e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

解決された問題

Apr 24, 2017

XenMobile 10.5には次の解決された問題が適用されています。アップグレードツールの解決された問題については、この記事の「XenMobileアップグレードツール」に記載されています。

XenMobileアプリケーションに関連する解決された問題については、「解決された問題」を参照してください。

iPhone6デバイスの場合、デバイスのIMEI/MEIDにバウンドされたワンタイムパスワード招待状を使ってデバイスを登録しようとすると、最初のプロファイルは正常にインストールできます。しかし、2番目のMDMプロファイルのインストールは失敗し、「プロファイルのインストールは失敗しました。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では、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。[#606162]

［設定］＞［Google Play資格情報］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 Server 10.4へのアップグレード後：

- **［ShareFile］**タブを開いても、ページが読み込まれない場合があり、情報が表示されません。
- デリバリーグループの追加や編集を行おうとすると、次のエラーメッセージが表示されることがあります。「500 Internal Server error」[663344, 663788, CXM-19085]

Mowblyフレームワークを使って開発したアプリをMDX Toolkitでラップすると、アプリのナビゲーションボタンが機能しなくなります。 [#654962]

Secure Hubで収集されたHDXアプリにアクセスすると、「アプリケーションの詳細を取得できませんでした。しばらくしてからもう一度お試しください」というエラーメッセージで失敗することがあります。 [#658058]

Citrix Launcherがデバイスに展開されると、バックグラウンドタスクにアプリが表示されません。[#680978]

App Controller 9.0のWebプロキシのJSONファイルで、Webプロキシユーザー名にエスケープされていないバックスラッシュ文字が含まれている場合、XenMobile Serverを起動できません。[CXM-13721]

Hazelcastによって管理されたXenMobileのクラスター展開において、クラスターのあるノードがHazelcastのメンバー一覧に断続的に表示されなくなることがあります。[CXM-16537]

IPSec VPNデバイスポリシーを構成すると、グループ名と共有シークレットが保存されず、デバイスから失われます。[CXM-17002]

10.3.6にアップグレードした後、有効なIDを複数持つデバイスを更新できません。更新の失敗が多い場合、XenMobileがクラッシュを繰り返す可能性があります。[CXM-17358]

クライアント証明書認証に使用される中間CA証明書で問題が発生することがあります。この問題によってAndroidデバイスでネットワークアクセスエラーが表示されます。[CXM-17401]

XenMobileをバージョン10.3.5から10.3.6に更新すると、SQLデータベースの構成で問題が発生することがあります。[CXM-17565]

オンプレミスバージョンのXenMobileは、ライセンスサーバーをXenMobileがチェックアウトしたライセンスに定期的に同期させます。同期によってライセンス数とデバイス数やユーザー数との一致が保証されます。このようにして、XenMobileが不

整合を検出すると、問題は24時間以内に解決されます。[CXM-18129]

XenMobileコンソールで、Wi-Fiポリシーのパスワードが任意であるにもかかわらず、指定することを要求されます。[CXM-18249]

日付形式が間違っているためにXenMobileがユーザープロファイルを展開できません。[CXM-18250]

XenMobileコンソールをInternet Explorer 11ブラウザーで使用している場合、LDAP構成の追加や編集ができません。[CXM-18324]

すべてのデバイスの種類でExchangeポリシーを作成し、そのデバイスポリシーに**$user.dnsroot**というドメインのマクロが含まれている場合、ポリシーを展開できません。[CXM-18545]

デリバリーグループ名にアンパサンド（&）が使用されている場合、そのデリバリーグループにポリシーを割り当てるとエラーが発生します。[CXM-18768]

[設定] > [iOS一括登録]で初めてDEP設定を構成した後、**[保存]**をクリックすると、次のエラーが表示されます。「Resources bag (container) with name 'Worx Home by Citrix' doesn't exist.」この問題を回避するには、DEP設定を構成した後、デリバリーグループ（**[構成] > [デリバリーグループ]**）を作成し、エラーページで**[OK]**をクリックします。デリバリーグループに必要なものは次のとおりです。

- **Device Enrollment Program Group**という名前のユーザーグループ
- **DEP**ソフトウェアインベントリポリシー
- 必須アプリの**Secure Hub by Citrix**

この問題が既存の登録に影響を与えないのは、Citrix Secure Hubが2016年10月6日にApple Storeに公開される前にDEPを構成した場合です。[CXM-19158]

登録招待状テンプレートまたは登録PINテンプレートに関して： テンプレートのメッセージに特定のマクロが含まれている場合、ユーザーに送信されたメッセージには、ユーザー情報ではなく、そのマクロが記載されます。特定のマクロとは、登録用URL（${enrollment.url}）と登録PIN（${enrollment.pin}）です。[CXM-19210]

エンタープライズアプリをアップロードできない場合があるのは、XenMobileがアプリケーションアイコンにアクセス可能であるが見つけられないからです。[CXM-19213]

証明書が複数のページにわたる場合、**[設定] > [PKIエンティティ] > [任意CA]**ページで、CA証明書の最初のページしか表示できません。[CXM-19736]

複数のデバイスに展開されたデリバリーグループに関して：**[構成] > [デリバリーグループ]**でデリバリーグループを選択し、**[展開]**の下のボタンをクリックすると、**[管理] > [デバイス]**ページに間違ったデバイス一覧が表示されます。[CXM-19737]

XenMobileアプリの更新プログラムをiOS App StoreまたはGoogle Playストアで入手できる場合： ユーザーがアプリを開いても、アプリの更新を促すメッセージがXenMobile Storeで表示されません。 [CXM-19927]

XenMobileマクロに$user.dnsrootが含まれていると、親ドメインと子ドメインがツリールート信頼関係にあるドメインの解決ができません。[CXM-20366]

sAMAccountNameがUPNの名前部分と異なる場合、クライアントプロパティSEND_LDAP_ATTRIBUTESのマクロ解決が失敗します。例：sAMAccountNameが「**samplename**」で、UPNが「**sample@example.com**」の場合。[CXM-20414]

XenMobileがMDMモードで、DEPフェーズで指定されたユーザーの資格情報でDEP登録を使用している場合： Secure Hubを登録後、短時間でデバイスから削除すると、サーバーが不整合状態になります。短時間とは、1時間のこともあります。[CXM

20924]

自動化された操作の後で、デバイスが自動的にコンプライアンス準拠状態になりません。[CXM-21006]

ユーザーグループ制限を含むカスタムRBAC役割を割り当てられたRBAC管理者の場合： ユーザーグループのActive Directoryユーザーがデバイスを登録する場合、 **[管理] > [デバイス]** ページの表示に時間がかかります。[CXM-21007, CXM-21009]

XenMobile 10.3.6にアップグレードした後、カスタムRBAC役割アクセスを持つ管理者は、RBAC構成でアクセスが制限されていても、ほかのドメインから登録されたデバイスを表示できます。[CXM-21008]

XenMobileのクラスターメンバーが一部のHTTP要求に応答しない場合があり、「**会社のネットワークを使用できません**」というエラーで登録ができません。[CXM-21010]

iOSの一括登録設定で「**デバイス登録のための資格情報を求める**」を有効にしている場合、どんな種類のDEP登録招待状でもXenMobile Serverでエラーが発生します。エラーには、Secure Hubのエラーメッセージ、XenMobileコンソールのエラーメッセージ、すべてのデバイスのMDM機能の喪失があります。この問題を回避するには、 **[管理] > [登録]** ページで影響を受けるユーザーの登録招待状をすべて削除します。次に、XenMobile Serverを再起動します。[CXM-21500]

XenMobileの紛失モードが開始する自動化された操作が、パスコードを設定したiOSデバイスで失敗します。この問題は、紛失モードで開始される次のすべての利用可能な操作で発生します。 **アプリのワイプ**、**アプリのロック**、**コンプライアンス違反としてデバイスをマーク**、**通知の送信**。[CXM-21579]

[分析] > [レポート] で生成されるデバイスとアプリのレポートで、デバイスごとのアプリのインストール数の表示が正しくありません。[CXM-21773]

パブリックアプリのSkype for BusinessをXenMobileコンソールで追加しても、アイコンが表示されない場合があります。たし、コンソールでアプリを検索して追加すれば、デバイスにそのアプリをインストールできます。[CXM-21774, #668341]

一部のAndroid用エンタープライズアプリケーションは、MDMモードまたはXMEモードで構成されたXenMobileコンソールにアップロードできません。[CXM-22377]

現在のMobile Country Codeなどの動的なデバイスプロパティに基づいてリソースを展開することができません。XenMobileは規則を無視して、リソース（デバイスポリシー、アプリ、操作など）をデバイスに展開できます。[CXM-22565]

XenMobileのCLIでサポートバンドルを作成できません。回避策として、XenMobileコンソールで次のように操作します。**[サポート] > [サポートバンドルの作成]** に移動し、 **[作成]** をクリックします。[CXM-23091]

XenMobile 10.3.6にアップグレードすると、Secure HubでHDXアプリが利用できなくなりました。ログに「Unable to get the Config xml data Host name.」というエントリが含まれます。[CXM-23177]

デバイスポリシーのプラットフォームの詳細のみを編集する場合、編集しても **[構成] > [デバイスポリシー]** の「**最終更新日**」の日時は変更されません。最終更新日時が変更されるのは、プラットフォームを追加または削除した後です。[CXM-23178]

Webブラウザーの言語がフランス語に設定されている場合、XenMobileコンソールでWi-Fiデバイスポリシーの作成も編集もできません。[CXM-23180]

iOSデバイスがアクティブでXenMobile Serverと通信していても、 **[管理] > [デバイス]** ページで非アクティブと表示されます。この問題は、ログに次のように記録されます。

java.lang.IllegalStateException: Cannot load backing target entity: has been deleted. [CXM-23181]

サーバープロパティ **[StorageZoneコネクタによる値のサポート]** が **[サポートなし]** で、XenMobileコンソールでShareFile

を構成する場合：別のコンソールページに移動した後で、**[構成] > [ShareFile]** ページに戻ると、構成が保存されていても **[ShareFile]** ページに構成が表示されません。この問題を回避するには、サーバープロパティ **[ShareFile構成の種類]** を **[エンタープライズ]** に変更します。[CXM-23337]

DEPデバイスを削除した後で再登録すると、再登録が「Invalid profile」エラーで失敗する場合があります。[CXM-24078]

このリリースには、CVE-2016-5195に対する多層防御対策（別名Linux Dirty Cow）が含まれています。

XenMobileアップグレードツール

XenMobile 9における展開にgpsstats.apkエンタープライズアプリが含まれる場合、XenMobile 10.4へのアップグレードが失敗する場合があります。[CXM-17992]

XenMobile 9からXenMobile 10.4へアップグレードした後、WindowsデバイスとiOSデバイスがMAM+MDMモードではなく、MDMモードになります。さらに、XenMobile Storeが起動しません。回避策として、ユーザーは移行したデバイスを再登録できます。[CXM-18532, CXM-23408]

XenMobile 9からXenMobile 10.4にアップグレードすると、以前の再登録によりXenMobileでアクティブでないMAM-onlyレコードの重複が発生します。この問題は、XenMobile 9がデバイスマネージャーでの登録を要求するように構成されていたとしても発生します。[CXM-18544]

XenMobile 9.0からXenMobile 10.4.xにアップグレードする間： アップグレードツールは、XME（MDM+MAM）モードで登録されたデバイスのデバイスプロパティテーブルのデバイス名を更新しません。[CXM-20821]

App Controllerデータベースに「**ユーザー名**」データ形式のユーザーが含まれる場合、XenMobile 9.0からXenMobile 10.xへのアップグレードが失敗します。代わりに、「**ドメイン\ユーザー名**」または「**ユーザー名@ドメイン**」データ形式を使用します。[CXM-21072]

.p12サーバー証明書へのパスの表記（大文字、小文字）がHTTPとHTTPSで異なる場合、XenMobile 9.0からXenMobile 10.4.xへのアップグレードが失敗します。たとえば、HTTPパスが「Certificates\MDM.p12」で、HTTPSパスが「certificates\MDM.p12」の場合。[CXM-21581]

XenMobile 9から10.xへアップグレードした後、XenMobile Storeのアプリが利用できません。また、XenMobileでローカルグループがデリバリーグループに割り当てられません。この問題が発生するのは、ローカルユーザーがローカルグループに属しており、そのローカルユーザーがデバイスを登録する場合です。[CXM-23375]

Device ManagerにActive Directoryユーザーのレコードが2つ登録されていて、それらのレコードが次のように一致しない場合、アップグレードは失敗します。

- 2つのレコードのUPNが異なる。たとえば、一方のユーザーレコードのUPNが「john.smith@eng.domain.com」で、他方のレコードが「john.smith@domain.com」の場合です。
- sAMAccountNameの2つのレコードの表記が大文字か小文字かで異なる場合。たとえば、一方のユーザーレコードのsAMAccountNameが「johns」で、他方のレコードが「JOHNS」の場合です。[CXM-23382]

XenMobile 9からXenMobile 10.xにアップグレードした後： iPhoneの構成ユーティリティまたはApple Configuratorを使ってDevice Managerで構成ポリシーをカスタマイズした場合、アップグレードしたXenMobileコンソールでそのポリシーの編集ができません。[CXM-23942]

既知の問題

May 11, 2017

XenMobile 10.5には次の既知の問題があります。アップグレードツールで解決された問題については、「XenMobileアップグレードツール」に記載しています。

XenMobileアプリケーションに関連する「既知の問題」を参照してください。

NetScaler 12.0.41.16を使用したSecure MailでSTAで構成されている場合、iOSおよびAndroidデバイスでメールを同期できません。この問題は、NetScaler 12.0ビルド41.22で解決されています。詳しくは、Support Knowledge Centerの記事を参照してください。[#685075]

StoreFrontをXenMobileと統合してHDXアプリを展開する場合、Active Directoryのパスワードを変更するとHDXアプリがXenMobile Storeで表示されなくなります。[CXM-9859]

XenMobile 10.4.2にアップグレードすると、ネストされたActive Directoryグループに含まれるユーザーのデバイスでAndroid for Workアプリが表示されません。[CXM-19930]

XenMobile 10.3.6からXenMobile 10.5にアップグレードすると、Android for Workを実行している登録済みデバイスの所有者名が「匿名」に変わることがあります。[CXM-19933]

XenMobileの構成で **[有効期限が切れたら証明書を更新]** を **[オフ]** にしている場合でも、ユーザーが証明書を更新できます。[CXM-20923]

StorageZoneコネクタに対する権限が設定されているグループのActive Directoryユーザーについて、 このグループからユーザーを移動させても、ShareFile for iOSユーザーはこれらのコネクタに関連付けられているネットワーク共有に引き続きアクセスできます。この問題を回避するには、ShareFile for iOSアプリを再インストールします。 [CXM-21859]

StorageZoneコネクタをデリバリーグループAからBに移動した場合でも、デリバリーグループAのShareFile for iOSユーザーは引き続きこのコネクタを使用できます。[CXM-21860]

XenMobileが自己署名証明書を使用する場合は、ユーザーはiOS 10.3デバイスをXenMobileに登録することができません。この制限は、iOS 10.3の変更によるものです。iOS 10.3以降を実行するデバイスをXenMobileに登録するには、XenMobileで信頼されるSSL証明書を使用する必要があります。[CXM-24120]

アプリの展開で、デバイスにアプリがインストールされていても一度も開いたことがない場合、ユーザーにアプリをインストールするようメッセージが表示されます。この問題は、アプリがサーバーで更新されていても、アプリが起動されるまでユーザーのデバイスでは更新されないため発生します。[CXM-32193]

XenMobileアップグレードツール

XenMobile 9からXenMobile 10.4にアップグレードすると、XenMobileでWindowsデバイスのポリシーを展開した後でもこれらのポリシーの一部がXenMobileコンソールに表示されます。具体的には、 **[管理] > [デバイス]** の **[割り当て済みポリシー]** ページの **[保留中]** タブにポリシーが残ったままになります。この問題を解決するには、保留中と表示されているポリシーを編集して再び展開します。こうすることで、 **[保留中]** タブからWindows Phoneのポリシーが消去されます。WindowsタブレットのWebクリップポリシーは **[保留中]** タブに残りますが、デバイス上では適切に動作します。[CXM-21769]

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

XenMobileの互換性

Jun 05, 2017

Important

- Citrixは、XenMobile業務アプリケーションに関してエンタープライズでの配信とパブリックアプリケーションストアでの配信の両方を2017年12月31日までサポートします。詳しくは、「Citrix製品のマトリックス」を参照してください。このサポート期限までに、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への移行をお願いいたします。期限以降は、パブリックアプリケーションストア配信のみがサポートされます。アプリ内ガイドによるXenMobileアプリのエンタープライズバージョンからパブリックストアバージョンへの移行について詳しくは、「アプリ内ガイドでパブリックストアアプリに移行」を参照してください。MDX Toolkitでは、アプリ開発者向けにエンタープライズラッピングが引き続きサポートされます。
- バージョン10.4では、Worx MobileアプリがXenMobileアプリに変更されました。XenMobileアプリの名前はすべて変更されました。詳しくは、「XenMobileアプリについて」を参照してください。

このトピックでは、連係可能なXenMobileコンポーネントのサポートされているバージョンを示しています。このコンポーネントには、NetScaler Gatewayと、XenMobileアプリのラップ、構成、配布に必要なMDX Toolkitのバージョンが含まれます。

サポートされているバージョンとアップグレードパス

XenMobile Serverとアプリに関しては、現在および2つ前のバージョンのXenMobileまでサポートされます。たとえば、現在のバージョンがXenMobile Server 10.5の場合、バージョン10.4とバージョン10.3.6もサポートされます。1つのバージョンには、リリースとService Packが両方含まれます。XenMobile 10.4は、完全版ではなくService Packです。

XenMobile 9の保守は終了しました。詳しくは、「製品のマトリックス」を参照してください。XenMobile 9から最新バージョンのXenMobileへのアップグレードをサポートしています。

	アップグレードのサポート対象	最新バージョン	アップグレード元
ラップされたエンタープライズアプリ（Secure Mailや Secure Webなど）	2つ前までのバージョン	10.4.5（iOS）、 10.4.6（Android）	10.3.10または10.4
パブリックストアアプリ（Secure HubやSecure Mail、Secure Webなど）	2つ前までのバージョン 自動更新を有効にしているユーザーは、App Storeから最新バージョンを受信できます。 最新のアプリでは、2つ前までのMDXファイルがサポー	10.5.20（Secure Hub） 10.5.20（Secure Mail） 10.5.20（Secure Web）	10.5.10または 10.5.15（Secure Hub） 10.5.10または 10.5.15（Secure Mail） 10.5および10.5.10（Secure Web）

	トされます。		たとえば、Secure Mailのバージョン10.5.20には、バージョン10.5.15またはバージョン10.5.10のMDXファイルとの互換性があります。
MDX	以前のバージョン	10.4.10	10.4.5
サーバー（オンプレミス）	2つ前までのバージョンおよびXenMobile 9 RP5からのアップグレード	10.5	10.4、10.3.6、XenMobile 9 RP5

XenMobileの互換性

新しい機能や修正された機能、およびポリシーの更新を利用するには、最新バージョンのMDX Toolkit、Secure Hub、およびXenMobileアプリをインストールすることをお勧めします。

- エンタープライズ配信のアプリケーション、MDX Toolkit、Secure Hub：
  - 最新バージョンのアプリとMDX Toolkitには、最新バージョンのSecure Hubが必要です。
  - 最新バージョンのアプリには、最新バージョンのMDX Toolkitが必要です。
  - 2つ前までのバージョンのアプリと1つ前のバージョンのMDX Toolkitは、最新のSecure Hubと互換性があります。
- クライアントおよびサーバー：最新バージョンのSecure Hub、MDX Toolkit、XenMobile Appsは、最新バージョンと2つ前までのバージョンのXenMobile Serverと互換性があります。
- パブリックストアアプリは、XenMobile 10.4以降とのみ互換性があります。
- ラップされたエンタープライズアプリがXenMobile 9と互換性があるのは、XenMobile 9がサポート停止になる2017年6月までです。

サポートされているNetScaler Gatewayのバージョン：

- 11.1.x
- 11.0.x
- 10.5.x

> **Important**
>
> XenMobileは、現在NetScaler 12.0.41.16をサポートしていません。この問題は、NetScaler 12.0ビルド41.22で解決されています。詳細および更新については、Support Knowledge Centerの記事を参照してください。

MDX Toolkit for iOSおよびAndroidのバージョン	**互換性のあるSecure Hubのバージョン**	
	Android	**iOS**

10.4.10 10.4.5	10.5.20 10.5.15	10.5.20 10.5.15
MDX Toolkit for Windows Phone	**互換性のあるSecure Hubのバージョン**	
10.3.9	10.3.5	
10.3.1	10.3	

> **注意**
>
> XenMobile 10.1では、Windows Phone 10はサポートされていません。
>
> XenMobile 9については、適切に機能させるためのパッチをアプリにインストールする必要があります。詳しくは、CTX217942を参照してください。

パブリックアプリケーションストアで入手できるアプリ

	Android	**iOS**
Secure Hub	10.5.20	10.5.20
Secure Mail	10.5.20	10.5.20
Secure Web	10.5.20	10.5.20
Secure Notes	10.4.5	10.4.5
Secure Tasks	10.4.5	10.4.5
QuickEdit	6.10	6.10
ShareFile	5.4	5.3
ShareConnect		3.3
ScanDirect		1.2.2

エンタープライズ配信で入手できるアプリ

XenMobile 10.xと9は以下の表に示すバージョンのWorxモバイル/XenMobileアプリをサポートしています。

アプリ	Android	iOS	Windows Phone [1]
Secure Hub	10.5.15 10.5.10	10.4.10 10.4.5	
Worx Home	10.3.10 10.3.9	10.3.10 10.3.9	10.0.3 10.0.0
Secure Forms		10.4.5 10.4.1	
Secure Mail	10.4.6 10.4.5	10.4.5 10.4.0.19	
WorxMail	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.7
Secure Notes	10.4.5 10.4.1	10.4.5 10.4.1	
Worx Notes	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Tasks	10.4.5 10.4.1	10.4.5 10.4.1	
WorxTasks	10.3.10 10.3.9	10.3.10 10.3.9	
Secure Web	10.4.5 10.4.1	10.4.5 10.4.1	

WorxWeb	10.3.10 10.3.9	10.3.10 10.3.9	10.2 10.0.3
QuickEdit[2]	6.10	6.10	
ScanDirect		1.2.2	
ShareConnect	3.2.341	3.3	
ShareFile	5.4	5.3	

[1] XenMobile 10.1では、Windows Phone 10はサポートされていません。

[2] XenMobileでは、QuickEdit、ShareConnect、ShareFileの最新バージョンのみがサポートされています。

ブラウザーサポート

XenMobile 10.xは、次のブラウザーをサポートしています。

- Internet Explorer（ただし、バージョン9以前は対象外）
- Chrome
- Firefox
- 自己ヘルプポータルで使用するためのモバイルデバイス上のSafari

XenMobile 10.xは、ほとんどの最新バージョンおよび1つ前のバージョンのブラウザーと互換性があります。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

ライセンス管理

Apr 13, 2017

ライセンス管理は、XenMobile ServiceとXenMobile Serverで異なります。

- XenMobile Serviceのライセンスは、Citrix Cloud運用チームが管理します。
- XenMobile ServerおよびNetScaler Gatewayにはライセンスが必要です。

  NetScaler Gatewayライセンスについて詳しくは、NetScaler Gatewayドキュメントの「ライセンス管理」を参照してください。XenMobileでは、Citrixライセンスサーバーを使ってライセンスを管理します。Citrixライセンスサーバーについて詳しくは、「Citrixライセンスシステム」を参照してください。

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

各XenMobileエディションで利用できるXenMobile機能を示すデータシートは、このPDF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
>
> 最新バージョンのXenMobileでは、Citrixライセンスサーバー11.12.1以降が必要です。それより前のバージョンのライセンスサーバーは、最新バージョンのXenMobileでは動作しません。

> ## 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

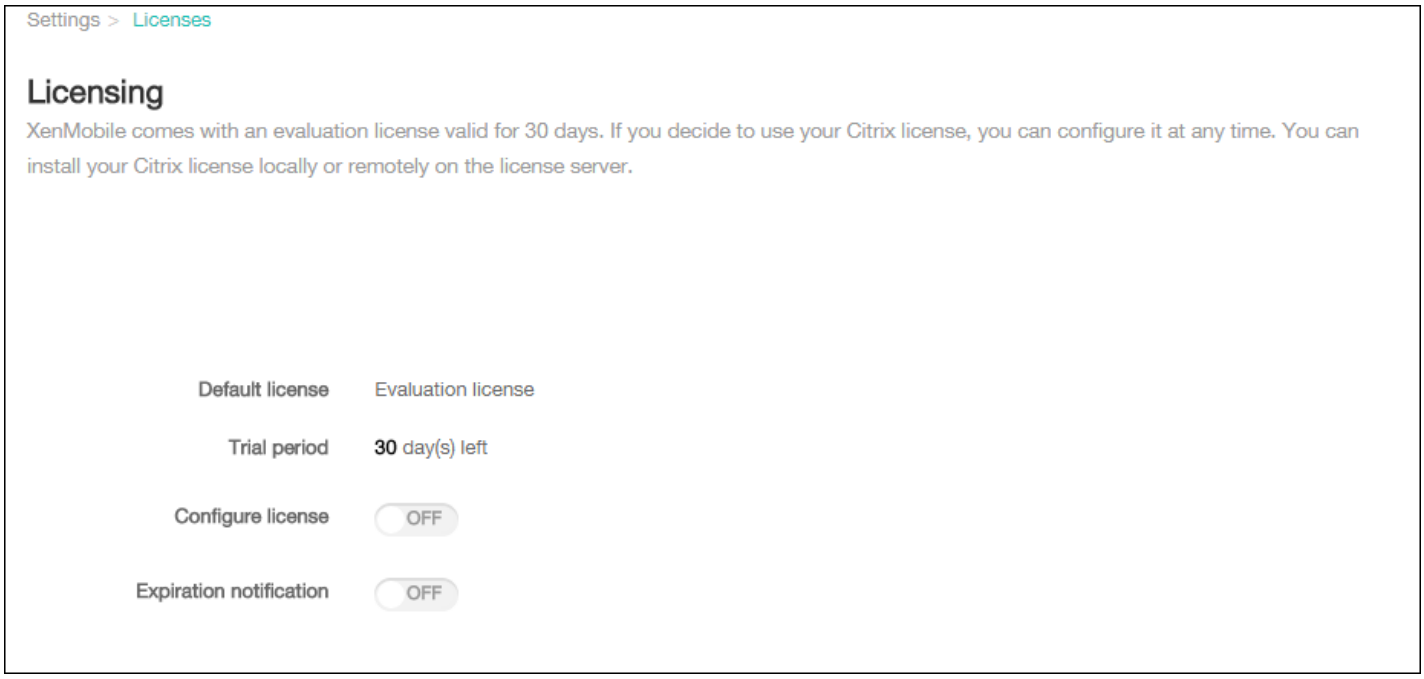
ライセンスがない場合、30日間は試用モードでXenMobileのすべての機能を操作することができます。この試用モードを使用できるのは、XenMobileのインストール時から30日間の1回限りです。有効なXenMobileライセンスを使用できるかどうかに関係なく、XenMobile Webコンソールへのアクセスはブロックされません。XenMobileコンソールで、試用期間の残り日数を参照できます。

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

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

XenMobileコンソールで［ライセンス］ページを開くには

XenMobileをインストールすると最初に **[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。**[設定]** 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）および種類が同じライセンスを複数追加した場合、表ではこれらのライセンスが1つの行として表示されます。この場合、**[ライセンス数合計]** と **[使用数]** に、共通するライセンスの合計数が表示されます。**[有効期限]** の日付は、共通するライセンスのうち最も後の有効期限を示します。

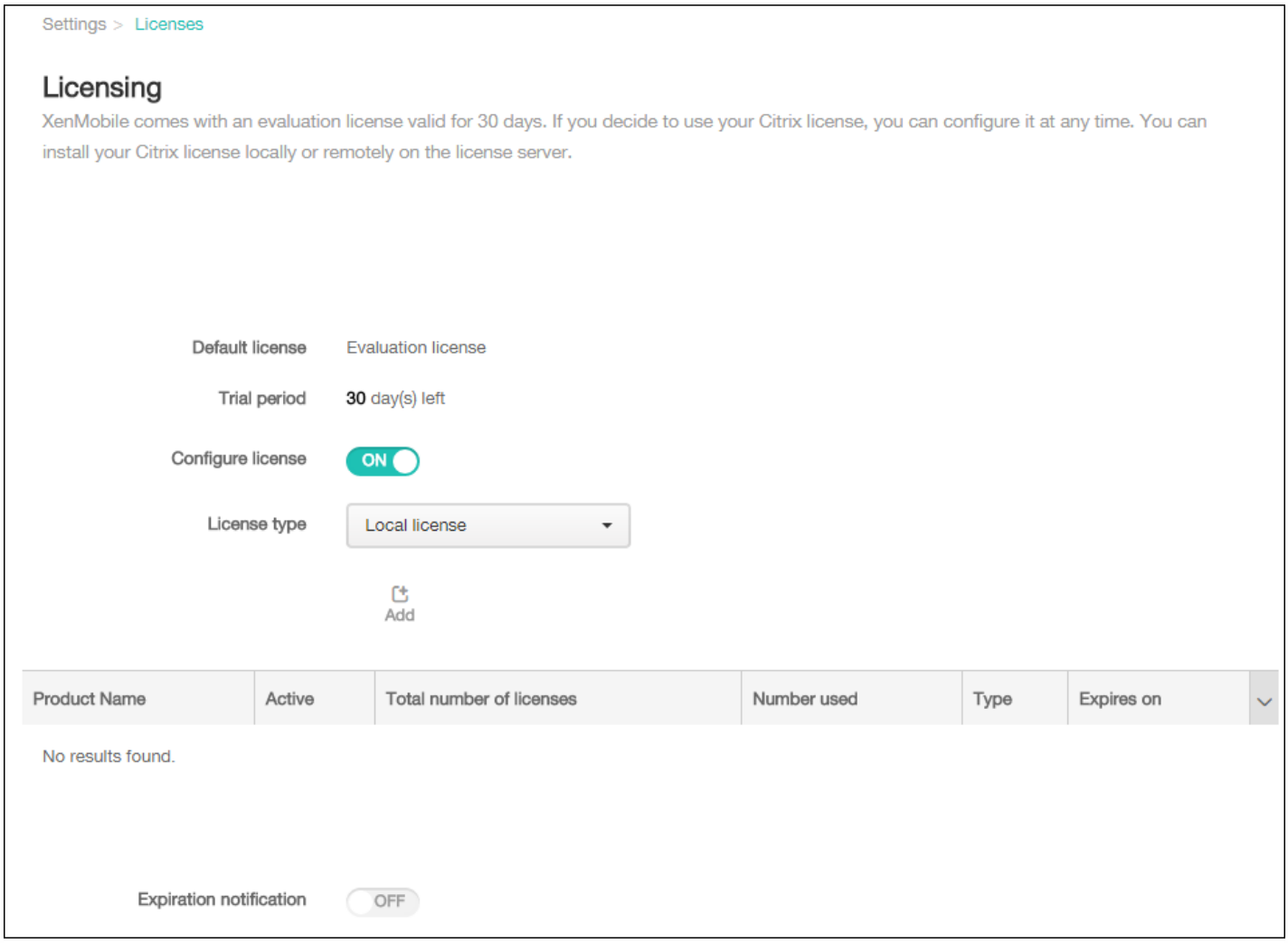
ローカルライセンスの管理は、すべてXenMobileコンソールで行います。

1. ライセンス管理コンソールを介してSimple License Serviceから、またはCitrix.comのアカウントから直接、ライセンスファイルを入手します。詳しくは、「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。**[設定]** ページが開きます。

3. **[ライセンス]** をクリックします。**[ライセンス]** ページが開きます。

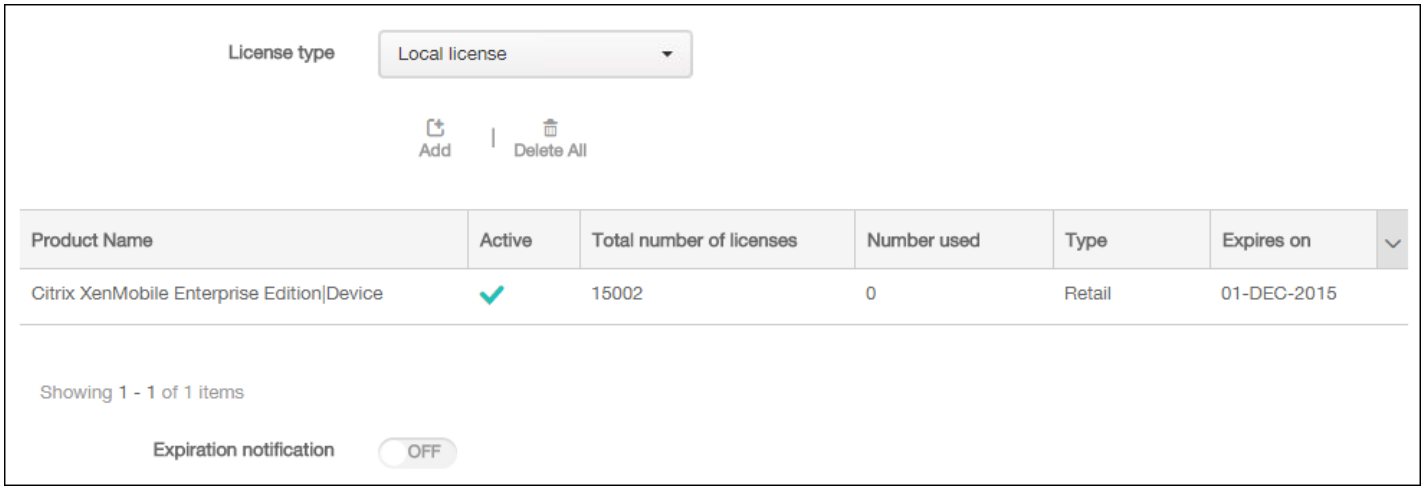
4. **[ライセンスを構成]** を **[オン]** に設定します。**[ライセンスの種類]** ボックス、**[追加]** ボタン、**[ライセンス]** の表が表示されます。**[ライセンス]** の表には、XenMobileで使用したライセンスが表示されます。Citrixライセンスをまだ追加していない場合、この表は空白です。



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

6. **[新しいライセンスの追加]** ダイアログボックスで、**[ファイルの選択]** をクリックし、ライセンスファイルの場所を参照します。

7. **[アップロード]** をクリックします。ライセンスがローカルにアップロードされ、表に表示されます。



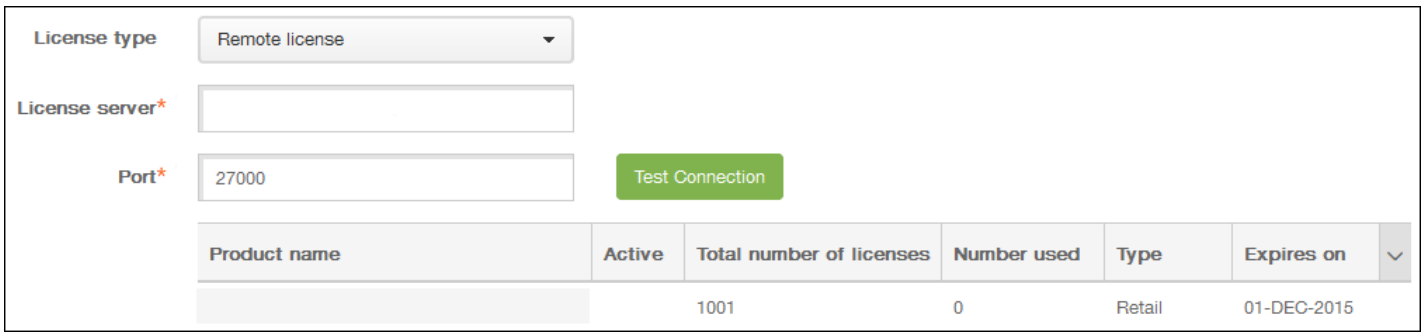
8. ライセンスが **[ライセンス]** ページの表に表示されたら、ライセンスをアクティブ化します。ライセンスが表の最初にある場合、ライセンスは自動的にアクティブ化されます。

リモートライセンスを追加するには

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

1. **[ライセンス]** ページで、 **[ライセンスを構成]** を **[オン]** に設定します。 **[ライセンスの種類]** ボックス、 **[追加]** ボタン、 **[ライセンス]** の表が表示されます。 **[ライセンス]** 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. **[ライセンスの種類]** を **[リモートライセンス]** に設定します。 **[追加]** ボタンが、 **[License server]** フィールドおよび **[Port]** フィールドと、 **[接続のテスト]** 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。

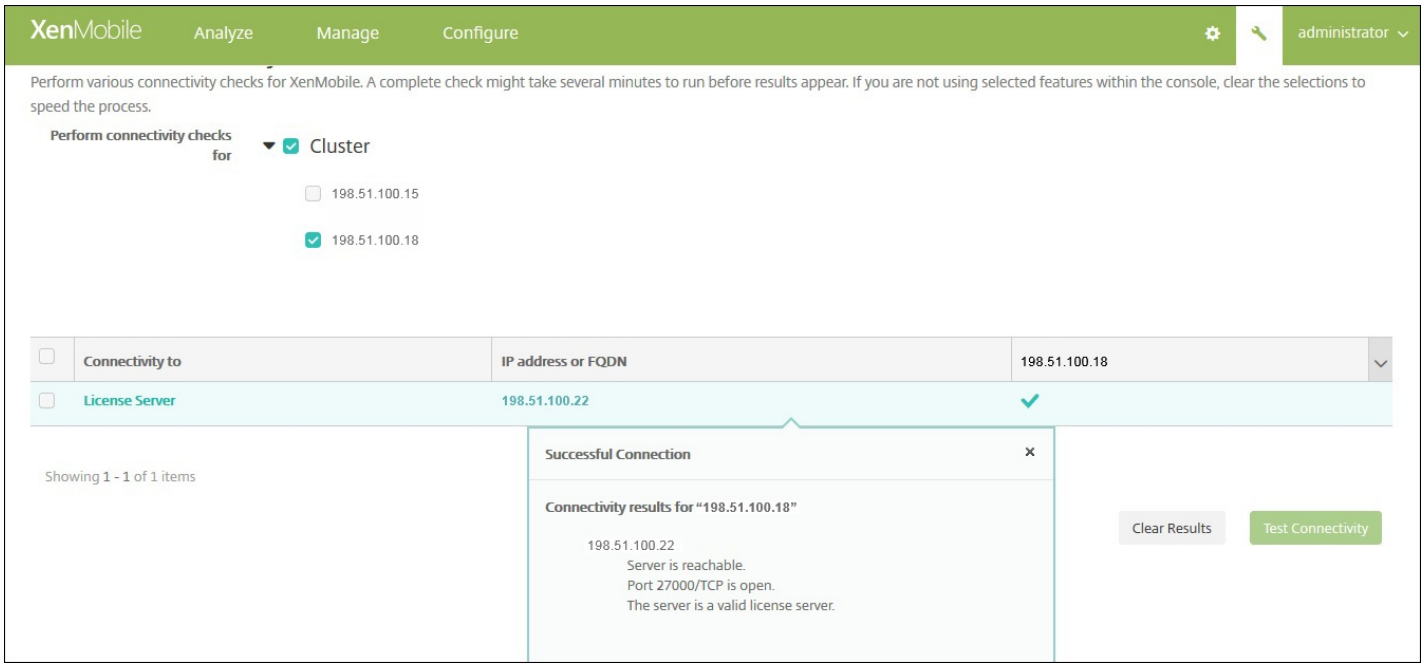
5. **[接続のテスト]** をクリックします。接続が成功した場合、XenMobileはライセンスサーバーに接続し、使用可能なライセンスがライセンスの表に表示されます。ライセンスが1つのみの場合は、自動的にアクティブ化されます。

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

- XenMobileがライセンスサーバーと通信できるか。

- ライセンスサーバーのライセンスは有効であるか。
- ライセンスサーバーはXenMobileと互換性があるか。

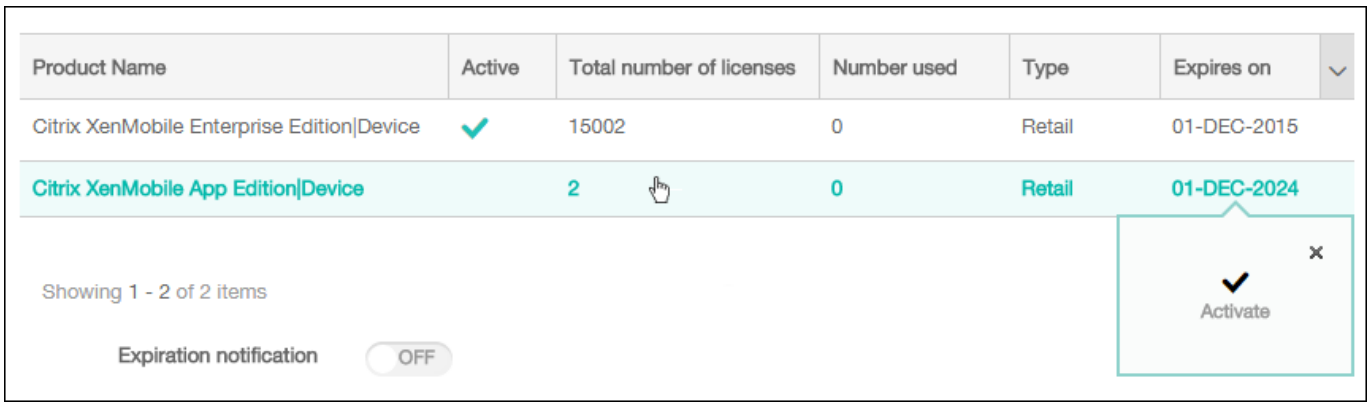
接続に失敗した場合は、表示されるエラーメッセージを確認し、必要な修正を加えてから、**[Test Connection]** をクリックします。



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に1つだけです。

1. **[Licensing]** ページの**ライセンスの表**で、アクティブ化するライセンスの行をクリックします。**[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。



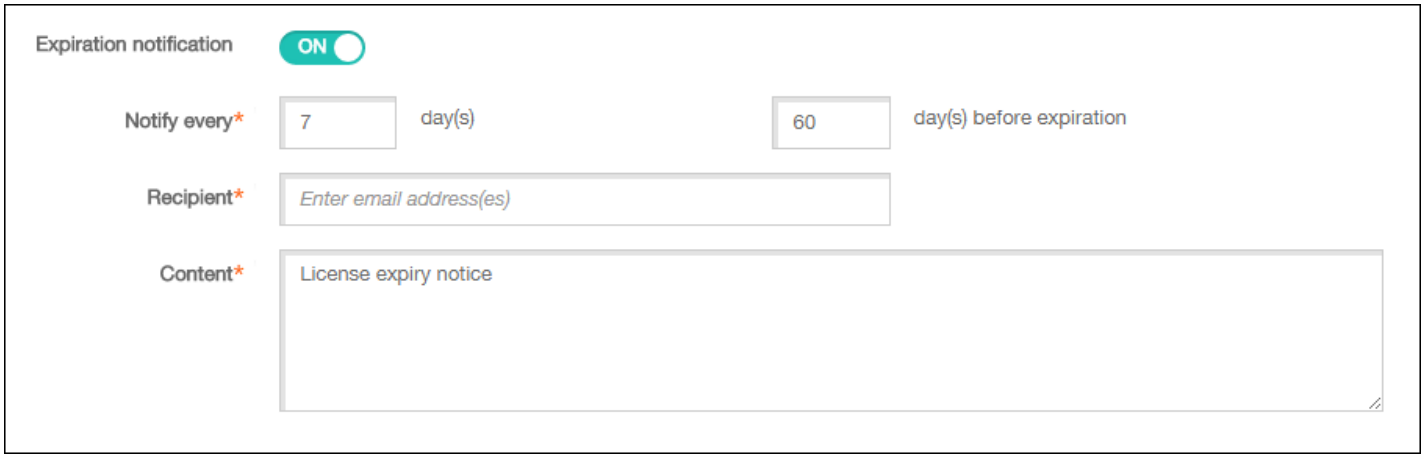
2. **[アクティブ化]** をクリックします。**[アクティブ化]** ダイアログボックスが開きます。
3. **[アクティブ化]** をクリックします。選択したライセンスがアクティブ化されます。

> **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。

- **通知間隔**： 次を入力します。
  - 通知が送信される頻度（**7**日ごとなど）。
  - 通知の送信を開始する時期（ライセンス有効期限の60日前など）。
- **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。設定に基づいて、 **[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。

FIPS 140-2への準拠

Feb 27, 2017

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： FIPSサポートを利用できるのは、XenMobileサーバーがオンプレミスにインストールされている場合のみです。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。

サポート対象のWindowsデバイスでは、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でサポートされ、Windows Phone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。

言語サポート

Apr 05, 2017

XenMobile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。このサポートの対象には、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。

この記事では、最新リリースのXenMobileでサポートされる言語の一覧を示します。

XenMobileコンソールおよびSelf Help Portal

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

XenMobileアプリ

○は、その個別言語でアプリケーションを使用できることを示しています。Secure Formsアプリは、現在英語でのみ利用できます。

注：バージョン10.4のリリース時点で、Worx Mobile AppsはXenMobile Appsに名前が変更されています。個別のXenMobileアプリの大部分も名前が変更されています。詳しくは、「XenMobileアプリについて」を参照してください。

iOSまたはAndroid

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
日本語	○	○	○	○	○	○
簡体字中国語	○	○	○	○	○	○
繁体字中国語	○	○	○	○	○	○
フランス語	○	○	○	○	○	○
ドイツ語	○	○	○	○	○	○
スペイン語	○	○	○	○	○	○

韓国語	○	○	○	○	○	○
ポルトガル語	○	○	○	○	○	○
オランダ語	○	○	○	○	○	○
イタリア語	○	○	○	○	○	○
デンマーク語	○	○	○	○	○	○
スウェーデン語	○	○	○	○	○	○
ヘブライ語	○	○	○	○	○	iOS 9のみ
アラビア語	○	○	○	○	○	○
ロシア語	○	○	○	○	○	○
トルコ語	○	○	Android のみ			

Windows：

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

右書きの言語のサポート

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

	iOS	Android
Secure Hub	○	○
Secure Mail	○	○
Secure Web	○	○
Secure Tasks	○	○
Secure Notes	○	○
QuickEdit	○	○

インストールと構成

Feb 27, 2017

以下の点に注意してください。

次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。

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。

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

インストール前チェックリスト

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	

		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。	XenMobile	
	• 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Secure Hub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	NetScaler Gateway	

	ワークセグメントを入力します。		
	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、「Citrixライセンスシステム」を参照してください。

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

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

	前提要件	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。

前提要件	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

前提要件	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

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

ユーザー接続：XenDesktop、XenApp、およびCitrix Secure Hubへのアクセス

NetScalerのQuick Configurationウィザードを使用して、XenMobileとNetScaler Gatewayの間、XenMobileとSecure Hubの間の接続設定を構成することをお勧めします。第2の仮想サーバーを作成し、Citrix ReceiverおよびWebブラウザーからWindow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。

	前提要件	コンポーネント	設定の記録
	NetScaler Gatewayのホスト名および外部URLを記録します。 外部URLは、ユーザーが接続するWebアドレスです。	XenMobile	
	NetScaler Gatewayコールバック URLを記録します。	XenMobile	
	仮想サーバーのIPアドレスおよびサブネットマスクを記録します。	NetScaler Gateway	
	Program Neighborhoodエージェントまたは 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	
	Secure Hubのパブリック FQDNを記録します。	NetScaler	

		Gateway	

XenMobileのインストール

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

> **注意**
>
> 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 Server 2012、またはWindows Server 2012 R2をインストールします。Hyper-Vの役割をインストールするときは、仮想ネットワークを作成するためにHyper-Vで使用されるサーバー上の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する場合は、「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。

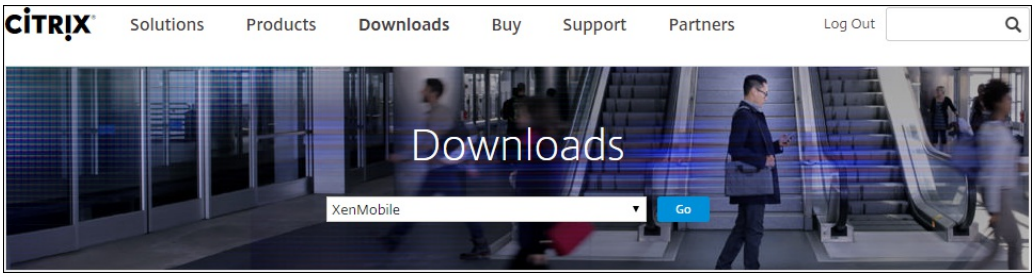
XenMobile製品ソフトウェアのダウンロード

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

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。

> **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

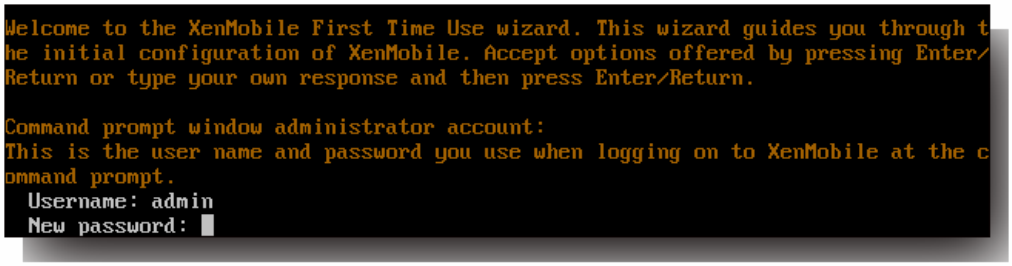
ロパティを構成しないようにお勧めします。それにより、高可用性構成で、2番目のXenMobile仮想マシンを複製してから再起動する場合に発生するIPアドレスの問題を回避できます。

2. XenMobile管理コンソールに、XenMobileサーバーの完全修飾ドメイン名またはノードのIPアドレスのみを使用してアクセスします。

3. ログオンして、初回ログオン画面の手順に従います。

コマンドプロンプトウィンドウでのXenMobileの構成

1. XenMobile仮想マシンをCitrix XenServer、Microsoft Hyper-V、またはVMware ESXiにインポートします。詳しくは、XenServer、Hyper-V、またはVMwareのドキュメントを参照してください。
2. ハイパーバイザーで、インポートしたXenMobile仮想マシンを選択してコマンドプロンプトビューを起動します。詳しくは、ハイパーバイザーのドキュメントを参照してください。
3. ハイパーバイザーのコンソールページから、コマンドプロンプトウィンドウでXenMobileの管理者のユーザー名とパスワードを入力して管理者アカウントを作成します。
   重要：
   コマンドプロンプトで作成する管理者アカウント、公開キー基盤（PKI）サーバー証明書、およびFIPSのパスワードを作成または変更すると、XenMobileでは以下の規則をActive Directoryユーザーを除くすべてのユーザーに適用します。Active DirectoryユーザーのパスワードはXenMobileの外部で管理されます。
   - パスワードは8文字以上にして、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. 以下の情報を入力して「y」を入力し、設定を確定します。
   1. XenMobileサーバーのIPアドレス
   2. ネットマスク
   3. デフォルトゲートウェイ。DMZのデフォルトゲートウェイのIPアドレスです。
   4. プライマリDNSサーバー。DNSサーバーのIPアドレスです。
   5. セカンダリDNSサーバー（オプション）

```
Network settings:
  IP address: 192.0.2.0
  Netmask: 225.225.225.128
  Default gateway: 203.0.113.3
  Primary DNS server: 192.0.2.4
  Secondary DNS server [optional]: 192.0.2.5

  Commit settings [y/n]: y
```

注： この図および後の図に示されているアドレスは実際に使用するためのものではなく、例示のみを目的としています。

5. 「y」を入力して、セキュリティを高めるためにランダムな暗号化パスフレーズを生成するか、「n」を入力して独自のパスフレーズを指定します。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。

```
Encryption passphrase:
  Generate a random passphrase to secure the server data? [y/n]: y
```

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、「FIPS」を参照してください。また、「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。

```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

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。

```
Database connection:
  Local or remote [l/r]: r
  Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi
  Use SSL [y/n]: n
  Server: 198.0.2.10
  Port: 5432
  Username: postgres
  Password:
```

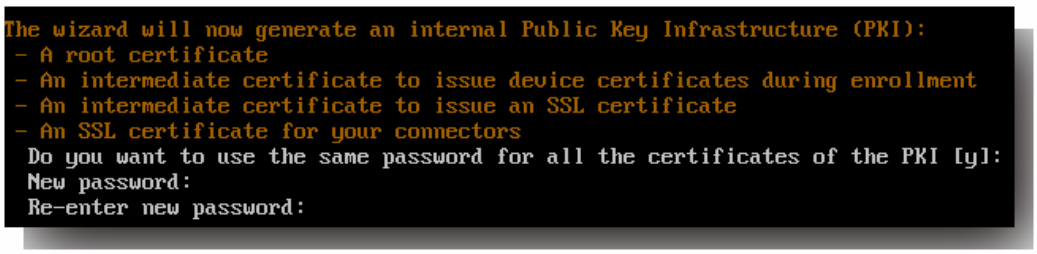
   1. データベースはローカルでもリモートでも構いません。ローカルの場合は「l」を、リモートの場合は「r」を入力します。
   2. データベースの種類を選択します。Microsoft SQLの場合は「mi」を、PostgreSQLの場合は「p」を入力します。
      重要：
      - Citrixでは、Microsoft SQLをリモートで使用することをお勧めします。XenMobileにはPostgreSQLが付属しており、ローカルまたはリモートで、テスト環境においてのみ使用する必要があります。
      - データベースの移行はサポートされていません。テスト環境で作成したデータベ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、 「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、「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。

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

注：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。

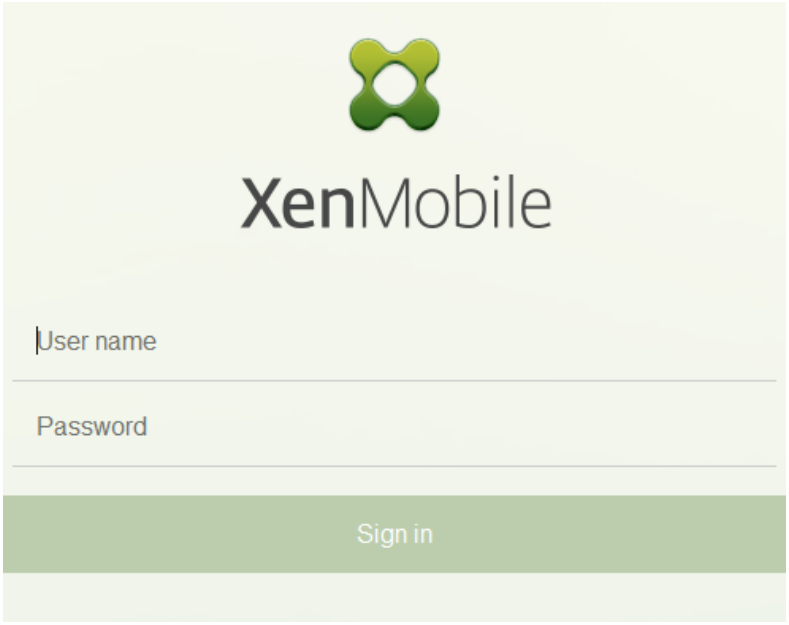
```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app...                              [ OK ]
Starting configuration app...
  application started successfully                         [ OK ]
Stopping main app...                                       [ OK ]
Starting main app...
  this may take a few minutes.....................................................
.................................
  application started successfully                         [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://203.0.113.8:4443/

