）を持つVPPライセンスが存在し、その場合、パブリックアプリケーションを配布できません。 [#631443]

ユーザーがデバイスを登録すると、Worx Homeがクラッシュして、アプリストアがロックされていることを示す403メッセージが表示されることがありました。 または、登録は正常に完了しても、アプリのダウンロード時に同じエラーが発生するか、「unable to fetch details」というエラーメッセージが表示されます。[#633515]

ユーザーがWindowsベースのデバイスのXenMobileコンソールで共有キーを使用してWi-Fiデバイスポリシーを構成しようとするときに、認証の種類をWPA PersonalまたはWPA-2 Personalに変更すると、共有キーオプションが正常に表示されないという問題がありました。 [#633897]

フォワードプロキシとして構成されているNetScalerがある場合、XenMobile 10.3の接続性チェックで誤った結果が返されるという問題がありました。 [#633902]

XenMobile 10.3.5へのアップグレード後、デバイスがMAMモードに登録されなくなるという問題がありました。 さらに、MDM+MAMモードで登録されているデバイスに対するポリシーとアプリの展開が失敗することがありました。 [#634034]

統合されたMDMとMAMが含まれるXenMobileのエディションで、LDAP設定の［user］検索フィールドがsamAccountNameに設定されていると、認証済みのDEPデバイスに対してMAM認証が失敗することがありました。 その結果、Worx Home登録が完了せず、デバイスがMDM-onlyモードで登録されていました。 [#637599]

XenMobileのスケーラビリティとパフォーマンス

Oct 25, 2016

XenMobileインフラストラクチャの規模を理解することはXenMobileを展開し構成する方法を決定するうえで重要な役割を果たします。 このトピックでは、小規模から大規模のエンタープライズ展開の要件を判断するうえでよくある質問に対する回答を提供します。

パフォーマンスとスケーラビリティのガイドライン

このトピックのデータは、XenMobile 10.3.6インフラストラクチャのパフォーマンスとスケーラビリティを判断するためのガイドラインとして使用することを想定しています。 サーバーとデータベースのスケーラビリティを構成する方法を判断するための2つの重要な要素は、スケーラビリティ（最大ユーザー数/デバイス数）とログオン数です。

- スケーラビリティは定義済みのワークロードを実行する同時ユーザーの最大数として定義されます。 XenMobileインフラストラクチャをロードするために使用されるフローについて詳しくは、「ワークロード」を参照してください。
- ログオン数は新規ユーザーのオンボーディングと既存ユーザーの認証の数として定義されます。
  - オンボーディング数は環境に初めて登録できる最大デバイス数です。 このトピックでは初回使用またはFTUと呼ばれます。このデータポイントはロールアウト戦略を調整するうえで重要です。
  - 既存ユーザー数は環境に対して認証される最大ユーザー数です。このユーザーは既に登録済みで自分のデバイスで接続したことがあります。 以下のテストには、登録済みユーザーに対するセッションの作成およびWorxMailとWorxWebアプリの実行が含まれます。

以下の表に、対応するXenMobile環境のテスト結果に基づくスケーラビリティのガイドラインを示します。

スケーラビリティ	最大45,000デバイス	
ログオン数	オンボーディング（FTU）	毎時最大833デバイス
	既存ユーザー	毎時最大2,812デバイス
構成	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	6ノードで構成されるXenMobileサーバークラスター
	データベース	Microsoft SQL Server外部データベース

Important

このレポートを自動化するには、デバイス数が1,000～60,000である必要があります。 デバイス数が60,000を超える場合の要件については、このレポートの範囲外です。

プロファイル設定のテスト

このセクションでは、Active Directoryの構成、XenMobileポリシーの数、アプリケーションの数や種類、ユーザーアクションのシミュレーション、および各ハードウェア構成に対して使用されるテストプロファイルと、この記事でテスト結果を導き出すために使用されるワークロードの、管理者アクションのシミュレーションについて説明します。

注意

このテストプロファイルは、XenMobileの以前のバージョンでスケーラビリティをテストするために使用されたプロファイルより多くのリソースを使用するように設計されています。 このため、これらのテスト結果は、以前のバージョンのスケーラビリティの結果と直接的には比較できません。

Active Directory（AD）構成：

- 100,000人の一意のADユーザー
- 200,000の一意のADグループ
- ADグループに対しては5階層レベル
- ADグループあたり200ユーザー

デリバリーグループ：
- 20のデリバリーグループ
- デリバリーグループに50のアプリケーションを割り当て
- デリバリーグループあたり10のADグループ

XenMobileデバイスポリシー：
- 300のデバイスポリシー
- ユーザーごとに20のデバイスポリシー

アプリケーション：
- 1つの公開ストアから200のネイティブアプリケーション
- 50のネイティブのエンタープライズ配布アプリケーション
- 100のWebおよびSoftware as a Service（SaaS）アプリケーション
- ユーザーあたり50のアプリケーション

XenMobileユーザーのアクション：
- 50の合計構成済みアクション
- Worx Storeは次のものを起動します：
  - 新規ユーザー（FTU）：4

    - 既存ユーザー（RU）：1
- アプリケーションは次のものを起動します：
    - MDX：1
    - Web/SaaS：1
- ユーザーあたり150のSTA検証

XenMobile管理者操作：
- デバイスの列挙（ヘルプデスク電話シナリオのシミュレーション）：8時間あたり32の操作（15～20分ごとに1つ）。
- レポートの生成：8時間あたり2回。

システム構成およびテスト結果

このセクションでは、使用したハードウェア構成と、オンボーディング（FTU）ワークロードおよび既存ユーザーワークロードのスケーラビリティテストの実行結果について説明します。

以下の表は、1,000-60,000デバイスのXenMobile環境に推奨されるハードウェアおよび構成を示します。 これらのガイドラインはテスト結果および関連するワークロードに基づいています。 推奨事は、「終了基準」に定義する許容可能なエラー発生の余地を考慮に入れたものです。

テスト結果の解析により、以下の結論が導かれました。

- ログオン数はシステムのスケーラビリティを判断するうえで重要な要素です。 初回ログオンに加えて、ログオン数は環境に構成されている認証タイムアウト値に左右されます。 たとえば、認証イムアウト値が低すぎると、ユーザーはより頻繁にログオン要求を実行する必要があります。 したがって、タイムアウト値が環境に与える影響を明確に理解する必要があります。
- NetScalerでのユーザーセッションあたりの接続数は重要な検討項目です。
- 最大のスケーラビリティを得るため、XenMobileにCPUおよびRAMのリソースを追加しました。
- 検証された最大の構成は6ノードのクラスター構成です。 6ノードを超える規模拡大にはXenMobileを追加で導入する必要があります。

次の表に、XenMobile構成、NetScaler Gatewayアプライアンス、クラスター設定、およびデータベースに基づく、推奨されるオンボーディングおよび既存ユーザーのログオン数を示します。 この表のデータを使用して、新しい展開、および既存の展開に対する既存ユーザー/デバイス数に最適な登録スケジュールを立てます。 構成のセクションは、登録とログオンのパフォーマンスデータと、推奨される適切なハードウェアの関係を示します。

予想されるデバイス数	1,000	10,000	30,000	45,000
実際のデバイス数	1,000	9,998	29,977	44,991
ログオン数				
オンボーディング（FTU)	250	625	833	833
既存ユーザー数（Worxのみ）	1,000	1,666	3,750	883
構成				
参照環境	VPX-XenMobileスタンドアロン	MPX-XenMobileスタンドアロン	MPX-XenMobileクラスター（3）	MPX-XenMobileクラスター（6）
NetScaler Gateway	2GBのRAMを搭載したVPX 2つの仮想CPU	MPX-10500	MPX-11500	MPX-11500
XenMobile - モード	スタンドアロン*	スタンドアロン*	クラスター	クラスター
XenMobile - クラスター	-	-	3	6
XenMobile - 仮想アプライアンス	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび6つの仮想CPU	16GBのRAMおよび8つの仮想CPU
Active Directory（AD)	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU	16GBのRMおよび4つの仮想CPU
データベース	外部	外部 - Microsoft SQL Server メモリ = 16GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 32GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 48GB 仮想CPU = 16

MPX-XenMobileクラスター（3）

クラスター

クラスター

クラスター

クラスター

8GBのRAMおよび4つの仮想CPU

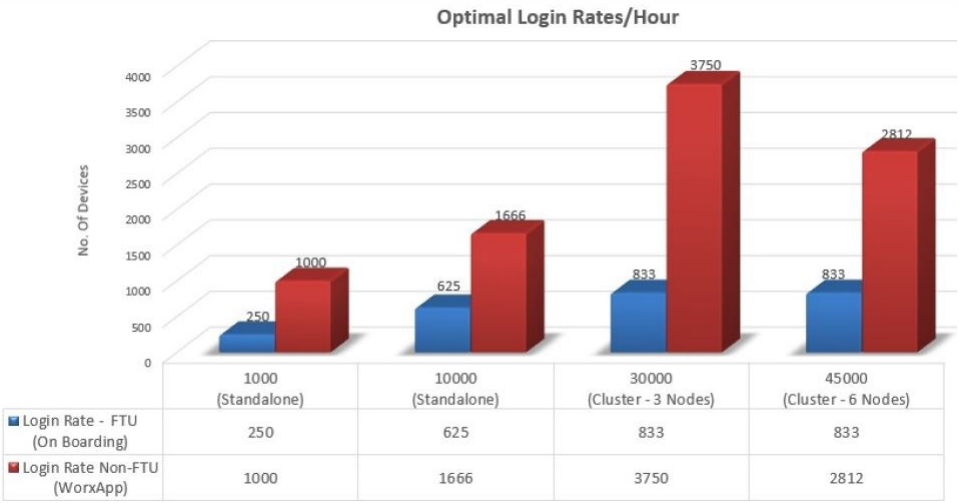
8GBのRAMおよび4つの仮想CPU

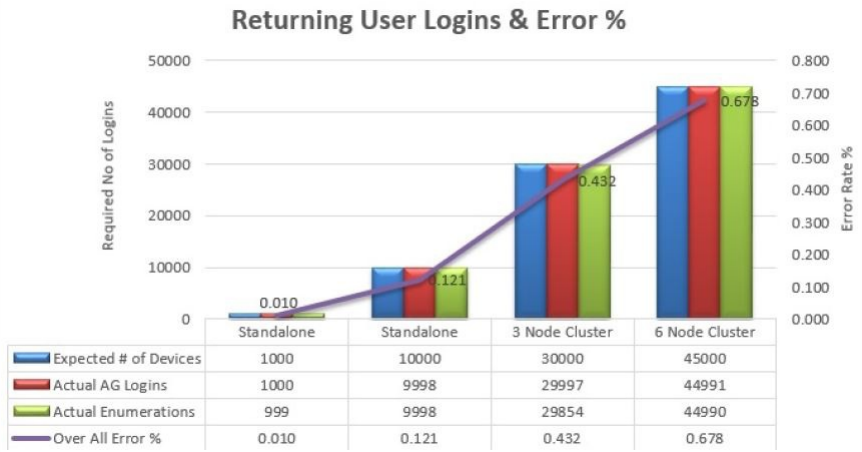
* スタンドアロン展開は、ユーザーに対する可用性が高くなければならないアプリケーションにはお勧めできません。 大部分のお客様には、高可用性のクラスタ展開をお勧めします。

注：システム規模に対して推奨される数を超過する登録やログオンがあったりハードウェアの性能が不足していたりすると、以下の事象が発生します。

次の情報は記録された追加のデータポイントを提供します。これらのデータポイントは前の表の結果に
影響を及ぼします。

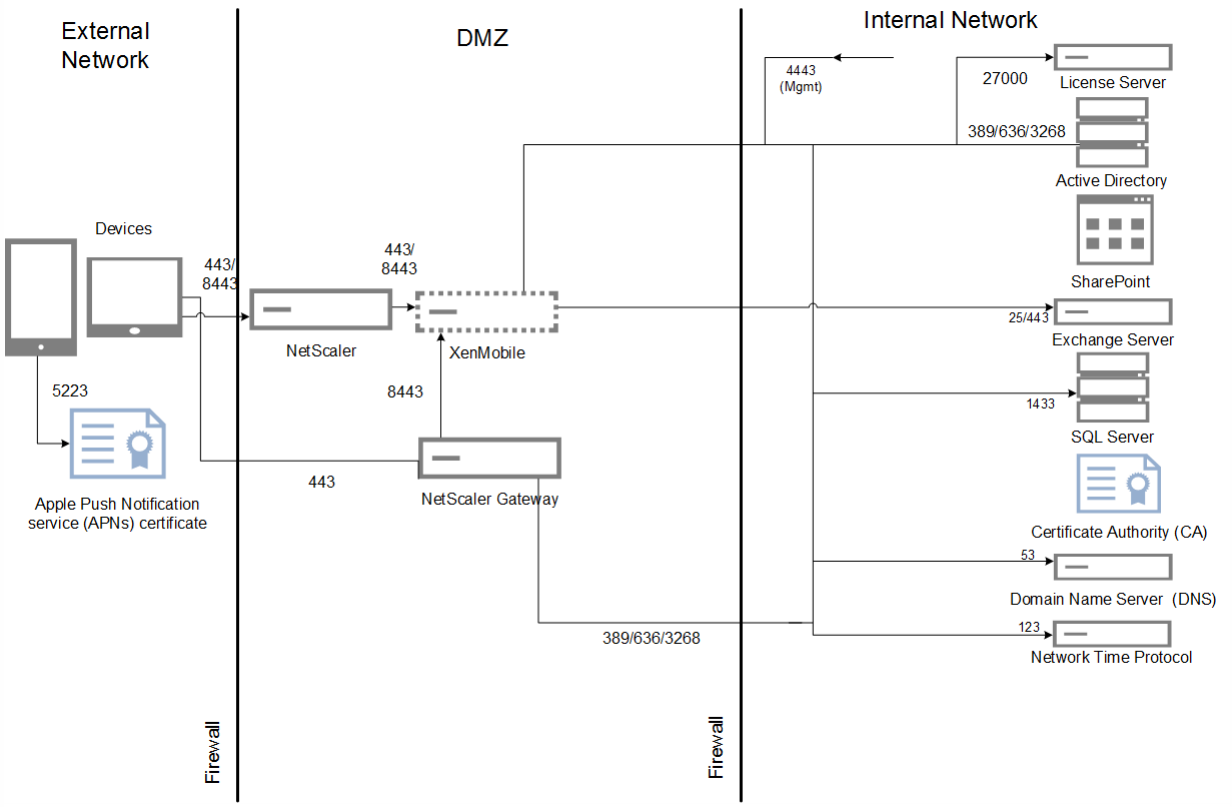
- 登録またはログオンの遅延（ラウンドトリップ時間）
  - 平均遅延時間の合計：0.5～1.5秒
  - NetScaler Gatewayログオンの平均遅延時間：120～440ミリ秒
  - WorxStore要求の平均遅延時間：2～3秒
- スケーラビリティの制限に達すると、インフラストラクチャコンポーネントにCPUおよびメモリの消費のような物理的なパフォーマンスの低下が見られます。
  - NetScaler GatewayおよびXenMobileアプライアンス上での無効な応答
  - 高負荷状態でのXenMobileコンソールの応答時間の遅延



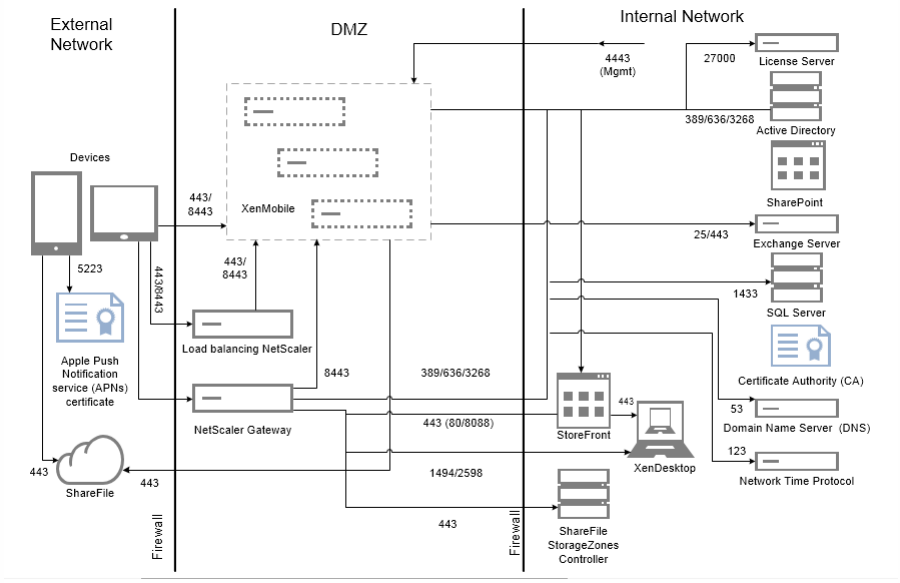


上の図のエラー率には各操作に対応する要求に対して発生する全体的なエラーが含まれており、ログオンに限定したものではありません。 終了基準」に定義するとおり、エラー率は各実行テストの1%という許容可能な範囲に収まっています。

次の図は、小規模な展開のリファレンスアーキテクチャを示しています。 これはスタンドアロンアーキテクチャで、10,000デバイスまでをサポートします。



次の図は、エンタープライズ展開のリファレンスアーキテクチャを示しています。 これはクラスターアーキテクチャで、HTTP経由のMAMに対するSSLオフロードが有効です。10,000デバイス以上サポートします。



テスト方法

ベンチマークを確立するため、XenMobile Enterpriseに対してテストを実行しました。 小規模および大規模な展開の両方を対象とし、測定には1,000～60,000デバイスを使用しました。

実世界のユースケースをシミュレートするためワークロードを作成しました。 これらのワークロードを各テストで実行し、登録およびログオン数への影響を調査しました。 テストの目標は、終了基準」に定義する許容可能なエラー発生の余地に収まる最適なログオン数を得ることでした。 ログオン数は、インフラストラクチャコンポーネントのハードウェア構成に対する推奨事項を判断するうえで重要な要素です。

オンボーディング（FTU）ワークロードのログオン要求には、自動検出、認証、およびデバイス登録の操作が含まれました。 アプリケーションのサブスクリプション、インストール、および起動操作は、テスト期間を通じて均等に分散されました。 これにより、実世界のユーザー行動のシミュレーションが提供されました。 テストの最後にセッションはログアウトされました。 既存ユーザーワークロードのログオン要求には、認証要求のみが含まれました。

ワークロード

ユーザーワークロードは以下のように定義されます。

ユーザーセッション/デバイス	各セッションのNetScaler Gatewayログオン、列挙、デバイス登録などが含まれます。
Worx Storeの起動	ユーザーがWorx Storeを複数回起動し、そのたびに、モバイルアプリ（Web/SaaS/MDX）かWindowsアプリ（HDX）かを問わず、複数のアプリをサブスクライブつまりインストールします。
デバイスあたりのWeb/SaaSアプリのSSO	XenMobileでSSOが完了して実際のアプリのURLを返すまでの、Web/SaaSアプリの起動シーケンスです。 実際のアプリにトラフィックは送信されませんでした。
デバイスあたりのMDXアプリのダウンロード	MDXアプリのダウンロード数です（これはWorx Storeの起動中いつでも発生する可能性があります）。 iOSの場合、Apple ITMSからのアプリの自動インストールが含まれます。これにより、NetScaler Gateway上で新しいトークン/tmsサービスAPIが活用されます。

注記と前提

以下のシナリオはスケーラビリティテストの対象外となります。 これらのシナリオは、今後のスケールテストの機能拡張で検討されます。

- パッケージの展開がテストされません。
- Windowsプラットフォームがテストされません。

ポリシーのプッシュは、iOSおよびAndroidデバイスでテストされています。
各XenMobileは最大10,000の接続を同時にサポートします。

テストは、ネットワーク遅延の問題を無視できるように、理想的なLANの条件で行われています。 実際のシナリオでは、特にアプリケーションのダウンロードに関して、スケーラビリティは利用可能なユーザーの帯域幅によっても大きく変わります。

再接続テスト

再接続テストは初回使用テストと既存ユーザーシナリオテストで個別に行われています。

再接続テストが最大15,000のデバイスに対して実行されました。

Androidでサポートされている再接続率は1秒あたり17デバイスです。 iOSの再接続率は1秒あたり8デバイスです。 これを実現するために、/opt/sas/tomcat/conf/server.xmlファイルのmaxThreadカウントは1000に設定しました。

要追加：推奨デバイス再接続ポリシーに関する情報

オンボーディング（FTU)ワークロード
オンボーディング（FTU）ワークロードは、XenMobile環境へのユーザーによる初めてのアクセスと定義されます。 このワークロードに含まれる操作は以下のとおりでした。

- 自動検出
- Enrollment
- Authentication
- デバイス登録
- アプリケーションの検出（Web、SaaS、およびモバイルMDXアプリ）
  - アプリケーションのサブスクリプション（画像とアイコンのダウンロードを含む）
  - サブスクライブされたMDXアプリのインストール
- デバイスの状態の確認を含むアプリケーションの起動（Web、SaaS、およびモバイルMDXアプリ）
- ポリシーのプッシュ（iOS）
- 最小限のWorxMailおよびWorxWeb接続（VPNトンネル） — 2接続
- XenMobile経由の必須アプリのインストール

次の表は、ワークロードのパラメーターの定義です。

Devices	デバイス登録	列挙	デバイスあたりのアプリの列挙	デバイスあたりのWorxStoreの起動	デバイスあたりのWeb/SaaSのSSO	デバイスあたりのMDXアプリのダウンロード	XenMobileサーバーによってトリガーされる必須アプリのダウンロード	デバイスあたりのプッシュされるポリシー（iOS）
1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Worxへの接続のみを使用する既存ユーザーのワークロード

次の表は、既存ユーザー（Worxへの接続のみを使用）のワークロードです。 このワークロードにより、WorxMailおよびWorxWebアプリを使用する1人のユーザーがシミュレートされました。 このミュレーションを使用して、XenMobile構成内のNetScaler Gatewayのスケーラビリティを測定しました。 この測定が可能になるのは、これら2つのWorxアプリのみを使用することでネットワークの負荷が最小限になるからです。 WorxWebアプリについては、ユーザーは内部Webサイトにアクセスしています。この場合XenMobileサーバーのSSOはトリガーされません。 このモードで含まれ操作は以下のとおりです。

- 認証（NetScaler GatewayとXenMobile）
- WorxMailおよびWorxWeb接続（VPNトンネル） — 4接続

以下の表は既存ユーザーのワークロードパラメーターを示します。

Devices	列挙	デバイスあたりのアプリの列挙	デバイスあたりのVPNトンネル[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. VPNトンネルの数は、WorxMailおよびWorxWebの接続の数に対応します。

次の表は、WorxMailおよびWorxWebの接続プロファイルの概要です。

デバイス接続	接続の種類	セッションあたりの送信データ[1]	セッションあたりの受信データ[1]
WorxMail接続 #1	タイプ1[2]	4.1MB	4.1MB
WorxMail接続 #2	タイプ1	6.3MB	12.5MB
WorxWeb接続 #1	タイプ2[3]	5.2MB	15.7MB
WorxWeb接続 #2	タイプ2	4.1MB	3.4MB
セッションあたりの転送バイト合計[1]		～19.7MB	～40.7MB

1.セッションあたり：8時間

タイプ1：長時間の非対称な送信および受信接続（Microsoft Exchangeのメールボックスに対するWorxMailの接続）。

タイプ2：閉じてしばらく待った後で再び開く、非対称な送信および受信接続（WorxWeb接続）

これらの推奨事項は、「中程度」のワークロードを自動化するためのWorxMailおよびWorxWebのプロファイルに基づいて
設定されています。 接続の詳細を変更すると解析結果に影響があります。 たとえば、ユーザーあたりの接続数を増やす場合、サポートされるNetScaler Gatewayセッションの数は減少する可能性があります。

WorxMailおよびWorxWebのプロファイル

各アプリで使用するプロファイルは、「非常に高負荷の」ワークロードを自動化することを目的としています。次の表は、WorxMailおよびWorxWebのプロファイルの詳細です。

中程度のワークロードのWorxMailプロファイル

1日あたりの送信メッセージ	20
1日あたりの受信メッセージ	80
1日あたりの読み取りメッセージ	80
1日あたりの削除メッセージ	20
平均メッセージサイズ（KB）	200

中程度のワークロードのWorxWebプロファイル

起動Webアプリ数	10
手動で開くWebページ数	10
Webアプリあたりの平均要求-応答ペア数	100
要求の平均サイズ（バイト）	300
応答の平均サイズ（バイト）	1000

構成とパラメーター

以下の構成を使用してスケーラビリティテストを実行しました。

- NetScaler Gatewayおよび負荷分散（LB）仮想サーバーを同じNetScaler Gatewayアプライアンスに共存させました。
- NetScalerのセッションタイムアウトを60分に設定しました。
- SSLトランザクションにNetScaler Gateway上の2048ビットキーを使用しました。

終了基準

この解析の基礎はログオン数です。 ログオン数によって、インフラストラクチャコンポーネントおよびコンポーネントそれぞれの構成のガイドラインが提供されます。 ログオン数は、以下のようなエラー発生の余地を考慮に入れたものであることに留意してください。

- 無効な応答
  - ステータスコードが200ではなく401/404の応答は無効とみなされます。
- 要求のタイムアウト
  - 120秒以内に応答があることが期待されます。
- 接続エラー
  - 接続がリセットされます。
  - 接続が突然終了されます。

全体的なエラー率が任意のデバイスから送信される要求数の合計の1%未満であれば、ログオン数は許容可能です。 エラーには、各個別のワークロード操作に対応するエラーはもちろん、CPUやメモリの消費のようなインフラストラクチャコンポーネントの物理的なパフォーマンスにかかわるものも含まれます。

ソフトウェアおよびハードウェアの詳細

以下の表は、これらのテストに使用されたXenMobileインフラストラクチャのソフトウェアを示します。

コンポーネント	バージョン
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n

XenMobile	10.3.0.824
外部データベース	Microsoft SQL Server 2014

以下のテーブルに示すXenServerプラットフォーム上で、スケーラビリティテストを実行しました。

ベンダー	Genuine Intel
Model	Intel Xeon CPU — E5645 @ 2.40GHz（CPU数24）

これにはインフラストラクチャの中核的なサービス（Active Directory、Windowsドメインネームサービス（DNS）、証明機関、Microsoft Exchangeなど）とXenMobileコンポーネント（XenMobile仮想アプライアンスおよび該当する場合はNetScaler Gateway VPX仮想アプライアンス）が含まれます。

XenMobileのスケーラビリティとパフォーマンス

Aug 02, 2016

XenMobileインフラストラクチャの規模を理解することはXenMobileを展開し構成する方法を決定するうえで重要な役割を果たします。 このトピックでは、小規模から大規模のエンタープライズ展開の要件を判断するうえでよくある質問に対する回答を提供します。

パフォーマンスとスケーラビリティのガイドライン

このトピックのデータは、XenMobile 10.3.6インフラストラクチャのパフォーマンスとスケーラビリティを判断するためのガイドラインとして使用することを想定しています。 サーバーとデータベースのスケーラビリティを構成する方法を判断するための2つの重要な要素は、スケーラビリティ（最大ユーザー数/デバイス数）とログオン数です。

- スケーラビリティは定義済みのワークロードを実行する同時ユーザーの最大数として定義されます。 XenMobileインフラストラクチャをロードするために使用されるフローについて詳しくは、「ワークロード」を参照してください。
- ログオン数は新規ユーザーのオンボーディングと既存ユーザーの認証の数として定義されます。
  - オンボーディング数は環境に初めて登録できる最大デバイス数です。 このトピックでは初回使用またはFTUと呼ばれます。このデータポイントはロールアウト戦略を調整するうえで重要です。
  - 既存ユーザー数は環境に対して認証される最大ユーザー数です。このユーザーは既に登録済みで自分のデバイスで接続したことがあります。 以下のテストには、登録済みユーザーに対するセッションの作成およびWorxMailとWorxWebアプリの実行が含まれます。

以下の表に、対応するXenMobile環境のテスト結果に基づくスケーラビリティのガイドラインを示します。

スケーラビリティ	最大45,000デバイス	
ログオン数	オンボーディング（FTU）	毎時最大833デバイス
	既存ユーザー	毎時最大2,812デバイス
構成	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	6ノードで構成されるXenMobileサーバークラスター
	データベース	Microsoft SQL Server外部データベース

Important

このレポートを自動化するには、デバイス数が1,000～60,000である必要があります。 デバイス数が60,000を超える場合の要件については、このレポートの範囲外です。

プロファイル設定のテスト

このセクションでは、Active Directoryの構成、XenMobileポリシーの数、アプリケーションの数や種類、ユーザーアクションのシミュレーション、および各ハードウェア構成に対して使用されるテストプロファイルと、この記事でテスト結果を導き出すために使用されるワークロードの、管理者アクションのシミュレーションについて説明します。

注意

このテストプロファイルは、XenMobileの以前のバージョンでスケーラビリティをテストするために使用されたプロファイルより多くのリソースを使用するように設計されています。 このため、これらのテスト結果は、以前のバージョンのスケーラビリティの結果と直接的には比較できません。

Active Directory（AD）構成：

- 100,000人の一意のADユーザー
- 200,000の一意のADグループ
- ADグループに対しては5階層レベル
- ADグループあたり200ユーザー

デリバリーグループ：
- 20のデリバリーグループ
- デリバリーグループに50のアプリケーションを割り当て
- デリバリーグループあたり10のADグループ

XenMobileデバイスポリシー：
- 300のデバイスポリシー
- ユーザーごとに20のデバイスポリシー

アプリケーション：
- 1つの公開ストアから200のネイティブアプリケーション
- 50のネイティブのエンタープライズ配布アプリケーション
- 100のWebおよびSoftware as a Service（SaaS）アプリケーション
- ユーザーあたり50のアプリケーション

XenMobileユーザーのアクション：
- 50の合計構成済みアクション
- Worx Storeは次のものを起動します：
  - 新規ユーザー（FTU）：4

- 既存ユーザー（RU）：1
- アプリケーションは次のものを起動します：
  - MDX：1
  - Web/SaaS：1
- ユーザーあたり150のSTA検証

XenMobile管理者操作：
- デバイスの列挙（ヘルプデスク電話シナリオのシミュレーション）：8時間あたり32の操作（15～20分ごとに1つ）。
- レポートの生成：8時間あたり2回。

システム構成およびテスト結果

このセクションでは、使用したハードウェア構成と、オンボーディング（FTU）ワークロードおよび既存ユーザーワークロードのスケーラビリティテストの実行結果について説明します。

以下の表は、1,000-60,000デバイスのXenMobile環境に推奨されるハードウェアおよび構成を示します。 これらのガイドラインはテスト結果および関連するワークロードに基づいています。 推奨事は、「終了基準」に定義する許容可能なエラー発生の余地を考慮に入れたものです。

テスト結果の解析により、以下の結論が導かれました。

- ログオン数はシステムのスケーラビリティを判断するうえで重要な要素です。 初回ログオンに加えて、ログオン数は環境に構成されている認証タイムアウト値に左右されます。 たとえば、認証イムアウト値が低すぎると、ユーザーはより頻繁にログオン要求を実行する必要があります。 したがって、タイムアウト値が環境に与える影響を明確に理解する必要があります。
- NetScalerでのユーザーセッションあたりの接続数は重要な検討項目です。
- 最大のスケーラビリティを得るため、XenMobileにCPUおよびRAMのリソースを追加しました。
- 検証された最大の構成は6ノードのクラスター構成です。 6ノードを超える規模拡大にはXenMobileを追加で導入する必要があります。

次の表は、XenMobile構成、NetScaler Gatewayアプライアンス、クラスタ設定、およびデータベースに基づく、推奨されるオンボーディングおよび既存ユーザーのログオン数を示しています。 この表のデータを使用して、新しい展開、および既存の展開に対する既存ユーザー/デバイス数に最適な登録スケジュールを立てます。 構成のセクションは、登録とログオンのパフォーマンスデータと、推奨される適切なハードウェアの関係を示します。

予想されるデバイス数	1,000	10,000	30,000	45,000
実際のデバイス数	1,000	9,998	29,977	44,991
ログオン数				
オンボーディング（FTU）	250	625	833	833
既存ユーザー数（Worxのみ）	1,000	1,666	3,750	883
構成				
参照環境	VPX-XenMobileスタンドアロン	MPX-XenMobileスタンドアロン	MPX-XenMobileクラスター（3）	MPX-XenMobileクラスター（6）
NetScaler Gateway	2GBのRAMを搭載したVPX 2つの仮想CPU	MPX-10500	MPX-11500	MPX-11500
XenMobile - モード	スタンドアロン*	スタンドアロン*	クラスター	クラスター
XenMobile - クラスター	-	-	3	6
XenMobile - 仮想アプライアンス	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび6つの仮想CPU	16GBのRAMおよび8つの仮想CPU
Active Directory（AD）	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU	16GBのRMおよび4つの仮想CPU
データベース	外部	外部 - Microsoft SQL Server メモリ = 16GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 32GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 48GB 仮想CPU = 16

MPX-XenMobileクラスター（3）

クラスター

クラスター

クラスター

クラスター

8GBのRAMおよび4つの仮想CPU

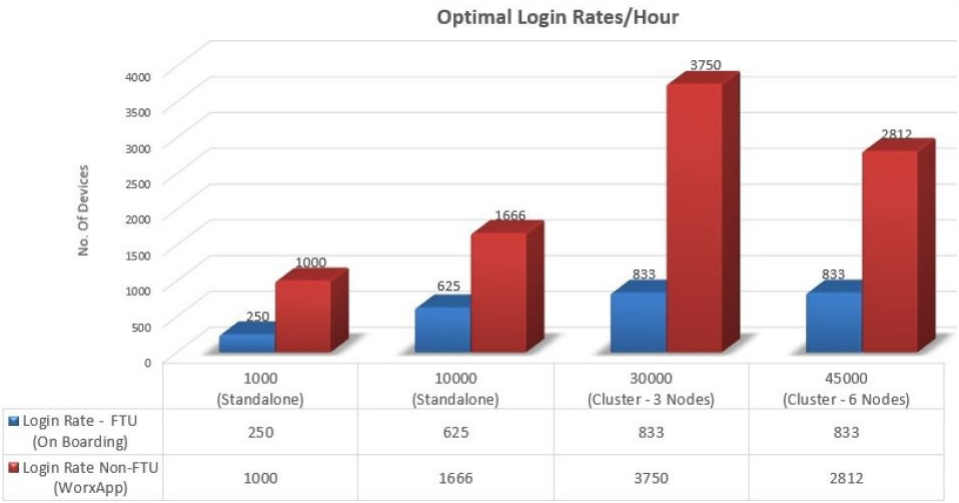
8GBのRAMおよび4つの仮想CPU

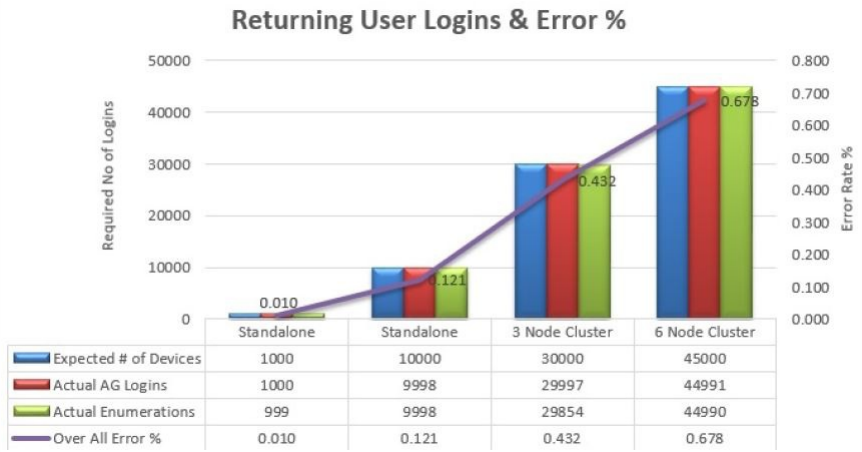
* スタンドアロン展開は、ユーザーに対する可用性が高くなければならないアプリケーションにはお勧めできません。 大部分のお客様には、高可用性のクラスタ展開をお勧めします。

注：システム規模に対して推奨される数を超過する登録やログオンがあったりハードウェアの性能が不足していたりすると、以下の事象が発生します。

次の情報は記録された追加のデータポイントを提供します。これらのデータポイントは前の表の結果に
影響を及ぼします。

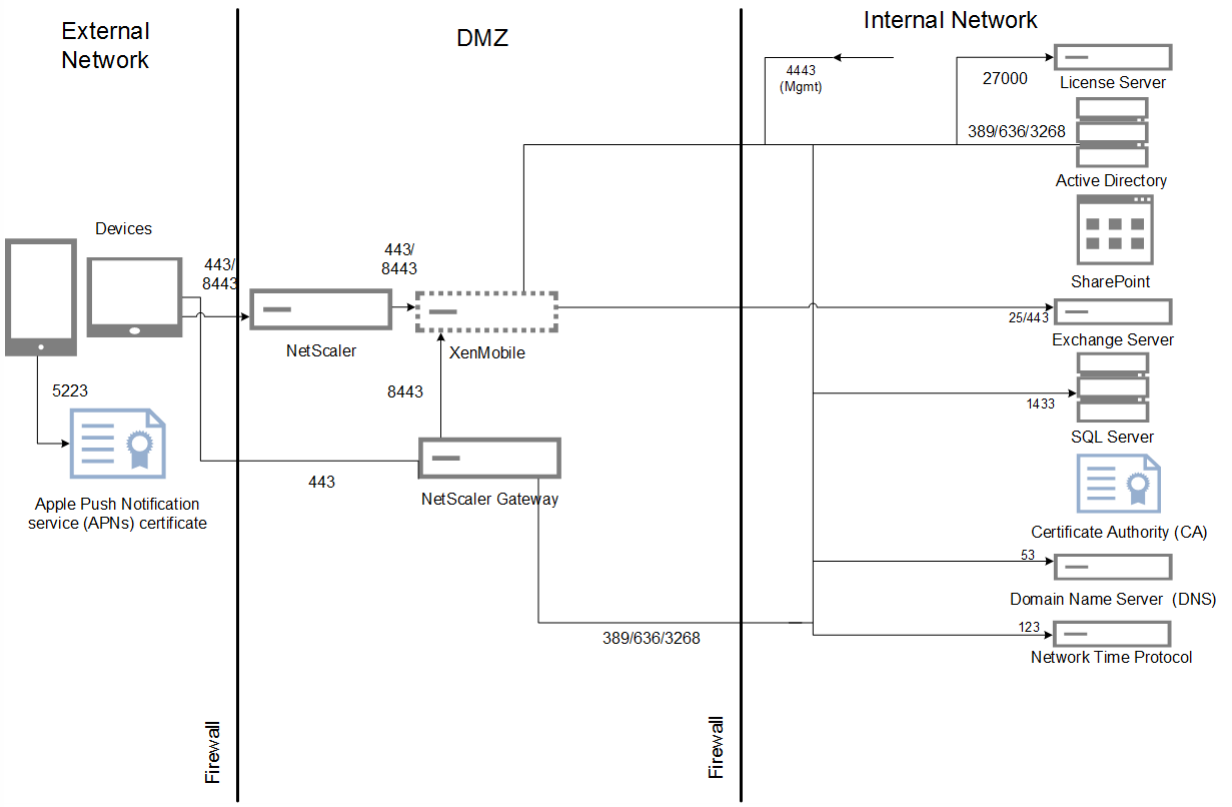
- 登録またはログオンの遅延（ラウンドトリップ時間）
  - 平均遅延時間の合計：0.5～1.5秒
  - NetScaler Gatewayログオンの平均遅延時間：120～440ミリ秒
  - WorxStore要求の平均遅延時間：2～3秒
- スケーラビリティの制限に達すると、インフラストラクチャコンポーネントにCPUおよびメモリの消費のような物理的なパフォーマンスの低下が見られます。
  - NetScaler GatewayおよびXenMobileアプライアンス上での無効な応答
  - 高負荷状態でのXenMobileコンソールの応答時間の遅延



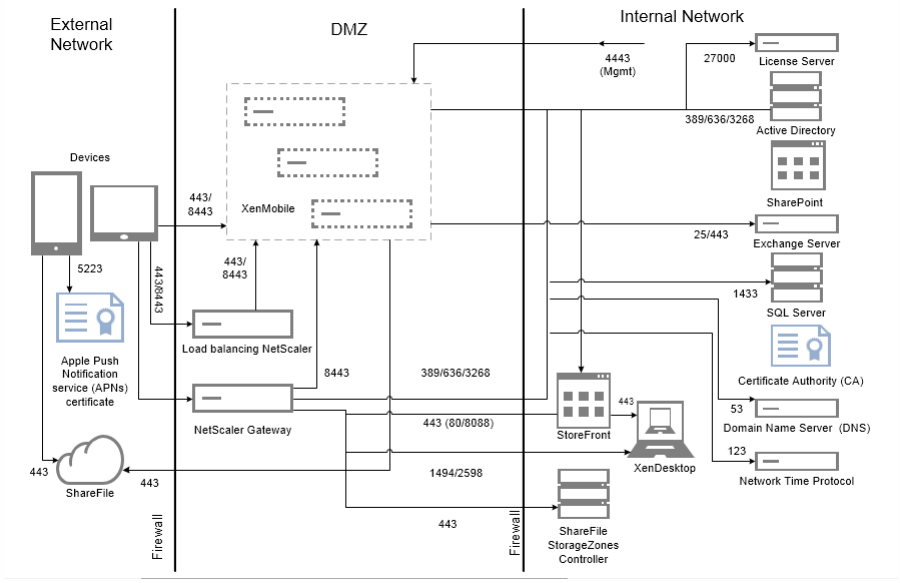


上の図のエラー率には各操作に対応する要求に対して発生する全体的なエラーが含まれており、ログオンに限定したものではありません。 終了基準」に定義するとおり、エラー率は各実行テストの1%という許容可能な範囲に収まっています。

次の図は、小規模な展開のリファレンスアーキテクチャを示しています。 これはスタンドアロンアーキテクチャで、10,000デバイスまでをサポートします。



次の図は、エンタープライズ展開のリファレンスアーキテクチャを示しています。 これはクラスターアーキテクチャで、HTTP経由のMAMに対するSSLオフロードが有効です。10,000デバイス以上サポートします。



テスト方法

ベンチマークを確立するため、XenMobile Enterpriseに対してテストを実行しました。 小規模および大規模な展開の両方を対象とし、測定には1,000～60,000デバイスを使用しました。

実世界のユースケースをシミュレートするためワークロードを作成しました。 これらのワークロードを各テストで実行し、登録およびログオン数への影響を調査しました。 テストの目標は、終了基準」に定義する許容可能なエラー発生の余地に収まる最適なログオン数を得ることでした。 ログオン数は、インフラストラクチャコンポーネントのハードウェア構成に対する推奨事項を判断するうえで重要な要素です。

オンボーディング（FTU）ワークロードのログオン要求には、自動検出、認証、およびデバイス登録の操作が含まれました。 アプリケーションのサブスクリプション、インストール、および起動操作は、テスト期間を通じて均等に分散されました。 これにより、実世界のユーザー行動のシミュレーションが提供されました。 テストの最後にセッションはログアウトされました。 既存ユーザーワークロードのログオン要求には、認証要求のみが含まれました。

ワークロード

ユーザーワークロードは以下のように定義されます。

ユーザーセッション/デバイス	各セッションのNetScaler Gatewayログオン、列挙、デバイス登録などが含まれます。
Worx Storeの起動	ユーザーがWorx Storeを複数回起動し、そのたびに、モバイルアプリ（Web/SaaS/MDX）かWindowsアプリ（HDX）かを問わず、複数のアプリをサブスクライブつまりインストールします。
デバイスあたりのWeb/SaaSアプリのSSO	XenMobileでSSOが完了して実際のアプリのURLを返すまでの、Web/SaaSアプリの起動シーケンスです。 実際のアプリにトラフィックは送信されませんでした。
デバイスあたりのMDXアプリのダウンロード	MDXアプリのダウンロード数です（これはWorx Storeの起動中いつでも発生する可能性があります）。 iOSの場合、Apple ITMSからのアプリの自動インストールが含まれます。これにより、NetScaler Gateway上で新しいトークン/tmsサービスAPIが活用されます。

注記と前提

以下のシナリオはスケーラビリティテストの対象外となります。 これらのシナリオは、今後のスケールテストの機能拡張で検討されます。

- パッケージの展開がテストされません。
- Windowsプラットフォームがテストされません。

ポリシーのプッシュは、iOSおよびAndroidデバイスでテストされています。
各XenMobileは最大10,000の接続を同時にサポートします。

テストは、ネットワーク遅延の問題を無視できるように、理想的なLANの条件で行われています。 実際のシナリオでは、特にアプリケーションのダウンロードに関して、スケーラビリティは利用可能なユーザーの帯域幅によっても大きく変わります。

再接続テスト

再接続テストは初回使用テストと既存ユーザーシナリオテストで個別に行われています。

再接続テストが最大15,000のデバイスに対して実行されました。

Androidでサポートされている再接続率は1秒あたり17デバイスです。 iOSの再接続率は1秒あたり8デバイスです。 これを実現するために、/opt/sas/tomcat/conf/server.xmlファイルのmaxThreadカウントは1000に設定しました。

要追加：推奨デバイス再接続ポリシーに関する情報

オンボーディング（FTU)ワークロード
オンボーディング（FTU）ワークロードは、XenMobile環境へのユーザーによる初めてのアクセスと定義されます。 このワークロードに含まれる操作は以下のとおりでした。

- 自動検出
- Enrollment
- Authentication
- デバイス登録
- アプリケーションの検出（Web、SaaS、およびモバイルMDXアプリ）
  - アプリケーションのサブスクリプション（画像とアイコンのダウンロードを含む）
  - サブスクライブされたMDXアプリのインストール
- デバイスの状態の確認を含むアプリケーションの起動（Web、SaaS、およびモバイルMDXアプリ）
- ポリシーのプッシュ（iOS）
- 最小限のWorxMailおよびWorxWeb接続（VPNトンネル） — 2接続
- XenMobile経由の必須アプリのインストール

次の表は、ワークロードのパラメーターの定義です。

Devices	デバイス登録	列挙	デバイスあたりのアプリの列挙	デバイスあたりのWorxStoreの起動	デバイスあたりのWeb/SaaSのSSO	デバイスあたりのMDXアプリのダウンロード	XenMobileサーバーによってトリガーされる必須アプリのダウンロード	デバイスあたりのプッシュされるポリシー（iOS）
1000	1000	1000	50	4	40	10	2	20
10000	10000	10000	50	4	40	10	2	20
30000	30000	30000	50	4	40	10	2	20
60000	60000	60000	50	4	40	10	2	20

Worxへの接続のみを使用する既存ユーザーのワークロード

次の表は、既存ユーザー（Worxへの接続のみを使用）のワークロードです。 このワークロードにより、WorxMailおよびWorxWebアプリを使用する1人のユーザーがシミュレートされました。 このミュレーションを使用して、XenMobile構成内のNetScaler Gatewayのスケーラビリティを測定しました。 この測定が可能になるのは、これら2つのWorxアプリのみを使用することでネットワークの負荷が最小限になるからです。 WorxWebアプリについては、ユーザーは内部Webサイトにアクセスしています。この場合XenMobileサーバーのSSOはトリガーされません。 このモードで含まれ操作は以下のとおりです。

- 認証（NetScaler GatewayとXenMobile）
- WorxMailおよびWorxWeb接続（VPNトンネル） — 4接続

以下の表は既存ユーザーのワークロードパラメーターを示します。

Devices	列挙	デバイスあたりのアプリの列挙	デバイスあたりのVPNトンネル[1]
1000	1000	50	3
10000	10000	50	3
30000	30000	50	3
60000	60000	50	3

1. VPNトンネルの数は、WorxMailおよびWorxWebの接続の数に対応します。

次の表は、WorxMailおよびWorxWebの接続プロファイルの概要です。

デバイス接続	接続の種類	セッションあたりの送信データ[1]	セッションあたりの受信データ[1]
WorxMail接続 #1	タイプ1[2]	4.1MB	4.1MB
WorxMail接続 #2	タイプ1	6.3MB	12.5MB
WorxWeb接続 #1	タイプ2[3]	5.2MB	15.7MB
WorxWeb接続 #2	タイプ2	4.1MB	3.4MB
セッションあたりの転送バイト合計[1]		～19.7MB	～40.7MB

1.セッションあたり：8時間

タイプ1：長時間の非対称な送信および受信接続（Microsoft Exchangeのメールボックスに対するWorxMailの接続）。

タイプ2：閉じてしばらく待った後で再び開く、非対称な送信および受信接続（WorxWeb接続）

これらの推奨事項は、「中程度」のワークロードを自動化するためのWorxMailおよびWorxWebのプロファイルに基づいて
設定されています。 接続の詳細を変更すると解析結果に影響があります。 たとえば、ユーザーあたりの接続数を増やす場合、サポートされるNetScaler Gatewayセッションの数は減少する可能性があります。

WorxMailおよびWorxWebのプロファイル

各アプリで使用するプロファイルは、「非常に高負荷の」ワークロードを自動化することを目的としています。次の表は、WorxMailおよびWorxWebのプロファイルの詳細です。

中程度のワークロードのWorxMailプロファイル

1日あたりの送信メッセージ	20
1日あたりの受信メッセージ	80
1日あたりの読み取りメッセージ	80
1日あたりの削除メッセージ	20
平均メッセージサイズ（KB）	200

中程度のワークロードのWorxWebプロファイル

起動Webアプリ数	10
手動で開くWebページ数	10
Webアプリあたりの平均要求-応答ペア数	100
要求の平均サイズ（バイト）	300
応答の平均サイズ（バイト）	1000

構成とパラメーター

以下の構成を使用してスケーラビリティテストを実行しました。

- NetScaler Gatewayおよび負荷分散（LB）仮想サーバーを同じNetScaler Gatewayアプライアンスに共存させました。
- NetScalerのセッションタイムアウトを60分に設定しました。
- SSLトランザクションにNetScaler Gateway上の2048ビットキーを使用しました。

終了基準

この解析の基礎はログオン数です。 ログオン数によって、インフラストラクチャコンポーネントおよびコンポーネントそれぞれの構成のガイドラインが提供されます。 ログオン数は、以下のようなエラー発生の余地を考慮に入れたものであることに留意してください。

- 無効な応答
  - ステータスコードが200ではなく401/404の応答は無効とみなされます。
- 要求のタイムアウト
  - 120秒以内に応答があることが期待されます。
- 接続エラー
  - 接続がリセットされます。
  - 接続が突然終了されます。

全体的なエラー率が任意のデバイスから送信される要求数の合計の1%未満であれば、ログオン数は許容可能です。 エラーには、各個別のワークロード操作に対応するエラーはもちろん、CPUやメモリの消費のようなインフラストラクチャコンポーネントの物理的なパフォーマンスにかかわるものも含まれます。

ソフトウェアおよびハードウェアの詳細

以下の表は、これらのテストに使用されたXenMobileインフラストラクチャのソフトウェアを示します。

コンポーネント	バージョン
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n

XenMobile	10.3.0.824
外部データベース	Microsoft SQL Server 2014

以下のテーブルに示すXenServerプラットフォーム上で、スケーラビリティテストを実行しました。

ベンダー	Genuine Intel
Model	Intel Xeon CPU — E5645 @ 2.40GHz（CPU数24）

これにはインフラストラクチャの中核的なサービス（Active Directory、Windowsドメインネームサービス（DNS）、証明機関、Microsoft Exchangeなど）とXenMobileコンポーネント（XenMobile仮想アプライアンスおよび該当する場合はNetScaler Gateway VPX仮想アプライアンス）が含まれます。

XenMobileサーバー10.3.5について

Oct 25, 2016
XenMobileコンソールで、以下のリリースからXenMobile 10.3.5に直接アップグレードできます。

- XenMobile 10.3 Rolling Patch 1
- XenMobile 10.3
- XenMobile 10.1 Rolling Patch 4
- XenMobile 10.1

アップグレードを行うには、xms_10.3.5.354.binを使用します。 XenMobileコンソールで、右上の歯車アイコンをクリックした後、 **[Release Management]** をクリックします。 **[Upgrade]** をクリックしてから、xms_10.3.5.354.binファイルをアップロードします。 コンソールでのアップグレードについて詳しくは、「XenMobileのアップグレード」を参照してください。

XenMobile 10.3.5を新たにインストールする場合は、「XenMobileのインストール」を参照してください。

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

XenMobile 10.3.5の新機能

XenMobile 10.3.5には、修正プログラムおよび次の新機能があります。

XenMobile Server 10.3.5のクラウドアップデート

クラウドサービスチームは、お使いのXenMobilサーバーのクラウド展開をバージョン10.3から10.3.5にダウンタイムなしでアップデートできます。

Android Mの動的許可

Android Mユーザーが4つの種類の権限を有効化またはブロックできるようにすることができます。 ユーザーがWorx Homeに登録すると、Worx Homeに対して次の権限を許可または拒否するように求める4つのメッセージが表示されます。

- Worx Homeが適切に機能するためのデバイス情報へのアクセス
- 電話の発着信の実行および管理
- デバイス上の写真、メディア、およびファイルへのアクセス
- デバイスの位置情報へのアクセス

iOSのTouch ID認証

このリリースでは、iOSユーザーがWorx Homeに加えてWorxアプリもTouch IDを使用することを再認証できるようにすることができます。 iOS 8およびiOS 9デバイスの場合、Worx Homeでシングルサインオンが有効で、Touch IDが有効な場合、PINを使用する代わりにこの組み合わせを使用できます。 NetScaler Gatewayによるオンライン認証が必要な場合でも、ユーザーは、PINを入力する必要があります。 このユーティリティを使用する状況として、以下の例があります。

- ユーザーセッションがタイムアウトになった。
- ユーザーがデバイスを再起動した。
- Worx Homeが現在実行中ではなく、ユーザーがWorx HomeまたはMDXアプリを起動した。

登録プロファイル

AndroidおよびiOSデバイスでXenMobileコンソールの **[構成] > [登録プロファイル]** ページに移動して、登録プロファイルを作成できるようになりました。 登録プロファイルをすべてのサーバーモードに適用できます。 複数の登録プロファイルを作成して、異なるデリバリーグループに関連付けることができます。

注： **[登録プロファイル]** ページはWindowsデバイスでは使用できません。 Windows デバイスの登録手順については、「Windowsデバイス」を参照してください。

ユーザーごとのデバイス制限の変更

以前は、サーバープロパティの **[ユーザーごとのデバイスの数]** で、ユーザーごとのデバイス制限を設定していました。 このサーバープロパティは、廃止され、 デバイス制限は新たに **[構成] > [登録プロファイル]** ページに移動して構成するようになりました。 また、以前はMDMでのみデバイス数を制限できましたが、 MAMのデバイス数も制限できるようになりました。

デフォルトでは、1人のユーザーが登録できるデバイスの数には制限があります。 詳しくは、 デバイス登録の制限」を参照してください。

言語サポート

XenMobile 10.3.5は、WorxStoreでヘブライ語と繁体中国語をサポートしています。

新しいMAM-onlyモード

XenMobile 10.3.5では、新しいMAM-onlyサーバーモードが搭載されます。 従来のMAMモードと新しいMAMモードを区別するため、このドキュメントでは新しいMAMモードを「MAM-only」と表記し、従来のMAMモードを「従来のMAMモード」と表記します。従来のMAM機能は以前と変わりませんが、今後のリリースで強化される予定はありません。

XenMobileのサーバーモードプロパティが**MAM**の場合、MAM-onlyモードが有効になります。 デバイスはMAMモードで登録します。

従来のMAM機能は、XenMobileサーバーモードプロパティが**ENT**であり、ユーザーがデバイス管理を行わないことを選択した場合に有効になります。 デバイスはMDM+MAMモードで登録します。 MAM+MDMモードでは、XenMobile 10.3.5へのアップグレードを行うかどうかにかかわらず、MDM管理を行わないユーザーに従来のMAM機能が提供されます。

注：以前は、サーバーモードプロパティを**MAM**に設定するのは、**ENT**に設定するのと同じ効果がありました。デバイスをMDM+MAMで登録すると、MDM管理を行わないユーザーは従来のMAM機能を使用できました。

MAM-onlyモードの利点には、（デバイスのパスコードだけではない）追加の暗号化、モバイルVPN、およびエンドユーザーのプライバシーの強化などがあり、BYOデバイスに最適です。

お使いのXenMobileサーバーのモードが現在MAMの場合、新しいMAM-onlyモードにアップグレードすると、以前はMDMだけで利用可能だった次の機能を利用できるようになります。 これらの機能は、Windows Phoneでは利用できません。

- **証明書ベースの認証**
  MAM-onlyモードでは、証明書ベースの認証がサポートされます。 ユーザーは、ADパスワードの有効期限が切れても、引き続きアプリにアクセスできます。 MAMデバイスを証明書ベースの認証に切り替える場合は、NetScaler Gatewayを設定する必要があります。 デフォルトでは、XenMobileの **[Settings] > [NetScaler Gateway]** の **[Deliver user certificate for authentication]** は **[Off]** に設定されており、これはユーザー名とパスワードの認証が使用されていることを意味します。 証明書ベースの認証を有効にするには、この設定を **[On]** に変更する必要があります。
- **Self Help Portal**では、エンドユーザーは独自のアプリロックとアプリワイプを実行できます。 これらの操作は、デバイス上のすべてのアプリに適用されます。 アプリロックとアプリワイプの操作は **[Configure] > [Actions]** で設定できま

す。

- [High Security]、［Invitation URL］、［Two Factor］を含む**すべての登録モード**は、 **［Manage］ > ［Enrollment］**で設定されます。
- AndroidおよびiOSデバイス向けの**デバイス登録制限**。 サーバープロパティ**［Number of Devices Per User］**は新しい**［Configure］ > ［Enrollment Profiles］**ページに移動され、新しいMAM-onlyモードにも適用されるようになりました。
- **MAM-only API**。 MAM-onlyデバイスでは、任意のRESTクライアントとXenMobile REST APIを使用してRESTサービスを呼び出し、XenMobileコンソールから公開されているサービスを呼び出します。
- このリリースで利用できるMAM-only APIでは、次のことができます。
  - 招待URLとワンタイムPINを送信する
  - デバイス一覧でアプリのロックとアプリのワイプを発行する

> **Important**
>
> MAM-onlyモードを使用するには、XenMobileをこの記事の説明に従って設定し、ユーザーは使用しているデバイスを再登録する必要があります。 登録に必要なXenMobileサーバーのFQDNをユーザーに提供してください。
>
> 新しいMAM-onlyモードでは、ENTモードと同様、デバイスの登録にXenMobileサーバーのFQDNを使用します。（従来のMAMモードでは、デバイスの登録にNetScaler GatewayのFQDNを使用します。）

このアップグレードによる登録デバイスへの影響

次の表は、XenMobile 10.3.5の新機能による登録デバイスへの影響の概要を示しています。

以下のように登録されているデバイスの場合：	**XenMobile 10.3.5では以下が提供されます。**	**管理者タスク**	**ユーザータスク**
MDM • サーバーモード：MDM	• いくつかのバグが修正されました。 • 新機能	XenMobile 10.3.5のインストール	なし
MDM+MAM • サーバーモード：ENT • デバイス管理を行うユーザー	• いくつかのバグが修正されました。 • 新機能	XenMobile 10.3.5のインストール	なし
MAM • サーバーモー	• いくつかのバグが修正されました。 • 新機能 注：この使用例では、デバイスは従来のMAMモード		

ド：ENT • デバイス管理を行わないユーザー	で登録されます。 これらのユーザーに新しいMAM機能を提供する場合は、該当のユーザーに対して新しいXenMobileサーバーをセットアップしてください。	XenMobile 10.3.5のインストール	なし
		従来のMAM 機能を使用し続けるには XenMobile 10.3.5のインストール	なし
MAM • サーバーモード：MAM	• いくつかのバグが修正されました。 • 新機能 • 新しいMAM-onlyモード用のオプションアップグレード	MAM-onlyモードにアップグレードするには 1. XenMobile10.3.5をインストールします。 2. 追加の、必要な設定については、次の「MAM-onlyモード設定の概要」を参照してください。	デバイスの再登録

MAM-onlyモード設定の概要

*MAM-onlyモード*は、エンタープライズライセンスや 上級ライセンスで使用される場合、MAMサーバーモードを参照します。 MAM-onlyモードは、XenMobile Serverのサーバーモードが ENTの場合に使用される *MAM+MDMモード*とは異なります。 MAM+MDMモードでは、MDM管理を行わないユーザーには、XenMobile 10.3.5へのアップグレードを行うかどうかにかかわらず、従来のMAM機能が提供されます。

> **Important**
>
> 従来のMAM機能はそれ以前のリリースと同様に機能し、今後のリリースで拡張されません。

次の表は、特定のライセンスの種類および機能のデバイスモードで使用するサーバーモードの概要を示しています。

現在のエディションのライセンス	デバイスを登録するモード	必要なサーバーモードプロパティの設定
ENT/ADV/MDM	MDMモード	MDM
ENT/ADV	MAMモード（MAM-onlyモードとも呼ばれます）	MAM
		ENT

ENT/ADV	MDM+MAMモード	デバイス管理を行わないユーザーは従来のMAMモードで操作します。

MAM-onlyモードは、以下の場合に*のみ*設定してください。

- XenMobileサーバーの現在の**サーバーモード**が**MAM**であり、 追加機能を使用するために新しいMAM-onlyモードに変更する必要がある場合。
- XenMobileサーバーに接続するすべてのユーザーにMAM-only機能を提供するために、XenMobileサーバーをセットアップする必要がある場合。

一般的なMAM-onlyモードの設定手順を次に示します。

1. XenMobile 10.3.5をインストールするか、XenMobile 10.3.5にアップグレードします。
2. **[Manage] > [Devices]** ページで、 **[Server Mode]** を確認します。 **[Server Mode]** が **[MDM]** または **[ENT]** の場合は、この手順を実行しないでください。構成がデバイス管理をサポートしなくなります。
3. XenMobileサーバーおよびインターネットへのファイアウォールのポート8443と443を開いて、デバイスがXenMobileサーバーに接続できるようにします。 登録はXenMobileサーバーで行う必要があります。
4. アップグレードするサーバーの **[Server Mode]** が **[MAM]** に設定されている場合は、次の手順に進みます。 XenMobile 10.3.5の新規インストールを実行している場合、XenMobileサーバーの **[Server Mode]** はデフォルトの **[ENT]** です。 MAM-onlyモードを有効にするには、サーバープロパティ **[Server Mode]** を **[MAM]** に設定する必要があります。 詳しくは、「MAM-onlyサーバーモードの構成」を参照してください。
5. 証明書ベースの認証を使用する場合は、証明書ベースの認証がサポートされるようにXenMobileおよびNetScaler Gatewayを設定します。 デフォルトでは、XenMobileの **[Settings] > [NetScaler Gateway]** の **[Deliver user certificate for authentication]** は **[Off]** であり、これはユーザー名とパスワードの認証が使用されていることを意味します。 証明書ベースの認証を有効にするには、この設定を **[On]** に変更する必要があります。 設定について詳しくは、「MAM-Onlyモードの証明書認証」を参照してください。
6. MAM-onlyモードで使用する通知テンプレートを選択またはセットアップする場合、登録招待状の送信でサポートされている方法はSMTPのみであることに注意してください。
7. ユーザーが新しいMAM-onlyモードにアップグレード中の場合は、ユーザーにXenMobileサーバーのFQDNを提供して、再登録が必要であることを通知してください。
   新しいMAM-Onlyモードでは、ENTモードと同様、デバイスの登録に XenMobileサーバーのFQDNを使用します。 （従来のMAMモードでは、デバイスの登録にNetScaler GatewayのFQDNを使用します。）

次の表は、従来のMAM機能（XenMobile 10.3およびXenMobile 10.3.5）と新しいMAM-onlyモード（XenMobile 10.3.5）の違いの概要を示しています。

登録シナリオおよびその他の機能	**XenMobile 10.3 従来のMAM（サーバーモードENT）**	**XenMobile 10.3.5 従来のMAM（サーバーモードENT）**	**XenMobile 10.3.5 MAM-onlyモード（サーバーモードMAM）**
証明書認証	サポートされません。	サポートされません。	サポートされます。 証明書認証を使用するには、NetScaler Gatewayが必要です。
展開要件	XenMobileサーバーは、デバイスから直接アクセスできるようにする必要はありません。	XenMobileサーバーは、デバイスから直接アクセスできるようにする必要はありません。	XenMobileサーバーはデバイスからアクセスできるようにする必要があります。

登録オプション	NetScaler Gateway FQDNを使用するか、登録しないことを選択してください。	NetScaler Gateway FQDNを使用するか、登録しないことを選択してください。	XenMobile Server FQDNを使用してください。
登録方法	[User name + Password]	[User name + Password]	[User name + Password]、[High Security]、[Invitation URL]、[Invitation URL + PIN]、[Invitation URL + Password]、[Two Factor]、[User name + PIN]
アプリロックおよびアプリワイプ	サポートされます。	サポートされます。	サポートされます。
アプリロックおよびアプリワイプのSelf Help Portalオプション	サポートされません。	サポートされません。	サポートされます。
アプリワイプの動作	アプリはデバイス上に残りますが、使うことはできません。アカウントはクライアントからのみ削除されます。	アプリはデバイス上に残りますが、使うことはできません。アカウントはクライアントからのみ削除されます。	アプリはデバイス上に残りますが、使うことはできません。アカウントはクライアントからのみ削除されます。
MAM-onlyユーザー向けの自動化された操作	サポートされません。	イベント、デバイスプロパティ、ユーザープロパティ操作がサポートされます。 インストールされたアプリベースの自動化された操作はサポートされません。	イベント、デバイスプロパティ、ユーザープロパティ操作がサポートされます。 インストールされたアプリベースの自動化された操作はサポートされません。
ADユーザーが削除された場合の組み込み操作	サポートされません。	アプリワイプはサポートされます。	アプリワイプはサポートされます。
登録の制限	MDMのみでサポートされます。サーバープロパティ経由で設定されます。	サポートされます。登録プロファイル経由で設定されます。	サポートされます。登録プロファイル経由で設定されます。

ソフトウェアインベントリ	サポートされます。XenMobileは、デバイスにインストールされているアプリケーションの一覧を作成します。	サポートされます。XenMobileは、デバイスにインストールされているアプリケーションの一覧を作成します。	サポートされません。

MAM-onlyモードの参照アーキテクチャ

XenMobileのMAM-only展開では、DMZまたは内部ネットワーク内でXenMobileサーバーのクラスターを展開できます。 いずれのシナリオでも、認証はNetScaler Gatewayを介して行われます。

XenMobile Enterpriseの展開とは異なり、XenMobile NetScaler Connector（XNC）およびXenMobile Mail Manager（XMM）は必要ありません。

リファレンスアーキテクチャ図については、『XenMobile展開ハンドブック』の「オンプレミス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。

MAM-only使用での注意事項

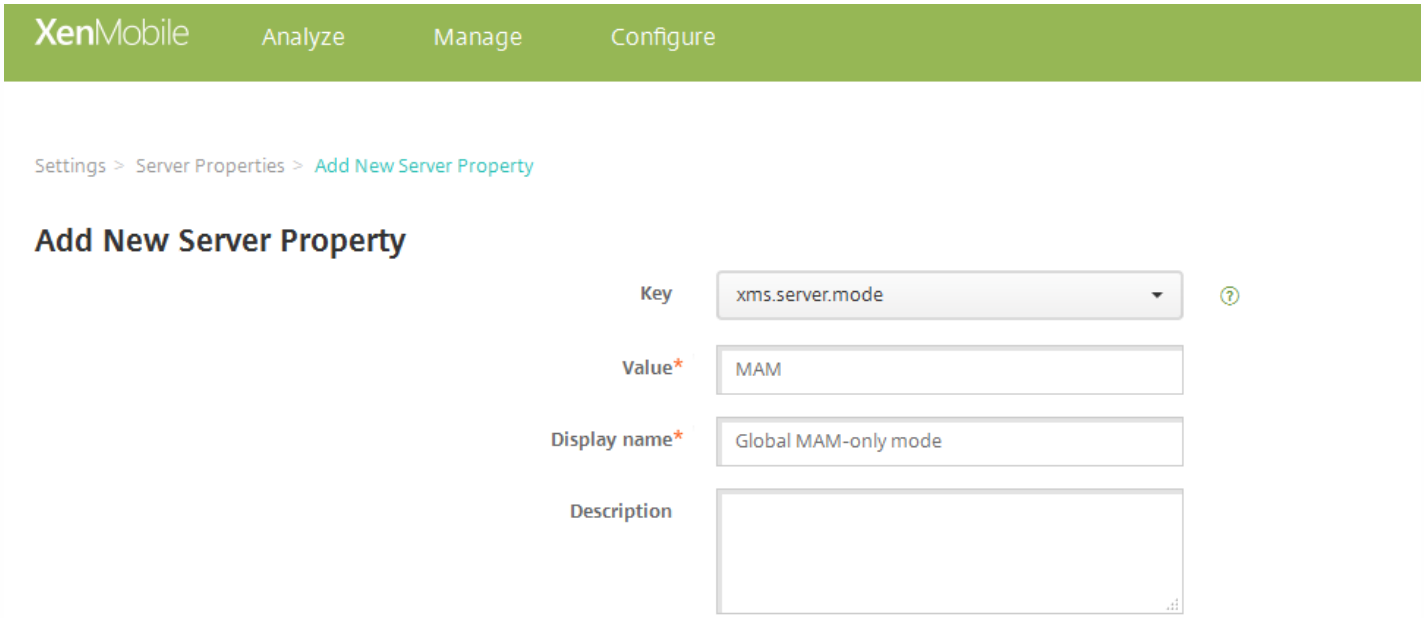
- 必須アプリケーションは自動的にインストールされません。 ユーザーがWorxStoreから手動で追加する必要があります。
- iOSユーザーは、iOS Developer証明書を信頼する必要があります。 Androidユーザーは、サードパーティのアプリケーションストアからインストールする設定を有効にする必要があります。
- ユーザーは、WorxStoreでのみアプリケーションの更新通知を受け取ります。
- ユーザーがWorx Homeを削除するかWorx Homeの登録を解除しても、インストール済みのアプリはユーザーにより削除されるまでデバイスに残ります。
- MAM-onlyモードでは、APNまたはGoogle Cloud Messagingはサポートされません。
- XenMobileコンソールでは、MAM-onlyモードで登録されたデバイスのジェイルブレイク/Root化の状態は表示されませんが、これらのデバイスには**ジェイルブレイクされたデバイスまたはRoot化済みデバイスのブロック**ポリシーが適用されます。

MAM-onlyサーバーモードの構成

新規インストールの実行後、サーバーはデフォルトでENTモードになります。 XenMobile 10.3.5でMAM-onlyモードを有効にするには、サーバーを次のように構成してください。

1. XenMonbileコンソールで、右上の歯車アイコンをクリックして **[Settings]** ページを開きます。
2. **[Settings]** ページで、 **[Server Properties]** をクリックします。
3. **[Add]** をクリックします。
4. **[Key]** で、 **[xms.server.mode]** をクリックします。
5. **[Value]** に「**MAM**」と入力します。
6. **[Display name]** に、 **[Server Properties]** 表に表示される説明を入力します。

説明を入力し（オプション）、 **[Save]** をクリックします。



Important

xms.server.modeプロパティをMAM-onlyに設定しても、XenMobileコンソールには依然としてMDMモードの領域（デバイスプロパティなど）が表示されます。 ただし、これらの設定は機能しません。

MAM-Onlyモード用の証明書認証

Aug 02, 2016

MAM-Onlyモードで証明書認証を使用するには、Microsoftサーバー、XenMobileサーバーを構成してから、NetScaler Gatewayサーバーを構成する必要があります。 この記事では、次の一般的な手順を詳しく説明します。

Microsoftサーバーの場合

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

XenMobileサーバーの場合

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

NetScaler Gateway：

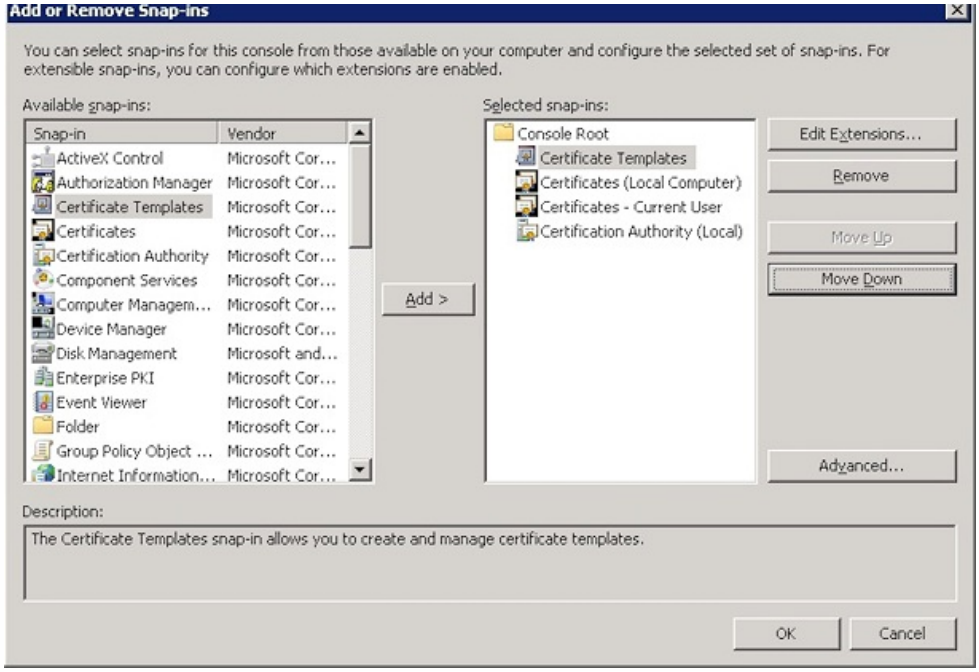
1. XenMobile MAM-Onlyモードの証明書認証用にNetScaler Gatewayを構成します。

証明書のスナップインをMicrosoft管理コンソールに追加するには

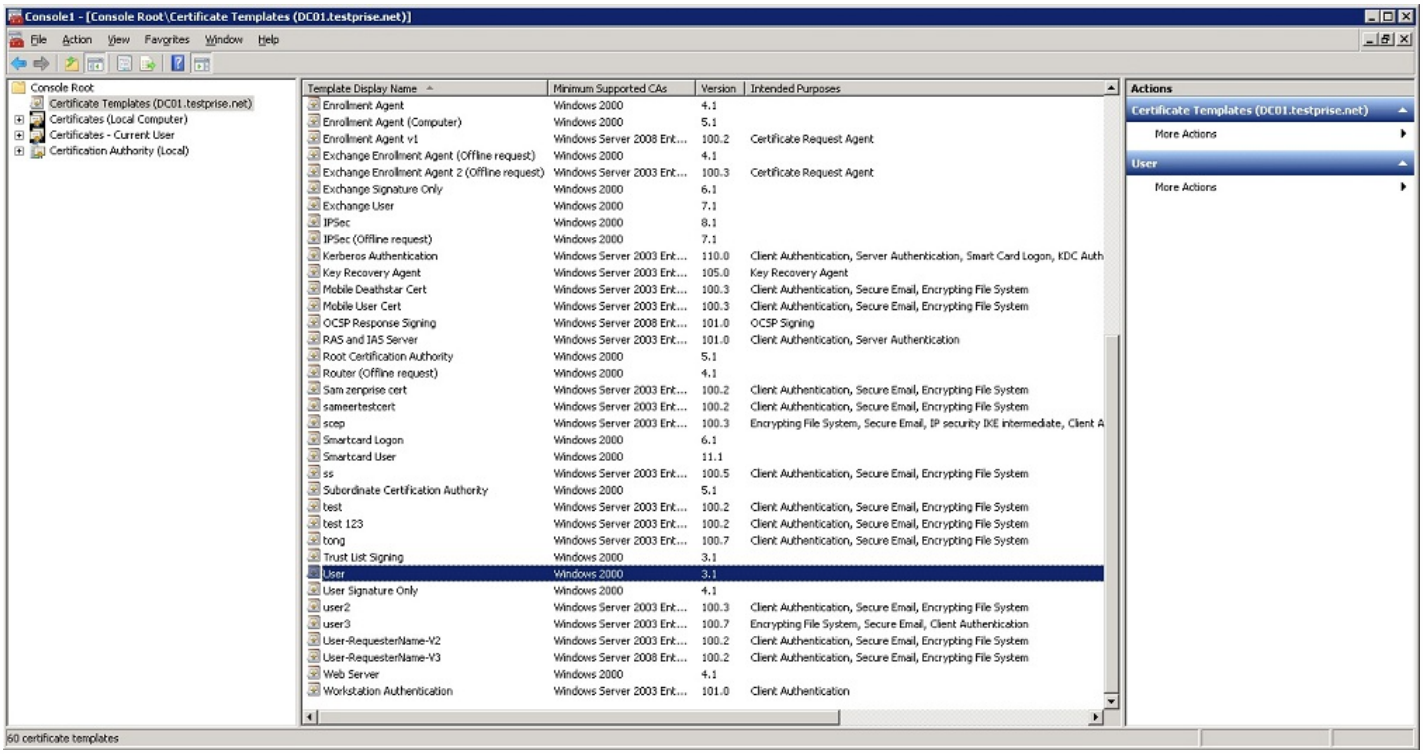
1. コンソールを開いて、**[スナップインの追加と削除]** をクリックします。

2. 次のスナップインを追加します。

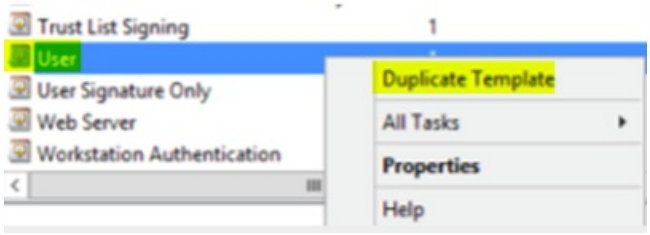
    証明書テンプレート
    証明書（ローカルコンピューター）
    証明書 - 現在のユーザー
    証明機関（CA）（ローカル）



3. **[証明書テンプレート]** を展開します。



4. **[ユーザー]** テンプレートと **[テンプレートの複製]** を選択します。

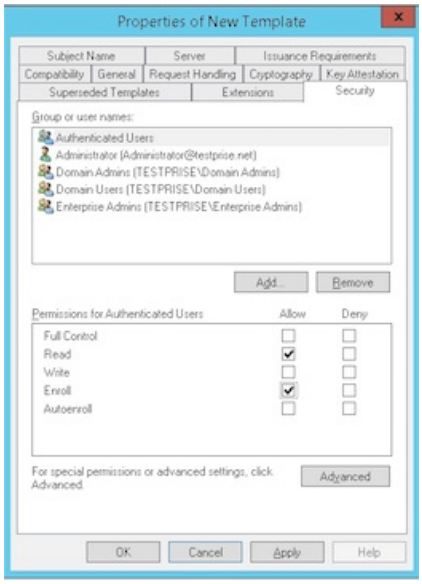


5. ［テンプレート］の表示名を入力します。

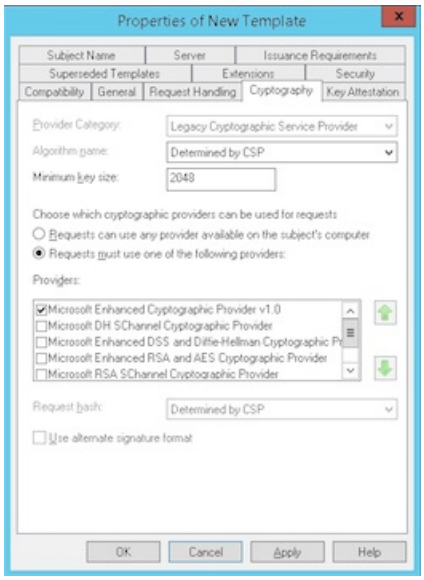
   重要：必要な場合以外は、 **[Active Directoryの証明書を発行する]** チェックボックスを選択しないでください。 このオプションが選択されると、すべてのユーザークライアント証明書がActive Directoryで発行/作成され、Active Directoryデータベースを圧迫する可能性があります。

6. テンプレートタイプとして［Windows 2003 Server］を選択します。 Windows 2012 R2の **[互換性]** で、 **[Certificate Authority]** を選択してWindows 2003を宛先として設定します。

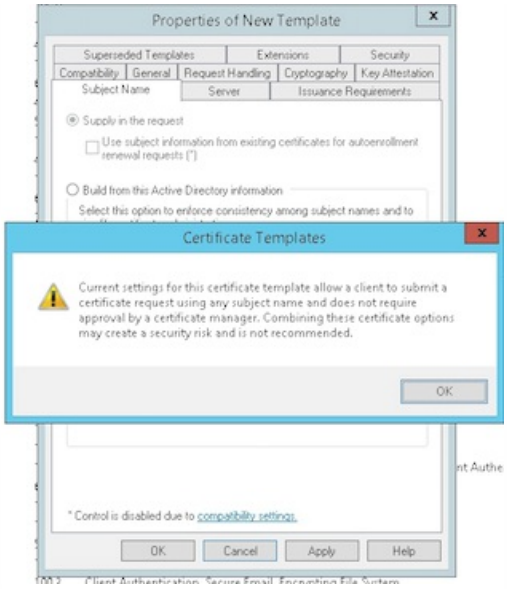
7. **[セキュリティ]** で、認証ユーザーの **[許可]** 列の **[登録]** オプションを選択します。



8. **[Cryptography]** で、XenMobileの構成中に入力する必要のあるキーサイズが入力されていることを確認します。



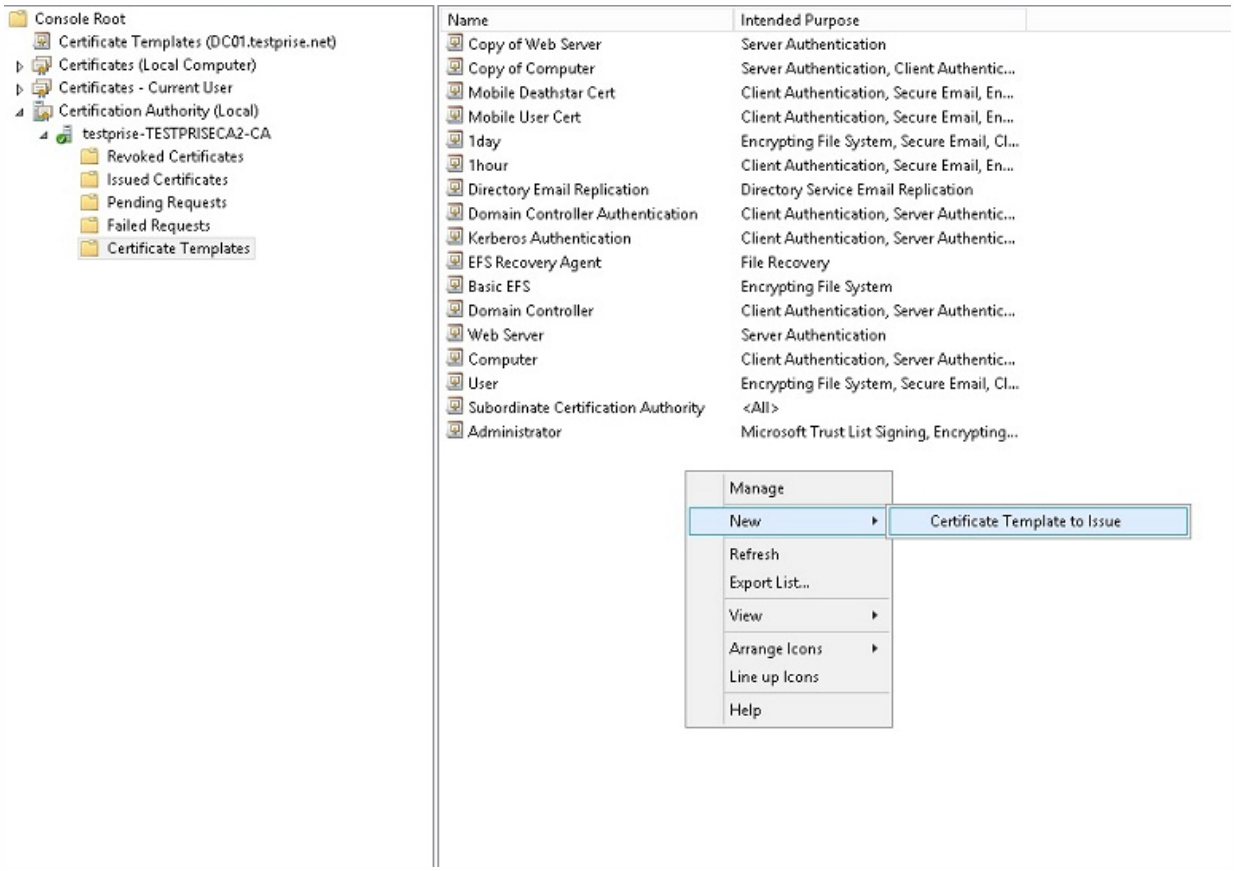
9. **[サブジェクト名]** で、 **[要求に含まれる]** を選択します。 変更を適用して、保存します。



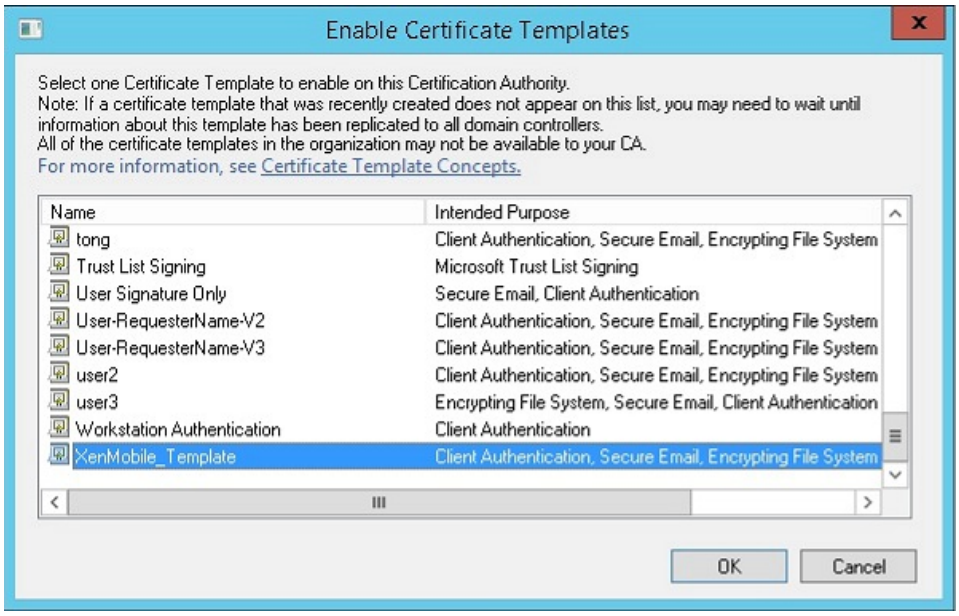
テンプレートを証明機関（CA）に追加するには

1. [**Certificate Authority**] に移動して、 [**証明書テンプレート**] を選択します。

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



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

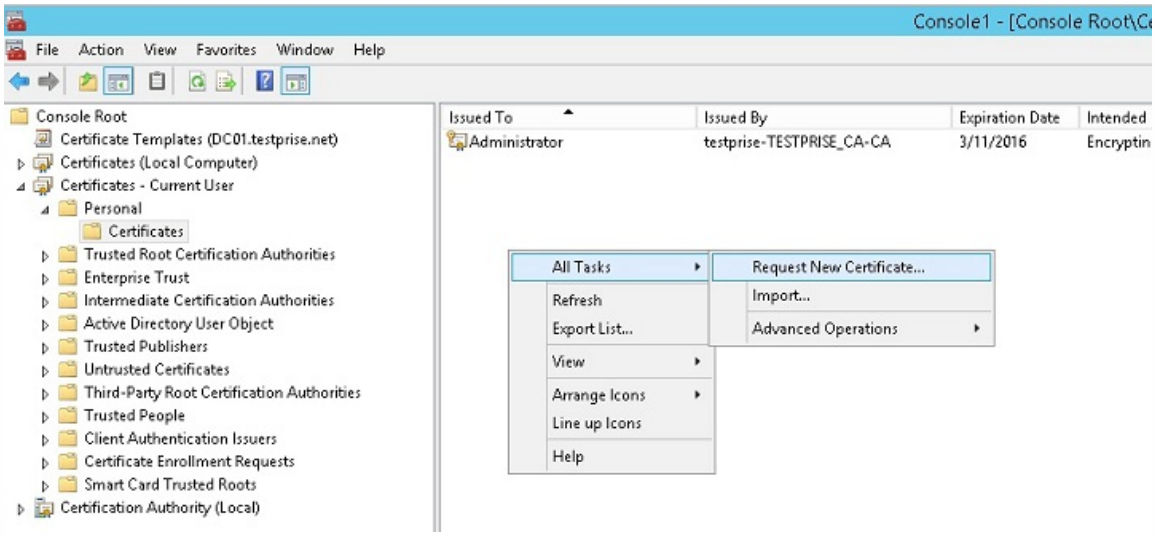


CAサーバーでPFX証明書を作成するには

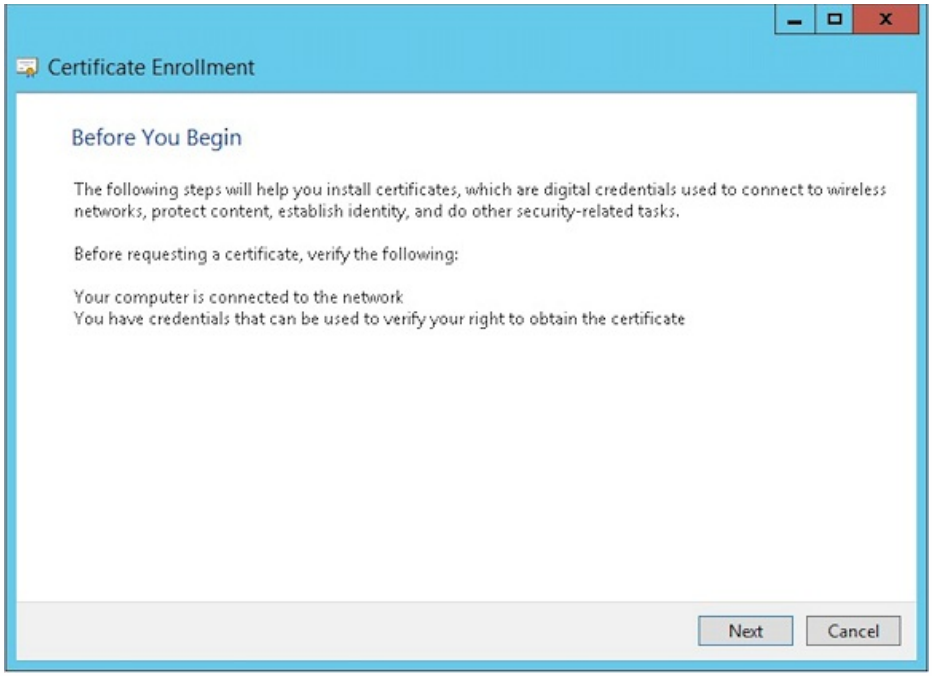
1. ログインしたサービスアカウントで、ユーザー.pfx certを作成します。 この.pfxファイルはXenMobileにアップロードされ、デバイスを登録するユーザーのためにユーザー証明書を要求します。

2. **[現在のユーザー]** で、 **[証明書]** を展開します。

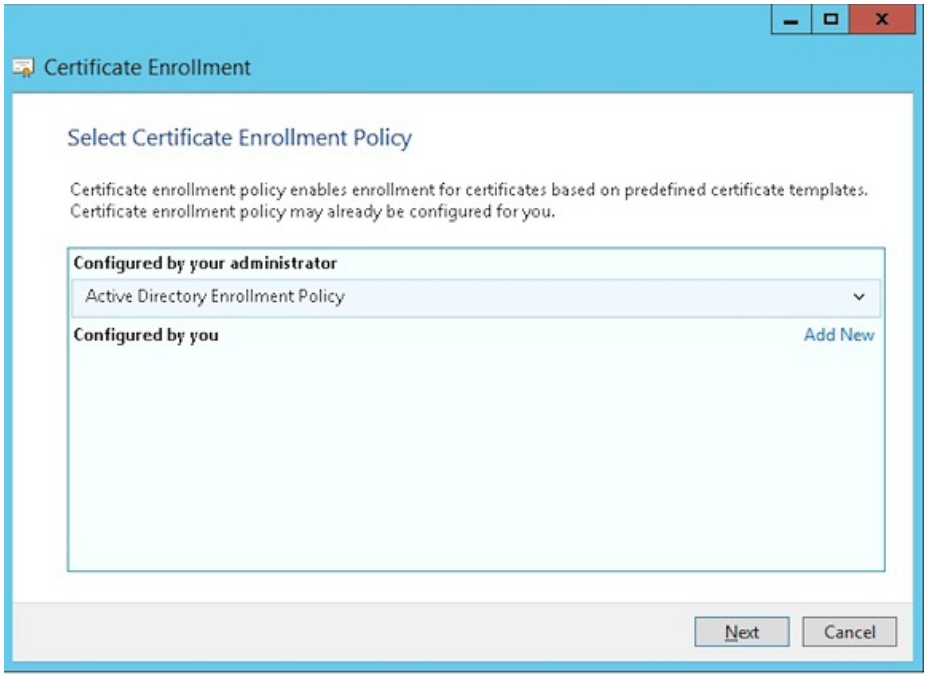
3. 右ペインで右クリックし、 **[Request New Certificate]** をクリックします。



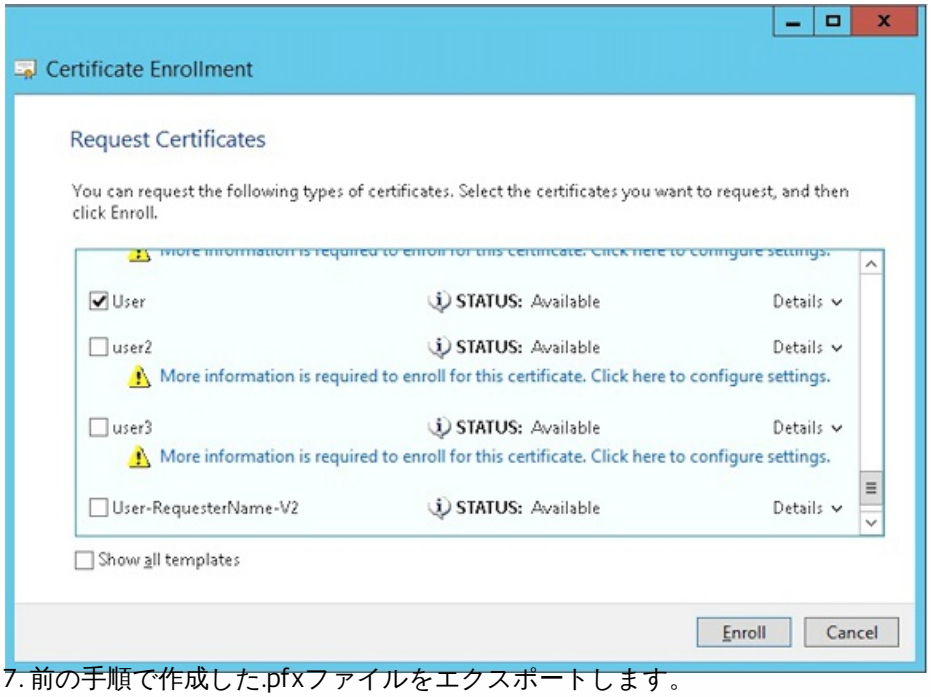
4. **[Certificate Enrollment]** 画面が表示されます。 **[次へ]** をクリックします。



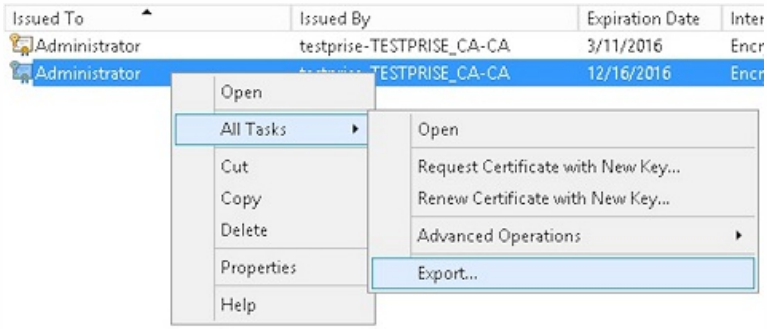
5. [**Active Directory登録ポリシー**] を選択して [**次へ**] をクリックします。



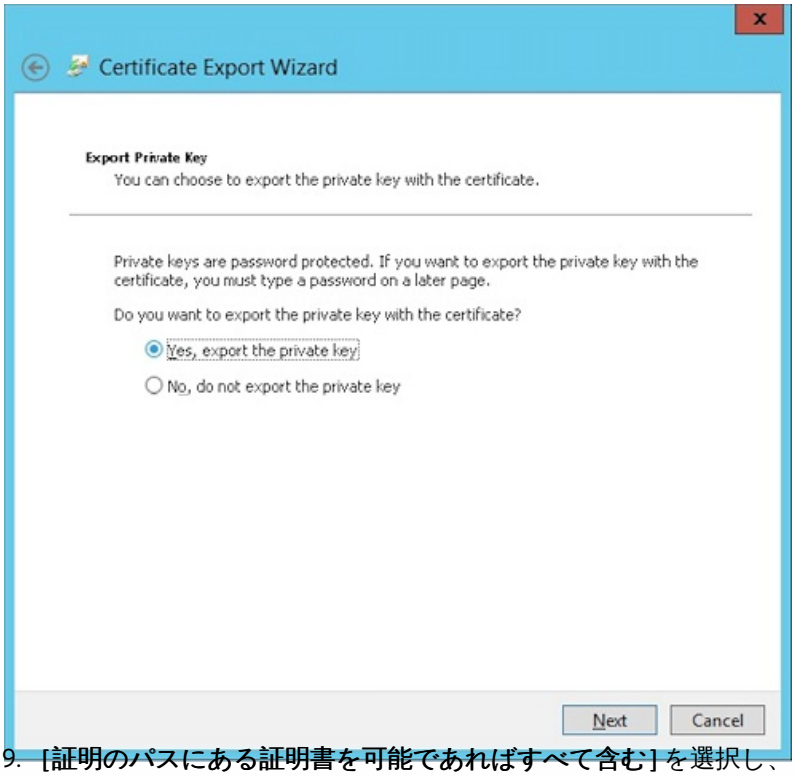
6. [**ユーザー**] テンプレートを選択し、 [**登録**] をクリックします。



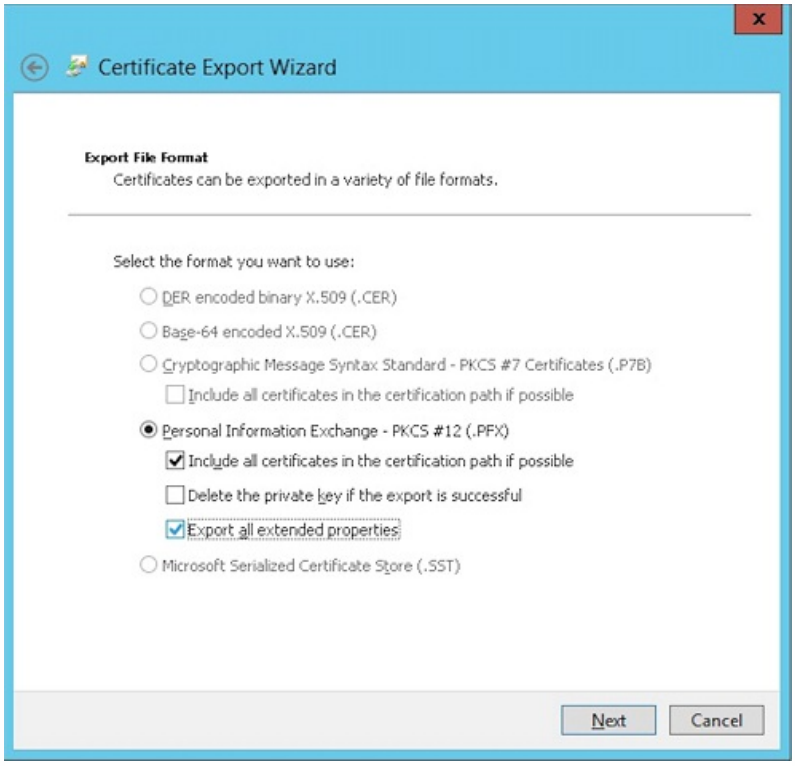
7. 前の手順で作成した.pfxファイルをエクスポートします。



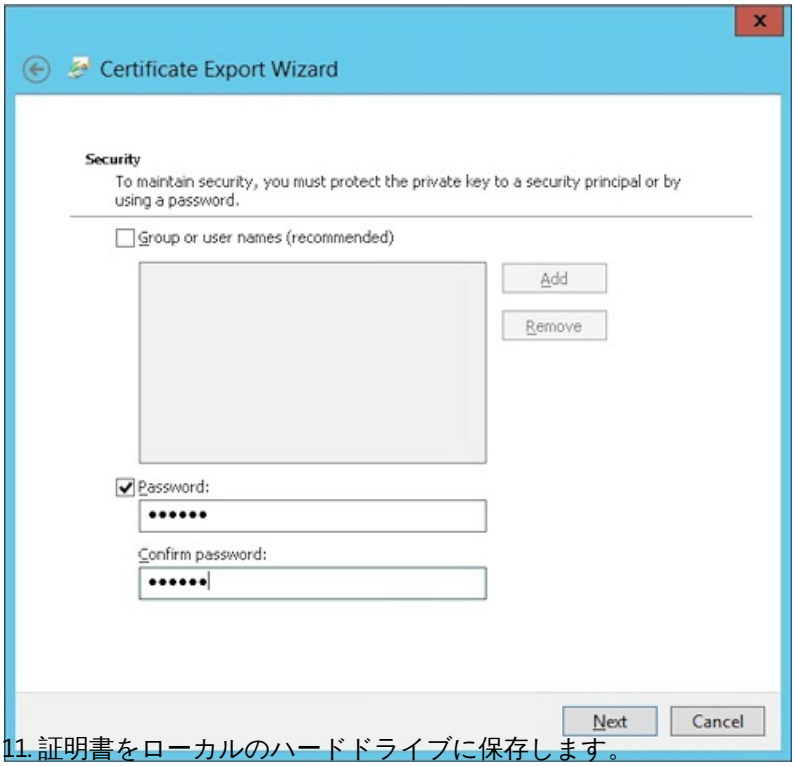
8. **[はい、秘密キーをエクスポートします]** をクリックします。



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



10. XenMobileに証明書をアップロードする際に使用するパスワードを設定します。



11. 証明書をローカルのハードドライブに保存します。

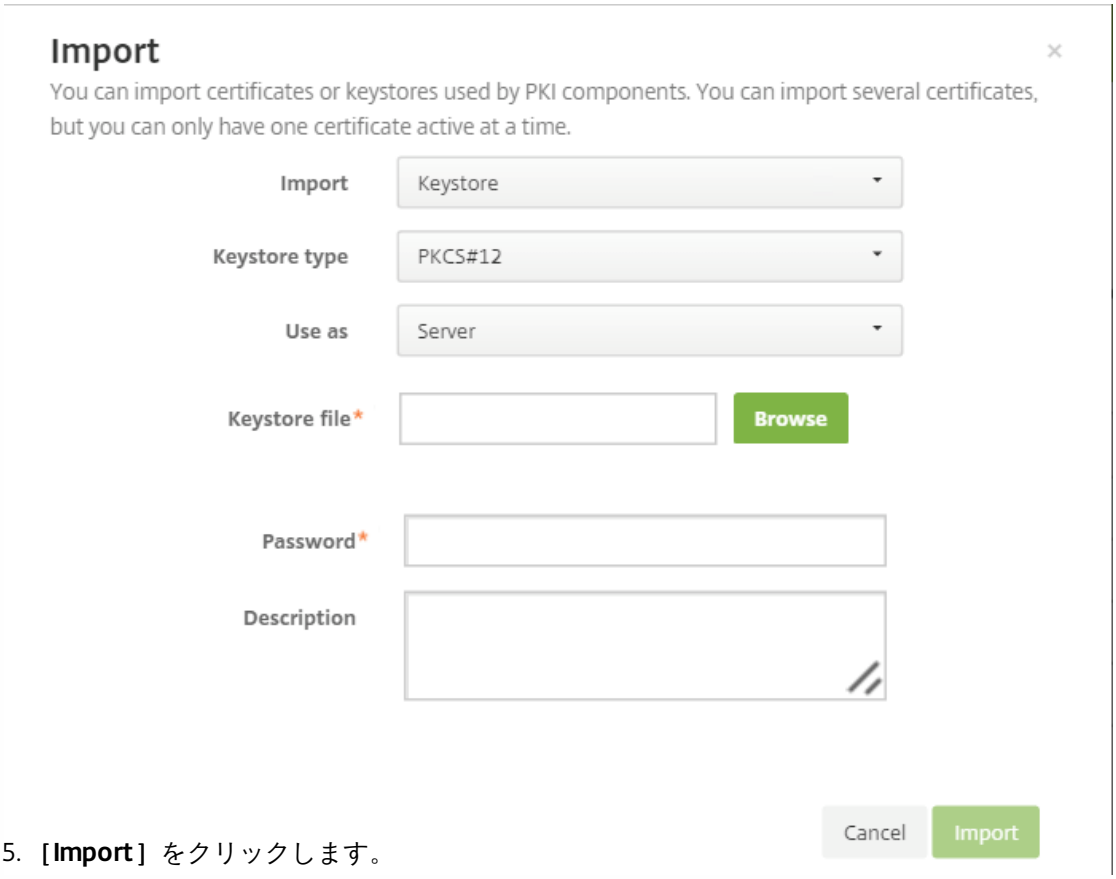
証明書をXenMobileにアップロードするには

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[設定]** 画面が表示されます。

2. **[証明書]** をクリックしてから、 **[インポート]** をクリックします。

3. 以下のパラメーターを入力します。

- **インポート**：Keystore
- **キーストアの種類**：PKCS#12
- **使用目的**：Server
- **Key File Name**： **[参照]** をクリックして、前の手順で作成した.pfx 証明書を選択します。
- **パスワード**：証明書と一緒に作成したパスワードを入力します。



5. [**Import**] をクリックします。

6. 証明書が正常にインストールされているか確認します。 ユーザー証明書として表示されているはずです。

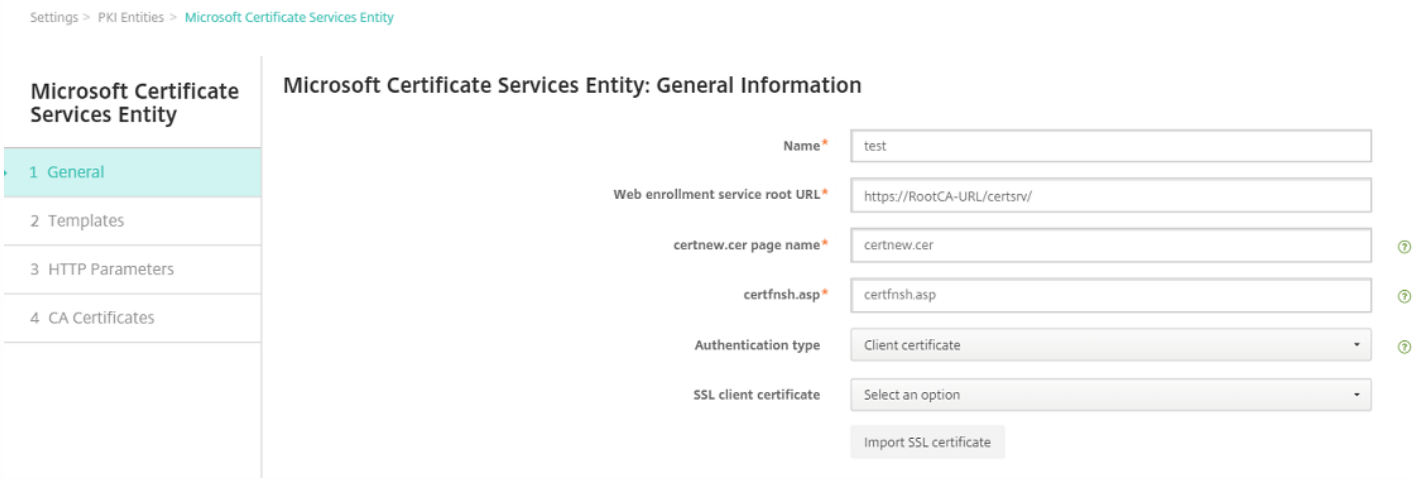
証明書に基づいた認証用PKIエンティティを作成するには

1. [**設定**] で、 [**詳細**] 、 [**証明書管理**] 、 [**PKIエンティティ**] の順に移動します。

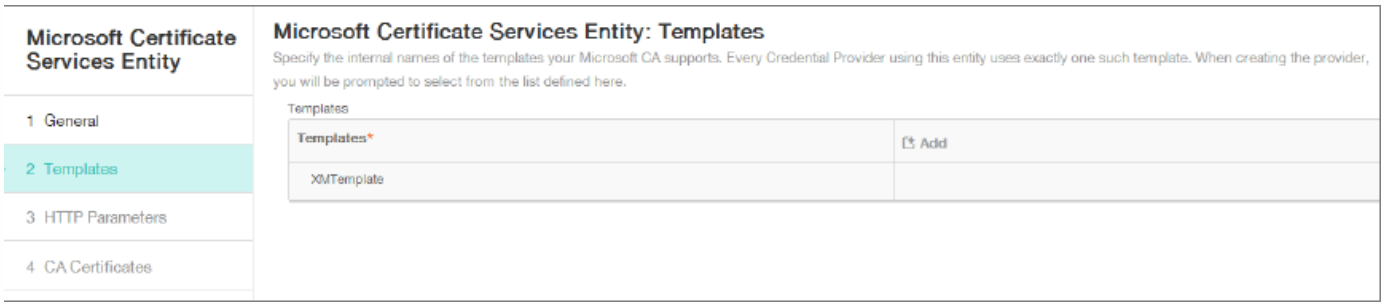
2. [**追加**] をクリックしてから、 [**Microsoft 証明書サービス エンティティ**] をクリックします。 [Microsoft 証明書サービス エンティティ: 一般的な情報] 画面が表示されます。

3. 以下のパラメーターを入力します。

- **名前**：任意の名前を入力します
- **Web 登録サービス ルート URL**: https://RootCA-URL/certsrv/
  注：URLパスの末尾が「/」で終わっていることを確認してください。
- **certnew.cer ページ名**：certnew.cer（デフォルト値）
- **certfnsh.asp**：certfnsh.asp（デフォルト値）
- **Authentication type**：クライアント証明書。
- **SSL クライアント証明書**: 署名済みのXenMobileクライアント証明書のルートCAを選択します。

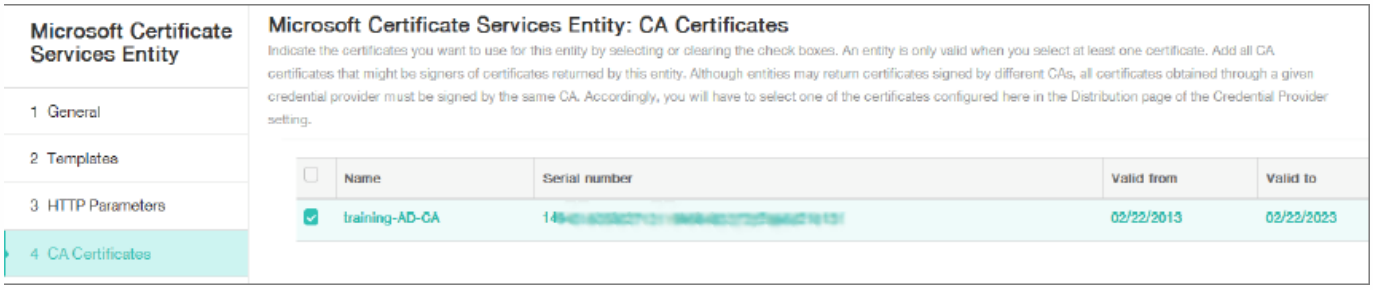


4. **[テンプレート]** で、Microsoft証明書を構成したときに作成したテンプレートを追加します。 空白を入れないように注意してください。



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. XenMobileクライアント証明書を発行するために使用するユーザー証明書を選択します。 これは、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。

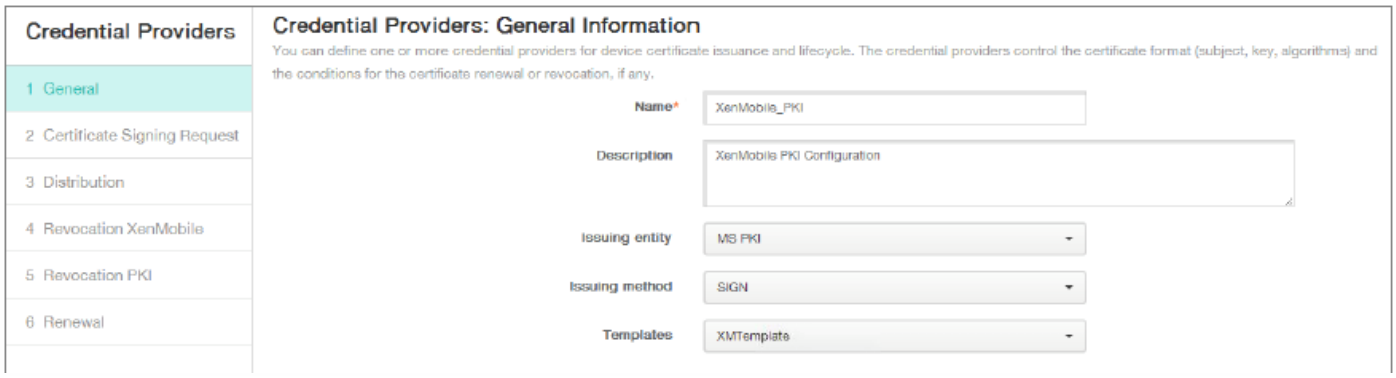
資格情報プロバイダーを構成するには

1. ［設定］で、 **[詳細]** 、 **[証明書管理]** 、 **[資格情報プロバイダー]** の順に移動します。

2. **[Add]** をクリックします。

3. **[全般]** で、次のパラメーターを入力します。

- **名前**：任意の名前を入力します。
- **アカウントの説明**：任意の説明を入力します。
- **発行エンティティ**：前に作成したPKIエンティティを選択します。
- **発行方式**：SIGN
- **テンプレート**：PKIエンティティに追加されたテンプレートを選択します。



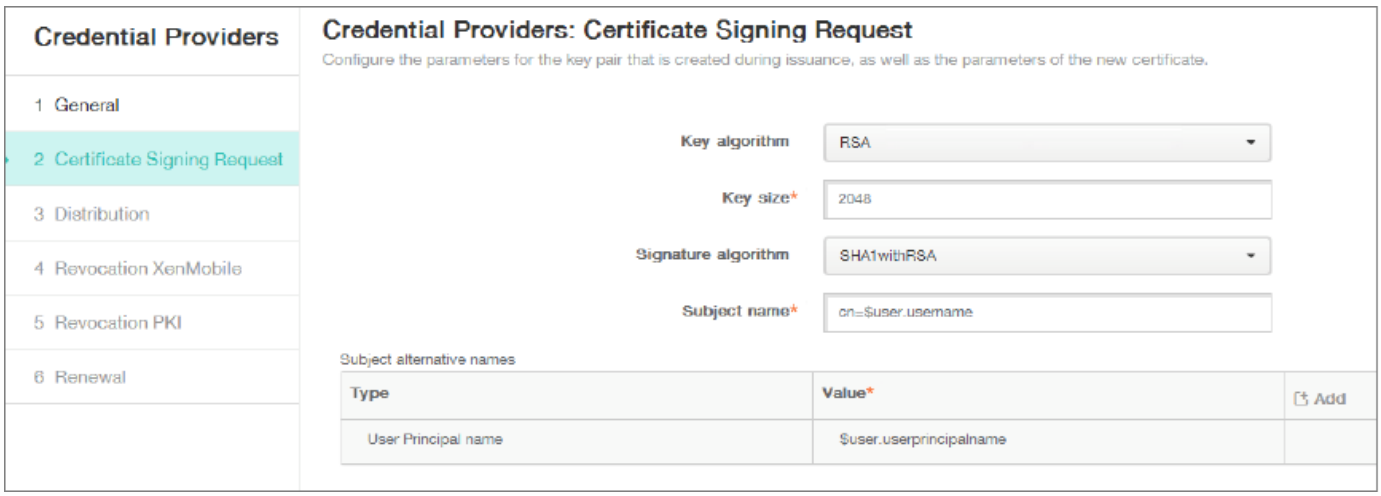
4. **[証明書署名要求]** をクリックしてから、次のパラメーターを入力します。

- **キー アルゴリズム**：RSA
- **キー サイズ**：2048
- **署名アルゴリズム**：SHA1withRSA
- **サブジェクト名**：cn=$user.username

  サブジェクト名はsAMAccountNameを参照します。 これにより、NetScalerが認証に［User Name］フィールドを使用できるようになります。

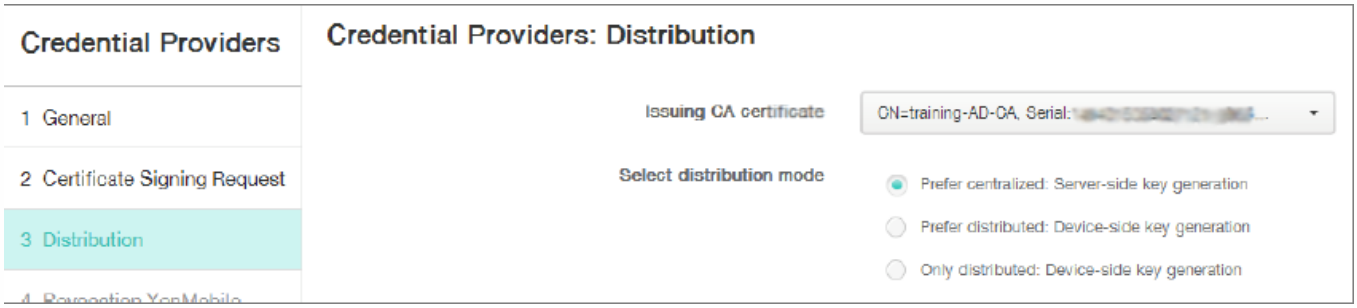
5. **[サブジェクトの別名]** の **[追加]** をクリックしてから、次のパラメーターを入力します。

- **種類**：ユーザープリンシパル名
- **値**：$user.userprincipalname



6. **[ディストリビューション]** をクリックし、次のパラメーターを入力します。

- **発行 CA 証明書**：署名済みのXenMobileクライアント証明書の発行CAを選択します。
- **ディストリビューション モードの選択**： **[優先集中: サーバー側のキー生成]** を選択します。

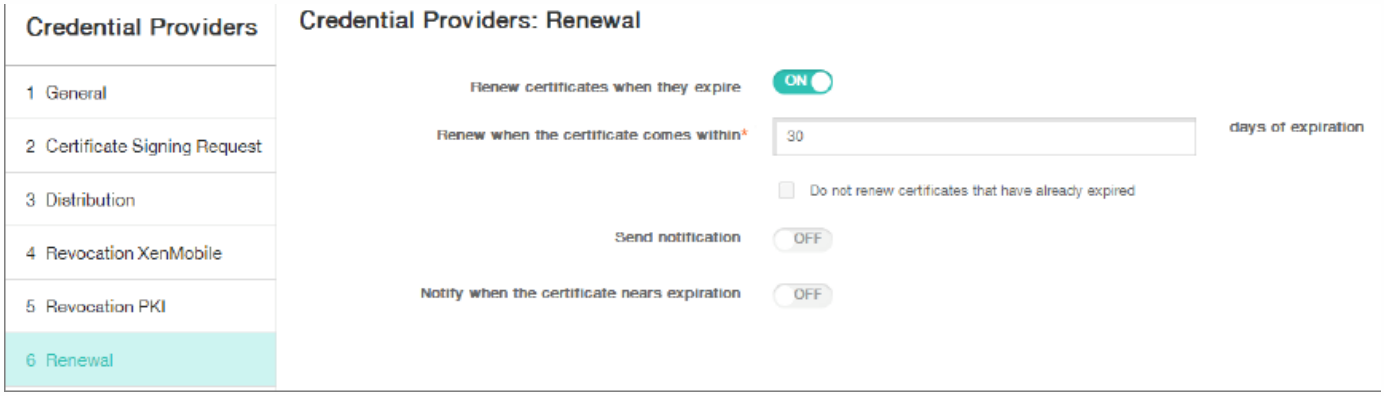


7. 次の2つのセクション（**Revocation XenMobile**と**Revocation PKI--**）で必要なパラメーターを設定します。 この記事では、このオプションをスキップします。

8. **[更新]** をクリックします。

9. **[有効期限が切れたら証明書を更新]** で **[オン]** を選択します。

10. そのほかの設定はすべてそのままにするか、必要な変更を加えます。



11. **[Save]** をクリックします。

XenMobileでNetScaler証明書の配信を構成するには

1. XenMobileコンソールにログオンして、右上の歯車アイコンをクリックします。 **[設定]** 画面が表示されます。

2. **[Server]** の下の **[NetScaler Gateway]** をクリックします。

3. NetScaler Gatewayがまだ追加されていない場合、 **[Add]** をクリックして、次のように設定を指定します。

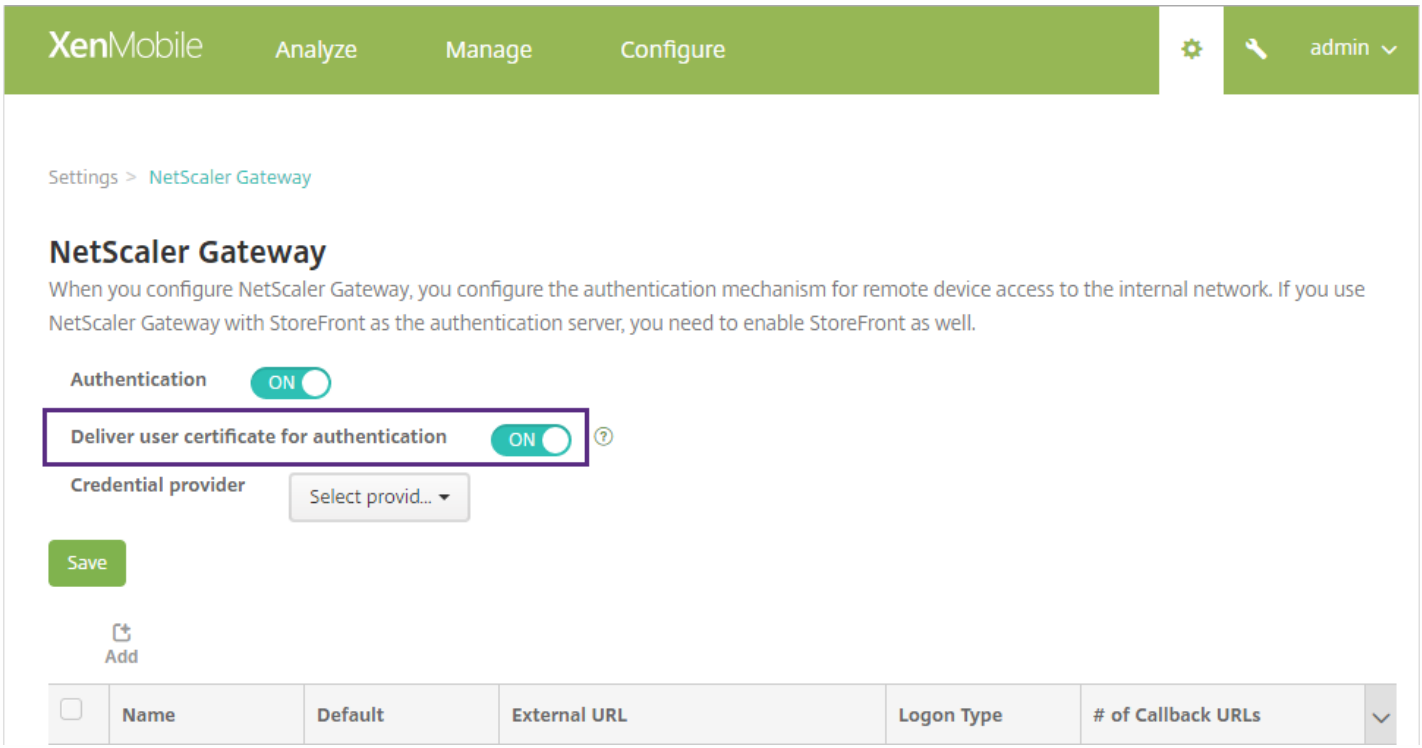
   External URL：https://YourNetScalerGatewayURL

   Logon Type：Certificate

   Password Required: OFF

   Set as Default: ON

4. [**Deliver user certificate for authentication**] で [**On**] を選択し、 [**Save**] をクリックします。



5. [**Credential Provider**] でプロバイダーを選択し、 [**Save**] をクリックします。

証明書認証用にNetScaler Gatewayを構成するには

次の手順で、XenMobile MAM-onlyモードの証明書認証用にNetScalerアプライアンスを構成します。

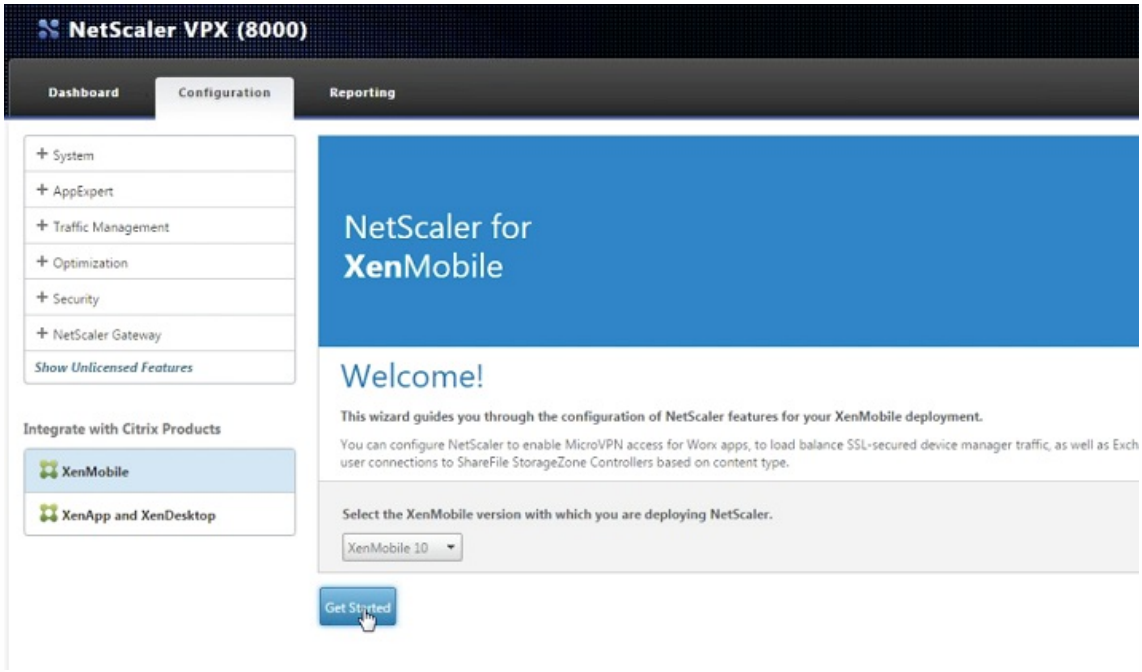
1. NetScalerにログオンします。

2. [**構成**] で、 [**Integrate with Citrix Products**] に移動し、 [**XenMobile**] を選択します。

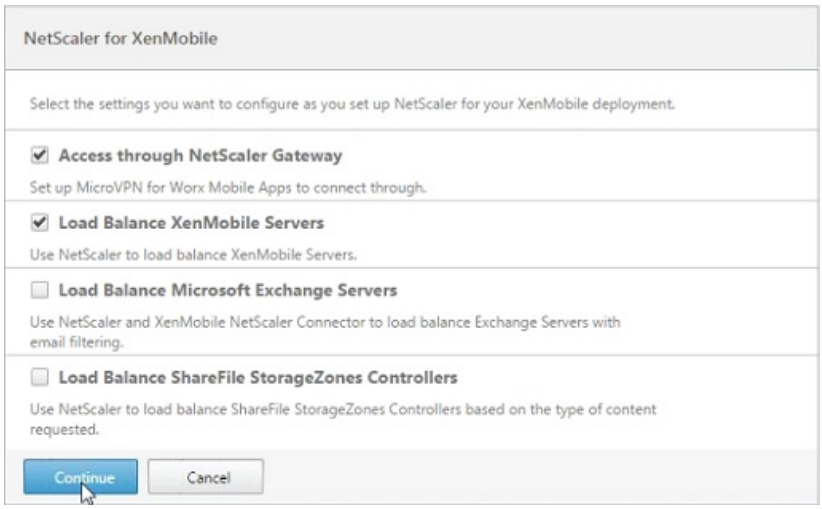
   これによって、XenMobile環境でNetScaler機能を構成するウィザードが開きます。

3. [**XenMobile 10**] を選択します。

4. [**開始**] をクリックします。



5. 次の画面で、 **[Access through NetScaler Gateway]** と **[Load Balance XenMobile Servers]** 選択してから、 **[続行]** をクリックします。



6. 次の画面で外部向けのNetScaler GatewayのIPアドレスを入力し、 **[続行]** をクリックします。

   NetScaler Gatewayのサーバー証明書画面が表示されます。

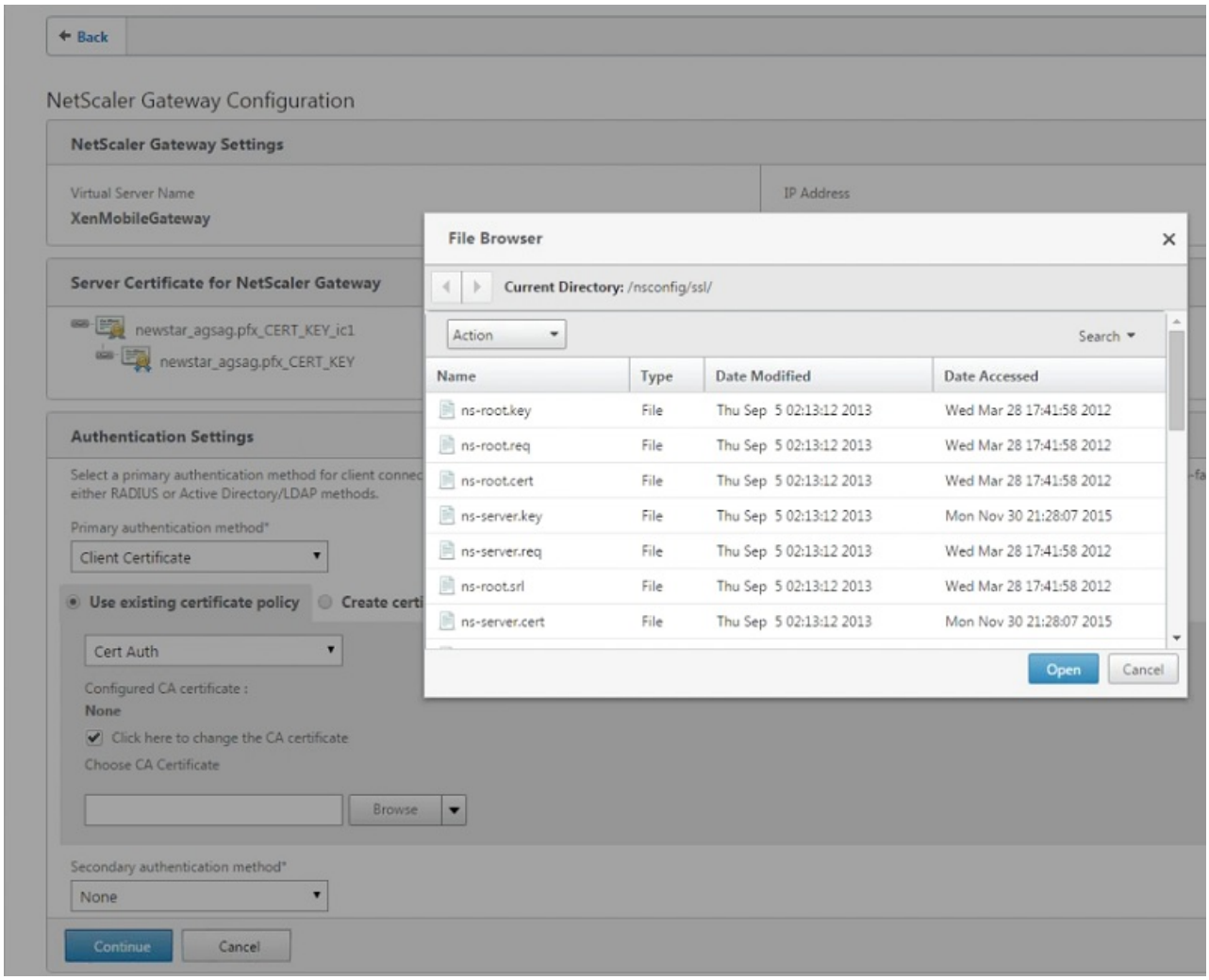
7. 既存の証明書を使用するか、証明書をインストールします。 **[続ける]** をクリックします。

   [認証設定] 画面が表示されます。

8. **[Primary authentication method]** フィールドで、 **[クライアント証明書]** を選択します。

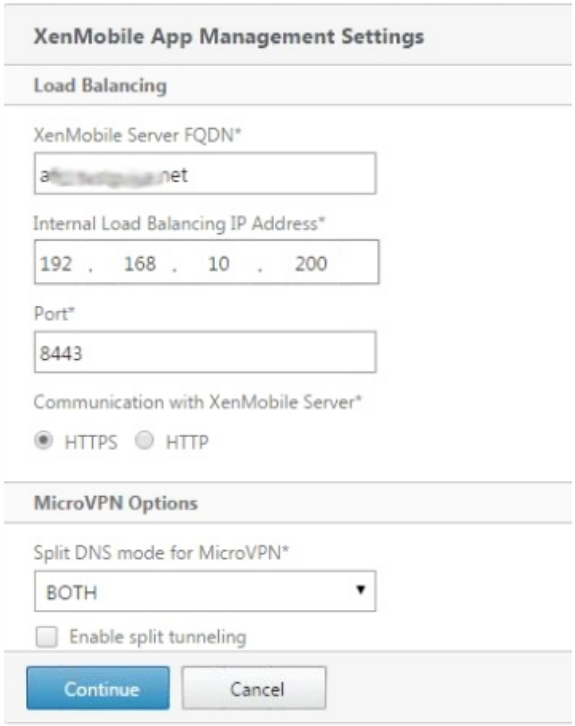
   これによって、次の2つのフィールドで自動的に **[Use existing certificate policy]** および **[Cert Auth]** を選択します。

9. **[Click here to change the CA certificate]** を選択してから、 **[参照]** 一覧から目的のCA証明書に移動します。



10. **[Second authentication method]** を **[なし]** のままにして、 **[続ける]** をクリックします。
11. **[負荷分散]** 画面で、XenMobileサーバーのFQDNとMAM-onlyの内部負荷分散IPアドレスを入力します。
12. これはSSLオフロード展開であるため、 **[Communication with XenMobile Server]** で **[HTTP]** を選択します。

    [Split DNS mode for MicroVPN] フィールドに、 **[両方]** が表示されます。
13. **[続ける]** をクリックします。



14. **[XenMobile Server Certificate]** 画面で、既存のサーバー証明書を選択するか、新しい証明書をインストールします。複数のXenMobileサーバーを実行している場合、各サーバーに証明書を追加します。 **[続ける]** をクリックします。

15. **[Device certificate]** 画面で、既にインストールされていない場合、この証明書をXenMobileコンソールからエクスポートする必要があります。 必要な操作：

    a. コンソールで、右上の歯車アイコンをクリックして、**[設定]** 画面を開きます。

    b. **[証明書]** をクリックして、一覧からCA証明書を選択します。

    c. **[Export]** をクリックします。

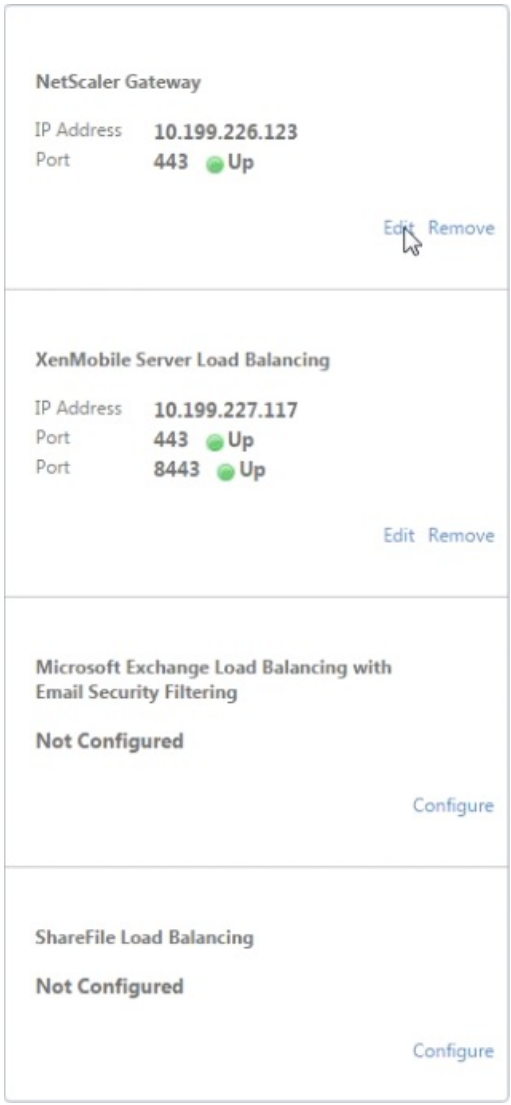
    d. NetScalerウィザードに戻って、インストールのためにエクスポート（ダウンロード）した証明書を選択します。

    e. **[続ける]** をクリックします。

既に構成したXenMobileサーバーのIPアドレスが表示されます。

16. **[続ける]** をクリックします。

    NetScalerダッシュボードで、NetScaler GatewayおよびXenMobileの負荷分散が構成されます。



デバイス登録の制限

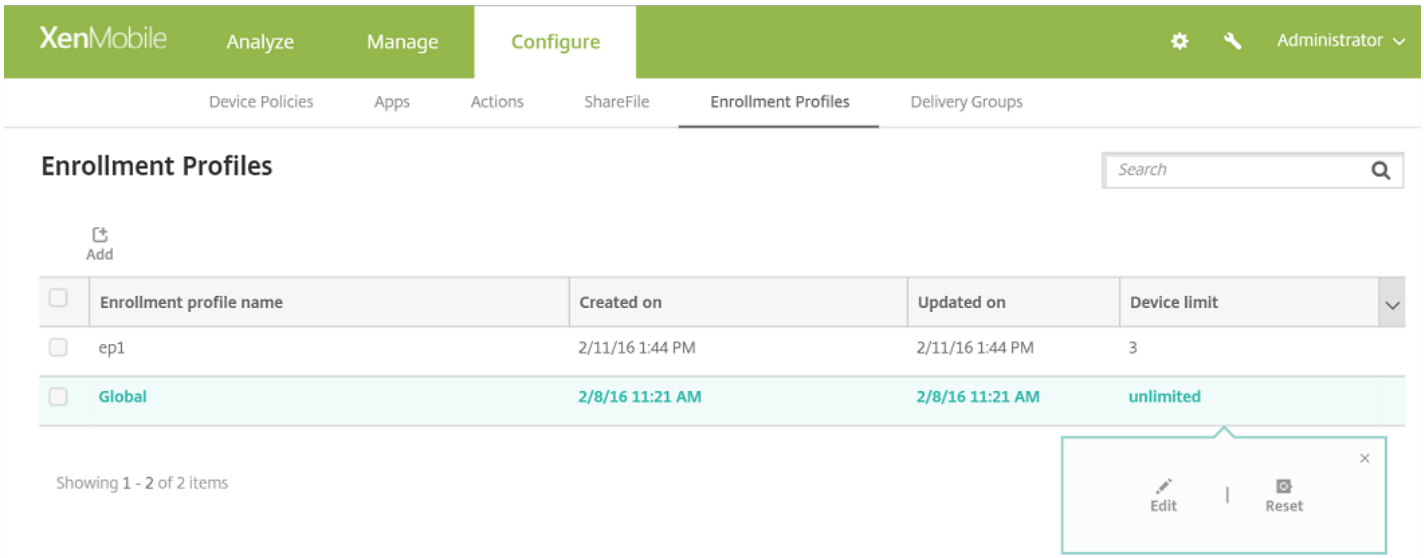
Aug 02, 2016

XenMobileコンソールのENT、MDM、MAMサーバーモードで、**[構成] > [登録プロファイル]** から、ユーザーが登録できるデバイスの数を制限できます。 制限はグローバルにまたはデリバリーグループごとに適用できます。 複数の登録プロファイルを作成して、異なるデリバリーグループに関連付けることができます。

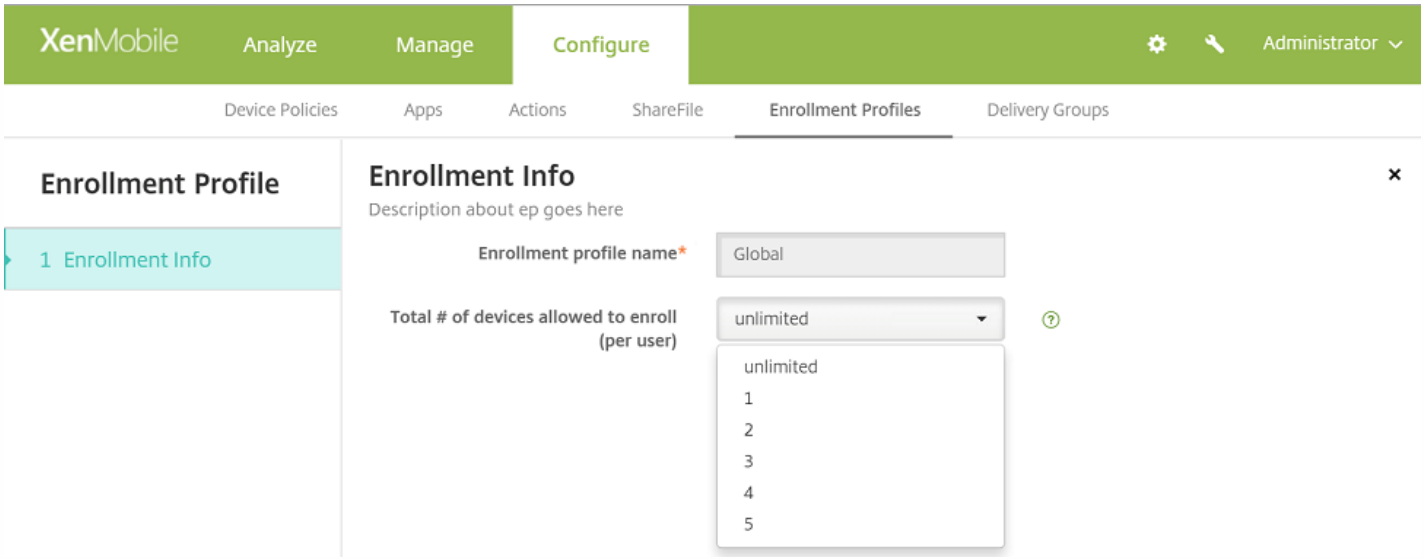
制限を設定しないと、ユーザーはデバイスをいくつでも登録できます。 この機能は、iOSおよびAndroidデバイスでのみサポートされます。 Windows デバイスの登録手順については、「 Windowsデバイス」を参照してください。

グローバルデバイス登録制限を構成するには

1. **[構成] > [登録プロファイル]** の順に移動します。
2. **[グローバル]** をクリックして、 **[編集]** を選択します。



[登録情報] 画面は、 **[グローバル]** を自動的にプロファイル名として表示します。 ここから、ユーザーが登録を許可された合計数のデバイスを選択します。 この制限は、すべてのXenMobile登録者に適用されます。

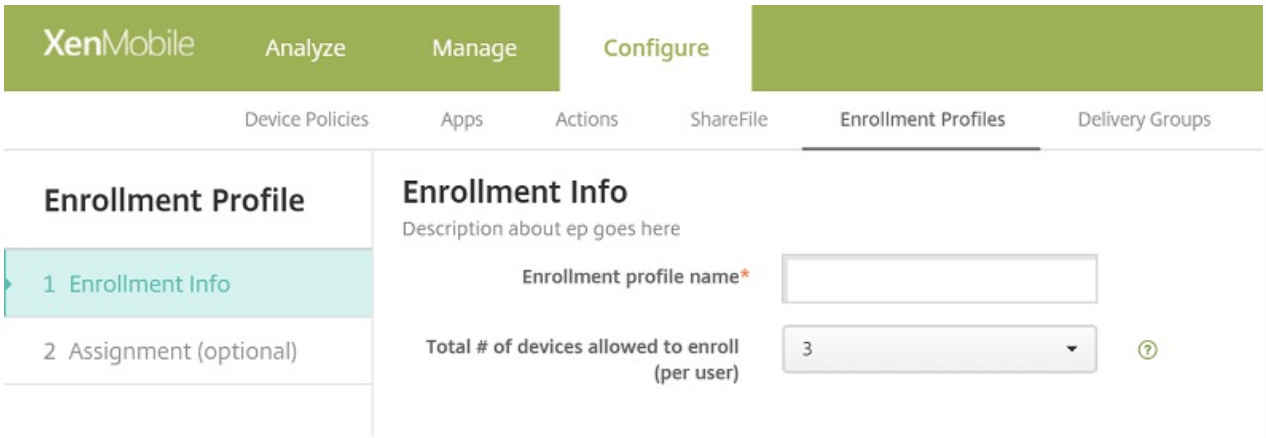


デリバリーグループのデバイス登録制限を構成するには

1. **[構成] > [登録プロファイル] > [追加]** の順に移動します。

   [登録情報] 画面が開きます。

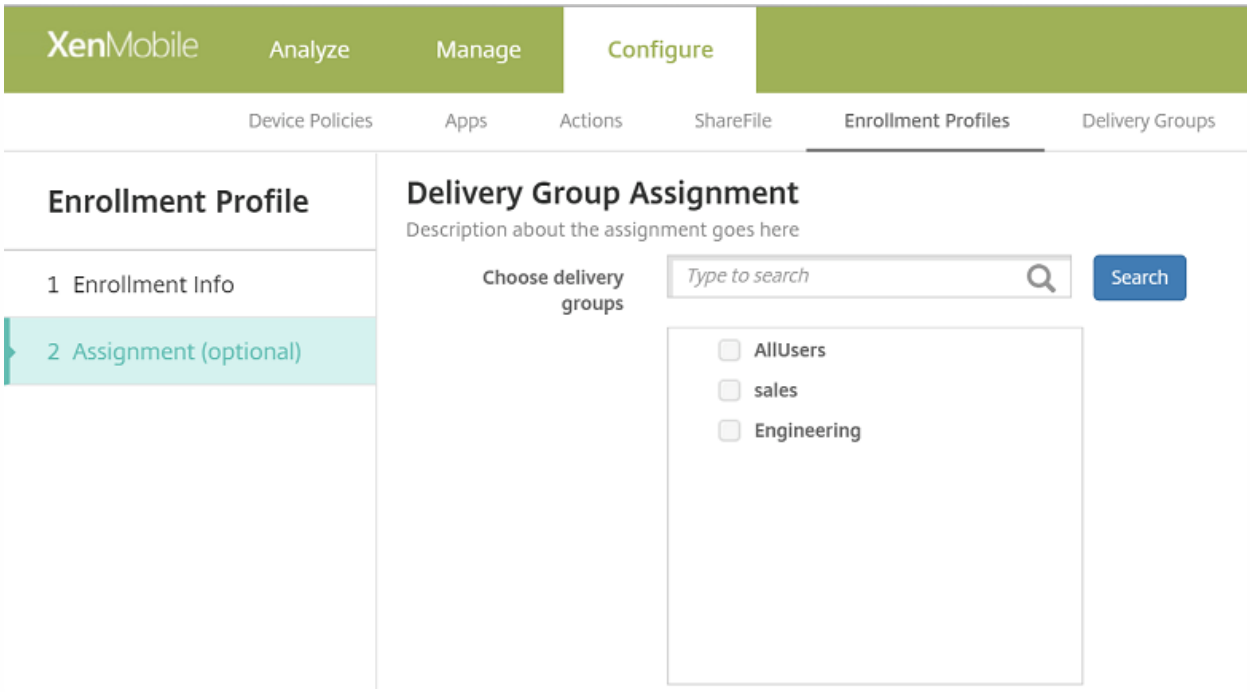
2. 新しい登録プロファイル名を入力してから、このプロファイルのメンバーに登録を許可するデバイスの数を選択します。



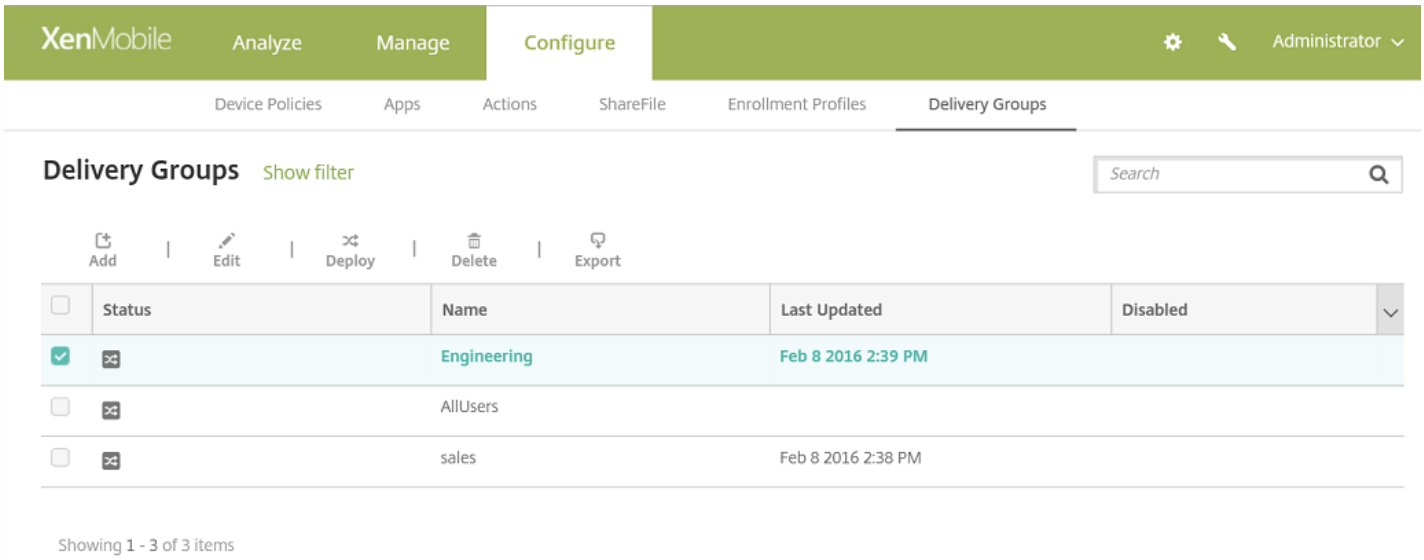
3. **[Next]** をクリックします。

   [デリバリーグループ割り当て] ページが開きます。

4. デバイス登録制限を適用するデリバリーグループを選択してから、**[保存]** をクリックします。

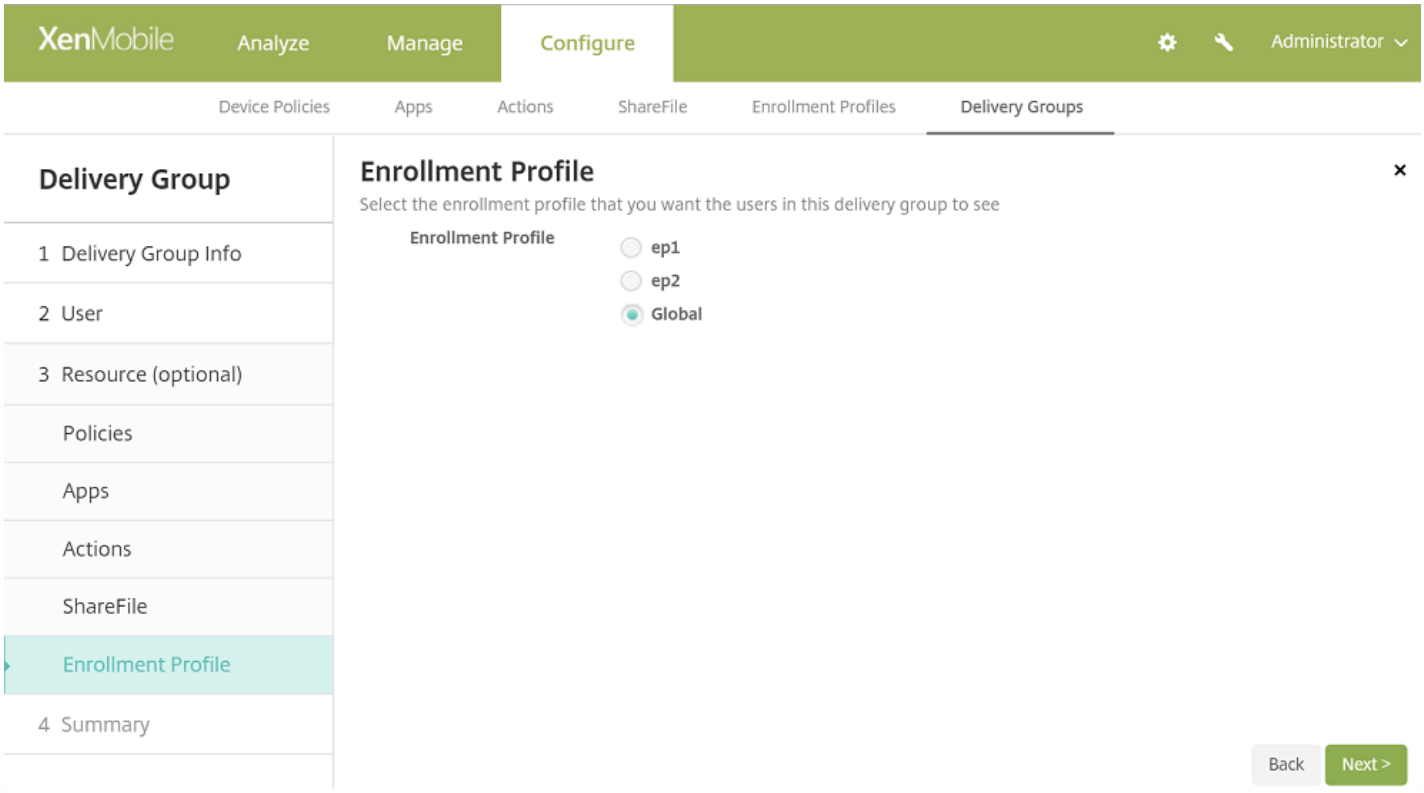


後からデリバリーグループの登録プロファイルを変更する必要がある場合は、**[構成] > [デリバリーグループ]** の順に移動します。 目的のグループを選択して、 **[編集]** クリックします。



[登録プロファイル] 画面が開きます。

5. この画面から、このデリバリーグループに適用する登録プロファイルを選択してから、**[次へ]** をクリックして変更を表示し、保存します。



デバイス登録制限のユーザーエクスペリエンス

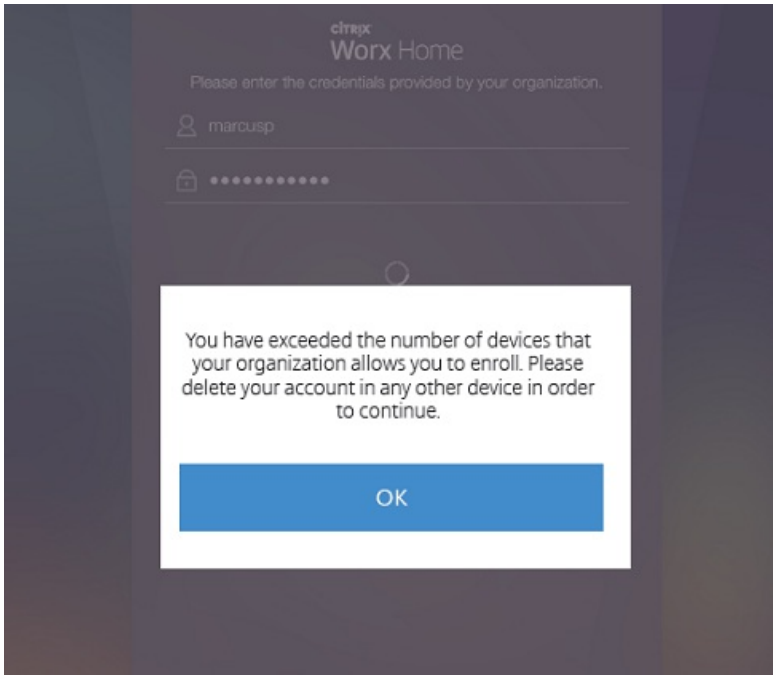
デバイス登録制限を設定してユーザーが新しいデバイスを登録する場合、以下の手順に従います。

1. Worx Homeにサインオンします。

2. 登録するサーバーアドレスを入力します。

3. 資格情報を入力します。

4. デバイス制限に達した場合、エラーメッセージが表示され、ユーザーにデバイス登録数を超過したため、管理者に問い合わせるように伝えます。



Worx Home登録画面が再度表示されます。

MAM-Onlyモード用のアプリロックとアプリワイプ操作

Aug 30, 2016

アクションを作成することによって、ユーザーのデバイスで特定のトリガー（未許可のアプリケーションのインストールやActive Directoryからのユーザーの削除など）に対する自動応答を設定します。 より深刻なアクションが必要と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。

XenMobile 10.3.5で開始すると、XenMobileにリストされたトリガーの4つのカテゴリすべてに応じて、デバイスでアプリケーションをワイプまたはロックします。4つのカテゴリは、ベント、デバイスプロパティ、ユーザープロパティ、インストールされたアプリケーション名です。 以前のバージョンでは、イベントカテゴリのみにこの機能がありました。

自動でアプリのワイプまたはロックを構成するには

1. XenMobileコンソールで、**[構成]の[アクション]**をクリックします。

2. **[アクション]**ページで、**[追加]**をクリックします。

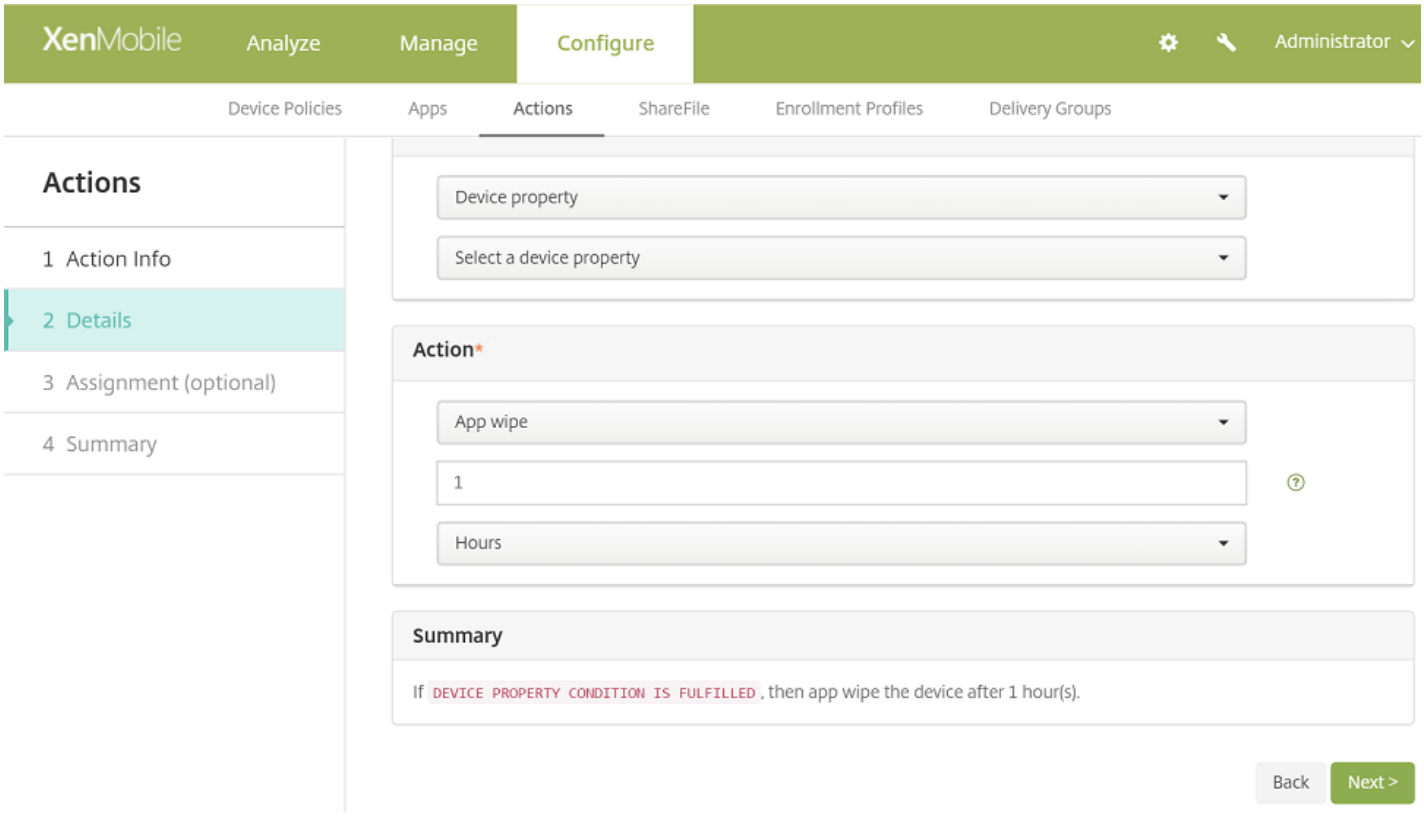
3. **[アクション情報]**ページで、アクションの名前および必要に応じて説明を入力します。

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、**[アプリのワイプ]**または**[アプリのロック]**のどちらかを選択します。

各オプションでは、自動で1時間の遅延が設定されていますが、遅延の期間は分単位、時間単位、日数単位を選択できます。遅延によって、ユーザーはアクションを実行する前に、修正のための時間を確保できます（修正が可能な場合）。 アプリのワイプとアプリのロックについて詳しくは、「RBACの役割とアクセス権」のトピックを参照してください。

> **注意**
>
> Active Directoryデータベースと XenMobileとの同期を許可するアクションが実行される前に、さらに約1時間、遅延を追加できます。



6. 展開規則を構成して、 **[次へ]** をクリックします。

7. デリバリーグループの割り当てと展開スケジュールを構成して、**[次へ]** をクリックします。

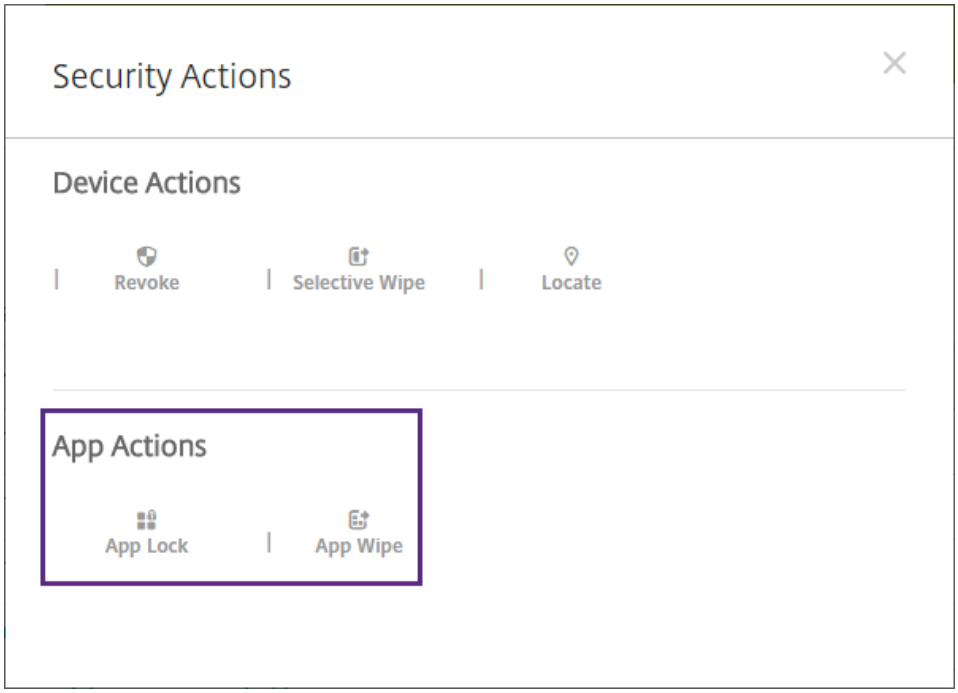
8. **[Save]** をクリックします。

アプリのロック、ロック解除、ワイプ、ワイプ解除を実行するには

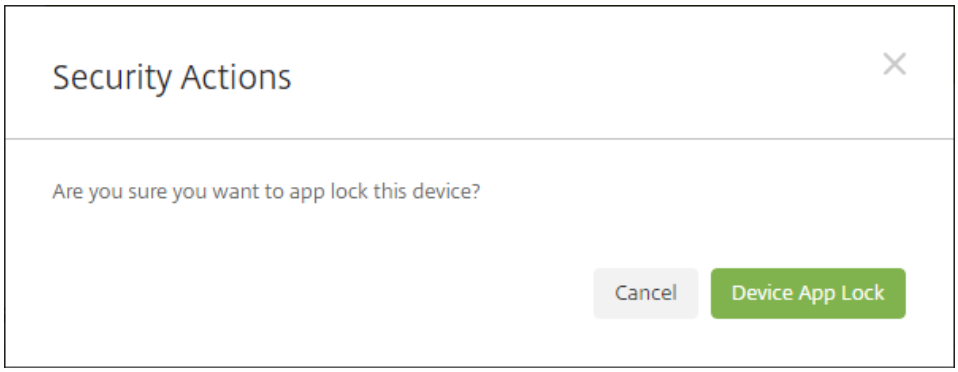
1. **[Manage] > [Devices]** に移動し、デバイスを選択して **[Secure]** をクリックします。

2. **[Security Actions]** ダイアログボックスで、アクションをクリックします。

   注：このダイアログボックスは、 無効になっているか、Active Directoryから削除されているユーザーのデバイスの状態を確認するために使用することもできます。 アプリロック解除またはアプリワイプ解除アクションが存在する場合、ユーザーのアプリが現在ロックまたはワイプされていることを意味します。

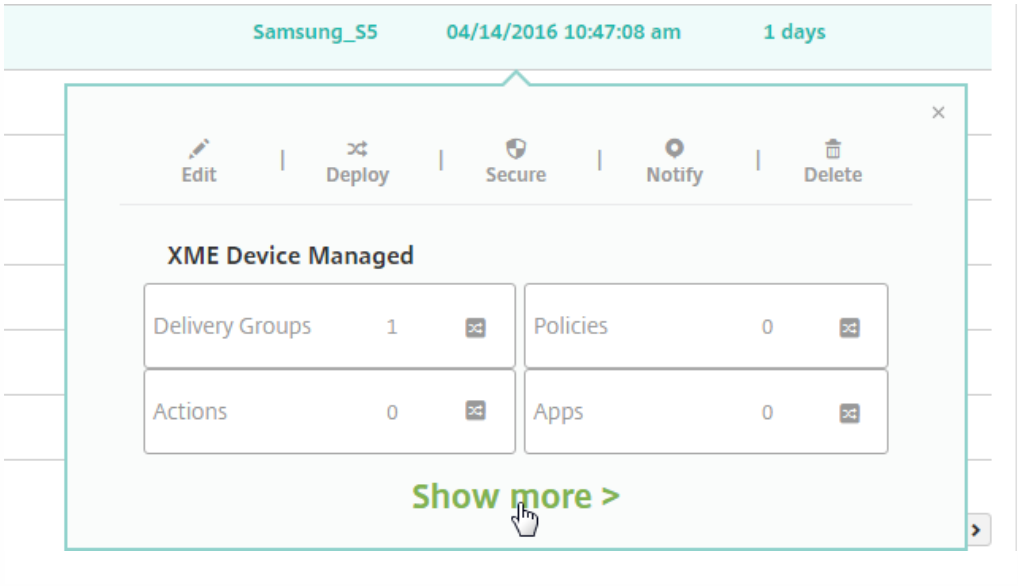


3. アクションを確認します。

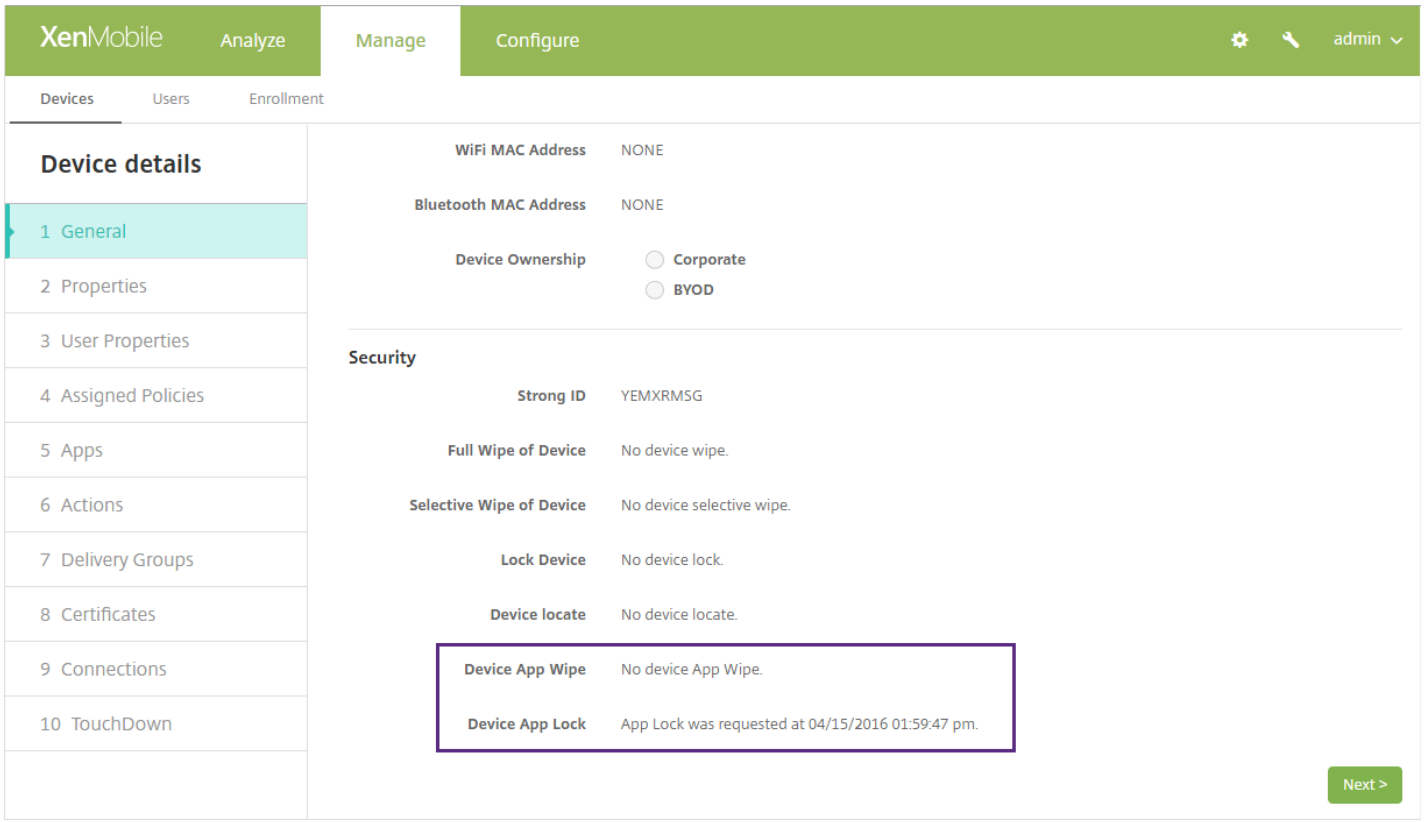


アプリロックとアプリワイプの状態を確認するには

1. **[Manage] > [Devices]** に移動し、デバイスをクリックしてから **[Show more]** をクリックします。



2. [**Device App Wipe**] および [**Device App Lock**] までスクロールします。



MAM-Onlyモード用のRESTサービスAPI

Aug 02, 2016

MAM-onlyデバイスでは、任意のRESTクライアントとXenMobile REST APIを使用して、XenMobileコンソールから公開されているRESTサービスを呼び出します。 APIについて、このセクションで説明しているサービスを呼び出すためにXenMobileコンソールにサインオンする必要はありません。

RESTクライアントを使用して、REST APIサービスを呼び出すことができます。

新しいREST APIは、以下を可能にします。

- **招待URLとワンタイムPINを送信する**

  XenMobile REST APIを使用して、ユーザーがセルフサービスポータルからBYODへのアクセスを要求できるようにします。 承認されると、システムはXenMobileサーバーを呼び出し、次のことを可能にする要求を発行します。

  - 登録招待状URLを作成し、ユーザーに送信する。

  - ワンタイムPINを作成し、ユーザーに送信する。

  注：この機能は、 iOSデバイスとAndroidデバイスでサポートされていますが、Windowsデバイスではサポートされていません。

- **デバイス一覧でアプリのロックとアプリのワイプを発行する**

  XenMobile APIを使用して、すべてのデバイスからユーザーのデバイスを検索して、デバイスのすべてのアプリをワイプする、アプリをロックするなどの操作ができます。

この記事の残りの部分は、XenMobile 10.3.5で使用できるデバイスAPIおよびワンタイムPIN登録用APIの一覧です。 現在使用できるAPIの完全な一覧については、 XenMobile REST APIリファレンスのPDFファイルをダウンロードしてください。

デバイスAPIsにキャッシュする

- Get Devices by Filters
- Get Device Information by ID
- Get Device applications by device ID
- Get Device actions by device ID
- Get Device delivery groups by device ID
- Get Device managed software inventory by device ID
- Get Device policies by device ID
- Get Device software inventory by device ID
- Get Device GPS Coordinates by device ID
- Send notification to a list of devices/users
- Authorize a list of devices
- Activation lock bypass on a list of devices
- App lock on a list of devices
- App wipe on a list of devices
- Container lock on a list of devices

- Cancel container lock on a list of devices
- Container unlock on a list of devices
- Cancel container unlock on a list of devices
- Reset container password on a list of devices
- Cancel reset container password a list of devices
- Disown a list of devices
- Locate a list of devices
- Cancel locating a list of devices
- GPS tracking a list of devices
- Cancel GPS tracking a list of devices
- Lock a list of devices
- Cancel locking a list of devices
- Unlock a list of devices
- Cancel unlocking a list of devices
- Deploy a list of devices
- Request an Airplay mirroring on a list of devices
- Cancel request for Airplay mirroring a list of devices
- Stop Airplay mirroring on a list of devices
- Cancel stop Airplay mirroring on a list of devices
- Clear the restrictions on a list of devices
- Cancel clear the restrictions on a list of devices
- Revoke a list of devices
- Make ring a list of devices
- Cancel ring on list of devices
- Wipe a list of devices
- Cancel wipe on list of devices
- Selective wipe a list of devices
- Cancel selective wipe on list of devices
- SD card wipe on a list of devices
- Cancel SD card wipe on list of devices
- Get all device known properties
- Get all device used properties
- Retrieve all device properties by device ID
- Update all device properties in bulk by device ID.
- Add or Update a device property by device ID
- Delete a device property by device ID
- Retrieve iOS MDM Status of device by device ID
- Generate pin code

ワンタイムPIN登録API

- Get Enrollment Modes
- Get Enrollment Information
- Trigger Enrollment Notification
- Create Enrollment Invitation
- Get Enrollment Records by Filter

XenMobile 10.3.5の既知の問題および解決された問題

Aug 30, 2016

XenMobile 10.3.5の既知の問題および解決された問題は次のとおりです。

既知の問題

- 制限事項：新しいMAM-onlyモードの機能（証明書ベースの認証、アプリロックおよびアプリワイプ操作、およびMAM-only API）は、Windows Phone では利用できません。
- ユーザーがWorx Homeに複数回再登録を行い、WorxStoreからアプリをインストールしようとすると、アプリが削除されたことを示すエラーが表示されます。 この問題を回避するには、XenMobileコンソールで［**Manage**］>［**Devices**］の順にクリックし、ユーザーの再登録を要求します。 [#611172]
- Windowsデバイスの登録には、SSLリスナー証明書が公開証明書である必要があります。 自己署名SSL証明書をアップロード済みの場合、登録は失敗します。 [#618390]
- デバイスの登録がXenMobileコンソールで設定された制限に達すると、デバイスにエラーメッセージは表示されませんが、ユーザーは登録できません。 [#623475]
- ユーザーがAzure Active DirectoryアカウントでXenMobileに登録すると、デバイスをワイプまたは失効しても、認証なしに再度登録できます。 これはサードパーティ製品の問題です。 [#628865]
- iOSデバイスをXenMobileコンソールから削除した後、ユーザーがデバイスをXenMobileエンタープライズモード（MAMおよびMDM）で再登録しようとすると、MAMモードの登録が失敗することがあります。 [#629021]
- XenMobileサーバーで証明書を更新するオプションを無効にすると、ユーザーはWorx Homeで期限切れの証明書を更新できます。 [#630894]
- マイナスのID（例：-123441212）を持つVPPライセンスが存在し、その場合、パブリックアプリケーションを配布できません。 [#631443]
- Google Playの資格情報が無効なデバイス IDで設定されている場合、Google Playのパブリックアプリケーションストアのアプリケーションを追加してからGoogle Play ストアでこのアプリケーション名を検索すると、検索が失敗するか、正しくない検索結果が表示されます。 [#633845]
- 現時点では、XenMobileの［**Settings**］>［**Google Play Credentials**］ページの記載に従って電話に「*#*#8255#*#*」と入力しても、Android IDを見つけることはできません。 デバイスIDの検索には、Google Playストアのデバイスアプリを使用してください。 [#633854]
- XenMobileコンソールで［**Settings**］、［**Role Based Access Control**］の順に選択すると、デフォルト設定に関連して次の問題が発生します。
  - Cloud環境のXenMobileコンソールで、［**共有デバイスの登録機能**］権限がデフォルトでAdminの役割に設定されます。 この権限はデフォルトで設定されるべきではありません。 [#638069]
  - コンソールの機能権限［**デバイスの放棄**］は廃止され、表示されるべきではありません。 [#638303]
  - オンプレミス環境のXenMobileで、Adminの役割にデフォルトで次の機能が選択されていません。 これらの設定は、デフォルトのAdminの役割やAdminテンプレートから作成されたその他の役割に必要なため、選択する必要があります。 [#638314]

    コンテナーのロック
    コンテナーのロック解除
    コンテナーのパスワードのリセット
    アクティベーションロックのバイパス
    デバイスの警報

- オンプレミスおよびCloud環境のXenMobileコンソールで、Adminの役割にデフォルトで次の機能が選択されていません。 これらの設定は、デフォルトのAdminの役割やAdminテンプレートから作成されたその他の役割に必要なため、選択

する必要があります。 [#638322]

AirPlayミラーリングの要求
AirPlayミラーリングの停止

解決された問題

- ShareFile SSO認証は、XenMobileとHyper-Vの間で発生する時刻同期の問題で失敗します。 [#588249]
- XenMobile LDAP設定で入れ子構造を有効にして、関連するドメイングループでデリバリーグループと役割ベースのアクセス制御（RBAC）設定を構成すると、後からLDAP設定でドメインを削除した際に、入れ子になったグループ情報がデータベースに残ります。 [#590363]
- ユーザーをActive Directoryから削除しても、該当ユーザーがWorxStoreを開き、アプリにサブスクライブできます。 [#592825]
- XenMobileコンソールで、パブリックアプリケーションストアのアプリケーションの更新をチェックすると、Worx Homeはパブリックアプリケーションストアのアプリケーションを最新のバージョンに更新しますが、デバイスの保留中の更新リストにアプリケーションが表示されたままになります。 [#593034]
- ユーザーがWorxMailのExchangeアカウントで予定表の招待を受信するとき、招待状が通常より遅れて届きます。 [#594542]
- iOSデバイスをDevice Enrollment Program（DEP）に登録すると、Worx HomeがiOSデバイスにダウンロードされないことがあります。 [#595822]
- NTPクライアントを構成しないと、ShareFileのSAMLシングルサインオン（SSO）エラーのような、時刻のずれの問題がXenMobileサーバーで発生する可能性があります。

  注：解決策を有効にするには、次の手順に従って構成します。

  1. XenMobileをインストールしたハイパーバイザー（Citrix XenServerまたは VMware ESXi）で、以下のコマンドラインインターフェイス（CLI）にログオンします。

  2. **[2] System**に移動します。

  3. **[3] Set NTP Server**に移動して、NTPサーバーの詳細を入力します。

  4. サーバーを再起動します。

  重要：システムがクラスターモードで構成されている場合、上記の手順に従って各ノードを構成します。 [#597757]

- ユーザーがアプリケーションまたはWebリンクをWorx Homeから削除しようとすると、次のエラーが表示されます。「Worx Homeで接続できません。」 [#599934]
- 複数のPINがユーザーの保留状態にあるとPIN-basedサーバーが応答不能になることがあります。 [#600264]
- VPPライセンスをXenMobileにインポートすると、ライセンスがAppleから払い戻された場合、そのライセンスがXenMobileで有効と判断されないことがあります。 その結果、iOSデバイスにWorxStoreからアプリケーションをインストールできなくなります。 [#601845]
- 操作を作成した後、デバイスポリシーやアプリケーションに使用されているものと同じ名前で操作の名前を変更すると、後から操作を削除できなくなります。 [#602958]
- Samsung Galaxy Note 5を使用してWorxStoreにアクセスすると、通常のフォーンビューではなくタブレットビューでWorx Store画面の一部が表示されます。 [#604295]
- Active Directoryグループの第1レベルから受信者にワンタイムPINを必要とする登録招待状を作成すると、入れ子状態のグループは招待状を受信しますが、登録は、入れ子の第3レベルのグループで失敗します。 この問題は、第3レベルのグループに直接招待状を送信した場合にも発生します。 [#603434]
- Advancedライセンスタイプで、XenMobileコンソールの ［Enrollment required］ チェックボックスを選択すると、ユー

ザーはMAM-onlyモードで登録してWorxStoreにアクセスできます。 [#604113]

- プロパティ**$user.dnsroot**と**$user.netbiosename**はマクロで使用され、ユーザープロパティを使ってポリシーを展開します。 **dnsroot**および**netbiosename**ユーザープロパティはXenMobile 10.1で廃止されました。 この修正によって、XenMobile 10.3で再度これらのプロパティが有効になります。 [#604240]
- XenMobileでiOSデバイス登録プログラムを構成しようとすると、無効なプロファイルエラーが発生します。 これはサードパーティ製品の問題です。 [#607143]
- XenMobileコンソールのクライアントのブランド設定で、ストア名には英数字（ASCII）のみ使用できます。デフォルトを非ASCII文字に変更すると、ユーザーはWorx Homeにサインインできなくなります。 [#609535]
- LDAPをユーザーやグループによって異なる基本識別名で構成すると、XenMobile 10.3に更新した後、デリバリーグループに新しいグループを追加できません。 [#610014]
- WiFiデバイスポリシーを構成するとき、展開スケジュールが **[以前の展開が失敗した場合のみ]** に設定されていても、デバイスが接続されると毎回デバイスにWiFiポリシーがプッシュされます。 [#610325]
- この修正は、Apache Commons Collectionsでオブジェクトの逆シリアル化の際のJavaゼロデイ脆弱性に対応します。 [#610427]
- ユーザーにXenMobileコンソールへのサインインを許可するRBACロールを設定する際、ユーザー名にsAMAccountName形式を使用すると、Self Help Portalにリダイレクトされます。 [#610915]
- 初めてXenMobile 10.1をインストールした後、またはXenMobile 9のMAMおよびMDMモードからXenMobile 10.1にアップグレードした後、 **[管理]** > **[デバイス]** のXenMobileコンソールでデリバリーグループとポリシーを更新すると、情報が異なるため、デリバリーグループやポリシーが誤った数になります。 [#611630]
- XenMobile 10.1より前のバージョンのXenMobileで構成されたLDAPドメインが10以上ある場合、XenMobile 10で、また XenMobile 10.1にアップグレードした後、XenMobileコンソールには10ドメインしか表示されません。 [#613502]
- ユーザーにパブリックアプリケーションの権限などを含めたRBACロールを設定していない場合、MDXアプリケーションを追加または更新できません。 [#614496]
- 初回のXenMobileの構成時にデフォルトのインスタンス名を変更すると、バージョン10.3にアップグレードしたとき、変更は保持されません。 その結果、登録されたデバイスが接続できなくなります。 [#614604]
- LDAPをロックアウト制限で構成すると、XenMobile 10.3にアップグレードした後、同じドメインの新しいユーザーが不正な資格情報（パスワードの入力間違いなど）でデバイスをWorx Homeに登録すると、Worx Homeが応答を停止して、SQLサーバーが失敗します。 [#615179]
- XenMobile 10.1からXenMobile 10.3への更新後、 **[招待の追加]** オプション を使用してユーザーに登録招待状を送信することができません。 [#616584]
- この修正では、1つのフォレストでLDAPマルチドメインルートのサポートを有効にします。 このサポートは、XenMobileで使用できます。XenMobile 10.xでは使用できません。 [#616633、#618899、#620541]
- XenMobileでiOS制限デバイスポリシーを構成して、 **[ユーザーにポリシーの削除を許可]** オプションのデフォルト値を変更すると、値は保存されません。 [#616751]
- サーバーにカスタムのインスタンス名があり、XenMobile 10.1からXenMobile 10.3に更新すると、ユーザーがデバイスを登録できません。 [#616954]
- ユーザーがXenMobileのEnterpriseモードでDEPデバイスを登録するとき、デバイスを工場出荷時の設定にリセットして（フルワイプ）、デバイスを再登録すると、Worx Homeは通常通りにデバイスに自動的に展開されません。 [#616986]
- XenMobileサーバーが約20分から30分経過してからリカバリモードになることがあります。これは、既知のJava Runtime Environment（JRE）の問題です。 サーバーの再起動後、この問題が再度発生します。 [#616992]
- iOSおよびAndroidデバイスの場合、 **[Settings]** > **[Client Branding]** で **[Store name]** を削除すると、Worx HomeからWorxStoreを開くことができません。 [#617003]
- .ipaファイルをXenMobileコンソールにアップロードすると、「no icon found（アイコンが見つかりません）」というエラーメッセージが表示されます。 [#617195]
- VPNデバイスポリシーを［アプリごとの VPN を有効化］および［オンデマンド マッチ アプリが有効］オプションを**[オン]** にして展開し、管理されているアプリケーションのアプリ属性ポリシーにVPNポリシーを適用すると、ユーザーが管理されているアプリケーションを開くとき、次の問題が発生します：VPN接続が通常通りに自動的に開始されません。 ユー

ザーは **[オンデマンドで接続]** 設定をデバイスで手動で有効にする必要があります。 [#617803]

- XenMobileコンソールの **[管理]** > **[ユーザー]** で、既存のユーザーの表示に遅延が発生します。 その結果、ローカルユーザーの操作を実行できません。 [#618094]
- XenMobile 10.xは、1つのActive DirectoryフォレストのLADPマルチドメインをサポートします。 [#618375]
- 登録招待状を送信して、HTMLコードを入力すると、ユーザーはHTMLリンクのないテキスト形式のメールを受信します。 [#618504]
- ユーザーが .appxファイルをWindows 10デバイス用のエンタープライズアプリケーションとしてアップロードすると、アプリケーションはデバイスに展開されません。 [#628611]
- ユーザーIDまたはパスワードの入力フィールドに特殊文字があると、ユーザーは、Windows 10デバイスをMDMモードのXenMobileに登録できません。 [#618870]
- iPadの場合、XenMobile 10.3では常に、XenMobileコンソールで設定した順序に関係なく最初に削除処理が行われます。 [#620459]
- XenMobileコンソールで既存のiOSエンタープライズアプリケーションを更新した際、.ipaファイルのバンドルIDが異なる場合、更新されたアプリケーションをデバイスに展開すると、デバイス上のアプリケーションの展開で問題が発生します。 [#621009]
- XenMobileサーバーでGoogle Play資格情報を追加するときに、エラー「無効なデバイス ID」が表示され、ログオンできません。 [#623182]
- XenMobileでVPPを使用してインポートしたアプリケーションを削除すると、トークンを削除して再度追加するまで、アプリケーションは自動的に再インポートされません。 [#623403]
- デバイスを削除するかワイプしても、このデバイスに関連付けられたVPPライセンスは自動的に解除されません。 その結果、別のデバイスでライセンスを使用するためには、手動でライセンスの関連付けを外す必要があります。 [#623716]

XenMobile Server 10.3について

Oct 25, 2016

XenMobileコンソールで、XenMobile 10.1からXenMobile 10.3へのアップグレードが行えます。 アップグレードを行うには、xms_10.3.0.824.binを使用します。 XenMobileコンソールで、右上の歯車アイコンをクリックした後、 **[Release Management]** をクリックします。 **[アップグレード]** をクリックしてから、 xms_10.3.0.824.binファイルをアップロードします。 コンソールでのアップグレードについて詳しくは、「XenMobileのアップグレード」を参照してください。

XenMobile 10.3を新たにインストールする場合は、「XenMobileのインストール」を参照してください。

> **注意**
>
> Remote Support Clientは、XenMobile Cloud Version 10.xのWindows CEおよびSamsung Androidデバイスでは利用できません。

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

XenMobile 10.3の新機能

XenMobile 10.3では、以下の新しい機能が追加されました。

一新されたコンソールの外観

XenMobile 10.3では、外観が一新されています。 コンソールは、色、フォント、タブが変わっただけでなく、機能も強化されています。

- コンソールの以前のバージョンの［Dashboard］タブは、新たに追加された［Analyze］タブの下に移動されました。 ［Analyze］タブには、新たに追加された［Reporting］タブも含まれています。 詳しくは、「レポート」を参照してください。
- ［Manage］タブに、ローカルユーザーおよびグループの管理を行う［Users］タブが新たに追加されました。
- ［Configure］タブに、ShareFileアカウントへの接続設定を構成する［ShareFile］タブが新たに追加されました。
- 以前は［Configure］タブの下にあった［Settings］には、コンソールの右上に表示される歯車アイコンをクリックしてアクセスするようになりました。
- ［Support］タブは、新しいタブとしてではなく、コンソールと同じタブに表示されるようになりました。

新しいプラットフォームのサポート

XenMobile 10.3では次のプラットフォームをサポートするようになりました。

- Mac OS X
- Android HTC
- Android Sony
- Samsung SEAMS
- Windows Mobile/CE
- Windows 10 Phone：XenMobile MDMモードとEnterpriseモードでのデバイス管理
- Windows 10デスクトップ/タブレット：XenMobile MDMモードとEnterpriseモードでのデバイス管理

Mac OS Xデバイスの登録手順については、「Mac OS Xデバイス」を参照してください。

Windows 10デバイスの登録手順については、「Windowsデバイス」を参照してください。

> **注意**
>
> XenMobile 10.3では、Symbianデバイスのサポートは廃止されました。

デバイスポリシー

XenMobile 10.3では、以下の新しいMDMポリシーを使用できます。

- **アプリケーションロック**： デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行をブロックするアプリの一覧を定義できます。 iOSおよびAndroidで使用できます。 デバイスポリシーは大部分のAndroid LおよびMデバイスで機能しますが、アプリのロックは、必要なAPIがGoogleによって廃止されたため、Android N以降のデバイスでは機能しません。
- **アプリケーションネットワーク使用状況**： ネットワーク使用状況規則を設定して、携帯データネットワークなどのネットワークを管理対象アプリケーションがどのように使用するのかを指定できます。 規則は管理対象のアプリケーションにのみ適用されます。 iOSで使用できます。
- **接続マネージャー**： インターネットまたはプライベートネットワークとアプリケーションの接続方法を構成します。 これらの設定は、Pocket PC（タッチスクリーンデバイス）でのみ機能します。 Windows Mobile/CEで使用できます。
- **Samsungコンテナーへのアプリケーションのコピー**: Samsungデバイスのアプリケーション向けに、SEAMSまたはKNOXコンテナーを作成できます。 Samsung SEAMSまたはSamsung KNOXで使用できます。
- **ファイルおよびフォルダーの削除**: 削除する必要があるファイルおよびフォルダーを指定できます。 Windows Mobile/CEで使用できます。
- **デバイス正常性構成証明**： Windows10のセキュリティおよびデータ損失防止（DLP）機能であるデバイス正常性構成証明を有効にし、Windows 10デバイスの状態を見極め、必要に応じてコンプライアンスアクションを実行できるようにします。 ペイロードは、Windows 10以降の監視対象デバイスでのみサポートされます。 Windows PhoneおよびWindowsタブレットで使用できます。
- **デバイス名**： デバイスを特定しやすくするために、iOSデバイスおよびMac OS Xデバイスに名前を設定できます。 デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。
- **レジストリ キーと値の削除**: 削除する必要があるレジストリキーおよび値を指定できます。 空の値は、エントリがレジストリキーであることを意味します。 Windows Mobile/CEで使用できます。
- **エンタープライズデータ保護**：エンタープライズデータ保護（EDP）を必要とするアプリケーションを、必要な適用レベルで指定できます。 このポリシーは、Windows PhoneおよびWindowsタブレットに適用されます。
- **iOSおよびMac OS Xプロファイルのインポート**: XenMobile 10.3では、このポリシーをMac OS X用に構成するオプションが追加されました。 このポリシーによって、iOSまたはMac OS Xのいずれかにデバイス構成XMLファイルをインポートできます。 XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。
- **レジストリ**： Windows Mobile/CEのレジストリには、アプリケーション、ドライバー、ユーザー設定、および構成設定に関するデータが格納されています。 Windows Mobile/CEデバイスの管理に使用するレジストリキーおよび値を定義できます。
- **壁紙**： .pngファイルまたは.jpgファイル追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。 iOS 7.1.2以降で使用できます。 iPadおよびiPhoneで異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。
- **Windows CE証明書**： 外部PKIから証明書を作成してデバイスに配布できます。

新規および既存のすべてのデバイスのプラットフォーム別マトリックスについては、「プラットフォーム別のXenMobileデバイスポリシー」を参照してください。

各プラットフォームの新機能および機能拡張の概要

iOS

- **新規デバイスポリシー**。 アプリケーションネットワーク使用状況、デバイス名、壁紙
- **管理対象から非管理対象へのアプリの割り当て**。 管理対象から非管理対象にアプリケーションを割り当てるためのiOS 9.0オプション： XenMobileコンソールでiOS用のパブリックアプリケーションストアのアプリケーションの設定を追加および構成する場合に、 **[Force app to be managed]** オプションを構成することができます。 このオプションは、デフォルトでは **[OFF]** に設定されます。 **[ON]** を選択した場合、アプリケーションが非管理対象としてインストールされたときに、ユーザーは監視対象ではないデバイスでのアプリケーションの管理を許可するように求められます。 詳しくは、「XenMobileへのパブリックアプリケーションストアのアプリケーションの追加」を参照してください。
- **新しい制限とApple Configurator 1.7.2ポリシーのオプション**。 詳しくは、「制限デバイスポリシー」を参照してください。
- **RequestMirroringコマンドおよびStopMirroringコマンドのサポート**。 詳しくは、「XenMobile REST APIリファレンス」を参照してください。
- **DEPデバイスセットアップアシスタントの拡張機能**。 詳しくは、「iOSデバイスの一括登録」を参照してください。
- **VPN OnDemandRulesキー**。 詳しくは、「VPNデバイスポリシー」を参照してください。

Android

- **Samsung KNOXコンテナーの構成**。 詳しくは、「Samsungコンテナーへのアプリケーションのコピーデバイスポリシー」を参照してください。
- **Samsung SAFE API**。 詳しくは、「XenMobile REST APIリファレンス」を参照してください。
- **Samsung AndroidデバイスのELMキー**。
- **アプリケーションロックデバイスポリシー**。 詳しくは、「アプリケーションロックデバイスポリシー」を参照してください。

Windows CE

- **資格情報プロバイダーの構成**。 詳しくは、「資格情報デバイスポリシー」を参照してください。
- **Windows CE証明書の構成**。 詳しくは、「Windows CE証明書デバイスポリシー」を参照してください。
- **レジストリ保持デバイスポリシー**詳しくは、「レジストリデバイスポリシー」を参照してください。
- **SMS受信時接続/通話時接続機能**。
- **その他の新規デバイスポリシー**: 接続マネージャー、ファイルおよびフォルダーの削除、レジストリキーおよび値の削除

Windows Phone 10およびWindowsタブレット10

- 新規デバイスポリシー：エンタープライズデータ保護、デバイス正常性構成証明
- Windows PhoneおよびWindowsタブレット用の新規デバイスポリシーオプション：

  アプリケーションインベントリ
  資格情報
  カスタムXML
  パスコード
  制限事項
  契約条件
  VPN
  WiFI

- Windowsタブレット用の新規デバイスポリシーオプション：

アプリケーションのアンインストール
サイドローディングキー
証明書署名
［Webclip
WorxStore

- Windows Phone用の新規デバイスポリシーオプション：

  エンタープライズハブ
  ストレージ暗号化

Mac OS X

- OTAEによる登録。 詳しくは、「Mac OS X」を参照してください。
- デバイスのプロパティ、証明書、レポート、およびサポートされているプロファイルを示す、XenMobileコンソールのデバイス管理情報。
- Mac OS Xデバイスのセキュリティアクション - 選択的なワイプ、ロック、取り消し、ワイプ。
- 新規デバイスポリシーオプション：

  名前
  iOSおよびMac OS Xプロファイルのインポート
  AirPlayミラー化
  アプリケーションインベントリ
  カレンダー（CalDav）
  連絡先（CardDAV）
  資格情報
  Exchange
  フォント
  LDAP
  メール
  パスコード
  プロファイル削除
  制限事項
  SCEP
  VPN
  ［Webclip
  WiFI

Android for Workをサポートする新機能および機能拡張

- **Androidより前のデバイスのサポート**

- **Android for Workでのデバイス所有者モードのプロビジョニング**

  Android for WorkアプリやBYODモードのAndroidデバイスを管理できるのに加えて、デバイス所有者モードのプロビジョニングによって、会社所有のデバイスを管理することもできます。 管理するには、デバイス間で近距離無線通信（NFC）バンプを使用します。 1台のデバイスでWorx Provisioning Toolアプリを実行して、特別な設定をしていない新しいデバイスまたは工場出荷時リセットされたデバイスをバンプします。 デバイス所有者モードは、Android 5.x.xが動作するほとんどのデバイスに対応した、会社所有デバイスのモードです。

- **Android for Work一括購入**

  Android for Workを有効にしたアプリに対して、XenMobileコンソールで一括購入ライセンスを管理できます。 Android for Workの一括購入プランを利用すると、組織のアプリやその他のデータの検索、購入、配布の処理が簡単になります。 Android for Work用のパブリックアプリケーションストアの有料アプリをXenMobileに追加するときに、一括購入ライセンスの状態（使用できるライセンス数の合計）を確認できます。 アプリをユーザーに展開した後には、現在使用中のライセンス数や、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を確認できます。 ユーザーを選択して［**Disassociate**］をクリックすると、そのユーザーへのライセンスの割り当てが終了し、別のユーザー向けにライセンスを空けることができます。 ただし、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。

共有デバイス

XenMobileでは、複数のユーザーが共有できるデバイスを構成できます。 詳しくは、「XenMobileでの共有デバイス」を参照してください。

言語サポート

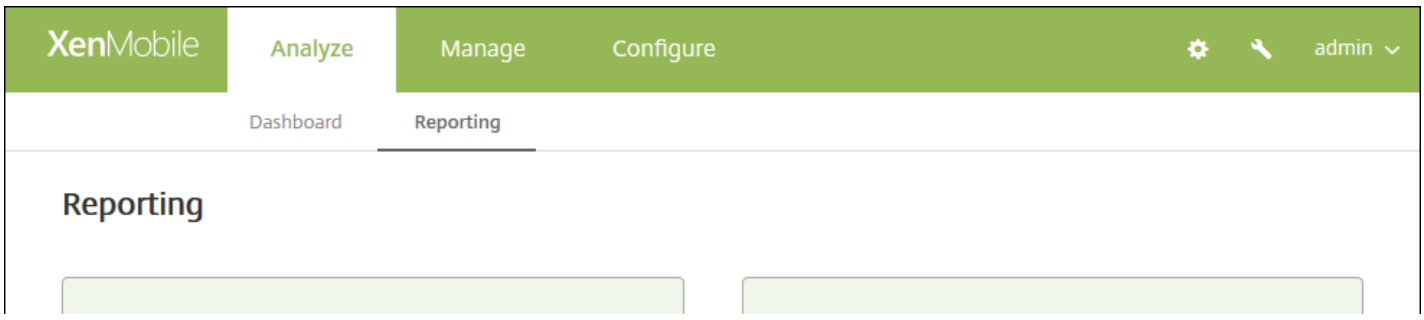
XenMobile 10.3のXenMobileコンソールは、韓国語、ドイツ語、およびポルトガル語をサポートしています。 MDXポリシーは、XenMobileコンソールでローカライズ表示されるようになりました。 詳しくは、「XenMobileの言語サポート」を参照してください。

レポート

［**Reporting**］タブから、XenMobileコンソールに提供されている以下の10種類の定義済みレポートを生成できます。

- **Apps by Devices & User**：ユーザーのデバイスに存在しているアプリケーションを一覧表示します。
- **Terms & Conditions**：使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。
- **Top 25 Apps**：ほとんどのユーザーのデバイスに存在している上位25のアプリケーションを一覧表示します。
- **Jailbroken/Rooted Devices**：ルート化済みiOSデバイスおよびジェイルブレイクされたAndroidデバイス一覧表示します。
- **Top 10 Apps – Failed Deployment**：展開に失敗したアプリケーションを一覧表示します。
- **Inactive Devices**：指定期間に非アクティブになったデバイスを一覧表示します。
- **Apps by Type & Category**：アプリケーションをバージョン別、種類別、およびカテゴリ別に一覧表示します。
- **Device Enrollment**：指定期間中に登録されたデバイスを一覧表示します。
- **Apps by Platform**：アプリケーションとアプリケーションバージョンを、デバイスプラットフォーム別およびバージョン別に一覧表示します。
- **Devices & Apps**：すべてのデバイス、デバイスデータ、およびインストールされているアプリケーションを一覧表示します。

レポートを実行するには、XenMobileコンソールで［**Analyze**］タブ、［**Reporting**］の順にクリックします。 レポートは.csv形式なので、Microsoft Excelのようなプログラムで開くことができます。 詳しくは、「XenMobileでのレポート」を参照してください。



Apps by Devices & User

List of apps that users have on their devices.

Report Data: device serial number, device platform, version, user name, ID, email, # of apps, deployment status.

Terms & Conditions

List of accepted and declined Terms and Conditions agreements by device users.

Report Data: document name, created on, platform, user name, delivery group, acceptance status.

Top 25 Apps

List of apps most users have installed.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Jailbroken/Rooted Devices

List of jailbroken iOS and rooted Android devices.

Report Data: device platform, model, version, serial number, user name, device mode, status.

Top 10 Apps - Failed Deployment

List of apps that have failed deployment.

Report Data: app name, # of deployments, deployment status, type, category, deployment date, app owner.

Inactive Devices

List of devices that have been inactive for a specified length of time.

Report Data: last activity, device mode, platform, version, user name, last authentication, device IMEI, serial number, model, first connection.

Apps by Type & Category

List of apps and app versions by app type (MDX, Public, Web & SaaS, Enterprise, Web Link) and defined categories.

Report Data: app name, version, # of deployments, deployment status, type, category, deployment date, app owner.

Device Enrollment

List of devices that have been enrolled during a specified length of time.

Report Data: first connection, device mode, platform, version, model, user name, last authentication, phone number.

Apps by Platform

List of apps and app versions installed on various device platforms and device versions.

Report Data: app name, version, # of deployments, deployment status, deployment date, app owner, device platform, version, model, model name.

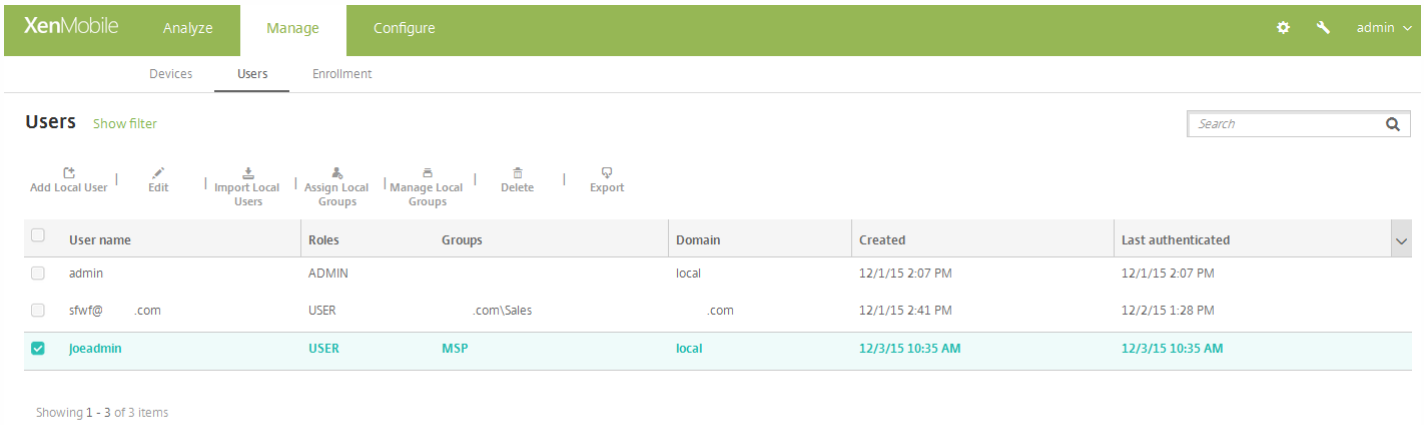
Devices & Apps

List of all devices, device data, and apps installed.

Report Data: device serial number, user name, ID, email, device platform, version, model, mode, status, last connection, enrollment status, enrollment date, device ownership, location, certificate expiration, app name, version, deployment status, type, category, deployment date, app owner, app ID.

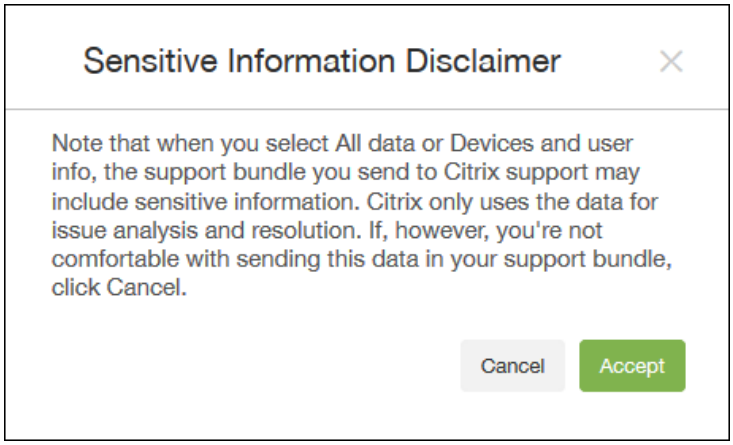
グループへのLDAPメンバー（ローカルユーザー）の追加

多くの組織はActive Directoryグループを構成していませんが、パイロット版などの特定の目的でローカルグループが必要になる場合があります。 XenMobile 10.3では、LDAP（ローカルグループのローカルユーザーメンバー）を作成できます。 作成後、ローカルグループを含むデリバリーグループを定義できます。 この一連のユーザーは、デバイスを再登録しなくても、デリバリーグループに割り当てられたアプリケーションおよびポリシーにアクセスすることができます。 詳しくは、「XenMobileでローカルユーザーを追加、編集、または削除するには」を参照してください。



サポートバンドルの使用許諾契約

サポートバンドルを初めてのCitrix Insight Services（CIS）にアップロードするときに、使用許諾契約への同意を求められます。 詳しくは、「XenMobileでのサポートバンドルの作成」を参照してください。



サポートバンドルのデータの匿名化

XenMobileでサポートバンドルを作成する場合、デフォルトでは、機密性の高いユーザー、サーバー、ネットワークのデータは匿名化されます。 この動作は、［Anonymization and De-anonymization］ページで変更することができます。 また、XenMobileがデータの匿名化時に保存したマッピングファイルをダウンロードすることもできます。 データの匿名化を解除したり、ユーザーまたはデバイスで発生した問題を特定したりする目的で、Citrixのサポートからこのファイルを要求される場

合があります。詳しくは、「サポートバンドルのデータの匿名化」を参照してください。

接続確認

［XenMobile Support］ページで、NetScaler Gatewayおよびそのほかのサーバーや場所へのXenMobileの接続を確認できます。詳しくは、「接続確認の実行」を参照してください。

Microsoft Azure

Windows 10デバイスをMicrosoft Azure ADに統合すると、Active Directory認証の統合手段としてAzureを使用してデバイスの登録を行うことができます。詳しくは、「Microsoft Azureの設定」を参照してください。

XenMobile Server 10.3の修正された問題

Aug 02, 2016

XenMobile 10.3では、次の問題が修正されています。 XenMobile 10.3.5で修正された問題については、XenMobile 10.3.5の「既知の問題」のトピックを参照してください。

キャリアSMSゲートウェイ経由でSMTPからメールを送信する場合に、メールアドレスにメール送信プレフィックスが2回追加される場合があります。 [#492629]

Cisco Identity Service EngineからXenMobileへのHTTP GET要求が、404エラーで失敗することがあります。 [#555554]

ファイルのアップロードポリシーが、Androidデバイスにファイルをプッシュするように設定されている場合、デバイスへのファイルのプッシュが失敗することがあります。 その場合に、デバイス上で「契約条件」の文が表示される場合があります。 [#564144]

モバイルデバイス管理（MDM：Mobile Device Management）のID証明書がSCEP（Simple Certificate Enrollment Protocol）によって配布され、組み込みの公開キー基盤を使用して発行される場合、これらのIDの更新時に、XenMobileが以前の証明書を適切に取り消さない場合があります。 その結果、影響を受けるデバイスがMDM機能を失う場合があります。 [#569999]

プロキシサーバーの構成後、接続チェックによって生成されるネットワークトラフィックがそのプロキシサーバーを通過せず、接続に失敗します。 [#571467]

ユーザーが子ドメインのメンバーである場合、SAMLアプリへの接続に失敗します。 [#571851]

iOS MDXアプリが［除外するデバイス］の一覧に含まれている場合、デバイスがモバイルアプリケーション管理のみのモード（MAMモード）のときにこのアプリがWorxStoreに表示されません。 [#571900]

XenMobile 10にアップグレードした後、デバイスの検索が最大30秒かかることがあり、CPU使用率も100%まで上昇します。 [#577010]

マルチノードクラスター環境でWorxWebを使用してイントラネットサイトをブラウズするときに、ユーザーがURLにアクセスできず、「Error Invalid OTT」というメッセージが表示されることがあります。[#577273]

XenMobileをプロキシサーバーと共に構成した場合、Google Playの資格情報の追加またはAndroidパブリックアプリケーションストアのアプリ作成を実行しようとすると失敗することがあります。 [#578727]

Internet Explorer 11の公開バージョンでXenMobileコンソールを開こうとすると、空のページが開きます。 [#578729]

このリリースでは、iOS 8用のWPA2パーソナルとWPA2エンタープライズがサポートされるようになりました。 [#579616]

XenMobileコンソールでアプリの追加またはアップロードを行う場合に、既存のアプリと同じアプリファイル名を使用してアプリをXenMobileにアップロードすると、エラーになることがあります。 [#580359]

Androidデバイスで、WorxアプリをWorx Storeからダウンロードすることができません。 [#582044]

マクロにユーザー名と電話番号を入力するときに、変換機能によって電話番号が正しく変換されません。 [#589130]

［アクティベーションロックのバイパス］コマンドが一部のiOSデバイスで機能しない場合があります。 [#589991]

「memberOf」プロパティの値が255文字を超えている場合、「No groups found」というエラーメッセージが表示されます。

ユーザーがWorx HomeからWindowsアプリを開こうとすると、列挙は成功しますが、アプリが開きません。「Could not

add account」というエラーメッセージが表示されます。[#590046]

チャレンジパスワードを求めるSimple Certificate Enrollment Protocol（SCEP）ポリシーを作成すると、そのポリシーを保存できません。 このリリースでは、チャレンジパスワードのフィールドが任意になりました。 [#590798]

プロキシサーバーを使用するようにXenMobileを構成した場合、Android for Workが外部Webサイトに接続できません。 [#591707]

IPAアプリをApp Controllerにアップロードしようとすると失敗し、「Invalid package type for selected app」というエラーメッセージが表示されます。このメッセージは、PNGイメージにエラーがある場合に表示されます。 [#592748]

ユーザーを登録しようとすると、「User does not exist」というエラーメッセージが表示されます。このエラーは、ユーザーの登録情報を削除して再登録した後に発生します。 この状況になったときには、Active Directoryにユーザーが再作成されます。 [#593028]

Microsoft OutlookまたはMicrosoft Exchangeアカウントからカレンダーの招待状を作成した場合、WorxMailに表示されるまでに長い時間がかかることがあります。 [#594542]

ワークフローの設定時に443（デフォルト）以外のポート番号を使用すると、ユーザーがそのワークフローのリンクを開くことができません。 [#599441]

ユーザーがXenMobileサーバーからデバイス上のAndroidアプリを更新できません。 [#601251]

Azure Active Directoryからユーザーを登録した場合に、ユーザーがWorxアプリにログオンできません。 [#608505]

2015年12月時点で、Nexmo SMSではHTTPS接続のみがサポートされます。 XenMobileのデフォルトでは、**[ON]** になっています。 この値を **[OFF]** に変更しても影響はありません。 アップグレード後もこの値は **[OFF]** と表示されますが、接続は安全です。 [#609306]

WorxStoreでは、ライセンスがデバイスのみに適用されている場合でも、Volume Purchase Program（VPP）が必要です。 [#610338]

XenMobile Server10.3の既知の問題

Aug 02, 2016

XenMobile 10.3の既知の問題は次のとおりです。 バージョン10.3.5で新たに確認された問題については、XenMobile 10.3.5の「既知の問題」のトピックを参照してください。

- 次のバージョンのNetScaler上でTLS 1.2セキュリティプロトコルを構成している場合に、XenMobileとNetScalerの統合に関する以下のバグがあります。
  - NetScaler 11.xの11.0.64より前のバージョン
  - 10.5.59
  - 10.5.58

  XenMobile MAM環境に、XenMobileサーバーとNetScaler Gateway間のNetScalerロードバランサーが構成されている場合、この問題は発生しません。

  NetScaler GatewayとMAMモードのXenMobile間の通信は、バックエンドのTLS 1.2セッションの問題により失敗します。 その結果、ユーザーは内部ネットワークへの接続時に、WorxStoreからアプリをダウンロードすることもShareFileからファイルをダウンロードすることもできません。 [#591600、#595713、#596566、#604409]
- 社内アプリのアンインストール後にアプリのプッシュが失敗します。 [#591450]
- アプリからライセンスを削除した後にも、アプリがユーザーデバイス上に残ります。 これはサードパーティ製品の問題です。 [#596656]
- ユーザーがMicrosoftワークアカウントを使用して個人デバイスを登録しようとすると、登録に失敗します。 [#597037]
- 契約条件ポリシーをデバイスに正常に展開した場合でも、XenMobileコンソールには、そのポリシーがインストール済みまたは保留中の状態として表示されません。 [#598407]
- Windows 10デバイスでは制限ポリシーが適用されますが、 ユーザーに対して、禁止された機能が無効になっているというメッセージが表示されません。 [#599064、#606651]
- パブリックアプリケーションおよびエンタープライズアプリケーションを含むカテゴリを追加してからXenMobileにデバイスを登録した場合、ユーザーがWorx Homeにアプリを同期すると、そのカテゴリが表示されません。 [#599495]
- 共有デバイスのRBACの作成時に「選択的なワイプ」デバイス権限を追加しなかった場合、ユーザーがiOSデバイス（XenMobile Enterpriseモード）のWorx Homeでアカウントを削除しようとするときに、手動でデバイスからデバイスマネージャープロファイルを削除する必要があります。 [#600705]
- アプリのアプリケーションインベントリポリシーとエンタープライズハブポリシーを展開し、別の名前と説明を指定してパブリックアプリケーションを作成した後、ユーザーがWorx Homeからそのアプリを開くと、アプリ名と説明が同じものになります。 [#600369]
- Microsoft SQL Serverの初回使用時にSSLモードで構成して、CA証明書がそのSQL Serverの証明書と対応していない場合、接続に失敗します。 SQL Serverの証明書に対応する適切なCA証明書を使用して接続を再試行しても、接続に失敗します。 その証明書を機能させるには、XenMobileサーバーを再起動してtrustStoreキャッシュを消去します。 [#602609]
- 共有ユーザーデバイスのユーザー名は英語にする必要があります。 共有デバイスではASCII文字以外のユーザー名はサポートされません。 [#605544]

- ユーザーがIMEIバインド（ユーザー名とパスワード）およびSMTPとSMSの通知用のワンタイムパスワード招待状を受信すると、1つ目のプロファイルは正常にインストールされますが、2つ目のプロファイルのインストールは失敗し、「Profile Installation Fails. A connection to the server could not be established」というエラーメッセージが表示されます。iPhone 6およびiPhone 6 Plusデバイスには IMEI番号とMEID番号があり、ワンタイムパスワードがIMEI番号ではなくMEID番号にバインドされます。 このIMEI番号をiPhoneのUDID（Unique Device Identifier）に置き換えるか、通常の電話番号を使用してください。 [#606162]

- XenMobile 10.3へのアップグレード後、ライセンス情報には30日間のお試し版として表示され、ライセンスサーバーの構成済みフラグがtrueに設定されます。 XenMobileサーバーへのアップグレード後、同じライセンスをサーバーにアップロードすることで、ライセンスのお試し版の期限が削除されます。 [#607939]

- Windows 8.1タブレットでは、ユーザーはデバイスから正常にアプリを削除できますが、 XenMobileコンソールのデバイスのプロパティにエンタープライズアプリケーションが引き続き表示されます。 [#608184]

- XenMobile Enterpriseモードでは、［アプリケーションのワイプ］オプションと［選択的なワイプ］オプションの機能が同じです。 [#608715]

- Internet Explorerでファイルを保存するか開くと、XenMobileサーバーが応答を停止します。 動作を再開するには、サーバーを再起動してください。 [#608724]

- XenMobile 10.3へのアップグレード後、禁止されたWebアドレスおよびブックマークが存在するにもかかわらず、Android for Workがブラウザーポリシーに表示されません。 [#609002]

- Windows 8.1およびWindows 10が動作するタブレットで、デバイスからアカウントを手動で削除した後も、一部のポリシーが残ります。 [#609201]

- Windows 10タブレットで、ユーザーがデバイスの自動更新設定を変更した場合、その変更がXenMobileコンソールの［Device Properties］の［Security Information］セクションに表示されません。 [#609254]

- WorxStore名では、英語（ASCII）文字だけがサポートされます。 [#609535]

- Internet ExplorerおよびFirefox Webブラウザーから証明書署名要求（CSR）をダウンロードしようとすると、「Webページを表示できません」というエラーが表示されて失敗します。Chrome WebブラウザーからのCSRのダウンロードは成功します。 [#609552]

- XenMobileコンソールにログオンして、**［Analyze］** > **［Reporting］**に移動し、 **［Inactive Devices］**をクリックすると、ファイルがダウンロードされずに空のページが表示されます。 [#609649]

- Citrix Workspace Cloudでワークスペースを構成するときに、デリバリーグループが、子および孫ドメインに属するActive Directoryのユーザーまたはグループによって更新されません。 [#609673]

- 複数の契約条件ポリシーが展開され、いずれのポリシーもデフォルトの契約条件ではない場合に、Windows 10デバイスの登録に失敗します。 [#609694]

- デリバリーグループからポリシーを削除する場合に、**［Summary］**をクリックしてポリシーを保存すると、そのリソースがデリバリーグループに残ります。 **［Summary］**ではなく**［Next］**をクリックすれば、デリバリーグループからポリシーが削除されます。 [#610109]

- Windows CEデバイスで元のファイル拡張子を維持するには、ポリシーでターゲットファイル名を指定しないでください。 [#610601]

- Mac OS X用のVPNデバイスポリシーを構成すると、**［VPN］**オプションが**［Connection Types］**の一覧に表示されま

す。 しかし、このオプションをMac OS Xデバイス用に構成することはできません。 [#612846]

- XenMobile 10.1から10.3に更新するときに、WorxStoreにカスタム名が設定されている場合は、ストア名をデフォルトの［**Store**］設定に変更して、この設定をデバイスに展開してから更新する必要があります。 そうしなければ、XenMobile 10.3の登録、Worx HomeおよびWorxStoreへのアクセス、iOSデバイスでのアプリの展開中に、カスタムストア名による問題が発生します。 [#614049]

- XenMobileコンソールでAndroid for Workを有効にすることができません。 Android for Workアカウント設定を構成し、Googleから取得したサービスアカウントID（数字のみのもの）を入力すると、設定の保存時にエラーになります。 数字と英字が含まれる以前のGoogleの形式を使用してサービスアカウントIDを入力した場合も同じエラーになります。この形式がXenMobileサーバーのサービスアカウントIDに対応していないからです。 これはサードパーティ製品の問題です。

  回避策として、Android for Workを有効にするには、GoogleクライアントIDのサーバープロパティを追加してください。

  1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 ［**Settings**］ページが開きます。
  2. ［**Add**］をクリックします。 ［**Add New Server Property**］ページが開きます。
  3. ［**Key**］の一覧で、 ［**Custom Key**］をクリックします。
  4. ［**Key**］ボックスに「**google.aw.enterprise.client.id**」と入力します。
  5. ［**Value**］ボックスに、クライアントIDの数字の部分（例：3838383838388383）を入力します。
  6. ［**Display name**］に、「Google domain client ID」などの表示名を入力します。
  7. ［**Save**］をクリックします。

  [#615118]

- Mac OS XコンピューターおよびiPadの場合、XenMobile 10.3では常に、XenMobileコンソールで設定した順序に関係なく最初に削除処理が行われます。 [#620459]

- iOS一括登録を有効にしてXenMobile SSL証明書のルート証明書（CA）を更新すると、デバイスの登録または再登録が失敗することがあります。 この問題は、自己署名証明書から公開証明書に変更するとき、新しいプロバイダーから証明書を購入するとき、または企業内証明書に移動するときに発生することがあります。 この問題は、既存の登録済みデバイスには影響しません。 この問題を解決するには、以下の手順に従います。

  1. XenMobileコンソールで、 ［**Settings**］ > ［**iOS Bulk Enrollment**］の順にクリックします。
  2. ［**DEP Configuration**］で、 ［**Allow Device Enrollment Program (DEP)**］の隣にある［**NO**］をクリックしてから［**Save**］をクリックします。 数秒間待機します。 この手順では、Apple DEPポータル上のDEPデバイスからの前のDEPプロファイルが削除されます。
  3. ［**Manage**］ > ［**Devices**］の順にクリックします。 DEP が登録された デバイスが列［**DEP registered**］に表示されないことを確認します。
  4. 再び［**Settings**］ > ［**iOS Bulk Enrollment**］をクリックします。
  5. ［**DEP Configuration**］で、 ［**Allow Device Enrollment Program (DEP)**］の隣にある［**YES**］をクリックしてから［**Save**］をクリックします。 数秒間待機します。 この手順では、すべてのDEPデバイスに新しいプロファイルが強制的に追加されます。
  6. ［**Test Connection**］をクリックして、XenMobileサーバーとApple DEPサーバー間の接続が機能していることを確認します。
  7. 再び［**Manage**］ > ［**Devices**］の順にクリックします。 すべてのDEPデバイスが 列［**DEP registered**］で新規に登録さ

れていることを確認します。

Apple DEPについて詳しくは、「iOSデバイスの一括登録」を参照してください。
[#635699]

アーキテクチャの概要

Oct 25, 2016

展開するXenMobileリファレンスアーキテクチャのXenMobileコンポーネントは、組織のデバイスまたはアプリケーションの管理要件がベースになります。 XenMobileコンポーネントはモジュール形式で、相互に依存しています。 たとえば、組織のユーザーのモバイルアプリケーションに対してリモートアクセスを提供する場合に、ユーザーが接続するデバイスの種類を追跡する必要があるとします。 このシナリオでは、NetScaler Gatewayを使用してXenMobileを展開します。 XenMobileでアプリケーションとデバイスを管理し、NetScaler Gatewayによって、ユーザーがネットワークに接続できるようにします。

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

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

上記の機能の一部またはすべてを実現するには、次の順番でXenMobileコンポーネントを展開することをお勧めします。

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

XenMobileは、XenMobileコンソールによるデバイス管理とアプリケーション管理を提供する統合ソリューションをサポートします。 ここでは、XenMobile展開のリファレンスアーキテクチャについて説明します。

実稼働環境では、スケーラビリティとサーバー冗長性を実現するために、XenMobileソリューションをクラスター構成で展開することをお勧めします。 また、NetScaler SSLオフロード機能を活用してXenMobileサーバーの負荷をさらに軽減し、ス

ループットを高めることができます。 NetScalerで2つの負荷分散仮想IPアドレスを構成することによってXenMobile 10.xのク
ラスタリングをセットアップする方法について詳しくは、「XenMobile 10のクラスタリングの構成」を参照してください。

障害回復展開環境向けのXenMobile 10 Enterprise Editionの構成方法（アーキテクチャ図を含む）について詳しくは、
「XenMobile障害回復ガイド」を参照してください。

以降のセクションでは、XenMobile展開のさまざまなリファレンスアーキテクチャについて説明します。 リファレンスアーキ
テクチャ図については、『XenMobile展開ハンドブック』の「オンプレミス展開のリファレンスアーキテクチャ」と「クラウ
ド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。 ポートの完全な一覧については、「XenMobileのポート要件」
を参照してください。

モバイルデバイス管理（MDM）モード

XenMobile MDM Editionでは、iOS、Android、Amazon、およびWindows Phoneのモバイルデバイス管理を使用できます
（「XenMobileでサポートされるデバイスプラットフォーム」参照）。XenMobileのMDM機能のみを使用する予定の場合
は、XenMobileをMDMモードで展開します。 たとえば、コーポレート発行のデバイスをMDMで管理して、デバイスポリシー
やアプリを展開し、アセットインベントリを取得して、デバイスワイプなどのアクションをデバイスで実行できるようにする
必要がある場合などです。

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

モバイルアプリケーション管理（MAM）モード

MAMはiOSおよびAndroidデバイスをサポートしていますが、Windows Phoneデバイスはサポートしていません
（「XenMobileでサポートされるデバイスプラットフォーム」参照）。XenMobileのMAM機能のみを使用する予定で、MDM
用に登録するデバイスがない場合は、XenMobileをMAMモード（MAM-onlyモードとも呼ばれます）で展開します。 たとえ
ば、BYOモバイルデバイスのアプリとデータをセキュリティ保護する必要がある場合や、エンタープライズモバイルアプリを
配信して、アプリのロックおよびデータのワイプを実行できるようにする必要がある場合などです。 デバイスをMDMに登録
することはできません。

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

MDM+MAMモード

MDMモードとMAMモードを併用すると、iOS、Android、およびWindows Phone向けのモバイルデバイス管理に加えて、モ
バイルアプリとデータの管理を行うこともできます（「XenMobileでサポートされるデバイスプラットフォーム」参照）。
XenMobileのMDM+MAM機能を使用する場合、XenMobileをENT（エンタープライズ）モードで展開します。 たとえば、
コーポレート発行のデバイスをMDMで管理する必要がある場合や、デバイスポリシーやアプリを展開し、アセットインベン
トリを取得し、およびデバイスをワイプできるようにする必要がある場合です。 さらに、エンタープライズモバイルアプリを
配信し、アプリのロックとデバイスのデータのワイプを実行できるようにする必要がある場合もあります。

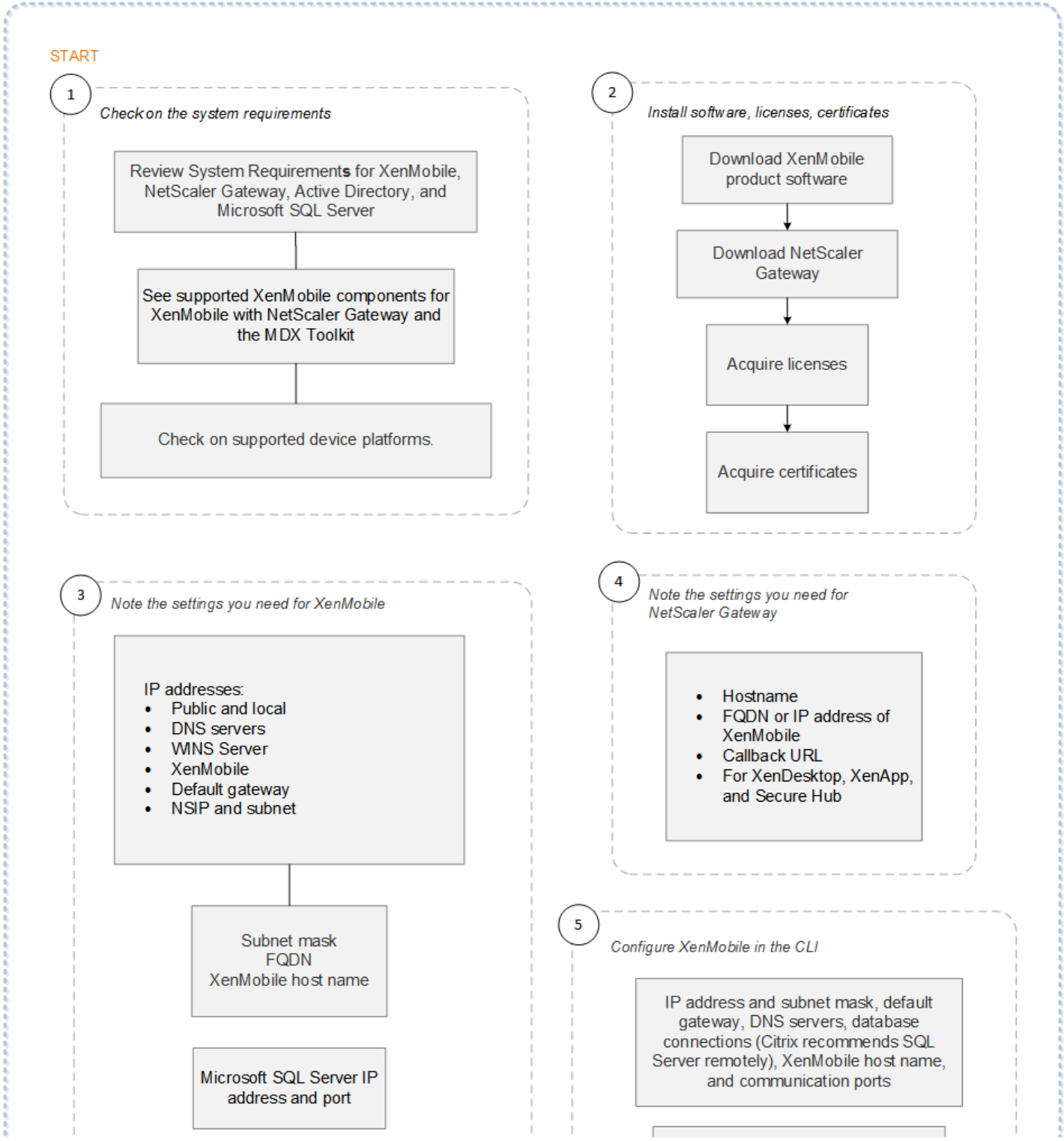
推奨展開モデルでは、XenMobileサーバーをDMZに配置し、NetScaler Gatewayをその前に配置して、XenMobileの追加保護
を提供します。

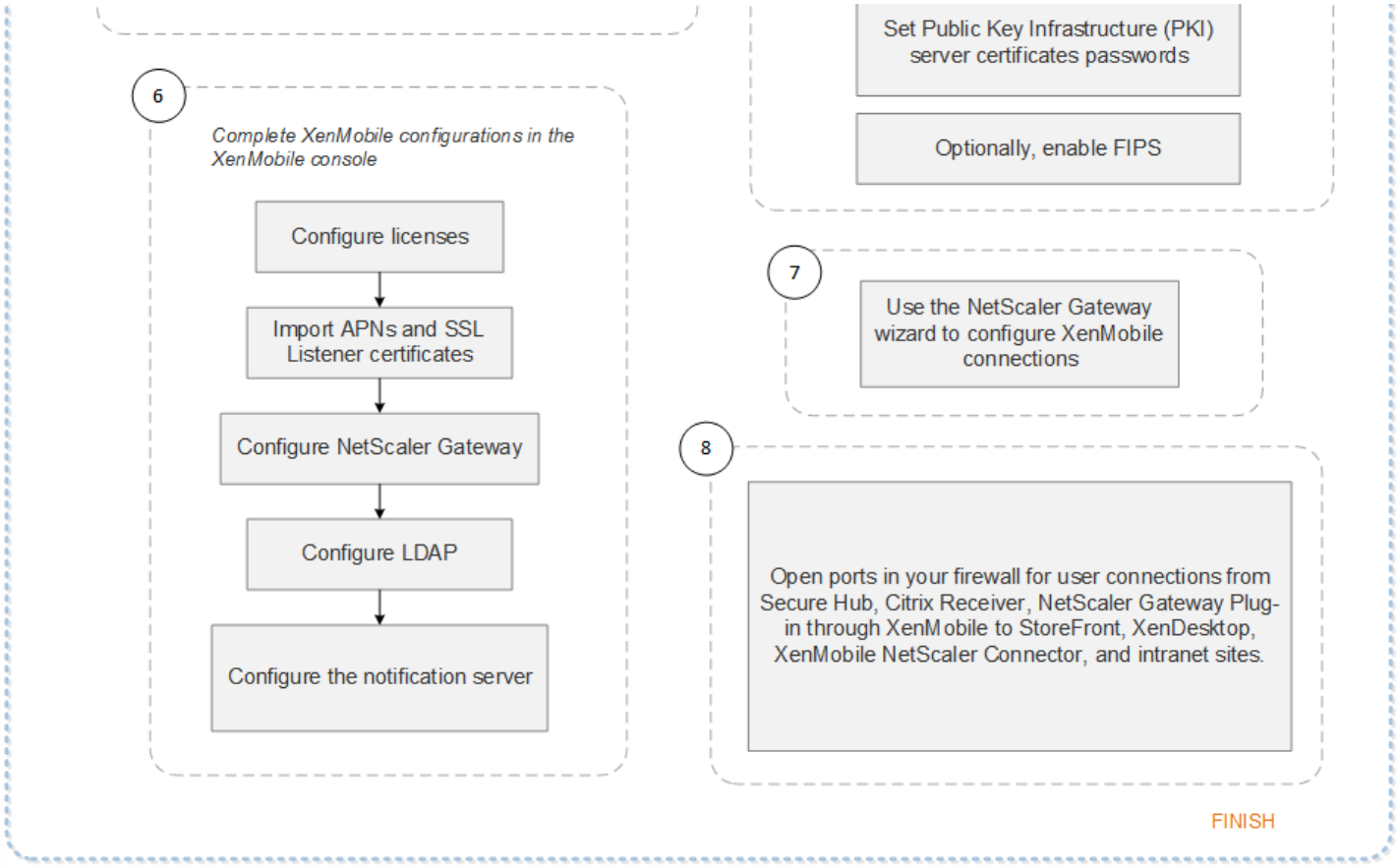
内部ネットワークのXenMobile - もう一つの展開オプションは、DMZではなく内部ネットワークにXenMobileサーバーを配置
します。 この展開は、ネットワークアプライアンスのみをDMZに配置できるようセキュリティポリシーが求める場合に使用
されます。 この展開ではXenMobileサーバーがDMZにないため、DMZからSQL ServerとPKIサーバーにアクセスできるよう
するため内部ファイヤフォール上にポートを開く必要がありません。

NetScaler Gatewayを使用するXenMobileの展開フローチャート

Oct 25, 2016

このフローチャートは、NetScaler Gatewayを使用してXenMobile 10.3を展開する場合の主な手順を示しています。 各手順のトピックのリンクは図に従っています。





1

- XenMobile 10.3のシステム要件
- XenMobileの互換性
- XenMobile 10.3でサポートされるデバイスプラットフォーム

2

- XenMobileのインストール
- XenMobileでの証明書
- XenMobileのライセンス

3

- XenMobileインストールチェックリスト

4

- XenMobileインストールチェックリスト

5

- コマンドプロンプトウィンドウでのXenMobileの構成

6

- WebブラウザーでのXenMobileの構成

7

- XenMobile環境の設定の構成

8

- XenMobileのポート要件

このフローチャートは、PDF形式でも入手できます。

XenMobile展開のフローチャート

XenMobileの展開規模

Oct 25, 2016

XenMobileインフラストラクチャの規模を理解することはXenMobileを展開し構成する方法を決定するうえで重要な役割を果たします。 このトピックでは、小規模から大規模のエンタープライズ展開の要件を判断するうえでよくある質問に対する回答を提供します。

パフォーマンスとスケーラビリティのガイドライン

このトピックのデータは、XenMobile 10.3インフラストラクチャのパフォーマンスとスケーラビリティを判断するためのガイドラインとして使用することを想定しています。 サーバーとデータベースのスケーラビリティを構成する方法を判断するための2つの重要な要素は、スケーラビリティ（最大ユーザー数/デバイス数）とログオン数です。

- スケーラビリティは定義済みのワークロードを実行する同時ユーザーの最大数として定義されます。 XenMobileインフラストラクチャをロードするために使用されるフローについて詳しくは、「ワークロード」を参照してください。
- ログオン数は新規ユーザーのオンボーディングと既存ユーザーの認証の数として定義されます。
  - オンボーディング数は環境に初めて登録できる最大デバイス数です。 このトピックでは初回使用またはFTUと呼ばれます。このデータポイントはロールアウト戦略を調整するうえで重要です。
  - 既存ユーザー数は環境に対して認証される最大ユーザー数です。このユーザーは既に登録済みで自分のデバイスで接続したことがあります。 以下のテストには、登録済みユーザーに対するセッションの作成およびWorxMailとWorxWebアプリの実行が含まれます。

以下の表に、対応するXenMobile環境のテスト結果に基づくスケーラビリティのガイドラインを示します。

スケーラビリティ	最大100,000デバイス	
ログオン数	オンボーディング（FTU)	毎時最大2,777デバイス
	既存ユーザー	毎時最大16,667デバイス
構成	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	10ノードで構成されるXenMobileサーバークラスター
	データベース	Microsoft SQL Server外部データベース

> **Important**
>
> このレポートを自動化するには、デバイス数が1,000～100,000である必要があります。 デバイス数が100,000を超える場合の要件については、このレポートの範囲外です。

システム構成およびテスト結果

このセクションでは、使用したハードウェア構成と、オンボーディング（FTU）ワークロードおよび既存ユーザーワークロー

ドのスケーラビリティテストの実行結果について説明します。

以下の表は、1,000-100,000デバイスのXenMobile環境に推奨されるハードウェアおよび構成を示します。 これらのガイドラインはテスト結果および関連するワークロードに基づいています。 推奨事項は、「終了基準」に定義する許容可能なエラー発生の余地を考慮に入れたものです。

テスト結果の解析により、以下の結論が導かれました。

- ログオン数はシステムのスケーラビリティを判断するうえで重要な要素です。 初回ログオンに加えて、ログオン数は環境に構成されている認証タイムアウト値に左右されます。 たとえば、認証タイムアウト値が低すぎると、ユーザーはより頻繁にログオン要求を実行する必要があります。 したがって、タイムアウト値が環境に与える影響を明確に理解する必要があります。
- NetScalerでのユーザーセッションあたりの接続数は重要な検討項目です。
- 128GBのRAM、300GBのディスクスペース、および24の仮想CPUを伴う外部データベース（SQL Server）を使用してテストを行いました。この仕様は実稼働環境にも推奨されます。
- 最大のスケーラビリティを得るため、XenMobileにCPUおよびRAMのリソースを追加しました。
- 検証された最大の構成は10ノードのクラスター構成です。 10ノードを超える規模拡大にはXenMobileを追加で導入する必要があります。

上の表は、XenMobile構成、NetScaler Gatewayアプライアンス、クラスター設定、およびデータベースに基づく、推奨されるオンボーディングおよび既存ユーザーのログオン数を示します。 この表のデータを使用して、新しい展開、および既存の展開に対する既存ユーザー/デバイス数に最適な登録スケジュールを立てます。 構成のセクションは、登録とログオンのパフォーマンスデータと、推奨される適切なハードウェアの関係を示します。

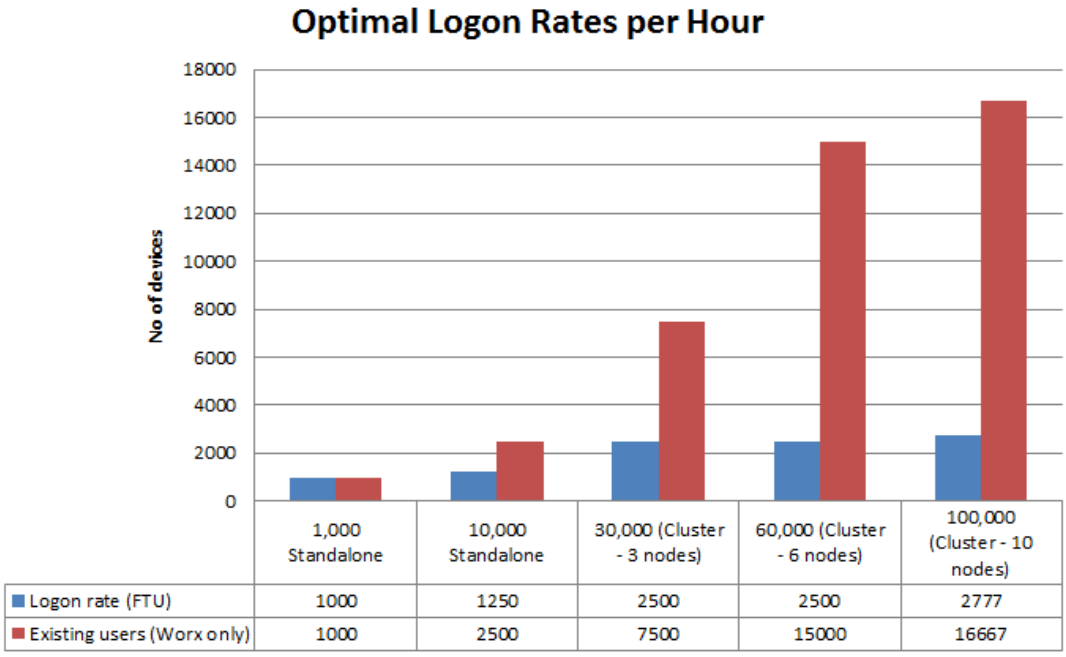
予想されるデバイス数	1,000	10,000	30,000	60,000	100,000
実際のデバイス数	1,000	9,997	29,976	59,831	99,645
ログオン数					
オンボーディング（FTU)	125	1,250	2,500	2,500	2,777
既存ユーザー数（Worxのみ）	1,000	2,500	7,500	15,000	16,667
構成					
参照環境	VPX-XenMobile スタンドアロン	MPX-XenMobileスタンドアロン	MPX-XenMobileクラスター（3）	MPX-XenMobileクラスター（6）	MPX-XenMobileクラスター（10）
NetScaler Gateway	2GBのRAMを搭載したVPX 2つの仮想CPU	MPX-10500		MPX-20500	

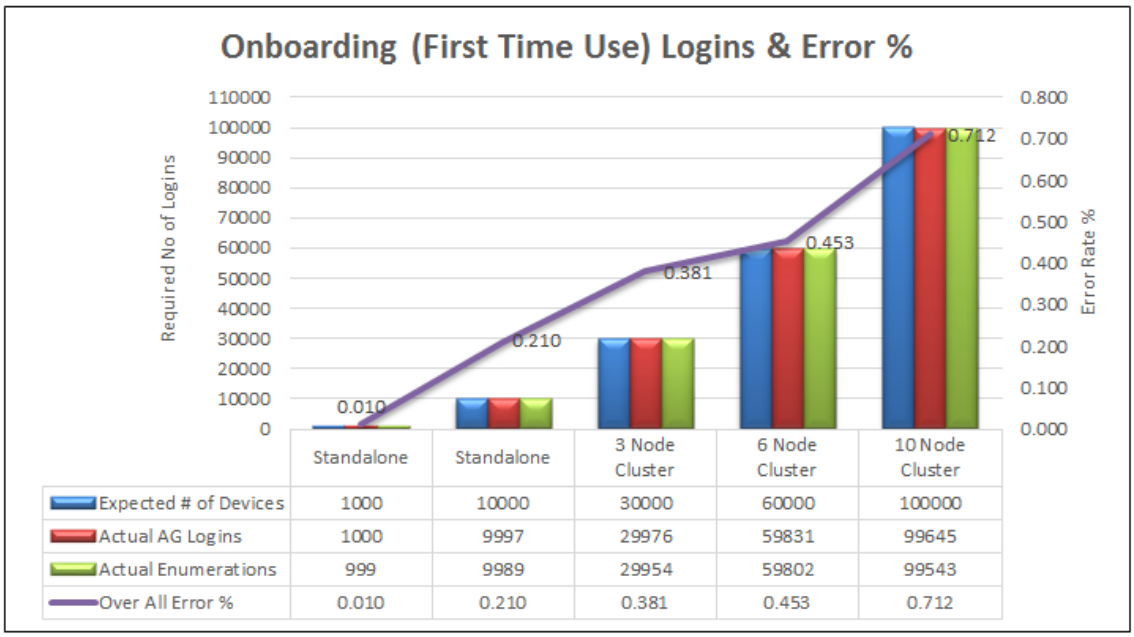
XenMobile - モード	スタンドアロン	スタンドアロン	クラスター		
XenMobile - クラスター	-	-	3	6	10
XenMobile - 仮想アプライアンス	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU
データベース	外部	外部 - Microsoft SQL Server メモリ = 16GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 16GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 32GB 仮想CPU = 12	外部 - Microsoft SQL Server メモリ = 32GB 仮想CPU = 16

注：システム規模に対して推奨される数を超過する登録やログオンがあったりハードウェアの性能が不足していたりすると、以下の事象が発生します。

次の情報は記録された追加のデータポイントを提供します。これらのデータポイントは前の表の結果に影響を及ぼします。

- 登録またはログオンの遅延（ラウンドトリップ時間）
  - 平均遅延時間の合計：0.5～1.5秒
  - NetScaler Gatewayログオンの平均遅延時間：120～440ミリ秒
  - WorxStore要求の平均遅延時間：2～3秒
- スケーラビリティの制限に達すると、インフラストラクチャコンポーネントにCPUおよびメモリの消費のような物理的なパフォーマンスの低下が見られます。
  - NetScaler GatewayおよびXenMobileアプライアンス上での無効な応答
  - 高負荷状態でのXenMobileコンソールの応答時間の遅延





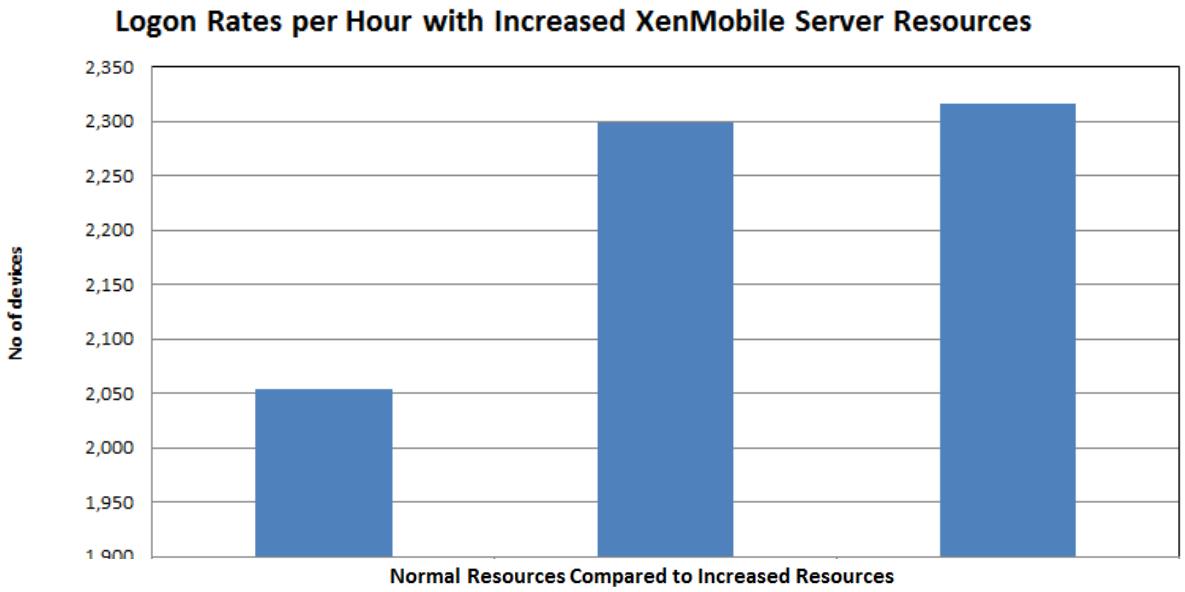
上の図のエラー率には各操作に対応する要求に対して発生する全体的なエラーが含まれており、ログオンに限定したものではありません。「終了基準」に定義するとおり、エラー率は各実行テストの1%という許容可能な範囲に収まっています。

XenMobile Enterprise Editionのリソース増加によるスケールテスト

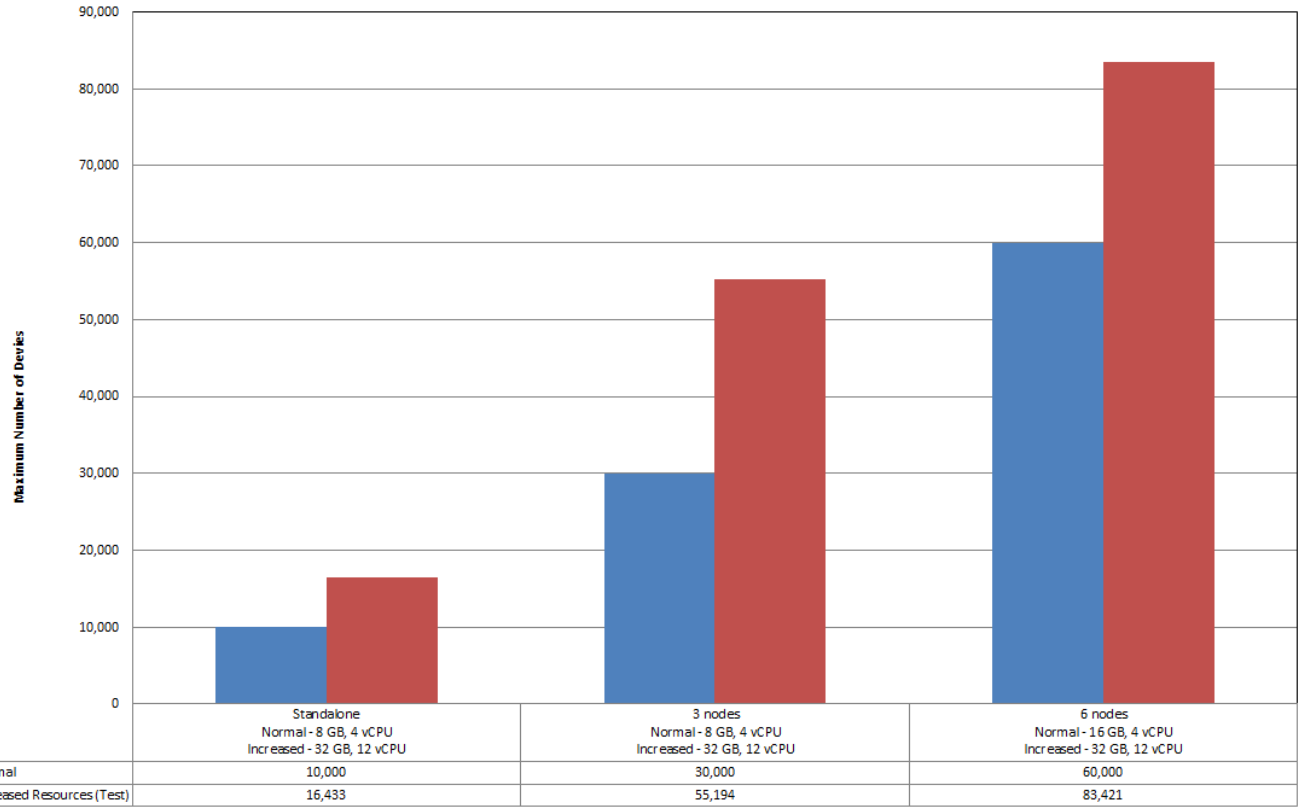
このテスト結果により、ノード数が比較的少ない状況で、XenMobile Enterprise Editionがより多くのデバイスをサポートするための展開戦略を考察できます。 このテストは、スケールアップ機能の測定を目的として、各XenMobileサーバーノードのハードウェアコンポーネント（中央処理装置とメモリ）のリソースを増やして実行されました。 その結果、標準のリソースを使用して同じノード数でテストを実行した場合と比較して、XenMobileサーバーノードによってサポートされるセッションおよびデバイスの最大数が増加しました。

スケーラビリティ

実際のデバイスの最大数	16,433	55,194	83,421
ログオン数			
導入時の初回使用 - 新規ユーザーの追加	2,054	2,299	2,317
構成			
参照環境	VPX-XenMobileスタンドアロン	MPX-XenMobileクラスター3	MPX-XenMobileクラスター6
NetScaler Gateway	MPX-10500	MPX-10500	MPX-20500
XenMobile - モード	スタンドアロン	クラスター	クラスター
XenMobile - クラスター	-	3	6
XenMobile - 仮想アプライアンス	メモリ - 32GB 仮想CPU - 12	メモリ - 32GB 仮想CPU - 12	メモリ - 32GB 仮想CPU - 12
Device Managerデータベース	外部 –S SQL Server メモリ - 16GB 仮想CPU - 12	外部 - SQL Server メモリ - 32GB 仮想CPU - 12	外部 - SQL Server メモリ - 32GB 仮想CPU - 16
Active Directory	メモリ - 8GB 仮想CPU = 4	メモリ - 16GB 仮想CPU - 4	メモリ - 16GB 仮想CPU - 4

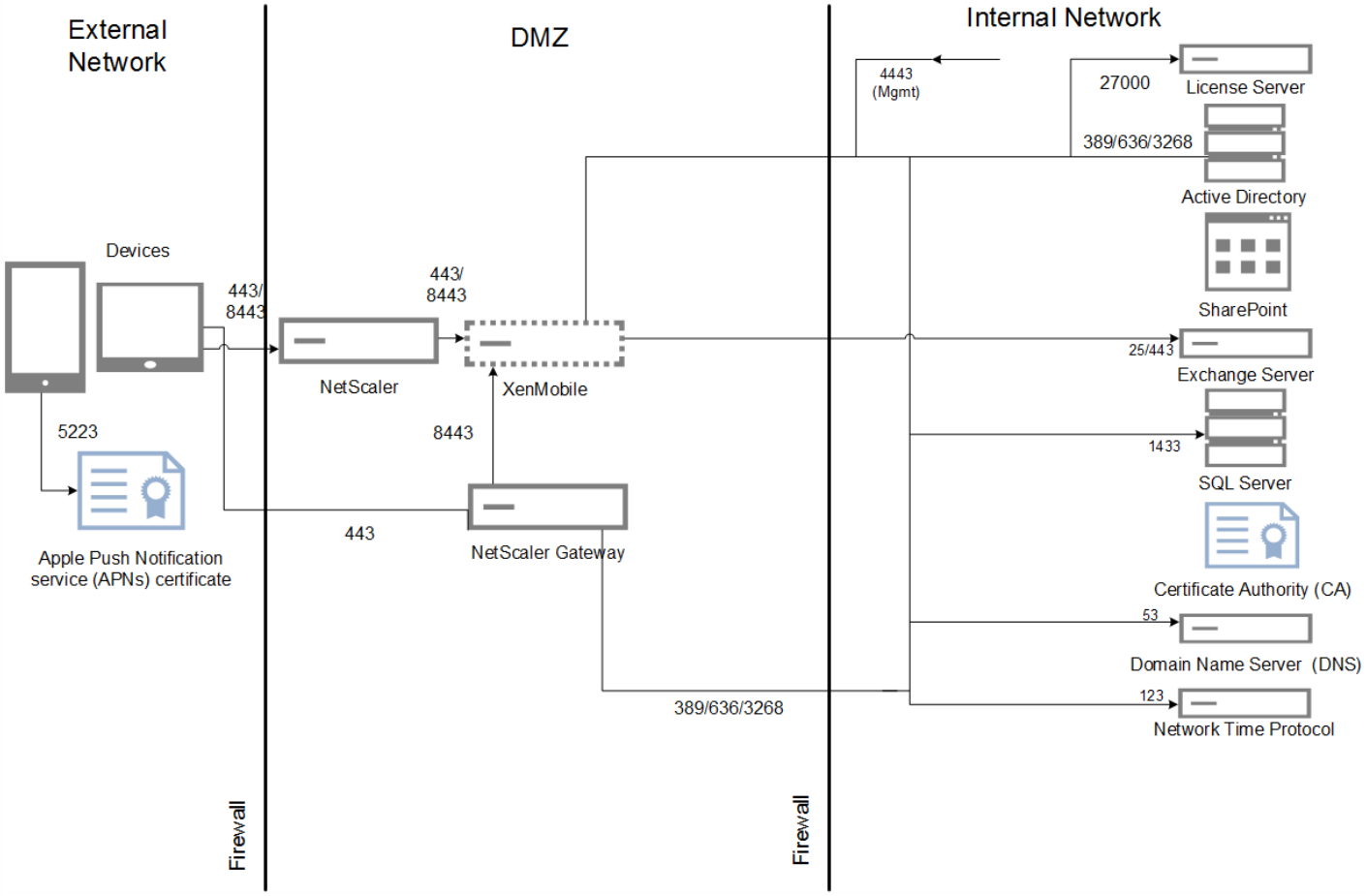


Normal Resources Compared to Increased Resources

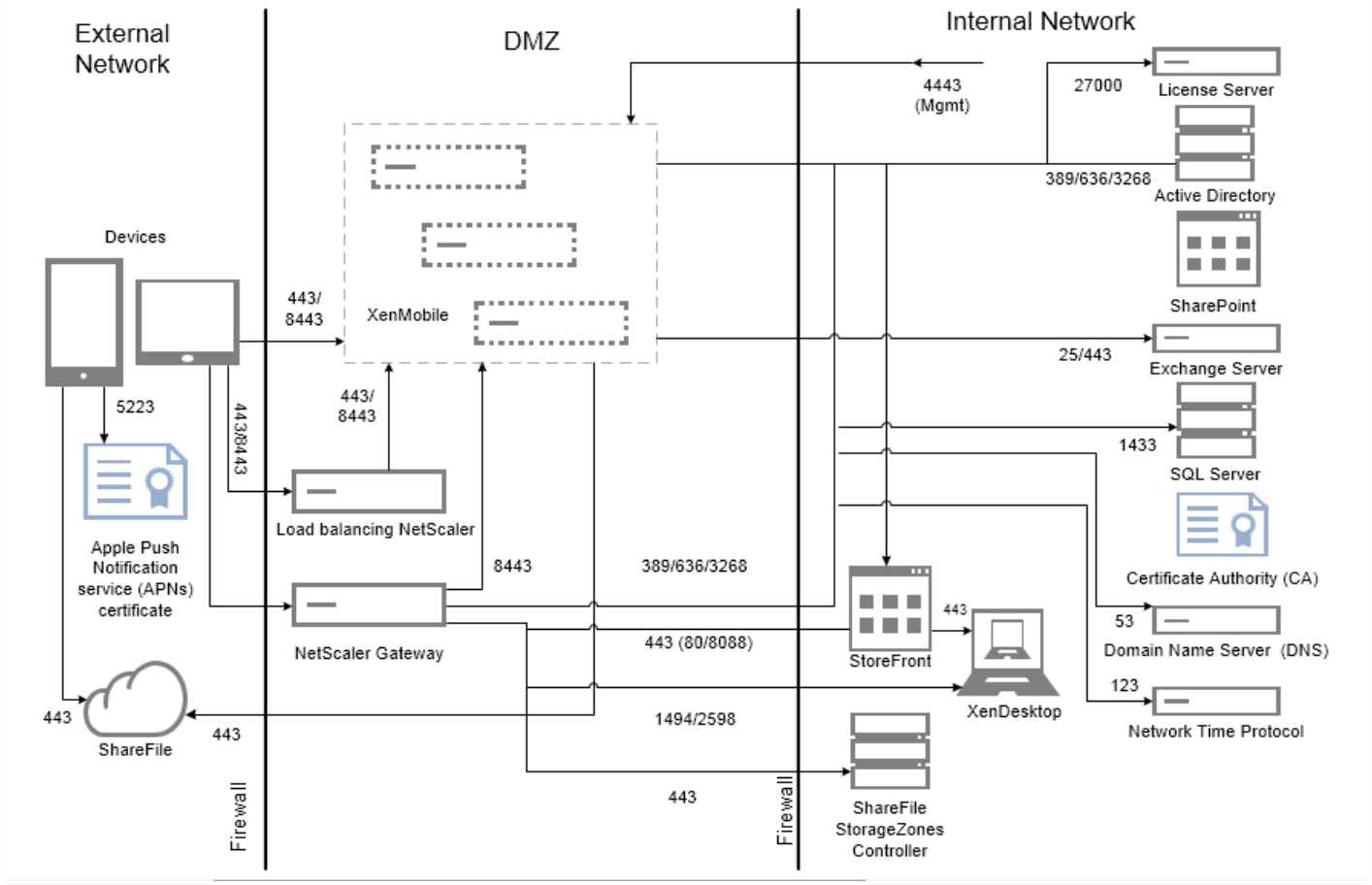


	Standalone Normal - 8 GB, 4 vCPU Increased - 32 GB, 12 vCPU	3 nodes Normal - 8 GB, 4 vCPU Increased - 32 GB, 12 vCPU	6 nodes Normal - 16 GB, 4 vCPU Increased - 32 GB, 12 vCPU
Normal	10,000	30,000	60,000
Increased Resources (Test)	16,433	55,194	83,421

次の図は、小規模な展開のリファレンスアーキテクチャを示しています。 これはスタンドアロンアーキテクチャで、10,000デバイスまでをサポートします。



次の図は、エンタープライズ展開のリファレンスアーキテクチャを示しています。 これはクラスターアーキテクチャで、HTTP経由のMAMに対するSSLオフロードが有効です。10,000デバイス以上をサポートします。



テスト方法

ベンチマークを確立するため、XenMobile Enterpriseに対してテストを実行しました。 小規模および大規模な展開の両方を対象とし、測定には1,000～100,000デバイスを使用しました。

実世界のユースケースをシミュレートするためワークロードを作成しました。 これらのワークロードを各テストで実行し、登録およびログオン数への影響を調査しました。 テストの目標は、「終了基準」に定義する許容可能なエラー発生の余地に収まる最適なログオン数を得ることでした。 ログオン数は、インフラストラクチャコンポーネントのハードウェア構成に対する推奨事項を判断するうえで重要な要素です。

オンボーディング（FTU）ワークロードのログオン要求には、自動検出、認証、およびデバイス登録の操作が含まれました。 アプリケーションのサブスクリプション、インストール、および起動操作は、テスト期間を通じて均等に分散されました。 これにより、実世界のユーザー行動のシミュレーションが提供されました。 テストの最後にセッションはログアウトされました。 既存ユーザーワークロードのログオン要求には、認証要求のみが含まれました。

ワークロード

ユーザーワークロードは以下のように定義されます。

ユーザーセッション/デバイス	各セッションのNetScaler Gatewayログオン、列挙、デバイス登録などが含まれます。
Worx Storeの起	ユーザーがWorx Storeを複数回起動し、そのたびに、モバイルアプリ（Web/SaaS/MDX）かWindows

動	アプリ（HDX）かを問わず、複数のアプリをサブスクライブつまりインストールします。
デバイスあたりのWeb/SaaSアプリのSSO	XenMobileでSSOが完了して実際のアプリのURLを返すまでの、Web/SaaSアプリの起動シーケンスです。 実際のアプリにトラフィックは送信されませんでした。
デバイスあたりのMDXアプリのダウンロード	MDXアプリのダウンロード数です（これはWorx Storeの起動中いつでも発生する可能性があります）。 iOSの場合、Apple ITMSからのアプリの自動インストールが含まれます。これにより、NetScaler Gateway上で新しいトークン/tmsサービスAPIが活用されます。

注記と前提

XenMobileのデバイスを30,000台以上に拡張するには、以下のサーバーパラメーターを調整する必要があります。

Configファイル - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/push_services.xml

-

Configファイル - /opt/sas/sw/tomcat/inst1/webapps/ROOT/WEB-INF/classes/ew-config.properties

- ios.mdm.apns.connectionPoolSize=15
- hibernate.c3p0.max_size=1000

すべてのXenMobileノードでこれらの変更を行ってから、サーバーを再起動する必要があります。

以下のシナリオはスケーラビリティテストの対象外となります。 これらのシナリオは、今後のスケールテストの機能拡張で検討されます。

- Androidに接続されたデバイスがテストされません。
- パッケージの展開がテストされません。
- Windowsプラットフォームがテストされません。

各XenMobileは最大10,000の接続を同時にサポートします。

テストは、ネットワーク遅延の問題を無視できるように、理想的なLANの条件で行われています。 実際のシナリオでは、特にアプリケーションのダウンロードに関して、スケーラビリティは利用可能なユーザーの帯域幅によっても大きく変わります。

オンボーディング（FTU)ワークロード

オンボーディング（FTU）ワークロードは、XenMobile環境へのユーザーによる初めてのアクセスと定義されます。 このワークロードに含まれる操作は以下のとおりでした。

- 自動検出
- Enrollment
- Authentication
- デバイス登録
- アプリケーションの検出（Web、SaaS、およびモバイルMDXアプリ）
  - アプリケーションのサブスクリプション（画像とアイコンのダウンロードを含む）
  - サブスクライブされたMDXアプリのインストール
- デバイスの状態の確認を含むアプリケーションの起動（Web、SaaS、およびモバイルMDXアプリ）
- ポリシーのプッシュ（iOS）
- 最小限のWorxMailおよびWorxWeb接続（VPNトンネル） — 2接続

- XenMobile経由の必須アプリのインストール

次の表は、ワークロードのパラメーターの定義です。

Devices	デバイス登録	列挙	デバイスあたりのアプリの列挙	デバイスあたりのWorxStoreの起動	デバイスあたりのWeb/SaaSのSSO	デバイスあたりのMDXアプリのダウンロード	XenMobileサーバーによってトリガーされる必須アプリのダウンロード	デバイスあたりのプッシュされるポリシー（iOS）
1000	1000	1000	14	4	4	2	2	2
10000	10000	10000	14	4	4	2	2	2
30000	30000	30000	14	4	4	2	2	2
60000	60000	60000	14	4	4	2	2	2
100000	100000	100000	14	4	4	2	2	2

Worxへの接続のみを使用する既存ユーザーのワークロード

次の表は、既存ユーザー（Worxへの接続のみを使用）のワークロードです。 このワークロードにより、WorxMailおよびWorxWebアプリを使用する1人のユーザーがシミュレートされました。 このシミュレーションを使用して、XenMobile構成内のNetScaler Gatewayのスケーラビリティを測定しました。 この測定が可能になるのは、これら2つのWorxアプリのみを使用することでネットワークの負荷が最小限になるからです。 WorxWebアプリについては、ユーザーは内部Webサイトにアクセスしています。この場合XenMobileサーバーのSSOはトリガーされません。 このモードで含まれる操作は以下のとおりです。

- 認証（NetScaler GatewayとXenMobile）
- WorxMailおよびWorxWeb接続（VPNトンネル） — 4接続

以下の表は既存ユーザーのワークロードパラメーターを示します。

Devices	列挙	デバイスあたりのアプリの列挙	デバイスあたりのVPNトンネル[1]
1000	1000	14	4
10000	10000	14	4
30000	30000	14	4

60000	60000	14	4
100000	100000	14	4

1. VPNトンネルの数は、WorxMailおよびWorxWebの接続の数に対応します。

次の表は、WorxMailおよびWorxWebの接続プロファイルの概要です。

デバイス接続	接続の種類	セッションあたりの送信データ[1]	セッションあたりの受信データ[1]
WorxMail接続 #1	タイプ1[2]	4.1MB	4.1MB
WorxMail接続 #2	タイプ1	6.3MB	12.5MB
WorxWeb接続 #1	タイプ2[3]	5.2MB	15.7MB
WorxWeb接続 #2	タイプ2	4.1MB	3.4MB
セッションあたりの転送バイト合計[1]		～19.7MB	～40.7MB

1.セッションあたり：8時間

タイプ1：長時間の非対称な送信および受信接続（Microsoft Exchangeのメールボックスに対するWorxMailの接続）。

タイプ2：閉じてしばらく待った後で再び開く、非対称な送信および受信接続（WorxWeb接続）

これらの推奨事項は、「中程度」のワークロードを自動化するためのWorxMailおよびWorxWebのプロファイルに基づいて設定されています。 接続の詳細を変更すると解析結果に影響があります。 たとえば、ユーザーあたりの接続数を増やす場合、サポートされるNetScaler Gatewayセッションの数は減少する可能性があります。

WorxMailおよびWorxWebのプロファイル

各アプリで使用するプロファイルは、「非常に高負荷の」ワークロードを自動化することを目的としています。次の表は、WorxMailおよびWorxWebのプロファイルの詳細です。

中程度のワークロードのWorxMailプロファイル

1日あたりの送信メッセージ	20
1日あたりの受信メッセージ	80
1日あたりの読み取りメッセージ	80

1日あたりの削除メッセージ	20
平均メッセージサイズ（KB）	200

中程度のワークロードのWorxWebプロファイル

起動Webアプリ数	10
手動で開くWebページ数	10
Webアプリあたりの平均要求-応答ペア数	100
要求の平均サイズ（バイト）	300
応答の平均サイズ（バイト）	1000

構成とパラメーター

以下の構成を使用してスケーラビリティテストを実行しました。

- NetScaler Gatewayおよび負荷分散（LB）仮想サーバーを同じNetScaler Gatewayアプライアンスに共存させました。
- SSLトランザクションにNetScaler Gateway上の2048ビットキーを使用しました。

終了基準

この解析の基礎はログオン数です。 ログオン数によって、インフラストラクチャコンポーネントおよびコンポーネントそれぞれの構成のガイドラインが提供されます。 ログオン数は、以下のようなエラー発生の余地を考慮に入れたものであることに留意してください。

- 無効な応答
  - ステータスコードが200ではなく401/404の応答は無効とみなされます。
- 要求のタイムアウト
  - 120秒以内に応答があることが期待されます。
- 接続エラー
  - 接続がリセットされます。
  - 接続が突然終了されます。

全体的なエラー率が任意のデバイスから送信される要求数の合計の1%未満であれば、ログオン数は許容可能です。 エラーには、各個別のワークロード操作に対応するエラーはもちろん、CPUやメモリの消費のようなインフラストラクチャコンポーネントの物理的なパフォーマンスにかかわるものも含まれます。

ソフトウェアおよびハードウェアの詳細

以下の表は、これらのテストに使用されたXenMobileインフラストラクチャのソフトウェアを示します。

コンポーネント	バージョン
NetScaler Gateway	11.0-62.10.nc 10.5-57.7.n
XenMobile	10.3.0.824
外部データベース	Microsoft SQL Server 2014

以下のテーブルに示すXenServerプラットフォーム上で、スケーラビリティテストを実行しました。

ベンダー	Genuine Intel
Model	Intel Xeon CPU — E5645 @ 2.40GHz（CPU数24）

これにはインフラストラクチャの中核的なサービス（Active Directory、Windowsドメインネームサービス（DNS）、証明機関、Microsoft Exchangeなど）とXenMobileコンポーネント（XenMobile仮想アプライアンスおよび該当する場合はNetScaler Gateway VPX仮想アプライアンス）が含まれます。

XenMobile Cloudについて

Aug 02, 2016

XenMobile Cloudは、アプリやデバイスでだけでなくユーザーやユーザーグループを管理するためのXenMobile EMM（Enterprise Mobility Management：エンタープライズモビリティ管理）環境を提供する製品サービスです。 XenMobile Cloudを使用することで、CitrixではCitrix Cloud Operationsグループを介してオンサイトのインフラストラクチャの構成とメンテナンスを行うことができます。 このように分離することで、ユーザーエクスペリエンスと、デバイス、ポリシー、アプリ管理それぞれに排他的に取り組むことができます。 また、XenMobile Cloudでは、ライセンスの購入および管理をサブスクリプション料金に置き換えます。

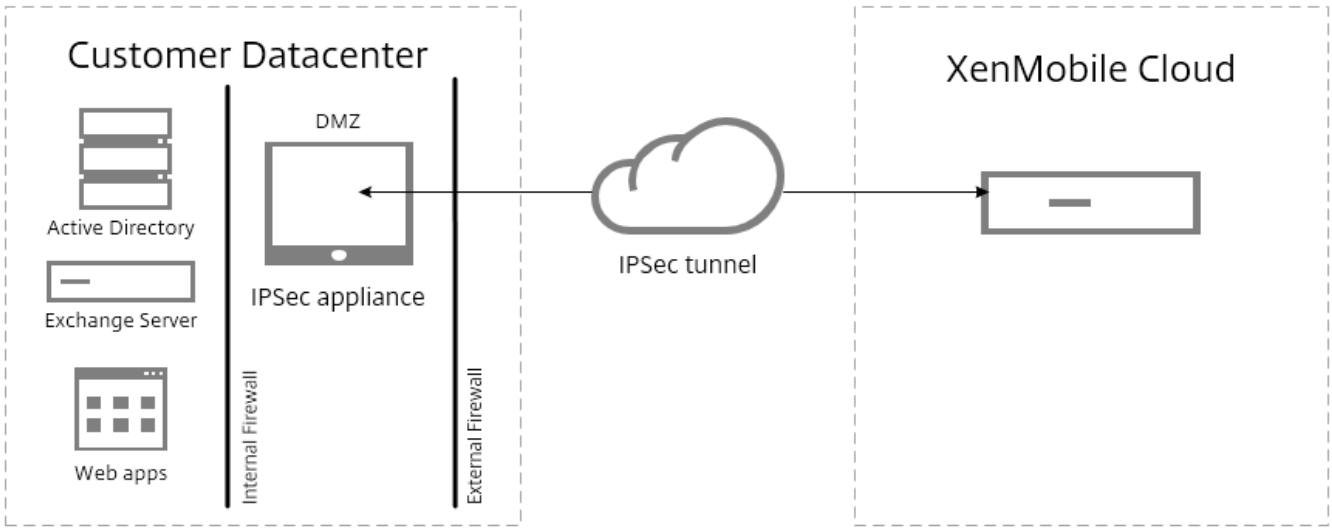
Cloud Operations管理者は、ネットワーク接続のメンテナンスと構成を行うだけでなく、NetScaler、XenApp、XenDesktop、StoreFront、ShareFileなどの各種のCitrix製品を統合します。 クラウド環境は、世界中にあるAmazonデータセンターでホストされ、高パフォーマンス、迅速な応答を実現し、サポートに対応します。

XenMobile Cloudの概要については、https://www.citrix.com/products/xenmobile/tech-info/cloud.htmlを参照してください。

注意

- Remote Support Clientは、XenMobile Cloud Version 10.xのWindows CEおよびSamsung Androidデバイスでは利用できません。
- XenMobile Cloudのサーバー側のコンポーネントは、FIPS 140-2に準拠していません。
- XenMobile Cloudでは、オンプレミスのsyslogサーバーとのsyslog統合はサポートされません。 代わりに、Xen Mobileコンソールの［Support］ページからログをダウンロードできます。 これを行う場合は、 **［Download All］**をクリックしてシステムログを取得する必要があります。 詳しくは、「XenMobileでのログファイルの表示および分析」を参照してください。

XenMobile Cloudの基本アーキテクチャを次の図に示します。詳細なリファレンスアーキテクチャ図は、『XenMobile Deployment Handbook』の、クラウド展開のリファレンスアーキテクチャについてのセクションを参照してください。



XenMobile Cloudアーキテクチャは、Citrix CloudBridgeをインストールおよび展開するか、データセンター内の既存のIPsec

ゲートウェイを使用することで、既存のインフラストラクチャに統合することができます。

また、このアーキテクチャでは、Cloud Operationsグループによって処理されるクラウドと自社のデータセンターのどちらでもNetScalerを使用できます。 データセンターで使用する場合は、NetScalerによって単一の管理ポイントが提供され、ユーザーIDとエンドポイントデバイスの両方に基づいてアクセスを制御しセッション内のアクションを制限できます。 この展開により、アプリケーションのセキュリティ、データ保護、およびコンプライアンス管理が強化されます。

Citrix CloudBridgeをダウンロードおよびインストールするには、https://www.citrix.com/downloads/cloudbridge.htmlを参照してください。

XenMobile Cloudの役割

XenMobile Cloudでは、XenMobileのオンプレミス展開と同じRBAC（Role Based Access Control：役割ベースのアクセス制御）を使用します。 XenMobile Cloudの違いは、Citrix Cloud Operationsグループがプロビジョニングを含む、インフラストラクチャを扱うすべての役割を処理することです。

次の図は、XenMobile CloudのRBACコンソールを示しています。

XenMobileには、システムの機能へのアクセスを論理的に区分するために、4つのデフォルトのユーザー役割が実装されています。 デフォルトの役割は次のとおりです。

- **Administrator**。 システムへのフルアクセスが許可されます。
- **Support**。 リモートサポートへのアクセスが許可されます。
- **User**。 ユーザーに、デバイスを登録できSelf Help Portalを使用できるアクセス権を与えます。
- **Provisioning**。 管理者に、Device Provisioningツールを使用してすべてのWindows Mobile/CEデバイスをグループとしてプロビジョニングする機能を与えます。 この役割は、Cloud Operationグループが処理します。

デフォルトの役割をテンプレートとして使用することもできます。テンプレートをカスタマイズして、デフォルトの役割によって定義されている機能には含まれない特定のシステム機能にアクセスするための権限を持つ、新しいユーザーの役割を作成できます。

役割をユーザー（ユーザーレベルで）や、Active Directoryグループ（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は、すべての権限が統合されてそのユーザーの権限が定義されます。 たとえば、ADGroupAのユーザーがマネージャーのデバイスを検索でき、ADGroupBのユーザーが従業員のデバイスをワイプできる場合、両方のグループに属するユーザーは、マネージャーおよび従業員のデバイスを検索し、ワイプすることができます。

注：ローカルユーザーに割り当てることができる役割は1つだけです。

XenMobileのRBAC機能を使用すると、次のことを実行できます。

- 新しい役割を作成する。
- 役割にグループを追加する。
- ローカルユーザーを役割に関連付ける。

管理者が割り当てることができる役割は次のとおりです。 この一覧にない役割は、Citrix Cloud Operationsグループが処理します。

主なセクション	セクション	ページ	ページを表示できる担当者
Dashboard	すべて	すべて	IT管理者
管理	Devices	すべて	IT管理者
管理	Enrollment	すべて	IT管理者
構成	デバイスポリシー	すべて	IT管理者
構成	Apps	すべて	IT管理者
構成	操作	すべて	IT管理者
構成	デリバリーグループ	すべて	IT管理者
構成	設定	証明書	クラウド管理者、IT管理者
構成	設定	通知テンプレート	IT管理者
構成	設定	Role Based Access Control	クラウド管理者、IT管理者
構成	設定	Enrollment	IT管理者
構成	設定	Local Users and Groups	クラウド管理者、IT管理者
構成	設定	Release Management	クラウド管理者、IT管理者
構成	設定	ワークフロー	IT管理者
構成	設定	資格情報プロバイダー	IT管理者

構成	設定	PKIエンティティ	IT管理者
構成	設定	クライアントのプロパティ	IT管理者
構成	設定	NetScaler Gateway	クラウド管理者のみ、またはIT管理者のみ
構成	設定	キャリアSMSゲートウェイ	IT管理者
構成	設定	通知サーバー	クラウド管理者、IT管理者
構成	設定	ActiveSync Gateway	IT管理者
構成	設定	iOS VPP	IT管理者
サポート	Log Operations	ログ設定	クラウド管理者、IT管理者、技術サポート
構成	設定	サーバープロパティ	クラウド管理者、IT管理者、技術サポート
構成	設定	Google Play資格情報	IT管理者
構成	設定	LDAP	IT管理者
構成	設定	ネットワークアクセス制御	IT管理者
サポート	Support Bundle	サポートバンドルの作成	クラウド管理者、技術サポート
構成	設定	iOSデバイス登録プログラム	IT管理者
構成	設定	Mobile Service Provider	IT管理者
構成	設定	Samsung KNOX	IT管理者
構成	設定	XenApp/ XenDesktop	IT管理者
構成	設定	ShareFile	IT管理者
サポート	詳細設定	クラスター情報	クラウド管理者、技術サポート

サポート	詳細設定	ガーベジコレクション	クラウド管理者、技術サポート
サポート	詳細設定	Javaメモリプロパティ	クラウド管理者、技術サポート
サポート	詳細設定	マクロ	IT管理者
FTU Wizard	Initial Configuration	NetScaler Gateway	クラウド管理者のみ、またはIT管理者のみ
構成	設定	Worx Home Support	IT管理者
構成	設定	Worx Store Branding	IT管理者
サポート	Diagnostics	NetScaler Gatewayの接続確認	クラウド管理者、IT管理者、技術サポート
サポート	Diagnostics	XenMobileの接続確認	クラウド管理者、IT管理者、技術サポート
サポート	Log Operations	ログ	クラウド管理者、IT管理者、技術サポート
サポート	詳細設定	PKI構成	クラウド管理者、IT管理者
サポート	ツール	APNS署名ユーティリティ	顧客、技術サポート
サポート	ツール	Citrix Insight Services	クラウド管理者、IT管理者、技術サポート
FTU Wizard	Initial Configuration	SSL証明書	クラウド管理者、IT管理者
FTU Wizard	Initial Configuration	LDAP構成	IT管理者
FTU Wizard	Initial Configuration	通知サーバー	クラウド管理者、IT管理者
FTU Wizard	Initial Configuration	概要	クラウド管理者、IT管理者
サポート	Links	Citrix Knowledge Center	クラウド管理者、IT管理者、技術サポート

サポート	ツール	NetScaler Connectorのデバイスステータス	IT管理者
サポート	Log Operations	Log Settings->Log Size	クラウド管理者、技術サポート

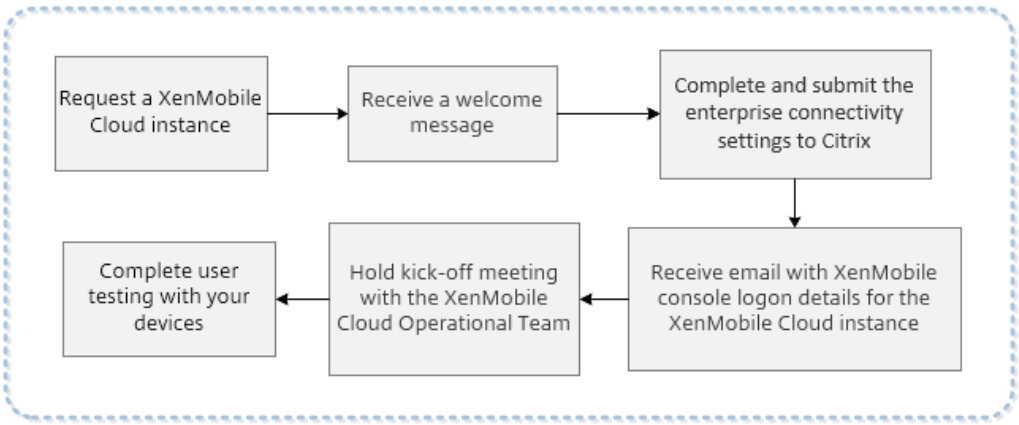
役割をカスタマイズする手順については、「RBACを使用した役割の構成」を参照してください。

サーバーノードの再起動を要求する場合は、技術サポート（https://www.citrix.com/contact/technical-support.html）に連絡してください。

XenMobile Cloudの前提条件および管理

Aug 02, 2016

以下の図に、XenMobile Cloudのインスタンスを申し込んでからユーザーが組織内でデバイスを使ってテストするまでの導入プロセスを構成する手順を示します。 XenMobile Cloudの評価または購入時には、XenMobile Cloudの中核的なサービスが正しく実行され構成されていることを保証するために、XenMobile Cloud運用チームが継続的に導入支援を提供し、コミュニケーションを図ります。



CitrixによりXenMobile Cloudソリューションがホストおよび提供されます。 ただし、XenMobile Cloudのインフラストラクチャを Active Directoryなどの企業サービスに接続するため、一部の通信およびポートの要件を満たす必要があります。 以下のセクションを確認して、XenMobile Cloudの展開に備えます。

XenMobile CloudのIPSecトンネルゲートウェイ

IPSecトンネルであるXenMobile Enterprise Connectorを使用して、Active Directoryなどの企業サービスにXenMobile Cloudインフラストラクチャを接続できます。

アマゾンウェブサービス（AWS）Webサイト（http://aws.amazon.com/vpc/faqs/）の一覧にあるIPsecゲートウェイは、XenMobile Cloudソリューションでテストされており、公式にサポートされます。 「Q： Amazon VPCで機能することが知られているカスタマーゲートウェイ装置にはどのようなものがありますか？」までスクロールして、サポートされるゲートウェイの一覧を参照してください。

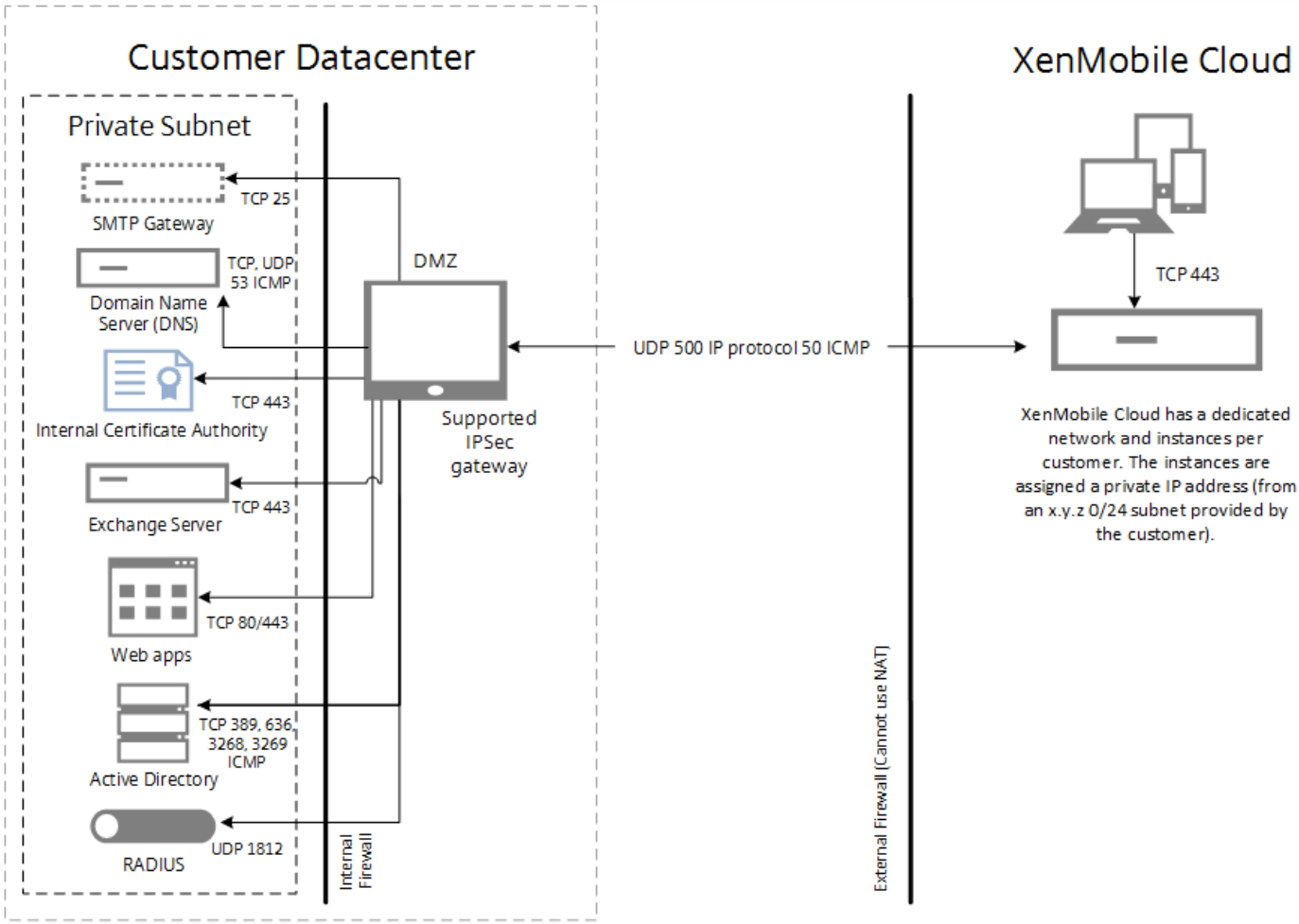
> ## 注意
>
> お使いのIPSecゲートウェイが承認済みリストに記載されていない場合もXenMobile Cloudと連動する可能性がありますが、セットアップに時間がかかったり、フォールバック計画として公式にサポートされるIPSecゲートウェイのいずれかを使用する必要が生じたりする可能性があります。

IPSecゲートウェイには直接IPアドレスを割り当てる必要があり、NAT（Network Address Translation：ネットワークアドレス変換）を使用することはできません。

AWS VPN接続では、永続的なキープアライブをカスタマー側で開始する必要があります。 お使いの環境からAmazon VPCサブネットへの永続的なpingを構成して、サービスの継続性を確保してください。

AWS VPNでは、IPsecゲートウェイで構成された複数のSecurity Associationはサポートされません。 トンネルごとに1つの一意のSecurity Associationペア（受信と送信で1つずつ）に制限されます。 規則とフィルターを統一して、不必要なトラフィックが生じないようにしてください。

以下の図に、XenMobile CloudソリューションでIPsecトンネルを構成して、さまざまなポートから企業サービスに接続する方法を示します。



以下の表は、IPSecトンネルの要件を含めて、XenMobile Cloud展開の通信およびポートの要件を示します。

接続元	接続先	プロトコル	ポート	説明
外部（境界）ファイアウォール – 受信規則				
XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	UPD	500	IPSec IKE構成。

XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	IPプロトコルID	50	IPSec ESPプロトコル。
XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	ICMP		トラブルシューティング用（セットアップ後に削除可能）。
外部（境界）ファイアウォール – 送信規則				
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	UDP	500	IPSec IKE構成。
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	IPプロトコルID	50、51	IPSec ESPプロトコル。
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	ICMP		トラブルシューティング用（セットアップ後に削除可能）。
内部ファイアウォール – 受信規則				
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内の内部DNSサーバー	TCP、UPP、ICMP	53	DNS解決。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のActive Directoryドメインコントローラー	LDAP（TCP）	389、636 3268、3269	ドメインコントローラーに対するユーザーのActive Directory認証およびディレクトリクエリ用。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のActive Directoryドメインコントローラー	ICMP		トラブルシューティング用（セットアップ全体の完了後に削除可能）。

未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のExchangeサーバー	SMTP（TCP）	25	オプション。XenMobileメール通知用。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のExchangeサーバー	HTTP、HTTPS（TCP）	80、443	ActiveSyncトラフィックがデバイスから（IPSecトンネル経由で）XenMobile Cloudインフラストラクチャを介してExchangeサーバーに送信される場合は、Exchange ActiveSyncが必要です。 ユーザーデバイスが、XenMobile IPSecトンネル経由でExchangeサーバーに接続する必要がなく、インターネット経由でパブリックなActiveSync FQDNと通信する場合は、これは不要です。
未使用でルーティング可能な顧客の/24サブネット[2]	イントラネット/Webサーバー、SharePointサーバーなどのアプリケーションサーバー	HTTP、HTTPS（TCP）	80、443	XenMobile IPSecトンネル経由の、イントラネットおよび/またはアプリケーションサーバーへのユーザーモバイルデバイスからのアクセス。 各アプリケーションサーバーを、アプリケーションにアクセスするために必要なポート番号（通常ポート80および/または443）と共にファイアウォール規則に追加する必要があります。
未使用でルーティング可能な顧客の/24サブネット[2]	PKIサーバー（オンプレミスPKIを使用する場合）	HTTPS（TCP）	443	オプション（XenMobile POCでは使用しません）： これは、XenMobile CloudインフラストラクチャとMicrosoft CAのようなオンプレミスPKIインフラストラクチャを統合して、XenMobileソリューションに証明書ベースの認証を設定するために活用できます。

未使用でルーティング可能な顧客の/24サブネット[2]	RADIUSサーバー	UDP	1812	オプション（XenMobile POCでは使用しません）： これは、XenMobileソリューションに2要素認証を設定するために使用できます。
内部ファイアウォール - 送信規則				
顧客の内部サブネット。このサブネットからXenMobileコンソールを使用可能にする必要があります。	未使用でルーティング可能な顧客の/24サブネット[2]	TCP	4443	XenMobile Cloudインフラストラクチャ内のXenMobile App Controller（MAM）コンソール。

[1]XenMobile CloudインスタンスおよびIPSecコンポーネントがXenMobile Cloudインフラストラクチャ内にプロビジョニングされるときに、XenMobile Cloudチームから提供されます。

[2]プロビジョニングプロセスの一環として顧客から提供される未使用の/24サブネット。このサブネットは顧客のデータセンター内の内部サブネットと競合せず、ルーティング可能です。

ユーザーのモバイルデバイス上のネイティブなメールクライアントからのメール接続を禁止または許可する機能など、ネイティブメールフィルタリングのためにXenMobile Mail ManagerまたはXenMobile NetScaler Connectorを展開することを計画している場合は、以下の追加要件を確認します。

XenMobile Apple APNS証明書

XenMobile Cloud展開でiOSデバイスを管理することを計画している場合は、Apple APNS証明書が必要です。 XenMobile Cloudソリューションを展開する前に証明書を準備する必要があります。 手順については、「APNS証明書の要求」を参照してください。

WorxMail for iOSのプッシュ通知証明書

WorxMail展開でプッシュ通知を活用したい場合は、iOS WorxMailのプッシュ通知のためにApple APNS証明書を準備する必要があります。 詳しくは、「WorxMail for iOSのプッシュ通知」を参照してください。

XenMobile MDX Toolkit

MDX Toolkitは、XenMobileを伴う安全な展開のためにアプリを準備する、アプリのラッピング技術です。 Citrix WorxMail、WorxNotes、QuickEditなどのアプリをラップするには、MDX Toolkitをインストールする必要があります。 詳しくは、「MDX Toolkitについて」を参照してください。

iOSアプリをラップする計画をしている場合は、必要なApple配布プロファイルを作成するためにApple開発者アカウントが必

要です。 詳しくは、MDX Toolkitのシステム要件およびApple Developer Webサイトを参照してください。

Windows Phone 8.1向けアプリをラップする計画をしている場合は、システム要件を参照してください。

Windows Phone登録のためのXenMobile自動検出

Windows Phone 8.1の登録のためにXenMobile自動検出を活用したい場合は、パブリックなSSL証明書を利用できるようにします。 詳しくは、「XenMobileでのユーザー登録の自動検出の有効化」を参照してください。

XenMobileコンソール

XenMobile Cloudソリューションでは、オンプレミスのXenMobile展開と同じWebコンソールを利用します。 このようにして、ポリシー管理、アプリ管理、デバイス管理などの日々のCloudソリューションの管理を、オンプレミスのXenMobile展開と同じ方法で行います。 XenMobileコンソールでのアプリおよびデバイスの管理について、「XenMobileコンソールの概要」を参照してください。

XenMobileデバイス登録

さまざまなデバイスプラットフォームに対するXenMobile登録オプションについては、「ユーザーとデバイスの登録」を参照してください。

XenMobileサポート

XenMobileコンソールでサポートされる関連情報およびツールにアクセスする方法について詳しくは、 「XenMobileのサポートおよび保守」を参照してください。

XenMobile Cloudにおけるモバイルプラットフォームのサポート

Aug 02, 2016

XenMobile Cloudインスタンスを申し込んだ後で、Android、iOS、およびWindowsプラットフォームのサポートの準備を開始できます。 お使いの環境に該当する手順を完了した後は、情報を手元に置いておき、XenMobileコンソールで設定を構成するときに使用できるようにします。

これらの要件は、XenMobile Cloudの導入プロセスを構成する全体的な通信およびポート要件の一部であることに注意してください。 詳しくは、「XenMobile Cloudの前提条件および管理」を参照してください。

Android

- Google Play資格情報を作成します。 詳しくは、Google Playの「Getting Started with Publishing」を参照してください。
- Android for Work管理者アカウントを作成します。 詳しくは、「XenMobileでのAndroid for Workによるデバイスの管理」を参照してください。
- Googleでのドメイン名を検証します。 詳しくは、「Verify your domain for Google Apps」を参照してください。
- APIを有効にしてAndroid for Workのサービスアカウントを作成します。 詳しくは、「Google for Work | Android」を参照してください。

iOS

- Apple IDおよび開発者アカウントを作成します。 詳しくは、Apple Developer Program Webサイトを参照してください。
- Appleプッシュ通知サービス（APNs）証明書を作成します。 詳しくは、Apple Push Certificates Portalを参照してください。
- Volume Purchase Program（VPP）の企業トークンを作成します。 詳しくは、「Apple Volume Purchasing Program」を参照してください。

Windows

- Microsoft Windowsストア開発者アカウントを作成します。 詳しくは、「Microsoft Windows Dev Center」を参照してください。
- Microsoft Windowsストア発行元IDを入手します。 詳しくは、「Microsoft Windows Dev Center」を参照してください。
- Symantecからエンタープライズ証明書を入手します。 詳しくは、「Microsoft Windows Dev Center」を参照してください。
- アプリケーション登録トークン（AET）を作成します。 詳しくは、「Microsoft Windows Dev Center」を参照してください。

システム要件

Oct 25, 2016

XenMobile 10.3を使用するには、以下のシステム環境が必要です。

- 以下のいずれかのサーバーオペレーティングシステム
  - XenServer（サポートされるバージョン：6.5.xまたは6.2.x）。詳細は「XenServer」を参照してください。
  - VMware（サポートされるバージョン：ESXi 5.1、ESXi 5.5、またはESXi 6.0）。詳しくは「VMware」を参照してください。 ESXi 6.0はXenMobile 10.3.xでのみサポートされます。
  - Hyper-V（サポートされるバージョン：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2）。詳しくは「Hyper-V」を参照してください。
- デュアルコアプロセッサ
- 4つの仮想CPU
- 8GBのRAM
- 50GBのディスクスペース

デバイスの数が10,000台以上の場合は以下の構成が推奨されます。

- ノードごとに8GBのRAM搭載のクアッドコアプロセッサ

バージョン10.3.xのXenMobileでは、Citrixライセンスサーバー11.12.1以降が必要です。

NetScaler Gatewayのシステム要件

XenMobile 10.3と共にNetScaler Gatewayを使用するには、以下のシステム環境が必要です。

- 以下のいずれかのサーバーオペレーティングシステム
  - XenServer（サポートされるバージョン：6.2.x、6.1.x、または6.0.x）
  - VMWare（サポートされるバージョン：ESXi 4.1、ESXi 5.1、ESXi 5.5、ESXi 6.0）
  - Hyper-V（サポートされるバージョン：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2）
- 2つの仮想CPU
- 2GBのRAM
- 20GBのディスクスペース

また、Active Directoryと通信できる必要があり、これにはサービスアカウントが必要です。 クエリおよび読み取りアクセス権限のみが必要です。

XenMobile 10.3のデータベース要件

XenMobileでは、次のいずれかのデータベースが必要です。

- Microsoft SQL Server

  XenMobileリポジトリでは、サポート対象バージョンのいずれかで稼動しているMicrosoft SQL Serverデータベースをサポートします（Microsoft SQL Serverデータベースについて詳しくは、「Microsoft SQL Server」を参照してください）。

  Microsoft SQL Server 2016
  Microsoft SQL Server 2014
  Microsoft SQL Server 2012
  Microsoft SQL Server 2008 R2
  Microsoft SQL Server 2008

XenMobile 10.1では、SQL ServerのAlwaysOn可用性グループがサポートされます。

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

注：XenMobileで使用される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。 SQL Serverのサービスアカウントについて詳しくは、Microsoft Developer Networkのサイトで以下のページを参照してください（以下のリンクからSQL Server 2014の情報にアクセスできます。 別のバージョンを使用している場合は、 **[Other Versions]** の一覧で適切なサーバーのバージョンを選択してください）。

サーバー構成 - サービスアカウント

Windowsのサービスアカウントと権限の構成

Server-Levelの役割

- PostgreSQL

  PostgreSQLはXenMobileに含まれます。 ローカルまたはリモートで使用できます。

  注： XenMobileの全エディションがRemote PostgreSQL 9.3.11 for Windowsをサポートしますが、次の制限事項があります。

  - サポートできるのは最大300台のデバイス

    300台を超える場合は、オンプレミスのSQL Serverを使用します。

  - クラスタリングはサポートしない

StoreFrontの互換性

StoreFront 3.6
StoreFront 3.5
StoreFront 3.0
StoreFront 2.6
Web Interface 5.4
XenApp/XenDesktop 7.9
XenApp/XenDesktop 7.8
XenApp/XenDesktop 7.7
XenApp/XenDesktop 7.6
XenApp/XenDesktop 7.5
XenApp 6.5

XenMobile 10.3のメールサーバーの要件

XenMobile 10.3では、以下のメールサーバーがサポートされます。

- Exchange 2016
- Exchange 2013
- Exchange 2010

XenMobileの互換性

Aug 02, 2016

連係可能なXenMobileコンポーネントの概要については、「XenMobileの互換性」を参照してください。

サポート対象のデバイスプラットフォーム

Aug 02, 2016

エンタープライズモビリティ管理についてXenMobile 10.xでサポートされるデバイスの完全な一覧については、「XenMobileでサポートされるデバイスプラットフォーム」を参照してください。

ポート要件

Oct 25, 2016

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

アプリケーションを管理するNetScaler GatewayおよびXenMobile用のポートの開放

ユーザーがWorx Home、Citrix Receiver、およびNetScaler Gateway Plug-inからNetScaler Gateway経由でXenMobile、StoreFront、XenDesktop、XenMobile NetScaler Connector、およびイントラネットWebサイトなどのそのほかの内部ネットワークリソースに接続できるようにするには、次のポートを開く必要があります。 NetScaler Gatewayについて詳しくは、NetScaler Gatewayのドキュメントの「Configuring Settings for Your XenMobile Environment」を参照してください。
NSIP（NetScaler IP）、VIP（Virtual Server IP：仮想サーバーIP）、SNIP（Subnet IP：サブネットIP）などのNetScaler所有のIPアドレスについて詳しくは、NetScalerのドキュメントの「How a NetScaler Communicates with Clients and Servers」を参照してください。

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

389	セキュリティで保護されないLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはMicrosoft Active Directory
443	Citrix ReceiverからStoreFrontへの接続またはReceiver for WebからXenAppおよびXenDesktopへの接続に使用されます。	Internet	NetScaler Gateway
	Web、モバイル、およびSaaSアプリケーションの配信のためのXenMobileへの接続に使用されます。	Internet	NetScaler Gateway
	デバイスとXenMobileサーバー間での一般的な通信に使用されます。	XenMobile	XenMobile
	登録のためにモバイルデバイスからXenMobileへの接続に使用されます。	Internet	XenMobile
	XenMobileからXenMobile NetScaler Connectorへの接続に使用されます。	XenMobile	XenMobile NetScaler Connector
	XenMobile NetScaler ConnectorからXenMobileへの接続に使用されます。	XenMobile NetScaler Connector	XenMobile
	証明書認証を行わない環境のコールバックURLに使用されます。	XenMobile	NetScaler Gateway
514	XenMobileとsyslogサーバー間の接続に使用されます。	XenMobile	Syslogサーバー
636	セキュリティで保護されるLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはActive Directory
1494	内部ネットワーク内のWindowsベースのアプリケーションへのICAコネクションに使用されます。 このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway	XenAppまたはXenDesktop
1812	RADIUS接続に使用されます。	NetScaler Gateway	RADIUS認証サーバー

2598	セッション画面の保持を使用した内部ネットワーク内のWindowsベースのアプリケーションへの接続に使用されます。 このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway	XenAppまたはXenDesktop
3268	Microsoft Global Catalogのセキュリティで保護されないLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはActive Directory
3269	Microsoft Global Catalogのセキュリティで保護されるLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはActive Directory
9080	NetScalerとXenMobile NetScaler Connector間のHTTPトラフィックに使用されます。	NetScaler	XenMobile NetScaler Connector
9443	NetScalerとXenMobile NetScaler Connector間のHTTPSトラフィックに使用されます。	NetScaler	XenMobile NetScaler Connector
45000 80	2つのXenMobile VMがクラスターで展開されている場合にそれらのVM間の通信に使用されます。	XenMobile	XenMobile
8443	登録、XenMobile Store、モバイルアプリケーション管理（MAM）に使用されます。	XenMobile NetScaler Gateway Devices Internet	XenMobile
4443	管理者がブラウザーを使用してXenMobileコンソールにアクセスする場合に使用されます。	アクセスポイント（ブラウザー）	XenMobile
	XenMobileの1つのクラスターノードからすべてのクラスターノードに関するログとサポートバンドルをダウンロードするために使用されます。	XenMobile	XenMobile
27000	外部のCitrixライセンスサーバーへのアクセスに使用されるデフォルトポート。	XenMobile	Citrixライセンスサーバー
7279	Citrixライセンスのチェックインおよびチェックアウトに使用されるデフォルトポート。	XenMobile	Citrixベンダーデーモン

デバイスを管理するXenMobileポートの開放

XenMobileがネットワーク内で通信できるようにするには、次のポートを開く必要があります。

TCPポート	説明	接続元	接続先
25	XenMobile通知サービスのデフォルトのSMTPポート。 SMTPサーバーで別のポートを使用する場合は、そのポートがファイアウォールによってブロックされないことを確認してください。	XenMobile	SMTPサーバー
80、443	Apple iTunes App Store（ax.itunes.apple.com）、Google Play（80を使用する必要があります）、またはWindows Phone StoreへのEnterprise App Store接続。 iOS上のCitrix Mobile Self-Serve、Worx Home for Android、またはWorx Home for Windows Phoneを介してアプリケーションストアからアプリケーションを公開するために使用されます。	XenMobile	Apple iTunes App Store（ax.itunes.apple.comおよび*.mzstatic.com） Apple Volume Purchase Program（vpp.itunes.apple.com） Windows Phoneの場合：login.live.comおよび*.notify.windows.com Google Play（play.google.com）
80または443	XenMobileとNexmo SMS Notification Relay間の送信接続に使用されます。	XenMobile	Nexmo SMS Relay Server
389	セキュリティで保護されないLDAP接続に使用されます。	XenMobile	LDAP認証サーバーまたはActive Directory
443	AndroidおよびWindows Mobileの登録およびエージェント設定に使用されます。	Internet	XenMobile
	AndroidおよびWindowsデバイス、XenMobile Webコンソール、およびMDM Remote Support Clientの登録およびエージェント設定に使用されます。	内部LANおよびWiFi	
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 Server
2195	iOSデバイスの通知およびデバイスポリシー	XenMobile	インターネット（パブリックIPア

	のプッシュのためのgateway.push.apple.comへのApple Push Notificationサービス（APNs）送信接続に使用されます。		ドレス17.0.0.0/8を使用しているAPNsホスト）
2196	iOSデバイスの通知およびデバイスポリシーのプッシュのためのfeedback.push.apple.comへのAPNs送信接続に使用されます。		
5223	Wi-FiネットワークのiOSデバイスから*.push.apple.comへのAPNs送信接続に使用されます。	WiFiネットワークのiOSデバイス	インターネット（パブリックIPアドレス17.0.0.0/8を使用しているAPNsホスト）
8081	オプションのMDM Remote Support Clientからアプリトンネルに使用されます。 デフォルトは8081です。	Remote Support Client	インターネット。ユーザーデバイスのアプリトンネル用（AndroidとWindowsのみ）
8443	iOSおよびWindows Phoneデバイスの登録に使用されます。	Internet LANおよびWiFi	XenMobile

自動検出サービスの接続のポート要件

このポート構成により、Worx Home for Androidのバージョン10.2および10.3から接続するAndroidデバイスで内部ネットワークからCitrix ADS（Auto Discovery Service：自動検出サービス）にアクセスできることを保証します。 ADSを介して利用可能なセキュリティ更新プログラムをダウンロードするとき、ADSにアクセスする能力は重要です。

注：ADS接続はプロキシサーバーと連動しない可能性があります。 このシナリオでは、ADS接続がプロキシサーバーをバイパスすることを可能にします。

証明書ピンニングの有効化に関心がある場合は、以下の前提条件となる作業を行う必要があります。

- **XenMobileサーバーとNetScalerの証明書を収集します**。 証明書はPEM形式で、秘密キーではなく公開証明書である必要があります。
- **Citrixサポートに証明書ピンニングの有効化を依頼します**。 このプロセスで、証明書の提出を求められます。

証明書ピンニングに追加された機能向上のため、デバイスは登録前にADSに接続する必要があります。 これにより、デバイスを登録する環境の最新のセキュリティ情報がWorx Homeで利用できることを保証します。 Worx HomeはADSに接続できないデバイスを登録しません。 したがって、内部ネットワーク内でADSアクセスを可能にすることは、デバイスの登録を有効にするために重要です。

Worx Home 10.2 for AndroidにADSへのアクセスを許可するには、以下のFQDNおよびIPアドレスのポート443を開放します。

FQDN	IP address
	54.225.219.53

discovery.mdm.zenprise.com	54.243.185.79 107.22.184.230 107.20.173.245 184.72.219.144 184.73.241.73 54.243.233.48 204.236.239.233 107.20.198.193

FIPS 140-2への準拠

Aug 02, 2016

米国立標準技術研究所（National Institute of Standards and Technologies：NIST）が発行しているFIPS（Federal Information Processing Standard：米国の情報処理標準）は、セキュリティシステムで使用される暗号化モジュールのセキュリティ要件を規定しています。 FIPS 140-2はこの標準の2つ目のバージョンです。 NIST検証済みFIPS 140モジュールについて詳しくは、http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdfを参照してください。

重要：XenMobile FIPSモードは、初回インストール時にのみ有効化できます。
注：HDXアプリケーションが使用されない限り、XenMobileモバイルデバイス管理のみ、XenMobileモバイルアプリケーション管理のみ、およびXenMobileエンタープライズはすべてFIPSに準拠しています。
iOSでは、すべての保存データおよび転送中データの暗号化操作で、OpenSSLおよびAppleにより提供されたFIPS認定済み暗号化モジュールが使用されます。 Androidでは、すべての保存データの暗号化操作およびモバイルデバイスからNetScaler Gatewayへのすべての転送中データの暗号化操作で、OpenSSLにより提供されたFIPS認定済み暗号化モジュールが使用されます。

Windows RT、Microsoft Surface、Windows 8 Pro、およびWindows Phone 8では、モバイルデータ管理（MDM）のためのすべての保存データおよび転送中データの暗号化操作で、Microsoftによって提供されたFIPS認定済み暗号化モジュールが使用されます。

XenMobileでは、すべての保存データおよび転送中データの暗号化操作で、OpenSSLにより提供されたFIPS認定済み暗号化モジュールが使用されます。 モバイルデバイスとNetScaler Gateway間では、モバイルデバイスについて上述した暗号化操作を組み合わせて、MDMフローのためのすべての保存データおよび転送中データがFIPS準拠の暗号化モジュールをエンドツーエンドで使用します。

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

MDXアプリケーションはWindows Phone 8.1でサポートされ、Windows Phone 8上でFIPS準拠の暗号化ライブラリおよびAPIを使用します。 Windows Phone 8.1上のMDXアプリケーションのすべての保存データおよびWindows Phone 8.1デバイスとNetScaler Gateway間のすべての転送中のデータは、これらのライブラリとAPIを使って暗号化されます。

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

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

XenMobileの言語サポート

Oct 25, 2016

Citrix WorxアプリケーションおよびXenMobileコンソールは英語以外の言語での使用にも適応しています。 これには、アプリケーションがユーザーの優先言語にローカライズされていない場合でも、英語以外の文字およびキーボード入力のサポートが含まれます。 全Citrix製品のグローバル化サポートについて詳しくは、http://support.citrix.com/article/CTX119253を参照してください。

Worxモバイルアプリの言語サポート

言語ごとに対応しているアプリを○で示します。 現在、Secure Formsは英語のみに対応しています。

iOS						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
日本語	○	○	○	○	○	○
簡体字中国語	○	○	○	○	○	○
繁体字中国語	○	○	○	○	○	○
フランス語	○	○	○	○	○	○
ドイツ語	○	○	○	○	○	○
スペイン語	○	○	○	○	○	○
韓国語	○	○	○	○	○	○
ポルトガル語	○	○	○	○	○	○
オランダ語	○	○	○	○	○	○
イタリア	○	○	○	○	○	○

語						
デンマーク語	○	○	○	○	○	○
スウェーデン語	○	○	○	○	○	○
ヘブライ語	○	○	○	○	○	○
アラビア語	○	○	○	○	○	○

Android						
	Worx Home	**WorxMail**	**WorxWeb**	**WorxNotes**	**WorxTasks**	**QuickEdit**
日本語	○	○	○	○	○	○
簡体字中国語	○	○	○	○	○	○
繁体字中国語	○	○	○	○	○	
フランス語	○	○	○	○	○	○
ドイツ語	○	○	○	○	○	○
スペイン語	○	○	○	○	○	○
韓国語	○	○	○	○	○	○
ポルトガ	○	○	○	○	○	○

ル語						
オランダ語	○	○	○	○	○	○
イタリア語	○	○	○	○	○	○
デンマーク語	○	○	○	○	○	○
スウェーデン語	○	○	○	○	○	○
ヘブライ語	○	○	○	○	○	
アラビア語	○	○	○	○	○	

Windows			
	Worx Home	**WorxMail**	**WorxWeb**
フランス語	○	○	○
ドイツ語	○	○	○
スペイン語	○	○	○
イタリア語	○	○	○
デンマーク語	○	○	○
スウェーデン語	○	○	○

Citrix製品のローカライズ状況については、Citrix Knowledge Centerを参照してください。

XenMobileコンソールの言語サポート

XenMobileコンソールは、簡体中国語、ドイツ語、フランス語、韓国語、およびポルトガル語に対応しています。

Right-to-Leftサポート

次の表では、アプリごとに中東地域言語の編集についてのサポート状況を示しています。 プラットフォームごとに使用可能な機能について○で示しています。

アプリ	iOS	Android	Windows Phone
Worx Home	○	○	
WorxMail	○	○	
WorxWeb	○	○	
WorxTasks	○	○	
WorxNotes	○	○	
QuickEdit	○	○	

インストール前のチェックリスト

Aug 02, 2016

このチェックリストを使用して、XenMobileをインストールするための前提条件と設定を記録できます。 各タスクまたは注には、要件が適用されるコンポーネントまたは機能を示す列があります。 インストール手順については、「XenMobileのインストール」を参照してください。

ネットワークの基本的な接続

以下はXenMobileソリューションに必要なネットワーク設定です。

•	前提条件または設定	コンポーネントまたは機能	設定の記録
	リモートユーザーが接続する完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を記録します。	XenMobile NetScaler Gateway	
	パブリックおよびローカルIPアドレスを記録します。 ネットワークアドレス変換（Network Address Translation：NAT）を設定するためのファイアウォールの構成にはこれらのIPアドレスが必要です。	XenMobile NetScaler Gateway	
	サブネットマスクを記録します。	XenMobile NetScaler Gateway	
	DNS IPアドレスを記録します。	XenMobile NetScaler Gateway	
	WINSサーバーのIPアドレスを記録します（該当する場合）。	NetScaler Gateway	
	NetScaler Gatewayのホスト名を調べて記録します。 注：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されたサーバー証明書に含まれます。 NetScaler Gatewayのインストールウィザードを使用してホスト名を構成できます。	NetScaler Gateway	
	XenMobileのIPアドレスを記録します。	XenMobile	

前提条件または設定	コンポーネントまたは機能	設定の記録
XenMobileのインスタンスを1つインストールする場合は、IPアドレスを1つ予約します。 クラスターを構成する場合は、必要なすべてのIPアドレスを記録します。 ● NetScaler Gateway上で構成された1つのパグリックIPアドレス ● NetScalser Gateway用の1つの外部DNSエントリ	NetScaler Gateway	
Webプロキシサーバーの IPアドレス、ポート、プロキシホストの一覧、および管理者のユーザー名とパスワードを記録します。 ネットワークにプロキシサーバーを展開する場合は、これらの設定はオプションです（該当する場合）。 注：Webプロキシのユーザー名を構成するときには、sAMAccountNameまたはユーザープリンシパル名（User Principal Name：UPN）のいずれかを使用できます。	XenMobile NetScaler Gateway	
デフォルトゲートウェイのIPアドレスを記録します。	XenMobile NetScaler Gateway	
システムIP（NSIP）アドレスとサブネットマスクを記録します。	NetScaler Gateway	
サブネットIP（SNIP）アドレスとサブネットマスクを記録します。	NetScaler Gateway	
NetScaler Gatewayの仮想サーバーIPアドレスとFQDNを証明書から記録します。 複数の仮想サーバーを構成する必要がある場合は、証明書からすべての仮想IPアドレスとFQDNを記録します。	NetScaler Gateway	
ユーザーがNetScaler Gatewayを通してアクセスできる内部ネットワークを記録します。 例：10.10.0.0/24 分割トンネリングが［On］に設定されているとき、ユーザーがWorx HomeまたはNetScaler Gateway Plug-inと接続するときにアクセスする必要のあるすべての内部ネットワークおよびネットワークセグメントを入力します。	NetScaler Gateway	
XenMobileサーバー、NetScaler Gateway、外部Microsoft SQL Server、およびDNSサーバーの間のネットワーク接続が到達可能であることを確認します。	XenMobile NetScaler Gateway	

ライセンス管理

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

•	ソフトウェア	コンポーネント	場所を記録します。
	ユニバーサルライセンスをCitrix Webサイトから入手します。 詳しくは、NetScaler Gatewayのライセンスのページを参照してください。	NetScaler Gateway XenMobile Citrixライセンスサーバー	

証明書

XenMobileおよびNetScaler Gatewayは、ほかのCitrix製品およびアプリケーションと接続するため、およびユーザーデバイスから接続するために、証明書が必要です。 詳しくは、「XenMobileでの証明書」を参照してください。

✓	ソフトウェア	コンポーネント	注
	必要な証明書を入手してインストールします。	XenMobile NetScaler Gateway	

ポート

XenMobileコンポーネントと通信できるように、ポートを開く必要があります。 開く必要があるポートの完全な一覧については、「XenMobileのポート要件」を参照してください。

✓	ソフトウェア	コンポーネント	注
	XenMobile用にポートを開きます。	XenMobile NetScaler Gateway	

データベース

データベース接続を構成する必要があります。 XenMobileリポジトリでは、サポート対象バージョン（Microsoft SQL Server 2014、SQL Server 2012、SQL Server 2008 R2、SQL Server 2008）のいずれかで稼動しているMicrosoft SQL Serverデータベースが必要です。 Citrixでは、Microsoft SQLをリモートで使用することをお勧めします。 XenMobileにはPostgreSQLが付属しており、ローカルまたはリモートで、テスト環境においてのみ使用する必要があります。

•	ソフトウェア	コンポーネント	設定の記録
	Microsoft SQL ServerのIPアドレスとポート。 XenMobileで使用されるSQL Serverのサービスアカウントに、DBcreator役割の権限があることを確認します。	XenMobile	

Active Directoryの設定

	ソフトウェア	コンポーネント	設定の記録
	Active Directoryのプライマリサーバーおよびセカンダリサーバーの IPアドレスおよびポートを記録します。 ポート636を使用する場合は、CAから取得したルート証明書をXenMobileにインストールし、［Use secure connections］オプションを［Yes］に変更します。	XenMobile NetScaler Gateway	
	Active Directoryドメイン名を記録します。	XenMobile NetScaler Gateway	
	Active Directoryサービスアカウントを記録します。ユーザーID、パスワード、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のクエリに使用するアカウントです。	XenMobile NetScaler Gateway	
	ユーザーベースDNを記録します。 これはユーザーを検索するディレクトリレベルです。たとえば、cn=users,dc=ace,dc=comです。NetScaler GatewayおよびXenMobileは、Active Directoryのクエリにこれを使用します。	XenMobile NetScaler Gateway	
	グループベースDNを記録します。 これはグループが置かれるディレクトリのレベルです。 NetScaler GatewayおよびXenMobileは、Active Directoryのクエリにこれを使用します。	XenMobile NetScaler Gateway	

XenMobileとNetScaler Gatewayの間の接続

	ソフトウェア	コンポーネント	設定の記録
	XenMobileのホスト名を記録します。	XenMobile	
	XenMobileのFQDNまたはIPアドレスを記録します。	XenMobile	
	ユーザーがアクセスできるアプリケーションを確認します。	NetScaler Gateway	

	ワイルドカードURLを記録します。	XenMobile コンポーネント	設定の記録

ユーザー接続：XenDesktop、XenApp、およびWorx Homeへのアクセス

NetScalerのQuick Configurationウィザードを使用して、XenMobileとNetScaler Gatewayの間、XenMobileとWorx Homeの間の接続設定を構成することをお勧めします。 第2の仮想サーバーを作成し、ReceiverおよびWebブラウザーからWindowsベースアプリケーションおよびXenAppおよびXenDesktopの仮想デスクトップにユーザーがアクセスできるようにします。同様に、NetScalerのQuick Configurationウィザードを使用して、これらの設定を構成することをお勧めします。

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

XenMobileのインストール

Oct 25, 2016

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

始める前に：XenMobileの展開の計画では、多くの検討事項があります。 エンドツーエンドXenMobile環境の推奨事項、よくある質問、およびユースケースについては、『XenMobile展開ハンドブック』を参照してください。 また、「XenMobile 10.3のシステム要件」と「XenMobileインストールチェックリスト」を参照してください。

> **注意**
>
> XenMobileはハイパーバイザーの時刻を使用するので、NTPサーバーまたは手動による構成を使用して、ハイパーバイザーの時刻が正しく構成されていることを確認してください。

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

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

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

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

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

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

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

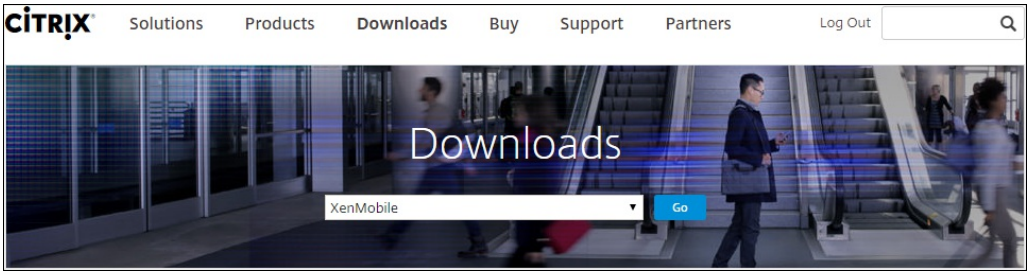
FIPS 140-2モード：XenMobile ServerをFIPSモードでインストールしようとする場合は、「XenMobileでのFIPSの構成」で説明されている一連の前提条件を完了させる必要があります。

XenMobile製品ソフトウェアのダウンロード

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

XenMobileのソフトウェアをダウンロードするには

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



5. ［Go］をクリックします。 ［XenMobile］ページが開きます。
6. ［XenMobile 10］を展開します。
7. ［XenMobile 10.0 Server］をクリックします。
8. ［XenMobile 10.0 Server］の各エディションのページで、XenServer、VMware、またはHyper-VにXenMobileをインストールするために使用する適切な仮想イメージの横の［Download］をクリックします。
9. 画面に表示される指示に従って、ソフトウェアをダウンロードします。

NetScaler Gatewayのソフトウェアをダウンロードするには

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

1. Citrixの Webサイトに移動します。
2. CitrixのWebサイトにログオンしていない 場合は、［Search］ボックスの横の［Log On］をクリックしてアカウントにログオンします。
3. ［Downloads］タブをクリックします。
4. ［Downloads］ページの製品一覧で、［NetScaler Gateway］を選択します。
5. ［Go］をクリックします。 ［NetScaler Gateway］ページが開きます。
6. ［NetScaler Gateway］ページで、実行するNetScaler Gatewayのバージョンを展開します。
7. ［Firmware］の下で、ダウンロードするアプライアンスソフトウェアのバージョンを選択します。
   注：ここで［Virtual Appliances］をクリックしてNetScaler VPXをダウンロードすることもできます。 この場合、対象のハイパーバイザーを選択するためのページが開きます。
8. ダウンロードするアプライアンスソフトウェアのバージョンを選択します。
9. ダウンロードするバージョンのアプライアンスソフトウェアの ページで、 適切な仮想アプライアンスの[ダウンロード］をクリックします。
10. 画面に表示される指示に従って、ソフトウェアをダウンロードします。

初回使用時のXenMobileの構成

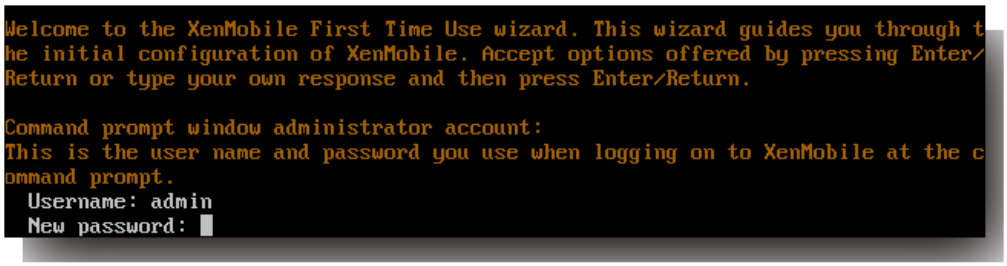
初回使用時のXenMobileの構成プロセスは2つの部分から成ります。

1. XenCenterまたはvSphereのコマンドラインコンソールを使用して、XenMobileのIPアドレスやサブネットマスク、デフォルトゲートウェイ、DNSサーバーなどを構成します。
2. XenMobile管理コンソールにログオンし、初回ログオン画面の手順に従います。

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

コマンドプロンプトウィンドウでのXenMobileの構成

1. XenMobile仮想マシンをCitrix XenServer、Microsoft Hyper-V、またはVMware ESXiにインポートします。 詳しくは、XenServer、Hyper-V、またはVMwareのドキュメントを参照してください。
2. ハイパーバイザーで、インポートしたXenMobile仮想マシンを選択してコマンドプロンプトビューを起動します。 詳しくは、ハイパーバイザーのドキュメントを参照してください。
3. ハイパーバイザーのコンソールページから、コマンドプロンプトウィンドウでXenMobileの管理者のユーザー名とパスワードを入力して管理者アカウントを作成します。
   重要：
   コマンドプロンプトで作成する管理者アカウント、公開キー基盤（PKI）サーバー証明書、およびFIPSのパスワードを作成または変更すると、XenMobileでは以下の規則をActive Directoryユーザーを除くすべてのユーザーに適用します。Active DirectoryユーザーのパスワードはXenMobileの外部で管理されます。
   - パスワードは8文字以上にして、以下の複雑度の条件のうち3つ以上を満たす必要があります。
     - 大文字（A～Z）
     - 小文字（a～z）
     - 数字（0～9）
     - 特殊文字（!、#、$、%など）



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

4. 以下のネットワーク情報を入力して「y」と入力して設定を確定します。
   1. IP address
   2. ネットマスク
   3. デフォルトゲートウェイ
   4. プライマリDNSサーバー
   5. セカンダリDNSサーバー（オプション）

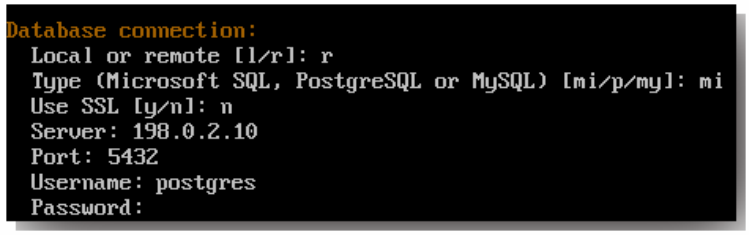
注：この図および後の図に示されているアドレスは使用されておらず、例示のみを目的としています。

5. 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「y」を入力して、セキュリティを高めるためにランダムな暗号化パスフレーズを生成するか、「n」を入力して独自のパスフレーズを指定します。 Citrixでは、「y」を入力してランダムなパスフレーズを生成することをお勧めします。 このパスフレーズは、機密データを保護するために使用される暗号化キーの保護手段の1つとして使用されます。 サーバーのファイルシステムに保存されたパスフレーズのハッシュが、データの暗号化と復号化でキーを取得するときに使用されます。 このパスフレーズを表示することはできません。

   注：環境を拡張して追加のサーバーを構成する場合は、独自のパスフレーズを指定する必要があります。 ランダムなパスフレーズを選択した場合、パスフレーズを表示する方法はありません。

6. 任意で、FIPS（Federal Information Processing Standard）を有効化します。 FIPSについて詳しくは、「XenMobileのFIPS 140-2への準拠」を参照してください。 また、「XenMobileでのFIPSの構成」で説明されている一連の前提条件を完了させる必要があります。

7. 以下の情報を入力してデータベース接続を構成します。



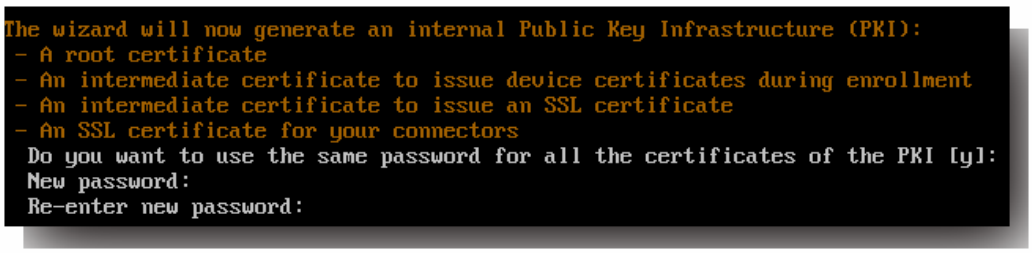
   1. データベースはローカルでもリモートでも構いません。 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「l」、リモートの場合は「r」を入力します。
   2. データベースの種類を選択します。 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「mi」、PostgreSQLの場合は「p」を入力します。
      重要：
      - Citrixでは、Microsoft SQLをリモートで使用することをお勧めします。 XenMobileにはPostgreSQLが付属しており、ローカルまたはリモートで、テスト環境においてのみ使用する必要があります。
      - データベースの移行はサポートされていません。 テスト環境で作成したデータベースを実稼働環境に移行することはできません。
   3. オプションとして、「y」を入力してデータベースでSSL認証を使用します。
   4. 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1つのホストサーバーで、デバイス管理サービスとアプリケーション管理サービスの両方を提供します。
   5. 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。 デフォルトのMicrosoft SQL用ポートは1433で、PostgreSQL用のポートは5432です。

6. データベース管理者のユーザー名を入力します。
7. データベース管理者のパスワードを入力します。
8. データベース名を入力します。
9. Enterキーを押してデータベース設定を確定します。

8. オプションとして、「y」を入力してXenMobileノードまたはインスタンスのクラスター化を有効にします。
   重要：XenMobileクラスターを有効にする場合は、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、システム構成を完了した後でポート80を必ず開放してください。 この操作は、すべてのクラスターノード上で完了する必要があります。
9. XenMobileサーバーの完全修飾ドメイン名（FQDN）を入力します。

10. Enterキーを押して設定を確定します。
11. 通信ポートを指定します。 ポートおよびその使用方法について詳しくは、「XenMobileのポート要件」を参照してください。
    注：Enterキー（Macの場合はReturnキー）を押して、デフォルトポートをそのまま使用します。

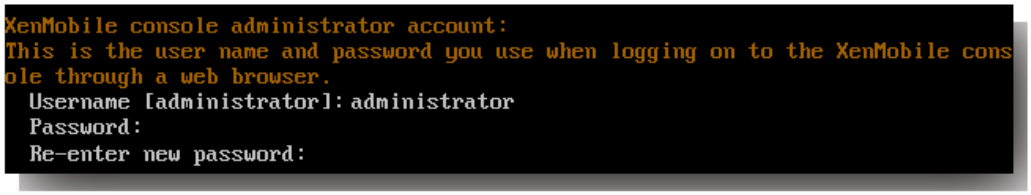
12. 初めてXenMobileをインストールしているので、以前のXenMobileリリースからのアップグレードに関する次の質問をスキップします。
13. 公開キー基盤（PKI）の各証明書に同じパスワードを使用する場合は「y」を入力します。 XenMobile PKI機能について詳しくは、「XenMobileでの証明書のアップロード」を参照してください。



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

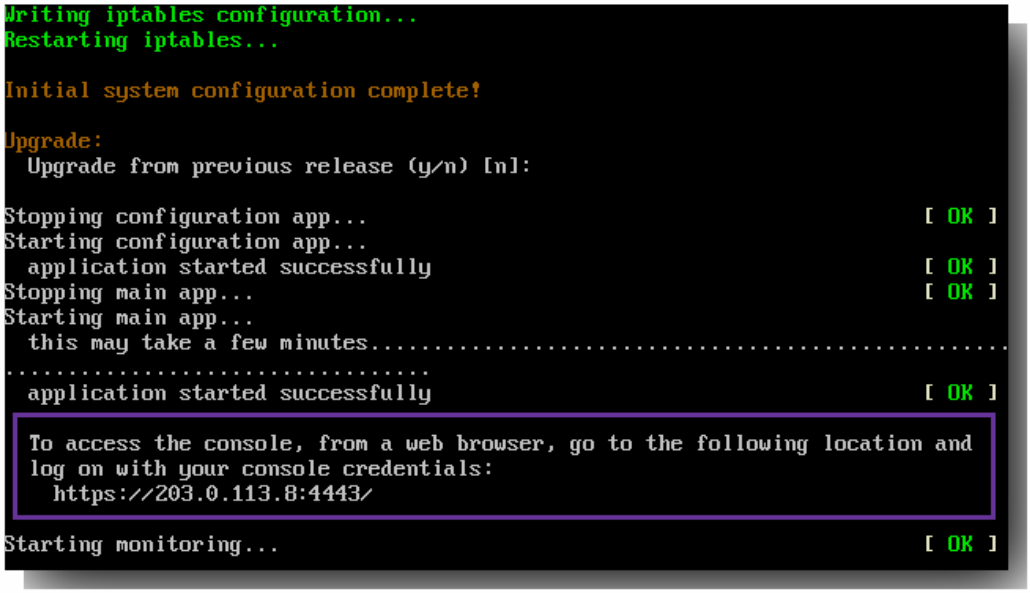
14. 新しいパスワードを入力し、確認のために新しいパスワードを再入力します。
    注：新しいパスワードを入力するとき、アスタリスクなどの文字は表示されません。 何も表示されません。

15. Enterキーを押して設定を確定します。
16. Webブラウザーを使用してXenMobileコンソールにログオンするための管理者アカウントを作成します。 これらの資格情報は後で使用するため、忘れないようにしてください。



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

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



WebブラウザーでのXenMobileの構成

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

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

3. ［Get Started］ページで［Start］をクリックします。［Licensing］ページが開きます。
4. ライセンスを構成します。XenMobileには30日間有効な評価版ライセンスが付属しています。ライセンスの追加と構成、および有効期限切れ通知の構成について詳しくは、「XenMobileのライセンス」を参照してください。
   重要：XenMobileのクラスターノード（インスタンス）を追加してXenMobileクラスタリングを使用する場合は、リモートサーバー上でCitrixライセンスサーバーを使用する必要があります。
5. ［Certificate］ページで、［Import］をクリックします。［Import］ダイアログボックスが開きます。
6. APNとSSLリスナー証明書をインポートします。証明書の取り扱いについて詳しくは、「XenMobileでの証明書」を参照してください。
   注：この手順にはサーバーの再起動が伴います。
7. 環境が該当する場合は、NetScaler Gatewayを構成します。NetScaler Gatewayの構成について詳しくは、「NetScaler GatewayとXenMobile」および「Configuring Settings for Your XenMobile Environment」を参照してください。
   注：
   - 組織の内部ネットワーク（またはイントラネット）の境界にNetScaler Gatewayを展開して、内部ネットワークのサーバー、アプリケーション、およびそのほかのネットワークリソースへの安全な単一のアクセスポイントを提供できます。この展開では、すべてのリモートユーザーが、内部ネットワークの任意のリソースにアクセスする前に、NetScaler Gatewayに接続する必要があります。
   - NetScaler Gatewayはオプションの設定ですが、ページでのデータ入力後にそのページから移動するには、必須フィールドを消去するか入力する必要があります。
8. Active Directoryからのユーザーとグループにアクセスするため、LDAP構成を完了します。LDAP接続の構成について詳しくは、「LDAP構成」を参照してください。
9. 通知サーバーを構成して、ユーザーにメッセージを送信できるようにします。通知サーバー構成について詳しくは、「XenMobileでの通知」を参照してください。

XenMobileでのFIPSの構成

Aug 02, 2016

XenMobileの米国の情報処理標準（FIPS：Federal Information Processing Standards）モードは、 すべての暗号化操作に対してFIPS 140-2証明済みライブラリを使用するようにサーバーを構成して、米国政府のカスタマーをサポートします。 XenMobileサーバーをFIPSモードでインストールすると、すべての静止データおよびXenMobileクライアントとサーバーの両方でやり取りされるデータをFIPS 140-2に完全に準拠させることができます。

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

- XenMobileデーターベースには外部のSQL Server 2012またはSQL Server 2014を使用する必要があります。 またSQL Serverをセキュアな SSL通信用に構成する必要があります。 SQL Serverに対するセキュアなSSL通信の構成手順については、「SQL Server Books Online」を参照してください。
- セキュアSSL通信を実行するには、SQL ServerにSSL証明書をインストールする必要があります。 SSL証明書は、商用CAの公開証明書または内部CAの自己署名証明書のいずれかにすることができます。 SQL Server 2014はワイルドカード証明書を受け付けることはできません。 そのため、SQL ServerのFQDN付きSSL証明書を要求することをお勧めします。
- SQL Serverに自己署名証明書を使用する場合、自己署名証明書を発行したルートCA証明書をコピーする必要があります。 ルートCA証明書は、インストール中にXenMobileサーバーにインポートされる必要があります。

FIPSモードの構成

FIPSモードは、XenMobileサーバーの初回セットアップ時にのみ有効にできます。 インストールが完了したら、FIPSを有効にはできません。 そのため、FIPSモードの使用を予定している場合は、XenMobileサーバーを最初からFIPSモードでインストールする必要があります。 またさらに、XenMobileクラスターがある場合は、すべてのクラスターノードでFIPSを有効にする必要があります。FIPSと非FIPS XenMobileサーバーを同じクラスター内に混在させることはできません。

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

1. セットアップ時に**FIPSモード**を有効にします。

2. SQL Server用のルートCA証明書をアップロードします。 SQL Serverで公開証明書ではなく自己署名SSL証明書を使用した場合は、このオプションについては **[Yes]** を選択して、次のいずれかを実行します。

    a. CA証明書をコピーして貼り付けます。

    b. CA証明書をインポートします。 CA証明書をインポートするには、XenMobileサーバーからHTTP URLを介してアクセスできるWebサイトに証明書を送信する必要があります。 詳しくは、このアーティクルで後述している「証明書のインポート」を参照してください。

3. SQL Serverのサーバー名とポート、SQL Serverにログインするための資格情報、およびXenMobileに対して作成するデータベース名を指定します。

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

4. Active Directoryアカウントを使用するには、「ドメイン\ユーザー名」形式で資格情報を入力します。

5. これらの手順が完了したら、XenMobileの初期セットアップを実行します。

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

証明書のインポート

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

SQLの前提条件

1. XenMobileからSQLインスタンスの接続をセキュリティで保護し、SQL Serverのバージョンは2012または2014が必要です。接続の保護については、「How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console」を参照してください。

2. サービスが適切に再開しない場合は、**Services.msc**を開いて次のようにチェックします。

    a. SQL Serverサービスで使用されたログオンアカウント情報をコピーします。

    b. SQL ServerでMMC.exeを開きます。

    c. ［**ファイル**］>［**スナップインの追加と削除**］の順に選択し、証明書アイテムをダブルクリックして証明書スナップインを追加します。 ウィザードの2つのページでコンピューターアカウントとローカルコンピューターを選択します。

    d. ［**OK**］をクリックします。

    e. ［**証明書（ローカルコンピューター）**］>［**個人**］>［**証明書**］の順に選択し、インポートされたSSL証明書を探します。

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

    g. ［**グループ名またはユーザー名**］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にはフルコントロールと読み取り権限のどちらもが付与されますが、秘密キーの読み取りだけが必要です。

    j. **MMC**を閉じ、SQLサービスを開始します。

3. SQLサービスが正常に開始されたか確認します。

インターネットインフォメーションサービス（IIS）の前提条件

1. ルート証明書（base 64）をダウンロードします。

2. ルート証明書をIISサーバー上のデフォルトの場所（C:\inetpub\wwwroot）にコピーします。

3. デフォルサイトに対して［**Authentication**］チェックボックスをオンにします。

4. ［**Anonymous**］を［**enabled**］に設定します。

5. ［**Enable report branding**］チェックボックスをオンにします。

6. .cerがブロックされていないか確認します。

7. ローカルサーバーのInternt Explorerブラウザーで.cerの場所を参照します（http://localhost/certname.cer）。 ルート証明書テキストがブラウザーに表示されます。

8. ルート証明書がInternet Explorerブラウザーに表示されない場合、ASPがIISで有効化次のようにして確認します。

   a. Server Managerを開きます。

   b. **[管理]** > **[役割と機能の追加]** の順に移動します。

   c. サーバーの役割で、 **[Webサーバー（IIS）]** 、 **[Webサーバー]** 、 **[アプリケーション開発]** の順に展開して **[ASP]** を選択します。

   d. **[次へ]** をクリックしてインストールを完了させます。

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

詳しくは、「Internet Information Services (IIS) 8.5」を参照してください。

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

初期FIPS構成中のルート証明書のインポート

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

- FIPSの有効化：はい
- ルート証明書のアップロード：はい
- コピー（c）またはインポート（i）：i
- インポートするHTTP URLの入力：http://cert.cer
- サーバー：
- 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：選択した名前。

XenMobileのアップグレード

Oct 25, 2016

XenMobileの新しいバージョンや重要な更新が利用可能になるとCitrix.comに公開され、各ユーザーレコードの連絡先に通知が送信されます。 使用しているバージョンに応じて、XenMobileのアップグレードには主に次の3つの選択肢があります。

- **XenMobile 9.0からのアップグレード** - MDM Edition、App Edition、およびEnterprise Edition
  まず、アップグレードツールを使用してXenMobile 10.1にアップグレードする必要があります。このツールは、Citrix.comのダウンロードページからダウンロードできます。 アップグレードツールの使用について詳しくは、「XenMobileのアップグレード」を参照してください。

  XenMobile 9からXenMobile 10.1にアップグレードして、その後、更新プログラムをXenMobile 10.3.xにインストールする場合、アップグレードツールの最新バージョンで、次の種類のデバイスのデータを移行できるようになりました。

  Windows CE
  Windows 10 Phone
  Windows 10タブレット

  アップグレードツールの現在のリリースでは、Multi-Tenant Console（MTC）がXenMobile 9.0で有効になっている場合、MTCで管理されているXenMobile 9インスタンスをスタンドアロンのXenMobile 10インスタンスに移行できます。 XenMobile 10ではMTCはサポートされないため、アップグレードしたインスタンスは個別に管理する必要があります。 詳しくは、「MTCテナントサーバーからXenMobile 10.1へのアップグレード」を参照してください。

- **XenMobile 10.1からXenMobile 10.3.xにアップグレードするには**
  この記事の説明に従って、XenMobileコンソールで **[Release Management]** ページを使用します。 XenMobile 10.3.xのインストールには、アップグレードツールは使用しません。

- **XenMobile 10.3.xソフトウェア、サービスパック、およびシステムパッチの新しいバージョンをインストールするには**
  この記事の説明に従って、XenMobileコンソールで **[Release Management]** ページを使用します。

Important

- XenMobile 10.1から10.3.xに更新するときに、WorxStoreにカスタム名が設定されている場合は、ストア名をデフォルトの**[Store]** 設定に変更して、この設定をデバイスに展開してから更新する必要があります。そうしなければ、XenMobile 10.3の登録、Worx HomeおよびWorxStoreへのアクセス、iOSデバイスでのアプリの展開中に、カスタムストア名による問題が発生します。 WorxStoreブランド設定について詳しくは、「iOSデバイス用のカスタムWorxStoreブランド設定を作成するには」を参照してください。
- XenMobile 10.3.xにアップグレードした後、XenMobile 10.3.xで以前のリリースで構成したWorxモバイルアプリを更新すると、アプリの設定内容がXenMobileコンソールに表示されなくなります。 これらのアプリの設定を再度編集して構成する必要があります。 アプリを再インストールする必要はありません。 この手順を行う必要があるのは一度だけです。将来の更新でアプリまたはサーバーを更新する場合、値は正常に維持されます。

アップグレードパスの概要

XenMobileサーバーのバージョン	リリース番号	アップグレード先	リリース番号	アップグレードパス	ダウンロード先
App Controller Patch 5を適用済みのXenMobile Server 9	9.0.0.97582	XenMobile Server 10.1	10.1.0.63030	XenMobile Server 9からXenMobile Server 10.1	ダウンロード（App Controller Patch 5とアップグレードツール）
XenMobile Server 10または10.1	10.1.0.63030	XenMobile Server 10.3	10.3.0.824	XenMobile Server 10または10.1から10.3へのアップグレード	ダウンロード
XenMobile Server 10.3	10.3.0.10004、10.3.0.10008、10.3.0.10010、10.3.0.10014、10.3.0.10016、10.3.0.10032、10.3.0.10036	XenMobile Server 10.3 Rollup Patch 3	10.3.0.10048	XenMobile Server 10.3から10.3 Rolling Patch 3へのアップグレード	ダウンロード
XenMobile Server 10.3	10.3.0.x	XenMobile Server 10.3.5	10.3.5.354	XenMobile Server 10.3から10.3.5へのアップグレード	ダウンロード
XenMobile Server 10.3.5	10.3.5.354	Service Pack適用済みのXenMobile Server 10.3.6	10.3.6.310	XenMobile Server 10.3.5から10.3.6へのアップグレード	ダウンロード

XenMobile 10.1またはXenMobile 10.3.xからアップグレードするには

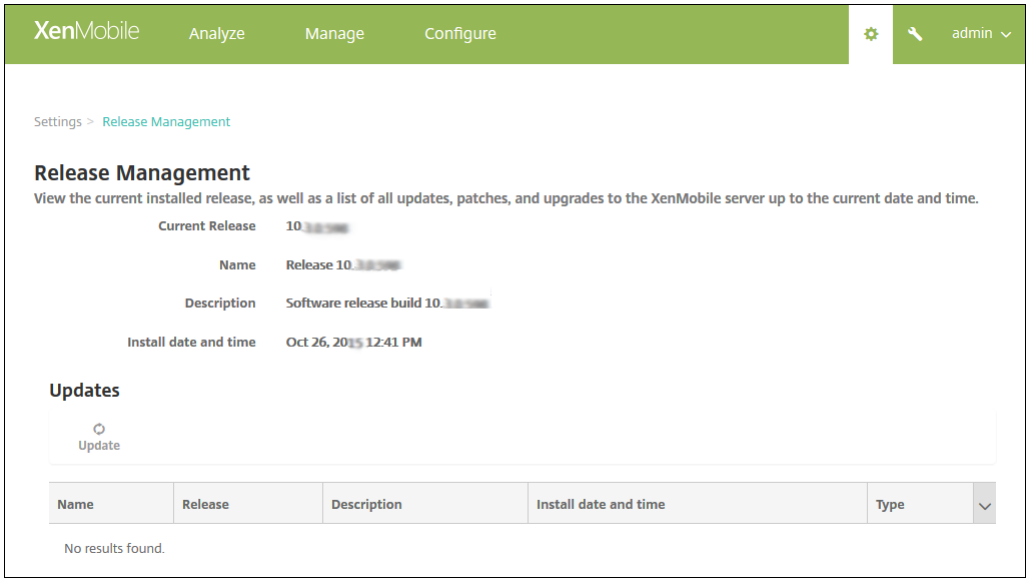
前提条件

- XenMobileの更新をインストールする前に、仮想マシン（VM）の機能を使用して、システムのスナップショットを取得してください。
- 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。
- 更新するバージョンに関しては、「システム要件」を参照してください。 XenMobile 10.3について詳しくは、 必要なシステム環境」を参照してください。

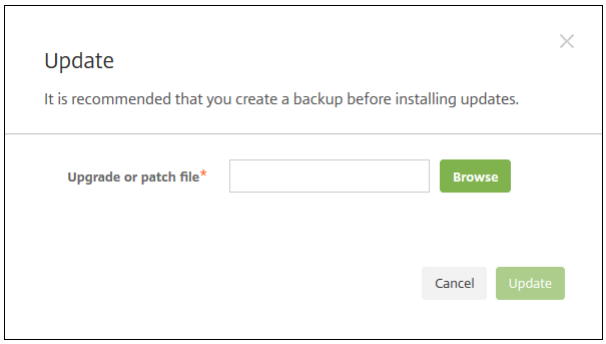
1. Citrix Webサイトのアカウントにログオンして、XenMobile Upgrade（.bin）ファイルを適切な場所にダウンロードします。

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

3. **[Release Management]** をクリックします。 **[Release Management]** ページが開きます。



3. **[Updates]** の下の **[Update]** をクリックします。 **[Update]** ダイアログボックスが開きます。



4. **[Browse]** をクリックしてCitrix.comからダウンロードしたXenMobileアップグレードファイルの場所に移動し、ファイルを選択します。

5. **[Update]** をクリックし、メッセージが表示されたらXenMobileを再起動します。

注：更新プログラムをインストールした後に、XenMobileの再起動が不要な場合もあります。 この場合は、更新プログラムのインストールが成功したことを示すメッセージが表示されます。 ただし、XenMobileの起動が必要な場合は、コマンドラインを使用する必要があります。 システムの再起動後にブラウザーのキャッシュを消去することが重要です。

重要：システムがクラスターモードで構成されている場合は、以下の手順に従って各ノードを更新します。

1. **[Settings]** > **[Release Management]** から、すべてのノードの.binファイルをアップロードします。

2. コマンドラインインターフェイスで、**[Settings]** のすべてのノードをシャットダウンします。

3. 1つのノードを起動し、サービスが実行中であることを確認します。

4. 他のノードを1つずつ起動します。

何らかの理由で更新が正常に完了しなかった場合は、問題を示すエラーメッセージが表示されます。 システムは更新を試行する前の状態に戻ります。

4. ［Browse］をクリックし、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保存した場所に移動して、そのファイルを選択します。

5. ［Update］をクリックし、メッセージが表示されたらXenMobileを再起動します。

注：更新プログラムをインストールした後に、XenMobileの再起動が不要な場合もあります。 この場合は、更新プログラムのインストールが成功したことを示すメッセージが表示されます。 ただし

重要：システムがクラスターモードで構成されている場合は、以下の手順に従って各ノードを更新します。

1. ノードを1つだけ除いてすべてシャットダウンします。
2. そのノードを更新します。
3. サービスが実行されていることを確認してから、次のノードを更新します。

何らかの理由で更新が正常に完了しなかった場合は、問題を示すエラーメッセージが表示されます。 システムは更新を試行する前の状態に戻ります。

4. ［Browse］をクリックし、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保存した場所に移動して、そのファイルを選択します。

5. ［Update］をクリックし、メッセージが表示されたらXenMobileを再起動します。

注：更新プログラムをインストールした後に、XenMobileの再起動が不要な場合もあります。 この場合は、更新プログラムのインストールが成功したことを示すメッセージが表示されます。 ただし

重要：システムがクラスターモードで構成されている場合は、以下の手順に従って各ノードを更新します。

1. ノードを1つだけ除いてすべてシャットダウンします。
2. そのノードを更新します。
3. サービスが実行されていることを確認してから、次のノードを更新します。

何らかの理由で更新が正常に完了しなかった場合は、問題を示すエラーメッセージが表示されます。 システムは更新を試行する前の状態に戻ります。

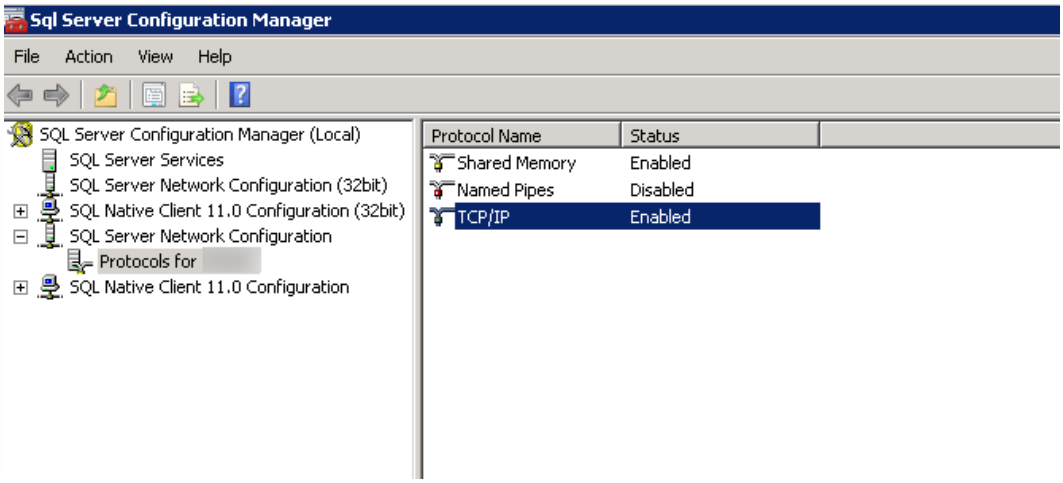
名前付きSQLインスタンスのサポート

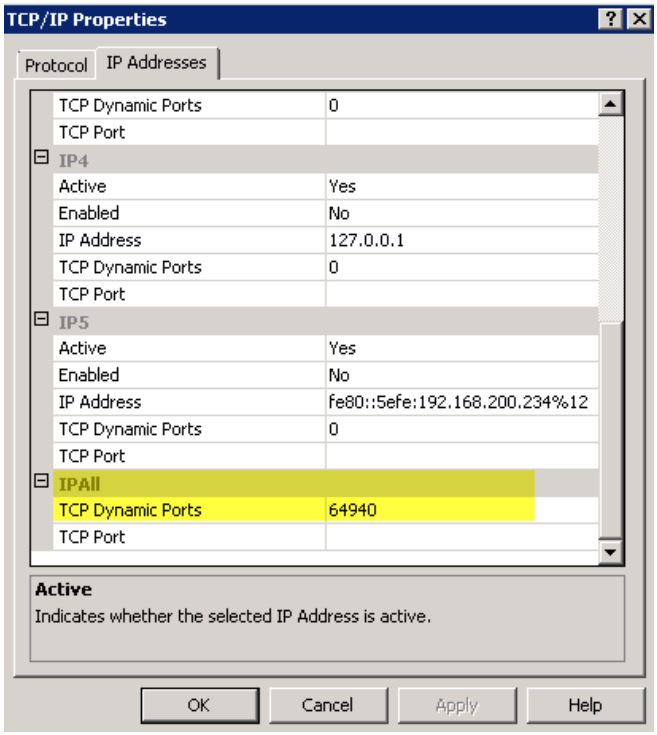
Aug 02, 2016

アップグレードツールを使用して、XenMobile 9.0からXenMobile 10.に、またXenMobile 9.0からXenMobile 10.1アップグレードできます。 XenMobile 9を名前付きSQLインスタンスに基づいて設定する場合は、この設定固有の手順に従う必要があります。 XenMobile 9環境が次の前提条件を満たす場合、このアーティクルの手順に従ってアップグレードを実行します。

- 外部SQL Serverデータベースでセットアップした XenMobile 9 MDM EditionまたはEnterprise Edition。
- 非デフォルトの名前付きインスタンスで実行中のSQL Serverデータベース。
- 静的または動的TCPポートでリスンしているSQL Server名前付きインスタンス。 次の図にあるように、名前付きインスタンスのTCP/IPプロトコルのIPアドレスを見て、この前提条件を確認できます。

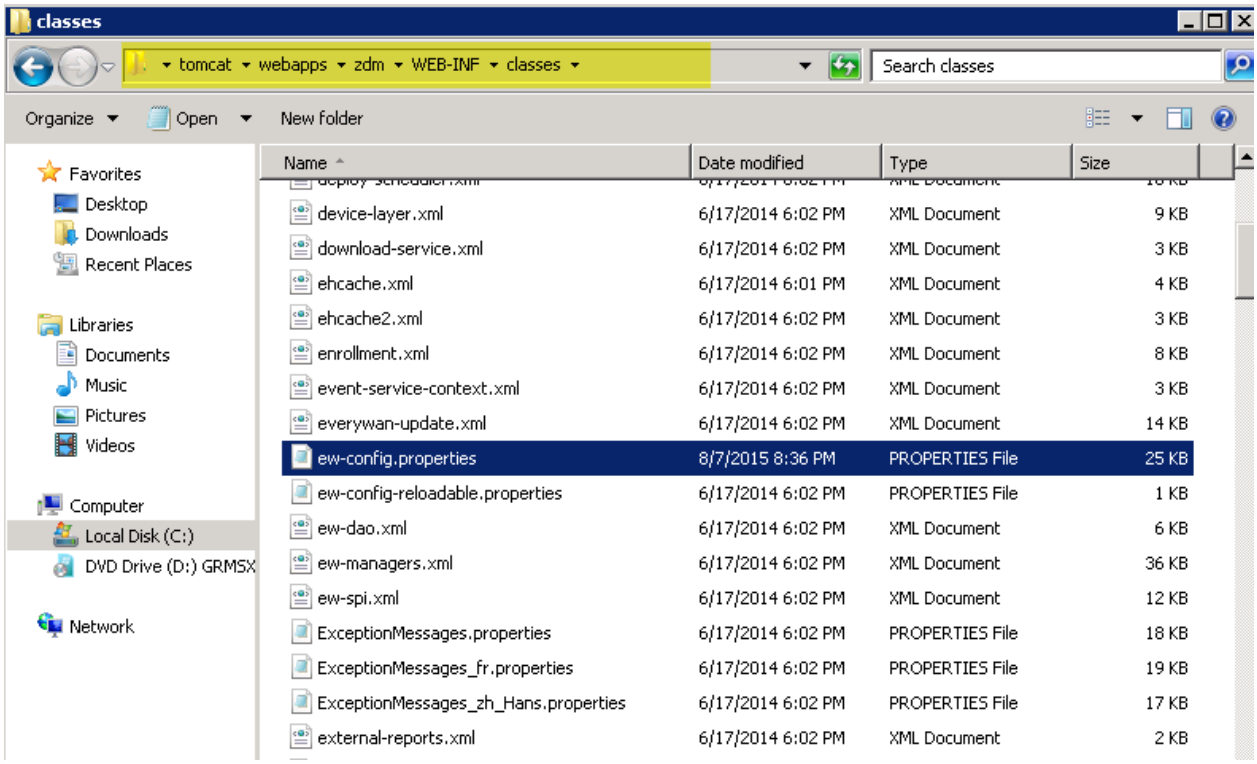
> ## 注意
>
> XenMobileはデータベースに対する持続的なアクセスを必要とするため、SQL Serverデータベースインスタンスは常時静的ポートで実行することをお勧めします。 この接続は、通常ファイヤウォールを介して実行されます。 その結果、ファイアウォールで適切なポートを開く必要があります。つまり、静的ポートで実行中のデータベースインスタンスが必要です。





SQL Server名前付けインスタンスでXenMobileをアップグレードする手順

1. Device Managerインストールディレクトリにアクセスして、ew-config.propertiesファイルを開きます。 このファイルは、tomcat/webapps/zdm/WEB-INF/classesにあります。



2. ew-config.propertiesファイルのDATASOURCE Configurationセクションで次のURLを探します：

pooled.datasource.url= jdbc:jtds:sqlserver:///;instance=

audit.datasource.url= jdbc:jtds:sqlserver:///;instance=

ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234              net/          -llaug;instance=
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          aug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                        ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://ah-234                /          -llaug;instance=
# Audit datasource host name
audit.datasource.hostname=ah-234              .net
# Audit datasource database
audit.datasource.database=          -llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

3. URLからインスタンス名を削除して、SQL Server FQDNの後にポートを追加します。 この場合、64940が必須ポートとなります。

pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

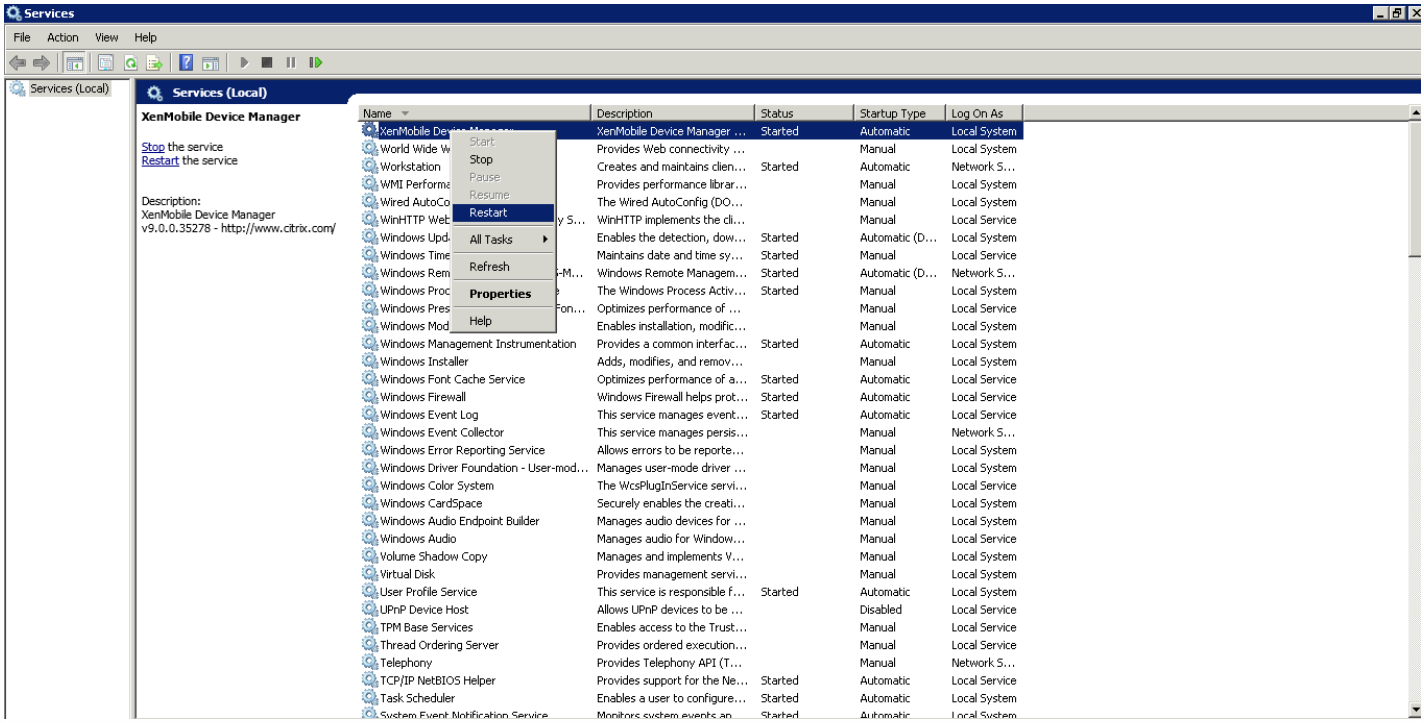
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

> ## 注意
>
> ew-config.propertiesファイルに対する変更についてバックアップ、 コピー、 あるいはメモを取っておくことをお勧めします。 この情報は、移行に失敗した場合に有用です。

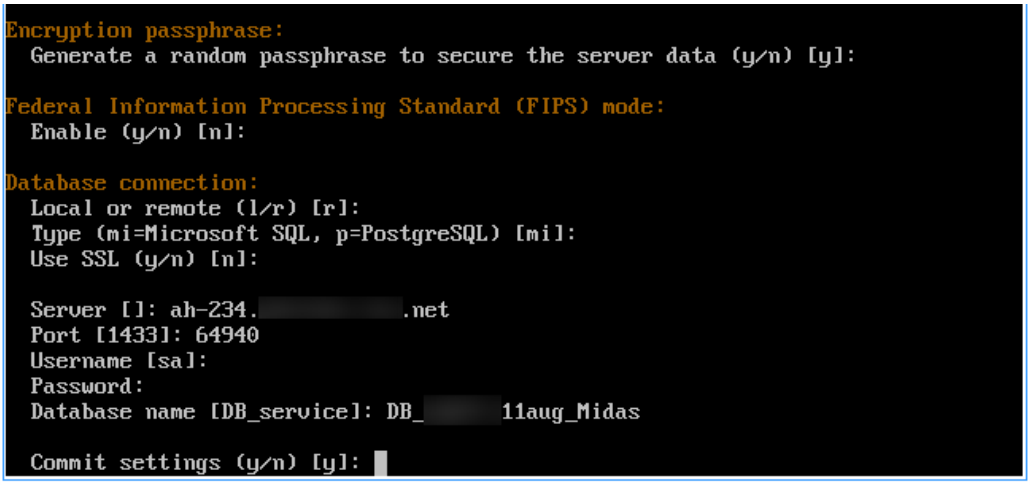
ew-config.properties

```
# For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/everywan
# For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress
# For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/everywan;instance=SQLExpress;domain=sparus-s
# Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@//localhost:1521/everywan
pooled.datasource.url=jdbc:jtds:sqlserver://ah-234.                net:                -llaug
# Pooled datasource host name
pooled.datasource.hostname=ah-234.          .net
# Pooled datasource database
pooled.datasource.database=          -llaug
# Pooled datasource user
pooled.datasource.user=sa
# Pooled datasource password
# For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
pooled.datasource.password={aes}                    ==

# No pooled datasource driver
#no.pooled.datasource.driver=org.postgresql.Driver
# No pooled datasource url
#no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everywan
# No pooled datasource user
#no.pooled.datasource.user=everywan
# No pooled datasource password
#no.pooled.datasource.password=everywan

# Audit datasource driver
audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
# Audit datasource url
audit.datasource.url=jdbc:jtds:sqlserver://                -inc.net:                -llaug
# Audit datasource host name
audit.datasource.hostname=ah-234.          .net
# Audit datasource database
audit.datasource.database=          llaug
# Audit datasource user
audit.datasource.user=sa
# Audit datasource password
```

4. Device Managerサービスを再起動します。 Device Managerインスタンスの応答時にデバイス接続を更新します。



5. 新しいXenMobile 10サーバーもまた名前付きSQLインスタンスと連携する必要があるかどうかを判別します。 必要がある場合、名前付きインスタンスが実行中のポートを識別します。 ポートが動的ポートの場合、それを静的ポートに変換することをお勧めします。その後、新しいXenMobileサーバーでデータベースセットアップの一部として静的ポートを構成します。



6. 次の手順に従って、XenMobile環境のアップグレードを続けます。

XenMobile 9.0のMDMエディション、App Edition、Enterprise EditionをXenMobile 10.1にアップグレードするには、アップグレードツールを使用します。 アップグレードツールはCitrix.comのダウンロードページからダウンロードできます。 詳しくは、「XenMobileのアップグレード」を参照してください。

XenMobile 10のクラスタリングの構成

Aug 02, 2016

XenMobileのバージョン10より前では、Device Managerをクラスターとして、App Controllerを高可用性ペアとして構成していました。 XenMobile 10では、XenMobile 9のDevice ManagerとApp Controllerが統合されました。 バージョン10では、高可用性はXenMobileに適用されなくなっています。 そのため、クラスタリングを構成するには、以下の2つの負荷分散仮想IPアドレスをNetScalerで構成する必要があります。

- **モバイルデバイス管理（MDM）負荷分散仮想IPアドレス**: クラスター内に構成されたXenMobileノードと通信するには、MDM負荷分散仮想IPアドレスが必要です。 この負荷分散はSSLブリッジモードで行われます。
- **モバイルアプリケーション管理（MAM）負荷分散仮想IPアドレス**: クラスター内に構成されたXenMobileノードとNetScaler Gatewayが通信するには、MAM負荷分散仮想IPアドレスが必要です。 XenMobile 10ではデフォルトで、NetScaler Gatewayからのすべてのトラフィックはポート8443で負荷分散仮想IPアドレスにルーティングされます。

この項目の手順では、新しいXenMobile仮想マシン（VM）を作成し、新しいVMを既存のVMに参加させることにより、クラスター設定を作成する方法について説明します。

前提条件

- 必要なXenMobileノードが完全に構成されていること
- MDM Lバンド用の1つの公開IPアドレスとMAM用の1つの公開IPアドレス
- サーバー証明書
- NetScaler Gateway仮想IPアドレス用の1つの空きIPアドレス

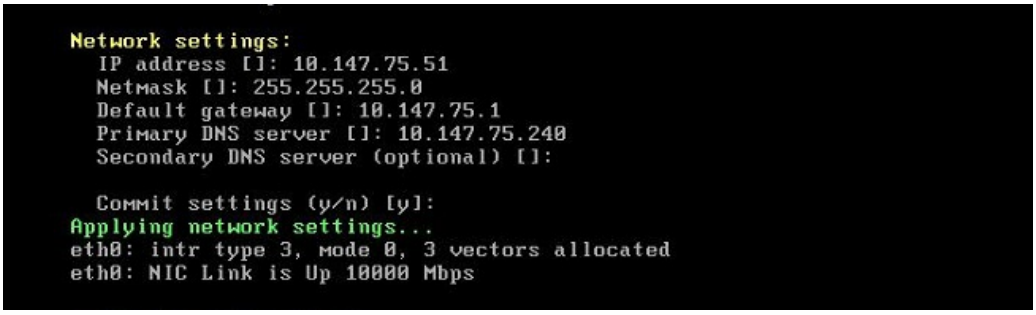
クラスター構成におけるXenMobile 10.xのリファレンスアーキテクチャ図については、「アーキテクチャの概要」を参照してください。

XenMobileクラスターノードのインストール

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

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

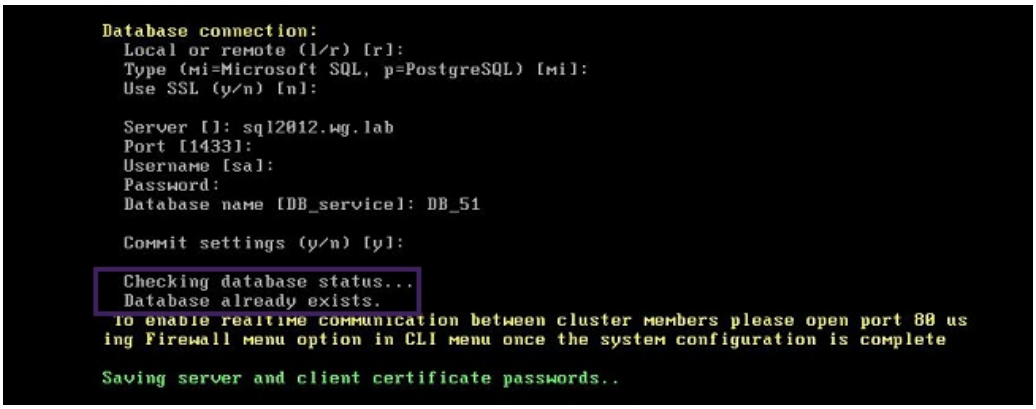
2. 次の図のようなネットワーク構成情報を指定します。



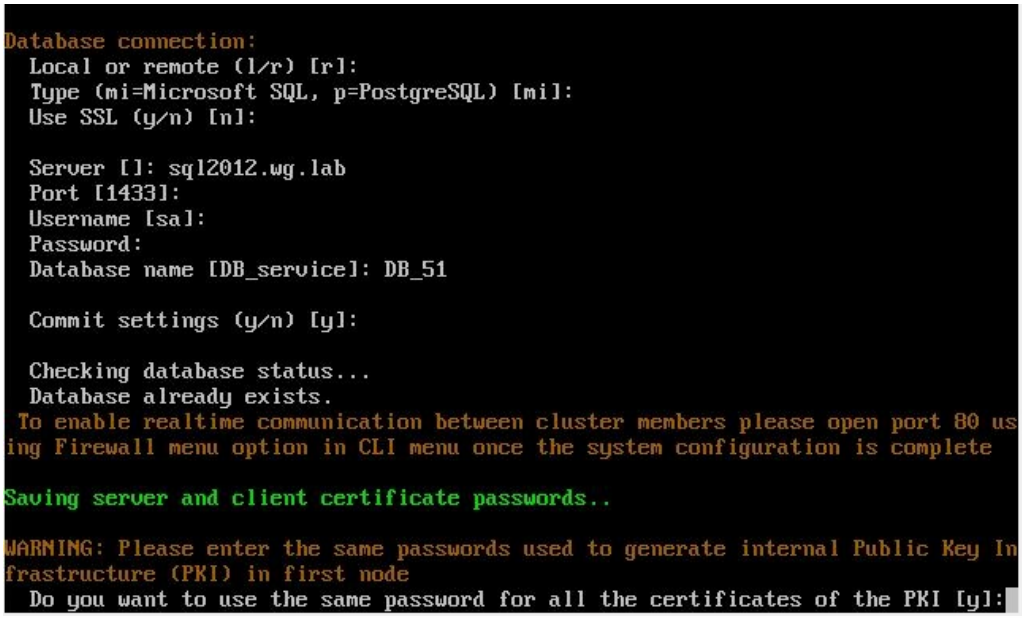
3. データ保護のためにデフォルトのパスワードを使用する場合、「y」を入力します。または「n」を入力して、新しいパスワードを入力します。

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

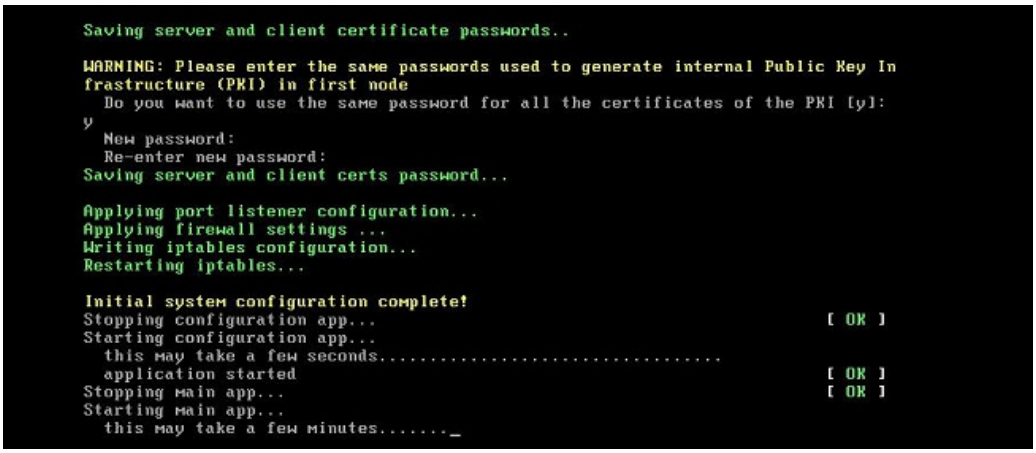
5. 完全に構成されたVMが指していたのと同じデータベースを指すように、データベースを構成します。次のメッセージが表示されます。Database already exists.