Starting monitoring...                                     [ OK ]
```

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。ライセンスをアップロードしない場合、30日間有効な評価版ライセンスを使用します。ライセンスの追加と構成、および有効期限切れ通知の構成について詳しくは、「ライセンス管理」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。iOSデバイスを管理するには、APNs証明書が必要です。証明書の取り扱いについて詳しくは、「証明書」を参照してください。

注： この手順ではサーバーを再起動する必要があります。
7. 環境が該当する場合は、NetScaler Gatewayを構成します。NetScaler Gatewayの構成について詳しくは、「NetScaler GatewayとXenMobile」および「XenMobile環境の設定の構成」を参照してください。

注：
- 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、次を参照してください。 通知。

Post-requisite：XenMobileサーバーを再起動して、証明書を有効にします。

XenMobileでのFIPSの構成

Feb 27, 2017

XenMobileの米国の情報処理標準（FIPS：Federal Information Processing Standards）モードは、すべての暗号化操作に対してFIPS 140-2証明済みライブラリのみを使用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。
- セキュアな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. 初期セットアップ時に**FIPSモード**を有効にします。

2. SQL Server用のルートCA証明書をアップロードします。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 **[はい]** 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、「XenMobileへの証明書のアップロード」を参照してください。

3. SQL Serverのサーバー名とポート番号、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。

    SQL ServerでMMC.exeを起動します。

    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サイト（C:\inetpub\wwwroot）にコピーします。

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

4. **[匿名]** を **[有効]** に設定します。

5. **[要求追跡の失敗]** 規則チェックボックスをオンにします。

6. .cerがブロックされていないか確認します。

7. ローカルサーバーのInternt Explorerブラウザーで.cerの場所を参照します（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で有効化されているかを次のようにして確認します。

a. Server Managerを開きます。

[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。

[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、「Web Server (IIS)」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://*<IIS サーバーの完全修飾ドメイン名>*cert.cer
- サーバー： *SQLサーバーの完全修飾ドメイン名*
- 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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

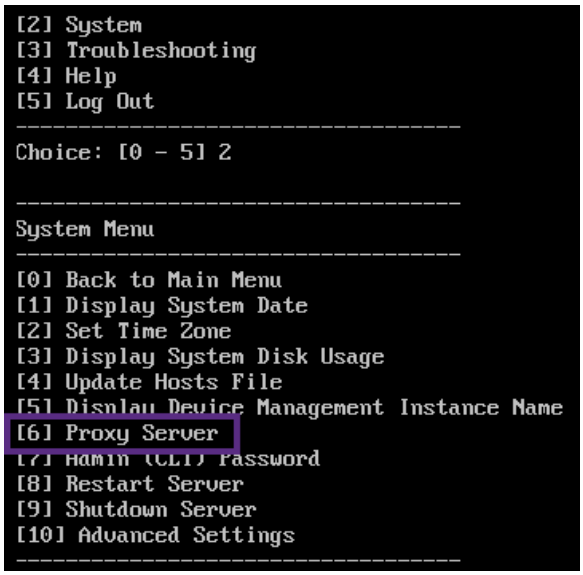
プロキシサーバーの有効化

Feb 27, 2017

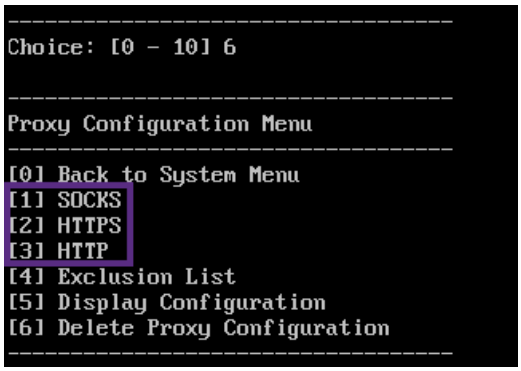
発信インターネットトラフィックを制御するために、そのトラフィックを発信するプロキシサーバーをXenMobileにセットアップできます。これを行うには、コマンドラインインターフェイス（CLI）でプロキシサーバーをセットアップする必要があります。プロキシサーバーのセットアップにはシステムの再起動が必要なことに注意してください。

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。



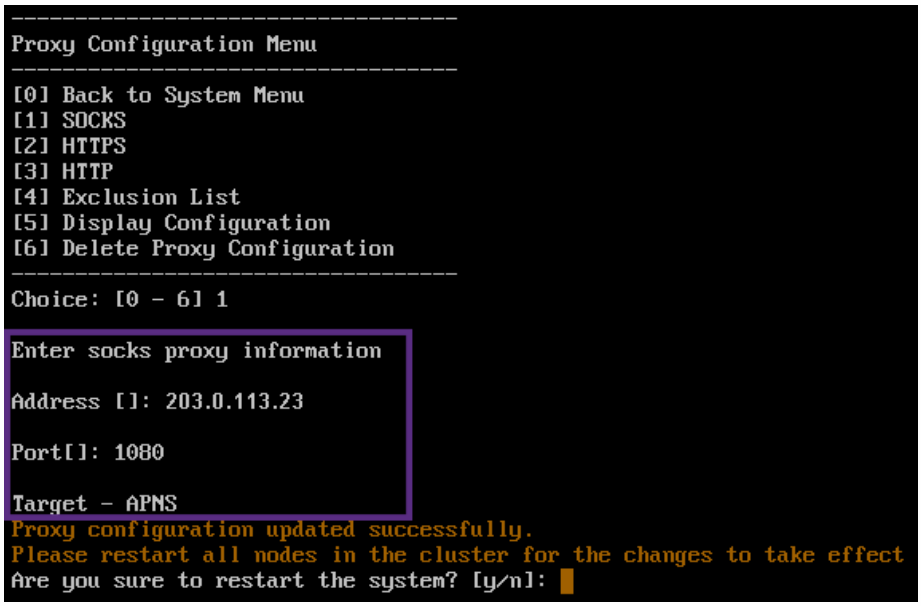
3. ［Proxy Configuration］メニューで、「**1**」と入力して［SOCKS］を選択するか、「**2**」と入力して［HTTPS］を選択するか、「**3**」と入力して［HTTP］を選択します。



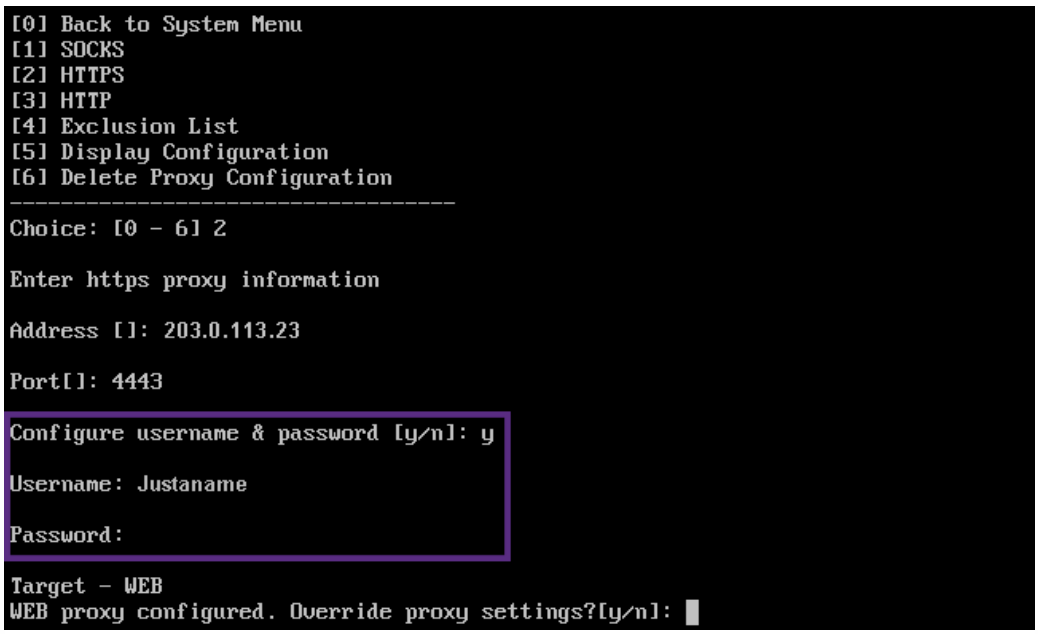
4. プロキシサーバーのIPアドレス、ポート番号、およびターゲットを入力します。プロキシサーバーの種類別の、サポートされるターゲットの種類については以下の表を参照してください。

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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

XenMobileコンソールの導入ワークフロー

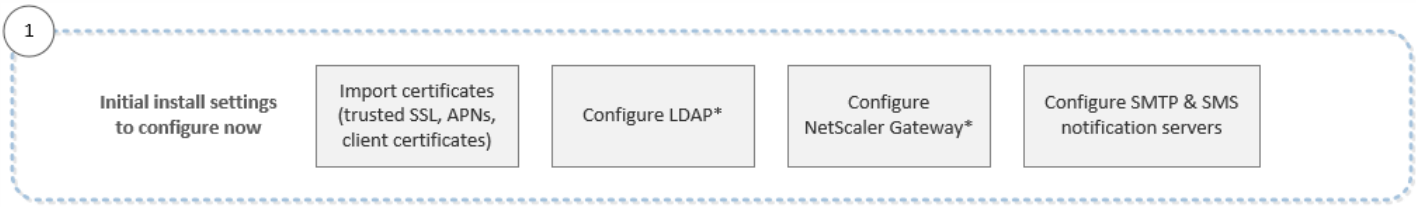
Mar 10, 2017

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

初期設定のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



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

- 認証
- NetScaler GatewayとXenMobile
- 通知

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

Android：

- Google Play資格情報を作成します。詳しくは、Google PlayのLaunch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、「Android at Work」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 G Suite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、ビジネス向けAndroidヘルプを参照してください。

iOS

- Apple IDおよび開発者アカウントを作成します。詳しくは、Apple Developer Program Webサイトを参照してください。
- Appleプッシュ通知サービス（APNs）証明書を作成します。XenMobile Service（クラウド）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。WorxMailの展開でプッシュ通知を使用する場合も、Apple APNs証明書が必要です。Apple APNs証明書の取得方法について詳しくは、Apple Push Certificates Portalを参照してください。XenMobileおよびAPNsについて詳しくは、「APNs証明書」および「WorxMail for iOSのプッシュ通知」を参照してください。
- Volume Purchase Program（VPP）の企業トークンを作成します。詳しくは、「Apple Volume Purchasing Program」を参

照してください。

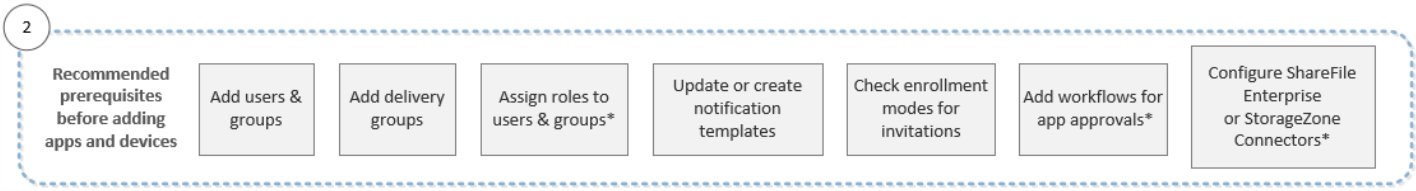
Windows：

- Microsoft Windowsストア開発者アカウントを作成します。詳しくは、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。
- Windows Phoneの登録のためにXenMobile自動検出を活用したい場合は、パブリックなSSL証明書を利用できるようにします。詳しくは、「XenMobile Autodiscoveryサービス」を参照してください。
- アプリケーション登録トークン（AET）を作成します。詳しくは、Microsoft Windows Dev Centerを参照してください。

コンソールの前提条件のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



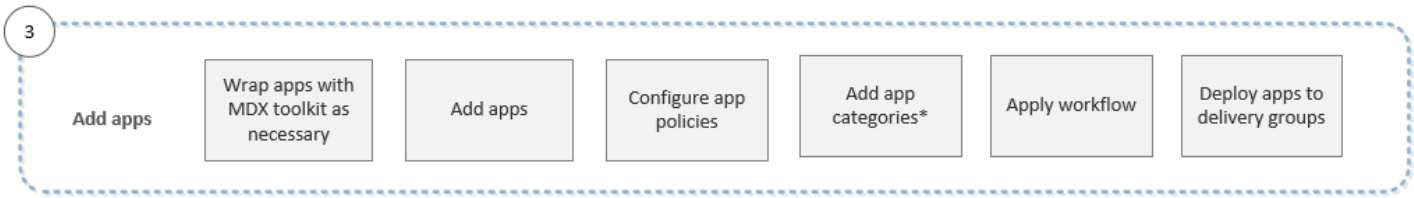
各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントの記事やセクションを参照してください。

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

アプリケーションの追加のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



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

- MDX Toolkitについて
- アプリケーションの追加
- MDXポリシーの概要

- ワークフローの作成および管理
- リソースの展開

デバイスの追加のワークフロー

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

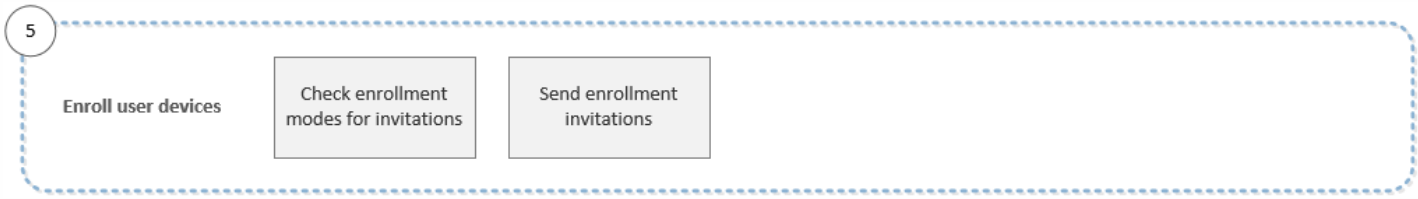
注：アスタリスクが付いている項目はオプションです。

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

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

ユーザーデバイスの登録のワークフロー

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



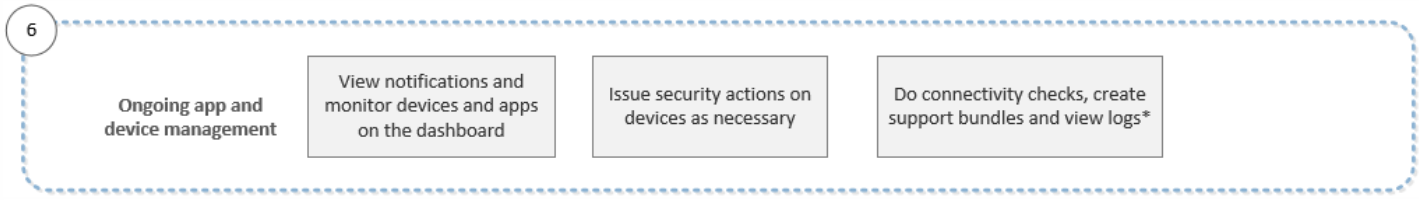
各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントを参照してください。

- ユーザーアカウント、役割、および登録
- 通知

アプリケーションおよびデバイスの継続的な管理のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



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

証明書および認証

Feb 27, 2017

XenMobileの動作では、複数のコンポーネントが認証に関与します。

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

  Secure HubではMDXセキュリティコンテナーも容易になります。Secure Hubは、ポリシーをプッシュし、アプリがタイムアウトするとNetScalerでセッションを作成し、MDXタイムアウトおよび認証エクスペリエンスを定義します。Secure Hubは、ジェイルブレイク検出、地理位置情報チェック、および適用するすべてのポリシーを担当します。

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

一要素、または二要素による認証方法の概要など、認証を構成する方法について検討すべき情報について詳しくは、『Deployment Handbook』のAuthenticationに関するトピックを参照してください。

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

- ドメインまたはドメイン+セキュリティトークン認証
- クライアント証明書、または証明書とドメイン認証の組み合わせ
- PKIエンティティ
- 資格情報プロバイダー
- APNs証明書
- ShareFileでのSAMLによるシングルサインオン
- Microsoft Azure Active Directoryサーバー設定

証明書

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。

> ### 注意
>
> iOS 10.3デバイスでは、自己署名証明書はサポートされません。XenMobileが自己署名証明書を使用する場合は、ユーザーはiOS 10.3デバイスをXenMobileに登録することができません。iOS 10.3以降を実行するデバイスをXenMobileに登録するには、XenMobileで信

> 頼されるSSL証明書を使用する必要があります。

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

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

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

次の表は、各XenMobileコンポーネントの証明書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	.p12（Windowsベースのコンピューターの.pfx）	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。 **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。
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。

アップロードする各証明書は、［証明書］の表で1つのエントリを持ち、その内容がまとめられています。証明書が必要なPK統合コンポーネントを構成するときは、コンテキスト依存の条件を満たすサーバー証明書を選択します。たとえば、

XenMobileをMicrosoft CAと統合するように構成する場合があります。Microsoft CAへの接続はクライアント証明書を使用して認証されます。

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

秘密キーの要件

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

コンソールへの証明書のアップロード

コンソールに証明書をアップロードする場合、主に2つのオプションがあります。

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

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

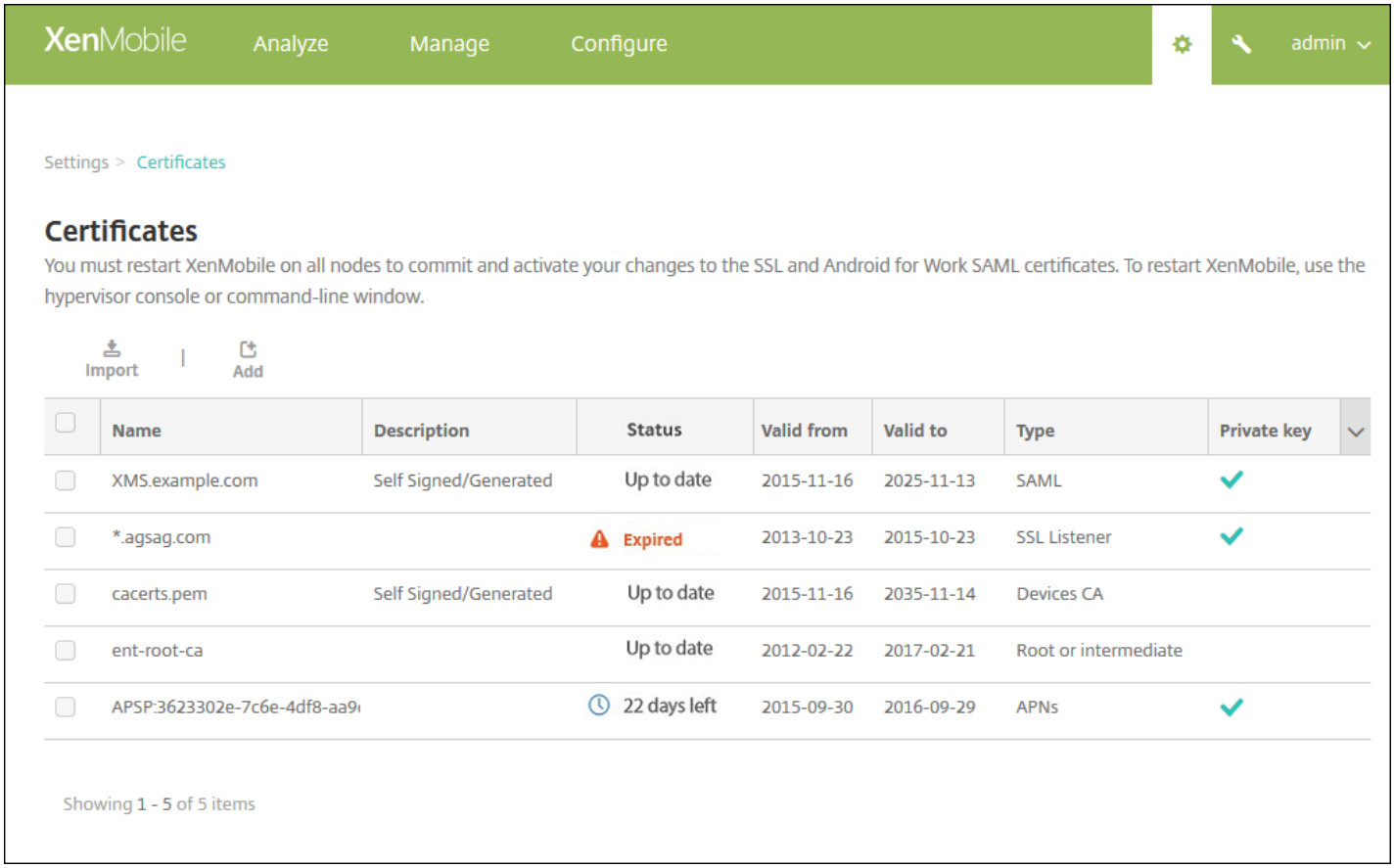
Microsoft CAエンティティを構成する場合は、CA証明書を指定します。CA証明書であるすべてのサーバー証明書の一覧からCA証明書を選択します。同様に、クライアント認証を構成する場合は、XenMobileが秘密キーを持っているすべてのサーバー証明書の一覧から選択できます。

キーストアをインポートするには

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

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

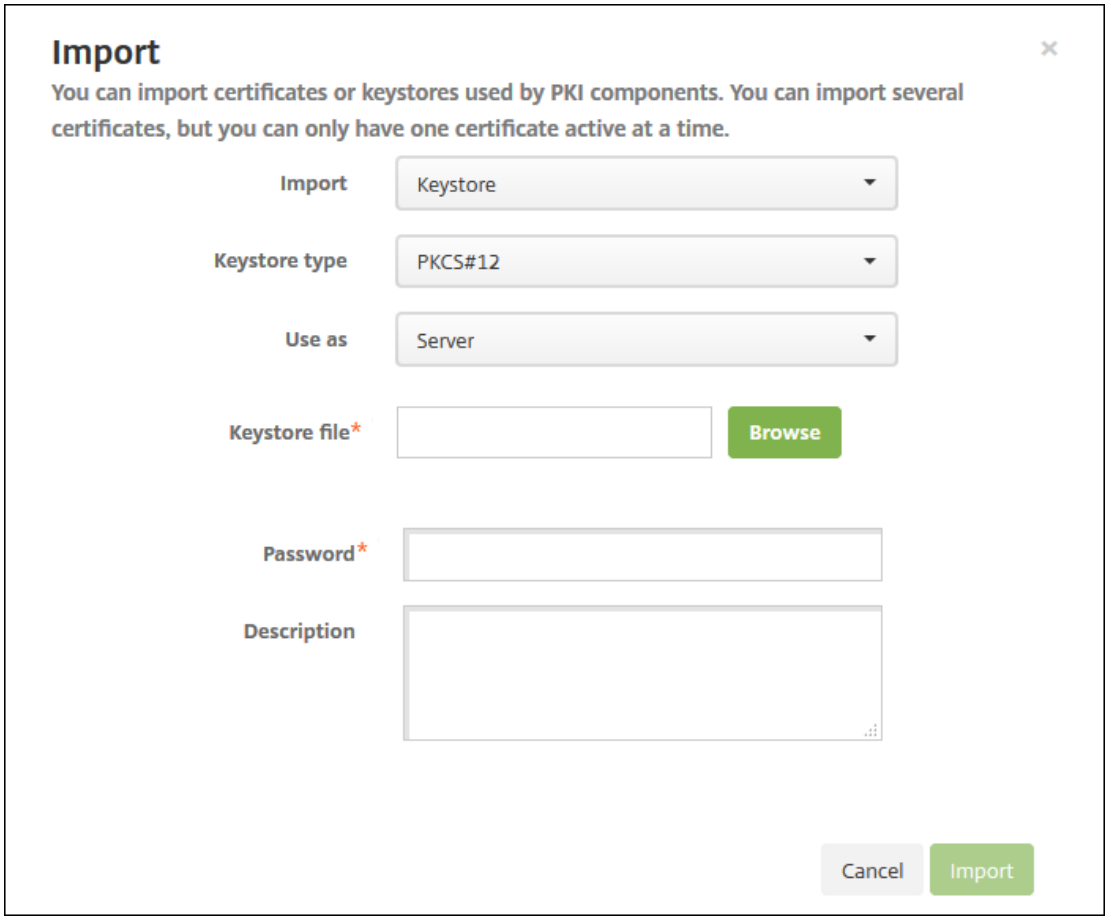
2. **[証明書]**をクリックします。**[証明書]**ページが開きます。



3. **[インポート]** をクリックします。 **[インポート]** ダイアログボックスが開きます。

4. 次の設定を構成します。

- **インポート**： ボックスの一覧から **[キーストア]** をクリックします。 **[インポート]** ダイアログボックスが、使用可能なキーストアオプションを反映した表示に変わります。



- **Keystore type**：ボックスの一覧から、［**PKCS#12**］を選択します。
- **使用目的**：一覧から、証明書の使用方法を選択します。以下の種類から選択できます。
  - **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SSOアクセスを提供できます。
  - **APNs**。AppleのAPNs証明書を使用すると、Apple Push Networkを使用してモバイルデバイスを管理できます。
  - **SSL 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**：インポートするファイル形式.p12（または、Windowsベースのコンピューターで.pfx）のキーストアを参照して指定します。
- **パスワード**：証明書に割り当てられたパスワードを入力します。
- **説明**：任意で、キーストアの説明を入力します。この説明は、ほかのキーストアと区別するときに役立ちます。

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

証明書をインポートするには

ファイルまたはキーストアエントリから証明書をインポートするときに、XenMobileは入力から証明書チェーンの作成を試行し、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、ファイルまたはキーストアエントリの証明書がチェーンを形成する場合にのみ機能します。たとえば、チェーン内の連続する各証明書が前の証明書発行者である場合などです。

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、**[証明書]** をクリックします。

2. **[証明書]** ページで、 **[インポート]** をクリックします。 **[インポート]** ダイアログボックスが開きます。

3. **[インポート]** ダイアログボックスの **[インポート]** の一覧から、まだ選択していない場合は **[証明書]** を選択します。

4. **[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. インポートするファイル形式.p12（または、Windowsベースのコンピューターで.pfx）のキーストアを参照して指定します。

6. 任意で、証明書の秘密キーファイルを参照して指定します。秘密キーは、証明書と共に暗号化と復号化で使用されます。

7. 任意で、証明書の説明を入力します。この説明は、ほかの証明書と区別するときに役立ちます。

8. **[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、または削除することができます。

XenMobileコンソールで、証明書を最も効率的に更新するには、以下の手順に従います。コンソールの右上にある歯車アイコンをクリックして **[設定]** ページを開き、 **[証明書]** をクリックします。 **[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。

XenMobile証明書の管理

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

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

XenMobileサーバー
MDM FQDN用のSSL証明書
SAML証明書（ShareFile用）

前記証明書およびその他の内部リソース（StoreFront/Proxyなど）用のルートおよび中間CA証明書
iOSデバイス管理用のAPN証明書
XenMobileサーバーのSecure Hub通知用の内部APNs証明書
PKIに接続するためのPKIユーザー証明書

MDX Toolkit
Apple Developer証明書
Appleプロビジョニングプロファイル（アプリケーションごと）
Apple APNs証明書（Citrix Secure Mail用）
Android Keystoreファイル
Windows Phone – Symantec証明書

NetScaler
MDM FQDN用のSSL証明書
Gateway FQDN用のSSL証明書
ShareFile SZC FQDN用のSSL証明書
Exchangeでの負荷分散用のSSL証明書（オフロード構成）
StoreFrontでの負荷分散用のSSL証明書
前記証明書用のルートおよび中間CA証明書

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

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

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

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

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

また、有効期限の30日前と10日前に、Appleから以下の情報を記載したメール通知を受信します。

「Apple IDカスタマーIDで作成した次のAppleプッシュ通知サービス証明書がまもなく期限切れです。これらの証明書を取り消した場合、または証明書が期限切れになった場合、既存のデバイスを再登録する必要があります。

ベンダーに連絡して新しい要求（署名済みCSR）を生成し、https://identity.apple.com/pushcertでAppleプッシュ通知サービ

ス証明書を更新してください。

よろしくお願いいたします。

Appleプッシュ通知サービス」

物理的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にプロビジョニングプロファイルで署名する必要があります。そのアプリケーションには対応する配布用証明書でも署名する必要があります。

有効なiOS配布証明書があるかを確認するには、以下の操作を行います。

1. Apple Enterprise Developerポータルから、MDX Toolkitでラップする各アプリで新しいプロビジョニングプロファイルと一意で明示的なアプリIDを作成します。有効なApp IDの例：com.CompanyName.ProductName。
2. Apple Enterprise Developerポータルから、**[Provisioning Profiles]** > **[Distribution]** に移動して、社内プロビジョニングプロファイルを作成します。前述の手順で作成されたApp IDごとに、この手順を繰り返します。
3. すべてのプロビジョニングプロファイルをダウンロードします。詳しくは、「iOSモバイルアプリ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であることを確認するには、以下の操作を行います。

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

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

Symantecは、Microsoft App Hubサービスのコード署名証明書を提供する唯一のプロバイダーです。開発者およびソフトウェアの発行元はMicrosoft App Hubに参加して、Windows MarketplaceからダウンロードされるWindows PhoneおよびXbox 360アプリケーションを配布します。詳しくは、「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た場合、Windows phoneユーザーは登録できません。ユーザーは同社が公開し署名したアプリのインストール、Windows phoneにインストールされた会社のアプリの起動ができなくなります。

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

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

Expiry MonitorおよびCommand Centerによって、NetScaler証明書の記録を確認できます。証明書の有効期限が切れるとCommand Centerから通知が送信されます。この2つのツールは、以下のNetScaler証明書の監視に役立ちます。

MDM FQDN用のSSL証明書
Gateway FQDN用のSSL証明書
ShareFile SZC FQDN用のSSL証明書
Exchangeでの負荷分散用のSSL証明書（オフロード構成）
StoreFrontでの負荷分散用のSSL証明書
前記証明書用のルートおよび中間CA証明書

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

PKIエンティティ

Feb 27, 2017

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証明書サービス

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

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、PK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（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。

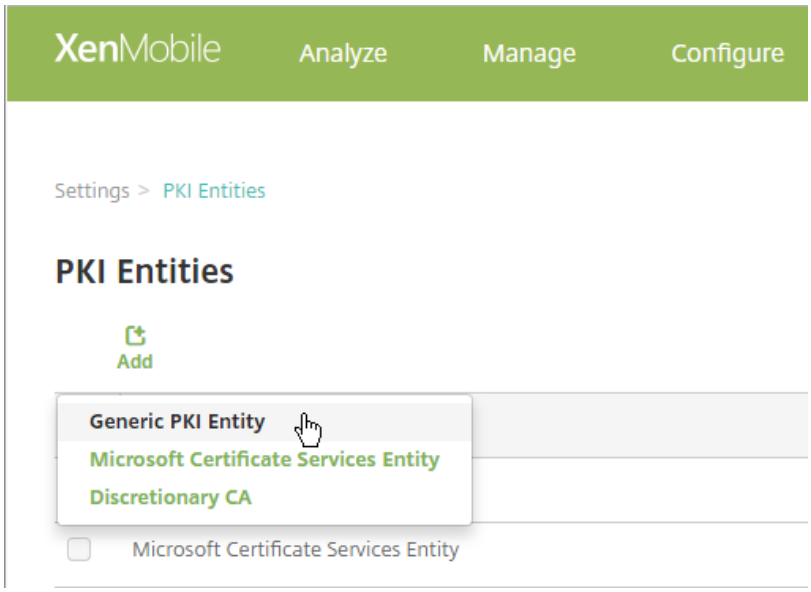
アダプターでの各PKI操作のサポートはオプションです。アダプターが特定の処理をサポートする場合、アダプターには対応する機能（署名、フェッチ、失効）があると見なされます。これらの各機能は一連のユーザーパラメーターに関連付けられている場合があります。

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。

1. XenMobileコンソールで、 **[設定]** > **[PKIエンティティ]** の順にクリックします。

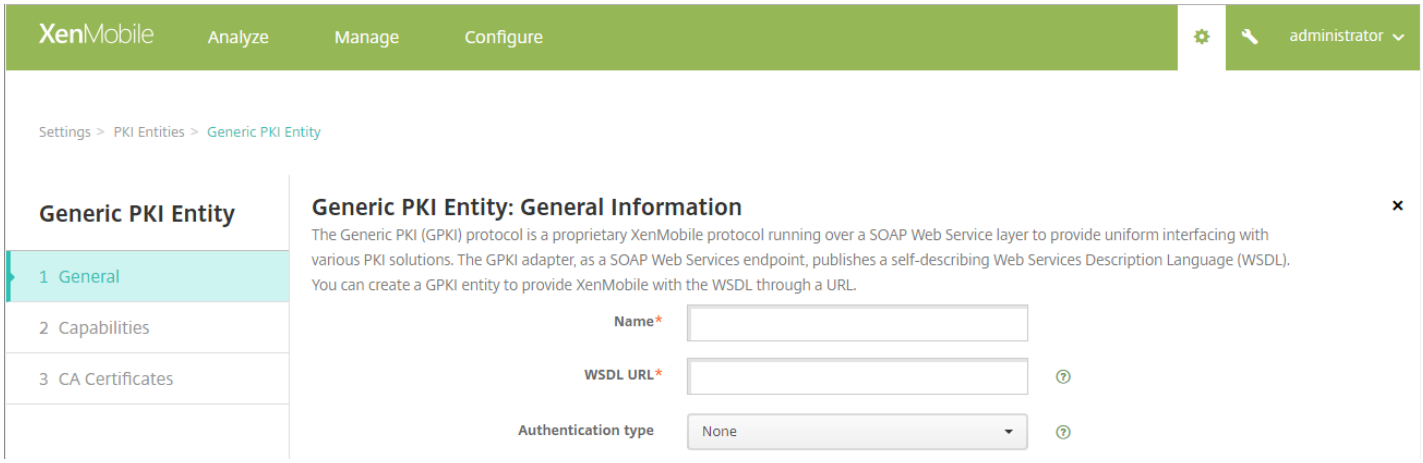
2. **[PKIエンティティ]** ページで、 **[追加]** をクリックします。

PKIエンティティの種類を示すメニューが表示されます。



3. **[汎用PKIエンティティ]** をクリックします。

［汎用PKIエンティティ：一般情報］ページが開きます。



4. **[汎用PKIエンティティ： 一般情報]** ページで次の操作を行います。

- **名前**： PKIエンティティの説明的な名前を入力します。
- **WSDL URL**：アダプターについて記述しているWSDLの場所を入力します。
- **Authentication type**：一覧から、使用する認証方法を選択します。
- **なし**
- **HTTP基本**： アダプターへの接続に必要なユーザー名とパスワードを指定します。
- **クライアント証明書**：適切なSSLクライアント証明書を選択します。

5. **[次へ]** をクリックします。

［汎用PKIエンティティ：アダプターの機能］ページが開きます。

6. **[汎用PKIエンティティ： アダプターの機能]** ページで、アダプターに関連付けられた機能とパラメーターを確認して、 **[次へ]** をクリックします。

[汎用PKIエンティティ： CA証明書の発行] ページが表示されます。

7. ［汎用PKIエンティティ：CA証明書の発行］ページで、エンティティで使用する証明書を選択します。

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 **[ディストリビューション]** ページで、ここで構成したいずれかの証明書を選択してください。

8. **[保存]** をクリックします。

［PKIエンティティ］の表にエンティティが表示されます。

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。

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、**[PKIエンティティ]** をクリックします。

2. **[PKIエンティティ]** ページで、 **[追加]** をクリックします。

PKIエンティティの種類を示すメニューが表示されます。

3. **[Microsoft証明書サービスエンティティ]** をクリックします。

[Microsoft証明書サービスエンティティ： 一般的な情報] ページが開きます。

4. **[Microsoft証明書サービスエンティティ： 一般的な情報]** ページで次の設定を構成します。

- **名前**：新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意の名前にする必要があります。
- **Web登録サービスルートURL**：Microsoft CA Web登録サービスのベースURL（https://192.0.2.13/certsrv/など）を入力します。URLには、HTTPまたはHTTP-over-SSLを使用します。
- **certnew.cerページ名**：certnew.cerページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- **certfnsh.asp**：certfnsh.aspページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- **認証の種類**： 使用する認証方法を選択します。
  - **なし**
  - **HTTP基本**： 接続に必要なユーザー名とパスワードを指定します。
  - **クライアント証明書**： 適切なSSLクライアント証明書を選択します。

5. **[接続のテスト]** をクリックして、サーバーがアクセス可能であることを確認します。アクセスできない場合、接続に失敗したことを示すメッセージが表示されます。構成設定をチェックしてください。

6. **[次へ]** 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 Certificate Servicesテンプレートの要件は、お使いのMicrosoft ServerバージョンのMicrosoftドキュメントを参照してください。XenMobileには、「証明書」で説明している証明書の形式以外、配布する証明書の要件はありません。

7. **[Microsoft証明書サービスエンティティ：テンプレート]** ページで **[追加]** をクリックし、テンプレートの名前を入力して、 **[保存]** をクリックします。追加する各テンプレートについて、この手順を繰り返します。

8. **[次へ]** をクリックします。

[Microsoft 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。

9. **[Microsoft証明書サービスエンティティ：パラメーター]** ページで **[追加]** をクリックし、追加するHTTPパラメーターの名前と値を入力して、 **[次へ]** をクリックします。

[Microsoft 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。

10. **[Microsoft証明書サービスエンティティ：CA証明書]** ページで、このエンティティで使用する証明書を選択します。

11. **[保存]** をクリックします。

［PKI Entities］の表にエンティティが表示されます。

XenMobileは、サードパーティ証明機関でのみ証明書失効一覧（CRL）をサポートします。Microsoft CAが構成されている場合、XenMobileはNetScalerを使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、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。

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、**[詳細]** の **[PKIエンティティ]** をクリックします。

2. **[PKIエンティティ]** ページで、 **[追加]** をクリックします。

PKIエンティティの種類を示すメニューが表示されます。

3. **[任意CA]** をクリックします。

任意CA： 一般情報] ページが開きます。

4. **[任意CA： 一般情報]** ページで次の操作を行います。

- **名前**： 任意CAの説明的な名前を入力します。
- **証明書要求に署名するためのCA証明書**： 一覧から、証明書要求に署名するために使用する任意CAの証明書を選択します。この証明書一覧は、 **[構成]** 、 **[設定]** 、 **[証明書]** 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. [次へ] をクリックします。

[任意CA： パラメーター] 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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

アップグレード

Apr 13, 2017

Important

XenMobile 10.5（オンプレミス）にアップグレードする前に

1. アップグレードするXenMobile Serverを実行する仮想マシンのRAMが4GB未満の場合、最低4GBにRAMを増設してください。実稼働環境では、推奨される最小RAM容量は8GBであることに留意願います。
2. Windowsタブレットの場合、デバイスのパスコードポリシーと制限ポリシーの構成をメモしてください。これらのポリシーはWMIベースではなくなりました。そのため、アップグレードによって既存の構成が削除されます。アップグレード後に、Windowsタブレットデバイスのパスコードポリシーと制限ポリシーを再構成してください。
3. XenMobile管理コンソールにアクセスするには、XenMobile Serverの完全修飾ドメイン名（登録FQDN）またはノードのIPアドレスを使用します。負荷分散用仮想IPアドレスまたはNAT'd IPアドレスによるコンソールへの直接のアクセス機能は、2017年3月22日にリリースされたXenMobile Server 10.5 Rolling Patch 1がインストールされていない限り利用できなくなりました。このパッチは2017年3月22日にリリースされました。詳しくは、https://support.citrix.com/article/CTX221304を参照してください。
4. 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。

XenMobileの新しいバージョンや重要な更新はCitrix.comに公開されます。さらに、各ユーザーレコードの連絡先に通知が送信されます。

XenMobileのアップグレードには次の選択肢があります。

- **XenMobile 9.0からXenMobileの最新リリースにアップグレードする。**
  XenMobileの最新リリースに標準のXenMobileアップグレードツールを使用します。詳しくは、このセクションの記事を参照してください。
  アップグレードツールは、XenMobile 9のすべてのエディション（MDM、AppおよびEnterprise）をサポートします。
  解決された問題と既知の問題については、「解決された問題」および「既知の問題」を参照してください。
  Citrix.comで以前のアップグレードツールをダウンロードすることはできなくなりました。

- **XenMobile 10.3.6またはXenMobile 10.4からXenMobile 10.5にアップグレードする。**
  XenMobileコンソールで **[リリース管理]** ページを使用します。詳しくは、この記事の手順を参照してください。
  XenMobile 9.0以外のバージョンには、アップグレードツールは使用しません。

- **XenMobile 10またはXenMobile 10.1からXenMobile 10.5にアップグレードする。**
  まず、XenMobileコンソールの **[リリース管理]** ページを使用して、XenMobile 10またはXenMobile 10.1からXenMobile 10.3.6にアップグレードします。次に、XenMobileコンソールの **[リリース管理]** ページを使用して、XenMobile 10.3.6からXenMobile 10.5にアップグレードします。詳しくは、この記事の手順を参照してください。これら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 Server version	Release number	Upgrade to	Release number	Upgrade path	Update location
XenMobile Server 9（App Controller Rolling Patch 9インストール済み）	9.0.0_97106	XenMobile Server 10.5	10.5.0.24	XenMobile Server 9から XenMobile Server 10.5	App Controller Rolling Patchの必須コンポーネントをダウンロードします。 • XenMobile 10.5用のアップグレードツールは XenMobile Serverに内蔵されています。 • 詳しくは、「アップグレードツールの前提条件」を参照してください。
XenMobile Server 10または XenMobile Server 10.1	10.1.0.63030	XenMobile Server 10.3.6	10.3.6	XenMobile 10または XenMobile 10.1から XenMobile 10.3.6にアップグレード	ダウンロード
XenMobile Server 10.3.6	10.3.6	XenMobile Server 10.5	10.5.0.24	XenMobile 10.3.xから XenMobile 10.5にアップグレード	ダウンロード
XenMobile Server 10.4	10.4.x	XenMobile Server 10.5	10.5.0.24	XenMobile 10.4から XenMobile 10.5にアップグレード	ダウンロード

[リリース管理] ページを使用して、サポートされているXenMobile 10のバージョン（上の表に記載）から最新バージョンのXenMobile Serverにアップグレードします。

前提条件

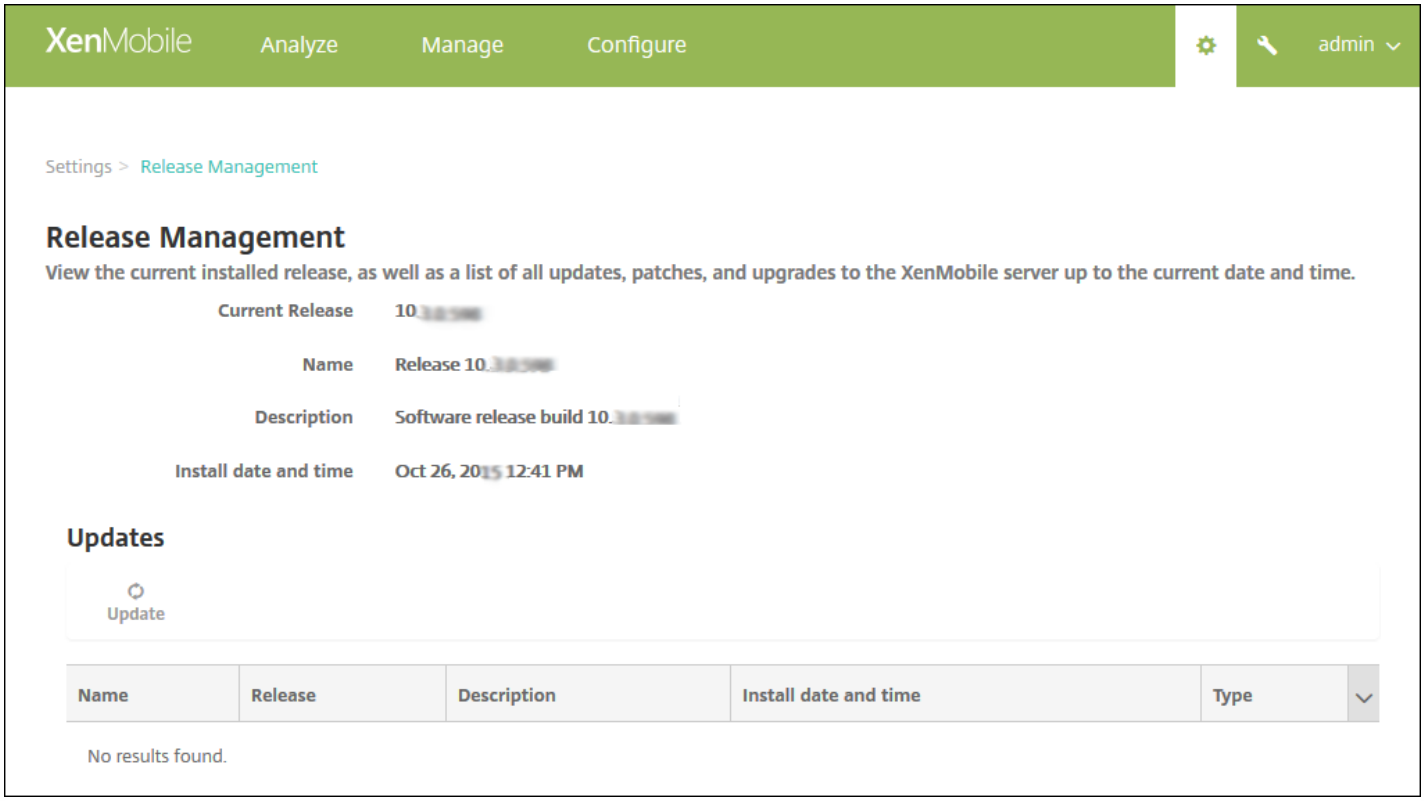
- XenMobileの更新をインストールする前に、仮想マシン（VM）の機能を使用して、システムのスナップショットを取得してください。
- システム構成データベースをバックアップしてください。
- 更新するバージョンに関しては、「システム要件」を参照してください。XenMobileの最新バージョンに関しては、「システム要件」を参照してください。

クラスター展開の場合、このトピックの最後にある手順を参照してください。

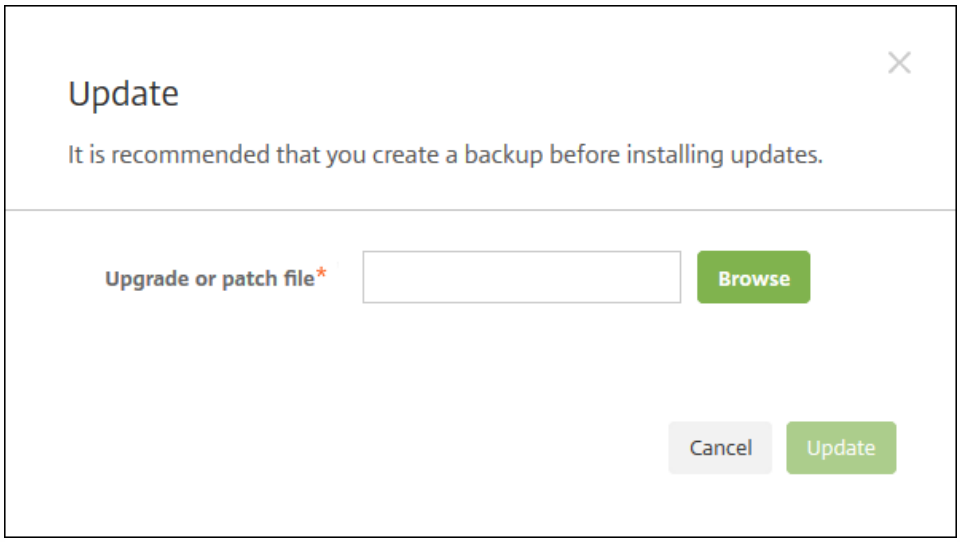
1. Citrix Webサイトのアカウントにログオンして、XenMobile Upgrade（.bin）ファイルを適切な場所にダウンロードします。

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。**[設定]** ページが開きます。

3. **[リリース管理]** をクリックします。**[リリース管理]** ページが開きます。



4. **[更新プログラム]** の下の **[更新]** をクリックします。 **[更新]** ダイアログボックスが開きます。



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

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

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

注：アップグレード後、XenMobileを再起動する必要があります。XenMobile CLIを使用してXenMobile Serverを再起動して

ください。システムの再起動後にブラウザーのキャッシュを消去することが重要です。

クラスター化されたXenMobile展開にアップグレードするには

システムがクラスターモードで構成されている場合、以下の手順に従ってXenMobile 10リリースから各ノードを更新します。

1. **[設定]** > **[リリース管理]** から、すべてのノードに.binファイルをアップロードします。

2. コマンドラインインターフェイスの **[システムメニュー]** ですべてのノードをシャットダウンします。

3. コマンドラインインターフェイスの **[システムメニュー]** で1つのノードを起動し、サービスが実行されているか確認します。

4. 他のノードを1つずつ起動します。

XenMobileが更新を完了できなかった場合は、問題を示すエラーメッセージが表示されます。XenMobileによってシステムに更新を試行する前の状態に戻ります。

アップグレードツールの前提条件

Feb 27, 2017

XenMobile 9.0から最新バージョンのXenMobileにアップグレードするには、XenMobile標準の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次のものをサポートします。

- すべてのXenMobile Serverモード（ENT、MAM、MDM）で登録されたiOSおよびAndroidデバイス
- MDMモードで登録済みのWindows Phoneおよびタブレット
- Enterpriseモードで登録済みのWindows Phone
- MDMモードのWindows CEデバイス

XenMobile 9.0でマルチテナントコンソール（Multi-Tenant Console：MTC）が有効化されている場合は、MTCを最新バージョンのXenMobileのスタンドアロンの展開に移行できます。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。この記事の前提条件を完了したら、「MTCテナントサーバーからXenMobileへのアップグレード」を参照してください。

最新バージョンのXenMobileは、NetScaler Gatewayのバージョン11.1.x、11.0.x、および10.5.xをサポートしています。

XenMobile内蔵のアップグレードツールは、NetScaler Gatewayのバージョン10.1.xもサポートしています。NetScaler Gateway 10.1を最新バージョンのXenMobileと共に使用することはサポートされていません。ただし、XenMobile内蔵のアップグレードツールを使用して、NetScaler Gateway 10.1の展開をアップグレードできます。その後で、NetScaler Gatewayをサポートされている最新バージョンにアップグレードすることをお勧めします。

> ## Important
>
> アップグレード処理は複雑です。アップグレードを開始する前に、必ず、この記事の説明に従って既知の問題を確認し、アップグレードを計画し、前提条件をすべて完了します。また、このブログにある前提条件のチェックリストは、アップグレードを計画する助けになります。
>
> アップグレードツールの実行後、すべてのアップグレード後要件を完了していることを確認します。
>
> 前提条件を完了していない場合、アップグレードが失敗することがあります。最新バージョンのXenMobileの新しいインスタンスをコマンドラインコンソールで構成し、アップグレードツールを再開する必要があります。

次の段階でアップグレードすることをお勧めします。

1. 体験版アップグレードをステージング環境で実行し、前提条件とアップグレードツールの手順をすべて完了します。まず体験版アップグレードを実行して、一連の過程がどのようなものになるか、実稼働環境を完全にアップグレードした後の予想結果の感触をつかむことをお勧めします。体験版アップグレードは、ユーザーデータでなく構成データのアップグレードをテストします。

NetScaler 11.1（または最小バージョンNetScaler 10.5）では、NetScaler for XenMobileウィザードを使用して、フレッシュなNetScalerをNetScaler GatewayおよびNetScaler負荷分散仮想サーバーに設定することをお勧めします。

2. 体験版アップグレードで、構成データ（たとえばLDAP、ポリシー、およびアプリ）が正しくアップグレードされたことを

確認します。テストデバイスを確認します。

3. 実際の稼働環境で実稼働環境のアップグレードを実行して本稼働に入ります。アップグレードのためのサービス停止時間を計画します。

体験版アップグレードと実稼働環境のアップグレードについて

XenMobileアップグレードツールを使用して、まずアップグレードをテストし、続いて実稼働環境を完全にアップグレードします。

体験版を選択した場合：
アップグレードツールが実稼働環境の構成データで体験版アップグレードを実行して、実稼働環境に影響を与えずにXenMobile 9.0と最新バージョンのXenMobile を比較できます。体験版アップグレードでは構成データのみがテストされます。デバイスデータ（XenMobile Enterprise Edition展開の場合）またはユーザーデータはテストされません。

体験版アップグレードの結果は、テストだけのためのものです。体験版アップグレード展開をアップグレードすることはできません。その代わりに、もう一度実稼働環境のアップグレードからはじめる必要があります。体験版アップグレードは、すべてのXenMobile 9.0エディションで動作します。

アップグレードを選択した場合:
アップグレードツールはまずすべての構成、デバイス、およびユーザーデータをXenMobile 9.0から、同じ完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を持つ最新バージョンのXenMobileの新しいインスタンスにコピーします。XenMobile 9.0は、新しいXenMobileサーバーインスタンスを実稼働環境に移すまで一切変更されません。

アップグレード後に新しいXenMobileサーバーインスタンスのコンソールにログオンすると、アップグレードでXenMobile 9.0から移行されたすべてのユーザーおよびデバイスデータが表示されます。

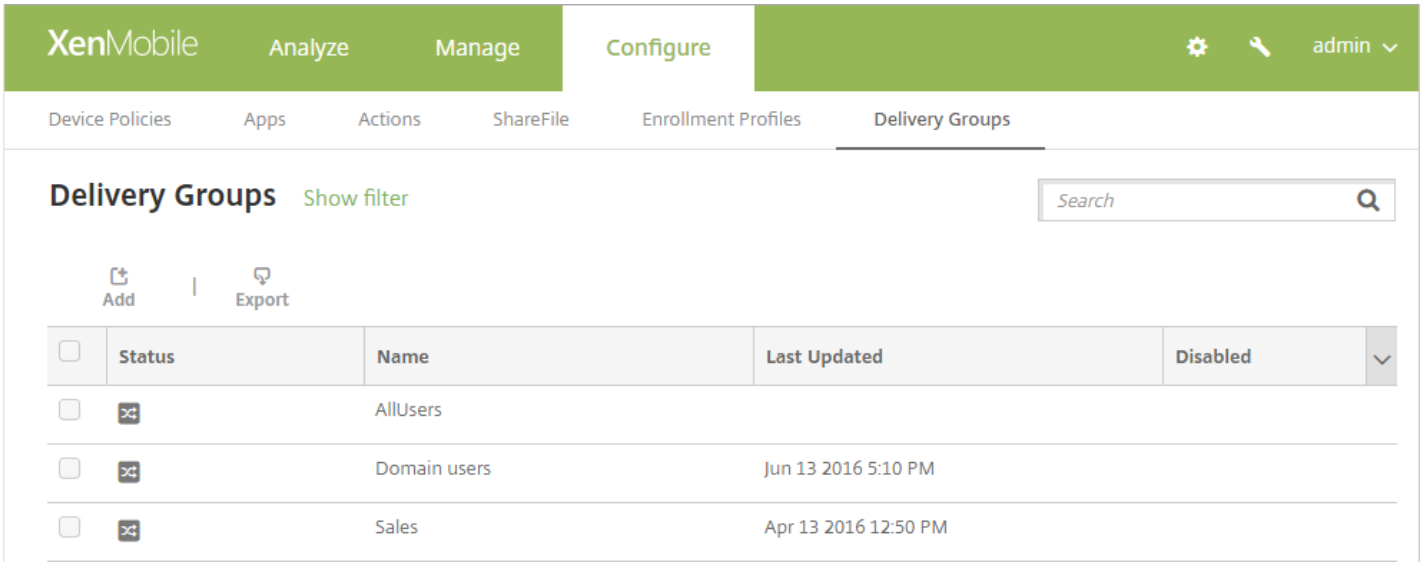
アップグレードツールで実行されない内容

アップグレードツールを使用した場合、次の情報は最新バージョンのXenMobileにアップグレードされません。

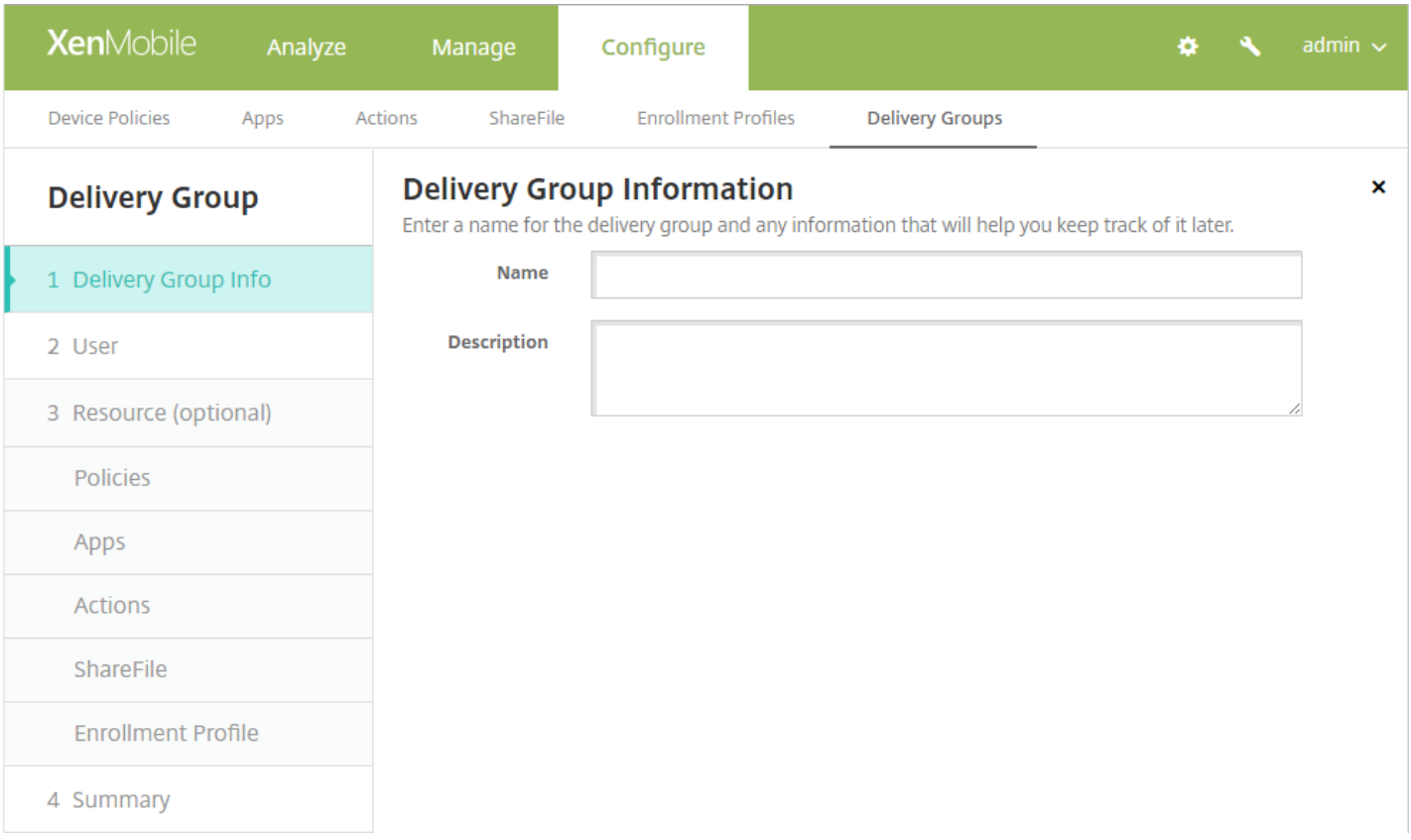
- ライセンス情報
- レポートのデータ
- サーバーグループのポリシーおよび関連する展開（最新バージョンのXenMobileでサポートされません）
- Managed Service Provider（MSP）グループ
- Windows 8.0に関連するポリシーおよびパッケージ
- 使用していない展開パッケージ（展開パッケージにユーザーまたはグループが割り当てられていない場合など）
- アップグレードログファイル内に記述されている、そのほかの構成またはユーザーデータ
- CXM Web（Citrix Secure Webに置き換えられます）
- DLPポリシー（Citrix Sharefileに置き換えられます）
- カスタムのActive Directoryの属性
- XenMobile 9.0で複数のブランド設定ポリシーを構成している場合、ブランド設定ポリシーはアップグレードされません。最近のバージョンのXenMobileでは1つのブランド設定ポリシーがサポートされます。正常に最新バージョンのXenMobileにアップグレードするには、XenMobile 9.0のブランド設定ポリシーを1つに維持する必要があります。
- コンソールへのアクセスの制限に使用される、XenMobile 9.0のauth.jspファイル内の設定。最新バージョンのXenMobileのコンソールへのアクセス制限は、コマンドラインインターフェイスで構成できるファイアウォール設定です。
- Syslogサーバーの構成
- XenMobile 9.0で構成されたフォーム入力コネクタ（最新バージョンのXenMobileでサポートされません）

XenMobileの変更

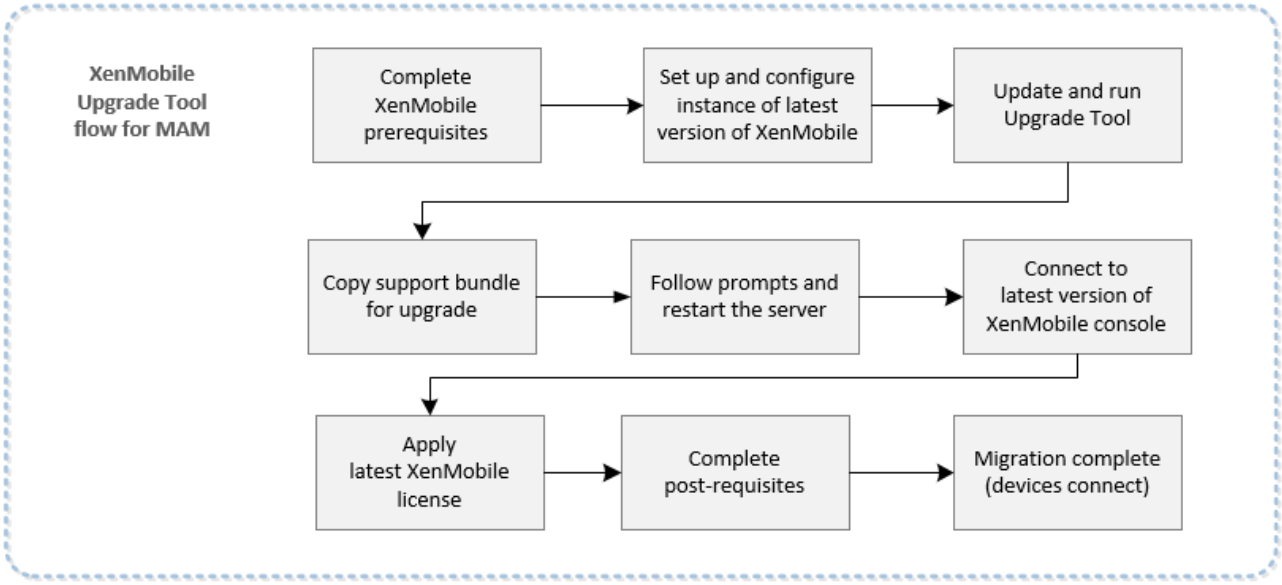
- アップグレードツールでは、ローカルグループに割り当てられたActive Directoryユーザーはアップグレードされません。後からActive Directoryユーザーをローカルグループに割り当てることができます。
- XenMobile 10では、入れ子になったローカルグループはサポートされていません。XenMobile 9からアップグレードすると、ローカルグループの階層がフラット化されます。
- 次の図に示すように、Device Managerの展開パッケージはXenMobileではデリバリーグループと呼ばれます。詳しくは、「リソースの展開」を参照してください。

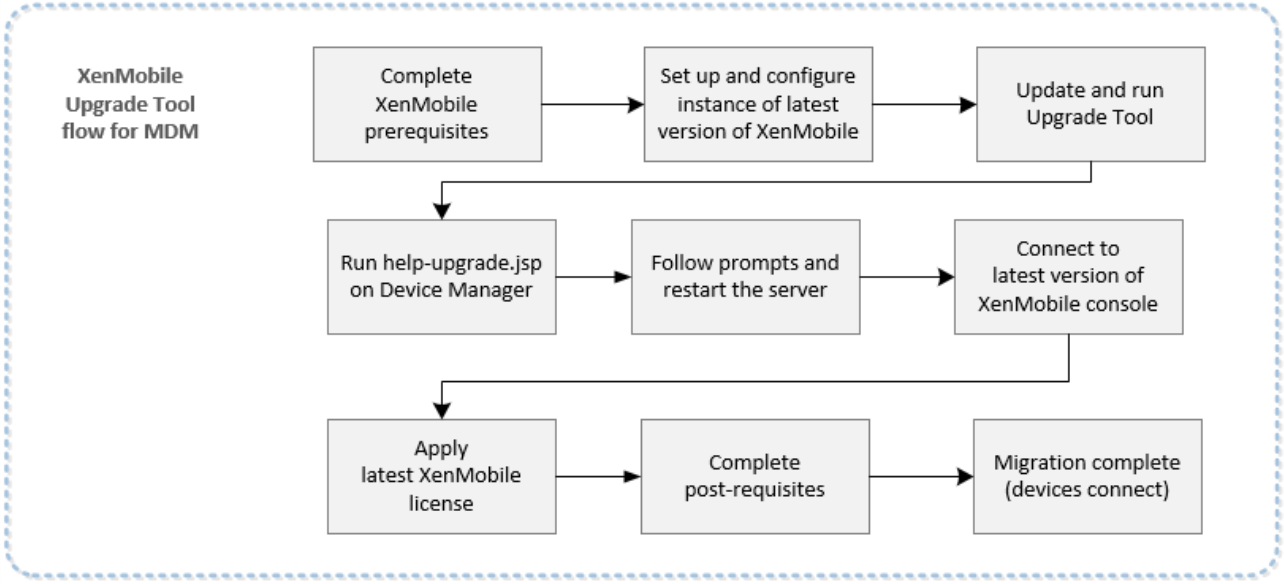


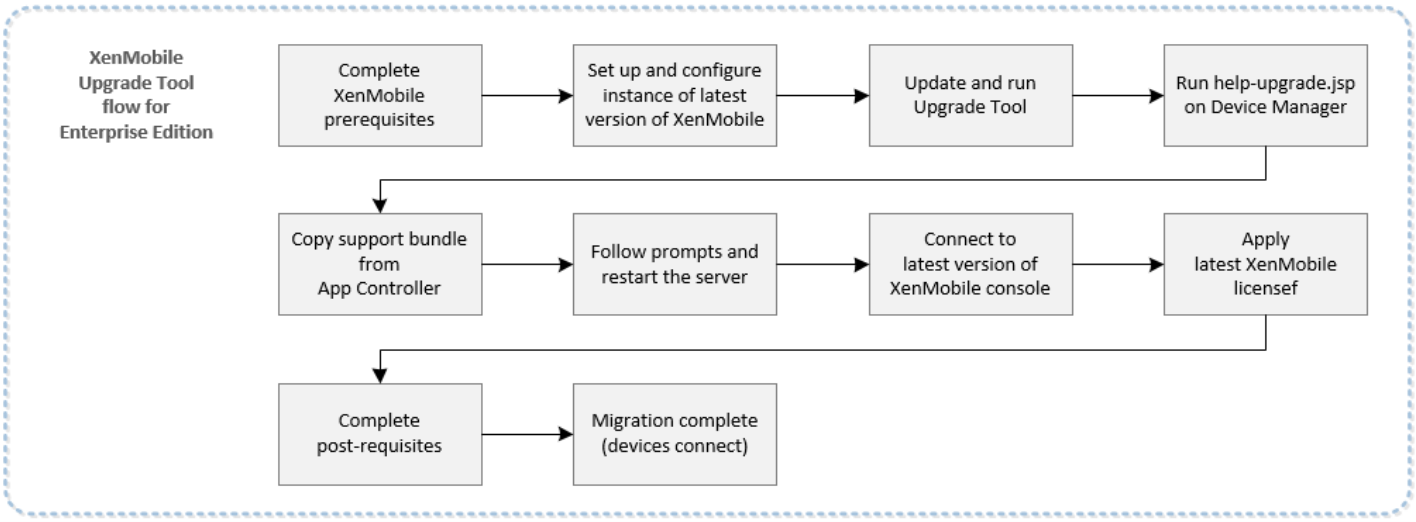
デリバリーグループ内では、リソースを必要とするユーザーのグループに必要なポリシー、アクション、およびアプリケーションを表示できます。



次の図は、XenMobile 9.0からアップグレードする場合に実行する基本的な手順を示しています。







Windows PhoneがEnterpriseモードで登録されており、Worx Home 9.xを使用している場合、XenMobile 9.0 Enterprise環境の最新バージョンのXenMobileへのアップグレードでは以下の手順が推奨されます。

1. Device Manager上のWorx HomeをWorx Home 10.2以降にアップグレードしてから、Worx Home 10.2を展開します。

2. ユーザーデバイスから手動でWorx Home 9.xをアンインストールします。

3. ユーザーに、Windows PhoneでDownload Hubにアクセスして、Device Managerで展開したWorx Home 10.2以降をインストールするように伝えます。

4. この記事で説明した前提条件の完了後、「XenMobileアップグレードツールの有効化および実行」の説明に従って、最新バージョンのXenMobileへアップグレードします。

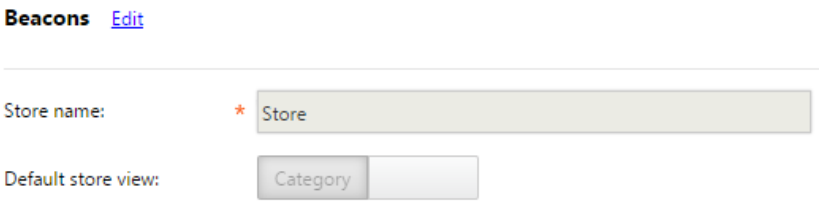
5. 「アップグレードツールのアップグレード後要件」の説明に従って、デバイスを接続するようにNetScalerを変更します。

https://support.citrix.com/article/CTX218552からXenMobile 9.0 App Controller Rolling Patch 9をダウンロードします。

App Controller管理コンソールで、**[設定] > [リリース管理]**の順にクリックします。**[アップデート]**をクリックして、ダウンロードしたパッチファイルを選択します。**[アップロード]**をクリックしてApp Controllerを再起動します。

登録済みのWindowsデバイスがアップグレード後も動作するように、XenMobile 9を最新バージョンのXenMobileにアップグレードする前にカスタムストア名をデフォルト値に戻す必要があります。詳しくは、http://support.citrix.com/article/CTX214553を参照してください。

MAMモードまたはEnterpriseモードのアップグレードで、App Controllerでストア名がデフォルトの「Store」から変更されている場合は、アップグレードのサポートバンドルを生成する前に、ストア名をデフォルト設定の「**Store**」に戻します。



Citrixライセンスサーバーなど関連コンポーネントの必要なバージョンは、「システム要件」やそのサブ記事を参照してください。

- **NetScaler**： NetScalerをアップグレードする前に、NetScaler構成ファイル（ns.conf）のコピーを必ず保存してください。Netscalerの現在のリリースには、使いやすいクイック展開ユーティリティと、NetScalerとXenMobileを統合する手順が順を追って表示されるNetScaler for XenMobileウィザードが含まれています。詳しくは、「XenMobile環境の設定の構成」およびFAQ: XenMobile 10 and NetScaler 10.5 Integrationを参照してください。
- **ファイアウォールポート**： 新しいXenMobileサーバーのIPに対して開放するファイアウォールのポートはXenMobile 9.0サーバーのIPに対して開放するポートと同様です。XenMobileの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。
- **LDAPサーバー**： 新しいXenMobileサーバーが1つまたは複数のLDAPサーバーに接続していることを確認します。サーバーを再起動するとき、アップグレード後のLDAPサーバーへの有効なルートがある必要があります。

次の表は、実行できるデータベースの移行オプションを示しています。システム要件については、「XenMobileのデータベース要件」を参照してください。

XenMobile 9.0から		最新バージョンのXenMobileへ
Enterprise Edition		
App Controller	**MDM**	
ローカルのPostgreSQL	ローカルのPostgreSQL	ローカルのPostgreSQL
ローカルのPostgreSQL	MS SQL	MS SQL
ローカルのPostgreSQL	リモートのPostgreSQL	リモートのPostgreSQL
App Edition		
ローカルのPostgreSQL		ローカルのPostgreSQL
ローカルのPostgreSQL		リモートのPostgreSQL
ローカルのPostgreSQL		MS SQL

MDM Edition	
ローカルのPostgreSQL	ローカルのPostgreSQL
MS SQL	MS SQL
リモートのPostgreSQL	リモートのPostgreSQL

XenMobileは、データベースの移行プロセスにおいて、XenMobile 9.0 Device Managerで実装されたデータベースソリューションにアクセスできる必要があります。たとえば、次のポートを開く必要があります。

- Microsoft SQL Serverの場合、デフォルトポートは1433です。
- PostgreSQLの場合、デフォルトポートは5432です。

PostgreSQLへのリモート接続を許可するには、次の手順を実行する必要があります。

1. ファイルpg_hba.confを開き、次の行を検索します。

```
host all all 127.0.0.1/32 md5
```

2. すべてのIPアドレスを許可するには、この行を次のように変更します。

```
host all all 0.0.0.0/0 md5
```

または、XenMobileサーバーのIPアドレスへの接続を許可する別のホストエントリを追加します。

```
host all all 10.x.x.x/32 md5
```

3. ファイルを保存します。

4. サービスを停止してから開始します。

5. postgresql.confファイルを開き、次の行を検索します。

```
#listen_addresses = 'localhost'
```

6. 行を次のように変更します。

```
listen_addresses = '*'
```

7. PostgreSQLサービスを停止して起動し、変更を適用します。

カスタムポートがデータベースソリューションに割り当てられている場合、XenMobile 9.0 Device Managerのファイアウォール保護でそのポートが許可されて開いている必要があります。こうすることで、XenMobileの新しいインスタンスがデータベースに接続し、必要な情報を移行できるようになります。

特殊文字（!、$、()、#、%、+、*、~、?、|、{}、および[]）を含むXenMobile 9.0の展開パッケージ名はアップグレードされ

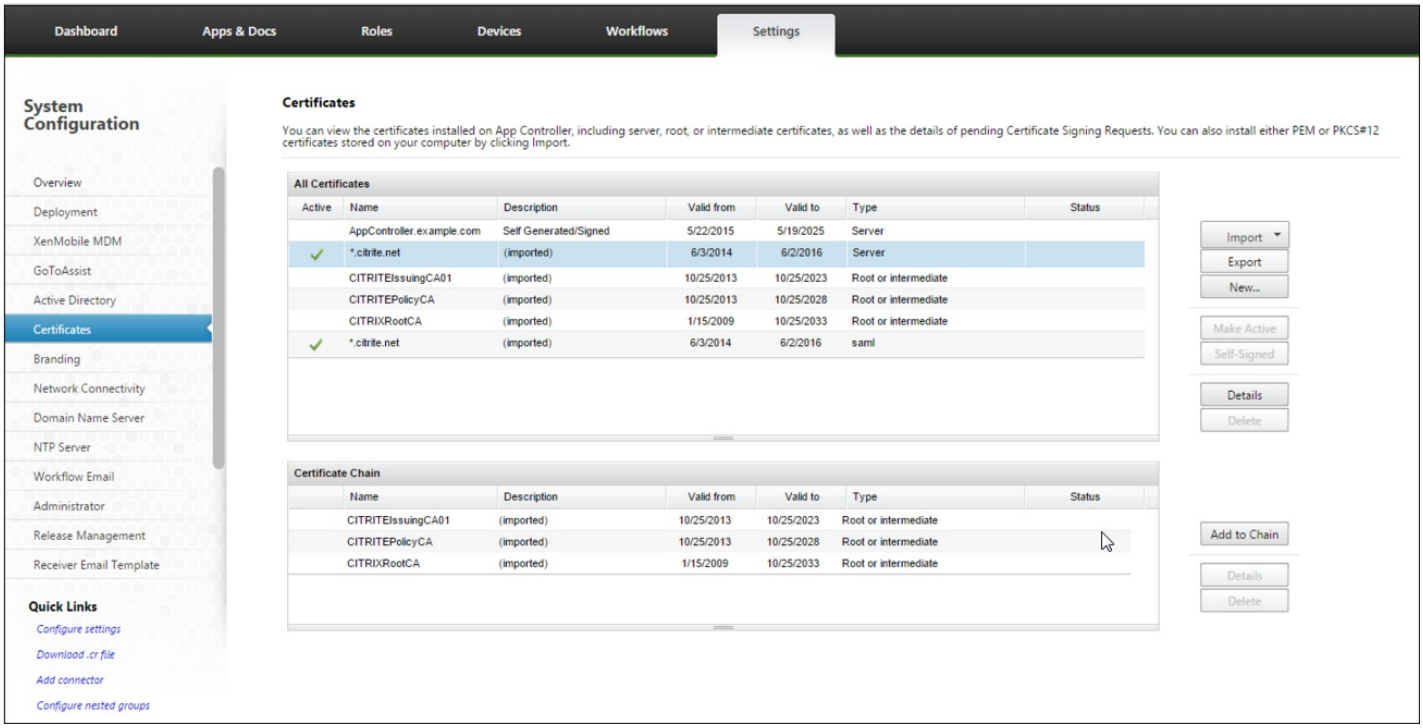
ますが、アップグレード後にXenMobileの新しいインスタンスのデリバリーグループを編集することはできません。さらに、XenMobile 9.0で作成されたローカルユーザーおよびローカルグループに開き角かっこ（[）が含まれていると、XenMobileの新しいインスタンスによる登録招待状の作成で問題が発生します。アップグレード前に、展開パッケージ名からすべての特殊文字を削除して、ローカルユーザーおよびローカルグループの名前から開き角かっこを削除します。

外部SSL証明書が、Citrixのサポート記事「How to Configure an External SSL Certificate」で示される条件を満たす必要があります。アップグレードを開始する前にpki.xmlを確認して、SSL証明書がこれらの条件を満たしていることを確認します。

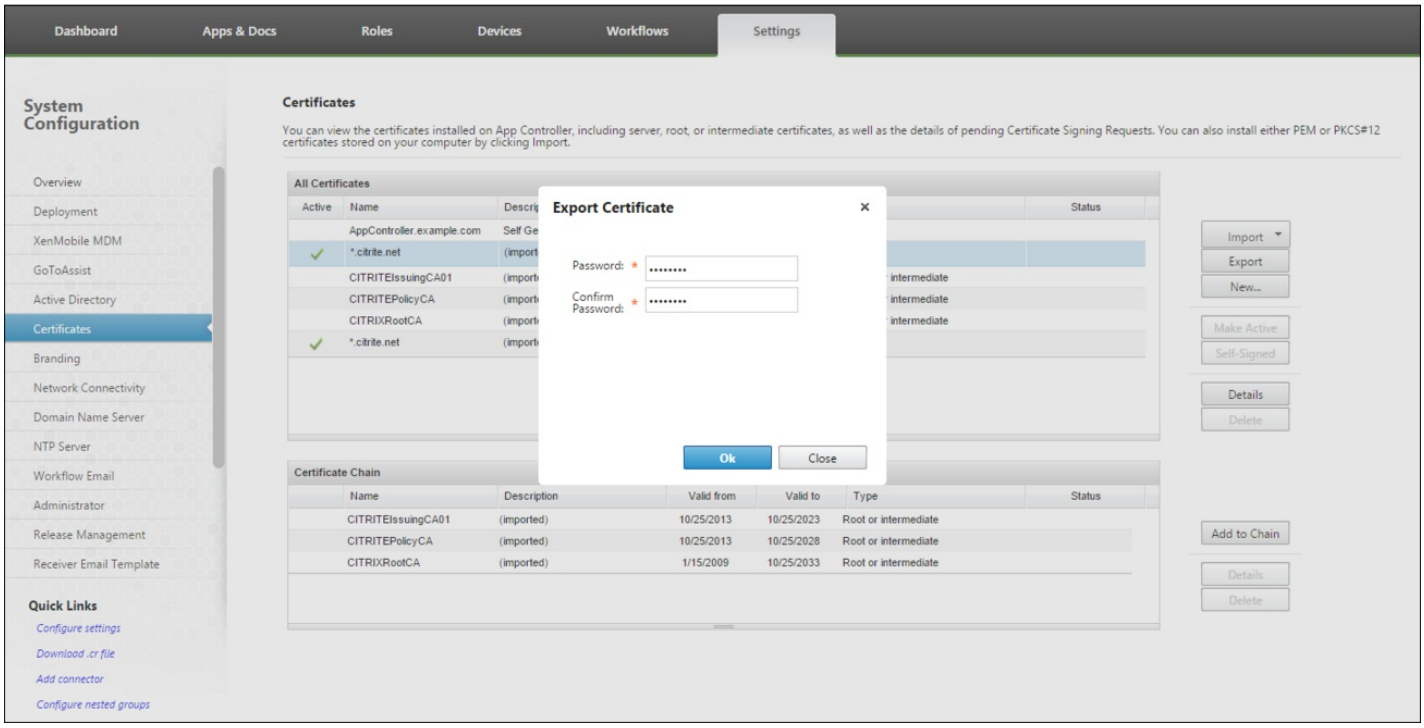
XenMobile 9.0 Enterprise Editionの展開をアップグレードする場合は、App Controllerのサーバー証明書をエクスポートする必要があります。後で、アップグレード後要件を処理するときに、サーバー証明書をNetScaler Gatewayにインポートする必要があります。以下の手順に従ってサーバー証明書をエクスポートします。

1. XenMobile 9.0 App Controllerにログオンして **[Certificates]** をクリックします。

2. 証明書一覧でエクスポートするサーバー証明書をクリックし、**[エクスポート]** をクリックします。



3. **[証明書のエクスポート]** ダイアログボックスの両方のフィールドに証明書のパスワードを入力して **[OK]** をクリックします。



FTP（File Transfer Protocol：ファイル転送プロトコル）またはSCP（Secure Copy Protocol：セキュアコピープロトコル）を使用して、XenMobileコマンドラインインターフェイスから暗号化されたサポートバンドルをアップロードすることができるサーバーを用意します。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

アップグレードツールのアップグレード後要件

Feb 27, 2017

アップグレードツールの実行後、次に行うべき一般的な手順が一覧表示されます。ご使用の環境のアップグレード後要件のタスクは、インストールされているNetScalerのバージョン、NetScaler for XenMobileウィザードを使用してNetScalerを構成したかどうか、およびXenMobileのエディションに基づいて異なる可能性があります。

以下のアップグレード後要件のタスクの一覧を確認し、ご使用の環境に該当するタスクをすべて実行するように注意してください。

1. XenMobileでライセンスを構成して、ユーザーの接続を有効にします詳しくは、手順を参照してください。

2. XenMobile 9.0を実行しているサーバーをDMZに展開していた場合は、XenMobileの外部DNSを、新しいXenMobileサーバーインスタンスを指すように変更します。

3. 負荷分散NetScalerアプライアンスを活用してXenMobile 9.0を実行しているサーバーを展開した場合は、NetScalerを以下のように変更します。

   a. 新しい負荷分散仮想サーバーをアップグレード用に構成します。詳しくは、手順を参照してください。

   b. App ControllerサーバーのFQDNがアップグレード用の新しいロードバランサーをポイントするようにアドレスレコードを構成します。詳しくは、手順を参照してください。

   c. 新しいXenMobile 10.1サーバーのIPアドレスを参照するように、Device Manager負荷分散仮想サーバーを変更します。詳しくは、手順を参照してください。

   d. 新しいXenMobileサーバーのFQDNを参照するようにNetScaler Gatewayを変更します。詳しくは、手順を参照してください。

   e. 次のタスクは以下の場合にのみ必要です。

      - NetScaler for XenMobileウィザード9を、NetScaler 11.1、11.0または10.5とともに使用する場合、または

      - NetScaler Gateway 10.1を使用している場合（非推奨）、または

      - NetScaler for XenMobileウィザードを使用しないでNetScaler for XenMobile 10.5以降を構成した場合。

   上記の場合の手順については、XenMobile Upgrade Tool 10.1のドキュメントで以下のトピックを参照してください。

   SSLブリッジのMDM構成に基づいて、新しいMAM負荷分散仮想サーバーを作成する
   SSLオフロードのMDM構成に基づいて、新しいMAM負荷分散仮想サーバーを作成する

4. 最新バージョンのXenMobileをクラスターで展開する場合は、XenMobileコマンドラインインターフェイス（CLI）を使用してクラスターのサポートを有効にし、新しいXenMobileノードに接続する必要があります。XenMobile CLIのヘルプは、「［Clustering］メニューオプション」を参照してください。

5 環境の必要に応じて、残りのアップグレード後要件を完了します。

この記事では、Secure Ticket Authority、Network Time Protocol（NTP）サーバー、XenMobileサーバーホスト名、アップグレードしなかった更新情報、カスタムストア名、およびアップグレード後のXenMobileデバイス登録に関連した設定のアップグレード後要件についても説明します。

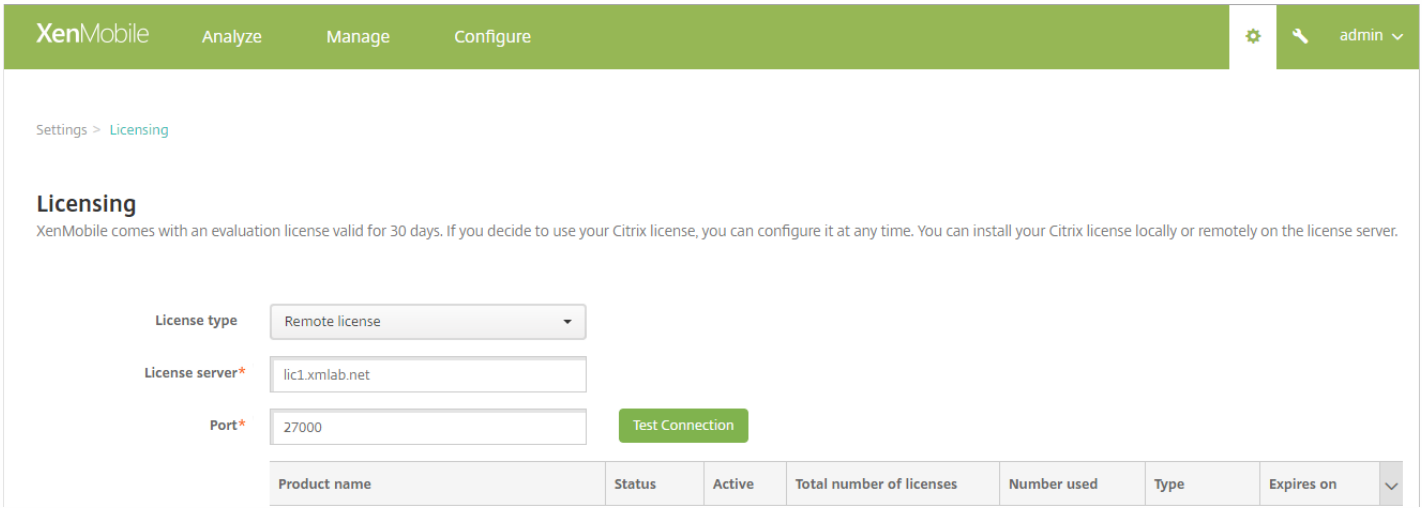
Citrix V6ライセンスは、最新バージョンのXenMobileでのみサポートされています。次のように、新しいXenMobileコンソールでローカルまたはリモートのライセンス構成を設定してユーザーの接続を有効にする必要があります。

1. 新しいライセンスファイルをダウンロードします。詳しくは、Citrix Licensingを参照してください。

2. 新しいXenMobileコンソールにログオンします。 https://:4443にアクセスします。

- MDMまたはENTのアップグレードの場合は、XenMobile 9.0 Device Managerの管理者資格情報を使用してログオンします。
- MAMアップグレードの場合は、XenMobile 9.0 App Controllerの管理者資格情報を使用してログオンします。

［Settings］>［Licensing］の順に移動します。



ローカルおよびリモートのライセンスの追加について詳しくは、「ライセンス管理」を参照してください。

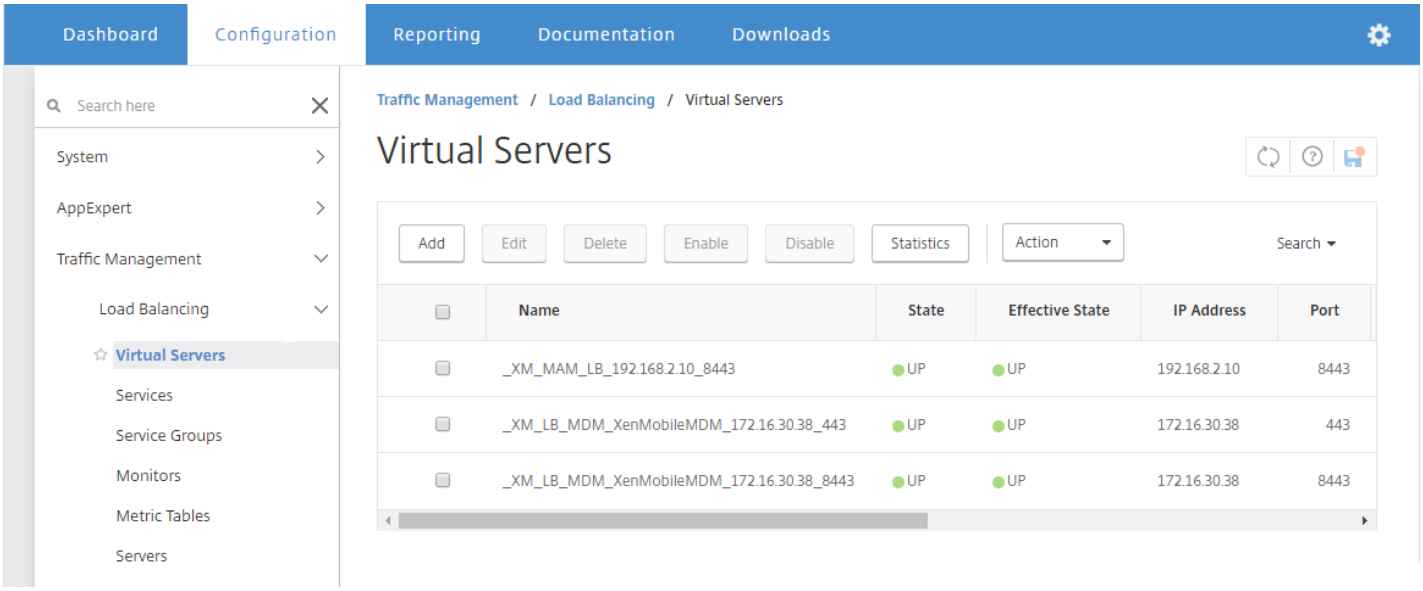
Important

このアップグレード後要件はXenMobile Enterprise Editionを実稼働環境でアップグレードする場合*にのみ*満たす必要があります。MAMまたはMDMのアップグレードでは不要です。

XenMobile Enterprise Editionを最新バージョンのXenMobileに実稼働環境でアップグレードした後では、XenMobile 9.0 App ControllerのFQDNに対して新しい負荷分散仮想サーバーを構成する必要があります。それには、NetScaler Gateway構成ツールを使用します。

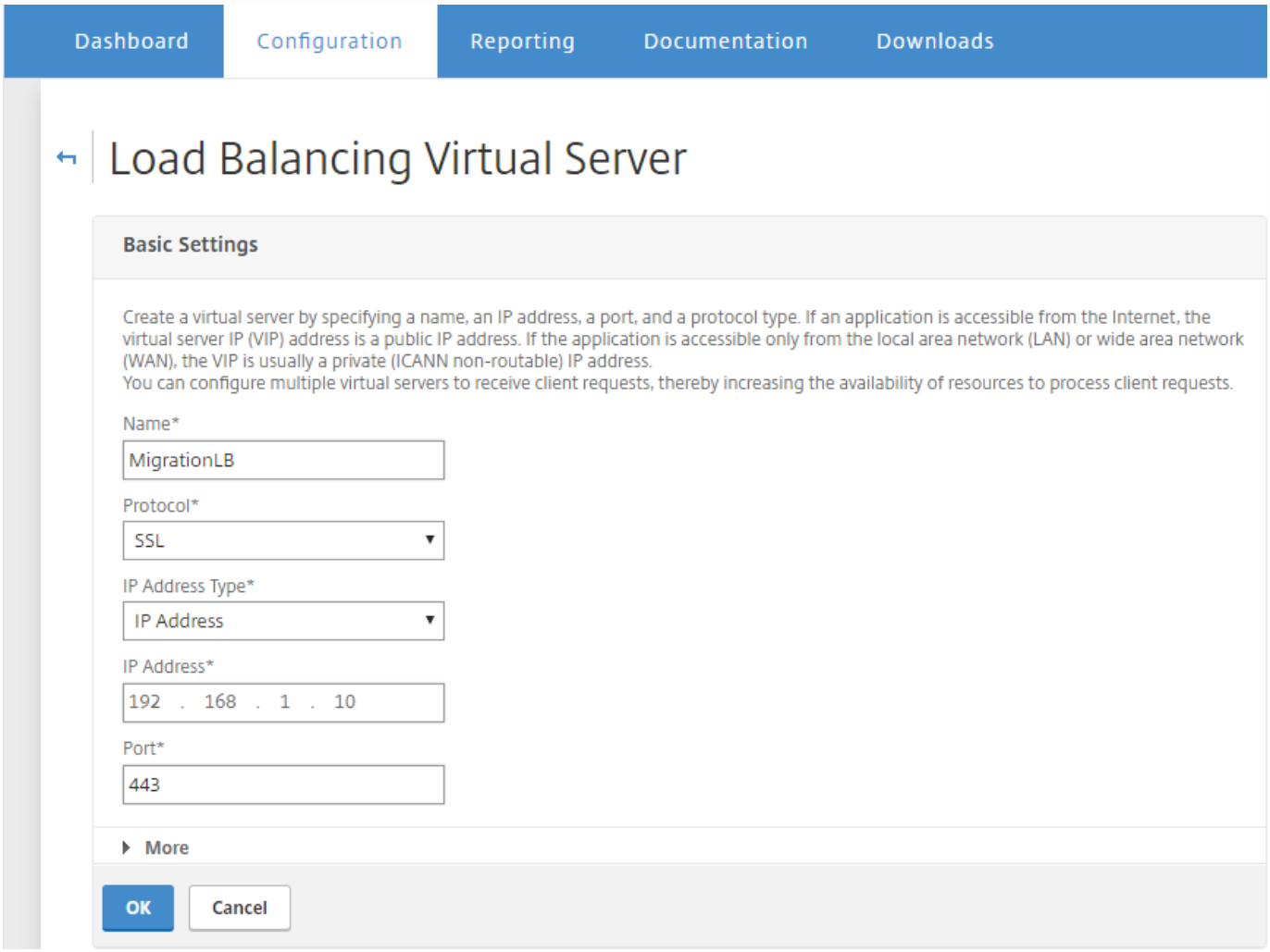
このセクションの画面例はNetScaler Gateway 11.1のものですが、NetScaler Gateway Version 11.0および10.5も同様です。

1. ［Traffic Management］>［Load Balancing］>［Virtual Servers］の順にクリックします。



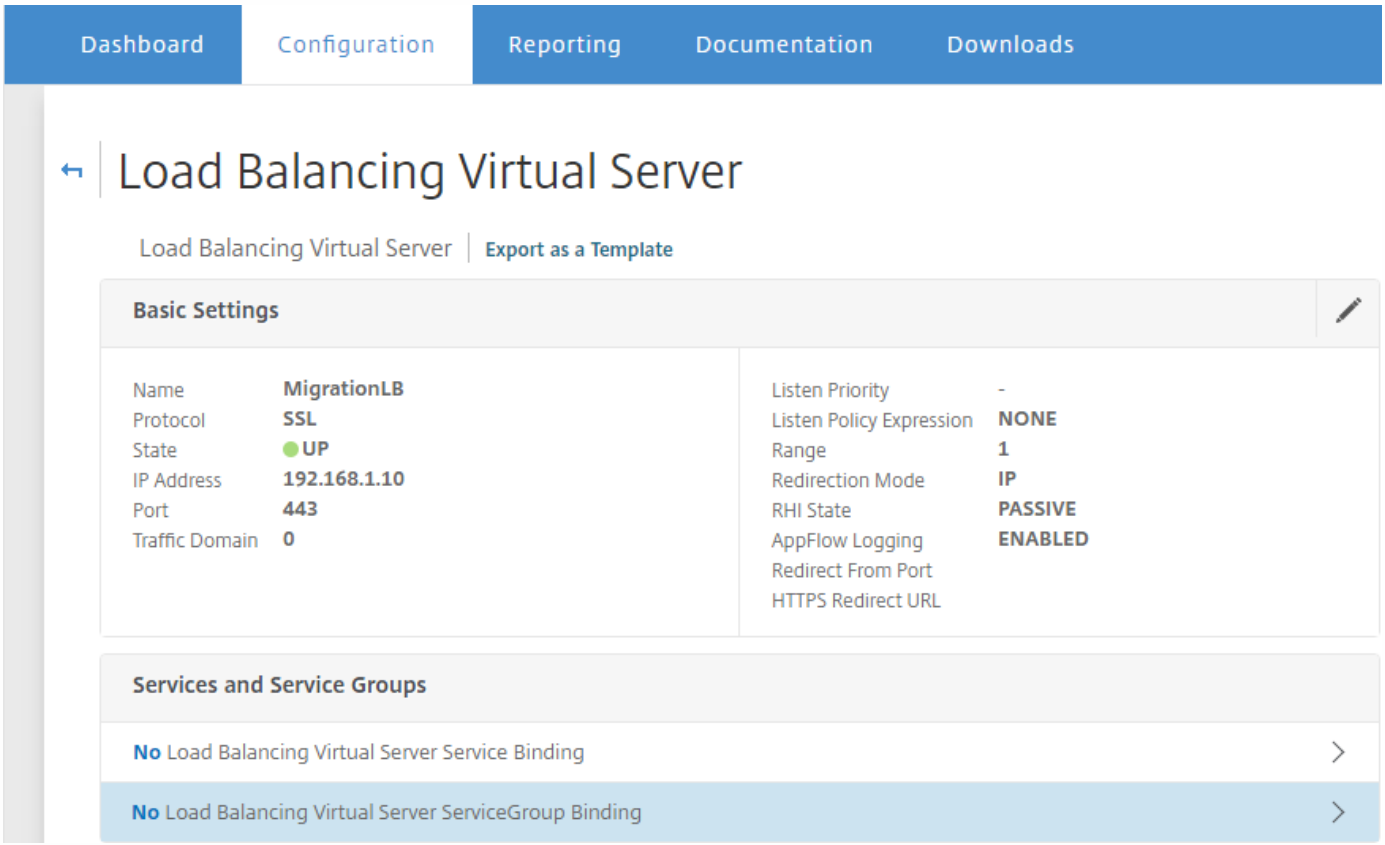
2. [Add] をクリックします。

3. [Load Balancing Virtual Server] ページで以下の設定を構成し、 [OK] をクリックします。

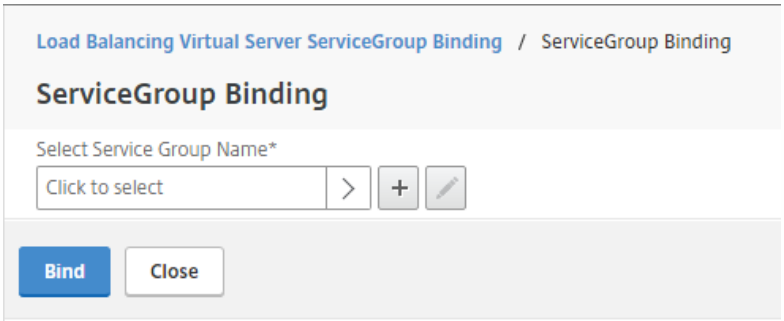


- Name：新しいロードバランサーの名前を入力します。
- Protocol： [SSL] に設定します。デフォルトは [HTTP] です。
- IP Address： 192.168.1.10などの、RFC 1918に準拠した新しいロードバランサーのIPアドレスを入力します。
- Port： [443] に設定します。

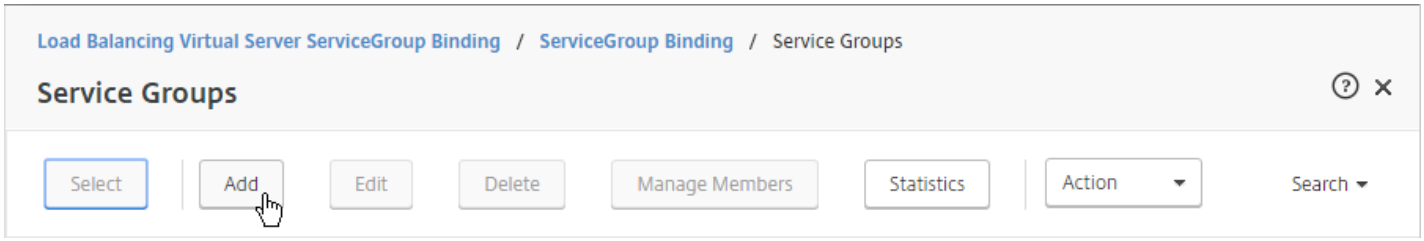
4. [Services and Service Groups] の下の [No Load Balancing Virtual Server Service Group Binding] をクリックします。



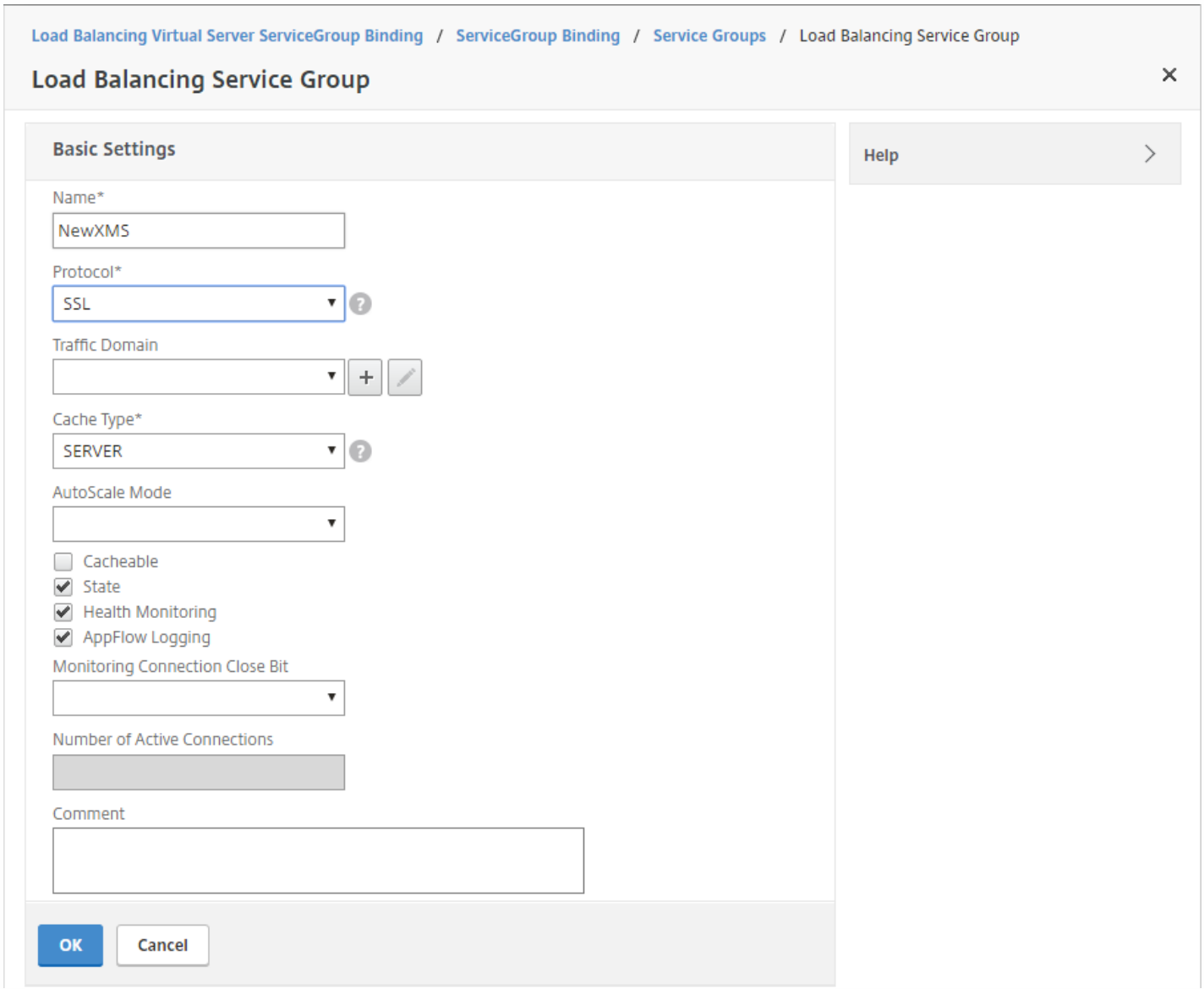
5. [Select Service Group Name] の下の [Click to Select] をクリックします。



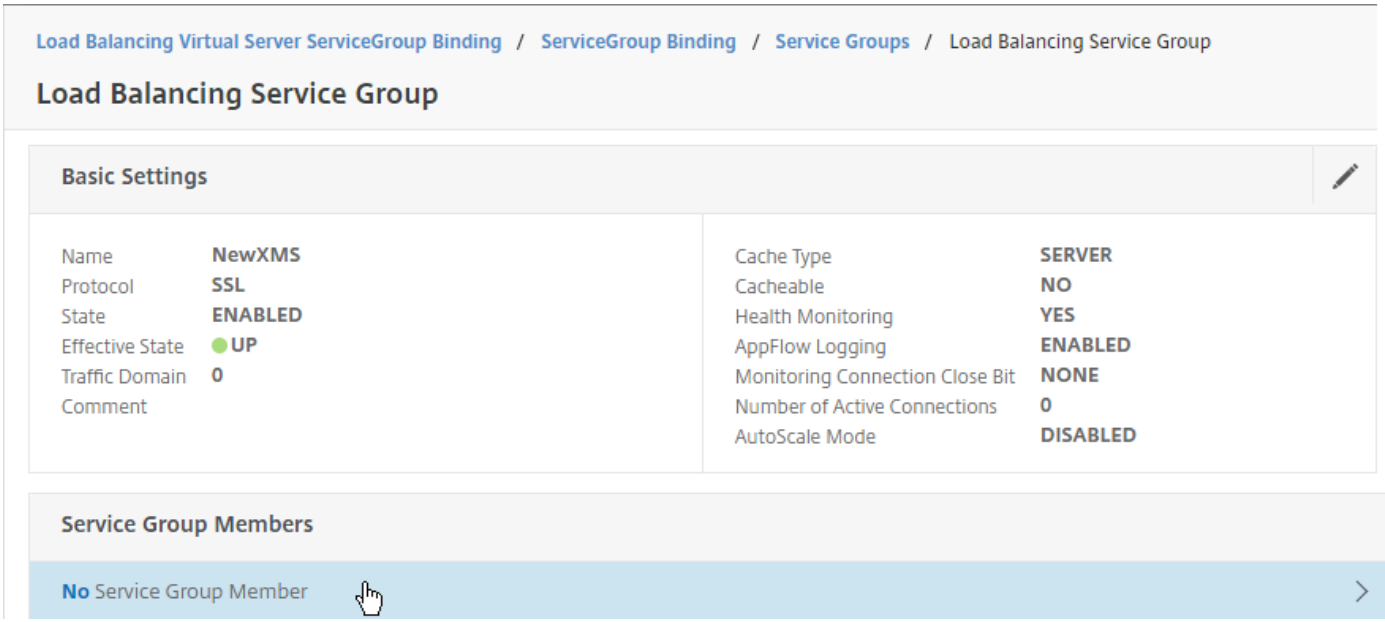
6. 新しいサービスグループを作成するには [Add] をクリックします。



7. [Load Balancing Service Group] ページで、新しいサービスグループの名前を入力して、プロトコルが[SSL] に設定されていることを確認してから [OK] をクリックします。

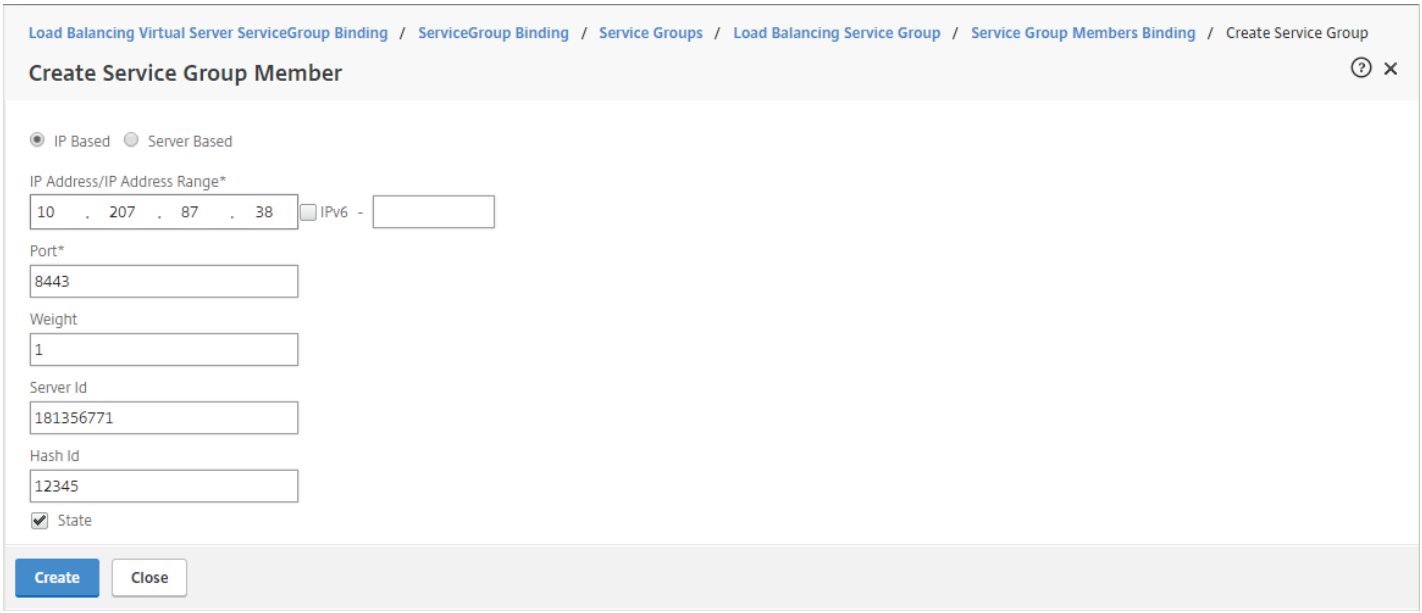


8. [No Service Group Member] をクリックします。

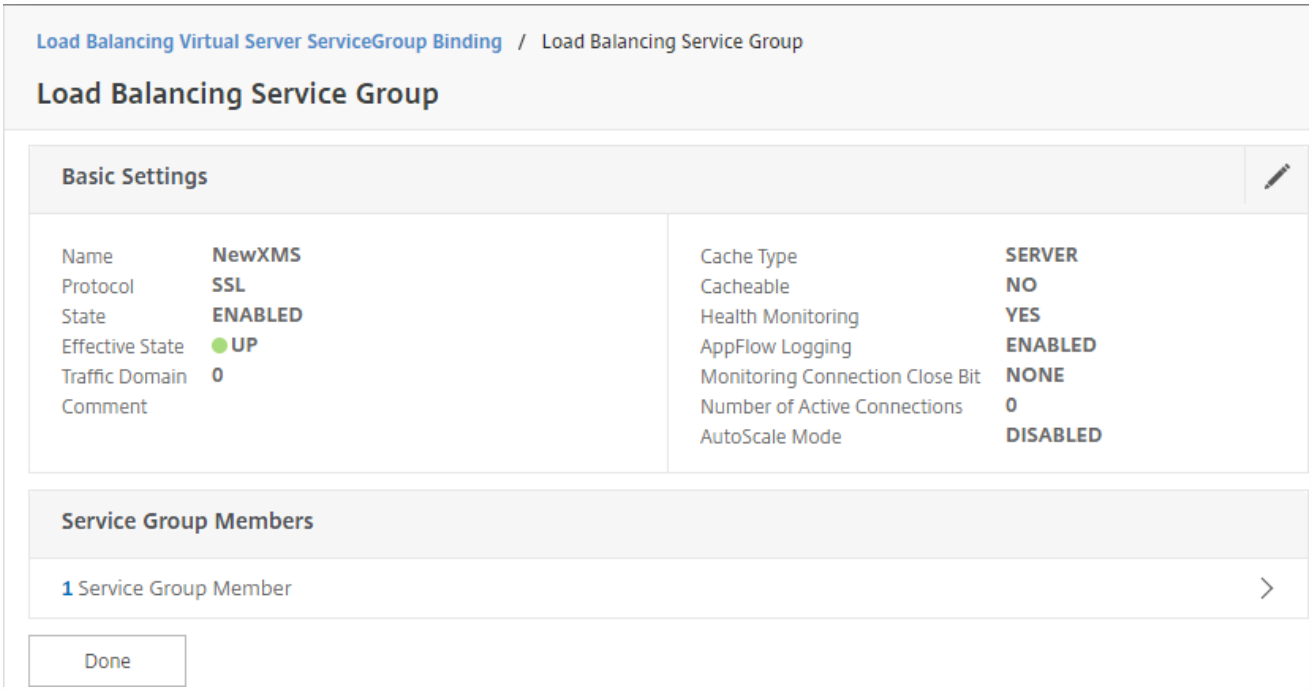


9. [Create Service Group Member] ページで以下の設定を構成します。

- IP Address/IP Address Range： 新しいXenMobileサーバーインスタンスのIPアドレスを入力します。
- Port： [8443] に設定します。
- Server ID： XenMobile 9.0のクラスター化環境から新しいXenMobileのクラスター化環境に移行する場合は、現在のXenMobileサーバーのサーバーノードIDを入力します。サーバーノードIDを確認するには、XenMobileサーバーのコマンドラインインターフェイス（CLI）にログオンして「1」と入力し、 [Clustering] メニューを開きます。CLIでは、サーバーノードIDは「Current Node ID」と表示されます。



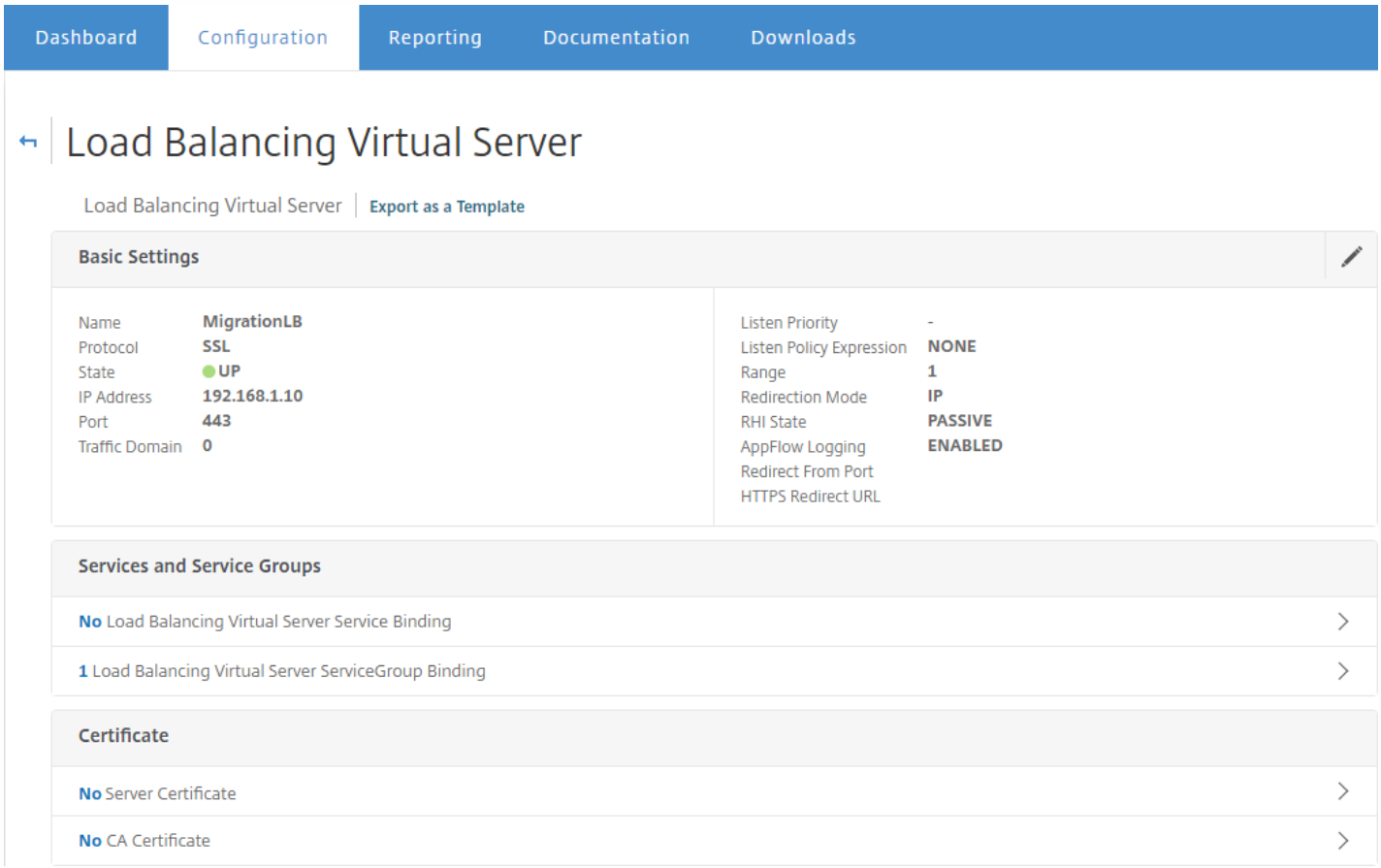
10. [Create] をクリックして [Done] をクリックします。



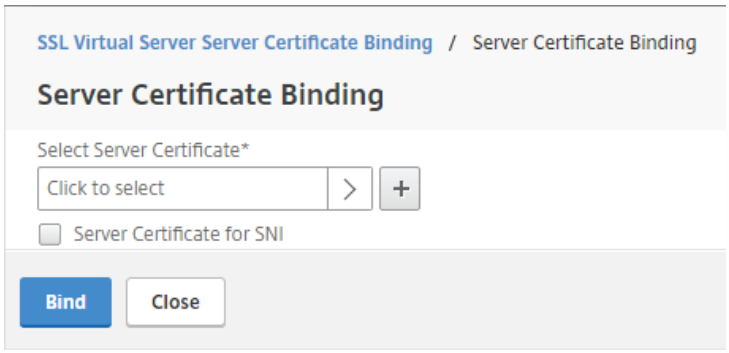
11. [Done] をクリックして、 [OK] をクリックします。

12. [Bind] をクリックして、次の画面で [Done] をクリックします。

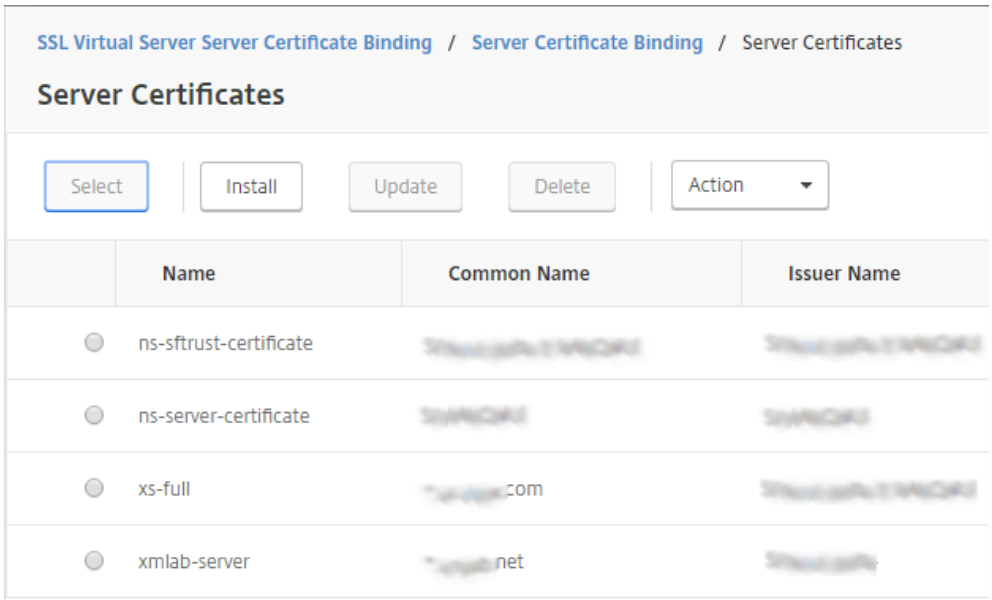
13. [Certificates] の下の [No Server Certificate] をクリックします。



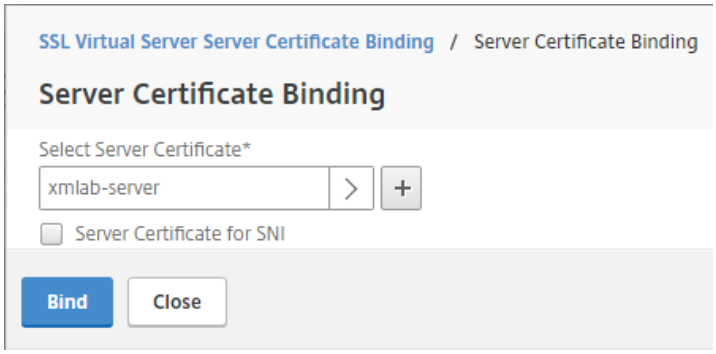
14. [Server Certificate Binding] の下の [Click to Select] をクリックします。

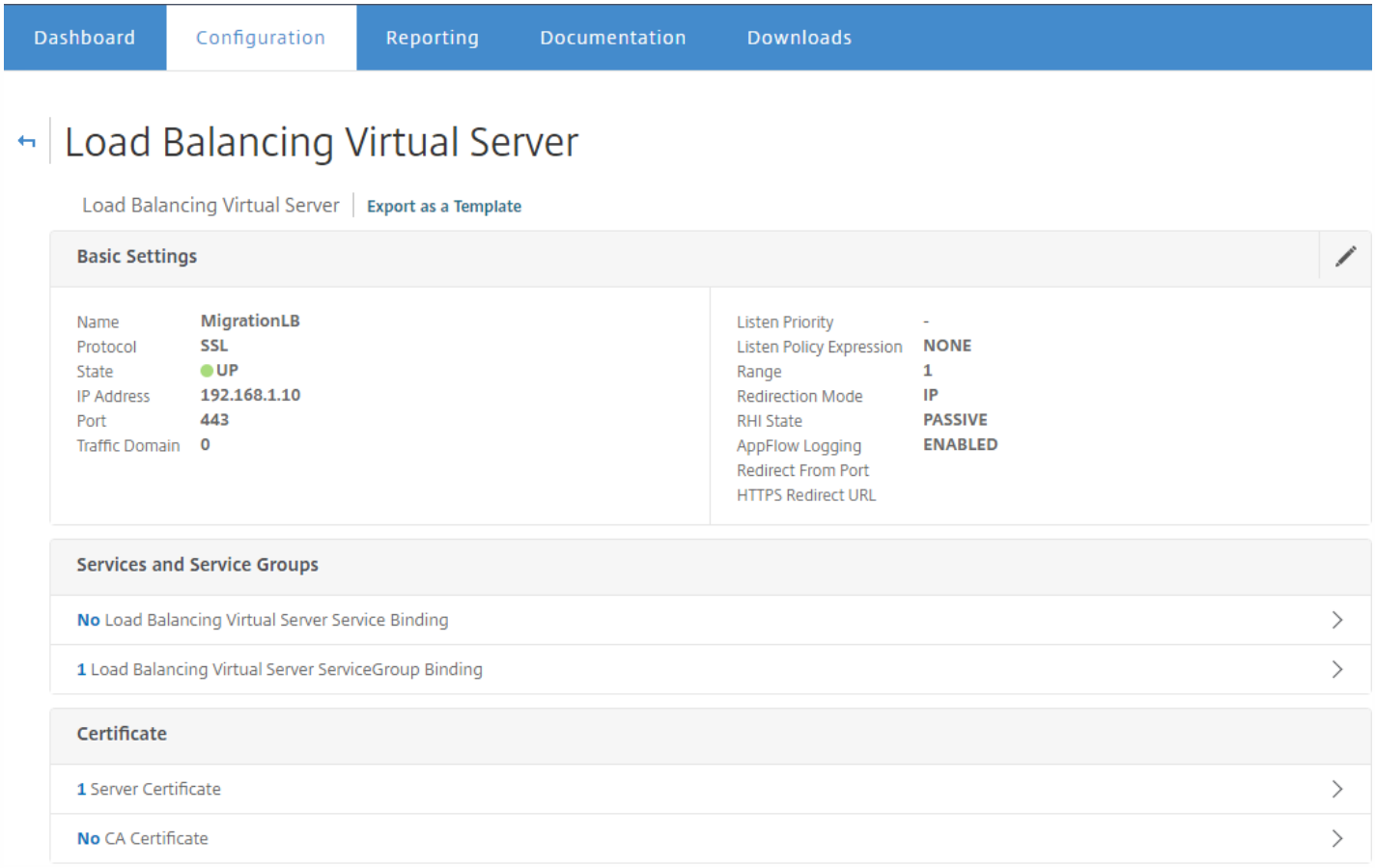


15. [Server Certificates] の下にある、「アップグレードツールの前提条件」でエクスポートしたXenMobile 9.0のサーバー証明書をクリックし、 [OK] をクリックします。

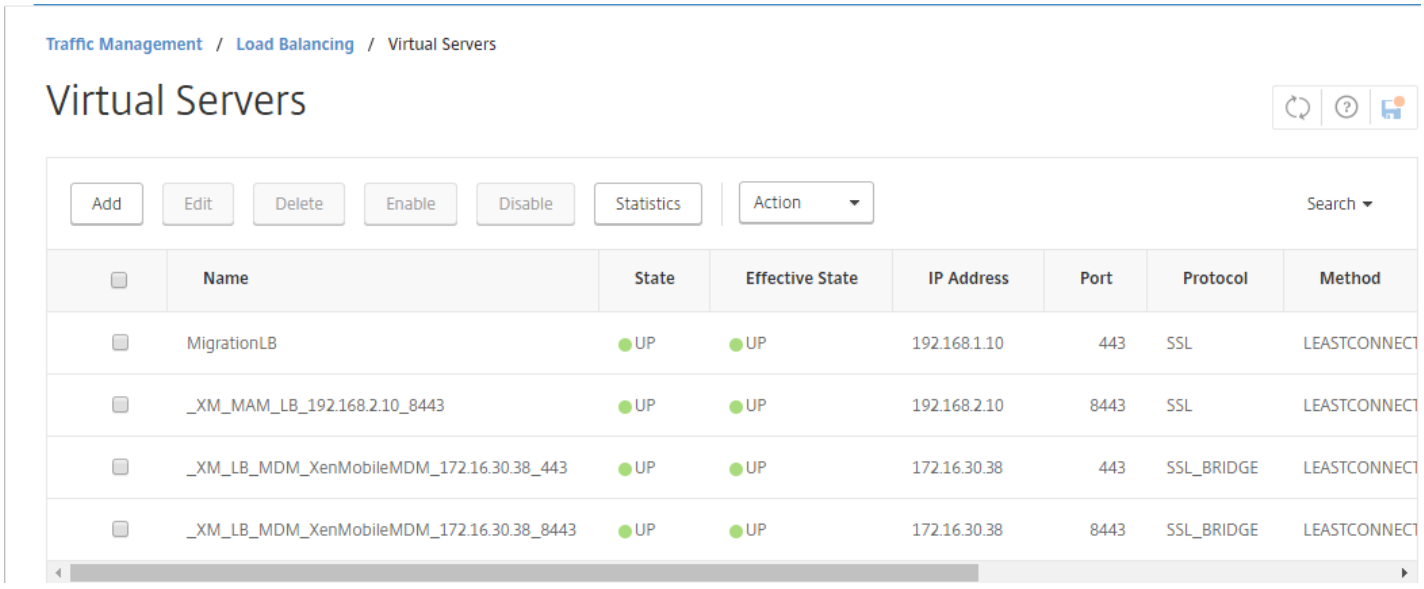


16. [Bind] をクリックして、次の画面で [Done] をクリックします。



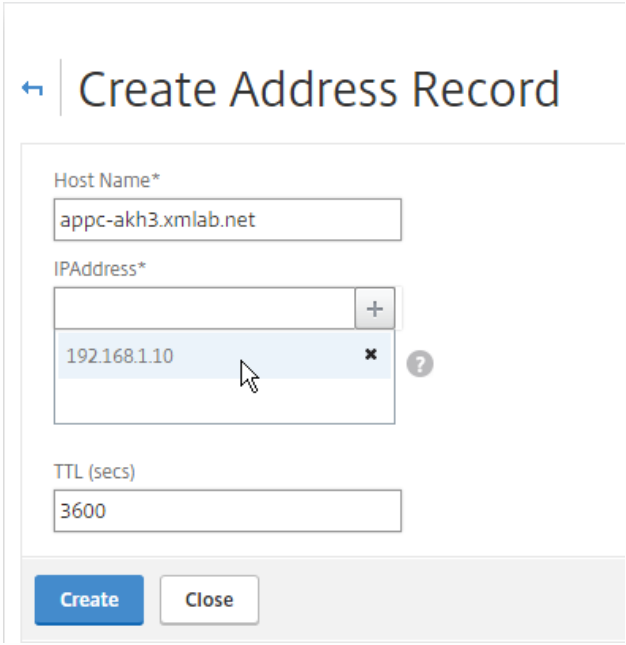


17. 更新ボタンをクリックしてサーバーが実行中であることを確認します。



1. NetScalerにログオンし、 [Traffic Management] > [DNS] > [Records] > [Address Records] の順にクリックし、 [Add] をクリックします。

> **注意**
>
> グローバルサーバーの負荷分散を構成している場合は、アドレスレコードを追加すると、グローバルサーバーの負荷分散システムがローカルIPアドレスを使用してサーバーに適切に応答するようになります。

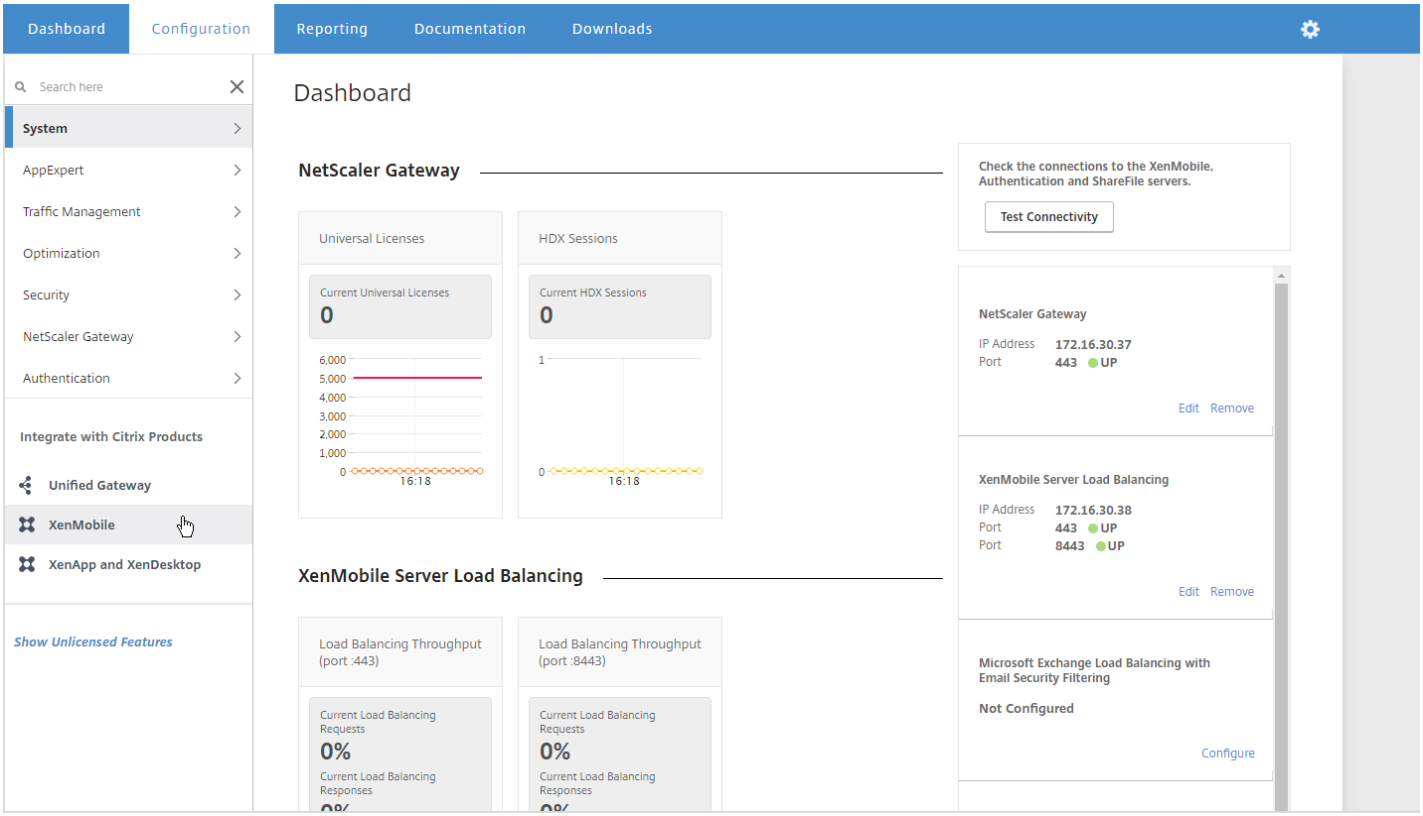


負荷分散NetScalerアプライアンスを活用してXenMobile 9.0を実行しているサーバーを展開した場合は、新しいXenMobileサーバーインスタンスの新しいIPアドレスで、NetScalerの負荷分散XenMobile 9.0 Device Managerインスタンスを構成する必要があります。

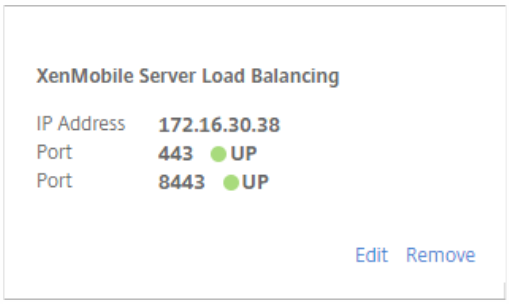
NetScaler 11.1を使用しているか、NetScaler 11.0または10.5を使用しているかに応じて、手順が異なります。

NetScaler 11.1の場合

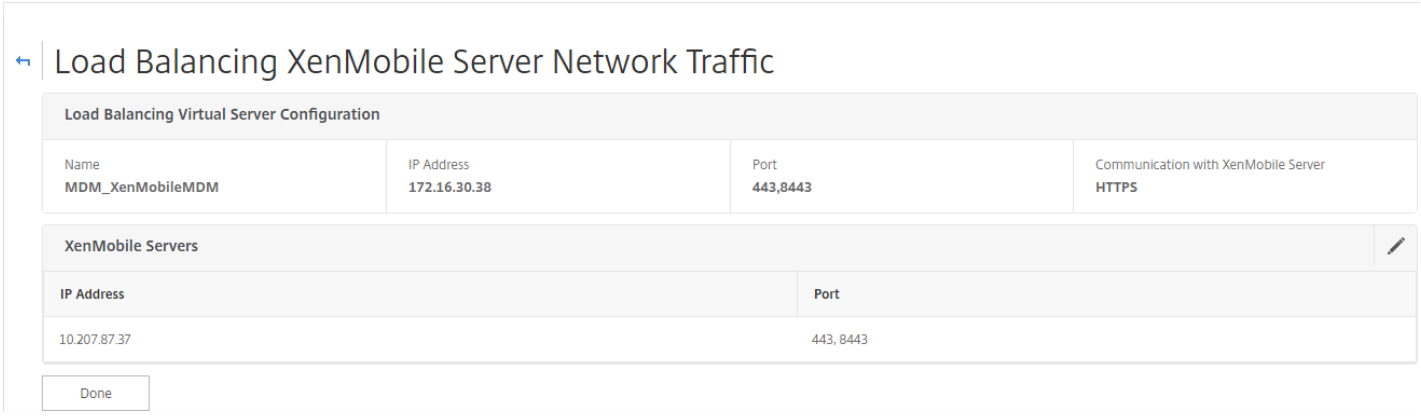
1. **[Integrate with Citrix Products]** の下の **[XenMobile]** をクリックします。



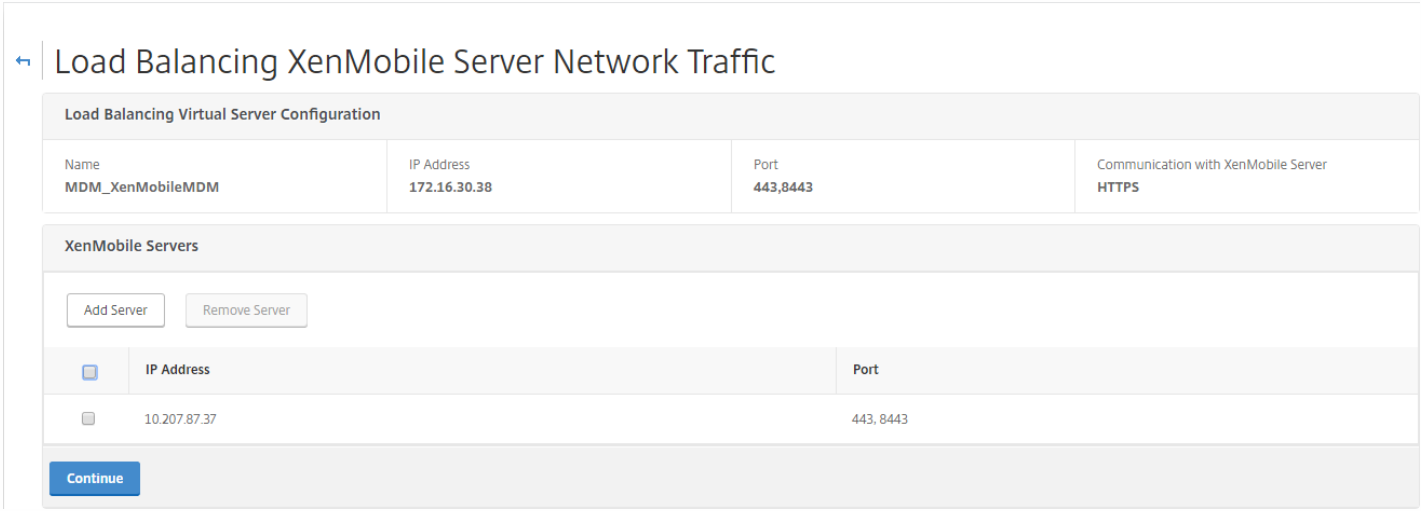
2. 画面右側の［XenMobile Server Load Balancing］の下の［Edit］をクリックします。



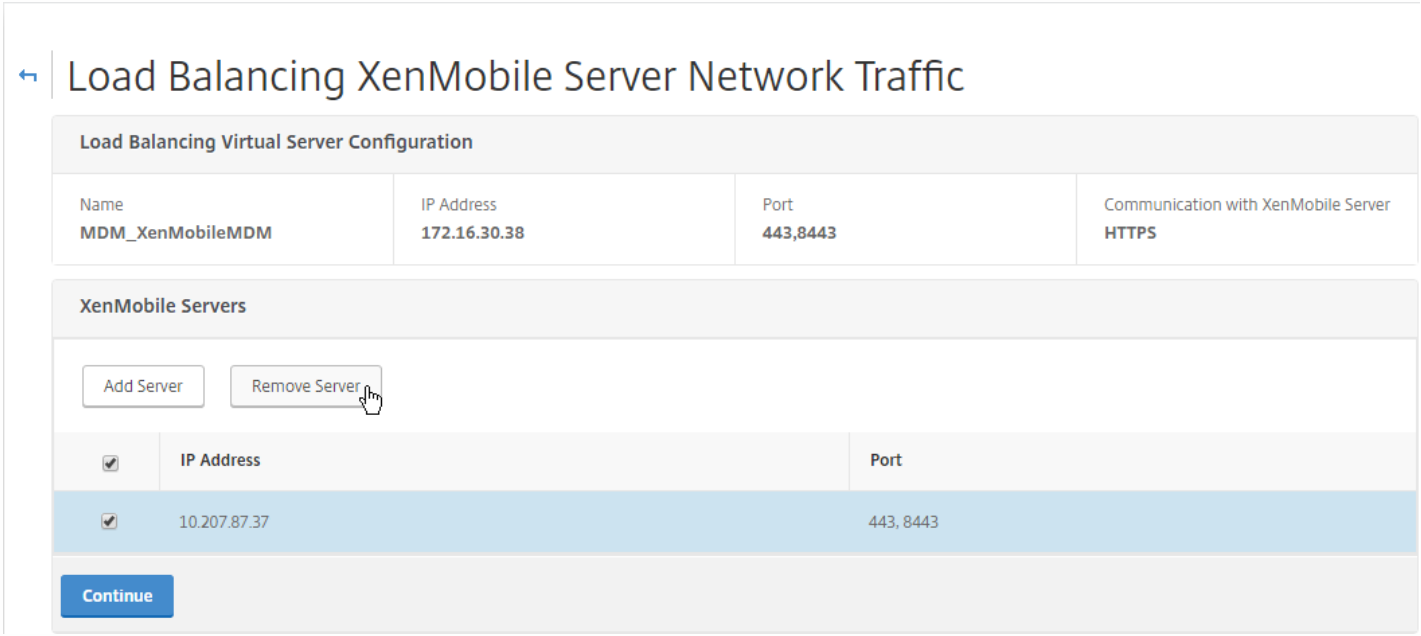
［Load Balancing XenMobile Server Network Traffic］ページが開きます。



3. XenMobile Serverのペンアイコンをクリックしてその設定を開きます。



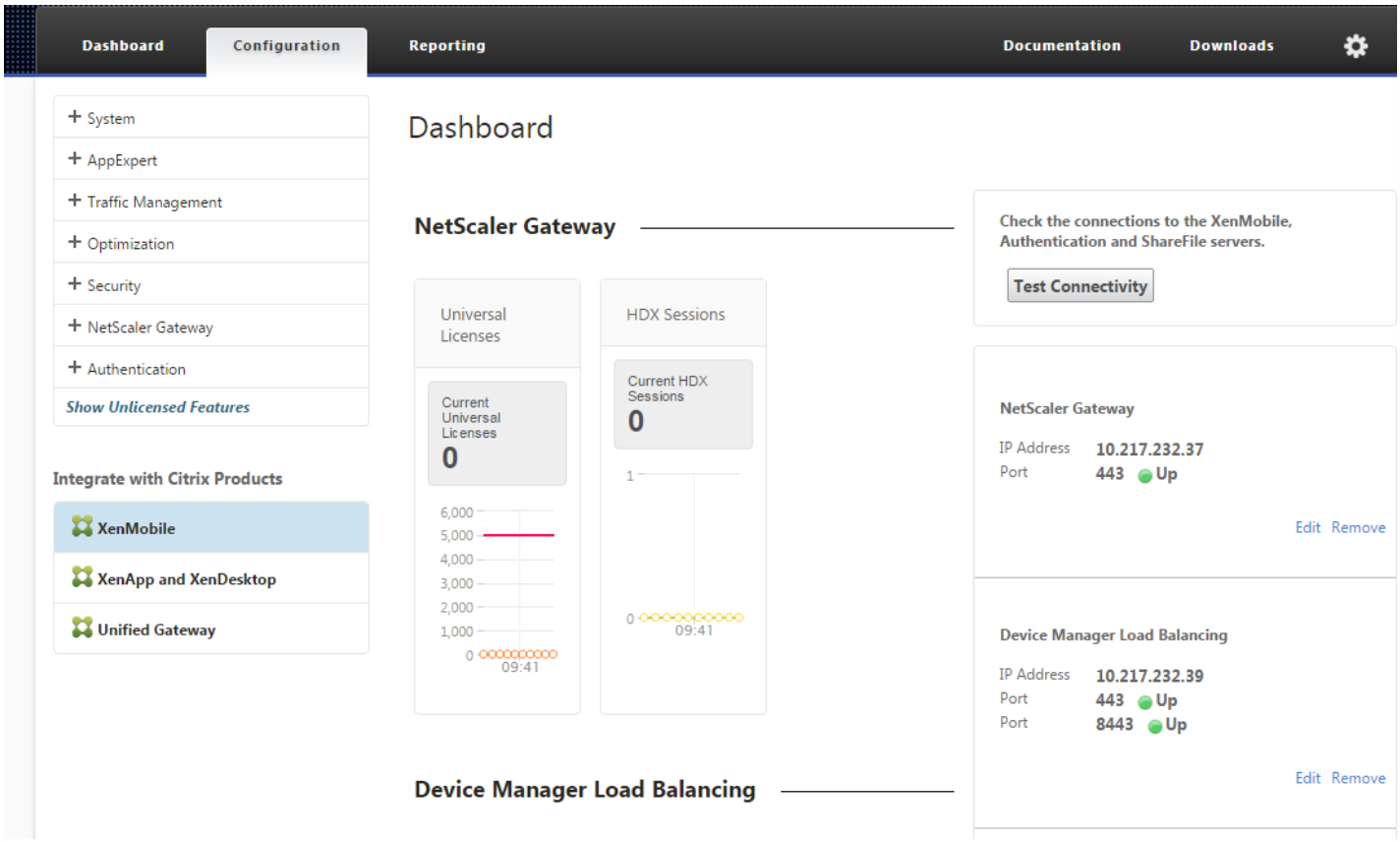
4. 9.0 Device ManagerのサーバーIPアドレスを選択して **[Remove Server]** をクリックします。



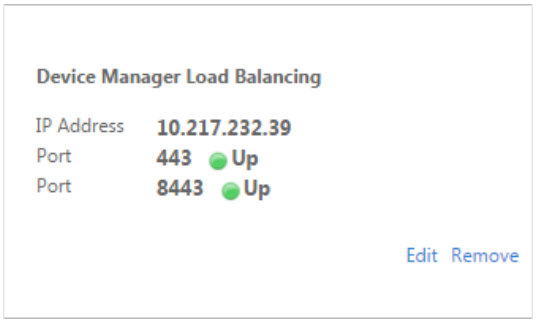
5. **[Add Server]** をクリックして新しいXenMobileサーバーのIPアドレスを追加します。

NetScaler のバージョン 11.0または10.5

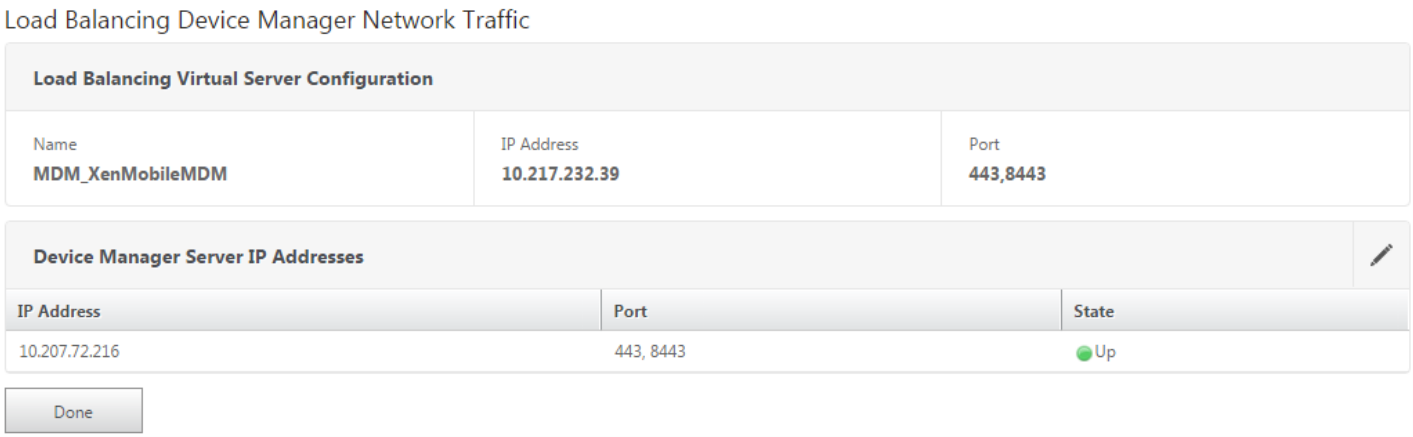
1. [Integrate with Citrix Products] の下の [XenMobile] をクリックします。



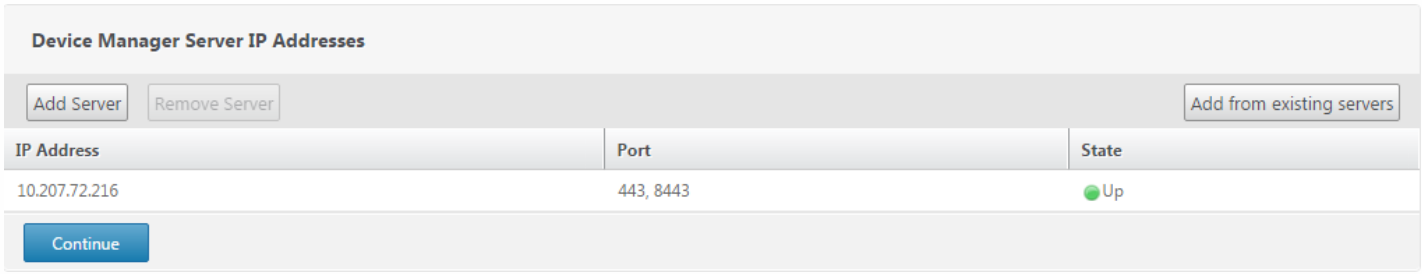
2. 画面右側の [Device Manager Load Balancing] の下の [Edit] をクリックします。



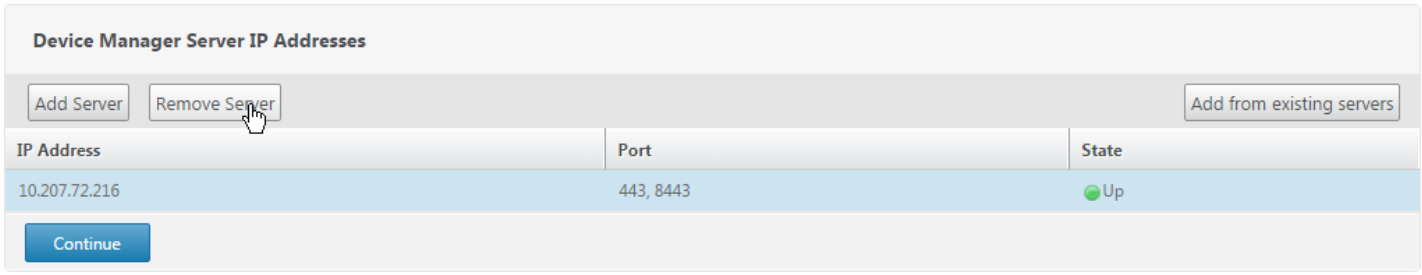
[Load Balancing Device Manager Network Traffic] ページが開きます。



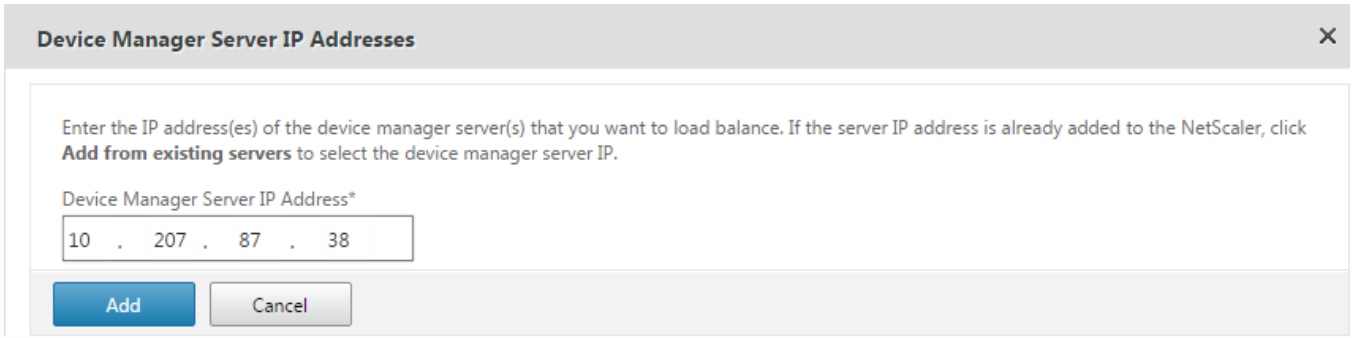
3. [Device Manager Server IP Addresses] のペンアイコンをクリックしてその設定を開きます。



4. 9.0 Device ManagerのサーバーIPアドレスを選択して [Remove Server] をクリックします。



5. [Add Server] をクリックして新しいXenMobileサーバーのIPアドレスを追加します。



この時点で、NetScaler GatewayはApp Controller FQDNをポイントしています。新しいXenMobileのFQDNをポイントするように、NetScalerを変更する必要があります。最新バージョンのXenMobileでは、ポート443ではなくポート8443をリスンします。NetScaler for XenMobileウィザード9を使用してNetScalerを設定する場合、次の表の例に示すように、FQDNにポート番号を含める必要があります。

XenMobile Enterprise Edition

新しいXenMobileのFQDNを参照するように、App ControllerのFQDNをXenMobile 9.0のDevice ManagerのFQDNにポート8443を続けたものに変更します。次の表は、一例です。

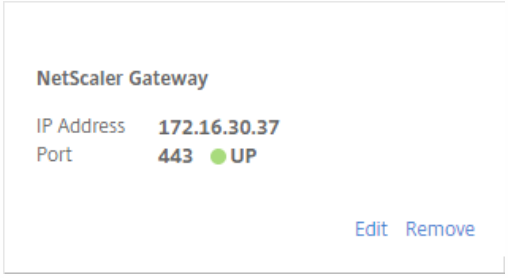
XenMobile 9.0のコンポーネント	コンポーネントのFQDN	新しいXenMobile Enterprise EditionのFQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	-
NetScaler Gateway	access.example.com	-

XenMobile App Edition

新しいXenMobileのFQDNを参照するように、App ControllerのFQDNをXenMobile 9.0のApp ControllerのFQDNにポート8443を続けたものに変更します。次の表は、一例です。

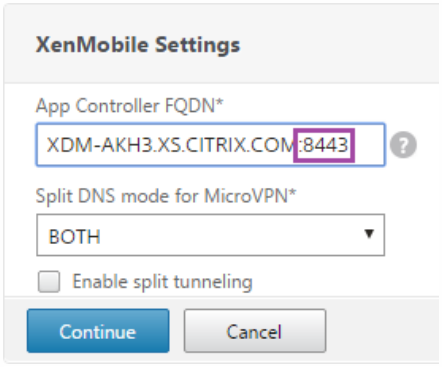
XenMobile 9.0のコンポーネント	コンポーネントのFQDN	新しいXenMobile Enterprise EditionのFQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	-

1. **[Integrate with Citrix Products]** の下の **[XenMobile]** をクリックします。
2. **[NetScaler Gateway]** の下の **[Edit]** をクリックします。



3. **[XenMobile Settings]** の隣にあるペンアイコンをクリックし、App ControllerのFQDNをXenMobileサーバーのFQDNに変

更して、FQDNに「:8443」を追加します。たとえば、「*SAMPLE-XENMOBILE.FQDN*.COM 8443」のようになります。

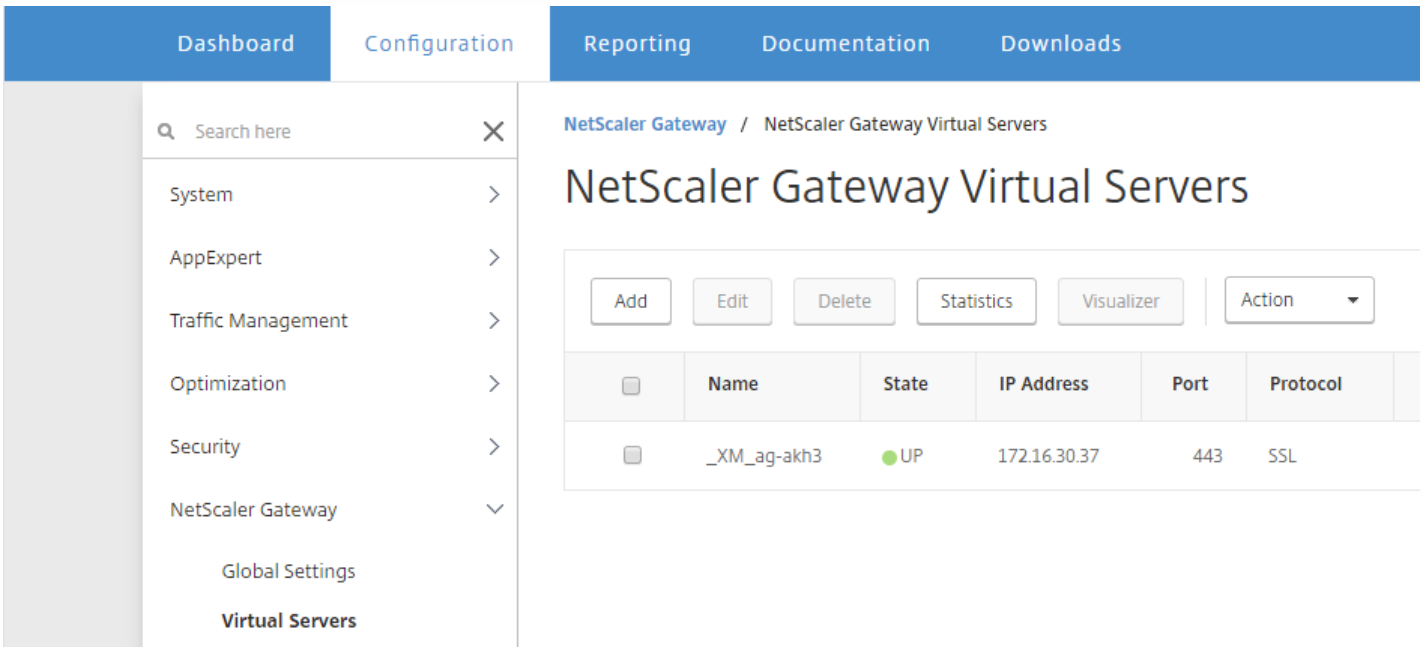


4. [Continue] 、 [Finish] の順にクリックします。

次に、DNSを更新して、Secure Ticket Authorityを実行しているサーバーのFQDNを、新しいXenMobileサーバーインスタンスのIPアドレスに解決する必要があります。アップグレード後要件の変更の後、Secure Ticket Authority ServerがNetScalerにバインドされていないのに [VPN Virtual Server STA Server Binding] の一覧に表示されることがあります。

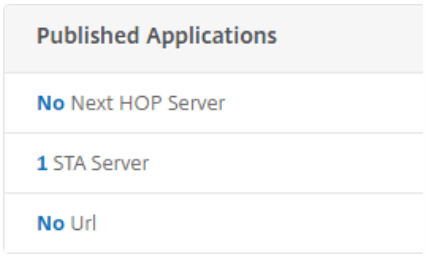
NetScaler Gatewayでは、次のように、Secure Ticket Authorityを実行しているサーバーのIPアドレスまたはFQDNを追加します。

1. [NetScaler Gateway] > [Virtual Servers] の順にクリックします。

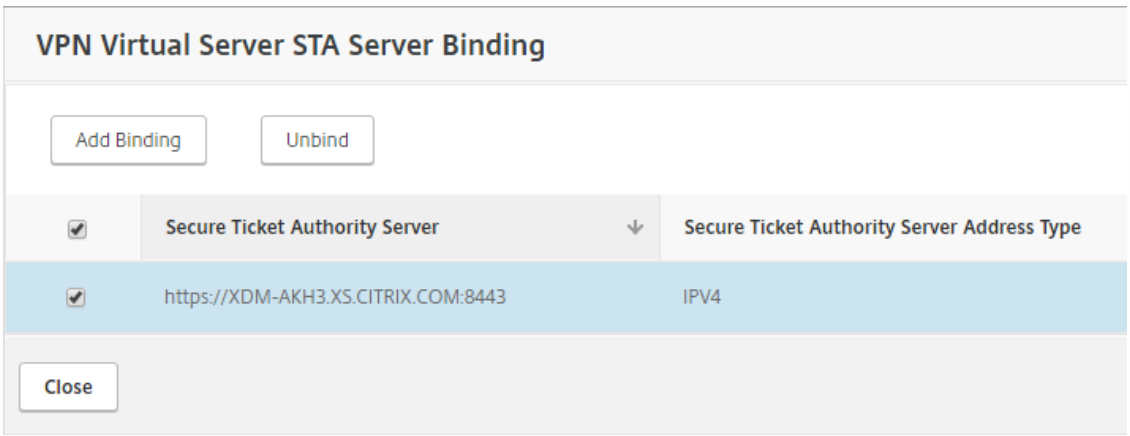


2. NetScaler Gateway仮想サーバーの設定が [Up] 状態であることを確認します。構成済みのNetScaler Gateway仮想サーバーを選択して [Edit] をクリックします。

3. [Published Applications] の下の [STA server] をクリックします。



4. 手順6で入力する、 **[Secure Ticket Authority Server]** のURLを記録します。一覧から［Secure Ticket Authority Server］を選択します。



5. **[Unbind]** をクリックして **[Add Binding]** をクリックします。