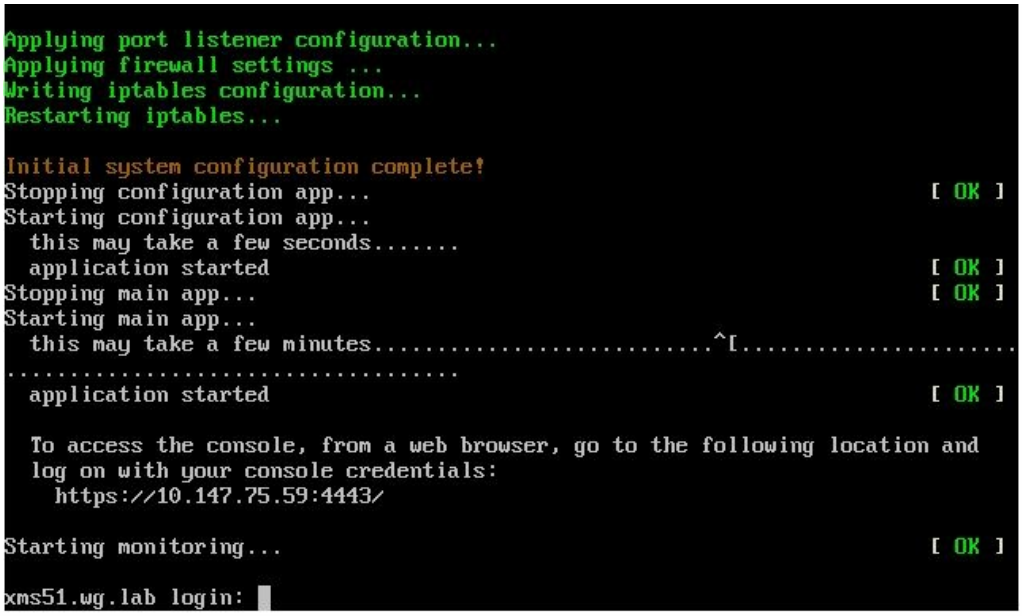
6. 最初のVMに付与した証明書のものと同じパスワードを入力してください。



パスワードの入力が完了すると、2台目のノードでの初期構成が完了します。

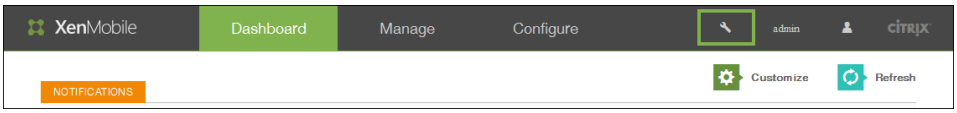


7. 構成が完了すると、サーバーが再起動され、ログオンダイアログボックスが開きます。

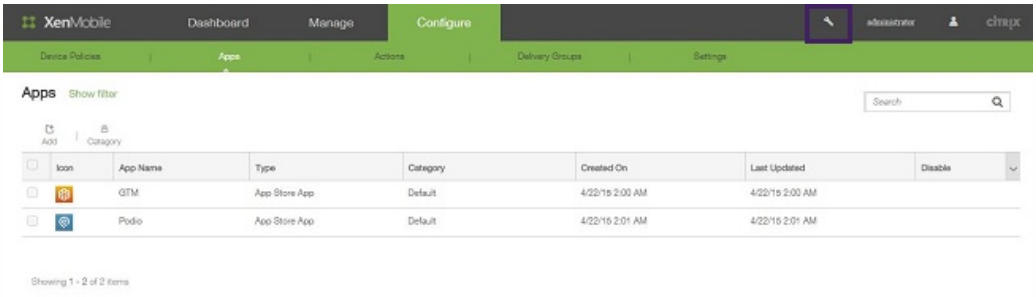


注：ログオンダイアログボックスは最初のVMのログオンダイアログボックスと同じです。 同じであるため、両方のVMで同じデータベースサーバーを使用していることが確認できます。

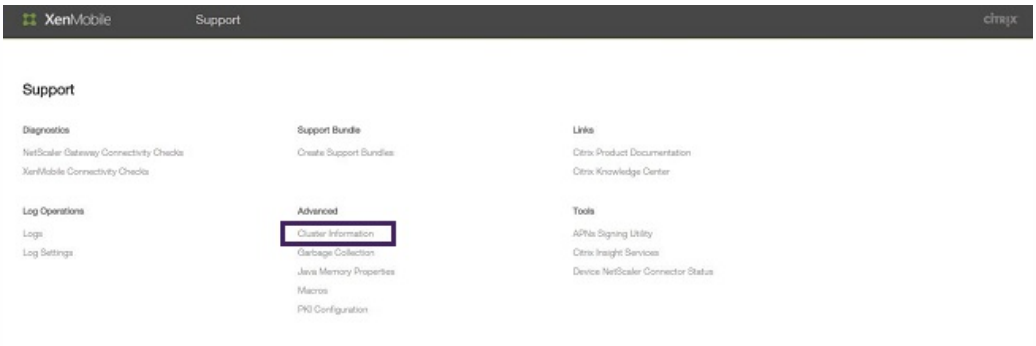
8. WebブラウザーでXenMobileコンソールを開くには、XenMobileの完全修飾ドメイン名（FQDN）を使用します。
9. ［Dashboard］で画面右上のツールアイコンをクリックします。



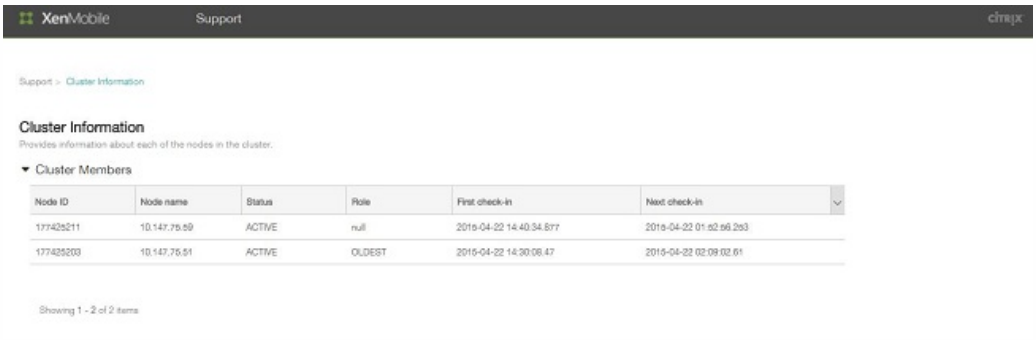
［Support］ページが開きます。



10. ［Advanced］の［クラスター情報］をクリックします。



クラスターのメンバー、デバイス接続情報、タスクなど、クラスターに関するすべての情報が表示されます。



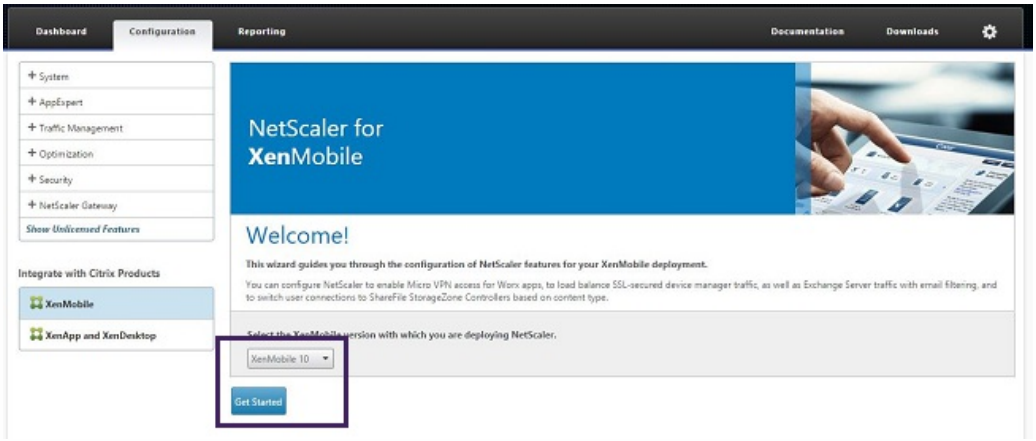
新しいノードがクラスターのメンバーになります。 別のノードを追加する場合も、手順は同じです。

NetScalerでXenMobileクラスターの負荷分散を構成するには

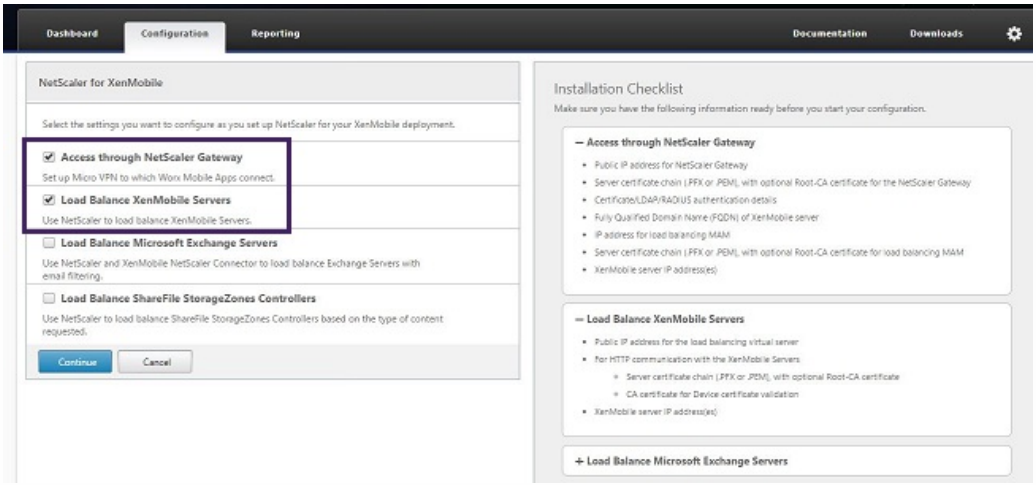
必要なノードをXenMobileクラスターのメンバーとして追加した後、クラスターにアクセスできるようにノードの負荷分散を行う必要があります。 負荷分散を行うには、NetScaler 10.5.xで利用可能なXenMobileウィザードを実行します。 ウィザードの実行によりXenMobileの負荷分散を行う手順は、以下のとおりです。

1. NetScalerにログオンします。

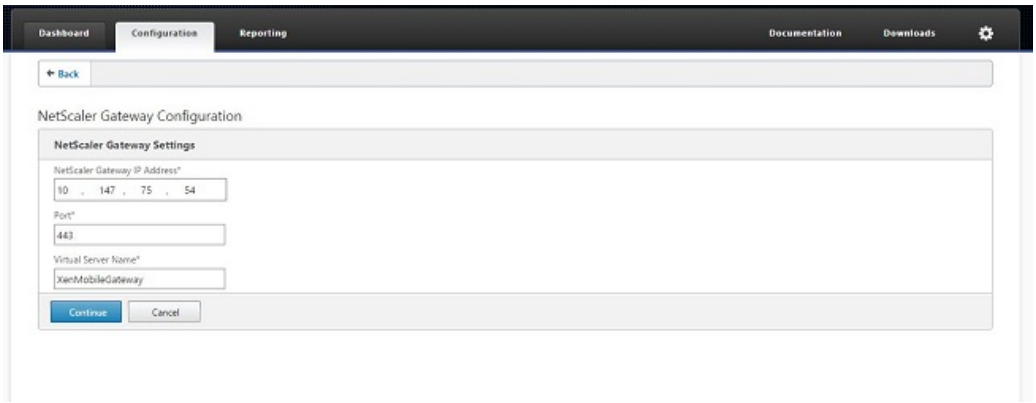
2. ［Configuration］タブで［XenMobile］をクリックし、［Get Started］をクリックします。



3. ［Access through NetScaler Gateway］チェックボックスと［Load Balance XenMobile Servers］チェックボックスをオンにし、［Continue］をクリックします。

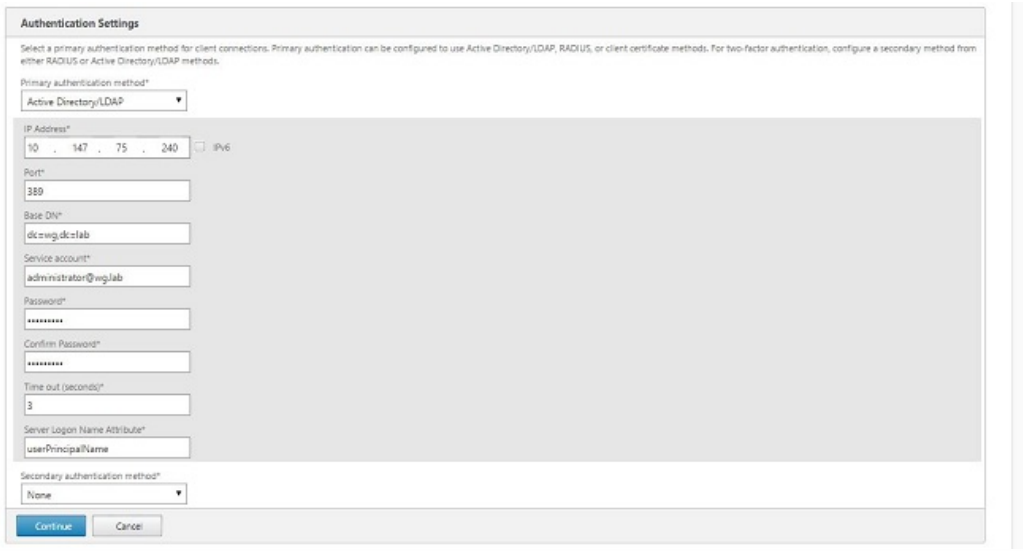


4. NetScaler GatewayのIPアドレスを入力し、［Continue］をクリックします。



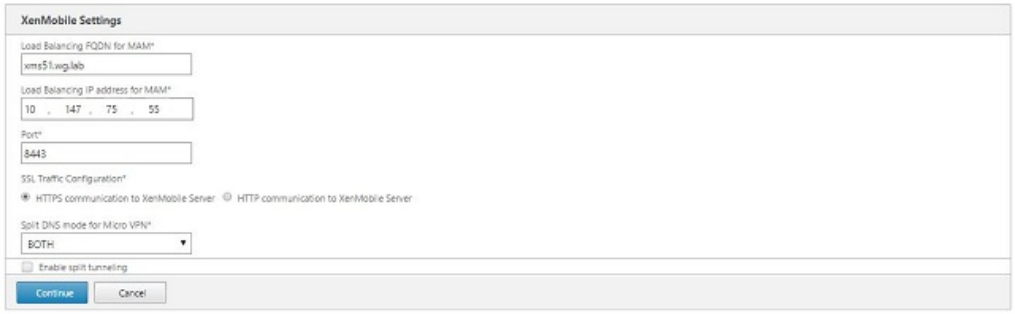
5. 以下のいずれかの方法でサーバー証明書をNetScaler Gatewayの仮想IPアドレスにバインドして［Continue］をクリックします。
   - ［Use existing certificate］で一覧からサーバーの証明書を選択します。
   - ［Install Certificate］タブをクリックして、新しいサーバーの証明書をアップロードします。

6. 認証サーバーの詳細を入力して、［Continue］をクリックします。



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

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

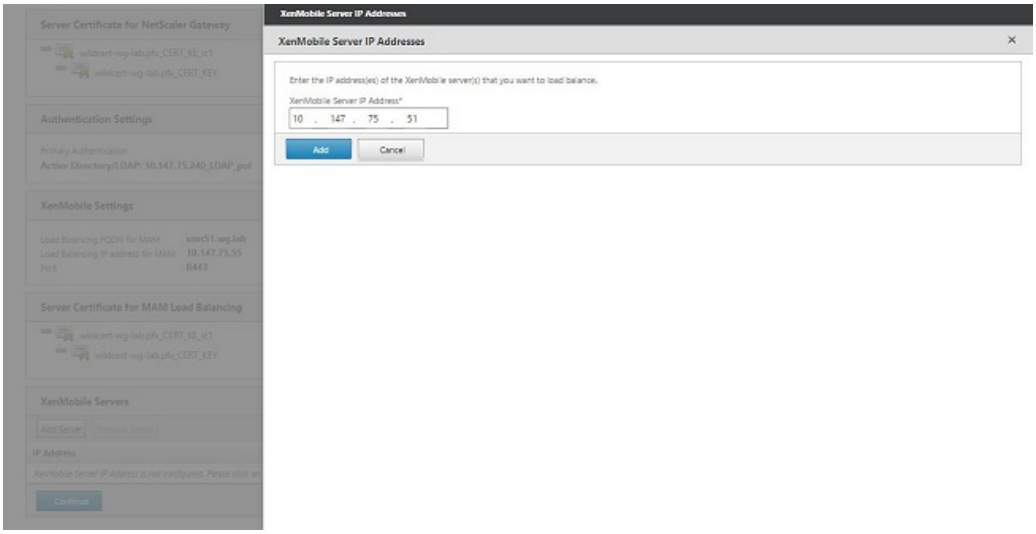


注：MAM負荷分散仮想IPアドレスのFQDNとXenMobileのFQDNが同じであることを確認してください。

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

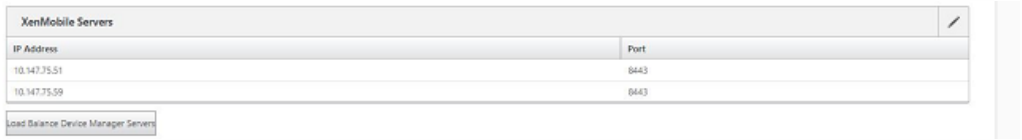
10. ［XenMobile Servers］の下で［Add Server］をクリックしてXenMobileノードを追加します。

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

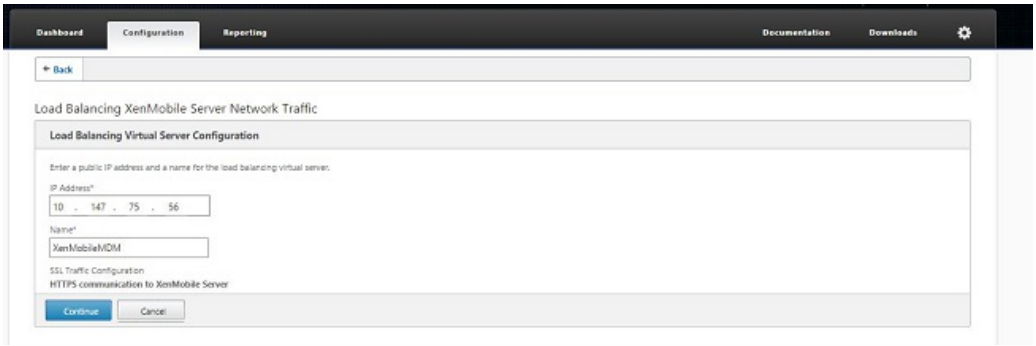


12. 手順10および11を繰り返して、XenMobileクラスターの一部であるXenMobileノードを追加します。追加したすべてのXenMobileノードが表示されます。 ［続ける］をクリックします。

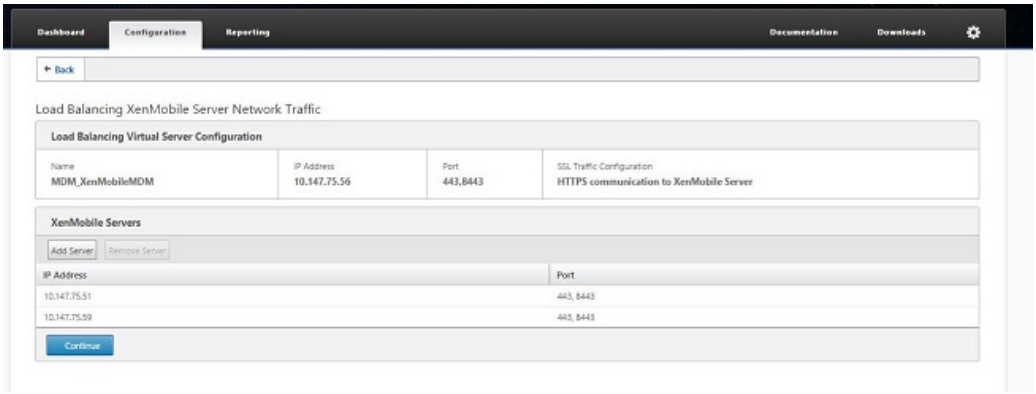
13. ［Load Balance Device Manager Servers］をクリックしてMDM負荷分散の構成を続行します。



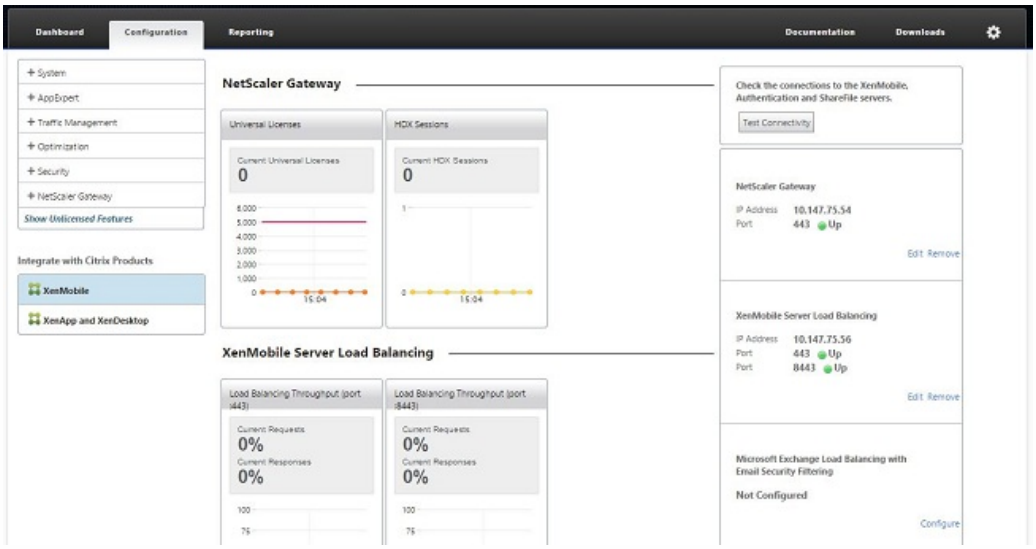
14. MDM負荷分散IPアドレス用に使用するIPアドレスを入力し、［Continue］をクリックします。



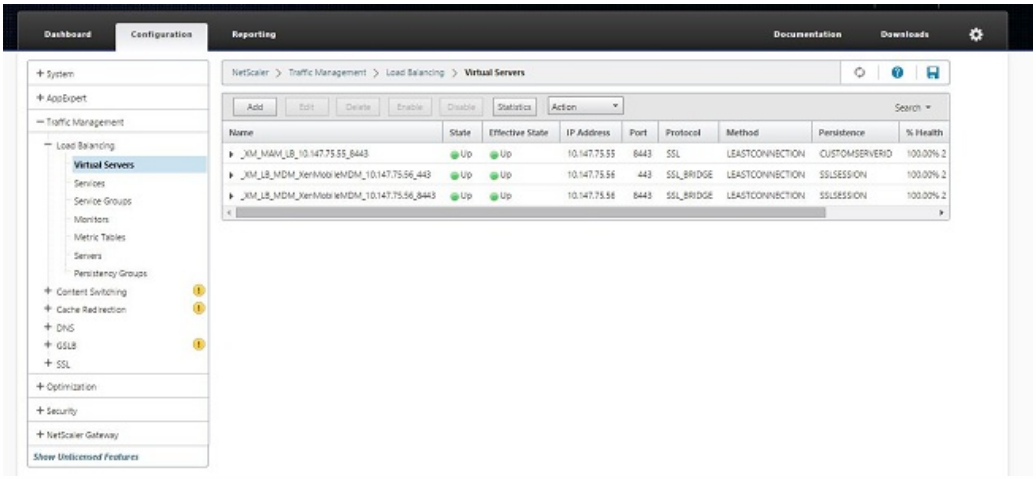
15. 一覧にXenMobileノードが表示されたら、［Continue］をクリックしてから［Done］をクリックして処理を完了します。



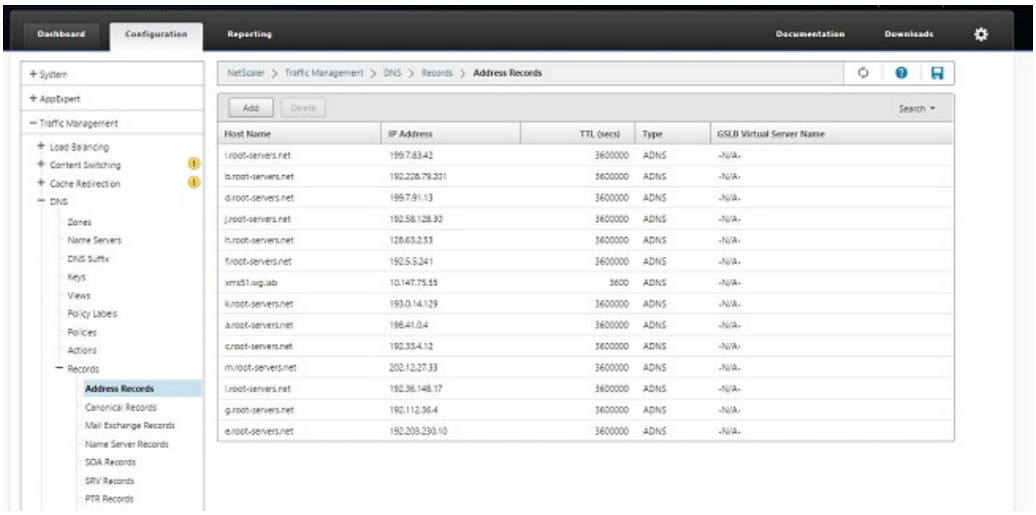
［XenMobile］ページに仮想IPアドレスのステータスが表示されます。



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



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

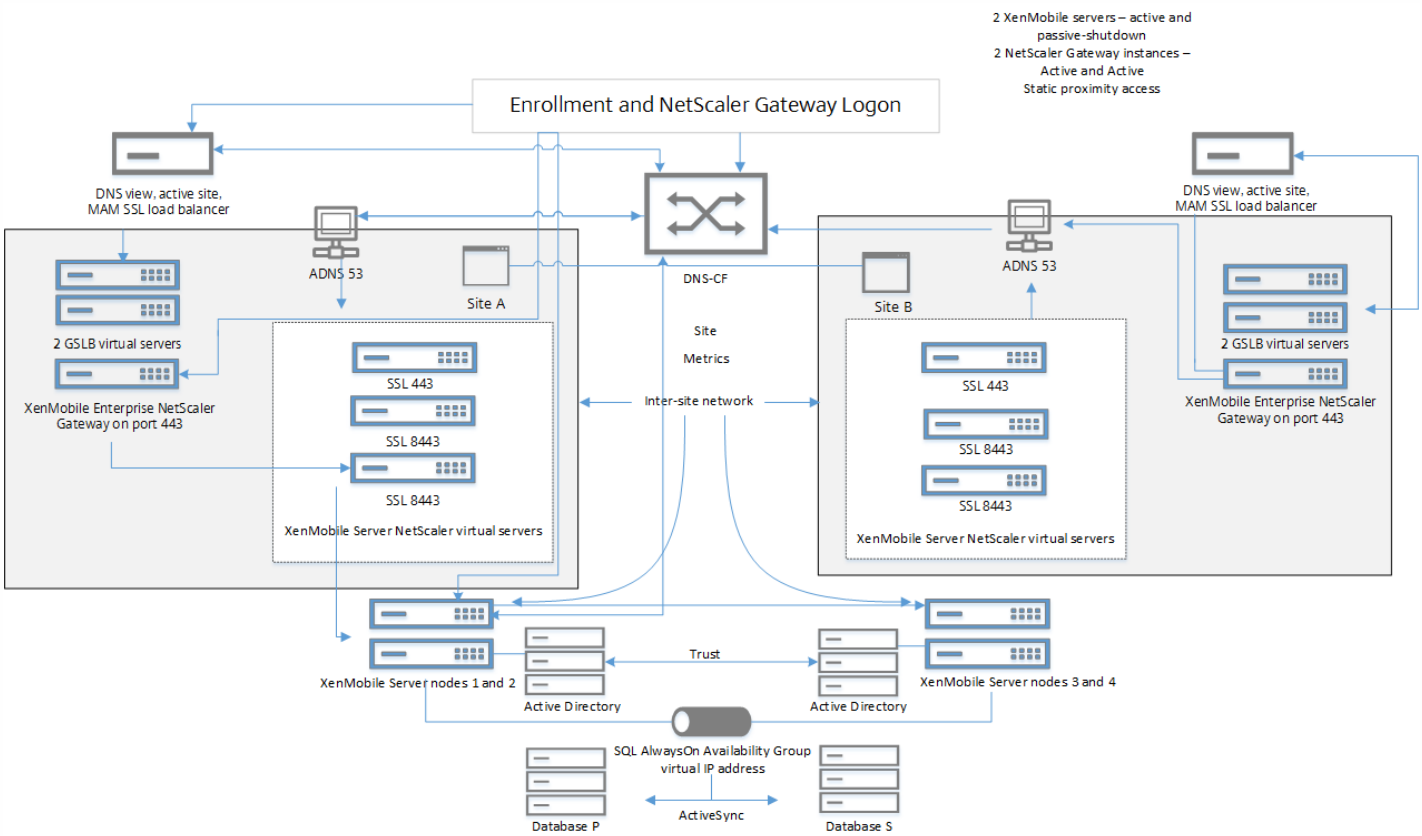


XenMobile障害回復ガイド

Aug 02, 2016

このガイドはPDFとして提供されており、XenMobile 10 Enterprise Editionでの障害回復用の展開環境の構成方法について説明しています。

次の図に、この障害回復用の展開環境のアーキテクチャを示します。この図はPDFとしてダウンロードすることもできます。



PDF XenMobile障害回復ガイド

PDF XenMobile障害回復のアーキテクチャ図

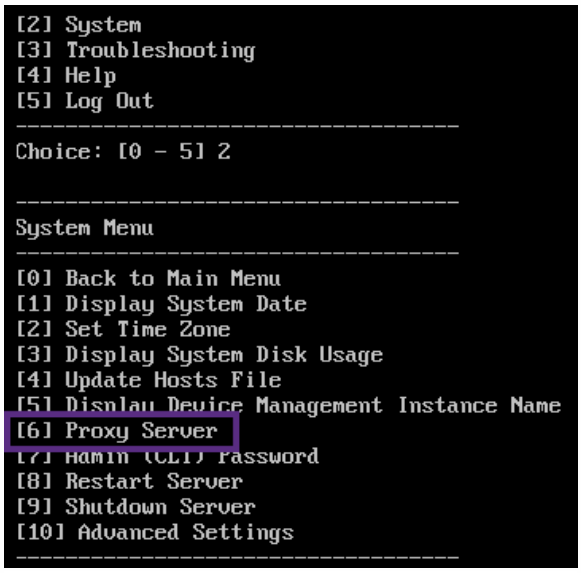
XenMobileでのプロキシサーバーの有効化

Aug 02, 2016

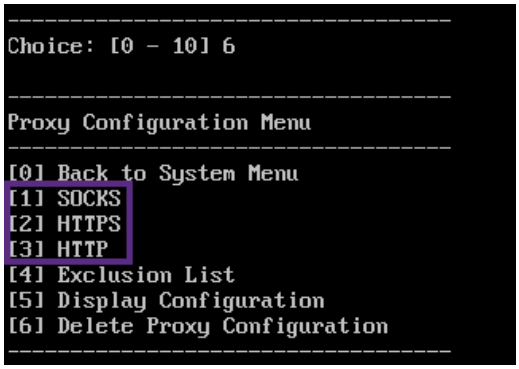
発信インターネットトラフィックを制御するために、そのトラフィックを発信するプロキシサーバーをXenMobileにセットアップできます。 これを行うには、コマンドラインインターフェイス（CLI）でプロキシサーバーをセットアップする必要があります。 プロキシサーバーのセットアップにはシステムの再起動が必要なことに注意してください。

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

2. ［System］メニューで、「**6**」と入力して［Proxy Server］メニューを選択します。



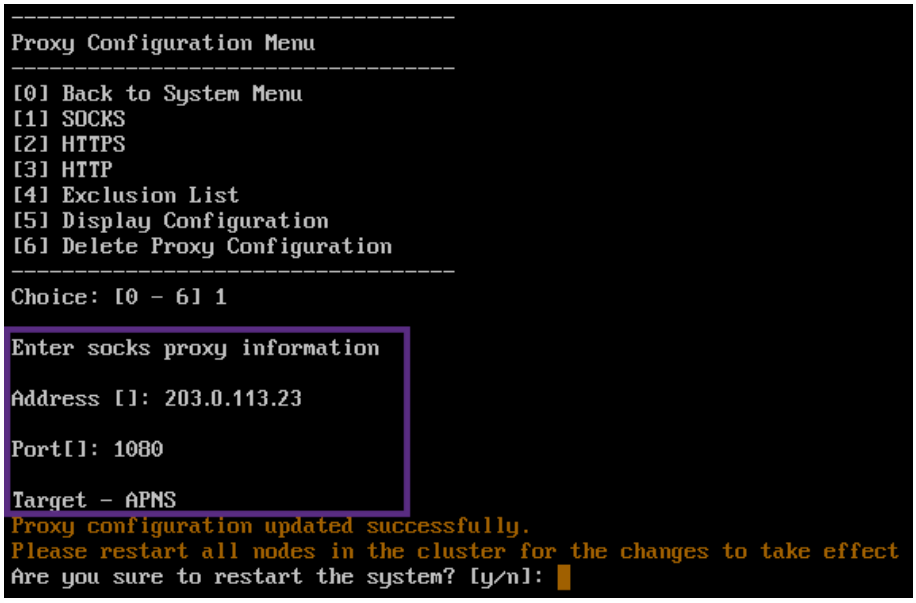
3. ［Proxy Configuration］メニューで、「**1**」と入力して［SOCKS］を選択するか、「**2**」と入力して［HTTPS］を選択するか、「**3**」と入力して［HTTP］を選択します。



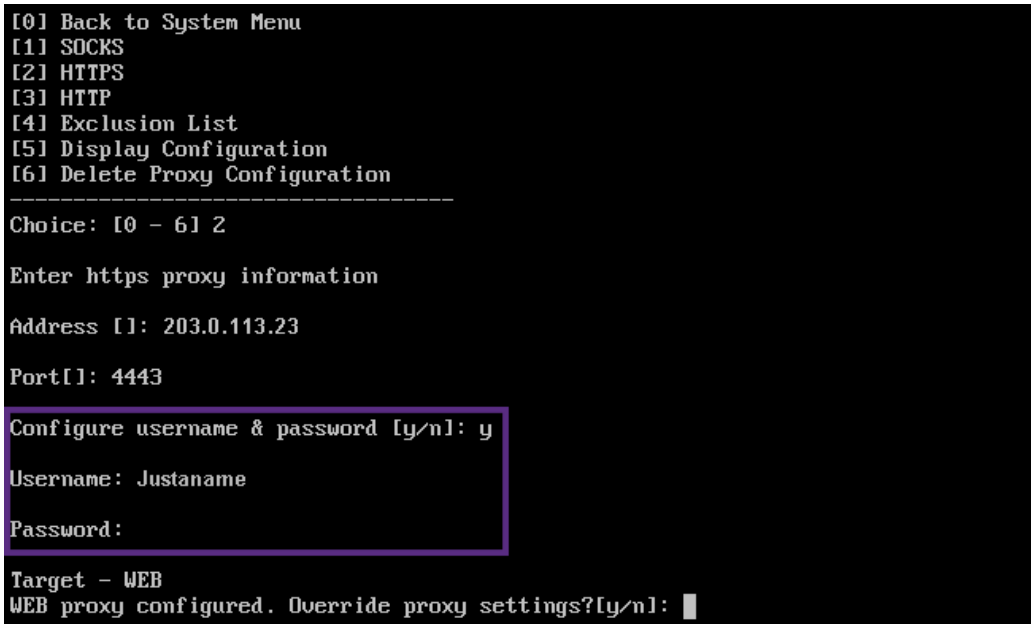
4. プロキシサーバーのIPアドレス、ポート番号、およびターゲットを入力します。 プロキシサーバーの種類別の、サポートされるターゲットの種類については以下の表を参照してください。

プロキシの種類	サポートされるターゲット
SOCKS	APNS

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



5. HTTPまたはHTTPSプロキシサーバーに認証用のユーザー名およびパスワードを構成する場合は「y」と入力し、ユーザー名とパスワードを入力します。



6.「**y**」と入力してプロキシサーバーのセットアップを完了します。

ライセンス管理

Oct 25, 2016

XenMobileおよびNetScaler Gatewayにはライセンスが必要です。 各エディションでどのXenMobile機能が利用できるかが表示されたデータシートは、このPDFを参照してください。

NetScaler Gatewayのライセンスについて詳しくは、「NetScaler Gatewayのライセンス」のページを参照してください。 Citrixライセンスサーバーについて詳しくは、 シトリックスライセンスシステムを参照してください。

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

XenMobileのライセンスをダウンロードする前に、Citrixライセンスサーバーをインストールする必要があります。 ライセンスファイルを生成するには、Citrixライセンスサーバーをインストールしたサーバー名が必要となります。 XenMobileをインストールする場合、そのサーバーにはデフォルトでCitrixライセンスサーバーがインストールされます。 または、既存のCitrixライセンスサーバー展開を使ってXenMobileのライセンスを管理できます。 Citrixライセンスサーバーのインストール、展開、および管理について詳しくは、 製品ライセンスの有効化を参照してください。

> ## 注意
>
> バージョン10.3.xのXenMobileでは、Citrixライセンスサーバー11.12.1以降が必要です。それより古いバージョンのライセンスサーバーはXenMobile 10.3.xで動作しません。

> ## Important
>
> XenMobileのノード（インスタンス）をクラスター化する場合は、リモートサーバー上でCitrixライセンスサーバーを使用する必要があります。

受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。 構成ファイルのバックアップコピーを保存すると、すべてのライセンスファイルもバックアップに含まれます。 ただし、最初に構成ファイルをバックアップせずにXenMobileを再インストールする場合は、元のライセンスファイルが必要になります。

XenMobileライセンスについての考慮事項

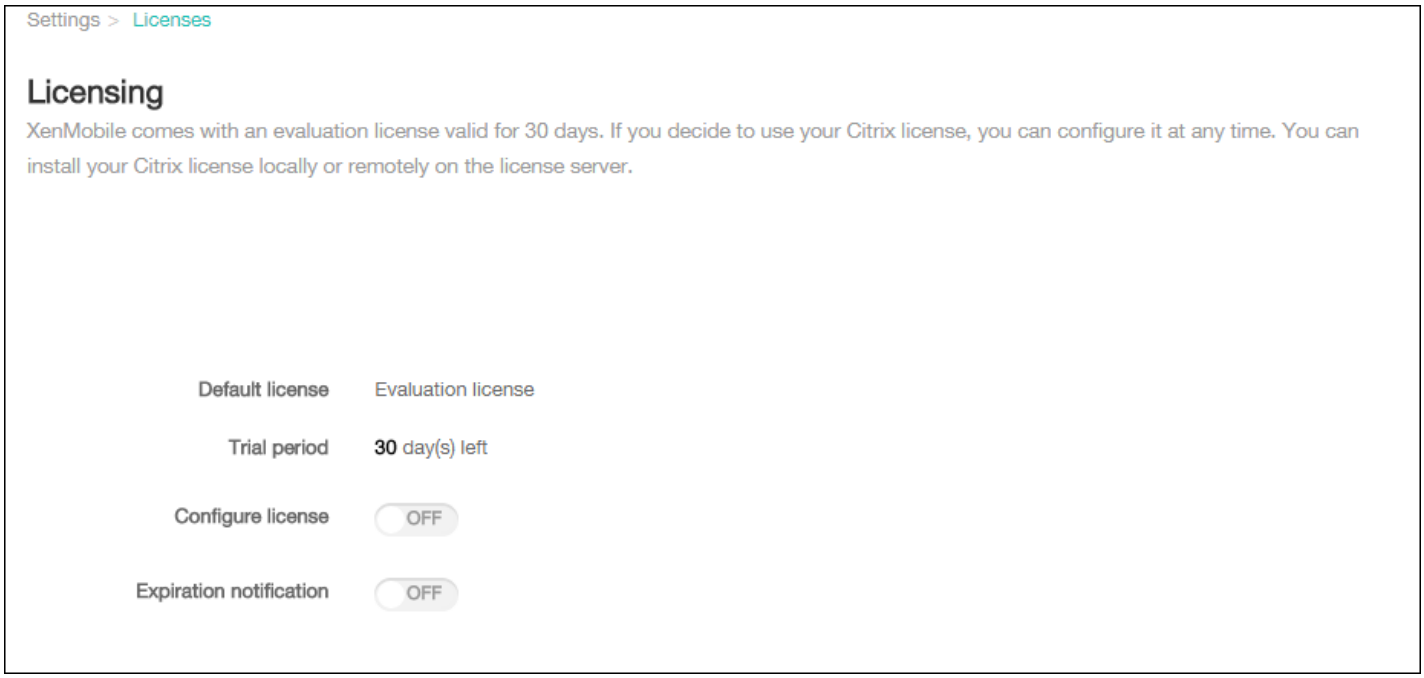
ライセンスがない場合、30日間は試用モードでXenMobileのすべての機能を操作することができます。 この試用モードを使用できるのは、XenMobileのインストール時から30日間の1回限りです。 有効なXenMobileライセンスを使用できるかどうかに関係なく、XenMobile Webコンソールへのアクセスはブロックされません。 試用期間の残り日数は、XenMobileコンソールで確認できます。

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

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

XenMobileコンソールで［Licensing］ページを開くには

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



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

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

ローカルライセンスを追加するには

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

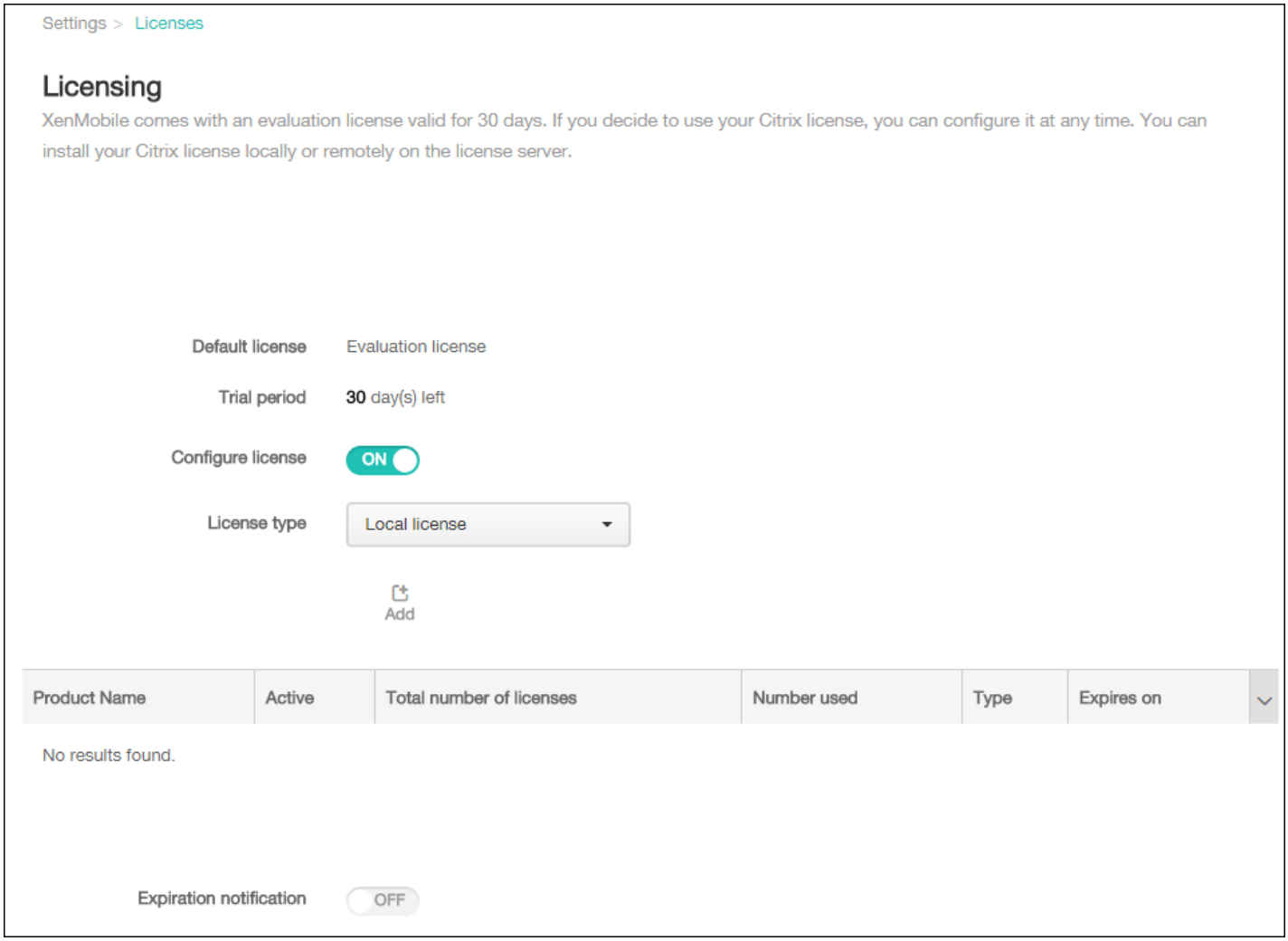
ローカルライセンスの管理は、すべてXenMobileコンソールで行います。

1. ライセンス管理コンソールを介してSimple License Serviceから、またはCitrix.comのアカウントから直接、ライセンスファイルを入手します。 詳しくは、「ライセンスファイルの入手」を参照してください。

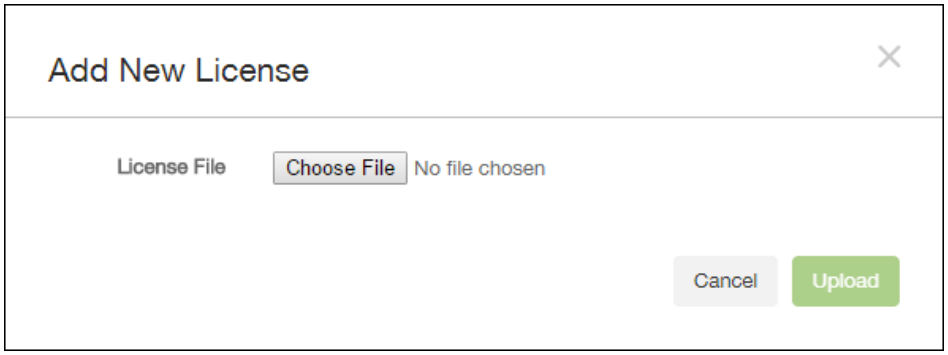
2. XenMobileコンソールで、右上の歯車アイコンをクリックします。［**Settings**］ページが開きます。

3. ［**Licensing**］をクリックします。 ［**Licensing**］ページが開きます。

4. ［**Configure license**］を［**On**］に設定します。 ［**License type**］ボックス、 ［**Add**］ボタン、 ［**Licensing**］の表が表示されます。 ［**Licensing**］の表には、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、この表は空白です。

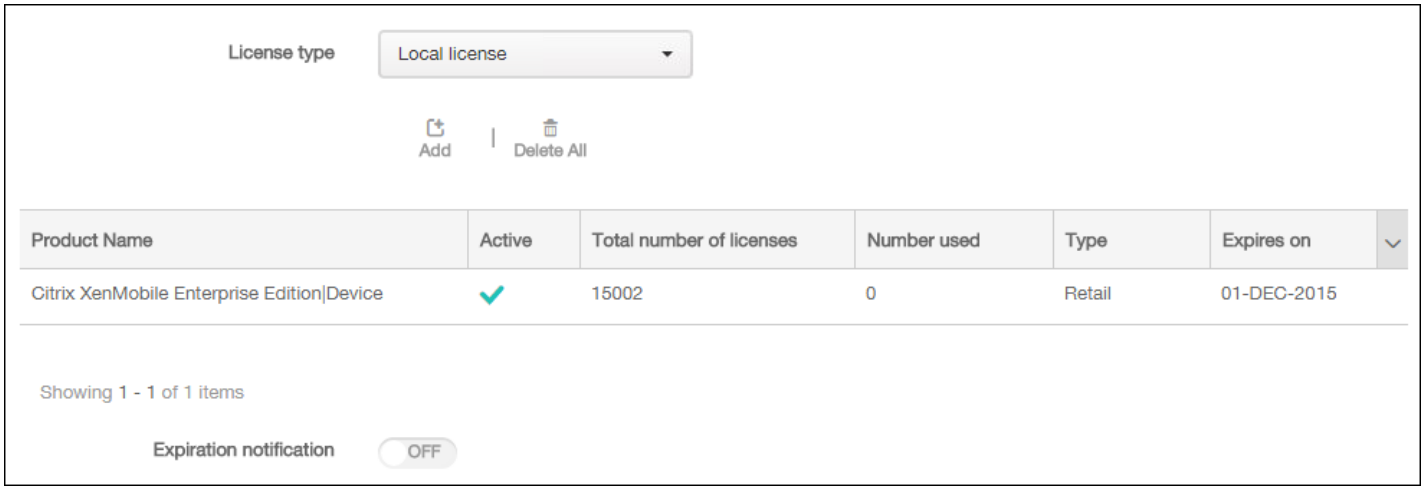


5. [**License type**] が [**Local license**] に設定されていることを確認して、 [**Add**] をクリックします。 [**Add New License**] ダイアログボックスが開きます。



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。 ライセンスがローカルにアップロードされ、表に表示されます。



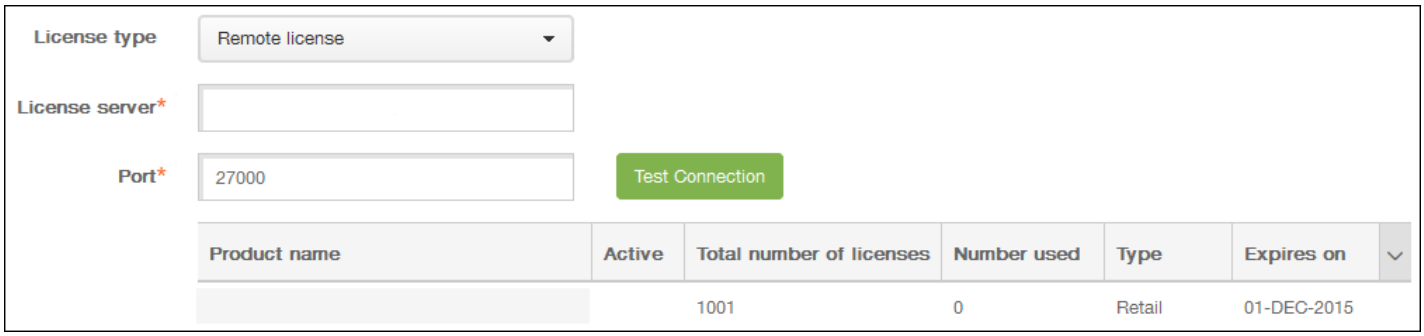
8. ライセンスが［**Licensing**］ページの表に表示されたら、ライセンスをアクティブ化します。 この表で最初のライセンスの場合、ライセンスは自動的にアクティブ化されます。

リモートライセンスを追加するには

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

1. ［**Licensing**］ページで、 ［**Configure license**］を［**On**］に設定します。 ［**License type**］ボックス、 ［**Add**］ボタン、 ［**Licensing**］の表が表示されます。 ［**Licensing**］の表には、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、この表は空白です。

3. ［**License type**］を［**Remote license**］に設定します。 ［**Add**］ボタンが、 ［**License server**］フィールドおよび［**Port**］フィールドと、 ［**Test Connectivity**］ボタンに置き換わります。



4. 次の設定を構成します。

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

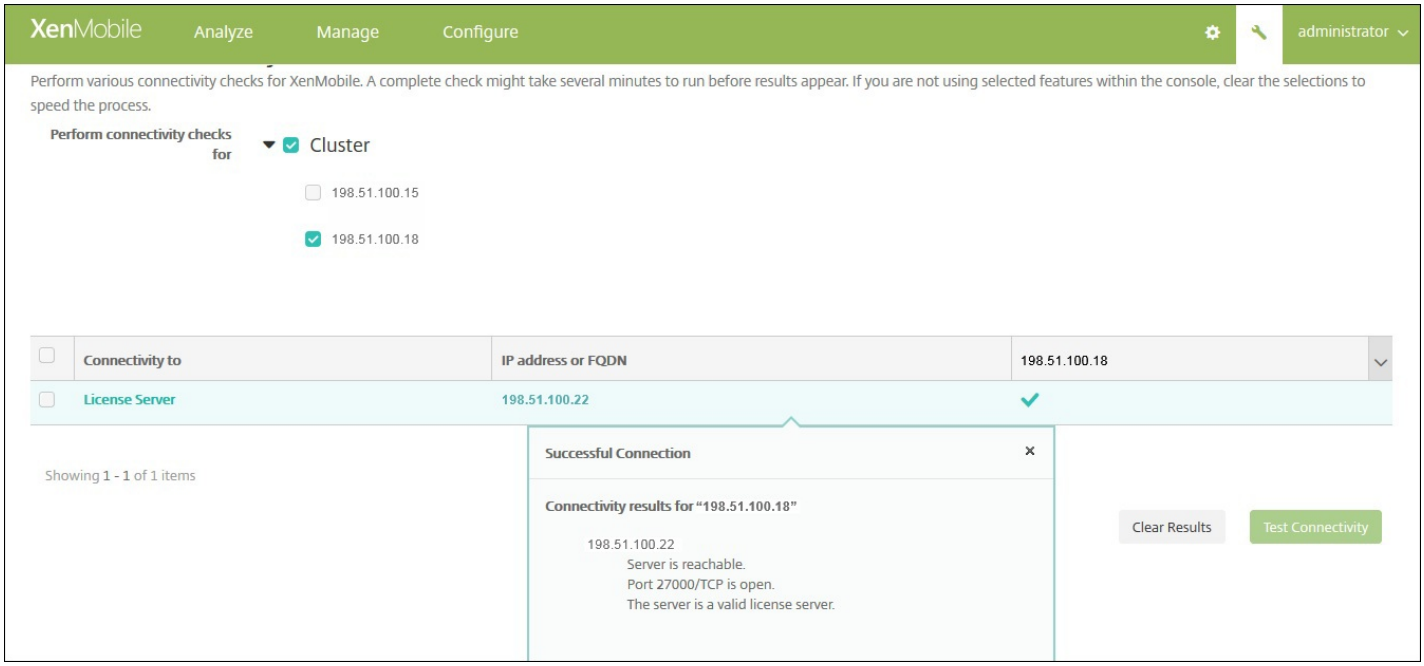
5. ［**Test Connection**］をクリックします。 接続が成功した場合、XenMobileはライセンスサーバーに接続し、使用可能なライセンスがライセンスの表に表示されます。 ライセンスが1つのみの場合は、自動的にアクティブ化されます。

［**Text Connection**］をクリックすると、XenMobileで以下のことが確認されます。

- XenMobileがライセンスサーバーと通信できるか。

- ライセンスサーバーのライセンスは有効であるか。
- ライセンスサーバーはXenMobileと互換性があるか。

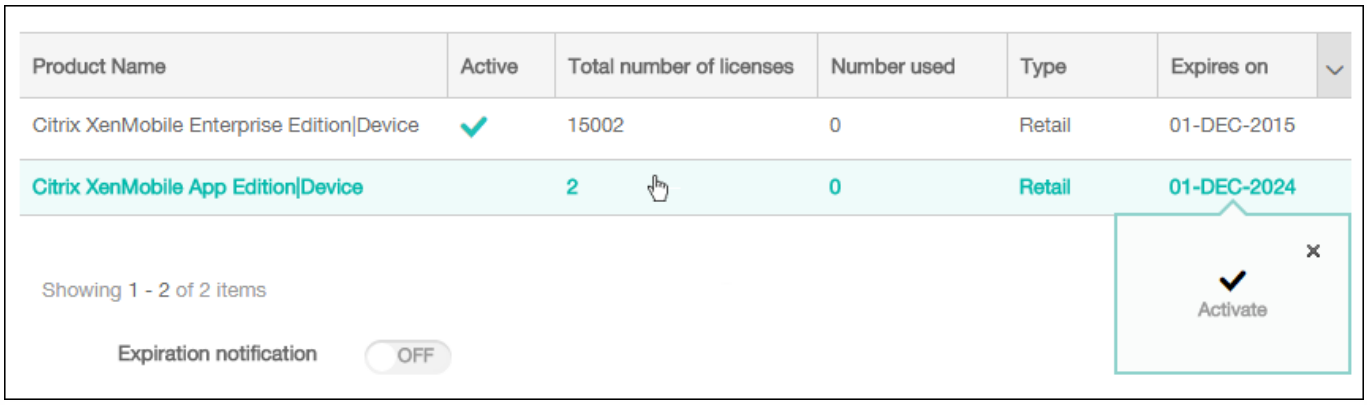
接続に失敗した場合は、表示されるエラーメッセージを確認し、必要な修正を加えてから、[**Test Connection**]をクリックします。



別のライセンスをアクティブ化するには

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

1. [**Licensing**]ページの[**Licensing**]の表で、アクティブ化するライセンスの行をクリックします。 [**Activate**]確認ダイアログボックスが、その行の横に表示されます。



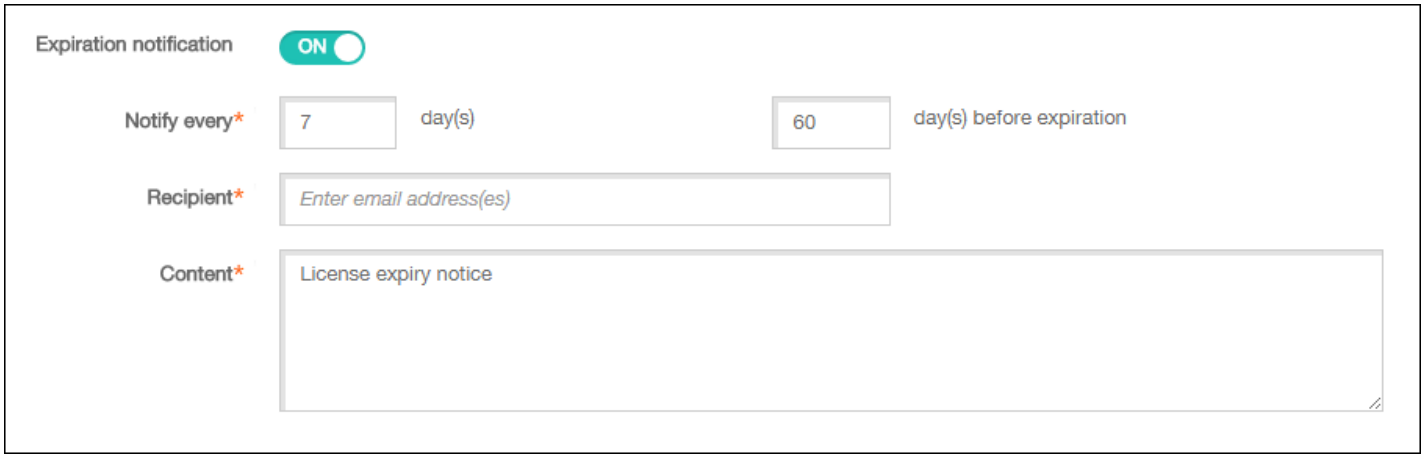
2. [**Activate**]をクリックします。 [**Activate**]ダイアログボックスが開きます。
3. [**Activate**]をクリックします。 選択したライセンスがアクティブ化されます。

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

有効期限通知を自動化するには

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

1. **[Licensing]** ページで、 **[Expiration notification]** を **[On]** に設定します。 通知に関連するフィールドが新たに表示されます。



2. 次の設定を構成します。

- **Notify every**：以下を入力します。
  - 通知が送信される頻度（7日ごとなど）。
  - 通知の送信を開始する時期（ライセンス有効期限の60日前など）。
- **Recipient**：自分またはライセンス担当者のメールアドレスを入力します。
- **Content**：受信者への有効期限通知メッセージの内容を入力します。

3. **[Save]** をクリックします。 有効期限の残りが設定した日数になると、 **[Recipient]** に入力した受信者への、 **[Content]** に入力したテキストを含むメールメッセージの送信が開始されます。 設定した頻度で通知が送信されます。

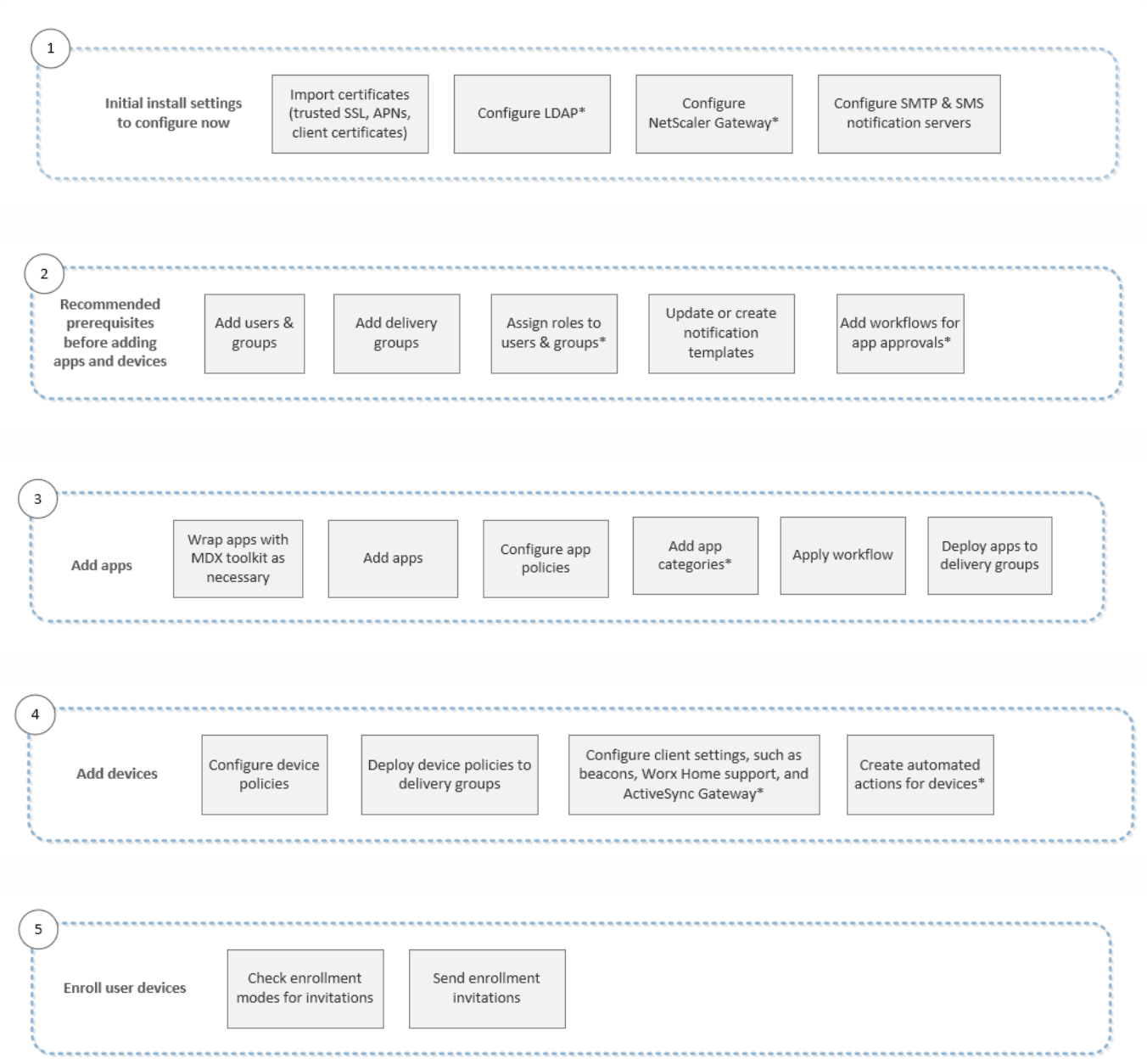
XenMobileコンソールの概要

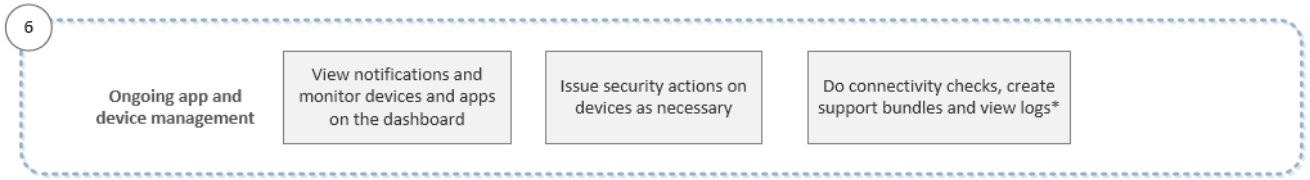
Aug 02, 2016

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

コンソールで次にどこへ進めばよいかを確認できるよう、以下の図に、アプリケーションおよびデバイスの継続的な管理を準備するための推奨されるワークフローを示しています。 最初の一連の推奨事項は、インストール手順実行中にスキップした可能性のある初期設定が対象になっています。

注：アスタリスクが付いている項目はオプションです。





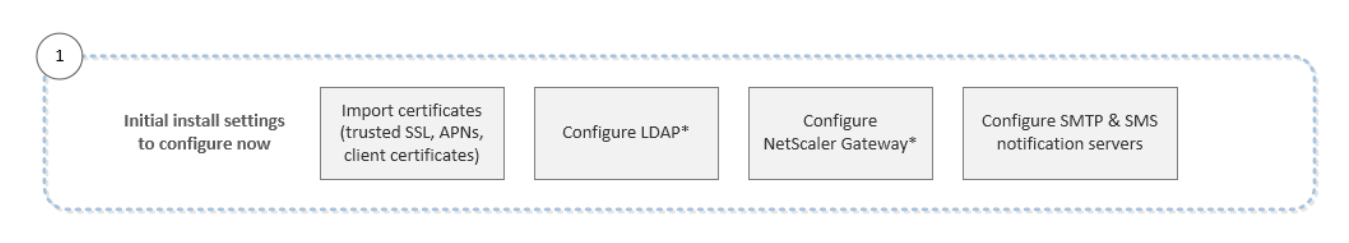
初期設定のワークフロー

Aug 02, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 初期構成画面に戻ることはできないため、インストール構成の一部をその時点でスキップした場合は、コンソールで以下の設定を構成できます。 ユーザー、アプリケーション、デバイスの追加を開始する前に、これらのインストール設定を完了することを考慮する必要があります。 設定を開始するには、コンソールの右上にある歯車アイコンをクリックします。

ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

注：アスタリスクが付いている項目はオプションです。



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

- XenMobileでの証明書
- LDAP構成
- NetScaler GatewayとXenMobile
- XenMobileでの通知

コンソールの前提条件のワークフロー

Oct 25, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。 ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

このワークフローは、アプリケーションとデバイスを追加する前に構成する、推奨される前提条件を示しています。
注：アスタリスクが付いている項目はオプションです。

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

- ユーザーアカウント、役割、および登録設定の構成
- XenMobileでのデリバリーグループの管理
- RBACを使用した役割の構成
- XenMobileで通知テンプレートを作成または更新するには
- 登録モードを構成してSelf Help Portalを有効化するには
- ワークフローを作成および管理するには

アプリケーションの追加のワークフロー

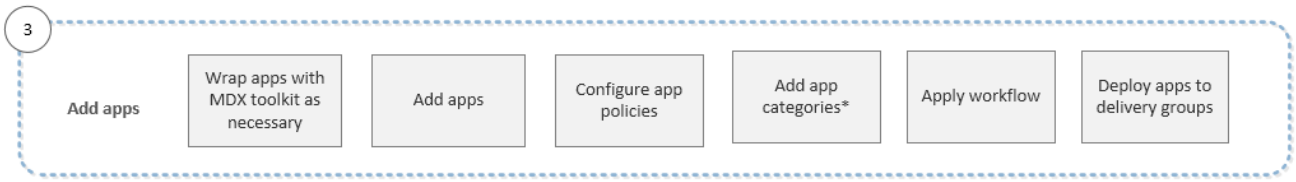
Oct 25, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。 ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

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

注：アスタリスクが付いている項目はオプションです。



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

- MDX Toolkitについて
- XenMobileへのアプリケーションの追加
- MDXポリシーの概要
- アプリケーションカテゴリを追加するには
- ワークフローを作成および管理するには
- XenMobileでのデリバリーグループの管理

デバイスの追加のワークフロー

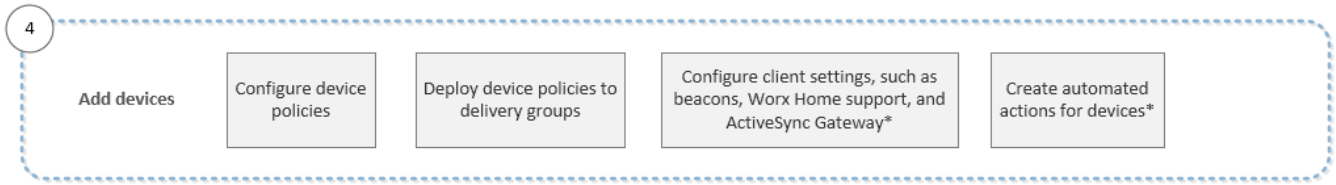
Aug 02, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。 次に、「アプリケーションの追加のワークフロー」に従ってアプリケーションを追加できます。 ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

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

注：アスタリスクが付いている項目はオプションです。



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

- XenMobileでのデバイスの追加およびデバイスの詳細の表示
- プラットフォーム別のXenMobileデバイスポリシー
- XenMobileでのデリバリーグループの管理
- XenMobileクライアント設定の構成
- XenMobileでの自動化された操作の作成

ユーザーデバイスの登録のワークフロー

Aug 02, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。 次に、「アプリケーションの追加のワークフロー」に従ってアプリを追加し、「デバイスの追加のワークフロー」に従ってデバイスを追加および登録できます。 ワークフロー全体を確認するには、 「XenMobileコンソールの概要」を参照してください。

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

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

- ユーザーアカウント、役割、および登録設定の構成
- 登録モードを構成してSelf Help Portalを有効化するには

アプリケーションおよびデバイスの継続的な管理のワークフロー

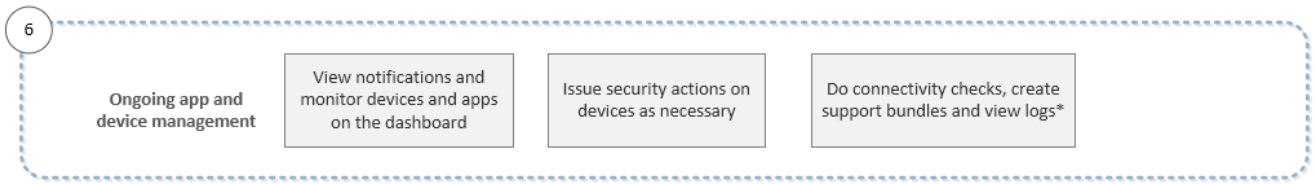
Aug 02, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。 インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。 次に、「アプリケーションの追加のワークフロー」に従ってアプリケーションを追加し、「デバイスの追加のワークフロー」に従ってデバイスを追加および登録できます。 最初の4つのワークフローが完了した後、「ユーザーデバイスの登録のワークフロー」に従ってユーザーデバイスを登録します。 ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

この6番目で最後のワークフローは、コンソールで実行可能であり推奨される、アプリケーションおよびデバイスの継続的な管理作業を示しています。

注：アスタリスクが付いている項目はオプションです。



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

XenMobileコンソールのフィルターおよび表

Aug 02, 2016

フィルターと表はXenMobileコンソールのあらゆる場所にあります。 これらは［Devices］、［Enrollment］、［Device Policies］、［Apps］、［Actions］、［Delivery Groups］タブはもちろん、［Settings］の下の多くのページにも含まれます。 フィルターでは、コンソールのいずれかの領域の情報を絞り込み、表示または操作したい情報を的確に見つけることができます。 表では、1つまたは複数の項目をクリックして、選択した項目に対する操作を実行するためのオプションを表示できます。 選択する項目の数によって、オプションは異なる場合があります。

以下の表は、共通オプションの一部とその場所を示しています。

メニューオプション	操作	オプションが表示される表
INIファイルに	表に新しい項目を追加する。	すべて
カテゴリ	アプリケーションのカテゴリを追加および管理する。	Apps
Copy URL	URLをクリップボードにコピーする。	Enrollment
DeleteまたはDelete All	選択した項目を永久に削除する。	すべて
ユーザーおよびデバイスに	ユーザーおよびデバイスにリソースを展開する。	DevicesおよびDelivery Groups
アプリケーションまたは	アプリケーションまたはAllUsersデリバリーグループを無効にする。	AppsおよびDelivery Groups
Edit	既存の項目を変更する。	Enrollment以外のすべて
Export	表の内容を.csvファイルに送る。	すべて
インポート	プロビジョニングファイルからデバイスを追加する。	Devices
	ファイルからローカルユーザーおよびグループを追加する。	Local Users and Groups
Manage Local Groups	管理するローカルグループを追加する。	Local Users and Groups
Notify	選択したユーザーおよびデバイスに通知を送信する。	EnrollmentおよびDevices
Refresh	表を更新する。	Devices
セキュア	選択したデバイスに対してセキュリティの操作を実行する。	Devices

Self Help Portal メニューオプション	登録のモードとしてSelf Help Portalを有効にする。 操作	Enrollment オプションが表示される表
Update	表内の値を更新する。	Release Management

XenMobileコンソールの表でオプションを表示するには

コンソールの表の情報に対するアクションを実行するためのさまざまなオプションを、いくつかの異なる方法で表示できます。

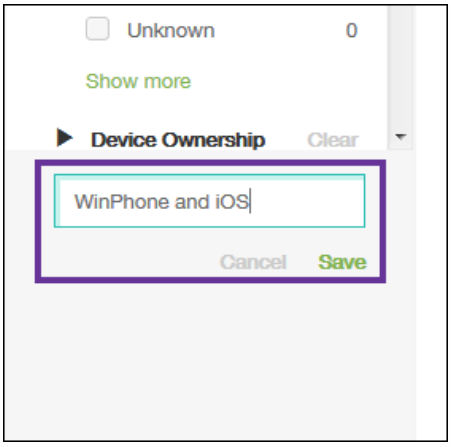
- 項目の横にあるチェックボックスをオンにして、一覧の上にオプションメニューを表示できます。
- 複数の項目の横にあるチェックボックスをオンにして、それらの項目すべてに対して操作を実行できます。 複数の項目に実行できる操作は表示している表によって異なります。
- 一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。［Show More］をクリックすると、項目の詳細が表示されます。 表示される操作は表示している表によって異なります。
- 名前の全体または一部を［Search］ボックスに入力して、一覧に表示される項目の数を絞り込むことができます。

コンソールの［Device Policies］領域の各ページに表示される項目は10個のみです。 ページの右下の三角をクリックして、前後のページに移動します。

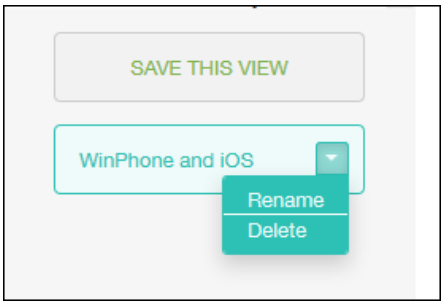
XenMobileコンソールで情報をフィルターするには

コンソールの［Devices］、［Enrollment］、［Device Policies］、［Apps］、［Actions］、［Delivery Groups］、［Local Users and Groups］などの領域で特定の一部の情報を表示する場合、選択した条件に基づいて一覧をフィルターできます。 次の手順では、例として［Devices］ページを使用していますが、コンソールのどのページでもフィルターの手順は同じです。

1. ［Devices］ページで、［Show Filter］をクリックします。
   フィルターパネルが開き、条件の一覧が表示されます。この条件を使用して、［Devices］の一覧をフィルターできます。初めてフィルターを表示したとき、すべての条件は 折りたたまれています。
2. フィルターの左にある三角をクリックしすると、そのフィルターで使用できる条件が表示されます。 各条件の右に表示されている数字は、その条件に一致するデバイスの数を表しています。
3. 使用するフィルター条件を選択します。［Devices］一覧が、選択した条件に一致するデバイスに絞り込まれます。
4. 次のいずれかを行います。
   - ［Hide Filter］をクリックして、フィルターされた一覧に対する操作を続けます。
   - ［Clear All］をクリックして、完全な一覧に戻します。
   - 特定の条件の横の［Clear］をクリックしてフィルターを削除し、フィルターされた一覧からこれらの項目を削除します。
5. 選択した条件をカスタムフィルターとして保存する場合は、［Filter］パネルの下部にある［Save the filter］フィールドに説明的な名前を入力して、［Save］をクリックします。フィルターを保存しない場合は、［Cancel］をクリックします。



6. フィルターを保存すると、［Filter］パネルの下部でそのフィルターを選択して表内の情報をフィルターできます。
   注：フィルター名の右の三角をクリックすると、フィルター名を変更したり、フィルターを削除したりできます。



XenMobileのレポート

Aug 02, 2016

XenMobileには、10種類の事前定義されたレポートが用意されており、アプリケーションおよびデバイスの展開を分析することができます。

- **Apps by Devices & User**：ユーザーのデバイスに存在しているアプリケーションを一覧表示します。
- **Terms & Conditions**：使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。
- **Top 25 Apps**：ほとんどのユーザーのデバイスに存在している上位25のアプリケーションを一覧表示します。
- **Jailbroken/Rooted Devices**：ルート化済みiOSデバイスおよびジェイルブレイクされたAndroidデバイス一覧表示します。
- **Top 10 Apps – Failed Deployment** - 展開に失敗したアプリケーションを一覧表示します。
- **Inactive Devices** - 指定期間に非アクティブになったデバイスを一覧表示します。
- **Apps by Type & Category** - アプリケーションをバージョン別、種類別、およびカテゴリ別に一覧表示します。
- **Device Enrollment**：指定期間中に登録されたデバイスを一覧表示します。
- **Apps by Platform** - アプリケーションとアプリケーションバージョンを、デバイスプラットフォーム別およびバージョン別に一覧表示します。
- **Devices & Apps** - すべてのデバイス、デバイスデータ、およびインストールされているアプリケーションを一覧表示します。

レポートは.csv形式なので、Microsoft Excelのようなプログラムで開くことができます。 次の表に、見出しおよびその見出しが使用されているレポートを示します。

Heading	説明	使用先
ACCEPTANCE_STATUS	使用条件の同意状態	契約条件
APP_CATEGORY	デバイス上でアプリケーションが表示されるカテゴリ（パブリックストアアプリケーション、エンタープライズアプリケーションなど）	Top 10 Apps – Failed Deployment、Apps by Type & Category、Devices & Apps
APP_ID	一意のアプリケーション識別子	Devices & Apps
APP_NAME	アプリケーション名	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Devices & Apps
APP_OWNER	アプリの所有者（例：Worxアプリの場合はCitrix.com）	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Apps by Platform、Devices & Apps
APP_TYPE	アプリの種類（例：パブリックアプリケーションストアまたはエンタープライズ）	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type &

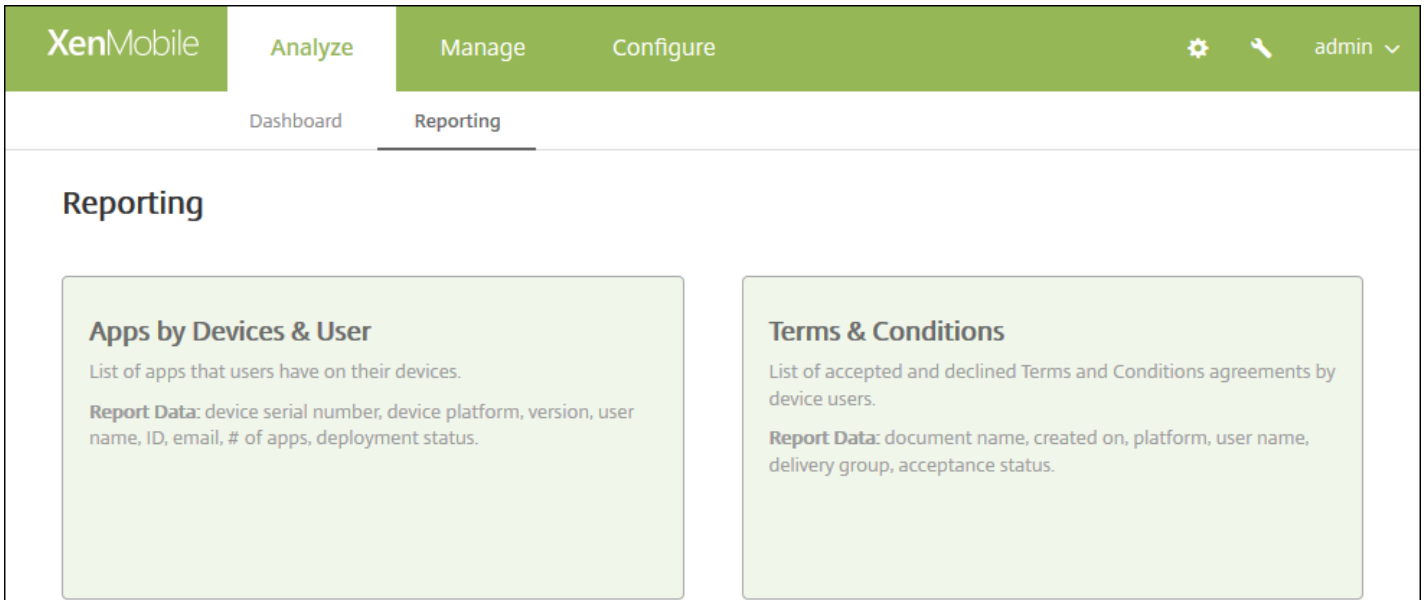
		Category、Devices & Apps
APP_VERSION	アプリケーションのバージョン	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Apps by Platform、Devices & Apps
APPS_ON_DEVICE	デバイスにインストールされているアプリケーションの数	Apps by Devices & User
CERTIFICATE_EXPIRATION	デバイスの証明書の有効期限が切れる日付	Devices & Apps
CREATION_DATE	使用条件ファイルの作成日	契約条件
DELIVERY_GROUP	展開済みのリソースに関連付けられているデリバリーグループ	契約条件
DEPLOYMENT_DATE	リソースが展開された日付	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Devices & Apps
DEPLOYMENT_SUCCESS、DEPLOYMENT_FAILED、DEPLOYMENT_PENDING	展開ステータス	Apps by Devices & User、Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Apps by Platform、Devices & Apps
DEPLOYMENT_TOTAL	展開が試行された回数の合計	Top 25 Apps、Top 10 Apps – Failed Deployment、Apps by Type & Category、Apps by Platform、Devices & Apps
DEVICE_MODE	デバイスモード（管理対象または非管理対象）	Jailbroken/Rooted Devices、Inactive Devices、Device Enrollment、Devices & Apps、Devices & Apps
DEVICE_OWNERSHIP	デバイスの所有権の分類（［BYOD］、［Corporate］、または［Unknown］）	Devices & Apps
DEVICE_PLATFORM	デバイスのプラットフォーム	Apps by Platform

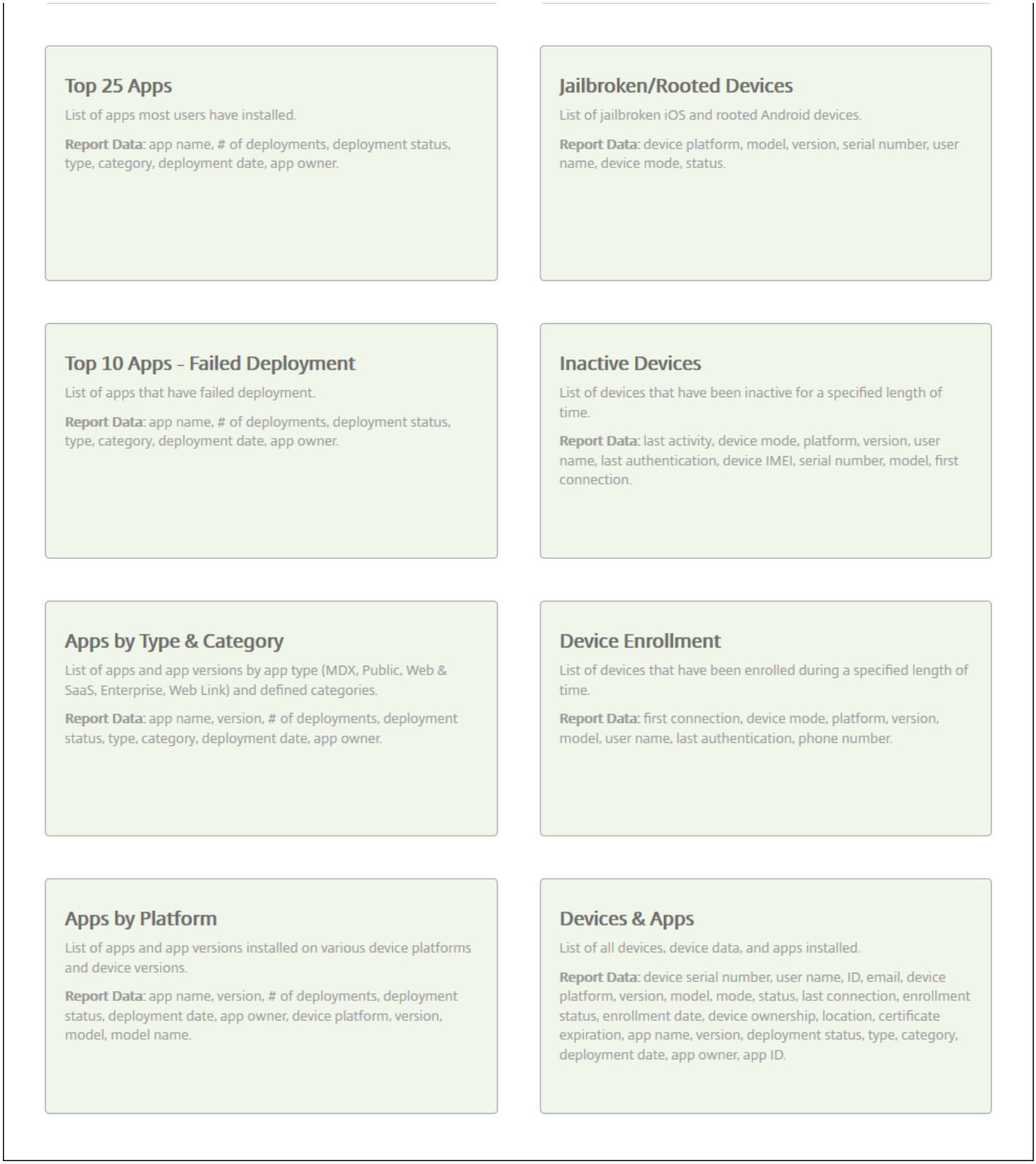
DEVICE_STATUS	デバイスコンプライアンスの状態	Devices & Apps
DEVICE_VERSION	デバイスのオペレーティングシステムのバージョン番号	Apps by Platform
DOCUMENT_NAME	使用条件ファイルの名前	契約条件
EMAIL	ユーザーのメールアドレス	Devices & Apps
ENROLLMENT_DATE	デバイスがXenMobileに登録された日付	Devices & Apps
ENROLLMENT_STATUS	デバイスの登録状態（登録済みまたは未登録）	Devices & Apps
FIRST_CONNECTION_DATE	デバイスが最初にXenMobileに接続した日付	Inactive Devices、Device Enrollment
IMEI	デバイスの国際移動体装置識別番号（IMEI）	Inactive Devices
LAST_ACTIVITY	最後のデバイスアクティビティの日付	Inactive Devices
LAST_AUTH_DATE	最後にデバイスがXenMobileへの認証を行った日付	Inactive Devices、Device Enrollment、Devices & Apps
LAST_USERNAME	デバイスに関連付けられている姓	Jailbroken/Rooted Devices、Inactive Devices、Device Enrollment
LOCATION	デバイスの地理的な場所	Devices & Apps
MANAGED	デバイスが管理対象であるかどうか	Jailbroken/Rooted Devices
MODEL	デバイスのモデル	Jailbroken/Rooted Devices、Inactive Devices、Device Enrollment、Apps by Platform
MODEL_NAME	デバイスのモデル	Devices & Apps
OS_VERSION	デバイスのオペレーティングシステムの	Apps by Devices & User、Inactive

	バージョン	Devices、Device Enrollment、Devices & Apps
PHONE_NUMBER	ユーザーの電話番号	Device Enrollment
PLATFORM	デバイスのプラットフォーム	Apps by Devices & User、Terms & Conditions、Jailbroken/Rooted Devices、Inactive Devices、Device Enrollment、Devices & Apps
SERIAL_NUMBER	デバイスのシリアル番号	Apps by Devices & User、Jailbroken/Rooted Devices、Inactive Devices、Devices & Apps
USER EMAIL	ユーザーのメールアドレス	Apps by Devices & User
USER_ID	一意のユーザー番号	Devices & Apps
USER_NAME	User name	Apps by Devices & User、Terms & Conditions、Devices & Apps
USERID	User ID	Apps by Devices & User

レポートを作成するには以下の手順を実行します。

1. XenMobileコンソールで **[Analyze]** タブをクリックして、 **[Reporting]** をクリックします。 **[Reporting]** ページが開きます。

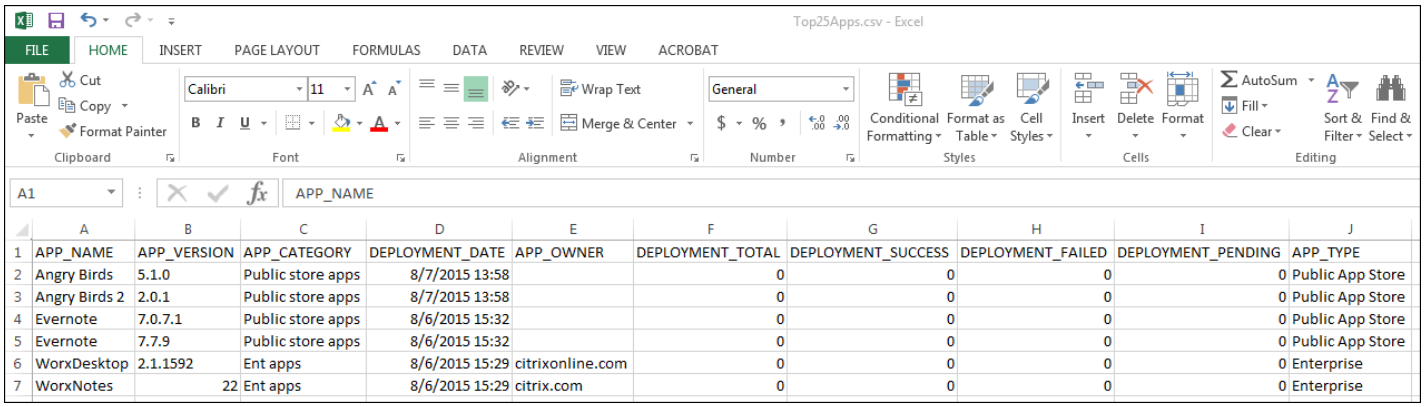




2. 作成するレポートを選択します。 使用するブラウザーに応じて、ファイルが自動的にダウンロードされるか、ファイルを保存するように求められます。

3. 作成するレポートごとに、手順2を繰り返します。

以下に、Microsoft Excelで開いたTop 25 Appsレポートの例を示します。



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORY	DEPLOYMENT_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	Angry Birds	5.1.0	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
3	Angry Birds 2	2.0.1	Public store apps	8/7/2015 13:58		0	0	0	0	Public App Store
4	Evernote	7.0.7.1	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
5	Evernote	7.7.9	Public store apps	8/6/2015 15:32		0	0	0	0	Public App Store
6	WorxDesktop	2.1.1592	Ent apps	8/6/2015 15:29	citrixonline.com	0	0	0	0	Enterprise
7	WorxNotes	22	Ent apps	8/6/2015 15:29	citrix.com	0	0	0	0	Enterprise

通知

Aug 02, 2016

XenMobileでの通知は以下の目的で利用できます。

- 多くのシステム関連機能に関して、選択したグループのユーザーに連絡します。 また、iOSデバイスを持つすべてのユーザー、コンプライアンスを満たしていないデバイスのユーザー、個人所有のデバイスを持つすべてのユーザーなど、特定のユーザーを対象にこれらの通知を行うこともできます。
- ユーザーとデバイスを登録します。
- コンプライアンスに関する問題が原因で、ユーザーのデバイスが社内ドメインからブロックされようとしているときや、デバイスがジェイルブレイクまたはルート化されたときなど、特定の条件が満たされた場合に（自動化された操作を使用して）ユーザーに自動的に通知します。 自動化された操作について詳しくは、「自動化された操作」を参照してください。

XenMobileで通知を送信するには、ゲートウェイおよび通知サーバーを構成する必要があります。 XenMobileで通知サーバーを設定して、SMTP（簡易メール転送プロトコル：Simple Mail Transfer Protocol）サーバーやショートメッセージサービス（SMS）のゲートウェイサーバーを構成し、電子メールやテキスト（SMS）通知をユーザーに送信することができます。 通知では、SMTPまたはSMSの2種類のチャネル経由でメッセージを送信できます。

- SMTPはコネクション型のテキストベースプロトコルで、通常はTCP（Transmission Control Protocol）経由で、メール送信者がコマンド文字列を発行して必要なデータを供給し、メール受信者と通信します。 SMTPセッションは、SMTPクライアント（メッセージの送信者）から送信されたコマンドと、コマンドに対応する、SMTPサーバーからの応答によって構成されます。
- SMSは、電話、 Web、またはモバイル通信システムのテキストメッセージサービスコンポーネントです。 標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

また、XenMobileでキャリアSMSゲートウェイを設定して、電話会社のSMSゲートウェイ経由で送信される通知を構成することもできます。 電話会社はSMSゲートウェイを使用して、通信ネットワークと相互にSMSメッセージを送受信します。 これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

このアーティクルの手順では、SMTPサーバー、SMSゲートウェイ、キャリアSMSゲートウェイの構成方法について説明します。

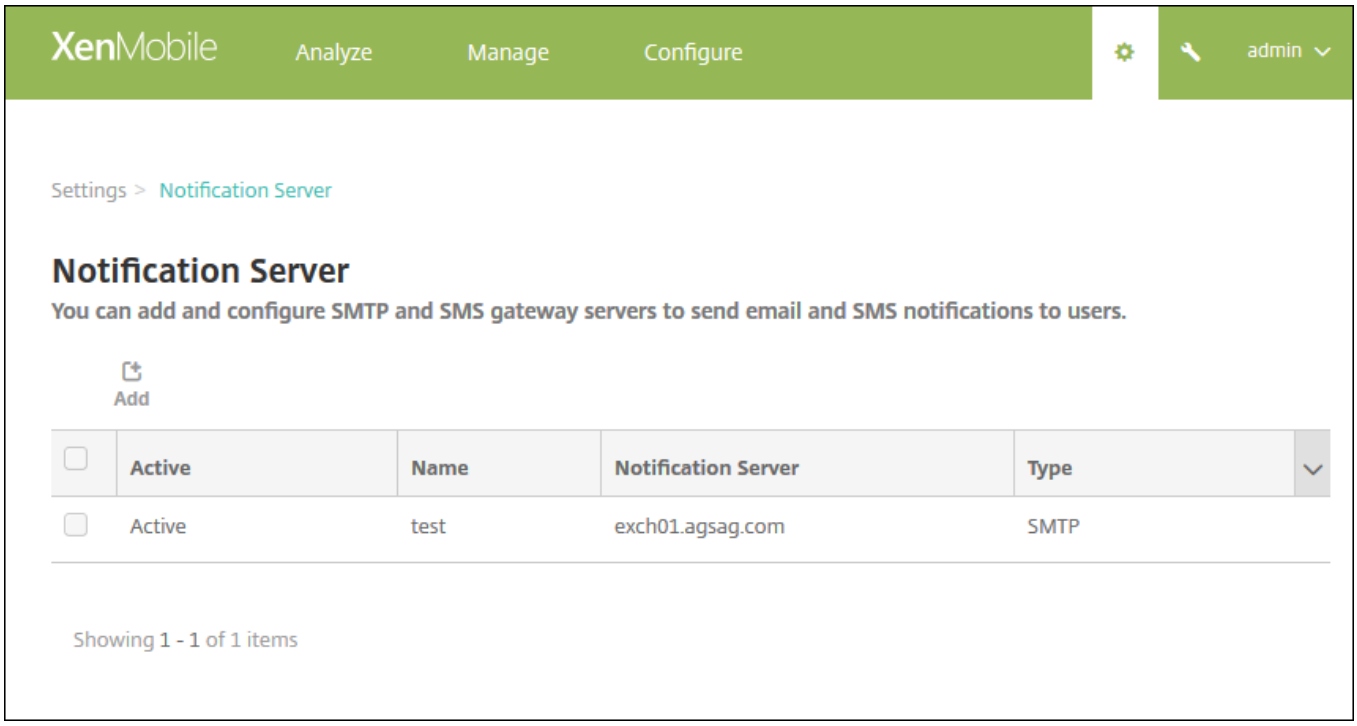
前提条件

- SMSゲートウェイを構成する前に、システム管理者に問い合わせてサーバー情報を確認してください。 SMSサーバーが社内サーバーでホストされているか、ホストされている電子メールサービスに含まれているかを確認することが重要です。後者の場合は、サービスプロバイダーのWebサイトからの情報が必要です。
- メッセージをユーザーに送信するためのSMTP通知サーバーを構成する必要があります。 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、ホストされている電子メールサービスの場合は、サービスプロバイダーのWebサイトで適切な構成情報を確認してください。
- SMTPサーバーとSMSサーバーは、それぞれ一度に1つのみがアクティブになります。
- 通知を正しく送信するには、ネットワークのDMZ内のXenMobileからポート25を開き、内部ネットワークのSMTPサーバーにポイントバックする必要があります。

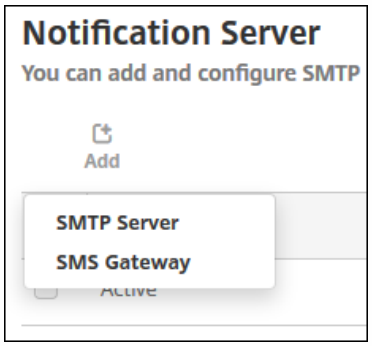
SMTPサーバーおよびSMSゲートウェイを構成するには

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

2. [**Notifications**] の下の [**Notification Server**] をクリックします。 [**Notification Server**] ページが開きます。

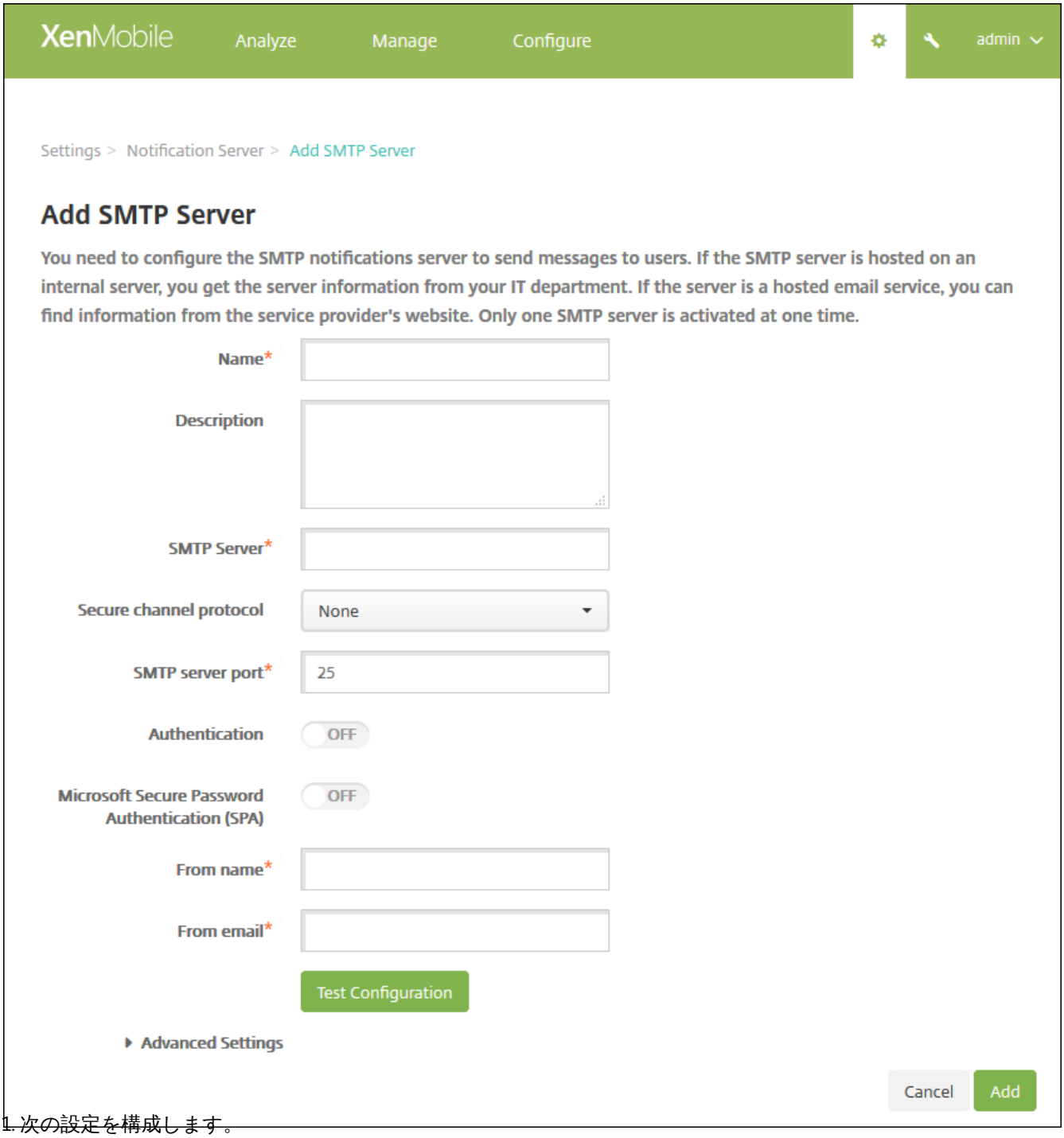


2. **[Add]** をクリックします。 SMTPサーバーまたはSMSゲートウェイを 構成するためのオプションが示された メニューが表示されます。



- SMTPサーバーを追加するには、 **[SMTP Server]** を選択します。この設定を構成する手順については、 「SMTPサーバーを追加するには」を参照してください。
- SMSゲートウェイを追加するには、 **[SMS Gateway]** を選択します。この設定を構成する手順については、 「SMSゲートウェイを追加するには」を参照してください。

SMTPサーバーを追加するには



1. 次の設定を構成します。

- **Name**：このSMTPサーバーアカウントに関連付ける名前を入力します。
- **Description**：任意で、サーバーの説明を入力します。
- **SMTP Server**：サーバーのホスト名を入力します。 ホスト名には、完全修飾ドメイン名（FQDN）またはIPを指定できます。
- **Secure channel protocol**：（サーバーが安全な認証を使用するよう構成されている場合）一覧から、サーバーが使用する適切なセキュアチャネルプロトコルとして［**SSL**］、［**TLS**］、または［**None**］を選択します。 デフォルトは［**None**］です。
- **SMTP server port**：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。
- **Authentication**：［**ON**］または［**OFF**］を選択します。 デフォルトは［**OFF**］です。

- ［**Authentication**］を有効にした場合は、次の設定を構成します。
  - **User name**：認証に使用するユーザー名を入力します。
  - **Password**：認証に使用するユーザーのパスワードを入力します。
- **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。
- **From Name**：クライアントがこのサーバーから通知メールを受信したとき、**メールの送信者**として表示される名前を入力します。 たとえば、「Corporate IT」です。
- **From email**：SMTPサーバーによって送信された通知に、メール受信者が返信する場合に使用されるメールアドレスを入力します。

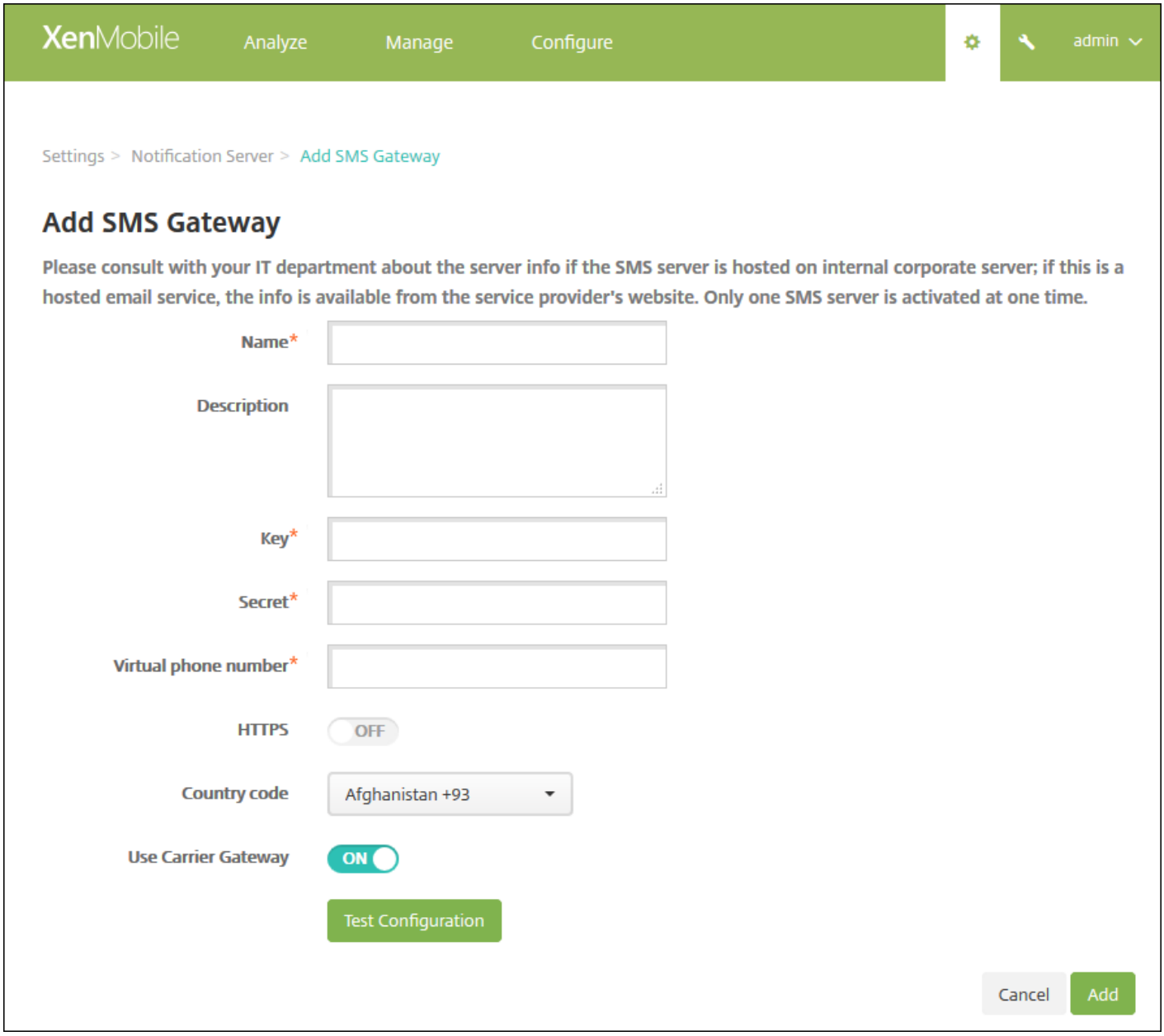
2. ［**Test Configuration**］をクリックして、テストのメール通知を送信します。

3. ［**Advanced Settings**］を展開して以下の設定を構成します。

- **番号 of SMTP retries**：SMTPサーバーからのメッセージの送信が失敗した場合に再試行する回数を入力します。 デフォルトは5です。
- **SMTP Timeout**：SMTP要求送信時に待機する時間（秒）を入力します。 送信しているメッセージが、タイムアウトに起因して失敗し続ける場合には、この値を大きくします。 この値を小さくするとタイムアウト回数が多くなり、配信されないメッセージが増える場合があるため、注意してください。 デフォルトは30秒です。
- **Maximum number of SMTP recipients**：SMTPサーバーによって送信される各メールメッセージの最大受信者数を入力します。 デフォルトは100です。

4. ［**Add**］をクリックします。

SMSゲートウェイを追加するには



注意

XenMobileはNexmo SMSメッセージのみをサポートします。 Nexmoメッセージを使用するためのアカウントがまだない場合は、Webサイトにアクセスしてアカウントを作成してください。

1. 次の設定を構成します。

- **Name**：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。
- **Description**：任意で、構成の説明を入力します。
- **Key**：アカウントをアクティブ化するときにシステム管理者から提供された、数値形式の識別子を入力します。 このフィールドは必須です。
- **Secret**：パスワードを紛失した場合や盗まれた場合にアカウントへのアクセスに使用する、システム管理者から提供され

シークレットを入力します。 このフィールドは必須です。

- **Virtual Phone Number**：このフィールドは、北米の電話番号（プレフィックスが+1）への送信時に使用されます。 Nexmo仮想電話番号を入力する必要があります。そのほかの場合は、意味のあるラベルまたは名前を入力します。 仮想電話番号はNexmoのWebサイトで購入できます。
- **HTTPS**：NexmoへのSMS要求の伝送にHTTPSを使用するかどうかを選択します。 デフォルトは[**OFF**]です。
- **Country Code**：一覧から、組織内受信者のデフォルトのSMS国コードプレフィックスを選択します。 このフィールドは常に+記号で始まります。 デフォルトは［**Afghanistan +93**］です。

2. ［**Test Configuration**］をクリックし、現在の構成を使用してテストメッセージを送信します。 認証エラーや仮想電話番号エラーなど、接続エラーが即時に検出され、表示されます。 メッセージは、携帯電話間で送信された場合と同様の所要時間で受信されます。

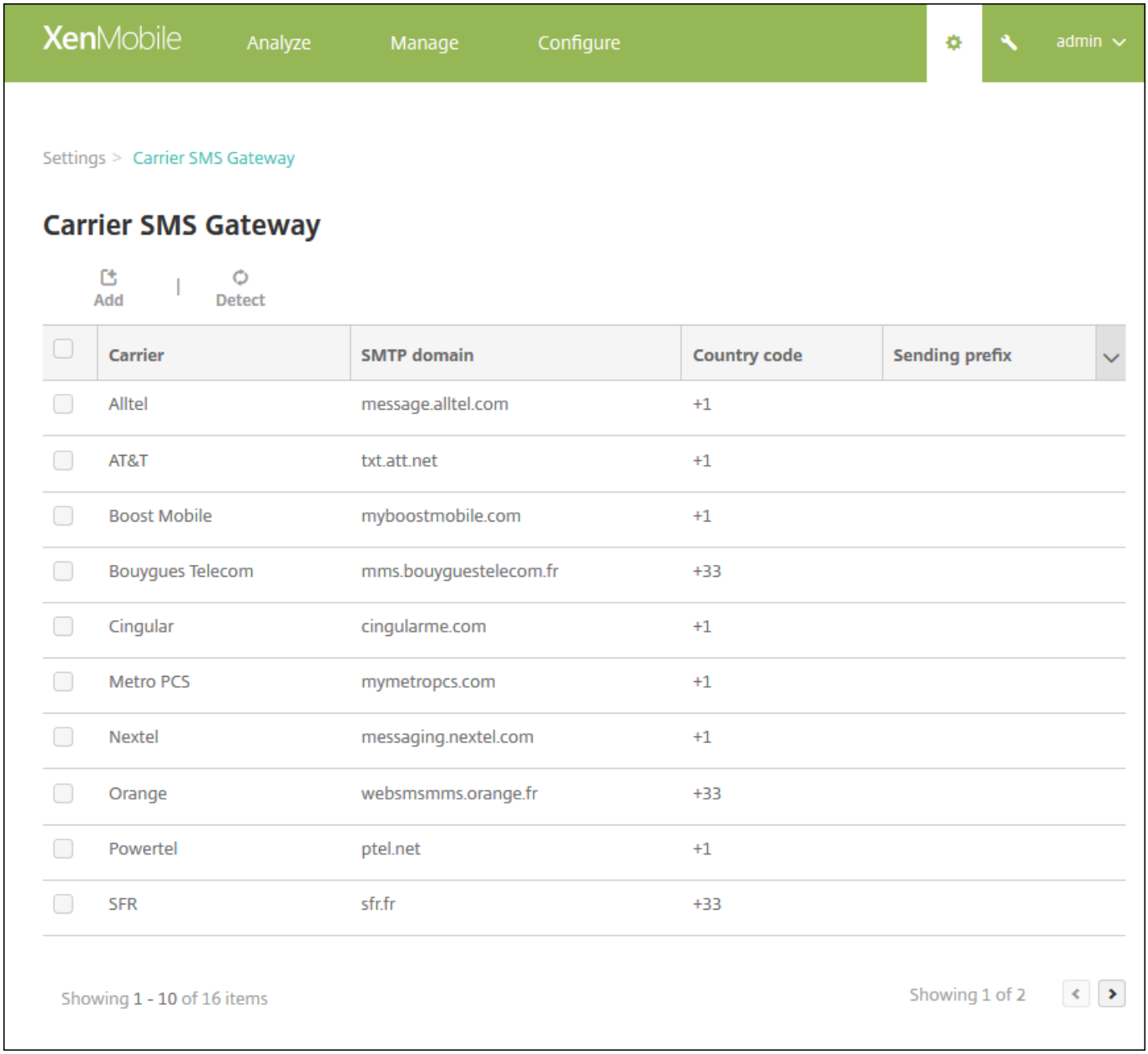
2. [**Add**]をクリックします。

キャリアSMSゲートウェイを追加するには

XenMobileでキャリアSMSゲートウェイを設定して、電話会社のSMSゲートウェイ経由で送信される通知を構成できます。 電話会社はショートメッセージサービス（SMS）ゲートウェイを使用して、通信ネットワークと相互にSMSメッセージを送受信します。 これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

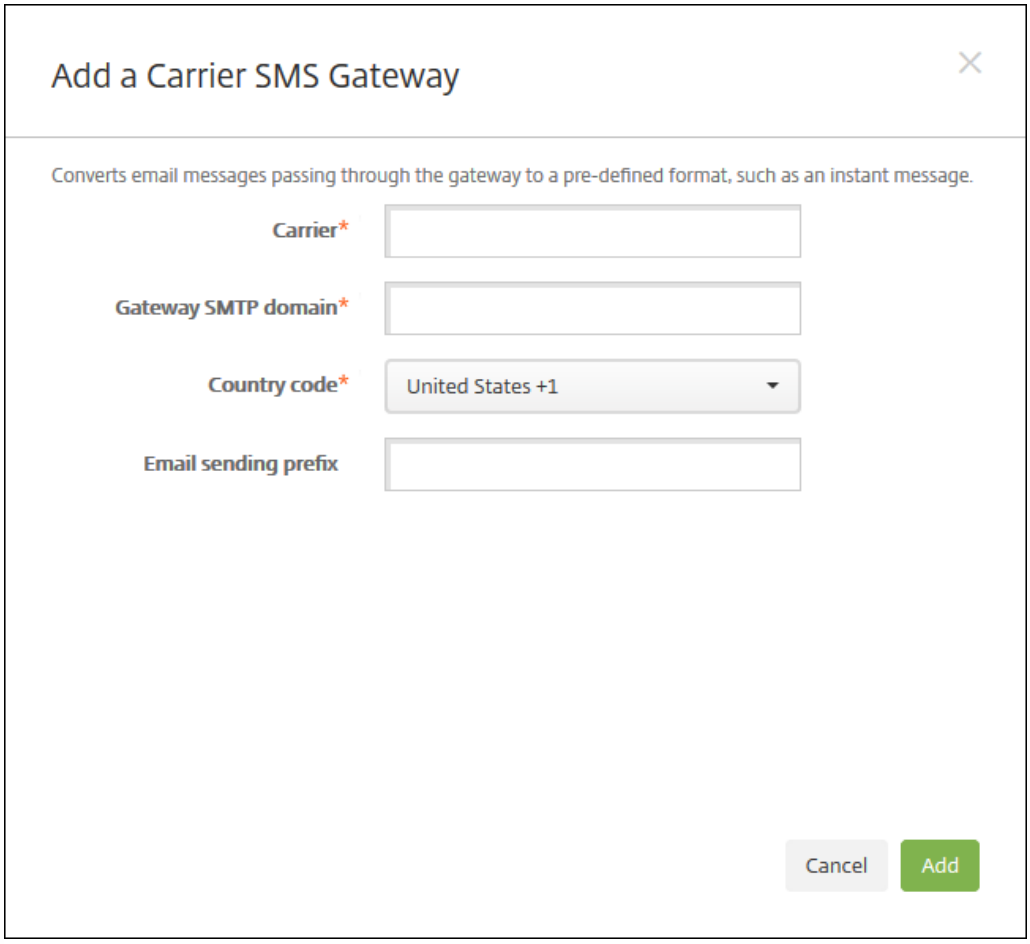
1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 ［**Settings**］ページが開きます。

2. ［**Notifications**］の下の［**Carrier SMS Gateway**］をクリックします。 ［**Carrier SMS Gateway**］ページが開きます。



3. 次のいずれかを行います。

- ゲートウェイを自動的に検出するには［**Detect**］をクリックします。 新しいキャリアが検出されなかったことを示すダイアログボックス、または登録済みのデバイス間で検出された新しいキャリアを一覧表示したダイアログボックスが開きます。
- ［**Add**］をクリックします。 ［**Add a Carrier SMS Gateway**］ダイアログボックスが開きます。



注：XenMobileはNexmo SMSメッセージのみをサポートします。 Nexmoメッセージを使用するためのアカウントがまだない場合は、Webサイトにアクセスしてアカウントを作成してください。

4. 次の設定を構成します。

- **Carrier**：電話会社の名前を入力します。
- **Gateway SMTP domain**：SMTPゲートウェイに関連付けられたドメインを入力します。
- **Country code**：一覧から、電話会社の国コードを選択します。
- **Email sending prefix**：任意で、メール送信プレフィックスを指定します。

5. [**Add**] をクリックして新しいキャリアを追加するか、[**Cancel**] をクリックして操作を取り消します。

NetScaler GatewayとXenMobile

Oct 25, 2016

XenMobileを使用してNetScaler Gatewayを構成すると、リモートデバイスで内部ネットワークにアクセスするための認証メカニズムが確立されます。 この機能を利用すると、モバイルデバイス上のアプリケーションからNetScaler Gatewayへのマイクロ VPNを作成し、イントラネット内にある社内サーバーにアクセスすることができます。 NetScaler Gatewayの構成はXenMobileコンソールで行います。

注：XenMobileでサポートされるNetScaler Gatewayのバージョンについては、「XenMobileの互換性」を参照してください。 NetScalerでXenMobile用にNetScaler Gatewayを設定する方法について詳しくは、「Configuring Settings for Your XenMobile Environment」を参照してください。

認証

XenMobile操作中の認証には、次のコンポーネントが関係します。

- **XenMobileサーバー**：登録に関わるセキュリティおよび登録操作の定義は、XenMobileサーバーで行います。 ユーザー登録オプションにより、登録をすべてのユーザーと招待されたユーザーのみのどちらに対して有効にするか、また2要素認証または3要素認証を必須にするかどうかなどを設定できます。 XenMobileのクライアントプロパティを使用して、Worx PIN認証を有効にしたり、PINの複雑度や有効期限を設定したりすることもできます。
- **NetScaler**：NetScalerはマイクロVPN SSLセッションの中断機能とネットワークの転送中保護機能を備えており、アプリへのユーザーアクセス時の毎回の認証動作を定義できます。
- **Worx Home**：Worx Homeは、XenMobileサーバーと連携して登録を処理します。 Worx Homeは、デバイス上でNetScalerと通信するエンティティです。セッションの有効期限が切れると、Worx HomeはNetScalerから認証チケットを取得してMDXアプリに渡します。 中間者攻撃を防止する証明書ピン留め機能を使用することをお勧めします。 詳しくは、「Worx Home」の「証明書ピン留め」を参照してください。

  また、Worx Homeではポリシーのプッシュ、アプリのタイムアウト時のNetScalerでの新規セッションの作成、MDXのタイムアウトおよび認証動作の定義を行うことができるため、MDXセキュリティコンテナーの使いやすさが向上します。 ほかにも、Worx Homeではジェイルブレイクの検出、地理位置情報のチェック、適用するポリシーの管理も行います。

- **MDXポリシー**：MDXポリシーにより、デバイス上にデータの格納場所が作成されます。 各種MDXポリシーで、NetScalerへのマイクロVPN接続のリダイレクト、オフラインモード制限の適用、各種クライアントポリシー（タイムアウトなど）の適用を行います。

認証について詳しくは、「認証」を参照してください。1要素認証と2要素認証、認証に関係するポリシー、設定、およびクライアントプロパティ、セキュリティが最低のものから最高のものまでの3種類のXenMobile構成例などについて説明されています。

構成について詳しくは、以下の記事を参照してください。

ドメインおよびセキュリティトークン認証の構成

クライアント証明書認証の構成

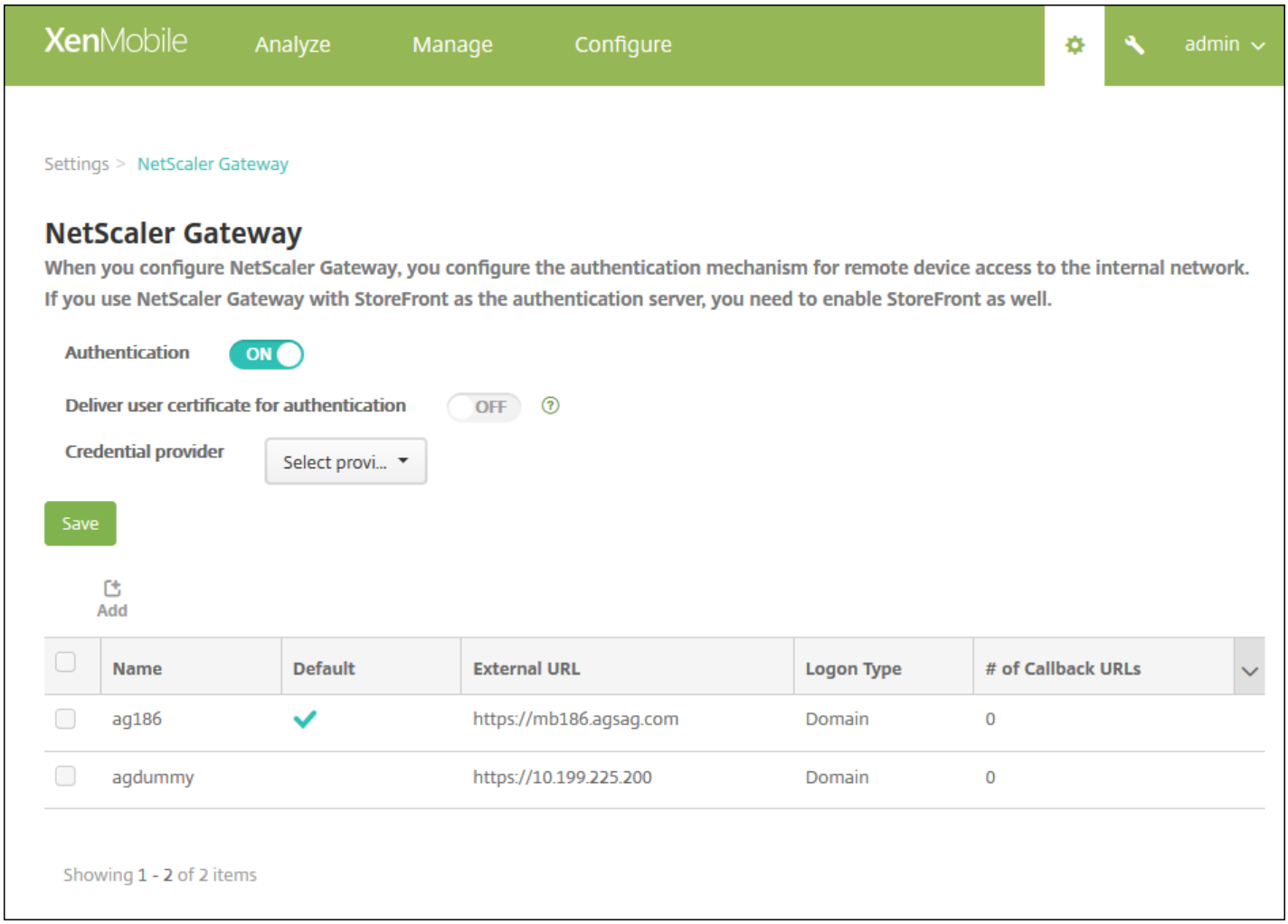
証明書認証およびセキュリティトークン認証のためのXenMobileの構成

XenMobileおよびShareFileアプリでのSAMLを使用するシングルサインオンの構成

NetScaler Gatewayを構成するには

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

2. **[Server]** の下の **[NetScaler Gateway]** をクリックします。 **[NetScaler Gateway]** ページが開きます。



次の設定を構成します。

- **Authentication**：暗号化を有効にするかどうかを選択します。 デフォルトは **[ON]** です。
- **Deliver user certificate for authentication**：XenMobileでWorx Homeと認証証明書を共有し、NetScaler Gatewayでクライアント証明書認証を処理できるようにするかどうかを選択します。 デフォルトは **[OFF]** です。
- **Credential Provider**：ボックスの一覧で、使用する資格情報プロバイダーを選択します。 詳しくは、 資格情報プロバイダー」を参照してください。

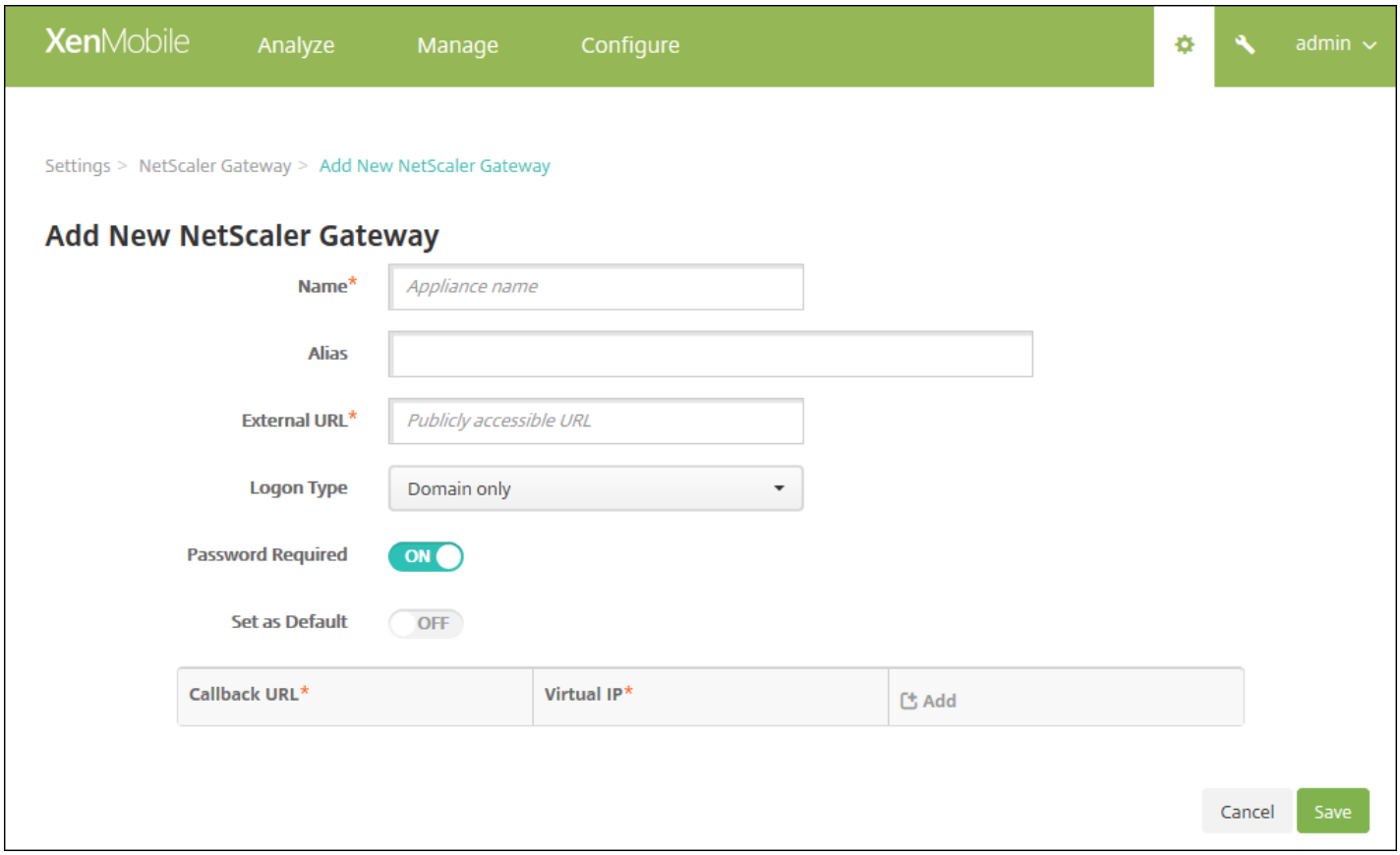
3. **[Save]** をクリックします。

新しいNetScaler Gatewayインスタンスを追加するには

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

2. **[Server]** の下の **[NetScaler Gateway]** をクリックします。 **[NetScaler Gateway]** ページが開きます。

3. **[Add]** をクリックします。 **[Add New NetScaler Gateway]** ページが開きます。



4. 次の設定を構成します。

- **[Name]** ：NetScaler Gatewayインスタンスの名前を入力します。
- **[Alias]** ：任意で、エイリアスを入力します。
- External URL：NetScaler Gatewayの、パブリックにアクセスできるURLを入力します。 たとえば、https://receiver.comなどです。
- **Logon type**：一覧から、ログオンの種類を選択します。 種類には、**[Domain only]** 、 **[Security token only]** 、 **[Domain and security token]** 、 **[Certificate]** 、 **[Certificate and domain]** 、 **[Certificate and security token]** があります。 デフォルトは **[Domain only]** です。

  複数のドメインを使用している場合、**[Domain only]** は無効です。 **[Certificate and domain]** を使用する必要があります。 **[Domain only]** など一部のオプションでは、 **[Password]** フィールドを変更できません。

  このログオンの種類の場合、このフィールドは常に **[ON]** です。 また、 **[Password Required]** フィールドのデフォルト値は、選択した **[Logon Type]** に基づいて変化します。

  [Certificate and security token] を使用する場合、NetScaler GatewayでWorx Homeがサポートされるようにするには、追加の設定が必要となります。 詳しくは、「証明書認証およびセキュリティトークン認証のためのXenMobileの構成」を参照してください。
- **Password Required**：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**[ON]** です。
- **Set as Default**：このNetScaler Gatewayをデフォルトとして使用するかどうかを選択します。 デフォルトは**[OFF]** です。

5. **[Save]** をクリックします。 新しいNetScaler Gatewayが追加され、表に表示されます。 表で名前をクリックして、イン

スタンスを編集または削除できます。

NetScaler Gatewayインスタンスを追加した後、コールバックURLを追加したり、NetScaler Gateway VPN仮想IPアドレスを指定したりすることができます。 **注**：この設定はオプションですが、特にXenMobileサーバーがDMZに配置されている場合に、セキュリティ強化のために構成できます。

1. ［NetScaler Gateway］画面の表でNetScaler Gatewayを選択し、 **［Add］** をクリックします。 **［Add New NetScaler Gateway］** ページが開きます。

2. コールバックURLが一覧表示されている表で、 **［Add］** をクリックします。

3. コールバックURLを指定します。 このフィールドは完全修飾ドメイン名（FQDN）を表し、要求元がNetScaler Gatewayであることを検証します。

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

LDAP構成

Aug 30, 2016

XenMobileでは、LDAP（Lightweight Directory Access Protocol）に準拠している1つまたは複数のディレクトリ（Active Directoryなど）への接続を構成することができます。 そしてこのLDAP構成を使用して、グループ、ユーザーアカウント、関連するプロパティをインポートします。 LDAPは、オープンソースで特定のベンダーに依存しないアプリケーションプロトコルであり、インターネットプロトコル（IP）ネットワーク経由で分散ディレクトリ情報サービスへのアクセスや管理を行うためのものです。 ディレクトリ情報サービスは、ネットワークで使用可能な、ユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。 LDAPは一般的に、シングルサインオン（SSO）をユーザーに提供するために利用されます。SSOでは（ユーザーごとに）1つのパスワードを複数のサービスで共有します。ユーザーは、会社のWebサイトに一度ログオンすれば、社内イントラネットに自動的にログインできます。

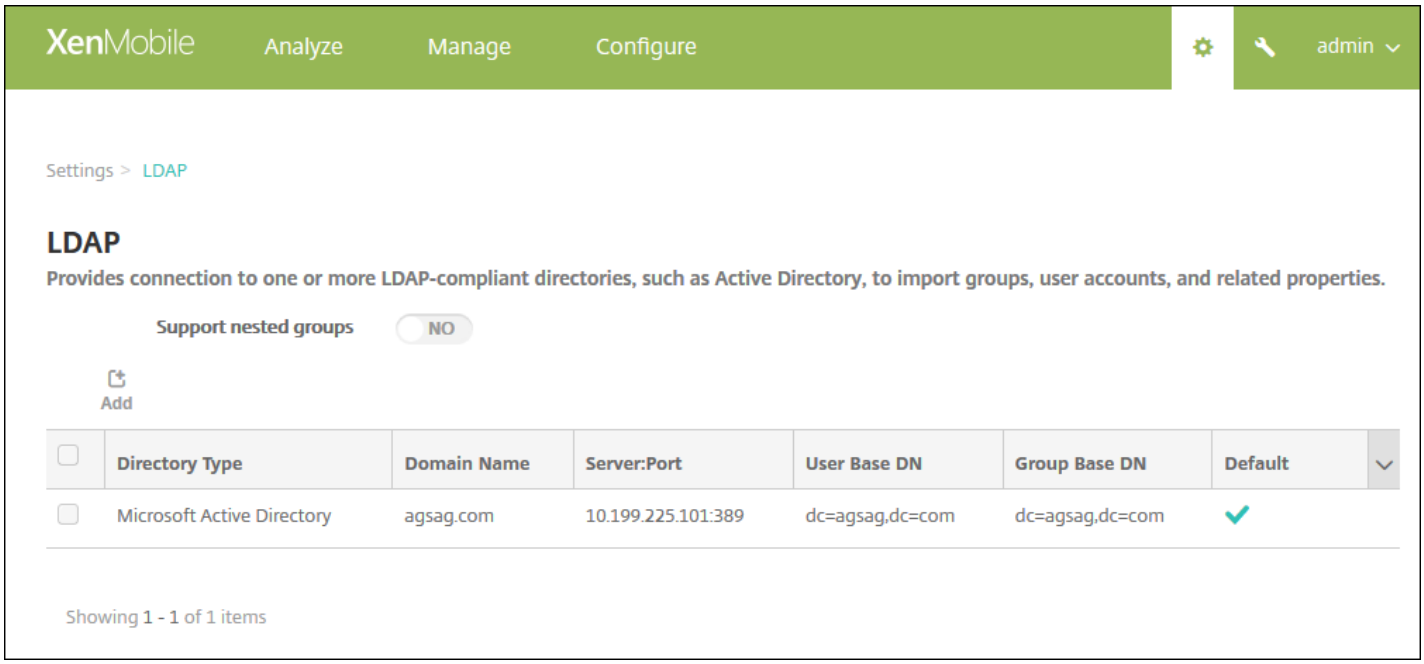
LDAPの動作

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

XenMobileでLDAP接続を追加するには

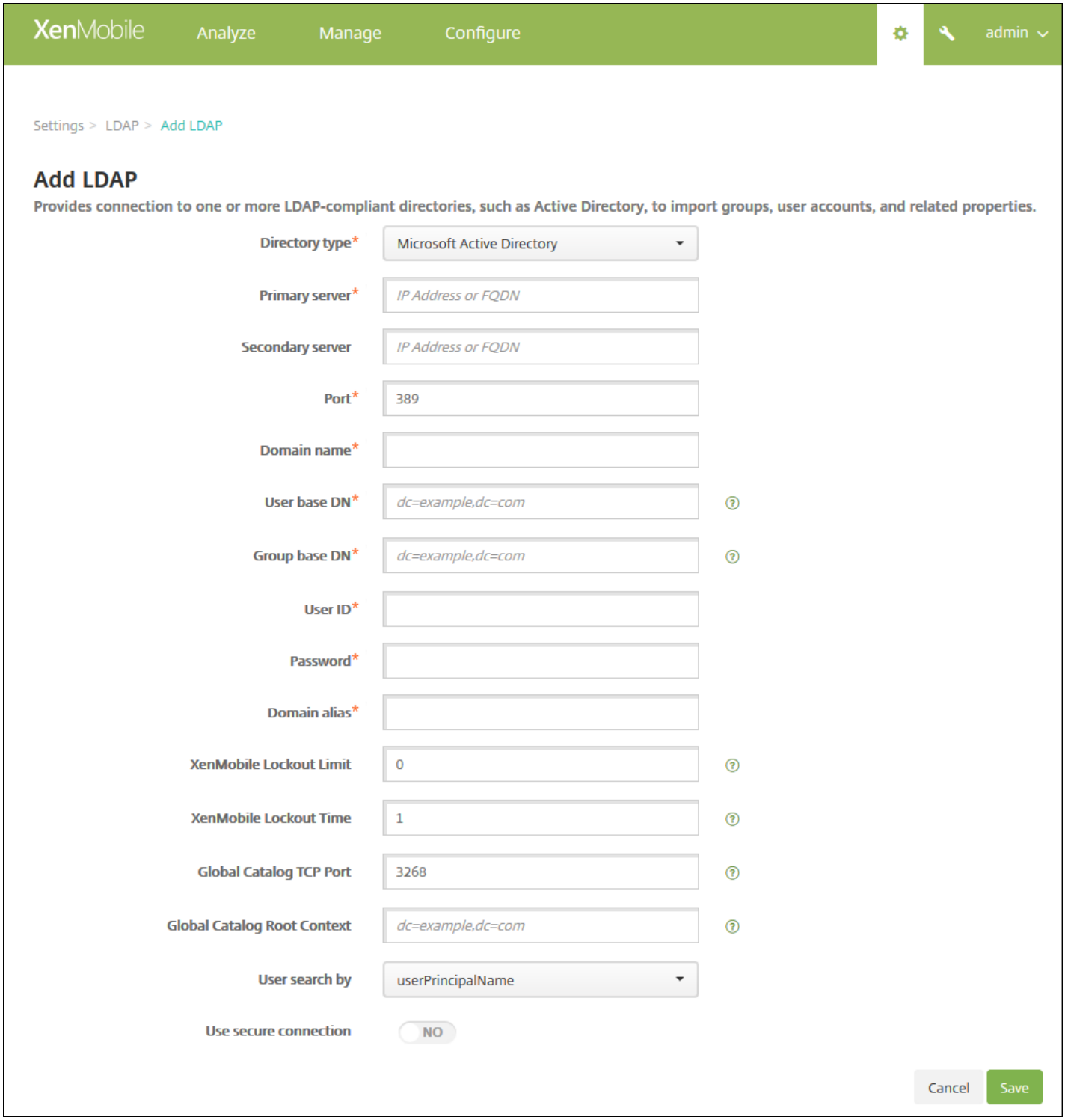
1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。

2. **[Server]** の下の **[LDAP]** をクリックします。 **[LDAP]** ページが開きます。 このページでは、LDAP準拠のディレクトリを追加、編集、削除することができます。



LDAP準拠のディレクトリを追加するには

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



2. 次の設定を構成します。

- **Directory type**：一覧から、適切なディレクトリの種類を選択します。 デフォルトは **[Microsoft Active Directory]** です。
- **Primary server**：LDAPで使用するプライマリサーバーを入力します。IPアドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
- **Secondary server**：任意で、セカンダリサーバーのIPアドレスまたはFQDNを入力します（構成されている場合）。
- **Port**：LDAPサーバーで使用するポート番号を入力します。 デフォルトでは、セキュリティ保護されていないLDAP接続用

のポート番号389に設定されています。 セキュリティ保護されたLDAP接続ではポート番号636、Microsoftのセキュリティ保護されていないLDAP接続では3268、Microsoftのセキュリティ保護されたLDAP接続では3269を使用します。

- **Domain name**：ドメイン名を入力します。
- **User base DN**：Active Directory内でのユーザーの位置を一意の識別子で入力します。 構文の例には、「ou=users, dc=example, or dc=com」などがあります。
- **Group base DN**：「cn=groupname」のように指定される、グループのベースDNグループ名を入力します。 たとえば、「cn=users, dc=servername, dc=net」で、「cn=users」はグループ名です。DNおよびサーバー名は、Active Directoryを実行しているサーバーの名前を表します。
- **User ID**：Active Directoryアカウントに関連付けられたユーザーIDを入力します。
- **Password**：ユーザーに関連付けられたパスワードを入力します。
- **Domain alias**：ドメイン名のエイリアスを入力します。
- **XenMobile Lockout Limit**：ログオンの試行失敗回数として、0～999の数値を入力します。 このフィールドを「0」に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
- **XenMobile Lockout Time**：ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、0～99999の数値を入力します。 このフィールドを「0」に設定すると、ロックアウト後にユーザーが待機する必要はなくなります。
- **Global Catalog TCP Port**：グローバルカタログサーバーのTCPポート番号を入力します。 デフォルトでは、TCPポート番号は3268に設定されています。SSL接続では、ポート番号3269を使用します。
- **Global Catalog Root Context**：任意で、Active Directoryでのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。 この検索では、標準のLDAP検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- **User search by**：一覧から、［**userPrincipalName**］または［**sAMAccountName**］を選択します。 デフォルトは［**userPrincipalName**］です。
- **Use secure connection**：セキュリティ保護された接続を使用するかどうかを選択します。 デフォルトは［**NO**］です。

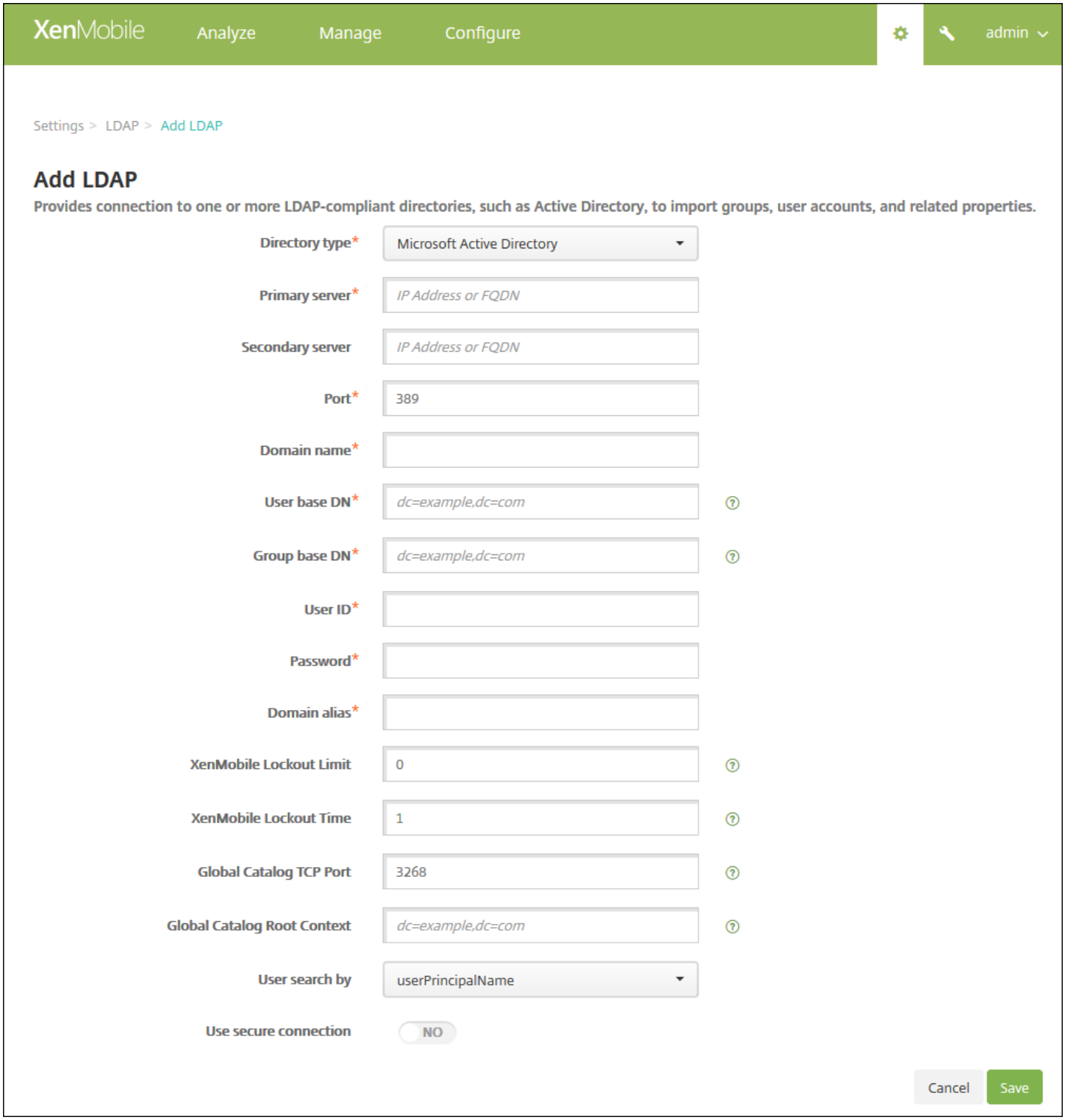
3. ［**Save**］をクリックします。

LDAP準拠のディレクトリを編集するには

1. ［**LDAP**］の表で、編集するディレクトリ選択します。

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

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



3. 必要に応じて以下の情報を変更します。

- **Connection type**：一覧から、適切なディレクトリ の種類を選択します。
- **Primary server**：LDAPで使用するプライマリサーバーを入力します。IPアドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
- **Secondary server**：任意で、セカンダリサーバーのIPアドレスまたはFQDNを入力します（構成されている場合）。
- **Port**：LDAPサーバーで使用するポート番号を入力します。 デフォルトでは、セキュリティ保護されていないLDAP接続用のポート番号389に設定されています。 セキュリティ保護されたLDAP接続ではポート番号636、Microsoftのセキュリティ

保護されていないLDAP接続では3268、Microsoftのセキュリティ保護されたLDAP接続では3269を使用します。

- **Domain name**：このフィールドは変更できません。
- **User base DN**：Active Directory内でのユーザーの位置を一意の識別子で入力します。 構文の例には、「ou=users, dc=example, or dc=com」などがあります。
- **Group base DN**：「cn=groupname」のように指定される、グループのベースDNグループ名を入力します。 たとえば、「cn=users, dc=servername, dc=net」で、「cn=users」はグループ名です。DNおよび サーバー名 は、Active Directoryを実行しているサーバーの名前を表します。
- **User ID**：Active Directoryアカウントに関連付けられたユーザーIDを入力します。
- **Password**：ユーザーに関連付けられたパスワードを入力します。
- **Domain alias**：ドメイン名のエイリアスを入力します。
- **XenMobile Lockout Limit**：ログオンの試行失敗回数として、0～999の 数値を 入力します。 このフィールドを「0」に設定すると、ユーザーがログオンの試行失敗によって ロックアウトされることは なくなります。
- **XenMobile Lockout Time**：ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、0～99999の数値を入力します。 このフィールドを「0」に設定すると、ロックアウト後にユーザーが待機する必要はなくなります。
- **Global Catalog TCP Port**：グローバルカタログサーバーのTCPポート番号を入力します。 デフォルトでは、TCPポート番号は3268に設定されています。SSL接続では、ポート番号3269を使用します。
- **Global Catalog Root Context**：任意で、Active Directoryでのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。 この検索では、標準のLDAP検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- **User search by**：一覧から、 **[userPrincipalName]** または **[sAMAccountName]** を選択します。
- **Use secure connection**：セキュリティ保護された接続を使用するかどうかを選択します。

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

LDAP準拠のディレクトリを削除するには

1. **[LDAP]** の表で、削除するデバイスを選択します。

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

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

ドメインおよびセキュリティトークン認証の構成

Oct 25, 2016

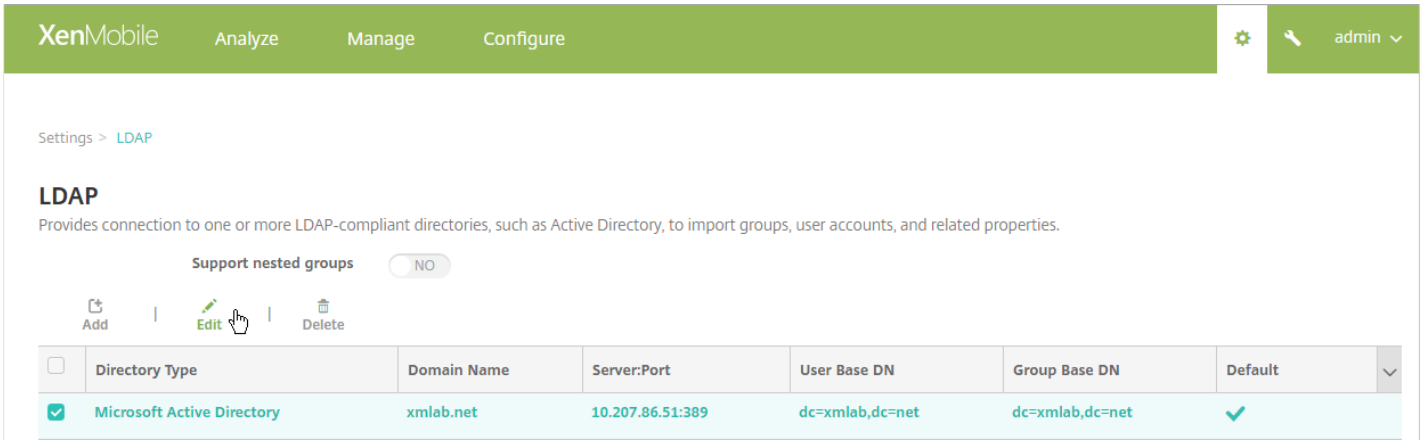
RADIUSプロトコルを使用して、LDAP資格情報とワンタイムパスワードによる認証をユーザーに要求するようにXenMobileを構成できます。

ユーザービリティを最適化するためにこの構成をWorx PINおよびActive Directoryパスワードキャッシュと組み合わせて、ユーザーがActive Directoryのユーザー名とパスワードを繰り返し入力する必要がないようにすることができます。 登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力する必要が生じます。

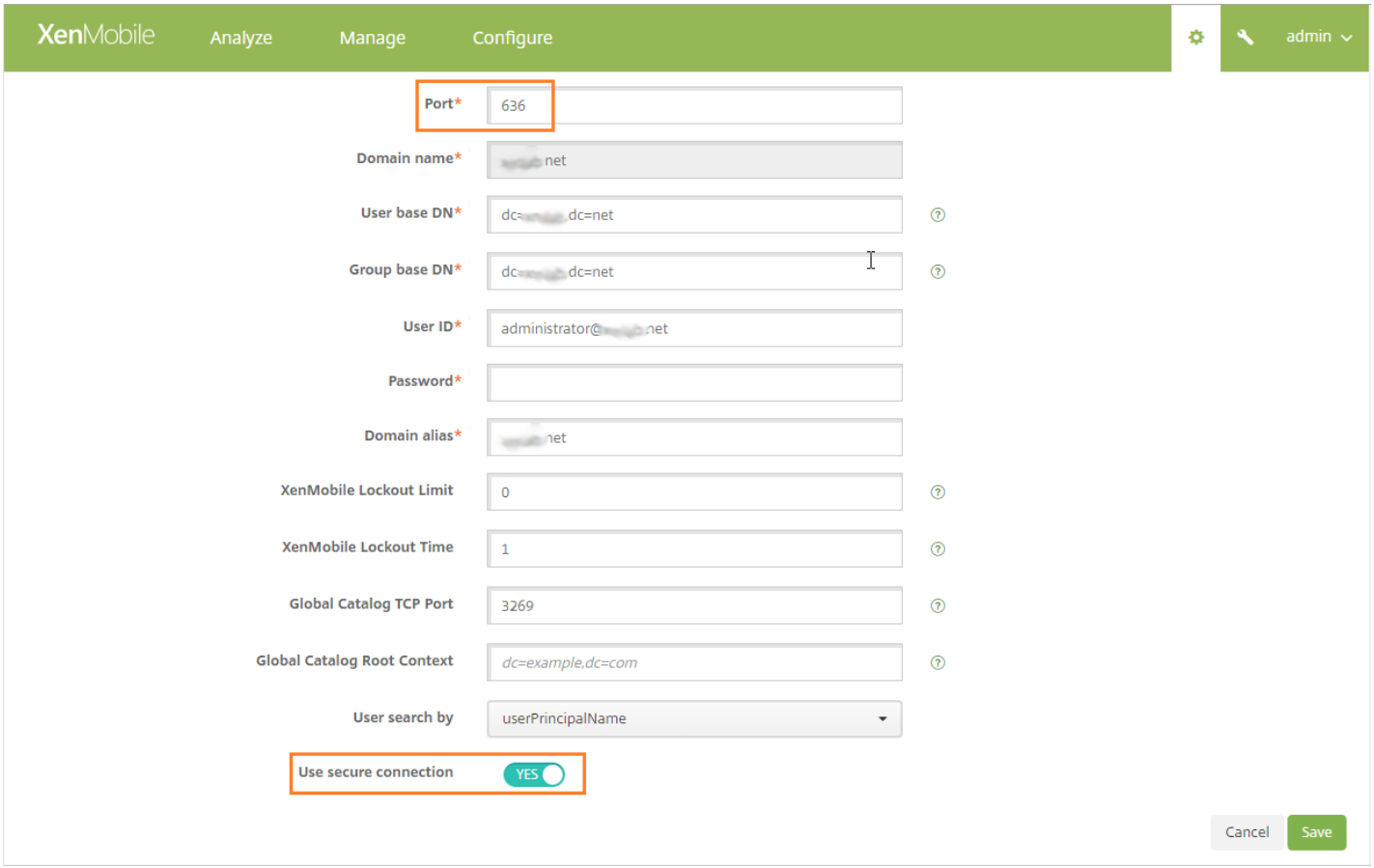
LDAP設定の構成

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

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



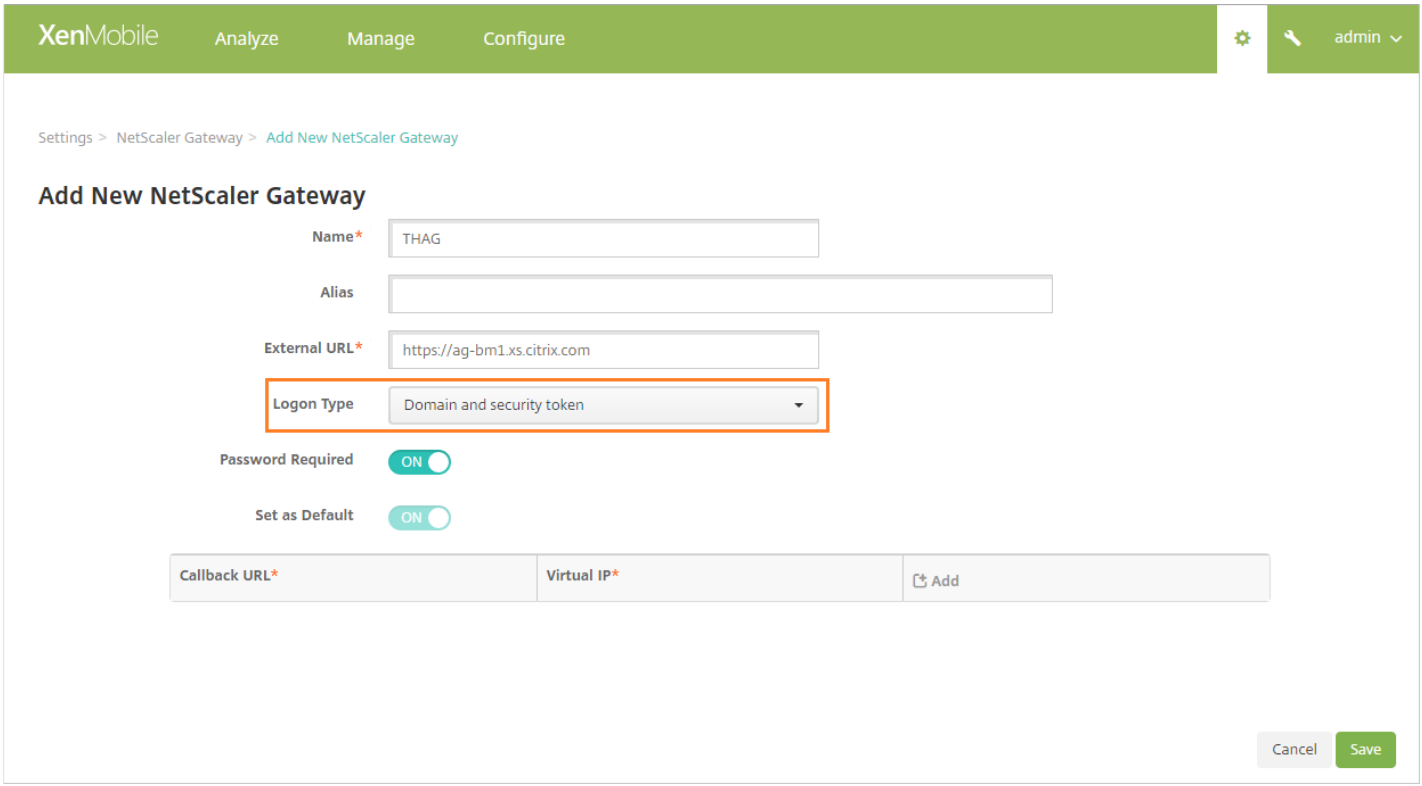
3. **[Port]** が**636**であることを確認します（セキュリティで保護されたLDAP接続の場合）。セキュリティで保護されたMicrosoft LDAP接続の場合は**3269**です。
4. **[Use secure connection]** を **[Yes]** に変更します。



NetScaler Gateway設定を構成する

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

1. **[Settings]** で **[NetScaler Gateway]** をクリックします。
2. NetScaler Gatewayを選択して **[Edit]** をクリックします。
3. **[Logon Type]** で **[Domain and security token]** を選択します。



Worx PINとActive Directoryパスワードキャッシュの有効化

Worx PINとActive Directoryパスワードキャッシュを有効化するには、**[Settings] > [Client Properties]** に移動し、チェックボックス **[Enable Worx PIN Authentication]** および **[Enable User Password Caching]** を選択します。詳しくは、「クライアントプロパティリファレンス」を参照してください。

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

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

証明書

Oct 25, 2016

XenMobileでは証明書を使用し、セキュリティで保護された接続を作成してユーザーを認証します。

XenMobileには、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生成される自己署名SSL（Secure Sockets Layer）証明書がデフォルトで含まれています。 このSSL証明書を、既知のCA（Certificate Authority：証明機関）からの信頼されるSSL証明書に置き換えることをお勧めします。

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

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

XenMobileでiOSデバイスを登録して管理するには、AppleのApple Push Notification service（APNs）証明書を設定および作成する必要があります。 手順については、「APN証明書の要求」を参照してください。

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

XenMobileコンポーネント	**証明書の形式**	**必要な証明書の種類**
NetScaler Gateway	PEM（BASE64） PFX（PKCS#12）	SSL、ルート NetScaler Gatewayによって自動的にPFXがPEMに変換されます。
XenMobile サーバー	PEMまたは PFX（PKCS#12）	SSL、SAML、APNS XenMobileはインストール処理中に完全なPKIも生成します。 XenMobileサーバーでは、拡張子「.pem」の証明書はサポートされません。 opensslコマンドを使用して、PEMファイルからPFXファイルを生成してください。 openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX（PKCS#12）	SSL、ルート

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

NetScaler GatewayおよびXenMobileサーバーの場合は、Verisign、DigiCert、Thawteなどの商用CAからサーバー証明書を取得することをお勧めします。 NetScaler GatewayまたはXenMobile構成ユーティリティから証明書署名要求（Certificate

Signing Request：CSR）を作成できます。 CSRの作成後、CAへ署名のために送信します。 CAから署名入り証明書を受け取ったら、NetScaler GatewayまたはXenMobileに証明書をインストールできます。

認証用のクライアント証明書

XenMobile環境では、クライアント証明書とLDAP認証の組み合わせが、最適なSSO機能とNetScalerでの2要素認証によって提供されるセキュリティが結びついている、セキュリティおよびユーザーエクスペリエンスの最高のソリューションです。 クライアント証明書とLDAPの両方を使用すると、ユーザーの知識（Active Directoryパスワード）と所有物（デバイス上のクライアント証明書）の両方を持つセキュリティが実現されます。 WorxMail（および他のいくつかのWorx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を伴うシームレスな新規ユーザーエクスペリエンスを自動的に構成して提供できます。 ユーザービリティを最適にするために、このオプションをWorx PINやActive Directoryパスワードのキャッシュと組み合わせることができます。

クライアント証明書認証は、仮想サーバーに提示されるクライアント証明書の属性に基づきます。 さらに、NetScaler Gateway上でルート証明書をその仮想サーバーにバインドする必要があります。 NetScaler Gatewayにログオンすると、そのユーザー名の情報が証明書の特定フィールドから抽出されます。 通常、このフィールドはSubject:CNです。 ユーザー名の抽出に成功すると、ユーザーの認証が完了します。 SSL（Secure Sockets Layer）ハンドシェイク時に有効な証明書が提供されなかったりユーザー名の抽出に失敗したりすると、認証に失敗します。

注：

- クライアント証明書による認証は、RADIUSなど、別の種類の認証とともに使用できます。
- クライアント証明書に基づいて認証するには、デフォルトの認証の種類としてクライアント証明書を指定します。 また、「証明書アクション」を作成して、クライアントのSSL証明書に基づいた認証時の動作を定義することもできます。
- WorxMail（および他のいくつかのWorx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を伴うシームレスな新規ユーザーエクスペリエンスを自動的に構成して提供できます。 ユーザービリティを最適にするために、このオプションをWorx PINやActive Directoryパスワードのキャッシュと組み合わせることができます。
- Netscaler Gatewayによるデバイス認証は、随意CAによって取得した証明書に対してはサポートされません。
- XenMobileは、共有デバイスのクライアント証明書認証をサポートしません。

XenMobile PKI

XenMobile PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）の統合機能を使用して、デバイスで使用するセキュリティ証明書の配布とライフサイクルを管理できます。

XenMobileはインストール処理中に、デバイス認証用の内部PKIを作成します。

外部PKIを使用して証明書をデバイスに発行し、構成ポリシーで使用することや、NetScaler Gatewayに対するクライアント認証で使用することもできます。

このPKIシステムの主要機能はPKIエンティティです。 PKIエンティティは、バックエンドコンポーネントをPKI処理用にモデル化します。 このコンポーネントは、Microsoft、RSA、Entrust、Symantex、OpenTrust PKIなどの企業インフラストラクチャの一部です。 PKIエンティティはバックエンドの証明書の発行と失効を処理します。 PKIエンティティは証明書のステータスに関する認証済みの情報源です。 XenMobile構成には、通常1つのバックエンドPKIコンポーネントにつき1つのPKIエンティティのみが含まれます。

PKIシステムの2つ目の機能は資格情報プロバイダーです。 資格情報プロバイダーとは、証明書の発行とライフサイクルの特定の構成を指します。 資格情報プロバイダーは、証明書の形式（サブジェクト、キー、アルゴリズム）および証明書の更新または失効の条件（該当する場合）などを管理します。 資格情報プロバイダーは処理をPKIエンティティに委任します。 つまり、資格情報プロバイダーはPKI処理が実行されるタイミングやそのときに使用するデータを管理しますが、PKIエンティテ

はそれらの処理の実行方法を管理します。 通常、XenMobile構成では、1つのPKIエンティティに多くの資格情報プロバイダーが含まれます。

XenMobileでの証明書の管理

XenMobile環境で使用する証明書の状態について、特に有効期限と関連付けられたパスワードを管理することをお勧めします。 このセクションでは、XenMobileでの証明書管理を簡単に行うための情報を提供します。

お使いの環境には、次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。

XenMobileサーバー
MDM FQDN用のSSL証明書
SAML証明書（ShareFile用）
上記証明書およびその他の内部リソース（StoreFrontやプロキシなど）用のルートCA証明書と中間CA証明書
iOSデバイス管理用のAPN証明書
XenMobileサーバーでのWorx Home通知用の内部APN証明書
PKIへの接続用のPKIユーザー証明書

MDX Toolkit
Apple Developerの証明書
Appleの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のAPN証明書（WorxMailで使用）
Androidのキーストアファイル
Windows Phone – Symantecの証明書

NetScaler
MDM FQDN用のSSL証明書
Gateway FQDN用のSSL証明書
ShareFile SZC（StorageZonesコネクタ）FQDN用のSSL証明書
Exchange負荷分散用のSSL証明書（オフロード構成）
StoreFront負荷分散用のSSL証明書
上記証明書用のルートCA証明書および中間CA証明書

XenMobileの証明書の有効期限ポリシー

証明書の失効を許可した場合、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るため、XenMobileリソースにアクセスできなくなります。

> **注意**
>
> 証明機関（CA：Certification Authority）により、有効期限前にSSL証明書を更新するように求められます。

WorxMail用のAPN証明書

Appleプッシュ通知サービス（APNs：Apple Push Notification service）の証明書は有効期限が1年間であるため、有効期限が切れる前にAPN SSL証明書を新しく作成して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、WorxMailのプッシュ通知に不整合が生じます。 また、アプリに対してプッシュ通知を送信することもできなくなります。

iOSデバイス管理用のAPN証明書

XenMobileでiOSデバイスを登録して管理するには、AppleのAPN証明書を設定および作成する必要があります。 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、管理者はユーザーのiOSデバイスを管理できなくなります。 詳しくは、「APN証明書の要求」を参照してください。

APN証明書の状態と有効期限は、**Apple Push Certificate Portal**にログオンして確認できます。 必ず、証明書を作成したときと同じユーザーで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から次の情報が記載されたメール通知が送信されます。

「AppleID <*CustomersID*>用に作成された次のAppleプッシュ通知サービス証明書が、<*Date*>に失効します。 この証明書を無効にする（失効させる）と、新しいプッシュ証明書を使用した既存デバイスの再登録が必要になります。

担当ベンダーに新しい証明書署名要求（署名入りのCSR）の作成を依頼してから、https://identity.apple.com/pushcertにアクセスしてお使いのAppleプッシュ通知サービス証明書を更新してください。

よろしくお願いします。

Appleプッシュ通知サービス」

MDX Toolkit（iOS配布証明書）

物理iOSデバイス（Apple App Storeのアプリケーション以外）上で実行するアプリケーションはすべて、プロビジョニングプロファイルおよび対応する配布証明書で署名する必要があります。

既存のiOS Developer for Enterprise証明書とプロビジョニングプロファイルは、iOS 9との互換性がない可能性があります。詳しくは、「iOS 9用のWorx Appsのラップ」を参照してください。

iOS配布証明書が有効かどうかを確認するには、次の手順を実行します。

1. Apple Enterprise Developerポータルで、MDX Toolkitを使用してラップするアプリごとに明示的なアプリIDを作成します。適切なアプリIDは、com.CompanyName.ProductNameなどです。
2. Apple Enterprise Developerポータルで［**Provisioning Profiles**］>［**Distribution**］の順に移動し、社内用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アプリIDごとに、この手順を繰り返します。
3. すべてのプロビジョニングプロファイルをダウンロードします。 詳しくは、「iOSモバイルアプリケーションのラップ」を参照してください。

すべてのXenMobileサーバー証明書が有効かどうかを確認するには、次の手順を実行します。

1. XenMobileコンソールで［**Settings**］、［**Certificates**］の順にクリックします。
2. APNs証明書、SSLリスナー証明書、ルート/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

キーストアとは、Androidアプリケーションの署名に使用する証明書が含まれるファイルのことです。キーの有効期限が切れると、ユーザーは新バージョンのアプリへシームレスにアップグレードすることができなくなります。

Symantec提供のWindows Phone用エンタープライズ証明書

Symantecは、Microsoft App Hubサービス用のコード署名証明書の独占プロバイダーです。 開発者とソフトウェアパブリッシャーがWindows Marketplaceでのダウンロード向けにWindows PhoneアプリケーションおよびXbox 360アプリケーションを配布するには、App Hubに参加する必要があります。 詳しくは、Symantecのドキュメントの「Symantec Code Signing

Certificates for Windows Phone」を参照してください。

証明書の有効期限が切れると、Windows Phoneユーザーは、会社により公開および署名されているアプリの登録とインストール、Windows Phoneにインストール済みの業務用アプリの起動ができなくなります。

NetScaler

NetScaler証明書の失効の対処方法について詳しくは、Citrix Support Knowledge Centerの「NetScalerでの証明書失効の対処方法」を参照してください。

NetScaler証明書の有効期限が切れると、ユーザーは失効した証明書に応じて、Worx Storeへの登録とアクセス、WorxMail使用時のExchange Serverへの接続、HDXアプリケーションの列挙と起動ができなくなります。

Expiry MonitorとCommand Centerを使用すると、NetScaler証明書の状況を把握でき、証明書が失効した時に通知を受け取ることもできます。 これら2つのツールでは、次のNetScaler証明書を監視できます。

MDM FQDN用のSSL証明書
Gateway FQDN用のSSL証明書
ShareFile SZC（StorageZonesコネクタ）FQDN用のSSL証明書
Exchange負荷分散用のSSL証明書（オフロード構成）
StoreFront負荷分散用のSSL証明書
上記証明書用のルートCA証明書および中間CA証明書

XenMobileでの証明書のアップロード

Oct 25, 2016

証明書はXenMobileサーバーで機能上使用されます。 XenMobileへの証明書のアップロードは、XenMobileコンソールの［**Certificates**］領域で行います。 これらの証明書には、CA（Certificate Authority：証明機関）証明書、RA（Registration Authority：登録機関）証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。 また、デバイスに展開する証明書のストレージの場所として［Certificates］領域を使用することができます。 これは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。

アップロードする各証明書は、［Certificates］の表で1つのエンティティとして表され、その内容がまとめられています。 証明書が必要なPKI統合コンポーネントを構成するときに、サーバー証明書の一覧からコンテキスト依存の条件を満たすサーバー証明書を選択するよう求めるメッセージが表示されます。 たとえば、XenMobileをMicrosoft CAと統合するように構成する場合があります。 Microsoft CAへの接続はクライアント証明書を使用して認証されます。

このセクションでは、証明書をアップロードする一般的な手順について説明します。 クライアント証明書の作成、アップロード、構成について詳しくは、「クライアント証明書認証の構成」を参照してください。

秘密キーの要件

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

コンソールへの証明書のアップロード

CAが要求に署名するために使用するCA証明書（秘密キーなし）とクライアント認証用のSSLクライアント証明書（秘密キーあり）をアップロードできます。 Microsoft CAエンティティを構成する場合は、CA証明書を指定する必要があります。CA証明書であるすべてのサーバー証明書の一覧から選択できます。 同様に、クライアント認証を構成する場合は、XenMobileが秘密キーを持っているすべてのサーバー証明書の一覧から選択できます。

XenMobileは、証明書の以下の入力形式をサポートします。

- PEMまたはDERでエンコードされた証明書ファイル
- PEMまたはDERでエンコードされた秘密キーファイルが関連付けられたPEMまたはDERでエンコードされた証明書ファイル
- PKCS#12キーストア（P12。WindowsのPFXとも呼ばれます）

重要： XenMobileサーバーでは拡張子「.pem」の証明書はサポートされません。 openssl コマンドを使用して、PEMファイルからPFXファイルを生成してください。

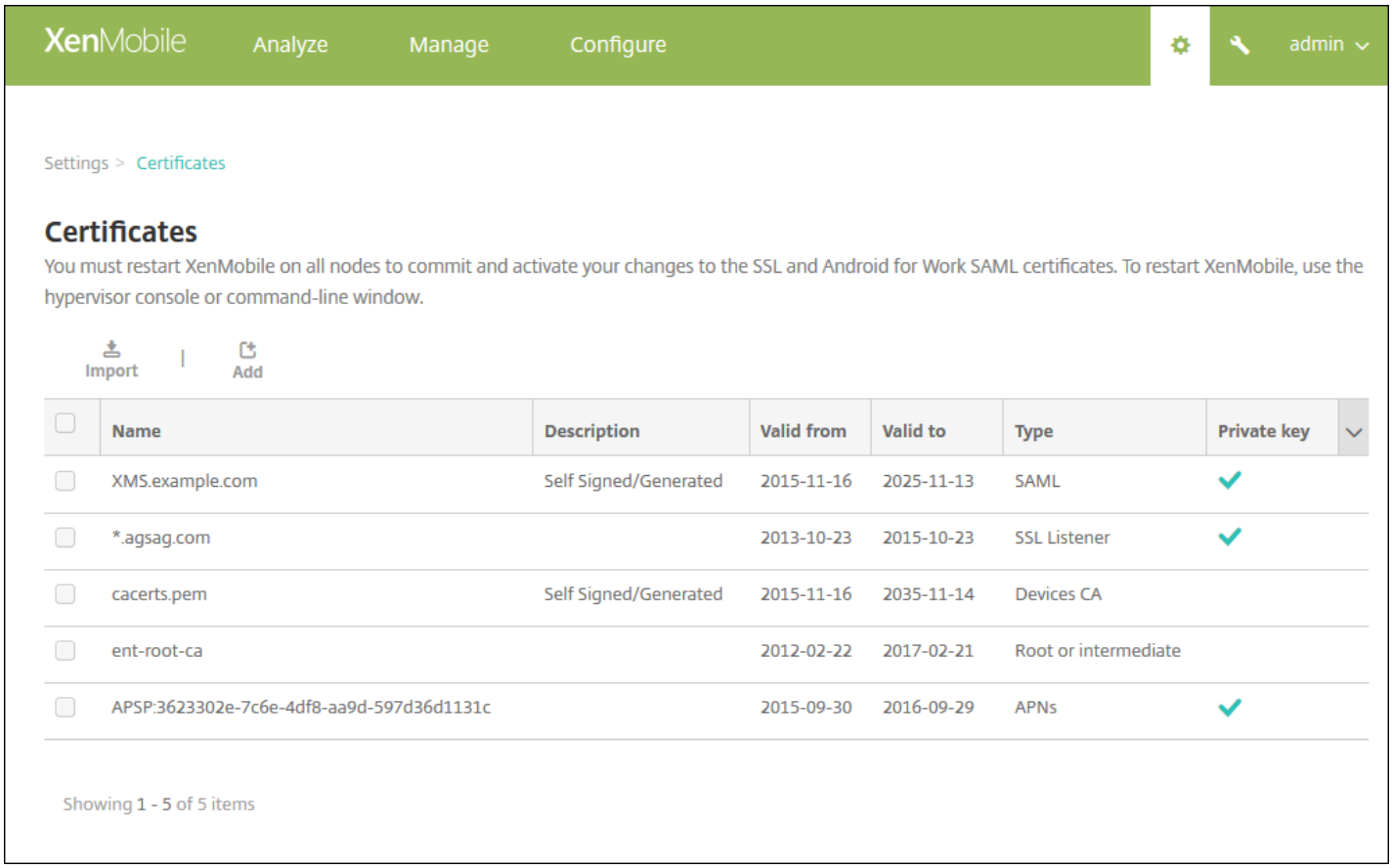
```
openssl pkcs12 -export -out certificate.pfx  -in certificate.pem
```

キーストアをインポートするには

設計上、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。 このため、キーストアから読み込むときに、読み込むエントリを識別するエントリエイリアスの指定を求めるメッセージが表示されます。 エイリアスを指定しない場合、ストアの最初のエントリが読み込まれます。 PKCS#12ファイルに含まれるエントリは通常1つだけであるため、キーストアの種類としてPKCS#12を選択した場合、エイリアスフィールドは表示されません。

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

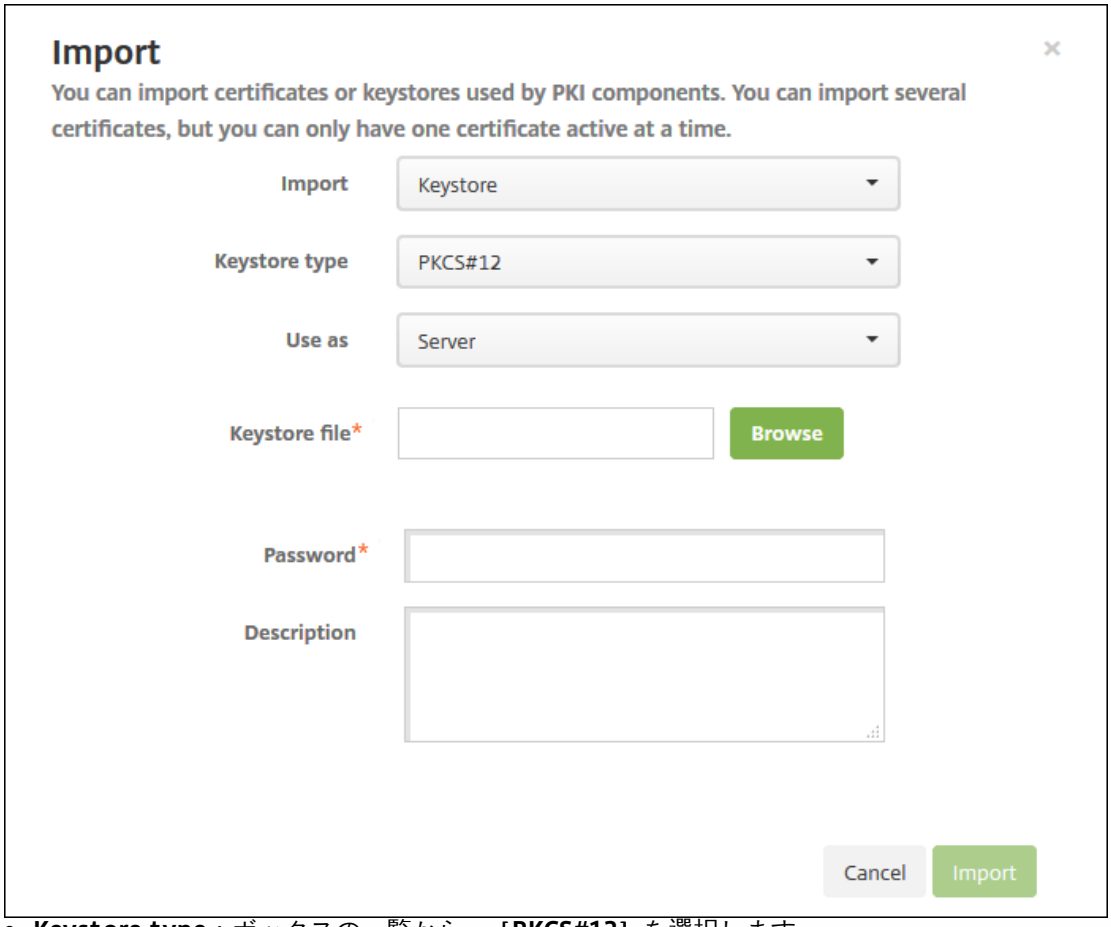
2. **［Certificates］**をクリックします。 **［Certificates］**ページが開きます。



3. **[Import]** をクリックします。 **[Import]** ダイアログボックスが開きます。

4. 次の設定を構成します。

- **Import**：ボックスの一覧から、**[Keystore]** を選択します。 **[Import]** ダイアログボックスが、使用可能なキーストアオプションを反映した表示に変わります。



- **Keystore type**：ボックスの一覧から、［**PKCS#12**］を選択します。
- **Use as**：ボックスの一覧から、キーストアの使用方法を選択します。 以下の種類から選択できます。
  - **Server**。 サーバー証明書はXenMobileサーバーで機能上使用される証明書で、XenMobile Webコンソールにアップロードされます。 サーバー証明書には、CA証明書、RA証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。 また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。 これは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。
  - **SAML**。 Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Webサイト、およびアプリケーションへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
  - **APNs**。 AppleのApple Push Notificationサービス（APNs）証明書を使用すると、Apple Push Networkを使用してモバイルデバイスを管理できます。
  - **SSL Listener**。 SSL（Secure Sockets Layer）リスナーは、XenMobileにSSL暗号化アクティビティを通知します。
- **Keystore file**：［**Browse**］をクリックしてインポートするキーストアファイルの場所に移動し、そのファイルを選択します。
- **Password**：証明書に割り当てられたパスワードを入力します。
- **Description**：任意で、キーストアの説明を入力します。この説明は、ほかのキーストアと区別するときに役立ちます。

5. ［**Import**］をクリックします。 キーストアが［**Certificates**］の表に追加されます。

証明書をインポートするには

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

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

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、**[Certificates]** をクリックします。

2. **[Certificates]** ページで、 **[Import]** をクリックします。 **[Import]** ダイアログボックスが開きます。

3. **[Import]** ダイアログボックスの **[Import]** の一覧から、まだ選択していない場合は **[Certificate]** を選択します。

4. **[Import]** ダイアログボックスが、使用可能な証明書オプションを反映した表示に変わります。 **[Use as]** の一覧から、キーストアの使用方法を選択します。 以下の種類から選択できます。

- **Server**。 サーバー証明書はXenMobileサーバーで機能上使用される証明書で、XenMobile Webコンソールにアップロードされます。 サーバー証明書には、CA証明書、RA証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。 また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。 このオプションは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。
- **SAML**。 Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Webサイト、およびアプリケーションへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
- **SSL Listener**。 SSL（Secure Sockets Layer）リスナーは、XenMobileにSSL暗号化アクティビティを通知します。

5. インポートする証明書を参照して指定します。

6. 任意で、証明書の秘密キーファイルを参照して指定します。 秘密キーは、証明書と組み合わせて暗号化と復号化で使用されます。

7. 任意で、証明書の説明を入力します。この説明は、ほかの証明書と区別するときに役立ちます。

8. **[Import]** をクリックします。証明書が［Certificates］の表に追加されます。

証明書の更新

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

証明書を最も効果的に更新するには、XenMobileコンソールで右上の歯車アイコンをクリックして［Settings］ページを開き、［Certificates］をクリックします。 ［Import］ダイアログボックスで、新しい証明書をインポートします。 サーバー証明書を更新すると、以前の証明書を使用していたコンポーネントが新しい証明書を使用するように自動的に切り替わります。 同様に、デバイスにサーバー証明書を展開している場合、証明書は次回展開するときに自動的に更新されます。

クライアント証明書認証の構成

Aug 02, 2016

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サーバーを構成してから、NetScaler Gatewayを構成する必要があります。 この記事では、次の一般的な手順を詳しく説明します。

Microsoftサーバーの場合

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

XenMobileサーバーの場合

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

NetScaler Gateway：

1. XenMobile MAMモードの証明書認証用にNetScaler Gatewayを構成します。

前提条件

- クライアント証明書認証およびSSL Offloadを使用するWindows Phone 8.1デバイスの場合、NetScaler内の両方の負荷分散仮想サーバー上のポート443に対するSSLセッション再利用を無効にする必要があります。 そうするには、vserver上でポート443に対して次のコマンドを実行します。

  ```
  set ssl vserver sessReuse DISABLE
  ```

  注：SSLセッション再利用を無効にすると、NetScalerで提供される最適化の一部が無効になり、NetScaler上のパフォーマンスが低下することがあります。

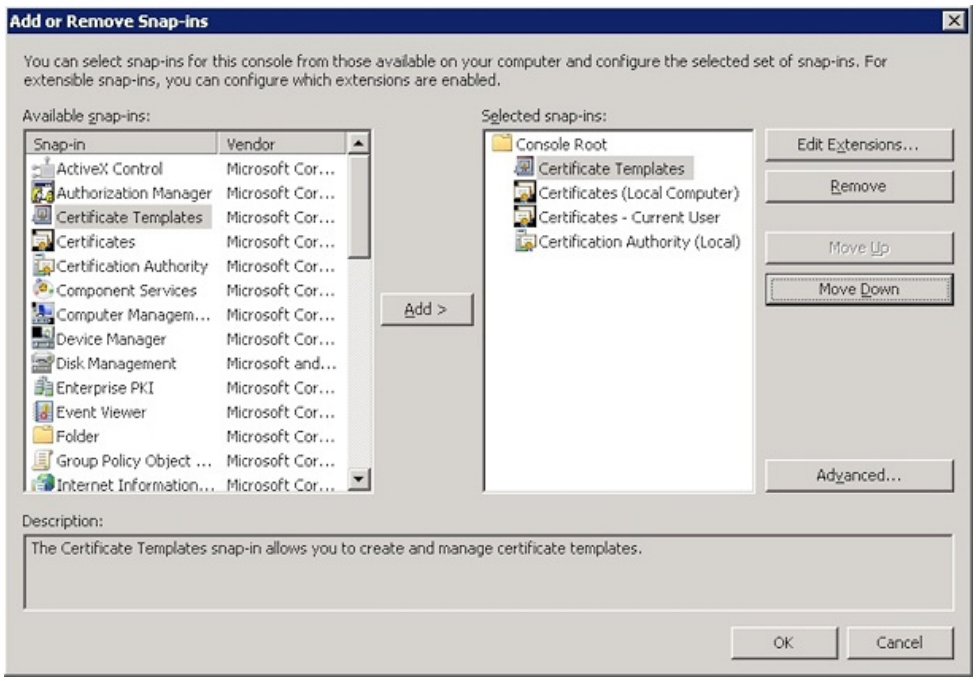
- Exchange ActiveSyncに対して証明書ベースの認証を構成するには、このMicrosoftのブログを参照してください。
- プライベートサーバー証明書を使用してExchange ServerへのActiveSyncトラフィックを保護する場合は、モバイルデバイスがすべてのルート証明書および中間証明書を持っていることを確認してください。 そうしない場合、WorxMailでのメールボックス設定時に、証明書ベースの認証が失敗します。 Exchange IIS Consoleコンソールでは、次のことが必要です。
  - XenMobileをExchangeと使用するためのWebサイトを追加し、Webサーバー証明書をバインドします。
  - ポート9443を使用します。
  - そのWebサイトに対して、Microsoft-Server-ActiveSync用とEWS用に、2つのアプリケーションを追加する必要があります。 それらの両方のアプリケーションに対して、 **[SSL Settings]** で **[Require SSL]** を選択します。
- 最新のMDX Toolkitを使用してiOS、AndroidおよびWindows Phone用のWorxMailがラップされていることを確認します。

証明書のスナップインのMicrosoft管理コンソールへの追加

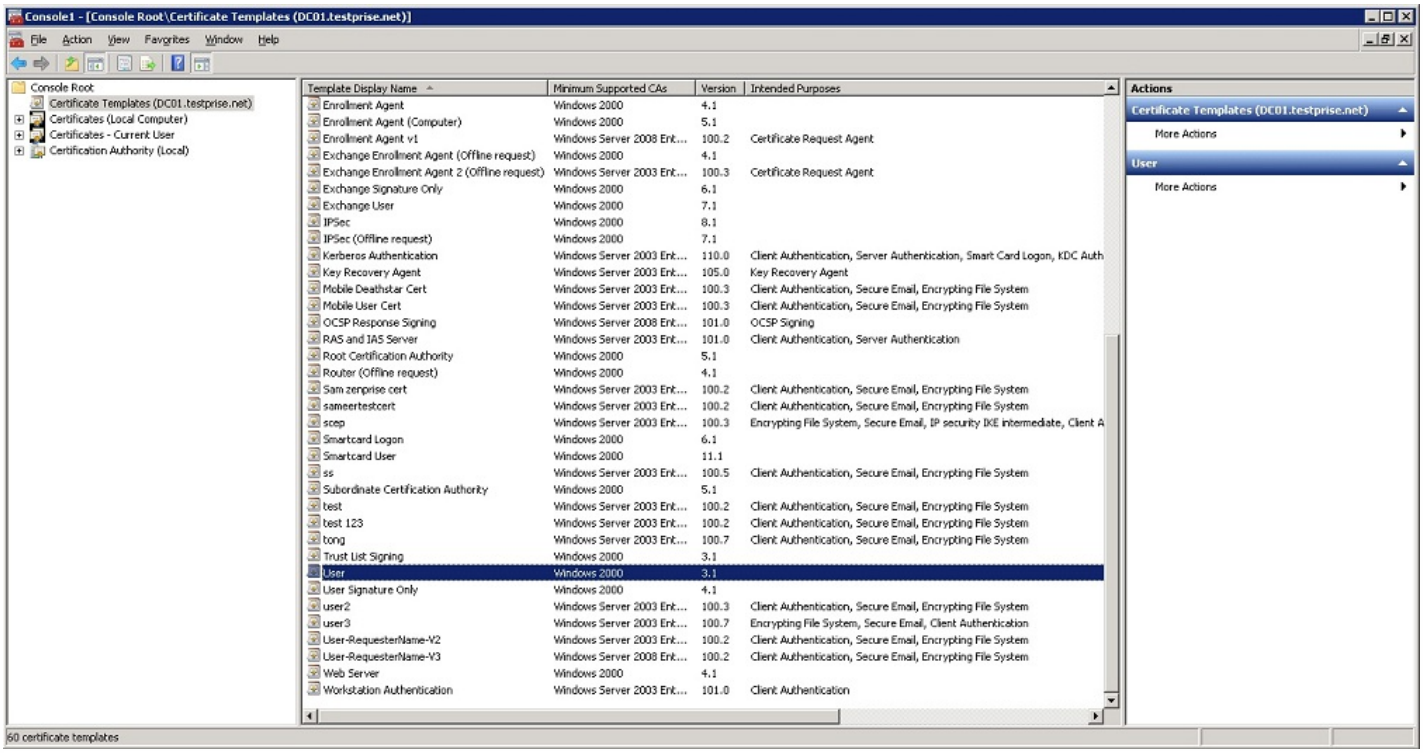
1. コンソールを開いて、**[スナップインの追加と削除]** をクリックします。

2. 次のスナップインを追加します。

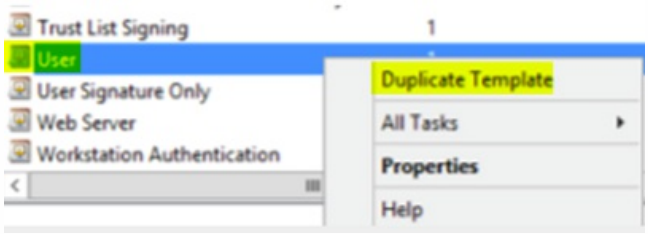
証明書テンプレート
証明書（ローカルコンピューター）
証明書 - 現在のユーザー
証明機関（CA）（ローカル）



3. **[証明書テンプレート]** を展開します。



4. **[User]** テンプレートと **[Duplicate Template]** を選択します。

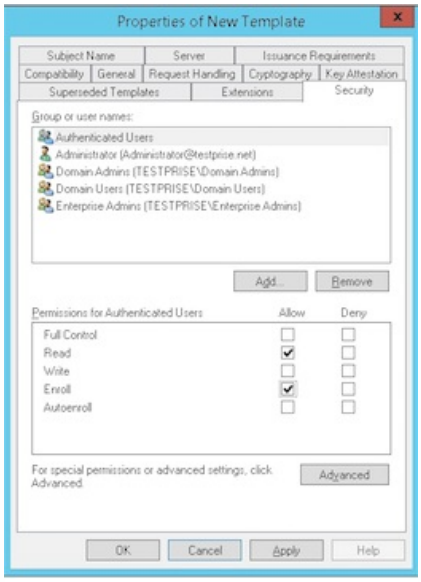


5. ［テンプレート］の表示名を入力します。

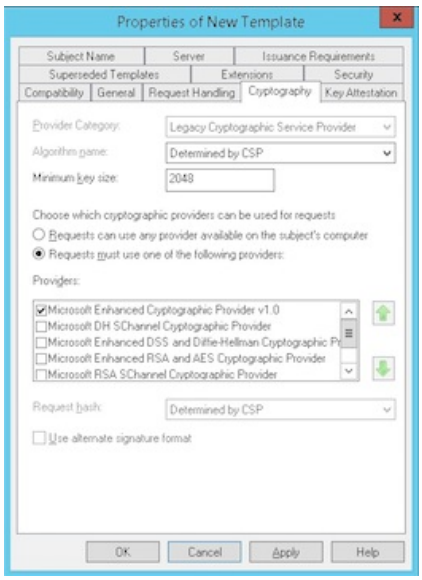
   重要：必要な場合以外は、 **[Active Directoryの証明書を発行する]** チェックボックスを選択しないでください。 このオプションが選択されると、すべてのユーザークライアント証明書がActive Directoryで発行/作成され、Active Directoryデータベースを圧迫する可能性があります。

6. テンプレートの種類には **[Windows 2003 Server]** を選択します。Windows 2012 R2の **[互換性]** で、 **[Certificate Authority]** を選択して **[Windows 2003]** を宛先として設定します。

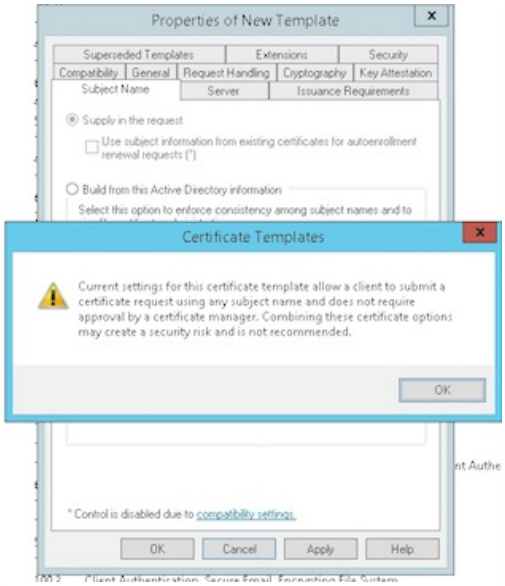
7. **[セキュリティ]** で、認証ユーザーの **[許可]** 列の **[登録]** オプションを選択します。



8. **[Cryptography]** で、XenMobileの構成中に入力する必要のあるキーサイズが入力されていることを確認します。



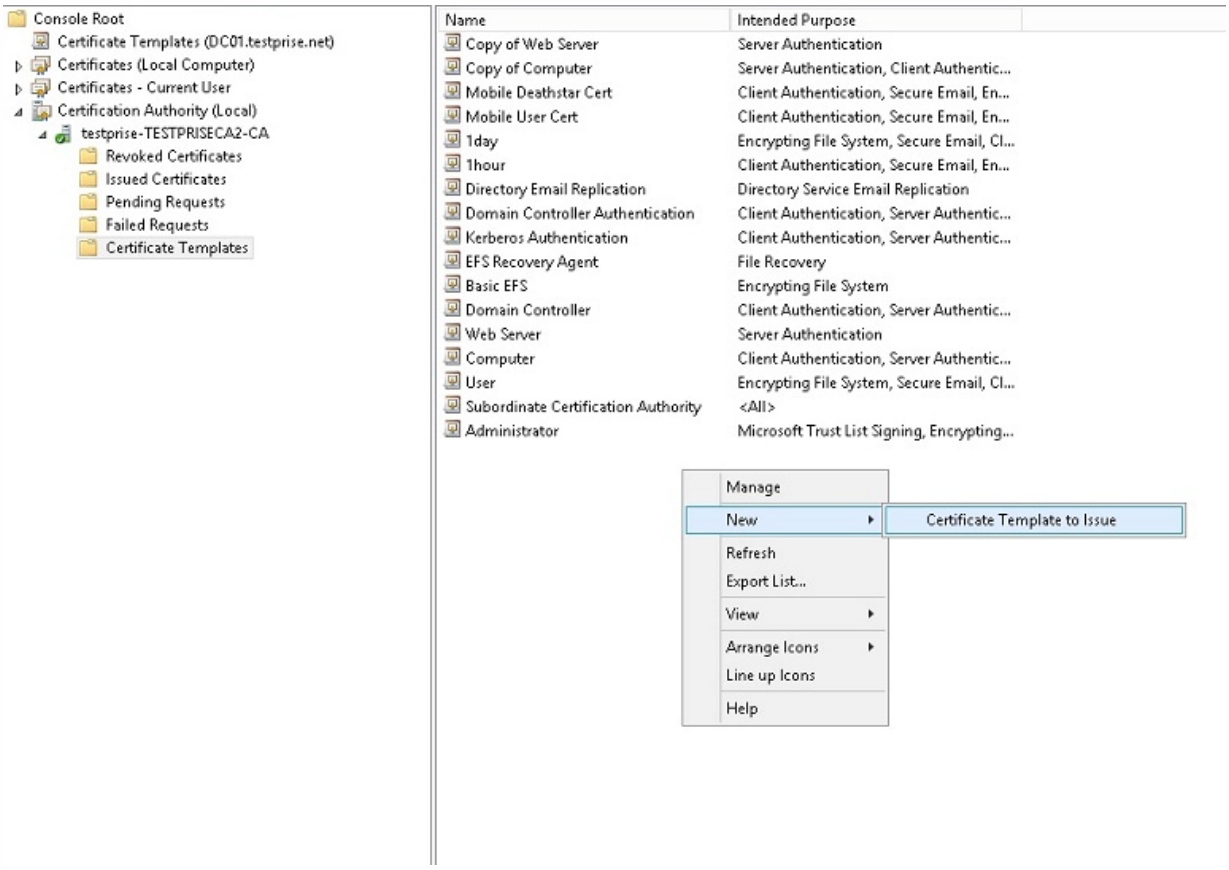
9. **[サブジェクト名]** で、 **[要求に含まれる]** を選択します。 変更を適用して、保存します。



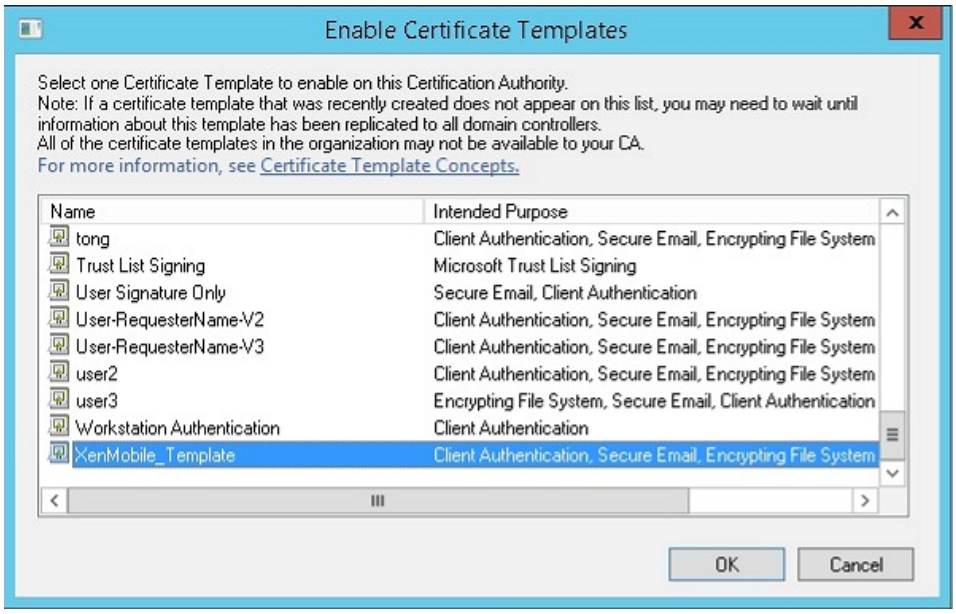
証明機関（CA）へのテンプレートの追加

1. **[Certificate Authority]** に移動して、 **[証明書テンプレート]** を選択します。

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



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

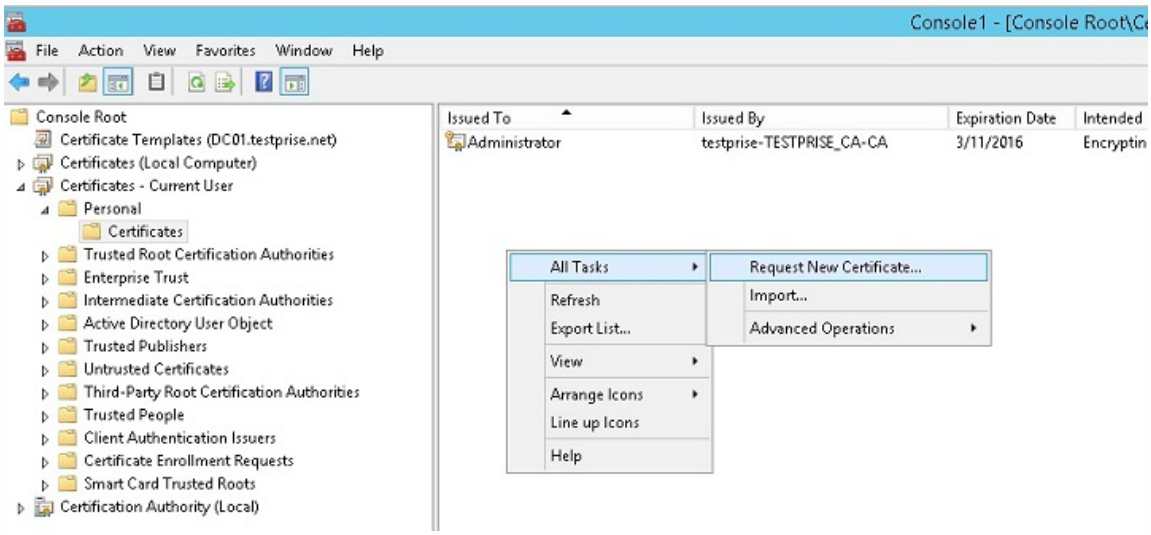


CAサーバーからのPFX証明書の作成

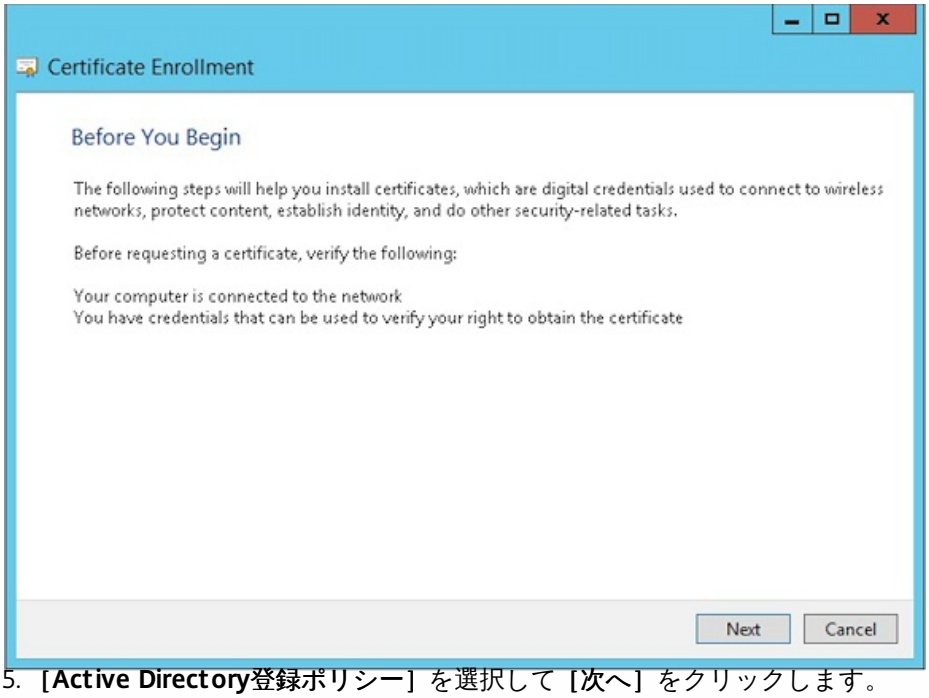
1. ログインしたサービスアカウントで、ユーザー.pfx certを作成します。 この.pfxファイルはXenMobileにアップロードされ、デバイスを登録するユーザーのためにユーザー証明書を要求します。

2. **[現在のユーザー]**で、 **[証明書]**を展開します。

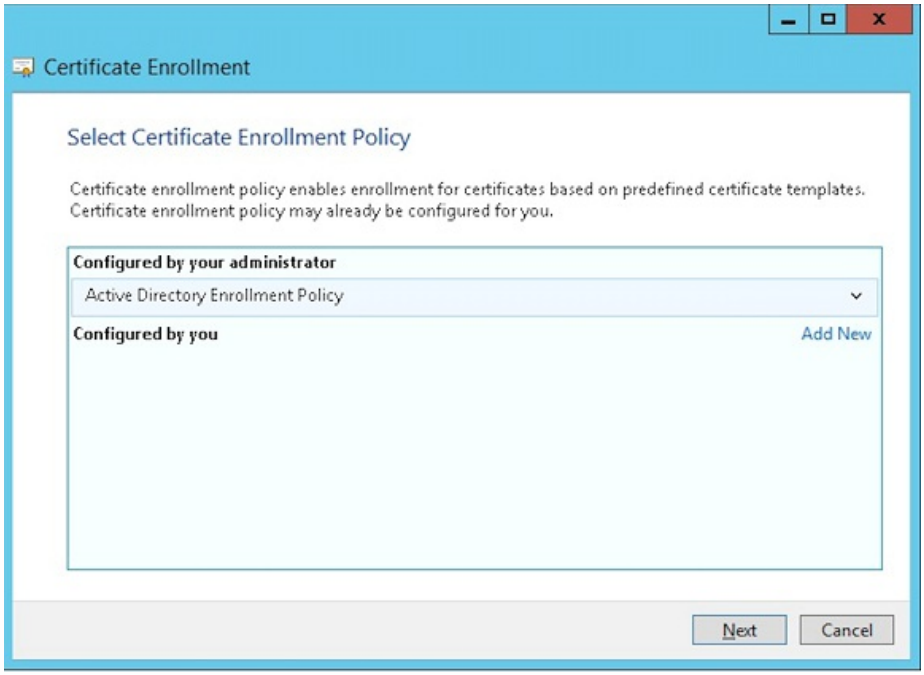
3. 右ペインで右クリックし、 **[Request New Certificate]**をクリックします。



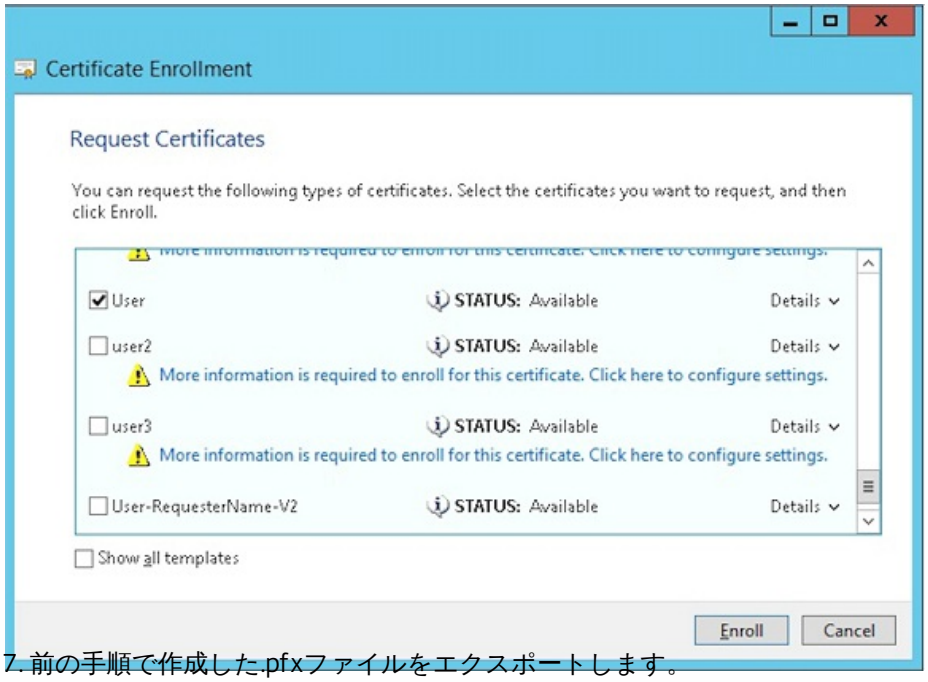
4. **[Certificate Enrollment]**画面が表示されます。 **[次へ]**をクリックします。



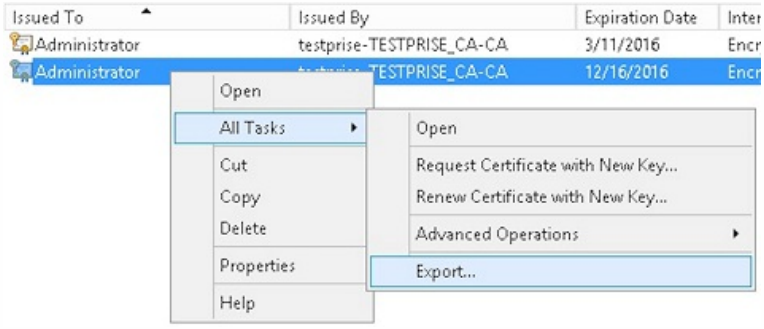
5. **[Active Directory登録ポリシー]** を選択して **[次へ]** をクリックします。



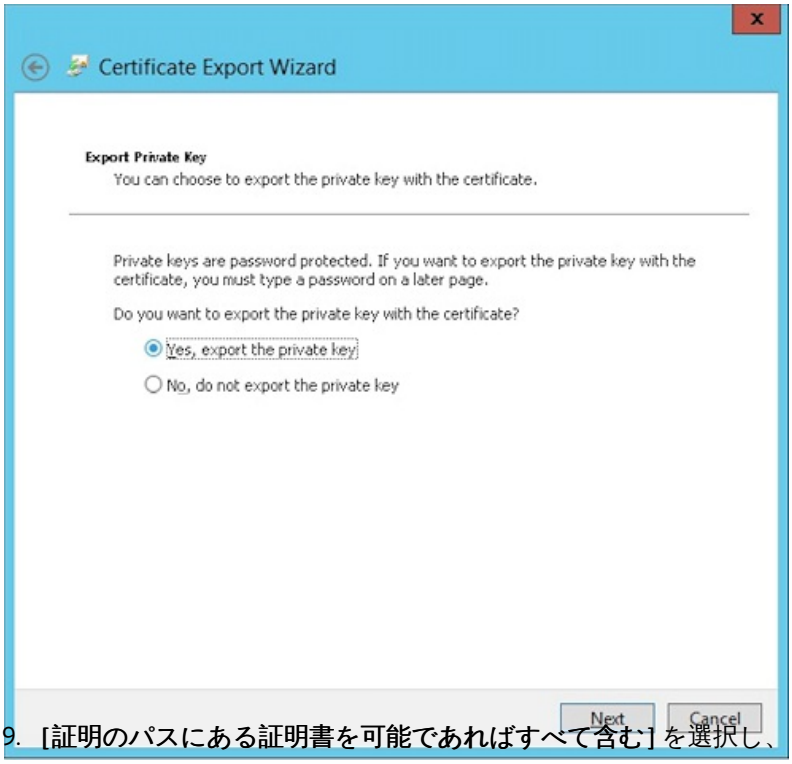
6. **[ユーザー]** テンプレートを選択し、 **[登録]** をクリックします。



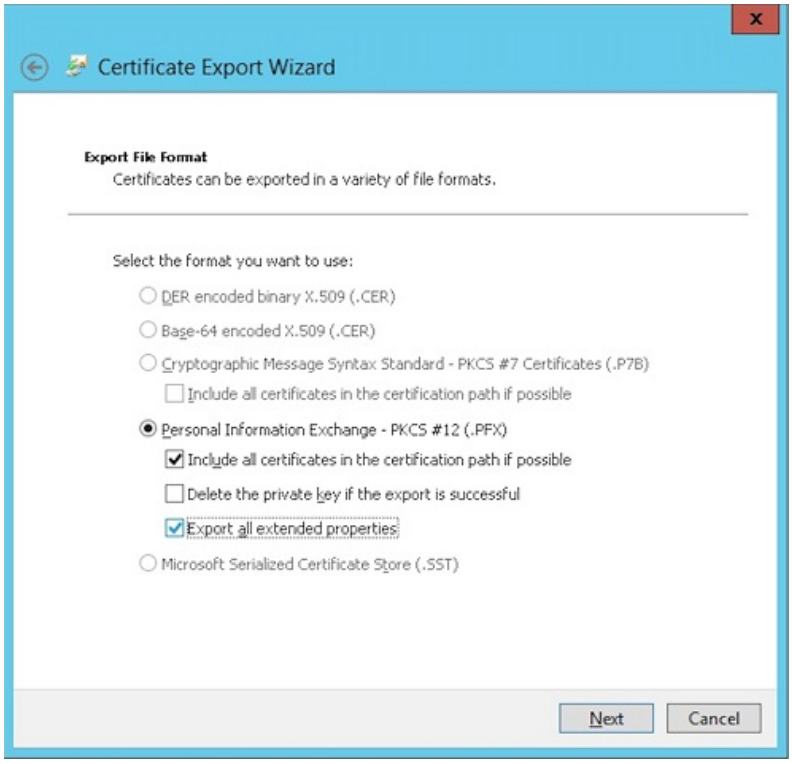
7. 前の手順で作成した.pfxファイルをエクスポートします。



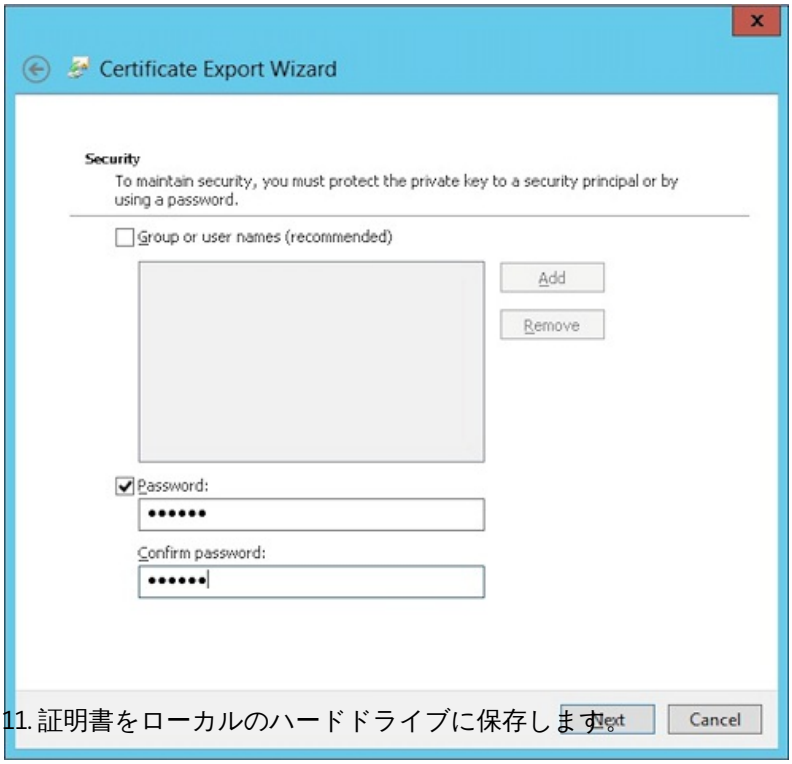
8. **[はい、秘密キーをエクスポートします]** をクリックします。



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



10. XenMobileに証明書をアップロードする際に使用するパスワードを設定します。



11. 証明書をローカルのハードドライブに保存します。

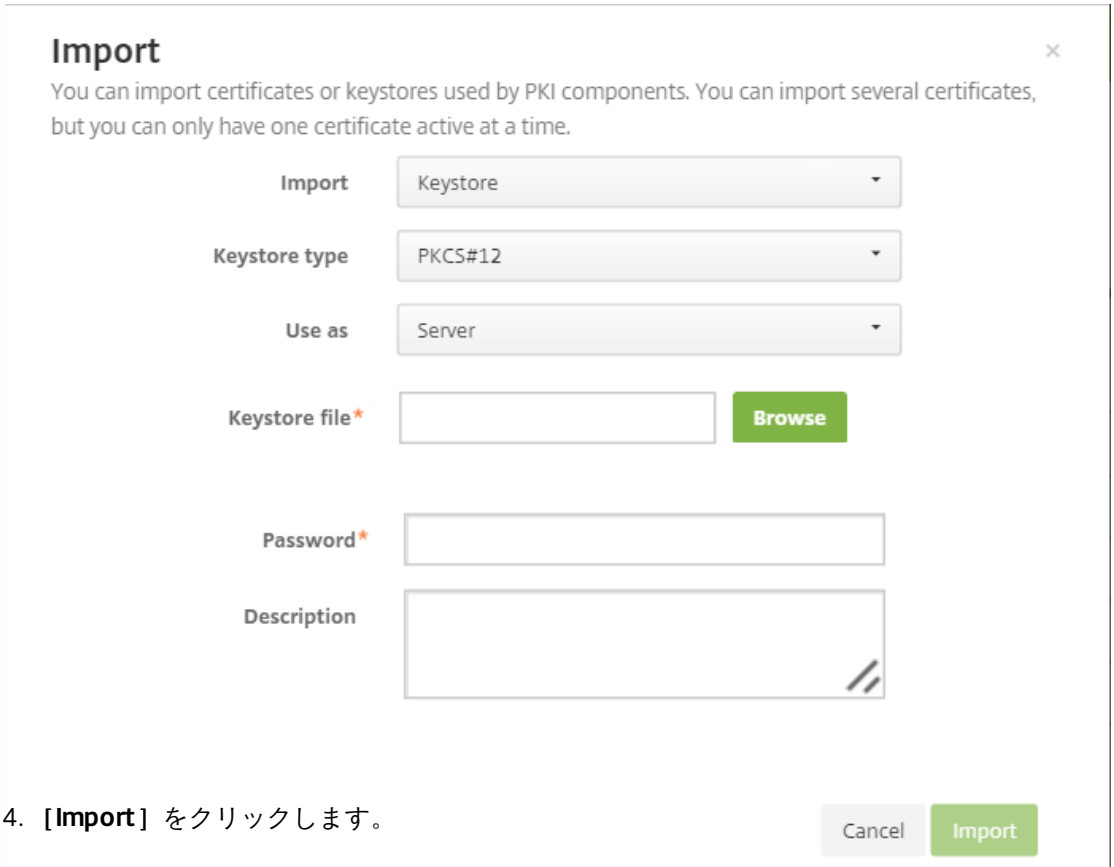
XenMobileへの証明書のアップロード

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[設定]** 画面が表示されます。

2. **[証明書]** をクリックしてから、 **[インポート]** をクリックします。

3. 以下のパラメーターを入力します。

- **インポート**：Keystore
- **キーストアの種類**：PKCS#12
- **使用目的**：Server
- **Key File Name**： ［参照］をクリックして、前の手順で作成した.pfx 証明書を選択します。
- **パスワード**：証明書と一緒に作成したパスワードを入力します。



4. **[Import]** をクリックします。

5. 証明書が正常にインストールされているか確認します。 ユーザー証明書として表示されているはずです。

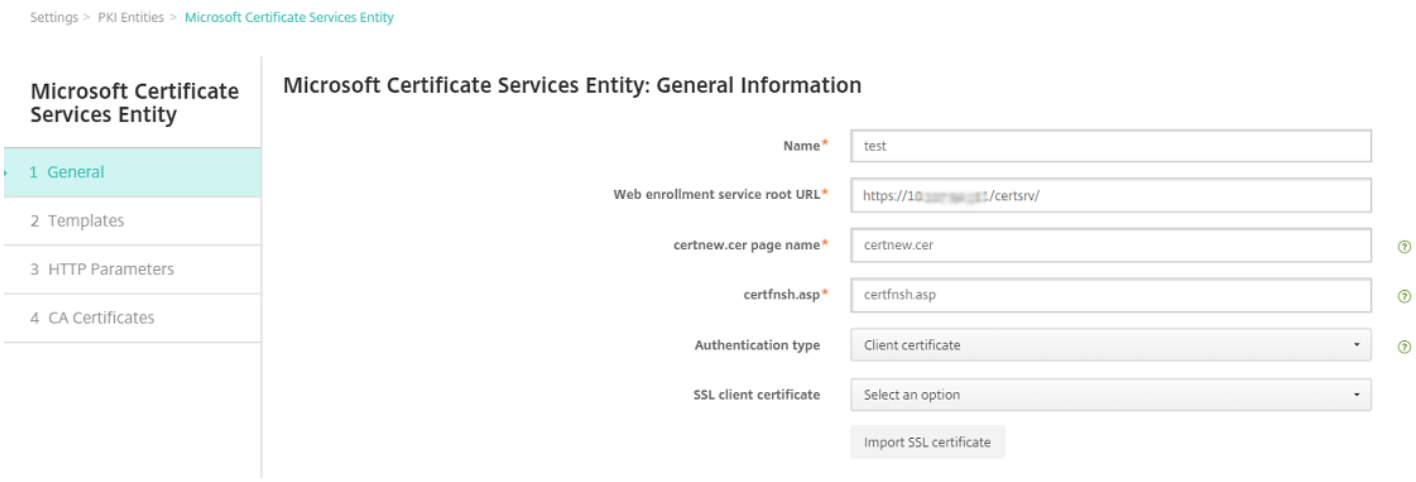
証明書に基づいた認証のためのPKIエンティティの作成

1. **[設定]** で、 **[詳細]** 、 **[証明書管理]** 、 **[PKIエンティティ]** の順に移動します。

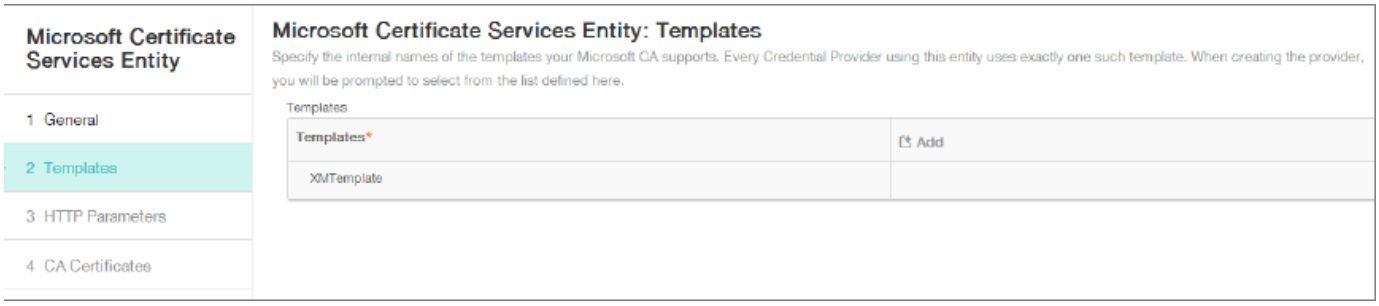
2. **[追加]** をクリックしてから、 **[Microsoft 証明書サービス エンティティ]** をクリックします。 **[Microsoft 証明書サービス エンティティ: 一般的な情報]** 画面が表示されます。

3. 以下のパラメーターを入力します。

- **名前**：任意の名前を入力します
- **Web 登録サービス ルート URL**：https://RootCA-URL/certsrv/
  URLパスの末尾が「/」で終わっていることを確認してください。
- **certnew.cer ページ名**：certnew.cer（デフォルト値）
- **certfnsh.asp**：certfnsh.asp（デフォルト値）
- **Authentication type**：クライアント証明書。
- **SSLクライアント証明書**：XenMobileクライアント証明書を発行するために使用するユーザー証明書を選択します。

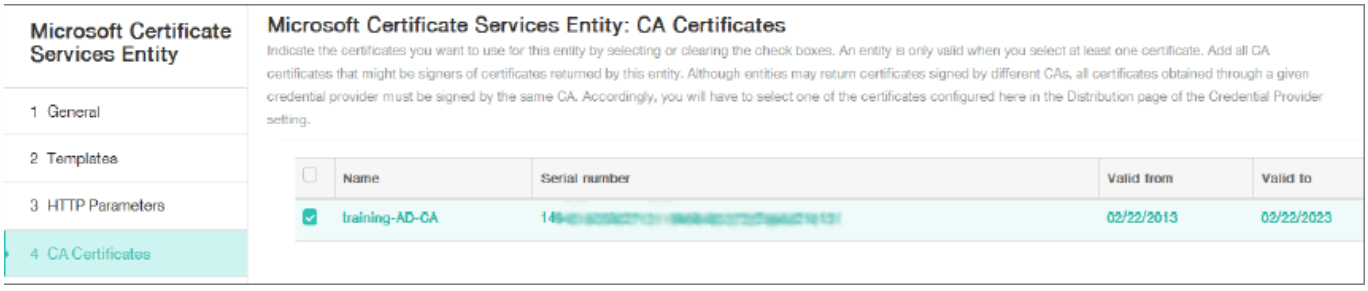


4. **[テンプレート]** で、Microsoft証明書を構成したときに作成したテンプレートを追加します。 空白を入れないように注意してください。



5. HTTPパラメーターをスキップし、 **[CA 証明書]** をクリックします。

6. 環境内で関連するルートCA証明書の名前を選択します。 このルートCA証明書は、XenMobileクライアント証明書からインポートされたチェーンの一部です。



7. **[Save]** をクリックします。

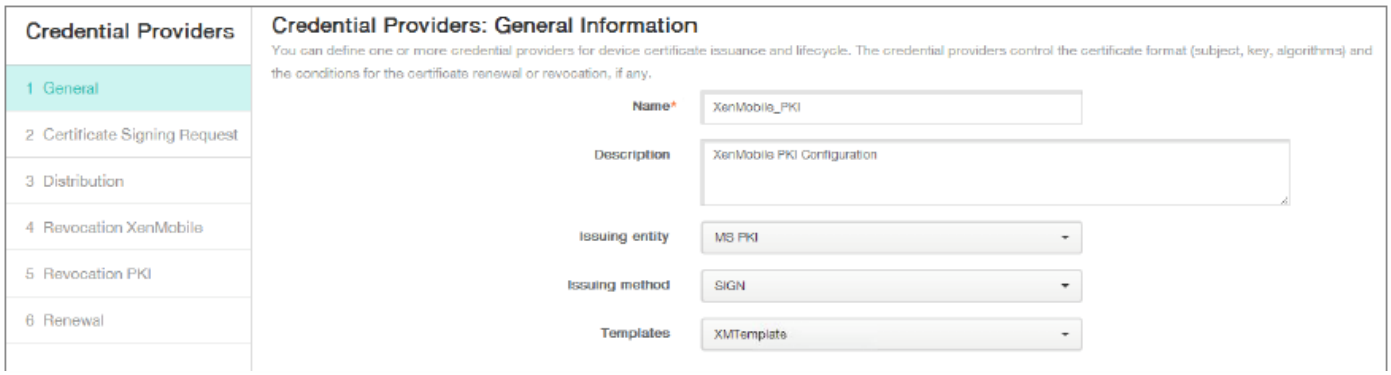
資格情報プロバイダーの構成

1. **[設定]** で、 **[詳細]** 、 **[証明書管理]** 、 **[資格情報プロバイダー]** の順に移動します。

2. **[Add]** をクリックします。

3. **[全般]** で、次のパラメーターを入力します。

- **名前**：任意の名前を入力します。
- **アカウントの説明**：任意の説明を入力します。
- **発行エンティティ**：前に作成したPKIエンティティを選択します。
- **発行方式**：SIGN
- **テンプレート**：PKIエンティティに追加されたテンプレートを選択します。



4. **[証明書署名要求]** をクリックしてから、次のパラメーターを入力します。

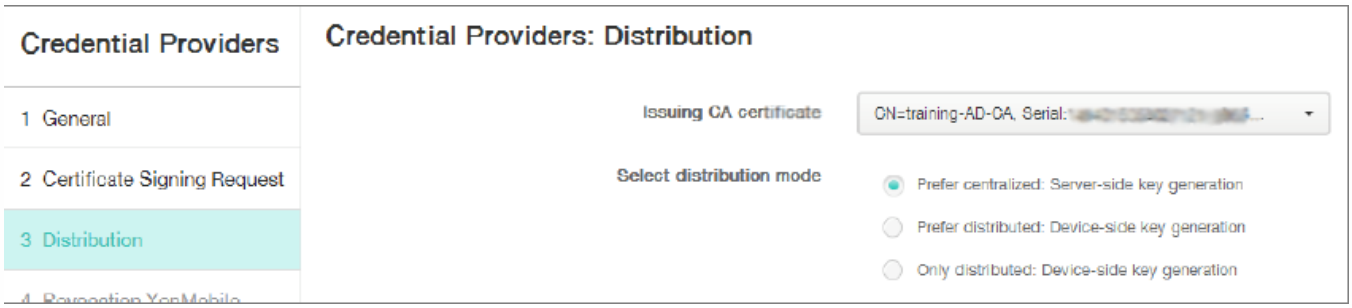
- **キー アルゴリズム**：RSA
- **キー サイズ**：2048
- **署名アルゴリズム**：SHA1withRSA
- **サブジェクト名**：cn=$user.username

[サブジェクトの別名] の **[追加]** をクリックしてから、次のパラメーターを入力します。

- **種類**：ユーザープリンシパル名
- **値**：$user.userprincipalname

5. **[ディストリビューション]** をクリックし、次のパラメーターを入力します。

- **発行 CA 証明書**：署名済みのXenMobileクライアント証明書の発行CAを選択します。
- **ディストリビューション モードの選択**： **[優先集中: サーバー側のキー生成]** を選択します。

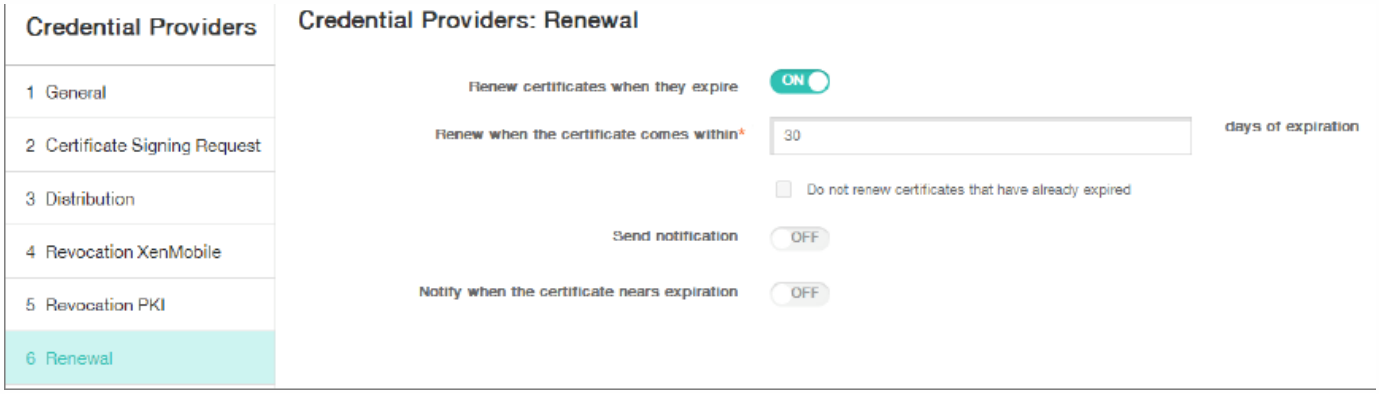


6. 次の2つのセクション（**Revocation XenMobile**と**Revocation PKI**）で必要なパラメーターを設定します。 この記事では、このオプションをスキップします。

7. **[更新]**をクリックします。

8. **[有効期限が切れたら証明書を更新]**で**[オン]**を選択します。

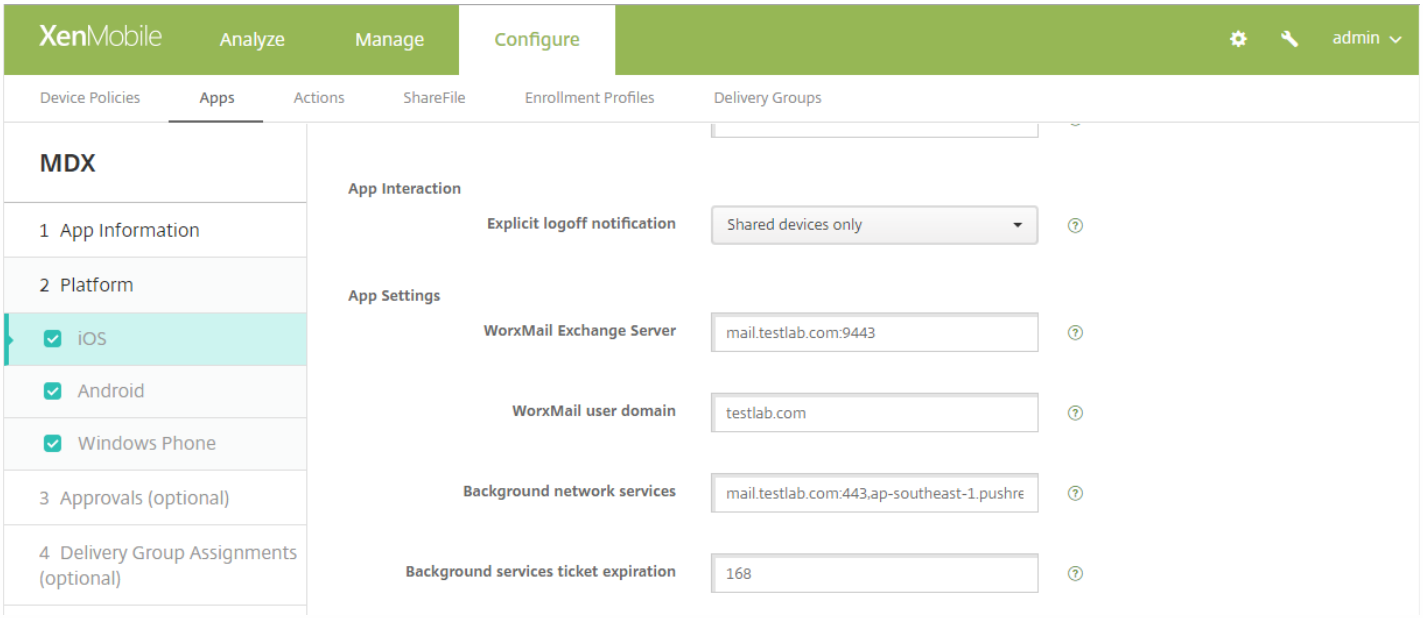
9. そのほかの設定はすべてそのままにするか、必要な変更を加えます。



10. **[Save]**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WorxMailを構成する

XenMobileにWorxMailを追加する場合、必ず**[App Settings]**の下でExchange設定を構成します。



XenMobileでのNetScaler証明書の配信の構成

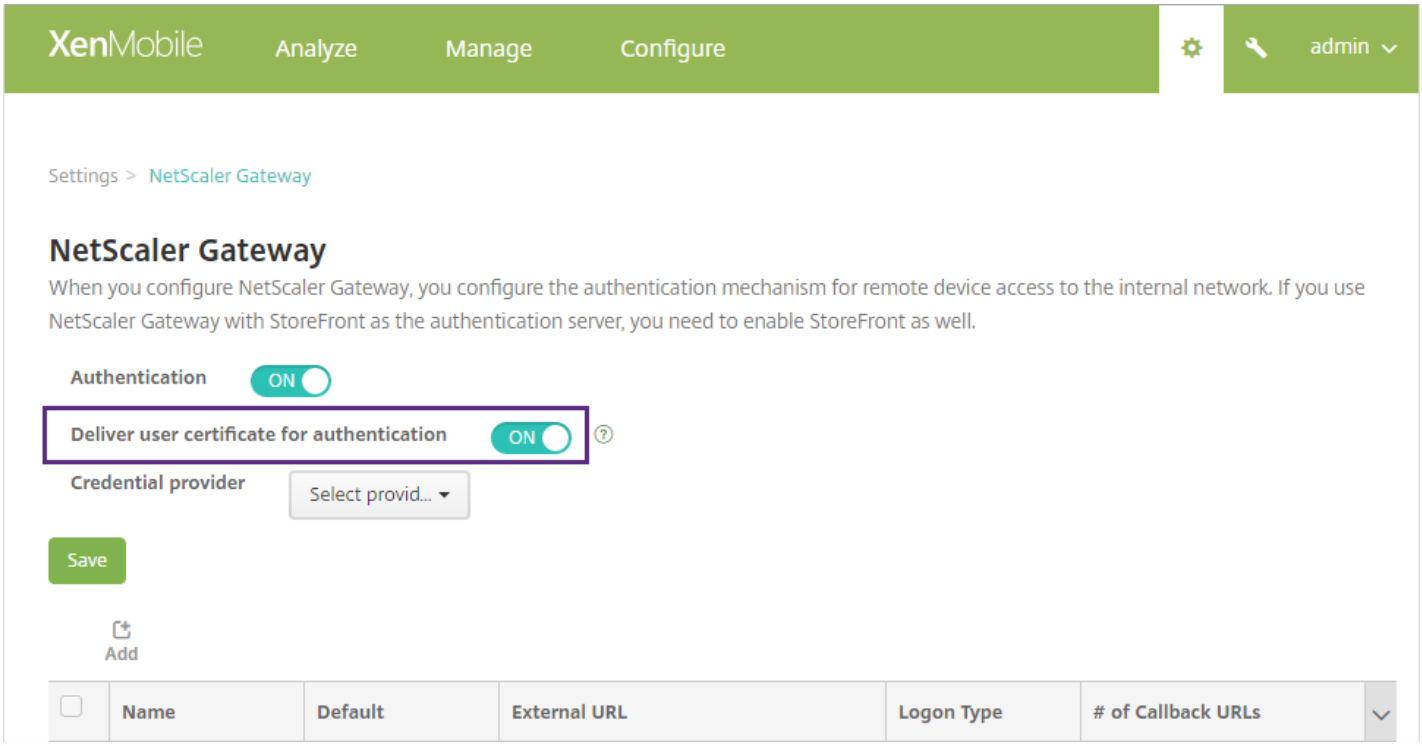
1. XenMobileコンソールにログオンして、右上の歯車アイコンをクリックします。**[設定]**画面が表示されます。

2. **[Server]**の下の**[NetScaler Gateway]**をクリックします。

3. NetScaler Gatewayがまだ追加されていない場合、**[Add]**をクリックして、次のように設定を指定します。

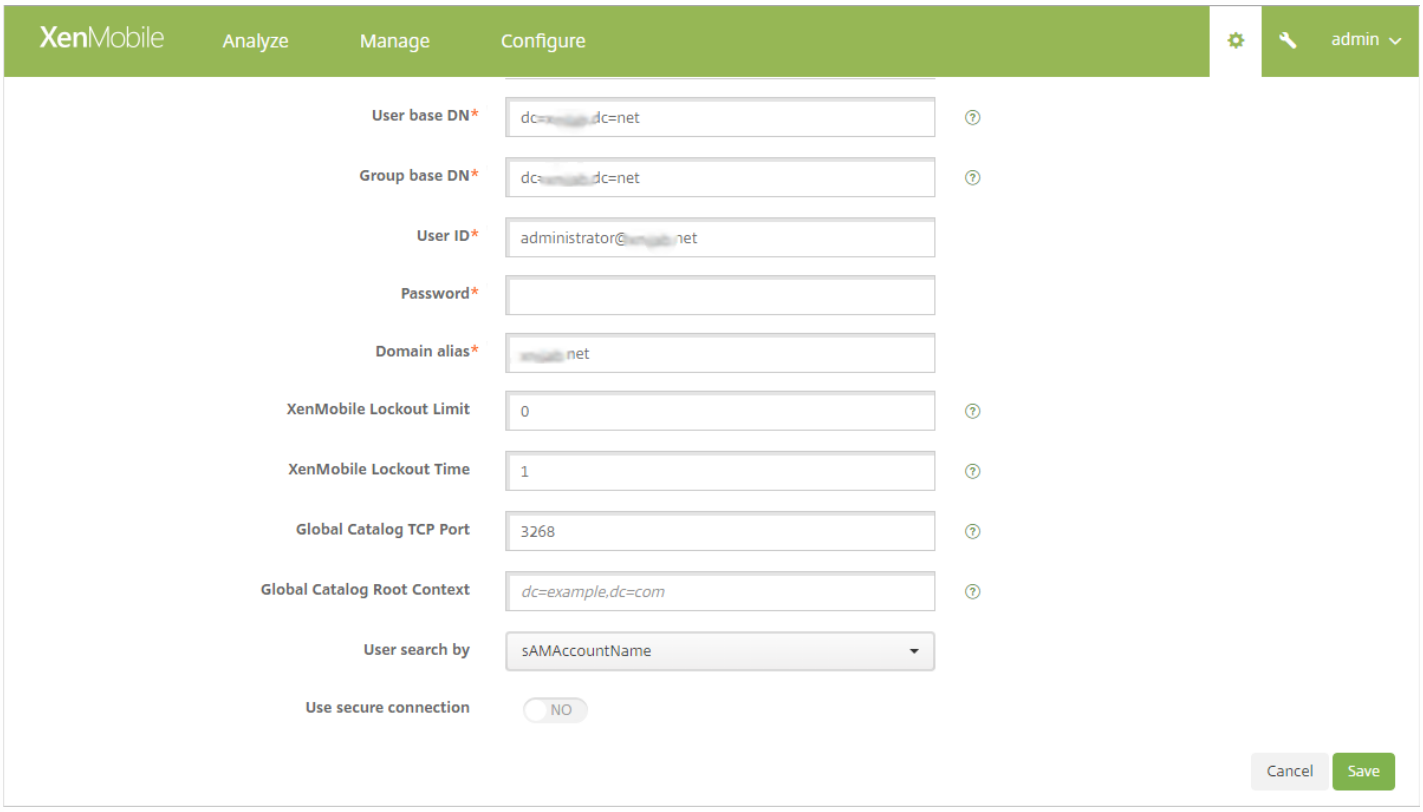
- **External URL**：https://YourNetScalerGatewayURL
- **Logon Type**：Certificate
- **Password Required**: OFF
- **Set as Default**: ON

4. **[Deliver user certificate for authentication]**で**[On]**を選択します。



5. [**Credential Provider**]でプロバイダーを選択し、[**Save**]をクリックします。

6. ユーザープリンシパル名（UPN）の代替としてユーザー証明書のsAMAccount属性を使用する場合、XenMobileでLDAPコネクタを次のように構成します：[**Settings**] > [**LDAP**]に移動し、ディレクトリを選択して［Edit］をクリックし、[**User search by**]で[**sAMAccountName**]を選択します。



Windows Phone 8.1デバイス用のEnterprise Hubポリシーの作成

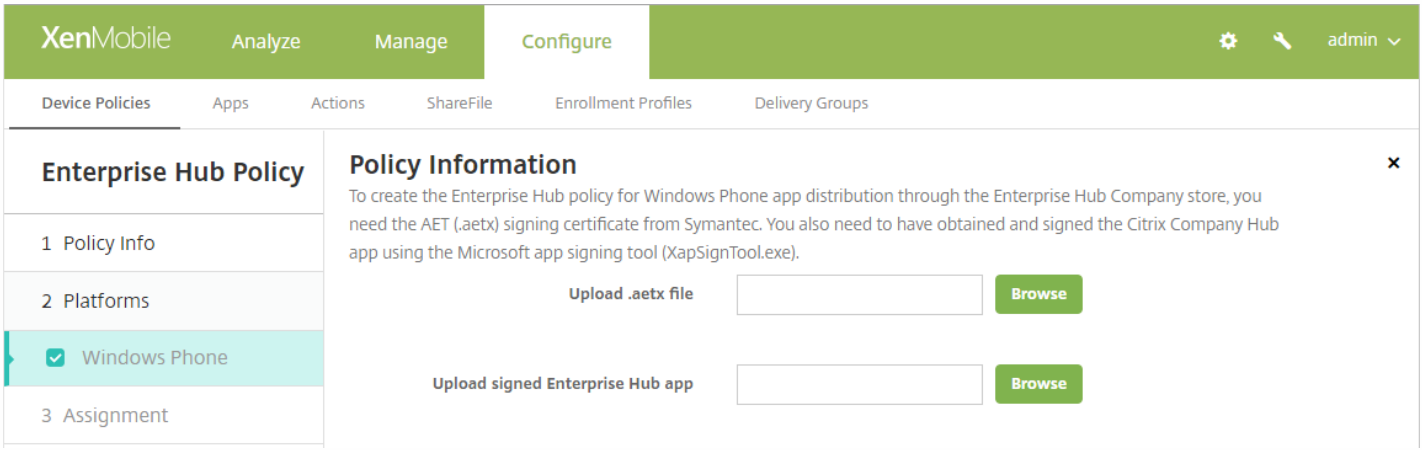
Windows Phone 8.1デバイスの場合、Enterprise Hubデバイスポリシーを作成して、AETXファイルおよびWorx Homeクライアントを配信する必要があります。

> **注意**
>
> AETXファイルとWorx Homeファイルの両方が、証明書プロバイダーからの同じエンタープライズ証明書と、Windowsストア開発者アカウントからの同じ発行元IDを使用していたことを確認します。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。

2. ［**Add**］をクリックした後、［**More**］>［**XenMobile Agent**］の下の［**Enterprise Hub**］をクリックします。

3. ポリシーに名前を付けた後で、必ずエンタープライズハブに対して適切な.AETXファイルと署名されたWorx Homeアプリを選択します。



4. ポリシーをデリバリーグループに割り当て、保存します。

NetScaler for XenMobileウィザードを使用して証明書認証用にNetScaler Gatewayを構成する

> **注意**
>
> NetScaler for XenMobileウィザードは1回のみ実行できます。 ウィザードをすでに使用した場合、「証明書認証用のNetScaler Gatewayの手動構成」の手順に従います。続いて、次のようにします。

次の手順で、XenMobileの証明書認証用にNetScalerアプライアンスを構成します。

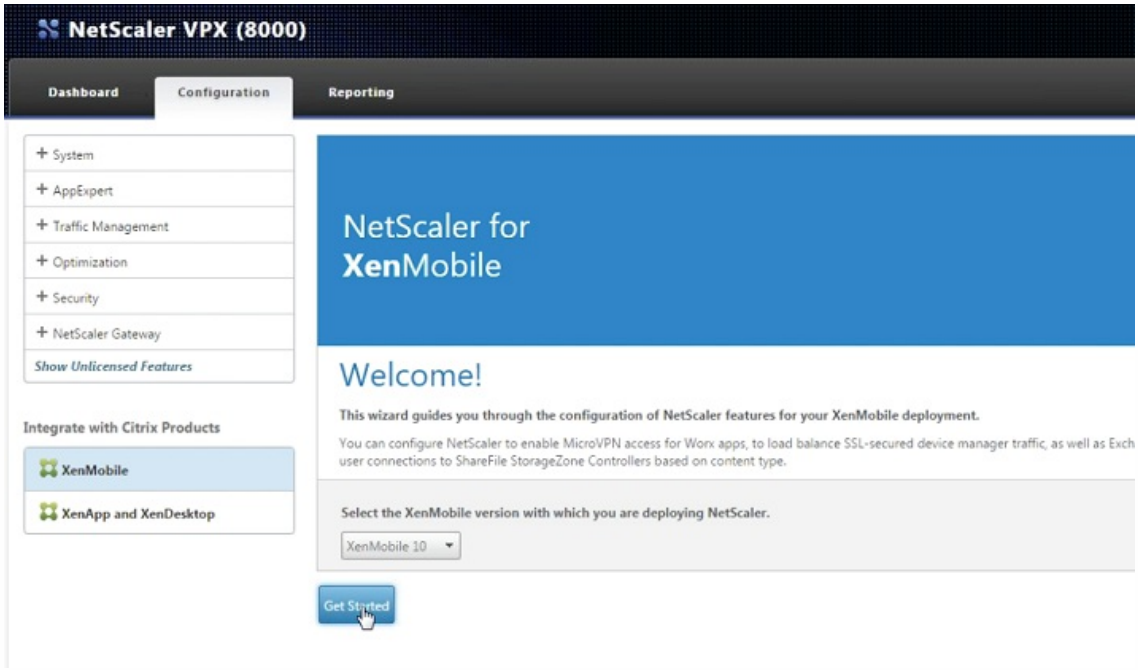
1. NetScalerにログオンします。

2. **[構成]** で、 **[Integrate with Citrix Products]** に移動し、 **[XenMobile]** を選択します。

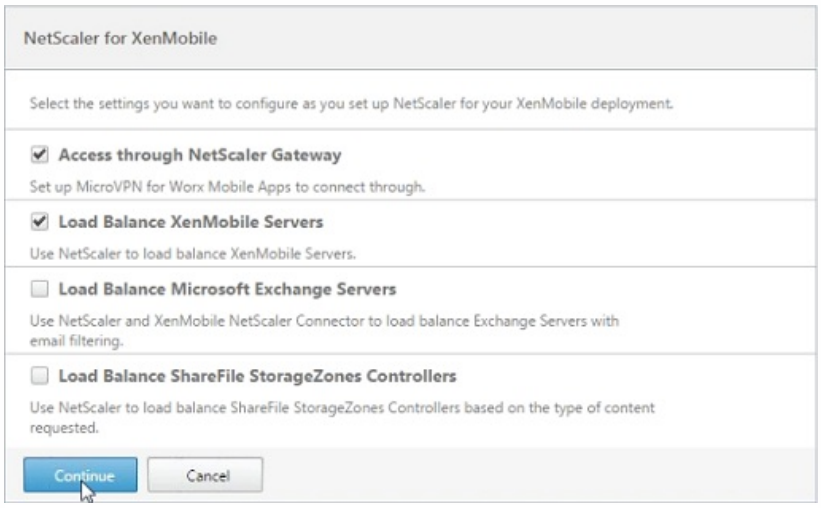
これによって、XenMobile環境でNetScaler機能を構成するウィザードが開きます。

3. **[XenMobile 10]** を選択します。

4. **[Get Started]** をクリックします。



5. 次の画面で、 **[Access through NetScaler Gateway]** （ENTモードおよびMAMモードの場合）と **[Load Balance XenMobile Servers]** 選択してから、 **[続行]** をクリックします。



6. 次の画面で外部向けのNetScaler GatewayのIPアドレスを入力し、 **[続行]** をクリックします。

NetScaler Gatewayのサーバー証明書画面が表示されます。

7. 既存の証明書を使用するか、証明書をインストールします。 **[続ける]** をクリックします。

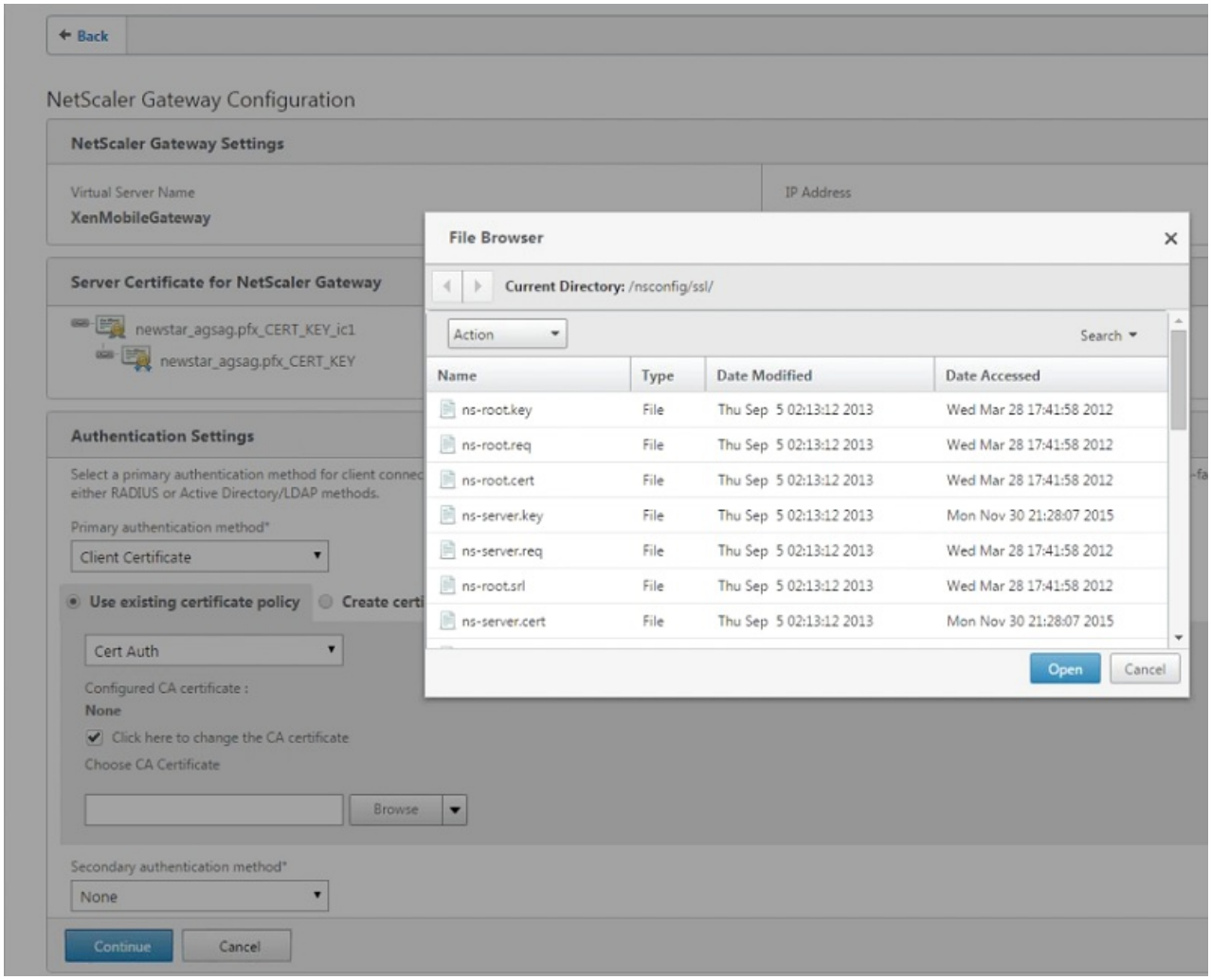
[認証設定] 画面が表示されます。

8. **[Primary authentication method]** フィールドで、 **[クライアント証明書]** を選択します。

これによって、次の2つのフィールドで自動的に **[Use existing certificate policy]** および **[Cert Auth]** を選択します。 次の手順では、証明書ポリシーがすでにあることを前提しています。

証明書を作成する必要がある場合、 **[Create certificate policy]** をクリックして、設定を完了します。 **[XenMobile Server Certificate]** 画面で、既存のサーバー証明書を選択するか、新しい証明書をインストールします。 複数のXenMobileサーバーを実行している場合、各サーバーに証明書を追加します。 **[Server Logon Name Attribute]** には、 **[userPrincipalName]** または **[samAccountName]** を指定します。

9. **[Click here to change the CA certificate]** を選択してから、 **[参照]** 一覧から目的のCA証明書に移動します。



10. **[Second authentication method]** を **[なし]** のままにして、 **[続ける]** をクリックします。

11. **[Device certificate]** 画面で、証明書がまだインストールされていない場合、XenMobileコンソールからこの証明書をエクスポートする必要があります。 必要な操作：

a. コンソールで、右上の歯車アイコンをクリックして、**[設定]** 画面を開きます。

b. **[証明書]** をクリックして、一覧からCA証明書を選択します。

c. **[Export]** をクリックします。

d. NetScalerウィザードに戻って、インストールのためにエクスポート（ダウンロード）した証明書を選択します。

e. **[続ける]** をクリックします。

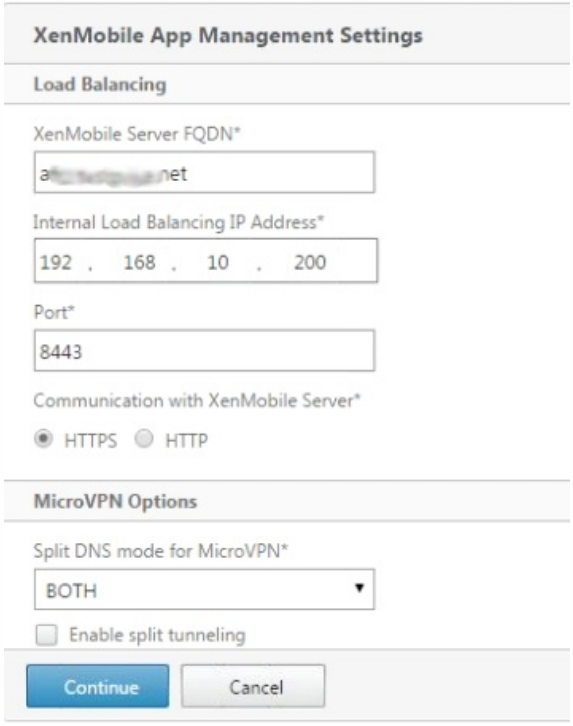
既に構成したXenMobileサーバーのIPアドレスが表示されます。

12. **[負荷分散]** 画面で、XenMobileサーバーのFQDNとMAM-onlyの内部負荷分散IPアドレスを入力します。

13. これはSSLオフロード展開であるため、**[Communication with XenMobile Server]** で **[HTTP]** を選択します。

[Split DNS mode for MicroVPN] フィールドに、 **[両方]** が表示されます。

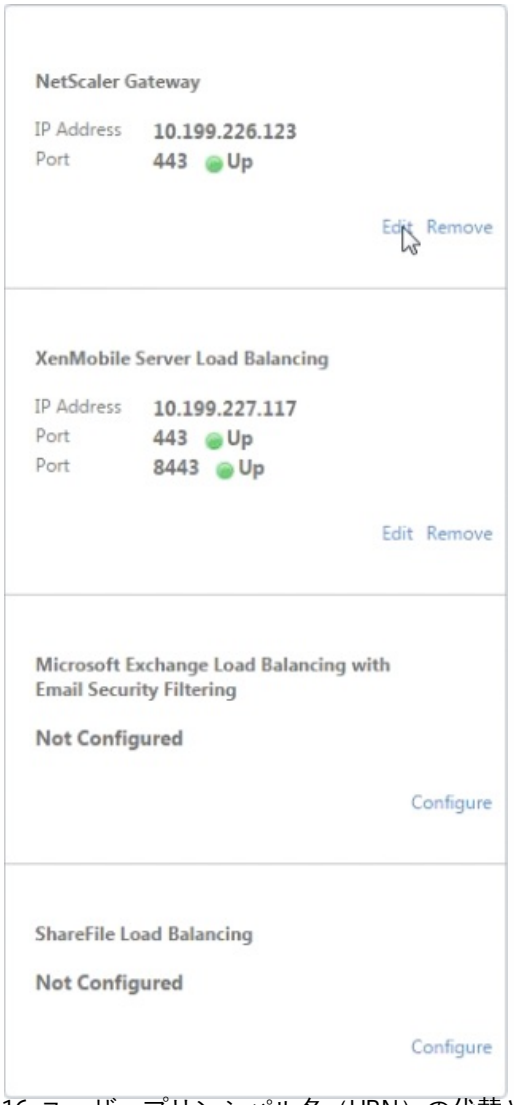
14. **[続ける]** をクリックします。



既に構成したXenMobileサーバーのIPアドレスが表示されます。

15. **[続ける]** をクリックします。

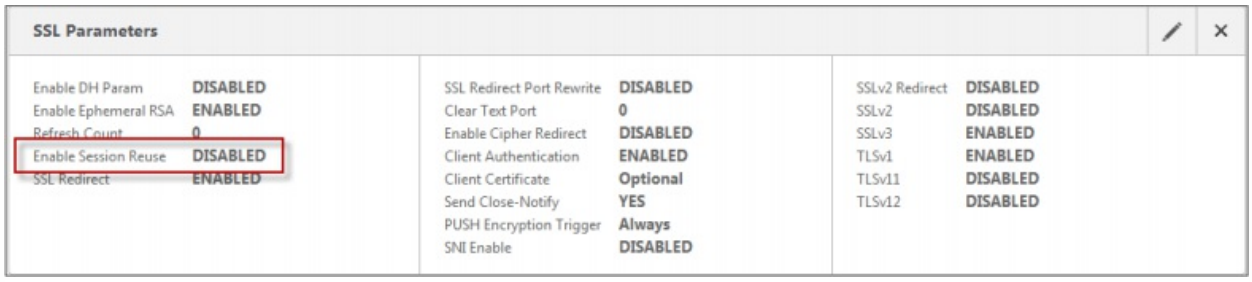
次のように、NetScalerダッシュボードで、NetScaler GatewayおよびXenMobileの負荷分散が構成されます。



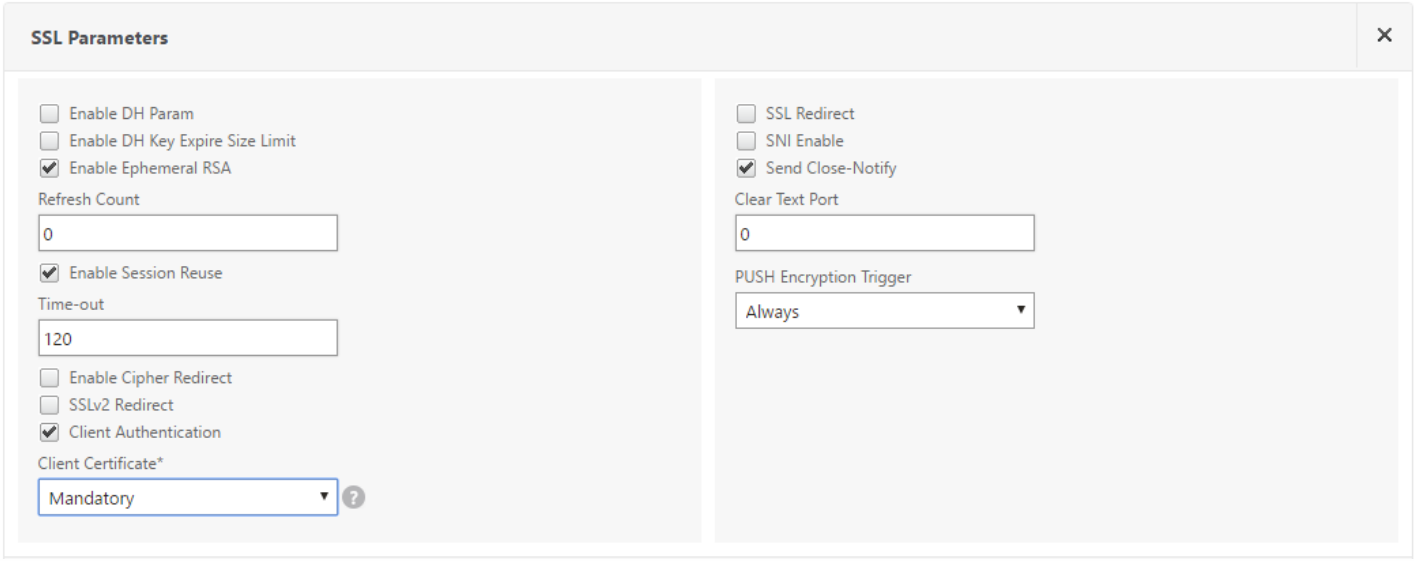
16. ユーザープリンシパル名（UPN）の代替としてユーザー証明書のsAMAccount属性を使用する場合、次のセクションの説明に従って証明書プロファイルを構成します。

証明書認証用のNetScaler Gatewayの手動構成

1. **[Traffic Management] > [Load Balancing] > [Virtual Servers]** の下で、各仮想サーバー（443と8443の両方）に移動し、 **[SSL Parameters]** を更新し、 **[Enable Session Reuse]** を **[DISABLED]** に設定します。



2. NetScaler Gateway仮想サーバーの **[Enable Client Authentication] > [Client Certificate]** で **[Client Authentication]** を選択し、 **[Client Certificate]** には **[Mandatory]** を選択します。



3. XenMobileが、**ユーザープリンシパル名**または**sAMAccount**を、Worx HomeによってNetScaler Gatewayに提供されたクライアント証明書から抽出できるように、新しい認証証明書ポリシーを作成します。

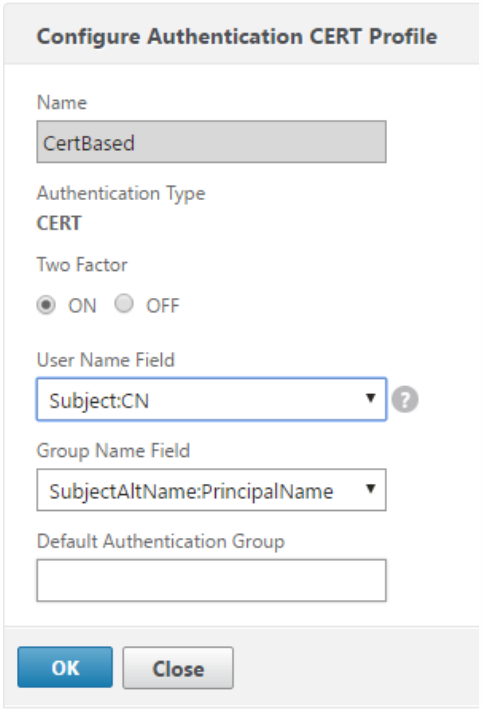
4. 証明書プロファイルに次のパラメーターを設定します。

Authentication Type：**CERT**

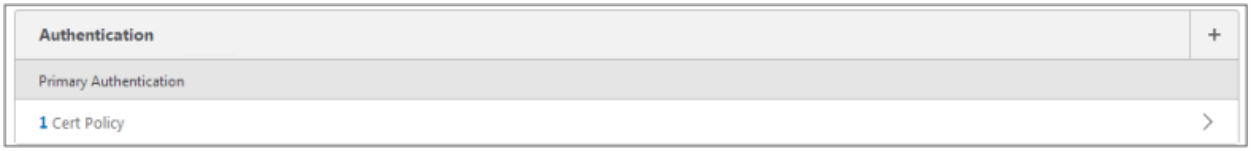
Two Factor：**ON**または**OFF**

User Name Field：**Subject:CN**

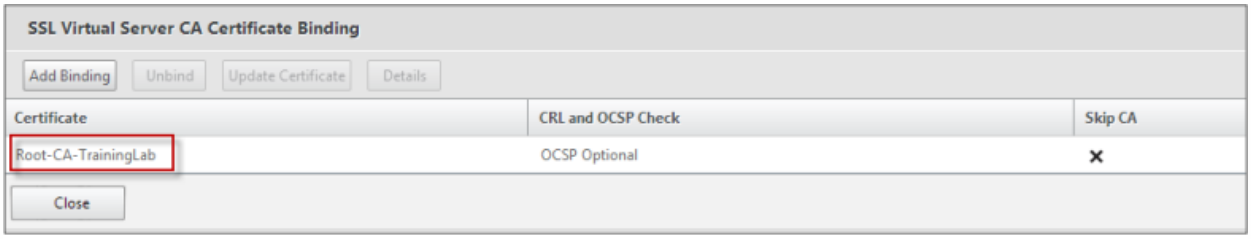
Group Name Field：**SubjectAltName:PrincipalName**



5. NetScaler Gateway仮想サーバーの［**Primary Authentication**］として、証明書認証ポリシーのみをバインドします。



6. NetScaler Gatewayに提示されたクライアント証明書の信頼を検証するには、ルートCA証明書をバインドします。



クライアント証明書構成のトラブルシューティング

構成が成功した場合、ユーザーワークフローは次のようになります。

1. ユーザーがモバイルデバイスを登録します。

2. XenMobileがユーザーにWorx PINを作成するよう求めます。

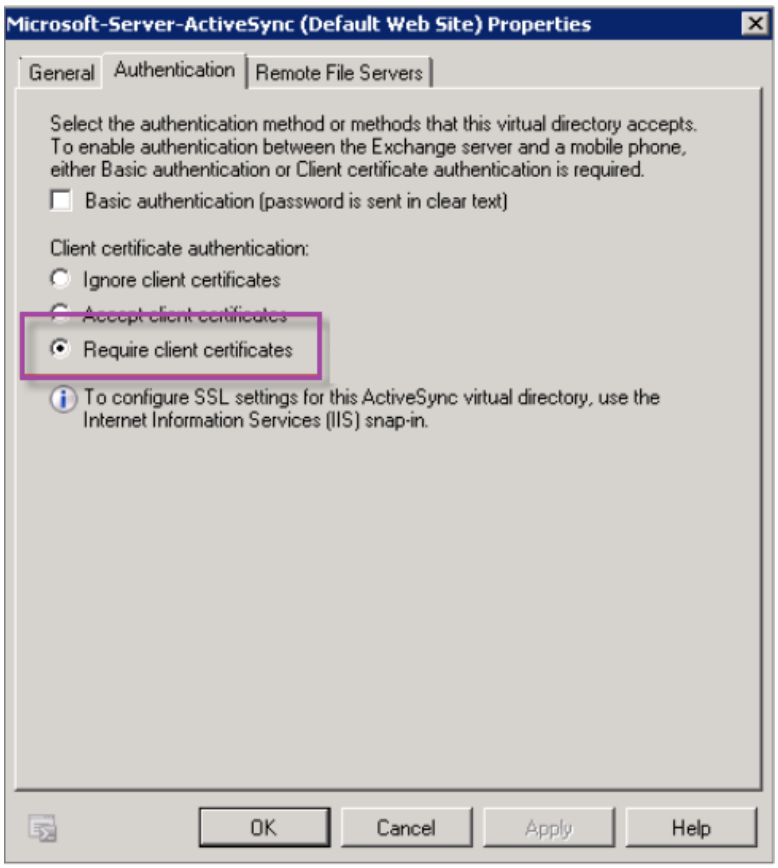
3. ユーザーがWorx Storeにリダイレクトされます。

4. ユーザーがiOS、AndroidまたはWindows Phone 8.1用のWorxMailを起動した場合、XenMobileはユーザーのメールボックスを構成するための適切な資格情報を求めません。 その代わりに、WorxMailはWorx Homeからのクライアント証明書を要求し、認証のためにMicrosoft Exchange Serverに送信します。 ユーザーがWorxMailを起動したときにXenMobileが資格情報を求めた場合、構成を確認します。

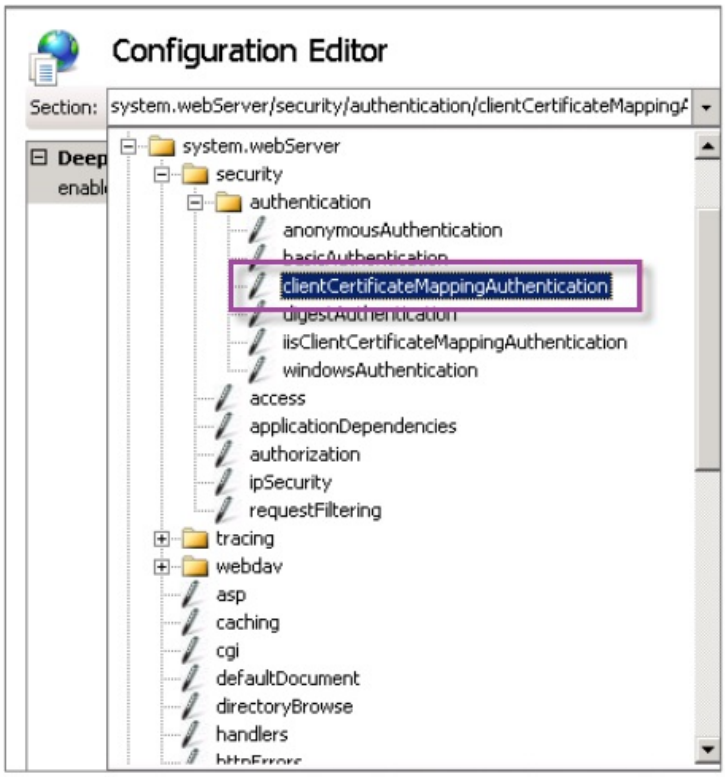
ユーザーはWorxMailをダウンロードしてインストールできるが、WorxMailがメールボックス構成時に構成を完了できない場合：

1. Microsoft Exchange Server ActiveSyncがプライベートSSLサーバー証明書を使用してトラフィックを保護している場合、ルート証明書または中間証明書がモバイルデバイスにインストールされていることを確認してください。

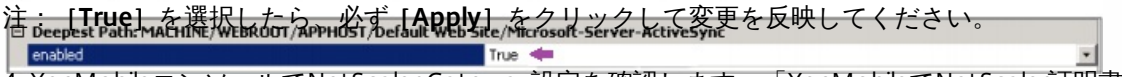
2. ActiveSyncに対して選択された認証の種類が［**Require client certificates**］であることを確認します。



3. Microsoft Exchange Serverで、**Microsoft-Server-ActiveSync**サイトのクライアント証明書マッピング認証が有効になっていることを確認します（デフォルトでは無効）。 オプションは、［**Configuration Editor**］>［**Security**］>［**Authentication**］にあります。



注：［**True**］を選択したら、必ず［**Apply**］をクリックして変更を反映してください。



4. XenMobileコンソールでNetScaler Gateway設定を確認します：「XenMobileでNetScaler証明書の配信を構成するには」の説明に従って、［**Deliver user certificate for authentication**］が［**ON**］で、［**Credential provider**］で適切なプロファイルが選択されていることを確認してください。

クライアント証明書がモバイルデバイスに配信されたかどうかを判定するには：

1. XenMobileコンソールで、［**Manage**］>［**Devices**］と移動して、デバイスを選択します。

2. ［**Edit**］または［**Show More**］をクリックします。

3. ［**Delivery Groups**］セクションに移動し、このエントリを検索します。

    NetScaler Gateway Credentials : Requested credential, CertId=

クライアント証明書ネゴシエーションが有効かどうか確認するには：

1. このnetshコマンドを実行して、IIS WebサイトにバインドされたSSL証明書構成を表示します。

    netsh http show sslcert

2. ［**Negotiate Client Certificate**］の値が［**Disabled**］の場合、次のコマンドを実行して有効化します。

    netsh http delete sslcert ipport=0.0.0.0:443

    netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable

たとえば、次のように設定します：

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

XenMobileを介してWindows Phone 8.1デバイスにルート証明書または中間証明書を配信できない場合：

- 電子メールを介してWindows Phone 8.1デバイスにルート証明書または中間証明書（.cer）ファイルを送信し、直接インストールします。

WorxMailがWindows Phone 8.1に正常にインストールされない場合：

- Enterpriseハブデバイスポリシーを使用して、XenMobile経由でアプリケーション登録トークン（.AETX）ファイルが配信されていることを確認します。
- アプリケーション登録トークンが、WorxMailをラップし、Worx Homeアプリに署名するために使用された証明書プロバイダーからの同じエンタープライズ証明書を使用して作成されたことを検証します。
- 同じ発行元IDが、Worx Home、WorxMail、およびアプリケーション登録トークンをラップし、署名するために使用されていることを確認します。

PKIエンティティ

Oct 25, 2016

XenMobileのPKI（Public Key Infrastructure：公開キーのインフラストラクチャ）エンティティ構成は、実際のPKI処理（発行、失効、状態情報）を実行するコンポーネントを表します。 これらのコンポーネントはXenMobileに対して内部（この場合は随意と呼ばれます）、またはそれらが企業インフラストラクチャの一部である場合はXenMobileに対して外部になります。

XenMobileは次の種類のPKIエンティティをサポートします。

- 随意CA（Certificate Authority：証明機関）
- 汎用PKIs（GPKIs）
- Microsoft Certificate Services

XenMobileでは、次のCAサーバーがサポートされます。

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

共通のPKI概念

種類に関係なく、すべてのPKIエンティティには以下の機能のサブセットがあります。

- 署名：証明書署名要求（CSR）に基づく新しい証明書の発行
- フェッチ：既存の証明書とキーペアの回収
- 失効：クライアント証明書の失効

CA証明書

PKIエンティティを構成するときに、XenMobileに、そのエンティティにより発行される（またはそのエンティティから回収される）証明書の署名者になるCA証明書を示す必要があります。 1つの同じPKIエンティティから、複数の異なるCAが署名した、（フェッチされたか、または新たに署名された）証明書が返されることがあります。 これらのCAそれぞれの証明書を、PKIエンティティ構成の一部として提供する必要があります。 これを行うため、証明書をXenMobileにアップロードして、PKIエンティティでそれらを参照します。 随意CAの場合、証明書は暗黙的に署名CA証明書になりますが、外部のエンティティの場合は、手動で証明書を指定する必要があります。

汎用PKI

汎用PKI（Generic PKI：GPKI）プロトコルは、さまざまなPKIソリューションとの統一された連携を目的としてSOAP Webサービスレイヤーで実行される独自のXenMobileプロトコルです。 GPKIプロトコルは、以下の3つの基本PKI処理を定義します。

- 署名：アダプターはCSRを取得し、それらの要求をPKIに送信して、新しい署名入り証明書を返すことができます。
- フェッチ：アダプターは既存の証明書とキーペア（入力パラメーターによる）をPKIから取得できます。
- 失効：アダプターはPKIで特定の証明書を失効させることができます。

GPKIプロトコルの受信側はGPKIアダプターです。 GPKIアダプターによって、基本処理がそのアダプターが作成された特定の種類のPKIに変換されます。 つまり、RSA用のGPKIアダプターと、もう1つEnTrust用のGPKIアダプターなどがあります。

GPKIアダプターは、SOAP Webサービスのエンドポイントとして、自己記述型のWeb Services Description Language（WSDL）定義を公開します。 GPKI PKIエンティティの作成は、URLを通じてまたはファイルそのものをアップ

ロードして、XenMobileにそのWSDL定義を提供することを意味します。

アダプターでの各PKI操作のサポートはオプションです。 アダプターが特定の処理をサポートする場合、アダプターには対応する機能（署名、フェッチ、失効）があると見なされます。 これらの各機能は一連のユーザーパラメーターに関連付けられている場合があります。

ユーザーパラメーターは、特定の処理についてGPKIアダプターで定義されるパラメーターで、XenMobileに値を提供する必要があります。 アダプターがサポートする処理（アダプターの機能）と各処理に必要なパラメーターは、XenMobileによりWSDLファイルを解析して決定されます。 選択した場合、SSLクライアント認証によってXenMobileとGPKIアダプターの間の接続が保護されます。

汎用PKIを追加するには

1. XenMobileコンソールで、 **[Configure]** 、 **[Settings]** 、 **[More]** 、 **[PKI Entities]** の順にクリックします。

2. **[PKI Entities]** ページで、 **[Add]** をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. **[Generic PKI Entity]** をクリックします。

[Generic PKI Entity: General Information] ページが開きます。

4. **[Generic PKI Entity: General Information]** ページで、以下を行います。

- **Name**：PKIエンティティの説明的な名前を入力します。
- **WSDL URL**：アダプターについて記述しているWSDLの場所を入力します。
- **Authentication type**：一覧から、使用する認証方法を選択します。
- なし
- **HTTP Basic**：アダプターへの接続に必要な ユーザー名 とパスワードを指定します。
- **Client certificate**：正しいSSLクライアント証明書を選択します。

5. **[Next]** をクリックします。

[Generic PKI Entity: Adapter Capabilities] ページが開きます。

6. **[Generic PKI Entity: Adapter Capabilities]** ページで、アダプターに関連付けられた機能とパラメーターを確認して、 **[Next]** をクリックします。

[Generic PKI Entity: Issuing CA Certificates] ページが開きます。

7. [Generic PKI Entity: Issuing CA Certificates] ページで、エンティティで使用する証明書を選択します。

注：エンティティからは、異なるCAによって署名された証明書が返される場合がありますが、特定の証明書プロバイダーから取得される証明書の署名は、すべて同じCAによって行われる必要があります。 したがって、**資格情報プロバイダー**設定を構成するときに **[Distribution]** ページで、ここで構成したいずれかの証明書を選択してください。

8. **[Save]** をクリックします。

[PKI Entities] の表にエンティティが表示されます。

Microsoft Certificate Services

XenMobileは、Web登録インターフェイスを通じてMicrosoft Certificate Servicesと連携します。 XenMobileはそのインター

フェイスを使用した新しい証明書の発行（GPKI署名機能と同等の機能）のみをサポートします。

XenMobileでMicrosoft CA PKIエンティティを作成するには、Certificate ServicesのWebインターフェイスのベースを指定する必要があります。 選択した場合、SSLクライアント認証によって、XenMobileとCertificate ServicesのWebインターフェイスとの間の接続が保護されます。

Microsoft Certificate Servicesエンティティを追加するには

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、**[More]** の **[PKI Entities]** をクリックします。

2. **[PKI Entities]** ページで、 **[Add]** をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. **[Microsoft Certificate Services Entity]** をクリックします。

[Microsoft Certificate Services Entity: General Information] ページが開きます。

4. [Microsoft Certificate Services Entity: General Information] ページで、以下を行います。

- Name：新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。 エンティティ名は一意の名前にする必要があります。
- Web enrollment service root URL：Microsoft CA Web登録サービスのベースURL（https://192.0.2.13/certsrv/など）を入力します。 URLには、HTTPまたはHTTP-over-SSLを使用します。
- certnew.cer page name：certnew.cerページの名前。 何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- certfnsh.asp：certfnsh.aspページの名前。 何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- Authentication type：一覧から、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指定します。
- Client certificate：正しいSSLクライアント証明書を選択します。

5. **[Next]** をクリックします。

[Microsoft Certificate Services Entity: Templates] ページが開きます。 このページで、Microsoft CAがサポートするテンプレートの内部名を指定します。 資格情報プロバイダーを作成するとき、ここで定義したテンプレートを一覧で選択します。 このエンティティを使用するすべての資格情報プロバイダーが、このようなテンプレートを1つだけ使用します。

Microsoft証明書サービステンプレートの要件については、お使いのバージョンのMicrosoft Serverに関するMicrosoftドキュメントを参照してください。 XenMobileで配信する証明書の要件は、「証明書」に記載されている証明書形式に関するもののみです。

6. **[Microsoft Certificate Services Entity: Templates]** ページで **[Add]** をクリックし、テンプレートの名前を入力して、 **[Save]** 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。

7. **[Next]** をクリックします。

[Microsoft Certificate Services Entity: HTTP parameters] ページが開きます。 このページで、Microsoft Web登録インターフェイスに対するHTTP要求にXenMobileが挿入するカスタムパラメーターを指定します。 これは、カスタマイズしたスクリプトをCAで実行している場合にのみ使用できます。

8. **[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**］ページが開きます。 このページでは、システムでこのエンティティを通じて取得される証明書の署名者をXenMobileに通知するよう要求されます。 CA証明書が更新された場合は、そのCA証明書をXenMobileで更新すると、変更がエンティティに透過的に適用されます。

9. ［**Microsoft Certificate Services Entity: CA Certificates**］ページで、このエンティティで使用する証明書を選択します。

10. ［**Save**］をクリックします。

［PKI Entities］の表にエンティティが表示されます。

NetScaler証明書失効一覧（CRL）

XenMobileは、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートします。 Microsoft CAが構成されている場合、XenMobileはNetScalerを使用して失効を管理します。 クライアント証明書ベースの認証を構成する場合、NetScaler証明書失効一覧（CRL）設定を構成する必要があるかどうか検討します。 ［**Enable CRL Auto Refresh**］。 この手順を使用すると、MAM-onlyモードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証することができなくなります。ユーザー証明書が失効してもユーザーによる生成が制限されるわけではないので、XenMobileは新しい証明書を再発行します。 この設定は、CRLが期限切れのPKIエンティティを確認する場合、PKIエンティティのセキュリティを強化します。

随意CA

随意CAは、CA証明書と関連の秘密キーをXenMobileに提供したときに作成されます。 XenMobileは、管理者が指定したパラメーターに従って、証明書の発行、失効、および状態情報を内部で処理します。

随意CAを構成するときに、そのCAに対してOCSP（Online Certificate Status Protocol）サポートをアクティブにするオプションがあります。 OCSPサポートを有効にした場合に限り、CAは発行する証明書にid-pe-authorityInfoAccess拡張を追加して、以下の場所にあるXenMobileの内部OSCPレスポンダーを指し示します。

https://server/instance/ocsp
OCSPサービスを構成するときに、該当の随意エンティティのOCSP署名証明書を指定する必要があります。 CA証明書そのものを署名者として使用できます。 CA秘密キーの不必要な漏えいを防ぐ場合（推奨）は、CA証明書で署名された、委任OCSP署名証明書を作成し、id-kp-OCSPSigning extendedKeyUsage拡張を含めます。

XenMobile OCSPレスポンダーサービスは、基本のOCSP応答と要求の以下のハッシュアルゴリズムをサポートします。

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

応答はSHA-256および署名証明書キーアルゴリズム（DSA、RSAまたはECDSA）で署名されます。

随意CAを追加するには

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、［**More**］の［**PKI Entities**］をクリックします。

2. ［**PKI Entities**］ページで、［**Add**］をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. ［**Discretionary CA**］をクリックします。

［**Discretionary CA: General Information**］ページが開きます。

4. ［**Discretionary CA: General Information**］ページで、以下を行います。

- **Name**：随意CAの説明的な名前を入力します。
- **CA certificate to sign certificate requests**：一覧から、証明書要求に署名するために使用する随意CAの証明書を選択します。 この証明書一覧は、［**Configure**］、［**Settings**］、［**Certificates**］でXenMobileにアップロードした、秘密キーのあるCA証明書から生成されます。

5. ［**Next**］をクリックします。

［**Discretionary CA: Parameters**］ページが開きます。

6. ［**Discretionary CA: Parameters**］ページで、以下を行います。
- **Serial number generator**：随意CAは発行する証明書のシリアル番号を生成します。 一覧で［**Sequential**］または［**Non-sequential**］を選択して、番号の生成方法を指定します。
- **Next serial number**：値を入力して、次に発行される番号を指定します。
- **Certificate valid for**：証明書の有効期間（日数）を入力します。
- **Key usage**：適切なキーを［**On**］に設定して、随意CAが発行する証明書の目的を指定します。 設定すると、CAによる証明書の発行がそれらの目的に限定されます。
- **Extended key usage**：追加パラメーターを追加するには、［**Add**］をクリックし、キー名を入力して［**Save**］をクリックします。

7. ［**Next**］をクリックします。

［**Discretionary CA: Distribution**］ページが開きます。

8. ［**Discretionary CA: Distribution**］ページで、配布モードを選択します。

- **Centralized: server-side key generation**。 この集中管理オプションをお勧めします。 サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
- **Distributed: device-side key generation**。 ユーザーデバイス上で秘密キーが生成されます。 この分散モードはSCEPを使用し、keyUsage keyEncryptionによるRA暗号化証明書とKeyUsage digitalSignatureによるRA署名証明書が必要です。 暗号化と署名で同じ証明書を使用できます。

9. ［**Next**］をクリックします。

［**Discretionary CA: Online Certificate Status Protocol (OCSP)**］ページが開きます。

［**Discretionary CA: Online Certificate Status Protocol (OCSP)**］ページで、以下を行います。

- このCAが署名する証明書にAuthorityInfoAccess（RFC2459）拡張を追加する場合は、［**Enable OCSP support for this CA**］を［**On**］に設定します。 この拡張は、CAのOCSPレスポンダー（https://<server>/<instance>/ocsp）を指し示します。
- OCSPサポートを有効にした場合は、OSCP署名CA証明書を選択します。 この証明書一覧は、XenMobileにアップロードしたCA証明書から生成されます。

10. ［**Save**］をクリックします。

［PKI Entities］の表に随意CAが表示されます。

資格情報プロバイダー

Aug 02, 2016

資格情報プロバイダーは、XenMobileシステムのさまざまな部分で使用する実際の証明書の構成です。 資格情報プロバイダーは、証明書がデバイス構成の一部であるかスタンドアロン（デバイスにそのままプッシュされる）であるかに関係なく、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。

デバイス登録によって証明書のライフサイクルは制約されます。 つまり、登録前に証明書は発行されませんが、登録の一部として一部の証明書が発行される場合があります。 また、1回の登録のコンテキスト内で内部PKIから発行された証明書は、登録が失効すると失効します。 管理関係が終了すると、証明書の有効性は維持されません。

1つの資格情報プロバイダーの構成を複数の場所で使用し、1つの構成によって任意の数の証明書を同時に管理することができます。 この場合、この全体は展開リソースおよび展開上にあります。 たとえば、資格情報プロバイダーPが構成Cの一部としてデバイスDに展開された場合、Dに展開される証明書はPの発行設定によって決まります。 同様に、Cが更新されるときにDの更新設定が適用され、Cが削除されたりDが失効したりしたときにはDの失効設定も適用されます。

この点を考慮し、XenMobileの資格情報プロバイダーの構成では以下を行います。

- 証明書のソースを決定します。
- 証明書を取得するときに使用する方法を決定します。新しい証明書に署名するか、既存の証明書とキーペアをフェッチ（回復）します。
- 発行または回復のパラメーターを決定します。 キーサイズ、キーアルゴリズム、識別名、証明書拡張などの証明書署名要求（Certificate Signing Request：CSR）パラメーターがあります。
- 証明書をデバイスに配信する方法を決定します。
- 失効条件を決定します。 管理関係が失われるとすべての証明書がXenMobileで失効しますが、構成によっては、関連付けられたデバイス構成が削除された場合など、以前の失効を指定する場合もあります。 また、条件によっては、XenMobileで関連付けられた証明書の失効がバックエンドのPKI（Public Key Infrastructure：公開キーのインフラストラクチャ）に送信されることがあります。つまりXenMobileでの証明書の失効によってPKIでも証明書が失効する場合があります。
- 更新設定を決定します。 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、期限が近くなると自動的に更新されるか、それとは別に、期限が近づくと通知が発行されます。

使用できる各種構成オプションの範囲は、主に、資格情報プロバイダーに対して選択したPKIエンティティの種類と発行方法によって異なります。

証明書の発行方法

証明書は2つの方法で取得でき、これを発行方法と呼びます。

- 署名。 この方法では、新しい秘密キーを作成し、CSRを作成してCA（Certificate Authority：証明機関）に送信し、署名してもらいます。 XenMobileは3種類のPKIエンティティによる署名方法をサポートします（Microsoft 証明書サービスエンティティ、汎用PKIエンティティ、任意CAエンティティ）。
- フェッチ。 この方法におけるXenMobileのための発行は、既存のキーペアの回復を意味します。 XenMobileは汎用PKIのフェッチ方法のみをサポートします。

資格情報プロバイダーは署名またはフェッチのうちいずれかの発行方法を使用します。 選択した方法は使用可能な構成オプションに影響します。 特に、CSR構成と分散配信は、発行方法が署名の場合にのみ使用できます。 フェッチされた証明書は常にPKCS#12としてデバイスに送信されます（署名方法の集中配信モードと同じ）。

証明書の配信

XenMobileでの証明書の配信には、集中と分散の2つのモードがあります。 分散モードはSCEP（Simple Certificate Enrollment Protocol）を使い、クライアントがこのプロトコルをサポートする状況でのみ使用できます（iOSのみ）。 場合によっては分散モードが必須となります。

資格情報プロバイダーで分散（SCEPを使用した）配信をサポートするには、特別な構成手順として、RA（Registration

Authority：登録機関）証明書の設定が必要です。 RA証明書が必要なのは、SCEPプロトコルを使用する場合、XenMobileが実際のCAに対する代理（登録機関）と同様に機能し、XenMobileはそのような役割を果たす権限があることをクライアントに証明する必要があるためです。 その権限は、XenMobileに前述の証明書を提供することにより確立されます。

RA署名とRA暗号化の2つの異なる証明書の役割が必要です（1つの証明書で両方の要件を満たすことができます）。 これらの役割には以下の制約があります。

- RA署名証明書には、X.509キー使用法デジタル署名が必要です。
- RA暗号化証明書には、X.509キー使用法キーの暗号化が必要です。

資格情報プロバイダーのRA証明書を構成するには、それらの証明書をXenMobileにアップロードし、資格情報プロバイダーでそれらの証明書にリンクします。

資格情報プロバイダーに証明書の役割について構成されている証明書がある場合、分散配信のみをサポートするとみなされます。 各資格情報プロバイダーは、集中モードを優先するか、分散モードを優先するか、または分散モードを必要とするように構成できます。 実際の結果はコンテキストに応じて異なります。コンテキストが分散モードをサポートしないにもかかわらず、資格情報プロバイダーに分散モードが必要な場合、展開は失敗します。 同様に、コンテキストに分散モードが必要な場合でも、資格情報プロバイダーが分散モードをサポートしていなければ、展開は失敗します。 ほかのすべての場合、優先設定が適用されます。

次の表は、XenMobile全体におけるSCEP分散を示しています。

コンテキスト	SCEPのサポート	SCEPの必要
iOSプロファイルサービス	はい	はい
iOSモバイルデバイス管理登録	はい	いいえ
iOS構成プロファイル	はい	いいえ
SHTP登録	いいえ	いいえ
SHTPの構成	いいえ	いいえ
Windows Phone登録	いいえ	いいえ
Windows Phoneの構成	いいえ	いいえ

証明書の失効

失効には以下の3つの種類があります。

- **内部失効**。 内部失効はXenMobileで維持されている証明書の状態に影響します。 この状態は、XenMobileに提示された証明書をXenMobileで評価するとき、または一部の証明書のOCSP状態に関する情報をXenMobileから提供する必要がある場合に考慮されます。 資格情報プロバイダー構成により、さまざまな条件下でこの状態がどのように影響を受けるかが決まります。 たとえば、資格情報プロバイダーでは、そのプロバイダーを通じて取得した証明書がデバイスから削除されたとき、失効済みのフラグが立てられるよう指定する場合があります。

- **外部に伝達される失効**。 失効XenMobileとも呼ばれるこの種類の失効は、外部のPKIから取得した証明書に適用されます。資格情報プロバイダー構成で定義された条件下で、証明書がXenMobileで内部失効すると、その証明書はPKIでも失効します。 失効を実行するための呼び出しを行うには、失効対応GPKI（General PKI：汎用PKI）エンティティが必要です。
- **外部で誘導される失効**。 失効PKIとも呼ばれるこの種類の失効も、外部のPKIから取得した証明書のみに適用されます。XenMobileで特定の証明書の状態が評価されるたびに、その状態についてPKIに照会されます。 PKIで証明書が失効している場合、XenMobileで証明書が内部失効します。 このメカニズムではOCSPプロトコルが使用されます。

これらの3つの種類は排他的ではなく、同時に適用されます。内部失効は外部失効または独立した検出により生じ、その結果、内部失効が外部失効を発生させる可能性があります。

証明書の書き換え

証明書の書き換えとは、既存の証明書の失効と別の証明書の発行を両方行うことです。

XenMobileでは、発行が失敗した場合にサービスが途絶えるのを防ぐため、以前の証明書が失効する前にまず新しい証明書の取得を試行します。 （SCEP対応の）分散配信を使用する場合、失効は証明書がデバイスに正しくインストールされてから一度だけ発生します。使用しない場合、新しい証明書がデバイスに送信される前に、インストールの成否に関係なく失効が発生することになります。

失効の構成では、特定の期間を日単位で指定する必要があります。 デバイスが接続されると、証明書のNotAfterの日付からこの指定した期間を引いて、現在の日付より後になっているかどうかがサーバーによって検証されます。 現在の日付より後になっている場合、書き換えが試行されます。

資格情報プロバイダーを作成するには

資格情報プロバイダーの構成は、主に、資格情報プロバイダーに対して選択した発行エンティティや発行方法により異なります。 内部エンティティを使用する資格情報プロバイダー（随意など）と、外部エンティティを使用する資格情報プロバイダー（Microsoft CAやGPKIなど）に区別することができます。 随意エンティティの発行方法は 常に署名です。つまり、各発行操作で、XenMobileはエンティティに対して選択されたCA証明書で新しいキーペアに署名します。 キーペアがデバイスまたはサーバーのどちらで生成されるかは、選択した分散方法によって異なります。

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックした後、［**More**］の［**Credential Providers**］をクリックします。

2. ［**Credential Providers**］ページで、 ［**Add**］をクリックします。

［**Credential Providers: General Information**］ページが開きます。

3. ［**Credential Providers: General Infomation**］ページで、以下を指定します。

- **Name**：新しいプロバイダー構成の一意の名前を入力します。 この名前はXenMobileコンソールのほかの部分で構成を参照するために後で使用されます。
- **Description**：資格情報プロバイダーの説明です。 このフィールドはオプションですが、後でこの資格情報プロバイダーの詳細を思い出すときに説明が役立ちます。
- **Issuing entity**：証明書発行エンティティを選択します。
- **Issuing method**： ［**Sign**］または［**Fetch**］をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。クライアント証明書による認証の場合は［**Sign**］を使用します。
- テンプレート一覧が使用できる場合は、資格情報プロバイダーのテンプレートを選択します。

4. ［**Next**］をクリックします。

注：これらのテンプレートは、［**Settings**］、 ［**More**］、 ［**PKI Entities**］の順にクリックすると開くページで、Microsoft

証明書サービスエンティティが追加されている場合に使用可能になります。

［**Credential Providers: Certificate Signing Request**］ページが開きます。

5. ［**Credential Providers: Certificate Signing Request**］ページで、以下を指定します。

- **Key algorithm**：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。
- **Key size**：キーペアのサイズ（ビット単位）を入力します。 これは必須フィールドです。
  注：許可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。 基になるハードウェアおよびソフトウェアに依存する偽陰性を回避するため、XenMobileではキーのサイズが強制されません。 資格情報プロバイダーの構成を実稼働環境でアクティブにする前に、必ずテスト環境でテストしてください。

- **Signature algorithm**：新しい証明書の値を選択します。 値はキーアルゴリズムによって異なります。
- **Subject name**：新しい証明書のサブジェクトの識別名（Distinguished Name：DN）を入力します。 例：CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation これは必須フィールドです。

  たとえば、クライアント証明書認証には次の設定を使用します。

  キー アルゴリズム：RSA
  キー サイズ：2048
  署名アルゴリズム：SHA1withRSA
  サブジェクト名：cn=$user.username

6. ［**Subject alternative names**］の表に新しいエントリを追加するには、［**Add**］をクリックします。 別名の種類を選択して、2つ目の列に値を入力します。

  クライアント証明書認証では、次のように指定します。

  種類：ユーザープリンシパル名
  値：$user.userprincipalname

注：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。

7. ［**Next**］をクリックします。

［**Credential Providers: Distribution**］ページが開きます。

8. ［**Credential Providers: Distribution**］ページで、以下を行います。

- ［**Issuing CA certificate**］の一覧から、提供されたCA証明書を選択します。 資格情報プロバイダーは随意CAエンティティを使用するため、資格情報プロバイダーのCA証明書は常にエンティティそのものに構成されているCA証明書になります。ここでは外部エンティティを使用する構成との整合性のために示されます。
- ［**Select distribution mode**］で、次のいずれかのキーの生成および配布方法をクリックします。
  - **Prefer centralized: Server-side key generation**。 この集中管理オプションをお勧めします。 このオプションはXenMobileでサポートされるすべてのプラットフォームをサポートし、NetScaler Gateway認証を使用する場合は必須です。 サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
  - **Prefer distributed: Device-side key generation**。 ユーザーデバイス上で秘密キーが生成および保存されます。 この分散モードはSCEPを使用し、keyUsage keyEncryptionによるRA暗号化証明書とKeyUsage digitalSignatureによるRA署名証明書が必要です。 暗号化と署名で同じ証明書を使用できます。
  - **Only distributed: Device-side key generation**。 このオプションは［Prefer distributed: Device-side key generation］

と同じように動作しますが、「Prefer」ではなく「Only」であるため、デバイス側でのキー生成が失敗した場合または使用できない場合にはオプションを使用できない点が異なります。

［**Prefer distributed: Device-side key generation**］または［**Only distributed: Device-side key generation**］を選択した場合は、［RA signing certificate］の一覧からRA署名証明書を選択し、［RA encryption certificate］の一覧からRA暗号化証明書を選択します。 両方に同じ証明書を使用できます。 これらの証明書のための新しいフィールドが表示されます。

9. ［**Next**］をクリックします。

［**Credential Providers: Revocation XenMobile**］ページが開きます。 このページで、XenMobileがこのプロバイダー構成により発行された証明書に内部で失効のフラグを設定する条件を構成します。

12. ［**Credential Providers: Revocation XenMobile**］ページで、以下を行います。

- ［**Revoke issued certificates**］で、証明書がいつ失効するかを示すいずれかのオプションを選択します。
- 証明書が失効したときにXenMobileから通知を送信する場合は、［**Send notification**］の値を［**On**］に設定して、通知テンプレートを選択します。

- XenMobileで証明書が失効したときに、PKIでも証明書を失効させる場合は、［**Revoke certificate on PKI**］を［**On**］に設定し、［**Entity**］の一覧からテンプレートを選択します。 ［Entity］の一覧には、失効機能で使用できるすべてのGPKIエンティティが表示されます。 XenMobileで証明書が失効すると、［Entity］の一覧から選択したPKIに、失効呼び出しが送信されます。

13. ［**Next**］をクリックします。

［**Credential Providers: Revocation PKI**］ページが開きます。 このページで、証明書が失効したときにPKIで行うアクションを特定します。 また、通知メッセージを作成するオプションもあります。

14. PKIで証明書を失効させる場合は、［**Credential Providers: Revocation PKI**］ページで以下を行います。

- ［**Enable external revocation checks**］の設定を［**On**］に変更します。 失効PKIに関連する追加のフィールドが表示されます。
- ［**OCSP responder CA certificate**］の一覧から、 証明書のサブジェクトの 識別名（Distinguished Name：DN）を選択します。 **注：**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**］の一覧から、証明書が失効したときにPKIエンティティで行う次のいずれかのアクションを選択します。

  Do nothing（何もしない）

  Renew the certificate（明書を更新する）

  Revoke and wipe the device（デバイスを取り消してワイプする）

- 証明書が失効したときにXenMobileから通知を送信する場合は、［**Send notification**］の値を［**On**］に設定します。

2つの通知オプションから選択できます。

- ［**Select notification template**］を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［Notification template］の一覧にあります。
- ［**Enter notification details**］を選択した場合は、独自の通知メッセージを作成できます。 受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

15. **[Next]** をクリックします。

[Credential Providers: Renewal] ページが開きます。 このページで、XenMobileを構成して次のことを実行できます。

- 証明書の更新、（オプション）証明書更新時の通知の送信（更新に関する通知）、および（オプション）既に期限が切れた証明書の操作からの除外
- 期限が近い証明書に関する通知の発行（更新前の通知）

16. 証明書が失効したら更新する場合は、 **[Credential Providers: Renewal]** ページ で、 **[Renew certificates when they expire]** を **[On]** に設定します。

追加のフィールドが表示されます。

- **[Renew when the certificate comes within]** フィールドに、 期限の 何日前に更新を行うかを入力します。
- 任意で、 **[Do note renew certificates that have already expired]** （既に期限が切れている証明書を更新しない）チェックボックスをオンにします。 **注：**この場合の「already expired（既に期限が切れている）」とは、証明書のNotAfterが過去の日付であることを意味し、証明書が失効しているという意味ではありません。 XenMobileでは、内部で失効した証明書は更新されません。

17. 証明書が更新されたときにXenMobileから通知を送信する場合は、 **[Send notification]** を **[On]** に設定します。 2つの通知オプションから選択できます。

- **[Select notification template]** を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、 [Notification template] の一覧にあります。
- **[Enter notification details]** を選択した場合は、独自の通知メッセージを作成できます。 受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

18. 証明書の期限が近いときにXenMobileから通知を送信する場合は、 **[Notify when certificate nears expiration]** を **[On]** に設定します。 2つの通知オプションから選択できます。

- **[Select notification template]** を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、 **[Notification template]** の一覧にあります。
- **[Enter notification details]** を選択した場合は、独自の通知メッセージを作成できます。 受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

19. **[Notify when the certificate comes within]** フィールドで、証明書の期限の何日前に通知を送信するかを入力します。

20. **[Save]** をクリックします。

資格情報プロバイダーが [Credential Provider] の表に追加されます。

APN証明書の要求

Aug 02, 2016

XenMobileでiOSデバイスを登録して管理するには、AppleのApple Push Notificationサービス（APN）証明書を設定および作成する必要があります。 ここでは、APN証明書を要求するための以下の基本的な手順の概要を説明します。

- Windows Server 2012 R2またはWindows 2008 R2 ServerとMicrosoftインターネットインフォメーションサービス（IIS）、またはMacコンピューターを使用して、CSR（Certificate Signing Request：証明書署名要求）を生成します。
- CSRにCitrixの署名を受けます。
- AppleのAPN証明書を要求します。
- 証明書をXenMobileにインポートします。

注：

- AppleのAPN証明書を使用すると、Apple Push Networkを使用してモバイルデバイスを管理できます。 証明書を失効させると、過失であっても故意であっても、デバイスを管理できなくなります。
- iOS Developer Enterprise Programを使用してMobile Device Managerプッシュ証明書を作成した場合は、既存の証明書をApple Push Certificates Portalに移行するためのアクションが必要になることがあります。

手順の概要を説明するトピックを以下に示します。この順番で実行してください。

手順1	IISでCSRを作成する MacでCSRを作成する	Windows Server 2012 R2またはWindows 2008 R2 ServerとMicrosoft IIS、またはMacコンピューターを使用してCSRを生成します。 この方法を使用することをお勧めします。
手順2	CSRに署名するには	XenMobile APNs CSR署名Webサイト（MyCitrix IDが必要）で、CitrixにCSRを送信します。 モバイルデバイス管理の署名証明書を使用して署名された.plist形式のファイルが返送されます。
手順3	署名済みのCSRをAppleに送信する	署名入りCSRをApple Push Certificate Portal（Apple IDが必要）でAppleに送信し、AppleのAPNs証明書をダウンロードします。
手順4	Microsoft IISを使用して.pfx APN証明書を作成するには Macコンピューターで.pfx APN証明書を作成するには OpenSSLを使用して.pfx APN証明書を作成する	（IIS、Mac、またはSSLで）APN証明書をPCKS #12（.pfx）証明書としてエクスポートします。
手順5	APN証明書をXenMobileにインポートする	証明書をXenMobileにインポートします。

Apple MDMプッシュ通知の移行情報

iOS Developer Enterprise Programで作成されたモバイルデバイス管理（MDM）プッシュ通知は、Apple Push Certificates Portalに移行されています。 この移行により、新しいMDMプッシュ通知の作成と既存のMDMプッシュ通知の更新、失効、およびダウンロードが影響を受けます。 そのほかの（MDM以外の）APN証明書には影響がありません。

MDMプッシュ通知がiOS Developer Enterprise Programで作成された場合、次の状況が当てはまります。

- 証明書が自動的に移行されます。
- ユーザーに影響を与えずに証明書をApple Push Certificates Portalで更新できます。
- 既存の証明書を失効またはダウンロードするには、iOS Developer Enterprise Programを使用する必要があります。

有効期限が近づいているMDMプッシュ通知がない場合は、何もする必要はありません。 有効期限が近づいているMDMプッシュ通知がある場合は、MDMソリューションプロバイダーに問い合わせてください。 次に、iOS Developer Programエージェントログを Apple IDと共にApple Push Certificates Portalに置きます。

すべての新しいMDMプッシュ通知は、Apple Push Certificates Portalで作成される必要があります。 iOS Developer Enterprise Programでは、com.apple.mgmtを含むBundle Identifier（APNsトピック）を持つApp IDを作成できなくなります。

注：証明書の作成に使用されたApple IDの記録をとる必要があります。 さらに、Apple IDは個人IDではなく会社IDでなければなりません。

Microsoft IISを使用してCSRを作成するには

iOSデバイスのAPNs証明書要求を生成するには、まずCSR（Certificate Signing Request：証明書署名要求）を作成します。 Windows 2012 R2またはWindows 2008 R2 Serverでは、Microsoft IISを使用してCSRを生成できます。

1. Microsoft IISを開きます。
2. IISのサーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ウィンドウで、**［証明書の要求の作成］**をクリックします。
4. 適切な識別名（Distinguished Name：DN）を入力して**［次へ］**をクリックします。
5. ［暗号化サービスプロバイダー］で**［Microsoft RSA SChannel Cryptographic Provider］**を選択して、ビット長として**［2048］**を選択し、**［次へ］**をクリックします。
6. ファイル名を入力してCSRを保存する場所を指定し、**［完了］**をクリックします。

MacコンピューターでCSRを作成するには

1. Mac OS Xを実行するMacコンピューターの**［アプリケーション］**>**［ユーティリティ］**で、キーチェーンアクセスアプリケーションを起動します。
2. **［キーチェーンアクセス］**メニューを開いて**［環境設定］**を選択します。
3. **［証明書］**タブをクリックして、**［OCSP］**および**［CRL］**のオプションを**［切］**に変更し、［環境設定］ウィンドウを閉じます。
4. **［キーチェーンアクセス］**メニューで、**［証明書アシスタント］**>**［認証局に証明書を要求］**の順に選択します。
5. 証明書アシスタントにより、次の情報の入力を求められます。
   1. **ユーザのメールアドレス**。 証明書の管理を担当する個人または役割アカウントのメールアドレス。
   2. **通称**。 証明書の管理を担当する個人または役割アカウントの通称。
   3. **CAのメールアドレス**。 認証局のメールアドレス。
6. **［ディスクに保存］**をクリックし、**［鍵ペア情報を指定］**チェックボックスをオンにして、**［続ける］**をクリックします。
7. CSRファイルの名前を入力してコンピューターにファイルを保存し、**［保存］**を選択します。
8. **［鍵のサイズ］**で［2048ビット］を選択し、アルゴリズムに**［RSA］**を選択してから**［続ける］**をクリックします。 APN

証明書プロセスの一環としてCSRファイルをアップロードする準備ができました。

9. 証明書アシスタンスによるCSRプロセスが完了してから**[完了]**をクリックします。

OpenSSLを使用してCSRを作成するには

Windows 2012 R2またはWindows 2008 R2 ServerとMicrosoftインターネットインフォメーションサービス（IIS）、またはMacコンピューターを使用して、Apple Push Notificationサービス（APNs）証明書のためにAppleに送信するCSR（Certificate Signing Request：証明書署名要求）を生成できない場合は、OpenSSLを使用することができます。

注：OpenSSLを使用してCSRを作成するには、まず、OpenSSLのWebサイトからOpenSSLをダウンロードしてインストールする必要があります。

1. OpenSSLをインストールしたコンピューターで、コマンドプロンプトまたはシェルから次のコマンドを実行します。
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. 証明書の名前に関する次のメッセージが表示されます。 要求された情報を入力します。
   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. 次のメッセージが表示されたら、CSRの秘密キーのパスワードを入力します。
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:

4. 結果のCSRをCitrixに送信します。

署名済みのCSRがメールで返送されてきます。

CSRに署名するには

証明書をAppleに送信する前に、Citrixの署名を受けてXenMobileで使用できるようにする必要があります。

1. ブラウザーで、XenMobile APNs CSR署名Webサイトに移動します。
2. **[Upload the CSR]**をクリックします。
3. 証明書に移動して選択します。
   注：証明書は.pem/txt形式である必要があります。

4. XenMobile APN CSR署名ページで、**[Sign]**をクリックします。 CSRが署名されて、構成されているダウンロードフォルダーに自動的に保存されます。

署名入りCSRをAppleに送信してAPN証明書を取得するには

署名入りCSR（Certificate Signing Request：証明書署名要求）をCitrixから受け取ったら、それをAppleに送信してAPN証明書を取得する必要があります。

注：一部のユーザーから、Apple Push Portalへのログイン時の問題が報告されています。 代わりの手段として、手順1でidentity.apple.comリンクにアクセスする前に、Apple Developer Portal（http://developer.apple.com/devcenter/ios/index.action）にログオンしても構いません。

1. Webブラウザーで、https://identity.apple.com/pushcertに移動します。
2. **[証明書識別情報を作成]** をクリックします。
3. Appleで初めて証明書を作成する場合は **[利用規約を読みました。内容に同意します。]** チェックボックスをオンにして、 **[同意します]** をクリックします。
4. **[ファイルの選択]** をクリックし、コンピューター上の署名入りCSRを指定して **[アップロード]** をクリックします。アップロードが成功したことを示す確認メッセージが表示されます。
5. **[ダウンロード]** をクリックして、.pem証明書を取得します。
   注：Internet Explorerを使用していて、ファイル拡張子がない場合は、 **[キャンセル]** を2回クリックして、次のウィンドウからダウンロードします。

Microsoft IISを使用して.pfx APN証明書を作成するには

XenMobileでAppleのAPN証明書を使用するには、Microsoft IISで証明書要求を完成させて、証明書をPCKS #12（.pfx）ファイルとしてエクスポートし、このAPN証明書をXenMobileにインポートする必要があります。

重要：このタスクには、CSRを生成するために使用したサーバーと同じIISサーバーを使用する必要があります。

1. Microsoft IISを開きます。
2. サーバー証明書アイコンをクリックします。
3. **[サーバー証明書]** ウィンドウで、 **[証明書の要求の完了]** をクリックします。
4. AppleのCertificate.pemファイルを指定します。 フレンドリ名または証明書名を入力して **[OK]** をクリックします。
5. 手順4で指定した証明書を選択して **[エクスポート]** をクリックします。
6. .pfx証明書の場所とファイル名およびパスワードを指定して **[OK]** をクリックします。
   注：XenMobileのインストール中にこの証明書のパスワードが必要になります。
7. .pfx証明書をXenMobileがインストールされるサーバーにコピーします。
8. XenMobileコンソールに管理者としてサインオンします。
9. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。
10. **[Certificates]** をクリックします。 **[Certificates]** ページが開きます。
11. **[Import]** をクリックします。 **[Import]** ダイアログボックスが開きます。
12. **[Import]** メニューから、 **[Keystore]** を選択します。
13. **[Use as]** から、 **[APNs]** を選択します。
14. **[Keystore]** ファイルで、 **[Browse]** をクリックしてインポートするキーストアファイルの場所に移動し、そのファイルを選択します。
15. **[Password]** ボックスに、証明書に割り当てられたパスワードを入力します。
16. **[Import]** をクリックします。

Macコンピューターで.pfx APN証明書を作成するには

1. Mac OS Xを実行する、CSRの生成に使用したものと同じMacコンピューターで、Appleから受け取ったProduction identity（.pem）証明書を見つけます。

2. 証明書ファイルをダブルクリックして、ファイルをキーチェーンにインポートします。
3. 特定のキーチェーンへの証明書の追加を確認するメッセージが表示された場合は、デフォルトの選択されたログインキーチェーンを維持して［**OK**］をクリックします。 新たに追加された証明書が証明書の一覧に表示されます。
4. 証明書をクリックして、［**ファイル**］メニューで［**エクスポート**］を選択し、証明書のPCKS #12（.pfx）証明書へのエクスポートを開始します。
5. XenMobileサーバーで使用するために証明書ファイルに一意の名前を付けて、証明書を保存する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. パスワードを入力して証明書をエクスポートします。 一意で強力なパスワードを使用することをお勧めします。 また、後で使用および参照するために証明書とパスワードを安全に保管するようにします。
7. キーチェーンアクセスアプリケーションによって、ログインパスワードまたは選択したキーチェーンを確認するメッセージが表示されます。 パスワードを入力して、［**OK**］をクリックします。 XenMobileサーバーで保存された証明書を使用する準備ができました。
   注：CSRを生成して証明書のエクスポートプロセスを完了した元のコンピューターとユーザーアカウントを保持しない場合は、ローカルシステムの個人キーと公開キーを保存するかエクスポートすることをお勧めします。 そうしなければ、再利用のためのAPN証明書へのアクセスは無効になり、CSRおよびAPNsプロセス全体を繰り返す必要があります。

OpenSSLを使用して.pfx APNs証明書を作成するには

OpenSSLを使用してCSR（Certificate Signing Request：証明書署名要求）を作成した後、OpenSSLを使用して.pfx APNs証明書を作成することもできます。

1. コマンドプロンプトまたはシェルで次のコマンドを実行します。
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. .pfx証明書ファイルのパスワードを入力します。 このパスワードは、証明書をXenMobileにアップロードするときに再び使用するので覚えておいてください。
3. .pfx証明書ファイルの場所を確認し、XenMobileコンソールを使用してアップロードできるようにXenMobileサーバーにコピーします。

APN証明書をXenMobileにインポートするには

新しいAPN証明書を要求して受け取ったら、そのAPN証明書をXenMobileにインポートして、最初の証明書として追加するか、既存の証明書を置き換えます。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。［**Settings**］ページが開きます。
2. ［**Certificates**］をクリックします。 ［**Certificates**］ページが開きます。
3. ［**Import**］をクリックします。 ［**Import**］ダイアログボックスが開きます。
4. ［**Import**］メニューから、［**Keystore**］を選択します。
5. ［**Use as**］から、［**APNs**］を選択します。
6. コンピューターの.p12ファイルを指定します。
7. パスワードを入力して、［**Import**］をクリックします。

XenMobileの証明書について詳しくは、「証明書」セクションを参照してください。

APN証明書を更新するには

APN証明書を更新するには、新しい証明書を作成する場合と同じ手順を実行する必要があります。 その後、Apple Push Certificates Portalにアクセスして、新しい証明書をアップロードします。 ログオンすると、既存の証明書（または、前のApple Developersアカウントからインポートされた証明書）が表示されます。 証明書を更新する場合は、証明書を作成する場合との唯一の違いとして、Certificates Portalで［**Renew**］をクリックします。 Certificates Portalにアクセスするには、このサイトの開発者アカウントが必要です。

注：APN証明書の有効期限を調べるには、［**Configure**］＞［**Settings**］＞［**Certificates**］の順にクリックします。 ただし、証明書の有効期限が切れていても証明書を失効させないでください。

1. Microsoftインターネットインフォメーションサービス（Internet Information Services：IIS）を使用してCSRを生成します。
2. XenMobile APNs CSR署名Webサイトで、新しいCSRをアップロードして［**Sign**］をクリックします。
3. 署名済みのCSRをApple Push Certificate PortalでAppleに送信します。
4. ［**Renew**］をクリックします。
5. Microsoft IISを使用してPCKS #12（.pfx）APN証明書を生成します。
6. XenMobileコンソールで新しいAPN証明書を更新します。 コンソールの右上にある歯車アイコンをクリックします。［**Settings**］ページが開きます。
7. ［**Certificates**］をクリックします。 ［**Certificates**］ページが開きます。
8. ［**Import**］をクリックします。 ［**Import**］ダイアログボックスが開きます。
9. ［**Import**］メニューから、［**Keystore**］を選択します。
10. ［**Use as**］から、［**APNs**］を選択します。
11. コンピューターの.p12ファイルを指定します。
12. パスワードを入力して、［**Import**］をクリックします。

ユーザーアカウント、役割、および登録設定

Aug 02, 2016

XenMobileコンソールの［Settings］ページで、ユーザーとグループ、ユーザーとグループの役割、登録モード、および招待状を構成します。 **［Settings］**ページを開くには、コンソールの右上にある歯車アイコンをクリックします。

［Settings］ページでは以下の操作を実行できます。

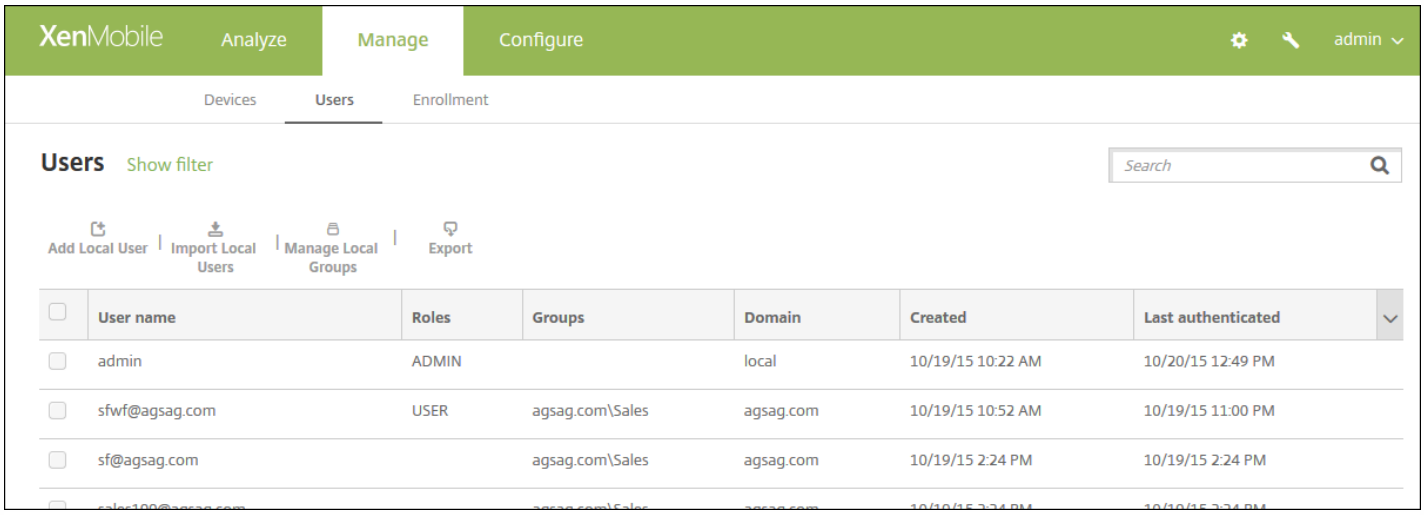
- **［Local Users and Groups］**をクリックして、ユーザーアカウントを手動で追加するか、.csvプロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理します。 詳しくは、次のページを参照してください。
  - XenMobileでローカルユーザーを追加、編集、または削除するには
  - .csvプロビジョニングファイルとプロビジョニングファイル形式を使用してユーザーアカウントをインポートするには
  - XenMobileでグループを追加または削除するには
- **［Enrollment］**をクリックして、最大7つのモードを構成します。それぞれに独自のセキュリティレベルを設定し、ユーザーがデバイスを登録するときや登録招待状を送信するときに必要ないくつかの手順を指定します。 詳しくは、次のページを参照してください。
  - 登録モードを構成してSelf Help Portalを有効化するには
  - XenMobileでのユーザー登録の自動検出の有効化
- **［Role-Based Access Control］**をクリックして、権限の定義済みセットである役割をユーザーとグループに割り当てます。 これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。 詳しくは、次のページを参照してください。
  - 「RBACを使用した役割の構成」および「RBACの役割とアクセス権」
- **［Notification Templates］**をクリックして、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを指定します。 Worx Home、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。 詳しくは、次のページを参照してください。
  - 通知テンプレートの作成および更新

XenMobileでローカルユーザーを追加、編集、または削除するには

Aug 02, 2016

ローカルユーザーアカウントをXenMobileに手動で追加したり、プロビジョニングファイルを使用してアカウントをインポートしたりすることができます。 プロビジョニングファイルからユーザーをインポートする手順については、「.csvプロビジョニングファイルを使用してユーザーアカウントをインポートするには」を参照してください。

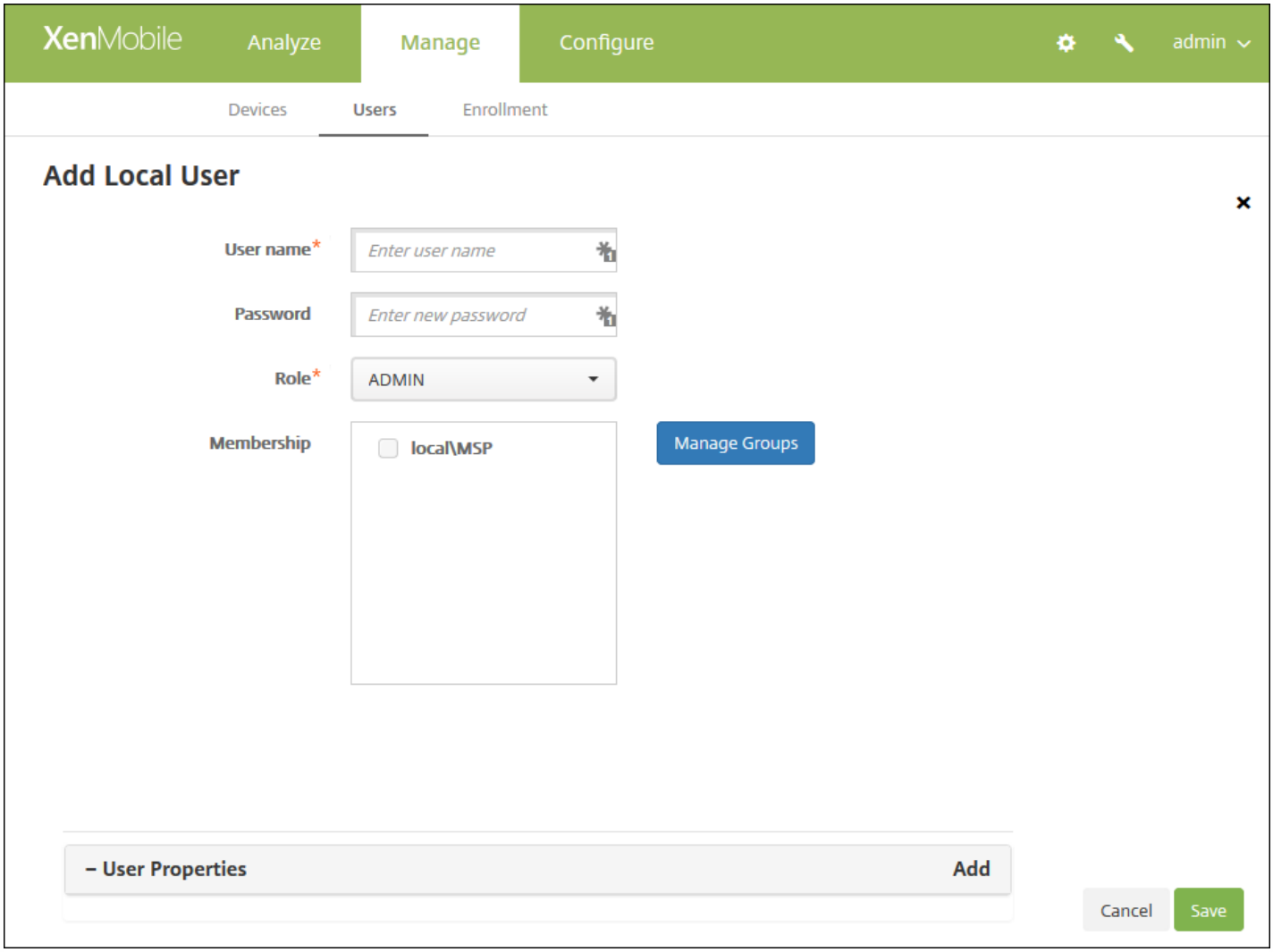
1. XenMobileコンソールで、 **[Manage]** の **[Users]** をクリックします。 **[Users]** ページが開きます。



ローカルユーザーを追加するには

この手順では、一度に単一のユーザーを追加します。 複数のユーザーを追加するには、「csvプロビジョニングファイルを使用してユーザーアカウントをインポートするには」を参照してください。

3. **[Users]** ページで、 **[Add Local User]** をクリックします。 **[Add Local User]** ページが開きます。



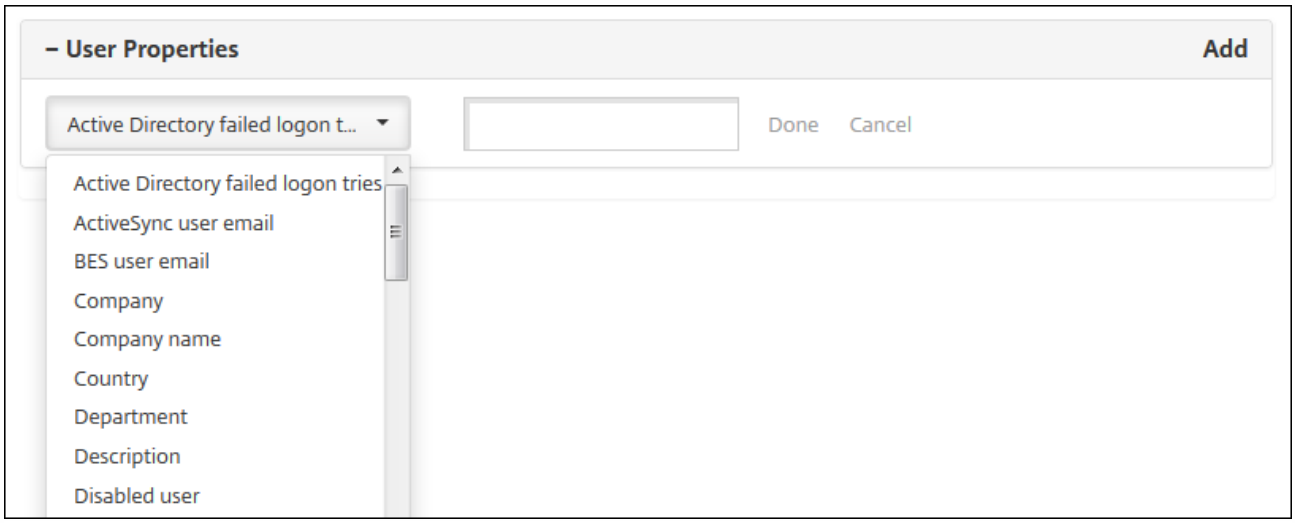
2. 次の設定を構成します。

- **User name**：ユーザーの名前を入力します。 これは必須フィールドです。 名前にはスペースや大文字、小文字を含めることができます。
- **Password**：任意で、ユーザーのパスワードを入力します。
- **Role**：一覧から、ユーザーの役割を選択します。 役割について詳しくは、「RBACを使用した役割の構成」および「RBACの役割とアクセス権」を参照してください。 選択できるオプションは以下のとおりです。
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Membership**：一覧から、ユーザーを追加するグループを選択します。
- **User properties**：任意でユーザープロパティを追加します。 追加するユーザープロパティごとに、**[Add]** をクリックして以下の操作を行います。
  - **User Properties**：一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
  - **[Done]** をクリックしてユーザープロパティを保存するか、**[Cancel]** をクリックして操作を取り消します。

  注：既存のユーザープロパティを削除するには、プロパティが含まれる行の上にマウスポインターを置き、右側の

［X］をクリックします。 プロパティがすぐに削除されます。

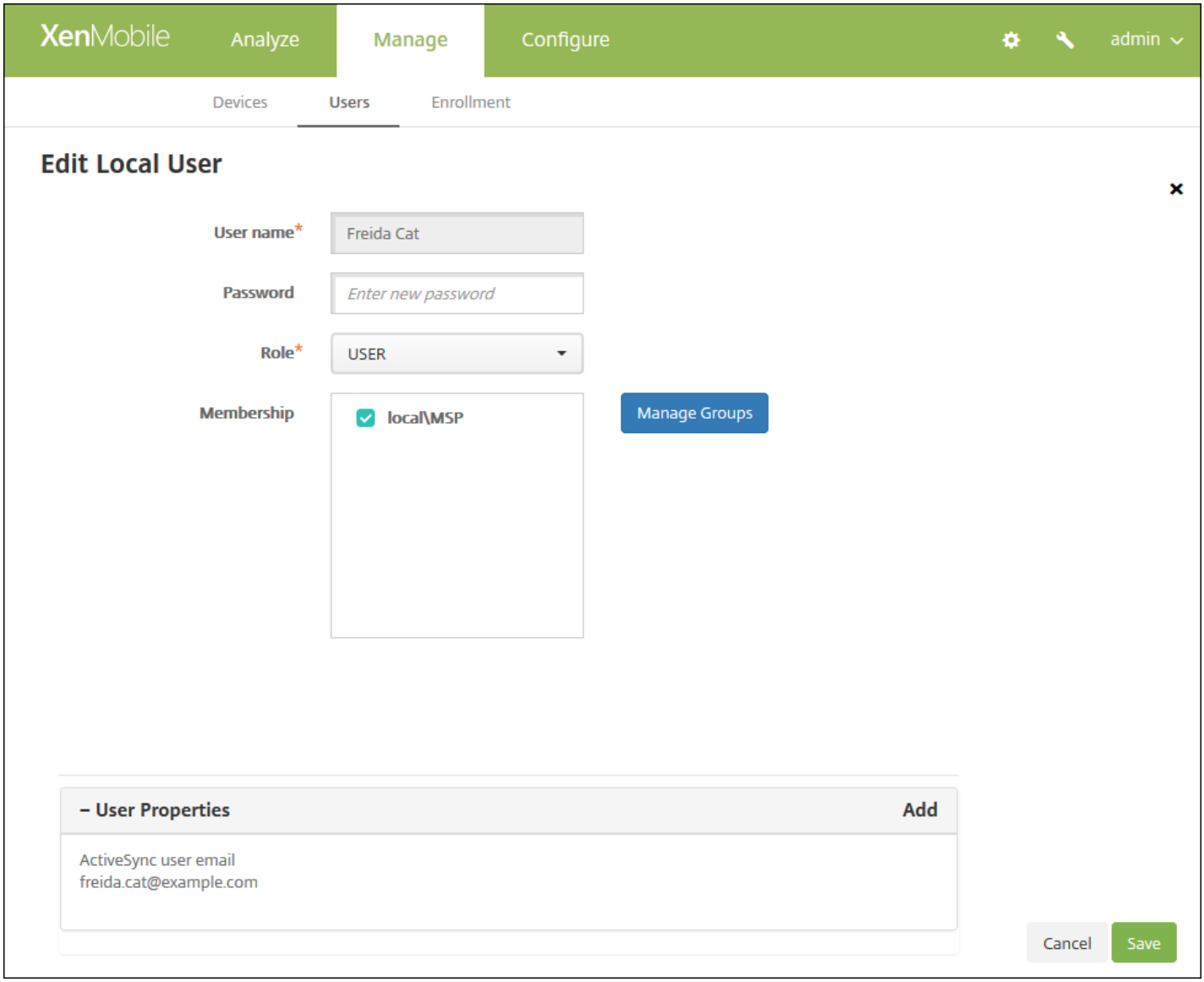
既存のユーザープロパティを編集するには、プロパティを選択して変更を加えます。［**Done**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。



3. ［**Save**］をクリックします。

ローカルユーザーを編集するには

1. ［**Users**］ページのユーザー一覧で、ユーザーをクリックして選択してから［**Edit**］をクリックします。 ［**Edit Local User**］ページが開きます。 表に含まれる項目の選択について詳しくは、「XenMobileコンソールのフィルターおよび表」を参照してください。



2. 必要に応じて以下の情報を変更します。

- **User name**：ユーザー名は変更できません。
- **Password**：ユーザーパスワードを変更または追加します。
- **Role**：一覧から、ユーザーの役割を選択します。
- **Membership**：一覧から、ユーザーを追加するグループを選択します。 ユーザーをグループから削除するには、グループ名の横にあるチェックボックスをオフにします。
- **User properties**：次のいずれかを行います。
  - 変更するユーザープロパティごとに、プロパティを選択して変更を加えます。 **[Done]** をクリックして変更した項目を保存するか、 **[Cancel]** をクリックして項目を変更せずそのままにします。
  - 追加するユーザープロパティごとに、 **[Add]** をクリックして以下の操作を行います。
    - **User Properties**：一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
    - **[Done]** をクリックしてユーザープロパティを保存するか、 **[Cancel]** をクリックして操作を取り消します。
  - 削除する既存のユーザープロパティごとに、プロパティが含まれる行の上にマウスポインターを置き、右側の［X］をクリックします。 プロパティがすぐに削除されます。

3. [**Save**] をクリックして変更を保存するか、 [**Cancel**] をクリックしてユーザーを変更せずそのままにします。

ローカルユーザーを削除するには

1. [**Users**] ページのユーザー一覧で、ユーザーをクリックして選択します。

   注：各ユーザーの横のチェックボックスをオンにして、削除するユーザーを複数選択できます。

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

3. [**Delete**] をクリックしてユーザーを削除するか、 [**Cancel**] をクリックして操作を取り消します。

ユーザーアカウントのインポート

Oct 25, 2016

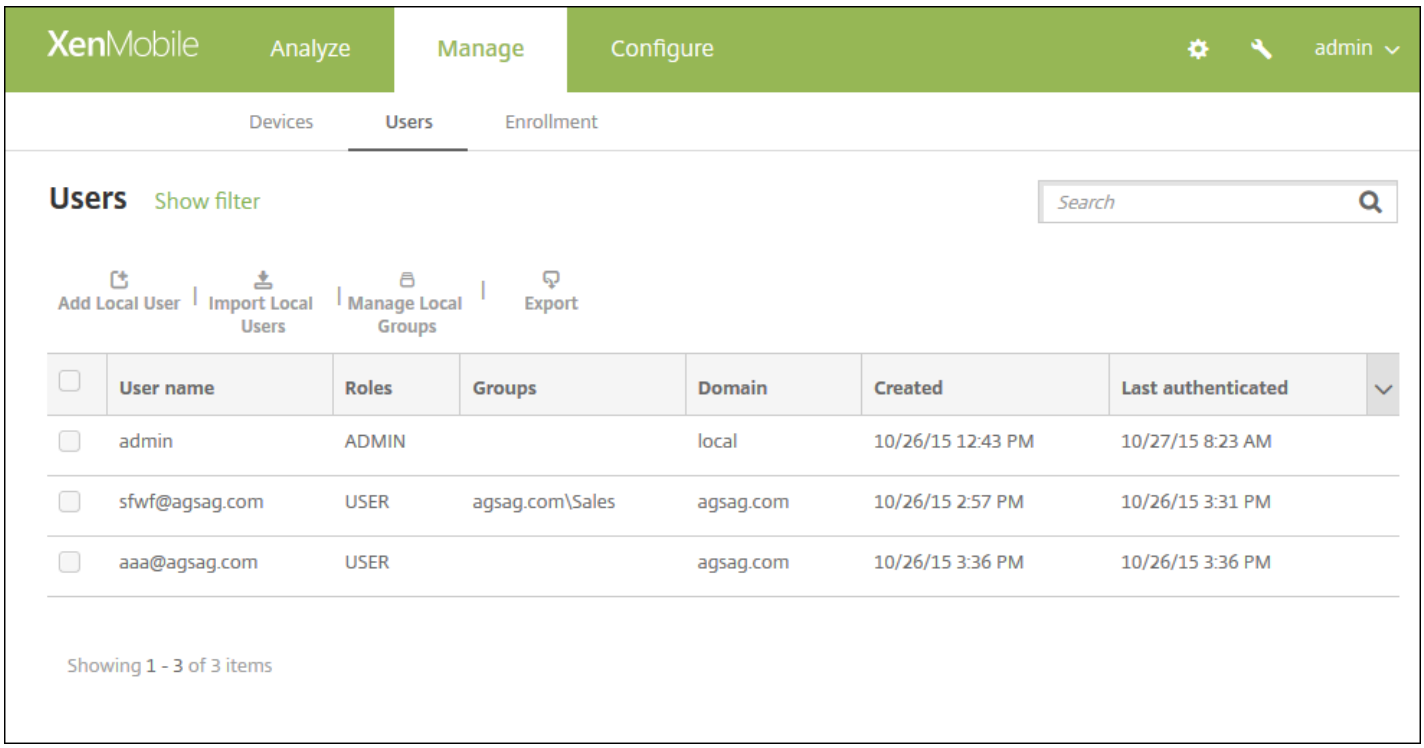
ユーザーアカウントやプロパティを、プロビジョニングファイルと呼ばれる.csvファイルからインポートできます。このファイルは手動で作成できます。 プロビジョニングファイルの形式について詳しくは、「プロビジョニングファイル形式」を参照してください。

注：

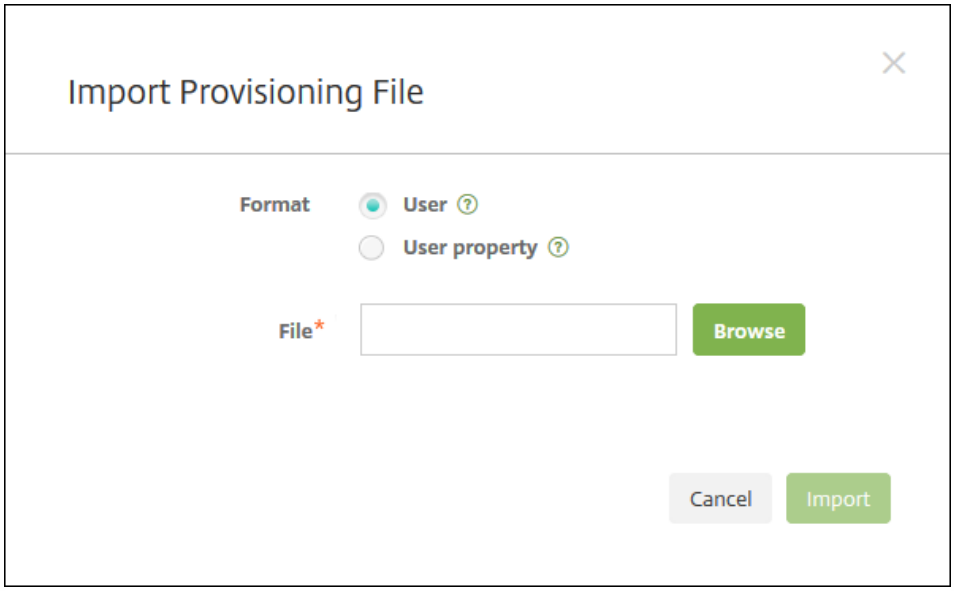
- LDAPディレクトリからユーザーをインポートする場合は、インポートファイルの中でユーザー名と共にドメイン名を使用します。 たとえば、username@domain.comのように指定します。 この構文を使用すると、インポートの速度が遅くなる余分なルックアップを行わずに済みます。
- XenMobileの内部ユーザーディレクトリにユーザーをインポートする場合は、インポートプロセスの速度を上げるため、デフォルトのドメインを無効にします。 内部ユーザーのインポートが完了した後で、デフォルトドメインを再び有効にできます。
- ローカルユーザーはユーザープリンシパル名（User Principal Name：UPN）形式で指定できますが、管理対象ドメインは使用しないことをお勧めします。たとえば、example.comが管理されている場合、このUPN形式のローカルユーザー「user@example.com」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後、以下の手順に従ってファイルをXenMobileにインポートします。

1. XenMobileコンソールで、［**Manage**］の［**Users**］をクリックします。 ［**Users**］ページが開きます。



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開きます。



3. インポートするプロビジョニングファイルの形式として、[**User**] または [**Property**] を選択します。

4. [**Browse**] をクリックして使用するプロビジョニングファイルの場所へ移動し、そのファイルを選択します。

5. [**Import**] をクリックします。

プロビジョニングファイル形式

Aug 30, 2016

手動で作成し、XenMobileへのユーザーアカウントとプロパティのインポートに使用するプロビジョニングファイルは、次のいずれかの形式である必要があります。

- ユーザープロビジョニングファイルのフィールド：user;passowrd;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では、フィールドをセミコロン（;）で区切ります。 フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。 たとえば、 プロパティ propertyV;test;1;2の場合、 プロビジョニングファイルには「propertyV\;test\;1\;2」と入力します。
- 役割として有効な値は、定義済みの役割のUSER、ADMIN、SUPPORT、DEVICE_PROVISIONINGのほか、自分で定義した追加の役割です。
- ピリオド文字（.）は、グループ階層を作成するための区切り文字として使用します。したがって、グループ名にピリオドを使用することはできません。
- 属性プロビジョニングファイル内のプロパティ属性は小文字にする必要があります。 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ファイルの内容例

エントリuser01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01の意味は以下のとおりです。

- 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「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ファイルの内容例

エントリuser01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 valueの意味は以下のとおりです。

- 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

グループの追加または削除

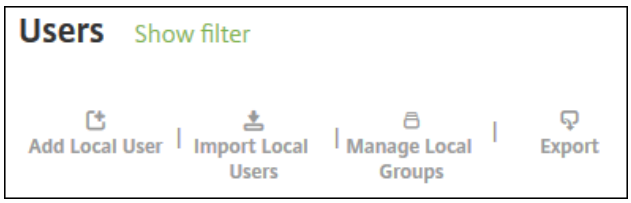
Aug 02, 2016

グループの管理は、XenMobileコンソールの［Manage Groups］ダイアログボックスで行います。このダイアログボックスは、［**Users**］ページ、［**Add Local User**］ページ、または［**Edit Local User**］からアクセスできます。 グループ編集コマンドはありません。 グループを削除する場合、グループを削除してもユーザーアカウントには影響しない点に注意してください。 グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。 また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリケーションやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。 ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

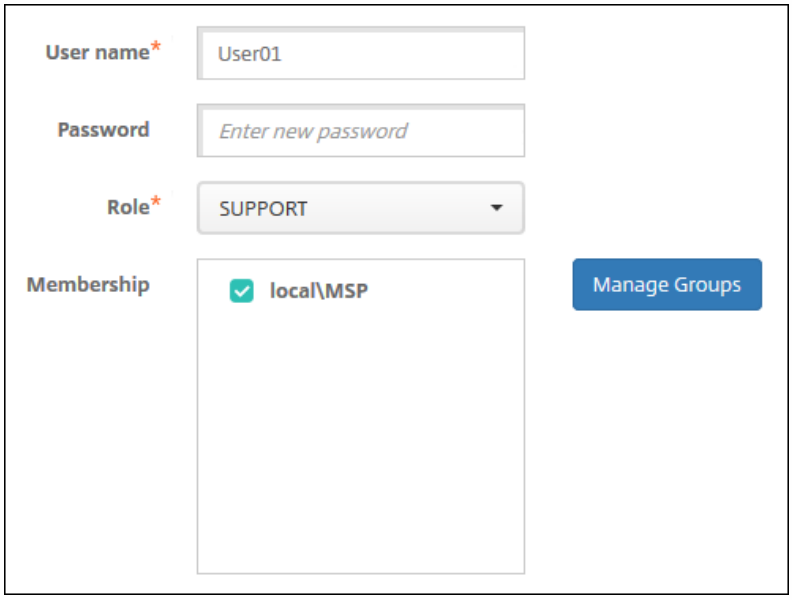
ローカルグループを追加するには

1. 次のいずれかを行います。

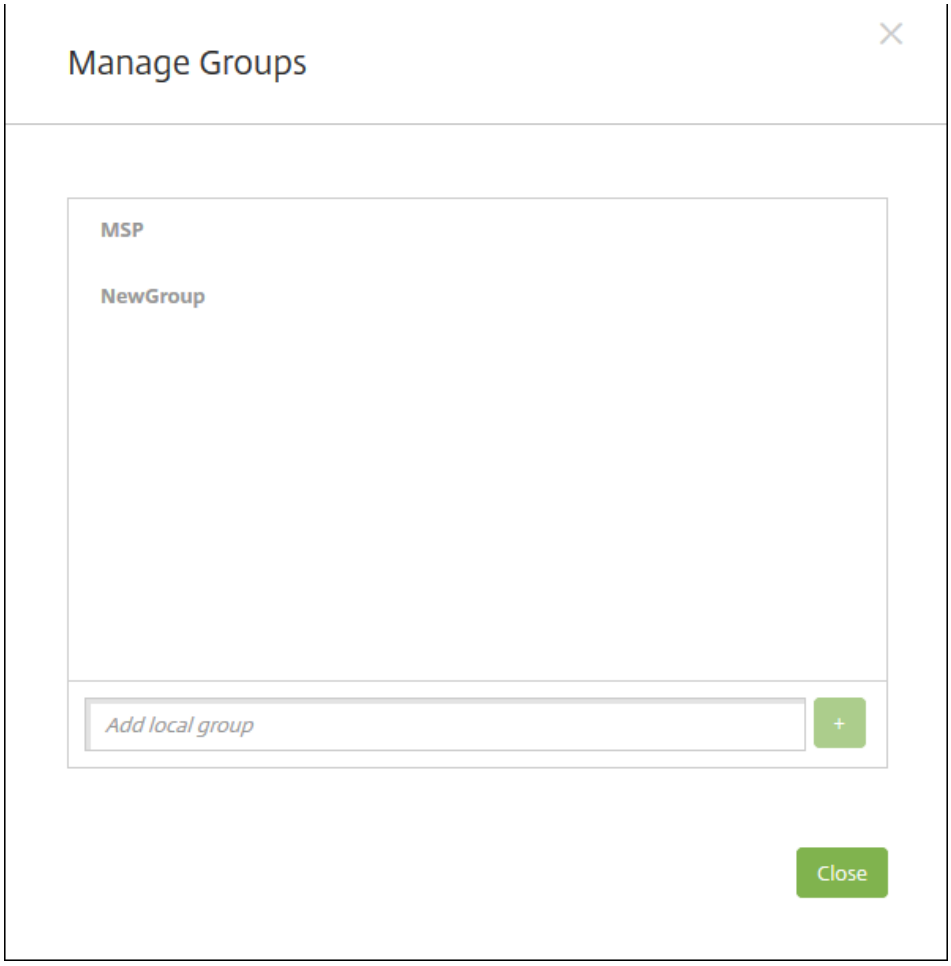
- ［**Users**］ページで、［**Manage Local Groups**］をクリックします。



- ［**Add Local User**］ページまたは［**Edit Local User**］ページで、［**Manage Groups**］をクリックします。



［**Manage Group**］ダイアログボックスが開きます。



2. グループの一覧の下で、新しいグループ名を入力してプラス記号（+）をクリックします。 ユーザーグループが一覧に追加されます。

3. **［Close］**をクリックします。

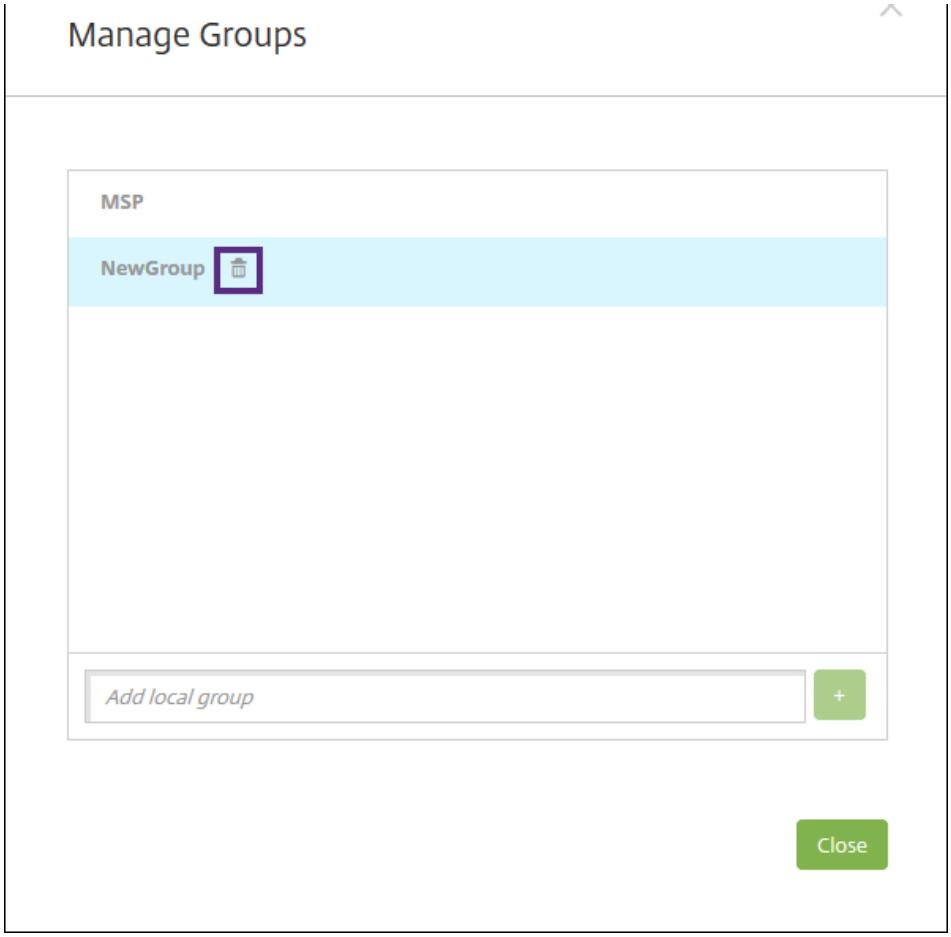
グループを削除するには

注：グループを削除してもユーザーアカウントには影響ありません。 グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。 また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリケーションやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。 ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