6. **[Secure Ticket Authority Server]** フィールドに手順4でメモしたURLを入力します。

7. **[Bind]** をクリックして **[Close]** をクリックし、 **[Done]** をクリックします。

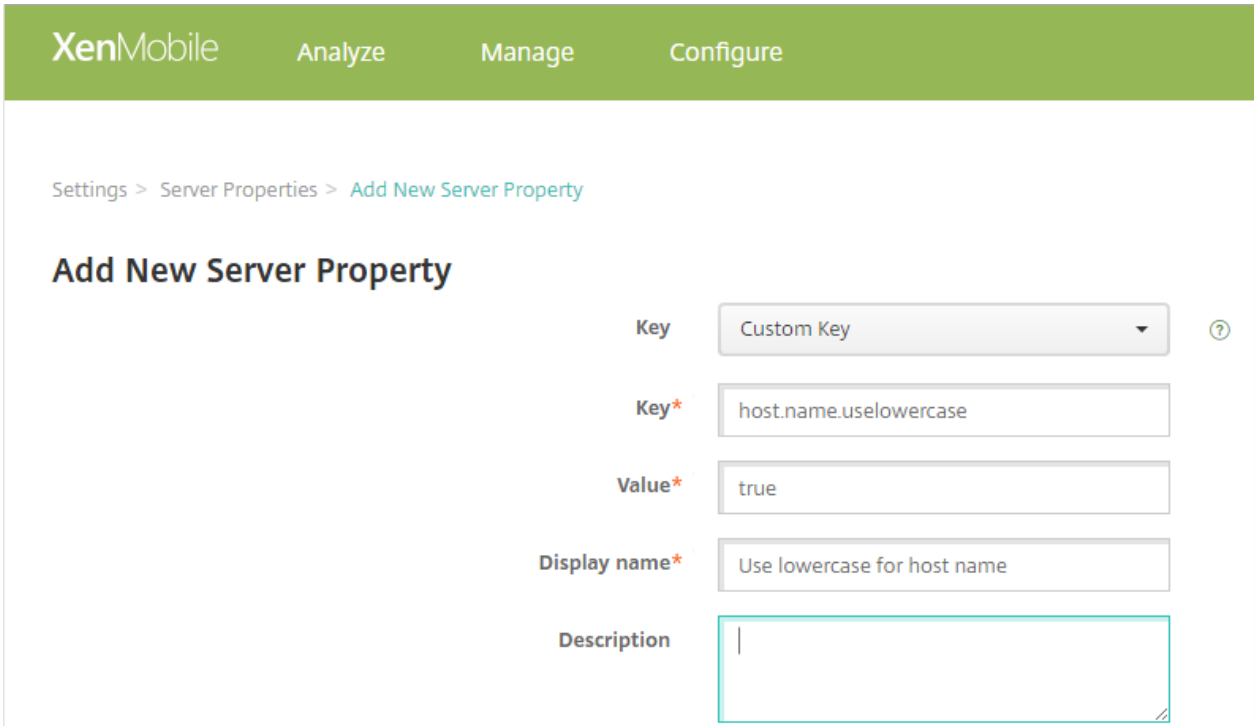
NetScalerの時刻とXenMobileサーバーの時刻が同期していることを確認します。可能であれば、NetScalerとXenMobileサーバーが同じパブリックNTP（Network Time Protocol：ネットワークタイムプロトコル）サーバーをポイントするようにします。

XenMobile 9.0ホスト名に大文字が含まれている場合、次の手順を実行して、モバイルデバイスがCitrix Storeにアクセスできるようにします。

1. 新しいXenMobileコンソールで、 **[設定] > [サーバープロパティ]** の順に選択します。

2. **[Add]** をクリックして、フィールドに次のように値を指定します。

- **Key**： **[Custom Key]** を選択します。
- **Key**：「**host.name.uselowercase**」と入力します。
- **Value**：「**true**」と入力します。
- **Display name**：キーの説明を入力します。



3. XenMobileサーバーを再起動します。

必要に応じて以下の情報を更新します。

- Managed Service Provider（MSP）グループ
- カスタムのActive Directoryの属性
- RBACの役割
  オンプレミスアップグレードの場合、RBAC設定に問題が生じます。詳しくは、 既知の問題」を参照してください。
- ログ設定
- migration.logファイル内に記述されている、構成またはユーザーデータ
- Syslogサーバーの構成

アップグレードする前、前提条件の手順の1つは、カスタムのCitrix Store名をそのデフォルト値に戻すよう変更することでした。その前提条件を実行しなかった場合は、次のいずれかのアップグレード後要件の手順に従ってから、最新バージョンのXenMobileサーバーを使用することができます。

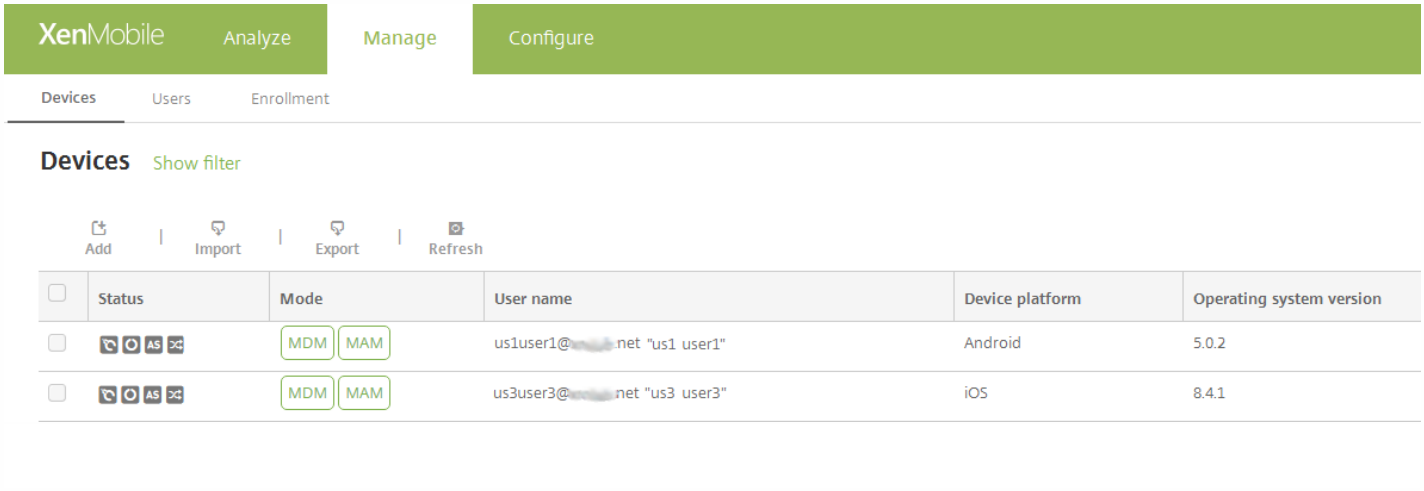
- 多数のWindowsデバイスがある場合、ストア名をデフォルト値に変更します。その後で、iOSおよびAndroidデバイスを使用して登録したエンドユーザーは、Citrix Secure Hub（旧Worx Home）からサインオフし、再びサインインする必要があります。
- WindowsデバイスがiOSおよびAndroidデバイスより少ない場合、Windowsユーザーにデバイスを再登録してもらうことをお勧めします。

この問題について詳しくは、http://support.citrix.com/article/CTX214553を参照してください。

ユーザーは、実稼働環境での最新バージョンのXenMobileへのアップグレード後にデバイスを再登録する必要はありません。デバイスは、ハートビートの間隔に基づいて、新しいXenMobileサーバーに自動的に接続されます。ただし、デバイスを再接

続する前にユーザーが再認証を求められる可能性があります。

ユーザーデバイスが接続されたら、XenMobileコンソールに次の図のようにデバイスが表示されることを確認します。



e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

RBACを使用した役割の構成

Apr 07, 2017

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。

*権限を適用すること*で、RBACの役割が管理する権限があるユーザーグループを定義します。デフォルトの管理者は、適用された権限設定を変更できません。適用された権限は、デフォルトですべてのユーザーに適用されます。

*割り当て*を実行して、RBACの役割をグループに割り当てて、そのユーザーグループがRBACの管理者権限を持つようにできます。

- Adminの役割
- Device Provisioningの役割
- Supportの役割
- ユーザーロール

RBACを使用した役割の構成

XenMobileの役割ベースのアクセス制御（Role-Based Access Control：RBAC）機能では、権限の定義済みセットである役割をユーザーとグループに割り当てることができます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。

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

- **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。

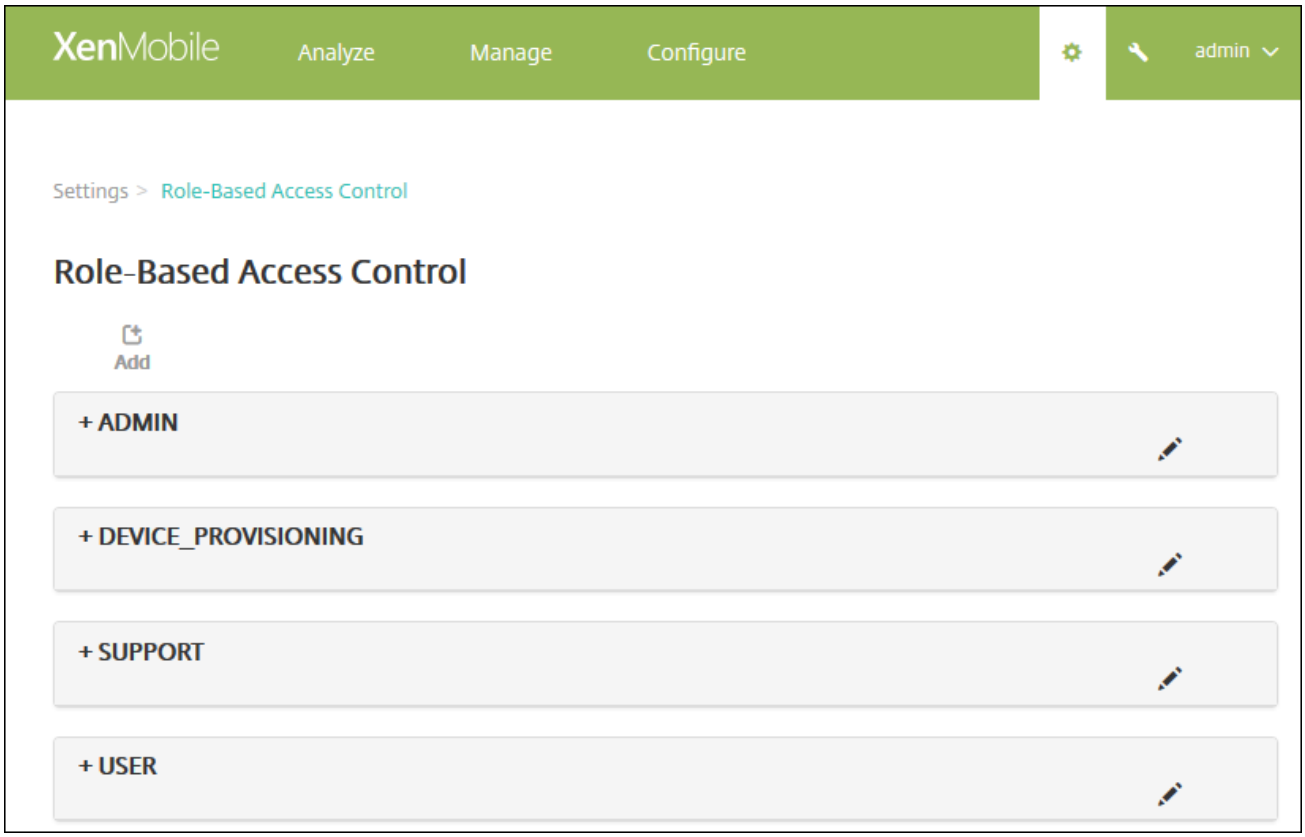
注： ローカルユーザーに割り当てることができる役割は1つだけです。

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. [Role-Based Access Control] をクリックします。[Role-Based Access Control] 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。

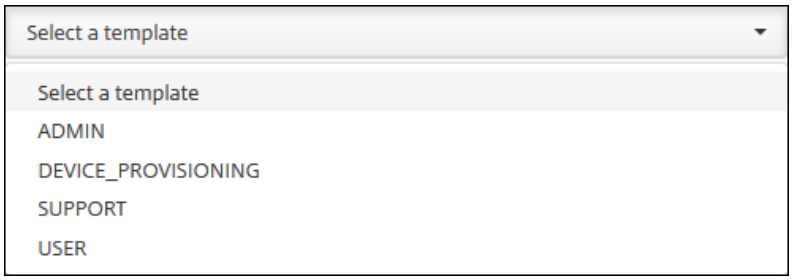
3. [Add] をクリックして新しいユーザー役割を追加したり、既存の役割の右にあるペンアイコンをクリックして役割を編集したり、以前定義した役割の右にあるごみ箱アイコンをクリックして役割を削除したりします。デフォルトのユーザー役割を削除することはできません。

- ［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。

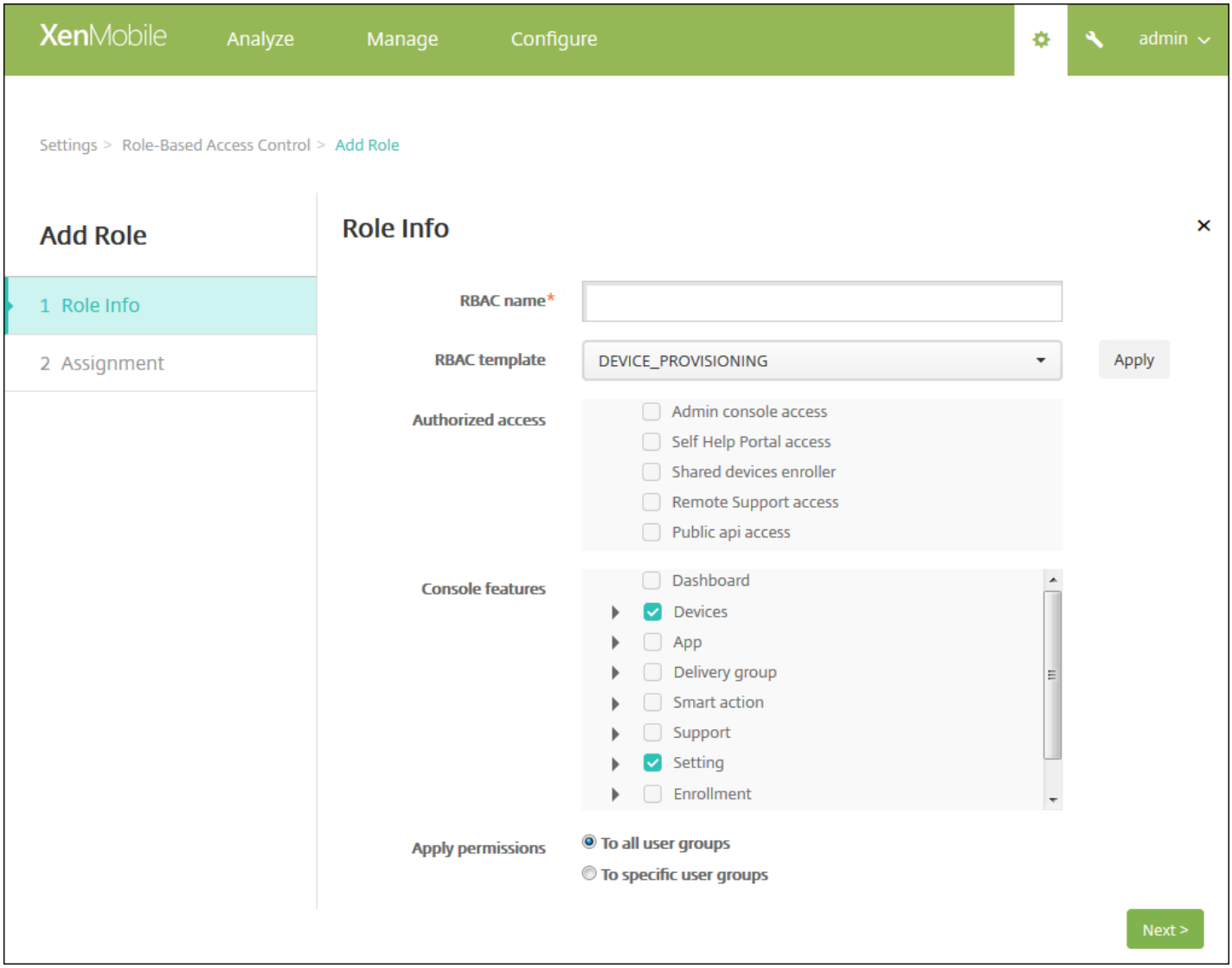
4. 新しいユーザー役割を作成するか、または既存のユーザー役割を編集するには、次の情報を入力します。

- 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。

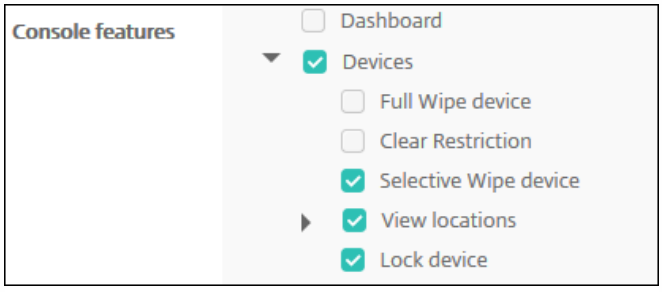


5. ［RBACテンプレート］フィールドの右にある［適用］をクリックして、選択したテンプレートで定義済みのアクセス権と機能権限を、［承認済みアクセス］および［コンソールの機能］にあるチェックボックスに反映させます。

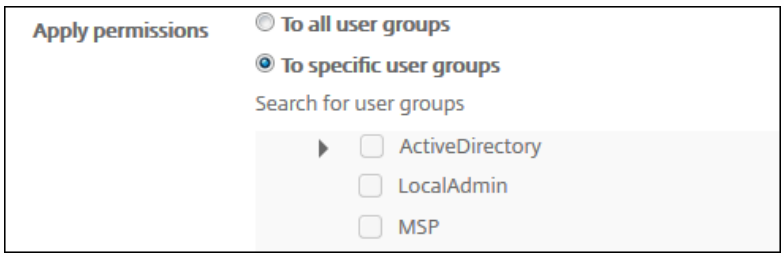


6. [Authorized access] および [Console Features] にあるチェックボックスをオンまたはオフにして、役割をカスタマイズします。

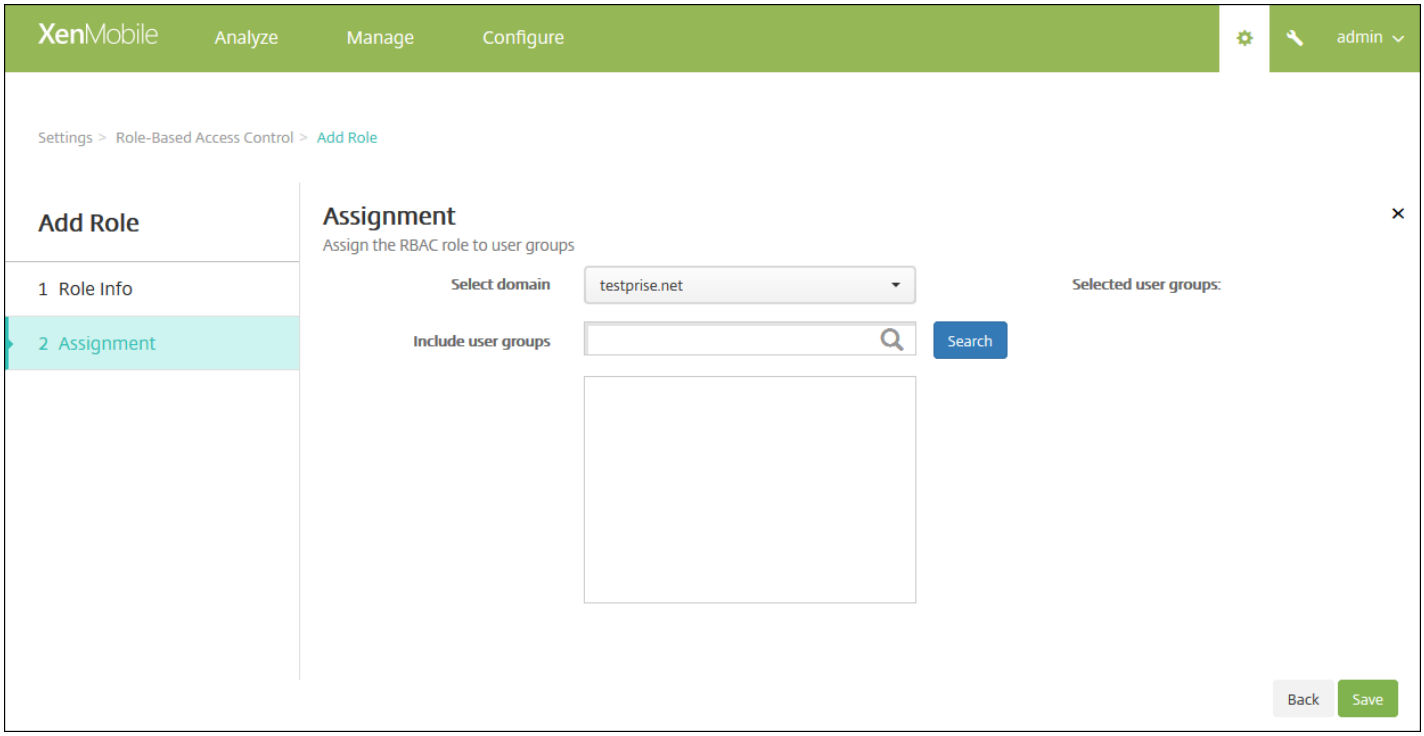
［Console feature］の横にある三角をクリックすると、その機能に固有の権限が表示され、オンまたはオフを選択できます。最上位のチェックボックスをオンにすると、そのコンソール部分に対するアクセスを禁止できます。最上位レベルよりのオプションを有効にするには、それらのオプションを個別にオンにする必要があります。たとえば、次の図で、 [Full Wipe device] オプションおよび [Clear Restrictions] オプションは、その役割を割り当てられたユーザーのコンソールには表示されません。一方で、チェックボックスがオンになっているオプションは表示されます。



7.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。

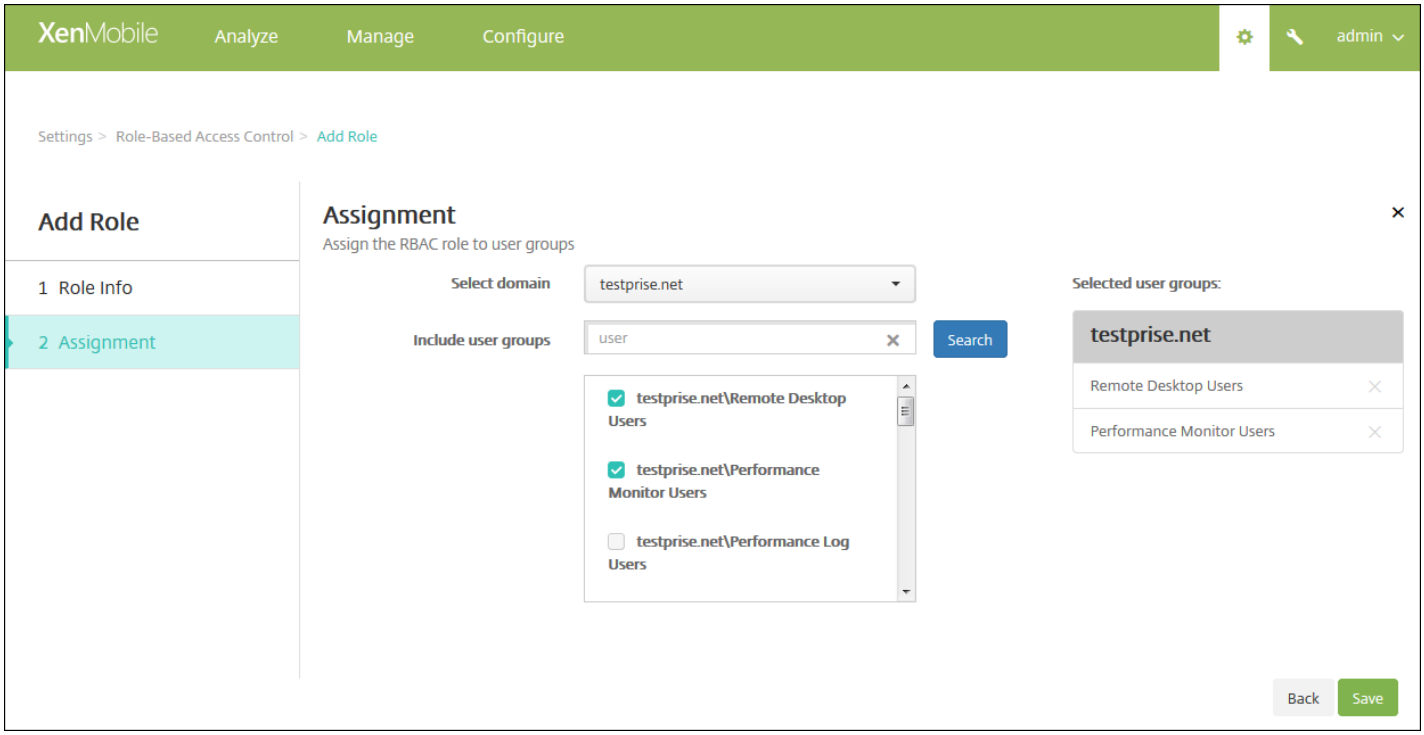


8. ［Next］をクリックします。［Assignment］ページが開きます。



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. [保存] をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

iOSデバイスのロック

Feb 27, 2017

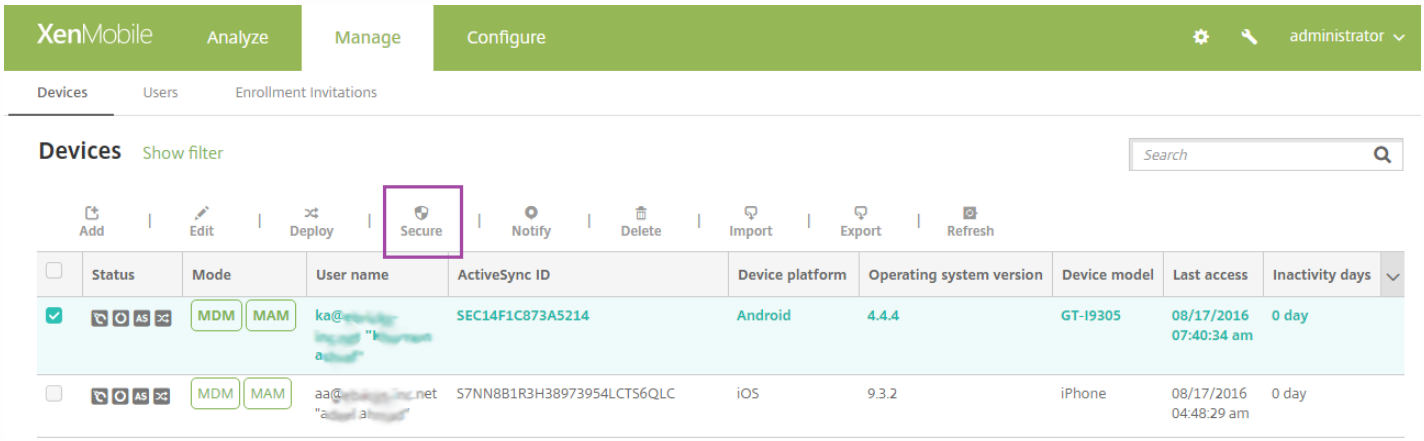
iOSデバイスをロックし、デバイスのロック画面にメッセージと電話番号を表示することができます。この機能は、iOS 7以降を実行しているデバイスでサポートされます。

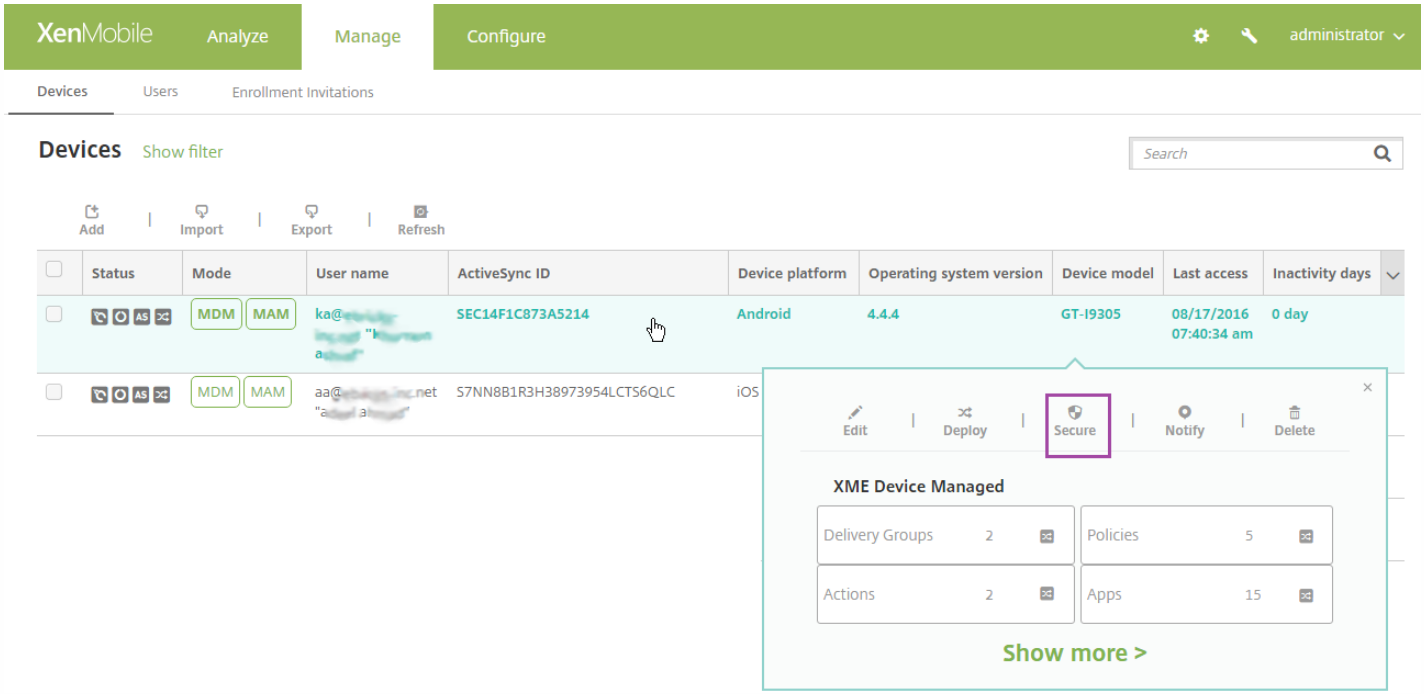
ロックされたデバイスにメッセージと電話番号を表示するためには、Passcodeポリシーが XenMobileコンソールで［true］に設定されている必要があります。あるいは、デバイス上でパスコードを手動で有効化する必要があります。

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。

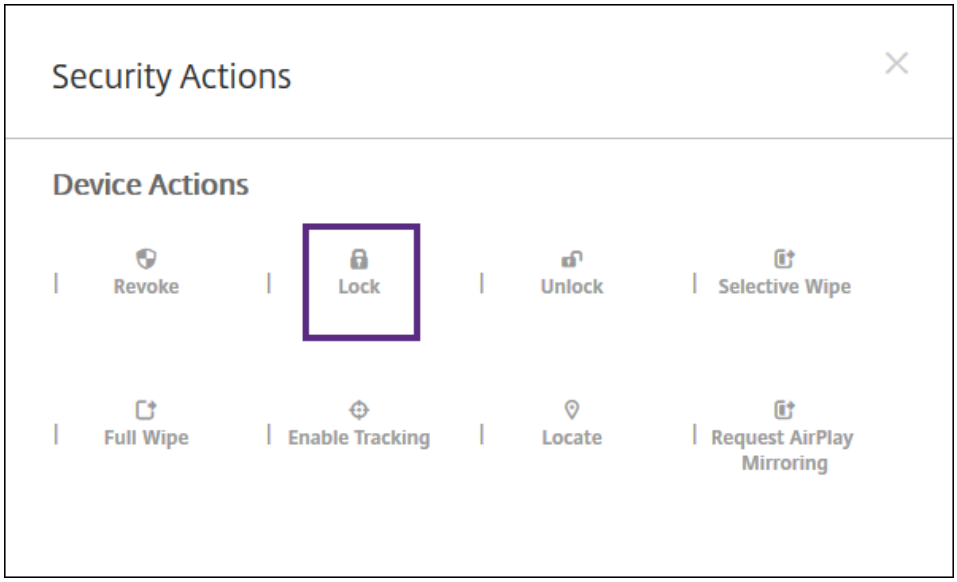
2. ロックするiOSデバイスを選択します。

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。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

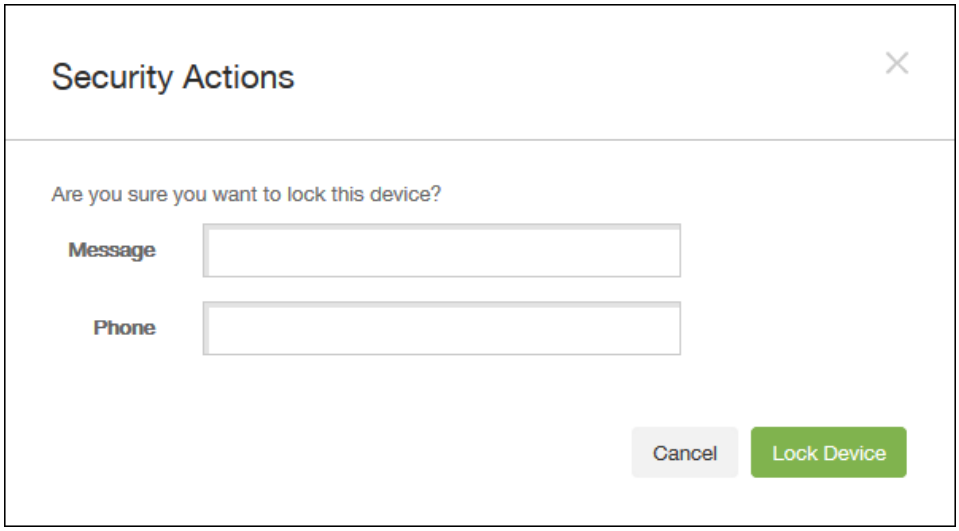




3. オプションメニューの［Secure］を選択します。［Security Actions］ダイアログボックスが開きます。



4. ［Lock］をクリックします。［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。

iOS 7以降を実行しているiPad：iOSは「Lost iPad」という文字列をユーザーが **[Message]** フィールドに入力した内容に追加します。iOS 7以降を実行しているiPhone： **[Message]** フィールドを空白にして電話番号を指定すると、Appleはメッセージ「Call owner」をデバイスのロック画面に表示します。

6. **[Lock Device]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

共有デバイス

Feb 27, 2017

XenMobileでは、複数のユーザーで共有可能な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、Citrix PIN、Touch ID、ユーザーエントロピー、2要素認証はサポートされません。

MDM+MAMモード

- iOSおよびAndroidタブレットでのみ使用できます。
- XenMobile 10.3以降でサポートされています。
- Active Directoryのユーザー名およびパスワード認証のみがサポートされます。
- クライアント証明書認証、Worx PIN、Touch ID、ユーザーエントロピー、2要素認証はサポートされません。
- MAMのみのモードはサポートされません。デバイスはMDMに登録する必要があります。
- Secure Mail、Secure Web、およびShareFileモバイルアプリのみがサポートされます。HDXアプリはサポートされません。
- Active Directoryユーザーのみがサポートされます。ローカルユーザーおよびグループはサポートされません。
- 既存のMDM-onlyモードの共有デバイスをMDM+MAMモードに更新するには、再登録が必要です。
- ユーザーは、XenMobile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XenMobile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。

MDM+MAMモードの前提条件

1. **Shared Device Enrollers**などの名前のActive Directoryグループを作成します。
2. 共有デバイスを登録するActive Directoryユーザーをこのグループに追加します。このために新しいアカウントが必要な場合は、新しいActive Directoryユーザー（**sdenroll**など）を作成して、このユーザーをActive Directoryグループに追加します。

共有デバイスの要件

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。

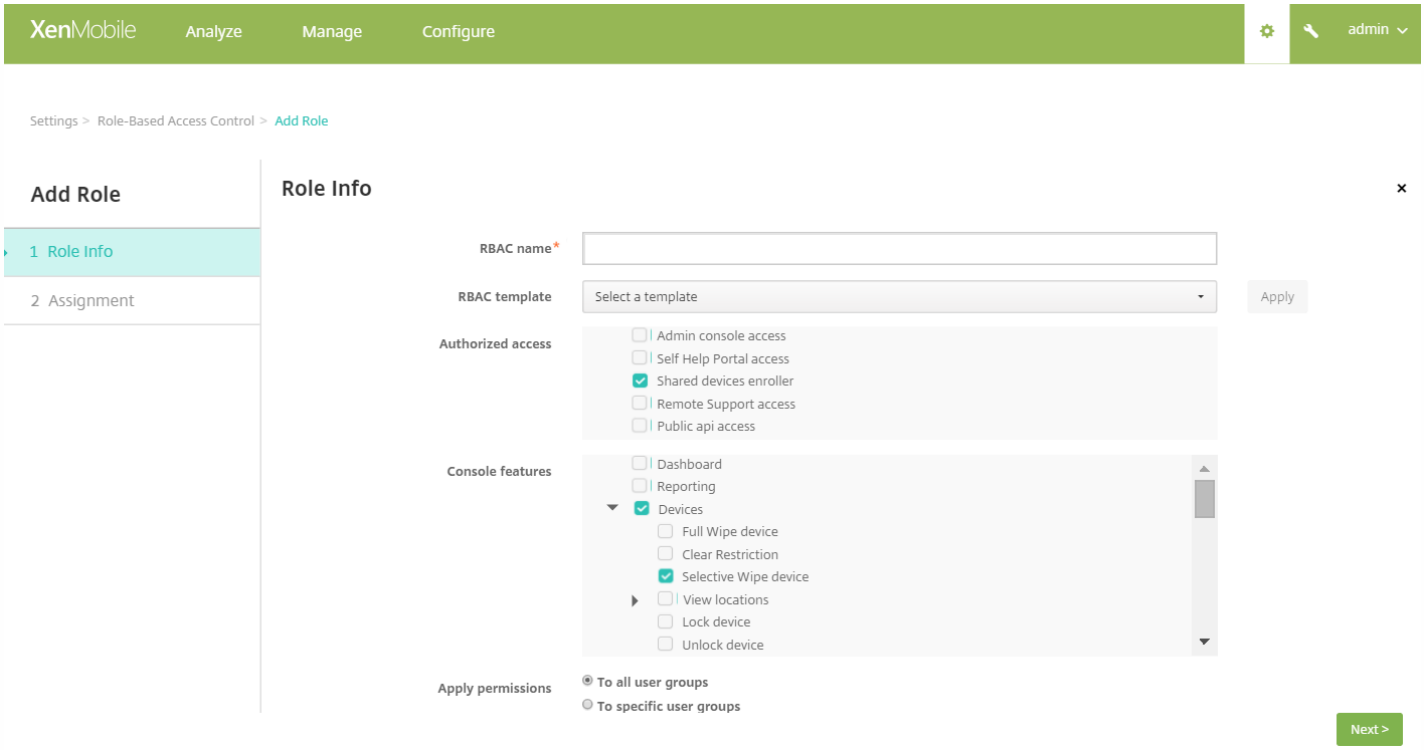
- iOS 9および10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x（MDM-onlyモード）

共有デバイスを構成するには

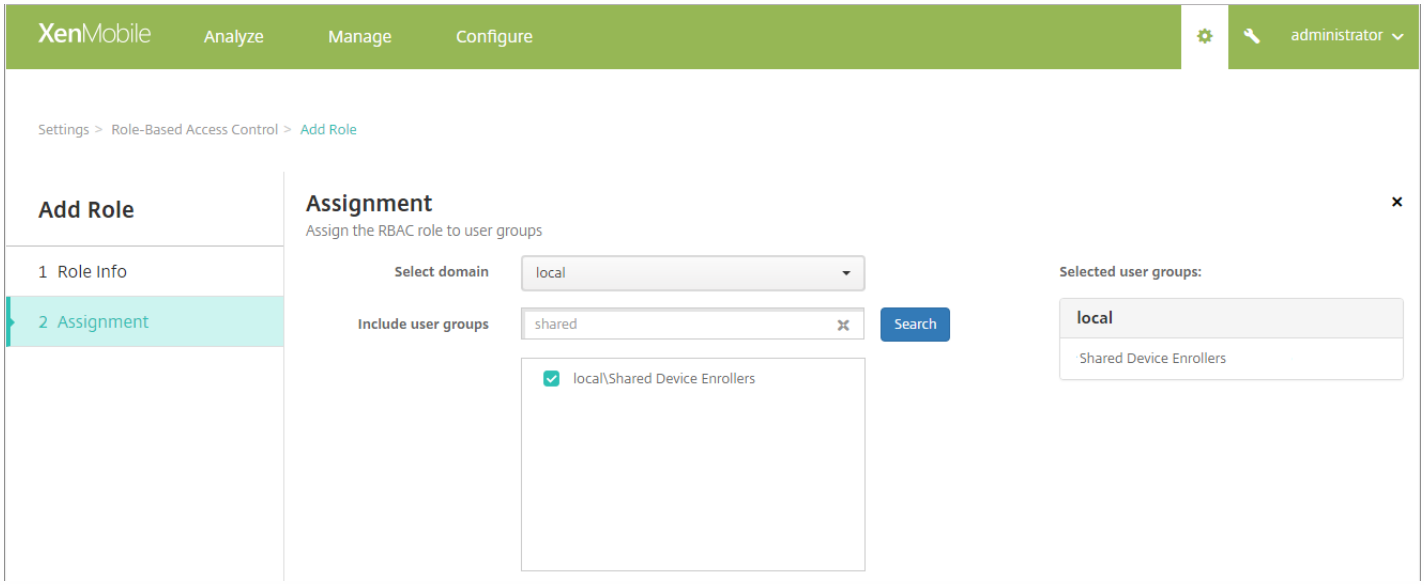
以下の手順に従って、共有デバイスを構成します。

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。**［Add Role］**画面が表示されます。
3. **［uthorized Access］**で［Shared Device Enrollment User］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Secure Hubから削除されます。

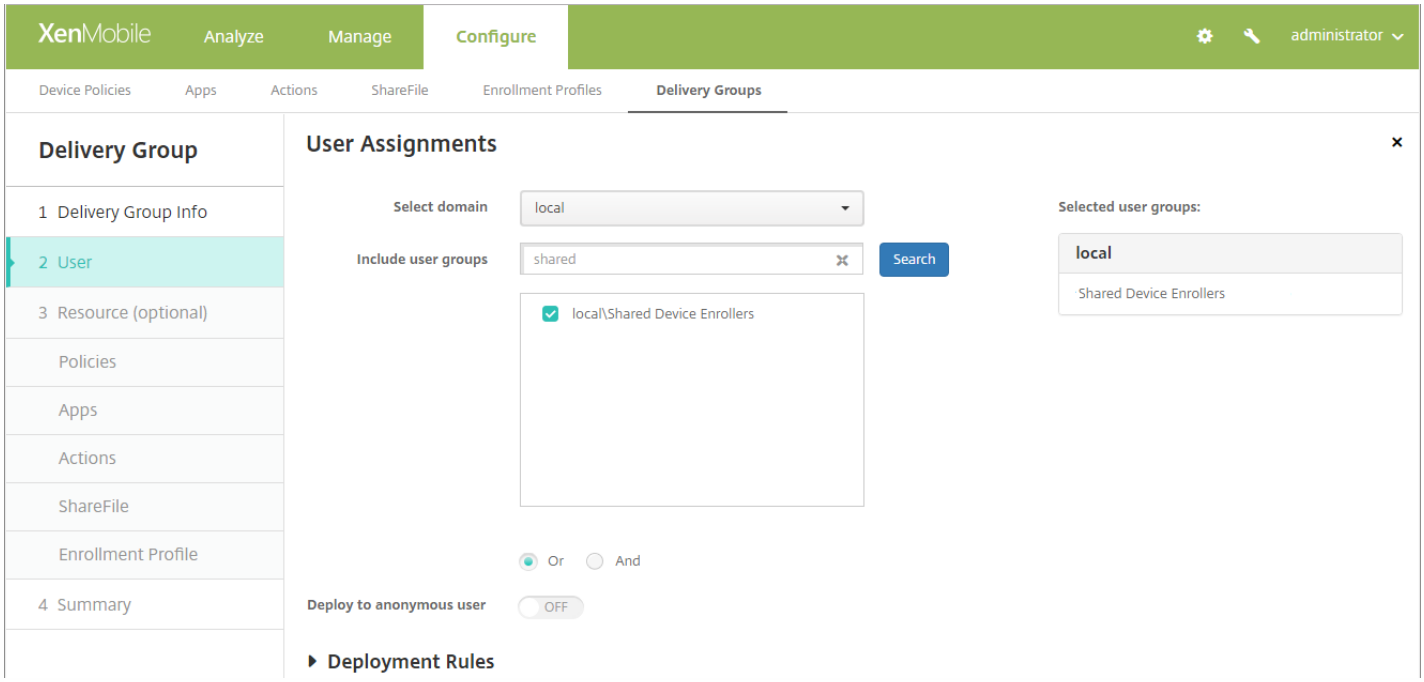
   ［適用権限］で、デフォルト設定の**［すべてのユーザー グループ］**を保持するか、特定のActive Directoryユーザーグループに**［特定のユーザー グループ］**で権限を割り当てます。



［**Next**］をクリックして［**Assignment**］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、Secure Hubをインストールし、共有デバイス登録ユーザーアカウントを使用してXenMobileにデバイスを登録します。XenMobileコンソールでデバイスを表示および管理できるようになります。詳しくは、「デバイスの登録」を参照してください。

6. 認証されたユーザーに異なるポリシーを適用したり、追加のアプリ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

MDMモード

ユーザーにはそのユーザーが使用できるリソースだけが表示され、すべての共有デバイスに同じエクスペリエンスが提供されます。共有デバイス登録ポリシーとアプリは常にデバイスに残ります。共有デバイス登録ユーザー以外のユーザーがSecure Hubにサインオンすると、そのユーザーのポリシーとアプリ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。

MDM+MAMモード

共有デバイス登録ユーザーによって登録されると、Secure MailとSecure Webがデバイスに展開されます。ユーザーデータはデバイスに安全に保持されます。ユーザーがSecure MailまたはSecure Webにサインオンした場合、データはほかのユーザーには表示されません。

Secure Hubにサインオンできるユーザーは、一度に1人だけです。前のユーザーがサインオフしてからでないと、次のユーザーはサインオンできません。セキュリティ上の理由から、共有デバイスにはユーザーの資格情報が保存されないので、ユーザーはサインオンのたびに資格情報を入力する必要があります。前のユーザーのためのリソースに新しいユーザーがアクセ

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Secure Mailポリシー

- Secure Mailのパフォーマンスを最適化するためには、デバイスを共有するユーザーの数に応じて**[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。その他のすべての設定はデバイスを共有しているユーザー間で共通です。

  通知
  署名
  不在
  メールの同期期間
  S/MIME
  スペルチェック

Android at Work

Feb 27, 2017

Android at Work（Android for Workから改称）は、Android 5.0以降を実行しているAndroidデバイスで使用できるセキュリティ保護されたワークスペースです。このワークスペースはビジネス用のアカウント、アプリ、データを個人のアカウント、アプリ、データから隔離します。XenMobileでは、デバイスに2個の作業プロファイルを作成できるため、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。ハードウェアの暗号化および展開するポリシーを組み合わせることで、デバイスで業務の領域と個人領域を安全に隔離できます。ユーザーの個人用の領域に影響を与えずに、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 Android Enterpriseのサイトを参照してください。

Google Playを使用して、アプリを追加、購入、および承認し、デバイスのAndroid at Workワークスペースに展開します。Google Play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展開できます。Android at 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を確認できます。状態に含まれる情報は、使用できる合計ライセンス数、使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレスです。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 at 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
- 管理されたプロファイルサポートがあり、Android 5.0以降のLollipopを実行しているデバイス
- Google Playがインストールされ ているGoogleアカウント
- デバイスで設定されたワークプロファイル

Android at 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 at 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 at Workサーバー設定を構成します。
- 少なくとも1つのAndroid at Workデバイスポリシーを作成します。
- Google Playアプリストアで Android at Workアプリを追加、購入、承認します。

Android at 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
- Google Play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用のGoogle Playの公開 :https://play.google.com/apps/publish
- サービスアカウント作成のためのGoogle Developer Console :https://console.developers.google.com

Android at Workの前提条件

XenMobileでAndroid at Workを管理するには、以下の作業が必要です。

- Android at 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 at 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設定を構成して、Androidアプリを管理できます。資格情報の作成について詳しくは、「Google Play資格情報」を参照してください。

Android at Workアカウントの作成

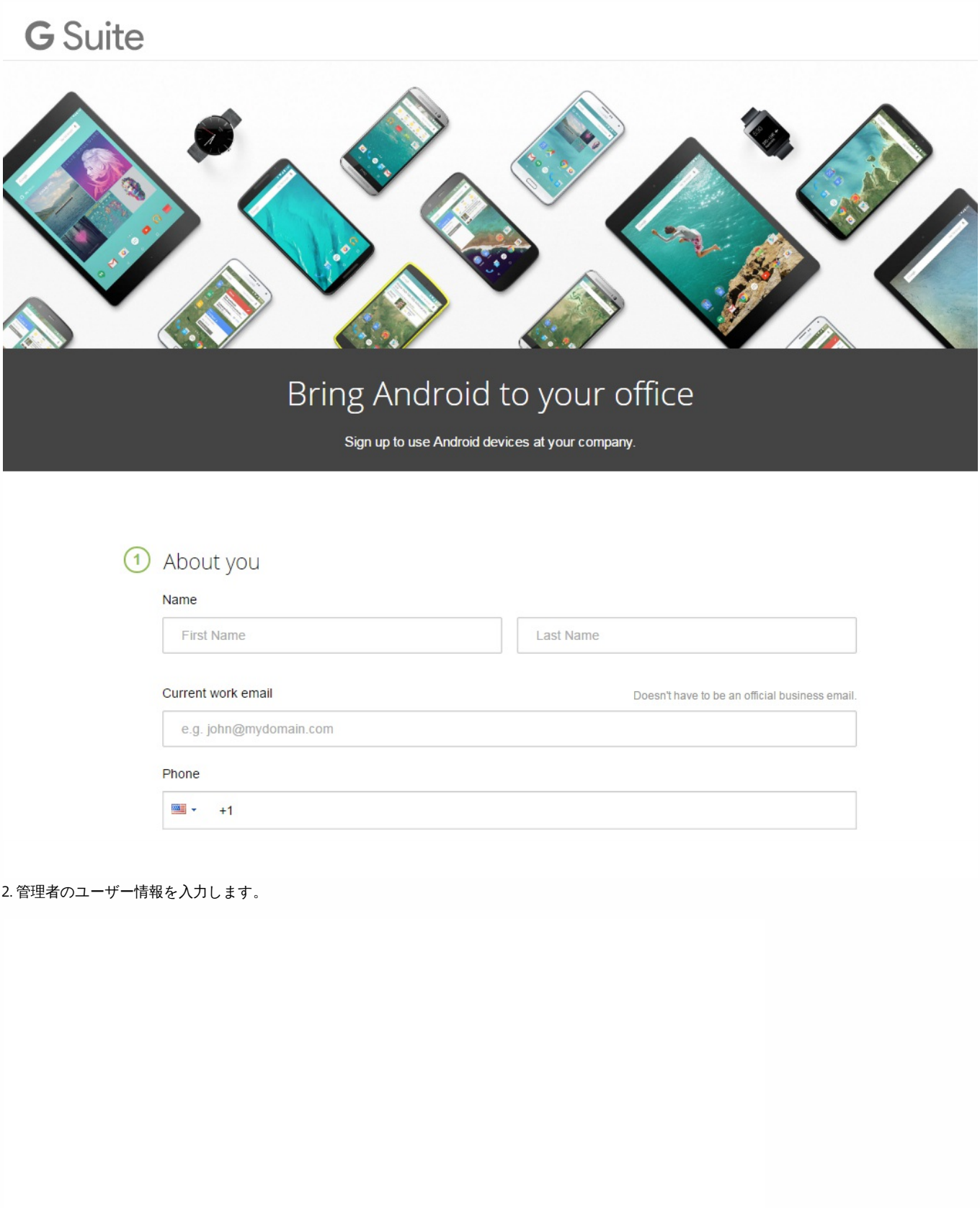
Android at Workアカウントを構成する前に、以下の前提条件を満たす必要があります。

- ドメイン名（たとえば、example.com）を所有している。
- Googleにドメインの所有権を検証させる。
- 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以降など）を介して、Android at Workを有効化し、管理します。

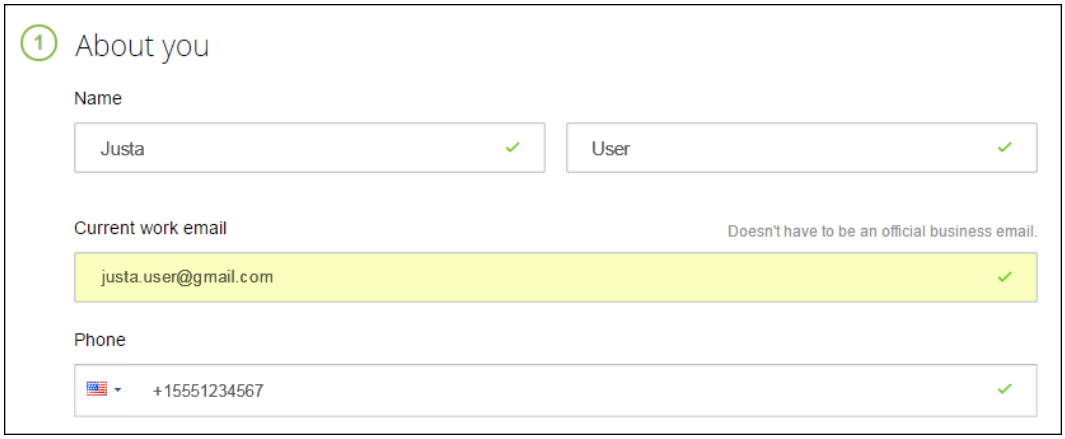
ドメイン名が既に s Googleで検証済みの場合は、「Android at Workサービスアカウントの設定とAndroid at Work証明書のダウンロード」の手順をスキップできます。

1.https://www.google.com/a/signup/?enterprise_product=ANDROID_WORKに移動します。

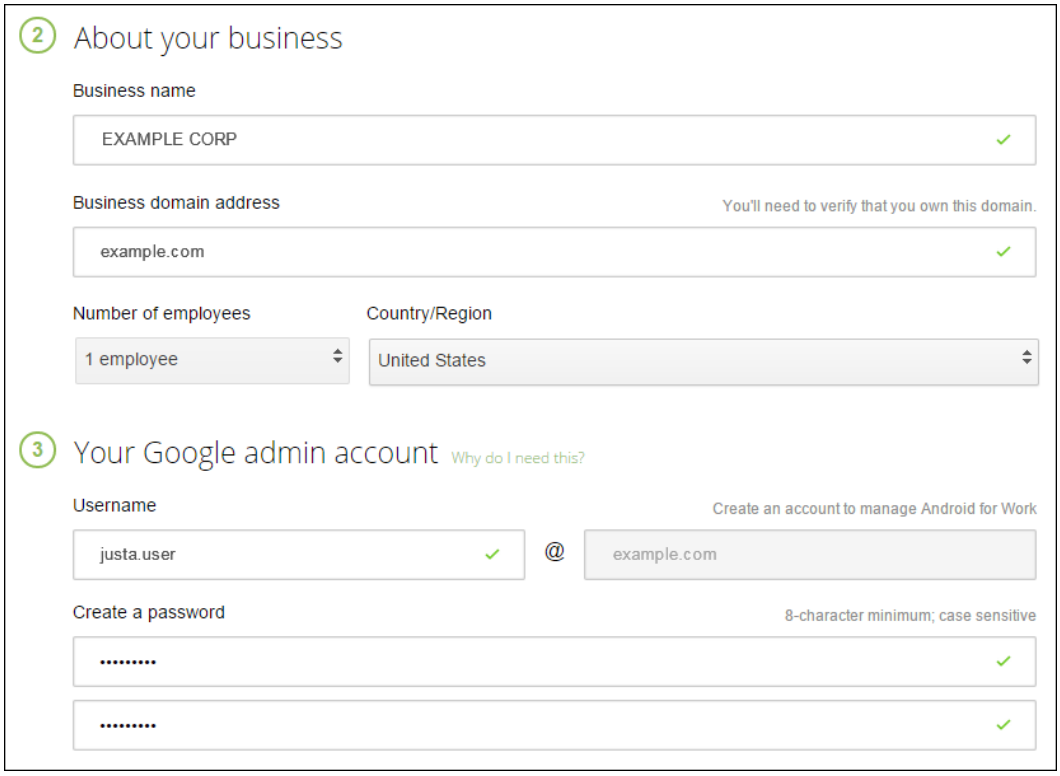
管理者情報と会社情報を入力する次のページが開きます。



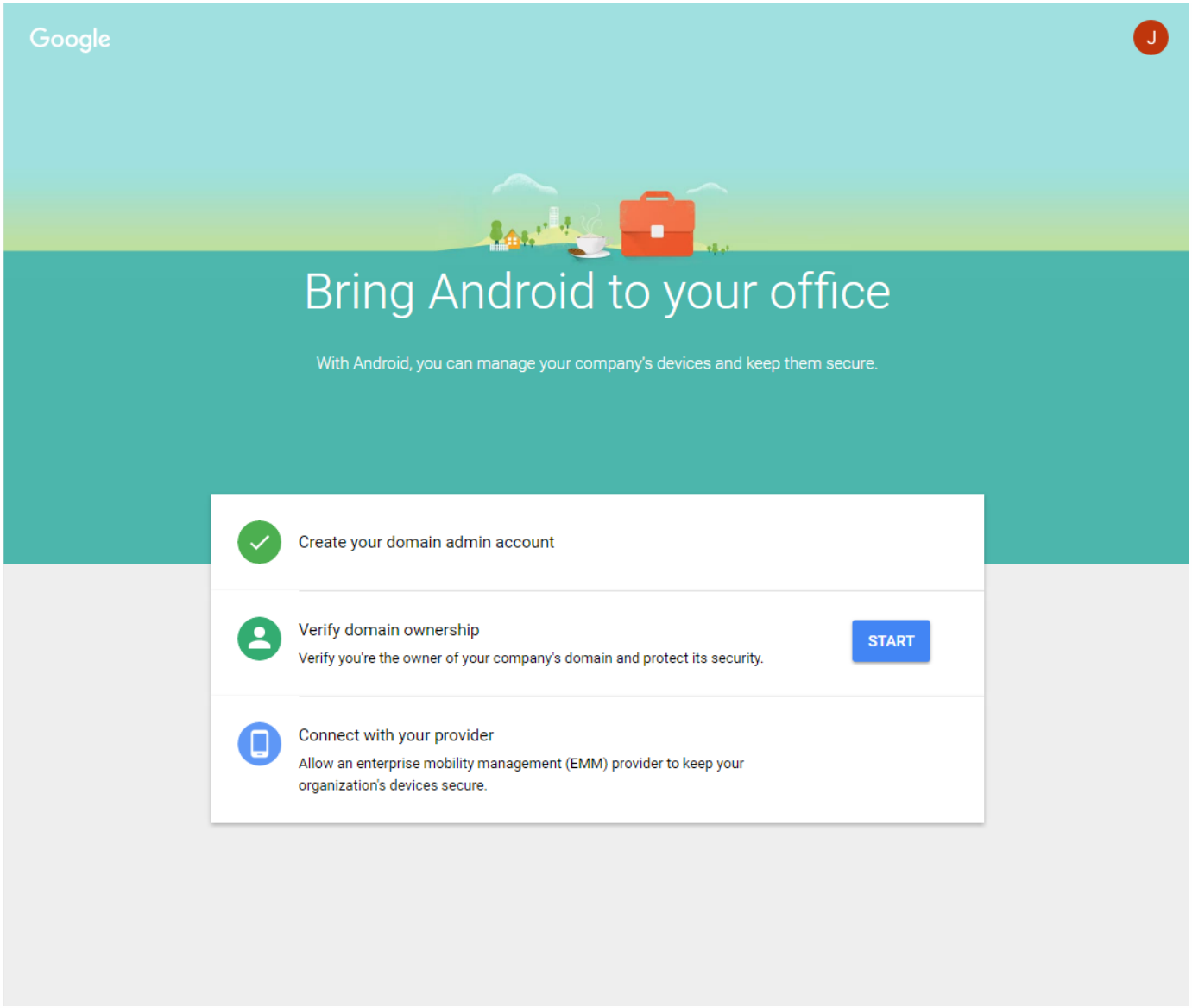
2. 管理者のユーザー情報を入力します。



3. 管理者のアカウント情報だけでなく、会社情報も入力してください。