1. 次のいずれかを行います。

- ［Users］ページで、 **［Manage Local Groups］**をクリックします。
- **［Add Local User］**ページまたは **［Edit Local User］**ページで、 **［Manage Groups］**をクリックします。

［Manage Groups］ダイアログボックスが開きます。



2. ［**Manage Groups**］ダイアログボックスで、削除するグループを選択します。
3. グループ名の右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。
4. ［**Delete**］をクリックして操作を確認し、グループを削除します。

   重要：この操作を元に戻すことはできません。

5. ［**Manage Groups**］ダイアログボックスで、［**Close**］をクリックします。

RBACを使用した役割の構成

Oct 25, 2016

XenMobileの役割ベースのアクセス制御（Role-Based Access Control：RBAC）機能では、権限の定義済みセットである役割をユーザーとグループに割り当てることができます。 これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。

XenMobileには、システムの機能へのアクセスを論理的に区分するために、4つのデフォルトのユーザー役割が実装されています。

- **Administrator**。 システムへのフルアクセスが許可されます。
- **Device Provisioning**。 Windows CEデバイスで基本的なデバイス管理へのアクセスが許可されます。
- **Support**。 リモートサポートへのアクセスが許可されます。
- **User**。 デバイスを登録でき、Self Help Portalにアクセスできるユーザーが使用します。

デフォルトの役割をテンプレートとして使用することもできます。テンプレートをカスタマイズして、デフォルトの役割によって定義されている機能には含まれない特定のシステム機能にアクセスするための権限を持つ、新しいユーザーの役割を作成できます。

役割をローカルユーザーに（ユーザーレベルで）割り当てることや、Active Directoryグループに割り当てることができます（そのグループ内のすべてのユーザーが同じ権限を持ちます）。 ユーザーが複数のActive Directoryグループに属している場合は、すべての権限が統合されてそのユーザーの権限が定義されます。 たとえば、ADGroupAのユーザーがマネージャーのデバイスを検索でき、ADGroupBのユーザーが従業員のデバイスをワイプできる場合、両方のグループに属するユーザーは、マネージャーおよび従業員のデバイスを検索し、ワイプすることができます。

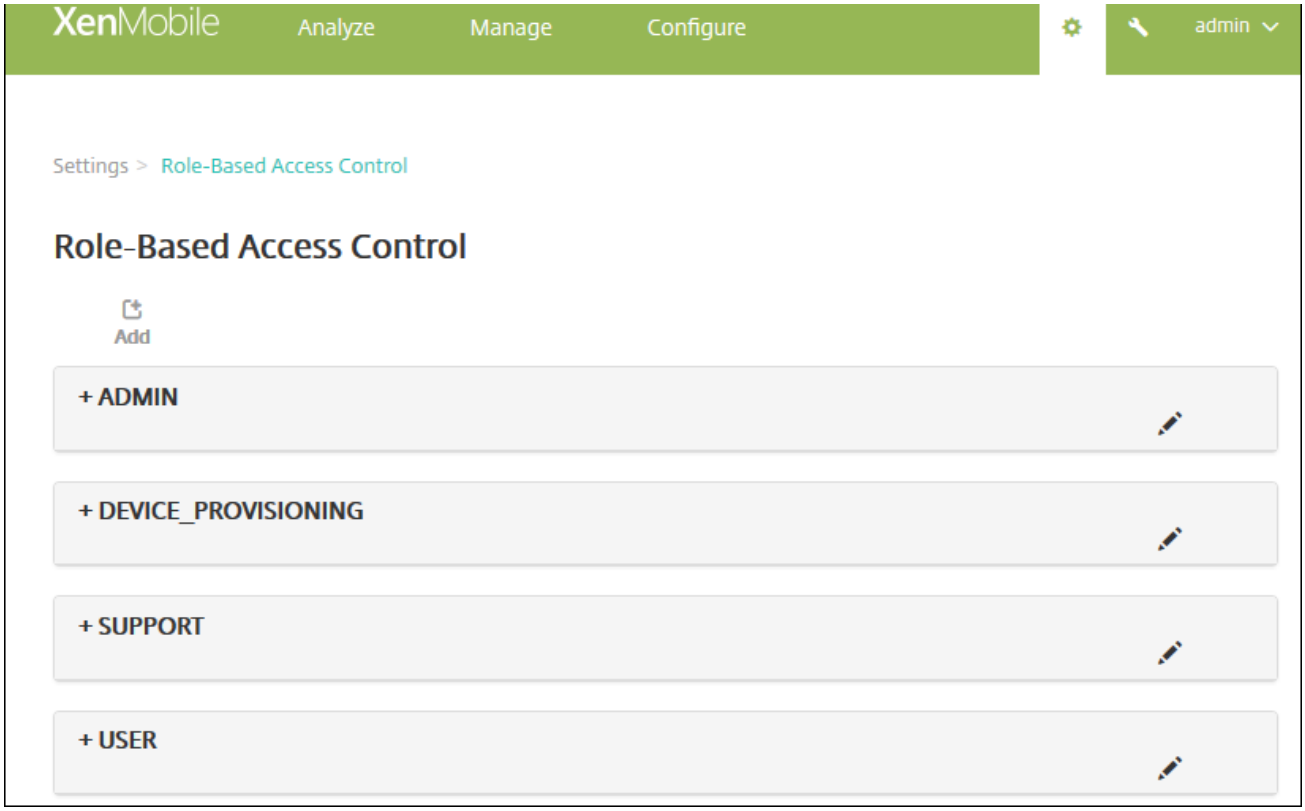
注：ローカルユーザーに割り当てることができる役割は1つだけです。

XenMobileのRBAC機能を使用すると、次のことを実行できます。

- 新しい役割を作成する。
- 役割にグループを追加する。
- ローカルユーザーを役割に関連付ける。

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

2. **[役割ベースのアクセス制御]** をクリックします。 **[役割ベースのアクセス制御]** ページが開き、4つのデフォルトのユーザー役割と、以前に追加した役割が表示されます。



役割の横のプラス記号（+）をクリックすると、次の図のように役割が展開され、その役割のすべての権限が表示されます。

3. **[Add]** をクリックして新しいユーザー役割を追加したり、既存の役割の右にあるペンアイコンをクリックして役割を編集したり、以前定義した役割の右にあるごみ箱アイコンをクリックして役割を削除したりします。 デフォルトのユーザー役割を削除することはできません。

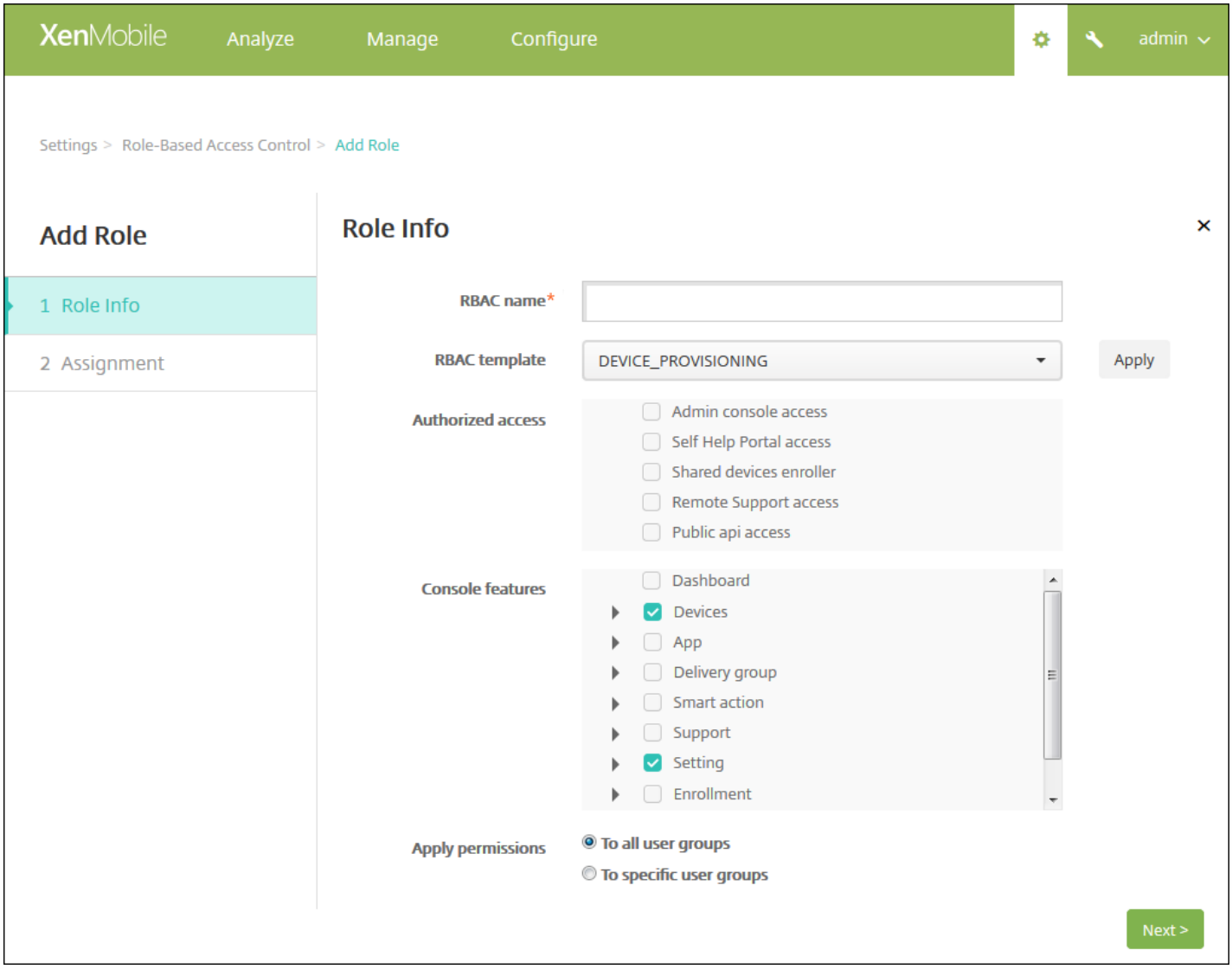
- **[Add]** またはペンアイコンをクリックすると、**[Add Role]** ページまたは **[Edit Role]** ページが開きます。
- ごみ箱アイコンをクリックすると、確認ダイアログボックスが開きます。 **[Delete]** をクリックすると、選択した役割が削除されます。

4. 新しいユーザー役割を作成するか、または既存のユーザー役割を編集するには、次の情報を入力します。

- **RBAC name**：新しいユーザー役割の説明的な名前を入力します。 既存の役割の名前は変更できません。
- **RBAC template**：任意で、新しい役割の開始点とするテンプレートを選択します。 既存の役割を編集する場合、テンプレートは選択できません。

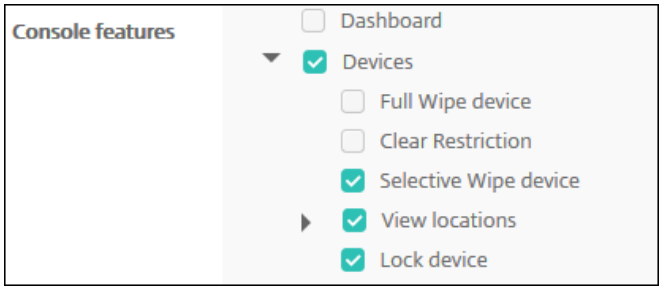
RBACテンプレートは、デフォルトのユーザー役割です。 RBACテンプレートによって、その役割に関連付けられているユーザーがシステムの機能に対して持つアクセス権を定義します。 RBACテンプレートを選択すると、 **[Authorized Access]** および **[Console Features]** フィールドで、その役割に関連付けられているすべての権限を参照できます。 テンプレートの使用はオプションです。 **[Authorized Access]** および **[Console Features]** フィールドで、役割に割り当てるオプションを直接選択することができます。

5. **[RBAC template]** フィールドの右にある **[Apply]** をクリックして、選択したテンプレートで定義されているアクセス権と機能権限を、 **[Authorized access]** および **[Console features]** にあるチェックボックスに反映させます。

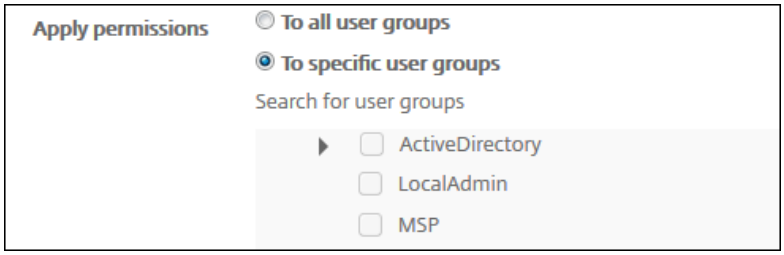


6. [**Authorized access**] および [**Console features**] にあるチェックボックスをオンまたはオフにして、役割をカスタマイズします。

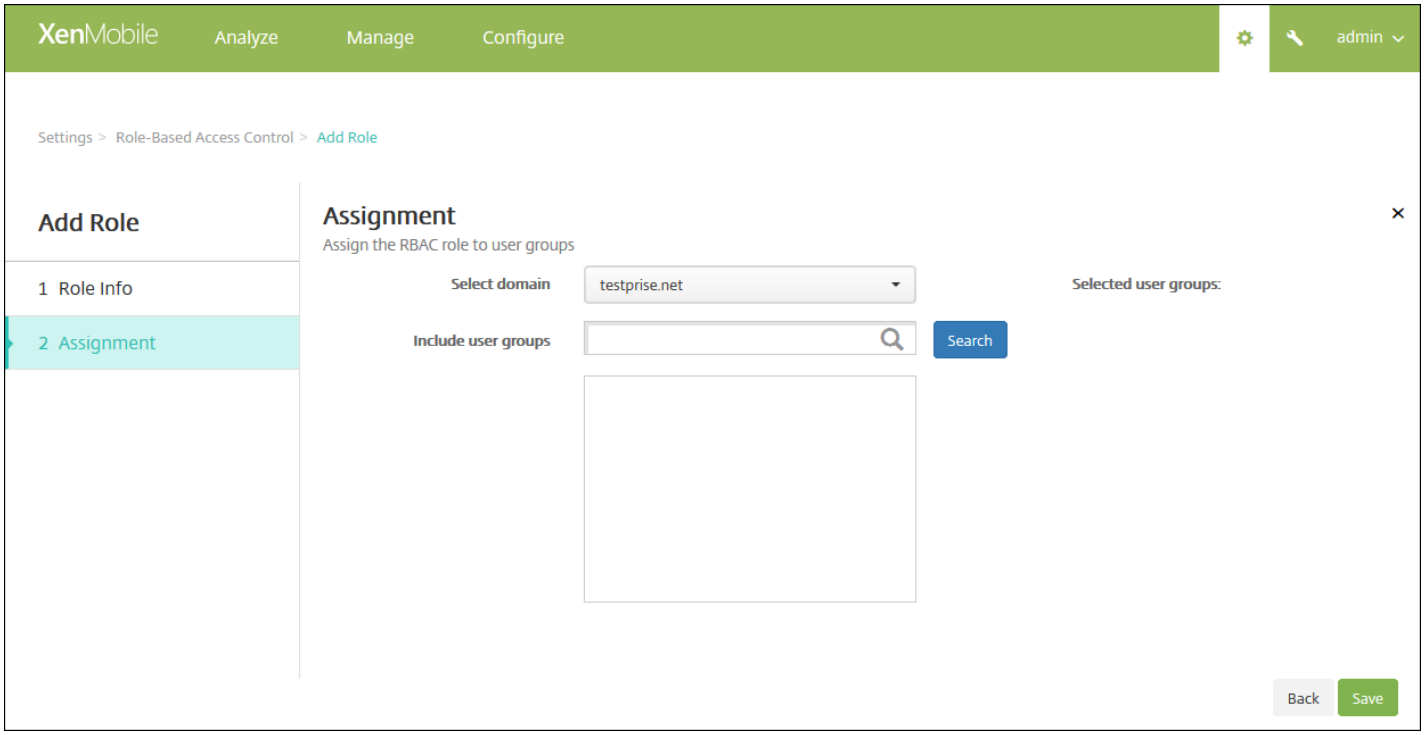
［Console feature］の横にある三角をクリックすると、その機能に固有の権限が表示され、オンまたはオフを選択できます。 最上位のチェックボックスをオンにすると、そのコンソール部分に対するアクセスを禁止できます。最上位レベルより下のオプションを有効にするには、それらのオプションを個別にオンにする必要があります。 次の図を例に取ると、ロールに割り当てられたユーザーのコンソールには、 [**Full Wipe device**] オプションおよび [**Clear Restrictions**] オプションは表示されませんが、チェックボックスがオンになっているオプションは表示されます。



7. **Apply permissions**：選択した権限を適用するグループを選択します。 [**To specific user groups**] をクリックするとグループの一覧が開き、1つまたは複数のグループを選択できます。

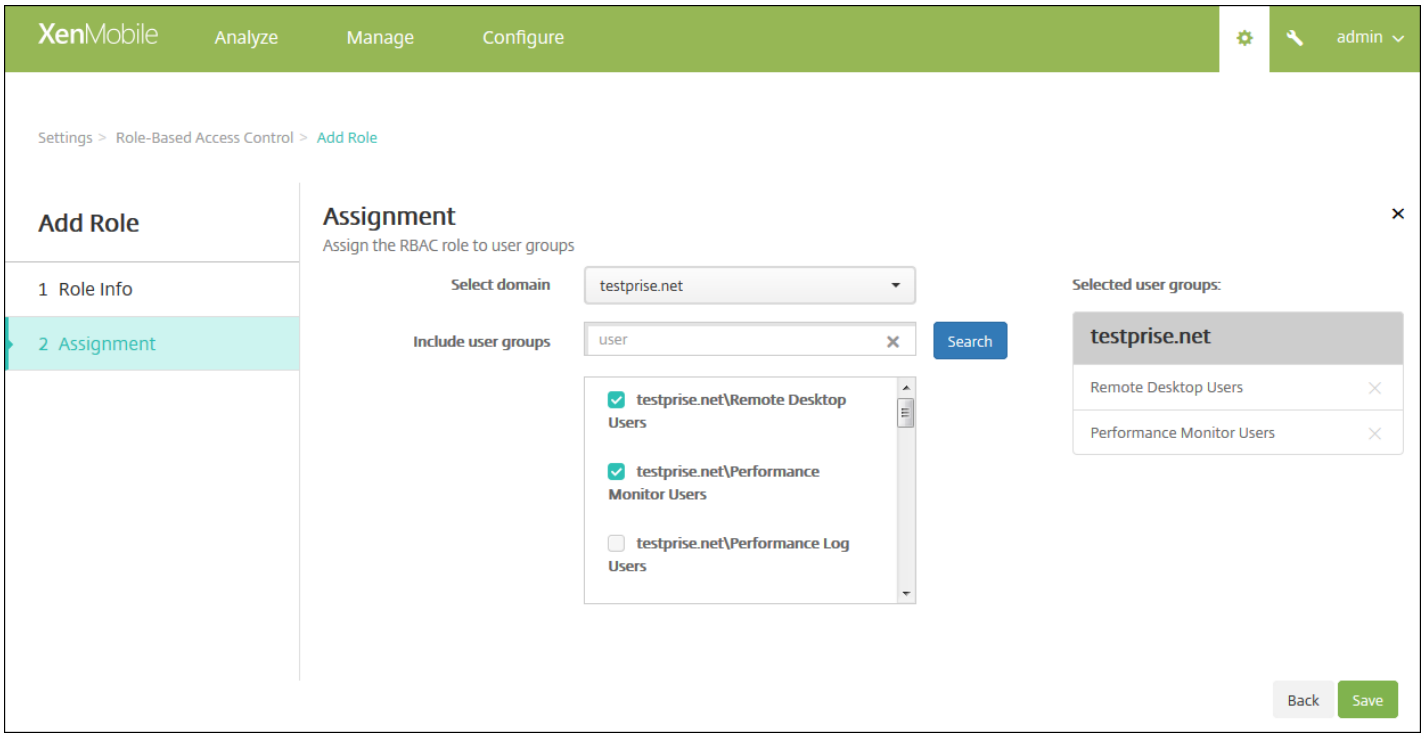


8. [**Next**] をクリックします。 [**Assignment**] ページが開きます。



9. ユーザーグループに役割を割り当てるための次の情報を入力します。

- **Select domain**：一覧から、ドメインを選択します。
- **Include user groups**： **[Search]** をクリックして使用可能なすべてのグループの一覧を表示するか、グループ名の全体または一部を入力してその名前を持つグループのみに一覧を絞り込みます。
- 表示された一覧で、役割を割り当てるユーザーグループを選択します。 ユーザーグループを選択すると、**[Selected user groups]** の一覧にグループが表示されます。



注：［**Selected user groups**］の一覧からユーザーグループを削除するには、ユーザーグループ名の横にある［X］をクリックします。

10. ［**Save**］をクリックします。

RBACの役割とアクセス権

Aug 30, 2016

定義済みの役割ベースのアクセス制御（Role-Based Access Control：RBAC）の各役割には、一定のアクセス権と機能権限が関連付けられています。 このトピックでは、これらの権限で実行できる内容について説明します。 組み込みの役割ごとのデフォルト権限に関する完全な一覧は、Role-Based Access Control Defaultsからダウンロードしてください。

RBACの役割を構成する方法については、「RBACを使用した役割の構成」を参照してください。

登録モードを構成してSelf Help Portalを有効化するには

Aug 02, 2016

デバイス登録モードを構成して、ユーザーがデバイスをXenMobileに登録できるようにします。 XenMobileには7つのモードがあり、それぞれに独自のセキュリティレベルと、ユーザーがデバイスを登録するときに行う必要がある手順があります。一部のモードはSelf Help Portalで使用可能にすることができます。ユーザーはSelf Help Portalにログオンして、デバイスを登録できる登録リンクを生成したり、登録招待状を自分に送信したりすることができます。

登録モードの構成は、XenMobileコンソールで［**Settings**］の［**Enrollment**］ページから行います。 登録招待状の送信は、XenMobileコンソールで［**Manage**］の［**Enrollment**］ページから行います（「XenMobileへのユーザーとデバイスの登録」を参照してください）。

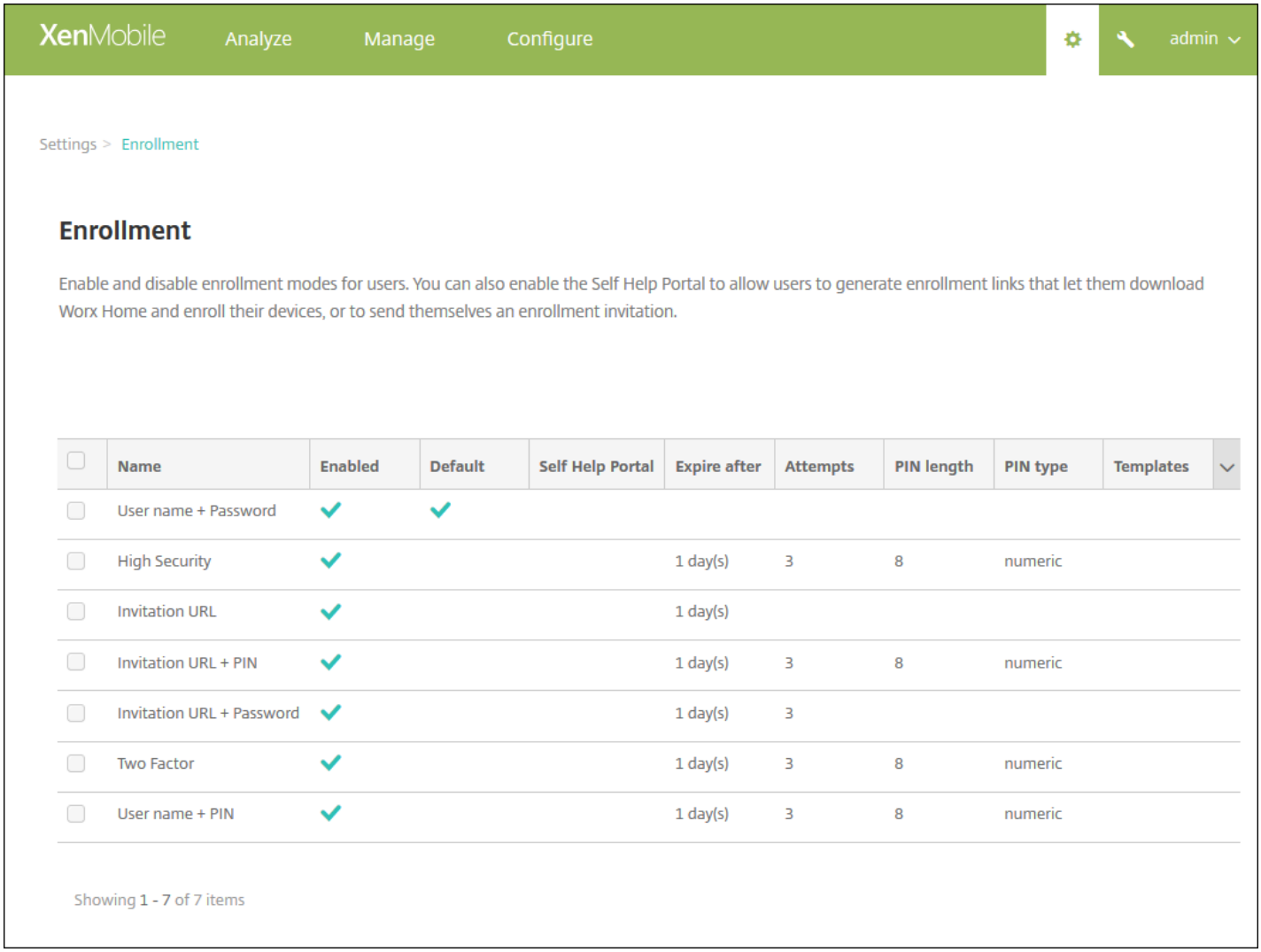
注：カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。 通知テンプレートについて詳しくは、「通知テンプレートの作成または更新」を参照してください。

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

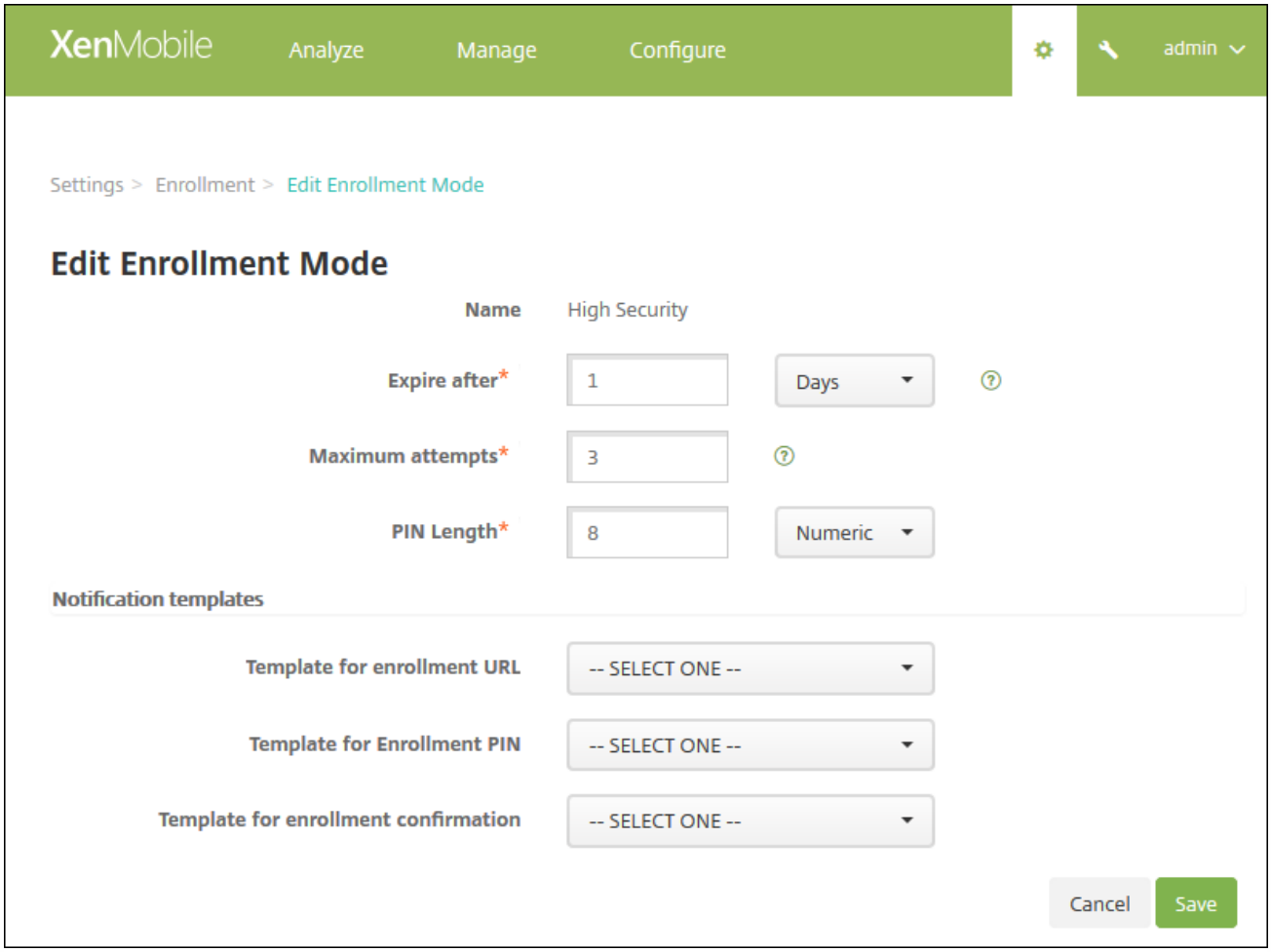
2. ［**Enrollment**］をクリックします。 ［**Enrollment**］ページが開き、すべての使用可能な登録モードの表が表示されます。デフォルトでは、すべての登録モードが有効です。

3. 一覧で登録モードを選択し、モードを編集してデフォルトに設定したり、モードを削除したり、ユーザーがSelf Help Portalからアクセスできるようにしたりします。

注：登録モードの横にあるチェックボックスをオンにすると、登録モード一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。



1. **[Enrollment]** の一覧で登録モードを選択し、[Edit] をクリックします。 **[Edit Enrollment Mode]** ページが開きます。 選択したモードによって、異なるオプションが表示される場合があります。



2. 必要に応じて以下の情報を変更します。

- **Expire after**： ユーザーがデバイスを登録できなくなる、有効期限を入力します。 この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。
  注：「0」を入力すると、招待状は期限切れになりません。

- **Days**：一覧から、 **[Expire after]** ボックスに入力した有効期限に応じて、 **[Days]** または **[Hours]** を選択します。
- **Maximum attempts**：登録処理からロックアウトされるまでにユーザーが実行できる登録の試行回数を入力します。 この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。
  注：「0」を入力すると、無制限に試行できます。

- **PIN length**：生成されるPINの桁数または文字数を入力します。
- **Numeric**：一覧から、PINの種類として、 **[Numeric]** または **[Alphanumeric]** を選択します。
- **Notification templates**：
  - **Template for enrollment URL**：一覧から、登録URLに使用するテンプレートを選択します。 たとえば、登録招待状テンプレートではテンプレートの構成方法に応じて、デバイスをXenMobileに登録できる電子メールまたはSMSをユーザーに送信します。 通知テンプレートについて詳しくは、「通知テンプレートおよび作成または更新」を参照してください。
  - **Template for enrollment PIN**：一覧から、登録PINに使用するテンプレートを選択します。
  - **Template for enrollment confirmation**：一覧から、登録が成功したことをユーザーに通知するときに使用するテンプレートを選択します。

3. [**Save**] をクリックします。

登録モードをデフォルトとして設定すると、別の登録モードを選択しない限り、そのモードがすべてのデバイス登録要求に対して使用されます。 デフォルトとして設定されている登録モードがない場合は、デバイス登録ごとに登録の要求を作成する必要があります。

注：デフォルトの登録モードとして設定できるのは、[**Username + Password**] 、 [**Two Factor**] 、 [**Username + PIN**] のいずれかのみです。
1. [**Username + Passwords**] 、 [**Two Factor**] 、 [**Username + PIN**] のいずれかを選択し、 デフォルトの 登録モードとして設定します。

注：デフォルトとして設定するには、選択したモードが有効化されている必要があります。
2. [**Default**] をクリックします。 これにより、選択したモードがデフォルトになります。 ほかの登録モードがデフォルトとして設定されていた場合、そのモードはデフォルトでなくなります。

登録モードを無効化すると、その登録モードは、グループ登録招待状でもSelf Help Portalでも使用できなくなります。 ある登録モードを無効化して別の登録モードを有効化することで、ユーザーがデバイスを登録できる方法を変更できます。

1. 登録モードを選択します。

注：デフォルトの登録モードは無効化できません。 デフォルトの登録モードを無効化するには、登録モードのデフォルト状態をまず解除する必要があります。
2. [**Disable**] をクリックします。 登録モードが有効でなくなります。

Self Help Portalで登録モードを有効化すると、ユーザーが個別にデバイスをXenMobileに登録できます。

注：

- Self Help Portalで登録モードを使用できるようにするには、登録が有効化され、通知テンプレートにバインドされている必要があります。
- Self Help Portalでは、登録モードを一度に1つのみ有効化できます。

1. 登録モードを選択します。

2. [**Self Help Portal**] をクリックします。 選択した登録モードをSelf Help Portalでユーザーが使用できるようになります。 Self Help Portalで既に有効化されていたモードがあった場合、ユーザーはそれを使用できなくなります。

XenMobileでのユーザー登録の自動検出の有効化

Aug 02, 2016

自動検出を使用するとユーザーの登録処理が簡単になります。 ネットワークユーザー名およびActive Directoryパスワードを使用してデバイスを登録することができます。併せてXenMobileサーバーについての詳細を入力する必要はありません。 ユーザーは、ユーザー名をユーザープリンシパル名（User Principal Name：UPN）形式で入力します（たとえば、user@mycompany.com）。

自動検出を有効化するには、AutoDiscoveryサービスポータル（https://xenmobiletools.citrix.com）にアクセスできます。 AutoDiscoveryサービスポータルについて詳しくは、「XenMobile AutoDiscovery Connectorサービス」を参照してください。

一部の限られた事例では、自動検出を有効化する場合にCitrixサポートへの連絡が必要な場合があります。 そうするために、以下の手順に従って展開の情報をCitrixテクニカルサポートチームに通知できます。また、Windowsデバイスの場合はSSL証明書も送信する必要があります。 Citrixでこの情報を受け取った後、ユーザーがデバイスを登録するときに、ドメイン情報が抽出されてサーバーアドレスにマップされます。 この情報はXenMobileデータベースで管理され、ユーザーが登録するときに常にアクセスして使用できます。

1. Autodiscoveryサービスポータル（https：//xenmobiletools.citrix.com）を使用して自動検出を有効化できない場合、Citrixサポートポータルでテクニカルサポートケースを開いて、以下の情報を提供してください。

- ユーザーが登録時に使用するアカウントを含むドメイン。
- XenMobileサーバーの完全修飾ドメイン名（FQDN）。
- XenMobileのインスタンス名。 デフォルトでは、インスタンス名はzdmであり、大文字と小文字が区別されます。
- ユーザーIDのタイプ。UPNまたはメールのいずれかにできます。 デフォルトでは、タイプはUPNです。
- デフォルトポート8443からポート番号を変更した場合は、iOS登録に使用されるポート。
- デフォルトポート443からポート番号を変更した場合は、XenMobileサーバーが接続を受け入れるポート。
- XenMobile管理者のメールアドレス（オプション）。

2. Windowsデバイスを登録する場合は、以下を実行します。

- enterpriseenrollment.mycompany.comの公式に署名された、非ワイルドカードSSL証明書を取得します。ここで、mycompany.comはユーザーが登録に使用するアカウントを含むドメインです。 要求に.pfx形式のSSL証明書とパスワードを添付します。
- DNSで正規名（CNAME）レコードを作成し、SSL証明書のアドレス（enterpriseenrollment.mycompany.com）をautodisc.zc.zenprise.comにマップします。ユーザーがWindowsデバイスを登録するときにUPNを使用する場合、XenMobileサーバーの詳細の入力だけでなく、Citrix登録サーバーはXenMobileサーバーの有効な証明書を要求するようにデバイスに指示します。

詳細情報および証明書（該当する場合）がCitrixサーバーに追加されると、テクニカルサポートケースが更新されます。 これで、ユーザーは自動検出による登録を開始できます。

注：複数のドメインを使用して登録する場合、マルチドメイン証明書を使用することもできます。 マルチドメイン証明書には、以下の構造が含まれている必要があります。

- 対応するプライマリドメインを指定する、SubjectDNおよびCN（たとえば、enterpriseenrollment.mycompany1.com）。
- 残りのドメインの適切なSAN（たとえば、enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.comなど）。

通知テンプレートの作成および更新

Aug 02, 2016

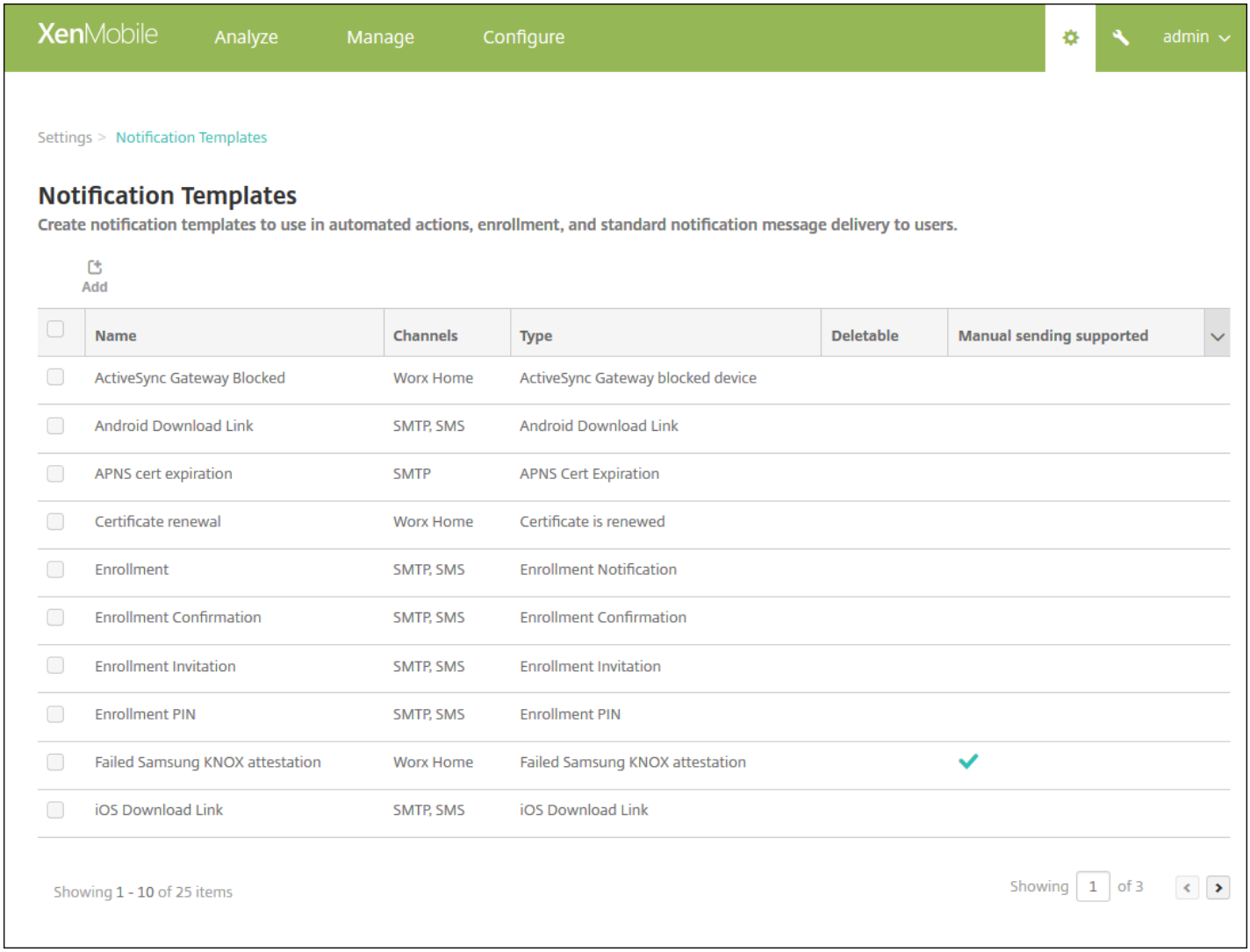
XenMobileで通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。 Worx Home、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。

XenMobileには、システム内のすべてのデバイスに対してXenMobileが自動的に応答する個別の種類のイベントを反映した、定義済みの通知テンプレートが多数用意されています。

注：SMTPまたはSMSチャネルを使用してユーザーに通知を送信する場合は、アクティブ化する前にチャネルを設定する必要があります。 通知テンプレートを追加するときにチャネルがまだ設定されていないと、チャネルを設定するよう求めるメッセージが表示されます。 詳しくは、「XenMobileでの通知」を参照してください。

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

2. **[Notification Templates]** をクリックします。 **[Notification Templates]** ページが開きます。



1. **[Add]** をクリックします。 SMSゲートウェイまたはSMTPサーバーが設定されていない場合、SMSおよびSMTP通知に関するメッセージが表示されます。 SMTPサーバーまたはSMSゲートウェイを今すぐ設定するか後で設定するかを選択できます。 **[Add Notification Template]** ページが開きます。

SMSまたはSMTPサーバーを今すぐ設定することを選択した場合は、**[Settings]** ページの **[Notification Server]** ページにリダイレクトされます。 使用するチャネルを設定した後、 **[Notification Template]** ページに戻って、通知テンプレートの追加または変更を続けることができます。

> ## Important
>
> SMSまたはSMTPサーバーの設定を後で行うことを選択した場合、通知テンプレートの追加または編集のときにこれらのチャネルをアクティブ化することはできません。つまり、ユーザー通知の送信にこれらのチャネルを使用することができません。

2. 次の設定を構成します。

- **Name**：テンプレートの説明的な名前を入力します。
- **Description**：テンプレートの説明を入力します。
- **Type**：一覧から、通知の種類を選択します。 選択した種類でサポートされるチャネルのみが表示されます。 定義済みテンプレートである［APNS Cert Expiration］テンプレートは1つだけ使用できます。 つまり、この種類の新しいテンプレートは追加できません。

注：テンプレートの種類の一部では、種類の下に *[Manual sending supported]* が表示されます。 これは、このテンプレートが **[Dashboard]** および **[Devices]** ページの **[Notifications]** 一覧に表示され、手動でユーザーに通知を送信できることを意味します。 いずれのチャネルの場合も、［Subject］フィールドまたは［Message］フィールドに以下のマクロが使われているテンプレートでは、手動送信は使用できません。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

3. **[Channels]** で、この通知で使用される各チャネルの情報を構成します。 一部またはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。

- **[Worx Home]** を選択した場合、iOSデバイスおよびAndroidデバイスのみが通知を受信し、通知はデバイスの通知トレイに表示されます。
- **[SMTP]** を選択した場合、ほとんどのユーザーはメールアドレスを使って登録するため、ほとんどのユーザーがメッセージを受信します。
- **SMS**を選択した場合、SIMカードが搭載されたデバイスのユーザーのみが通知を受信します。

Worx Home：

- **Activate**：クリックして通知チャネルを有効にします。
- **Message**：ユーザーに送信されるメッセージを入力します。 Worx Homeを使用する場合、このフィールドは必須です。
- **Sound File**：一覧から、ユーザーが通知を受信したときに再生される通知音を選択します。

SMTP：

- **Activate**：クリックして通知チャネルを有効にします。

  重要：SMTP通知は、SMTPサーバーが既に設定されている場合にのみ有効化できます。

- **Sender**：任意で、通知の送信者（名前、メールアドレス、またはその両方）を入力します。
- **Recipient**：このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMTP受信者アドレスに送信されるようにするためのマクロが事前設定されています。 テンプレートのマクロは変更しないでください。 アドレスをセミコロン（;）で区切って追加することにより、ユーザー以外の受信者（社内の管理者など）を追加することもできます。 アドホック通知を送信するには、このページで個別に受信者を入力するか、 **[Manage]** の **[Devices]** ページでデバイスを選択して、そこから通知を送信します。 詳しくは、「XenMobileでのデバイスの追加およびデバイスの詳細の表示」を参照してください。
- **Subject**：通知の説明的な件名を入力します。 このフィールドは必須です。
- **Message**：ユーザーに送信されるメッセージを入力します。

SMS：

- **Activate**：クリックして通知チャネルを有効にします。

  重要：SMS通知は、SMSゲートウェイが既に設定されている場合にのみ有効化できます。
- **Recipient**：このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMS受信者アドレスに送信されるようにするためのマクロが事前設定されています。 テンプレートのマクロは変更しないでください。 アドホック通知を送信するには、個別に受信者を入力するか、 **[Manage]** の **[Devices]** ページでデバイスを選択します。
- **Message**：ユーザーに送信されるメッセージを入力します。 このフィールドは必須です。

5. **[Add]** をクリックします。すべてのチャネルが正しく構成されている場合、 **[Notification Templates]** ページに、SMTP、SMS、Worx Homeの順に表示されます。 正しく構成されていないチャネルがあれば、正しく構成されているチャネルの後に表示されます。

1. 通知テンプレートを選択します。 選択したテンプレートに固有の編集ページが開き、**[Type]** フィールド以外のすべてを変更することができます。チャネルをアクティブ化または非アクティブ化することもできます。

2. **[Save]** をクリックします。

注：自分で追加した通知テンプレートのみを削除できます。定義済みの通知テンプレートは削除できません。

1. 既存の通知テンプレートを選択します。

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

2. **[Delete]** をクリックして通知テンプレートを削除するか、 **[Cancel]** をクリックして通知テンプレートの削除を取り消します。

デリバリーグループの管理

Aug 02, 2016

デバイスの構成および管理は、通常XenMobileでリソース（ポリシーおよびアプリケーション）および操作を作成し、デリバリーグループを使用してそれらをパッケージ化します。 XenMobileがリソースおよび操作をデリバリーグループでプッシュする順番は、*展開順*と呼ばれます。 このトピックでは、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のリソースや操作の展開順を変更する方法、ユーザーが複数のデリバリーグループに存在し、重複および競合するポリシーがある場合、XenMobileが展開順を決定する方法について説明します。

デリバリーグループによって、ポリシー、アプリケーション、アクションを組み合わせて展開する対象となるデバイスのユーザーのカテゴリを指定します。 通常、デリバリーグループへの追加は、ユーザーの会社、国、部門、オフィスの住所、役職などの特性に基づいて行われます。 デリバリーグループを使用することにより、どのユーザーがどのリソースをいつ取得するかを詳細に管理できます。 デリバリーグループは、全員に展開することや、より絞り込んで定義したユーザーグループに展開することができます

デリバリーグループへの展開とは、デリバリーグループに属するiOS、Windows Phone、Windowsタブレットデバイスを持つすべてのユーザーがXenMobileに再接続するようにプッシュ通知を送信することを意味します。これによってデバイスを再評価し、アプリケーション、ポリシー、アクションを展開できるようにします。そのほかのプラットフォームデバイスを持つユーザーは、接続済みの場合は直ちにリソースを受信します。接続済みでない場合は、スケジュール設定ポリシーに基づいて次に接続したときにリソースを受信します。

デフォルトのAllUsersデリバリーグループは、XenMobileをインストールして構成するときに作成されます。 このグループには、すべてのローカルユーザーとActive Directoryユーザーが含まれます。 AllUsersグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

展開順の作成

展開順はXenMobileがリソースをデバイスにプッシュする順番です。 展開順はXenMobileのMDMモードでのみサポートされます。

展開順を判断する際、XenMobileはポリシー、アプリ、操作、デリバリーグループにフィルターを適用して条件（展開規則、展開スケジュール）を制御します。 デリバリーグループを追加する前に、展開の目的に合わせてこのセクションの情報を参照してください。

以下は、展開順に関する主な概念の要約です。

- **展開順：**XenMobileがリソース（ポリシーやアプリ）および操作をデバイスにプッシュする順序です。 契約条件やソフトウェアインベントリのような一部のポリシーの展開順は、ほかのリソースに影響を与えません。 アクションが展開される順序はほかのリソースに影響を与えません。したがって、XenMobileでリソースが展開されるとき、リソースの位置は無視されます。
- **展開規則：** XenMobileは、展開規則によってデバイスプロパティを指定して、ポリシー、アプリ、操作、デリバリーグループをフィルター処理できます。 たとえば、ドメイン名が特定の値に一致した場合、展開規則が展開パッケージをプッシュするよう指定できます。
- **展開スケジュール：** XenMobileは、展開スケジュールを使用して、操作、アプリ、デバイスポリシーを指定し、これらのアイテムの展開を制御できます。 展開が即座に実行されるか、特定の日時に実行されるか、展開条件に従って実行されるかを指定できます。

以下の表は、特定のオブジェクトまたはリソースに関連付けてこれらをフィルター処理したり、これらの展開を制御するさまざまな条件です

オブジェクト/リソース	フィルター/制御条件
デバイスポリシー	デバイスのプラットフォーム デバイスプロパティに基づく展開規則 展開スケジュール
アプリ	デバイスのプラットフォーム デバイスプロパティに基づく展開規則 展開スケジュール
操作	デバイスプロパティに基づく展開規則 展開スケジュール
デリバリーグループ	ユーザー/グループ デバイスプロパティに基づく展開規則

通常の環境では、複数のデリバリーグループが単一ユーザーに割り当てられ、次のような状況が発生する可能性があります。

- デリバリーグループ内に重複したオブジェクトが存在する。
- 1つ以上のデリバリーグループが単一ユーザーに割り当てられることによって、特定のポリシーに異なる構成が存在する。

このような状況が発生した場合、XenMobileは、デバイスに配布し実行するすべてのオブジェクトの展開順を計算します。 計算の手順はデバイスプラットフォームに共通です。

計算の手順：

1. ユーザーやグループのフィルターおよび展開規則に基づいて、特定のユーザーが存在するすべてのデリバリーグループを判断します。
2. 選択されたデリバリーグループ内で、デバイスプラットフォーム、展開規則、展開スケジュールのフィルターが適用されるすべてのリソース（ポリシー、操作、アプリ）の順序一覧を作成します。 順序のアルゴリズムは、次のとおりです。

    a. ユーザー定義の展開順があるデリバリーグループのリソースを、展開順がないデリバリーグループの前に配置します。 こうする理由は、これらの手順の後に説明します。

    b. 同じ条件のデリバリーグループの中から、デリバリーグループ名に従ってリソースを順序付けします。 たとえば、デリバリーグループAのリソースをデリバリーグループBの前に配置します。

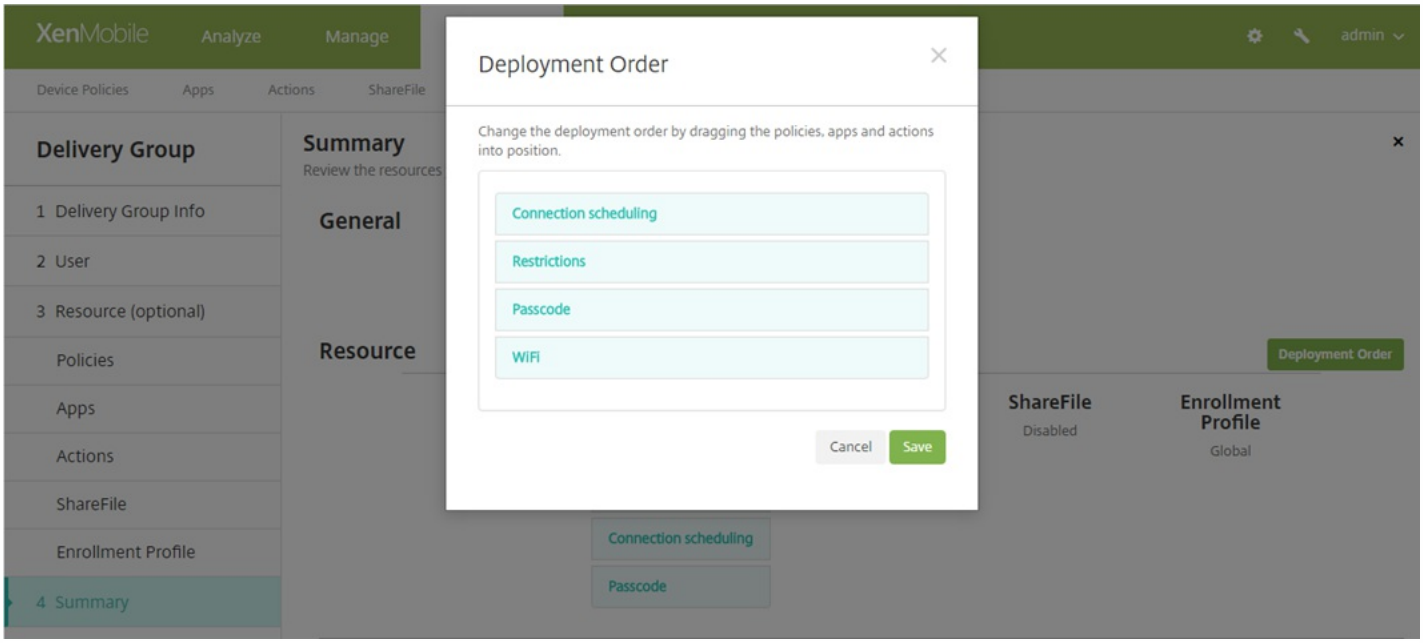
    c. 並べ替え中、デリバリーグループのリソースにユーザー定義の展開順が指定されている場合、その順序を保持します。 そうでない場合は、デリバリーグループ内でリソースをリソース名で並べ替えることができます。

d. 同じリソースが複数回表示される場合、重複するリソースを削除します。

リソースに関連したユーザー定義の順序を持つリソースを、ユーザー定義の順序のないリソースの前に展開します。 リソース
は、ユーザーに割り当てられた複数のデリバリーグループに存在する可能性があります。 上記の手順で示されたように、計算
のアルゴリズムは余分なリソースを削除し、この一覧の最初のリソースのみを配布します。 この方法で重複するリソースを削
除することによって、XenMobile管理者が定義する順序をXenMobileに適用します。

たとえば、次のような2つのデリバリーグループがあるとします。

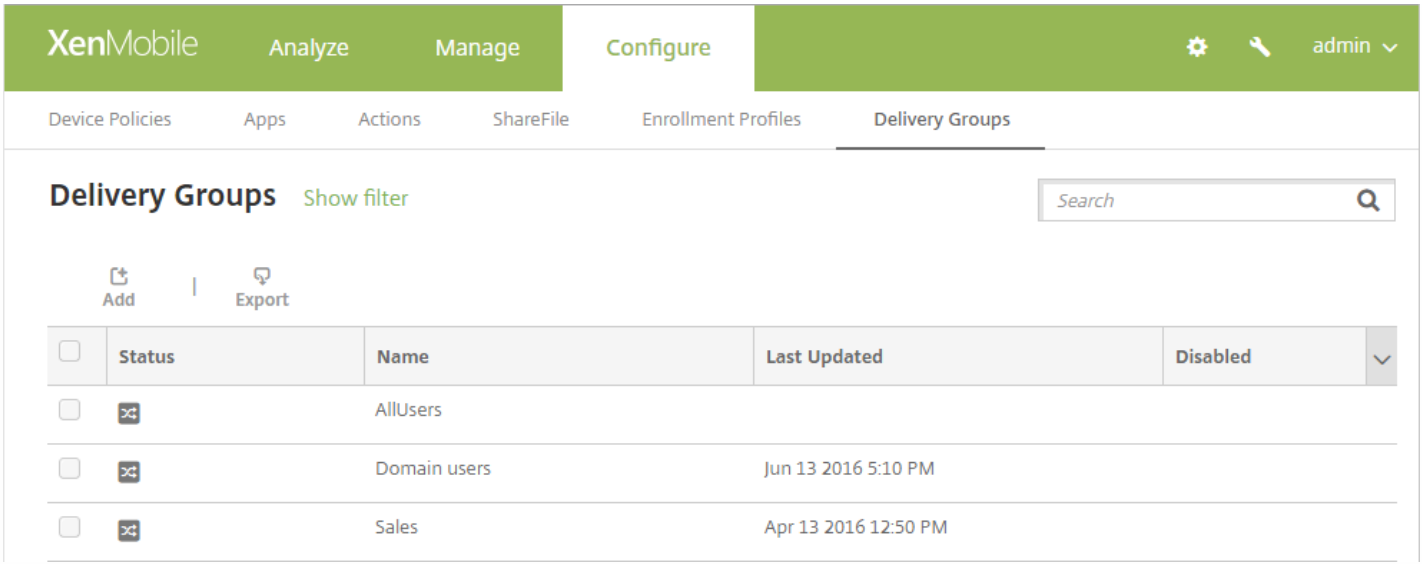
- デリバリーグループ「Account Manager 1」：リソース順序は [**unspecified**] 。ポリシー**WiFi**および**Passcode**を含みます。
- デリバリーグループ「Account Manager 2」：リソース順序は [**specified**] 、ポリシー**Connection scheduling**、**Restrictions**、**Passcode**および**WiFi**を含みます。 この事例では、**WiFi**ポリシーの前に**Passcode**ポリシーを配信するように指定されます。



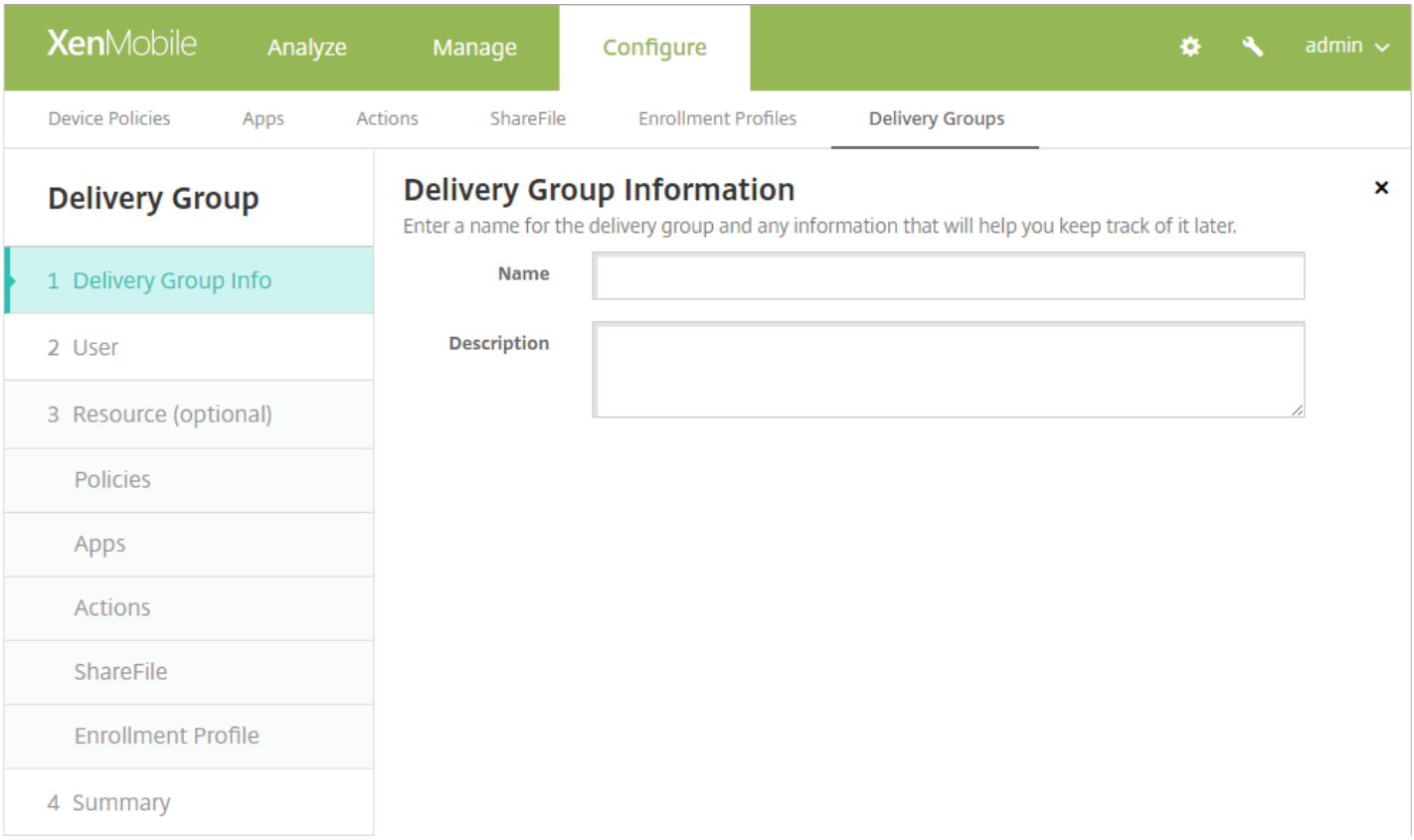
計算アルゴリズムが名前のみを基準に展開グループを順序づけた場合、XenMobileはデリバリーグループAccount Manager 1から開始して、この順序で展開を実行します：**WiFi**、**Passcode**、**Connection scheduling**および**Restrictions**。 XenMobileは、Account Manager 2デリバリーグループの重複する**Passcode**および**WiFi**を無視します。

ただし、Account Manager 2グループには管理者が指定した展開順序があるため、計算アルゴリズムは、Account Manager 2デリバリーグループからのリソースを、Account Manager 1デリバリーグループからのものより一覧で上位に配置します。 その結果、XenMobileはこの順序でポリシーをデプロイします：**Connection scheduling**、**Restrictions**、**Passcode**、および**WiFi**。 XenMobileは、Account Manager 1デリバリーグループからのポリシー**WiFi**および**Passcode**を無視します。重複しているためです。 このアルゴリズムは、XenMobile管理者によって指定された順序を優先します。

1. XenMobileコンソールで、 **[構成]** 、 **[デリバリー グループ]** の順にクリックすると、 **[デリバリー グループ]** ページが表示されます。



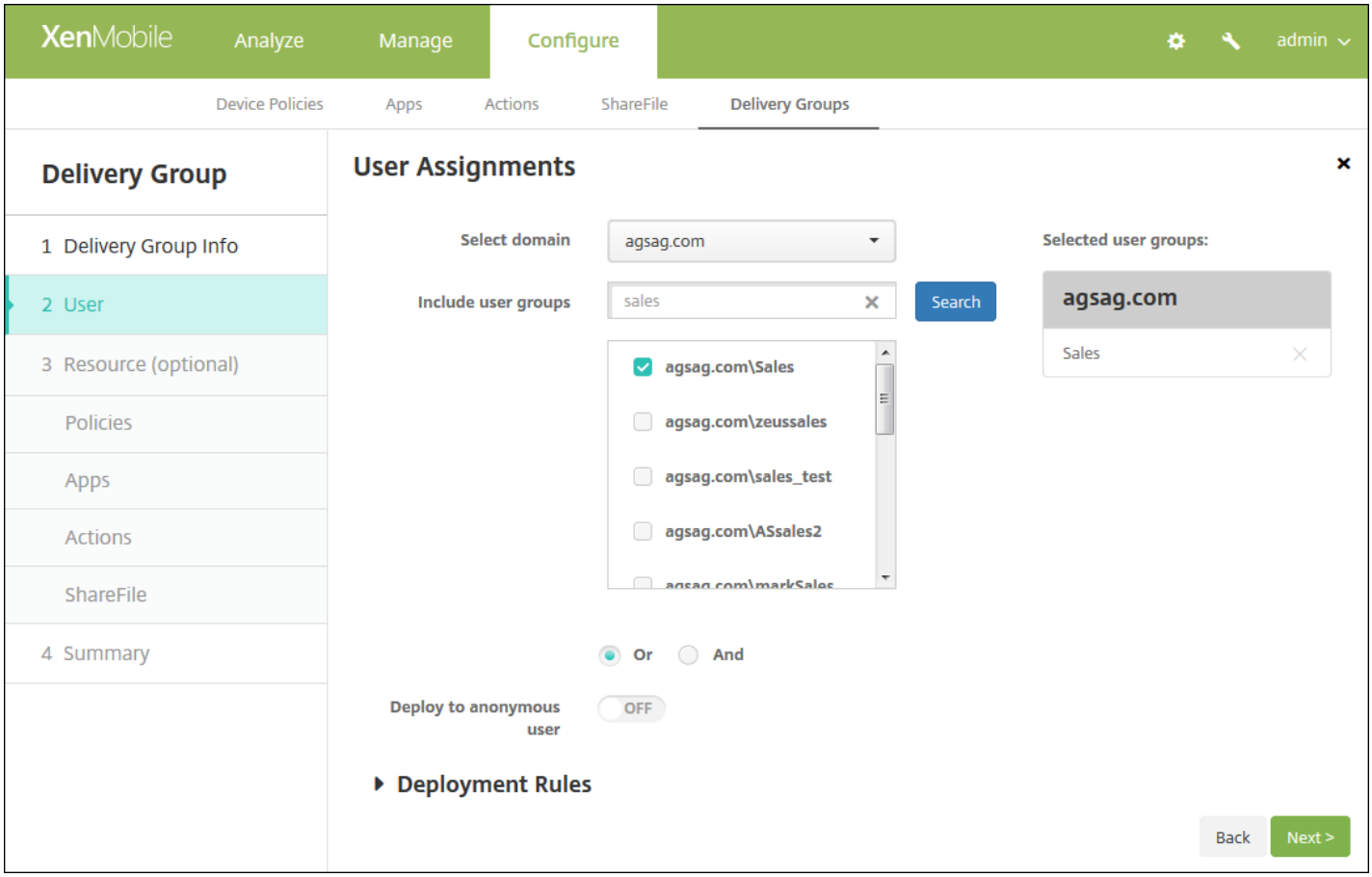
2. **[デリバリー グループ]** ページで、 **[追加]** をクリックすると、 **[デリバリー グループ情報]** ページが表示されます。



3. **[デリバリー グループ情報]** ページで、以下の情報を入力します。

- **Name**：デリバリーグループの説明的な名前を入力します。
- **Description**：任意で、デリバリーグループの説明を入力します。

4. **[次へ]** をクリックすると、 **[ユーザー割り当て]** ページが表示されます。



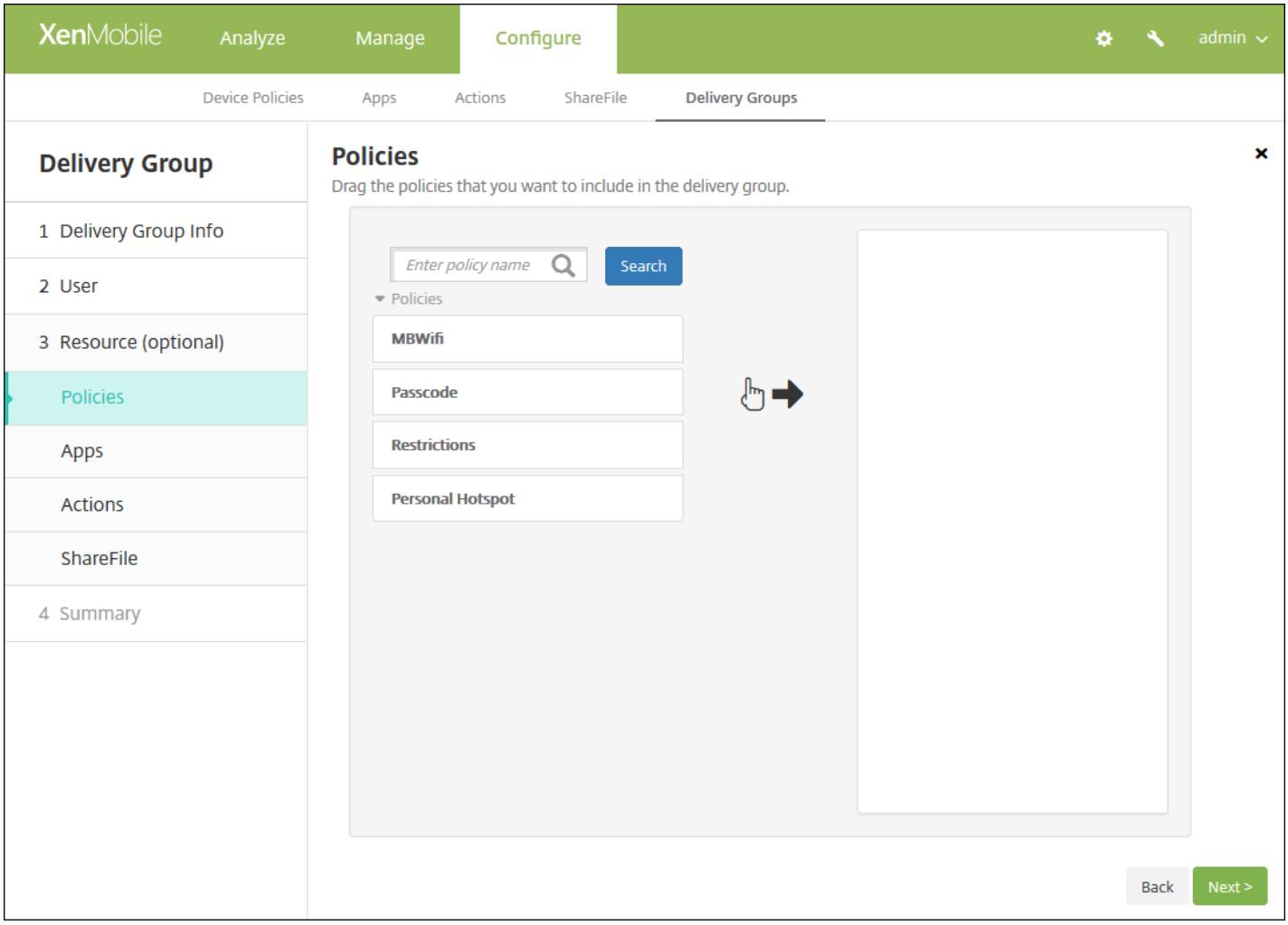
5. 次の設定を構成します。

- **Select domain**：一覧から、ユーザーを選択するドメインを選択します。
- **Include user groups**：次のいずれかを行います。
  - ユーザーグループの一覧で、追加するグループを選択すると、 選択されたグループが **[選択したユーザー グループ]** 一覧に表示されます。
  - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - グループ名の全体または一部を検索ボックスに入力して **[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。
    - **[選択したユーザー グループ]** の一覧からユーザーグループを削除するには、次のいずれかを行います。
      - **[選択したユーザー グループ]** の一覧で、削除する各グループの横にある **[X]** をクリックします。
      - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。 一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
      - グループ名の全体または一部を検索ボックスに入力して **[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。 一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
- **Or/And**：リソースが展開されるユーザーがいずれかのグループに属していればよいか（ [Or] ）、すべてのグループに属している必要があるか（ [And] ）を選択します。
- **匿名ユーザーに 展開**：デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。

  注：認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

任意のリソースをデリバリーグループに追加して、特定のポリシーを追加したり、必須および任意のアプリケーションを提供したり、自動アクションを追加したり、コンテンツおよびデータへのシングルサインオンに対してShareFileを有効にしたりすることができます。 次のセクションでは、ポリシー、アプリケーション、アクションを追加する方法と、ShareFileを有効にする方法について説明します。 デリバリーグループには、これらのリソースの一部またはすべてを追加できます。また、何も追加しないでおくこともできます。 あるリソースの追加をスキップするには、追加するリソースを選択するか、 **[Summary]** をクリックしてリソースの追加を省略します。

ポリシーの追加



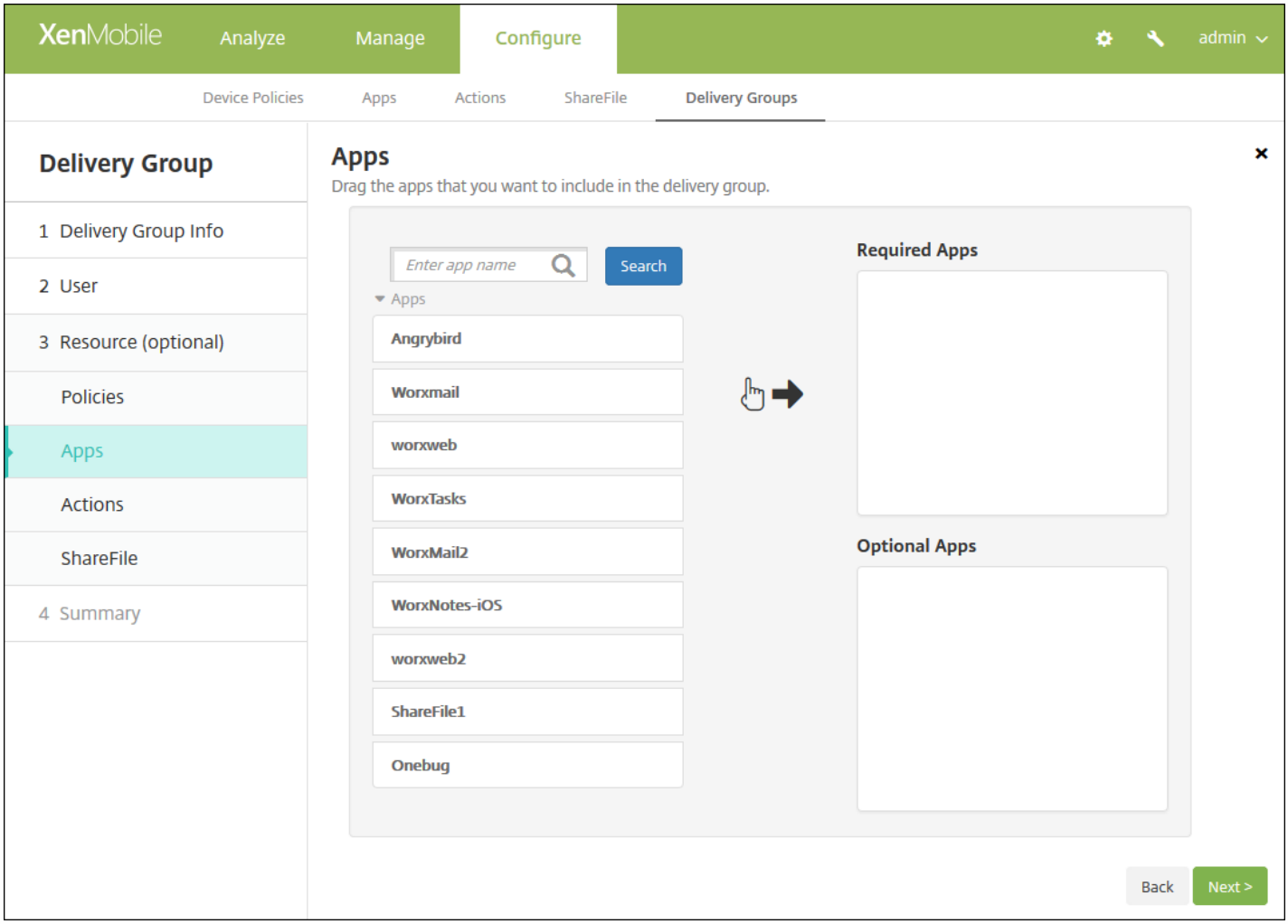
1. 追加するポリシーごとに、以下の操作を行います。

- 使用可能なポリシーの一覧をスクロールして、追加するポリシーを見つけます。
- または、ポリシーの一覧を絞り込むため、検索ボックスにポリシー名の全体または一部を入力して **[Search]** をクリックします。
- 追加するポリシーをクリックして、右側のボックス内へドラッグします。

注：ポリシーを削除するには、右側のボックス内のポリシー名の横にある **[X]** をクリックします。

2. **[Next]** をクリックします。 **[Apps]** ページが開きます。

アプリケーションの追加



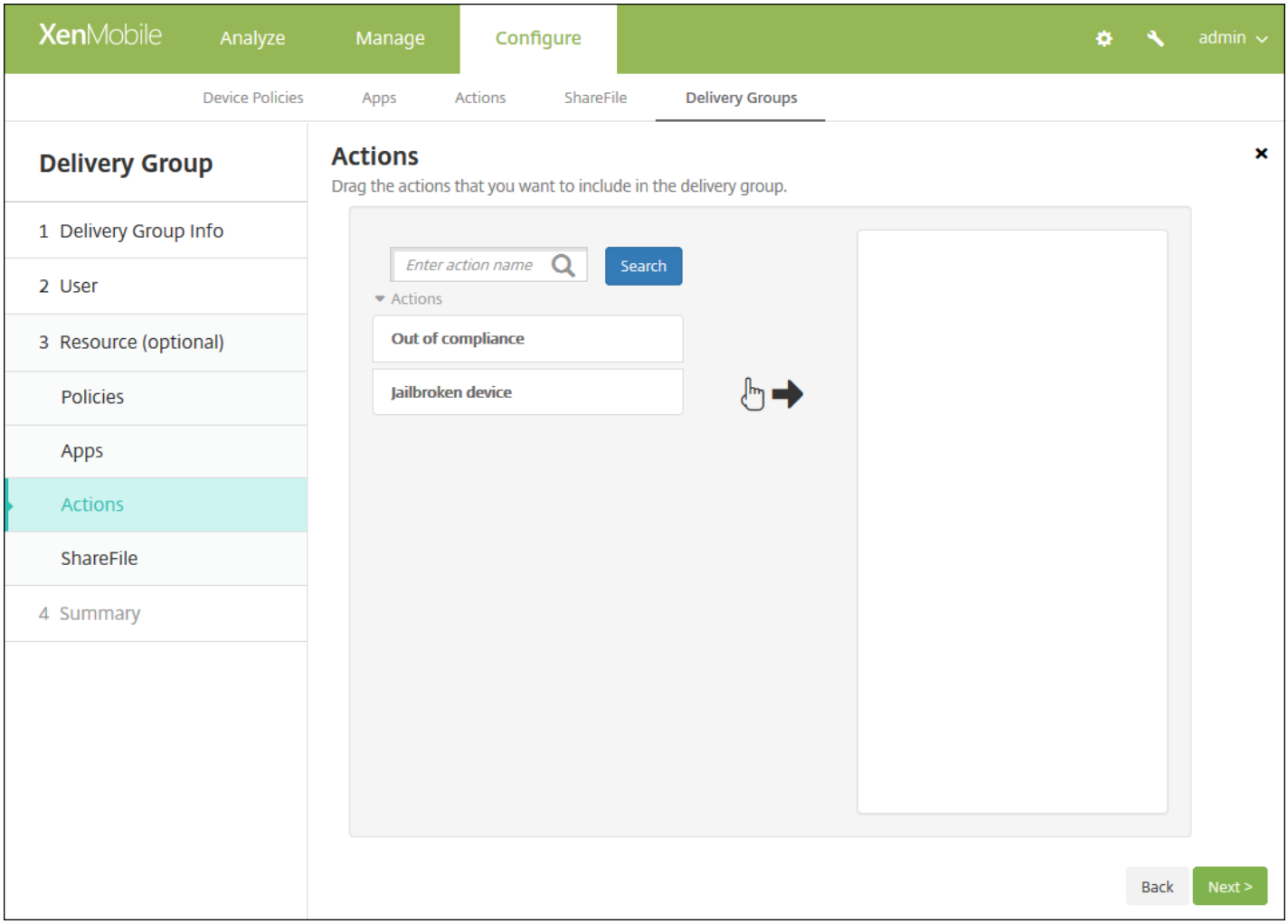
1. 追加するアプリケーションごとに、以下の操作を行います。

- 使用可能なアプリケーションの一覧をスクロールして、追加するアプリケーションを見つけます。
- または、アプリケーションの一覧を絞り込むため、検索ボックスにアプリケーション名の全体または一部を入力して［**Search**］をクリックします。
- 追加するアプリケーションをクリックして、［**Required Apps**］ボックス内または［**Optional Apps**］ボックス内へドラッグします。

注：アプリケーションを削除するには、右側のボックス内のアプリケーション名の横にある［**X**］をクリックします。

2. ［**Next**］をクリックします。［**Actions**］ページが開きます。

アクションの追加



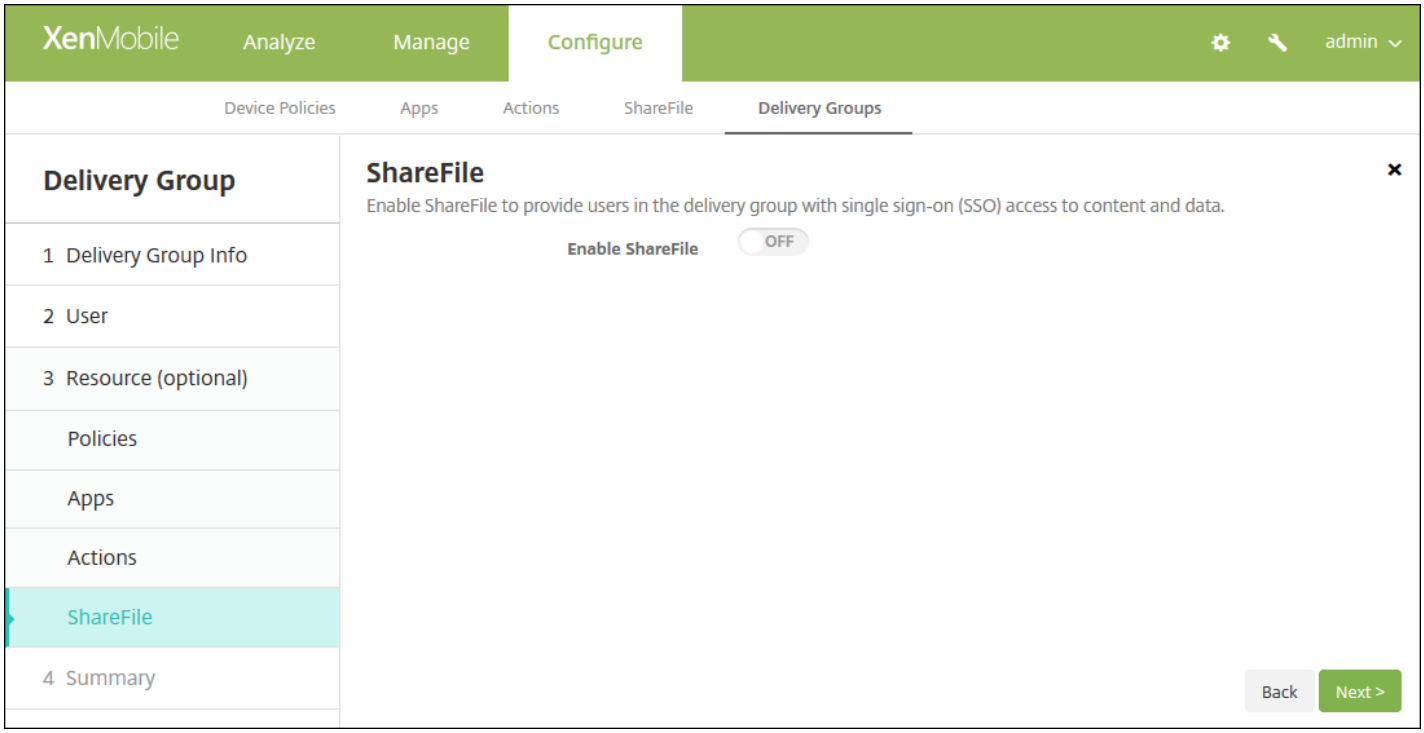
1. 追加する アクション ごとに、以下の操作を行います。

- 使用可能なポリシーの一覧をスクロールして、追加するアクションを見つけます。
- または、アクションの一覧を絞り込むため、検索ボックスにアクション名の全体または一部を入力して[**Search**]をクリックします。
- 追加するアクションをクリックして、右側のボックス内へドラッグします。

注：アクションを削除するには、右側のボックス内のアクション名の横にある[**X**]をクリックします。

2. [**Next**]をクリックします。 [**ShareFile**]ページが開きます。

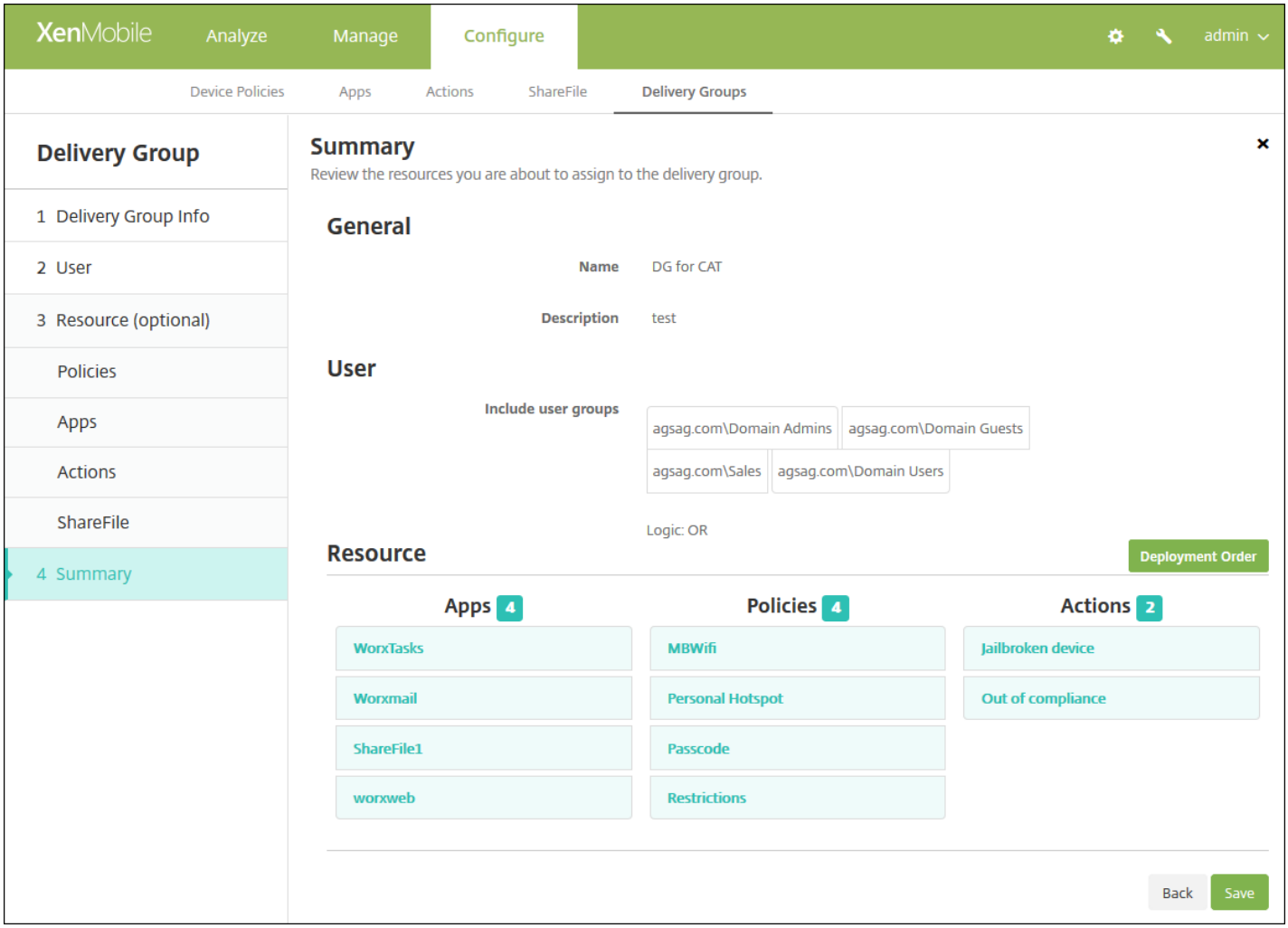
Enable ShareFile



1. 次の設定を構成します。

- **Enable ShareFile**： [**ON**] を選択して、コンテンツおよびデータへのShareFileシングルサインオンアクセスを有効にします。

2. [**Next**] をクリックします。 [**Summay**] ページが開きます。



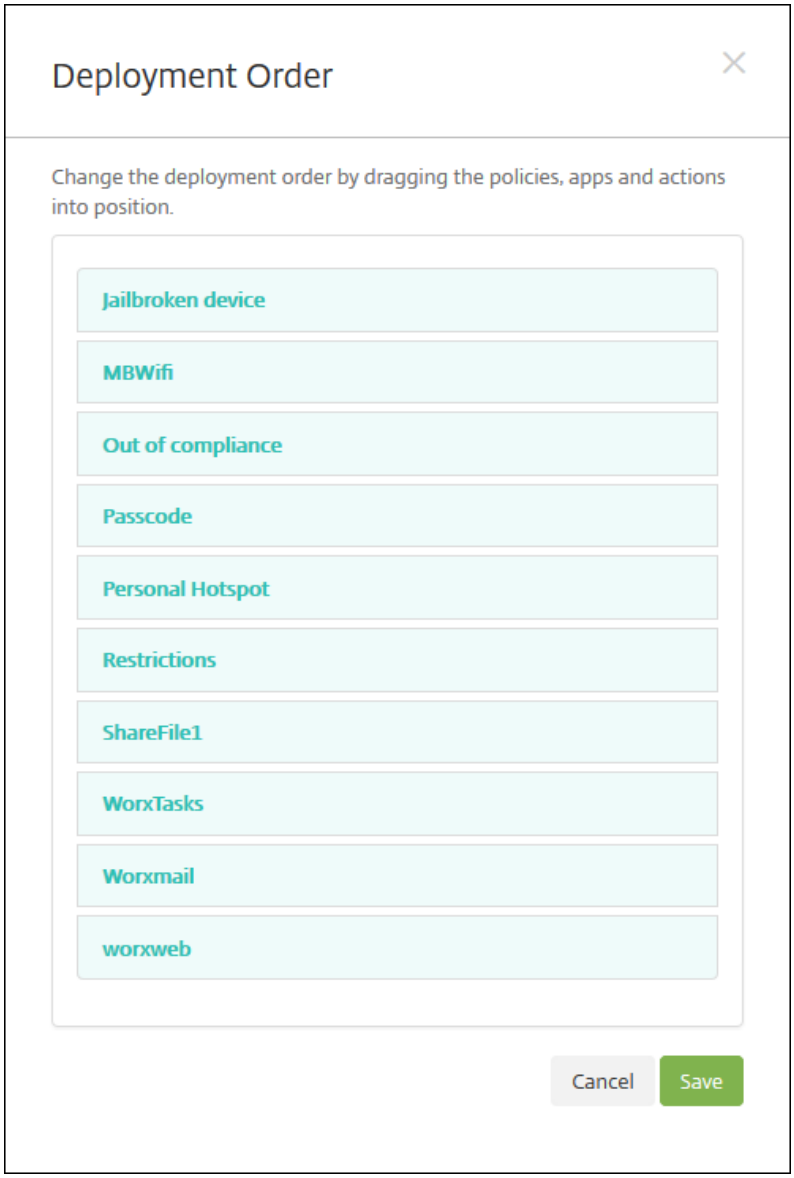
［**概要**］ ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。［Summary］ページには、リソースがカテゴリ別に表示されます。展開順序を反映してはいません。

1. 構成の調整が必要な場合は、 ［**戻る**］ をクリックして前のページに戻ります。

2. 展開順序を表示するか、展開順序を並べ替えるには、［**Deployment Order**］をクリックします。

3. ［**Save**］をクリックして、デリバリーグループを保存します。

1. ［**Deployment Order**］をクリックします。 ［**Deployment Order**］ダイアログボックスが開きます。



2. リソースをクリックして展開する場所にドラッグします。 展開順序を変更すると、一覧の上から下への順にリソースが展開されます。

3. [**Save**] をクリックして、展開順序を保存します。

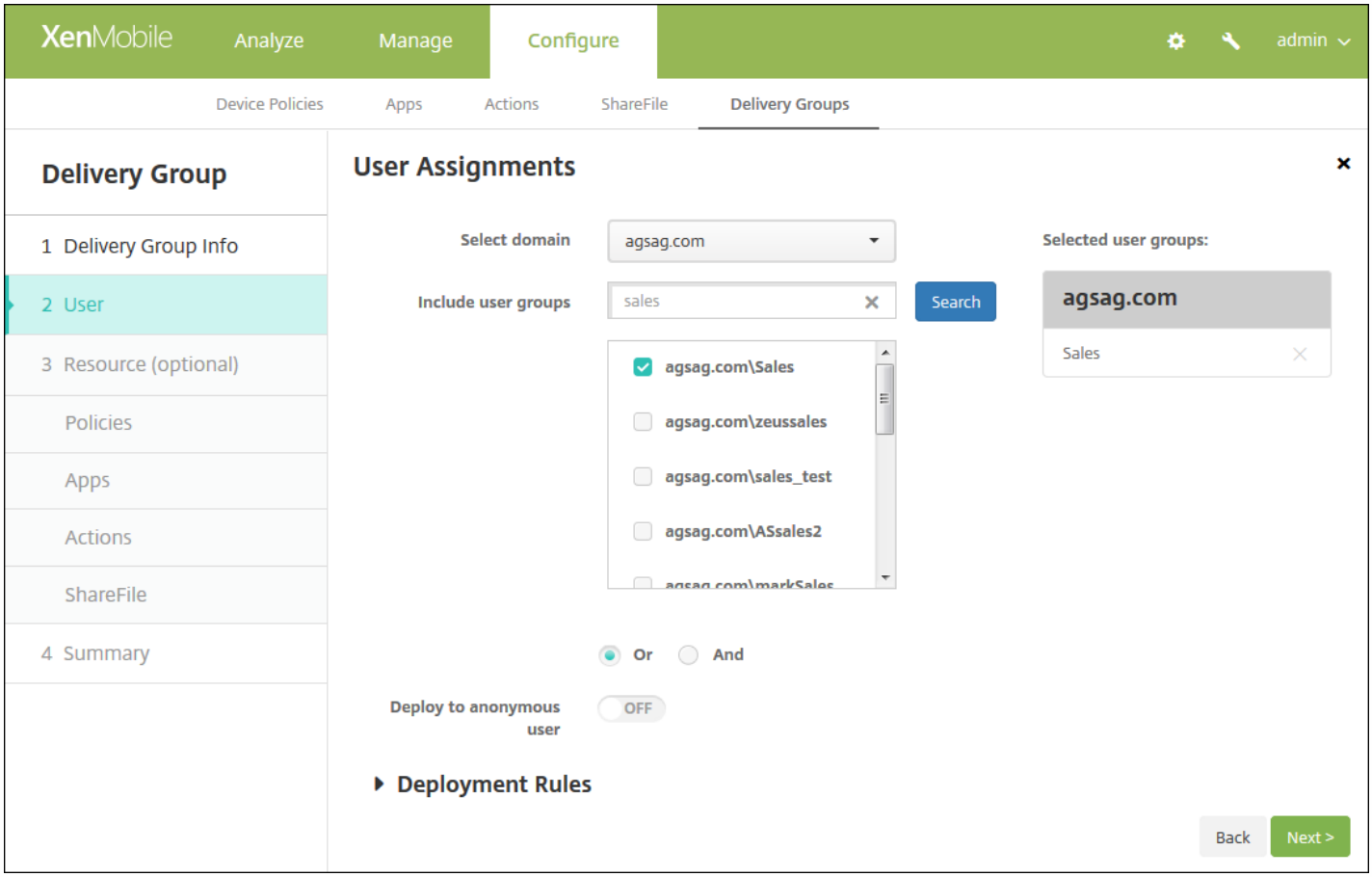
1. [**Delivery Groups**] ページで、デリバリーグループ名の横にある チェックボックス をオンにするか、デリバリーグループ名を含む行をクリックしてデリバリーグループを選択し、 [**Edit**] をクリックします。 [**Delivery Group Information**] 編集ページが開きます。

> **注意**
>
> デリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に[**Edit**] コマンドが表示されます。

2. [**Description**] ボックスに説明を追加するか、または既存の説明を変更します。

注：既存のグループの名前は変更できません。

3. [**Next**] をクリックします。 [**User Assignments**] ページが開きます。



4. [**Select User Groups**] ページで、以下の情報を入力または変更します。

- **Select domain**：一覧から、ユーザーを選択するドメインを選択します。
- **Include user groups**：次のいずれかを行います。
  - ユーザーグループの一覧で、追加するグループを選択します。 選択したグループが[**Selected user groups**] 一覧に表示されます。
  - [**Search**] をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - グループ名の全体または一部を検索ボックスに入力して [**Search**] をクリックし、ユーザーグループの一覧を絞り込みます。

    注：ユーザーグループを削除するには、[**Search**] をクリックし、ユーザーグループの一覧で削除するグループの横にある チェックボックス をオフにします。 グループ名の全体または一部を検索ボックスに入力して [**Search**] をクリックすると、一覧に表示されるユーザーグループ数を絞り込むことができます。

- **Or/And**：展開対象のユーザーがいずれかのグループに属していればよいか（ [Or] ）、すべてのグループに属している必要があるか（ [And] ）を選択します。
- **Deploy to anonymous user**：デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。

  注：認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

5. [**Deployment Rules**] を展開し、前に述べた手順の手順5で実行したように、設定を構成します。

6. [**Next**] をクリックします。 [**Delivery Group Resources**] ページが開きます。 このページでポリシー、アプリケーション、アクションを追加または削除します。 この手順をスキップするには、 [**Delivery Group**] の [**Summary**] をクリックしてデリバリーグループ構成の概要情報を表示します。

リソースの変更が完了したら、 [**Next**] をクリックするか、 [**Delivery Group**] の [**Summary**] をクリックします。

8. [**Summary**] ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順序を変更できます。

9. 構成の調整が必要な場合は、 [**Back**] をクリックして前のページに戻ります。

10. リソースの展開順序を並べ替えるには [**Deployment Order**] をクリックします。展開順序の変更について詳しくは、「展開順序を変更するには」を参照してください。

11. [**Save**] をクリックして、デリバリーグループを保存します。

> **注意**
>
> AllUsersは、有効化または無効化することができる唯一のデリバリーグループです。

1. [**Delivery Groups**] ページで、 [**AllUsers**] の横にあるチェックボックスをオンにするか、 [AllUsers] を含む行をクリックして、AllUsersデリバリーグループを選択します。 次に、以下のいずれかを行います。

注： [AllUsers] を選択した方法に応じて、AllUsersデリバリーグループの上または右側に [**Enable**] または [**Disable**] コマンドが表示されます。

- AllUsersデリバリーグループを無効化するには、 [**Disable**] をクリックします。 このコマンドは、 [AllUsers] が有効（デフォルト）になっている場合にのみ使用できます。 デリバリーグループの表の [**Disabled**] の見出しの下に、 [**Disabled**] が表示されます。
- AllUsersデリバリーグループを有効化するには、 [**Enable**] をクリックします。 このコマンドは、 [AllUsers] が現在無効になっている場合にのみ使用できます。 デリバリーグループの表の [**Disabled**] の見出しの下の [**Disabled**] の表示が消えます。

デリバリーグループへの展開とは、デリバリーグループに属するiOS、Windows Phone、Windowsタブレットデバイスを持つすべてのユーザーがXenMobileに再接続できるようにプッシュ通知を送信することを意味します。 これによってデバイスを再評価し、アプリケーション、ポリシー、アクションを展開できるようにします。 そのほかのプラットフォームデバイスを持つユーザーは、接続済みの場合は直ちにリソースを受信します。接続済みでない場合は、スケジュール設定ポリシーに基づいて次に接続したときにリソースを受信します。

注： ユーザーのAndroidデバイスで、Worx Storeの [Updated Available] の一覧に更新されたアプリケーションが表示されるようにするには、最初にアプリケーションインベントリポリシーをユーザーのデバイスに展開しておく必要があります。

1. [**デリバリー グループ**] ページで、次のいずれかを行います。

- 複数のデリバリーグループに同時に展開するには、展開するグループの横にあるチェックボックスをオンにします。

- 1つのデリバリーグループに展開するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

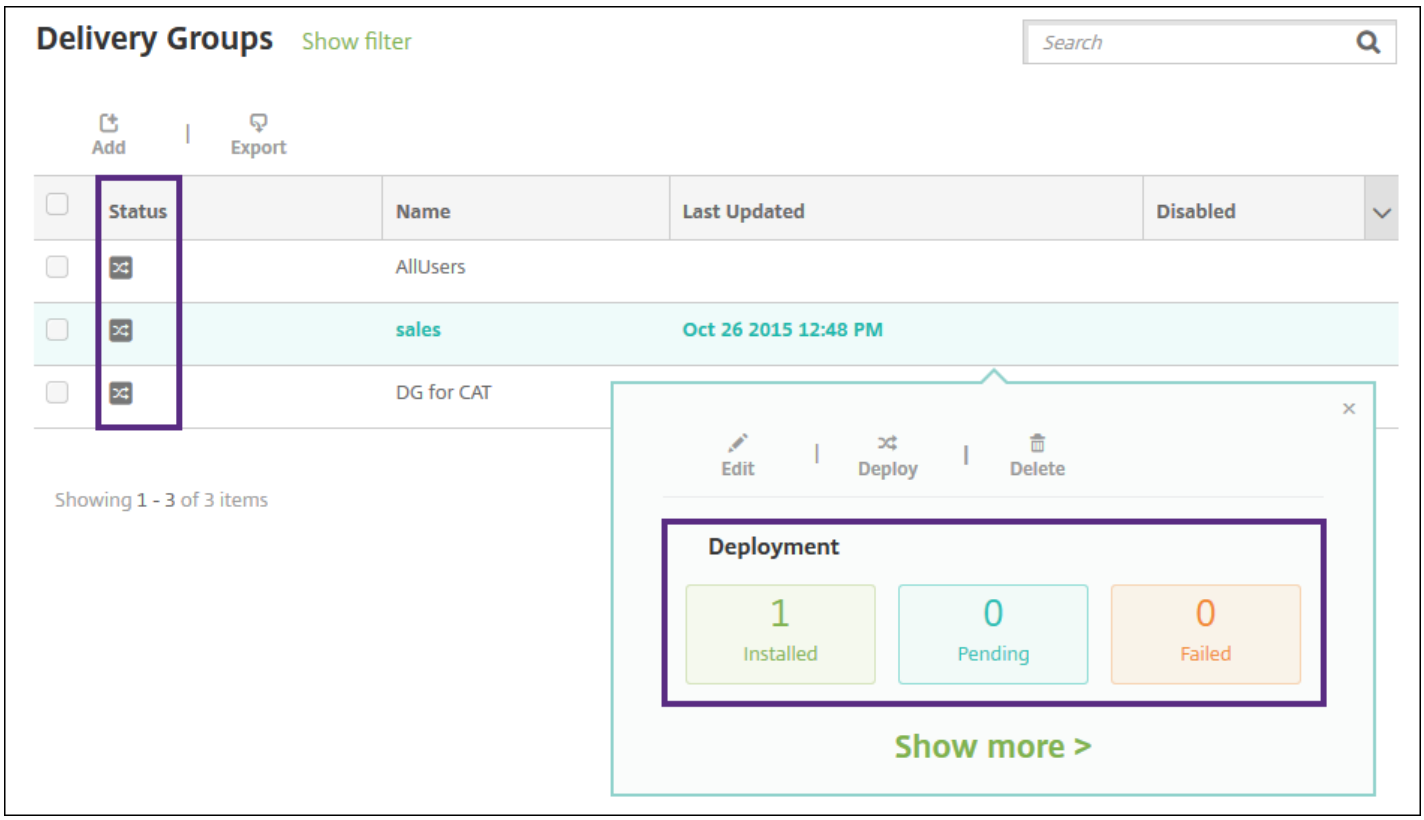
2. **[展開]** をクリックします。

注： 1つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に **[展開]** コマンドが表示されます。

アプリケーション、ポリシー、操作を展開するグループが一覧にあることを確認して、**[展開]** をクリックします。デバイスプラットフォームとスケジュール設定ポリシーに基づいて、選択したグループにアプリケーション、ポリシー、操作が展開されます。

[デリバリー グループ] ページで、次のいずれかの方法により展開ステータスを確認できます。

- デリバリーグループの **[ステータス]** の見出しの下で、展開エラーを示す展開アイコンを確認します。
- デリバリーグループを含む行をクリックし、**[Installed]（インストール済み）**、**[Pending]（保留中）**、**[Failed]（失敗）** の展開を示すオーバーレイを表示します。



注意

AllUsersデリバリーグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

1. **[Delivery Groups]** ページで、次のいずれかを行います。

- 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。
- 1つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

2. **[Delete]** をクリックします。 **[Delete]** ダイアログボックスが開きます。

注：1つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に**[Delete]** コマンドが表示されます。

3. **[Delete]** をクリックします。

> **Important**
>
> このアクションを元に戻すことはできません。

1. **[Delivery Groups]** の表の上にある **[Export]** をクリックします。 XenMobileによって **[Delivery Groups]** の表の情報が抽出され、.csvファイルに変換されます。

2. .csvファイルを開くか、保存します。 使用するブラウザーに応じて、手順が異なります。 操作を取り消すこともできます。

ユーザーとデバイスの登録

Aug 30, 2016

ユーザーデバイスをリモートで安全に管理するには、ユーザーデバイスをXenMobileに登録する必要があります。 XenMobil クライアントソフトウェアがユーザーデバイスにインストールされ、ユーザーのIDが認証され、XenMobileとユーザーのプ ファイルがインストールされます。 デバイスの登録後、XenMobileコンソールで、ポリシーの適用、アプリケーションの展開、データのデバイスへのプッシュ、紛失または盗難されたデバイスのロック、ワイプ、および捜索などのデバイス管理タスクを実行できます。

注：iOSデバイスユーザーを登録する前に、APN証明書を要求する必要があります。 詳しくは、 「XenMobileでの証明書」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にアクセスするには、XenMobileコンソールで[**Manage**] の [**Enrollment**] をクリックします。

Androidデバイス

Aug 02, 2016

1. AndroidデバイスでGoogle PlayストアまたはAmazonアプリストアに移動して、Citrix Worx Homeアプリケーションをダウンロードしてからアプリケーションをタップします。
2. インストールを求めるメッセージが表示されたら、［次へ］をクリックし、［インストール］をクリックします。
3. インストールが完了したら、［開く］をタップします。
4. 会社の資格情報（組織のXenMobileサーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなど）を入力し、［次へ］をクリックします。
5. ［デバイス管理者を有効にしますか］画面で、［有効にする］をタップします。
6. 会社のパスワードを入力し、［サインオン］をタップします。
7. XenMobileの構成方法によっては、Worx PINの作成を求められる場合があります。Worx PINは、Worx Homeやそのほかのworx準拠アプリ（WorxMail、WorxWeb、ShareFileなど）へのサインオンに使用できます。 Worx PINは2回入力する必要があります。 ［Worx PINの作成］画面で、6つの数字からなるPINを入力します。
8. PINを再入力します。 Worx Homeが開きます。 その後、Worx Storeにアクセスし、Androidデバイスにインストールできるアプリを確認することができます。
9. 登録の後でアプリをユーザーデバイスに自動的にプッシュするようにXenMobileを構成している場合は、アプリのインストールを求めるメッセージがユーザーに表示されます。 ［インストール］をタップしてアプリをインストールします。

デバイスを再登録する前に、そのデバイスの登録がまず解除されます。 登録が解除されてから再登録されるまでの間、そのデバイスはXenMobileコンソールのデバイスインベントリー覧には表示されますが、XenMobileで管理されなくなります。デバイスがXenMobileで管理されていない間は、そのデバイスを追跡したり、デバイスのコンプライアンスを監視したりすることができません。

1. Worx Homeアプリケーションをタップして開きます。
2. アプリケーションウィンドウの左上にある［設定］アイコンをタップします。
3. ［Re-Enroll］をタップします。 デバイスの再登録を確認するメッセージが表示されます。
4. ［OK］をタップします。 これにより、デバイスの登録が解除されます。
5. 画面の指示に従って、デバイスを再登録します。

iOSデバイス

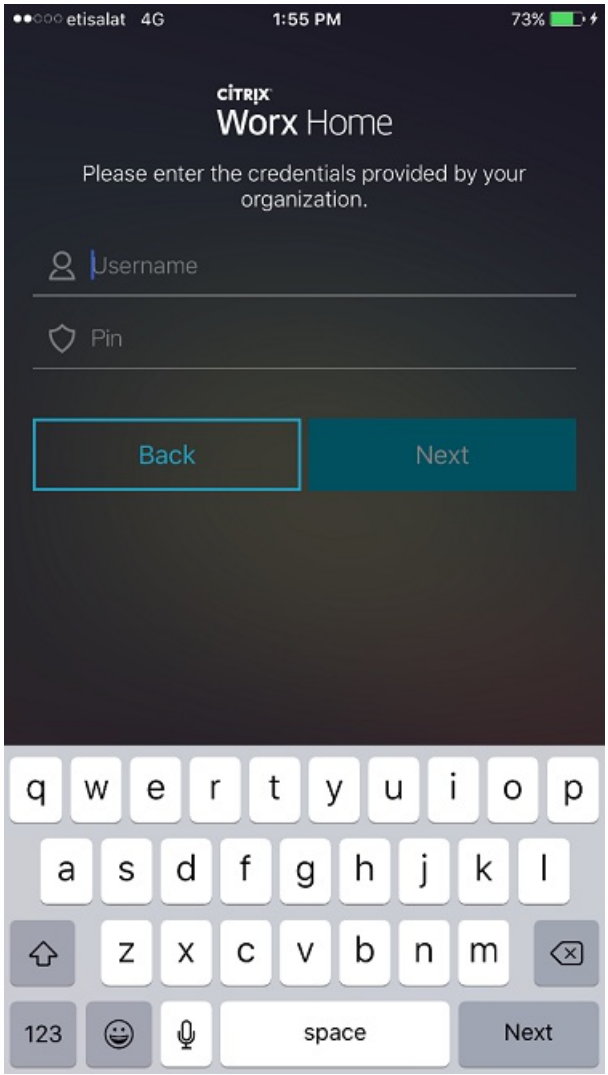
Aug 02, 2016

1. Worx Homeアプリをデバイスの Apple iTunes App Storeからダウンロードした後、アプリをデバイスにインストールします。

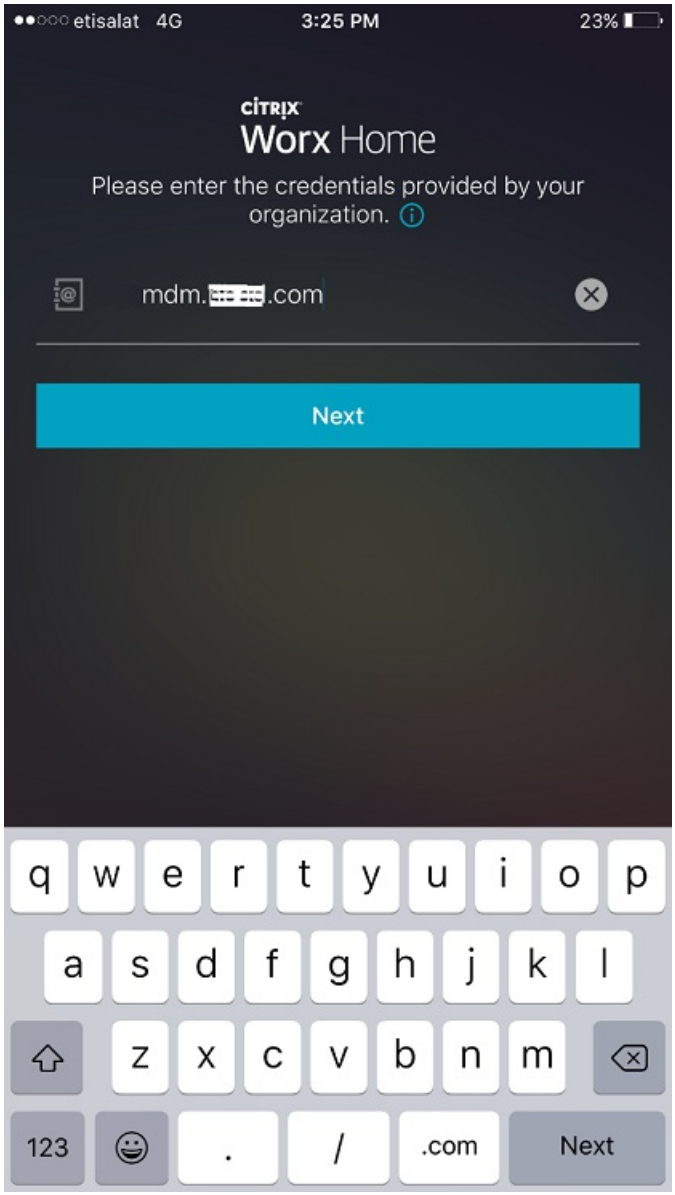
2. iOSデバイスのホーム画面で、Worx Homeアプリをタップします。

3. Worx Homeアプリが開いたら、会社のXenMobileサーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールなどの会社の資格情報を入力し、**[次へ]**をクリックします。

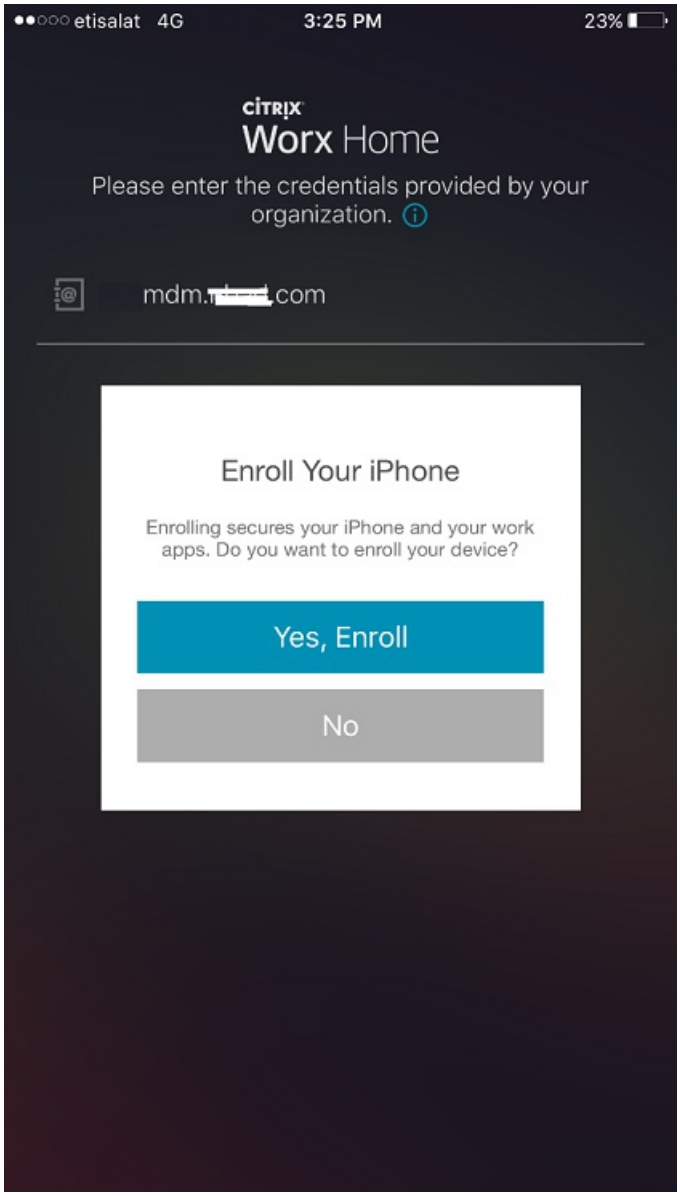
表示される画面は、XenMobileの構成方法に応じて、次の例と異なる可能性があります。

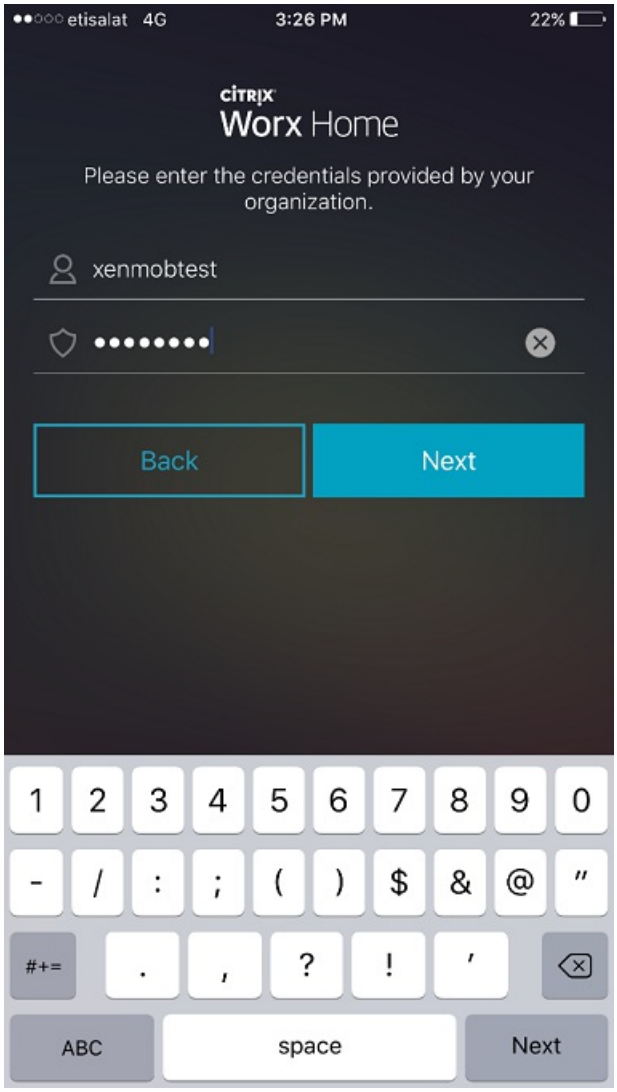


4. ヘルプデスクから提供されたアドレスを入力します。



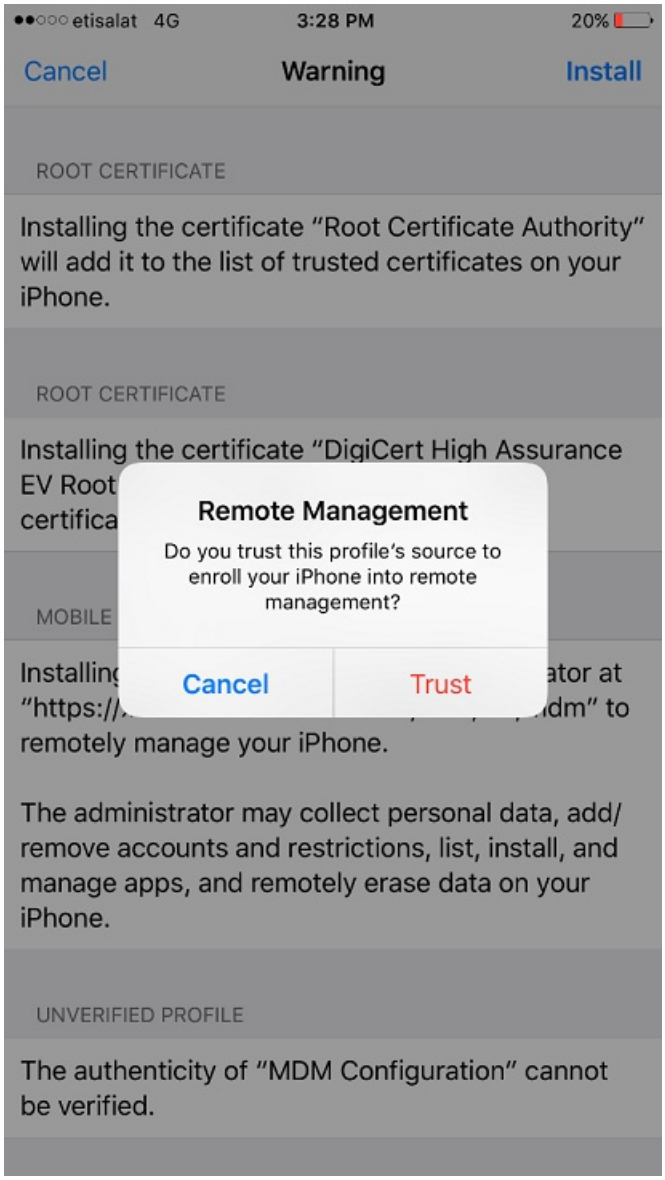
5.登録するよう求められたら **[Yes, Enroll]** をクリックし、続いて画面の指示に従って資格情報を入力します。



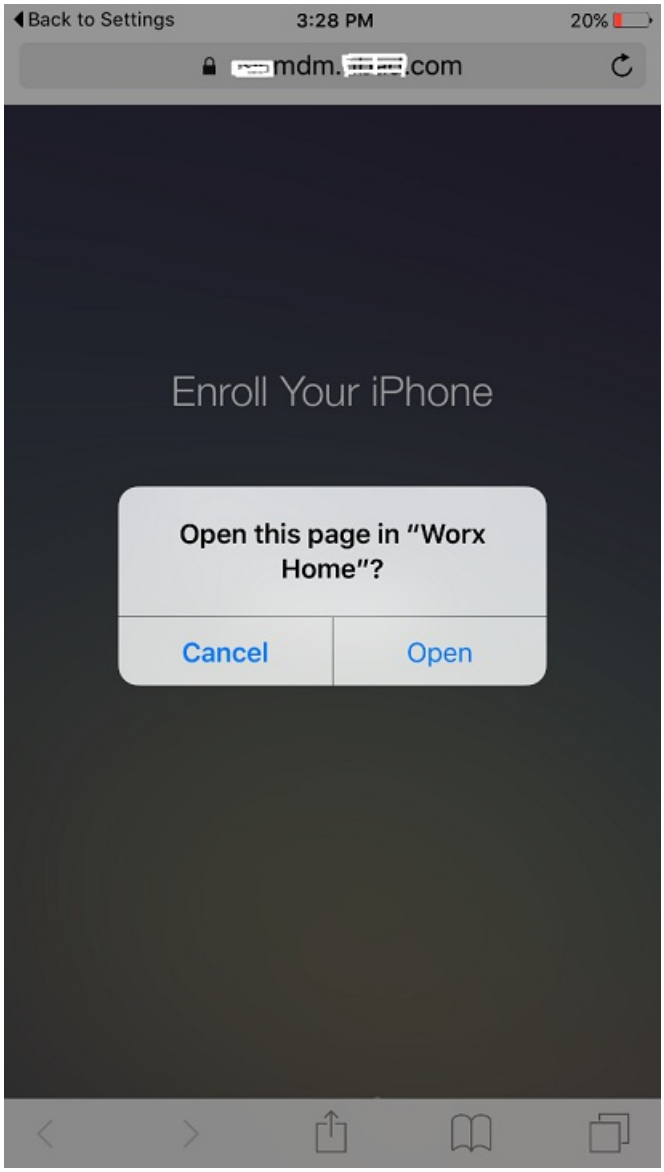


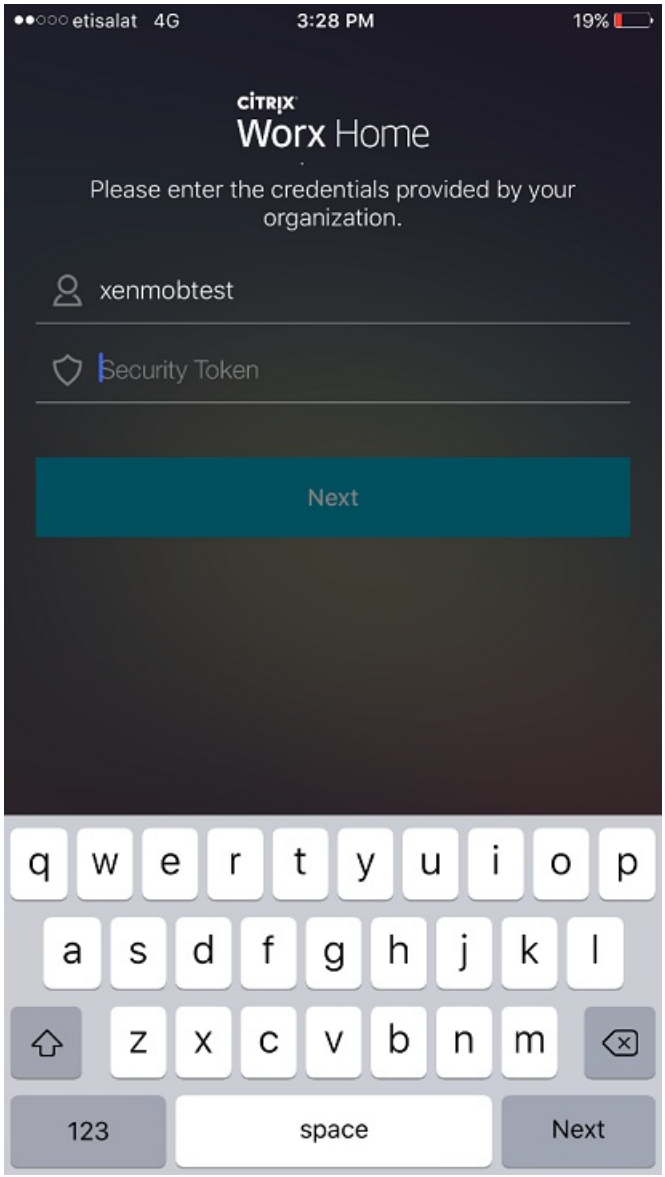
6. **[インストール]**をタップして、Citrix Profileサービスをインストールします。

7. **[Trust]** をタップします。



8. **[Open]** をタップし、続いて資格情報を入力します。





Mac OS Xデバイス

Aug 02, 2016

XenMobileには、OS Xが実行されているMacを登録することができます。 登録は、Macユーザーが各自のデバイスから直接行います。

Macの登録手順は以下のとおりです。

1. 任意で、XenMobileコンソールでMacのデバイスポリシーを設定します。 デバイスポリシーについて詳しくは、 デバイスポリシー」を参照してください。 Mac用に構成できるデバイスポリシーを確認するには、 「プラットフォーム別のXenMobileデバイスポリシー」を参照してください。

2. 登録リンク（https://serverFQDN:8443/zdm/macos/otae）を送信します。ユーザーはこのリンクをSafariで開きます。 ここで、

- serverFQDNは、XenMobileが動作するサーバーの完全修飾ドメイン名（FQDN）です。
- ポート8443は、デフォルトのセキュアポートです。別のポートを構成している場合は、8443ではなく、構成済みのポートを使用します。
- zdmは、サーバーのインストール時に使用されるインスタンス名です。

インストールリンクの送信について詳しくは、「インストールリンクを送信するには」を参照してください。

3. 必要に応じて、ユーザーが証明書をインストールします。 ユーザーに証明書のインストールを求めるメッセージが表示されるかどうかは、管理者がiOSおよびMac OS用の公式に信頼されるSSL証明書および公式に信頼されるデジタル署名証明書を構成したかどうかによって異なります。 証明書について詳しくは、「証明書」を参照してください。

4. ユーザーがMacにサインオンします。

5. Macのデバイスポリシーがインストールされます。

これで、モバイルデバイスを管理するのと同じように、XenMobileでMacを管理できるようになります。

Windowsデバイス

Aug 02, 2016

XenMobileには、以下のWindowsオペレーティングシステムが動作するデバイスを登録できます。

- Windows 8.1および10
- Windows Phone 8.1および10

WindowsおよびWindows Phoneのユーザーはデバイスから直接登録します。

ユーザー登録のため自動検出およびWindows検出サービスを構成して、WindowsおよびWindows Phoneデバイスの管理を有効にする必要があります。

> **注意**
>
> Windowsデバイスの登録には、SSLリスナー証明書が公開証明書である必要があります。 自己署名SSL証明書をアップロード済みの場合、登録は失敗します。

ユーザーは、Windows RT 8.1、Windows 8.1 ProとWindows 8.1 Enterprise（32ビットと64ビット）の両方、およびWindows 10を実行しているデバイスを登録できます。 Windowsデバイスの管理を有効にするには、自動検出およびWindows検出サービスを構成することをお勧めします。 詳しくは、「ユーザー登録のためにXenMobileで自動検出を有効にするには」を参照してください。

1 デバイスで使用可能なWindows Updateをすべて確認し、インストールします。 この手順は、Windows 8からWindows 8.1にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。

2. チャームメニューで **[設定]** をタップします。

- Windows 8.1の場合は、 **[ネットワーク]** > **[ワークスペース]** の順にタップします。
- Windows 10の場合は、 **[アカウント]** > **[職場のアクセス]** > **[デバイス管理に登録にする]** の順にタップします。

3. コーポレートメールアドレスを入力してから **[オンにする]** （Windows 8.1）または **[続行]** （Windows 10）をタップします。 ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します（例：foo@mydomain.com）。 これによって、Windowsの埋め込みデバイス管理によって登録が実行される、既知のMicrosoftの制限を回避できます。 **[サービスに接続しています]** ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。 デバイスがXenMobileサーバーを自動的に検出し、登録処理が開始されます。

4. パスワードを入力します。XenMobileのユーザーグループのメンバーであるアカウントに関連付けられたパスワードを使用します。

5. Windows 8.1の場合は、 **[IT 管理者によるアプリやサービスの管理を許可する]** ダイアログボックスでデバイスの管理に同意することを示し、次に **[オンにする]** をタップします。 Windows 10の場合は、 **[使用条件]** 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、次に **[同意する]** をタップします。

自動検出なしでWindowsデバイスを登録することができます。 しかし、自動検出を構成するようお勧めします。 自動検出な

しで登録すると、希望するURLに接続する前にポート80を呼び出すことになるため、実稼働環境でのベストプラクティスとは みなせません。 このような処理は、テスト環境や概念実証展開でのみ使用するようにしてください。

1 デバイスで使用可能なWindows Updateをすべて確認し、インストールします。 この手順は、Windows 8からWindows 8.1 にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。

2. チャームメニューで **[設定]** をタップします。

- Windows 8.1の場合は、 **[ネットワーク]** > **[ワークスペース]** の順にタップします。
- Windows 10の場合は、 **[アカウント]** > **[職場のアクセス]** > **[デバイス管理に登録にする]** の順にタップします。

3. 会社のメールアドレスを入力します。

4. Windows 10では、自動検出が構成されていない場合、手順5で説明されているようにサーバーの詳細を入力できるオプシ ンが表示されます。 Windows 8.1では、 **[サーバーアドレスを自動検出する]** がオンに設定されている場合、タップしてこの オプションをオフにします。

5. **[サーバーアドレスを入力してください]** フィールドに以下のアドレスを入力します。

- Windows 8.1の場合、「https://*serverfqdn:8443/serverInstance*/Discovery.svc」という形式でサーバーアドレスを入力しま す。 未認証のSSL接続に8443以外のポートが使用される場合、このアドレスの*8443*の箇所にそのポート番号を指定しま す。
- Windows 10の場合、「https://beta.managedm.com:8443/zdm/wpe」というアドレスを入力します。 未認証のSSL接続に 8443以外のポートが使用される場合、このアドレスの *8443* の箇所にそのポート番号を指定します。

6. パスワードを入力します。

7. Windows 8.1の場合は、 **[IT 管理者によるアプリやサービスの管理を許可する]** ダイアログボックスでデバイスの管理に 同意することを示し、次に **[オンにする]** をタップします。 Windows 10の場合は、 **[使用条件]** 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、次に **[同意する]** をタップします。

XenMobileでWindows Phoneデバイスを登録するには、ユーザーはActive Directoryまたは内部ネットワークのメールアドレ スおよびパスワードを入力する必要があります。 自動検出がセットアップされていない場合、ユーザーはXenMobileサーバ のサーバーWebアドレスも必要です。 以下の手順に従って、デバイスを登録します。

注：Windows Phoneの業務用ストアを介してアプリケーションを展開する場合は、ユーザーが登録する前に、（署名済みの Citrix Worx Home、サポートする各プラットフォーム向けWindows Phoneアプリを使って）Enterprise Hubポリシーを構成し ます。
1 Window Phoneのメイン画面で **[設定]** アイコンをタップします。

2. Windows Phone 8.1の場合は、 **[システム]** > **[ワークスペース]** の順にタップし、次に **[アカウントの追加]** をタップし ます。 Windows 10 Phoneの場合は、 **[アカウント]** > **[職場のアクセス]** > **[デバイス管理に登録にする]** の順にタップしま す。

3. 次の画面でメールアドレスとパスワードを入力し、 **[サインイン]** をタップします。

ドメインに自動検出が構成されている場合、以降のいくつかの手順で求められる情報は自動的に抽出されます。 手順8. に進みます。

ドメインに自動検出が構成されていない場合、次の手順に進みます。ローカルユーザーとして登録するには、ドメイン 名は正しいものの、存在しないメールアドレスを入力します（例：foo@mydomain.com）。 これによって既知の

Microsoftの制限を回避できます。 **[サービスに接続しています]** ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。

4. 次の画面でXenMobileサーバーのWebアドレスを、「https://://wpe」のように入力します。 たとえば、https://mycompany.mdm.com:8443/zdm/wpeなどです。 **注**：実際の実装に合わせてポート番号を選択する必要がありますが、iOSの登録に使用したポートと同じポートを使用してください。

5. ユーザー名とドメインを介して認証が検証される場合、ユーザー名とドメインを入力し、次に**[サインイン]** をタップします。

6. 証明書に関する問題を通知する画面が表示された場合、そのエラーの原因は自己署名入り証明書の使用です。 サーバーが信頼できる場合、 **[続行]** をタップします。 信頼できない場合は、 **[キャンセル]** をタップします。

7. Windows Phone 8.1で、アカウントを追加すると **[業務用アプリをインストール]** というオプションが表示されます。 管理者が業務用アプリストアを構成済みの場合、このオプションをオンにして、 **[完了]** をタップします。 このオプションをオフにした場合、業務用アプリストアを受信するには再登録が必要になります。

8. Windows Phone 8.1で、 **[アカウントが追加されました]** 画面で **[完了]** をタップします。

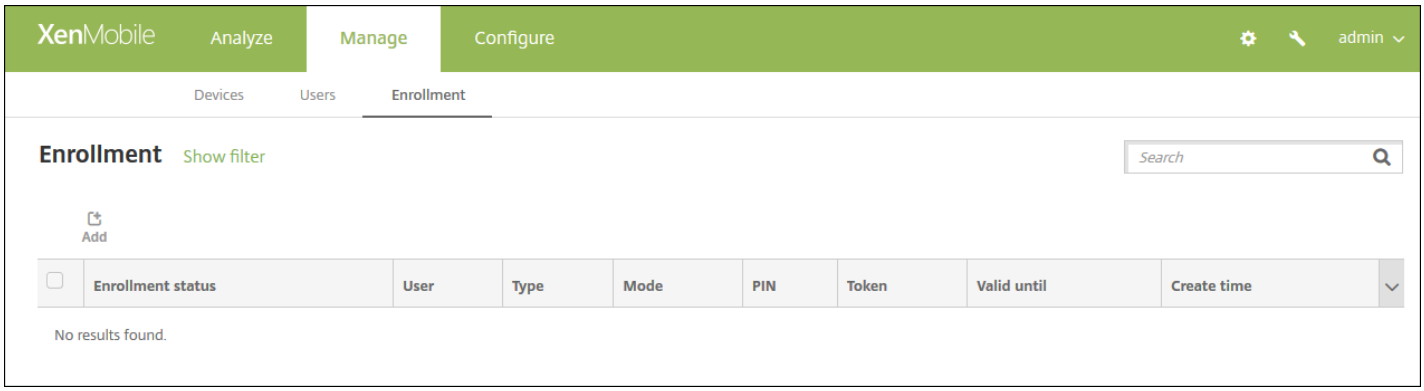
9. サーバーへの接続を強制的に実行するには、［最新の情報に更新］アイコンをタップします。 デバイスを手動でサーバーに接続できない場合、XenMobileは再接続を試行します。 XenMobileは3分ごとに5回連続でデバイスに接続し、その後は2時間ごとに接続します。 この接続頻度は、 **[Server properties]** にある［Windows **WNS Heartbeat Interval**］で変更できます。 登録の完了後、Worx Homeがバックグラウンドで登録を実行します。 インストールが完了してもそれについては何も通知されません。 **[すべてのアプリ]** 画面からWorx Homeを開きます。

XenMobileでの登録招待状の送信

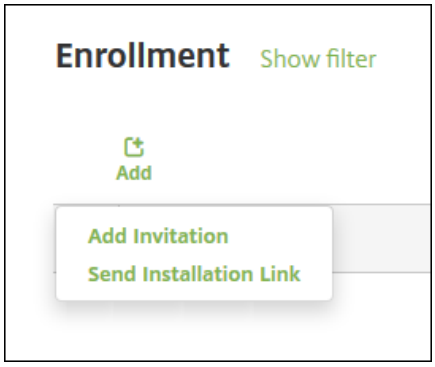
Oct 25, 2016

XenMobileコンソールで、iOSデバイスまたは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。 iOS、Android、Windows、またはMac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。

1. XenMobileコンソールで、［**Manage**］の［**Enrollment**］をクリックします。 ［**Enrollment**］ページが開きます。

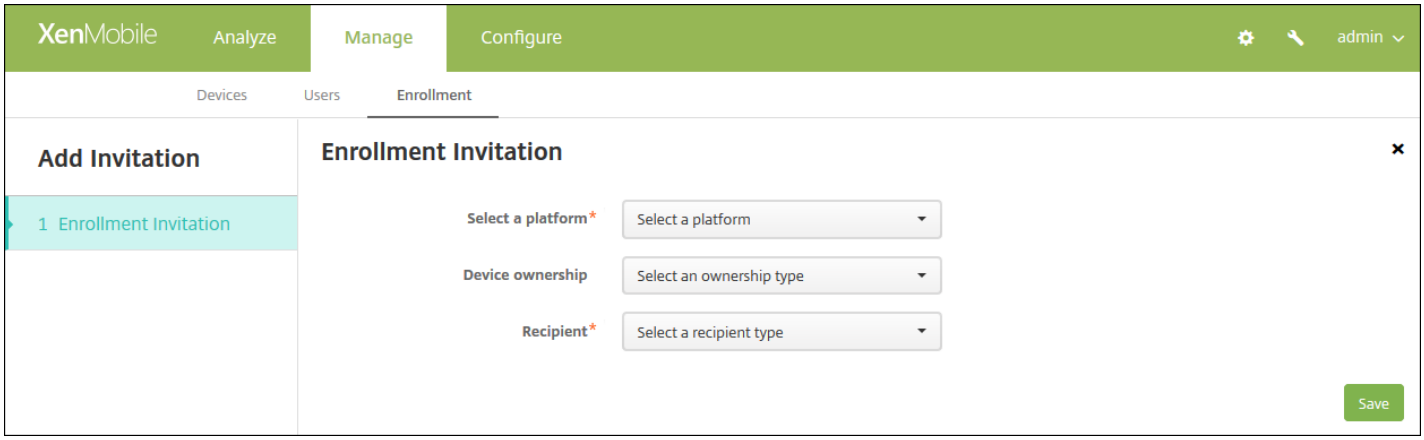


2. ［**Add**］をクリックします。 登録オプションが示されたメニューが表示されます。



- 登録招待状をユーザーまたはグループに送信するには、［**Add Invitation**］を選択します。この設定の構成手順については、「招待状を送信するには」を参照してください。
- SMTPまたはSMS経由で登録インストールリンクを受信者の一覧に送信するには、［**Send Installation Link**］を選択します。この設定の構成手順については、「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。

1 . ［**Add Invitation**］をクリックします。 ［**Enrollment Invitation**］画面が開きます。

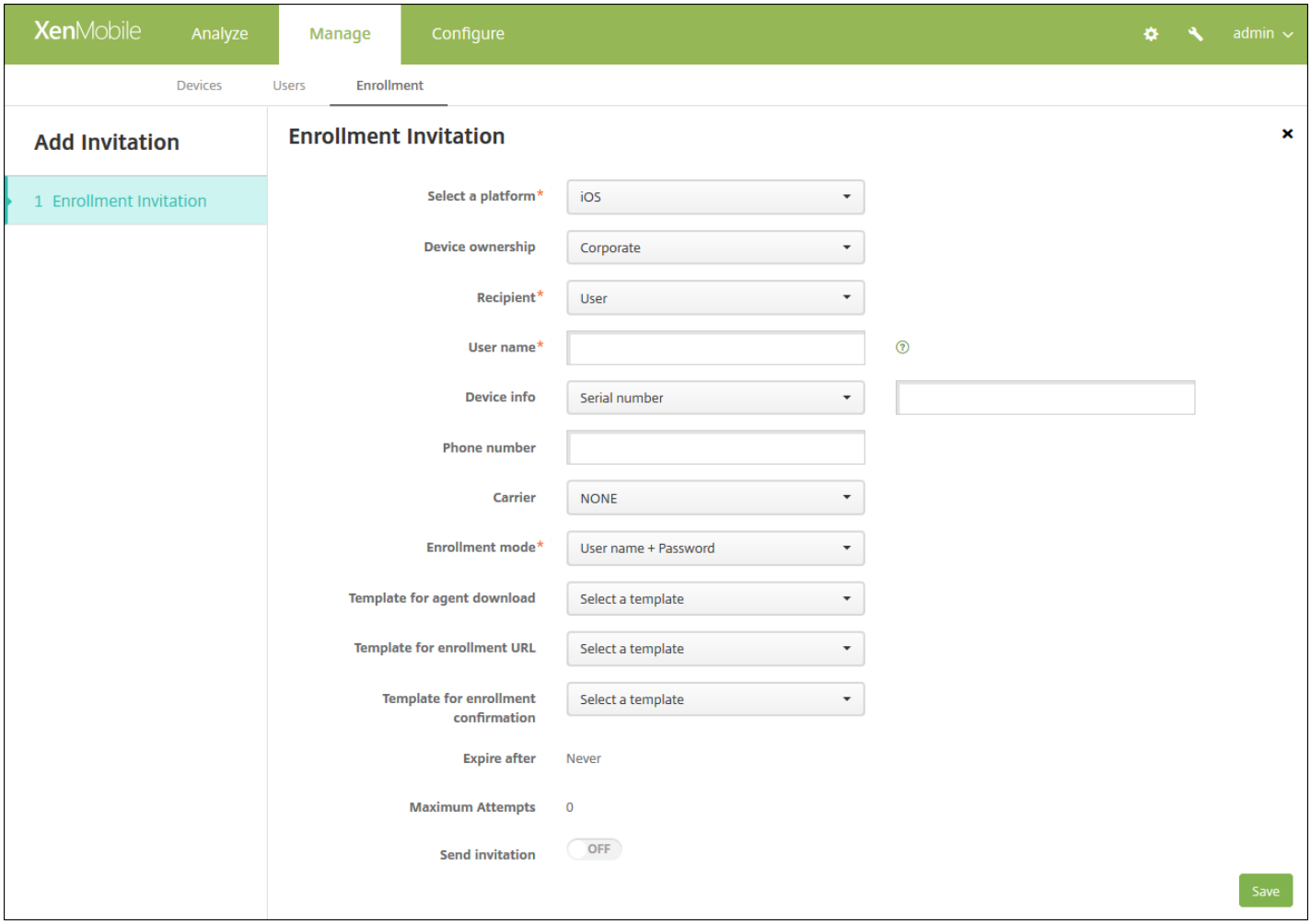


2. 次の設定を構成します。

- **Select a platform**：一覧から、［**iOS**］または［**Android**］を選択します。
- **Device ownership**：一覧から、［**Corporate**］または［**Employee**］を選択します。
- **Recipient**：一覧から、［**User**］または［**Group**］を選択します。

選択した宛先に応じて、追加の構成設定が表示されます。［**User**］の設定については「登録招待状をユーザーに送信するには」を、［**Gourp**］の設定については「登録招待状をグループに送信するには」を参照してください。

登録招待状をユーザーに送信するには



1. **[User]**について、次の設定を構成します。

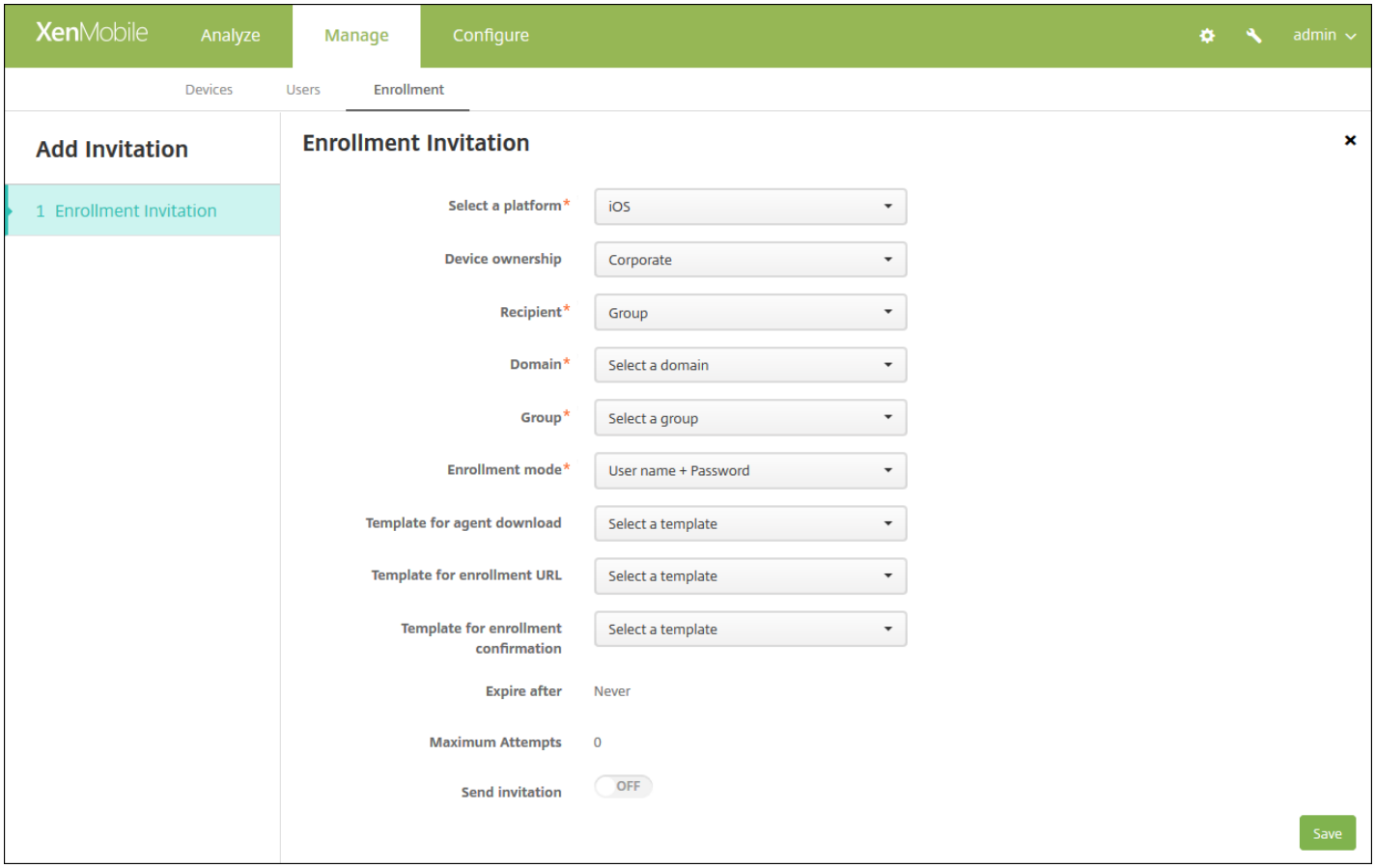
- **User name**：ユーザー名を入力します。ユーザーは、XenMobileサーバーのローカルユーザー、またはActive Directoryのユーザーとして存在している必要があります。 ローカルユーザーの場合、通知を送信できるようにユーザーの電子メールプロパティが設定されていることを確認します。 Active Directoryユーザーの場合、LDAPが構成されていることを確認します。
- **Device info**：一覧から、 **[Serial number]** 、 **[UDID]** 、 **[IMEI]**のいずれかを選択します。オプションを選択すると、デバイスに応じて値を入力できるフィールドが表示されます。
- **Phone number**：任意で、ユーザーの電話番号を入力します。
- **Carrier**：一覧から、ユーザーの電話番号を関連付ける電話会社を選択します。
- **Enrollment mode**：一覧から、ユーザーに求める登録の方法を選択します。 デフォルトは、 **[User name + Password]**です。 選択できるオプションは以下のとおりです。
  - High Security
  - Invitation URL
  - Invitation URL + PIN
  - Invitation URL + Password
  - Two Factor
  - User name + PIN

  注：:PINを含む登録モードを選択すると、 **[Template for enrollment PIN]**フィールドが表示されます。このフィールドで、 **[Enrollment PIN]**を選択します。

- **Template for agent download**：一覧から、登録招待に使用するテンプレートを選択します。この一覧では、プラットフォームの種類に基づいてオプションが決まります。 たとえば、プラットフォームとして［**iOS**］を選択した場合、オプションとして［**iOS Download Link**］が表示されます。
- **Template for enrollment URL**：一覧から、［**Enrollment Invitation**］を選択します。
- **Template for enrollment confirmation**：一覧から、［**Enrollment Confirmation**］を選択します。
- **Expire after**：このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。 登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Maximum Attempts**：このフィールドは登録処理を行う上限回数を示すものであり、登録モードを構成するときに設定します。 登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Send invitation**：招待状をすぐに送信する場合は［**ON**］を選択し、［**Enrollment**］ページの表に招待状を追加するだけの場合は［**OFF**］を選択します。

2. ［**Send invitation**］を有効にした場合は［**Save and Send**］をクリックし、それ以外の場合は［**Save**］をクリックします。 ［**Enrollment**］ページの表に招待状が追加されます。

登録招待状をグループに送信するには



1. 次の設定を構成します。

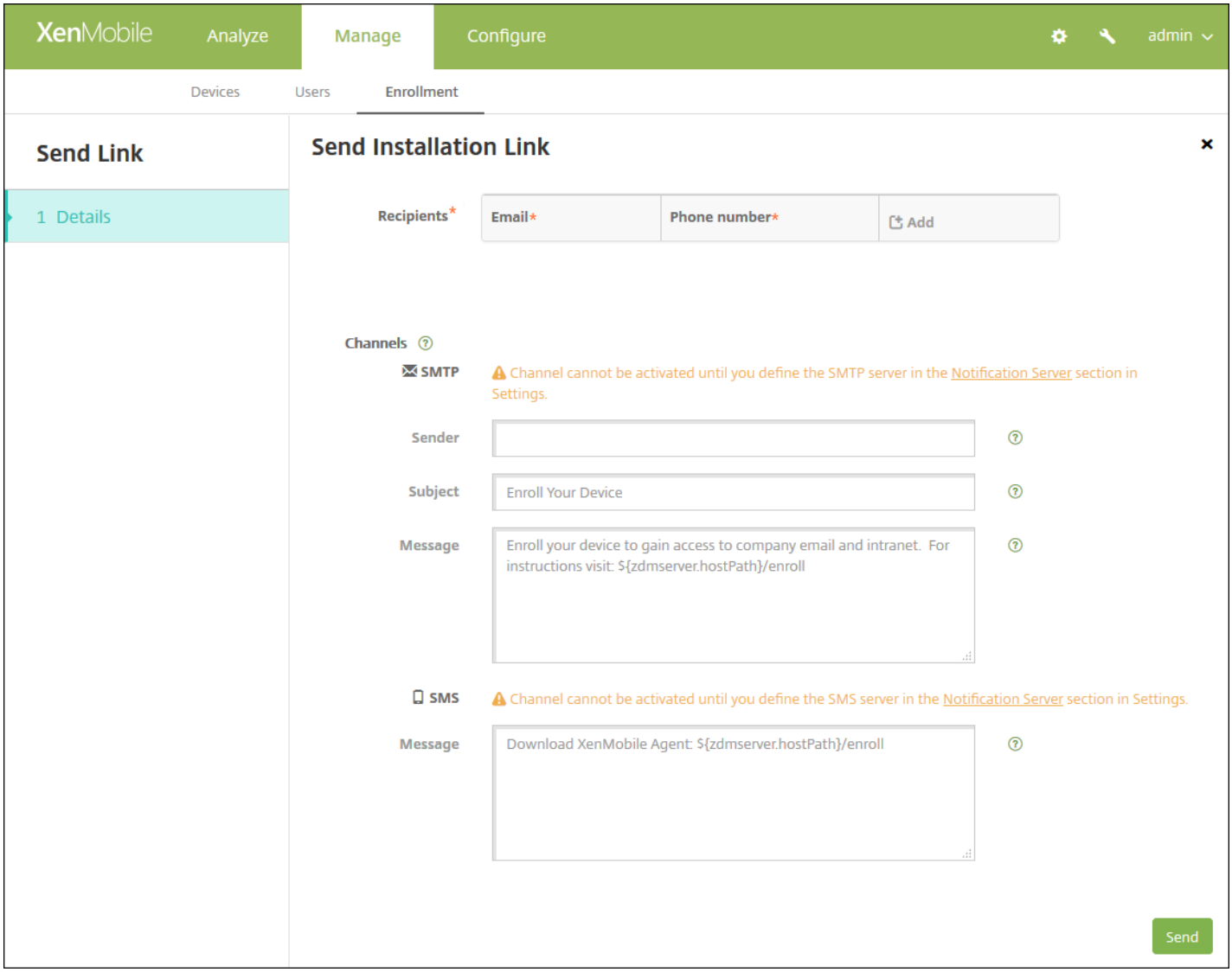
- **Domain**：一覧から、グループを選択するドメインを選択します。
- **Group**：一覧から、招待状の宛先グループを選択します。
- **Enrollment mode**：一覧から、グループ内のユーザーに求める登録の方法を選択します。 デフォルトは、［**User name + Password**］です。 選択できるオプションは以下のとおりです。
  - High Security

- Invitation URL
- Invitation URL + PIN
- Invitation URL + Password
- Two Factor
- User name + PIN

  注：:PINを含む登録モードを選択すると、 **[Template for enrollment PIN]** フィールドが表示されます。このフィールドで、 **[Enrollment PIN]** を選択します。

- **Template for agent download**：一覧から、登録招待に使用するテンプレートを選択します。この一覧では、プラットフォームの種類に基づいてオプションが決まります。 たとえば、プラットフォームとして **[iOS]** を選択した場合、オプションとして **[iOS Download Link]** が表示されます。
- **Template for enrollment URL**：一覧から、 **[Enrollment Invitation]** を選択します。
- **Template for enrollment confirmation**：一覧から、 **[Enrollment Confirmation]** を選択します。
- **Expire after**：このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。 登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Maximum Attempts**：このフィールドは登録処理を行う上限回数を示すものであり、登録モードを構成するときに設定します。 登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Send invitation**：招待状をすぐに送信する場合は **[ON]** を選択し、 **[Enrollment]** ページの表に招待状を追加するだけの場合は **[OFF]** を選択します。

2. **[Send invitation]** を有効にした場合は **[Save and Send]** をクリックし、それ以外の場合は **[Save]** をクリックします。 **[Enrollment]** ページの表に招待状が追加されます。



登録インストールリンクを送信する前に、**[Settings]** ページでチャネル（SMTPまたはSMS）を構成する必要があります。 詳しくは、「通知」を参照してください。

1. 次の設定を構成します。

- **Recipient**：追加する宛先ごとに、**[Add]** をクリックして以下の操作を行います。
  - **Email**：送信先のメールアドレスを入力します。 このフィールドは必須です。
  - **Phone number**：送信先の電話番号を入力します。 このフィールドは必須です。
  - **[Save]** をクリックします。

  注：既存の送信先を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

  既存の送信先を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

- **Channels**：登録インストールリンクの送信に使用するチャネルを選択します。 通知はSMTPまたはSMSで送信するこ

とができます。 **[Settings]** ページの **[Notification Server]** でサーバー設定を構成するまでは、これらのチャネルをアクティブ化できません。 詳しくは、「通知」を参照してください。

- **SMTP**：次の設定を任意で構成します。 これらのフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
  - **Sender**： 任意で送信者を入力します。
  - **Subject**:：任意でメッセージの件名を入力します。 たとえば、「Enroll your device」などです。
  - **Message**：任意で、送信先に送信されるメッセージを入力します。 たとえば、「Enroll your device to gain access to organizational apps and email.」などです。
- **SMS**：以下の設定を構成します。 このフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
  - **Message**：送信先に送信されるメッセージを入力します。 SMSベースの通知の場合、このフィールドは必須です。

    注：北米の場合、160文字を超えるSMSメッセージは複数のメッセージとして配信されます。

2. **[Send]** をクリックします。

注意

環境がSAMAccountNameを使用している場合、ユーザーが招待状を受け取ってリンクをクリックした後、認証を完了するには、ユーザー名を編集する必要があります。 たとえば、SAMAccountName@domainname.comからドメイン名を削除する必要があります。

XenMobileでの共有デバイス

Aug 02, 2016

XenMobileでは、複数のユーザーが共有できるデバイスを構成できます。 共有デバイス機能を使用すると、たとえば、病院の臨床医は、特定のデバイスを持ち歩くのではなく、近くにある任意のデバイスを使用して、アプリケーションやデータにアクセスできます。 場合によっては、法執行機関、リテール、製造などの現場で交代勤務労働者にデバイスを共有させ、機器費用の削減を図る必要があります。

共有デバイスに関する注意点

MDMモード

- iOSおよびAndroid搭載のタブレットおよびスマートフォンで使用できます。 XenMobile Enterpriseの共有デバイスでは、基本的なデバイス登録プログラム（DEP）による登録はサポートされません。 共有デバイスをこのモードで登録するするには、認証済みのDEPを使用する必要があります。
- クライアント証明書認証、Worx PIN、Touch ID、ユーザーエントロピーはサポートされません。

MDM+MAMモード

- iOSおよびAndroidタブレットでのみ使用できます。
- XenMobile 10.3.xサーバーとクライアントでのみサポートされています。
- MAMのみのモードはサポートされません。 デバイスはMDMに登録する必要があります。
- WorxMail、WorxWeb、およびShareFileモバイルアプリ（バージョン4.4）のみがサポートされます。 HDXアプリはサポートされません。
- Active Directoryユーザーのみがサポートされます。ローカルユーザーおよびグループはサポートされません。
- 既存のMDM-onlyモードの共有デバイスをMDM+MAMモードに更新するには、再登録が必要です。
- ユーザーは、WorxアプリケーションおよびMDXラップしたアプリケーションのみを共有できます。デバイスのネイティブのアプリケーションは共有できません。
- 最初の登録時にダウンロードすれば、新しいユーザーがデバイスにログオンするたびにWorxアプリケーションがダウンロードされることはありません。 新しいユーザーは、デバイスを起動して、サインインし、使用を始めることができます。
- セキュリティのために、Android上で各ユーザーのデータを隔離する場合は、XenMobileコンソールで**[Disallow rooted devices]**ポリシーを**[オン]**にする必要があります。

共有デバイスの登録の前提条件

共有デバイスを登録する前に、以下の操作を行う必要があります。

- 共有デバイス登録ユーザーの役割を作成します。 「RBACを使用した役割の構成」を参照してください。
- 共有デバイスユーザーを作成します。 「XenMobileでローカルユーザーを追加、編集、または削除するには」を参照してください。
- 共有デバイス登録ユーザーに適用されるベースポリシー、アプリーション、およびアクションを含むデリバリーグループを作成します。 「デリバリーグループの管理」を参照してください。

1. **Shared Device Enrollers**などの名前のActive Directoryグループを作成します。
2. 共有デバイスを登録するActive Directoryユーザーをこのグループに追加します。 このために新しいアカウントが必要な場合は、新しいActive Directoryユーザー（**sdenroll**など）を作成して、このユーザーをActive Directoryグループに追加します。

共有デバイスの要件

サイレントインストールやアプリケーションの削除など、最善のユーザーエクスペリエンスが提供されるよう、共有デバイスの構成は以下のプラットフォームで行うことをお勧めします。

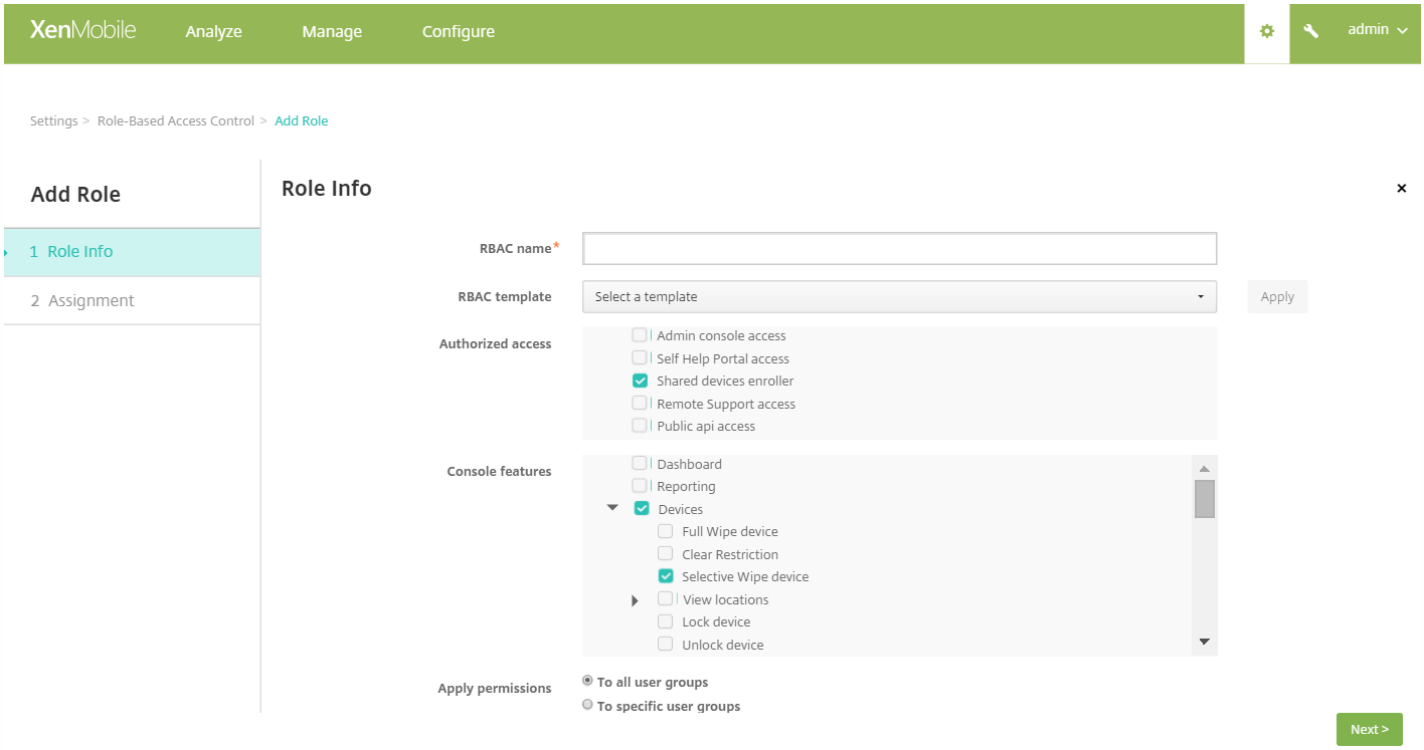
- iOS 9
- iOS 8
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x（MDM-onlyモード）

共有デバイスを構成するには

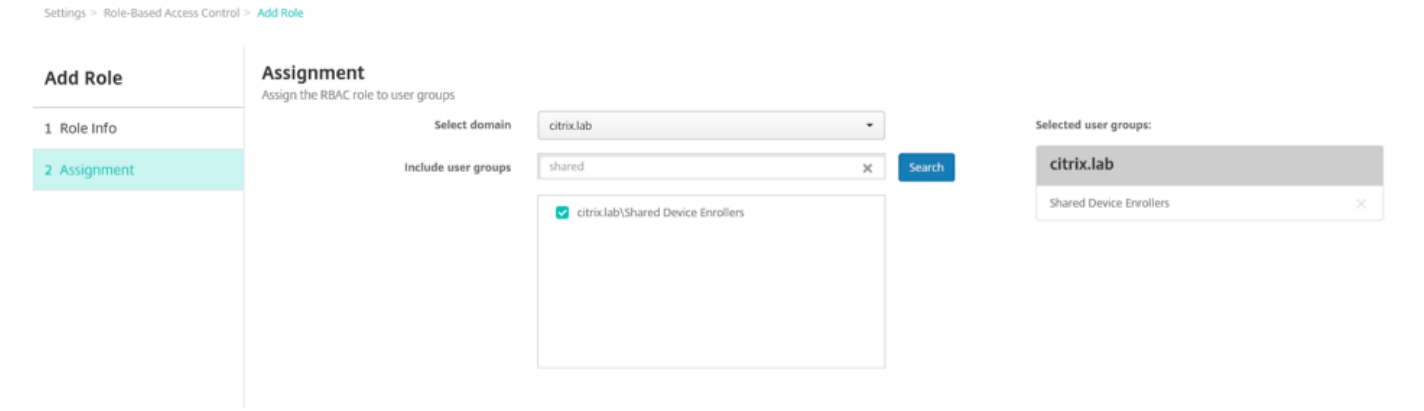
以下の手順に従って、共有デバイスを構成します。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 [Settings]ページが開きます。
2. **[Role-Based Access Control]**、**[Add]**の順にクリックします。 **[役割の追加]**画面が表示されます。
3. **[承認済みのアクセス]**で**[共有デバイスの登録機能]**権限を持つ**Shared Device Enrollment User**という名前の共有デバイス登録ユーザーの役割を作成します。 **[Console features]**の**[Devices]**を展開し、**[Selective Wipe device]**をオンにします。 この設定によって、共有デバイス登録機能アカウントにプロビジョニングされたアプリとポリシーは、デバイスの登録が解除されるとWorx Homeから削除されます。

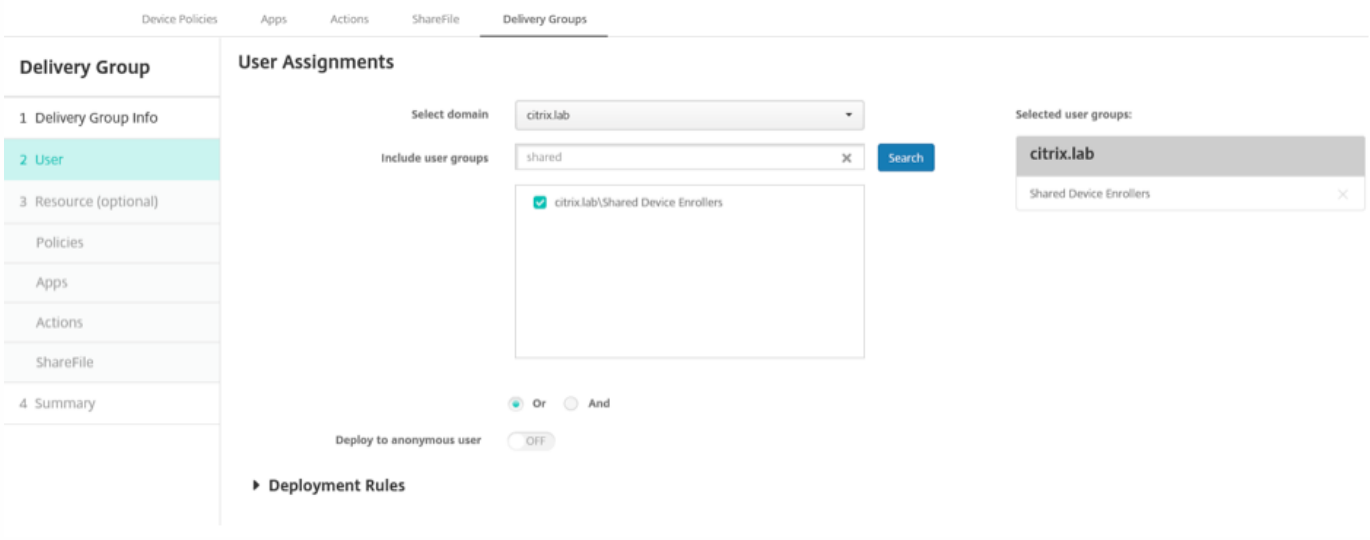
   [適用権限]で、デフォルト設定の**[すべてのユーザー グループ]**を保持するか、特定のActive Directoryユーザーグループに**[特定のユーザー グループ]**で権限を割り当てます。



［次へ］をクリックして［割り当て］画面に進みます。 作成したばかりの共有デバイス登録の役割を、前提条件の手順1で共有デバイス登録ユーザーのために作成したActive Directoryグループに割り当てます。 下の図で**citrix.lab**はActive Directoryドメイン、**Shared Device Enrollers**はActive Directoryグループです。



4. ユーザーがサインオンしていないときにデバイスに適用するベースポリシー、アプリケーション、アクションを含むデリバリーグループを作成し、共有デバイス登録ユーザーActive Directoryグループにそのデリバリーグループを関連付けます。



5. 共有するデバイスで、Worx Homeをインストールし、共有デバイス登録ユーザーアカウントを使用してXenMobileにデバイスを登録します。 XenMobileコンソールでデバイスを表示および管理できるようになります。 詳しくは、「デバイスの登録」を参照してください。

6. 認証されたユーザーに異なるポリシーを適用したり、追加のアプリケーションを提供するには、そのユーザーに関連付け、共有デバイスにのみ展開するデリバリーグループを作成する必要があります。 グループを作成するときは、展開規則を構成して、パッケージが共有デバイスに展開されるようにします。 詳しくは「展開規則の構成」を参照してください。

7. デバイスの共有を停止するには、選択的ワイプを実行して、共有デバイス登録ユーザーアカウントおよび展開されたアプリケーションとポリシーをデバイスから削除します。

共有デバイスのユーザーエクスペリエンス

ユーザーにはそのユーザーが使用できるリソースだけが表示され、すべての共有デバイスに同じエクスペリエンスが提供されます。 共有デバイス登録ポリシーとアプリは常にデバイスに残ります。 共有デバイス登録ユーザー以外のユーザーがWorx Homeにサインオンすると、そのユーザーのポリシーとアプリケーションがデバイスに展開されます。 ユーザーがサインオフすると、共有デバイス登録に必要とされているものを除いて、ポリシーおよびアプリケーションは削除されます。

共有デバイス登録ユーザーによって登録されると、WorxMailとWorxWebがデバイスに展開されます。 ユーザーデータはデバイスに安全に保持されます。 ユーザーがWorxMailまたはWorxWebにサインオンすると、データはほかのユーザーには表示されません。

Worx Homeにサインオンできるユーザーは、一度に1人だけです。 前のユーザーがサインオフしてからでないと、次のユーザーはサインオンできません。 セキュリティ上の理由から、共有デバイスにはユーザーの資格情報が保存されないので、ユーザーはサインオンのたびに資格情報を入力する必要があります。 前のユーザーのためのリソースに新しいユーザーがアクセスできないように、前のユーザーに関連付けられているポリシー、アプリケーション、データが削除されている間、新しいユーザーはサインオンできません。

共有デバイス登録によって、アプリケーションのアップグレード プロセスが変更されることはありません。 通常通り、共有

デバイスユーザーにアップグレードをプッシュし、共有デバイスユーザーはデバイス上でアプリケーションをアップグレードできます。

推奨されるWorxMailポリシー

- WorxMailの最適なパフォーマンスのためには、デバイスを共有するユーザーの数に応じて**[Max sync period]**を設定します。 無制限同期を許可することは推奨されません。

デバイスを共有するユーザーの数	推奨される［Max sync period］
21～25	1週間以内
6～20	2週間以内
5以下	1か月以内

- **［Enable contact export］**を禁止して、ユーザーの連絡先がデバイスを共有する他のユーザーにさらされないようにします。

- iOSでは、次の設定のみをユーザーごとに設定できます。 その他の設定は、デバイスを共有するユーザー間で共通になります。

  通知
  署名
  不在
  メール期間の同期
  S/MIME
  スペルチェック

XenMobileでのAndroid for Workによるデバイスの管理

Oct 25, 2016

Android for Workは、Android 5.0以降を実行するAndroidデバイスで使用できる安全なワークスペースであり、ビジネス用のアカウント、アプリ、データを個人用のアカウント、アプリ、データから分離します。 XenMobileでは、ユーザーにデバイスに個別のワークプロファイルを作成させることで、BYOD（Bring Your Own Device）と会社が所有するAndroidデバイスの両方を管理できます。このワークプロファイルと、ハードウェア暗号化、管理者が展開するポリシーを組み合わせることで、会社用の領域と個人用の領域がデバイス上で安全に分割されます。 会社用のすべてのポリシー、アプリ、およびデータをリモートで管理でき、ユーザーの個人用の領域に影響を与えずにデバイスからポリシー、アプリ、およびデータをワイプできます。サポートされているAndroidデバイスについて詳しくは、Googleのデバイスのページを参照してください。

XenMobileでは、Android 4.0～4.4を実行するデバイスを管理することもできます。そのためには、Android 5.0以降を実行するデバイスで作成されたワークスペースと同等の機能を提供するAndroid for Workアプリのダウンロードとインストールをユーザーに実行させます。

Google Play for Workを使用して、アプリを追加、購入、および承認し、デバイスのAndroid for Workワークスペースに展開します。 Google Play for Workを使用してプライベートなAndroidアプリ、パブリックアプリ、およびサードパーティアプリを公開することができます。 Android for Work用にパブリックアプリケーションストアの有料アプリをXenMobileに追加するときに、一括購入ライセンスの状態（使用できるライセンス数の合計、現在使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレス）を確認できます。 詳しくは、「XenMobileへのパブリックアプリケーションストアのアプリケーションの追加」を参照してください。

Android for Workの要件

- パブリックにアクセスできるドメイン
- Google管理者アカウント
- 管理プロファイル サポート実装のAndroid 5.0以上のLollipopを実行するデバイス、またはAndroid for Workアプリ実装のAndroid 4.0～4.4(Ice Cream Sandwich、Jelly Bean、およびKitKat）を実行するデバイス
- ユーザーの個人用プロファイルにGoogle Playがインストールされたgoogleアカウント
- デバイスで設定されたワークプロファイル

Android for Workアプリ制限を設定するには、次の手順を実行する必要があります。

- GoogleのAndroid for Work設定タスクを完了します。
- 一連のGoogle Play資格情報を作成します。
- Android for Workサーバー設定を構成します。
- 少なくとも1つAndroid for Workデバイスポリシーを作成します。
- Google Play for WorkアプリストアでAndroid for Workアプリを追加、購入、および承認します。

Android for Workを管理する場合は、次のリンクを使用できます。

- Google管理コンソール：https://admin.google.com/AdminHome
- Play for Work管理コンソール：https://play.google.com/work/apps
- プライベートチャネルおよびセルフホストアプリケーションのPlay公開 :https://play.google.com/apps/publish
- サービスアカウント作成のためのGoogle Developer's Console :https://console.developers.google.com

XenMobileでAndroid for Workを管理するには、以下の作業が必要です。

- Android for Workアカウントの作成
- サービスアカウントのセットアップ
- Android for Work証明書のダウンロード
- Google Admin SDKおよびMDM APIの有効化。
- ディレクトリとGoogle Playを使用するためのサービスアカウントの承認。
- バインドトークンを入手します。

次のセクションでは、このそれぞれのタスクの実行方法を説明します。 これらのタスクを完了すると、XenMobileで一連のGoogle Play資格情報を作成し、Android for Work設定を構成して、Android for Workアプリを管理できます。

> **警告**
>
> サードパーティの既知の問題が存在することから、XenMobileコンソールを使用してAndroid for Workを有効にできない場合があります。 この問題の詳細と、回避策としてのサーバープロパティの構成方法については、「XenMobile Server 10.3の既知の問題」の#615118を参照してください。

Android for Workアカウントの作成

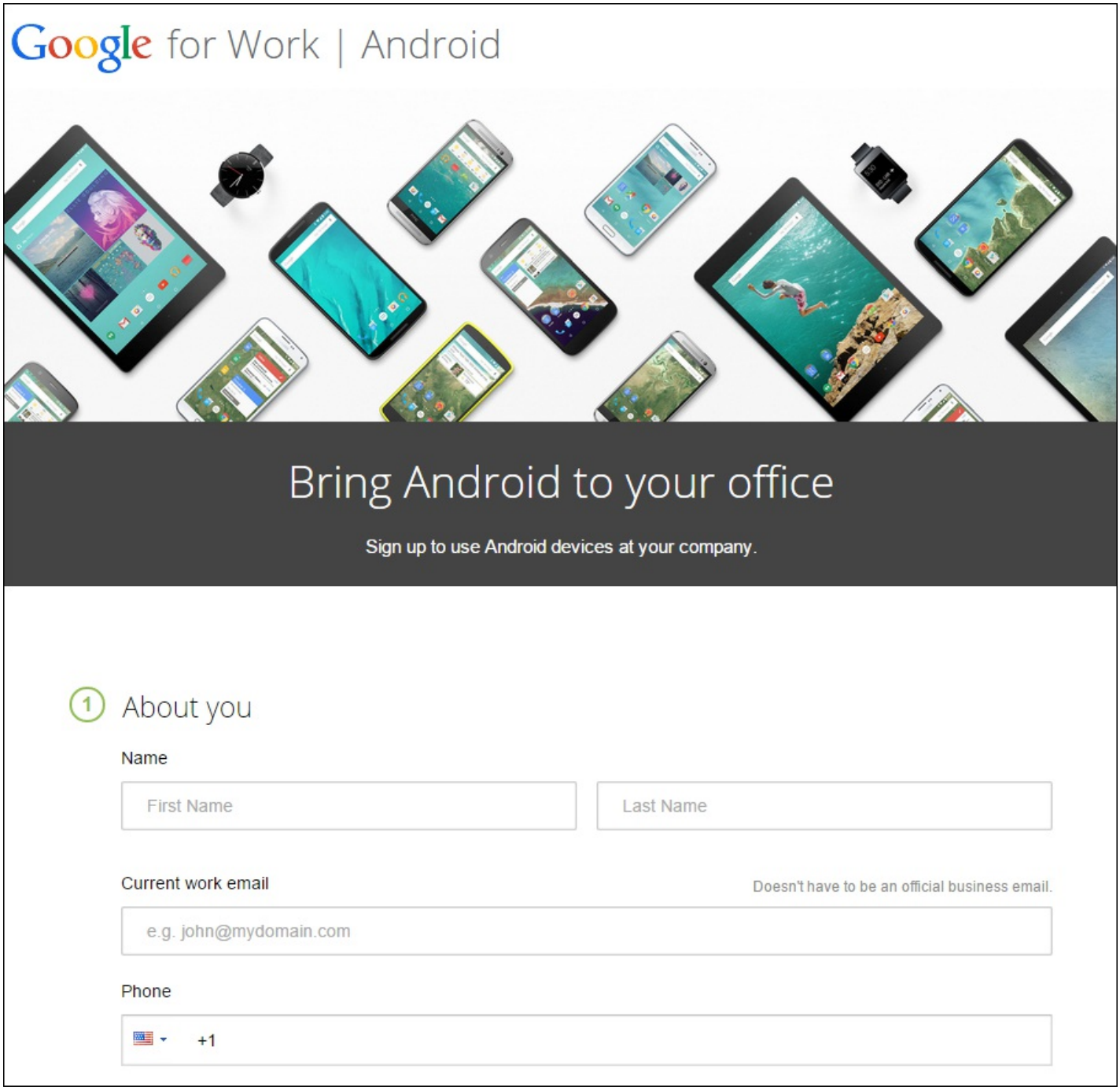
Android for Workアカウントを構成する前に、以下の前提条件を満たす必要があります。

- ドメイン名（たとえば、example.com）を所有している必要があります。
- Googleにドメインの所有権を検証させる必要があります。
- EMM（Enterprise Mobility Management：エンタープライズモビリティ管理）プロバイダー（XenMobile 10.1以降）を介して、Android for Workを有効化し、管理する必要があります。

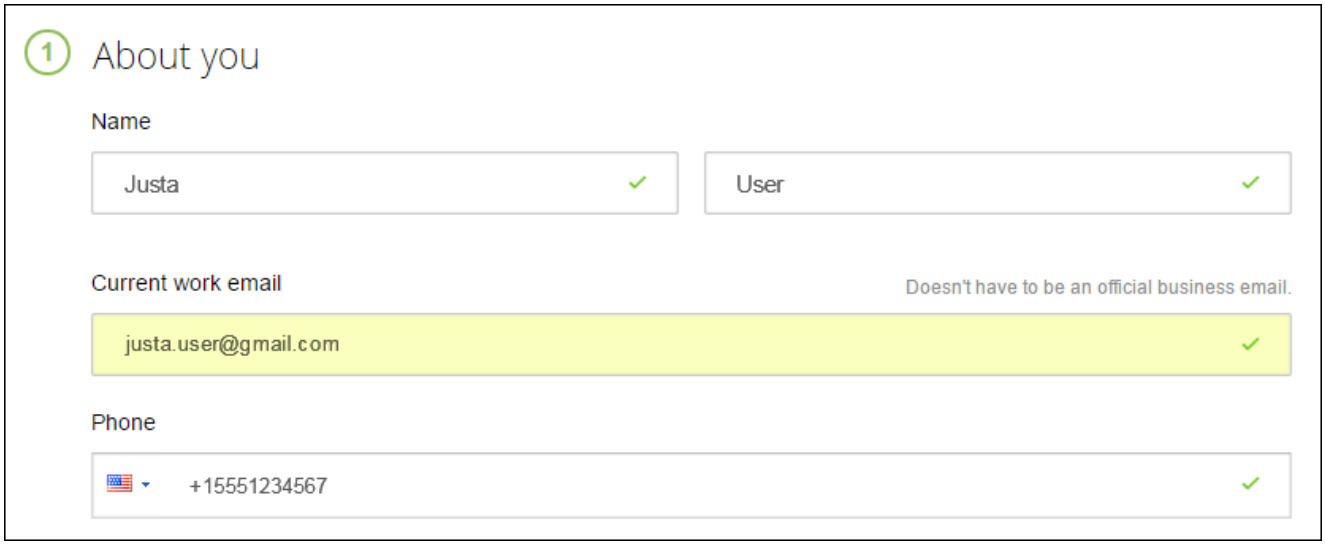
ドメイン名がすでにGoogleで検証済みの場合は、「Android for Workサービスアカウントの設定とAndroid for Work証明書のダウンロード」の手順をスキップできます。

1. https://www.google.com/a/signup/?enterprise_product=ANDROID_WORKにアクセスします。

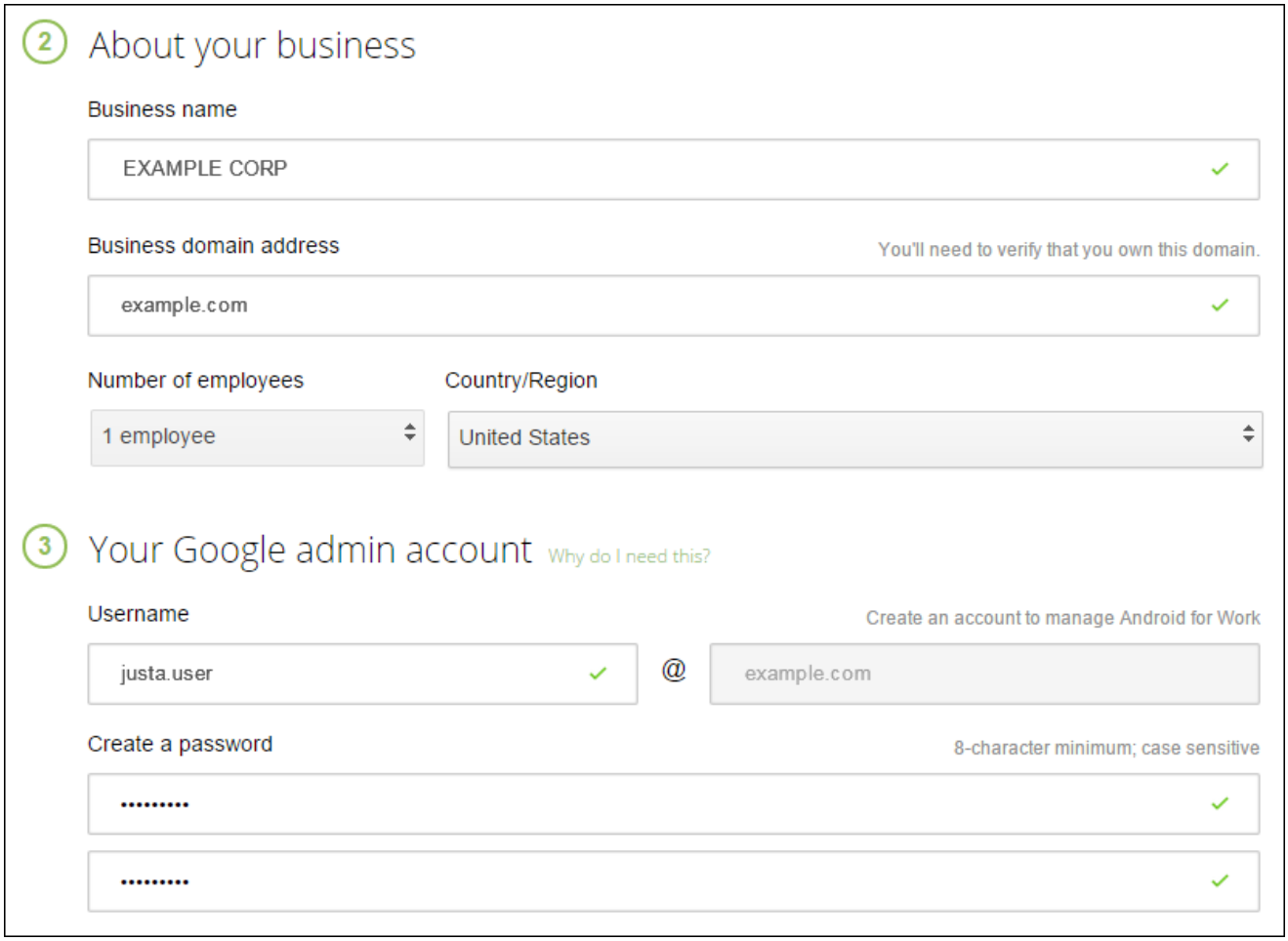
以下のページが表示されるので、管理者情報と会社情報を入力します。



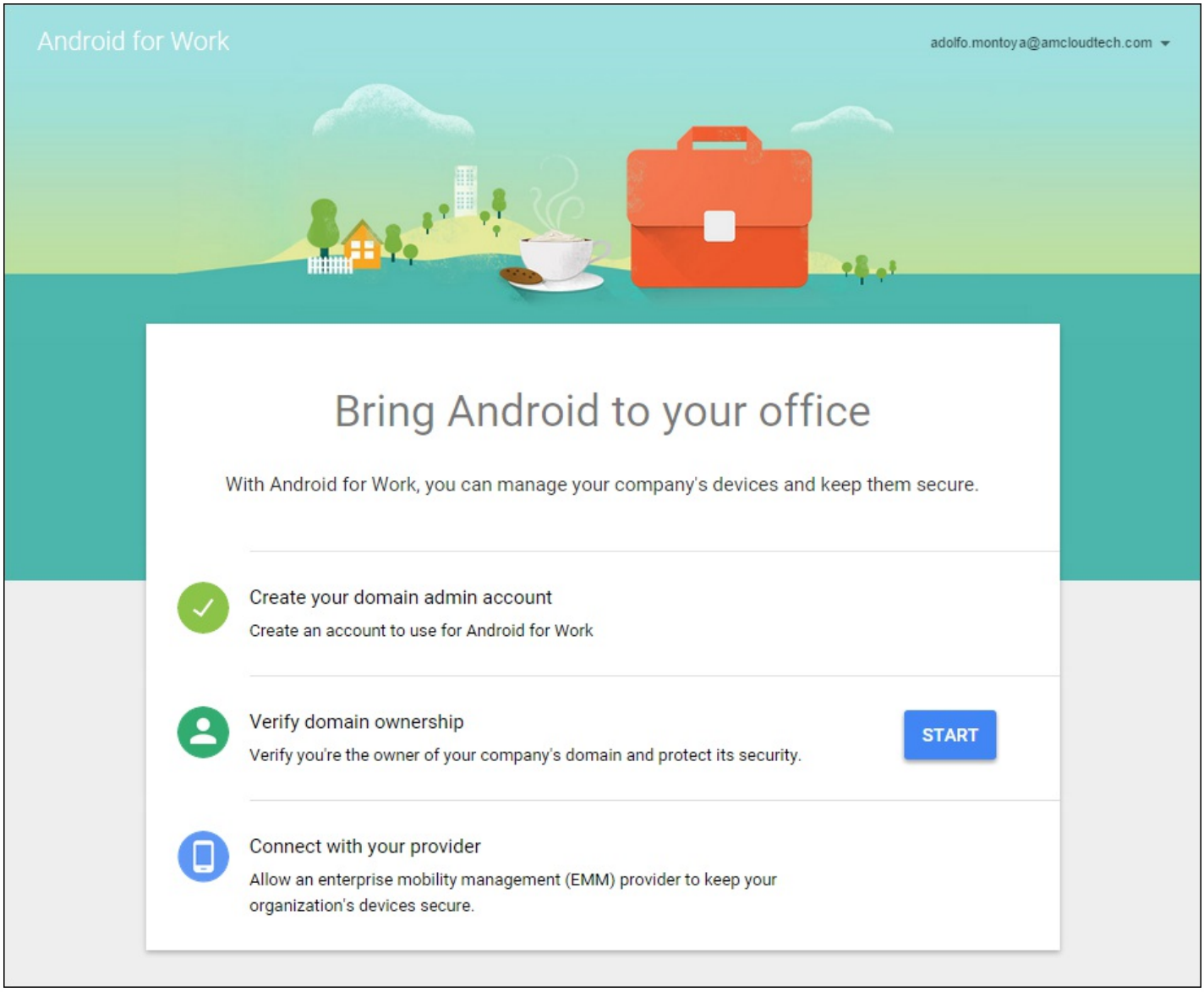
2.管理者のユーザー情報を入力します。



3.会社情報と管理者アカウント情報を入力します。



プロセスの最初の手順が完了します。以下のページが開きます。

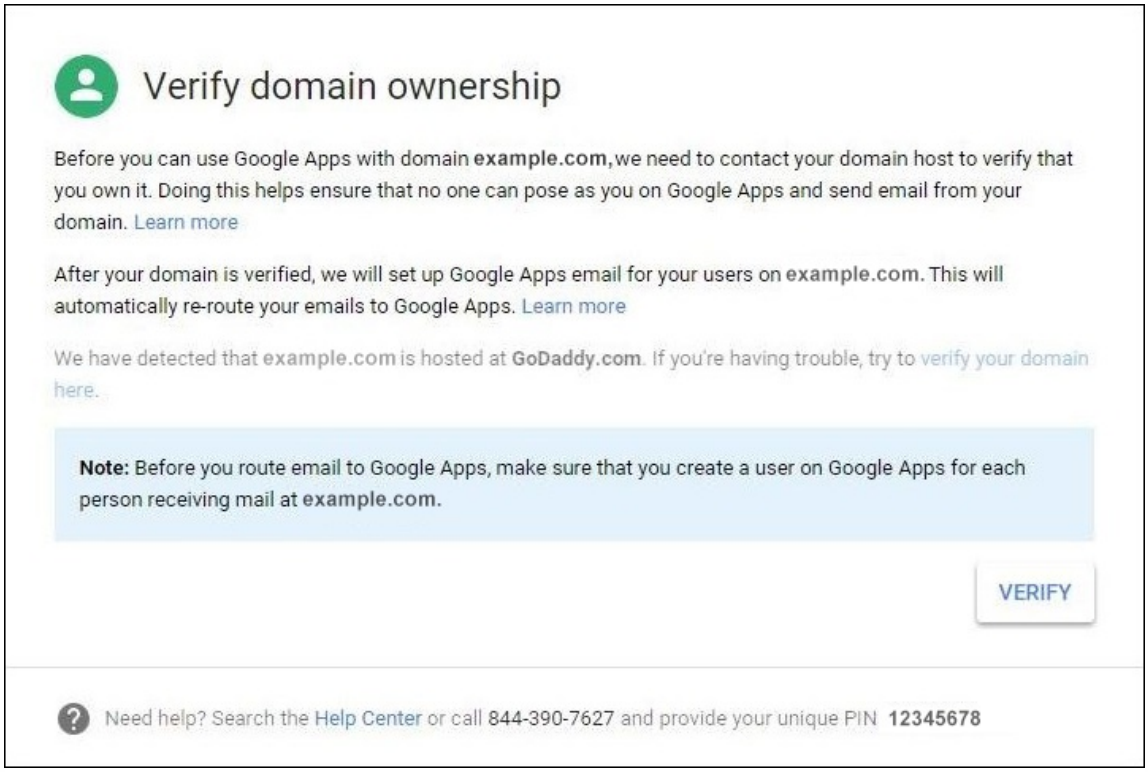


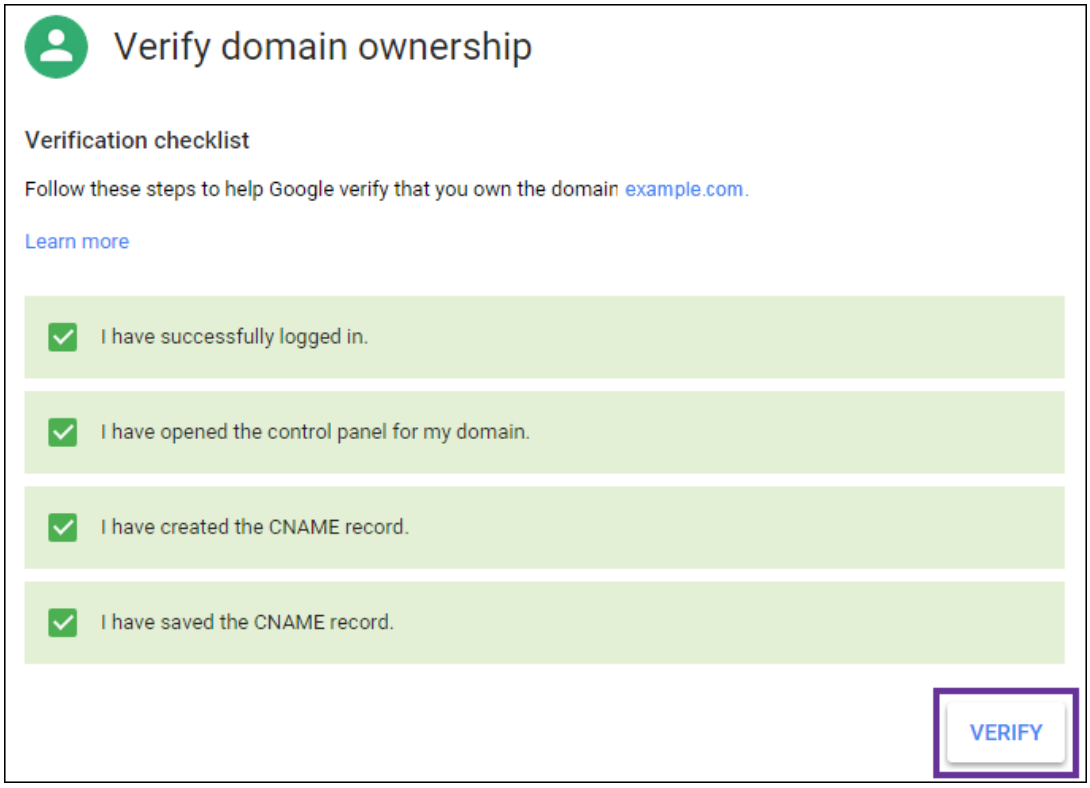
ドメイン所有権の検証

ここで、Googleにドメインの検証を許可する必要があります。 ドメインの検証方法には3つあります。ドメインホストのWeサイトにTXTまたはCNAMEレコードを追加するか、ドメインのWebサーバーにHTMLファイルをアップロードするか、タグをホームページに追加します。 Googleでは最初の方法を推奨しています。 ドメインの所有権を検証する手順についてはこの記事では扱いませんが、必要な情報はhttps://support.google.com/a/answer/6095407/に記載されています。

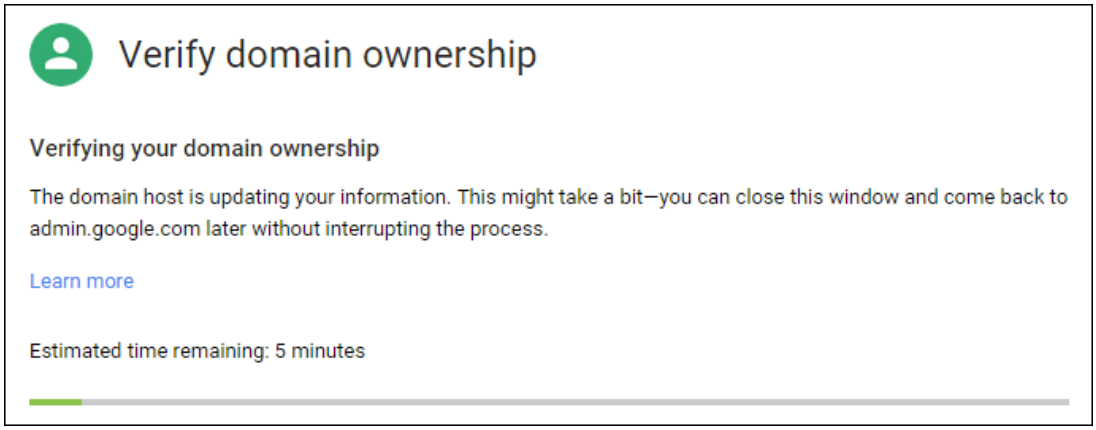
1. **[Start]** をクリックして、ドメインの検証を開始します。 **[Verify domain ownership]** ページが開きます。 画面の指示に従ってドメインを検証します。

2. 完了したら、 **[Vetiry]** をクリックします。

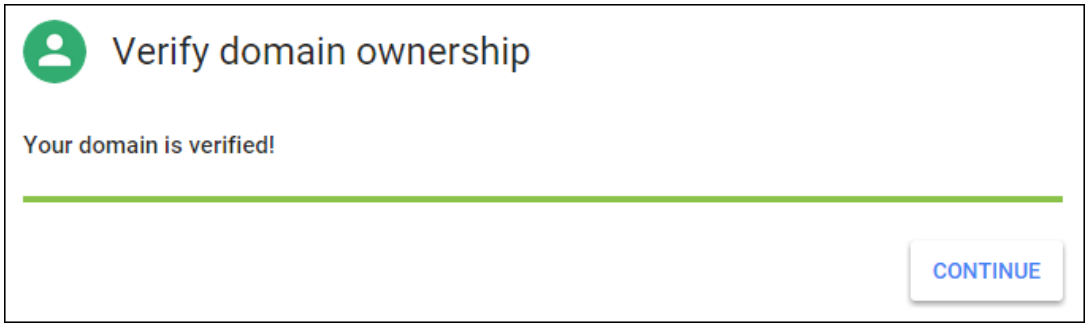




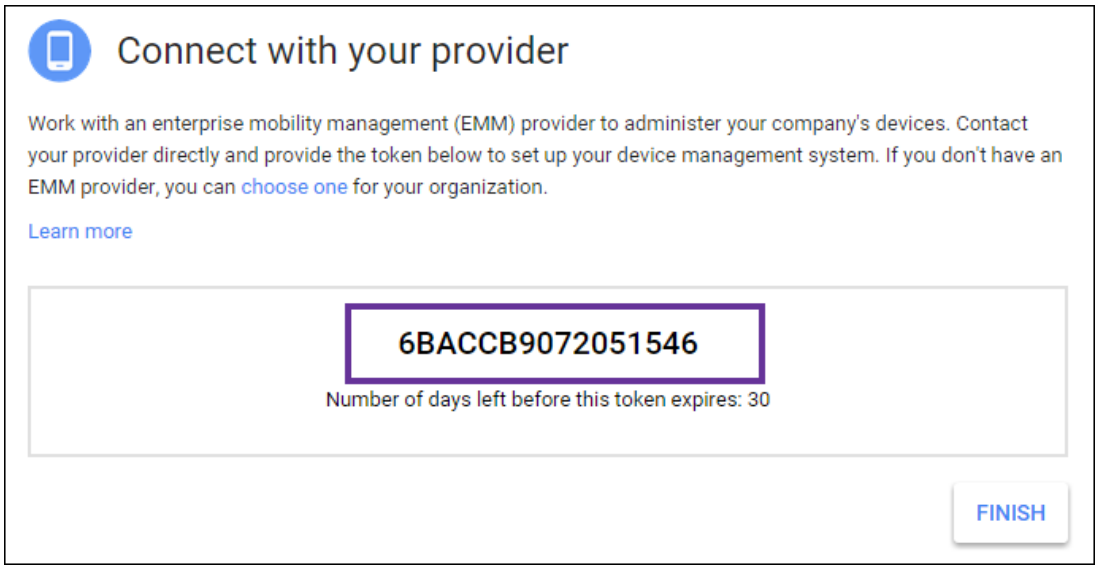
3. Googleによってドメイン所有権が検証されます。



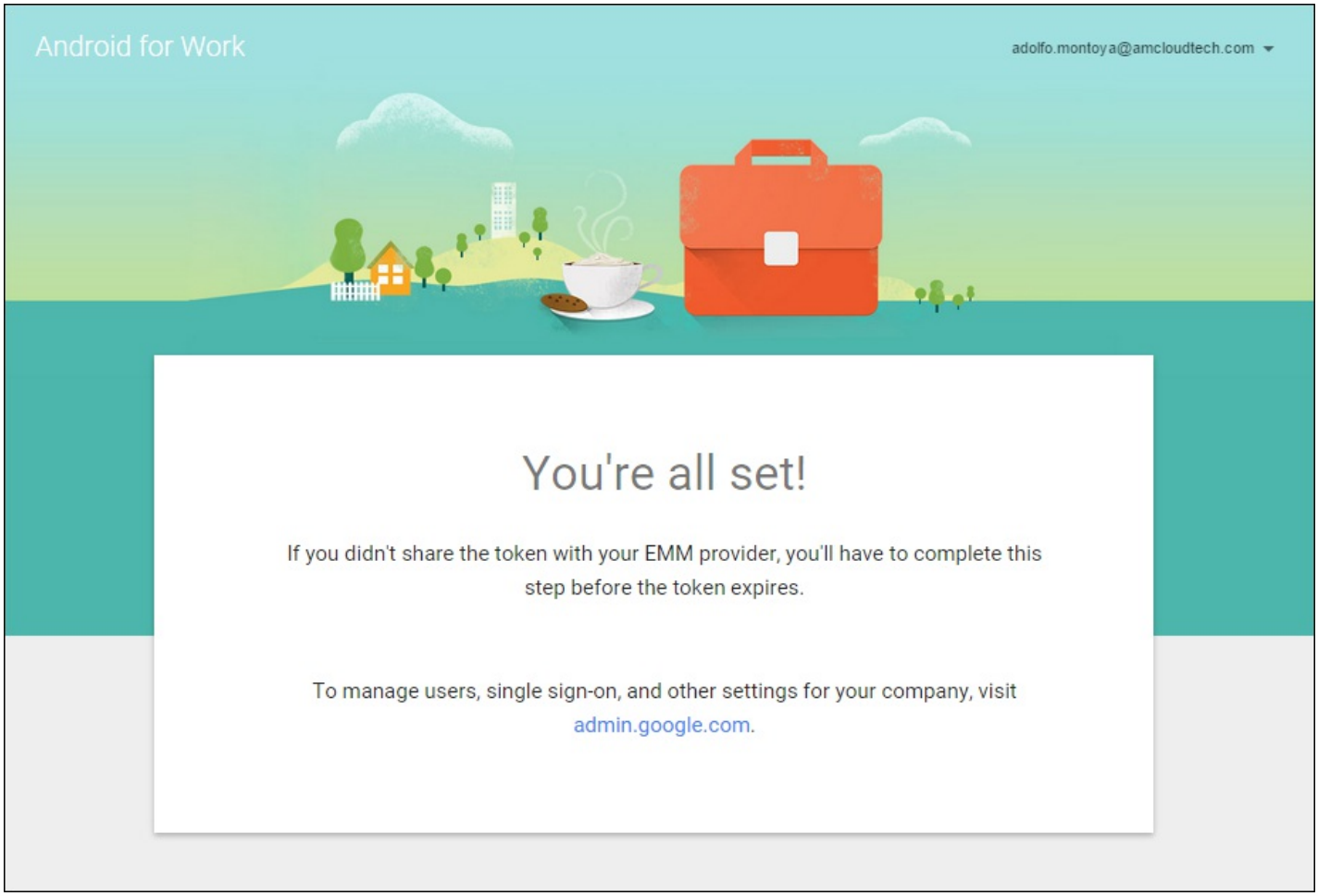
4.検証が成功すると、次のページが開きます。 **[続ける]** をクリックします。



5. Citrixに提供しAndroid for Work設定を構成するときに使用するEMMバインドトークンが、Googleによって作成されます。トークンをコピーして保存します。後でセットアップ中に必要になります。



6. **[Finish]** をクリックしてAndroid for Workの設定を完了します。



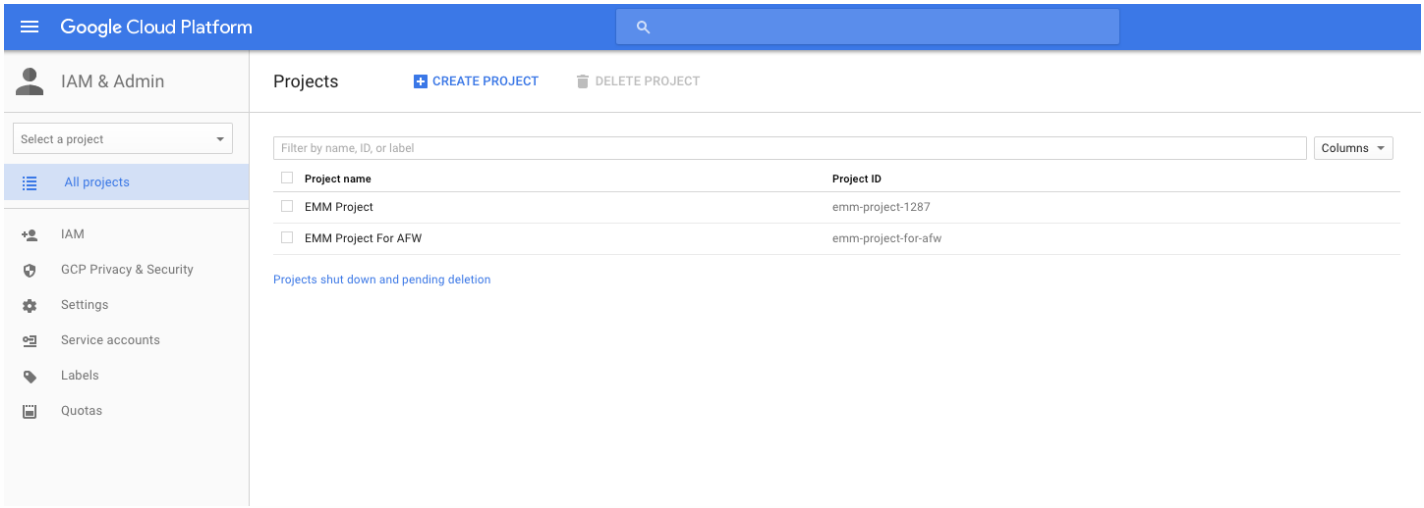
Android for Workサービスアカウントを作成すると、Google Adminコンソールにログオンして Android for Workのモビリティ管理設定を管理できます。

Android for Workサービスアカウントの設定とAndroid for Work証明書のダウンロード

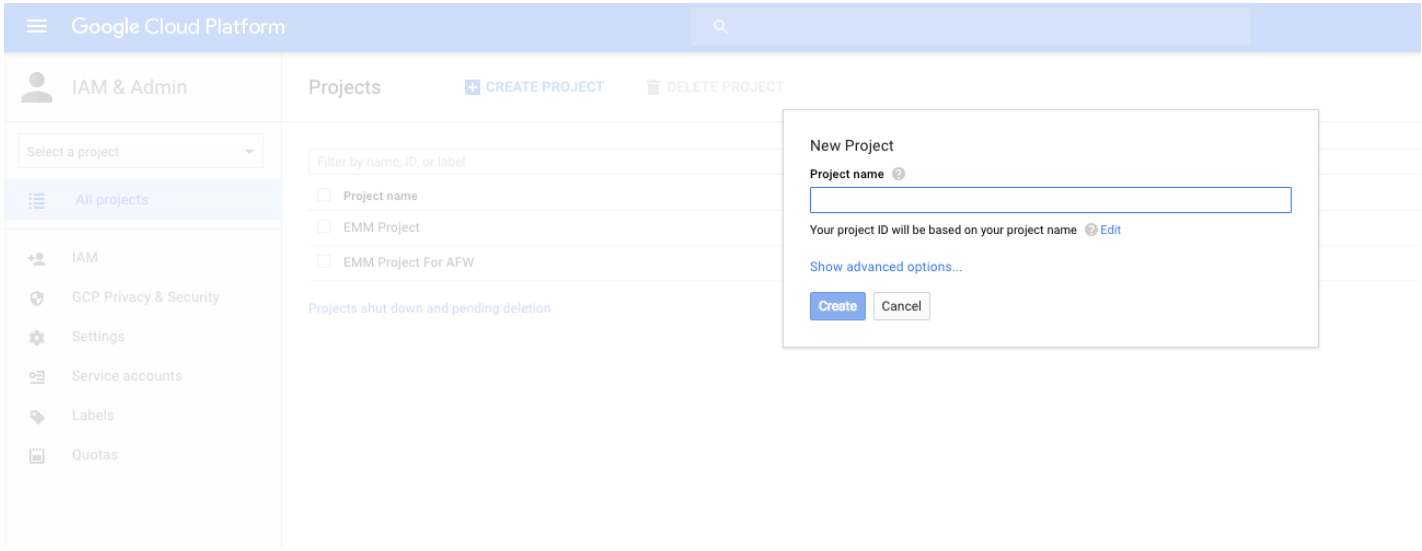
XenMobileからGoogle PlayサービスおよびDirectoryサービスにアクセスできるようにするには、Googleのデベロッパー用プロジェクトポータルを使用して新しいサービスアカウントを作成する必要があります。 このサービスアカウントは、XenMobileとAndroid for Work用のGoogleの各種サービスのサーバー間通信で使用します。 使用されている承認プロトコルについて詳しくは、https://developers.google.com/identity/protocols/OAuth2ServiceAccountを参照してください。

1. Webブラウザーでhttps://console.cloud.google.com/projectを開いて、Google管理者の資格情報でログオンします。

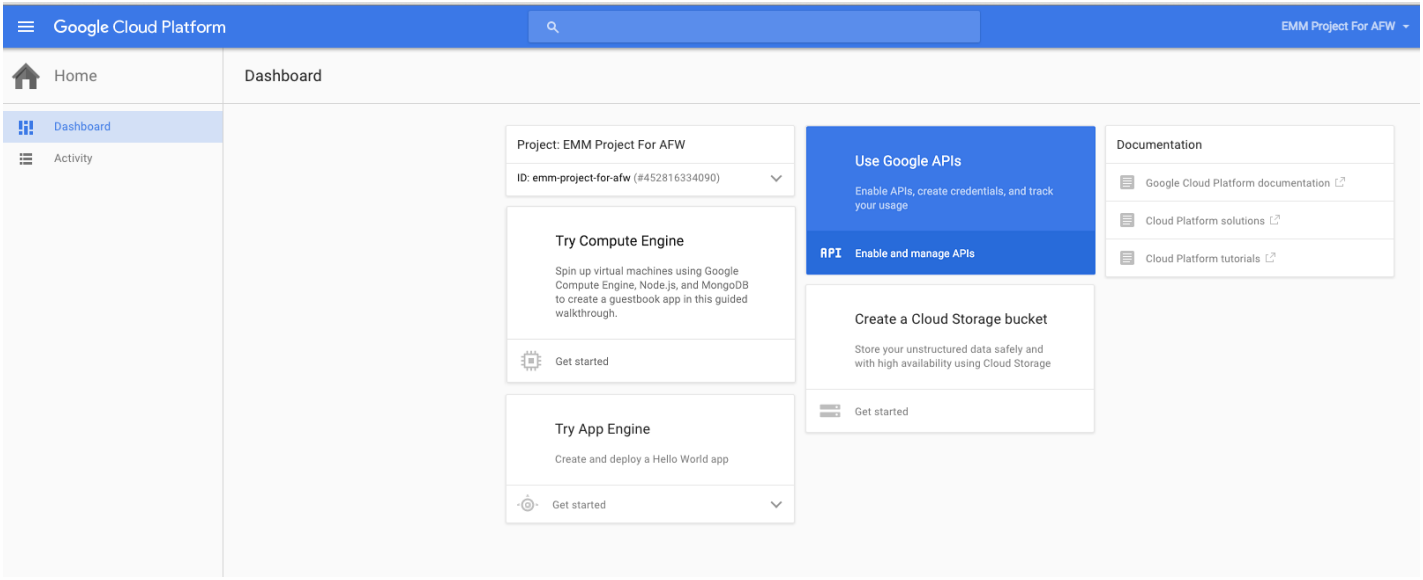
2. **[Projects]**の一覧で、 **[Create Project]**をクリックします。



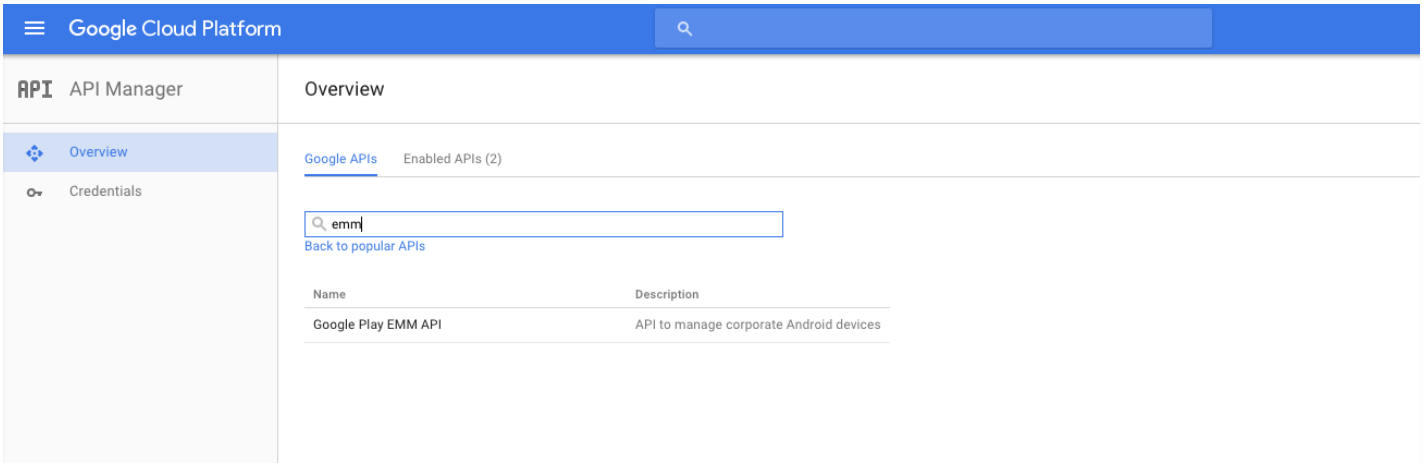
3. ［**Project name**］ボックスに、プロジェクトの名前を入力します。



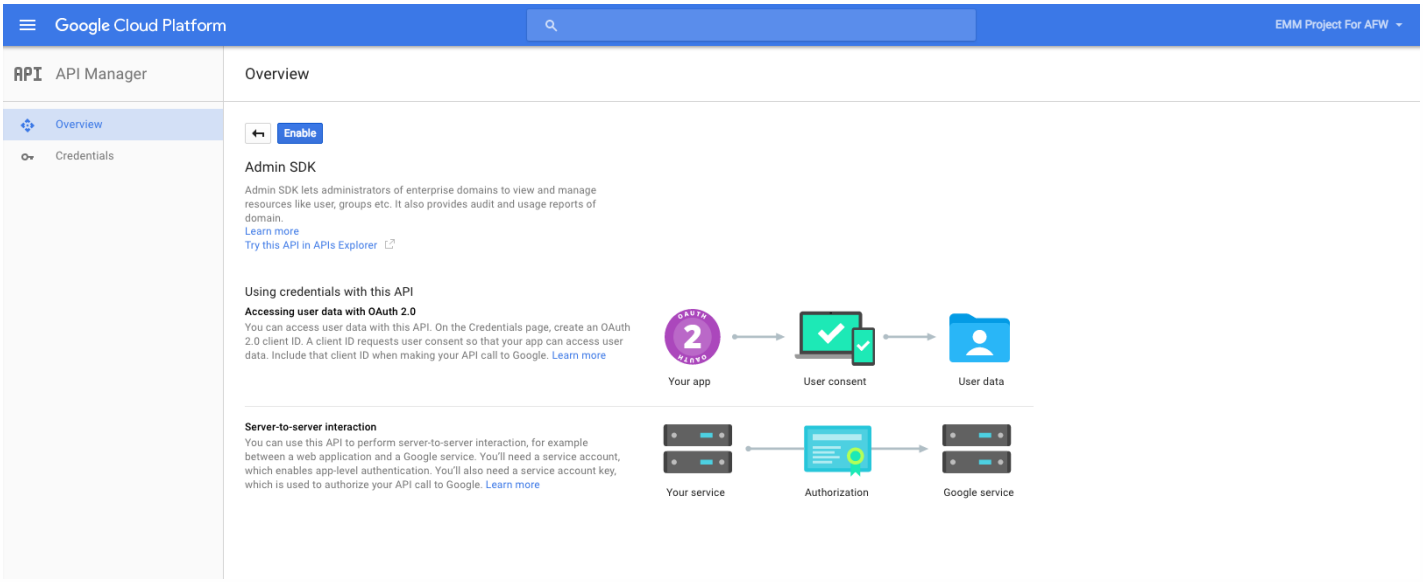
4. ［Dashboard］ページで、［**Use Google APIs**］をクリックします。



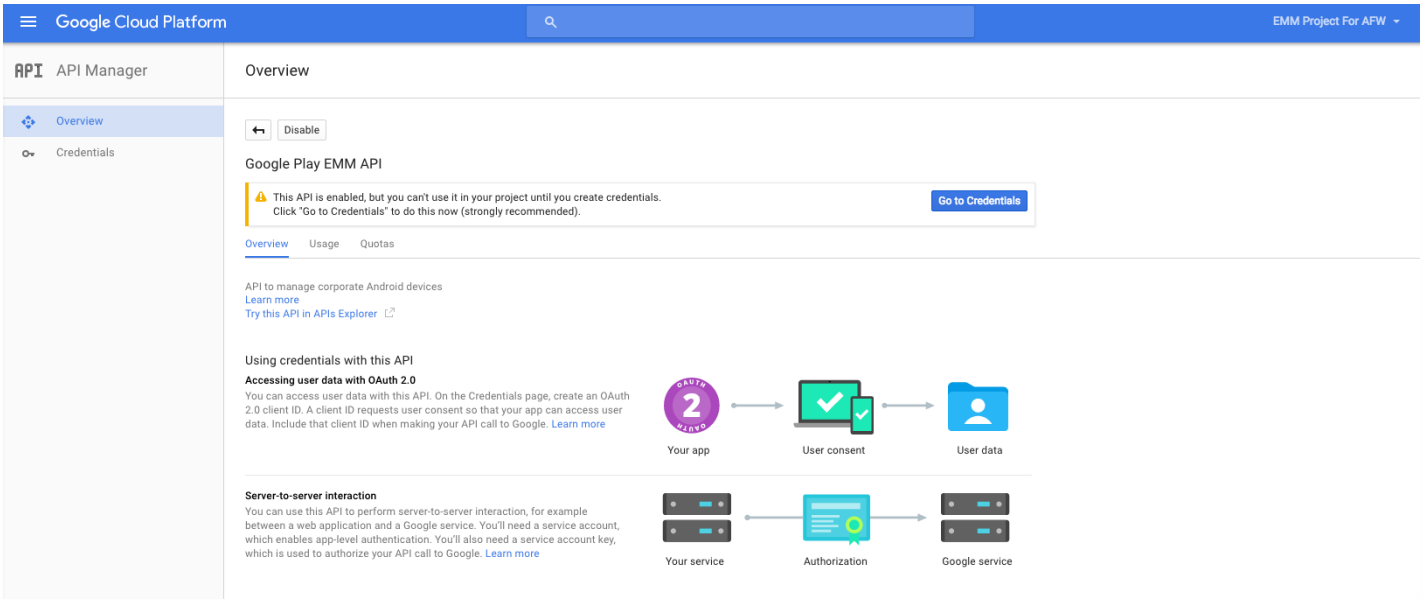
5. ［Google APIs］ページの［**Search**］ボックスに「**EMM**」と入力し、その検索結果をクリックします。



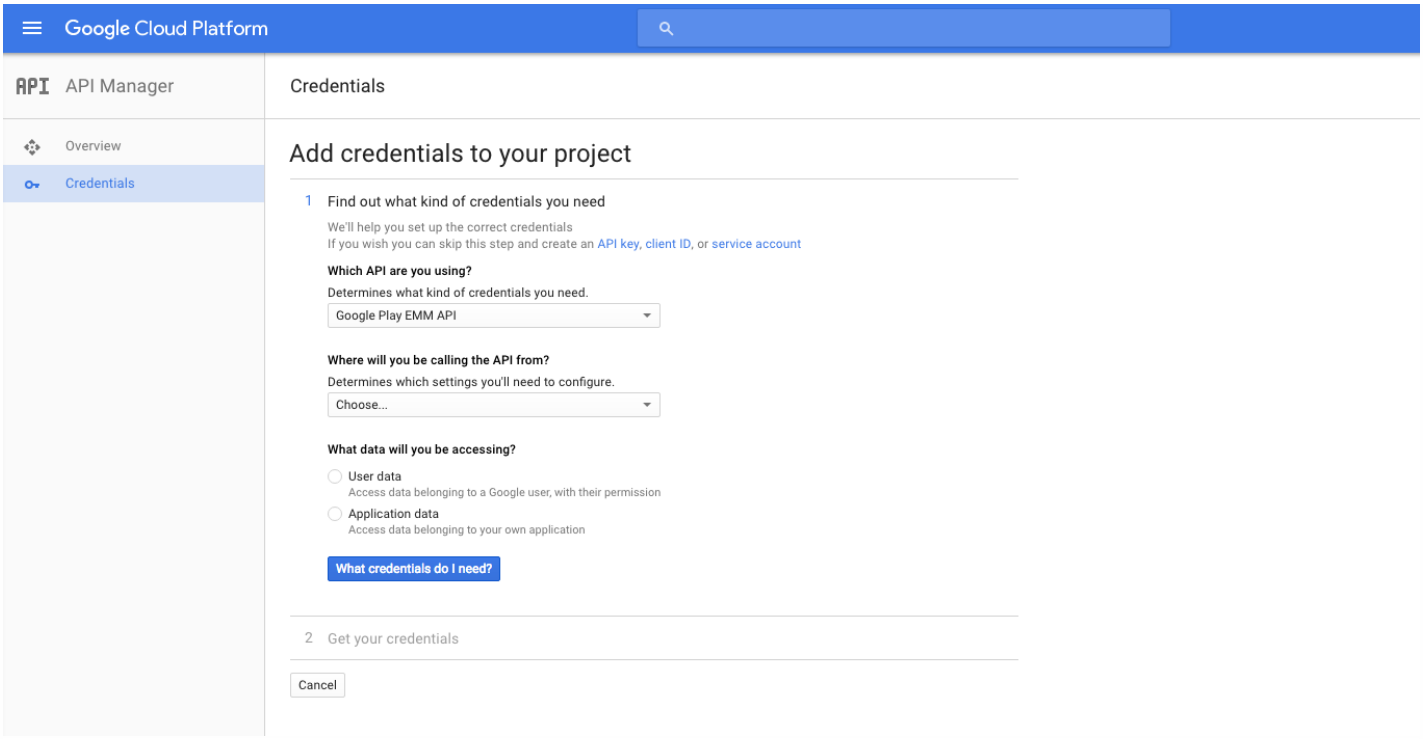
6. ［Overview］ページで、［**Enable**］をクリックします。



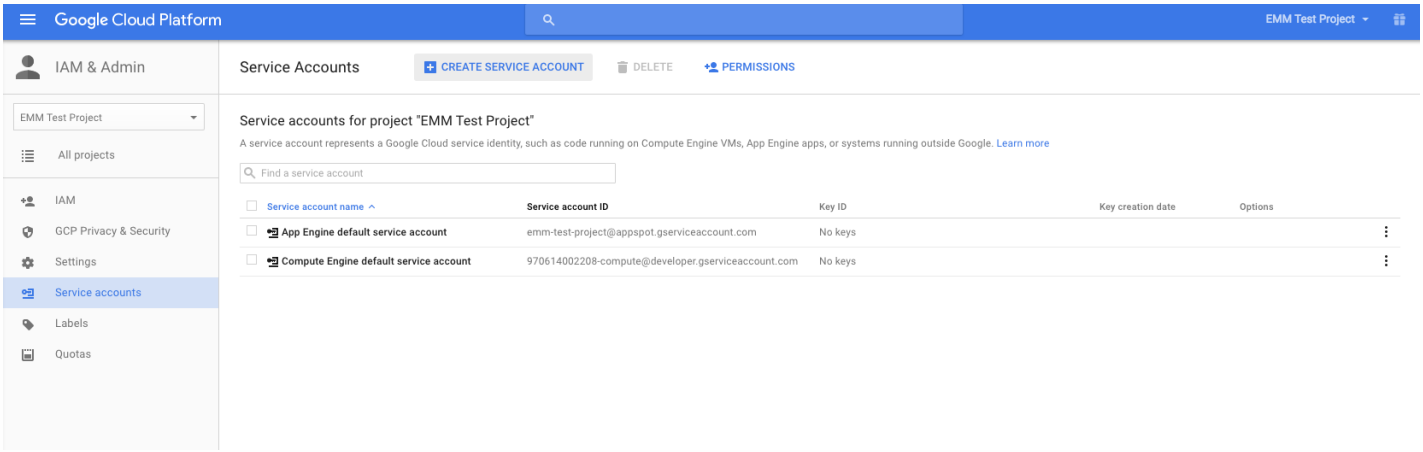
7. [**Google Play EMM API**] の横にある [**Go to Credentials**] をクリックします。



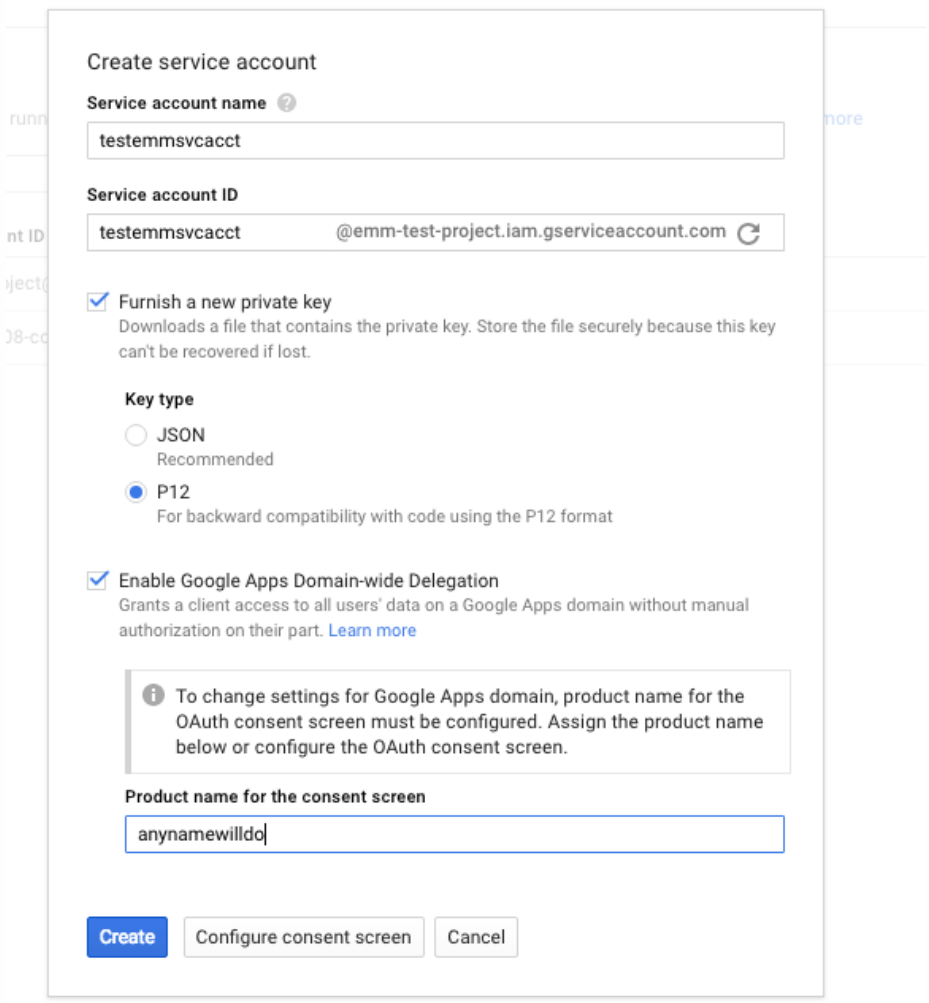
8. [**Add credentials to our project**] の一覧の手順1で、 [**service account**] をクリックします。



9. [**Service Accounts**] ページで、 [**Create Service Account**] をクリックします。

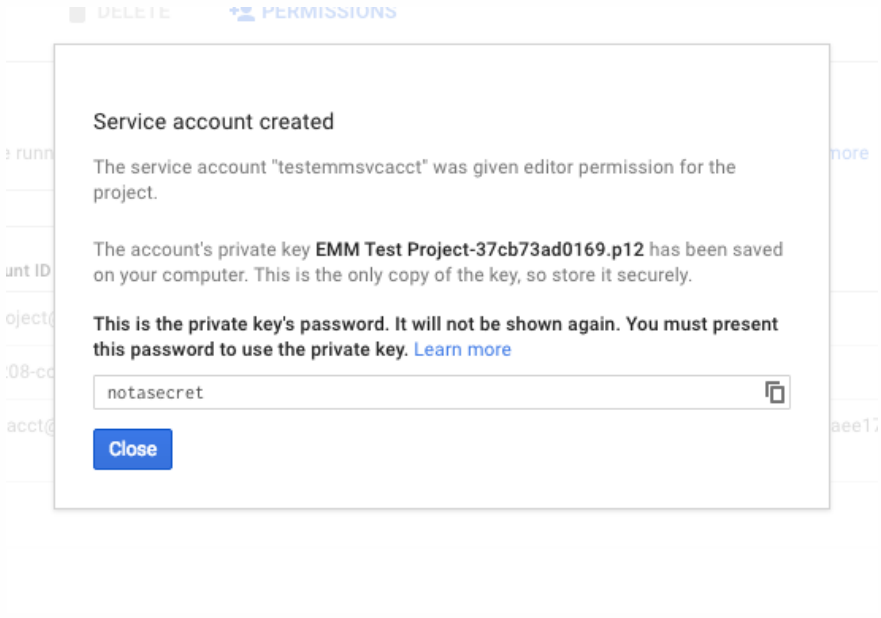


10. [**Create service account**] で、 [**Furnish a new private key**] チェックボックスをオンにし、 [**P12**] を選択します。 [**Enable Google Apps Domain-wide Delegation**] チェックボックスをオンにして、 [**Create**] をクリックします。

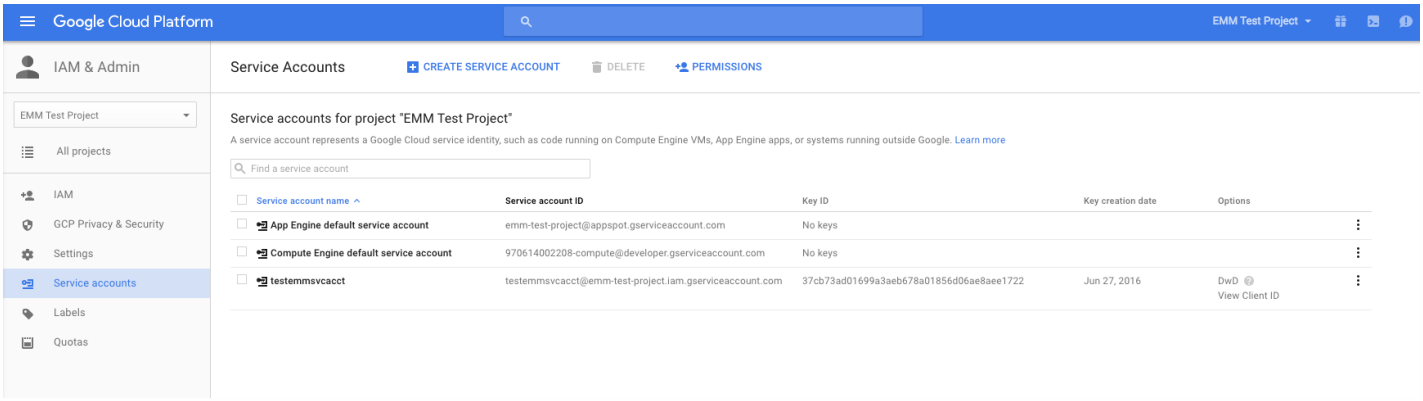


証明書（P12ファイル）がコンピューターにダウンロードされます。 証明書を安全な場所に保存してください。

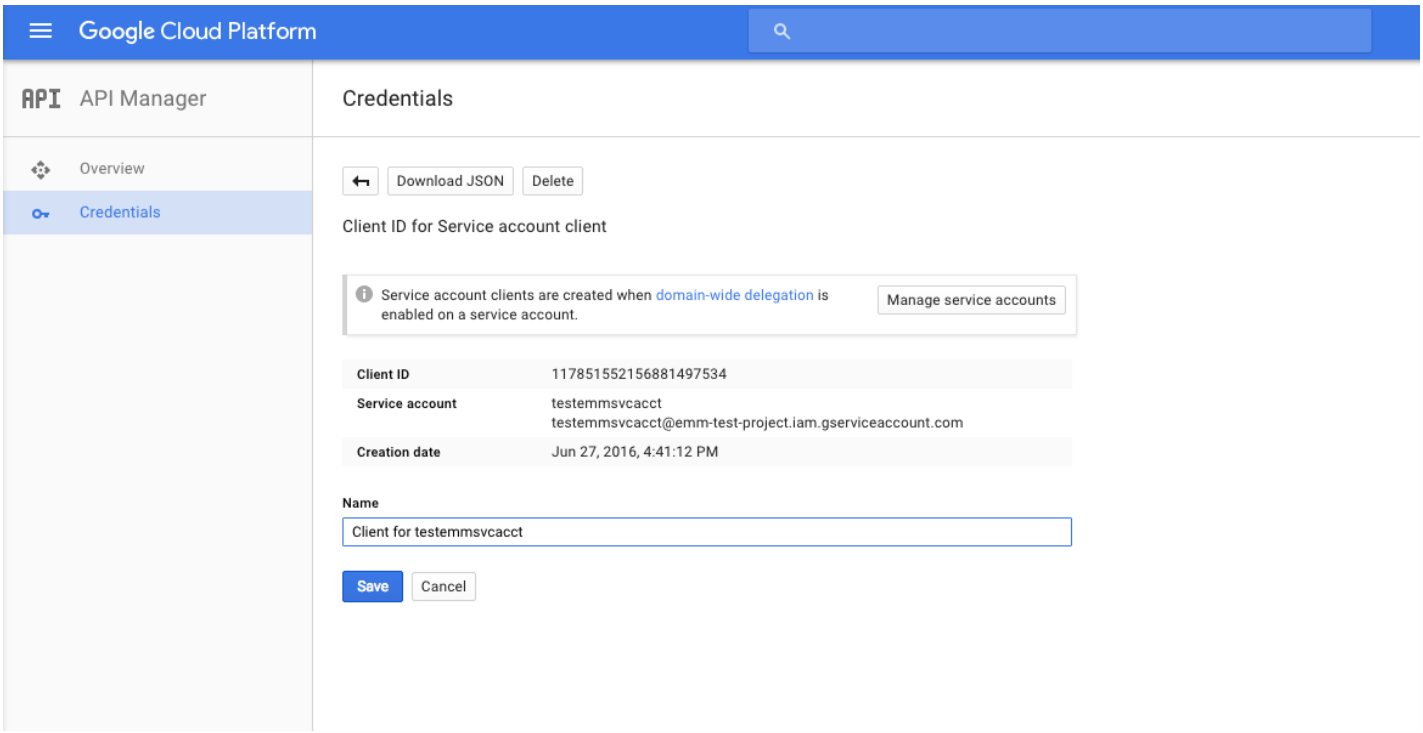
11. **[Service account created]**確認画面で、 **[Close]**をクリックします。



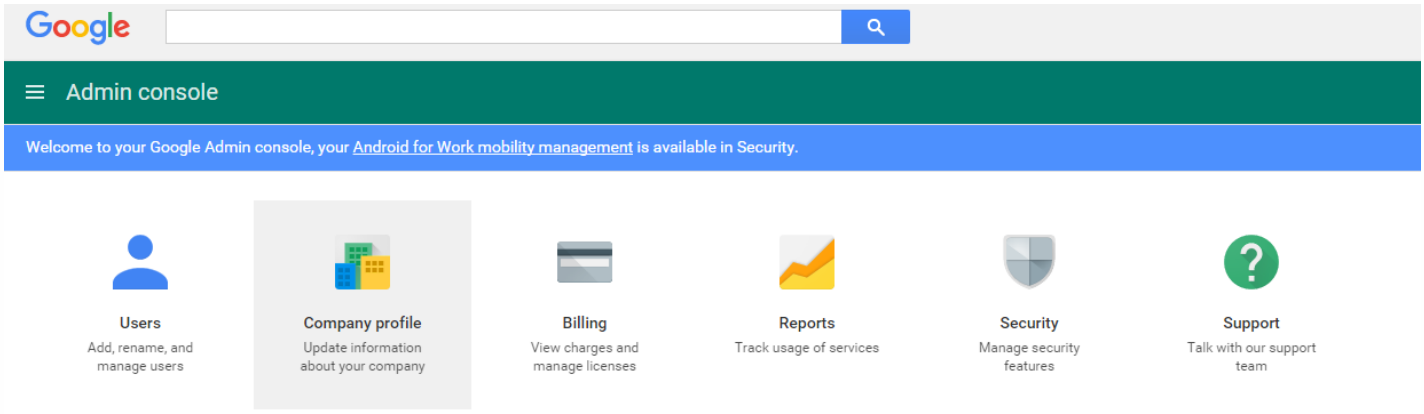
12. **[Permissions]** ページで **[Service accounts]** をクリックし、サービスアカウントの **[Options]** の下で、 **[View Client ID]** をクリックします。



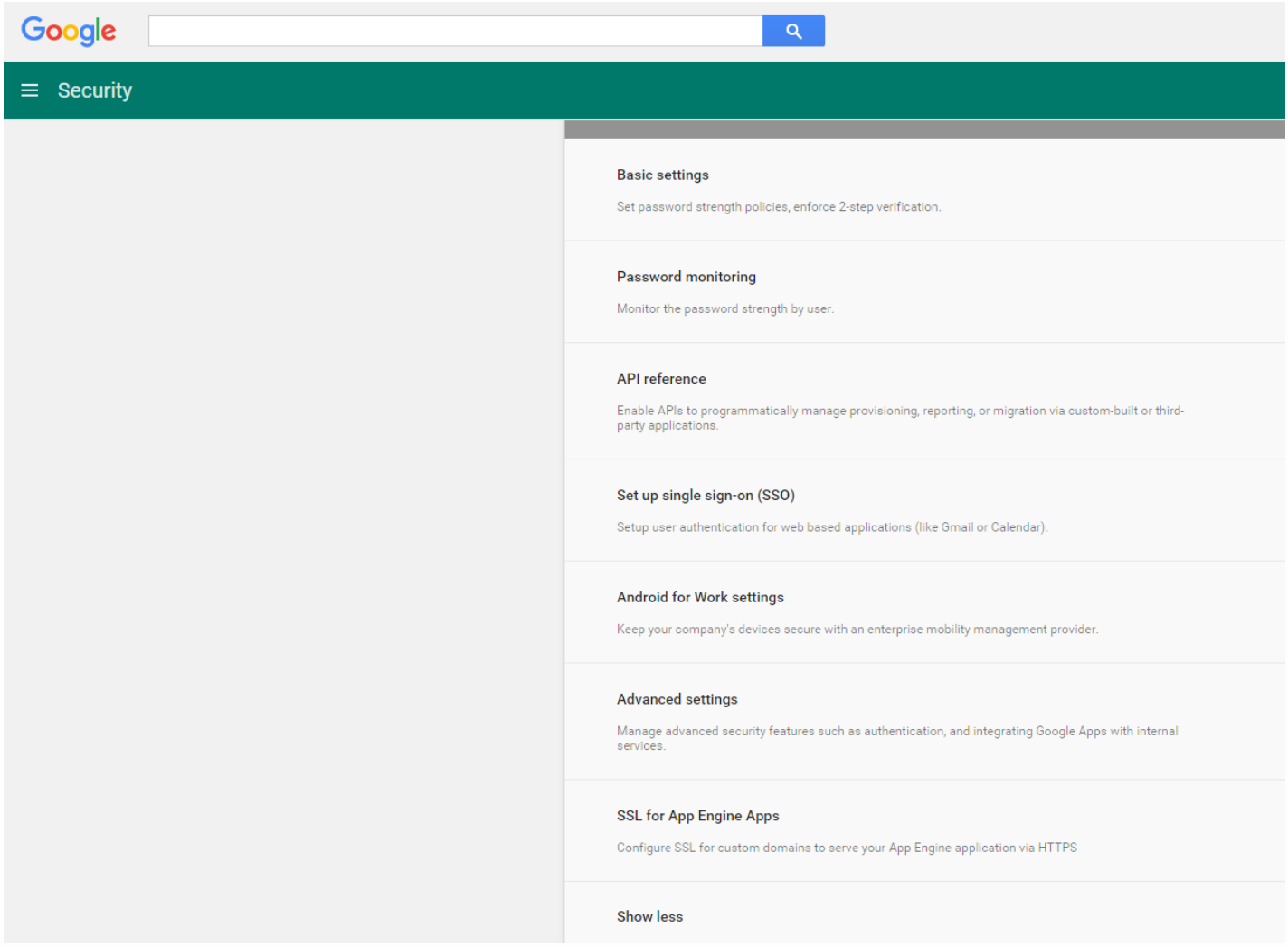
13. Google管理コンソールでアカウントの承認に必要になる詳細情報が表示されます。 **[Client ID]** と **[Service account ID]** を、後でこの情報を引き出せる場所にコピーします。 この情報は、ドメイン名と共に、ホワイトリスト作成の目的でCitrixサポートに送信する際に必要になります。



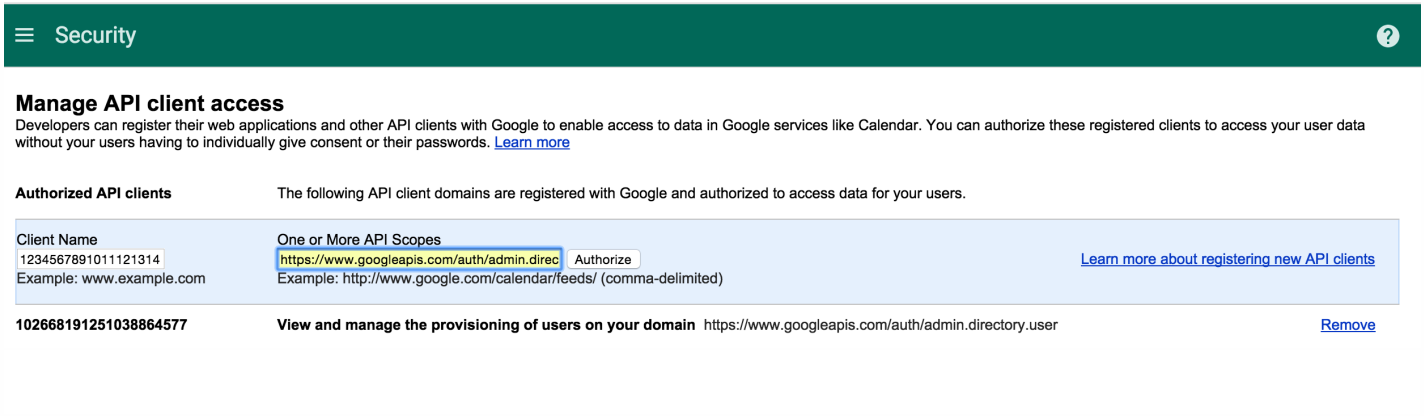
14. 自分のドメインのGoogle管理コンソールを開き、 **[Security]** をクリックします。



15. **[Android for Work settings]** をクリックします。



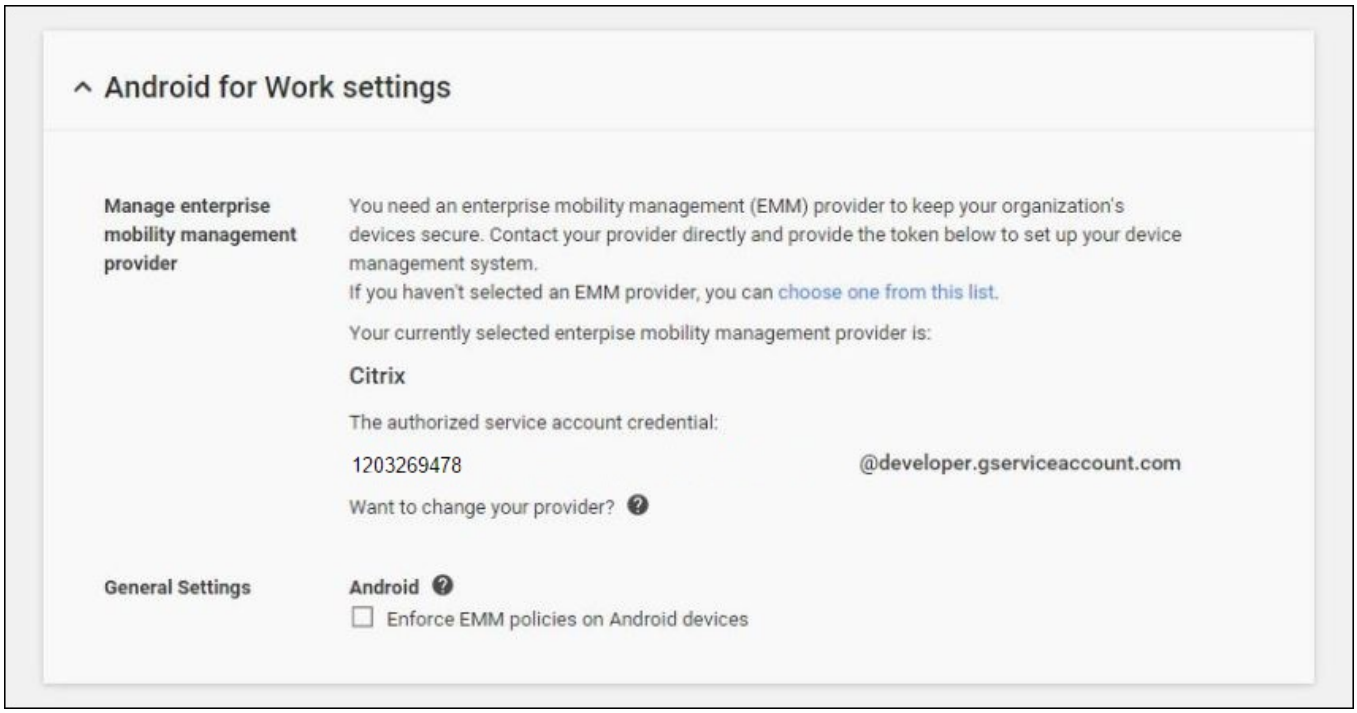
16. **[Client Name]** ボックスに前の手順で保存したクライアントIDを入力し、**[One or More API Scopes]** ボックスに「https://www.googleapis.com/auth/admin.directory.user」と入力して、 **[Authorize]** をクリックします。



XenMobileを使用してAndroid for Workデバイスを管理するには、Citrixテクニカルサポート（https://www.citrix.com/contact/technical-support.html）にドメイン名、サービスアカウント、およびバインド トークンを伝える必要があります。 CitrixはトークンをEMM（Enterprise Mobility Management：エンタープライズモビリティ管理）プロバイダーとしてのXenMobileにバインドします。

1. バインドを確認するには、Google Adminポータルにログオンして**[Security]**をクリックします。

2. **[Android for Work settings]**をクリックします。 Google Android for WorkアカウントがEMMプロバイダーとしてのCitrixにバインドされていることが表示されます。

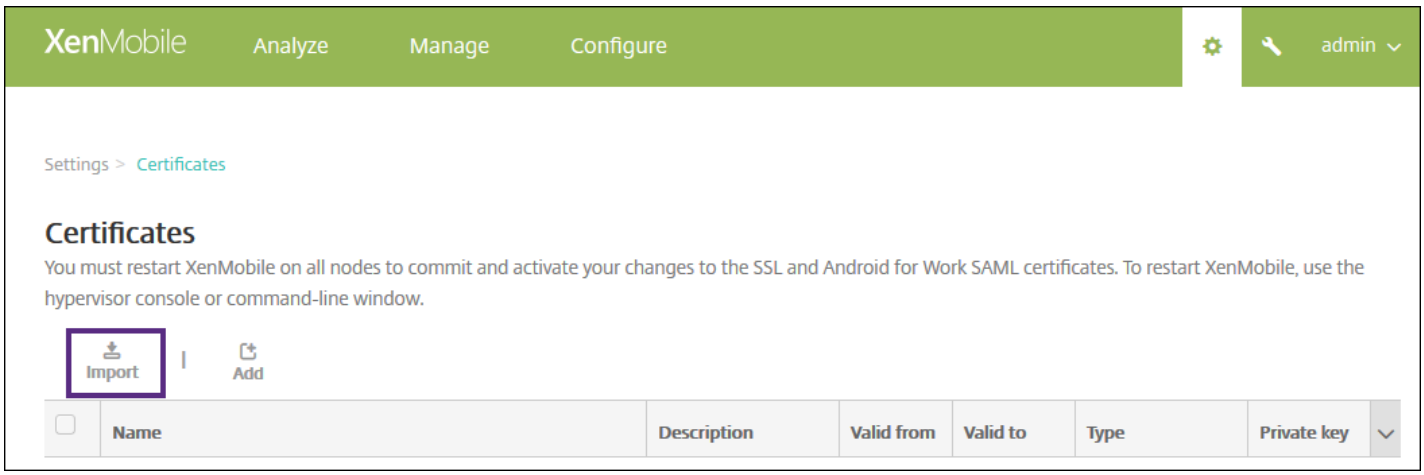


トークンのバインドを確認した後で、XenMobileを使用してAndroid for Workデバイオスの管理を開始できます。 手順14.で生成したP12証明書をインポートし、Android for Workサーバー設定をセットアップし、SAMLベースのシングルサインオンを有効化し、少なくとも1つAndroid for Workデバイスポリシーを定義する必要があります。

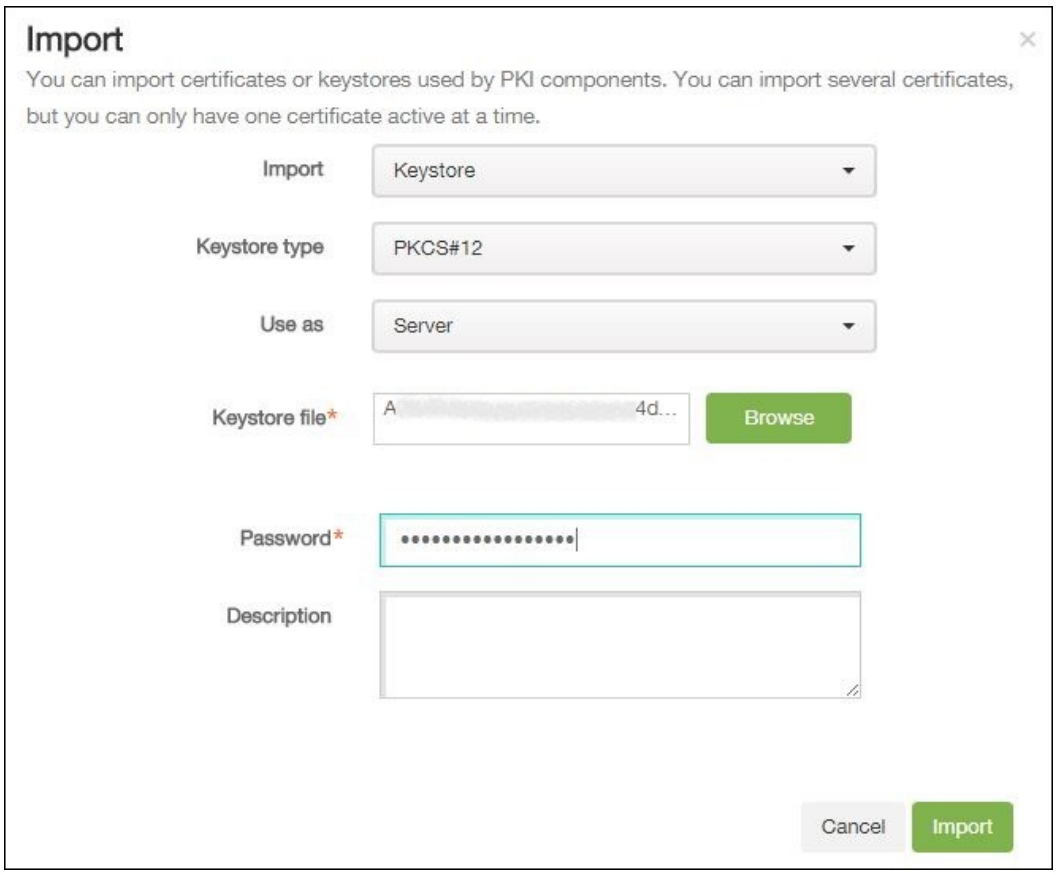
以下の手順に従ってAndroid for WorkのP12証明書をインポートします。

1. XenMobileコンソールにログオンします。

2. コンソールの右上にある歯車アイコンをクリックして **[Settings]** ページを開き、 **[Certificates]** をクリックします。 **[Certificates]** ページが開きます。



3. **[Import]** をクリックします。 **[Import]** ダイアログボックスが開きます。



次の設定を構成します。

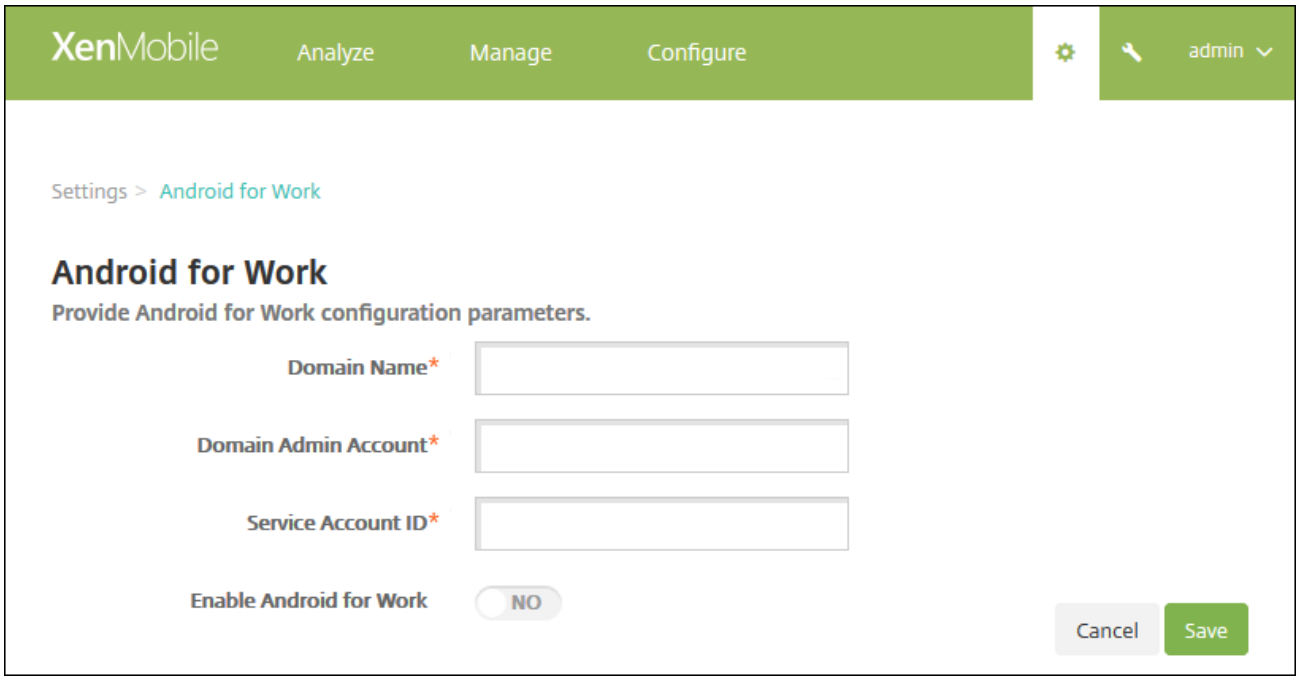
- **Import**：ボックスの一覧から、 **[Keystore]** を選択します。
- **Keystore type**：ボックスの一覧から、 **[PKCS#12]** を選択します。

- **Use as**：ボックスの一覧から、［**Server**］を選択します。
- **Keystore file**：［**Browse**］をクリックして、P12証明書を選択します。
- **Password**：キーストア のパスワードを入力します。
- **Description**：任意で、証明書の説明を入力します。

4. ［**Import**］をクリックします。

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

2. ［**Server**］の下の［**Android for Work**］をクリックします。［**Android for Work**］ページが開きます。



次の設定を構成します。

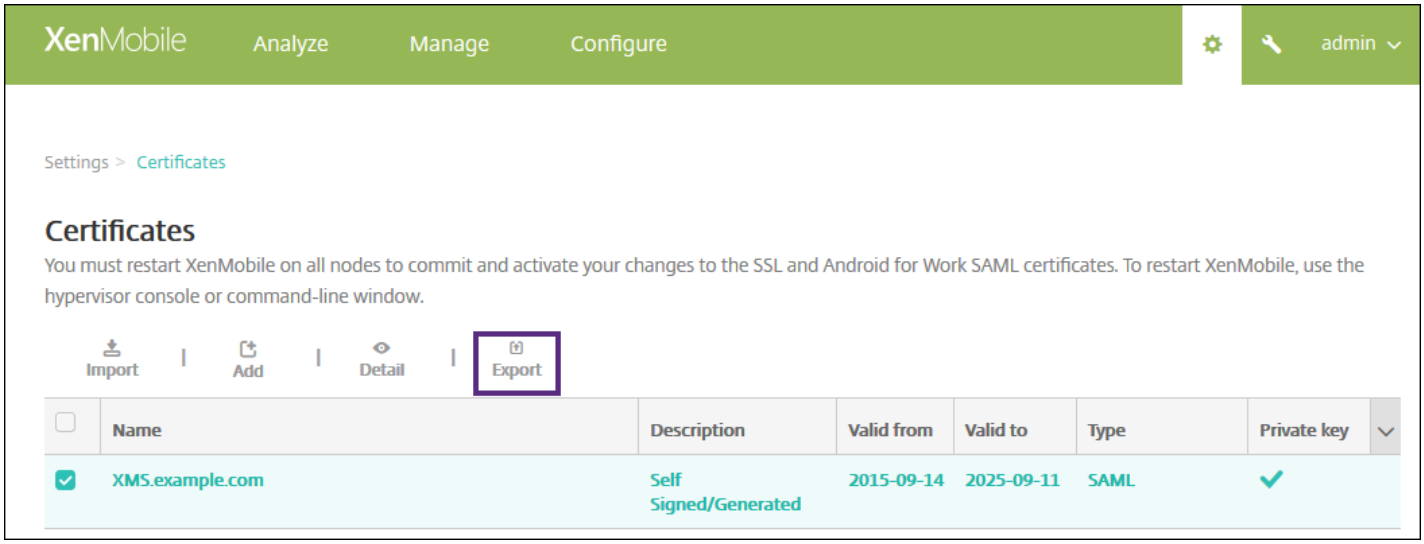
- **Domain name**：Android for Workのドメイン名を入力します（例：domain.com）。
- **Domain Admin Account**：ドメイン管理者のユーザー名を入力します（例：Google Developer Portalで使用しているメールアカウント）。
- **Service Account ID**：サービスアカウントIDを入力します（例：Google Service Accountに関連付けられたメールアドレス（serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com））。
- **Enable Android for Work**：クリックして、Android for Workを有効または無効にします。

3. ［**Save**］をクリックします。

1. XenMobileコンソールにログオンします。

2. コンソールの右上にある歯車アイコンをクリックします。［**Settings**］ページが開きます。

3. ［**Certificates**］をクリックします。［**Certificates**］ページが開きます。

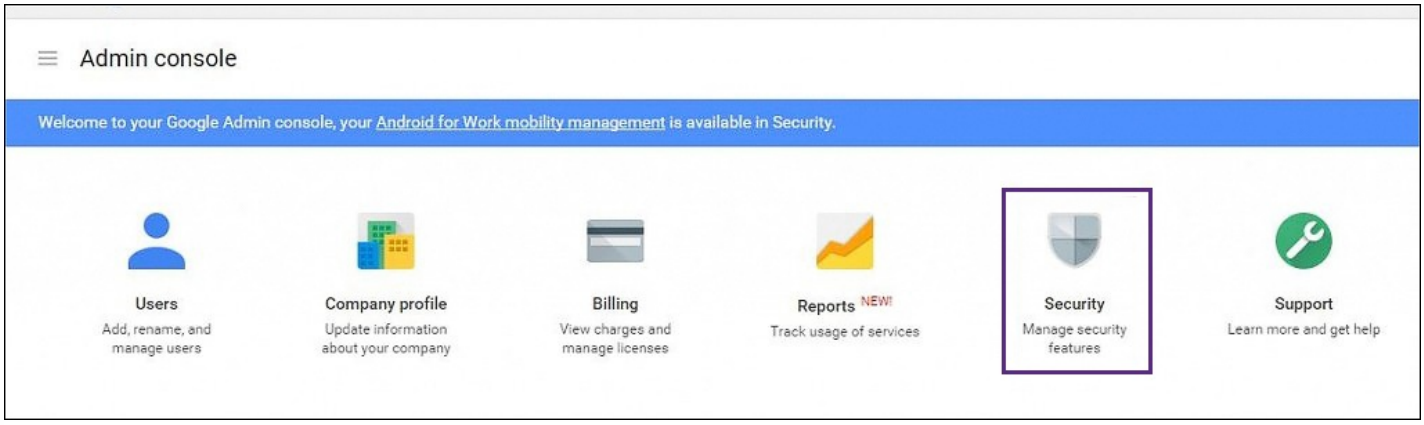


3. 証明書の一覧から、SAML証明書を選択します。

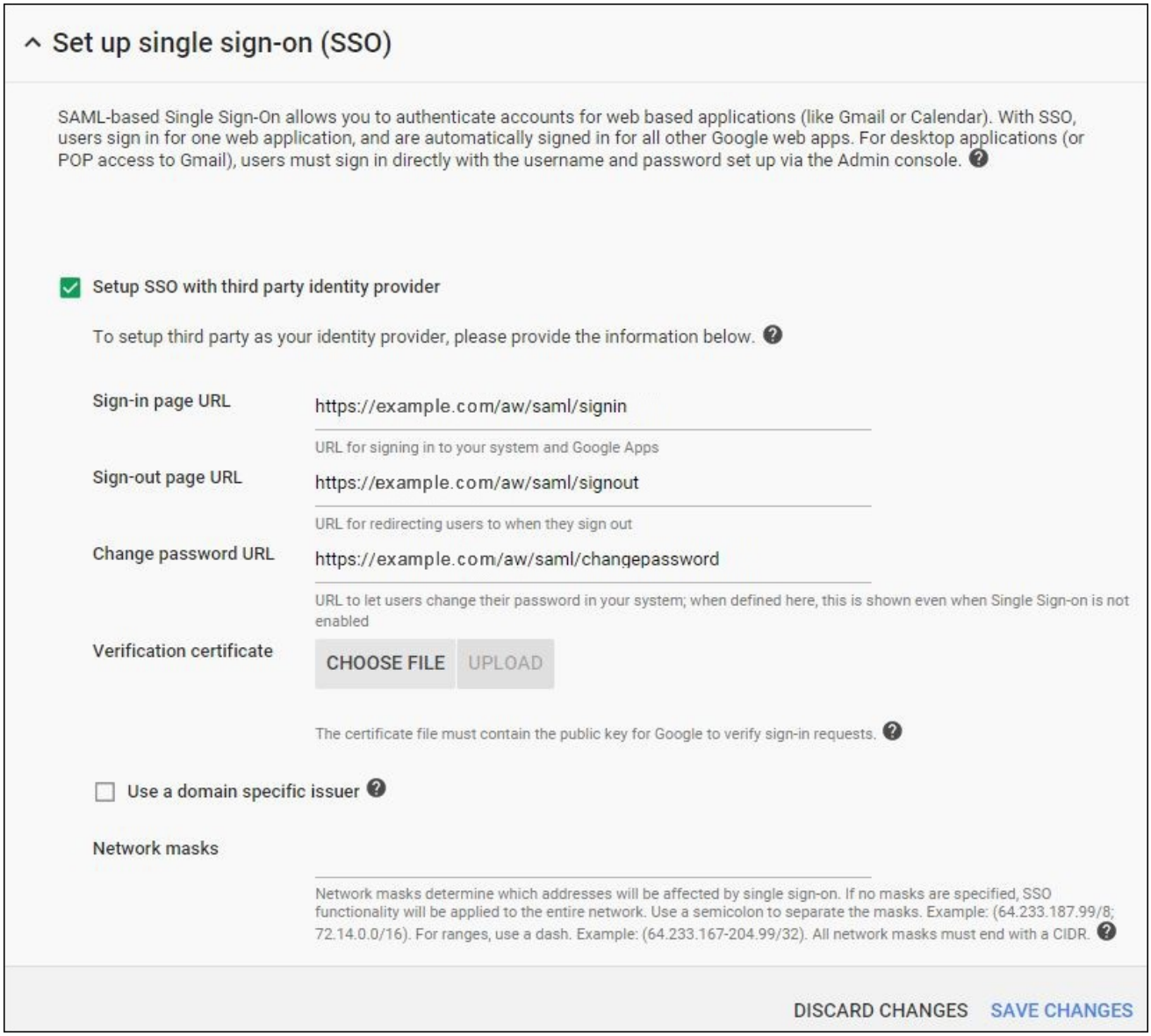
4. **[Export]** をクリックして証明書をコンピューターに保存します。

5. Google Adminポータル（https://admin.google.com）にAndroid for Work管理者の資格情報でログオンします。

6. **[Security]** をクリックします。



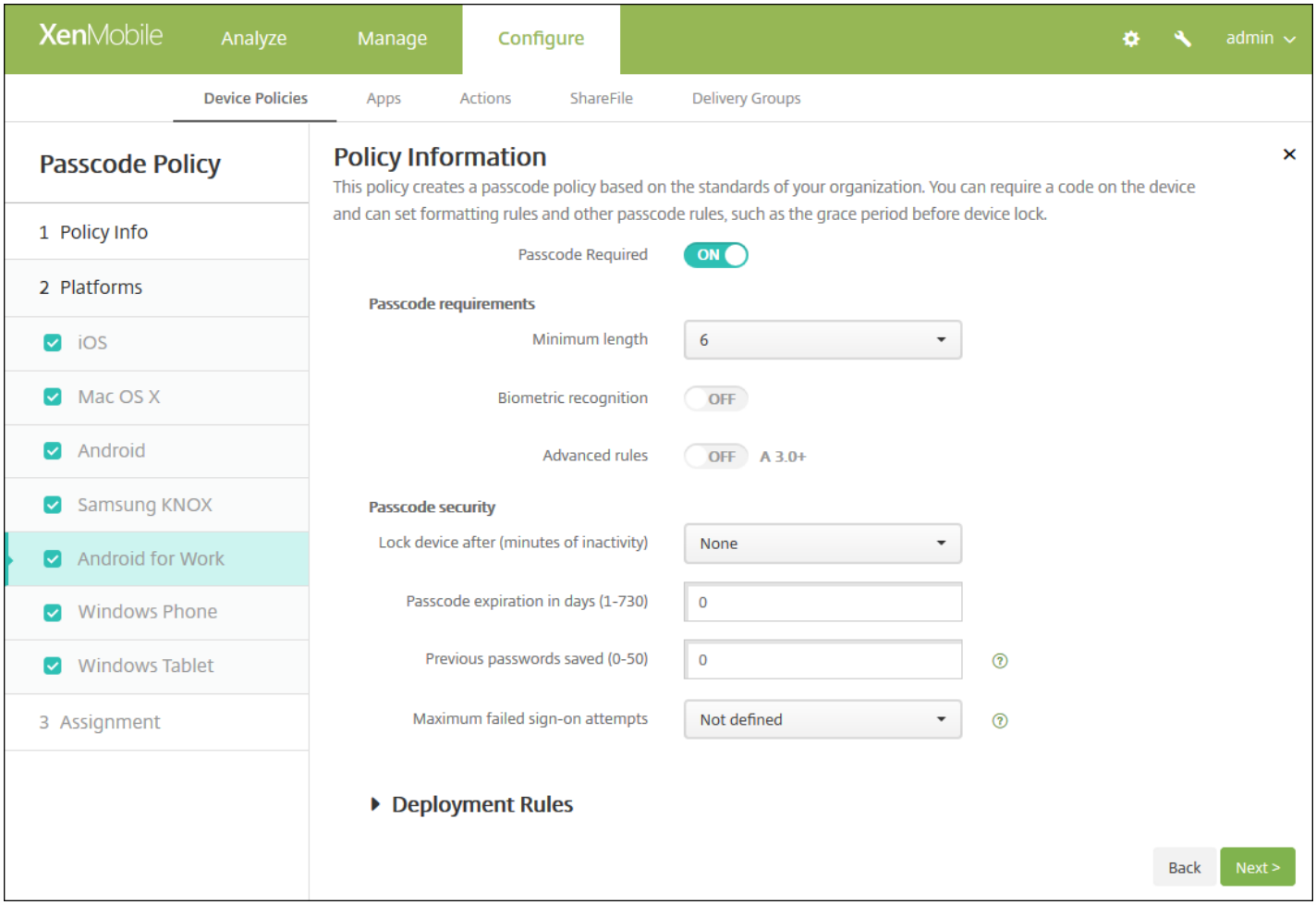
7. **[Security]** の下の **[Set up single sign-on（SSO）]** をクリックして以下の設定を構成します。



- **Sign-in page URL**：お使いのシステムおよびGoogle Appsに 設定して、 URLを入力します。 次に例を示します。 https:///aw/saml/signin。
- **Sign-out page URL**：ユーザーが サインアウト時にリダイレクトされるURLを入力します。 次に例を示します。 https:///aw/saml/signout.
- **Change password URL**：ユーザーがシステム内でパスワードを変更するときにアクセスするURLを入力します。 次に例を示します。 https:///aw/saml/changepassword。 ここで定義すると、SSOが利用できないときにもユーザーにこのURLが表示されます。
- **Verification certificate**： ［CHOOSE FILE］をクリックして、XenMobileからエクスポートされたSAML証明書を選択します。

8. **［SAVE CHANGES］**をクリックします。

望ましい任意のデバイスポリシーをセットアップできますが、パスコードポリシーをセットアップして、ユーザーが初めて登録するときにデバイスでのパスコード設定を必須にすることをお勧めします。



デバイスポリシーの基本的なセットアップ手順は以下のとおりです。

1. XenMobileコンソールにログオンします。

2. **[Configure] > [Device Policies]** をクリックします。

3. **[Add]** をクリックして、 **[Add a New Policy]** ダイアログボックスから追加するポリシーを選択します。この例では **[Passcode]** をクリックします。

4. **[Policy Information]** ページに入力します。

5. **[Android for Work]** をクリックしてポリシーの設定を構成します。

6. ポリシーをデリバリーグループに割り当てます。

Android for Workで使用できるその他のデバイスポリシーの設定について詳しくは、 「プラットフォーム別のXenMobileデバイスポリシー」を参照してください。

Android for Workアカウント設定の構成

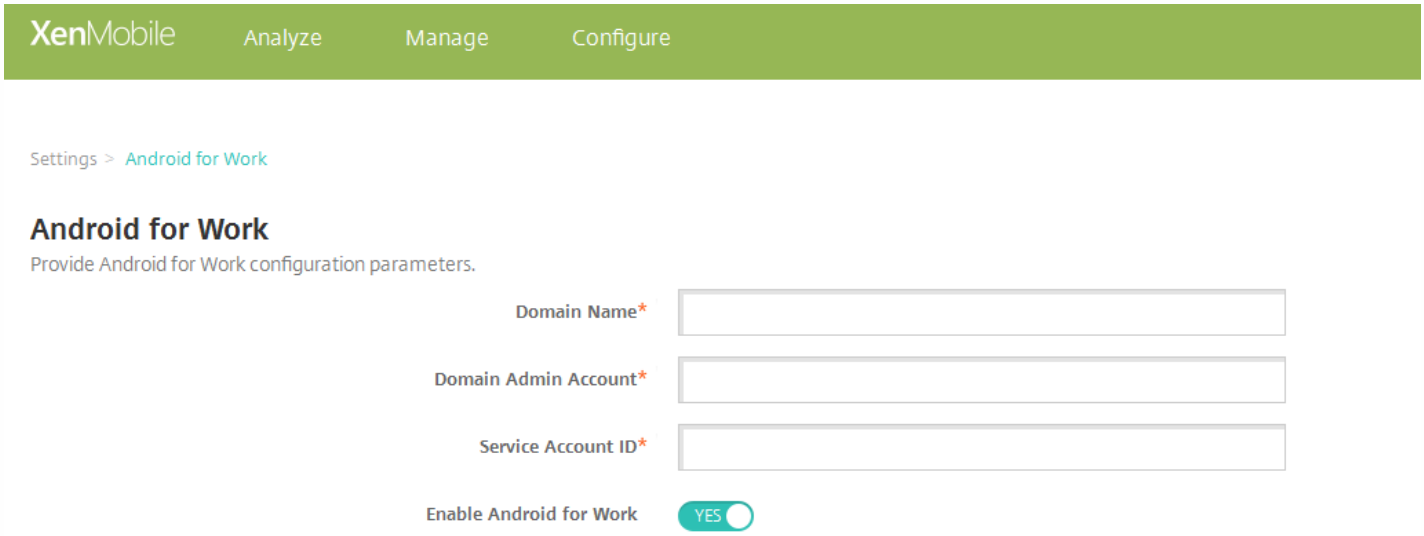
Aug 02, 2016

> **警告**
>
> サードパーティの既知の問題が存在することから、XenMobileコンソールを使用してAndroid for Workを有効にできない場合があります。 この問題の詳細と、回避策としてのサーバープロパティの構成方法については、「XenMobile Server 10.3の既知の問題」の#615118を参照してください。

ユーザーのデバイスでAndroid for Workのアプリケーションとポリシーを管理できるようにするには、XenMobileでAndroid for Workのドメインおよびアカウント情報を設定する必要があります。 しかし、その前に、ドメイン管理者を設定し、サービスアカウントIDとバインドトークンを取得するために、GoogleでAndroid for Workの設定作業を完了しておく必要があります。 GoogleでのAndroid for Workの設定作業について詳しくは、「Android for Workを使用したデバイスの管理」を参照してください。

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

2. **[Server]** の下の **[Android for Work]** をクリックします。 **[Android for Work]** 構成ページが開きます。



3. **[Android for Work]** ページで以下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**：ドメイン管理者のユーザー名を入力します。
- **Service Account ID**：GoogleのサービスアカウントIDを入力します。
- **Enable Android for Work**：Android for Workを有効にするかどうかを選択します。

4. **[Save]** をクリックします。

Android for Workでのデバイス所有者モードのプロビジョニング

Aug 02, 2016

Android for Workをデバイス所有者モードでプロビジョニングするには、NFC（Near-Field Communications；近距離無線通信）バンプを使用して、このドキュメントに記載されている手順に従ってWorx Provisioning Toolを実行しているデバイスと工場出荷時設定に復元されているデバイスの間でデータを転送する必要があります。 デバイス所有者モードは、会社所有のデバイスでのみ利用できます。

NFCが使用される理由 工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびそのほかの通信モードは無効になっています。 この状態のデバイスが理解する通信プロトコルはNFCのみです。

XenMobile環境におけるAndroid for Workの展開の概要について詳しくは、「XenMobileでのAndroid for Workによるデバイスの管理」を参照してください。

- Android for Work対応のXenMobileサーバー – バージョン10.1および10.3。
- デバイス所有者モードでAndroid for Work向けにプロビジョニングされた、工場出荷時設定にリセットされたデバイス。これを行うための手順については後述します。
- 構成済みのWorx Provisioning Toolを実行している、NFC機能が備わった別のデバイス。 Worx Provisioning Toolは、Worx Home 10.3またはCitrixダウンロードページから入手できます。

1つのデバイスにインストールできる、EMM（Enterprise Mobility Management；エンタープライズモビリティ管理）アプリ管理対象のAndroid for Workプロファイルは1つだけです。 XenMobileでは、Worx HomeがEMMアプリです。 1つのデバイスにつき許可されるプロファイルは1つだけです。 2つ目のEMMアプリを追加すると、1つ目のEMMアプリが削除されます。

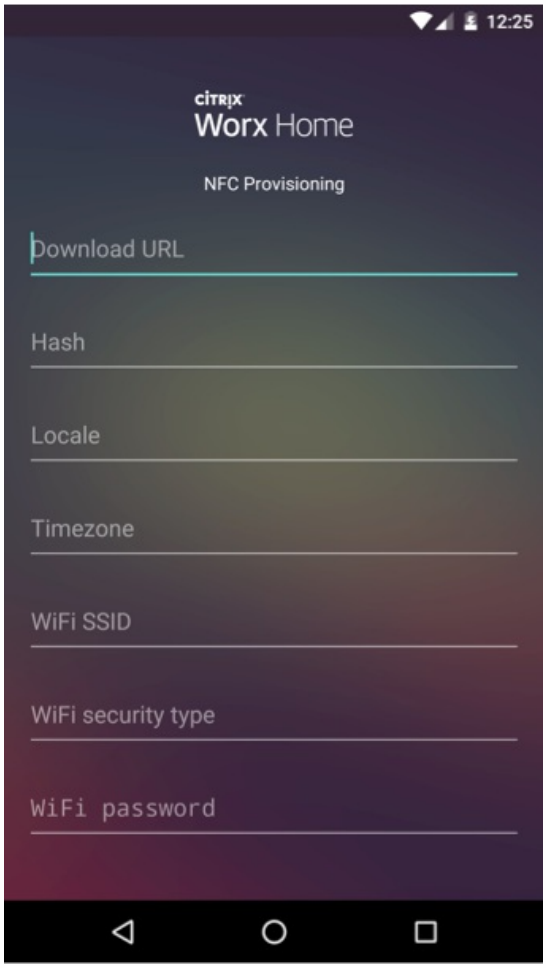
デバイス所有者モードは、特別な設定をしていない新しいデバイスまたは工場出荷時の設定にリセットされたデバイスで開始できます。 XenMobileでデバイス全体を管理します。

工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータをNFCバンプ経由で送信してAndroid for Workを開始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（Worx Home）のパッケージ名。
- デバイスがEMMプロバイダーアプリをダウンロードできるイントラネット/インターネット上の場所。
- ダウンロードが正常に完了したかどうかを確認するEMMプロバイダーアプリのSHA1ハッシュ。
- 工場出荷時の設定にリセットされたデバイスがEMMプロバイダーアプリに接続してダウンロードできるようにするWi-Fi接続の詳細 （現時点では、Androidはこのフローについて802.1x Wi-Fiをサポートしていません）。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、Worx Provisioning Toolのデータが工場出荷時の設定にリセットされたデバイスに送信されます。 このデータはその後、管理者設定でのWorx Homeのダウンロードに使用されます。 タイムゾーンと場所の値を入力しない場合、新しいデバイスではAndroidによって自動的にこれらの値が構成されます。

NFCバンプを行う前に、Worx Provisioning Toolを構成する必要があります。 この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFCバンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルから入力することもできます。 入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

ファイルの名前を**nfcprovisioning.txt**にして、/sdcard/Downloadsフォルダーにあるデバイスの SDカードに格納します。 アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには、次のデータを含める必要があります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<ダウンロード場所>
これが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になります。 上の画面で入力したSSID、セキュリティの種類、およびパスワードを使用してNFCバンプを行ってから、工場出荷時の設定にリセットされたデバイスがWi-Fiを接続した後に、このデバイスにこの場所へのダウンロード用のアクセス権を設定する必要があります。 URLは通常のURLで、特別な形式にする必要はありません。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=
これがEMMプロバイダーアプリのチェックサムとなります。 これは、インストールが成功したことを確認するために使用されます。 ハッシュの取得方法については後述します。

android.app.extra.PROVISIONING_WIFI_SSID=
これは、Worx Provisioning Toolを実行しているデバイスが接続されているWi-FiのSSIDです。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
サポートされる値はWEPおよびWPA2です。 Wi-Fiが保護されていない場合、このフィールドは空白にする必要があります。

android.app.extra.PROVISIONING_WIFI_PASSWORD=
Wi-Fiが保護されていない場合、このフィールドは空白にする必要があります。

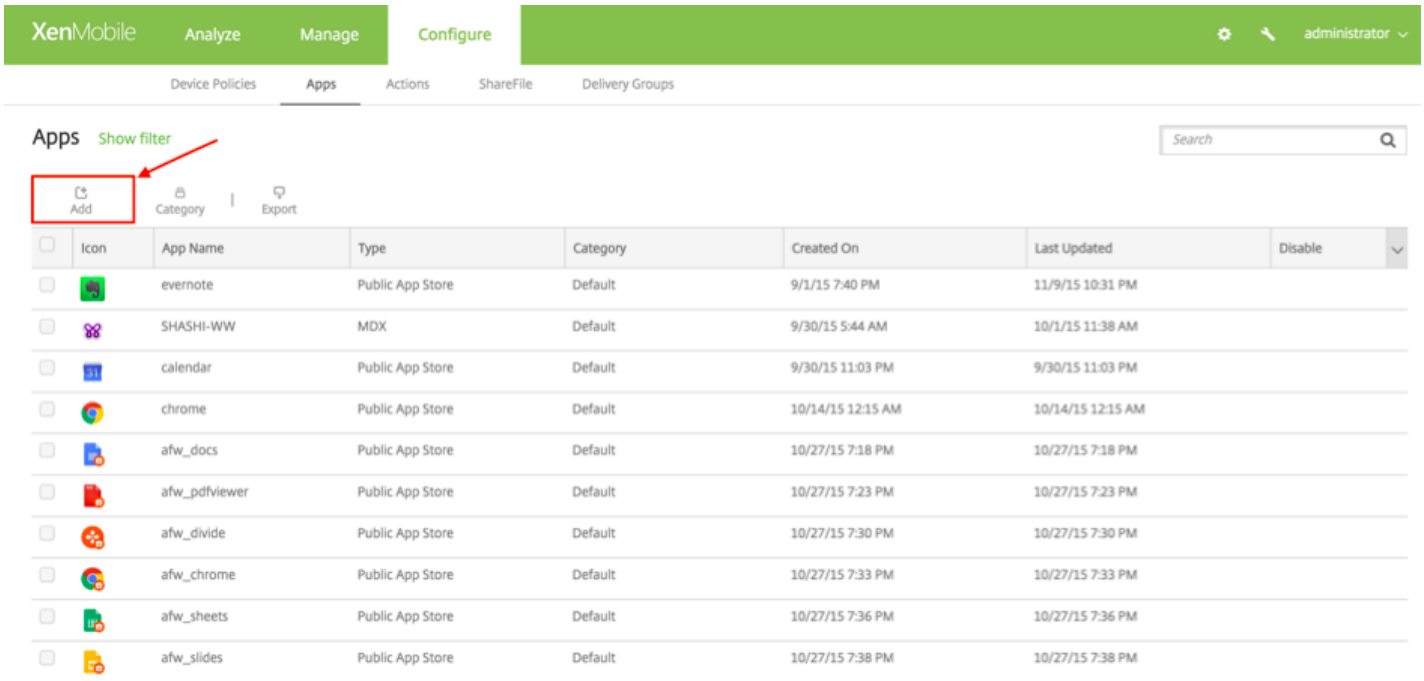
android.app.extra.PROVISIONING_LOCALE=<ロケール>
言語コードと国コードを入力します。 言語コードは、ISO 639-1で定義されている小文字で2文字のISO言語コード（「en」など）です。 国コードは、ISO 3166-1で定義されている大文字で2文字のISO国コード（「US」など）です。 たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。 コードを入力しない場合、国と言語は自動的に入力されます。

android.app.extra.PROVISIONING_TIME_ZONE=<タイムゾーン>
デバイスが実行されるタイムゾーンです。フォームの地域/場所のOlson名を入力します。 たとえば、米国太平洋標準時の場合は「America/Los_Angeles」です。 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=<パッケージ名>
この値はWorx Homeとしてアプリにハードコードされるため、必須ではありません。 ここでは、情報の完全性を守るためだけに記載しています。

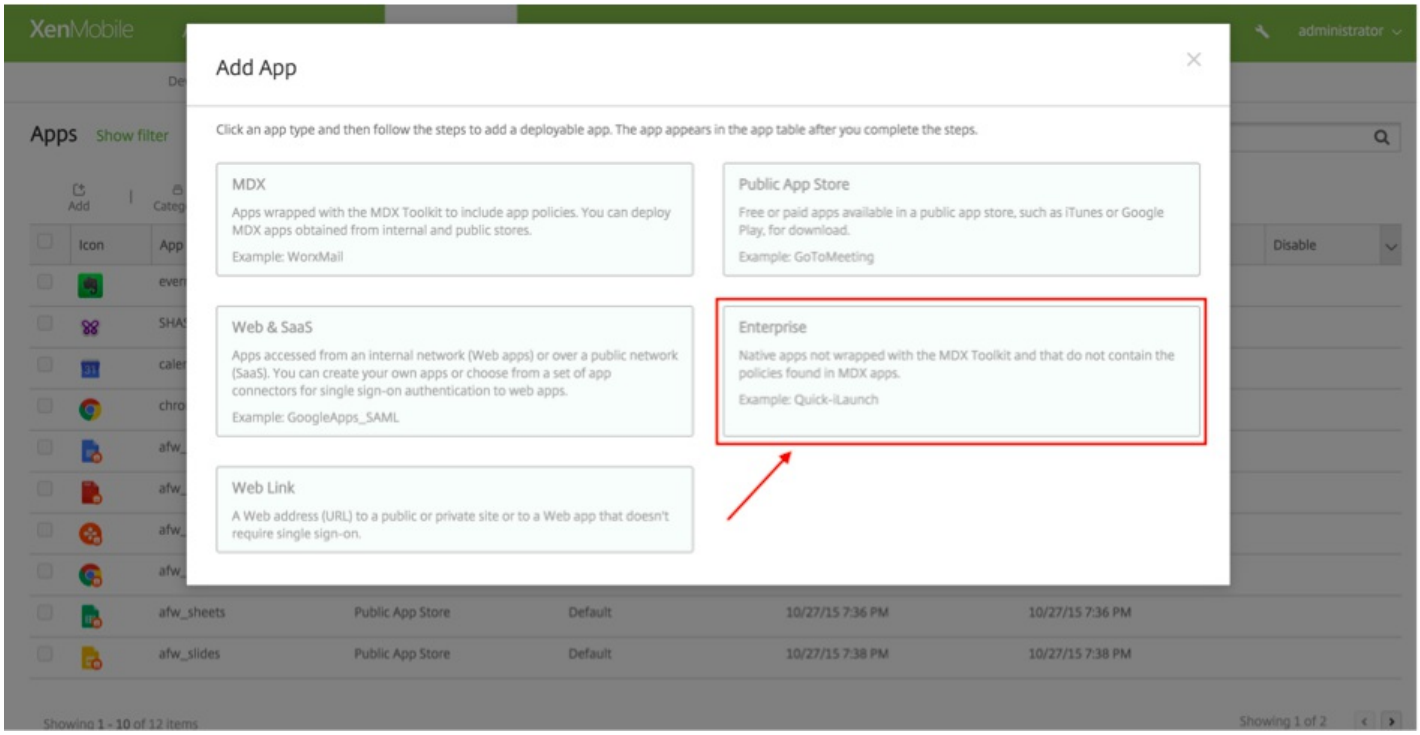
アプリのチェックサムを取得するには、そのアプリをエンタープライズアプリとして追加します。

1. XenMobileコンソールで、 **[構成]** 、 **[アプリ]** 、 **[追加]** の順にクリックします。



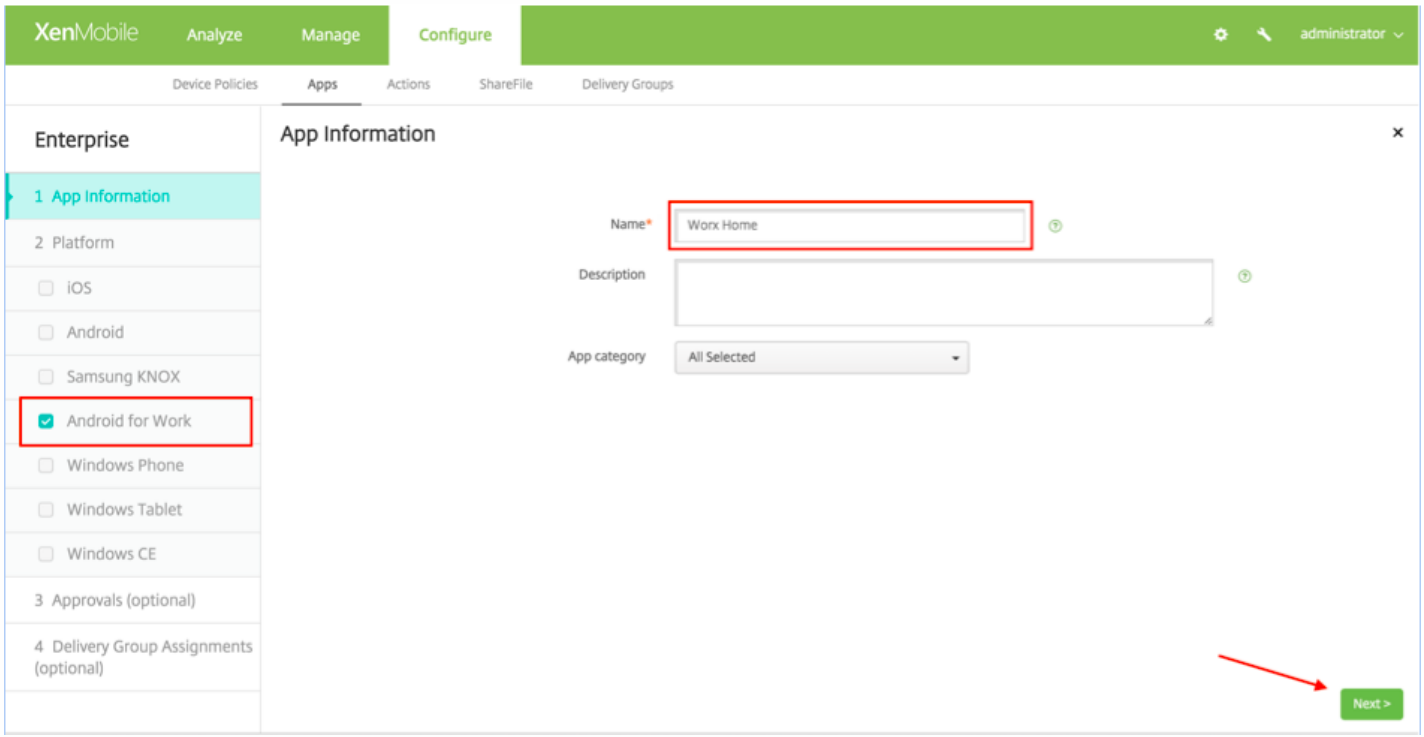
［Add App］ウィンドウが開きます。

2. [エンタープライズ] をクリックします。



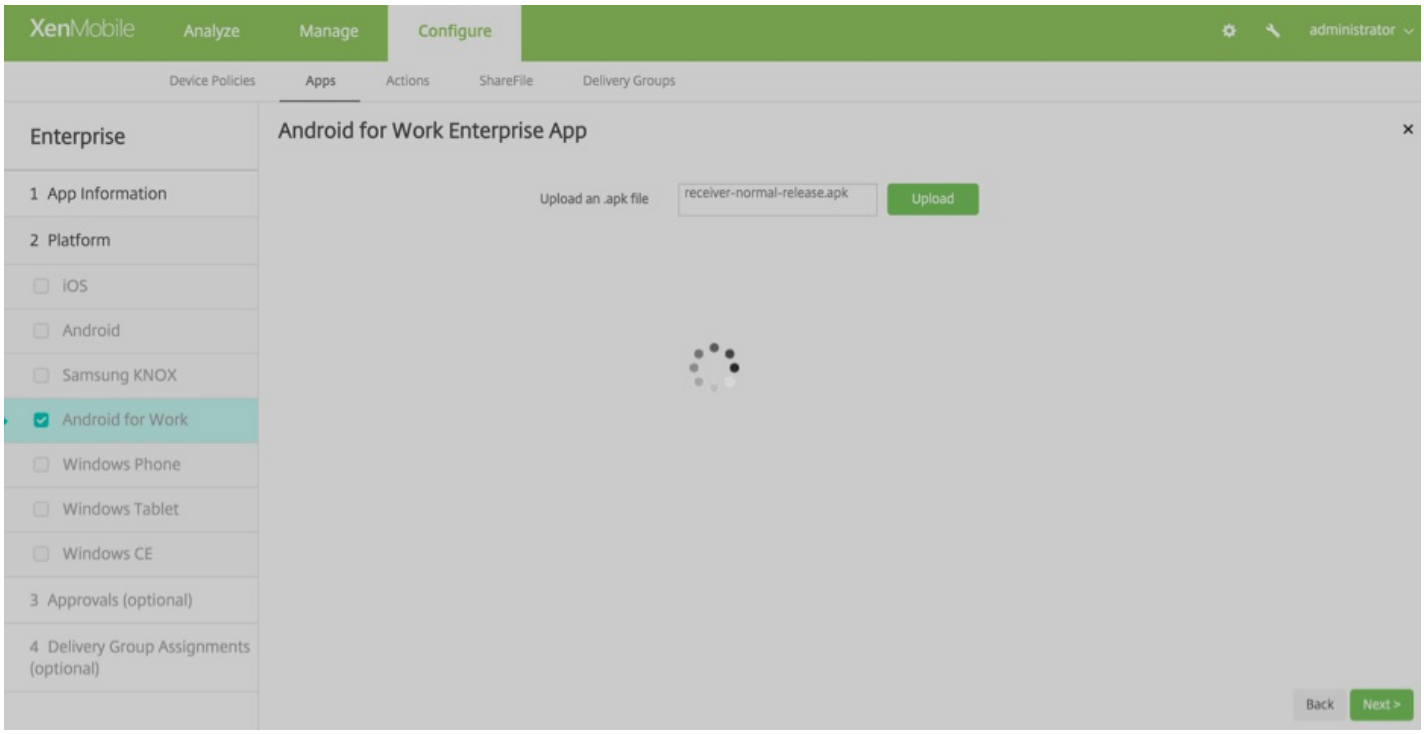
[**App Information**] 画面が開きます。

3. 次の構成を選択して [**次へ**] をクリックします。

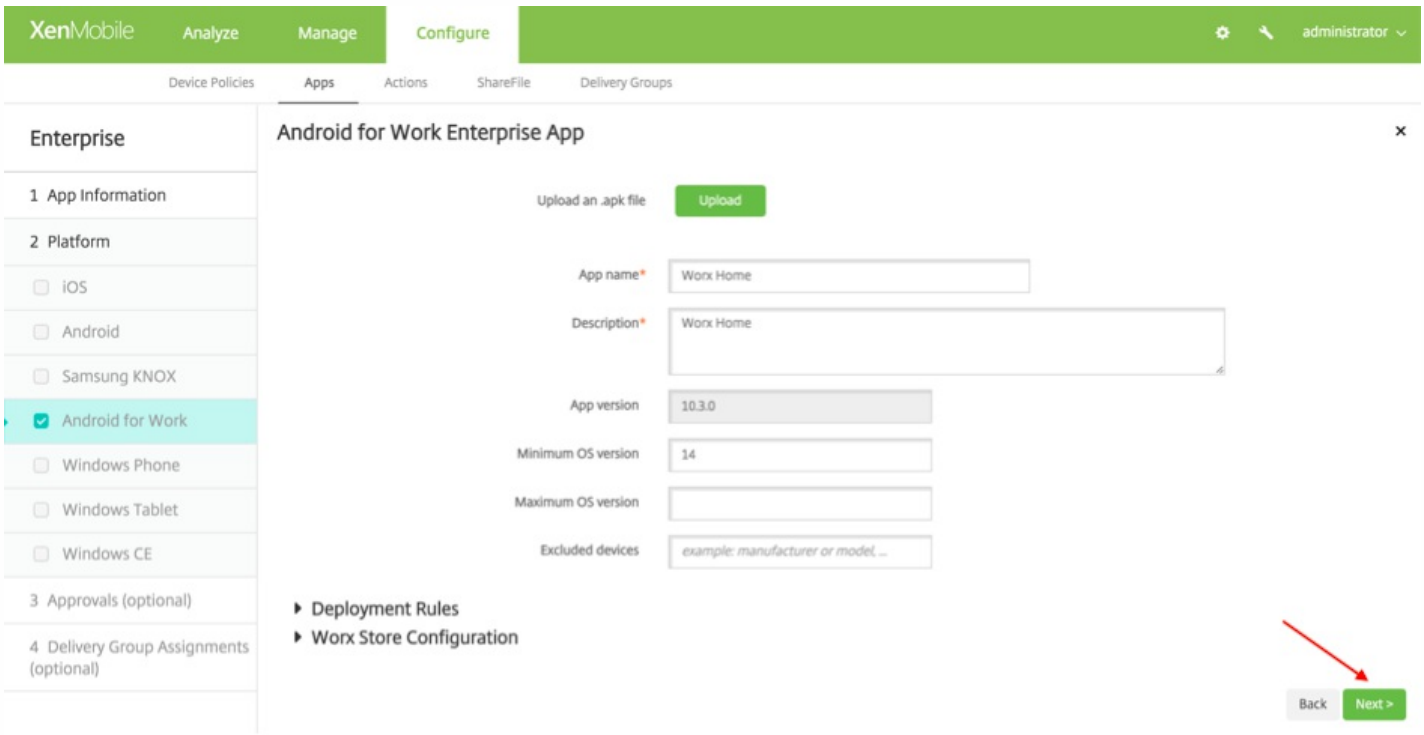


[**Android for Work Enterprise App**] 画面が開きます。

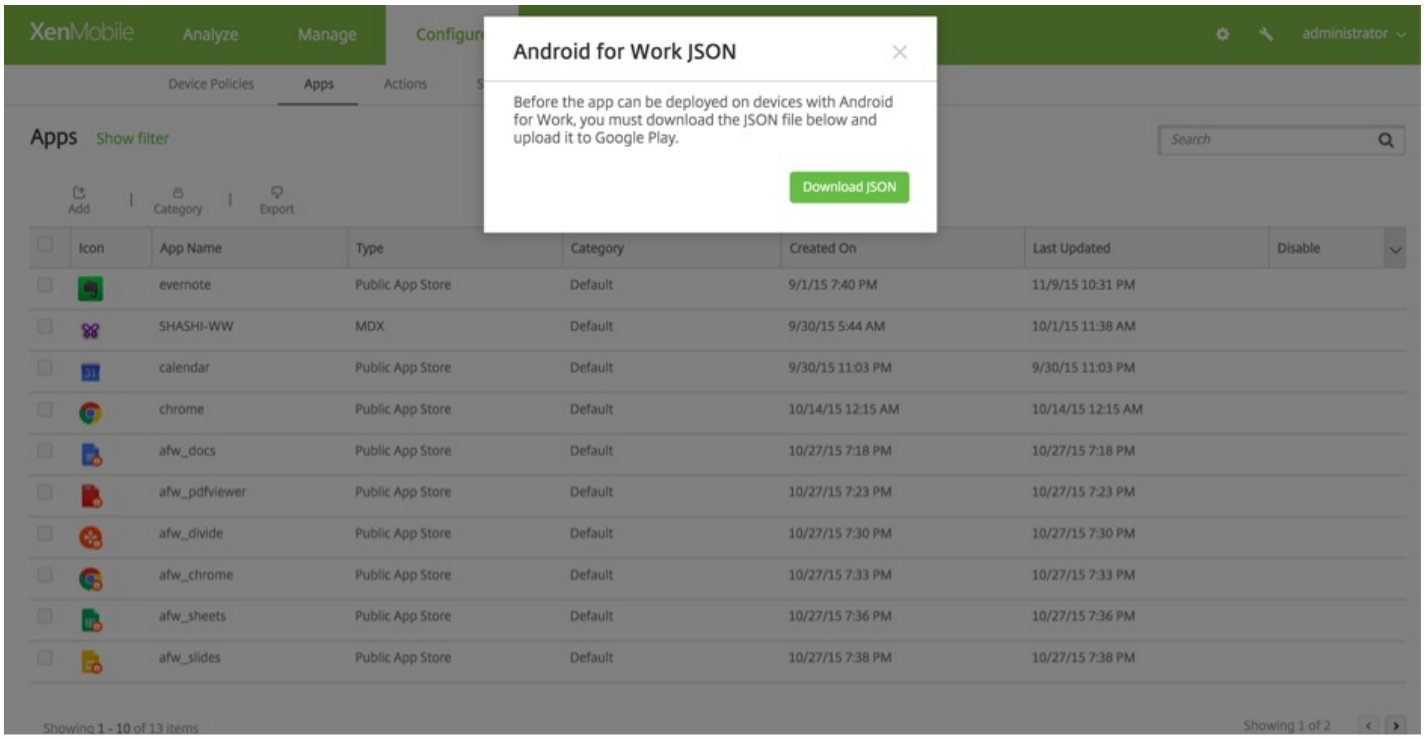
4. .apkへのパスを入力し、［次へ］をクリックしてファイルをアップロードします。



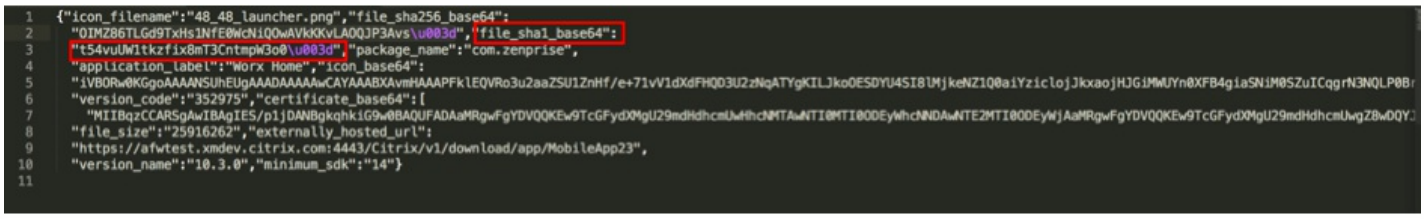
アップロードが完了すると、アップロードされたパッケージの詳細が表示されます。



5. ［次へ］をクリックしてJSONファイルをダウンロードする画面を表示します。このファイルは、この後Google Playへのアップロードに使用します。 Worx Homeの場合、Google Playにアップロードする必要はありませんが、SHA1を読み込む元になるJSONファイルが必要です。



以下の図に、典型的なJSONファイルの例を示します。



6. **file_sha1_base64の値**をコピーして、この値をWorx Provisioning Toolの **[ハッシュ]** フィールドで使用します。 **注：** ハッシュはURLセーフのものにする必要があります。

- **+**記号はすべて**-**に変換します。
- **/**記号はすべて**_**に変換します。
- 末尾の**\u003d**は**=**に置き換えます。

ハッシュをデバイスのSDカードのnfcprovisioning.txtファイルに格納すると、安全のための変換が行われます。 ただし、ハッシュを手動で入力すると、URLの安全性は入力者の責任になります。

Worx Provisioning Toolでは、以下のライブラリがソースコードに使用されています。

- v7 appcompat library by Google（Apache license 2.0）
- Design support library by Google（Apache license 2.0）
- v7 Palette library by Google（Apache license 2.0）
- Butter Knife by Jake Wharton（Apache license 2.0）

展開規則の構成

Oct 25, 2016

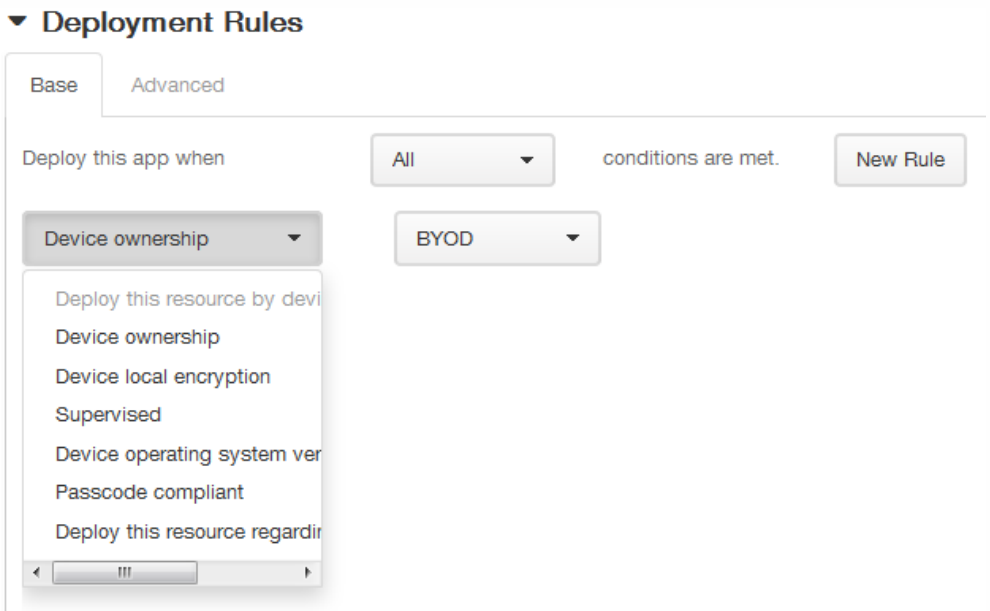
ここでは、以下の内容について説明します。

- 展開規則 - パッケージの展開結果に影響を与えるパラメーターです。
- 展開スケジュール - XenMobileからパッケージがデバイスにプッシュされるタイミングを指定するオプションです。

展開規則の構成

展開規則は、パッケージの展開結果に影響を与えるパラメーターです。 展開規則は、デバイスのプロパティ、アプリ、操作を指定できます。 XenMobileは、デバイスプロパティで指定した展開規則によって、ポリシー、アプリ、操作、デリバリーグループをフィルター処理して、パッケージの展開順を判断します。 詳しくは「展開順を変更するには」を参照してください。

特定のオペレーティングシステムバージョン、特定のハードウェアプラットフォーム、またはそのほかの組み合わせに基づいてパッケージを展開することができます。 デバイスプロパティ、アプリ、操作を追加および編集するために使用するウィザードには、**基本的な**規則エディターと**高度な**規則エディターがあります。**高度な規則エディター**の概観は自由形式のエディターです。 次の図は、アプリケーションを追加または編集するときに使用できる［**Deployment Rules**］画面を示しています。



基本的な展開規則は、あらかじめ定義されたテストと、その結果のアクションで構成されています。 可能であれば、テスト例に結果があらかじめ組み込まれます。 たとえば、ハードウェアプラットフォームに基づくパッケージ展開では、既知のプラットフォームがすべて結果のテストに組み込まれ、規則の作成時間が大幅に短縮されてエラーが発生する可能性も低くなります。

パッケージに規則を追加するには、［**New rule**］をクリックします。

注：規則ビルダーには各テストに固有の詳細情報が含まれています。

新しい規則を作成するには、規則テンプレートを選択し、条件の種類を選択して、規則をカスタマイズします。 規則のカスタマイズには説明の変更も含まれます。 設定の構成が完了したら、その規則をパッケージに追加します。

規則は、必要に応じていくつでも追加できます。 すべての規則に一致した場合にパッケージが展開されます。

[Advanced] タブをクリックすると、 **[Advanced Rule Editor]** が表示されます。

このモードでは、規則間の関係を指定できます。 使用できる演算子は、**AND**、**OR**、および**NOT**です。

展開スケジュールの構成

XenMobileでは、操作、アプリ、デバイスポリシーに対して指定する展開スケジュールを使用して、これらのアイテムの展開を制御できます。 展開が即座に実行されるか、特定の日時に実行されるか、展開条件に従って実行されるかを指定できます。 構成した展開スケジュールはすべてのプラットフォームについて同一です。

すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]** の設定は適用されません。 iOSではAppleプッシュ通知サービス（APN）が使用されます。

展開スケジュールオプションを変更しない場合、展開は接続のたびに即座に行われます。 展開スケジュールのオプションは次のとおりです。

Deploy：デフォルトは **[ON]** です。 展開を行わない場合は、この設定を **[OFF]** に変更します。

Deployment Schedule：デフォルトでは **[Now]** です。 展開の時間を指定するには、 **[Later]** を選択してから日付を選択し、時刻を入力します。

Deployment condition：デフォルトでは **[On every connection]** です。 展開を制限するには、この設定を **[Only when previous deployment has failed]** に変更します。

Deploy for always-on connection：デフォルトでは **[OFF]** です。 このポリシーはAndroidデバイスにのみ適用されます。 XenMobileの **[Background Deployment]** サーバープロパティでは、Androidデバイスに展開する各ポリシーの **[Deploy for always-on connections]** を **[ON]** に設定する必要があります。 常時接続について詳しくは、『XenMobile展開ハンドブック』で、「XenMobileの動作の調整」の「その他のサーバーの最適化」と「Androidデバイスの展開スケジュールの最適化」、および「デバイスポリシーおよびアプリケーションポリシー」の「スケジュール設定ポリシー」を参照してください。

デバイスの追加およびデバイスの詳細の表示

Aug 02, 2016

XenMobileサーバーのデータベースには、モバイルデバイスの一覧が保存されます。 各モバイルデバイスは、一意のシリアル番号またはIMEI（International Mobile Station Equipment Identity）/MEID（Mobile Equipment Identifier）識別番号よって定義されます。 XenMobileコンソールにデバイスを追加するには、手動でデバイスを追加するか、ファイルからデバイスの一覧をインポートします。 デバイスプロビジョニングファイル形式について詳しくは、「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。

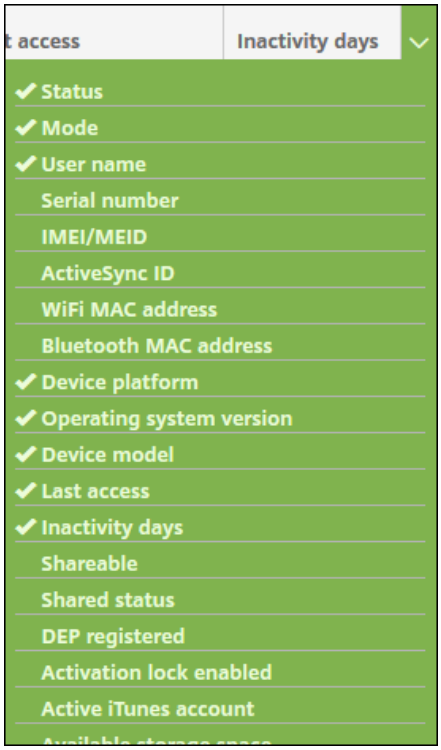
コンソールの［**Devices**］ページには各デバイスとその情報の一覧を示す表があり、［**Status**］（デバイスのジェイルブレイク状態、管理されているかどうか、Active Sync Gatewayが使用可能であるかどうか、および展開状態を表すアイコン）、［**Mode**］（モードがMDMなのか、MAMなのか、その両方なのか）、［**User name**］、［**Device platform**］、［**Operating system version**］、［**Device model**］、［**Last access**］、［**Inactivity days**］が示されます。

手動によるデバイスの追加、デバイスプロビジョニングファイルからのデバイスのインポート、デバイスの詳細の編集、デバイスへの通知の送信、デバイスの削除を行うことができます。 デバイス表のデータ全体を.csvファイルにエクスポートして、このファイルからカスタムレポートを生成することもできます。 すべてのデバイスの属性がエクスポートされますが、フィルターを適用している場合は、.csvファイルの作成時にそのフィルターが考慮されます。

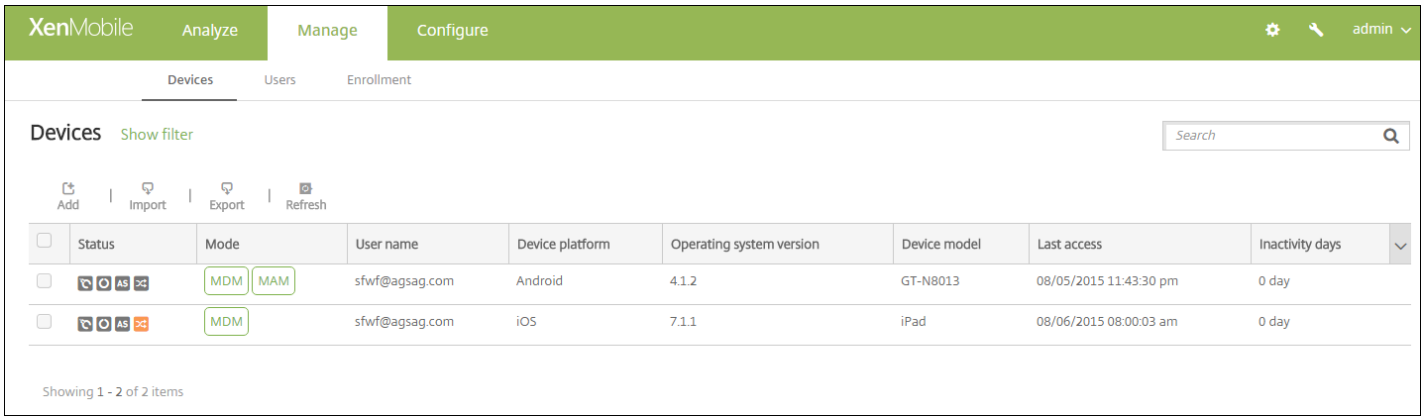
注：これらはデフォルトの見出しです。 末尾の見出しの下向き矢印をクリックし、追加で表示する見出しをオンにしたり表示しない見出しをオフにしたりして、［**Devices**］ページの表に示される内容をカスタマイズできます。

［**Devices**］表の使用可能なアクションに関する手順については、次のセクションを参照してください。

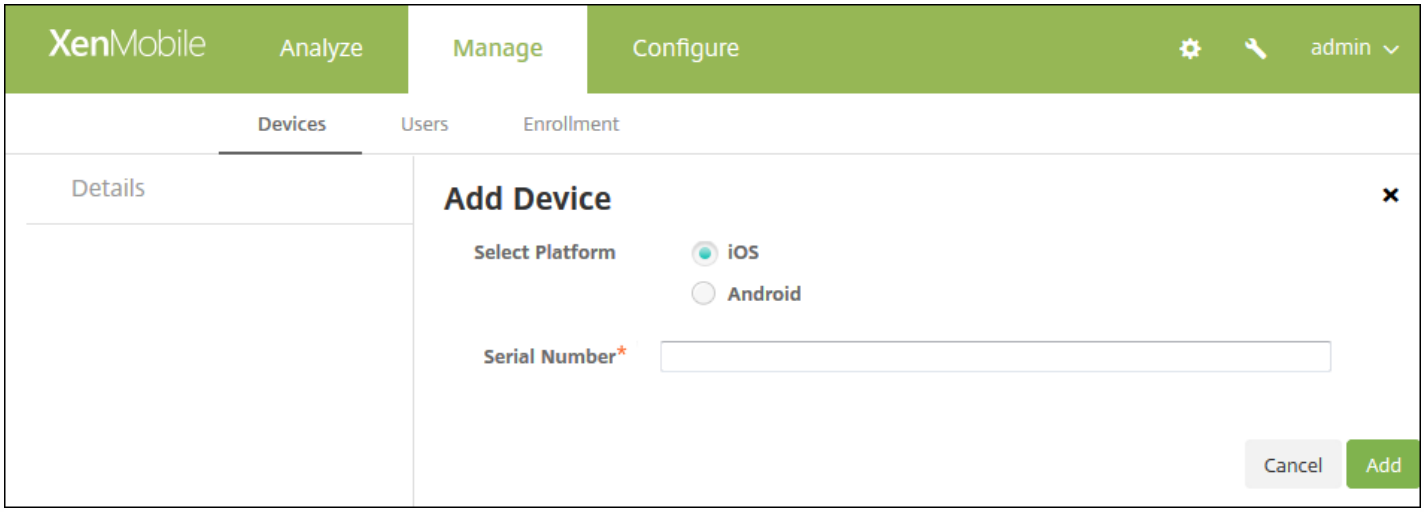
- 手動によるデバイスの追加
- デバイスプロビジョニングファイルからのデバイスのインポート
- デバイスの編集
- デバイスへの通知の送信
- デバイスの削除
- .csvファイルへの［**Devices**］の表のエクスポート



1.XenMobileコンソールで、［**Manage**］の［**Devices**］をクリックします。［**Devices**］ページが開きます。



2.［**Add**］をクリックします。［**Add Device**］ページが開きます。

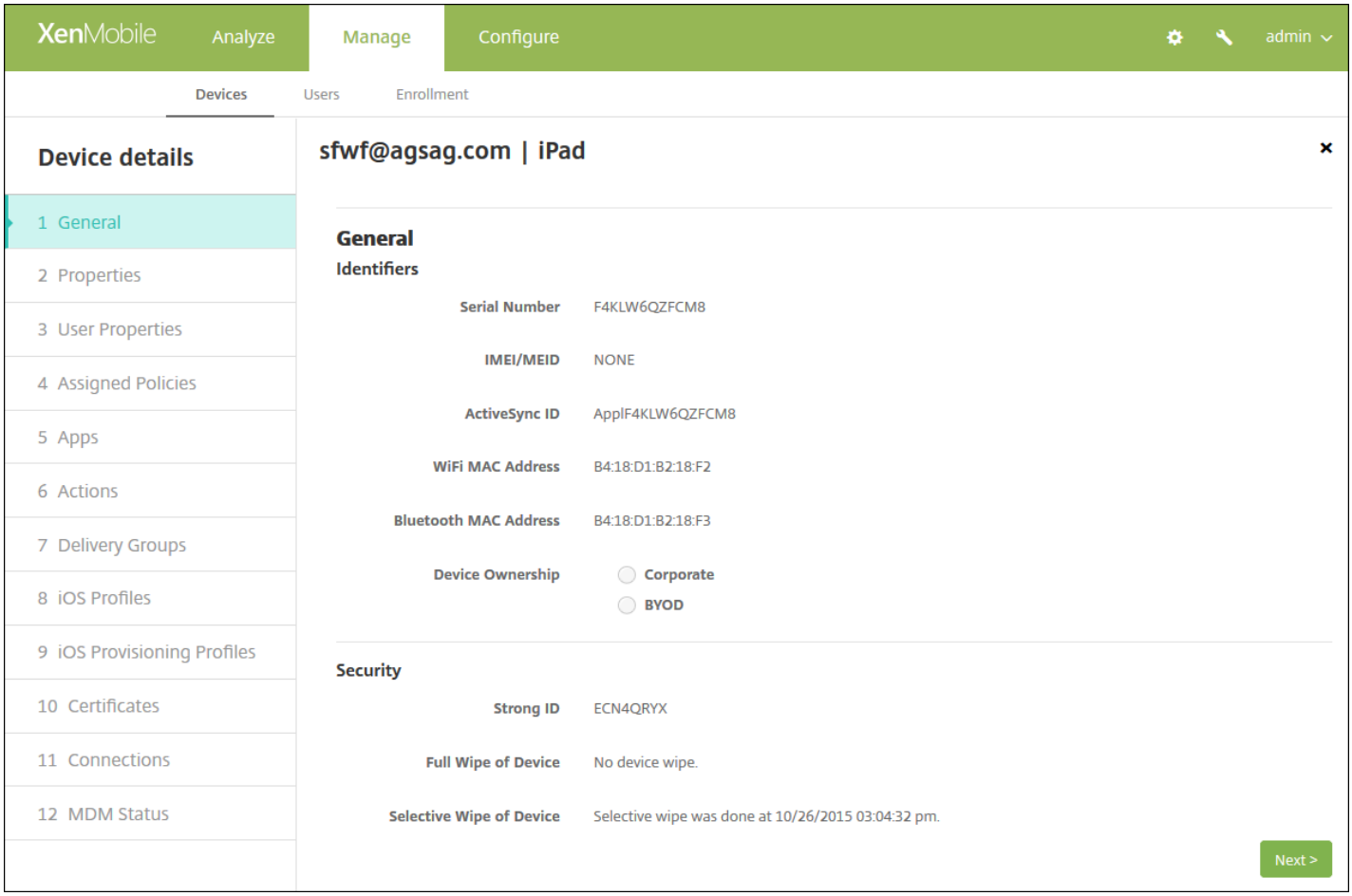


3. 次の設定を構成します。

- **Select platform**：［**iOS**］または［**Android**］を選択します。
- **Serial Number**：デバイスのシリアル番号を入力します。
- **IMEI/MEID**：Androidデバイスに限り、任意で、デバイスのIMEi/MEID情報を入力します。

4.［**Add**］をクリックします。［**Devices**］の表に示される一覧の一番下に、追加したデバイスが表示されます。追加したデバイスを一覧で選択して表示されるメニューで［**Edit**］をクリックし、デバイスの詳細を表示して確認します。

注：デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。



5. [**General Identifiers**] で、表示される次の情報を確認します（表示される項目はプラットフォームの種類によって異なります）。

- シリアル番号
- IMEI/MEID
- ActiveSync ID
- WiFi MAC Address
- Bluetooth MAC Address
- Device Ownership

6. [**Security**] で、表示される次の情報を確認します（表示される項目はプラットフォームの種類によって異なります）。

- Strong ID
- Full Wipe of Device
- Selective Wipe of Device
- Lock Device
- Device Unlock
- Device locate
- Device Enable Tracking
- Device Disown
- Activation Lock Bypass
- Device Clear Restrictions
- Request AirPlay Mirroring

- Stop Airplay Mirroring

注：iOSデバイスのロックはiOS 7以降で使用できます。

7. [**Next**] をクリックします。 [**Properties**] ページが開きます。ここでデバイスにプロパティを追加できます。

8. [**Add**] をクリックします。 使用可能なプロパティ一覧のボックスが表示されます。

9. 追加するプロパティごとに、以下の操作を行います。

- プロビジョニングするプロパティを選択して、値を設定します。 たとえば、プロパティ[**Activation lock enabled**] を選択し、 [**Yes**] または [**No**] のいずれかの値を設定できます。
- [**Done**] をクリックします。

10. [**Next**] をクリックします。

注：プロパティを追加すると、すべて [**Properties**] の下に表示されます。 後で [**Properties**] ページに戻ると、プロパティが複数のカテゴリに分かれています。

[**Assigned Policies**] 以降のセクションには、デバイスの概要情報が含まれています。

- **Assigned Policies**：展開済み、保留中、失敗のポリシー数を含む、割り当て済みポリシー数が表示されます。 各ポリシーの名前、種類、最新展開の情報も表示されます。
- **Apps**：インストール済み、保留中、失敗のアプリケーション数を含む、最新のインベントリ時点のアプリケーション数が表示されます。
- **Installed**：名前、所有権、バージョン、作成者、サイズ、インストール済み、識別子、種類の各情報が表示されます。
- **Pending and ailed apps**：名前、最新展開、識別子、種類の各情報が表示されます。
- **Actions**：展開済み、保留中、失敗のアクション数を含む、アクション数が表示されます。 各アクションの名前および最新展開の情報が表示されます。
- **Delivery Groups**：成功、保留中、失敗のデリバリーグループ数が表示されます。 各アクションの**デリバリーグループ**と時刻の情報が表示されます。 また、**デリバリーグループ**の状態、アクション、所有者、日付などのさらに詳細な情報も表示されます。
- **iOS Profiles**（iOSデバイスのみ）：名前、種類、組織、説明など、最新のiOSプロファイルインベントリが表示されます。
- **Certificates**：有効な証明書と期限切れまたは失効した証明書の数が表示され、種類、プロバイダー、発行者、シリアル番号、有効期間の開始日および終了日の情報も表示されます。
- **Connections**：最初の接続状態と最後の接続状態が表示されます。 各接続のユーザー名、最後から2番目の認証、最後の認証が表示されます。
- **TouchDown**（Androidデバイスのみ）：最後のデバイス認証と最後のユーザー認証の情報が表示されます。 それぞれ該当するポリシー名とポリシー値が表示されます。

12. [**Save**] をクリックします。

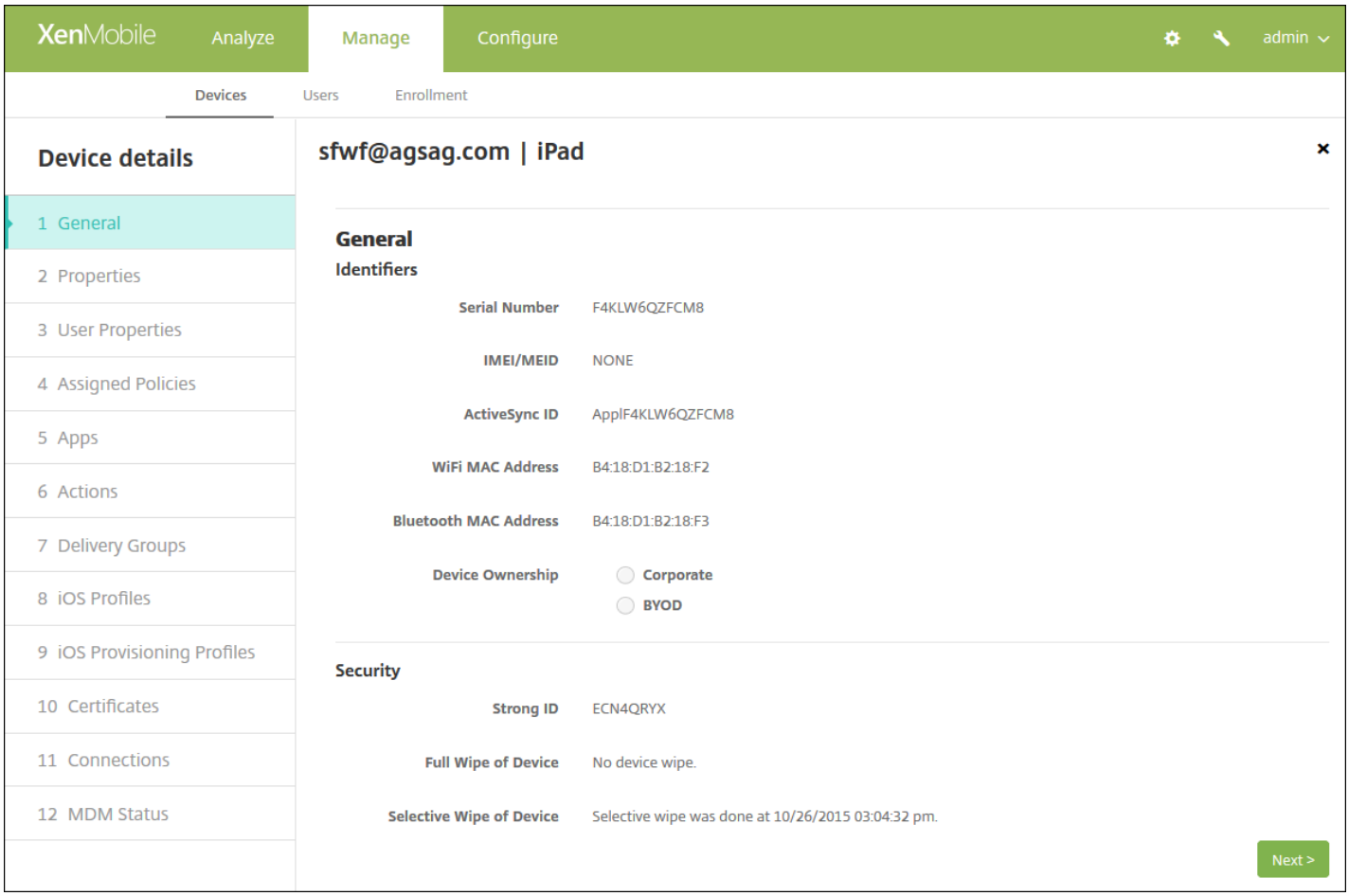
モバイル事業者やデバイス製造元が提供するファイルをインポートしたり、独自のデバイスプロビジョニングファイルを作成したりすることができます。「デバイスプロビジョニングファイル形式」を参照してください。

1. [**Devices**] の表の上にあるメニューで、 [**Import**] をクリックします。 [**Import Provisioning File**] ダイアログボックスが開きます。

2. [**Browse**] をクリックしてインポートするファイルの場所へ移動し、そのファイルを選択します。

3. [**Import**] をクリックします。 インポートされたファイルが [**Devices**] の表に追加されます。

1. 編集するデバイスを選択し、[Edit] をクリックします。 [Device Details] ページが開きます。



[**General Identifiers**] で変更できるフィールドは [**Device Ownership**] のみで、 [**Corporate**] または [**BYOD**] に設定できます。

3. [**Next**] をクリックすると、 [**Properties**] ページが表示されます。

4. [**Properties**] ページでは、プロパティを追加、編集、または削除できます。

- プロパティを追加するには、プロパティを追加するカテゴリで［Add］をクリックし、表示される一覧からプロパティを選択して、プロパティの値を追加します。 [**Done**] をクリックします。
- プロパティを編集するには、プロパティを選択して設定を変更し、[**Done**] または [**Cancel**] をクリックします。
- プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の［X］をクリックします。 項目が直ちに削除されます。

5. [**Next**] をクリックします。次に開くページは、選択したデバイスによって異なります。 デバイスによって、[**User Properties**] が開く場合と、 [**Assigned Policies**] が開く場合があります。

6. [**User Properties**] が開いた場合は、以下の手順に従ってユーザープロパティを追加、編集、または削除することができます。［Assigned Properties］が開いた場合は、残りのページにデバイスの概要情報が表示されます。 これらのページについて詳しくは、「デバイスを手動で追加するには」を参照してください。

注： [**User Properties**] ページの上側の部分は編集できません。

- 追加するユーザープロパティごとに、 [**Add**] をクリックして以下の操作を行います。
  - 表示される一覧から、追加するプロパティを選択してプロパティの値を入力し、[**Done**] または [**Cancel**] をクリックします。
- プロパティを編集するには、プロパティを選択して設定を変更し、[**Done**] または [**Cancel**] をクリックします。
- プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の［X］をクリックします。 項目が直ちに削除されます。

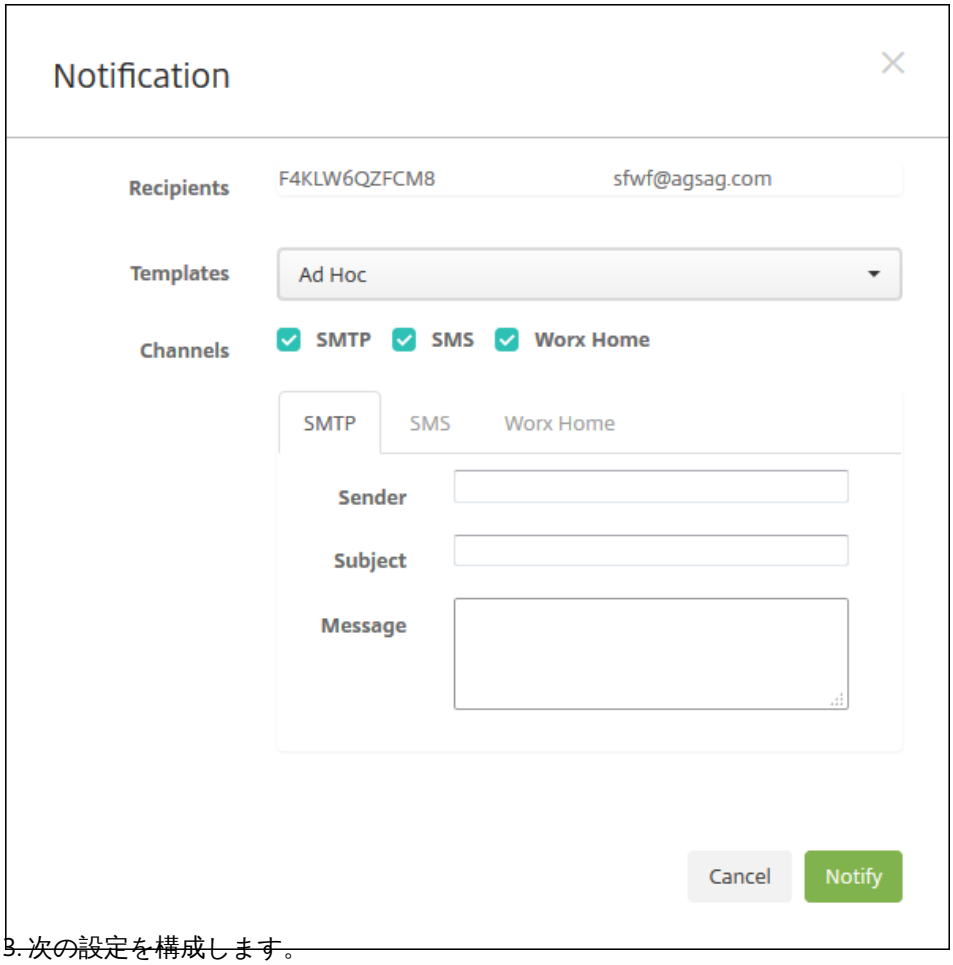
7. 後続の各ページで、概要情報を確認して [**Next**] をクリックします。

8. 最後のページで [**Save**] をクリックして、デバイスの変更を保存します。

［Devices］ページで、デバイスに通知を送信できます。 通知について詳しくは、 「XenMobileで通知テンプレートを作成または更新するには」を参照してください。

1. 通知を送信するデバイスを選択します。

2. [**Notify**] をクリックします。 [**Notification**] ダイアログボックスが開きます。 [**Recipients**] フィールドに、通知を受信するすべてのデバイスの一覧が表示されます。



3. 次の設定を構成します。

- **Templates**：一覧から、送信する通知の種類を選択します。 **[Ad Hoc]** を選択した場合を除き、 **[Subject]** フィールドおよび **[Message]** フィールドには、選択したテンプレートで構成済みのテキストが入力されます。
- **Channels**：メッセージの送信方法を選択します。 デフォルトは、 **[SMTP]** 、 **[SMS]** 、および **[Worx Home]** です。 **[SMTP]** タブ、 **[SMS]** タブ、および **[Worx Home]** タブをクリックすると、それぞれのメッセージ形式を表示できます。
- **Sender**：オプションで送信者を入力します。
- **Subject**：アドホックメッセージの場合、件名を入力します。
- **Message**：アドホックメッセージの場合、メッセージを入力します。

4. **[Notify]** をクリックします。

1. ［Devices］の表で、削除するデバイスを選択します。
2. ［Delete］をクリックします。 確認ダイアログボックスが開きます。 もう一度［Delete］をクリックします。
   重要：この操作を元に戻すことはできません。

1. **[Devices]** の表の上にある **[Export]** をクリックします。 XenMobileによって［Delivery］の表の情報が抽出され、.csvファイルに変換されます。

2. .csvファイルを開くか、保存します。 使用するブラウザーに応じて、手順が異なります。 操作を取り消すこともできます。

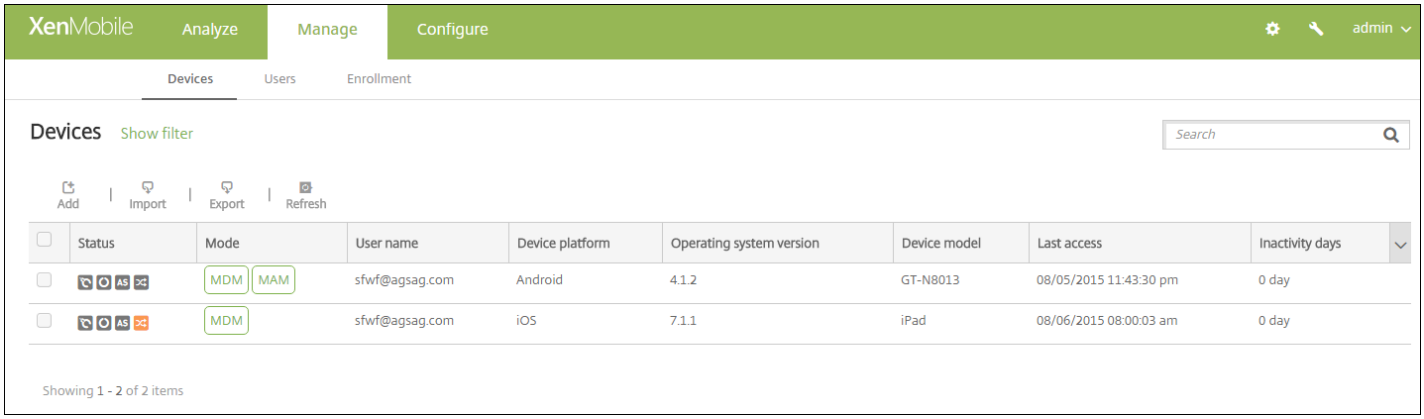
iOSデバイスのロック

Aug 02, 2016

iOSデバイスをロックし、デバイスのロック画面にメッセージと電話番号を表示することができます。 この機能は、iOS 7および8デバイスでサポートされます。

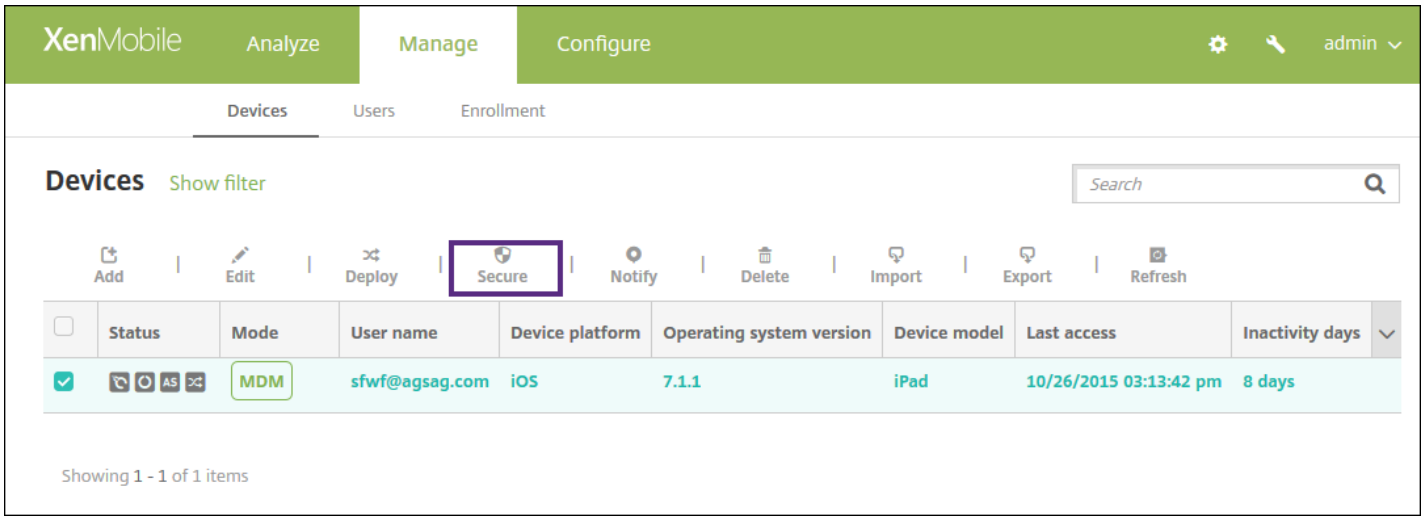
ロック画面にメッセージと電話番号を含めるように設定した場合、メッセージと電話番号は、管理者がXenMobileコンソールでパスコードポリシーも設定した場合、またはユーザーがデバイスのパスコードを手動で有効にしている場合にのみ、ロックされたデバイスに表示されます。

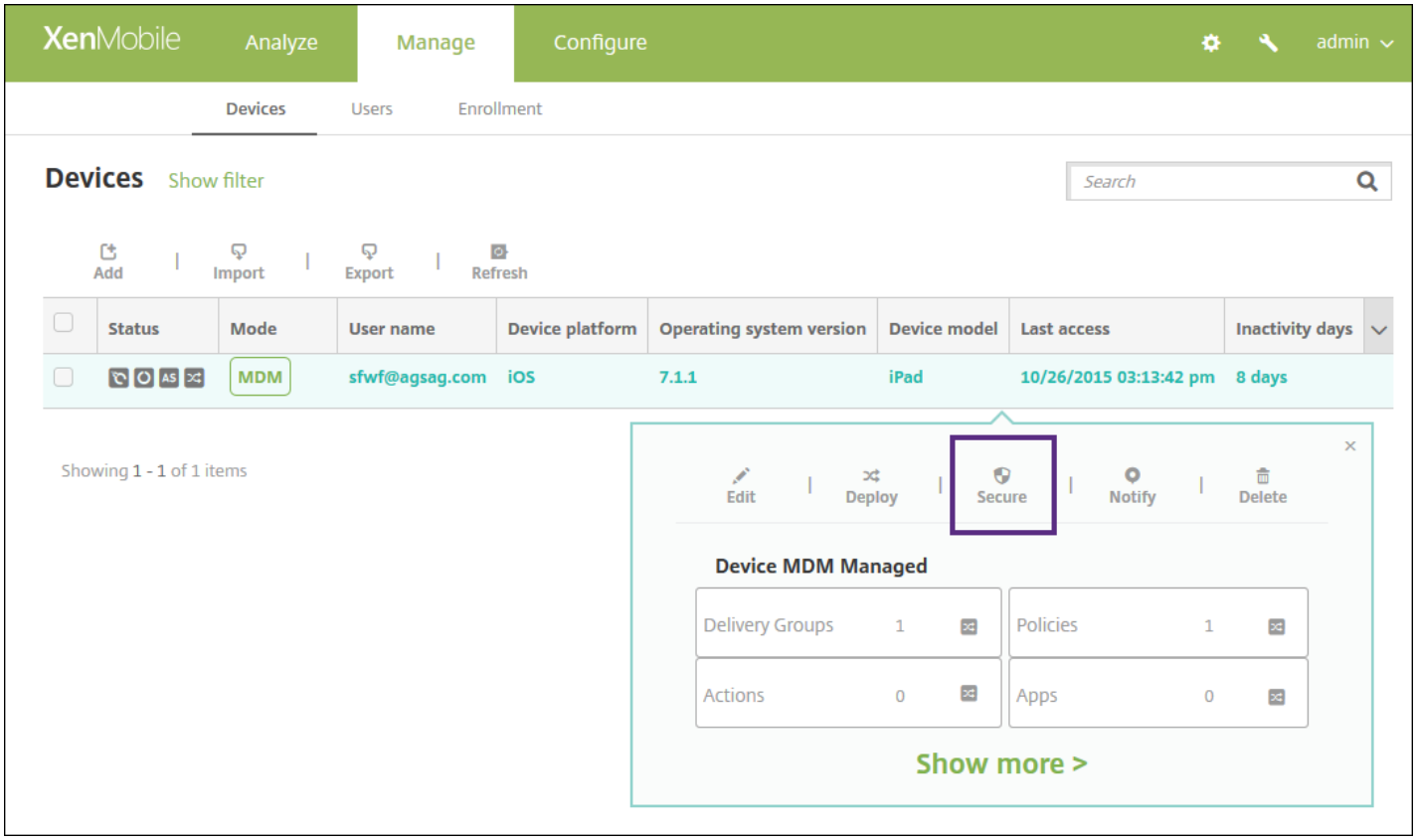
1.XenMobileコンソールで、［**Manage**］の［**Devices**］をクリックします。 ［**Devices**］ページが開きます。



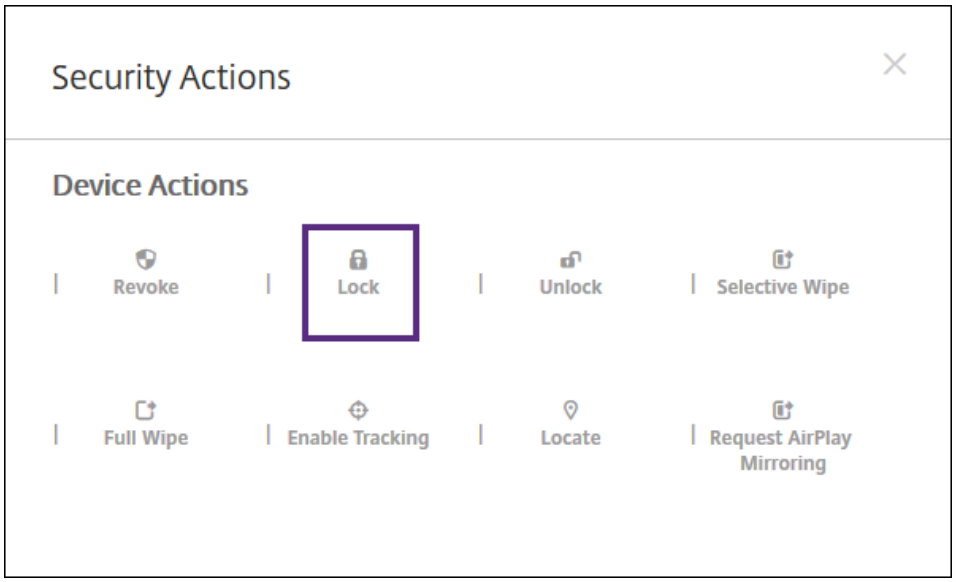
2.ロックするiOSデバイスを選択します。

デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。

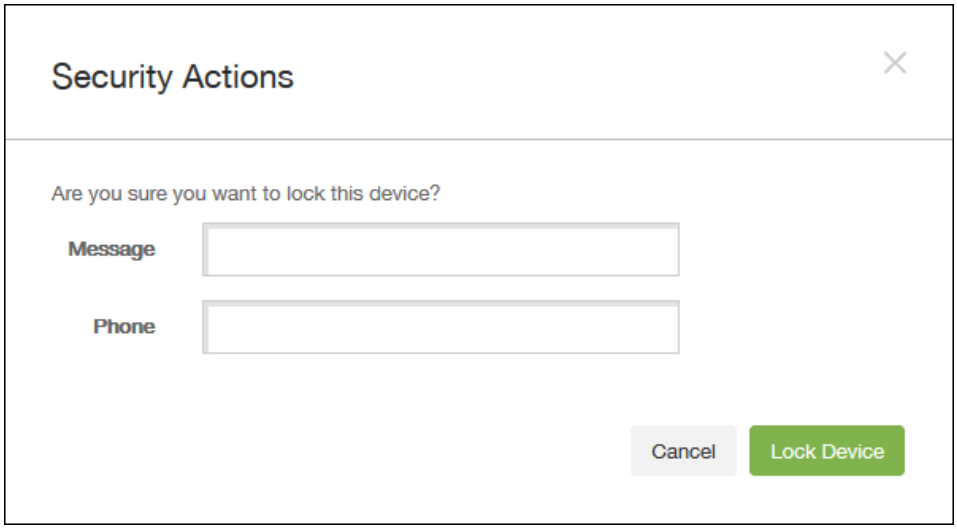




3.オプションメニューの［**Secure**］を選択します。 ［**Security Actions**］ダイアログボックスが開きます。



4. ［**Lock**］を選択します。 ［**Security Actions**］確認ダイアログボックスが開きます。



5.必要に応じて、デバイスのロック画面に表示するメッセージと電話番号を入力します。

6. **[Lock Device]** をクリックします。

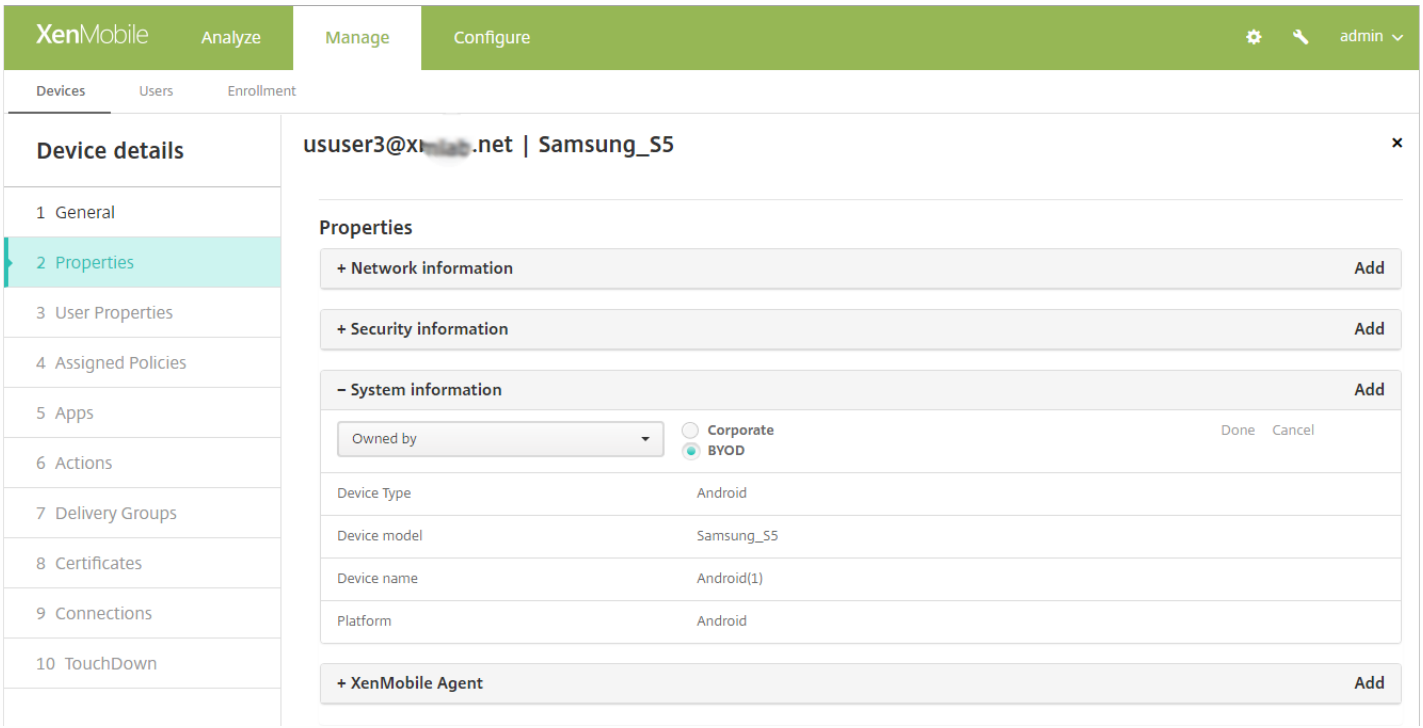
ユーザーデバイスの手動タグ付け

Aug 02, 2016

次のいずれかの方法で、XenMobileのデバイスに手動でタグ付けすることができます。

- 招待状に基づく登録処理中
- Self Help Portal登録処理中
- デバイスの所有権をデバイスプロパティとして追加する

組織または個人所有のいずれかとして、デバイスにタグ付けするオプションが用意されています。 Self Help Portalを使ってデバイスを自動登録するときに、組織または個人所有のいずれかとして、デバイスにタグを付けることもできます。 次の図に示すように、手動でデバイスをタグ付けすることもできます。XenMobileコンソールの［**Devices**］タブからデバイスにプロパティを追加し、［**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）を選択します。



デバイスプロビジョニングファイル形式

Aug 02, 2016

多くのモバイル事業者やデバイス製造元は、認証済みモバイルデバイスの一覧を提供しています。この一覧を使用すると、モバイルデバイスの長い一覧を手動で入力する必要がなくなります。 XenMobileは、Android、iOS、Windowsの3種類のサポート対象デバイスすべてに共通のインポートファイル形式をサポートしています。

手動で作成し、XenMobileへのデバイスのインポートに使用するプロビジョニングファイルは次の形式である必要があります。

> SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

注：

- ファイルの文字セットはUTF-8を指定してください。
- プロビジョニングファイル内では、フィールドをセミコロン（;）で区切ります。 フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。 たとえば、プロパティ propertyV;test;1;2の場合、 プロビジョニングファイルには「propertyV\;test\;1\;2」と入力します。
- IMEIが指定されていない場合は、SerialNumberが必須です。
- シリアル番号はiOSデバイスの識別子であるため、iOSデバイスではSerialNumberが必須です。
- SerialNumberが指定されていない場合は、IMEIが必須です。
- 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内で、以下の各行がデバイスを示しています。

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

最初のエントリは以下を意味しています。

- SerialNumber：1050BF3F5173010816100655105903 91
- IMEI：15244201625379901
- OperatingSystemFamily：WINDOWS
- ProertyName：propertyN
- PropertyValue：propertyV\;test\;1\;2;prop 2

デバイスポリシー

Oct 25, 2016

ポリシーを作成して、XenMobileとデバイスの連携方法を構成できます。 多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。 そのため、iOS、Android、Windowsデバイスの間で異なるほか、Androidを実行するデバイスの製造元によっても違いがある場合があります。 プラットフォーム別のポリシーについては、「プラットフォーム別のXenMobileデバイスポリシー」を参照してください。

新しいポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定のデリバリーグループを作成します。
- 必要なCA証明書をインストールします。

デバイスポリシーの基本的な作成手順は次のとおりです。

1. ポリシーの名前と説明を指定します。
2. 1つまたは複数のプラットフォームを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

XenMobileで次のデバイスポリシーを構成できます。

デバイスポリシー名	デバイスポリシーの説明
AirPlayミラー化	XenMobileでデバイスポリシーを追加して、特定のAirPlayデバイス（Apple TVやほかのMacコンピューターなど）をユーザーのiOSデバイスに追加することができます。 また、デバイスを監視対象デバイスのホワイトリストに追加して、ユーザーをホワイトリストにあるAirPlayデバイスのみに限定するオプションもあります。
AirPrint	AirPrintデバイスポリシーで、AirPrintプリンターをユーザーのiOSデバイスのAirPrintプリンター一覧に追加できます。 このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。 注： ● このポリシーはiOS 7.0以降に適用されます。 ● 各プリンターのIPアドレスとリソースパスがあることを確認してください。
Android for Workアプリケーション制限	このポリシーによって、Android for Workアプリに関連する制限を変更できますが、そのためには、次の前提条件を満たす必要があります。 ● GoogleのAndroid for Work設定タスクを完了します。 詳しくは、「XenMobileでのAndroid for Workによるデバイスの管理」を参照してください。 ● 一連のGoogle Play資格情報を作成します。 詳しくは、「Google Play資格情報」を参照してください。 ● Android for Workアカウントの作成 詳しくは、「Android for Workアカウントの作成」を参

	照してください。 • Android for WorkアプリをXenMobileに追加します。 詳しくは、「XenMobileへのアプリケーションの追加」を参照してください。
APN	このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマーAPNを使用しない組織で使用します。 APNポリシーによって、特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。 ほとんどの新しい電話機において、この設定は既に定義されています。
アプリケーションアクセス	XenMobileのアプリケーションアクセスデバイスポリシーでは、デバイスへのインストールが必須のアプリケーション、デバイスにインストール可能なアプリケーション、デバイスへのインストールが禁止されるアプリケーションの一覧を定義できます。 次に、そのアプリケーション一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。
アプリケーション属性	このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
アプリケーション構成	このポリシーでは、管理された構成をサポートするApp Storeアプリケーションをリモートで構成できます。XML構成ファイル（プロパティ一覧またはplistと呼ばれるファイル）をユーザーのiOSデバイスに展開して、アプリケーションのさまざまな設定および動作を構成できます。
アプリケーションインベントリ	アプリケーションインベントリポリシーにより、管理されているデバイスのアプリケーションのインベントリを収集できます。その後、インベントリは、それらのデバイスに展開されたアプリケーションアクセスポリシーと比較されます。 この方法で、アプリケーションのブラックリスト（アプリケーションアクセスポリシーで禁止）またはホワイトリスト（アプリケーションアクセスポリシーで必須）に表示されるアプリケーションを検出し、それに応じた操作を実行することができます。
アプリケーションロック	XenMobileでは、ポリシーを作成して、デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行を禁止するアプリの一覧を定義できます。 このポリシーは、iOSデバイスとAndroidデバイスの両方に対して構成できますが、ポリシーが実際にどのように機能するかは各プラットフォームで異なります。 たとえば、iOSデバイスで複数のアプリを禁止することはできません。 注：デバイスポリシーは大部分のAndroid LおよびMデバイスで機能しますが、アプリのロックは、必要なAPIがGoogleによって廃止されたため、Android N以降のデバイスでは機能しません。 また、iOSデバイスで選択できるiOSアプリは、ポリシーあたり1つのみです。 つまり、ユーザーはデバイスを使用して1つのアプリを実行することのみできます。 アプリのロックポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。

アプリケーションネットワーク使用状況	ネットワーク使用状況規則を設定して、iOSデバイスで管理対象のアプリケーションが携帯データネットワークなどのネットワークをどのように使用するのかを指定できます。 規則は管理対象のアプリケーションにのみ適用されます。 管理対象のアプリケーションとは、XenMobileを使用してユーザーのデバイスに展開されるアプリケーションです。 これには、ユーザーがXenMobileを使用して展開することなく直接デバイスにダウンロードしたアプリケーションや、デバイスのXenMobileへの登録時に既にデバイスにインストールされていたアプリケーションは含まれません。
アプリケーション制限	このポリシーによって、ユーザーによるSamsung KNOXデバイスへのインストールを禁止するアプリケーションのブラックリストを作成したり、ユーザーによるインストールを許可するアプリケーションのホワイトリストを作成したりできます。
アプリトンネル	アプリトンネルポリシーは、モバイルアプリケーションのサービスの継続性およびデータ転送の信頼性を向上させるように構成できます。 アプリトンネルは、モバイルデバイスアプリケーションのクライアントコンポーネントとアプリケーションサーバーコンポーネント間のプロキシパラメーターを定義します。 また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。 注：このポリシーで定義したトンネルを使用して送信されるアプリケーショントラフィックは、XenMobileを経由してから、アプリケーションを実行するサーバーにリダイレクトされます。
アプリケーションのアンインストール	アプリケーションアンインストールポリシーにより、さまざまな理由でユーザーのデバイスからアプリケーションを削除できます。 この理由には、特定のアプリケーションをサポートしなくなったことや、会社が既存アプリケーションから異なるベンダーが提供する類似アプリケーションへの置き換えを希望していることなどがあります。 このポリシーがユーザーのデバイスに展開されると、アプリケーションが削除されます。 Samsung KNOX以外のデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージが表示されます。Samsung KNOXデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージは表示されません。
アプリケーションのアンインストール制限	このポリシーによって、ユーザーがアンインストールできる、またはアンインストールできないアプリを指定できます。
Webブラウザー	ブラウザーデバイスポリシーを作成して、ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、ユーザーのデバイスで使用できるブラウザー機能を制限したりすることができます。 Samsungデバイスでは、ブラウザーを完全に無効にすることや、ポップアップ、JavaScript、Cookie、オートフィル、不正Webサイト警告の適用の有無を有効または無効にすることができます。 Android for Worksデバイスでは、特定のURLをブラックリストまたはホワイトリストに追加したり、特定のセキュアブラウザーのブックマークを追加したりすることができます。
カレンダー（CalDav）	XenMobileでデバイスポリシーを追加して、カレンダー（CalDAV）アカウントをユーザーのiOSデバイスまたはMax OS Xデバイスに追加し、CalDAVをサポートするサーバーとそのデバ

	イスのスケジュールデータを同期することができます。
移動体通信	このポリシーを使用すると、モバイルネットワーク設定を構成できます。
接続マネージャー	XenMobileでは、インターネットおよびプライベートネットワークに自動的に接続するアプリケーションの接続設定を指定できます。 このポリシーはWindows Pocket PCでのみ使用できます。
接続スケジュール	このポリシーは、AndroidおよびWindows Mobileデバイスが MDM管理、アプリのプッシュ、ポリシーの展開のためにXenMobileサーバーに接続する際に必要です。 このポリシーを送信せず、Google GCMを有効にしていない場合、デバイスはサーバーに接続することができません。 このため、デバイスの登録では、ベースパッケージでこのポリシーをプッシュする必要があります。
連絡先（CardDAV）	XenMobileでデバイスポリシーを追加して、iOS連絡先（CardDAV）アカウントをユーザーのiOSデバイスまたはMac OS Xデバイスに追加し、CardDAVをサポートするサーバーとそのデバイスの連絡先データを同期することができます。
Samsungコンテナーへのアプリケーションのコピー	デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナーまたはKNOXコンテナーにコピーされるように指定できます。 SEAMSコンテナーにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナーにコピーされたアプリケーションは、ユーザーがKNOXコンテナーにサインインした場合のみ使用できます。
資格情報	XenMobileで資格情報デバイスポリシーを作成し、XenMobileのPKI構成（PKIエンティティ、キーストア、資格情報プロバイダー、サーバー証明書など）を使用した統合認証を有効にすることができます。 資格情報について詳しくは、「XenMobileでの証明書」を参照してください。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、「資格情報デバイスポリシー」の記事で説明しています。 注：このポリシーを作成するには、各プラットフォームで使用する予定の資格情報と、証明書およびパスワードが必要です。
Samsungコンテナーへのアプリケーションのコピー	デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナーまたはKNOXコンテナーにコピーされるように指定できます。 サポートされるデバイスの詳細については、SamsungのSamsung KNOX Supported Devicesを参照してください。 SEAMSコンテナーにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナーにコピーされたアプリケーションは、ユーザーがKNOXコンテナーにサインインした場合のみ使用できます。
資格情報	WiFiポリシーと連携して使用されることの多いこのポリシーによって、組織が認証証明書を必要とする内部のリソースに認証証明書を展開することができます。

カスタムXML	以下の機能をカスタマイズする場合、XenMobileでカスタムXMLポリシーを作成できます。 ● プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。 ● デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。 ● ソフトウェアのアップグレード。アプリケーションやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。 ● 障害管理。デバイスからのエラーおよび状態レポートの受信などです。 WindowsでOpen Mobile Alliance Device Management（OMA DM）APIを使用して、カスタムXML構成を作成します。 OMA DM APIを使用したカスタムXMLの作成については、このトピックでは扱いません。 OMA DM APIの使用について詳しくは、Microsoft Developer Networkサイトの「OMA Device Management」を参照してください。
ファイルおよびフォルダーの削除	XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のファイルまたはフォルダーを削除できます。
レジストリ キーと値の削除	XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のレジストリキーおよび値を削除することができます。
デバイス正常性構成証明	XenMobileでは、分析目的で特定のデータおよびランタイム情報をHealth Attestation Service（HAS）に送信させ、Windows 10デバイスに正常性状態を報告させるポリシーを作成することができます。 HASは、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスからXenMobileに送信されます。 XenMobileは正常性構成証明書を受信すると、その内容に基づいて、管理者が以前に設定した自動アクションを展開します。 HASによって検証されるデータは以下のとおりです。 ● AIKの有無 ● Bit Lockerの状態 ● ブートデバッグが有効化されているかどうか ● ブートマネージャーのバージョン ● コードの整合性チェックが有効化されているかどうか ● コード整合性のバージョン ● DEP ポリシー ● ELAMドライバーが起動されているかどうか ● 発行元 ● カーネルのデバッグが有効化されているかどうか ● PCR ● リセット回数 ● 再起動の回数 ● セーフモードが有効化されているかどうか ● SBCPハッシュ ● セキュアブートが有効化されているかどうか ● テスト署名が有効化されているかどうか ● VSMが有効であること。 ● WinPEが有効であること。