プロセスの最初の手順が完了します。以下のページが開きます。



ドメイン所有権の検証

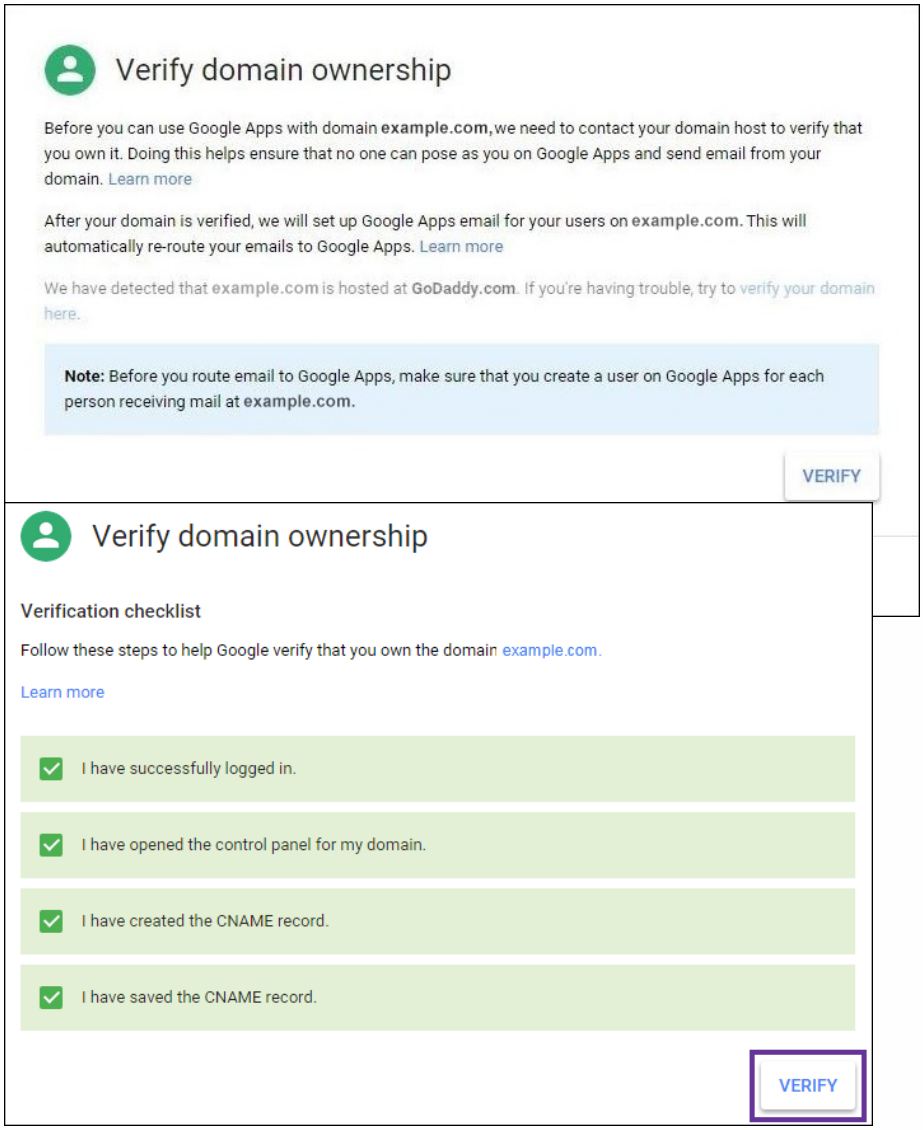
以下のいずれかの方法で、Googleがドメインを検証できるようにします。

- ドメインホストのWebサイトにTXTまたはCNAMEレコードを追加します。
- HTMLファイルをドメインのWebサーバーにアップロードします。
- ホームページにタグを追加します。Googleでは最初の方法を推奨しています。ドメインの所有権を検証する手順についてはこの記事では扱いませんが、必要な情報はhttps://support.google.com/a/answer/6095407/に記載されています。

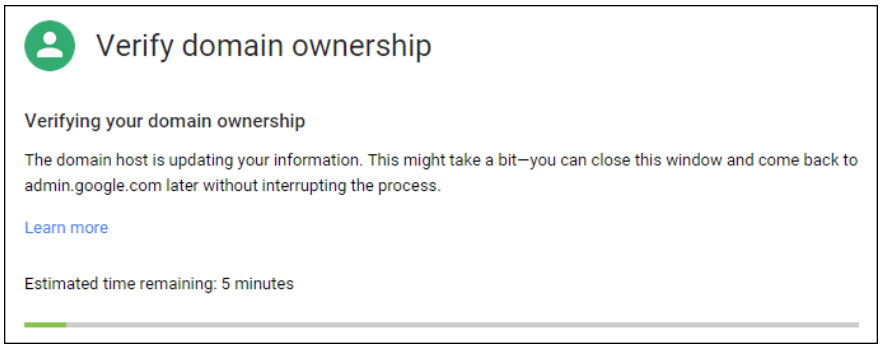
1. **[Start]** をクリックして、ドメインの検証を開始します。

[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。

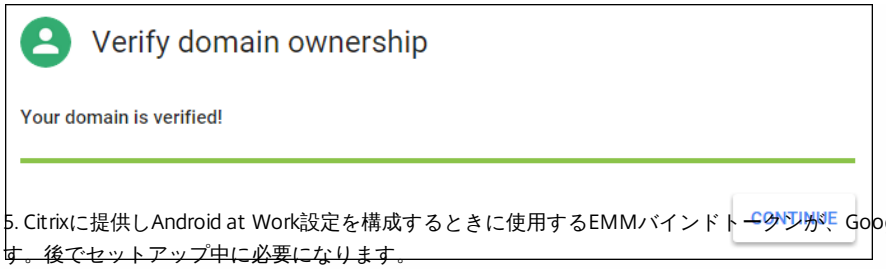
2. **[Verify]** をクリック します。



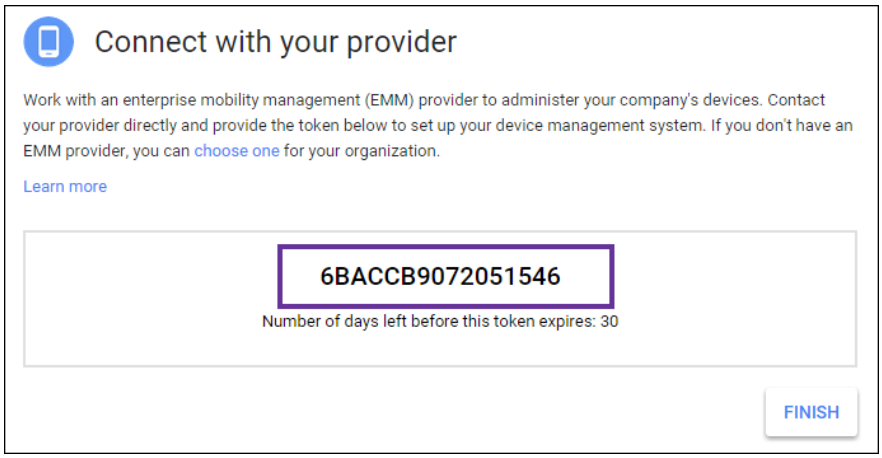
3. Googleによってドメイン所有権が検証されます。



4. 検証が成功すると、次のページが開きます。 **[Continue]** をクリックします。



5. Citrixに提供しAndroid at 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 at Workの設定を完了します。ドメインの検証に成功したことを示すページが表示されます。

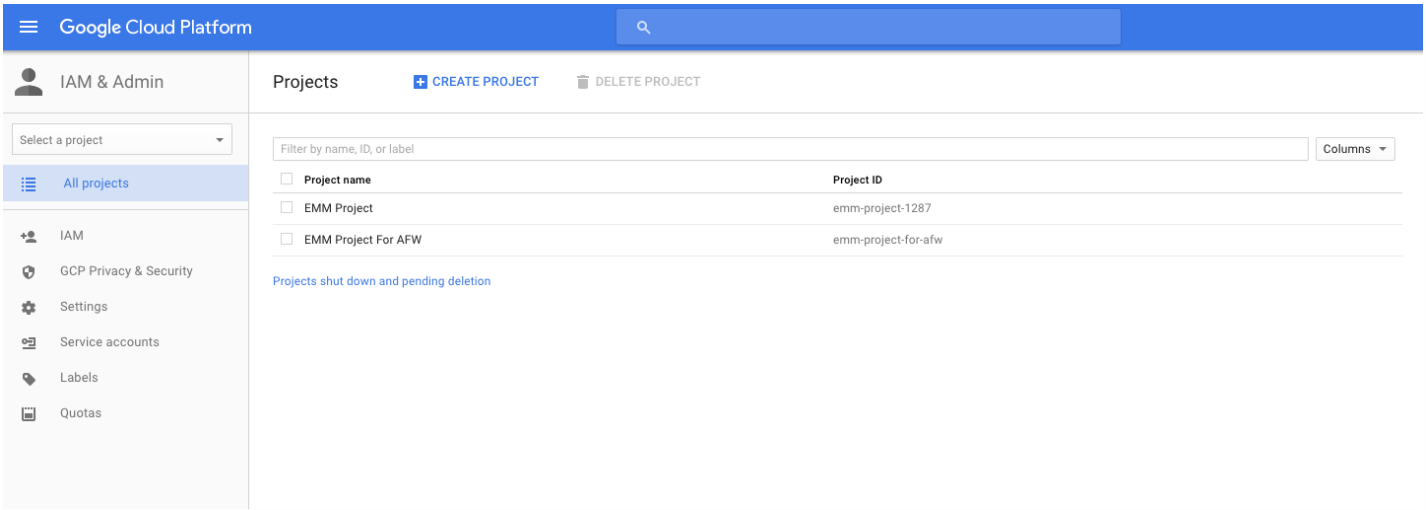
Android at Workサービスアカウントを作成すると、Google Adminコンソールにサインインしてモビリティ管理設定を管理できます。

Android at Workサービスアカウントの設定とAndroid at Work証明書のダウンロード

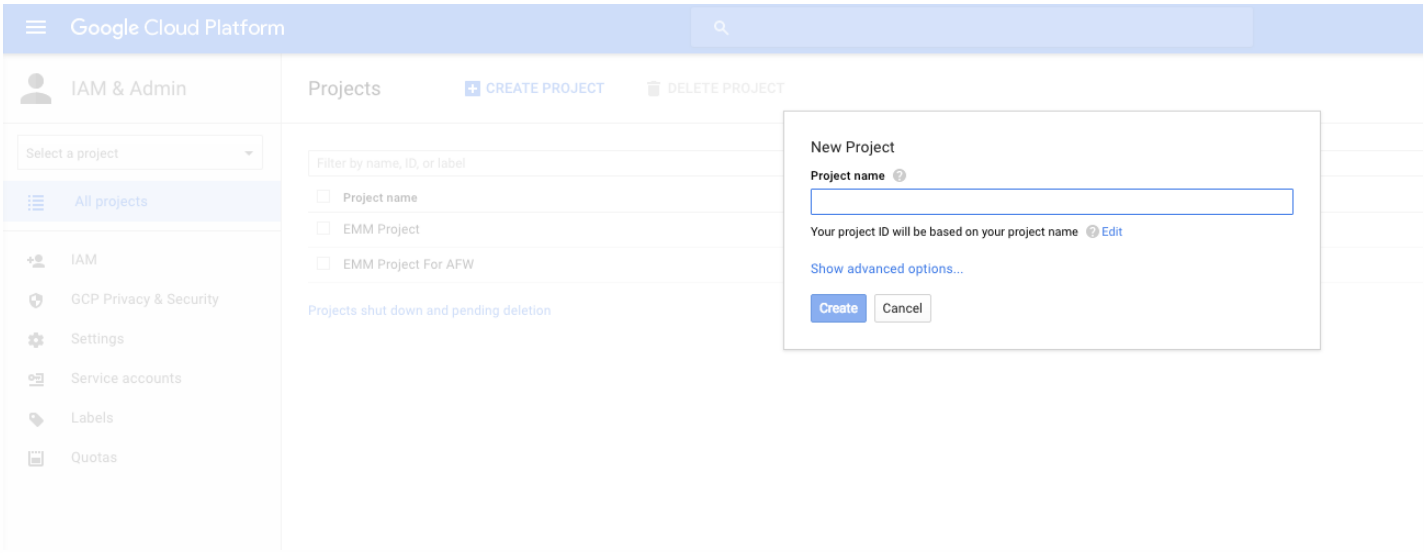
XenMobileからGoogle PlayサービスおよびDirectoryサービスにアクセスできるようにするには、Googleのデベロッパー用プロジェクトポータルを使用してサービスアカウントを作成する必要があります。このサービスアカウントは、XenMobileとAndroid at Work用のGoogleの各種サービスのサーバー間通信で使用します。使用されている承認プロトコルについて詳しくは、https://developers.google.com/identity/protocols/OAuth2ServiceAccountを参照してください。

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サインインします。

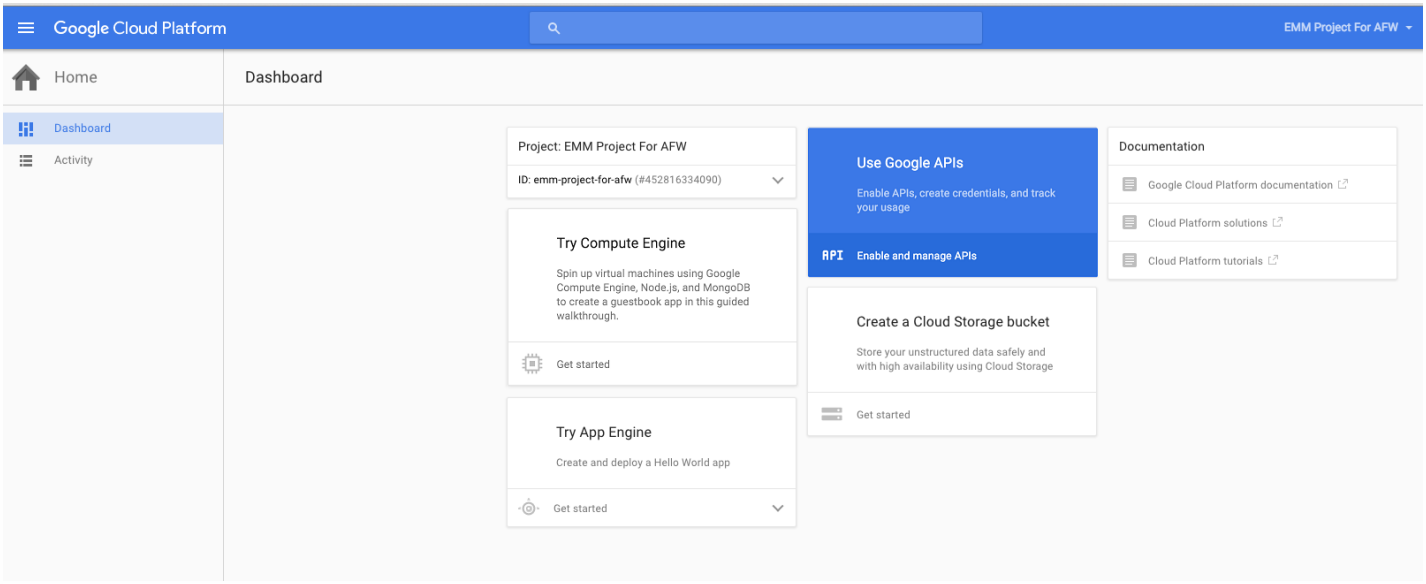
2. **[Projects]** の一覧で、 **[Create Project]** をクリックします。



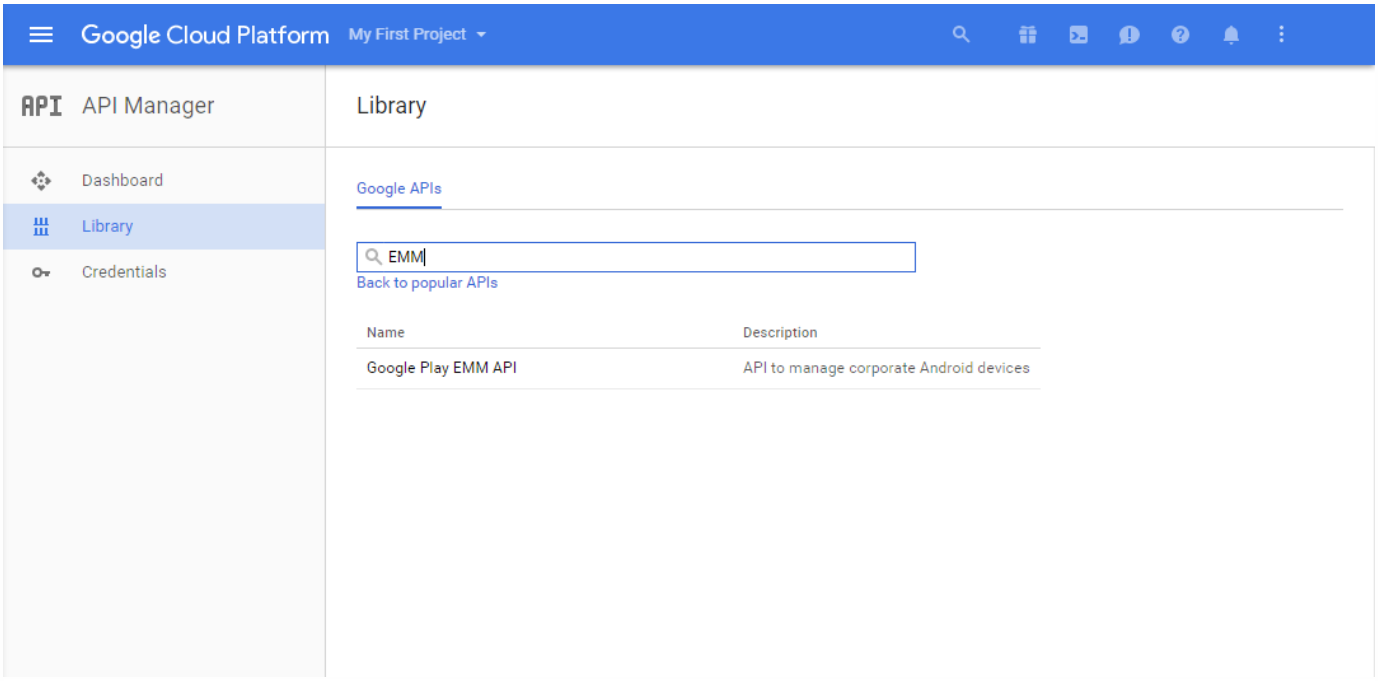
3. **[Project name]** ボックスに、プロジェクトの名前を入力します。



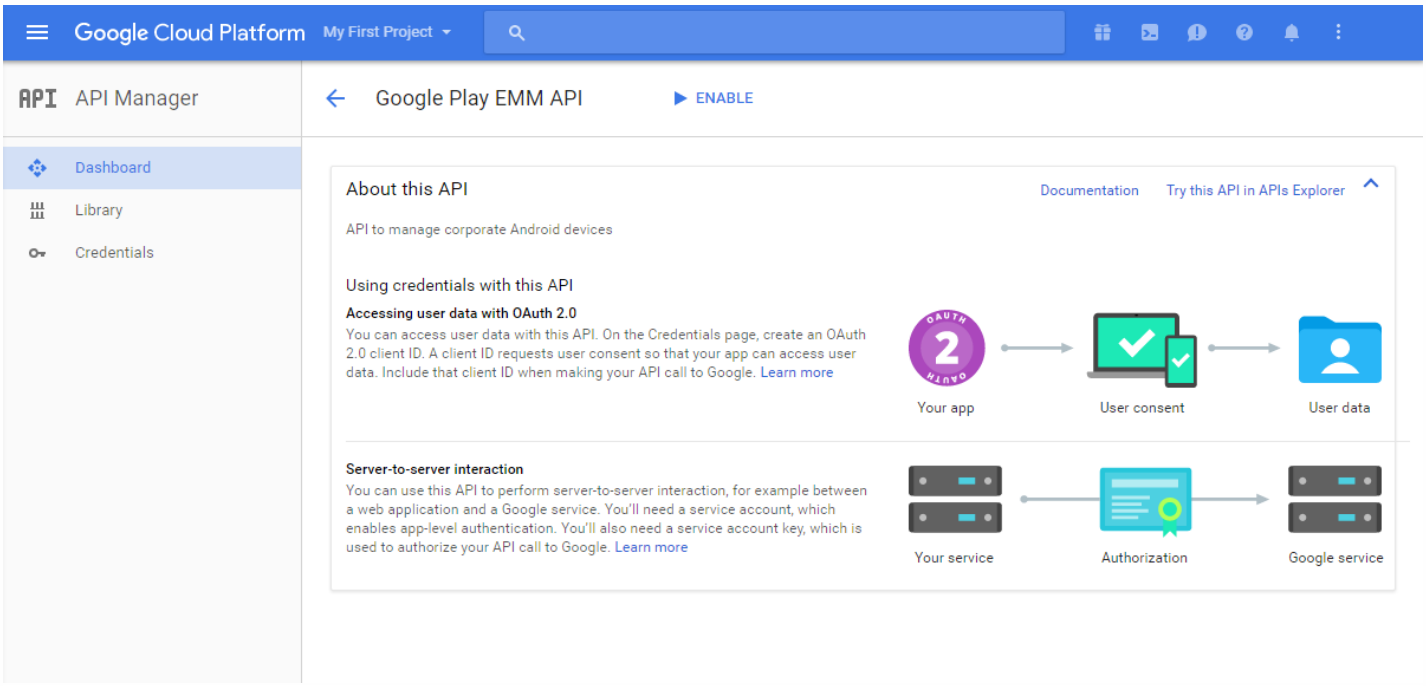
4. [**Dashboard**] ページで、 [Use Google APIs] をクリックします。



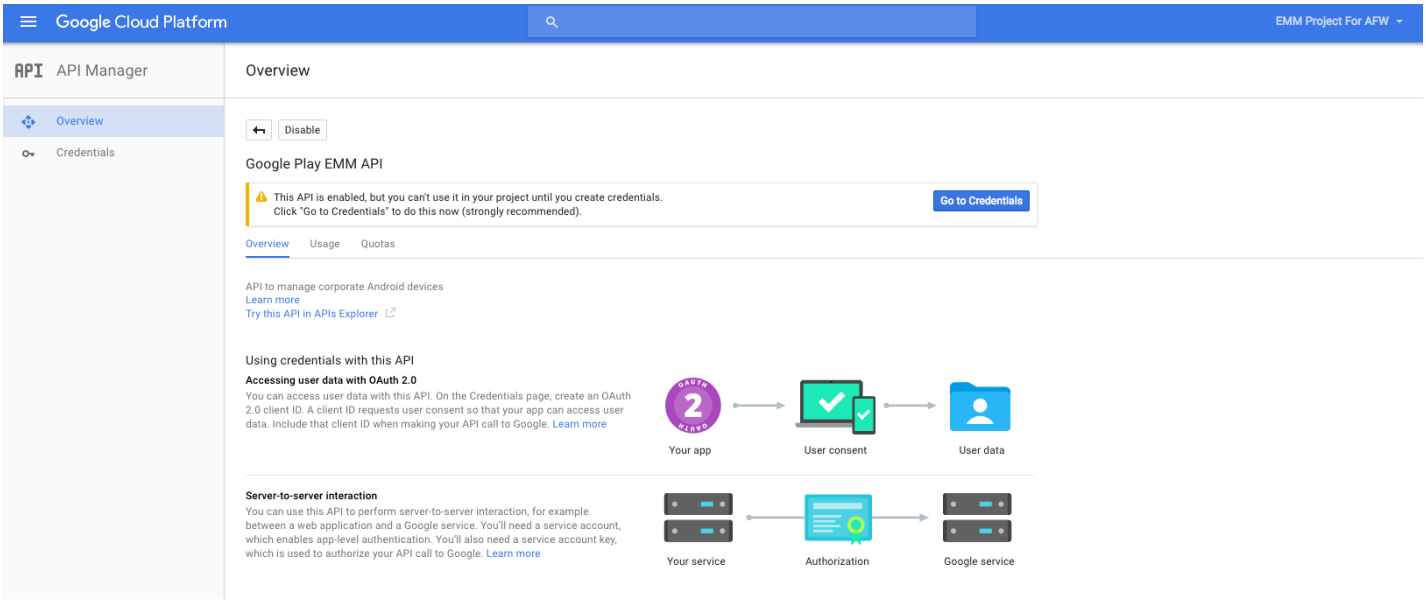
5. [**Library**] をクリックして、 [**Search**] に**EMM**と入力して、検索結果をクリックします。



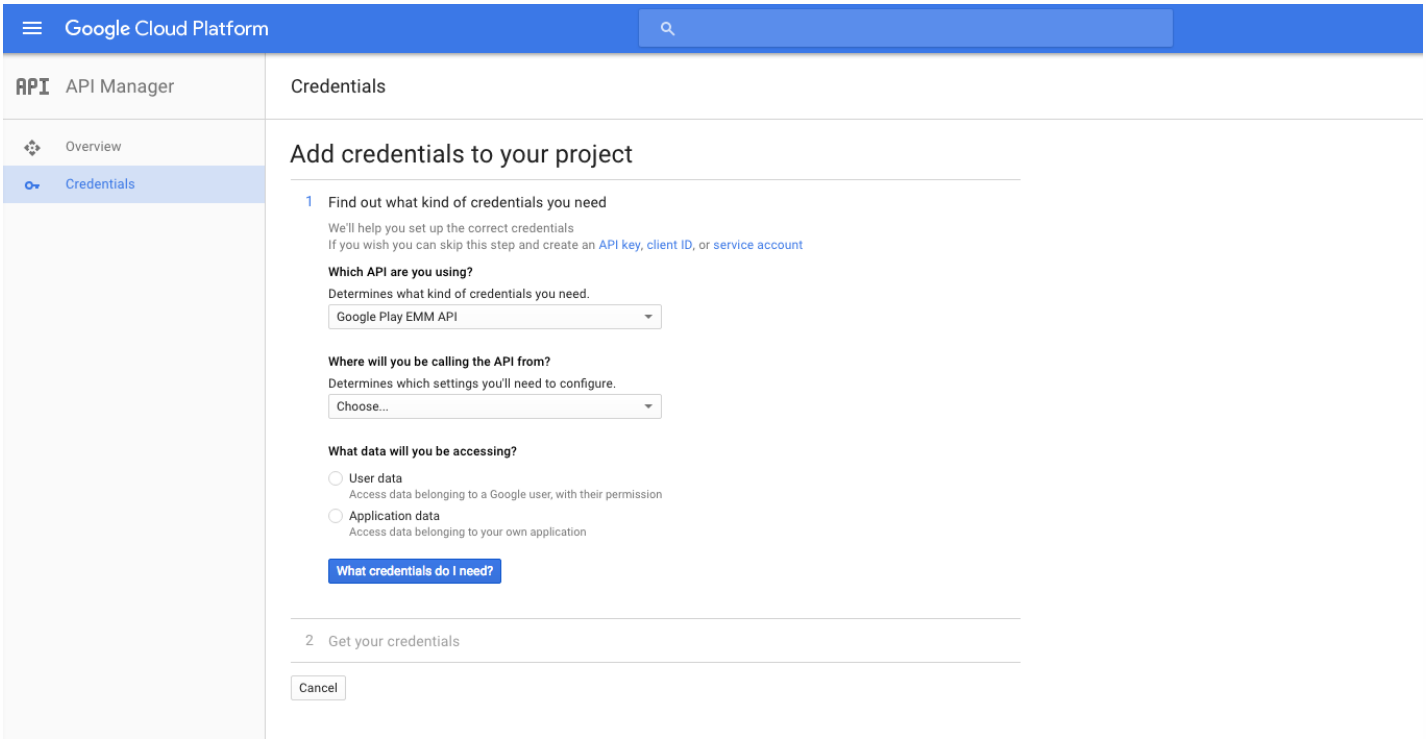
6. **[Overview]** ページで、 **[Enable]** をクリックします。



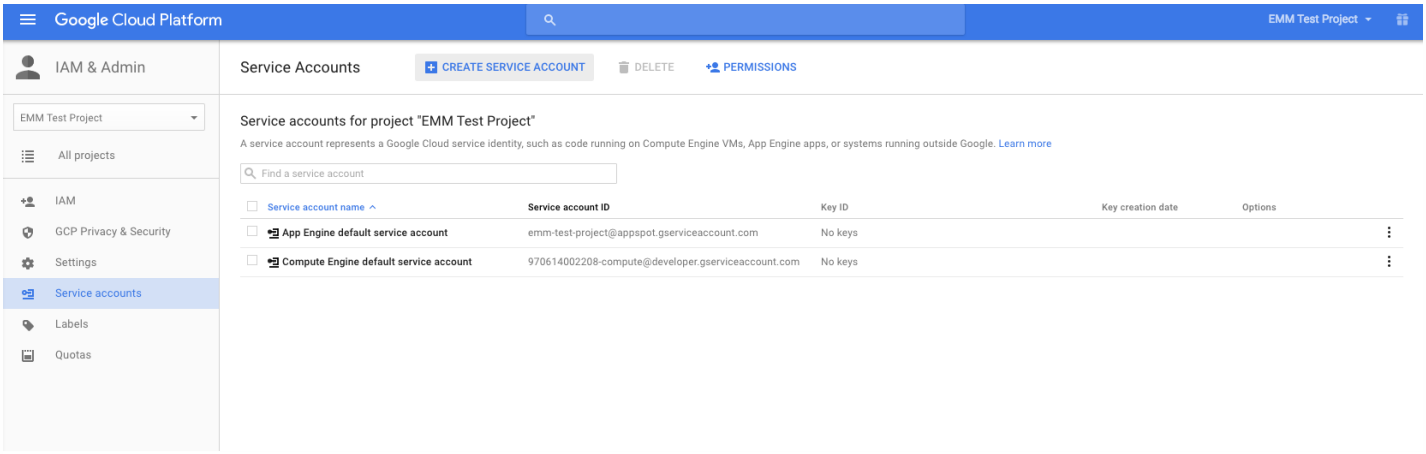
7. **[Google Play EMM API]** の横にある **[Go to Credentials]** をクリックします。



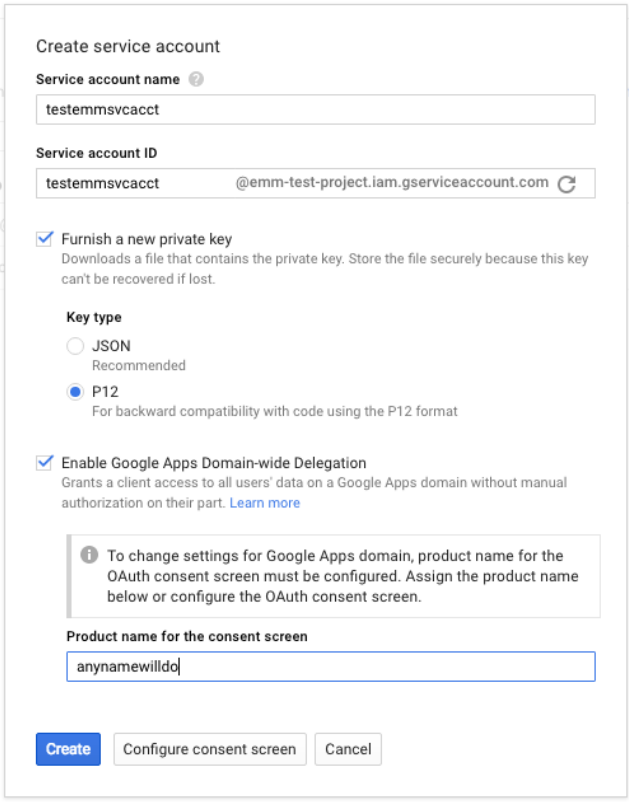
8. **[Add credentials to our project]**の一覧の手順1で、 **[service account]**をクリックします。



9. **[Service Accounts]**ページで、 **[Create Service Account]**をクリックします。

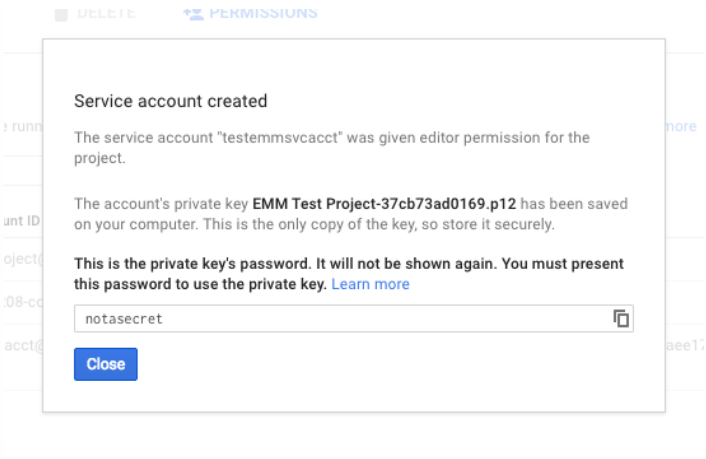


10. **[Create service account]** で、アカウントに名前を付けて、 **[Furnish a new private key]** をオンにします。 **[P12]** を選択して、 **[Enable Google Apps Domain-wide Delegation]** をオンにし、 **[Create]** をクリックします。

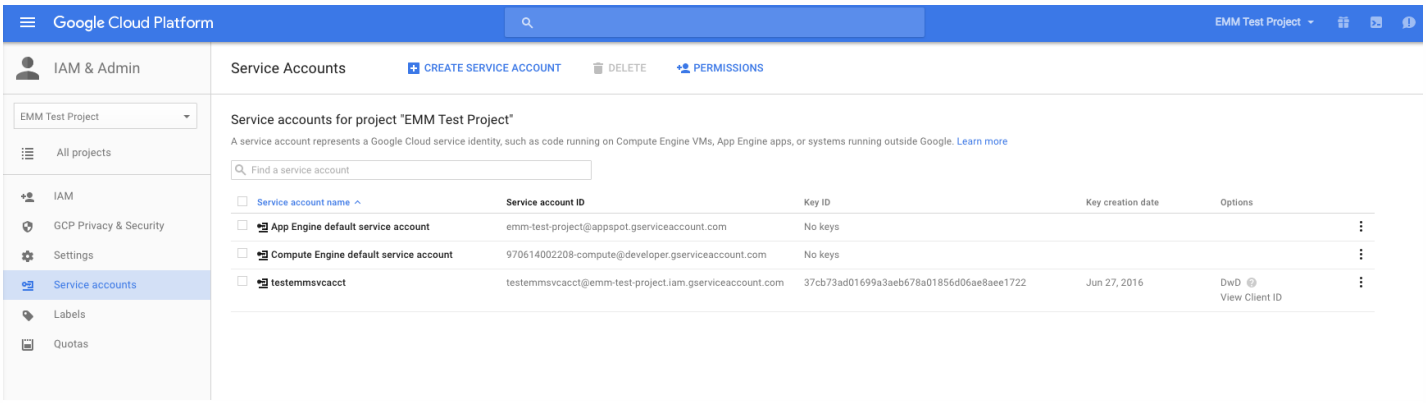


証明書（P12ファイル）がコンピューターにダウンロードされます。証明書を安全な場所に保存してください。

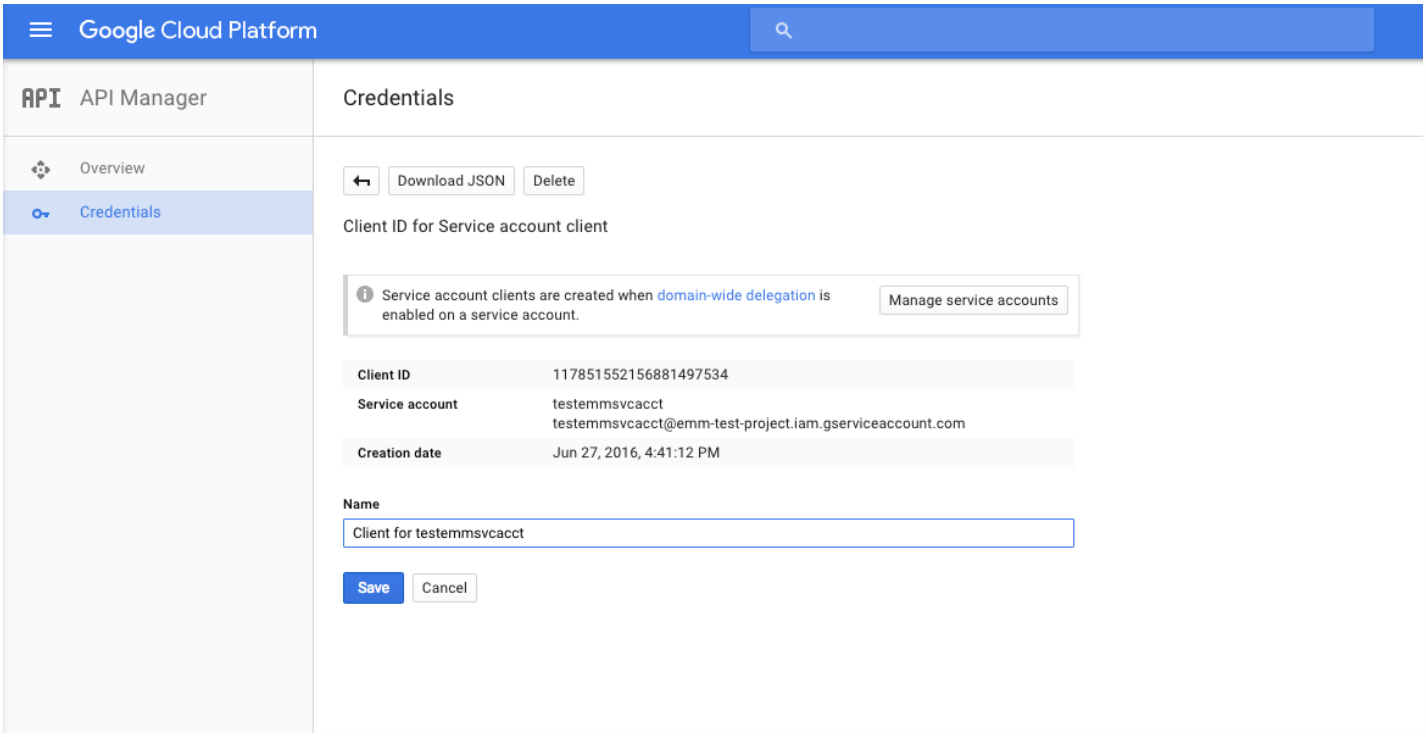
11. **[Service account created]** 確認画面で、 **[Close]** をクリックします。



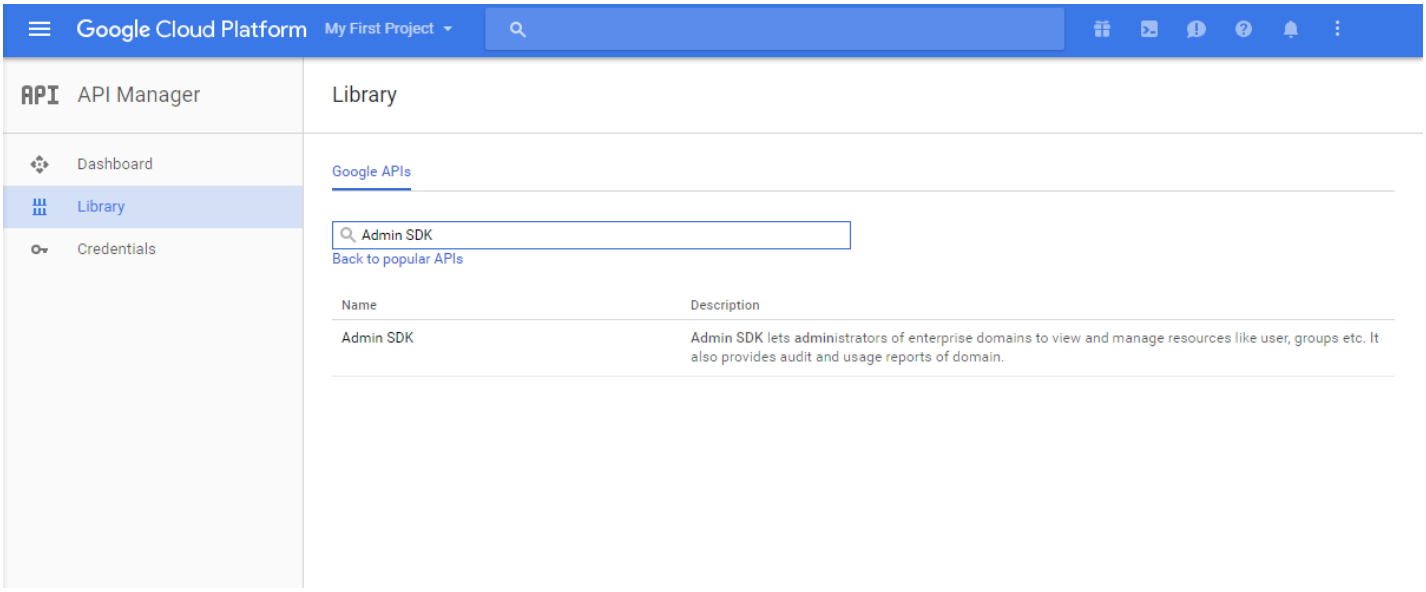
12. [**Permissions**] ページで [**Service accounts**] をクリックし、サービスアカウントの [**Options**] の下で、 [**View Client ID**] をクリックします。



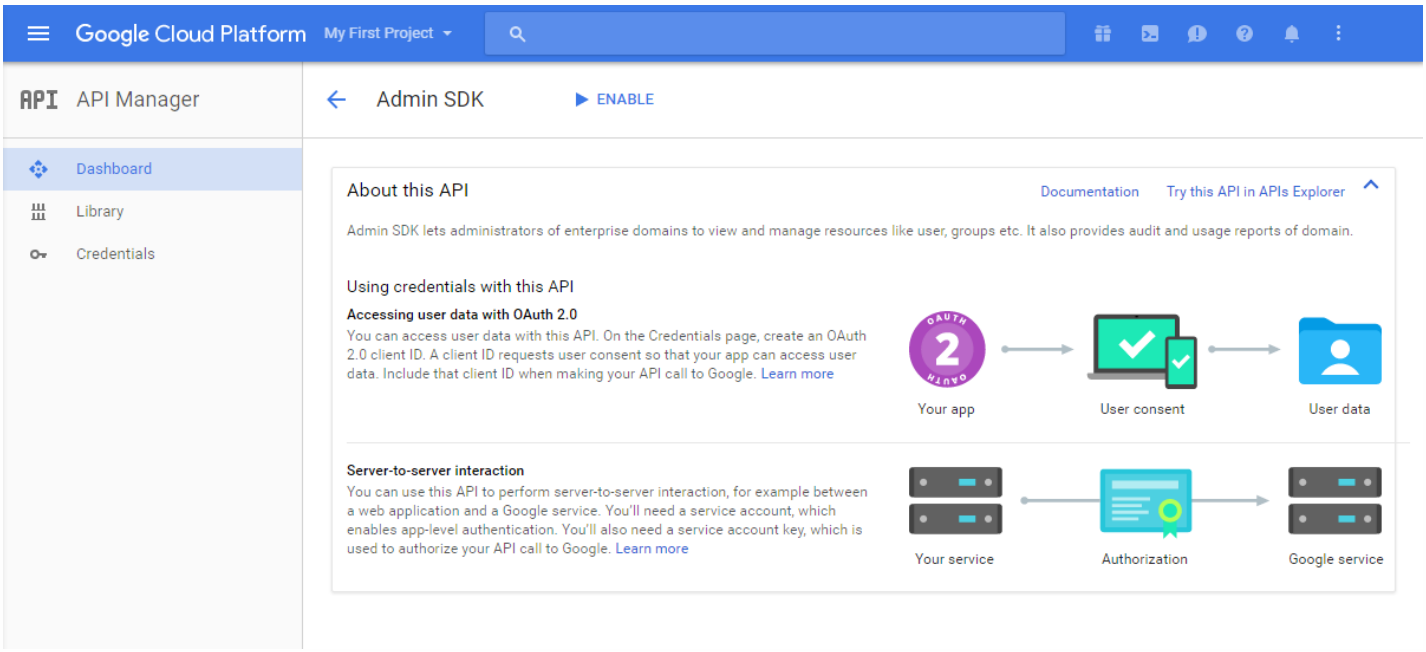
13. Google管理コンソールでアカウントの承認に必要になる詳細情報が表示されます。[**Client ID**] と [**Service account ID**] を、後でこの情報を引き出せる場所にコピーします。この情報は、ドメイン名と共に、ホワイトリスト作成の目的でCitrixサポートに送信するときに必要になります。



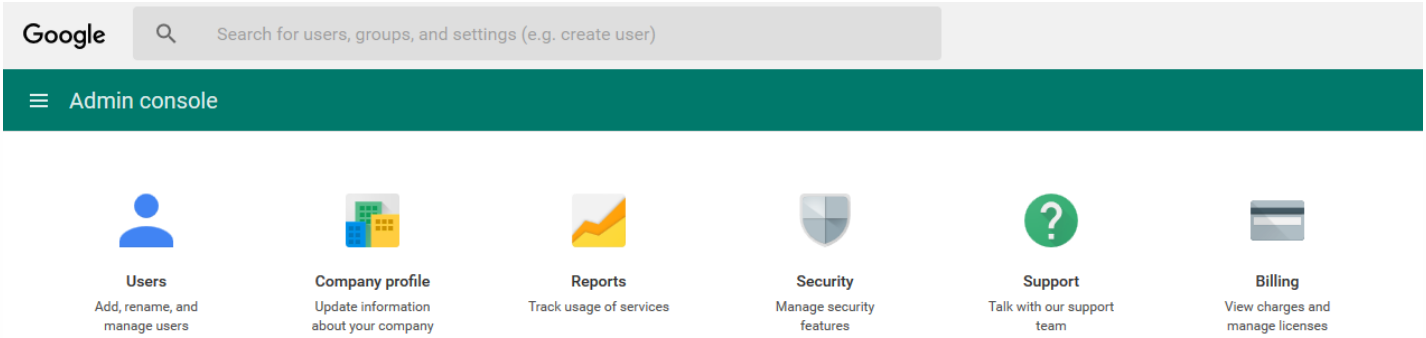
14. [**Library**] ページで**Admin SDK**を検索して、検索結果をクリックします。



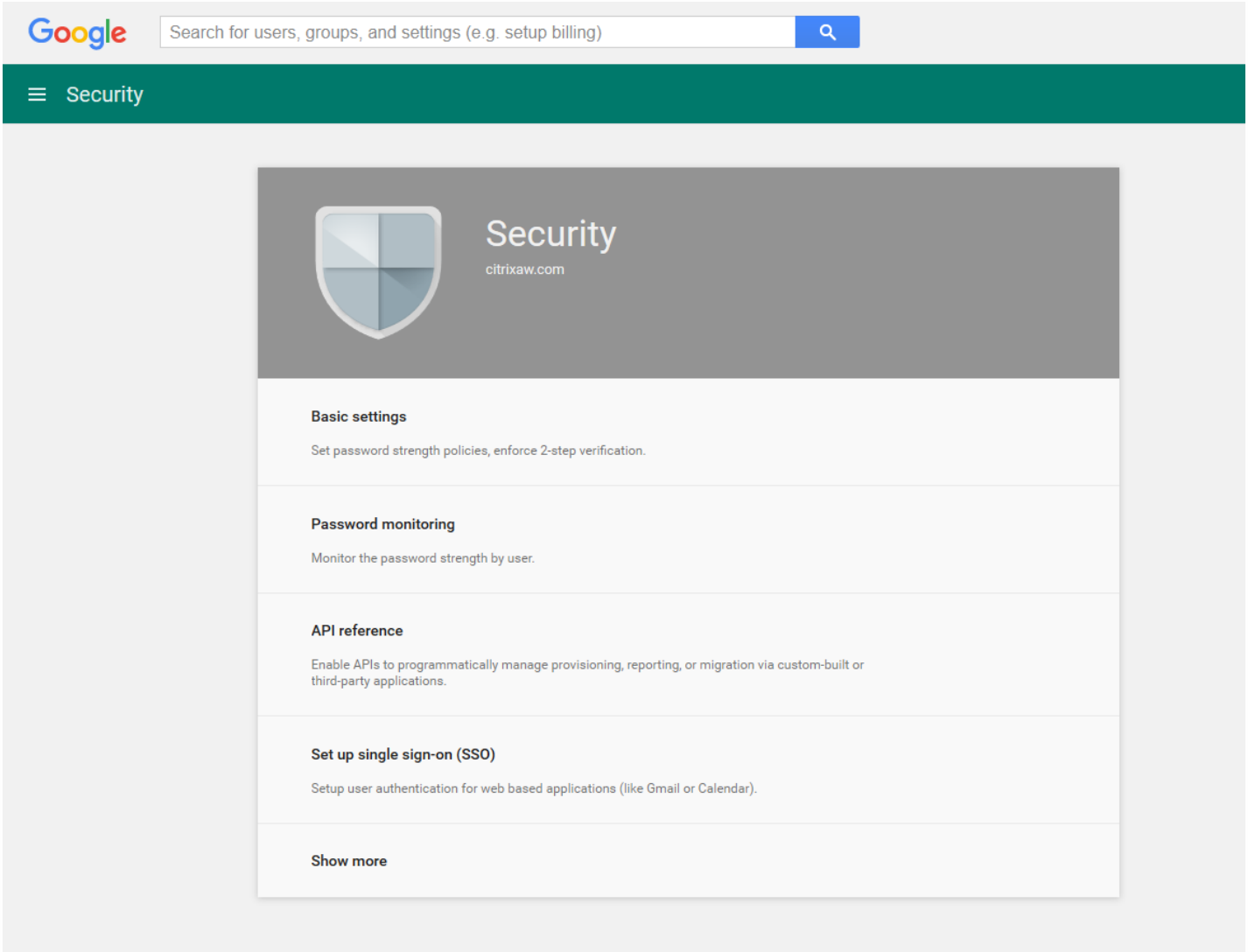
15. **[Overview]** ページで、 **[Enable]** をクリックします。

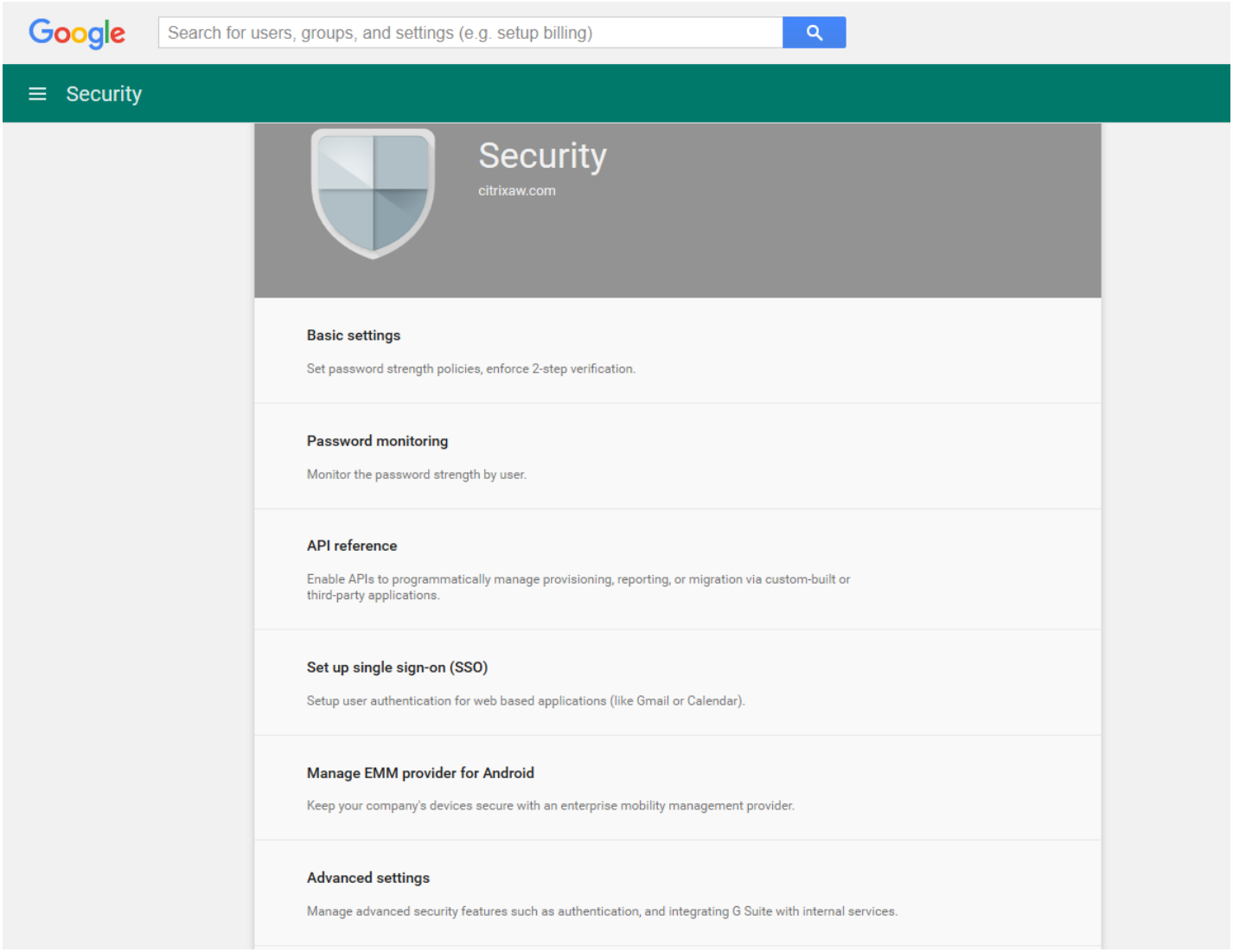


16. ユーザーのドメインのGoogle管理コンソールを開き、 **[Security]** をクリックします。

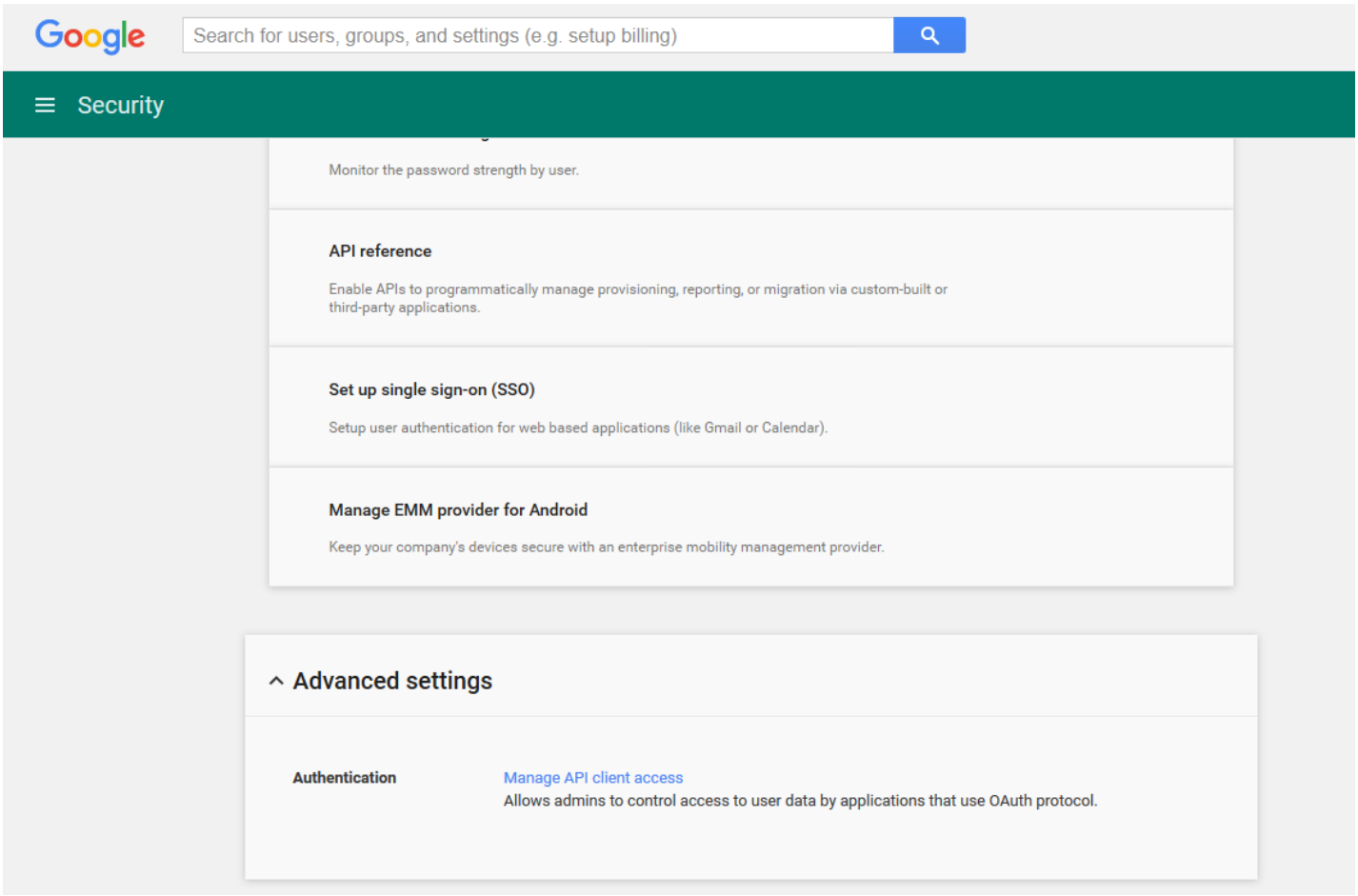


17. **[Settings]** ページで **[Show more]** をクリックして、 **[Advanced settings]** を選択します。

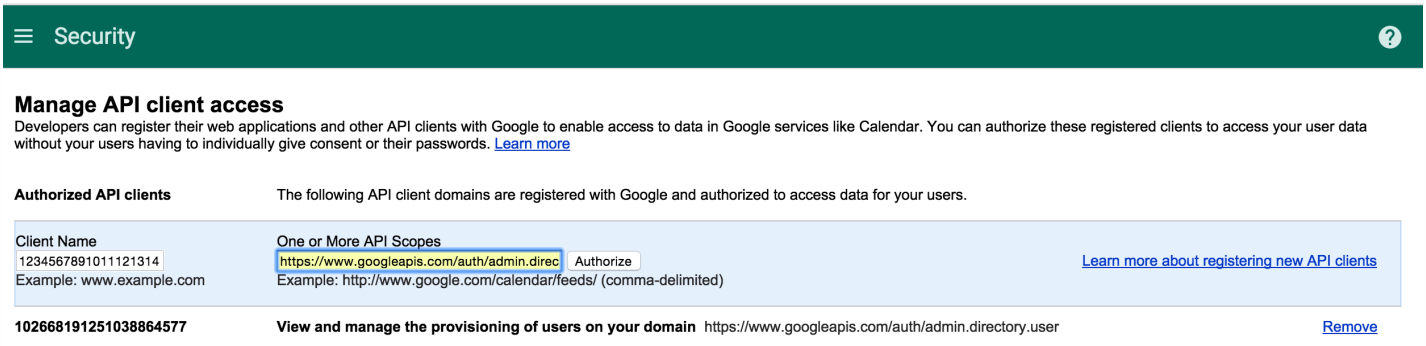




18. **[Manage API client access]** をクリックします。



19. **[Client Name]** ボックスに前の手順で保存したクライアントIDを入力し、**[One or More API Scopes]** ボックスに「https://www.googleapis.com/auth/admin.directory.user」と入力して、 **[Authorize]** をクリックします。



EMMへのバインド

XenMobileを使用してAndroidデバイスを管理するには、Citrixテクニカルサポートにドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。CitrixはトークンをEMM（エンタープライズモビリティ管理）プロバイダーとしてのXenMobileにバインドします。Citrixテクニカルサポートへのお問い合わせは、Citrixテクニカルサポートを参照してください。

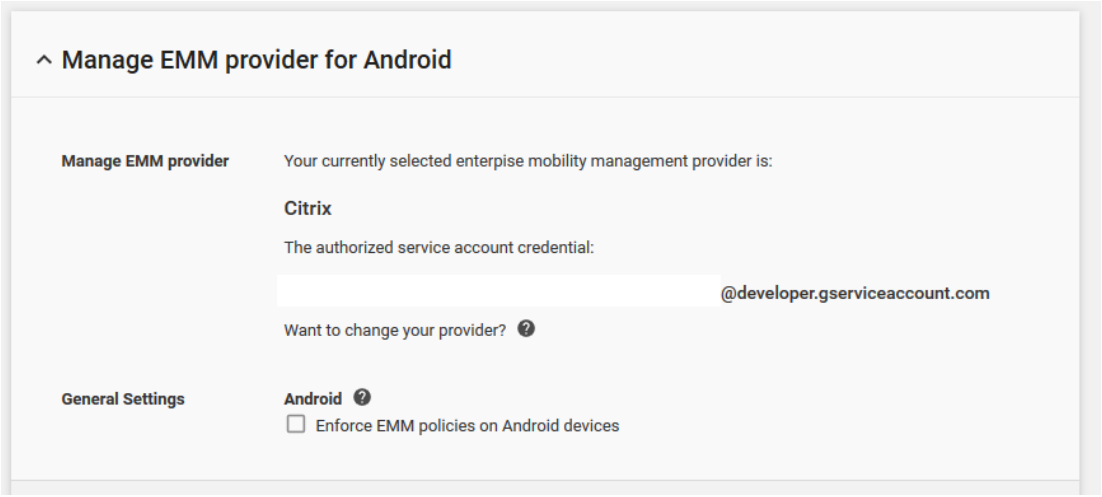
1. バインドを確認するには、Google Adminポータルにサインインして**[Security]** をクリックします。

2. **[Manage EMM provider for Android]** をクリックします。

Google Android at 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コンソールを使用してAndroidデバイスの管理を開始できます。手順14で生成したP12証明書をインポートします。Android at 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 at Workデバイスポリシーを

定義する必要があります。

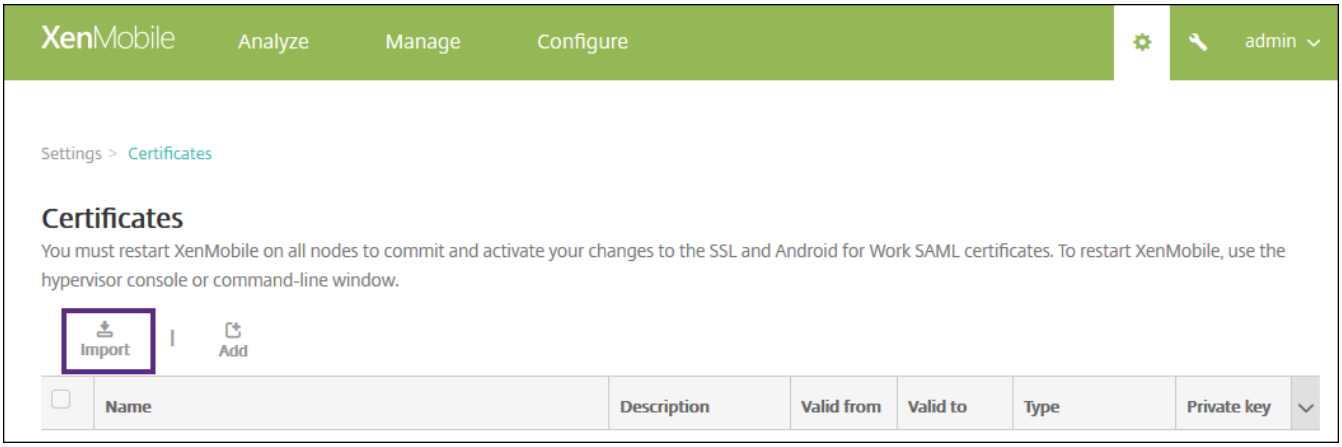


P12証明書のインポート

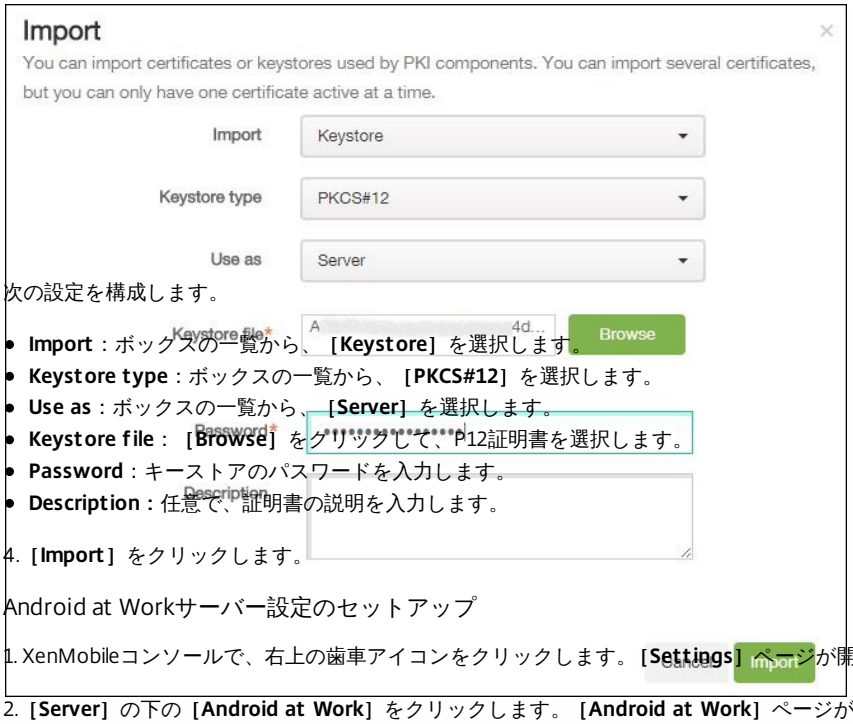
以下の手順に従ってAndroid at WorkのP12証明書をインポートします。

1. XenMobileコンソールにサインインします。

2. コンソールの右上にある歯車アイコンをクリックして[**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。



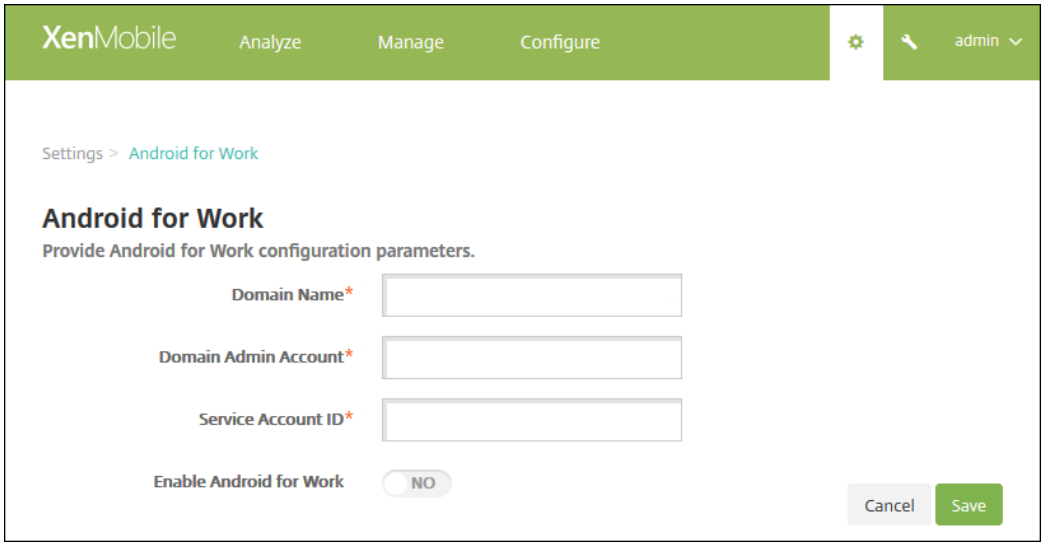
次の設定を構成します。

- **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。

Android at Workサーバー設定のセットアップ

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



次の設定を構成します。

- **Domain name**：Android at 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 at Work**：クリックして、Android at Workを有効または無効にします。

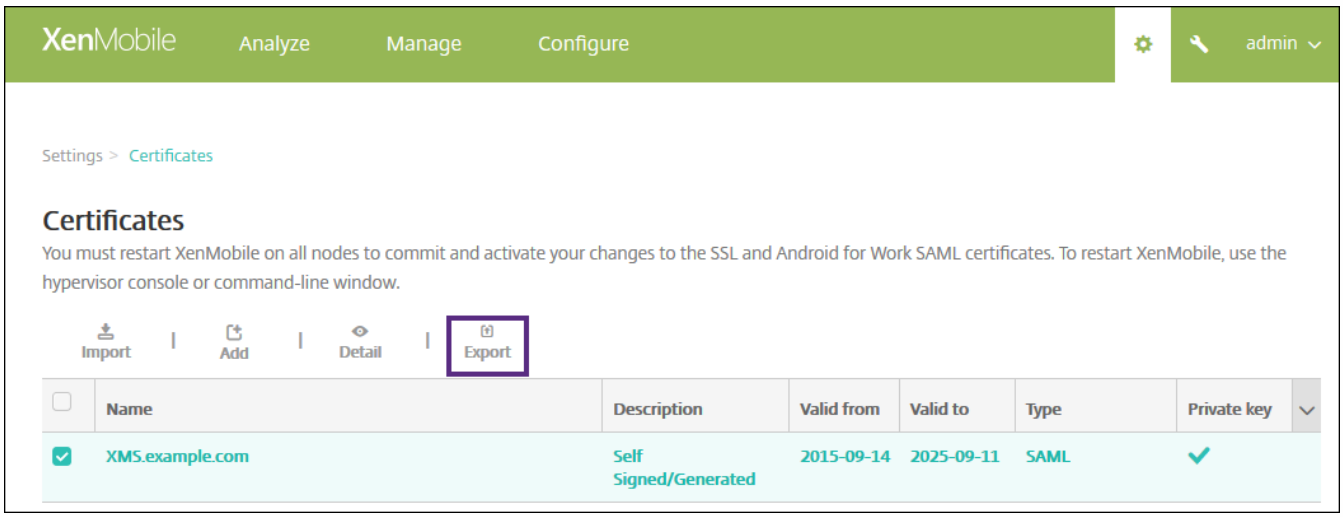
3. ［**Save**］をクリックします。

SAMLベースのシングルサインオンの有効化

1. XenMobileコンソールにサインインします。

2. コンソールの右上にある歯車アイコンをクリックします。**[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。

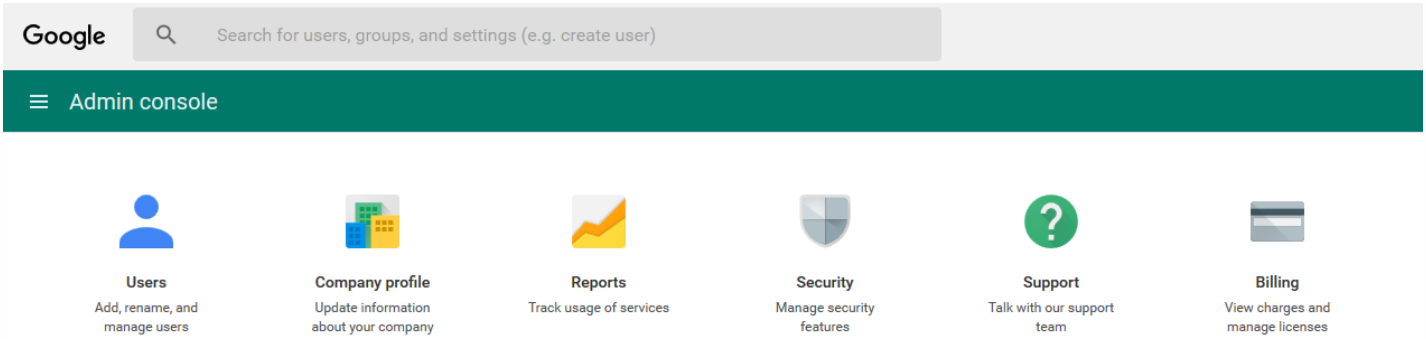


3. 証明書の一覧から、SAML証明書を選択します。

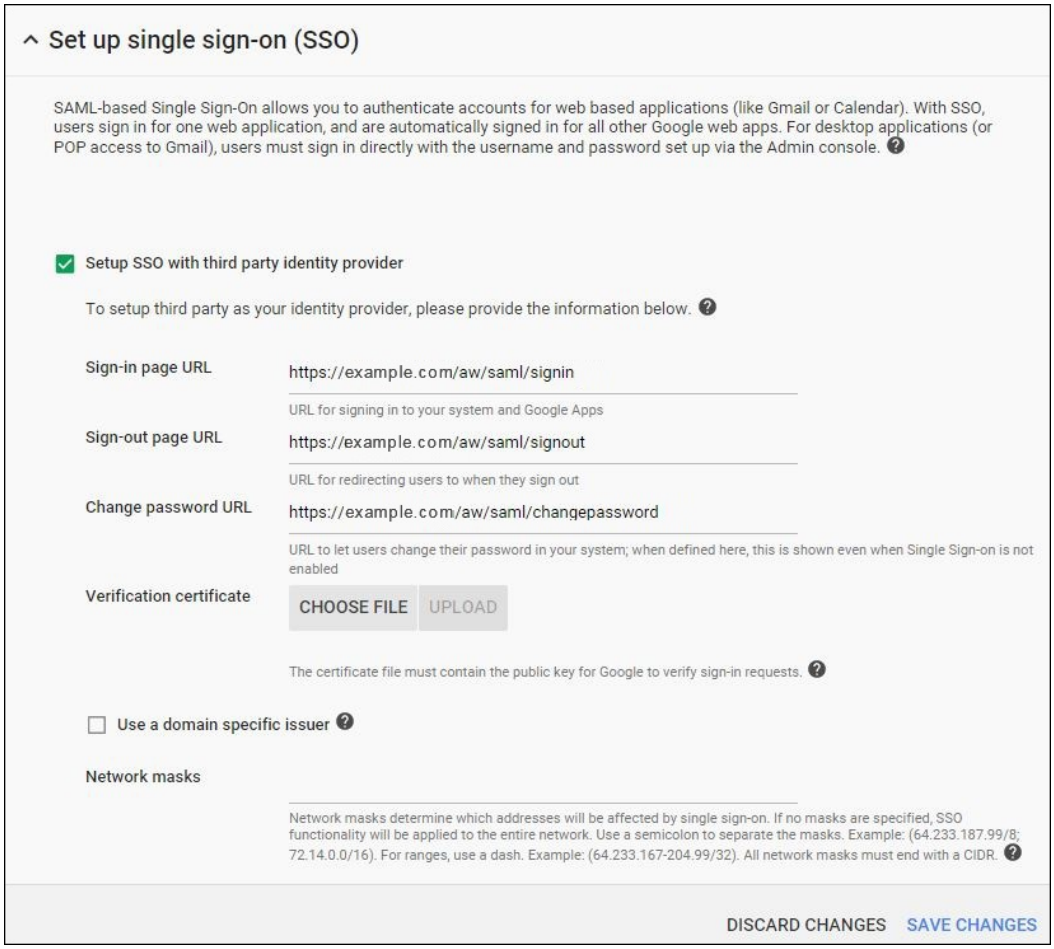
4. **[Export]** をクリックして証明書をコンピューターに保存します。

5. Android at Workの管理者資格情報でGoogle Adminポータルにサインインします。ポータルへのアクセスについて詳しくは,Google Admin portalを参照してください。

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。

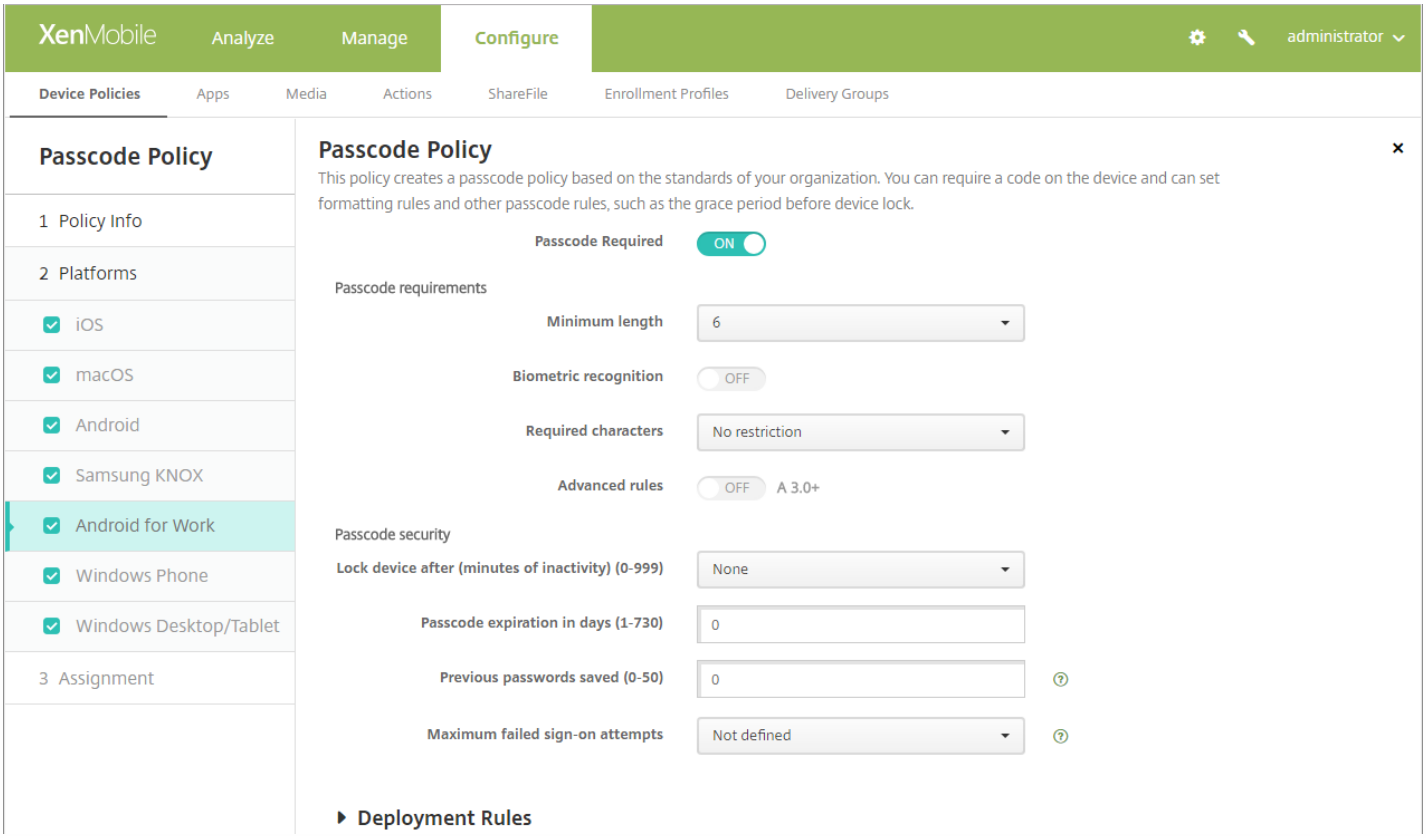


- **Sign-in page URL**：お使いのシステムおよびGoogle Appsにサインインするユーザーのためのを入力します。例：https:///aw/saml/signin。
- **Sign-out page URL**：ユーザーがサインアウト時にリダイレクトされるURLを入力します。例：https:///aw/saml/signout
- **Change password URL**：ユーザーがシステム内でパスワードを変更するときにアクセスするURLを入力します。例：https:///aw/saml/changepassword。このフィールドが定義されると、SSOが使用できない場合でもこのメッセージが表示されます。
- **Verification certificate**：**[CHOOSE FILE]**をクリックして、XenMobileからエクスポートされたSAML証明書を選択します。

8. **[SAVE CHANGES]**をクリックします。

Android at Workデバイスポリシーのセットアップ

パスコードポリシーをセットアップして、ユーザーが初めて登録するときにデバイスでのパスコード設定を必須に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コンソールにサインオンします。

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 at 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。

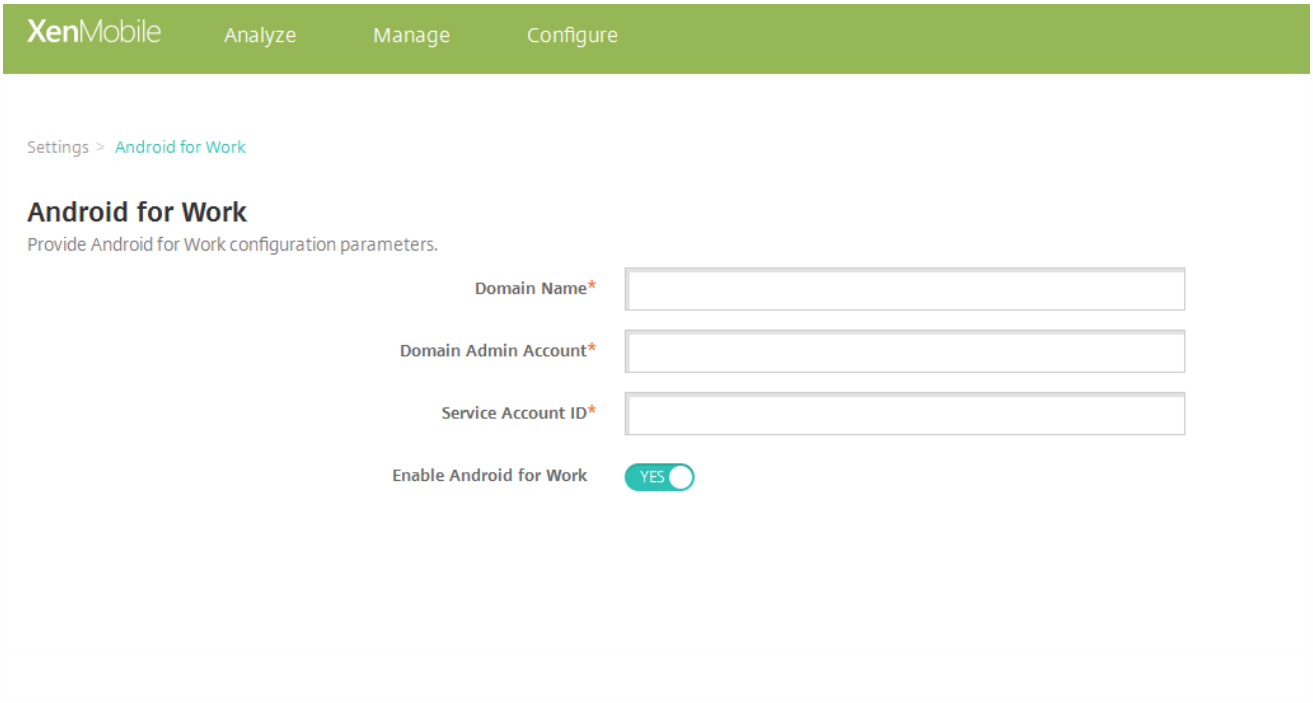
Android for Workで使用できるその他のデバイスポリシーの設定について詳しくは、「プラットフォーム別のXenMobileデバイスポリシー」を参照してください。

Android at Workアカウント設定の構成

ユーザーのデバイスでAndroidのアプリとポリシーを管理できるようにするには、XenMobileでAndroid at 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。最初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 at Workの設定を完了しておく必要があります。

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックします。**[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 at Workでのデバイス所有者モードのプロビジョニング

デバイス所有者モードでAndroid at Workをプロビジョニングする場合、2つのデバイス間でNFC（Near-Field Communications；近距離無線通信）バンプを使用してデータを転送する必要があります。一方のデバイスでXenMobile Provisioning Toolを実行して、もう一方のデバイスを工場出荷時設定に復元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使用する通信プロトコルはNFCのみです。

前提条件

- Android at Workを有効にしたXenMobile Serverバージョン10.4。
- デバイス所有者モードでAndroid at 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。この前提条件を完了する手順については、後述します。
- 構成済みのProvisioning Toolを実行している、NFC機能が備わった別のデバイス。Provisioning Toolは、Secure Hub 10.4またはCitrixダウンロードページから入手できます。

各デバイスにはエンタープライズモビリティ管理（EMM）アプリで管理されたAndroid at Workプロファイルが1つのみ存在します。XenMobileで、Secure HubはEMMアプリです。各デバイスには、1つのプロファイルしか許可されません。2つ目のEMMアプリを追加すると、1つ目のEMMアプリが削除されます。

デバイス所有者モードは、新しいデバイスまたは工場出荷時の設定にリセットされたデバイスで開始できます。XenMobileでデバイス全体を管理します。

デバイス所有者モードでのNFCバンプ

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 at Workを初期化する必要があります。

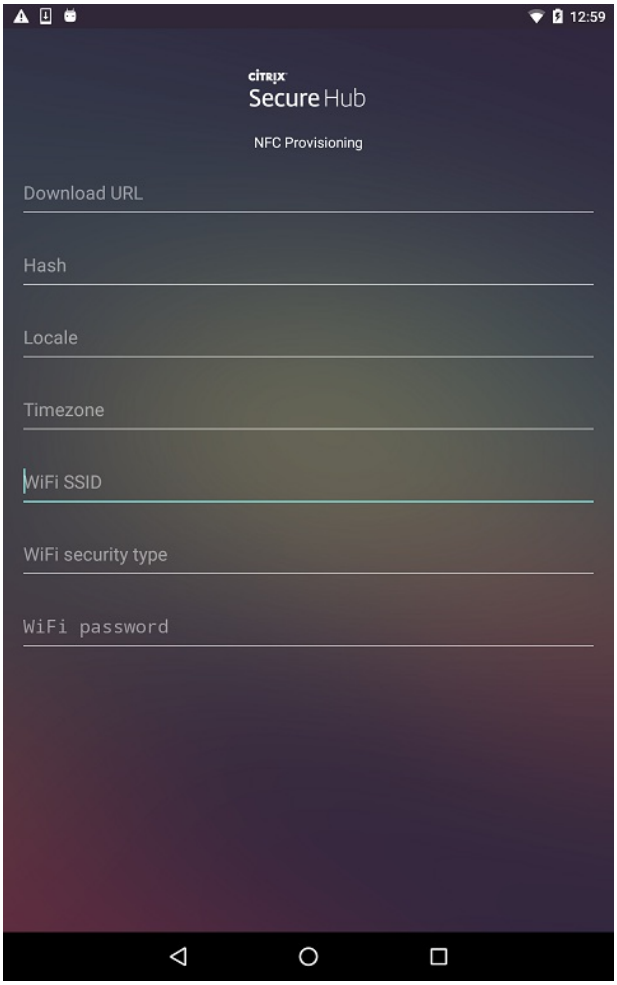
- デバイス所有者として機能するEMMプロバイダーアプリ（この場合は、Secure Hub）のパッケージ名。
- デバイスがEMMプロバイダーアプリをダウンロードできるイントラネット/インターネット上の場所。

- ダウンロードが正常に完了したかどうかを確認するEMMプロバイダーアプリのSHA1ハッシュ。
- 工場出荷時の設定にリセットされたデバイスがEMMプロバイダーアプリに接続してダウンロードできるようにするWi-Fi 接続の詳細。注：現時点では、Androidはこの手順での802.1x Wi-Fiをサポートしていません。
- デバイスのタイムゾーン（オプション）。
- デバイスの地理的な場所（オプション）。

２つのデバイスがバンプされると、Provisioning Toolのデータが工場出荷時の設定にリセットされたデバイスに送信されます。このデータはその後、管理者設定でのSecure Hubのダウンロードに使用されます。タイムゾーンと場所の値を入力しない場合、新しいデバイスではAndroidによって自動的にこれらの値が構成されます。

XenMobile Provisioning Toolの構成

NFCバンプを行う前に、Provisioning Toolを構成する必要があります。この構成はその後、工場出荷時の設定にリセットされたデバイスに、NFCバンプ中に転送されます。



必須項目にデータを直接入力することも、テキストファイルから入力することもできます。次の手順では、テキストファイルを構成する方法と各フィールドに説明を含める方法について説明します。入力後のデータはアプリでは保存されないため、テキストファイルを作成して、今後の使用に備えて情報を保存しておくことをお勧めします。

テキストファイルを使用してProvisioning Toolを構成するには

ファイルの名前をnfcprovisioning.txtにして、/sdcard/フォルダーにあるデバイスのSDカードに格納します。アプリによってこのテキストファイルが読み込まれ、値が入力されます

テキストファイルには、次のデータを含める必要があります。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
この行は、EMMプロバイダーアプリのイントラネット/インターネットの場所です。工場出荷時設定のデバイスがNFCバンプの後にWi-Fiに接続した場合、デバイスはダウンロードのためにこの場所にアクセスする必要があります。URLは通常のURLで、特別な形式にする必要はありません。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=
この行は、EMMプロバイダーアプリのチェックサムです。このチェックサムはダウンロードが成功したかを検証するために使用されます。チェックサムを取得する手順については、後述します。

android.app.extra.PROVISIONING_WIFI_SSID=
この行は、Provisioning Toolを実行しているデバイスが接続されているWi-FiのSSIDです。

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
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、このフィールドを空白にする必要があります。

android.app.extra.PROVISIONING_LOCALE=
言語コードおよび国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で2文字のISO言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で2文字のISO国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en_US」と入力します。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=
これはデバイスが実行されているタイムゾーンです。フォームの地域/場所のOlson名を入力します。たとえば、米国太平洋標準時の場合は「America/Los_Angeles」です。名前を入力しない場合、タイムゾーンは自動的に入力されます。

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
このデータは必要ありません。値はSecure Hubとしてアプリにハードコードされます。ここでは、情報の完全性を守るためだけに記載しています。

WPA2を使用して保護されたWi-Fiの場合、完了した**nfcprovisioning.txt**ファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

保護されていないWi-Fiの場合、完了したnfcprovisioning.txtファイルは以下の例のようになります。

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d
```

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

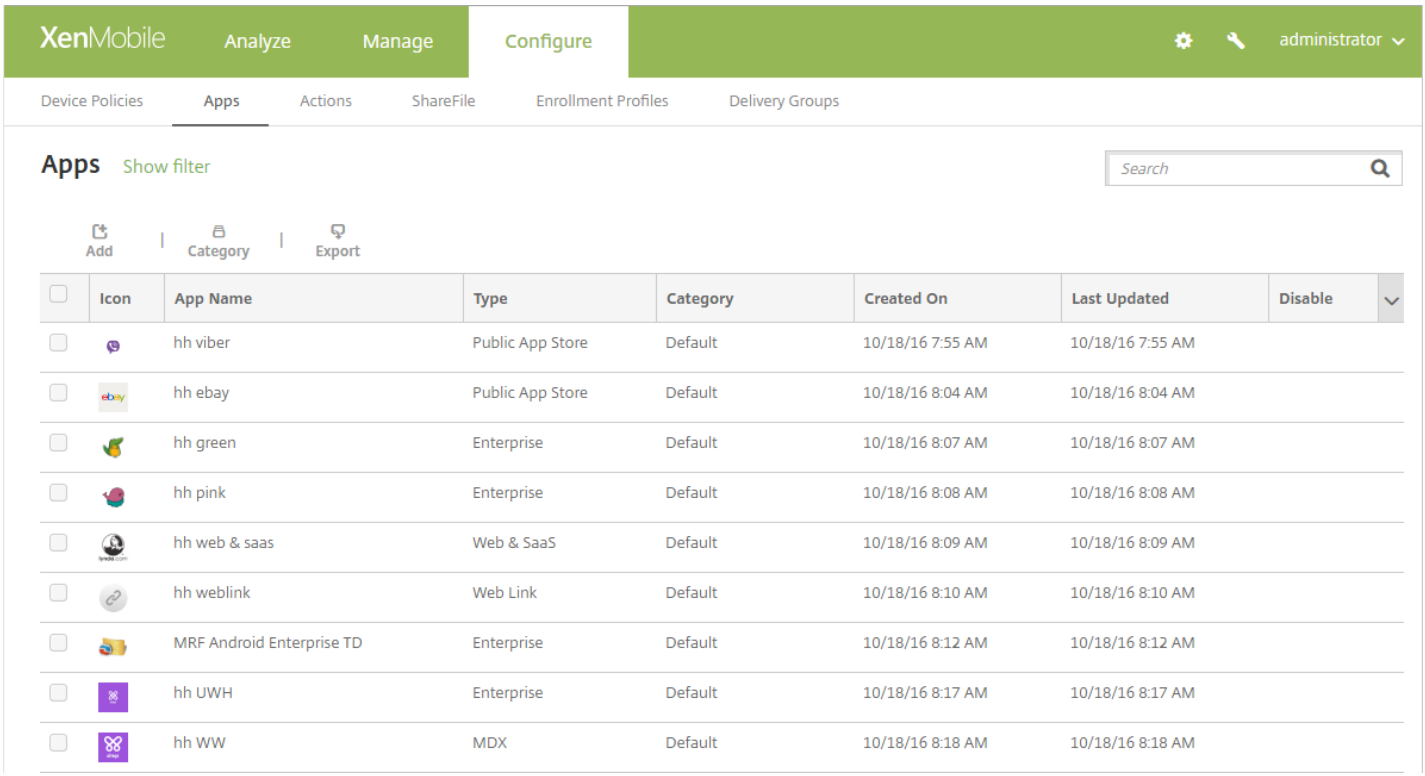
android.app.extra.PROVISIONING_LOCALE=en_US

android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles

Secure Hubチェックサムを取得するには

アプリのチェックサムを取得するには、そのアプリをエンタープライズアプリとして追加します。

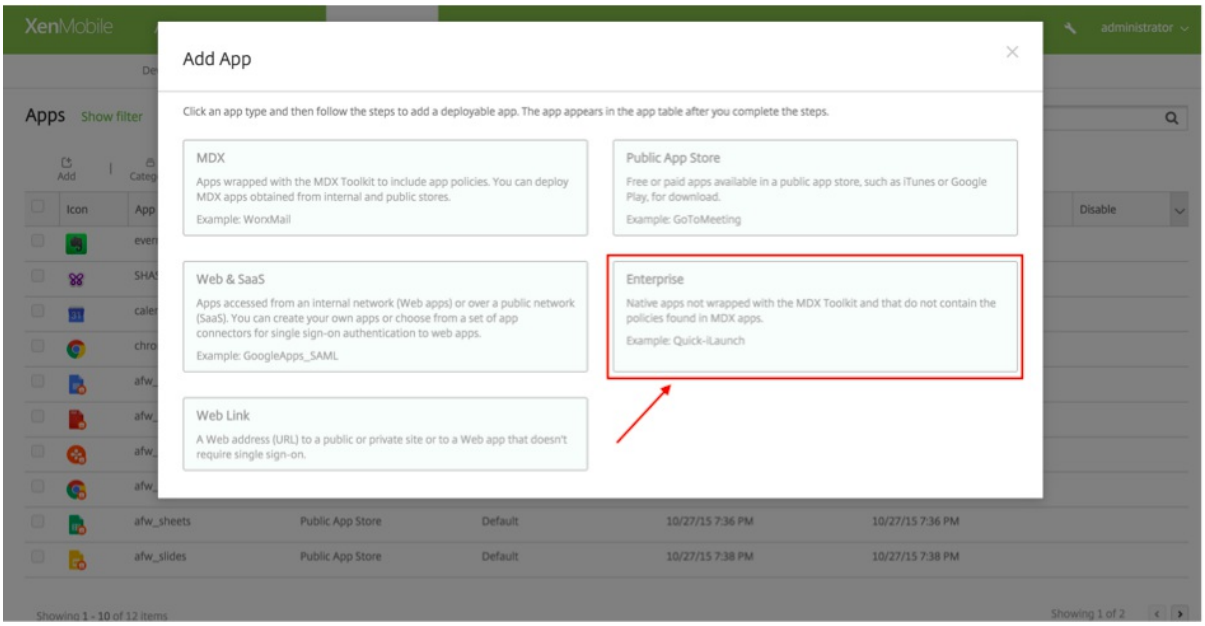
1. XenMobileコンソールで、**[構成] > [アプリ]** と移動して、**[追加]** をクリックします。



[アプリの追加] ウィンドウが開きます。

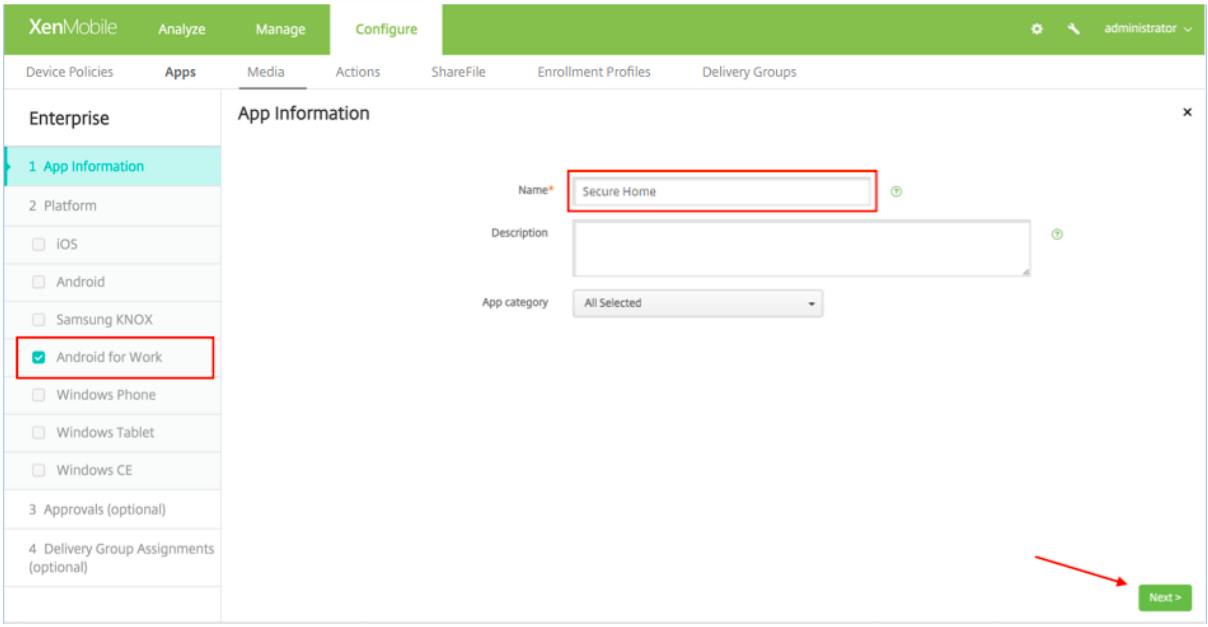
2. **[Enterprise]** をクリックします。

[App Information] ページが開きます。



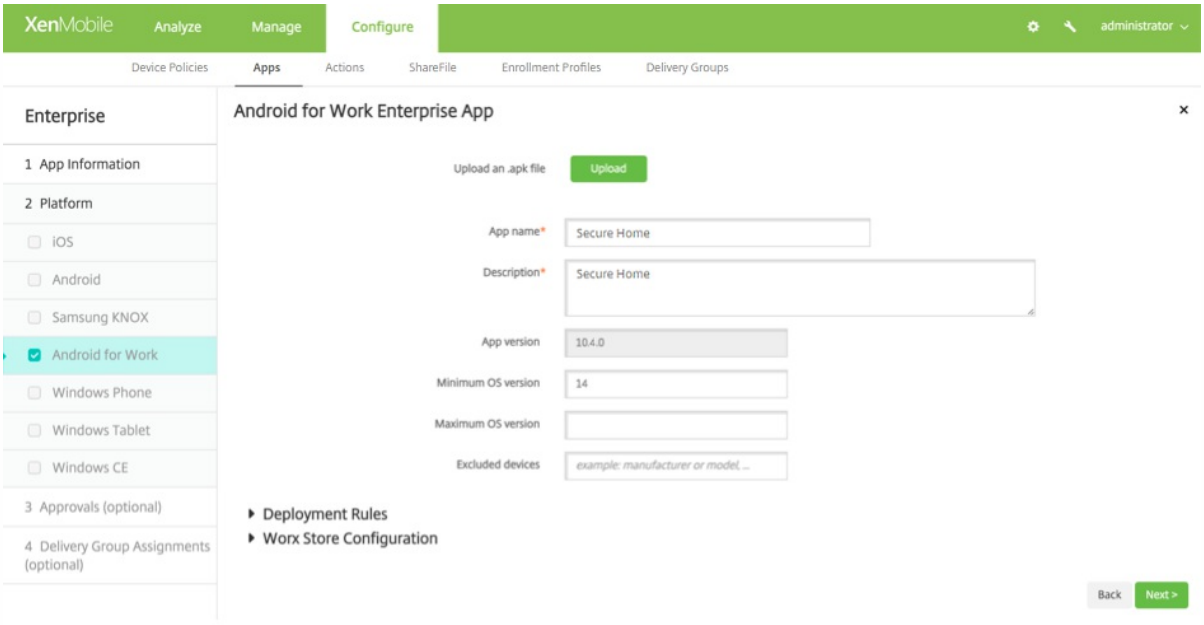
3. 次の構成を選択して［**次へ**］をクリックします。

［**Android for Work Enterprise App**］画面が開きます。

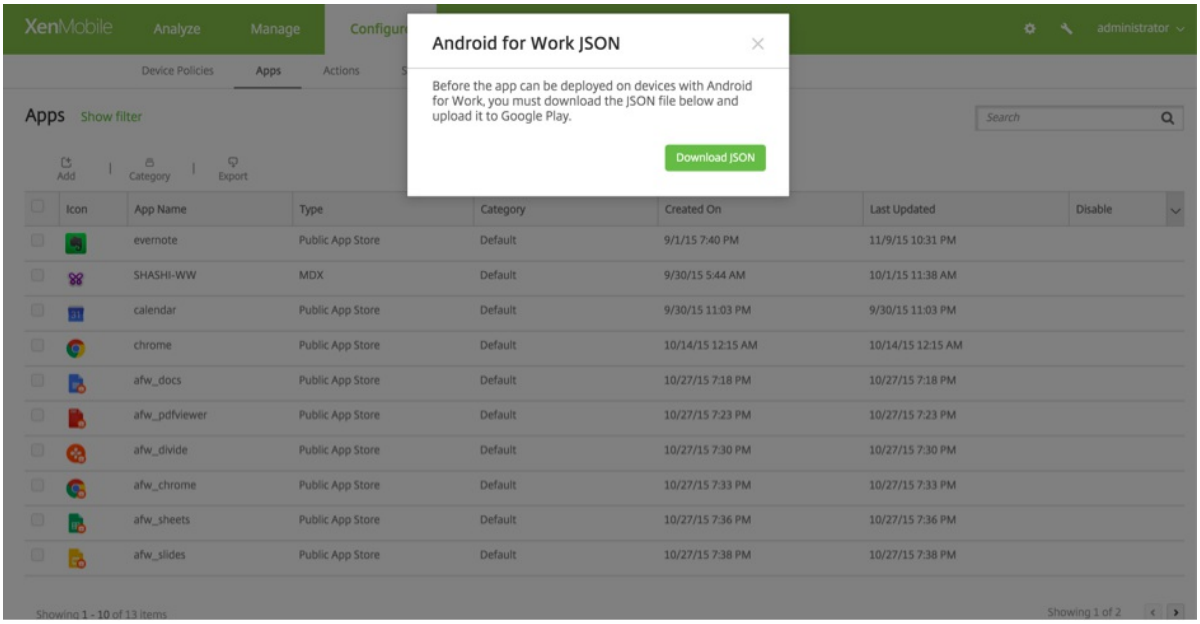


4. .apkへのパスを入力し、［**Next**］をクリックしてファイルをアップロードします。

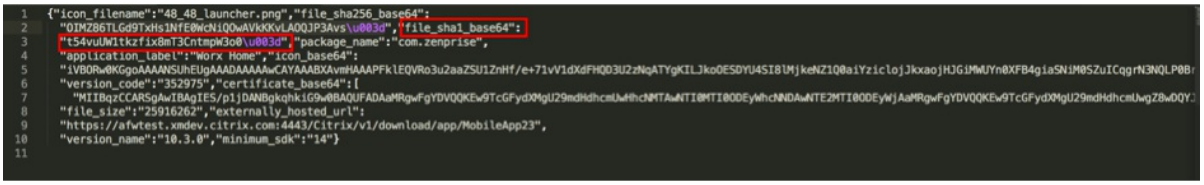
アップロードが完了すると、アップロードされたパッケージの詳細が表示されます。



5. **[Next]** をクリックしてJSONファイルをダウンロードするページを表示します。このファイルは、この後Google Playへのアップロードに使用します。Secure Hubの場合、Google Playにアップロードする必要はありませんが、SHA1を読み込む元になるJSONファイルが必要です。



以下の図に、典型的なJSONファイルの例を示します。



6.**file_sha1_base64**の値をコピーして、この値をProvisioning Toolの **[Hash]** 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、URIの安全性は入力者の責任になります。

使用するライブラリ

Provisioning Toolでは、以下のライブラリがソースコードに使用されています。

- v7 appcompatライブラリ：Google（Apache license 2.0）
- Design support library：Google（Apache license 2.0）
- v7 paletteライブラリ：Google（Apache license 2.0）
- Butter Knife：Jake Wharton（Apache license 2.0）

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

Samsung KNOX

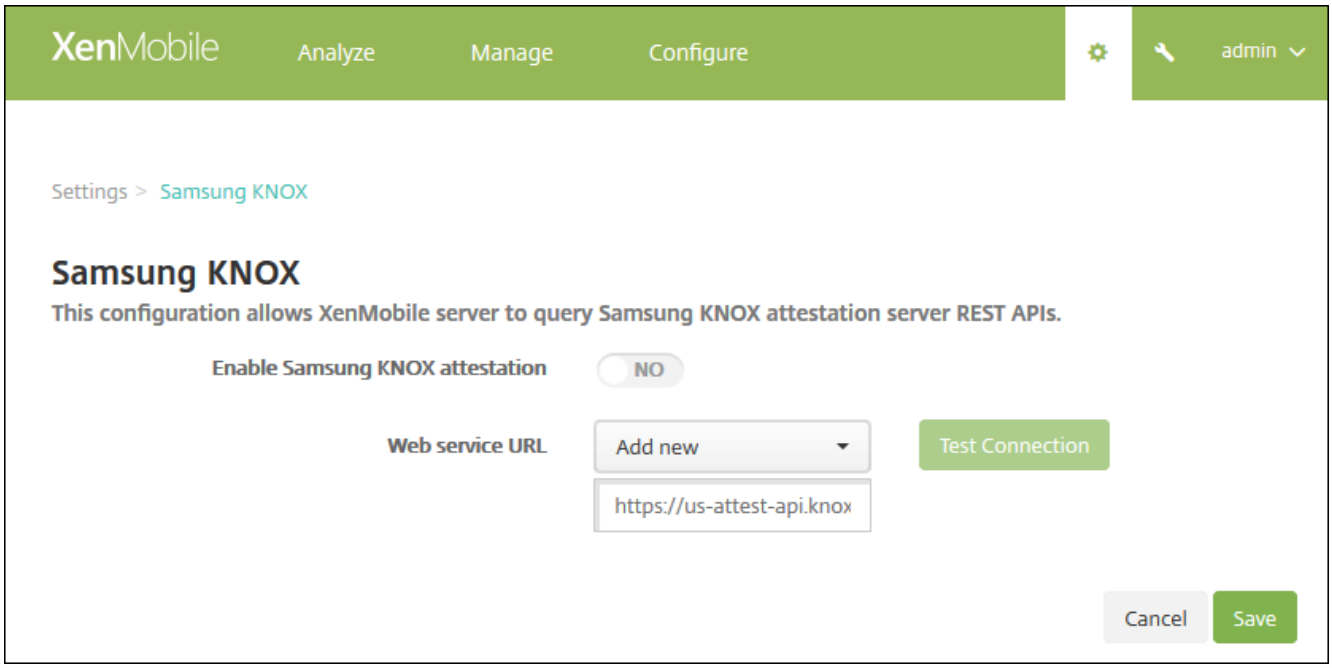
Feb 27, 2017

XenMobileを構成して、Samsung KNOX認証サーバーREST APIに対するクエリを実行できます。

Samsung KNOXは、オペレーティングシステムとアプリケーションを複数レベルで保護する、ハードウェアセキュリティ機能を利用します。このセキュリティの1つのレベルは、認証を通じてプラットフォームに存在します。認証サーバーは、モバイルデバイスのコアシステムソフトウェア（ブートローダーおよびカーネルなど）の検証機能を備えています。検証は、信頼できる起動時に収集されたデータに基づいて実行時に行われます。

1. XenMobile Webコンソールで、右上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. **[プラットフォーム]**の**[Samsung KNOX]**をクリックします。**[Samsung KNOX]**ページが開きます。



3. **[Samsung KNOX構成証明を有効にする]**で、Samsung KNOX認証を有効にするかどうかを選択します。デフォルトは**[いいえ]**です。

4. **[Samsung KNOX構成証明を有効にする]**を**[はい]**に設定すると、**[WebサービスURL]**オプションが有効になります。一覧から、次のいずれかを選択します。

   a. 適切な認証サーバーを選択します。

   b. **[新規追加]**を選択して、WebサービスURLを入力します。

5. **[接続のテスト]**をクリックして、接続を検証します。成功、または失敗のメッセージが表示されます。

6. **[保存]**をクリックします。

> ## 注意
>
> Samsung KNOX Mobile Enrollmentを使用すると、複数のSamsung KNOXデバイスを手動で構成することなく、XenMobile（または、

その他のモバイルデバイスマネージャー）に各デバイスを登録できるようになります。詳しくは、「Samsung KNOX Bulk Enrollment」を参照してください。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

デバイスポリシー

Jul 13, 2017

ポリシーを作成して、XenMobileとデバイスの連携方法を構成できます。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、プラットフォーム間で異なる場合や、Androidデバイスの製造元によっても違いがある場合があります。

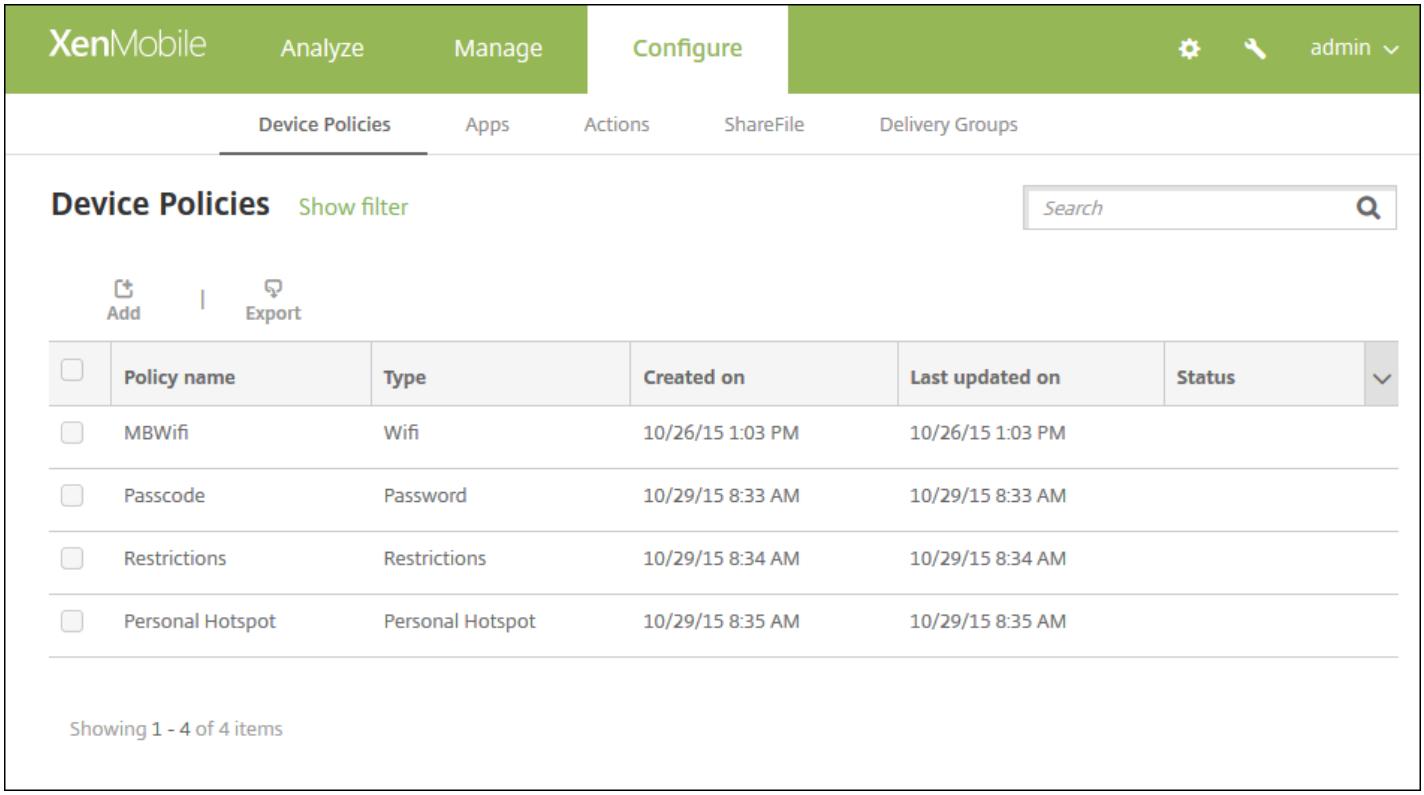
プラットフォーム別ポリシーのマトリックスについては、「Device Policies by Platform Matrix PDF」を参照してください。各デバイスポリシーの概要説明については、この記事の「デバイスポリシーの概要」を参照してください。

> ## Important
>
> ポリシーを作成する前に、以下の要件を満たしてください。
>
> - 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のポリシーを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

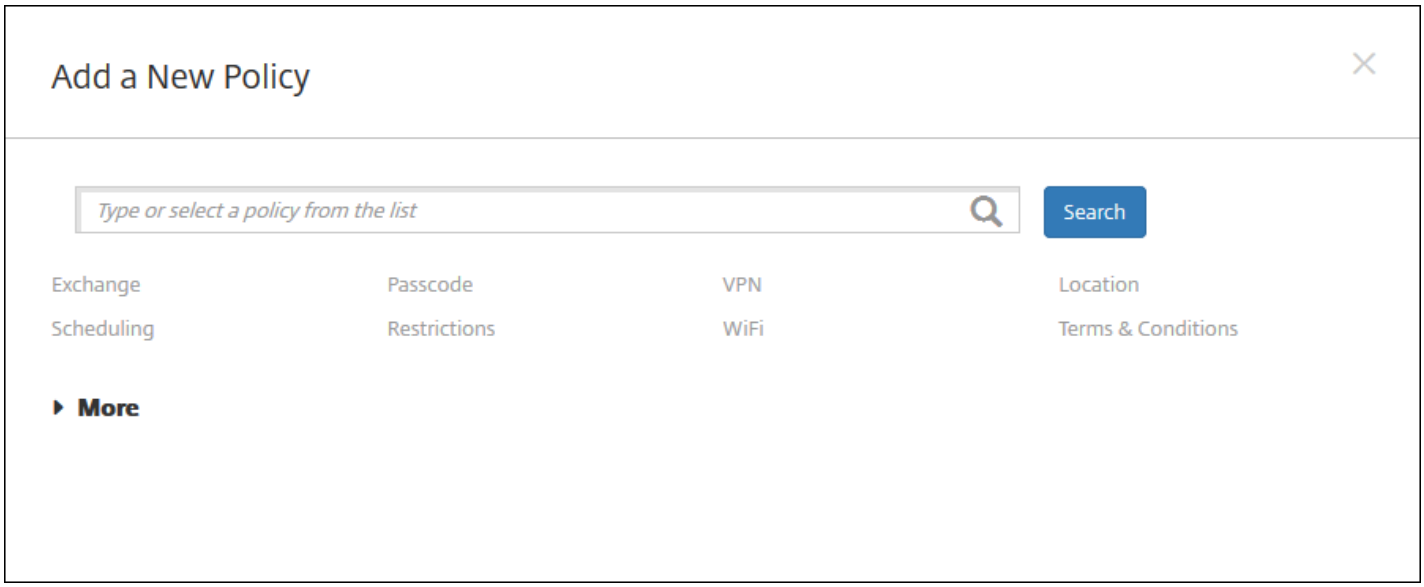
デバイスポリシーを作成し、管理するには、**[構成] > [デバイスポリシー]** の順に選択します。



デバイスポリシーの追加

1. **[デバイスポリシー]** ページで、 **[追加]** をクリックします。

[新しいポリシーの追加] ダイアログボックスが開きます。 **[詳細]** を展開してさらにポリシーを表示します。

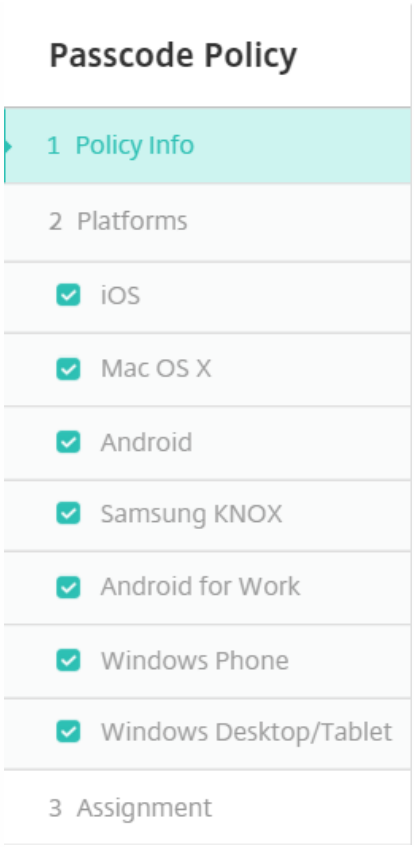


2. 追加するポリシーを検索するには、次のいずれかを実行します。

- ポリシーをクリックします。
  選択したポリシーの［**ポリシー情報**］ページが開きます。
- 検索ボックスにポリシー名を入力します。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。その結果、選択したポリシーのみが残ります。それをクリックして、そのポリシーの［**ポリシー情報**］ページを開きます。
  選択したポリシーが［**詳細**］領域の中にある場合、［**詳細**］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： 一覧に表示されるのは、ポリシーでサポートされるプラットフォームのみです。



4. **[ポリシー情報]** ページで必要な情報を入力して、**[次へ]** をクリックします。**[ポリシー情報]** ページにはポリシー名などの情報が集約されているため、ポリシーの識別や追跡に役立ちます。このページはすべてのポリシーで類似しています。

5. プラットフォームページの入力を完了します。手順3で選択した各プラットフォームのページが開きます。これらのページはポリシーごとに異なります。ポリシーはプラットフォームによって異なる可能性があります。すべてのポリシーがすべてのプラットフォームに適用される訳ではありません。

展開規則を構成するには

注：展開規則の構成について詳しくは、「リソースの展開」を参照してください。

a. **[展開規則]** を展開して以下の設定を構成します。デフォルトでは **[基本]** タブが表示されます。

- 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは **[すべて]** です。
- **[新しい規則]** をクリックして条件を定義します。
- 一覧から **[デバイス所有権]** や **[BYOD]** などの条件を選択します。
- 条件をさらに追加する場合は、**[新しい規則]** をもう一度クリックします。必要なだけいくつでも条件を追加できます。

b. **[詳細]** タブをクリックし、ブール値オプションを使用して規則を組み合わせます。**[基本]** タブで選択した条件が表示されます。

c. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。

- **[および]**、**[または]**、または **[非]** をクリックします。
- 一覧から、規則に追加する条件を選択します。次に右側のプラス記号（+）をクリックし、規則に条件を追加します。

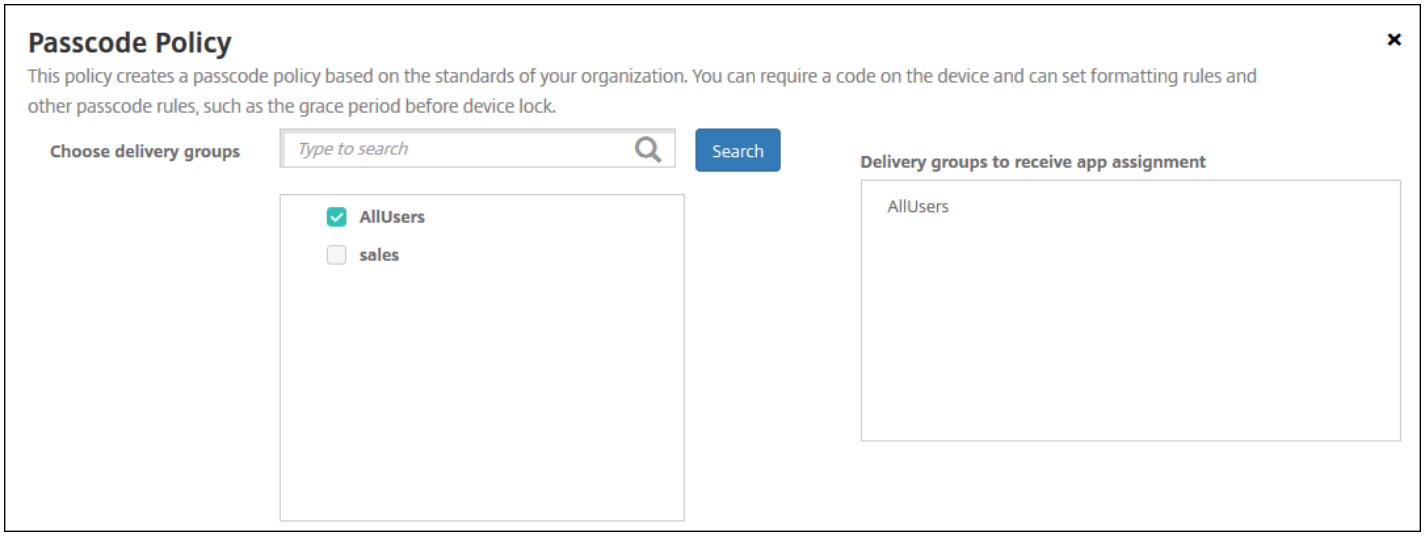
いつでも、条件をクリックして選択し、**[編集]**をクリックして条件を変更したり、**[削除]**をクリックして条件を削除したりすることができます。

- **[新しい規則]**をクリックして別の条件を追加します。

6. **[次へ]**をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、**[割り当て]**ページに移動します。

7. **[割り当て]**ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、**[アプリ割り当てを受信するためのデリバリーグループ]**ボックスにそのグループが表示されます。

注：**[アプリ割り当てを受信するためのデリバリーグループ]**ボックスは、デリバリーグループを選択するまで表示されません。

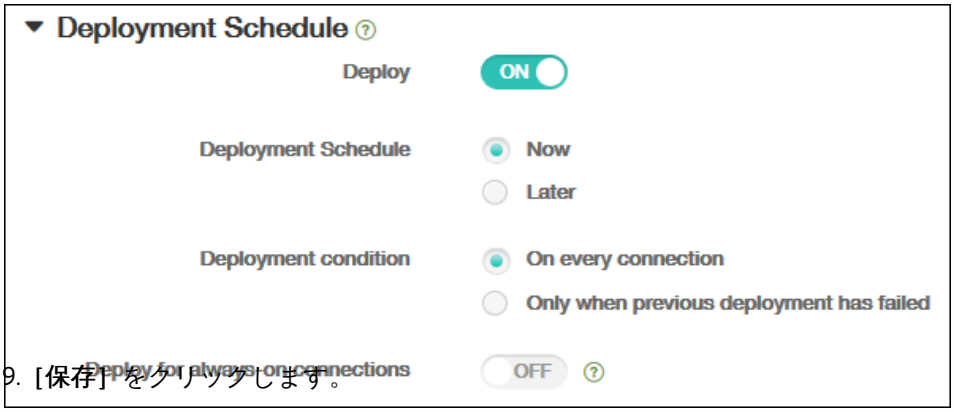


8. **[割り当て]**ページで**[展開スケジュール]**を展開して以下の設定を構成します。

- **[展開]**の横の**[オン]**をクリックすると展開がスケジュールされ、**[オフ]**をクリックすると展開が行われません。デフォルトのオプションは**[オン]**です。
- **[展開スケジュール]**の横の**[すぐに]**または**[あとで]**をクリックします。デフォルトのオプションは**[すぐに]**です。
- **[あとで]**をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]**の横の**[接続するたび]**をクリックするか、**[以前の展開が失敗した場合のみ]**をクリックします。デフォルトのオプションは、**[接続するたび]**です。
- **[常時接続に対する展開]**の横の**[オン]**または**[オフ]**をクリックします。デフォルトのオプションは**[オフ]**です。

注：

- このオプションは、**[設定]**の**[サーバープロパティ]**において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]**は適用されません。

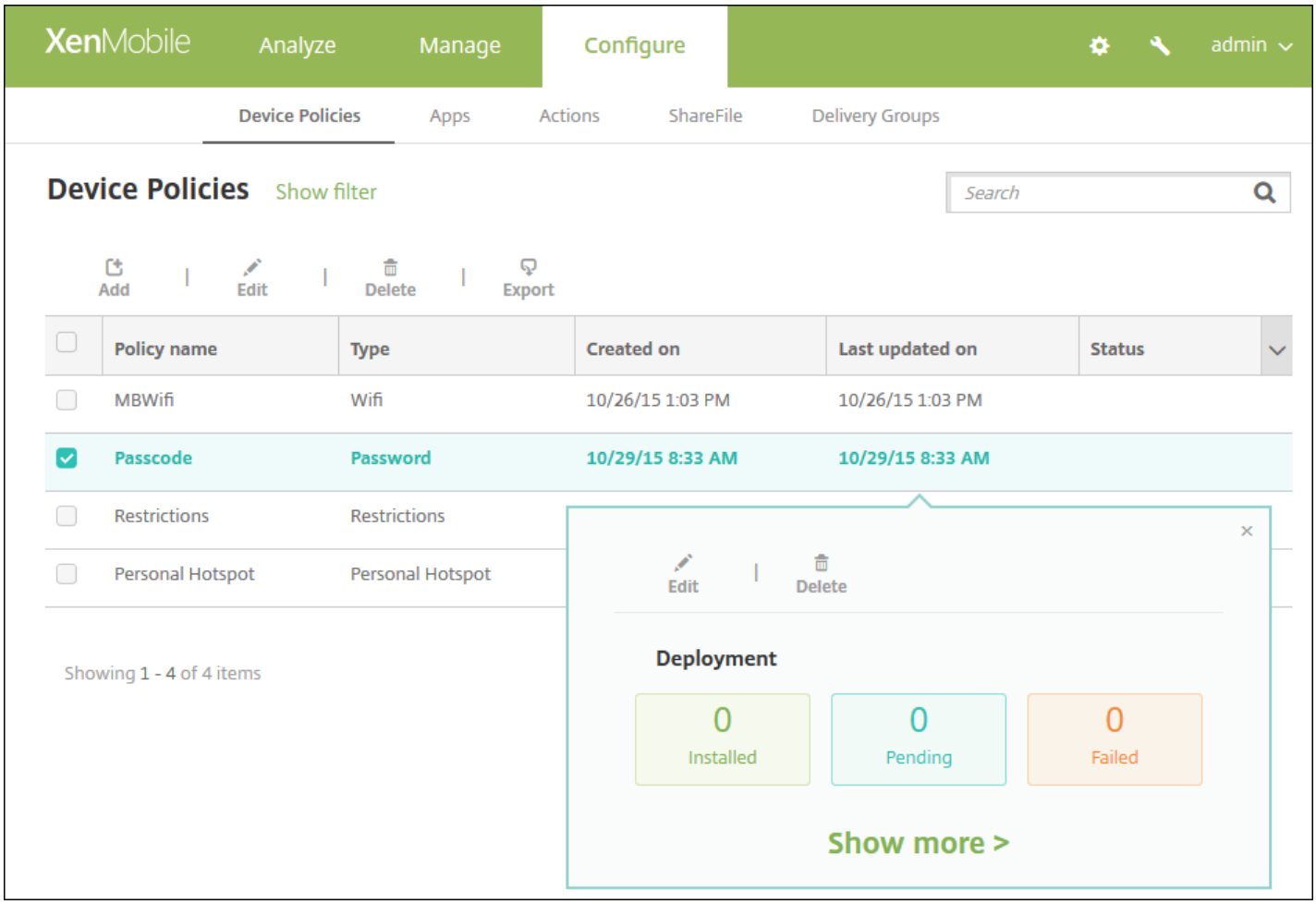


9. **[保存]** をクリックします。

ポリシーが **[デバイスポリシー]** の表に表示されます。

デバイスポリシーの編集または削除

ポリシーを編集または削除するには、ポリシーの横にあるチェックボックスをオンにして、ポリシー一覧の上にオプションメニューを表示します。または、一覧でポリシーをクリックして、その項目の右にオプションメニューを表示します。



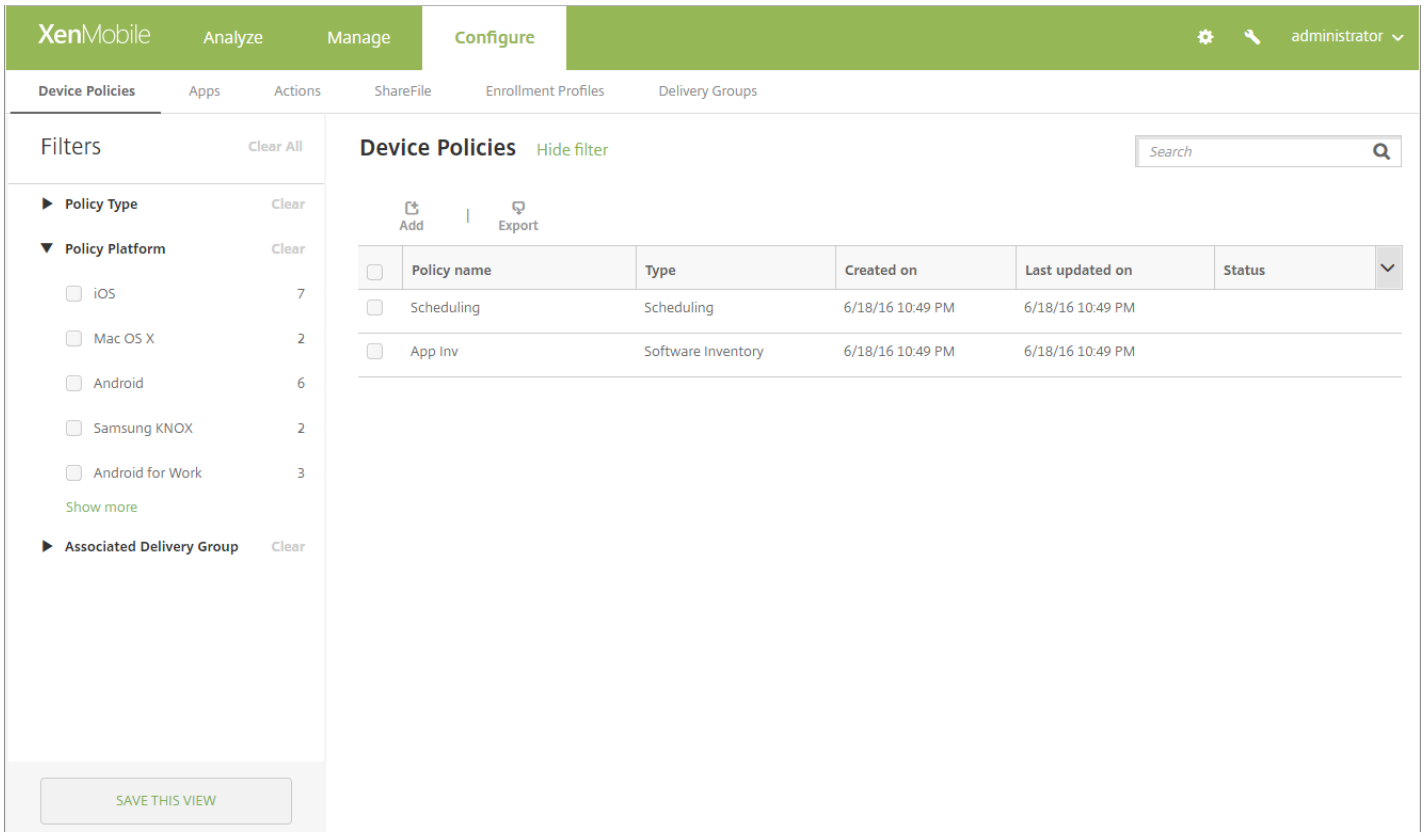
ポリシーの詳細を表示するには、**[詳細表示]** をクリックします。

デバイスポリシーのすべての設定を編集するには、**[編集]** をクリックします。

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

追加されたデバイスポリシーの一覧のフィルター

ポリシーの種類、プラットフォーム、および関連するデリバリーグループで追加されたポリシー一覧にフィルターすることができます。 [構成] > [デバイスポリシー] ページで、 [フィルターを表示] をクリックします。一覧で、表示する項目のチェックボックスをオンにします。



[このビューを保存] をクリックしてフィルターを保存します。フィルターの名前が、 [このビューを保存] ボタンの下のボタンに表示されます。

デバイスポリシーの概要

デバイスポリシー名	デバイスポリシーの説明
AirPlayミラー化	このiOSポリシーによって、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iOSデバイスに追加できます。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	このポリシーでは、AirPrintプリンターを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。iOS 7.0以降で利用できます。 注：各プリンターのIPアドレスとリソースパスがあることを確認してください。
Android for Workアプリケーション制限	このポリシーによって、Android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設定タスクを完了します。詳しくは、「Android at Work」を参照してください。 • AndroidアプリをXenMobileに追加します。詳しくは、「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。このポリシーによって、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	このポリシーでは、以下のアプリケーションの一覧を定義することができます。 • そのデバイスにインストールする必要があるアプリケーション • またはそのデバイスにインストールできるアプリケーション • またはそのデバイスにインストールしてはいけないアプリケーション 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	このポリシーでは、iOSデバイスのための属性（管理対象アプリのバンドルIDやアプリごとのVPN識別子など）を指定できます。
アプリケーション構成	このポリシーでは、管理対象の構成をサポートするアプリケーションのさまざまな設定や動作をリモートで構成できます。そのために、XML構成ファイル（プロパティリスト、またはplistと呼ばれる）をiOSデバイスに展開します。または、キー/値ペアをWindows 10 phone、デスクトップ、タブレットデバイスに展開します。
アプリケーションインベントリ	このポリシーでは、管理対象デバイス上のアプリケーションのインベントリを収集できます。XenMobileは、次にインベントリをそのデバイスに展開されたアプリケーションアクセスポリシーと比較します。この方法で、アプリケーションアクセスのブラックリストまたはホワイトリストにあるアプリケーションを検出し、それに応じて対応できます。
アプリケーションロック	このポリシーはユーザーがデバイス上で実行できるアプリケーション、または実行できないアプリケーションの一覧を定義します。 このポリシーは、iOSデバイスとAndroidデバイスの両方に対して構成できますが、ポリシーが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。 アプリのロックポリシーは、ほとんどのAndroid LおよびMデバイスで機能します。ただし、アプリの

	ロックポリシーは、Googleが必要となるAPIを廃止したため、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。その結果、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	このポリシーでは、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。管理対象のアプリケーションに次のアプリケーションは含まれていません。 ● ユーザーがデバイスに直接ダウンロードするアプリケーション。すなわち、アプリケーションはXenMobileを使用して展開されていません。 ● 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。
アプリケーション制限	このポリシーでは、Samsung KNOXデバイスへのユーザーによるインストールを禁止するアプリのブラックリストを作成します。ユーザーによるインストールを許可するアプリのホワイトリストも作成できます。
アプリ アンインストール	このポリシーでは、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。たとえば、特定のアプリケーションのサポートを希望していないことがあります。または、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	このポリシーでは、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	このポリシーでは、ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、デバイスで使用できるブラウザー機能を定義したりすることができます。Samsungデバイスでは、ブラウザーを無効にすることや、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。
カレンダー (CalDav)	このポリシーでは、カレンダー（CalDAV）アカウントをiOSまたはMac OS Xデバイスに追加します。CalDAVアカウントによって、ユーザーはスケジュールデータをCalDAVをサポートするサーバーと同期させることができます。
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	このポリシーでは、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。
連絡先(CardDAV)	このポリシーでは、iOS連絡先（CardDAV）アカウントをiOSまたはMac OS Xデバイスに追加します。CardDAVアカウントによって、ユーザーは連絡先データをCardDAVをサポートするサーバーと同期させることができます。
Samsungコンテナーへのアプリケーションのコピー	このポリシーでは、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を、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します。SEAMSコンテナーにコピーされたアプリケーションは、デバイス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	このポリシーでは、XenMobile PKI構成で統合認証を有効にします。たとえば、PKIエンティティ、キーストア、資格情報プロバイダー、サーバー証明書などを使用します。資格情報について詳しくは、「証明書と認証」を参照してください。 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。
カスタムXML	このポリシーでは、以下の機能がカスタマイズされます。 • デバイスの構成や、機能の有効化/無効化などのプロビジョニング • 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のデバイス構成 • 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のソフトウェアのアップグレード • デバイスからのエラーおよび状態レポートの受信などの障害管理 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の使用については、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。
Defender	このポリシーはデスクトップおよびタブレットのWindows 10でWindows Defender設定を構成します。
ファイルおよびフォルダーの削除	このポリシーでは、Windows Mobile/CEデバイスから特定のファイルまたはフォルダーを削除します。
レジストリ キーと値の削除	このポリシーでは、Windows Mobile/CEデバイスから特定のレジストリキーおよび値を削除します。

デバイス正常性構成証明	このポリシーでは、Windows 10デバイスにデバイスの正常性状態を報告させます。そのため、分析目的で特定のデータおよびランタイム情報をHealth Attestation Service （HAS）に送信させます。HASは、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスからXenMobileに送信されます。XenMobileは正常性構成証明書を受信すると、その内容に基づいて、管理者が構成した自動アクションを展開します。 詳しくは、MicrosoftのDevice HealthAttestation CSPページを参照してください。
デバイス名	このポリシーでは、デバイスを特定できるように、iOSデバイスおよびMac OS Xデバイスに名前を設定します。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。マクロについて詳しくは、「マクロ」を参照してください。
エンタープライズ ハブ	Windows Phoneのこのポリシーでは、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。 XenMobileでは、Windows Phone Secure Hubの1つのモードについて、1つのEnterprise Hubポリシーだけがサポートされています。たとえば、複数のEnterprise Hubポリシーをさまざまなバージョンの Secure Home for XenMobile Enterprise Edition用に作成する必要はありません。デバイスの登録中にのみ最初のEnterprise Hubポリシーを展開できます。
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。MDM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。または、コンテナー化されたSecure Mailアプリケーションを使用してActiveSyncメールを送信することができます。
ファイル	このポリシーでは、ユーザーに対して特定の機能を実行するスクリプトファイルをXenMobileに追加します。または、Androidデバイスユーザーがデバイスでアクセスできるドキュメントファイルを追加することができます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。たとえば、Androidユーザーに会社のドキュメントまたはPDFファイルを送信するには、そのファイルをデバイスに展開します。そしてユーザーにファイルがある場所を知らせます。
フォント	このポリシーでは、iOSデバイスおよびMac OS Xデバイスにフォントを追加します。フォントはTrueType（.TTF）またはOpenType（.OFT）である必要があります。フォントコレクション（.TTCまたは.OTC）はサポートされません。iOSの場合、このポリシーはiOS 7.0以降にのみ適用されます。
ホーム画面のレイアウト	このポリシーでは、iOS 9.3以降の監視対象デバイスのホーム画面について、アプリとフォルダーのレイアウトを指定します。
iOSおよびMac OS Xプロファイルのインポート	このポリシーでは、iOSおよびOS Xデバイス用のデバイス構成XMLファイルをXenMobileにインポートします。XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。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	このポリシーでは、Samsung SAFEデバイスでのアプリケーションの使用を制限します。利用可能なアプリケーションを特定のアプリケーションに制限できます。このポリシーは、特定の種類またはクラ

	スのアプリケーションのみを実行することを目的とするコーポレートデバイスで役立ちます。また、このポリシーを使用して、キオスクモードのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。
ランチャー構成	Androidデバイス用のこのポリシーでは、Citrix Launcher向けに以下を指定します。 • 許可されたアプリケーション • Citrix Launcherアイコン用のカスタムロゴ画像 • Citrix Launcherのカスタム背景画像 • Citrix Launcherを終了するためのパスワード要件
LDAP	iOSデバイスのこのポリシーでは、LDAPサーバーホスト名などの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。
場所	このポリシーでは、そのデバイスのGPSがSecure Hubに対応している場合に、地図上で位置を検出できるデバイスを許可します。このポリシーをデバイスに展開した後、XenMobile Serverから位置を確認するコマンドを送信することができます。デバイスはその後位置情報を返信します。XenMobileは、ジオフェンシングおよび追跡ポリシーもサポートします。
メール	このポリシーでは、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します。
管理対象ドメイン	このポリシーでは、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。iOS 8以降の監視対象デバイスでは、URLまたはサブドメインを使用することで、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御できます。
MDMオプション	このポリシーでは、監視対象のiOS 7.0以降のモバイルデバイスで［iPhoneとiPadを探す］の［アクティベーションロック］を管理することができます。iOSデバイスを監視対象モードにする手順については、「iOSデバイスおよびmacOSデバイスの一括登録」を参照してください。
組織情報	このポリシーでは、XenMobileがiOSデバイスに展開するアラートメッセージの組織情報を指定します。iOS 7以降で利用できます。
パスコード	このポリシーでは、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。デバイス上でパスコードの複雑さやタイムアウトを設定できます。
個人用ホットスポット	このポリシーでは、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。ユーザーは、個人用ホットスポット機能を介してiOSデバイスの携帯データネットワーク接続で接続します。iOS 7.0以降で利用できます。