	詳しくは、MicrosoftのHealthAttestation CSPページを参照してください。
名前	デバイス名ポリシーでは、デバイスを特定しやすくするために、iOSデバイスおよびMac OS Xデバイスに名前を設定できます。 デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。 マクロについて詳しくは、「XenMobileのマクロ」を参照してください。
エンタープライズハブ	Windows PhoneのEnterprise Hubデバイスポリシーでは、Enterprise Hub Companyストアを通じてアプリケーションを配布できます。 このポリシーを作成するには以下が必要です。 ● SymantecからのAET（.aetx）署名証明書 ● Microsoftのアプリケーション署名ツール（XapSignTool.exe）を使用して署名されたCitrix Company Hubアプリケーション 注：XenMobileでは、Windows Phone Worx Homeの1つのモードについて、1つのEnterprise Hubポリシーがサポートされています。 たとえば、Windows Phone Worx Home for XenMobile Enterprise Editionをアップロードするために、複数のEnterprise Hubポリシーをさまざまなバージョンの Work Home for XenMobile Enterprise Edition用に作成する必要はありません。 デバイスの登録中に最初のEnterprise Hubポリシーを展開するだけです。
Exchange	XenMobileでは、電子メールを送信する2つのオプションがあります。 コンテナー化されたWorxMailアプリを使用してActiveSyncメールを送信するか、MDM Exchangeポリシーを使用してデバイス上のネイティブの電子メールクライアントでActiveSyncメールを有効にできます。
Files	このポリシーで、ユーザーに対して特定の機能を実行するスクリプトファイル、またはAndroidデバイスユーザーがデバイスでアクセスできるドキュメントファイルを、XenMobileに追加できます。 ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。 たとえば、Androidユーザーが会社のドキュメントまたは.pdfファイルを受け取るようにする場合は、ファイルをデバイスに展開し、ユーザーにファイルがある場所を知らせます。 このポリシーで追加できるファイルの種類は次のとおりです。 ● テキストベースのファイル（.xml、.html、.pyなど） ● ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル ● Windows MobileおよびWindows CEのみ：MortScriptで作成されたスクリプトファイル
フォント	XenMobileでこのデバイスポリシーを追加して、追加フォントをユーザーのiOSデバイスおよびMac OS Xデバイスに追加することができます。 フォントはTrueType（.ttf）またはOpenType（.oft）である必要があります。 フォントコレクション（.ttcまたは.otc）はサポートされません。 注：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。

iOSおよびMac OS Xプロファイルのインポート	iOSおよびOS Xデバイス用のデバイス構成MXLファイルをXenMobileにインポートできます。 XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。 Apple Configuratorの使用による構成ファイルの作成について詳しくは、AppleのConfiguratorヘルプページを参照してください。
キオスク	XenMobileでキオスクポリシーを作成して、特定のアプリケーションのみをSamsung SAFEデバイスで使用できるように指定することができます。 このポリシーは、特定の種類またはクラスのアプリケーションのみを実行するように設計されているコーポレートデバイスで役立ちます。 また、このポリシーを使用して、デバイスがキオスクモードのときのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。 注： • キオスクモード用に指定したすべてのアプリケーションが、ユーザーのデバイスに既にインストールされている必要があります。 • 一部のオプションは、Samsungモバイルデバイス管理（MDM）API 4.0以降にのみ適用されます。
LDAP	XenMobileでiOSデバイスのLDAPポリシーを作成して、必要なアカウント情報など、使用するLDAPサーバーに関する情報を指定できます。 また、LDAPサーバーの照会に使用するLDAP検索ポリシーのセットが提供されます。 このポリシーを構成するには、LDAPホスト名が必要です。
Location	位置情報ポリシーは地図上で位置を検出できるデバイスのGPSがWorxHomeに対応している場合に使用できます。 このポリシーがデバイスでプッシュされると、管理者はXenMobileサーバーから位置を確認するコマンドを送信し、デバイスは位置情報を返信します。 ジオフェンシングおよび追跡ポリシーもサポートされます。
メール	XenMobileでメールデバイスポリシーを追加して、ユーザーのiOSデバイスまたはMac OS Xデバイスのメールアカウントを構成することができます。
管理対象ドメイン	このポリシーによって、メールおよびSafariブラウザーに適用する管理対象ドメインを定義できます。 管理対象ドメインを使用すると、Safariを使用してドメインからダウンロードしたドキュメントを開くことができるアプリケーションを制御して、会社のデータを保護することができます。 URLまたはサブドメインを使用して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御します。 このポリシーは、iOS 8以降の監視対象デバイスでのみサポートされます。 iOSデバイスをSupervisedモードに設定する手順については、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。 ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。 ユーザーがSafariを使用して、管理対象Webドメイン一覧に含まれているWebドメインから取得したアイテム（ドキュメントや添付ファイルなど、ダウンロードしたもの）を開こうとす

	ると、適切な社内アプリケーションによってアイテムが開かれます。 アイテムが管理対象Webドメイン一覧にあるWebドメインから取得されたものでない場合、ユーザーは社内アプリケーションでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリケーションを使用する必要があります。
Microsoft Exchange ActiveSync	Exchange ActiveSyncデバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchangeでホストされている会社のメールにアクセスできるようにすることができます。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、Microsoft Exchange ActiveSyncのトピックで説明しています。
MDMオプション	XenMobileでデバイスポリシーを作成して、監視対象のiOS 7.0以降のモバイルバイスで［iPhone/iPadを探す］の［アクティベーションロック］を管理することができます。 iOSデバイスをSupervisedモードに設定する手順については、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」または「iOSバルク登録」を参照してください。 アクティベーションロックは、紛失したり、盗まれたりしたデバイスが再アクティベーションされないようにすることを目的とした［iPhone/iPadを探す］の機能であり、ユーザーのApple IDおよびパスワードを必須にすることで、誰かが［iPhone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ションして使用したりするのを防ぎます。XenMobileでは、MDMオプションデバイスポリシーでアクティベーションロックを有効にすることにより、必須とされているApple IDおよびパスワードの入力をバイパスできます。ユーザーから返却されたデバイスで［iPhoneを探す］が有効になっていた場合、Appleの資格情報なしでXenMobileコンソールからデバイスを管理することができます。
組織情報	XenMobileでデバイスポリシーを追加して、XenMobileからiOSデバイスにプッシュされるアラートメッセージ用の組織情報を指定できます。 このオプションはiOS 7以降のデバイスで使用できます。
パスコード	パスコードポリシーによって、管理対象デバイスにPINコードまたはパスワードを適用できます。 このパスコードポリシーは、デバイス上でパスコードの複雑さやタイムアウトを設定します。
個人用ホットスポット	このポリシーによって、iOSデバイスの個人用ホットスポット機能を介して携帯データネットワーク接続を使用することにより、ユーザーがWiFiネットワーク圏外にいてもインターネットに接続できるようにすることができます。 iOS 7.0以降で利用できます。
プロファイル削除	XenMobileで、アプリケーションプロファイル削除デバイスポリシーを作成することができます。 ポリシーを展開すると、ユーザーのiOSデバイスまたはMac OS Xデバイスからアプリケーションプロファイルが削除されます。
プロビジョニングプロファイル	iOSエンタープライズアプリを開発しコード署名するときは、通常は、iOSデバイスで実行するアプリにAppleが求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーが開くためにタップするとそのアプリはクラッシュします。

	プロビジョニングプロファイルの主な問題は、Apple Developer Portalで生成されてから1年で期限が切れるので、ユーザーによって登録されたすべてのiOSデバイス上のすべてのプロビジョニングファイルの期限を追跡する必要があることです。 期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。 解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信する、プロビジョニングプロファイルをWebポータルに置いてダウンロードとインストールを可能にする、という2つの方法があります。 これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Webポータルにアクセスして適切なプロファイルをダウンロードしインストールすることを求めたりするので、エラーが発生する傾向があります。 このプロセスをユーザーが意識しないで済むように、XenMobileではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。 紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。
プロビジョニングプロファイルの削除	デバイスプリシーを使用してiOSプロビジョニングプロファイルを削除できます。 プロビジョニングプロファイルについて詳しくは、「プロビショニングプロファイルの追加」を参照してください。
プロキシDHCP	XenMobileでデバイスポリシーを追加して、Windows Mobile/CEおよびiOS 6.0以降を実行しているデバイスのグローバルHTTPプロキシ設定を指定できます。 グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。 注：このポリシーを展開する前に、グローバルHTTPプロキシを設定するすべてのiOSデバイスを必ずSupervisedモードに設定してください。 詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。
レジストリ	Windows Mobile/CEのレジストリには、アプリケーション、ドライバー、ユーザー設定、および構成設定に関するデータが格納されています。 XenMobileでは、Windows Mobile/CEデバイスを管理するためのレジストリキーおよび値を定義できます。
リモートサポート	XenMobileでリモートサポートポリシーを作成して、ユーザーのSamsung KNOXデバイスへのリモートアクセスを行うことができます。 次の2種類のサポートを構成できます。 ● ［Basic］は、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率とCPU使用率）、インストールされているソフトウェアフォルダーの内容など、デバイスに関する診断情報を表示できます。 ● ［Premium］は、色の制御（メインウィンドウまたは独立した浮動ウィンドウ）、ヘルプデスクとユーザーの間のVoIP（Voice-over-IP）セッションの確立、設定の構成、ヘルプデスクとユーザーの間のチャットセッションの確立など、デバイスの画面をリモート制御できます。
制限事項	制限ポリシーによって、管理者は管理対象デバイスをロックダウンしたり、機能を制御するさまざまなオプションを使用できます。 文字通り数百の制限オプションがあり、デバイスの

	カメラやマイクを無効にしたり、ローミング規則の適用やアプリケーションストアのようなサードパーティサービスへのアクセスなどに対応します。 XenMobileでデバイスポリシーを追加して、ユーザーのデバイス、電話、タブレットなどの特定の機能を制限できます。 プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。 このデバイスポリシーでは、デバイスの特定の機能（カメラなど）をユーザーが使用することを許可または制限します。 また、セキュリティ制限、メディアコンテンツの制限、ユーザーがインストールできる（できない）アプリケーションの種類の制限を設定できます。 ほとんどの制限設定は、デフォルトでは［ON］（許可）に設定されています。 例外は、iOSセキュリティの強制機能とすべてのWindowsタブレット機能です。デフォルトで［OFF］（制限）に設定されています。 ヒント：いずかのオプションで［ON］を選択すると、ユーザーがその操作を実行またはその機能を使用できるようになります。 次に例を示します。 • Camera。 ［ON］の場合、ユーザーはデバイスでカメラを使用できます。 ［OFF］の場合、ユーザーはデバイスでカメラを使用できません。 • ［Screen shots］。 ［ON］の場合、ユーザーはデバイスでスクリーンショットを取得できます。 ［OFF］の場合、ユーザーはデバイスでスクリーンショットを取得できません。
移動	XenMobileでデバイスポリシーを追加して、ユーザーのiOSデバイスおよびWindows Mobile/CEデバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。 音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。 iOSの場合、このポリシーはiOS 5.0以降のデバイスでのみ使用できます。
Samsung SAFEファイアウォール	このポリシーにより、Samsungデバイスのファイアウォール設定を構成できます。 デバイスにアクセスを許可するIPアドレス、ポート、ホスト名、またはデバイスのアクセスをブロックするIPアドレス、ポート、ホスト名を入力します。 プロキシおよびプロキシ再ルーティングの設定を構成することもできます。
Samsung MDMライセンスキー	XenMobileはSamsung for Enterprise（SAFE）およびSamsung KNOXポリシーの両方をサポートし、拡張しています。 SAFEは、モバイルデバイス管理（MDM：Mobile Device Management）ソリューションとの統合を通じてビジネス向けのセキュリティおよび機能拡張を提供するソリューションファミリーです。 Samsung KNOXは、企業向けにより高いセキュリティで保護されたAndroidプラットフォームを提供する、SAFEプログラム内のソリューションです。 SAFEのポリシーおよび制限を展開する前に、組み込みのSamsung Enterprise License Management（ELM）キーをデバイスに展開することによってSAFE APIを有効にする必要があります。 また、Samsung KNOX APIを有効にするには、Samsung ELMキーの展開に加え、Samsung KNOX License Management System（KLMS）を使用してSamsung KNOXライセンスを購入する必要もあります。 Samsung KLMSはモバイルデバイス管理（MDM：Mobile Device Management）ソリューションに有効なライセンスをプロビジョニングし、モバイルデバイスでSamsung KNOX APIをアクティブ化できるようにします。 これらのライセンスはSamsungから取得する必要があり、Citrixからは提供されません。

	Worx HomeをSamsung ELMキーと共に展開し、SAFEおよびSamsung KNOX APIを有効にする必要があります。 SAFE APIが有効になっていることは、デバイスプロパティをチェックすることで確認できます。 Samsung ELMキーが展開されると、［Samsung MDM API available］設定が［True］に設定されます。
SCEP	このポリシーでiOSデバイスとMax OS Xデバイスを構成し、SCEP（Simple Certificate Enrollment Protocol）を使用して外部SCEPサーバーから証明書を取得することができます。 XenMobileに接続されているPKIからSCEPを使用してデバイスに証明書を配布する場合は、PKIエンティティとPKIプロバイダーを分散モードで作成する必要があります。 詳しくは、「PKIエンティティ」を参照してください。
サイドローディングキー	XenMobileのサイドローディングにより、Windows Storeから購入していないアプリケーションをWindows 8.1デバイスに展開できます。 最もよくある場合として、会社用に開発し、Windowsストアで公開したくないアプリケーションをサイドロードします。 アプリケーションをサイドロードするには、サイドローディングキーとキーアクティブ化を構成して、アプリケーションをユーザーのデバイスに展開します。 このポリシーを作成する前に以下の情報が必要です。 • サイドローディングプロダクトキー。Microsoftボリュームライセンスサービスセンターにサインインして取得します。 • キーアクティブ化。サイドローディングプロダクトキーを取得した後に、コマンドラインを使用して作成します。
証明書署名	XenMobileでデバイスポリシーを追加して、APPXファイルへの署名に使用される署名証明書を構成することができます。 署名証明書は、ユーザーにAPPXファイルを配布して、ユーザーがWindowsタブレットにアプリケーションをインストールできるようにする場合に必要です。
Single Sign On（SSO）アカウント	XenMobileでシングルサインオン（SSO）アカウントを作成して、ユーザーが1回サインオンするだけで、さまざまなアプリケーションからXenMobileおよび社内リソースにアクセスすることができるようにします。 デバイスに資格情報を保存する必要はありません。 SSOアカウントエンタープライズユーザーの資格情報は、App Storeからのアプリケーションを含む複数のアプリケーションで使用されます。 このポリシーは、Kerberos認証バックエンドで動作するように設計されています。 注：このポリシーはiOS 7.0以降にのみ適用されます。
ストレージ暗号化	XenMobileでストレージ暗号化デバイスポリシーを作成して、内部ストレージと外部ストレージを暗号化したり、デバイスによっては、ユーザーがデバイスでストレージカードを使用できないようにしたりします。 Samsung SAFE、Windows Phone、Android Sonyデバイスに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ストレージ

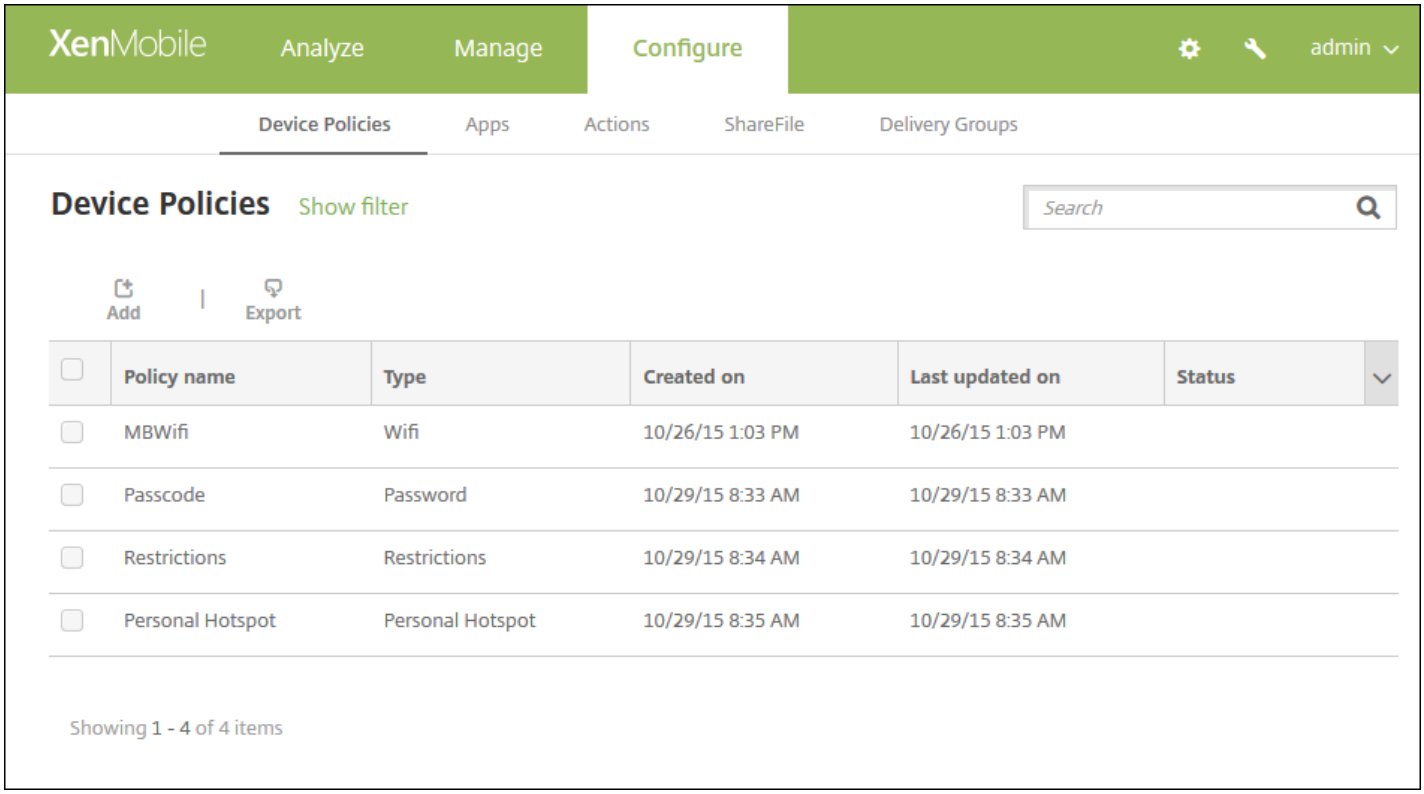
	暗号化ポリシーのトピックで説明しています。
サブスクライブされたカレンダー	XenMobileでデバイスポリシーを追加して、サブスクライブされたカレンダーをユーザーのiOSデバイスのカレンダー一覧に追加することができます。 サブスクライブできる公開カレンダーの一覧は、www.apple.com/downloads/macosx/calendarsにあります。 注：ユーザーのデバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みである必要があります。
契約条件	社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、XenMobileで契約条件デバイスポリシーを作成します。 ユーザーがXenMobileにデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。 契約条件を拒否すると、登録処理が取り消されます。 社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。 展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。 Androidデバイスおよびiosデバイスの場合は、PDFファイルを提供する必要があります。 Windowsデバイスの場合は、テキスト（TXT）ファイルと付属のイメージファイルを提供する必要があります。
VPN	従来のVPN Gatewayテクノロジーでバックエンドシステムにアクセスを提供する必要がある場合、このVPNポリシーを使用してVPNゲートウェイ接続の詳細をデバイスにプッシュできます。 このポリシーでは、さまざまなVPNプロバイダー（Citrix VPNに加えてCisco AnyConnect、Juniperなど）がサポートされています。 また、このポリシーをCAにリンクして、オンデマンドでVPNオンデマンドを有効にできます（VPNゲートウェイがこのオプションをサポートしている場合）。 XenMobileでデバイスポリシーを追加して、VPN（Virtual Private Network：仮想プライベートネットワーク）の設定を構成し、ユーザーのデバイスが社内リソースに安全に接続できるようにすることができます。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、VPNのトピックで説明しています。
壁紙	.pngファイルまたは.jpgファイル追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。 iOS 7.1.2以降で使用できます。 iPadおよびiPhoneで異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。
Webコンテンツフィルター	XenMobileでデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトとAppleのオートフィルター機能を組み合わせて使用して、iOSデバイスでWebコンテンツをフィルタリングできます。 このポリシーはiOS 7.0以降のSupervisedモードのデバイスでのみ使用できます。 iOSデバイスをSupervisedモードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。
[Webclip	このポリシーでは、ショートカットやWebクリップをWebサイトに配置してユーザーデバイ

	スのアプリと一緒に表示できます。 iOS、Mac OS X、AndroidデバイスのWebクリップを表す独自のアイコンを指定できます。Windowsタブレットのみ、ラベルおよびURLが必要になります。
WiFi	WiFiポリシーによって、管理者はSSID、認証データ、構成データなどWiFiルーターの詳細を簡単に管理対象デバイスにプッシュできます。 WiFiポリシーでは、ネットワークの名前と種類、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の有無や、そのほかのWiFi関連事項を、特定のプラットフォームのすべてのユーザーに対して一貫的に定義し、ユーザーデバイスのWiFiネットワークへの接続方法を管理できます。 左側の一覧にある関連プラットフォームのWiFi設定を構成できますが、プラットフォームごとに必要な値が異なります。これらの値について詳しくは、このセクションのWiFiのトピックで説明しています。
Windows CE証明書	このデバイスポリシーを追加して、外部のPKIを基にWindows Mobile/CE PKI証明書を作成し、ユーザーのデバイスに配布できます。 証明書およびPKIエンティティについて詳しくは、「証明書」を参照してください。
Worx Store	XenMobileでポリシーを作成して、iOS、Android、またはWindowsタブレットデバイスのホーム画面でWorx StoreのWebクリップを表示するかどうかを指定できます。
XenMobileオプション	XenMobileオプションポリシーを追加して、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのWorx Homeの動作を構成します。
XenMobileのアンインストール	XenMobileでこのデバイスポリシーを追加して、XenMobileをAndroidデバイスおよびWindows Mobile/CEデバイスからアンインストールすることができます。 このポリシーを展開すると、展開グループ内のすべてのデバイスからXenMobileが削除されます。

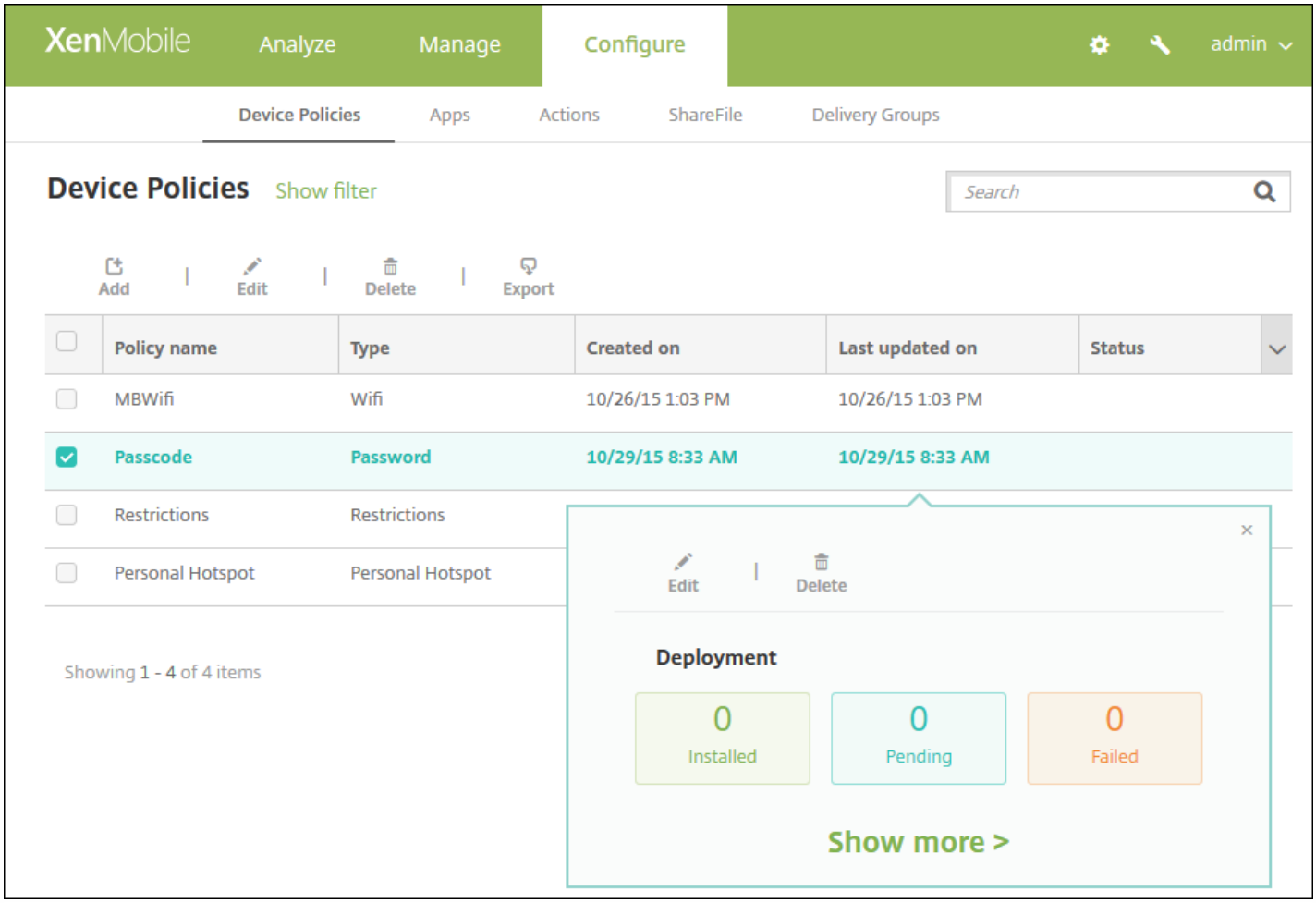
コンソールの［Device Policies］ページ

デバイスポリシーの操作は、XenMobileコンソールの**［Device Policies］**ページで行います。 **［Device Policies］**ページにアクセスするには、 **［Configure］の［Device Policies］**をクリックします。 このページで新しいポリシーを追加したり、既存のポリシーの状態を確認したり、ポリシーを編集または削除したりすることができます。

［Device Policies］ページには、現在のポリシーをすべて示す表があります。



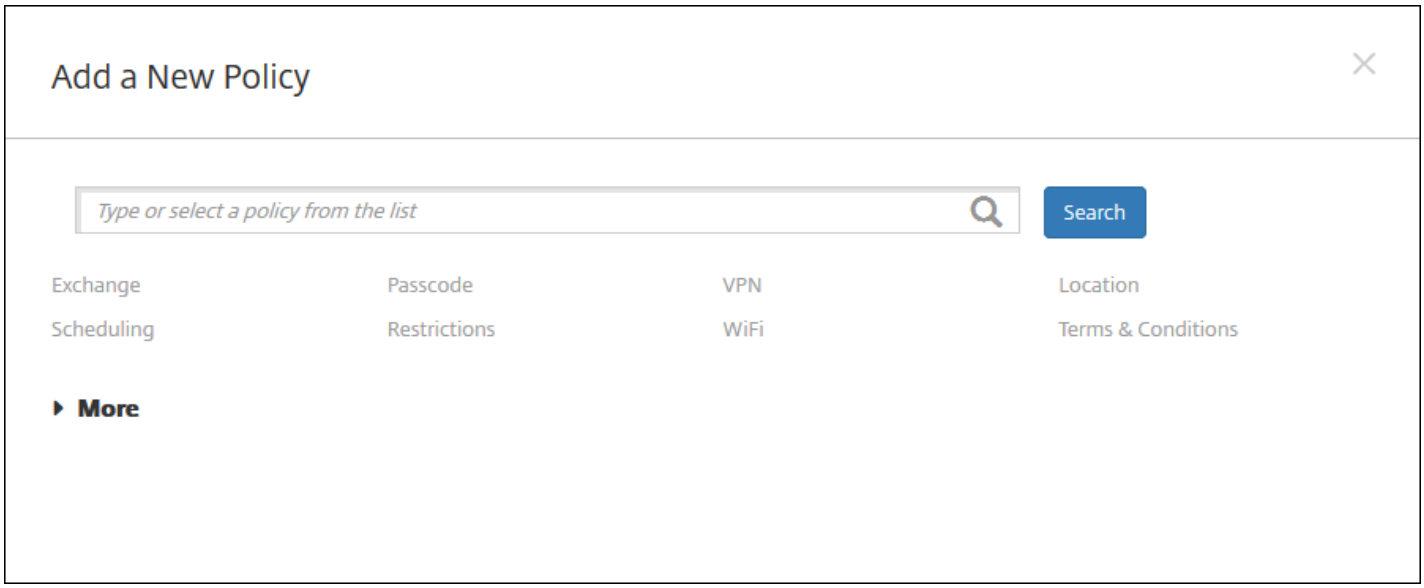
［**Device Policies**］ページでポリシーを編集または削除するには、ポリシーの横のチェックボックスをオンにしてポリシー一覧の上に表示されるオプションメニューを使用するか、一覧内でポリシーをクリックして項目の右側に表示されるオプションメニューを使用します。 ［**Show More**］をクリックすると、ポリシーの詳細が表示されます。



デバイスポリシーを追加するには

1. [**Device Policies**] ページで、 [**Add**] をクリックします。

[**Add a New Policy**] ダイアログボックスが開きます。 [**More**] を展開するとほかのポリシーを表示できます。

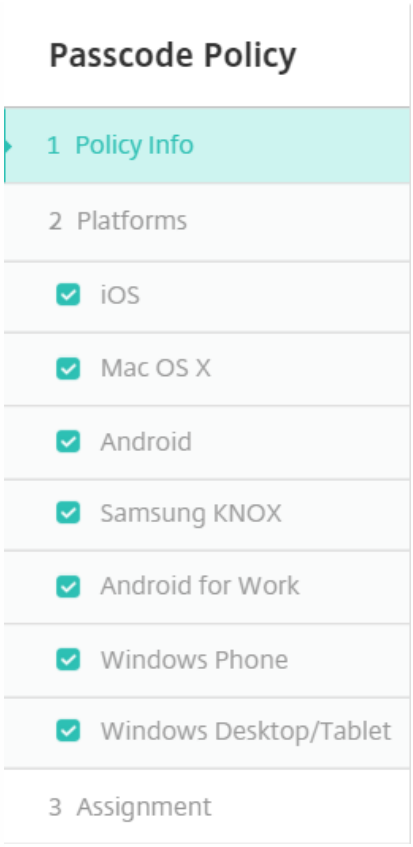


2. 追加するポリシーを検索するには、次のいずれかを実行します。

- ポリシーをクリックします。
  選択したポリシーの［**Policy Information**］ページが開きます。
- 検索フィールドにポリシーの名前を入力します。 入力すると一致候補が表示されます。 一覧の中に目的のポリシーがあれば、それをクリックします。 選択したポリシーのみがダイアログボックス内に残ります。 それをクリックして、そのポリシーの［**Policy Information**］ページを開きます。
  重要：選択したポリシーが［**More**］領域の中にある場合、［**More**］を展開した場合にのみ表示されます。

3. ポリシーに含めるプラットフォームを選択します。 選択したプラットフォームの構成ページが手順5.で表示されます。

注：ポリシーでサポートされるプラットフォームのみが一覧に表示されます。

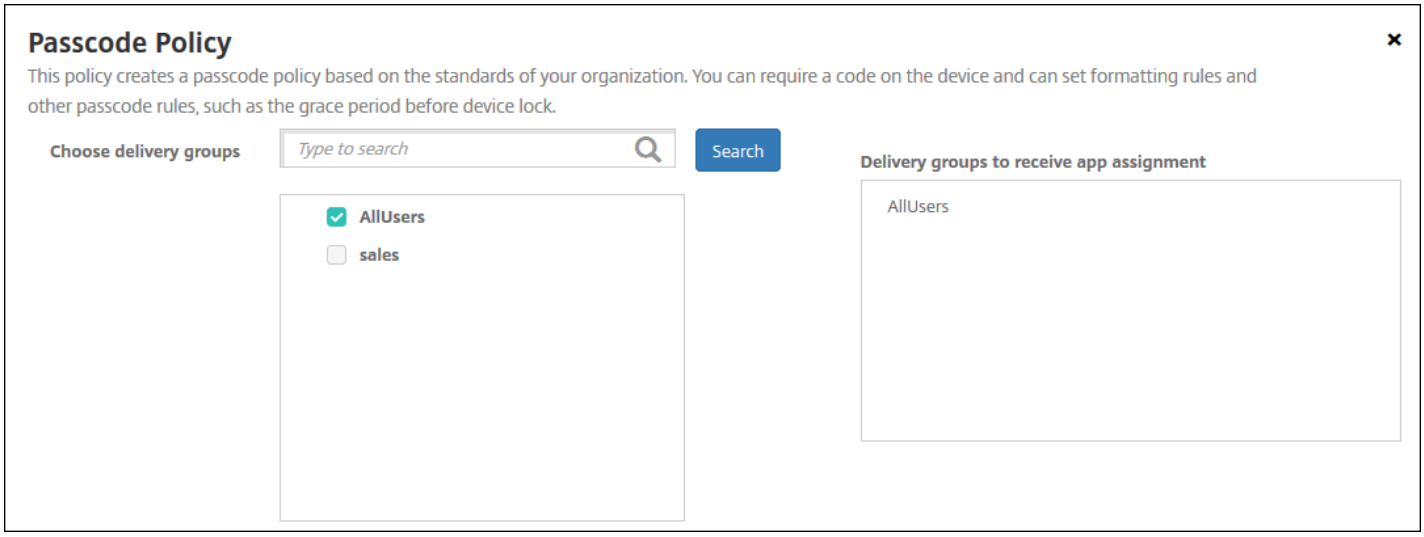


4. [**Policy Information**] ページで必要な情報を入力して、 [**Next**] をクリックします。 [**Policy Information**] ページにはポリシー名などの情報が集約されているため、ポリシーの識別や追跡に役立ちます。 このページはすべてのポリシーで類似しています。

5. プラットフォームページの入力を完了します。 手順3.で選択した各プラットフォームのページが開きます。 これらのページはポリシーごとに異なります。 各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でサポートされるわけではありません。 [**Next**] をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、 [**Assignment**] ページに移動します。

6. [**Assignments**] 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、 [**Delivery groups to receive app assignment**] ボックスにそのグループが表示されます。

注： [Delivery groups to receive app assignment] ボックスは、デリバリーグループを選択するまで表示されません。



7. [**Save**] をクリックします。

ポリシーが [**Device Policies**] の表に追加されます。

デバイスポリシーを編集または削除するには

1. [**Device Policies**] の表で、編集または削除するポリシーの横のチェックボックスをオンにします。
2. [**Edit**] または [**Delete**] をクリックします。

- [**Edit**] をクリックした場合、いずれかまたはすべての設定を編集できます。
- [**Delete**] をクリックした場合、確認ダイアログボックスで、もう一度 [**Delete**] をクリックします。

プラットフォーム別のXenMobileデバイスポリシー

Aug 30, 2016

プラットフォーム別のポリシーを確認するには、「Device Policies by Platform Matrix PDF」を参照してください。

デバイスポリシーの追加と構成は、XenMobileコンソールの［**Configure**］の［**Device Policies**］をクリックすると開くページで実行できます。
XenMobile 10.3は、以下のプラットフォームのデバイスポリシーをサポートしています。

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Phone 8/Windows 10 Mobile
- Windows 8およびWindows 10 Desktop/Tablet（.86）

> ## 注意
>
> XenMobile 10.3では、Symbianデバイスのサポートは廃止されました。

AirPlayミラーリングデバイスポリシー

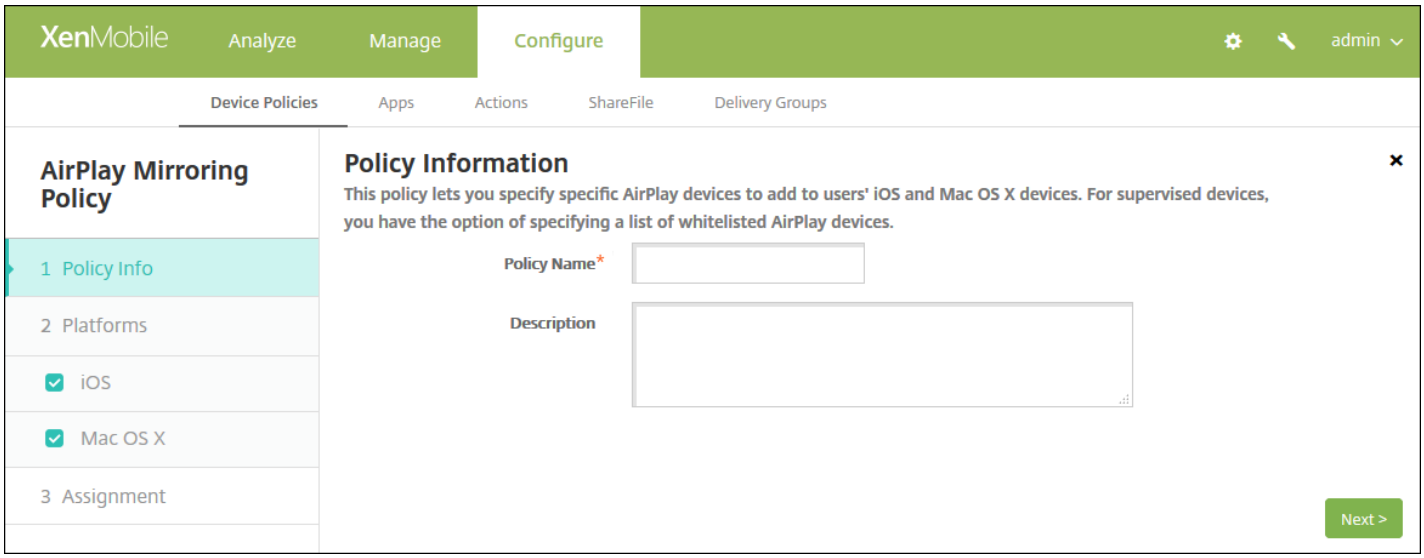
Aug 30, 2016

Apple AirPlay機能を使用すると、Apple TVを介してiOSデバイスからTV画面にコンテンツをワイヤレスでストリーム配信したり、デバイス上の表示をTV画面またはほかのMacコンピューターに正確にミラーリングしたりすることができます。

XenMobileでデバイスポリシーを追加して、特定のAirPlayデバイス（Apple TVやほかのMacコンピューターなど）をユーザーのiOSデバイスに追加することができます。 また、デバイスを監視対象デバイスのホワイトリストに追加して、ユーザーがホワイトリストにあるAirPlayデバイスのみに限定するオプションもあります。 デバイスをSupervisedモードに設定する方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。
注：続行する前に、追加するすべてのデバイスのデバイスIDとパスワードがあることを確認してください。
1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**More**］を展開した後、［**End user**］の下の［**AirPlay Mirroring**］をクリックします。 ［**AirPlay Mirroring Policy**］ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

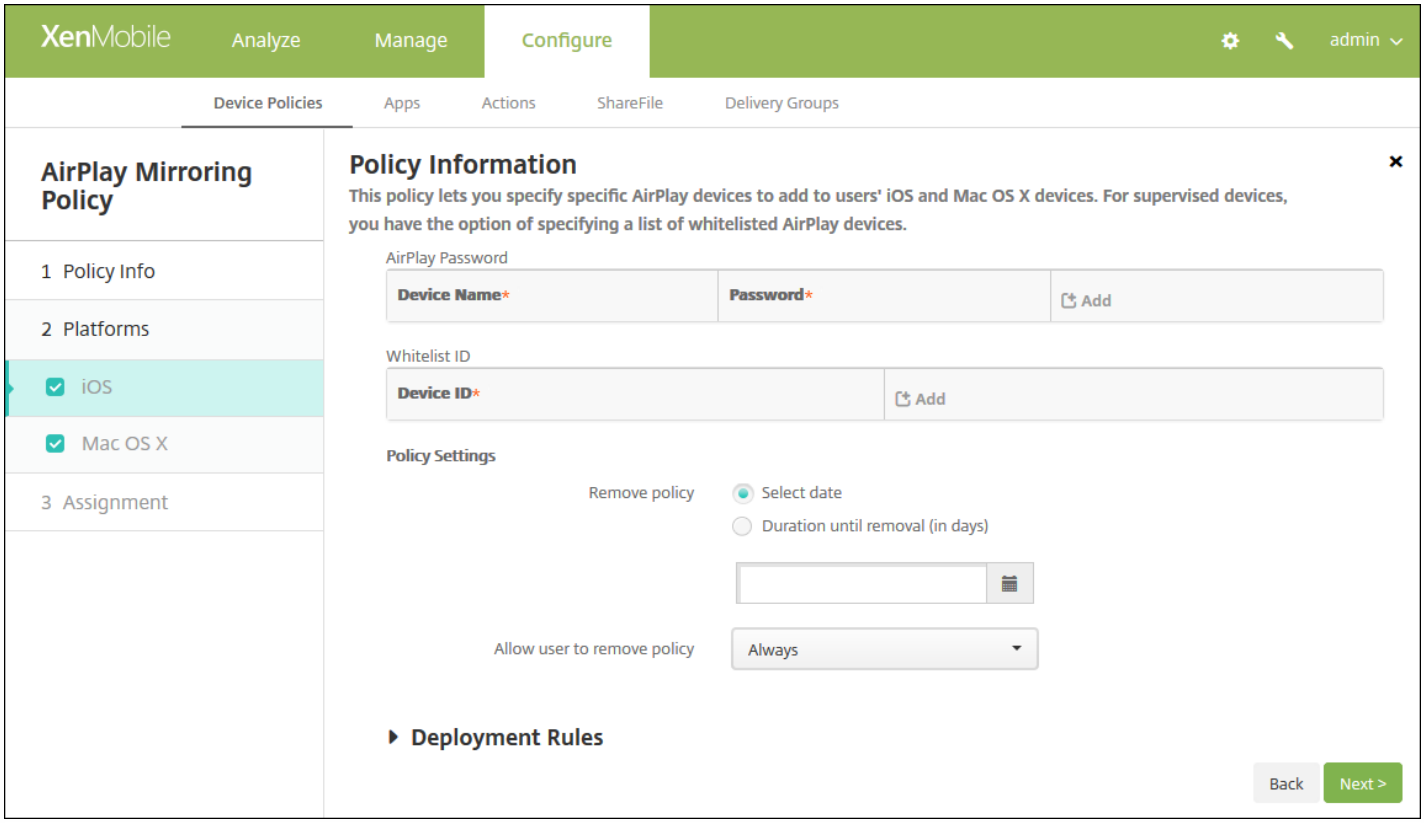
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Policy Platforms**］ページが開きます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



次の設定を構成します。

- **AirPlay Password**：追加するデバイスごとに、［**Add**］をクリックして以下の操作を行います。
  - **Device ID**：ハードウェアのアドレス（MACアドレス）を「xx:xx:xx:xx:xx:xx」の形式で入力します。 このフィールドでは大文字と小文字が区別されません。
  - **Password**：任意で、デバイスのパスワードを入力します。
  - ［**Add**］をクリックしてデバイスを追加するか、［**Cancel**］をクリックしてデバイスの追加を取り消します。
- **Whitelist ID**：この一覧は、監視対象ではないデバイスでは無視されます。 この一覧には、ユーザーのデバイスで使用できるAirPlayデバイスのデバイスIDのみを追加できます。 一覧に追加するAirPlayデバイスごとに、［**Add**］をクリックして以下の操作を行います。
  - **Device ID**：デバイスIDを「xx:xx:xx:xx:xx::xx」の形式で入力します。 このフィールドでは大文字と小文字が区別されません。
  - ［**Add**］をクリックしてデバイスを追加するか、［**Cancel**］をクリックしてデバイスの追加を取り消します。

    注：既存のデバイスを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

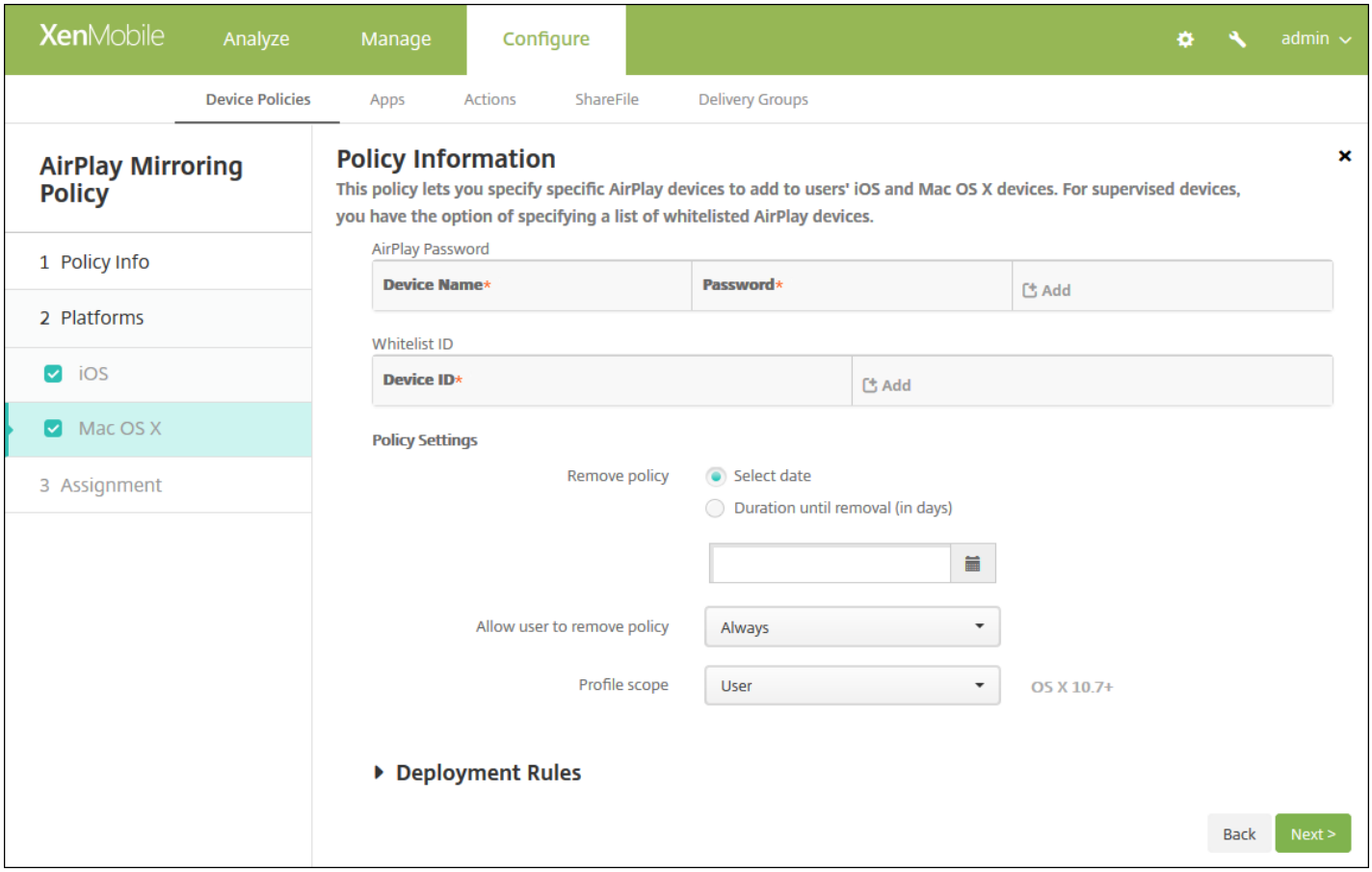
    既存のデバイスを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

- **ポリシー設定**
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択し

ます。

- ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **AirPlay Password**：追加するデバイスごとに、［**Add**］をクリックして以下の操作を行います。
  - **Device ID**：ハードウェアのアドレス（MACアドレス）を「xx:xx:xx:xx:xx::xx」の形式で入力します。 このフィールドでは大文字と小文字が区別されません。
  - **Password**：任意で、デバイスのパスワードを入力します。
  - ［**Add**］をクリックしてデバイスを追加するか、［**Cancel**］をクリックしてデバイスの追加を取り消します。
- **Whitelist ID**：この一覧は、監視対象ではないデバイスでは無視されます。 この一覧には、ユーザーのデバイスで使用できるAirPlayデバイスのデバイスIDのみを追加できます。 一覧に追加するAirPlayデバイスごとに、［**Add**］をクリックして以下の操作を行います。
  - **Device ID**：デバイスIDを「xx:xx:xx:xx:xx::xx」の形式で入力します。 このフィールドでは大文字と小文字が区別されません。
  - ［**Add**］をクリックしてデバイスを追加するか、［**Cancel**］をクリックしてデバイスの追加を取り消します。

  注：既存のデバイスを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

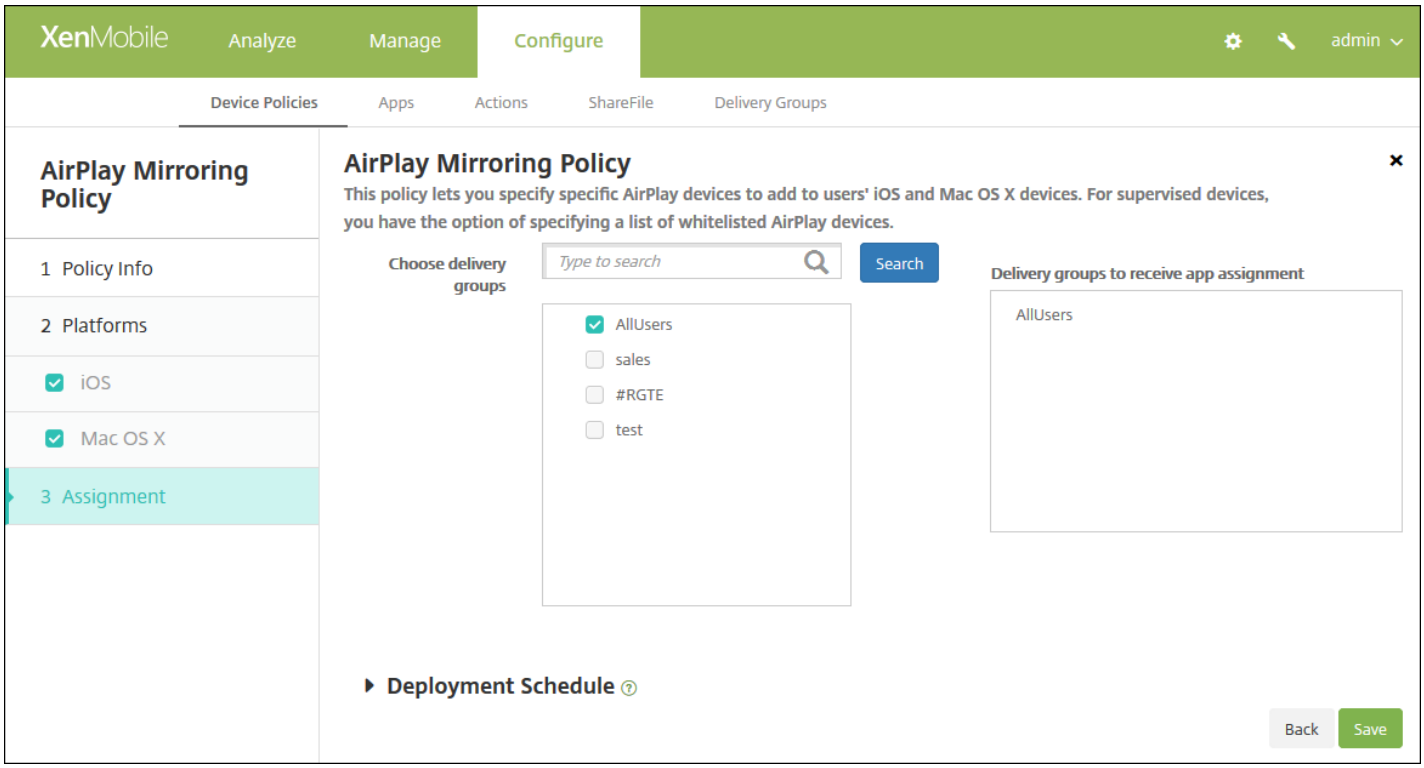
  既存のデバイスを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックし

ます。 項目を変更し、 [Save] をクリックして変更した項目を保存するか、 [Cancel] をクリックして項目を変更せずそのままにします。

- ポリシー設定
  - [Remove policy] の横の [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。
  - [Profile scope] の横にある、 [User] または [System] を選択します。 デフォルトは [User] です。

7. 展開規則の構成

8. [Next] をクリックします。 [AirPlay Mirroring Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

10. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、 [OFF] をクリックすると展開が行われません。 デフォルトのオプションは [ON] です。 [OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。 デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。 デフォルトのオプションは、 [On every connection] です。

- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

AirPrintデバイスポリシー

Aug 02, 2016

XenMobileでデバイスポリシーを追加して、AirPrintプリンターをユーザーのiOSデバイスのAirPrintプリンター一覧に追加できます。 このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。

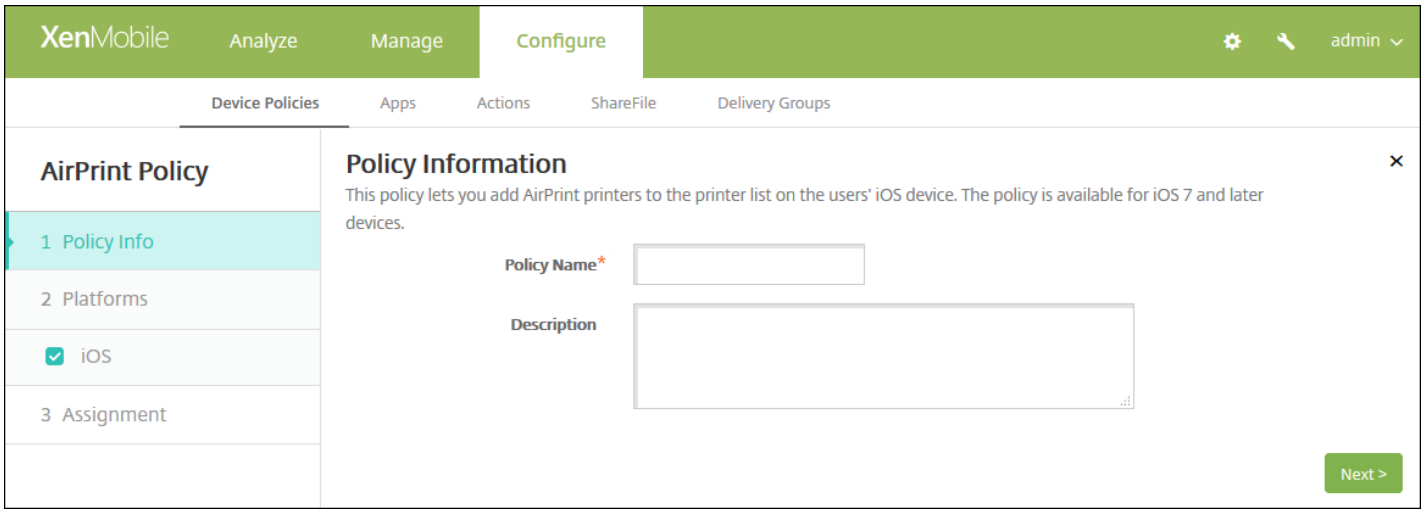
注：

- このポリシーはiOS 7.0以降に適用されます。
- 各プリンターのIPアドレスとリソースパスがあることを確認してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

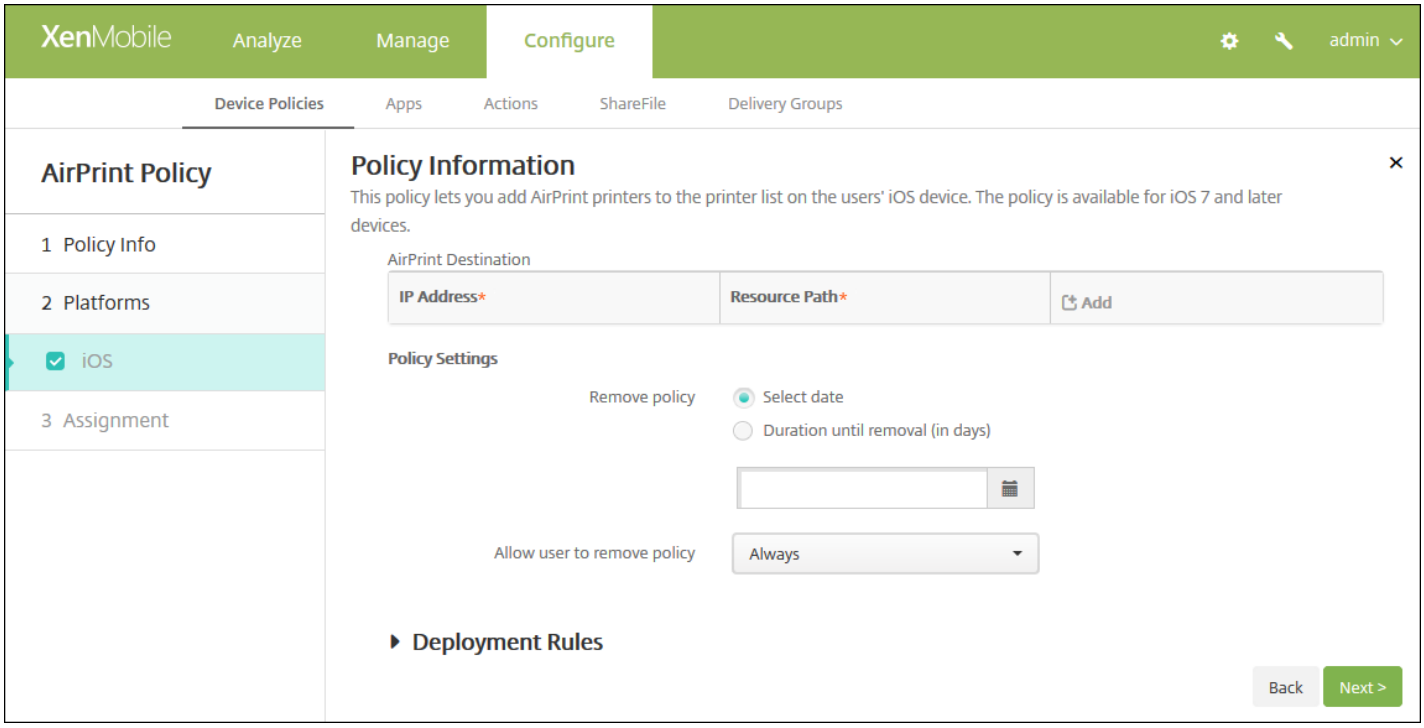
3. **[More]** をクリックした後、 **[End user]** の下の **[AirPrint]** をクリックします。 **[AirPrint Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[iOS Platform Information]** ページが開きます。



6. 次の設定を構成します。

- **AirPrint Destination**：追加するAirPrint対応プリンターごとに、［**Add**］をクリックして以下の操作を行います。
  - **IP Address**：AirPrintプリンターのIPアドレスを入力します。
  - **Resource Path**：プリンターに関連付けられているリソースパスを入力します。 この値は、_ipps.tcp Bonjourレコードのパラメーターに対応します。 たとえば、printers/Canon_MG5300_series or printers/Xerox_Phaser_7600。
  - ［**Save**］をクリックしてプリンターを追加するか、［**Cancel**］をクリックしてプリンターの追加を取り消します。

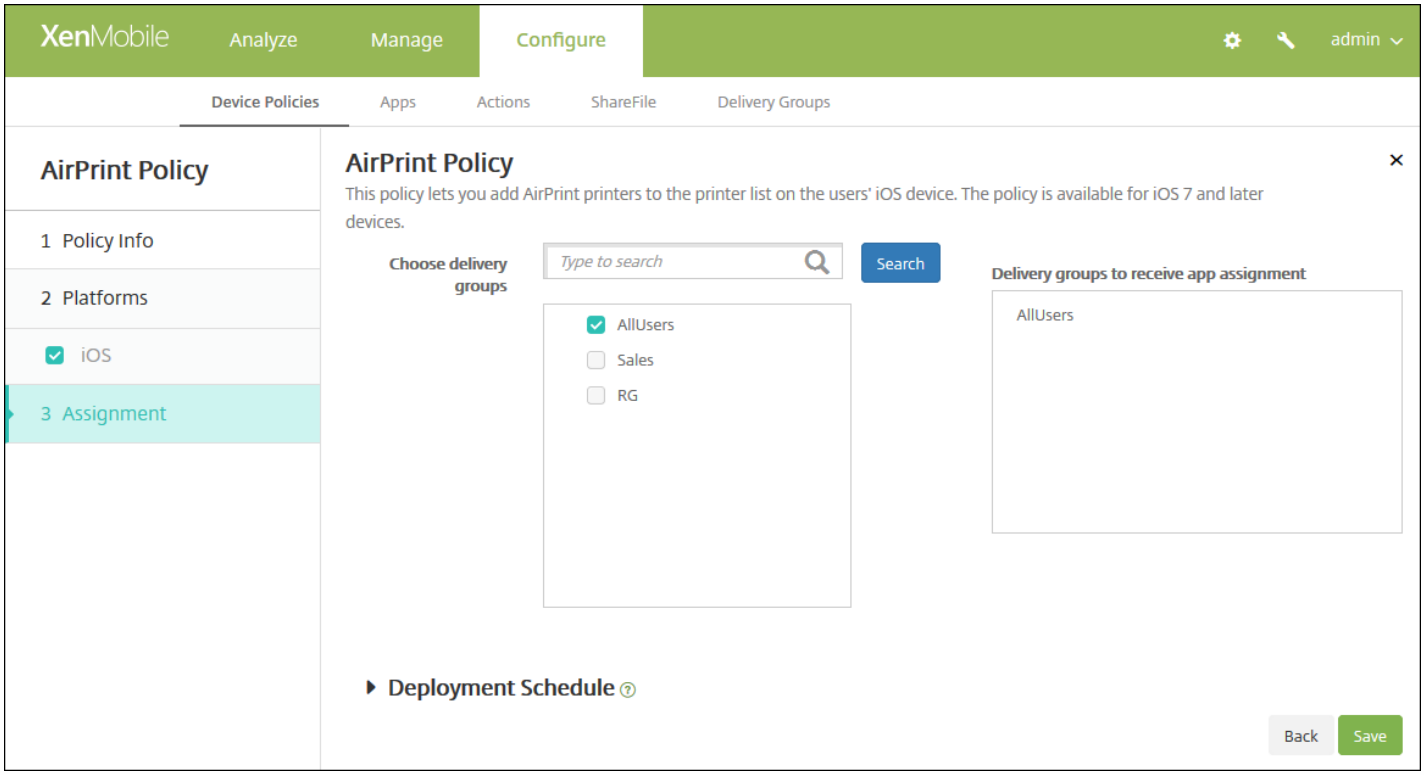
    注：既存のプリンターを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

    既存のプリンターを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

- **ポリシー設定**
  - ［**Policy Settings**］の下の［**Remove policy**］の横にある、［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**AirPrint Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

Android for Workアプリ制限ポリシー

Aug 02, 2016

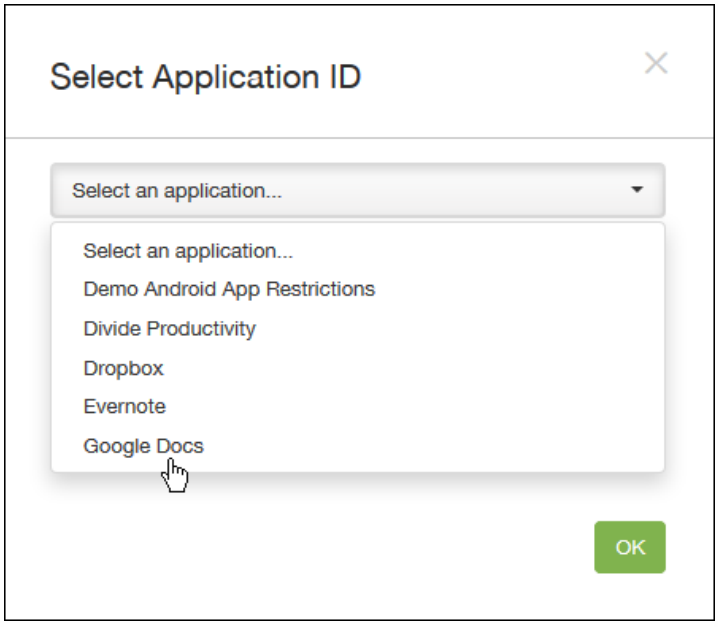
Android for Workアプリに関連する制限を変更できますが、そのためには、次の前提条件を満たす必要があります。

- GoogleのAndroid for Work設定タスクを完了します。 詳しくは、「Android for Workでのデバイスの管理」を参照してください。
- 一連のGoogle Play資格情報を作成します。 詳しくは、「Google Play資格情報」を参照してください。
- Android for Workアカウントを作成します。 詳しくは、「Android for Workアカウントの作成」を参照してください。
- Android for WorkアプリをXenMobileに追加します。 詳しくは、「XenMobileへのアプリケーションの追加」を参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

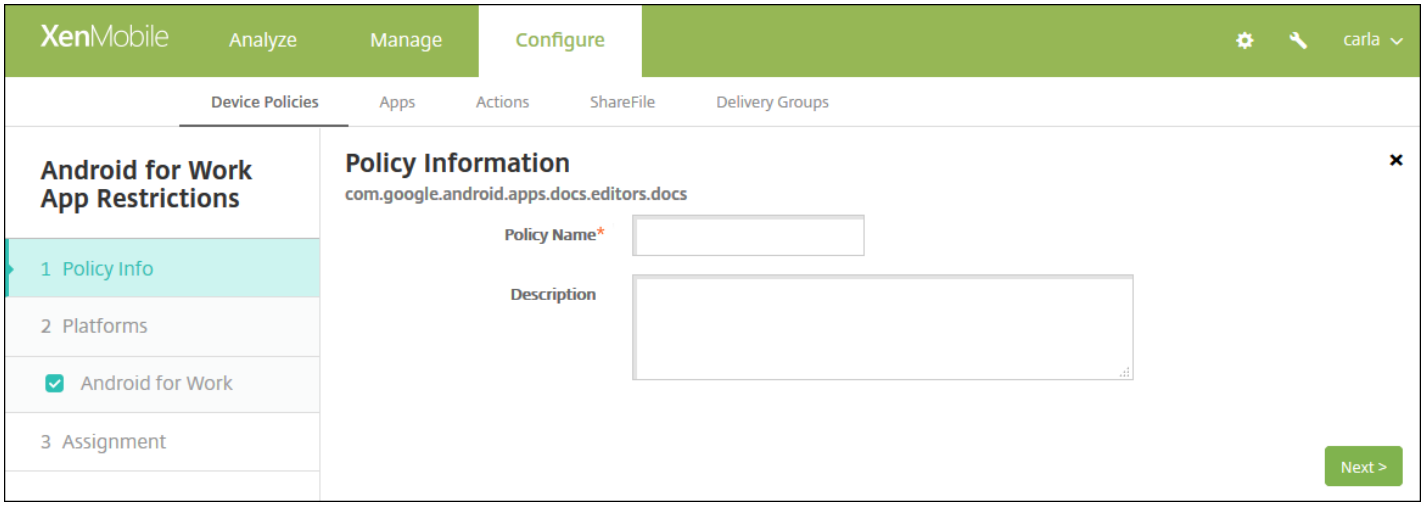
2.新しいポリシーを追加するために **[Add]** をクリックします。 **[Add a New Policy]** ページが開きます。

3. **[More]** を展開し、 **[Security]** で **[Android for Work App Restrictions]** をクリックします。 アプリの選択を求めるダイアログボックスが開きます。



4.一覧から、制限の適用先のアプリを選択して、 **[OK]** をクリックします。

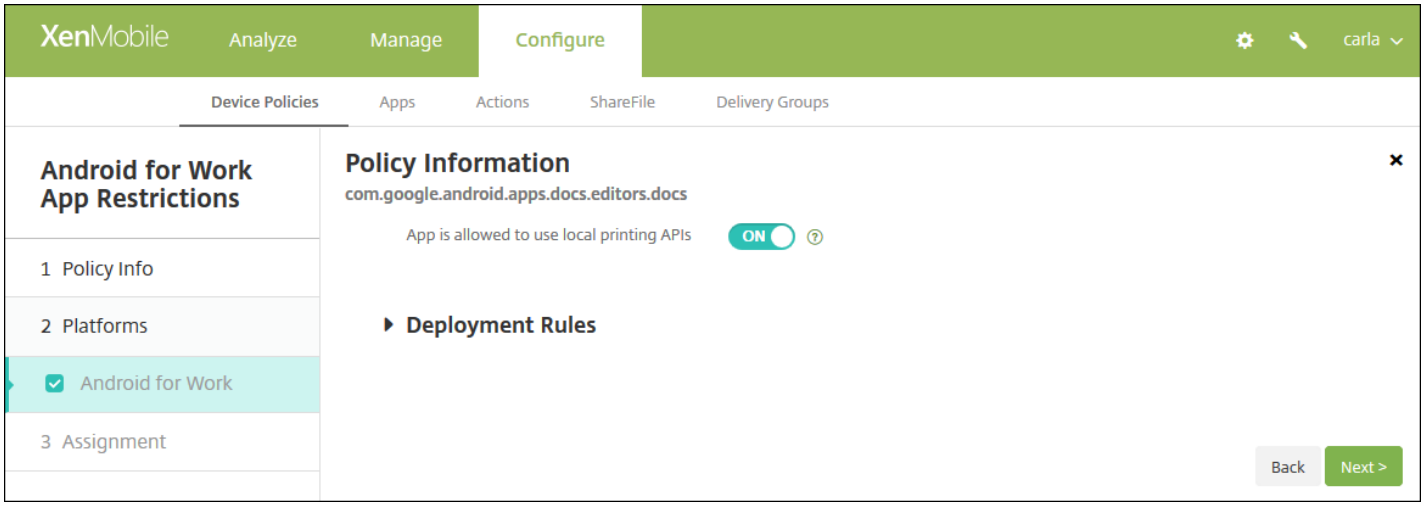
- XenMobileに追加されたAndroid for Workアプリがない場合は、続行できません。 XenMobileへのアプリの追加について詳しくは、「XenMobileへのアプリケーションの追加」を参照してください。
- アプリに制限が関連付けられていない場合は、その効果についての通知が表示されます。 **[OK]** をクリックして、このダイアログボックスを閉じます。
- アプリに制限が関連付けられている場合は、 **[Android for Work App Restrictions Policy]** 情報ページが開きます。



［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

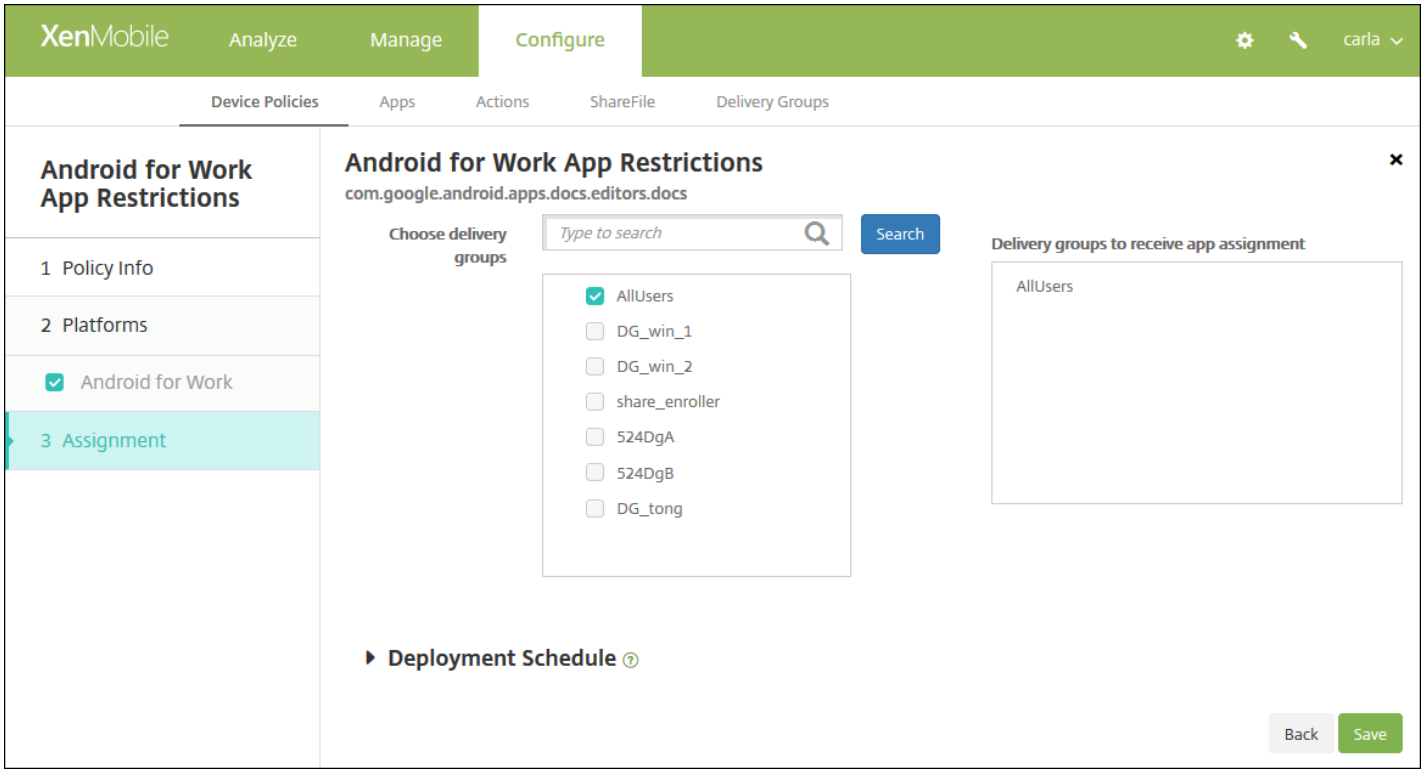
6. ［**Next**］をクリックします。 ［**Android for Work Platform**］ページが開きます。



7. 選択したアプリケーションの設定を構成します。 表示される設定は、選択したアプリに関連付けられている制限によって異なります。

8. 展開規則の構成

9. ［**Next**］をクリックします。 ［**Android for Work App Restrictions Policy**］割り当てページが開きます。



10. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

11. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただし、 [**Deploy for always on connection**] は適用されません。

12. [**Save**] をクリックします。

APNデバイスポリシー

Aug 02, 2016

iOS、Android、Windows Mobile/CEデバイスのカスタムアクセスポイント名（APN）デバイスポリシーを追加できます。 このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマーAPNを使用しない組織で使用します。 APNポリシーによって、特定の電話会社の汎用パケット無線サービス（General Packet Radio Service：GPRS）にデバイスを接続するときに使用される設定が決まります。 ほとんどの新しい電話機において、この設定は既に定義されています。

iOSの設定

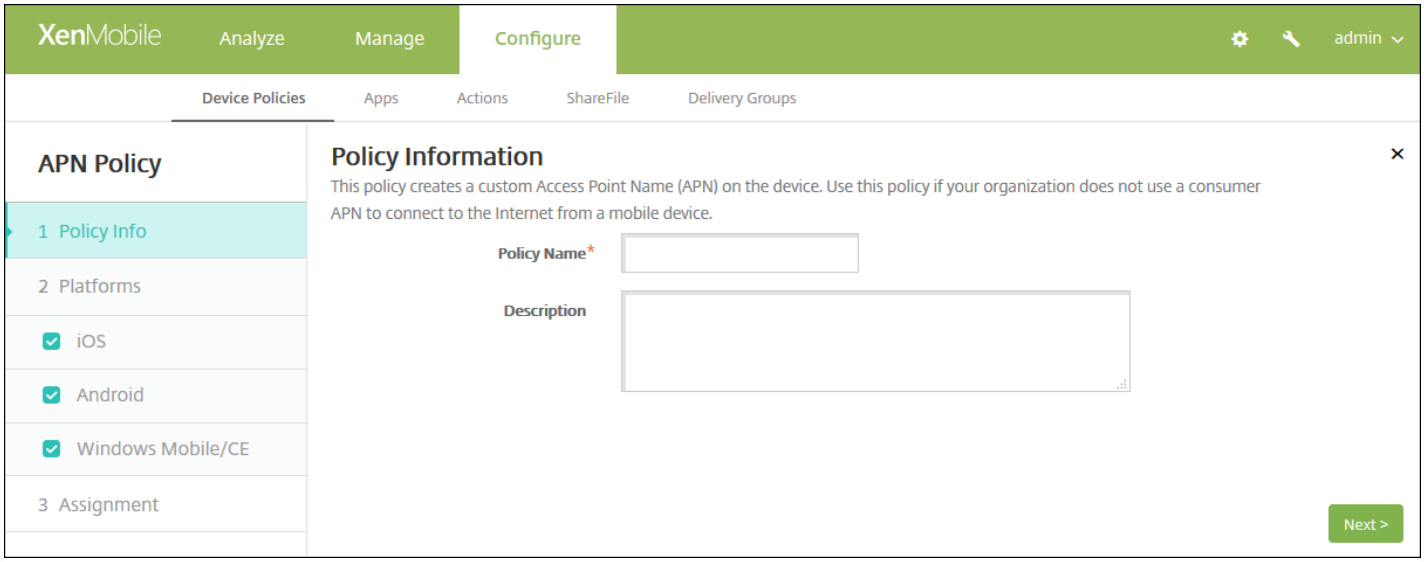
Androidの設定

Windows Mobile/CEの設定

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**More**］をクリックした後、［**Network access**］の下の［**APN**］をクリックします。 ［**APN Policy**］情報ページが開きます。



［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

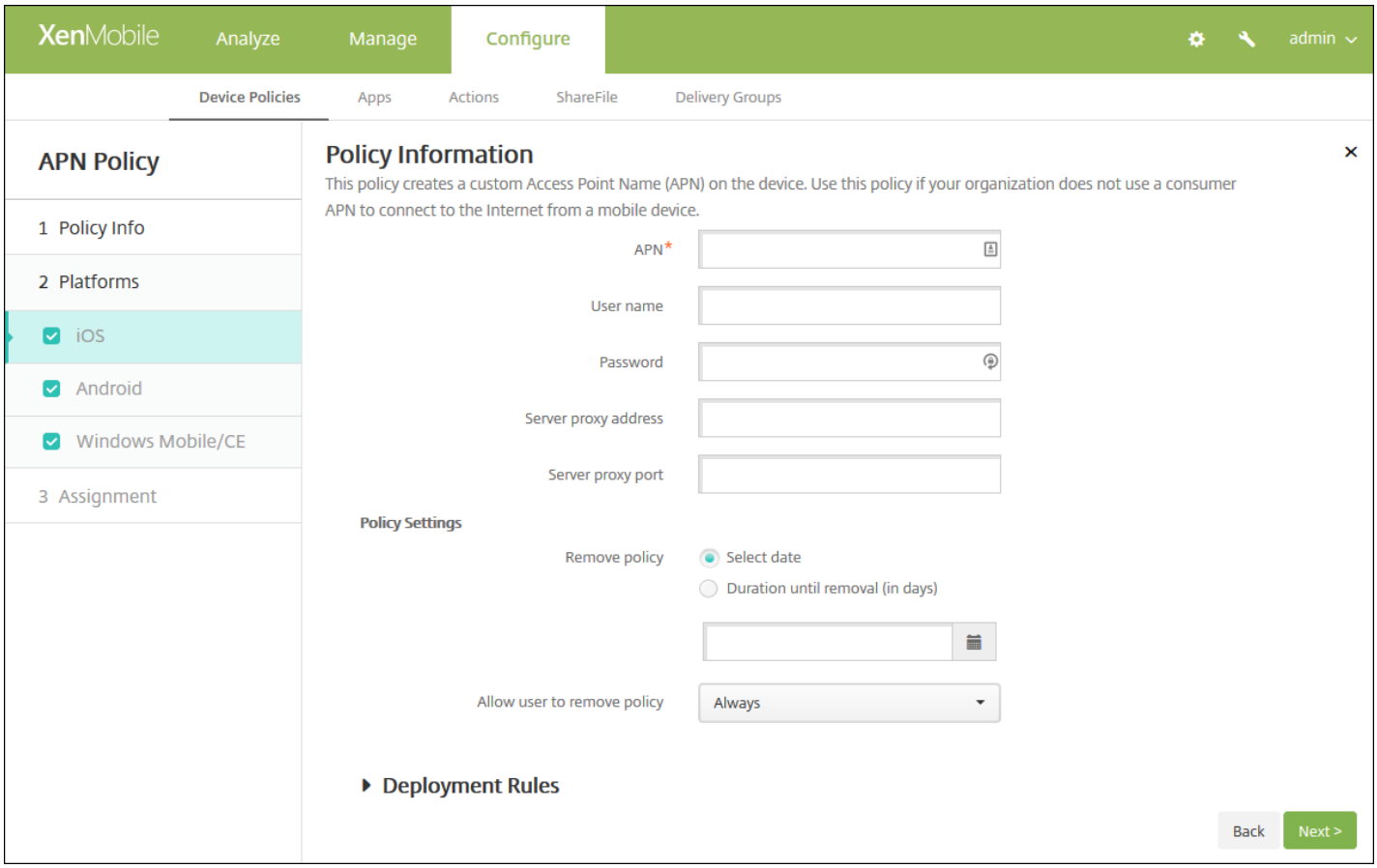
5. ［**Next**］をクリックします。 ［**Policy Platforms**］ページが開きます。

注： ［**Policy Platforms**］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォームが表示されます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

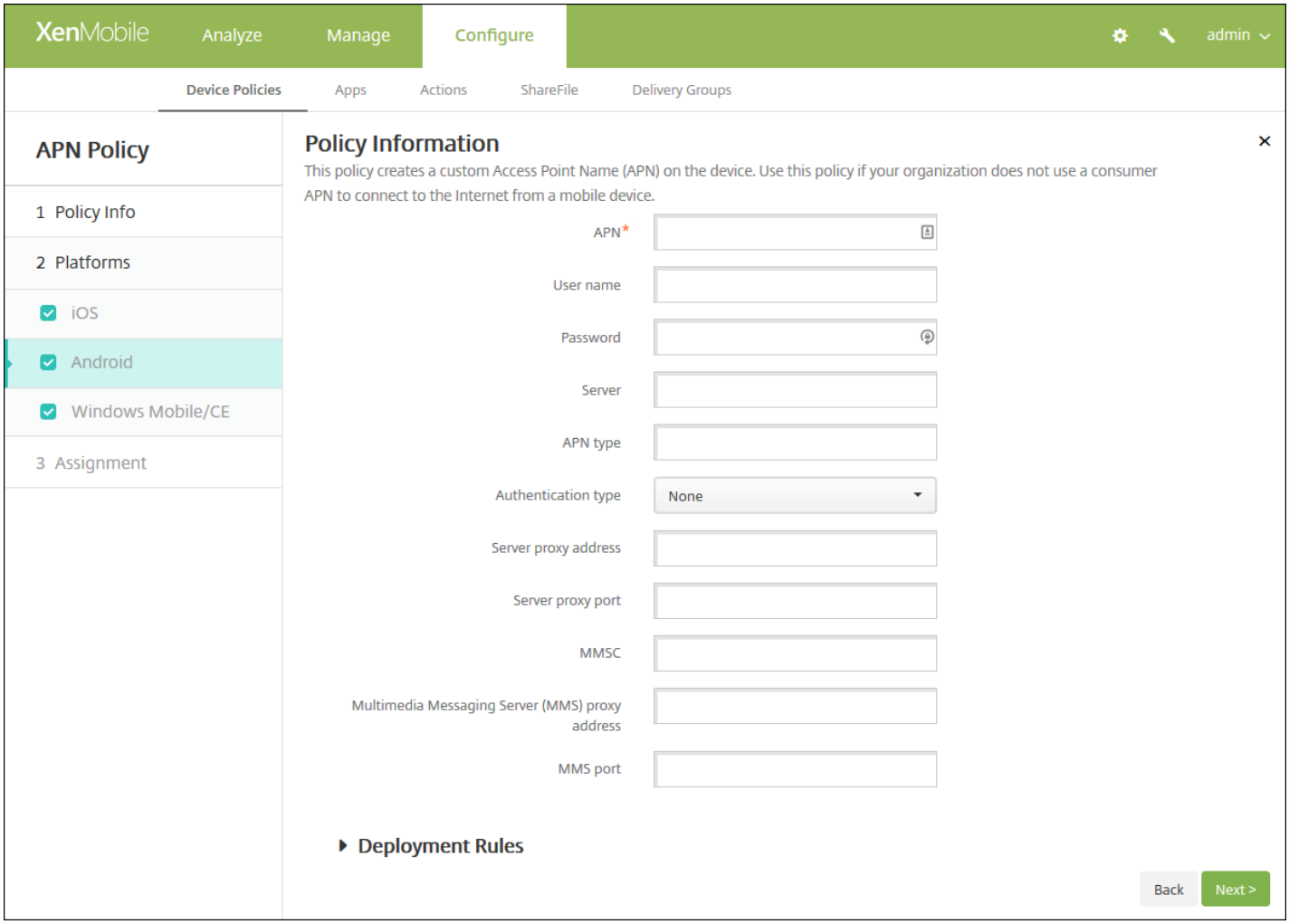
iOSの設定の構成



次の設定を構成します。

- **APN**：アクセスポイントの名前を入力します。 これは承認されているiOSのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **User name**：このAPNのユーザー名を指定する文字列です。 ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password**：このAPNのユーザーのパスワードです。 難読化のために、パスワードはエンコードされます。 ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **Server proxy address**：APNプロキシのIPアドレスまたはURLです。
- **Server proxy port**：APNプロキシのポート番号です。 サーバーのプロキシアドレスを入力した場合は必須です。
- **［Policy Settings］**の下の**［Remove policy］**の横にある、**［Select date］** または**［Duration until removal (in days)］**を選択します。
  - **［Select date］**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **［Allow user to remove policy］**の一覧で、**［Always］**、**［Password required］**、**［Never］**のいずれかを選択します。
  - **［Password required］**を選択した場合、**［Removal password］**の横に必要なパスワードを入力します。

Androidの設定の構成

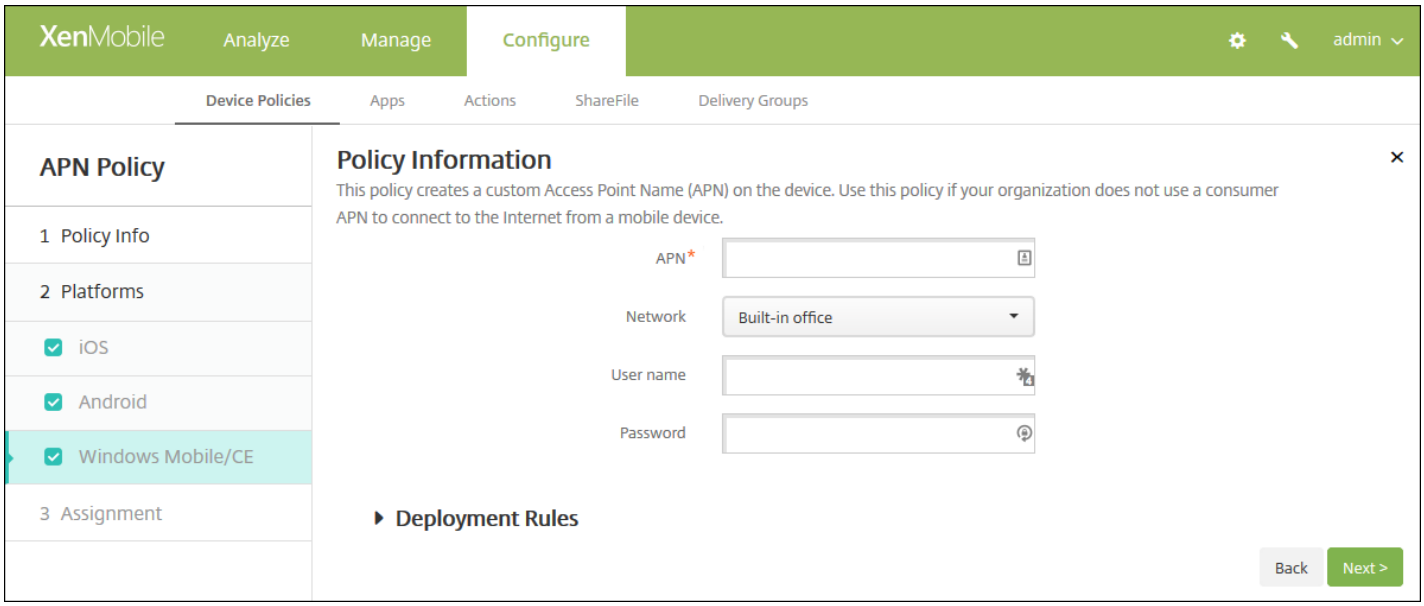


次の設定を構成します。

- **APN**：アクセスポイントの名前を入力します。 これは承認されているAndroidのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **User name**：このAPNのユーザー名を指定する文字列です。 ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password**：このAPNのユーザーのパスワードです。 難読化のために、パスワードはエンコードされます。 ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **Server**：この設定はスマートフォンに 先行するもので、通常は空白です。 標準のWebサイトにアクセスできない、または標準のWebサイトを表示できない電話機用のワイヤレスアプリケーションプロトコル（WAP）ゲートウェイサーバーを参照します。 サイト
- **APN type**：この設定は、電話会社が想定しているアクセスポイントの使用方法に一致している必要があります。 内容はAPNサービス指定子のコンマ区切り文字列であり、携帯電話会社が公開している定義と一致している必要があります。 以下に例を示します。
  - *。 すべてのトラフィックがこのアクセスポイントを経由します。
  - mms。 マルチメディアトラフィックがこのアクセスポイントを経由します。
  - default。 マルチメディアトラフィックを含め、すべてのトラフィックがこのアクセスポイントを経由します。
  - supl。 SUPL（Secure User Plane Location）は補助GPSに関連付けられています。
  - dun。 ダイヤルアップ ネットワークは古いため、ほとんど使用されません。
  - hipri。 高優先度ネットワークです。

- fota。 FOTA（Firmware over the air）は、ファームウェア更新の受信に使用されます。
- **Authentication type**：ボックスの一覧で、使用する認証の種類を選択します。 デフォルトは［None］です。
- **Server proxy address**：電話会社のAPN HTTPプロキシのIPアドレスまたはURLです。
- **Server proxy port**：APNプロキシのポート番号です。 サーバーのプロキシアドレスを入力した場合は必須です。
- **MMSC**：電話会社が提供するMMSゲートウェイサーバーのアドレスです。
- **Multimedia Messaging Server (MMS) proxy address**：これは、MMSトラフィック用のマルチメディアメッセージングサービスサーバーです。 MMSはSMSの後継で、画像やビデオなどのマルチメディアコンテンツを含む大きいサイズのメッセージを送信できます。 これらのサーバーは特定のプロトコルを必要とします（MM1、... MM11など）。
- **MMS port**：MMSプロキシに使用されるポートです。

Windows Mobile/CEの設定の構成

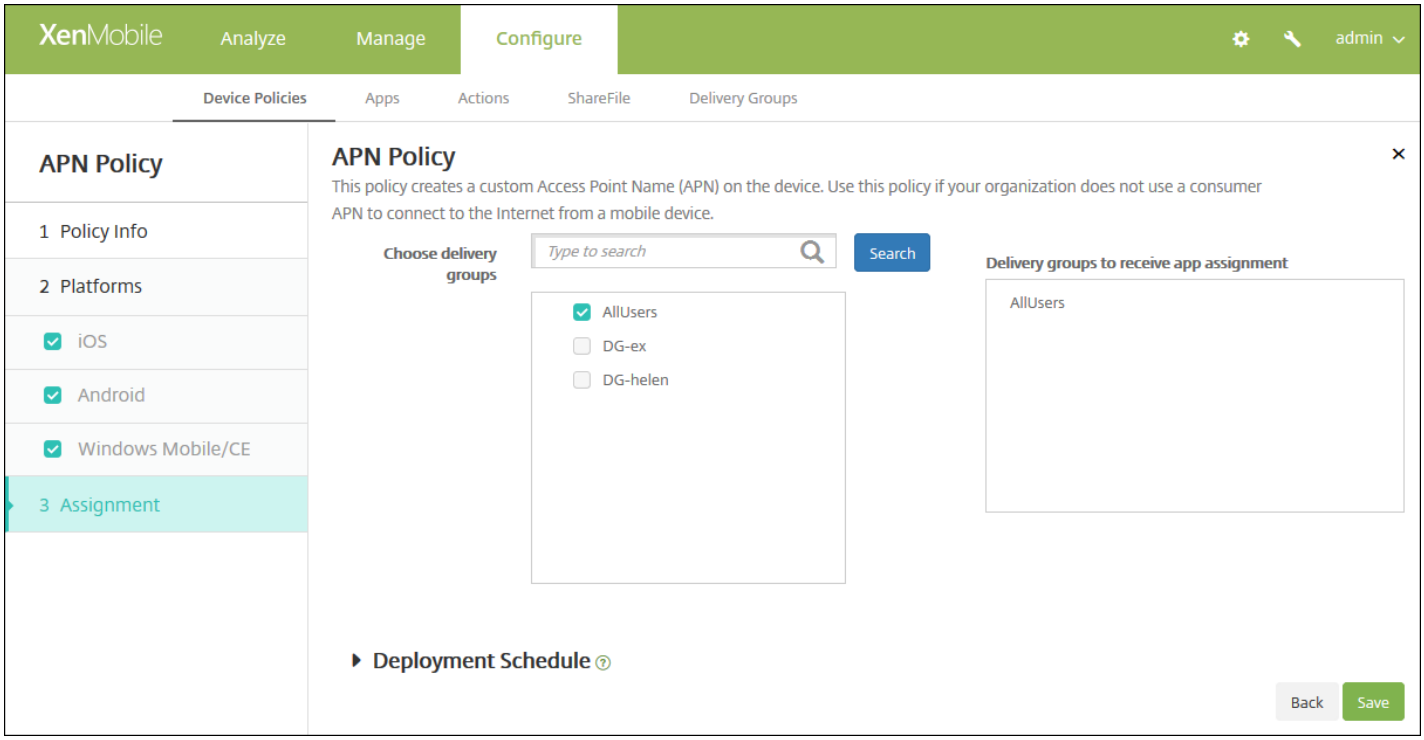


次の設定を構成します。

- **APN**：アクセスポイントの名前を入力します。 これは承認されているAndroidのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **Network**：一覧から、使用するネットワークの種類を選択します。 デフォルトは［**Built-in office**］です。
- **User name**：このAPNのユーザー名を指定する文字列です。 コマンド ユーザー名 がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password**：このAPNのユーザーのパスワードです。 難読化のために、パスワードはエンコードされます。 ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**APN Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

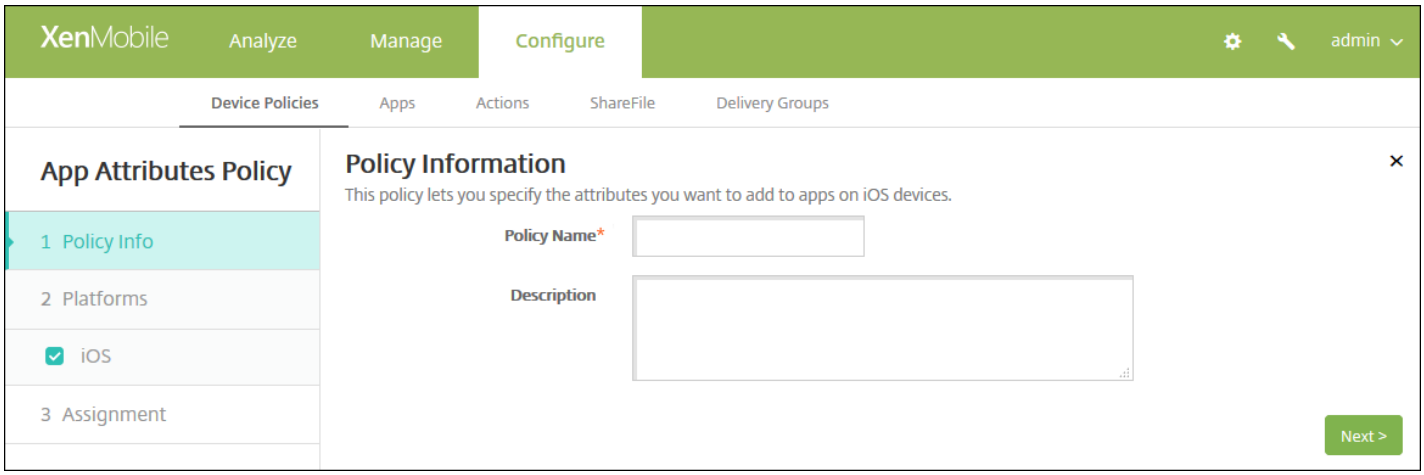
注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

アプリケーション属性デバイスポリシー

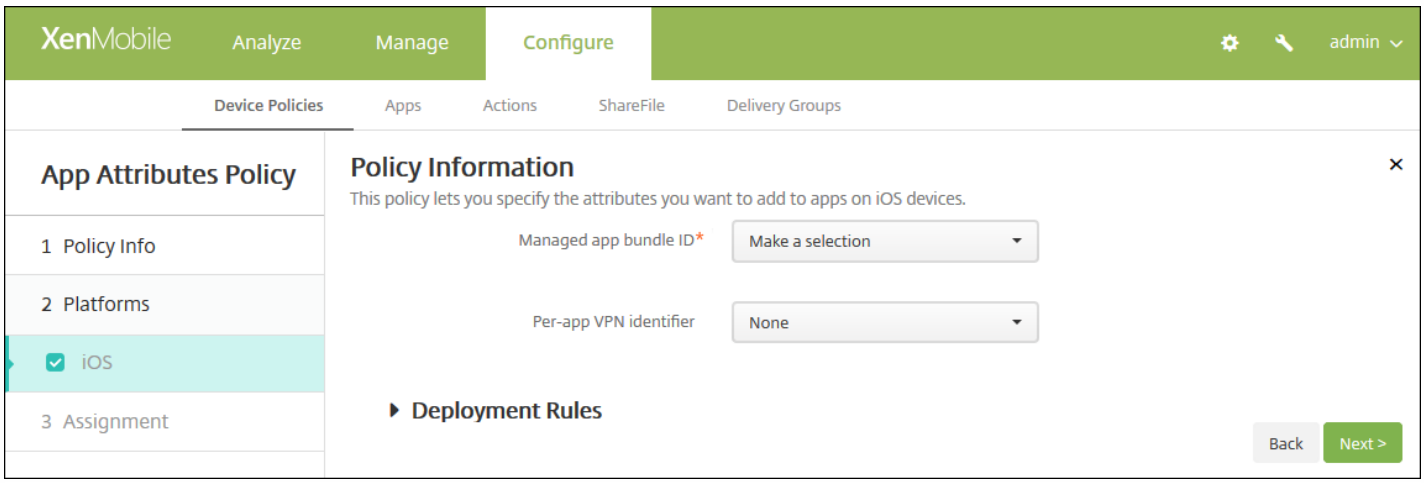
Aug 02, 2016



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[App Attributes]** プラットフォーム情報ページが開きます。

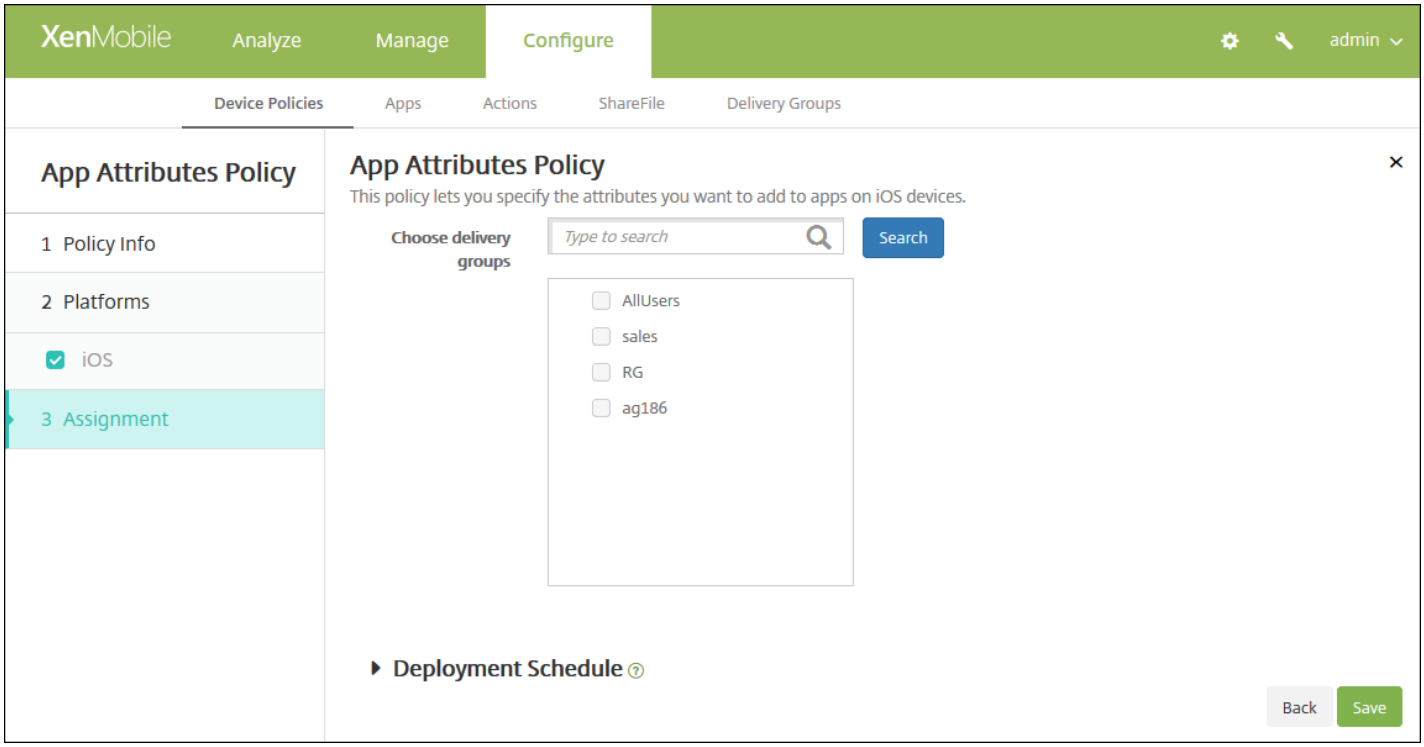


6. 次の設定を構成します。

- **Managed app bundle ID**：一覧からアプリケーションバンドルIDを選択するか、**[Add new]** をクリックします。
  - **[Add new]** をクリックした場合は、表示されるフィールドにアプリケーションバンドルIDを入力します。
- **Per-app VPN identifier**：一覧から、アプリケーションごとのVPN IDを選択します。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 [App Uninstall Policy] 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 [Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [Deploy for always on connection] は適用されません。

11. **[Save]** をクリックします。

アプリケーションアクセスデバイスポリシー

Aug 02, 2016

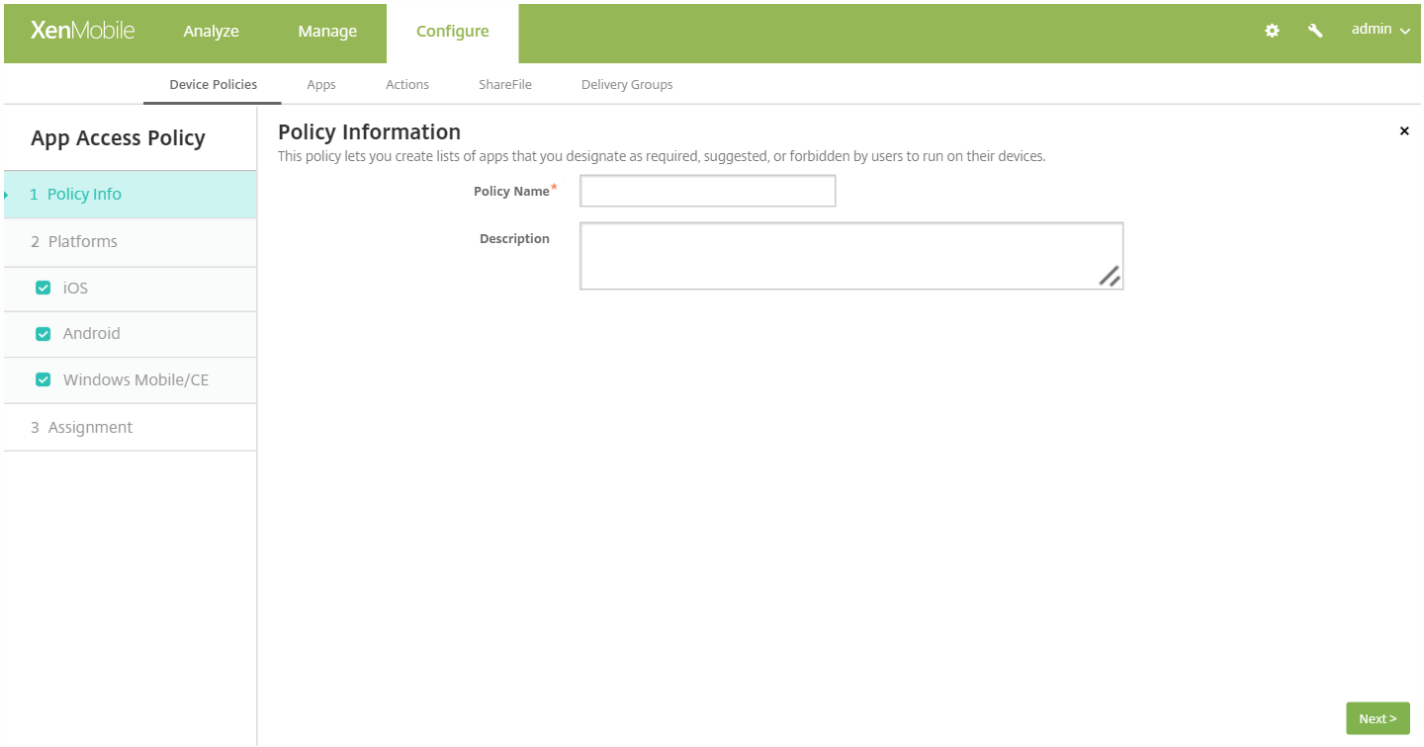
XenMobileのアプリケーションアクセスデバイスポリシーでは、デバイスへのインストールが必須のアプリケーション、デバイスにインストール可能なアプリケーション、デバイスへのインストールが禁止されるアプリケーションの一覧を定義できます。 次に、そのアプリケーション一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。 アプリケーションアクセスポリシーは、iOS、Android、Windows Mobile/CEデバイスに対して作成できます。

アクセスポリシーは一度に1種類のみ構成できます。 必須アプリケーション、推奨アプリケーション、禁止アプリケーションのいずれかの一覧のポリシーを追加できますが、同じアプリケーションアクセスポリシー内に混在させることはできません。 一覧の種類ごとにポリシーを作成する場合、XenMobileでどのポリシーがどのアプリケーション一覧に適用されるかがわかるようにするため、各ポリシーの名前付けに注意することをお勧めします。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** を展開し、 **[Apps]** の下の **[App Access]** をクリックします。 **[App Access Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。

[Platforms] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

6. 選択したプラットフォームごとに、次の設定を構成します。

- **Access policy**：［Required］、［Suggested］、［Forbidden］のいずれかをクリックします。 デフォルトは［Required］です。
- 1つまたは複数のアプリケーションを一覧に追加するには、**[Add]** をクリックして以下の操作を行います。
  - **App name**：アプリケーション名を入力します。
  - **App Identifier**：任意で、アプリケーション識別子を入力します。
  - **[Save]** または **[Cancel]** をクリックします。
  - 追加するアプリケーションごとに上記の手順を繰り返します。

    注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、 **[Save]** をクリックして変更した項目を保存するか、 **[Cancel]** をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8.［Next］をクリックします。 次のプラットフォームのページまたは **[App Access Policy]** 割り当てページが開きます。

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

アプリケーション構成デバイスポリシー

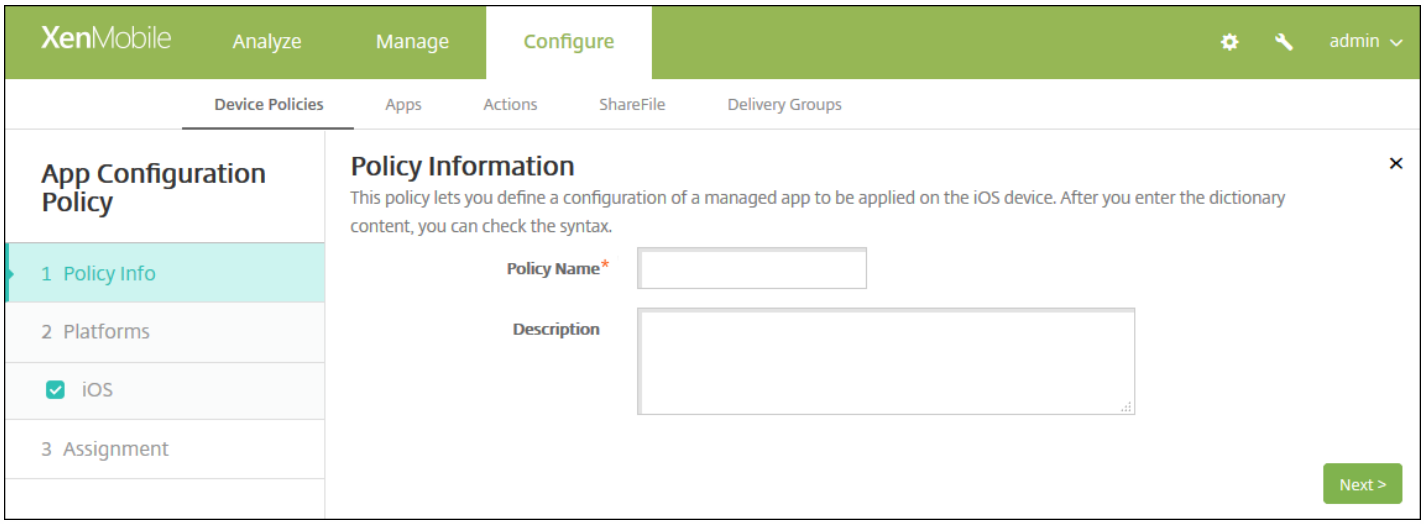
Aug 02, 2016

XML構成ファイル（プロパティ一覧またはplistと呼ばれるファイル）をユーザーのiOSデバイスに展開して、アプリケーションのさまざまな設定および動作を構成することにより、 管理対象の構成をサポートするApp Storeアプリケーションをリモートで構成できます。 実際に構成できる設定および動作はアプリケーションによって異なるため、このアーティクルでは扱いません。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ページが開きます。

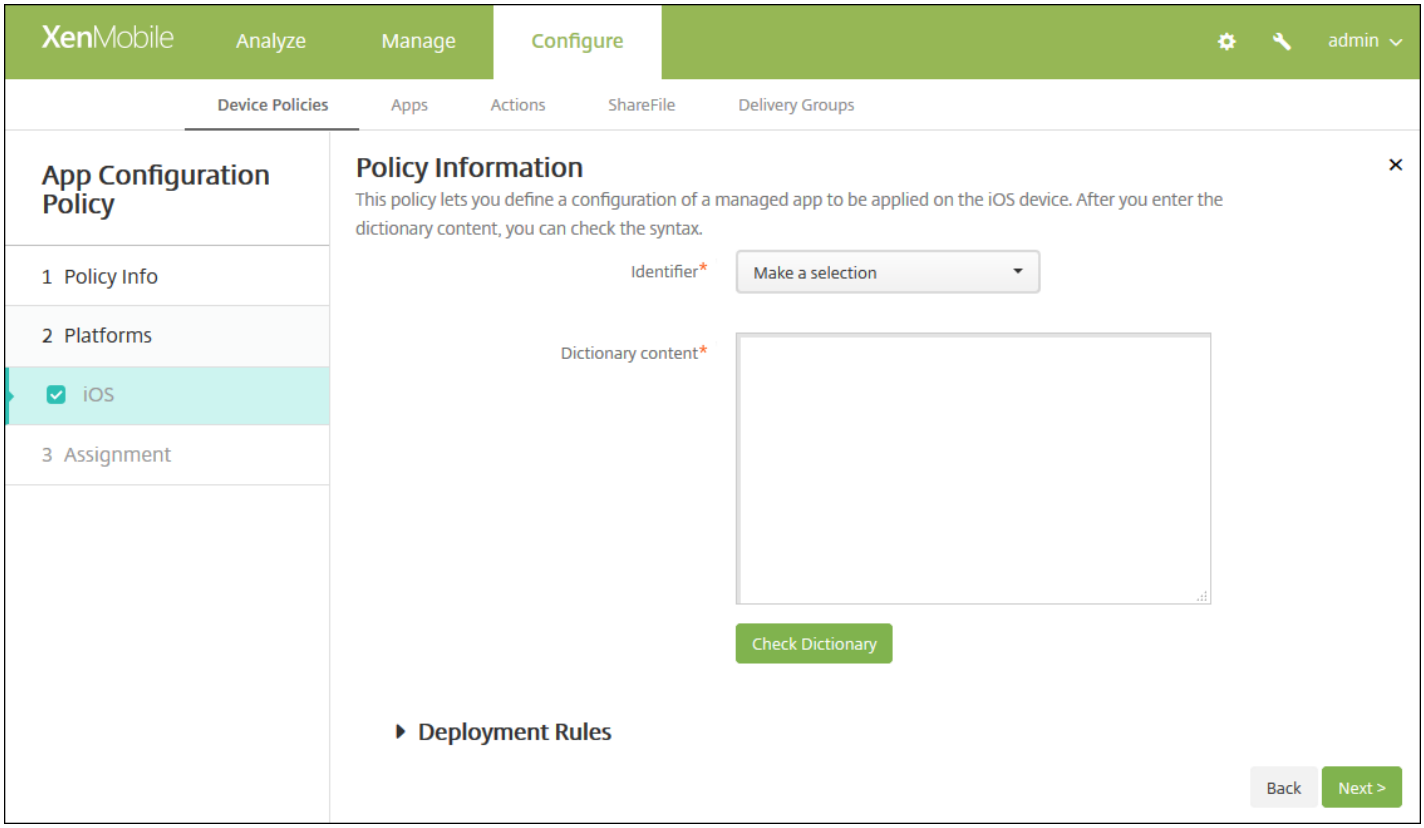
3. **[More]** を展開し、 **[Apps]** で **[App Configuration]** をクリックします。 **[App Configuration Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[iOS Platform]** 情報ページが開きます。

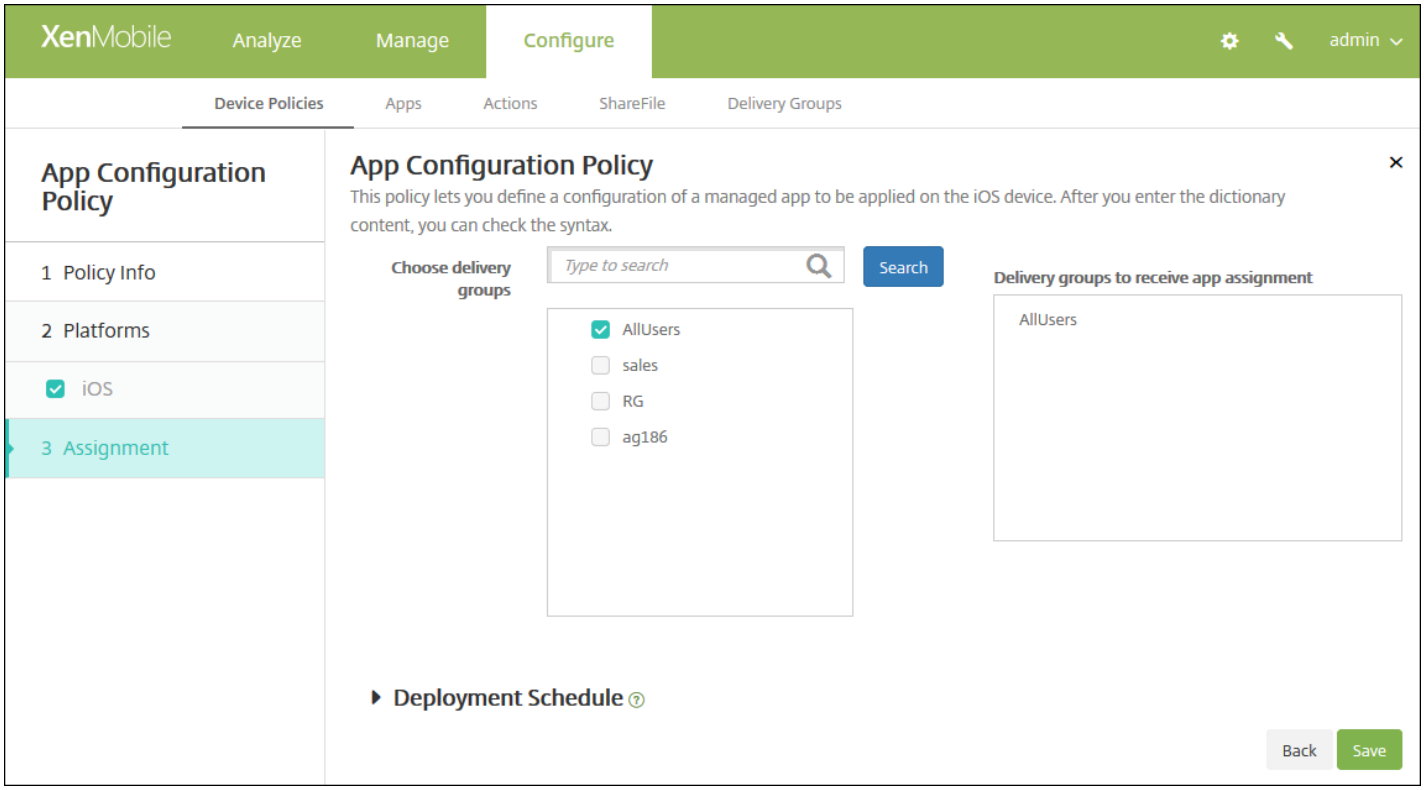


6. 次の設定を構成します。

- **Identifier**：一覧から構成するアプリケーションを選択するか、［**Add new**］をクリックして新しいアプリケーションを一覧に追加します。
  - ［**Add new**］をクリックした場合は、表示されるフィールドにアプリケーションIDを入力します。
- **Dictionary content**：XMLプロパティ一覧（plist）構成情報を入力するか、コピーして貼り付けます。
- ［**Check Dictionary**］をクリックします。 XenMobileがXMLを検証します。 エラーがなければ、コンテンツボックスの下に「**Valid XML**」と表示されます。 コンテンツボックスの下に何らかの構文エラーが表示された場合は、続行する前にエラーを修正する必要があります。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**App Configuration Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

アプリケーションインベントリデバイスポリシー

Aug 02, 2016

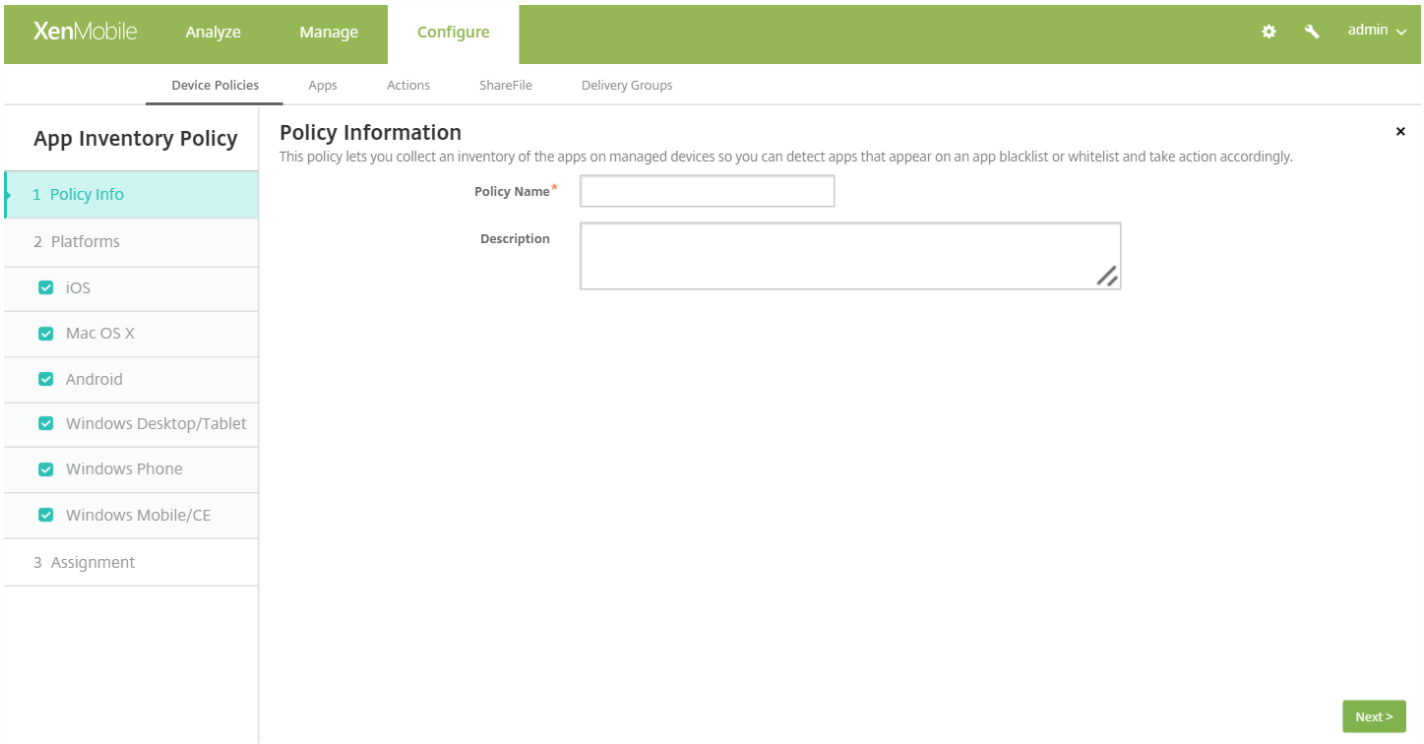
XenMobileのアプリケーションインベントリポリシーにより、管理されているデバイスのアプリケーションのインベントリを収集できます。その後、インベントリは、それらのデバイスに展開されたアプリケーションアクセスポリシーと比較されます。 この方法で、アプリケーションのブラックリスト（アプリケーションアクセスポリシーで禁止）またはホワイトリスト（アプリケーションアクセスポリシーで必須）に表示されるアプリケーションを検出し、それに応じた操作を実行することができます。 アプリケーションアクセスポリシーは、iOS、Mac OS X、Android（Android for Work対応デバイスを含む）、Windowsデスクトップ/タブレット、Windows Phone、Windows Mobile/CEデバイスに対して作成できます。

> **Important**
>
> ユーザーのAndroidデバイスで、WorxStoreの［Updates Available］の一覧に更新されたアプリケーションが表示されるようにするには、最初にこのポリシーをユーザーのデバイスに展開しておく必要があります。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ページが開きます。

3. ［**More**］を展開し、 ［**Apps**］の下の［**App Inventory**］をクリックします。 ［**App Inventory Policy**］ページが開きます。

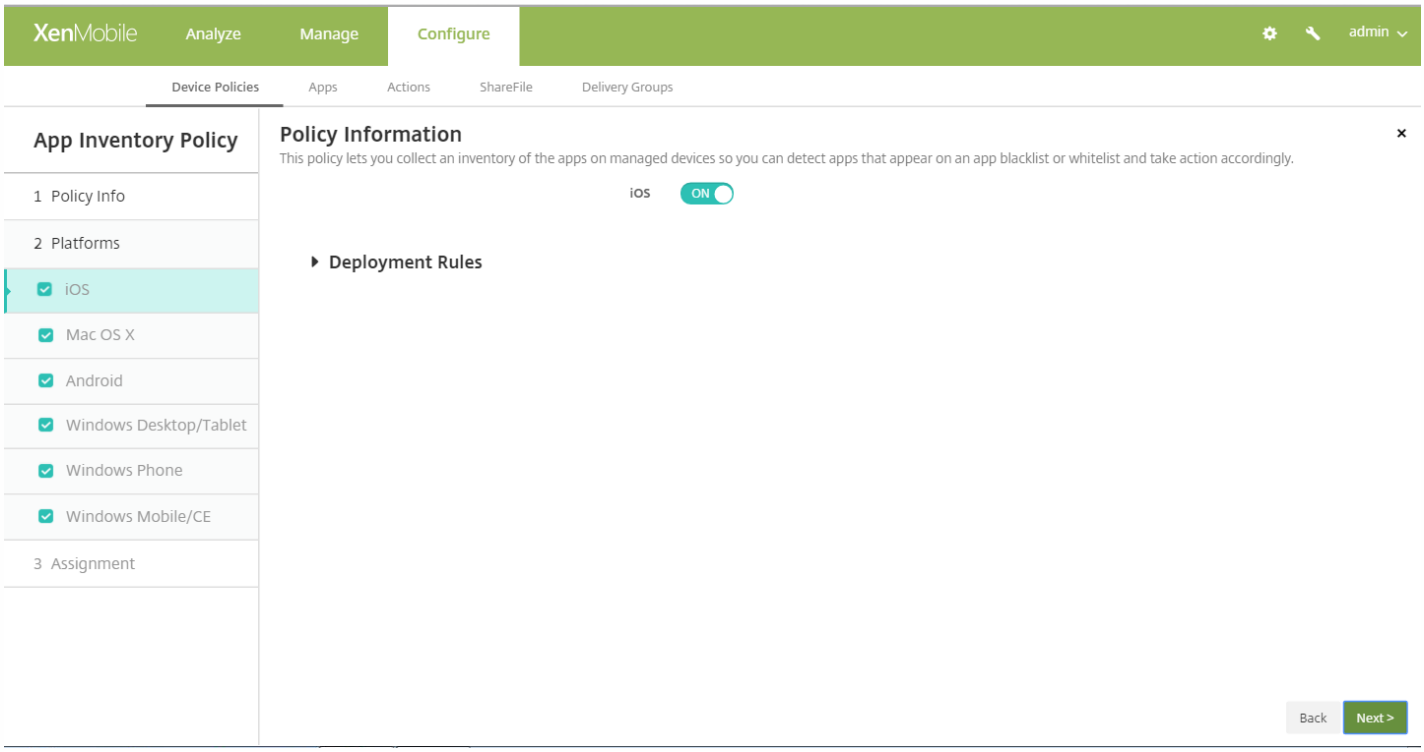


4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。

- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Policy Platforms**] ページが開きます。



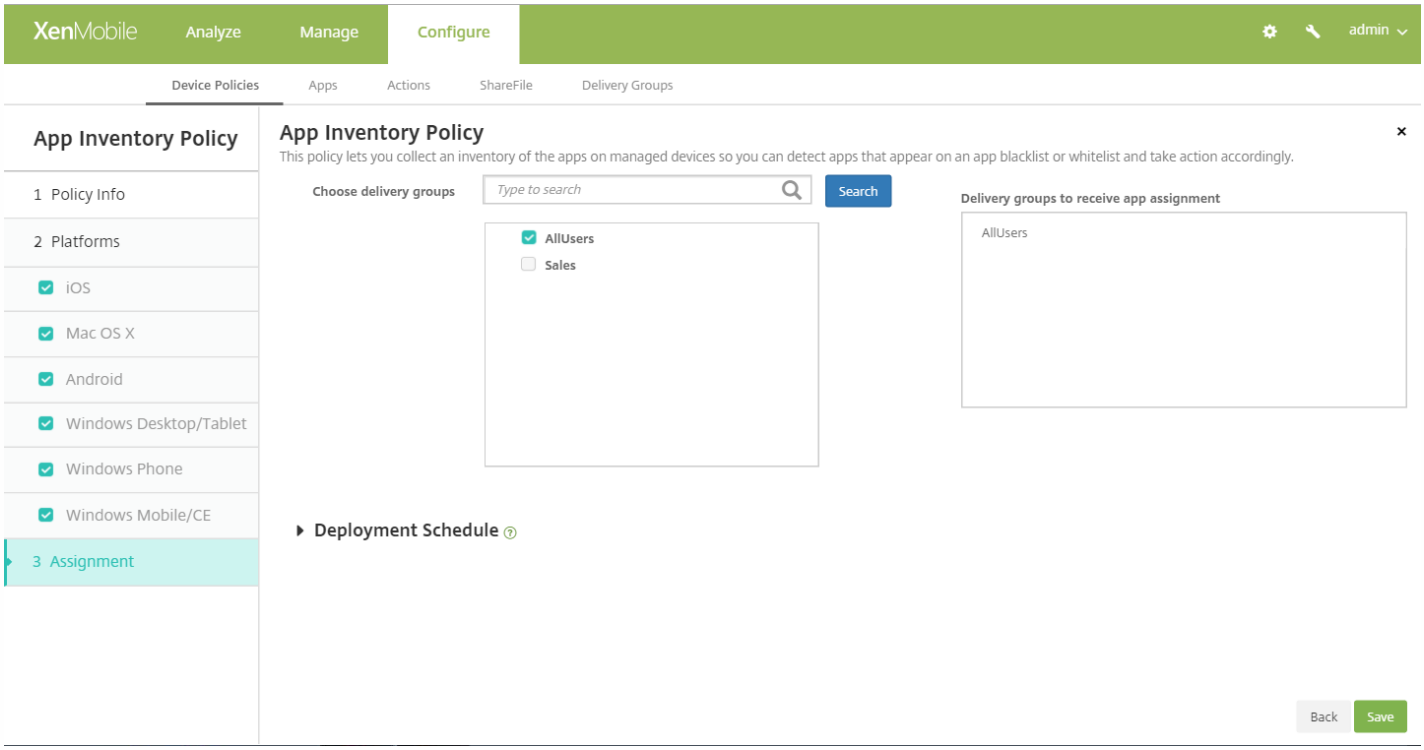
[**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

6. 選択したプラットフォームごとに、デフォルト設定のままにしておくか、設定を [**OFF**] に変更します。 デフォルトは [**ON**] です。

7. 展開規則を構成します。

8. [**Next**] をクリックします。 [**App Inventory Policy**] 割り当てページが開きます。



9. [Choose delivery groups]の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の[Delivery groups to receive app assignment]一覧に表示されます。

10. [Deployment Schedule]を展開して以下の設定を構成します。

- [Deploy]の横の[ON]をクリックすると展開がスケジュールされ、[OFF]をクリックすると展開が行われません。 デフォルトのオプションは[ON]です。 [OFF]を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule]の横の[Now]または[Later]をクリックします。 デフォルトのオプションは[Now]です。
- [Later]をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition]の横の[On every connection]をクリックするか、[Only when previous deployment has failed]をクリックします。 デフォルトのオプションは、[On every connection]です。
- [Deploy for always-on connection]の横の[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]です。

注：

- このオプションは、**[Settings]**の**[Server Properties]**において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]**は適用されません。

11. **[Save]**をクリックします。

アプリケーションロックデバイスポリシー

Aug 30, 2016

XenMobileでは、ポリシーを作成して、デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行を禁止するアプリの一覧を定義できます。 このポリシーは、iOSデバイスとAndroidデバイスの両方に対して構成できますが、ポリシーが実際にどのように機能するかは各プラットフォームで異なります。 たとえば、iOSデバイスで複数のアプリを禁止することはできません。

同様に、iOSデバイスの場合、ポリシーあたり1つのiOSアプリのみ選択できます。 つまり、ユーザーはデバイスを使用して1つのアプリを実行することのみできます。 アプリのロックポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。

また、iOSデバイスは、アプリのロックポリシーをプッシュするように監視される必要があります。

デバイスポリシーは大部分のAndroid LおよびMデバイスで機能しますが、アプリのロックは、必要なAPIがGoogleによって廃止されたため、Android N以降のデバイスでは機能しません。

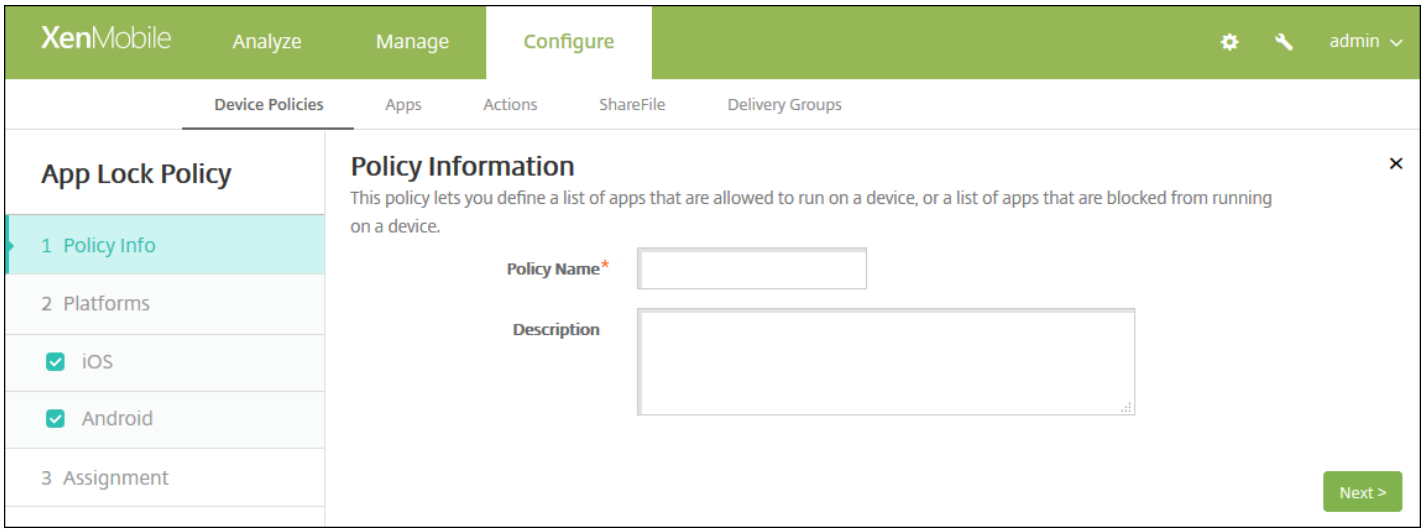
iOSの設定

Androidの設定

1. XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** を展開し、 **[Security]** の下の **[App Lock]** をクリックします。 **[App Lock Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

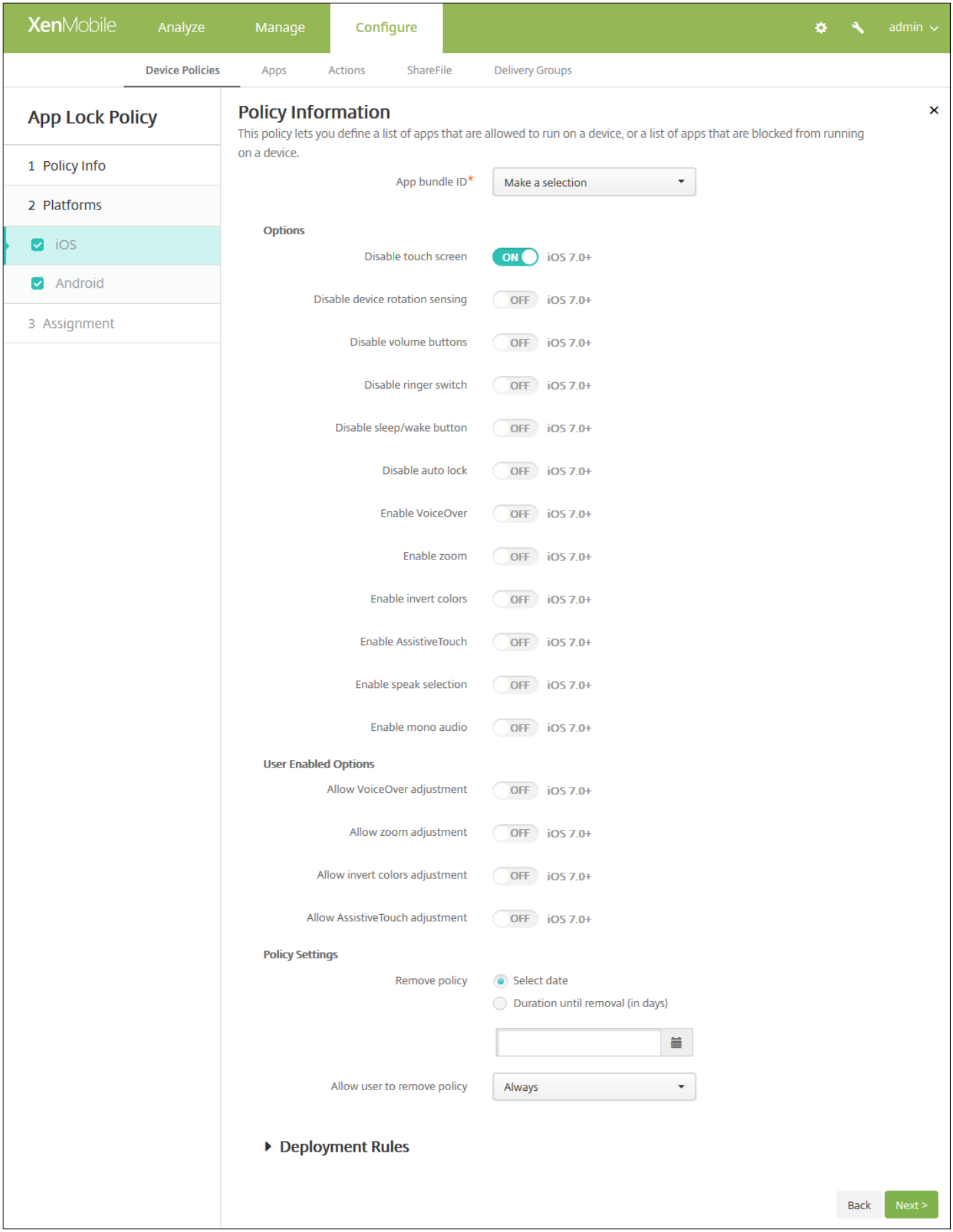
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：必要に応じて、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Platforms]** ページが開きます。

6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

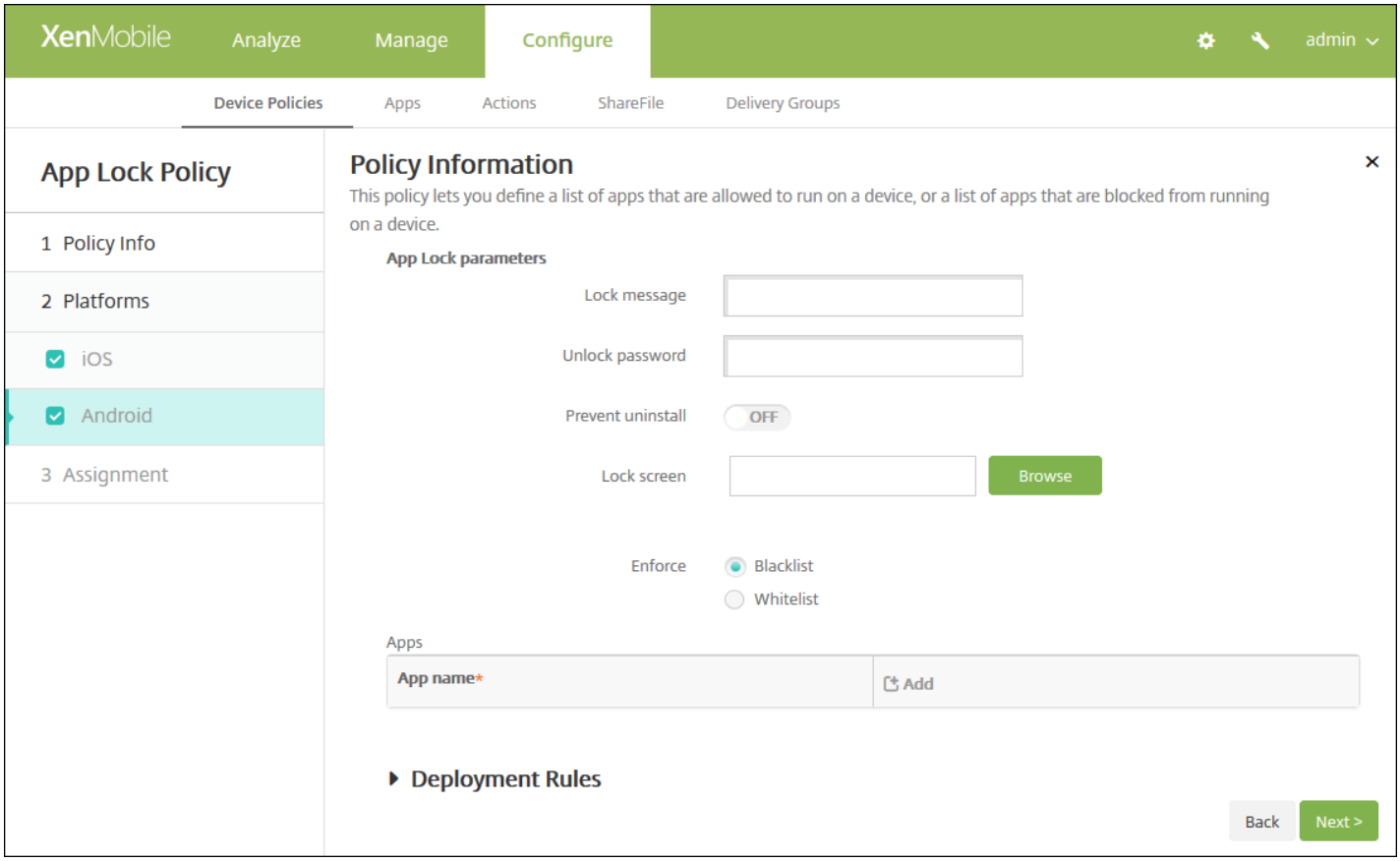
iOSの設定の構成



次の設定を構成します。

- **App bundle ID**：一覧からこのポリシーを適用するアプリケーションを選択するか、[**Add new**] をクリックして、新しいアプリケーションを一覧に追加します。 [**Add new**] をクリックした場合は、表示されるフィールドにアプリケーション名を入力します。
- **Options**：以下の各オプションは、iOS 7.0以降にのみ適用されます。 [Disable touch screen] を除き、各オプションのデフォルトは [**OFF**] です（[Disable touch screen] はデフォルトで [**ON**] に設定されています）。
  - Disable touch screen
  - Disable device rotation sensing
  - Disable volume buttons
  - Disable ringer switch - **注：**このオプションが無効の場合、着信動作は、スイッチが最初に無効化されたときの場所に依存します。
  - Disable sleep/wake button
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom
  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
- **User Enabled Options**：以下の各オプションは、iOS 7.0以降にのみ適用されます。 どのオプションも、デフォルトは [**OFF**] です。
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment
  - Allow AssitiveTouch adjustment
- **ポリシー設定**
  - o [**Remove policy**] の横にある [**Select date**] または [**Duration until removal (in days)**] をクリックします。
  - o [**Select date**] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - o [**Allow user to remove policy**] の一覧で、 [**Always**] 、 [**Password required**] 、 [**Never**] のいずれかを選択します。
  - o [**Password required**] を選択した場合、 [**Removal password**] の横に必要なパスワードを入力します。

Androidの設定の構成



次の設定を構成します。

- **App Lock parameters**
  - **Lock message**：ユーザーがロックされているアプリケーションを開こうとしたときに表示されるメッセージを入力します。
  - **Unlock password**：アプリケーションのロックを解除するパスワードを入力します。
  - **Prevent uninstall**：ユーザーにアプリケーションのアンインストールを許可するかどうかを選択します。 デフォルトは **[OFF]** です。
  - **Lock screen**： [Browse] をクリックして、デバイスのロック画面に表示するイメージファイルの場所に移動し、ファイルを選択します。
  - **Enforce**： **[Blacklist]** をクリックしてデバイスでの実行を禁止するアプリケーションの一覧を作成するか、 **[Whitelist]** をクリックしてデバイスでの実行を許可するアプリケーションの一覧を作成します。
- **Apps**： **[Add]** をクリックして、以下の操作を行います。
  - **App name**：一覧からホワイトリストまたはブラックリストに追加するアプリケーションの名前を選択するか、**[Add new]** をクリックして、選択可能なアプリケーションの一覧に新しいアプリケーションを追加します。
  - **[Add new]** をクリックした場合は、表示されるフィールドにアプリケーション名を入力します。
  - **[Save]** または **[Cancel]** をクリックします。
  - ホワイトリストまたはブラックリストに追加するアプリケーションごとに、上記の手順を繰り返します。

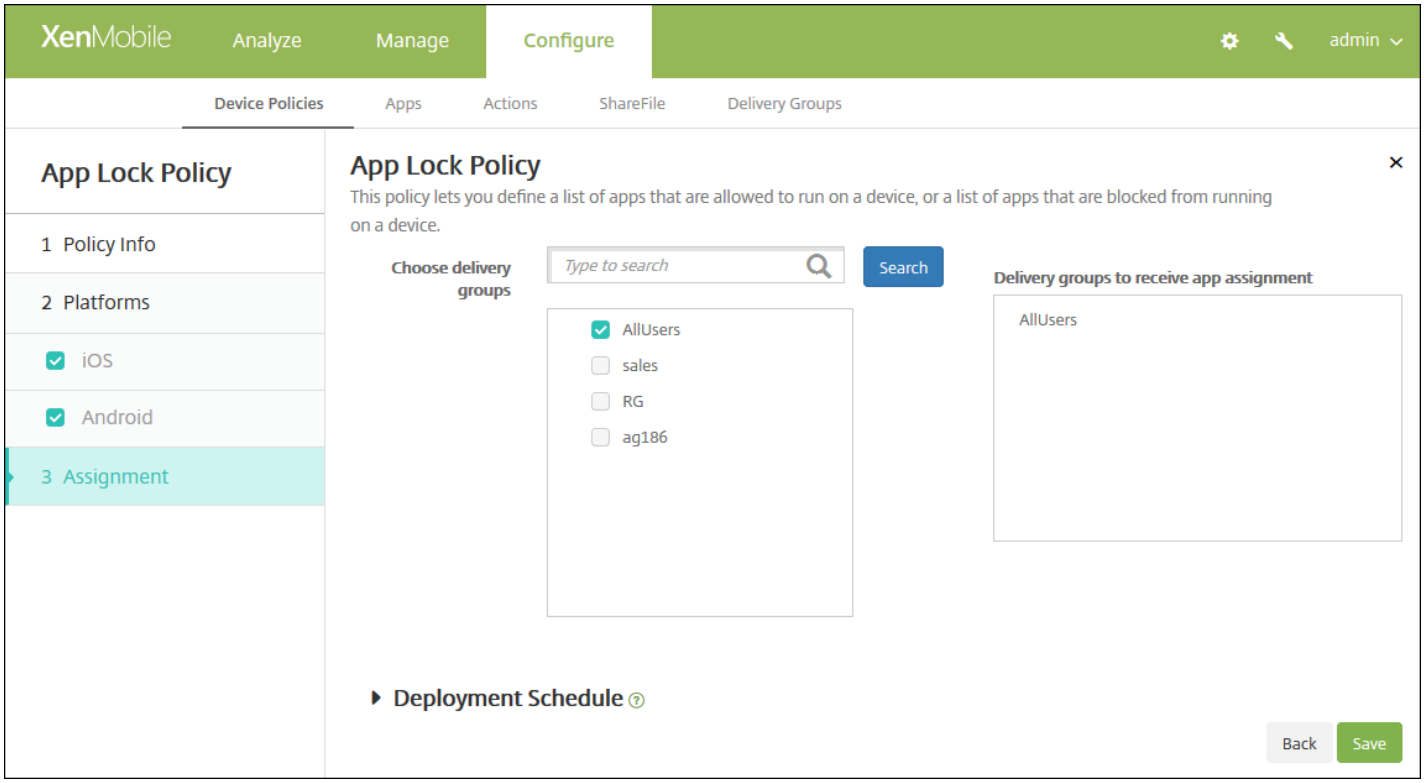
  注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

  既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをク

リックします。 項目を変更し、 [**Save**] をクリックして変更した項目を保存するか、 [**Cancel**] をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8. [**Next**] をクリックします。 [**App Lock Policy**] 割り当てページが表示されます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. **[Save]** をクリックします。

アプリケーションネットワーク使用状況デバイスポリシー

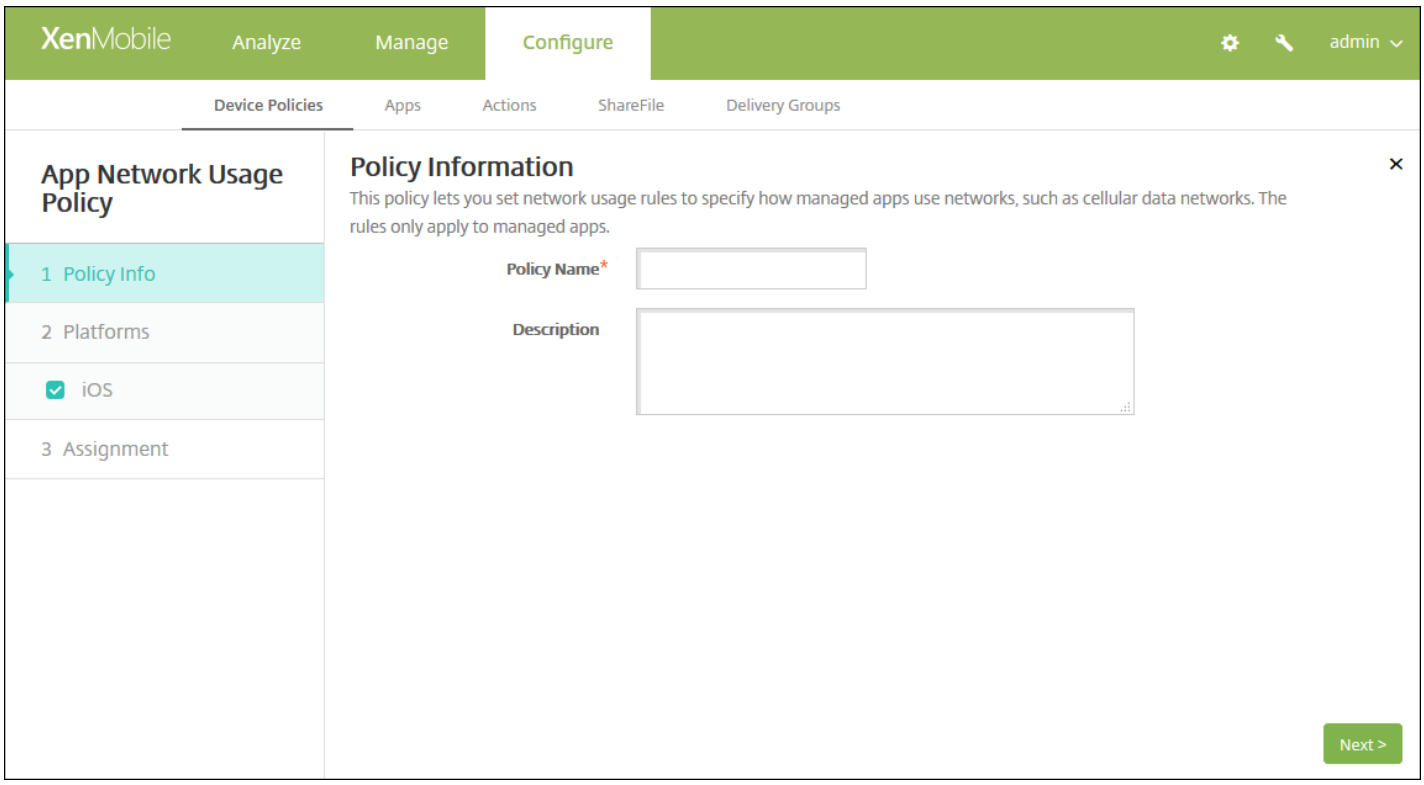
Aug 02, 2016

ネットワーク使用状況規則を設定して、iOSデバイスで管理対象のアプリケーションが携帯データネットワークなどのネットワークをどのように使用するのかを指定できます。 規則は管理対象のアプリケーションにのみ適用されます。 管理対象のアプリケーションとは、XenMobileを使用してユーザーのデバイスに展開されるアプリケーションです。 これには、ユーザーがXenMobileを使用して展開することなく直接デバイスにダウンロードしたアプリケーションや、デバイスのXenMobileへの登録時に既にデバイスにインストールされていたアプリケーションは含まれません。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

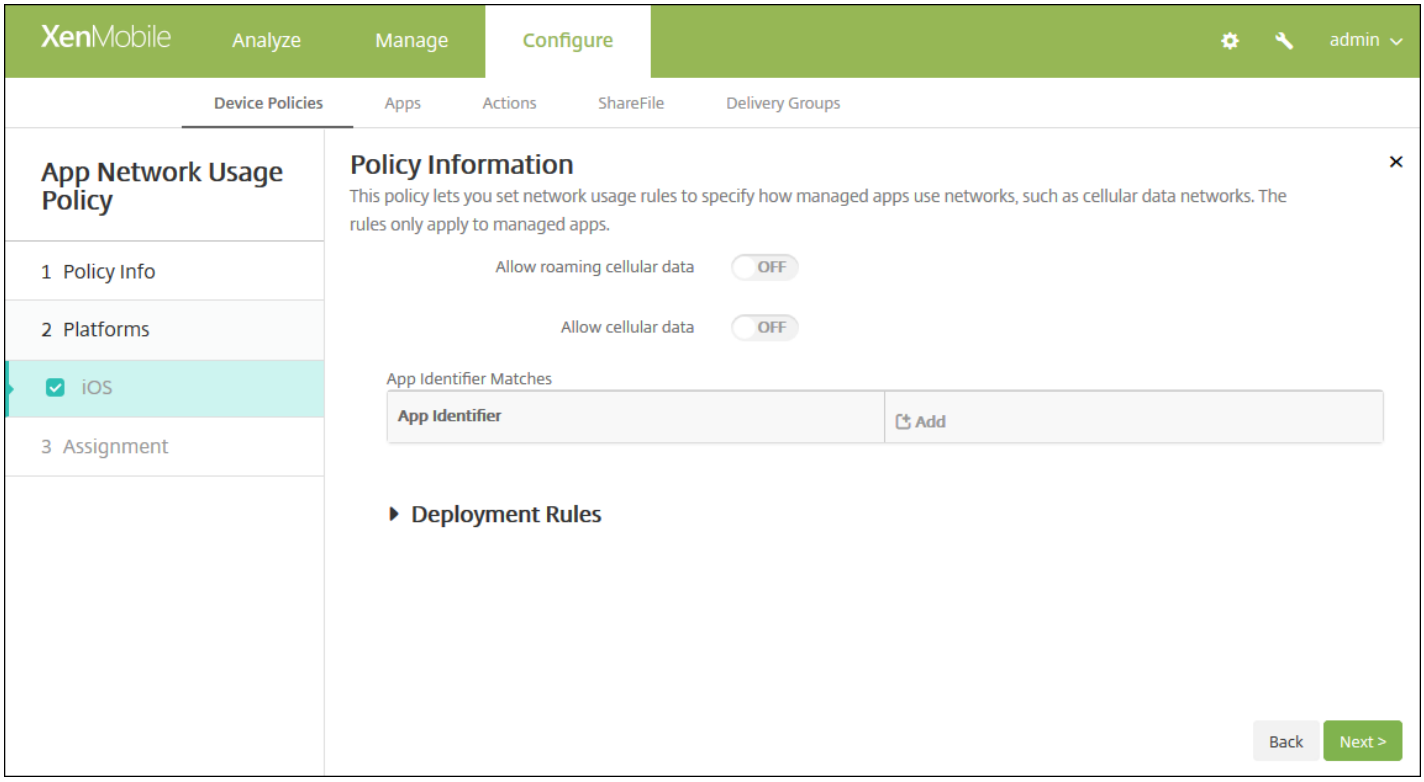
3. **[More]** を展開し、 **[Apps]** で **[App Network Usage]** をクリックします。 **[App Network Usage Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. 次の設定を構成します。

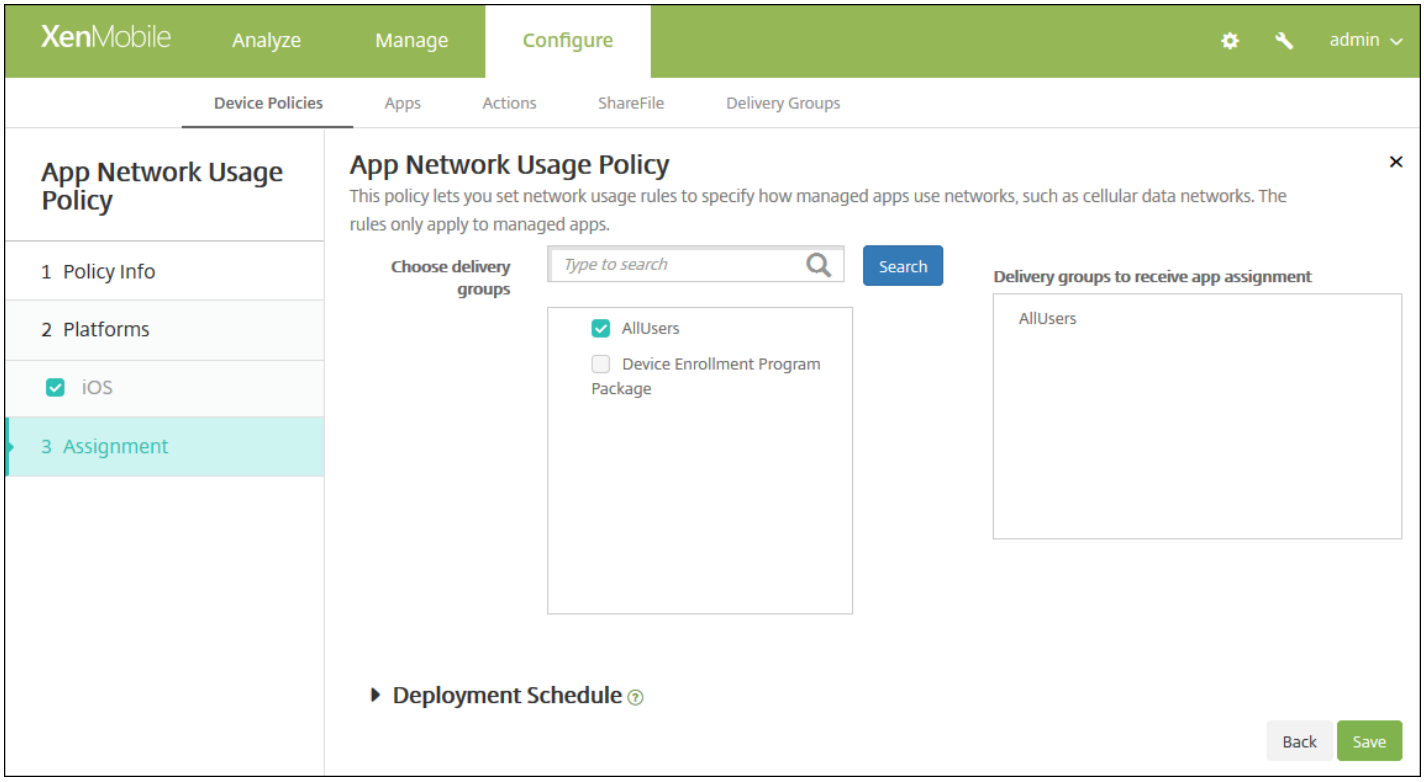
- **Allow roaming cellular data**：指定したアプリケーションに、ローミング中に携帯データネットワーク接続を使用することを許可するかどうかを選択します。 デフォルトは［**OFF**］です。
- **Allow cellular data**：指定したアプリケーションに、携帯データネットワーク接続を使用することを許可するかどうかを選択します。 デフォルトは［**OFF**］です。
- **App Identifier Matches**：一覧に追加するアプリケーションごとに、［**Add**］をクリックして以下の操作を行います。
  - **App Identifier**：アプリケーション識別子を入力します。
  - ［**Save**］をクリックしてアプリケーションを一覧に追加するか、［**Cancel**］をクリックして操作を取り消します。

    注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**App Network Usage Policy**］割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックしてポリシーを保存します。

アプリケーション制限デバイスポリシー

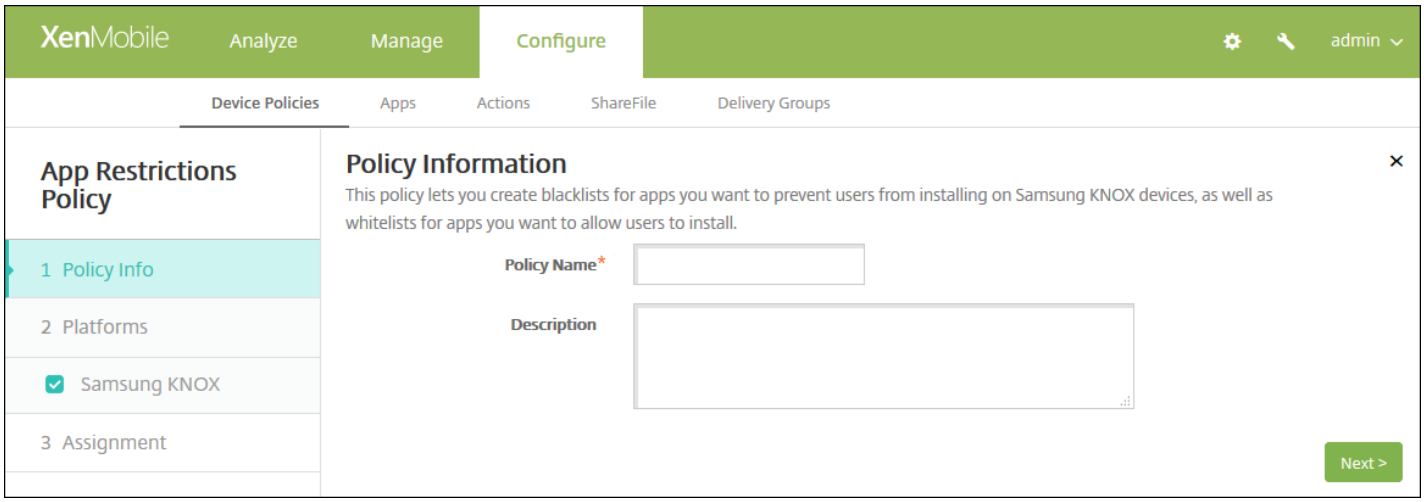
Aug 02, 2016

ユーザーによるSamsung KNOXデバイスへのインストールを禁止するアプリケーションのブラックリストを作成したり、ユーザーによるインストールを許可するアプリケーションのホワイトリストを作成したりできます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add New Policy**］ダイアログボックスが開きます。

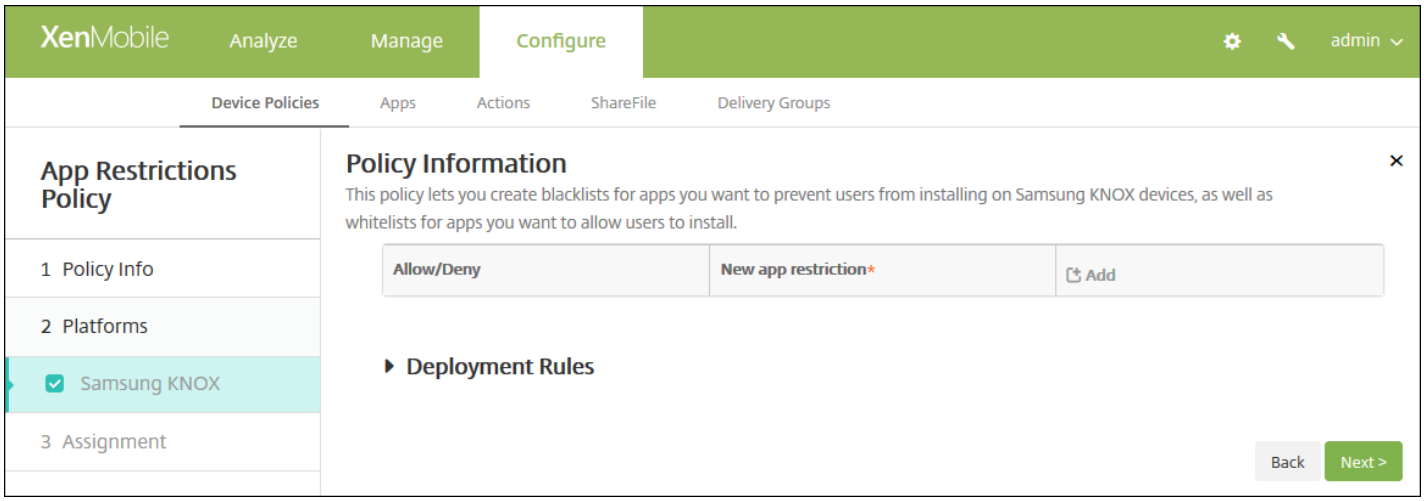
3.［**More**］を展開し、［**Security**］の下の［**App Restrictions**］をクリックします。［**App Restrictions Policy**］情報ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Samsung KNOX Platform**］ページが開きます。



6. ［Allow/Deny］の一覧に追加するアプリケーションごとに、**［Add］**をクリックして以下の操作を行います。

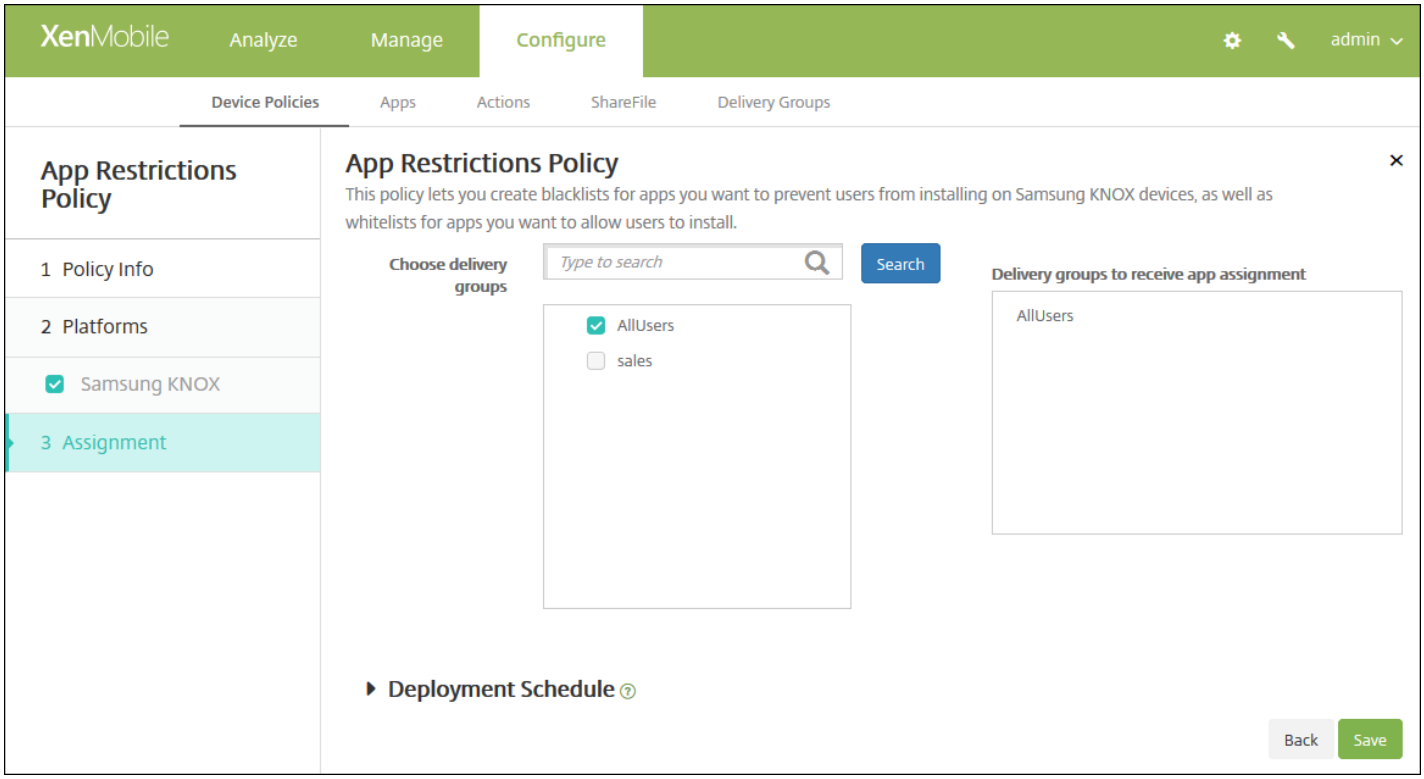
- **Allow/Deny**：ユーザーにアプリケーションのインストールを許可するかどうかを選択します。
- **New app restriction**：アプリケーションパッケージID（例：com.kmdm.af.crackle）を入力します。
- ［Allow/Deny］の一覧にアプリケーションを保存する場合は**［Save］**をクリックし、保存しない場合は**［Cancel］**をクリックします。

  注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには**［Delete］**をクリックし、項目をそのままにするには**［Cancel］**をクリックします。

  既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、 **［Save］**をクリックして変更した項目を保存するか、 **［Cancel］**をクリックして項目を変更せずそのままにします。

7. 展開規則を構成します。

8. **［Next］**をクリックします。 **［App Restrictions Policy］**割り当てページが開きます。



9. **［Choose delivery groups］**の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが**［Delivery groups to receive app assignment］**一覧に表示されます。

10. **［Deployment Schedule］**を展開して以下の設定を構成します。

- **［Deploy］**の横の**［ON］**をクリックすると展開がスケジュールされ、**［OFF］**をクリックすると展開が行われません。 デフォルトのオプションは**［ON］**です。 **［OFF］**を選択した場合、そのほかのオプションを構成する必要はありません。
- **［Deployment schedule］**の横の**［Now］**または**［Later］**をクリックします。 デフォルトのオプションは**［Now］**で

す。

- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

アプリケーショントンネリングデバイスポリシー

Aug 02, 2016

アプリトンネルは、モバイルアプリケーションのサービスの継続性およびデータ転送の信頼性を向上させるように設計されています。 アプリトンネルは、モバイルデバイスアプリケーションのクライアントコンポーネントとアプリケーションサーバコンポーネント間のプロキシパラメーターを定義します。 また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。 アプリケーショントンネリングポリシーは、Androidデバイスおよび Windows Mobile/CEデバイスに対して構成できます。

注：このポリシーで定義したトンネルを使用して送信されるアプリケーショントラフィックは、XenMobileを経由してから、アプリケーションを実行するサーバーにリダイレクトされます。

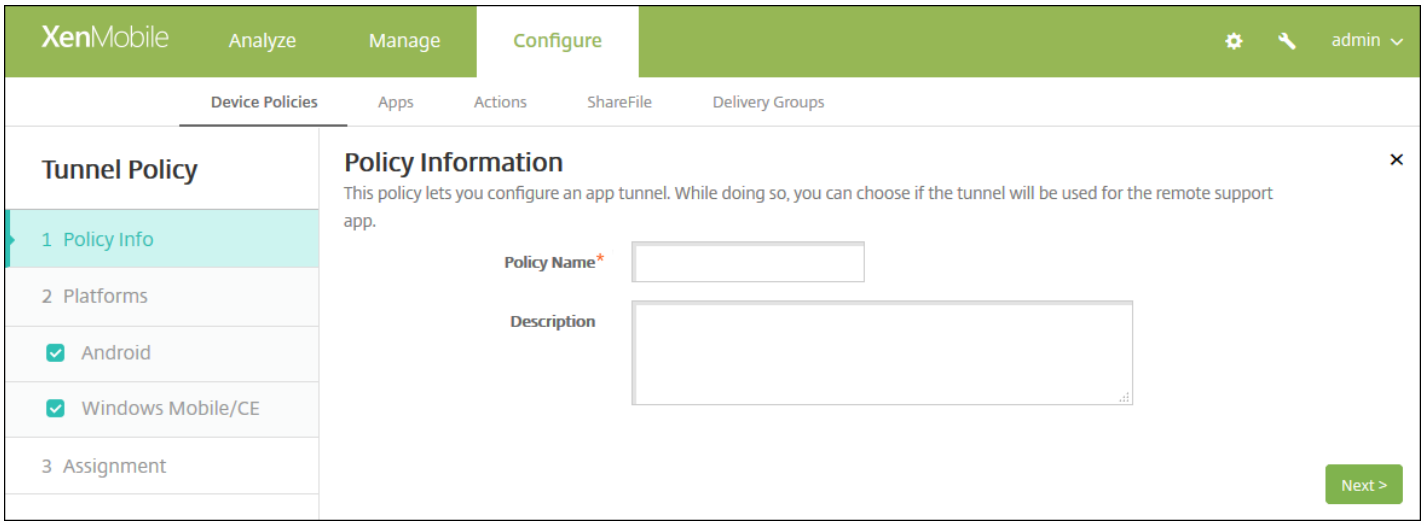
Androidの設定

Windows Mobile/CEの設定

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**More**］をクリックした後、［**Network access**］の下の［**Tunnel**］をクリックします。 ［**Tunnel Policy**］ページが開きます。



［**Policy Information**］ペインで、以下の情報を入力します。

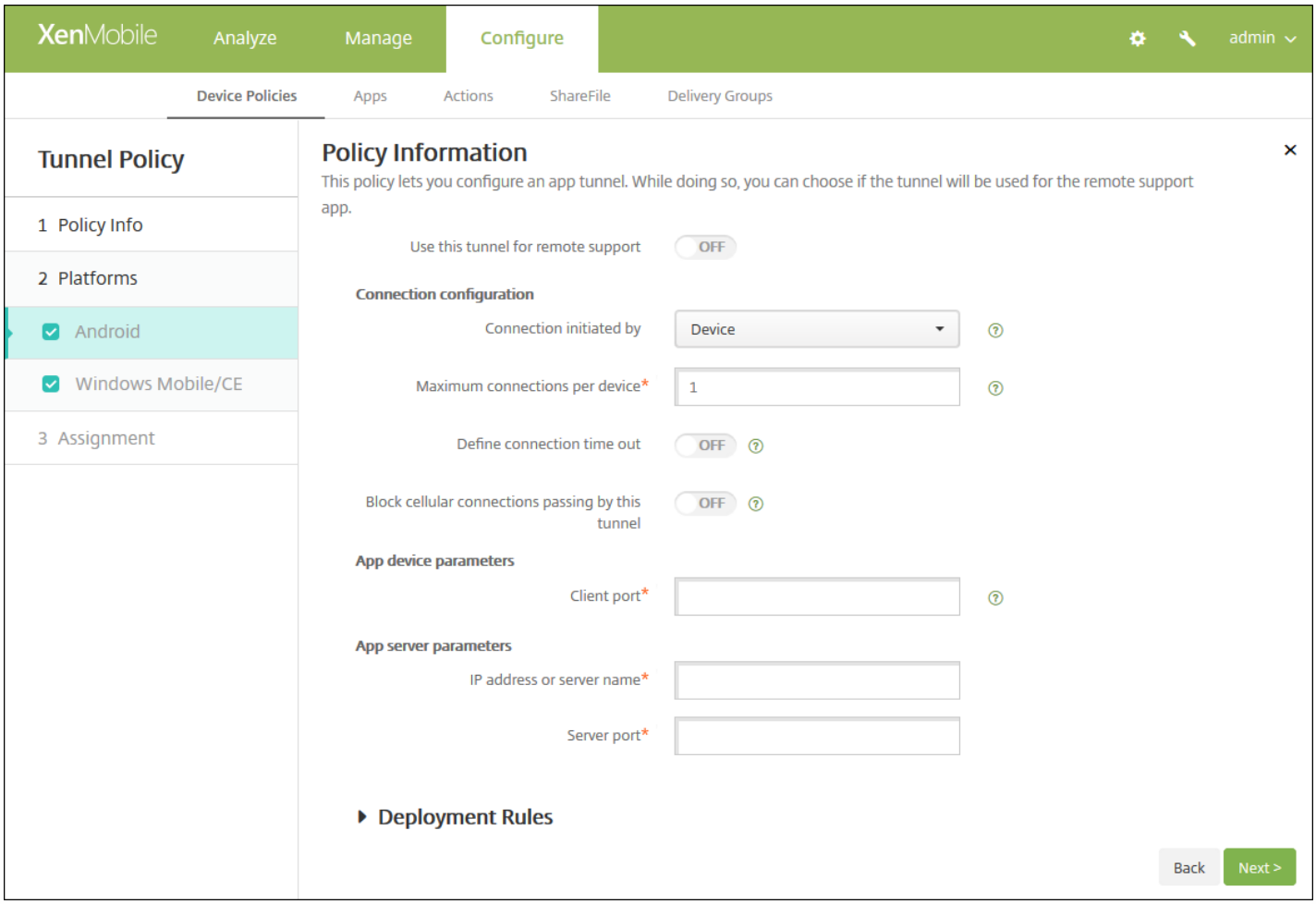
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Policy Platforms**］ページが開きます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

Androidの設定の構成



次の設定を構成します。

- **[Use this tunnel for remote support]**：トンネルをリモートサポートで使用するかどうかを選択します。

  注：リモートサポートを選択するかどうかによって、構成手順が異なります。

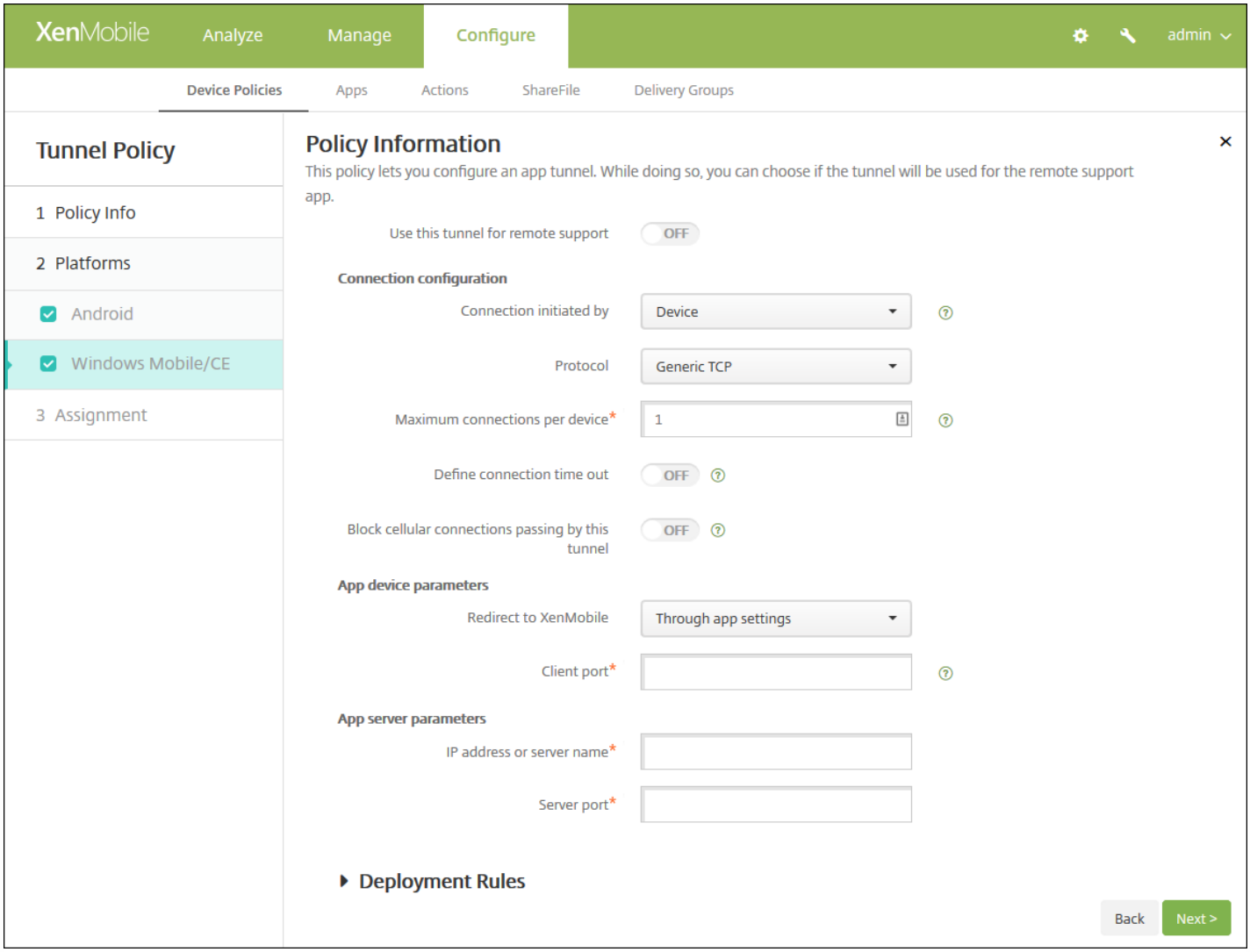
- リモートサポートを選択しない場合、以下の手順を実行します。
  - **Connection initiated by**：一覧から**[Device]**または**[Server]**を選択して、接続の開始元を指定します。
  - **Maximum connections per device**：数値を入力して、アプリケーションが確立できる同時TCP接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**：**[Define connection time out]**を**[On]**に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。

    注：WiFiおよびUSB接続はブロックされません。

  - **Client port**：クライアントのポート番号を入力します。 ほとんどの場合、この値はサーバーポートと同じです。
  - **IP address or server name**：アプリケーションサーバーの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

イスで開始する接続にのみ適用されます。
  - **Server port**：サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - **Use this tunnel for remote support**：［**On**］に設定します。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**：［**Define connection time out**］を［**On**］に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Use SSL connection**：このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。
    注：WiFiおよびUSB接続はブロックされません。

Windows Mobile/CEの設定の構成



次の設定を構成します。

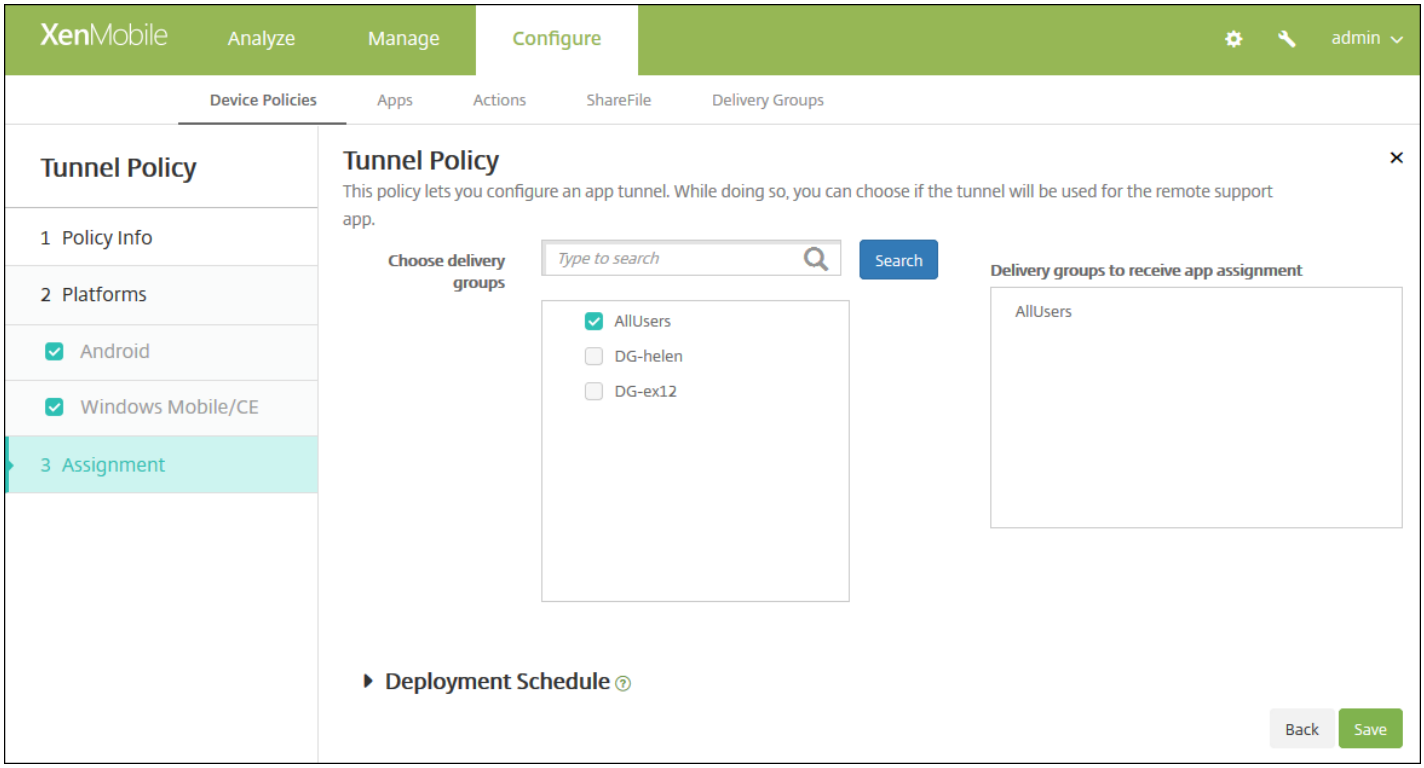
- ［**Use this tunnel for remote support**］：トンネルをリモートサポートで使用するかどうかを選択します。

注：リモートサポートを選択するかどうかによって、構成手順が異なります。

- リモートサポートを選択しない場合、以下の手順を実行します。
  - **Connection initiated by**： 一覧から［**Device**］または［**Server**］を選択して、接続の開始元を指定します。
  - **Protocol**：一覧から、使用するプロトコルを選択します。 デフォルトは［**Generic TCP**］です。
  - **Maximum connections per device**：数値を入力して、アプリケーションが確立できる同時TCP接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**： ［**Define connection time out**］を［**On**］に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。
    注：WiFiおよびUSB接続はブロックされません。
  - **Redirect to XenMobile**：一覧から、XenMobileへのデバイスの接続方法を選択します。 デフォルトは［**Through app settings**］です。
    - ［**Using a local alias**］を選択した場合は、 ［**Local alias**］にエイリアスを入力します。 デフォルト値は［**localhost**］です。
    - ［**An IP address range**］を選択した場合は、 ［**IP address range from**］に開始IPアドレスを入力し、 ［**IP address range to**］に終了IPアドレスを入力します。
  - **Client port**：クライアントのポート番号を入力します。 ほとんどの場合、この値はサーバーポートと同じです。
  - **IP address or server name**：アプリケーションサーバーのIPアドレスまたは名前を入力します。 このフィールドはデバイスで開始する接続にのみ適用されます。
  - **Server port**：サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - **Use this tunnel for remote support**： ［**On**］に設定します。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**： ［Define connection time out］を［On］に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Use SSL connection**：このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。
    注：WiFiおよびUSB接続はブロックされません。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Tunnel Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

アプリケーションアンインストールデバイスポリシー

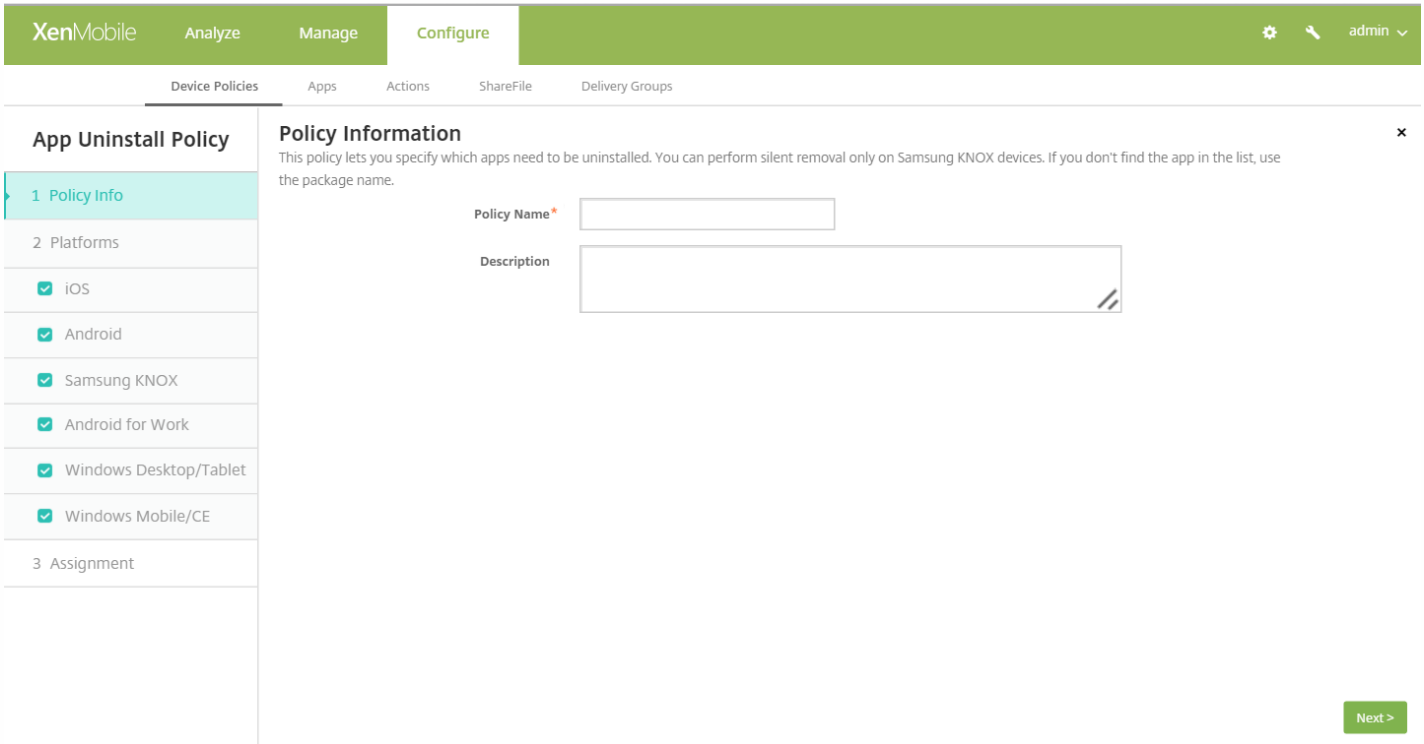
Aug 02, 2016

iOS、Android、Samsung KNOX、Android for Work、Windowsデスクトップ/タブレット、およびWindows Mobile/CEのプラットフォームに対するアプリケーションアンインストールポリシーを作成できます。 アプリケーションアンインストールポリシーにより、さまざまな理由でユーザーのデバイスからアプリケーションを削除できます。 この理由には、特定のアプケーションをサポートしなくなったことや、会社が既存アプリケーションから異なるベンダーが提供する類似アプリケーションへの置き換えを希望していることなどがあります。 このポリシーがユーザーのデバイスに展開されると、アプリケーションが削除されます。 Samsung KNOX以外のデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージが表示されます。Samsung KNOXデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージは表示されません。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**More**］を展開し、 ［**Apps**］の下の［**App Uninstall**］をクリックします。 ［**App Uninstall Policy**］ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

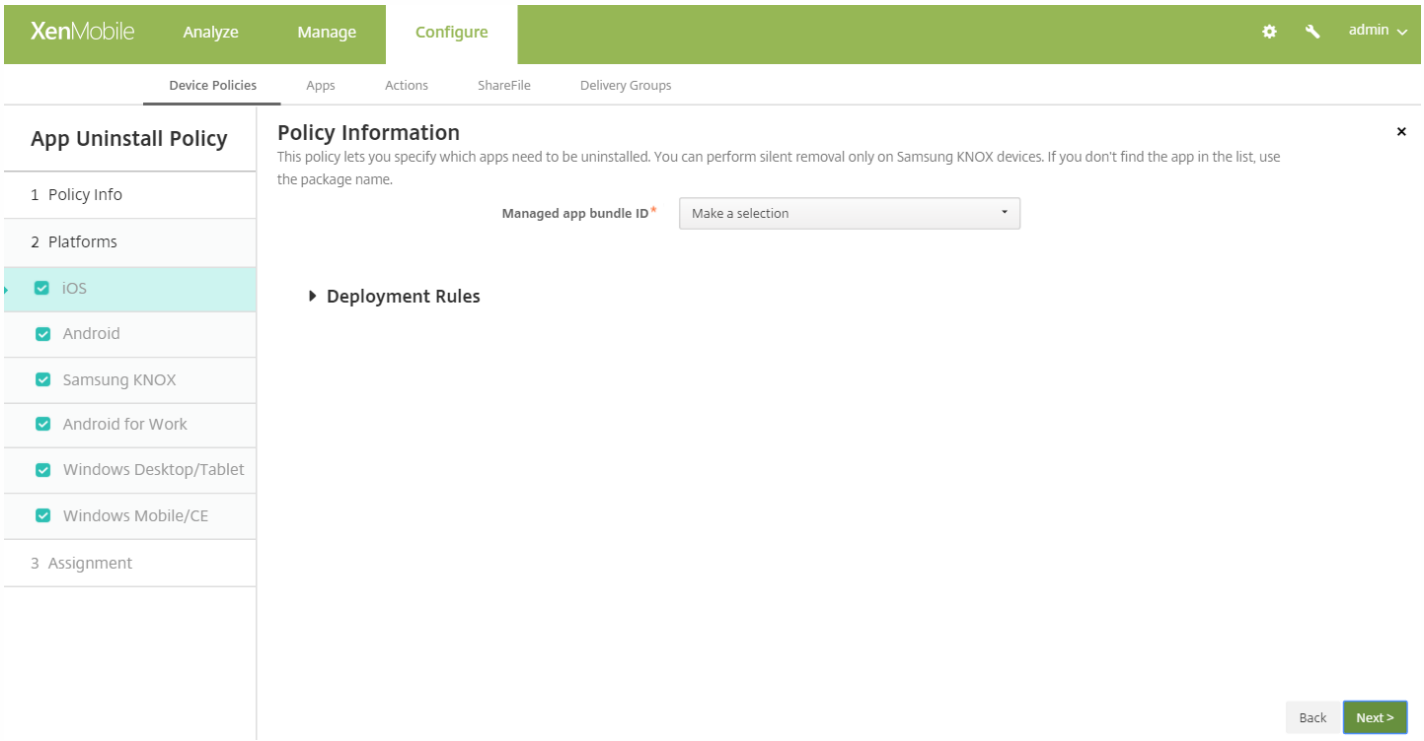
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Policy Platforms**］ページが開きます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

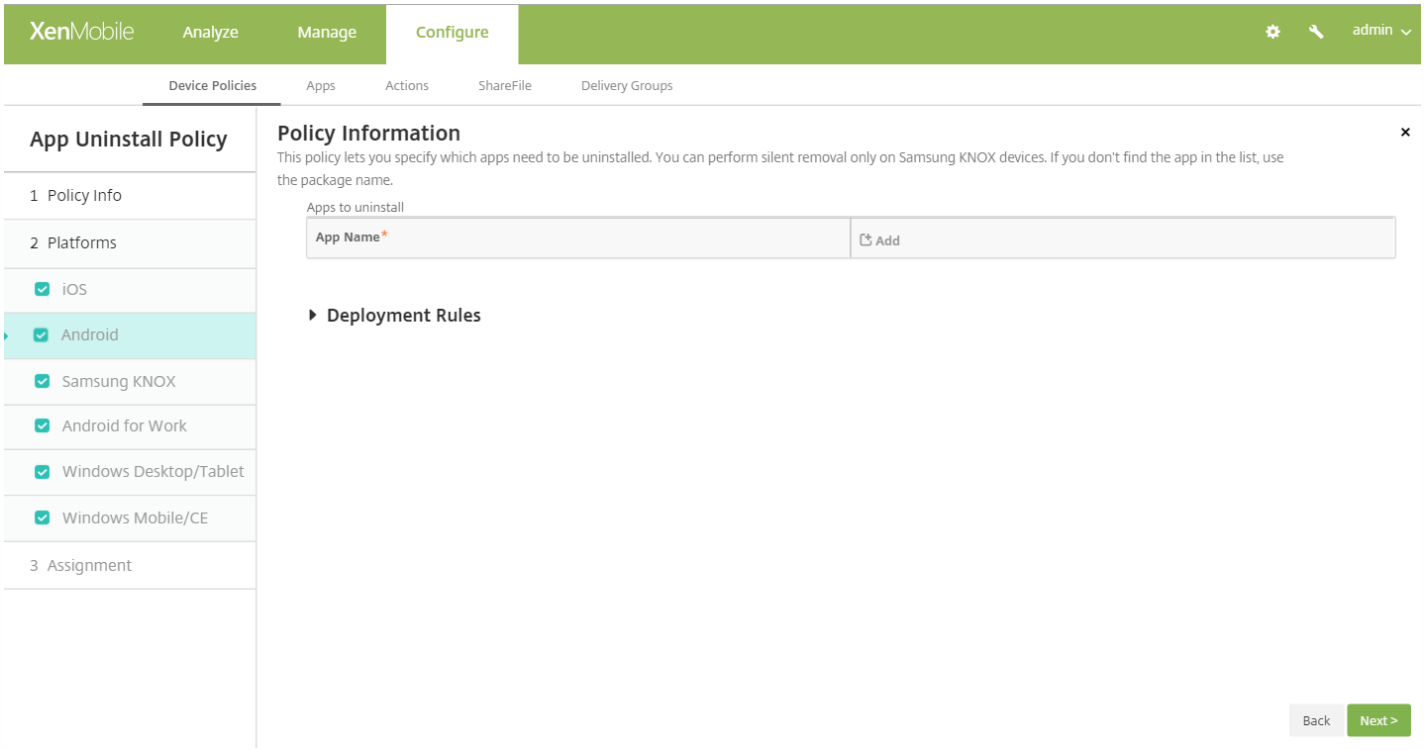
iOSの設定の構成



次の設定を構成します。

- **Managed app bundle ID**：一覧で、既存のアプリケーションを選択するか、［**Add new**］をクリックします。 このプラットフォームに対してアプリケーションが構成されていない場合は一覧が空になるため、新しいアプリケーションを追加する必要があります。
  - ［**Add**］をクリックすると、アプリケーション名を入力できるフィールドが表示されます。

ほかのすべてのプラットフォーム設定の構成



次の設定を構成します。

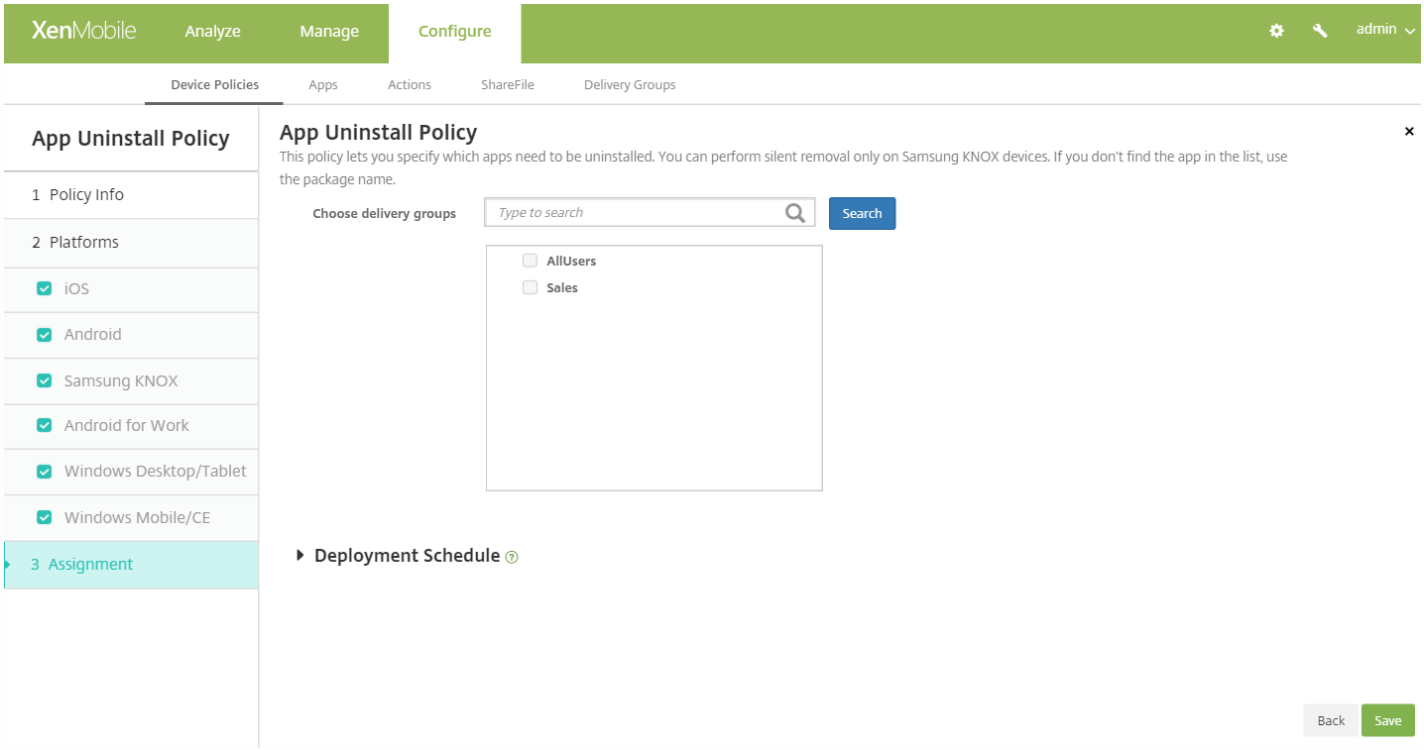
- **Apps to uninstall**：追加するアプリケーションごとに、［**Add**］をクリックして以下の操作を行います。
  - **App name**：一覧で既存のアプリケーションを選択するか、［**Add new**］をクリックして新しいアプリケーション名を入力します。 このプラットフォームに対してアプリケーションが構成されていない場合は一覧が空になるため、新しいアプリケーションを追加する必要があります。
  - ［**Add**］をクリックしてアプリケーションを追加するか、［**Cancel**］をクリックしてアプリケーションの追加を取り消します。

    注：アンインストールポリシーから既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**App Uninstall Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

アプリケーションアンインストール制限デバイスポリシー

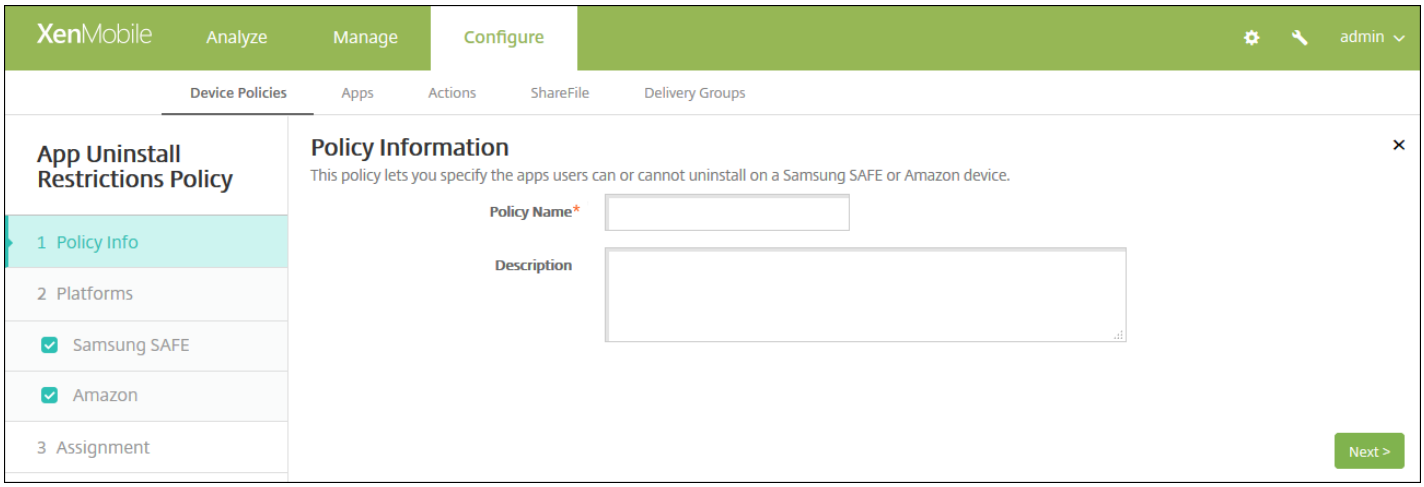
Aug 02, 2016

ユーザーにSamsung SAFEデバイスまたはAmazonデバイスでのアンインストールを許可するアプリケーションを指定することができます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。

2.［**Add**］をクリックします。［**Add a New Policy**］ダイアログボックスが開きます。

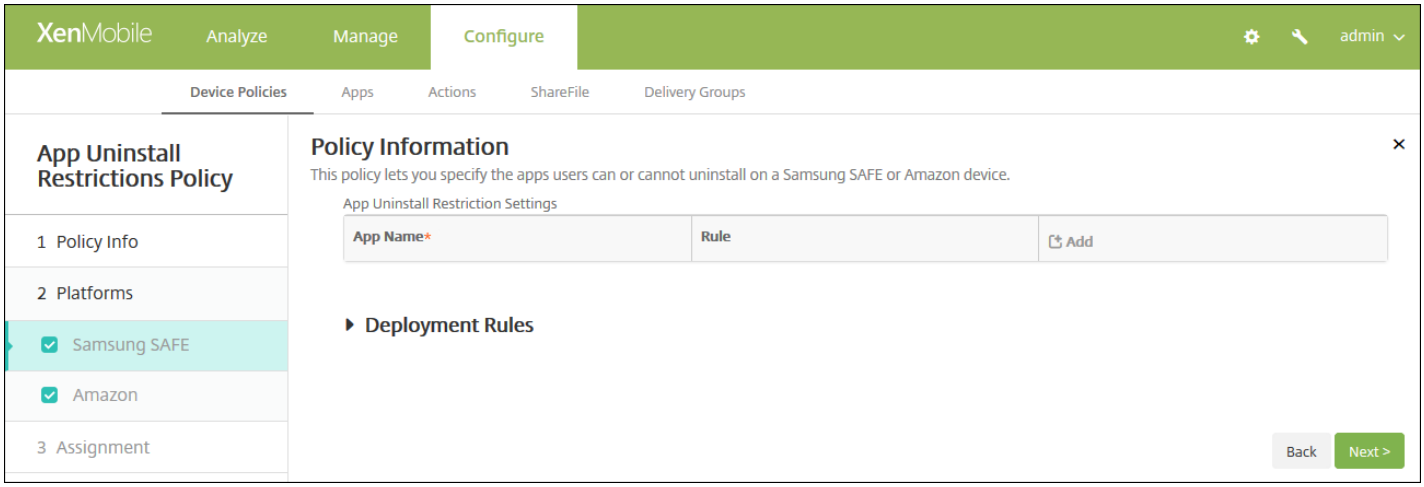
3.［**More**］を展開し、［**Apps**］で［**App Uninstall Restrictions**］をクリックします。［**App Uninstall Restrictions Policy**］情報ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Policy Platforms**］ページが開きます。



6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、次の設定を構成します。

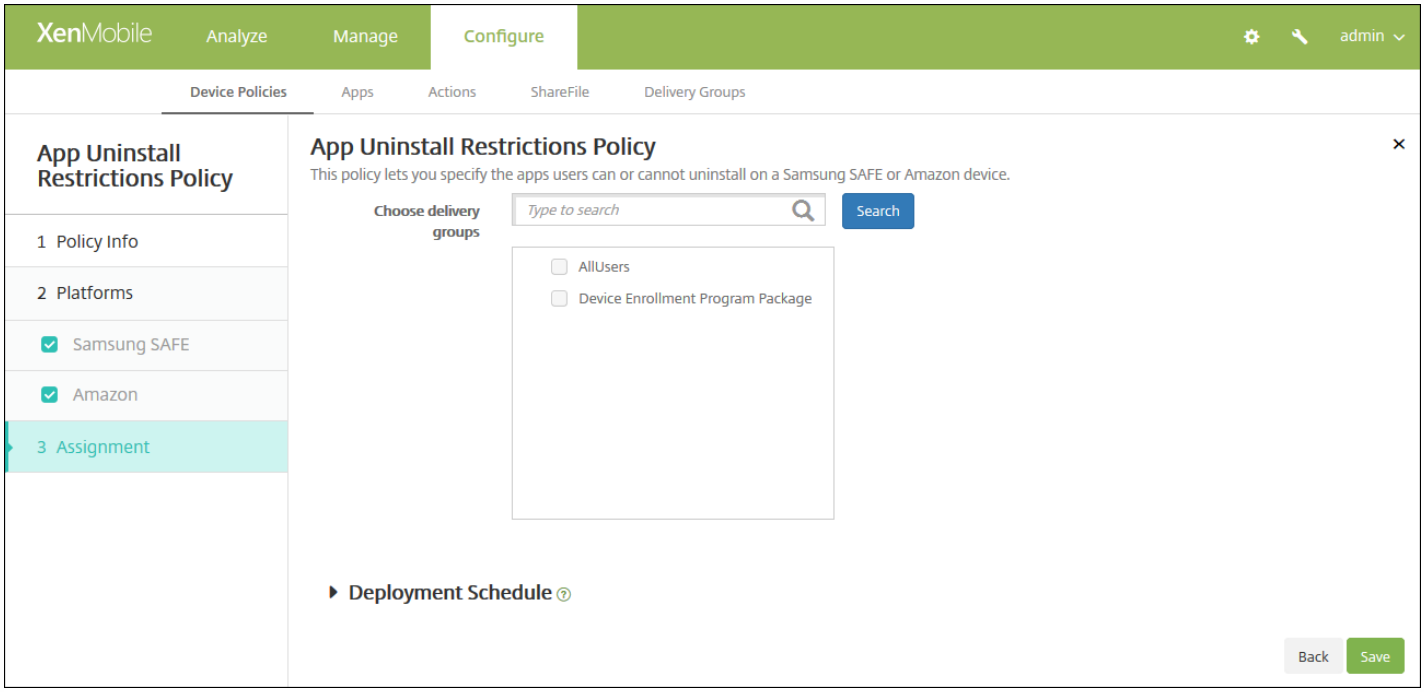
- **App Uninstall Restrictions Settings**：追加するアプリケーション規則ごとに、 [**Add**] をクリックして以下の操作を行います。
  - **App name**：一覧でアプリケーションをクリックするか、または [**Add new**] をクリックして新しいアプリケーションを追加します。
  - **Rule**：ユーザーがアプリケーションをアンインストールできるかどうかを選択します。 デフォルトの設定ではアンインストールが許可されています。
  - [**Save**] または [**Cancel**] をクリックします。

    注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには [**Delete**] をクリックし、項目をそのままにするには [**Cancel**] をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、 [**Save**] をクリックして変更した項目を保存するか、 [**Cancel**] をクリックして項目を変更せずそのままにします。

8. 展開規則の構成

9. [**Next**] をクリックします。 [**App Uninstall Restrictions Policy**] 割り当てページが開きます。



10. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

11. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

ブラウザーデバイスポリシー

Aug 02, 2016

Samsung SAFE、Samsung KNOX、およびAndroid for Wordデバイスの ブラウザーデバイスポリシーを作成して、 ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、ユーザーのデバイスで使用できるブラウザー機能を制限したりすることができます。 Samsungデバイスでは、ブラウザーを完全に無効にすることや、ポップアップ、JavaScript、Cookie、オートフィル、不正Webサイト警告の適用の有無を有効または無効にすることができます。 Android for Worksデバイスでは、特定のURLをブラックリストまたはホワイトリストに追加したり、特定のセキュアブラウザーのブックマークを追加したりすることができます。

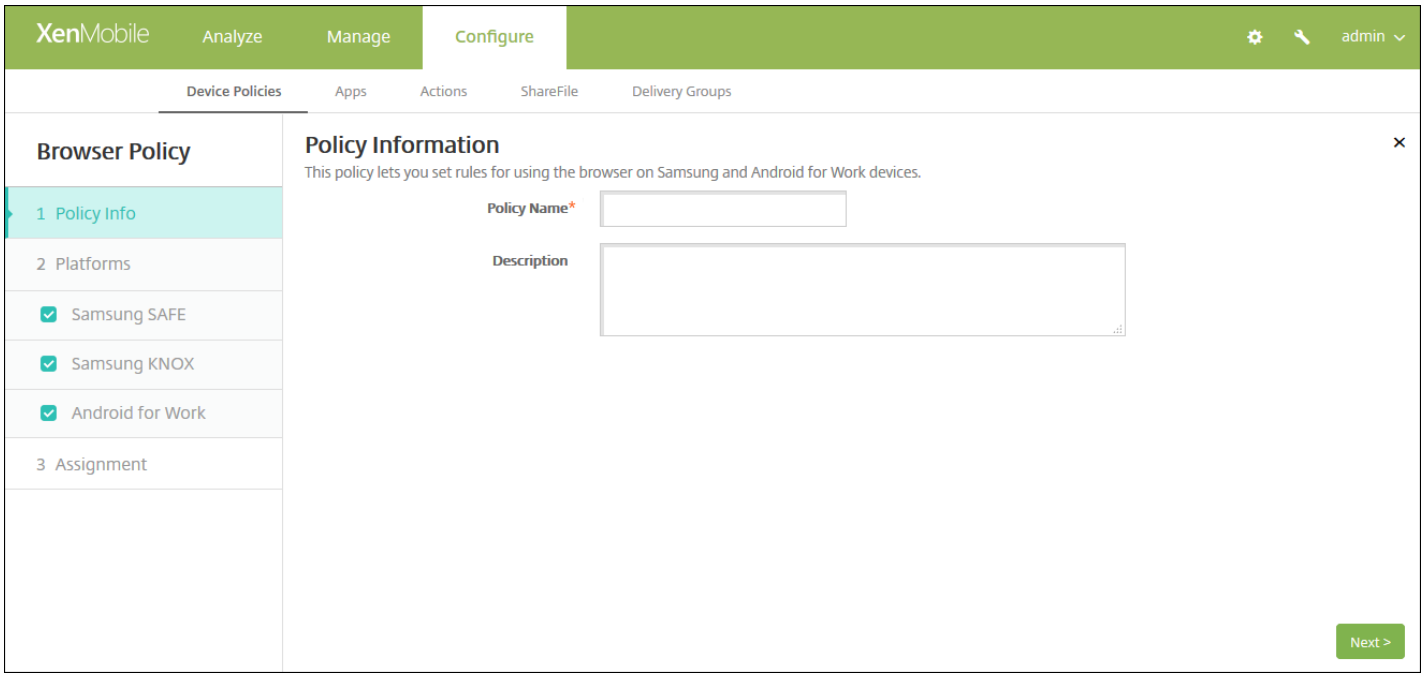
Samsung SAFEおよびSamsung KNOXの設定

Android for Workの設定

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2.新しいポリシーを追加するために **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** をクリックした後、 **[Apps]** の下の **[Browser]** をクリックします。 **[Browser Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

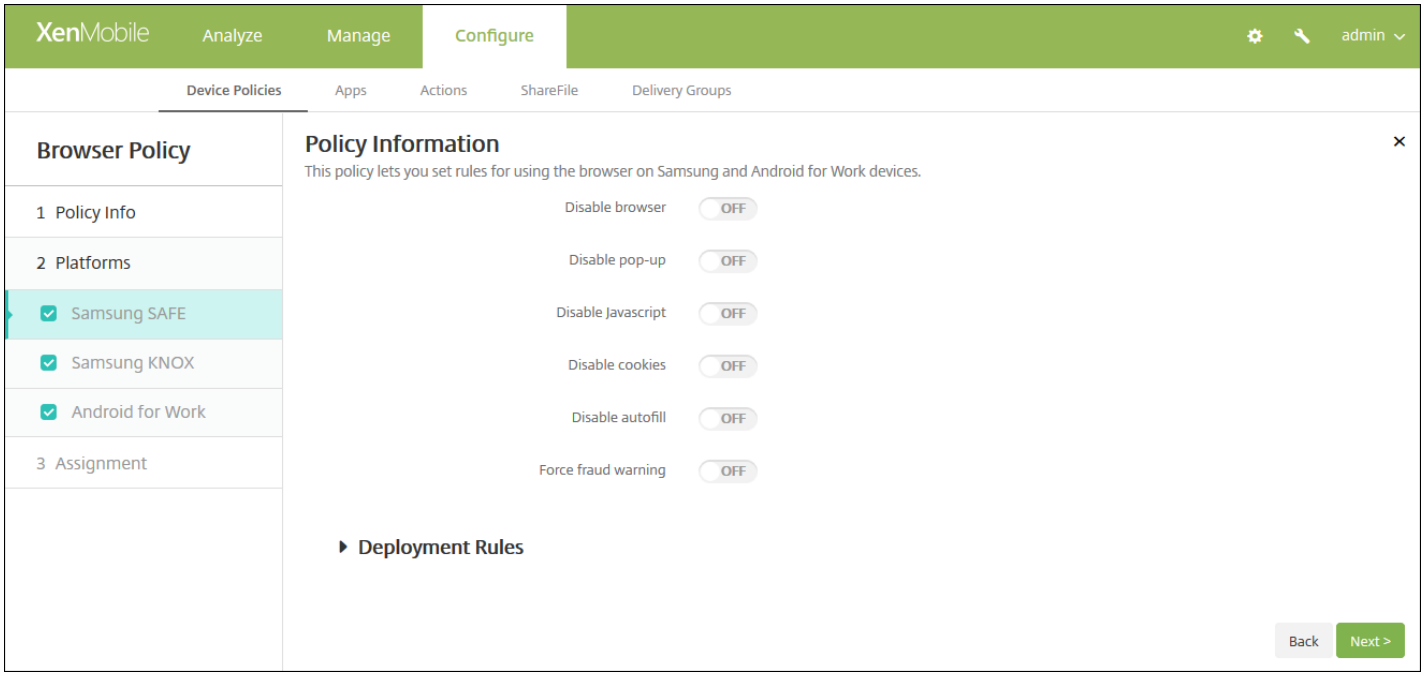
5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ

以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

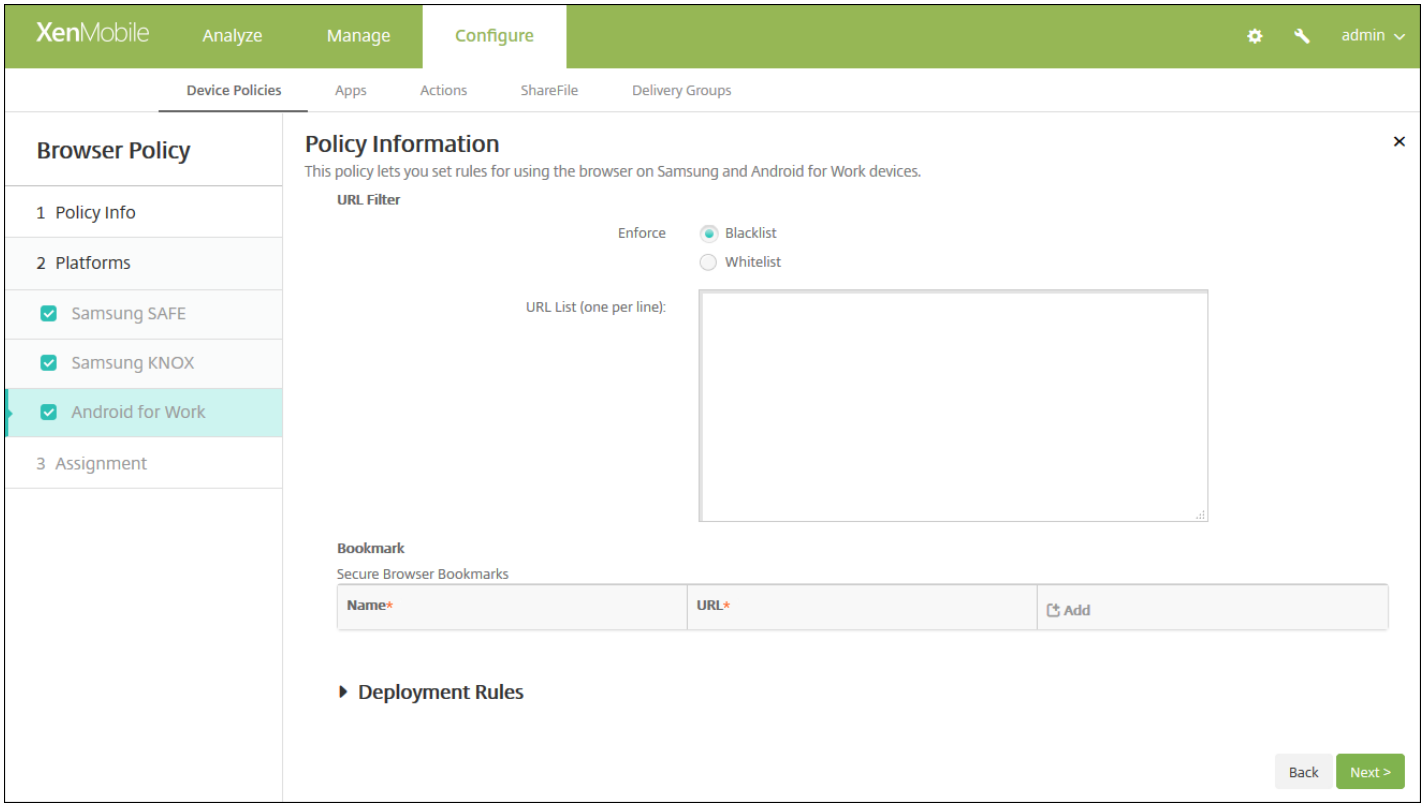
Samsung SAFEおよびSamsung KNOXの設定の構成



次の設定を構成します。

- **Disable browser**：ユーザーのデバイスでSamsungブラウザーを完全に無効にするかどうかを選択します。 デフォルトは **[OFF]** で、ユーザーはブラウザーを使用できます。 ブラウザーを無効にした場合、以下のオプションは表示されなくなります。
- **Disable pop-up**：ブラウザーでポップアップメッセージを許可するかどうかを選択します。
- **Disable Javascript**：ブラウザーでJavaScriptの実行を許可するかどうかを選択します。
- **Disable cookies**：Cookieを許可するかどうかを選択します。
- **Disable autofill**：ユーザーがブラウザーのオートフィル機能をオンにできるかどうかを選択します。
- **Force fraud warning**：ユーザーが不正な、または信頼できないWebサイトを参照したときに、警告メッセージを表示するかどうかを選択します。

Android for Workの設定の構成

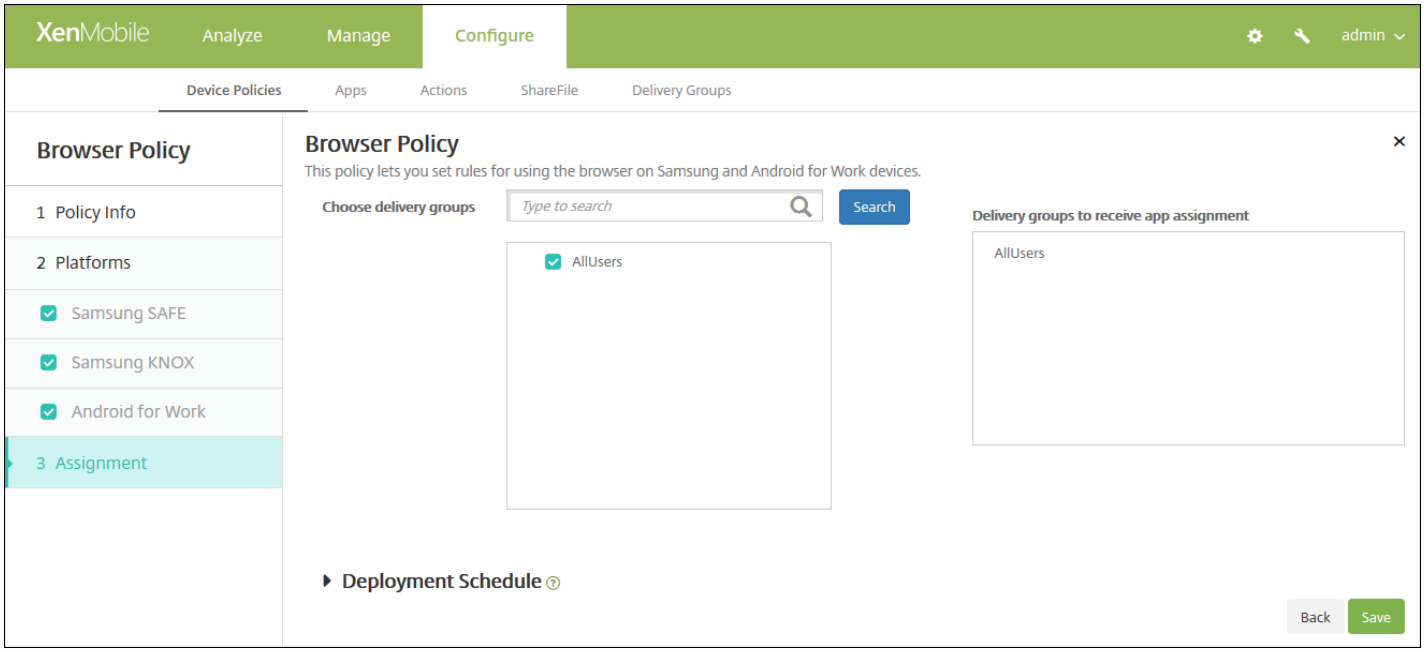


次の設定を構成します。

- ［**URL Filter**］で、以下の設定を構成します。
  - **Enforce**：［**Blacklist**］または［**Whitelist**］を選択します。［**Blacklist**］を選択した場合、ユーザーは管理者が指定したURLを*除く*すべてのURLにアクセスできます。［**Whitelist**］を選択した場合、ユーザーは管理者が指定したURLに*のみ*アクセスできます。
  - **URL List**：［**Enforce**］で選択した種類のリストにURLを（各行に1つずつ）入力します。
- ［**Bookmark**］の下の［**Add**］をクリックして、［**Name**］および［**URL**］にユーザーのセキュアブラウザーに表示されるブックマークの名前とURLを入力します。

7. 展開規則の構成

8. ［**Next**］をクリックします。［**Browser Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

カレンダー（CalDav）デバイスポリシー

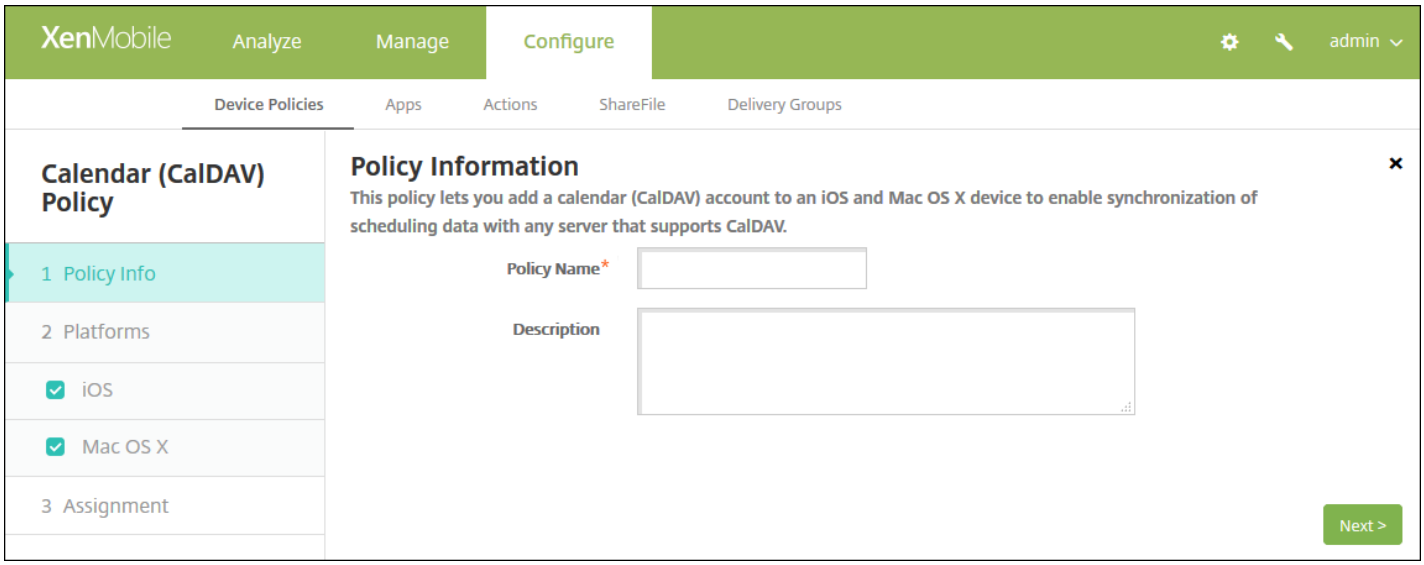
Aug 02, 2016

XenMobileでデバイスポリシーを追加して、カレンダー（CalDAV）アカウントをユーザーのiOSデバイスまたはMax OS Xデバイスに追加し、CalDAVをサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add a New Policy**］ダイアログボックスが開きます。

3.［**More**］を展開した後、［**End user**］の下の［**Calendar（CalDAV）**］をクリックします。
［**Calendar（CalDAV）Policy**］ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

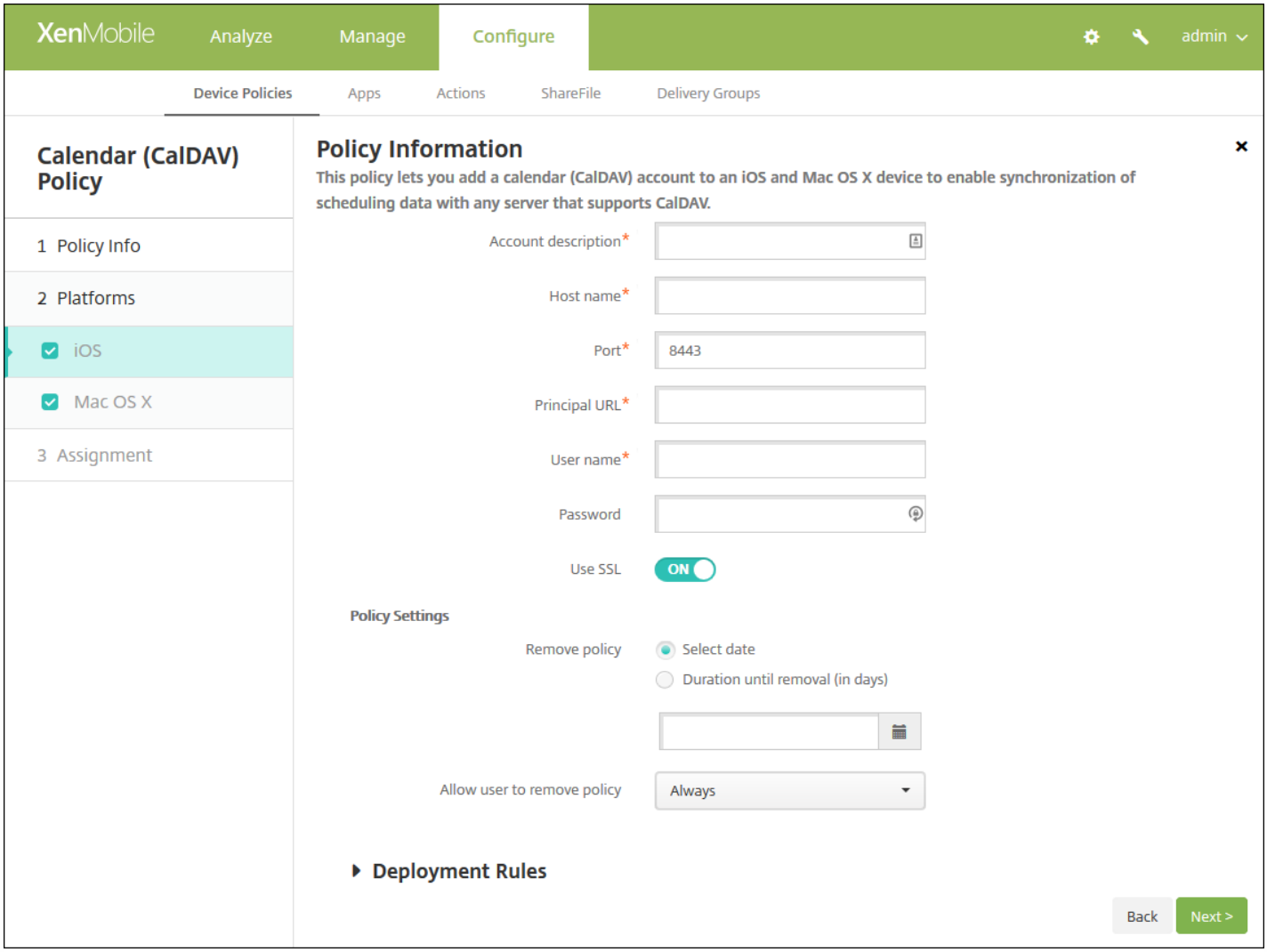
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Platforms**］ページが開きます。

6.［**Platforms**］の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

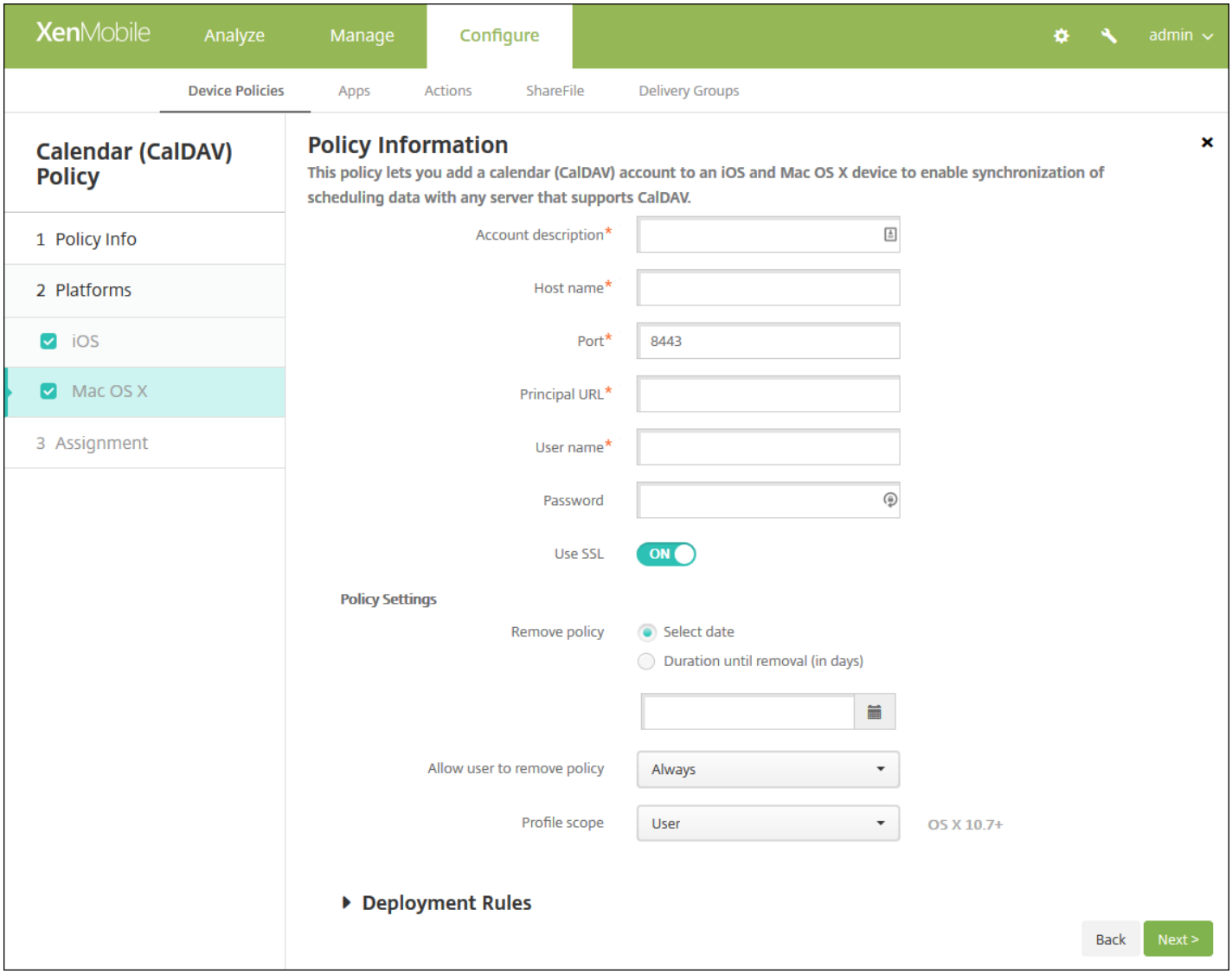
iOSの設定の構成



次の設定を構成します。

- **Account description**：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。
- **Host name**：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。
- **Port**：CalDAVサーバーへの接続用ポートを入力します。 このフィールドは必須です。 デフォルトは**8443**です。
- **Principal URL**：ユーザーのカレンダーに対するベースURLを入力します。
- **User name**：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。
- **Password**：任意で、ユーザーのパスワードを入力します。
- **Use SSL**：CalDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［**ON**］です。
- **ポリシー設定**
  - ［**Remove policy**］の横にある［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



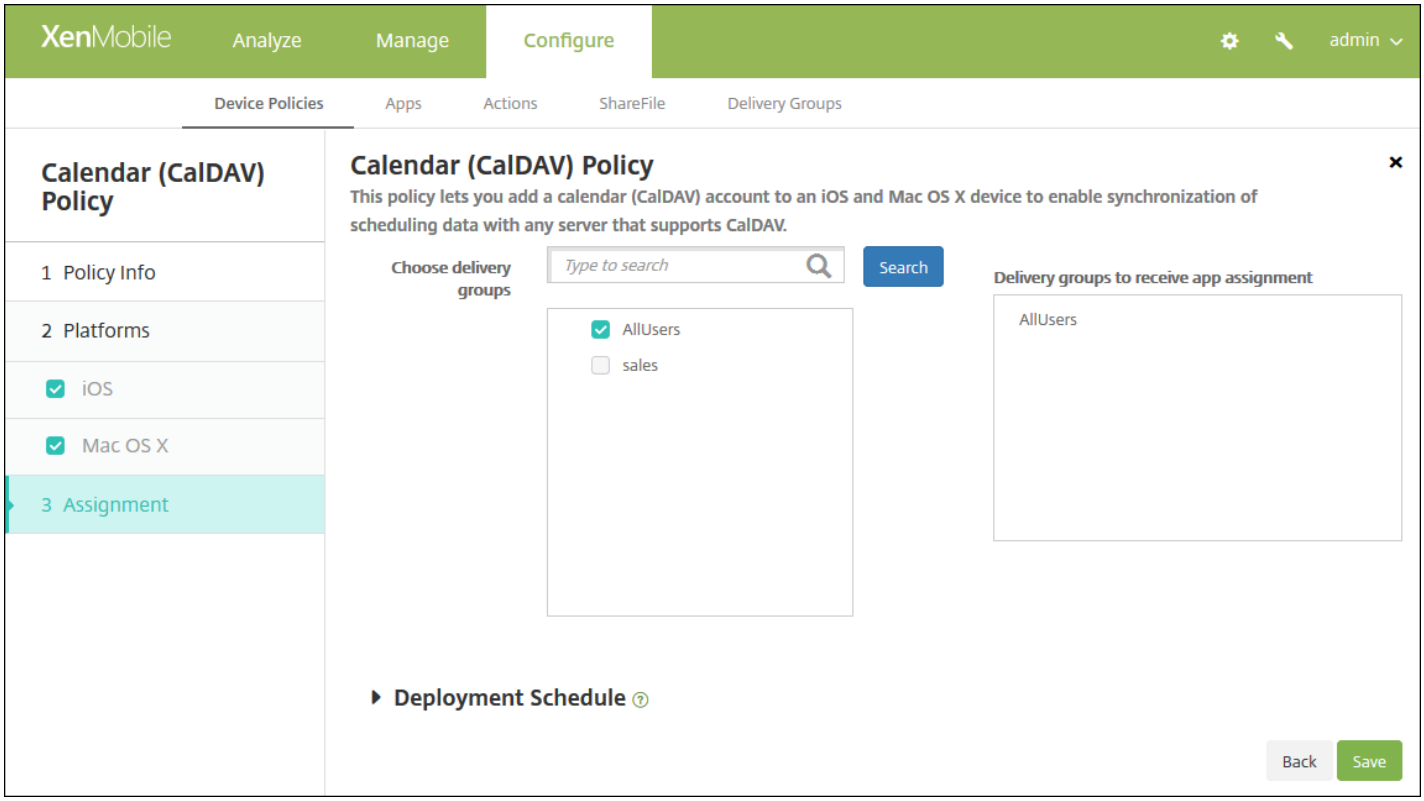
次の設定を構成します。

- **Account description**：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。
- **Port**：CalDAVサーバーへの接続用ポートを入力します。 このフィールドは必須です。 デフォルトは**8443**です。
- **Principal URL**：ユーザーのカレンダーに対するベースURLを入力します。
- **User name**：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。
- **Password**：任意で、ユーザーのパスワードを入力します。
- **Use SSL**：CalDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［**ON**］です。
- **ポリシー設定**
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、 ［**Always**］、 ［**Password required**］、 ［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、 ［**Removal password**］の横に必要なパスワードを入力します。
  - ［**Profile scope**］の横にある、 ［**User**］または［**System**］を選択します。 デフォルトは［**User**］です。 このオプ

ションはOS X 10.7以降でのみ使用できます。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[Calendar（CalDAV）Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

モバイルデバイスポリシー

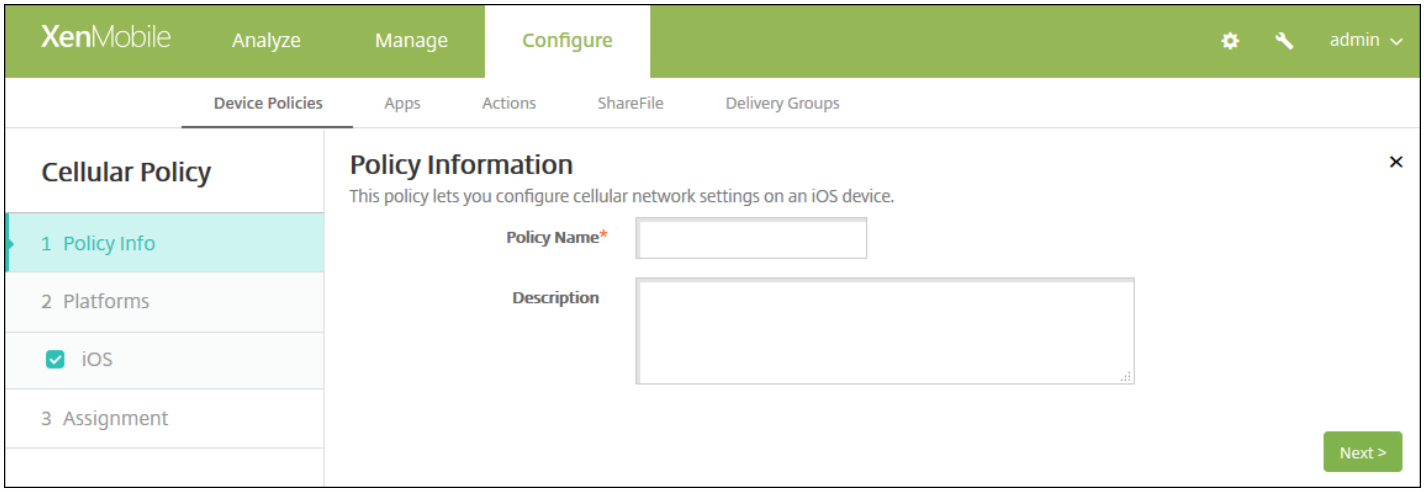
Aug 02, 2016

このポリシーを使用すると、iOSデバイスのモバイルネットワーク設定を構成できます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add a New Policy**］ページが開きます。

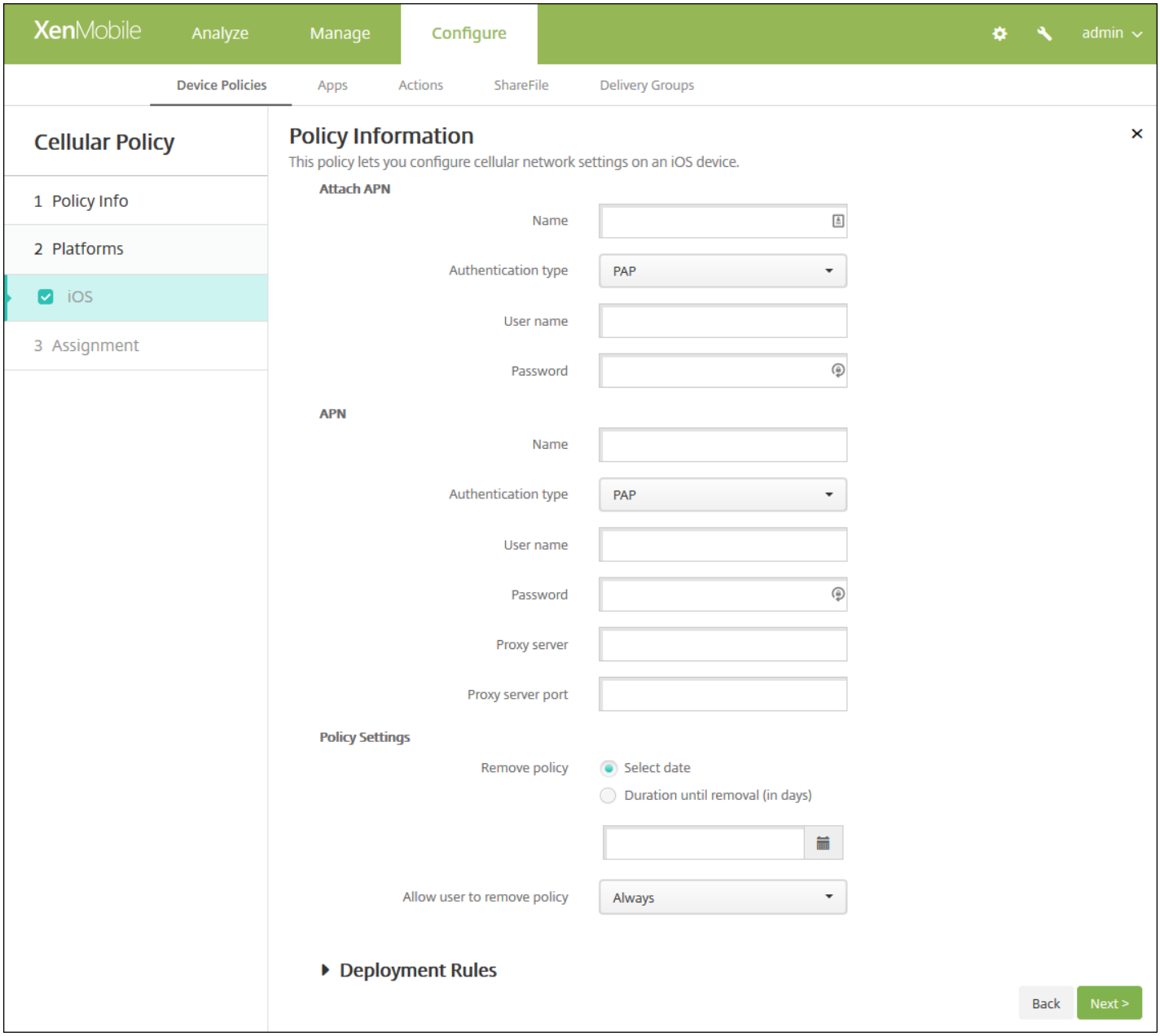
3.［**More**］を展開した後、［**Network Access**］の下の［**Celluar**］をクリックします。［**Cellular Network Policy**］情報ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**iOS Platform**］情報ページが開きます。



6. 次の設定を構成します。

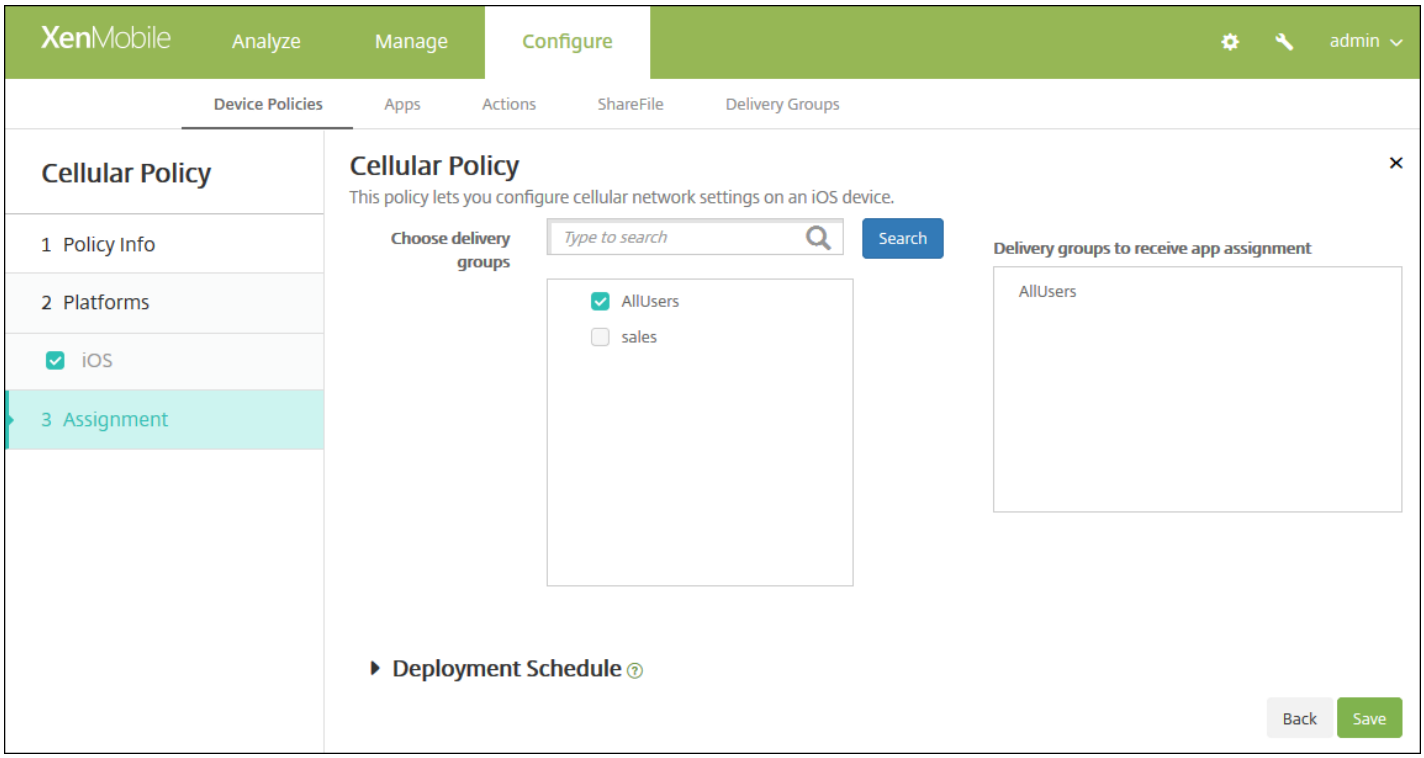
- **Attach APN**
  - **Name**：この構成の名前を入力します。
  - **Authentication type**：一覧から、［**CHAP**］（Challenge-Handshake Authentication Protocol：チャレンジハンドシェイク認証プロトコル）または［**PAP**］（Password Authentication Protocol：パスワード認証プロトコル）のいずれかを選択します。 デフォルトは［**PAP**］です。
  - **User name**：認証に使用するユーザー名を入力します。
- **APN**
  - **Name**：APN（Access Point Name：アクセスポイント名）構成の名前を入力します。
  - **Authentication type**：一覧から、［**CHAP**］または［**PAP**］を選択します。 デフォルトは［**PAP**］です。
  - **User name**：認証に使用するユーザー名を入力します。
  - **Password**：認証に使用するパスワードを入力します。

- **Proxy server**：プロキシサーバーのネットワークアドレスを入力します。

- ポリシー設定
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

7. 展開規則の構成

8. ［**Next**］をクリックします。［**Cellular Network Policy**］割り当てページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。 デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、 **[Settings] の [Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

接続マネージャーデバイスポリシー

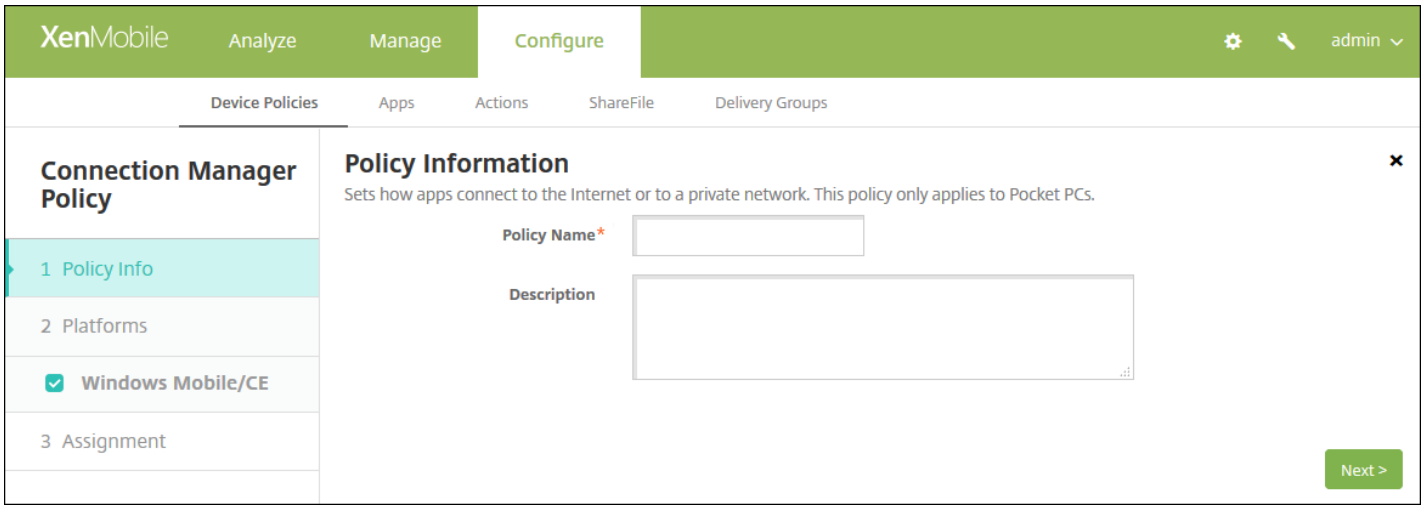
Aug 02, 2016

XenMobileでは、インターネットおよびプライベートネットワークに自動的に接続するアプリケーションの接続設定を指定できます。 このポリシーはWindows Pocket PCでのみ使用できます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

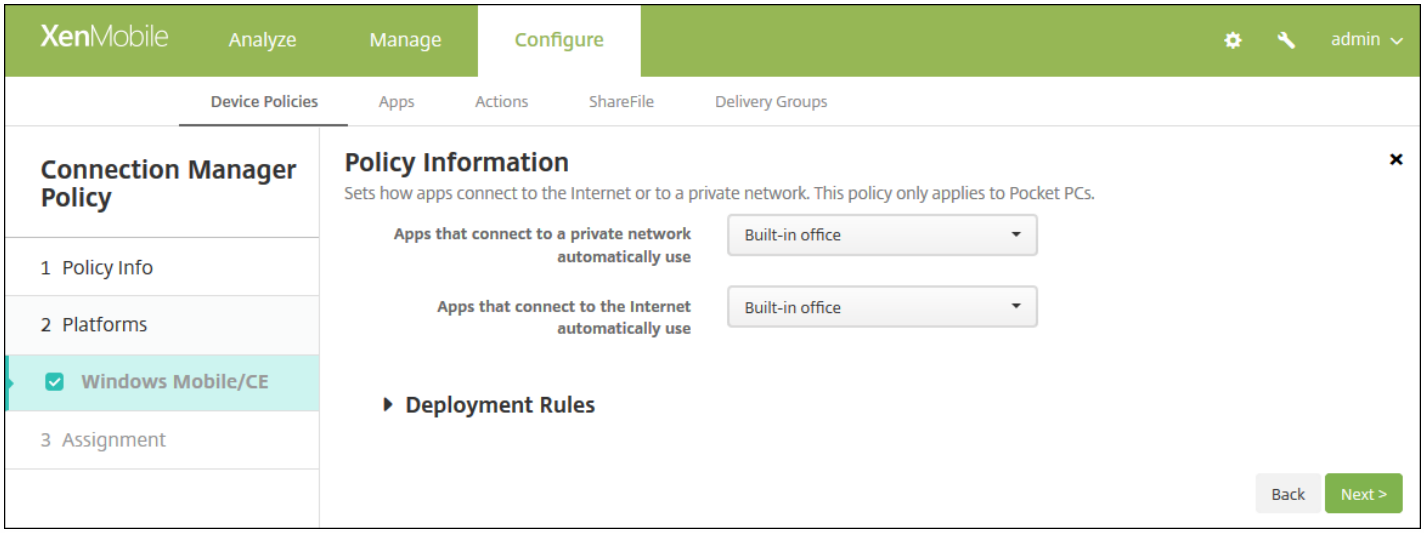
3. ［**More**］をクリックした後、［**Network access**］の下の［**Connection Manager**］をクリックします。 ［**Connection Manager Policy**］情報ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Windows Mobile/CE Platform**］ページが開きます。



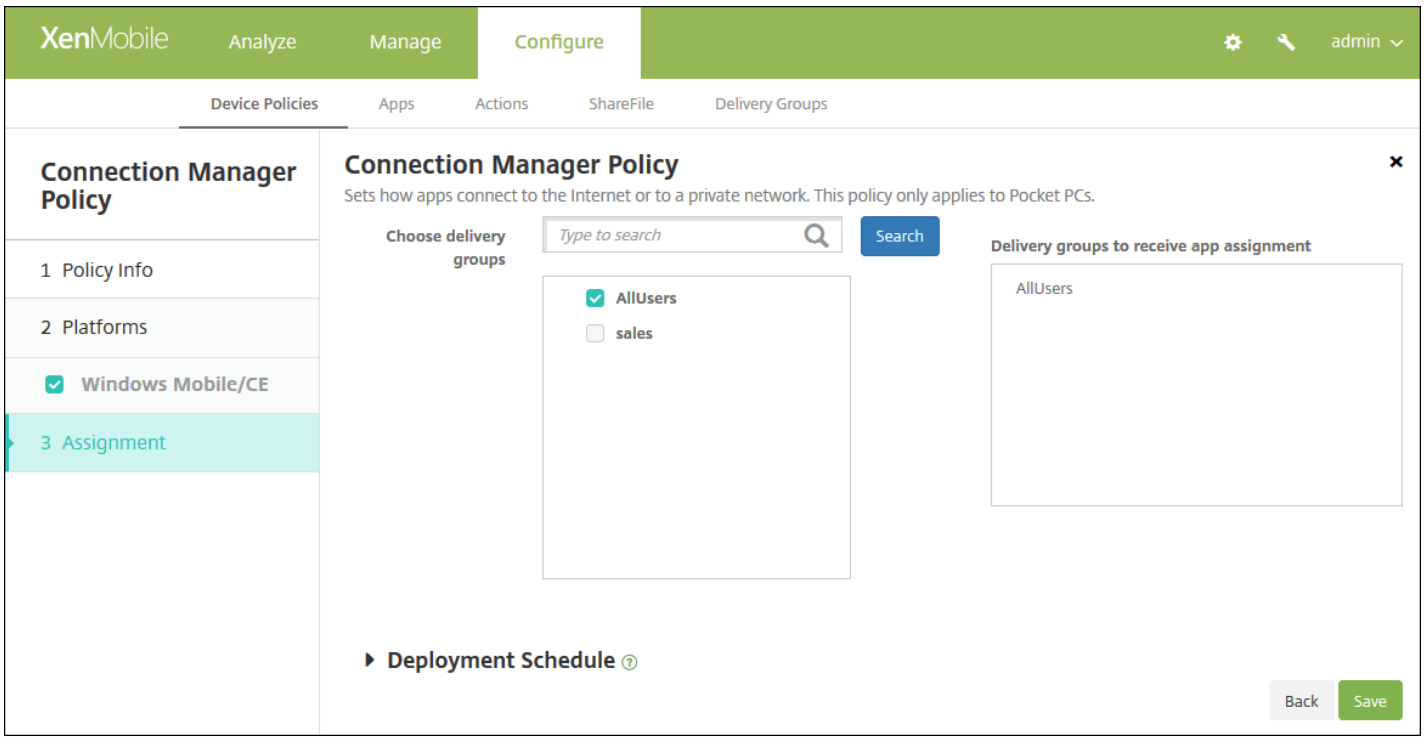
6. 次の設定を構成します。

注： **[Built-in office]** は、すべての接続先が社内イントラネットであることを意味します。**[Built-in Internet]** は、すべての接続先がインターネットであることを意味します。

- **Apps that connect to a private network automatically use** : 一覧から、 **[Built-in office]** または **[Built-in Internet]** を選択します。 デフォルトは **[Built-in office]** です。
- **Apps that connect to the Internet automatically use**一覧から、 **[Built-in office]** または **[Built-in Internet]** を選択します。 デフォルトは **[Built-in office]** です。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[Connection Manager]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

接続スケジュールデバイスポリシー

Aug 02, 2016

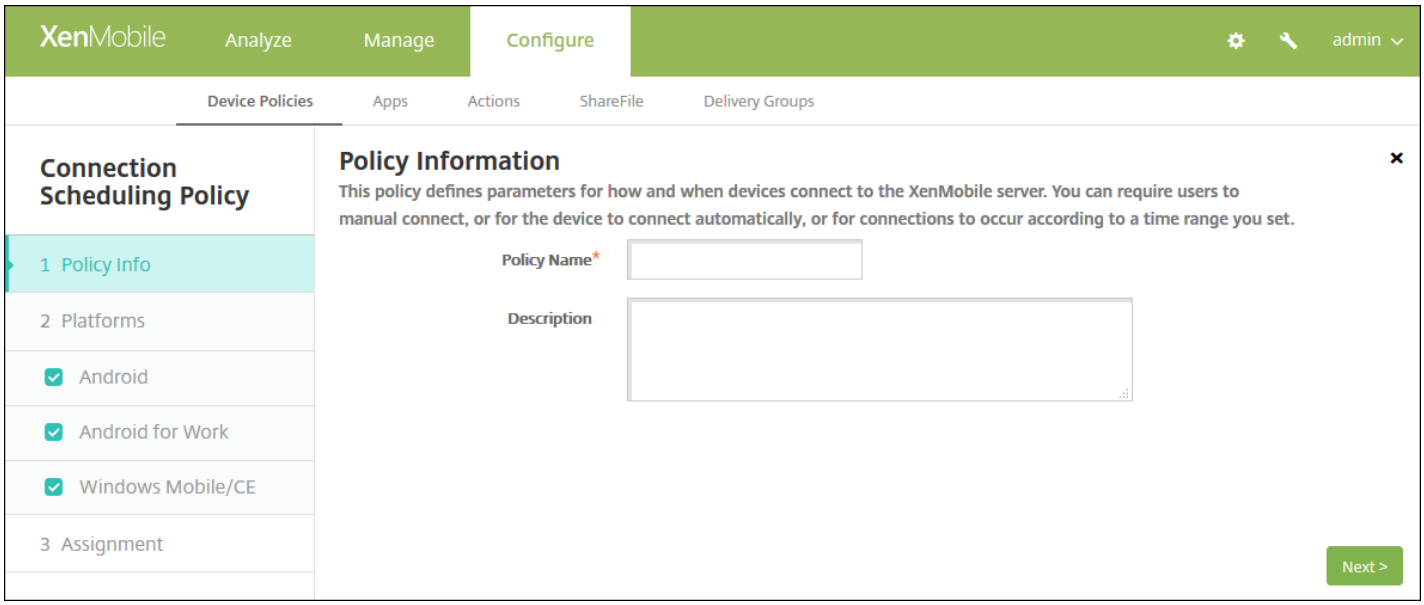
接続スケジュールポリシーを作成して、ユーザーのデバイスをXenMobileに接続する方法と時間を管理します。 このポリシーは、Android for Work対応デバイスに対しても構成できます。

ユーザーが手動でデバイスを接続するか、デバイスが永続的に接続されたままにするか、定義した期間内にデバイスが接続されるようにするかを指定できます。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

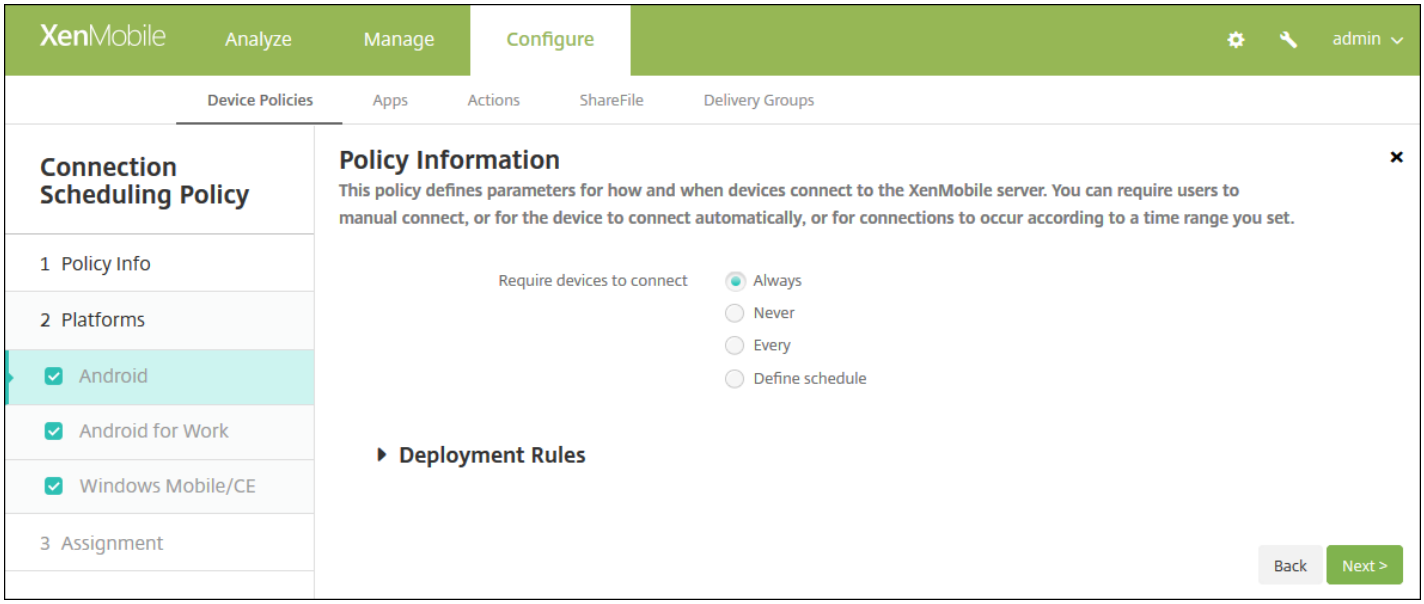
3. **[Scheduling]** をクリックします。 **[Connection Scheduling Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順8.を参照してプラットフォームの展開規則を設定します。

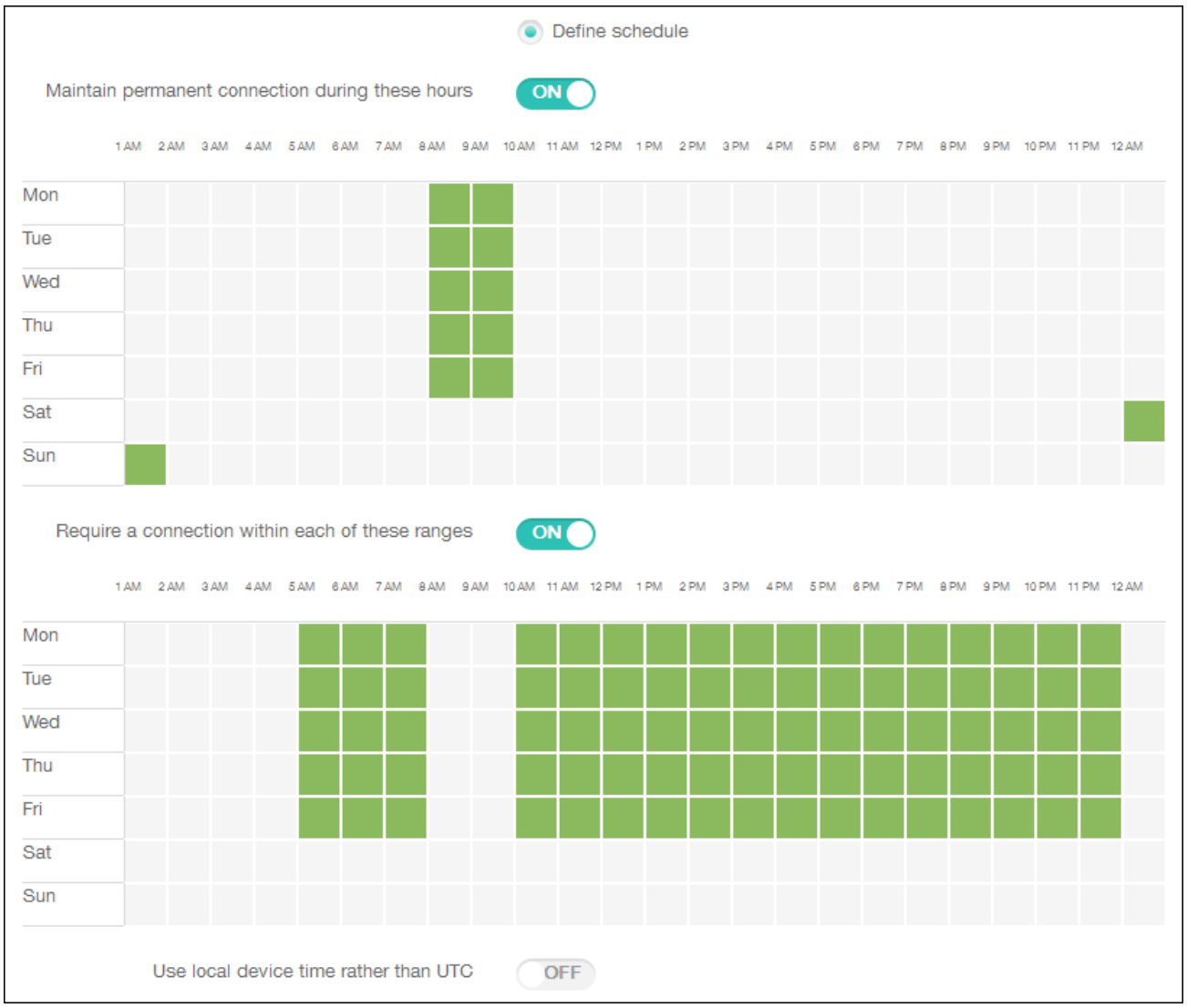
7. 選択したプラットフォームごとに、次の設定を構成します。

- **Require devices to connect**：このスケジュールに対して設定するオプションをクリックします。
  - **Always**：接続のオンライン状態を永続的に維持します。 ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobileサーバーへの再接続を試行し、一定の間隔でコントロールパケットを送信することによって接続を監視します。このオプションは、最適化されたセキュリティに対してのみお勧めします。 **[Always]** を選択する場合は、デバイスで**トンネルポリシー**の **[Define connection time-out]** 設定も使用して、接続によりバッテリーが切れないようにします。 接続のオンライン状態を維持することにより、ワイプやロックなどのセキュリティコマンドを必要に応じてデバイスにプッシュできます。 デバイスに展開された各ポリシーで、 **[Deployment Schedule]** の **[Deploy for always-on connections]** オプションを選択する必要もあります。
  - **Never**：手動で接続します。 ユーザーはデバイスでXenMobileから接続を開始する必要があります。デバイスにセキュリティポリシーを展開できず、新しいアプリやポリシーを受信しなくなるため、実稼働環境ではこのオプションはおすすめしません。
  - **Every**：指定された間隔で接続されます。 このオプションが有効な状態でロックやワイプなどのセキュリティポリシーを送信すると、この操作は次回デバイスが接続されたときに処理されます。 このオプションを選択すると、 **[Connec every N minutes]** フィールドが表示されます。このフィールドに、デバイスが再接続されるまでの分数を入力する必要があります。 デフォルトは**20**です。
  - **Define schedule**：有効にすると、ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後にXenMobile サーバーへの再接続を試行し、定義した期間中、一定の間隔でコントロールパケットを送信することによって接続を監視します。 接続期間の定義方法については、「接続期間の定義」を参照してください。
    - **Maintain permanent connection during these hours**：定義した期間中、ユーザーのデバイスが接続されている必要があります。
    - **Require a connection within each of these ranges**：定義した期間内に1回以上、ユーザーのデバイスが接続される必要があります。
    - **Use local device time rather than UTC**：定義した期間を、UTC（Coordinated Universal Time：協定世界時）ではなくローカルデバイスの時間に同期させます。

接続期間の定義

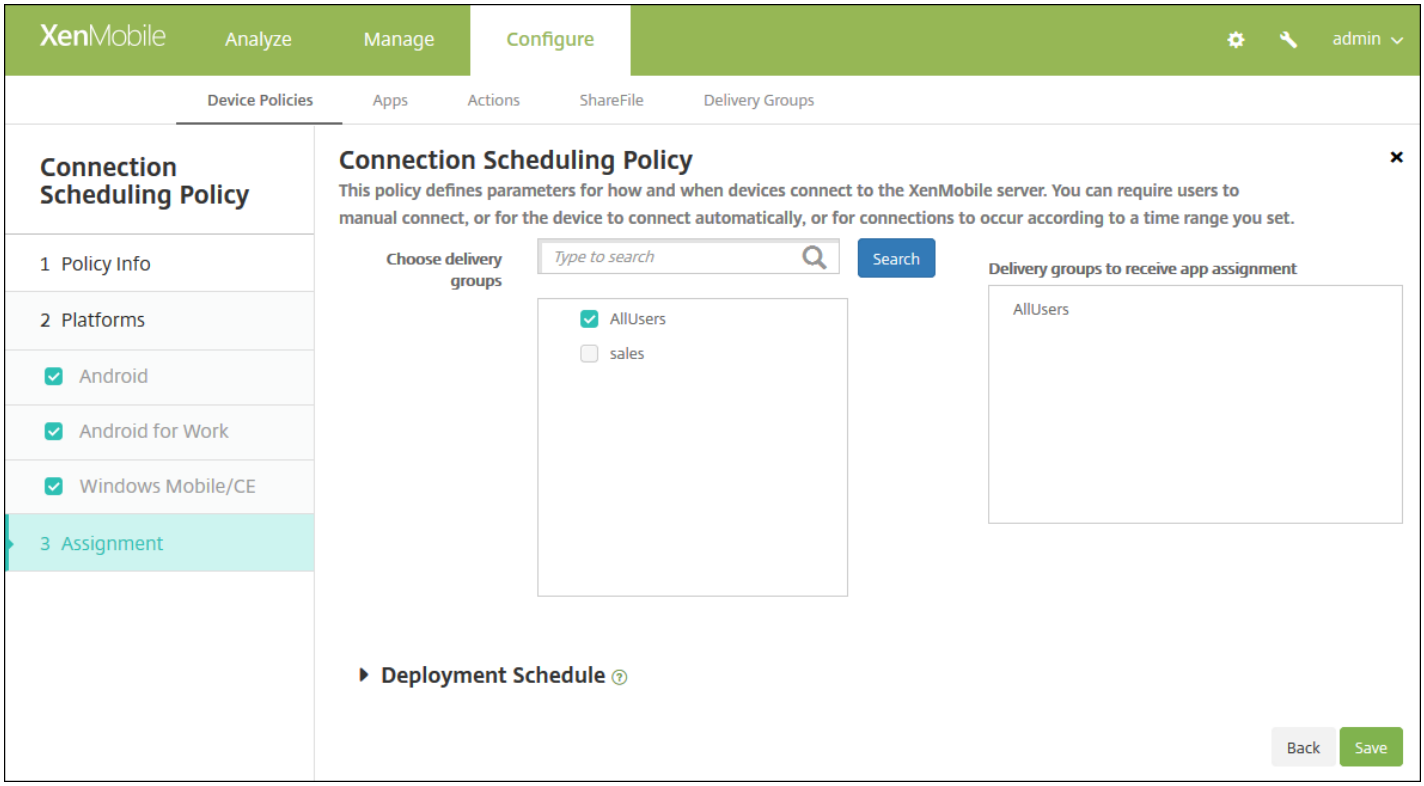
以下のオプションを有効にすると時間軸が表示されます。これを使用して必要な期間を定義できます。 特定の時間内に永続的な接続を必要とするオプション、または特定の期間内に1回の接続を必要とするオプションのいずれか、またはその両方を有効にできます。 時間軸の各四角は30分間であるため、毎平日の8:00 AM～9:00 AMに接続が必要な場合は、時間軸で毎平日の［8 AM］と［9 AM］の間の2つの四角をクリックします。

たとえば、次の図の2つの時間軸では、毎平日の8:00 AM～9:00 AMに永続的な接続、土曜日の12:00 AM～日曜日の1:00 AMに永続的な接続、毎平日の5:00 AM～8:00 AMまたは10:00 AM～11:00 PMに1回以上の接続が必要です。



8. 展開規則の構成

9. ［**Next**］をクリックします。 ［**Connection Scheduling Policy**］割り当てページが開きます。



10. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

11. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

12. **[Save]** をクリックします。

連絡先（CardDAV）デバイスポリシー

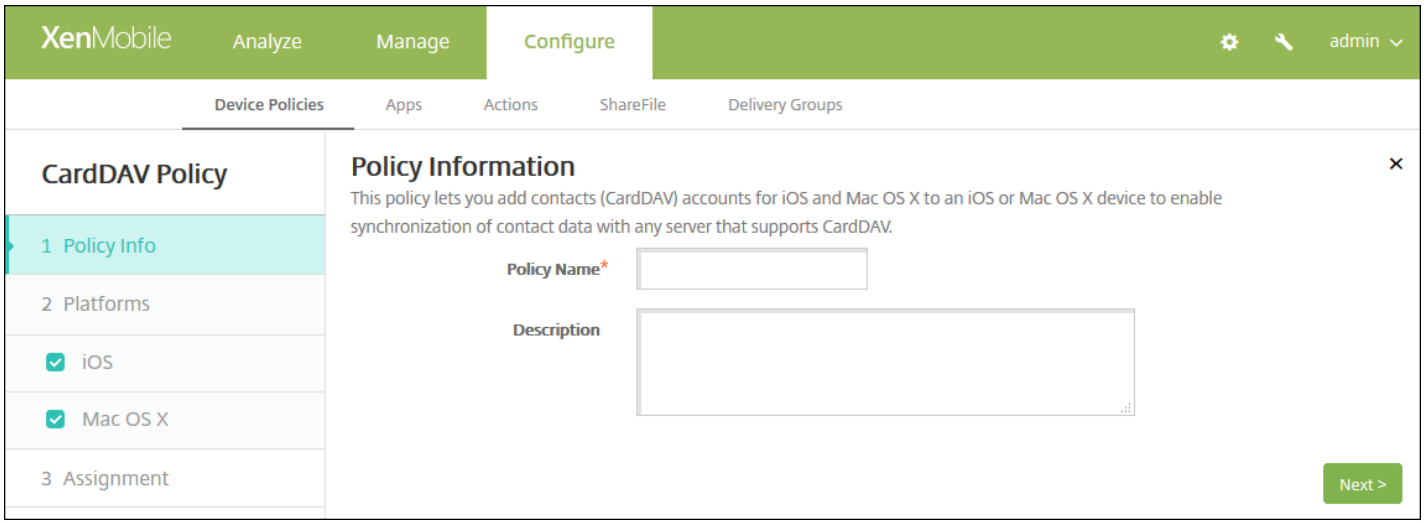
Aug 02, 2016

XenMobileでデバイスポリシーを追加して、iOS連絡先（CardDAV）アカウントをユーザーのiOSデバイスまたはMac OS Xデバイスに追加し、CardDAVをサポートするサーバーとそのデバイスの連絡先データを同期することができます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add a New Policy**］ダイアログボックスが開きます。

3.［**More**］を展開し、［**Security**］の下の［**Contacts CardDAV**］をクリックします。［**CardDAV Policy**］ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

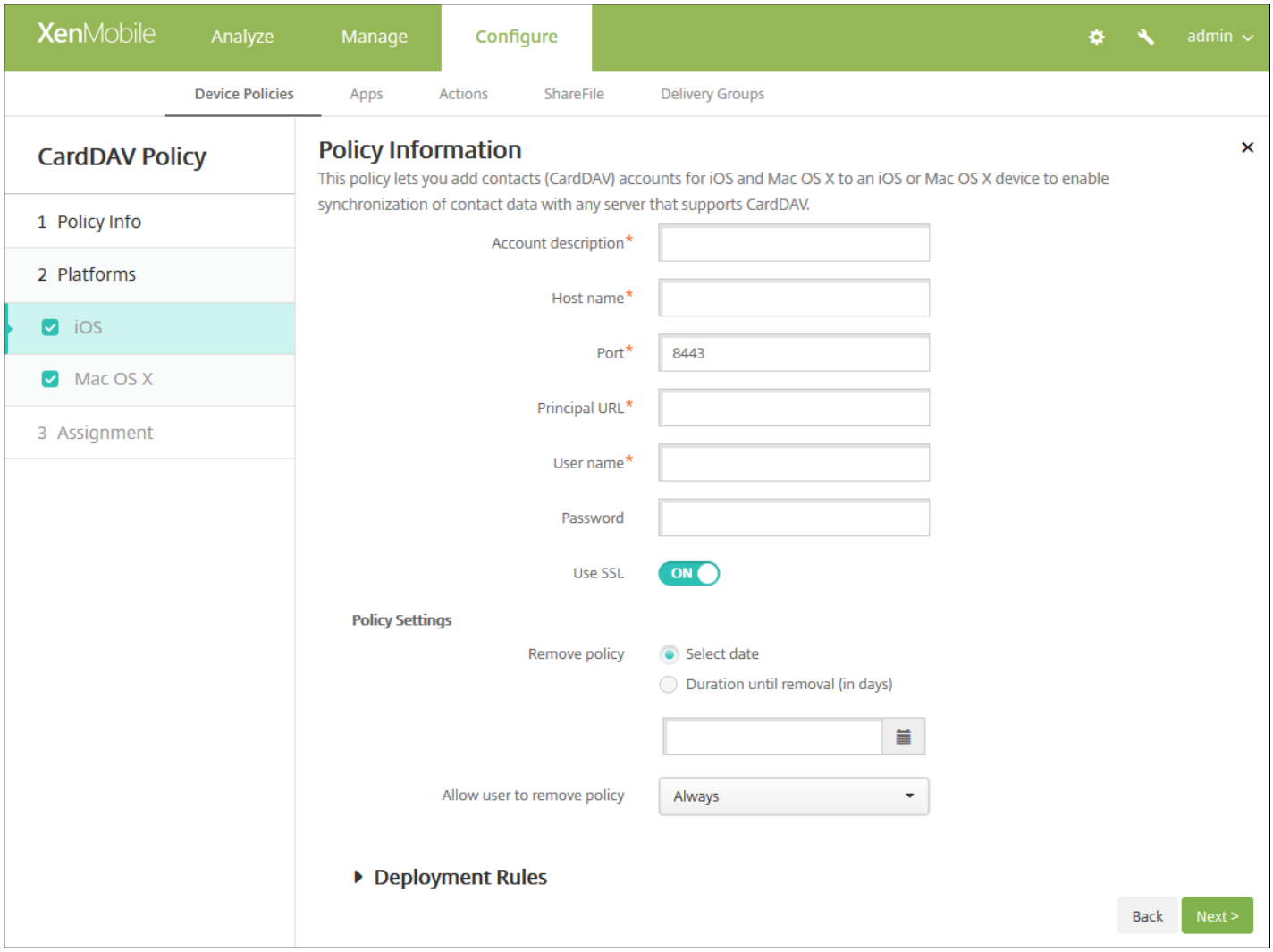
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Platforms**］ページが開きます。

6.［**Platforms**］の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

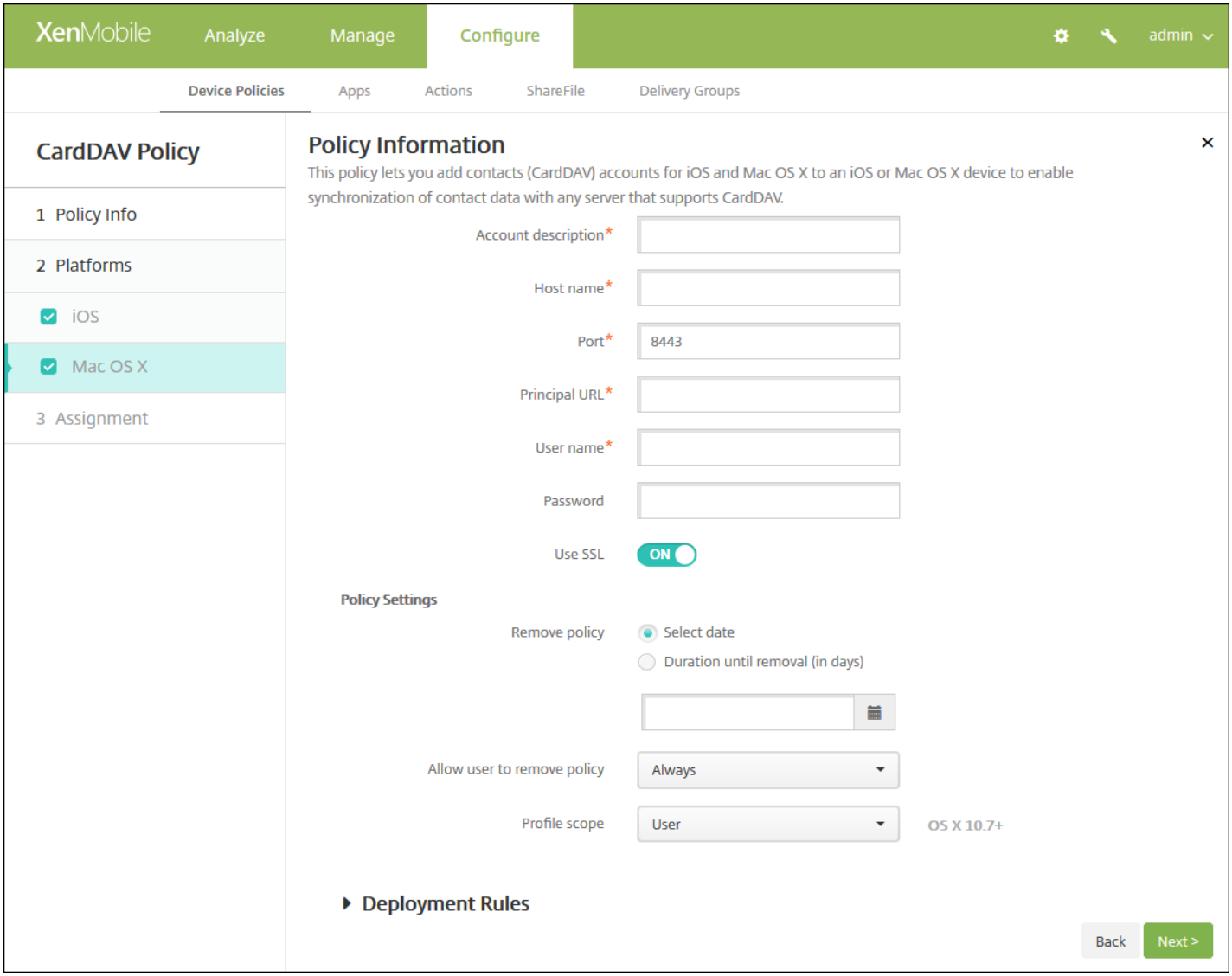
iOSの設定の構成



次の設定を構成します。

- **Account description**：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。
- **Host name**：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。
- **Port**：CardDAVサーバーへの接続用ポートを入力します。 このフィールドは必須です。 デフォルトは**8443**です。
- **Principal URL**：ユーザーのカレンダーに対するベースURLを入力します。
- **User name**：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。
- **Password**：任意で、ユーザーのパスワードを入力します。
- **Use SSL**：CardDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［**ON**］です。
- ポリシー設定
  - ［**Remove policy**］の横にある［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［Removal password］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



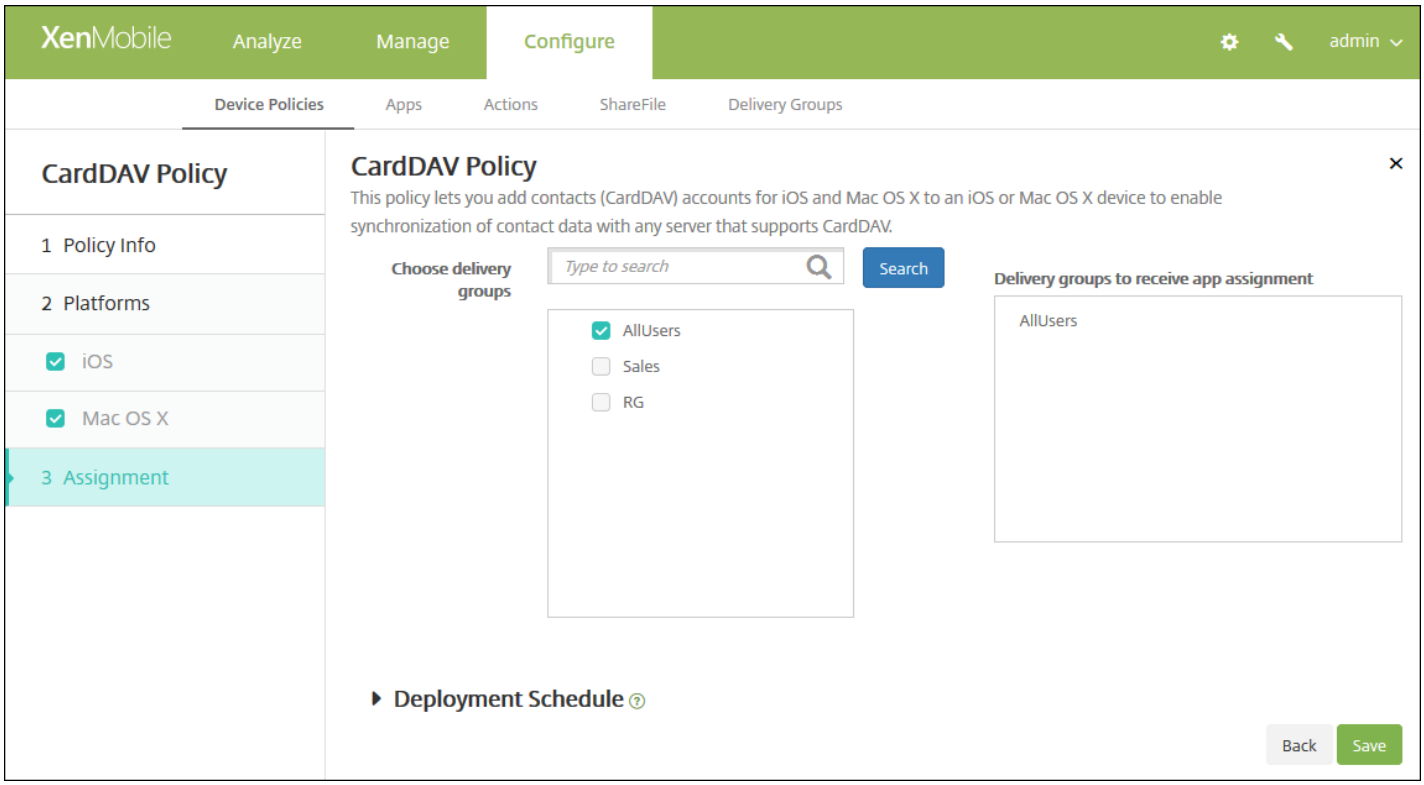
次の設定を構成します。

- **Account description**：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。
- **Host name**：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。
- **Port**：CardDAVサーバーへの接続用ポートを入力します。 このフィールドは必須です。 デフォルトは**8443**です。
- **Principal URL**：ユーザーのカレンダーに対するベースURLを入力します。
- **User name**：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。
- **Password**：任意で、ユーザーのパスワードを入力します。
- **Use SSL**：CardDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［**ON**］です。
- ポリシー設定
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［Removal password］の横に必要なパスワードを入力します。
  - ［**Profile scope**］の横にある、［**User**］または［**System**］を選択します。 デフォルトは［**User**］です。 このオプ

ションはOS X 10.7以降でのみ使用できます。

7. 展開規則を構成します。

8. [**Next**] をクリックします。 [**CardDAV Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. **[Save]** をクリックします。

Samsungコンテナーへのアプリケーションのコピーデバイスポリシー

Aug 02, 2016

デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナーまたはKNOXコンテナーにコピーされるように指定できます（サポートされるデバイスについて詳しくは、Samsung のSamsung KNOX Supported Devicesページを参照してください）。 SEAMSコンテナーにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナーにコピーされたアプリケーションは、ユーザーが KNOXコンテナーにログインする場合にのみ 使用できます。

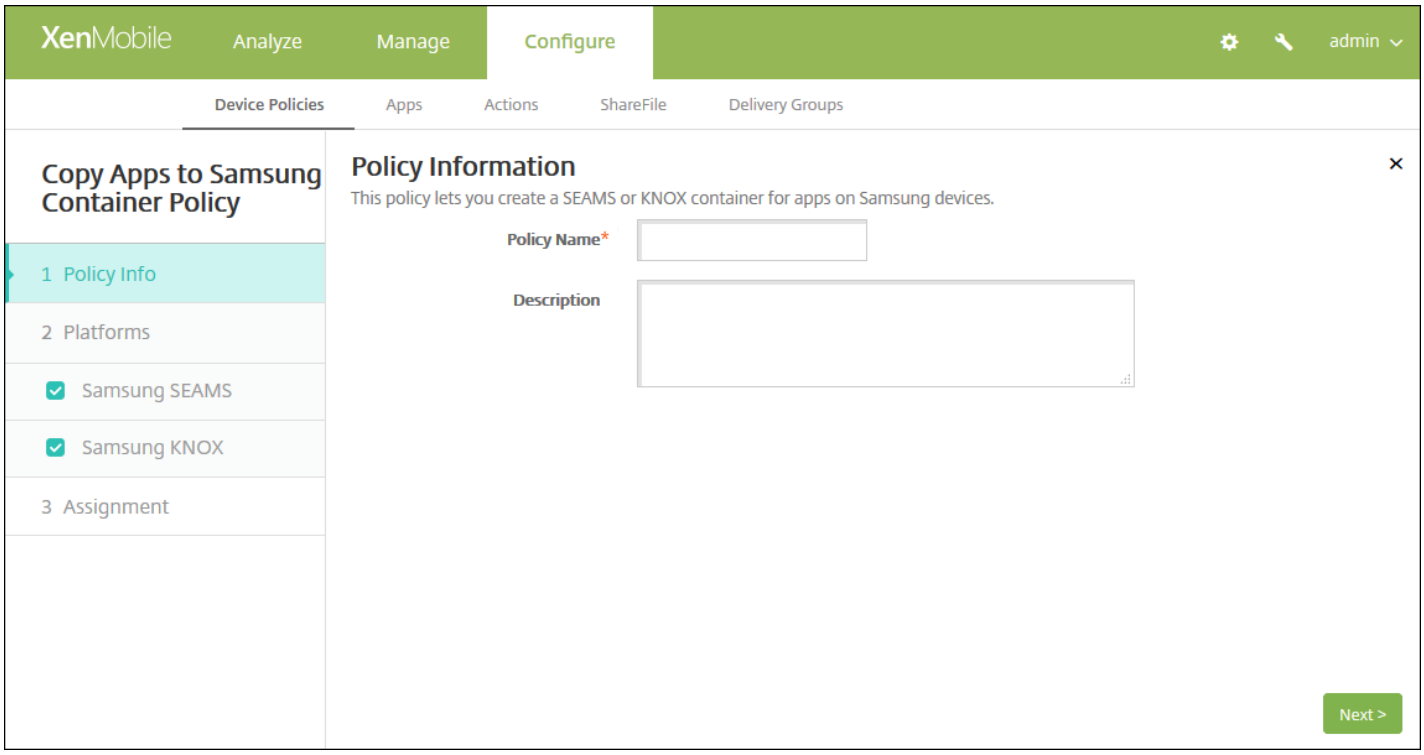
前提条件：

- デバイスをXenMobileに登録する必要があります。
- Samsung MDMキー（ELMおよびKLM）を展開する必要があります（展開方法について詳しくは、「Samsung MDMライセンスキーデバイスポリシー」を参照してください）。
- アプリケーションがデバイスにインストール済みである必要があります。
- デバイスでKNOXを初期化して、アプリケーションをKNOXコンテナーにコピーします。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

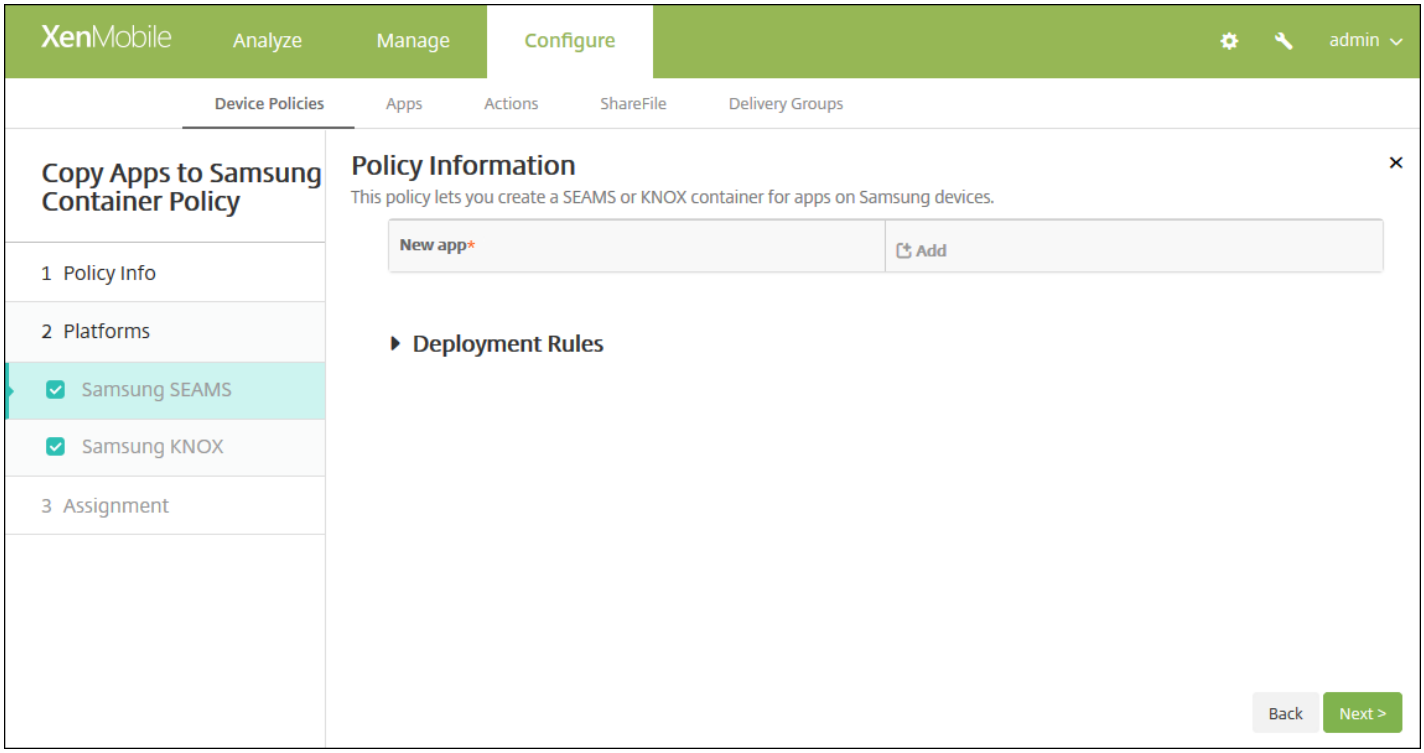
3. ［**More**］を展開し、 ［**Security**］の下の［**Copy Apps to Samsung Container**］をクリックします。 ［**Copy Apps to Samsung Container Policy**］情報ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. [Platforms] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順8.を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、次の設定を構成します。

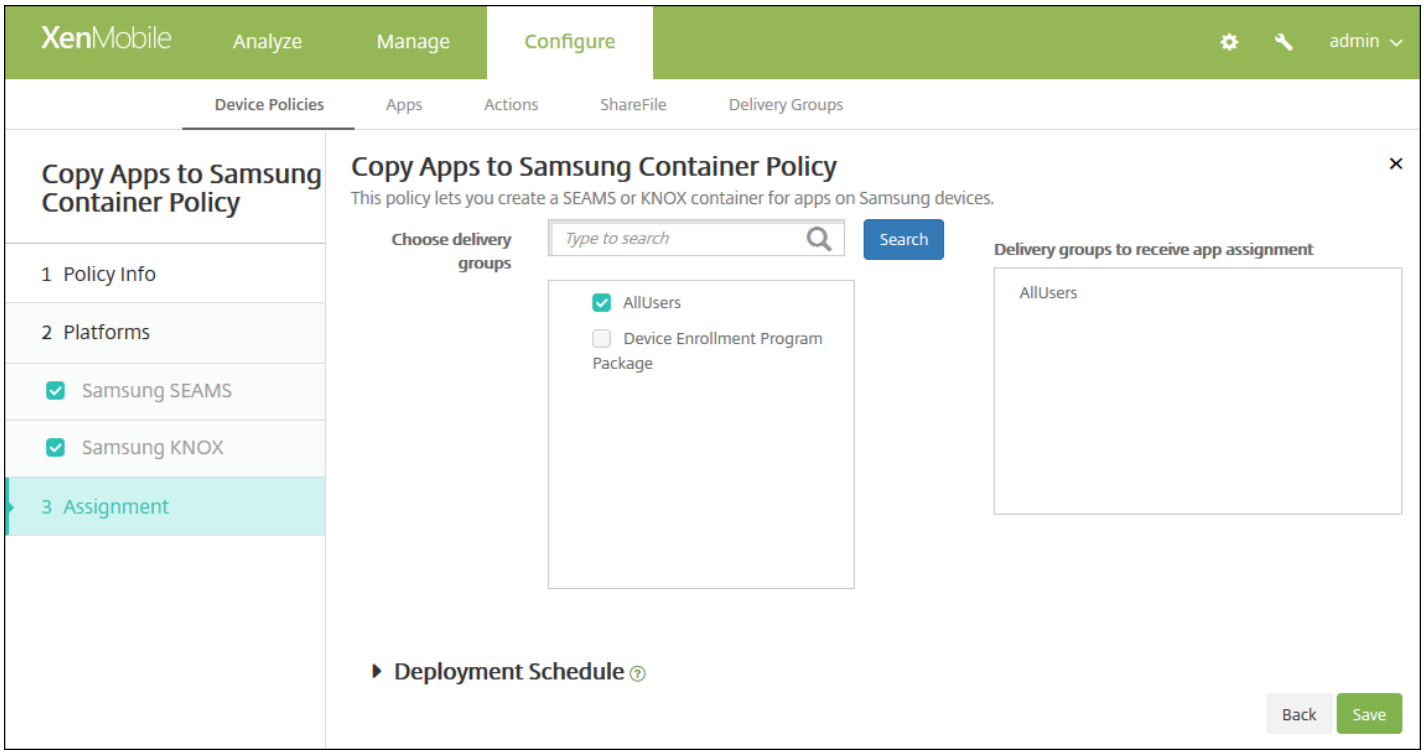
- **New app**：一覧に追加するアプリケーションごとに、**[Add]** をクリックして以下の操作を行います。
  - パッケージIDを入力します。たとえば、LacingArtアプリケーションの場合は 「com.mobiwolf.lacingart」と入力します。
  - **[Save]** または **[Cancel]** をクリックします。

  注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

  既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、 **[Save]** をクリックして変更した項目を保存するか、 **[Cancel]** をクリックして項目を変更せずそのままにします。

8. 展開規則の構成

8. **[Next]** をクリックします。 次のプラットフォームのページまたはポリシーの **[Copy Apps to Samsung Container Policy]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [Deploy for always on connection] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

ポリシーが正常に展開されると、SEAMSアプリケーションは [**Device details**] ページの見出し [**Location: Enterprise SEAMS Location**] の下に、KNOXアプリケーションは見出し [**Location: Enterprise Location**] の下に表示されます。

資格情報デバイスポリシー

Aug 02, 2016

XenMobileで資格情報デバイスポリシーを作成し、XenMobileのPKI構成（PKIエンティティ、キーストア、資格情報プロバイダー、サーバー証明書など）を使用した統合認証を有効にすることができます。 資格情報について詳しくは、「証明書」を参照してください。

資格情報ポリシーは、iOS、Mac OS X、Android、Android for Work、Windowsデスクトップ/タブレット、Windows Mobile/CE、Windows Phoneデバイスに対して作成できます。 プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

iOSの設定

Mac OS Xの設定

AndroidおよびAndroid for Workの設定

Windowsデスクトップ/タブレットの設定

Windows Mobile/CEの設定

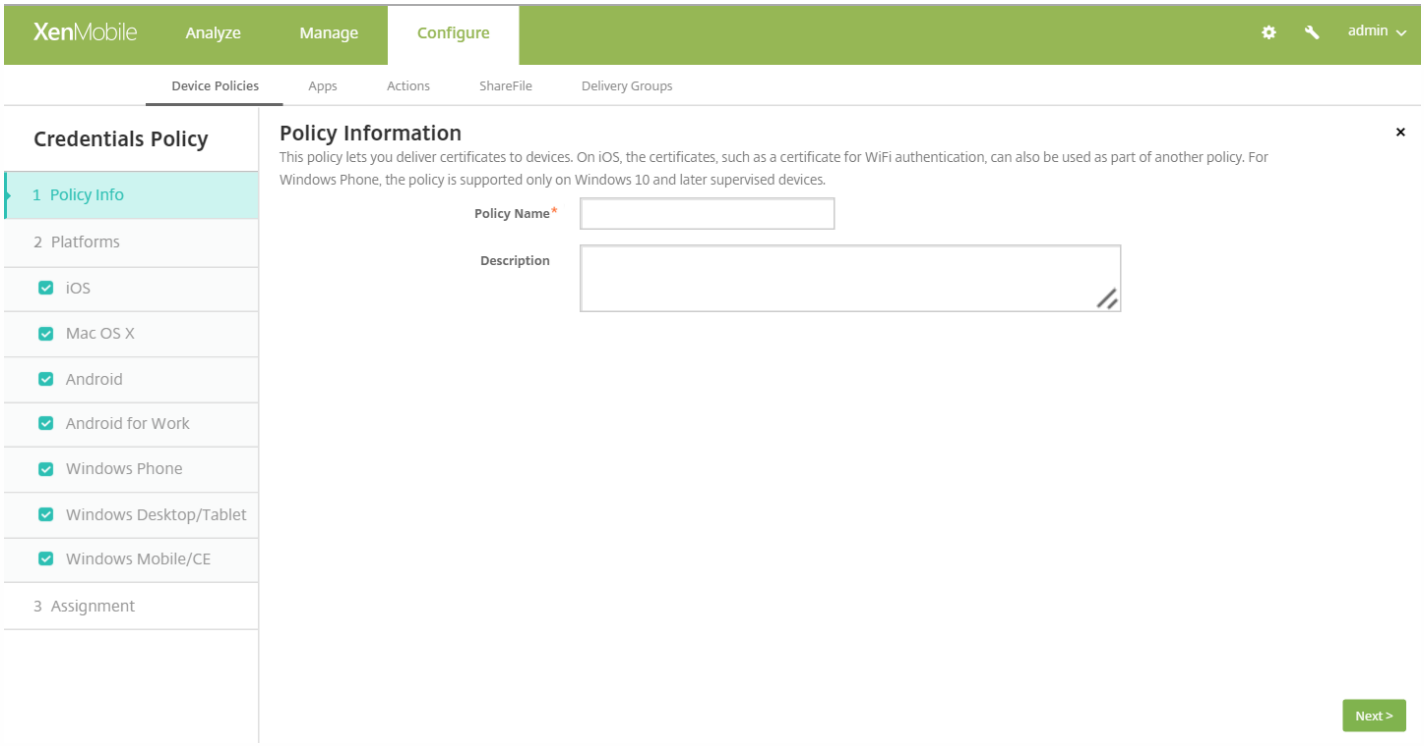
Windows Phoneの設定

このポリシーを作成するには、各プラットフォームで使用する予定の資格情報と、証明書およびパスワードが必要です。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add New Policy]** ダイアログボックスが開きます。

3. **[More]** を展開した後、 **[Security]** の下の **[Credentials]** をクリックします。 **[Credentials Policy]** 情報ページが開きます。



4. [**Policy Information**] ペインで、以下の情報を入力します。

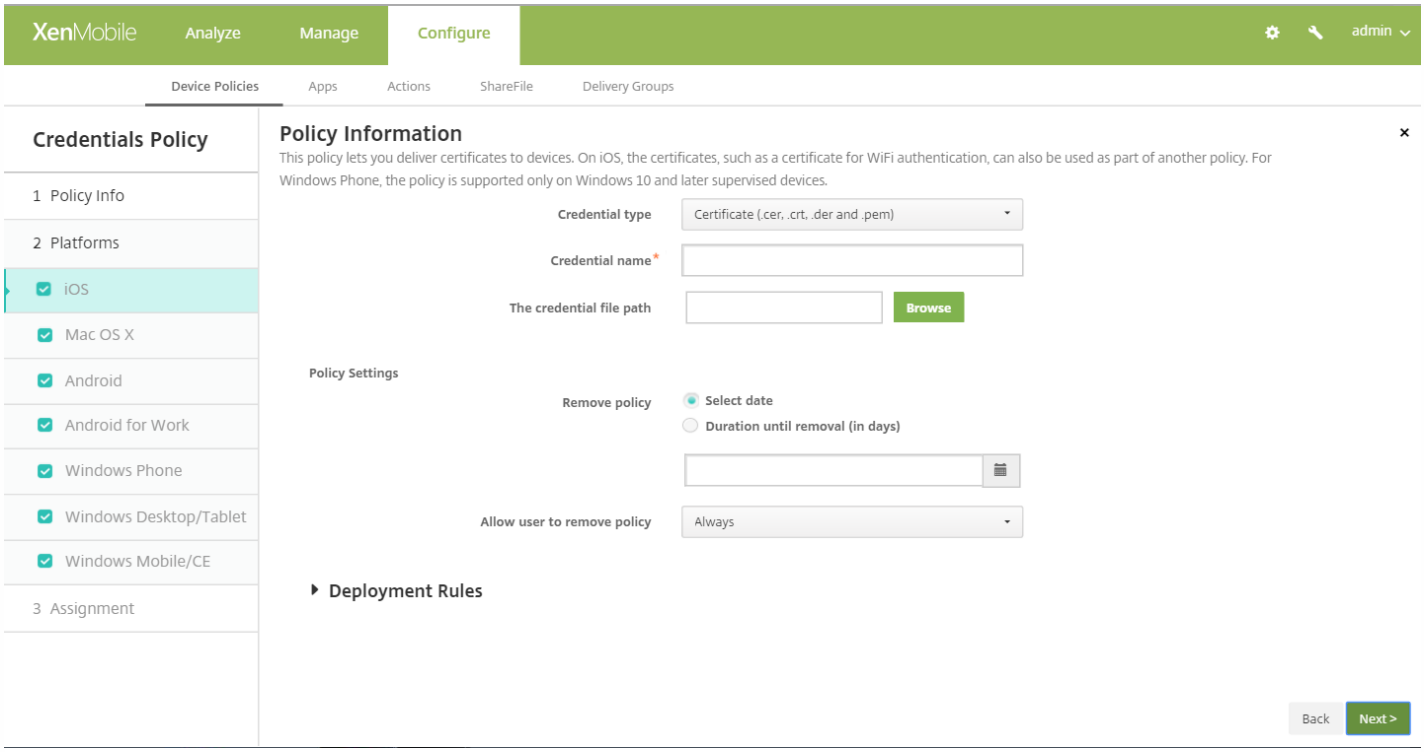
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Policy Platforms**] ページが開きます。

6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

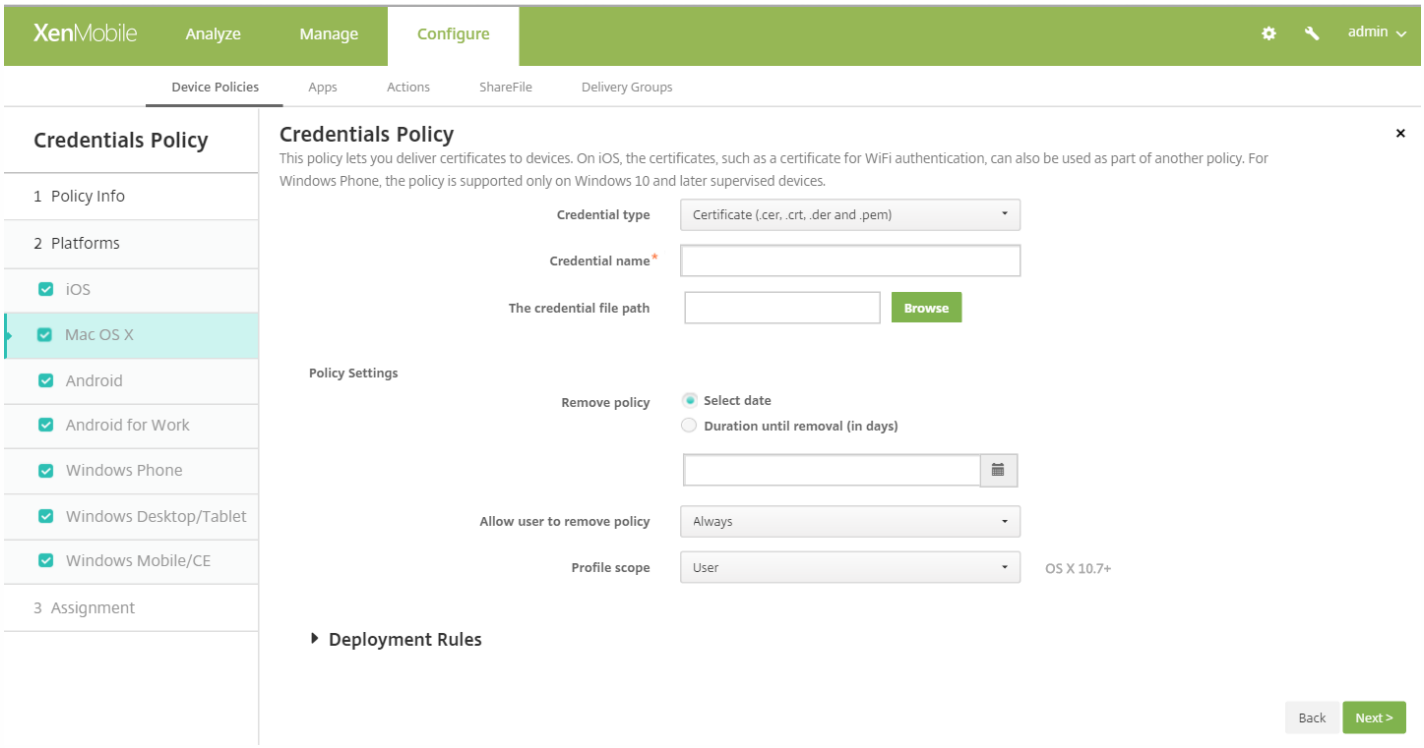
iOSの設定の構成



次の設定を構成します。

- **Credential type**：一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
  - **キーストア**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
    - **Password**：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**
    - **Server certificate**：ボックスの一覧で、使用する証明書を選択します。
  - **資格情報プロバイダー**
    - **Credential provider**：ボックスの一覧で、資格情報プロバイダーの名前を選択します。
- **ポリシー設定**
  - ［**Remove policy**］の横にある［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

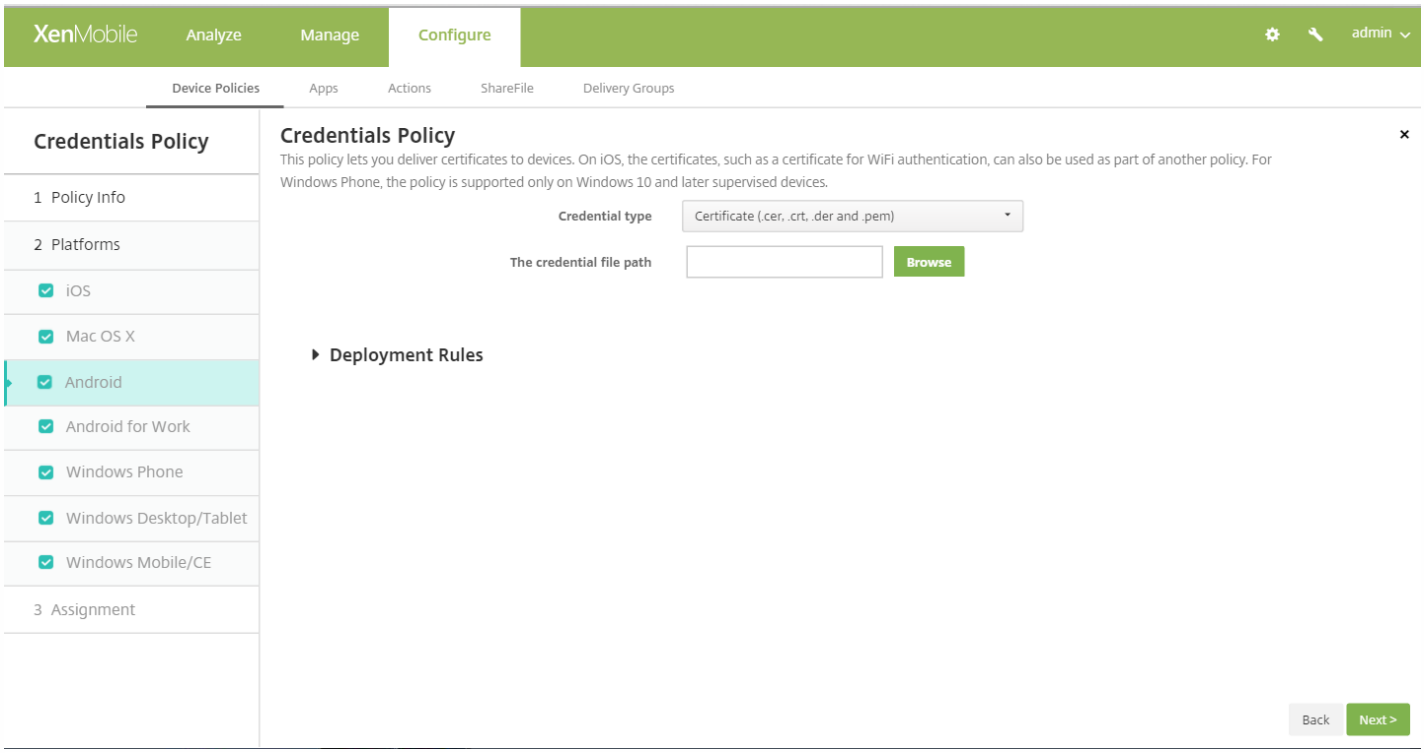
Mac OS Xの設定の構成



次の設定を構成します。

- **Credential type**：一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
  - **キーストア**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
    - **Password**：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**
    - **Server certificate**：ボックスの一覧で、使用する証明書を選択します。
  - **資格情報プロバイダー**
    - **Credential provider**：ボックスの一覧で、資格情報プロバイダーの名前を選択します。
- **ポリシー設定**
  - **［Remove policy］**の横の**［Select date］** または**［Duration until removal (in days)］**を選択します。
  - **［Select date］**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **［Allow user to remove policy］**の一覧で、**［Always］**、**［Password required］**、**［Never］**のいずれかを選択します。
  - **［Password required］**を選択した場合、**［Removal password］**の横に必要なパスワードを入力します。
  - **［Policy scope］**の横にある、**［User］**または**［System］**を選択します。デフォルトは**［User］**です。このオプションはOS X 10.7以降でのみ使用できます。

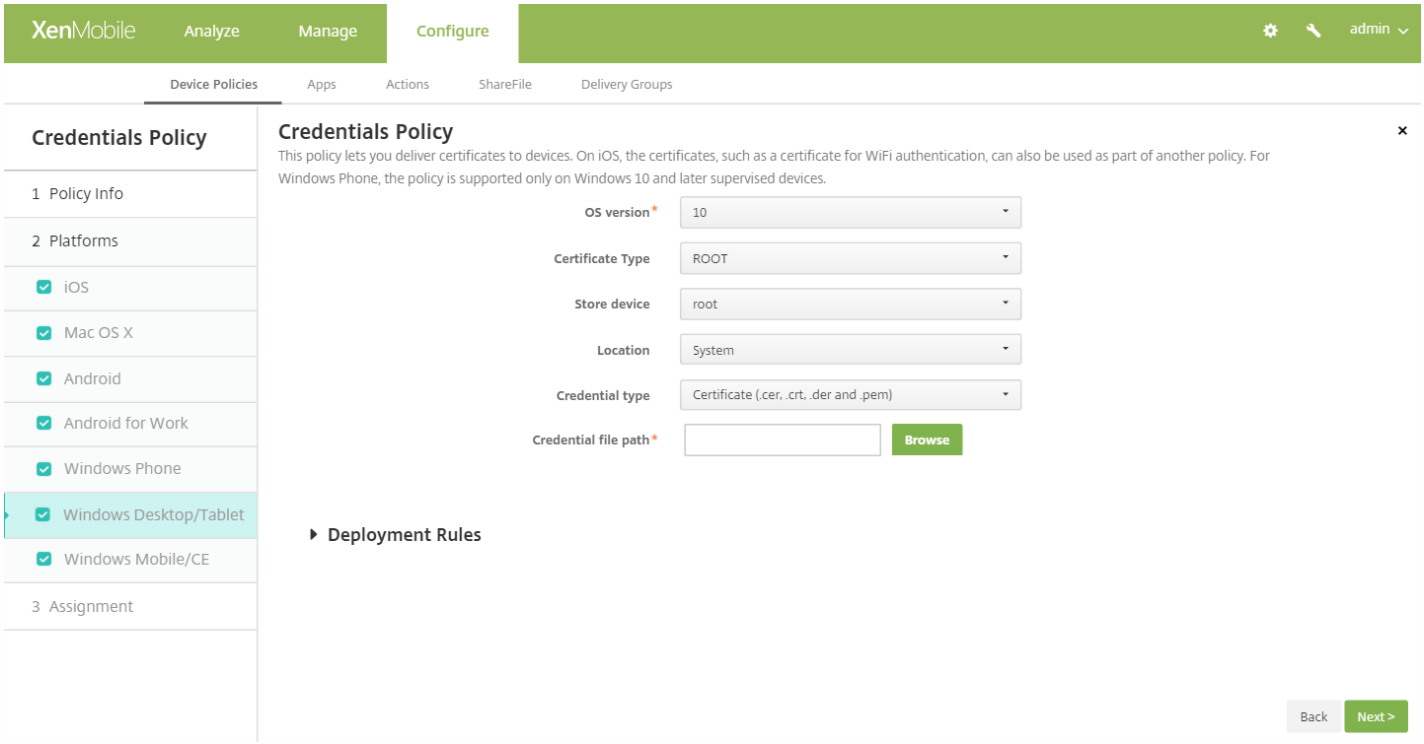
AndroidおよびAndroid for Workの設定の構成



次の設定を構成します。

- **Credential type**：一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
  - **キーストア**
    - **Credential name**：資格情報の固有の名前を入力します。
    - **The credential file path**：［Browse］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。
    - **Password**：キーストア パスワードを入力します。
  - **サーバー証明書**
    - **Server certificate**：ボックスの一覧で、使用する証明書を選択します。
  - **資格情報プロバイダー**
    - **Credential provider**：ボックスの一覧で、資格情報プロバイダーの名前を選択します。

Windowsデスクトップ/タブレットの設定の構成



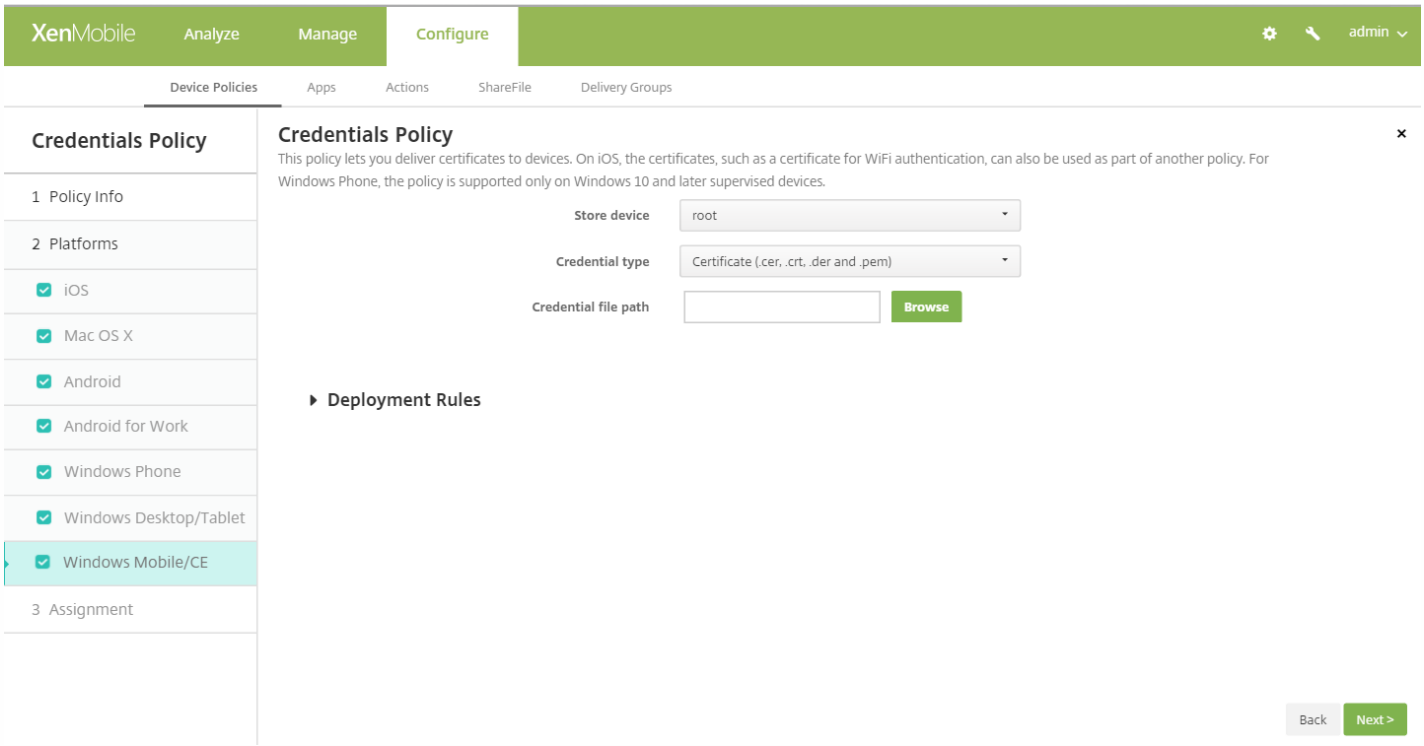
次の設定を構成します。

- **OSVersion**：一覧から、Windows 8.1の場合は［**8.1**］を、Windows 10の場合は［**10**］を選択します。 デフォルトは**10**です。

Windows 10の設定

Windows 8.1の設定

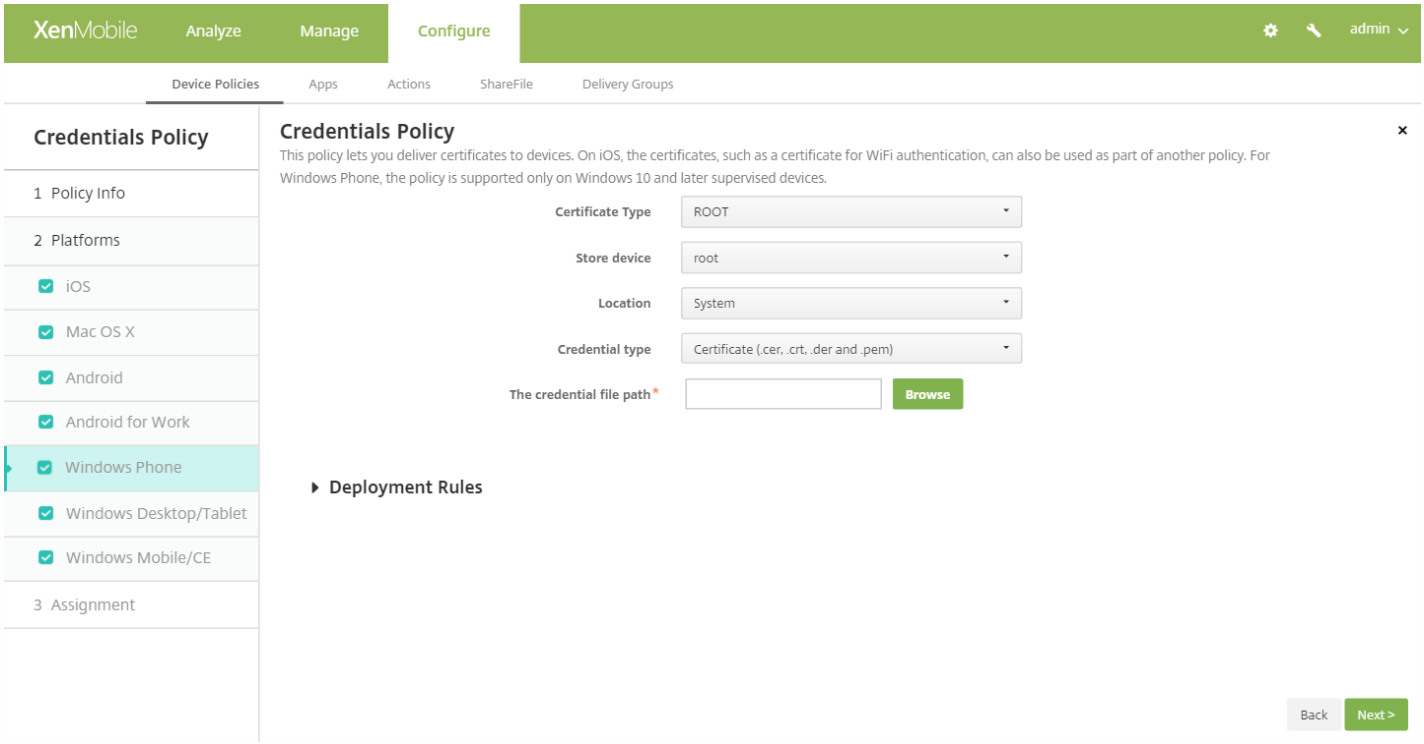
Windows Mobile/CEの設定の構成



次の設定を構成します。

- **Store device**：ボックスの一覧から、資格情報の証明書ストアの場所を選択します。 デフォルトは**[root]**です。 次のオプションがあります。
  - **Privileged execution trust authorities** - このストアに属する証明書で署名されたアプリケーションが、特権信頼レベルで実行されます。
  - **Unprivileged execution trust authorities** - このストアに属する証明書で署名されたアプリケーションが、標準信頼レベルで実行されます。
  - **SPC (Software Publisher Certificate)** - .cabファイルの署名にソフトウェア発行元証明書（SPC）が使用されます。
  - **root** - ルート証明書 または自己署名証明書を含む証明書ストア。
  - **CA** - 暗号化情報を含む証明書ストア（中間証明機関を含む）。
  - **MY** - エンドユーザーの個人証明書を含む証明書ストア。
- **Credential type**：Windows Mobile/CEデバイスの場合、資格情報の種類は証明書のみです。
- **The credential file path**： **[Browse]**をクリックして資格情報ファイルの場所に移動し、そのファイルを選択します。

Windows Phoneの設定の構成

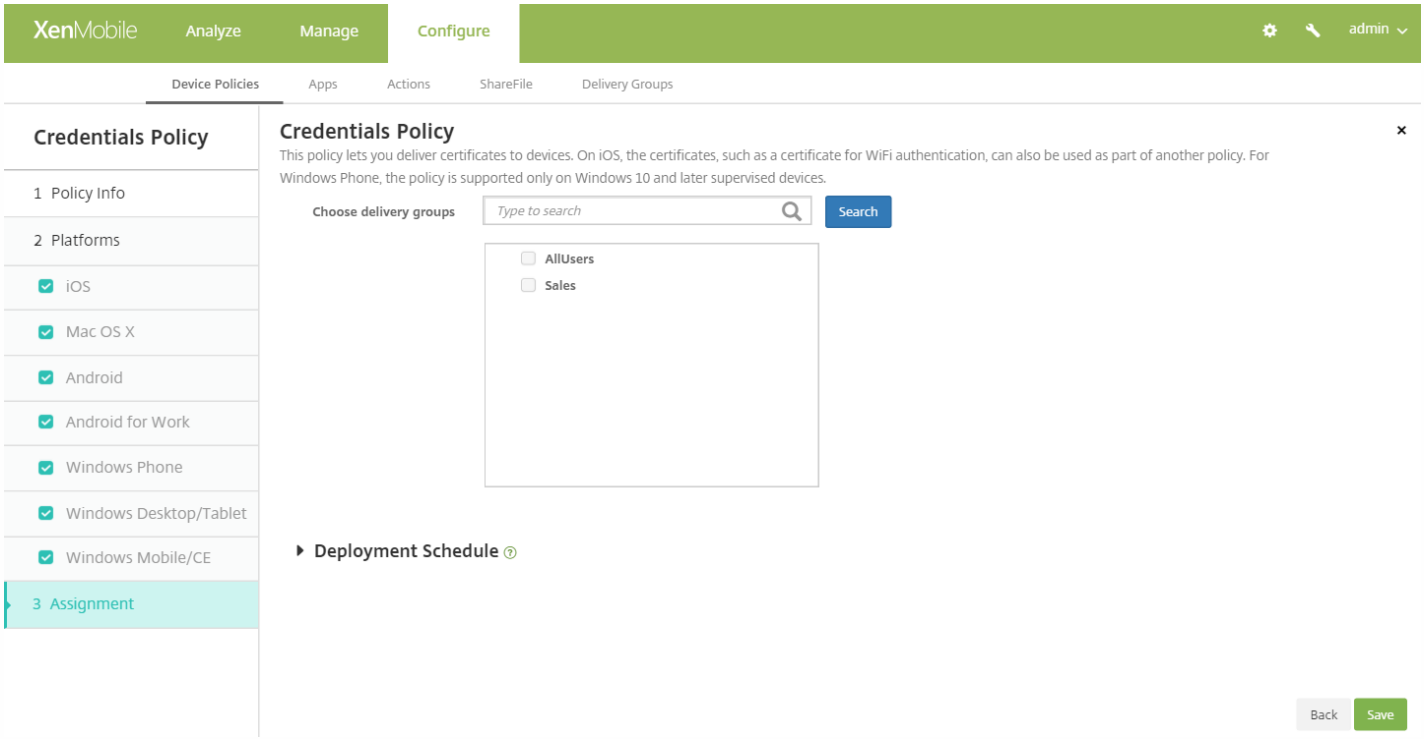


次の設定を構成します。

- **Certificate Type**：一覧から、［ROOT］または［CLIENT］を選択します。
- **［ROOT］**を選択した場合は、次の設定を構成します。
  - **Store device**：資格情報の証明書ストアの場所に応じて、ボックスの一覧で**［root］**、**［My］**、**［CA］**のいずれかを選択します。 **［My］**を選択すると、証明書はユーザーの証明書ストアに保存されます。
  - **Location**：Windows Phoneの場合、場所は［System］のみです。
  - **Credential type**：Windows Phoneの場合、資格情報の種類は証明書のみです。
  - **Credential file path**：**［Browse］**をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
- **［CLIENT］**を選択した場合は、次の設定を構成します。
  - **Location**：Windows Phoneの場合、場所は**［System］**のみです。
  - **Credential type**：Windows Phoneの場合、資格情報の種類は**キーストア**のみです。
  - **Credential name**：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。
  - **Credential file path**：［Browse］をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
  - **Password**：資格情報に関連付けられたパスワードを入力します。 このフィールドは必須です。

7. 展開規則の構成

8. **［Next］**をクリックします。 **［Credentials Policy］**割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

カスタムXMLデバイスポリシー

Aug 02, 2016

Windows Phone、Windowsデスクトップ/タブレット、Windows Mobile/CEデバイスの以下の機能をカスタマイズする場合、XenMobileでカスタムXMLポリシーを作成できます。

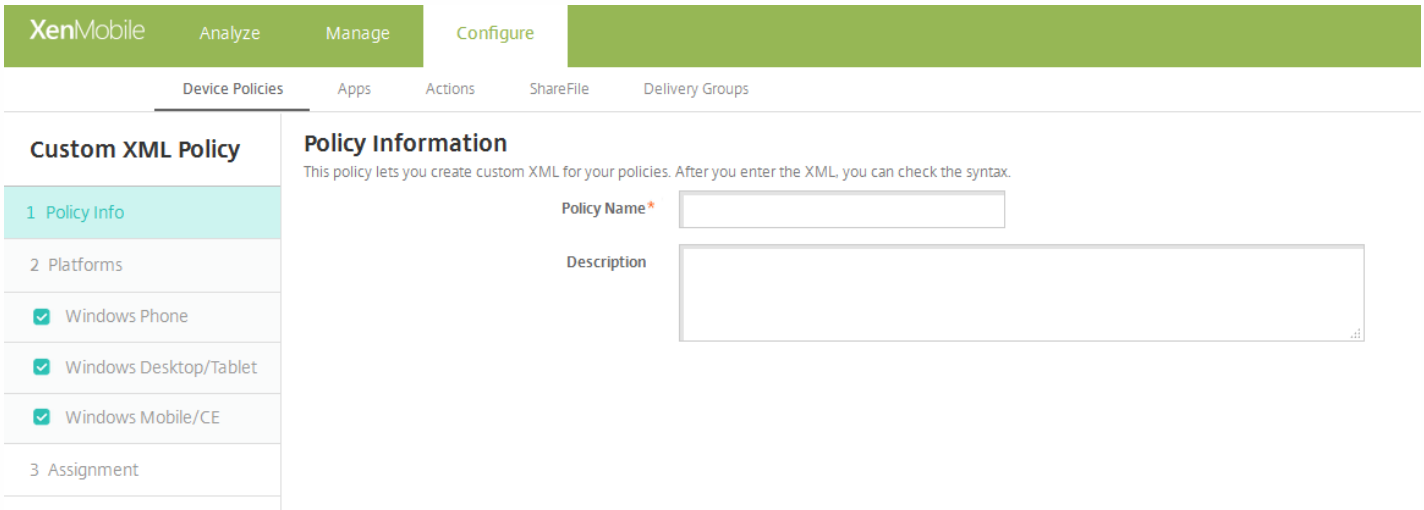
- プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。
- デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。
- ソフトウェアのアップグレード。アプリケーションやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。
- 障害管理。デバイスからのエラーおよび状態レポートの受信などです。

WindowsでOpen Mobile Alliance Device Management（OMA DM）APIを使用して、カスタムXML構成を作成します。 OMA DM APIを使用したカスタムXMLの 作成については、 このトピックでは扱いません。 OMA DM APIの使用について 詳しくは、 Microsoft Developer Networkサイトの「OMA Device Management」を参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add New Policy]** ダイアログボックスが開きます。

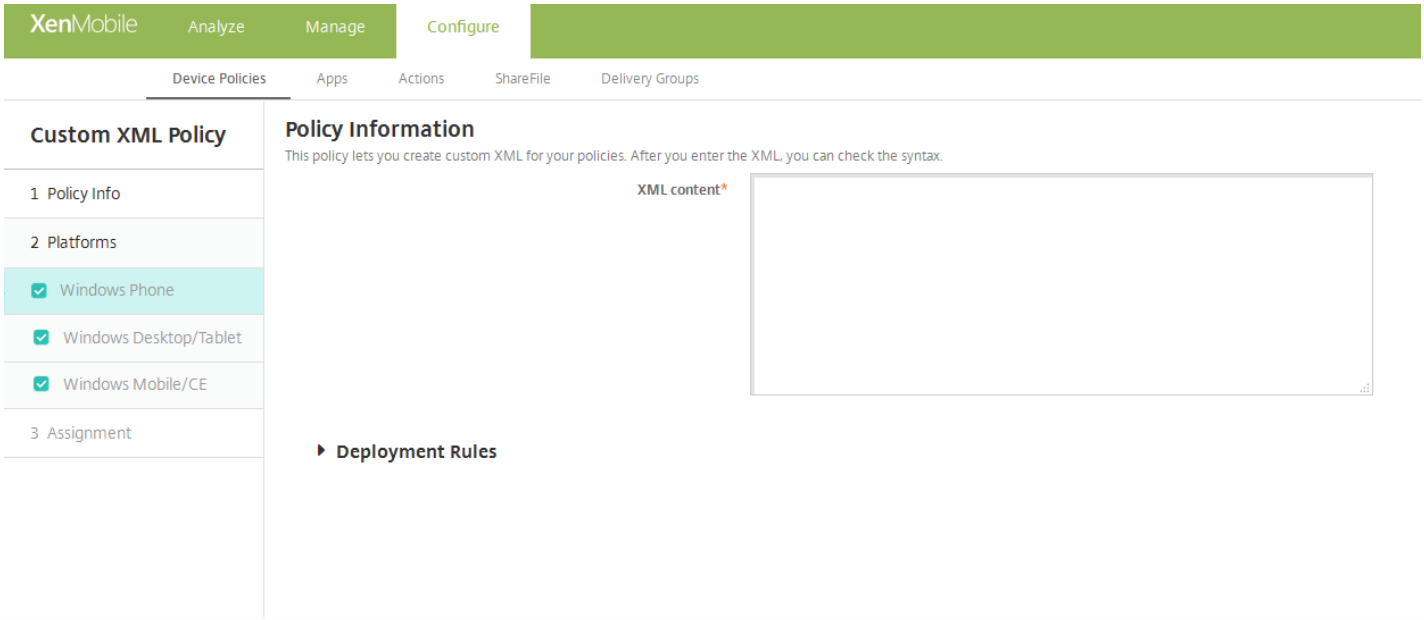
3. **[More]** を展開した後、 **[Custom]** の下の **[Custom XML]** をクリックします。 **[Custom XML Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

7. 選択したプラットフォームごとに、次の設定を構成します。

- [**XML content**] ：ポリシーに追加するカスタムXMLコードを入力するか、コピーして貼り付けます。

8. 展開規則の構成

9. [**Next**] をクリックします。 XenMobileでXMLコンテンツの構文がチェックされます。 構文エラーがある場合、コンテンツボックスの下に表示されます。 続行するにはエラーを修正する必要があります。

構文エラーがない場合は、 [**Custom XML Policy**] 割り当てページが開きます。

[**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

11. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。

- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。

12. **[Save]** をクリックします。

ファイルおよびフォルダーの削除デバイスポリシー

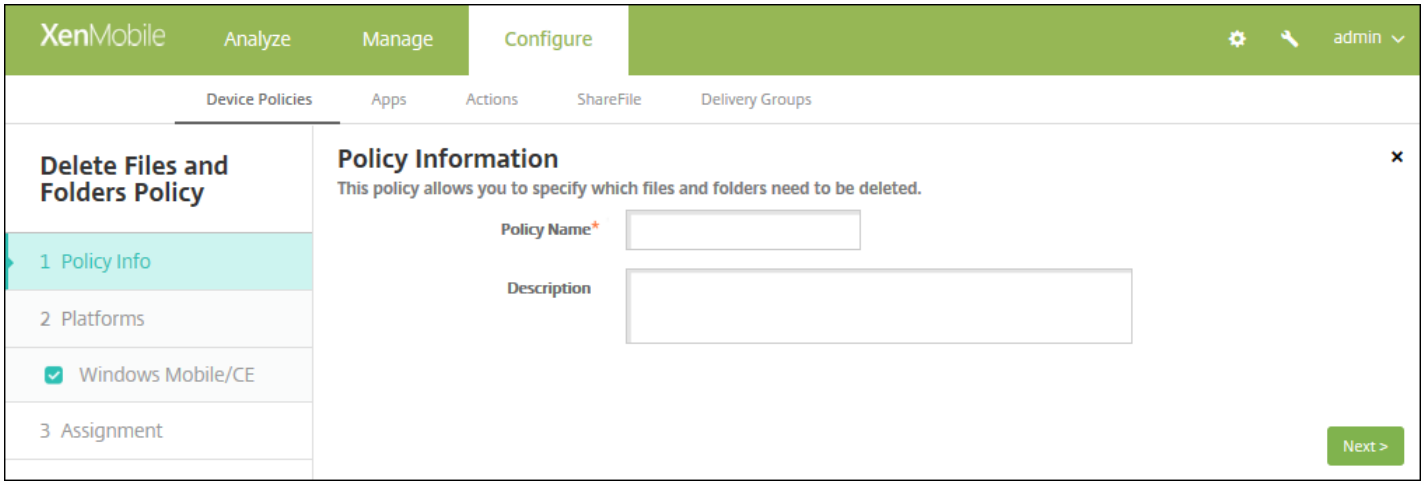
Aug 02, 2016

XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のファイルまたはフォルダーを削除できます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add New Policy**］ダイアログボックスが開きます。

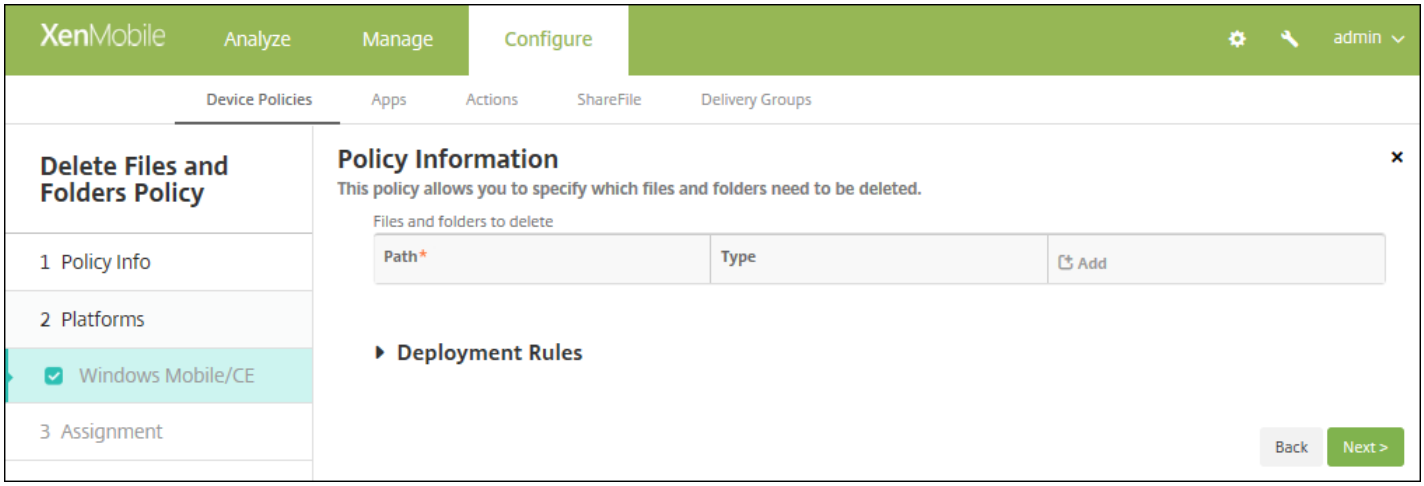
3.［**More**］を展開し、［**Apps**］で［**Delete Files and Folders**］をクリックします。［**Delete Files and Folders Policy**］情報ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Windows Mobile/CE Platform**］ページが開きます。



6. 次の設定を構成します。

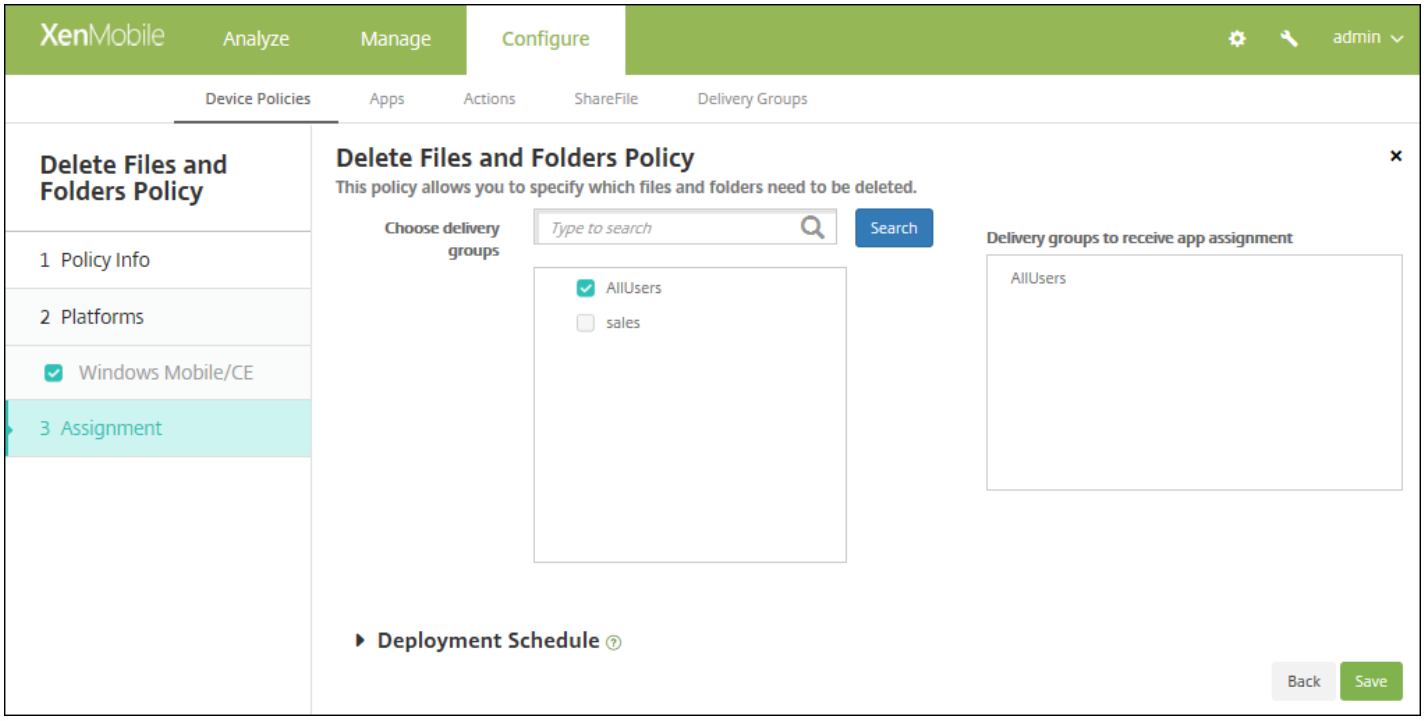
- **Files and folders to delete**：削除するファイルまたはフォルダーごとに、［Add］をクリックして以下の操作を行います。
  - **Path**：ファイルまたはフォルダーまでのパスを入力します。
  - **Type**：一覧から、［File］または［Folder］を選択します。 デフォルトは［File］です。
  - ［**Save**］をクリックしてファイルまたはフォルダーを保存するか、［**Cancel**］をクリックして操作を取り消します。

    注：既存の項目を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

    既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Delete Files and Folders Policy**］割り当てページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。

- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

レジストリキーおよび値デバイスポリシーの削除

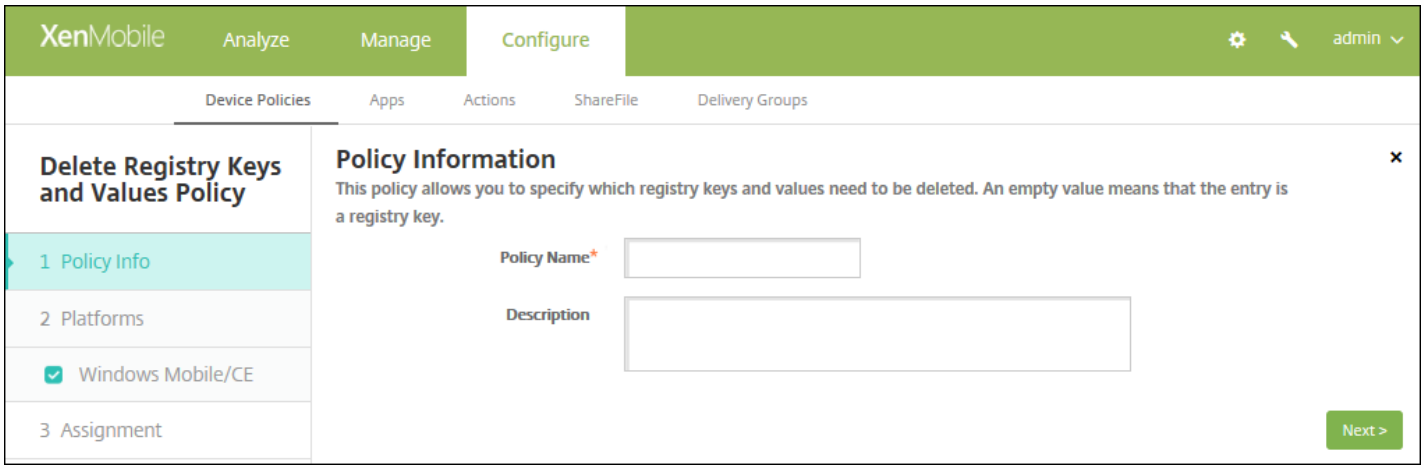
Aug 02, 2016

XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のレジストリキーおよび値を削除することができます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add New Policy**］ダイアログボックスが開きます。

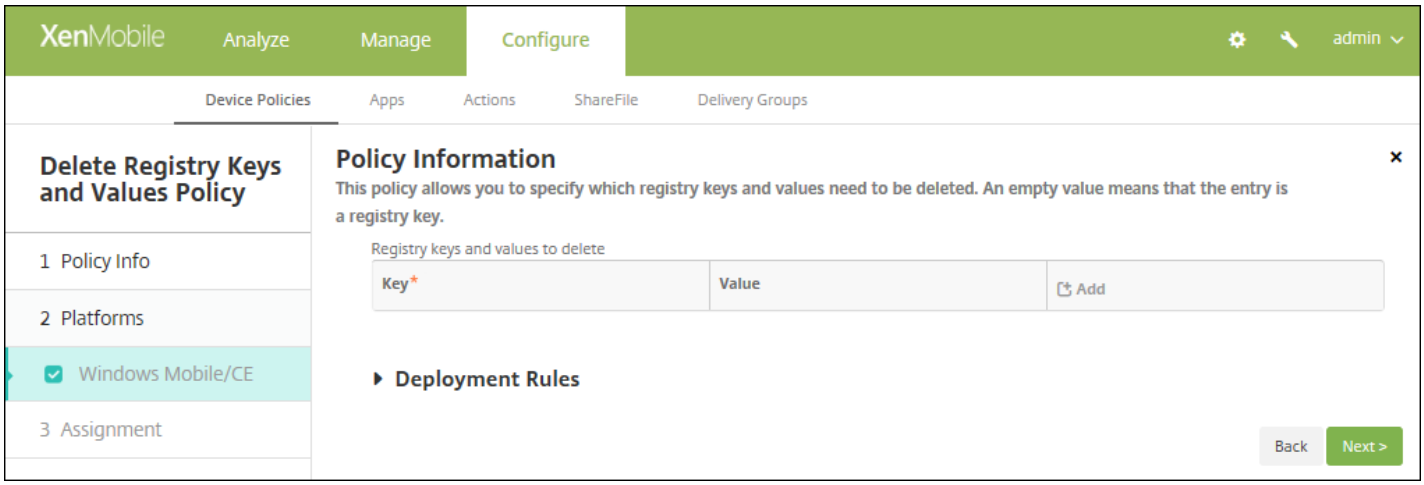
3.［**More**］を展開した後、［**Apps**］の下の［**Delete Registry Keys and Values**］をクリックします。［**Delete Registry Keys and Values Policy**］情報ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Windows Mobile/CE Platform**］ページが開きます。



6. 次の設定を構成します。

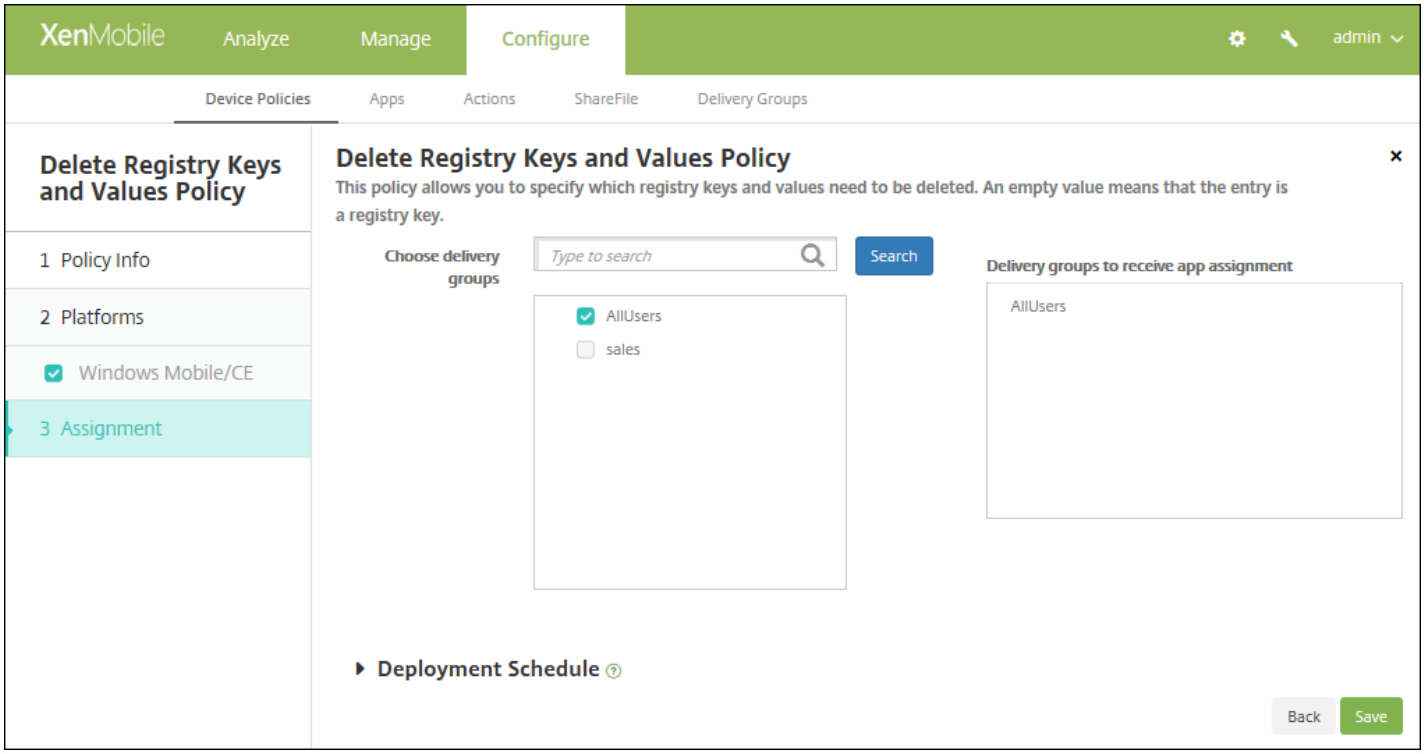
- **Registry keys and values to delete**：削除するレジストリキーおよび値ごとに、［**Add**］をクリックして以下の操作を行います。
  - **Key**：レジストリキーのパスを入力します。 これは必須フィールドです。レジストリキーのパスは、HKEY_CLASSES_ROOT\、HKEY_CURRENT_USER\、HKEY_LOCAL_MACHINE\、またはHKEY_USERS\で始まる必要があります。
  - **Value**：削除する値の名前を入力します。または、レジストリキー全体を削除する場合は、このフィールドを空白のままにします。
  - ［**Save**］をクリックしてキーおよび値を保存するか、［**Cancel**］をクリックして操作を取り消します。

  注：既存の項目を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

  既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

7. 展開規則を構成します。

8. ［**Next**］をクリックします。 ［**Delete Registry Keys and Values Policy**］割り当てページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。

デフォルトのオプションは［**ON**］です。［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。

- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

11. ［**Save**］をクリックします。

デバイス正常性構成証明デバイスポリシー

Aug 02, 2016

XenMobileでは、分析目的で特定のデータおよびランタイム情報をHealth Attestation Service（HAS）に送信させ、Windows 10デバイスに正常性状態を報告させることができます。 HASは、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスからXenMobileに送信されます。 XenMobileは正常性構成証明書を受信すると、その内容に基づいて、管理者が以前に設定した自動アクションを展開します。

HASによって検証されるデータは以下のとおりです。

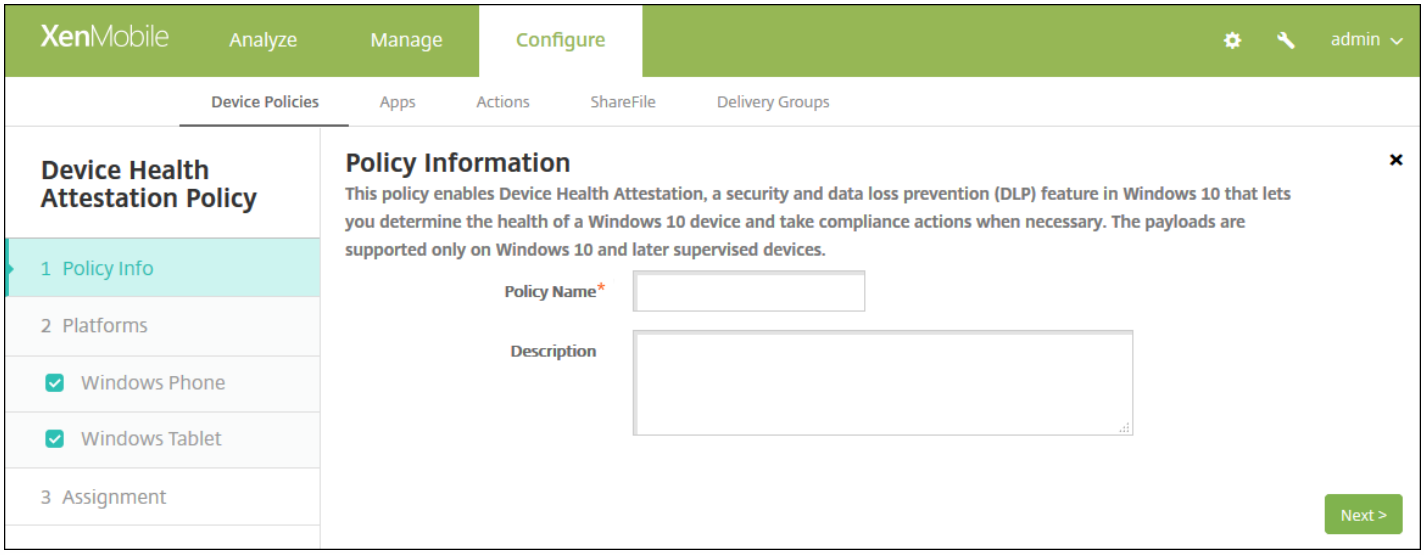
- AIKの有無
- Bit Lockerの状態
- ブートデバッグが有効化されているかどうか
- ブートマネージャーのバージョン
- コードの整合性チェックが有効化されているかどうか
- コード整合性のバージョン
- DEP ポリシー
- ELAMドライバーが起動されているかどうか
- 発行元
- カーネルのデバッグが有効化されているかどうか
- PCR
- リセット回数
- 再起動の回数
- セーフモードが有効化されているかどうか
- SBCPハッシュ
- セキュアブートが有効化されているかどうか
- テスト署名が有効化されているかどうか
- VSMが有効であること。
- WinPEが有効であること。

詳しくは、MicrosoftのHealthAttestation CSPページを参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2.新しいポリシーを追加するために **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** をクリックした後、 **[Custom]** の下の **[Device Health Attestation Policy]** をクリックします。 **[Device Health Attestation Policy]** 情報ページが開きます。