プロファイルの削除	このポリシーを展開すると、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	このポリシーでは、エンタープライズ配信のプロビジョニングプロファイルを指定してデバイスに送信します。iOSエンタープライズアプリを開発し、コード署名をするときは、通常は、プロビジョニングプロファイルを含めます。Appleは、iOSデバイスで実行するアプリについてはプロファイルを要求します。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。
プロビジョニングプロファイルの削除	このポリシーでは、iOSプロビジョニングプロファイルを削除します。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デバイスポリシー」を参照してください。
プロキシ	このポリシーでは、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します。グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。
レジストリ	Windows Mobile/CE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。このポリシーでは、Windows Mobile/CEデバイスの管理に使用するレジストリキーおよび値を定義します。
リモートサポート	このポリシーでは、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。
制限事項	このポリシーでは、管理対象デバイスをロックダウンしたり、機能を制御する数百のオプションが提供されています。制限オプションの例：カメラやマイクの無効化、ローミング規則の適用、アプリ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の適用。
移動	このポリシーでは、iOSデバイスおよびWindows Mobile/CEデバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成します。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。iOSの場合、このポリシーはiOS 5.0以降のデバイスで使用できます。
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	このポリシーでは、SAFEのポリシーおよび制限を展開する前に、デバイスに展開する必要がある組み込みのSamsung Enterprise License Management（ELM）キーを指定します。XenMobileはSamsung for Enterprise（SAFE）およびSamsung KNOXポリシーの両方をサポートし、拡張しています。
スケジュール設定	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 Serverに接続する際に必要です。このポリシーをデバイスに送信せず、Google FCMを有効にしない場合、デバイスはサーバーに接続することができません。
SCEP	このポリシーでは、iOSデバイスおよびMac OS Xデバイスを構成し、外部SCEPサーバーから証明書を取得します。XenMobileに接続されているPKIからSCEPを使用してデバイスに証明書を配布することもできます。そのためには、PKIエンティティとPKIプロバイダーを分散モードで作成します。詳しくは、「PKIエンティティ」を参照してください。
SSOアカウント	このポリシーでは、ユーザーが1回サインオンするだけで、XenMobileおよび社内リソースにアクセスすることができるように、シングルサインオン（SSO）アカウントを作成します。デバイスに資格情報を保存する必要はありません。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認証と互換性があります。iOS 7.0以降で利用できます。
ストレージ暗号化	このポリシーでは、内部ストレージおよび外部ストレージを暗号化します。一部のデバイスについては、このポリシーによって、ユーザーがデバイスでメモリカードを使用できなくなります。
サブスクライブされたカレンダー	このポリシーでは、サブスクライブされたカレンダーをiOSデバイスのカレンダー一覧に追加します。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。 ユーザーのデバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みであることを確認します。
契約条件	このポリシーでは、ユーザーが社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに要求します。ユーザーがXenMobileにデバイスを登録するときに、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。
トンネル	このポリシーは、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、最初にXenMobileを経由します。その後、トラフィックはアプリを実行するサーバーにリダイレクトされます。
VPN	このポリシーでは、従来のVPN Gatewayテクノロジを使用するバックエンドシステムへのアクセスを提供します。このポリシーでは、デバイスに展開できるVPNゲートウェイ接続の詳細を提供します。XenMobileは、Cisco AnyConnect、Juniper、およびCitrix VPNなどの、いくつかのVPNプロバイダーをサポートしています。VPNゲートウェイがこのオプションをサポートしている場合、このポリシーをCAにリンクして、VPNオンデマンドを有効にできます。

壁紙	このポリシーでは.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します。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します。
Webコンテンツフィルター	このポリシーでは、iOSデバイスのWebコンテンツをフィルターします。XenMobileは、Appleのオートフィルター機能およびホワイトリストとブラックリストに追加したサイトを使用します。iOS 7.0以降の監視対象デバイスでのみ利用できます。iOSデバイスを監視モードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスを監視モードにする」を参照してください。
Webクリップ	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します。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	このポリシーでは、管理者がWiFiルーターの詳細を管理対象デバイスに展開することを許可します。ルーターの詳細には、SSID、認証データ、構成データなどがあります。
Windows CE証明書	このポリシーでは、外部のPKIを基にWindows Mobile/CE PKI証明書を作成し、ユーザーのデバイスに配布します。証明書およびPKIエンティティについて詳しくは、「証明書と認証」を参照してください。
XenMobile Store	このポリシーでは、XenMobile Store Webクリップが、ユーザデバイスのホーム画面に表示されるかどうかを指定します。
XenMobileオプション	このポリシーでは、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのSecure Hubの動作を構成します。
XenMobileのアンインストール	このポリシーでは、XenMobileをAndroidデバイスおよびWindows Mobile/CEデバイスからアンインストールします。このポリシーを展開すると、展開グループ内のすべてのデバイスからXenMobileが削除されます。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

APNデバイスポリシー

Feb 27, 2017

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

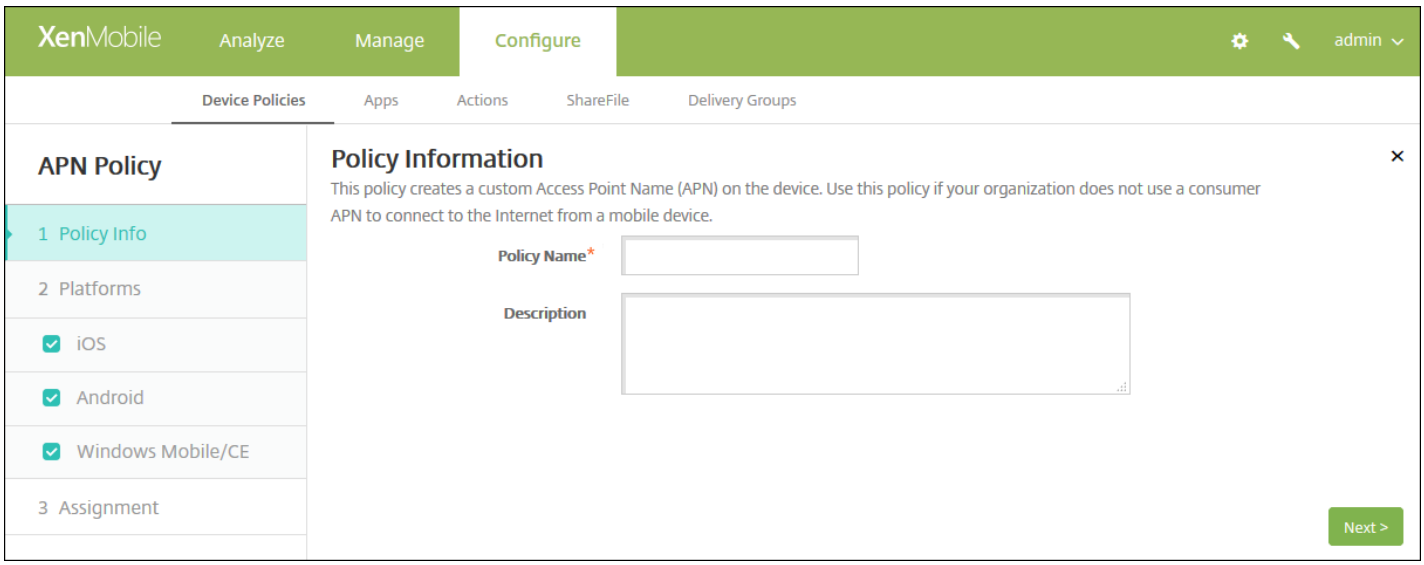
Androidの設定

Windows Mobile/CEの設定

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[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。



4. **[ポリシー情報]** 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。

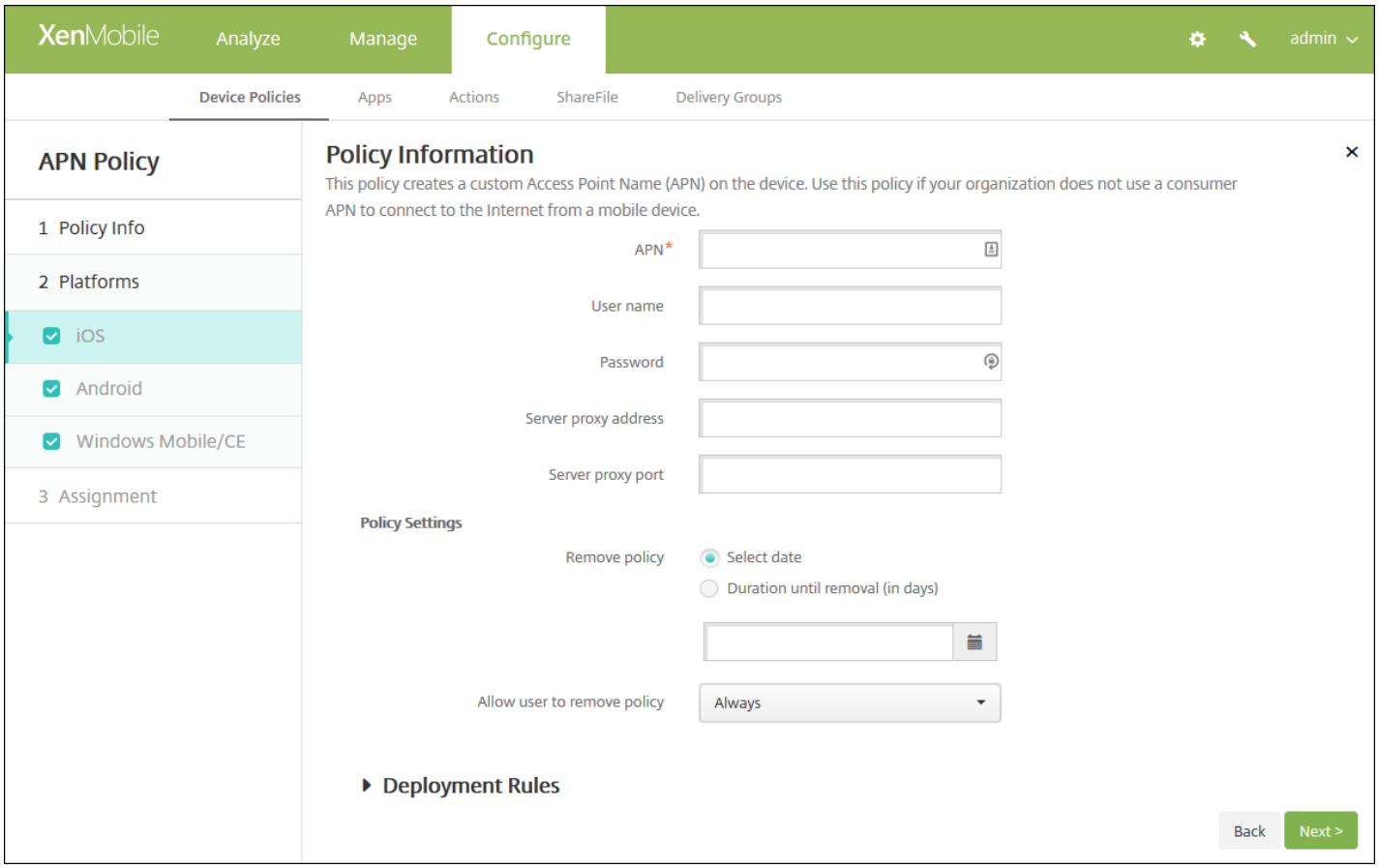
5. **[次へ]** をクリックします。**[ポリシープラットフォーム]** ページが開きます。

注： **[ポリシープラットフォーム]** 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. **[プラットフォーム]** で、追加するプラットフォームをオンにします。

1つのプラットフォームの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。

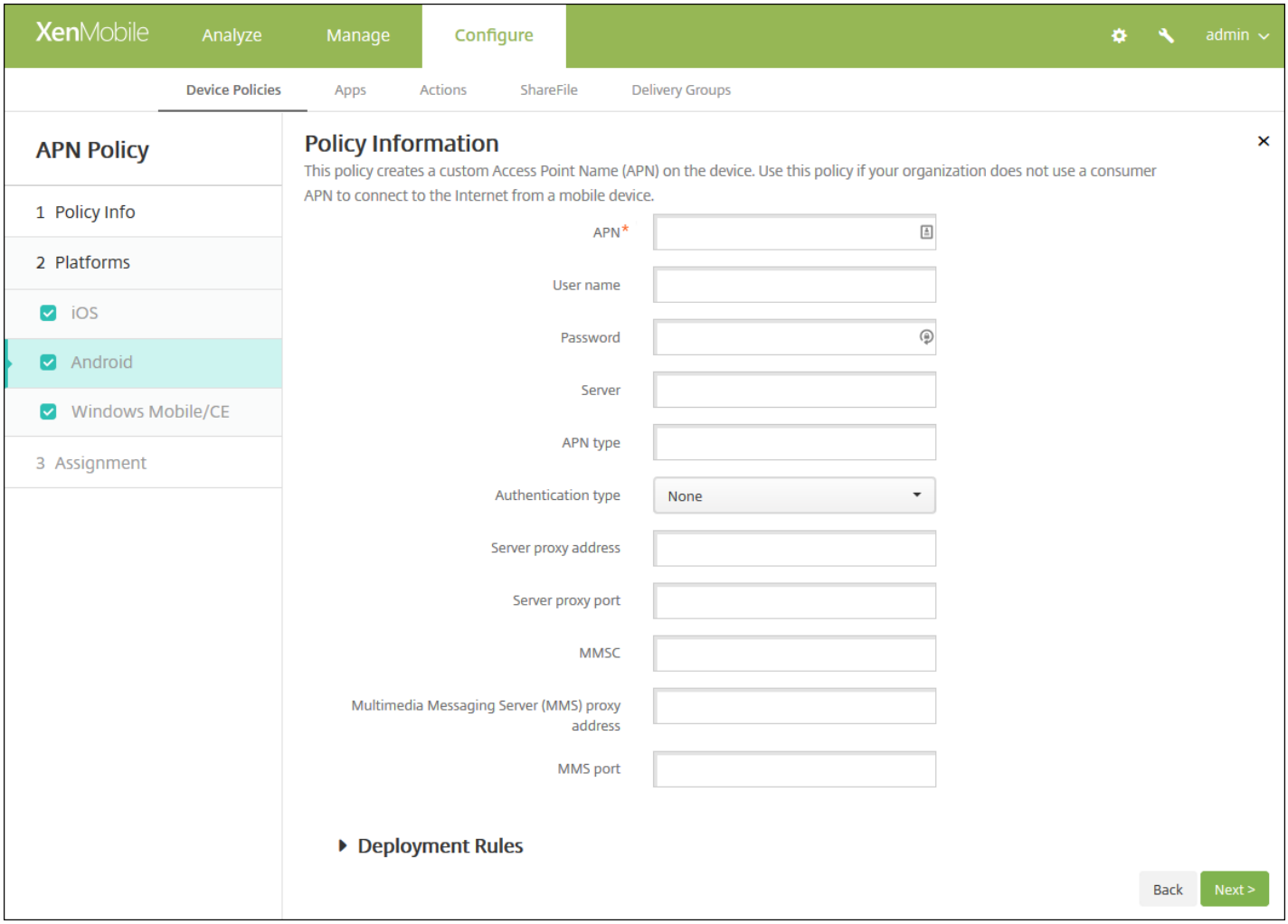
iOSの設定の構成



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。
- **ユーザー名**： このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **パスワード**： このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **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。
- **[ポリシー設定]** の下の **[ポリシーの削除]** の横にある、 **[日付を選択]** または **[削除までの期間 (日) を指定]** をクリックします。
  - **[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。
  - **[パスワードが必要]** を選択した場合、 **[削除のパスワード]** の横に必要なパスワードを入力します。

Androidの設定の構成



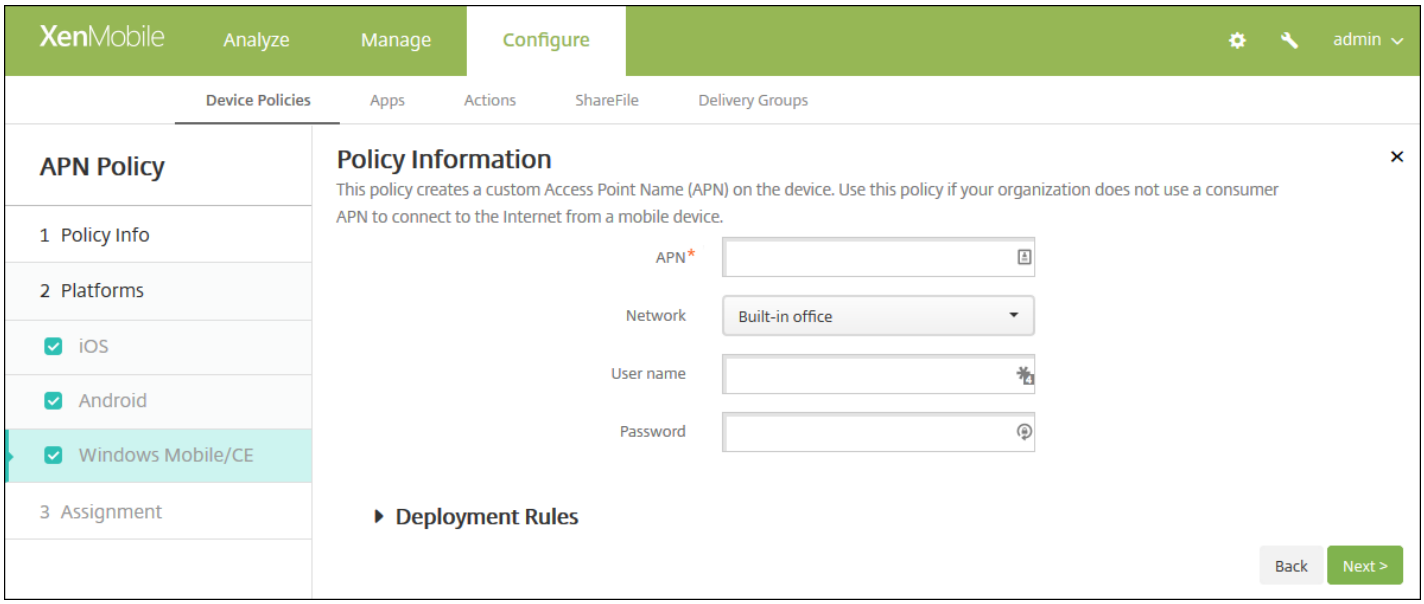
次の設定を構成します。

- **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。
- **ユーザー名**： このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **パスワード**： このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **サーバー**： この設定はスマートフォンに先行するもので、通常は空白です。標準のWebサイトにアクセスできない、または標準のWebサイトを表示できない電話機用のワイヤレスアプリケーションプロトコル（WAP）ゲートウェイサーバーを参照します。
- **APN 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。

- **認証の種類**： 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［なし］です。
- **サーバープロキシアドレス**：電話会社のAPN HTTPプロキシのIPアドレスまたはURLです。
- **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。

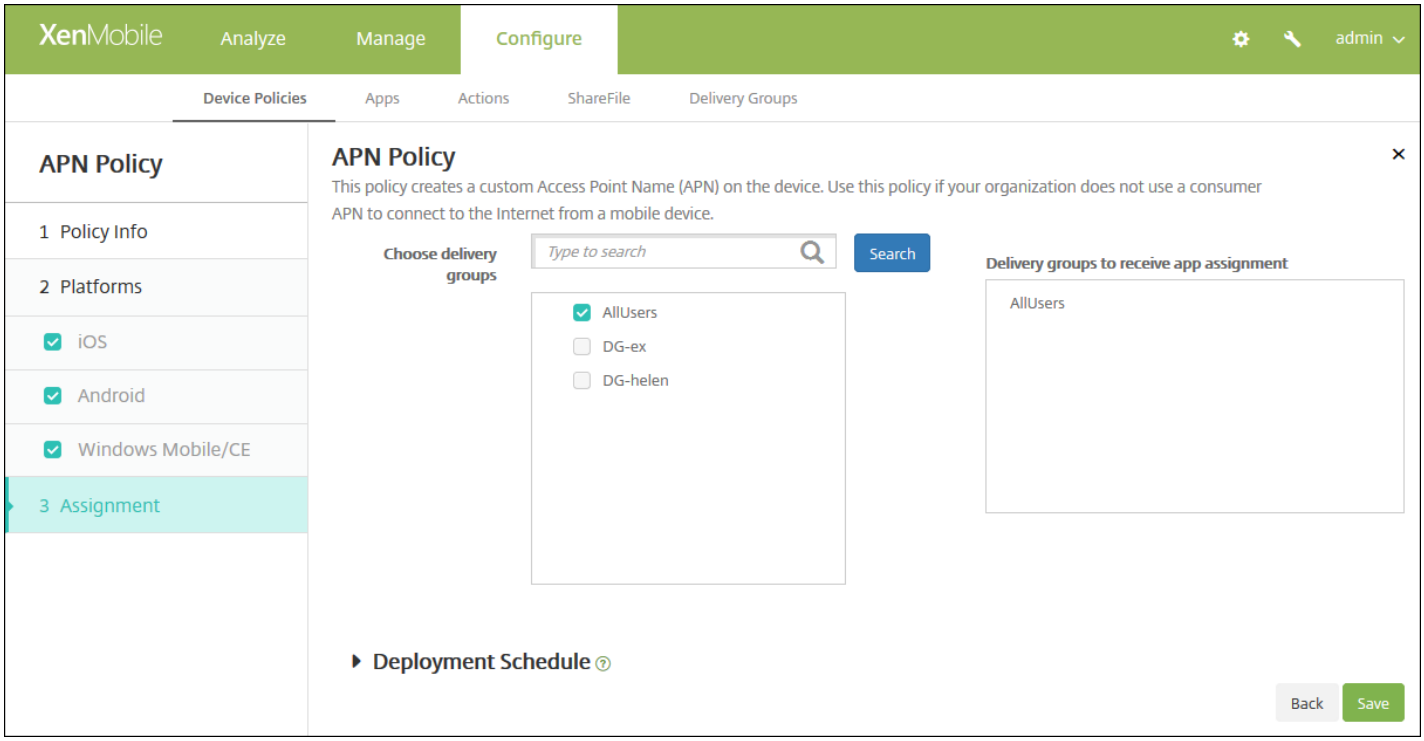
Windows Mobile/CEの設定の構成



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。
- **ネットワーク**： 一覧から、使用するネットワークの種類を選択します。デフォルトは **[Built-in office]** です。
- **ユーザー名**： このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **パスワード**： このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。

8. **[次へ]** をクリックします。 **[APNポリシー]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

アプリケーション属性デバイスポリシー

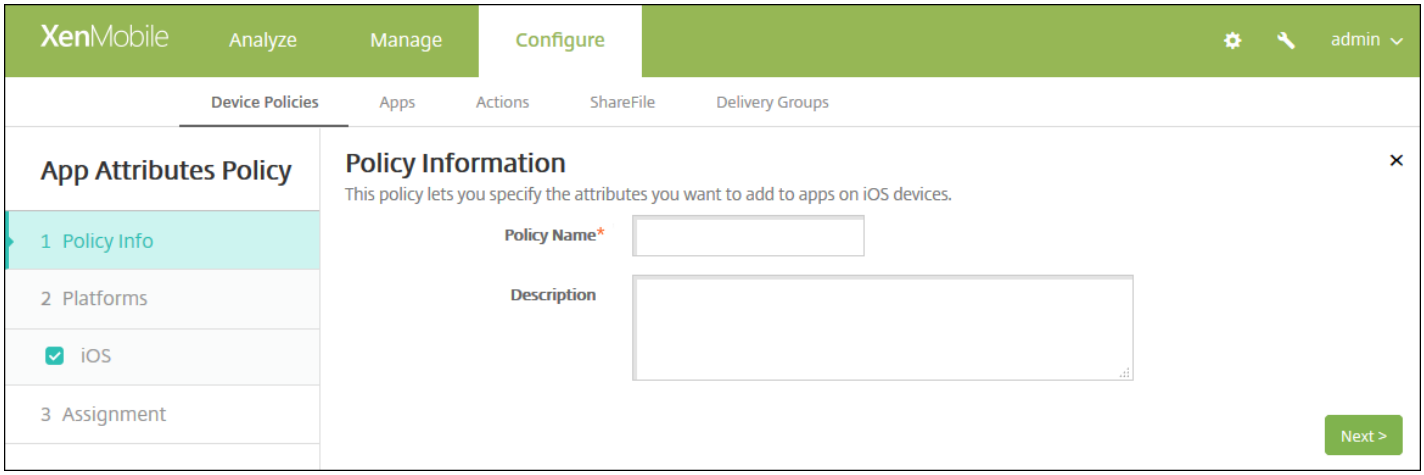
Mar 07, 2017

アプリケーション属性デバイスポリシーで、iOSデバイスのための属性（管理対象アプリのバンドルIDやアプリごとのVPN識別子など）を指定できます。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ページが開きます。

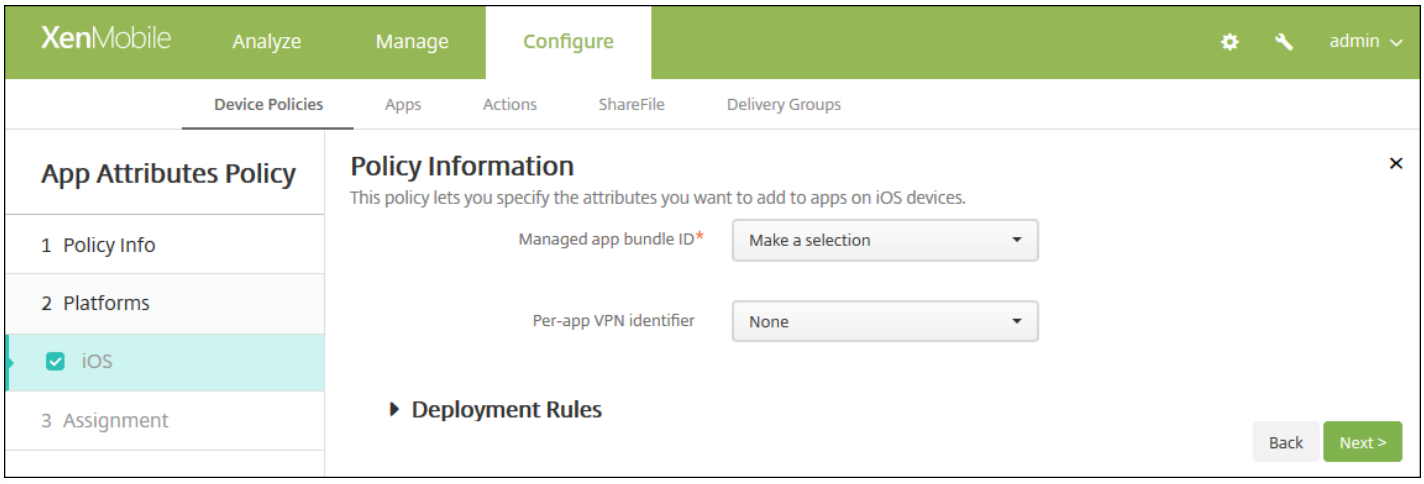
3. **[More]** を展開し、 **[Apps]** の下の **[App Attributes]** をクリックします。 **[App Attributes Policy]** プラットフォーム情報ページが開きます。



4. **[ポリシー情報]** 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。

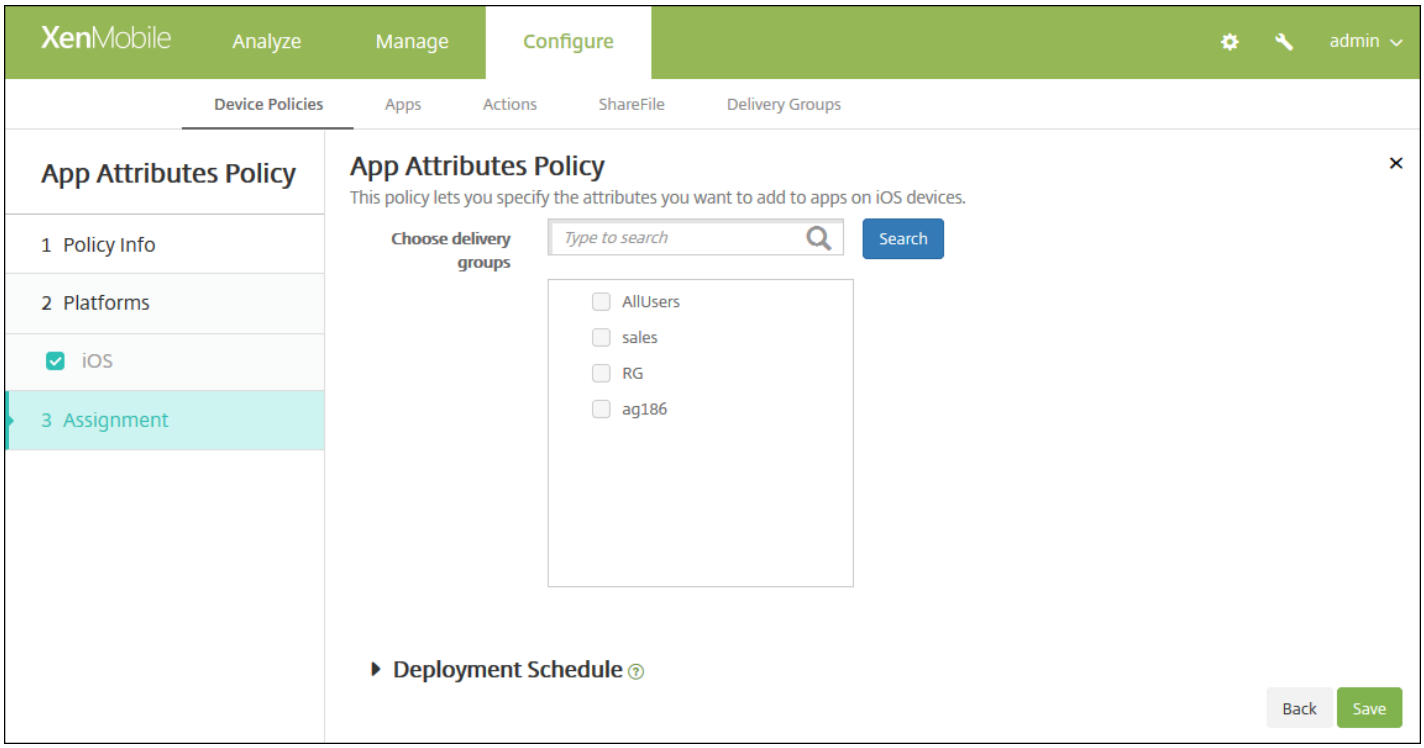
5. **[Next]** をクリックします。 **[App Attributes]** プラットフォーム情報ページが開きます。



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。

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. ［**デリバリーグループを選択**］の横に、デリバリーグループを入力して検索します。または、ポリシーを割り当てるグループを一覧から1つまたは複数選択します。選択したグループが［**アプリ割り当てを受信するためのデリバリーグループ**］一覧に表示されます。

10. ［**展開スケジュール**］を展開して以下の設定を構成します。

- ［**展開**］の横の［**オン**］をクリックすると展開がスケジュールされ、［**オフ**］をクリックすると展開が行われません。デフォルトのオプションは［**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［**すぐに**］です。
- ［**あとで**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**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、［**接続するたび**］です。
- ［**常時接続に対する展開**］の横の［**オン**］または［**オフ**］をクリックします。デフォルトのオプションは［**オフ**］です。

注：

- このオプションは、［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. **［保存］**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

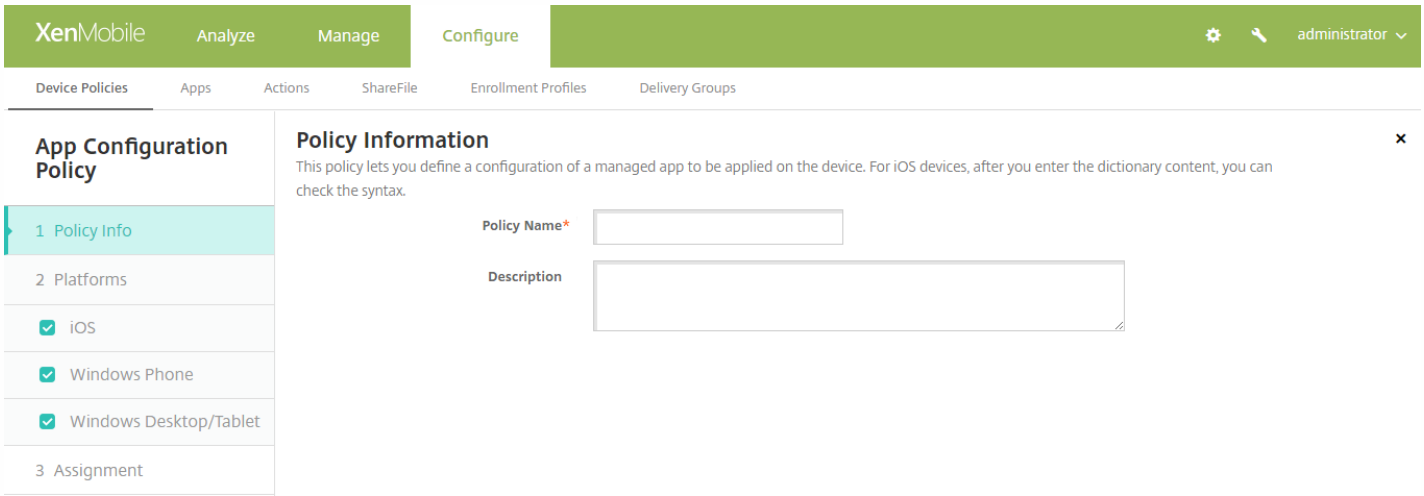
Feb 27, 2017

管理された構成をサポートする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plis
と呼ばれるファイル）をユーザーのiOSデバイスに展開するか、キー/値ペアをWindows 10 Phone、タブレット、またはデス
クトップデバイスに展開できます。構成では、アプリのさまざまな設定や動作を指定します。 XenMobileは、ユーザーがア
リをインストールしたデバイスに構成をプッシュします。 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、 **[構成]** の **[デバイスポリシー]** 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. **[ポリシー情報]** ペインで、以下の情報を入力します。

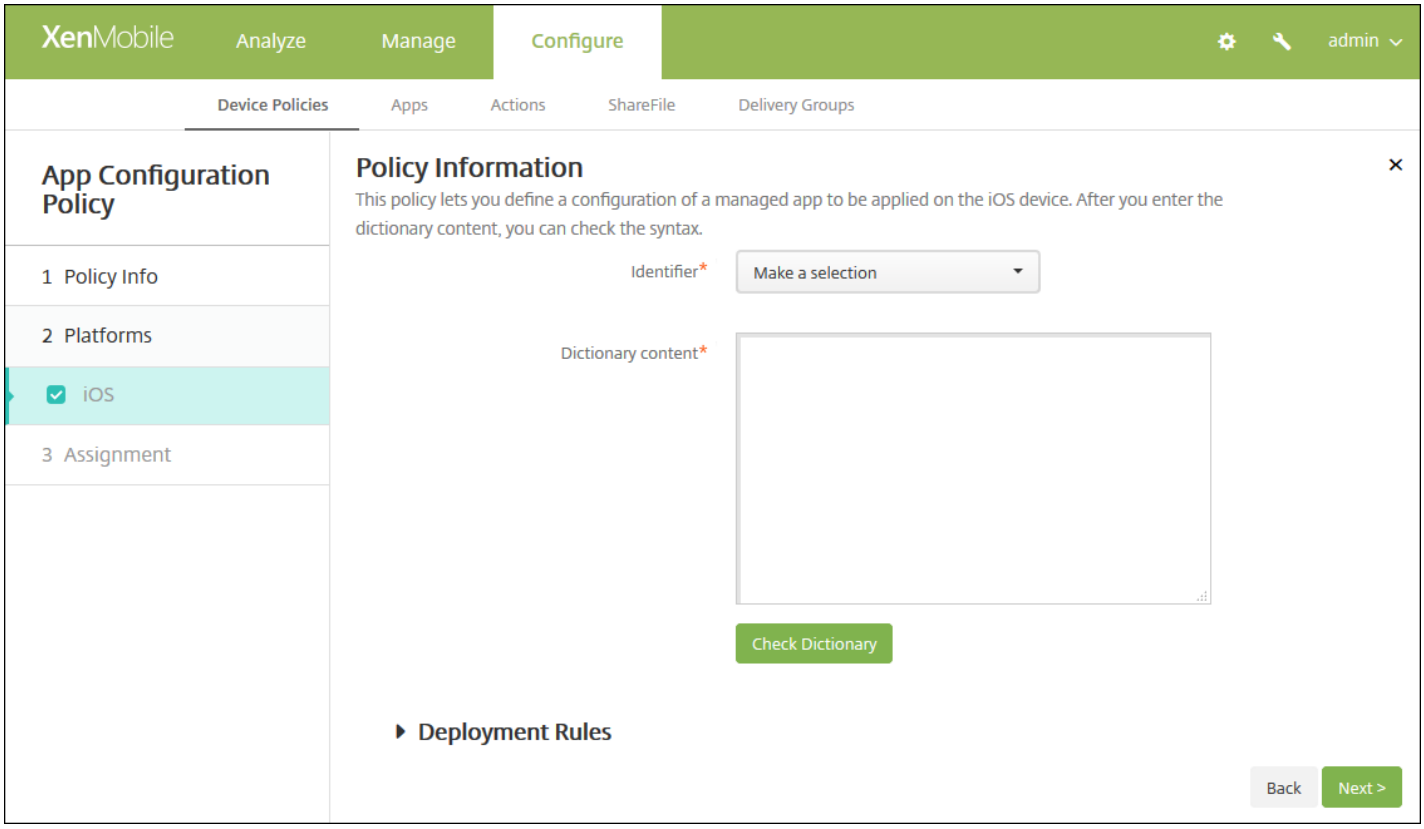
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[Policy Platforms]** ページが開きます。

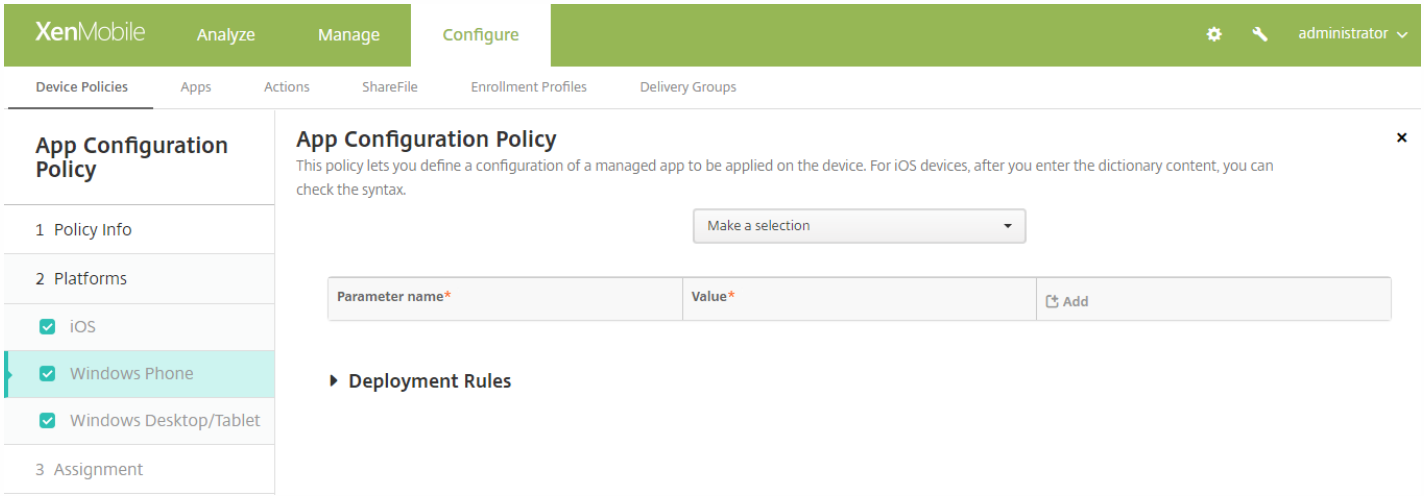
   [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

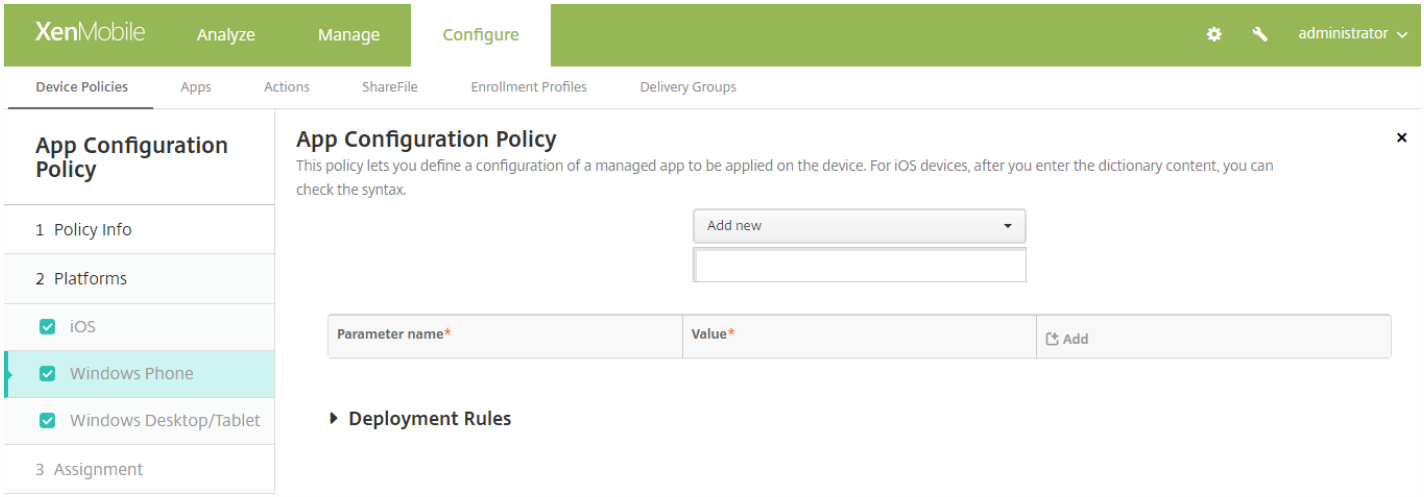
   1つのプラットフォームの設定の構成が完了したら、手順6を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



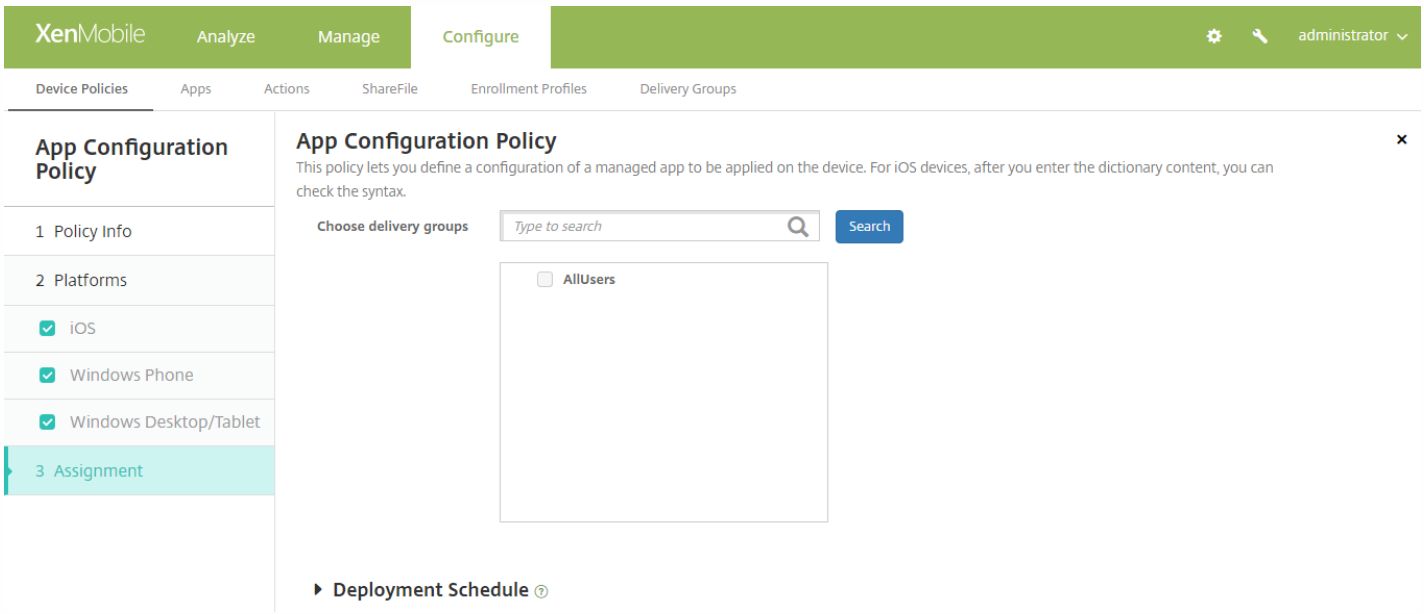
Windows Phoneまたはデスクトップ/タブレットの設定の構成





6. 展開規則を構成します。

7. [Next] をクリックします。 [App Configuration Policy] 割り当てページが開きます。



8. [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。

9. [Deployment Schedule] を展開して以下の設定を構成します。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、 [オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。 [オフ] を選択した場合、そのほかのオプションを構成する必要はありません。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [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、 [接続するたび] です。
- [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

注：

- このオプションは、［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。

10. ［保存］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

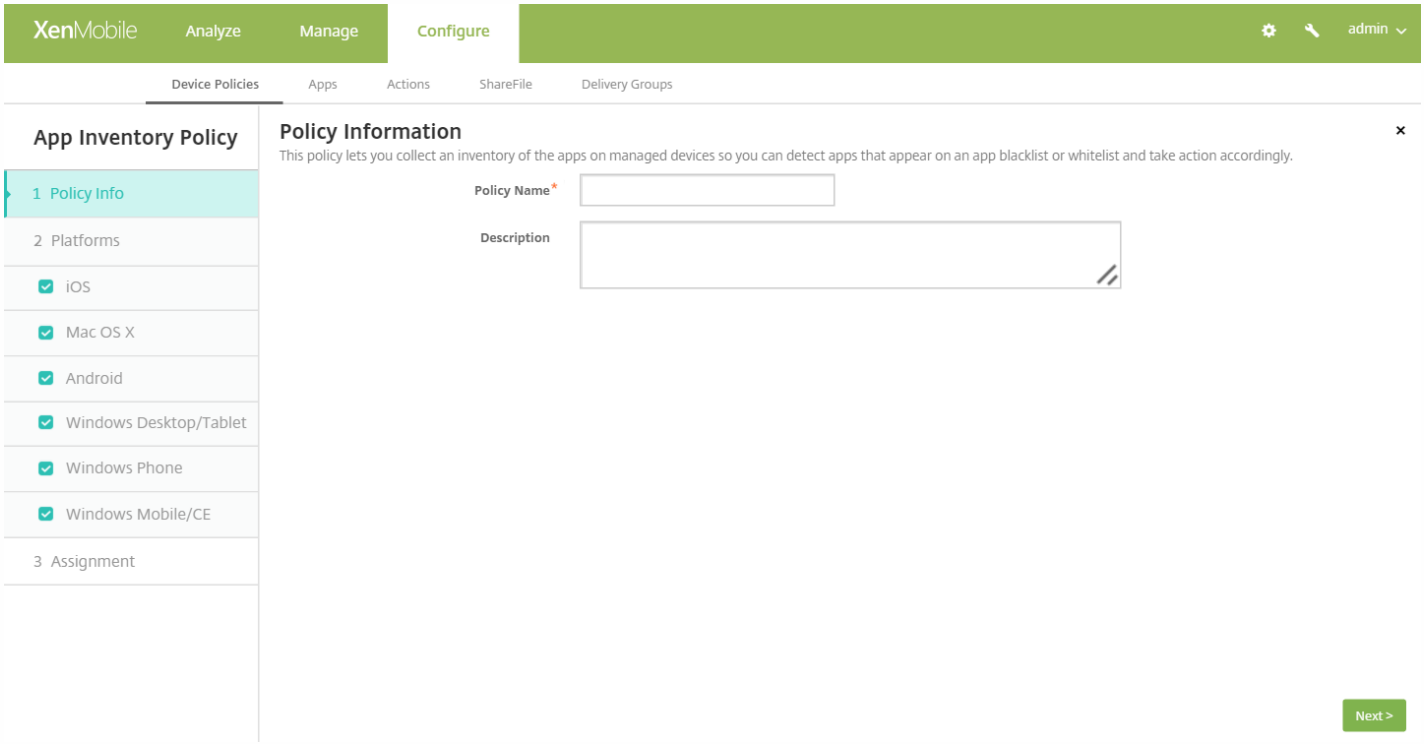
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]の[デバイスポリシー]**をクリックします。**[デバイスポリシー]**ページが開きます。

2. **[Add]**をクリックします。**[Add a New Policy]**ページが開きます。

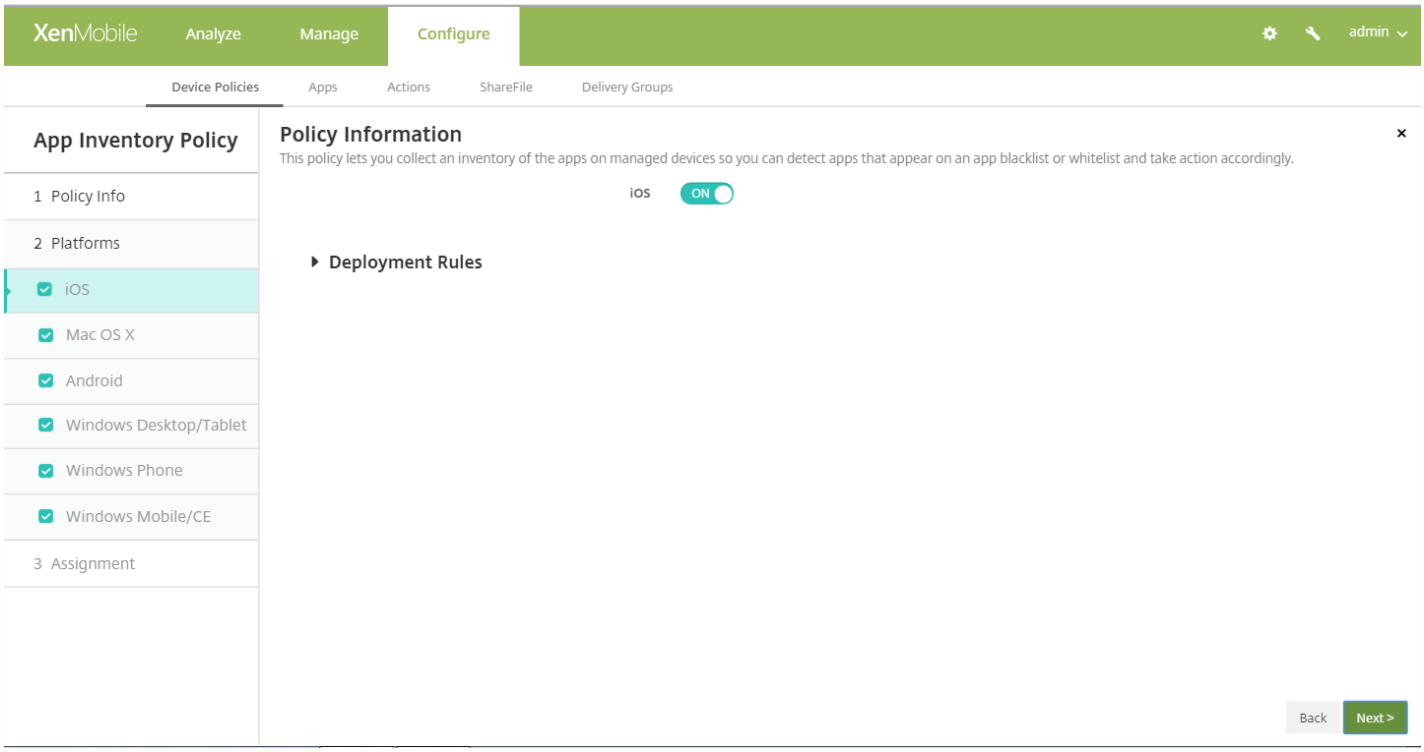
3. **[More]**を展開し、**[Apps]**の下の**[App Inventory]**をクリックします。**[App Inventory Policy]**ページが開きます。



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. **[次へ]**をクリックします。**[Policy Platforms]**ページが開きます。



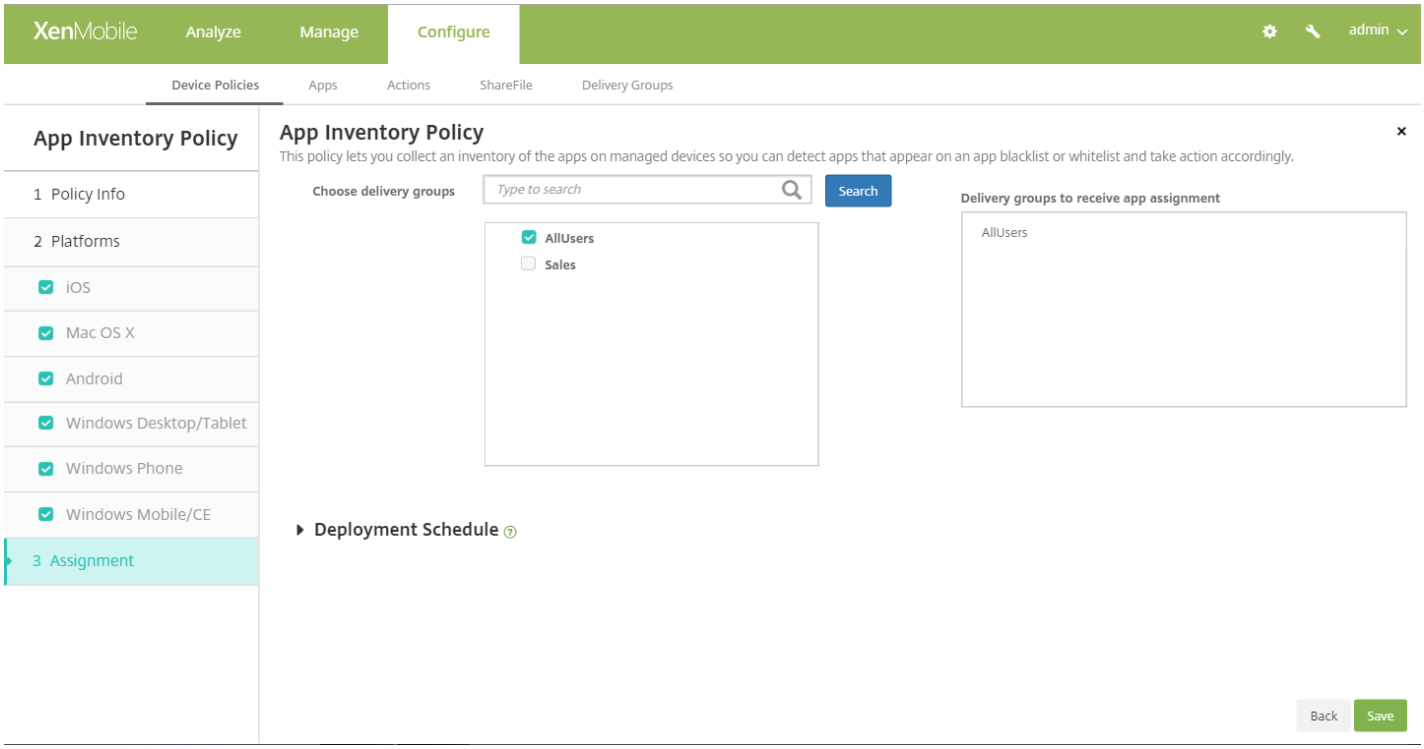
[Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

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] の一覧に表示されます。

10. [展開スケジュール] を展開して以下の設定を構成します。

- [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。[オフ] 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 [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、[以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [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 [オフ] 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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

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

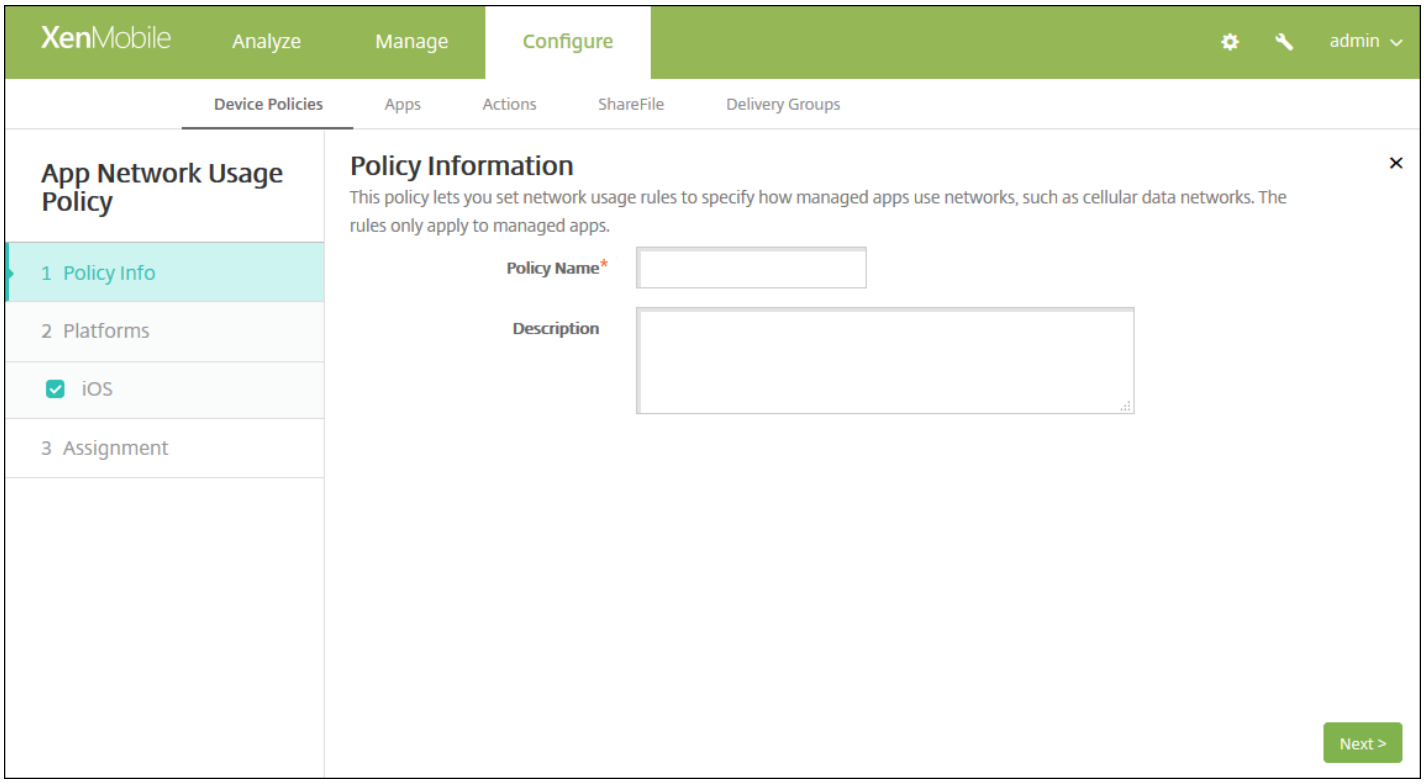
Feb 27, 2017

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. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

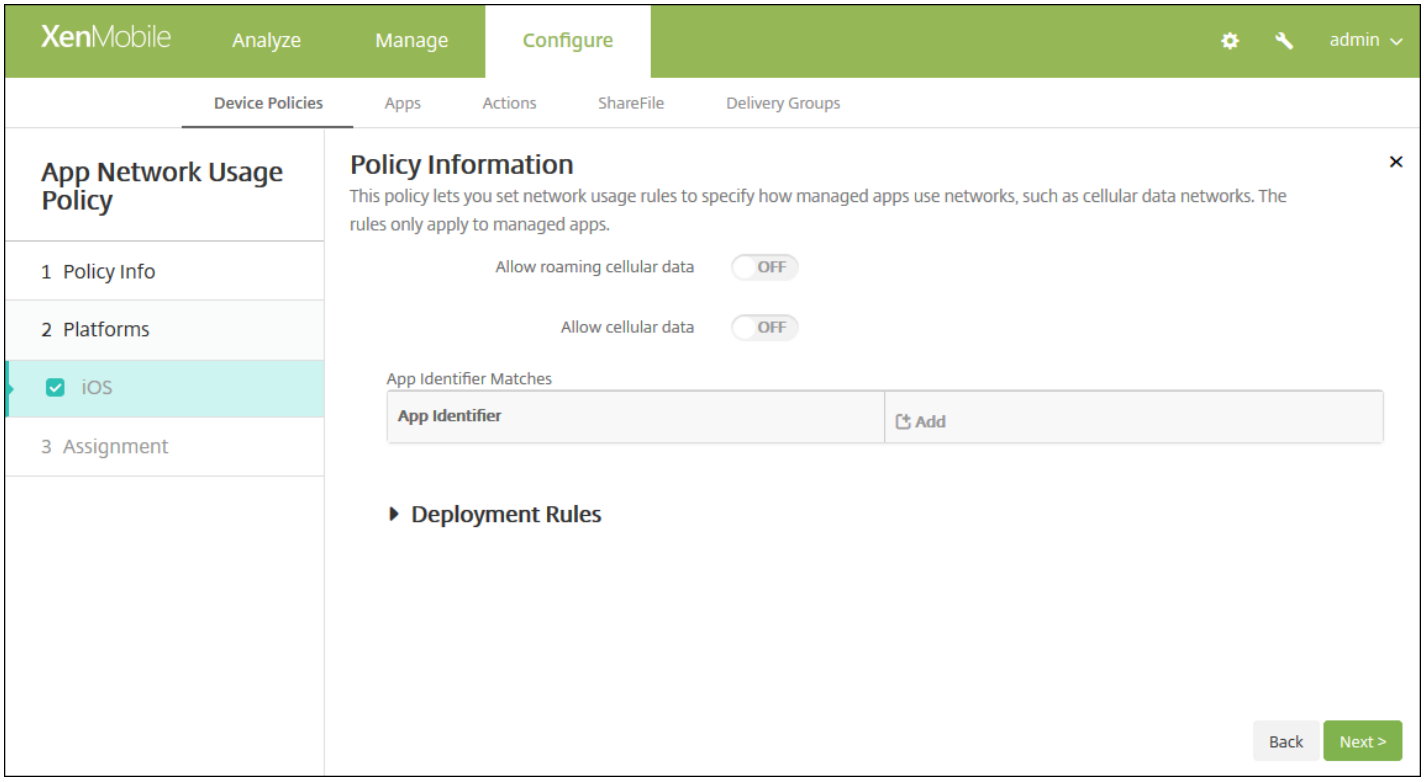
3. **[More]** を展開し、**[Apps]** で **[App Network Usage]** をクリックします。**[App Network Usage Policy]** 情報ページが開きます。



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。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** 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。

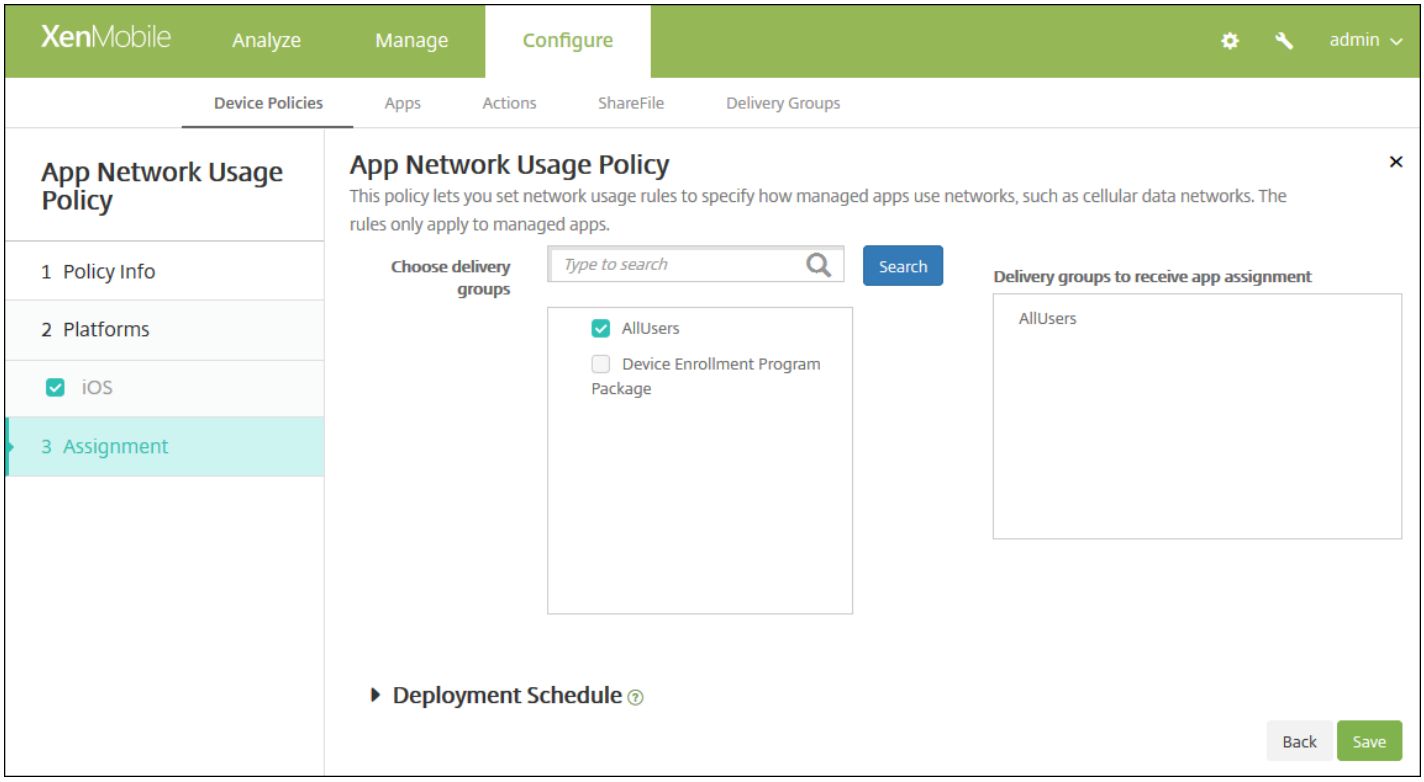
- Allow roaming cellular data： 指定したアプリケーションに、ローミング中に携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは［OFF］です。
- Allow cellular data： 指定したアプリケーションに、携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは［OFF］です。
- App Identifier Matches： 一覧に追加するアプリケーションごとに、［Add］をクリックして以下の操作を行います。
  - **アプリ識別子**： アプリのIDを入力してください。
  - ［保存］をクリックしてアプリケーションを一覧に保存するか、［キャンセル］をクリックして操作を取り消します。

  注： 既存のアプリを削除するには、その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 Network Usage Policy］割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[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、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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、**[常時接続に対する展開]** 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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

アプリケーショントンネリングデバイスポリシー

Feb 27, 2017

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ーコンポーネント間のプロキシパラメーターを定義します。また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。アプリケーショントンネリングポリシーは、Androidデバイスおよび Windows Mobile/CEデバイスに対して構成できます。

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。

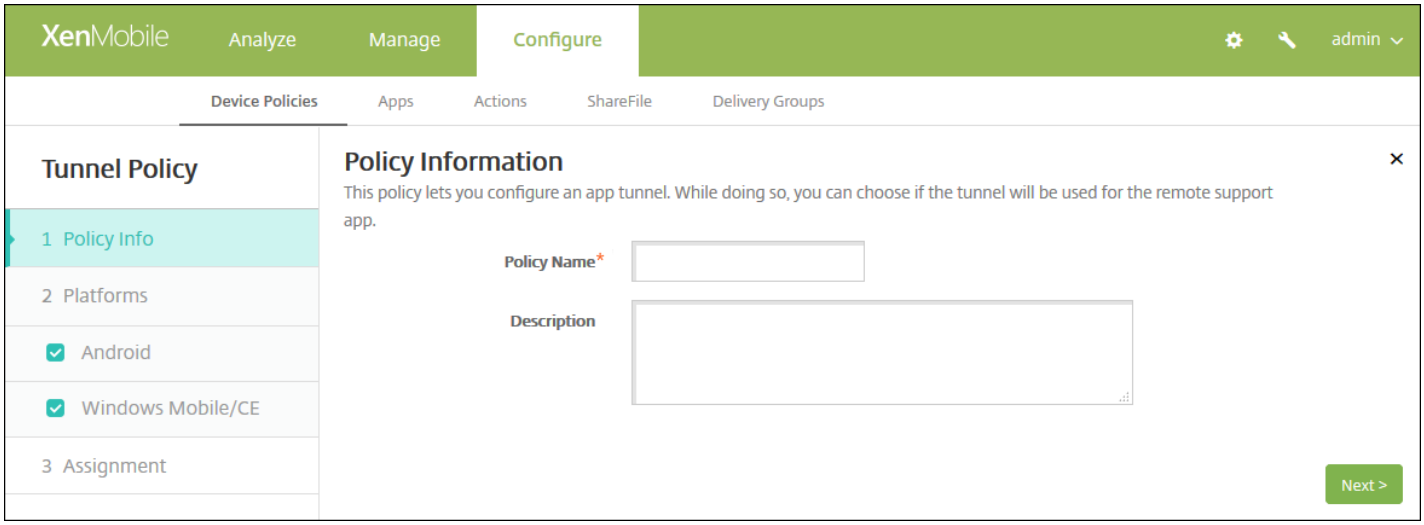
Androidの設定

Windows Mobile/CEの設定

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[詳細]** をクリックした後、**[ネットワークアクセス]** の下の **[トンネル]** をクリックします。**[トンネルポリシー]** ページが開きます。