4. [**Policy Information**] ペインで、以下の情報を入力します。

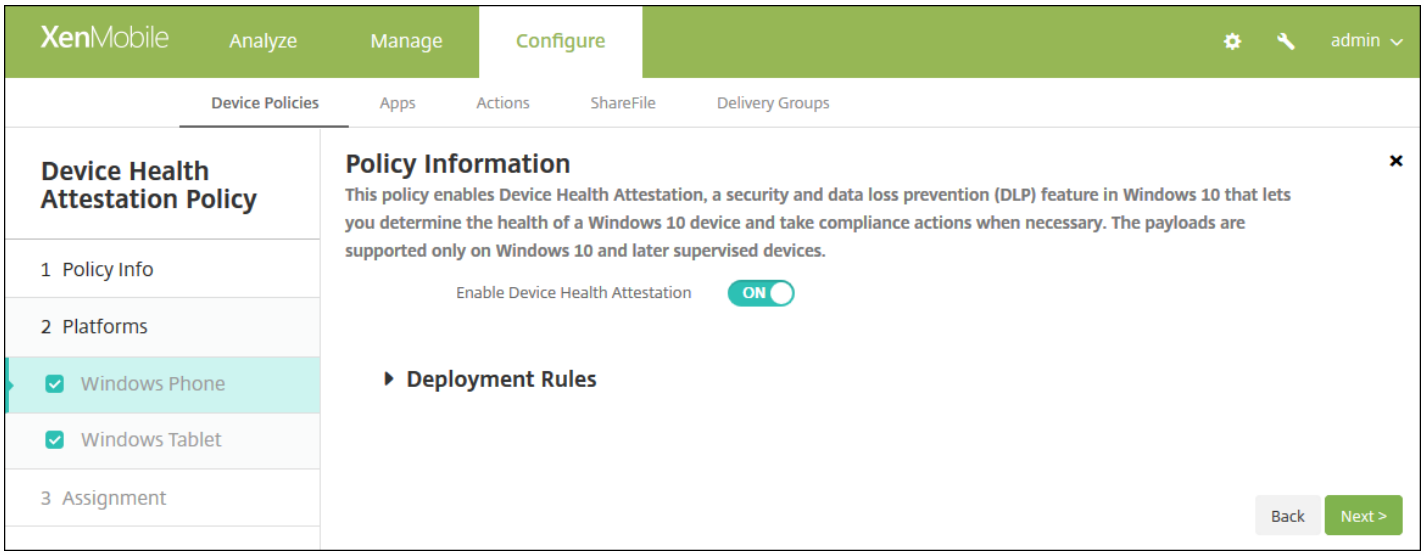
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Policy Platforms**] ページが開きます。

6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

Windows PhoneおよびWindowsタブレットの設定の構成

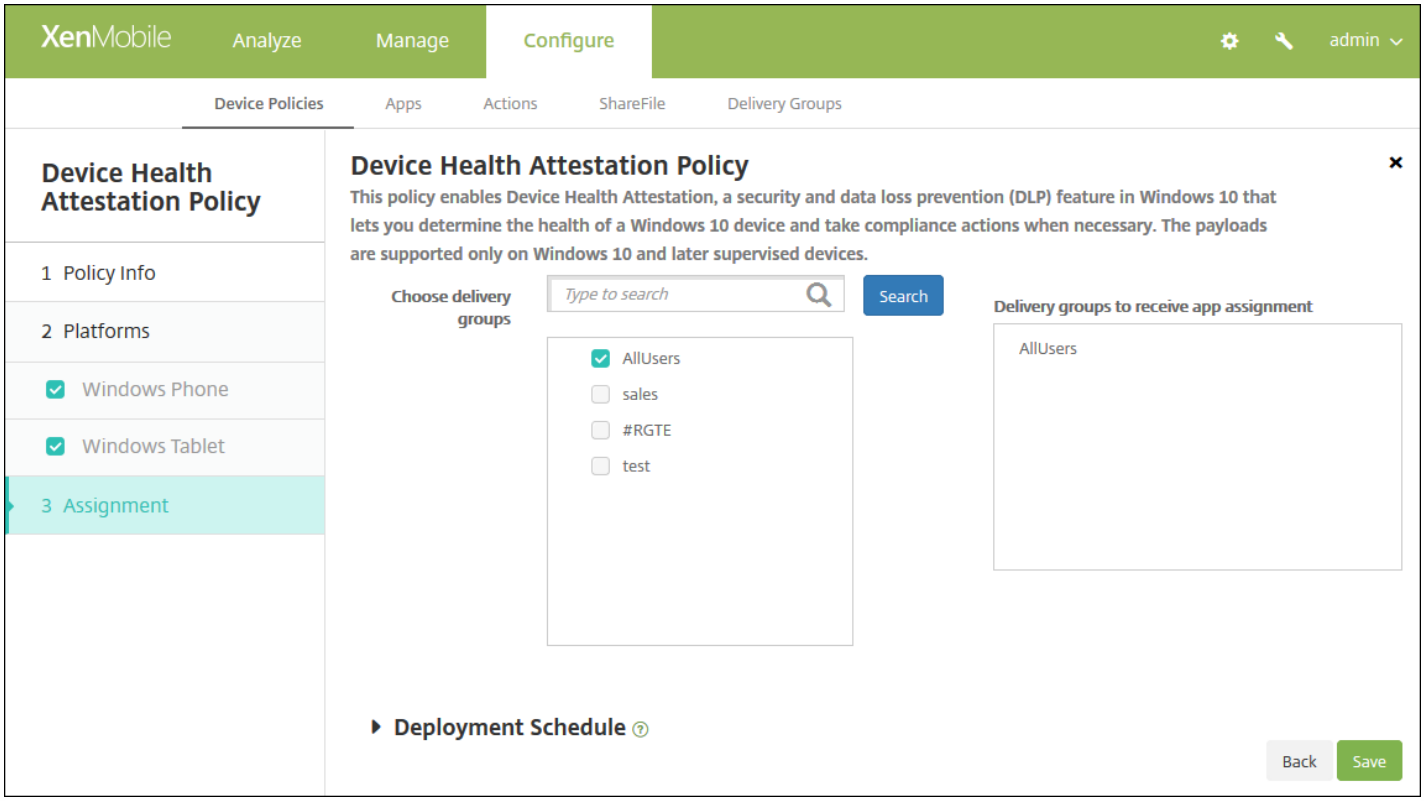


選択したプラットフォームごとに、次の設定を構成します。

- **Enable Device Health Attestation Policy**：デバイス正常性構成証明を必須とするかどうかを選択します。 デフォルトは [**OFF**] です。

7. 展開規則の構成

8. [**Next**] をクリックします。 [**Device Health Attestation Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. **[Save]** をクリックします。

デバイス名デバイスポリシー

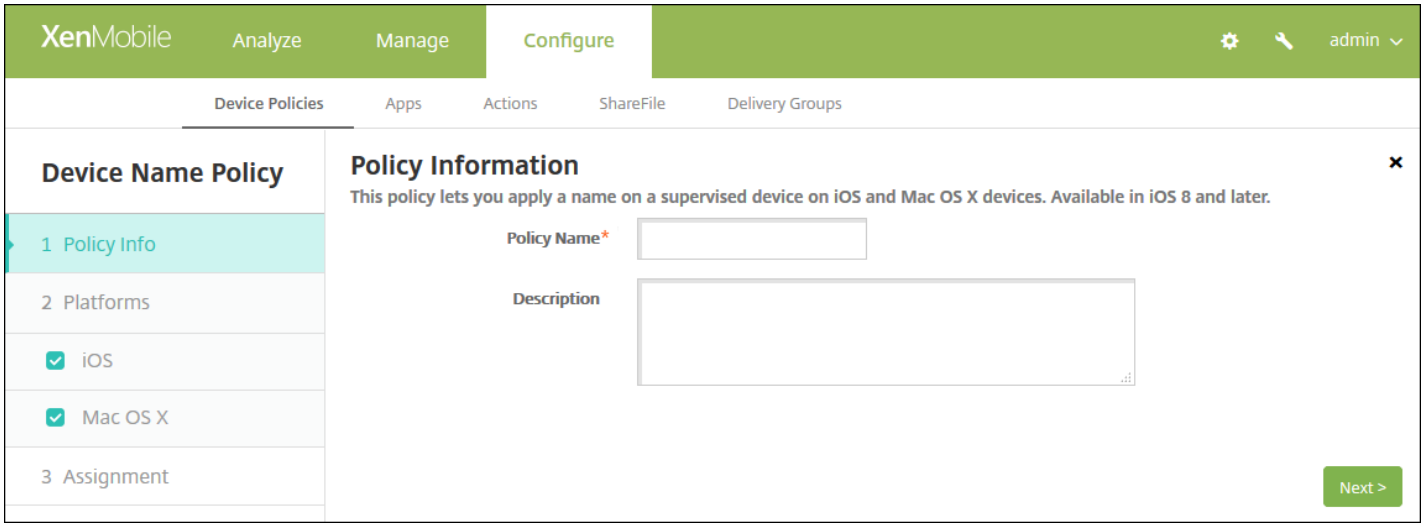
Aug 02, 2016

デバイスを特定しやすくするために、iOSデバイスおよびMac OS Xデバイスに 名前 を設定できます。 デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。 たとえば、デバイス名をデバイスのシリアル号として設定するには、${device.serialnumber}を使用します。 デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.comを使用します。 マクロについて詳しくは、「XenMobileのマクロ」を参照してください。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ページが開きます。

3. ［**More**］を展開した後、［**End user**］の下の［**Device Name**］をクリックします。 ［**Device Name Policy**］情報ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

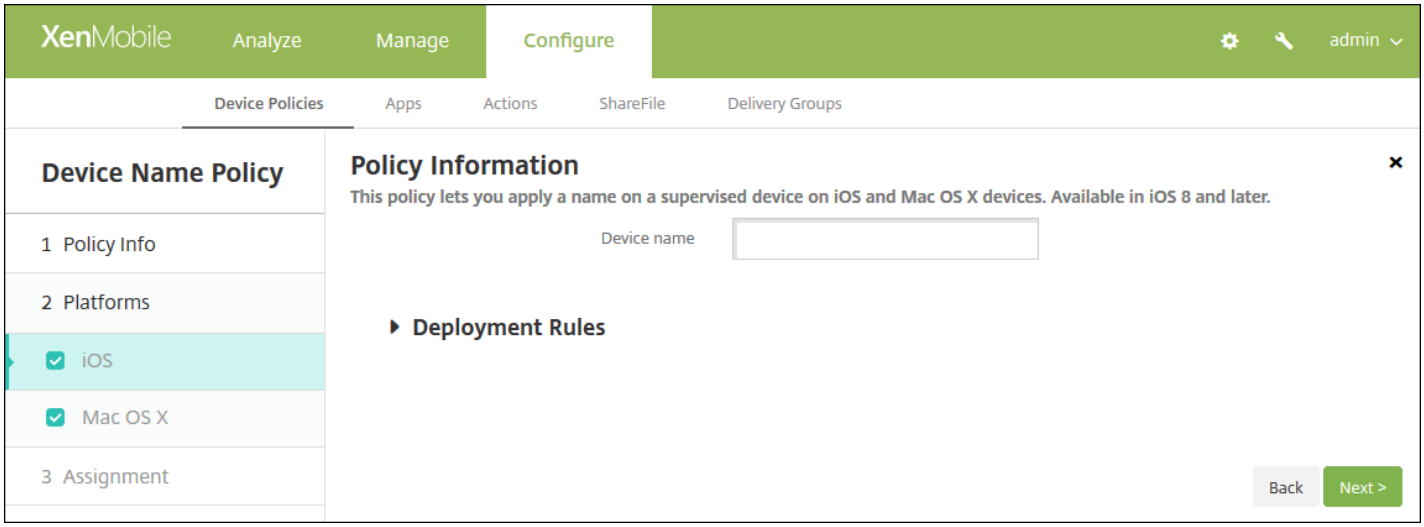
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Policy Platforms**］ページが開きます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSおよびMac OS Xの設定の構成

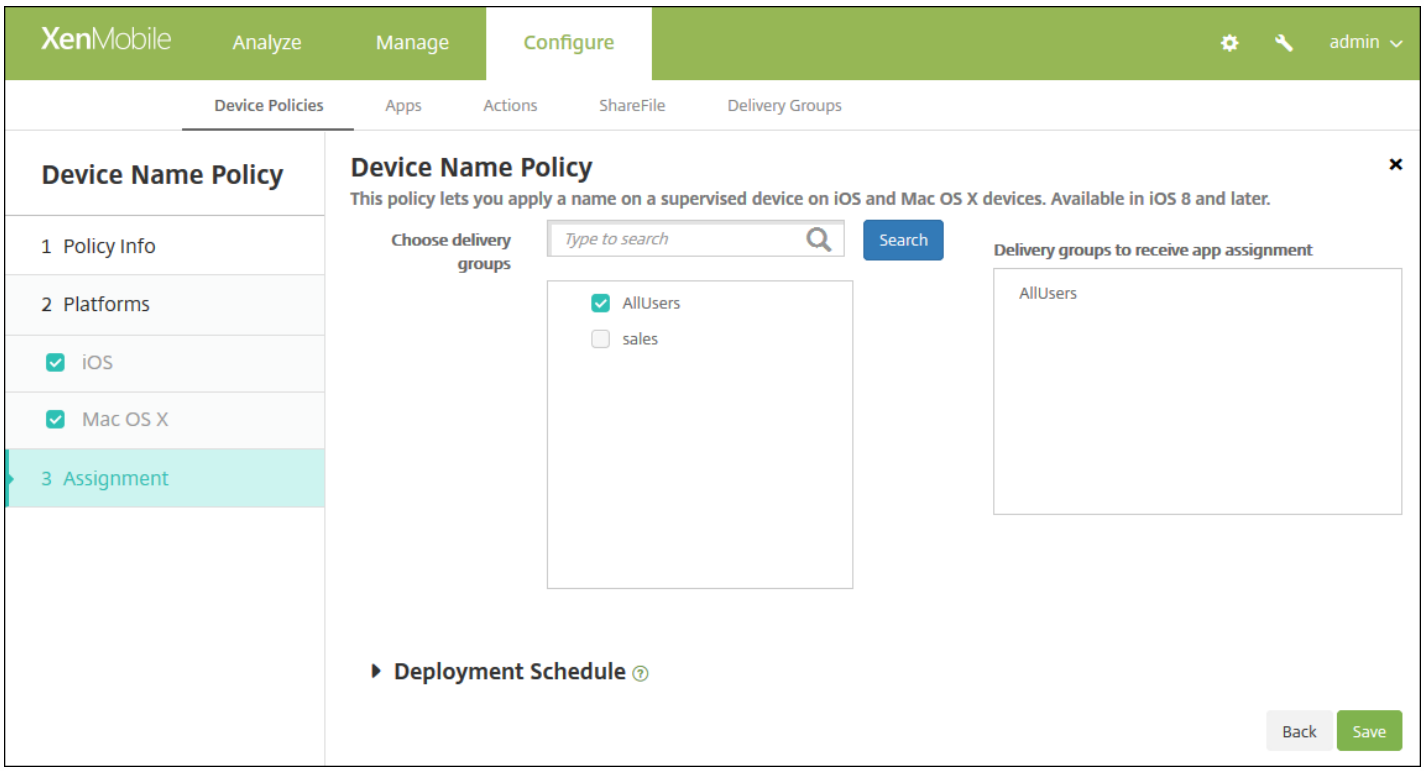


選択したプラットフォームごとに、次の設定を構成します。

- **Device name**：マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。 たとえば、デバイス名を各デバイスのシリアル番号に設定するには、${device.serialnumber}を使用します。デバイス名にユーザーの名前を含めるには、${device.serialnumber} ${ user.username}を使用します。

7. 展開規則の構成

8. [**Next**] をクリックします。 [**Device Name Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

Enterprise Hubデバイスポリシー

Aug 02, 2016

Windows PhoneのEnterprise Hubデバイスポリシーでは、Enterprise Hub Companyストアを通じてアプリケーションを配布できます。

このポリシーを作成するには以下が必要です。

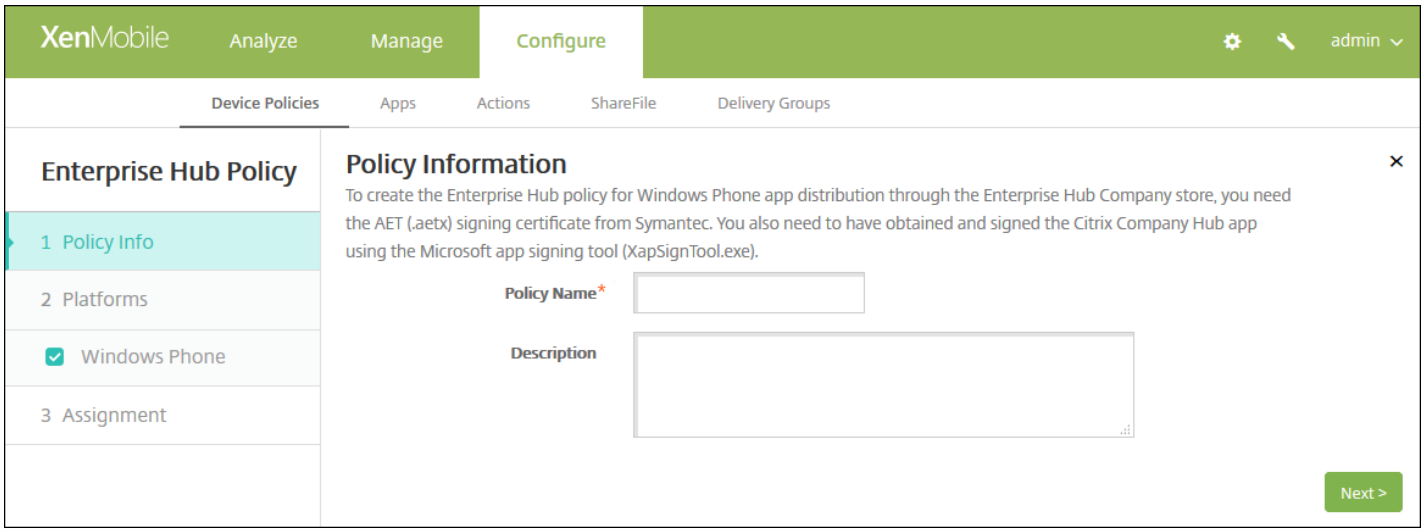
- SymantecからのAET（.aetx）署名証明書
- Microsoftのアプリケーション署名ツール（XapSignTool.exe）を使用して署名されたCitrix Company Hubアプリケーション

注：XenMobileでは、Windows Phone Worx Homeの1つのモードについて、1つのEnterprise Hubポリシーがサポートされています。 たとえば、Windows Phone Worx Home for XenMobile Enterprise Editionをアップロードするために、複数のEnterprise Hubポリシーをさまざまなバージョンの Work Home for XenMobile Enterprise Edition用に作成する必要はありません。 デバイスの登録中に最初のEnterprise Hubポリシーを展開するだけです。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

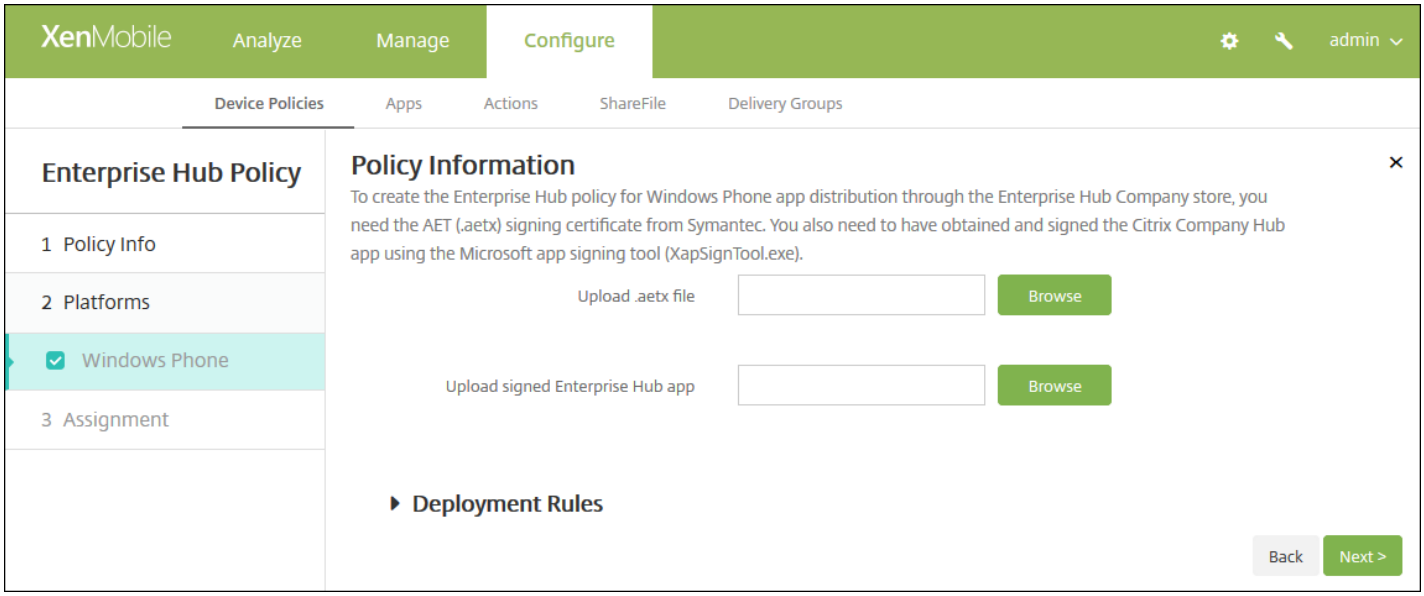
3. **[More]** をクリックした後、 **[XenMobile agent]** の下の **[Enterprise Hub]** をクリックします。 **[Enterprise Hub Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Windows Phone]** プラットフォームページが開きます。

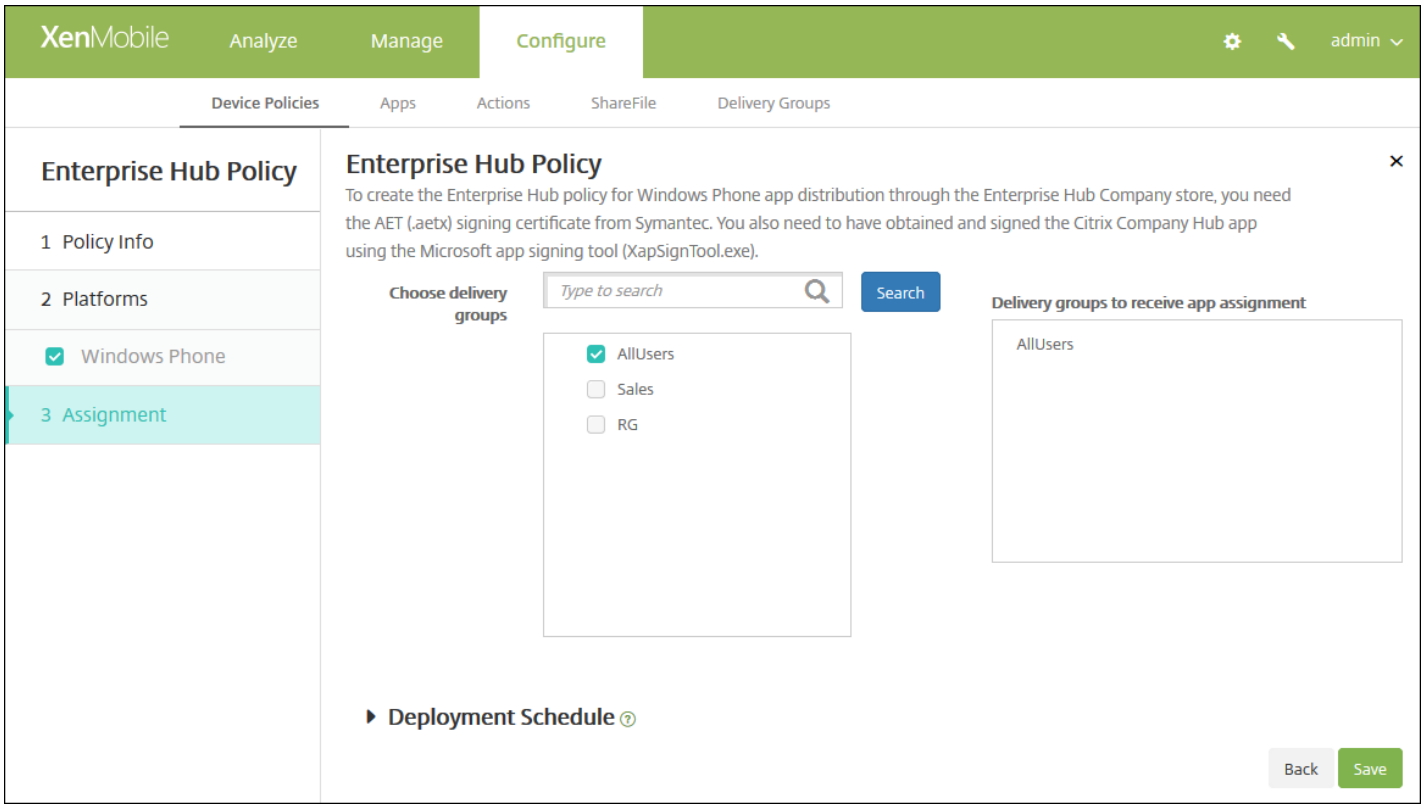


6. 次の設定を構成します。

- **Upload .aetx file**： **[Browse]** をクリックして.aetxファイルの場所に移動し、そのファイルを選択します。
- **Upload signed Enterprise Hub app**： **[Browse]** をクリックしてEnterprise Hubアプリケーションの場所に移動し、アプリケーションを選択します。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Enterprise Hub Policy]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

ファイルデバイスポリシー

Aug 02, 2016

ユーザーに対して特定の機能を実行するスクリプトファイル、またはAndroidデバイスユーザーがデバイスでアクセスできるドキュメントファイルを、XenMobileに追加できます。 ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。 たとえば、Androidユーザーが会社のドキュメントまたは.pdfファイルを受け取るようにする場合は、ファイルをデバイスに展開し、ユーザーにファイルがある場所を知らせます。

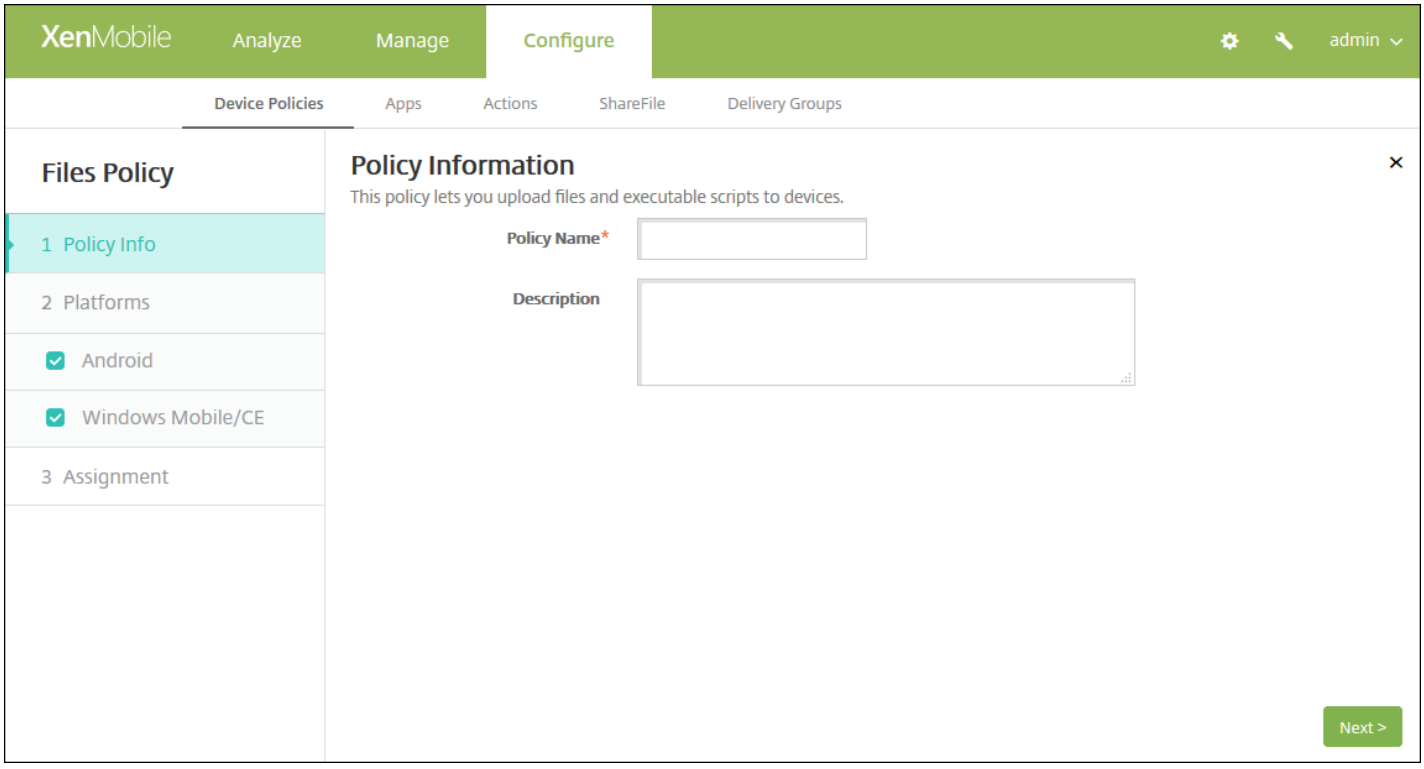
このポリシーで追加できるファイルの種類は次のとおりです。

- テキストベースのファイル（.xml、.html、.pyなど）
- ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル
- Windows MobileおよびWindows CEのみ：MortScriptで作成されたスクリプトファイル

1. XenMobileコンソールで、 **[構成]** 、 **[デバイス ポリシー]** の順にクリックすると、 **[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。

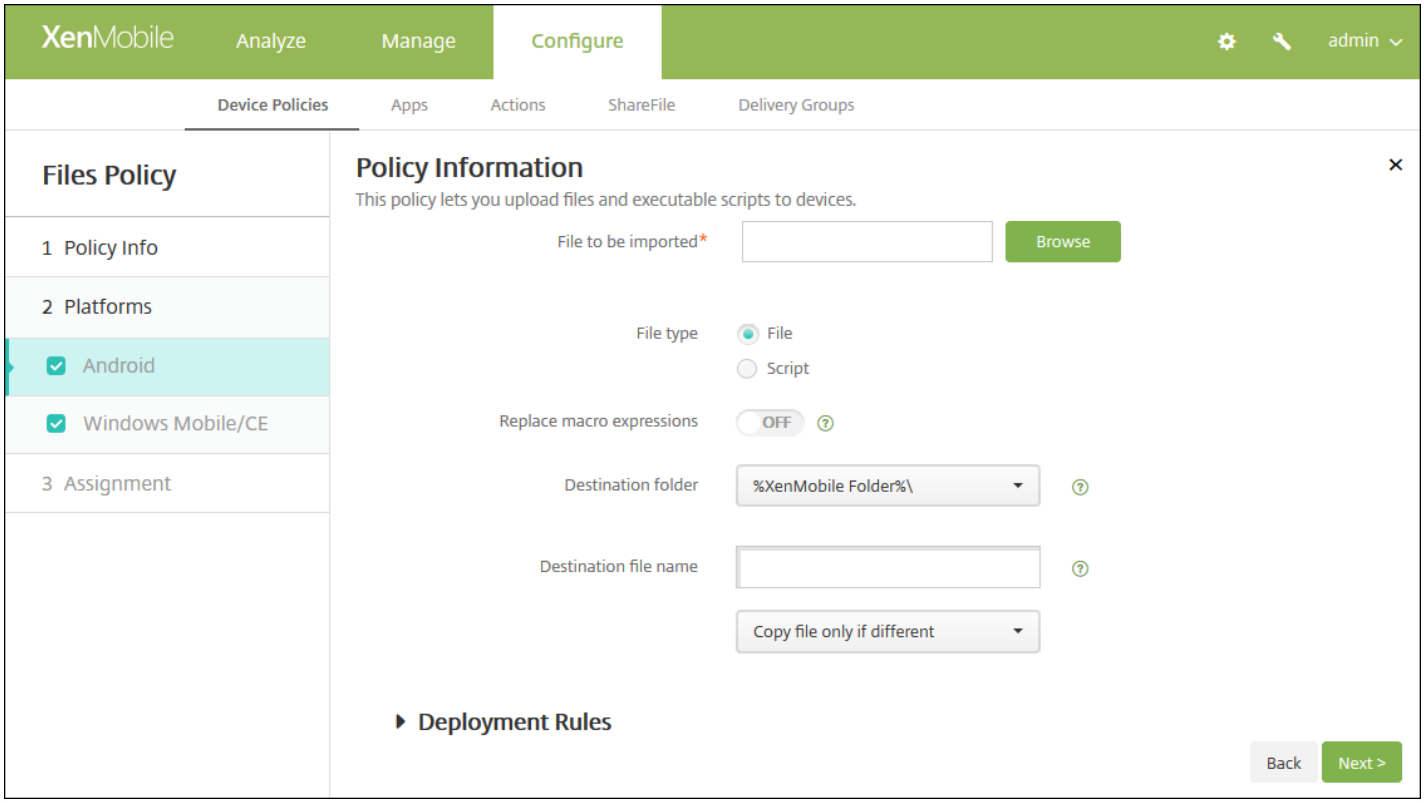
3. **[More]** を展開し、 **[Apps]** の下の **[Files]** をクリックします。 **[Files Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

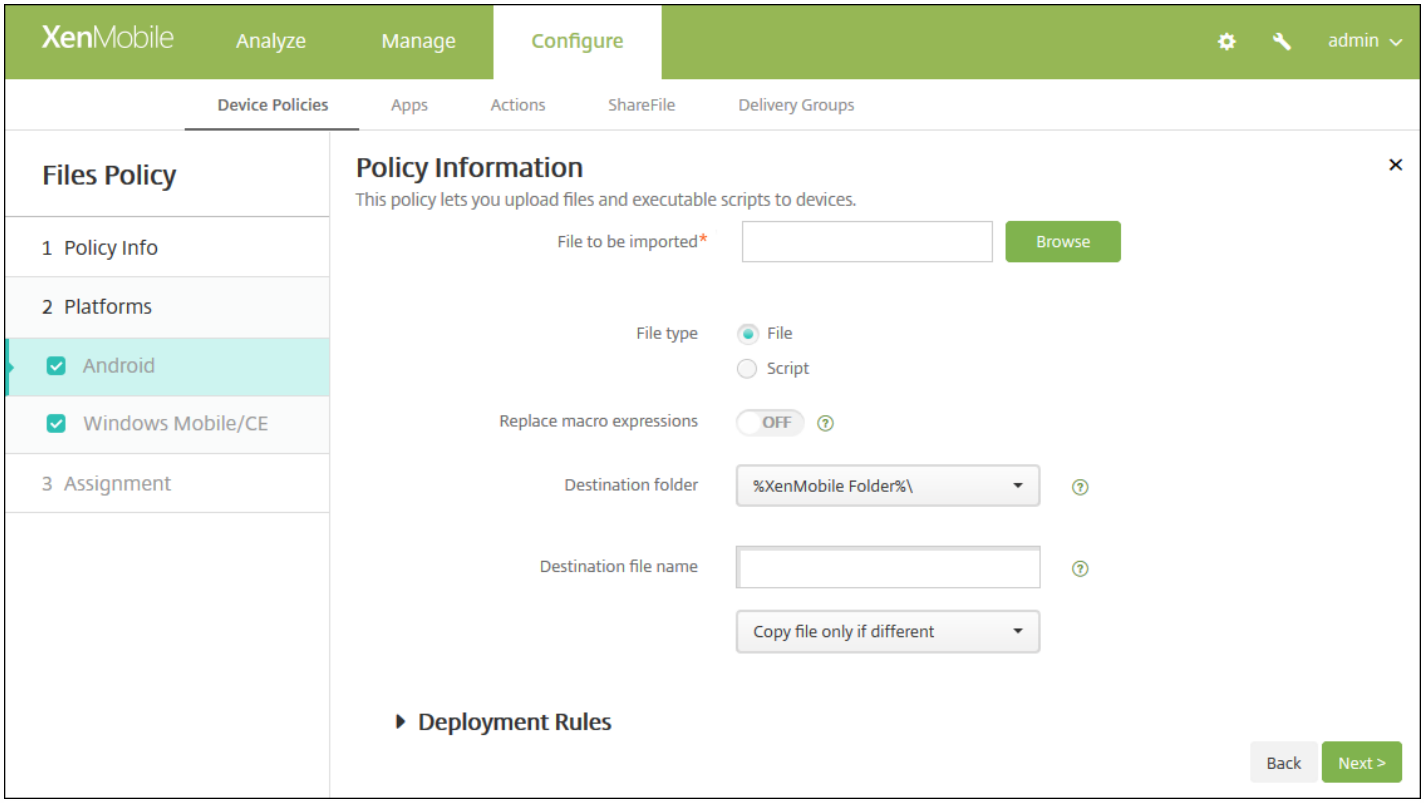
5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

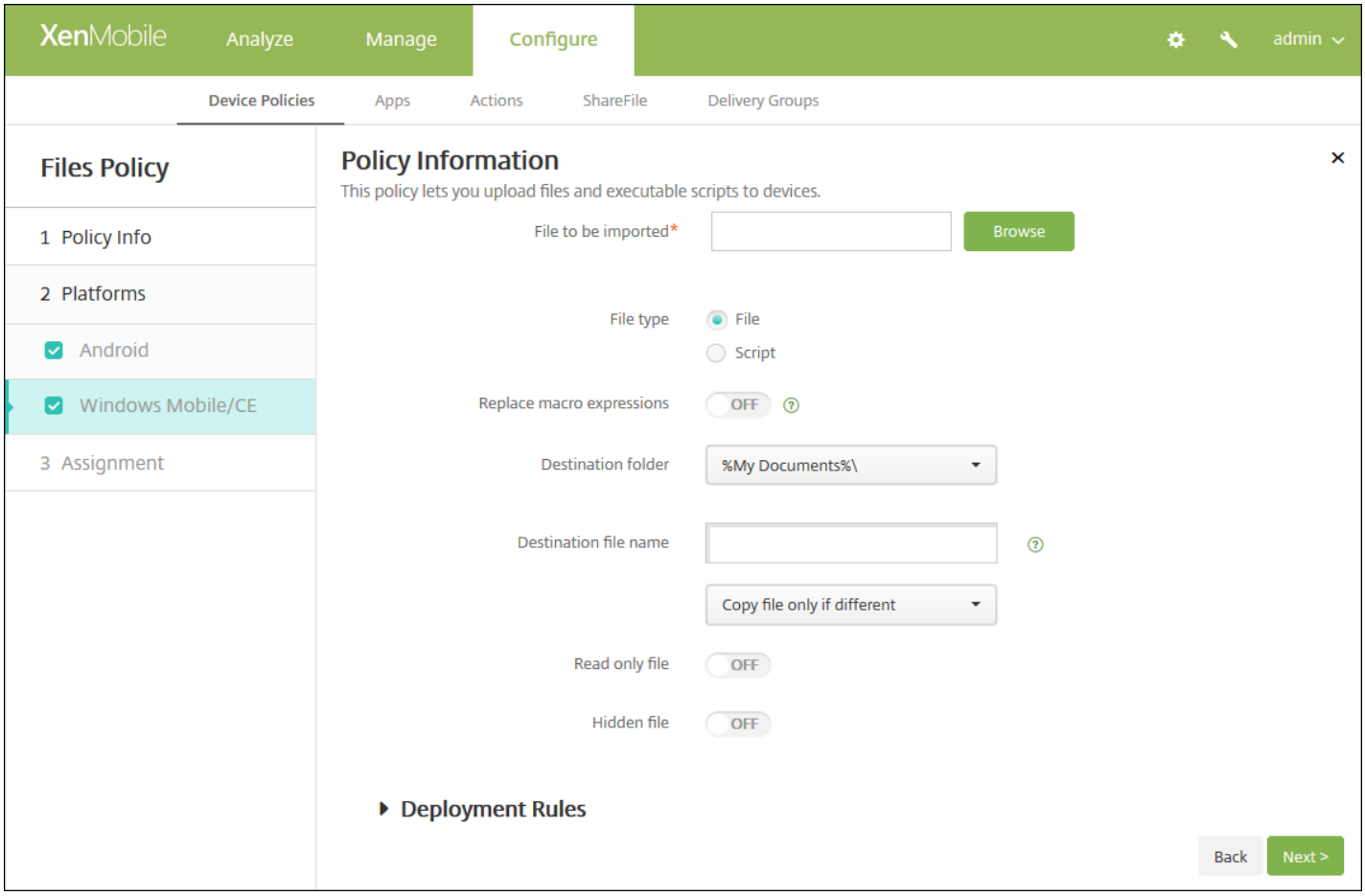
Androidの設定の構成



次の設定を構成します。

- **File to be imported**：［Browse］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。
- **File type**：［**File**］または［**Script**］を選択します。［**Script**］を選択すると、［**Execute immediately**］が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは［**OFF**］です。
- **Replace macro expressions**：スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは［**OFF**］です。
- **Destination folder**：一覧からアップロードしたファイルを格納する場所を選択するか、［**Add new**］をクリックして、一覧にない場所を選択します。また、パス識別子の先頭に%XenMobile Folder%\または%Flash Storage%\というマクロを使用することもできます。
- **Destination file name**：オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- **Copy file only if different**：一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。

Windows Mobile/CEの設定の構成

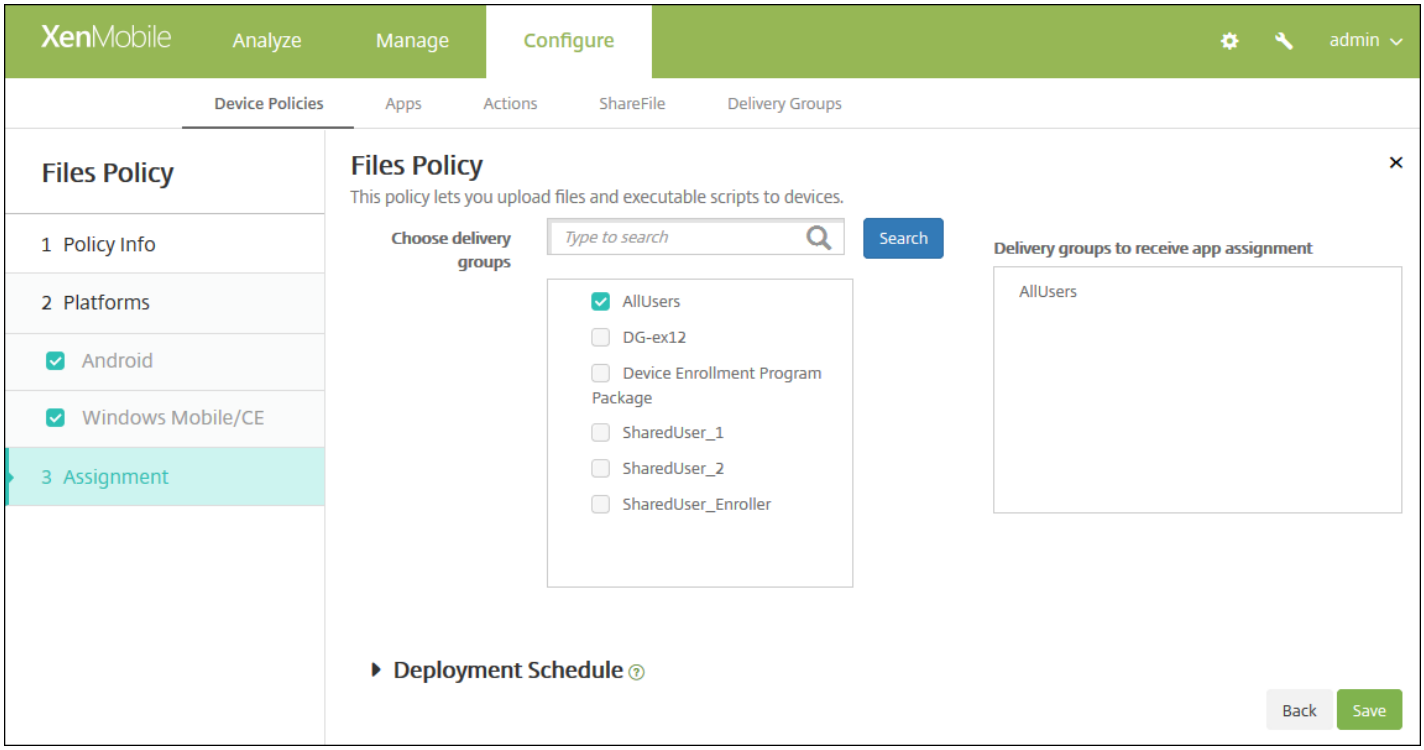


次の設定を構成します。

- **File to be imported**：［Browse］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。
- **File type**［**File**］または［**Script**］を選択します。［**Script**］を選択すると、［**Execute immediately**］が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは［**OFF**］です。
- **Replace macro expressions**：スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは［**OFF**］です。
- **Destination folder**：一覧からアップロードしたファイルを格納する場所を選択するか、［**Add new**］をクリックして、一覧にない場所を選択します。また、パス識別の先頭に以下のマクロを使用することもできます。
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**：オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- **Copy file only if different**：一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。
- **Read only file**：ファイルが読み取り専用かどうかを選択します。デフォルトは［**OFF**］です。
- **Hidden file**：ファイルをファイル一覧で非表示にするかどうかを選択します。デフォルトは［**OFF**］です。

7. 展開規則を構成します。

8. [**Next**] をクリックします。 [**Files Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

フォントデバイスポリシー

Aug 02, 2016

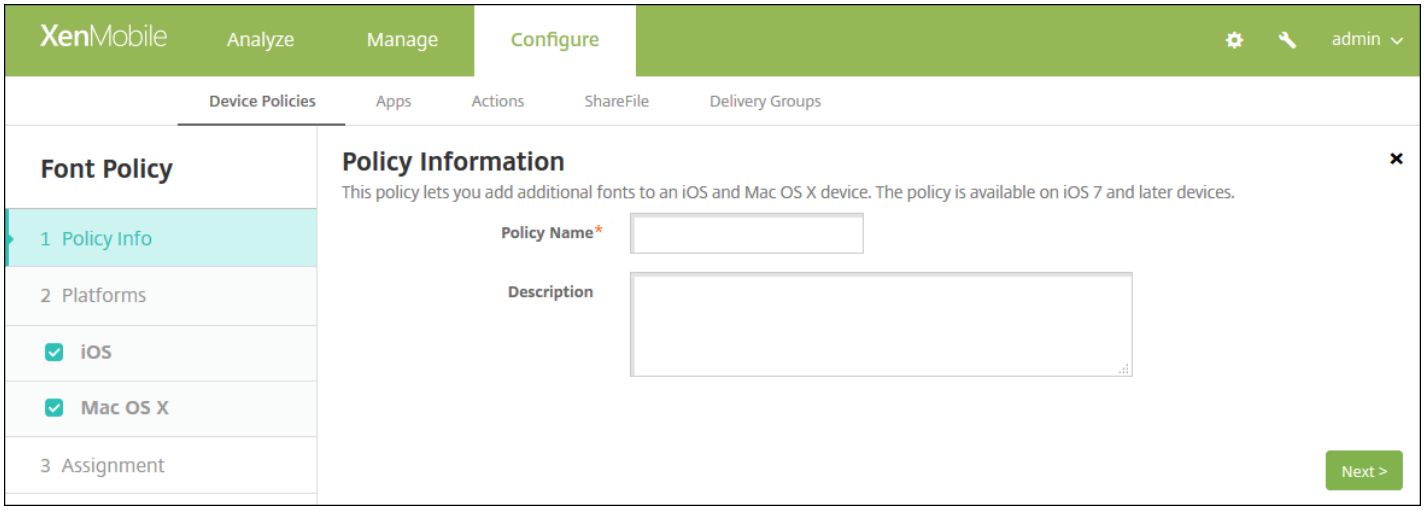
XenMobileでデバイスポリシーを追加して、追加フォントをユーザーのiOSデバイスおよびMac OS Xデバイスに追加することができます。 フォントはTrueType（.ttf）またはOpenType（.oft）である必要があります。 フォントコレクション（.ttcまたは.otc）はサポートされません。

注：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。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** をクリックした後、 **[End user]** の下の **[Font]** をクリックします。 **[Font Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

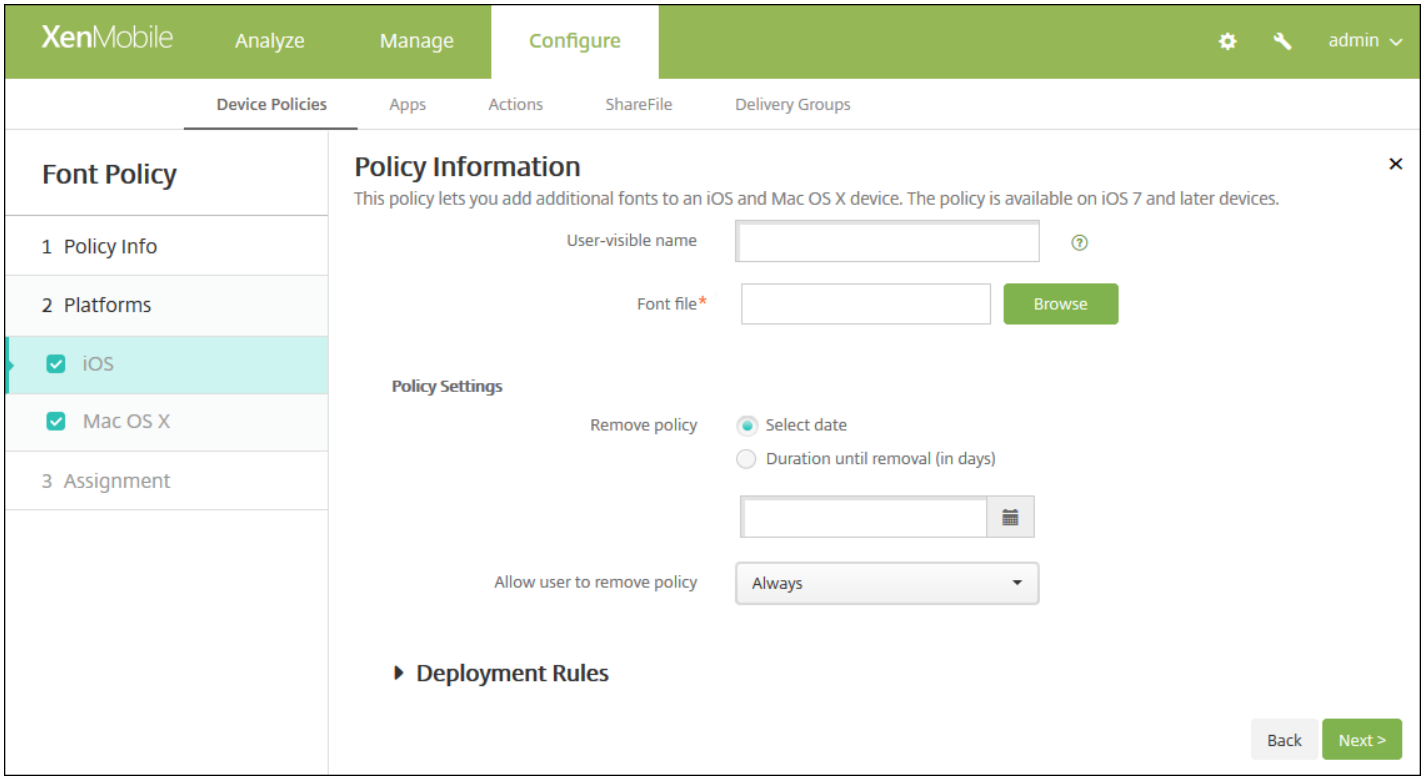
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Platforms]** ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

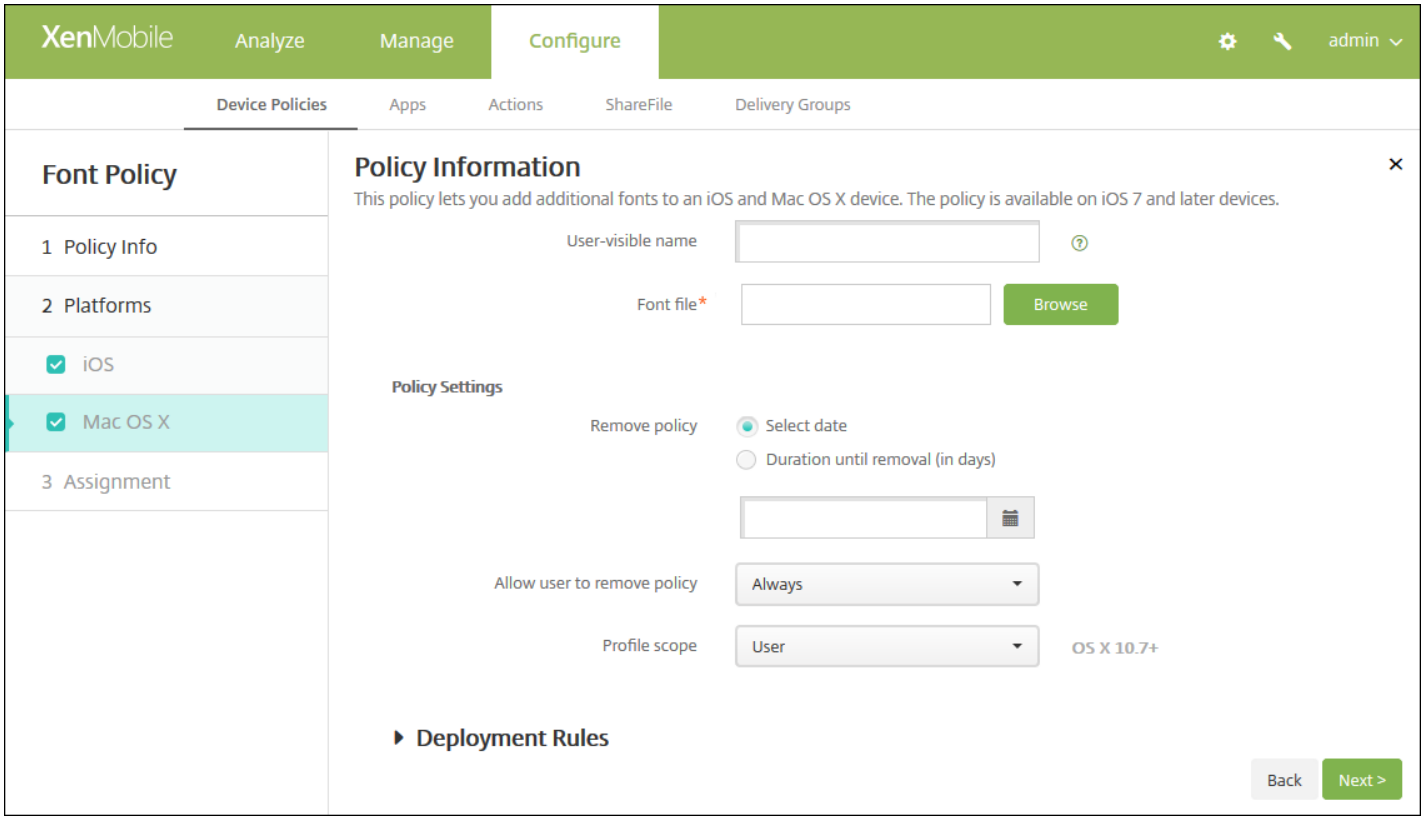
iOSの設定の構成



次の設定を構成します。

- **User-visible name**：ユーザーのフォント一覧に表示される名前を入力します。
- **Font file**：［**Browse**］をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、そのファイルを選択します。
- **ポリシー設定**
  - ［**Remove policy**］の横の［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成

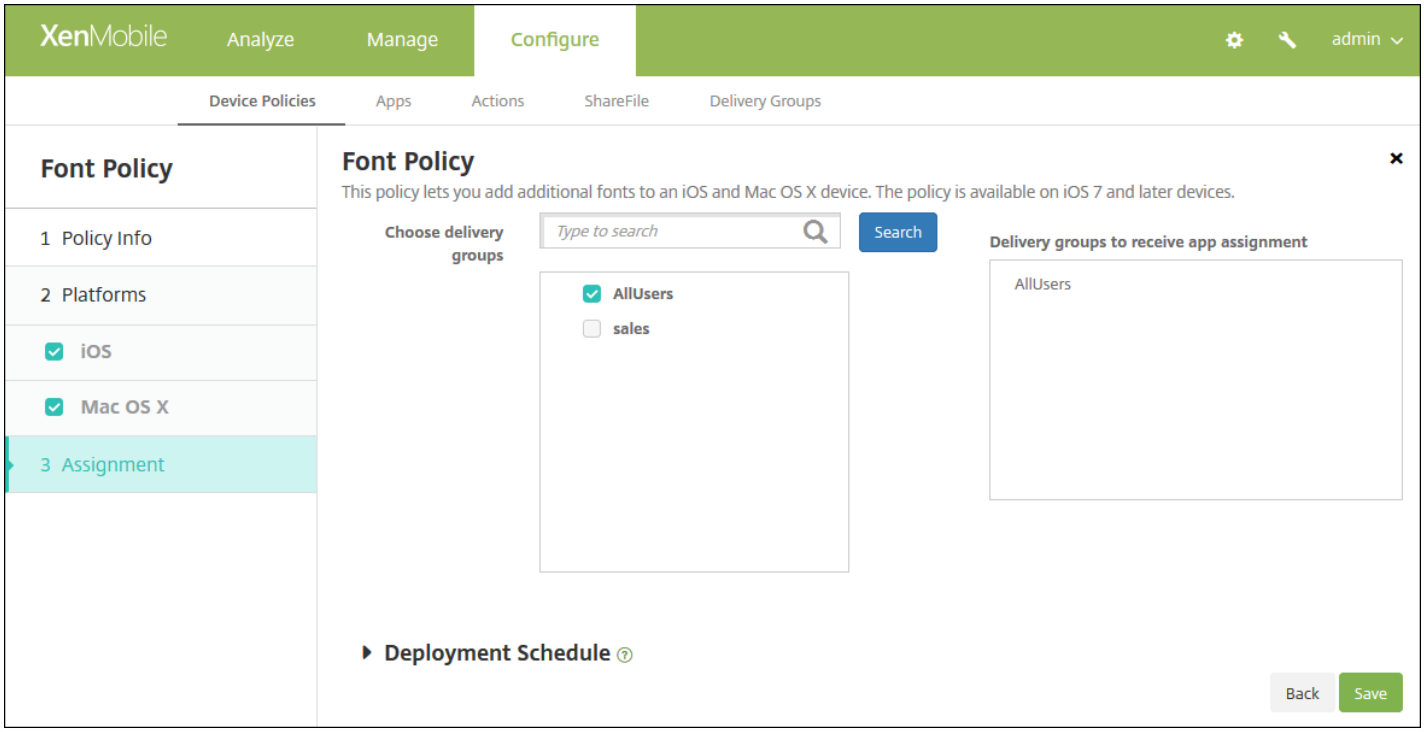


次の設定を構成します。

- **User-visible name**：ユーザーのフォント一覧に表示される名前を入力します。
- **Font file**：［**Browse**］をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、そのファイルを選択します。
- ポリシー設定
  - ［**Remove policy**］の横の［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。
  - ［**Profile scope**］の横にある、［**User**］または［**System**］を選択します。デフォルトは［**User**］です。このオプションはOS X 10.7以降でのみ使用できます。

7. 展開規則を構成します。

8. ［**Next**］をクリックします。［**Font Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

iOSおよびMac OS Xプロファイルのインポートデバイスポリシー

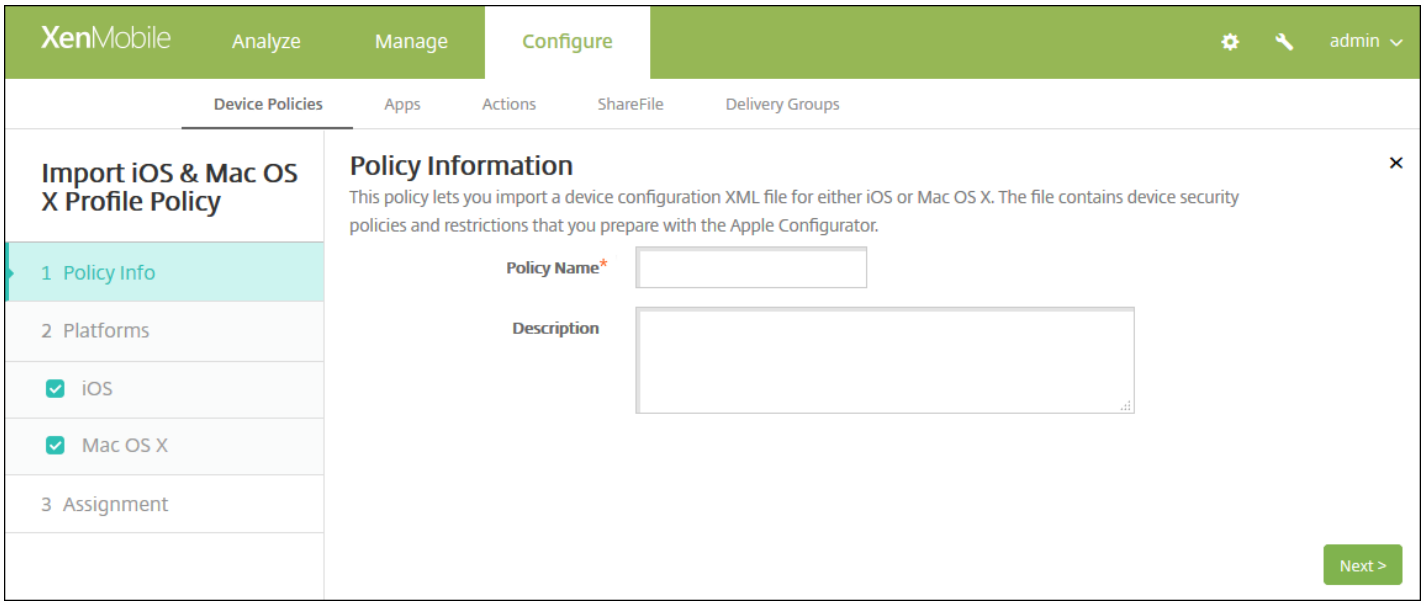
Aug 02, 2016

iOSおよびOS Xデバイス用のデバイス構成MXLファイルをXenMobileにインポートできます。 XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。 Apple Configuratorの使用による構成ファイルの作成について詳しくは、AppleのConfiguratorヘルプページを参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

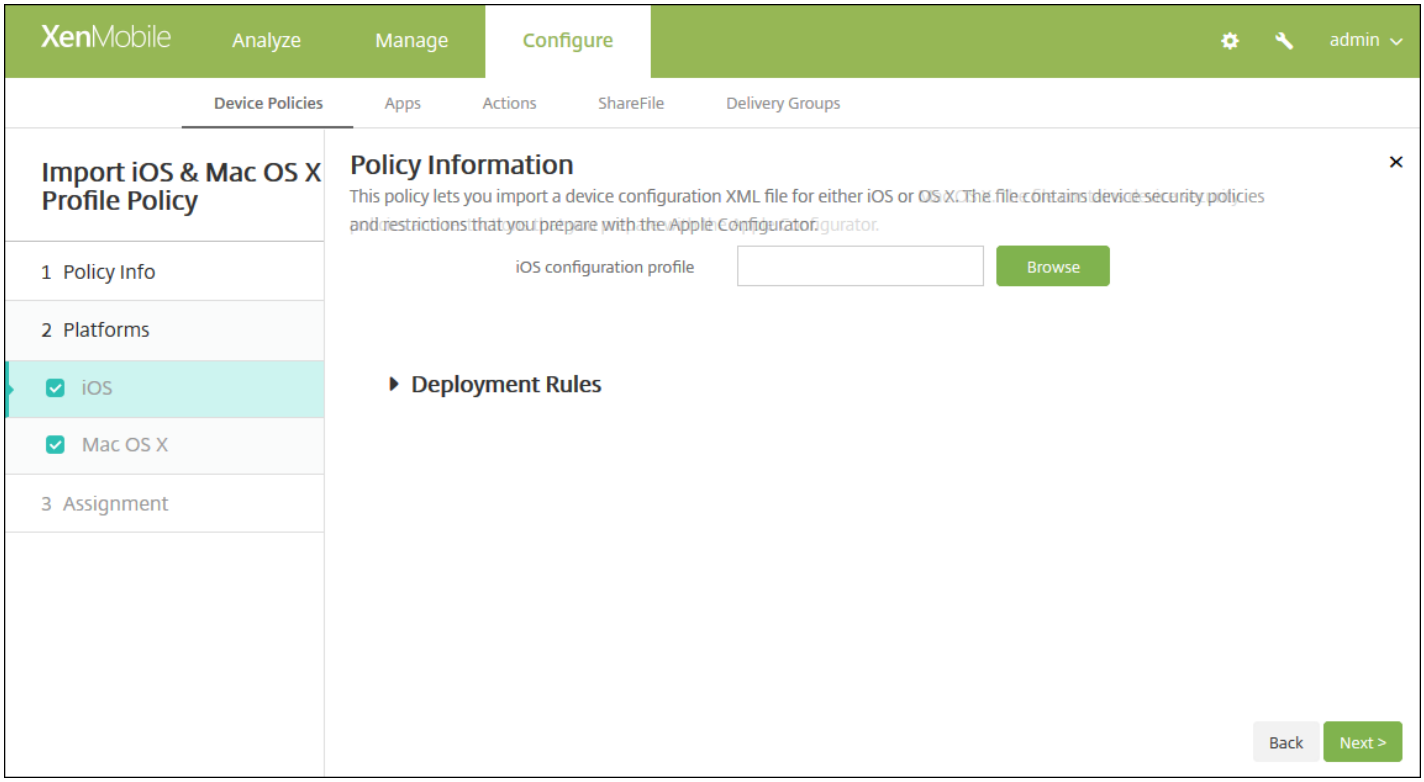
3. **[More]** を展開した後、 **[Custom]** の下の **[Import iOS & Mac OS X Profile]** をクリックします。 **[Import iOS & Mac OX X Profile Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

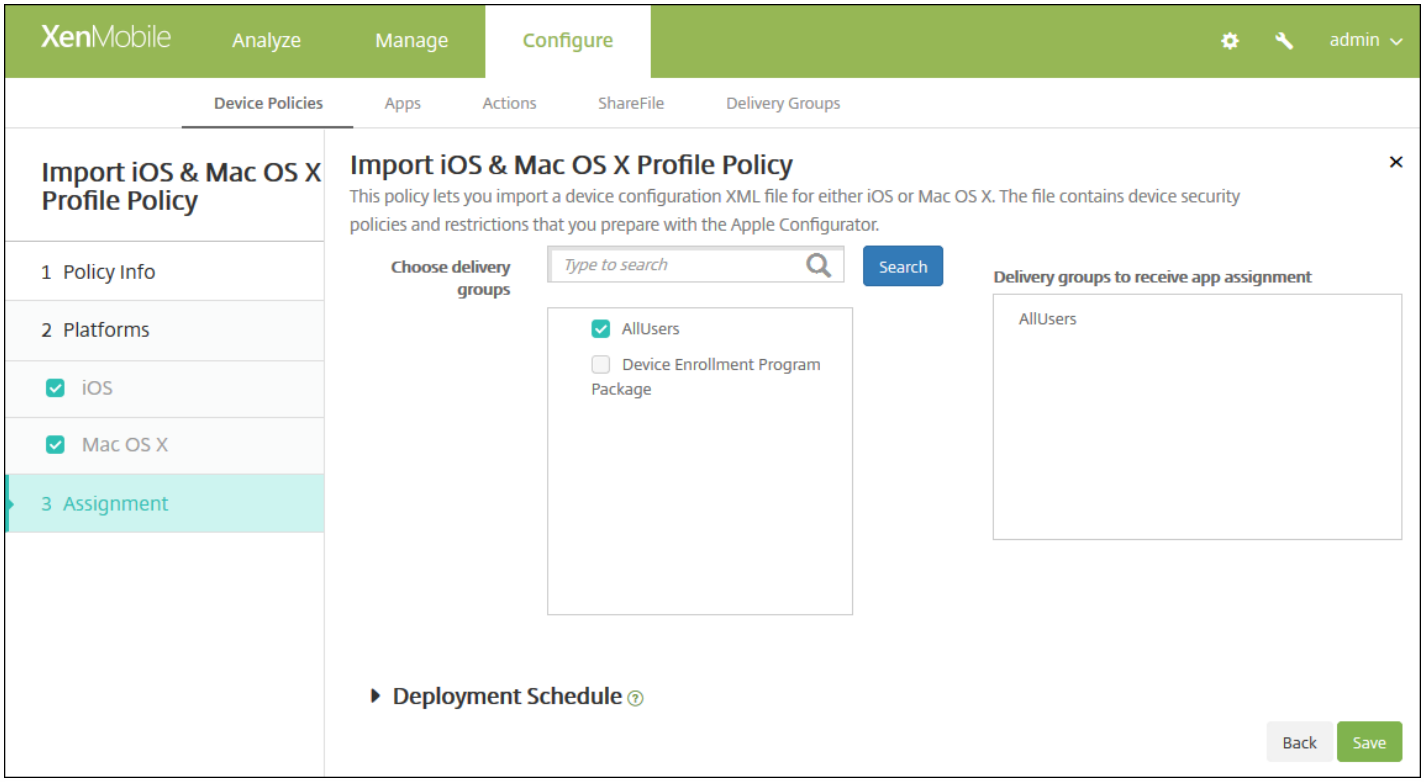
1つのプラットフォームの設定の構成が完了したら、手順8.を参照してプラットフォームの展開規則を設定します。 .

7. 選択したプラットフォームごとに、次の設定を構成します。

- **iOS configuration profile**または**Mac OS X configuration profile**： ［**Browse**］をクリックしてインポートする構成ファイルの場所に移動し、そのファイルを選択します。

8. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Import iOS & Mac OX X Profile Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックしてポリシーを保存します。

キオスクデバイスポリシー

Aug 02, 2016

XenMobileでキオスクポリシーを作成して、特定のアプリケーションのみをSamsung SAFEデバイスで使用できるように指定することができます。 このポリシーは、特定の種類またはクラスのアプリケーションのみを実行するように設計されているコーポレートデバイスで役立ちます。 また、このポリシーを使用して、デバイスがキオスクモードのときのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。

Samsung SAFEデバイスをキオスクモードにするには

1.「Samsung MDMライセンスキーデバイスポリシー」の説明に従って、モバイルデバイス上でSamsung SAFE APIキーを有効にします。 この手順で、Samsung SAFEデバイス上でポリシーを有効にします。

2.「接続スケジュールデバイスポリシー」の説明に従って、Androidデバイスの接続スケジュールポリシーを有効にします。この手順で、Androidデバイスの接続をXenMobileに戻すことができます。

3. 次のセクションの説明に従って、キオスクデバイスポリシーを追加します。

4. 適切なデリバリーグループに、それら3つのデバイスポリシーを割り当てます。 他のポリシー（たとえばアプリケーションインベントリ）をデリバリーグループに含めるかどうかを検討します。

後でキオスクモードからデバイスを削除するには、[**Kiosk mode**]を[**Disable**]に設定した新しいキオスクデバイスポリシーを作成します。 デリバリーグループを更新して、キオスクモードを有効にしたキオスクポリシーを削除し、キオスクモードを無効にするキオスクポリシーを追加します。

キオスクデバイスポリシーを追加するには

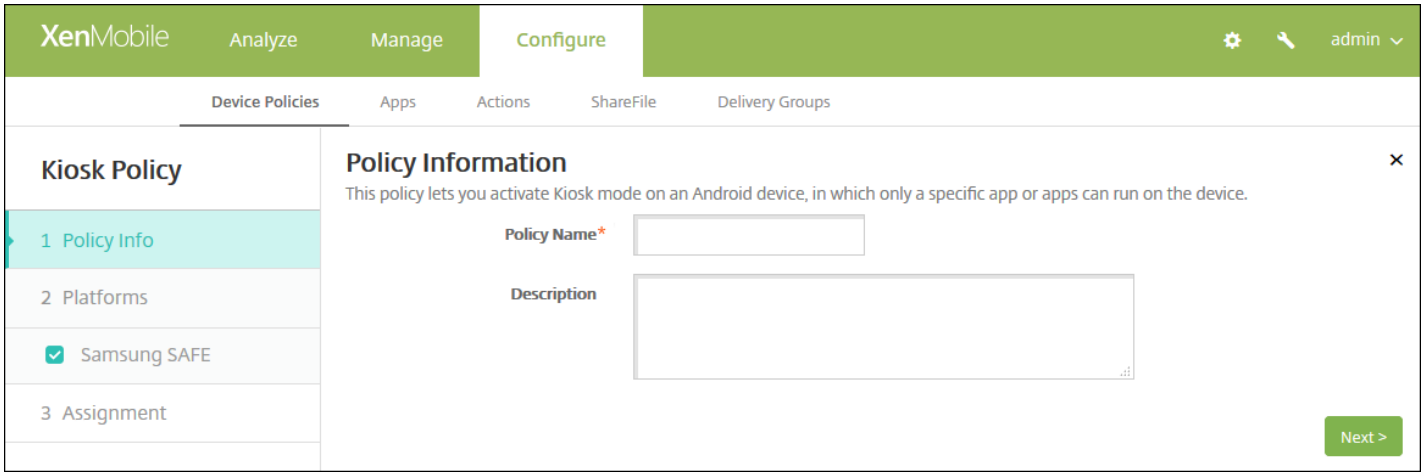
注：

- キオスクモード用に指定したすべてのアプリケーションが、ユーザーのデバイスに既にインストールされている必要があります。
- 一部のオプションは、Samsungモバイルデバイス管理（MDM）API 4.0以降にのみ適用されます。

1.XenMobileコンソールで、[**Configure**]の[**Device Policies**]をクリックします。 [**Device Policies**]ページが開きます。

2. [**Add**]をクリックします。 [**Add a New Policy**]ダイアログボックスが開きます。

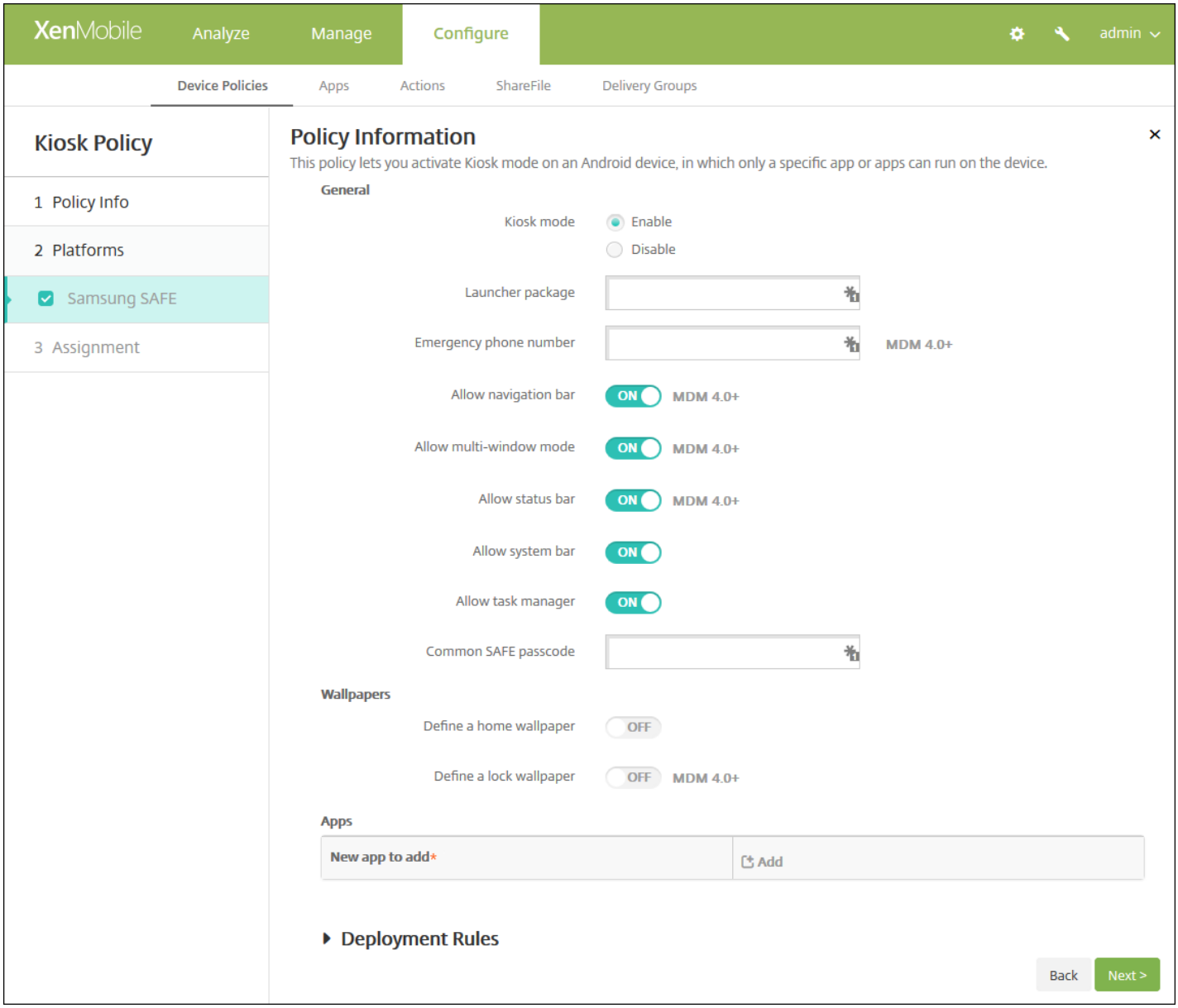
3. [**More**]を展開した後、[**Security**]の下の[**Kiosk**]をクリックします。 [**Kiosk Policy**]ページが開きます。



4. [**Policy Information**] ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Samsung SAFE Platform**] 情報ページが開きます。



6. 次の設定を構成します。

- **Kiosk mode**： [**Enable**] または [**Disable**] をクリックします。 デフォルトは [**Enable**] です。 [**Disable**] をクリックすると、以下のオプションはすべて表示されなくなります。
- **Launcher package**：ユーザーがキオスクアプリケーションを起動できる社内用ランチャーを開発した場合を除き、このフィールドは空白のままにしておくことをお勧めします。 社内用ランチャーを使用している場合、ランチャーアプリケーションパッケージの完全な名前を入力します。
- **Emergency phone number**：オプションで、電話番号を入力します。 紛失したデバイスの発見者が会社に連絡するときに、この番号を使用できます。 MDM 4.0以降にのみ適用されます。
- **Allow navigation bar**：キオスクモードのときに、ユーザーがナビゲーションバーを表示して使用できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。 デフォルトは [**ON**] です。
- **Allow multi-window mode**：キオスクモードのときに、ユーザーが複数のウィンドウを使用できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。 デフォルトは [**ON**] です。
- **Allow status bar**：キオスクモードのときに、ユーザーがステータスバーを表示できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。 デフォルトは [**ON**] です。

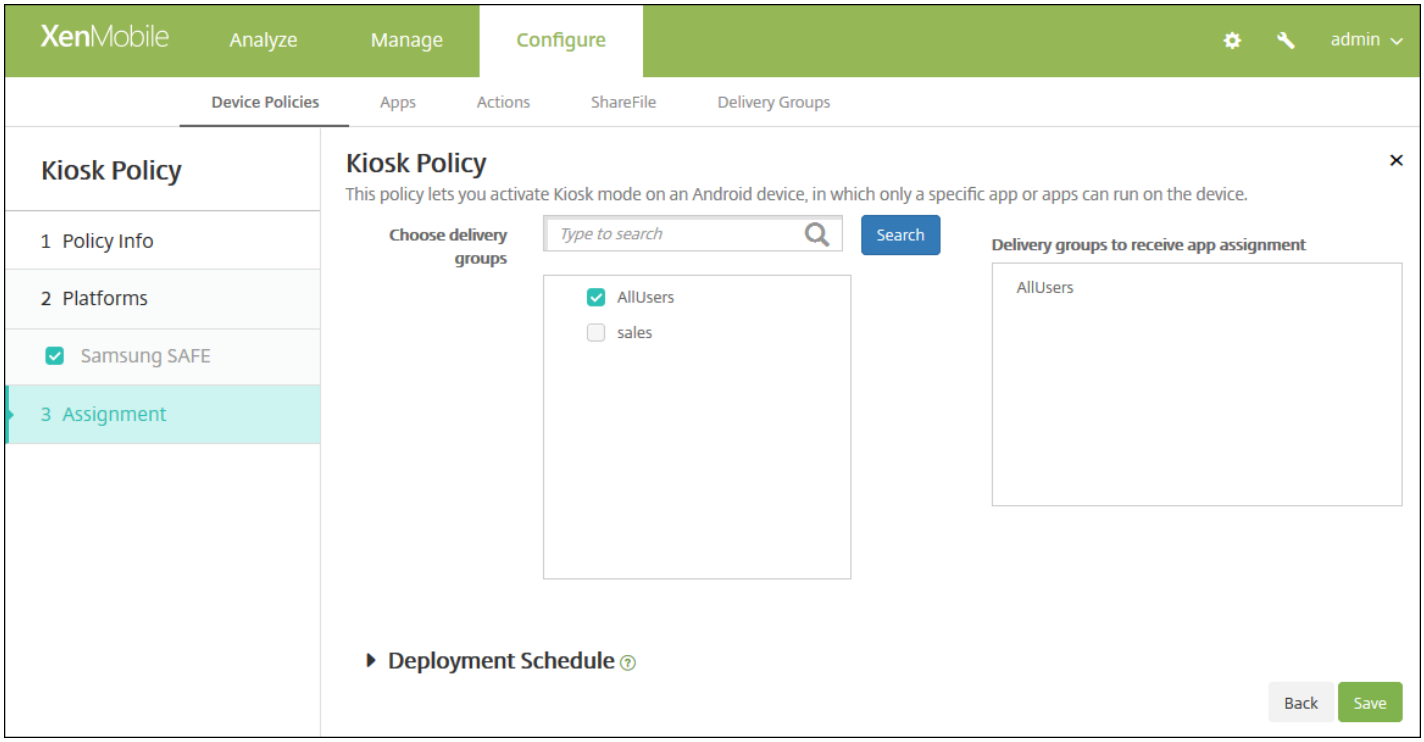
- **Allow system bar**：キオスクモードのときに、ユーザーがシステムバーを表示できるようにするかどうかを選択します。デフォルトは［**ON**］です。
- **Allow task manager**：キオスクモードのときに、ユーザーがタスクマネージャーを表示して使用できるようにするかどうかを選択します。 デフォルトは［**ON**］です。
- **Common SAFE passcode**：すべてのSamsung SAFEデバイスを対象とする汎用パスコードポリシーを設定した場合、オプションとして、このフィールドにパスコードを入力します。
- **Wallpapers**
  - **Define a home wallpaper**：キオスクモードのときに、ホーム画面でカスタムイメージを使用するかどうかを選択します。 デフォルトは［**OFF**］です。
    - **Home image**：［**Define a home wallpaper**］を有効にした場合、［**Browse**］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
  - **Define a lock wallpaper**：キオスクモードのときに、ロック画面でカスタムイメージを使用するかどうかを選択します。 デフォルトは［**OFF**］です。 MDM 4.0以降にのみ適用されます。
    - **Lock image**：［**Define a lock wallpaper**］を有効にした場合、［**Browse**］をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
- **Apps**：キオスクモードに追加するアプリケーションごとに、［**Add**］をクリックして以下の操作を行います。
  - **New app to add**：追加するアプリケーションの完全な名前を入力します。 たとえば、「com.android.calendar」を入力すると、ユーザーがAndroidのカレンダーアプリケーションを使用できます。
  - ［**Save**］をクリックしてアプリケーションを追加するか、［**Cancel**］をクリックしてアプリケーションの追加を取り消します。

    注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［**Delete**］をクリックし、項目をそのままにするには［**Cancel**］をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［**Save**］をクリックして変更した項目を保存するか、［**Cancel**］をクリックして項目を変更せずそのままにします。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Kiosk Policy**］割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

LDAPデバイスポリシー

Aug 02, 2016

XenMobileでiOSデバイスのLDAPポリシーを作成して、必要なアカウント情報など、使用するLDAPサーバーに関する情報を指定できます。 また、LDAPサーバーの照会に使用するLDAP検索ポリシーのセットが提供されます。

このポリシーを構成するには、LDAPホスト名が必要です。

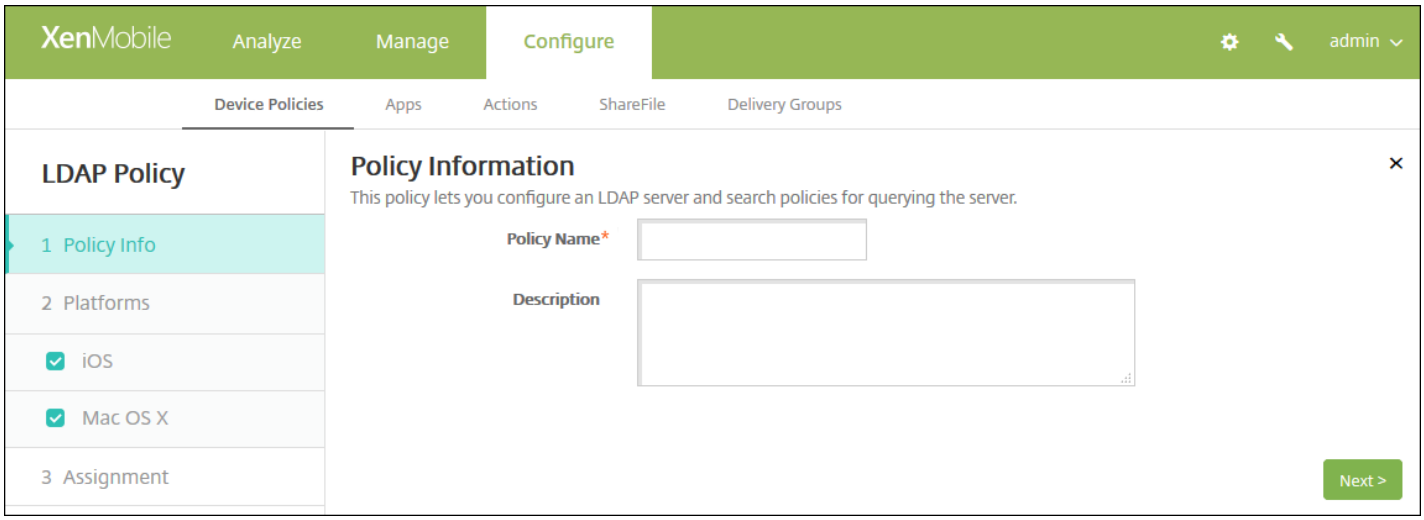
iOSの設定

Mac OS Xの設定

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2.新しいポリシーを追加するために **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** を展開した後、 **[End user]** の下の **[LDAP]** をクリックします。 **[LDAP Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

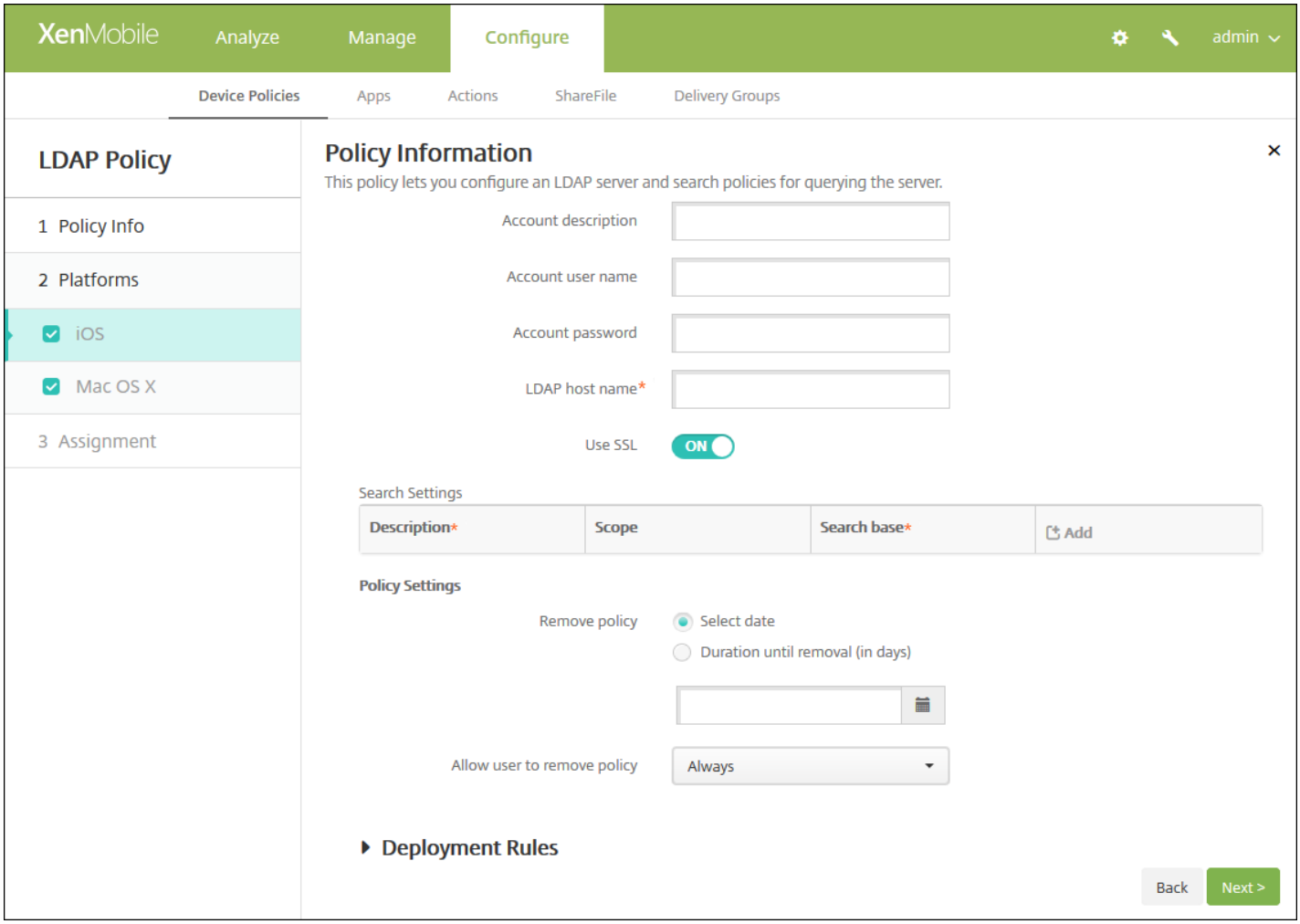
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** 情報ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



次の設定を構成します。

- **Account description**：オプションで、アカウントの説明を入力します。
- **Account user name**：オプションで、ユーザー名を入力します。
- **Account password**：オプションで、パスワードを入力します。 これは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP host name**：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。
- **Use SSL**：LDAPサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは **[ON]** です。
- **Search Settings**：LDAPサーバーの照会に使用する検索設定を追加します。 必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも1つ入力してください。 **[Add]** をクリックして、以下の操作を行います。
  - **[Description]**：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。
  - **Scope**：ボックスの一覧で **[Base]**、**[One level]**、**[Subtree]** のいずれかを選択して、LDAPツリーをどの深さまで検索するかを定義します。 デフォルトは［Base］です。
    - ［Base］を選択すると、［Search base］で参照されているノードを検索します。
    - ［One level］を選択すると、［Base］を選択した場合の検索対象ノードとその1つ下のレベルを検索します。
    - ［Subtree］を選択すると、［Base］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
- **Search base**：検索の開始位置とするノードへのパスを入力します。 たとえば、「ou=people」や「0=example corp」

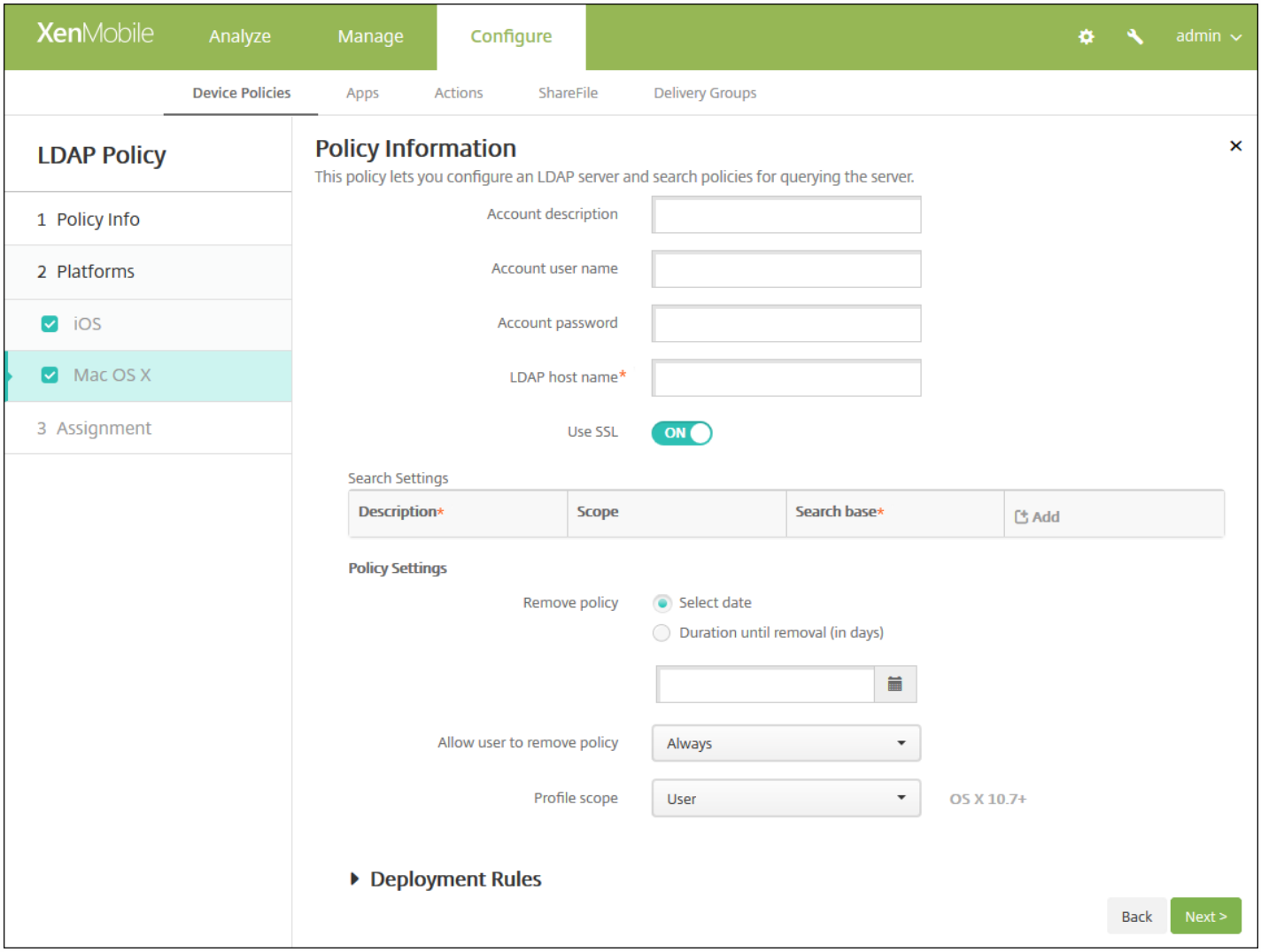
です。 このフィールドは必須です。

- ［**Save**］をクリックして検索設定を追加するか、［Cancel］をクリックして検索設定の追加を取り消します。
- 追加する検索設定ごとに上記の手順を繰り返します。

> 注：既存の検索設定を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。
>
> 既存の検索設定を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

- ［**Policy Settings**］の下の［**Remove policy**］の横にある、［**Select date**］または［**Duration until removal (in days)**］をクリックします。
- ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
- ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **Account description**：オプションで、アカウントの説明を入力します。
- **アカウント ユーザー名**：任意で、ユーザー名を入力します。
- **Account password**：オプションで、パスワードを入力します。 これは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP host name**：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。
- **Use SSL**：LDAPサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［**ON**］です。
- **Search Settings**：LDAPサーバーの照会に使用する検索設定を追加します。 必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも1つ入力してください。 ［**Add**］をクリックして、以下の操作を行います。
  - ［**Description**］：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。
  - **Scope**：ボックスの一覧で［**Base**］、［**One level**］、［**Subtree**］のいずれかを選択して、LDAPツリーをどの深さまで検索するかを定義します。 デフォルトは［Base］です。
    - ［Base］を選択すると、［Search base］で参照されているノードを検索します。
    - ［One level］を選択すると、［Base］を選択した場合の検索対象ノードとその1つ下のレベルを検索します。
    - ［Subtree］を選択すると、［Base］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - **Search base**：検索の開始位置とするノードへのパスを入力します。 たとえば、「ou=people」や「0=example corp」です。 このフィールドは必須です。
  - ［**Save**］をクリックして検索設定を追加するか、［Cancel］をクリックして検索設定の追加を取り消します。
  - 追加する検索設定ごとに上記の手順を繰り返します。

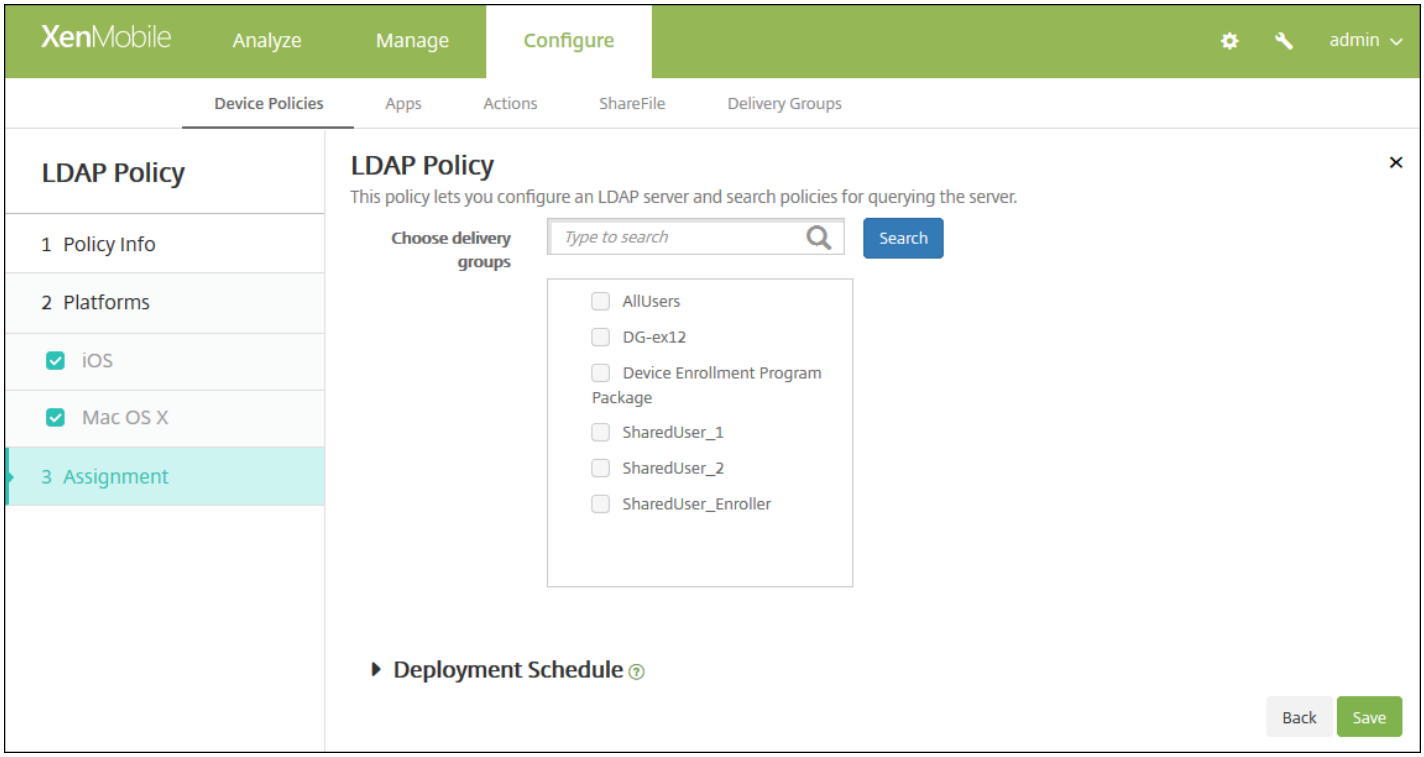
    注：既存の検索設定を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

    既存の検索設定を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

- ［**Policy Settings**］の下の［**Remove policy**］の横にある、［**Select date**］または［**Duration until removal (in days)**］をクリックします。
- ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
- ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。
- ［**Profile scope**］で、［**User**］または［**System**］を選択します。 デフォルトは［**User**］です。 このオプションはOS X 10.7以降でのみ使用できます。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**LDAP Policy**］割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックしてポリシーを保存します。

位置情報デバイスポリシー

Aug 02, 2016

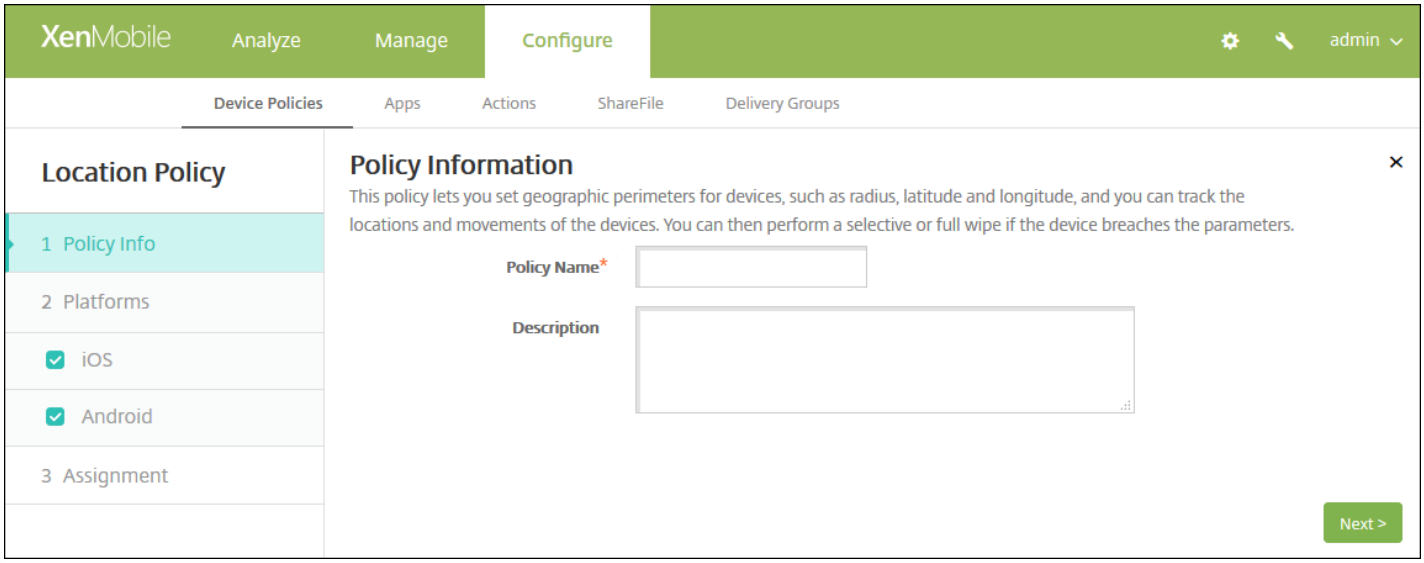
XenMobileで位置情報デバイスポリシーを作成して、地理的な境界を適用したり、ユーザーのデバイスの位置や移動を追跡したりすることができます。 定義された境界（*ジオフェンス*）の外にユーザーが出た場合、XenMobileで選択的ワイプまたは完全なワイプを直ちに実行することができます。また、許可された場所にユーザーが戻ることができるように、一定の時間が経過してから実行することもできます。

位置情報デバイスポリシーは、iOSおよびAndroidに対して作成できます。 プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[Location]** をクリックします。 **[Location Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

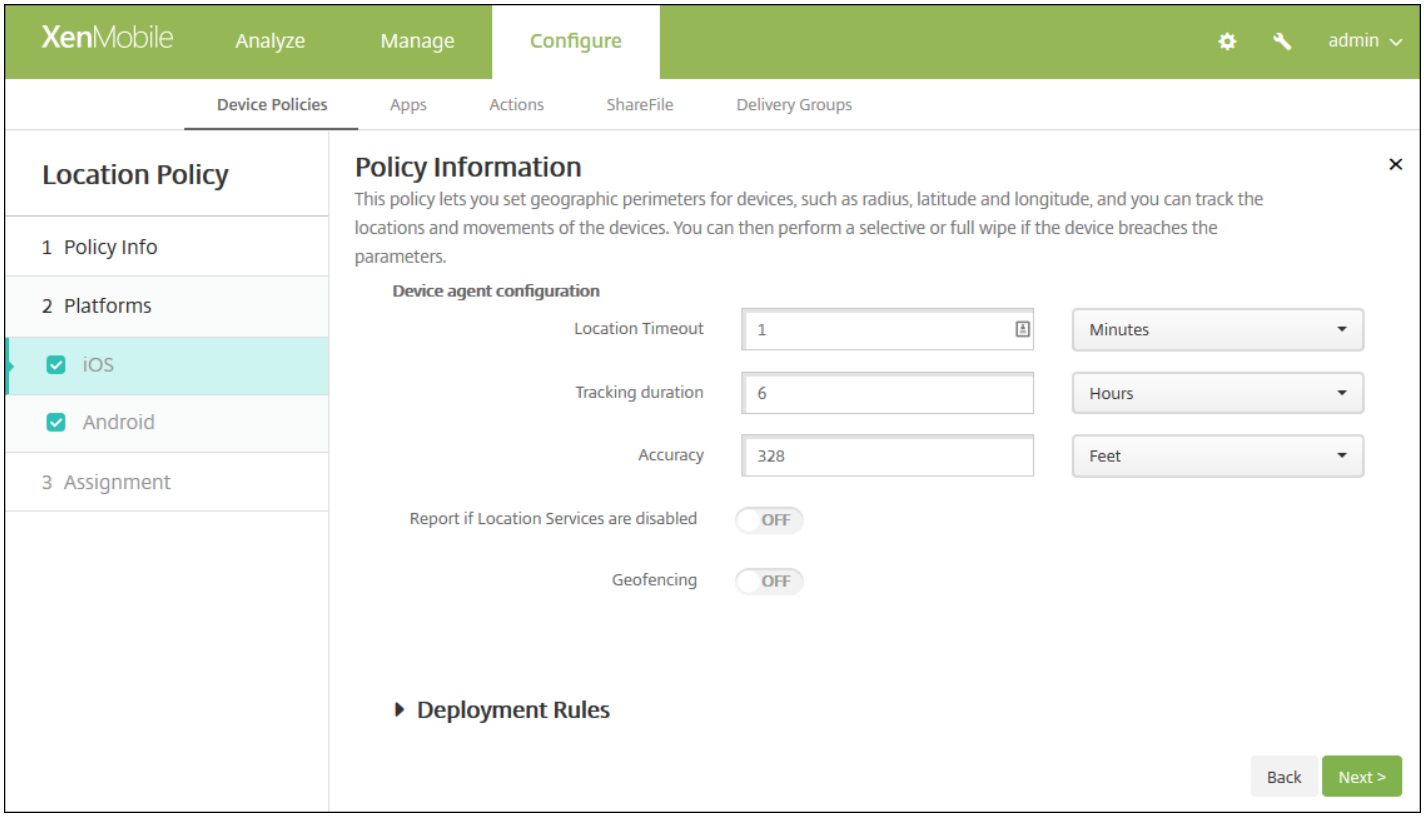
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Platforms]** ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

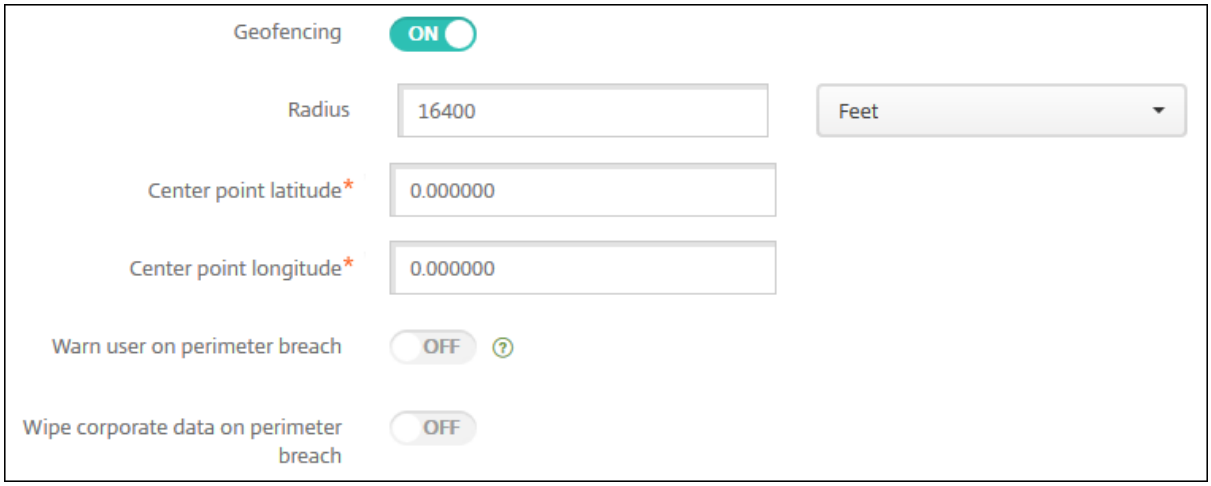
1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



次の設定を構成します。

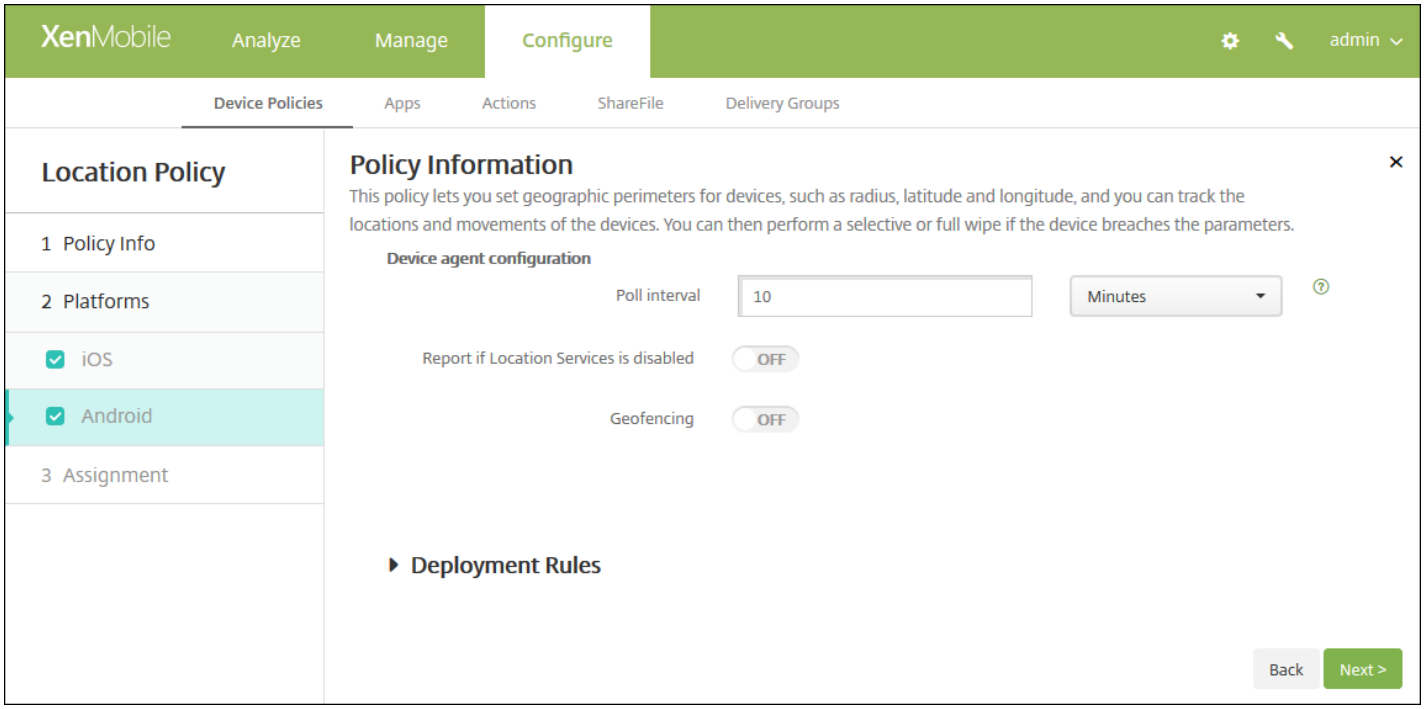
- **Location timeout**：数値を入力して、ボックスの一覧で［**Seconds**］または［**Minutes**］を選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。 有効な値は、60～900秒または1～15分です。 デフォルトは1分です。
- **Tracking duration**：数値を入力して、ボックスの一覧で［**Hours**］または［**Minutes**］を選択し、XenMobileがデバイスを追跡する時間を設定します。 有効な値は、1～6時間または10～360分です。 デフォルトは6時間です。
- **Accuracy**：数値を入力して、ボックスの一覧で［**Meters**］、［**Feet**］、［**Yards**］のいずれかを選択し、XenMobileがデバイスを追跡する精度を設定します。 有効な値は、10～5000ヤード、10～5000m、または30～15000フィートです。 デフォルトは328フィートです。
- **Report if Location Services are disabled**：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。 デフォルトは［**OFF**］です。
- **Geofencing**



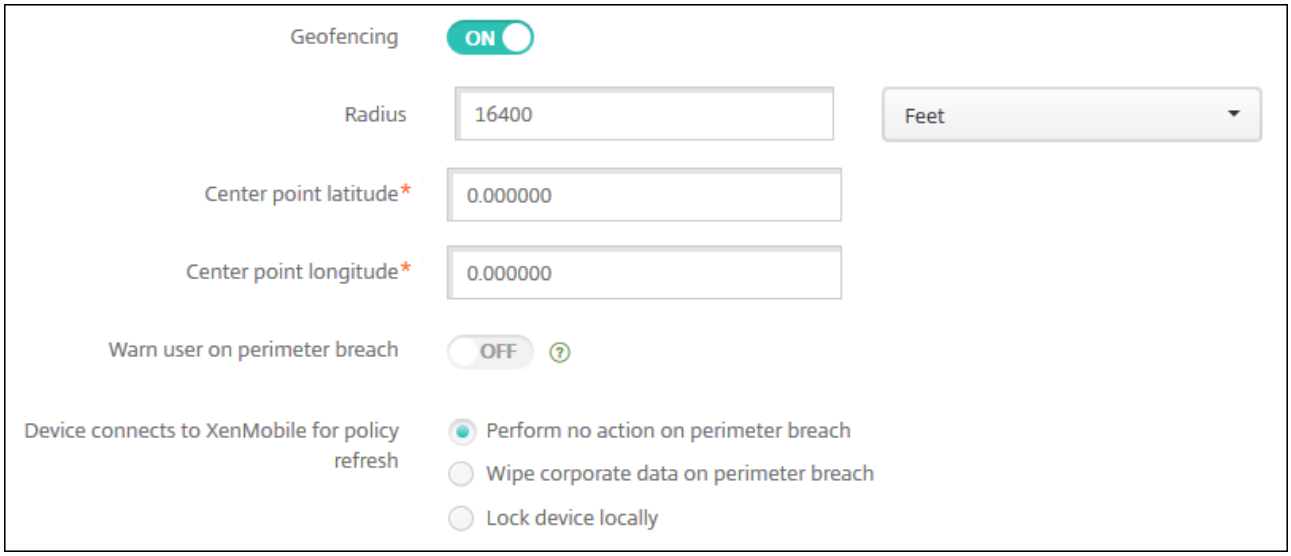
［Geofencing］を選択した場合は、次の設定を構成します。

- **Radius**：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。 デフォルトは16,400フィートです。 有効な半径の値は次のとおりです。
  - 164～164000フィート
  - 50～50000m
  - 54～54680ヤード
  - 1～31マイル
- **Center point latitude**：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- **Center point longitude**：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- **Warn user on perimeter breach**：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。 デフォルトは**［OFF］**です。 警告メッセージの表示にXenMobileへの接続は必要ありません。
- **Wipe corporate data on perimeter breach**：ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。 デフォルトは**［OFF］**です。 このオプションを有効にすると、**［Delay on local wipe］**フィールドが表示されます。
  - 数値を入力し、一覧から**［Seconds］**または**［Minutes］**を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。 これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。 デフォルトは0秒です。

Androidの設定の構成



- **Poll interval**：数値を入力して、ボックスの一覧で［**Minutes**］、［**Hours**］、［**Days**］のいずれかを選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。 有効な値は、1～1440分、1～24時間、または任意の日数です。 デフォルトは10分です。 この値を10分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- **Report if Location Services are disabled**：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。 デフォルトは［**OFF**］です。
- **Geofencing**



［Geofencing］を選択した場合は、次の設定を構成します。

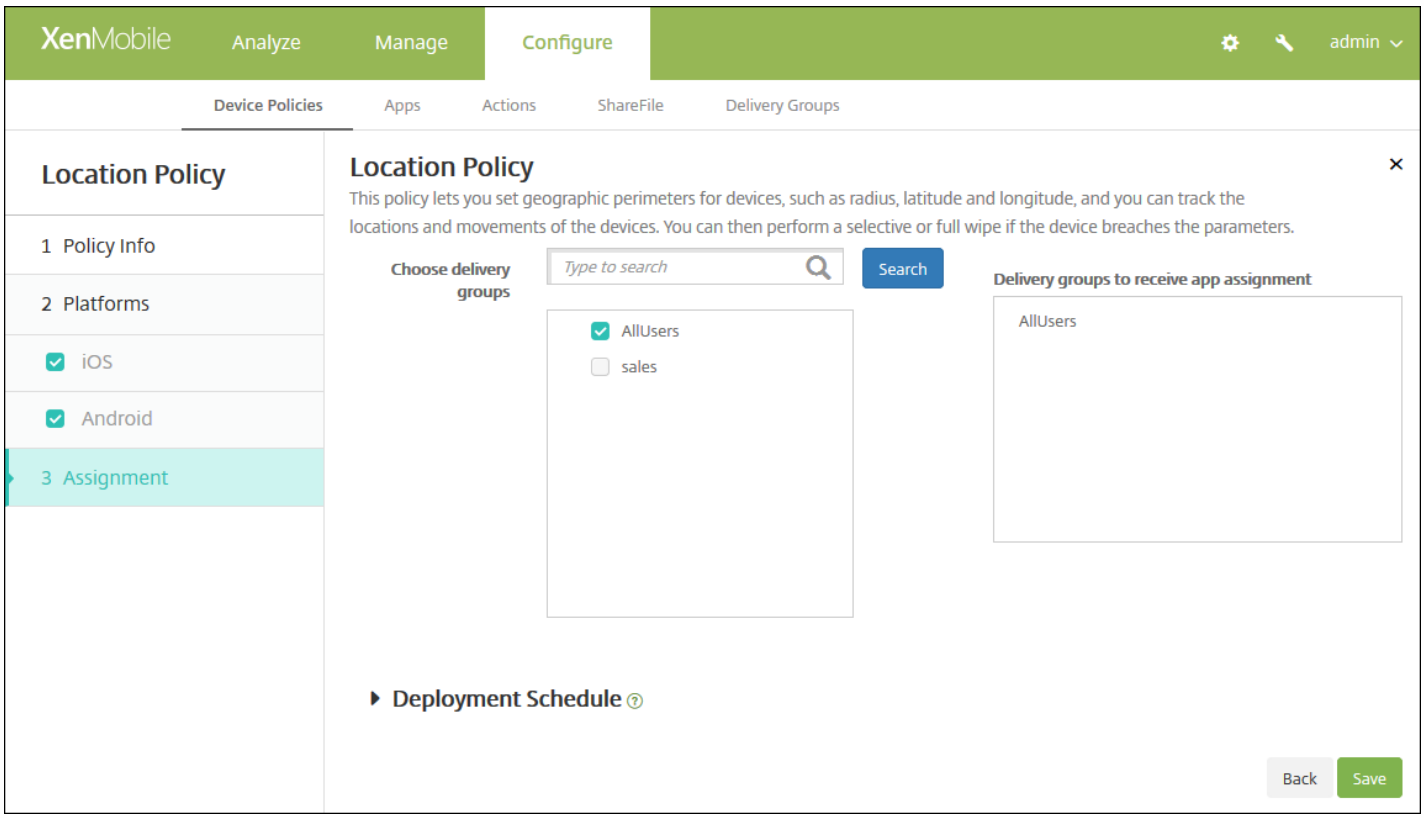
- **Radius**：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。 デフォルトは16,400フィートです。 有効な半径の値は次のとおりです。

- 164～164000フィート
- 1～50km
- 50～50000m
- 54～54680ヤード
- 1～31マイル

- **Center point latitude**：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- **Center point longitude**：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- **Warn user on perimeter breach**：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。 デフォルトは **[OFF]** です。 警告メッセージの表示にXenMobileへの接続は必要ありません。
- **Device connects to XenMobile for policy refresh**：ユーザーが境界の外に出た場合のオプションを以下から1つ選択します。
  - **Perform no action on perimeter breach**：何もしません。 これがデフォルトの設定です。
  - **Wipe corporate data on perimeter breach**：指定した時間が経過すると、企業データがワイプされます。 このオプションを有効にすると、 **[Delay on local wipe]** フィールドが表示されます。
    - 数値を入力し、一覧から［Seconds］または［Minutes］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。 これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。 デフォルトは0秒です。
  - **Delay on lock**：指定した時間が経過すると、ユーザーのデバイスがロックされます。 このオプションを有効にすると、 **[Delay on lock]** フィールドが表示されます。
    - 数値を入力し、一覧から［Seconds］または［Minutes］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。 これにより、デバイスがXenMobileによってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。 デフォルトは0秒です。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[Location Policy]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

メールデバイスポリシー

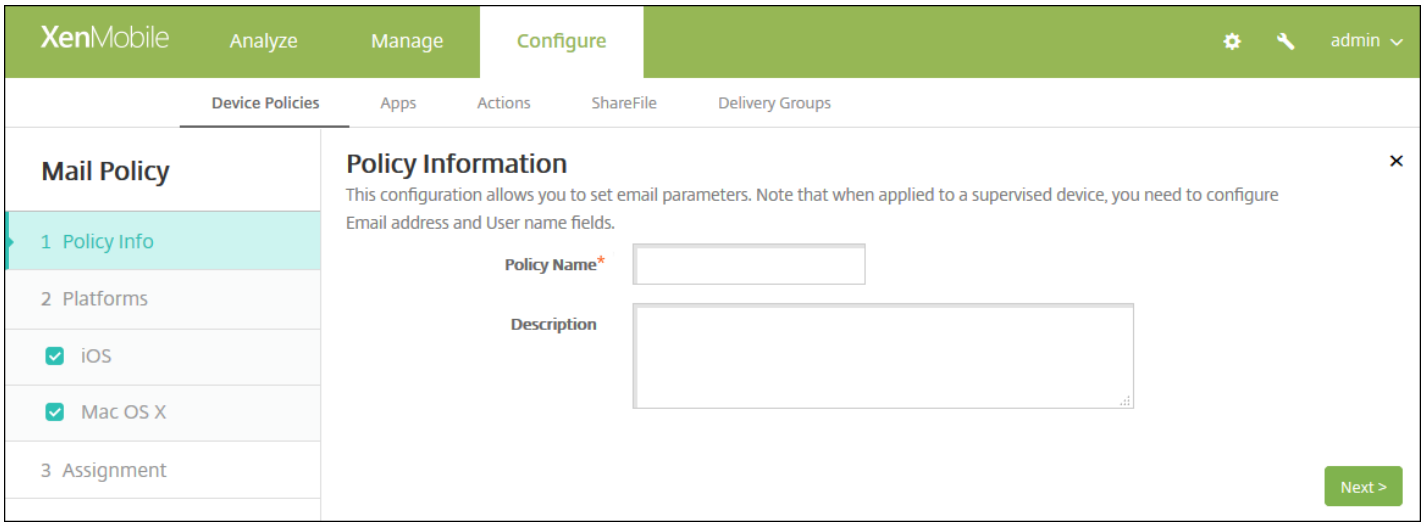
Aug 02, 2016

XenMobileでメールデバイスポリシーを追加して、ユーザーのiOSデバイスまたはMac OS Xデバイスのメールアカウントを構成することができます。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.新しいポリシーを追加するために［**Add**］をクリックします。［**Add a New Policy**］ダイアログボックスが開きます。

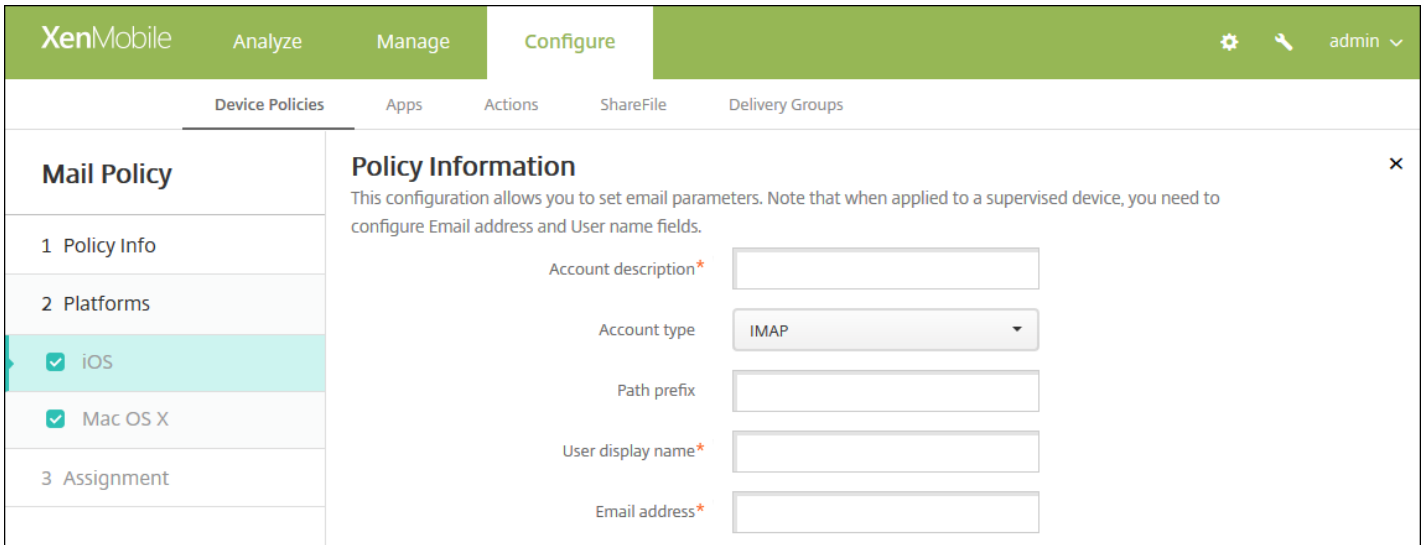
3. ［**More**］をクリックした後、［**End user**］の下の［**Mail**］をクリックします。［**Mail Policy**］ページが開きます。

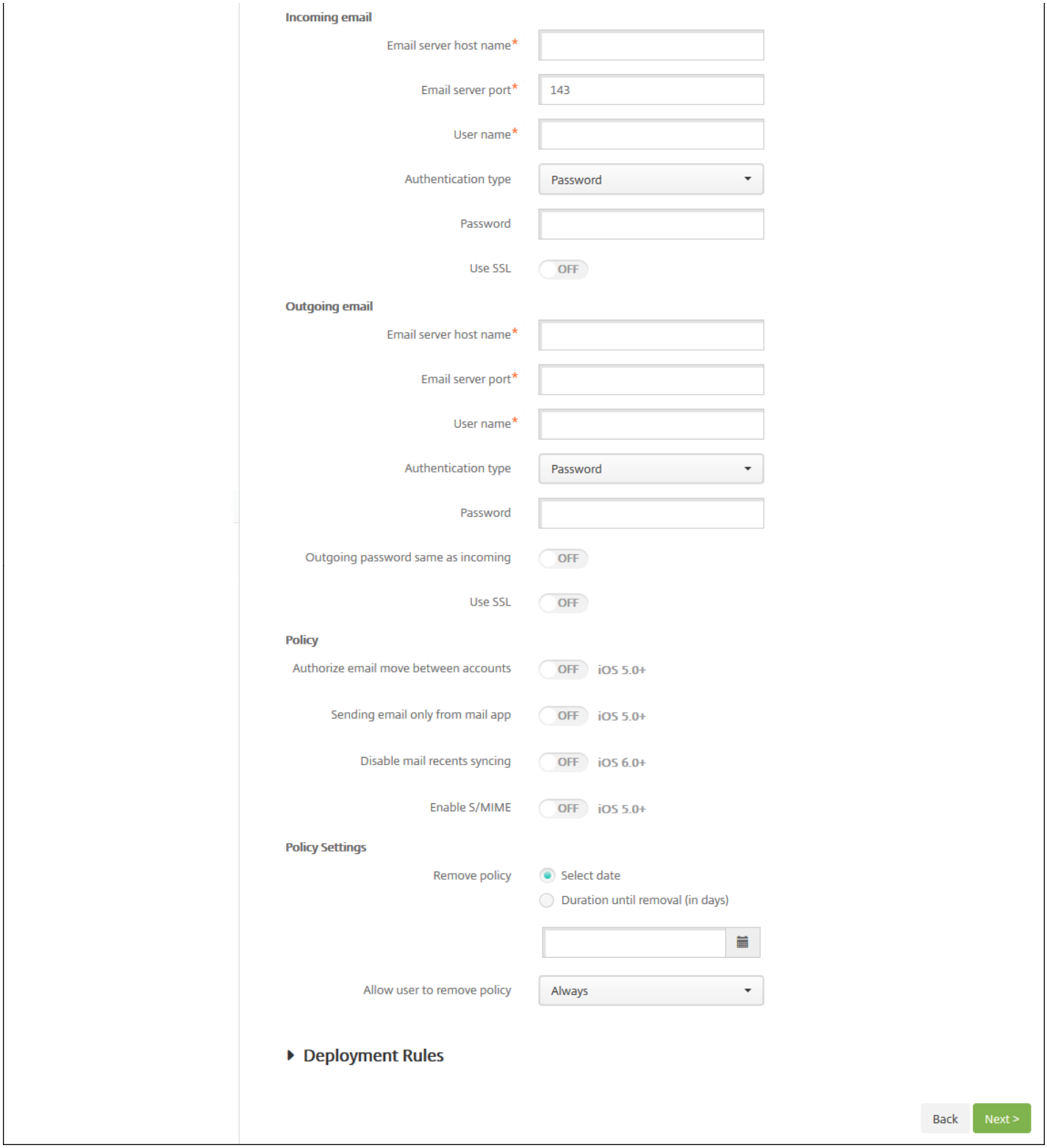


4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。［**Mail Policy Platforms**］ページが開きます。





6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順8.を参照してプラットフォームの展開規則を設定します。

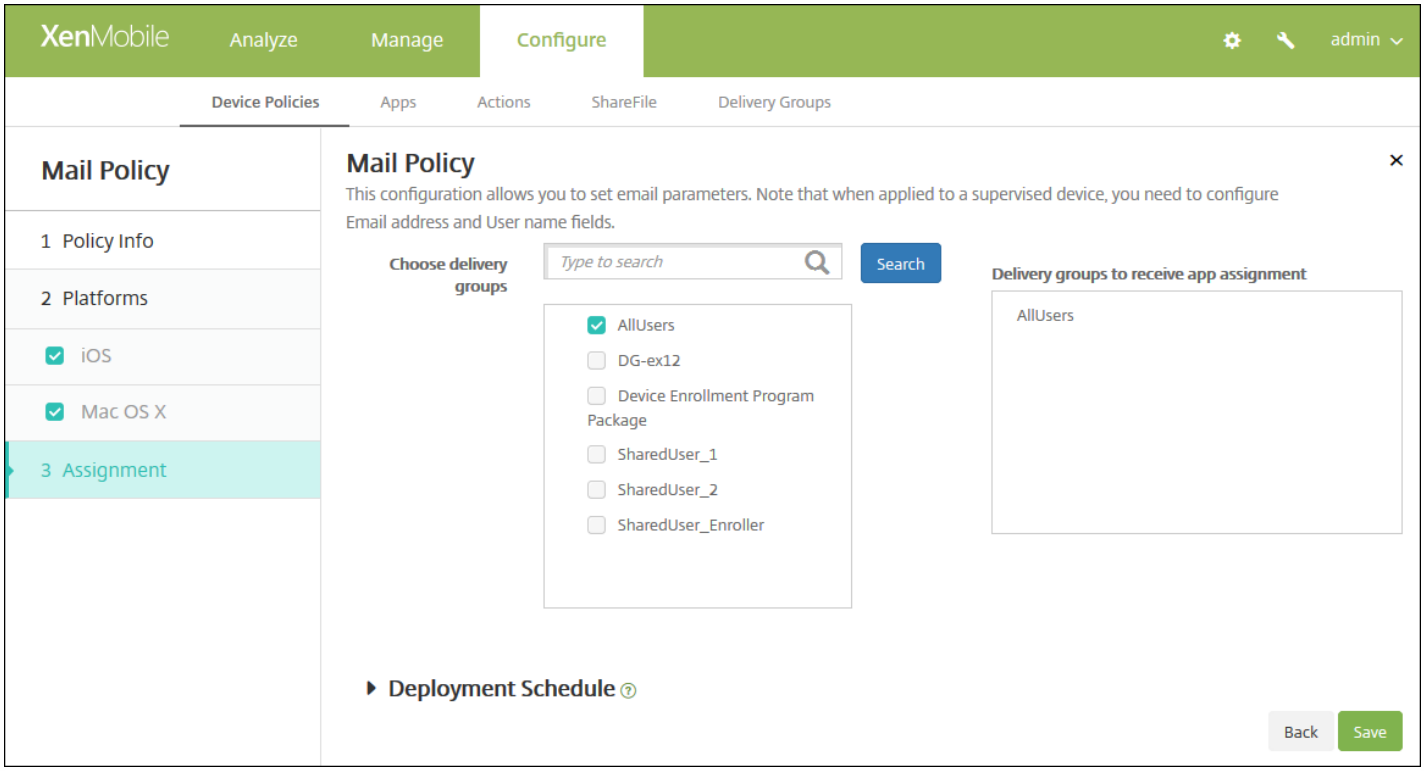
7. 選択したプラットフォームで次の設定を構成します。

- **Account description**：メールおよび設定アプリケーションに表示される、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。
- **Account type**：ボックスの一覧で［**IMAP**］または［**POP**］を選択し、ユーザーアカウントで使用するプロトコルを選択します。 デフォルトは［**IMAP**］です。 ［**POP**］を選択した場合、以下の［**Path prefix**］オプションは表示されなくなります。
- **Path prefix**：**INBOX**、または**INBOX**ではない場合は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。
- **User display name**：メッセージなどで使用する完全な ユーザー名 を入力します。 このフィールドは必須です。
- **Email address**：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**
  - **Email server host name**：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。
  - **Email server port**：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。
  - **User name**：メールアカウントの ユーザー名 を入力します。 この名前は一般的に、ユーザーのメールアドレスの@記号より前の部分と同じです。 このフィールドは必須です。
  - **Authentication type**：ボックスの一覧で、使用する認証の種類を選択します。 デフォルトは［**Password**］です。 ［**None**］を選択した場合、以下の［**Password**］フィールドは表示されなくなります。
  - **Password**：任意で、受信メールサーバーのパスワードを入力します。
  - **Use SSL**：受信メールサーバーでSSL（Secure Socket Layer）認証を使用するかどうかを選択します。 デフォルトは［**OFF**］です。
- **送信メール設定**
  - **Email server host name**：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。
  - **Email server port**：送信メールサーバーのポート番号を入力します。 ポート番号を入力しなかった場合、指定されたプロトコルのデフォルトポートが使用されます。
  - **User name**：メールアカウントの ユーザー名 を入力します。 これは一般的に、ユーザーのメールアドレスの@記号より前の部分と同じです。 このフィールドは必須です。
  - **Authentication type**：ボックスの一覧で、使用する認証の種類を選択します。 デフォルトは［**Password**］です。 ［**None**］を選択した場合、以下の［**Password**］フィールドは表示されなくなります。
  - **Password**：任意で、送信メールサーバーのパスワードを入力します。
  - **Outgoing password same as incoming**：受信パスワードと送信パスワードが同じであるかどうかを選択します。 デフォルトは［OFF］で、パスワードが異なることを意味します。 ［**ON**］に設定した場合、直前の［**Password**］フィールドは表示されなくなります。
  - **Use SSL**：送信メールサーバーでSSL（Secure Socket Layer）認証を使用するかどうかを選択します。 デフォルトは［**OFF**］です。
- **ポリシー**
  - **注：**iOSの設定を構成する場合、これらのオプションはiOS 5.0以降にのみ適用されます。Mac OS Xを構成する場合、制限はありません。
  - **Authorize email move between accounts**：ユーザーが 電子メール をこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。 デフォルトは［**OFF**］です。
  - **Sending email only from mail app**：ユーザーの 電子メールの送信をiOSメールアプリケーションからのみに制限するかどうかを選択します。
  - **Disable mail recents syncing**：ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。 デフォルトは［**OFF**］です。 このオプションはiOS 6.0以降にのみ適用されます。
  - **Enable S/MIME**：このアカウントでS/MIME認証および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］に設定した場合、以下の2つのフィールドが表示されます。
  - **Signing identity credential**：ボックスの一覧で、使用する署名資格情報を選択します。
  - **Encryption identity credential**：ボックスの一覧で、使用する暗号化資格情報を選択します。
- **ポリシー設定**
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］を選択します。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、 ［**Always**］、 ［**Password required**］、 ［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、 ［**Removal password**］の横に必要なパスワードを入力します。
  - **Deployment scope**：一覧から、 ［**User**］または［**System**］を選択します。 デフォルトは［**User**］です。 このオプションはMax OS X 10.7以降でのみ使用できます。

8. 展開規則の構成

9. ［**Next**］をクリックします。 ［**Mail Policy**］割り当てページが開きます。



10. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［**Delivery groups to receive app assignment**］一覧に表示されます。

11. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment**

has failed］をクリックします。 デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、［**Settings**］>［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

12. ［**Save**］をクリックしてポリシーを保存します。

管理対象ドメインデバイスポリシー

Aug 02, 2016

メールおよびSafariブラウザーに適用する管理対象ドメインを定義できます。 管理対象ドメインを使用すると、Safariを使用してドメインからダウンロードしたドキュメントを開くことができるアプリケーションを制御して、会社のデータを保護することができます。 URLまたはサブドメインを使用して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御します。 このポリシーは、iOS 8以降の監視対象デバイスでのみサポートされます。 iOSデバイスをSupervisedモードに設定する手順については、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

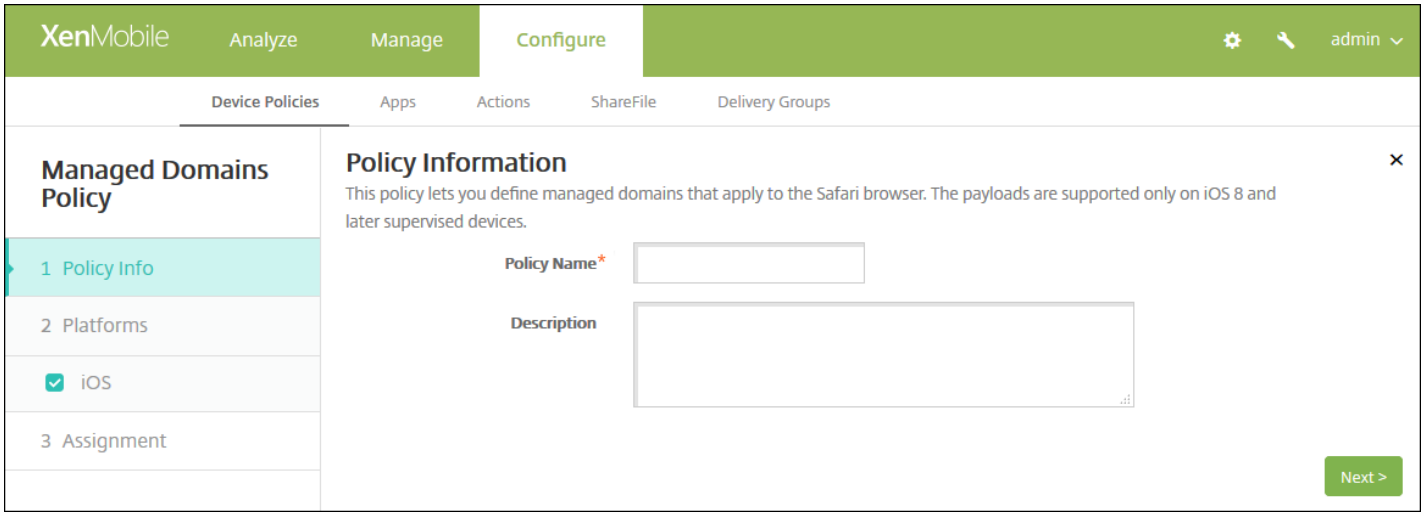
ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。

ユーザーがSafariを使用して、管理対象Webドメイン一覧に含まれているWebドメインから取得したアイテム（ドキュメントや添付ファイルなど、ダウンロードしたもの）を開こうとすると、適切な社内アプリケーションによってアイテムが開かれます。 アイテムが管理対象Webドメイン一覧にあるWebドメインから取得されたものでない場合、ユーザーは社内アプリケーションでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリケーションを使用する必要があります。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add New Policy**］ダイアログボックスが開きます。

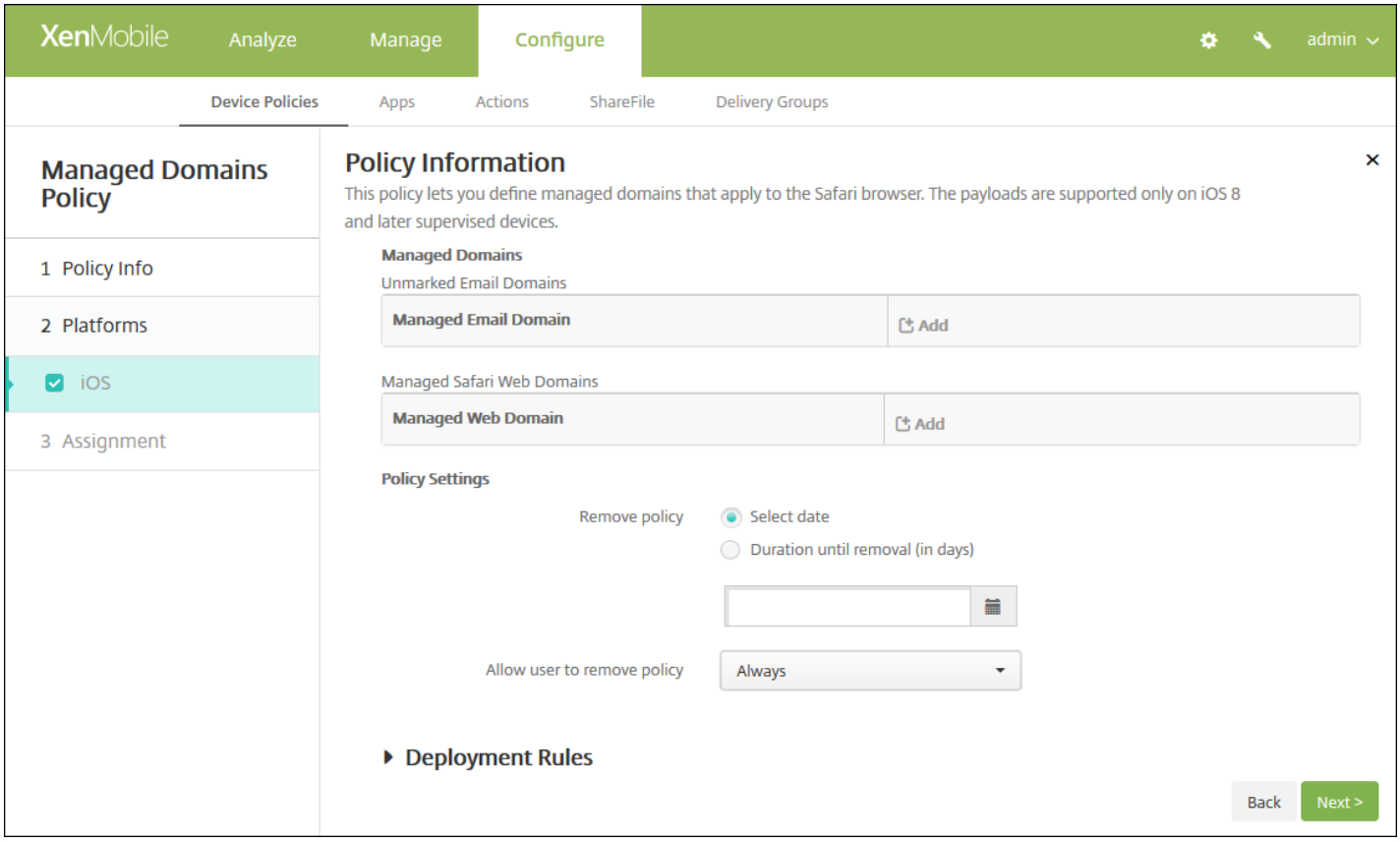
3. ［**More**］を展開した後、［**Security**］の下の［**Managed domains**］をクリックします。 ［**Managed Domains Policy**］情報ページが開きます。



4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**iOS Platform**］ページが開きます。



ドメインを指定する方法

6. 次の設定を構成します。

- **管理対象ドメイン**
  - **Unmarked Email Domains**：一覧に含めるメールドメインごとに、**[Add]** をクリックして以下の操作を行います。
    - **Managed Email Domain**：メールドメインを入力します。
    - **[Save]** をクリックしてメールドメインを保存するか、**[Cancel]** をクリックして操作を取り消します。
  - **Managed Safari Web Domains**：一覧に含めるWebドメインごとに、**[Add]** をクリックして以下の操作を行います。
    - **Managed Web Domain**：Webドメインを入力します。
    - **[Save]** をクリックしてWebドメインを保存するか、**[Cancel]** をクリックして操作を取り消します。

      注：既存のドメインを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

      既存のドメインを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

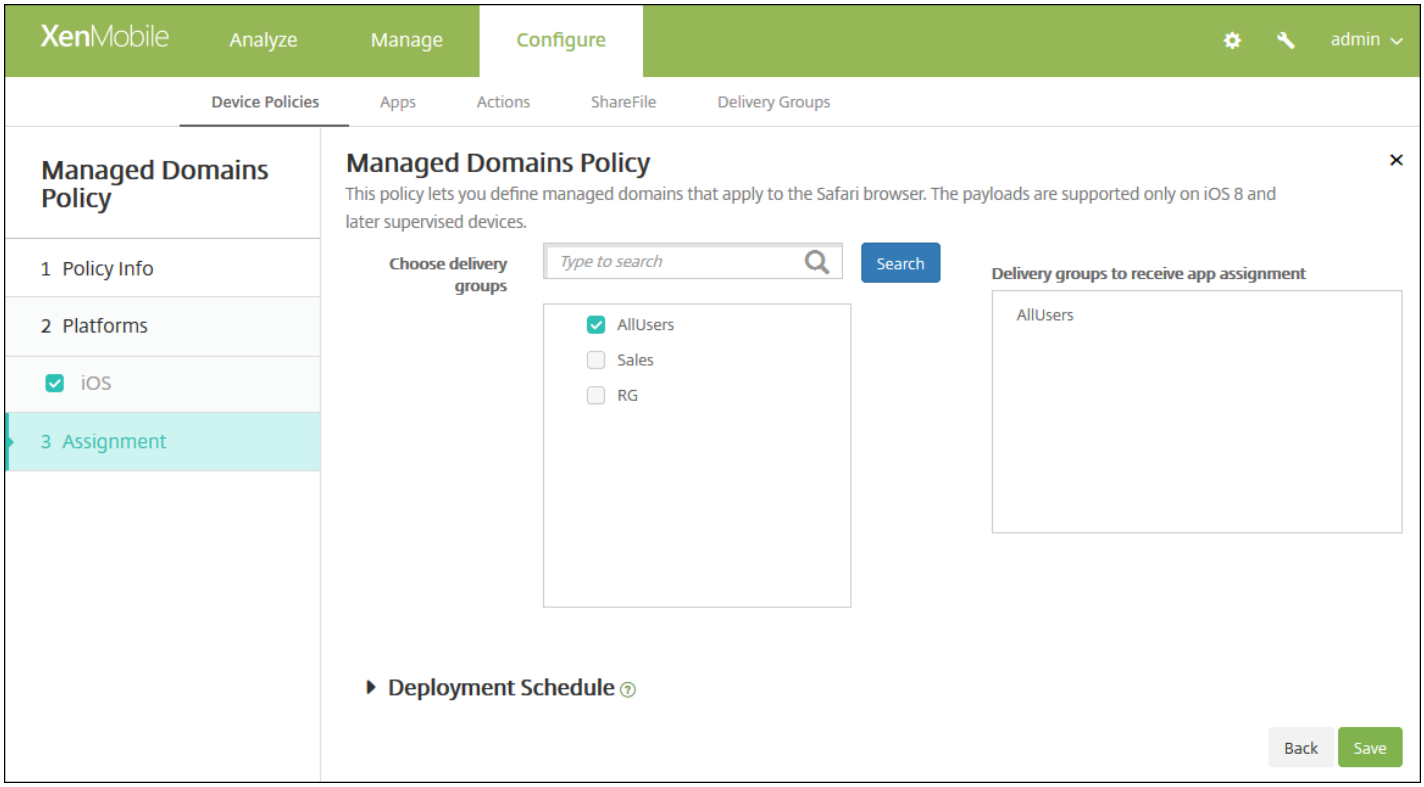
- **ポリシー設定**
  - **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択しま

す。

- ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Managed Domains Policy**］割り当てページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。 デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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］です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

11. **[Save]** をクリックします。

MDMオプションデバイスポリシー

Aug 02, 2016

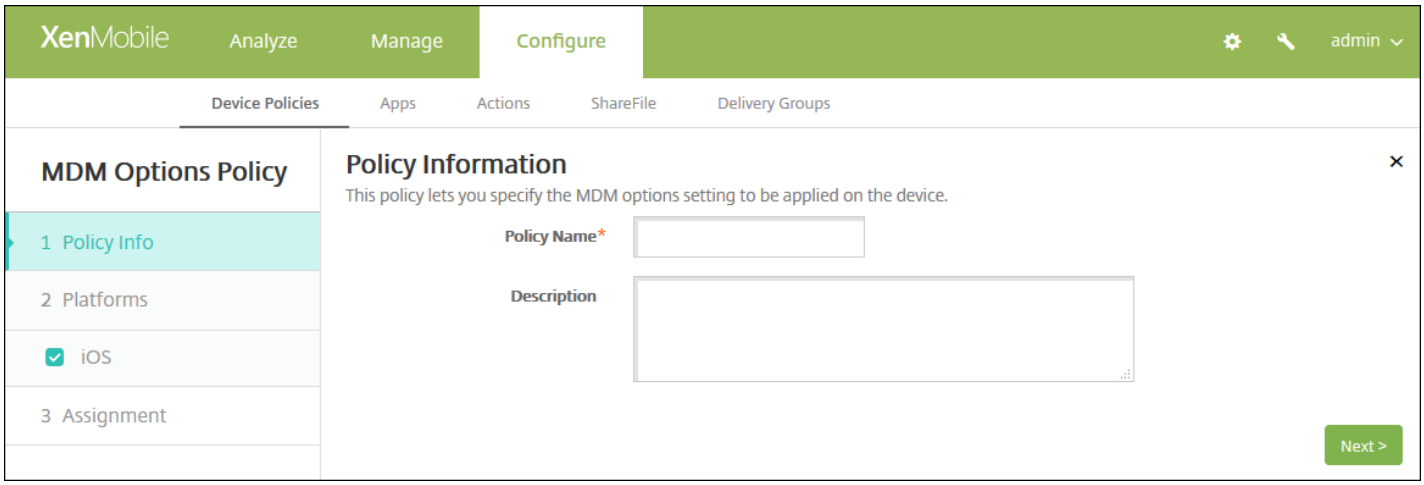
XenMobileでデバイスポリシーを作成して、監視対象のiOS 7.0以降のモバイルバイスで［iPhone/iPadを探す］の［アクティベーションロック］を管理することができます。 iOSデバイスをSupervisedモードに設定する手順については、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」または「iOSバルク登録」を参照してください。

アクティベーションロックは、紛失したり、盗まれたりしたデバイスが再アクティベーションされないようにすることを目的とした［iPhone/iPadを探す］の機能であり、ユーザーのApple IDおよびパスワードを必須にすることで、誰かが［iPhone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ションして使用したりするのを防ぎます。 XenMobileでは、MDMオプションデバイスポリシーでアクティベーションロックを有効にすることにより、必須とされているApple IDおよびパスワードの入力をバイパスできます。 ユーザーから返却されたデバイスで［iPhoneを探す］が有効になっていた場合、Appleの資格情報なしでXenMobileコンソールからデバイスを管理することができます。

1.XenMobileコンソールで、 **［Configure］の［Device Policies］**をクリックします。 **［Device Policies］**ページが開きます。

2. **［Add］**をクリックします。 **［Add a New Policy］**ダイアログボックスが開きます。

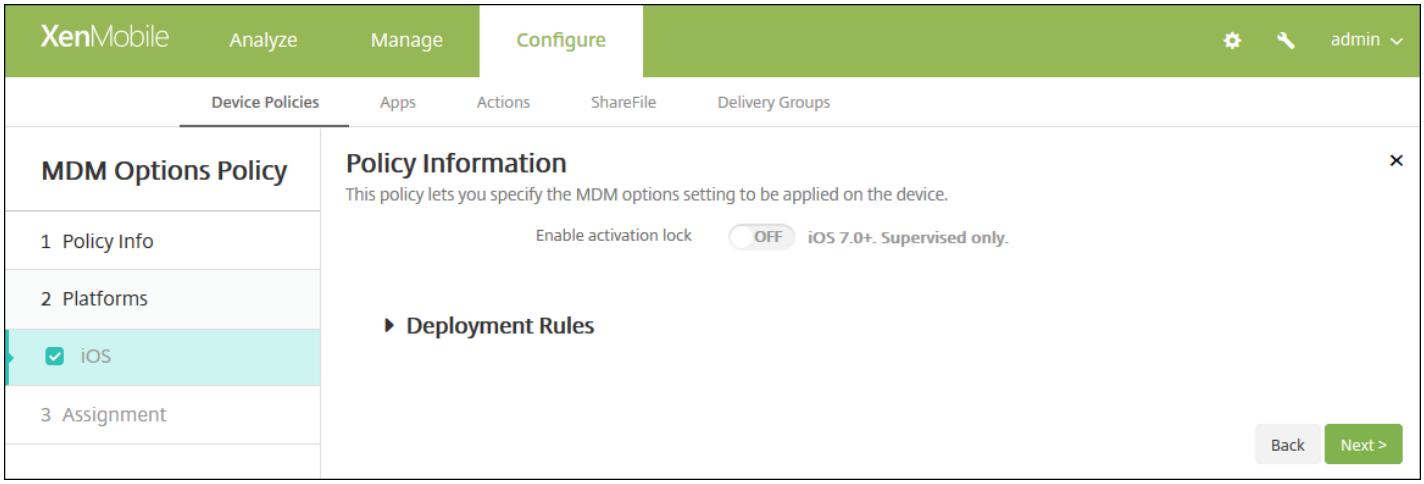
3. **［More］**を展開した後、 **［End user］**の下の**［MDM Options］**をクリックします。 **［MDM Options Policy］**情報ページが開きます。



4. **［Policy Information］**ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **［Next］**をクリックします。 **［iOS MDM Policy Platform］**ページが開きます。

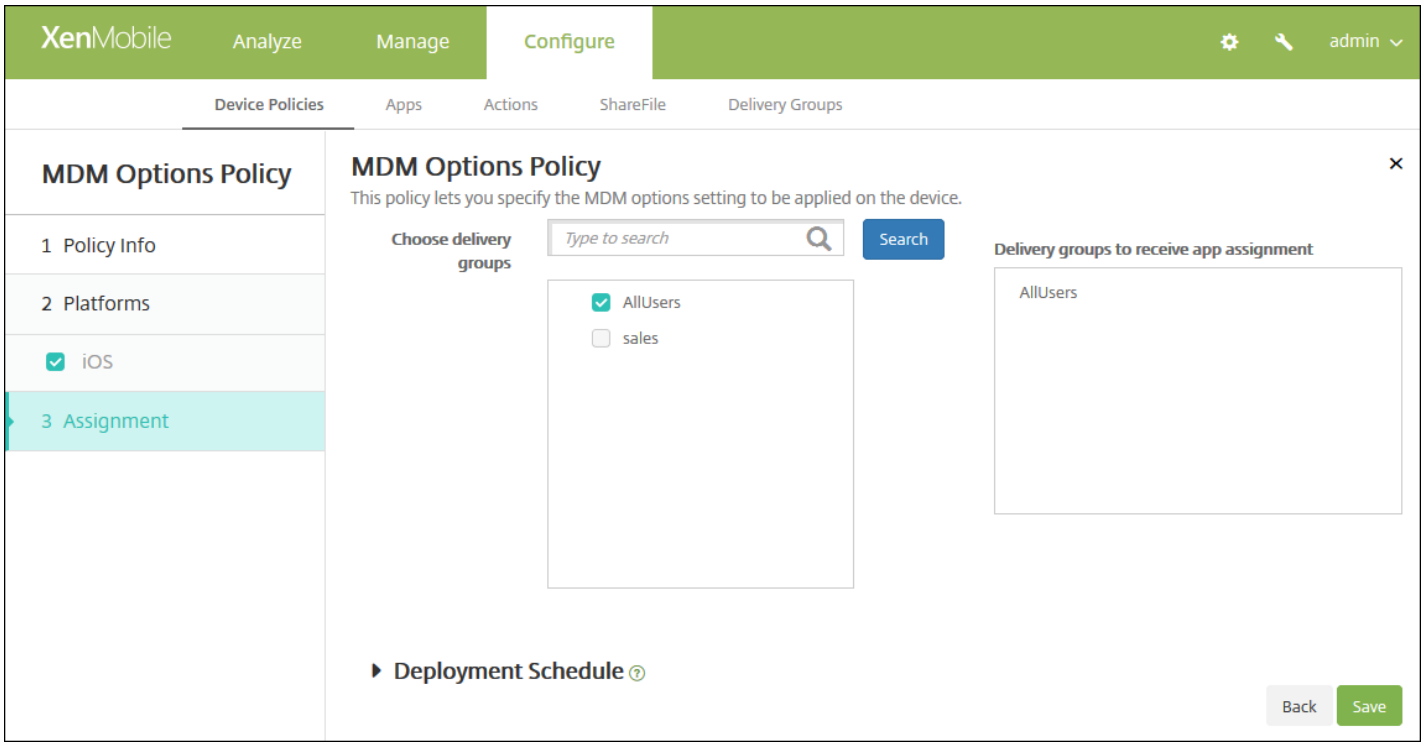


6. 次の設定を構成します。

- **Enable Activation Lock**：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 **[OFF]** です。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[MDM Options Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。

デフォルトのオプションは［**ON**］です。［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。

- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

11. ［**Save**］をクリックします。

Microsoft Exchange ActiveSyncデバイスポリシー

Aug 02, 2016

Exchange ActiveSyncデバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchangeでホストされている会社のメールにアクセスできるようにすることができます。 iOS、MAC OS X、Android HTC、Android TouchDown、Android for Work、Samsung SAFE、Samsung KNOX、Windows Phoneに対してポリシーを作成できます。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、以下のセクションで説明しています。

iOSの設定

Mac OS Xの設定

Android HTCの設定

Android TouchDownの設定

Android for Workの設定

Samsung SAFEおよびSamsung KNOXの設定

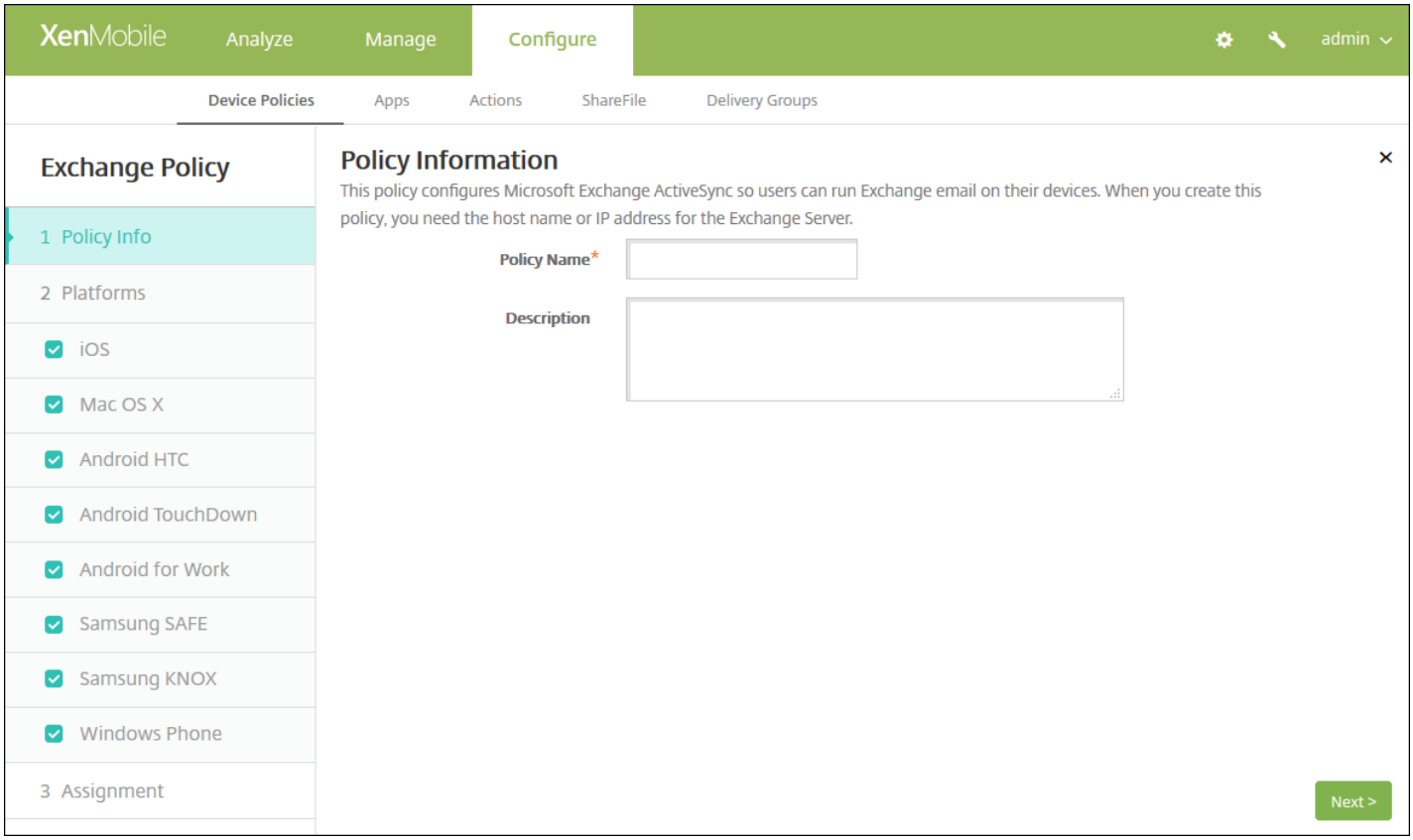
Windows Phoneの設定

このポリシーを作成するには、事前にExchange Serverの ホスト名 またはIPアドレスを把握しておく必要があります。

1.XenMobileコンソールで、 [**Configure**] の [**Device Policies**] をクリックします。 [**Device Policies**] ページが開きます。

2. [**Add**] をクリックします。 [**Add a New Policy**] ダイアログボックスが開きます。

3. [**Exchange**] をクリックします。 [**Exchange Policy**] 情報ページが開きます。



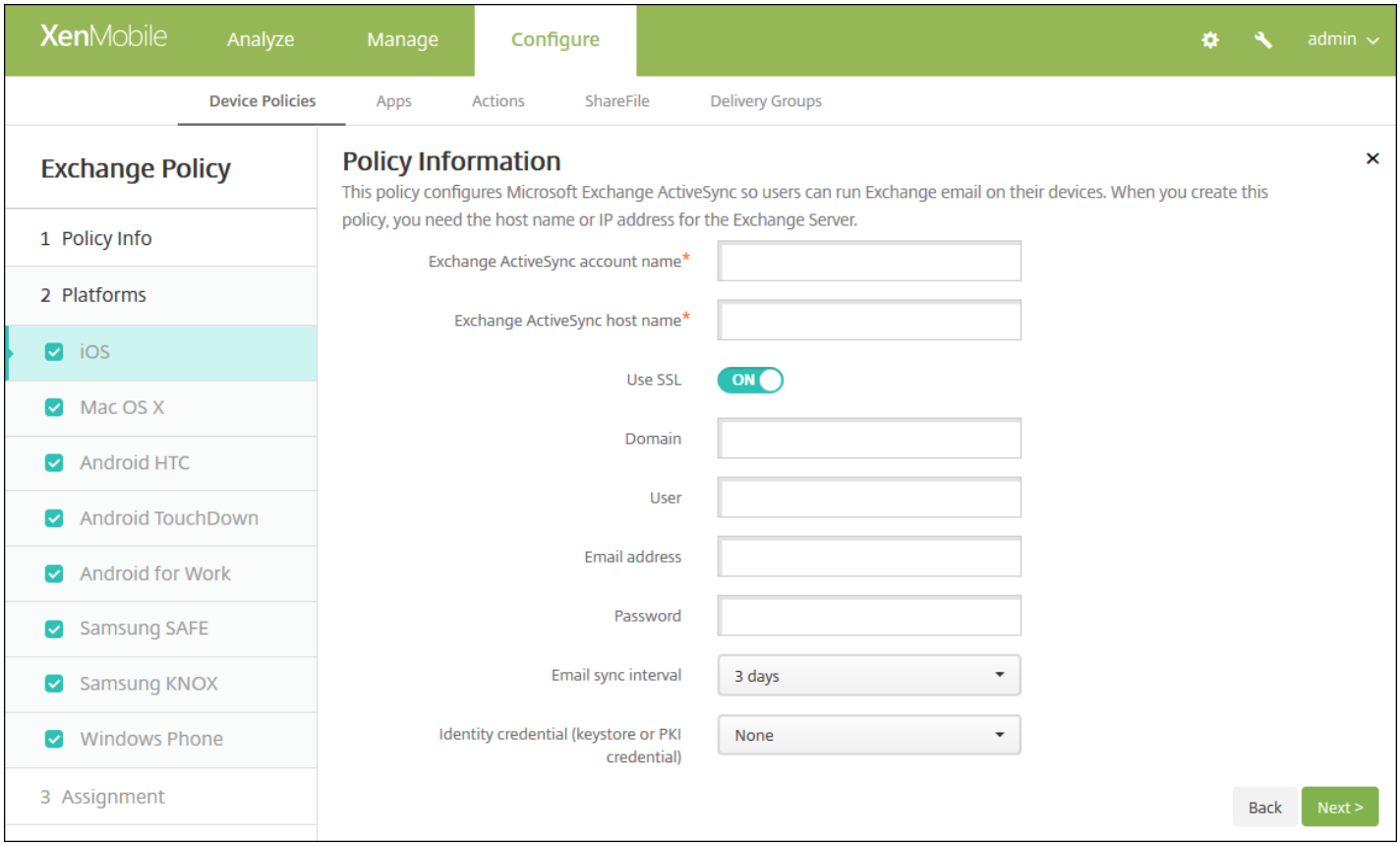
4. [**Policy Information**] ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成

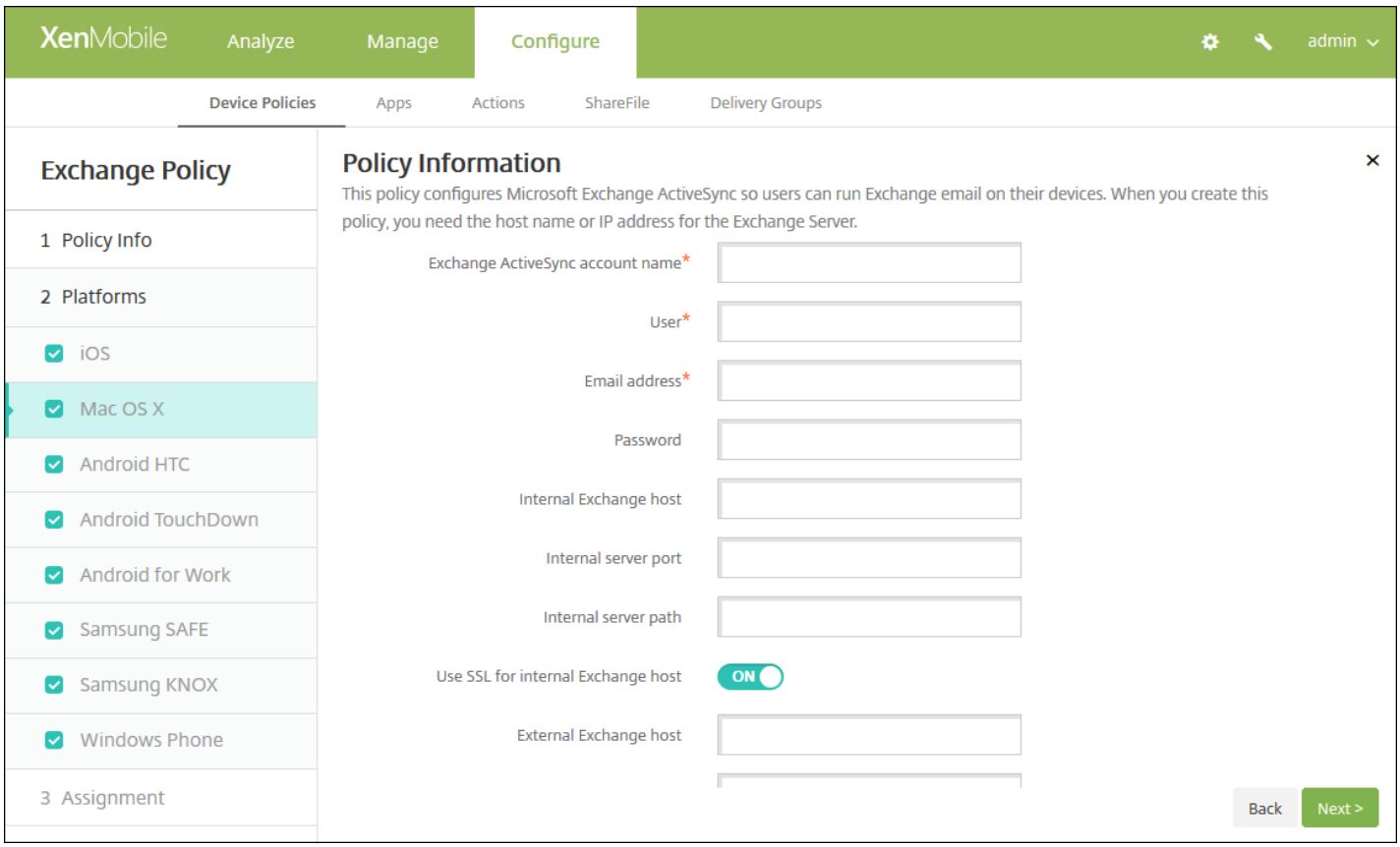


次の設定を構成します。

- **Exchange ActiveSync account name**：ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **Exchange ActiveSync host name**：メールサーバーのアドレスを入力します。
- **Use SSL**：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。 デフォルトは［**ON**］です。
- **Domain**：Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User**：Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address**：ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email sync interval**：一覧から、メールをExchange Serverと同期する頻度を選択します。 デフォルトは、［**3 days**］です。
- **Identity credential　(キーストア or PKI)**：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。 このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。 デフォルトは［**None**］です。
- **Authorize email move between accounts**：ユーザーが 電子メール をこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。 デフォルトは［**OFF**］です。
- **Send email only from email app**：ユーザーの電子メールの送信をiOSメールアプリケーションからのみに制限するかどうかを選択します。 デフォルトは［**OFF**］です。
- **Disable email recent syncing**：ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。 デフォルトは［**OFF**］です。 このオプションはiOS 6.0以降にのみ適用されます。

- **Enable S/MIME**：このアカウントでS/MIME認証および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**］に設定した場合、以下の2つのフィールドが表示されます。
  - **Signing identity credential**： デフォルトは［**None**］です。
  - **Encryption identity credential**： デフォルトは［**None**］です。
- **Enable per message S/MIME switch**：ユーザーがメッセージごとに送信メールを暗号化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。

Mac OS Xの設定の構成

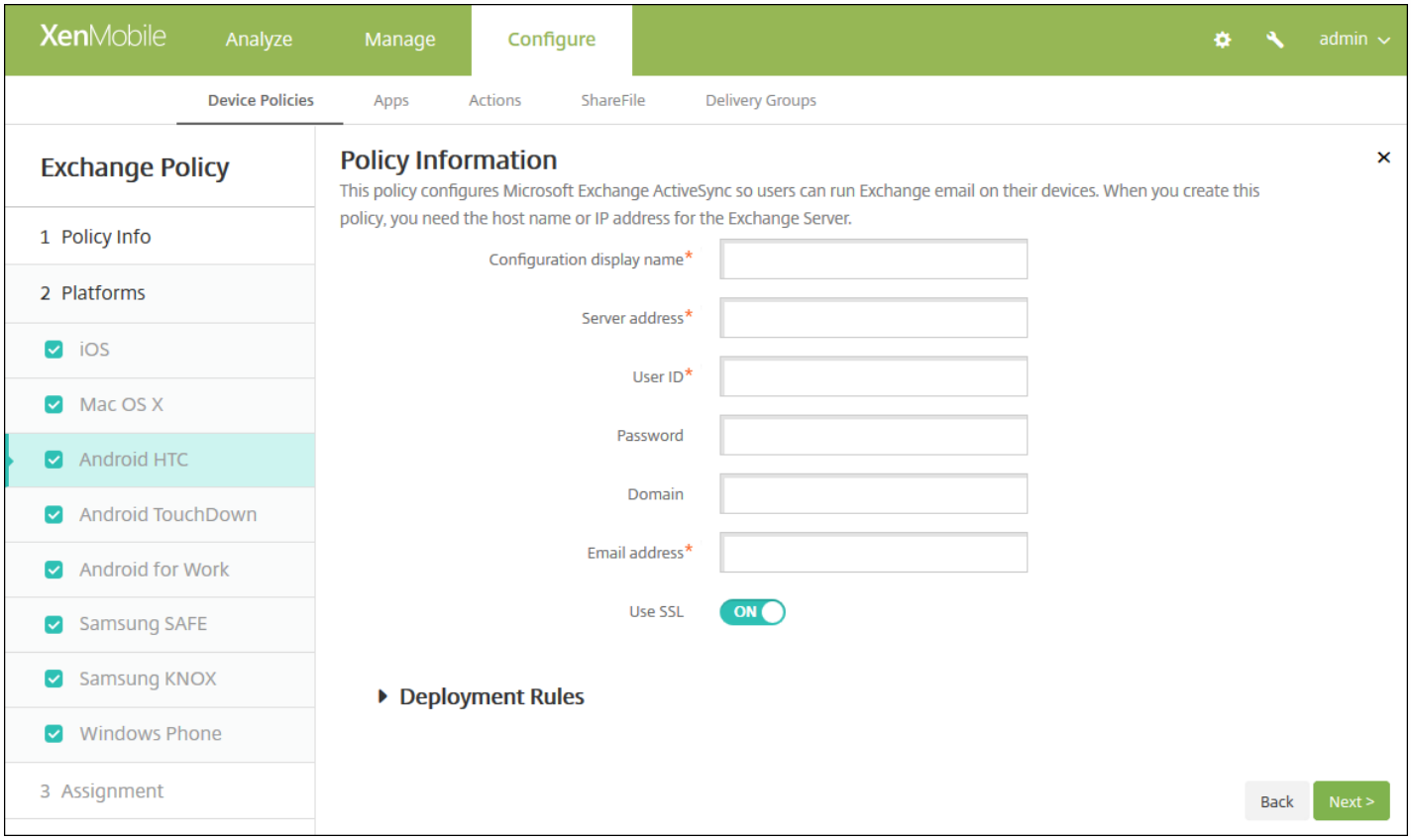


次の設定を構成します。

- **Exchange ActiveSync account name**：ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **User**：Exchangeユーザーアカウントのユーザー名を指定します。 このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address**：ユーザーの完全なメールアドレスを指定します。 このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Internal Exchange host**：Exchangeのホスト名を内部と外部で別のものにする場合、任意で内部のExchangeホスト名を入力します。
- **Internal server port**：Exchangeのサーバーポートを内部と外部で別のものにする場合、任意で内部のExchangeサーバーのポート番号を入力します。
- **Internal server path**：Exchangeのサーバーパスを内部と外部で別のものにする場合、任意で内部のExchangeサーバーパスを入力します。
- **Use SSL for internal Exchange host**：ユーザーのデバイスと内部のExchangeホスト間の接続をセキュリティで保護するかどうかを選択します。 デフォルトは［**ON**］です。

- **External Exchange host**：Exchangeのホスト名を内部と外部で別のものにする場合、任意で外部のExchangeホスト名を入力します。
- **External server port**：Exchangeのサーバーポートを内部と外部で別のものにする場合、任意で外部のExchangeサーバーのポート番号を入力します。
- **External server path**：Exchangeのサーバーパスを内部と外部で別のものにする場合、任意で外部のExchangeサーバーパスを入力します。
- **Use SSL for external Exchange host**：ユーザーのデバイスと外部のExchangeホスト間の接続をセキュリティで保護するかどうかを選択します。 デフォルトは **[ON]** です。
- **Allow Mail Drop**：ユーザーが2台のMac間で、既存のネットワークに接続することなくワイヤレスでファイルを共有できるようにするかどうかを選択します。 デフォルトは **[OFF]** です。

Android HTCの設定の構成

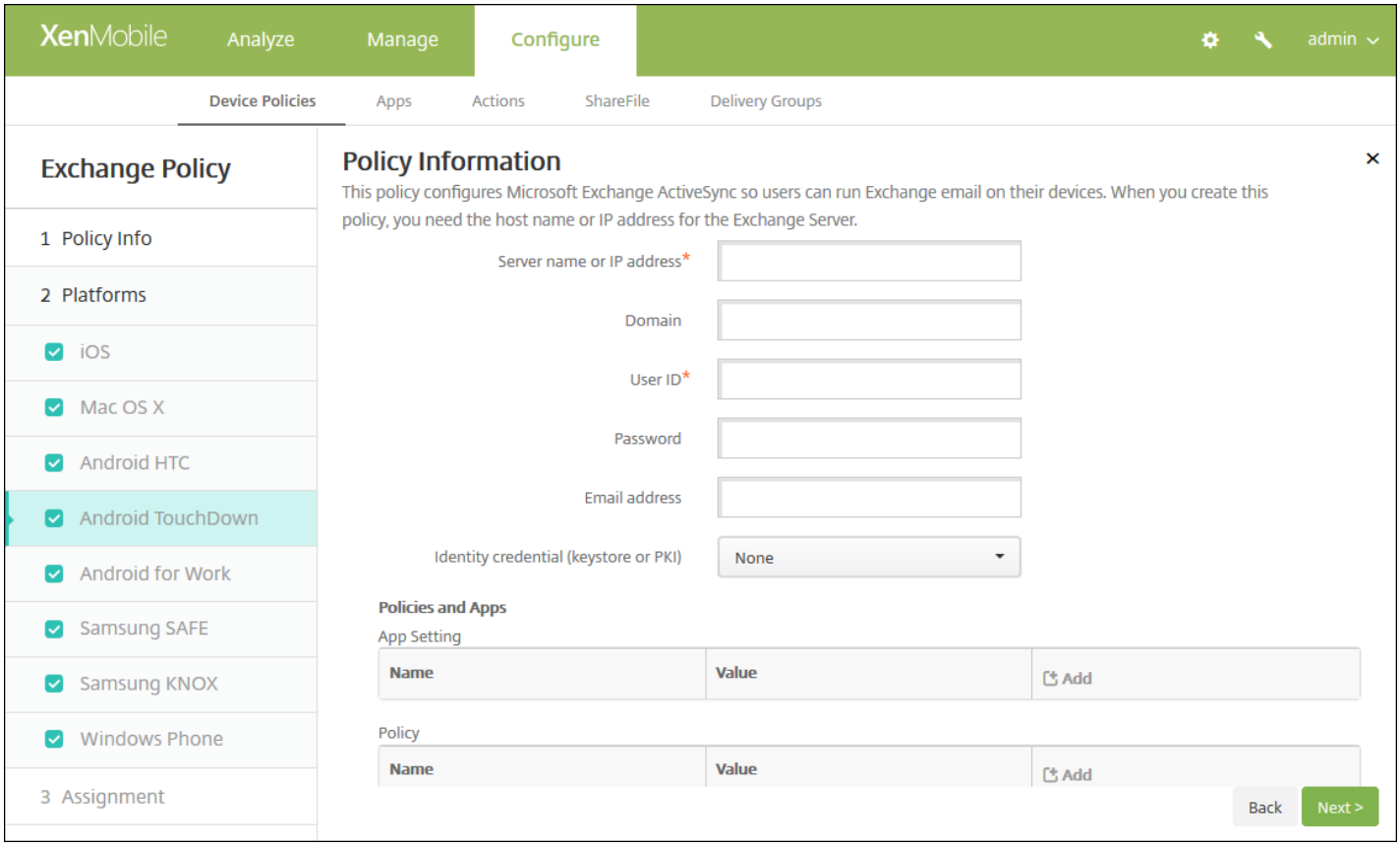


次の設定を構成します。

- **Configuration display name**：ユーザーのデバイスで表示される、このポリシーの名前を入力します。
- **Server address**：Exchange Serverの ホスト名 またはIPアドレスを入力します。
- **User ID**：Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Domain**：Exchange Serverがあるドメインを入力します。 このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **Email address**：ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Use SSL**：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。 デフォルト

は［**ON**］です。

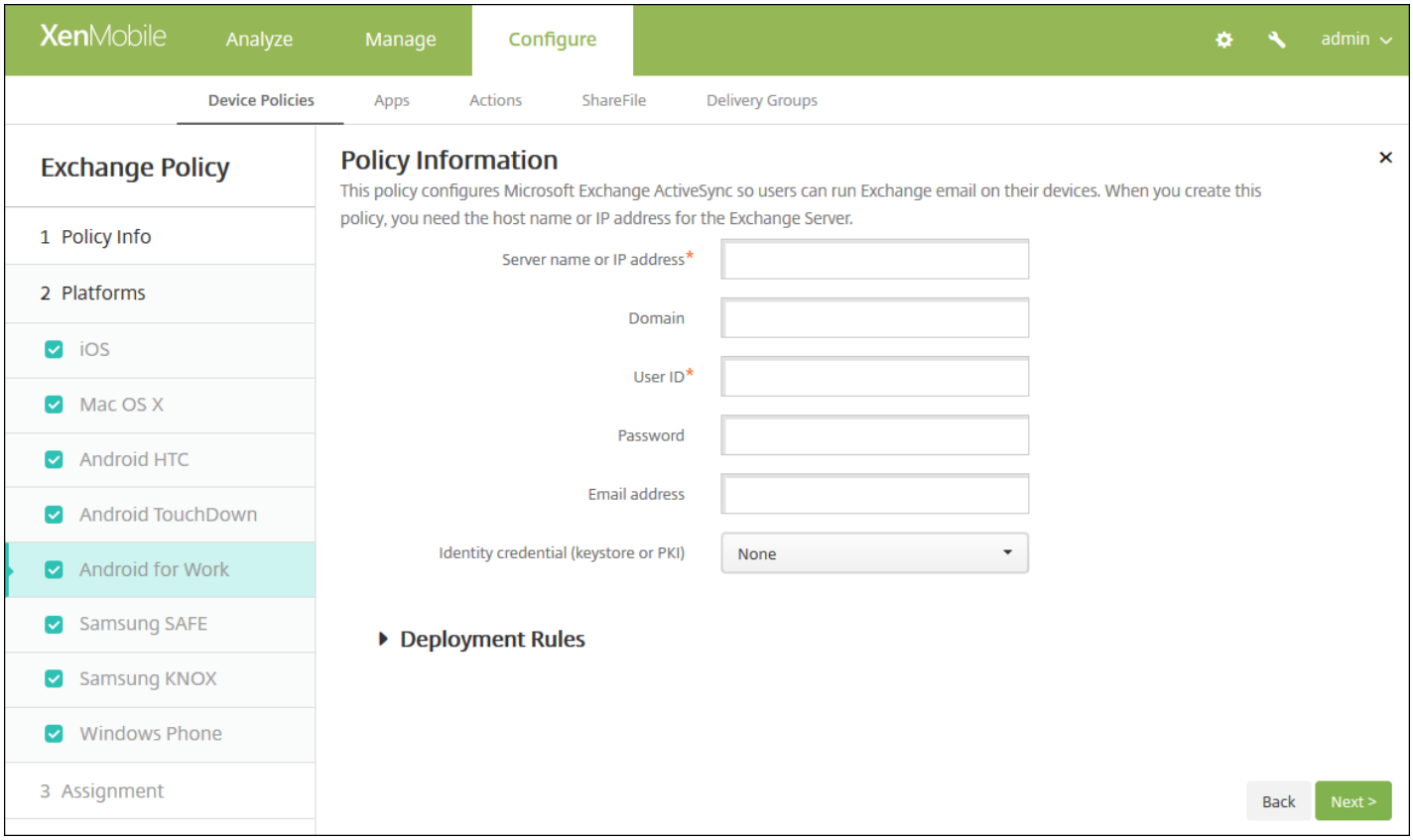
Android TouchDownの設定の構成



次の設定を構成します。

- **Server name or IP address**：Exchange Serverの ホスト名 またはIPアドレスを入力します。
- **Domain**：Exchange Serverがあるドメインを入力します。 このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID**：Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address**：ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Identity credential　(キーストア or PKI)**：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。 このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。 デフォルトは［**None**］です。
- **App Setting**：オプションで、このポリシーのTouchDownアプリケーション設定を追加します。
- **Policy**：オプションで、このポリシーのTouchDownポリシーを追加します。

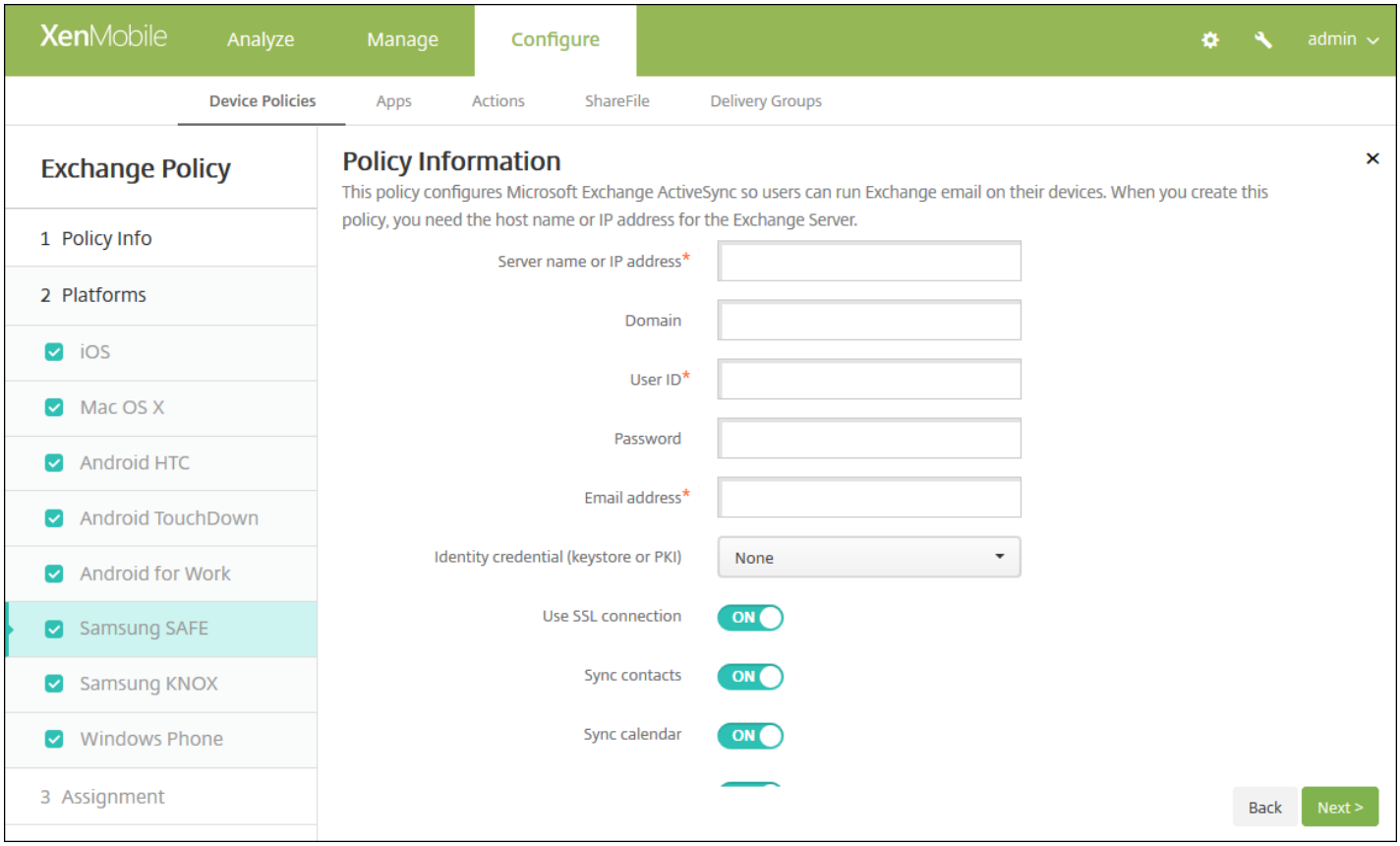
Android for Workの構成



次の設定を構成します。

- **Server name or IP address**：Exchange Serverの ホスト名 またはIPアドレスを入力します。
- **Domain**：Exchange Serverがあるドメインを入力します。 このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID**：Exchangeユーザーアカウントのユーザー名を指定します。 このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address**：ユーザーの完全なメールアドレスを指定します。 このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Identity credential　(キーストア or PKI)**：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。 このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。 デフォルトは［**None**］です。

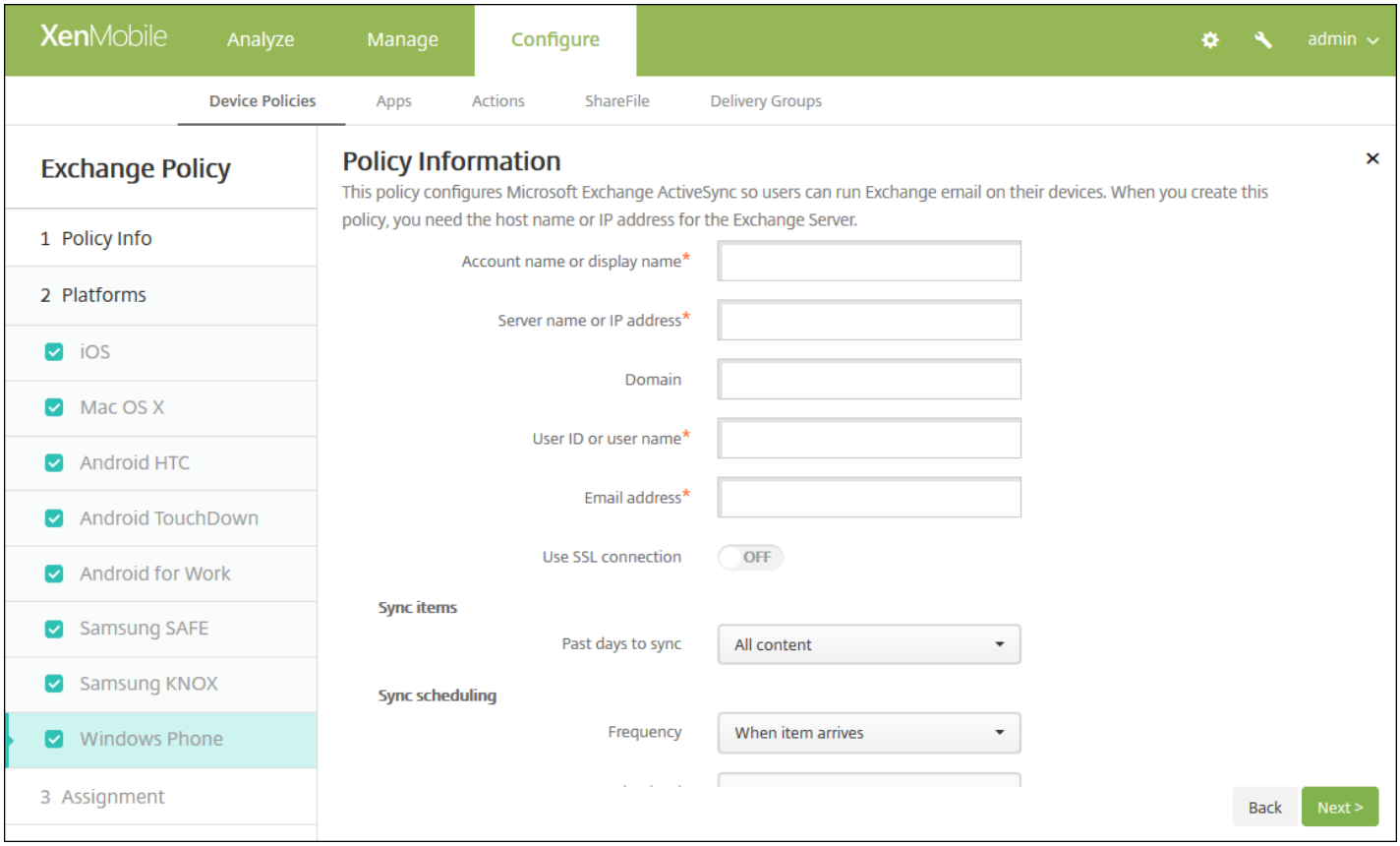
Samsung SAFEおよびSamsung KNOXの設定の構成



次の設定を構成します。

- **Server name or IP address**：Exchange Serverの ホスト名 またはIPアドレスを入力します。
- **Domain**：Exchange Serverがあるドメインを入力します。 このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID**：Exchangeユーザーアカウントのユーザー名を指定します。 このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password**：任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address**：ユーザーの完全なメールアドレスを指定します。 このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Identity credential　(キーストア or PKI)**：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。 このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。
- **Use SSL connection**：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは **[ON]** です。
- **Sync contacts**：デバイスとExchange Serverの間でユーザーのアドレス帳を同期できるようにするかどうかを選択します。 デフォルトは **[ON]** です。
- **Sync calendar**：デバイスとExchange Serverの間でユーザーのカレンダーを同期できるようにするかどうかを選択します。デフォルトは **[ON]** です。
- **デフォルト account**： ユーザーのExchangeアカウントをデバイスから送信するメールのデフォルトにするかどうかを選択します。 デフォルトは **[ON]** です。

Windows Phoneの設定の構成



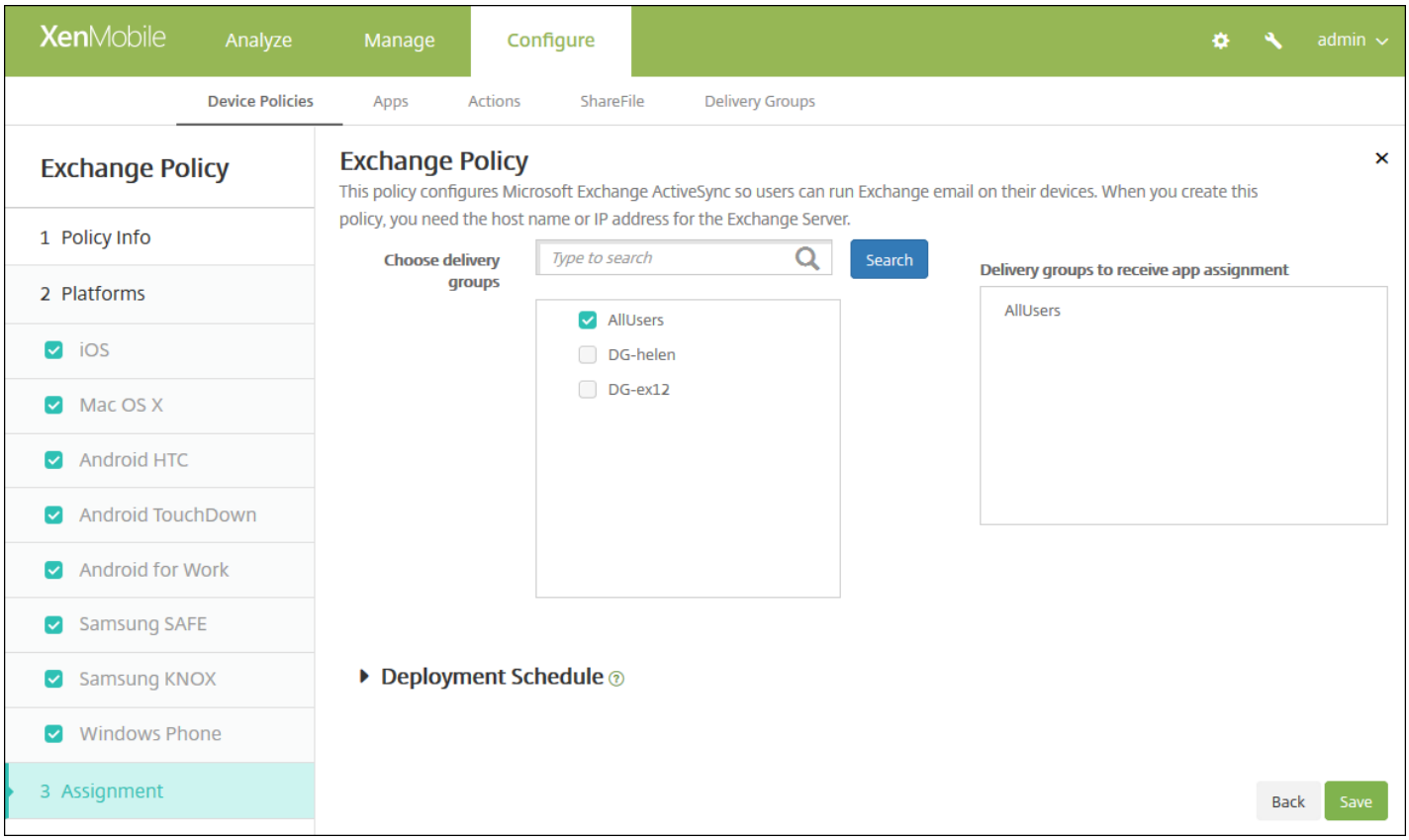
次の設定を構成します。

注：このポリシーを使ってユーザーパスワードを設定することはできません。 ユーザーはポリシーがプッシュされた後に、デバイスでパラメーターを設定する必要があります。

- **Account name or display name**：Exchange ActiveSyncアカウント名を入力します。
- **Server name or IP address**：Exchange Serverのホスト名またはIPアドレスを入力します。
- **Domain**：Exchange Serverがあるドメインを入力します。 このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID or user name**：Exchangeユーザーアカウントのユーザー名を指定します。 このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address**：ユーザーの完全なメールアドレスを指定します。 このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Use SSL connection**：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。 デフォルトは **[OFF]** です。
- **Past days to sync**：ボックスの一覧で、デバイス上のすべてのコンテンツをExchange Serverと過去にさかのぼって同期する日数を選択します。 デフォルトは **[All content]** です。
- **Frequency**：ボックスの一覧で、Exchange Serverからデバイスへ送信されるデータの同期に使用するスケジュールを選択します。 デフォルトは **[When it arrives]** です。
- **Logging level**：ボックスの一覧で、 **[Disabled]** 、 **[Basic]** 、または **[Advanced]** を選択して、Exchangeのアクティビティをログ記録する詳細レベルを指定します。 デフォルトは **[Disabled]** です。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[Exchange Policy]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

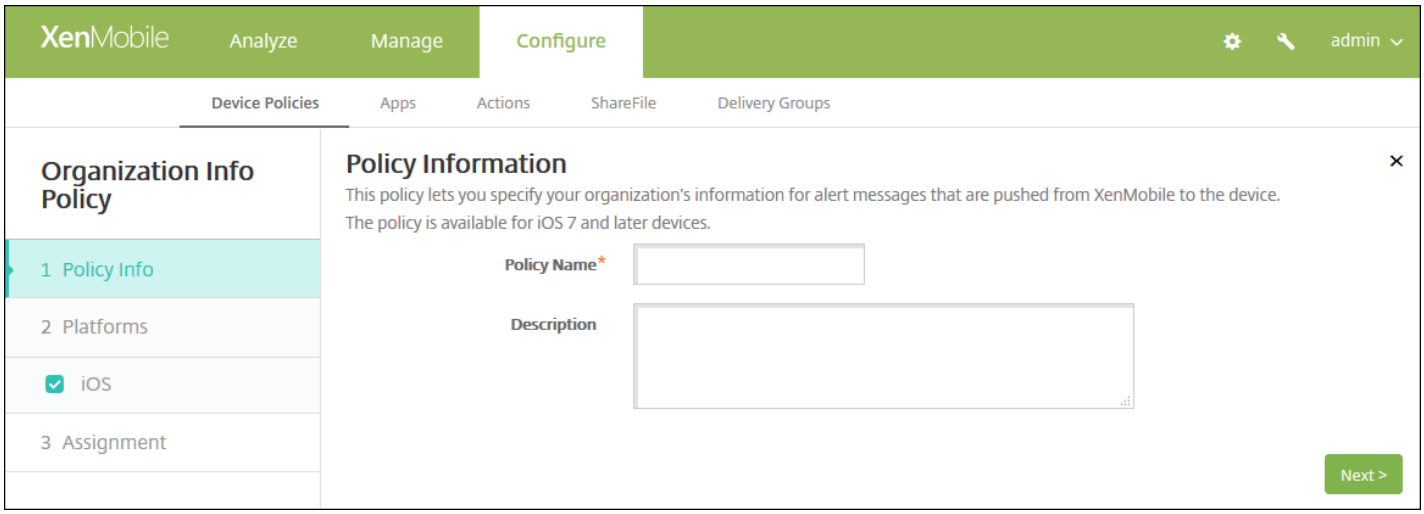
10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

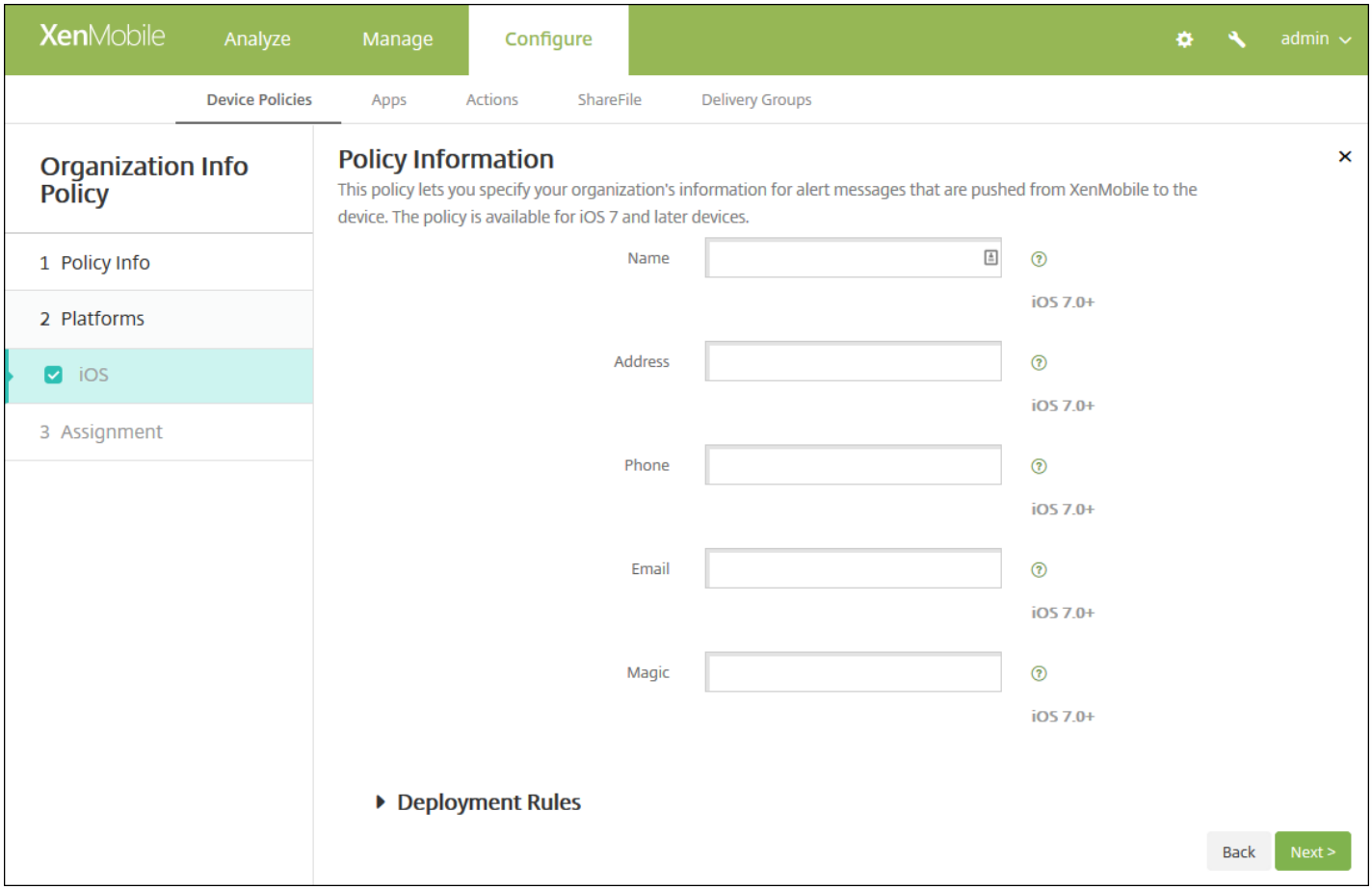
注：

- このオプションは、[**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

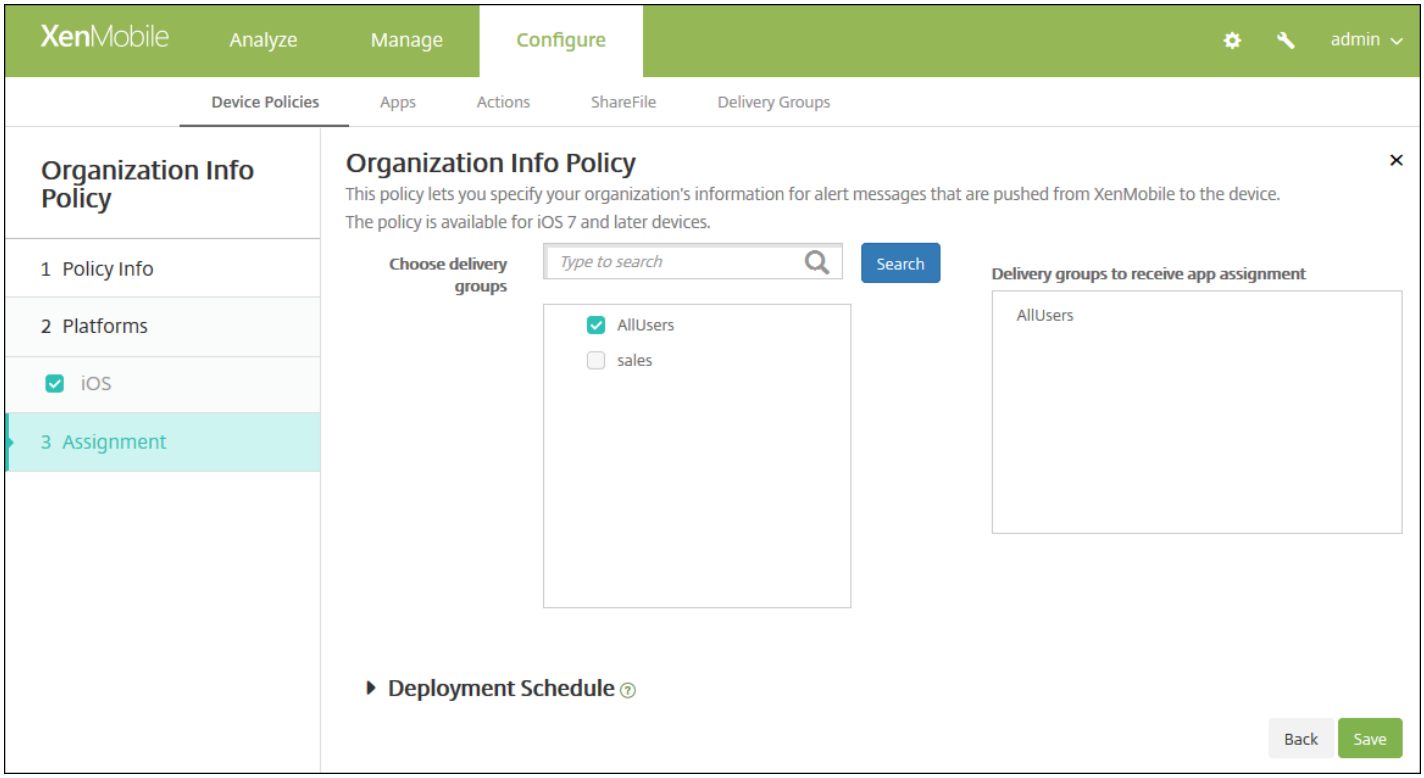
11. [**Save**] をクリックします。



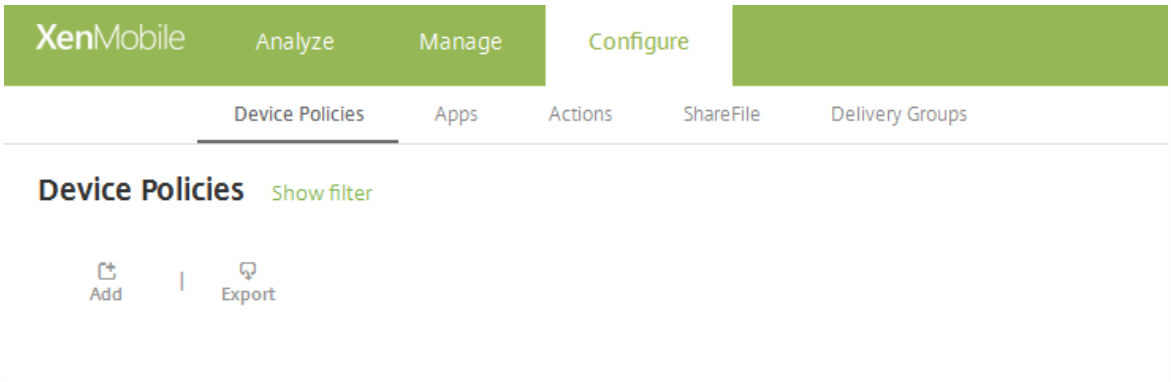
-
-

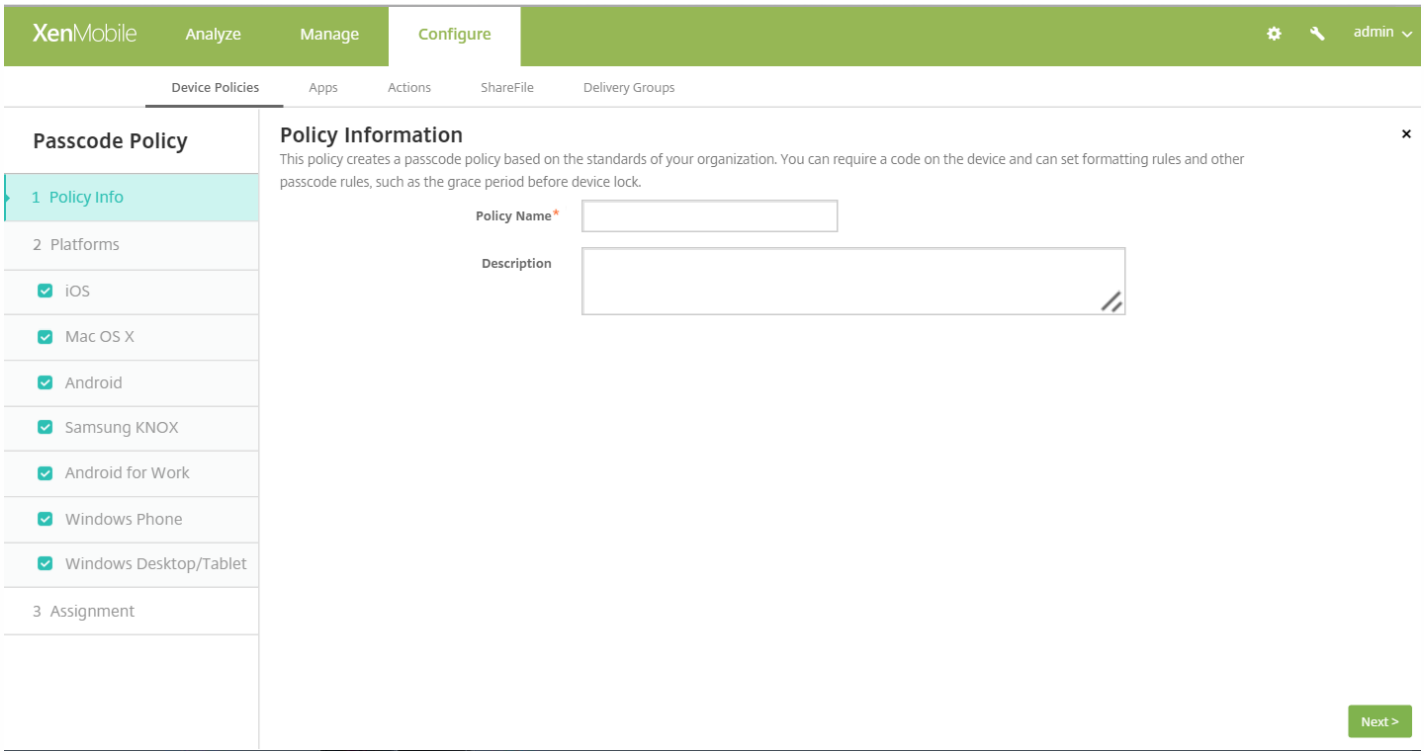


-
-
-
-
-



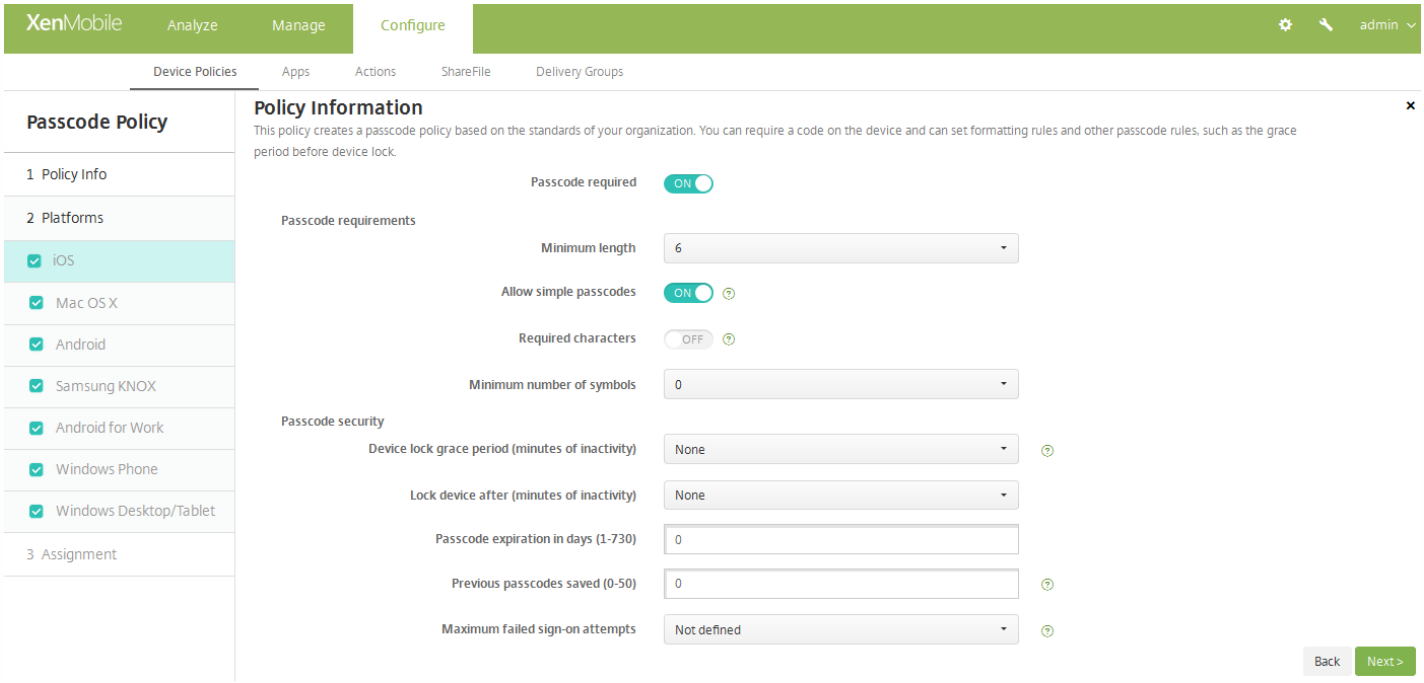
-
-
-
-
-
-
-





-
-

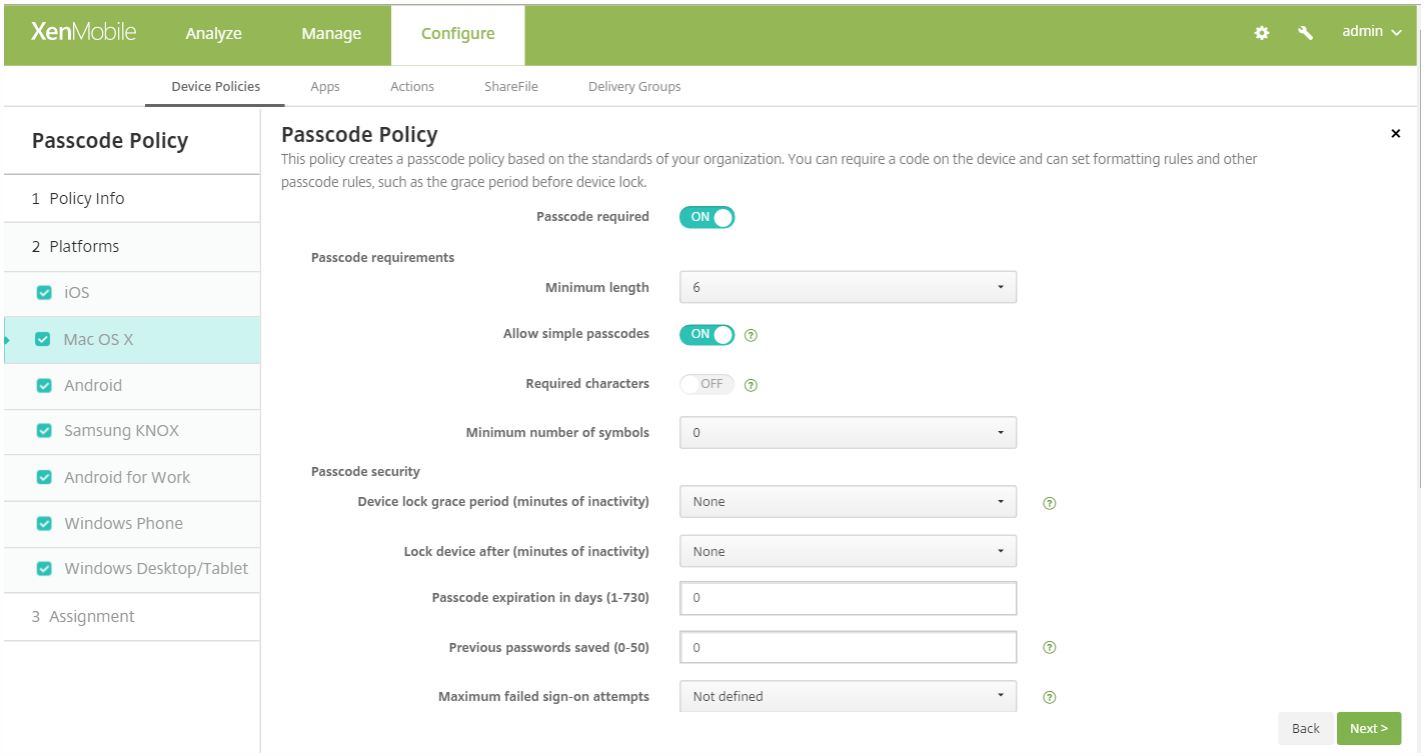
iOSの設定の構成



-
-
  -
  -
  -
  -
-
  -
  -
  -
  -
  -
-
  -
  -

-
-

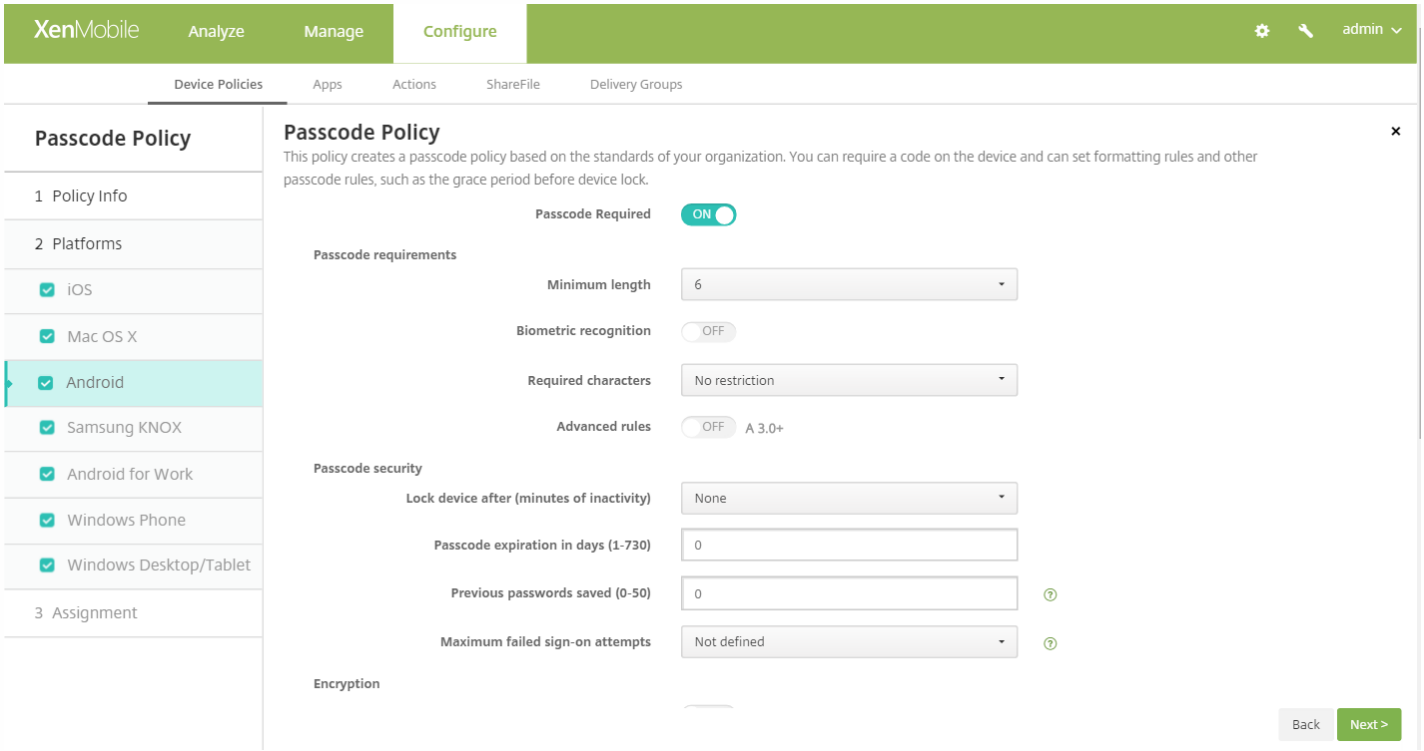
Mac OS Xの設定の構成



-
-
-
-
  -
  -
    -
    -
-
  -
    -

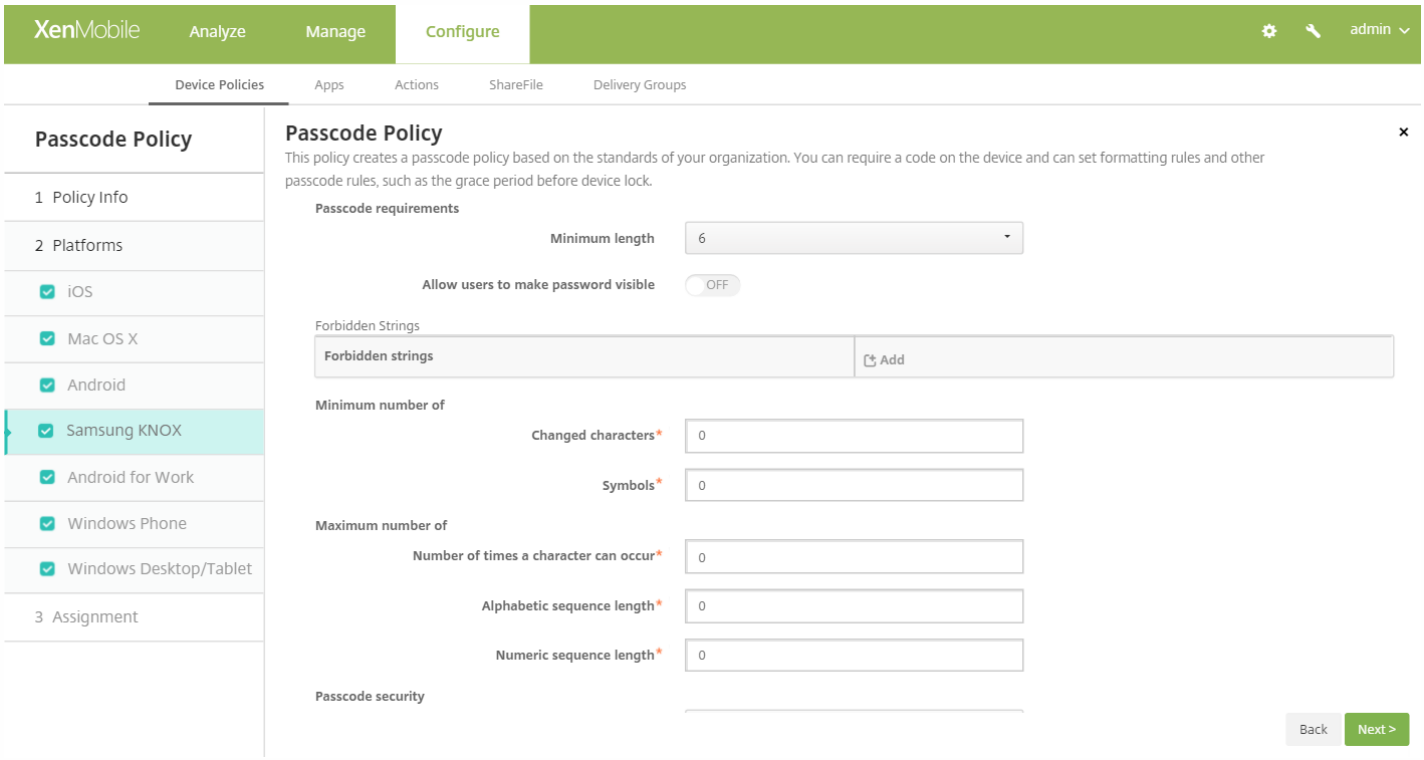
-
-
-
-
-
  -
  -
  -
  -
  -

Androidの設定の構成

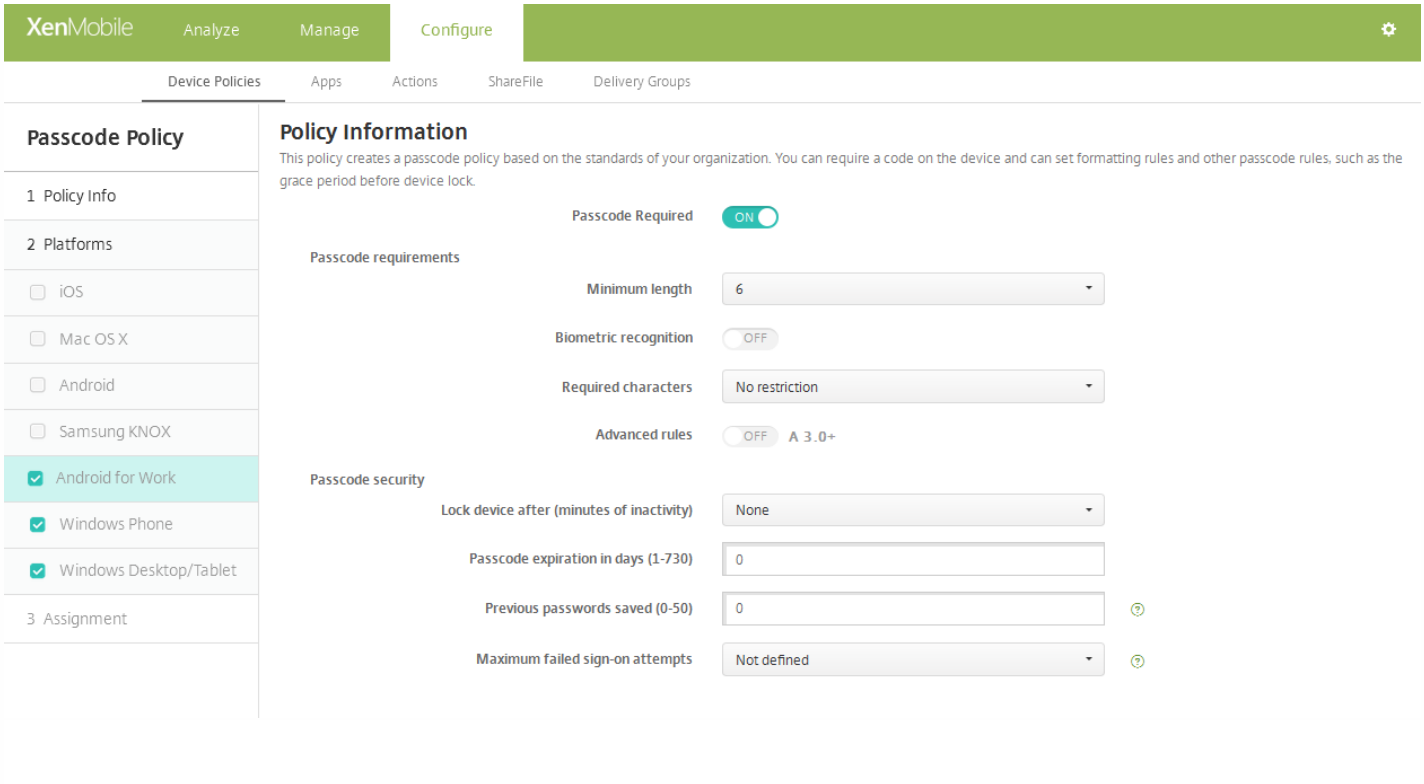


-

Samsung KNOXの設定の構成



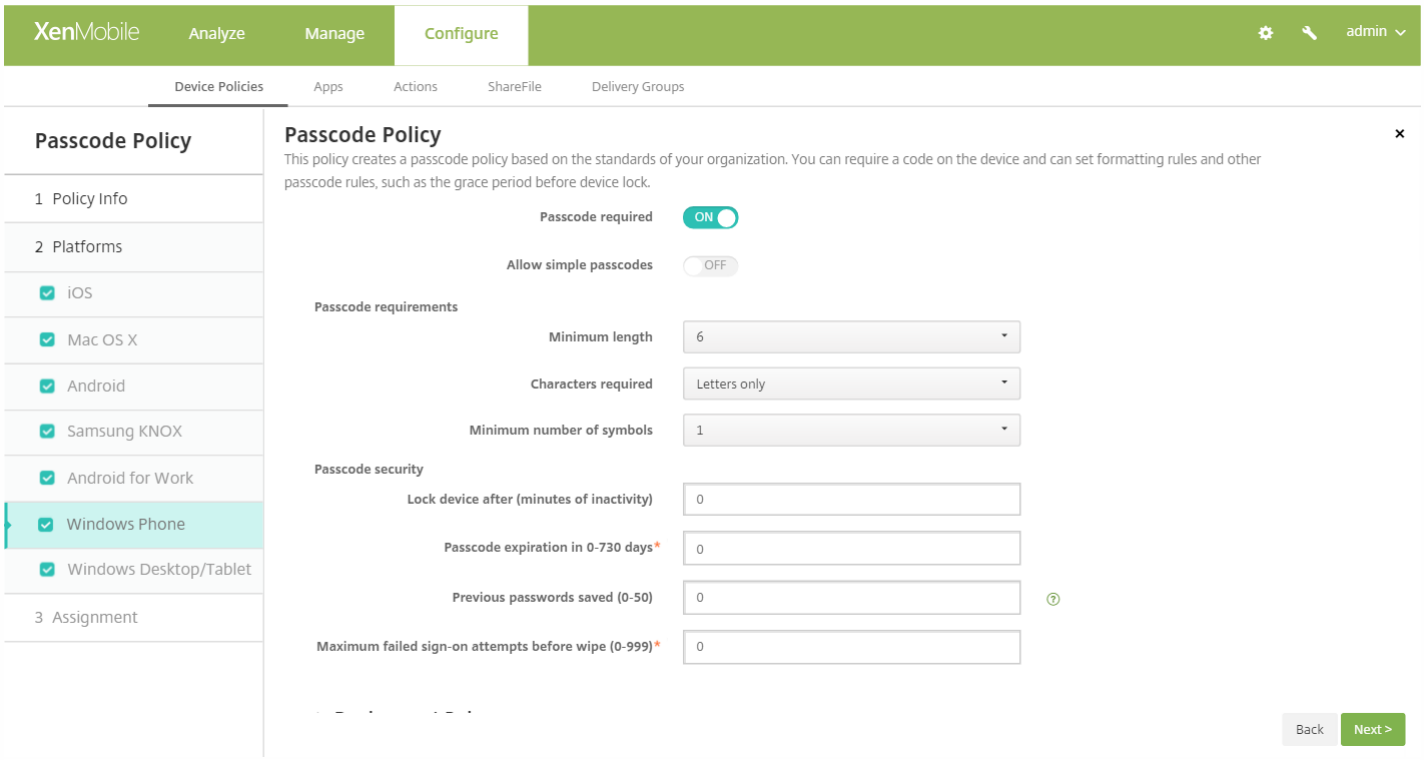
Android for Workの設定の構成



-
-
  -
  -
  -
  -
  -
    -
    -
    -
    -
    -
    -
-
  -
  -

-
-

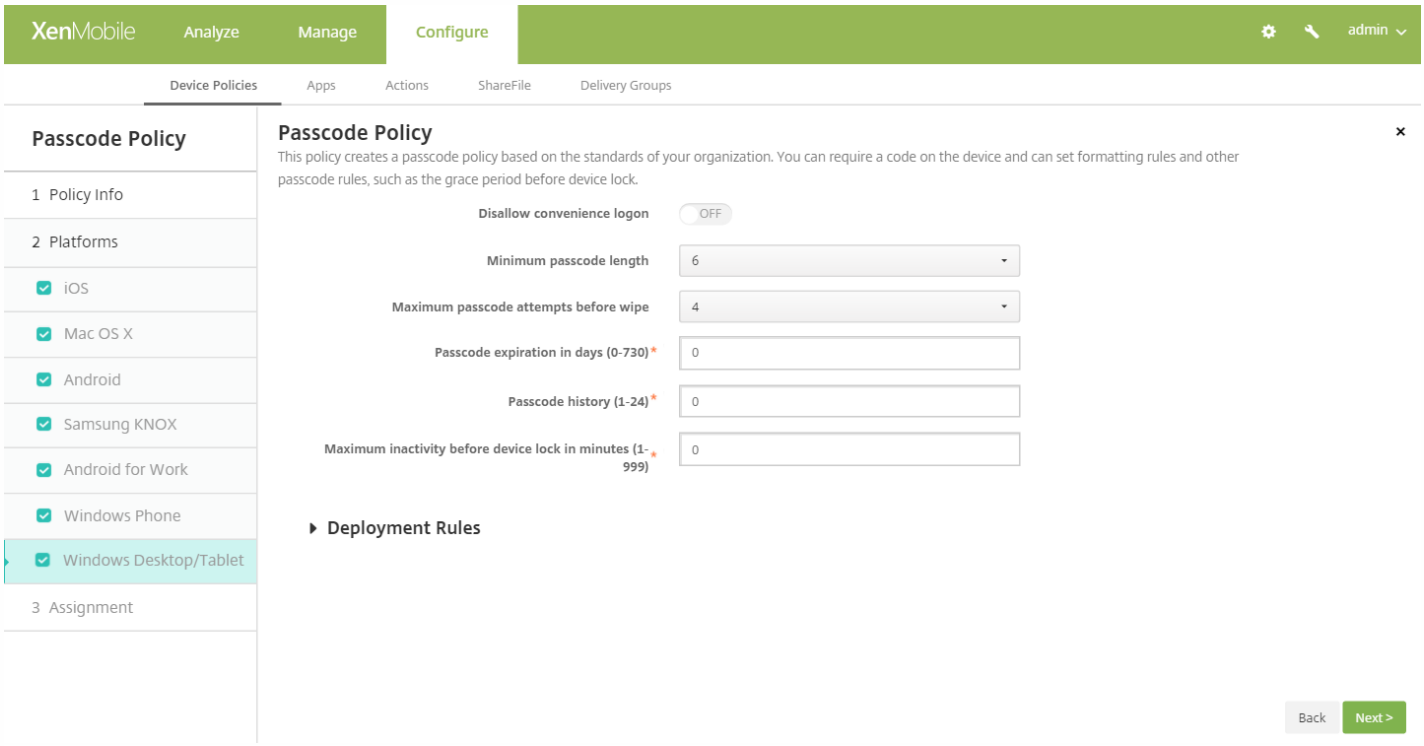
Windows Phoneの設定の構成



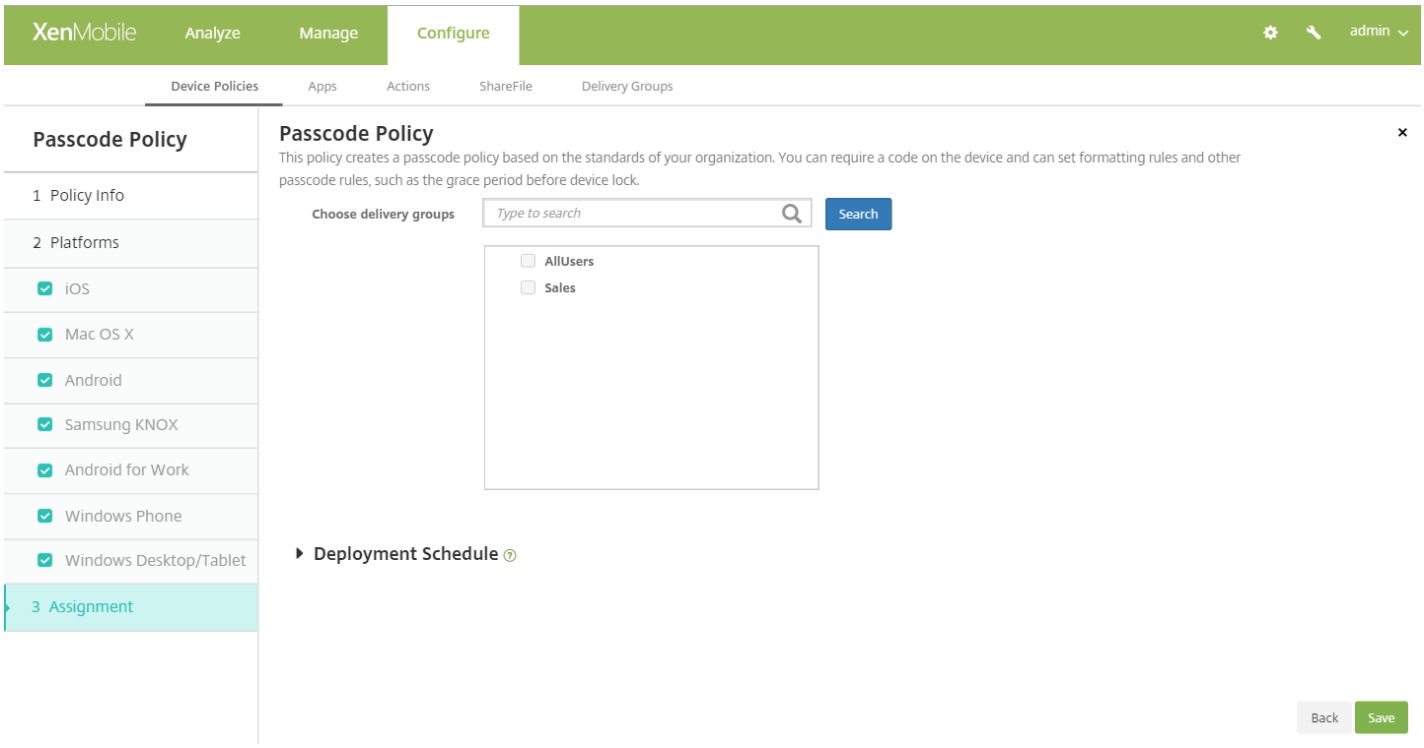
-
-
-
  -
  -
  -
-
  -
  -

-
-

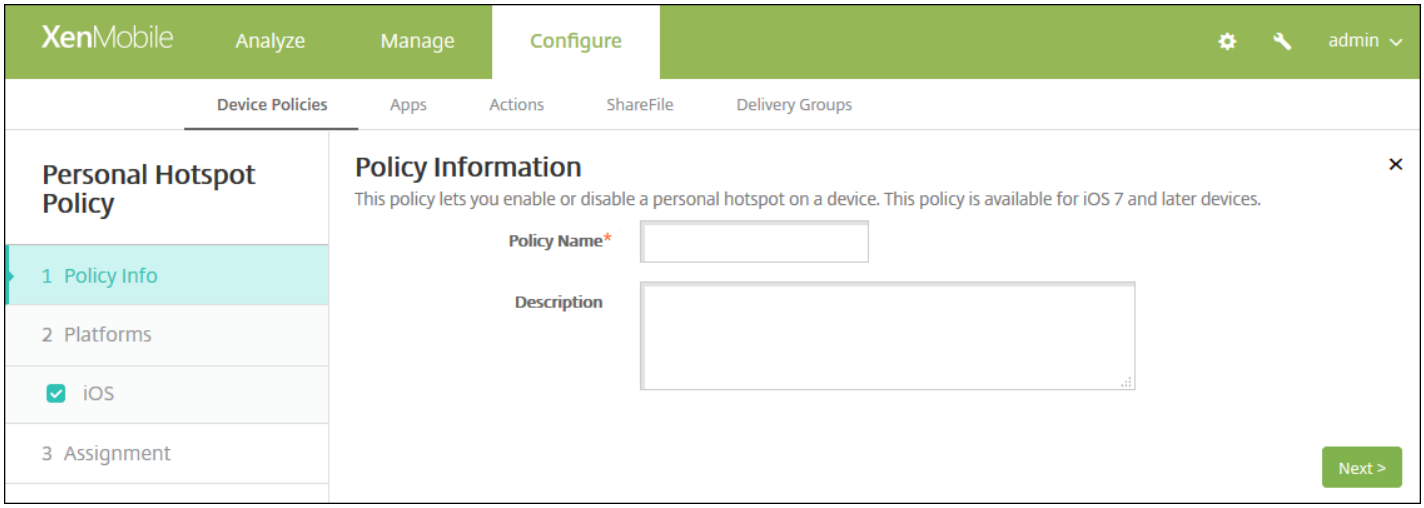
Windowsデスクトップ/タブレットの設定の構成



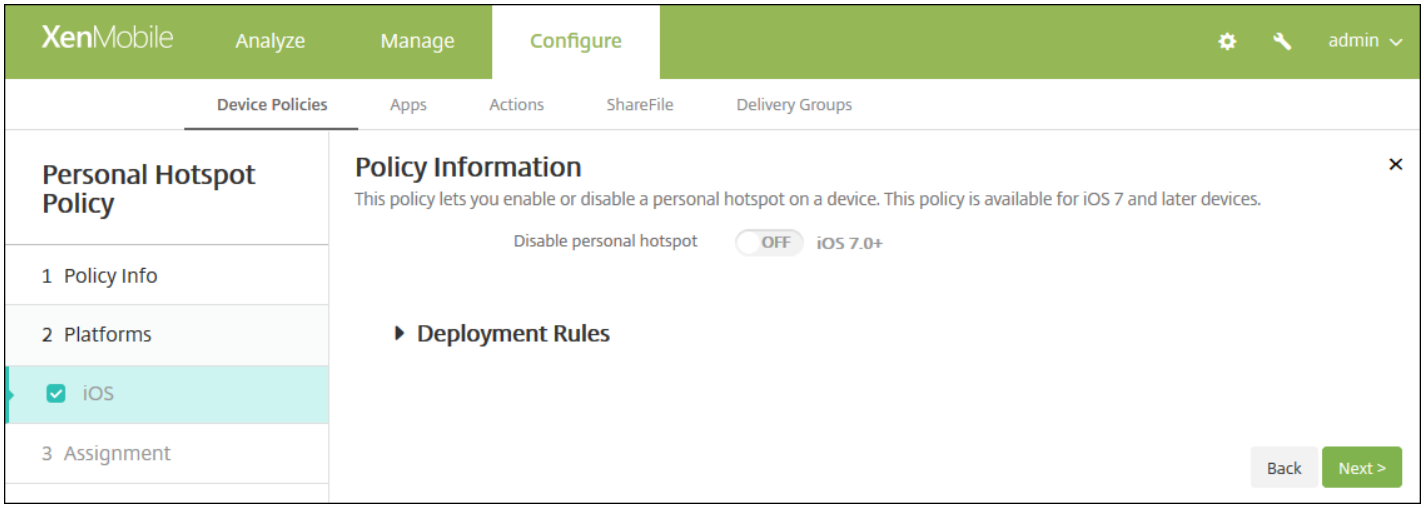
-
-
-
-
-
-

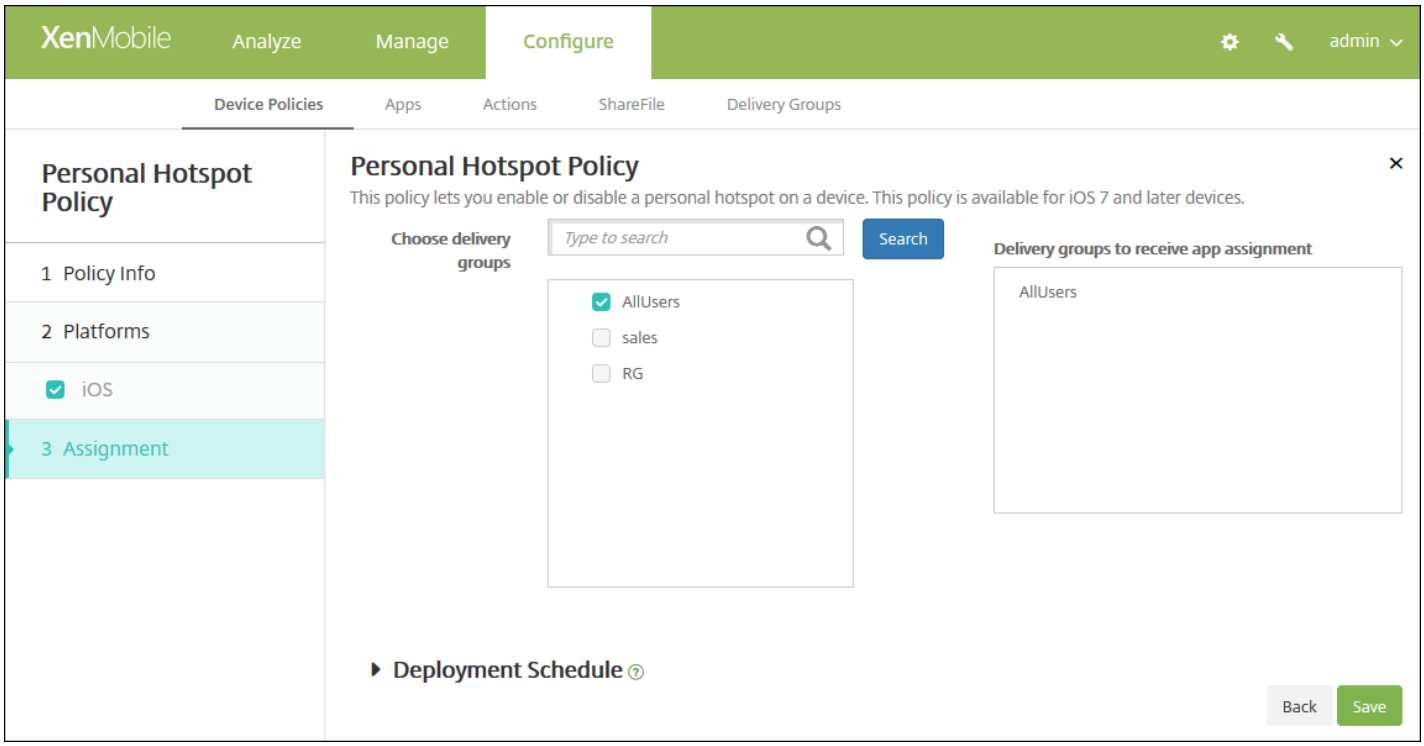


-
-
-
-
-
-
-

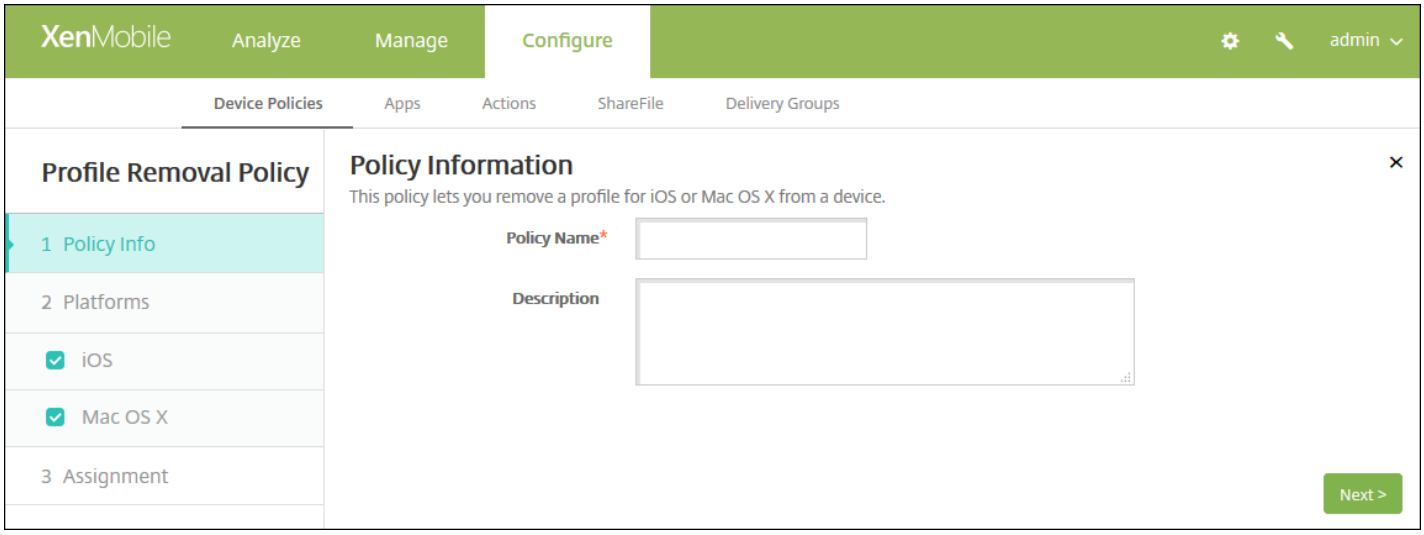


-
-



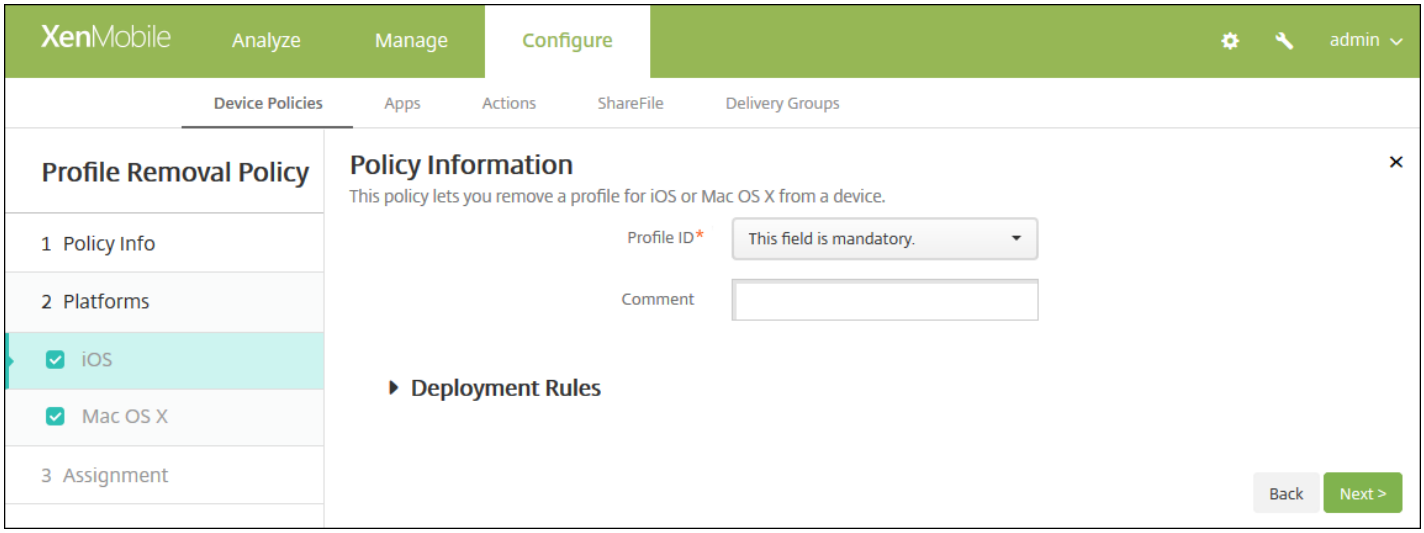


-
-



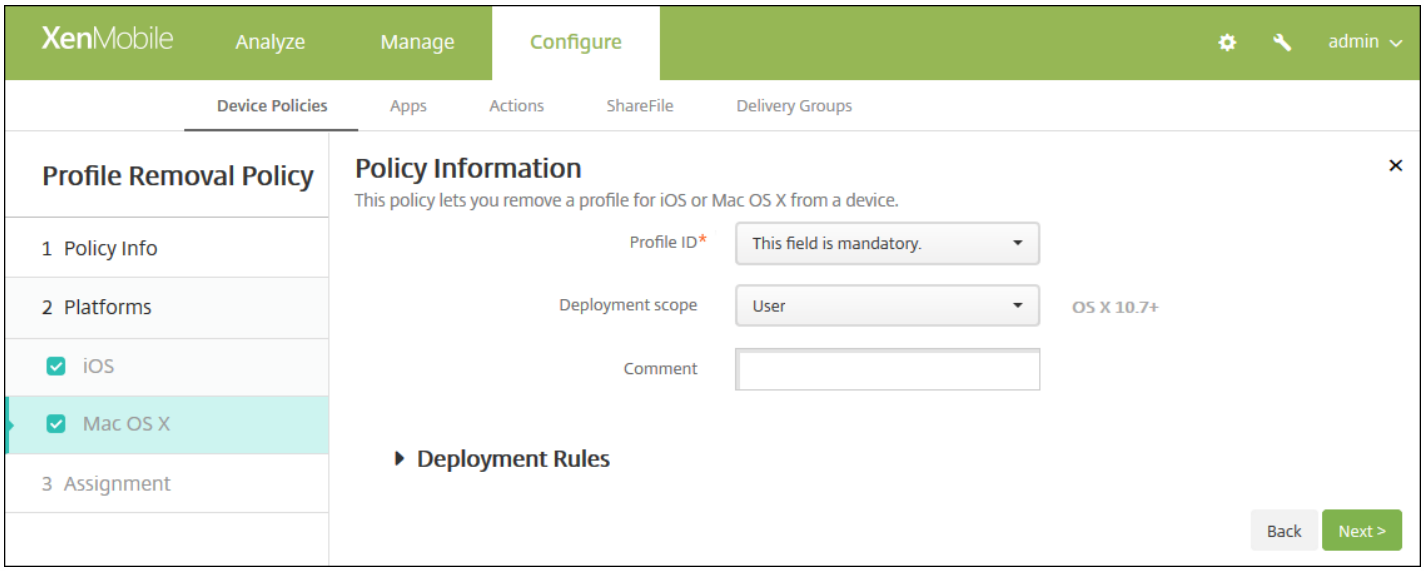
-
-

iOSの設定の構成

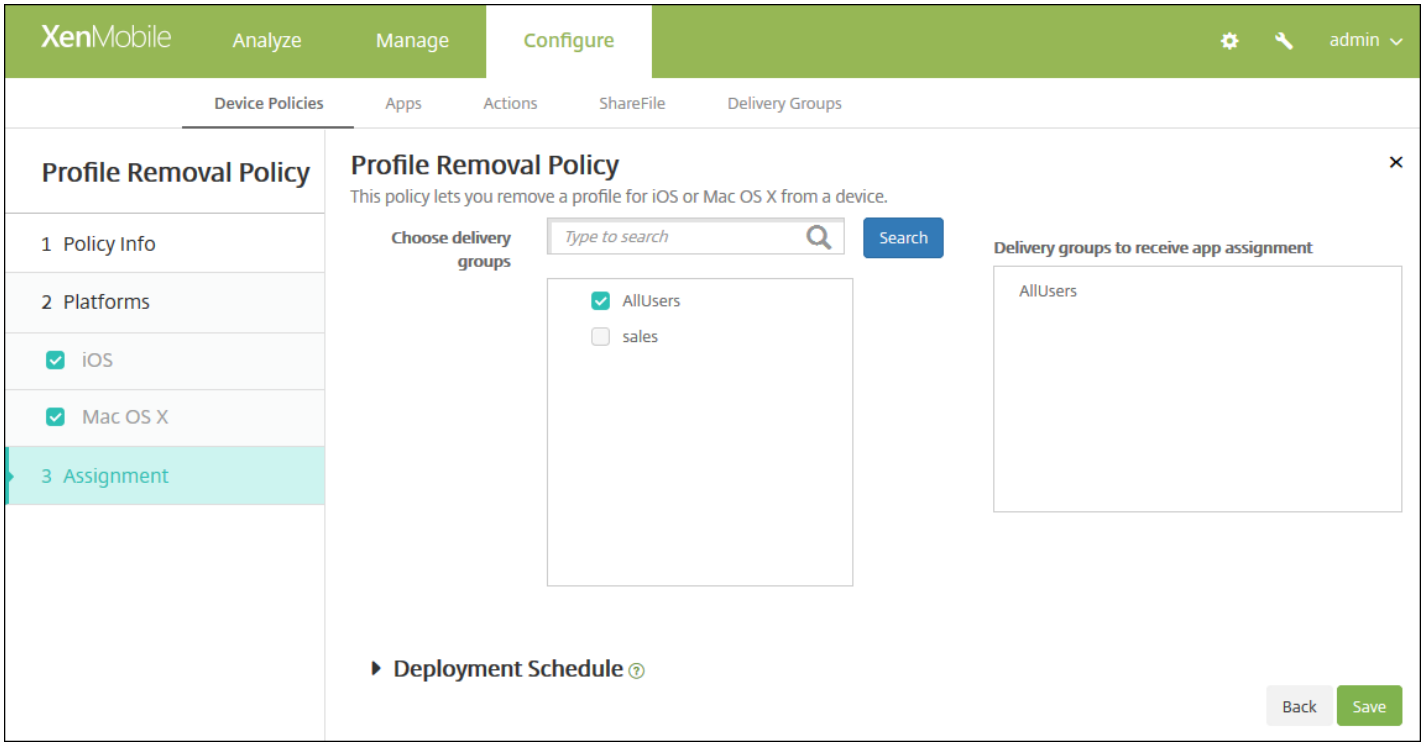


-
-

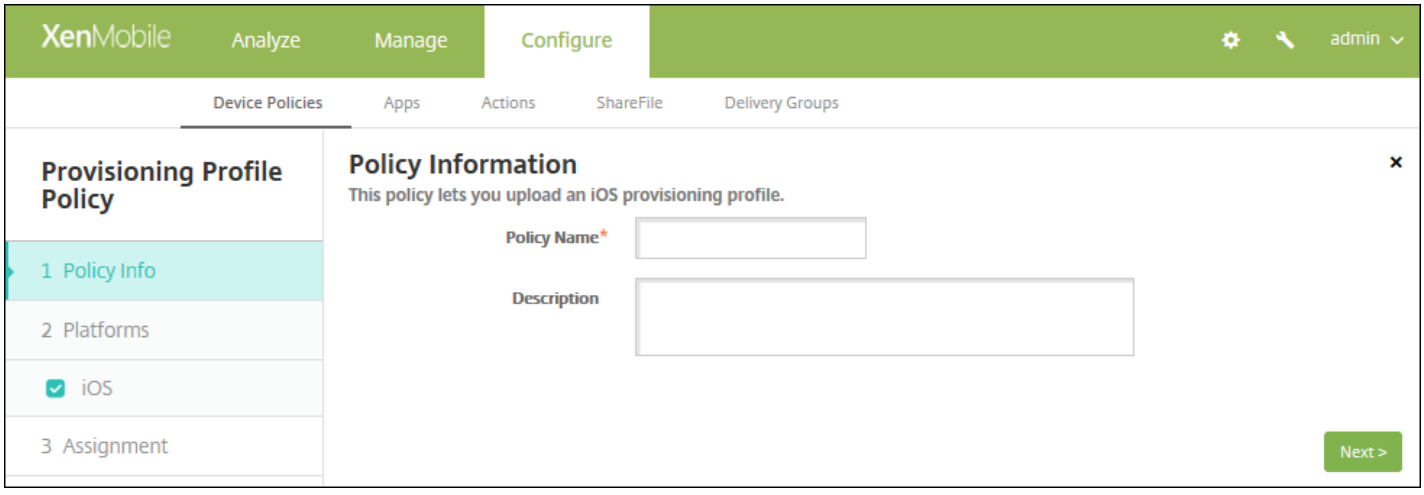
Mac OS Xの設定の構成



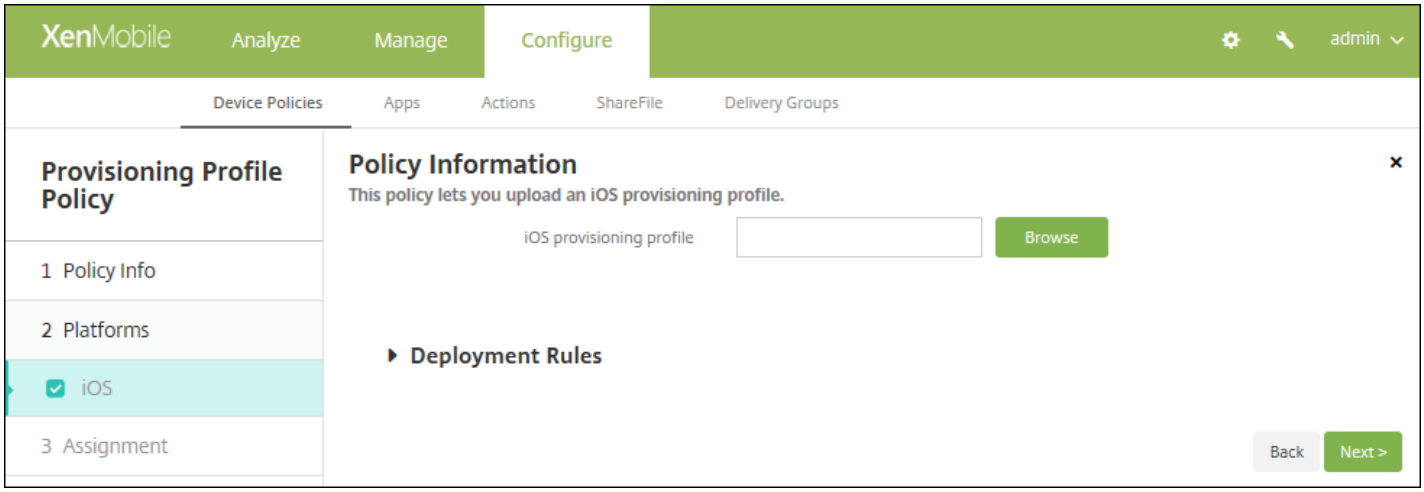
-
-
-

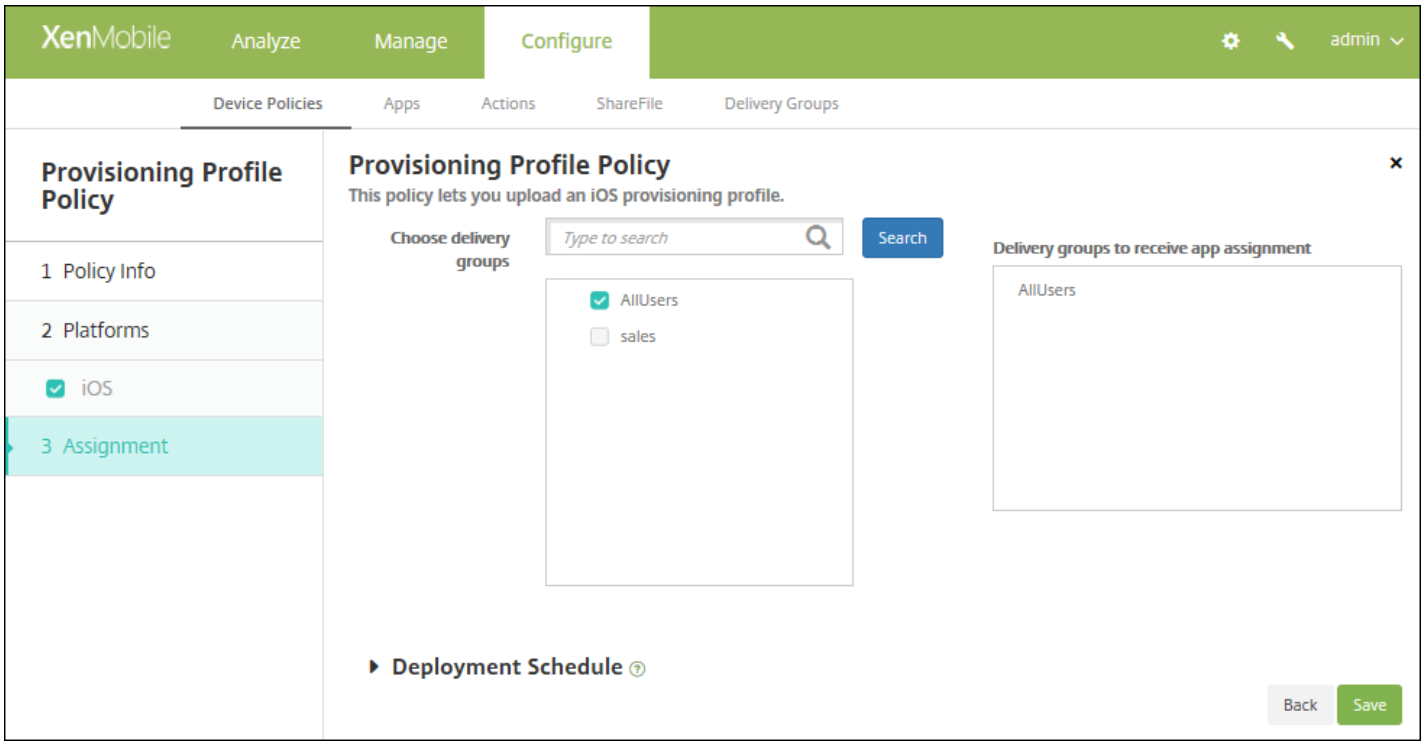


-
-
-
-
-
-
-

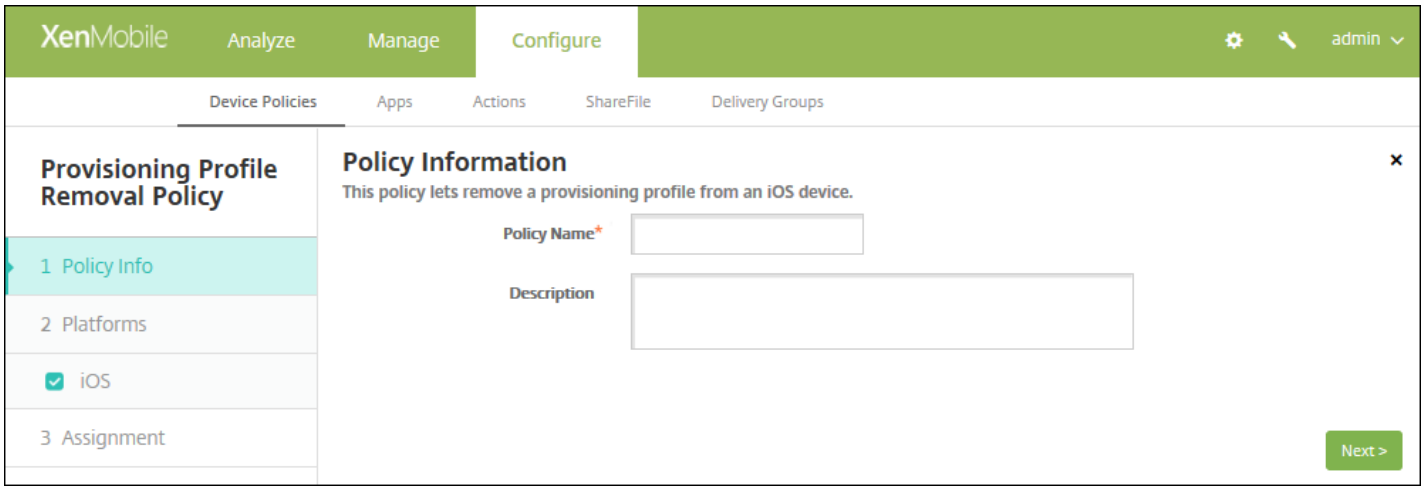


-
-

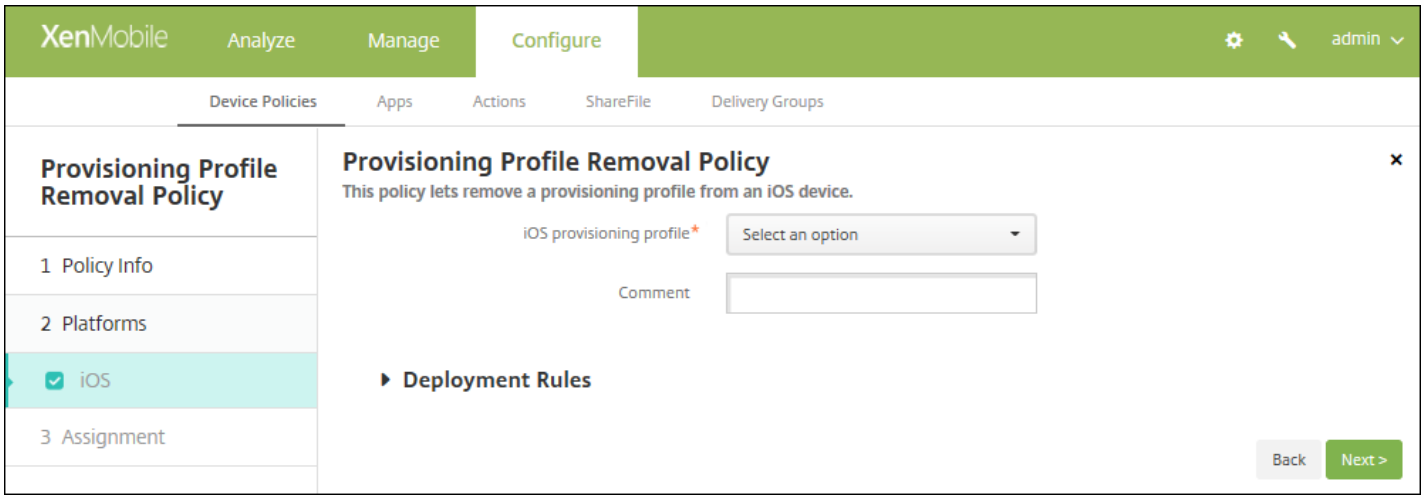




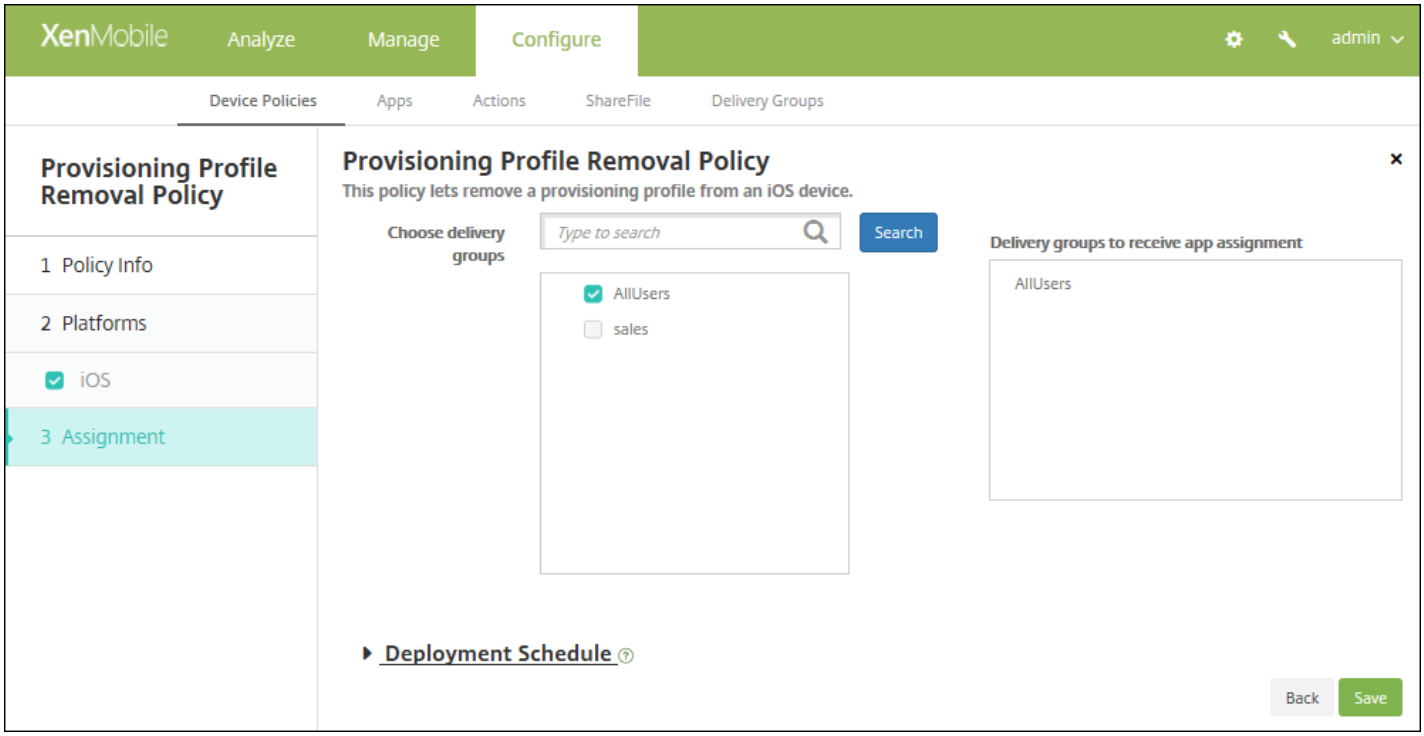
-
-
-
-
-
-
-



-
-

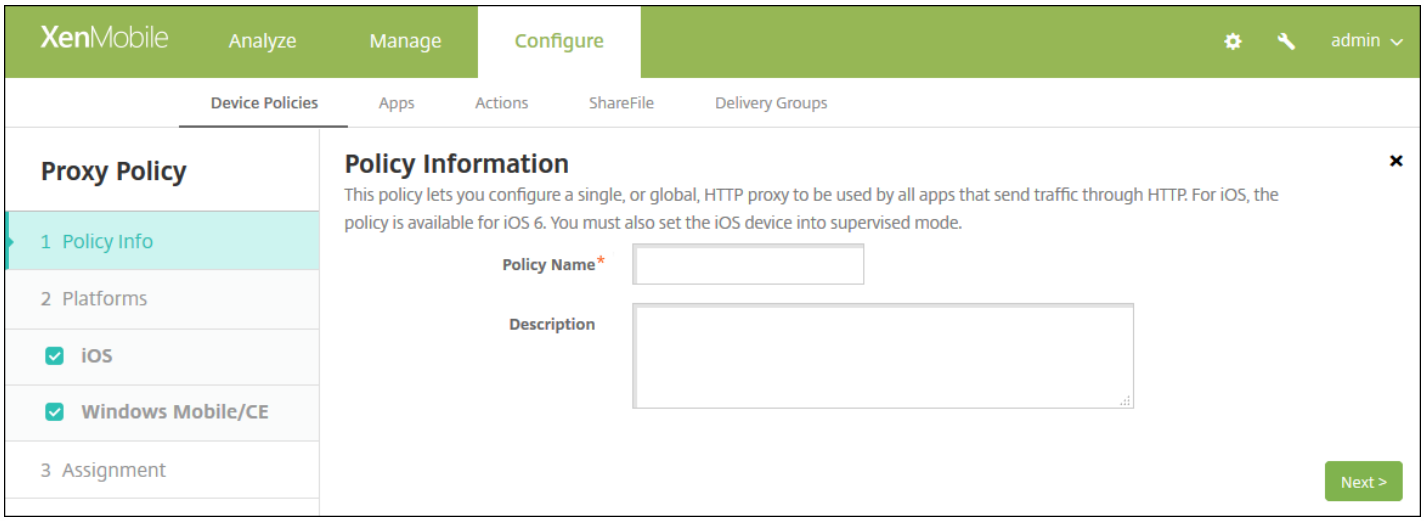


-
-



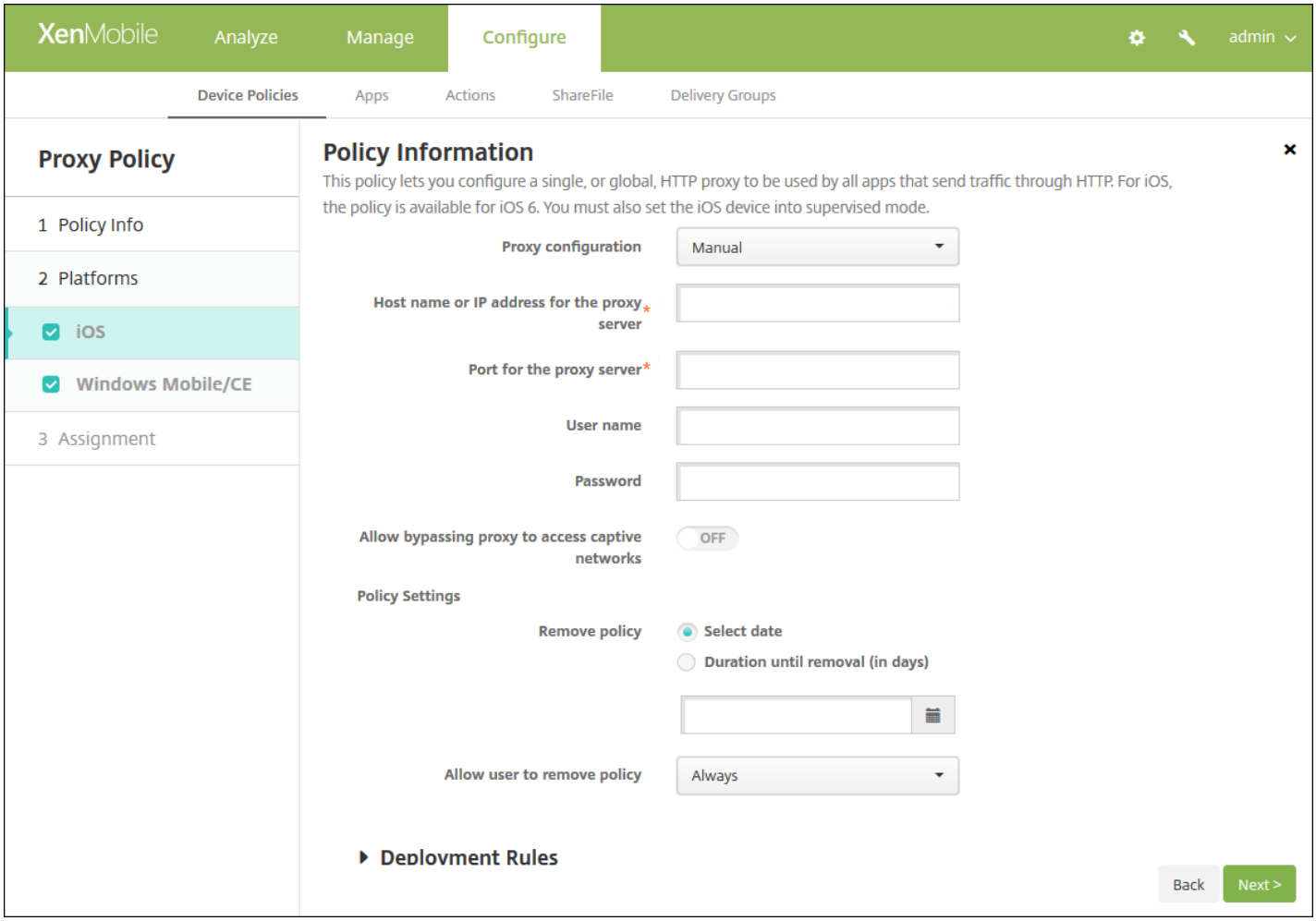
-
-
-
-

-
-



-
-

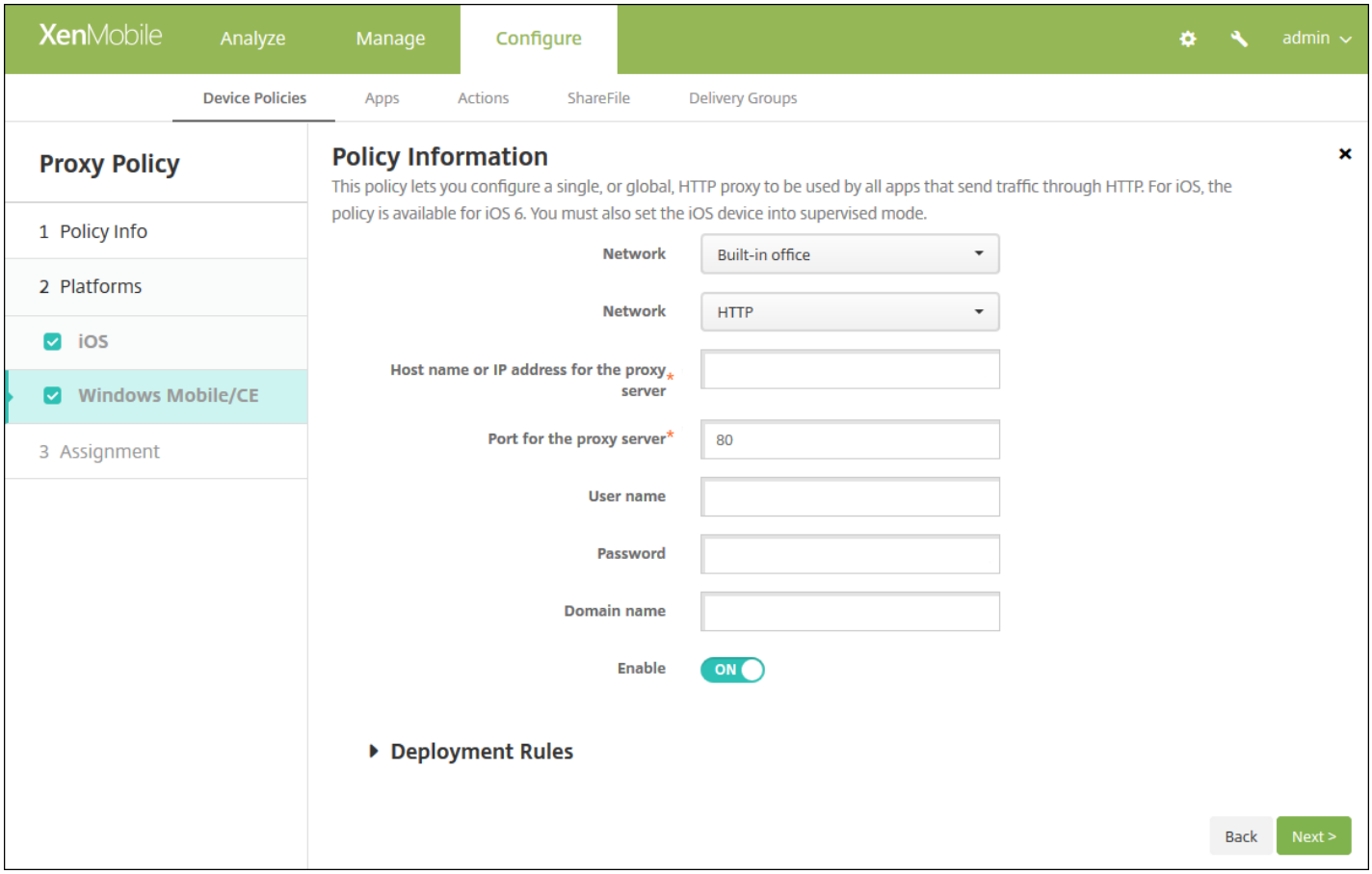
iOSの設定の構成



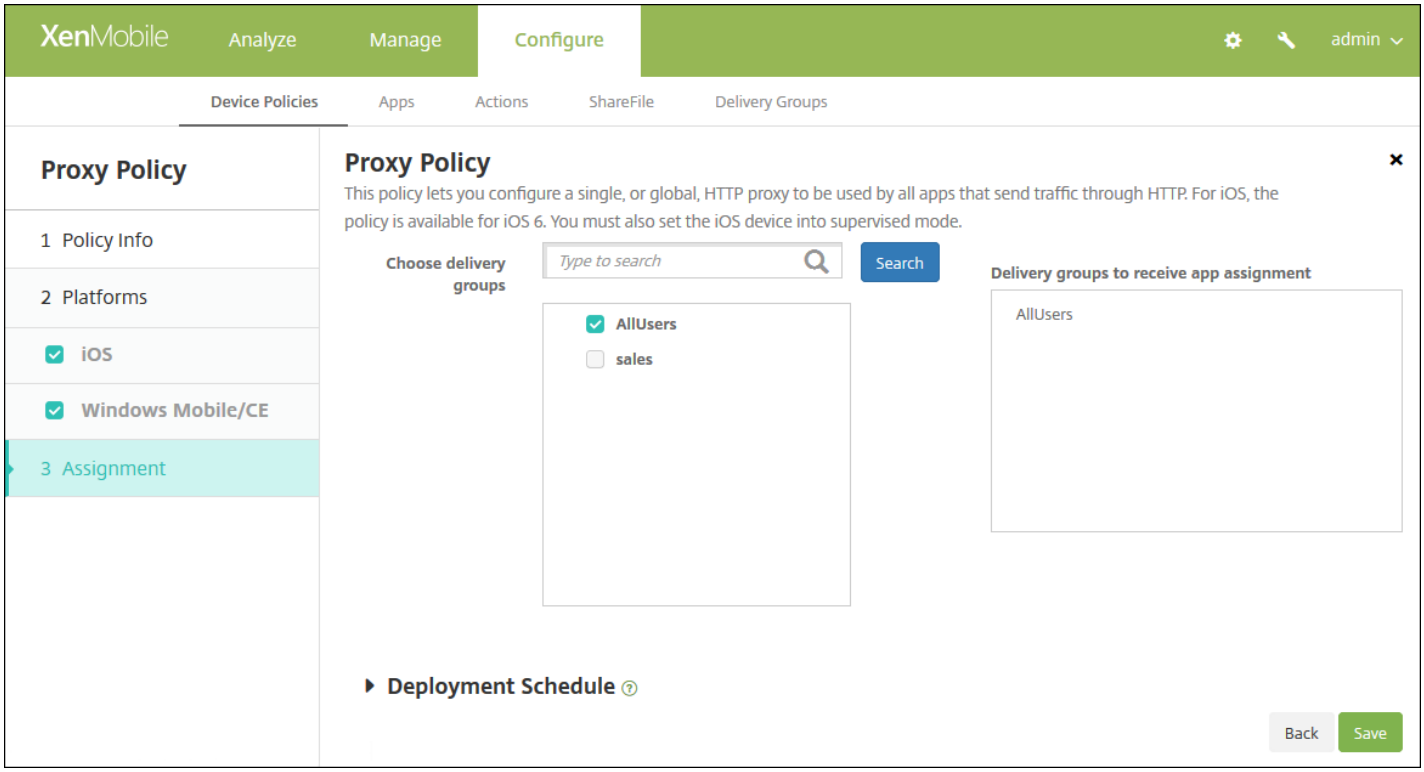
-
  -
    -
    -
    -
    -
  -
    -
    -
-
-
  -

-
-
-

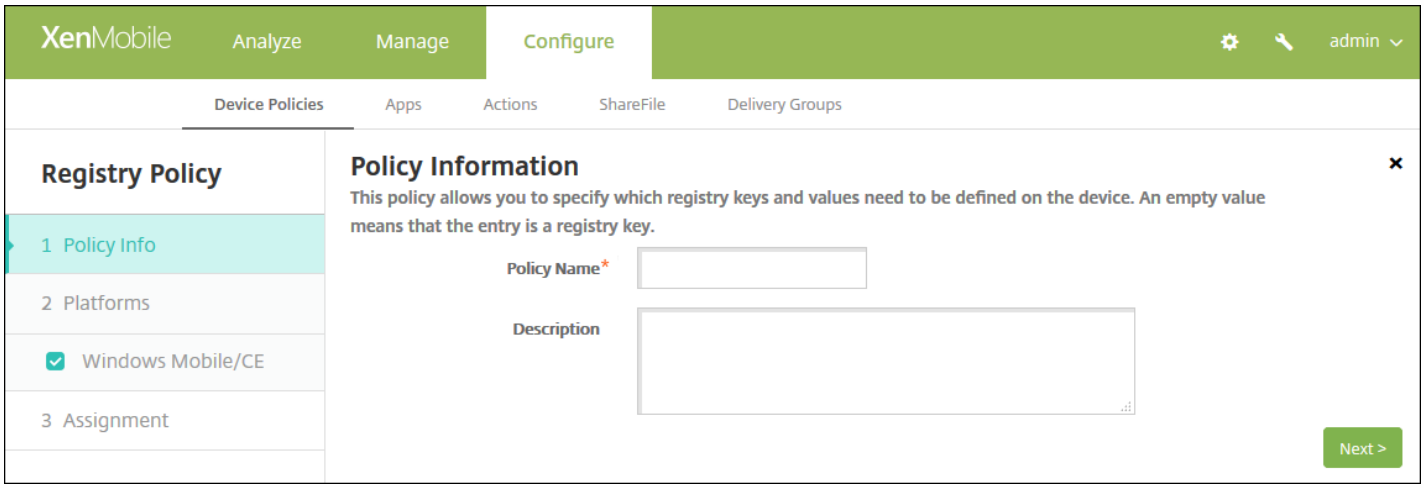
Windows Mobile/CEの設定の構成



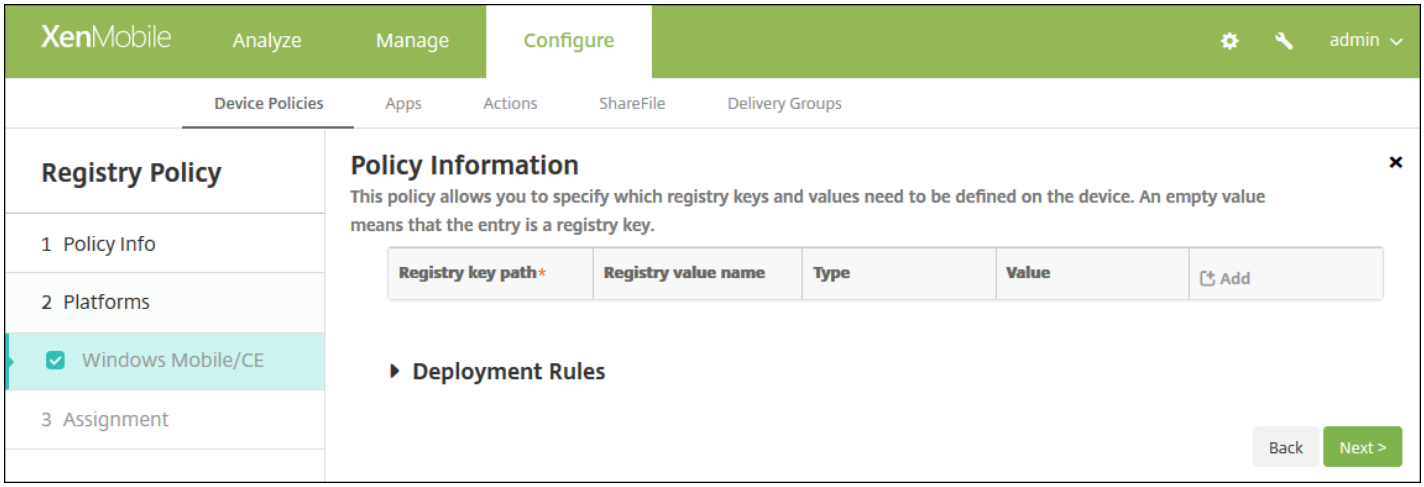
-
  -
  -
  -
  -
-
  -
  -
  -
  -
-

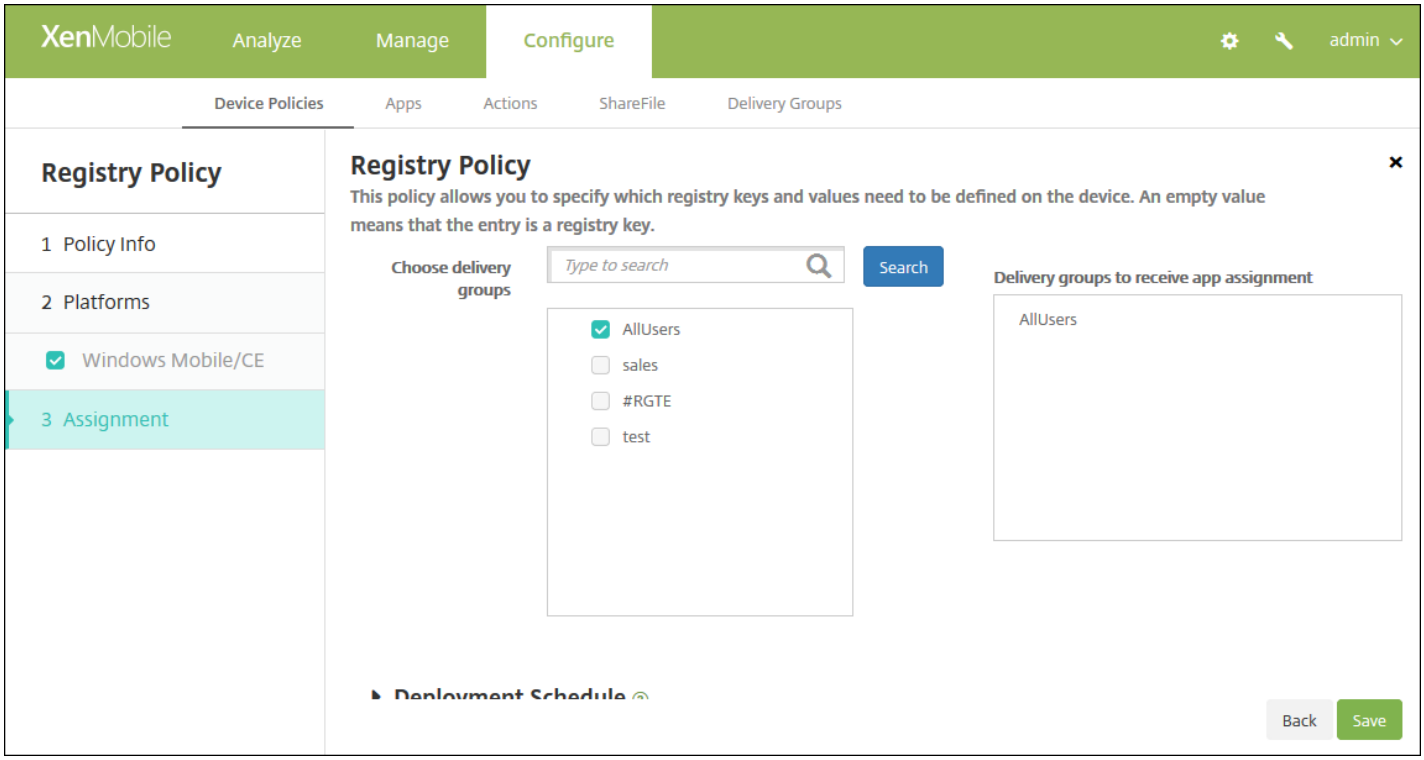


-
-



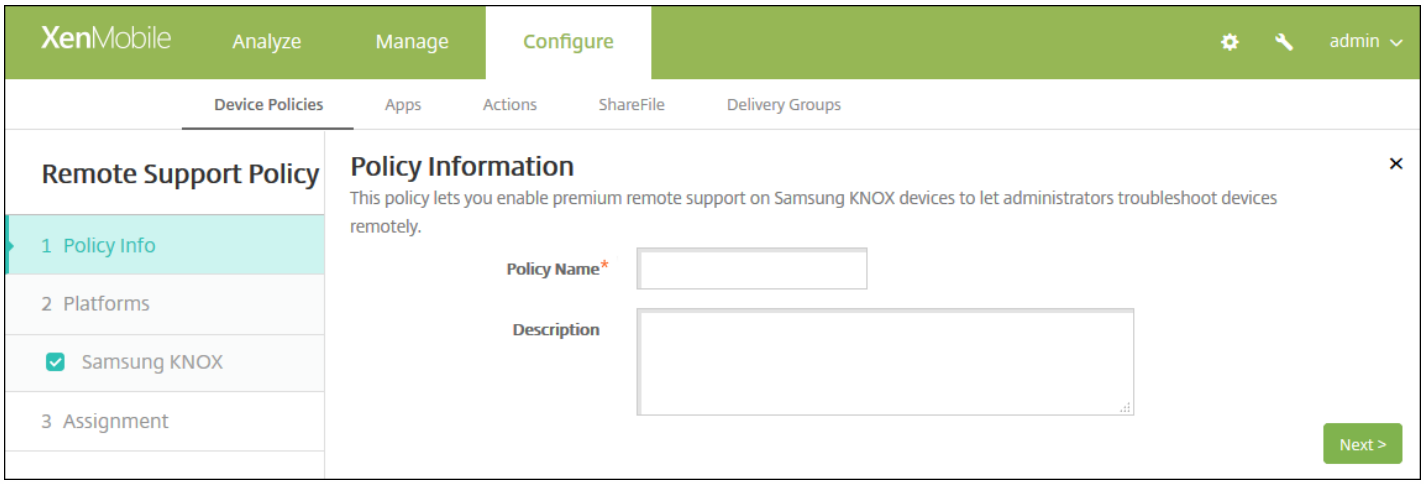
-
-



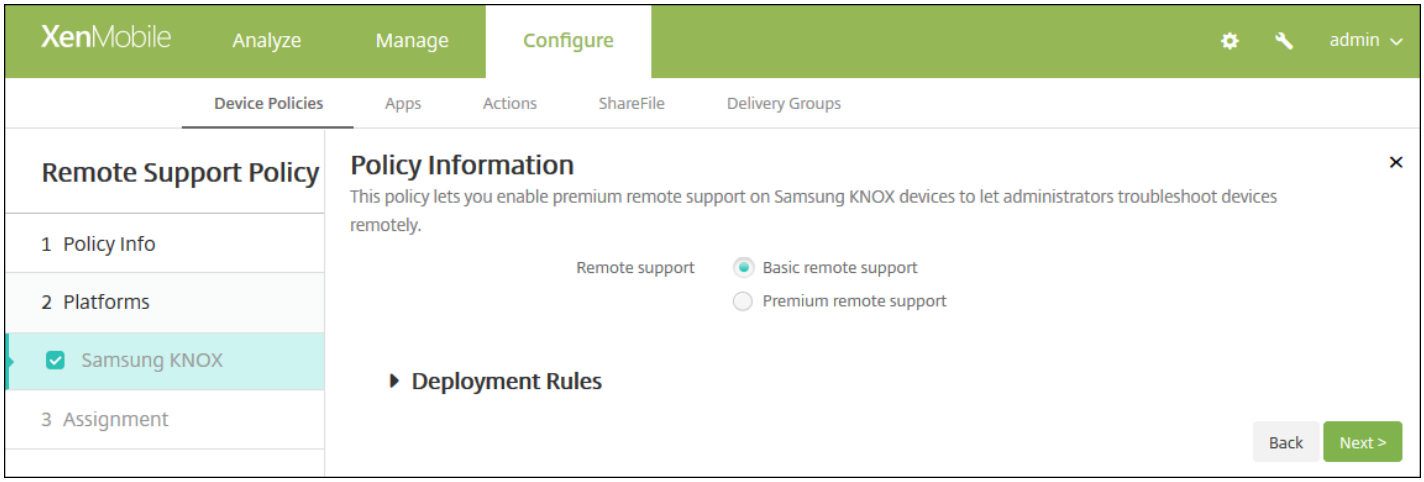


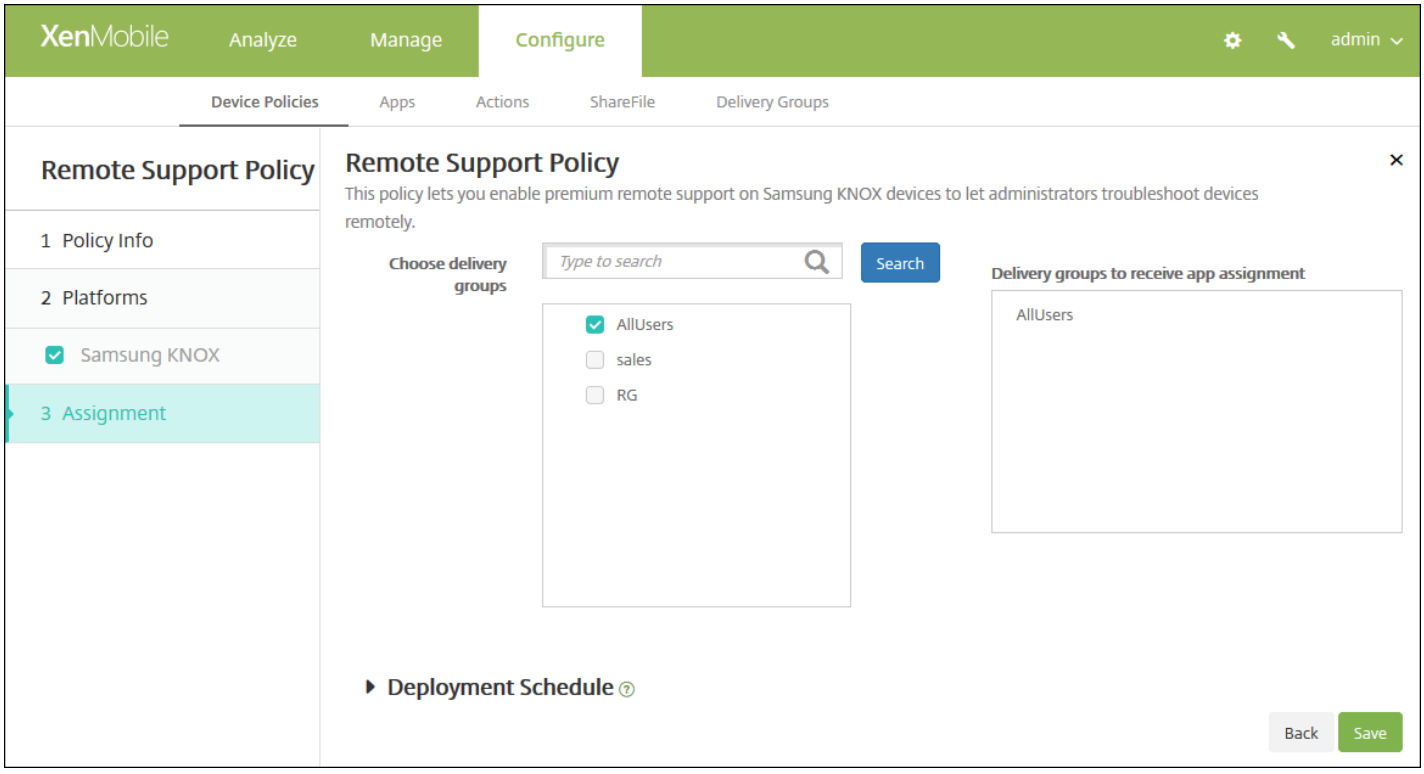
-
-
-
-
-
-
-

-
-
-
-
-
-



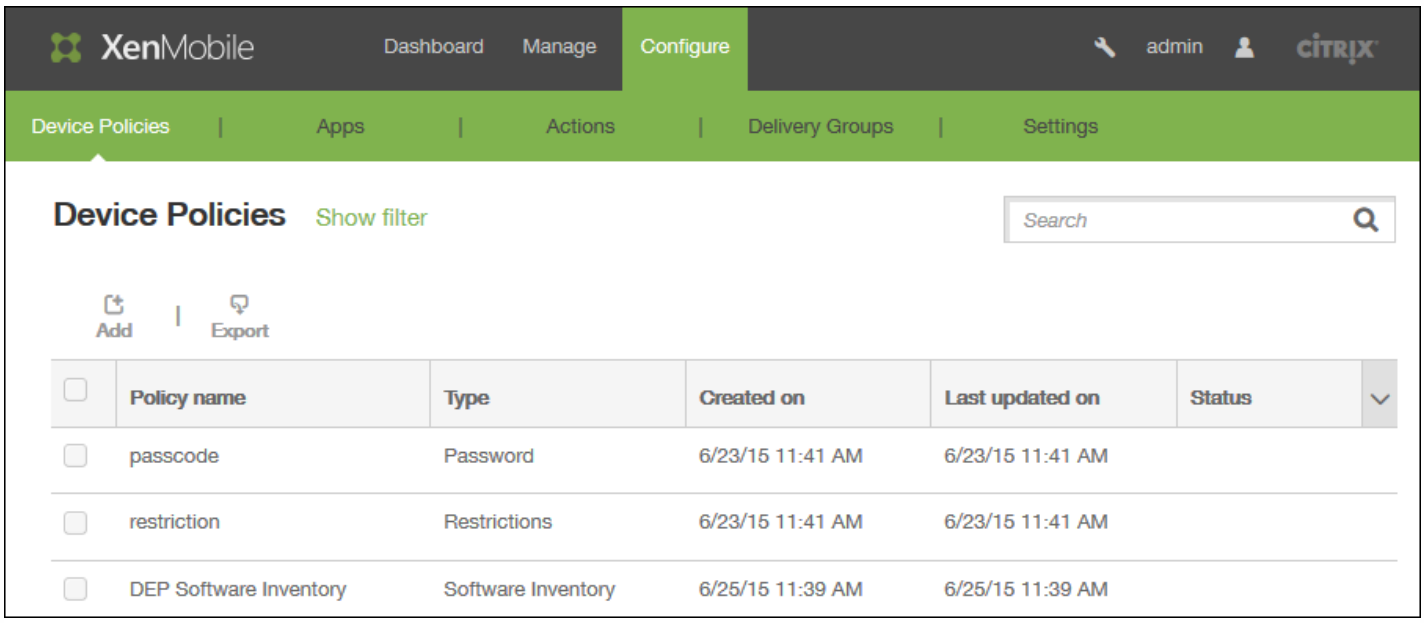
-
-

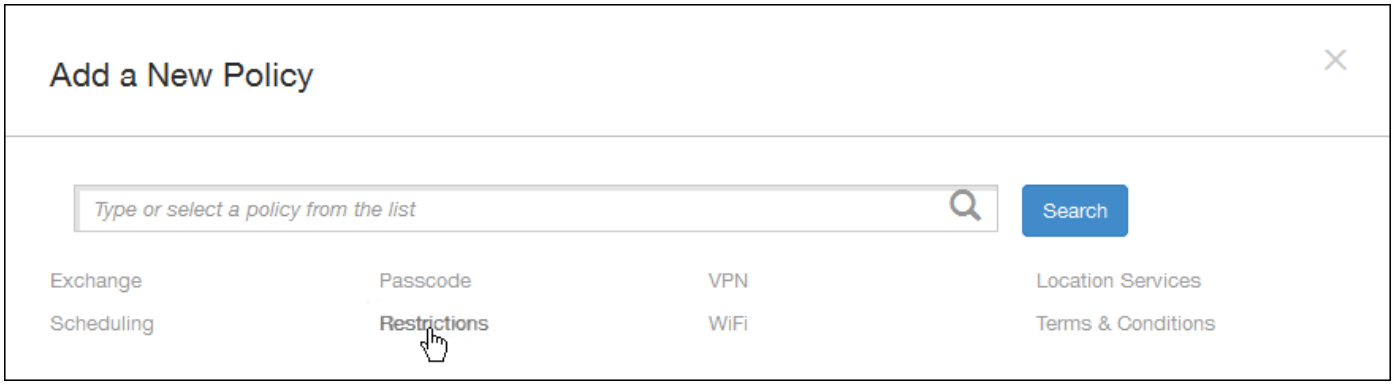


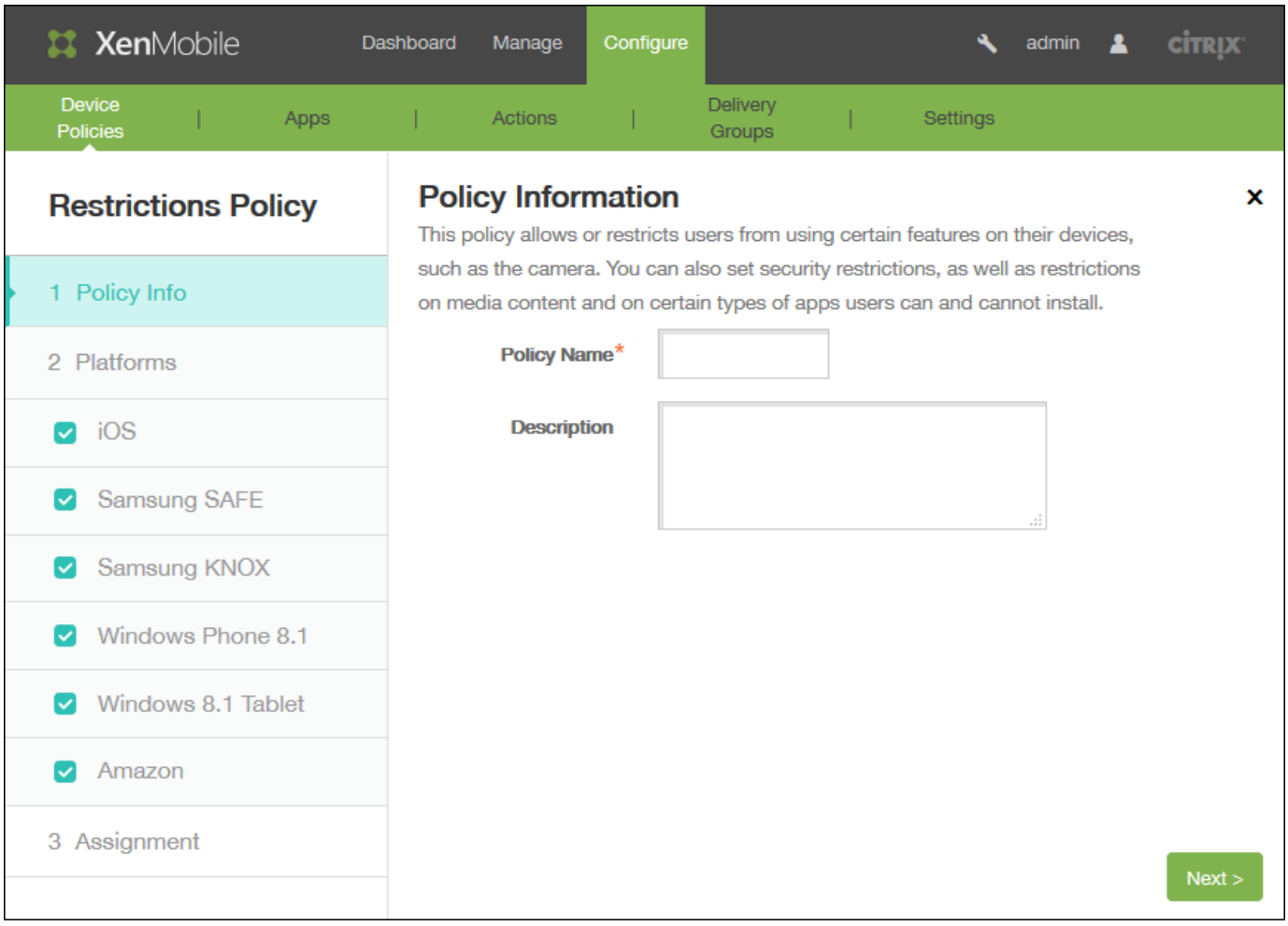


-
-
-
-
-
-
-

-
-

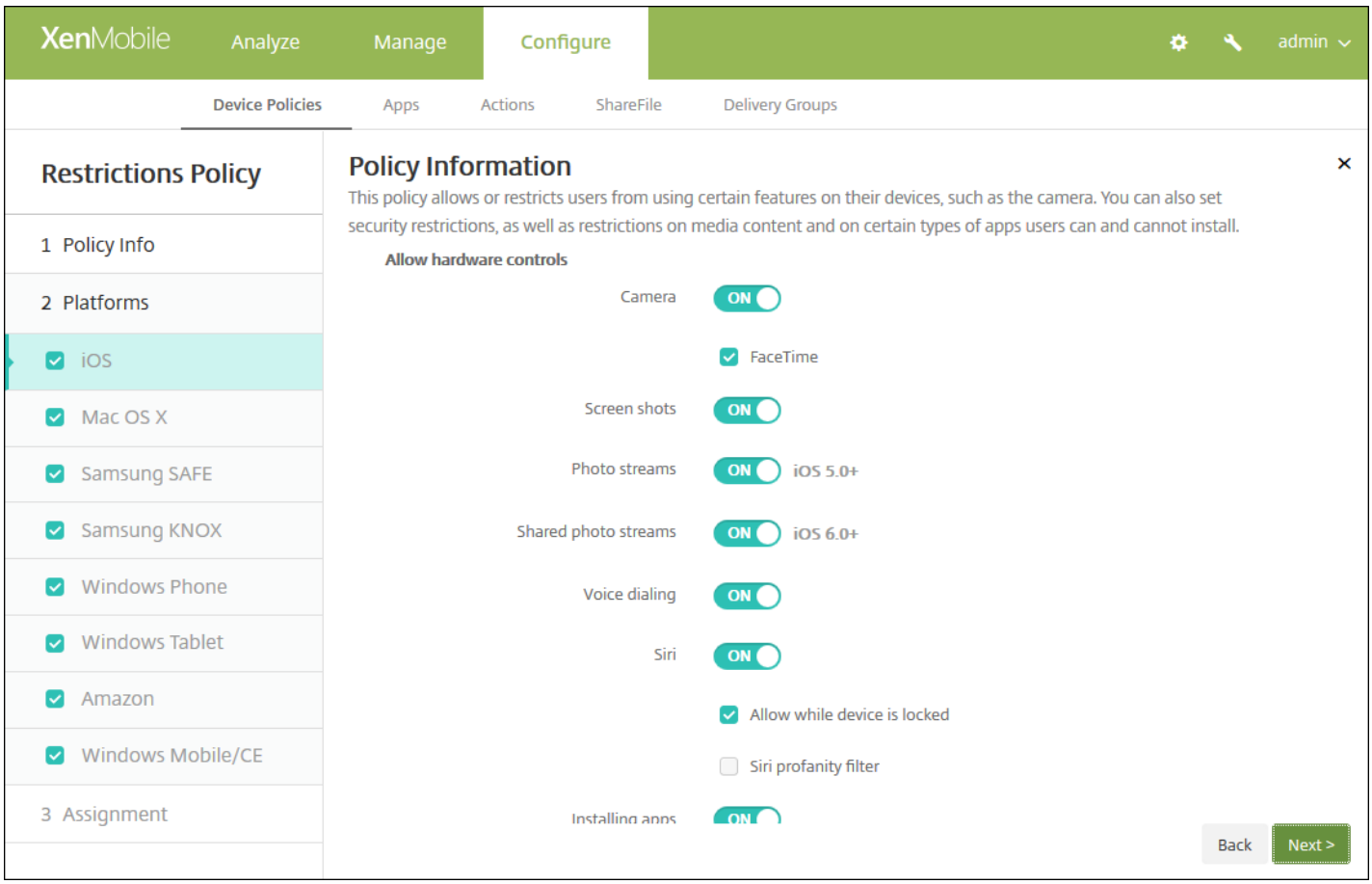




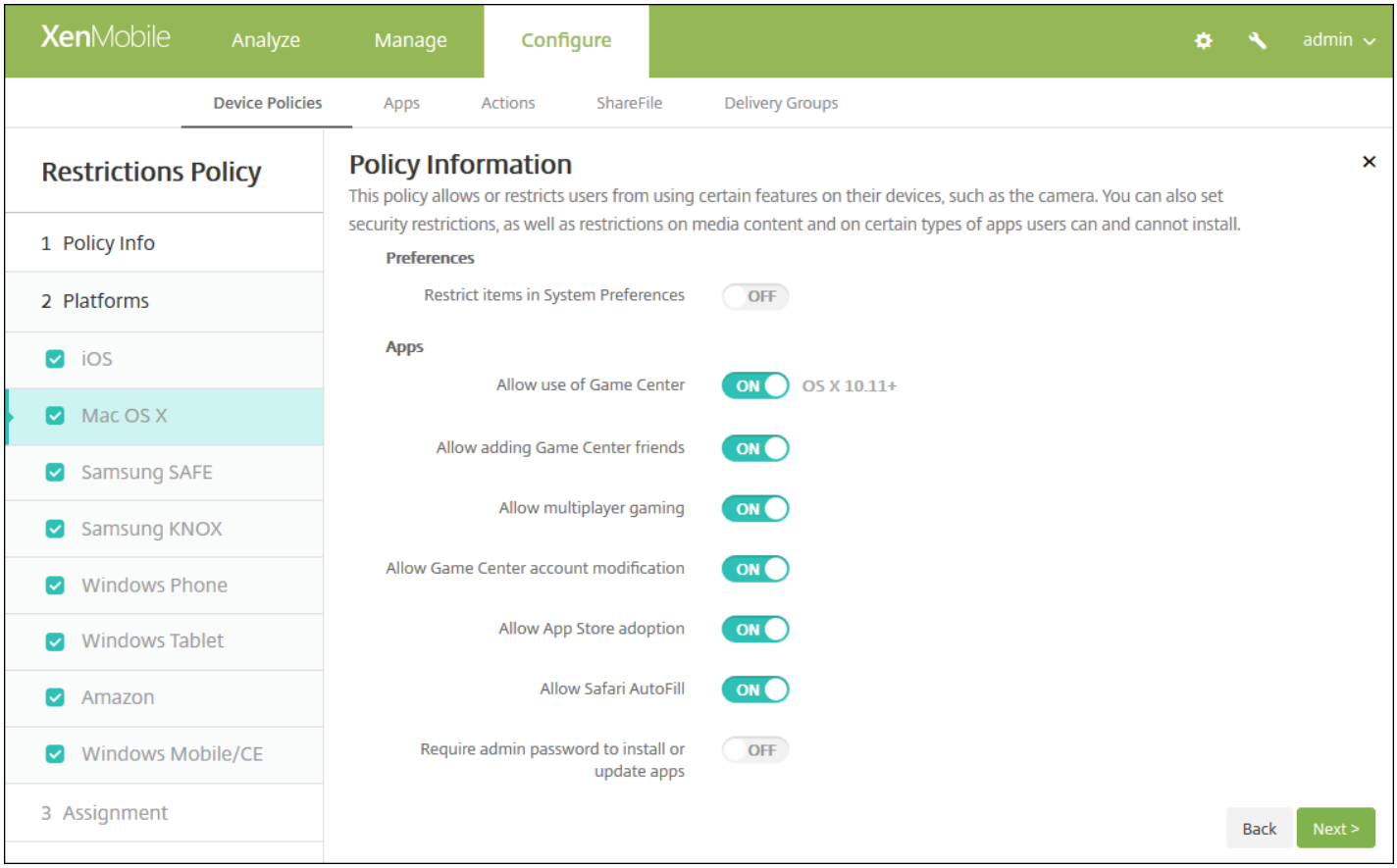


-
-

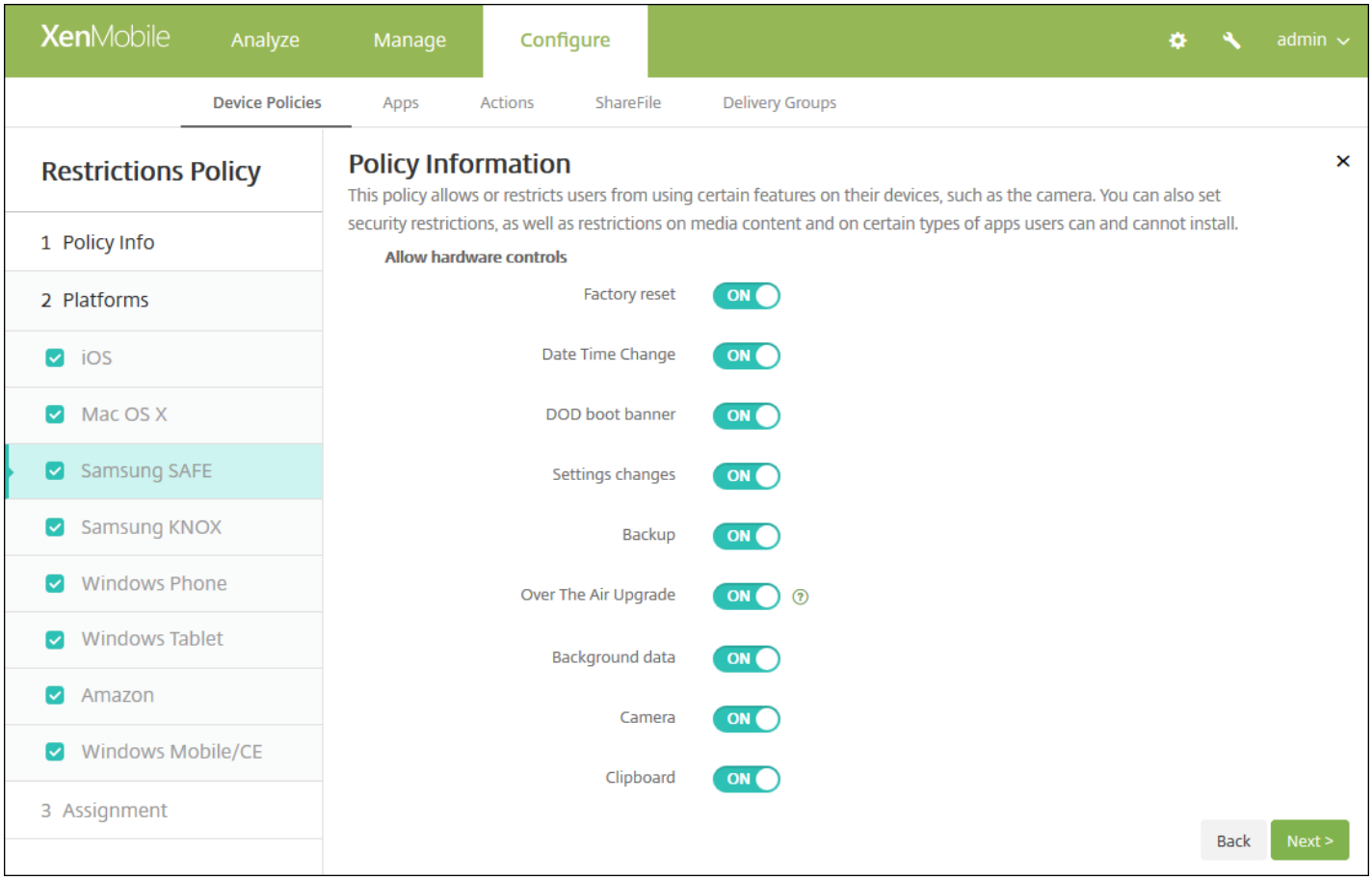
[iOS] を選択した場合は、次の設定を構成します。



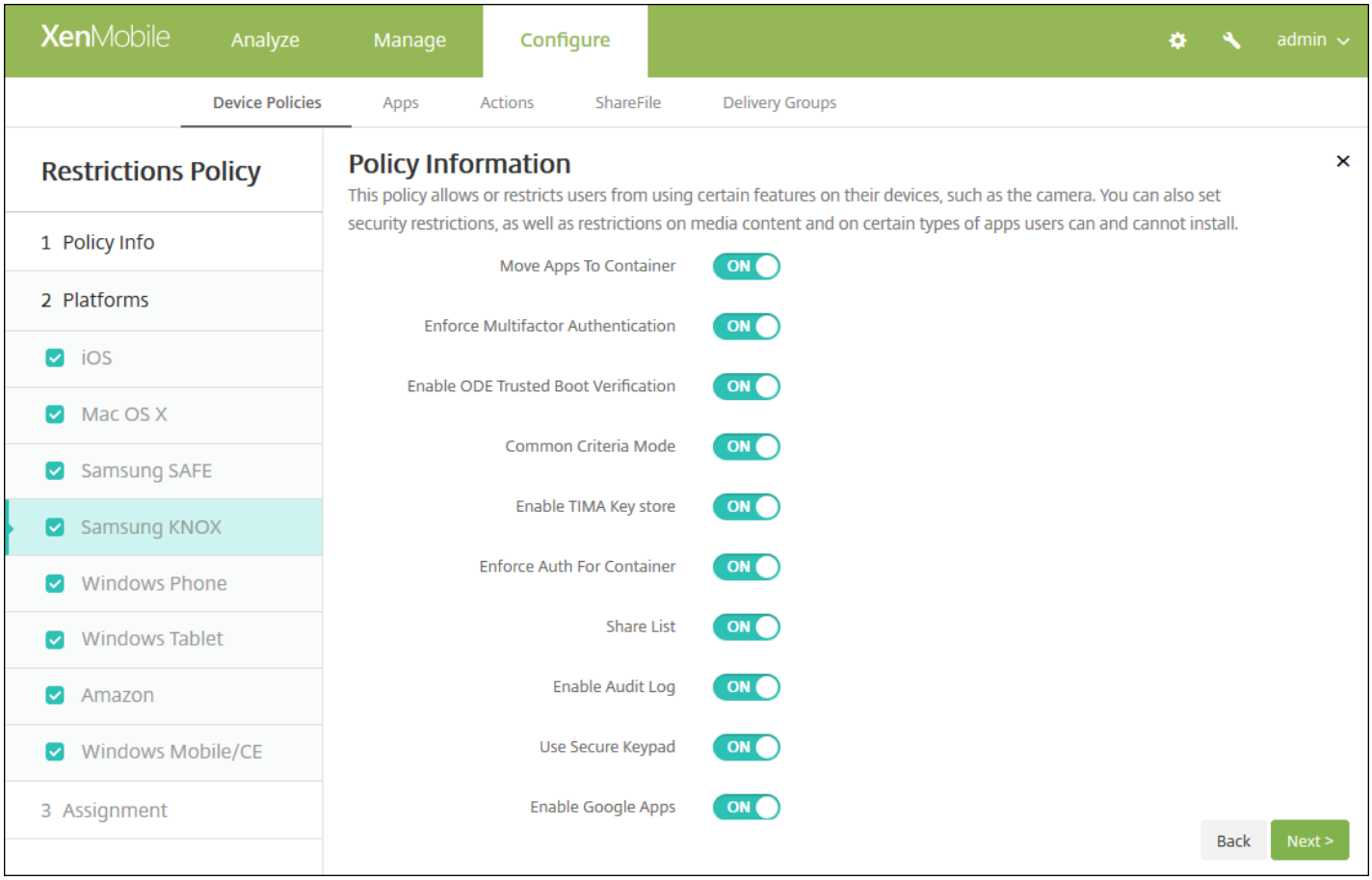
Mac OS Xの設定の構成



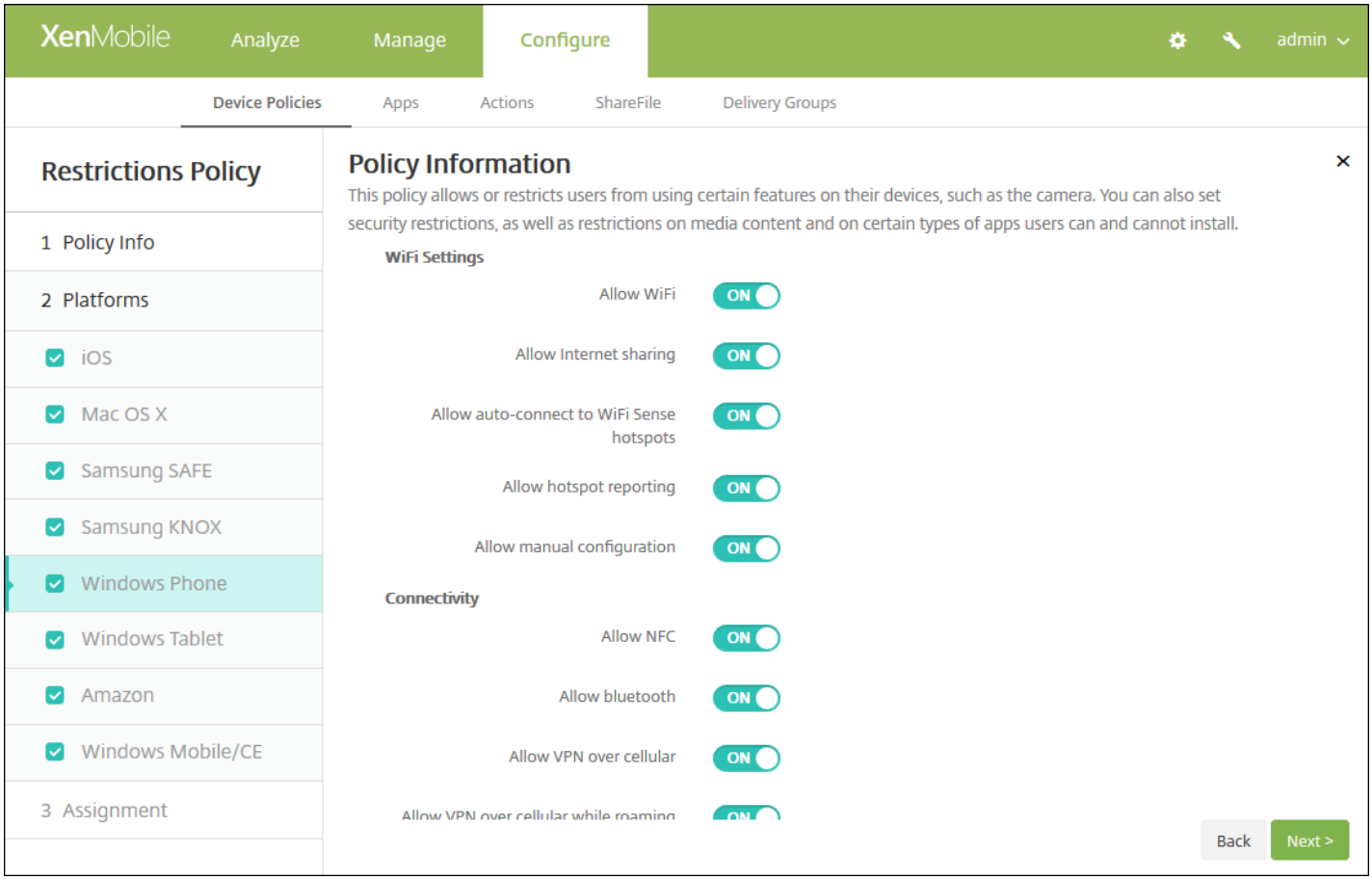
Samsung SAFEの設定の構成



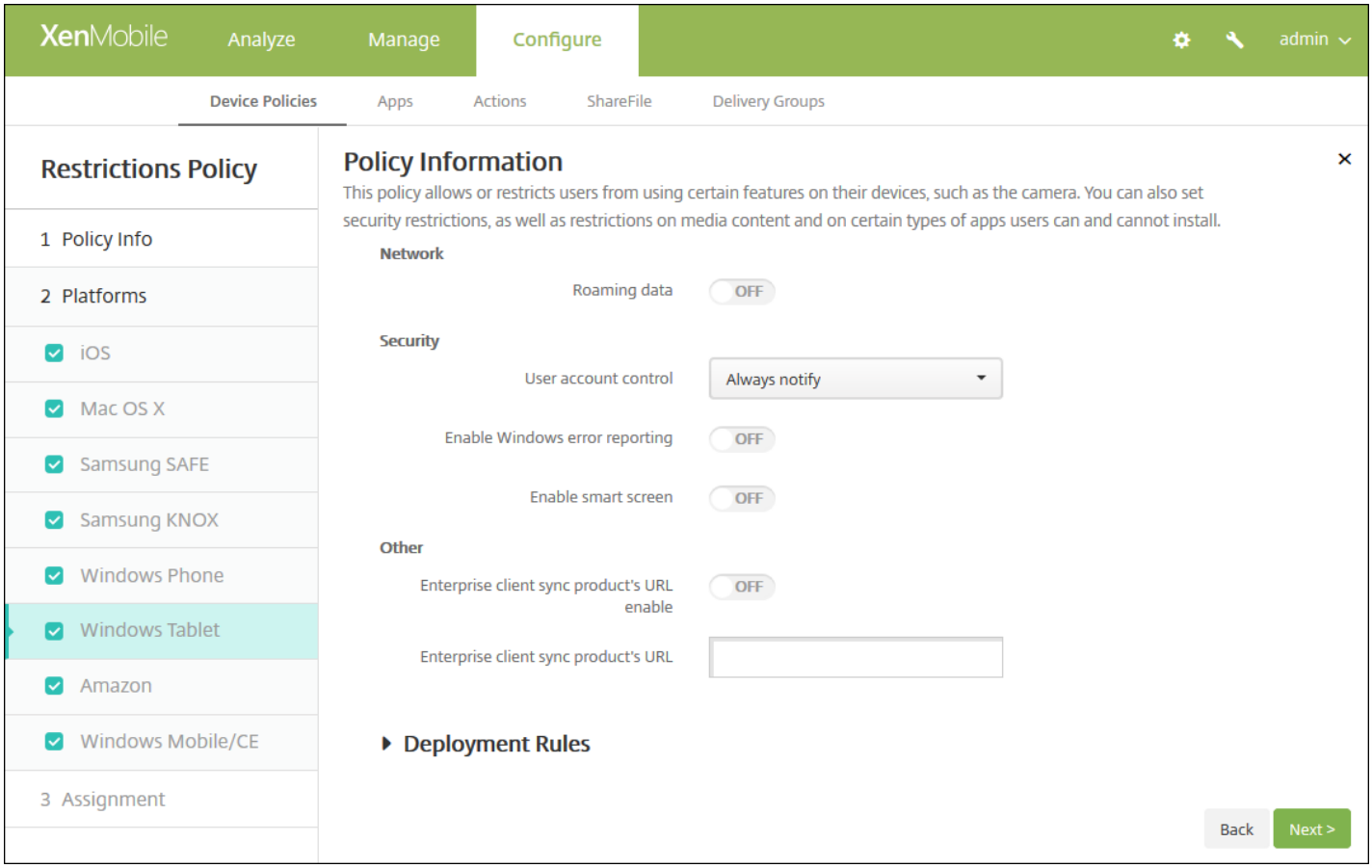
Samsung KNOXの設定の構成



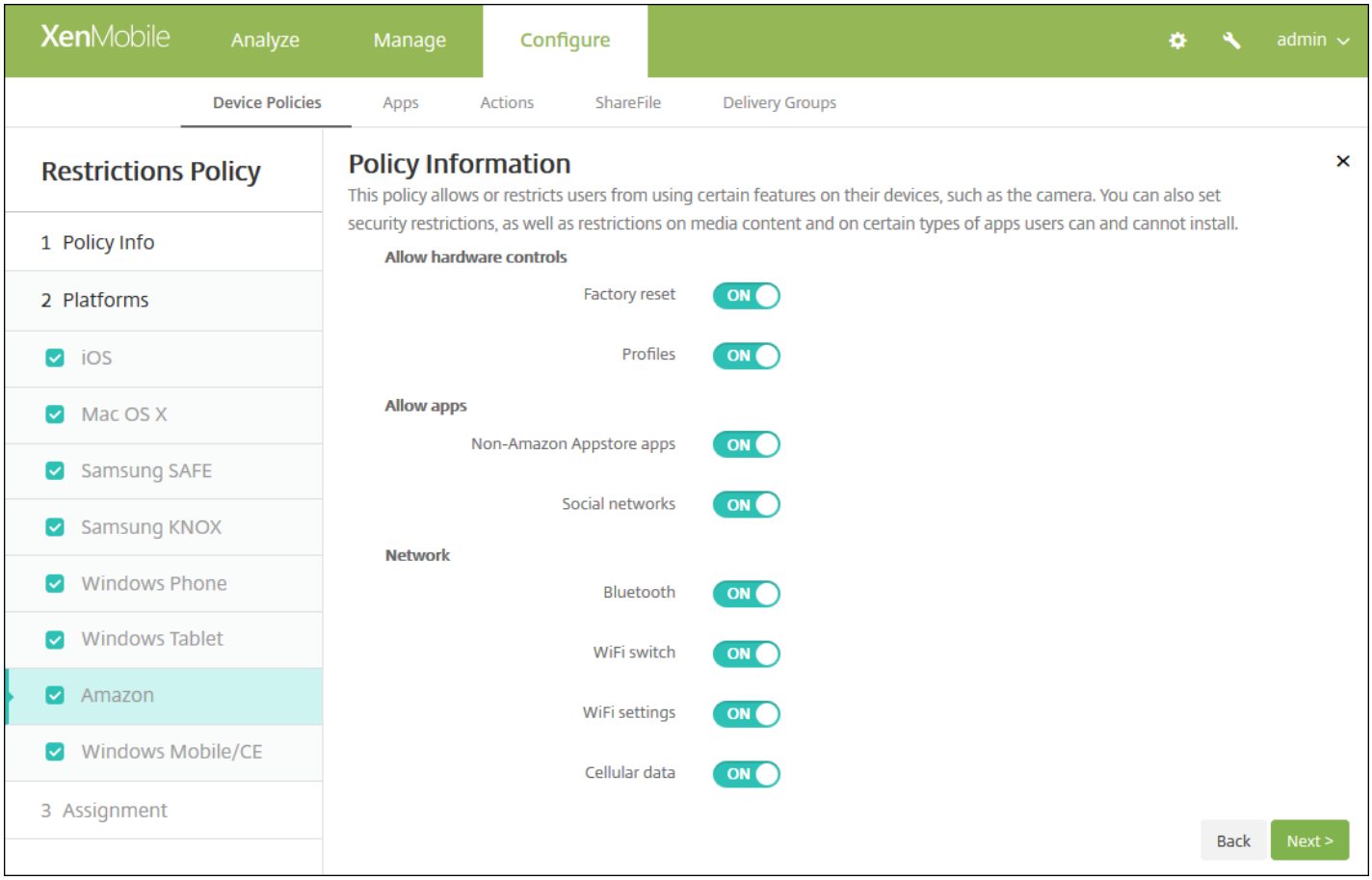
Windows Phoneの設定の構成



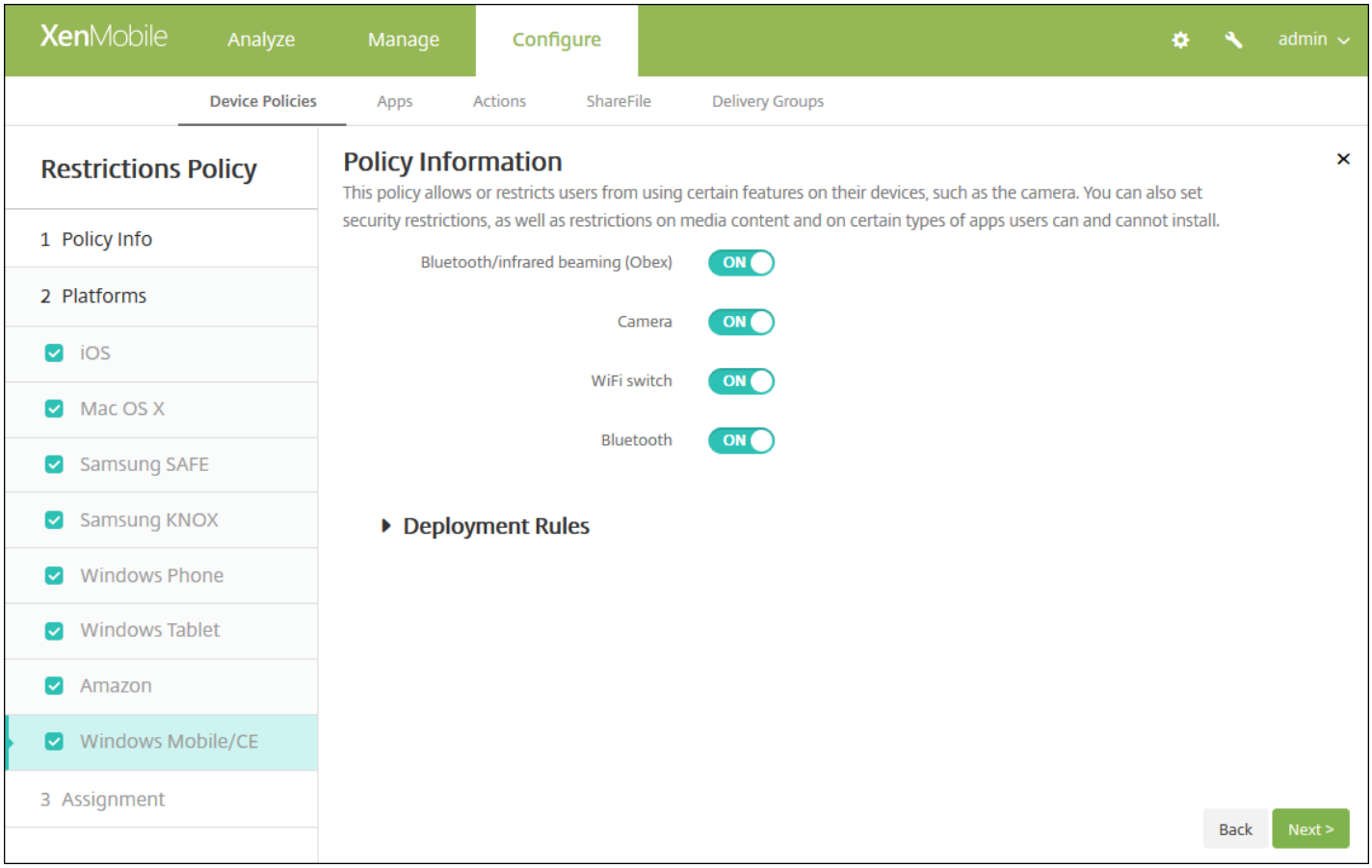
Windowsタブレットの設定の構成

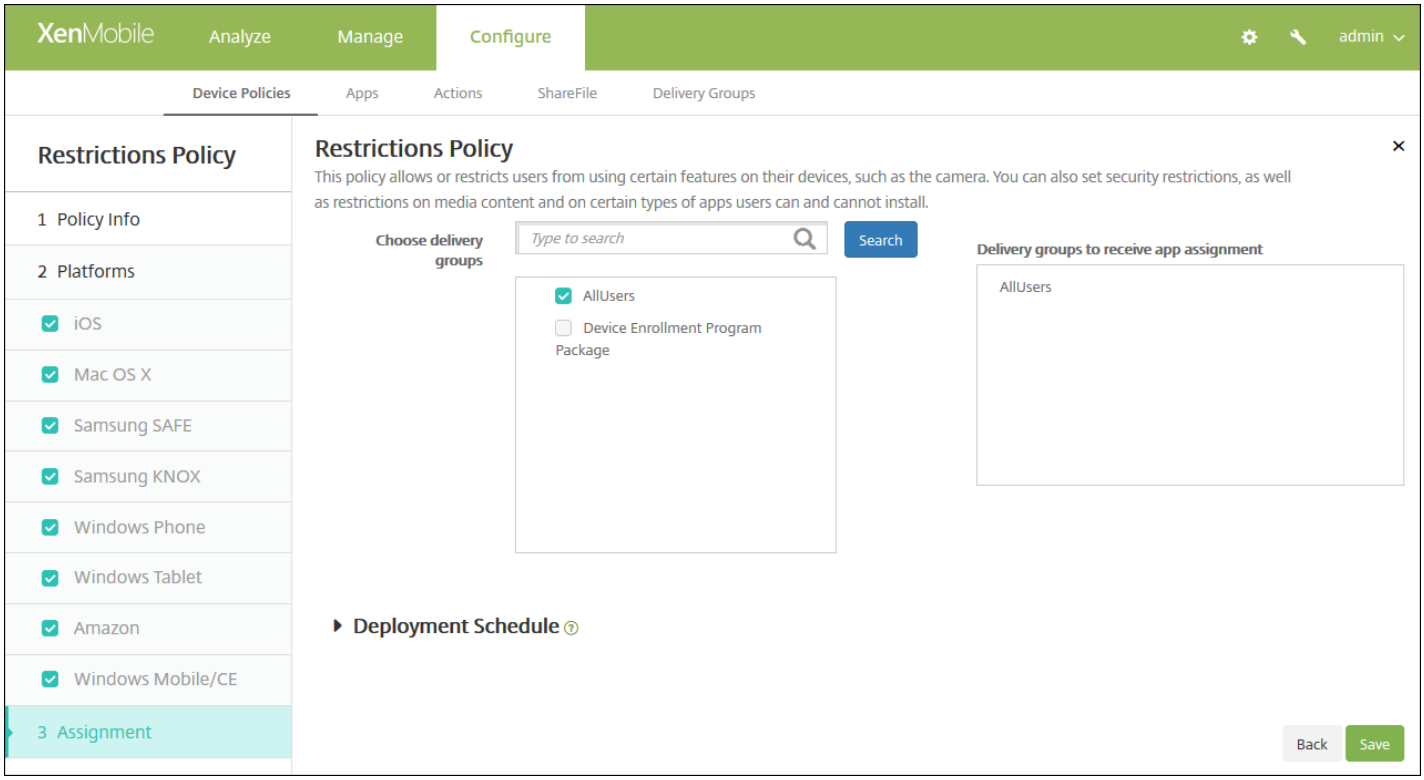


Amazonの設定の構成

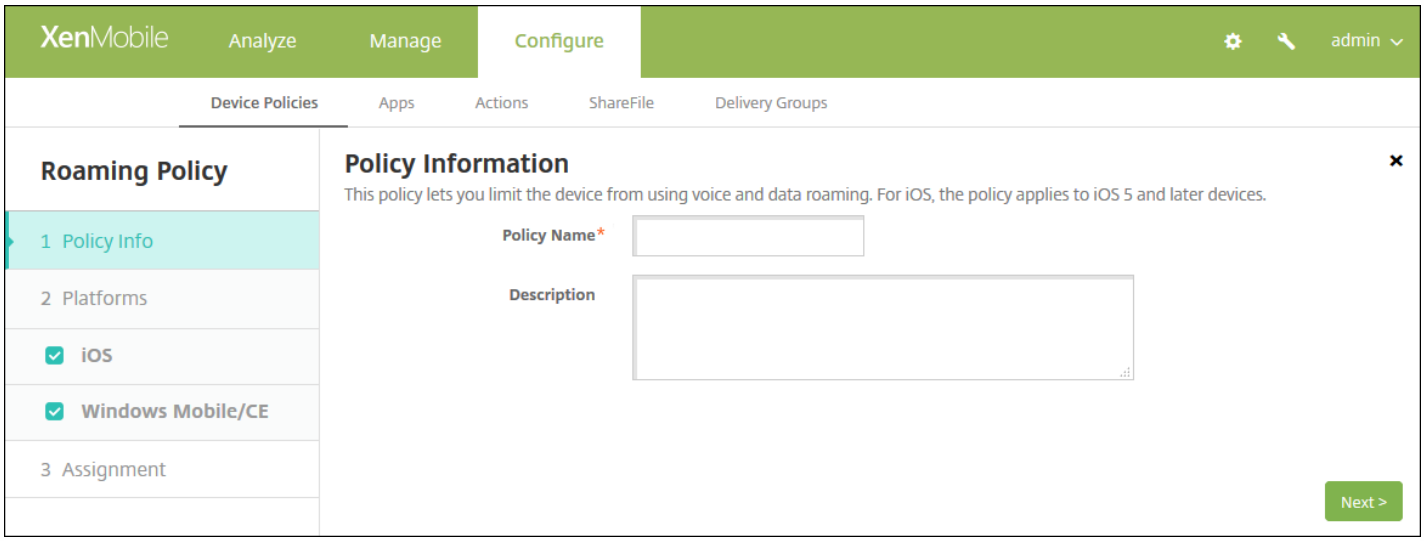


Windows Mobile/CEの設定の構成



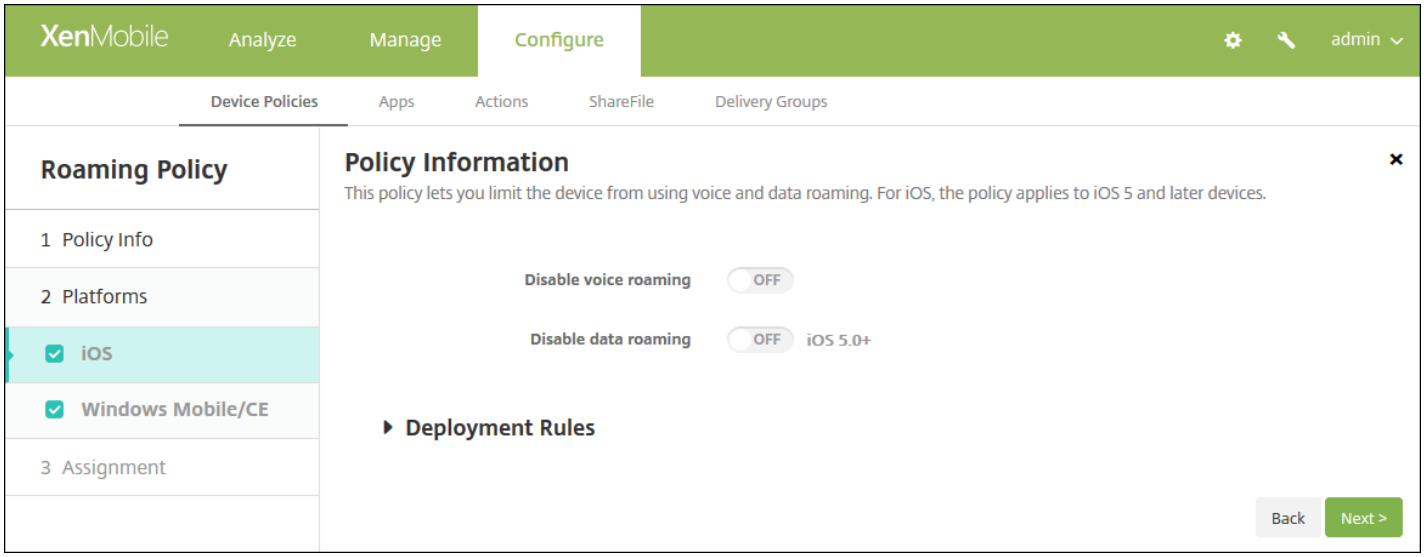


-
-
-
-
-
-
-



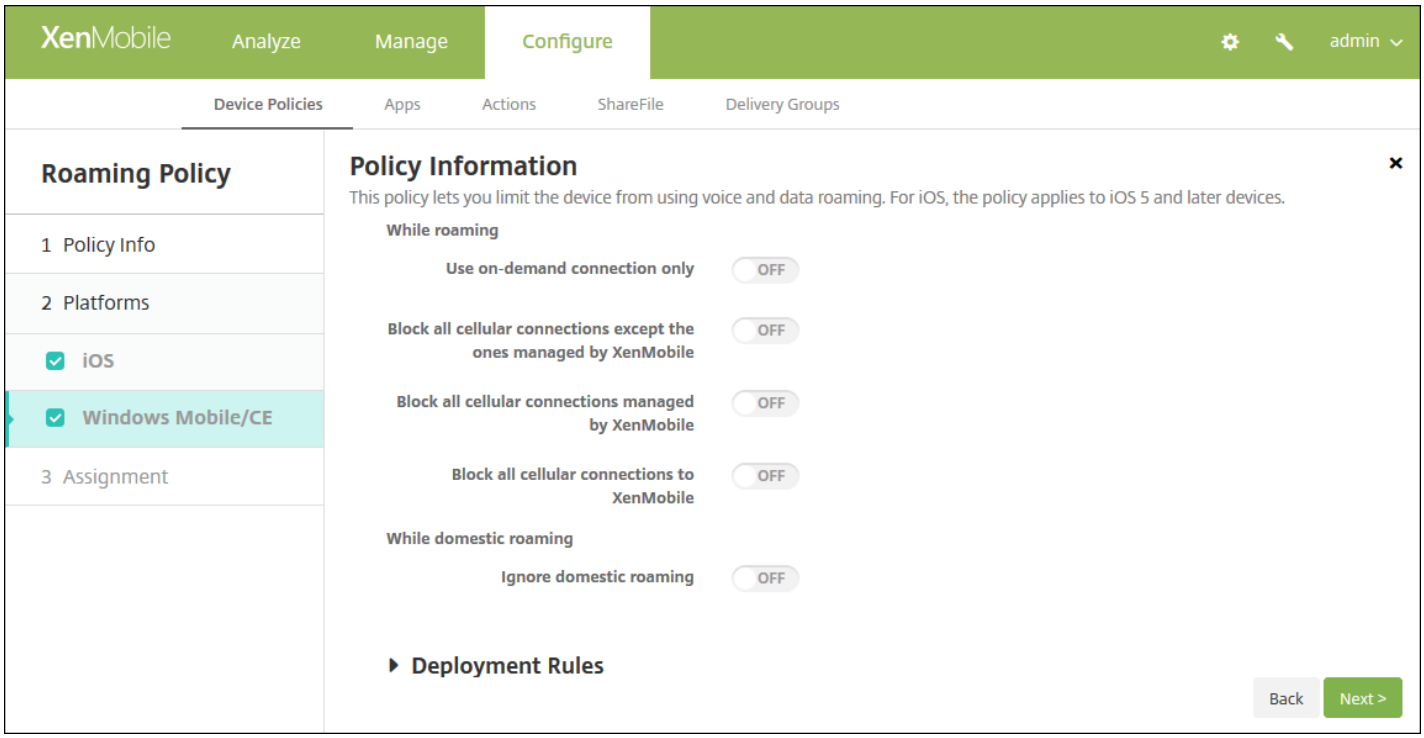
-
-

iOSの設定の構成



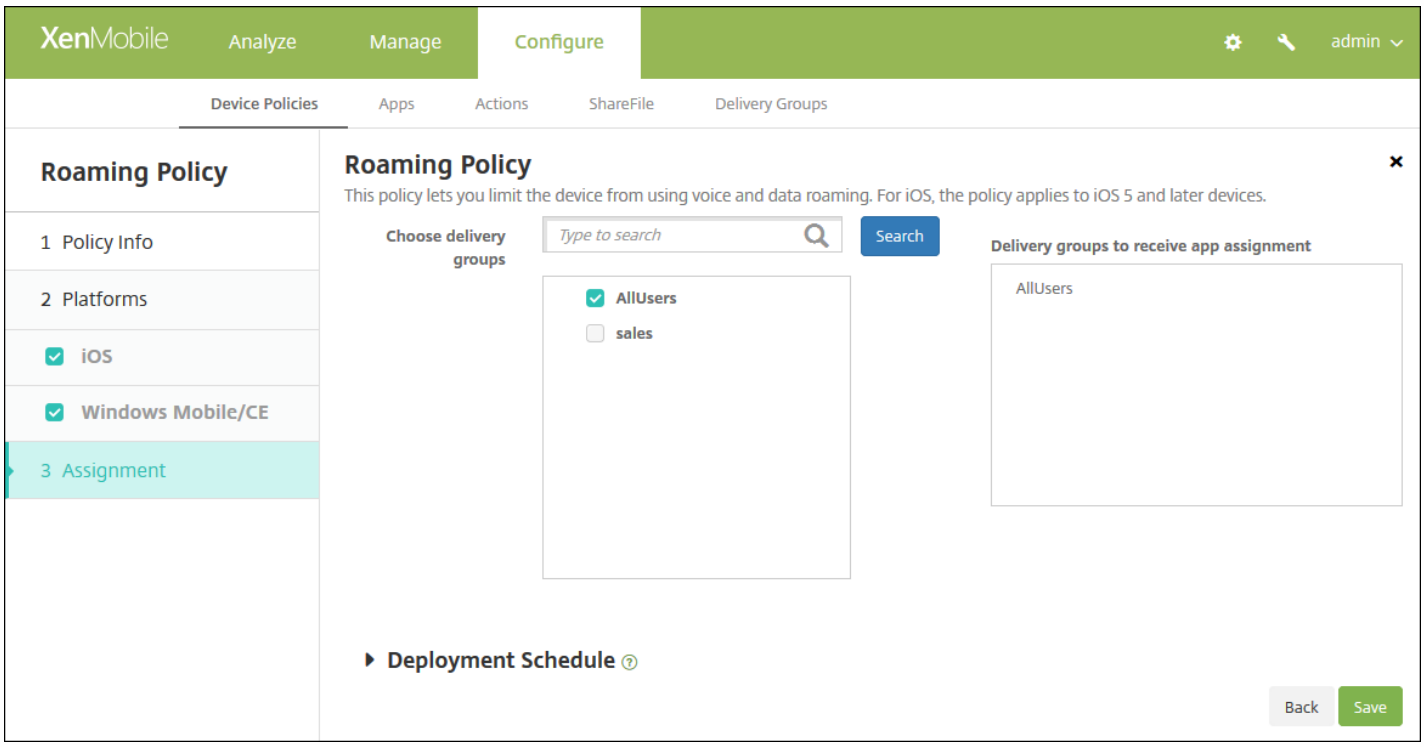
-
-

Windows Mobile/CEの設定の構成



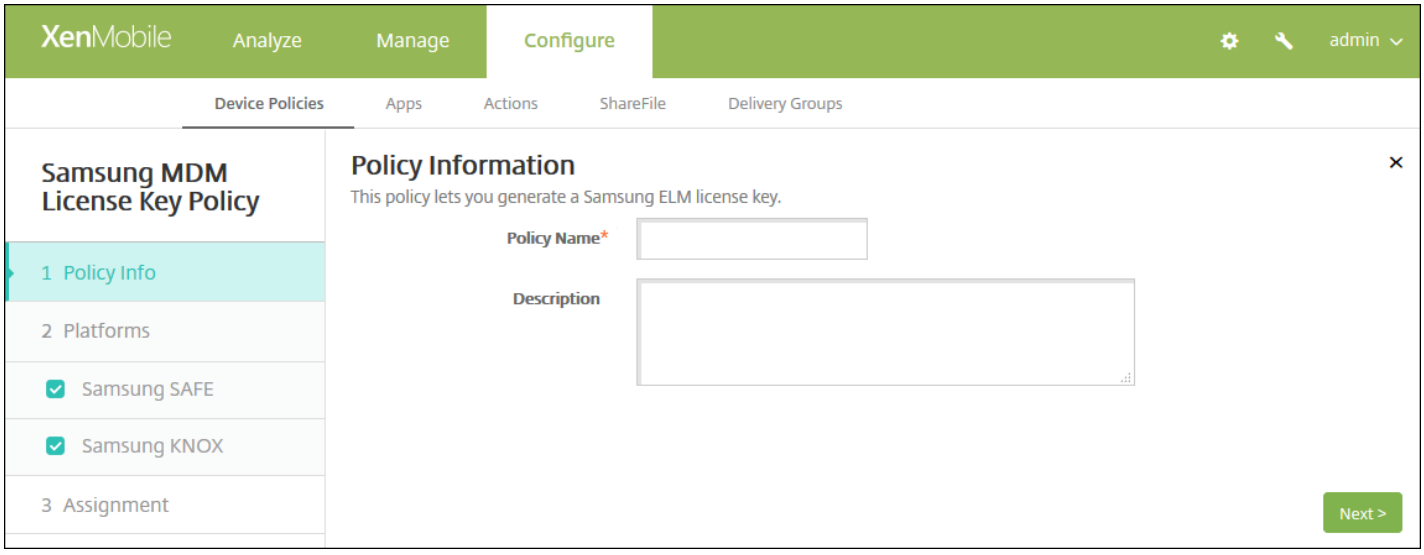
-
  -

-
-
-
-
-



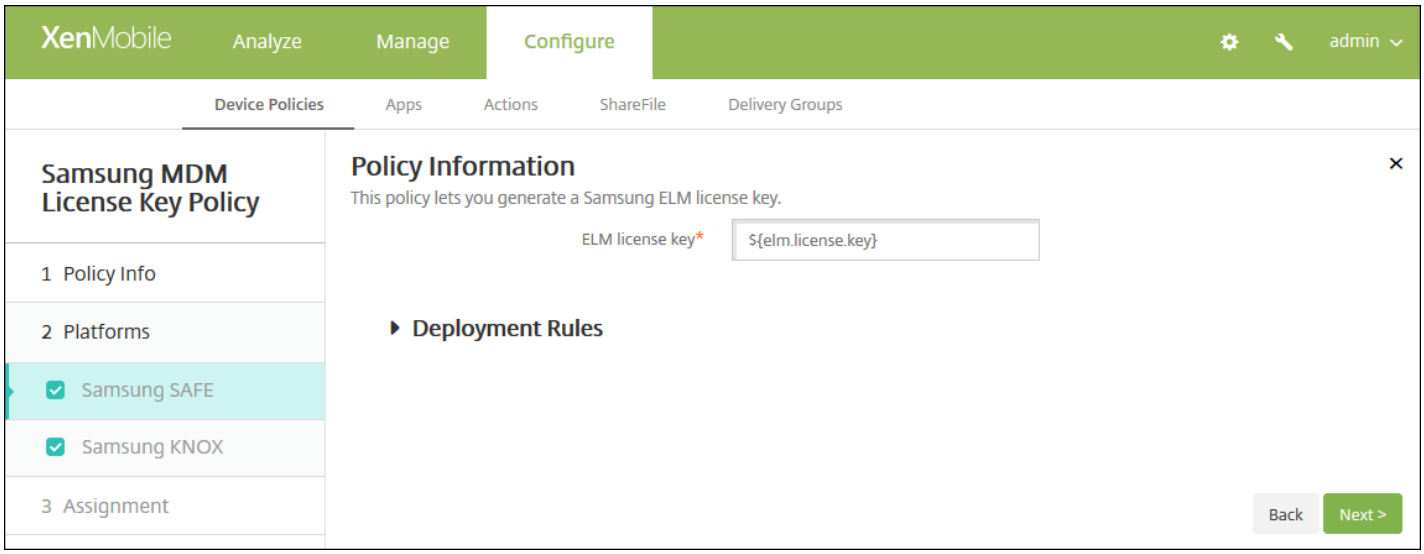
-

-
-
-
-
-
-



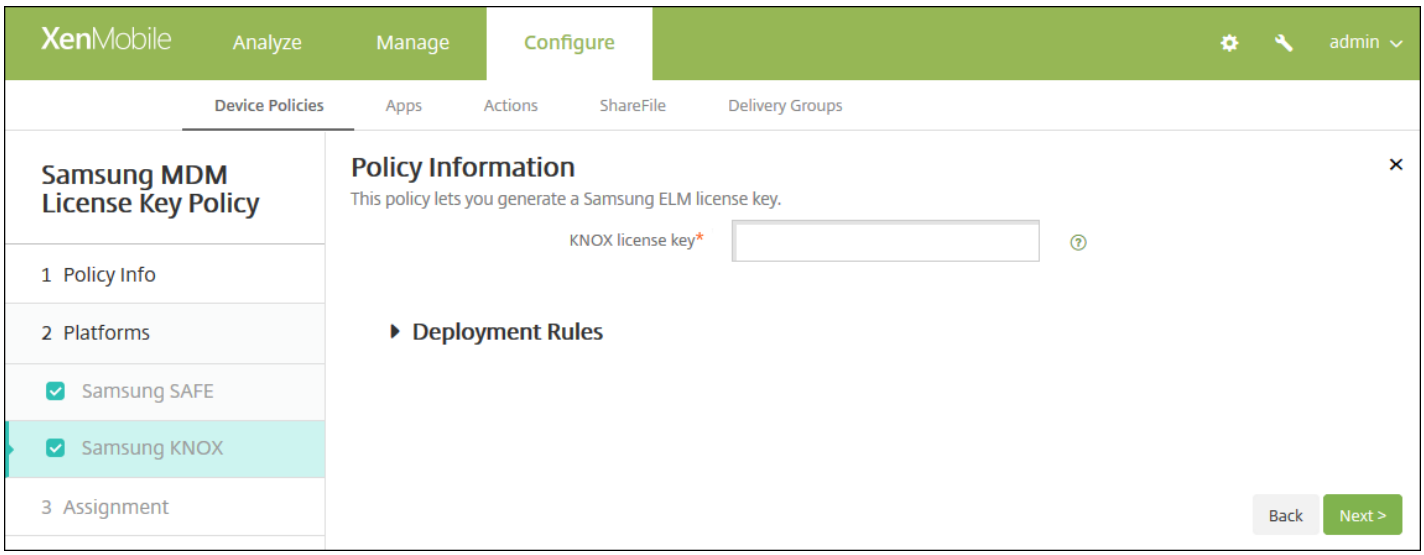
-
-

Samsung SAFEの設定の構成

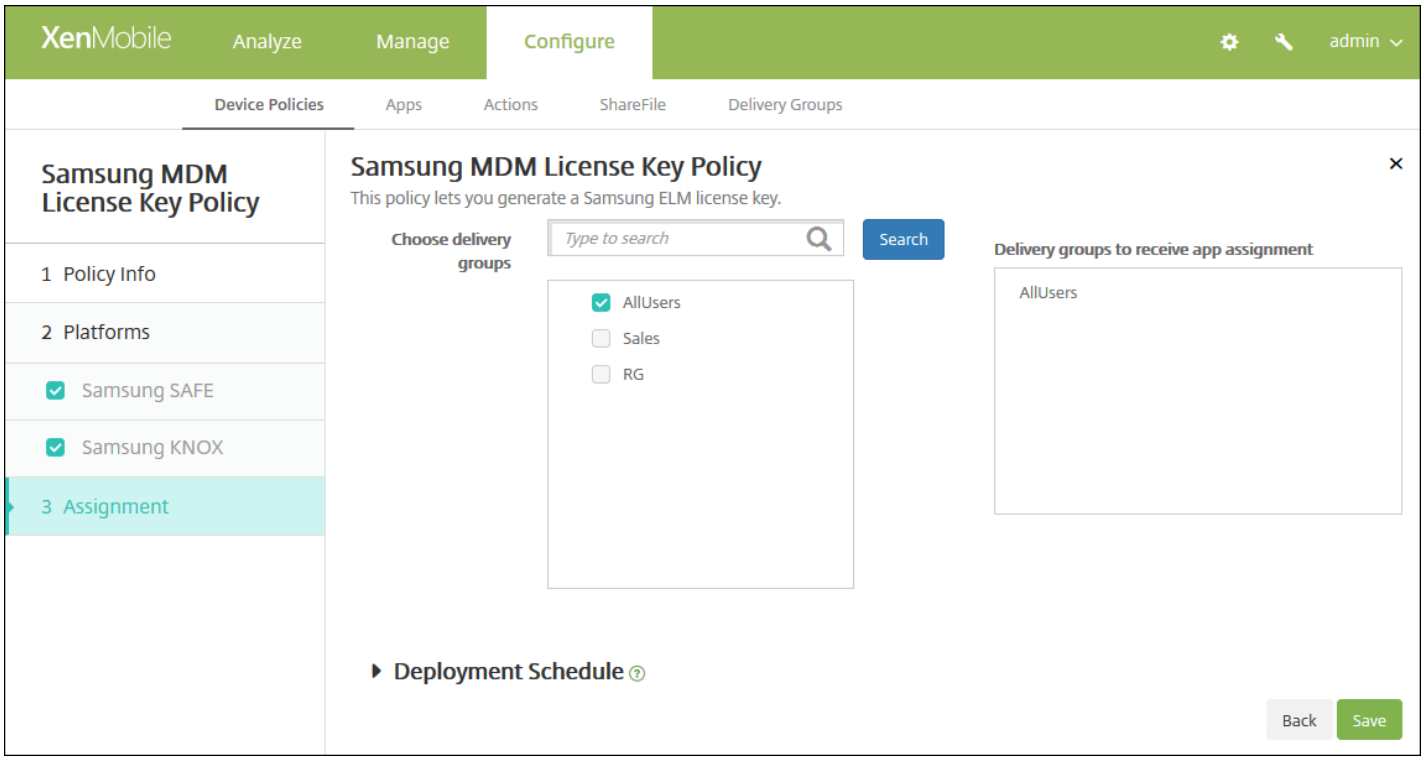


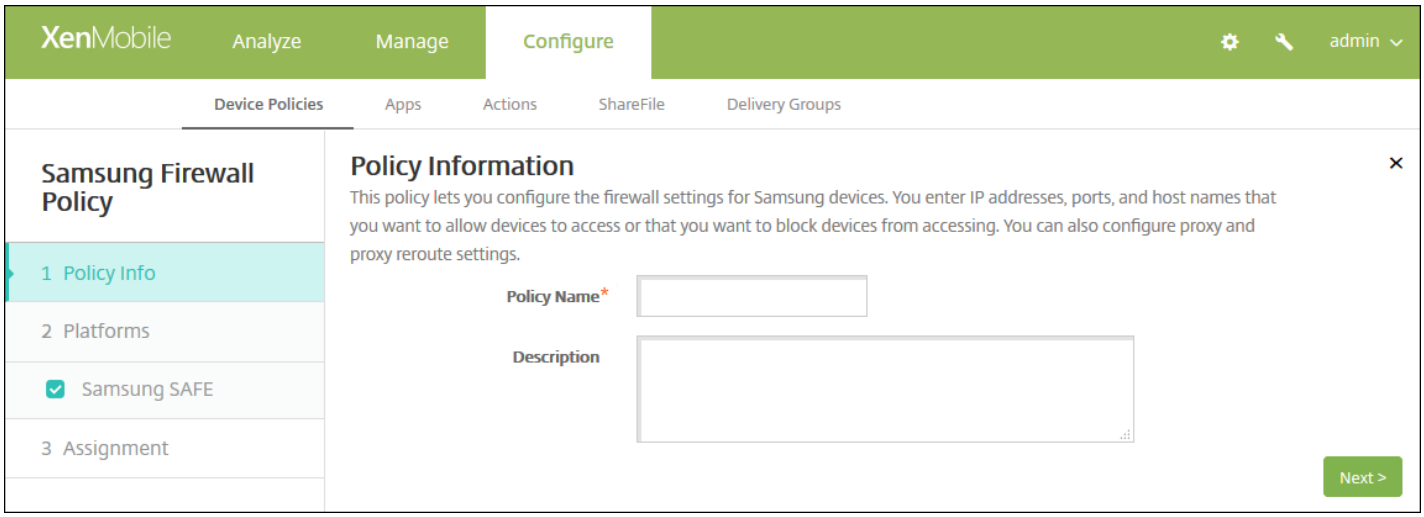
-

Samsung KNOXの設定の構成

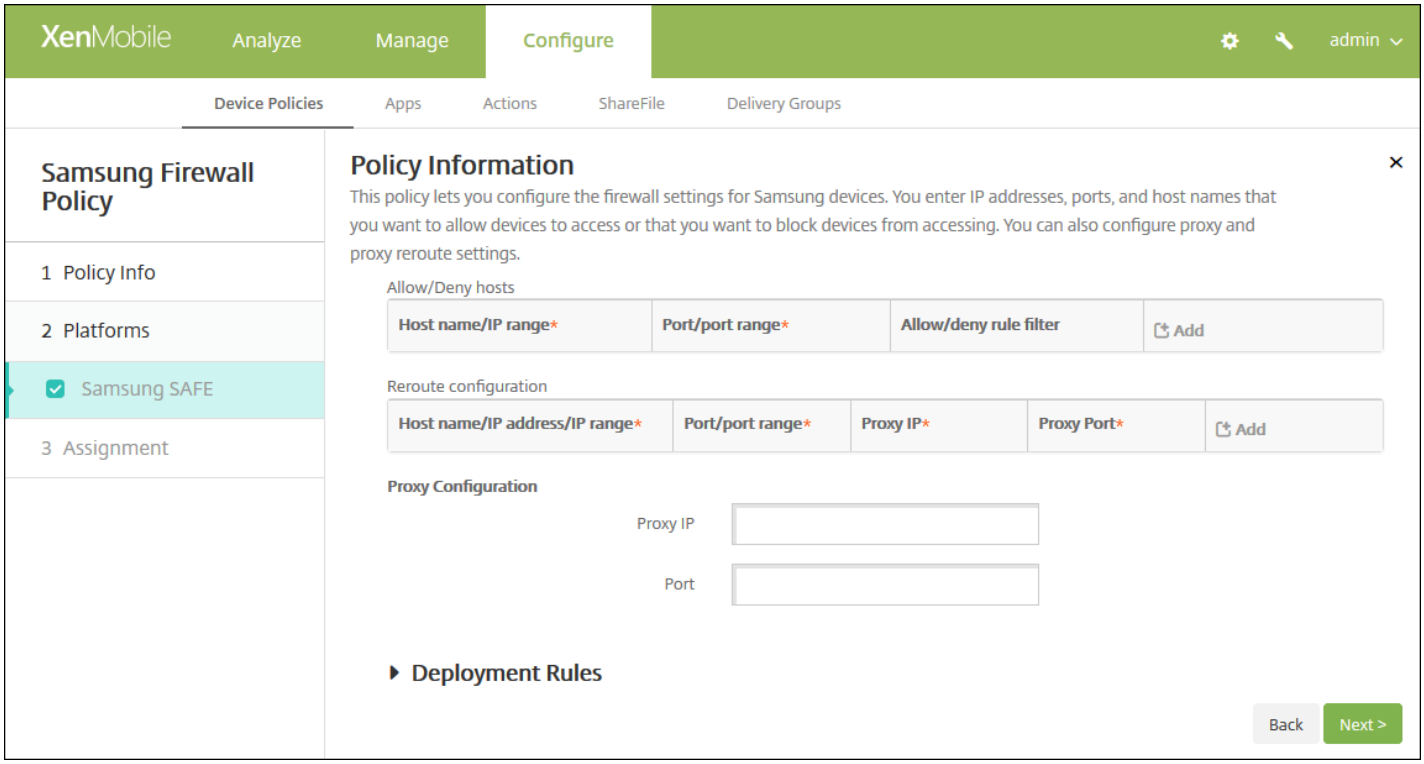


-

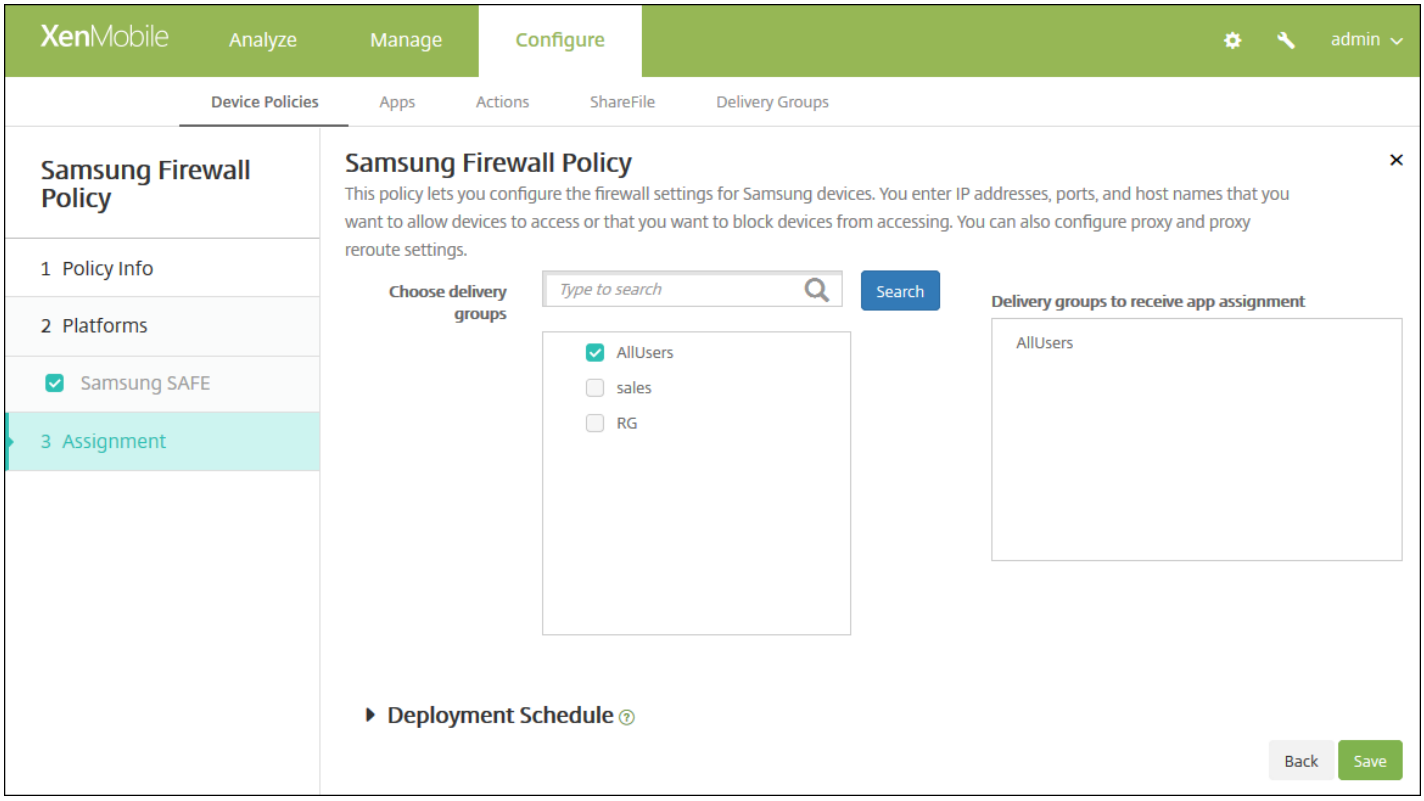




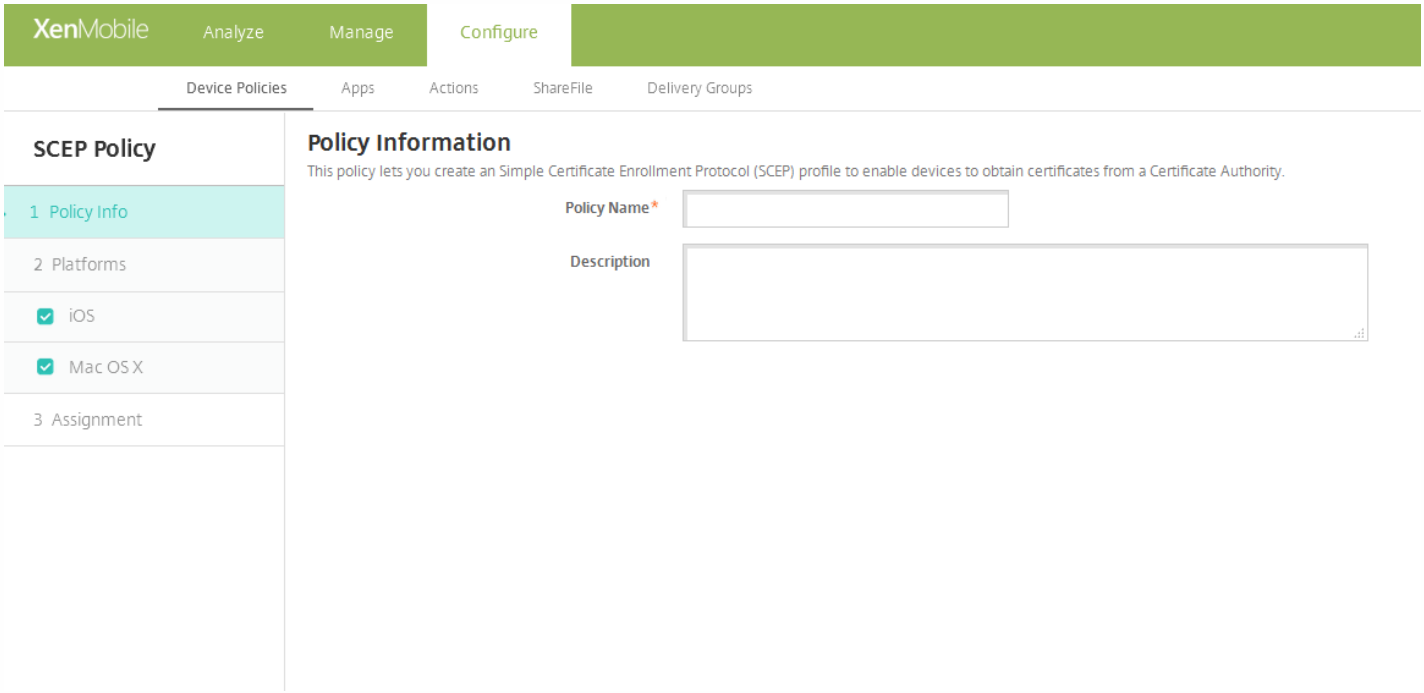
-
-



-
  -
    -
    -
    -
  -
-
  -
    -
    -
    -
    -
    -
-
  -
  -

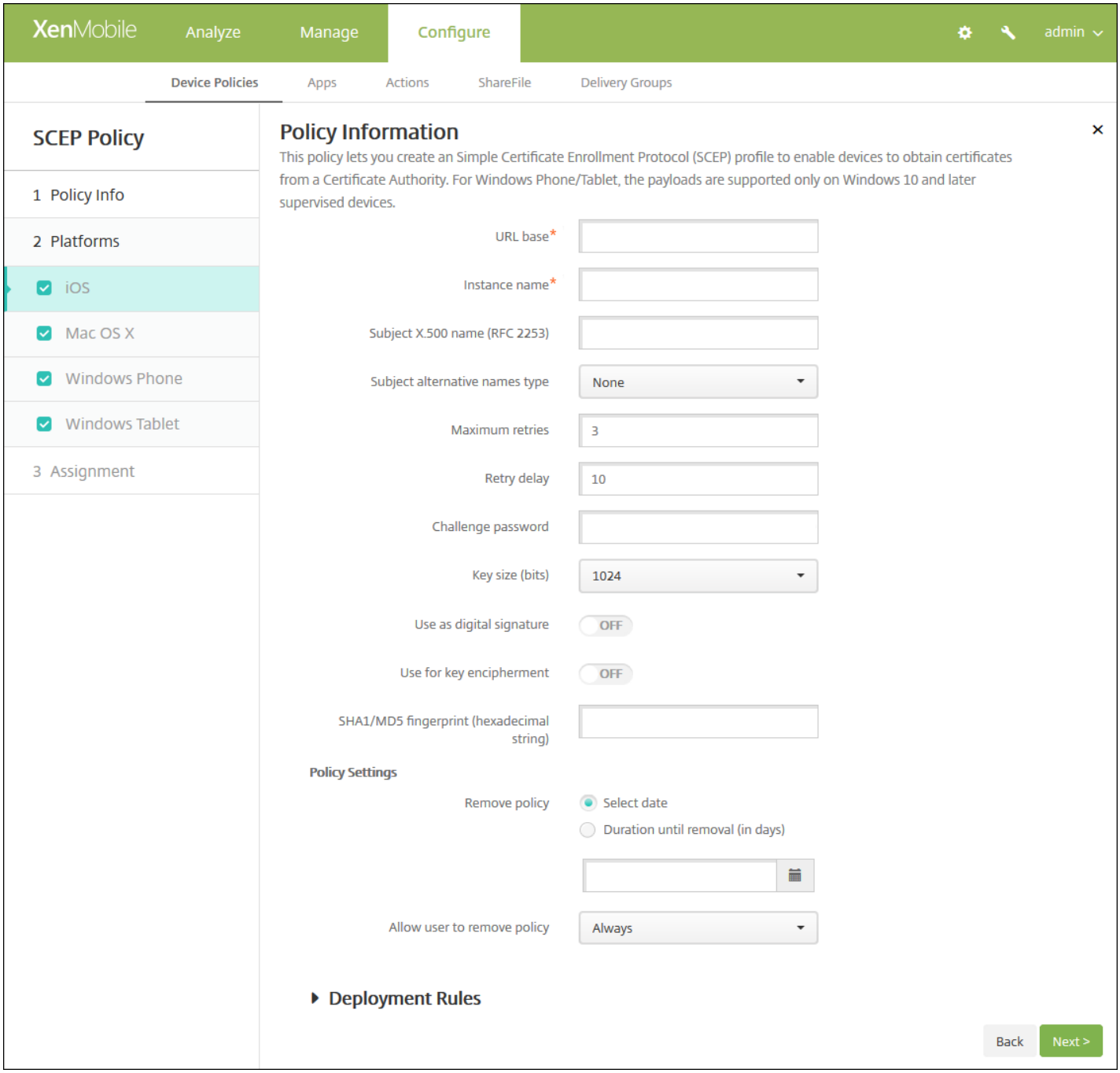


-
-
-
-
-
-
-



-
-

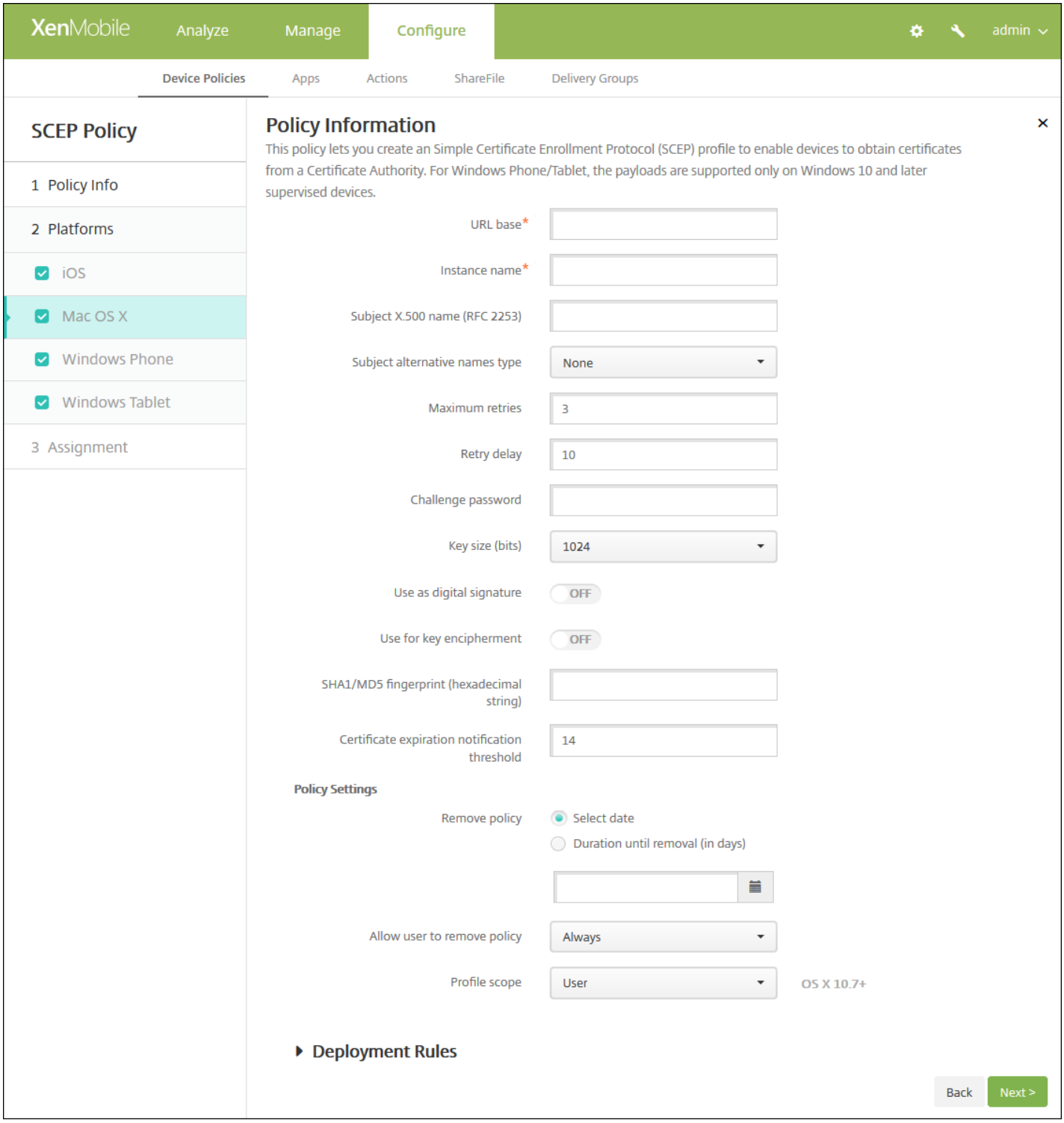
iOSの設定の構成



-
-

-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -

Mac OS Xの設定の構成

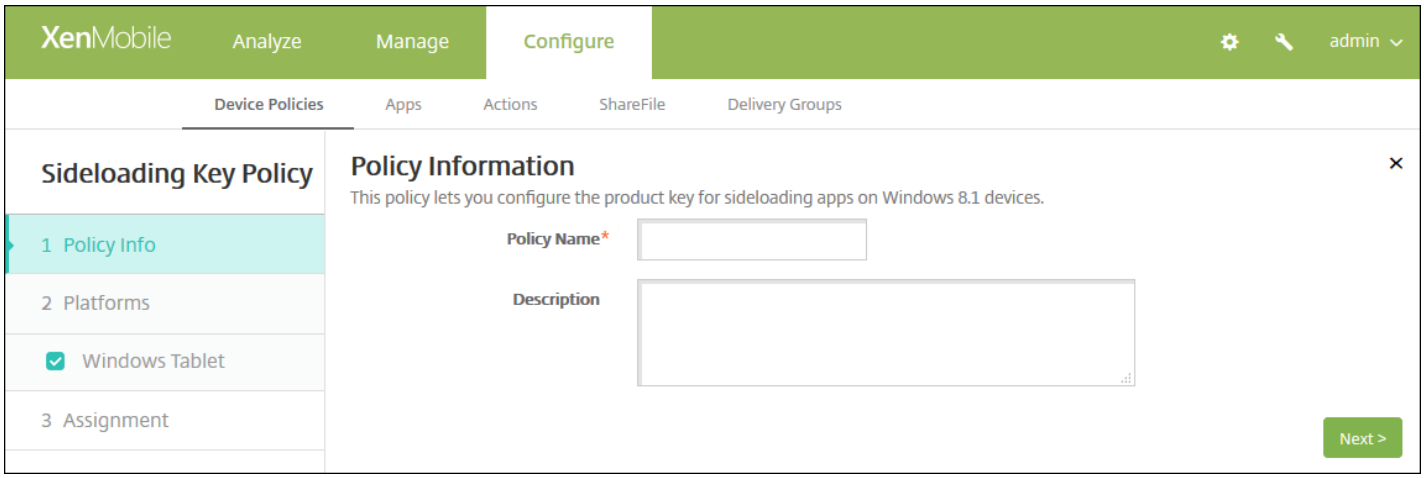


-
-

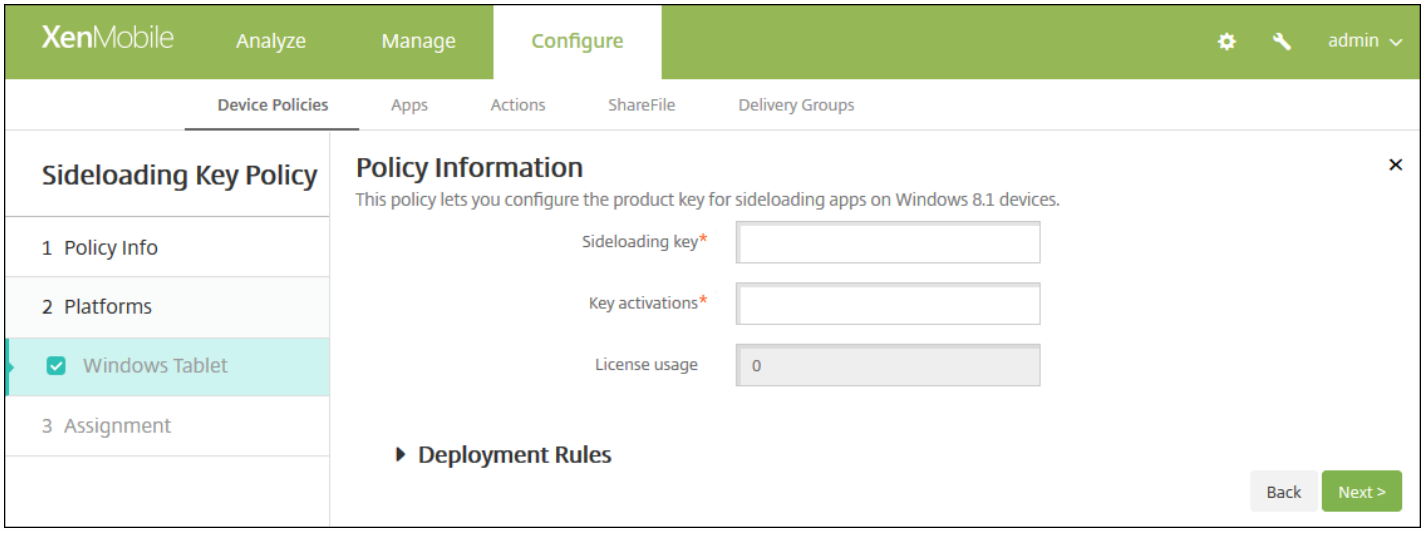
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -
  -
-

-
-
-
-
-
-

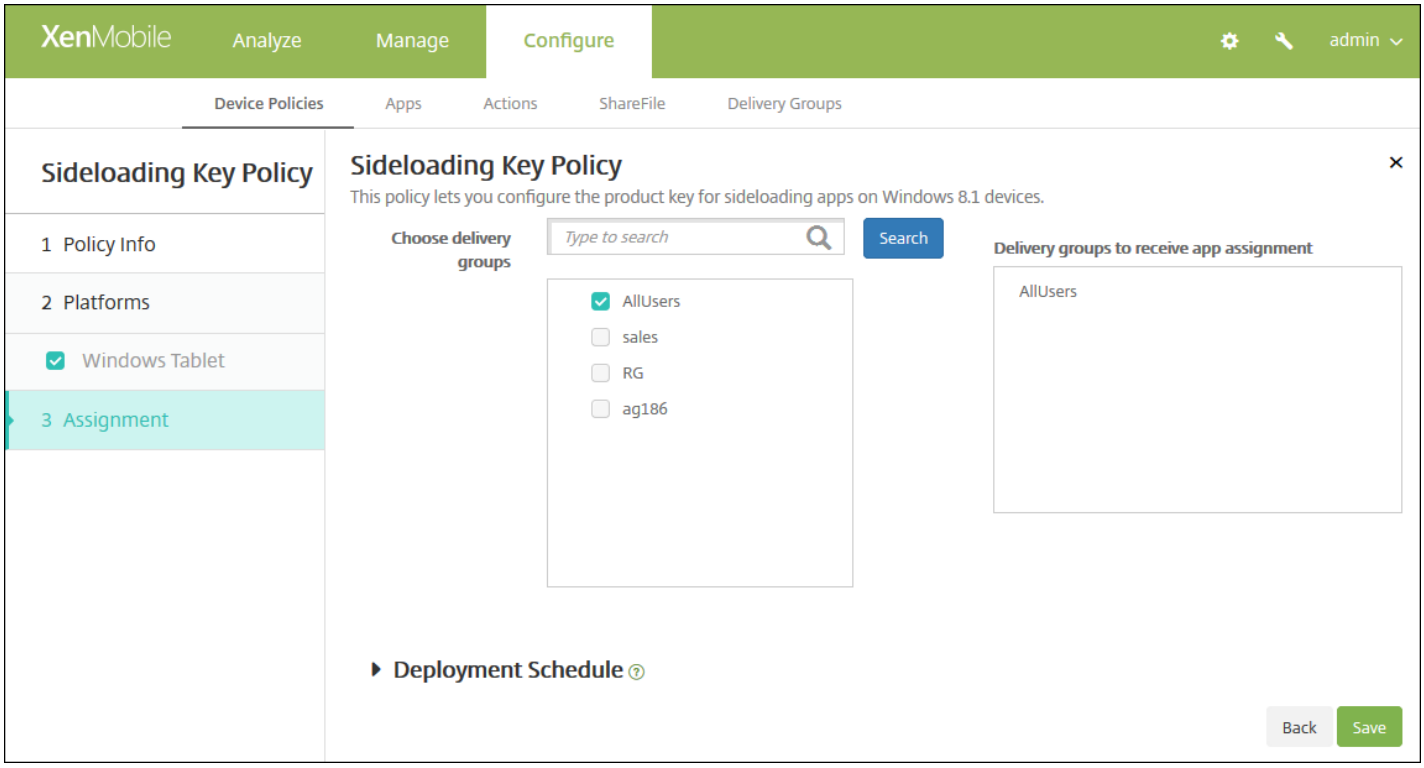
-
-



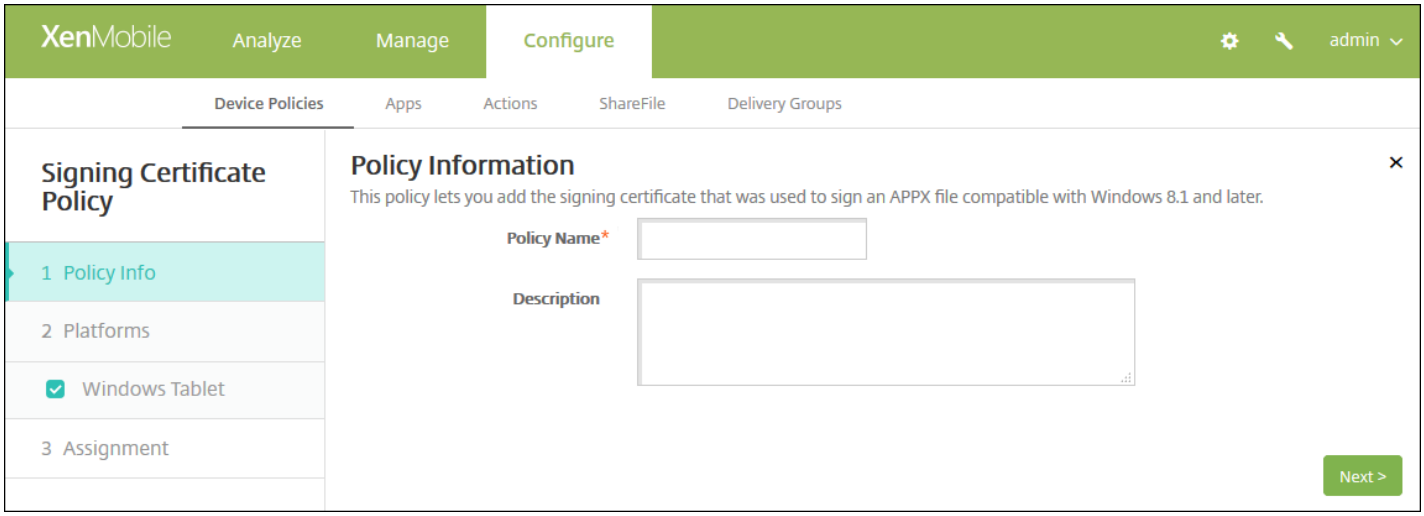
-
-



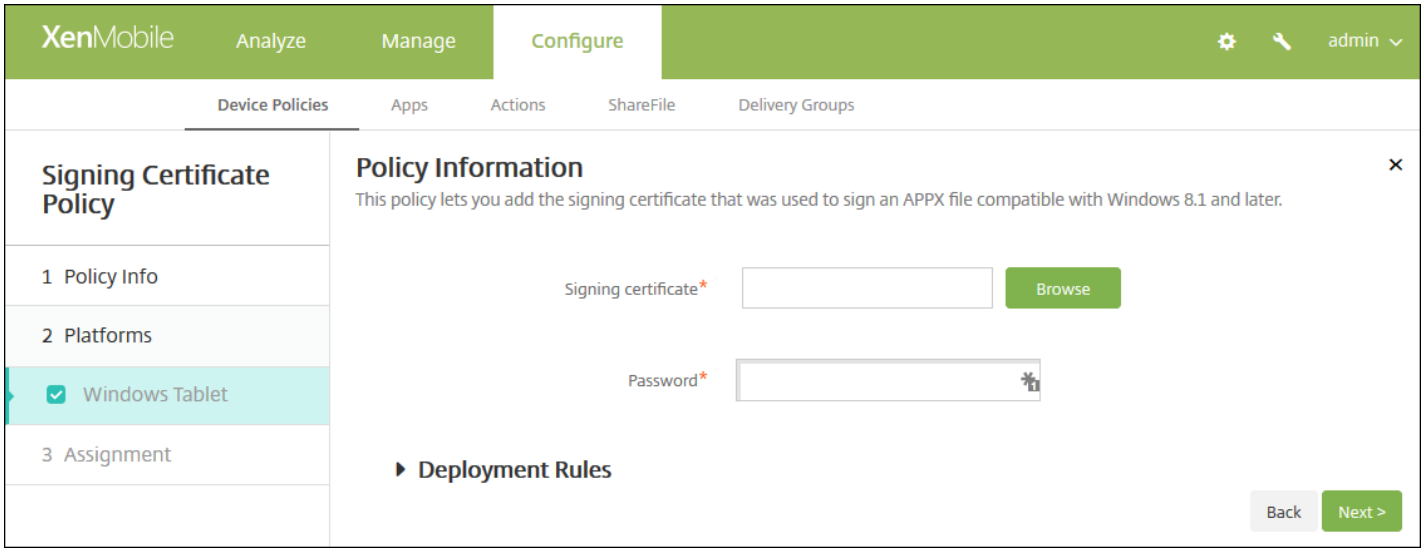
-
-
-



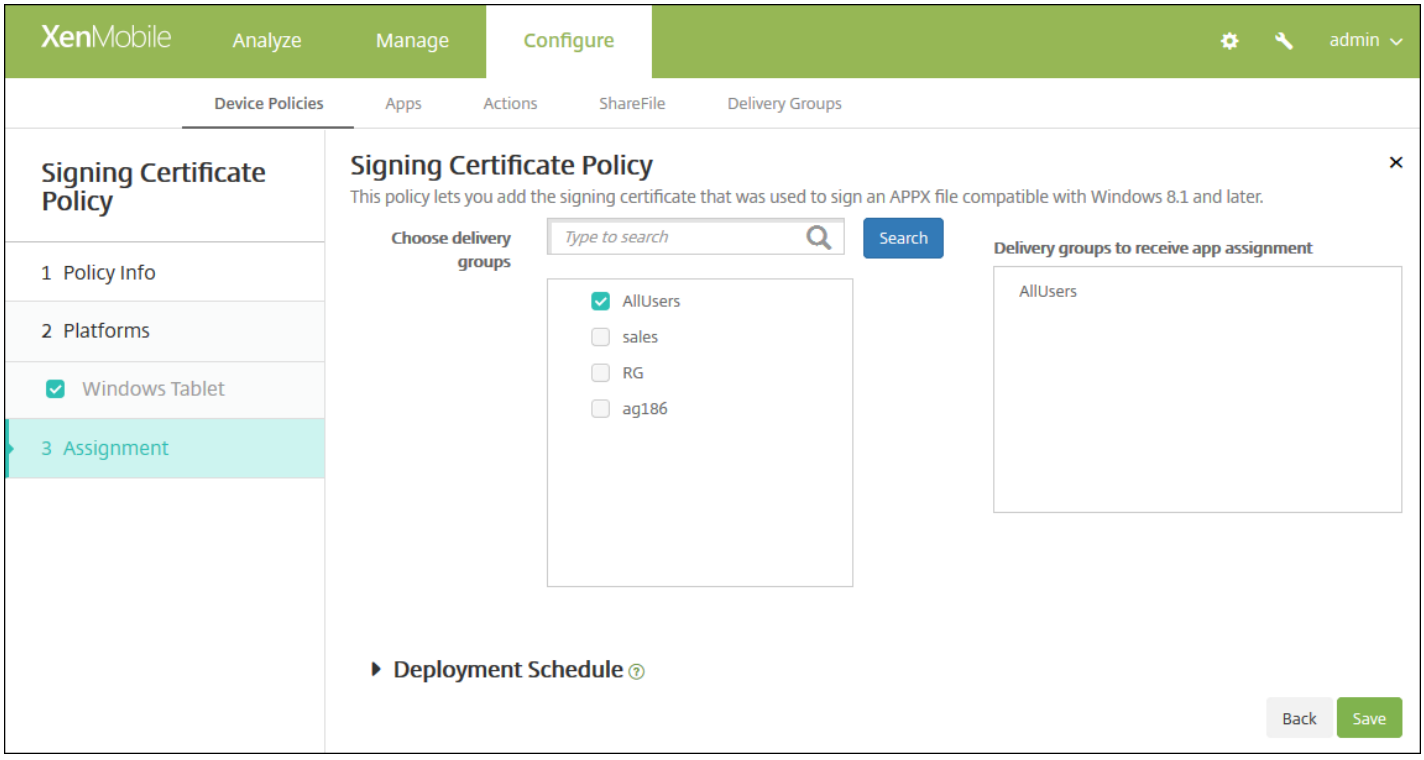
-
-
-
-
-
-
-



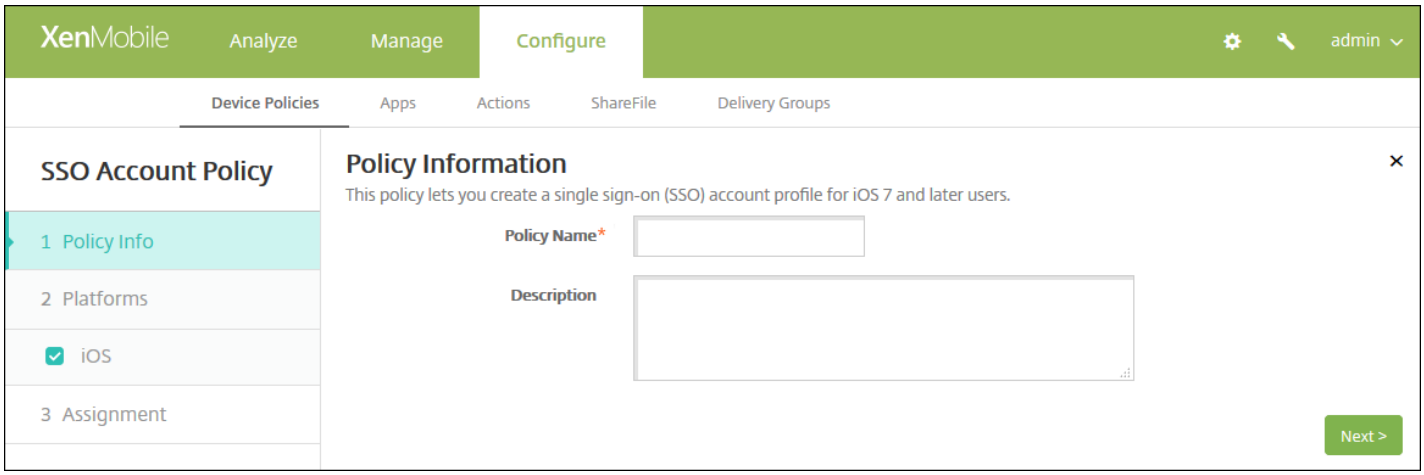
-
-



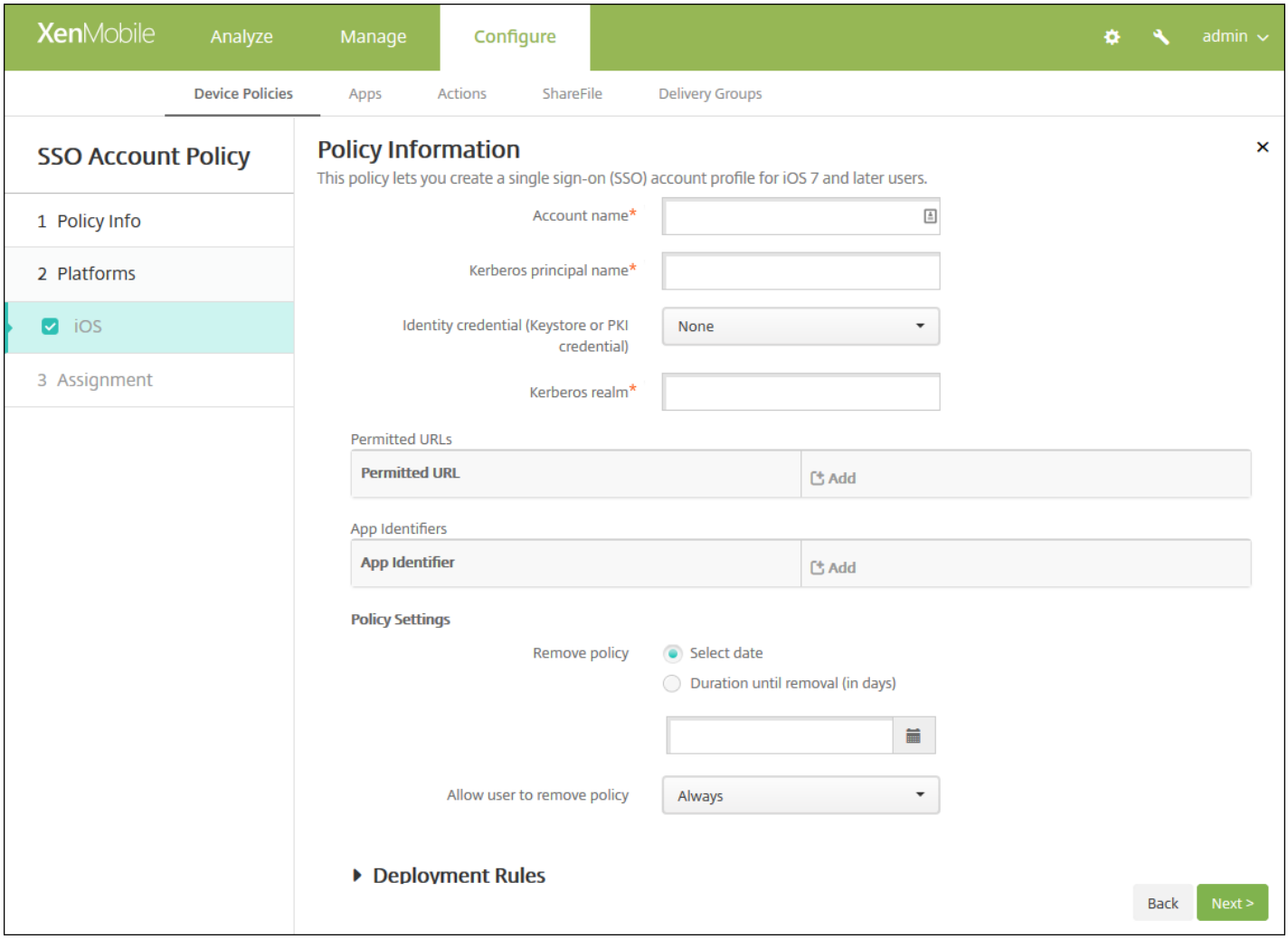
-
-



-
-
-
-
-
-
-

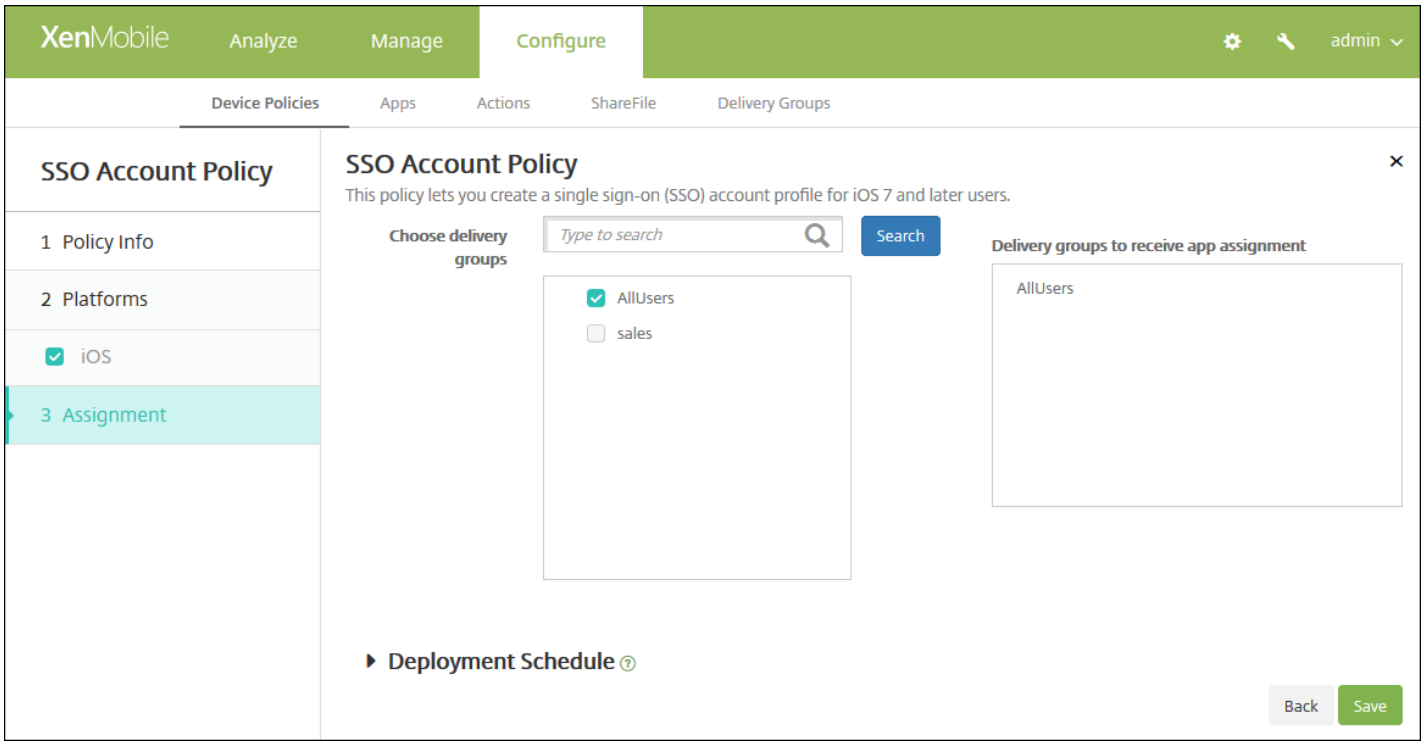


-
-

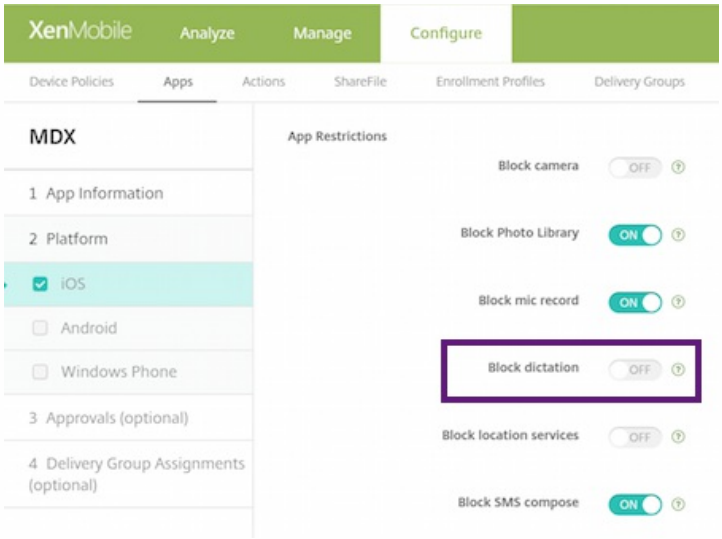


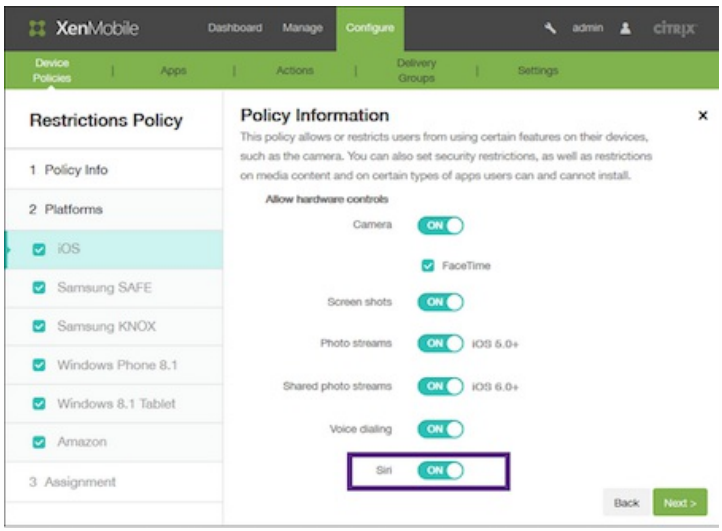
-
-
-
-
-
  -
  -

-
  -
  -
-
  -
  -
  -
  -



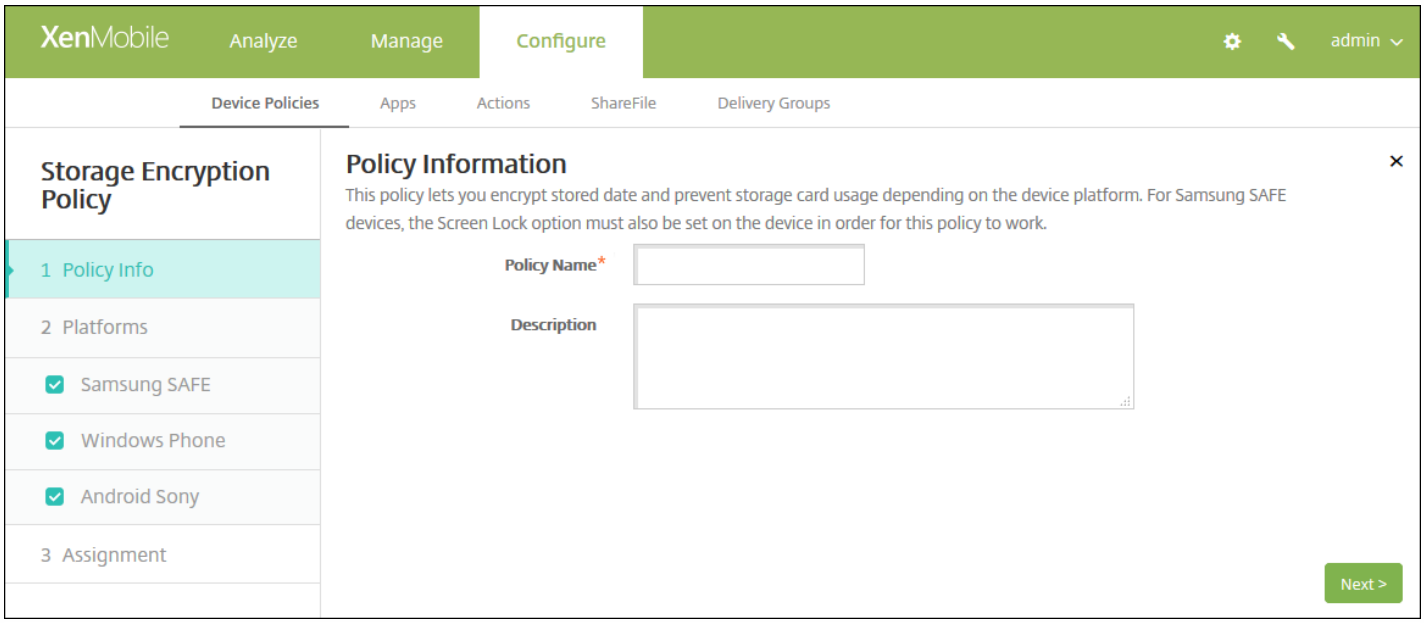
-
-
-
-
-
-
-





-
-

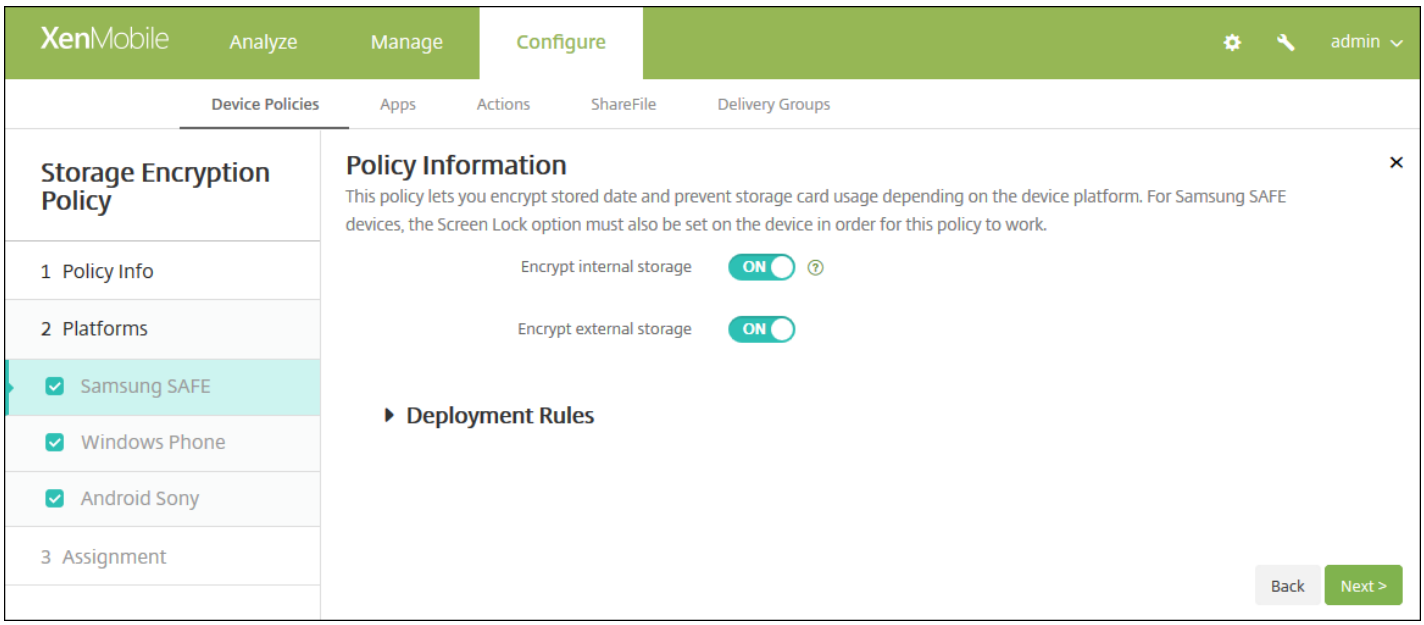
-
-
-



-

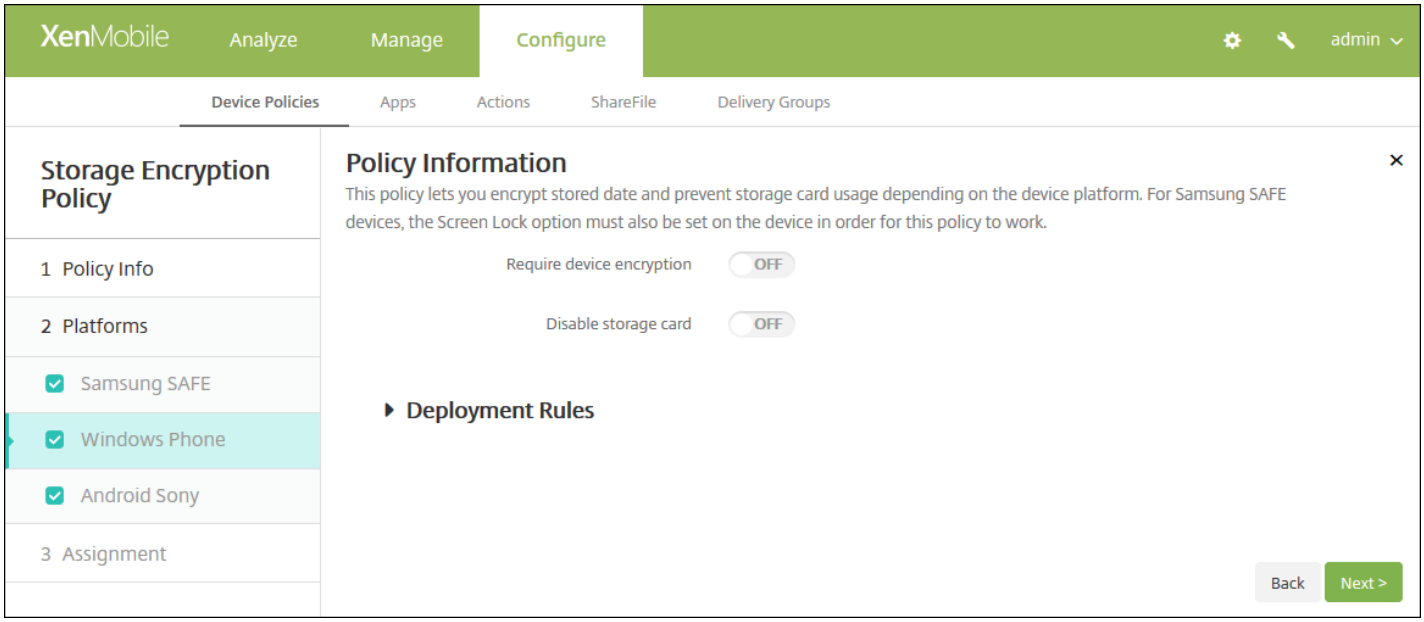
-

Samsung SAFEの設定の構成



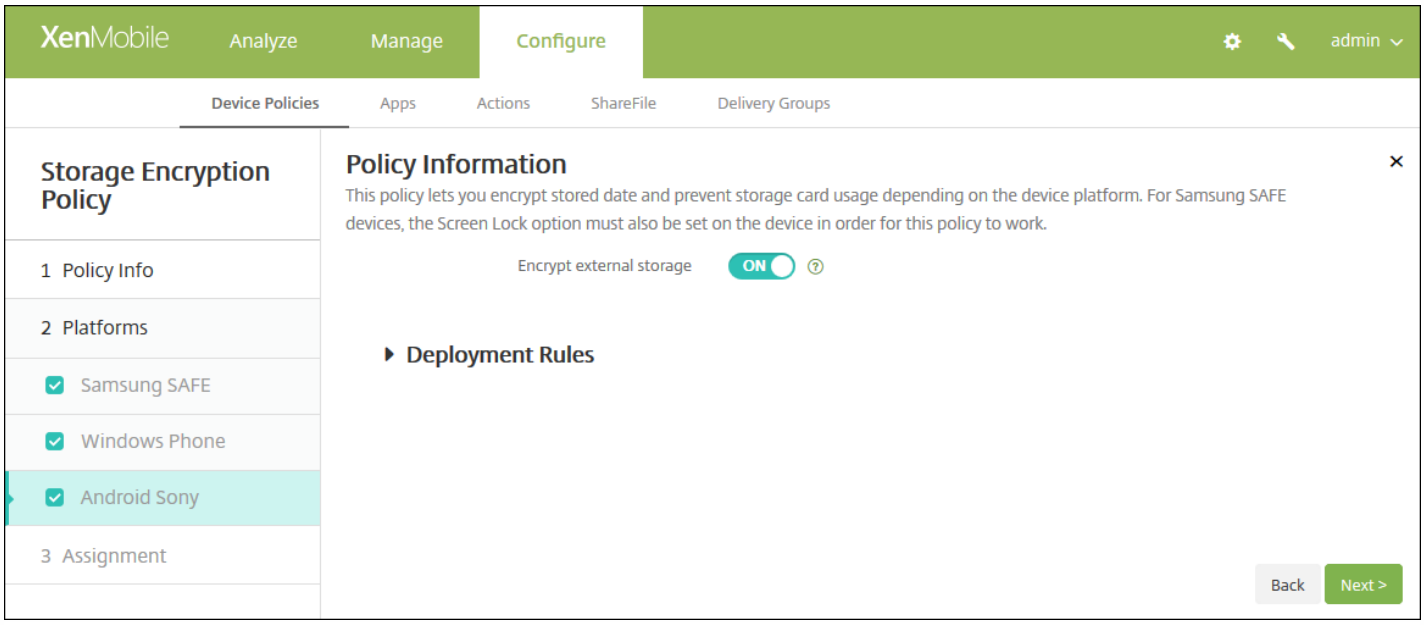
-
-

Windows Phoneの設定の構成

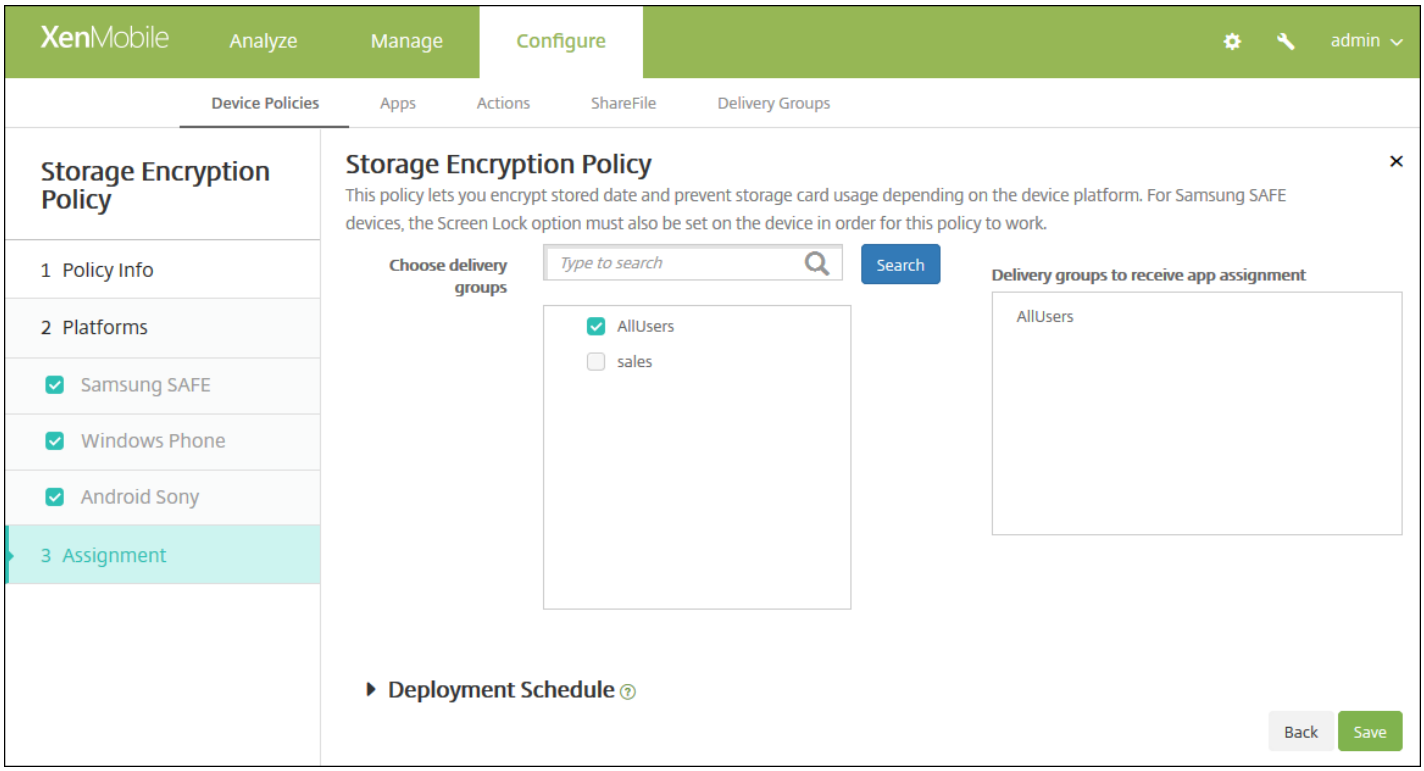


-
-

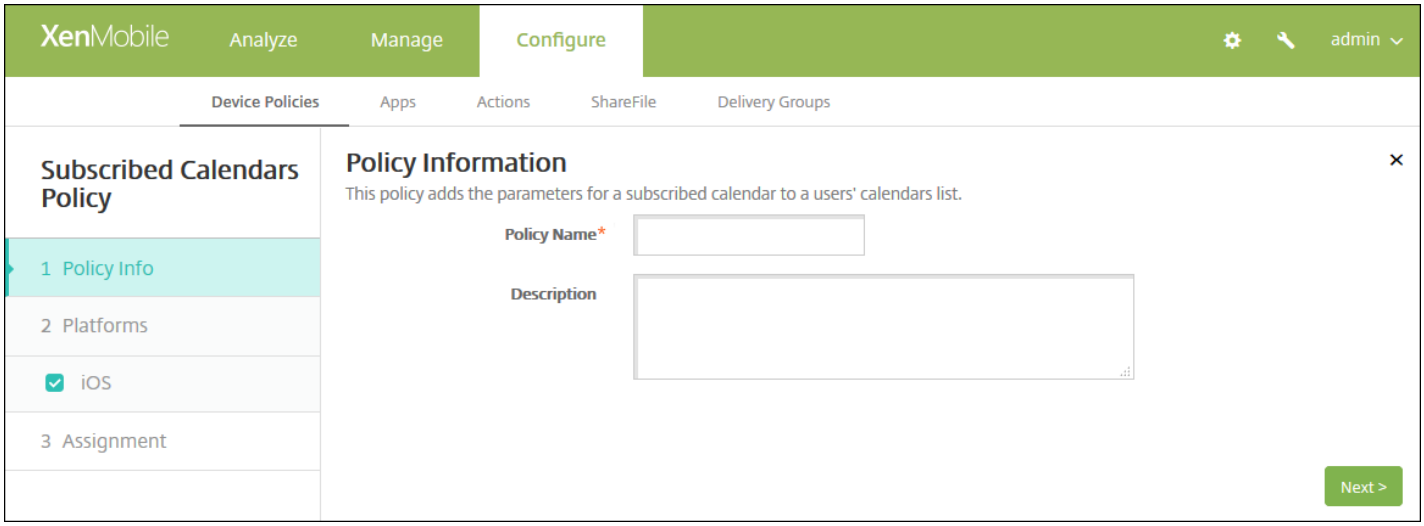
Android Sonyの設定の構成



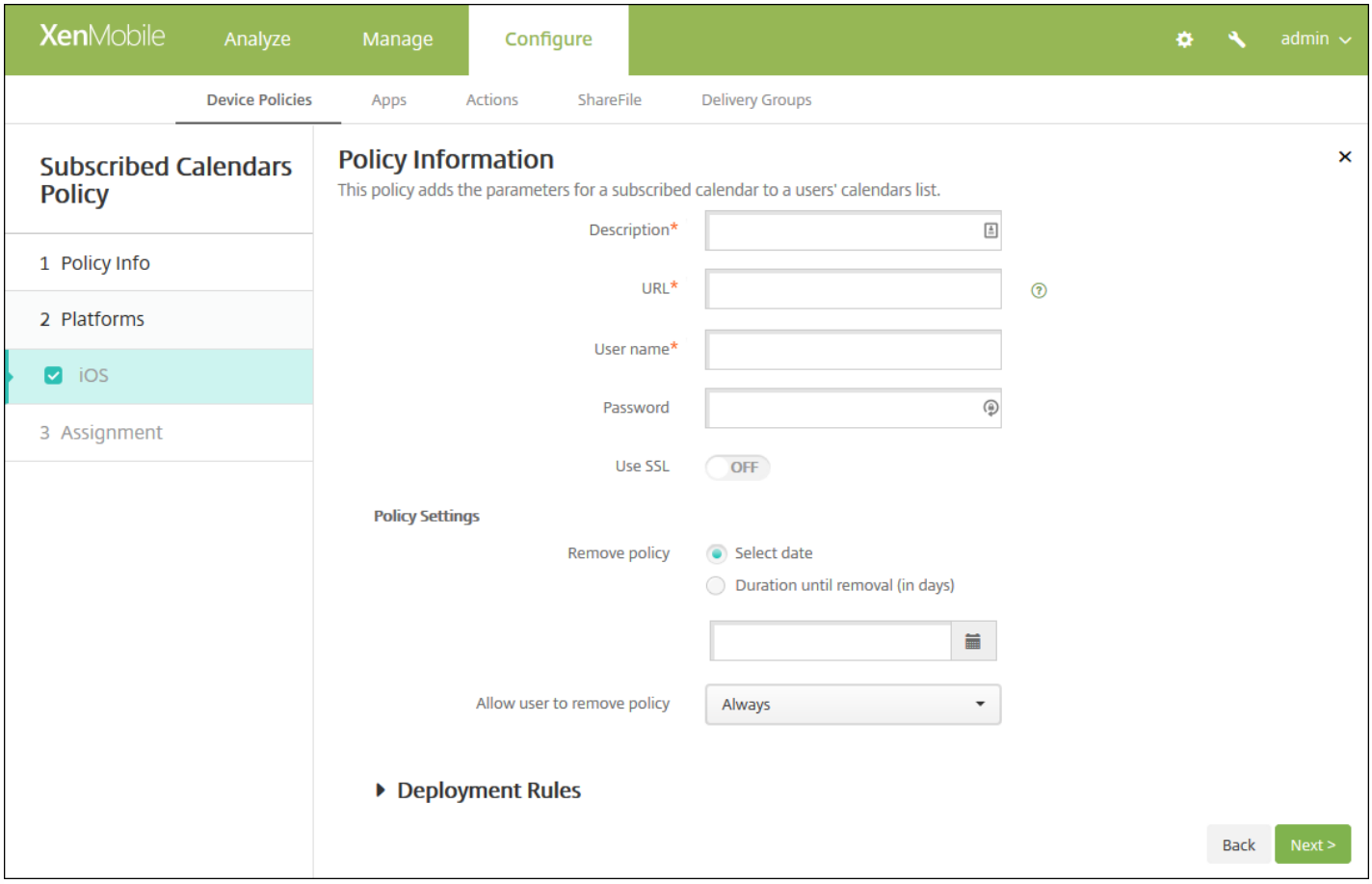
-



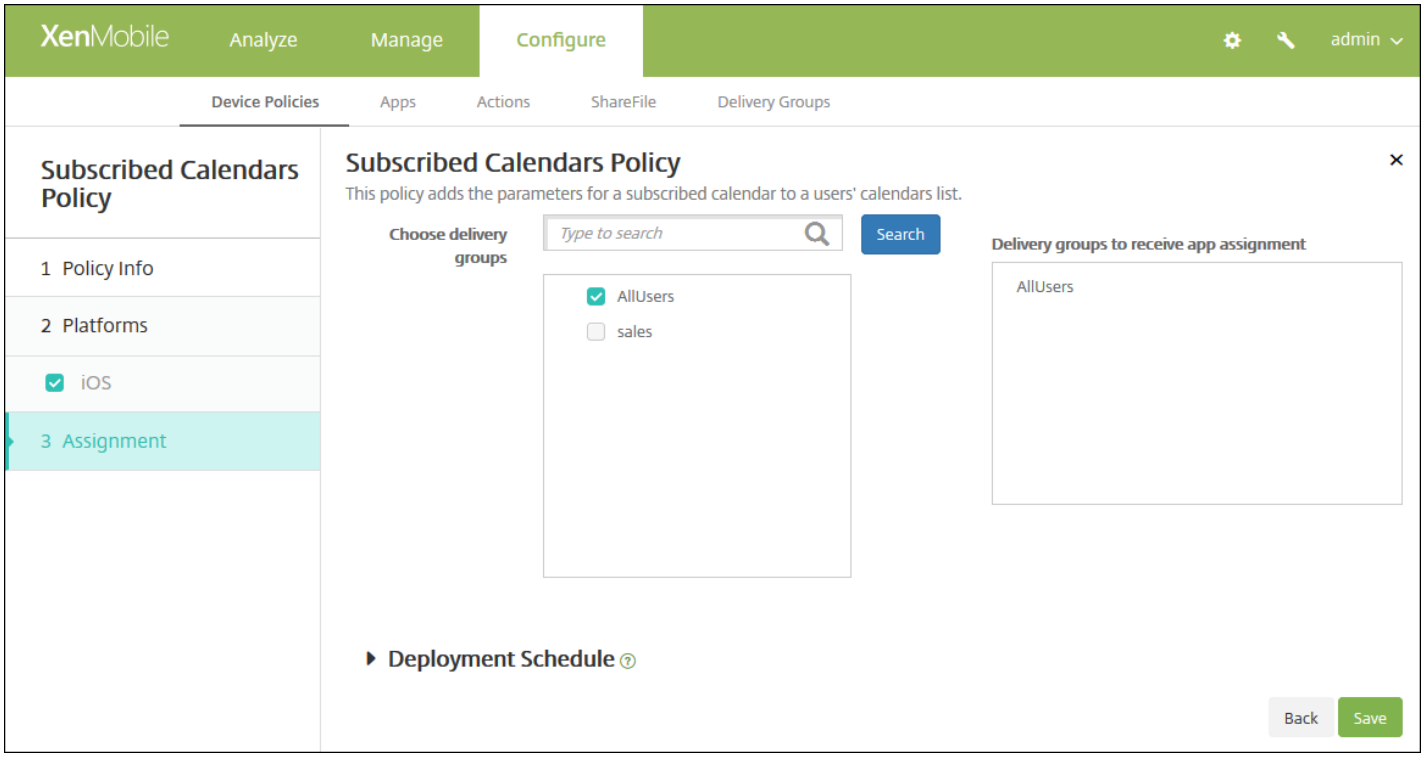
-
-
-
-
-
-
-



-
-



-
-
-
-
-
-
  -
  -
  -
  -



-
-
-
-
-
-
-

契約条件デバイスポリシー

Aug 02, 2016

社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、XenMobileで契約条件デバイスポリシーを作成します。 ユーザーがXenMobileにデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。 契約条件を拒否すると、登録処理が取り消されます。

社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。 展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。 Androidデバイスおよびiosデバイスの場合は、PDFファイルを提供する必要があります。 Windowsデバイスの場合は、テキスト（TXT）ファイルと付属のイメージファイルを提供する必要があります。

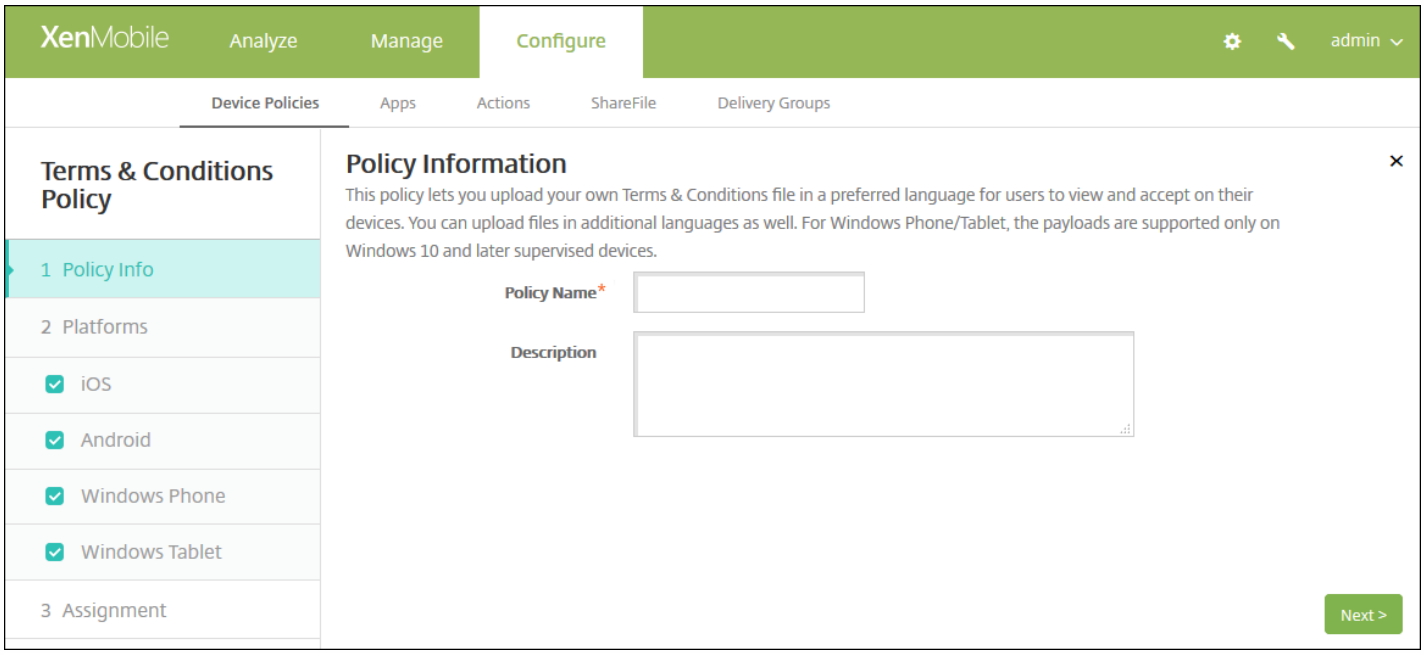
iOSおよびAndroidの設定

Windows PhoneおよびWindowsタブレットの設定

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

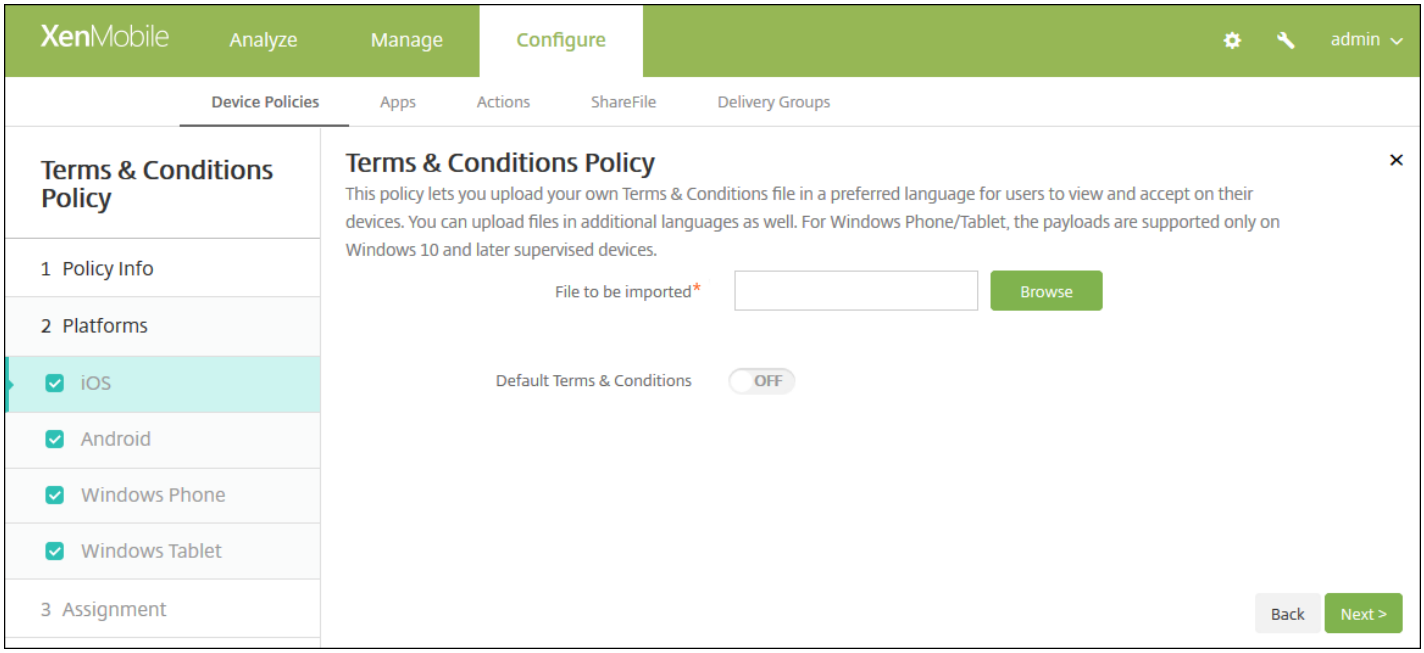
3. ［**Terms & Conditions**］をクリックします。 ［**Terms & Conditions Policy**］ページが開きます。



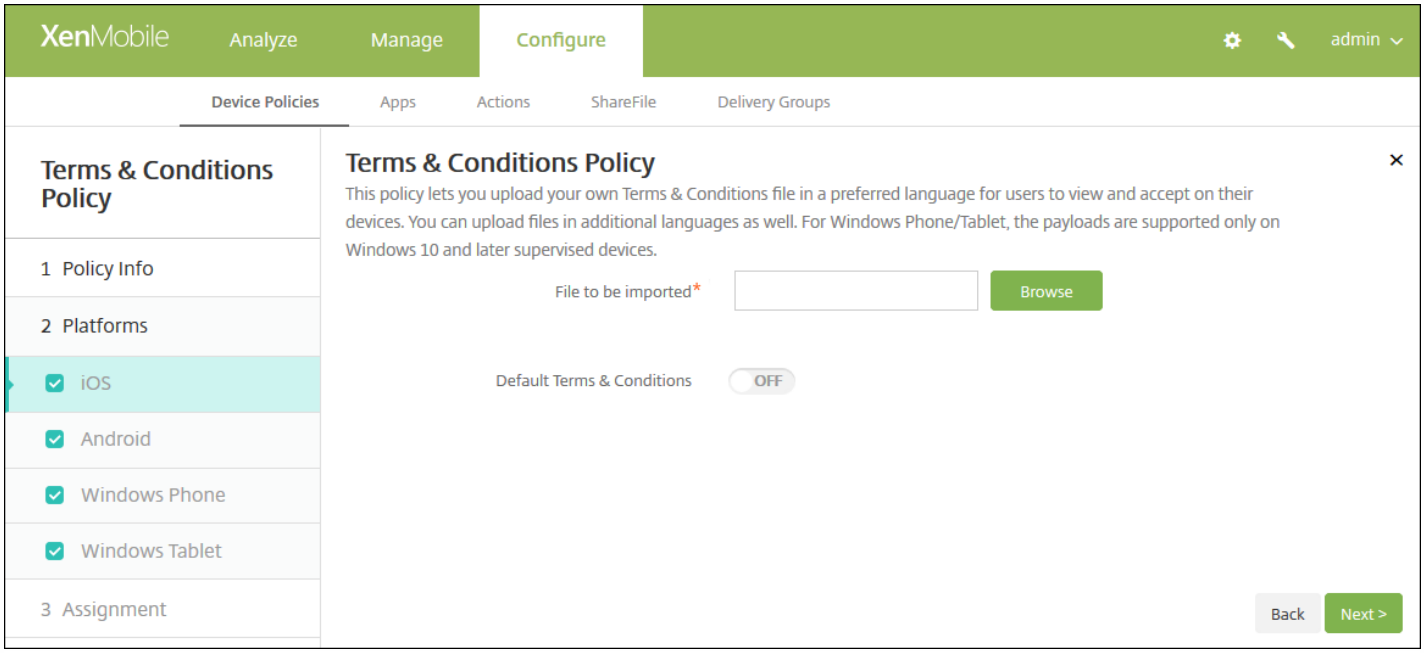
4. ［**Policy Information**］ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. ［**Next**］をクリックします。 ［**Terms & Conditions Platforms**］情報ページが開きます。



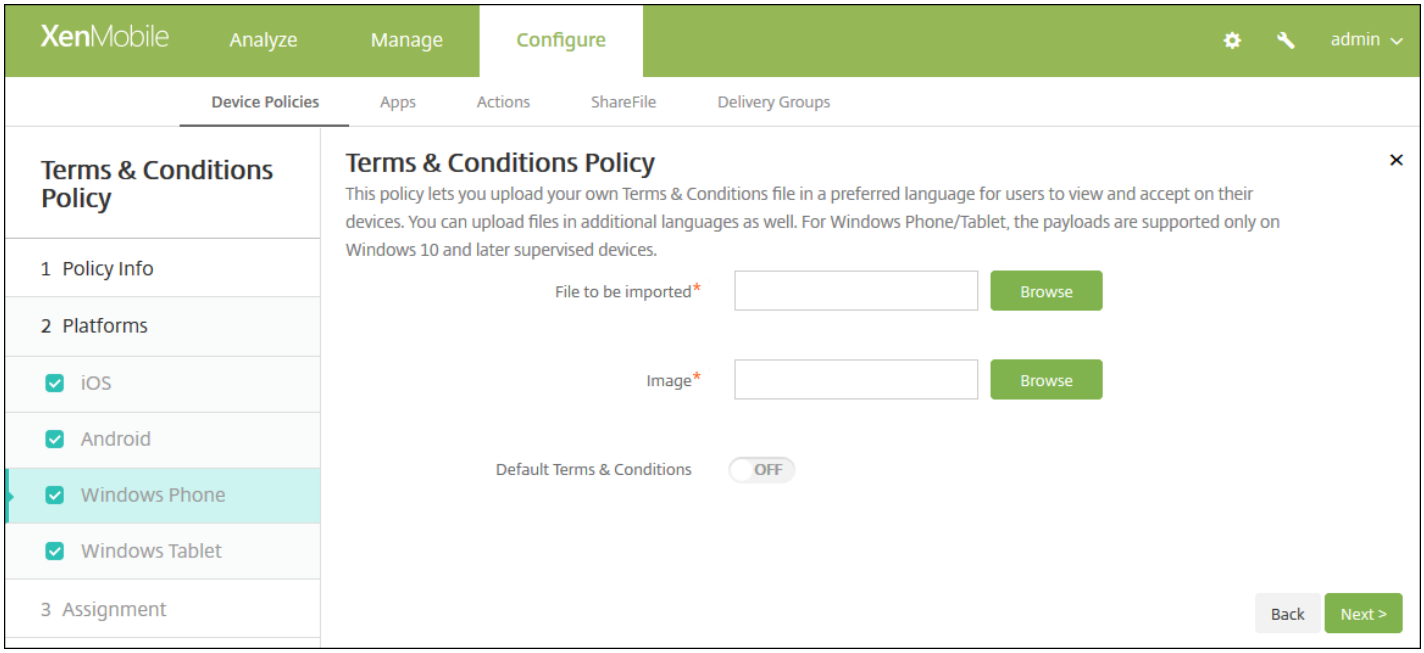
iOSおよびAndroidの設定



次の設定を構成します。

- **File to be imported**： **[Browse]** をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。
- **Default Terms & Conditions**：このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。 デフォルトは **[OFF]** です。

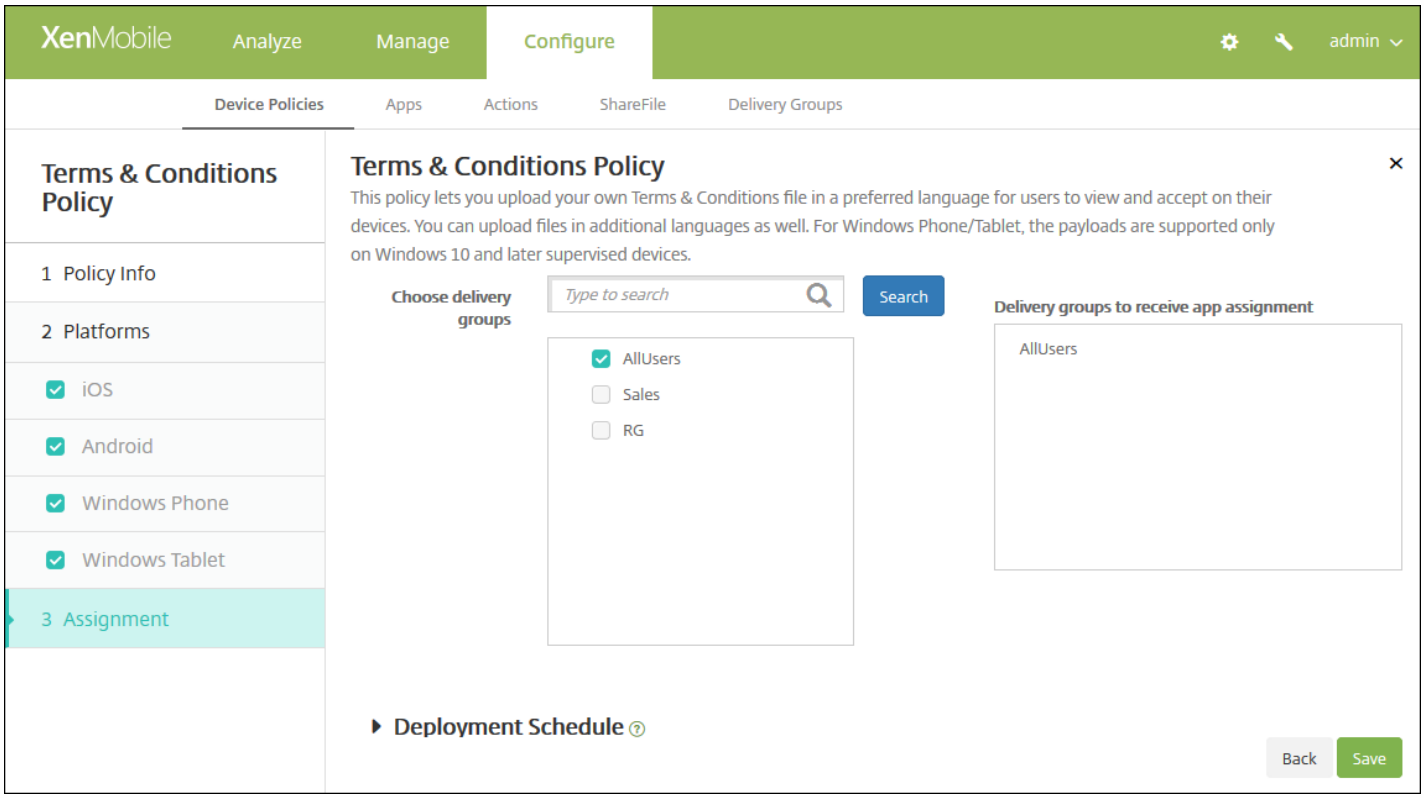
Windows PhoneおよびWindowsタブレットの設定



次の設定を構成します。

- **File to be imported**： **[Browse]** をクリックしてインポートする契約条件ファイルの場所に移動し、そのファイルを選択します。
- **Image**： **[Browse]** をクリックしてインポートするイメージファイルの場所へ移動し、そのファイルを選択します。
- **Default Terms & Conditions**：このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。 デフォルトは **[OFF]** です。

6. **[Next]** をクリックします。 **[Terms & Conditions Policy]** 割り当てページが開きます。



7. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

8. [**Save**] をクリックします。

Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには

Aug 02, 2016

Apple Configuratorを使用するには、AppleコンピューターでOS X 10.7.2以降を実行している必要があります。

> **Important**
>
> デバイスをSupervisedモードにすると、特定のバージョンのiOSがデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリケーションがデバイスから完全に消去されます。

1. iTunesからApple Configuratorをインストールします。
2. iOSデバイスをAppleコンピューターに接続します。
3. Apple Configuratorを起動します。 監視の準備が整っているデバイスがあることがConfiguratorに表示されます。
4. デバイスの監視の準備を行うには：
    1. ［監視］コントロールを［オン］に切り替えます。 構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。
    2. 必要に応じてデバイスの名前を指定します。
    3. 最新バージョンのiOSをインストールする場合、［iOS］ボックスの一覧で［最新］を選択します。
5. デバイスの監視の準備が整ったら、［準備］をクリックします。

VPNデバイスポリシー

Oct 25, 2016

XenMobileでデバイスポリシーを追加して、VPN（Virtual Private Network：仮想プライベートネットワーク）の設定を構成し、ユーザーのデバイスが社内リソースに安全に接続できるようにすることができます。 VPNポリシーは、iOS、Android（Android for Work対応デバイスを含む）、Samsung SAFE、Samsung KNOX、Windowsタブレット、Windows Phone、Amazonの各プラットフォームに対して構成できます。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

iOSの設定

Mac OS Xの設定

Androidの設定

Samsung SAFEの設定

Samsung KNOXの設定

Windows Phoneの設定

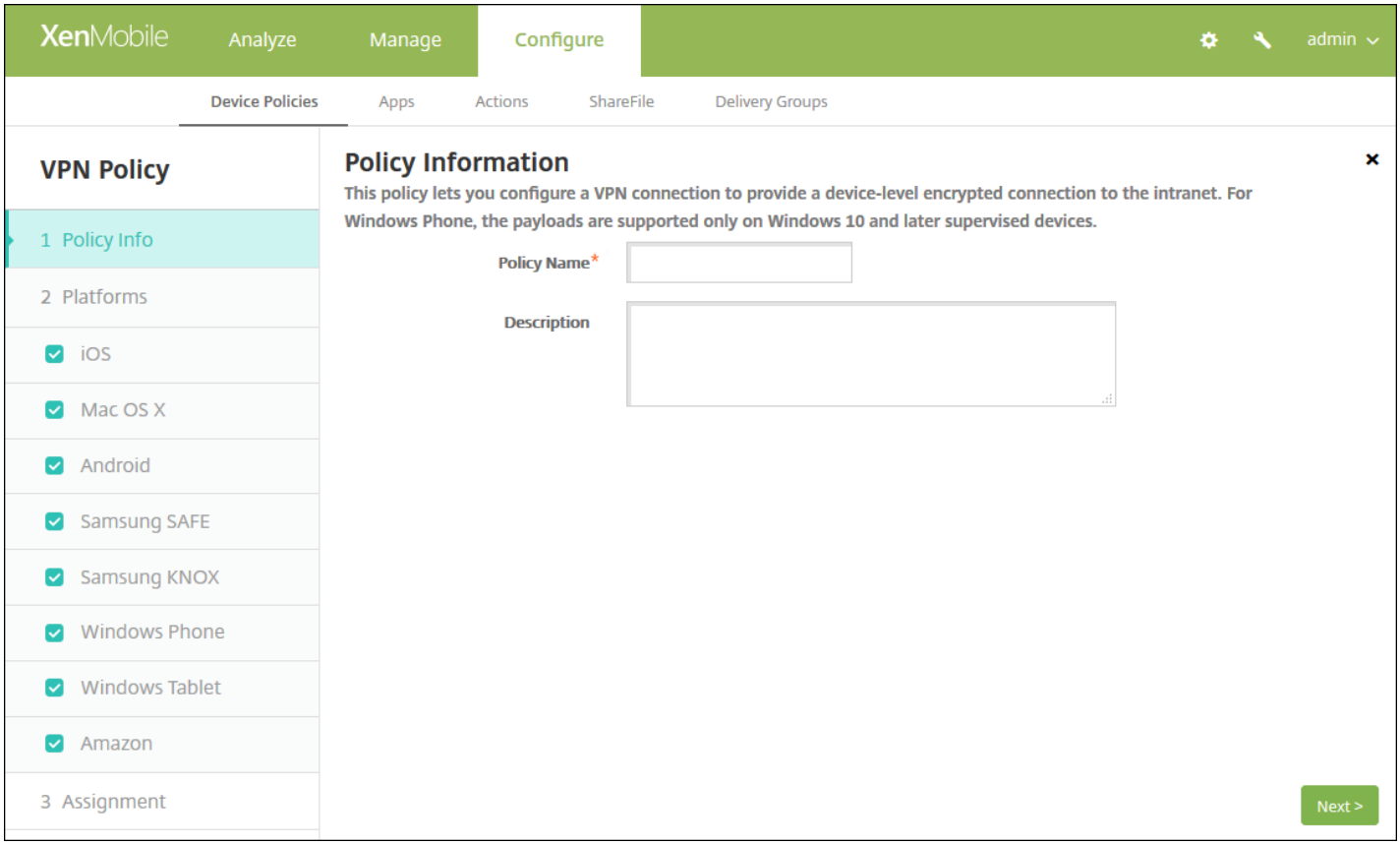
Windowsタブレットの設定

Amazonの設定

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**VPN**］をクリックします。 ［**VPN Policy**］ページが開きます。



4. [**Policy Information**] ペインで、以下の情報を入力します。

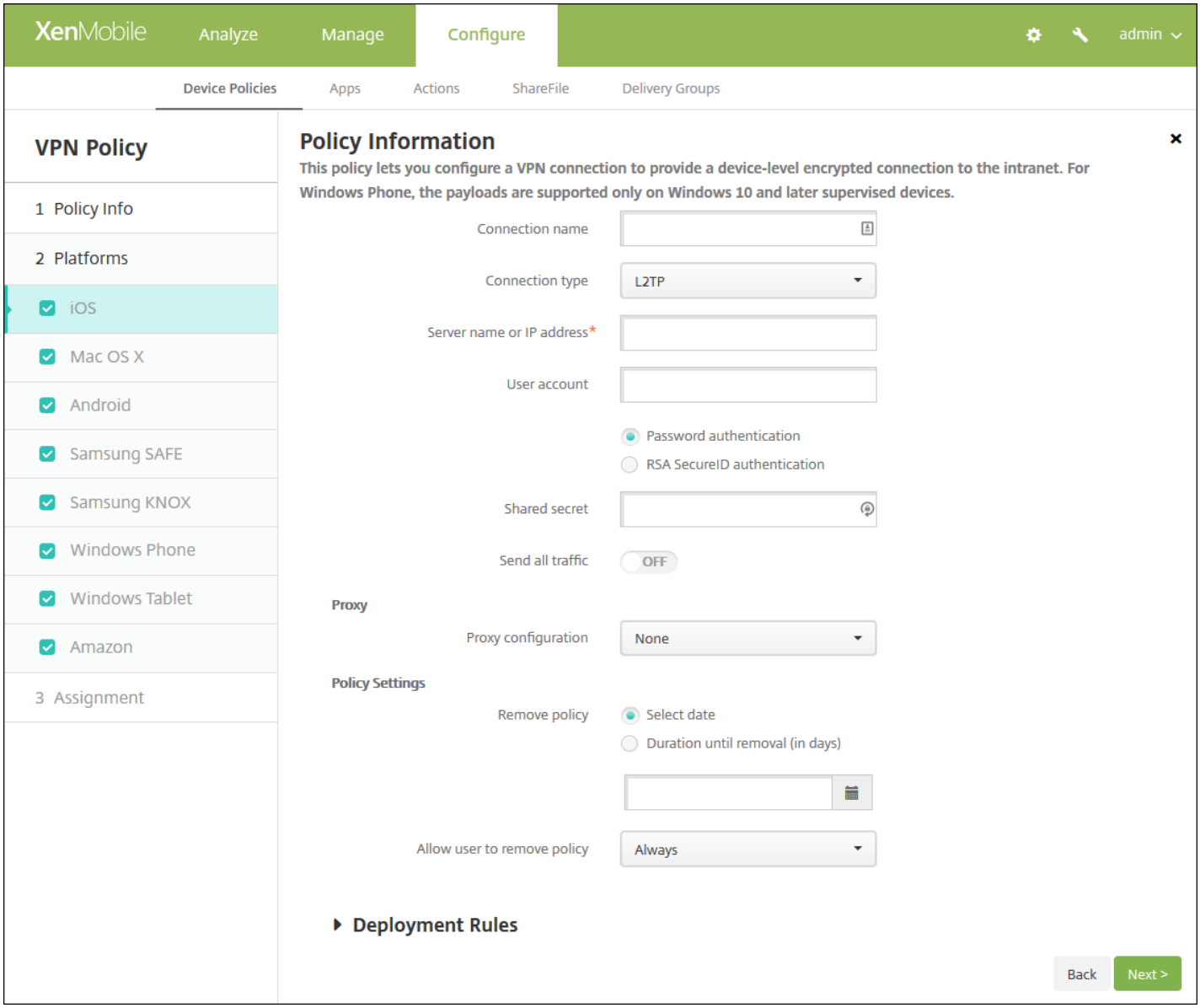
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Policy Platforms**] ページが開きます。 [**Policy Platforms**] ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォームが表示されます。

6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 構成しないプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



次の設定を構成します。

- **Connection name**：接続の名前を入力します。
- **Connection type**：一覧から、この接続において使用するプロトコルを選択します。 デフォルトは[**L2TP**] です。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証
  - **PPTP**：Point-to-Pointトンネリング
  - **IPSec**：社内VPN接続
  - **Cisco AnyConnect**：Cisco AnyConnect VPNクライアント
  - **Juniper SSL**：Juniper Networks SSL VPNクライアント
  - **F5 SSL**：F5 Networks SSL VPNクライアント
  - **SonicWALL Mobile Connect**：iOS用Dell統合VPNクライアント
  - **Ariba VIA**：Aruba Networks仮想インターネットアクセスクライアント
  - **IKEv2（iOS only）**：iOS専用インターネットキー交換バージョン2
  - **Citrix VPN**：iOS用Citrix VPNクライアント
  - **Custom SSL**：カスタムSSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

L2TPプロトコルの構成

PPTPプロトコルの構成

IPSecプロトコルの構成

Cisco AnyConnectプロトコルの構成

Juniper SSLプロトコルの構成

F5 SSLプロトコルの設定

SonicWALLプロトコルの構成

Ariba VIAプロトコルの構成

IKEv2プロトコルの構成

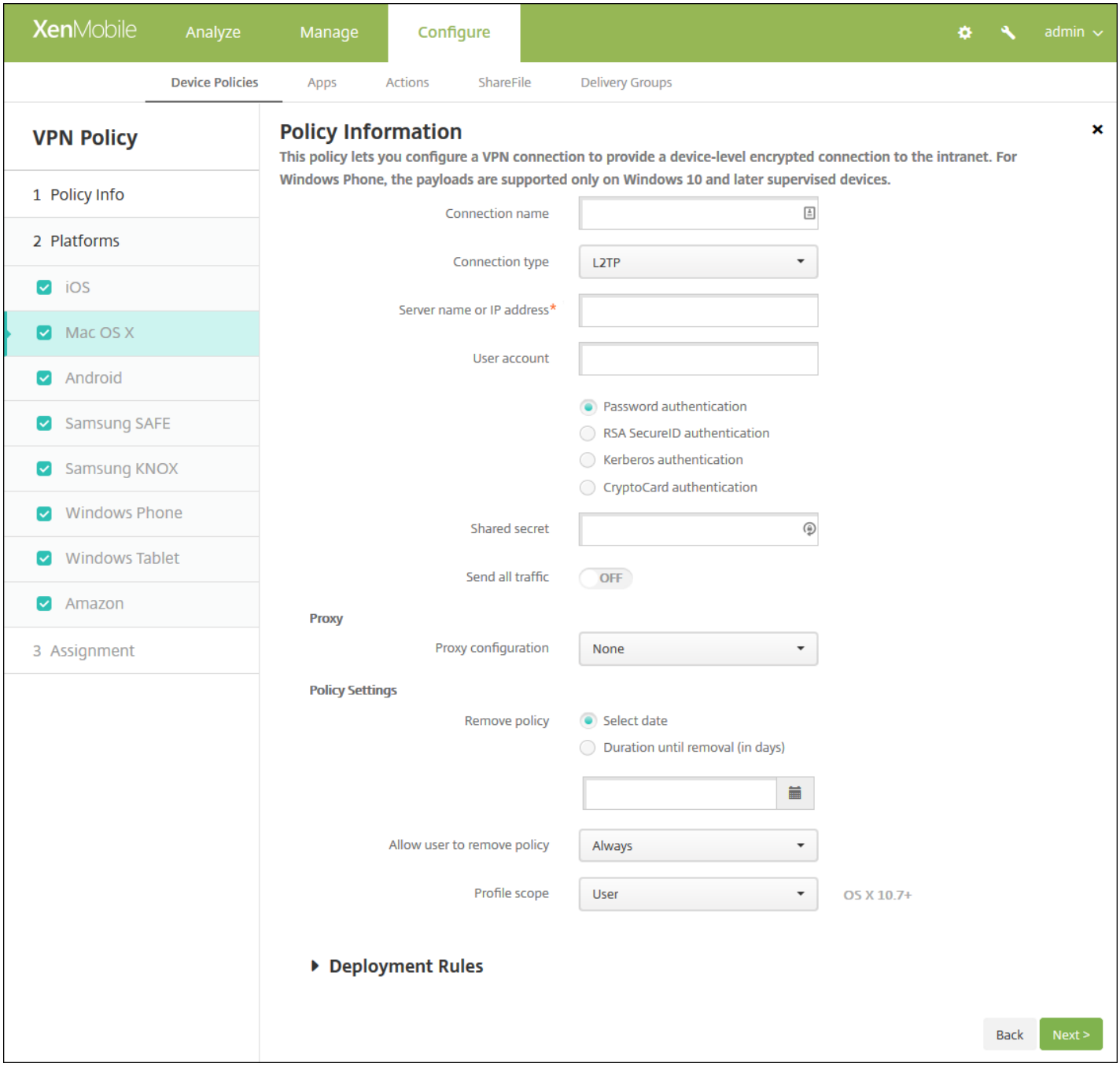
Citrix VPNプロトコルの構成

カスタムSSLプロトコルの構成

［Enable VPN on demand］オプションの構成

- **プロキシDHCP**
  - **Proxy configuration**：一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。 デフォルトは［**None**］です。
    - ［**Manual**］を有効にした場合は、次の設定を構成します。
      - **Host name or IP address for the proxy server**：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。
      - **Port for the proxy server**：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。
      - **User name**：任意で、プロキシサーバーのユーザー名を入力します。
      - **Password**：任意で、プロキシサーバーのパスワードを入力します。
    - ［**Automatic**］を選択した場合は、次の設定を構成します。
      - **Proxy server 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**
  - ［**Policy Settings**］の下の［**Remove policy**］の横にある、［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **Connection name**：接続の名前を入力します。
- **Connection type**：一覧から、この接続において使用するプロトコルを選択します。 デフォルトは［L2TP］です。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証
  - **PPTP**：Point-to-Pointトンネリング
  - **IPSec**：社内VPN接続
  - **Cisco AnyConnect**：Cisco AnyConnect VPNクライアント
  - **Juniper SSL**：Juniper Networks SSL VPNクライアント
  - **F5 SSL**：F5 Networks SSL VPNクライアント
  - **SonicWALL Mobile Connect**：iOS用Dell統合VPNクライアント

- **Ariba VIA**：Aruba Networks仮想インターネットアクセスクライアント
- **Citrix VPN**：Citrix VPNクライアント
- **Custom SSL**：カスタムSSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

L2TPプロトコルの構成

PPTPプロトコルの構成

IPSecプロトコルの構成

Cisco AnyConnectプロトコルの構成

Juniper SSLプロトコルの構成

F5 SSLプロトコルの構成

SonicWALLプロトコルの構成

Ariba VIAプロトコルの構成

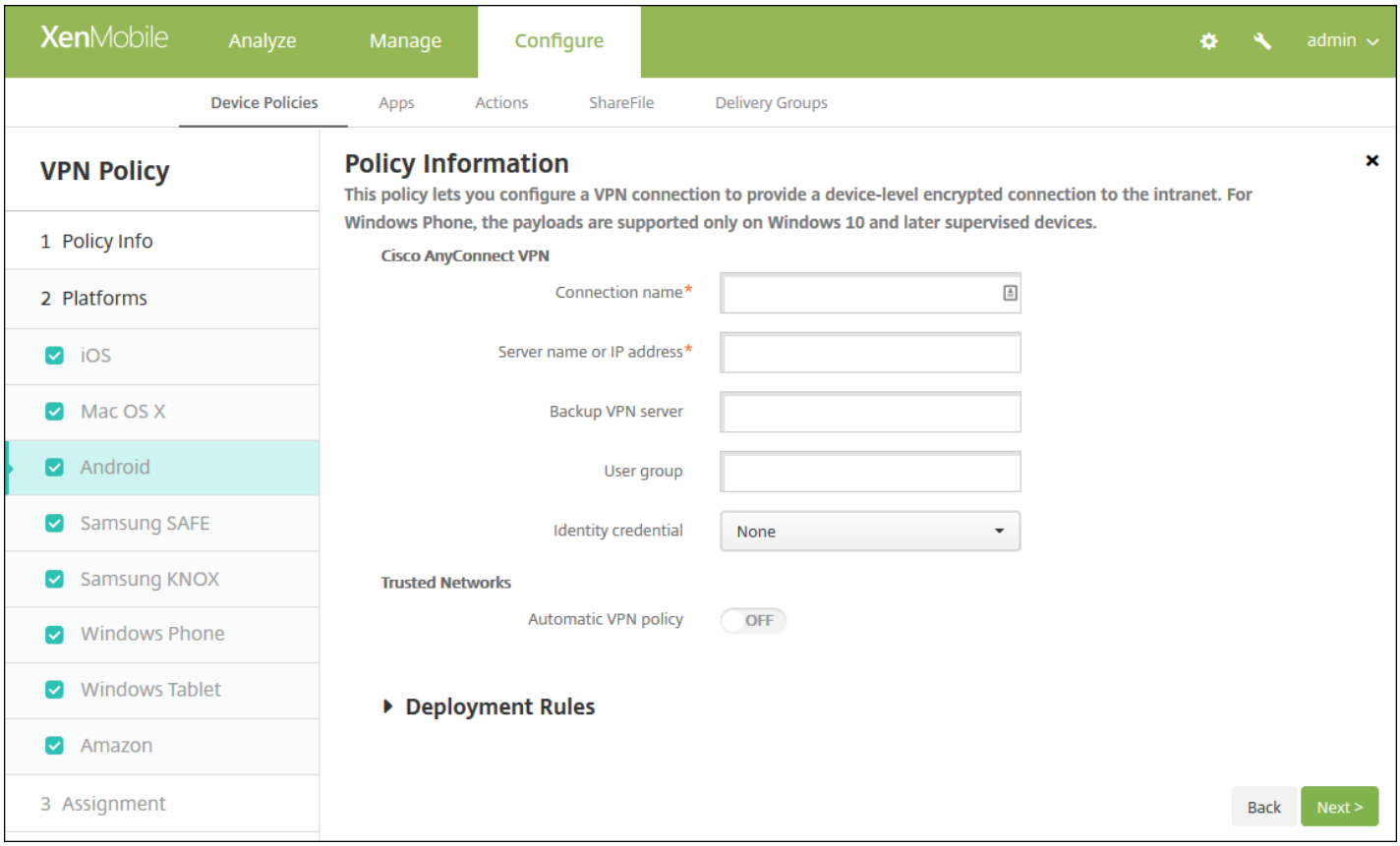
Citrix VPNプロトコルの構成

カスタムSSLプロトコルの構成

［Enable VPN on demand］オプションの構成

- プロキシDHCP
  - **Proxy configuration**：一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。 デフォルトは［**None**］です。
    - ［**Manual**］を有効にした場合は、次の設定を構成します。
      - **Host name or IP address for the proxy server**：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。
      - **Port for the proxy server**：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。
      - **User name**：任意で、プロキシサーバーのユーザー名を入力します。
      - **Password**：任意で、プロキシサーバーのパスワードを入力します。
    - ［**Automatic**］を選択した場合は、次の設定を構成します。
      - **Proxy server 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
  - ［**Policy Settings**］の下の［**Remove policy**］の横にある、［**Select date**］または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。
  - ［**Profile scope**］の横にある、［**User**］または［**System**］を選択します。 デフォルトは［**User**］です。 このオプションはOS X 10.7以降でのみ使用できます。

Androidの設定の構成



次の設定を構成します。

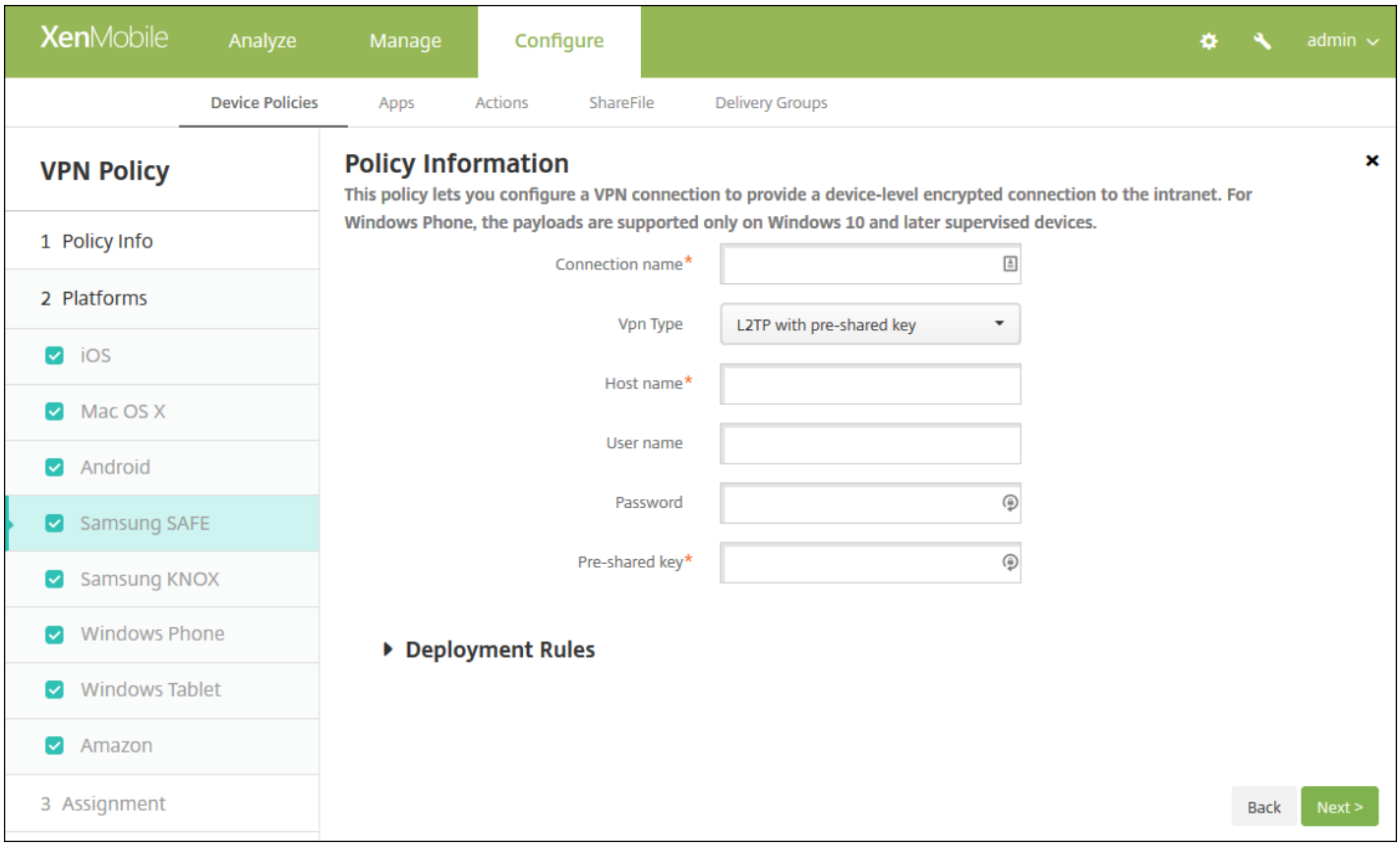
- **Cisco AnyConnect VPN**
  - **Connection name**：Cisco AnyConnect VPN接続の名前を入力します。 このフィールドは必須です。
  - **Server name or IP address**：VPNサーバーの名前またはIPアドレスを入力します。 このフィールドは必須です。
  - **Backup VPN server**：バックアップVPNサーバー情報を入力します。
  - **User group**：ユーザーグループ情報を入力します。
  - **Identity credential**：一覧から、ID資格情報を選択します。
- **Trusted Networks**
  - **Automatic VPN policy**：このオプションをオンまたはオフにして、信頼できるネットワークおよび信頼できないネットワークに対するVPNの動作方法を設定します。 有効にした場合は、次の設定を構成します。
    - **Trusted network policy**：一覧から、目的のポリシーを選択します。 デフォルトは **[Disconnect]** です。 選択できるオプションは以下のとおりです。
      - **Disconnect**：クライアントにより、信頼できるネットワーク圏内のVPN接続が終了されます。 これがデフォルトの設定です。
      - **Connect**：クライアントにより、信頼できるネットワーク圏内のVPN接続が開始されます。
      - **Do Nothing**：クライアントによるアクションはありません。
      - **Pause**：信頼できるネットワーク圏外でVPNセッションが確立された後、信頼済みとして構成されたネットワークにユーザーがアクセスすると、VPNセッションが（切断ではなく）一時停止されます。 ユーザーが信頼できるネットワークから離れると、セッションが再開されます。 これにより、信頼できるネットワークを離れた後に新しいVPNセッションを確立する手間が省かれます。
    - **Untrusted network policy**：一覧から、目的のポリシーを選択します。 デフォルトは **[Connect]** です。 選択でき

るオプションは以下のとおりです。
  - **Connect**：クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。
  - **Do Nothing**：クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。 このオプションにより、［Always-on VPN］が無効化されます。
- **Trusted domains**：クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるドメインサフィックスごとに、 **[Add]** をクリックして以下の操作を行います。
  - **Domain**：追加するドメインを入力します。
  - **[Save]** をクリックしてドメインを保存するか、**[Cancel]** をクリックして操作を取り消します。
- **Trusted servers**：クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるサーバーアドレスごとに、 **[Add]** をクリックして以下の操作を行います。
  - **Servers**：追加するサーバーを入力します。
  - **[Save]** をクリックしてサーバーを保存するか、**[Cancel]** をクリックして操作を取り消します。

    注：既存のサーバーを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。 項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

    既存のサーバーを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。 項目を変更し、 **[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

Samsung SAFEの設定の構成



次の設定を構成します。

- **Connection name**：接続の名前を入力します。
- **Vpn Type**：一覧から、この接続で使用するプロトコルを選択します。 デフォルトは**[L2TP with pre-shared key]**です。 選択できるオプションは以下のとおりです。
  - **L2TP with pre-shared key**：レイヤー2トンネリングプロトコルと事前共有キー認証。 これがデフォルトの設定です。
  - **L2TP with certificate**：レイヤー2トンネリングプロトコルと証明書。
  - **PPTP**：Point-to-Pointトンネリング。
  - **Enterprise**：社内VPN接続。 バージョン2.0よりも前のSAFEに適用可能です。
  - **Generic**：一般的なVPN接続。 バージョン2.0以降のSAFEに適用可能です。

以下のセクションでは、上記のVPNの種類ごとに構成オプションを示します。

[L2TP with pre-shared key]プロトコルの構成

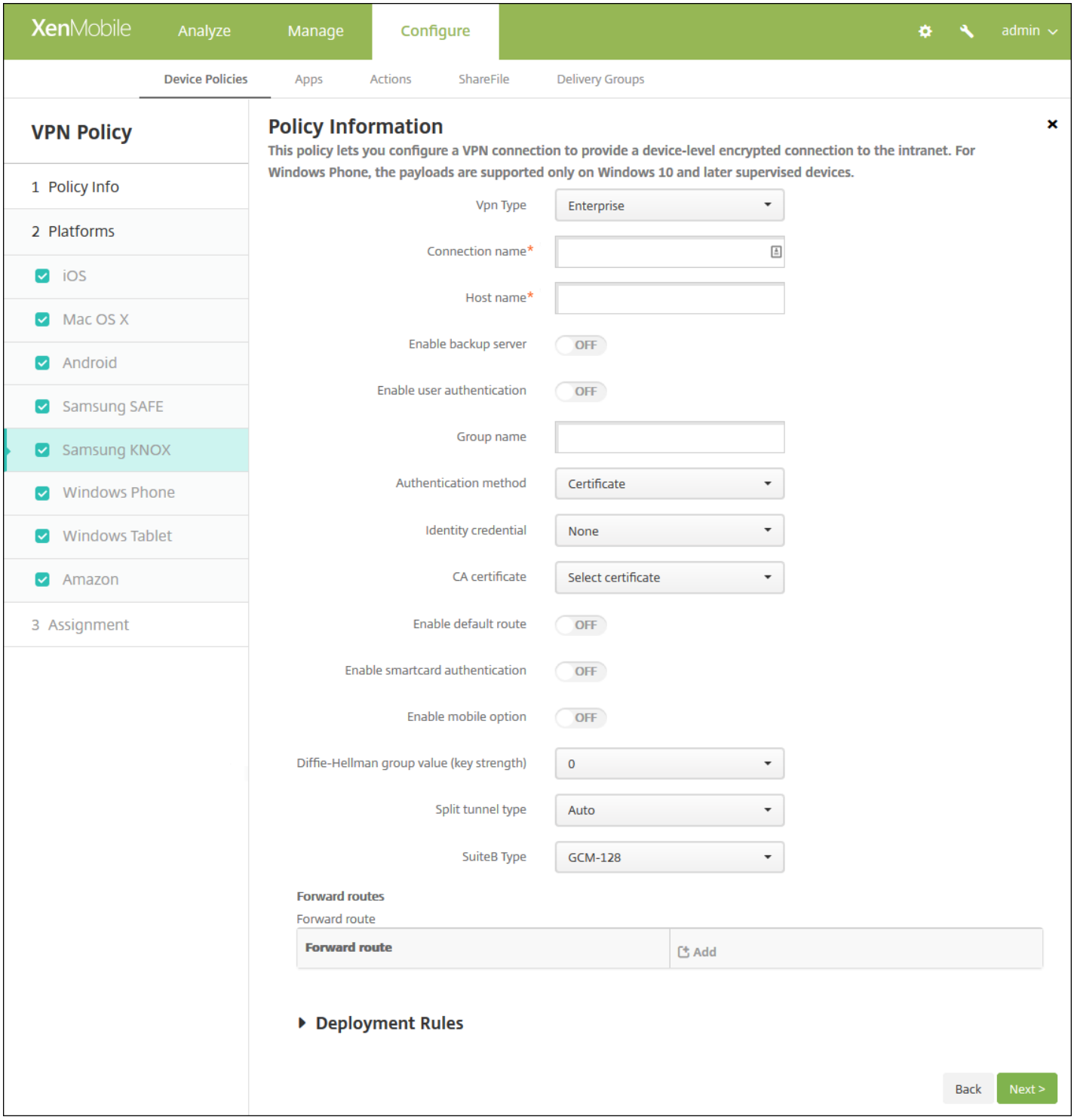
[L2TP with certificate]プロトコルの構成

[PPTP]プロトコルの構成

[Enterprise]プロトコルの構成

[Generic]プロトコルの構成

Samsung KNOXの設定の構成



注：Samsung KNOXのポリシーを構成した場合、ポリシーはSamsung KNOXコンテナーにのみ適用されます。

次の設定を構成します。

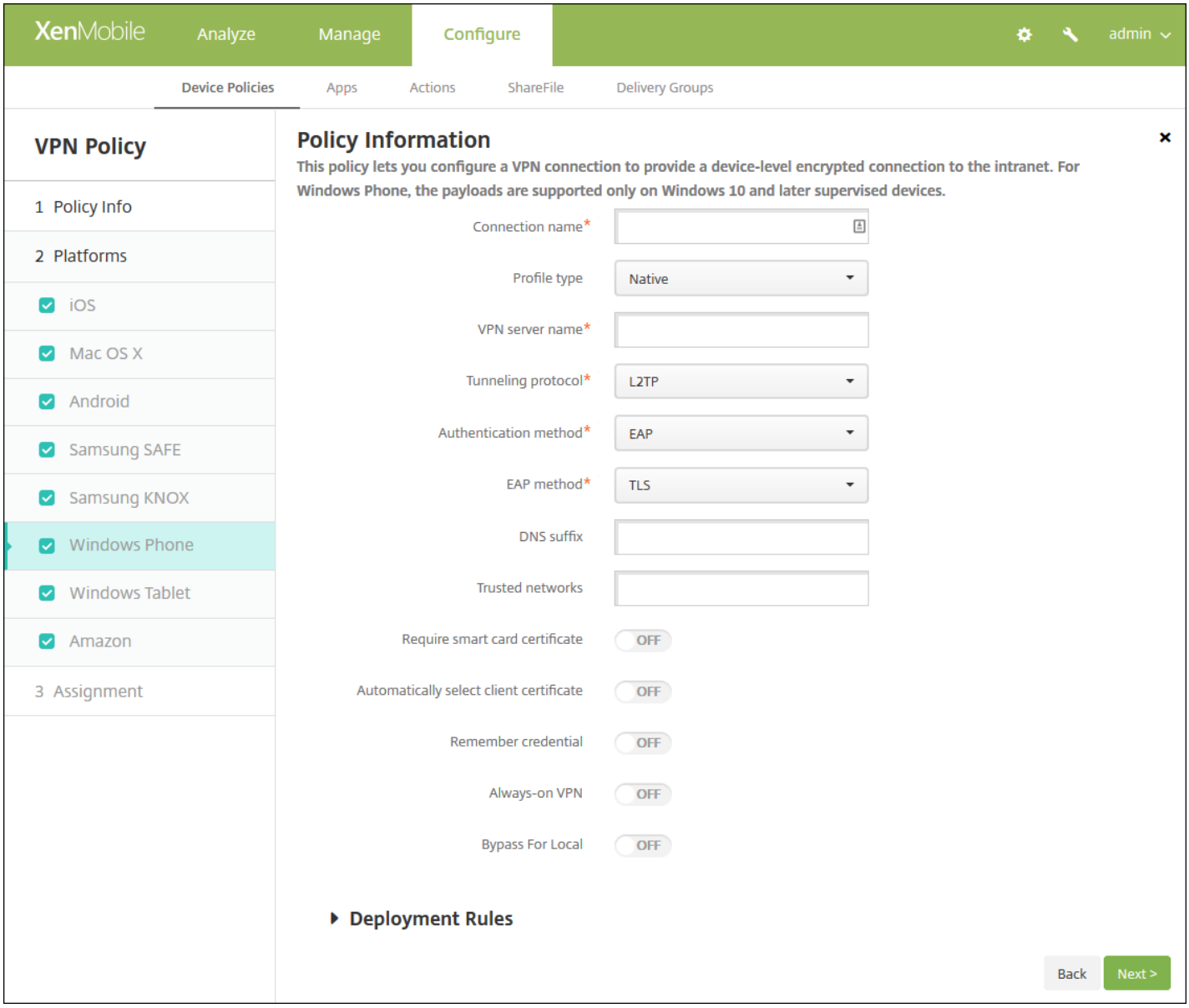
- **Vpn Type**：一覧から、構成するVPN接続の種類として **[Enterprise]** （バージョン2.0よりも前のKNOXに適用可能）または **[Generic]** （バージョン2.0以降のKNOXに適用可能）をクリックします。 デフォルトは **[Enterprise]** です。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

［Enterprise］プロトコルの構成

［Generic］プロトコルの構成

Windows Phoneの設定の構成



注：これらの設定は、Windows 10以降の監視対象Windows Phoneでのみサポートされます。

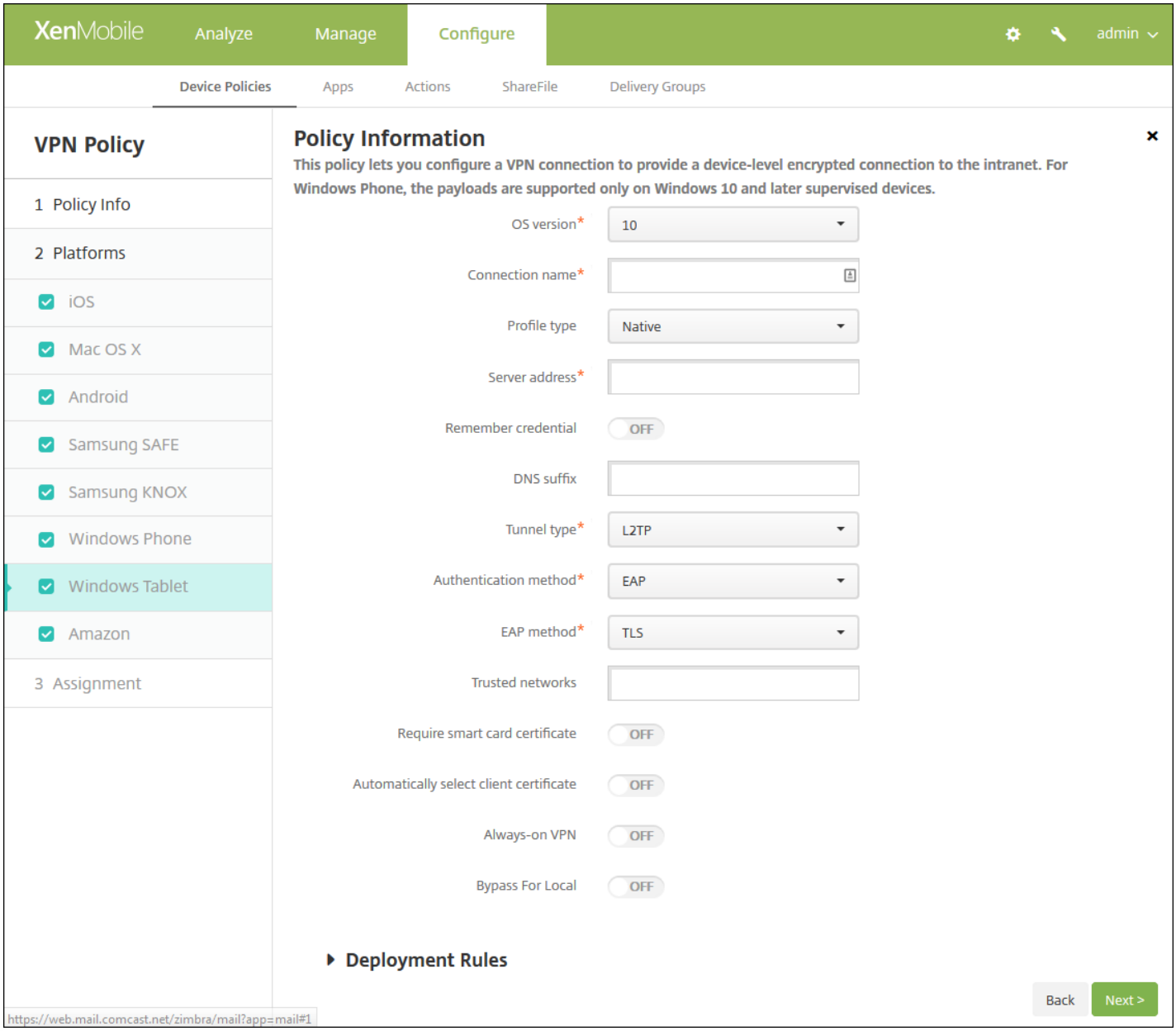
次の設定を構成します。

- **Connection name**：接続の名前を入力します。 このフィールドは必須です。
- **Profile type**：一覧から、 **[Native]** または **[Plugin]** を選択します。 デフォルトは **[Native]** です。 次のセクションでは、各オプションの設定について説明します。
- **Configure Native profile type settings**：以下の設定は、ユーザーのWindows Phoneに組み込まれているVPNに適用されます。
  - **VPN server name**：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。
  - **Tunneling protocol**：一覧から、使用するVPNトンネルの種類を選択します。 デフォルトは **[L2TP]** です。 選択でき

るオプションは以下のとおりです。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証
  - **PPTP**：Point-to-Pointトンネリング
  - **IKEv2**：インターネットキー交換バージョン2
- **Authentication method**：一覧から、使用する認証方法を選択します。 デフォルトは **[EAP]** です。 選択できるオプションは以下のとおりです。
  - **EAP**：拡張認証プロトコル。
  - **MSChapV2**：相互認証にMicrosoftのチャレンジハンドシェイク認証を使用します。 トンネルの種類に［IKEv2］を選択した場合、このオプションは使用できません。 ［MSChapV2］を選択すると、 **[Automatically use Windows credentials]** オプションが表示されます。デフォルトは **[OFF]** です。
- **EAP method**：一覧から、使用するEAP方法を選択します。 デフォルトは **[TLS]** です。 ［MSChapV2］認証が有効になっている場合、このフィールドは使用できません。 選択できるオプションは以下のとおりです。
  - **TLS**：Transport Layer Security
  - **PEAP**：保護された拡張認証プロトコル
- **DNS Suffix**：DNSサフィックスを入力します。
- **Trusted networks**：アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。 たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- **Require smart card certificate**：スマートカード証明書を必須とするかどうかを選択します。 デフォルトは［OFF］です。
- **Automatically select client certificate**：認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。 デフォルトは［OFF］です。 ［Require smart card certificate］が有効になっている場合、このオプションは使用できません。
- **Remember credential**：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、可能な場合に資格情報がキャッシュされます。
- **Always on VPN**：VPNを常にオンにするかどうかを選択します。 デフォルトは［OFF］です。 有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
- **Bypass For Local**：ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

- **Configure Plugin protocol type**：以下の設定は、Windows Storeから取得し、ユーザーのデバイスにインストールしたVPNプラグインに適用されます。
  - **Server address**：VPNサーバーのURL、 ホスト名、またはIPアドレスを入力します。
  - **Client app ID**：VPNプラグインのパッケージファミリ名を入力します。
  - **Plugin Profile XML**：使用するカスタムVPNプラグインプロファイルの場所に［Browse］をクリックして移動し、ファイルを選択します。 形式などの詳細については、プラグインプロバイダーにお問い合わせください。
  - **DNS Suffix**：DNSサフィックスを入力します。
  - **Trusted networks**：アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。 たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - **Remember credential**：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、可能な場合に資格情報がキャッシュされます。
  - **Always on VPN**：VPNを常にオンにするかどうかを選択します。 デフォルトは［OFF］です。 有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
  - **Bypass For Local**：ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

Windowsタブレットの設定の構成



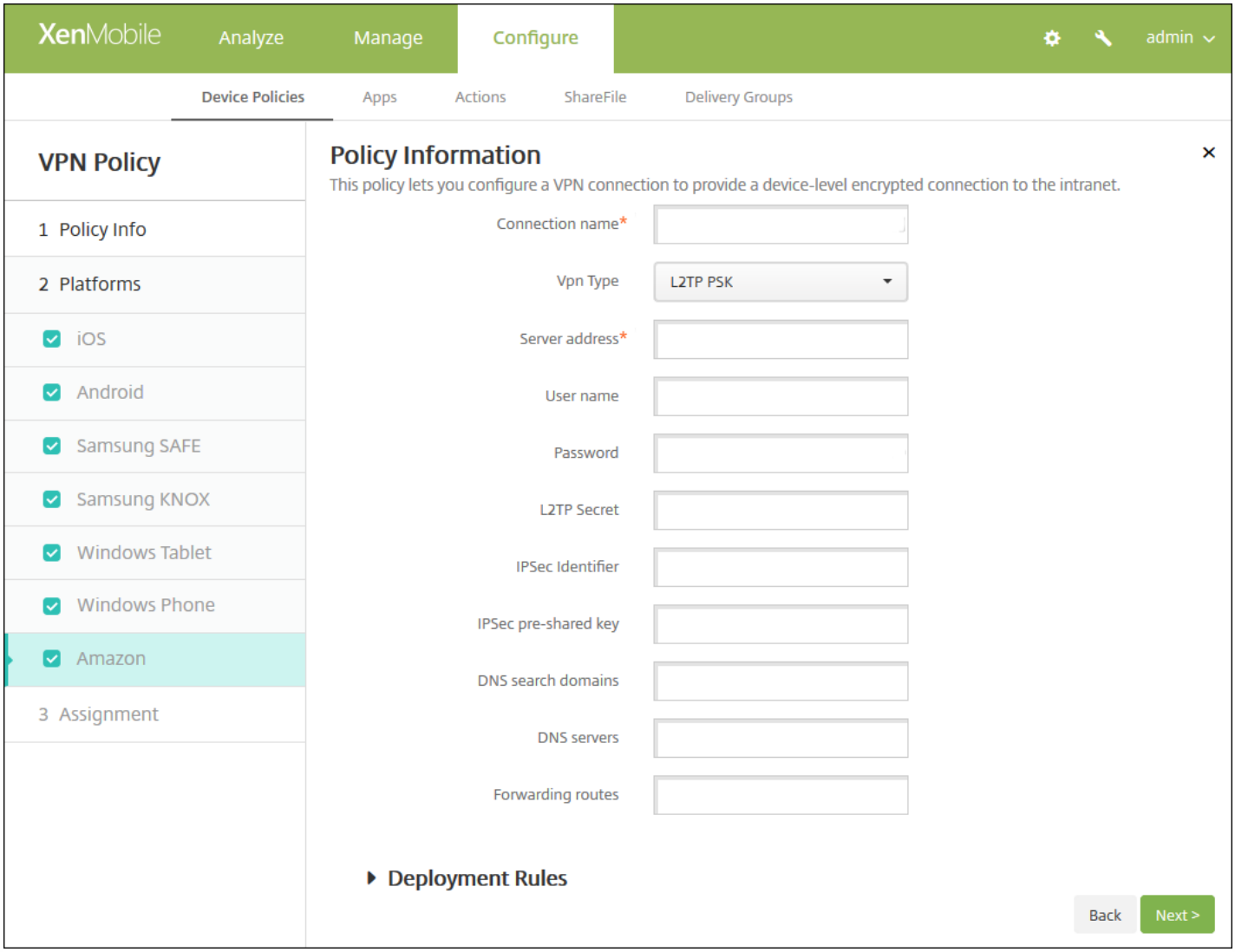
次の設定を構成します。

- **OS Version**：一覧から、Windows 8.1の場合は［**8.1**］を、Windows 10の場合は［**10**］を選択します。デフォルトは［**10**］です。

Windows 10の設定の構成

Windows 8.1の設定の構成

Amazonの設定の構成



次の設定を構成します。

- **Connection name**：接続の名前を入力します。
- **Vpn type**：一覧から、接続の種類を選択します。 選択できるオプションは以下のとおりです。
  - **L2TP PSK**：レイヤー2トンネリングプロトコルと事前共有キー認証。 これがデフォルトの設定です。
  - **L2TP RSA**：レイヤー2トンネリングプロトコルとRSA認証。
  - **IPSEC XAUTH PSK**：インターネットプロトコルセキュリティと事前共有キーおよび拡張認証。
  - **IPSEC HYBRID RSA**：インターネットプロトコルセキュリティとハイブリッドRSA認証。
  - **PPTP**：Point-to-Pointトンネリング

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

L2TP PSKの設定の構成

L2TP RSAの設定の構成

IPSEC XAUTH PSKの設定の構成

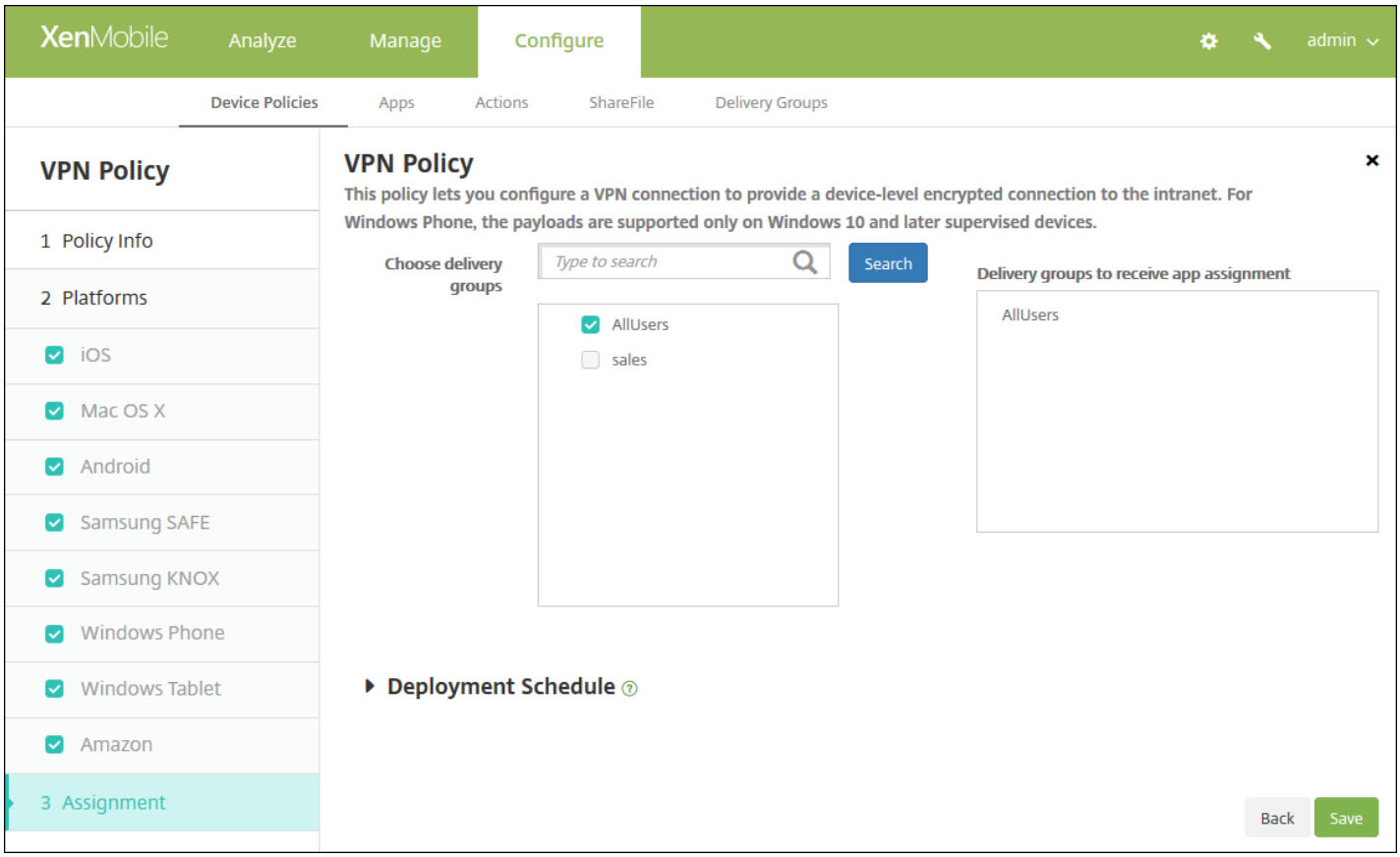
IPSEC AUTH RSAの設定の構成

IPSEC HYBRID RSAの設定の構成

PPTP設定の構成

7. 展開規則を構成します。

8. [**Next**] をクリックします。 [**VPN Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] の一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。 このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

11. ［**Save**］をクリックします。

壁紙デバイスポリシー

Aug 02, 2016

.pngファイルまたは.jpgファイル追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。 iOS 7.1.2以降で使用できます。 iPadおよびiPhoneで 異なる 壁紙を使用するには、別の壁紙ポリシーを作成して、適切なユーザーに展開する必要があります。

次の表に、Apple社がiOSデバイス用に推奨しているイメージサイズを示します。

デバイス		イメージサイズ（ピクセル）
iPhone	**iPad**	
4、4s		640 x 960
5、5c、5s		640 x 1136
6、6s		750 x 1334
6 Plus		1080 x 1920
	Air、2	1536 x 2048
	4、3	1536 x 2048
	Mini 2、3	1536 x 2048
	Mini	768 x 1024

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。 ［**Device Policies**］ページが開きます。

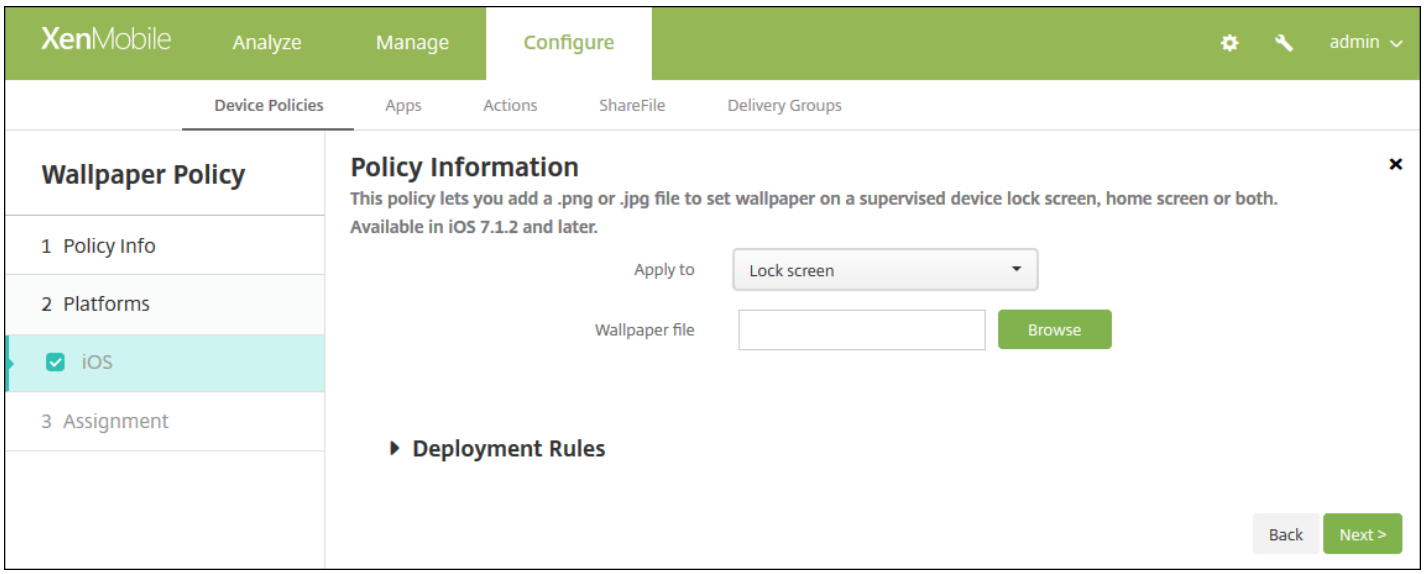
2. ［**Add**］をクリックします。 ［**Add a New Policy**］ダイアログボックスが開きます。

3. ［**More**］を展開した後、［**End User**］の下の［**Wallpaper**］をクリックします。 ［**Wallpaper Policy**］ページが開きます。

4. [**Policy Information**] ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. [**Next**] をクリックします。 [**Policy Platforms**] ページが開きます。

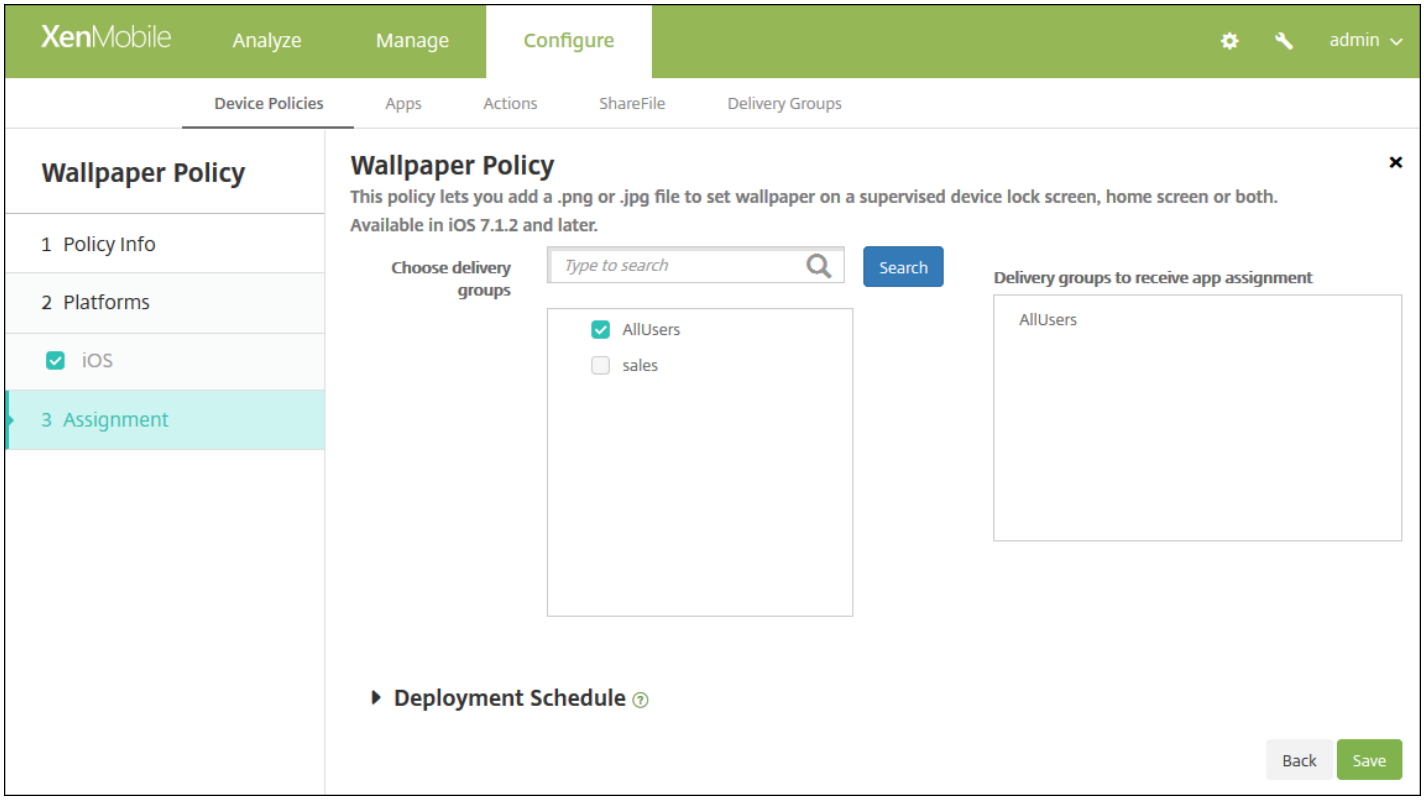


次の設定を構成します。

- **Apply to**：一覧から、 [**Lock screen**] 、 [**Home (icon list) screen**] 、 [**Lock and home screens**] のいずれかを選択して、壁紙を表示する場所を設定します。
- **Wallpaper file**： [**Browse**] をクリックして壁紙ファイルの場所に移動し、ファイルを選択します。

7. 展開規則の構成

8. [**Next**] をクリックします。 [**Wallpaper Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、 [**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただし、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

Webコンテンツデバイスポリシー

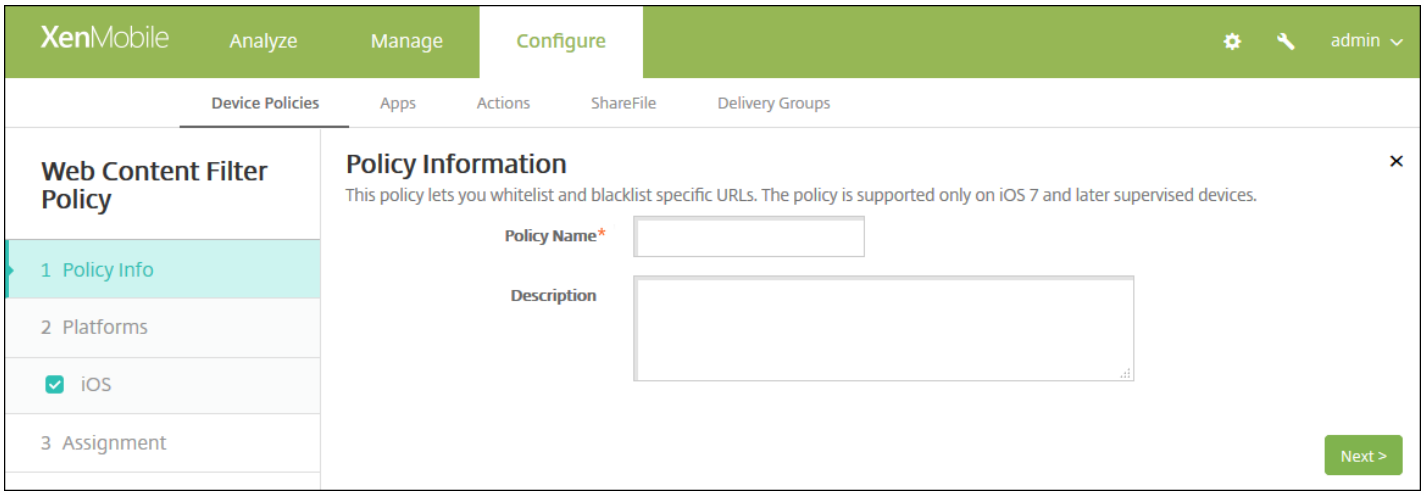
Aug 02, 2016

XenMobileでデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトとAppleのオートフィルター機能を組み合わせて使用して、iOSデバイスでWebコンテンツをフィルタリングできます。 このポリシーはiOS 7.0以降のSupervisedモードのデバイスでのみ使用できます。 iOSデバイスをSupervisedモードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

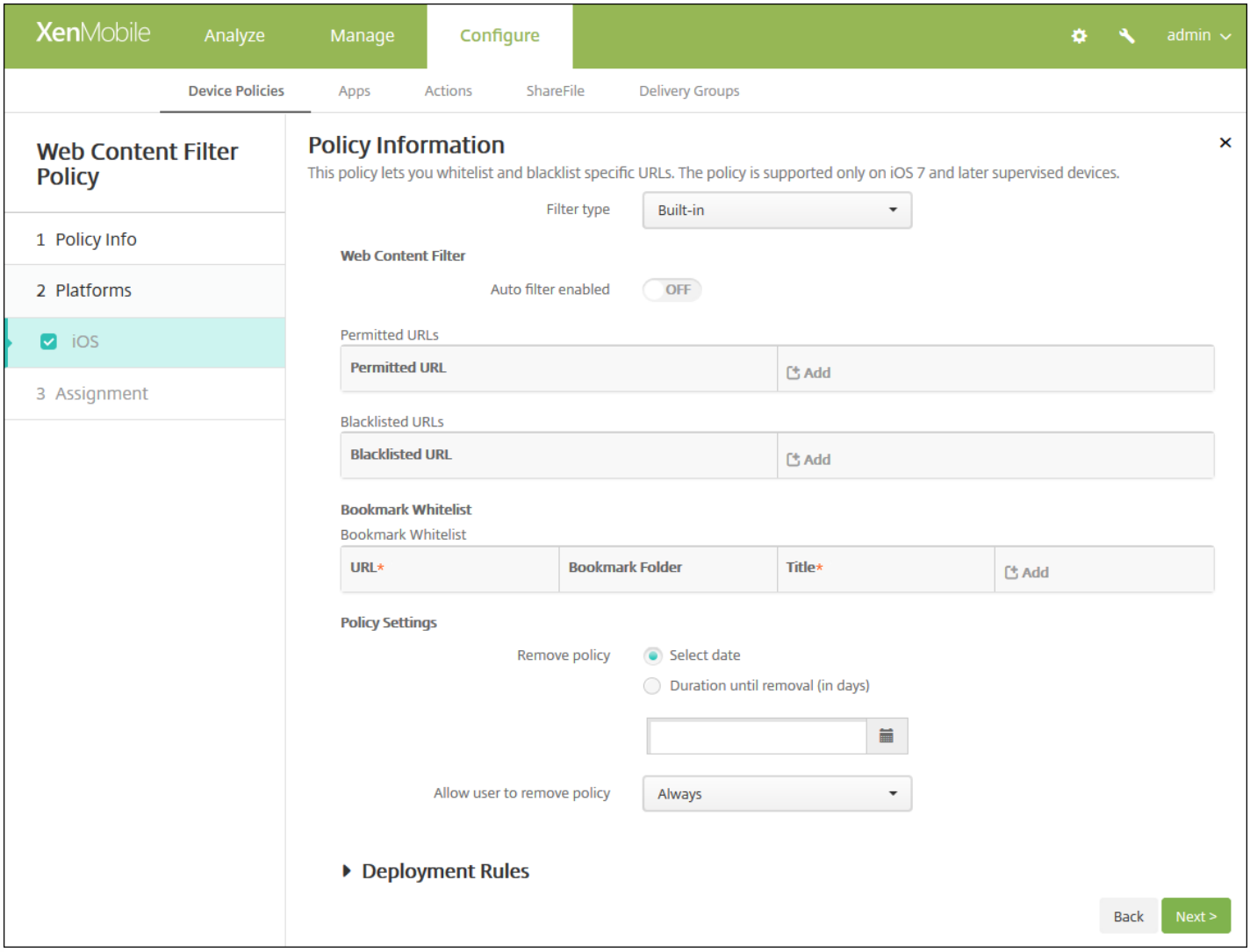
3. **[More]** をクリックした後、 **[Security]** の下の **[Web Content Filter]** をクリックします。 **[Web Content Filter Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[iOS Platform]** 情報ページが開きます。



6. 次の設定を構成します。

- **Filter type**：一覧から［**Built-in**］または［**Plug-in**］を選択し、選択したオプションに応じた手順を実行します。 デフォルトは［**Built-in**］です。

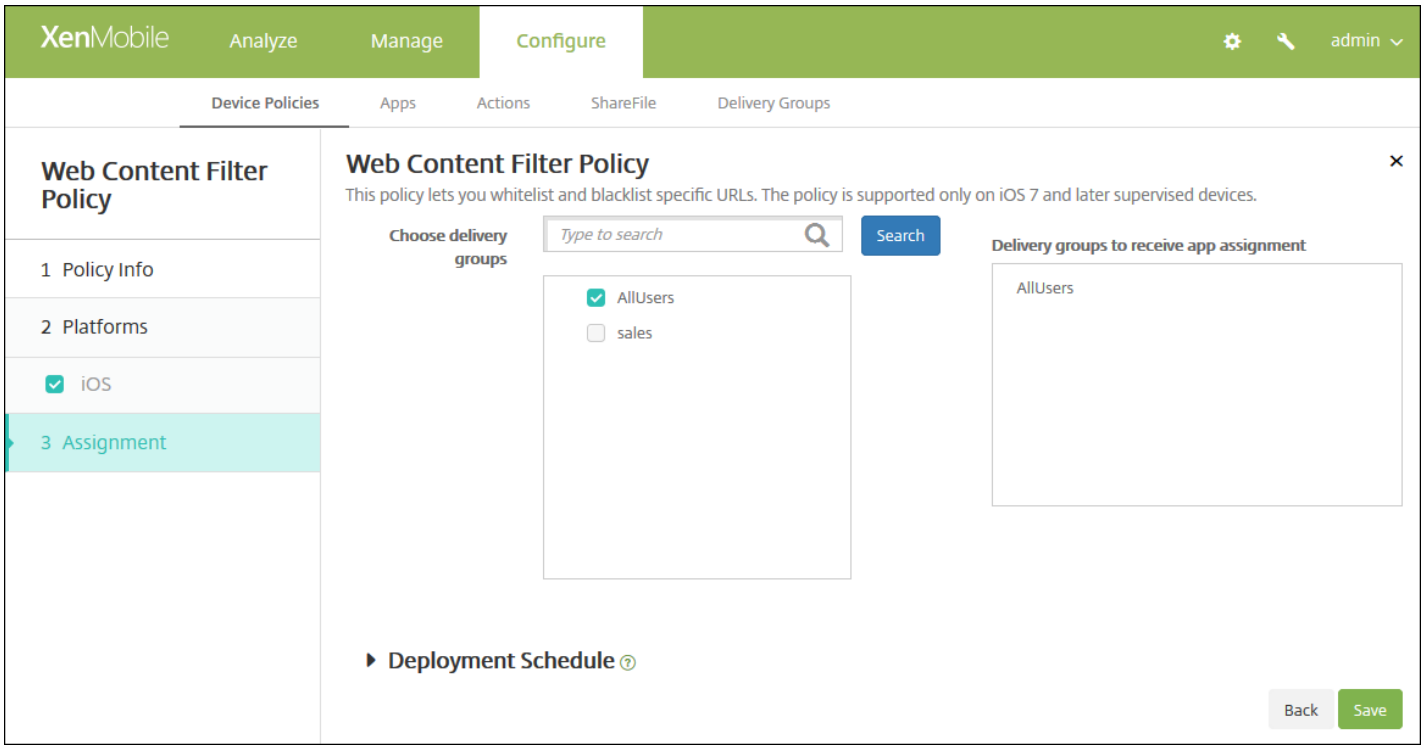
組み込みフィルターの種類の設定

プラグインフィルターの種類の設定

- **ポリシー設定**
  - ［**Remove policy**］の横の［**Select date**］ または［**Duration until removal (in days)**］をクリックします。
  - ［**Select date**］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［**Allow user to remove policy**］の一覧で、［**Always**］、［**Password required**］、［**Never**］のいずれかを選択します。
  - ［**Password required**］を選択した場合、［**Removal password**］の横に必要なパスワードを入力します。

7. 展開規則の構成

8. ［**Next**］をクリックします。 ［**Web Content Filter Policy**］割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、**[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

Webクリップデバイスポリシー

Aug 02, 2016

ユーザーのデバイス上にWebサイトへのショートカット（Webクリップ）を配置し、アプリケーションと並べて表示できます。 iOS、Mac OS X、およびAndroidデバイスについては、 Webクリップ を表す独自のアイコンを指定できます。Windowタブレットのみ、ラベルおよびURLが必要になります。

iOSの設定

Mac OS Xの設定

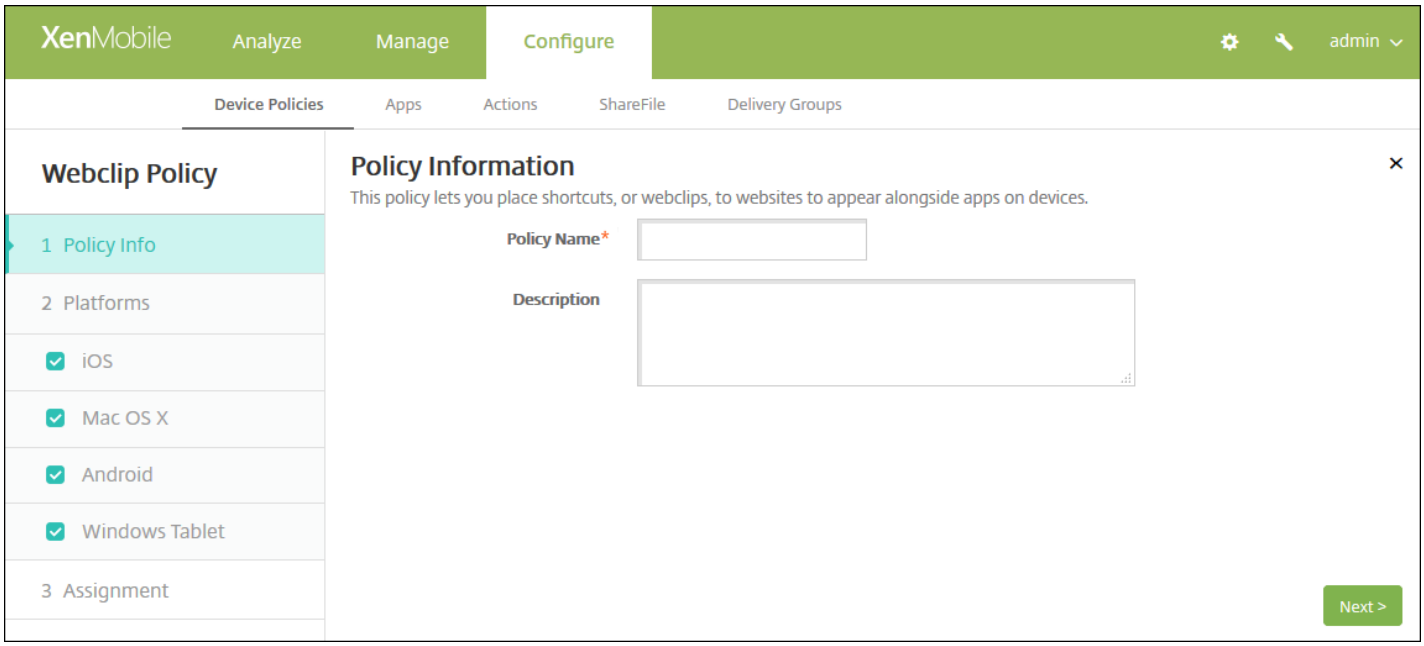
Androidの設定

Windowsタブレットの設定

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

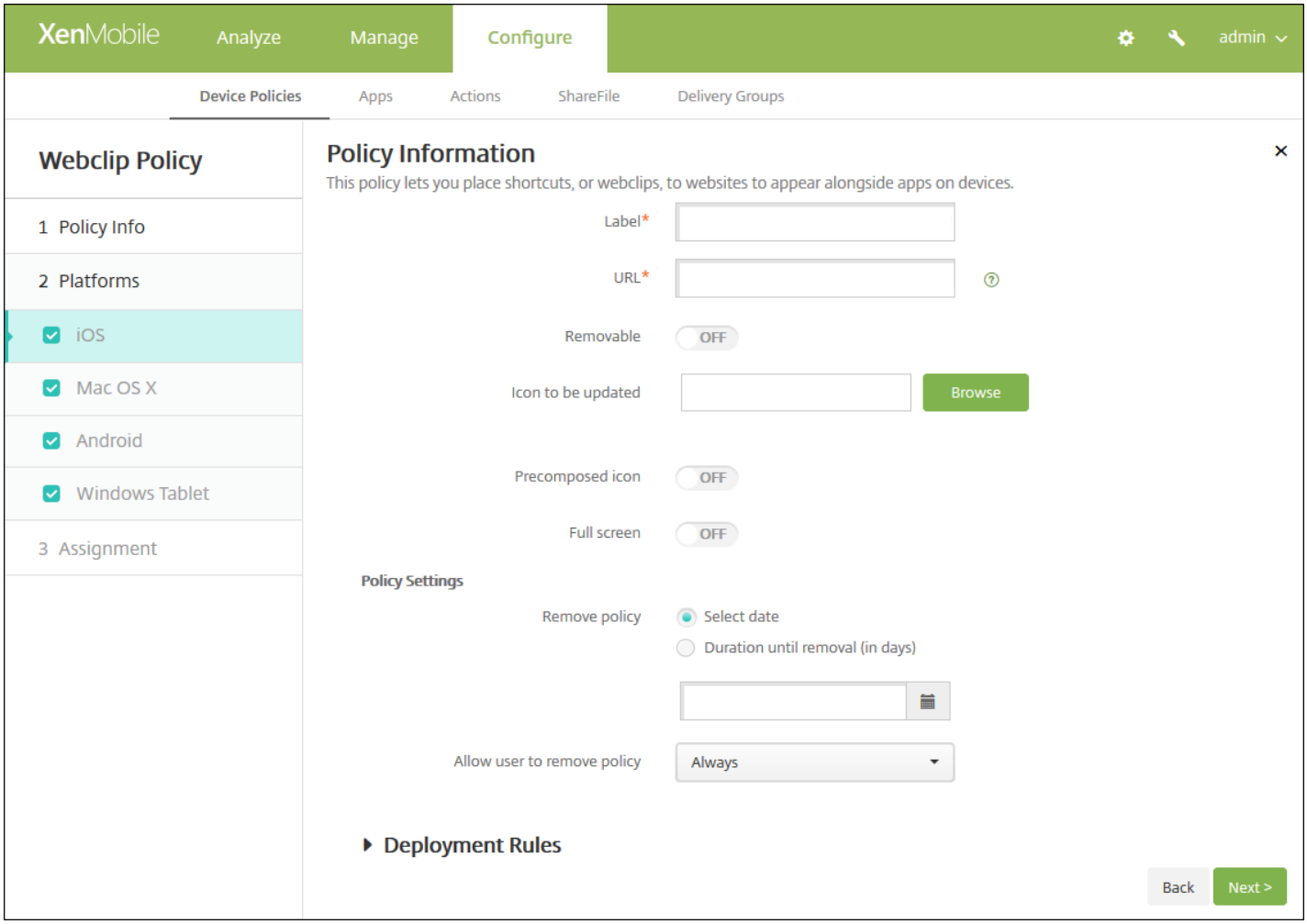
3. **[More]** を展開し、 **[Apps]** の下の **[Webclip]** をクリックします。 **[Webclip Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

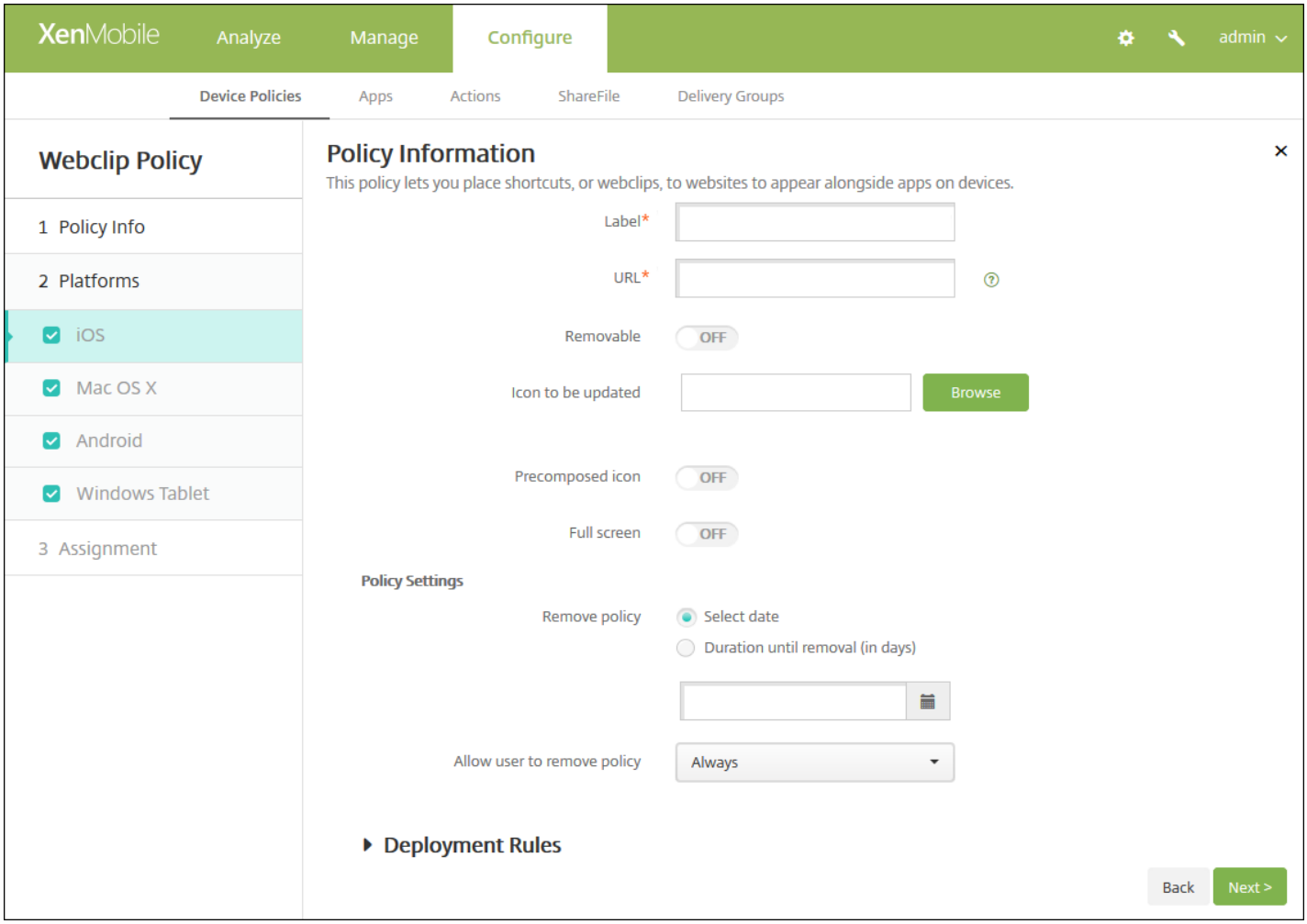
5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. **[Platforms]**の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

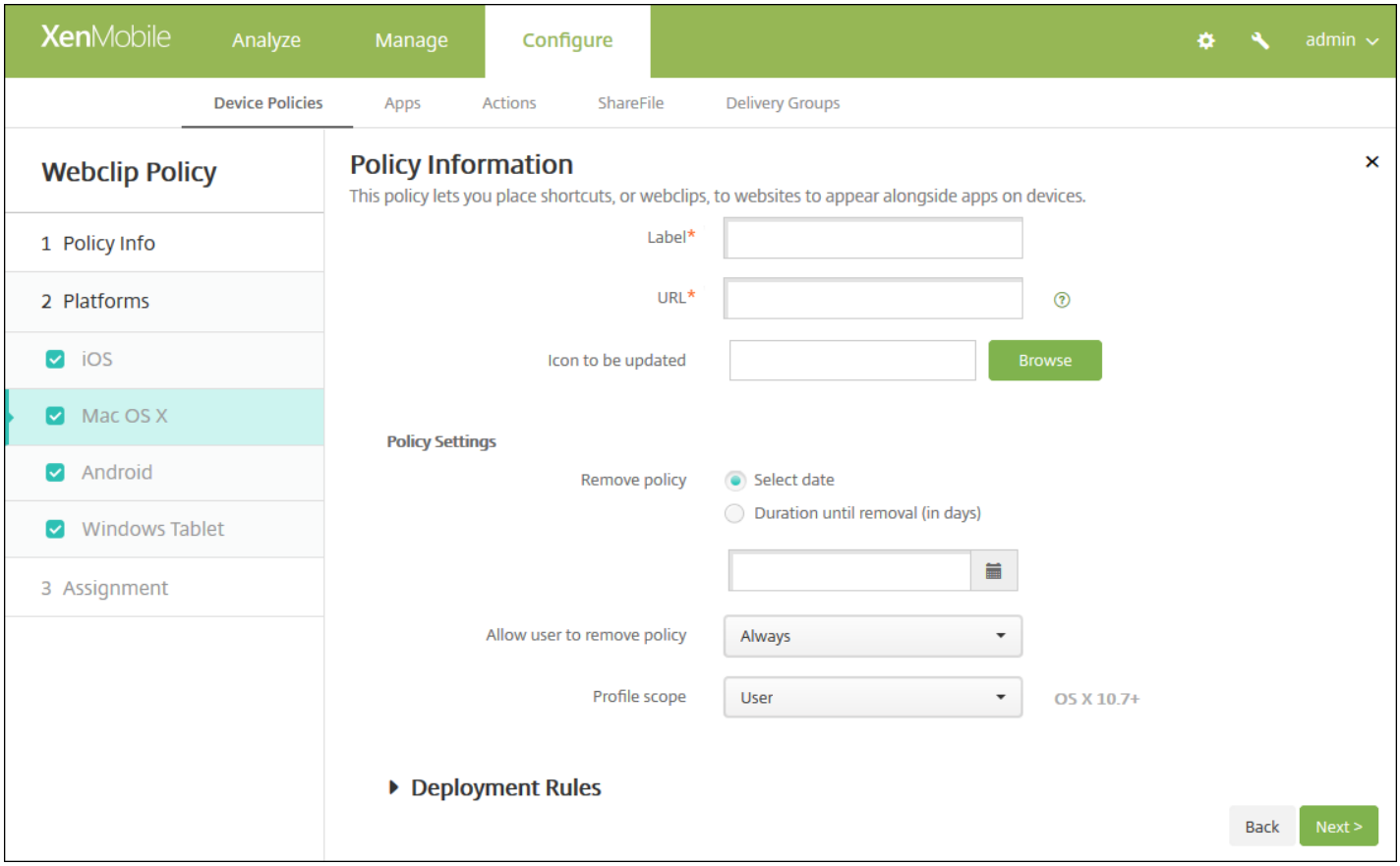
iOSの設定の構成



次の設定を構成します。

- **Label**：Webクリップとともに表示するラベルを 入力します。
- **URL**：Webクリップに関連付けるURLを 入力します。 URLはプロトコル（例：http://server）で始まる必要があります。
- **Removable**：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**[OFF]** です。
- **Icon to be updated** ： **[Browse]** をクリックしてWebクリップに使用するアイコンファイルの場所に移動し、ファイルを選択します。
- **Precomposed icon**：アイコンにエフェクト（角丸、影付き、反射光）を適用するかどうかを選択します。 デフォルトは **[OFF]** で、エフェクトが追加されます。
- **Full screen**：リンクされているWebページを全画面モードで開くかどうかを選択します。 デフォルトは**[OFF]** です。
- **ポリシー設定**
  - **[Remove policy]** の横の **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、 **[Always]** 、 **[Password required]** 、 **[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、 **[Removal password]** の横に必要なパスワードを入力します。

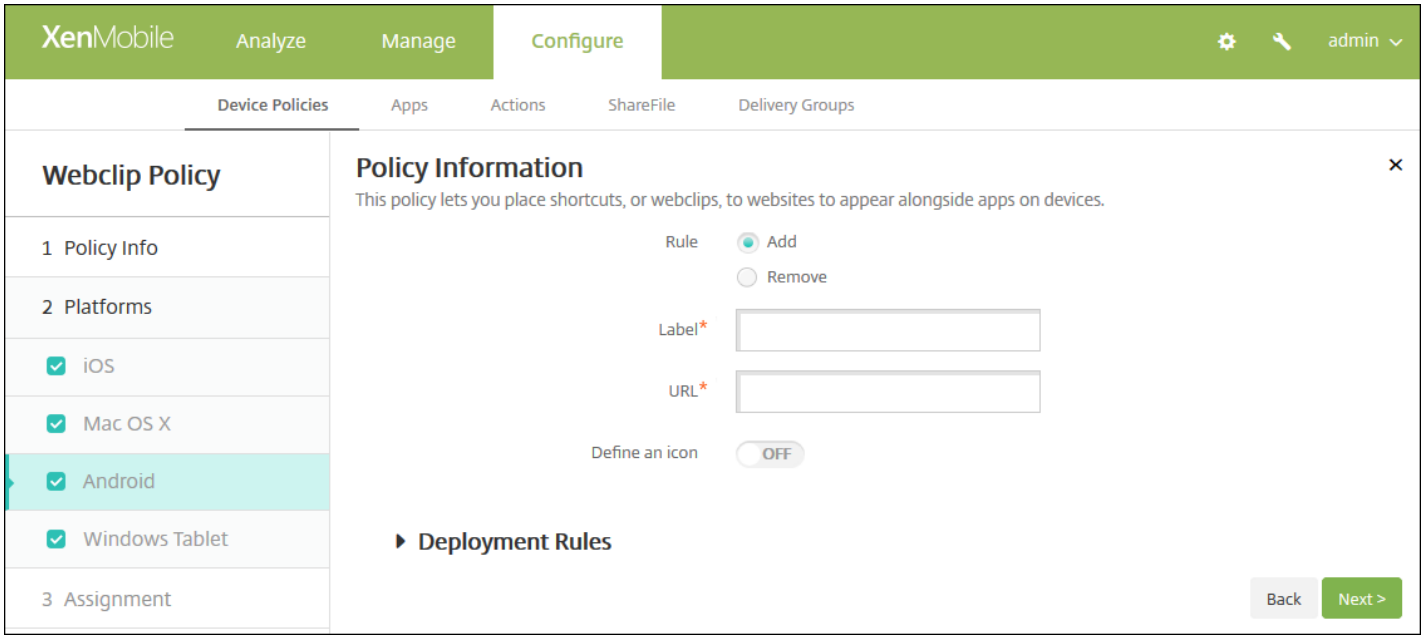
Mac OS Xの設定の構成



次の設定を構成します。

- **Label**：Webクリップとともに表示するラベルを 入力します。
- **URL**：Webクリップに関連付けるURLを 入力します。 URLはプロトコル（例：http://server）で始まる必要があります。
- **Icon to be updated** ： ［Browse］をクリックしてWebクリップに使用するアイコンファイルの場所に移動し、ファイルを選択します。
- **ポリシー設定**
  - **［Remove policy］**の横の **［Select date］** または **［Duration until removal (in days)］**をクリックします。
  - **［Select date］**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **［Allow user to remove policy］**の一覧で、 **［Always］**、 **［Password required］**、 **［Never］**のいずれかを選択します。
  - **［Password required］**を選択した場合、 **［Removal password］**の横に必要なパスワードを入力します。
  - **［Profile scope］**の一覧から、 **［User］**または **［System］**を選択します。 このオプションはOS X 10.7以降で使用できます。

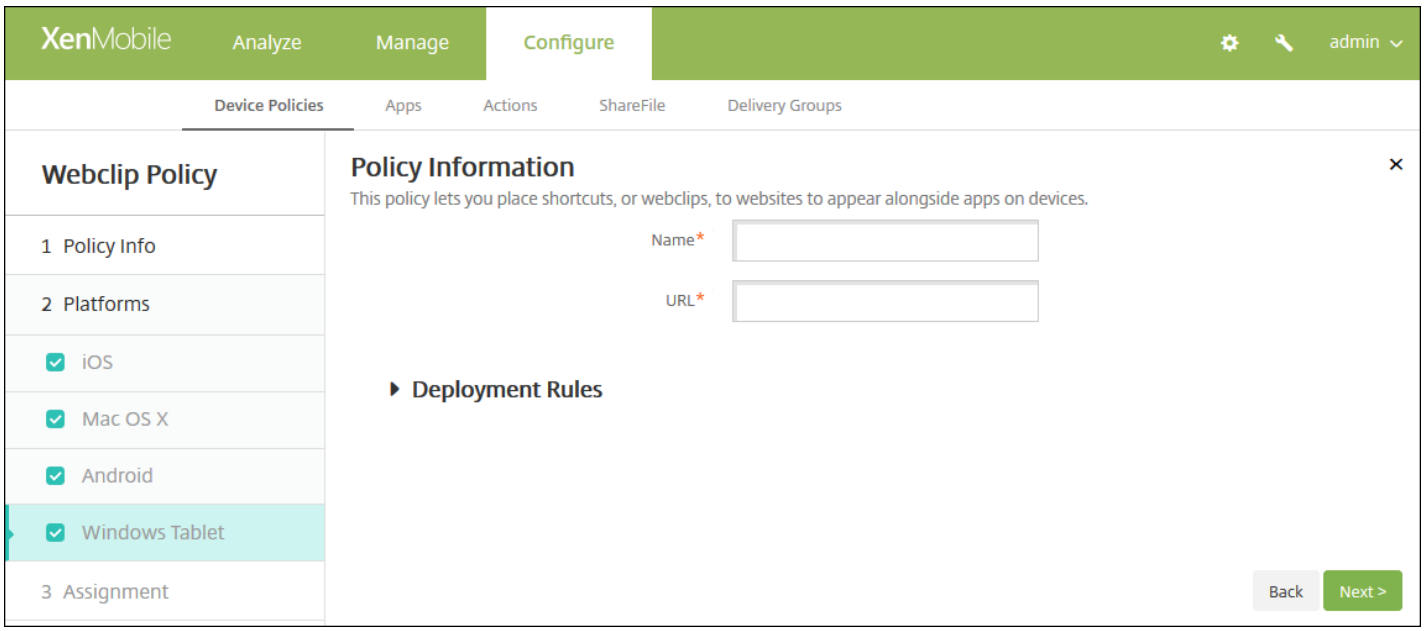
Androidの設定の構成



次の設定を構成します。

- **Rule**：このポリシーでWebクリップを追加または削除するかどうかを 選択します。 デフォルトは［Add］です。
- **Label**：Webクリップとともに表示するラベルを 入力します。
- **URL**：Webクリップに関連付けるURLを 入力します。
- **Define an icon**：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**[OFF]** です。
- **Icon file**： **[Define an icon]** が **[ON]** の場合は、 **[Browse]** をクリックしてアイコンファイルの場所に移動し、ファイルを選択します。

Windowsタブレットの設定の構成

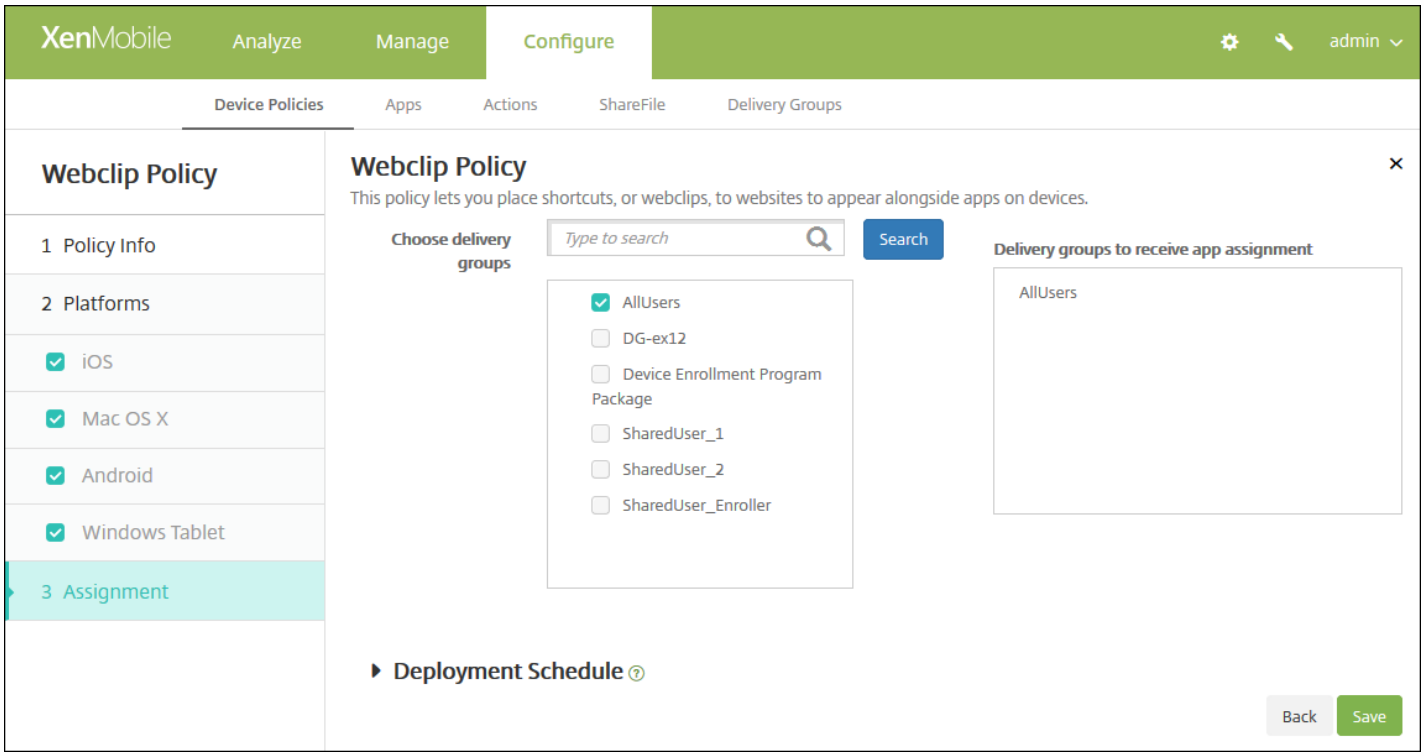


次の設定を構成します。

- **Name**：Webクリップとともに表示するラベルを 入力します。
- **URL**：Webクリップに関連付けるURLを 入力します。

7. 展開規則を構成します。

8. [**Next**] をクリックします。 [**Webclip Policy**] 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用さ

れます。ただし、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックしてポリシーを保存します。

WiFiデバイスポリシー

Aug 02, 2016

XenMobileコンソールの［Device Policies］ページを使用して、XenMobileで新しいWiFiデバイスポリシーを作成するか、既存のWiFiデバイスポリシーを編集します。 WiFiポリシーでは、ネットワークの名前と種類、認証およびセキュリティポリシー、プロキシ サーバーの使用の有無や、 そのほかのWiFi関連事項を、特定のプラットフォームのすべてのユーザーに対して一貫的に定義し、ユーザーデバイスのWiFiネットワークへの接続方法を管理できます。

ユーザーのWiFi設定は、iOS、Mac OS X、Android（Android for Work対応デバイスを含む）、Windows Phone、Windowsタブレットの各プラットフォームについて構成できます。 プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

iOSの設定

Mac OS Xの設定

Androidの設定

Windows Phoneの設定

Windowsタブレットの設定

Important

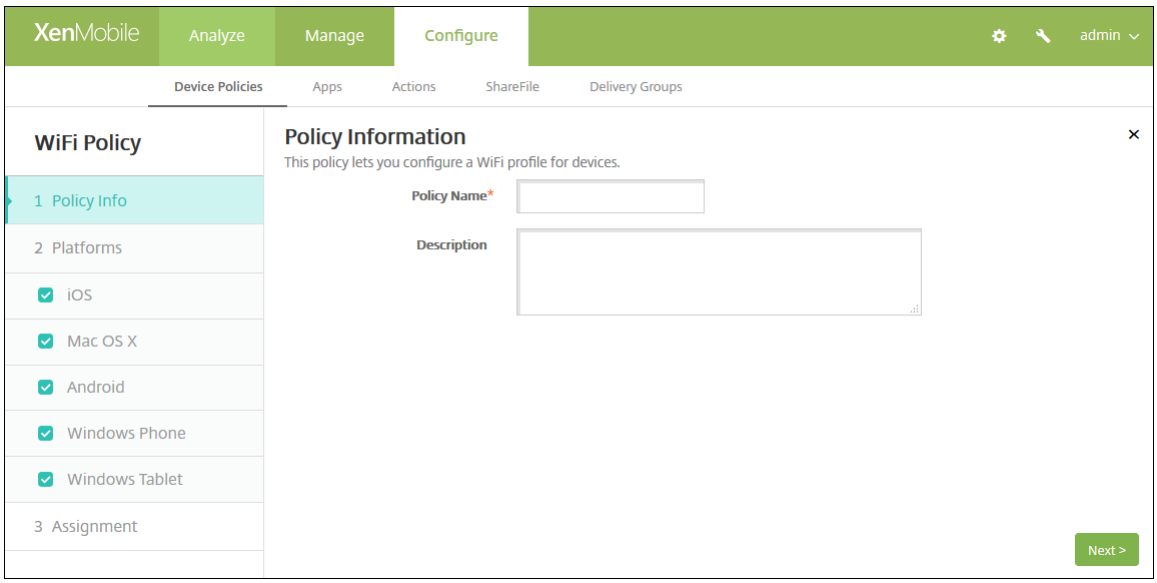
新しいポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定の展開グループを作成します。
- ネットワークの名前と種類を確認します。
- 使用する予定の認証またはセキュリティの種類を確認します。
- 必要な場合、プロキシサーバーの情報を確認します。
- 必要なCA証明書をインストールします。
- 必要な共有キーを取得します。

1.XenMobileコンソールで、 **［Configure］の［Device Policies］**をクリックします。 **［Device Policies］**ページが開きます。

2. **［Add］**をクリックします。 **［Add a New Policy］**ダイアログボックスが開きます。

3. **［WiFi］**をクリックします。 **［WiFi Policy］**ページが開きます。



4. **［Policy Information］**ペインで、以下の情報を入力します。

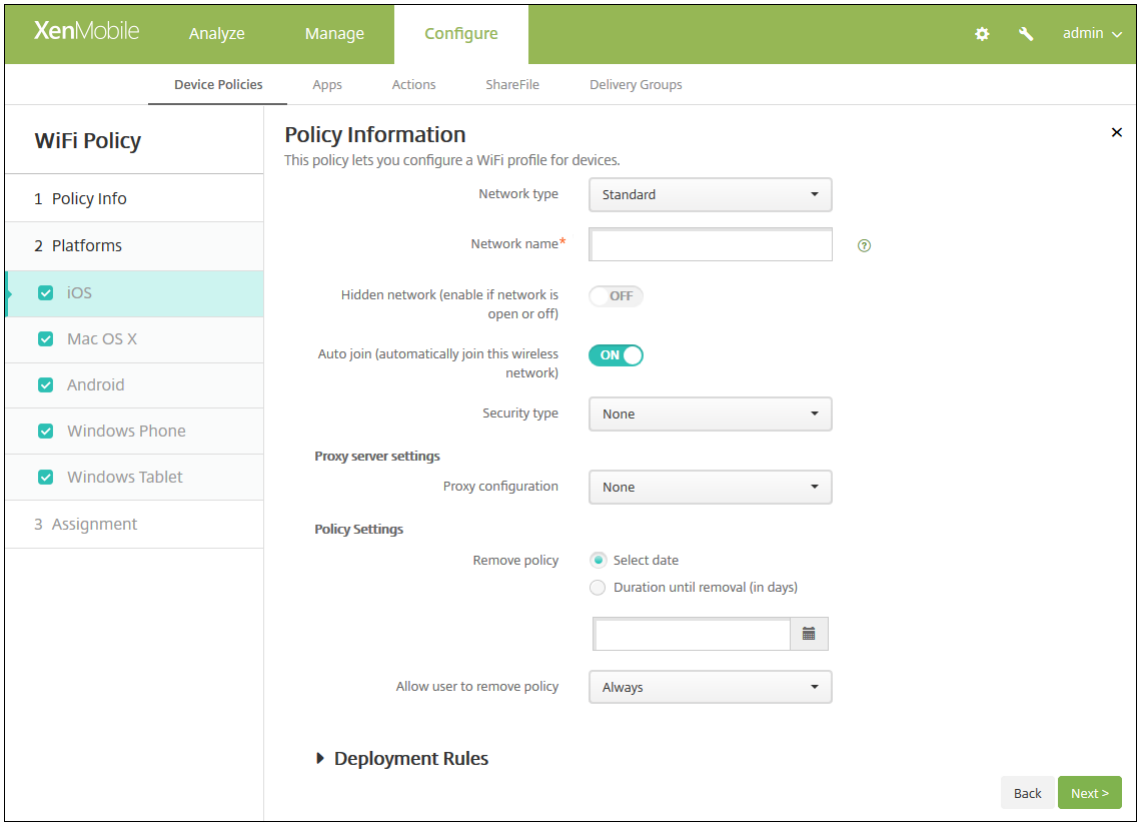
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **［Next］**をクリックします。 **［Platforms］**ページが開きます。

6. **［Platforms］**の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



次の設定を構成します。

- **Network type**：一覧から、［**Standard**］、［**Legacy Hotspot**］、または［**Hotspot 2.0**］を選択して、使用する予定のネットワークの種類を設定します。
- **Network Name**：デバイスの使用可能なネットワークの一覧に表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **Hidden network (enable if network is open or off)**：ネットワークを隠しネットワークにするかどうかを選択します。
- **Auto Join (automatically join this wireless network)**：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。 デフォルトは［**ON**］です。
- **Security type**：一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0**には適用されません。
  - None（そのほかの構成は不要）
  - WEP
  - WPA/WPA2 Personal
  - Any（Personal）
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Any（Enterprise）

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

WPA、WPA Personal、Any (Personal)

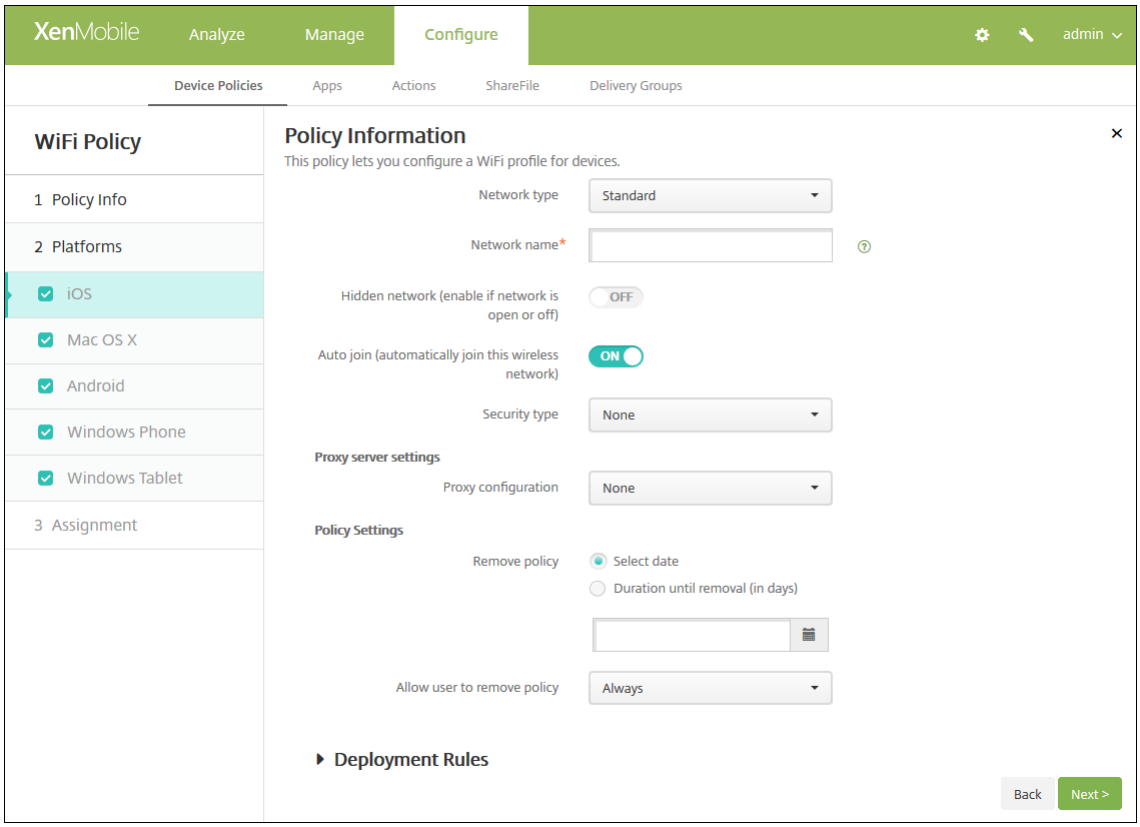
WEP Enterprise、WPA Enterprise、WPA2 Enterprise、Any (Enterprise)

- **プロキシサーバーの設定**
  - **Proxy configuration**：一覧から、［None］、［Manual］、または［Automatic］を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は［None］で、そのほかの構成は不要です。
  - ［**Manual**］を選択した場合は、次の設定を構成します。
    - **Hostname/IP address**：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。
    - **Port**：プロキシサーバーのポート番号を入力します。
    - **Username**：任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - **Password**：任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［**Automatic**］を選択した場合は、次の設定を構成します。
    - **Server 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。
    - **Allow direct connection if PAC is unreachable**：PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。 デフォルトは［**ON**］です。 このオプションはiOS 7.0以降でのみ使用できます。
- **Hotspot 2.0**
  - **Displayed operator name**：表示するオペレーター名を入力します。 iOS 7.0以降に適用されます。
  - **Domain name**：WiFi Hotspot 2.0のネゴシエーションに使用するドメイン名を入力します。 iOS 7.0以降に適用されます。
  - **Allow connecting to roaming partner networks**：デバイスがローミングパートナーネットワークに接続することを許可するかどうかを選択します。 iOS 7.0以降に適用されます。
  - **Roaming Consortium Organization Identifiers (OI)**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するローミングコンソーシアムOIを追加します。
  - **Network Access Identifier（NAI）realm names**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するNAIレルム名を追加します。
  - **Mobile Country Codes（MCCs）and Mobile Network Configurations（MNCs）**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するMCCおよびMNCペアを追加します。 どの文字列も厳密に6桁である必要があります。

［Protocols, accepted EAP types］、［Protocols, EAP-FAST］、［Authentication］について詳しくは、前のセクションを参照してください。

- **ポリシー設定**
  - ［Remove policy］の横の［Select date］または［Duration until removal (in days)］をクリックします。
  - ［Select date］をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
  - ［Password required］を選択した場合、［Removal password］の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **Network type**：一覧から、［Standard］、［Legacy Hotspot］、または［Hotspot 2.0］を選択して、使用する予定のネットワークの種類を設定します。
- **Network Name**：デバイスの使用可能なネットワークの一覧に表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **Hidden network (enable if 上 is open or off)**：ネットワークを隠しネットワークにするかどうかを選択します。
- **Auto Join (automatically join this wireless network)**：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。デフォルトは［ON］です。
- **Security type**：一覧から、使用する予定のセキュリティの種類を選択します。**Hotspot 2.0**には適用されません。
  - None（そのほかの構成は不要）
  - WEP
  - WPA/WPA2 Personal
  - Any（Personal）
  - WEP Enterprise
  - WPA/WPA2 Enterprise
  - Any（Enterprise）

以下では、上記の接続の種類ごとに、構成するオプションを示します。

WPA、WPA Personal、WPA 2 Personal、Any (Personal)

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、Any (Enterprise)

- **Use as a Login Window configuration**：ユーザーの認証に、ログインウィンドウで入力したものと同じ資格情報を使用するかどうかを選択します。
- **プロキシサーバーの設定**
  - **Proxy configuration**：一覧から、［None］、［Manual］、または［Automatic］を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は［None］で、そのほかの構成は不要です。
  - ［Manual］を選択した場合は、次の設定を構成します。
    - **Hostname/IP address**：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。
    - **Port**：プロキシサーバーのポート番号を入力します。
    - **User name**：任意で、プロキシサーバーへの認証に使用する ユーザー名を入力します。
    - **Password**：任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - ［Automatic］を選択した場合は、次の設定を構成します。
    - **Server 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。

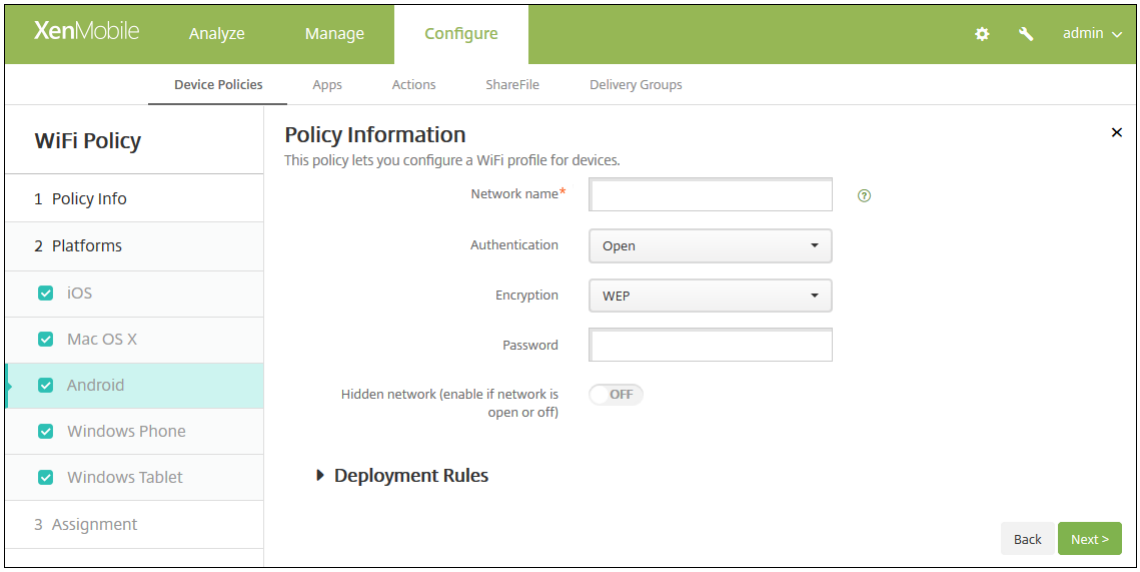
- **Allow direct connection if PAC is unreachable**：PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。 デフォルトは**[ON]** です。 このオプションはiOS 7.0以降でのみ使用できます。

- **Hotspot 2.0**
  - **Displayed operator name**：表示するオペレーター名を入力します。 iOS 7.0以降に適用されます。
  - **Domain name**：WiFi Hotspot 2.0のネゴシエーションに使用するドメイン名を入力します。 iOS 7.0以降に適用されます。
  - **Allow connecting to roaming partner networks**：デバイスがローミングパートナーネットワークに接続することを許可するかどうかを選択します。 iOS 7.0以降に適用されます。
  - **Roaming Consortium Organization Identifiers (OI)**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するローミングコンソーシアムOIを追加します。
  - **Network Access Identifier（NAI）realm names**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するNAIレルム名を追加します。
  - **Mobile Country Codes（MCCs）and Mobile Network Configurations（MNCs）**：任意で、WiFi Hotspot 2.0のネゴシエーションに使用するMCCおよびMNCペアを追加します。 どの文字列も厳密に6桁である必要があります。

    [Protocols, accepted EAP types]、**[Protocols, EAP-FAST]**、**[Authentication]** について詳しくは、前のセクションを参照してください。

- **ポリシー設定**
  - **[Remove policy]** の横の **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
  - **[Profile scope]** の横にある、**[User]** または **[System]** を選択します。 デフォルトは **[User]** です。 このオプションはOS X 10.7以降でのみ使用できます。

Androidの設定の構成



次の設定を構成します。

- **Network name**：ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Authentication**：一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - Open
  - Shared
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

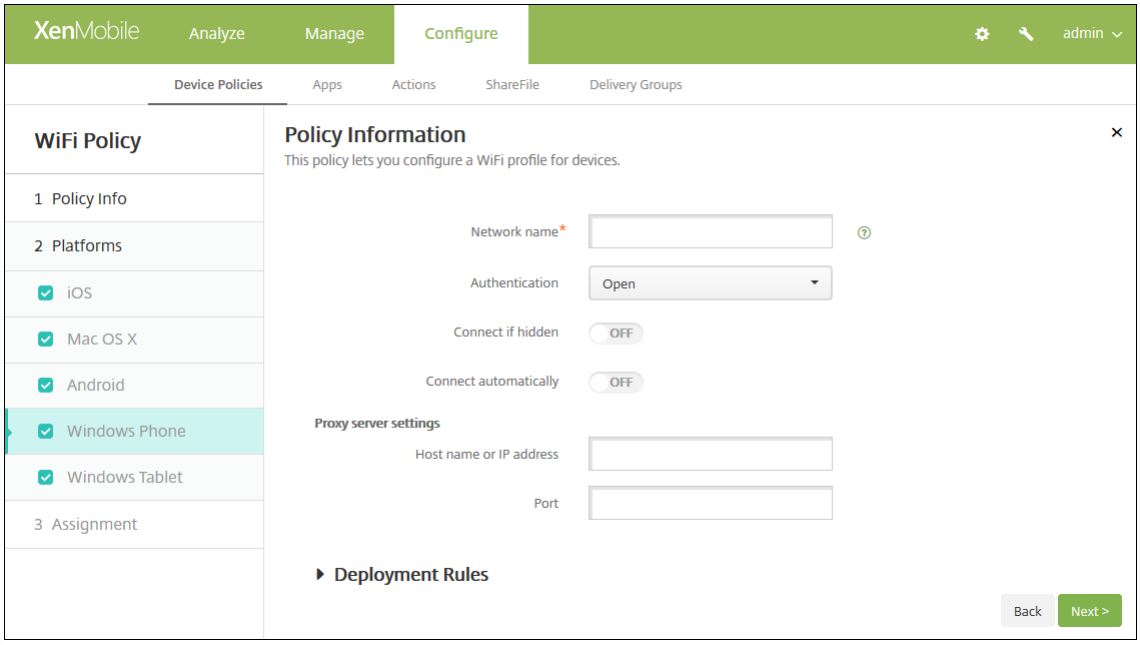
Open、Shared

WPA、WPA-PSK、WPA2、WPA2-PSK

802.1x

- **Hidden network（Enable if network is open or off）**：ネットワークを隠しネットワークにするかどうかを選択します。

Windows Phoneの設定の構成



次の設定を構成します。

- **Network name**：ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Authentication**：一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA-2 Enterprise

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

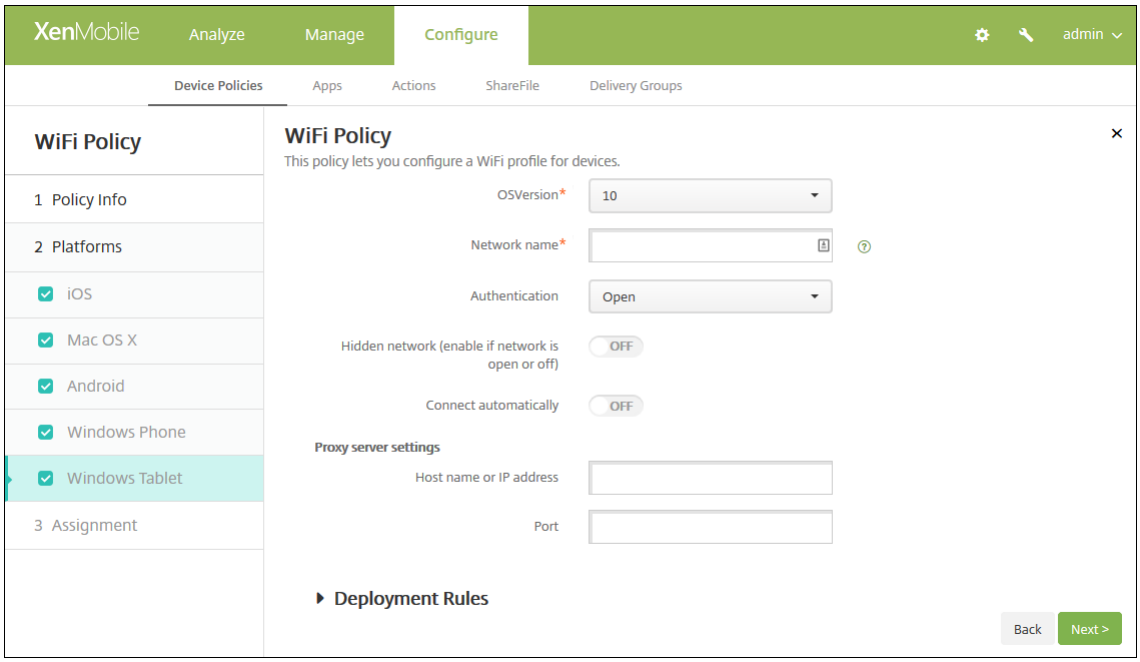
Open

WPA Personal、WPA-2 Personal

WPA-2 Enterprise

- **プロキシサーバーの設定**
  - **Host name or IP address**：プロキシサーバーの名前またはIPアドレスを入力します。
  - **Port**：プロキシサーバーのポート番号を入力します。

Windowsタブレットの設定の構成



次の設定を構成します。

- **OSVersion**：一覧から、Windows 8.1の場合は［**8.1**］を、Windows 10の場合は［**10**］を選択します。 デフォルトは**10**です。

Windows 10の設定

- **Authentication**：一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

Open

WPA Personal、WPA-2 Personal

WPA-2 Enterprise

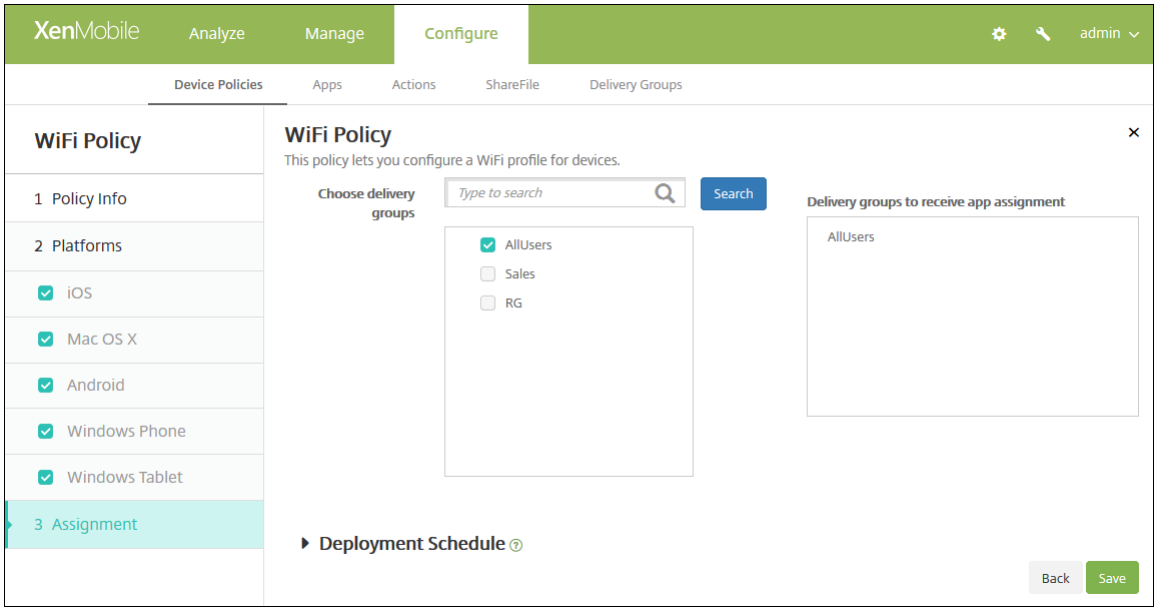
Windows 8.1の設定

- **Network name**：ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Authentication**：一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - Open
  - WPA Personal
  - WPA-2 Personal
  - WPA Enterprise
  - WPA-2 Enterprise
- **Hidden network（Enable if network is open or off）**：ネットワークを隠しネットワークにするかどうかを選択します。
- **Connect automatically**：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。

7. 展開規則を構成します。

8. ［**Next**］をクリックします。 ［**WiFi Policy**］割り当てページが開きます。

8. ［**Next**］をクリックします。 ［**WiFi Policy Assignment**］ページが開きます。
8. ［**Next**］をクリックします。 ［**WiFi Policy Assignment**］ページが開きます。
8. ［**Next**］をクリックします。 ［**WiFi Policy Assignment**］ページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。 デフォルトのオプションは、［**On every connection**］です。

- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

Windows CE証明書デバイスポリシー

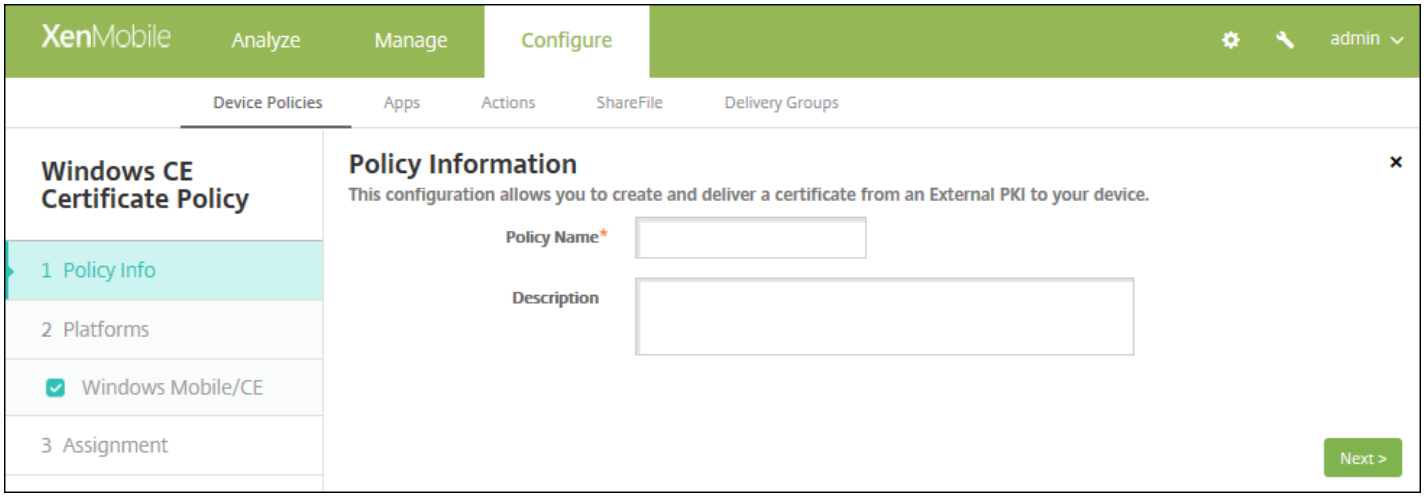
Aug 02, 2016

XenMobileでは、外部のPKIを基にWindows Mobile/CE証明書を作成し、ユーザーのデバイスに配布するデバイスポリシーを作成できます。 証明書およびPKIエンティティについて詳しくは、「証明書」を参照してください。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add New Policy]** ダイアログボックスが開きます。

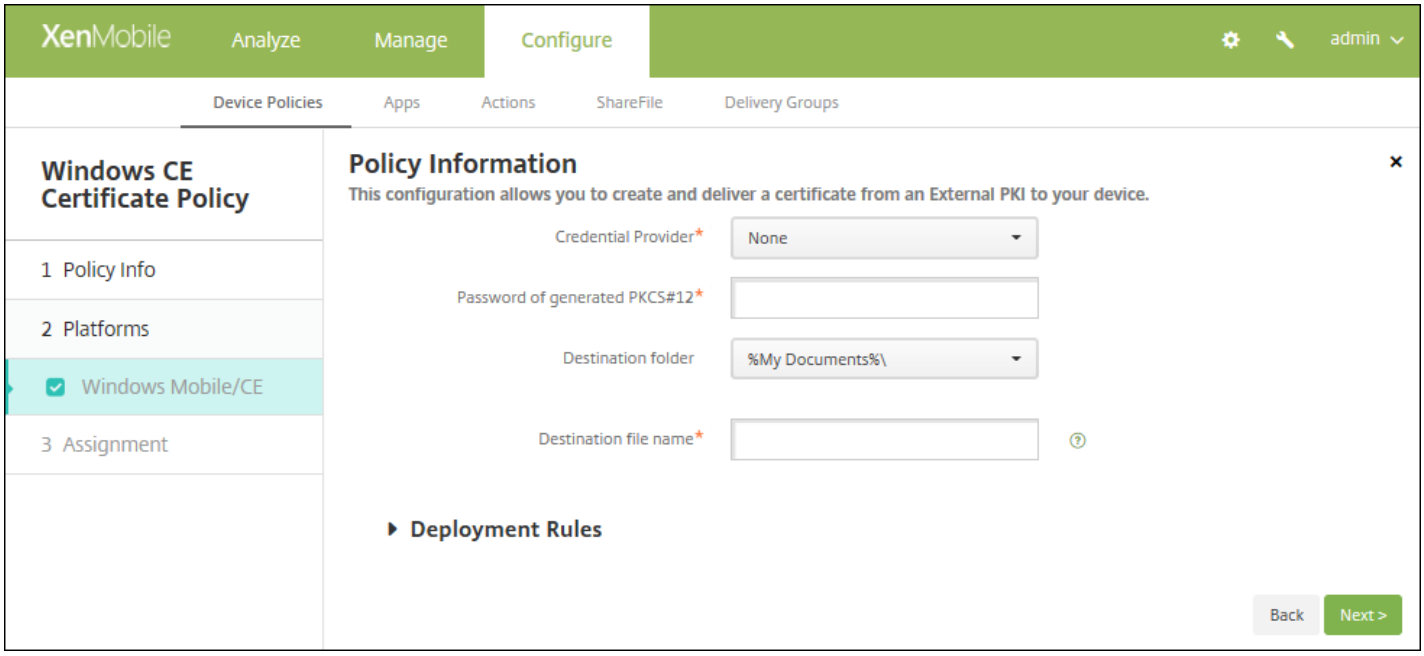
3. **[More]** を展開した後、 **[Security]** の下の **[Windows CE Certificate]** をクリックします。 **[Windows CE Certificate Policy]** 情報ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Windows CE Certificate Policy Platform]** 情報ページが開きます。

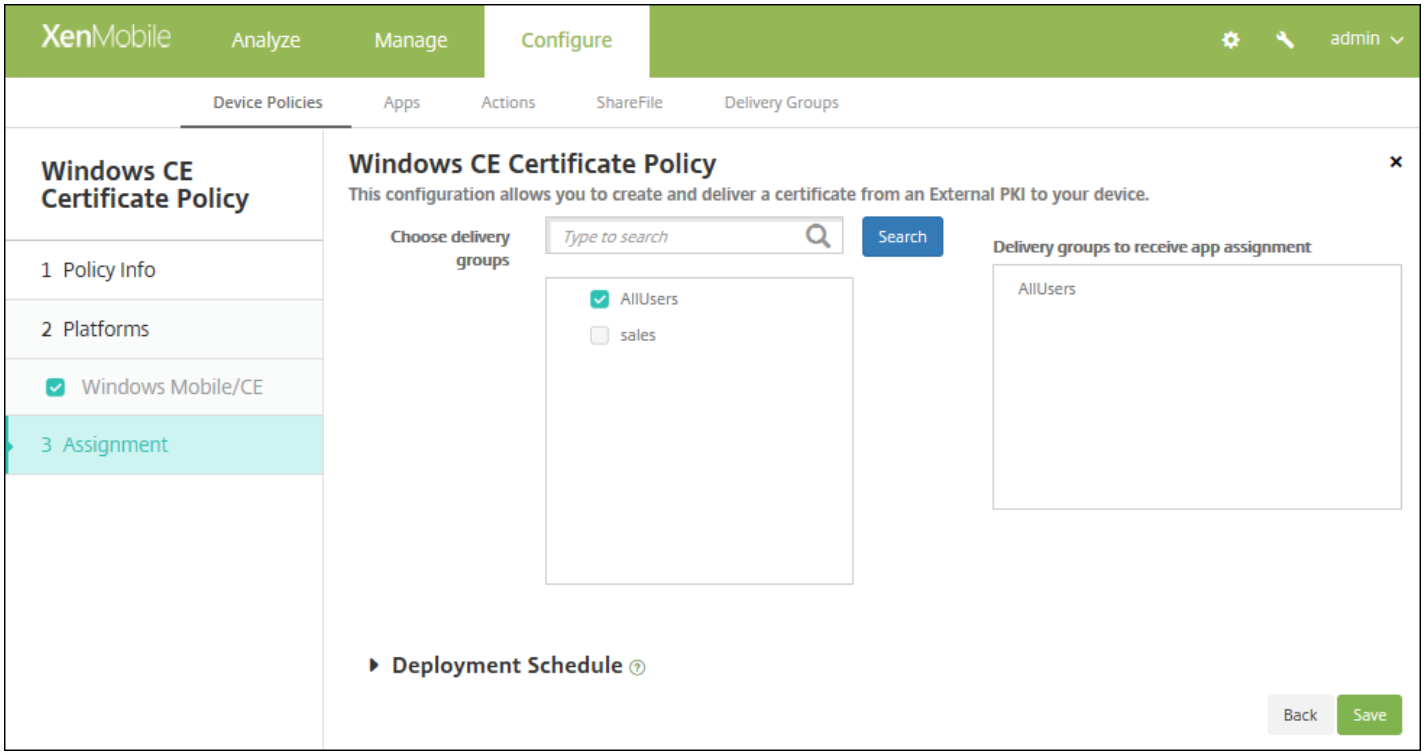


6. 次の設定を構成します。

- **Credential provider**：ボックスの一覧で、資格情報プロバイダーを選択します。 デフォルトは **[None]** です。
- **Password of generated PKCS#12**：資格情報の暗号化に使用するパスワードを入力します。
- **Destination folder**：一覧から資格情報の宛先フォルダーを選択するか、 **[Add new]** をクリックして、一覧に表示されていないフォルダーを追加します。 事前定義済みのオプションは以下のとおりです。
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name**：資格情報ファイルの名前を入力します。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[Windows CE Certificate Policy]** 割り当てページが開きます。



9. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[On every connection] です。
- [**Deploy for always-on connection**] の横の [**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] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

Worx Storeデバイスポリシー

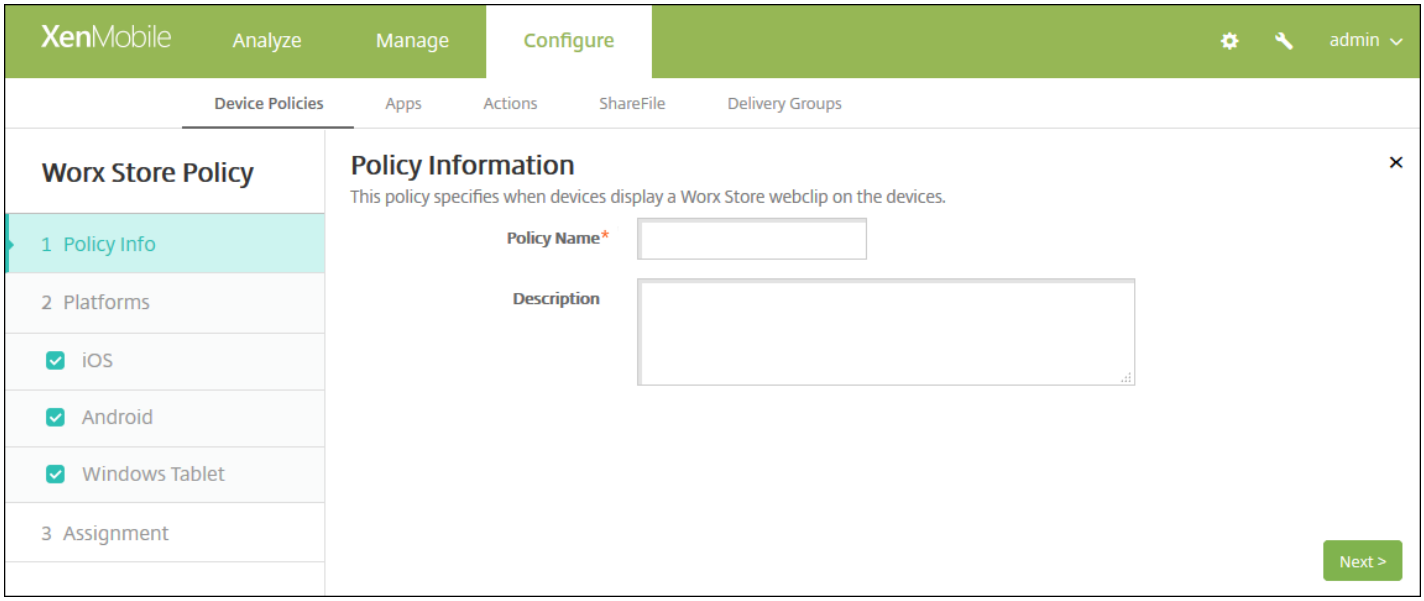
Aug 02, 2016

XenMobileでポリシーを作成して、iOS、Android、またはWindowsタブレットデバイスの ホーム画面に Worx Store Webクリップを表示するかどうかを指定できます。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

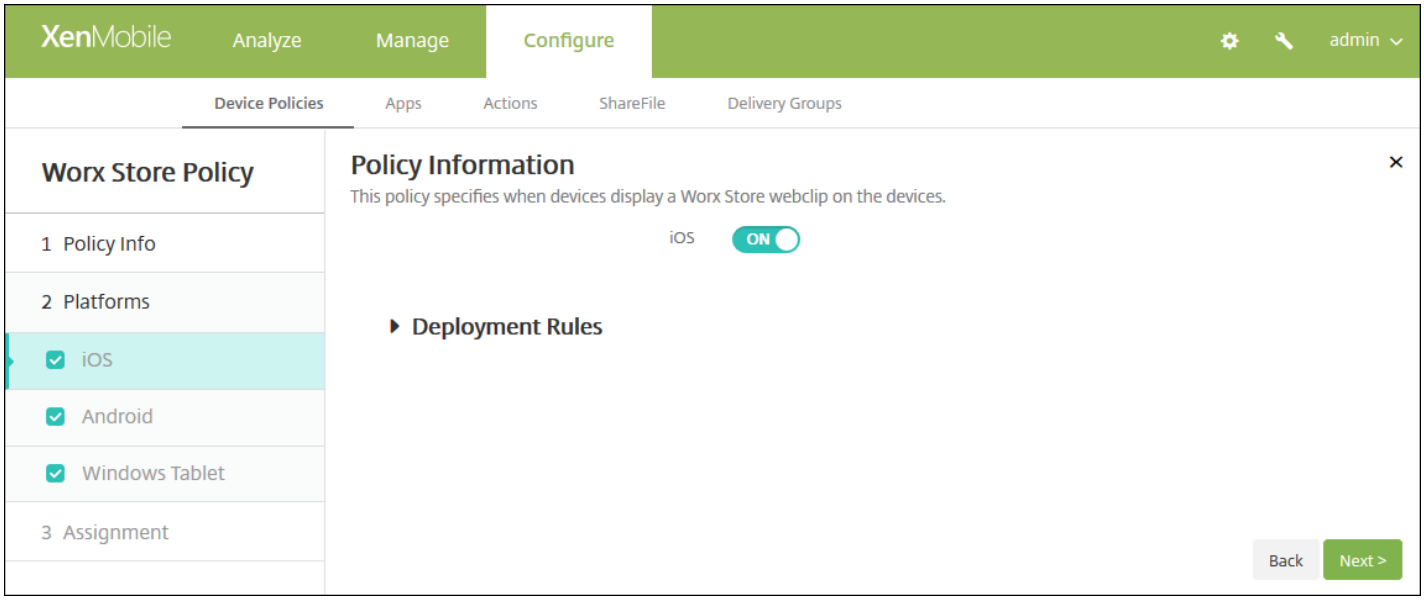
3. **[More]** を展開した後、 **[Apps]** の下の **[Worx Store]** をクリックします。 **[Worx Store Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：必要に応じて、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Platforms]** ページが開きます。



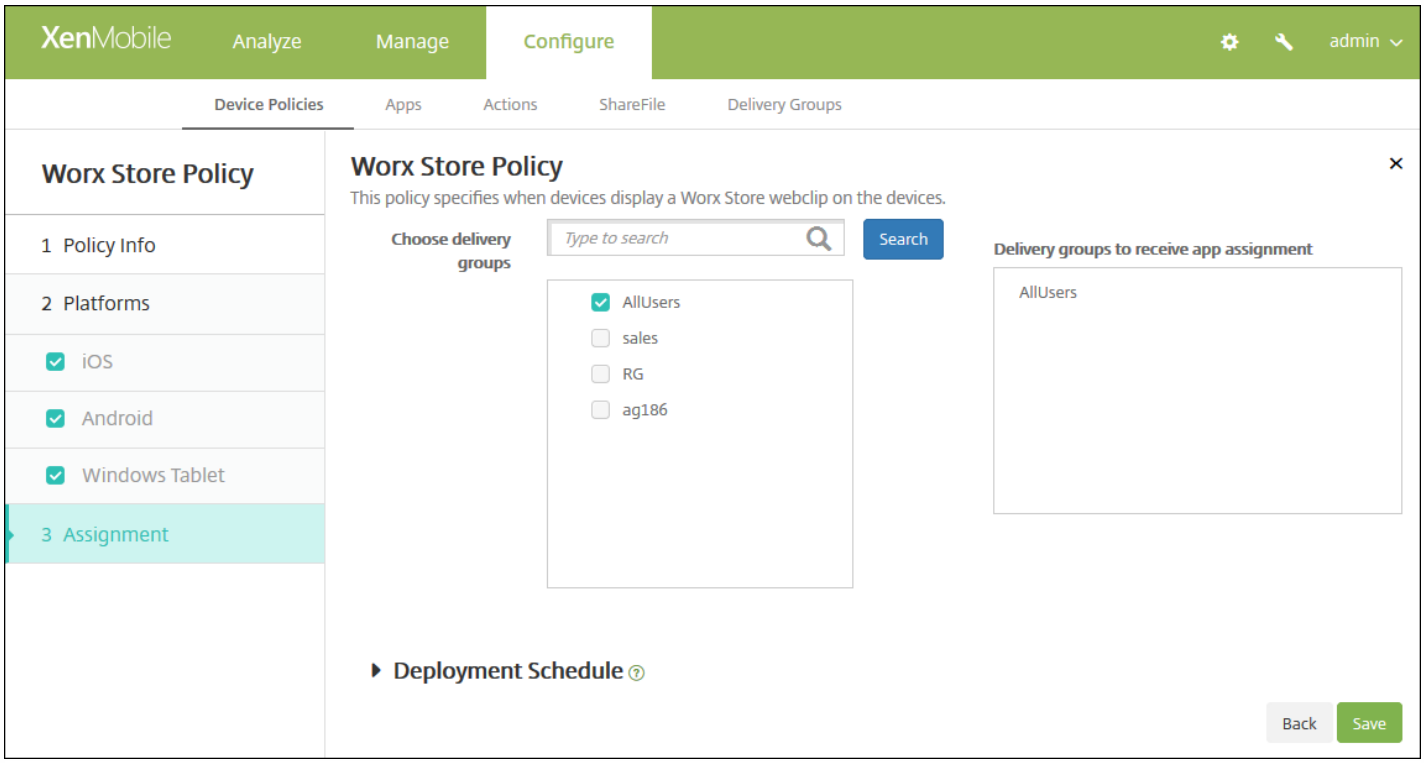
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

7. 構成するプラットフォームごとに、ユーザーデバイスにWorx Store Webクリップ を表示するかどうかを選択します。 デフォルトは **[ON]** です。

各プラットフォームの構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

8. 展開規則の構成

9. **[Next]** をクリックします。 **[Worx Store Policy]** 割り当てページが表示されます。



10. [**Choose delivery groups**] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の [**Delivery groups to receive app assignment**] 一覧に表示されます。

11. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、 [**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、 [**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、 [**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注 :

- このオプションは、 [**Settings**] > [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

12. [**Save**] をクリックします。

XenMobileオプションデバイスポリシー

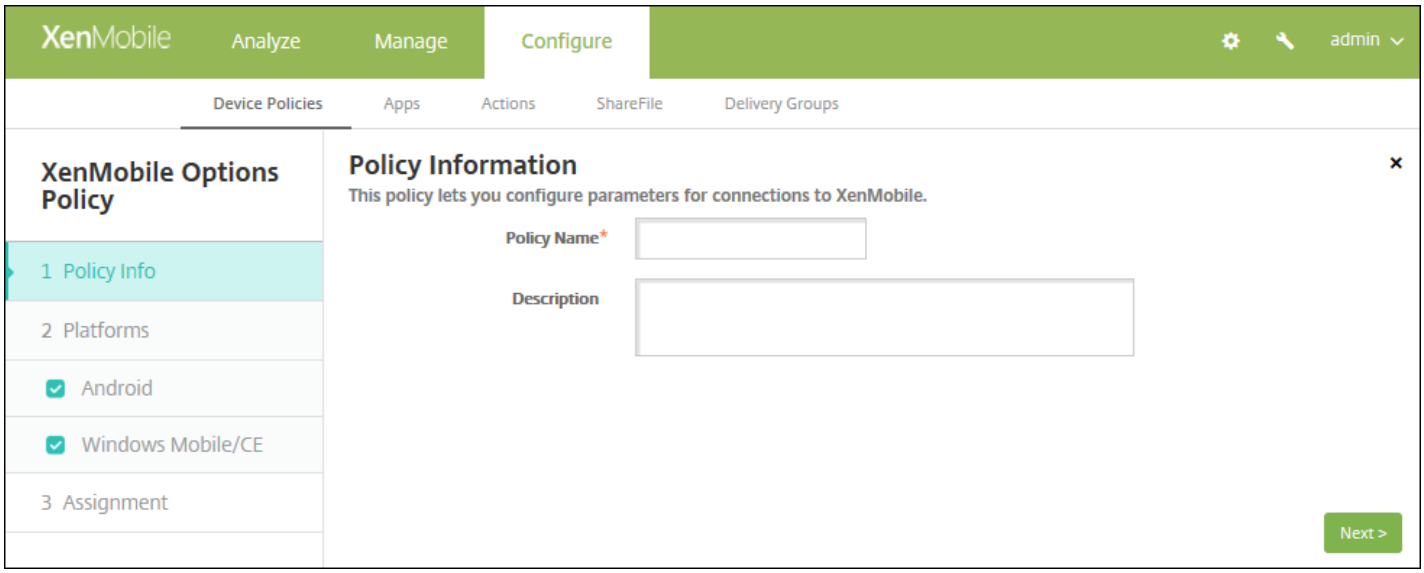
Aug 02, 2016

XenMobileオプションポリシーを追加して、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのWorx Homeの動作を構成します。

1.XenMobileコンソールで、［**Configure**］の［**Device Policies**］をクリックします。［**Device Policies**］ページが開きます。

2.［**Add**］をクリックします。［**Add a New Policy**］ダイアログボックスが開きます。

3.［**More**］をクリックした後、［**XenMobile agent**］の下の［**XenMobile Options**］をクリックします。［**XenMobile Options Policy**］ページが開きます。



4.［**Policy Information**］ペインで、以下の情報を入力します。

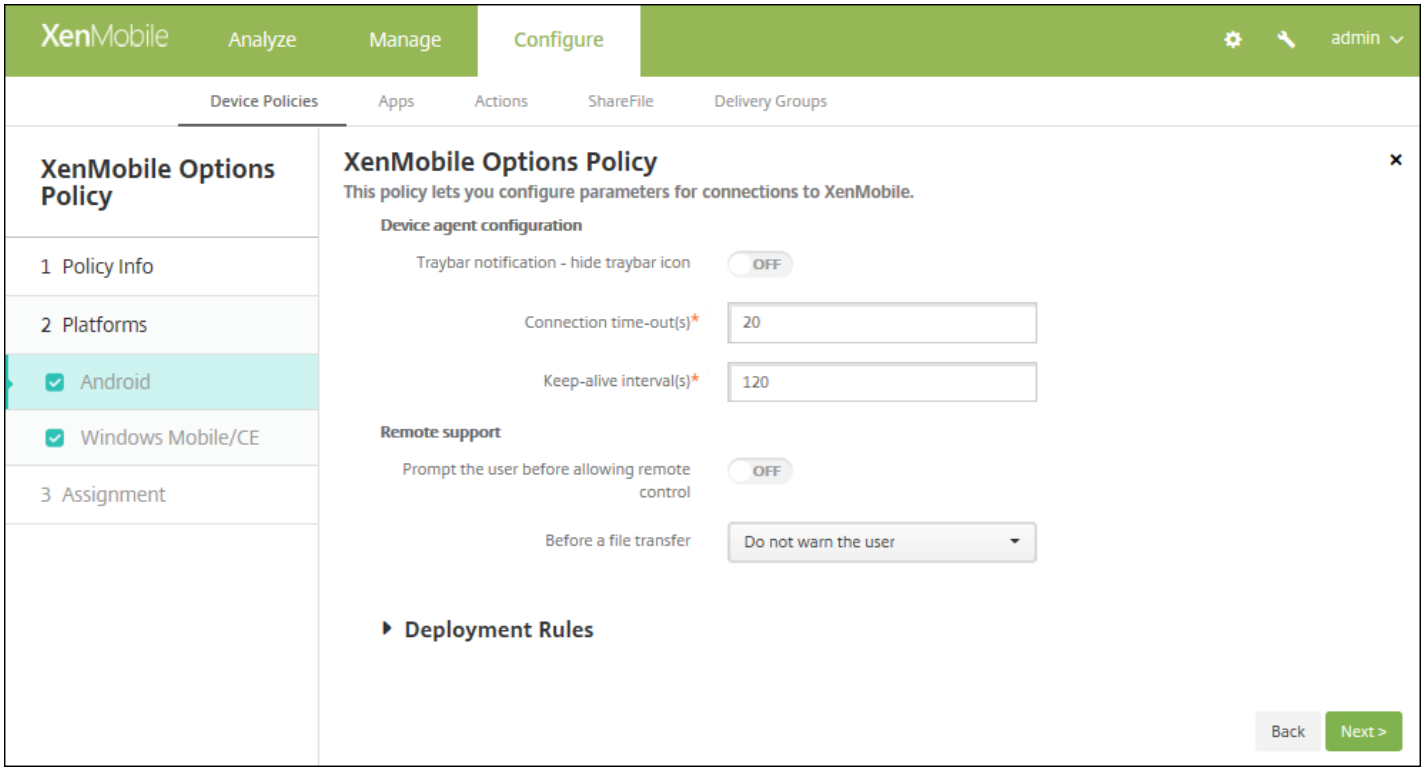
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5.［**Next**］をクリックします。［**Policy Platforms**］ページが開きます。

6.［**Platforms**］の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

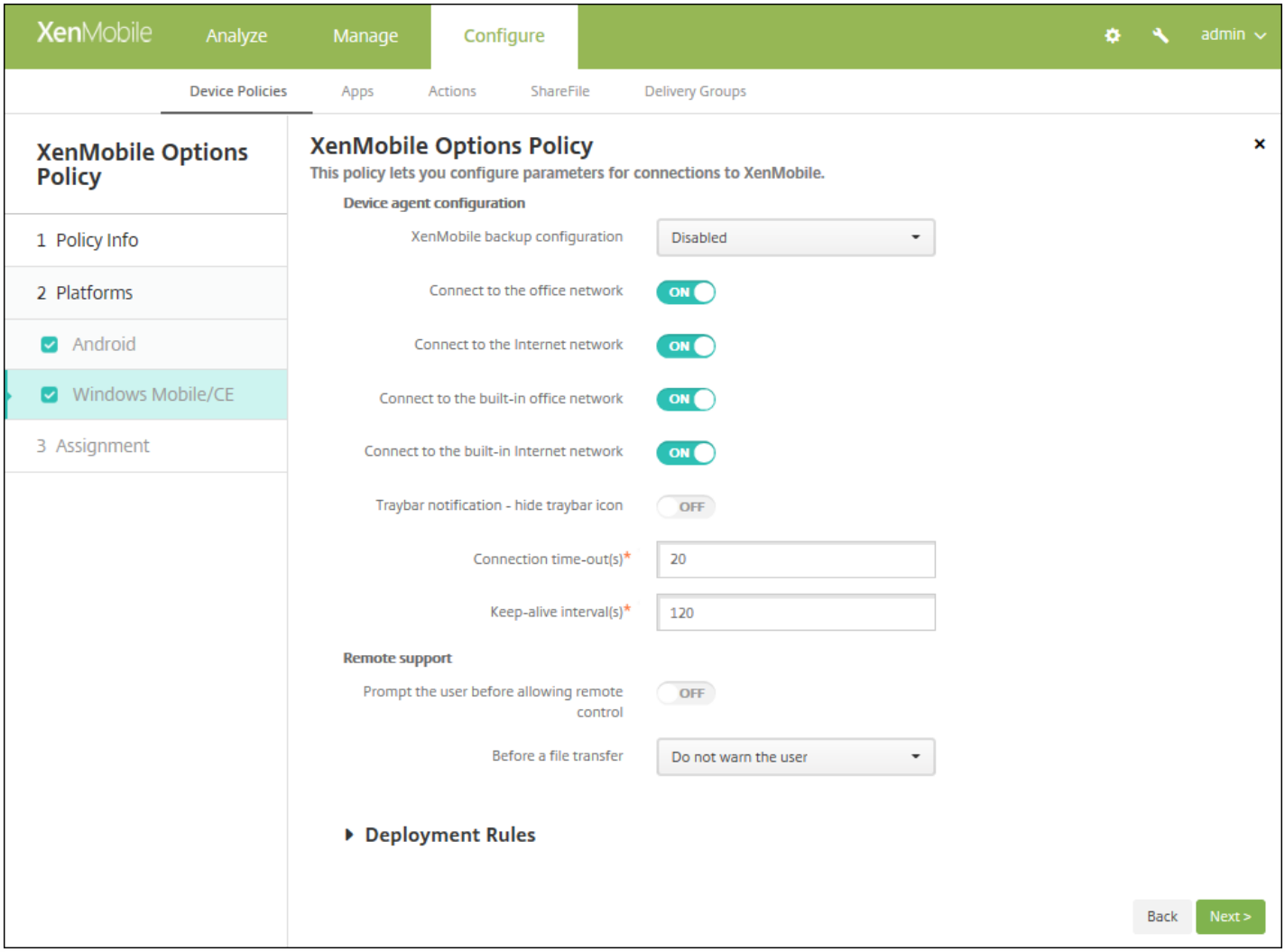
Androidの設定の構成



次の設定を構成します。

- **Traybar notification - hide traybar icon**：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［**OFF**］です。
- **Connection: time-out(s)**：接続のアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、接続はタイムアウトになります。 デフォルトは20秒です。
- **Keep-alive interval(s)**：接続を開いたままにする時間（秒）を入力します。 デフォルトは120秒です。
- **Prompt the user before allowing remote control**：リモートサポート制御を許可する前に、ユーザーに対するダイアログボックスを開くかどうかを選択します。 デフォルトは［**OFF**］です。
- **Before a file transfer**：一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。 使用可能な値は、［**Do not warn the user**］、［**Warn the user**］、および［**Ask for user permission**］です。 デフォルトは［**Do not warn the user**］です。

Windows Mobile/CEの設定の構成



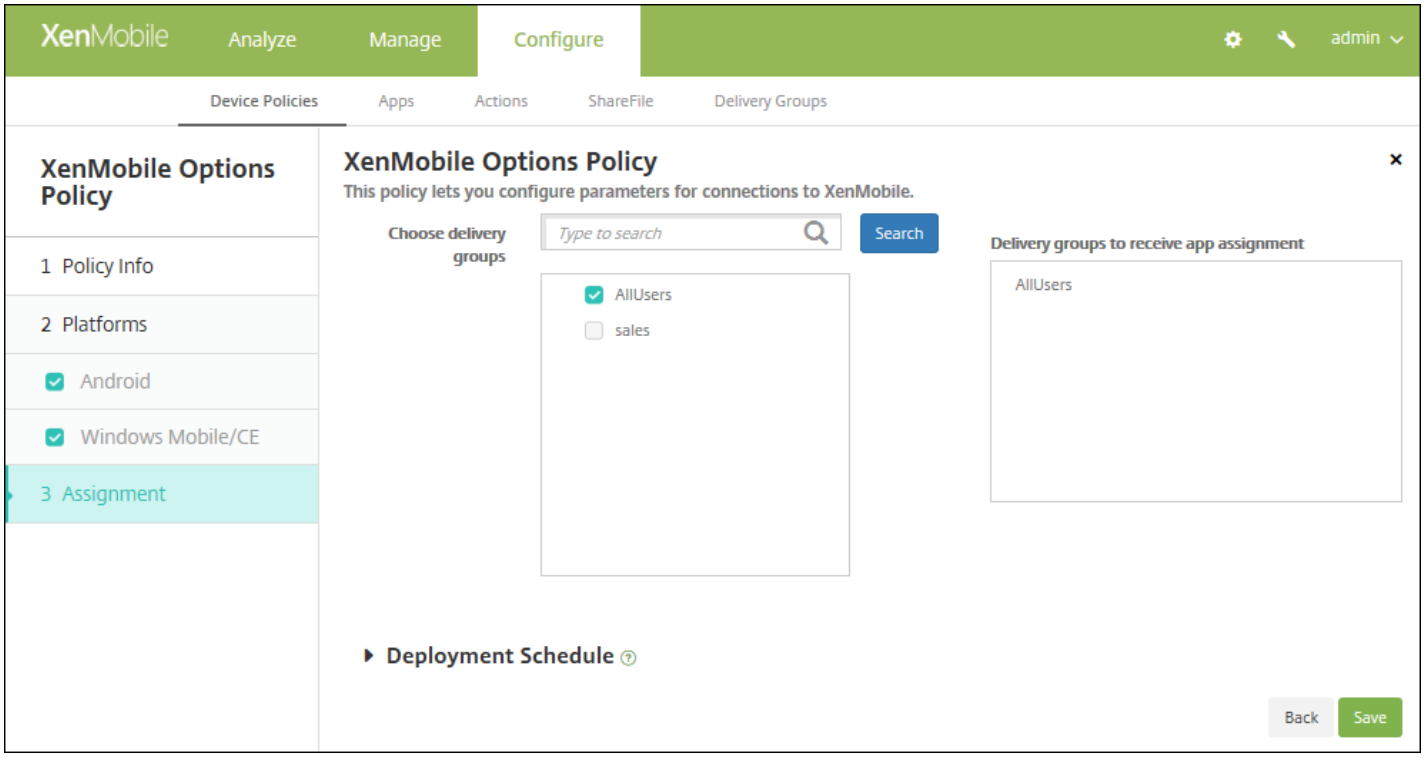
次の設定を構成します。

- **Device agent configuration**
  - **XenMobile backup configuration**：一覧から、ユーザーのデバイスにXenMobileの構成をバックアップするためのオプションを選択します。 デフォルトは［**Disabled**］です。 選択できるオプションは以下のとおりです。
    - Disabled
    - At first connection after XenMobile installation
    - At first connection after each device reboot
  - **Connect to the office network**
  - **Connect to the Internet network**
  - **Connect to the built-in office network**： ［**ON**］に設定した場合、XenMobileによりネットワークが自動的に検出されます。
  - **Connect to the built-in Internet network**： ［**ON**］に設定した場合、XenMobileによりネットワークが自動的に検出されます。
  - **Traybar notification - hide traybar icon**：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［**OFF**］です。
  - **Connection time-out(s)**：接続のアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、接続はタイムアウトになります。 デフォルトは20秒です。
  - **Keep-alive interval(s)**：接続を開いたままにする時間（秒）を入力します。 デフォルトは120秒です。

- **Remote support**
  - **Prompt the user before allowing remote control**：リモートサポート制御を許可する前に、ユーザーに対するダイアログボックスを開くかどうかを選択します。 デフォルトは［**OFF**］です。
  - **Before a file transfer**：一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。 使用可能な値は、［**Do not warn the user**］、［**Warn the user**］、および［**Ask for user permission**］です。 デフォルトは［**Do not warn the user**］です。

7. 展開規則を構成します。

8. ［**Next**］をクリックします。 ［**XenMobile Options Policy**］割り当てページが開きます。



9. ［**Choose delivery groups**］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

10. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［**OFF**］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。 デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

11. ［**Save**］をクリックします。

XenMobileアンインストールデバイスポリシー

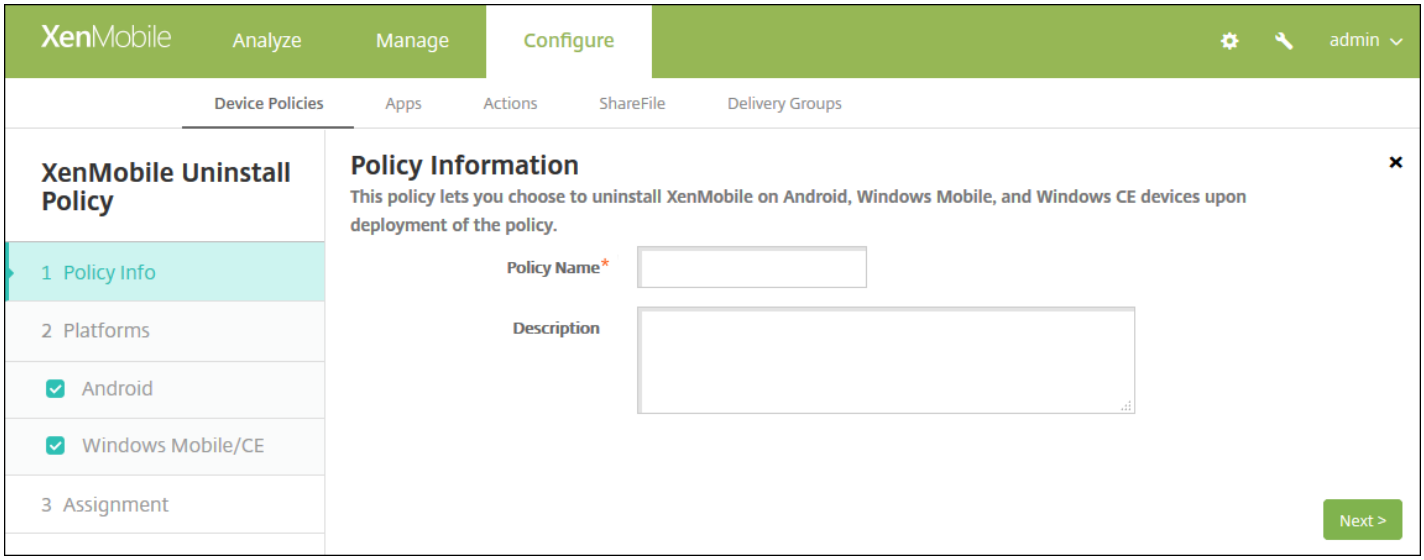
Aug 02, 2016

XenMobileでデバイスポリシーを追加して、XenMobileをAndroidデバイスおよびWindows Mobile/CEデバイスからアンインストールすることができます。 このポリシーを展開すると、展開グループ内のすべてのデバイスからXenMobileが削除されます。

1.XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。

3. **[More]** を展開した後、 **[XenMobile agent]** の下の **[XenMobile Uninstall]** をクリックします。 **[XenMobile Uninstall Policy]** ページが開きます。



4. **[Policy Information]** ペインで、以下の情報を入力します。

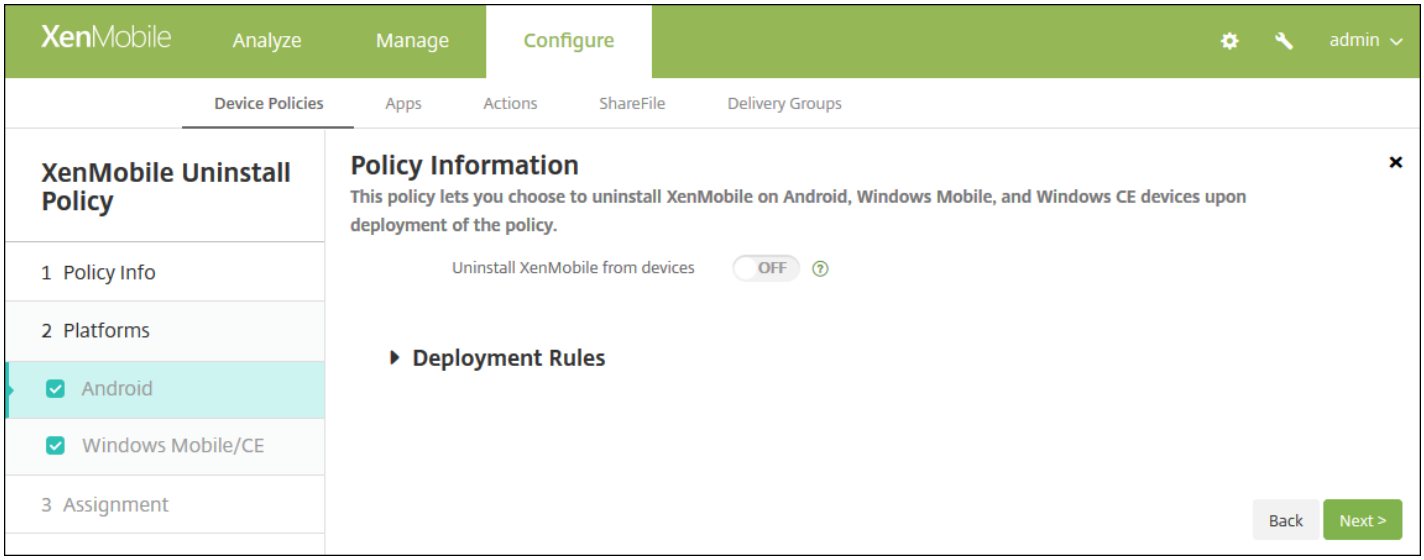
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。 **[Policy Platforms]** 情報ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

AndroidおよびWindows Mobile/CEの設定の構成

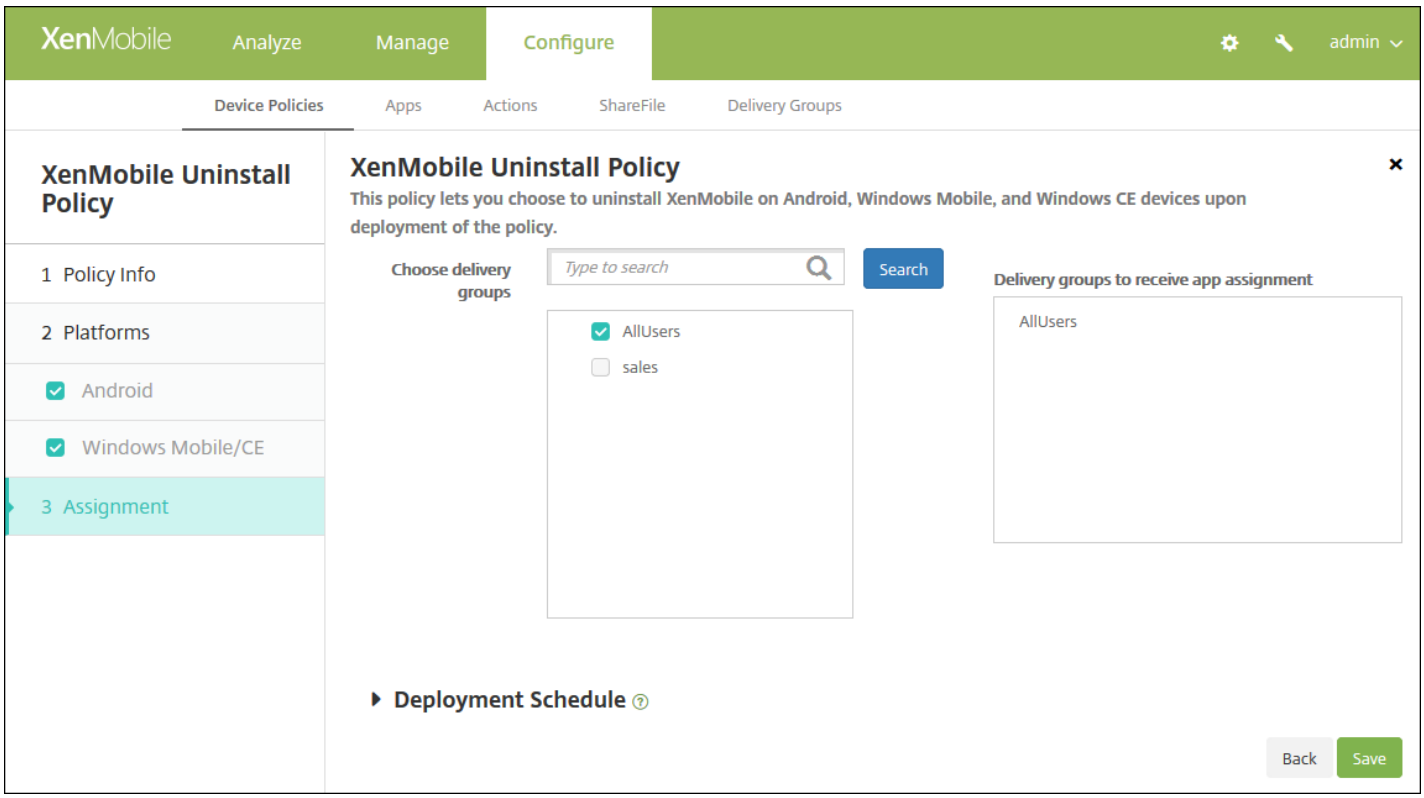


選択したプラットフォームごとに、次の設定を構成します。

- **Uninstall XenMobile from devices**：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 **[OFF]** です。

7. 展開規則の構成

8. **[Next]** をクリックします。 **[XenMobile Uninstall Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、 **[Settings]** > **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

XenMobileへのアプリケーションの追加

Aug 02, 2016

アプリケーションをXenMobileに追加して管理します。 アプリケーションはXenMobileコンソールに追加します。このコンソールでは、アプリケーションをカテゴリ別に分類し、ユーザーに展開することができます。

以下の種類のアプリケーションをXenMobileに追加できます。

- **MDX**。 MDX Toolkitでラップされたアプリケーション（および関連付けられたポリシー）です。 内部ストアおよび公開ストアから取得したMDXアプリケーションを展開します。 たとえば、WorxMailです。
- **パブリックアプリケーションストア**。 これらのアプリケーションには、iTunesやGoogle Playなどのパブリックアプリケーションストアで無料または有料で提供されているアプリケーションが含まれます。 たとえば、GoToMeetingです。 Android for Workのアプリケーションもこのカテゴリに分類されます。
- **WebおよびSaaS**。 これらのアプリケーションには、内部ネットワークからアクセスされるアプリケーション（Webアプリケーション）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ケーション（SaaS）が含まれます。 独自のアプリケーションを作成するか、一連のアプリケーションコネクタの中から選択して、既存のWebアプリケーションのシングルサインオン認証に使用することができます。 たとえば、GoogleApps_SAMLです。
- **エンタープライズ**。 これらのアプリケーションは、MDX Toolkitでラップされておらず、MDXアプリケーションに関連付けられたポリシーを含んでいない、ネイティブアプリケーションです。
- **Webリンク**。 パブリックサイトやプライベートサイト、またはシングルサインオンを必要としないWebアプリケーションのWebアドレス（URL）です。

> ## 注意
>
> iOSおよびSamsung Androidアプリのサイレントインストールがサポートされます。 サイレントインストールとは、ユーザーはデバイスに展開するアプリのインストールを求められず、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には、以下の前提条件を満たす必要があります。
>
> - iOSアプリの場合、管理されているiOSデバイスがSupervisedモードである必要があります。 詳しくは、 Āpple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。
> - Androidアプリの場合、Samsung for Enterprise（SAFE）またはKNOXポリシーがデバイスで有効になっている必要があります。 このためには、Samsung MDMライセンスキーデバイスポリシーを設定して、Samsung ELMおよびKNOXライセンスキーを生成します。 詳しくは、「Samsung MDMライセンスキーデバイスポリシー」を参照してください。

モバイルおよびMDXアプリケーションのしくみ

XenMobileでは、Worx Home、WorxMail、WorxWebなどのWorx Appsを含むiOS、Max OS X、Android、およびWindowsアプリケーションと、MDXポリシーの使用がサポートされます。 XenMobileコンソールを使用し、アプリケーションをアップロードしてユーザーデバイスに配信できます。 Worx Appsに加えて、次の種類のアプリケーションを追加できます。

- 自社開発のカスタムアプリケーション。
- MDXポリシーを使ってデバイスの機能を許可または制限するアプリケーション。

Citrixは、Citrixのロジックおよびポリシーでios、Max OS X、Android、およびWindowsデバイス用のアプリケーションをラップするためのMDX Toolkitを提供しています。 このツールは、組織内で作成されたアプリケーションまたは社外で作成されたアプリケーションに安全に対処できます。

WebおよびSaaSアプリケーションのしくみ

XenMobileには、一連のアプリケーションコネクタが用意されています。これらは、WebアプリケーションおよびSaaS（Software as a Service：サービスとしてのソフトウェア）アプリケーションのSSO（Single Sign-On：シングルサインオン）を構成するためのテンプレートで、ユーザーアカウントを作成したり管理したりすることもできます。 XenMobileには、Security Assertion Markup Language（SAML）コネクタが含まれています。 SAMLコネクタは、SSOおよびユーザーアカウント管理用のSAMLプロトコルをサポートするWebアプリケーションで使用されます。 XenMobileは、SAML 1.1およびSAML 2.0をサポートします。

また、独自のエンタープライズSAMLコネクタを構築することもできます。

エンタープライズアプリケーションのしくみ

XenMobileでは、独自のアプリケーションコネクタを作成したり、Android for Workアプリケーションをアップロードしたりできます。 この種のアプリケーションは、通常は内部ネットワークに存在します。 ユーザーはWorx Homeを使ってそのアプリケーションに接続できます。 エンタープライズアプリケーションを追加する場合は、アプリケーションコネクタを同時に作成します。

パブリックアプリケーションストアのしくみ

Apple App Store、Google Play、およびWindows Storeからアプリケーションの名前と説明を取得するための設定を構成できます。 ストアからアプリケーション情報を取得すると、XenMobileにより既存の名前と説明が上書きされます。

Webリンクのしくみ

Webリンクはインターネットサイトまたはイントラネットサイトの Webアドレスです。 Webリンクは、SSOを必要としないWebアプリケーションも参照できます。 Webリンクの構成が完了すると、リンクはWorx Storeにアイコンとして表示されます。 ユーザーがWorx Homeを使ってログオンすると、リンクは使用可能なアプリケーションおよびデスクトップの一覧と共に表示されます。

コンソールを使用してアプリケーションを追加するには、次の手順に従います。

- アプリケーションに関する情報の追加
- iOSやAndroidなどの各サポート対象プラットフォーム向けアプリケーションの選択および構成
- オプションの承認方法の定義
- オプションのデリバリーグループ割り当ての設定

1. XenMobileコンソールで、**[Configure]** の **[Apps]** をクリックします。 **[Apps]** ページが開きます。

注：XenMobileコンソールに初めて接続した場合、**[Apps]** の表は空白になっています。使用できるオプションは **[Add]** と **[Category]** のみです。

2. **[Add]** をクリックし、追加する種類に関する、以下の記事の手順に従います。

- XenMobileへのMDXアプリケーションの追加
- XenMobileへのパブリックアプリケーションストアのアプリケーションの追加
- XenMobileへのWebおよびSaaSアプリケーションの追加
- XenMobileへのエンタープライズアプリケーションの追加
- XenMobileへのWebリンクアプリケーションの追加

アプリケーションを追加すると、**[Apps]** ページの表にアプリケーションが表示されます。このページで、アプリケーションの編集や分類をいつでも行うことができます。

注意

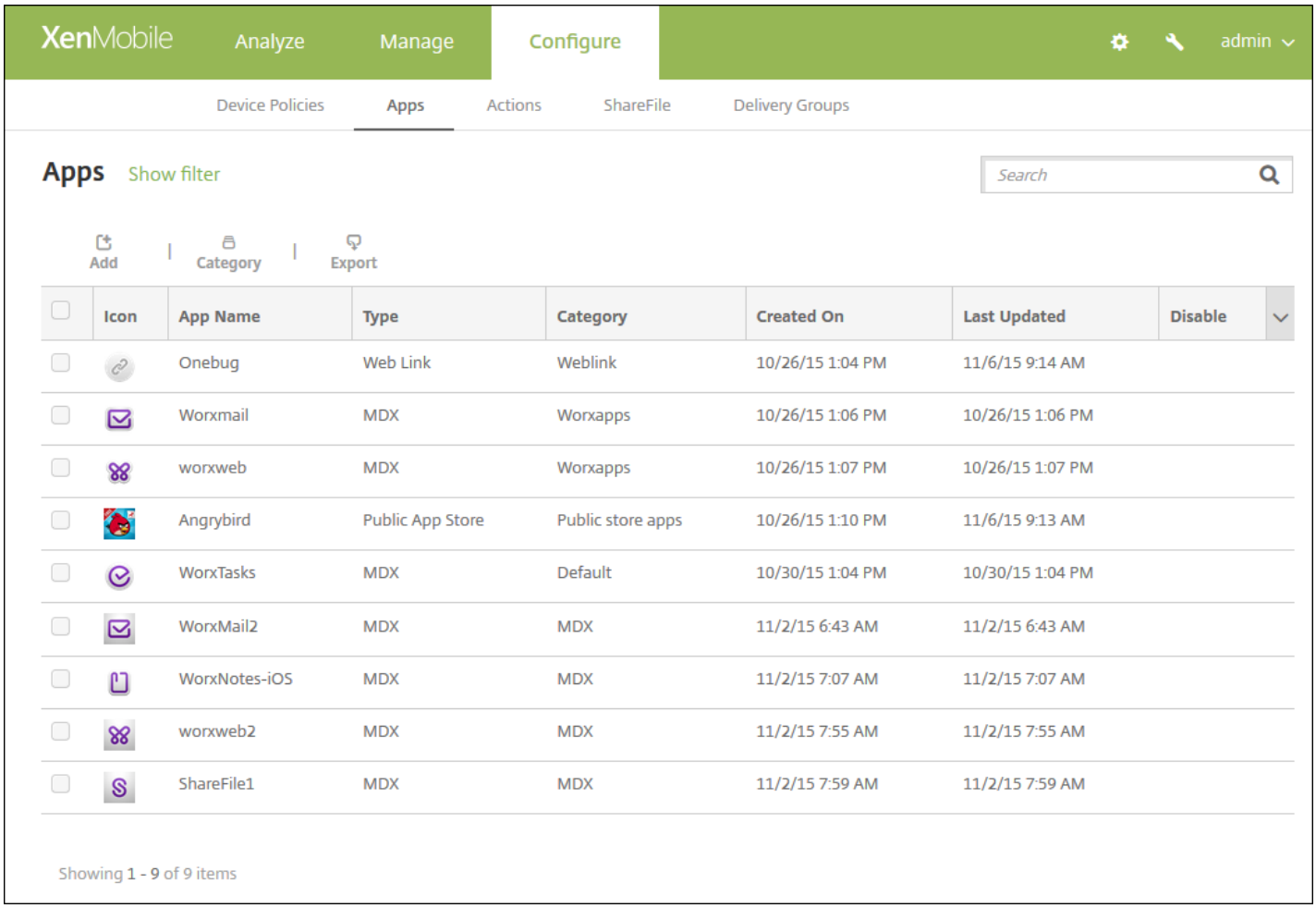
XenMobile 10.3にアップグレードした後、XenMobile 10.3で以前のリリースで構成したWorxモバイルアプリを更新すると、アプリの設定内容がXenMobileコンソールに表示されなくなります。 これらのアプリで設定を再度編集、構成する必要があります。 アプリを再インストールする必要はありません。 この手順が必要なのは一度だけです。将来アプリやサーバーを更新しても、この値はそのまま保持されます。

XenMobileへのMDXアプリケーションの追加

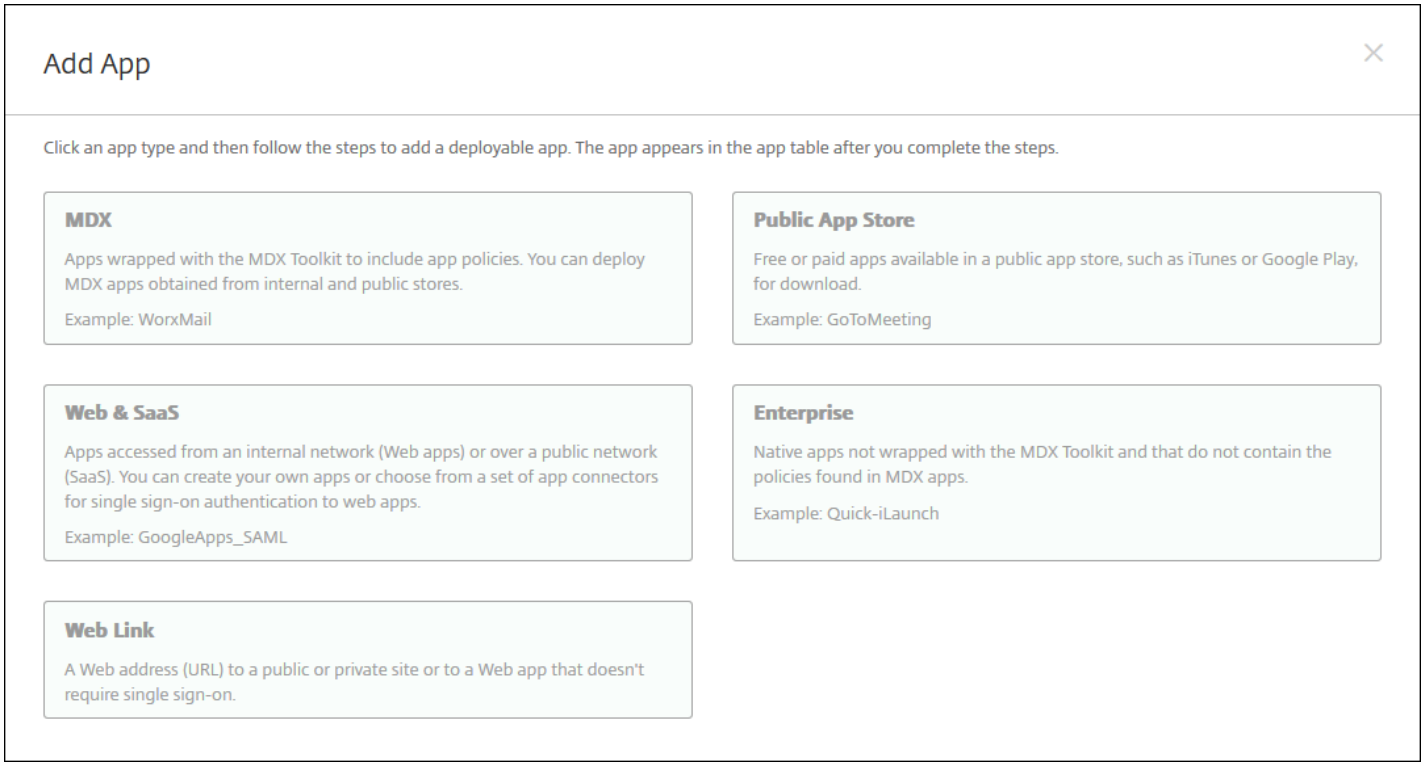
Aug 02, 2016

iOS、Android、またはWindows Phoneデバイス用のラップされたMDXモバイルアプリケーションを取得したら、そのアプリケーションをXenMobileにアップロードできます。 アプリケーションをアップロードした後、アプリケーションの詳細とポリシー設定を構成できます。 各デバイスプラットフォームの種類で使用できるアプリケーションポリシーについて詳しくは、「iOS、Android、およびWindows Phone用のMDXポリシーの概要」と、 このセクションのポリシーに関する詳細な説明を参照してください。

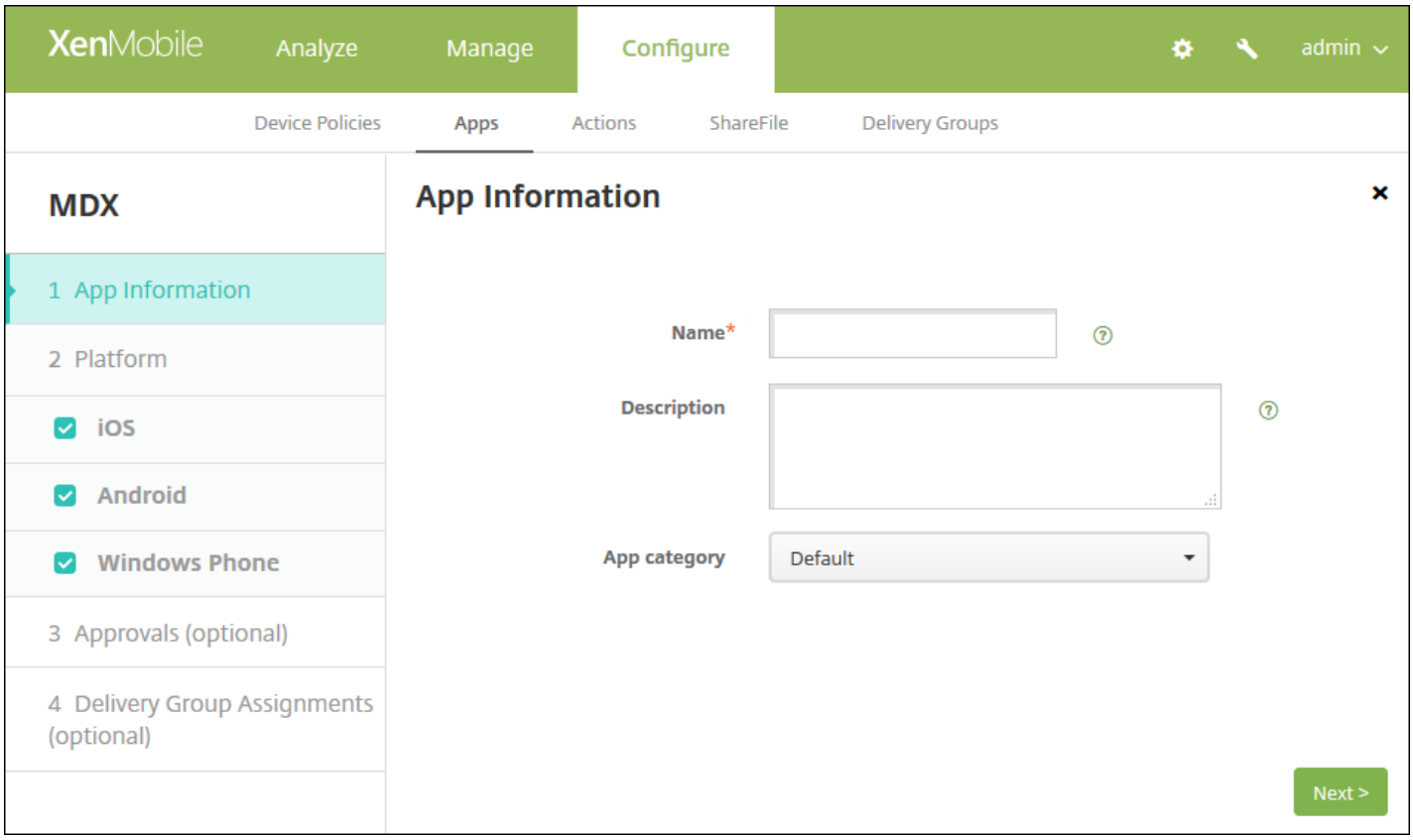
1. XenMobileコンソールで、 **[構成] > [アプリ]** をクリックすると、 **[アプリ]** ページが表示されます。



2. **[Add]** をクリックします。 **[Add App]** ダイアログボックスが開きます。



3. [**MDX**] をクリックします。 [**MDX App Information**] ページが開きます。



4. [**アプリケーション情報**] ペインで、以下の情報を入力します。

- **Name**：アプリケーションの説明的な名前を入力します。 この情報は、［**Apps**］の表の［**App Name**］の下に表示されます。
- **Description**：任意で、アプリケーションの説明を入力します。
- **App category**：任意で、一覧から、アプリケーションを追加するカテゴリを選択します。 アプリケーションカテゴリについて詳しくは、「XenMobileでのアプリケーションカテゴリの作成」を参照してください。

5. ［**Next**］をクリックします。 ［**App Platforms**］ページが開きます。

6. ［**Platforms**］の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順11.を参照してプラットフォームの展開規則を設定します。

7. S ［**アップロード**］ をクリックしてアップロードする.mdxファイルの場所へ移動し、そのファイルを選択します。

- iOS VPP B2Bアプリケーションを追加する場合は、［**Your application is a VPP B2B application?**］をクリックして、一覧から使用するB2B VPPアカウントを選択します。

8. ［**Next**］をクリックします。 アプリケーション詳細ページが開きます。

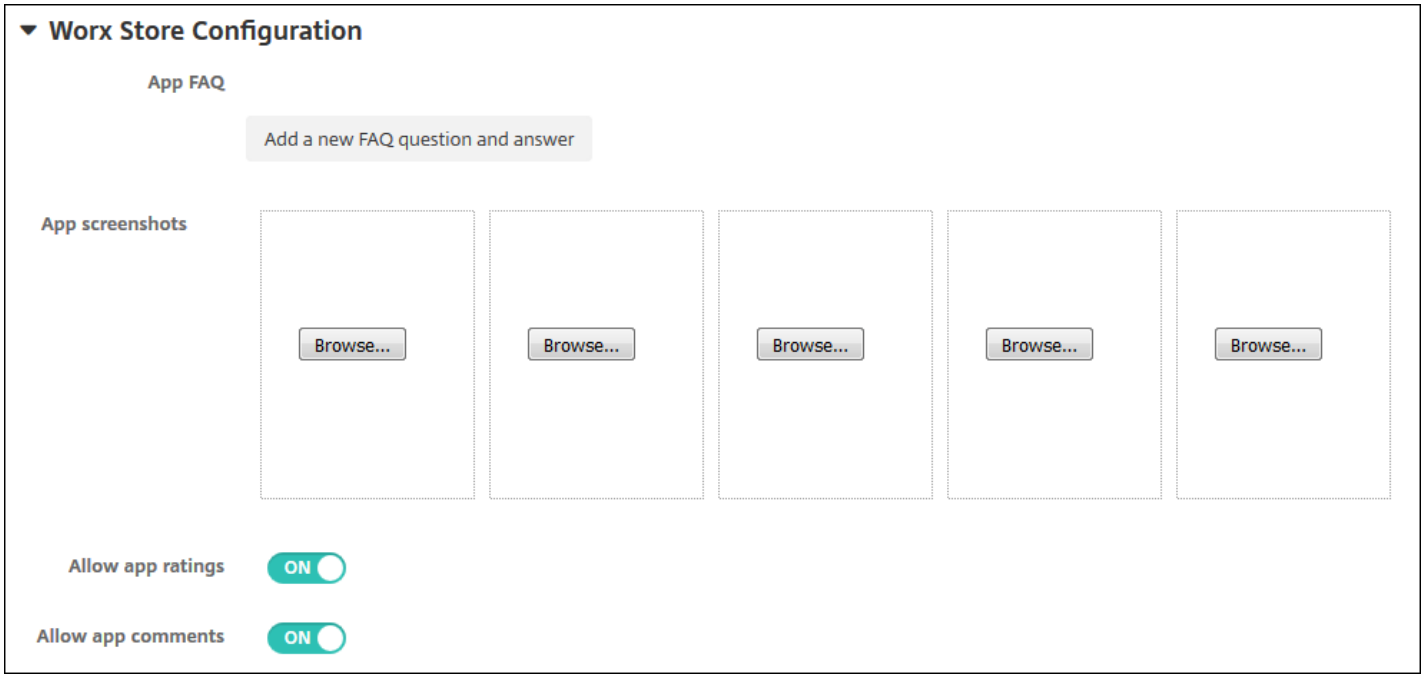
9. 次の設定を構成します。

- **File name**：アプリケーションに関連付けられているファイル名を入力します。
- **App Description**：アプリケーションの説明を入力します。
- **App version**：任意で、アプリケーションのバージョン番号を入力します。
- **Minimum OS version**：任意で、アプリケーションを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
- **Maximum OS version**：任意で、アプリケーションを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
- **Excluded devices**：任意で、アプリケーション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。
- **Remove app if MDM profile is removed**：MDMプロファイルが削除された場合にデバイスからアプリケーションを削除するかどうかを選択します。 デフォルトは［**ON**］です。
- **Prevent app data backup**：ユーザーがアプリケーションデータをバックアップできないようにするかどうかを選択します。 デフォルトは［**ON**］です。
- **Force app to be managed**：アプリケーションが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリケーションの管理を許可するように求めるかどうかを選択します。 デフォルトは［**ON**］です。 iOS 9.0以降で使用できます。

10. **MDXポリシー**を構成します。 MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、ネットワーク要件、その他アクセス、暗号化、アプリケーション相互作用、アプリケーション制限、アプリケーションネットワークアクセス、アプリケーションログ、アプリケーションジオフェンスなどのポリシー領域で適用するオプションが含まれます。 XenMobileコンソールでは、ポリシーごとに、ポリシーを説明するヒントが提供されます。 ポリシーが適用されるプラットフォームの種類を示す表など、MDXアプリケーションのアプリケーションポリシーについて詳しくは、「iOS、Android、およびWindows Phone用のMDXポリシーの概要」を参照してください。

11. 展開規則の構成

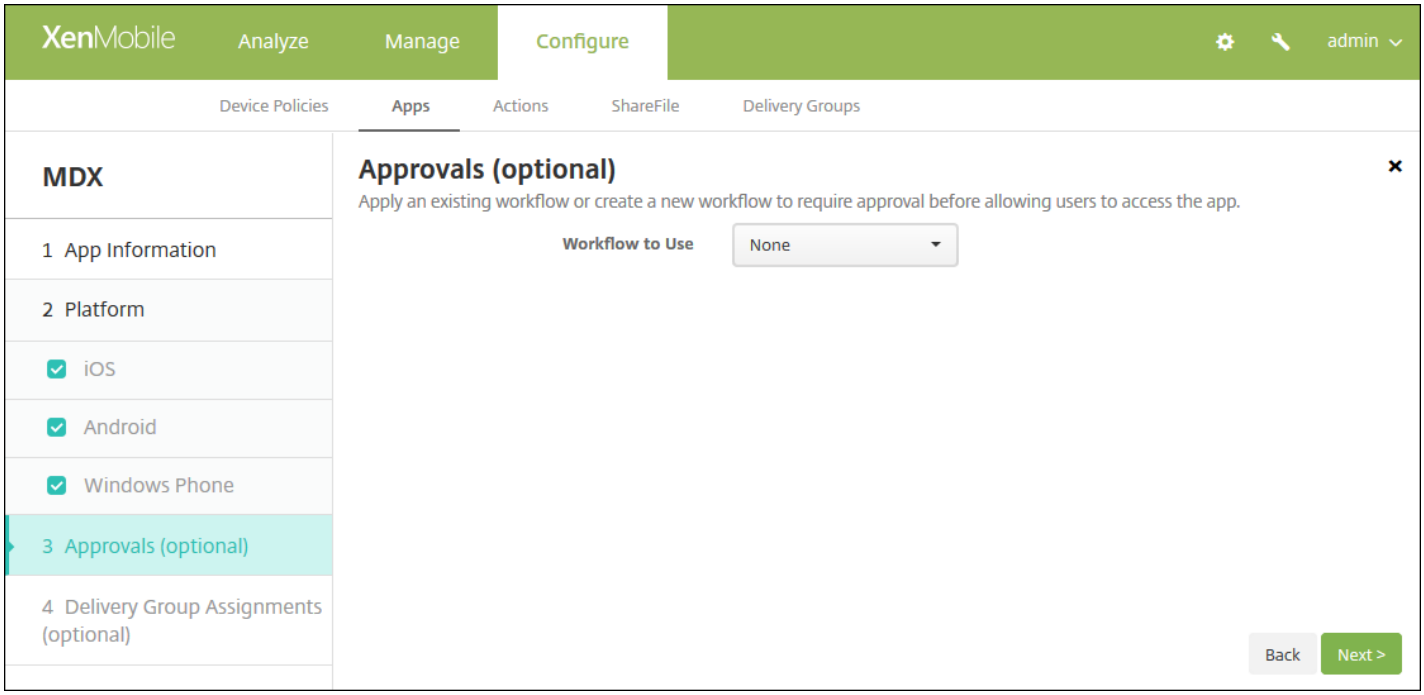
12. ［**Worx Store Configuration**］を展開します。



任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは**[ON]** です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。 デフォルトは **[ON]** です。

13. **[Next]** をクリックします。 **[Approvals]** ページが開きます。



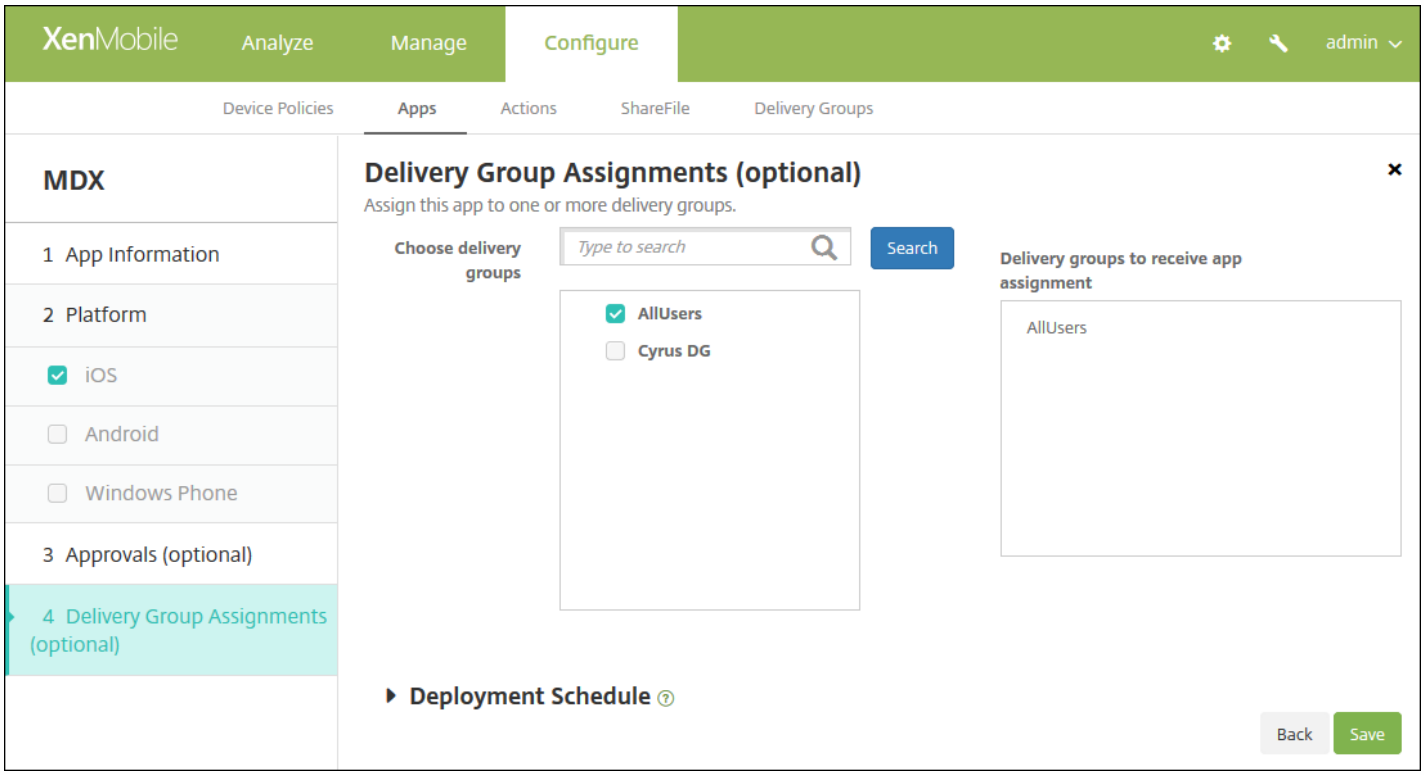
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。 承認ワークフローを設定する必要がない場合は、手順15に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use**：一覧から既存のワークフローを選択するか、［**Create a new workflow**］をクリックします。 デフォルトは［**None**］です。
- ［**Create a new workflow**］を選択した場合は、次の設定を構成します。
  - **Name**：ワークフローの固有の名前を入力します。
  - **Description**：任意で、ワークフローの説明を入力します。
  - **Email Approval Templates**：一覧から、割り当てる電子メール承認テンプレートを選択します。 このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。 デフォルトは［1 level］です。 選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers**：検索フィールドに、追加で必要なユーザーの名前を入力して、［**Search**］をクリックします。 名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが［**Selected additional required approvers**］の一覧に表示されます。
    - ［**Selected additional required approvers**］の一覧からユーザーを削除するには、次のいずれかを行います。
      - ［**Search**］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して［**Search**］をクリックし、検索結果を絞り込みます。
      - ［**Selected additional required approvers**］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにし

ます。

14. [**Next**] をクリックします。 [**Delivery Group Assignment**] ページが開きます。



15. [**Choose delivery groups**] の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

16. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

17. [**Save**] をクリックします。

XenMobileでのアプリケーションカテゴリの作成

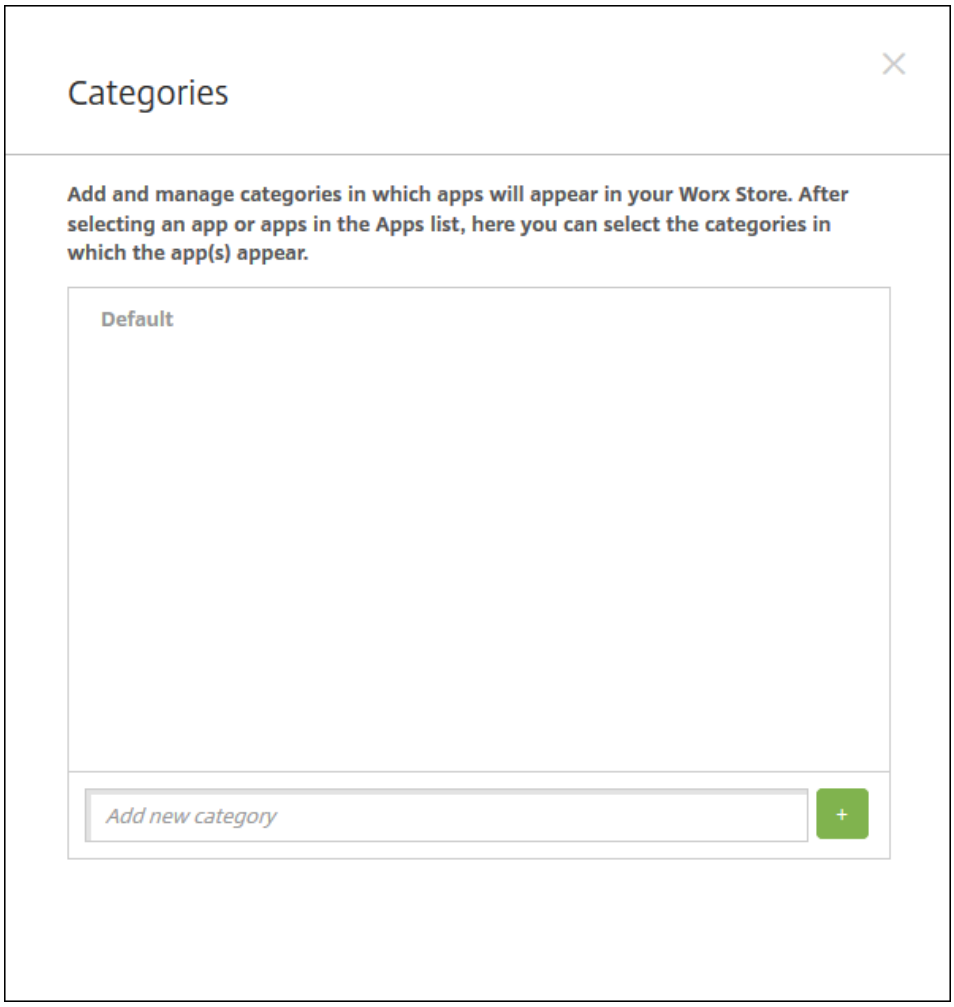
Aug 02, 2016

ユーザーがWorx Homeにログオンすると、XenMobileで追加および設定したアプリケーション、Webリンク、ストアの一覧が表示されます。 管理者がアプリケーションカテゴリを使用することにより、ユーザーは指定されたアプリケーション、ストア、またはWebリンクだけにアクセスできます。 たとえば、「Finance」カテゴリを作成して財務関連のアプリケーションを追加したり、 「Sales」カテゴリを構成して営業関連のアプリケーションを追加したりすることができます。

XenMobileコンソールの［**Apps**］ページで、カテゴリを構成します。 次に、アプリケーション、Webリンク、ストアを追加または編集するとき、構成した1つまたは複数のカテゴリにアプリケーションを追加できます。

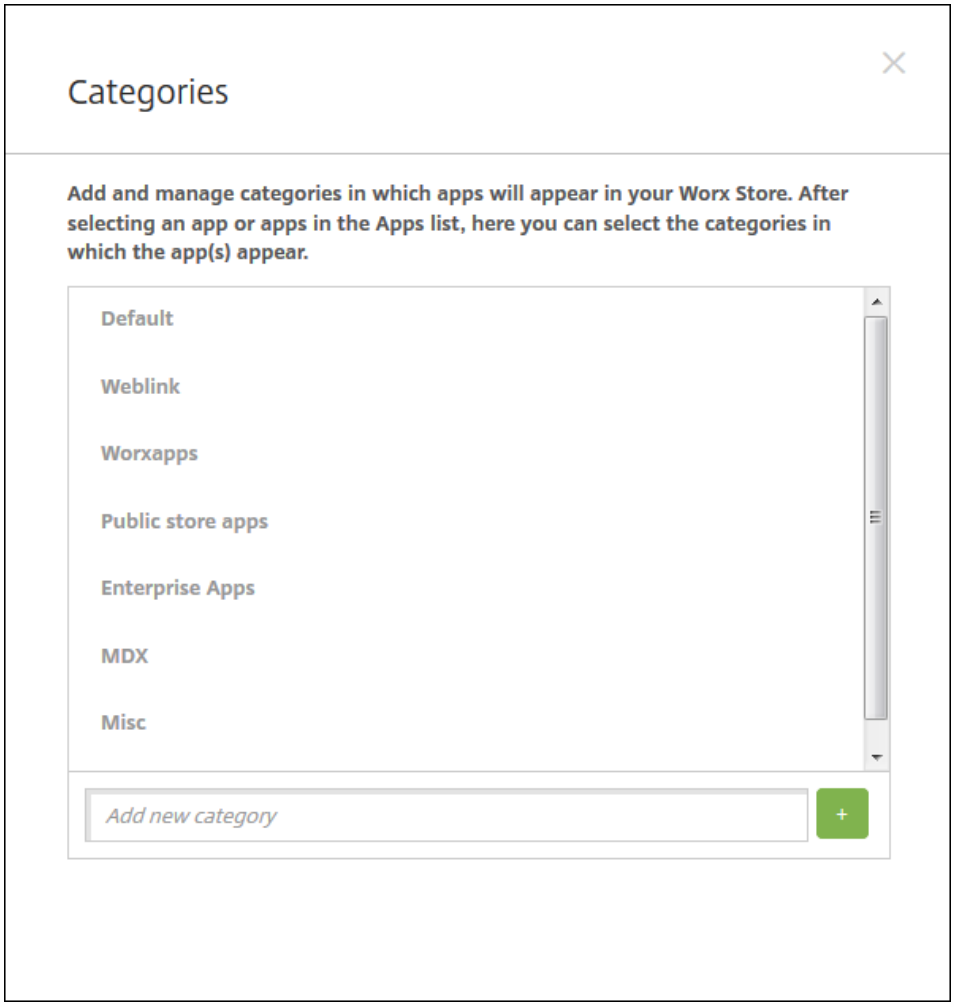
1. XenMobileコンソールで、［**Configure**］の［**Apps**］をクリックします。 ［**Apps**］ページが開きます。

2. ［**Category**］をクリックします。 ［**Categories**］ダイアログボックスが開きます。



3. 追加するカテゴリごとに、以下の操作を行います。

- ダイアログボックス下部にある［**Add a new category**］フィールドに、追加するカテゴリの名前を入力します。 たとえば、「*Enterprise Apps*」と入力して、エンタープライズアプリケーションのカテゴリを作成することができます。
- プラス記号（+）をクリックしてカテゴリを追加します。 新しく作成したカテゴリが追加され、［**Categories**］ダイアログボックスに表示されます。



4. カテゴリの追加が終了したら、［**Categories**］ダイアログボックスを閉じます。

5. ［**Apps**］ページで、既存のアプリケーションを新しいカテゴリに分類できます。

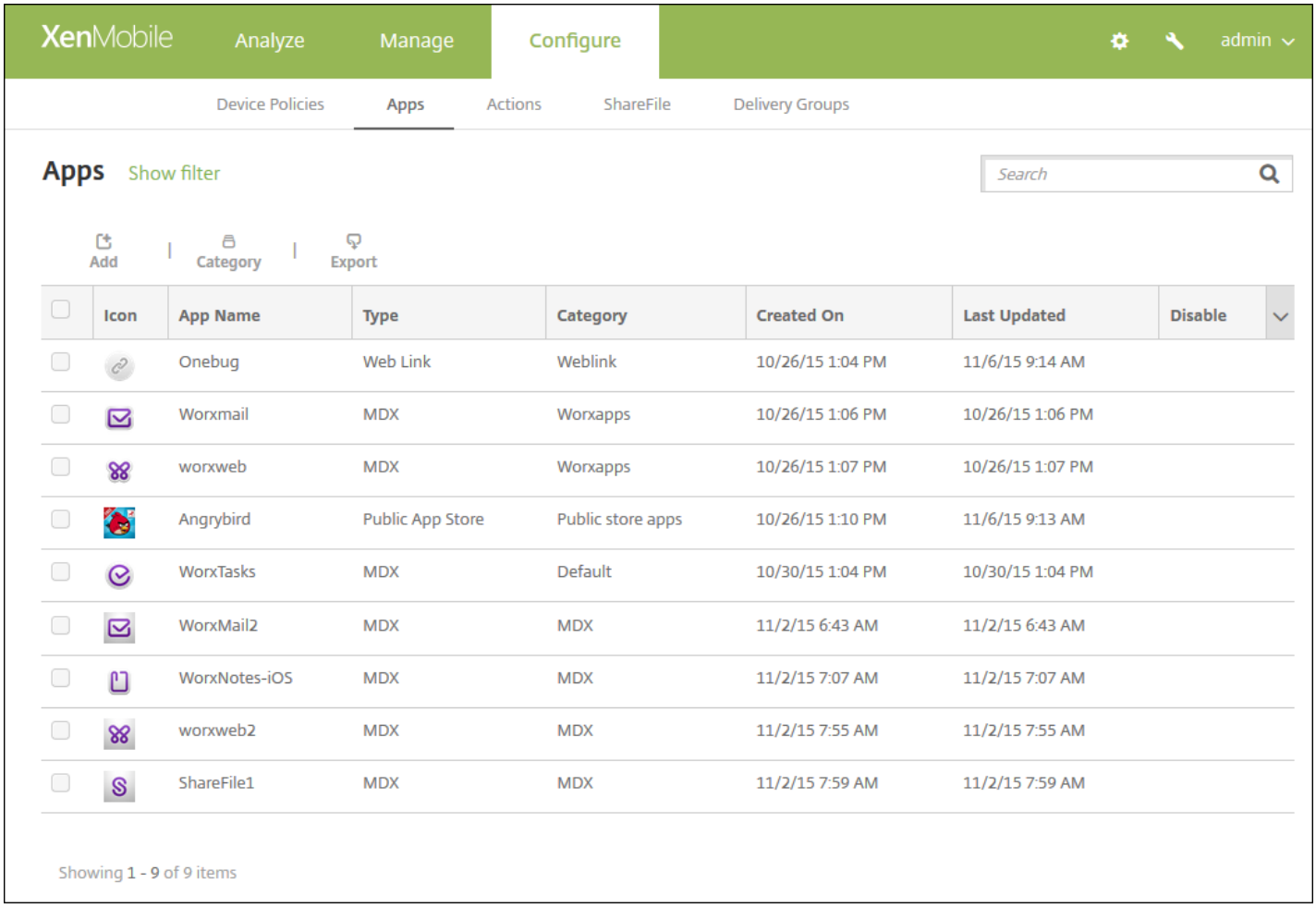
- 分類するアプリケーションを選択します。
- ［**Edit**］をクリックします。［**App Information**］ページが開きます。
- ［**App category**］の一覧で、新しいカテゴリのチェックボックスをオンにしてカテゴリを適用します。既存のカテゴリ アプリケーションに適用しないものについては、チェックボックスをオフにします。
- ［**Delivery Groups Assignments**］タブをクリックするか、後続の各ページで［**Next**］をクリックして、残りのアプリケーションセットアップページに示される手順に従います。
- ［**Delivery Groups Assignments**］のページの［**Save**］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 アプリケーションに適用され、［**Apps**］の表に表示されます。

XenMobileへのパブリックアプリケーションストアのアプリケーションの追加

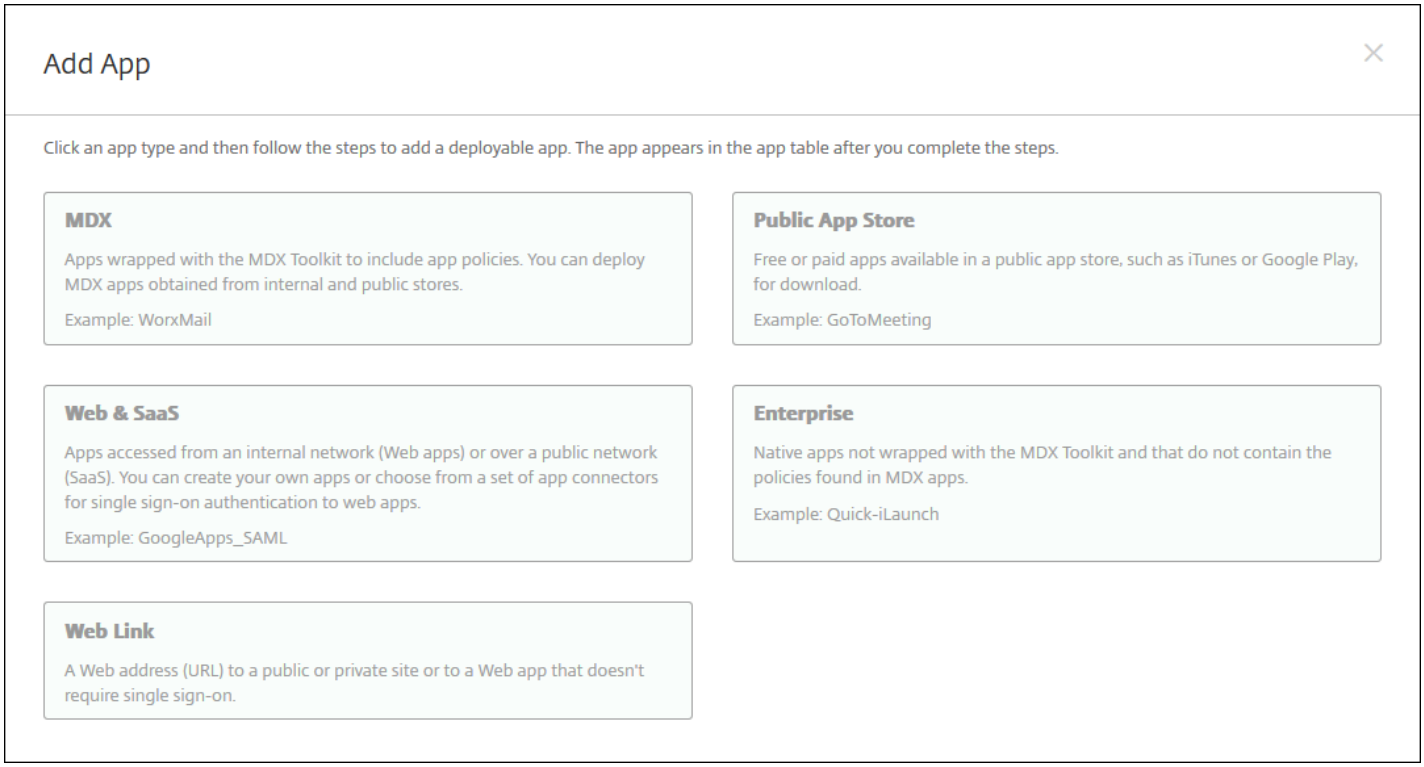
Oct 25, 2016

iTunesやGooglePlayなどのパブリックアプリケーションストアで入手できる無料または有料のアプリケーションをXenMobil
に追加できます。 たとえば、GoToMeetingです。 Android for Work用にパブリックアプリケーションストアの有料アプリを
追加するときに、一括購入ライセンスの状態（使用できるライセンス数の合計、現在使用中のライセンス数、ライセンスを
用している各ユーザーのメールアドレス）を確認できます。 Android for Workの一括購入プランを利用すると、組織のアプ
やその他のデータの検索、購入、配布の処理が簡単になります。

1. XenMobileコンソールで、 **[Configure]** の **[Apps]** をクリックします。 **[Apps]** ページが開きます。



2. **[Add]** をクリックします。 **[Add App]** ダイアログボックスが開きます。



3. **[Public App Store]** をクリックします。 **[App Information]** ページが開きます。

4. **[App Information]** ペインで、以下の情報を入力します。

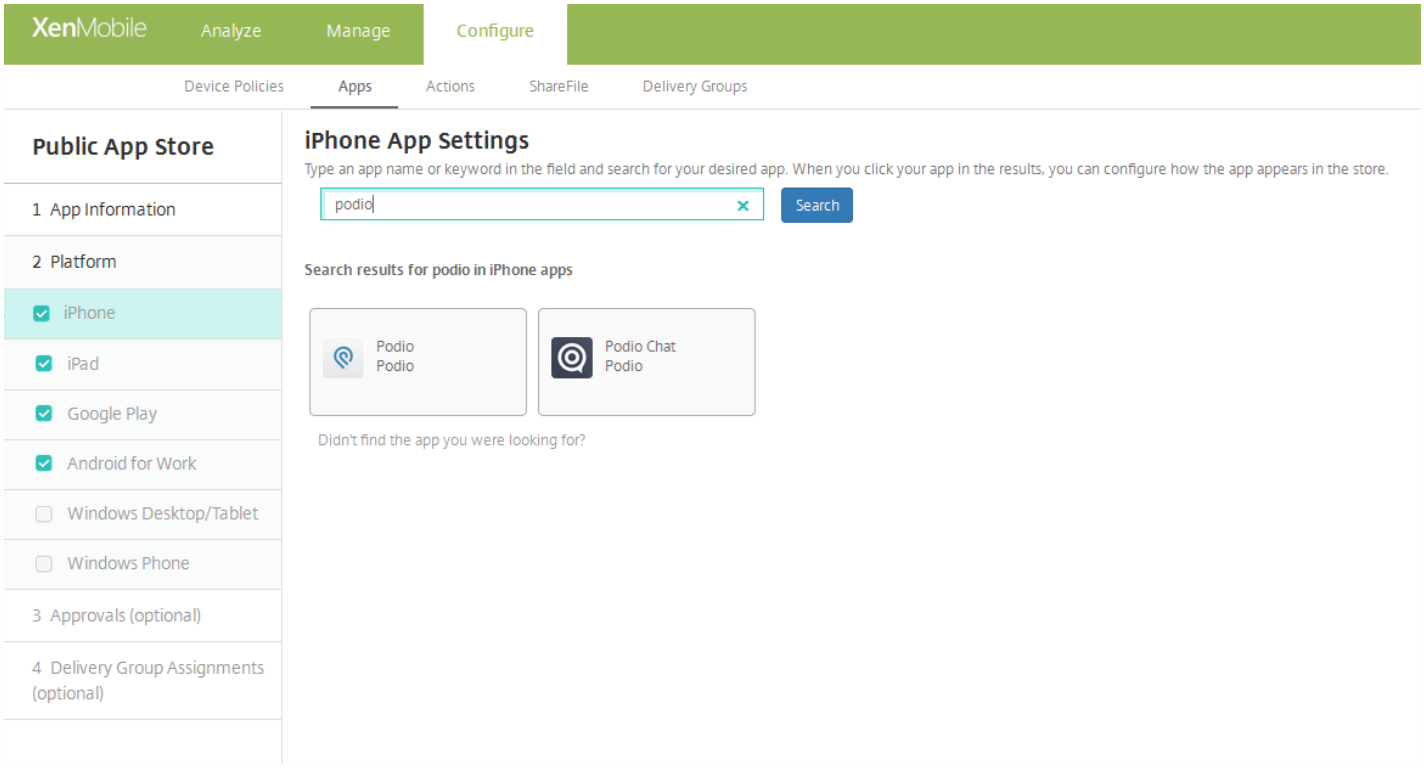
- **Name**：アプリケーションの説明的な名前を入力します。 この情報は、［Apps］の表の［App Name］の下に表示されます。
- **Description**：任意で、アプリケーションの説明を入力します。
- **App category**：任意で、一覧から、アプリケーションを追加するカテゴリを選択します。 アプリケーションカテゴリについて詳しくは、「XenMobileでのアプリケーションカテゴリの作成」を参照してください。

5. **[Next]** をクリックします。 **[App Platforms]** ページが開きます。

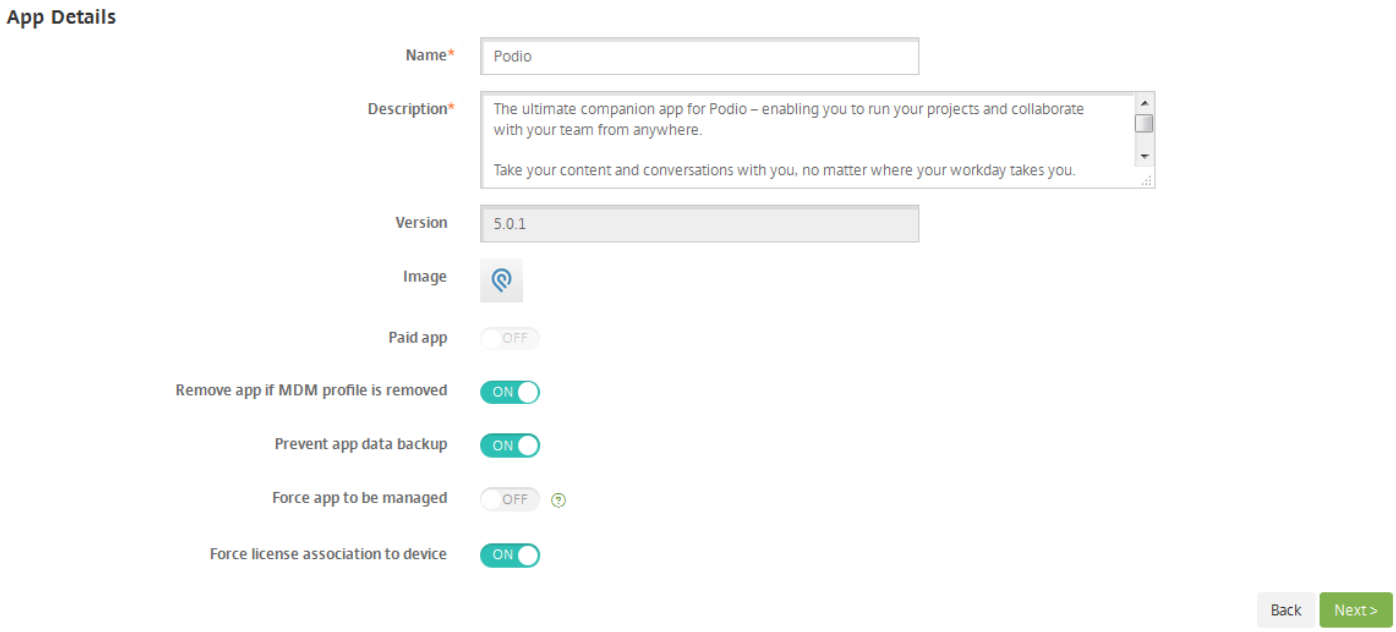
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10.を参照してプラットフォームの展開規則を設定します。

7. 追加するアプリケーションの名前を検索ボックスに入力し、**[Search]** をクリックして、アプリケーションを選択します。 検索条件に一致するアプリケーションが表示されます。 次の図は、「*podio*」の検索結果を示しています。



8. 追加するアプリケーションをクリックします。 **[App Details]** フィールドには、選択したアプリケーションに関連する情報（名前、説明、バージョン番号、関連付けられたイメージなど）が事前に設定されています。



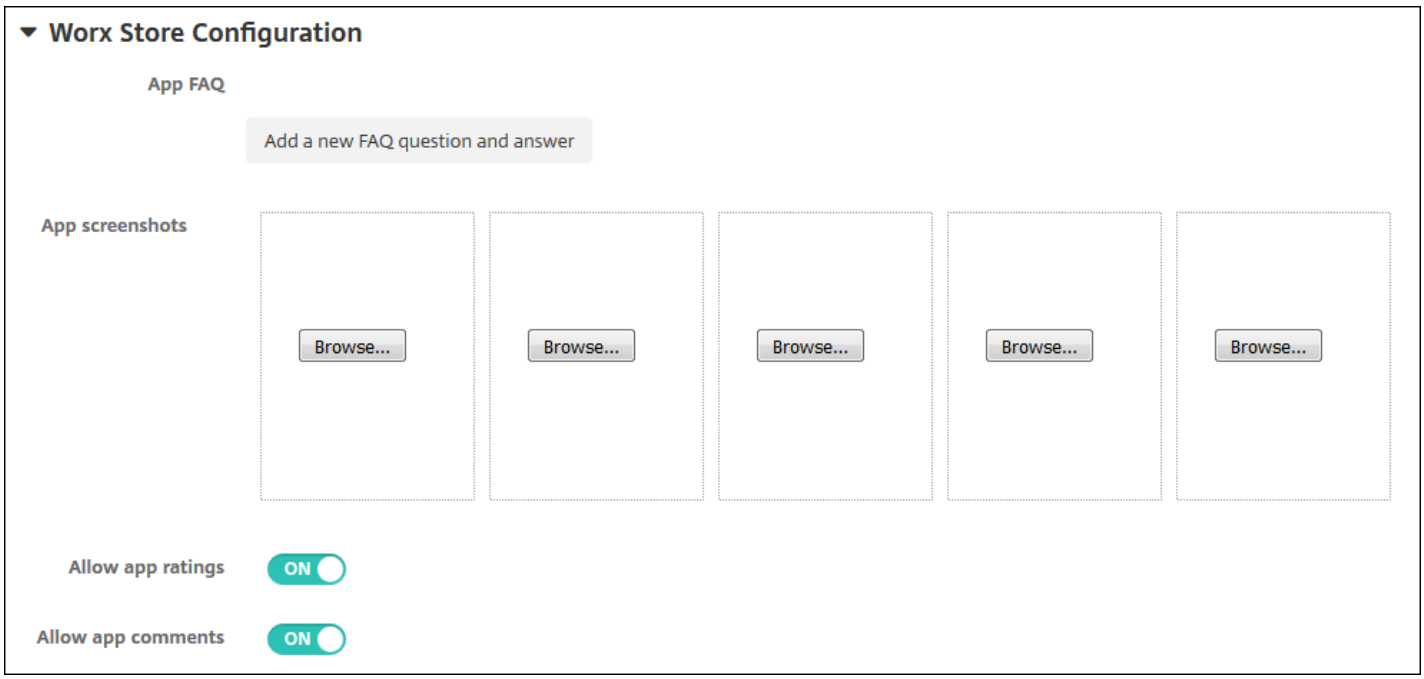
9. 次の設定を構成します。

- 必要に応じて、アプリケーションの名前と説明を変更します。
- **Paid app**：このフィールドは事前に構成されており、変更できません。

- **Remove app if MDM profile is removed**：MDMプロファイルが削除された場合にアプリケーションを削除するかどうかを選択します。 デフォルトは［**ON**］です。
- **Prevent app data backup**：アプリケーションのデータをバックアップできないようにするかどうかを選択します。 デフォルトは［**ON**］です。
- **Force app to be managed**：アプリケーションが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリケーションの管理を許可するように求めるかどうかを選択します。 デフォルトは［**OFF**］です。 iOS 9.0以降で使用できます。
- **Force license to association to device**：デバイスの関連付けを有効にして開発されたアプリケーションを、ユーザーではなくデバイスに関連付けるかどうかを選択します。 iOS 9以降で利用できます。 選択したアプリケーション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。

10. 展開規則の構成

11. ［**Worx Store Configuration**］を展開します。

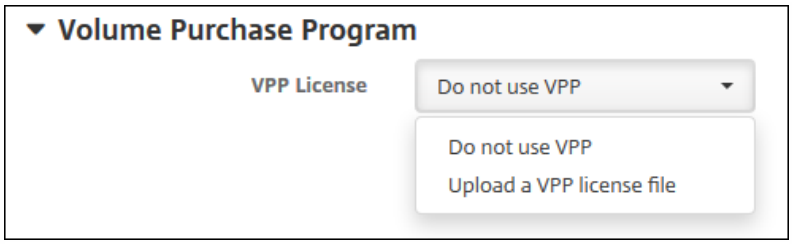


任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは［ON］です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。

12. ［**Volume Purchase Program**］を展開するか、Android for Workの場合は［**Bulk Purchase**］を展開します。

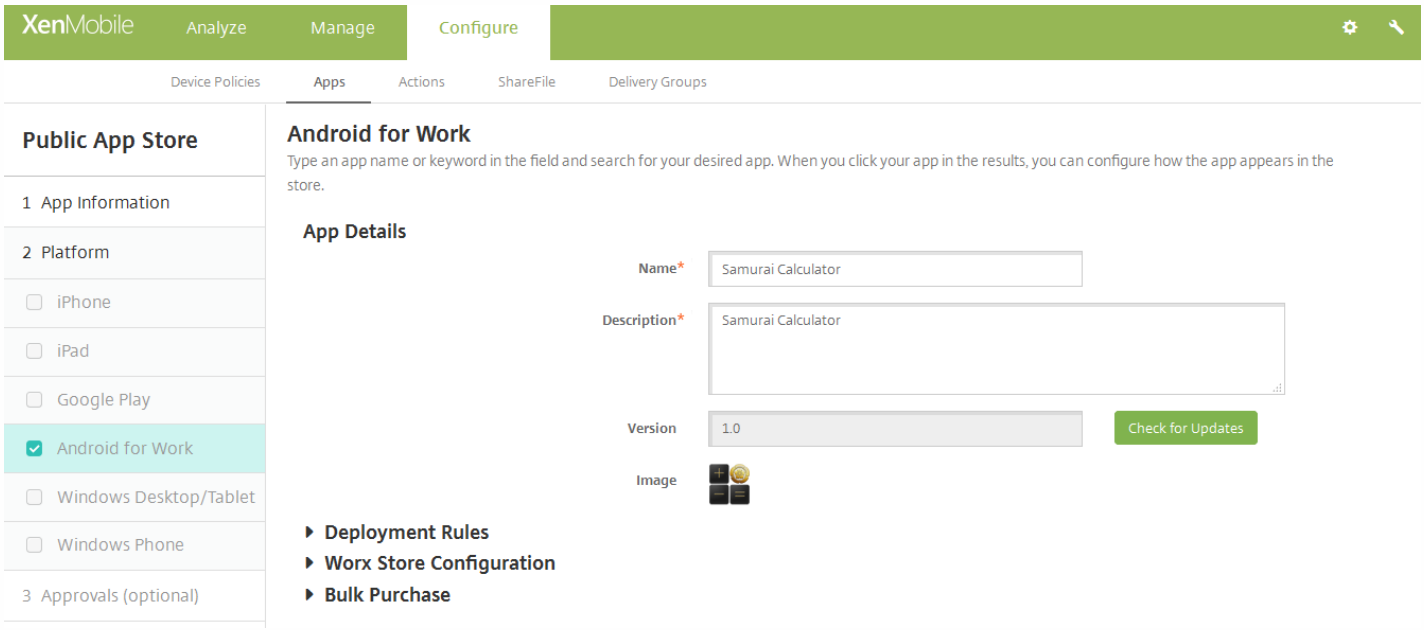
このVolume Purchase Programについて、次の手順に従います。



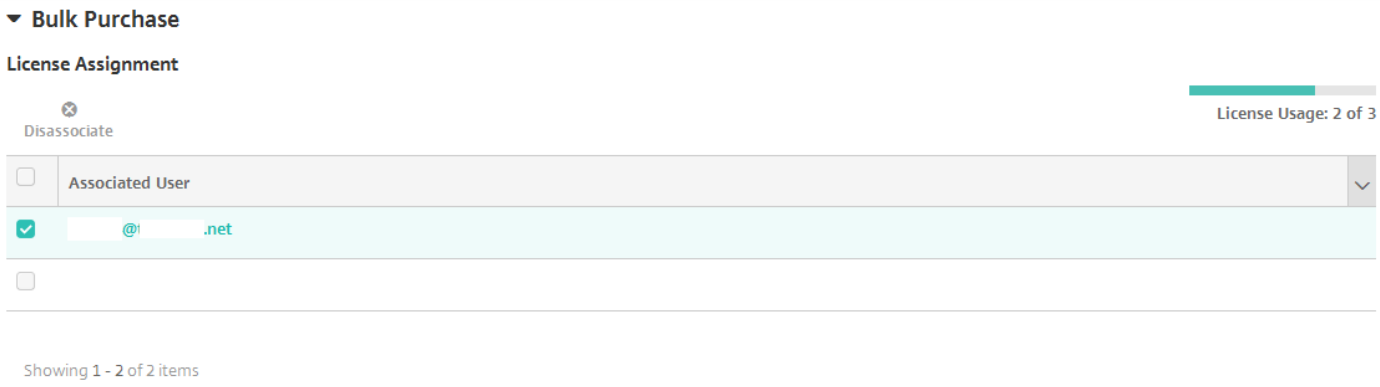
a. 9. XenMobileでアプリケーションのVPPライセンスを適用できるようにする場合は、［**VPP license**］の一覧から、［**Upload a VPP license file**］を選択します。

b. 10. ダイアログボックスが開いたら、ライセンスをインポートします。

Android for Workの一括購入の場合は、［**Bulk Purchase**］セクションを展開します。



［License Assignment］の表に、そのアプリケーションについての使用できる合計数と、現在使用されているライセンス数が表示されます。 ユーザーを選択して［**Disassociate**］をクリックすると、そのユーザーへのライセンスの割り当てが終了し、別のユーザー向けにライセンスを空けることができます。 ただし、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。



13. **[Next]** をクリックします。 [Approvals] ページが開きます。

ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。 承認ワークフローを設定する必要がない場合は、次の手順に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use**：一覧から既存のワークフローを選択するか、**[Create a new workflow]** をクリックします。 デフォルトは **[None]** です。
- **[Create a new workflow]** を選択した場合は、次の設定を構成します。
  - **Name**：ワークフローの固有の名前を入力します。
  - **Description**：任意で、ワークフローの説明を入力します。
  - **Email Approval Templates**：一覧から、割り当てる電子メール承認テンプレートを選択します。 このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。 デフォルトは **[1 level]** です。 選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers**：検索フィールドに、追加で必要なユーザーの名前を入力して、**[Search]** をクリックします。 名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが **[Selected additional required approvers]** の一覧に表示されます。
    - **[Selected additional required approvers]** の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[Search]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
    - **[Selected additional required approvers]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

14. **[Next]** をクリックします。 **[Delivery Group Assignment]** ページが開きます。

15. **[Choose delivery groups]** の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧てグループを選択します。 選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

16. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

17. ［**Save**］をクリックします。

XenMobileへのWebおよびSaaSアプリケーションの追加

Aug 02, 2016

XenMobileコンソールを使用して、モバイル、エンタープライズ、Web、SaaS（Software as a Service）アプリケーションへのSSO（Single Sign-On：シングルサインオン）認証をユーザーに提供できます。 アプリケーションのSSOは、アプリケーションコネクタのテンプレートを使用して有効にできます。 XenMobileで使用できるコネクタの種類の一覧については、「アプリケーションコネクタの種類の一覧」を参照してください。 XenMobileで独自のコネクタを構築することもできます。

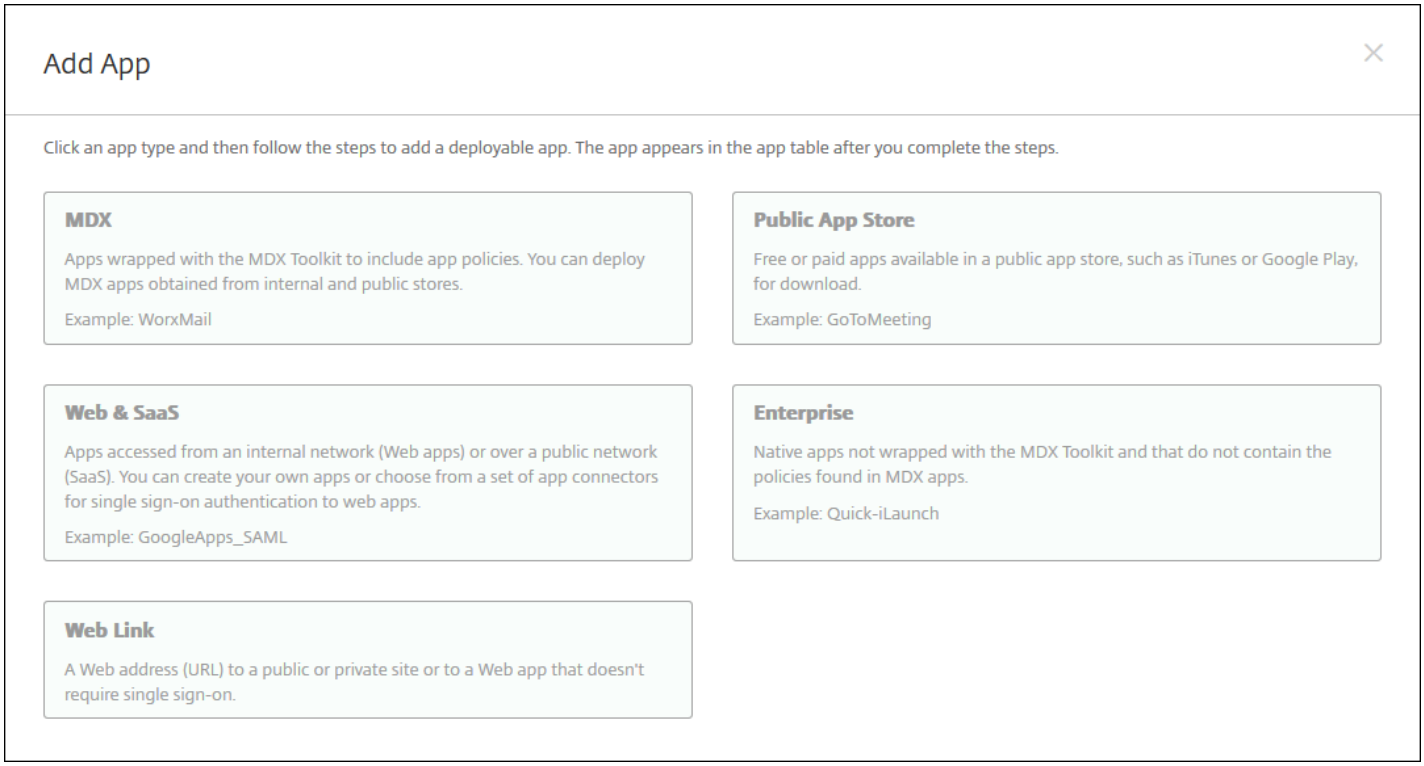
次の情報を指定することによって、コネクタを設定します。

- 異なる名前（オプション）。 コンソールで表示されるいずれかのアプリケーションコネクタを使用します。 ［Box connector］はサポートされなくなりました。
- アプリケーションの説明。
- FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）を使用したWebアドレス。 たとえば、LinkedInをアプリケーション一覧に追加する場合、http://www.linkedin.comにアクセスして［サインイン］をクリックします。 ログオンページが表示されたら、Webアドレスhttps://www.linkedin.comを使用してアプリケーションを構成します。
- アプリケーションの場所（インターネットと内部ネットワークのどちらか）。
- SSOの資格情報。 ユーザーはアプリケーションの資格情報を使用できます。
- アプリケーションのカテゴリ。 カテゴリを使用してWorx Homeでアプリケーションを整理できます。
- XenMobileで構成するアプリケーションごとのアプリケーションポリシー。
- すべてのアプリケーションのワークフロー承認設定。 アプリケーションの割り当て先となるユーザーのデリバリーグループを承認できる個人を指定します。

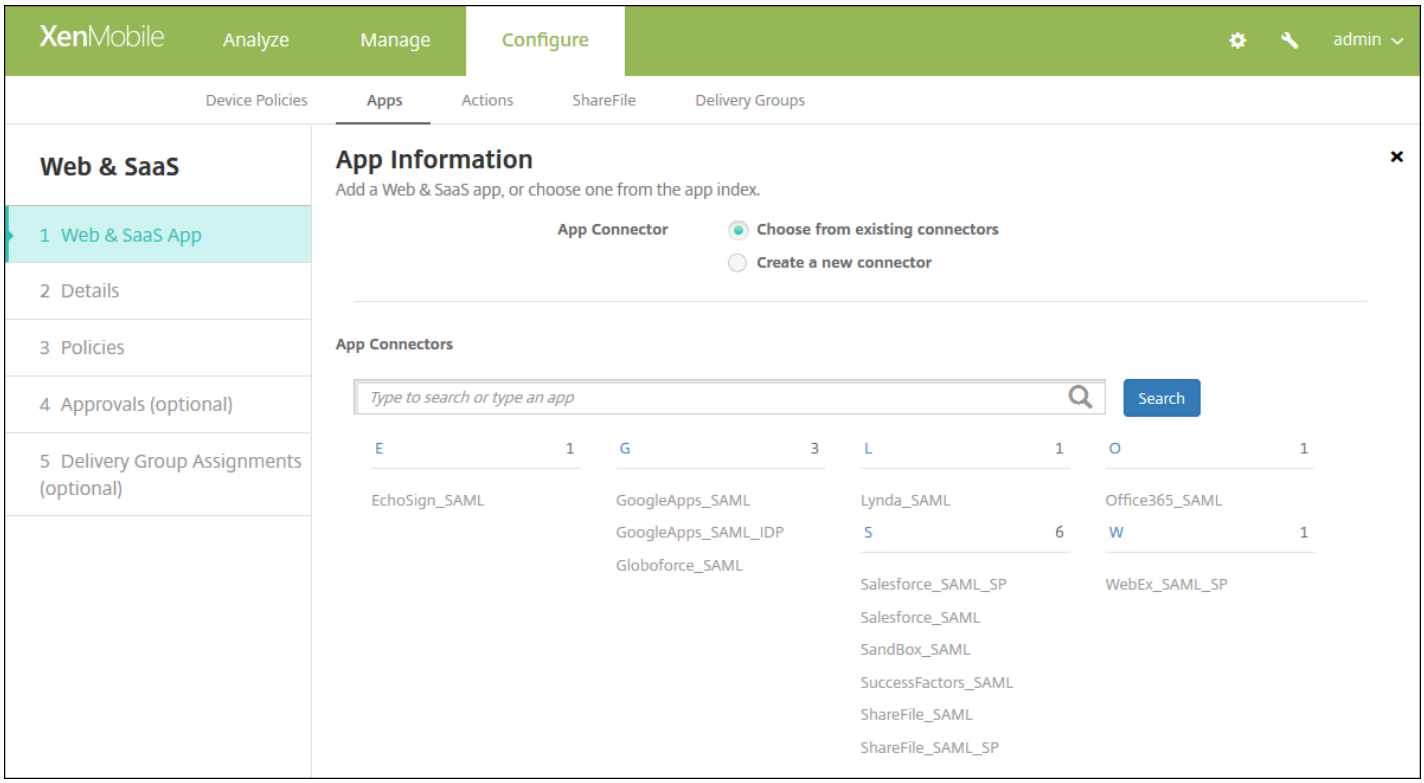
アプリケーションがSSOのみに対応している場合に、前記の設定の構成を完了してその設定を保存すると、アプリケーションがXenMobileコンソールの［**Apps**］タブに表示されます。

1. XenMobileコンソールで、［**Configure**］の［**Apps**］をクリックします。 ［**Apps**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add App**］ダイアログボックスが開きます。



3. [**Web & SaaS**] を選択します。 [**App Information**] ページが開きます。



4. 次の設定を構成します。

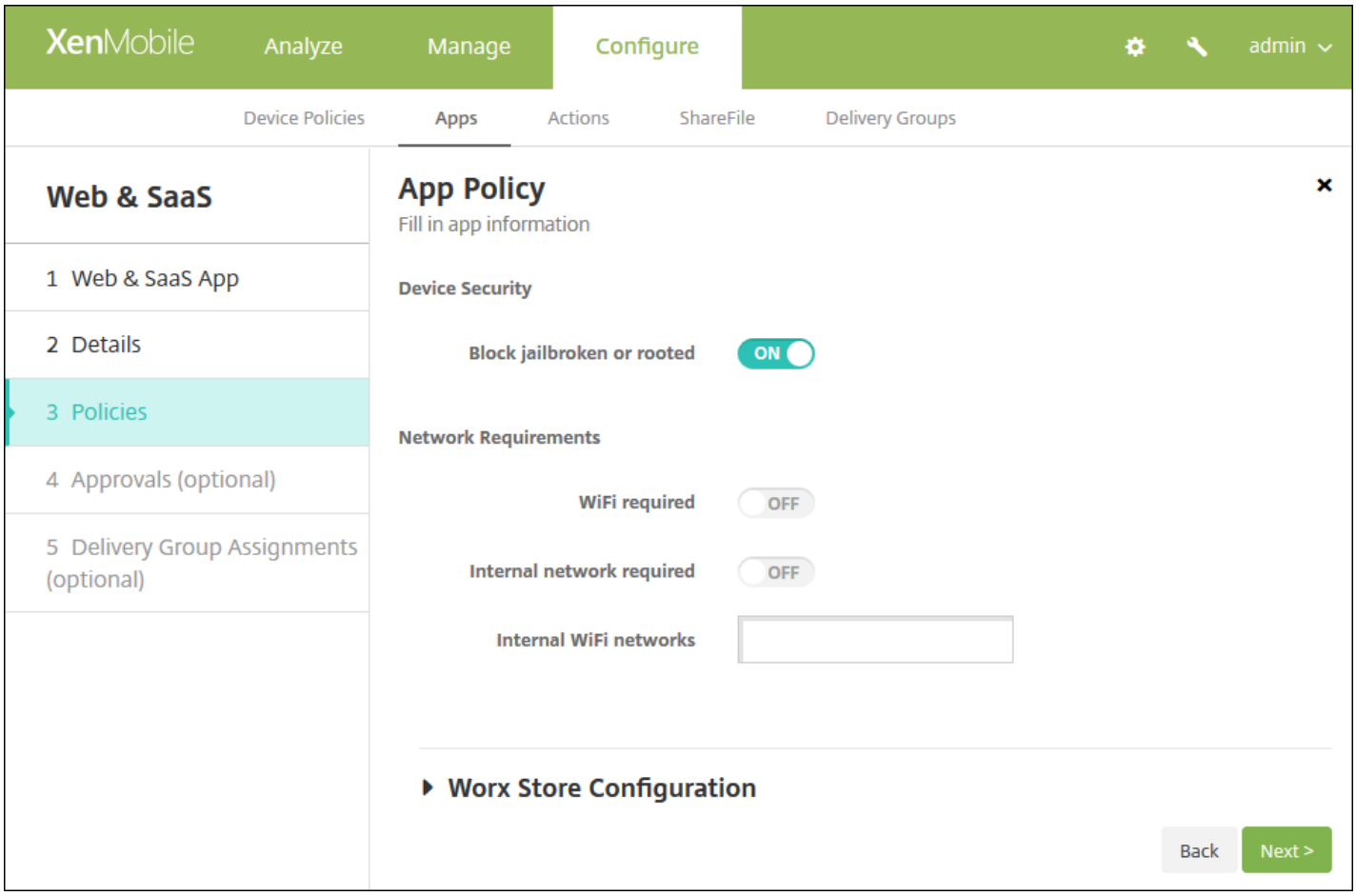
- **App Connector**： [**Choose from existing connector**] または [**Create a new connector**] をクリックします。 デ

フォルトは［**Choose from existing connector**］です。

- ［**Create a new connector**］をクリックすると、新しいコネクタを定義できるフィールドが表示されます。
  - 次の設定を構成します。
    - **Name**：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。
    - **Description**：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。
    - **Logon URL**：ユーザーがサイトにログオンするときに使用するURLを入力するか、コピーして貼り付けます。 このフィールドは必須です。
    - **SAML version**：［1.1］または［2.0］を選択します。 デフォルトは**1.1**です。
    - **Entity ID**：SAMLアプリケーションのIDを入力します。
    - **Relay State URL**：SAMLアプリケーションのWebアドレスを入力します。 リレーステートURLはアプリケーションからの応答URLです。
    - **Name ID format**：［Email Address］または［Unspecified］を選択します。 デフォルトは［**Email Address**］です。
    - **ACS URL**：IDプロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービスURL（ACS URL）を入力します。 ACS URLでは、ユーザーがシングルサインオン機能を使用できます。
    - **Image**：デフォルトのCitrixイメージを使用するのか、独自のアプリケーションイメージをアップロードするのかを選択します。 デフォルトは［Use default］です。
      - 独自のイメージをアップロードする場合は、［**Browse**］をクリックしてアップロードするファイルの場所に移動し、ファイルを選択します。 このファイルはPNGファイルである必要があります。JPEGファイルやGIFファイルはアップロードできません。 カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。
  - ［**Add**］をクリックします。 ［**Details**］ページが開きます。
- ［**Choose from existing connector**］をクリックした場合、または新しいコネクタの設定後に［**Add**］をクリックすると、［**Details**］ページが開きます。
- 次の設定を構成します。
  - **App name**：事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
  - **App description**：事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
  - **URL**：事前に入力されているURLをそのまま使用するか、アプリケーションのWebアドレスを入力します。 選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
  - **Domain name**：該当する場合、アプリケーションのドメイン名を入力します。 このフィールドは必須です。
  - **App is hosted in internal network**：内部ネットワークのサーバーでアプリケーションを実行するかどうかを選択します。 ユーザーがリモートから内部アプリケーションに接続する場合は、NetScaler Gatewayを介して接続する必要があります。 このオプションを［**ON**］に設定すると、VPNキーワードがアプリケーションに追加され、NetScaler Gatewayを介して接続できるようになります。 デフォルトは［**OFF**］です。
  - **App category**：一覧から、アプリケーションに適用する任意のカテゴリを選択します。
  - **User account provisioning**：アプリケーションのユーザーアカウントを作成するかどうかを選択します。 Globalforce_SAMLコネクタを使用している場合は、このオプションを有効にして、シームレスなSSO統合が行われるようにする必要があります。
  - ［**User account provisioning**］を有効にした場合は、次の設定を構成します。
    - **Service Account**
      - **User name**：アプリケーション管理者の名前を入力します。 このフィールドは必須です。
      - **Password**：アプリケーション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。
    - **User Account**
      - **When user entitlement ends**：一覧から、ユーザーがアプリケーションへのアクセスを許可されなくなった場合に実行するアクションを選択します。 デフォルトは［**Disable account**］です。 選択できるオプションは以下のとおりです。
        - Disable account

        - Keep account
        - Remove account
    - **User Name Rule**
        - 追加するユーザー名の規則ごとに、以下の操作を行います。
            - **User attributes**：一覧から、規則に追加するユーザー属性を選択します。
            - **Length（characters）**：一覧から、ユーザー名の規則で使用するユーザー属性の文字数を選択します。 デフォルトは［**All**］です。
            - **Rule**：追加した各ユーザー属性が、ユーザー名の規則に自動的に追加されます。
- **Password Requirement**
    - **Length**：ユーザーパスワードの最小文字数を入力します。 デフォルトは**8**です。
- **パスワードの有効期限**
    - **Validity (days)**：パスワードの有効期間（日数）を入力します。 有効な値は0～90です。 デフォルトは**90**です。
    - **Automatically reset password after it expires**：有効期限が切れたときにパスワードを自動的にリセットするかどうかを選択します。 デフォルトは［**OFF**］です。 このフィールドを無効すると、ユーザーはユーザーパスワードの有効期限が切れたときにアプリケーションを開くことができなくなります。

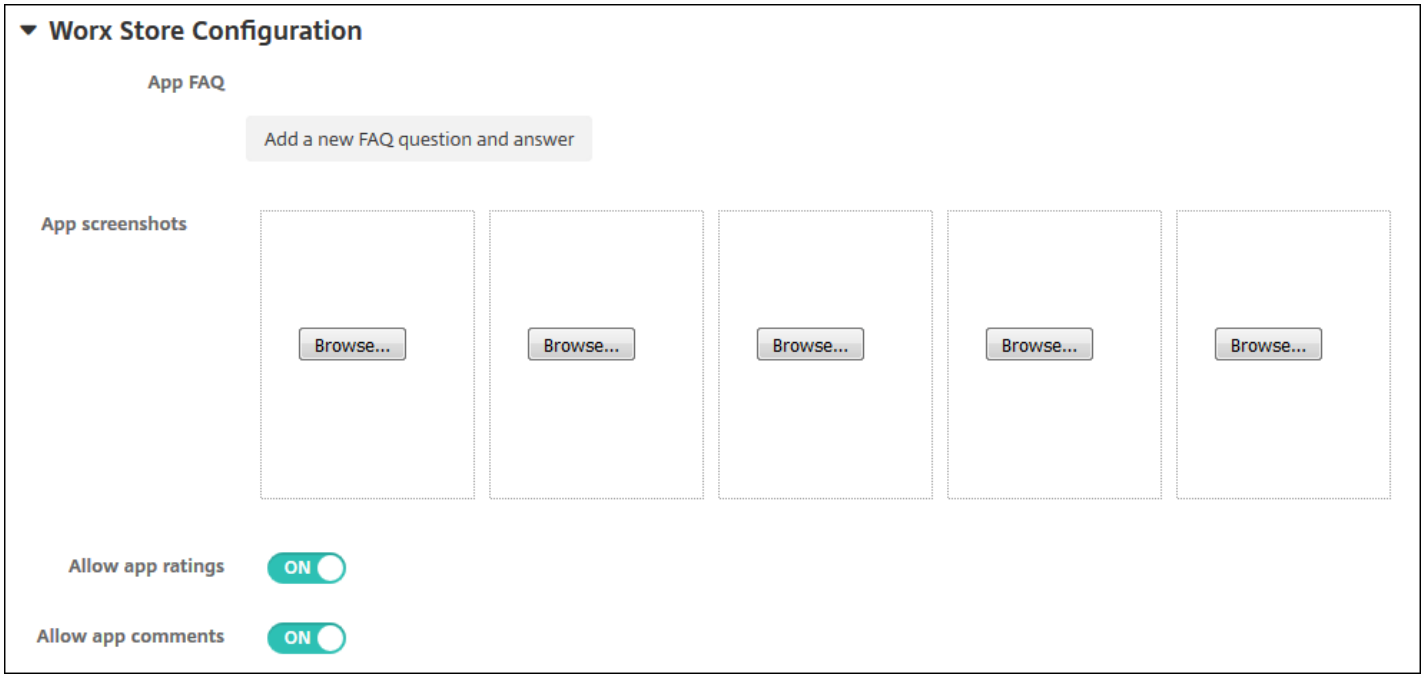
5. ［**Next**］をクリックします。 ［**App Policy**］ページが開きます。



- 次の設定を構成します。
    - デバイスセキュリティ
        - **Block jailbroken or rooted**：ジェイルブレーク済みまたはルート化済みのデバイスによるアプリケーションへのアクセスをブロックするかどうかを選択します。 デフォルトは［**ON**］です。

- ネットワーク要件
  - **WiFi required**：アプリケーションの実行にWiFi接続が必要であるかどうかを選択します。 デフォルトは**[OFF]**です。
  - **Internal network required**：アプリケーションの実行に内部ネットワークが必要であるかどうかを選択します。 デフォルトは［**OFF**］です。
  - **Internal WiFi networks**：［**WiFI required**］を有効にした場合は、使用する内部WiFiネットワークを入力します。

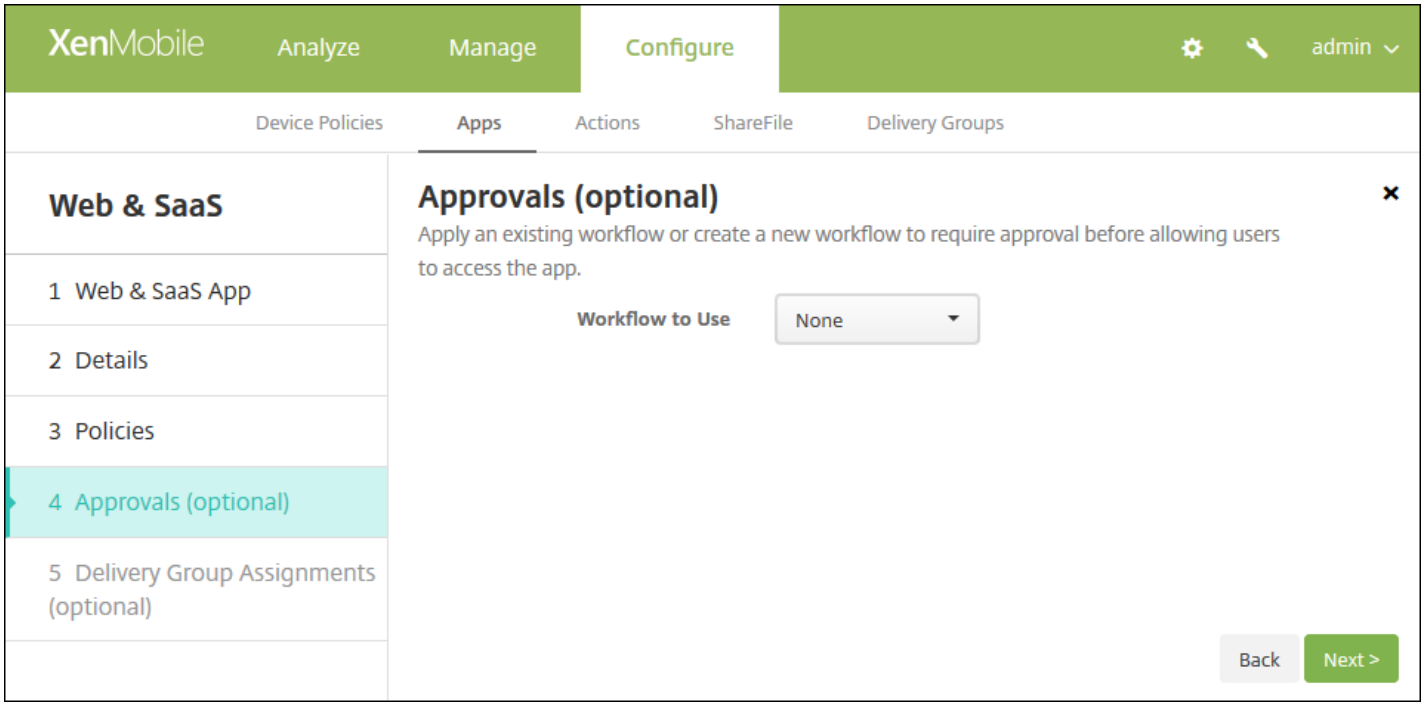
6. ［**Worx Store Configuration**］を展開します。



任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは**[ON]**です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。 デフォルトは［**ON**］です。

7. ［**Next**］をクリックします。 ［**Approvals**］ページが開きます。



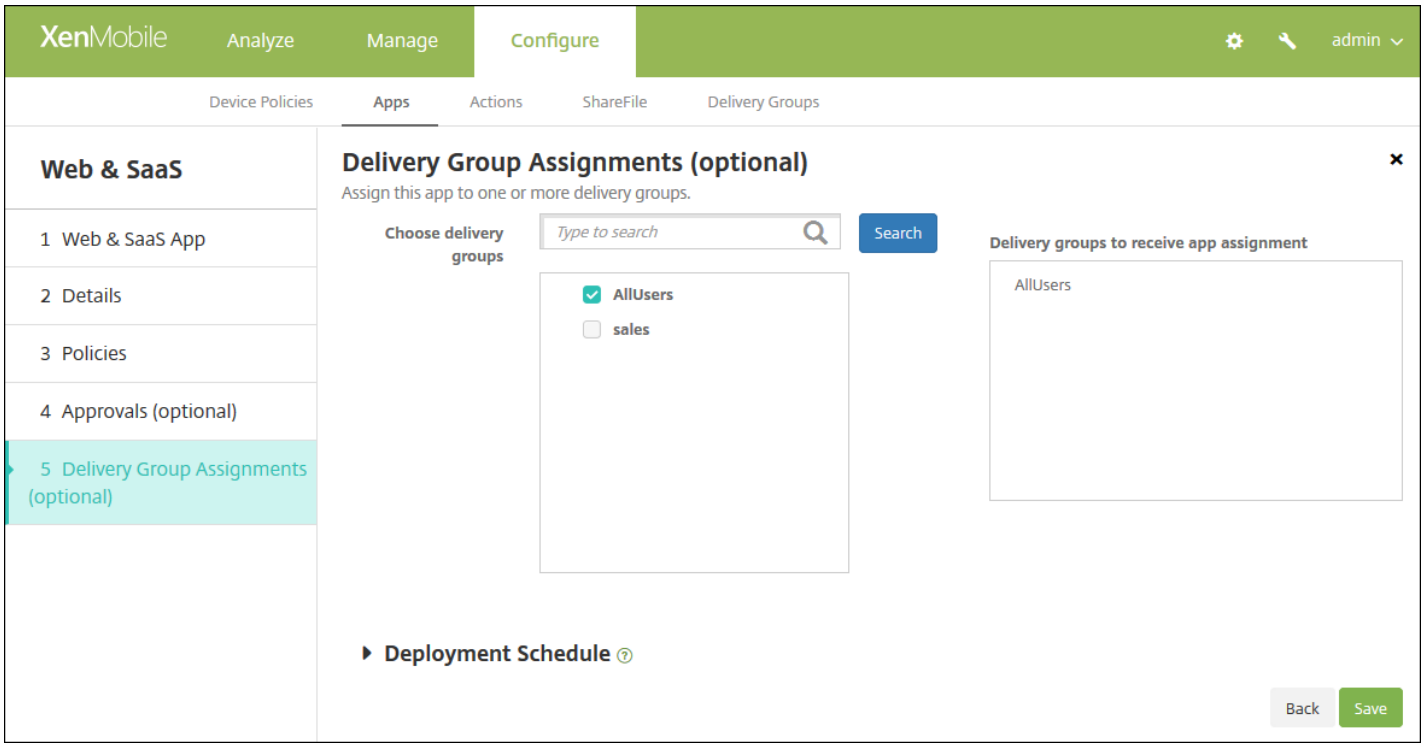
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。 承認ワークフローを設定する必要がない場合は、手順8に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use**：一覧から既存のワークフローを選択するか、［**Create a new workflow**］をクリックします。 デフォルトは［**None**］です。
- ［**Create a new workflow**］を選択した場合は、次の設定を構成します。
  - **Name**：ワークフローの固有の名前を入力します。
  - **Description**：任意で、ワークフローの説明を入力します。
  - **Email Approval Templates**：一覧から、割り当てる電子メール承認テンプレートを選択します。 このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。 デフォルトは［**1 level**］です。 選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers**：検索フィールドに、追加で必要なユーザーの名前を入力して、［**Search**］をクリックします。 名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが［**Selected additional required approvers**］の一覧に表示されます。
    - ［**Selected additional required approvers**］の一覧からユーザーを削除するには、次のいずれかを行います。
      - ［**Search**］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して［**Search**］をクリックし、検索結果を絞り込みます。
      - ［**Selected additional required approvers**］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにし

ます。

8. [**Next**] をクリックします。 [**Delivery Group Assignment**] ページが開きます。



9. [**Choose delivery groups**] の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

10. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

11. [**Save**] をクリックします。

Application Connectorの種類の一覧

Aug 02, 2016

次の表に、XenMobile内で使用できるコネクタとコネクタの種類を示します。 また、各コネクタがユーザーアカウント管理をサポートするかどうかについても示します。ユーザーアカウント管理がサポートされる場合、管理者は新しいアカウントを自動的に作成したり、ワークフローを使って作成したりできます。

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
EchoSign_SAML	○	○
Globoforce_SAML		注：このコネクタを使用する場合は、［User Management for Provisioning］を有効にして、シームレスなSSO統合が行われるようにする必要があります。
GoogleApps_SAML	○	○
GoogleApps_SAML_IDP	○	○
Lynda_SAML	○	○
Office365_SAML	○	○
Salesforce_SAML	○	○
Salesforce_SAML_SP	○	○
SandBox_SAML	○	
SuccessFactors_SAML	○	
ShareFile_SAML	○	
ShareFile_SAML_SP	○	
WebEx_SAML_SP	○	○

XenMobileへのエンタープライズアプリケーションの追加

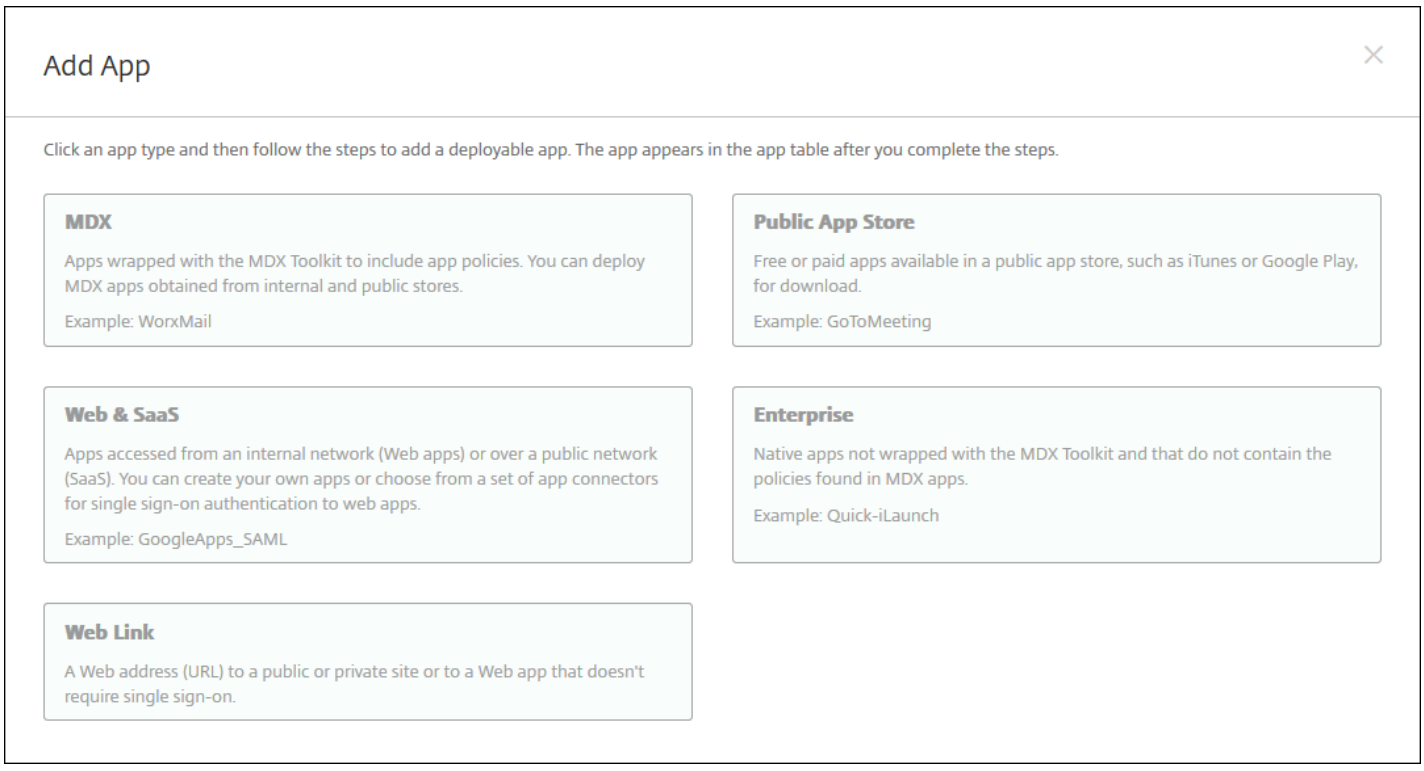
Aug 02, 2016

XenMobileのエンタープライズアプリケーションとは、MDX Toolkitでラップされておらず、MDXアプリケーションに関連付けられたポリシーを含んでいない、ネイティブアプリケーションを意味します。 エンタープライズアプリケーションのアップロードは、XenMobileコンソールの［**Apps**］タブで行うことができます。 エンタープライズアプリケーションは、以下のプラットフォーム（および対応するファイルの種類）をサポートします。

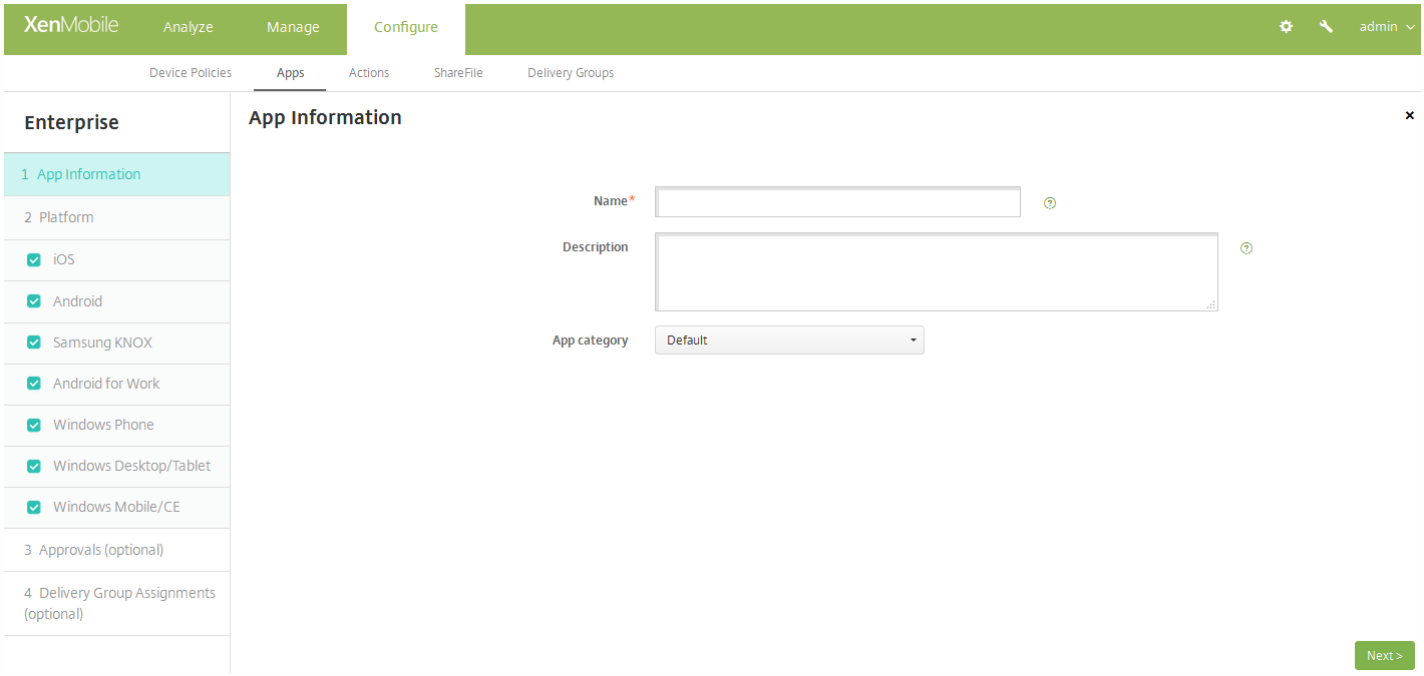
- iOS（.ipaファイル）
- Android（.apkファイル）
- Samsung KNOX（.apkファイル）
- Android for Work（.apkファイル）
- Windows Phone（.xapまたは.appxファイル）
- Windowsタブレット（.appxファイル）
- Windows Mobile/CE（.cabファイル）

XenMobileコンソールで、［**Configure**］の［**Apps**］をクリックします。 ［**Apps**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add App**］ダイアログボックスが開きます。



3. ［**Enterprise**］をクリックします。 ［**App Information**］ページが開きます。



4. [**App Information**] ペインで、以下の情報を入力します。

- **Name**：アプリケーションの説明的な名前を入力します。 この情報は、 [Apps] の表の [App Name] の下に表示されます。
- **Description**：任意で、アプリケーションの説明を入力します。
- **App category**：任意で、一覧から、アプリケーションを追加するカテゴリを選択します。 アプリケーションカテゴリについて詳しくは、「XenMobileでのアプリケーションカテゴリの作成」を参照してください。

5. [**Next**] をクリックします。 [**App Platforms**] ページが開きます。

6. [**Platforms**] の下で、追加するプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10.を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、 [**Browse**] をクリックしてアップロードするファイルの場所に移動し、そのファイルを選択します。

8. [**Next**] をクリックします。 プラットフォームのアプリケーション情報ページが開きます。

9. プラットフォームの種類について、以下の設定を構成します。

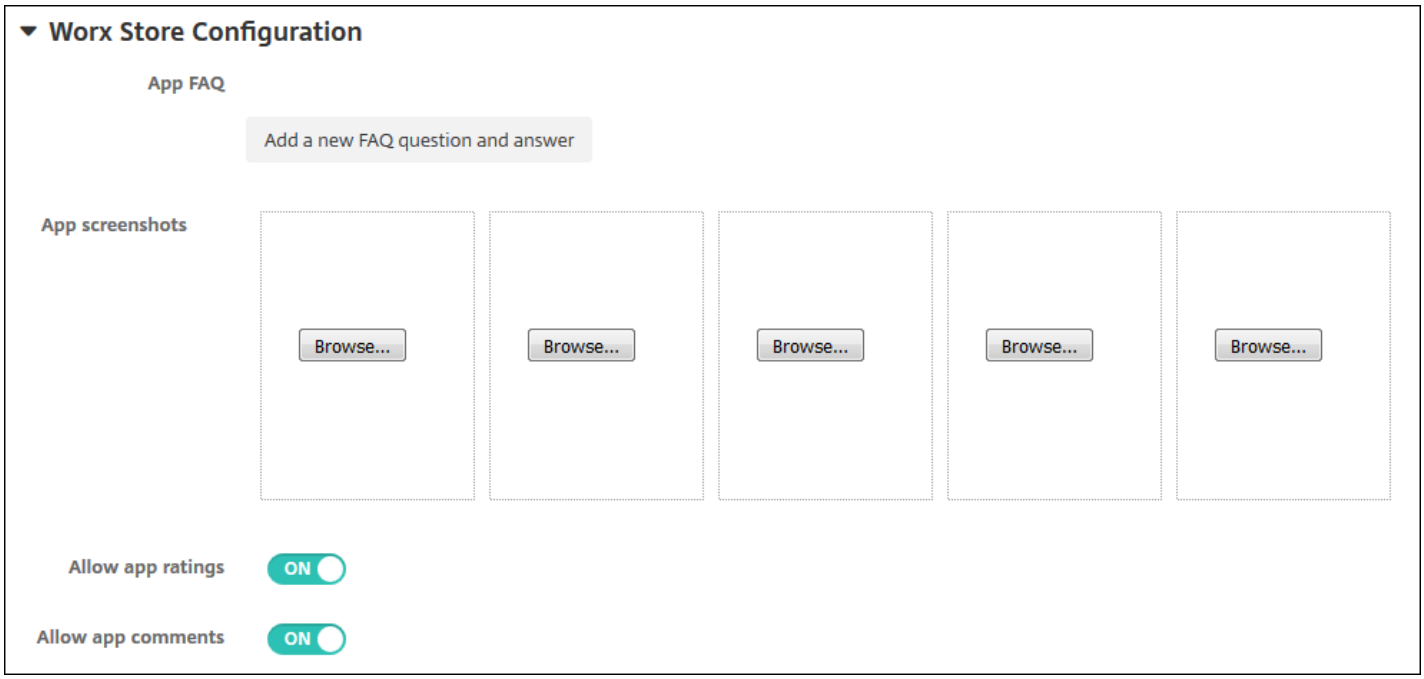
- **File name**：任意で、アプリケーションの名前を新たに入力します。
- **App Description**：任意で、アプリケーションの説明を新たに入力します。
- **App version**：このフィールドは変更できません。
- **Minimum OS version**：
- **Maximum OS version**：
- **Excluded devices**：
- **Remove app if MDM profile is removed**：MDMプロファイルが削除された場合にデバイスからアプリケーションを削除するかどうかを選択します。 デフォルトは [**ON**] です。
- **Prevent app data backup**：アプリケーションのデータをバックアップできないようにするかどうかを選択します。 デ

フォルトは［**ON**］です。

- **Force app to be managed**：非管理対象のアプリケーションをインストールして、監視対象デバイスのユーザーにアプリケーションの管理を許可するよう求める場合は、［ON］を選択します。 ユーザーがこの要求を受け入れた場合、アプリケーションは管理対象になります。 この設定は、iOS 9.xデバイスに適用されます。

10. 展開規則の構成

11. ［**Worx Store Configuration**］を展開します。



任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは**[ON]**です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。 デフォルトは［**ON**］です。

12. ［**Next**］をクリックします。 ［**Approvals**］ページが開きます。

ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。 承認ワークフローを設定する必要がない場合は、手順13に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use**：一覧から既存のワークフローを選択するか、［**Create a new workflow**］をクリックします。 デフォルトは［**None**］です。
- ［Create a new workflow］を選択した場合は、次の設定を構成します。

- **Name**：ワークフローの固有の名前を入力します。
- **Description**：任意で、ワークフローの説明を入力します。
- **Email Approval Templates**：一覧から、割り当てる電子メール承認テンプレートを選択します。 このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
- **Levels of manager approval**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。 デフォルトは［**1 level**］です。 選択できるオプションは以下のとおりです。
  - Not Needed
  - 1 level
  - 2 levels
  - 3 levels
- **Select Active Directory domain**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
- **Find additional required approvers**：検索フィールドに、追加で必要なユーザーの名前を入力して、［**Search**］をクリックします。 名前はActive Directoryで取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが［**Selected additional required approvers**］の一覧に表示されます。
  - ［**Selected additional required approvers**］の一覧からユーザーを削除するには、次のいずれかを行います。
    - ［**Search**］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して［**Search**］をクリックし、検索結果を絞り込みます。
    - ［**Selected additional required approvers**］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

13. ［**Next**］をクリックします。 ［**Delivery Group Assignment**］ページが開きます。

14. ［**Choose delivery groups**］の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが［**Delivery groups to receive app assignment**］一覧に表示されます。

15. ［**Deployment Schedule**］を展開して以下の設定を構成します。

- ［**Deploy**］の横の［**ON**］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［**ON**］です。 ［**OFF**］を選択した場合、そのほかのオプションを構成する必要はありません。
- ［**Deployment schedule**］の横の［**Now**］または［**Later**］をクリックします。 デフォルトのオプションは［**Now**］です。
- ［**Later**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**Deployment condition**］の横の［**On every connection**］をクリックするか、［**Only when previous deployment has failed**］をクリックします。 デフォルトのオプションは、［**On every connection**］です。
- ［**Deploy for always-on connection**］の横の［**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**］です。

注：

- このオプションは、［**Settings**］の［**Server Properties**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［**Deploy for always on connection**］は適用されません。

16. ［**Save**］をクリックします。

XenMobileへのWebリンクアプリケーションの追加

Aug 02, 2016

XenMobileで、パブリックサイトやプライベートサイト、またはシングルサインオン（SSO）を必要としないWebアプリケーションのWebアドレス（URL）を設置できます。

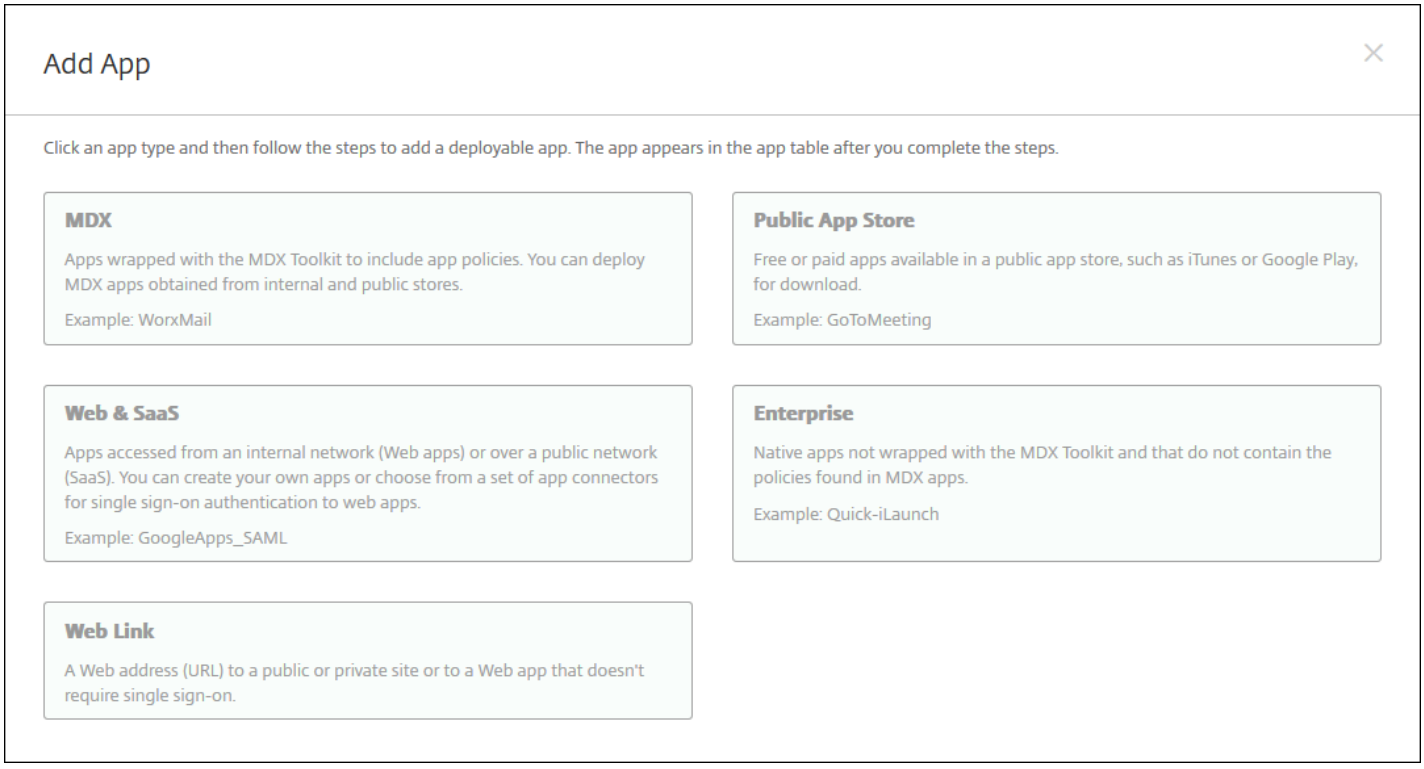
Webリンクの構成は、XenMobileコンソールの［**Apps**］タブで行うことができます。 Webリンクの構成が完了すると、リンクは［**Apps**］の表にある一覧にリンクアイコンとして表示されます。 ユーザーがWorx Homeを使ってログオンすると、リンクは使用可能なアプリケーションおよびデスクトップの一覧と共に表示されます。

リンクを追加するには、次の情報を指定します。

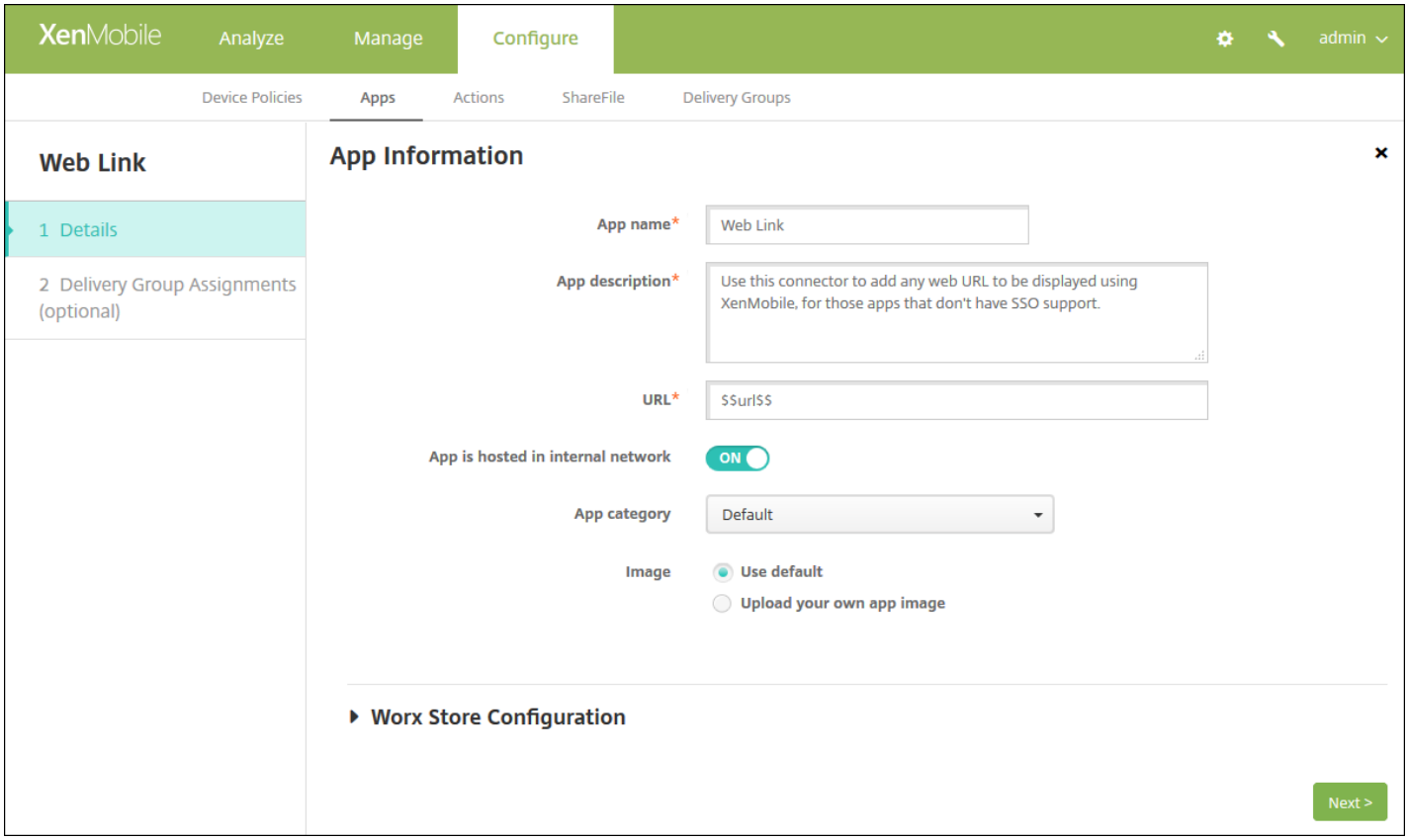
- リンクの名前
- リンクの説明
- Webアドレス（URL）
- カテゴリ
- 役割
- .png形式の画像（オプション）

1. XenMobileコンソールで、［**Configure**］の［**Apps**］をクリックします。 ［**Apps**］ページが開きます。

2. ［**Add**］をクリックします。 ［**Add App**］ダイアログボックスが開きます。



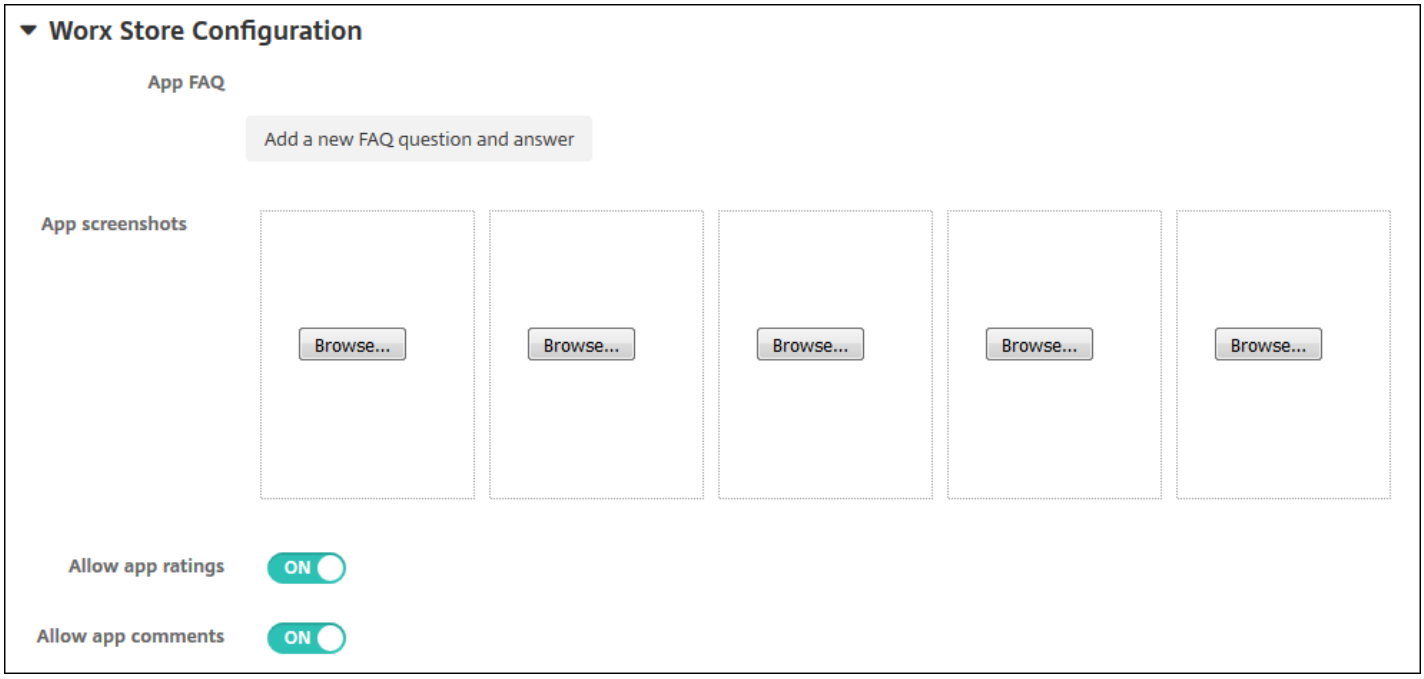
3. ［**Web Link**］をクリックします。 ［**App Information**］ページが開きます。



4. 次の設定を構成します。

- **App name**：事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- **App description**：事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL**：事前に入力されているURLをそのまま使用するか、アプリケーションのWebアドレスを入力します。 選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
- **App is hosted in internal network**：内部ネットワークのサーバーでアプリケーションを実行するかどうかを選択します。 ユーザーがリモートから内部アプリケーションに接続する場合は、NetScaler Gatewayを介して接続する必要があります。 このオプションを［**ON**］に設定すると、VPNキーワードがアプリケーションに追加され、NetScaler Gatewayを介して接続できるようになります。 デフォルトは［**OFF**］です。
- **App category**：一覧から、アプリケーションに適用する任意のカテゴリを選択します。
- **Image**：デフォルトのCitrixイメージを使用するのか、独自のアプリケーションイメージをアップロードするのかを選択します。 デフォルトは［Use default］です。
  - 独自のイメージをアップロードする場合は、［**Browse**］をクリックしてアップロードするファイルの場所に移動し、ファイルを選択します。 このファイルはPNGファイルである必要があります。JPEGファイルやGIFファイルはアップロードできません。 カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。

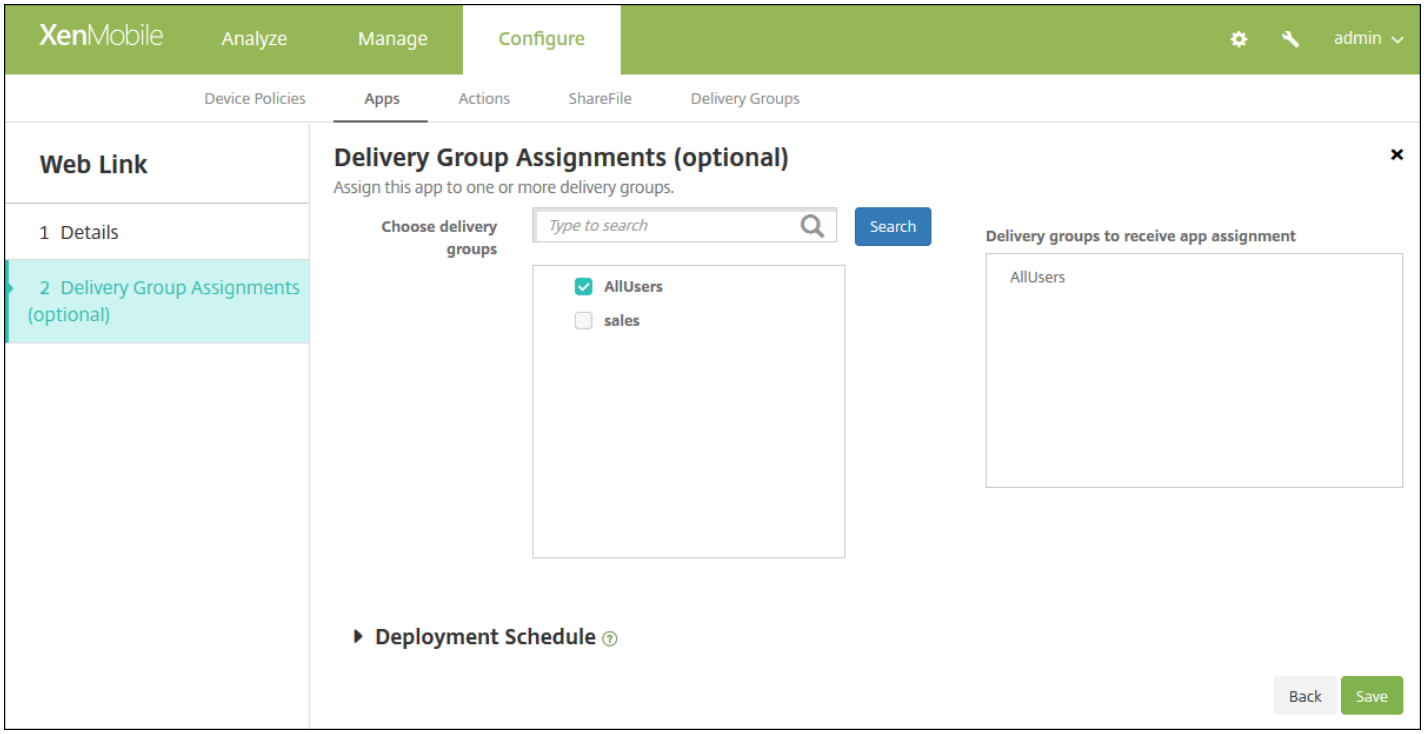
5. ［**Worx Store Configuration**］を展開します。



任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは［ON］です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。 デフォルトは［ON］です。

6. **［Next］**をクリックします。 **［Delivery Group Assignment］**ページが開きます。



7. [**Choose delivery groups**] の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

8. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [**Deploy for always-on connection**] の横の [**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**] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、[**Deploy for always on connection**] は適用されません。

9. [**Save**] をクリックします。

XenMobileでのワークフローの作成および管理

Oct 25, 2016

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。 ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。 その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

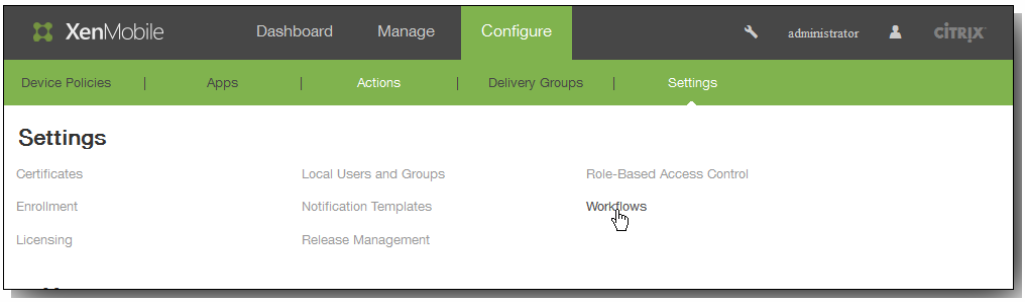
XenMobileを初めて構成するときに、ワークフローの電子メール設定を構成します。 ワークフローを使用するように電子メール設定を構成する必要があります。 ワークフローの電子メール設定はいつでも変更できます。 これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

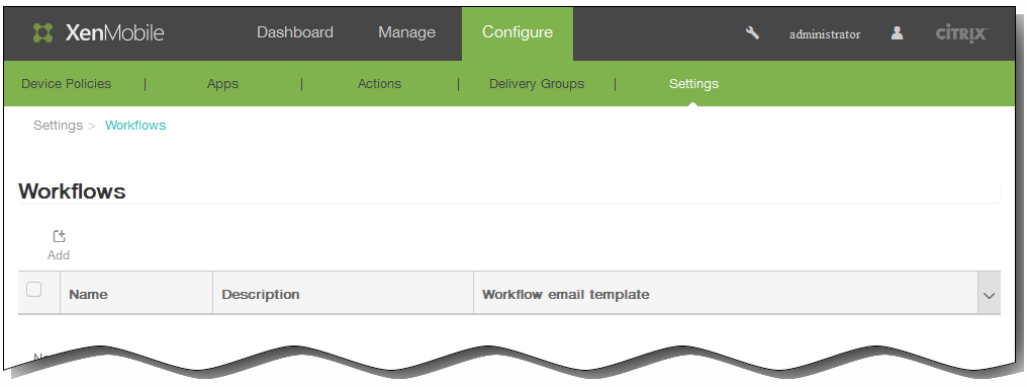
XenMobileの次の2つの方法でワークフローを構成できます。

- XenMobileコンソールの［Workflows］ページ。 ［Workflows］ページでは、アプリケーションの構成で使用する複数のワークフローを構成できます。 ［Workflows］ページでワークフローを構成するとき、アプリケーションを構成するときのワークフローを選択できます。
- アプリケーションコネクタを構成するとき、アプリケーションで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。 「XenMobileへのアプリケーションの追加」を参照してください。

ユーザーアカウントの管理者承認を最大3レベルまで割り当てることができます。 ユーザーアカウントを承認するユーザーかほかにも必要な場合は、ユーザーの名前またはメールアドレスを使用してユーザーを検索し、追加の承認者として選択することができます。 ユーザーが見つかったら、そのユーザーをワークフローに追加します。 ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

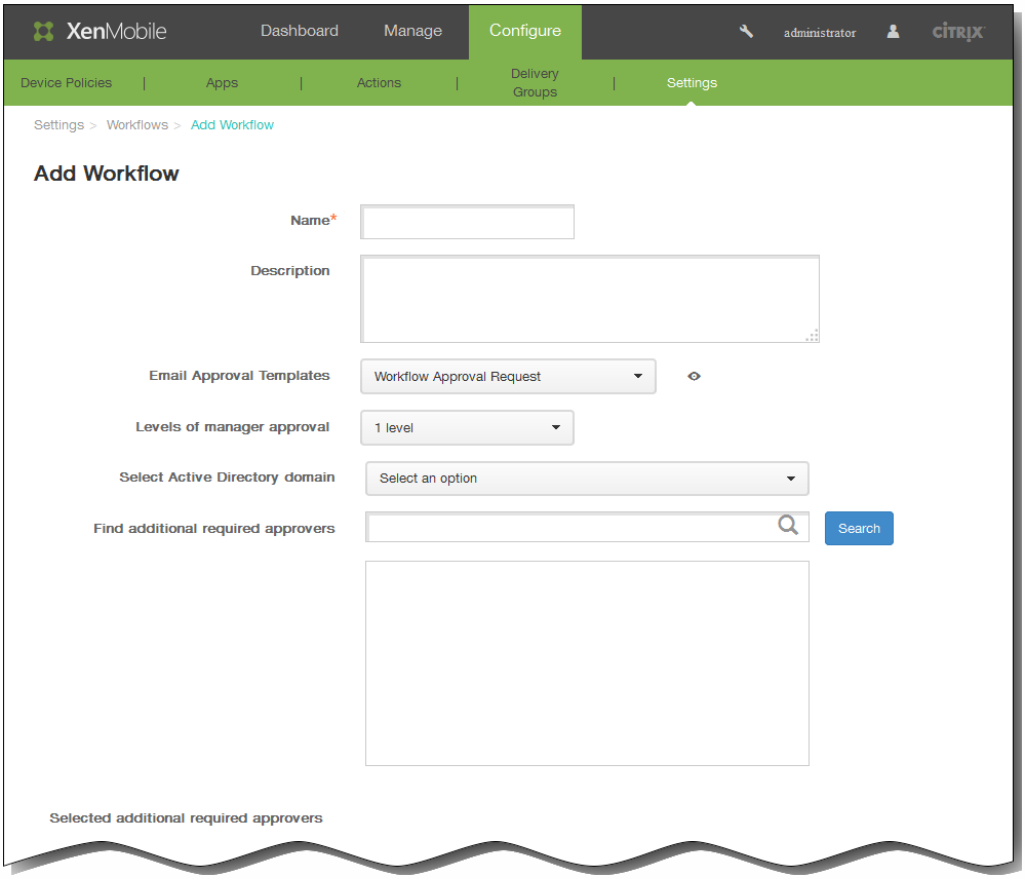
1. XenMobileコンソールで、［Configure］、［Settings］、［Workflows］の順にクリックします。



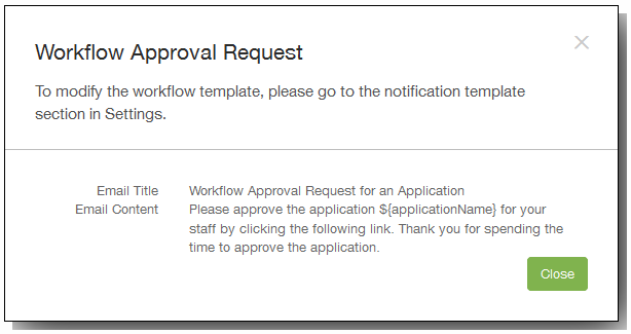


［Workflows］ページが開きます。

2. ［Workflows］ページで、［Add］をクリックします。 ［Add Workflow］ページが開きます。



3. ［Add Workflow］ページの［Name］フィールドに、ワークフローの一意の名前を入力します。
4. ［Description］ボックスに、オプションでワークフローの説明を入力します。
5. ［Email Approval Templates］の一覧から、割り当てる電子メール承認テンプレートを選択します。 電子メールテンプレートの作成は、XenMobileコンソールの［Settings］の［Notification Templates］セクションで行います。 このフィールドの右にある、目のアイコンをクリックすると、以下のヒントが表示されます。



6. ［Levels of manager approval］の一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。
7. ［Select Active Directory domain］の一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
8. ［Find additional required approvers］の横の検索フィールドに、追加で必要なユーザーの名前を入力して、［Search］をクリックします。 名前はActive Directoryで取得されます。

9. ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが［Selected additional required approvers］の一覧に表示されます。 ［Selected additional required approvers］の一覧からユーザーを削除するには、次のいずれかを行います。
   - ［Search］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
   - 名前の全体または一部を検索ボックスに入力して［Search］をクリックし、検索結果を絞り込みます。

   ［Selected additional required approvers］の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

10. ［Save］をクリックします。
    作成したワークフローが［Workflows］ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリケーションを表示したり、ワークフローを削除したりできます。 ワークフローを作成した後でワークフローを編集することはできません。 承認レベルまたは承認者が異なるワークフローが必要な場合は、新しいワークフローを作成する必要があります。

ワークフローの詳細の表示および削除を行うには

1. ［Workflows］ページの既存のワークフローの一覧で、表の行をクリックするかワークフローの横にあるチェックボックスをオンにして、特定のワークフローを選択します。
2. ワークフローを削除するには、［Delete］をクリックします。 確認ダイアログボックスが開きます。 もう一度［Delete］をクリックします。
   重要：この操作を元に戻すことはできません。

XenMobileでのMDXまたはエンタープライズアプリケーションのアップグレード

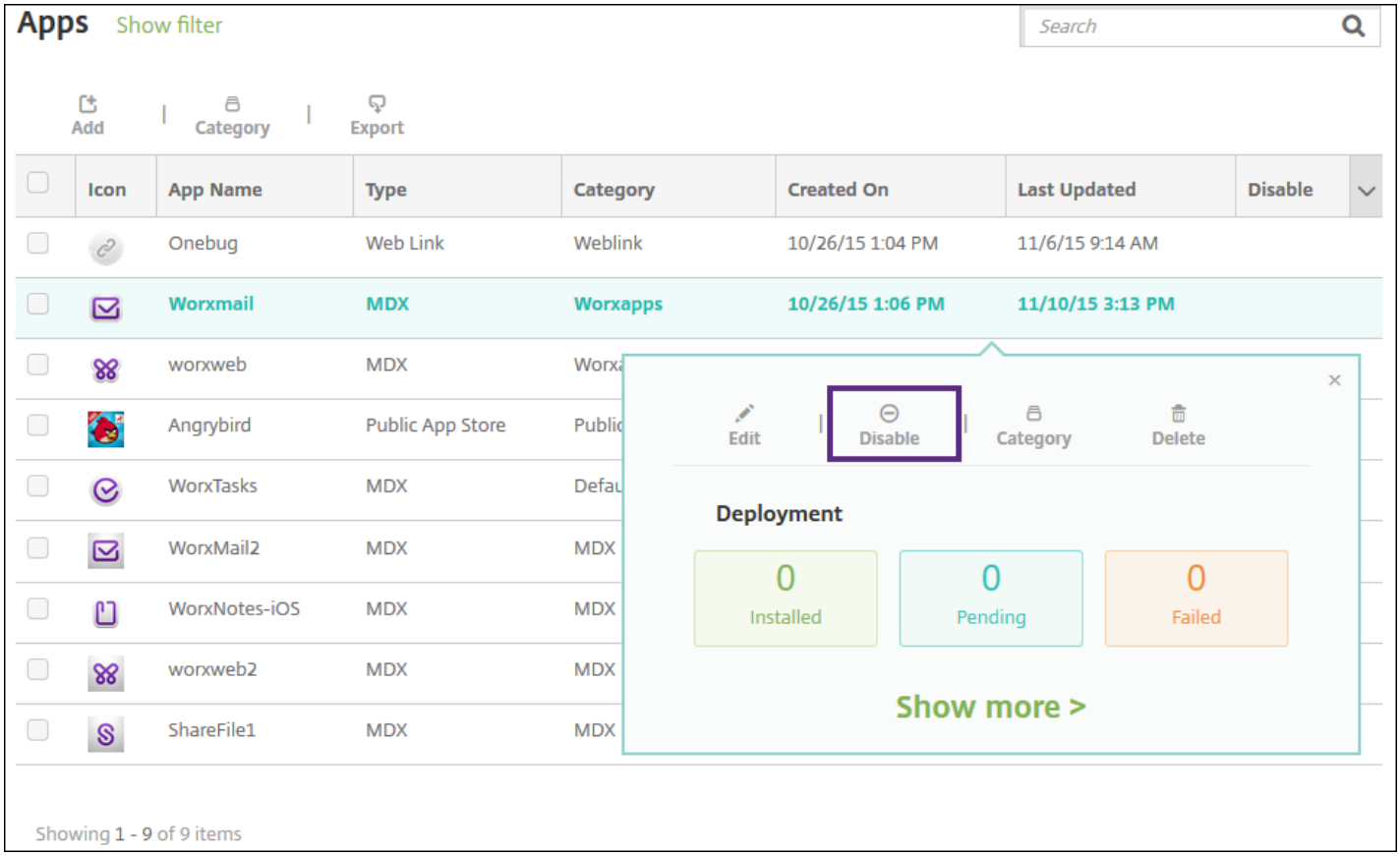
Aug 02, 2016

XenMobileでMDXまたはエンタープライズアプリケーションをアップグレードするには、XenMobileコンソールでアプリケーションを無効にしてから、アプリケーションの新しいバージョンをアップロードします。

1. XenMobileコンソールで、［**Configure**］の［**Apps**］をクリックします。［**Apps**］ページが開きます。

2. 管理対象デバイス（モバイルデバイス管理でXenMobileに登録されたデバイス）の場合は、スキップして手順4に進みます。非管理対象デバイス（エンタープライズアプリケーション管理の目的のみでXenMobileに登録されたデバイス）の場合は、次の手順に従います。

- ［**Apps**］の表で、アプリケーションの横のチェックボックスをオンにするか、更新するアプリケーションを含む行をクリックします。
- 表示されるメニューで、［**Disable**］をクリックします。［**Disable**］ダイアログボックスが開きます。



- このダイアログボックスで、［**Disable**］をクリックします。アプリケーションの［**Disable**］列に「*Disabled*」と表示されます。

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
	Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

注：アプリケーションを無効にすると、アプリケーションが保守モードになります。 アプリケーションが無効になっている場合、ユーザーはログオフ後にそのアプリケーションに再接続することはできません。 アプリケーションの無効化は任意の設定ですが、アプリケーションの機能の問題を避けるために、アプリケーションを無効にすることをお勧めします。 ポリシーを更新する場合や、XenMobileにアプリケーションをアップロードするのと同時にユーザーがダウンロードを要求する場合などに問題が発生することがあります。

4. **[Apps]**の表で、アプリケーションの横のチェックボックスをオンにするか、更新するアプリケーションを含む行をクリックします。

5. 表示されるメニューで、 **[Edit]**をクリックします。 アプリケーションに対して最初に選択したプラットフォームが選択された状態で、 **[App Information]**ページが開きます。

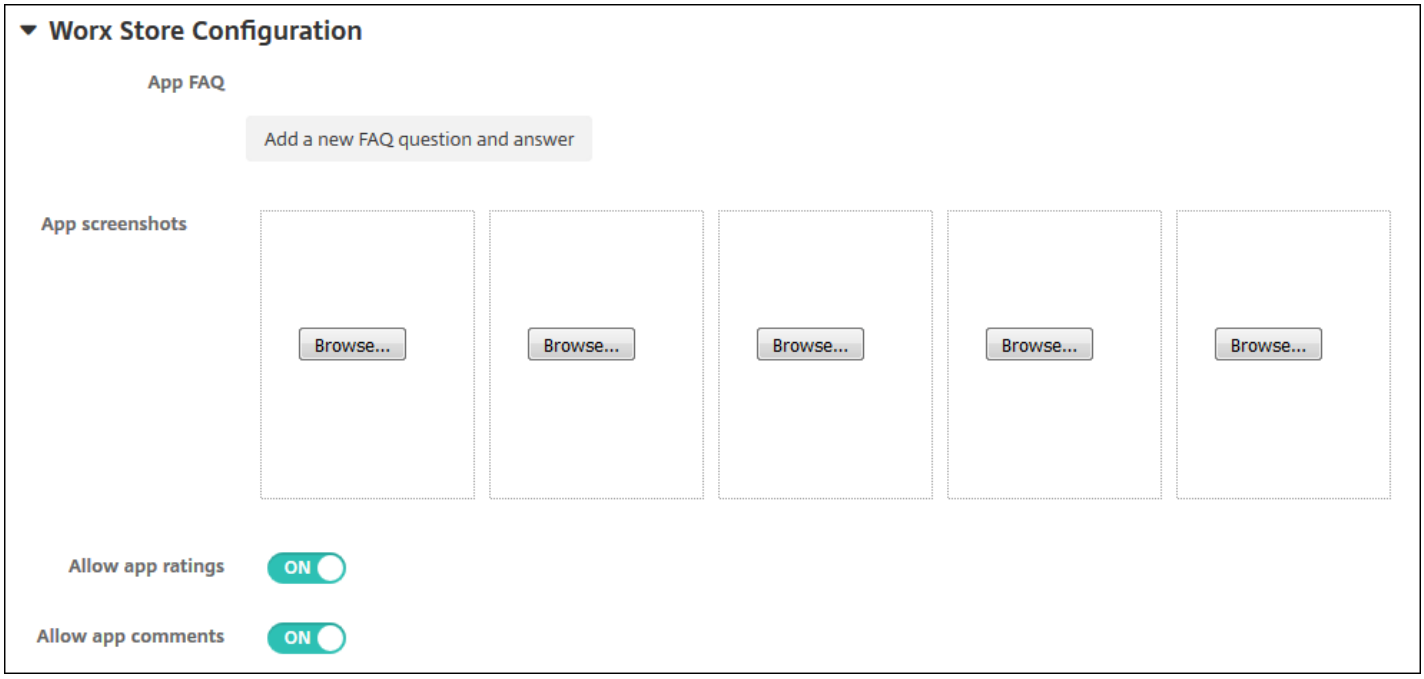
6. 次の設定を構成します。

- **Name**：任意で、アプリケーション名を変更します。
- **Description**：任意で、アプリケーションの説明を変更します。
- **App category**：任意で、アプリケーションカテゴリを変更します。

7. **[Next]**をクリックします。 最初に選択したプラットフォームのページが開きます。 選択したプラットフォームごとに、以下の操作を行います。

- **[Upload]**をクリックしてアップロードするファイルの場所に移動し、置き換えるファイルを選択します。 アプリケーションがXenMobileにアップロードされます。
- 任意で、プラットフォームのアプリケーションの詳細とポリシー設定を変更します。
- 任意で、展開規則の構成（手順7を参照）およびWorx Storeの構成（手順8を参照）を行います。

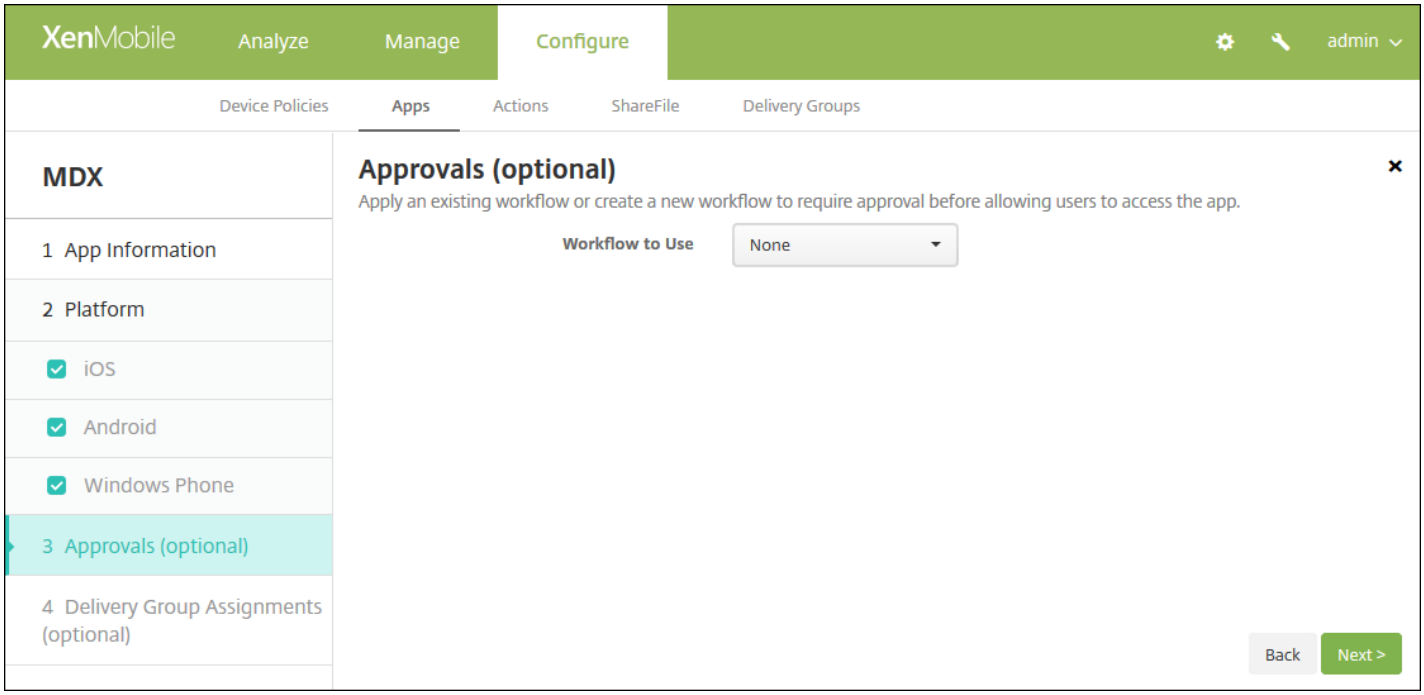
9. **[Worx Store Configuration]**を展開します。



任意で、アプリケーションに関するFAQや、Worx Storeに表示される画面キャプチャを追加できます。 また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ**：アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots**：アプリケーションをWorx Storeで分類しやすくするための画面キャプチャを追加します。 アップロードするグラフィックはPNGである必要があります。 GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings**：ユーザーにアプリケーションの評価を許可するかどうかを選択します。 デフォルトは**[ON]**です。
  - **Allow app comments**：選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。 デフォルトは**[ON]**です。

10. **[Next]**をクリックします。 **[Approvals]**ページが開きます。



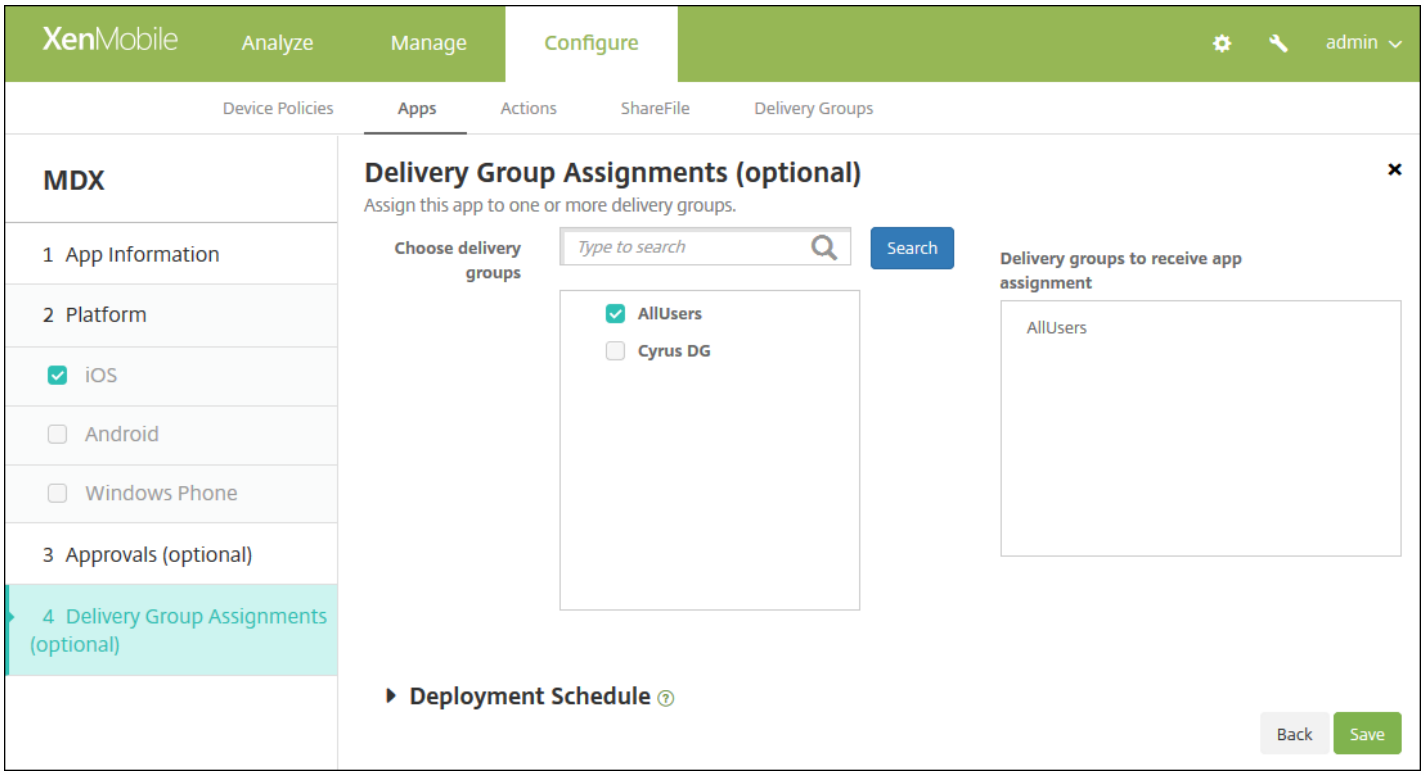
11. ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。 承認ワークフローを設定する必要がない場合は、手順12に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use**：一覧から既存のワークフローを選択するか、**[Create a new workflow]**をクリックします。 デフォルトは、Noneです。
- **[Create a new workflow]**を選択した場合は、次の設定を構成します。
  - **Name**：ワークフローの固有の名前を入力します。
  - **Description**：任意で、ワークフローの説明を入力します。
  - **Email Approval Templates**：一覧から、割り当てる電子メール承認テンプレートを選択します。 このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。 デフォルトは**[1 level]**です。 選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers**：検索フィールドに、追加で必要なユーザーの名前を入力して、**[Search]**をクリックします。 名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。 ユーザーの名前とメールアドレスが**[Selected additional required approvers]**の一覧に表示されます。
  - [Selected additional required approvers]の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[Search]**をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して**[Search]**をクリックし、検索結果を絞り込みます。
    - **[Selected additional required approvers]**の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。 一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにしま

す。

12. [**Next**] をクリックします。 [**Deliver Group Assignment**] ページが開きます。



13. [**Choose delivery groups**] の横に、アプリケーションを割り当てるデリバリーグループを入力して検索するか、一覧てグループを選択します。 選択したグループが [**Delivery groups to receive app assignment**] 一覧に表示されます。

14. [**Deployment Schedule**] を展開して以下の設定を構成します。

- [**Deploy**] の横の [**ON**] をクリックすると展開がスケジュールされ、[**OFF**] をクリックすると展開が行われません。 デフォルトのオプションは [**ON**] です。 [**OFF**] を選択した場合、そのほかのオプションを構成する必要はありません。
- [**Deployment schedule**] の横の [**Now**] または [**Later**] をクリックします。 デフォルトのオプションは [**Now**] です。
- [**Later**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [**Deployment condition**] の横の [**On every connection**] をクリックするか、[**Only when previous deployment has failed**] をクリックします。 デフォルトのオプションは、[**On every connection**] です。
- [Deploy for always-on connection] の横の [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] です。

注：

- このオプションは、[**Settings**] の [**Server Properties**] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 [**Deploy for always on connection**] は適用されません。

15. [**Save**] をクリックします。 [**Apps**] ページが開きます。

16. 手順2でアプリケーションを無効にした場合は、次の手順に従います。

- [**Apps**] の表で更新したアプリケーションをクリックして選択し、表示されるメニューで [**Enable**] をクリックします。
- 確認ダイアログボックスが表示されたら、[**Enable**] をクリックします。 これで、ユーザーがアプリケーションにアクセスでき、アプリケーションのアップグレードを求める通知を受信できるようになりました。

Microsoft Office 365アプリの有効化

Aug 30, 2016

MDXコンテナーを開いて、WorxMail、WorxWeb、およびShareFileがMicrosoft Office 365アプリにドキュメントやデータを転送するようにできます。 詳しくは、「Office 365とWorxMail、WorxWeb、ShareFileとの対話式操作を有効にする」を参照してください。

MDXアプリケーションポリシーの概要

Aug 02, 2016

制限事項とCitrixの推奨事項が注に記載されたiOS、Android、およびWindows PhoneのMDXアプリケーションポリシーの一覧については、MDX Toolkitのドキュメントの「MDXアプリケーションポリシーの概要」を参照してください。

XenMobileおよびShareFileアプリでのSAMLを使用するシングルサインオンの構成

Oct 25, 2016

XenMobileとShareFileを構成し、セキュリティアサーションマークアップランゲージ（SAML）を使用して、MDXツールキットでラップされたShareFile Mobileアプリはもちろん、Webサイト、Outlook Plug-in、Syncクライアントなどのラップされていないシングルサインオンアクセス（SSO）を提供することができます。

- **ラップされている ShareFile アプリの場合。** ShareFile Mobileアプリを介してShareFileにログオンするユーザーは、ユーザー認証のためにWorx Homeにリダイレクトされ、SAMLトークンを取得します。 認証が成功した後で、ShareFile Mobileアプリから ShareFile にSAMLトークンが送信されます。 最初のログオンの後は、ユーザーはSSOを介してShareFile Mobileアプリにアクセスし、毎回ログオンしなくてもWorxMailのメールにShareFileからドキュメントを添付できます。
- **ラップされていない ShareFile クライアントの場合。** Webブラウザーまたはほかの ShareFile クライアントを介して ShareFile にログオンするユーザーは、ユーザー認証のためにXenMobileにリダイレクトされ、SAMLトークンを取得します。 認証が成功した後で、SAMLトークンが ShareFile に送信されます。 最初のログオンの後は、毎回ログオンしなくてもユーザーはSSOを介して ShareFile クライアントにアクセスできます。

リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の「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。

前提条件

XenMobileおよびShareFileアプリにSSOを構成する前に、以下の前提条件を満たす必要があります。

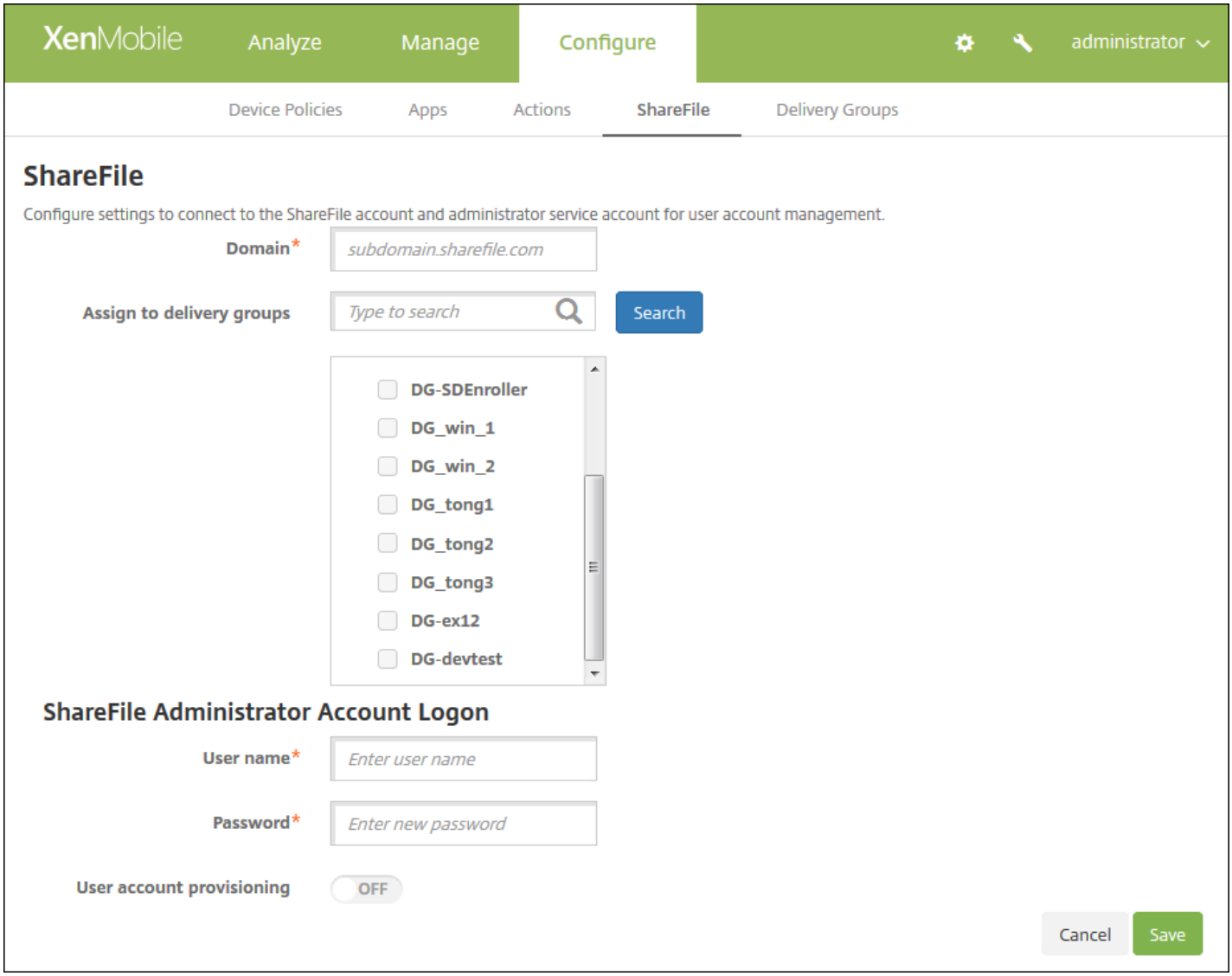
- MDX Toolkit Version 9.0.4移行（ShareFile Mobileアプリ用）
- 適切なShareFile Mobileアプリ：
  - ShareFile for iPhone Version 3.0.x
  - ShareFile for iPad Version 2.2.x
  - ShareFile for Android Version 3.2.x
- Worx Home 9.0（ShareFile Mobileアプリケーション用） - 必要に応じて、iOSまたはAndroidバージョンをインストールします。
- ShareFile管理者アカウント

XenMobileおよびShareFileに接続できることを確認します。

ShareFileアクセスを構成する

ShareFileのためにSAMLを設定する前に、以下のようにShareFileアクセス情報を入力します。

1. XenMobile Webコンソールで、［**Configure**］の［**ShareFile**］をクリックします。 ［**ShareFile**］構成ページが開きます。



2. 次の設定を構成します。

- **Domain**：ShareFileサブドメイン名を入力します。たとえば、「example.sharefile.com」です。
- **Assign to delivery groups**：ShareFileと共にSSOを使用するデリバリーグループを選択または検索します。
- **ShareFile Administrator Account Logon**
  - **User name**：ShareFile管理者のユーザー名を入力します。 このユーザーには管理特権が必要です。
  - **Password**：ShareFile管理者のパスワードを入力します。
  - **User account provisioning**：XenMobileでユーザープロビジョニングを有効にする場合はこのオプションをオンにします。ユーザープロビジョニングにShareFile User Management Toolを使用する計画である場合は無効のままにします。

    注：選択した役割にShareFileアカウントを持たないユーザーが含まれる場合も、［User account provisioning］が有効であればそのユーザーに自動的にShareFileアカウントがプロビジョニングされます。 構成をテストするために、メンバーが少ない役割を使用することをお勧めします。 これにより、多くのユーザーがShareFileアカウントを持たない可能性を避けることができます。

3. ［**Save**］をクリックします。

ラップされたShareFile MDXアプリケーション用のSAMLの設定

以下の手順がiOSおよびAndroidのアプリおよびデバイスに当てはまります。

1. MDX ToolkitでShareFile Mobileアプリをラップします。 MDX Toolkitによるアプリのラップについて詳しくは、「MDX Toolkitによるアプリケーションのラップ」を参照してください。

2. XenMobileコンソールで、ラップされたShareFile Mobileアプリをアップロードします。 MDXアプリケーションのアップロードについて詳しくは、「MDXアプリケーションをXenMobileに追加するには」を参照してください。

3. 「ShareFileアクセスを構成する」で構成した管理者のユーザー名とパスワードでShareFileにログオンしてSAML設定を検証します。

4. ShareFileおよびXenMobileが同じタイムゾーンで構成されていることを確認します。

注：構成したタイムゾーンに関して、XenMobileに正しい時刻が表示されていることを確認します。 正しい時刻が表示されていない場合は、SSOエラーが発生している可能性があります。

ShareFile Mobileアプリを検証する

1. まだ行っていない場合は、ユーザーデバイスにWorx Homeをインストールして構成します。

2. Worx StoreからShareFile Mobileアプリをダウンロードしてインストールします。

3. ShareFile Mobileアプリを開始します。 ユーザー名やパスワードの入力を求められずにShareFileが開始されます。

WorxMailで検証する

1. まだ行っていない場合は、ユーザーデバイスにWorx Homeをインストールして構成します。

2. Worx StoreからWorxMailをダウンロード、インストール、および設定します。

3. 新規メールを開いて **[ShareFileから添付]** をタップします。 メールに添付できるファイルがユーザー名とパスワードを入力しなくても表示されます。

ほかのShareFileクライアントのためにNetScaler Gatewayを構成する

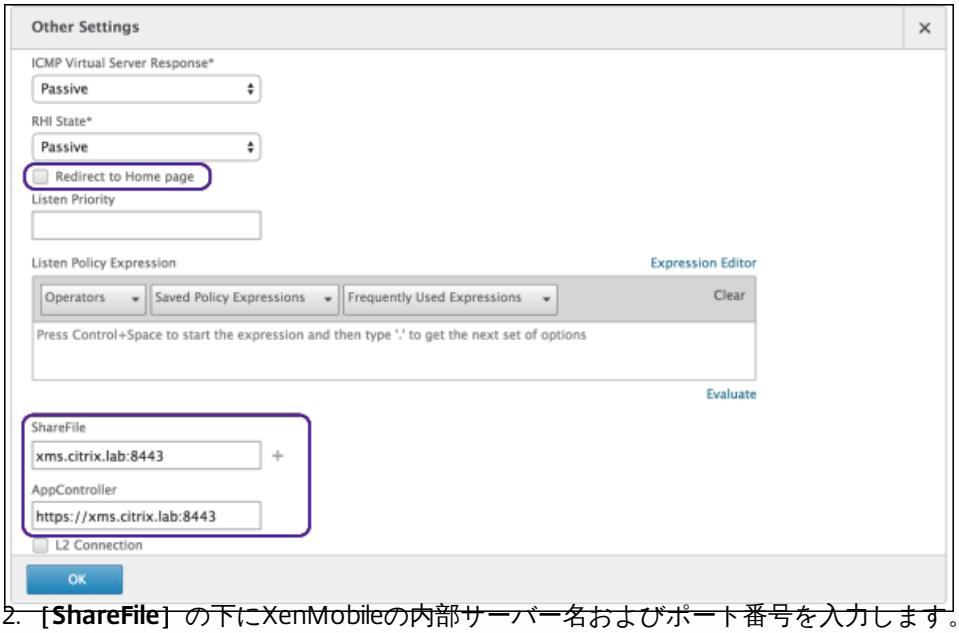
Webサイト、Outlook Plug-in、Syncクライアントなどのラップされていないクライアントへのアクセスを構成するには、以下のようにNetScaler Gatewayを構成して、SAML IDプロバイダーとしてのXenMobileの使用をサポートする必要があります。

- ホームページのリダイレクトを無効にする。
- ShareFileのセッションポリシーとプロファイルを作成する。
- NetScaler Gateway仮想サーバーにポリシーを構成する。

ホームページのリダイレクトを無効にする

構成されたホームページの代わりに本来要求された内部URLをユーザーが見られるように、/cginfraパスから送られる要求に対するデフォルトの動作を無効にする必要があります。

1. XenMobileのログオンに使用されるNetScaler Gateway仮想サーバーの設定を編集します。 NetScaler 10.5で、**[Other Settings]** に移動して **[Redirect to Home Page]** チェックボックスをオフにします。



2. [**ShareFile**] の下にXenMobileの内部サーバー名およびポート番号を入力します。

3. [**AppController**] の下にXenMobileのURLを入力します。

この構成により、/cginfraパスを介して入力したURLに対する要求が承認されます。

ShareFileのセッションポリシーと要求プロファイルを作成する

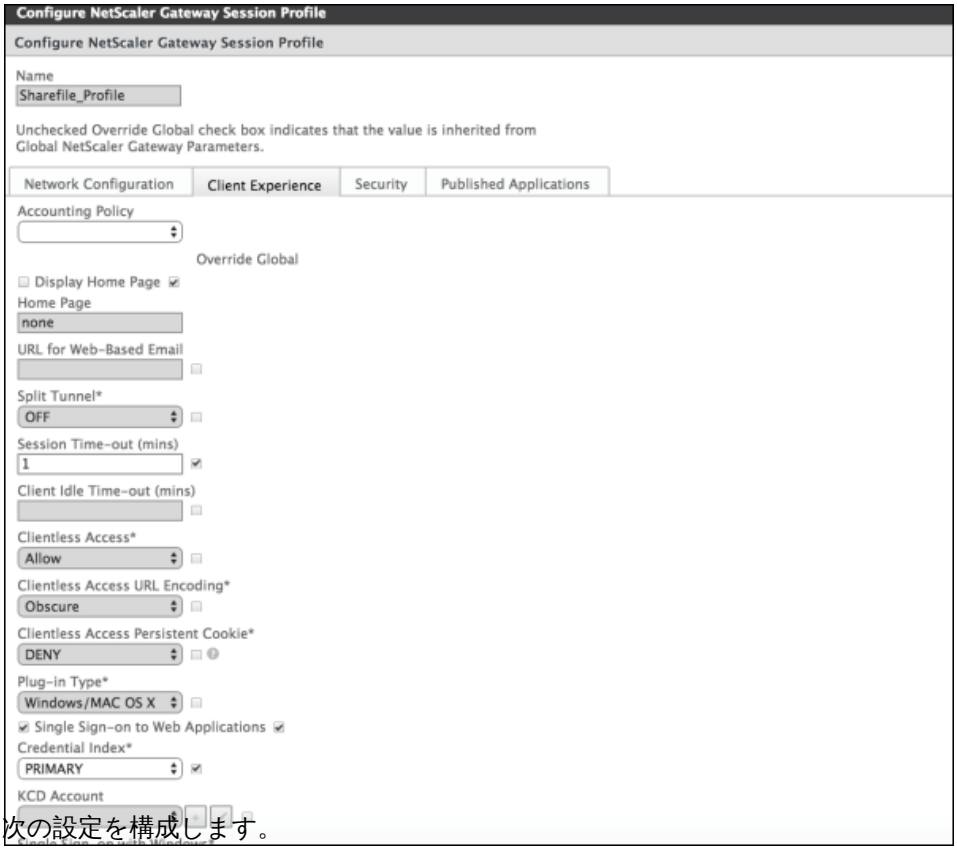
以下の設定を構成してShareFileセッションポリシーと要求プロファイルを作成します。

1. NetScaler Gateway構成ユーティリティの左側のナビゲーションペインで、[**NetScaler Gateway**]、[**Policies**]、[**Session**] の順にクリックします。

2. 新しいセッションポリシーを作成します。[**Policies**] タブで [**Add**] をクリックします。

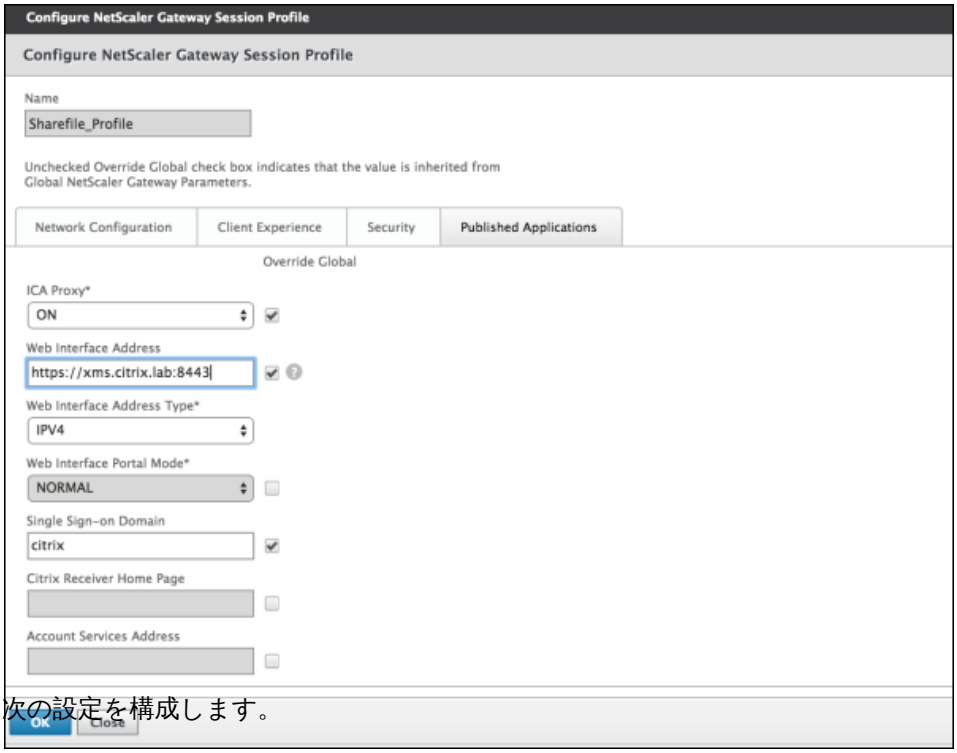
3. [**Name**] ボックスに「**ShareFile_Policy**」と入力します。

4. [**+**] をクリックして新しい操作を作成します。[**Create NetScaler Gateway Session Profile**] ページが開きます。



次の設定を構成します。

- **Name**：「ShareFile_Profile」と入力します。
- **[Client Experience]** タブをクリックし、以下の設定を構成します。
  - **Home Page**：「none」と入力します。
  - **Session Time-out (mins)**：「1」と入力します。
  - **Single Sign-on to Web Applications**：この設定を選択します。
  - **Credential Index**：一覧で［PRIMARY］をクリックします。
- **[Published Applications]** タブをクリックします。



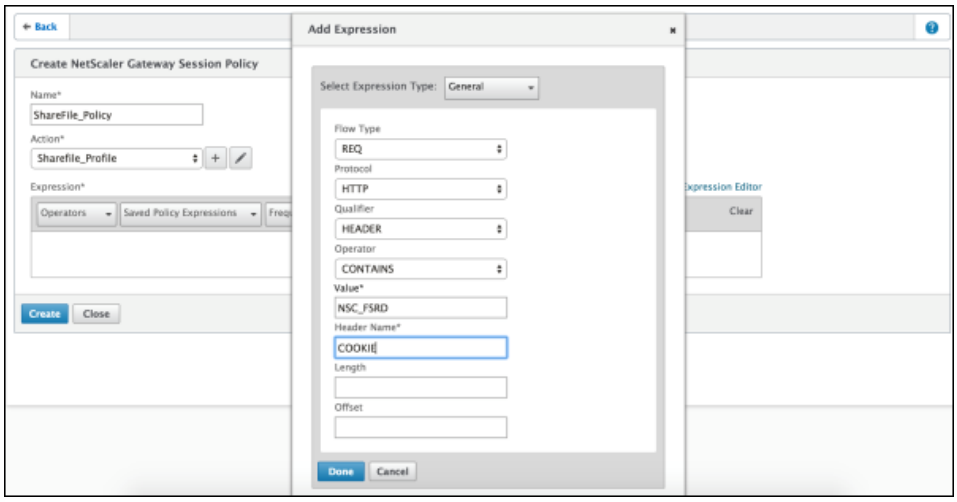
次の設定を構成します。

- o **ICA Proxy**：一覧で［**ON**］を選択します。
- o **Web Interface Address**：XenMobileサーバーのURLを入力します。
- o **Single Sign-on Domain**：Active Directoryドメイン名を入力します。

  注：WNetScaler Gatewayセッションプロファイルを構成するとき、［**Single Sign-on Domain**］に入力するドメインサフィックスをLDAPに定義するXenMobileドメインエイリアスと一致させる必要があります。

5. ［**Create**］をクリックしてセッションプロファイルを定義します。

6. ［**Expression Editor**］をクリックします。



次の設定を構成します。

- **Value**：「NSC_FSRD」と入力します。
- **Header Name**：「COOKIE」と入力します。

- ［**Done**］をクリックします。

7. ［**Create**］をクリックして［**Close**］をクリックします。

NetScaler Gateway仮想サーバーにポリシーを構成する

以下の設定をNetScaler Gateway仮想サーバーに構成します。

NetScaler Gateway構成ユーティリティの左側のナビゲーションペインで、［**NetScaler Gateway**］の［**Virtual Servers**］をクリックします。

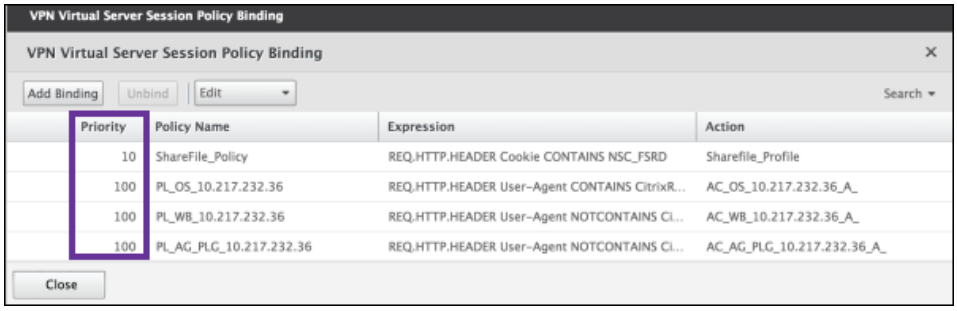
2. ［**Details**］ペインでNetScaler Gateway仮想サーバーをクリックします。

3. ［**Edit**］をクリックします。

4. ［**Configured policies**］の［**Session policies**］をクリックし、［**Add binding**］をクリックします。

5. ［**ShareFile_Policy**］を選択します。

6. 以下の図に示すように、このポリシーの優先順位が一覧表示されるほかのポリシーよりも高くなるように、選択したポリシーに対して自動生成される［**Priority**］の番号を最も小さい数に変更します。



7. ［**Done**］をクリックして、NetScaler構成を保存します。

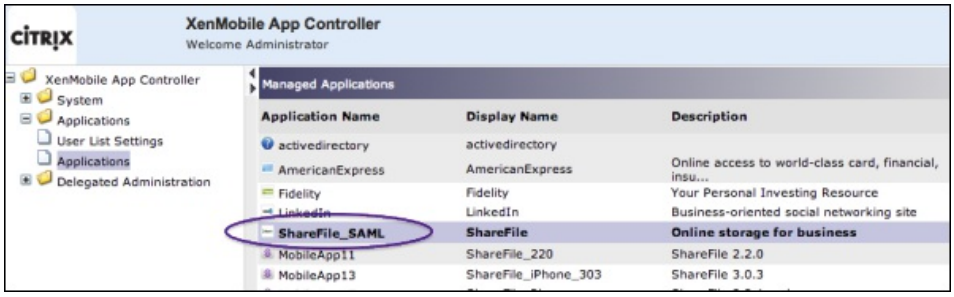
非MDX ShareFileアプリに対してSAMLを構成する

以下の手順に従って、ShareFile構成のための内部アプリ名を見つけます。

1. 「**https://:4443/OCA/admin/**」にアクセスしてXenMobile管理ツールにログオンします。「OCA」は必ず大文字で入力してください。

2. ［**View**］の一覧で、［**Configuration**］をクリックします。

3. **[Applications]** の **[Applications]** をクリックし、 **[Display Name]** が「ShareFile」のアプリの **[Application Name]** を記録します。



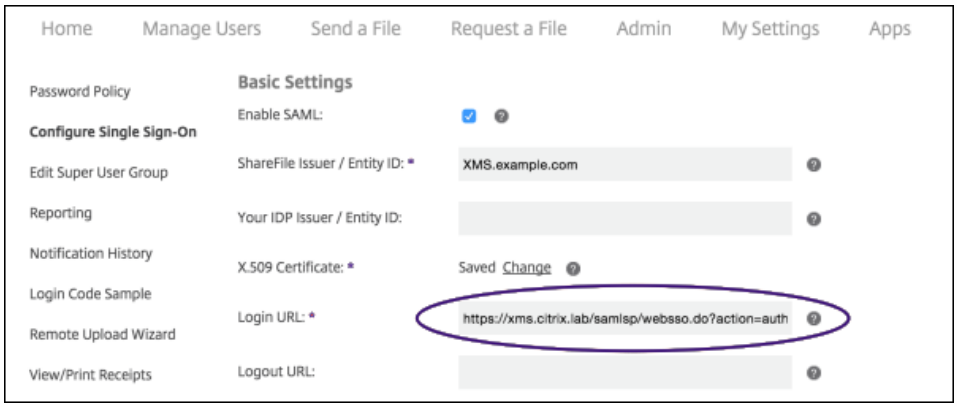
ShareFile.comのSSO設定を変更する

1. ShareFileアカウント（https://.sharefile.com）にShareFile管理者としてログオンします。

2. ShareFileのWebインターフェイスで **[管理]** をクリックし、 **[シングルサインオンの構成]** を選択します。

3. **[ログインURL]** を以下のように編集します。

[ログインURL] は「https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1」のように表示されているはずです。



- NetScaler Gateway仮想サーバーの外部FQDNおよび「/cginfra/https/」をXenMobileサーバーのFQDNの前に挿入し、XenMobileサーバーのFQDNの後に「8443」を追加します。

  これで、URLは「https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1」のようになるはずです。

- パラメーター**&app=ShareFile_SAML_SP**を、「非MDX ShareFileアプリに対してSAMLを構成する」の手順3で確認したShareFile内部アプリ名に変更します。 デフォルトで内部名は「**ShareFile_SAML**」ですが、構成を変更するたびに数字が内部名に付加されます（ShareFile_SAML_2、ShareFile_SAML_3など）。

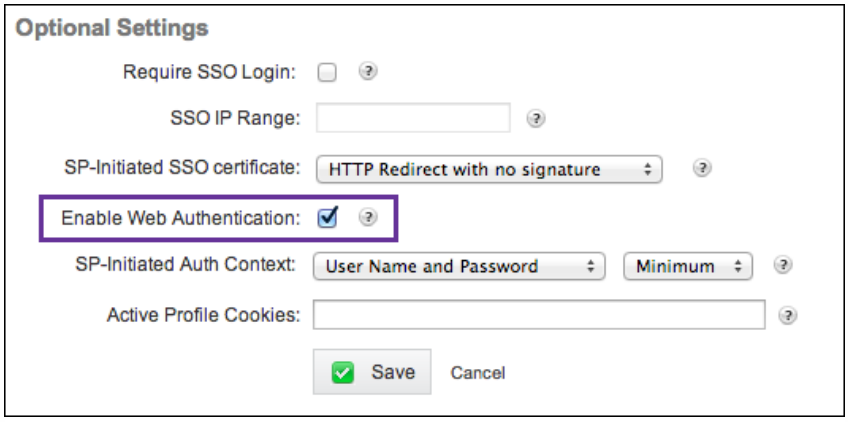
  これで、URLは「https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1」のようになるはずです。

- 「&nssso=true」をURLの最後に追加します。

  これで、変更したURLは「https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**」のようになるはずです。

  重要：XenMobileコンソールでShareFileアプリを編集または再作成したりShareFile設定を変更したりするたびに、内部アプリ名に新しい番号が付加されます。これは、ShareFile Webサイトでログインも更新して、更新されたアプリ名を反映する必要があるということを意味します。

4. **[オプション設定]**の下の**[Web認証の有効化]**チェックボックスをオンにします。



構成を検証する

以下の操作を実行して構成を検証します。

1. ブラウザーでhttps://sharefile.com/saml/loginにアクセスします。

NetScaler Gatewayのログオンフォームにリダイレクトされます。 リダイレクトされない場合は前の構成設定を検証します。

2. NetScaler GatewayおよびXenMobile構成環境のユーザー名とパスワードを入力します。

.sharefile.comにあるShareFileフォルダーが表示されます。 ShareFileフォルダーが表示されない場合は、正しいログオン資格情報を入力したかどうか確認します。

自動化された操作

Oct 25, 2016

XenMobileで自動化された操作を作成して、イベント、ユーザー、デバイスプロパティ、またはユーザーデバイスでのアプリケーションの存在に対する対応をプログラミングします。 自動化された操作を作成する場合は、操作のトリガーに基づいてユーザーのデバイスがXenMobileに接続されたときに、そのデバイスに及ぼす効果を設定します。 イベントがトリガーされたときに、より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信できます。

たとえば、事前にブラックリストに追加したアプリケーション（例：Words with Friends）を検出する場合は、ユーザーのデバイスでWords with Friendsが検出されたときに、そのデバイスをコンプライアンス違反に設定するトリガーを指定できます。 この操作では次に、そのアプリケーションを削除して、デバイスが再度コンプライアンス遵守状態に戻す必要があることが通知されます。 デバイスを選択的にワイプするなどのより深刻な操作を実行するまでに、ユーザーがコンプライアンス遵守状態に戻すのを待機する時間制限を設定できます。

自動的に発生する効果は、次の範囲から設定します。

- デバイスに選択的ワイプまたは完全なワイプを実行する。
- デバイスをコンプライアンス不遵守に設定する。
- デバイスを取り消す。
- より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信する。

注：ユーザーに通知するには、XenMobileがメッセージを送信できるように、[Settings]で通知サーバー（SMTPおよびSMS）を構成している必要があります。「XenMobileでの通知」を参照してください。 また、続行する前に使用予定の通知テンプレートを設定します。 通知テンプレートの設定について詳しくは、「XenMobileで通知テンプレートを作成または更新するには」を参照してください。

ここでは、XenMobileで自動化された操作を追加、編集、およびフィルタリングする方法について説明します。

1. XenMobileコンソールで、**[Configure]**の**[Actions]**をクリックします。 **[Actions]**ページが開きます。

2. **[Actions]**ページで、次のいずれかを行います。

- 新しい操作を追加するには**[Add]**をクリックします。
- 編集または削除する既存の操作を選択します。 使用するオプションをクリックします。

注：操作の横にあるチェックボックスをオンにすると、操作一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。

3. **[Action Information]**ページが開きます。

4. **[Action Information]**ページで、次の情報を入力または変更します。

- **Name**：操作を一意に識別する名前を入力します。 このフィールドは必須です。
- **Description**：操作の意図する内容を説明します。

5. **[Next]**をクリックします。 **[Action details]**ページが開きます。

注：次の例は**[Event]**トリガーの設定方法を示しています。 別のトリガーを選択した場合、この図で示されているものとは異なるオプションになります。

6. **[Action details]**ページで、次の情報を入力または変更します。

- **[Trigger]**の一覧で、この操作に対するイベントトリガーの種類をクリックします。 各トリガーの意味は次のとおりです。

- **Event**：定義済みのイベントに対応します。
- **Device property**：MDMモードで収集されたデバイスのデバイス属性を確認して、それに対応します。
- **User property**：ユーザー属性（通常、Active Directoryからの属性）に対応します。
- **Installed app name**：インストール中のアプリケーションに対応します。 MAM-onlyモードには適用されません。 デバイスでアプリケーションインベントリポリシーを有効にする必要があります。 デフォルトでは、アプリケーションインベントリポリシーはすべてのプラットフォームで有効です。 詳しくは、「アプリケーションインベントリデバイスポリシーを追加するには」を参照してください。

7. 次の一覧で、トリガーに対する応答をクリックします。

8. [**Action**] の一覧で、トリガーの条件が満たされたときに実行される操作をクリックします。 [**Send notification**] 以外では、トリガーの原因となった問題をユーザーが解決できる期間を選択します。 その期間内に問題が解決されない場合は、選択した操作が実行されます。 実行できるアクションは次のとおりです。

- **Selectively wipe the device**：個人のデータとアプリケーションは残して、企業のすべてのデータとアプリケーションをデバイスから消去します。
- **Completely wipe the device**：デバイスからすべてのデータやアプリケーションを消去します。デバイスに設置されている場合、メモリカードもその対象となります。
- **Revoke the device**：デバイスからXenMobileへの接続を禁止します。
- **App lock**：デバイスのすべてのアプリケーションへのアクセスを拒否します。 Androidでは、ユーザーはまったくXenMobileにログインできなくなります。 iOSでは、ユーザーはまだログインできますが、アプリケーションにアクセスできません。
- **App wipe**：Androidでは、これによりユーザーのXenMobileアカウントが削除されます。 iOSでは、これにより、ユーザーがXenMobile機能にアクセスするために必要な暗号キーが削除されます。
- **Mark the device as out of compliance**：デバイスを規則違反として設定します。
- **Send notification**：ユーザーへのメッセージの送信

以降の手順では、通知の送信方法について説明します。

9. 次の一覧で、通知に使用するテンプレートを選択します。 選択したイベントに関連する通知テンプレートが表示されます。

注：ユーザーに通知するには、XenMobileがメッセージを送信できるように、［Settings］で通知サーバー（SMTPおよびSMS）を構成している必要があります。「XenMobileでの通知」を参照してください。 また、続行する前に使用予定の通知テンプレートを設定します。 通知テンプレートの設定について詳しくは、「XenMobileで通知テンプレートを作成または更新するには」を参照してください。

注：テンプレートを選択した後、［Preview notification message］をクリックして通知をプレビュー表示できます。

10. 以下のフィールドで、操作が実行されるまでの遅延（日単位、時間単位、または分単位）と、トリガーの原因となった問題をユーザーが解決するまでに操作を繰り返す間隔を設定します。

11. [**Summary**] で、意図したとおりに、自動化された操作を作成したことを確認します。

12. アクション詳細を構成したら、プラットフォームごとに個別に展開規則を構成できます。 これを行うには、選択した各プラットフォームに対して、手順13を実行します。

14. 操作のプラットフォームの展開規則の構成が完了したら、[**Next**] をクリックします。 [**Actions assignment**] ページが 開きます。 ここで操作をデリバリーグループまたはグループに割り当てます。 この手順はオプションです。

15. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の **[Delivery groups to receive app assignment]** 一覧に表示されます。

16. [Deployment Schedule] を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。 デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。 デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。 デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[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]** です。
  注： このオプションは、 **[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。

注： 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

17. **[Next]** をクリックします。 **[Summary]** ページが 開きます。 ここで操作の構成を確認できます。

18. **[Save]** をクリックして変更を保存します。

XenMobileのマクロ

Aug 02, 2016

XenMobileでは、強力なマクロが提供されています。マクロにはいろいろな用途がありますが、たとえば、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にユーザーまたはデバイスのプロパティデータを設定できます（一部の操作の場合）。 マクロを使用すると、単一のポリシーを構成して大きなユーザーベースに展開し、各対象ユーザーに固有の値を表示させることができます。 たとえば、何千人ものユーザーがいるExchangeプロファイルにユーザーのメールボックスの値を事前に設定できます。

この機能は現在、iOSおよびAndroidデバイスの構成とテンプレートの場合にのみ使用できます。

ユーザーマクロの定義

以下のユーザーマクロは常に使用できます。

- loginname （ユーザー名 + domainname）
- username（loginname ドメイン名を除去したもの、ある場合）
- domainname （ドメイン名またはデフォルトドメイン）

以下の管理者が定義するプロパティも使用できる場合があります。

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox

- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname （前に説明したプロパティを上書きします）

さらに、ユーザーがLDAPなどの認証サーバーを使用して認証されている場合、そのストアでユーザーに関連付けられているすべてのプロパティを使用できます。

マクロの構文

マクロの形式は次のとおりです。

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

原則として、ドル記号（$）に続くすべての構文は中かっこ（{ }）で囲む必要があります。

- 修飾されたプロパティ名は、ユーザープロパティ、デバイス プロパティ、 またはカスタムプロパティを示します。
- 修飾されたプロパティ名は、プレフィックスと実際のプロパティ名で構成されます。
- ユーザープロパティの形式は、${user.[PROPERTYNAME] (prefix="user.")}です。
- デバイスプロパティの形式は、${device.[PROPERTYNAME] (prefix="device.")}です。

たとえば、${user.username}はポリシーのテキストフィールドにユーザー名の値を設定します。 これは、複数のユーザーが使用するExchange ActiveSyncプロファイルおよびそのほかのプロファイルを構成するのに便利です。

カスタムマクロ（ユーザーが定義するプロパティ）の場合、プレフィックスは${custom}です。 です。プレフィックスは省略できます。

注：プロパティ名の大文字と小文字は区別されます。

XenMobileクライアント設定

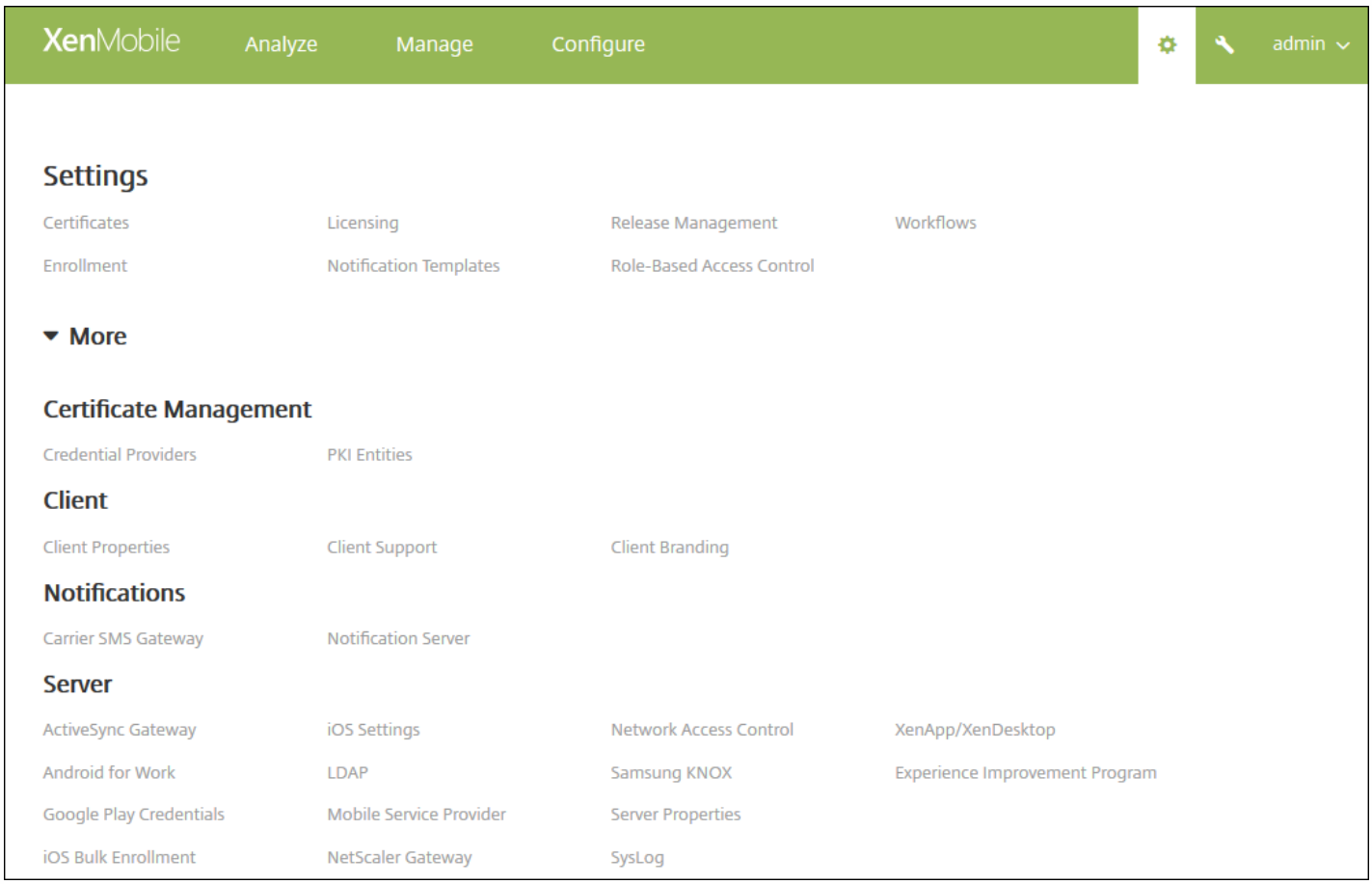
Aug 02, 2016

XenMobileコンソールで構成するXenMobileクライアント設定には以下が含まれます。

- クライアントのプロパティ
- クライアントのサポート
- クライアントのブランド設定

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

3. ［**Client**］で、構成するオプションをクリックします。



iOSデバイス用のカスタムWorx Storeブランド設定を作成するには

Oct 25, 2016

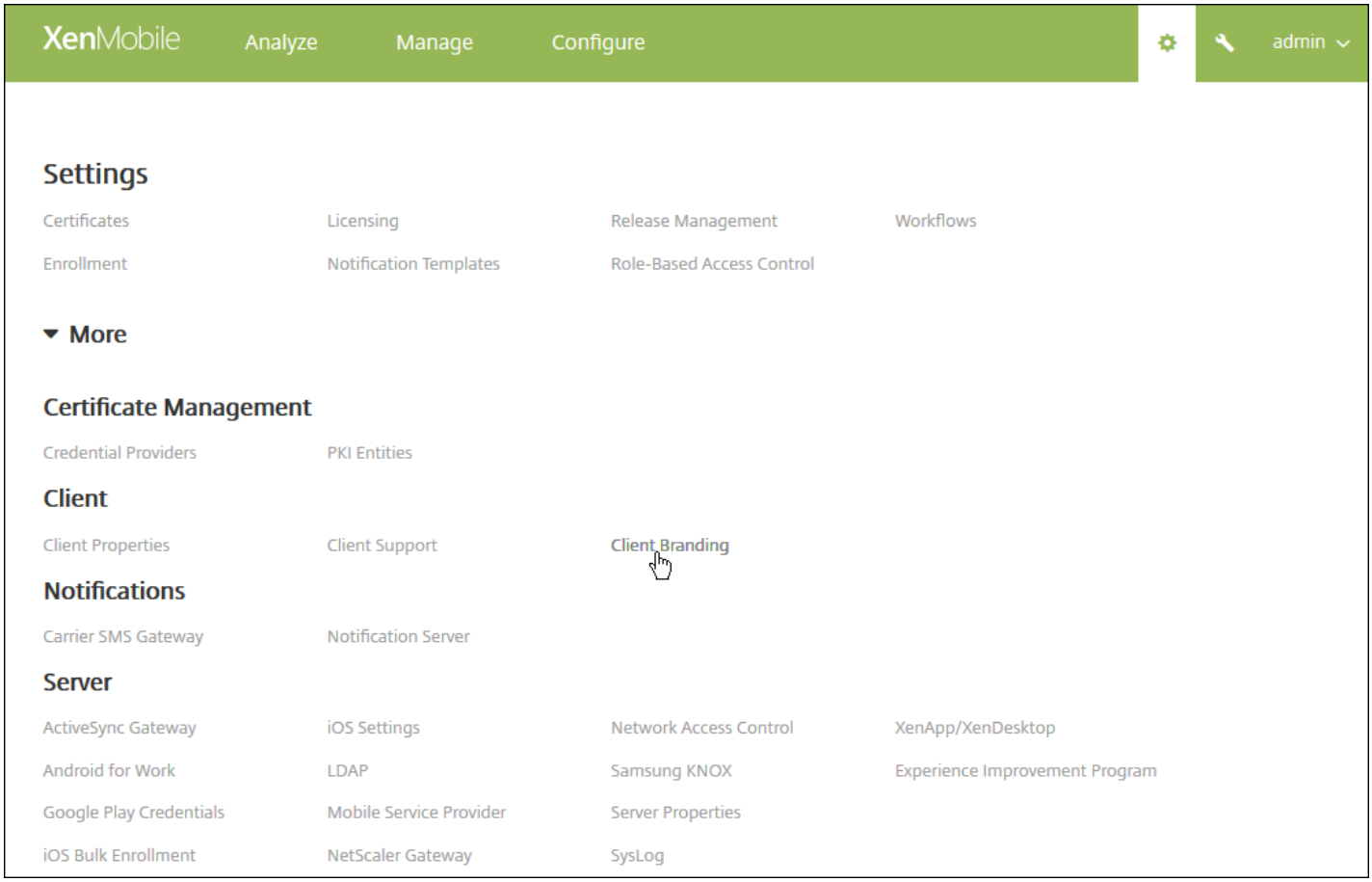
ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、iOSおよびAndroidのモバイルデバイス上でSecure HubおよびXenMobile Storeのブランドを設定することができます。

注：始める前に、カスタム画像を準備してアクセスできるようにしてください。

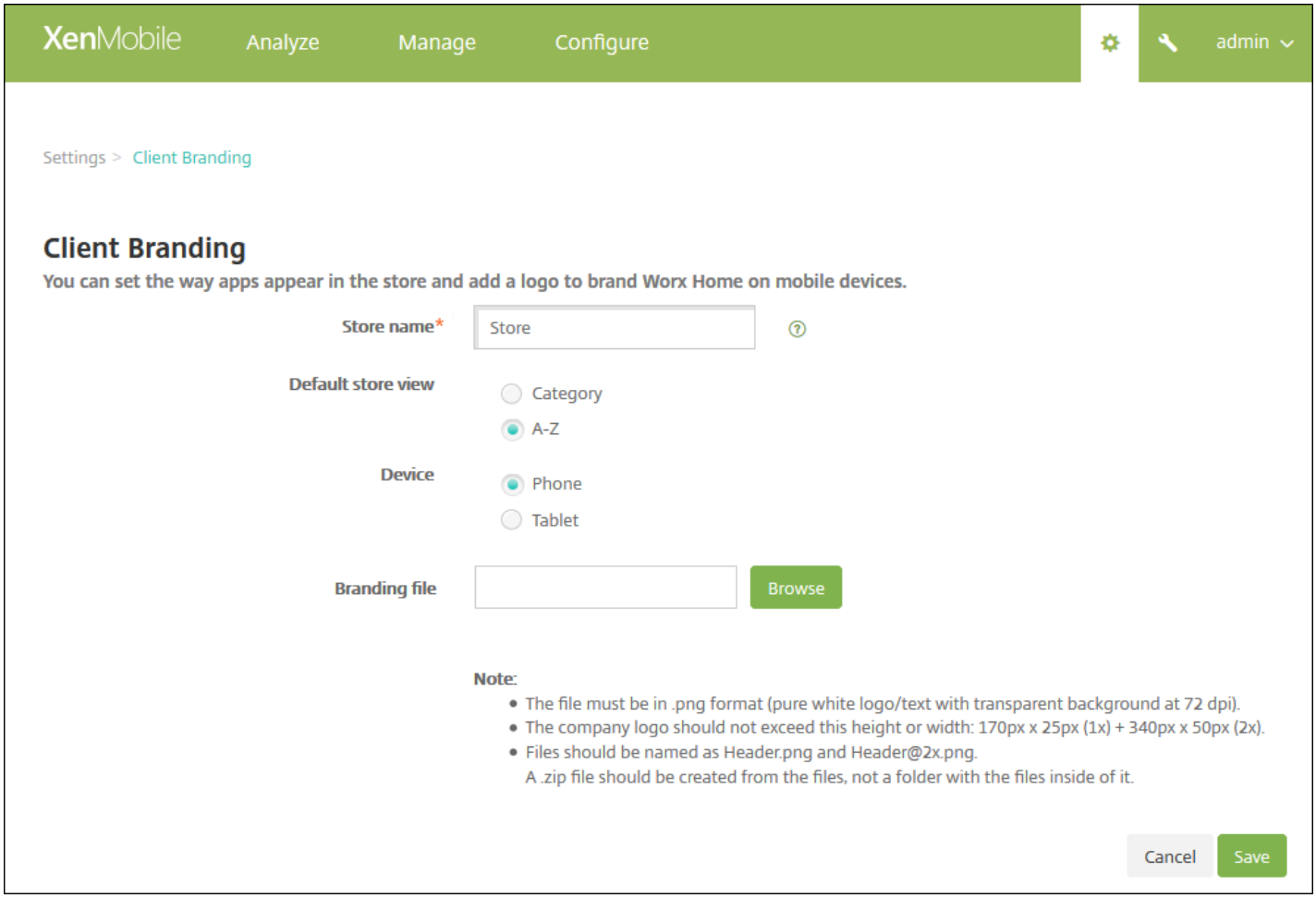
カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および340px×50px（2x）を超過しないようにする必要があります。
- ファイルの名前はHeader.pngおよびHeader@2x.pngにします。
- ファイルを含むフォルダーではなく、ファイルから.zipファイルを作成します。

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



2. ［**Client**］の下の［**Create Branding**］をクリックします。［**Client Branding**］ページが開きます。



次の設定を構成します。

- **Store name**：ユーザーのアカウント情報に含まれるストア名が表示されます。 この名前を変更すると、ストアサービスへのアクセスに使用されるURLも変更されます。 通常、デフォルトの名前をそのまま使用します。
- **Default store view**：［**Category**］または［**A-Z**］を選択します。 デフォルトは［**A-Z**］です。
- **Device option**：［**Phone**］または［**Tablet**］を選択します。 デフォルトは［**Phone**］です。
- **Branding file**：［**Browse**］をクリックしてブランド設定に使用するイメージまたはイメージの.zipファイルの場所に移動し、ファイルを選択します。

3. ［**Save**］をクリックします。

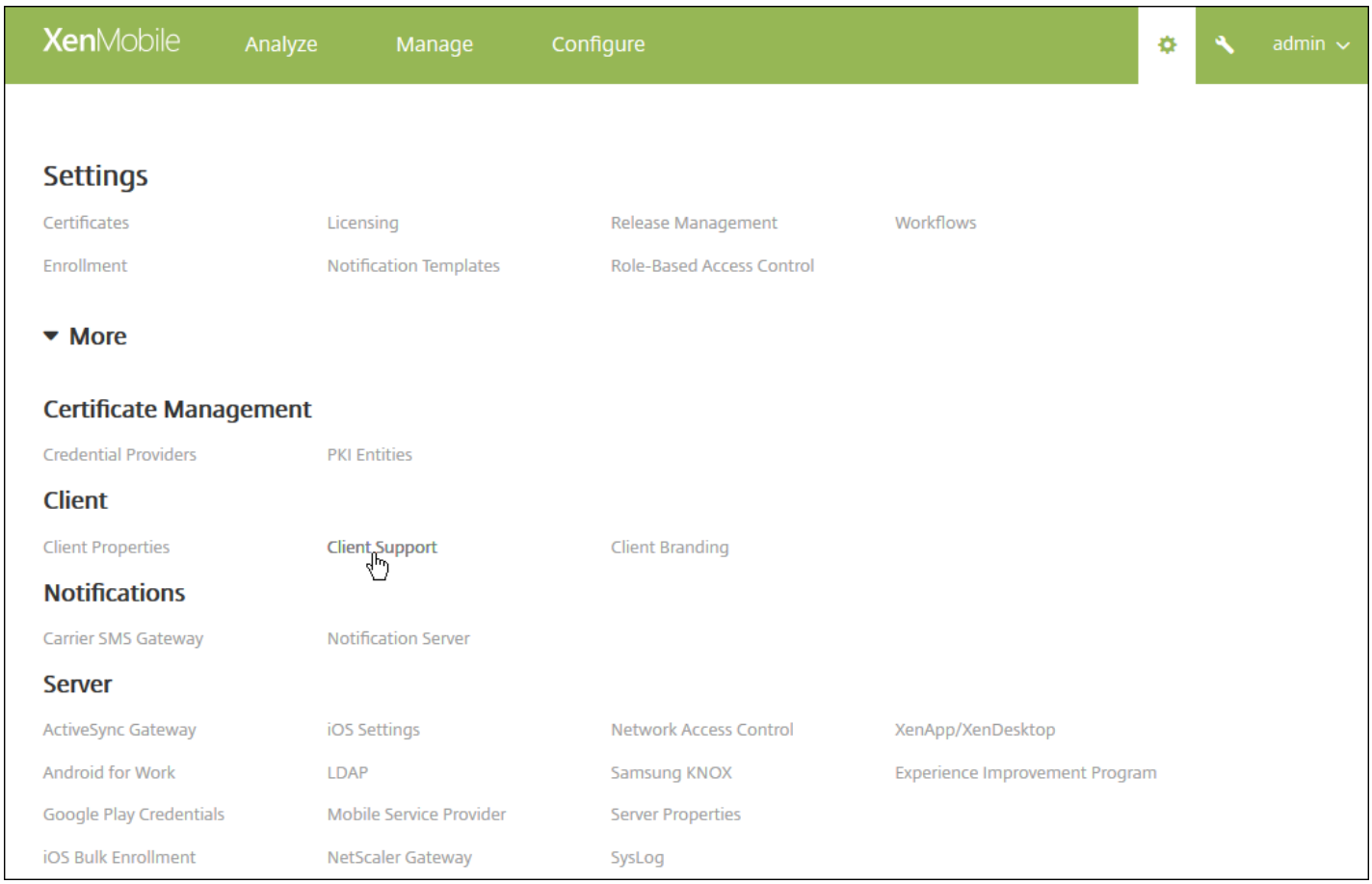
このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、パッケージをユーザーのデバイスに展開する必要があります。

Worx HomおよびGoToAssistサポートオプションの作成

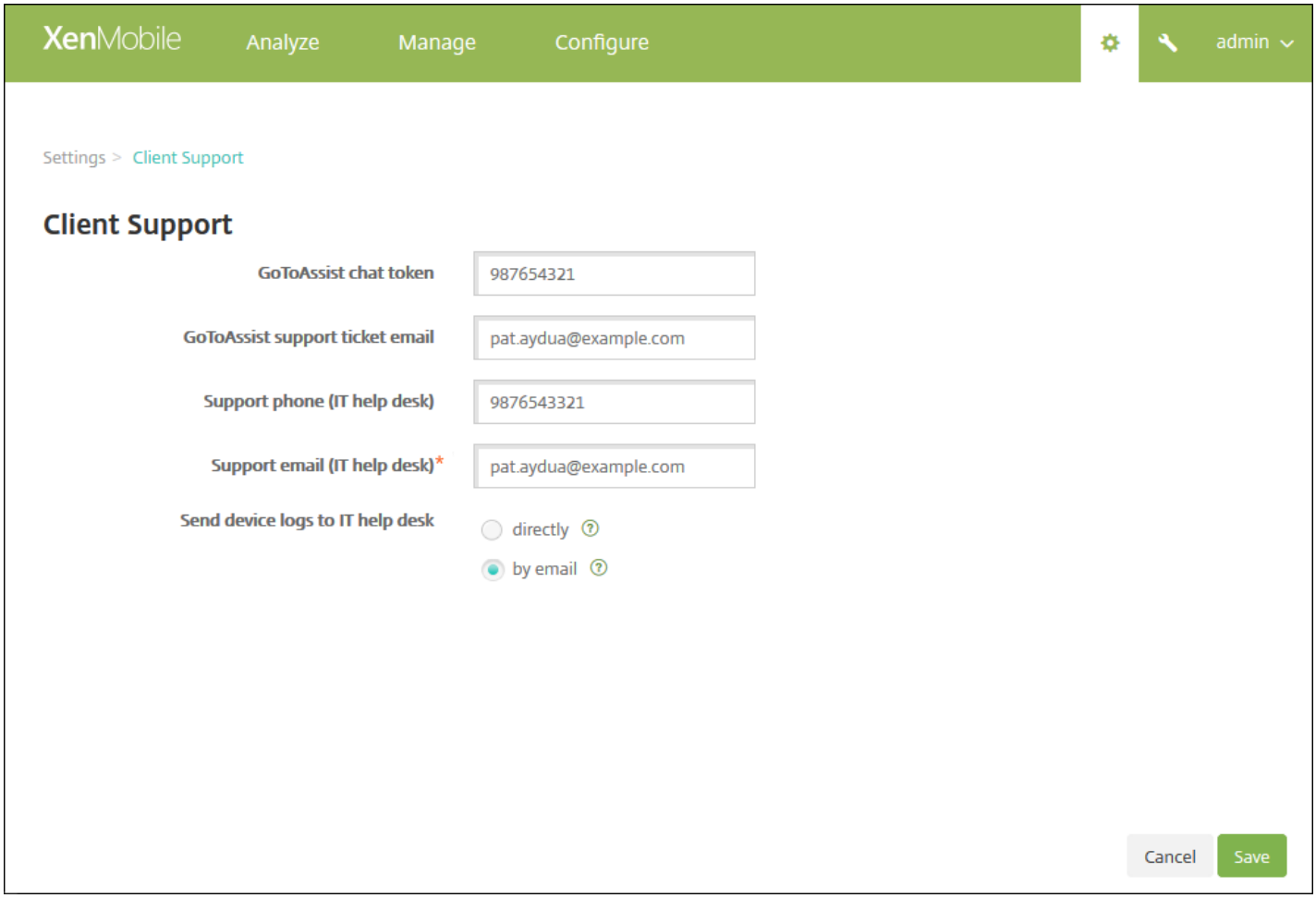
Oct 25, 2016

メールアドレス、電話番号、およびGoToAssistトークンを指定することにより、サポートスタッフへのさまざまな連絡方法をユーザーに提供できます。 ユーザーがデバイスからサポートを要求すると、管理者が設定したオプションが表示されます。

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



2. **[Client]** の下の **[Client Support]** をクリックします。 **[Client Support]** ページが開きます。



3. 次の設定を構成します。

- **GoToAssist chat token**：GoToAssistセッションを開始するためにユーザーに提供されるトークンを入力します。
- **GoToAssist support ticket email**：GoToAssistサポートチケットで使用するメールアドレスを入力します。
- **Support phone (IT help desk)**：ITヘルプデスクの電話番号を入力します。
- **Support email (IT help desk)**：ITヘルプデスク担当者のメールアドレスを入力します。
- **Send device logs to IT help desk**：デバイスログの送信方法として［**directly**］または［**by email**］を選択します。 デフォルトは［**by email**］です。
  - ［**directly**］を有効にすると、［ShareFile にログを保存］の設定が表示されます。 ［ShareFile にログを保存］を有効にすると、ログが直接ShareFileに送信されます。有効にしない場合、ログはXenMobileに送信された後、ITヘルプデスクにメールで送信されます。 さらに、 ［**If sending directly fails, use email**］オプションが表示されます。このオプションはデフォルトで有効化されています。 サーバーに問題が生じたときにログの送信にクライアントのメールを使用しない場合は、このオプションを無効にすることができます。 ただし、このオプションを無効にすると、サーバーに問題があってもログが送信されません。
  - ［**by email**］を有効にすると、常にログの送信にクライアントのメールが使用されます。

4. ［**Save**］をクリックします。

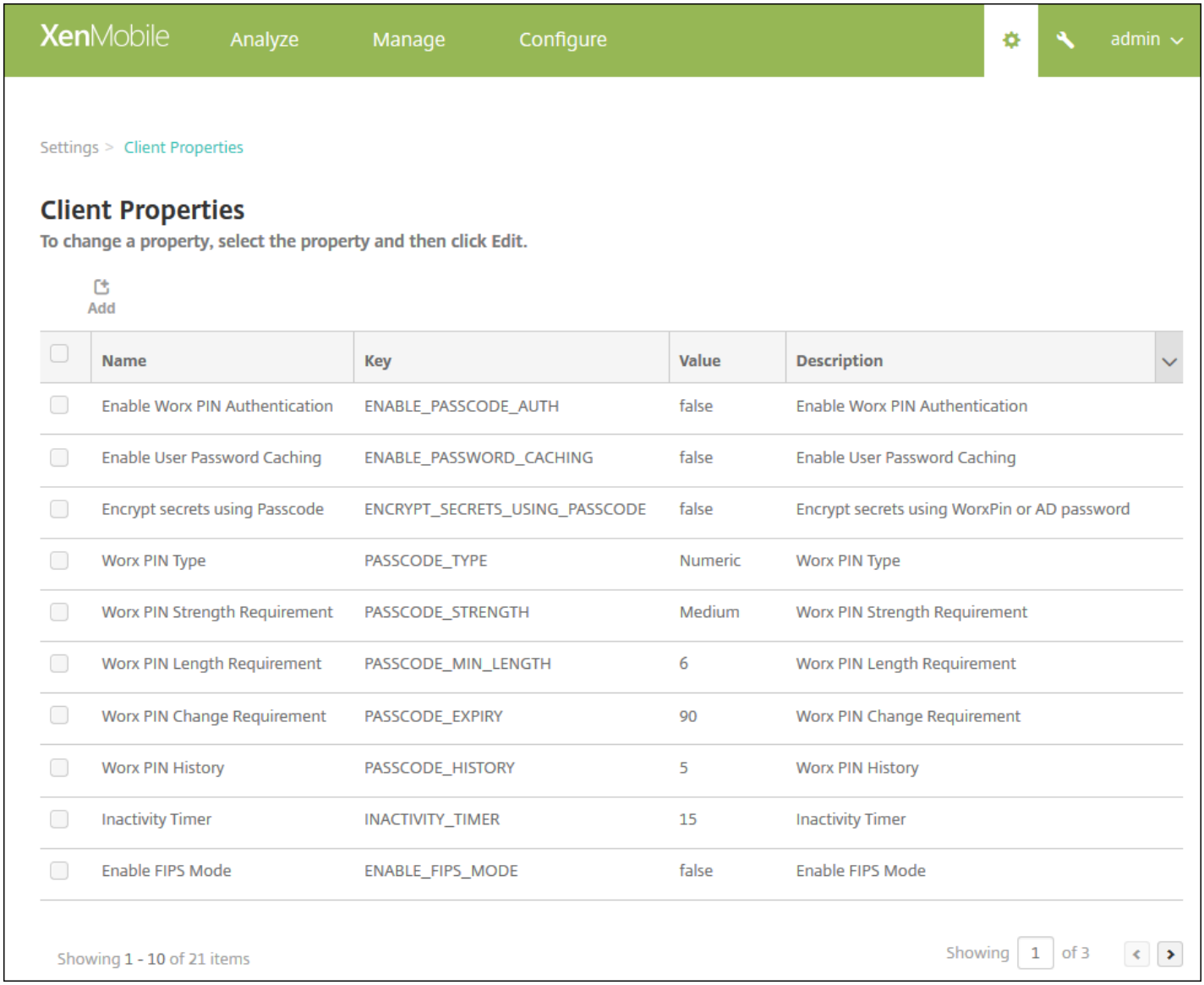
クライアントプロパティを追加、編集、または削除するには

Aug 02, 2016

クライアントプロパティには、ユーザーのデバイスのWorx Home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、Worx PINなどの詳細設定を構成することができます。 クライアントプロパティはCitrixサポートから取得します。

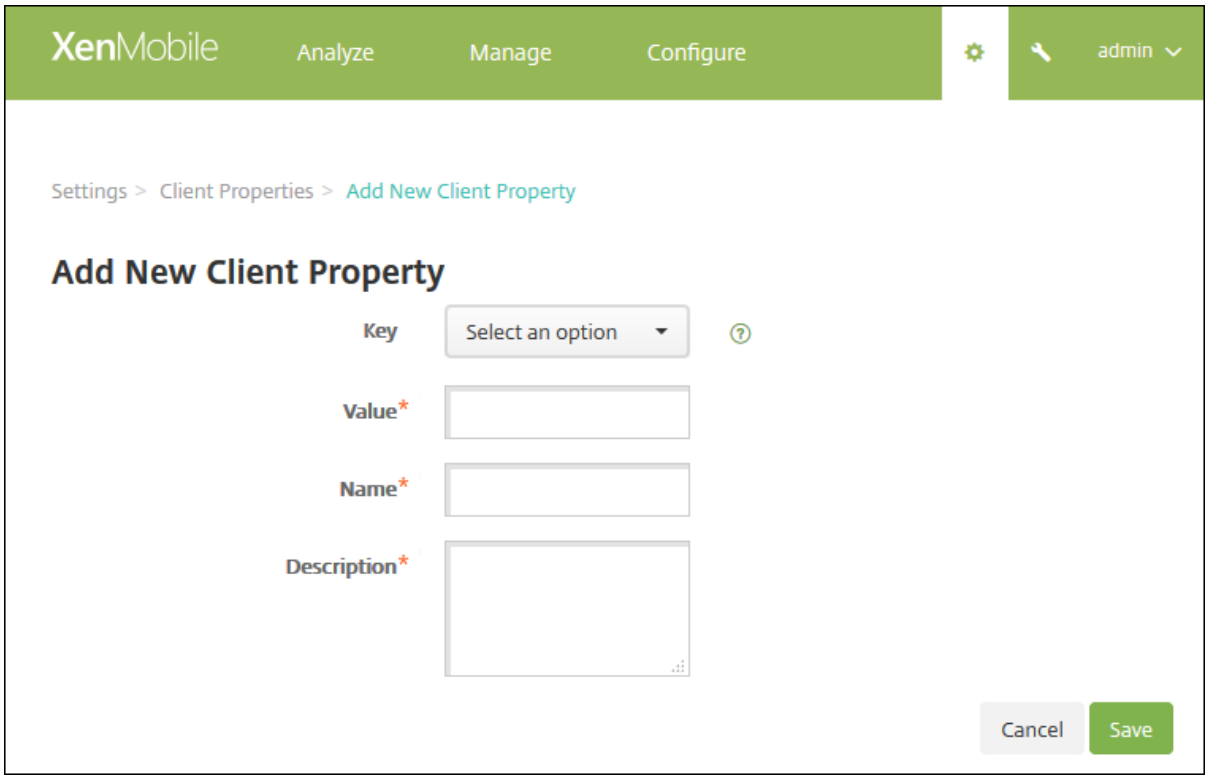
クライアントプロパティは、クライアントアプリケーション（特にWorx Home）のリリースごとに変更されます。 クライアントプロパティについて詳しくは、「クライアントプロパティリファレンス」を参照してください。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。
2. **[Client]** の下の **[Client Properties]** をクリックします。 **[Client Properties]** ページが開きます。 このページでは、クライアントプロパティを追加、編集、または削除できます。



クライアントプロパティを追加するには

1. [**Add**] をクリックします。 [**Add New Client Property**] ページが開きます。



2. 次の設定を構成します。

- **Key**：一覧から、追加するプロパティキーを選択します。**重要**：変更を行う前にCitrixのサポート担当者に問い合わせるか、変更を行うための特殊キーを要求してください。
- **Value**：選択したプロパティの値を入力します。
- **Name**：プロパティの名前を入力します。
- **Description**：プロパティの説明を入力します。

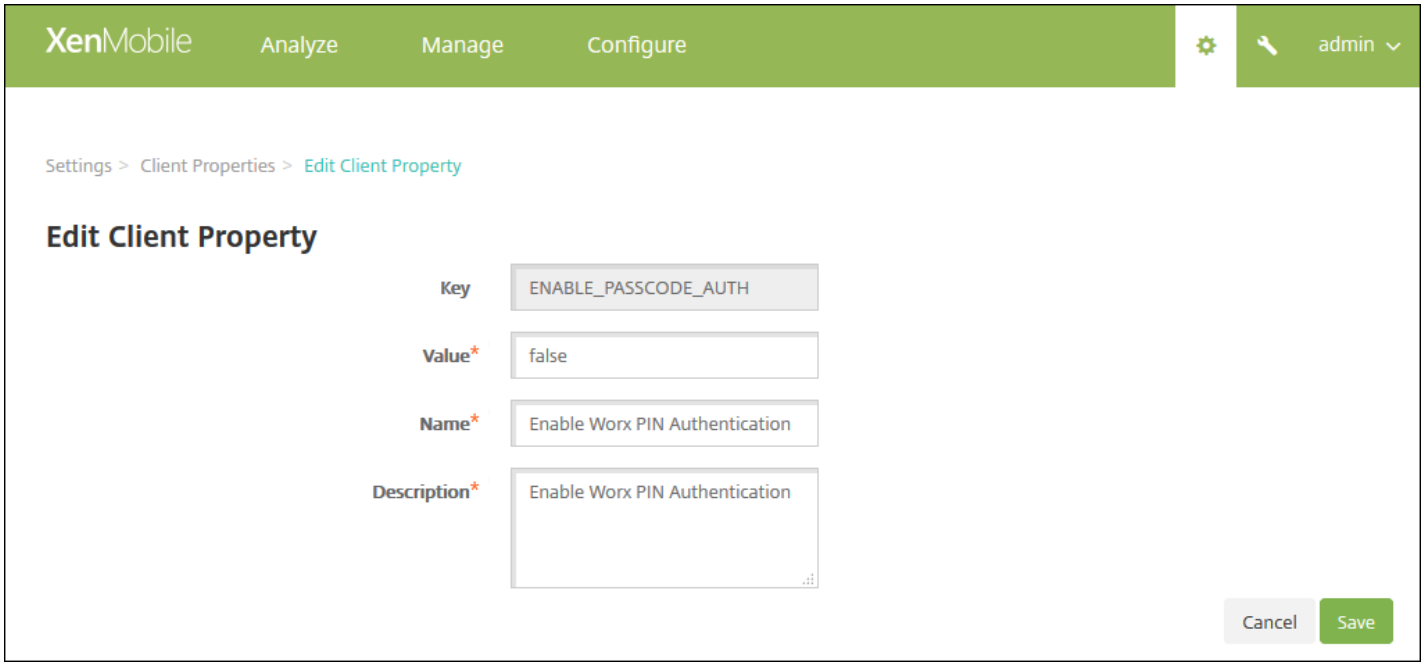
3. [**Save**] をクリックします。

クライアントプロパティを編集するには

1. [**Client Properties**] の表で、編集するクライアントプロパティを選択します。

注：クライアントプロパティの横にあるチェックボックスをオンにすると、クライアントプロパティ一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。

2. [**Edit**] をクリックします。 [**Edit Client Property**] ページが開きます。



3. 必要に応じて以下の情報を変更します。

- **Key**：このフィールドは変更できません。
- **Value**：プロパティの値です。
- **Name**：プロパティの名前です。
- **Description**：プロパティの説明です。

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

クライアントプロパティを削除するには

1. [**Client Properties**] の表で、削除するクライアントプロパティを選択します。

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

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

クライアントプロパティリファレンス

Aug 02, 2016

次に、XenMobileの定義済みクライアントプロパティとそのデフォルトの設定を示します。

CONTAINER_SELF_DESTRUCT_PERIOD

表示名：Self-Destruct

非アクティブな状態で一定の日数を経過すると、自動削除機能により、WorxHomeおよび管理対象アプリケーションにアクセスできなくなります。 有効期限を過ぎると、アプリケーションは使用できなくなり、XenMobileサーバーへのユーザーデバイスの登録が解除されます。 データのワイプでは、各インストール済みアプリケーションのアプリケーションデータ（アプリケーションキャッシュ、ユーザーデータなど）が消去されます。 非アクティブ状態とは、サーバーが一定期間、ユーザーの検証をするための認証要求を受け取っていない状態です。 たとえば、このポリシーに30日を設定した場合、ユーザーがWorx Homeまたはほかのアプリケーションを30日を超えて使用しない状況が続くと、このポリシーが適用されます。

このグローバルセキュリティポリシーは、既存のアプリケーションロックポリシーおよびワイプポリシーの機能拡張であり、iOSおよびAndroidのプラットフォームに適用されます。

このグローバルポリシーを構成するには、[**Settings**]、[**Client**]の順に選択し、カスタムキーCONTAINER_SELF_DESTRUCT_PERIODを追加します。

値：日数

ENABLE_WORXHOME_CEIP

表示名： Enable Worx Home CEIP

このキーにより、カスタマーエクスペリエンス向上プログラムがオンになります。 このプログラムにより、構成および使用データが定期的に、匿名でCitrixに送信されます。 このデータは、XenMobileの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。

値： trueまたはfalse

デフォルト値：false

ENABLE_PASSCODE_AUTH

表示名：Enable Worx PIN Authentication

このキーを使用すると、Worx PIN機能を有効にできます。 ユーザーは、Worx PINまたはパスコードにより、Active Directoryパスワードの代わりに使用するPINを定義するように求められます。 ENABLE_PASSWORD_CACHINGが有効になっているとき、またはXenMobileで証明書認証を使用しているときは、この設定が自動的に有効になります。

ユーザーがオフライン認証を実行している場合、Worx PINがローカルで検証されて、要求したアプリやコンテンツへのアクセスがユーザーに許可されます。 ユーザーがオンライン認証を実行している場合、Worx PINまたはパスコードを使用してActive Directoryパスワードまたは証明書がロック解除されて、XenMobileとの認証を実行するために送信されます。

設定可能な値：trueまたはfalse

デフォルト値：false

ENABLE_PASSWORD_CACHING

表示名：Enable User Password Caching

このキーを使用すると、ユーザーのActive Directoryパスワードをモバイルデバイス上にローカルにキャッシュできます。 このキーをtrueに設定すると、ユーザーはWorx PINまたはパスコードを設定するように求められます。 このキーをtrueに設定する場合は、ENABLE_PASSCODE_AUTHキーをtrueに設定する必要があります。

設定可能な値：trueまたはfalse

デフォルト値：false

ENCRYPT_SECRETS_USING_PASSCODE

表示名：Encrypt secrets using Passcode

このキーでは、機密データをプラットフォームベースのネイティブな格納場所（iOSキーチェーンなど）ではなく、モバイルデバイスのSecret Vaultに格納できます。 この構成キーにより、重要な成果物を強力に暗号化できますが、ユーザーエントロピー（ユーザーだけが知るユーザーが生成するランダムなPINコード）も追加されます。

ユーザーデバイスのセキュリティを強化するために、このキーを有効にすることをお勧めします。

注：このキーを有効にすると、Worx PINでの認証を求められる回数が大幅に増えるため、ユーザーエクスペリエンスに影響します。

設定可能な値：trueまたはfalse

デフォルト値：false

PASSCODE_TYPE

表示名：Worx PIN Type

このキーで、数字のWorx PINまたは英数字のWorxパスコードのいずれをユーザーが定義できるようにするのかを定義します。 ［Numeric］を選択した場合、ユーザーは数字のWorx PINのみを定義できます。 ［Alphanumeric］を選択した場合、ユーザーは文字と数字を組み合わせたWorxパスコードを使用できます。

Note: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Worx PINまたはパスコードを設定するように求められます。

設定可能な値：NumericまたはAlphanumeric

デフォルト値：Numeric

PASSCODE_STRENGTH

表示名：Worx PIN Strength Requirement

このキーで、Worx 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Worx PINまたはパスコードを設定するように求められます。

設定可能な値：Low、Medium、またはStrong

デフォルト値：Medium

次の表は、PASSCODE_TYPEで選択する設定に基づいた、各強度設定のパスワード規則を示しています。

パスコードの強度	数字パスコードの規則	英数字パスコードの規則
低	すべての数字を任意の順序で使用できます。	1つ以上の数字と1つ以上の文字が含まれている必要があります。 使用不可：AAAaaa、 aaaaaa、 abcdef 使用可：aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa
中（デフォルト設定）	1.すべての数字を同じにすることはできません。 たとえば、444444は使用できません。 2.すべての数字を連続した数字にすることはできません。 たとえば、123456や654321は使用できません。 使用可：444333、124567、136790、555556、788888	パスコード強度「Low」の規則に加えて、以下の規則が適用されます。 1.文字およびすべての数字を同じにすることはできません。 たとえば、aaaa11、aa11aa、またはaaa111は使用できません。 2.連続した文字および連続した数字は使用できません。 たとえば、abcd12、bcd123、123abc、xy1234、xyz345、またはcba123は使用できません。 使用可：aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1#、Ab123~
Strong	Worx PINのパスコード強度「Medium」と同じです。	パスコードに1つ以上の数字、1つ以上の特殊記号、1つ以上の大文字、および1つ以上の小文字が含まれている必要があります。 使用不可：abcd12、Abcd12、dfgh12、jkrtA2 使用可：Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#

PASSCODE_MIN_LENGTH

表示名：Worx PIN Length Requirement

このキーでは、Worxパスコードの許容最小文字数を定義します。

設定可能な値：1～99

デフォルト値：6

PASSCODE_EXPIRY

表示名：Worx PIN Expiry Requirement

このキーで、Worx PINまたはパスコードが有効な期間（日単位）を定義します。この期間を過ぎると、ユーザーはWorx PINまたはパスコードを変更する必要があります。 この設定を変更すると、ユーザーの現在のWorx PINまたはパスコードの有効期限が切れた場合のみ、新しい値が設定されます。

設定可能な値：1またはそれ以上。1から99までの間を推奨

デフォルト値：90

注： ユーザーがPINをリセットする必要がないようにするには、値を高い値に設定してください（例：100,000,000,000）。 有効期限を1から99日の間で設定し、その期間中に大きな値に変更した場合、PINは最初に設定した期間の最終日に満期になり、満期がその後に設定されることはありません。

PASSCODE_HISTORY

表示名：Worx PIN History

このキーで、Worx PINまたはパスコードの変更時にユーザーが再利用できない、以前に使用したWorx PINまたはパスコードの個数を定義します。 この設定を変更すると、ユーザーがWorx PINまたはパスコードを次回再設定したときに新しい値が設定されます。

設定可能な値：1～99

デフォルト値：5

INACTIVITY_TIMER

表示名：Inactivity Timer

このキーで、ユーザーがデバイスを非アクティブにした後で、Worx PINまたはパスコードの入力を求められずにアプリにアクセスする時間（分単位）を定義します。 MDXアプリでこの設定を有効にするには、［App Passcode］設定を［On］に設定する必要があります。 ［App Passcode］設定を［Off］に設定すると、ユーザーは完全認証を実行するようWorx Homeにリダイレクトされます。 この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。

注：iOSでは、Inactivity TimerはMDXアプリだけでなくWorx Homeへのアクセスにも対応します。

設定可能な値：正の整数

デフォルト値：15

DISABLE_LOGGING

表示名：Disable logging

このキーでは、ユーザーが自分のデバイスのログを収集およびアップロードする機能を無効にできます。 Worx Homeおよびすべてのインストール済みMDXアプリのロギングが無効になります。 ユーザーは［Support］ページから任意のアプリにログを送信することはできません。メール作成ダイアログボックスは開きますが、ログは添付されません。ロギングが無効になっているというメッセージが追加されます。 ユーザーのデバイスに対する効果に加えて、Worx HomeおよびMDXアプリのXenMobileコンソールでログ設定を変更することはできません。

このキーをtrueに設定すると、Worx Homeによって［Block application logs］が［true］に設定され、新しいポリシーが適用されたときにMDXアプリのロギングが停止します。

設定可能な値：trueまたはfalse

Default value：false（ロギングは有効です）

ENABLE_CRASH_REPORTING

表示名：Enable Crash reporting

このキーでは、Worx AppsのCrashlyticsを使用するクラッシュの報告を有効または無効にします。

設定可能な値：trueまたはfalse

デフォルト値：true

DEVICE_LOGS_TO_IT_HELP_DESK

表示名：Send device logs to IT help desk

このキーで、ITヘルプデスクへのログ送信機能を有効または無効にします。

設定可能な値：trueまたはfalse

デフォルト値：false

ON_FAILURE_USE_EMAIL

表示名：On failure use Email to send device logs to IT help desk.

このキーで、メールを使用してITにデバイスログを送信する機能を有効または無効にします。

設定可能な値：trueまたはfalse

デフォルト値：true

PASSCODE_MAX_ATTEMPTS

表示名：Worx PIN Maximum Attempts

このキーで、完全認証が必要になる前に、ユーザーが誤ったWorx PINまたはパスコードを入力できる回数を定義します。 完全認証に成功した後で、ユーザーは新しいWorx PINまたはパスコードを作成するように求められます。

設定可能な値：正の整数

デフォルト値：15

ENABLE_TOUCH_ID_AUTH

表示名：Enable Touch ID Authentication

このキーでは、（機能搭載済みの）デバイスのTouch ID認証使用機能を有効または無効にします。 ユーザーがアプリケーションを起動したときにTouch IDの使用を求めるメッセージが表示されるように、ユーザーのデバイスはWorx PII対応で、かつユーザーエントロピーがfalseに設定されている必要があります。

設定可能な値：trueまたはfalse

デフォルト値：false

ENABLE_WORXHOME_GA

表示名： Enable Google Analytics in WorxHome

このキーでは、WorxHomeのGoogle Analyticsを使用したデータ収集機能を有効または無効にします。 この設定を変更した場合、ユーザーが次回WorxHomeにログオンすると初めて新しい値が設定されます。

設定可能な値：trueまたはfalse

デフォルト値：true

XenMobileサーバー設定

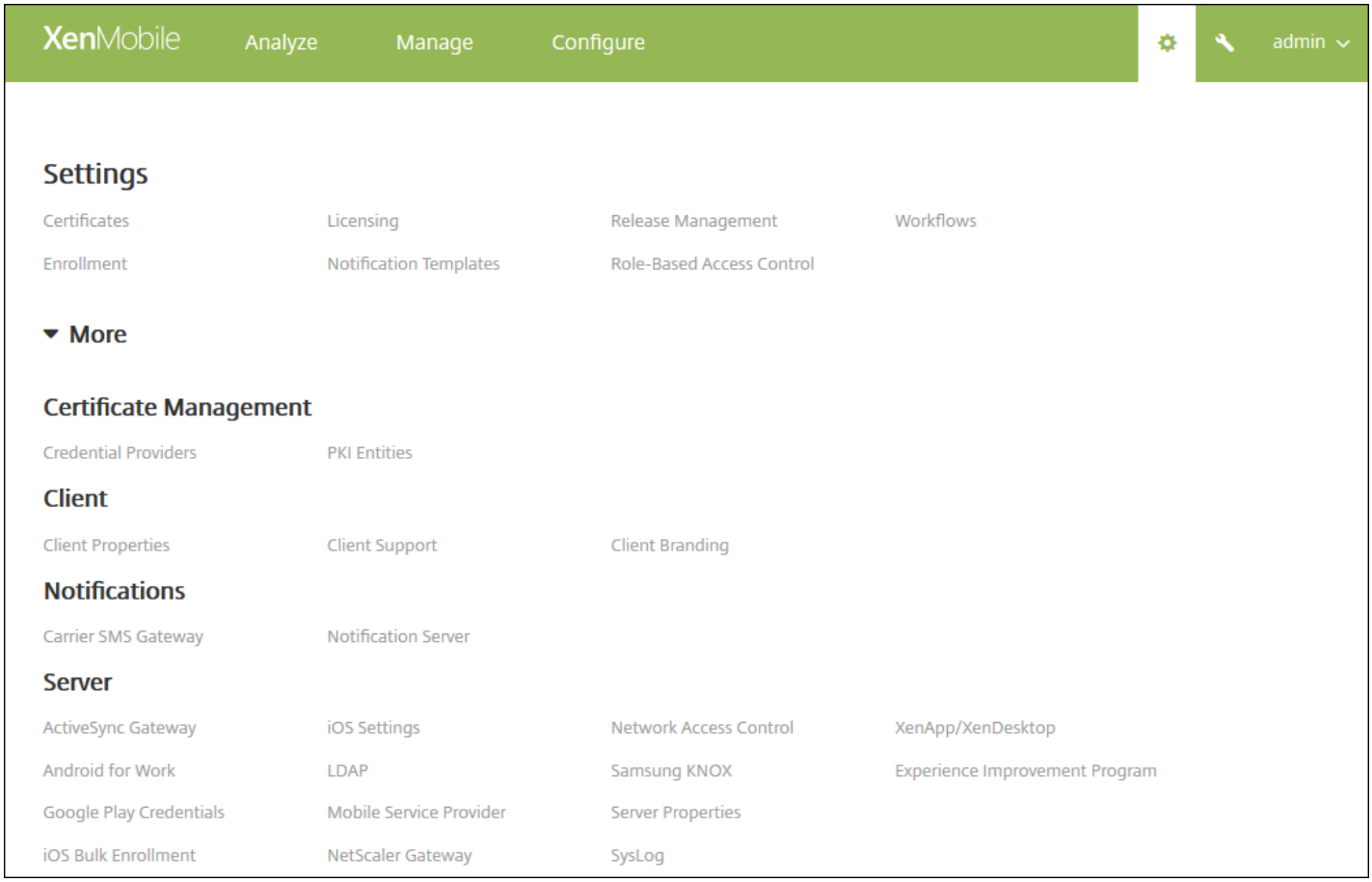
Aug 02, 2016

XenMobileコンソールで構成するXenMobileサーバー設定には以下が含まれます。

- ActiveSync Gateway
- Android for Work
- エクスペリエンス向上プログラム
- Google Play資格情報
- iOSバルク登録
- iOSの設定
- LDAP
- Microsoft Azure
- Mobile Service Provider
- NetScaler Gateway
- ネットワークアクセス制御
- Samsung KNOX
- サーバープロパティ
- Syslog
- XenApp/XenDesktop

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

2. **[Server]** で、構成するオプションをクリックします。



XenMobileでのActiveSyncゲートウェイ

Aug 02, 2016

ActiveSyncは、Microsoftが開発したモバイルデータ同期プロトコルです。 ActiveSyncは、ハンドヘルドデバイスやデスクトップ（またはラップトップ）コンピューターとデータを同期します。 XenMobileでActiveSyncゲートウェイの規則を構成できます。 こうした規則に従って、デバイスはActiveSyncデータへのアクセスを許可または拒否します。 たとえば、［不足必須アプリ］規則をアクティブ化すると、XenMobileはアプリ アクセス ポリシーで必須アプリをチェックし、必須アプリが見つからない場合はActiveSyncデータへのアクセスを拒否します。

XenMobileでは、次の規則がサポートされます。

匿名デバイス：デバイスが匿名モードではないかを確認します。 これは、デバイスが再接続を試みたとき、XenMobileがユーザーを再認証できない場合に確認のために使用します。

Samsung KNOX 構成証明に失敗しました：デバイスが、Samsung KNOX構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ：デバイス上にアプリアクセスポリシーで定義された禁止アプリがないかを確認します。

暗示的許可および拒否：これは、ActiveSync ゲートウェイのデフォルトの操作です。その他のフィルター規則条件を満たしていないすべてのデバイスのデバイス一覧を作成し、一覧に基づいて接続を許可または拒否します。 一致する規則がなければ、デフォルトは［暗示的許可］になります。

非アクティブ デバイス：［サーバー プロパティ］でデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。

不足必須アプリ：デバイスにアプリ アクセス ポリシーで定義された必須アプリの不足がないかを確認します。

非推奨アプリ：デバイスにアプリ アクセス ポリシーで定義された非推奨アプリがないかを確認します。

非準拠パスワード：ユーザーパスワードが正しいかを確認します。 XenMobileが、iOSおよびAndroidデバイス上で、現在デバイスにあるパスワードがデバイスに送られたパスコードポリシーに準拠しているかを確認します。 たとえばiOSの場合、ユーザーはXenMobileがデバイスにパスコードを送ってから60分以内に、パスワードを設定する必要があります。 さもなければ、ユーザーがパスワードを設定する前に、パスコードが非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス外かどうかを確認します。 このプロパティは通常、自動化された操作によって変更されたり、XenMobile APIを使用するサードパーティによって変更されたりします。

失効状態：デバイスの証明書が失効していないかを確認します。 証明書が失効したデバイスは、再度認証されるまで再登録できません。

ルート化されたAndroidおよびジェイルブレークしたiOSデバイス:AndroidまたはiOSデバイスがジェイルブレークされていないかを確認します。

非管理デバイス：デバイスがまだXenMobileの管理下にあるかを確認します。 たとえば、MAMモードで実行されているデバイス、あるいは登録されていないデバイスは、管理下にありません。

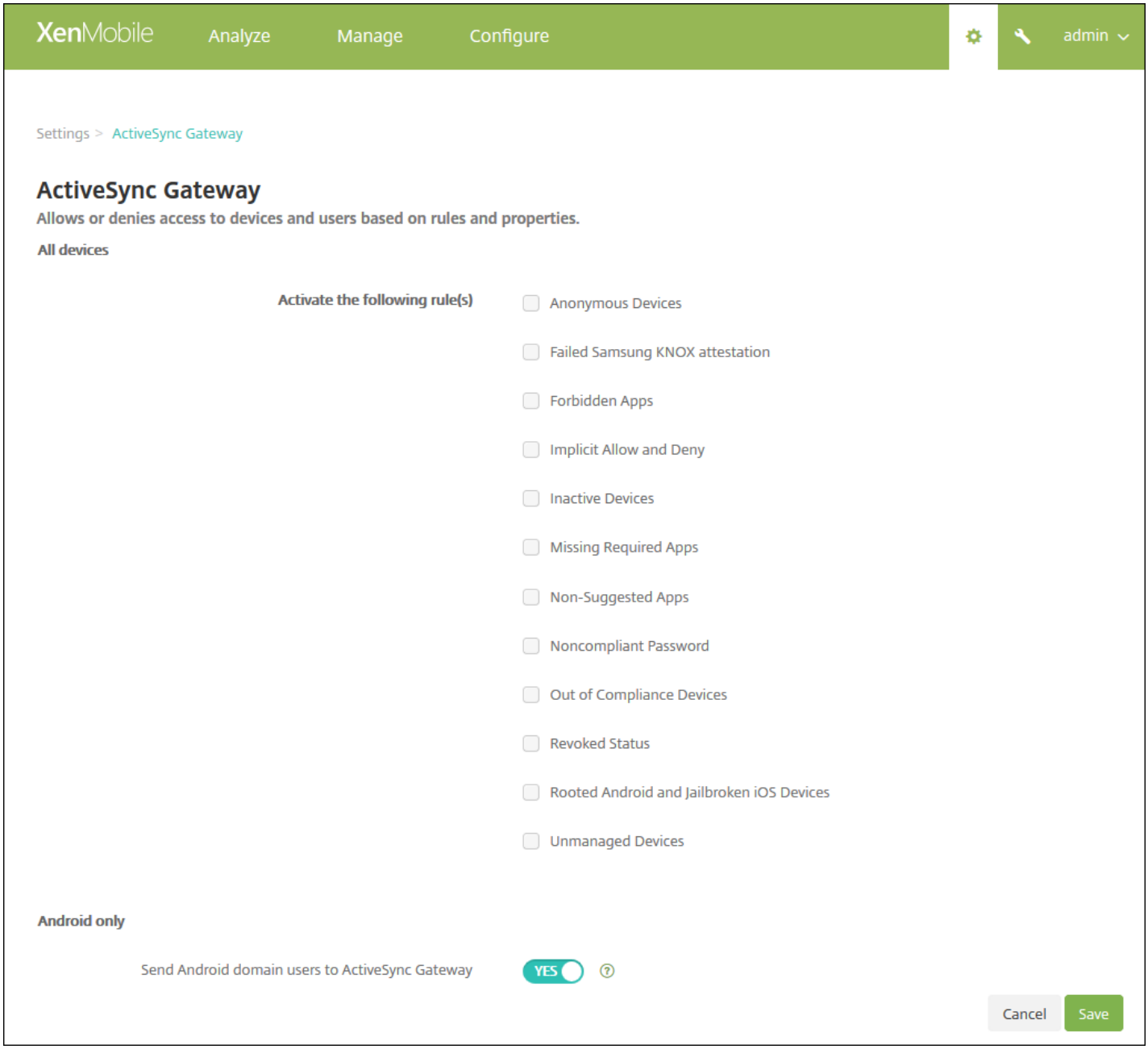
Androidドメイン ユーザーをActiveSync Gatewayに送信：［はい］をクリックすることで、XenMobileによって、Androidデバイスの情報がActiveSyncゲートウェイに送信されるようにします。 このオプションを有効にすると、Androidデバイスユーザーの ActiveSync識別子がXenMobileにない場合でも、XenMobileによってAndroidデバイスの情報が ActiveSyncゲート

ウェイに送信されます。

ActiveSyncゲートウェイ設定を構成するには

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

2. **[サーバー]** の下の **[ActiveSyncゲートウェイ]** をクリックします。 **[ActiveSyncゲートウェイ]** ページが開きます。



3. **[Activate the following rules]** で、有効にする1つまたは複数のルールをオンにします。

4. **[Android-only]** の **[Androidドメインユーザー をActiveSync Gatewayに送信]** で **[はい]** をクリックし、XenMobileによってAndroidデバイスの情報がSecure Mobile Gatewayに送信されるようにします。

5. [**Save**] をクリックします。

Google Play資格情報

Aug 30, 2016

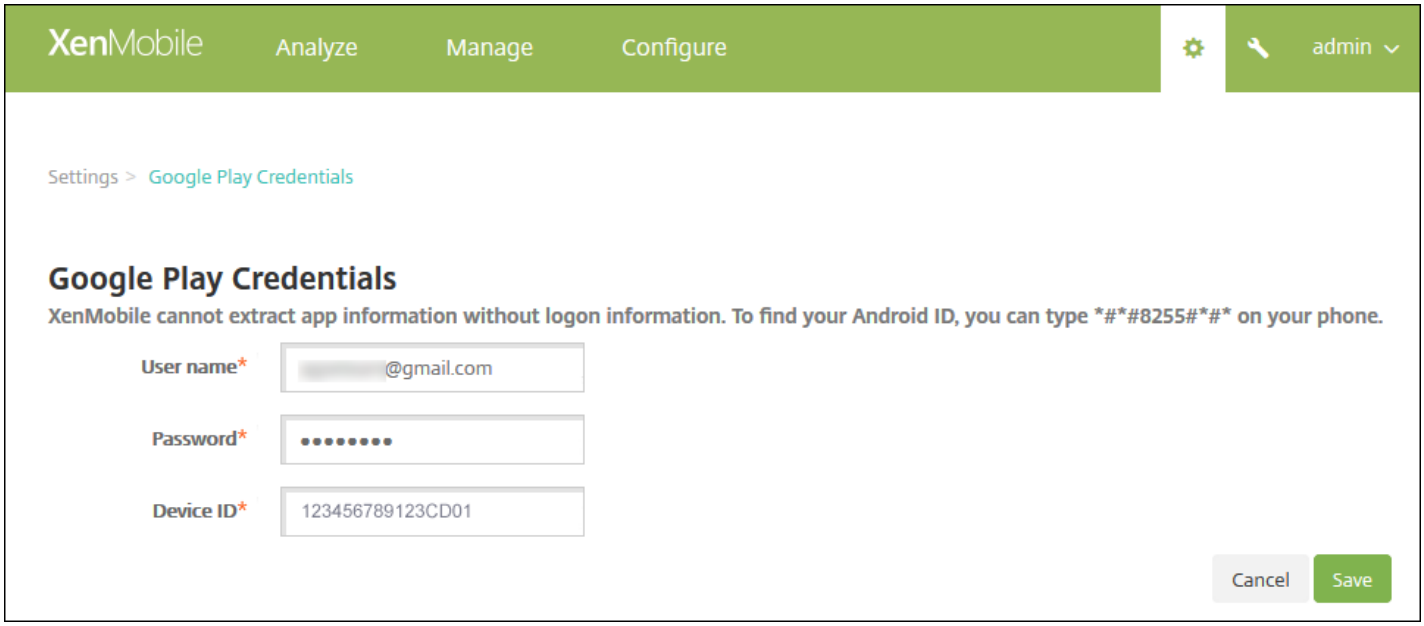
XenMobileでは、Google Play資格情報を使用してデバイスのアプリケーション情報を抽出します。

注：Android IDを確認するには、お使いの電話機で「*#*#8255#*#*」を入力します。 お使いのデバイスタイプ上でコードによりデバイスIDを検出できない場合、デバイスIDを導出するデバイスIDサードパーティ製アプリを使用できる場合があります。 取得する必要があるIDは、Google Services Framework IDとラベルGSF IDです。

重要：XenMobileでアプリケーション情報の抽出を有効にするには、安全でない接続を許可するようにGmailアカウントを構成する必要があります。 手順については、Googleサポートサイトを参照してください。

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

2. **[Server]** の下の **[Google Play Credentials]** をクリックします。 **[Google Play Credentials]** ページが開きます。



3. 次の設定を構成します。

- **User name**：Google Playアカウントに関連付けられた名前を入力します。
- **Password**：ユーザーパスワードを入力します。
- **Device ID**：Android IDを入力します。
  Android IDを確認するには、お使いの電話機で「*#*#8255#*#*」を入力します。

3. **[Save]** をクリックします。

iOSデバイスの一括登録

Aug 02, 2016

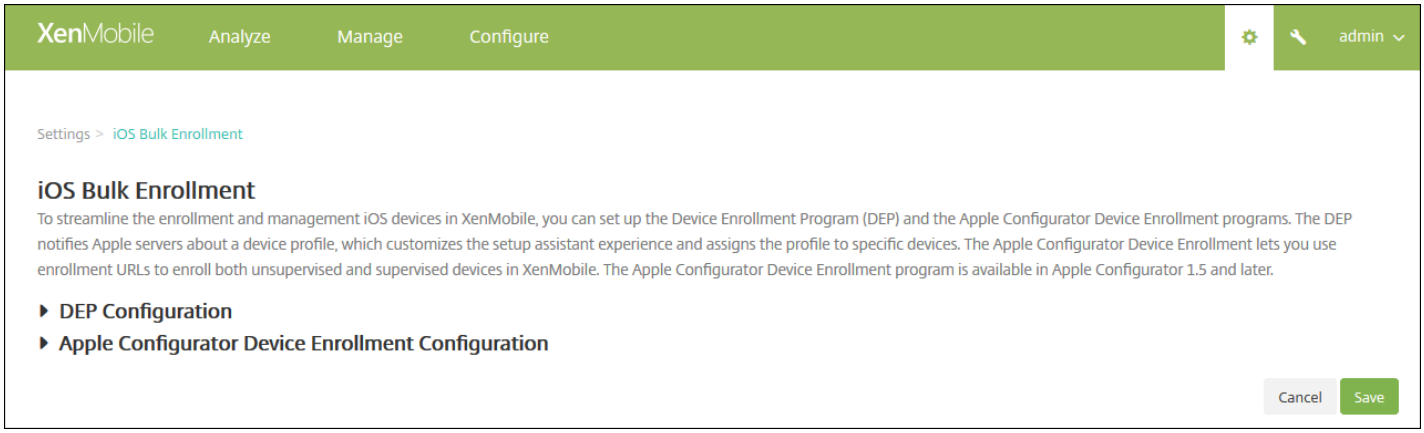
次の2つの方法で多数のiOSデバイスをXenMobileに追加できます。 AppleのDevice Enrollment Program（DEP）を使用して、Appleまたはプログラムに参加しているApple正規販売店または通信事業者から直接購入したデバイスを登録することができます。 または、 Appleから直接購入したかどうかにかかわらず、Apple Configuratorを使用してデバイスを登録できます。

DEPでは、実物のデバイスを直に設定つまり準備する必要はありません。デバイスのシリアル番号または発注番号をDEP経由で送信すると、デバイスが構成されXenMobileに登録されます。 ユーザーは、登録されたデバイスをすぐに使い始めることができます。 さらに、DEPでデバイスをセットアップすると、ユーザーが初めてデバイスを起動したときに入力する必要のある設定アシスタントの手順の一部を省略できます。 DEPのセットアップについて詳しくは、AppleのDevice Enrollment Programページを参照してください。

Apple Configuratorの場合は、OS X 10.7.2以降およびApple Configuratorアプリが動作するAppleコンピューターにデバイスを接続します。 Apple Configuratorを介して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で、初めてデバイスをXenMobileに接続すると、ポリシーが適用されデバイスの管理を開始できます。 Apple Configuratorの使用について詳しくは、AppleのApple Configuratorページを参照してください。

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

2. **[Server]** の下の **[iOS Bulk Enrollment]** をクリックします。 **[iOS Bulk Enrollment]** ページが開きます。



DEP設定を構成する場合は、「DEP設定の構成」を参照します。Apple Configurator設定を構成する場合は、「Apple Configurator設定の構成」を参照します。

DEP設定の構成

続行する前に、deploy.apple.comでApple DEPアカウントを作成しておく必要があります。 DEPアカウントの作成後、仮想MDMサーバーをセットアップしてXenMobileとAppleの通信を許可します。 これを実行するには、XenMobile公開キーをAppleにアップロードする必要があります。 Appleが公開キーを受信したら、XenMobileにインポートするサーバートークンが返されます。 次の手順に従って、XenMobileとApple間での通信を確立します。

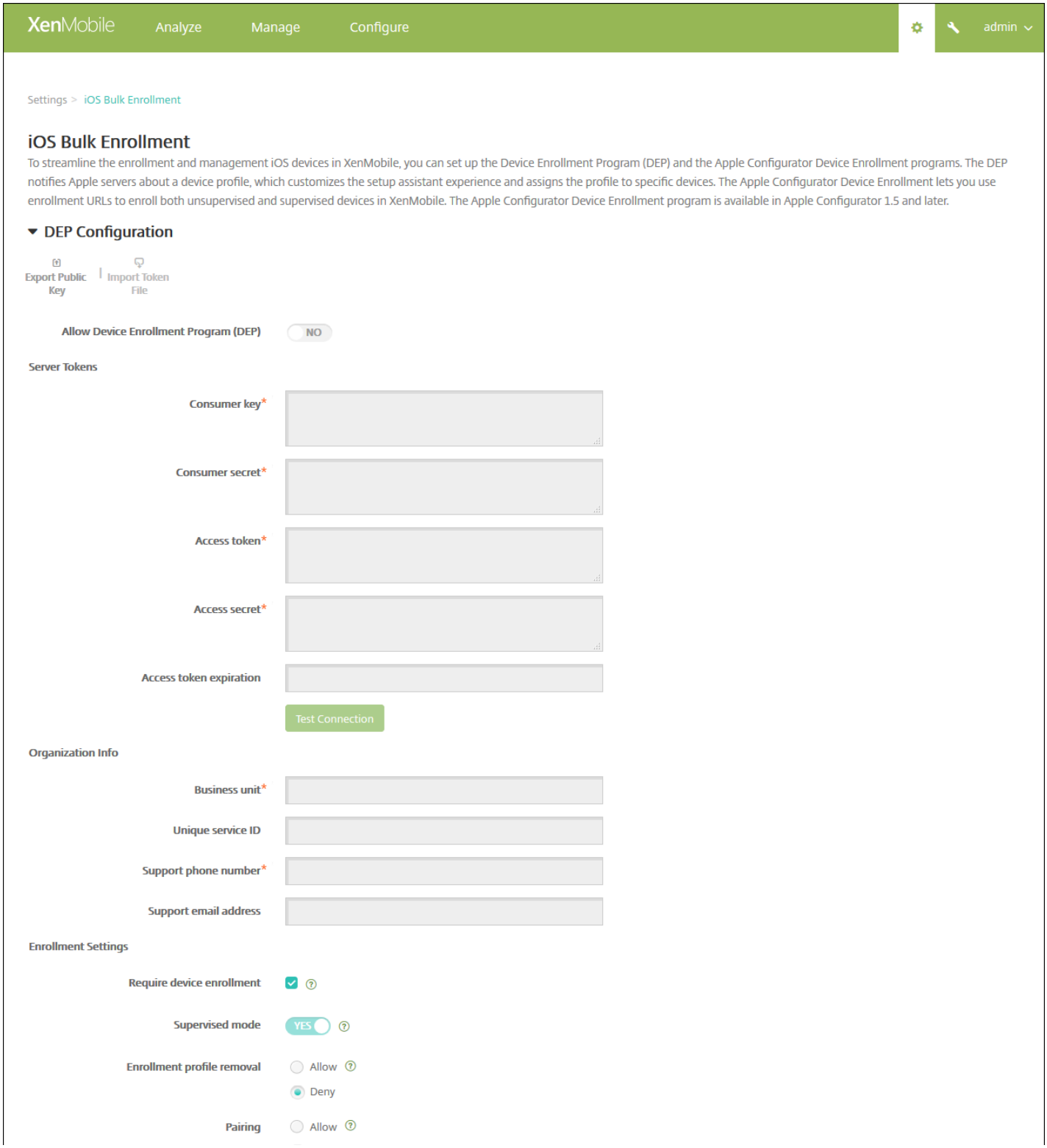
1. 公開キーを取得してAppleにアップロードするには、 **[iOS Bulk Enrollment]** ページで、 **[DEP Configuration]** を展開し、 **[Export Public Key]** をクリックしてファイルをコンピューターに保存します。

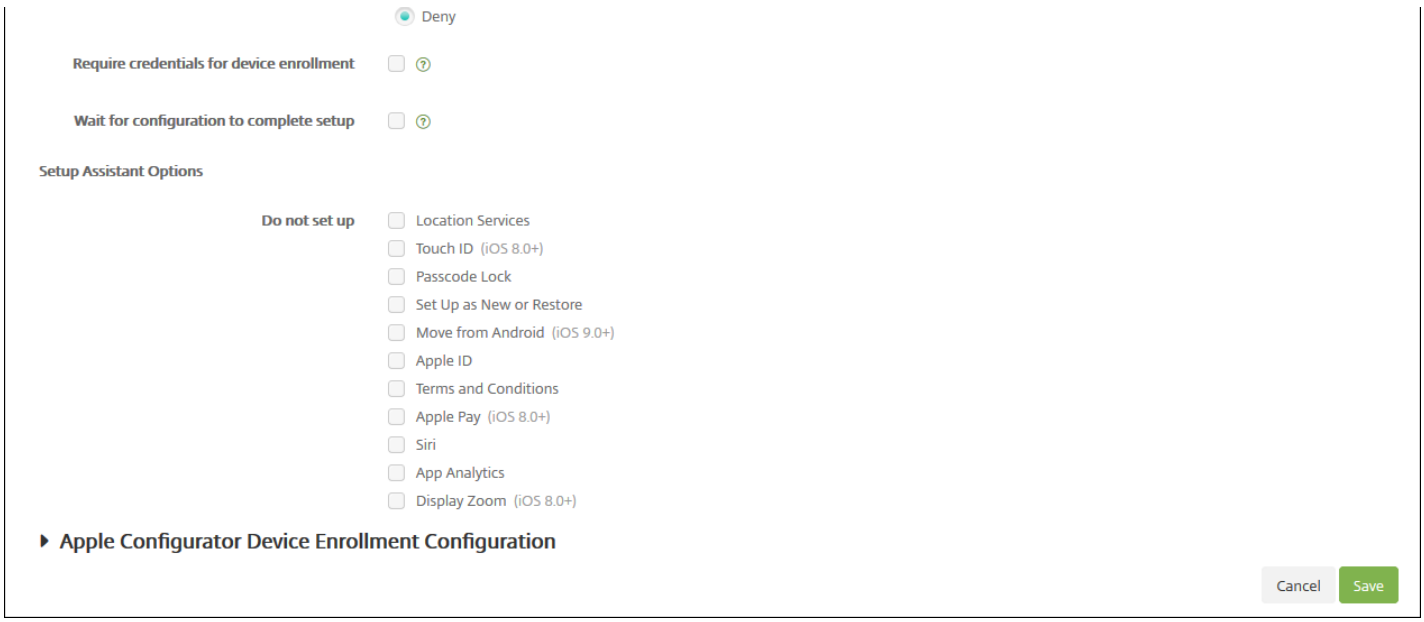
2. deploy.apple.comにアクセスして、DEPアカウントにログインし、MDMサーバーのセットアップ手順に従います。 この処理の一部として、Appleによりサーバートークンが提供されます。

3. [**iOS Bulk Enrollment**] ページで [**Import Token File**] をクリックして、Appleサーバートークンを XenMobile に追加します。

4. トークンファイルが XenMobile にアップロードされると、[**Server tokens**] フィールドに値が自動的に入ります。

5. [**Test Connectivity**] をクリックして、XenMobile と Apppleが通信できるか確認します。 接続テストに失敗したら、すべてに必要なポートが開いているか確認します。ほとんどの場合で、これが障害の原因です。 XenMobile で開く必要があるポートについて詳しくは、「ポート要件」を参照してください。





6. 次の設定を構成してDEP構成を完了します。

Organization Information

- **Business unit**： デバイスを割り当てる事業単位または部門を入力します。 このフィールドは必須です。
- **Unique service ID**：任意で、一意のIDを入力します。
- **Support phone number**：ユーザーがセットアップ時にサポートが必要となった場合に連絡するサポートの電話番号を入力します。 このフィールドは必須です。
- **Support email address**：任意で、サポートのメールアドレスを入力します。

Enrollment Settings

- **Require device enrollment**：ユーザーにデバイス登録を要求するかどうかを選択します。 デフォルトでは登録が必要です。
- **Supervised mode**：DEPで登録したデバイスをApple Configuratorで管理する場合、または［**Wait for configuration to complete setup**］が有効な場合は、［**Yes**］に設定する必要があります。 デフォルトは［**Yes**］です。 iOSデバイスをSupervisedモードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。
- **Enrollment profile removal**：リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。 デフォルトは ［**Deny**］. です。
- **Pairing**：DEPで登録したデバイスをiTunesおよびApple Configuratorで管理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［**Deny**］です。
- **Require credentials for device enrollment**：DEPのセットアップ時にユーザーに資格情報の入力を要求するかどうかを選択します。 これはiOS 7.1以降で使用できます。 **注**：初回のセットアップでDEPを有効にしており、このオプションをオンにしない場合、DEPユーザー、Worx Home、ソフトウェアインベントリ、DEP展開グループなどのDEPコンポーネントが最初から作成されます。 このオプションをオンにした場合は、ユーザーが資格情報を入力するまでコンポーネントは作成されません。 そのため、後でこのオプションをオフにしても、これらのDEPコンポーネントは存在しないため、資格情報を入力していないユーザーはDEP登録を実行できません。 その場合、DEPコンポーネントを追加するには、DEPアカウントを無効化してもう一度有効化する必要があります。
- **Wait for configuration to complete setup**：すべてのMDMリソースがユーザーのデバイスに展開されるまで、デバイスをSetup Assistantモードのままにしておく必要があるかどうかを選択します。 これはiOS 9.0以降のSupervisedモードのデバ

イスでのみ使用できます。

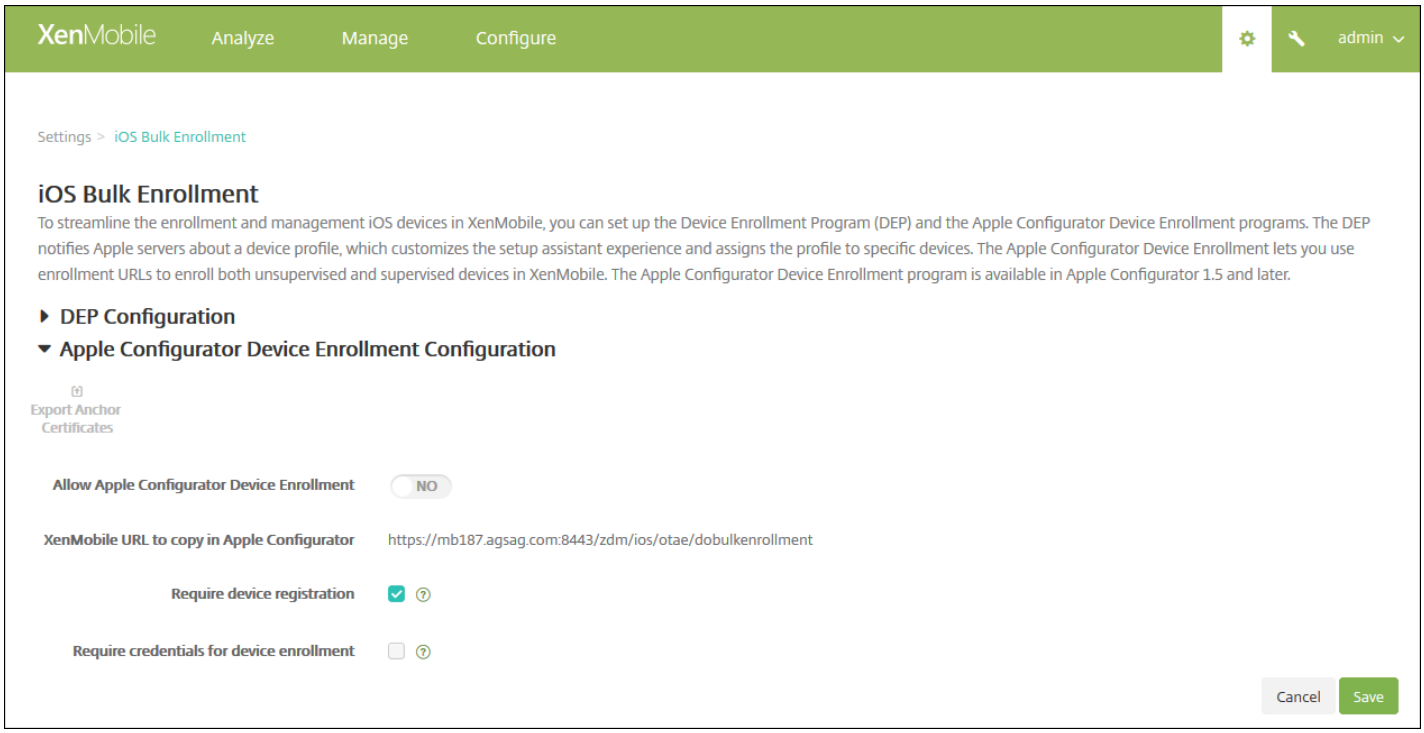
- **注：**Appleのドキュメントには、デバイスがSetup Assistantモードの間は以下のコマンドが機能しない場合があると述べられています。
  - InviteToProgram
  - InstallApplication
  - ApplyRedemptionCode
  - InstallMedia
  - RequestMirroring
  - DeviceLock

セットアップ

ユーザーが初めてデバイスを起動して使用するときに実行する必要がないiOS設定アシスタントの手順（すなわち、スキップできる手順）を選択します。

- **Location Services**：デバイスに位置情報サービスを設定します。
- **Touch ID**：iOS 8.0以降のデバイスにTouch IDを設定します。
- **Passcode Lock**：デバイスのパスコードを作成します。
- **Set up as New or Restore**：新規に、またはiCloudかiTunesのバックアップからデバイスを設定します。
- **Move from Android**：AndroidデバイスからiOS 9以降のデバイスへのデータ転送を有効にします。 このオプションは、［**Set up as New or Restore**］がオンの場合（すなわち、手順をスキップする場合）にのみ使用できます。
- **Apple ID**：デバイスのApple IDアカウントを設定します。
- **Terms and Conditions**：デバイスの使用契約条件に対する同意をユーザーに要求します。
- **Apple Pay**：iOS 8.0以降のデバイスにApple Payを設定します。
- **Siri**：デバイスでSiriを使用するかどうかを選択します。
- **App Analytics**：クラッシュデータおよび使用状況の統計情報をAppleと共有するかどうかを設定します。
- **Display Zoom**：iOS 8.0以降のデバイスにディスプレイ解像度（標準またはズーム）を設定します。

Apple Configurator設定の構成



1. [**Apple Configurator Device Enrollment Configuration**]を展開します。

2. [**Enable Apple Configurator Device Enrollment**]を[**Yes**]に設定します。

3. 以下の設定を確認して構成します。

- **MDM server URL to copy in Apple Configurator**：この読み取り専用のフィールドはAppleと通信するXenMobileサーバーのURLです。このURLをコピーして、後の手順でApple Configuratorに貼り付けます。 Apple Configurator 2の場合、登録URLは、XenMobileサーバーの完全修飾ドメイン名（FQDN）またはIPアドレスです（例：mdm.server.url.com）。
- **Require device registration**：この設定を選択する場合は、デバイスを登録する前に、構成済みのデバイスをXenMobileの[**Devices**]タブに手動でまたはCSVファイルを介して追加する必要があります。 これにより、未知のデバイスの登録を防ぎます。 デフォルトでは、デバイスの追加が必要です。
- **Require credentials for device enrollment**：iOS 7.1以降のデバイスのユーザーに対して、登録時に資格情報の入力を要求します。 デフォルトでは資格情報は不要です。

> **注意**
>
> XenMobileサーバーで信頼済みのSSL証明書を使用する場合は、次の手順をスキップします。

4. [**Export Anchor Certs**]をクリックして、 certchain.pemファイルをOS Xキーチェーン（ログインまたはシステム）に保存します。

5. Apple Configuratorを開始して[**Prepare**]、[**Setup**]、[**Configure Settings**]の順に選択します。

6. Configuratorの[**Device Enrollment**]設定の[**MDM server URL**]フィールドに、手順4のMDMサーバーURLを貼り付けます。

7. XenMobileで信頼済みのSSL証明書を使用しない場合は、[**Device Enrollment**]設定の[**Anchor certificates**]にルート証明書およびSSLサーバー証明書をコピーします。

8. DockコネクタUSBケーブルを使用して、最大で30台のデバイスを同時にApple Configuratorが動作するMacに接続して構成します。 Dockコネクタがない場合は、1台または複数のPowered USB 2.0高速ハブを使用してデバイスを接続します。

9. [**Prepare**]をクリックします。 Apple Configuratorを使用したデバイスの準備について詳しくは、Apple Configuratorのヘルプページ「Prepare devices」を参照してください。

10. Apple Configuratorで必要なデバイスポリシーを構成します。

11. 準備ができたデバイスから電源を入れてiOS設定アシスタントを開始し、初回使用のためにデバイスを準備します。

Apple DEPを使用しているときに証明書を更新するには

XenMobile Secure Sockets Layer（SSL）証明書が更新されたら、XenMobileコンソールで[**Settings**] > [**Certificates**]の順に選択し、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、[**SSL Listener**]をクリックして証明書がSSLに使用されるようにします。 サーバーを再起動すると、新しいSSL証明書が使用されるようになります。 XenMobileの証明書について詳しくは、「XenMobileでの証明書のアップロード」を参照してください。

SSL証明書を更新するときに、Apple DEPとXenMobileの間の信頼関係を再構築する必要はありません。 ただし、この記事の」記の手順に従って、いつでもDEP設定を再構成できます。

Apple DEPについて詳しくは、Appleのドキュメントを参照してください。

この設定に関する既知の問題および解決方法について詳しくは、「XenMobile Server 10.3の既知の問題」を参照してください。

Apple DEPを介したiOSデバイスの展開

Aug 02, 2016

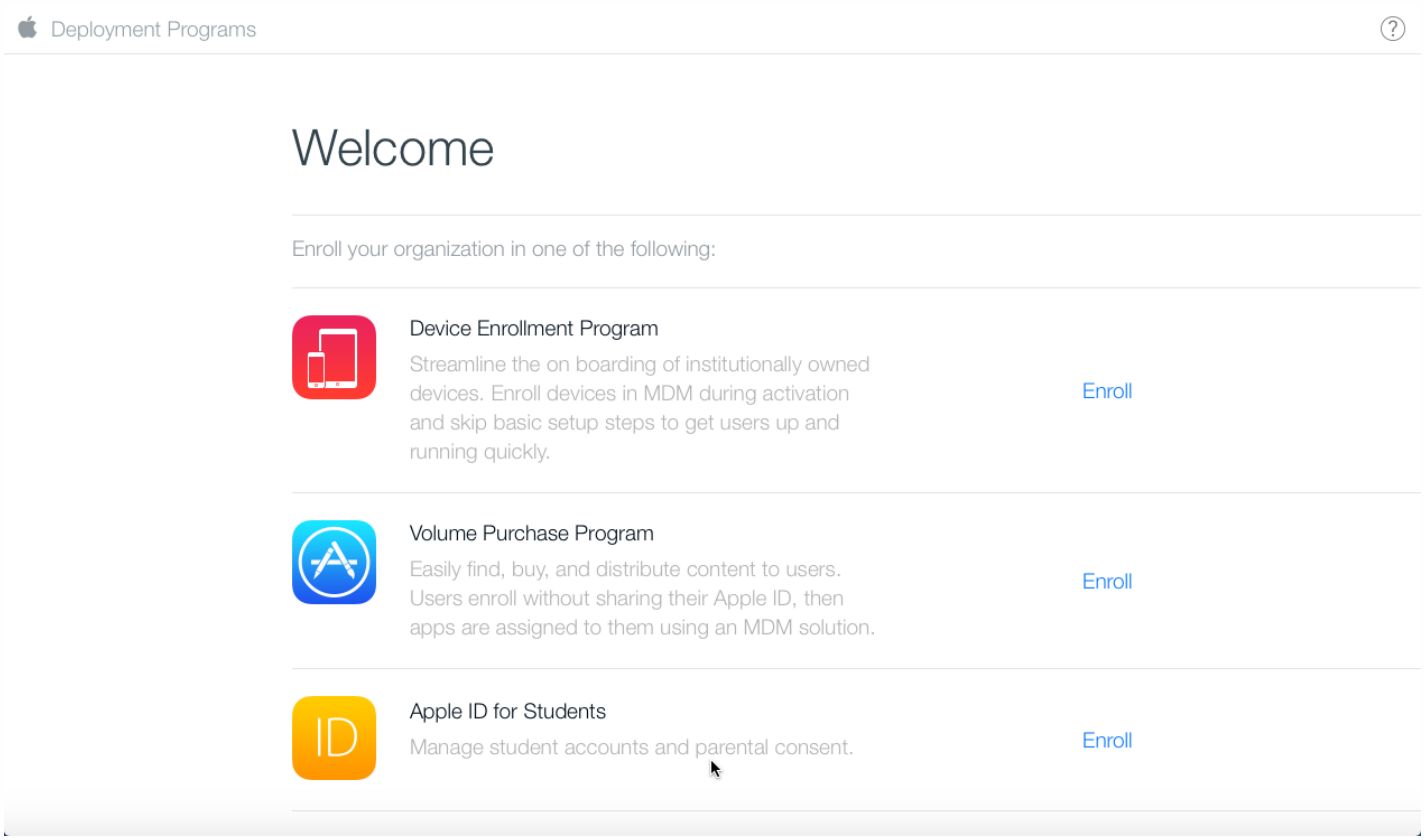
XenMobileでApple DEP for iOSデバイス登録および管理を利用できるようにするには、Apple Developer Enterprise Program（DEP）アカウントが必要です。 Apple DEPへサインアップするために組織で必要となるのは主に次のものです。

- 会社または機関の電話番号とメールアドレス
- 検証の連絡先
- 会社または機関の情報（D-U-N-S／税金ID）
- Appleカスタマー番号

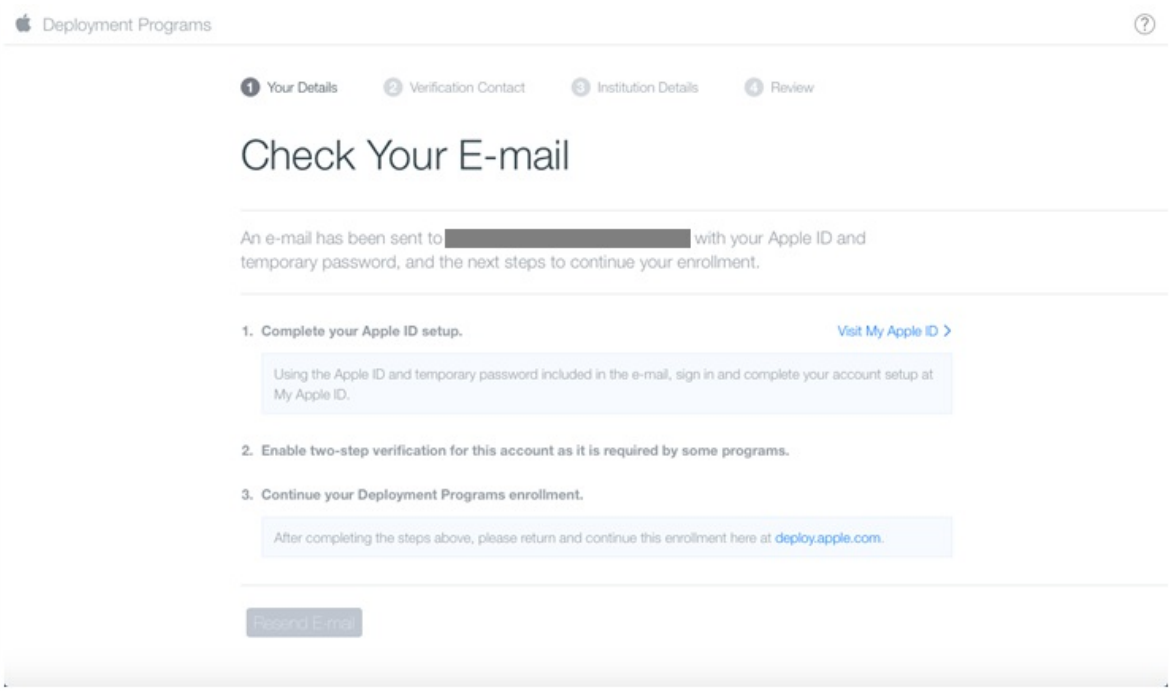
Apple DEPについて詳しくは、Apple社のこのPDFファイルを参照してください。 Apple DEPは個人ではなく法人向けのものたということに留意する必要があります。 またApple DEPアカウントを作成するため、相当量の会社の詳細および情報について提供の必要があることを認識しておく必要もあります。これはつまり、カスタマーがアカウントを要求してその承認を受信するまでに、時間がかかることがあるということです。

Apple DEPの申し込み

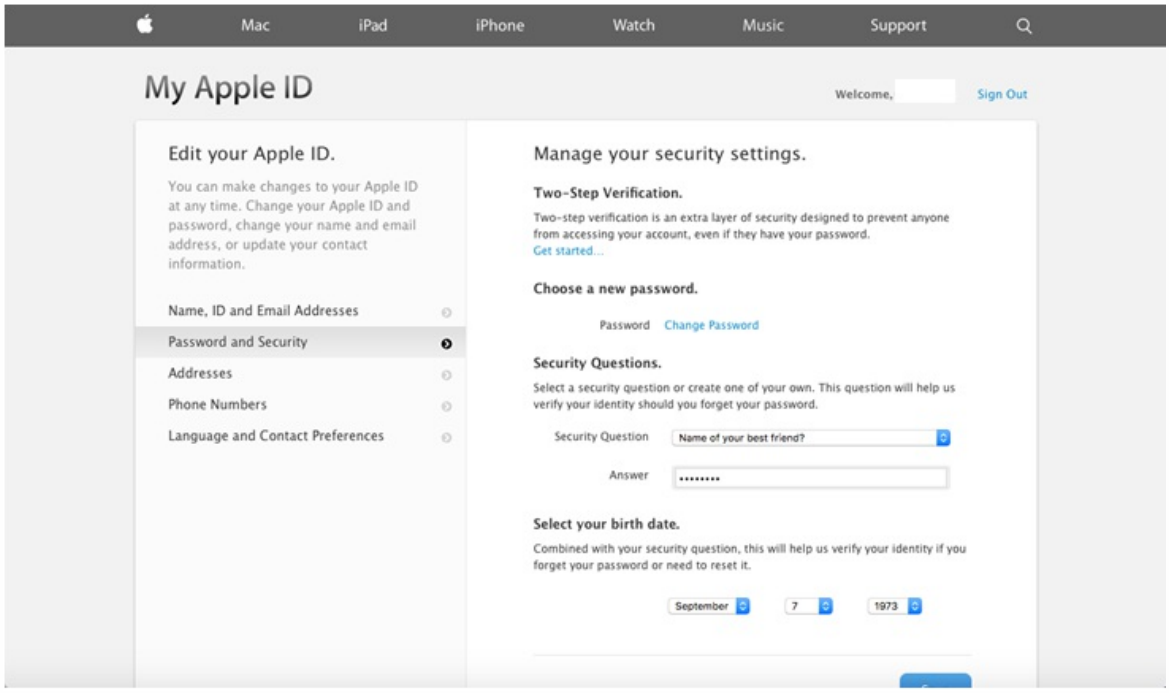
DEPアカウントを申し込む場合、ベストプラクティスはdep@company.comなど組織に紐づけされたメールアドレスを使うことです。



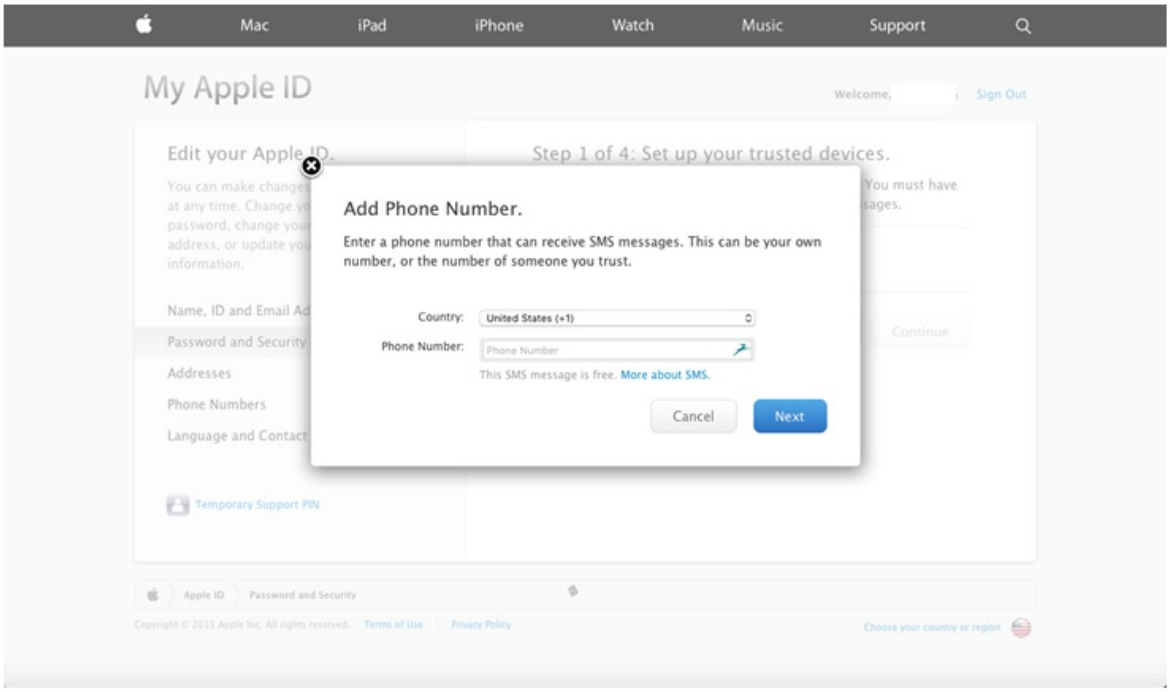
1. 組織に関する情報を入力した後、メール経由で新しいApple IDの一時パスワードを受け取ります。



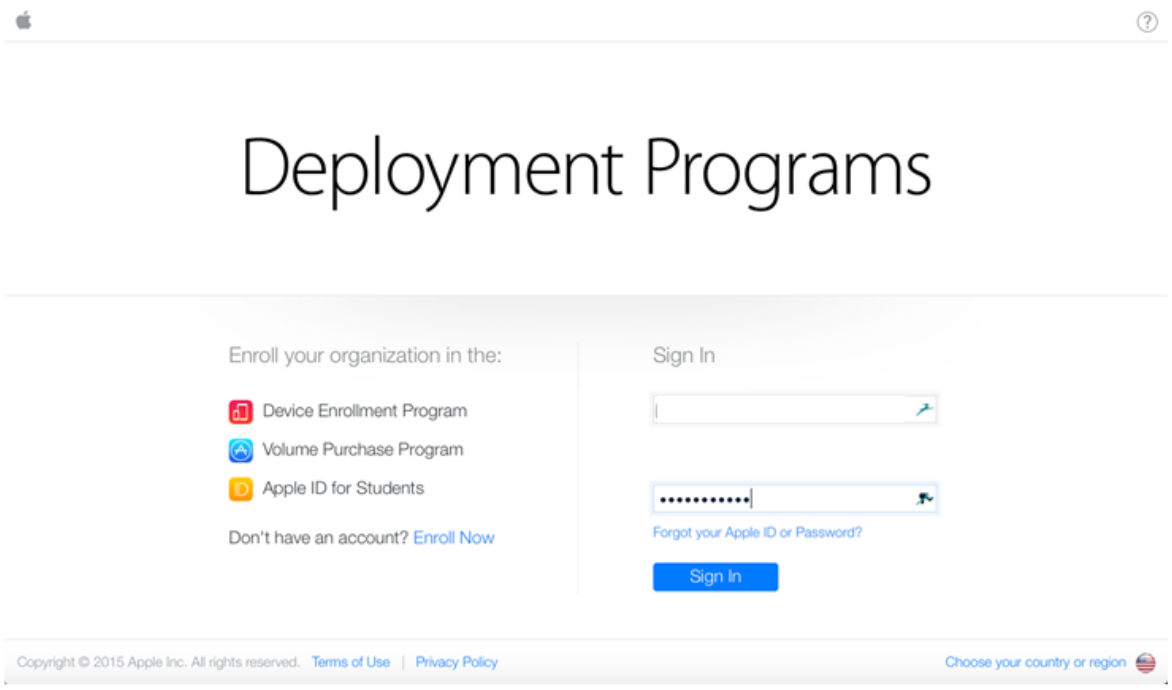
2. 次に、Apple IDでサインインしてアカウントのセキュリティ設定を完了させます。



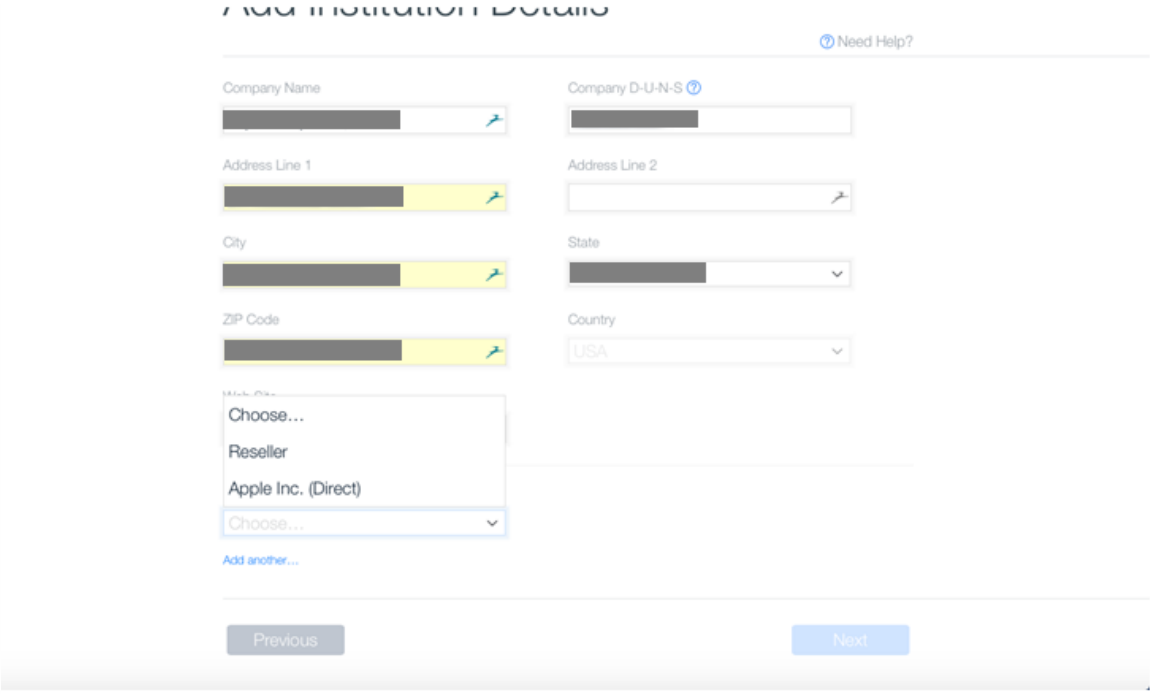
3. 2段階認証を構成して有効にします。これは、DEP Portalで使用するために必要です。 この手順では、2段階認証用の4ケタのPINを受信する電話番号を追加します。



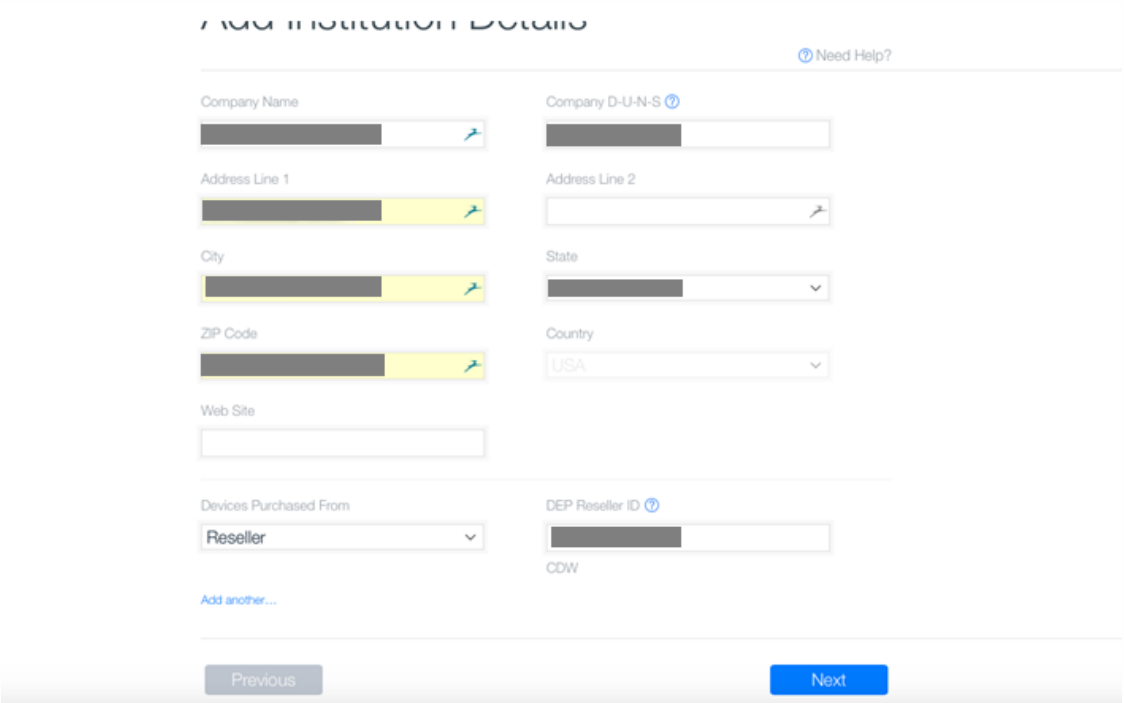
4. DEP Portalにログインし、セットアップしたばかりの2段階認証を使用するアカウント構成を完了させます。

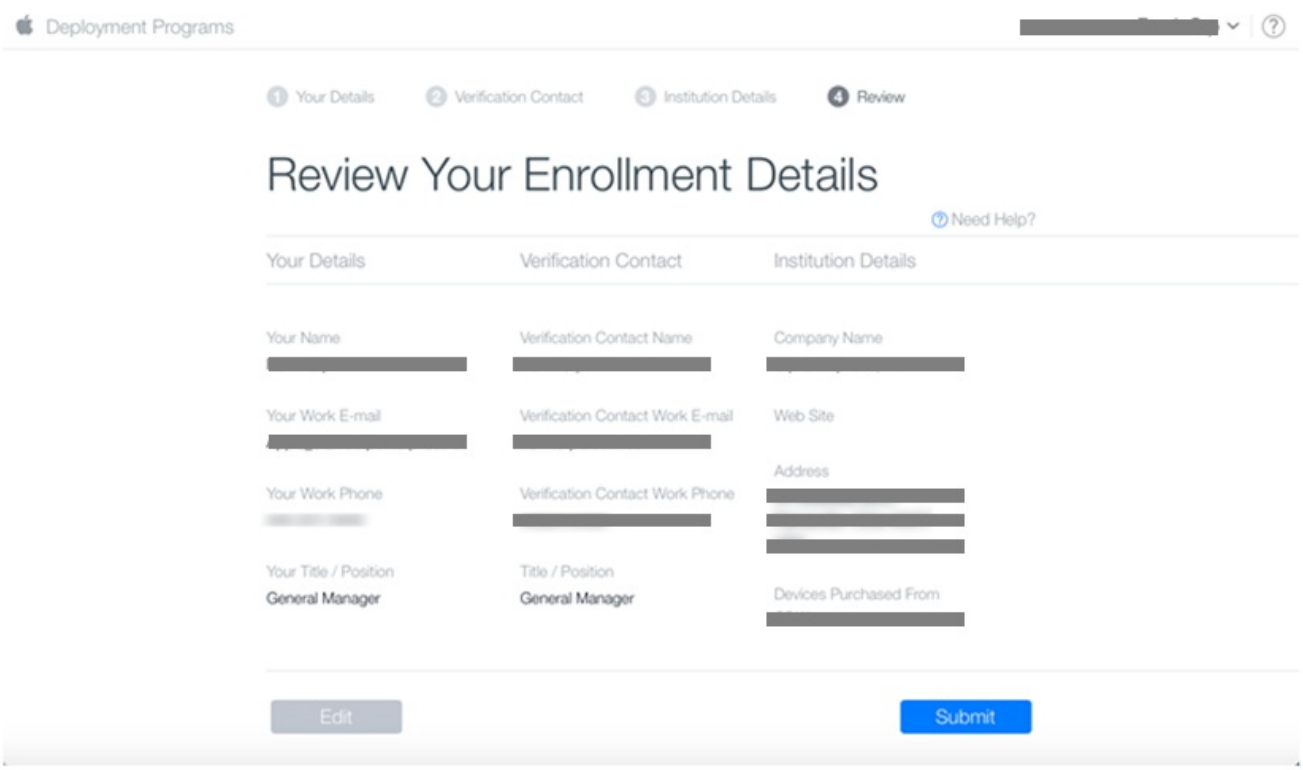


5. 会社の詳細を追加して、デバイスを購入する場所を選択します。 購入オプションについては、 DEP対応デバイスの注文」を参照してください。

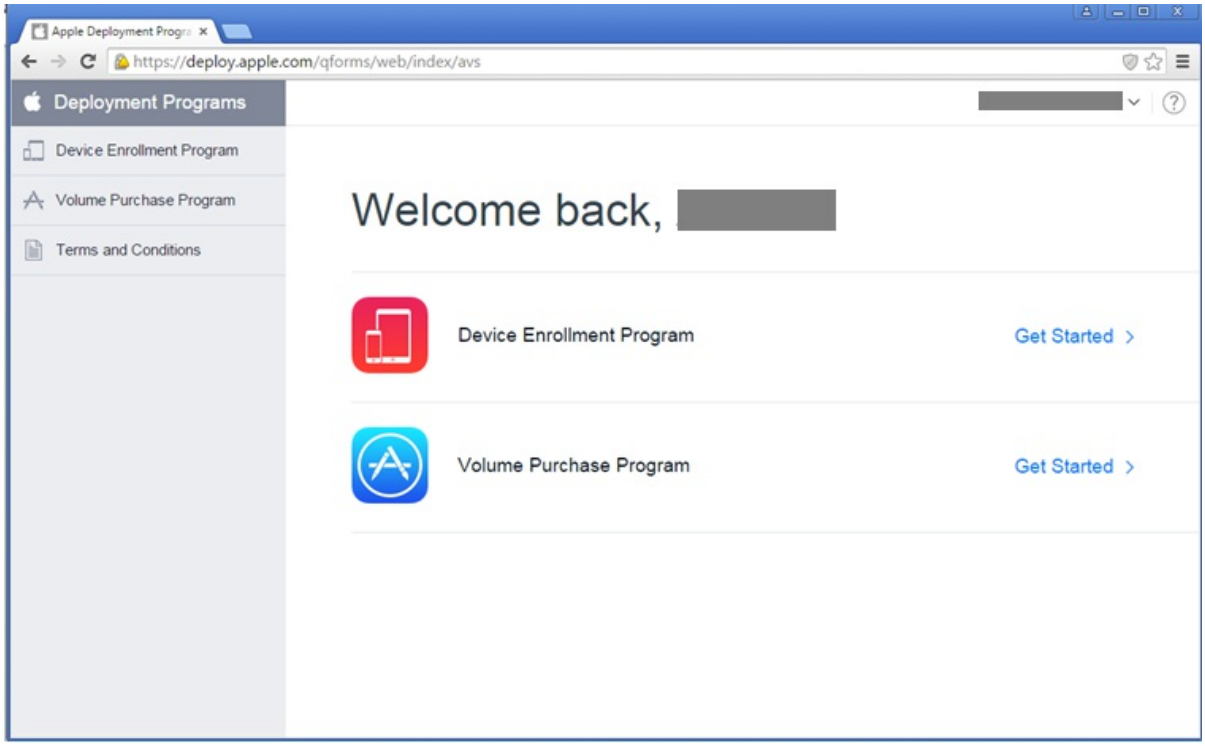


6. Apple Customer NumberまたはDEP Reseller IDを追加して、登録の詳細を認証し、Appleがアカウントを承認するのを待ちます。





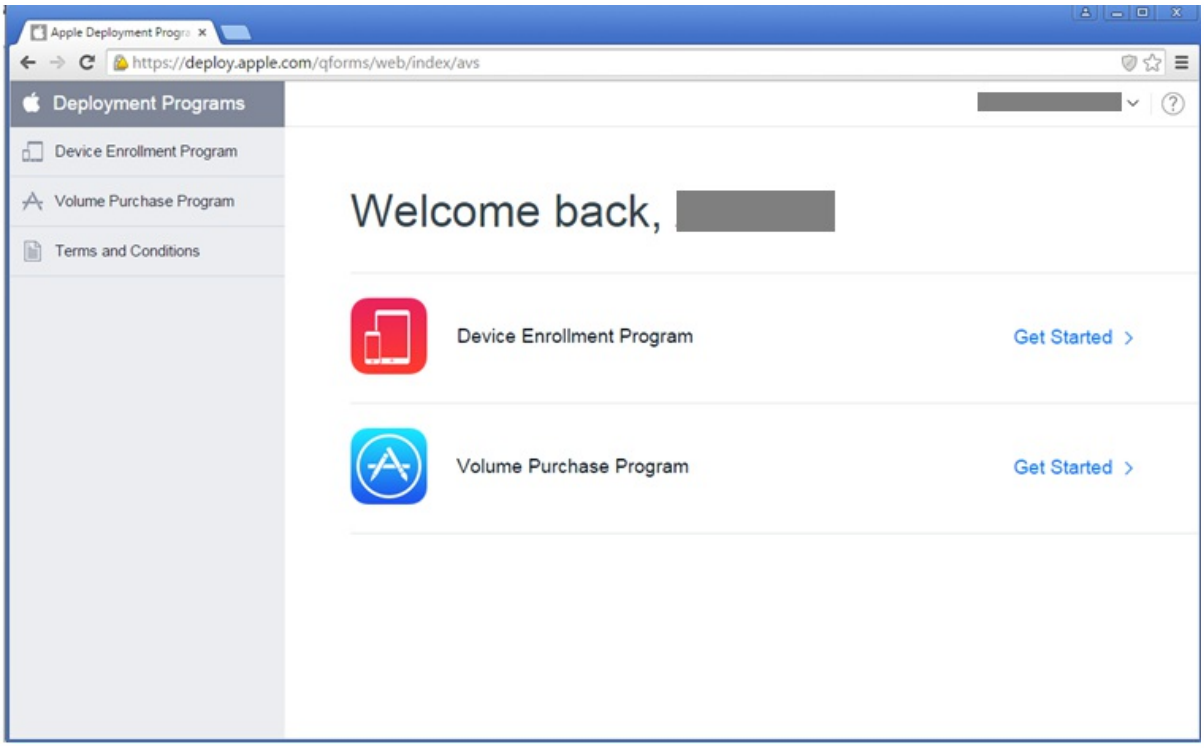
7. Appleからログオン資格情報を受け取ったら、Apple DEP Portalにログインします。 その後で、次のセクションに示す手順に従ってXenMobileでアカウントに接続します。



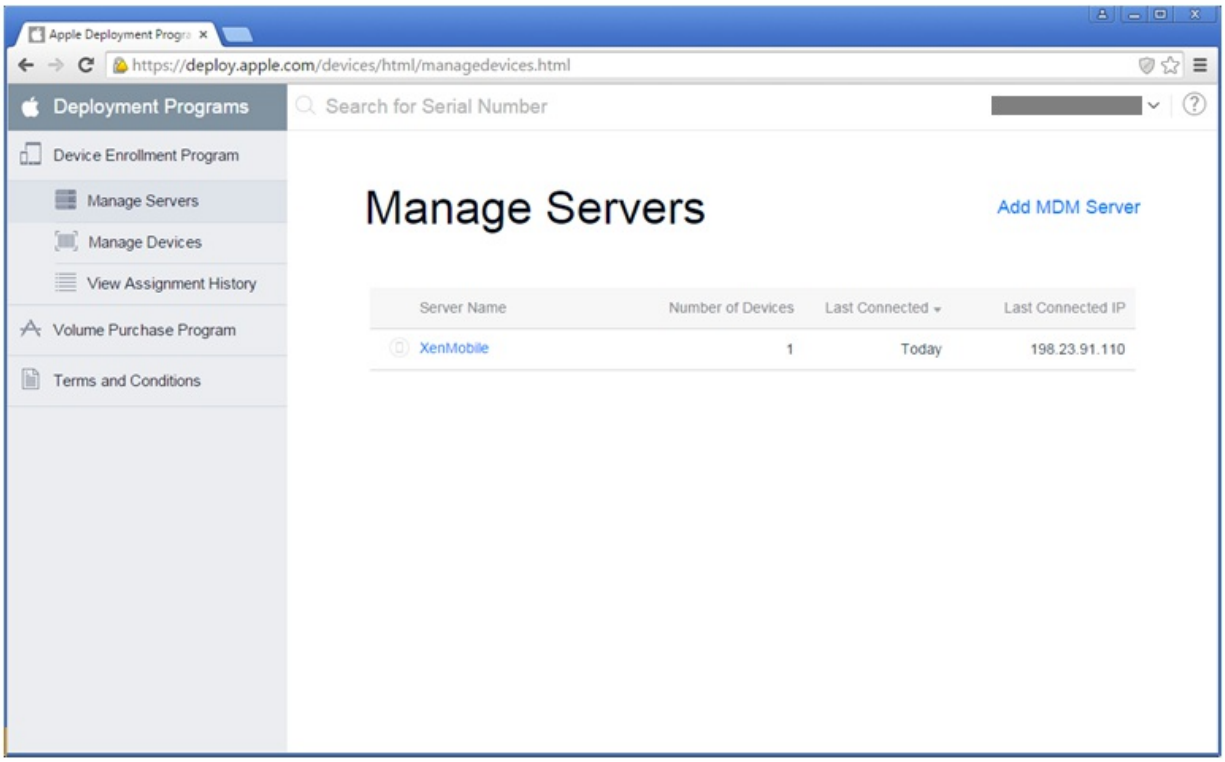
Apple DEPアカウントとXenMobileの統合

このセクションで示す手順に従い、XenMobileサーバー展開でApple DEPアカウントに接続します。

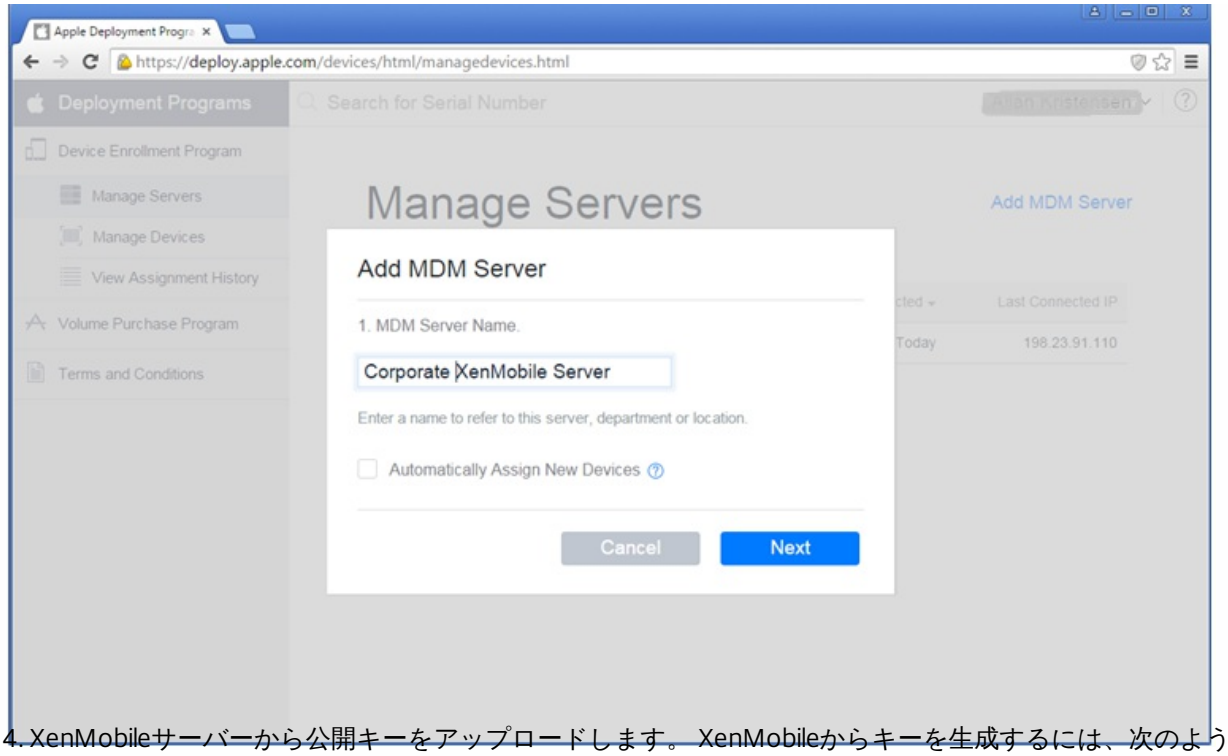
1. Apple DEP Portalの左側にある［**Device Enrollment Program**］をクリックします。



2. **[Manage Servers]** をクリックし、右側にある **[Add MDM Server]** をクリックします。



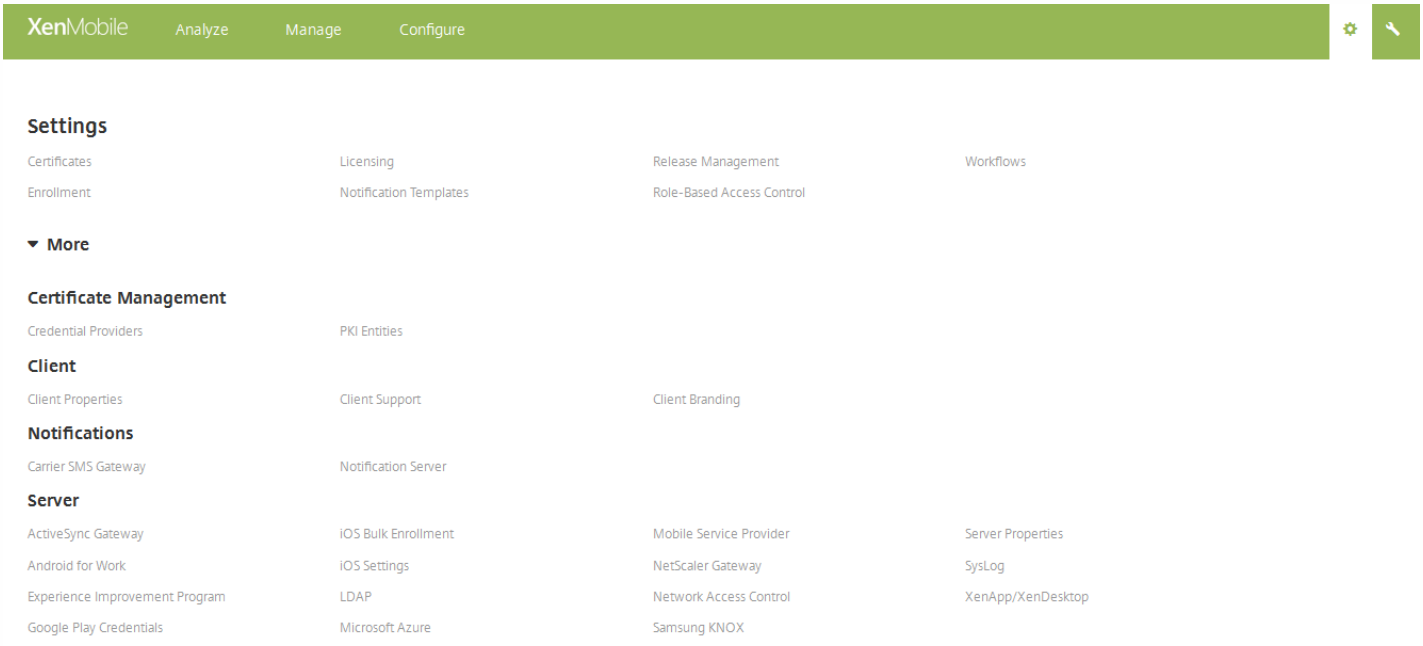
3. **[Add MDM Server]** にXenMobileサーバーの名前を入力し、 **[Next]** をクリックします。



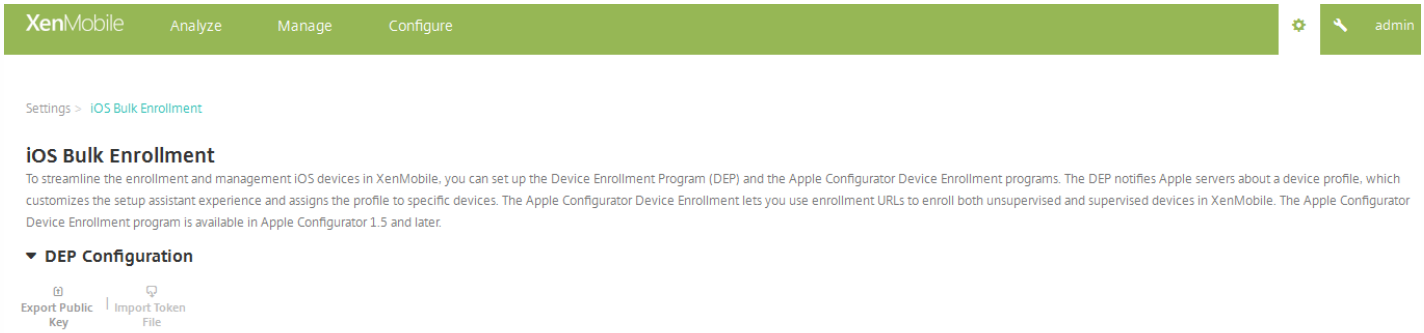
4. XenMobileサーバーから公開キーをアップロードします。 XenMobileからキーを生成するには、次のようにします。

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

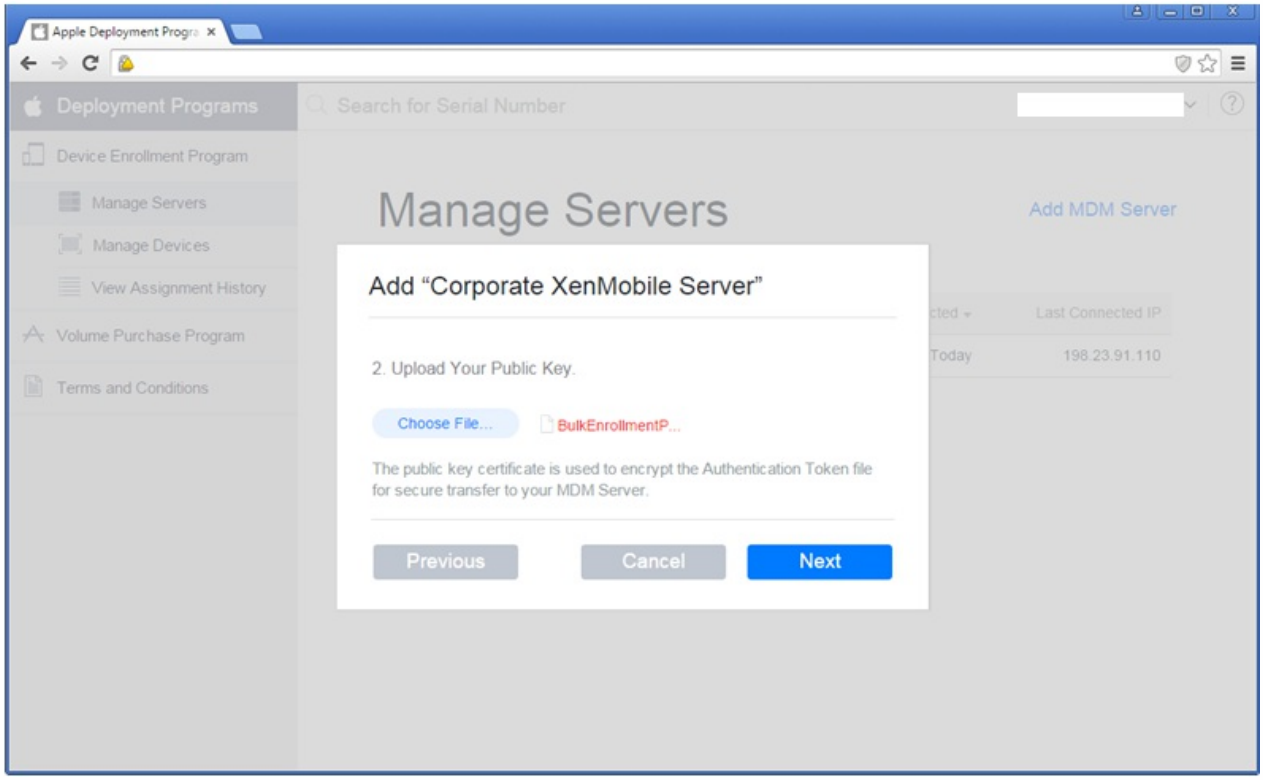
b. **[詳細]** で **[iOS 一括登録]** をクリックします。



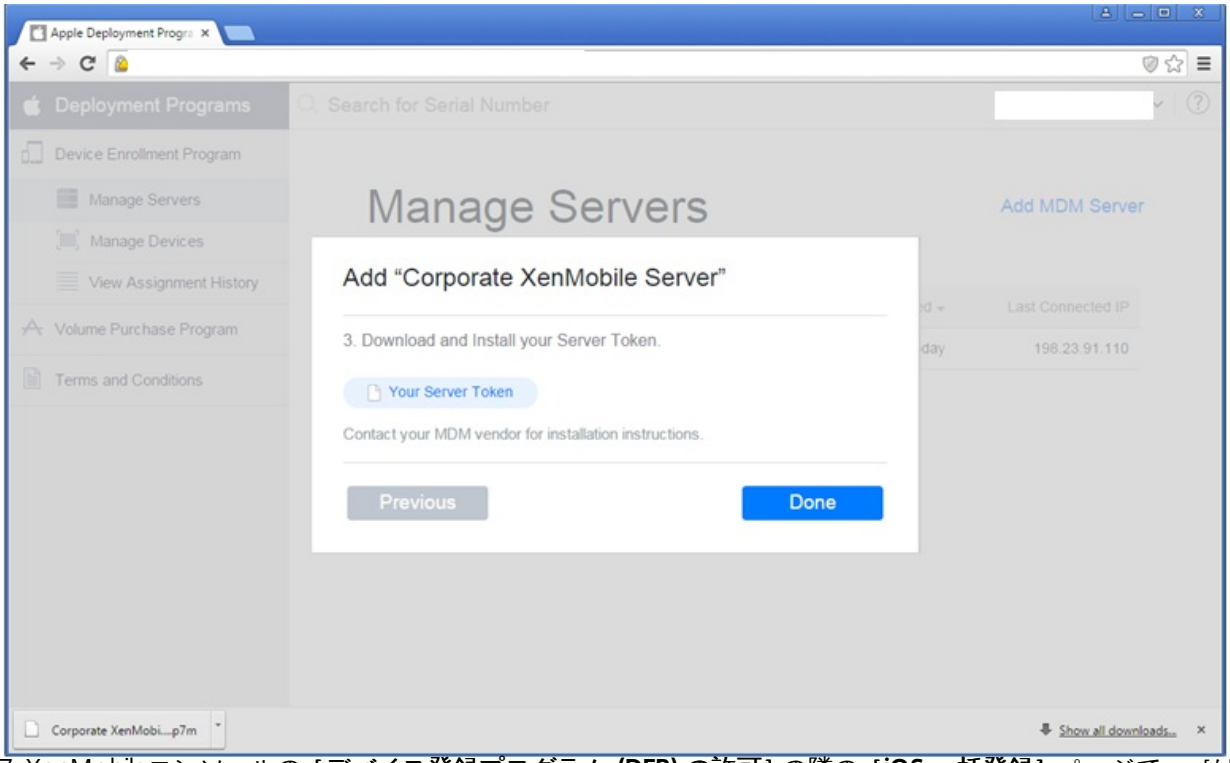
b. **[iOS 一括登録]** ページで **[DEP 構成]** を展開してから、 **[公開キーのエクスポート]** をクリックします。 公開キーがダウンロードされます。



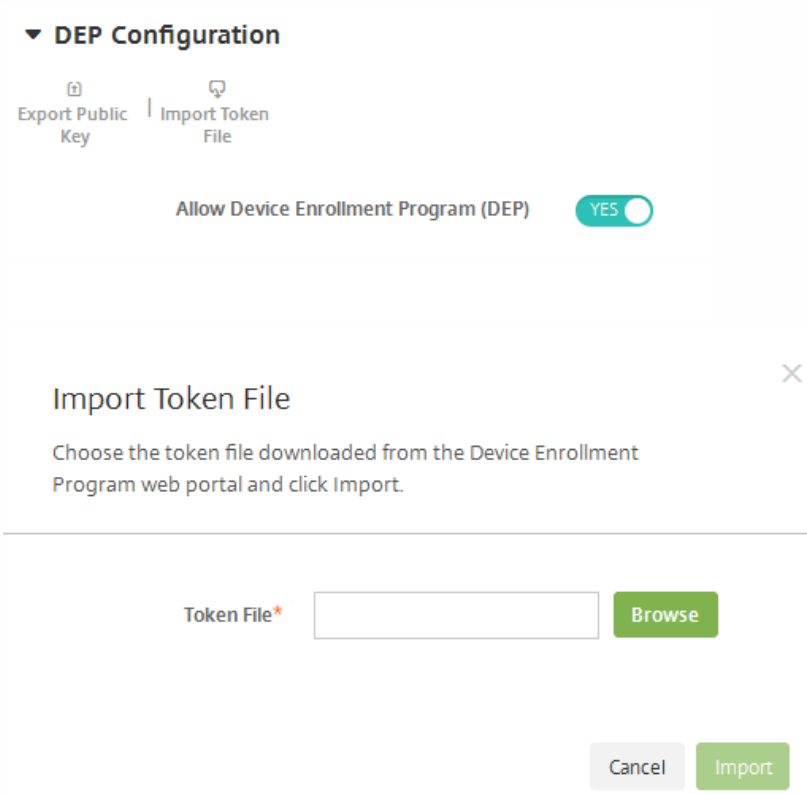
5. Apple DEP Portalで、 **[Choose file]** をクリックしてダウンロードしたばかりの公開キーを選択し、次に**[Next]** をクリックします。



6. **[Your Server Token]** をクリックして、ブラウザーからダウンロードされるサーバートークンを生成し、**[Done]** をクリックします。

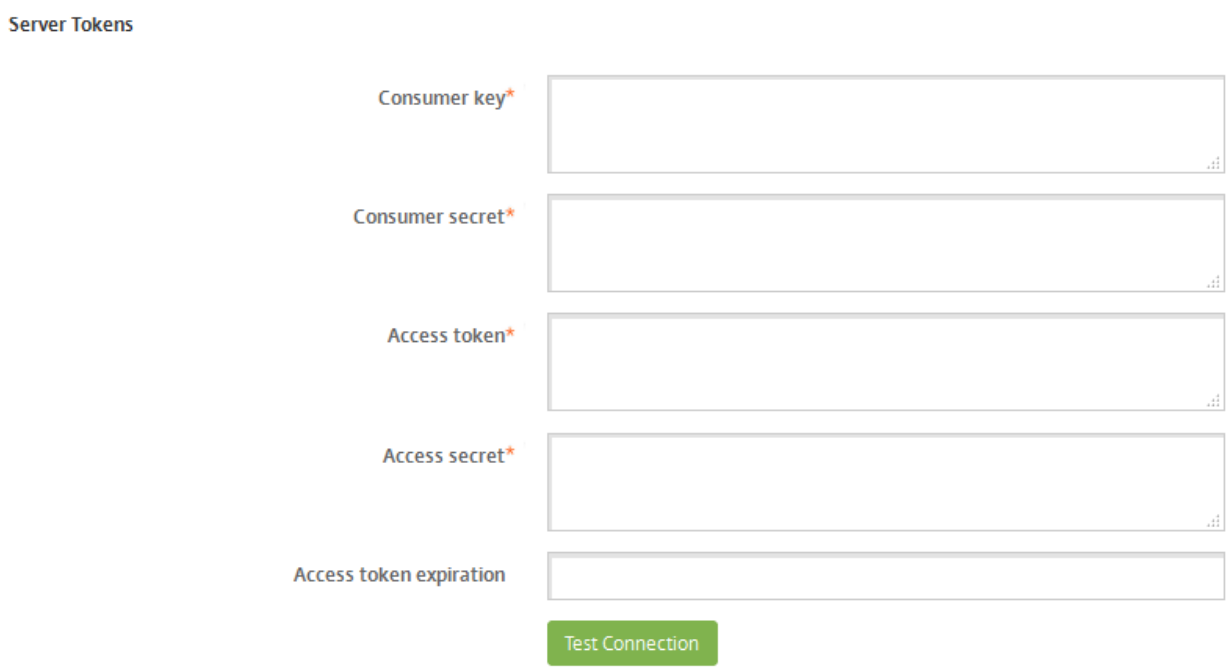


7. XenMobileコンソールの [**デバイス登録プログラム (DEP) の許可**] の隣の [**iOS 一括登録**] ページで、［はい］をクリックし、 [**トークン ファイルのインポート**] をクリックして前の手順でダウンロードしたトークンファイルをアップロードします。



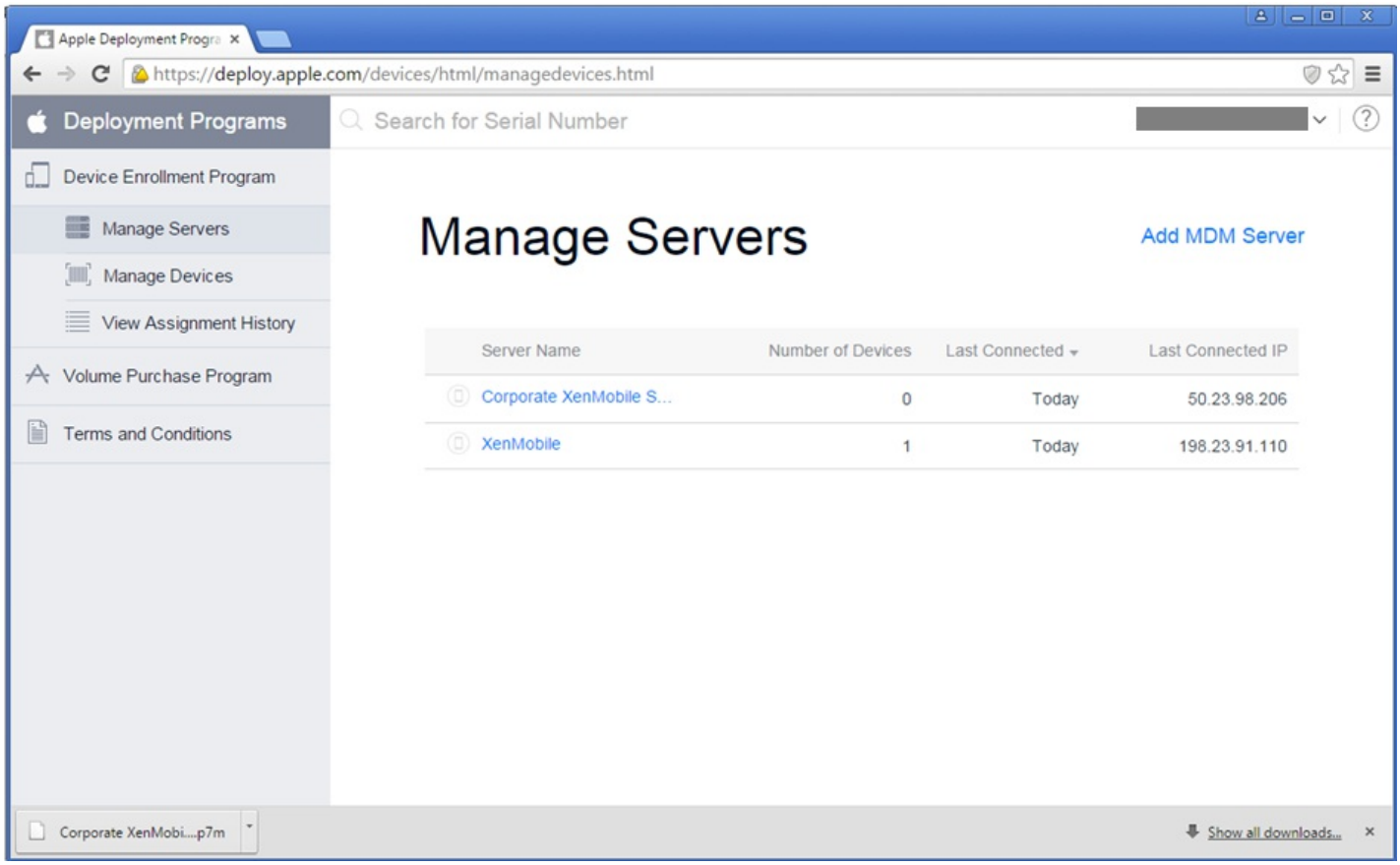
トークンファイルをインポートした後、Apple DEPトークン情報がXenMobileコンソールに表示されます。

8. [**Test Connection**] をクリックしてApple DEP接続をXenMobileで認証します。



9. [**iOS Bulk Enrollment**] ページで追加の設定を完了させて、Apple DEPデバイスに実装するApple DEPコントロールとポリシーを選択し、 [**Save**] をクリックします。

XenMobileサーバーがApple DEP Portalに表示されます。



DEP対応デバイスの注文

DEP対応デバイスをAppleから直接、またはDEP対応認証リセラーまたはキャリアから注文できます。 Appleから注文するには、Apple DEP Portal内でApple Customer IDを提供して、AppleがApple DEPアカウントにデバイス購入を割り当てられるようにする必要があります。

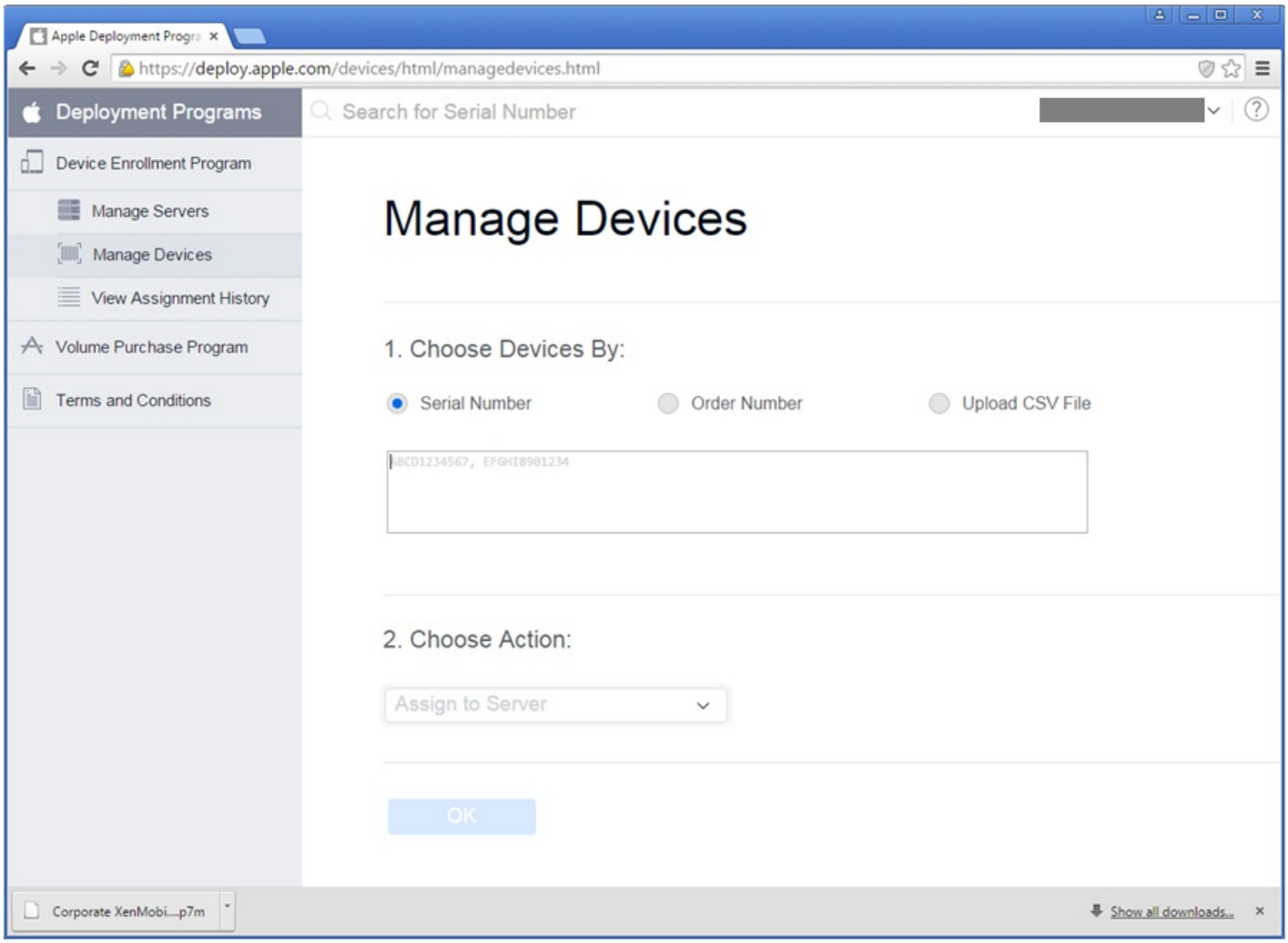
リセラーやキャリアから注文するには、Appleリセラーまたはキャリアに Apple DEPに参加しているかどうかを問い合わせます。 デバイスを購入する場合、リセラーのApple DEP IDが必要です。 Apple DEPリセラーをApple DEPアカウントに追加するにはこの情報が必要となります。 承認されたら、リセラーのApple DEP IDを追加した後にDEPカスタマーIDを受け取ります。 DEPカスタマーIDをリセラーに提供します。リセラーはこのIDを使ってデバイス購入に関する情報をAppleに送信します。 詳しくは、AppleのWebサイトを参照してください。

DEP対応デバイスの管理

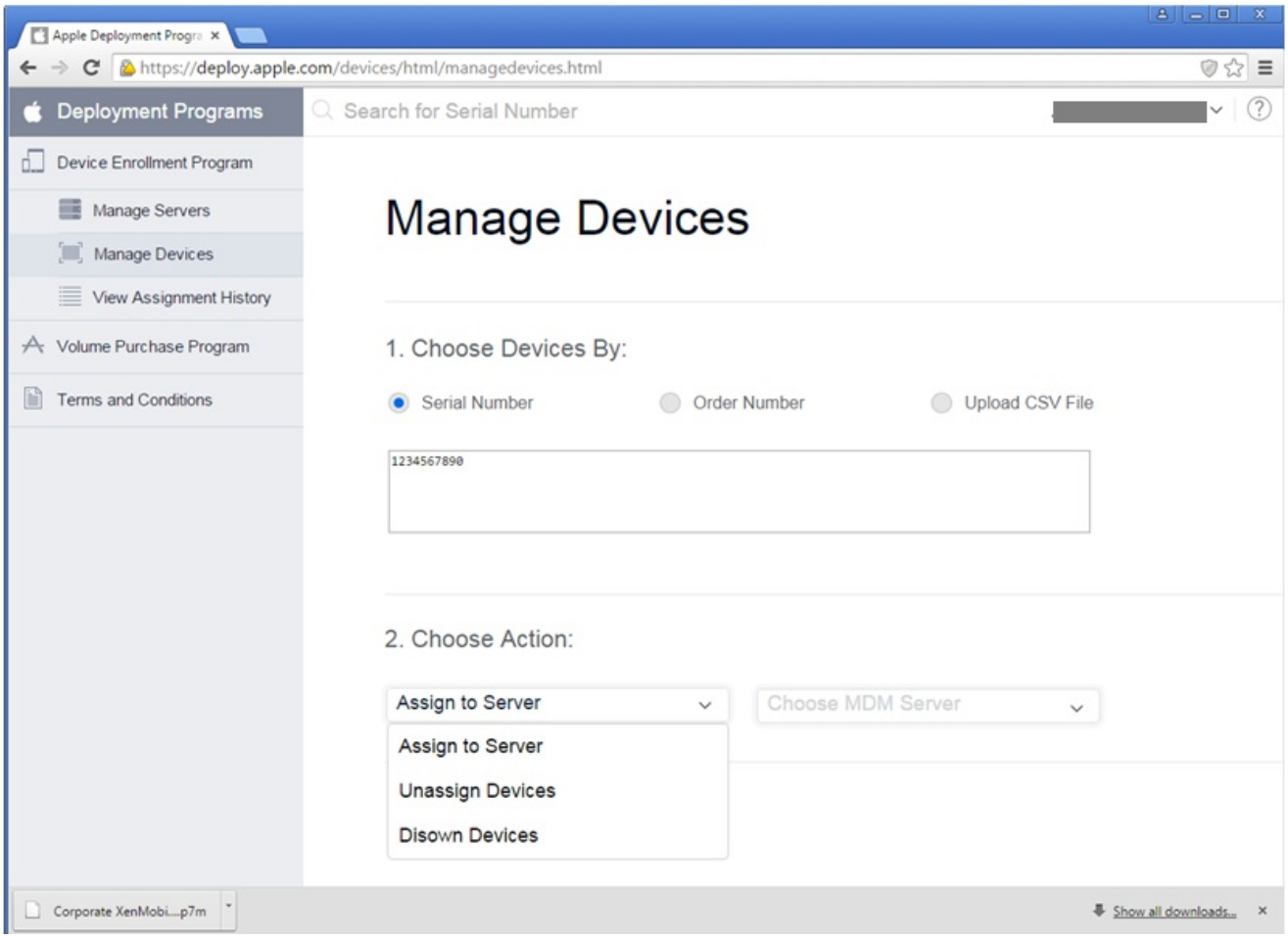
これらの手順に従って、DEP Portalを介してApple DEPアカウント内でデバイスをXenMobileサーバーに割り当てます。

1. Apple DEP Portalにログオンします。

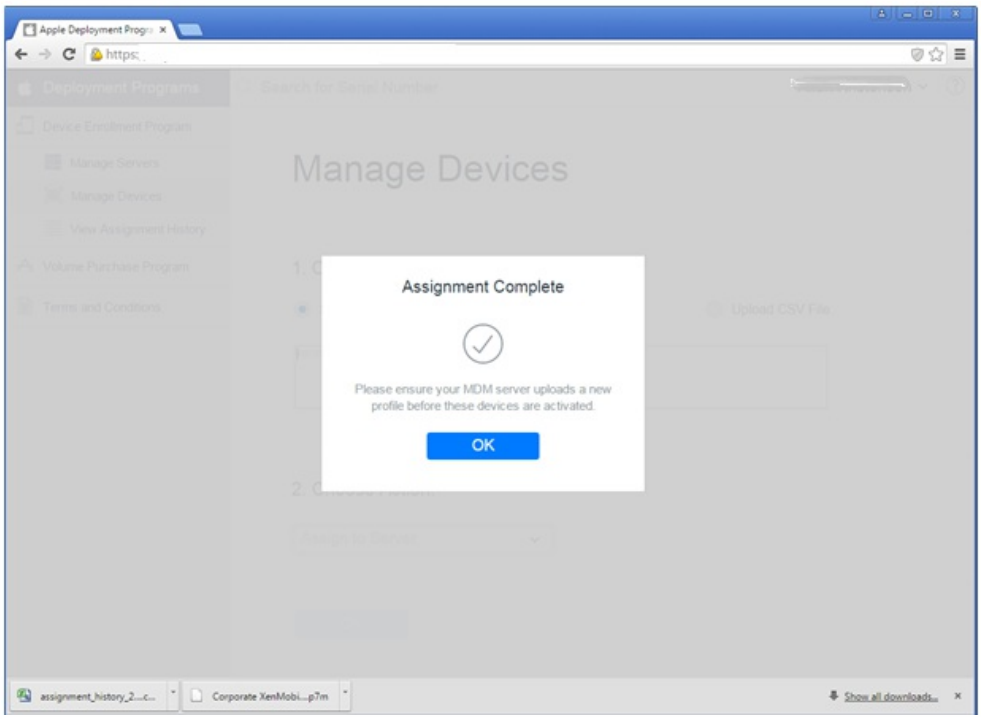
2. **[Device Enrollment Program]** をクリックして **[Manage Devices]** をクリックし、次に **[Choose Devices By]** でApple DEP対応デバイスをアップロードして定義するためのオプションである **[Serial Number]** 、 **[Order Number]** 、または **[Upload CSV File]** を選択します。



3. デバイスをXenMobileサーバーに割り当てるため、[**Choose Action**] で [**Assign to Server**] をクリックしてから一覧内でXenMobileサーバーの名前をクリックし、 [**OK**] をクリックします。



Apple DEPデバイスが選択したXenMobileサーバーに割り当てられました。



Apple DEP対応デバイス登録のユーザーエクスペリエンス

ユーザーがApple DEP対応デバイスを登録する場合の手順は次の通りです。

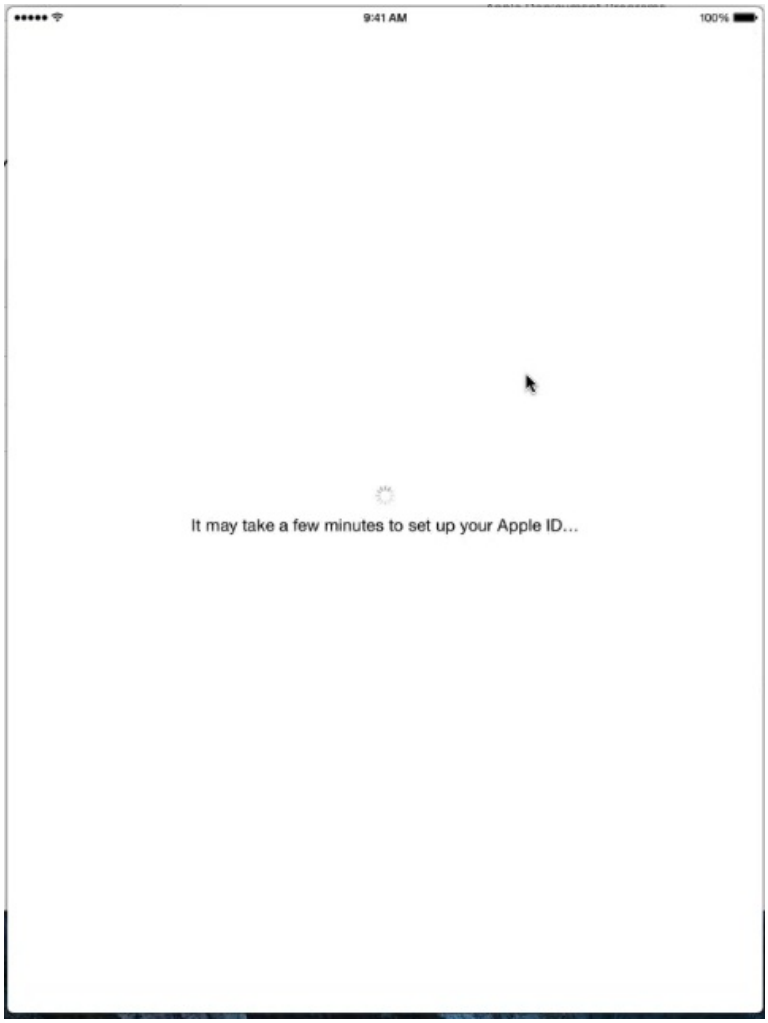
1. Apple DEP対応デバイスを開始します。

2. 構成ウィザードを使ってiOSデバイスで初期設定を構成します。

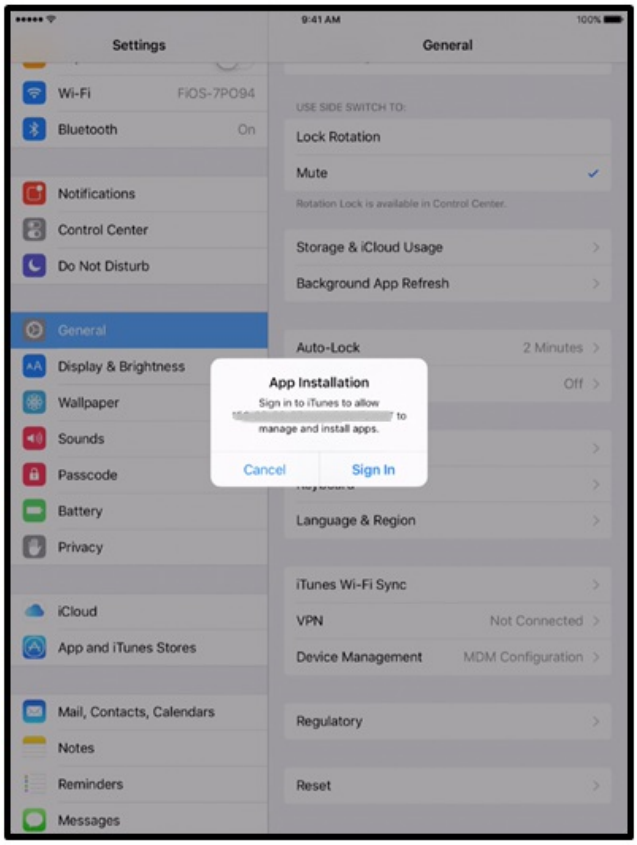
3. デバイスが自動的にXenMobileデバイス登録処理を開始します。 ウィザードの指示に従って、Apple DEP対応デバイスに割り当てられたXenMobileサーバー内にデバイスを登録します。

Apple DEP登録処理が、Apple DEP対応デバイスの初期iOS構成フローの一部として自動的に開始されます。

4. XenMobileコンソールで構成したApple DEP構成がApple DEP対応デバイスに配信されます。 ユーザーはウィザードの指示に従って、デバイスを構成します。



5. Worx Homeのダウンロードが可能になるよう、iTunesへのサインインを求めるプロンプトが表示されることがあります。



6. Worx Homeを開いて資格情報を入力します。 ポリシーにより求められる場合、Worx PINを作成して検証するようプロンプトが表示されることがあります。

必須アプリについてのリマインダーがデバイスに表示されます。

iOS Volume Purchase Planの設定

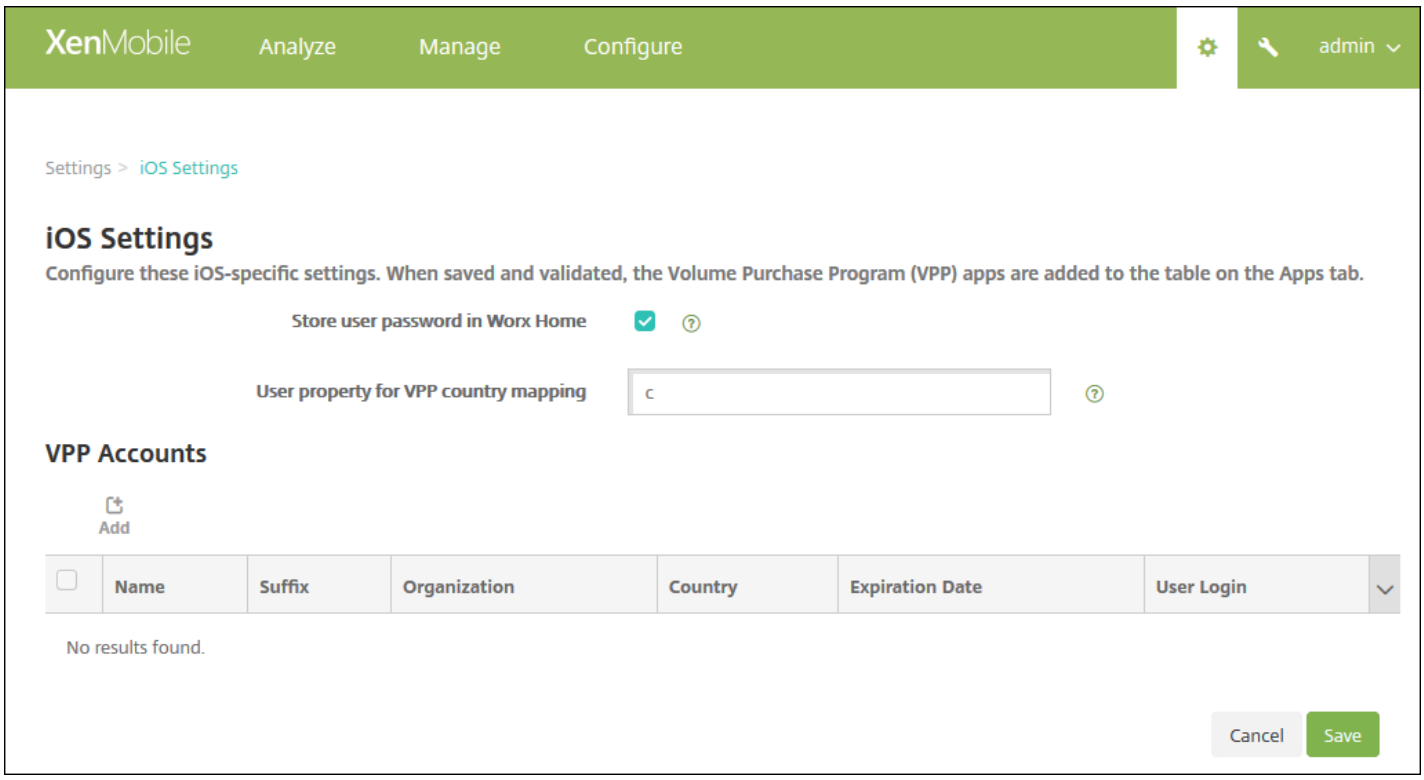
Aug 02, 2016

XenMobileで、iOS Volume Purchase Plan（VPP）に固有の設定を構成できます。 iOS VPPを利用すると、組織のアプリケーションやそのほかの大量なデータの検索、購入、配布の処理が簡単になります。 VPPは、組織のコンテンツニーズを管理するためのシンプルでスケーラブルなソリューションを提供します。

XenMobileでiOS VPP設定を保存して検証すると、購入したアプリケーションがXenMobileコンソールの［Apps］タブの表に追加されます。

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

2. **［Server］**の下の**［iOS Settings］**をクリックします。 **［iOS Settings］**構成ページが開きます。



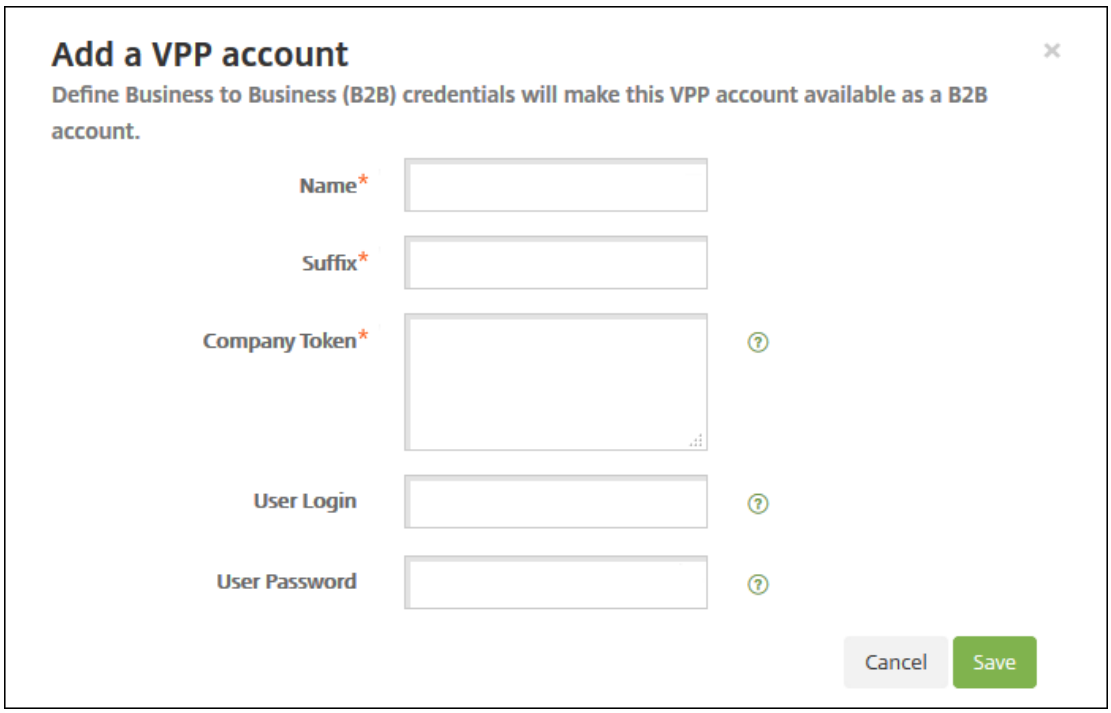
3. 次の設定を構成します。

- **Store user password in Worx Home**：XenMobile認証用のユーザー名とパスワードをWorx Homeに安全に保存するかどうかを選択します。 デフォルトでは情報は保存されます。
- **User property for Volume Purchasing Program (VPP) country mapping**：ユーザーが国固有のアプリケーションストアからアプリケーションをダウンロードできるようにするコードを入力します。

  このマッピングはVPPのプロパティプールの選択に使用されます。 たとえば、ユーザープロパティが米国で、アプリケーションのVPPコードが日本で配布されている場合、そのユーザーはそのアプリケーションをダウンロードすることはできません。 国マッピングコードについて詳しくは、VPPプラン管理者に問い合わせてください。

VPP Accounts

- 追加するVPP アカウント ごとに、［**Add**］をクリックします。 ［**Add VPP account**］ダイアログボックスが開きます。



追加するアカウントごとに、次の設定を構成します。

- **Name**：VPPアカウント名を入力します。
- **Suffix**：VPPアカウントを介して取得したアプリケーションに表示されるサフィックスを入力します。
- **Company Token**：Appleから取得したVPPサービストークンを入力するか、コピーして貼り付けます。 トークンを取得するには、Apple VPPポータルの［アカウント概要］ページで［ダウンロード］をクリックし、VPPファイルを生成してダウンロードします。 このファイルには、サービストークンのほかに、国コードや有効期限などの他の情報も含まれます。 ファイルを安全な場所に保存します。
- **User Login**：任意で、認証済みVPPアカウントの ユーザー名を入力します。
- **User Password**：任意で、VPPアカウントのユーザーパスワードを入力します。

5. ［**Save**］をクリックしてダイアログボックスを閉じます。

6. ［**Save**］をクリックしてiOS設定を保存します。

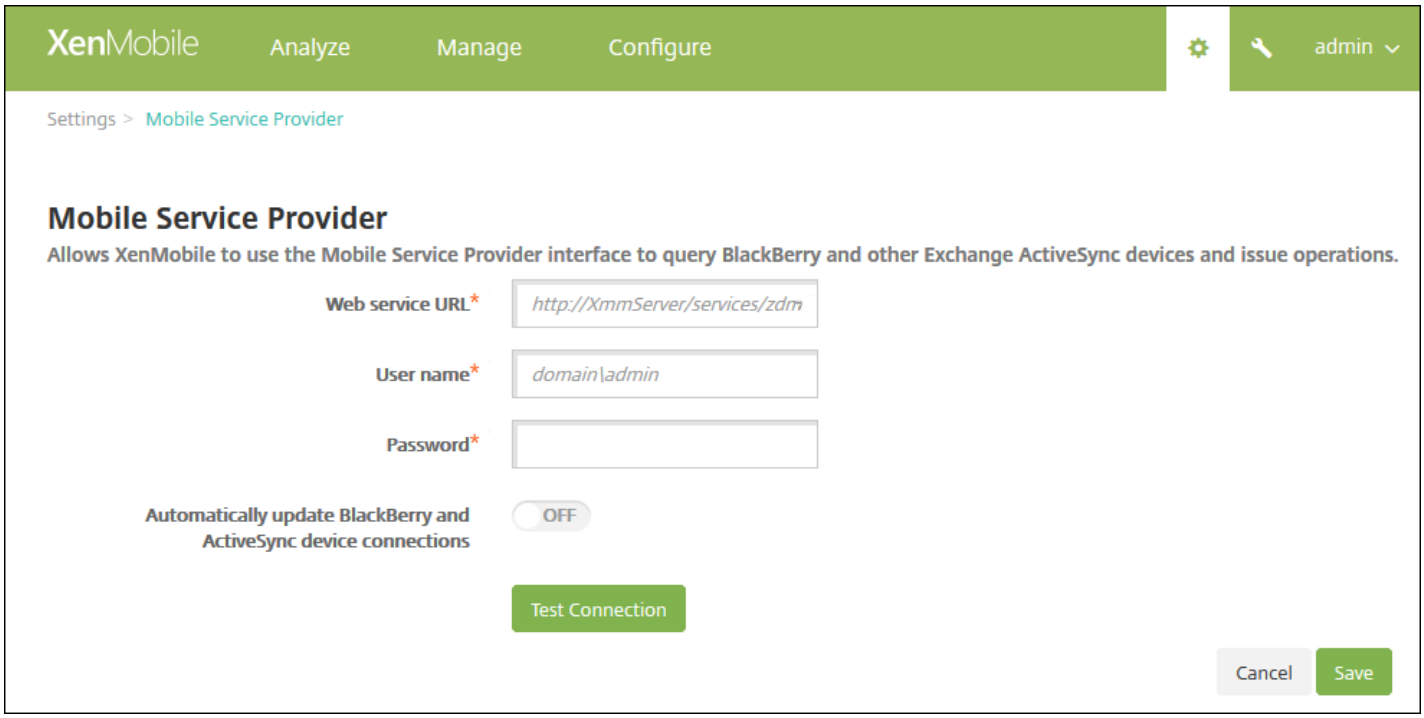
Mobile Service Provider

Aug 02, 2016

XenMobileでMobile Service Providerインターフェイスの使用を有効にして、BlackBerryやそのほかのExchange ActiveSyncデバイスに対してクエリを実行したり、操作を発行したりすることができます。

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

2. **[Server]** の下の **[Mobile Service Provider]** をクリックします。 **[Mobile Service Provider]** ページが開きます。



3. 次の設定を構成します。

- **Web service URL**：WebサービスのURL（http://XmmServer/services/xdmserviceなど）を入力します。
- User name：「domain\admin」の形式でユーザー名を入力します。
- **Password**：パスワードを入力します。
- **Automatically update BlackBerry and ActiveSync device connections**：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 **[OFF]** です。
- **[Test Connection]** をクリックして、接続を検証します。

4. **[Save]** をクリックします。

ネットワークアクセス制御

Aug 02, 2016

XenMobileで、Cisco ISEなどのNAC（Network Access Control：ネットワークアクセス制御）アプライアンスをネットワークで設定する場合は、フィルターで規則またはプロパティに基づいてデバイスをNACに準拠または非準拠として設定することができます。 XenMobileの管理対象デバイスが指定された条件を満たしておらず、その結果［非準拠］としてマークされている場合、そのデバイスはNACアプライアンスによりネットワーク上でブロックされます。

XenMobileコンソールの一覧で、デバイスを非準拠として設定する条件を1つまたは複数選択します。

XenMobileは、次のNACコンプライアンスフィルターをサポートします。

匿名デバイス： デバイスが匿名モードではないかを確認します。 これは、デバイスが再接続を試みたとき、XenMobileがユーザーを再認証できない場合に確認のために使用します。

Samsung KNOXで構成証明に失敗しました： デバイスが、Samsung KNOX構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ： デバイス上に［アプリアクセスポリシー］で定義された禁止アプリがないかを確認します。

暗示的許可および拒否： これは、ActiveSync ゲートウェイのデフォルトの操作です。その他のフィルター規則条件を満たしていないすべてのデバイスのデバイス一覧を作成し、一覧に基づいて接続を許可または拒否します。 一致する規則がなければ、デフォルトは［暗示的許可］になります。

非アクティブデバイス： ［サーバー プロパティ］でデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。

不足必須アプリ： デバイスに［アプリ アクセス ポリシー］で定義された必須アプリの不足がないかを確認します。

非推奨アプリ： デバイスに［アプリ アクセス ポリシー］で定義された非推奨アプリがないかを確認します。

非準拠パスワード： ユーザーパスワードが正しいかを確認します。 XenMobileが、iOSおよびAndroidデバイス上で、現在デバイスにあるパスワードがデバイスに送られたパスコードポリシーに準拠しているかを確認します。 たとえばiOSの場合、ユーザーはXenMobileがデバイスにパスコードを送ってから60分以内に、パスワードを設定する必要があります。 さもなければ、ユーザーがパスワードを設定する前に、パスコードが非準拠になる可能性があります。

コンプライアンス外デバイス： ［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス外かどうかを確認します。 このプロパティは通常、自動化された操作によって変更されたり、XenMobile APIを使用するサードパーティによって変更されたりします。

失効状態： デバイスの証明書が失効していないかを確認します。 証明書が失効したデバイスは、再度認証されるまで再登録できません。

ルート化されたAndroidおよびジェイルブレークしたiOSデバイス：AndroidまたはiOSデバイスがジェイルブレークされていないかを確認します。

非管理デバイス： デバイスがまだXenMobileの管理下にあるかを確認します。 たとえば、MAMモードで実行されているデバイス、あるいは登録されていないデバイスは、管理下にありません。

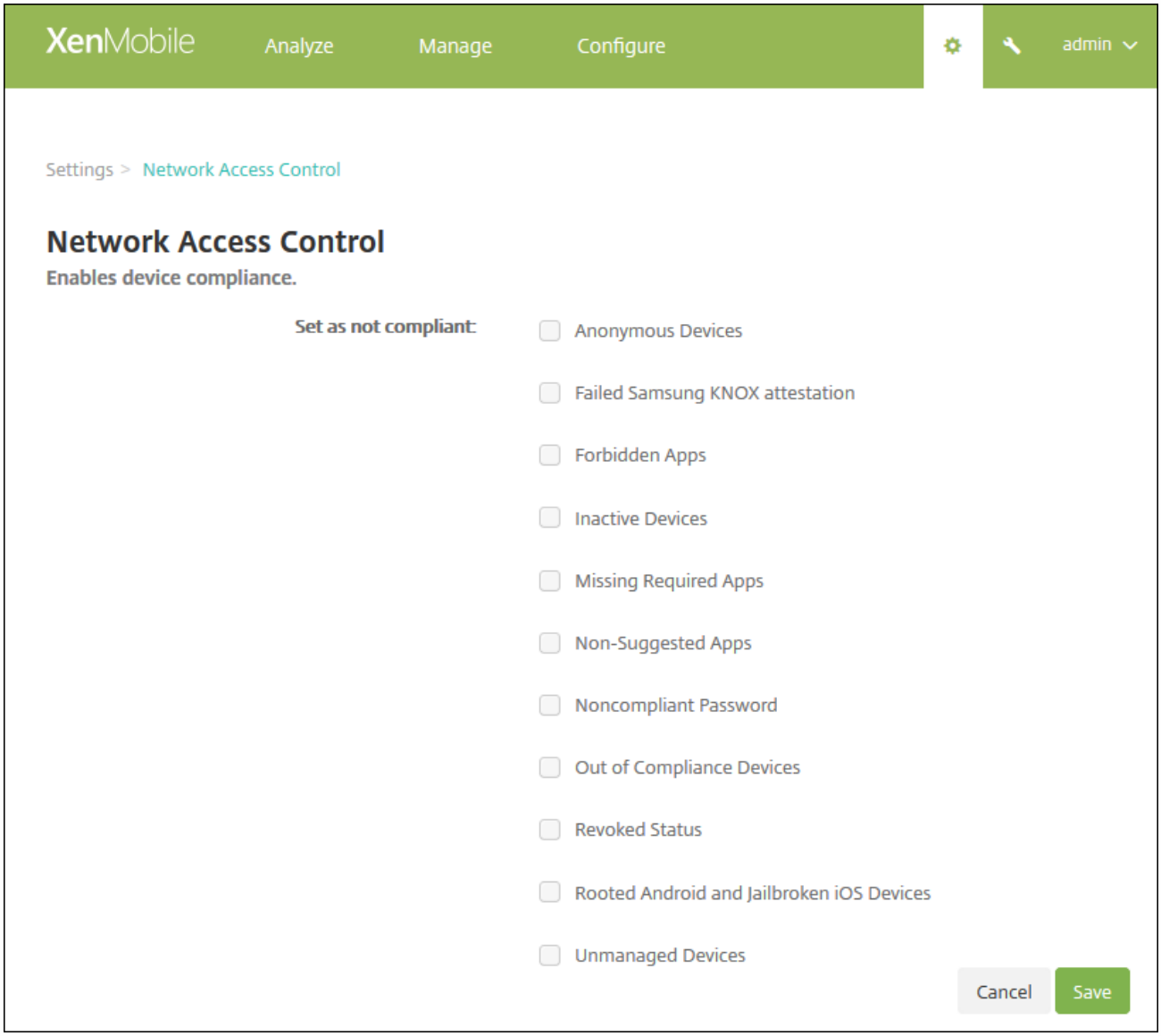
Androidドメイン ユーザーをActiveSync Gatewayに送信： ［はい］ をクリックすることで、XenMobileがAndroidデバイスの情報をActiveSyncゲートウェイに送信されるようにします。 このオプションを有効にすると、Androidデバイスユーザーの

ActiveSync識別子がXenMobileにない場合でも、XenMobileによってAndroidデバイスの情報が ActiveSyncゲートウェイに送信されます。

> **注意**
>
> ［Implicit Compliant］または［Not Compliant］フィルターは、XenMobileによる管理対象デバイスでのみデフォルト値を設定します。たとえば、ブラックリストに入っているアプリケーションがインストールされているデバイスや、登録されていないデバイスは［Not-Compliant］としてマークされ、NACアプライアンスによりネットワークからブロックされます。

ネットワークアクセス制御の構成

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。［**Settings**］ページが開きます。
2. ［**Server**］の下の［**Network Access Control**］をクリックします。［**Network Access Control**］ページが開きます。



3. **[非準拠として設定]** フィルターで有効にしたい項目のチェックボックスを選択します。
4. **[保存]** をクリックします。

Samsung KNOX

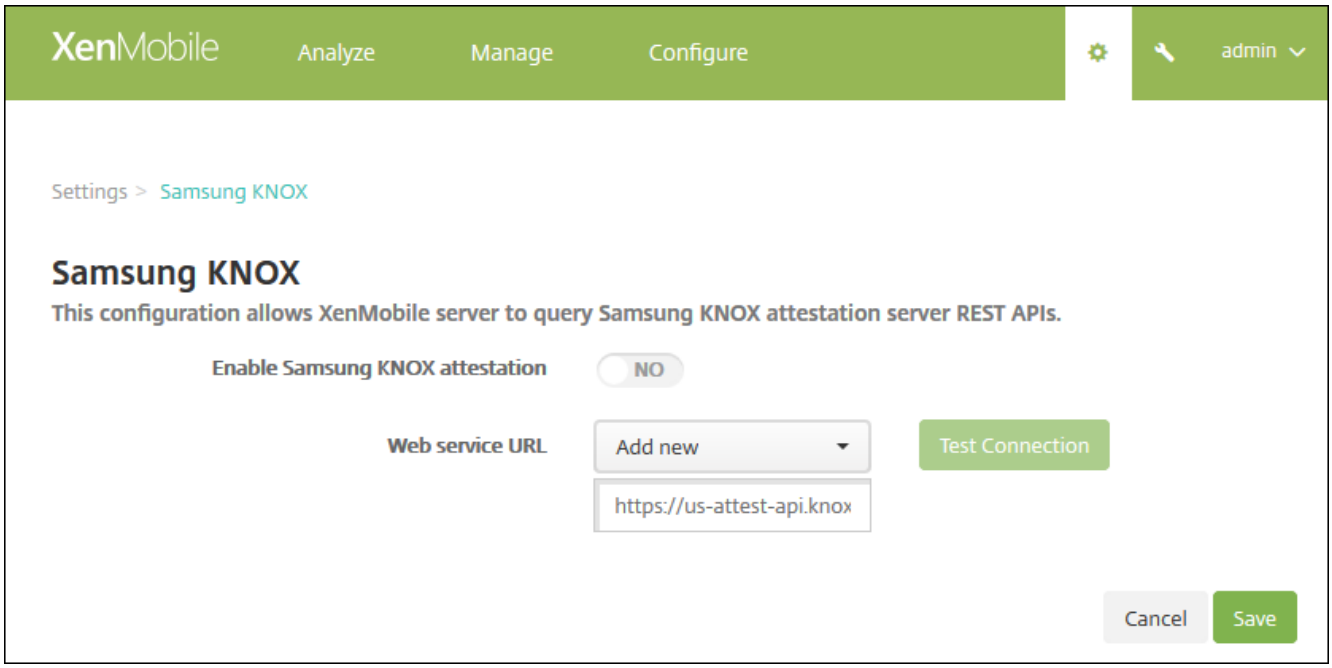
Aug 02, 2016

XenMobileを構成して、Samsung KNOX認証サーバーREST APIに対するクエリを実行できます。

Samsung KNOXは、オペレーティングシステムとアプリケーションを複数レベルで保護する、ハードウェアセキュリティ機能を利用します。 このセキュリティの1つのレベルは、認証を通じてプラットフォームに存在します。 認証サーバーは、信頼できる起動時に収集されるデータに基づき、実行時に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。

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

2. **[Server]** の下の **[Samsung KNOX]** をクリックします。 **[Samsung KNOX]** ページが開きます。



3. 次の設定を構成します。

- **Enable Samsung KNOX attestation**：Samsung KNOX認証を有効にするかどうかを選択します。 デフォルトは **[NO]** です。 **[Enable Samsung KNOX attestation]** を有効にすると、 **[Web service URL]** オプションが有効になります。
- 一覧から、適切な認証サーバーを選択します。

4. **[Test Connection]** をクリックして、接続を検証します。

5. **[Save]** をクリックします。

> ## 注意
>
> SamSung KNOX Mobile Enrollmentを使用すると、複数のSamsung KNOXデバイスをXenMobile（または、その他のMobile Device Manager）に登録する場合に、各デバイスを手動で構成する必要がありません。 詳しくは、「Samsung KNOX Bulk Enrollment」を

参照してください。

サーバープロパティを追加、編集、または削除するには

Aug 02, 2016

XenMobileには、サーバー全体の操作に適用される100以上のプロパティがあります。 この文書では重要なサーバープロパティおよびサーバープロパティを 追加、編集、または削除する方法について説明します。

サーバープロパティ定義

Audit Log Cleanup Execution Time

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

Audit Log Cleanup Interval (in Days)

XenMobileサーバーが監査ログを保持する日数。 デフォルトは**1**です。

Audit Logger

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

Audit Log Retention (in Days)

XenMobileサーバーが監査ログを保持する日数。 デフォルトは**7**です。

Deploy Log Cleanup (in Days)

XenMobileサーバーが展開ログを保持する日数。 デフォルトは**7**です。

Disable SSL Server Verification

Trueの場合、次の条件がすべて満たされていると、SSLサーバー証明書確認が無効になります：XenMobileサーバーで証明書ベースの認証を有効にしている、Microsoft CAサーバーが証明書の発行元である、XenMobileサーバーによってルートが信頼されていない内部CAが証明書に署名している。 デフォルト値は **True**です。

Inactivity Timeout in Minutes

XenMobileサーバーのパブリックAPIを使用してXenMobileコンソールやサードパーティ製アプリケーションにアクセスした非アクティブな管理者がログアウトされるまでの分数。 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 **5**です。

NetScaler Single Sign-On

Falseの場合、NetScalerからXenMobileサーバーへのシングルサインオン実行中にXenMobileコールバック機能が無効にされます。 コールバック機能は、NetScaler Gateway構成にコールバックURLが含まれる場合に、NetScaler Gatewayセッション IDの確認に使用されます。 デフォルト値は **False**です。

Session Log Cleanup (in Days)

XenMobileサーバーがセッションログを女児する日数。 デフォルトは**7**です。

Unauthenticated App Download for Android Devices

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

Unauthenticated App Download for Windows Devices

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

XAM One-Time Ticket

ワンタイム認証トークン（OTT）がアプリケーションをダウンロードするのに有効なミリ秒の数。 このプロパティは、未認証のアプリケーションのダウンロードを許可するかどうかを指定するプロパティ**Unauthenticated App download for Android**および**Unauthenticated App download for Windows**とともに機能します。 デフォルトは **3600000**です。

XenMobile MDM Self Help Portal console max inactive interval (minutes)

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

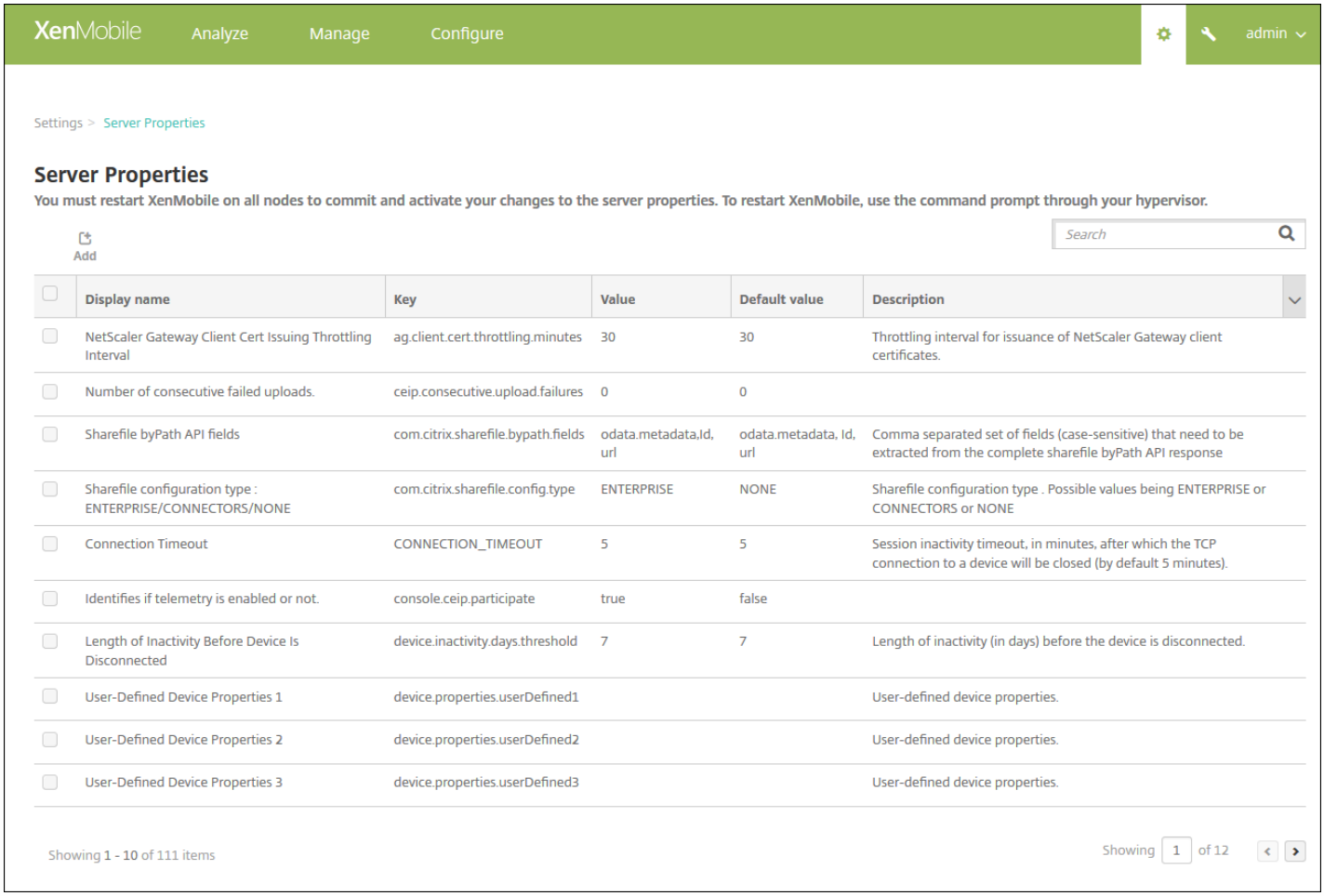
サーバープロパティを追加、編集、または削除するには

XenMobileで、サーバーにプロパティを適用できます。 変更を行った後、すべてのノードでXenMobileを再起動し、変更を確定して有効化する必要があります。

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

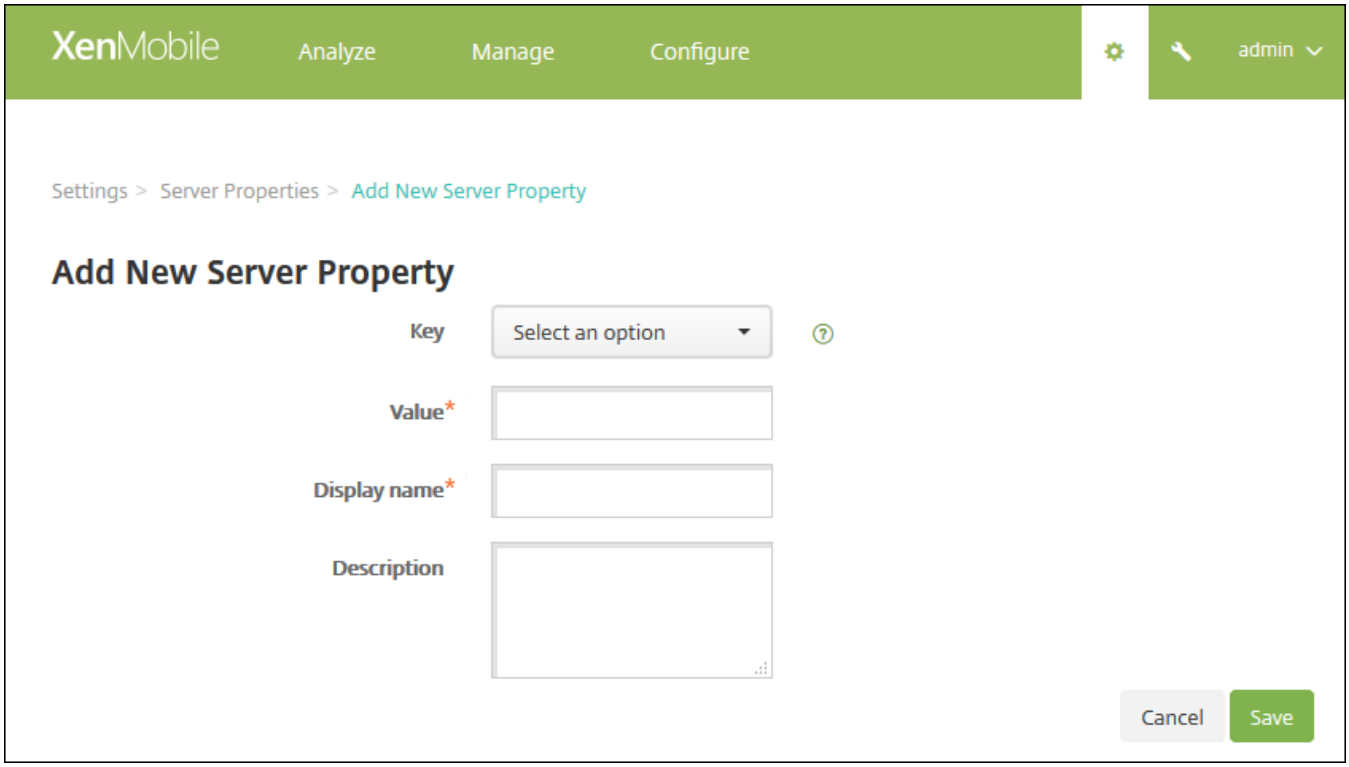
1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。

2. **[Server]** の下の **[Server Properties]** をクリックします。 **[Server Properties]** ページが開きます。 このページでは、サーバープロパティを追加、編集、または削除できます。



サーバープロパティを追加するには

1. **[Add]** をクリックします。 **[Add New Server Property]** ページが開きます。



2. 次の設定を構成します。

- **Key**：一覧から、適切なキーを選択します。 キーでは大文字と小文字が区別されます。 変更を行う前にCitrixのサポート担当者に問い合わせるか、特殊キーを要求する必要があります。
- **Value**：選択したキーに応じて値を入力します。
- **Display name**： **[Server Properties]** の表に表示される、新しいプロパティ値の名前を入力します。
- **Description**：任意で、新しいサーバープロパティの説明を入力します。

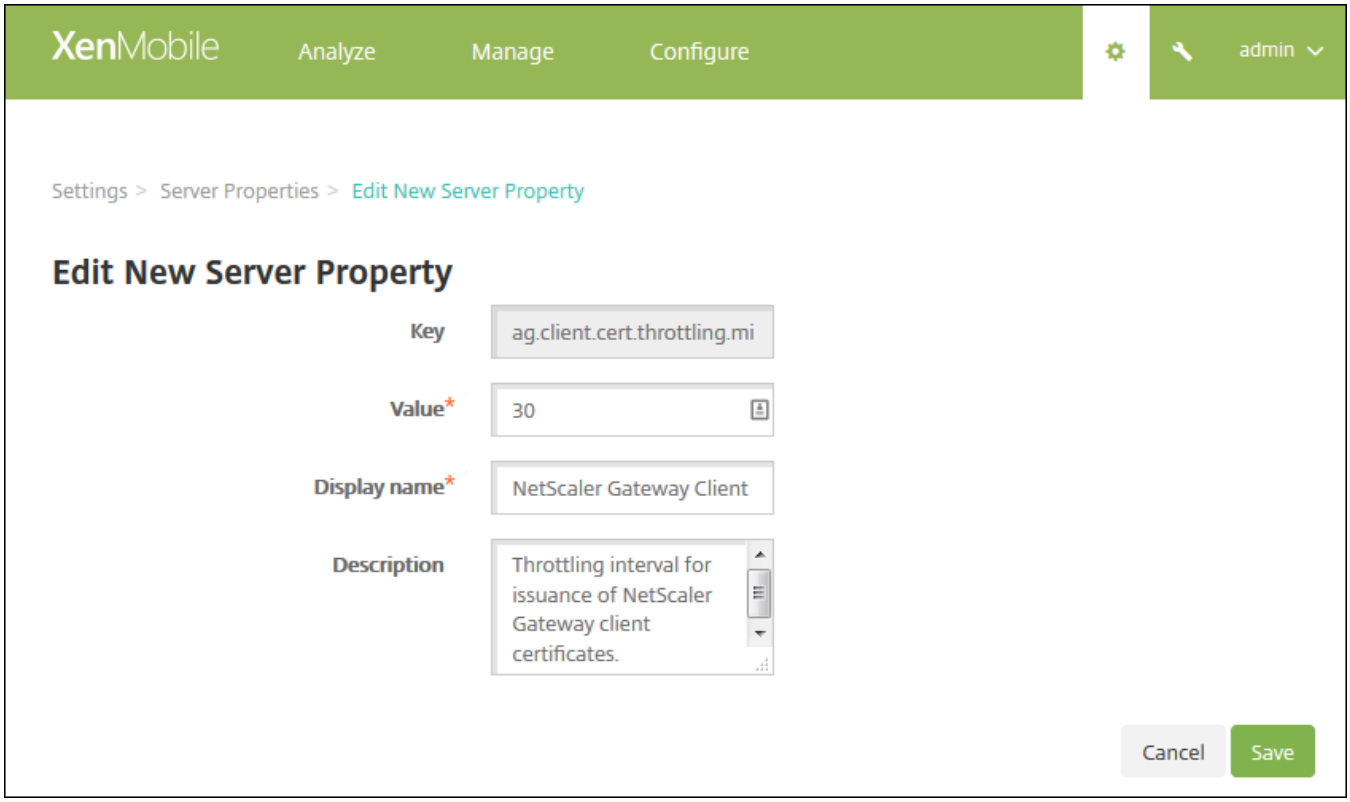
3. **[Save]** をクリックします。

サーバープロパティを編集するには

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

> **注：**サーバープロパティの横にあるチェックボックスをオンにすると、サーバープロパティ一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。

2. **[Edit]** をクリックします。 **[Edit New Server Property]** ページが開きます。



3. 必要に応じて以下の情報を変更します。

- **Key**：このフィールドは変更できません。
- **Value**：プロパティの値です。
- **Display Name**：プロパティの名前です。
- **Description**：プロパティの説明です。

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

サーバープロパティを削除するには

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

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

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

XenMobileの有効なサーバーモードの構成

Aug 02, 2016

XenMobileのサーバーモードはサーバープロパティに含まれる値セットです。 MAM、MDM、またはENTに設定することができ、アプリケーション管理、デバイス管理、またはアプリケーションおよびデバイス管理に対応しています。 次の表に示すように、デバイスの登録方法に応じて、サーバーモードプロパティを設定します。 ライセンスの種類にかかわらず、サーバーモードのデフォルト値はENTです。

サーバーモードの設定について詳しくは、「サーバープロパティを追加、編集、または削除するには」を参照してください。

次の表は、特定のライセンスの種類および機能のデバイスモードで使用するサーバーモードの概要を示しています。

現在のエディションのライセンス	デバイスを登録するモード	必要なサーバーモードプロパティの設定
ENT/ADV/MDM	MDMモード	MDM
ENT/ADV	MAMモード（MAM-onlyモードとも呼ばれます）	MAM
ENT/ADV	MDM+MAMモード	ENT デバイス管理を行わないユーザーは従来のMAMモードで操作します。

*有効なサーバーモード*とは、サーバーモードとインストールされているライセンスの種類の組み合わせです。 MDMライセンスの場合は、サーバーモードにかかわらず、有効なサーバーモードは常にMDMです。 これは、MDMエディションの場合、サーバーモードをMAMまたはENTに設定しても、アプリケーション管理を有効にできないことを意味します。 エンタープライズおよび上級ライセンスの場合、有効なサーバーモードはサーバーモードに一致します。

サーバーモードは、ライセンスがアクティブ化または削除されるたびに、そしてサーバープロパティでサーバーモードが変更されるときにサーバーログに追加されます。 ログファイルの作成と表示については、「XenMobileのサポートおよび保守」を参照してください。

Syslog

Aug 02, 2016

XenMobileを構成して、ログファイルをシステムログ（Syslog）サーバーに送信できます。 サーバーのホスト名またはIPアドレスが必要です。

Syslogは、監査モジュール（アプライアンス上で実行）とサーバー（リモートシステムで実行可能）の2つのコンポーネントを使用する、標準ロギングプロトコルです。 Syslogプロトコルでは、データ転送でユーザーデータプロトコル（UDP）を使用します。 管理者イベントとユーザーイベントが記録されます。

サーバーを構成して、以下の種類の情報を収集できます。

- XenMobileで実行されたアクションの記録が含まれるシステムログ
- XenMobileのシステムアクティビティの時系列の記録が含まれる監査ログ

syslogサーバーが アプライアンスから 収集したログ情報は、メッセージ形式でログファイルに保存されます。 通常、これらのメッセージには次の情報が含まれています。

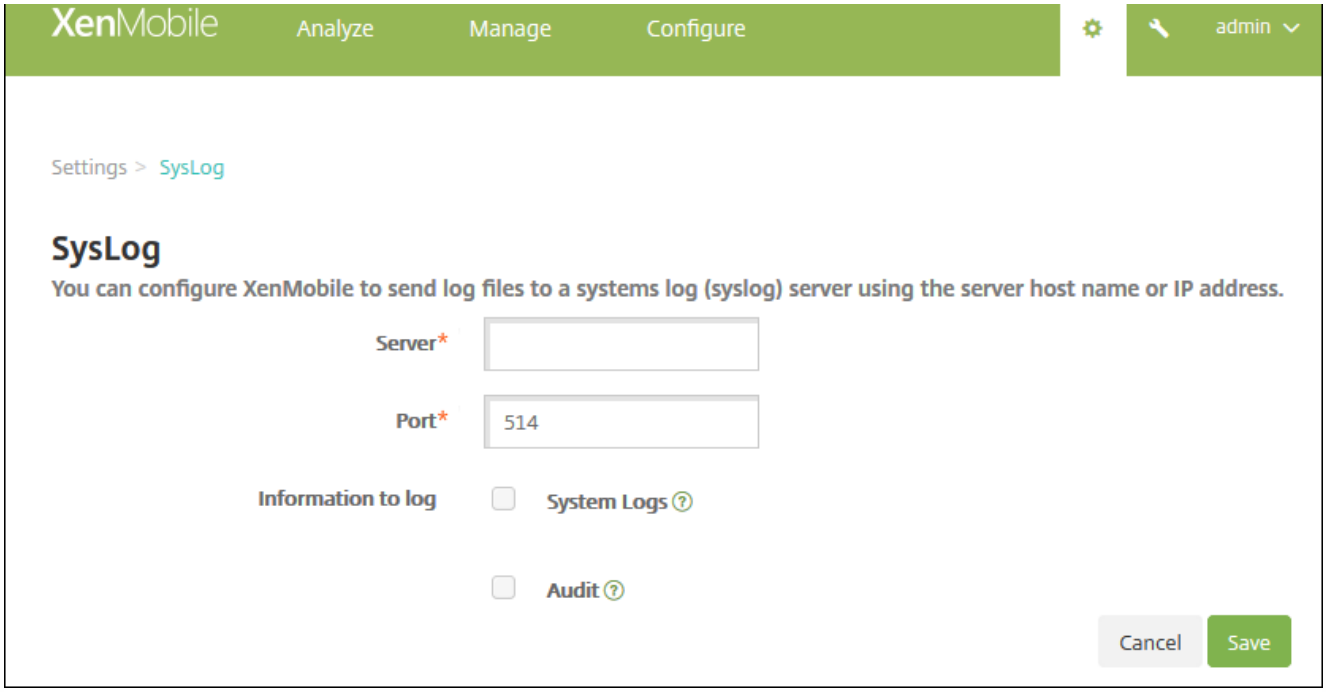
- ログメッセージを生成したアプライアンスのIPアドレス
- タイムスタンプ
- メッセージの種類
- イベントに関連付けられたログレベル（重要、エラー、通知、警告、情報、デバッグ、アラート、または緊急）
- メッセージの情報

この情報を使用してアラートの原因を分析したり、必要に応じて修正作業を行ったりすることができます。

> ## 注意
>
> XenMobileクラウド環境では、オンプレミスのsyslogサーバーとのsyslog統合はサポートされません。 代わりに、Xen Mobileコンソールの［Support］ページからログをダウンロードできます。 これを行う場合は、 **［Download All］**をクリックしてシステムログを取得する必要があります。 詳しくは、「XenMobileでのログファイルの表示および分析」を参照してください。

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

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



3. 次の設定を構成します。

- **Name**：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。
- **Port**：ポート番号を入力します。 デフォルトのポート番号は、514です。
- **Information to log**： **[System Logs]** チェックボックスおよび **[Audit]** チェックボックスをオンまたはオフにします。
  - システムログには、XenMobileで実行されたアクションが含まれます。
  - 監査ログには、XenMobileのシステムアクティビティの時系列の記録が含まれます。

4. **[Save]** をクリックします。

XenAppおよびXenDesktopを構成するには

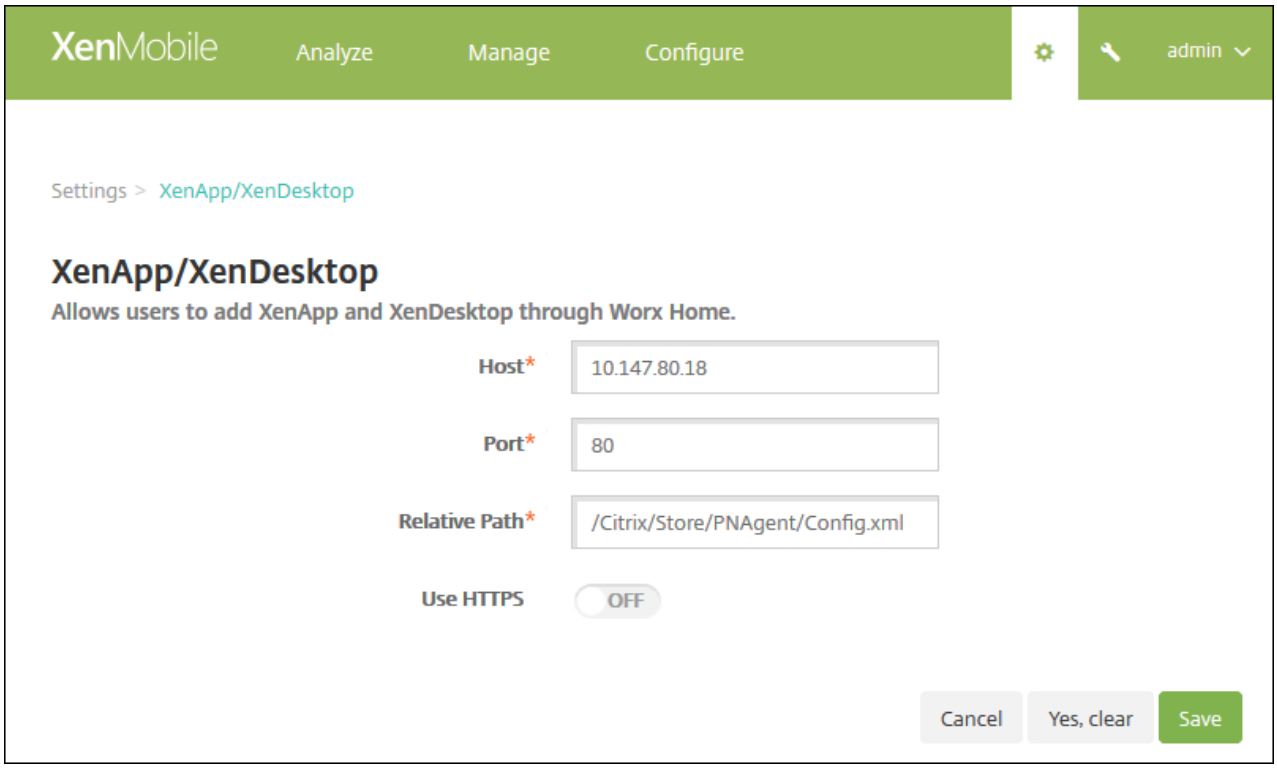
Aug 02, 2016

XenMobileでは、XenAppおよびXenDesktopからアプリケーションを収集して、Worx Storeでモバイルデバイスユーザーがそのアプリケーションを使用できるようにすることができます。 ユーザーは、Worx Store内から直接アプリケーションをサブスクライブして、Worx Homeから起動します。 アプリケーションを起動するために、 Receiverをユーザーのデバイスにインストールする必要があります。ただし、構成する必要はありません。

この設定を構成するには、Web InterfaceサイトまたはStoreFrontの完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）またはIPアドレスと、ポート番号が必要です。

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

2. **[XenApp/XenDesktop]** をクリックします。 **[XenApp/XenDesktop]** ページが開きます。



3. 次の設定を構成します。

- **Host:**：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。
- **Port**：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。
- **Relative Path**：パスを入力します。 たとえば、「/Citrix/PNAgent/config.xml」と入力します。
- **Use HTTPS**：Web InterfaceサイトまたはStoreFrontとクライアントデバイスの間で安全な認証を有効にするかどうかを選択します。 デフォルトは **[OFF]** です。

4. **[Save]** をクリックします。

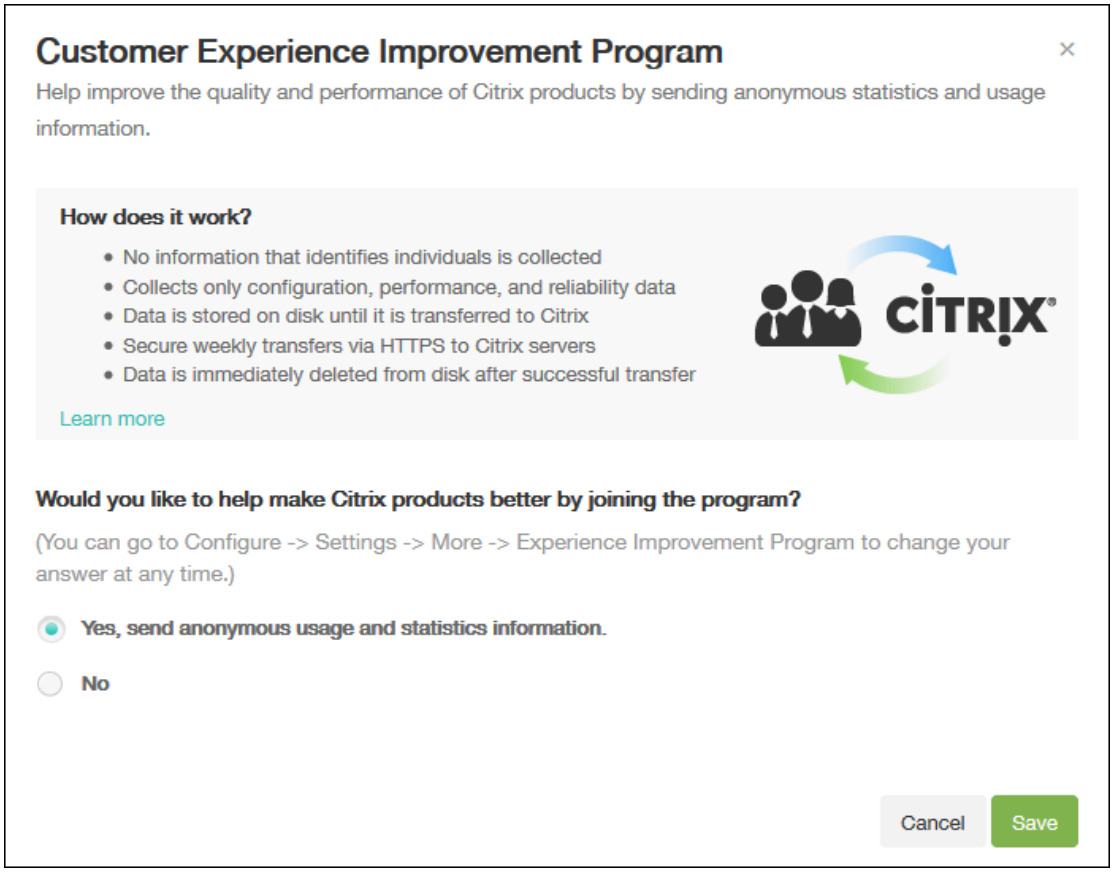
カスタマーエクスペリエンス向上プログラム

Aug 02, 2016

Ctrixカスタマーエクスペリエンス向上プログラム（CEIP）では、XenMobileの構成および使用に関するデータが匿名で収集され、そのデータがCitrixに自動的に送信されます。 このデータは、XenMobileの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。 CEIPへのご参加は任意です。 XenMobileの初回インストール時、または更新のインストール時に、CEIPへの参加が可能です。 選択した場合、データは通常週単位で、パフォーマンスおよび使用に関するデータは時間単位で収集されます。 これらのデータはディスク上に格納され、1週間ごとにHTTPSにより安全にCitrixに送信されます。 CEIPに参加するかどうかは、XenMobileコンソールで変更できます。 CEIPについて詳しくは、『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。

XenMobileのインストールまたは更新時のCEIP

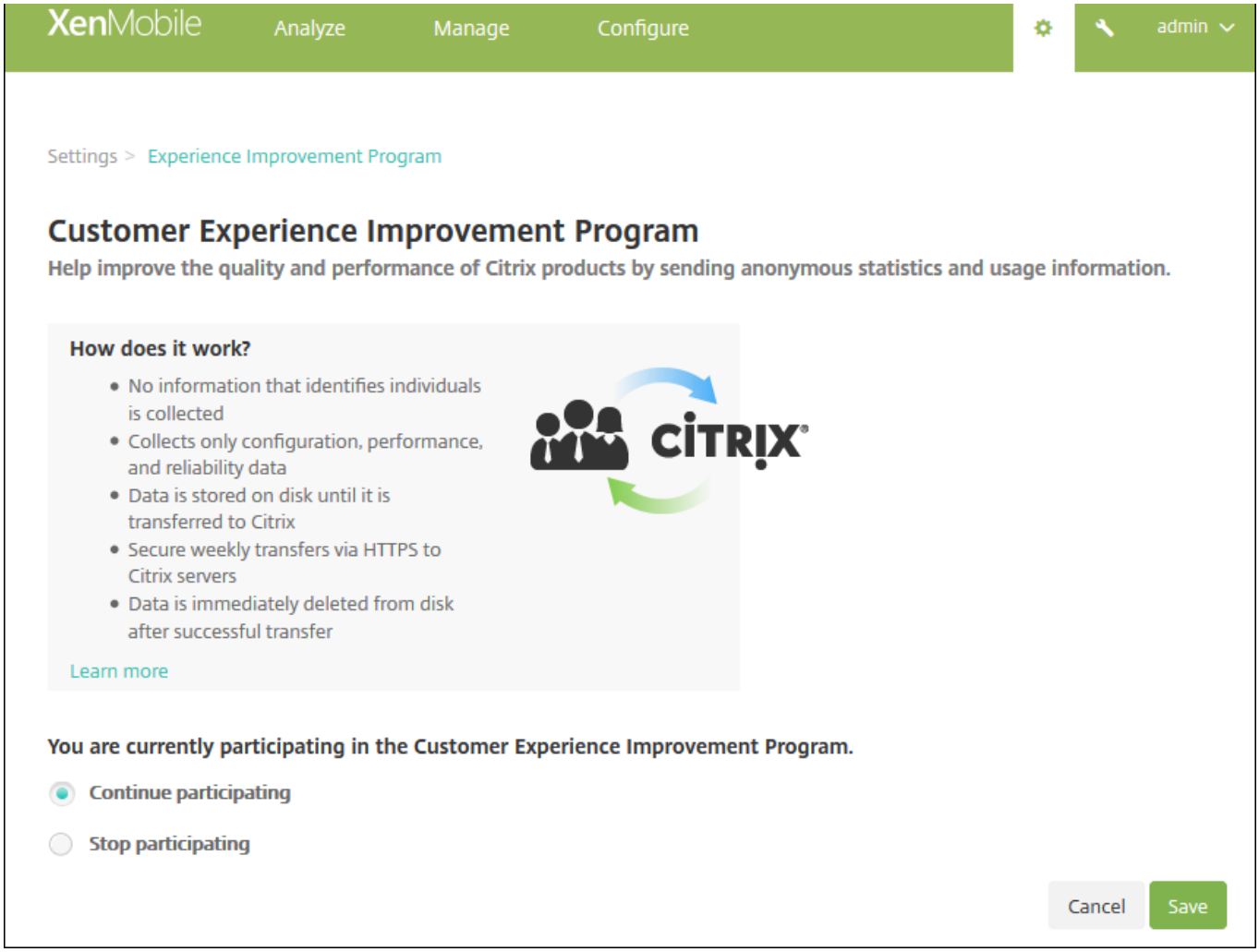
XenMobileの初回インストール時、または更新時に、以下のダイアログボックスが表示されます。ここで、参加するかどうかを選択し、 **[Save]** をクリックします。



CEIP参加設定の変更

1. CEIP参加設定を変更するには、XenMobileコンソールで右上の歯車アイコンをクリックして **[Settings]** ページを開きます。

2. **[Server]** の下で **[Experience Improvement Program]** をクリックします。 **[Customer Experience Improvement Program]** ページが開きます。 表示される実際のページは、現在CEIPに参加しているかどうかによって異なります。



3.現在CEIPに参加していて、中止を希望する場合、**[Stop participating]** をクリックします。

4.現在CEIPに参加していなくて、開始を希望する場合、**[Start participating]** をクリックします。

5. **[Save]** をクリックします。

Microsoft Azureの設定

Aug 02, 2016

Windows 10が実行されているデバイスを、AzureをActive Directory認証の統合手段として使用して登録します。 管理者は、以下のいずれかの方法を用いてWindows 10デバイスをMicrosoft Azure ADに統合できます。

- 初めてデバイスの電源を入れたときに、特別な設定をすることなくAzure AD統合の一部としてMDMに登録する。
- デバイスを構成したあとに、［Windows Settings］ページからAzure AD統合の一部としてMDMに登録する。

XenMobileとMicrosoft Azureを統合するには、Microsoft Azure Active Directoryのプレミアムライセンスが必要です。 ライセンスは、Windows 10デバイスを使用するユーザーがAzure ADを使用して登録できるようにMDMとAzure ADの統合を有効化するために必要です。 プレミアムライセンスの取得について詳しくは、「Microsoft Azure」を参照してください。 価格について詳しくは、「Azure Active Directoryの価格」を参照してください。

WindowsデバイスユーザーがAzureを使用して登録するには、管理者がXenMobileでMicrosoft Azureサーバーの設定を構成し、さらにWindowsデバイス用の契約条件デバイスポリシーを設定する必要があります。 ここでは、Microsoft Azureの設定の構成方法について説明します。 Windowsデバイスの契約条件デバイスポリシーの構成については、「契約条件デバイスポリシー」を参照してください。

XenMobileでMicrosoft Azureサーバーの設定を構成する前に、Azure ADポータルにログオンして、以下の操作を行う必要があります。

1. カスタムドメインを登録して、ドメインを検証します。 詳しくは、「Azure Active Directoryへの独自のドメイン名の追加」を参照してください。

2 ディレクトリ統合ツールを使用して、オンプレミスのディレクトリをAzure Active Directoryに拡張します。 詳しくは、「ディレクトリ統合」を参照してください。

3. MDMをAzure ADの信頼できるパーティーにします。 そのためには、**［Azure Active Directory］**、**［Applications］**の順にクリックして、**［Add］**をクリックします。 ギャラリーから**［Add an application］**を選択します。 **［MOBILE DEVICE MANAGEMENT］**に移動して、**［On-premise MDM application］**を選択し、設定を保存します。

4. アプリケーションで、XenMobileサーバー検出、使用条件エンドポイント、およびAPP ID URIを以下のように構成します。

- MDM検出URL：https://:8443/zdm/wpe
- MDM契約条件URL：https://:8443/zdm/wpe/tou
- APP ID URI：https://:8443/

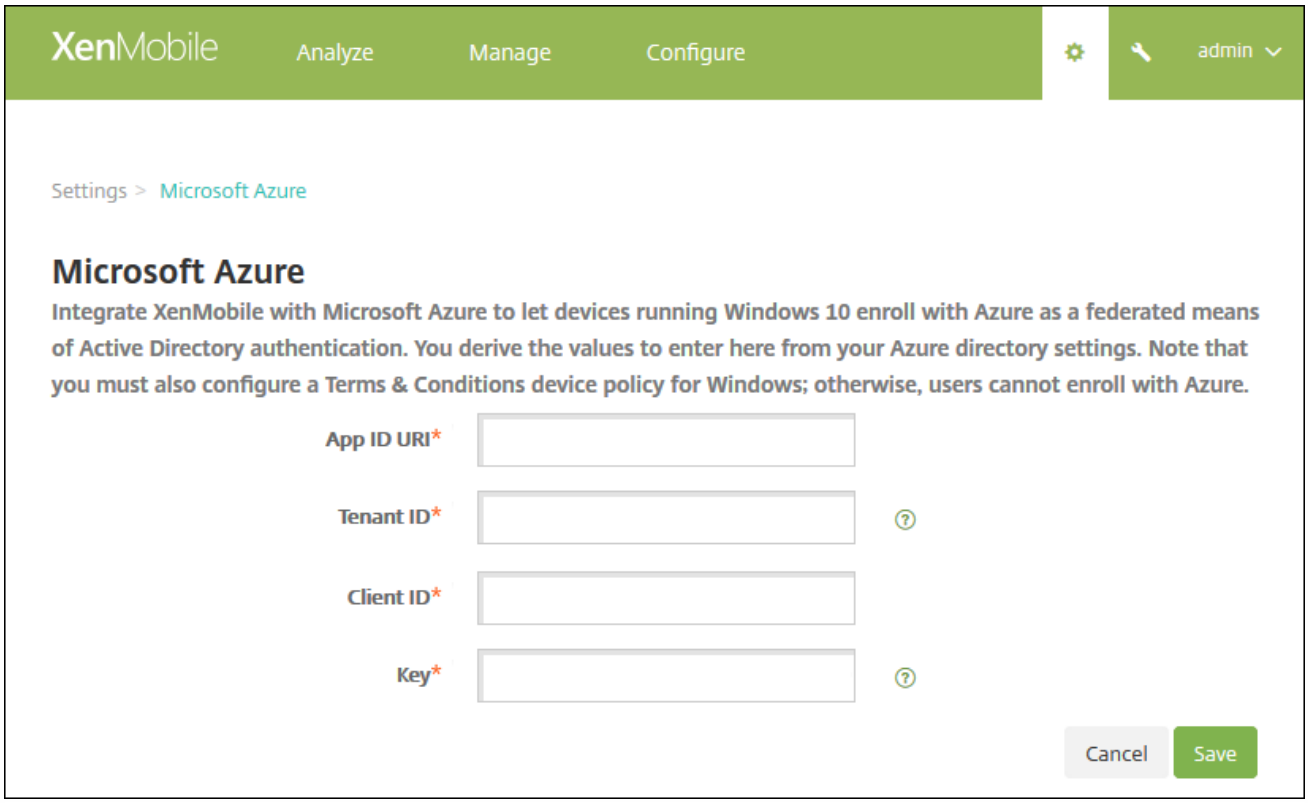
5. 手順3で作成したオンプレミスMDMアプリケーションを選択し、**［Manage devices for these users］**オプションを有効にして、すべてのユーザーまたは特定のユーザーグループに対してMDM管理を有効にします。

また、XenMobileコンソールで設定を構成するには、Microsoft Azureアカウントの以下の情報を記録しておく必要があります。

- App ID URI - XenMobileを実行しているサーバーのURL
- Tenet ID - ［Azure application settings］ページに記載
- Client ID - アプリケーションの一意の識別子
- Key - ［Azure application settings］ページに記載

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

2. [**Server**] の下の [**Microsoft Azure**] をクリックします。 [**Microsoft Azure**] ページが開きます。



3. 次の設定を構成します。

- **App ID URI**：Azure設定の構成時に入力した、XenMobileを実行しているサーバーのURLを入力します。
- **Tenant ID**： [Azure application settings] ページから値をコピーします。 ブラウザーのアドレスバーに表示されている、数字と文字から成る部分をコピーします。 たとえば、https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem ...とある場合、テナントIDは「*abc123-abc123-abc123*」です。
- **Client ID**： [Azure Configure] ページから値をコピーして貼り付けます。 これはアプリケーションの一意の識別子です。
- **Key**： [Azure application settings] ページから値をコピーします。 [**Keys**] の下で、一覧から期間を選択し、設定を保存します。 キーは、コピーしてこのフィールドに貼り付けることができます。 キーは、Microsoft Azure ADでアプリケーションがデータを読み取ったり書き込んだりする場合に必要です。

4. [**Save**] をクリックします。

Important

ユーザーがWindowsデバイスでAzure ADに参加する場合、XenMobileで構成されたWorxStoreおよびWebリンクデバイスポリシーについては、ローカルユーザーではなくAzure ADユーザーのみが使用できます。 ローカルユーザーがこれらのデバイスポリシーを使用するには、次の手順を実行する必要があります。

1 [**Settings**] > [**About**] > [**Join Azure AD**] で、Azureユーザーの代わりにAzure ADに参加します。

2. Windowsからサインアウトし、Azure ADアカウントを使用してサインインします。

Google Cloud Messaging

Aug 02, 2016

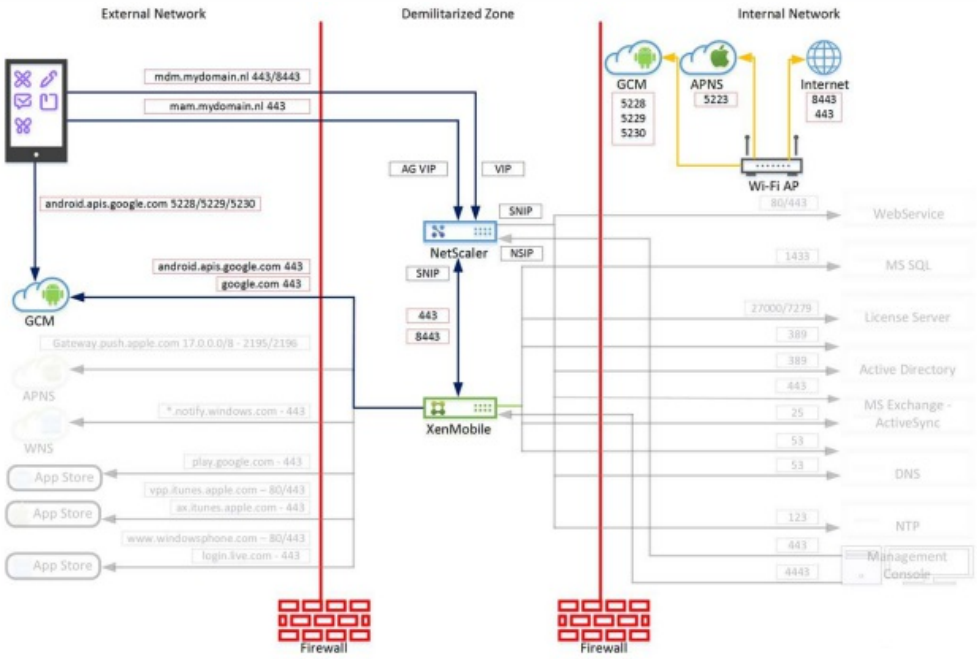
Active poll period MDXポリシーの代わりにGoogle Cloud Messaging（GCM）を使用して、AndroidデバイスがXenMobileに接続するタイミングと方法を制御することもできます。 この記事に記載されている構成では、セキュリティアクションや展開コマンドによって、ユーザーにXenMobiileサーバーへの再接続を求めるプッシュ通知がWorx Homeに送信されます。

前提条件

- XenMobile 10.3.x
- 最新のWorx Homeクライアント
- Googleデベロッパーアカウントの資格情報
- Android.apis.google.comおよびGoogle.comに向けたXenMobileのポート443の開放

アーキテクチャ

次の図は、外部および内部ネットワークにおけるGCMの通信フローを示しています。

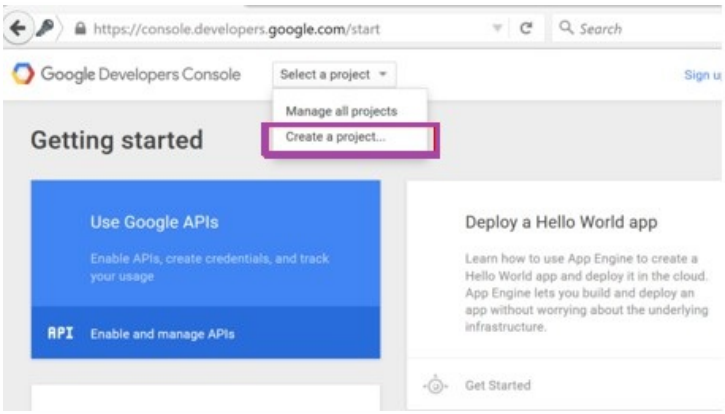


GoogleアカウントをGCM向けに構成するには

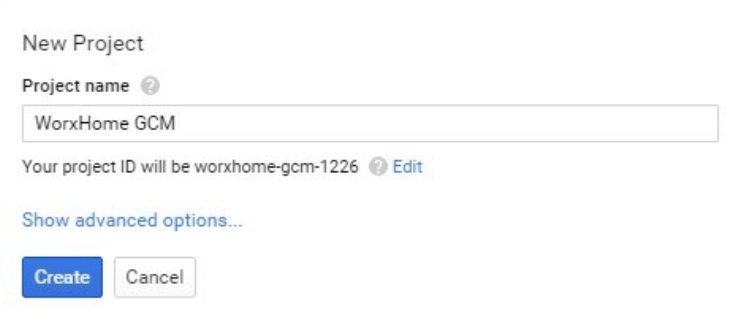
1. Googleデベロッパーアカウントの資格情報を使用して次のURLにログオンします。

   https://console.developers.google.com

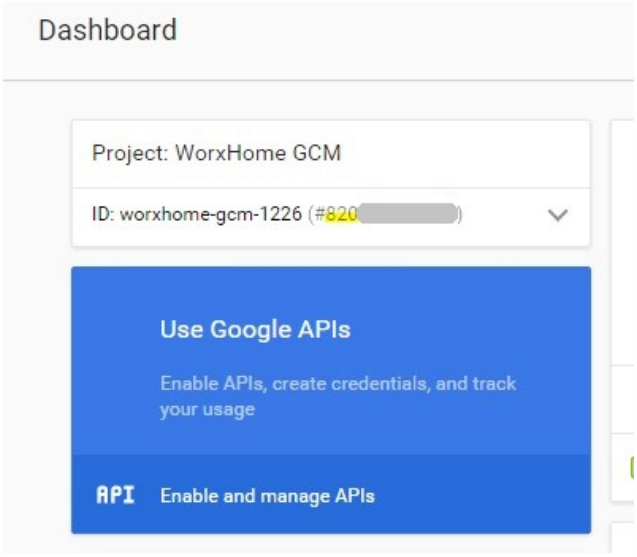
2. ［**Select a project**］から、［**Create a project**］を選択します。



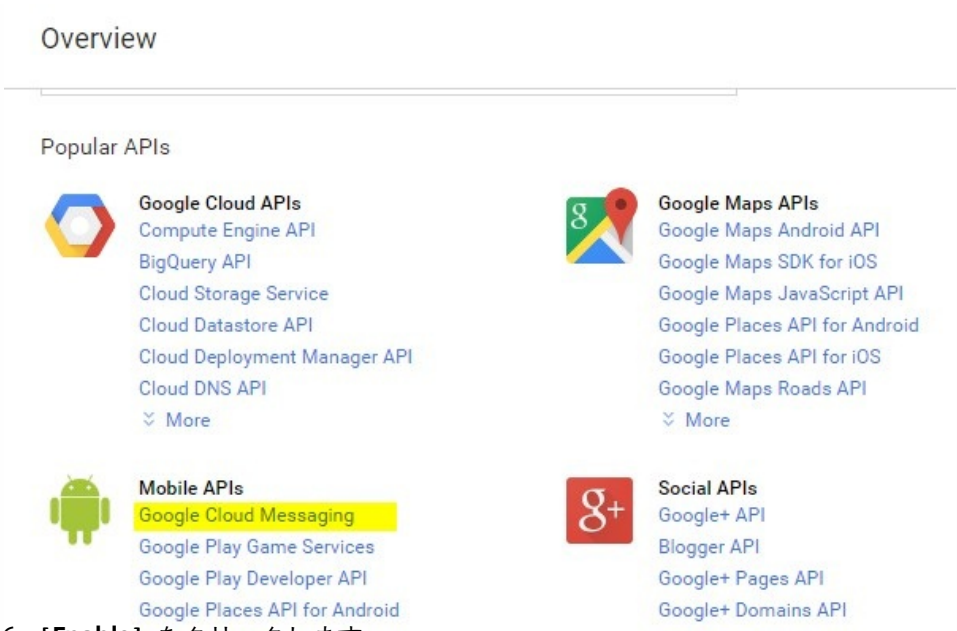
3. プロジェクト名を入力し、［**Create**］をクリックします。



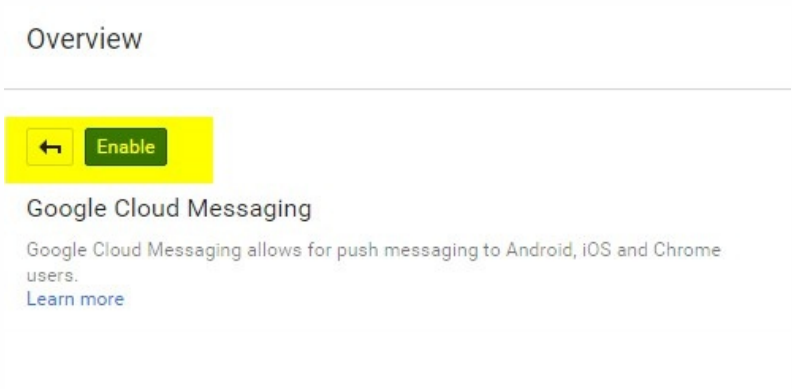
4. ダッシュボードで、送信者ID（下の図で強調表示されている部分）がプロジェクトIDの横に表示されます。 送信者IDをメモします。このIDは後でXenMobileサーバー設定で入力する必要があります。 ［**Use Google APIs**］をクリックします。



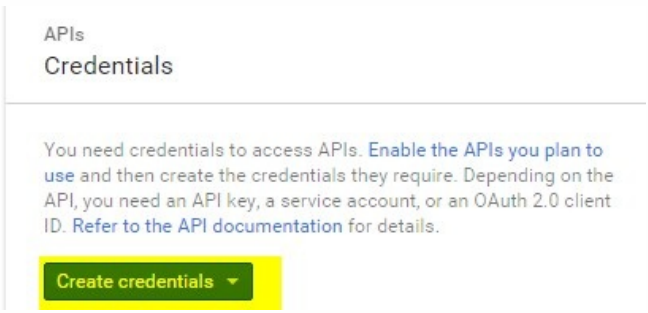
5. ［**Mobile APIs**］セクションで、［**Google Cloud Messaging**］をクリックします。



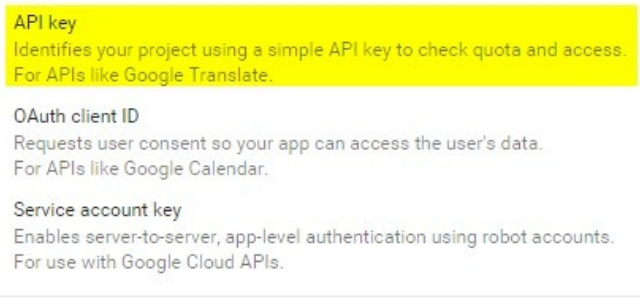
6. [**Enable**] をクリックします。



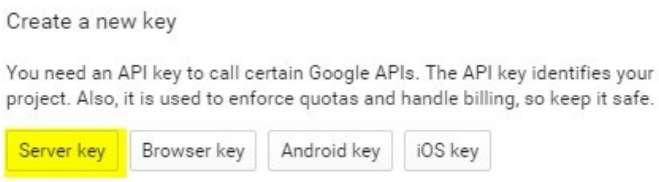
7. [**Credentials**] の下の [**Create credentials**] をクリックします。



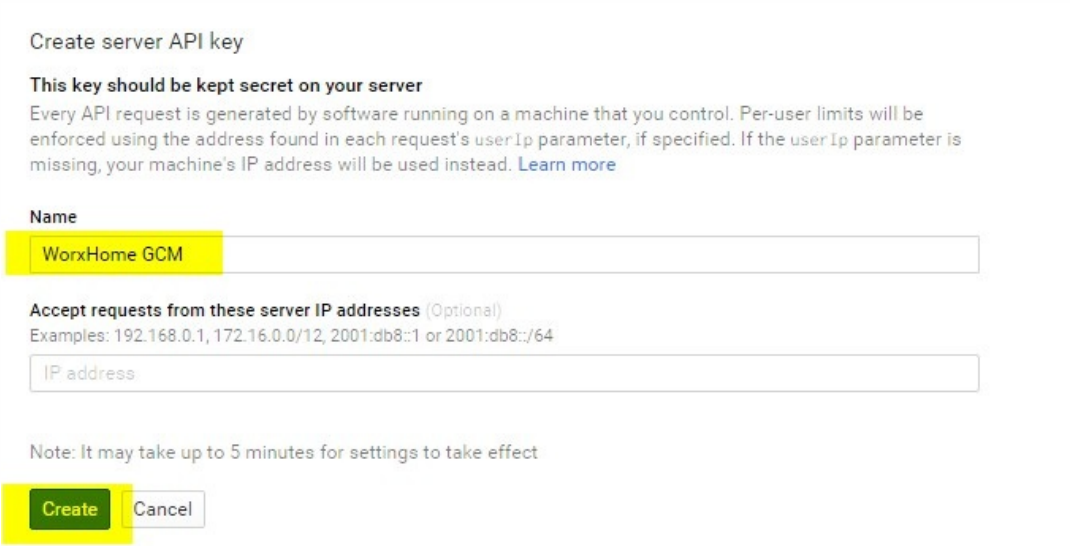
8. [**API key**] をクリックします。



9. **[Create a new key]** の下の **[Server key]** をクリックします。



10. **[Create server API key]** で、**名前**（この例ではプロジェクト名を使用しています）を入力し、**[Create]** をクリックします。



11. API キーをメモします。 これはXenMobileの構成で必要になります。

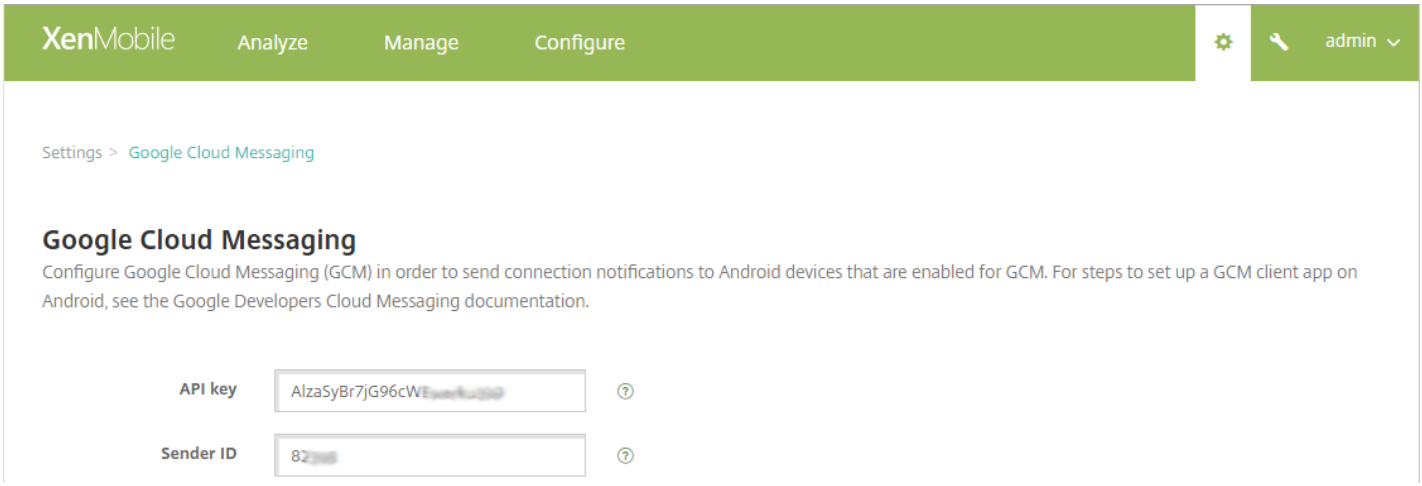
XenMobileをGCM向けに構成するには

1. XenMobile管理コンソールにログオンし、**[Settings]** > **[Google Cloud Messaging]** の順に選択します。

a. **[API key]** で、GCM構成の最後の手順でコピーしたGCM APIキーを入力します。

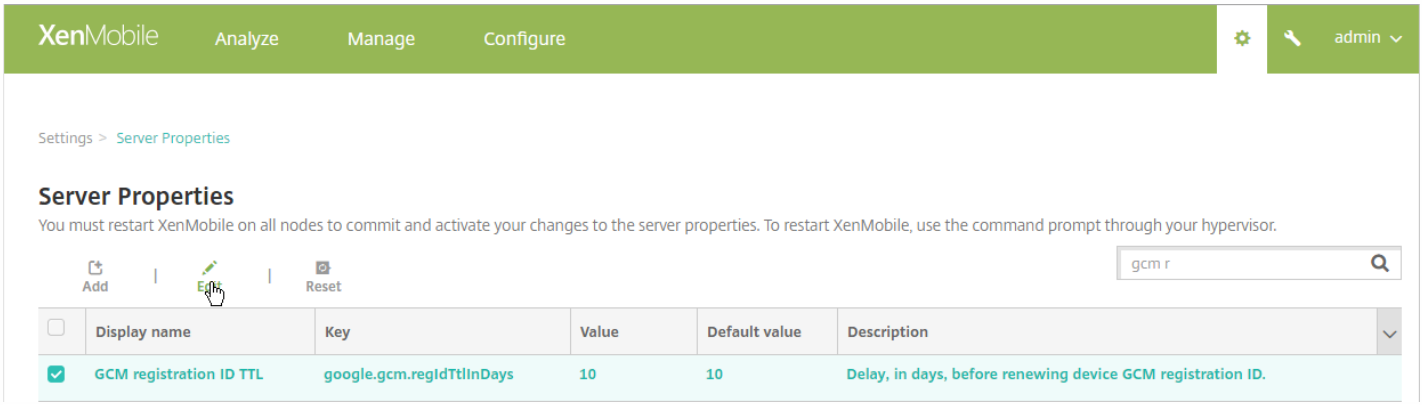
b. **[Sender ID]** で、前の手順でメモしておいた送信者IDの値を入力して **[Save]** をクリックします。

注： **[Settings]** > **[Google Cloud Messaging]** ページは、XenMobile 10.3.6の新しいページです。 最新のXenMobileリリースを使用していない場合は、 **[Settings]** > **[Server]** の順に移動して、 **[API key]** （google.gcm.apiKey）および **[Sender ID]** （google.gcm.senderid）を更新してください。

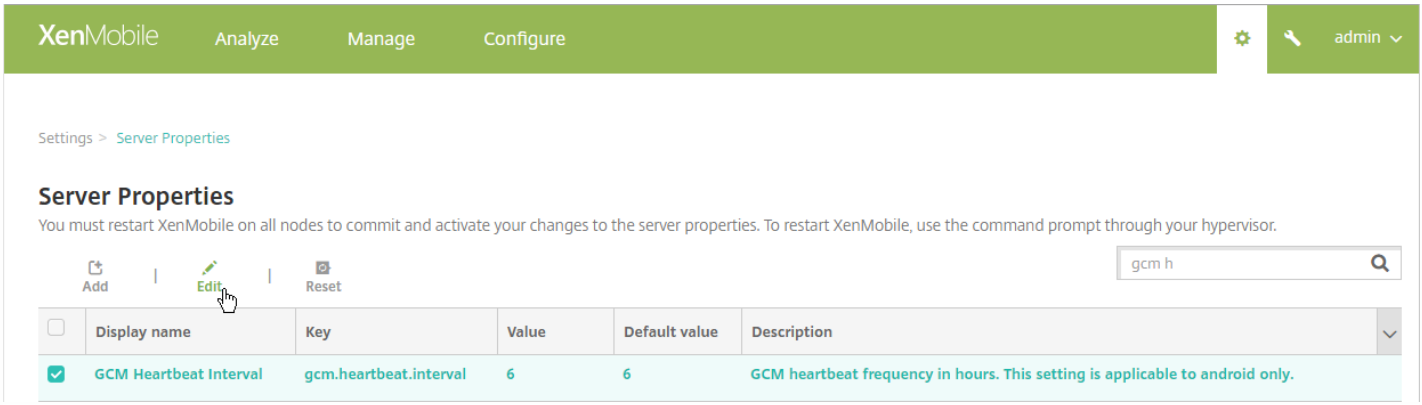


2. 次のいずれかのプロパティのデフォルト設定を変更する必要がある場合は、 **[Settings]** > **[Server Properties]** の順にクリックします。

- **GCM Registration ID TTL**：デバイスのGCM登録IDが更新されるまでのデフォルトの猶予期間は10日間です。 この値を変更するには、検索ボックスに「**gcm r**」と入力し、 **[GCM Registration ID TTL]** をクリックしてから **[Edit]** をクリックします。



- **GCM Heartbeat Interval**：XenMobileとGCMサーバーとのデフォルトの通信間隔は6時間です。 この値を変更するには、検索ボックスに「**gcm h**」と入力し、 **[GCM Heartbeat Interval]** をクリックしてから **[Edit]** をクリックします。

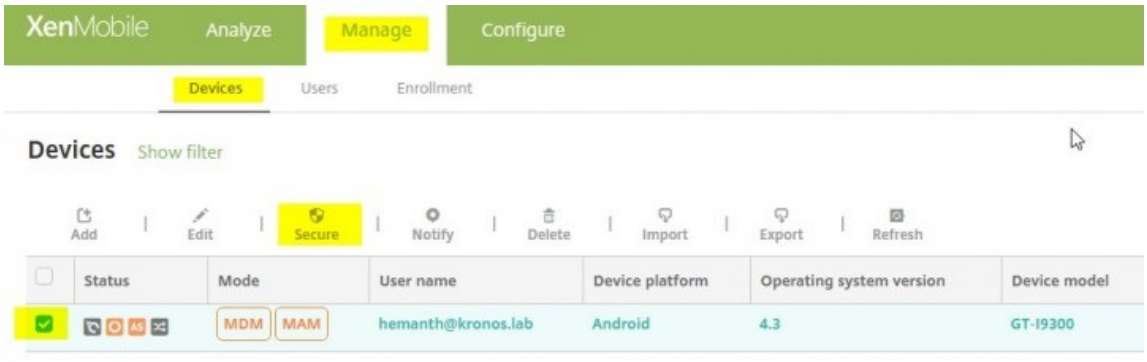


構成をテストするには

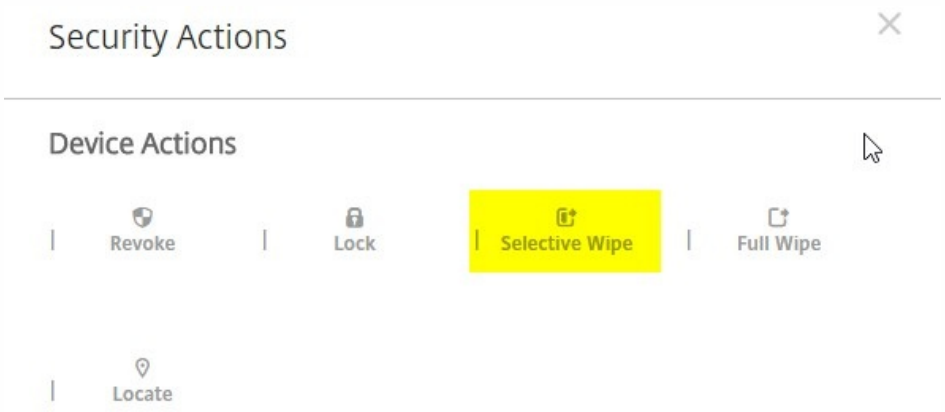
1. Androidデバイスを登録します。

2. このデバイスを少しの時間アイドル状態にして、XenMobileサーバーから切断します。

3. XenMobile管理コンソールにログオンして［**Manage**］をクリックし、Androidデバイスを選択して［**Secure**］をクリックします。



4. ［**Device Actions**］で、［**Selective Wipe**］をクリックします。



正常に構成されている場合、XenMobileに再接続せずにデバイスで選択的なワイプが行われます。

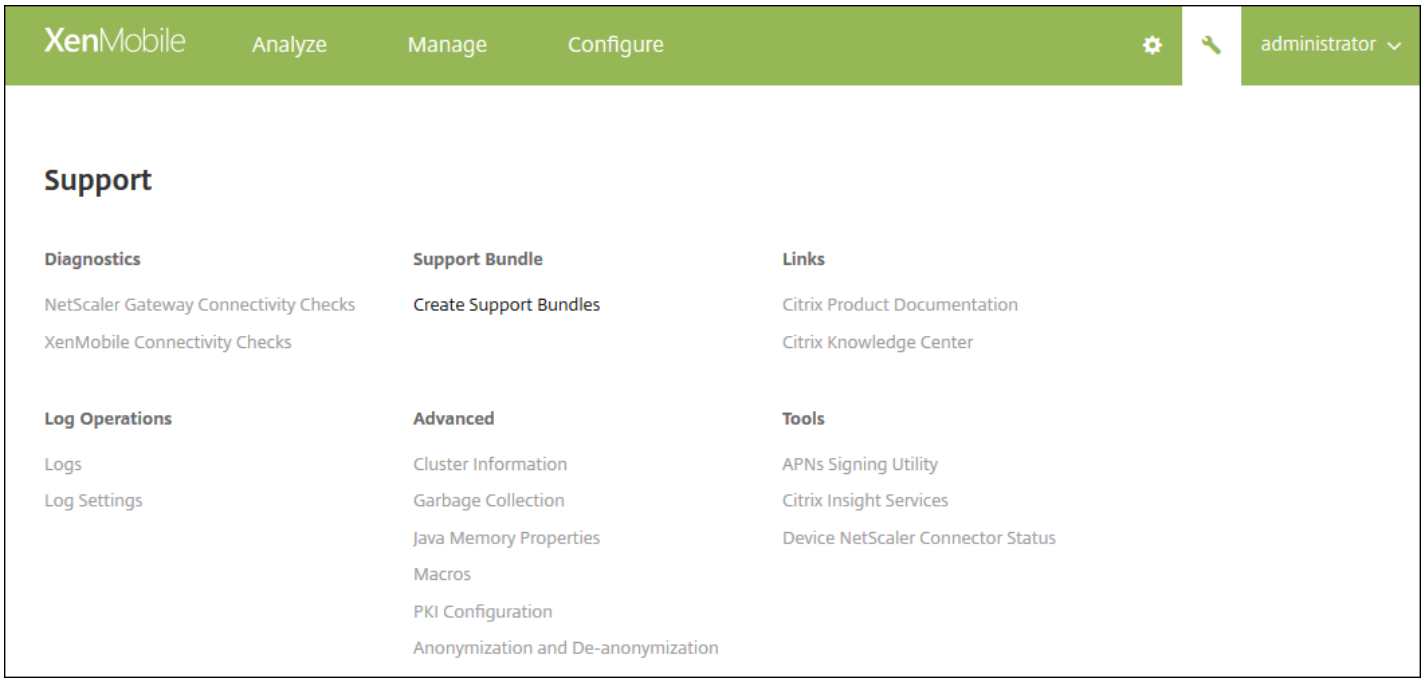
XenMobileのサポートおよび保守

Aug 02, 2016

［XenMobile Support］ページを使用して、サポートに関連する多くの情報とツールにアクセスします。 また、コマンドラインインターフェイスからもアクションを実行できます。 詳しくは、「XenMobileコマンドラインインターフェイスオプション」を参照してください。

XenMobileコンソールで、右上のレンチアイコンをクリックします。

［Support］ページが開きます。



［Support］ページを使用して以下を行います。

- 診断へのアクセス
- サポートバンドルの作成
- Citrixの製品ドキュメントおよびKnowledge Centerへのリンクへのアクセス
- ログ操作へのアクセス
- 一連の詳細情報および構成オプションからの選択
- 一連のツールおよびユーティリティへのアクセス

接続確認の実行

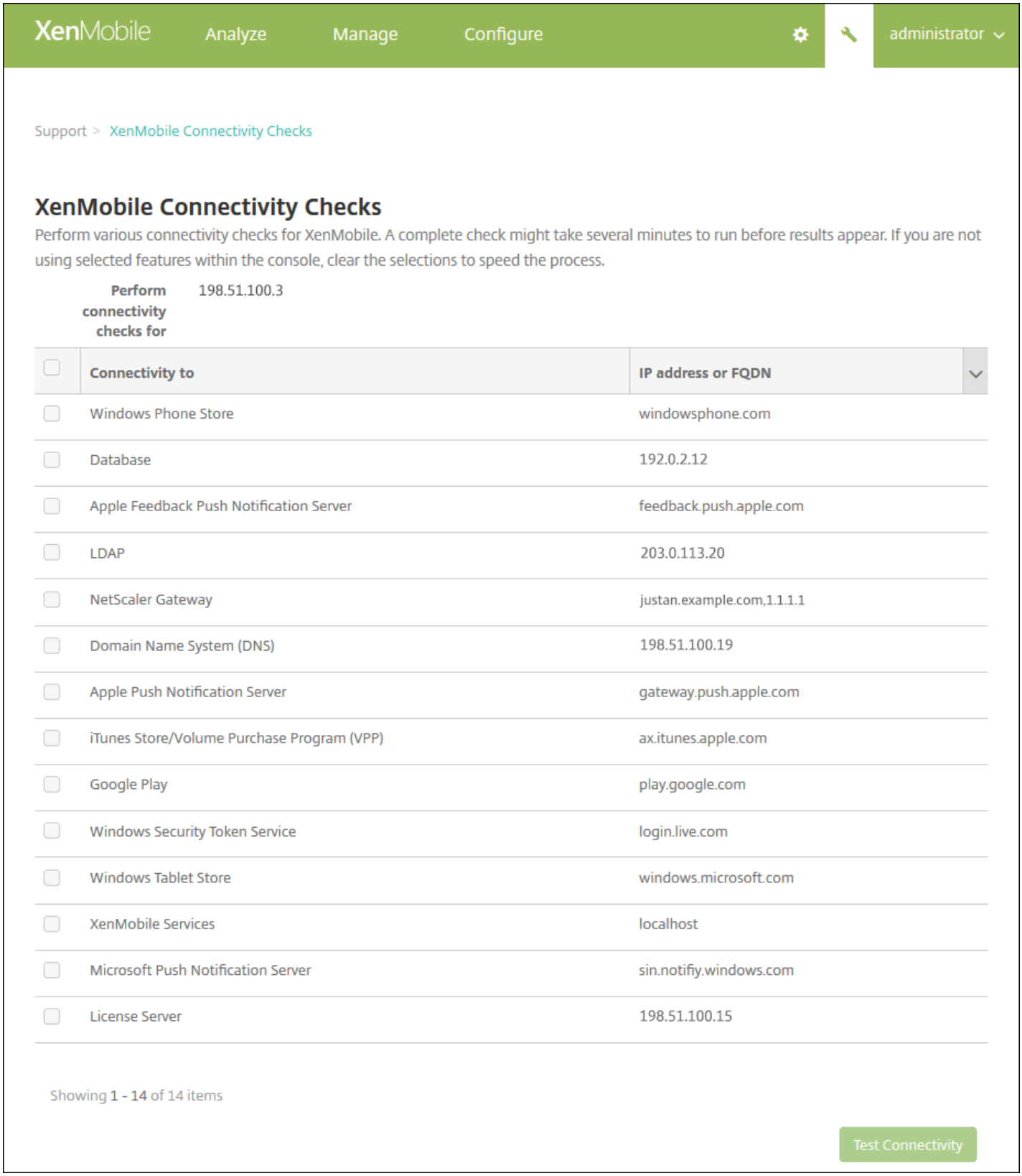
Aug 02, 2016

［**XenMobile Support**］ページで、NetScaler Gatewayおよびそのほかのサーバーや場所へのXenMobileの接続を確認できます。

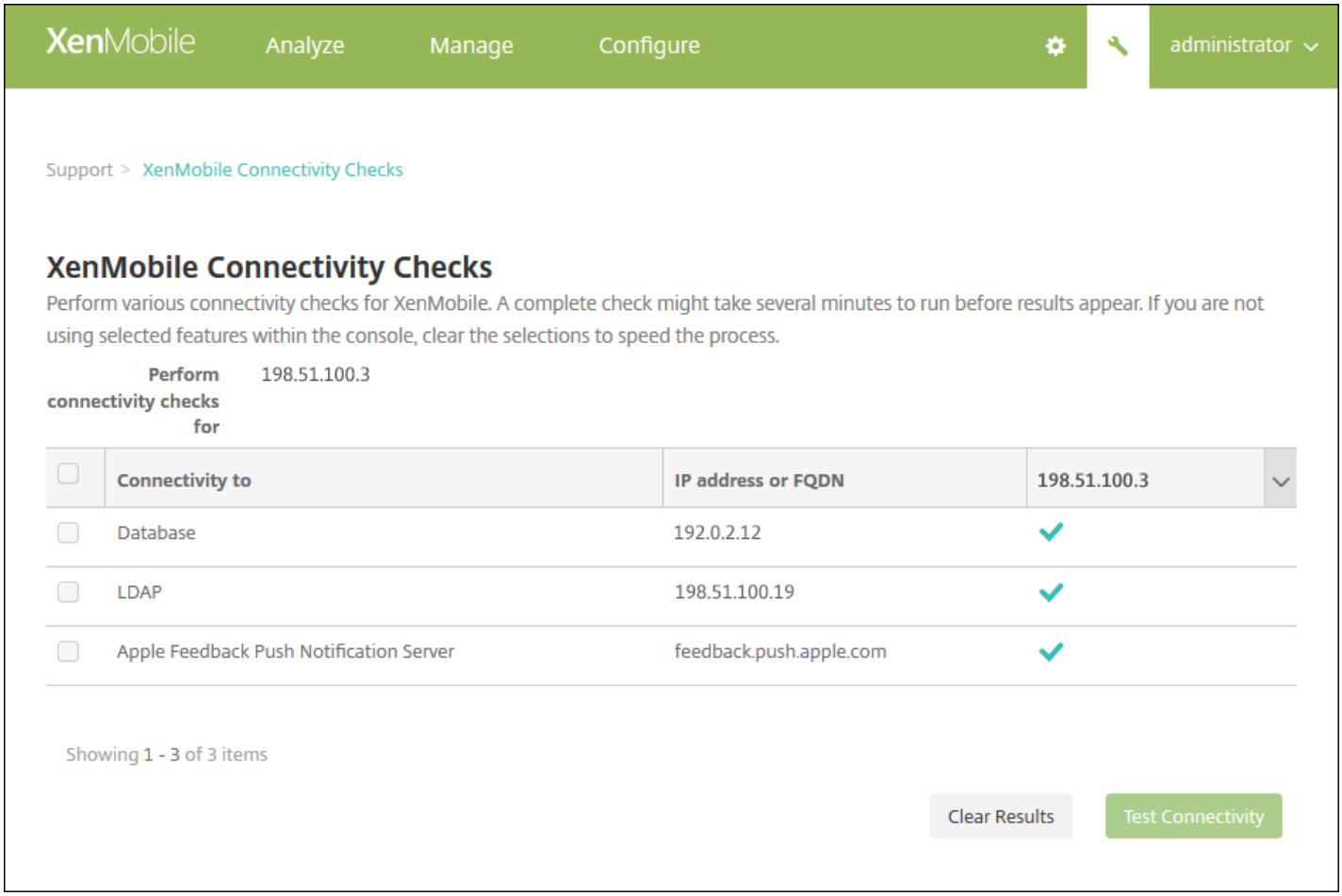
XenMobileの接続確認の実行

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。［**Support**］ページが開きます。

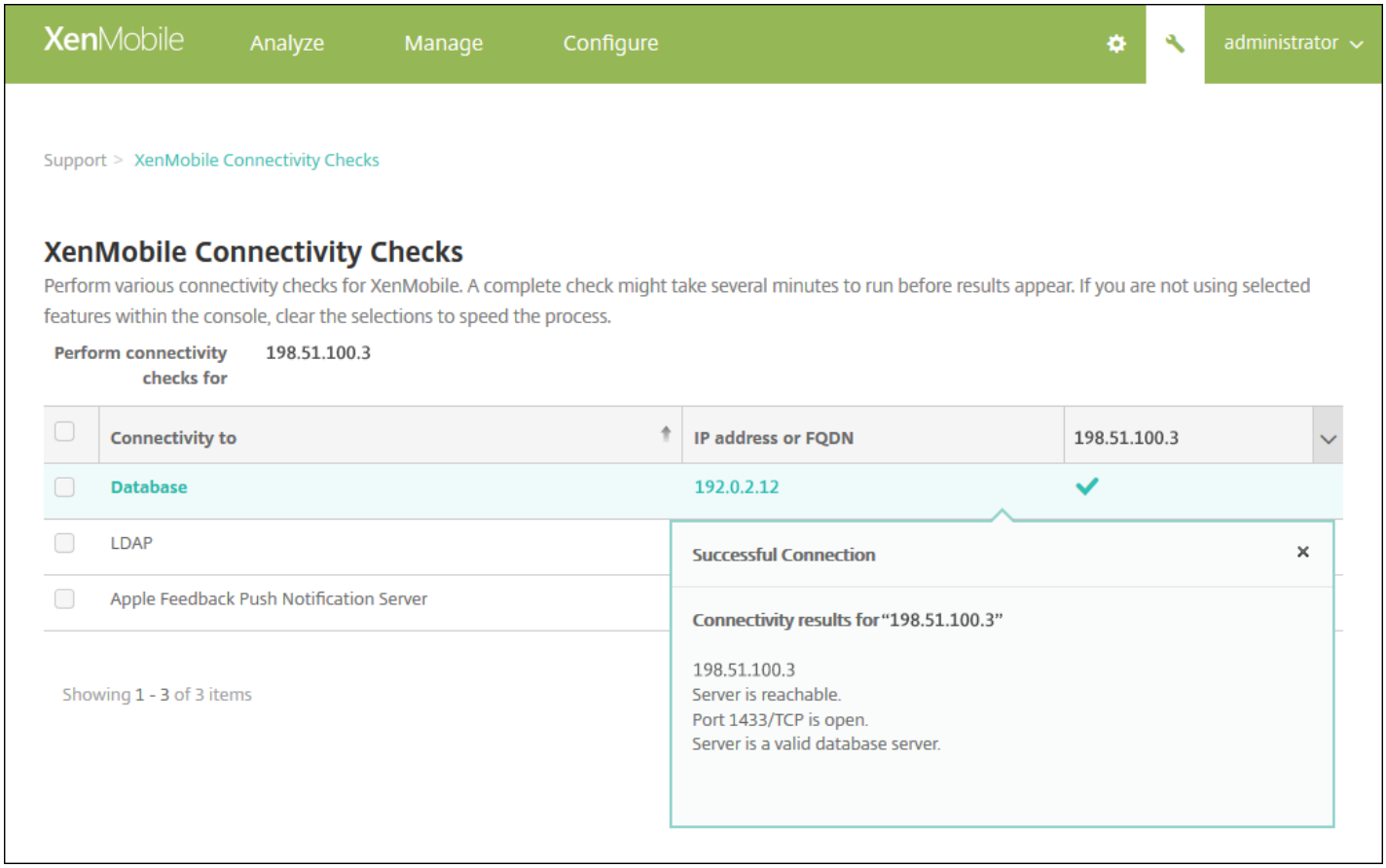
2. ［**Diagnostics**］の下の［**XenMobile Connectivity Checks**］をクリックします。［**XenMobile Connectivity Checks**］ページが開きます。 XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。



2. 接続テストに含めるサーバーをオンにして、**[Test Connectivity]** をクリックします。 [Test Results] ページが開きます。

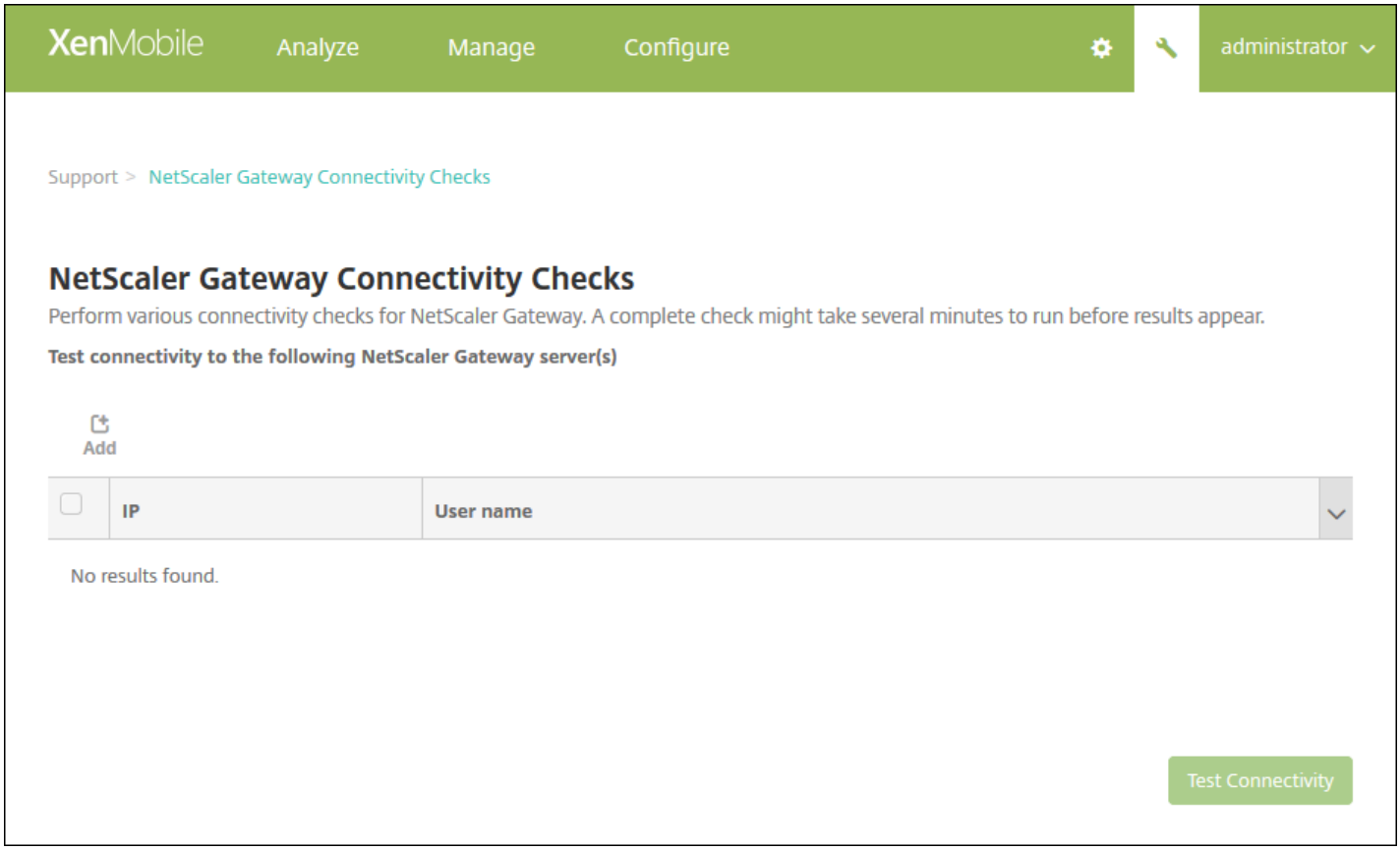


3. [Test Results] の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

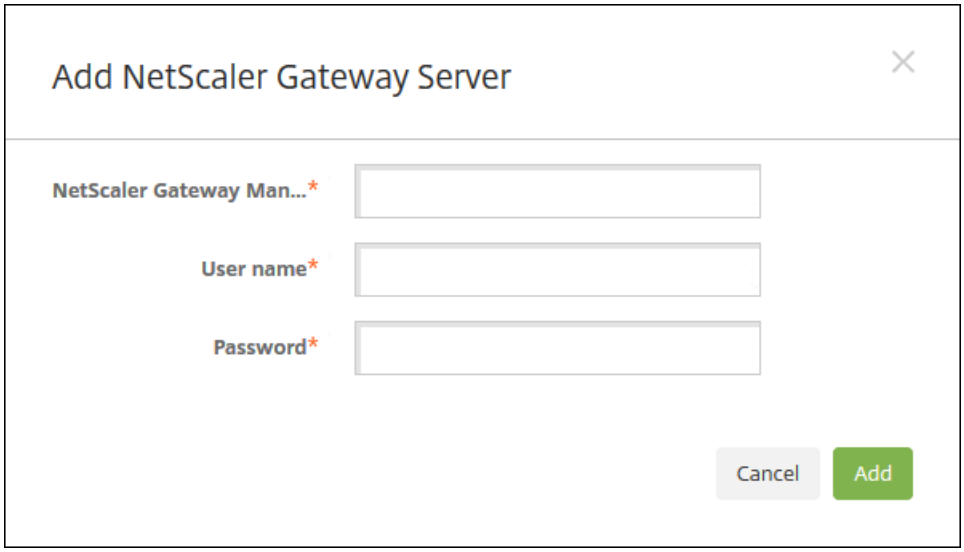


NetScaler Gatewayの接続確認の実行

1. **[Support]** ページで、 **[Diagnostics]** の下の **[NetScaler Gateway Connectivity Checks]** をクリックします。 **[NetScaler Gateway Connectivity Checks]** ページが開きます。 NetScaler Gatewayサーバーが追加されていない場合、表は空白です。



2. **[Add]** をクリックします。 **[Add NetScaler Gateway Server]** ダイアログボックスが開きます。



3. **[NetScaler Gateway Management IP]** ボックスに、テストするNetScaler Gatewayを実行しているサーバーのIPアドレスを入力します。

注：既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、IPアドレスは入力されています。

4. このNetScaler Gatewayの管理者資格情報を入力します。

注：既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、ユーザー名は入力されています。

5. **[Add]** をクリックします。 NetScaler Gatewayが、 **[NetScaler Gateway Connectivity Checks]** ページの表に追加されます。

6. **[Test Connectivity]** をクリックします。 [Test Results] の表に結果が表示されます。

7. [Test Results] の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

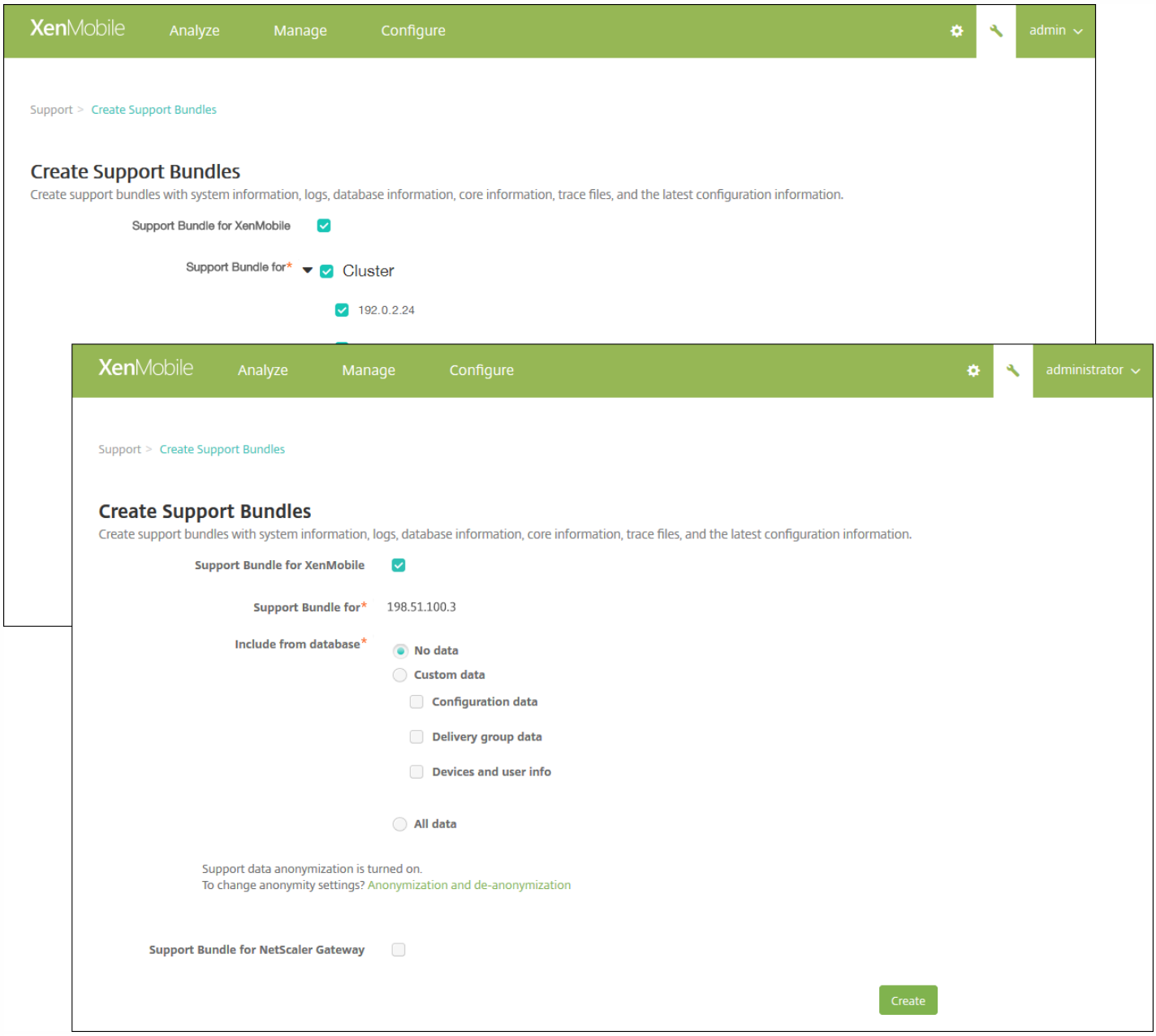
XenMobileでのサポートバンドルの作成

Aug 02, 2016

Citrixに問題を報告する場合や問題をトラブルシューティングする場合、サポートバンドルを作成してCitrix Insight Services（CIS）にアップロードできます。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。［**Support**］ページが開きます。

2. ［**Support**］ページで、［**Create Support Bundles**］をクリックします。［**Create Support Bundles**］ページが開きます。 XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。



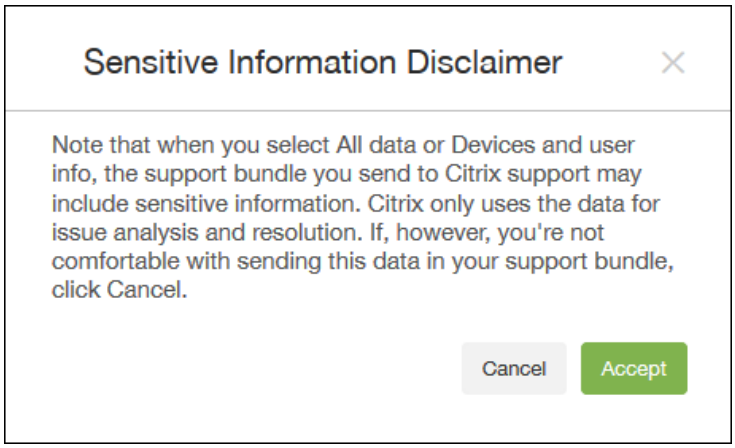
3. ［**Support Bundle for XenMobile**］チェックボックスがオンになっていることを確認します。

4. XenMobile環境内にクラスターノードがある場合は、**[Support Bundle for]** ですべてのノードを選択するか、データの取得先にするノードの組み合わせを選択できます。

5. **[Include from Database]** で、次のいずれかを実行します。

- **[No data]** をクリックします。
- **[Custom data]** をクリックして、次のいずれかまたはすべてをオンにします。
  - **Configuration data**：証明書構成とデバイスマネージャーポリシーを含めます。
  - **Delivery group data**：アプリケーションの種類やアプリケーションデリバリーポリシー詳細など、アプリケーションのデリバリーグループの情報を含めます。
  - **Devices and user info**：デバイスポリシー、アプリケーション、アクション、デリバリーグループを含めます。
- **[All data]** をクリックします。

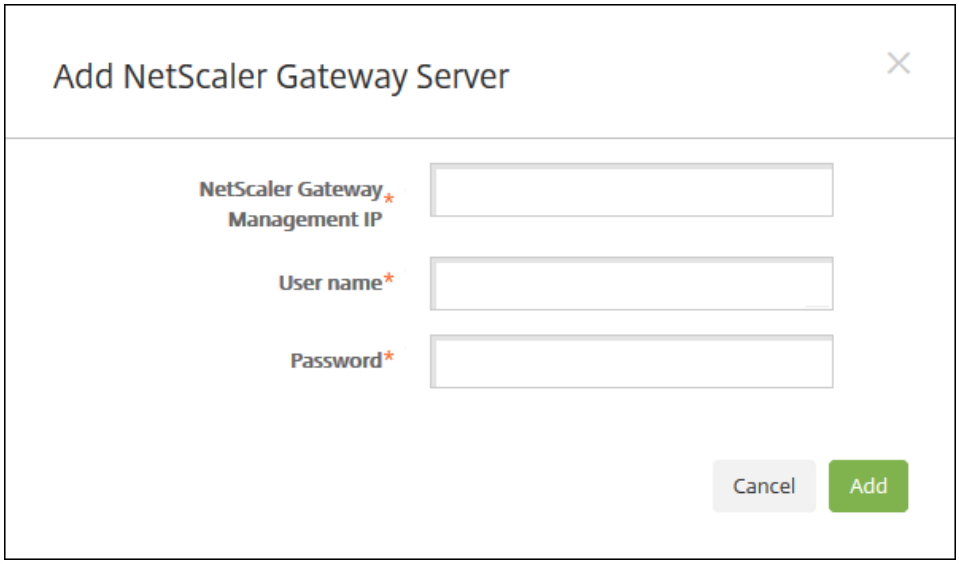
注： **[Devices and user info]** または **[All data]** を選択し、かつこれが初めて作成するサポートバンドルである場合は、**[Sensitive Information Disclaimer]** ダイアログボックスが開きます。 免責事項を読み、**[Accept]** または **[Cancel]** をクリックします。 **[Cancel]** をクリックした場合は、サポートバンドルをCitrixにアップロードできません。 **[Accept]** をクリックした場合は、サポートバンドルをCitrixにアップロードでき、次回デバイスやユーザーデータを含むサポートバンドルを作成するときに免責事項が表示されなくなります。



6. **[Include from database]** の下には、機密性の高いユーザー、サーバー、ネットワークのデータをサポートバンドルで匿名化するかどうかについての通知があります。 デフォルト設定では、データは匿名化されます。 この設定は、**[Anonymization and de-anonymization]** リンクをクリックすると変更することができます。 データの匿名化について詳しくは、「サポートバンドルでのデータの匿名化」を参照してください。

6. NetScaler Gatewayからのサポートバンドルを含める場合は、**[Support Bundle for NetScaler Gateway]** をオンにして以下を行います。

- **[Add]** をクリックします。 **[Add NetScaler Gateway Server]** ダイアログボックスが開きます。



- **[NetScaler Gateway Management IP]** ボックスに、サポートバンドルの取得先にするNetScaler GatewayのNetScaler管理IPアドレスを入力します。

  注：既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、IPアドレスは入力されています。

- **[User name]** ボックスと **[Password]** ボックスに、NetScaler Gatewayを実行しているサーバーへのアクセスに必要なユーザー資格情報を入力します。

  注：既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、ユーザー名は入力されています。

7. **[Add]** をクリックします。 新しいNetScaler Gatewayサポートバンドルが表に追加されます。

8. 手順7.を繰り返し、ほかのNetScaler Gatewayサポートバンドルを追加します。

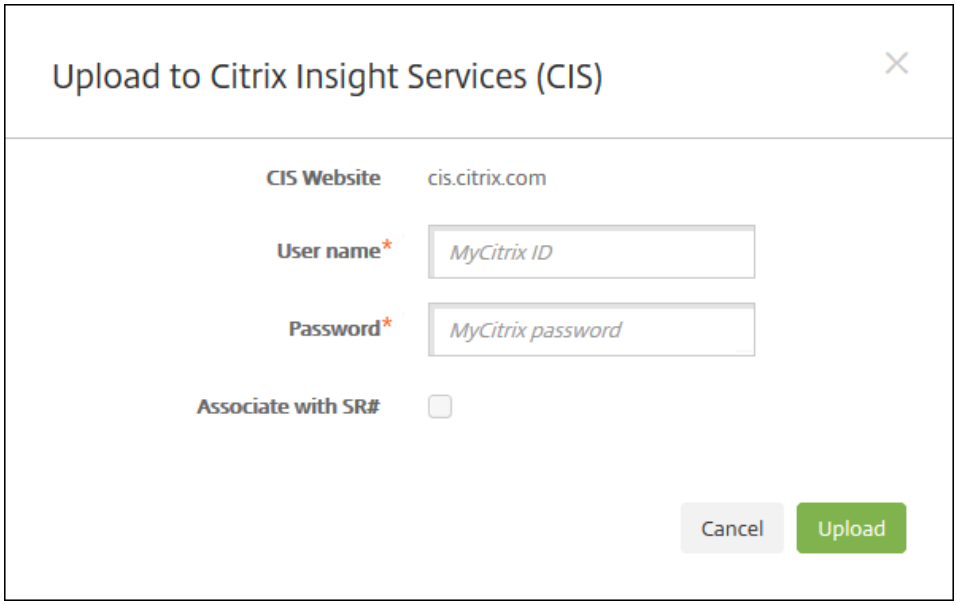
9. **[Create]** をクリックします。 サポートバンドルが作成され、**[Upload to CIS]** と **[Download to Client]** の2つの新しいボタンが表示されます。

「Citrix Insight Servicesへのサポートバンドルのアップロード」または「コンピューターへのサポートバンドルのダウンロード」に進みます。

Citrix Insight Servicesへのサポートバンドルのアップロード

サポートバンドルを作成した後、Citrix Insight Services（CIS）にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。 以下の手順は、CISにバンドルをアップロードする方法を示しています。 CISにアップロードするには、MyCitrixのIDおよびパスワードが必要です。

1. **[Create Support Bundles]** ページで、 **[Upload to CIS]** をクリックします。 **[Upload to Citrix Insight Services (CIS)]** ダイアログボックスが開きます。



2. [**User Name**] ボックスにMyCitrix IDを入力します。

3. [**Password**] ボックスにMyCitrixパスワードを入力します。

4. このバンドルを既存のサービスリクエスト番号に関連付ける場合は、[**Associate with SR#**] チェックボックスをオンにし、新たに表示される2つのフィールドで以下を実行します。

- [**SR#**] ボックスに、このバンドルを関連付けるサービスリクエスト番号（8桁）を入力します。
- [**SR Description**] ボックスに、SRの説明を入力します。

5. [**Upload**] をクリックします。

CISにサポートバンドルをアップロードするのはこれが初めてであり、ほかの製品を介してCISのアカウントを作成したことがなく、かつデータの収集とプライバシーについての契約に同意していない場合は、以下のダイアログボックスが表示されます。アップロードを開始する前にこの契約に同意する必要があります。 CISのアカウントを作成済みで、以前に契約に同意している場合は、サポートバンドルが直ちにアップロードされます。

6. 契約を読み、 **[Agree and upload]** をクリックします。 サポートバンドルがアップロードされます。

コンピューターへのサポートバンドルのダウンロード

サポートバンドルを作成した後、CISにバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。 問題のトラブルシューティングを自分で行う場合は、サポートバンドルをコンピューターにダウンロードします。

［Create Support Bundles］ページで、［Download to Client］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。

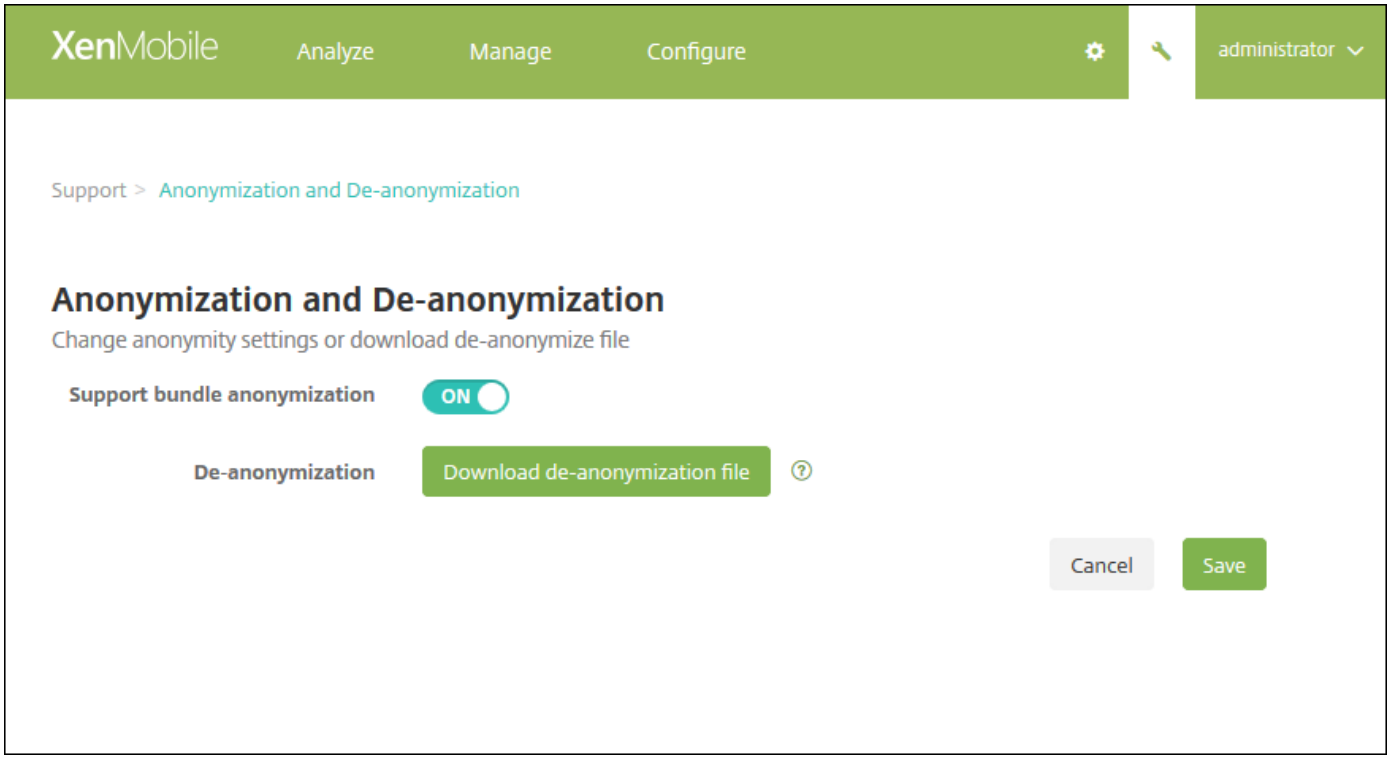
サポートバンドルのデータの匿名化

Aug 02, 2016

XenMobileでサポートバンドルを作成する場合、デフォルトでは、機密性の高いユーザー、サーバー、ネットワークのデータは匿名化されます。 この動作は、［Anonymization and De-anonymization］ページで変更することができます。 また、XenMobileがデータの匿名化時に保存したマッピングファイルをダウンロードすることもできます。 データの匿名化を解除したり、ユーザーまたはデバイスで発生した問題を特定したりする目的で、Citrixのサポートからこのファイルを要求される場合があります。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。［**Support**］ページが開きます。

2. ［**Support**］ページで、［**Advanced**］の下の［**Anonymization and De-anonymization**］をクリックします。［**Anonymization and De-anonymization**］ページが開きます。



3. ［**Support bundle anonymization**］で、データを匿名化するかどうかを選択します。 デフォルトは［**ON**］です。

4. Citrixのサポートで問題の診断に特定のデバイスまたはユーザーの情報が必要な場合にサポートに送信するマッピングファイルを、［**De-anonymization**］の横の［**Download de-anonymization file**］をクリックしてダウンロードします。

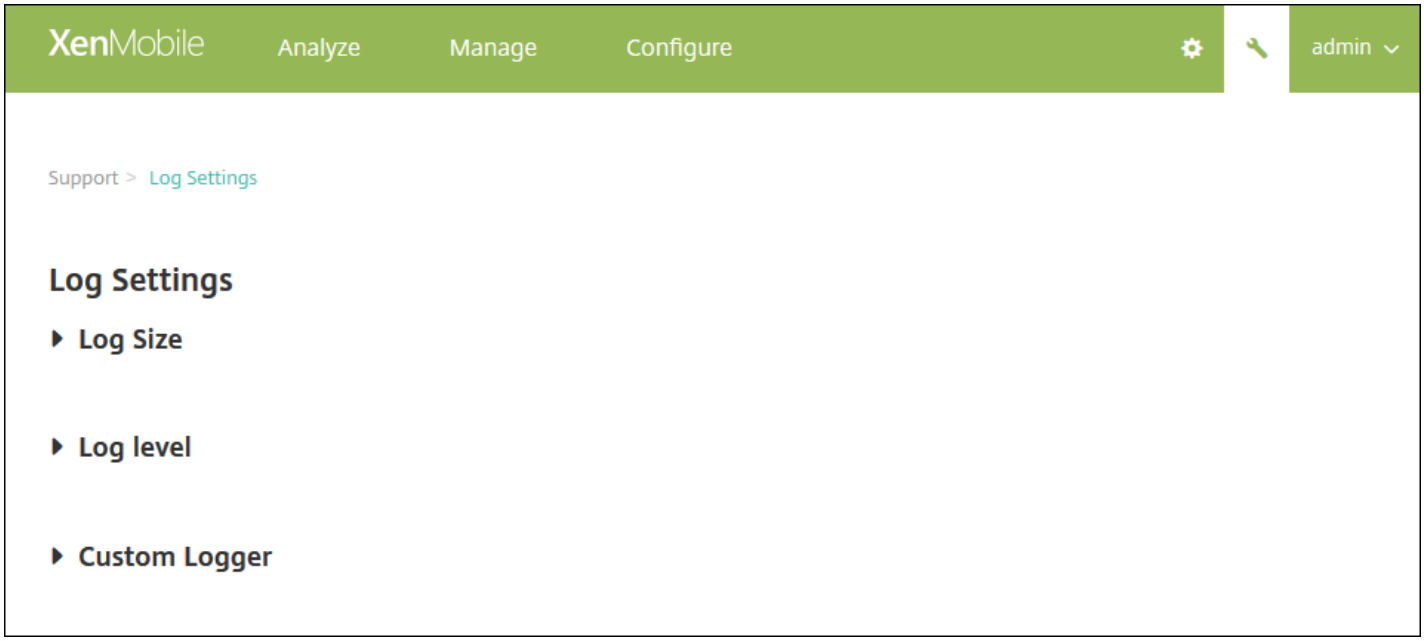
ログ設定の構成

Aug 02, 2016

ログ設定を構成して、XenMobileで生成されるログの出力をカスタマイズすることができます。 XenMobileサーバーをクラスター化している場合は、XenMobileコンソールでログ設定を構成すると、その設定はクラスター内のほかのすべてのサーバーと共有されます。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。 **[Support]** ページが開きます。

2. **[Log Operations]** の下の **[Log Settings]** をクリックします。 **[Log Settings]** ページが開きます。

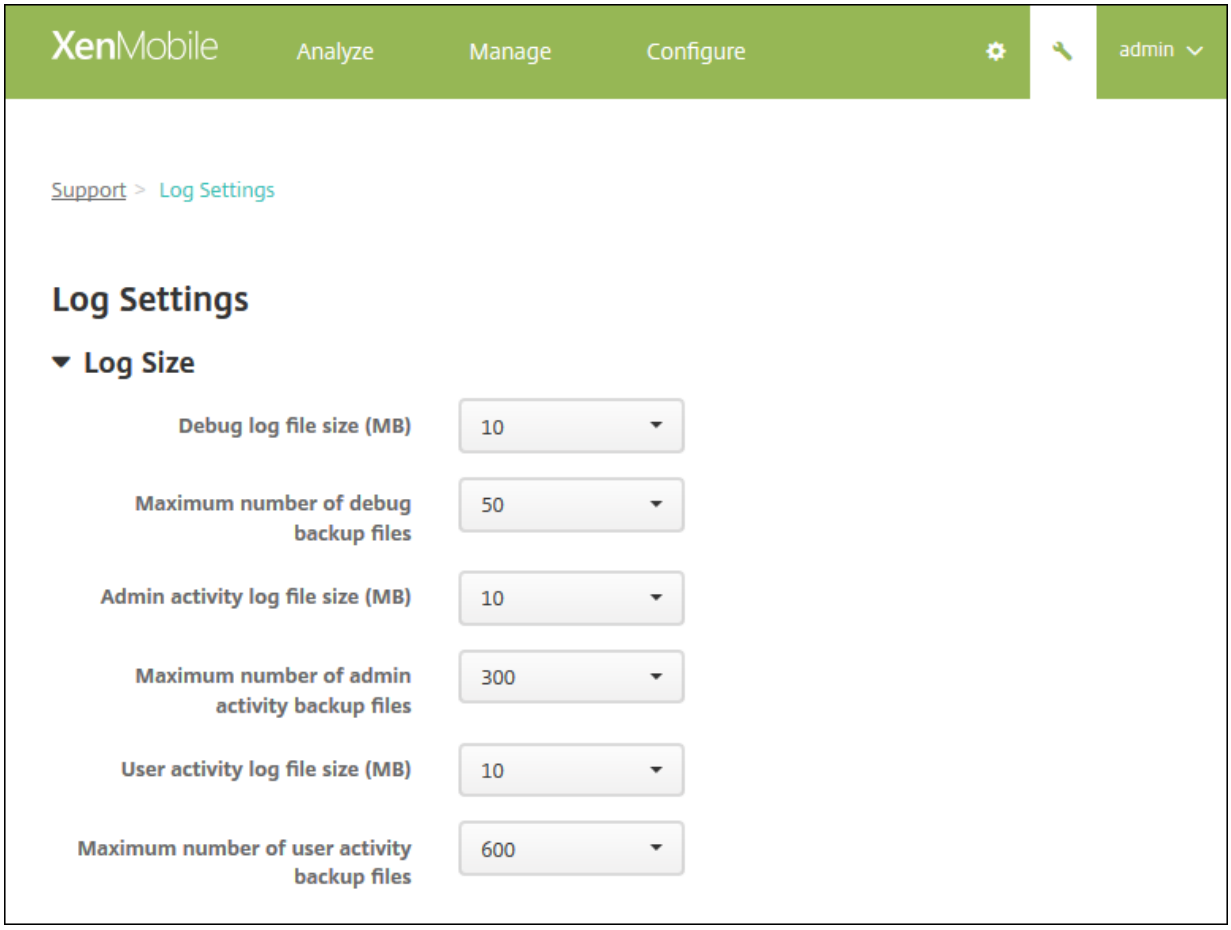


[Log Settings] ページでは、以下のオプションにアクセスできます。

- **Log Size**。 このオプションを使用して、ログファイルのサイズと、データベースで保持されるログのバックアップファイルの最大数を制御します。 ログのサイズは、XenMobileでサポートされる各ログ（デバッグログ、管理者アクティビティログ、およびユーザーアクティビティログ）に適用されます。
- **Log level**。 このオプションを使用して、ログレベルを変更したり、設定を永続的にしたりします。
- **Customer Logger**。 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。

[Log Size] のオプションを構成するには

1. **[Log Settings]** ページで **[Log Size]** を展開します。



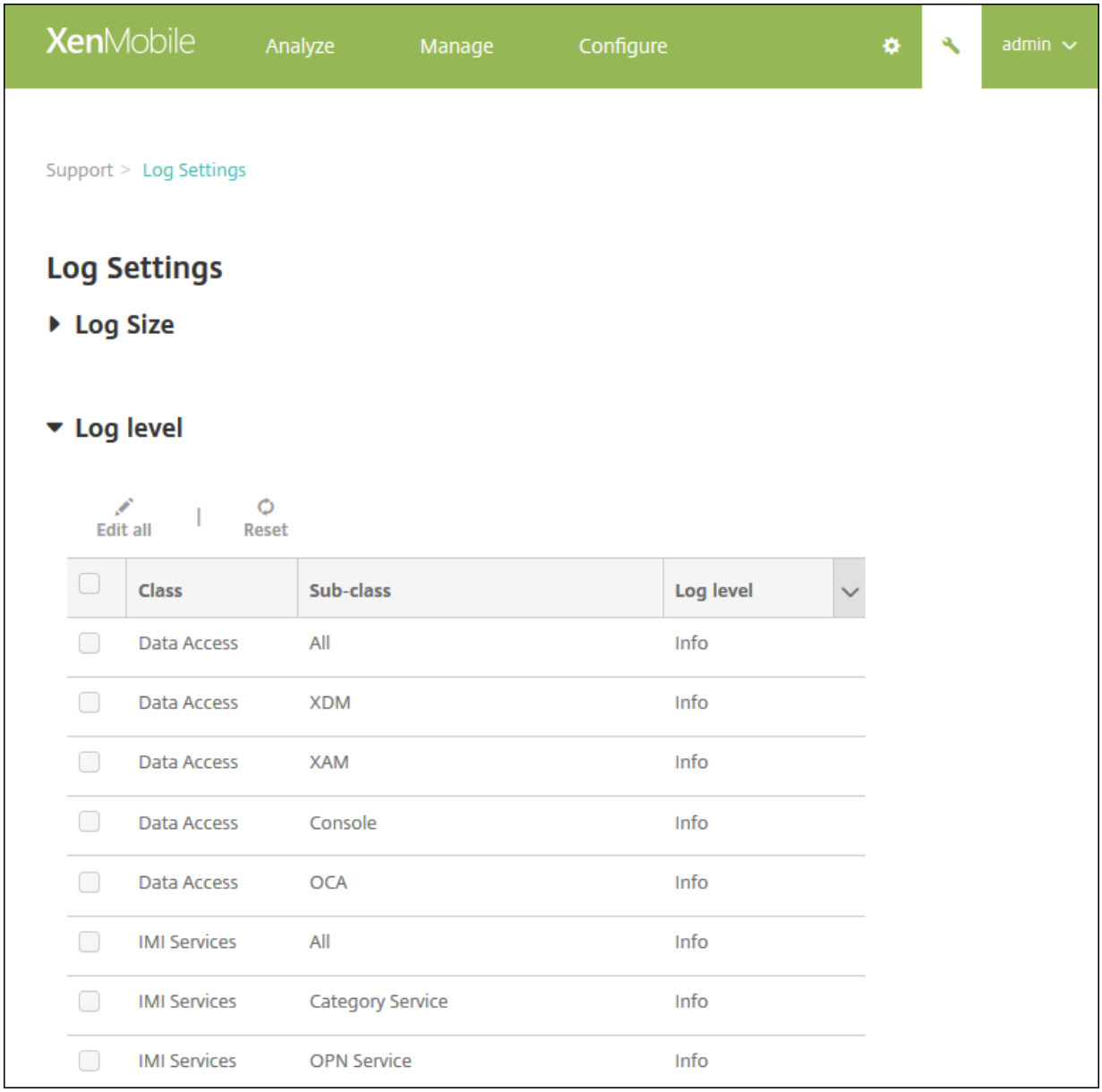
2. 次の設定を構成します。

- **Debug log file size（MB）**：一覧からサイズ（5～20MB）を選択して、デバッグファイルの最大サイズを変更します。デフォルトのファイルサイズは**10 MB**です。
- **Maximum number of debug backup files**：サーバーにより保持されるデバッグファイルの最大数をクリックします。デフォルトでは、サーバーに50件のバックアップファイルが保持されます。
- **Admin activity log file size（MB）**：一覧からサイズ（5～20MB）を選択して、管理者アクティビティファイルの最大サイズを変更します。 デフォルトのファイルサイズは**10 MB**です。
- **Maximum number of admin activity backup files**：サーバーにより保持される管理者アクティビティファイルの最大数をクリックします。 デフォルトでは、サーバーに300件のバックアップファイルが保持されます。
- **User activity log file size（MB）**：一覧からサイズ（5～20MB）を選択して、ユーザーアクティビティファイルの最大サイズを変更します。 デフォルトのファイルサイズは**10 MB**です。
- **Maximum number of user activity backup files**：サーバーにより保持されるユーザーアクティビティファイルの最大数をクリックします。 デフォルトでは、サーバーに300件のバックアップファイルが保持されます。

［Log Level］のオプションを構成するには

ログレベルを設定することにより、XenMobileでログに収集される情報の種類を指定できます。 すべてのクラスに同じレベルを設定することも、個別のクラスに特定のレベルを設定することもできます。

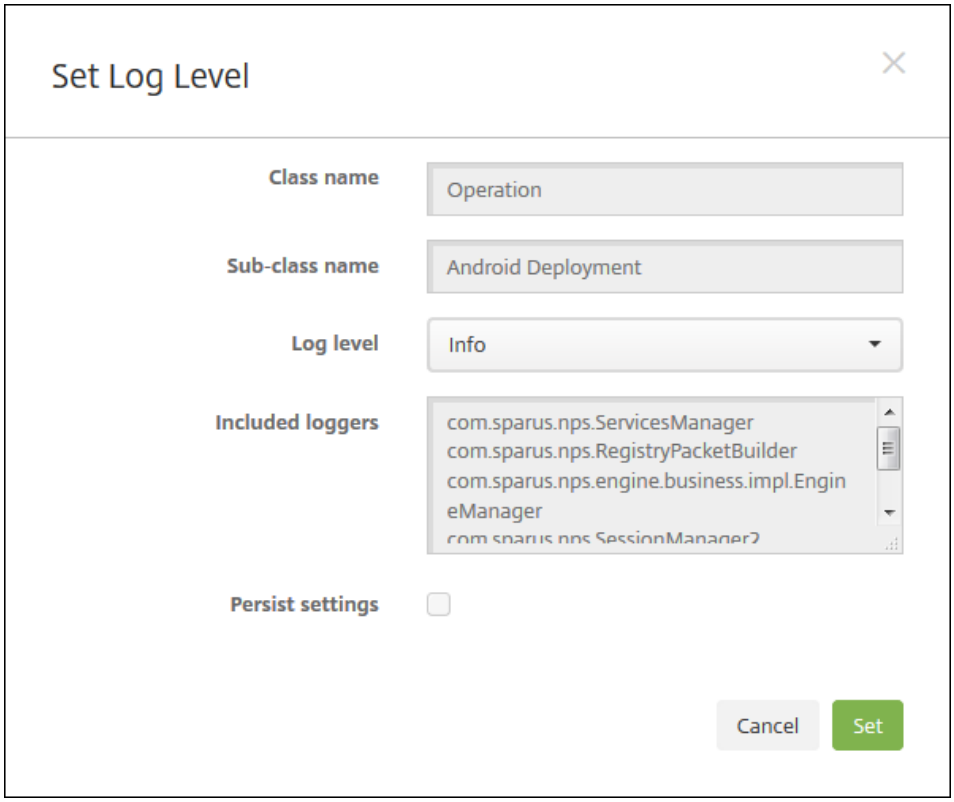
1. **［Log Settings］**ページで**［Log level］**を展開します。 すべてのログクラスの表が表示されます。



2. 次のいずれかを行います。

- 1つのクラスの横のチェックボックスをクリックして [**Set Level**] をクリックし、そのクラスのログレベルのみを変更します。
- [**Edit all**] をクリックしてログレベルの変更を表内のすべてのクラスに適用します。

[**Set Log Level**] ダイアログボックスが開き、ログレベルを設定したり、XenMobileサーバーを再起動したときにログレベルの設定を保持するかどうかを選択したりできます。

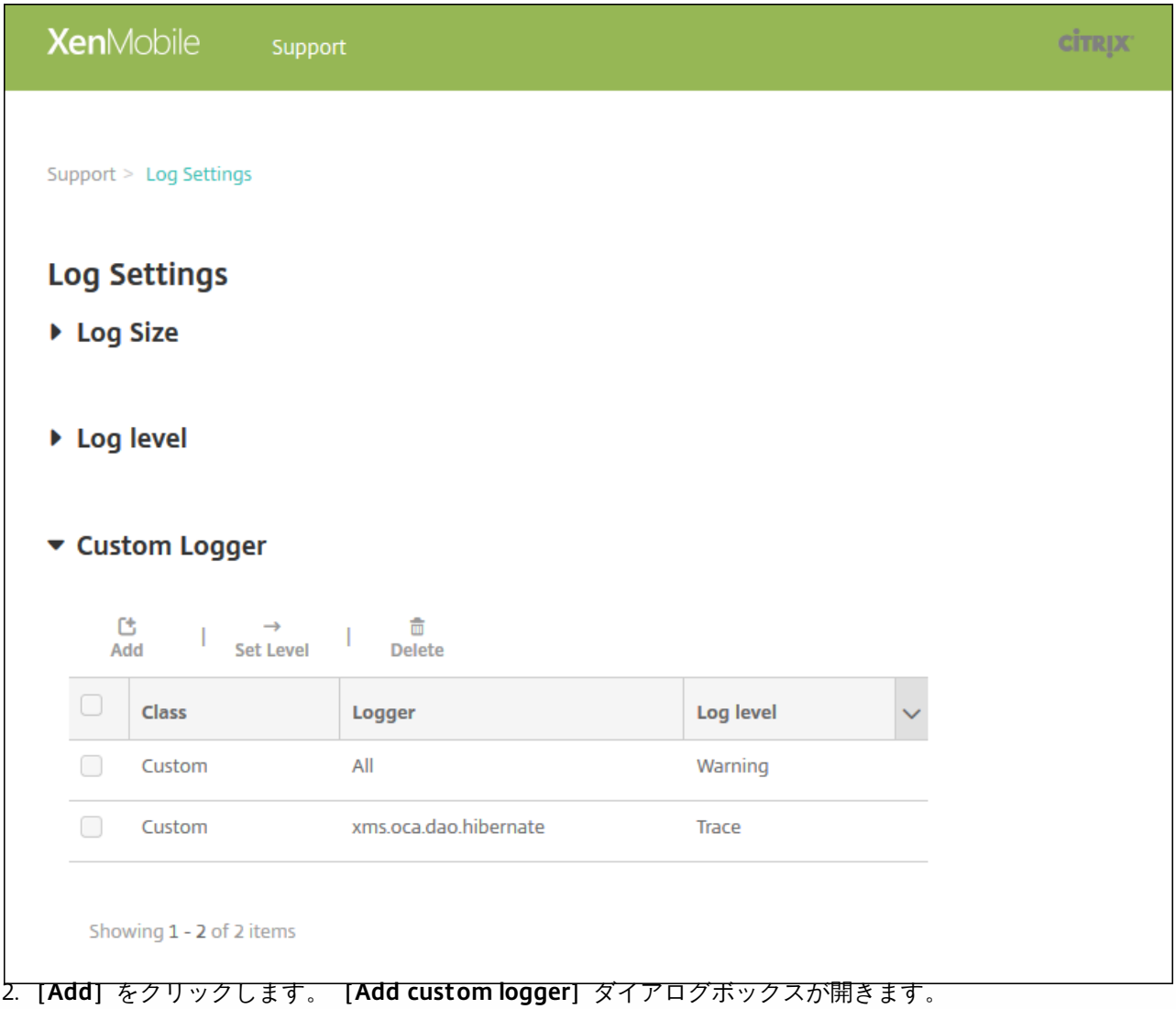


- **Class Name**：すべてのクラスのログレベルを変更する場合はこのフィールドに［All］と表示されます。そうでない場合は個別のクラス名が表示されます。編集できません。
- **Sub-class name**：すべてのクラスのログレベルを変更する場合はこのフィールドに［All］と表示されます。そうでない場合は個別のクラスのサブクラス名が表示されます。編集できません。
- **Log level**：一覧でログレベルをクリックします。 サポートされるログレベルは以下のとおりです。
  - Fatal
  - Error
  - Warning
  - Info
  - Debug
  - Trace
  - Off
- **Included Loggers**：すべてのクラスのログレベルを変更する場合はこのフィールドは空白です。そうでない場合は個別のクラスに対して現在構成されているロガーが表示されます。編集できません。
- **Persist settings**：サーバーを再起動してもログレベルの設定を維持する場合はこのチェックボックスをオンにします。このチェックボックスがオフの場合は、サーバーを再起動するとログレベル設定がデフォルト設定に戻ります。

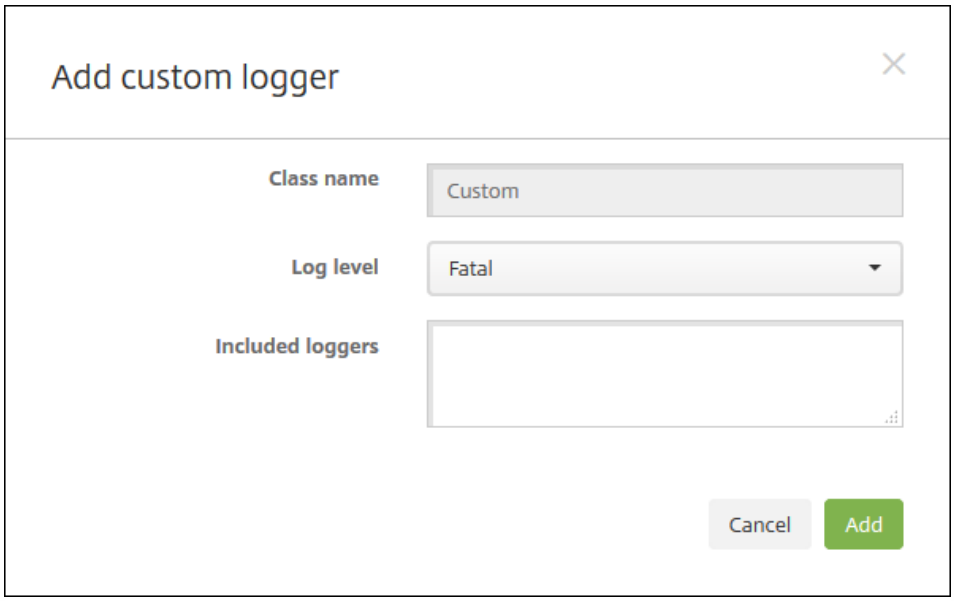
3. ［**Set**］をクリックして変更を確定します。

カスタムロガーを追加するには

1. ［**Log Settings**］ページで［**Custom Logger**］を展開します。 ［**Custom Logger**］の表が表示されます。 カスタムロガーがまだ追加されていない場合、最初はこの表が空白の状態で表示されます。



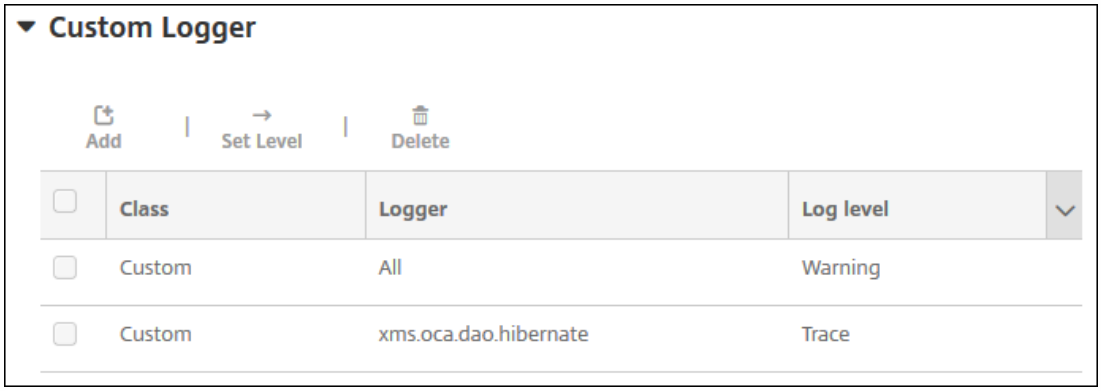
2. [**Add**] をクリックします。 [**Add custom logger**] ダイアログボックスが開きます。



3. 次の設定を構成します。

- **Class Name**：このフィールドには［**Custom**］と表示されます。編集できません。
- **Log level**：一覧でログレベルをクリックします。 サポートされるログレベルは以下のとおりです。
  - Fatal
  - Error
  - Warning
  - Info
  - Debug
  - Trace
  - Off
- **Included Loggers**：カスタムロガーに含める特定のロガーを入力するか、このフィールドを空白にしてすべてのロガーが含まれるようにします。

4. ［**Add**］をクリックします。 カスタムロガーが［**Custom Logger**］の表に追加されます。



カスタムロガーを削除するには

1. ［**Log Settings**］ページで［**Custom Logger**］を展開します。

2. 削除するカスタムロガーを選択します。

2. ［**Delete**］をクリックします。 カスタムロガーを削除するかどうかを確認するダイアログボックスが開きます。［**OK**］をクリックします。

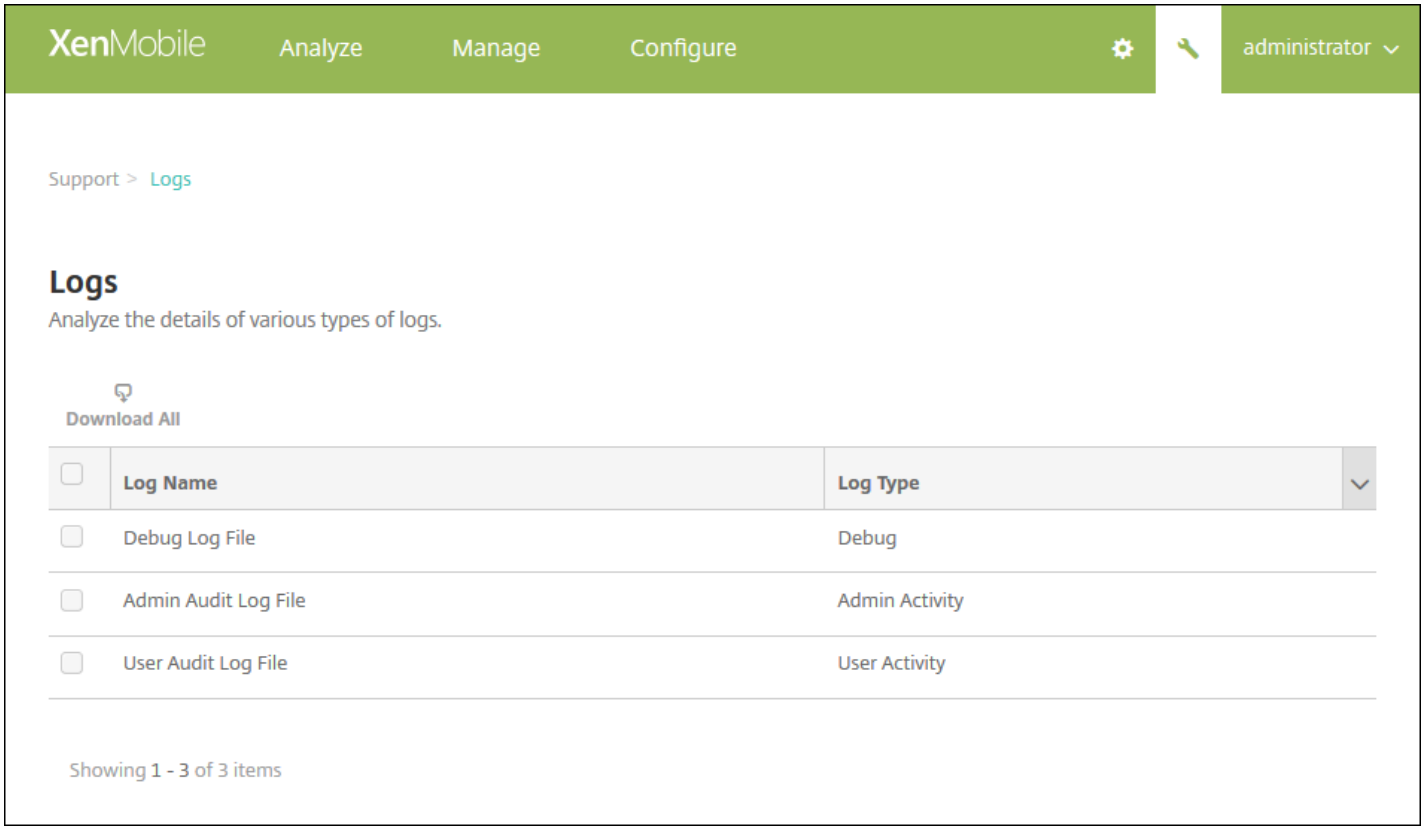
重要：この操作を元に戻すことはできません。

XenMobileでのログファイルの表示および分析

Aug 02, 2016

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。［**Support**］ページが開きます。

2. ［**Log Operations**］の下の［**Logs**］をクリックします。 ［**Logs**］ページが開きます。 表に個別のログが表示されます。



3. 表示するログをオンにします。

- デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrixのサポート担当者向けの有用な情報が含まれています。
- 管理監査ログファイルには、XenMobileコンソール上の活動についての監査情報が含まれています。
- ユーザー監査ログファイルには構成済みユーザーに関連する情報が含まれています。

4. 表の上にあるアクションを使用して、すべてダウンロード、表示、回転、単一ログのダウンロード、選択したログの削除を行います。

注：

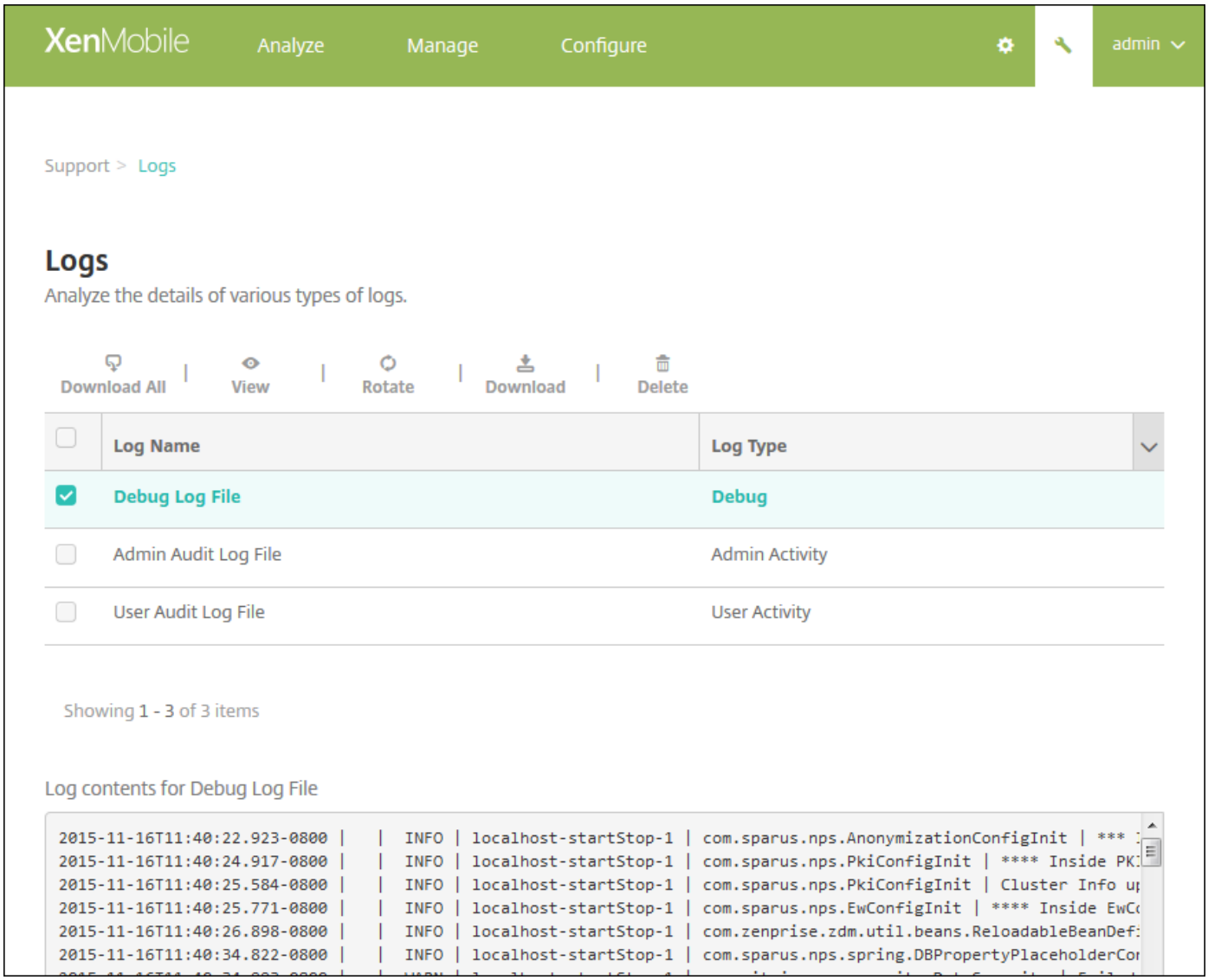
- 複数のログファイルを選択した場合は、［**Download All**］と［**Delete**］のみを使用できます。
- XenMobileサーバーをクラスター化している場合は、接続しているサーバーのログのみを表示できます。 ほかのサーバーのログを表示するには、ダウンロードオプションのいずれかを使用します。

5. 次のいずれかを行います。

- **Download All**：システム上に存在するすべてのログ（デバッグ、管理監査、ユーザー監査、サーバーのログなど）をダウ

ンロードします。

- **View**：表の下に選択したログの内容を表示します。
- **Rotate**：現在のログファイルをアーカイブし、ログエントリを取得するための新しいファイルを作成します。 ログファイルをアーカイブするときに、ダイアログボックスが開きます。 **[Rotate]** をクリックして続行します。
- **Download**：選択されている単一の種類のログファイルのみをダウンロードします。アーカイブ済みの同じ種類のログもダウンロードされます。
- **Delete**：選択したログファイルを完全に削除します。



リモートサポート

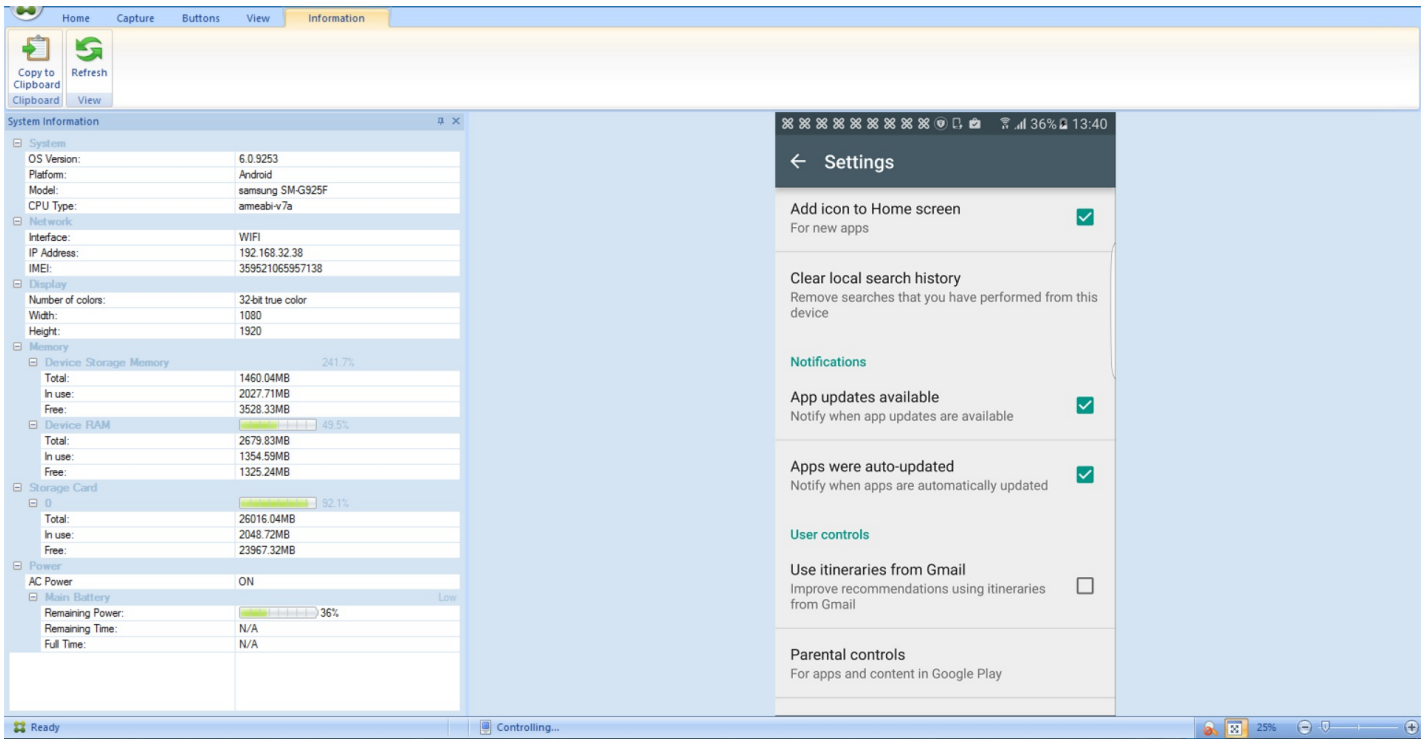
Aug 02, 2016

Remote Supportを使用すると、ヘルプデスクの担当者は管理対象のWindowsおよびAndroidモバイルデバイスをリモートで制御できます。 Remote Supportは、すべてのWindows Mobileデバイスおよび AndroidのSamsung SAFEデバイスで使用できます。 iOSデバイスのリモート制御はサポートされていません。

> ## 注意
>
> XenMobile Remote Supportは、XenMobile Cloud Version 10.xでは利用できません。

リモート制御セッション時の動作は次のようになります。

- ユーザーのモバイルデバイスには、リモート制御セッションがアクティブであることを示すアイコンが表示されます。
- Remote Supportアプリケーションウィンドウが開いて、［Remote Contorol］ウィンドウに制御対象デバイスが表示されます。



Remote Supportでは、以下の機能が提供されます。

- ユーザーのモバイルデバイスにリモートでログオンし、デバイスの画面を制御する。 ユーザーはヘルプデスク担当者による画面の移動を確認できるため、ユーザーのトレーニングとしても役に立つことがあります。
- リアルタイムでリモートデバイス内を移動して修復する。 構成の変更、オペレーティングシステムの問題のトラブルシューティング、問題があるアプリケーションやプロセスの無効化または終了を行うことができます。
- ネットワークアクセスの無効化、不正プロセスの停止、アプリまたはマルウェアの削除をリモートに実行することで、ほかのモバイルデバイスに脅威が広がる前に、その脅威を隔離して封じこめる。

- ユーザーがデバイスを見つけられるように、デバイスの着信音や電話の発信をリモートで有効にする。 デバイスを見つけることができなかった場合は、重要なデータが侵害されないように、デバイスにワイプを実行できます。

Remote Supportでは、サポート担当者に次の機能も提供されます。

- 1つまたは複数のXenMobileサーバーについて、接続しているすべてのデバイスの一覧を表示する。
- デバイスのモデル、オペレーティングシステムのレベル、IMEI（International Mobile Station Equipment Identity）およびシリアル番号、メモリおよびバッテリーの状態、接続状態などのシステム情報を表示する。
- XenMobileサーバーのユーザーおよびグループを表示する。
- アクティブなプロセスの表示や停止、およびモバイルデバイスの再起動を行うためのデバイスタスクマネージャーの実行。
- モバイルデバイスと中央ファイルサーバー間の双方向のリモートファイル転送を実行する。
- 1つまたは複数のモバイルデバイスに対するソフトウェアプログラムの一括ダウンロードおよびインストール。
- デバイスのレジストリキーのリモートからの構成。
- 携帯電話ネットワークによる狭帯域幅接続でのレスポンスを最適化するリアルタイムのデバイス画面リモート制御。
- さまざまなモバイルデバイスブランドおよびモデルのデバイススキンを表示する。 スキンエディターを表示して、新規デバイスモデルの追加および物理キーのマッピングを行うことができます。
- デバイス画面の取り込み、記録、再生により、デバイスでの一連のビデオAVIファイル作成操作を記録できるようにする。
- 共有ホワイトボード、VoIPベースの音声通信、およびチャットによるモバイルユーザーとサポート担当者間のLive Meeting。

Remote Supportのシステム要件

Remote Supportソフトウェアは、以下の要件を満たすWindousベースのコンピューターにインストールします。 ポートの要件については、「ポート要件」を参照してください。

サポートされるプラットフォーム

- Intel Xeon/Pentium 4-1GHz以上のワークステーションクラス
- 512MB以上のRAM
- 100MB以上の空きディスク領域

サポートされるオペレーティングシステム

- Microsoft Windows 2003 Server Standard EditionまたはEnterprise Edition SP1以降
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2以降
- Microsoft Windows Vista SP1以降
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Remote Supportソフトウェアをインストールするには

1. Remote Supportのインストーラーをダウンロードするには、XenMobile 10ダウンロードページにアクセスしてアカウントにログオンします。
2. **[Tools]** を展開して、XenMobile Remote Support v9をダウンロードします。
   現在、Remote Supportのファイル名はXenMobileRemoteSupport-9.0.0.35265.exeです。

3. Remote Supportインストーラーをダブルクリックし、表示されるインストールウィザードの指示に従います。

コマンドラインからRemote Supportをインストールするには：

次のコマンドを実行します。

<*RemoteSupport*>.exe /S

ここで、<*RemoteSupport*>はインストールプログラムの名前です。 次に例を示します。

XenMobileRemoteSupport-9.0.0.35265.exe /S

Remote Supportソフトウェアのインストール時には、次の変数を使用できます。

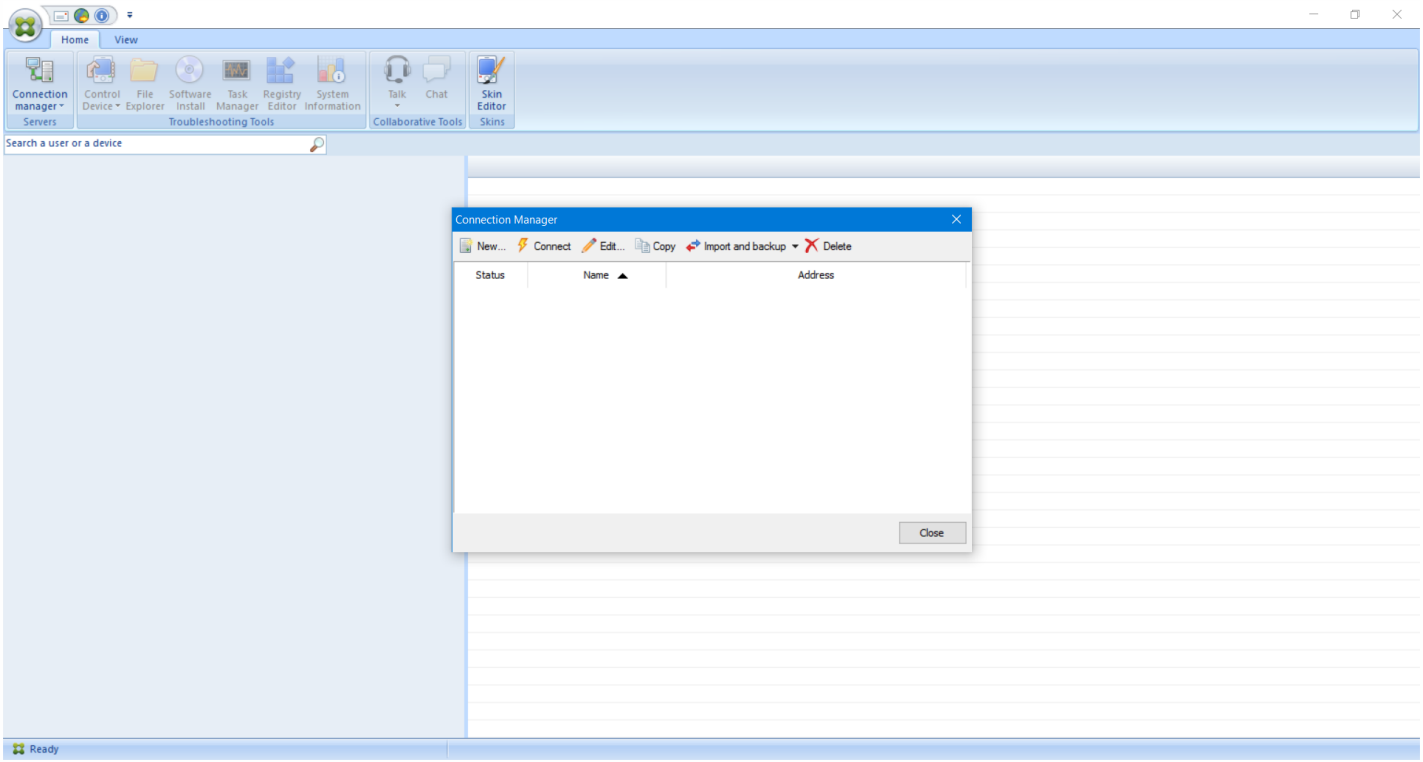
- /S：デフォルトのパラメーターを使用してRemote Supportソフトウェアをサイレントインストールします。
- /D=dir:。カスタムのインストールディレクトリを指定します。

Remote SupportをXenMobileに接続するには

管理対象デバイスへのリモートサポート接続を確立するには、Remote Supportからの接続を、該当のデバイスを管理するXenMobileサーバーに追加する必要があります。 この接続は、AndroidおよびWindows Mobile/CEデバイス向けのデバイスポリシーであるトンネルポリシーで定義されたアプリトンネル上で実行されます。 Remote SupportをXenMobileに接続するには、アプリトンネルを「アプリトンネリングデバイスポリシー」の説明に従って定義する必要があります。

1. Remote Supportソフトウェアを起動し、XenMobileの資格情報を使用してログオンします。

2. [**Connection Manager**]で、 [**New**]をクリックします。



3. [**Connection Configuration**]ダイアログボックスの [**Server**]タブで、次の値を入力します。

[**Configuration name**] に構成エントリの名前を入力します。

[**Server IP address or name**] にXenMobileサーバーのIPアドレスまたはDNS名を入力します。

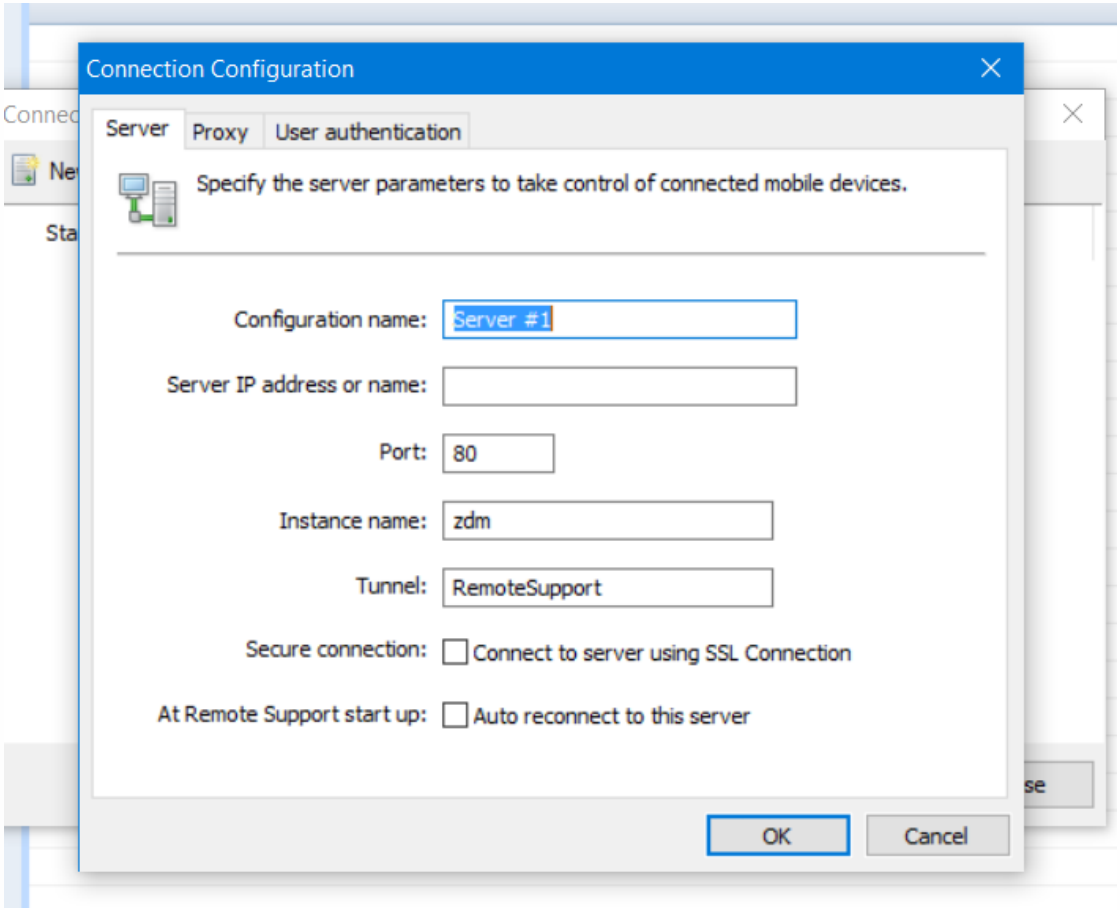
[**Port**] に、XenMobileサーバー構成で定義されているTCPポート番号を入力します。

XenMobileがマルチテナント環境に含まれている場合は、[**Instance name**] にインスタンス名を入力します。

[**Tunnel**] にトンネルポリシーの名前を入力します。

[**Connect to server using SSL Connection**] チェックボックスをオンにします。

Remote Supportアプリケーションが起動するたびに、構成したXenMobileサーバーに接続するには、[**Auto reconnect to this server**] チェックボックスをオンにします。



4. [**Proxy**] タブで、 [**Use a http proxy server**] を選択して次の情報を入力します。

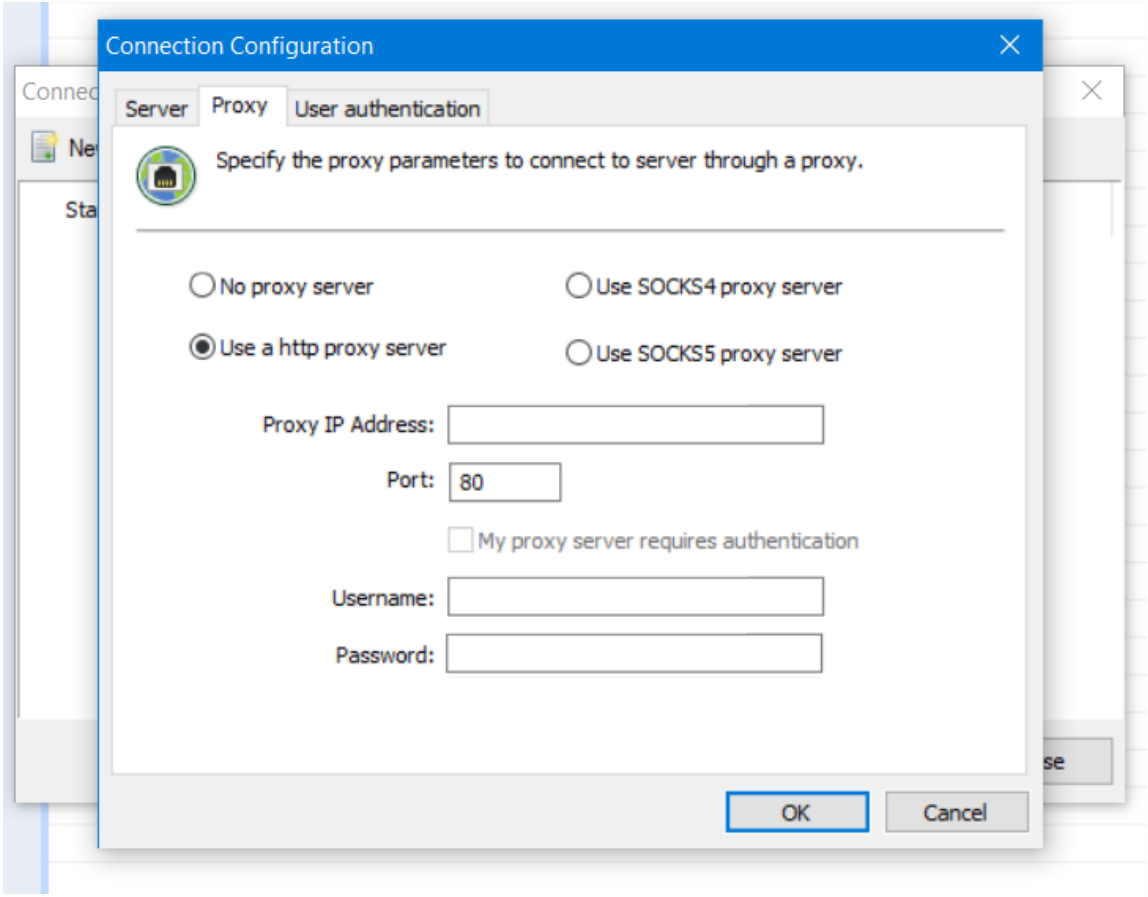
   [**Proxy IP Address**] に、プロキシサーバーのIPアドレスを入力します。

   [**Port**] に、プロキシで使用するTCPポート番号を入力します。

   プロキシサーバーでトラフィックの許可に認証が必要な場合は、[**My proxy requires authentication**] チェックボックスをオンにします。

   [**Username**] に、プロキシサーバーで認証するユーザー名を入力します。

   [**Password**] に、プロキシサーバーで認証するパスワードを入力します。



5. [**User Authentication**] タブで、 [**Remember my login and password**] チェックボックスをオンにして資格情報を入力します。

6. [**OK**] をクリックします。

XenMobileに接続するには、作成した接続をダブルクリックし、この接続用に構成したユーザー名とパスワードを入力します。

Samsung Knoxデバイスでリモートサポートを有効にするには

XenMobileでリモートサポートポリシーを作成して、ユーザーのSamsung

KNOXデバイスへのリモートアクセスを行うことができます。 次の2種類のサポートを構成できます。

- [Basic] は、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率とCPU使用率）、インストールされているソフトウェアフォルダーの内容など、デバイスに関する診断情報を表示できます。
- [Premium] は、色の制御（メインウィンドウまたは独立した浮動ウィンドウ）、ヘルプデスクとユーザーの間のVoIP（Voice-over-IP）セッションの確立、設定の構成、ヘルプデスクとユーザーの間のチャットセッションの確立など、デバイスの画面をリモート制御できます。

リモートサポートポリシーの構成について詳しくは、「リモートサポートデバイスポリシー」を参照してください。

リモートサポートセッションを使用するには

Remote Supportを起動すると、Remote Supportアプリケーションウィンドウの左側に、XenMobile管理コンソールで定義されているXenMobileユーザーグループが表示されます。 デフォルトでは、現在接続されているユーザーが含まれているグループのみが表示されます。 ユーザーエントリの横に、各ユーザーのデバイスが表示されます。

1. すべてのユーザーを表示するには、左側の列の各グループを展開します。
   XenMobileサーバーに現在接続されているユーザーは、緑のアイコンで表示されます。
2. すべてのユーザー（現在接続されていないユーザーを含む）を表示するには、[**View**] をクリックし、 [**Non-connected devices**] を選択します。
   接続されていないユーザーは、緑のアイコンなしで表示されます。

XenMobileサーバーに接続されているもののユーザーに割り当てられていないデバイスは、匿名モードで表示されます （一覧に「**Anonymous**」と表示されます）。これらのデバイスは、ログインユーザーのデバイスと同じように制御できます。

デバイスを制御するには、デバイスの行をクリックしてデバイスを選択してから、[**Control Device**] をクリックします。 デバイスが [Remote Control] ウィンドウに表示されます。 管理対象デバイスを操作する方法の例を以下に示します。

- デバイス画面のメインウィンドウまたは別の浮動ウィンドウを制御する（色の制御を含む）。
- ヘルプデスクとユーザー間のVoIP（Voice-over-IP）セッションを確立する。 VoIP設定を構成します。
- ユーザーとのチャットセッションを確立する。
- デバイスのタスクマネージャーにアクセスして、メモリの使用率、CPUの使用率、実行中のアプリケーションなどのアイテムを管理する。

- モバイルデバイスのローカルディレクトリを探索する。 ファイルを転送する。
- Windows Mobileデバイス上のデバイスレジストリを編集する。
- デバイスシステム情報およびインストールされているすべてのソフトウェアを表示する。
- XenMobileサーバーとモバイルデバイスの接続状態を更新する。

XenMobileコマンドラインインターフェイスオプション

Aug 02, 2016

XenMobileをインストールしたハイパーバイザー（Citrix XenServer、Microsoft Hyper-V、VMware ESXi）で、以下のコマンドラインインターフェイス（CLI）オプションにいつでもアクセスできます。

以下は［Main menu］（メインメニュー）から選択できるオプションで、［Configuration］、［Clustering］、［System］、［Troubleshooting］の4つのオプションがメニューの最初に表示されます。

Main menu

---

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

Choice: [0 - 5]

［Configuration］メニューオプション

メインメニューから［Configuration］オプションを選択すると、次のメニューが表示されます。

[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

Choice: [0 - 4]

［Network］オプションを選択した場合は、変更を保存するために再起動を求めるメッセージが表示されます。

［Firewall］オプションを選択した場合は、以下のメッセージが表示されます。

Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:

- comma separated list of hosts or networks

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

- enter c as value to clear list

HTTPサービス

ポート：80

Enable access (y/n) [y]:

Management HTTPS service

ポート：4443

Enable access (y/n) [y]:

SSHサービス

Port [22]:

Enable access (y/n) [y]:

Access white list []:

Management API (for initial staging) HTTPS service

Port [30001]:

Enable access (y/n) [y]:

Access white list []:

リモートサポートトンネル

Port [8081]:

Enable access (y/n) [n]:

［Database］オプションを選択した場合は、以下のメッセージが表示されます。

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

［Clustering］メニューオプション

メインメニューから［Clustering］オプションを選択すると、次のメニューが表示されます。

[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

Choice: [0 - 5]

クラスタリングの有効化を選択すると、次のメッセージが表示されます。

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

クラスタリングの無効化を選択すると、次のメッセージが表示されます。

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

クラスタリングが無効になっている場合に［Cluster member white list］を選択すると、次のメッセージが表示されます。

Cluster is disabled. Please enable it.

クラスタリングを有効にした場合は、次のオプションが表示されます。

Current White List:

- comma separated list of hosts or network

- 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を選択すると、次のメッセージが表示されます。

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

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

Hazlecast Cluster Members:

[IP address listed]

NOTE: If an configured node is not part of the cluseter, please reboot that node.

［System］メニューオプション

メインメニューから［System］オプションを選択すると、次のメニューが表示されます。

---

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

Choice: [0 - 9]

［Troubleshooting］メニューオプション

メインメニューから［Troubleshooting］オプションを選択すると、次のメニューが表示されます。

---

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

Choice: [0 - 3]

［Network Utilities］オプションを選択した場合は、次のメニューが表示されます。

---

[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

Choice: [0 - 7]

［Logs］オプションを選択した場合は、次のメニューが表示されます。

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

XenMobile Analyzerツール

Oct 25, 2016

XenMobile Analyzerは、インストールやその他の機能についてのXenMobileに関連する問題の診断とトラブルシューティングを行うことができる、クラウドベースのツールです。 このツールにより、XenMobile環境内でのデバイスまたはユーザーの登録と認証の問題がチェックされます。

このチェックを有効にするには、お使いのXenMobileサーバーをポイントするようにツールを構成して、サーバーの展開の種類、モバイルプラットフォーム、認証の種類、テスト用のユーザー資格情報などの情報を入力する必要があります。 設定が完了するとツールはサーバーに接続し、構成の問題をチェックするために環境をスキャンします。 XenMobile Analyzerで問題が検出されると、ツールにより問題を修正するための推奨事項が示されます。

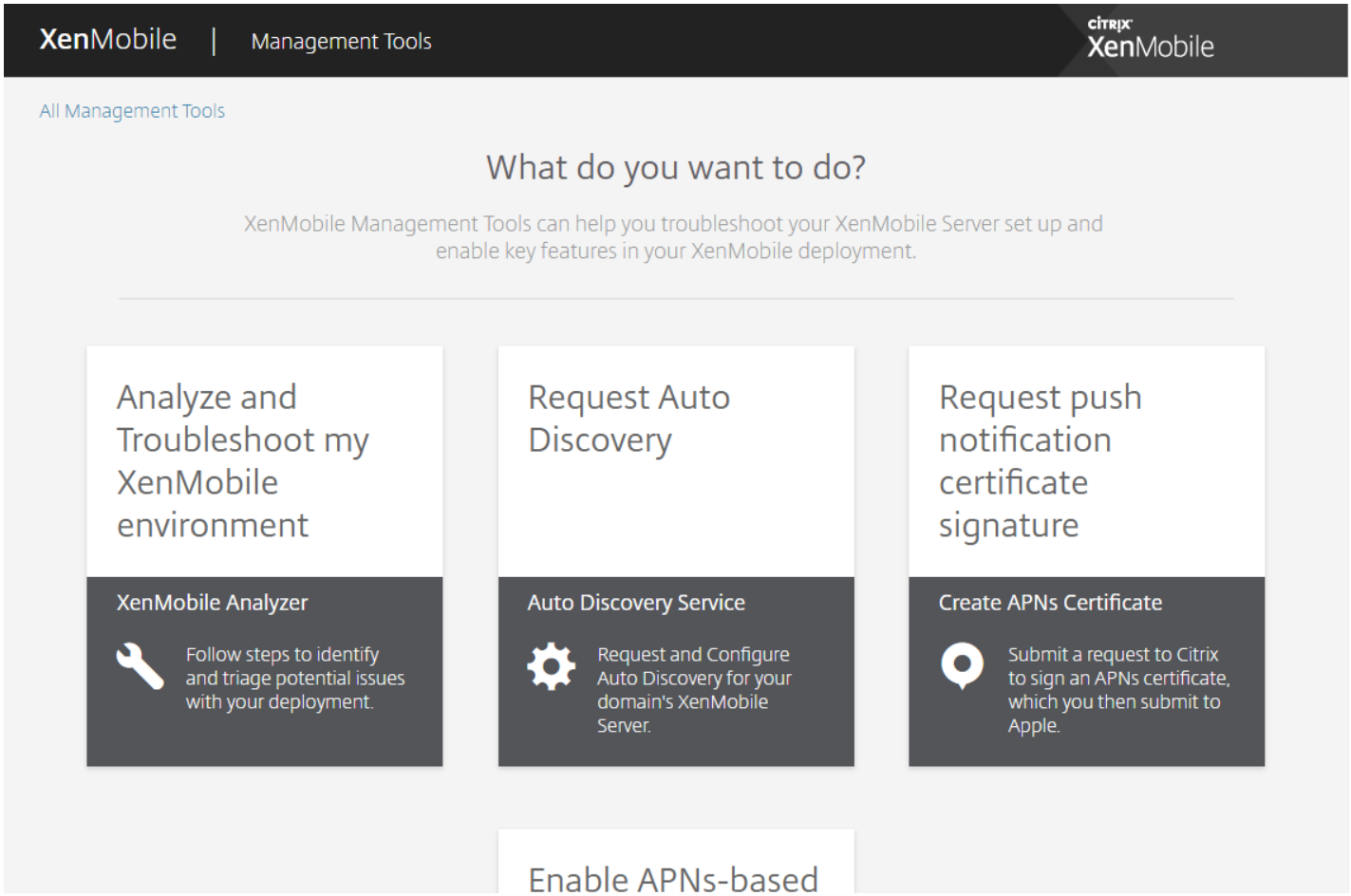
XenMobile Analyzerの主な機能

- 安全な、クラウドベースのマイクロサービスを提供して、すべてのXenMobile関連の問題点をトラブルシューティングします。
- XenMobileの構成関連の問題点がある場合、正確な推奨事項を提供します。
- サポートへの問い合わせ件数を低減し、より短時間でのXenMobile環境のトラブルシューティングを可能にします。
- XenMobileサーバーリリースに対してゼロデイサポートを提供します。
- iOSカスタム登録を有効化します。XenMobile（8443番ポート以外）のカスタムポートのサポート。
- 信頼できないか不完全なサーバー証明書に対して証明書受け入れダイアログボックスを表示します。
- 2要素認証シナリオを自動的に検出します。
- イントラネットサイトへのWorxWebの到達可能性をテストします。
- WorxMail Auto Discoveryサービスのチェックを行います。
- ShareFileへのシングルサインオンのチェックを行います。
- NetScalerのカスタムポートサポートを有効化します。
- 英語版以外のブラウザーをサポートします。

前提条件

製品	サポートされるバージョン
XenMobileサーバー	10.3.0 - 10.3.6
NetScaler Gateway	10.5～11.1
クライアント登録シミュレーション	iOSまたはAndroid

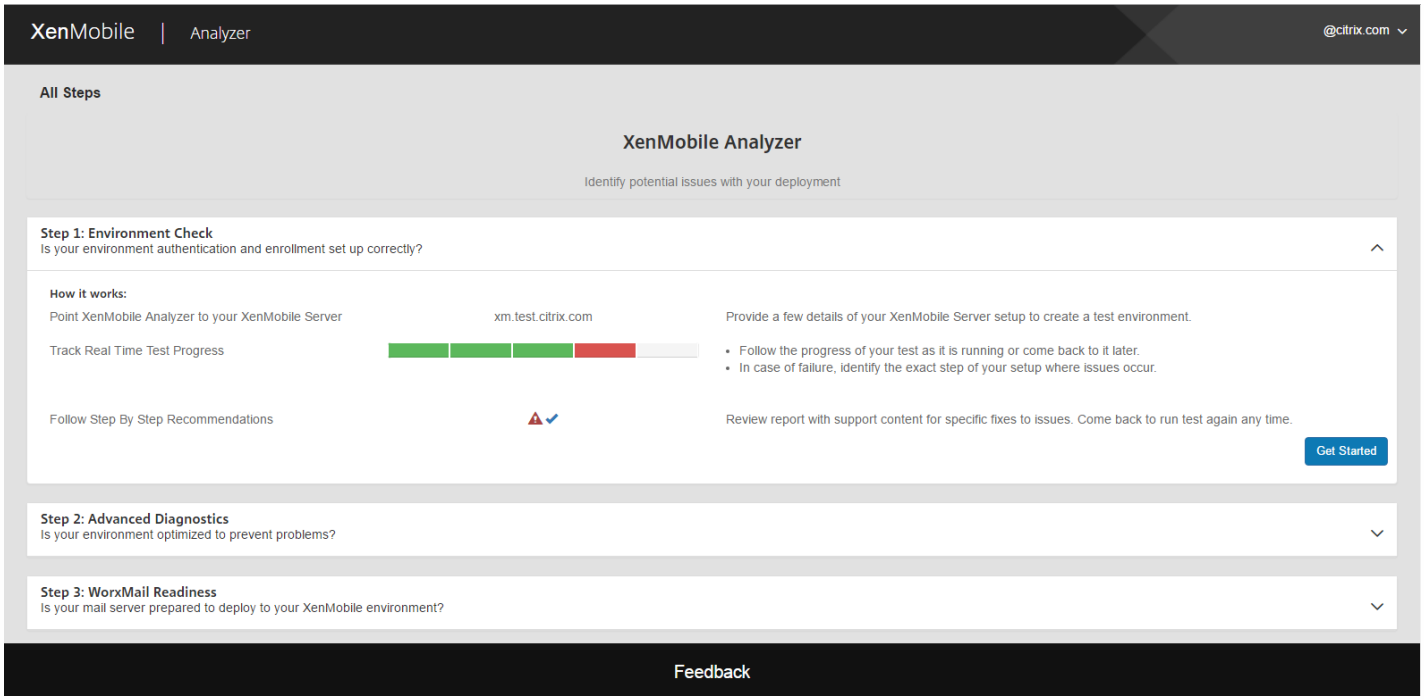
MyCitrix資格情報を使用して、https://xenmobiletools.citrix.comからツールにアクセスします。 表示された［XenMobile Management Tools］ページで、XenMobile Analyzerを起動し、 **［Analyze and Troubleshoot my XenMobile Environment］**をクリックします。



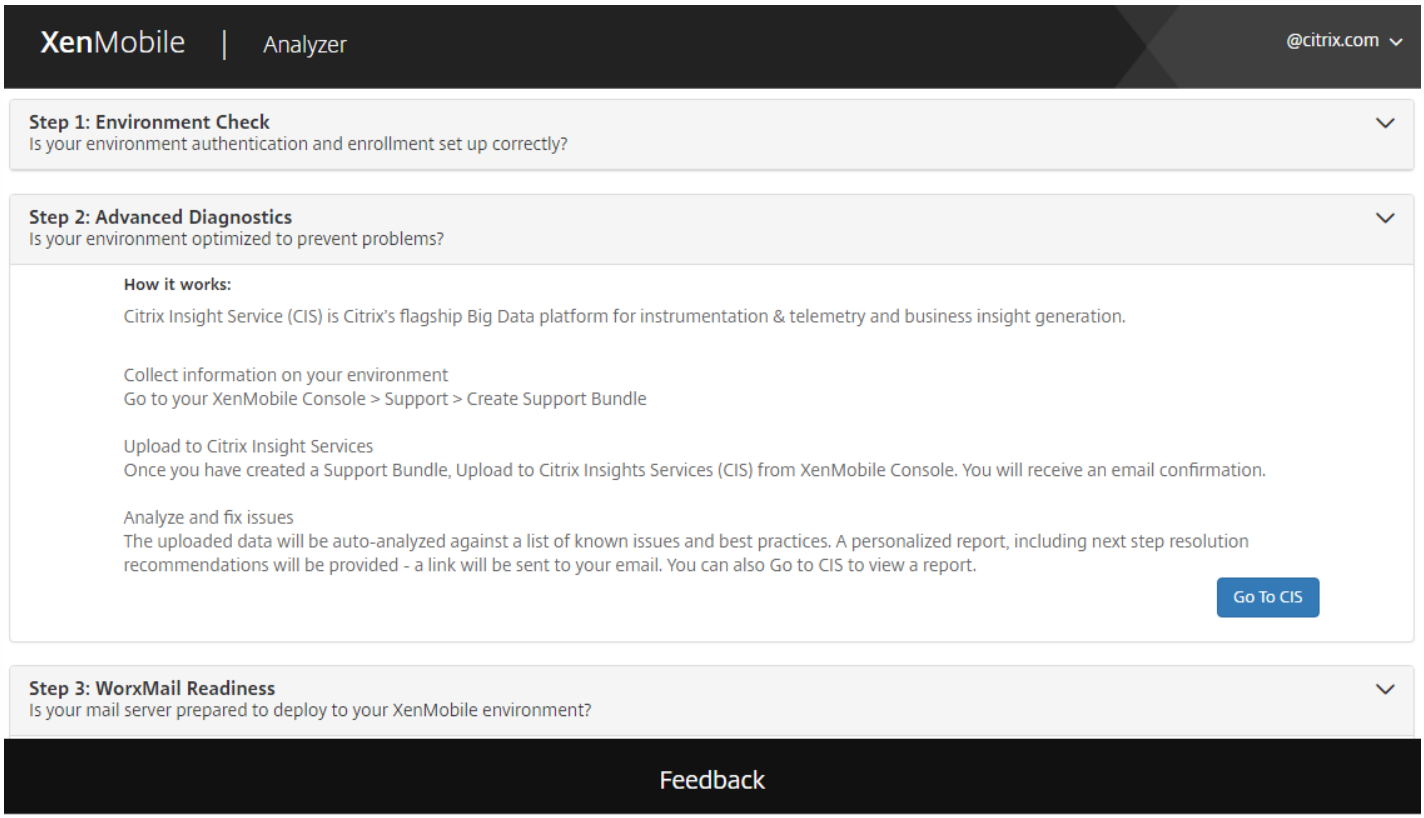
XenMobile Analyzerには、トリアージプロセスを実行しサポートチケットを削減するための5つの主要な手順があります。この手順により、かかる費用を抑えることができます。

手順は次のとおりです。

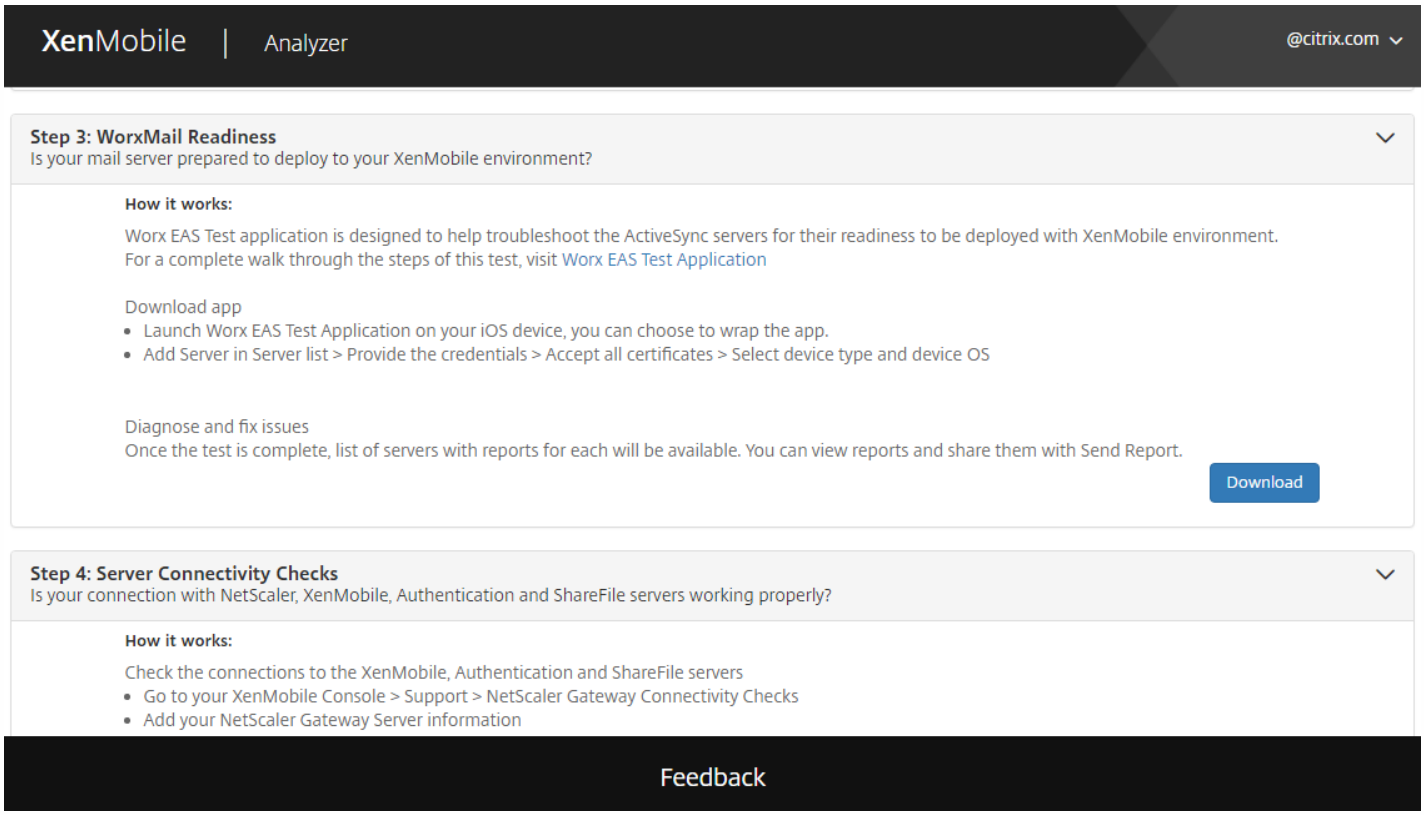
1. **Environment Check** - この手順では、設定に問題がないかどうかをチェックするテストを設定します。 また、デバイス、ユーザー登録、および認証に関する問題についての推奨事項も示されます。



2. **Advanced Diagnostics** - この手順では、環境チェックで見逃された可能性のある問題を見つけるための、Citrix Insight Servicesの使用に関する情報が提供されます。

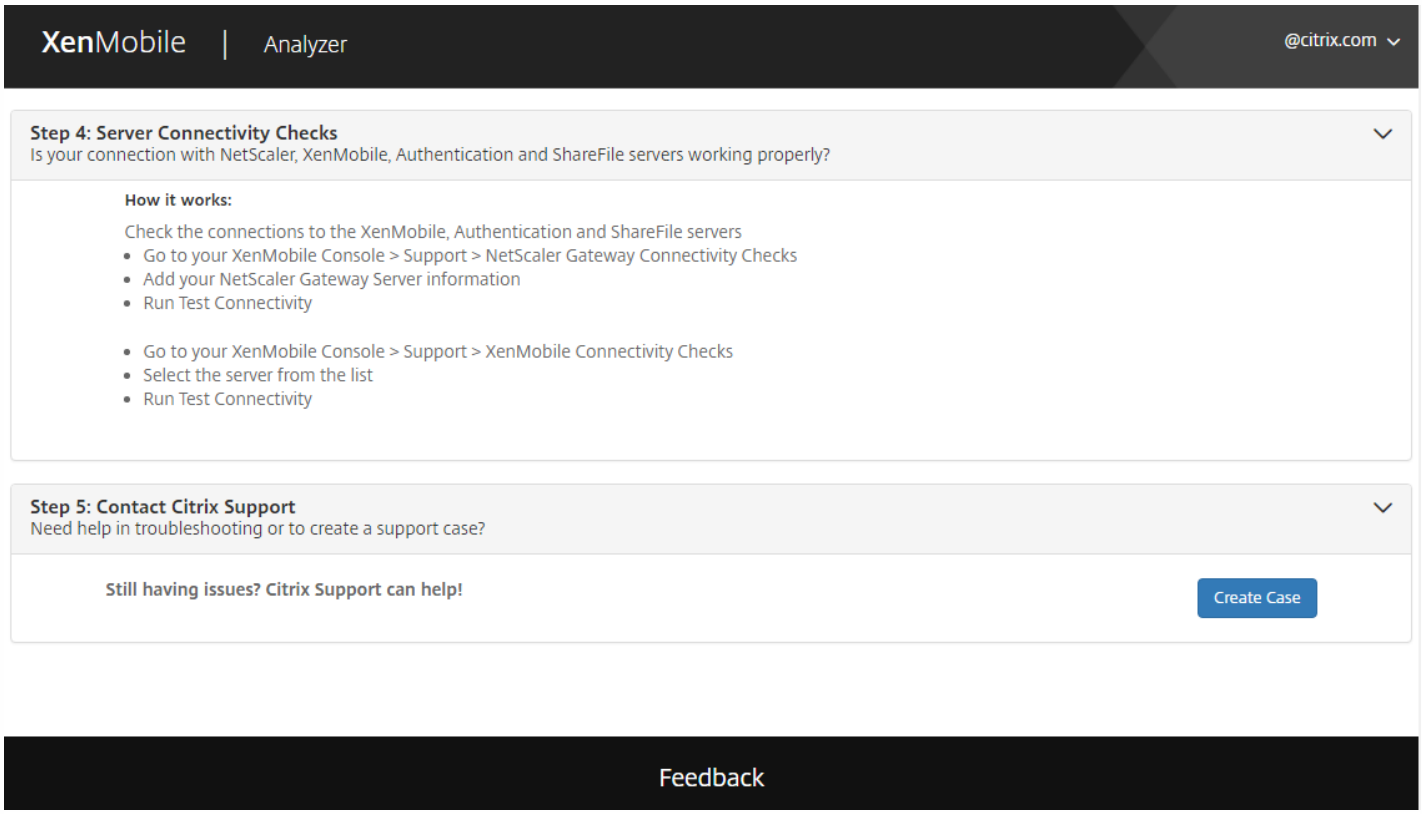


3. **WorxMail Readiness** - この手順では、Worx Exchange ActiveSync Testアプリケーションをダウンロードします。このアプリケーションを使用すると、XenMobile環境へのActiveSyncサーバーの展開に関するトラブルシューティングを行うことができます。



4. **Server Connectivity Checks** - この手順では、サーバーの接続性をテストする方法が示されます。

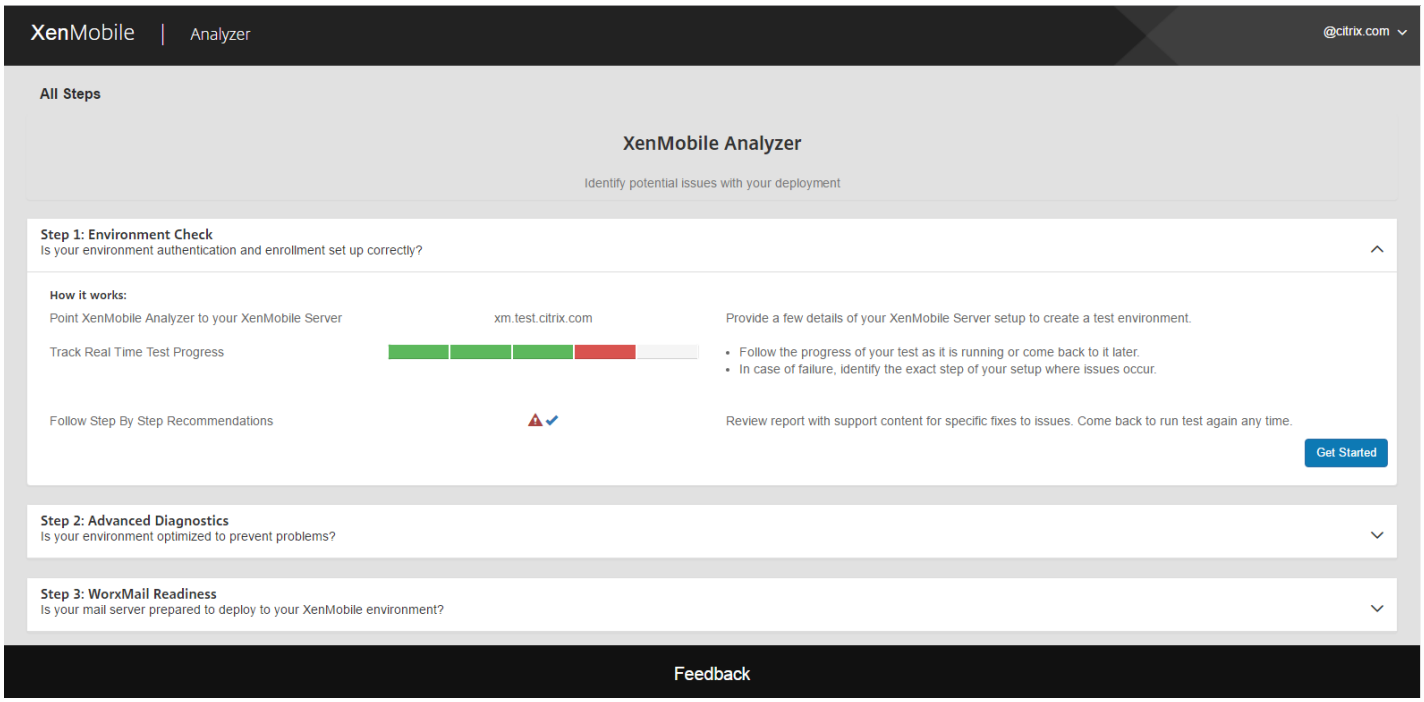
5. **Contact Citrix Support** - この手順では、依然として問題が発生する場合にCitrixサポートケースを登録するためのサイトのリンクが表示されます。



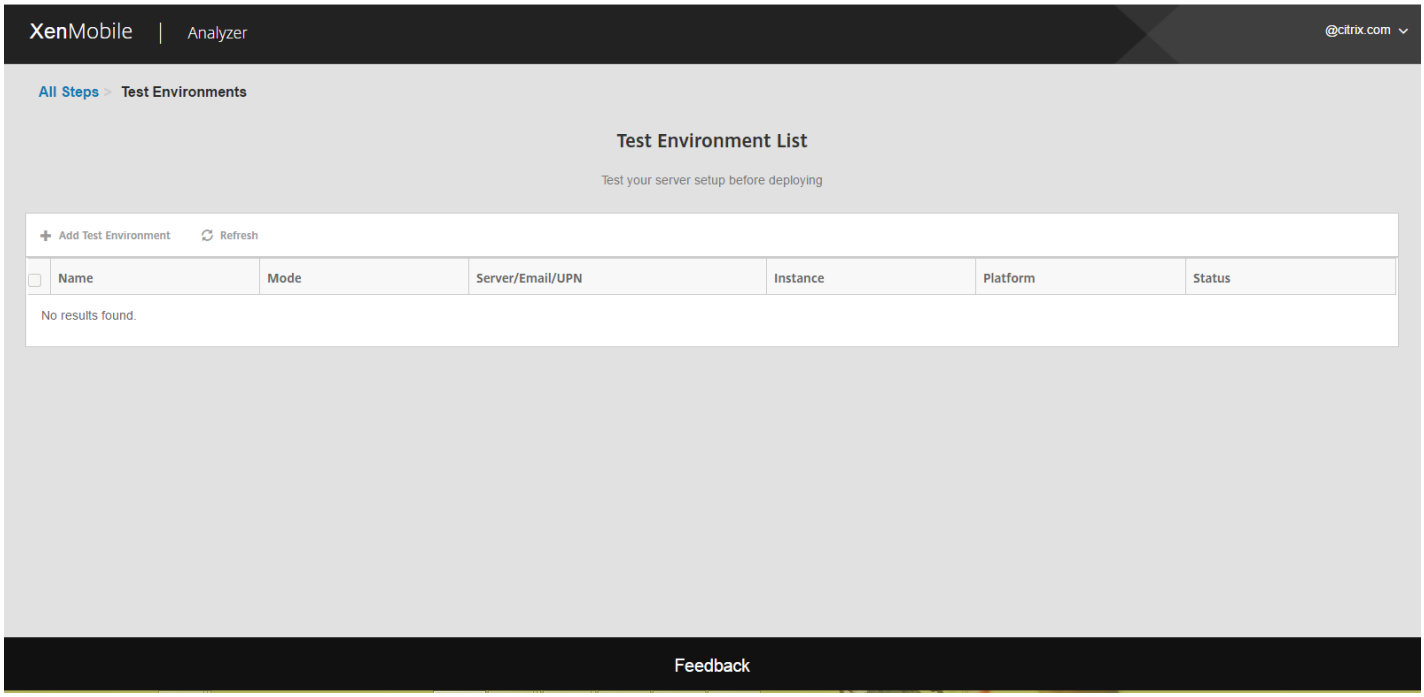
以下のセクションで、これらの手順についてより詳しく説明します。

環境チェックの実行

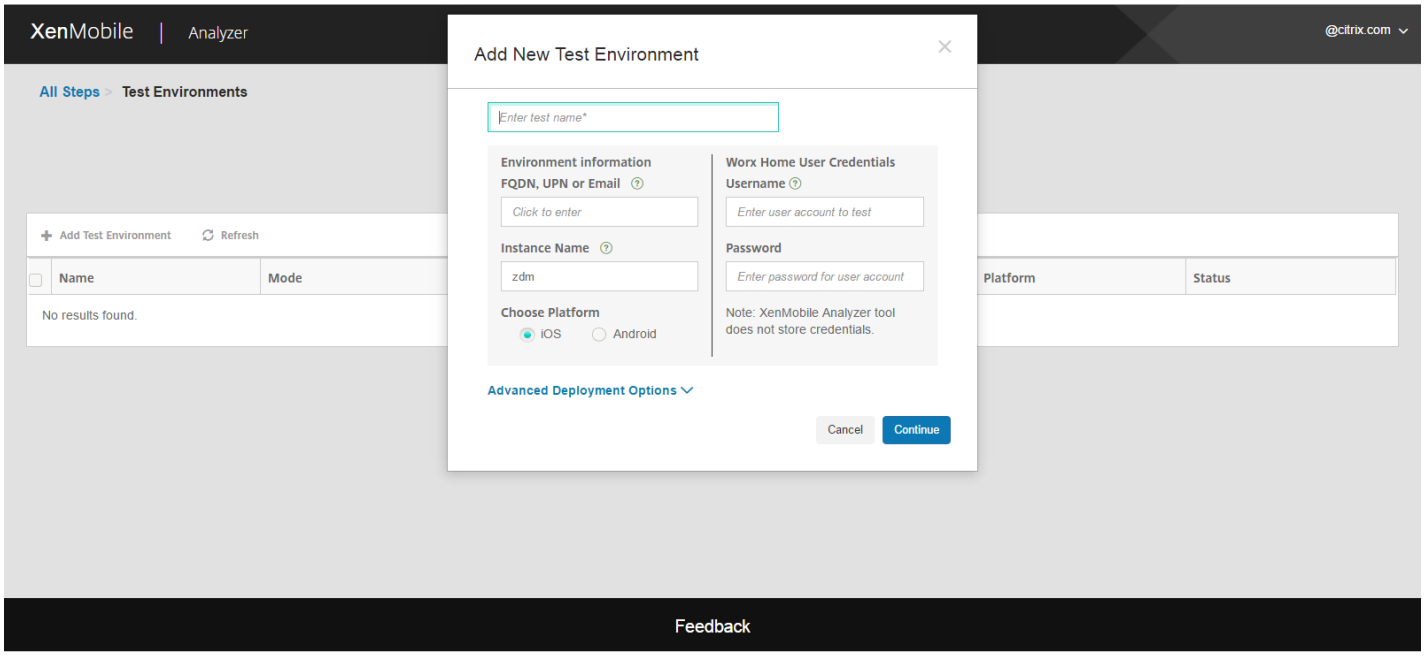
1. XenMobile Analyzerにログオンし、［**Step 1: Environment Checks**］をクリックします。
2. ［**Get Started**］をクリックします。



3. ［**Add Test Environment**］をクリックします。



4. **[Add Test Environment]**ダイアログボックスで、次の操作を行います。



a. 今後テストを特定できるように、テストの一意の名前を入力します。

b. 登録用の招待URLがある場合は、**[Advance Deployment Options]**をクリックします。 このオプションが展開されたら、 **[Do you have invitation URL]**チェックボックスをオンにして招待URLを入力します。 このフィールドを空白のままにすると、XenMobileサーバー、ユーザー名、およびその他の詳細がツールにより自動て検出されます。

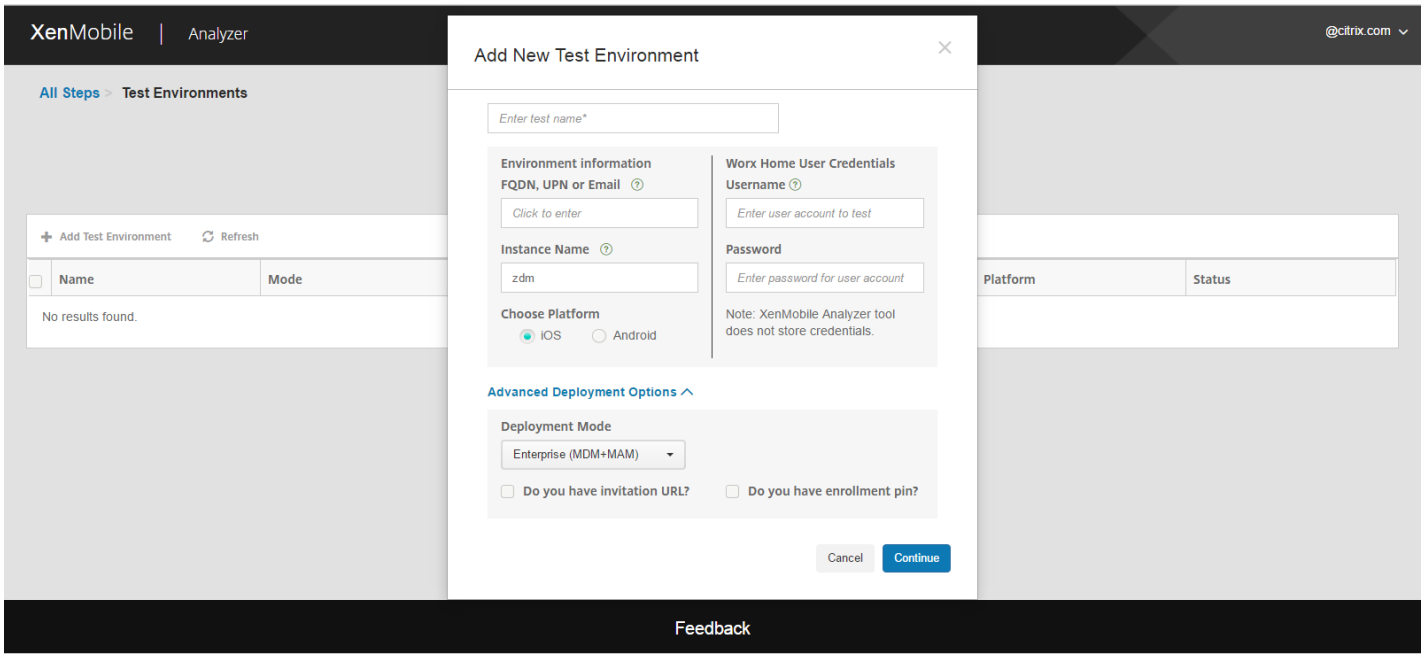
c. 招待URLがない場合は、サーバー情報を手動で入力できます。

d. **［Deployment Mode］**リストで、使用中のXenMobile展開モードを選択します。

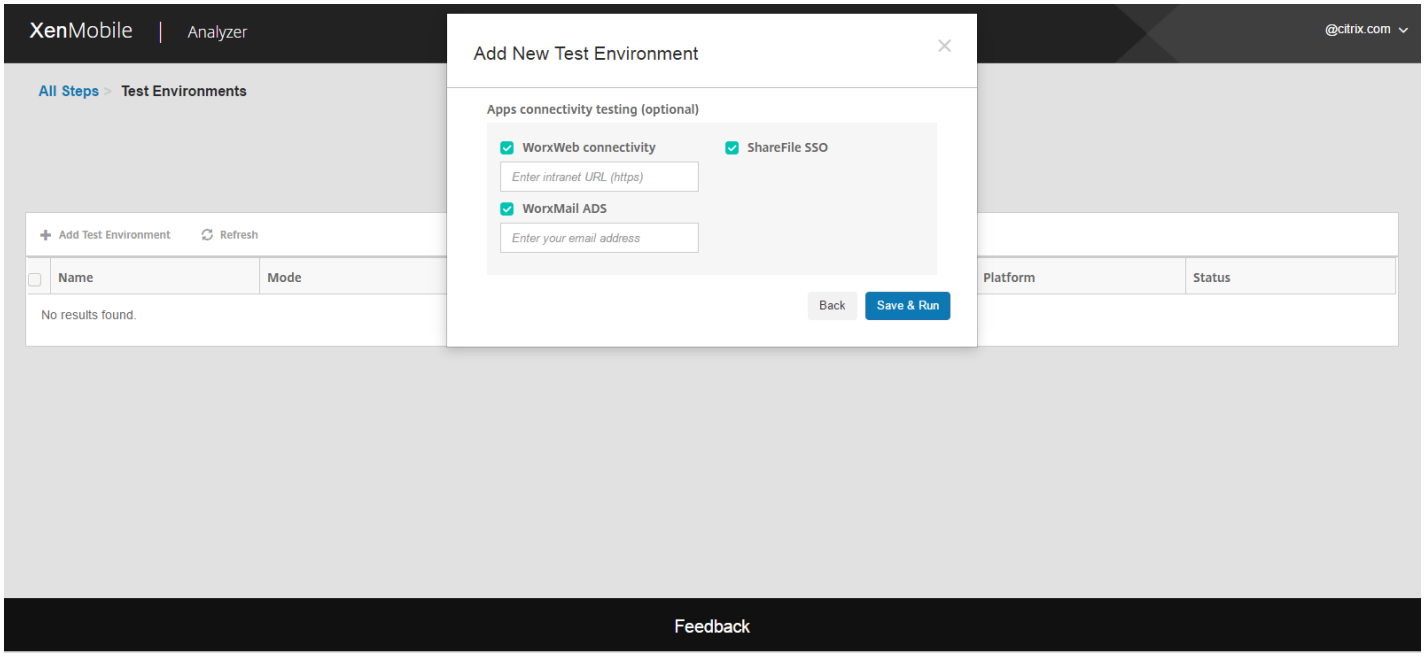
e. カスタムインスタンスを使用している場合は、**［Instance Name］**にその値を入力します。

f. **［Choose Platform］**で、テスト用のプラットフォームとして**iOS**または**Android**を選択します。

g. **［Username］**と**［Password］**に、認証に使用するユーザー名とパスワードを入力します。 環境で2要素認証用を構成している場合は、**［Two Factor Authentication］**チェックボックスをオンにして、2つ目のパスワードを入力します。



5. **［Continue］**をクリックします。



6. 実行するアプリケーションレベルのテストを選択します。 次のテストを選択できます（複数可）。

   a. WorxWeb Connectivity： イントラネットのURLを指定します。 ツールにより、入力したURLの到達可能性がテストされます。 このテストでは、イントラネットのURLへの接続時にWorxWebアプリで生じる可能性のある、接続に関する問題が検出されます。

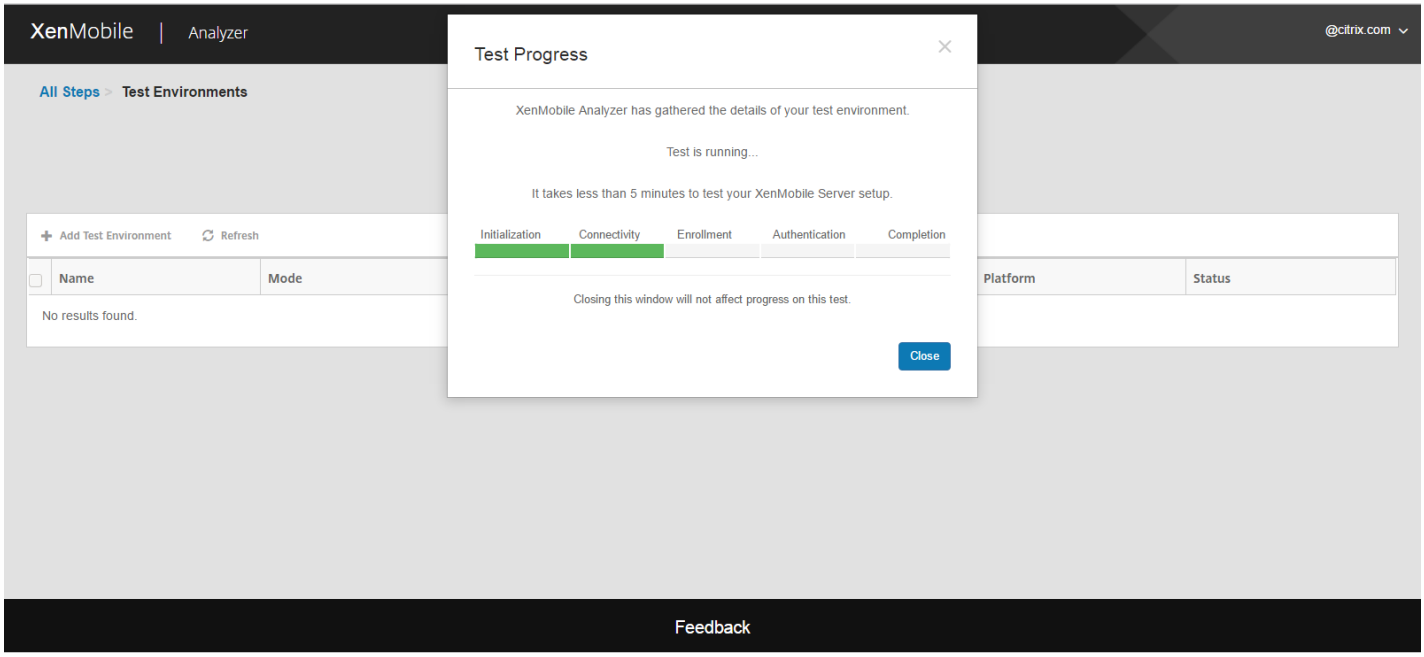
   b. WorxMail ADS： ユーザーの電子メールIDを指定します。 このIDを使用して、XenMobile環境にあるMicrosoft Exchange Serverの自動検出機能がテストされます。 WorxMail Auto Discovery関連の問題があるかどうかが検出されます。

   c. ShareFile SSO： このテストを選択した場合、ShareFileのDNS解決が正常に行われるかどうか、および指定したユーザー資格情報でShareFileシングルサインオン（SSO）を行うことができるかどうかがテストされます。

7. **[Save & Run]** をクリックしてテストを開始します。

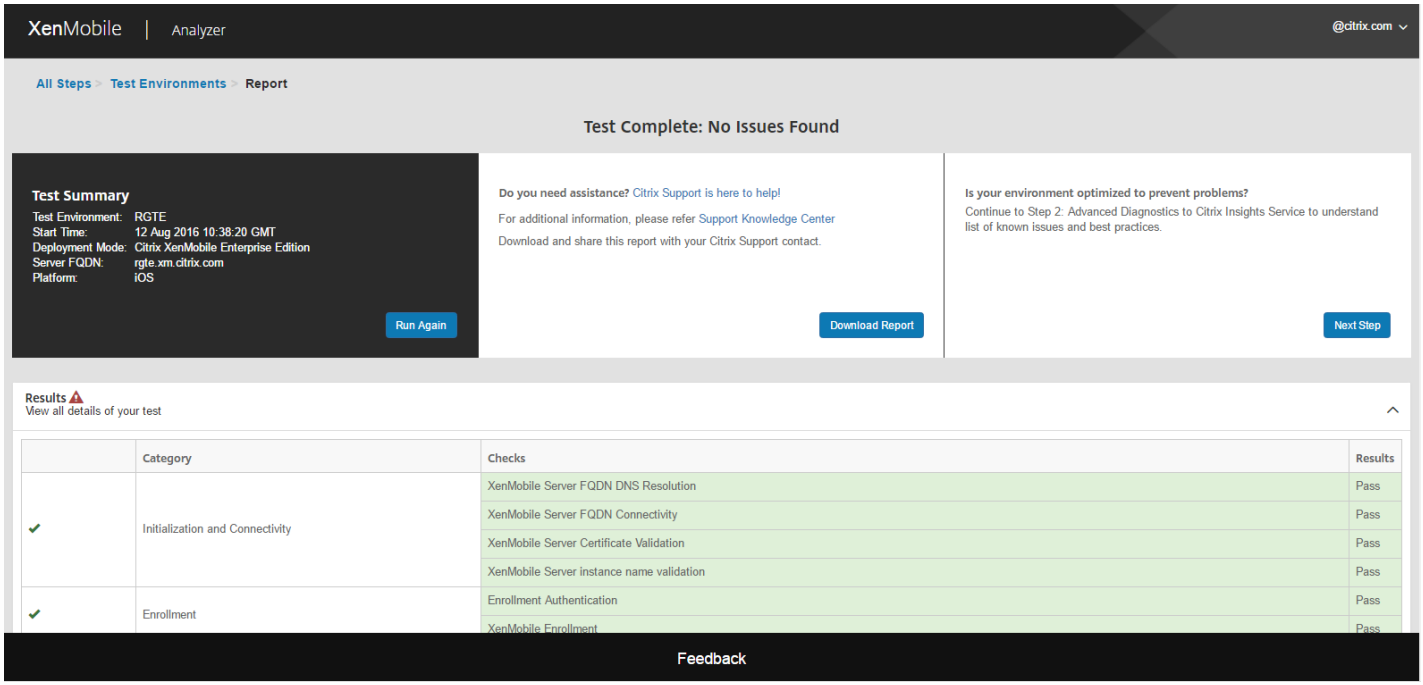
進行状況が表示されます。 この進行状況を示すダイアログボックスは開いたままにしても、閉じても構いません。どちらの場合でもテストは続行されます。

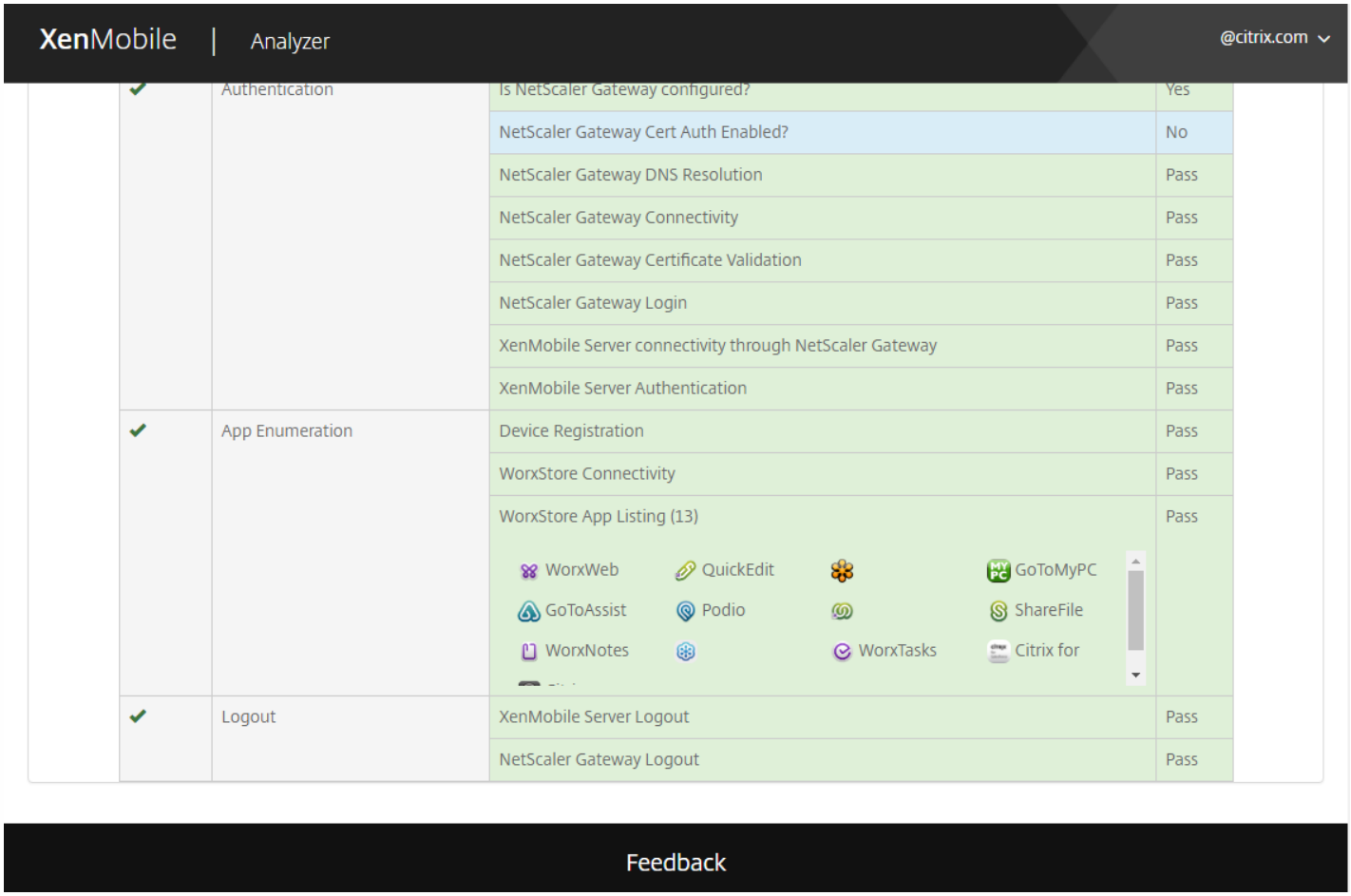
問題なく完了したテストは緑色で表示されます。 失敗したテストは赤色で表示されます。



8. 進行状況を示すダイアログボックスを閉じた後、**[Test Environments List]** ページに戻って **[View Report]** アイコンをクリックすると、テスト結果を確認することができます。

   [Results] ページには、テストの詳細、推奨項目、結果が表示されます。





Citrix Knowledge Baseの記事に関連する推奨事項がある場合は、該当の記事がこのページに一覧表示されます。

9. **[Results]** タブをクリックすると、個別のカテゴリーとツールが実行したテストが、結果とともに表示されます。

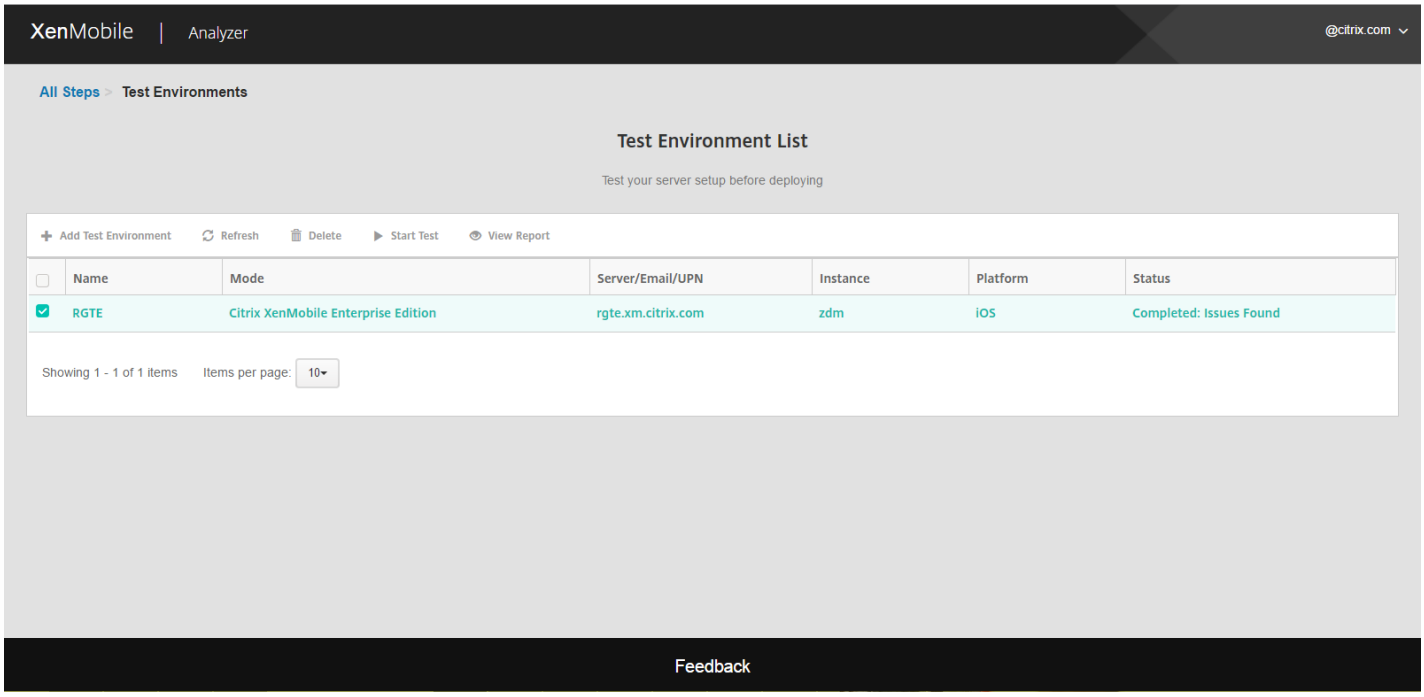
a. レポートをダウンロードするには、［**Download Report**］をクリックします。

b. テスト環境の一覧に戻るには、［**Test Environments**］をクリックします。

c. 同じテストをもう一度実行するには、［**Run Again**］をクリックします。

d. 別のテストをもう一度実行するには、［**Test Environments**］に戻って再実行するテストを選択し、［**Start Test**］をクリックします。

e. XenMobile Analyzerの次のステップに進むには、［**Next Step**］をクリックします。



XenMobile Analyzerの手順2～5の実行

XenMobile Analyzerの環境チェック手順では直接操作してテストを実行しますが、手順2～5では役立つ情報が提供されます。これらの各手順では、XenMobile環境を正しく設定するために使用できる他のツールに関する情報が提供されます。

- **手順 2 - Advanced Diagnostics**：この手順では、環境に関する情報を収集して、Citrix Insight Servicesにアップロードします。 このツールによってデータが分析され、環境に合ったレポートが推奨される解決方法とともに提供されます。
- **手順 3 - WorxMail Readiness**：この手順では、Worx Exchange ActiveSync Testアプリケーションをダウンロードして実行します。 このアプリケーションでは、XenMobile環境への展開についてのActiveSyncサーバーのトラブルシューティングを行います。 アプリケーションを実行した後に、レポートを確認したり他のユーザーと共有したりできます。
- **手順 4 - Server Connectivity Checks**：この手順では、XenMobileサーバー、認証サーバー、およびShareFileサーバーへの接続を確認するための手順が示されます。
- **手順 5 - Contact Citrix Support**：他のすべての手順が失敗した場合は、Citrixサポートでサポートチケットを作成できます。

既知の問題

XenMobile Analyzerに関する既知の問題は次のとおりです。

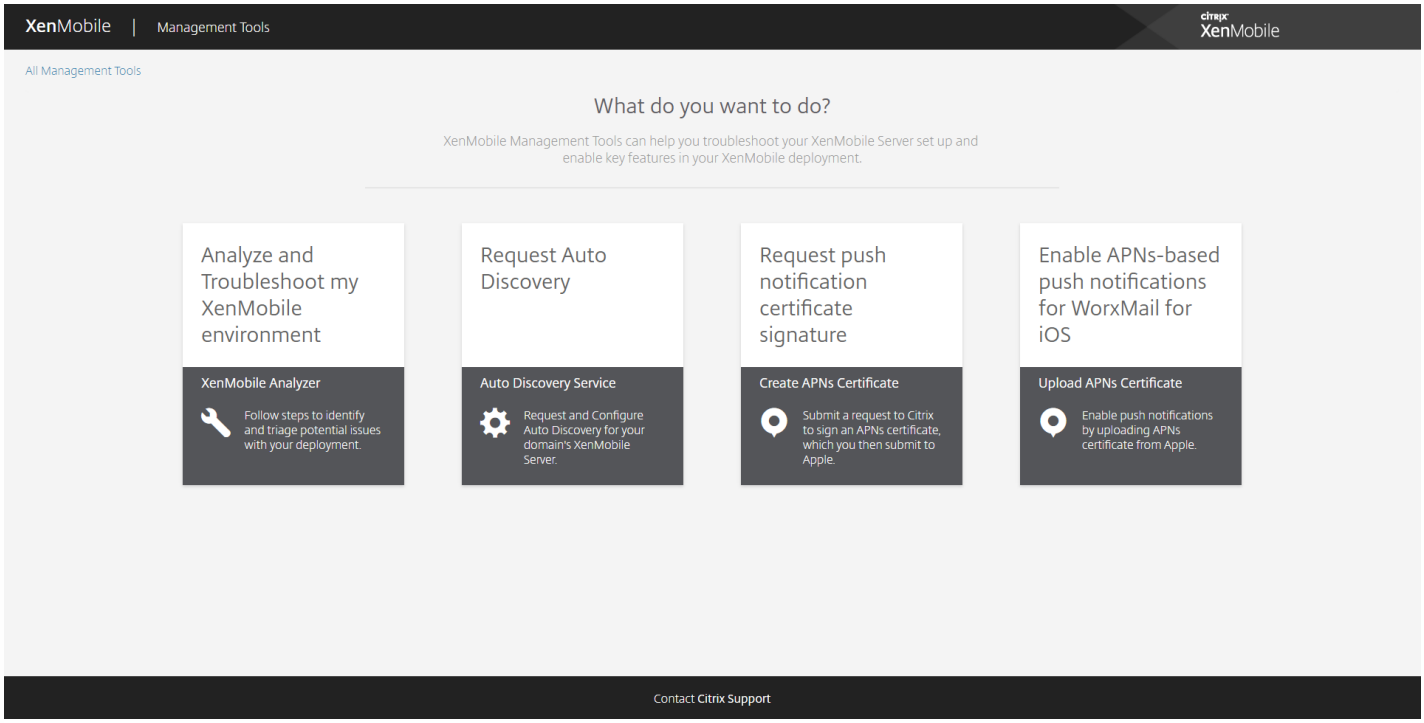
- XenMobile Serverにプラットフォーム制限ポリシーが設定されている場合、一覧に記載されるアプリの数は、クライアントに応じて異なることがあります。
- WorxWebのイントラネット接続に関するチェックを実行する場合、テキストボックスに複数のURLを入力することはできません。
- WorxHomeの共有デバイス認証機能は使用できません。

XenMobile AutoDiscoveryサービス

Aug 02, 2016

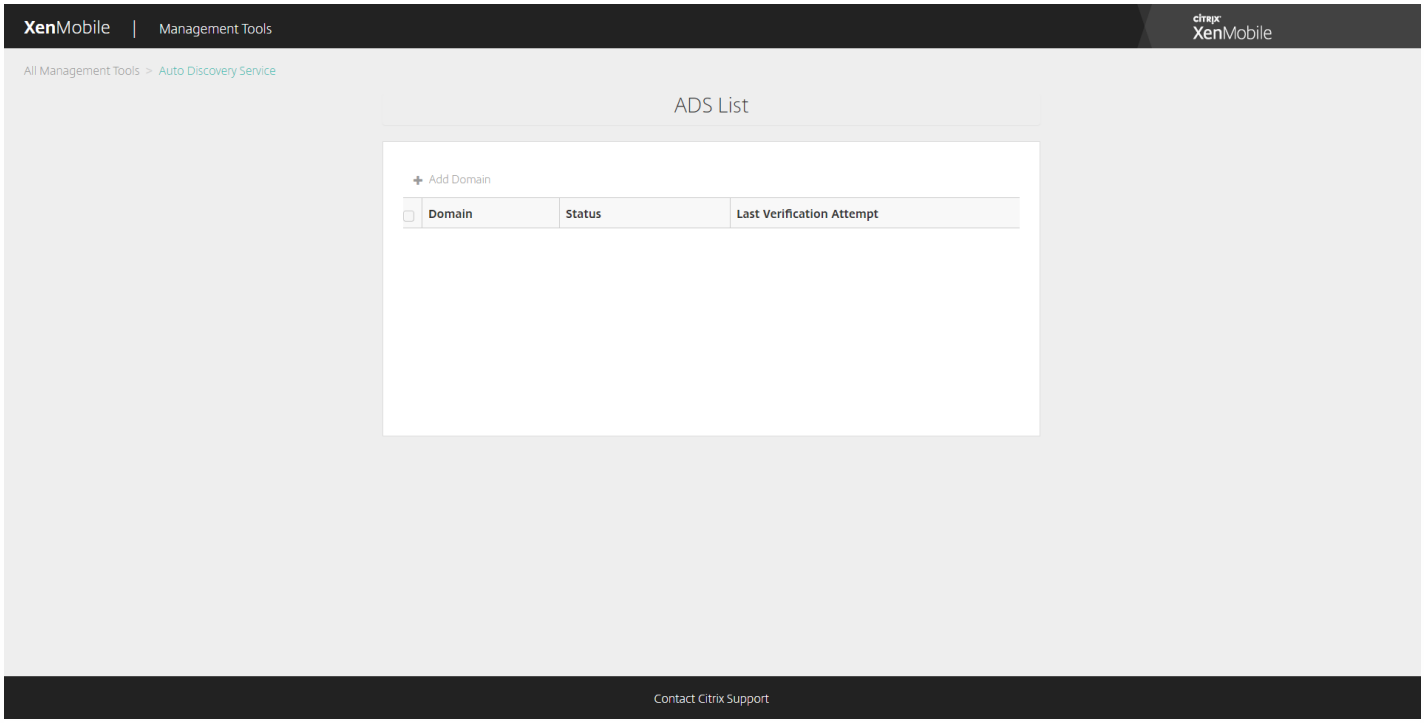
多くのXenMobile展開にとって、自動検出は重要な要素となります。 自動検出を使用するとユーザーの登録処理が簡単になります。 ユーザーは、ネットワークユーザー名とActive Directoryパスワードを使用してデバイスを登録できます。XenMobileサーバーの詳細を入力する必要はありません。 ユーザーは、ユーザー名をユーザープリンシパル名（User Principal Name：UPN）形式で入力します（たとえば、user@mycompany.com）。 XenMobile AutoDiscoveryサービスを使用すると、Citrixサポートの補助を受けずに自動検出レコードを作成または編集できます。

XenMobile AutoDiscoveryサービスにアクセスするには、https://xenmobiletools.citrix.comに移動して［**Request Auto Discovery**］をクリックします。

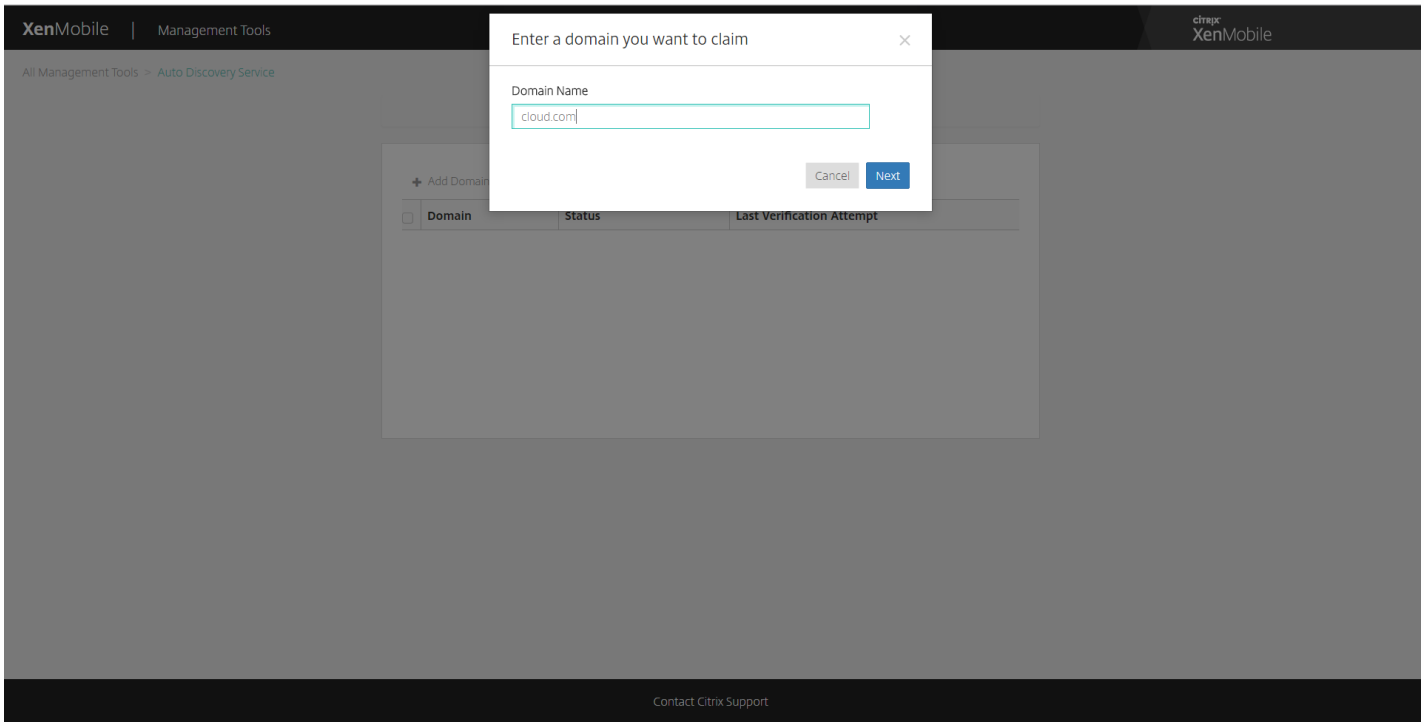


AutoDiscoveryのリクエスト

1. AutoDiscoveryサービスのページでは、まずドメインを指定する必要があります。［**Add Domain**］をクリックします。



2. 表示されたダイアログボックスで、お使いのXenMobile環境のドメイン名を入力してから[**Next**]をクリックします。



3. 次の手順では、ユーザーがドメインの所有者であることを確認するための手順が示されます。

a. XenMobileツールポータルで提供されたDNSトークンをコピーします。

b. ドメインホスティングプロバイダーポータルで、ドメインのゾーンファイルにDNS TXTレコードを作成します。

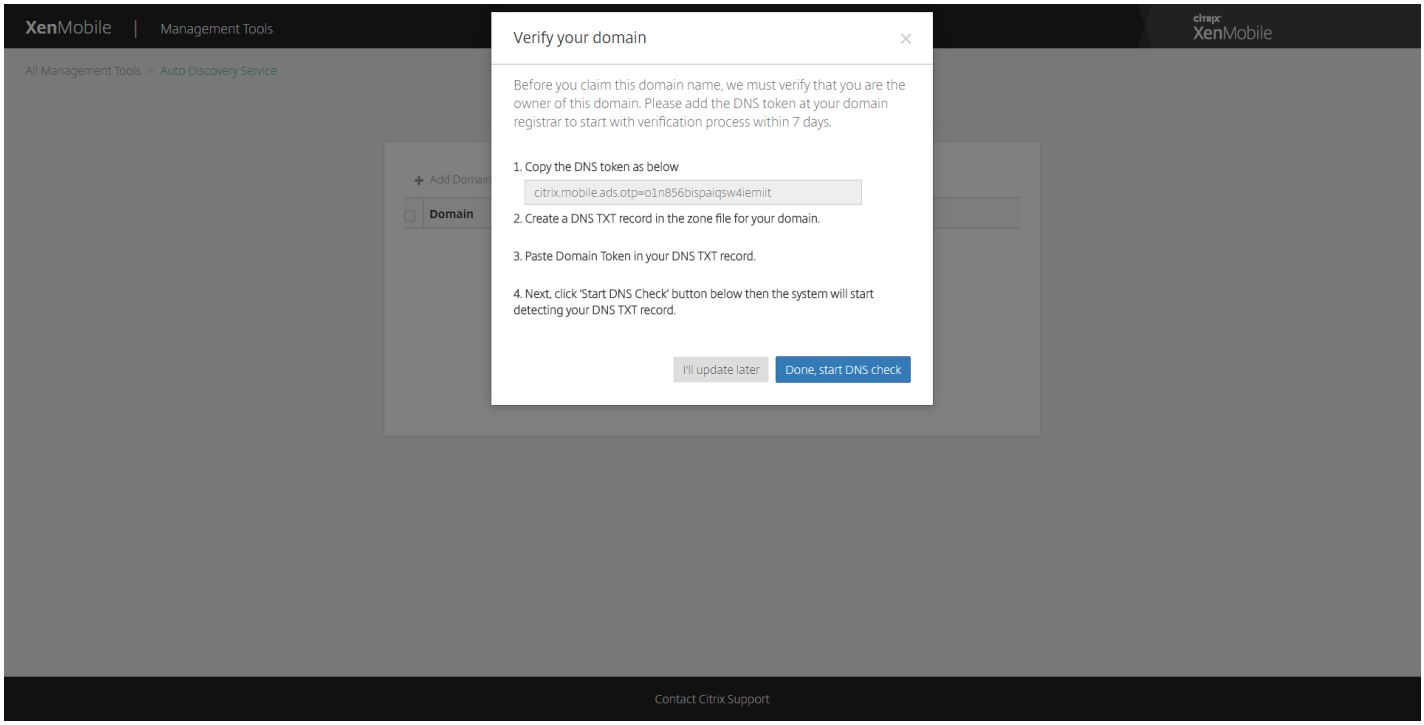
DNS TXTレコードを作成するには、上の手順2で追加したドメインのドメインホスティングプロバイダーポータルにログインする必要があります。 ドメインホスティングポータルでは、ドメインネームサーバーレコードを編集したり、カスタムのTXTレコードを追加したりできます。 サンプルドメインdomain.comのホスティングポータルでのDNS TXTエントリの追加の例。

c. DNS TXTレコードにドメイントークンを貼り付け、ドメインネームサーバーレコードを保存します。

d. XenMobileツールポータルに戻って［Done］をクリックし、DNSチェックを開始します。

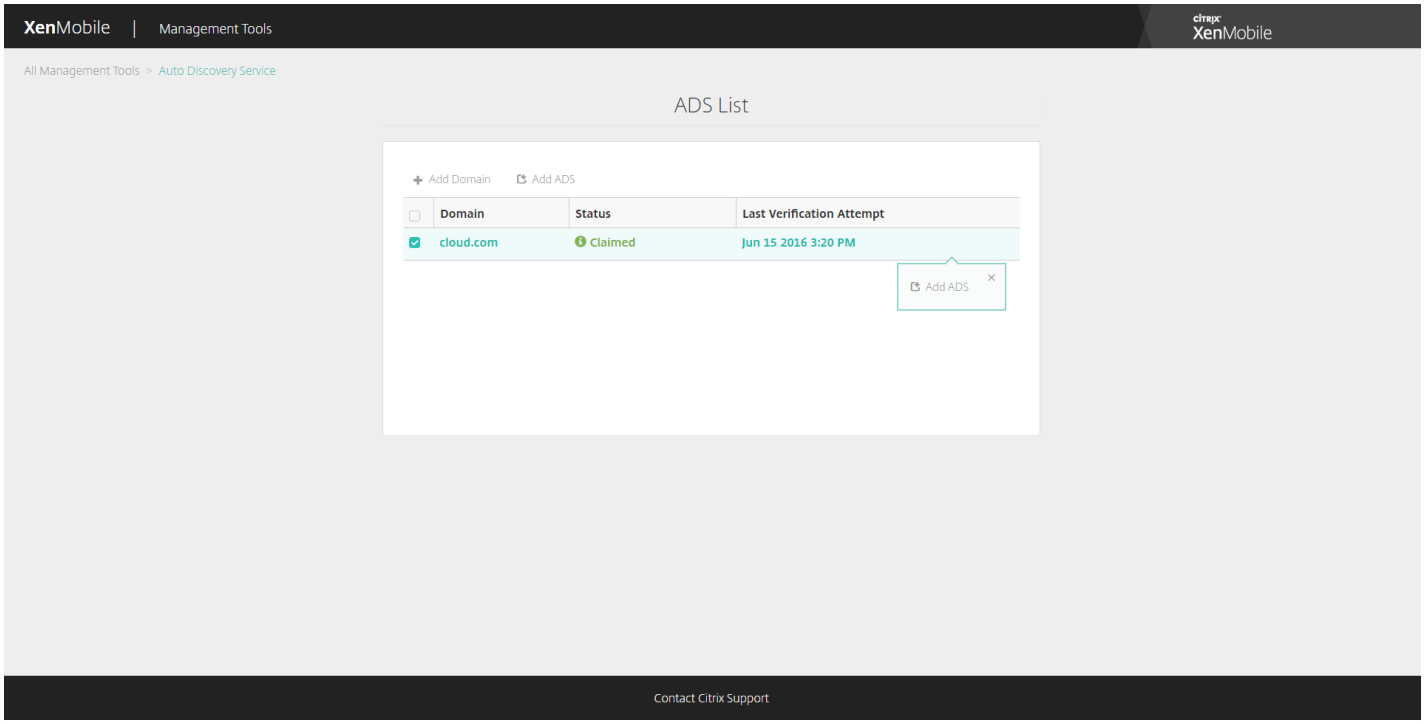
作成したDNS TXTレコードが検出されます。 または、［I'll update later］をクリックして、レコードを保存することもできます。 ［Waiting］レコードを選択して［DNS Check］をクリックするまで、DNSチェックは開始されません。

このチェックにかかる時間は最短で約1時間ですが、応答が返されるまでに最大2日かかることがあります。 さらに、ステータスの変更を確認するには、ポータルを閉じてから再びアクセスする必要がある場合もあります。

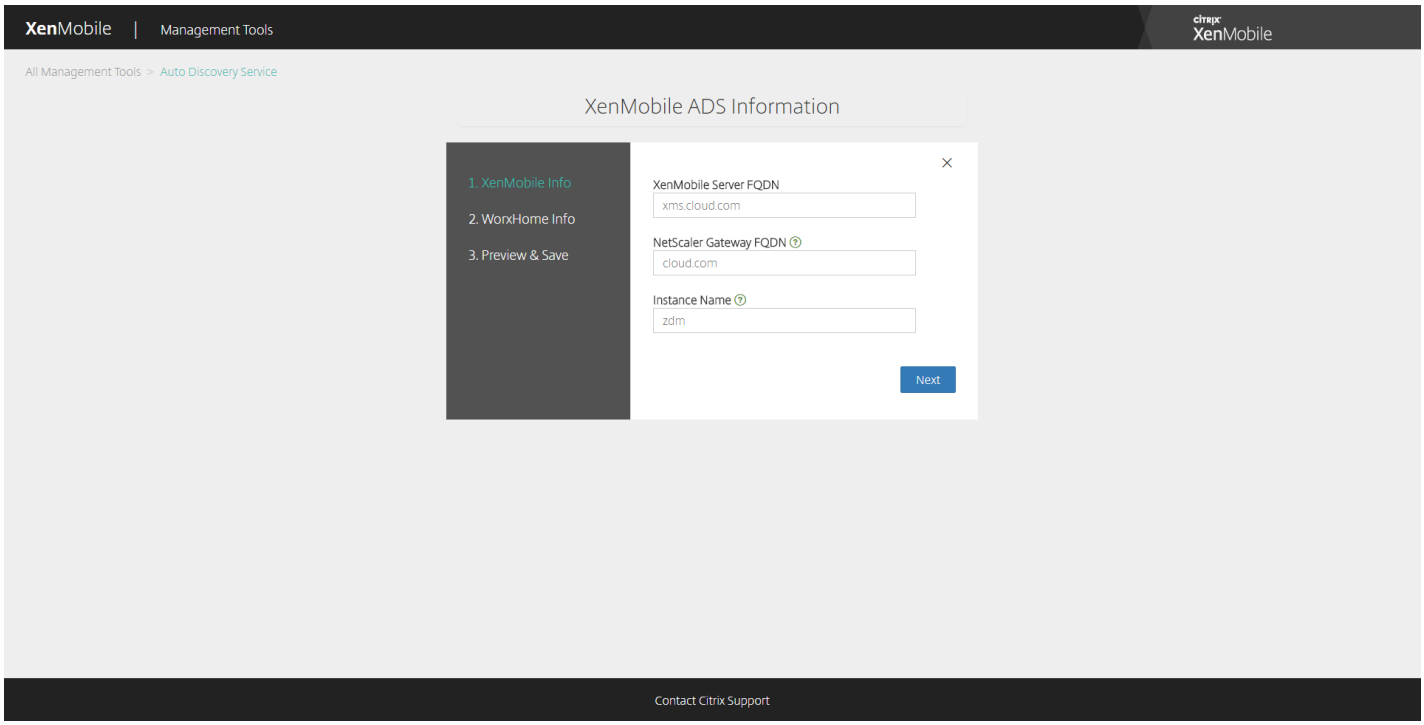


4. ドメインを指定すると、AutoDiscoveryサービス情報を入力できるようになります。 自動検出をリクエストするドメインレコードを右クリックしてから、 **［Add ADS］**をクリックします。

ドメインにすでにAutoDiscoveryレコードがある場合、Citrixテクニカルサポートに事例を記録して、必要に応じて詳細を変更します。



5. **XenMobileサーバーの完全修飾ドメイン名**、**NetScaler Gatewayの完全修飾ドメイン名**、および**インスタンス名**を入力して、［**Next**］をクリックします。 不明な場合、デフォルトインスタンスの「zdm」を追加します。



6. Worx Homeに次の情報を入力して、［**Next**］をクリックします。

a. **User ID Type**：ユーザーが**電子メールアドレス**または**UPN**でサインオンするIDのタイプを選択します。

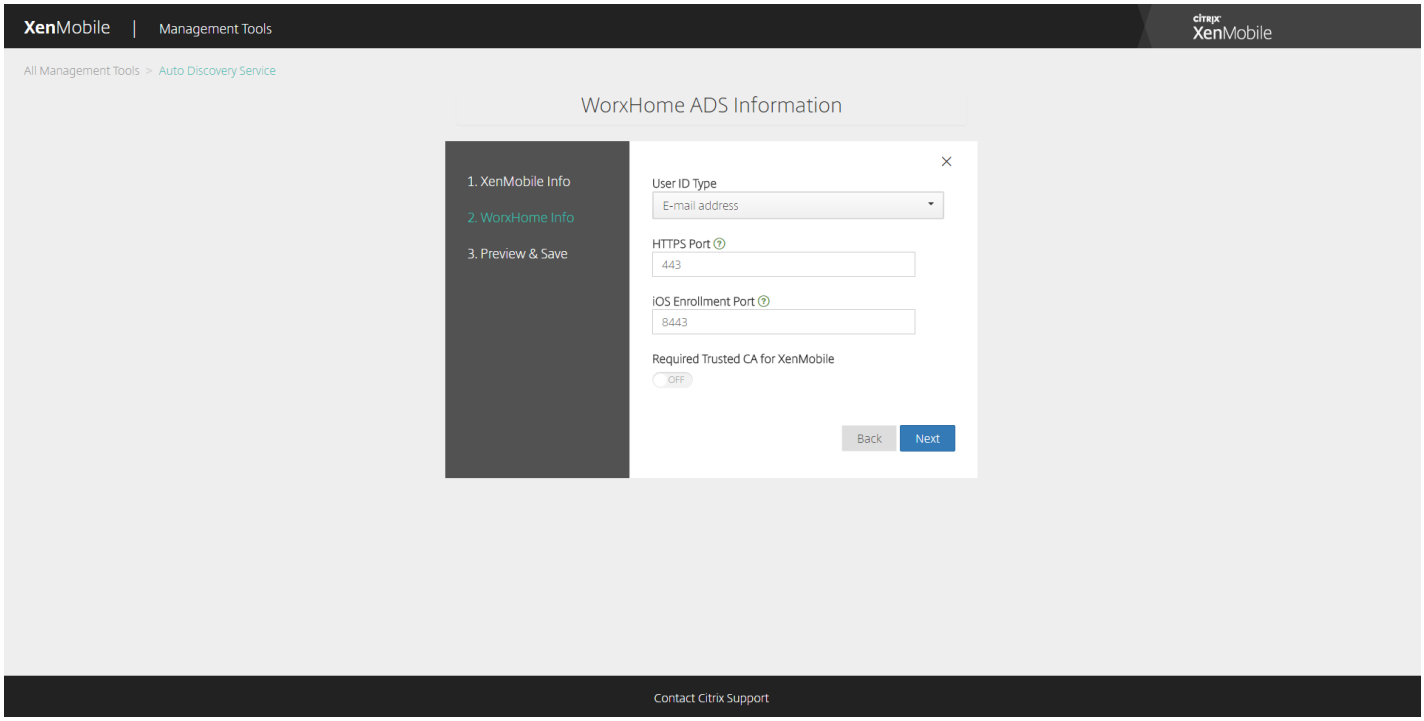
UPNは、ユーザーのUPN（ユーザープリンシパル名）がメールアドレスと同じである場合に使用されます。 どち

らの方法も、サーバーアドレスを検出するために入力したドメインを使用します。 **メールアドレス**の場合、ユーザーはユーザー名とパスワードを入力するよう求められます。**UPN**の場合はパスワードを入力するよう求められます。

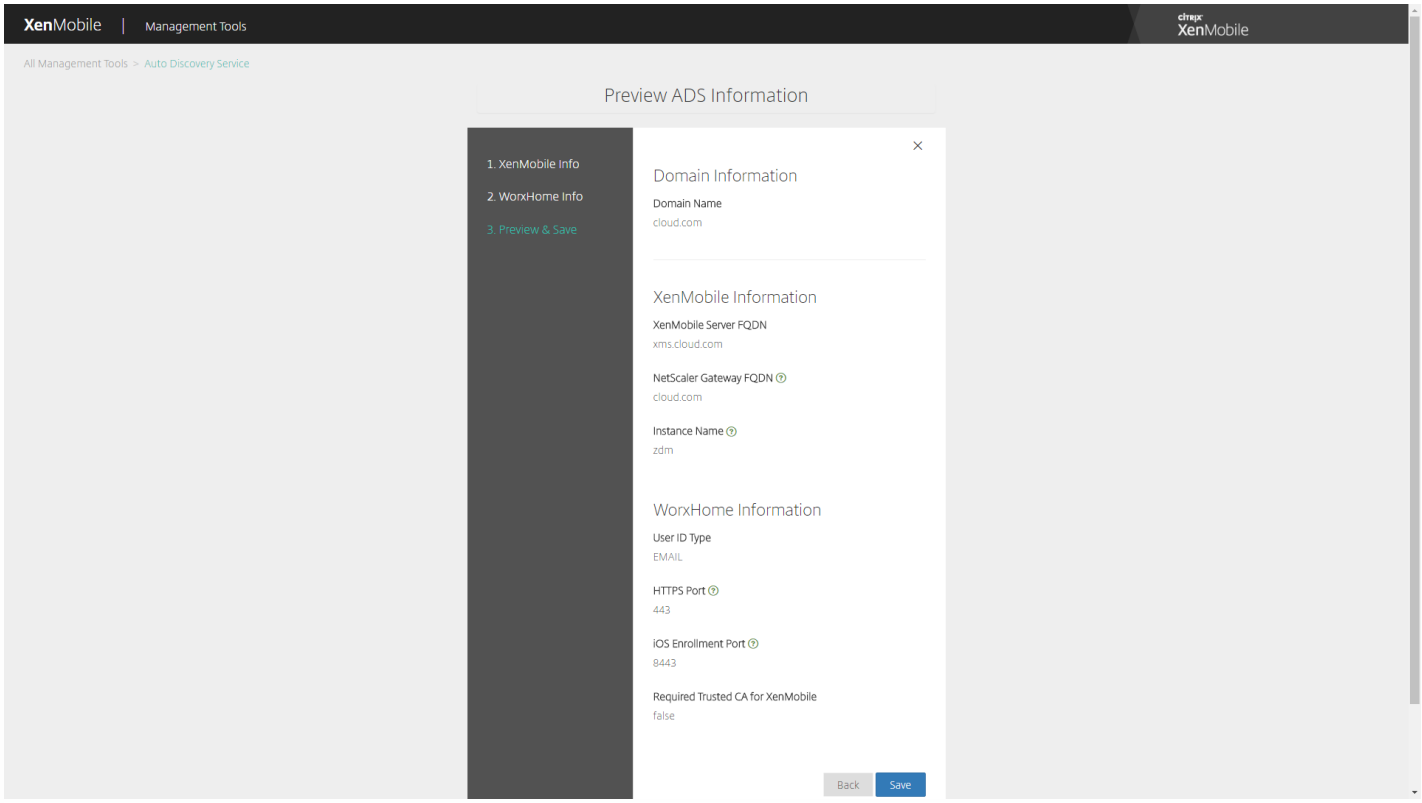
b. **HTTPS Port**：HTTPSでWorx Homeサーバーにアクセスするときに使用するポートを入力します。 通常、これはポート443です。

c. **iOS Enrollment Port**：iOS登録時にWorx Homeへのアクセスに使用するポートを入力します。 通常、これはポート8443です。

d. **Required Trusted CA for XenMobile**：XenMobileへのアクセスで信頼された機関からの証明書が必要かどうかを指定します。 このオプションは、必要に応じて **[OFF]** または **[ON]** にできます。 現時点では、この機能のために証明書をアップロードすることはできません。 この機能を使用する場合は、Citrixサポートに電話して自動検出のセットアップを依頼する必要があります。 証明書ピン留めについて詳しくは、Worx Homeトピックの、証明書ピン留めについてのセクションを参照してください。 証明書ピン留めが機能するために必要なポートについては、「XenMobile Port Requirements for ADS Connectivity」のサポート記事を参照してください。



7. 概要ページに、これまでの手順で入力したすべての情報が表示されます。 データが正しいことを確認し、**[Save]** をクリックします。



XenMobile REST APIリファレンス

Aug 02, 2016

XenMobile REST APIにより、 XenMobileコンソールで公開されるサービスを呼び出すことができます。 RESTクライアントを 使用して、RESTサービスを呼び出すことができます。 APIについて、サービスを呼び出すためにXenMobileコンソールにサインオンする必要はありません。

現在使用できるAPIの完全な一覧については、XenMobile REST APIリファレンスのPDFファイルをダウンロードしてください。 この記事には、APIの完全なセットは含まれません。

REST APIへのアクセスに必要な権限

REST APIにアクセスするには、次の権限 のうち1つが必要です。

- 役割ベースのアクセス構成の一部として設定されたパブリックAPIアクセス権限（役割ベースのアクセスの設定について詳しくは、「 RBACを使用した役割の構成」を参照してください）
- スーパーユーザー権限

REST APIサービスを呼び出すには

RESTクライアントまたはCURLコマンドを使用して、REST APIサービスを呼び出すことができます。 以下の例では、Advanced REST client for Chromeを使用します。

> **注意**
>
> 以下の例のホスト名とポート番号は、自分の環境に合わせて変更してください。

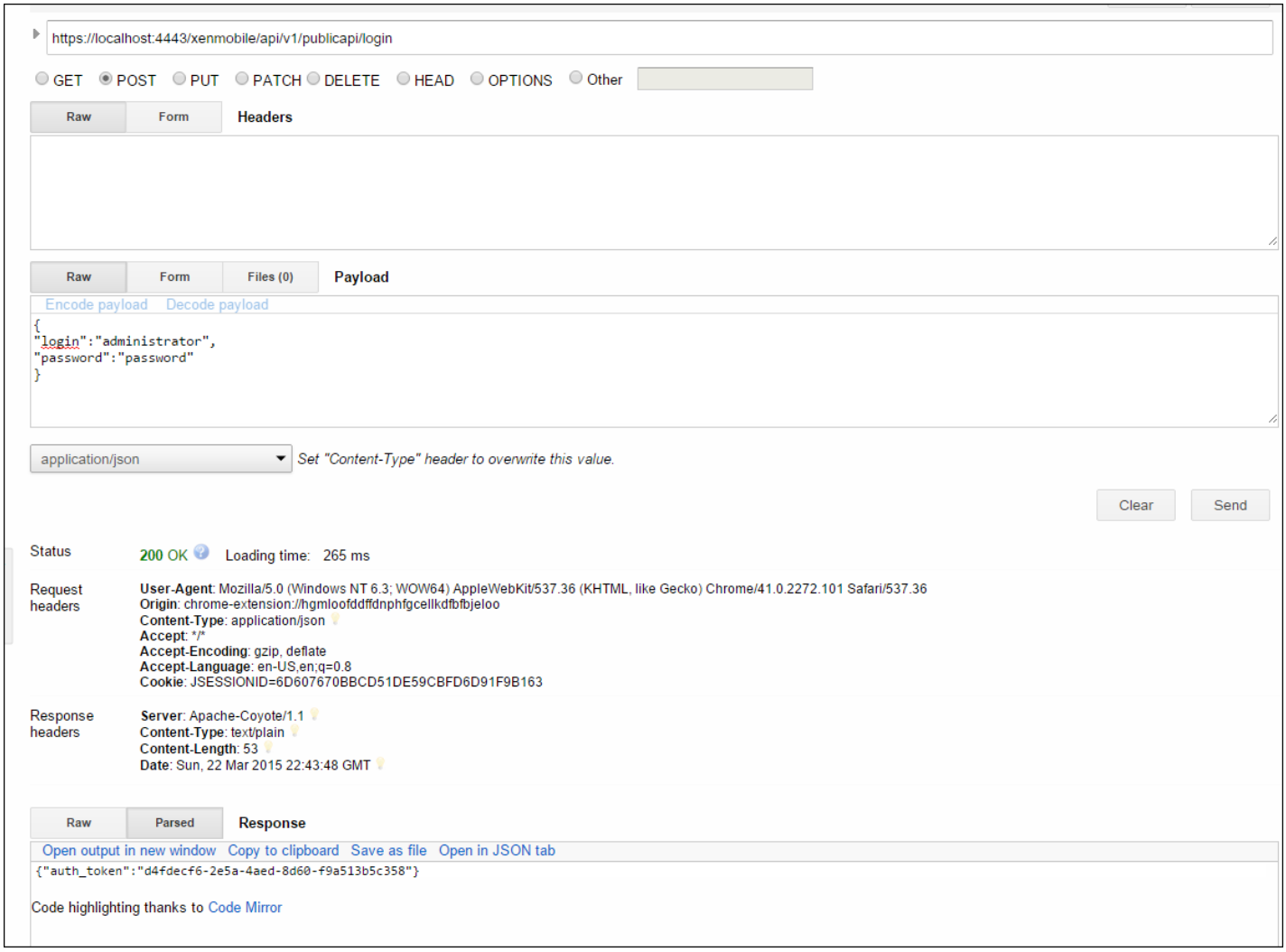
Login

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/authentication/login

Request: { "login":"administrator", "password":"password" }

Method type: POST

Content type: application/json



Get Delivery Groups by filter

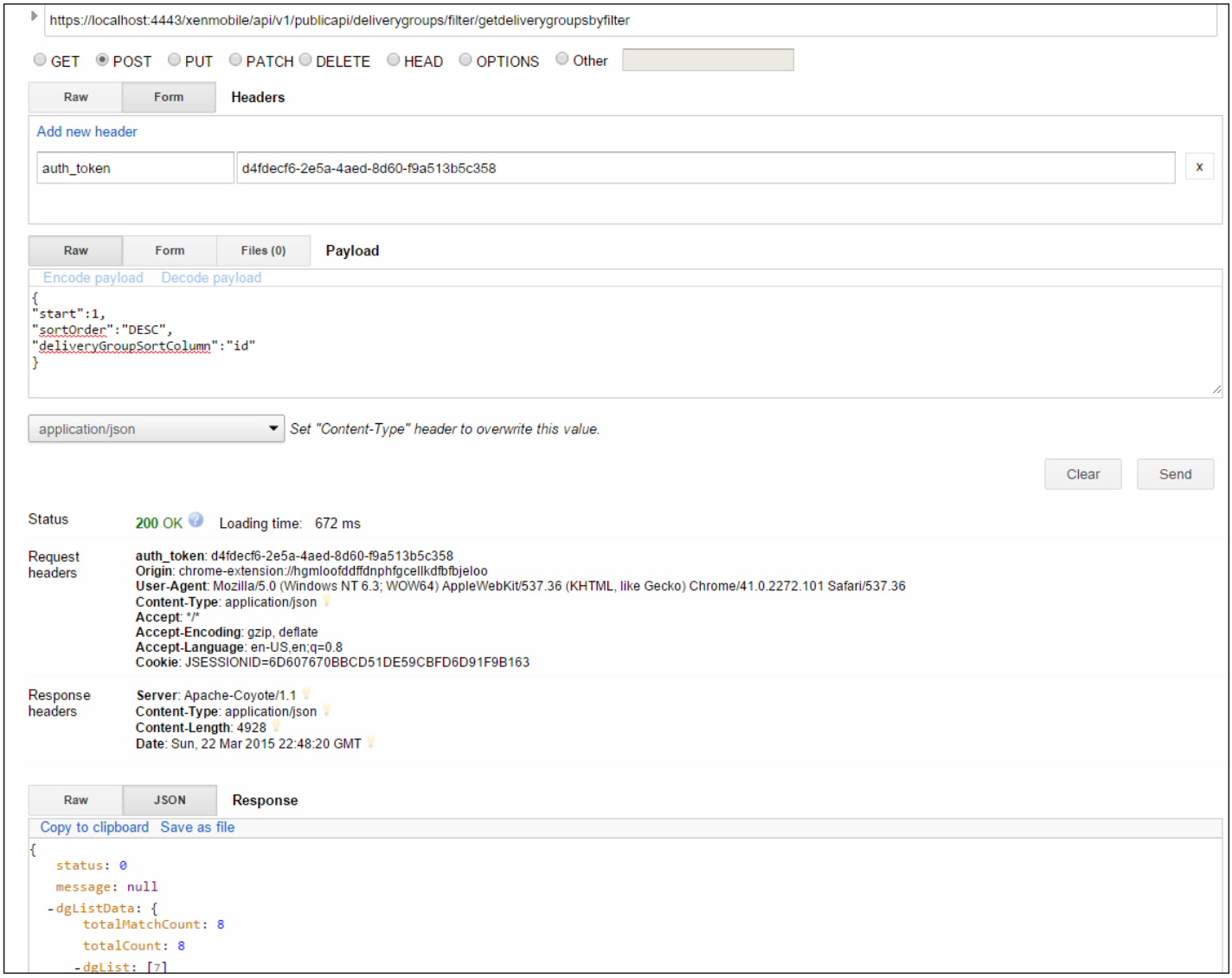
URL: /xenmobile/api/v1/deliverygroups/filter

Request コピー

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

    "search":"add"

}
```

Method type: POST

Content type: application/json



REST APIの定義

以降のセクションで、このPDFに記載されている一部のAPIについて説明します。 完全なAPIの文書については、PDFを参照してください。

必ず、以下の例のホスト名とポート番号は、自分の環境に合わせて変更してください。

パブリックAPIにログオンするには

ユーザーの資格情報を受け入れ、既存のAuthenticationManagerを使ってユーザーを認証します。 AuthenticationManagerが初めてユーザーを認証する場合、要求ヘッダーに置かれる認証トークンが生成されます。

URL：https://<ホスト名>:4443/xenmobile/api/v1/authentication/login

リクエストの種類：POST

リクエストパラメーター コピー

```
{ "login":"administrator", "password":"password" }
```

応答例 コピー

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

CWCを介してパブリックAPIにログオンするには

ユーザーの資格情報を受け入れ、既存のAuthenticationManagerを使ってユーザーを認証します。 AuthenticationManagerが初めてユーザーを認証する場合、要求ヘッダーに置かれる認証トークンが生成されます。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/authentication/cwclogin

リクエストの種類：POST

リクエストヘッダー：認証 – CWSAuth service=<サービスキー>

リクエストパラメーター コピー

```
{“context”:”customer or cloud”, “customerId”:”customer ID”}
```

応答例 コピー

```
{

    "auth-token":"authentication token"

}
```

パブリックAPIからログアウトするには

ユーザーがログオンして現在のユーザーをログアウトした時に発行される認証トークンを削除します。 ユーザー名と認証トークンが必要です。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/authentication/logout

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

リクエストパラメーター コピー

```
{“login”:”administrator”}
```

応答例 コピー

```
{"Status":"user administrator logged out successfully."}
```

証明書を管理するには

証明書管理操作により、パブリックAPIを介して証明書を表示、削除、インポート、および追加できます。

Get all certificates

データベースのすべての証明書を返します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

リクエストパラメーター：なし

応答例 コピー


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
                "signatureAlgo": "SHA1WithRSAEncryption",
```



```
"version": null,

"serialNum": "348237881800118418457268346483687164l3",

"issuerName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,

    "state": null,

    "country": null,

    "description": null

},

"subjectName": {

    "certString": "DC=com,DC=example,CN=ent-root-ca",

    "emailAddress": null,

    "commonName": "ent-root-ca",

    "orgUnit": null,

    "org": null,

    "locality": null,
```



```
                    "state": null,

                    "country": null,

                    "description": null

                }

            }

        }

    ],

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Delete certificates

特定の証明書を削除します。 削除される各証明書の証明書IDが必要です。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/publicapi/certificates

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

リクエストパラメーター コピー

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Import certificate as SAML certificate

SAML証明書として指定の証明書をインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/certificate/saml

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'saml',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Import certificate as server certificate

サーバー証明書として指定の証明書をインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/certificate/server

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Import certificate as listener certificate

SSLリスナー証明書として指定の証明書をインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/certificate/listener

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'listener',
    'keystoreType':'PKCS12',
    'uploadType':'certificate',
    'description':'test description'
}
uploadFile = <the actual file to be uploaded>
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Create certificate

自己署名証明書またはCA署名が必要なCSR要求を作成します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/csr

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Application/form_url_encoded

リクエストパラメーター コピー

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```

応答例 コピー

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Export certificate

指定の証明書をダウンロードします。 次の表に、この操作を行うパラメーターを示します。

パラメーター	必須	説明
id	はい	数字で表した証明書ID

password	エクスポートされている証明書に割り当てられたパスワード。
exportPrivateKey	プライベートキーをエクスポートするかどうかを示すフラグ。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/export

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "id": "300",

    "password": "1111",

    "exportPrivateKey": true

}
```

応答例：成功した要求に証明書文字列を表示します。

キーストアを管理するには

パブリックAPIを介してキーストアをインポートできます。

サーバーキーストアのインポート

サーバーキーストアをインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/keystore/server

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


SAMLキーストアのインポート

SAMLキーストアをインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/keystore/saml

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'keystore',

    'description':'test description'

}

    uploadFile = <certificate file>

    uploadFile = <private key file>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


APNsキーストアのインポート

APNSキーストアをインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/keystore/apns

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':apns,

    'keystoreType':'PKCS12',

    'uploadType':'keystore',

    'description':'test description'

    }

uploadFile = <certificate file>

uploadFile = <private key file>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

                "topicNameMismatch": false,

                "certExpired": false,

                "certNotYetValid": false,

                "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

          "topicNameMismatch": false,

          "certExpired": false,

          "certNotYetValid": false,

          "malformed": false

    }

}
```


SSLリスナーキーストアのインポート

SSLキーストアをインポートします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/certificates/import/keystore/listener

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター コピー

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

          "topicNameMismatch": false,

          "certExpired": false,

          "certNotYetValid": false,

          "malformed": false

    },

"certificate": null,

"apnsCheckObj": {

          "topicNameMismatch": false,

          "certExpired": false,

          "certNotYetValid": false,

          "malformed": false

    }

}
```


ライセンスを管理するには

パブリックAPIを介してライセンスを管理できます

Get license information

すべてのライセンスに関する情報を一覧表示します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー


```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
```



```
        licenseList: []

    {

        sadate: "2015.1210"

        notice: "Example Systems Inc."

        vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"

        licensesInUse: 0

        licensesAvailable: 102

        overdraftLicenseCount: 2

        p_E_M: "CXM_ENTU_UD"

        serialNumber: "cxmretailent1000user"

        licenseType: "Retail"

        expirationDate: "01-DEC-2015"

    }

    licenseNotification:

    {

        id: 1

        notificationEnabled: false

        notifyFrequency: 7

        notifyNumberDaysBeforeExpire: 60

        recepientList: ""
```

```
            emailContent: "License expiry notice"

        }

    }

}
```

ライセンス情報の保存

すべてのライセンス情報を保存します。

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,
```

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success"
}
```

ライセンスファイルのアップロード

指定のライセンスファイルをアップロードします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses/upload

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – Multipart/form-data

リクエストパラメーター：uploadFile =

応答例 コピー

```
{
   "status": 0,
   "message": "Success"
}
```

Activate license

指定のライセンスをアクティブにします。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses/activate/{license type}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター：アクティブ化したライセンスURLにライセンスの種類を追加します。

応答例 コピー

```
{

    "status": 0,

    "message": "Success"

    "cpLicenseServer": null

}
```

すべてのライセンスの削除

すべてのライセンスを削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses/remove

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "isConnected": null

}
```

Test license server

ライセンスサーバーで接続性チェックを実行します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses/testserver/

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "serverAddress": "192.0.2.7",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": null,

    "licenseType": null,

    "isServerConfigured": null,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": null,

    "isScheduleNotificationNeeded": null,

    "licenseList": [],

    "licenseNotification": null

}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "isConnected": true
}
```

Get earliest expiration date

有効期限が最も早いライセンスを検索します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/licenses/getexpirationdate

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "expiredDate": 1448956800000,

    "daysBeforeExpire": 229,

    "daysInPOC": 0

}
```

LDAP構成を管理するには

次の表は、LDAP構成操作で使用するパラメーターの一覧です。

パラメーター	必須	説明
primaryHost	はい	プライマリLDAPサーバーのIPアドレスまたはホスト名。 IPアドレスまたはFQDNとして入力します。
secondaryHost	いいえ	セカンダリLDAPサーバーのIPアドレスまたはホスト名。 IPアドレスまたはFQDNとして入力します。
port	はい	LDAPサーバーのポート番号
username	はい	有効なLDAPサーバーのユーザー名
password	はい	ユーザー名のパスワード
userBaseDN	はい	
lockoutLimit	いいえ	

lockoutTime	いいえ	
useSecure	いいえ	
userSearchBy	はい	UPNまたはsamaccountでユーザーを検索
domain	はい	一意のLDAPサーバーのドメイン名
domainAlias	はい	LDAPドメインのエイリアス
globalCatalogPort	いいえ	
gcRootContext	いいえ	
groupBaseDN	はい	
isDefault	いいえ	LDAP構成がデフォルトかどうかを示すGET応答の一部。
名	いいえ	LDAP構成の更新または削除に使用される一意なIDであるGET応答の一部。

List LDAP configuration

XenMobileのLDAP構成全体を一覧で表示します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/ldap

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userBa

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","use

    ]

}
```

Add new LDAP configuration

新しいLDAP王政を追加します。 ドメイン名は一意である必要があり、ほかのLDAP構成と同じものにはできません。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/msactivedirector

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

応答例 コピー

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Edit LDAP configuration

既存のLDAP構成を編集します。ただし、編集操作でドメインを変更することはできません。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/msactivedirector/{name}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Set default LDAP configuration

指定のLDAP構成をデフォルトとして設定します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/default/{name}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Delete LDAP configuration

指定のLDAP構成を削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/ldap/{name}

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

NetScaler Gateway構成を管理するには

NetScaler Gateway構成を管理できます。 次の表は、NetScaler Gateway操作で使用するパラメーターの一覧です。

パラメーター	必須	説明
名	はい	一意のNetScaler Gateway名
alias	いいえ	
url	はい	NetScaler Gatewayの公然とアクセス可能なURL
passwordRequired	はい	
logonType	はい	有効な値：domain-only、domain-token、domain-certificate、certificate-only、certificate-token、token-only
callback	いいえ	
で	はい	NetScaler Gateway構成を追加または編集する場合にtrueまたはfalseに設定します。 このパラメーターが渡されない場合、デフォルトはfalseに設定されます。
id	いいえ	NetScaler Gateway構成の更新または削除に使用される一意なIDであるGET応答の一部。

List all NetScaler Gateway configurations

XenMobileのNetScaler Gateway構成全体を一覧で表示します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/netscaler

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",
```

```
            "logonType":"domain",

            "default":"false",

            "id":"",

            “callback”: [{“callbackUrl”:http://example.com,

            “ip”:”192.0.2.8”}]

            }

      ]

}
```

Add new NetScaler Gateway configuration

新しいNetScaler Gateway構成を追加します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/netscaler

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Edit NetScaler Gateway configuration

指定のNetScaler Gateway構成を編集します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/netscaler/{id}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain",

    "default": true,

    "callback": [{"callbackUrl":http://ag.com,

    "ip":"192.0.2.8"}]

}
```

Delete NetScaler Gateway configuration

指定のNetScaler Gateway構成を削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/netscaler/{id}

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Set default NetScaler configuration

指定のNetScaler Gateway構成をデフォルトとして設定します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/netscaler/default/{id}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

SMSおよびSMTP通知サーバー構成を管理するには

SMSサーバーおよびSMTPサーバーの構成を追加、編集、アクティブ化（デフォルトとして設定）、および削除できます。次の表は、SMSサーバーおよびSMTPサーバー構成の操作で使用するパラメーターの一覧です。

パラメーター	必須	説明
名	はい	一意のSMS/SMTP構成名です。
serverType	いいえ	GETリクエストのサーバーにより送信された通知サーバーの種類（SMSまたはSMTP）
active	いいえ	サーバーが通知に使用されているかどうかを示します。 種類ごとに1つのサーバーだけをアクティブにできます。
id	いいえ	サーバーの更新、削除、またはアクティブ化に使用される一意のID。
description	いいえ	サーバーの説明。
SMSパラメーター		
key	はい	
secret	はい	
virtualPhoneNumber	はい	電話番号形式である必要があります。
https	はい	デフォルトはfalse。
country	はい	
carrierGateway	はい	デフォルトはfalse。
SMTPパラメーター		
secureChannelProtocol	はい	使用するセキュリティプロトコルの種類です。 有効な値：None、SSL、TLS。 デフォルトはNoneです。
port	はい	

authentication	はい	認証を使用するかどうか指定します。 有効な値は、trueおよびfalseです。
username	認証がtrueの場合は、はい。	
password	認証がtrueの場合は、はい。	
msSecurePasswordAuth	はい	デフォルトはfalse。
fromName	はい	
fromEmail	はい	
numOfRetries	いいえ	整数。 デフォルトは5です。
timeout	いいえ	整数。 デフォルトは30です。
maxRecipients	いいえ	整数。 デフォルトは100です。

List all SMS and SMTP servers

XenMobileのすべてのSMSおよびSMTPサーバーを一覧で表示します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Accept – application/json

応答例 コピー

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Get server details

サーバーIDによりサーバーに関する詳細を取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/{id}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Accept – application/json

SMS応答の例 コピー

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

SMTP応答の例 コピー

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Add SMS server configuration

SMSサーバー構成を追加します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/sms

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Edit SMS server configuration

指定のSMSサーバー構成を編集します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/sms/{id}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "name":"displayName",
    "description":"",
    "server":"192.0.2.9",
    "carrierGateway":"true",
    "country":"+93",
    "https":"false”,
    “key”: “123456”,
    "secret":"secretKey",
    "virtualPhoneNumber":"4085552222",
    "carrierGateway":"true"
}
```

Add SMTP server configuration

SMTPサーバー構成を追加します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/smtp

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Edit SMTP configuration

指定のSMTP構成を編集します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/smtp/{id}

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Delete server configuration

指定のSMSまたはSMTPサーバー構成を削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/{id}

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Set default SMS configuration

指定のSMSサーバー構成をデフォルトとして設定します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/activate/sms/{id}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Set default SMTP configuration

指定のSMTPサーバー構成をデフォルトとして設定します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/notificationserver/activate/smtp/{id}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

ローカルユーザーとグループを管理するには

次のサービスを使用すると、ローカルユーザーとグループを管理できます。

Get all users

すべてのローカルユーザーを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
    "status": 0
```

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }

]
```



```
    ]

}
```

Get one user

指定のローカルユーザーを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups/{name}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```

```
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

Add user

指定の属性のユーザーを追加します。

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
```

```
"user": {
    "userid": 0,
    "username": "justaname_XX",
    "password": "password",
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": null,
    "lastAuthenticated": null,
    "domainName": null,
    "adUser": false
```



```
        "vppUser": false
    }
}
```

Update user

ユーザー属性を更新します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
        },
    "groups": [
        "MSP"
        ],
    "role": "USER",
    "username": "justaname_XX",
    "password": "password"
}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
```

```
"message": "success",
"user": {
    "userid": 108,
    "username": "justaname_XX",
    "password": null,
    "confirmPassword": null,
    "groups": [
        "MSP"
    ],
    "attributes": {
        "badpwdcount": "4",
        "asuseremail": "justa.name@example.com",
        "company": "example",
        "mobile": "4695557854"
    },
    "role": "USER",
    "roles": null,
    "createdOn": "3/27/15 1:10 PM",
    "lastAuthenticated": "3/27/15 1:10 PM",
    "domainName": null,
    "adUser": false
```



```
        "vppUser": false
    }
}
```

Change user password

ユーザーのパスワードをリセットします。また、更新ローカルユーザー呼び出しでユーザーのパスワードを変更できます。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups/resetpassword

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "username": “administrator”,
    “password”: “newPassword”
}
```

応答例 コピー

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Delete users

指定のユーザーを削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups/resetpassword

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{ justaname XX }
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Delete one user

指定のユーザーを削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups/

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Import provisioning file

ローカルユーザーデータを含むファイルをアップロードします。 更新されるファイルは.csv形式である必要があります。 プロビジョニングファイルについて詳しくは、「プロビジョニングファイル形式」を参照してください。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/localusersgroups/importprovisioningfile

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

アプリを管理するには

以下のサービスを使用すると、アプリを管理できます。

Get all apps by filter

指定のフィルターパラメーターを元にアプリを取得します。

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/application/filter

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン
コンテンツの種類 – application/json

サンプル要求データ コピー

```
{
    "start": 0,
    "limit": 10,

    "applicationSortColumn": "name",
    "sortOrder": "DESC",
    "enableCount": false,
    "search": "Worx",
    "filterIds":"['application.deliverygroup#<DG_Name>@_fn_@app.dg','application.deliverygroup#<DG_Name>@_fn_@app.dg
}
```

サンプル応答データ コピー

```
{

  "status": 0,

  "message": "Success",

  "applicationListData": {

    "totalMatchCount": 2,

    "totalCount": 2,

    "appList": [{

      "id": 2,

      "name": "WorxNotes",

      "description": "Worx Notes Application",

      "createdOn": "6/7/16 3:55 PM",

      "lastUpdated": "6/7/16 5:11 PM",

      "disabled": false,

      "nbSuccess": 0,

      "nbFailure": 0,

      "nbPending": 0,

      "schedule": null,

      "permitAsRequired": true,

      "iconData": "iVBORw0KGgoAAAANSUhEUgAAAHgAAAB4CAYAAAA5ZDbSAAA.....",

      "appType": "MDX",
```



```
    "categories": ["Default"],
    "roles": null,
    "workflow": null,
    "vppAccount": null
  }, {
    "id": 1,
    "name": "Angry Bird",
    "description": "",
    "createdOn": "6/7/16 3:53 PM",
    "lastUpdated": "6/7/16 3:54 PM",
    "disabled": false,
    "nbSuccess": 0,
    "nbFailure": 0,
    "nbPending": 0,
    "schedule": null,
    "permitAsRequired": true,
    "iconData": "/9j/4AAQSkZJRgABAQEAAQABAAD/2wBDAAYEBQYFBAYGBQYHBwYIChA...",
    "appType": "App Store App",
    "categories": ["Default"],
    "roles": null,
```



```
        "workflow": null,
        "vppAccount": null
      }]
    }
}
```

Get mobile apps by container

指定のコンテナーのモバイルアプリを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/application/mobile/{containerId}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "result": {
        "id": 14,
        "name": "testApp",
        "description": "",
        "createdOn": null,
```

```
"lastUpdated": null,
"disabled": false,
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"schedule": {
    "enableDeployment": true,
    "deploySchedule": "NOW",
    "deployScheduleCondition": "EVERYTIME",
    "deployDate": null,
    "deployTime": null,
    "deployInBackground": false
},
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
"workflow": null,
```



```
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
    "rules": null,
    "appType": "mobile_ios",
    "uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
   "id": 0,
    "store": {
        "rating": {
            "rating": 0,
            "reviewerCount": 0
```



```
        },
        "screenshots": [],
        "faqs": [],
        "storeSettings": {
            "rate": true,
            "review": true
        }
    },
    "policies": [
        {
            "policyName": "ReauthenticationPeriod",
            "policyValue": "480",
            "policyType": "integer",
            "policyCategory": "Authentication",
            "title": "Reauthentication period (minutes)",
            "description": "\nDefines the period before a user is challenged to authenticate again. ",
            "units": "minutes",
            "explanation": null
        },
        {
```



```
                "policyName": "BlockJailbrokenDevices",

                "policyValue": "true",

                "policyType": "boolean",

                "policyCategory": "Device Security",

                "title": "Block jailbroken or rooted",

                "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",

                "units": null,

                "explanation": null

            },

            {

                "policyName": "CertificateLabel",

                "policyValue": "",

                "policyType": "string",

                "policyCategory": "Network Access",

                "title": "Certificate label",

                "description": "\nThe label for the certificate.\n                                                    Default value is em

                "units": null,

                "explanation": null

            }

        ]
```



```
        },
        "android": null,
        "android_knox": null,
        "android_work": null,
        "windows": null,
        "windows_tab": null
    }
}
```

Get public store apps by container

指定のコンテナーからパブリックストアアプリを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/application/mobile/appstore/{containerId}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

Delete app container

指定のアプリコンテナーを削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/application/{containerId}

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

デリバリーグループ構成を管理するには

以下のサービスを使用すると、デリバリーグループ構成を管理できます。

Get delivery groups by filter

指定のフィルターパラメーターを使ってデリバリーグループを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups/filter

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{

  "start": 1,

  "sortOrder": "DESC",

  "deliveryGroupSortColumn": "id",

  “limit”:10,

  "search": "add"

}
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "dgListData": {

        "totalMatchCount": 7,
```

```
"totalCount": 10,

"dgList": [

    {

        "id": null,

        "name": "add delivery group 6.0",

        "description": "testing add delivery group 6.0",

    "groups": [[{

            {

                "id": 1null,

        "userListId": 1null,

        "name": "MSPTESTLOCALGROUP",

        "uniqueName": "MSPTESTLOCALGROUP",

        "uniqueId": "MSPTESTLOCALGROUP",

        "domainName": "local",

        "primaryToken": 0null,

            }"objectSid": null

        ],},

    {

        "id": null,

        "userListId": null,
```



```
        "name": "AC08EP61S75",
        "uniqueName": "AC08EP61S75",
        "uniqueId": "AC08EP61S75",
        "domainName": "local",
        "primaryToken": null,
        "objectSid": null
    }],
    "users": [{
        "uniqueName": null,
        "domainName": "local",
        "name": null,
        "objectId": "shankar",
        "customProperties": {
            "name": "value",
            "name1": "value1"
        },
        "uniqueId": "shankar"
    }],
        "zoneId": null,
        "zoneDomain": null,
```



```
"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\

"disabled": false,

"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

      {

            "name": "Web Link",

            "required": false

      },

      {

            "name": "GoogleApps_SAML",

            "required": true

      }

],

"devicePolicies": [

      "test terms conditions"

],

"smartActions": [

      "shankar ganesh"
```



```
        ],
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    },
    {
        "id": null,
        "name": "add delivery group 5.0",
        "description": "testing add delivery group 5.0",
        "groups": [
            {
                "id": 1,
                "userListId": 1,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
                "domainName": "local",
                "primaryToken": 0
            }
        ],
```



```
"zoneId": null,

"zoneDomain": null,

"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\

"disabled": false,

"lastUpdated": 1426891345698,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

      {

            "name": "GoogleApps_SAML",

            "required": true

      },

      {

            "name": "Web Link",

            "required": false

      }

],

"devicePolicies": [

      "test terms conditions"

],
```



```
                    ],
                    "smartActions": [
                        "shankar ganesh"
                    ],
                    "nbSuccess": 0,
                    "nbFailure": 0,
                    "nbPending": 0
                }
            ]
        }

}
```

Get delivery group by name

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups/{name}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
```

```
"role": {
    "id": null,
    "name": "AllUsers",
    "description": "default role",
    "groups": [],
    "zoneId": null,
    "zoneDomain": null,
    "rules": null,
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": false,
    "roledefLangVersionId": 1,
    "applications": [
        {
            "name": "test mdx",
            "required": false
        },
        {
            "name": "test all",
            "required": false
```



```
        },
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
    "smartActions": [
        "justa name"
    ],
```



```
        "nbSuccess": 0,
        "nbFailure": 0,
        "nbPending": 0
    }
}
```

Edit delivery group

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{
   "name": "temp3",
   "description": "temp3 desc",
   "applications": [
{
            "name": "TESTAPP",
             "priority": -1,
             "required": false
```

```
            "required" : false

                    }     ],

    "devicePolicies": [

        {

            "name":"test terms conditions",

            "priority":-1

         }

      ],

    "smartActions": [

        {

           "name":"Smart Action Name 1",

           "priority":-1

         }

      ],

  "groups": [

     {

  "uniqueName": "AC08EP61S75",

        "domainName": "local",

        "name": "AC08EP61S75",

        "objectSid": "AC08EP61S75",

"uniqueId": "AC08EP61S75",

"customProperties": {

     "gr1": "gr1",

     "gr2": "gr2"
```



```
    }

      }

    ],

    "users": [

      {

        "uniqueName": "testuser",

        "domainName": "local",

        "name": " testuser ",

        "objectId": " testuser "

      }

    ],

    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" tes

}
```

応答例 コピー

```
{

    "status": 0,
```

```
        "message": "Success",

"role": {

            "id": null,

            "name": "temp4",

            "description": "temp4 desc",

            "zoneId": null,

            "zoneDomain": null,

            "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\

            "disabled": false,

            "lastUpdated": null,

            "anonymousUser": false,

            "roledefLangVersionId": null,

            "applications": [

                {

                "name": "TESTAPP2",

                "priority": -1,

                "required": false

            },

{

                "name": "TESTAPP2",
```



```
                "priority": -1,

                "required": false

            }

            ],

            "devicePolicies": [

                {

                "name": "TestPolicy1",

                "priority": -1

            },

{

                "name": "TestPolicy",

                "priority": -1

            }

            ],

            "smartActions": [

{

                "name": "TestAction2",

                "priority": -1

            },

{
```

```
            "name": "TestAction3",

            "priority": -1

        }

    ],

        "nbSuccess": 0,

        "nbFailure": 0,

        "nbPending": 0,

        "groups": [{

              "uniqueName": "AC08EP61S75",

             "domainName": "local",

            "name": "AC08EP61S75",

             "objectSid": "AC08EP61S75",

            "uniqueId": "AC08EP61S75",

            "customProperties": {

              "gr1": "gr1",

                "gr2": "gr2"

             }

        }],

        "users": [{

            "uniqueName": " tempuser ",
```



```
                "domainName": "local",

                "name": " tempuser ",

                "objectId": " tempuser ",

                "customProperties": null,

                "uniqueId": " tempuser "

        }]


    }
```

Add delivery group

デリバリーグループを追加します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{

  "name": "temp3",

  "description": "temp3 desc",

  "applications": [

{
```

```
            "name": "TESTAPP",
            "priority": -1,
            "required": false
                    }      ],
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
      ],
    "smartActions": [
        {
           "name":"Smart Action Name 1",
           "priority":-1
        }
      ],
   "groups": [
     {
  "uniqueName": "AC08EP61S75",
        "domainName": "local",
        "name": "AC08EP61S75",
        "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
```

```
"customProperties": {
      "gr1": "gr1",
      "gr2": "gr2"
    }}
    ],
    "users": [
      {
        "uniqueName": "testuser",
        "domainName": "local",
        "name": " testuser ",
        "objectId": " testuser "
      }
    ],
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\" tes
}
```

応答例 コピー

```
{
      "status": 0,
      "message": "Success",
```

```
"role": {
        "id": null,
        "name": "temp4",
        "description": "temp4 desc",
        "zoneId": null,
        "zoneDomain": null,
        "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\
        "disabled": false,
        "lastUpdated": null,
        "anonymousUser": false,
        "roledefLangVersionId": null,
        "applications": [
            {
            "name": "TESTAPP2",
            "priority": -1,
            "required": false
         },
{
            "name": "TESTAPP2",
            "priority": -1,
```



```
                "required": false
            }
            ],
            "devicePolicies": [
                {
                "name": "TestPolicy1",
                "priority": -1
            },
{
                "name": "TestPolicy",
                "priority": -1
            }
            ],
            "smartActions": [
{
                "name": "TestAction2",
                "priority": -1
            },
{
                "name": "TestAction3",
```



```
                "priority": -1
            }
        ],
            "nbSuccess": 0,
            "nbFailure": 0,
            "nbPending": 0,
            "groups": [{
                "uniqueName": "AC08EP61S75",
          "domainName": "local",
          "name": "AC08EP61S75",
          "objectSid": "AC08EP61S75",
"uniqueId": "AC08EP61S75",
"customProperties": {
      "gr1": "gr1",
      "gr2": "gr2"
   }         }],
            "users": [{
                "uniqueName": " tempuser ",
                "domainName": "local",
                "name": " tempuser ",
```



```
                "name": "tempuser",

                "objectId": "tempuser",

                "customProperties": null,

                "uniqueId": "tempuser"

            }]


    }
```

Delete delivery group

指定のデリバリーグループを削除します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups

リクエストの種類：DELETE

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
[ "add delivery group 11.0" ]
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "roleNames": [

        "add delivery group 11.0"

    ]

}
```

Enable or Disable Delivery Group

指定のデリバリーグループを有効化または無効化します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/deliverygroups/{delivery group name}/{enable/disable}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "roleName": "AllUsers"

}
```

サーバープロパティを管理するには

以下のサービスを使用すると、XenMobileサーバープロパティを管理できます。

Get all server properties

すべての現在のXenMobileサーバーのプロパティを取得できます。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 1,

            "name": "ios.mdm.pki.ca-root.certificatefile",
```

```
        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",

        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,

        "markDeleted": false
```



```
        },
        {
            "id": 3,
            "name": "ios.mdm.enrolment.checkRemoteAddress",
            "value": "false",
            "displayName": "iOS Device Management Enrollment - Check Remote Address",
            "description": "",
            "defaultValue": "false",
            "displayFlag": true,
            "editFlag": true,
            "deleteFlag": false,
            "markDeleted": false
        },
    ]
}
```


Get server properties by filter

指定のフィルターパラメーターを使ってサーバープロパティを取得します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties/filter

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "start": 0,

    "limit": 1000,

    "orderBy": "name",

    "sortOrder": "desc",

    "searchStr": "justaserver1"

}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "allEwProperties": [
        {
            "id": 154,
            "name": "justaserver123",
            "value": "justaserver1",
            "displayName": "justarserver display name",
            "description": "justaserver description",
            "defaultValue": "justaserver1",
            "displayFlag": true,
            "editFlag": true,
            "deleteFlag": true,
            "markDeleted": false
        }
    ]
}
```


Add server property

指定のサーバープロパティを追加します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "name": "Key 2",

    "value": "Value 1",

    "displayName": "Display Name 1",

    "description": "Description 1"

}
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Edit server properties

指定のサーバープロパティを編集します。

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Reset server properties

指定のサーバープロパティをリセットします。

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties/reset

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{

    "names": [,

        "justaname7"

        ]

}
```

応答例 コピー

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Delete server properties

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/serverproperties

リクエストの種類 : DELETE

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエストパラメーター コピー

```
{
    "justaname3",
    "justaname4"
}
```

応答例 コピー

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

デバイスを管理するには

以下のサービスを使用すると、XenMobileでデバイスを管理できます。

Get Devices by Filter

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/filter

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リスエストパラメーターはすべて任意です。

sortOrderの有効な値は、ASC、DSC、およびDESCです。

sortColumnの有効な値は、ID、SERIAL、IMEI、ACTIVESYNCID、WIFIMAC、BLUETOOTHMAC、OSFAMILY、SYSTEM_OEM、SYSTEM_PLATFORM、SYSTEM_OS_VERSION、DEVICE_PROPERTY、LASTAUTHDATE、INACTIVITYDAYS、ISACTIVE、LASTUSER、BLCOMPLIANT、WLCOMPLIANT、RLCOMPLIANT、MANAGED、SHAREABLE、およびBULKPROFILESTATUSです。

リクエストパラメーター コピー

```
{

   "start": "0-999",

   "limit": "0-999",

   "sortOrder": "ASC",

   "sortColumn": "ID",

   "search": "Any search term",

   "enableCount": "false",

   "constraints": "{'constraintList':[{'constraint':'DEVICE_OS_FAMILY','parameters':[{'name':'osFamily','type':'STRING','value':'iOS

   "filterIds": "['group#/group/MSP@_fn_@normal']"

}
```

応答例 コピー

```
{

   "id": "1-9999999",

   "jailBroken": "true/false",
```

```
"managed": "true/false",

"gatewayBlocked": "true/false",

"deployFailed": "1-999",

"deployPending": "1-999",

"deploySuccess": "1-999",

"mdmKnown": "true/false",

"mamRegistered": "true/false",

"mamKnown": "true/false",

"userName": "user name",

"serialNumber": "serial number",

"imeiOrMeid": "IMEI/MEID",

"activeSyncId": "Active sync ID",

"wifiMacAddress": "WiFi MAC address",

"blueToothMacAccress": "Bluetoothi MAC address",

"devicePlatform": "Device platform",

"osVersion": "Operating system version of the device",

"deviceModel": "Device model information",

"lastAccess": "Timestamp when the device was last accessed",

"inactivityDays": "Number of days device has been inactive",

"shareable": "Flag indicating if the device is shareable",
```

```
    "sharedStatus": "Get shareable status of the device",

    "depRegistered": "Flag indicating if the device is DEP registered",

    "deviceName": "Name of the device",

    "deviceType": "Phone/Tablet",

    "productName": "Product name",

    "platform": "Platform of the device"

}
```

Get Devices by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "device": {

  "htcMdm": true,

  "managedByZMSP": true,

  "serialNumber": "string",

  "id": 0,
```

```
"applications": [
 {
  "resourceType": "APP_NATIVE",
  "resourceTypeLabel": "string",
  "packageInfo": "string",
  "statusLabel": "string",
  "lastUpdate": 0,
  "status": "SUCCESS",
  "name": "string"
 }
],
"smartActions": [
 {
  "resourceType": "APP_NATIVE",
  "resourceTypeLabel": "string",
  "packageInfo": "string",
  "statusLabel": "string",
  "lastUpdate": 0,
  "status": "SUCCESS",
  "name": "string"
```



```
  }
],
"platform": "string",
"osFamily": "WINDOWS",
"nbSuccess": 0,
"nbFailure": 0,
"nbPending": 0,
"deliveryGroups": [
  {
    "statusLabel": "string",
    "linkey": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
  }
],
"lastAuthDate": 0,
"sharedStatus": "INACTIVE",
"managed": true,
"smqStatus": "ACCESS_ALLOWED",
```



```
"mdmKnown": true,
"mamKnown": true,
"mamRegistered": true,
"lastUsername": "string",
"imei": "string",
"activesyncid": "string",
"wifimac": "string",
"bluetoothmac": "string",
"inactivityDays": 0,
"shareable": true,
"bulkProfileStatus": "NO_BULK",
"deviceType": "string",
"softwareInventory": [
 {
  "version": "string",
  "blacklistCompliant": true,
  "suggestedListCompliant": true,
  "packageInfo": "string",
  "installCount": 0,
  "installTimeStamp": 0,
```



```
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
   }
  ],
  "deviceActions": [
   {
    "actionType": "WIPE",
    "failedTime": 0,
    "doneTime": 0,
    "askedTime": 0
   }
  ],
  "managedSoftwareInventory": [
   {
    "version": "string",
    "blacklistCompliant": true,
    "suggestedListCompliant": true,
    "packageInfo": "string",
```



```
    "packageInfo": "string",
    "installCount": 0,
    "installTimeStamp": 0,
    "author": "string",
    "container": 0,
    "name": "string",
    "size": 0
   }
  ],
  "policies": [
   {
    "resourceType": "APP_NATIVE",
    "resourceTypeLabel": "string",
    "packageInfo": "string",
    "statusLabel": "string",
    "lastUpdate": 0,
    "status": "SUCCESS",
    "name": "string"
   }
  ],
  "active": true
```



```
 "active": true,
"xmlId": "string",
"deviceUsers": [
 {
  "user": {
   "displayName": "string",
   "id": 0,
   "xmlId": "string",
   "properties": [
    {
     "displayName": "string",
     "id": 0,
     "b64": true,
     "group": "string",
     "name": "string",
     "value": "string"
    }
   ]
  },
  "lastAuthDate": 0,
```



```
    "prevAuthDate": 0,
    "userLogin": "string"
   }
  ],
  "packageStates": [
   {
    "packageName": "string",
    "packageId": 0,
    "statusLabel": "string",
    "date": 0,
    "status": "PENDING"
   }
  ],
  "pushState": "ENQUEUED",
  "pushStateLabel": "string",
  "lastPushDate": 0,
  "lastSentNotification": 0,
  "lastRepliedNotification": 0,
  "strongId": "string",
  "lastSoftwareInventoryTime": 0,
```



```
"firstConnectionDate": 0,
"lastIOSProfileInventoryTime": 0,
"lastUser": {
 "displayName": "string",
 "id": 0,
 "xmlId": "string",
 "properties": [
  {
   "displayName": "string",
   "id": 0,
   "b64": true,
   "group": "string",
   "name": "string",
   "value": "string"
  }
 ]
},
"blacklistCompliant": true,
"suggestedListCompliant": true,
"requiredListCompliant": true,
```



```
"devicePropertiesTimestamp": 0,

"revoked": true,

"mamDeviceId": "string",

"deviceToken": "string",

"typeInst": 0,

"appLock": true,

"appWipe": true,

"mamReady": true,

"validCertificates": [

 {

  "credentialProviderId": "string",

  "type": "string",

  "issuerName": "string",

  "startDate": 0,

  "endDate": 0,

  "revoked": true,

  "certificateNumber": "string"

 }

],

"revokedCertificates": [
```



```
    {
      "credentialProviderId": "string",
      "type": "string",
      "issuerName": "string",
      "startDate": 0,
      "endDate": 0,
      "revoked": true,
      "certificateNumber": "string"
    }
  ],
  "authorizeEnabled": true,
  "revokeEnabled": true,
  "lockEnabled": true,
  "cancelLockEnabled": true,
  "unlockEnabled": true,
  "cancelUnlockEnabled": true,
  "containerLockEnabled": true,
  "cancelContainerLockEnabled": true,
  "containerUnlockEnabled": true,
  "cancelContainerUnlockEnabled": true,
```



```
"containerPwdResetEnabled": true,

"cancelContainerPwdResetEnabled": true,

"wipeEnabled": true,

"cancelWipeEnabled": true,

"clearRestrictionsEnabled": true,

"cancelClearRestrictionsEnabled": true,

"corpWipeEnabled": true,

"cancelCorpWipeEnabled": true,

"sdCardWipeEnabled": true,

"cancelSdCardWipeEnabled": true,

"locateEnabled": true,

"cancelLocateEnabled": true,

"enableTrackingEnabled": true,

"disableTrackingEnabled": true,

"disownEnabled": true,

"activationLockBypassEnabled": true,

"ringEnabled": true,

"cancelRingEnabled": true,

"newPinCode": "string",

"oldPinCode": "string",
```



```
"lockMessage": "string",
"resetPinCode": true,
"scanTime": "string",
"screenSharingPwd": "string",
"iosprofileInventory": [
 {
  "iosConfigInventories": [
   {
    "description": "string",
    "type": "string",
    "organization": "string",
    "identifier": "string",
    "name": "string"
   }
  ],
  "description": "string",
  "organization": "string",
  "managed": true,
  "identifier": "string",
  "receivedDate": 0,
```



```
    "encrypted": true,
    "name": "string"
   }
  ],
  "iosprovisioningProfileInventory": [
   {
    "managed": true,
    "uuid": "string",
    "expiryDate": 0,
    "name": "string"
   }
  ],
  "erasedMemoryCard": true,
  "gpsCoordinates": [
   {
    "gpsTimestamp": 0
   }
  ],
  "lastGpsCoordinate": {
   "gpsTimestamp": 0
```



```
},
"gpsFilterStartDate": 0,
"gpsFilterEndDate": 0,
"wipePinCode": "string",
"lockPhoneNumber": "string",
"dstDevIdUsed": true,
"dstValue": "string",
"smartActionsFailure": true,
"policiesFailure": true,
"applicationsFailure": true,
"touchdownProperties": [
 {
  "category": "string",
  "name": "string",
  "value": "string"
 }
],
"appUnwipeEnabled": true,
"requestMirroringEnabled": true,
"cancelRequestMirroringEnabled": true,
```



```
"stopMirroringEnabled": true,

"cancelStopMirroringEnabled": true,

"knownByZMSP": true,

"wipeDeviceFlag": true,

"lockDeviceFlag": true,

"appWipeEnabled": true,

"appLockEnabled": true,

"appUnlockEnabled": true,

"bulkEnrolled": true,

"nbAvailable": 0,

"hasContainer": true,

"connected": true,

"properties": [

 {

  "displayName": "string",

  "id": 0,

  "b64": true,

  "group": "string",

  "name": "string",

  "value": "string"
```



```
    }

   ]

  }

 }
```

Get Device Apps by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/apps

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "applications": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


Get Device Actions by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/actions

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "actions": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```

Get Device Delivery Groups by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/deliverygroups

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deliveryGroups": [

  {

   "statusLabel": "string",

   "linkey": "string",

   "lastUpdate": 0,

   "status": "SUCCESS",

   "name": "string"

  }

 ]

}
```

Get Managed Software Inventory by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/managedswinventory

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```


Get Policies by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/policies

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "policies": [
  {
   "resourceType": "APP_NATIVE",
   "resourceTypeLabel": "string",
   "packageInfo": "string",
   "statusLabel": "string",
   "lastUpdate": 0,
   "status": "SUCCESS",
   "name": "string"
  }
 ]
}
```


Get Software Inventory by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/{device_id}/softwareinventory

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー


```
{
 "status": 0,
 "message": "string",
 "softwareInventory": [
  {
   "version": "string",
   "blacklistCompliant": true,
   "suggestedListCompliant": true,
   "packageInfo": "string",
   "installCount": 0,
   "installTimeStamp": 0,
   "author": "string",
   "container": 0,
   "name": "string",
   "size": 0
  }
 ]
}
```

Get GPS Coordinates by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/locations/{device_id}

クエリパラメーター :

startDate – 座標フィルターの開始日
endDate – 座標フィルターの終了日

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceCoordinates": {

  "deviceCoordinateList": {

   "deviceCoordinateList": [

    {

     "gpsTimestamp": 0

    }

   ],

   "startDate": 0,

   "endDate": 0

  }

}
```

Send Notification to a List of Devices or Users

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/notify

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{
 "smtpFrom": "Test",
 "to": [
  {
   "deviceId": "1",
   "email": "user@test.com",
   "osFamily": "iOS",
   "serialNumber": "F7NLX6WDF196",
   "smsTo": "+123456676",
   "token": {
    "type": "apns",
    "value": "dfb2fb351a4fb068e40858ecad572e317e6c39b4fa7de6fb29ea1ad7e2254499"
   }
  }
 ],
 "smtpSubject": "This is test subject",
 "smtpMessage": "This is test message",
 "smsMessage": "This is test message",
 "agentMessage": "This is test message",
 "sendAsBCC": "true",
```



```
"smtp": "true",

"sms": "true",

"agent": "true",

"templateId": "-1",

"agentCustomProps": {

 "sound": "Casino.wav"

}
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "notificationRequests": {
  "smtpNotifRequestId": 0,
  "smsNotifRequestId": 0,
  "smsGatewayNotifRequestId": 0,
  "apnsAgentNotifRequestId": 0,
  "shtpAgentNotifRequestId": 0
 }
}
```

Authorize a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/authorize

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply Activation Lock Bypass on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/activationLockBypass

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply App Lock on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/appLock

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply App Wipe on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/appWipe

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply Container Lock on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerLock

クエリパラメーター : newPinCode – AndroidコンテナーのPINコード

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Container Lock on a List of Devices

URL: https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerLock/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Apply Container Unlock on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerUnlock

クエリパラメーター : newPinCode – AndroidコンテナーのPINコード

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Container Unlock on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerUnlock/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Reset Container Password on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerPwdReset

クエリパラメーター : newPinCode – AndroidコンテナーのPINコード

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Reset Container Password on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/containerPwdReset/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Disown a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/disown

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Locate a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/locate

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Locate a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/locate/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Apply GPS Tracking on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/track

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel GPS Tracking on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/track/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Lock a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/lock

クエリパラメーター:

newPinCode – AndroidおよびSymbianデバイスのPINコードは4～16文字にする必要があります。 Wondowsデバイスの PINコードは4桁にする必要があります。
resetPinCode – ロックリクエストにPINコードのリセットリクエストを追加します。 Windows Phone 8.1でのみ使用で

きます。
lockMessage – ロックリクエストにメッセージを追加します。 iOS 7以降でのみ使用できます。
phoneNumber – ロックリクエストに電話番号を追加します。 iOS 7以降でのみ使用できます。

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Lock of a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/lock/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Unlock a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/unlock

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Unlock of a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/unlock/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Deploy a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/refresh

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Request AirPlay Mirroring on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/requestMirroring

クエリパラメーター:

dstName – 宛先名（宛先名または宛先デバイスIDのいずれか）
dstDevId – 宛先デバイスのMACアドレス（宛先名または宛先デバイスIDのいずれか）
scanTime – スキャンする間隔（秒）

screenSharingPwd – 画面共有のパスワード

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Request for AirPlay Mirroring on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/requestMirroring/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Stop AirPlay Mirroring on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/stopMirroring

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Stop AirPlay Mirroring on a List of Devcies

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/stopMirroring/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Clear All Restrictions on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/restrictions/clear

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Cancel Clear All Restrictions on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/restrictions/clear/cancel

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Revoke a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/revoke

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Ring a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/ring

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Ringing a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/ring/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Wipe a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/wipe

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Wipe of a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/wipe/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Selectively Wipe a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/selwipe

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Selectively Wiping a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/selwipe/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Wipe the SD Cards on a List of Devices

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/sdcardwipe

リクエストの種類：POST

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceActionMessages": {
  "devicesActionParameters": {
   "description": "string",
   "messageList": [
    {
     "id": "string",
     "message": "string"
    }
   ]
  }
 }
}
```

Cancel Wiping SD Cards on a List of Devices

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/sdcardwipe/cancel

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
[1,2]
```

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceActionMessages": {

  "devicesActionParameters": {

   "description": "string",

   "messageList": [

    {

     "id": "string",

     "message": "string"

    }

   ]

  }

 }

}
```

Get All Known Properties on a Device

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/knownProperties

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "knownProperties": {
  "knownProperties": {
   "knownPropertyList": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string",
     "group": "EVERYWAN",
     "groupLabel": "string"
    }
   ]
  }
}
```

Get All Used Properties on a Device

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/usedProperties

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "deviceUsedPropertiesList": {
  "deviceUsedProperties": {
   "deviceUsedPropertiesParameters": [
    {
     "name": "string",
     "type": "STRING",
     "displayName": "string"
    }
   ]
  }
 }
}
```

Get All Device Properties by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/properties/{deviceId}

リクエストの種類：GET

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{
 "status": 0,
 "message": "string",
 "devicePropertiesList": {
  "deviceProperties": {
   "startIndex": 0,
   "devicePropertyParameters": [
    {
     "name": "string",
     "value": "string",
     "id": 0,
     "displayName": "string",
     "group": "string",
     "b64": true
    }
   ],
```

```
    "totalCount": 0

  }

 }

}
```

Update All Device Properties by Device ID

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/properties/{deviceId}

リクエストの種類：PUT

リクエストヘッダー：auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{

  "properties": [

    {

      "name": "ACTIVE_ITUNES",

      "value": "0"

    }

  ]

}
```

応答例 コピー

```
{

 "status": 0,

 "message": "string"

}
```

Add or Update a Device Property by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/properties/{deviceId}

リクエストの種類 : POST

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

リクエスト例 コピー

```
{

 "name": "PROPERTY_NAME",

 "value": "PROPERTY_VALUE"

}
```

応答例 コピー

```
{

 "status": 0,

 "message": "string"

}
```

Delete a Device Property by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/properties/{deviceId}

リクエストの種類 : DELETE

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string"

}
```

Get iOS Device MDM Status by Device ID

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/mdmStatus/{deviceId}

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "deviceMdmStatus": {

  "deviceMdmStatusParameters": {

     "pushState": "ENQUEUED",

     "lastPushDate": 0,

     "lastRepliedNotification": 0,

     "lastSentNotification": 0,

     "pushStateLabel": "string"

   }

 }

}
```

Generate PIN code

URL : https://<ホスト名>:<ポート番号>/xenmobile/api/v1/device/pincode/generate

クエリパラメーター : pinCodeLength – 要求したPINコードの長さ

リクエストの種類 : GET

リクエストヘッダー : auth_token – ユーザーのログオン時に取得される認証トークン

Content type – application/json

応答例 コピー

```
{

 "status": 0,

 "message": "string",

 "pinCode": {

  "answer": "string"

 }

}
```


XenMobile SOAP API

Aug 30, 2016

XenMobileでのモバイルデバイス管理には、以下のSOAP WebサービスAPIを使用できます。 XenMobile用のAPIおよびSDKは、XenMobile Developer Communityのサイトでダウンロードできます。

Web Service Definition Language（WSDL）名	呼び出し
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

getDeviceInfo

getDeviceInformationForUser

getDeviceProperties

getLastUser

getManagedStatus

getMasterKeyList

getSoftwareInventory

getStrongID

getUserDevices

isEnforceSSL

isEnforceStrongAuthentication

locateDevice

lockDevice

putDeviceProperties

registerDeviceForUser

removeDevice

resetDeploymentState

revoke

unlockDevice

wipeDevice

	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	browseOtp
	createOtp
	getAvailableEnrollmentModes
	getOtpInfo
	revokeOtp
	triggerNotification

XenMobile Mail Manager 10

Oct 25, 2016

XenMobile Mail Managerには、XenMobileの機能を拡張する以下の機能が備わっています。

- Exchange ActiveSync（EAS）デバイスに対するダイナミックアクセス制御。 EASデバイスのExchangeサービスに対するアクセスを自動的に許可または禁止できます。
- Exchangeが提供するEASデバイスパートナーシップ情報にアクセスする機能のXenMobileへの提供。
- モバイルデバイスでEASワイプを実行する機能のXenMobileへの提供。
- Blackberryデバイスに関する情報にアクセスしたり、ワイプやパスワードリセットなどの制御操作を実行したりする機能のXenMobileへの提供。

XenMobile Mail Managerをダウンロードするには、Citrix.comのXenMobile 10サーバーのサーバーコンポーネントのセクションに移動します。

XenMobile Mail Manager 10.1の新機能

アクセス規則

［Rule Analysis］ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。

デフォルトのアクセス権（Allow、Block、またはUnchanged）とActiveSyncコマンドモード（PowerShellまたはSimulation）は、XenMobile展開に構成されている各Microsoft Exchange環境ごとに別々に設定されます。

スナップショット

スナップショット履歴に表示されるスナップショットの最大数を構成できます。

メジャースナップショット時にどのエラーを無視するかを構成できます。 無視可能に構成されていないエラーがメジャースナップショットから返された場合、スナップショットの結果は破棄されます。

エラーを無視可能と構成するには、XMLエディターを使用してconfig.xmlファイルを次のように編集します。

- Exchange ServerがOffice 365の場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。 正規表現がサポートされます。
- Exchange Serverがオンプレミスの場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。 正規表現がサポートされます。
- 複数のExchange環境が構成されている場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='目的のExchange環境に対応するID']/ExchangeServer/Specialists/PowerShellノードに移動します。 IgnorableErrors子ノードをPowerShellノードに追加し、無視するエラーそれぞれに対して、 IgnorableErrorsノードにError子ノードを追加し、CDATAセクションで照合するテキストを設定します。 正規表現がサポートされます。

config.xmlを保存して、XenMobile Mail Managerサービスを再起動します。

PowerShellおよびExchange

XenMobile Mail Managerは、使用するコマンドレットを、接続先のExchangeのバージョンに基づいて動的に決定するようになりました。 たとえば、Exchange 2010の場合はGet-ActiveSyncDeviceを使用しますが、Exchange 2013およびExchange 2016の場合はGet-MobileDeviceを使用します。

Exchangeの構成

Exchange Server構成は、XenMobile Mail Managerサービスを再起動せずに編集および更新できます。

Exchange環境の［概要］タブに追加された2つの新しい列には、各環境のコマンドモード（PowerShellまたはSimulation）とアクセスモード（Allow、Block、またはUnchanged）が表示されます。

トラブルシューティングおよび診断

Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

コンソールの［Configuration］ウィンドウの［Test Connectivity］ボタンを使用してExchangeサービスの接続性をテストすると、サービスが使用するすべての読み取り専用コマンドレットが実行され、構成されたユーザーのRBAC権限テストがExchange Serverに対して実行され、エラーや警告が色分けされて表示されます（警告は青と黄、エラーは赤とオレンジ）。

新しいトラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。 すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

サポートシナリオでは、コンソールで診断ダイアログボックスを選択することで、XenMobile Mail Managerによって管理されるすべてのデバイス上のすべてのメールボックスのすべてのプロパティを保存できます。

サポートシナリオで、トレースレベルのログがサポートされるようになりました。

Authentication

XenMobile Mail Managerは、オンプレミス展開でBasic認証をサポートします。 これにより、XenMobile Mail ManagerサーバーがExchange Serverが存在するドメインのメンバーでなくても、XenMobile Mail Managerを使用できるようになります。

解決された問題

アクセス規則

XenMobile Mail Managerは、Active Directory（AD）グループに1000人以上のユーザーが含まれる場合でも、ADグループのすべてのユーザーにローカルアクセス制御ルールを適用します。 過去のバージョンのXenMobile Mail Managerでは、ADグループの最初の1000人のユーザーだけにローカルアクセス制御ルールを適用していました。 [#548705]

1000人以上のユーザーが含まれるActive Directoryグループに対してクエリを行った場合、XenMobile Mail Managerコンソールが応答しなくなることがあります。 [CXM-11729]

［LDAP Configuration］ウィンドウに不正確な認証モードが表示されないようになりました。 [CXM-5556]

スナップショット

ユーザー名にアポストロフィが含まれていても、マイナースナップショットが失敗しなくなりました。 [#617549]

パイプライン化が無効化されたサポートシナリオで（XenMobile Mail Managerコンソールの［Configuration］ウィンドウで［Disable Pipelining］オプションを選択）、オンプレミスExchange環境でもメジャースナップショットが失敗しなくなりました。 [#586083]

パイプライン化が無効化されたサポートシナリオで（XenMobile Mail Managerコンソールの［Configuration］ウィンドウで［Disable Pipelining］オプションを選択）、詳細スナップショットと簡易スナップショットのどちらのために環境が構成されているかに関係なく、詳細スナップショット用のデータが収集されなくなりました。 詳細スナップショット用のデータが収集されるのは、環境が詳細スナップショット用に構成されているときだけになりました。 [#586092]

初期インストール後の最初のメジャースナップショットがエラーになることがあり、その場合、XenMobile Mail Managerサービスが再起動されるまで、XenMobile Mail Managerがあらためてメジャースナップショットを実行することはできませんでした。 そのようなことはもう発生しません。 [CXM-5536]

XenMobile Mail Manager 10について

XenMobile Mail Manager 10.1について

Oct 25, 2016

XenMobile Mail Manager 10.1では、以下の新しい機能が追加されました。

アクセス規則

［Rule Analysis］ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。

デフォルトのアクセス権（Allow、Block、またはUnchanged）とActiveSyncコマンドモード（PowerShellまたはSimulation）は、XenMobile展開に構成されている各Microsoft Exchange環境ごとに別々に設定されます。

スナップショット

スナップショット履歴に表示されるスナップショットの最大数を構成できます。

メジャースナップショット時にどのエラーを無視するかを構成できます。 無視可能に構成されていないエラーがメジャースナップショットから返された場合、スナップショットの結果は破棄されます。

エラーを無視可能と構成するには、XMLエディターを使用してconfig.xmlファイルを次のように編集します。

- Exchange ServerがOffice 365の場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。 正規表現がサポートされます。 手順7に進みます。
- Exchange Serverがオンプレミスの場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。 正規表現がサポートされます。 手順7に進みます。
- 複数のExchange環境が構成されている場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='目的のExchange環境に対応するID']/ExchangeServer/Specialists/PowerShellノードに移動します。 IgnorableErrors子ノードをPowerShellノードに追加し、無視するエラーそれぞれに対して、照合するテキストをCDATAセクションに含むError子ノードをIgnorableErrorsノードに追加します。 正規表現がサポートされます。

config.xmlを保存して、XenMobile Mail Managerサービスを再起動します。

PowerShellおよびExchange

XenMobile Mail Managerは、使用するコマンドレットを、接続先のExchangeのバージョンに基づいて動的に決定するようになりました。 たとえば、Exchange 2010の場合は**Get-ActiveSyncDevice**を使用しますが、Exchange 2013およびExchange 2016の場合は**Get-MobileDevice**を使用します。

Exchangeの構成

Exchange Server構成は、XenMobile Mail Managerサービスを再起動せずに編集および更新できます。

Exchange環境の［概要］タブに追加された2つの新しい列には、各環境のコマンドモード（PowerShellまたはSimulation）とアクセスモード（Allow、Block、またはUnchanged）が表示されます。

トラブルシューティングおよび診断

Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

コンソールの［Configuration］ウィンドウの **[Test Connectivity]** ボタンを使用してExchangeサービスの接続性をテストすると、サービスが使用するすべての**読み取り専用**コマンドレットが実行され、構成済みユーザーのRBAC権限テストがExchange Serverに対して実行

されて、エラーや警告が色分けされて表示されます（警告は青と黄、エラーは赤とオレンジ）。

新しいトラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。 すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

サポートシナリオでは、コンソールで診断ダイアログボックスを選択することで、XenMobile Mail Managerによって管理されるすべてのデバイス上のすべてのメールボックスのすべてのプロパティを保存できます。

サポートシナリオで、トレースレベルのログがサポートされるようになりました。

Authentication

XenMobile Mail Managerは、オンプレミス展開でBasic認証をサポートします。 これにより、XenMobile Mail ManagerサーバーがExchange Serverが存在するドメインのメンバーでなくても、XenMobile Mail Managerを使用できるようになります。

解決された問題

アクセス規則

XenMobile Mail Managerは、Active Directoryグループに1,000人以上のユーザーが含まれる場合でも、Active Directoryグループのすべてのユーザーにローカルアクセス制御ルールを適用します。 過去のバージョンのXenMobile Mail Managerでは、Active Directoryグループの最初の1,000人のユーザーだけにローカルアクセス制御ルールを適用していました。 [#548705]

1,000人以上のユーザーが含まれるActive Directoryグループに対してクエリを行った場合、XenMobile Mail Managerコンソールが応答しなくなることがあります。 [CXM-11729]

［LDAP Configuration］ウィンドウに不正確な認証モードが表示されないようになりました。 [CXM-5556]

スナップショット

ユーザー名にアポストロフィが含まれていても、マイナースナップショットが失敗しなくなりました。 [#617549]

パイプライン化が無効化されたサポートシナリオで（XenMobile Mail Managerコンソールの［Configuration］ウィンドウで**[Disable Pipelining]**オプションを選択）、オンプレミスExchange環境でもメジャースナップショットが失敗しなくなりました。 [#586083]

パイプライン化が無効化されたサポートシナリオでは（XenMobile Mail Managerコンソールの［Configuration］ウィンドウで**[Disable Pipelining]**オプションを選択）、環境を詳細スナップショット用と簡易スナップショット用のどちらに構成していても詳細スナップショット用のデータが収集されることはなくなりました。 詳細スナップショット用のデータが収集されるのは、環境が詳細スナップショット用に構成されているときだけになりました。 [#586092]

初期インストール後の最初のメジャースナップショットがエラーになることがあり、その場合、XenMobile Mail Managerサービスが再起動されるまで、XenMobile Mail Managerがあらためてメジャースナップショットを実行することはできませんでした。 そのようなことはもう発生しません。 [CXM-5536]

XenMobile Mail Manager 10について

Oct 25, 2016

- XenMobile Mail Manager 10にアップグレードする間、インストールされたXenMobile Mail Managerのバージョンは常に8.5として表示されます。ただし、XenMobile Mail Managerのアップグレードは実行されます。 [#539520]
- マイナースナップショットの「devices found」報告で混乱が生じることがあります。 マイナースナップショットがメジャースナップショットの開始に引き続いて実行される場合、後続のマイナースナップショットの概要では同じデバイスが「new」として報告されることがあります。
- XenMobile Mail Managerは、Active Directoryグループに1000人以上のユーザーが含まれる場合でも、グループの最初の1000人のユーザーにのみローカルアクセス制御ルールを適用することがあります。

PowerShellまたはExchangeの管理

特定のMicrosoft Exchange環境（主にOffice 365）では、帯域幅を効果的に制限するXenMobile Mail Managerに制限が課され、アプリケーションがPowerShell要求またはコマンドを発行できなくなります。 現在では、Exchange構成タブで代わりのPowerShellコマンドレットパスウェイを使用できます。これにより、XenMobile Mail Managerが代替スナップショットモードになります。このモードでは、元のデータパスが回避されます。

新しいフラグで、Microsoft Office 365以外の環境のAllowRedirectionフラグを公開できます。 Microsoft Exchange構成タブを使用してこのフラグを有効化します。

規則の管理

LDAPローカル規則で、大規模なActive Directory環境の整理されていない数のグループがサポートされるようになりました。

XenMobileではWorxMailクライアントのデバイス情報が重複します。 この問題を解決するには、XenMobile Mail ManagerのManaged Service Provider（MSP）の部分で正規表現のサポートを有効にする必要があります。こうすることで、XenMobileに返されるレコードセットがフィルタリングされます。 フィルターに一致するデバイスはXenMobileに返されません。

MSP

BlackBerry Enterprise Server（BES）から削除されるユーザーがローカルデータベースから削除されるようになりました。

UI

永続的プロセスが実行されているシナリオで、進行状況のダイアログボックスクラスを使用できるようになりました。 このようなプロセスでは、XenMobile Mail Managerからユーザーにフィードバックが送信され、取り消す機会が提供されます（該当する場合）。

新しいMicrosoft Exchangeインスタンスのデフォルト値が［Shallow］に設定されるようになりました。

インストーラー

Zenpriseを参照するコンポーネントがXenMobile Mail Managerを反映するように変更されました。

インストールパスが見つからない場合、インストーラーがハングします。

インストール後に、サポートバイナリおよびスクリプトがSupportフォルダーに配置されるようになりました。

Windowsの［スタート］メニューで、XenMobile Mail Managerのショートカットが\Citrix\XenMobile Mail Managerフォルダーに配置されるようになりました。

サポート

サポートモデルでは、config.xmlファイルの追加によってトラブルシューティング機能を有効化できます。 このファイルを使用して、Citrixが問題をトラブルシューティングするのに役立てることができます。 このリリースのXenMobile Mail Managerでは、この機能はMicrosoft Exchange構成の［追加］と［編集］の画面にのみ適用されます。

注：Shiftキーを押しながら構成ユーティリティを開いて、このトラブルシューティング機能を有効化することもできます。

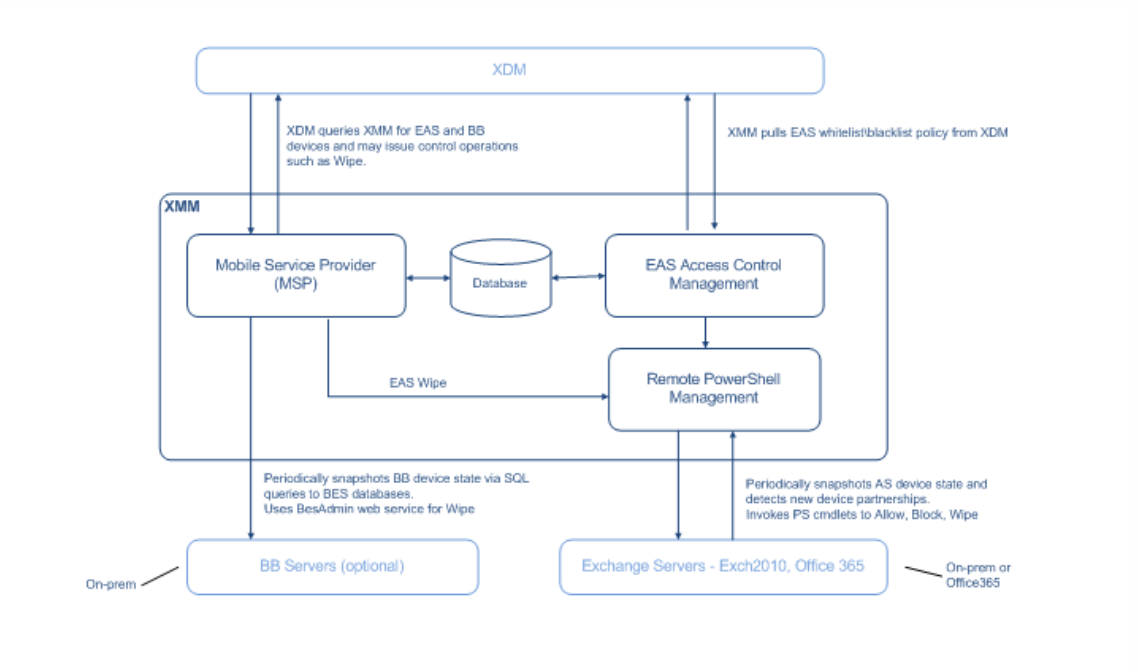
ログ記録機能

PowerShellから返されるエラーメッセージに、関連するGUIDが含まれるようになりました。 この値を使用して、［Snapshot History］詳細タブに表示される内容を制御します。

アーキテクチャ

Oct 25, 2016

次の図は、XenMobile Mail Managerの主要コンポーネントを示しています。 リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の「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。



次の3つの主要コンポーネントがあります。

- **Exchange ActiveSync Access Control Management**。 XenMobileと通信して、XenMobileからExchange ActiveSyncポリシーを取得します。さらに、このポリシーをローカルに定義されているポリシーと統合して、Exchangeへのアクセスを許可または拒否するExchange ActiveSyncデバイスを決定します。 ローカルポリシーにより、Active Directoryのグループ、ユーザー、デバイスの種類、またはデバイスのユーザーエージェント（一般的にはモバイルプラットフォームのバージョン）によってアクセス制御できるように、ポリシー規則を拡張できます。
- **Remote PowerShell Management**。 リモートのPowerShellコマンドのスケジュール設定と呼び出しを処理して、Exchange ActiveSync Access Control Managementによって編集されたポリシーを有効にします。 定期的にExchange ActiveSyncデータベースのスナップショットを取得し、新規の、または変更されたExchange ActiveSyncデバイスを検出します。
- Mobile Service Provider。 XenMobileでExchange ActiveSyncデバイスやBlackBerryデバイスに対してクエリを実行したり、ワイプなどの制御操作を発行したりできるように、Webサービスインターフェイスを提供します。

システム要件および前提条件

Oct 25, 2016

XenMobile Mail Managerを使用するには、以下のシステム環境が必要です。

- Windows Server 2008 R2（英語ベースのサーバーであることが必須）
- Microsoft SQL Server 2008、SQL Server 2012、SQL Server 2016、SQL Server Express 2008、SQL Server 2012、または Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5。
- Blackberry Enterprise Service, version 5（オプション）

Microsoft Exchange Serverのサポートされる最小バージョン

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

- Windows Management Frameworkがインストールされていること。
  - PowerShell V5、V4、およびV3
- PowerShell実行ポリシーがSet-ExecutionPolicy RemoteSignedによってRemoteSignedに設定されていること。
- XenMobile Mail Managerを実行しているコンピューターとリモートのExchange Serverの間で、TCPポート80が開いていること。

Exchangeを実行しているオンプレミスコンピューターの要件

権限。 Exchangeの構成UIで指定される資格情報を使用してExchange Serverに接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセスが付与される必要があります。

- **Exchange Server 2010 SP2の場合**：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Exchange Server 2013およびExchange Server 2016の場合**：
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

- フォレスト全体を表示するようにXenMobile Mail Managerが構成されている場合は、次のコマンドレットを実行するための権限が付与されている必要があります。 Set-AdServerSettings -ViewEntireForest $true
- 指定された資格情報には、リモートシェルを介して、Exchange Serverに接続する権限が与えられている必要があります。 デフォルトでは、Exchangeをイン

ストールしたユーザーがこの権限を持ちます。
- Microsoft TechNetサポート技術情報「about_Remote_Requirements」によれば、リモート接続を確立してリモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。 ブログの投稿「You Don't Have to Be An Administrator to Run Remote PowerShell Commands」によれば、 Set-PSSessionConfiguration を使用して管理要件を無視できます。ただし、このコマンドの詳細のサポートと説明については、このドキュメントでは扱いません。
- Exchange Serverは、HTTPを介してリモートPowerShell要求をサポートするように構成されている必要があります。 通常、必要なのはExchange Serverでのみ のPowerShellコマンドを実行する管理者のみです。 WinRM QuickConfig。
- Exchangeには多くの調整ポリシーがあります。 調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。 Exchange 2010の場合、1人のユーザーに許可されている同時接続数のデフォルトは18です。 接続数の上限に達すると、XenMobile Mail Managerは Exchange Serverに接続できなくなります。 PowerShellの同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。 関心がある場合は、PowerShellによるリモート管理に関連するExchangeの調整ポリシーについて調べてください。

Office 365 Exchangeの要件

- **権限**。 Exchangeの構成UIで指定される資格情報を使用してOffice 365に接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセスが付与される必要があります。
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- 指定された資格情報には、リモートシェルを介して、Office 365サーバーに接続する権限が与えられている必要があります。 デフォルトでは、Office 365のオンライン管理には、必要な権限が備えられています。
- Exchangeには多くの調整ポリシーがあります。 調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。 Office 365の場合、1人のユーザーに許可されている同時接続数のデフォルトは3です。 接続数の上限に達すると、XenMobile Mail ManagerはExchange Serverに接続できなくなります。 PowerShellの同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。 関心がある場合は、PowerShellによるリモート管理に関連する、Exchangeの調整ポリシーについて調べてください。

インストールおよび構成

Oct 25, 2016

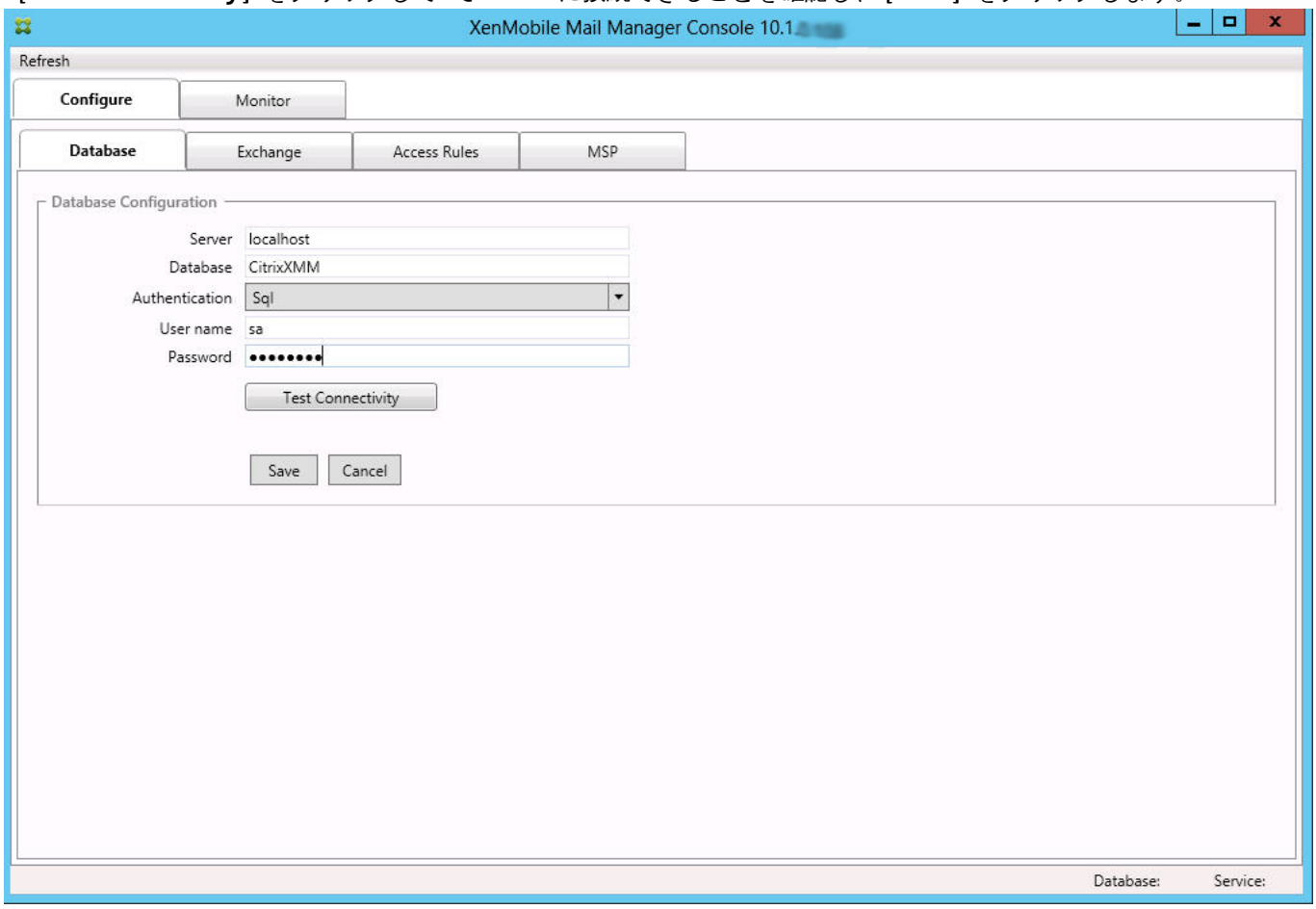
1. XmmSetup.msiファイルをクリックして、インストーラーのプロンプトに従い、XenMobile Mail Managerをインストールします。

2. セットアップウィザードの最後の画面で、 **[Launch the Configure utility]** を選択されたままにしておきます。 または、 **[スタート]** メニューの **[XenMobile Mail Manager]** を選択します。

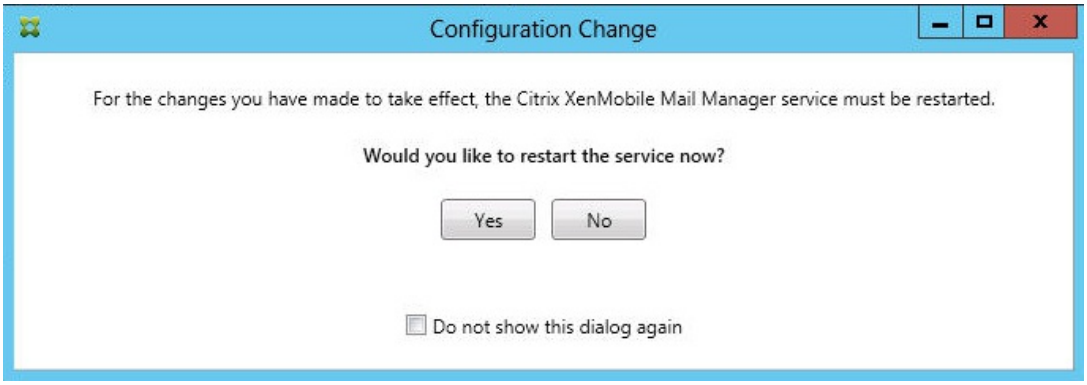
3. 次のデータベースプロパティを構成します。
    1. **[Configure]** の **[Access Rules]** タブを選択します。
    2. SQL Serverの名前（デフォルトはlocalhost）を入力します。
    3. データベースはデフォルトのCitrixXmmのままにします。
    4. SQLに使用される次のいずれかの認証モードを選択します。

- **Sql**。 有効なSQLユーザーのユーザー名とパスワードを入力します。
- **Windows Integrated**。 このオプションを選択した場合、XenMobile Mail Managerサービスのログオン資格情報を、SQL Serverにアクセスするための権限を持つWindowsアカウントに変更する必要があります。 これを行うには、 **[コントロールパネル]**、 **[管理ツール]**、 **[サービス]**の順に選択し、XenMobile Mail Managerサービスエントリを右クリックし、 **[ログオン]**タブをクリックします。
  注：BlackBerryデータベース接続に対しても［Windows Integrated］を選択している場合は、ここで指定されているWindowsアカウントにBlackBerryデータベースへのアクセスも付与する必要があります。

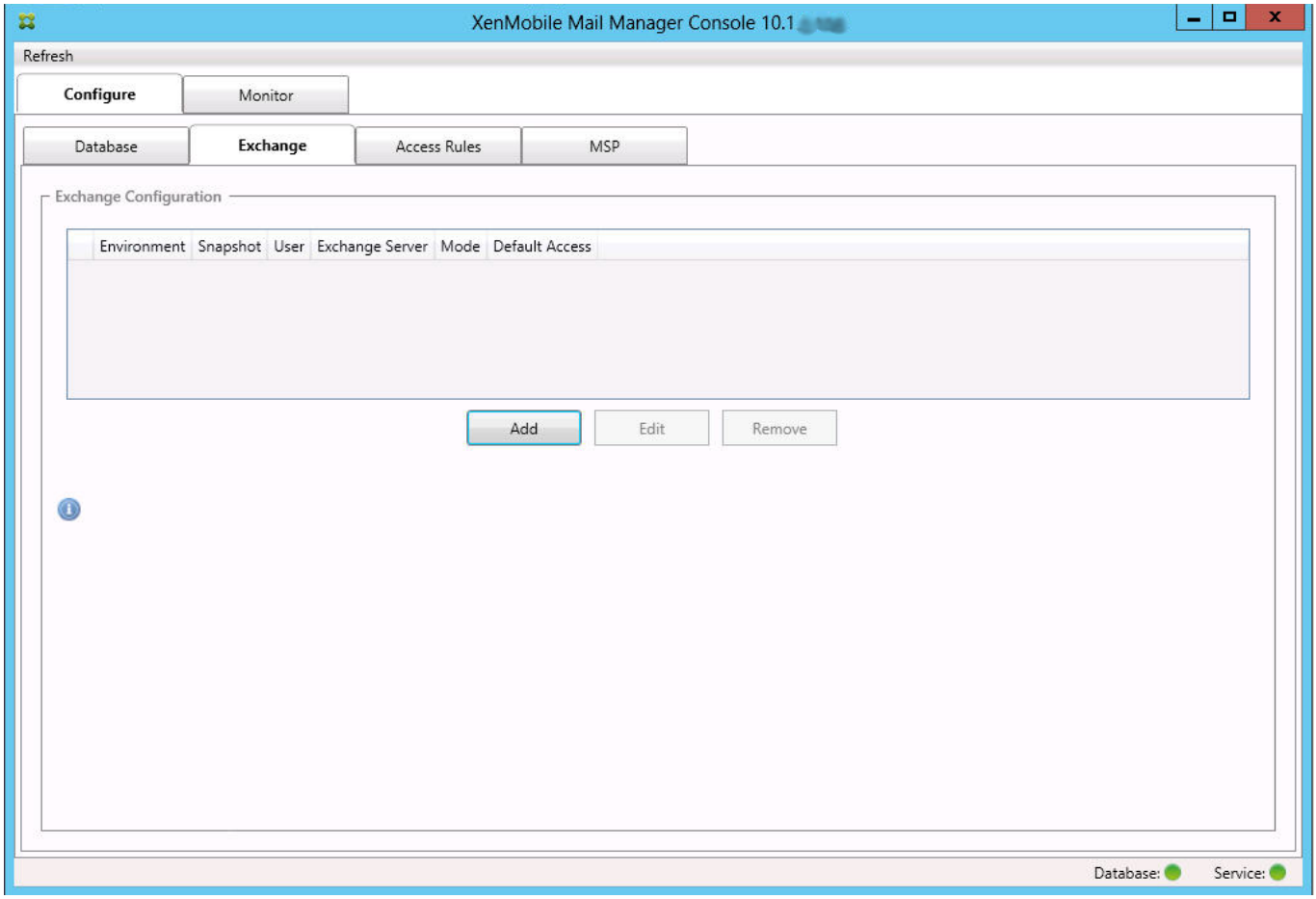
5. **[Test Connectivity]**をクリックしてSQL Serverに接続できることを確認し、 **[Save]**をクリックします。



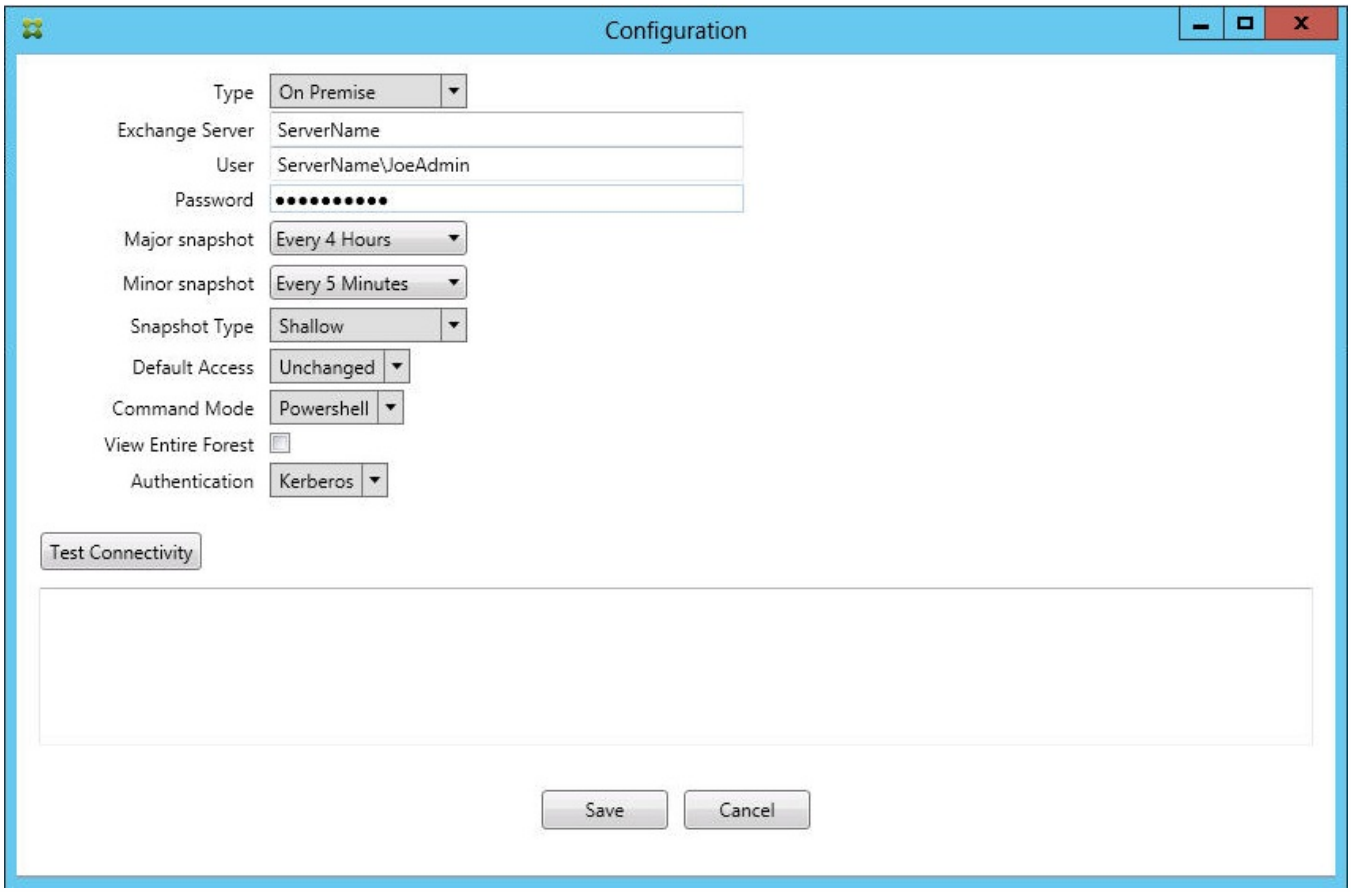
4. サービスの再起動を求めるメッセージが表示されます。 **[Yes]**をクリックします。



5. 1つまたは複数のExchange Serverを構成します。
   1. 単一のExchange環境を管理している場合は、単一のサーバーを指定する必要があるのみです。複数のExchange環境を管理している場合は、Exchange環境ごとに単一のExchange Serverを指定する必要があります。
   2. **[Configure]の[Exchange]タブ**をクリックします。



3. **[Add]** をクリックします。
4. Exchange Server環境の種類として **[On Premise]** または **[Office 365]** を選択します。

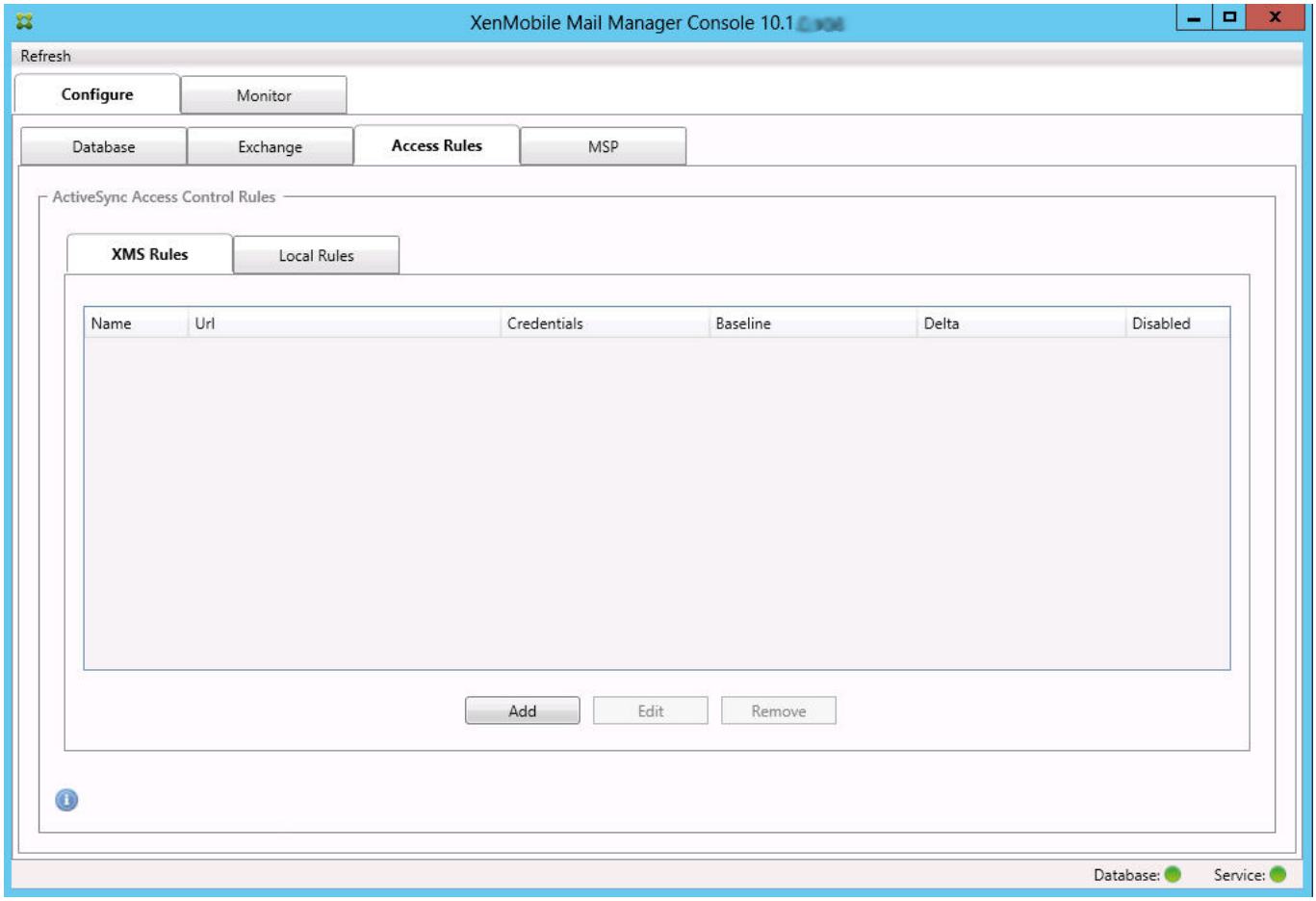


5. **［On Premise］**を選択した場合は、リモートPowerShellコマンド用に使用するExchange Serverの名前を入力します。
6. 要件セクション内で指定されているとおりの、Exchange Serverに対する適切な権限を持つWindows IDのユーザー名を入力します。
7. ユーザーのパスワードを**［Password］**ボックスに入力します。
8. メジャースナップショットを実行するスケジュールを選択します。 メジャースナップショットにより、すべてのExchange ActiveSyncパートナーシップが検出されます。
9. マイナースナップショットを実行するスケジュールを選択します。 マイナースナップショットにより、新しく作成されたExchange ActiveSyncパートナーシップが検出されます。
10. スナップショットの種類として、**［Deep］**または**［Shallow］**を選択します。 通常、簡易スナップショットははるかに高速で、XenMobile Mail ManagerのExchange ActiveSyncアクセス制御機能をすべて実行するには十分です。 詳細スナップショット（XenMobileで、非管理対象デバイスを照会できます）は、処理にかかる時間が著しく長くなることがあり、Mobile Service ProviderがActiveSyncに対して有効にされている場合にのみ必要です。
11. ［Default Access］で、**［Allow］**、**［Block］**、または**［Unchanged］**を選択します。 これにより、明示的なXenMobileまたはローカル規則で特定されたものを除くすべてのデバイスの処理方法が制御されます。 ［Allow］を選択した場合は該当するすべてのデバイスに対するActiveSyncアクセスが許可され、［Block］を選択した場合はアクセスが拒否され、［Unchanged］を選択した場合は変更されません。
12. ［ActiveSync Command Mode］で、**［PowerShell］**または**［Simulation］**を選択します。
    - ［PowerShell］モードでは、XenMobile Mail ManagerはPowerShellコマンドを発行し、目的のアクセス制御を有効にします。
    - ［Simulation］モードでは、XenMobile Mail ManagerはPowerShellコマンドを発行しませんが、想定しているコマンドと結果をデータベースに記録します。 ［Simulation］モードでは、［PowerShell］モードを有効にした場合の結果を［Monitor］タブを使って確認できます。
13. Exchange環境でActive Directoryフォレスト全体を表示するようにXenMobile Mail Managerを構成するには、**［View Entire Forest］**をオンにします。
14. 認証プロトコルとして、**［Kerberos］**または**［Basic］**を選択します。 XenMobile Mail Managerは、オンプレミス展開

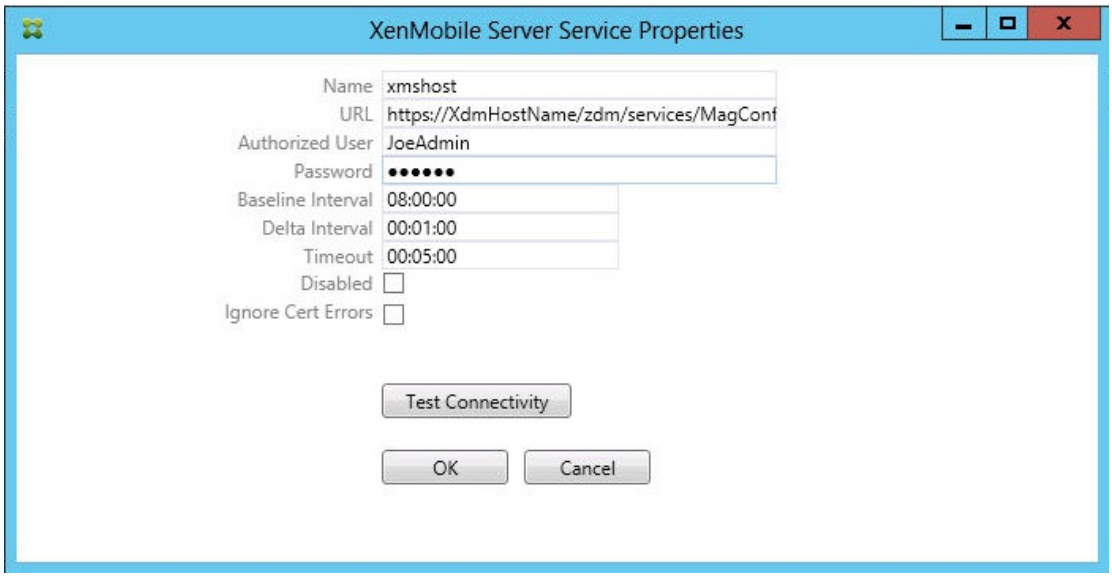
でBasic認証をサポートします。 これにより、XenMobile Mail ManagerサーバーがExchange Serverが存在するドメインのメンバーでなくても、XenMobile Mail Managerを使用できるようになります。

15. **[Test Connectivity]** をクリックしてExchange Serverに接続できることを確認し、**[Save]** をクリックします。
16. サービスの再起動を求めるメッセージが表示されます。 **[Yes]** をクリックします。

6. アクセス規則を構成します。
   1. **[Configure]** > **[Access Rules]** タブを選択します。
   2. **[XDM Rules]** タブをクリックします。

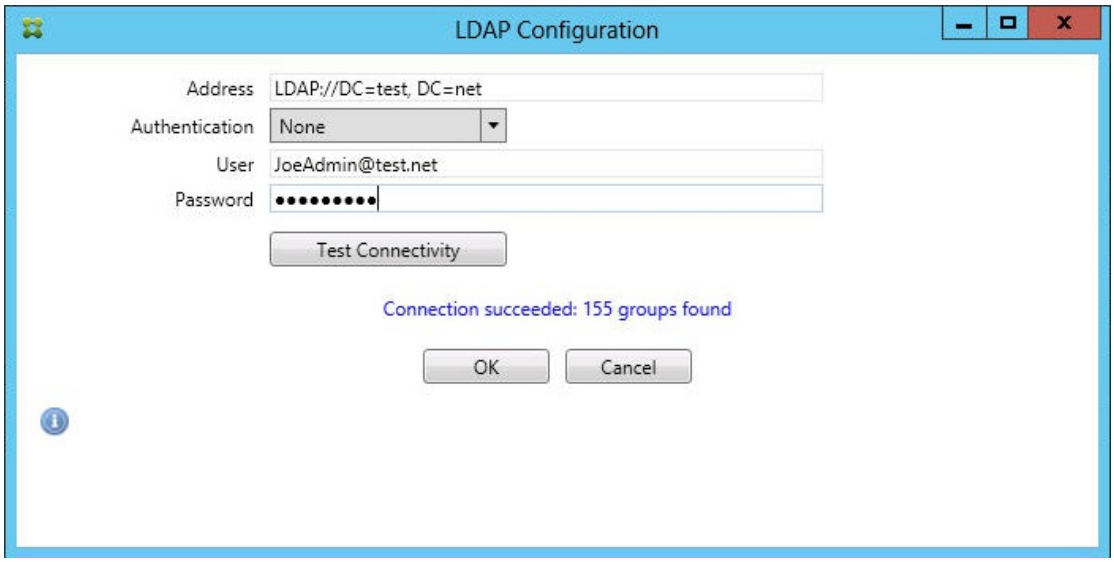


3. **[Add]** をクリックします。



4. XenMobileサーバー規則の名前（XdmHostなど）を入力します。
5. XenMobileサーバーを参照するようにURL文字列を変更します。たとえば、サーバー名がXdmHostである場合は、「http://XdmHostName/zdm/services/MagConfigService」と入力します。
6. サーバーで認証されているユーザーを入力します。
7. そのユーザーのパスワードを入力します。
8. **[Baseline Interval]** 、 **[Delta Interval]** 、および **[Timeout]** はデフォルト値のままにします。
9. **[Test Connectivity]** をクリックして、サーバーへの接続を確認します。
   注： [Disabled] チェックボックスがオンの場合は、XenMobile MailサービスでXenMobileサーバーからポリシーが収集されません。
10. **[OK]** をクリックします。

7. **[Local Rules]** タブをクリックします。
   1. Active Directoryのグループに対して使用するローカル規則を作成する場合は、**[Configure LDAP]** をクリックし、LDAP接続プロパティを構成します。

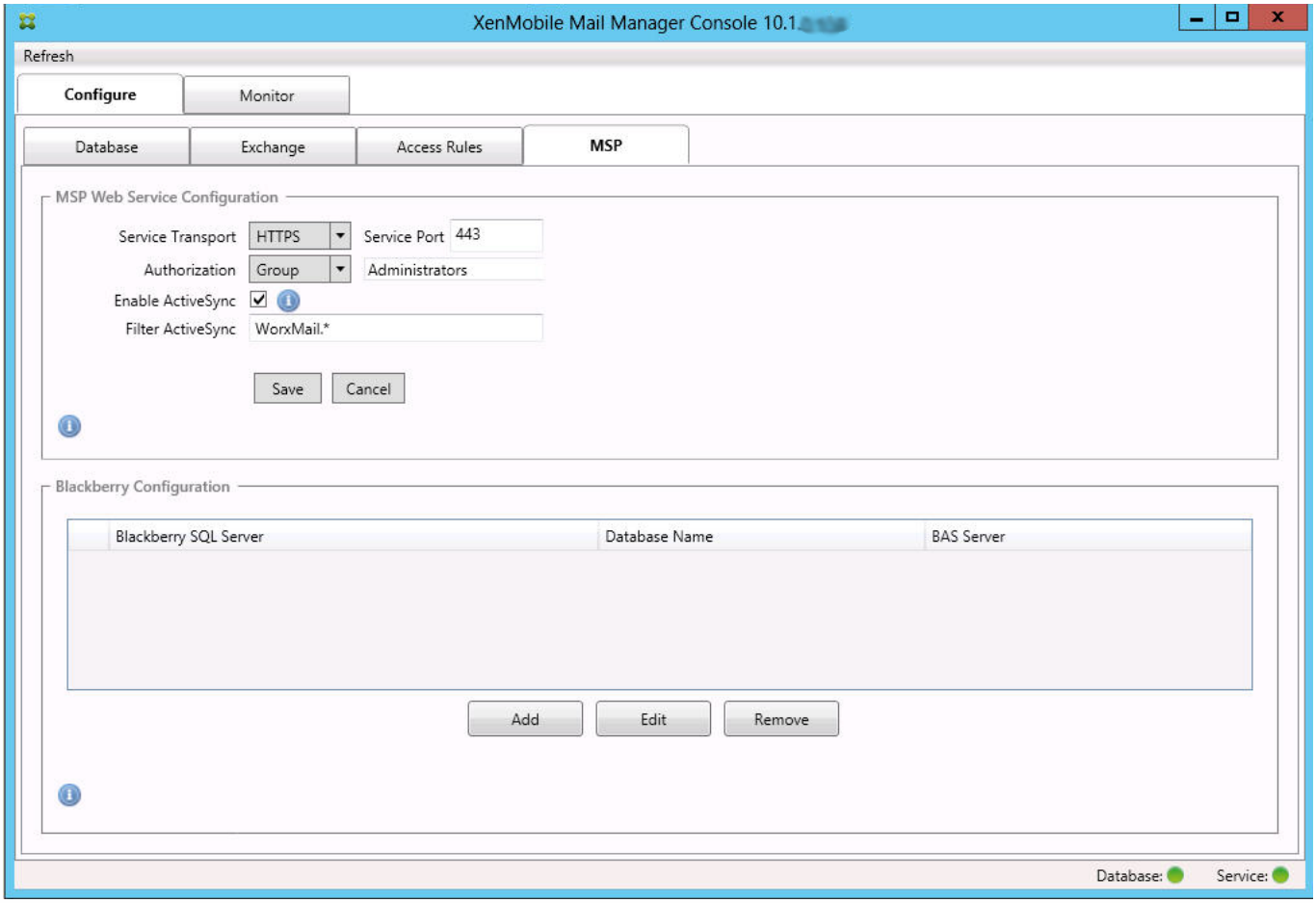


   2. **[ActiveSync Device ID]** 、 **[Device Type]** 、 **[AD Group]** 、 **[User]** 、またはデバイスの **[UserAgent]** に基づいてローカル規則を追加できます。 一覧で、適切な種類を選択します。 詳しくは「XenMobile Mail Managerのアクセス制

御規則」を参照してください。

3. 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。
   注：グループ以外のすべての種類の場合、システムはスナップショットで見つかったデバイスに依存しています。 したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。
4. テキスト値を選択し、［**Allow**］または［**Deny**］をクリックして右側の［**Rule List**］ペインに追加します。 ［**Rule List**］ペインの右側にあるボタンを使用して、規則の順序を変更したり、規則を削除したりすることができます。 指定したユーザーおよびデバイスに対して、規則は表示順に評価され、上位の規則（より上部に近い規則）に一致すると以降の規則が無効になるので、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規則とユーザー「Matt」をブロックする下位の規則がある場合、MattのiPadは許可されます。この理由は、「iPad」規則の効果の優先度が「Matt」規則よりも高いからです。
5. 規則一覧内の規則の分析を実行して、上書き、競合、または補足構造の可能性を検出する場合は、［**Analyze**］をクリックします。
6. ［**Save**］をクリックします。

8. Mobile Service Providerを構成します。
   注：Mobile Service Providerはオプションであり、Mobile Service Providerインターフェイスを使用して非管理対象デバイスを照会するようにXenMobileがさらに構成されている場合にのみ必要です。
   1. ［**Configure**］>［**MSP**］タブをクリックします。

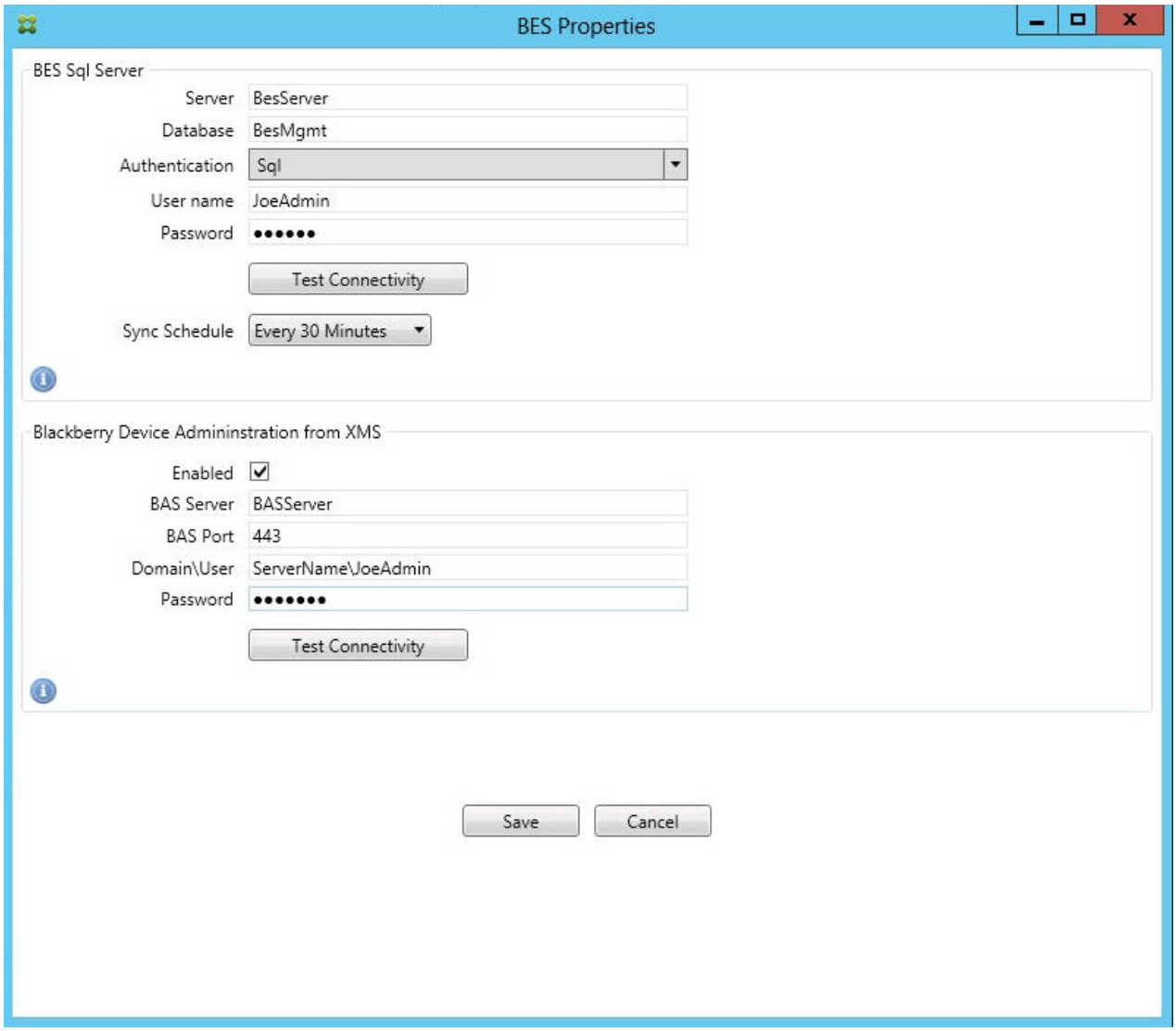


   2. Mobile Service Providerサービスのサービストランスポートの種類（［**HTTP**］または［**HTTPS**］）を設定します。
   3. Mobile Service Providerサービスのサービスポート（通常、80または443）を設定します。
      注：ポート443を使用する場合は、IISのこのポートにバインドされたSSL証明書が必要です。
   4. 承認グループまたはユーザーを設定します。これにより、XenMobileからMobile Service Providerサービスに接続できる

ユーザーまたは一連のユーザーが設定されます。

5. ActiveSyncクエリを有効または無効に設定します。
   注：XenMobileサーバーでActiveSyncクエリが有効の場合は、Exchange Serverのスナップショットの種類を［**Deep**］に設定する必要があります。これにより、スナップショットの取得に重大なパフォーマンスコストがかかる場合があります。
6. 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。 必要に応じてこの動作を変更するには、［**Filter ActiveSync**］フィールドを変更します。
   注：空白は、すべてのデバイスがXenMobileに転送されることを意味します。
7. ［**Save**］をクリックします。

9. 任意で、1つまたは複数のBlackBerry Enterprise Server（BES）を構成します。
   1. ［**Add**］をクリックします。
   2. BES SQL Serverのサーバー名を入力します。



   3. BES管理データベースのデータベース名を入力します。
   4. 認証モードを選択します。［Windows Integrated authentication］を選択する場合、XenMobile Mail Managerサービスのユーザーアカウントが、BES SQL Serverへの接続に使用するアカウントになります。
      注：XenMobile Mail Managerデータベース接続に対しても［Windows Integrated］を選択している場合は、ここで指定したWindowsアカウントにXenMobile Mail Managerデータベースへのアクセスも付与する必要があります。
   5. ［**SQL authentication**］を選択する場合は、ユーザー名とパスワードを入力します。

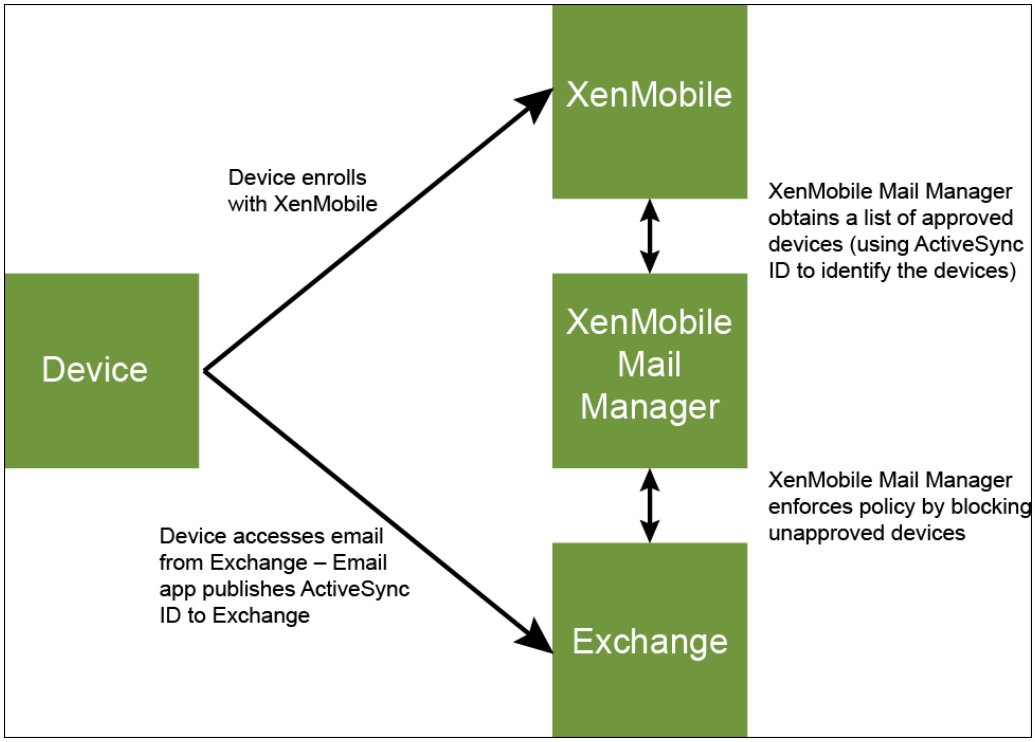
6. **[Sync Schedule]**を設定します。これは、BES SQL Serverへの接続とデバイス更新のチェックに使用するスケジュールです。
7. **[Test Connectivity]**をクリックして、SQL Serverへの接続をテストします。
   注：［Windows Integrated］を選択している場合、このテストでは、XenMobile Mail Managerサービスのユーザーではなく、現在ログオンしているユーザーが使用されるため、SQL認証が正確にテストされません。
8. XenMobileからのBlackBerryデバイスのリモートでのワイプやResetPasswordをサポートする場合は、**[Enabled]**チェックボックスをオンにします。
   1. BESの完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を入力します。
   2. 管理者Webサービスで使用するBESポートを入力します。
   3. BESサービスに必要な完全修飾ユーザー名とパスワードを入力します。
   4. **[Test Connectivity]**をクリックして、BESへの接続をテストします。
   5. **[Save]**をクリックします。

ActiveSync IDによるメールポリシーの適用

Aug 02, 2016

企業のメールポリシーによっては、特定のデバイスで企業メールを使用することが認められない場合があります。 このポリシーに従うには、そのようなデバイスから従業員が企業メールにアクセスできないようにする必要があります。 XenMobile Mail ManagerおよびXenMobileを連携させ、そのようなメールポリシーを適用することができます。 XenMobileで企業メールアクセスのポリシーを設定し、未承認のデバイスがXenMobileに登録されたときにXenMobile Mail Managerでポリシーを適用します。

デバイス上のメールクライアントはデバイスIDを使用してExchange Server（またはOffice 365）にクライアントの存在を通知します。このIDはActiveSync IDとしても知られており、デバイスを一意に識別するために使用されます。 Worx Homeでは同様の識別子を取得し、デバイスが登録されるとXenMobileにこの識別子を送信します。 XenMobile Mail Managerで2つのデバイスIDを比較することによって、特定のデバイスに企業メールへのアクセスを許可するかどうかが判定されます。 次の図は、この概念を示しています。



デバイスがExchangeに公開したIDと異なるActiveSync IDがXenMobileからXenMobile Mail Managerに送信されると、XenMobile Mail ManagerからExchangeに対してそのデバイスに対する処理を指示できません。

ほとんどのプラットフォームでActiveSync IDのマッチングは確実に動作しますが、一部のAndroidの実装で、デバイスが送信するActiveSync IDとメールクライアントがExchangeに通知するIDが異なることが判明しています。 この問題を緩和するため、次のことを実行できます。

- Samsung SAFEプラットフォームでは、デバイスのActiveSync構成をXenMobileからプッシュします。
- ほかのすべてのAndroidプラットフォームでは、XenMobileからTouchdownアプリとTouchdown ActiveSync構成の両方をXenMobileからプッシュします。

ただし、これにより従業員がAndroidデバイスにTouchdown以外のメールクライアントをインストールすることを防げるわけ

ではありません。 企業メールアクセスポリシーの適切な適用を保証するために、セキュリティについて防御的なスタンスをとり、静的なポリシーを［Deny by default］に設定することでXenMobile Mail Managerでメールを禁止するように構成することができます。 これは、従業員がAndroidデバイスにTouchdown以外のメールクライアントを構成し、ActiveSync IDの検出が適切に動作しない場合は、従業員は企業メールへのアクセスを拒否されるということを意味します。

アクセス制御規則

Oct 25, 2016

XenMobile Mail Managerでは、Exchange ActiveSyncデバイスのアクセス制御を動的に構成するための、規則に基づく手法が提供されます。 XenMobile Mail Managerのアクセス制御規則は、一致式と目的のアクセス状態（許可またはブロック）の2つで構成されます。 特定のExchange ActiveSyncデバイスに対して規則を評価して、その規則がデバイスに適用されるかどうか、またはデバイスと一致するかどうかを判別できます。 一致式にはいくつかの種類があります。たとえば、規則は、特定のデバイスの種類のすべてのデバイス、特定のExchange ActiveSyncデバイスID、特定のユーザーのすべてのデバイスと一致するなどの条件を指定できます。

規則一覧の規則を追加、削除、および並べ替えているときに **[Cancel]** をクリックすると、規則一覧が最初に開いたときの状態に戻ります。 **[Save]** をクリックしない限り、構成ツールを閉じるとこのウィンドウに対して加えた変更が失われます。

XenMobile Mail Managerには、ローカル規則、XenMobileサーバー規則（別名XDM規則）、およびデフォルトのアクセス規則の3種類の規則があります。

ローカル規則： ローカル規則が最も優先されます。デバイスがローカル規則と一致すると、規則の評価は停止します。XenMobileサーバー規則とデフォルトのアクセス規則は参照されません。 ローカル規則は、［Configure］、［Access Rules］の順にクリックし、［Local Rules］タブから、XenMobile Mail Managerに対してローカルに構成します。 サポート一致は、特定のActive Directoryグループ内のユーザーのメンバーシップに基づきます。 サポート一致は、次のフィールドの正規表現に基づきます。

- Active SyncデバイスID
- ActiveSyncデバイスの種類
- ユーザープリンシパル名（User Principal Name：UPN）
- ActiveSyncユーザーエージェント（通常、デバイスプラットフォームまたはメールクライアント）

メジャースナップショットが完了し、デバイスが検出されている限り、通常の規則または正規表現の規則のいずれかを追加できます。 メジャースナップショットが完了していない場合、正規表現の規則のみを追加できます。

XenMobileサーバー規則： XenMobileサーバー規則は、管理対象デバイスに関する規則を提供する外部のXenMobileサーバーへの参照です。 XenMobileサーバーは、デバイスがジェイルブレイク済みかどうかや、デバイスに禁止アプリケーションが含まれているかどうかなど、XenMobileが認識しているプロパティに基づいてデバイスが許可されるか、ブロックされるかを識別する独自の高レベルの規則を使用して構成できます。 XenMobileでは、高レベルの規則が評価され、許可またはブロックする一連のActiveSyncデバイスIDが生成されて、これらがXenMobile Mail Managerに配信されます。

デフォルトのアクセス規則： デフォルトのアクセス規則は、すべてのデバイスと一致する可能性があり、常に最後に評価されるという点で独特です。 この規則は、あらゆる状況に対応できる規則です。つまり、特定のデバイスがローカル規則とXenMobleサーバー規則のいずれにも一致しない場合は、デフォルトのアクセス規則での目的のアクセス状態によってデバイスにおける目的のアクセス状態が決まります。

- Default Access – Allow。 ローカル規則とXenMobleサーバー規則のいずれにも一致しないすべてのデバイスが許可されます。
- Default Access – Block。 ローカル規則とXenMobleサーバー規則のいずれにも一致しないすべてのデバイスがブロックされます。
- Default Access - Unchanged。 ローカル規則とXenMobleサーバー規則のいずれにも一致しないすべてのデバイスのアクセス状態は、XenMobile Mail Managerによって変更されません。 ExchangeによってデバイスがQuarantineモードになっている場合、アクションは実行されません。たとえば、Quarantineモードからデバイスを削除する方法は、ローカル規則またはXDM規則で隔離を明示的に上書きすることのみです。

規則の評価について

ExchangeからXenMobile Mail Managerに報告されるデバイスごとに、次のように優先度の高い順に規則が評価されます。

- ローカル規則
- デフォルトのアクセス規則
- XenMobileサーバー規則

一致が検出されると、評価は停止します。 たとえば、ローカル規則が特定のデバイスと一致すると、そのデバイスはXenMobileサーバー規則とデフォルトのアクセス規則のどちらに対しても評価されません。 このことは、特定の種類の規則内でも当てはまります。 たとえば、ローカル規則一覧で特定のデバイスに対する一致が複数ある場合でも、最初の一致が見つかった時点で評価は停止します。

デバイスプロパティが変更されたとき、デバイスが追加または削除されたとき、または規則自体が変更されたときは、現在定義されている一連の規則がXenMobile Mail Managerによって再評価されます。 メジャースナップショットにより、構成可能な間隔でデバイスのプロパティ変更または削除が確認されます。 マイナースナップショットにより、構成可能な間隔で新しいデバイスが確認されます。

Exchange ActiveSyncにも、アクセスを管理する規則があります。 XenMobile Mail Managerのコンテキストでこれらの規則がどのように機能するかを理解することが重要です。 Exchangeは、個人の適用除外、デバイスの規則、組織の設定という3つのレベルの規則で構成できます。 XenMobile Mail Managerでは、リモートPowerShell要求をプログラムで発行して個人の適用除外一覧に反映させることで、アクセス制御を自動化します。 これらは、特定のメールボックスに関連する、許可またはブロックするExchange ActiveSyncデバイスIDの一覧です。 展開すると、XenMobile Mail ManagerはExchange内の適用除外一覧の管理機能を効果的に引き継ぎます。 詳細については、このMicrosoftの技術文書を参照してください。

分析は、同じフィールドに対して複数の規則が定義されている場合に特に便利です。 規則間の関係をトラブルシューティングできます。 規則フィールドの観点から分析を実行します。たとえば、ActiveSyncデバイスID、ActiveSyncデバイスの種類、ユーザー、ユーザーエージェントなどの照合されるフィールドに基づくグループで規則が分析されます。

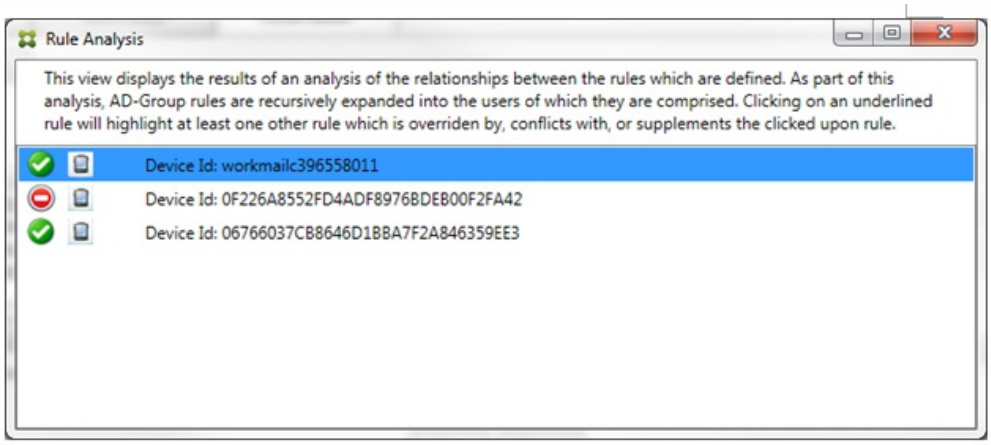
規則の用語：

- **上書き規則**。 同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。 一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- **競合規則**。 同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。 競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- **補足規則**。 正規表現の規則が複数あるので、2つ（またはそれ以上）の正規表現を1つの正規表現の規則に結合できるか、またはそれらの機能が重複していないようにする必要がある場合に補足が発生します。 補足規則もアクセス（許可/ブロック）で競合する場合があります。
- **プライマリ規則**。 プライマリ規則は、ダイアログボックス内でクリックされた規則です。 この規則は、実線の罫線で囲まれて示されます。 この規則には、上方向または下方向を指す1つまたは2つの緑色の矢印も示されます。 矢印が上方向を指している場合は、プライマリ規則よりも優先される補助規則があることを示しています。 矢印が下方向を指している場合は、プライマリ規則よりも優先度の低い補助規則があることを示しています。 アクティブにできるプライマリ規則は、常に1つのみです。
- **補助規則**。 補助規則は、上書き、競合、または補足の関係のいずれかで、プライマリ規則と何らかの関係を持ちます。 この規則は、破線の罫線で囲まれて示されます。 各プライマリ規則に対して、1対多の補助規則を指定できます。 下線付きのエントリをクリックしたときに強調表示される補助規則は、常にプライマリ規則の観点から示されます。 たとえば、補助規則がプライマリ規則によって上書きされたり、プライマリ規則とアクセスで競合したり、プライマリ規則を補足したりします。

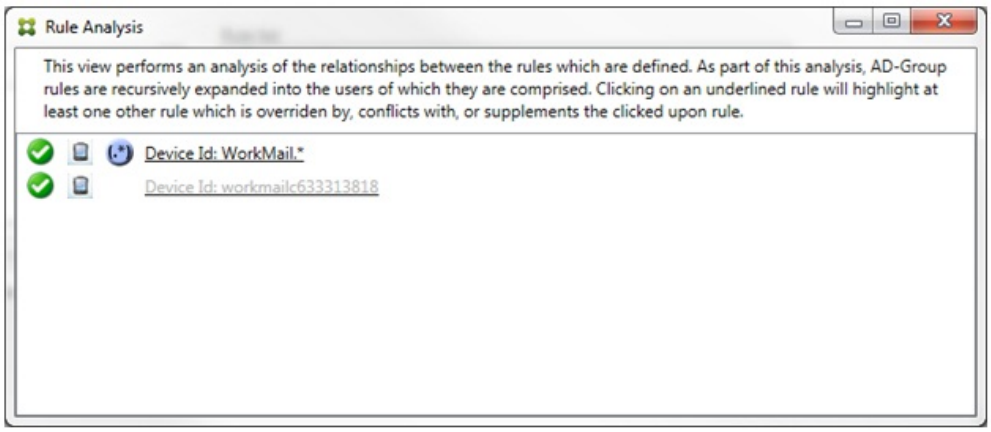
［Rule Analysis］ダイアログボックスのルールの種類の外観

競合、上書き、または補足がない場合、［Rule Analysis］ダイアログボックスに下線付きのエントリは表示されません。 どのアイテムをクリックしても影響はありません。通常の選択済みアイテムの表示になります。

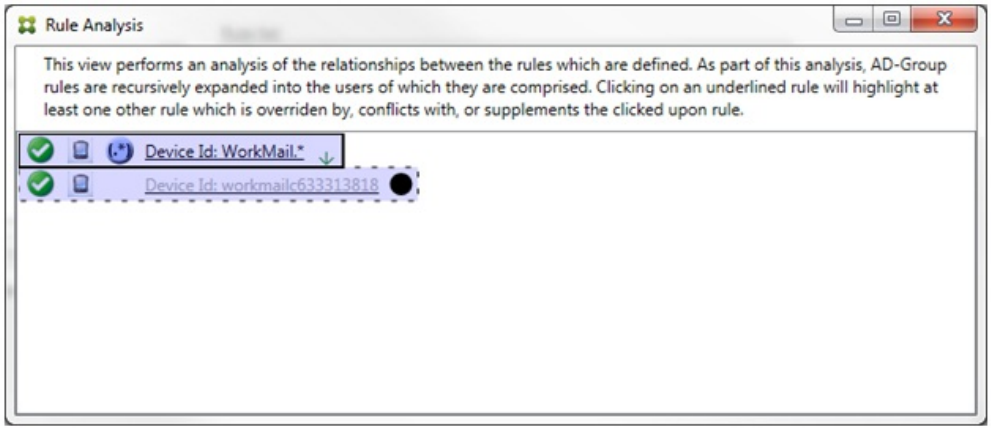
［Rule Analysis］ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。



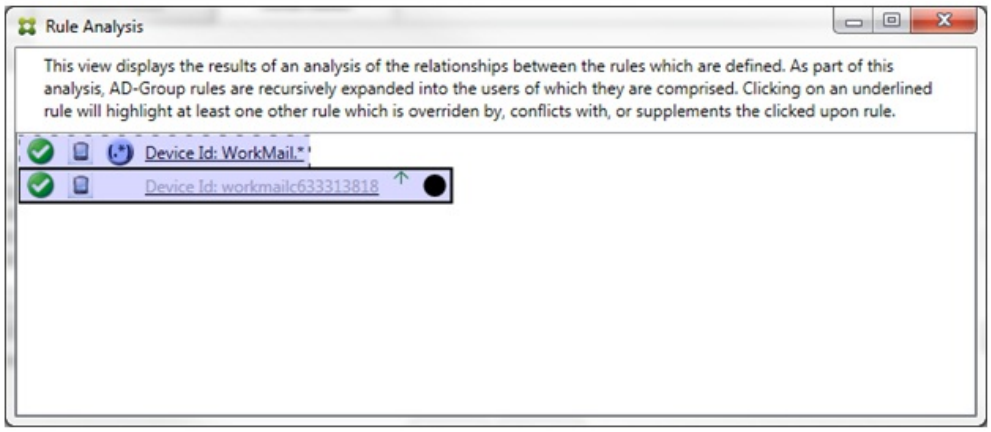
上書きが発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。 1つまたは複数の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。 上書きされた規則をクリックして、その規則を上書きした規則を確認できます。 規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。 たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます。



最も優先度の高い規則をクリックすると、ダイアログボックスの表示は次のようになります。

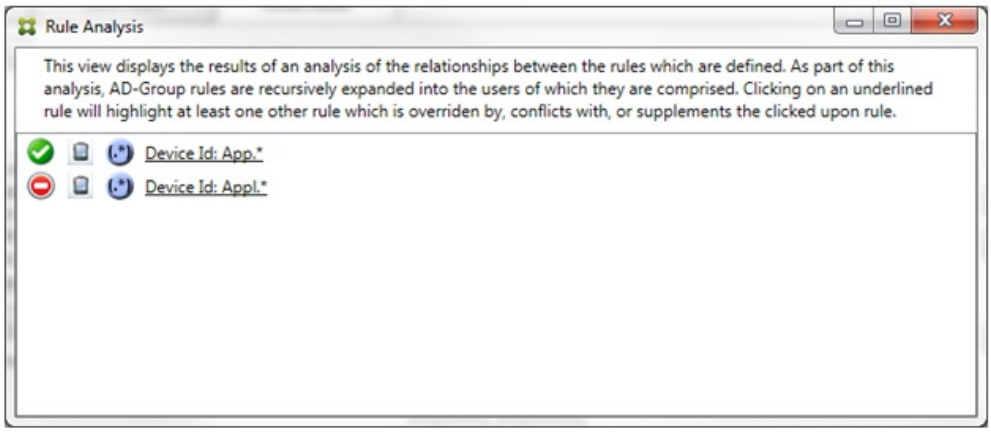


この例では、正規表現の規則WorkMail.*がプライマリ規則（実線の罫線で表示）で、通常の規則workmailc633313818が補助規則（破線の罫線で表示）です。 補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。 上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります。

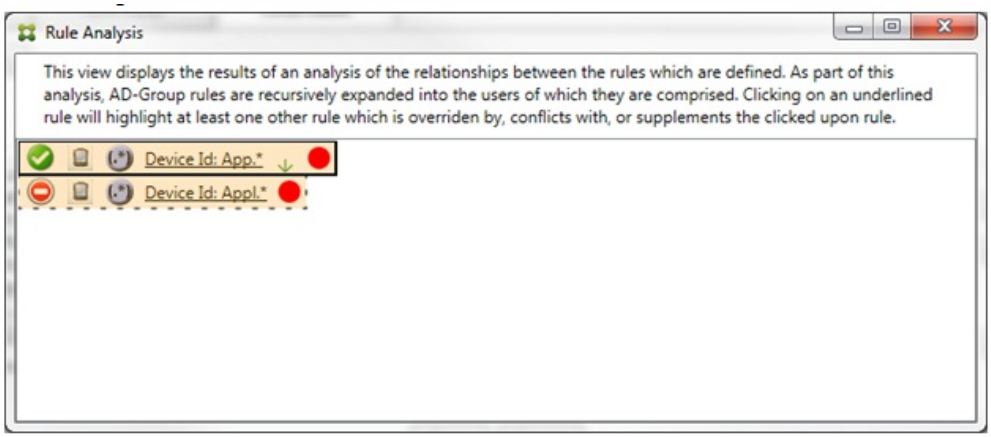


上記の例では、正規表現の規則WorkMail.*が補助規則（破線の罫線で表示）で、通常の規則workmailc633313818がプライマリ規則（実線の罫線で表示）です。 こうしたシンプルな例では、大きな違いはありません。 より複雑な例については、このトピックで後述する複雑な式の例を参照してください。 多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

競合が発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。 競合している規則は赤色の点で示されます。 相互に競合のみが発生している規則は、2つ以上の正規表現の規則が定義されている場合に限り発生します。 ほかのすべての競合のシナリオでは、競合のみではなく、上書きも発生します。 シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます。

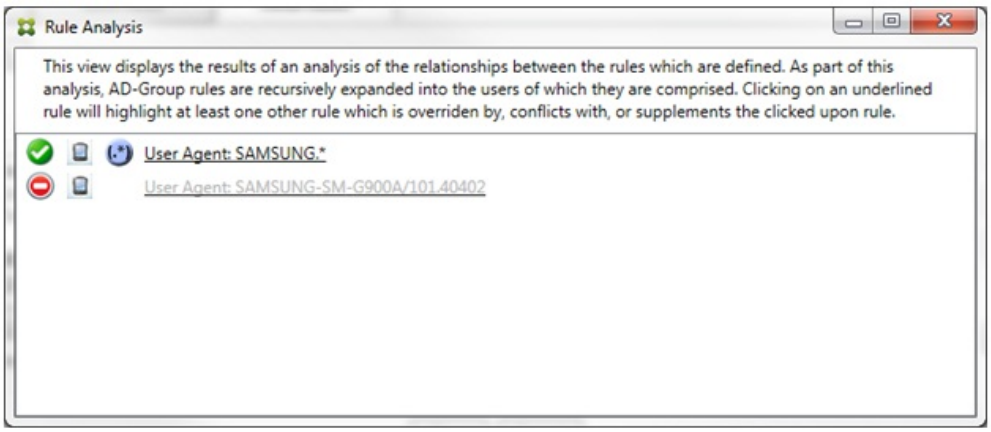


2つの正規表現の規則を確認すると、最初の規則で「App」がデバイスIDに含まれるすべてのデバイスを許可し、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスを拒否することがわかります。 さらに、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは決して拒否されません。 最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



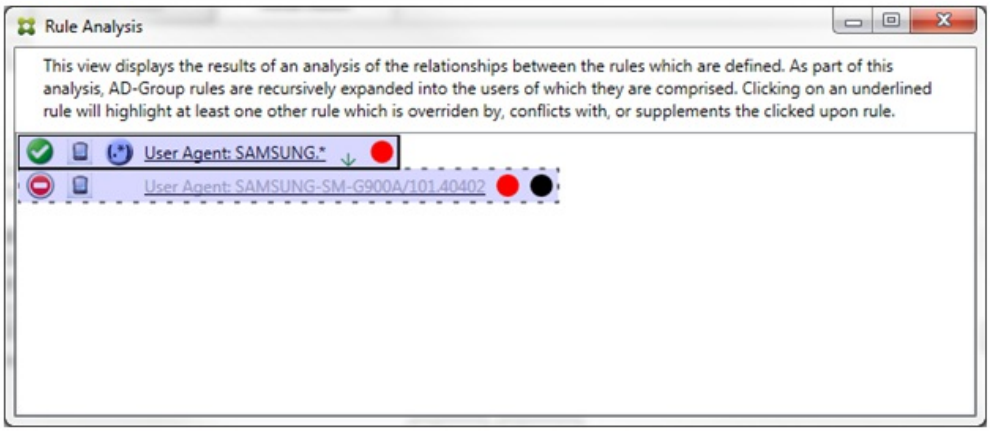
前述のシナリオでは、プライマリ規則（正規表現の規則App.*）と補助規則（正規表現の規則Appl.*）の両方が黄色で強調表示されます。 これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

競合と上書きの両方を含むシナリオでは、プライマリ規則（正規表現の規則App.*）と補助規則（正規表現の規則Appl.*）の両方が黄色で強調表示されます。 これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。



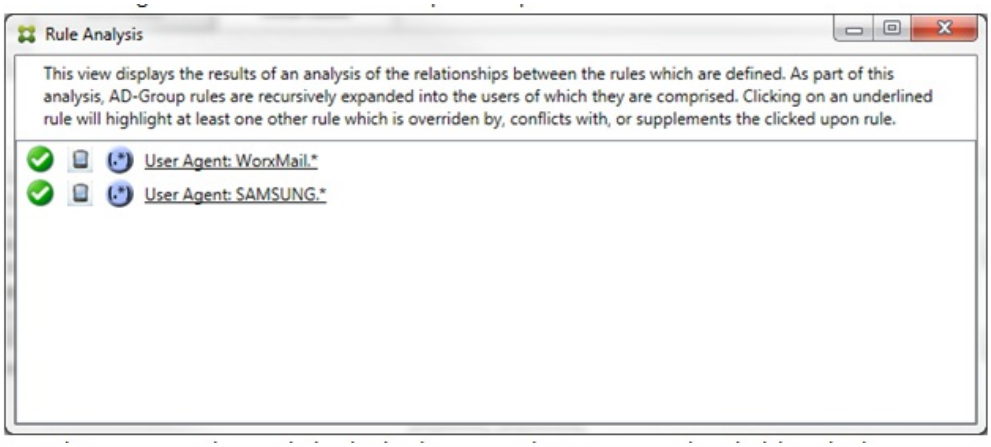
上記の例では、最初の規則（正規表現の規則SAMSUNG.*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。 2つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

正規表現の規則をクリックすると、ダイアログボックスの表示は次のようになります。

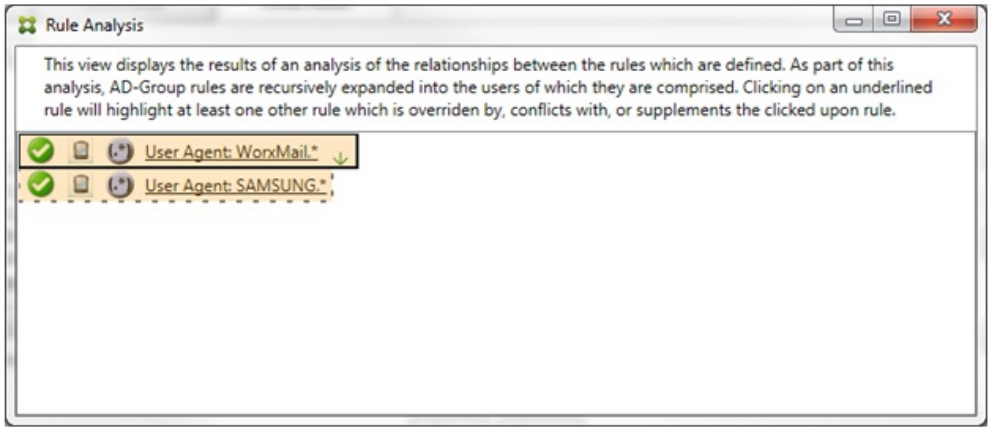


プライマリ規則（正規表現の規則SAMSUNG.*）の末尾には赤色の点が付けられて、アクセス状態が1つまたは複数の補助規則と競合していることが示されます。 補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には、アクセス状態がプライマリ規則と競合していることを示す赤色の点に加えて、その規則が上書きされて非アクティブであることを示す黒点が付けられます。

2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。 相互に補足のみが発生している規則には、正規表現の規則のみが定義されています。 相互に補足が発生している規則は、黄色のオーバーレイで示されます。 シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます。



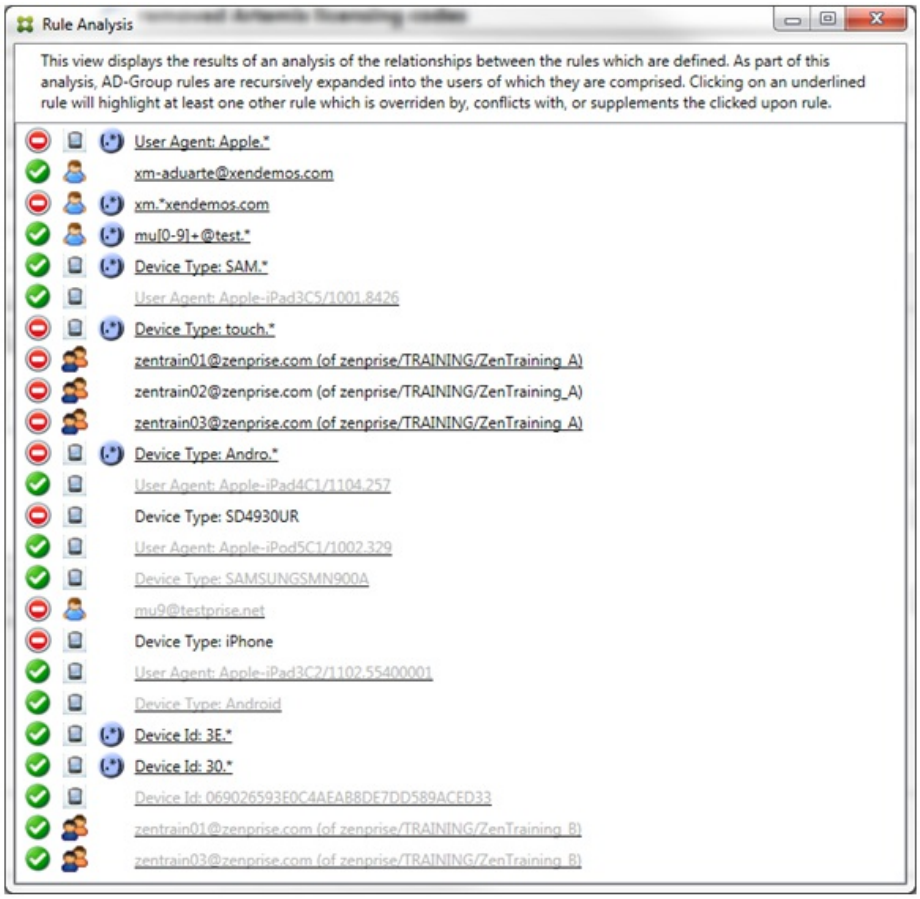
目視で確認すると、両方の規則が正規表現の規則で、両方ともXenMobile Mail Managerの［ActiveSync device ID］フィールドに適用されていることが容易にわかります。 最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



プライマリ規則（正規表現の規則WorxMail.*）が黄色のオーバーレイで強調表示され、正規表現の補助規則がほかに1つ以上存在することが示されます。 補助規則（正規表現の規則SAMSUNG.*）が黄色のオーバーレイで強調表示され、この規則とプライマリ規則の両方が、XenMobile Mail Manager内の同じフィールド（この場合は、［ActiveSync device ID］フィールド）に適用されている正規表現の規則であることが示されます。正規表現は重複する場合としない場合があります。 正規表現が適切に作成されているかどうかの判断は、ユーザーに委ねられます。

複雑な式の例

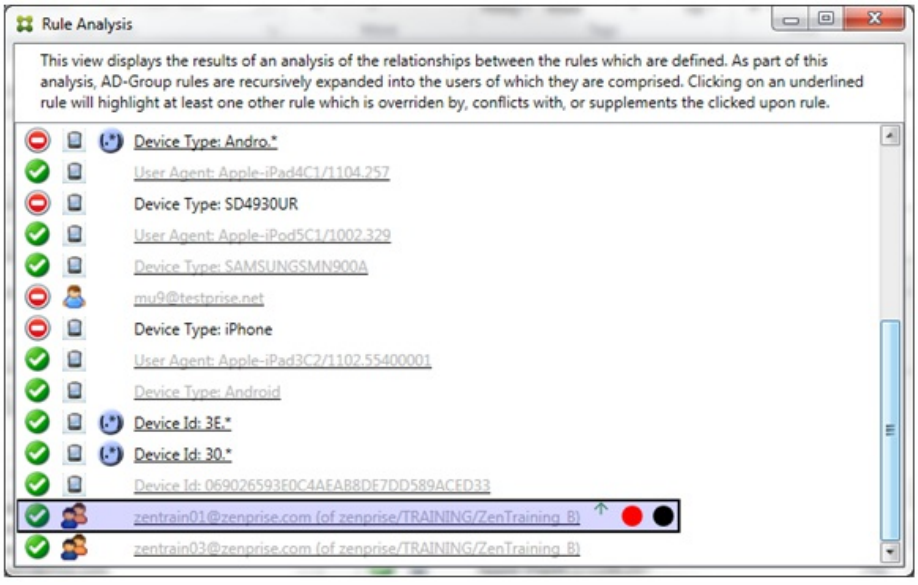
発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。 次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。 次の図では、ほとんどのアイテムに下線が付けられています。 多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。 同様に、(.*) アイコンで示される多数の正規表現の規則も一覧に含まれています。



上書きの分析方法

特定の規則を上書きした規則を確認するには、その規則をクリックします。

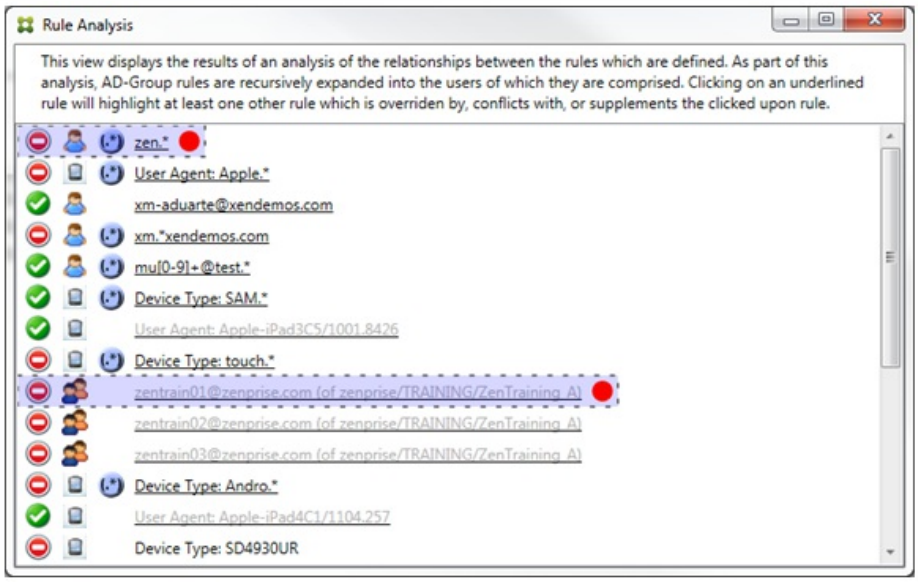
例1：この例では、zentrain01@zenprise.comが上書きされた理由を調べます。



このプライマリ規則（zentrain01@zenprise.comがメンバーとして属するADグループ規則zenprise/TRAINING/ZenTraining B）には、次の特性があります。

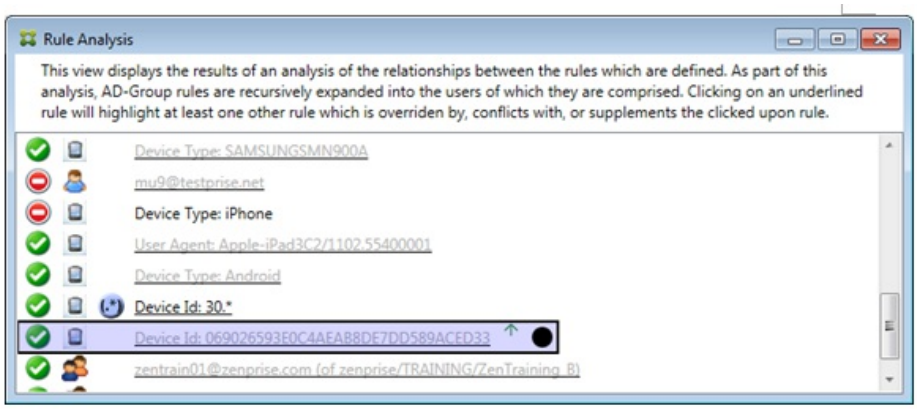
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（すべての補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、1つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます。



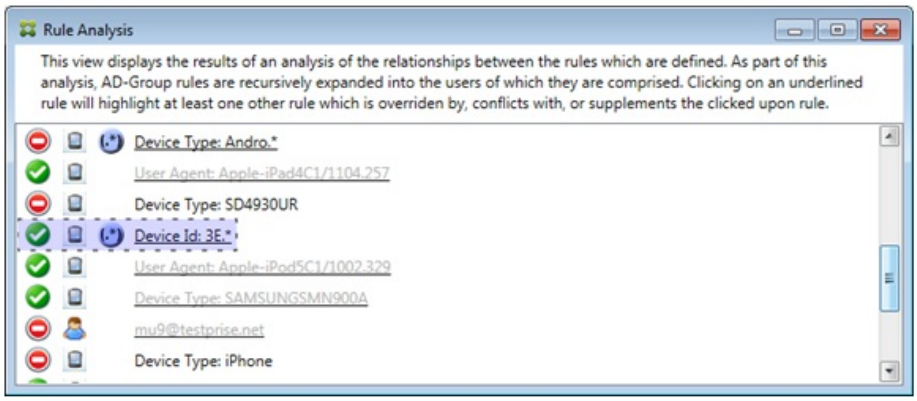
この場合、プライマリ規則を上書きする2つの補助規則（正規表現の規則zen.*と通常の規則zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)）があります。 後者の補助規則の場合、Active Directoryグループ規則ZenTraining Aにユーザーzentrain01@zenprise.comが含まれる一方で、Active Directoryグループ規則ZenTraining Bにもユーザーzentrain01@zenprise.comが含まれることになります。 ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、プライマリ規則は上書きされています。 プライマリ規則のアクセスが許可で、両方の補助規則のアクセスがブロックであるので、これらすべての末尾に赤色の点が付けられて、アクセスが競合していることも示されています。

例2：次の例は、ActiveSyncデバイスIDが069026593E0C4AEAB8DE7DD589ACED33であるデバイスが上書きされた理由を示しています。



このプライマリ規則（通常のデバイスIDの規則069026593E0C4AEAB8DE7DD589ACED33）には、次の特性があります。

- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、補助規則がそのプライマリ規則を上書きして、非アクティブであることを示す黒色の円が付けられている。



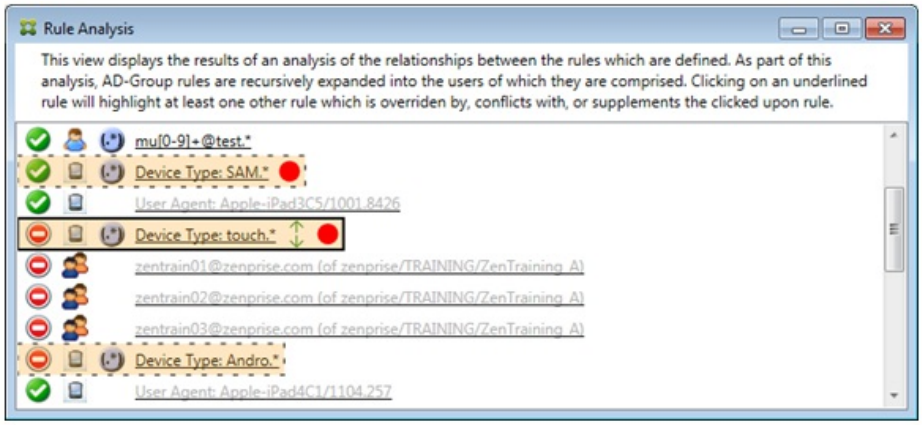
この場合、単一の補助規則（正規表現のActiveSyncデバイスIDの規則3E.*）がプライマリ規則を上書きします。正規表現3E.*が069026593E0C4AEAB8DE7DD589ACED33に一致するので、プライマリ規則は評価されません。

補足および競合の分析方法

この場合、プライマリ規則は正規表現のActiveSyncデバイスの種類の規則touch.*です。特性は次のとおりです。

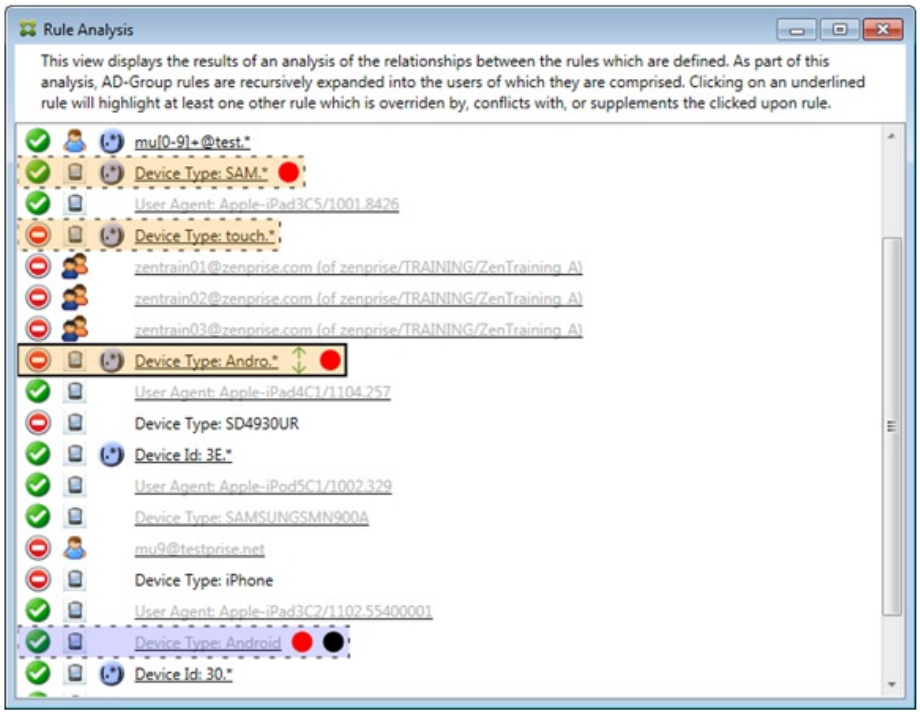
- 実線の罫線で囲まれ、特定の規則フィールド（この場合は、ActiveSyncデバイスの種類）に対して複数の正規表現の規則が使用されているという警告として、黄色のオーバーレイが適用されている。
- 上方向および下方向をそれぞれ指す2つの矢印が付けられ、より優先度の高い1つ以上の補助規則とより優先度の低い1つ以上の補助規則が存在することが示されている。
- 横に赤色の円が付けられ、1つ以上の補助規則のアクセスが許可に設定されて、プライマリ規則のアクセス状態のブロックと競合することが示されている。
- 2つの補助規則（正規表現のActiveSyncデバイスの種類の規則SAM.*と正規表現のActiveSyncデバイスの種類の規則Andro.*）が存在する。
- 両方の補助規則が破線の罫線で囲まれ、補助規則であることが示されている。

- 両方の補助規則に黄色のオーバーレイが適用され、ActiveSyncデバイスの種類の規則フィールドにこれらが補足として適用されていることが示されている。
- このようなシナリオでは、正規表現の規則が冗長でないようにする必要がある。



規則の高度な分析方法

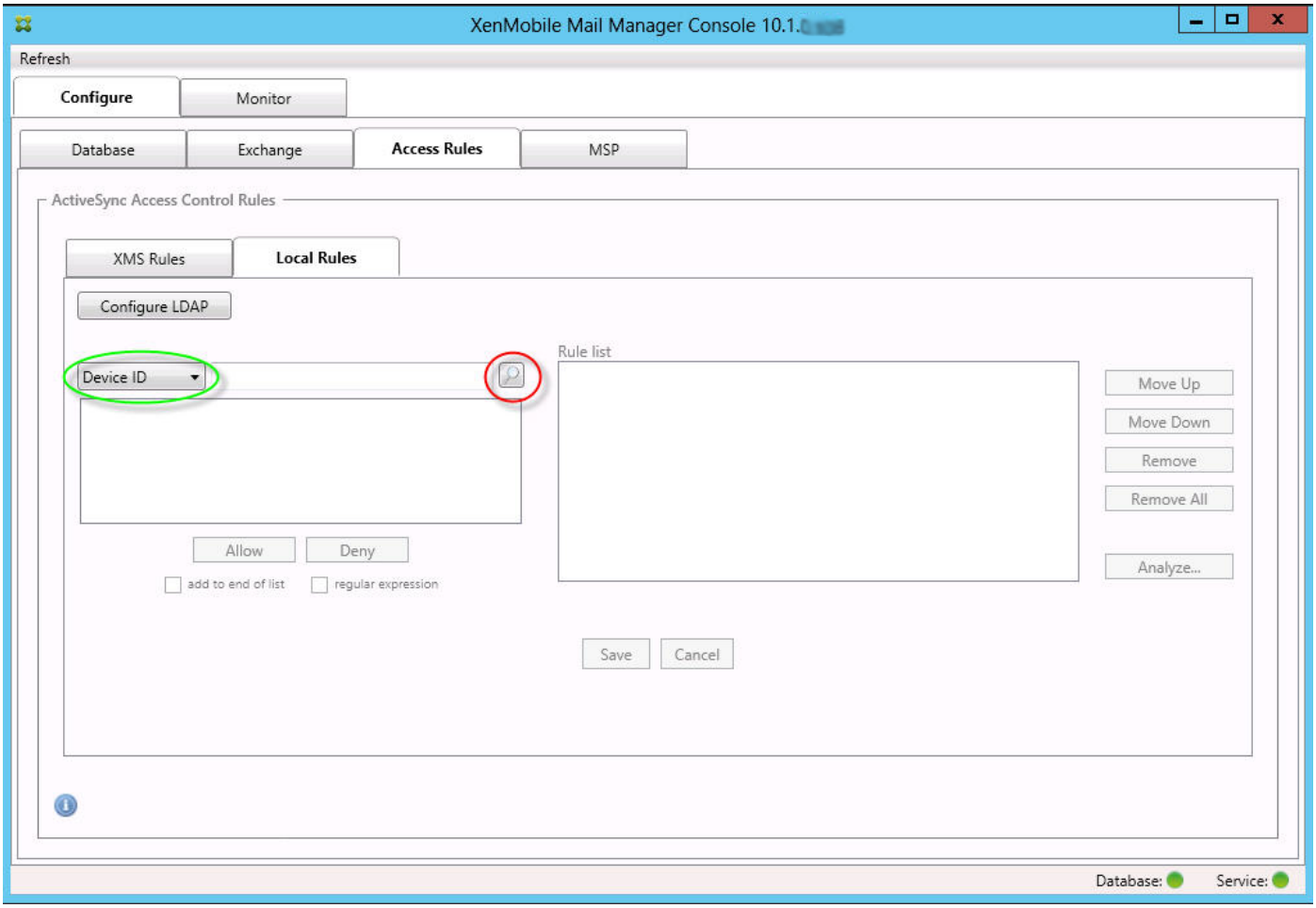
次の例では、規則の関係が常にプライマリ規則の観点から示されるしくみを確認します。 前述の例では、デバイスの種類の規則フィールドに適用され、値がtouch.*である正規表現の規則をクリックした場合を示しました。補助規則Andro.*をクリックすると、別の一連の補助規則が強調表示されます。



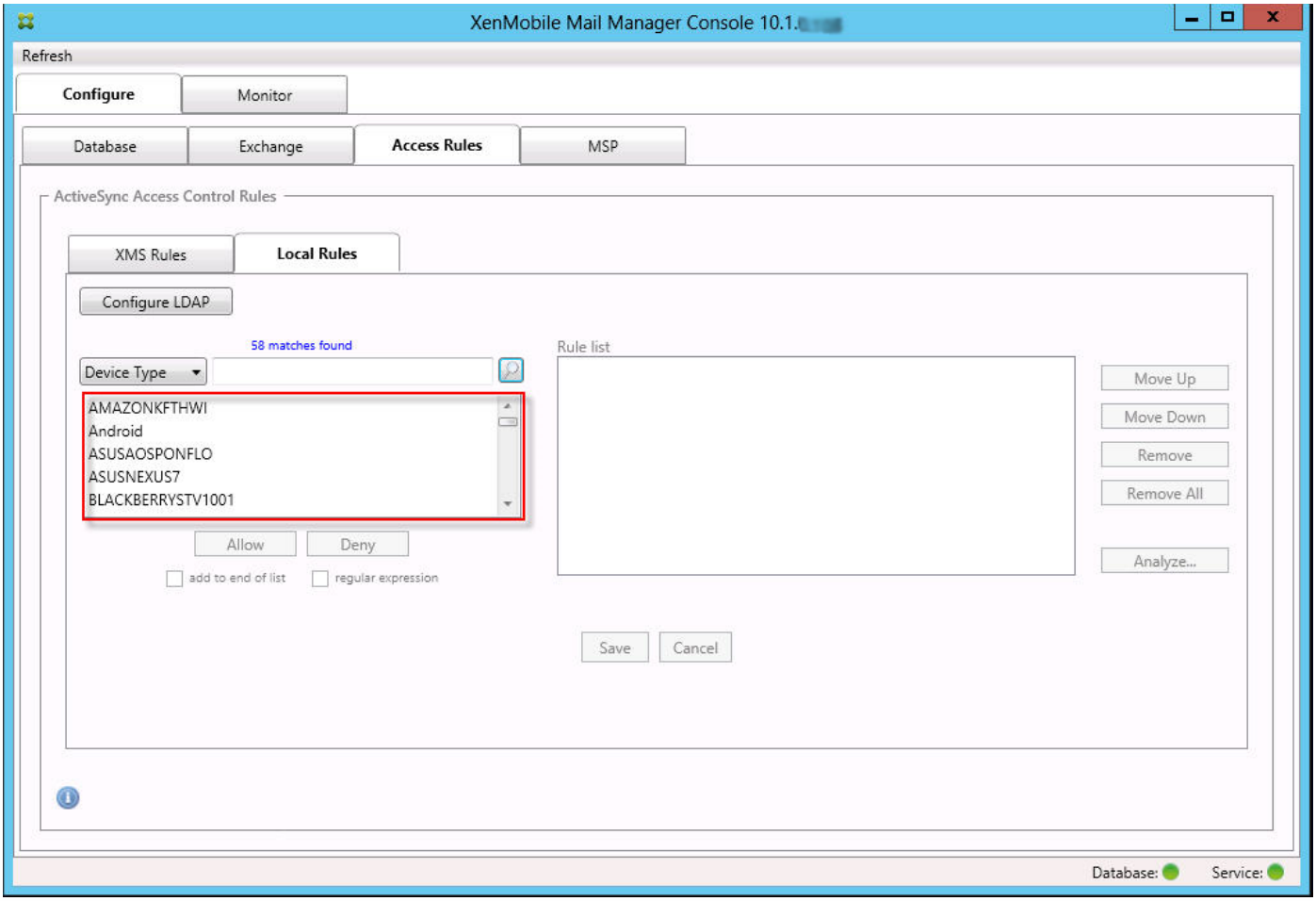
この例では、規則の関係に含まれる上書きされた規則が示されています。 この規則は、通常のActiveSyncデバイスの種類の規

則Androidです。この規則は上書きされ（淡色のフォントで示され、横に黒点が付けられています）、プライマリ規則（正規表現のActiveSyncデバイスの種類の規則Andro.*。この規則は、クリック前は補助規則でした）のアクセスと競合しています。前述の例では、その時点でのプライマリ規則（正規表現のActiveSyncデバイスの種類の規則touch.*）の観点からは関係しなかったので、通常のActiveSyncデバイスの種類の規則Androidは補助規則として表示されていませんでした。

1. ［Access Rules］タブをクリックします。

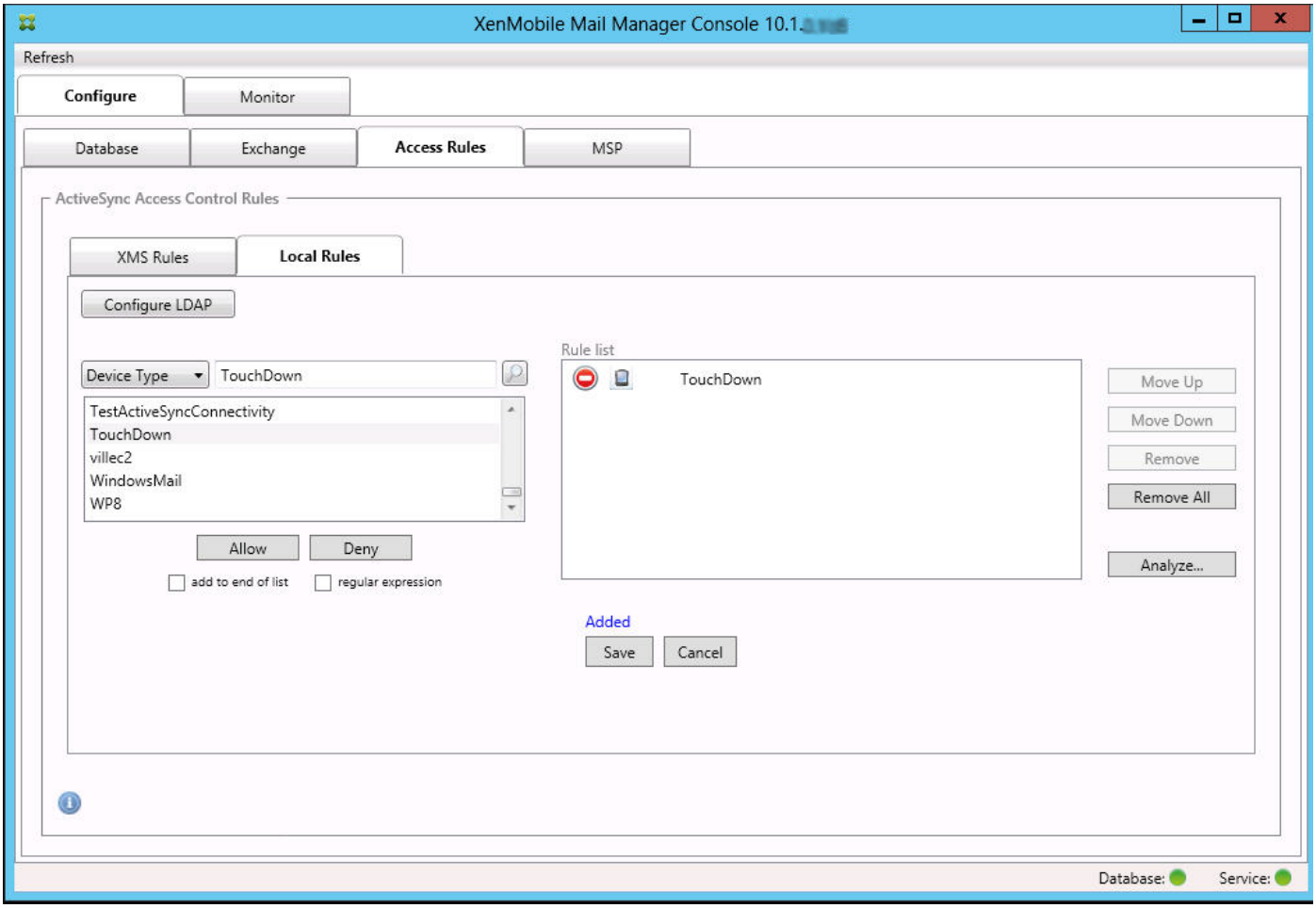


2. ［Device ID］一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。 この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 表示されたリストボックスでいずれかのアイテムをクリックして、次のいずれかのオプションをクリックします。
   - Allow：すべての一致するデバイスに対して、ActiveSyncトラフィックを許可するようにExchangeが構成されます。
   - Deny：すべての一致するデバイスに対して、ActiveSyncトラフィックを拒否するようにExchangeが構成されます。

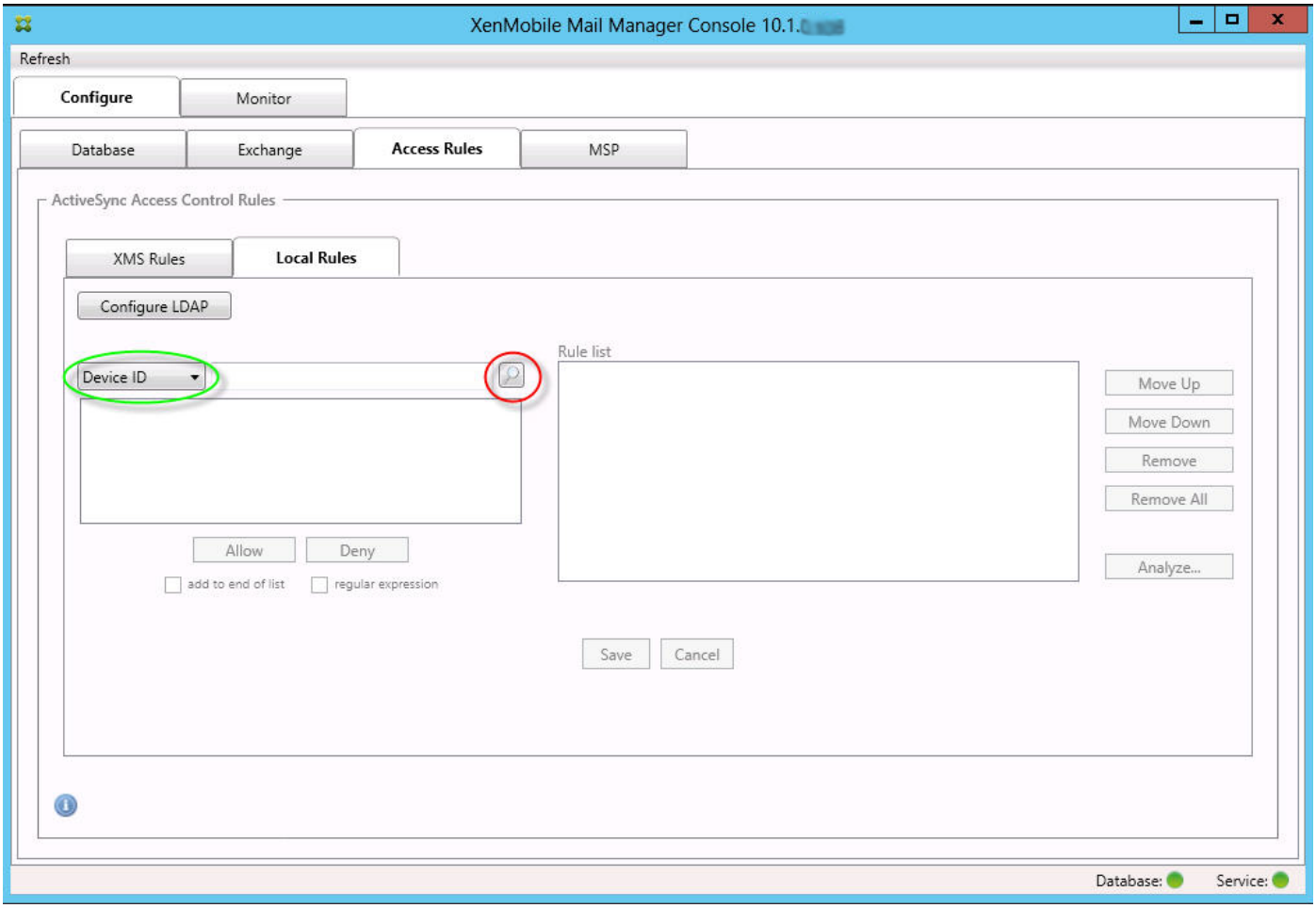
   この例では、デバイスの種類がTouchDownであるすべてのデバイスのアクセスが拒否されます。



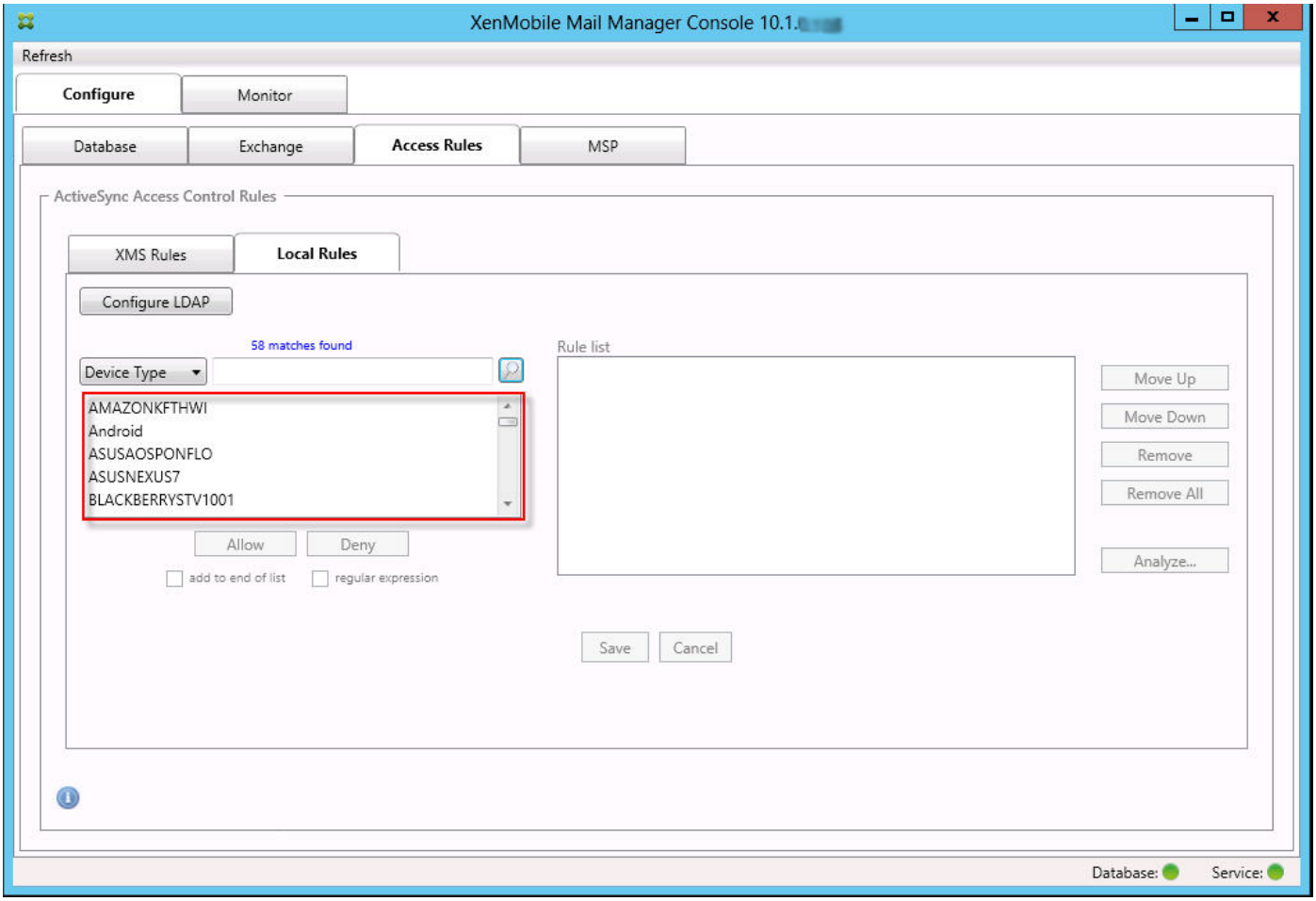
正規表現のローカル規則は、横に表示されるアイコンで識別できます。(.*)。 正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

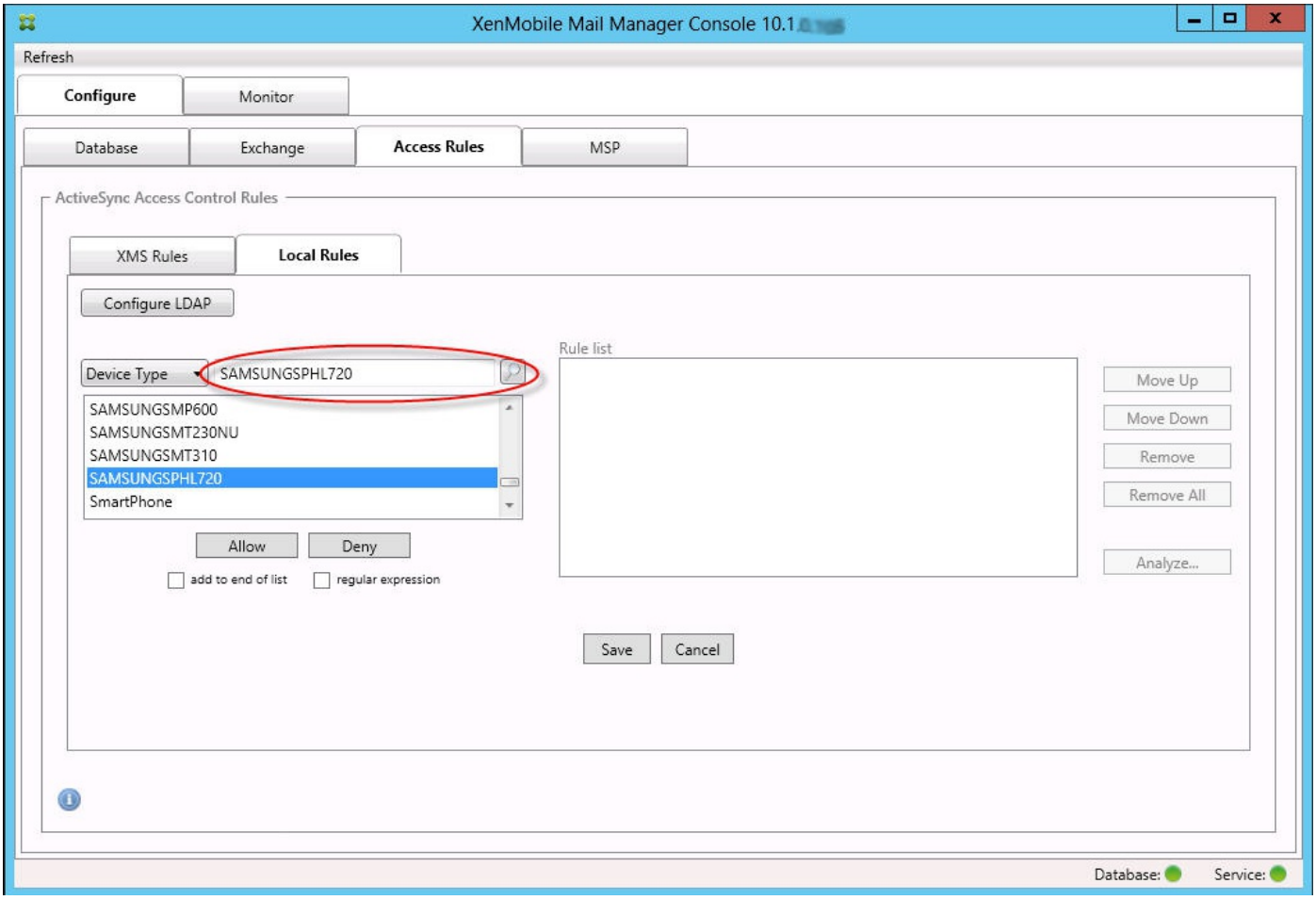
1. ［Access Rules］タブをクリックします。



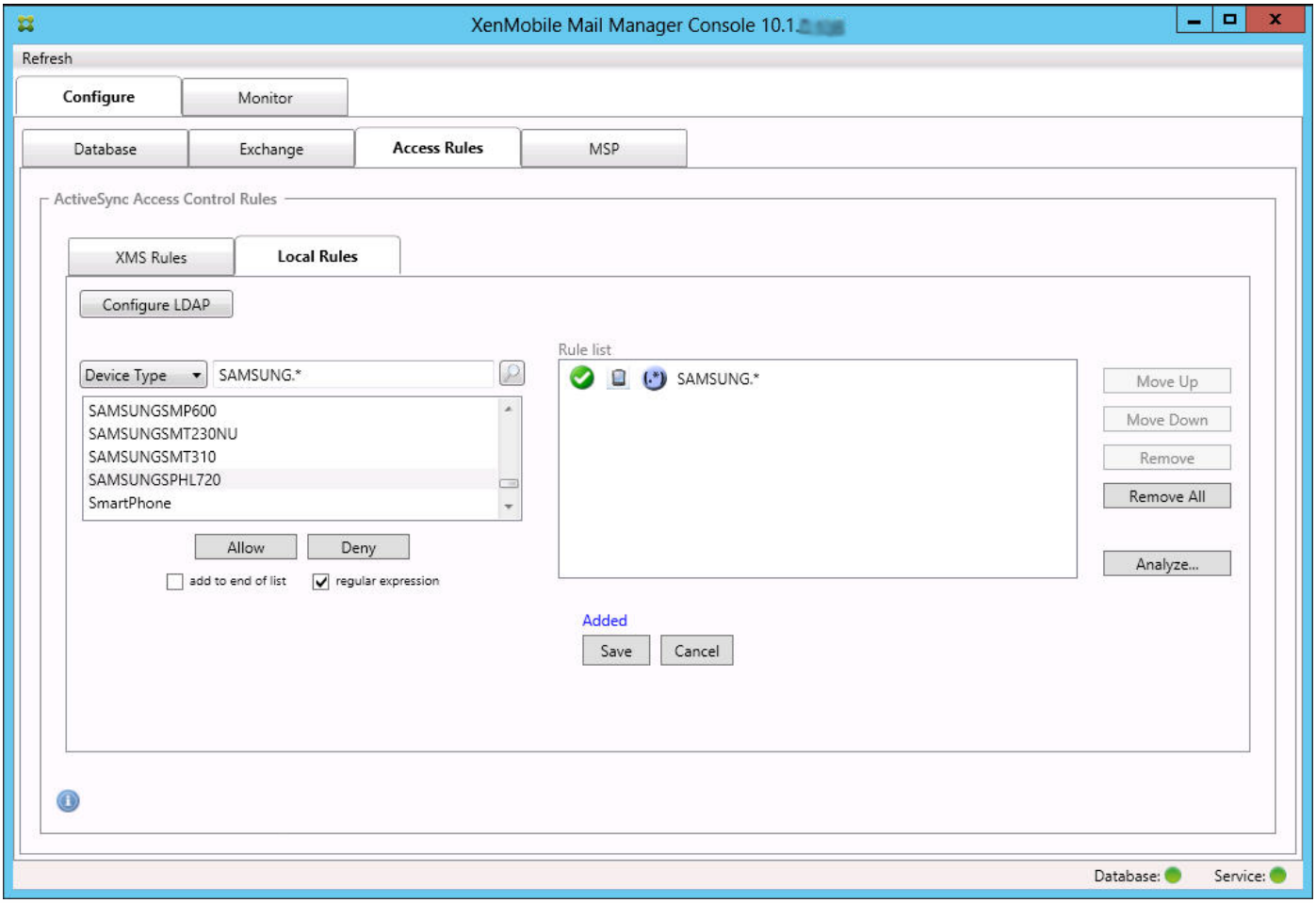
2. ［Device ID］一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。 この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



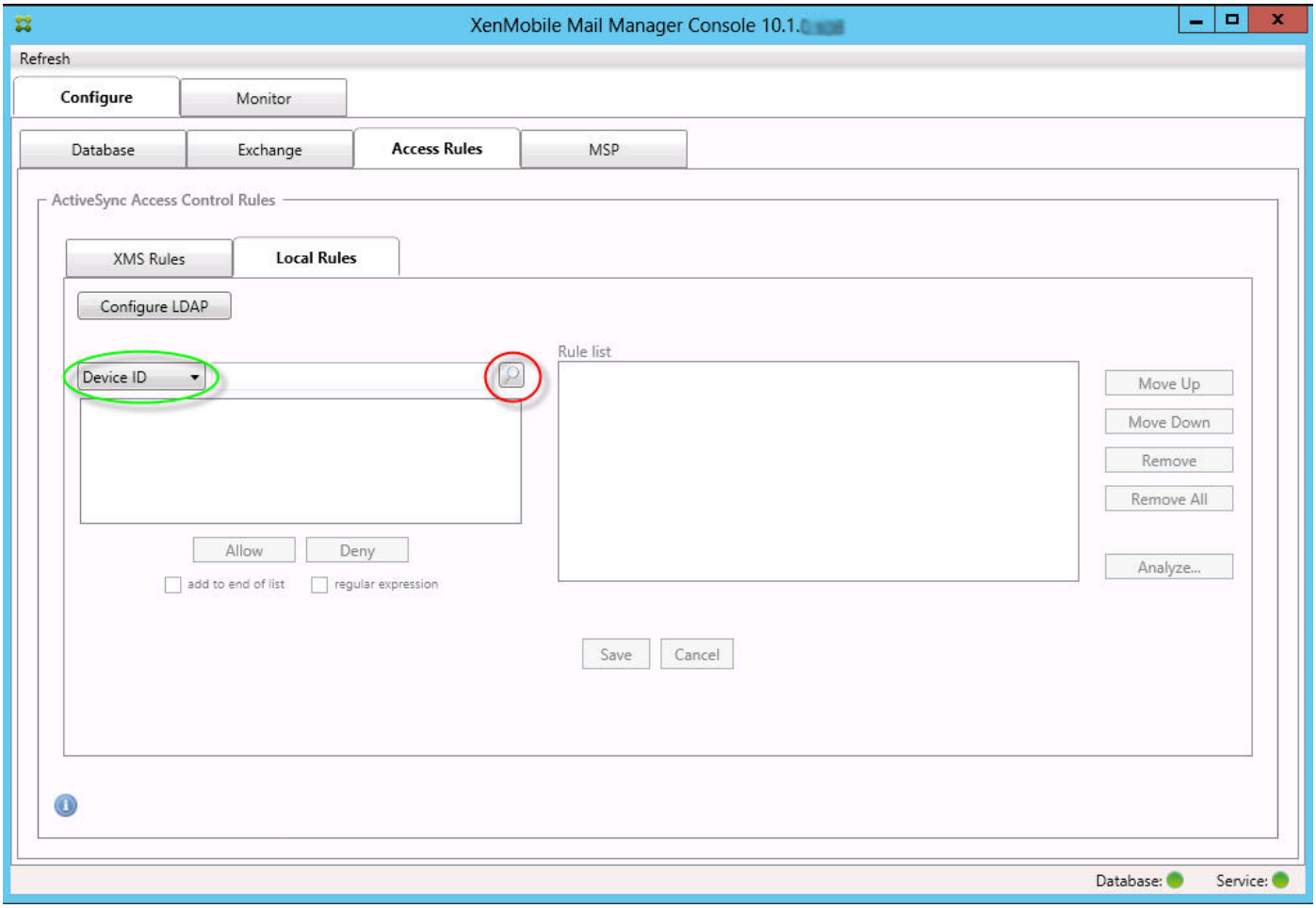
4. 結果一覧でいずれかのアイテムをクリックします。 この例では、SAMSUNGSPHL720が選択され、[Device Type]に隣接するテキストボックスに表示されています。



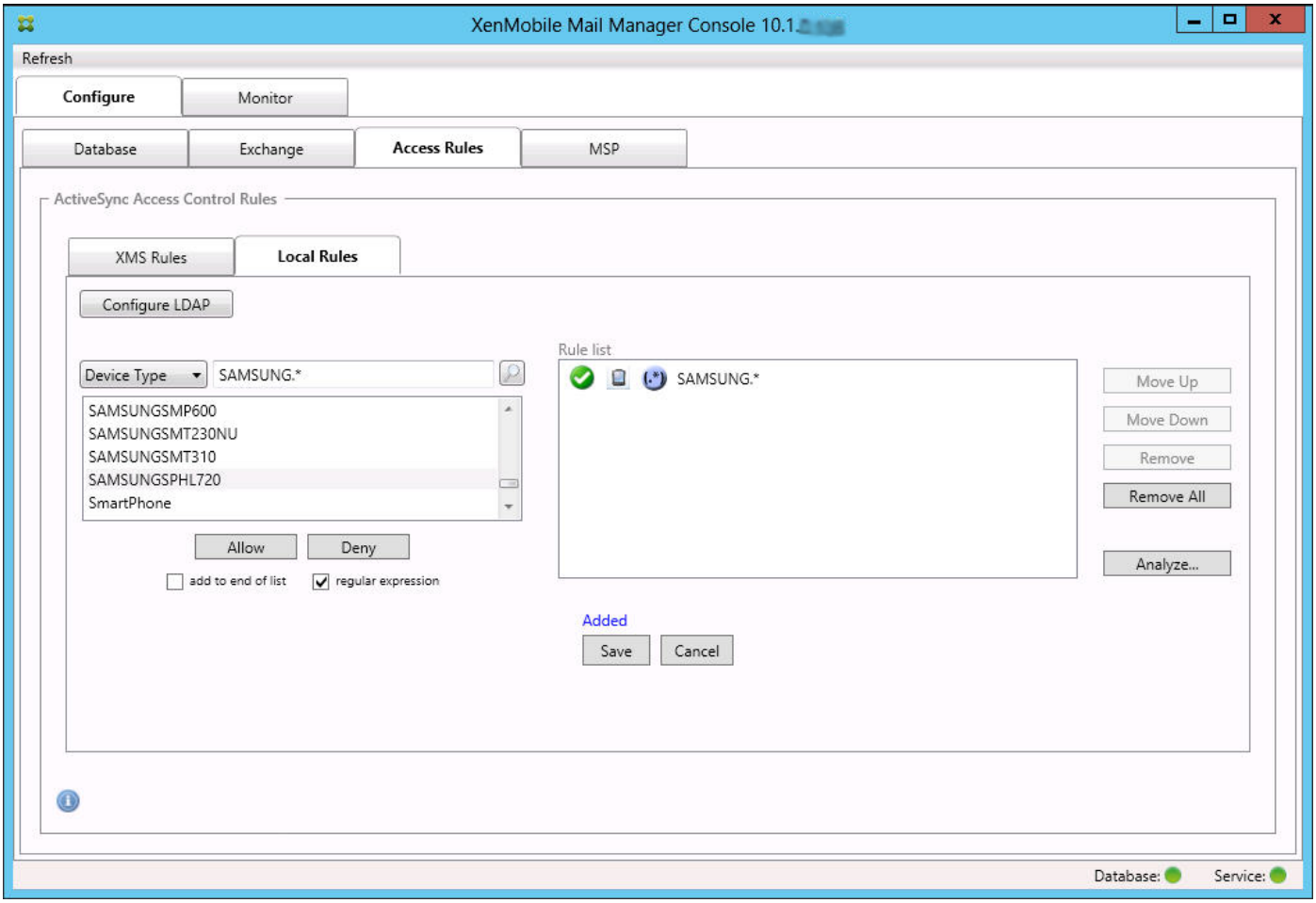
5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。
   1. 選択済みアイテムのテキストボックス内をクリックします。
   2. SAMSUNGSPHL720からSAMSUNG.*にテキストを変更します。
   3. ［regular expression］チェックボックスをオンにします。
   4. ［Allow］をクリックします。



1. ［Local Rules］タブをクリックします。
2. 正規表現を入力するには、［Device ID］一覧と選択済みアイテムのテキストボックスの両方を使用する必要があります。

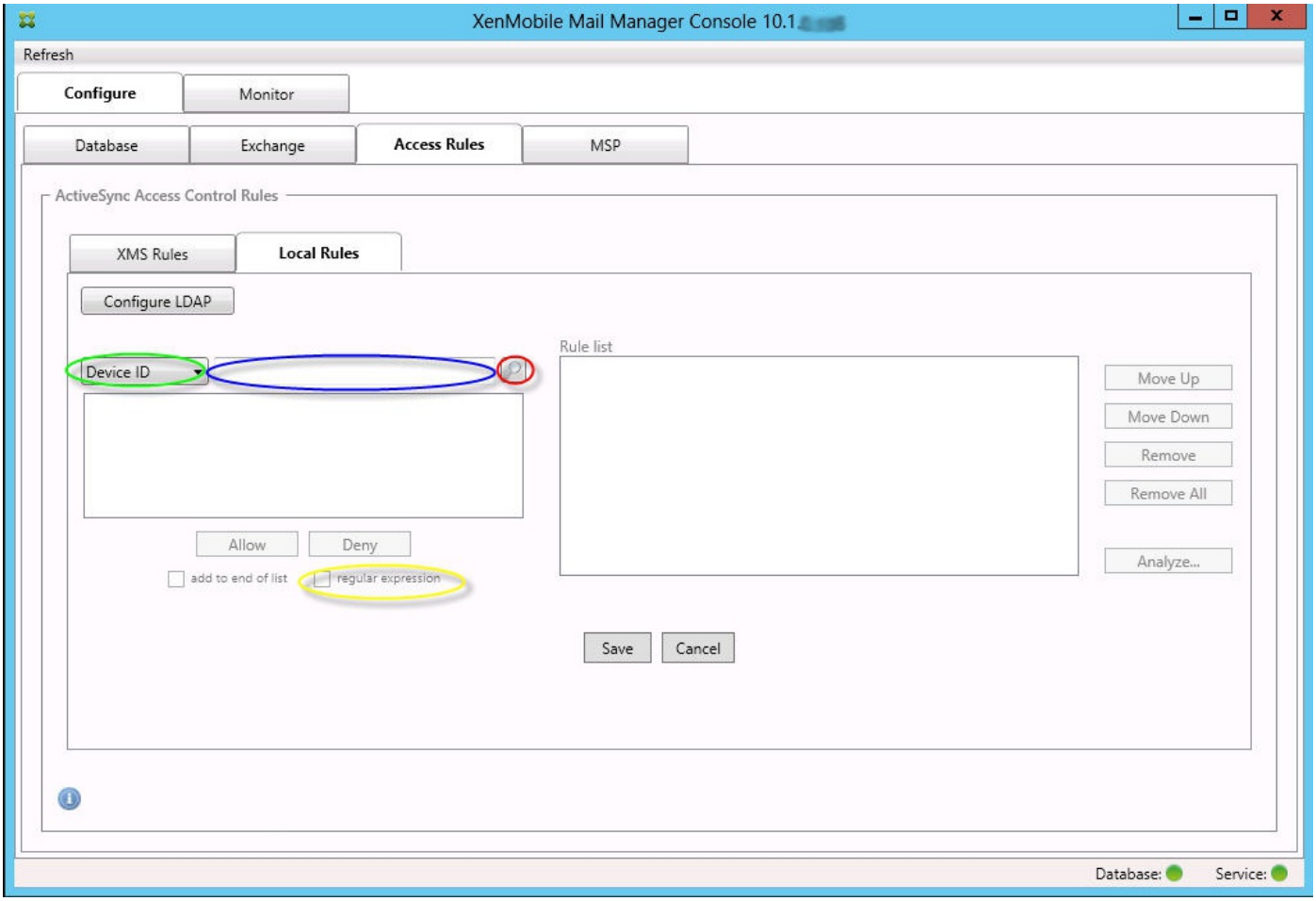


3. 照合するフィールドを選択します。 この例では［Device Type］を使用します。
4. 正規表現を入力します。 この例では次の文字列を使用します：samsung.*
5. ［regular expression］チェックボックスをオンにして、［Allow］または［Deny］をクリックします。 この例では、［Allow］を選択し、最終結果は次のようになります

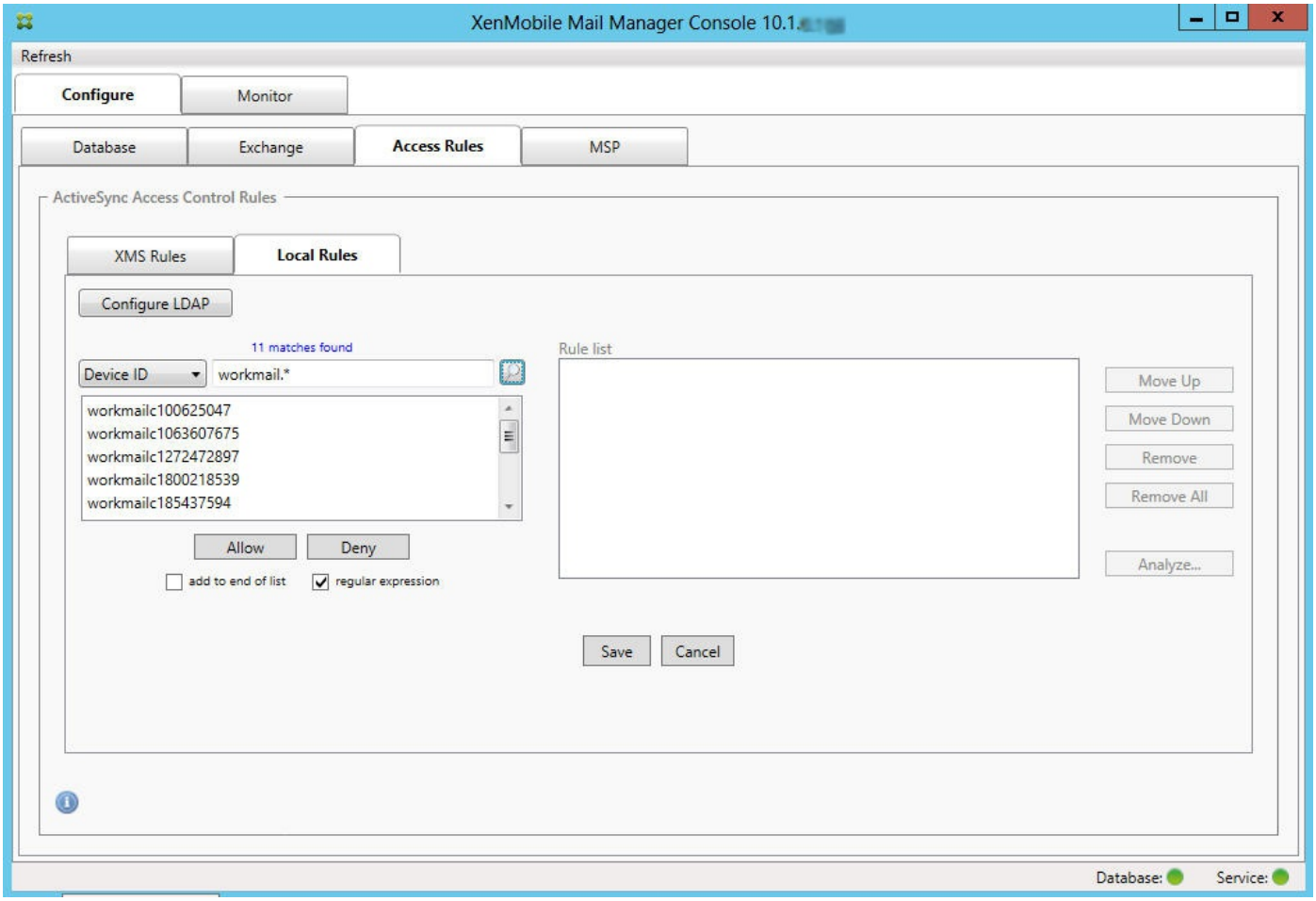


［regular expression］チェックボックスをオンにして、特定の式に一致する特定のデバイスの検索を実行できます。 この機能は、メジャースナップショットが正常に完了している場合にのみ利用できます。 正規表現の規則を使用しない場合でも、この機能を使用できます。 たとえば、ActiveSyncデバイスIDにテキスト「workmail」が含まれるすべてのデバイスを検出するとします。 これを行うには、以下の手順に従います。

1. ［Access Rules］タブをクリックします。
2. デバイスの照合フィールドセレクターが［Device ID］（デフォルト）に設定されていることを確認します。

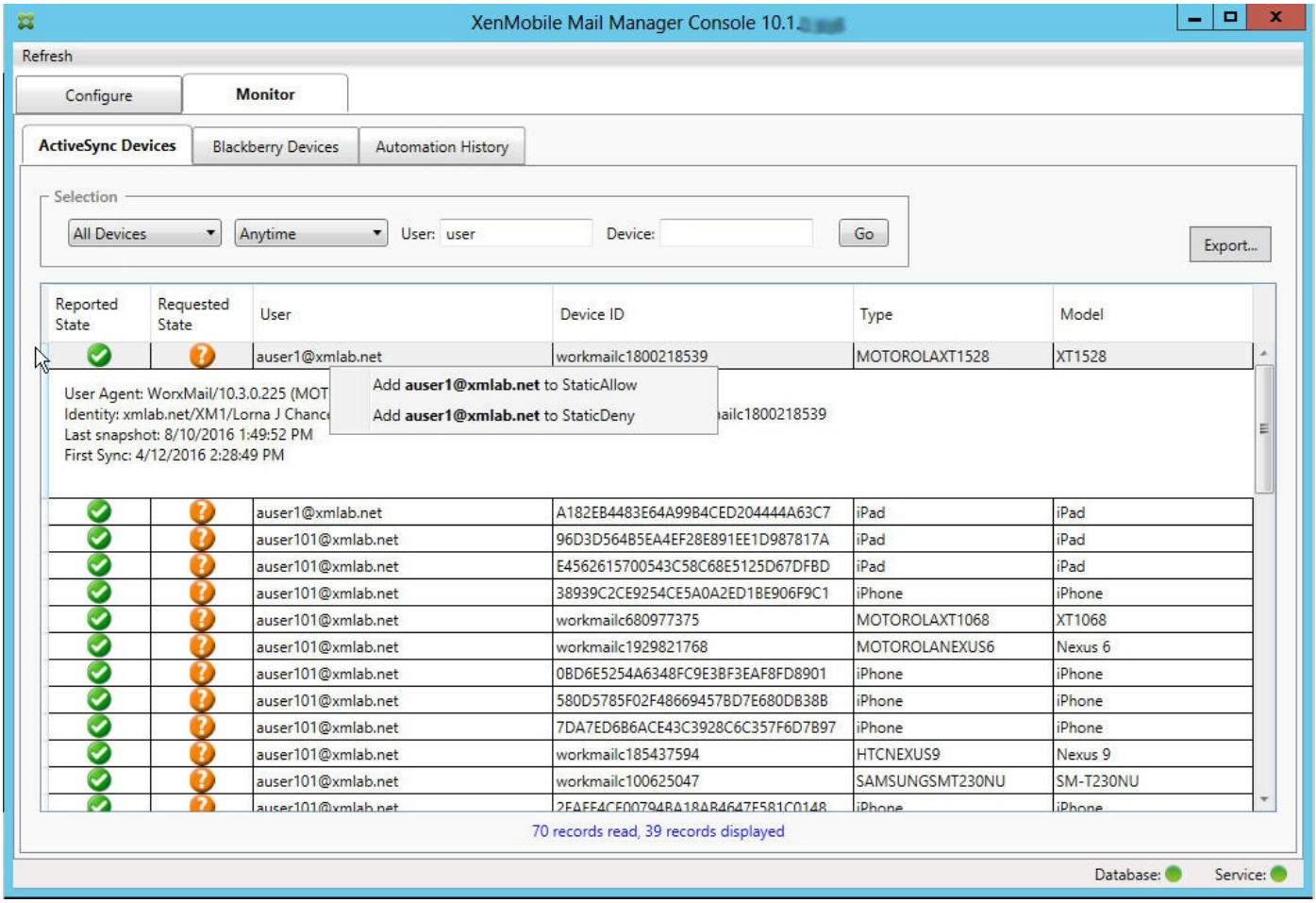


3. 選択済みアイテムのテキストボックス内（上記の図に青色で示されています）をクリックし、「workmail.*。
4. ［regular expression］チェックボックスをオンにして、虫眼鏡アイコンをクリックし、次の図に示すように一致を表示します。



［ActiveSync Devices］タブで、ユーザー、デバイスID、またはデバイスの種類に基づく静的規則を追加できます。

1. ［ActiveSync Devices］タブをクリックします。
2. 一覧で、ユーザー、デバイス、またはデバイスの種類を右クリックして、選択内容を許可するか、または拒否するかを選択します。
   次の図は、user1を選択したときの許可/拒否オプションを示しています。



デバイス監視

Aug 02, 2016

XenMobile Mail Managerの［Monitor］タブでは、検出されたExchange ActiveSyncデバイスおよびBlackBerryデバイスと、これまで自動で発行されたPowerShellコマンドの履歴を参照できます。 ［Monitor］タブには、次の3つのタブがあります。

- ActiveSync Devices：
  - ［Export］をクリックして、表示されているActiveSyncデバイスパートナーシップをエクスポートできます。
  - ［User］、［Device ID］、または［Type］列を右クリックし、許可またはブロックから適切な規則の種類を選択して、ローカル（静的）規則を追加できます。
  - 展開した行を折りたたむには、Ctrlキーを押しながらその行をクリックします。
- Blackberry Devices
- Automation History

［Configure］タブにはすべてのスナップショットの履歴が表示されます。 スナップショットの履歴には、スナップショットの作成時刻、作成にかかった時間、検出されたデバイス数、発生したすべてのエラーが表示されます。

- ［Exchange］タブで、目的のExchange Serverの情報アイコンをクリックします。
- ［MSP］タブで、目的のBlackBerry Serverの情報アイコンをクリックします。

トラブルシューティングおよび診断

Oct 25, 2016

XenMobile Mail Managerでは、エラーなどの動作情報がログファイル（\log\XmmWindowsService.log）に記録されます。 また、Windowsイベントログに、重要なイベントが記録されます。

一般的なエラーを以下に示します。

XenMobile Mail Manager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ます。 一般的な原因は次のとおりです。

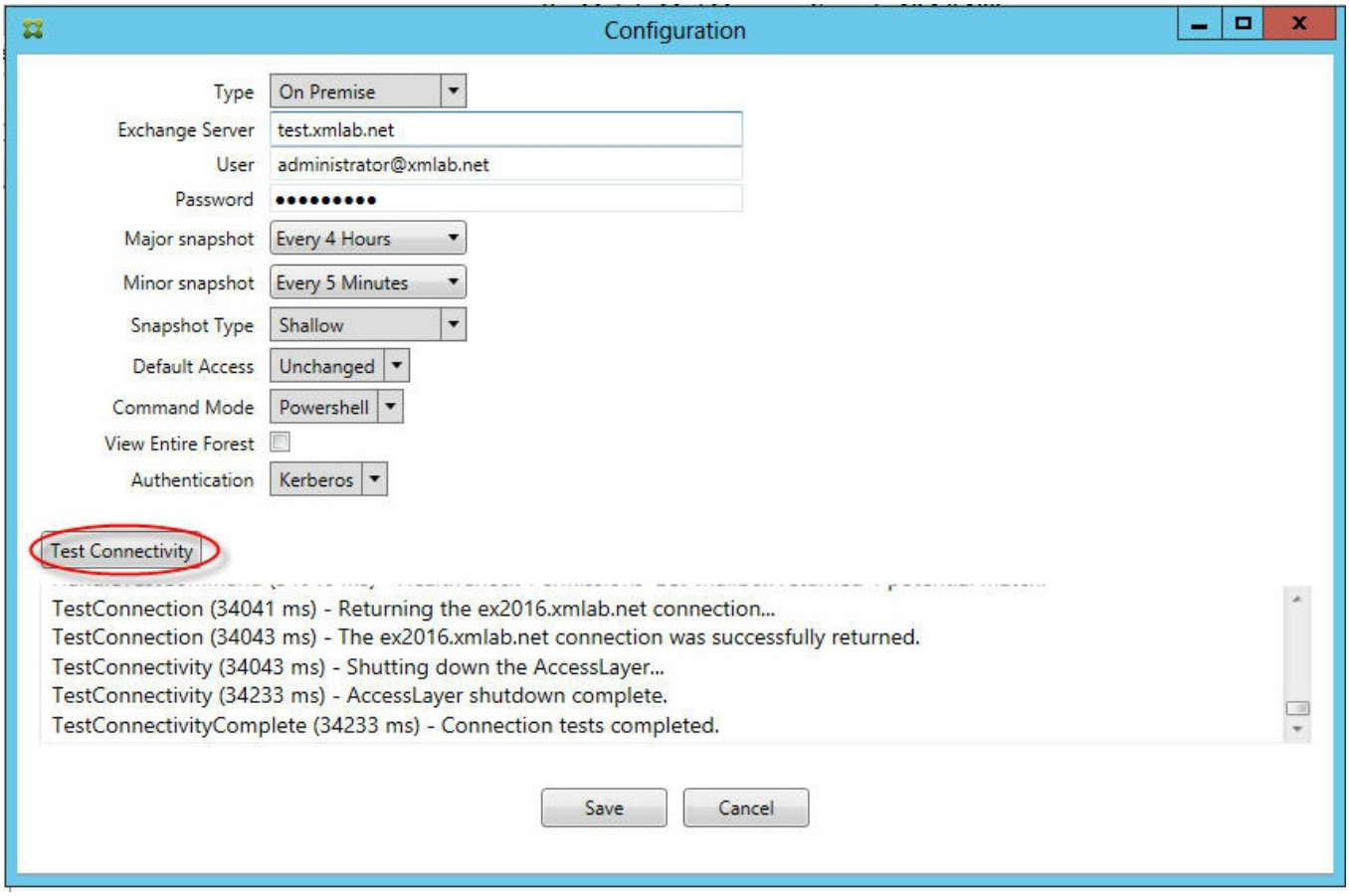
- XenMobile Mail ManagerサービスがSQL Serverにアクセスできない。 これは、次の問題が原因である可能性があります。
  - SQL Serverサービスが実行されていない。
  - 認証に失敗した。
    ［Windows Integrated authentication］が構成されている場合、XenMobile Mail Managerサービスのユーザーアカウントは、許可されたSQLログオンである必要があります。 XenMobile Mail Managerサービスのアカウントは、デフォルトではローカルシステムですが、ローカルの管理者権限を持つ任意のアカウントに変更できます。 ［SQL authentication］が構成されている場合、SQLログオンがSQLで適切に構成されている必要があります。
- Mobile Service Provider（MSP）に対して構成されたポートが使用できない。 システムのほかのプロセスで使用されていないリッスンポートを選択する必要があります。

XenMobileがMSPに接続できない

XenMobile Mail Managerコンソールの［Configure］の［MSP］タブで、MSPサービスポートとトランスポートが適切に構成されていることを確認します。 承認グループまたはユーザーが適切に設定されていることを確認します。
HTTPSが構成されている場合は、有効なSSLサーバー証明書がインストールされている必要があります。 IISがインストールされている場合は、証明書のインストールにIISマネージャーを使用できます。 IISがインストールされていない場合、証明書のインストールについて詳しくは、https://msdn.microsoft.com/ja-jp/library/ms733791.aspxを参照してください。

XenMobile Mail Managerには、MSPサービスへの接続をテストするためのユーティリティプログラムが含まれています。 <InstallFolder>MspTestServiceClient.exeプログラムを実行して、URLと資格情報をXenMobileで構成されるURLと資格情報に設定して、［Test Connectivity］をクリックします。 これにより、XenMobileサービスが発行するWebサービス要求がシミュレートされます。 HTTPSが構成されている場合は、サーバーの実際のホスト名（SSL証明書で指定された名前）を指定する必要があります。

注：［Test Connectivity］をクリックするときは、少なくとも1つActiveSyncDeviceレコードがあることを確認してください。レコードがないとテストが失敗する可能性があります。



Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

トラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。 すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

XenMobile NetScaler Connector

Oct 25, 2016

XenMobile NetScaler Connectorでは、Exchange ActiveSyncプロトコルのリバースプロキシとして動作するNetScalerに、ActiveSyncクライアントのデバイスレベルの認証サービスを提供します。 認証は、XenMobile内で定義されたポリシーの組み合わせと、XenMobile NetScaler Connectorによりローカルで定義されたルールによって制御されます。

詳しくは、次の記事を参照してください。

- XenMobile NetScaler Connector
- XenMobileでのActiveSyncゲートウェイ

リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の「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。