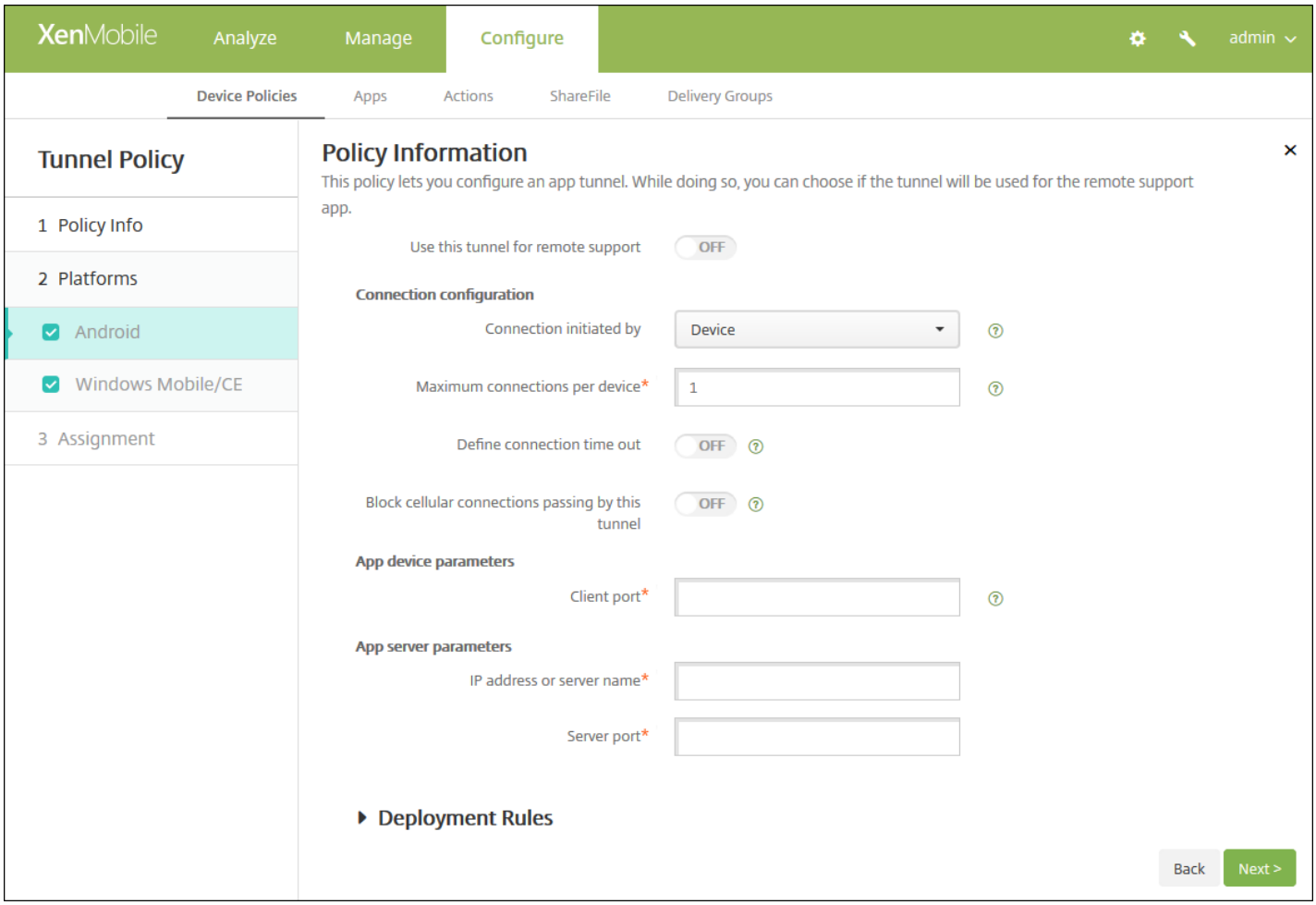
4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **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. **[次へ]** をクリックします。**[Policy Platforms]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



次の設定を構成します。

- **このトンネルをリモートサポートに使用**：トンネルをRemote Supportに利用するかどうか選択します。

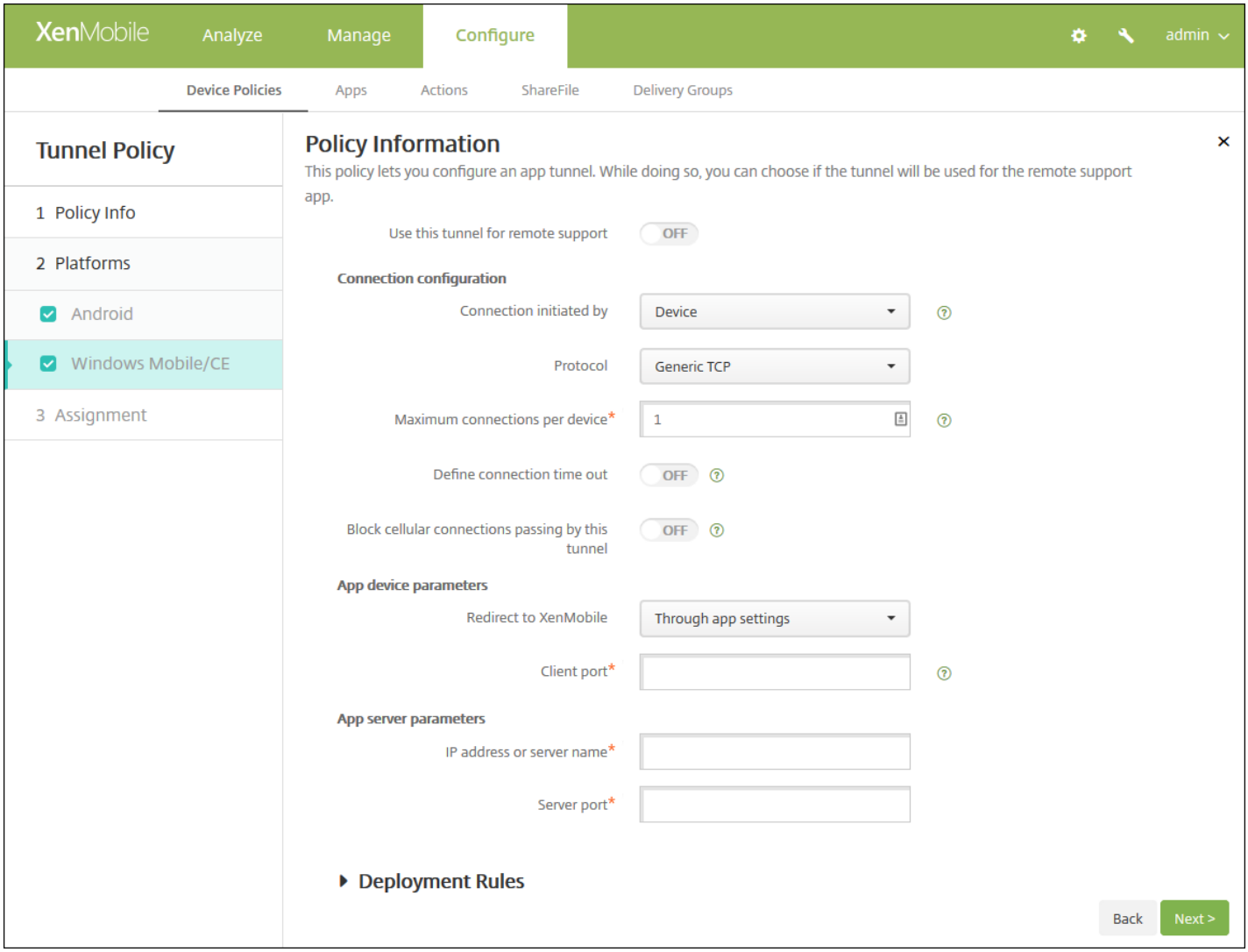
  注： リモートサポートを選択するかどうかによって、構成手順が異なります。

- 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。
  - **接続を開始する側**： **[デバイス]**または**[サーバー]**を選択して、接続の開始元を指定します。
  - **デバイスごとの最大接続数**： 数値を入力して、アプリケーションが確立できる同時TCP接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - **接続のタイムアウト**を定義： アプリ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。
    - **接続タイムアウト**： **[接続のタイムアウトを定義]**を**[オン]**に設定した場合に、アプリ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。
  - **このトンネルを通過する携帯ネットワーク接続をブロック**: ローミング中にこのトンネルをブロックするかどうか選択します。
    注： WiFiおよびUSB接続はブロックされません。

  - **クライアントポート**： クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。

- **IP 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。
- **サーバーポート**： サーバーのポート番号を入力します。

- リモートサポートを選択する場合、以下の手順を実行します。
  - **このトンネルをリモートサポートに使用**: **[オン]** に設定します。
  - **接続のタイムアウトを定義**： アプリ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。
    - **接続タイムアウト**： **[接続のタイムアウトを定義] を [オン]** に設定した場合に、アプリ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。
  - **SSL接続を使用**： このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **このトンネルを通過する携帯ネットワーク接続をブロック**: ローミング中にこのトンネルをブロックするかどうか選択します。
    注： WiFiおよびUSB接続はブロックされません。



次の設定を構成します。

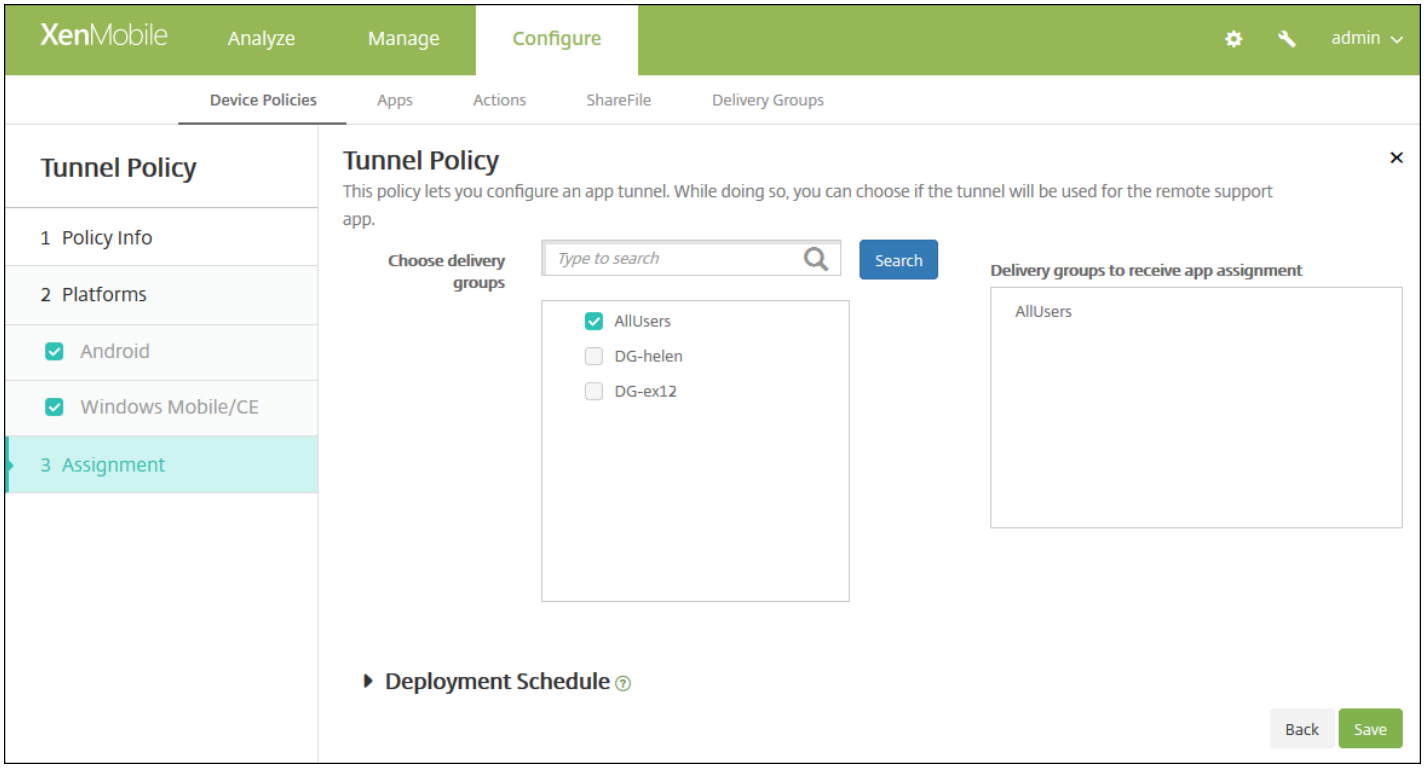
- **このトンネルをリモートサポートに使用**: トンネルをRemote Supportに利用するかどうか選択します。

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。
  - **接続を開始する側**： ［**デバイス**］または［**サーバー**］を選択して、接続の開始元を指定します。
  - **プロトコル**： 一覧から、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。
  - **接続のタイムアウト**を定義： 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。
    - **接続タイムアウト**： ［**接続のタイムアウトを定義**］を［**オン**］に設定した場合に、アプリ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。
  - **このトンネルを通過する携帯ネットワーク接続をブロック**: ローミング中にこのトンネルをブロックするかどうか選択します。
    注： WiFiおよびUSB接続はブロックされません。
  - **XenMobileにリダイレクト**： 一覧から、XenMobileへのデバイスの接続方法を選択します。デフォルトは［**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。
    - ［**IP アドレスの範囲で**］を選択した場合は、［**IP アドレスの範囲: 開始アドレス**］に開始IPアドレスを入力し、［IP アドレスの範囲: 終了アドレス］に終了IPアドレスを入力します。
  - **クライアントポート**： クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
  - **IP 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。
  - **サーバーポート**： サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - **このトンネルをリモートサポートに使用**: ［**オン**］に設定します。
  - **接続のタイムアウト**を定義： アプリ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。
    - **接続タイムアウト**： ［接続のタイムアウトを定義］を［オン］に設定した場合に、アプリ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。
  - **SSL接続を使用**： このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **このトンネルを通過する携帯ネットワーク接続をブロック**: ローミング中にこのトンネルをブロックするかどうか選択します。
    注： WiFiおよびUSB接続はブロックされません。

7. 展開規則を構成します。

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] の一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

アプリケーションアンインストールデバイスポリシー

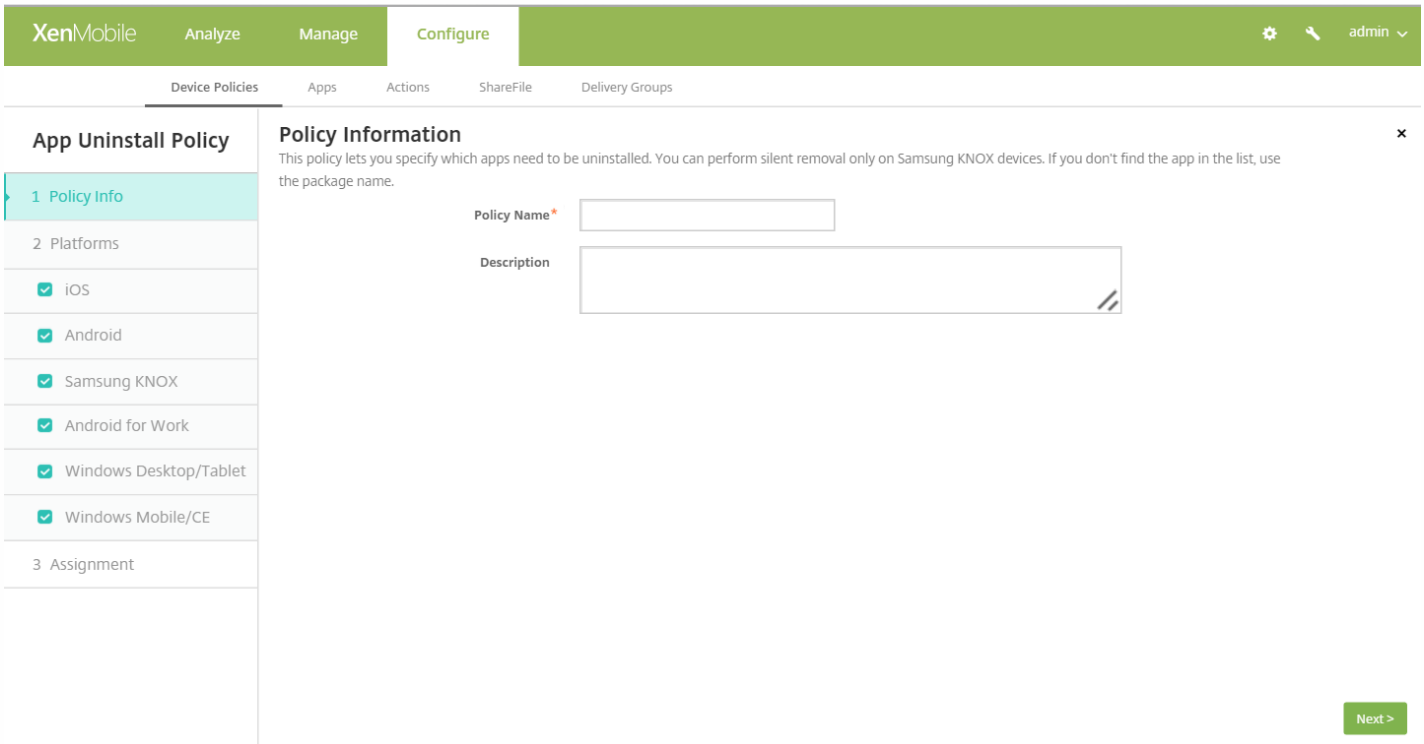
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[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。



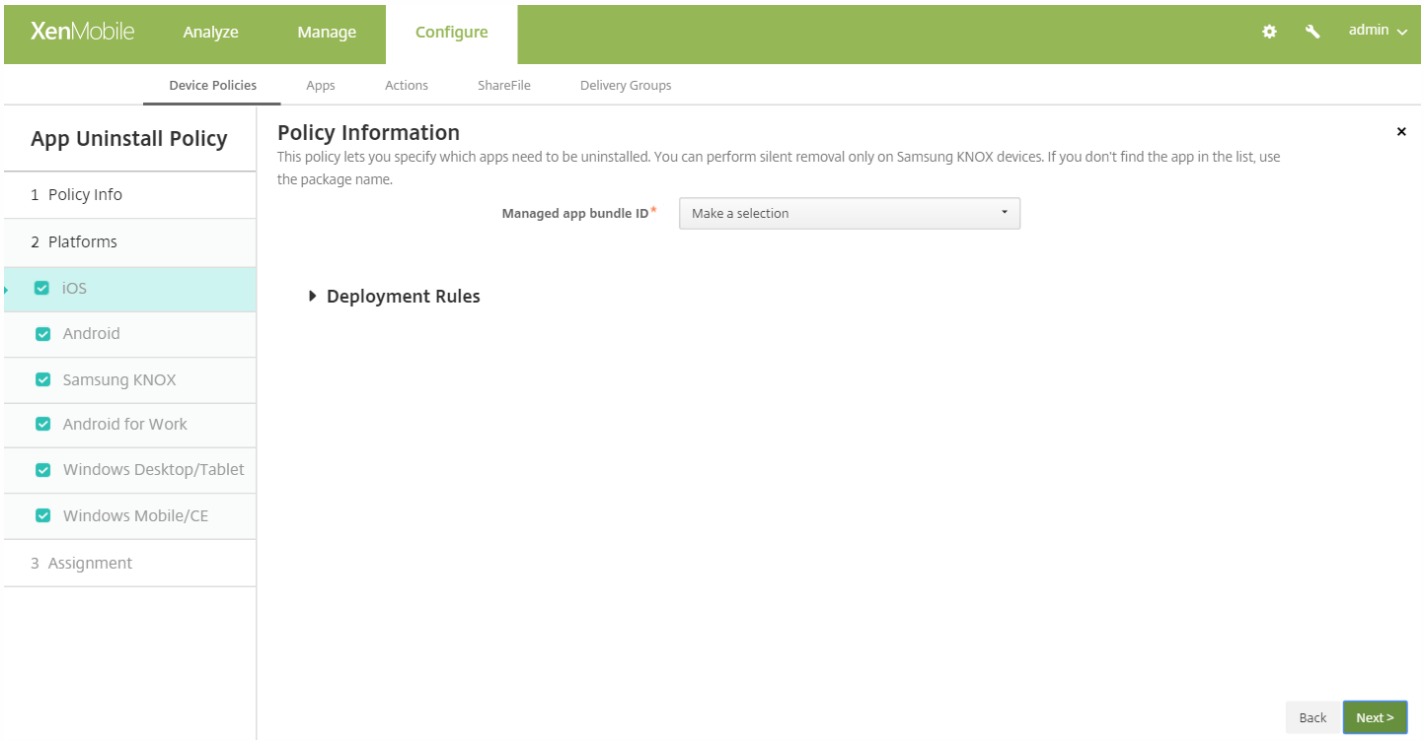
4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。**[Policy Platforms]** ページが開きます。

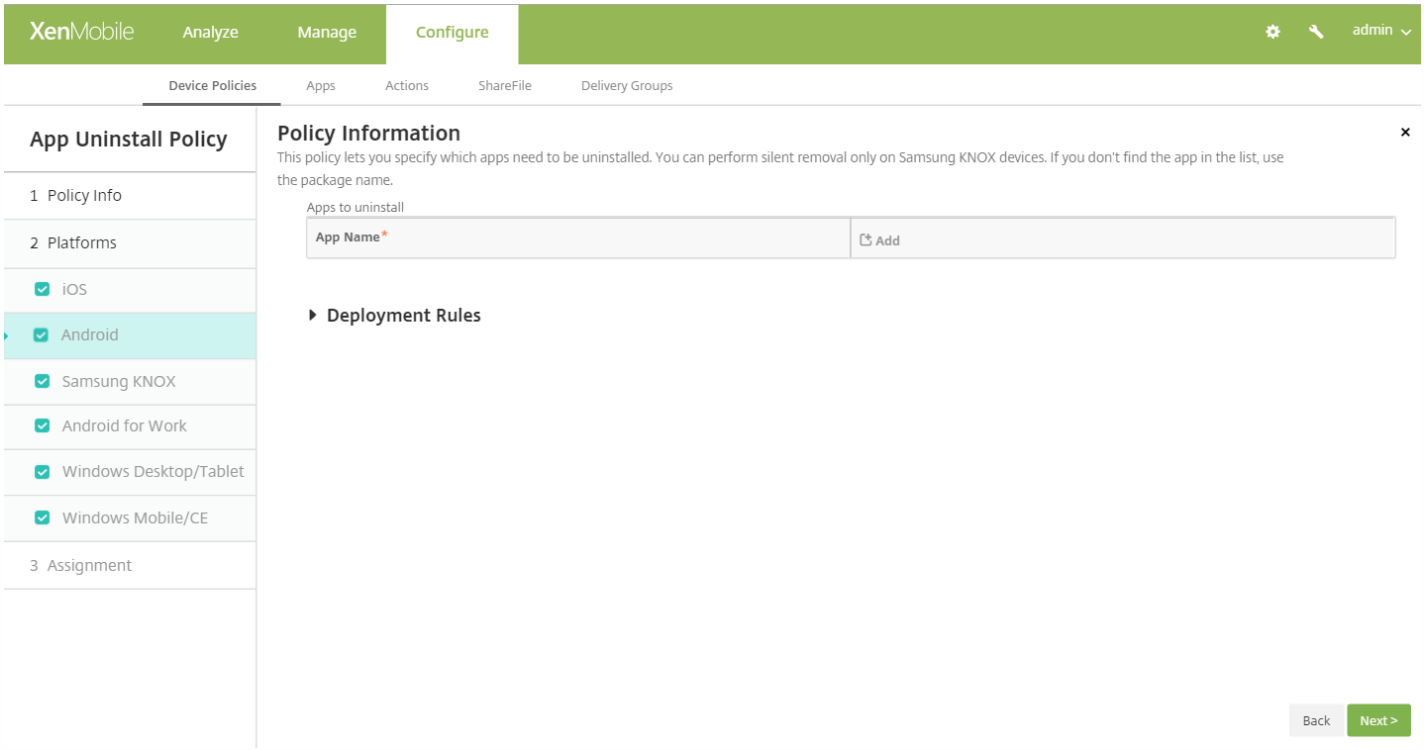
6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



次の設定を構成します。

- **管理対象アプリのバンドルID**：一覧で、既存のアプリケーションを選択するか、**[新規追加]**をクリックします。このプラットフォームに対してアプリ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。



次の設定を構成します。

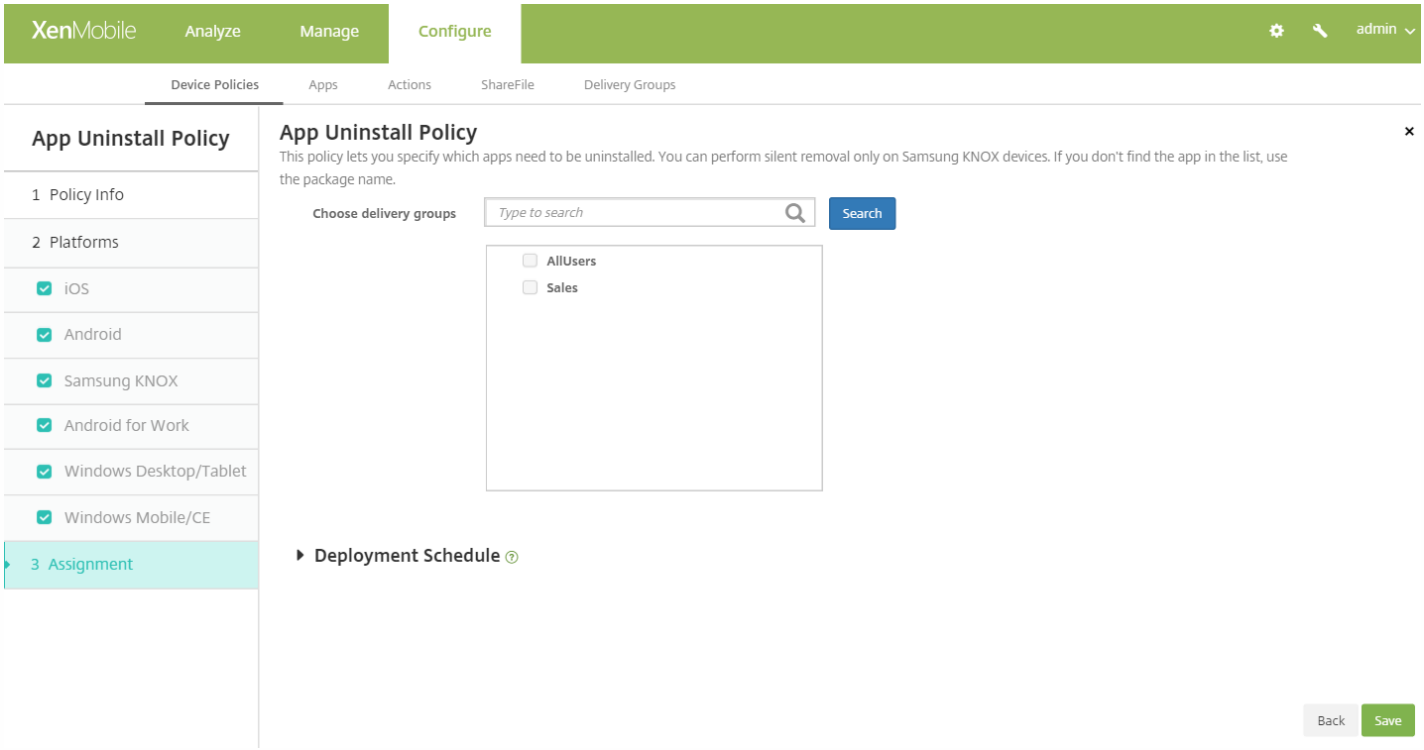
- Apps to uninstall： 構成パラメーターごとに、［Add］をクリックして以下の操作を行います。
  - **アプリ名**： 一覧で既存のアプリケーションを選択するか、**［新規追加］**をクリックして新しいアプリケーション名を入力します。このプラットフォームに対してアプリケーションが構成されていない場合は一覧が空になるため、新しいアプリケーションを追加する必要があります。
  - **［追加］**をクリックしてアプリケーションを追加するか、**［キャンセル］**をクリックしてアプリケーションの追加を取り消します。

    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. 展開規則を構成します。

8. **［次へ］**をクリックします。**［アプリアンインストールポリシー］**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. [展開スケジュール] を展開して以下の設定を構成します。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[オフ] を選択した場合、そのほかのオプションを構成する必要はありません。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、[以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [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 [オフ] です。

注：

- このオプションは、[設定] の [サーバープロパティ] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[常時接続に対する展開] は適用されません。

11. [保存] をクリックします。

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

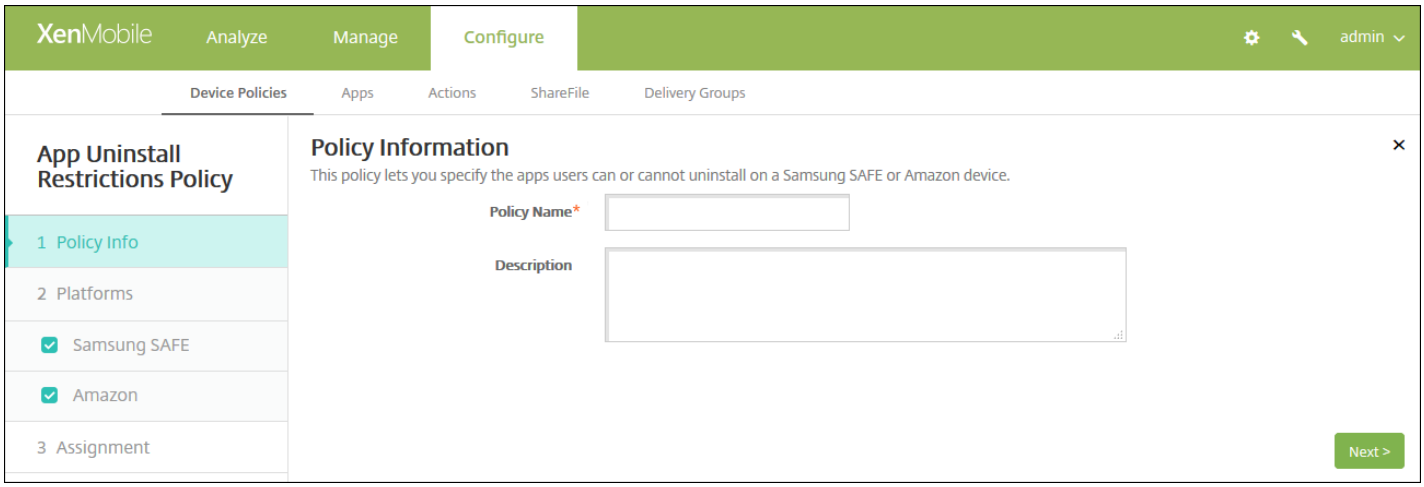
Feb 27, 2017

ユーザーにSamsung SAFEデバイスまたはAmazonデバイスでのアンインストールを許可する、または許可しないアプリ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. ［追加］をクリックします。［新しいポリシーの追加］ダイアログボックスが開きます。

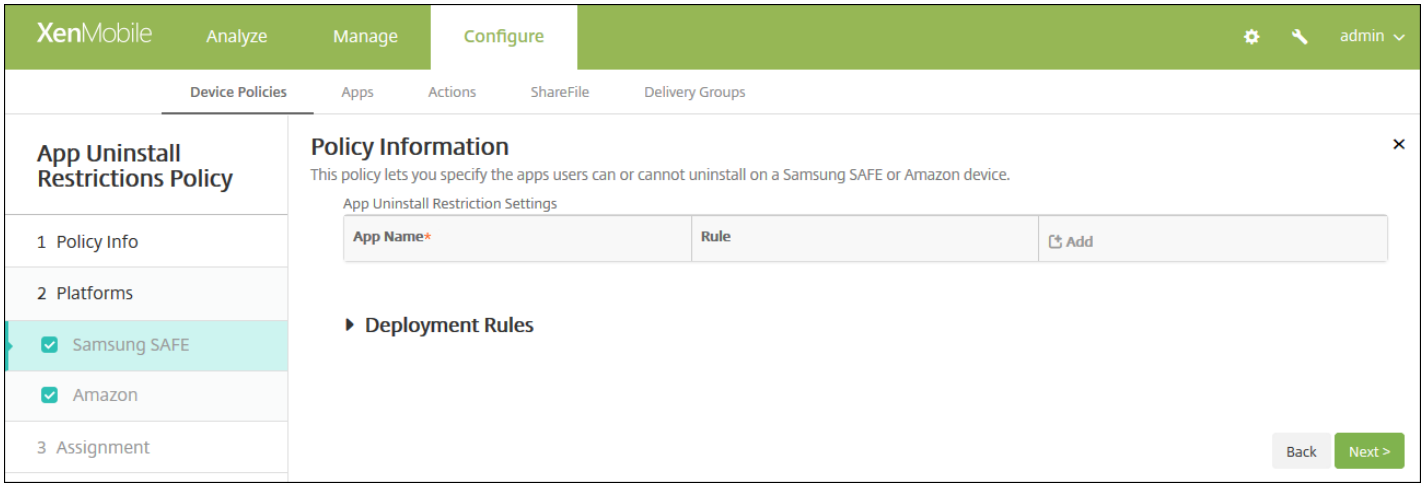
3. ［More］を展開し、［Apps］で［AppUninstall Restrictions］をクリックします。［App Uninstall Restrictions Policy］情報ページが開きます。



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。
- **説明**：任意で、ポリシーの説明を入力します。

5. ［次へ］をクリックします。［Policy Platforms］ページが開きます。



6. [プラットフォーム] で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

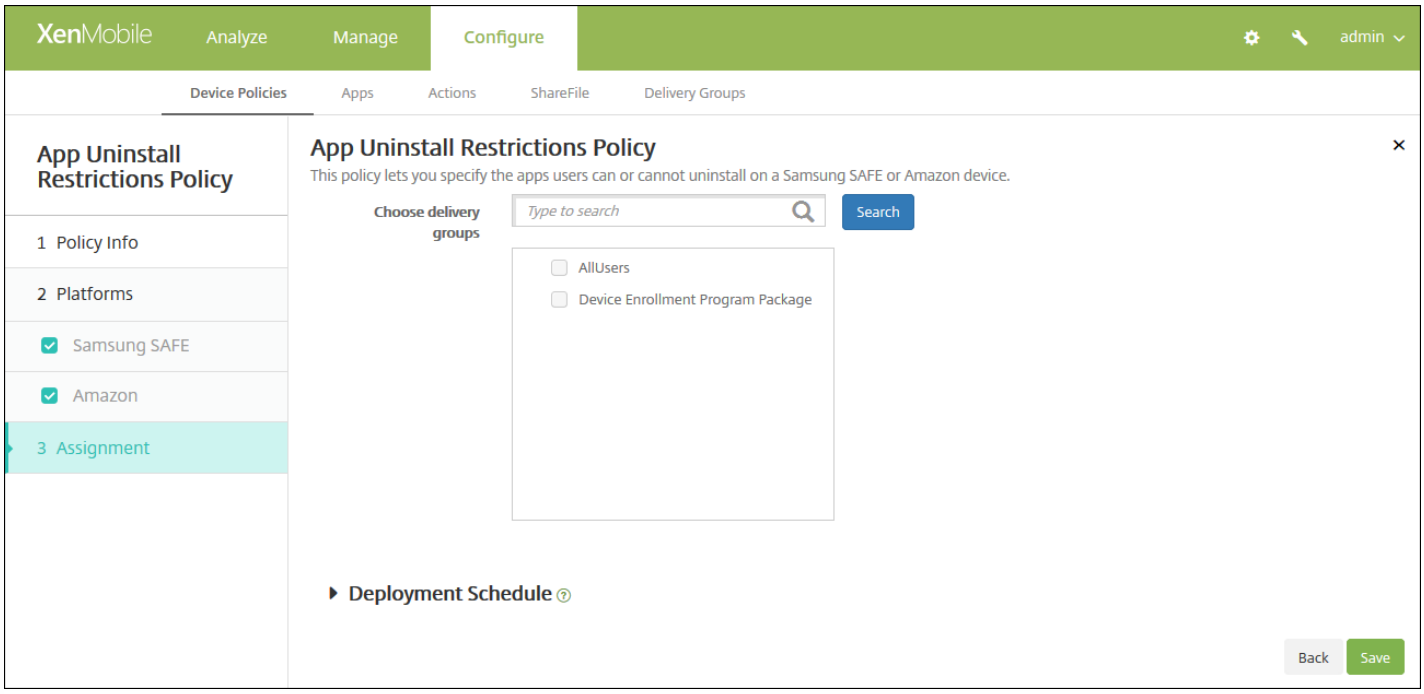
- App Uninstall Restrictions Settings： 追加するアプリ規則ごとに、 [Add] をクリックして以下の操作を行います。
  - App Name： 一覧でアプリをクリックするか、または [新規追加] をクリックして新しいアプリを追加します。
  - ： ユーザーがアプリをアンインストールできるかどうかを選択します。 デフォルトの設定ではアンインストールが許可されています。
  - [Save] または [Cancel] をクリックします。

    注： 既存のアプリを削除するには、その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. 展開規則を構成します。

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。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[オフ] を選択した場合、そのほかのオプションを構成する必要はありません。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [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。
- [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

注：

- このオプションは、[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。

12. [Save] をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

モバイルデバイスポリシー

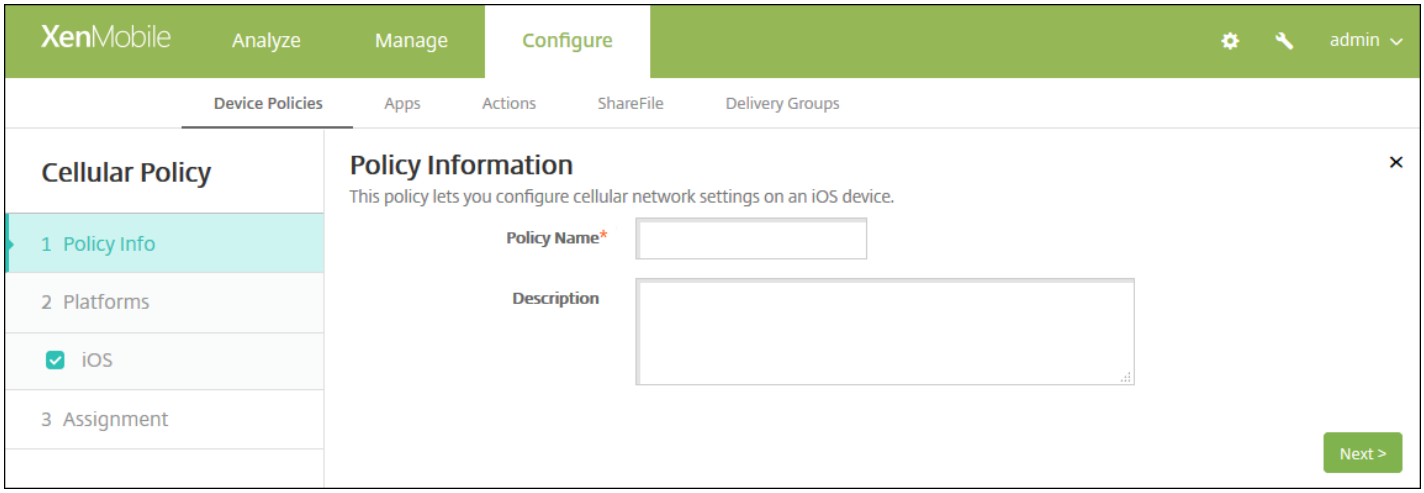
Feb 27, 2017

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、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。

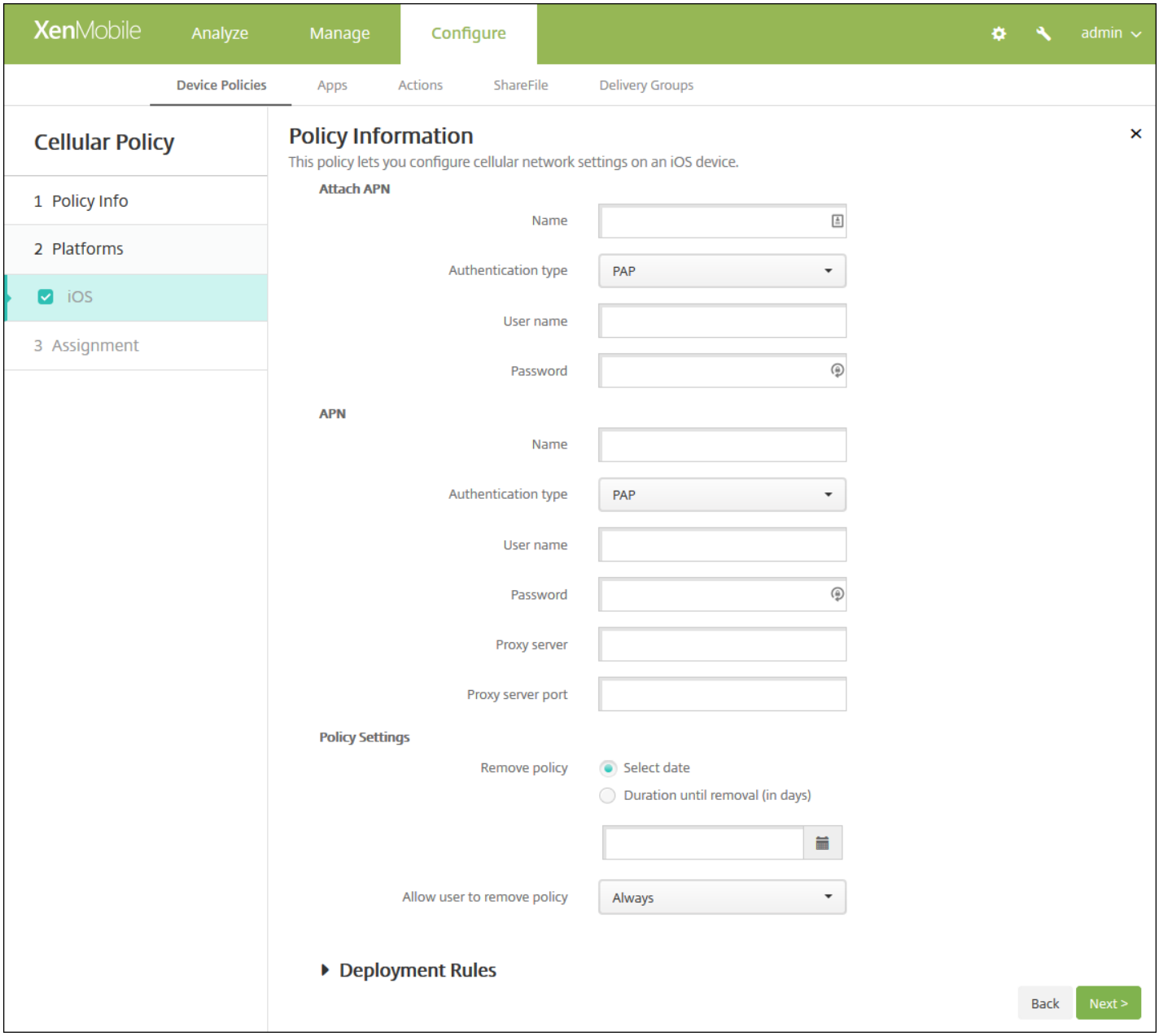
3. **[More]** を展開した後、**[Network Access]** の下の **[Celluar]** をクリックします。**[Cellular Network Policy]** 情報ページが開きます。



4. **[ポリシー情報]** 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。

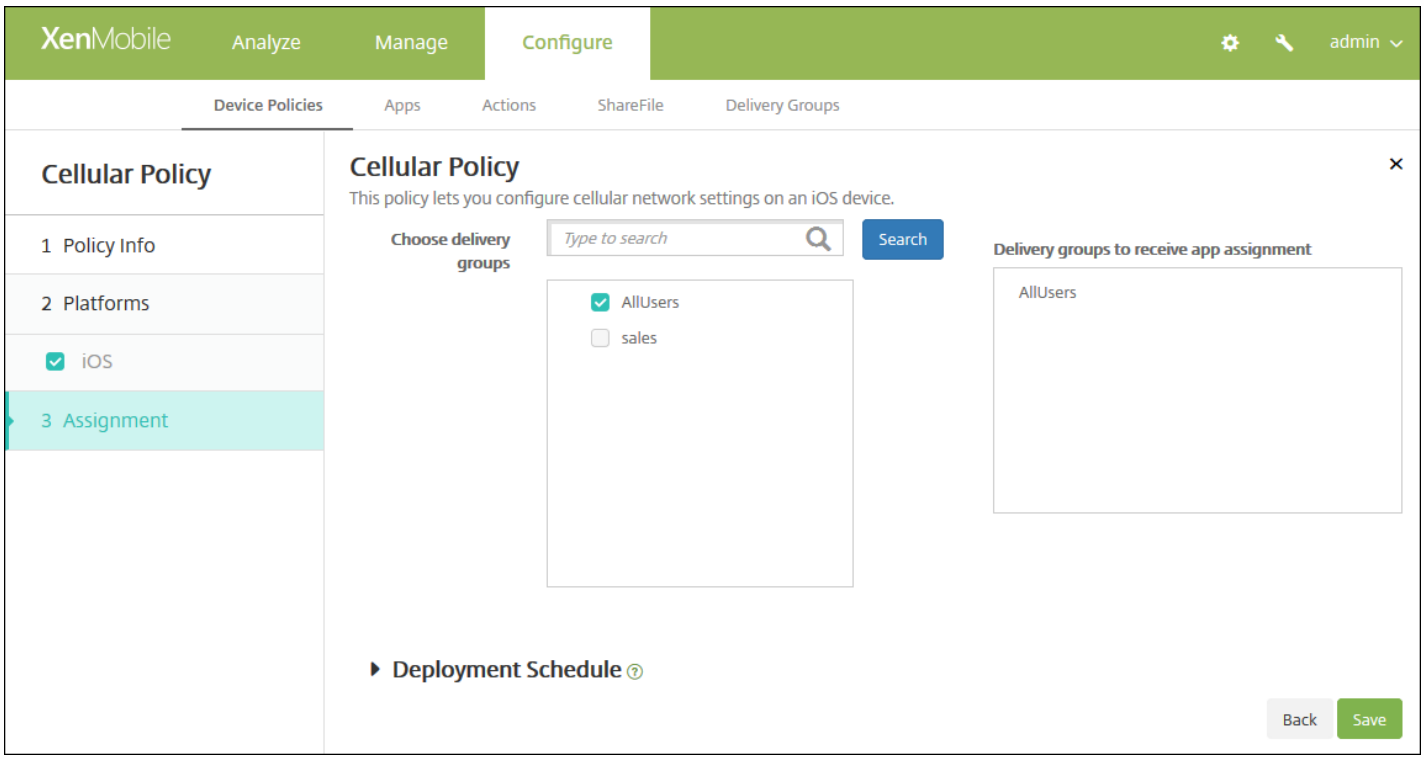
- **APNをアタッチ**
  - **Name**：この構成の名前を入力します。
  - **Authentication type**：一覧から、**[CHAP]**（Challenge-Handshake Authentication Protocol：チャレンジハンドシェイク認証プロトコル）または**[PAP]**（Password Authentication Protocol：パスワード認証プロトコル）のいずれかを選択します。デフォルトは**[PAP]**です。
  - **User name**：認証に使用するユーザー名を入力します。
- **APN**
  - **Name**：APN（Access 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。

- **プロキシサーバー**：プロキシサーバーのネットワークアドレスを入力します。

- **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。

7. 展開規則を構成します。

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. [**デリバリーグループを選択**] 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 [**アプリ割り当てを受信するためのデリバリーグループ**] 一覧に表示されます。

10. [**展開スケジュール**] を展開して以下の設定を構成します。

- [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 [**オン**] です。 [**オフ**] 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。
- [**展開スケジュール**] の横の [**すぐに**] または [**あとで**] をクリックします。デフォルトのオプションは [**すぐに**] です。
- [**あとで**] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [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 [**オフ**] 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、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

連絡先（CardDAV）デバイスポリシー

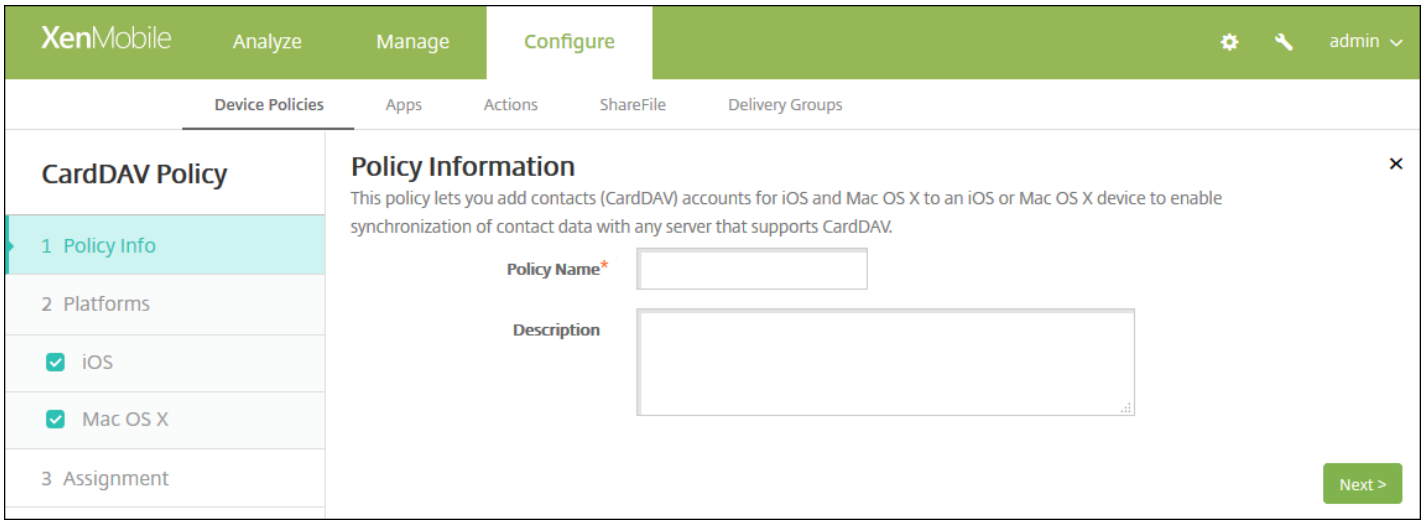
Feb 27, 2017

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、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[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。



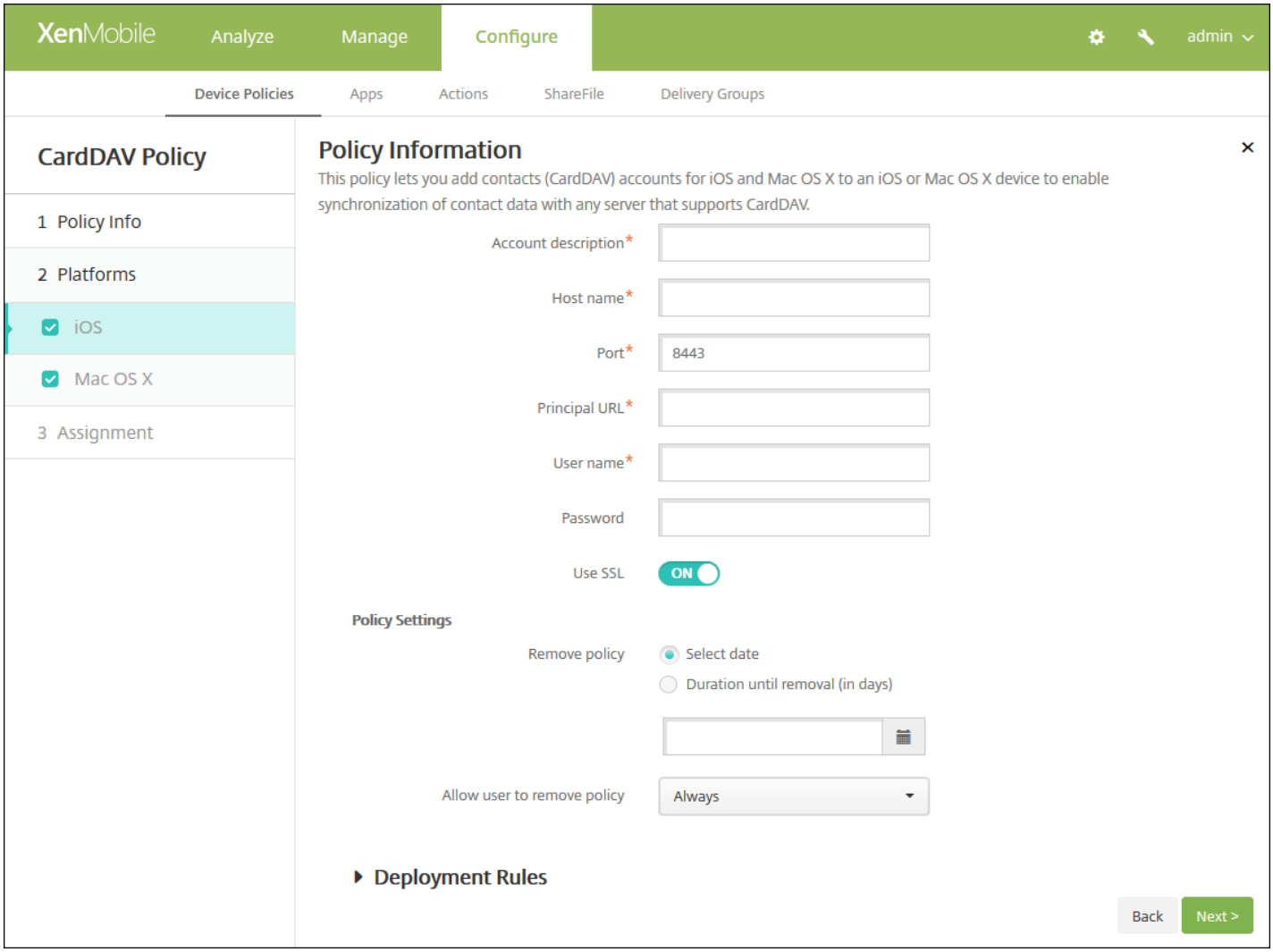
4. **[Policy Information]** ペインで、以下の情報を入力します。

- **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. **[次へ]** をクリックします。**[プラットフォーム]** ページが開きます。

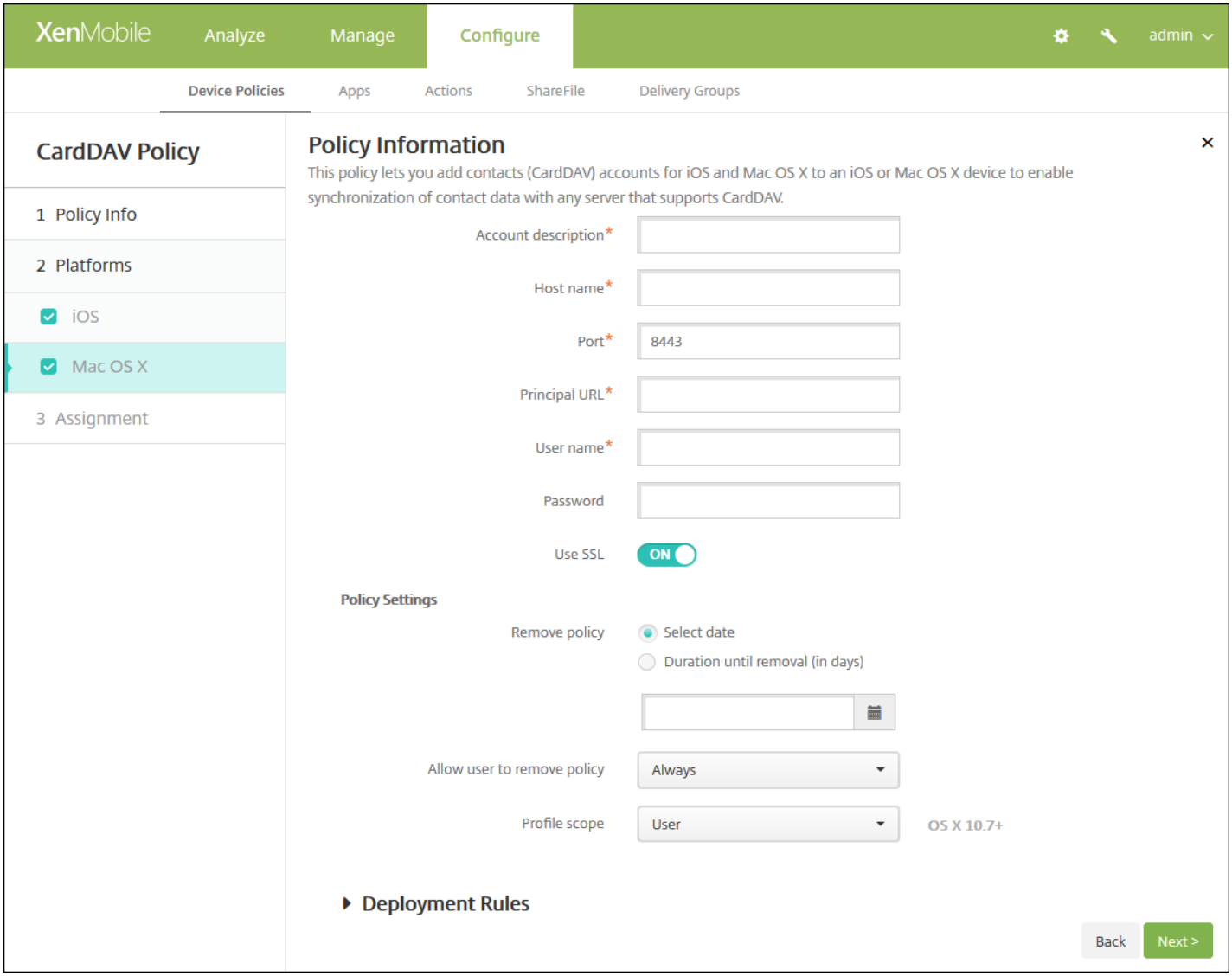
6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



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。



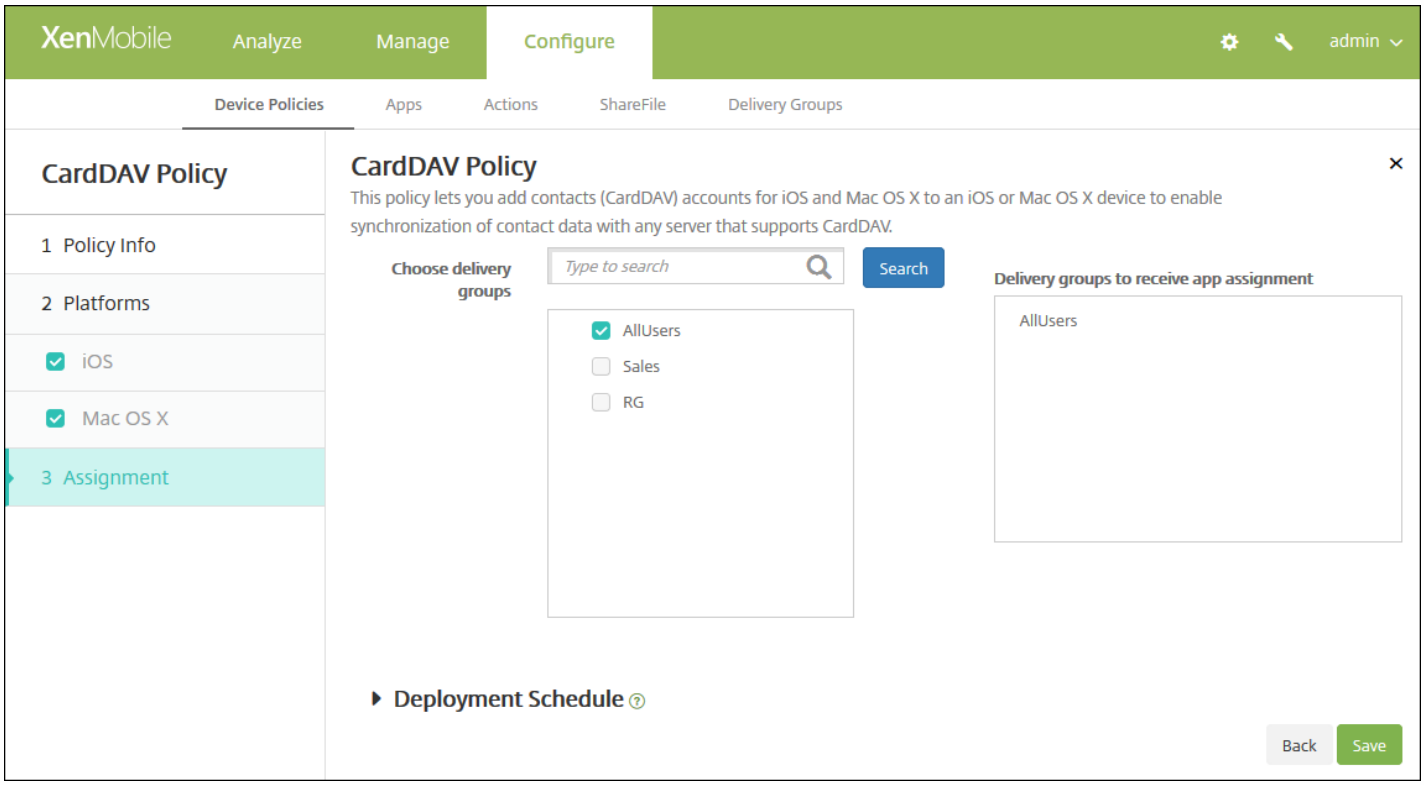
次の設定を構成します。

- **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。
  - [パスワードが必要]を選択した場合、[削除パスワード]の横に必要なパスワードを入力します。
  - [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. [次へ] をクリックします。 [CardDAVポリシー] 割り当てページが開きます。



9. [デリバリーグループを選択] の横に、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 [アプリ割り当てを受信するためのデリバリーグループ] 一覧に表示されます。

10. [展開スケジュール] を展開して以下の設定を構成します。

- [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 [オン] です。 [オフ] 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。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、 [以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、 [接続するたび] です。
- [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 [オフ] です。

注：

- このオプションは、 [設定] の [サーバープロパティ] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 [常時接続に対する展開] は適用されません。

11. **[保存]** をクリックします。

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

Feb 27, 2017

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コンテナーにサインインした場合のみ使用できます。

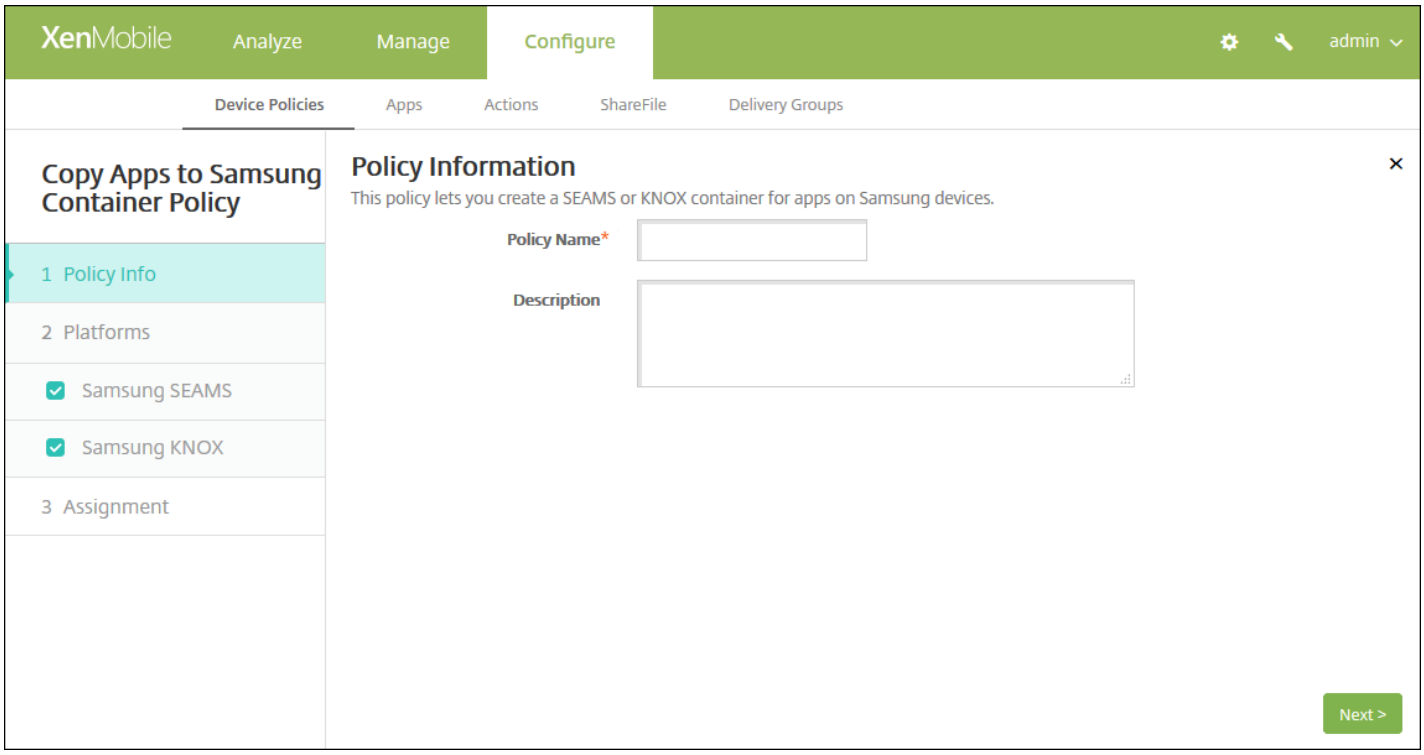
前提条件：

- 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. **［追加］**をクリックします。**［新しいポリシーの追加］**ダイアログボックスが開きます。

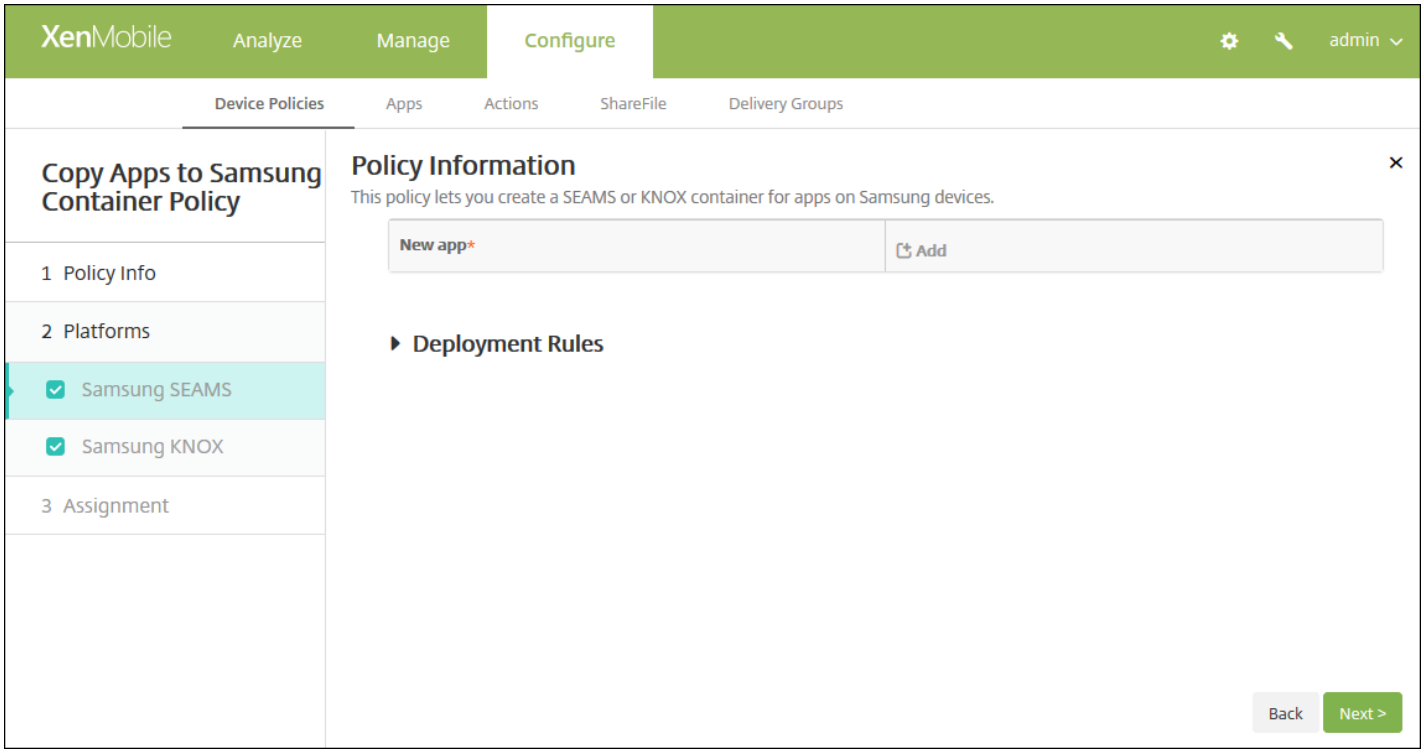
3. 3.［More］を展開し、［Security］の下の［Copy Apps to Samsung Container］をクリックします。［Copy Apps to Samsung Container Policy］情報ページが開きます。



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。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** 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. 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。

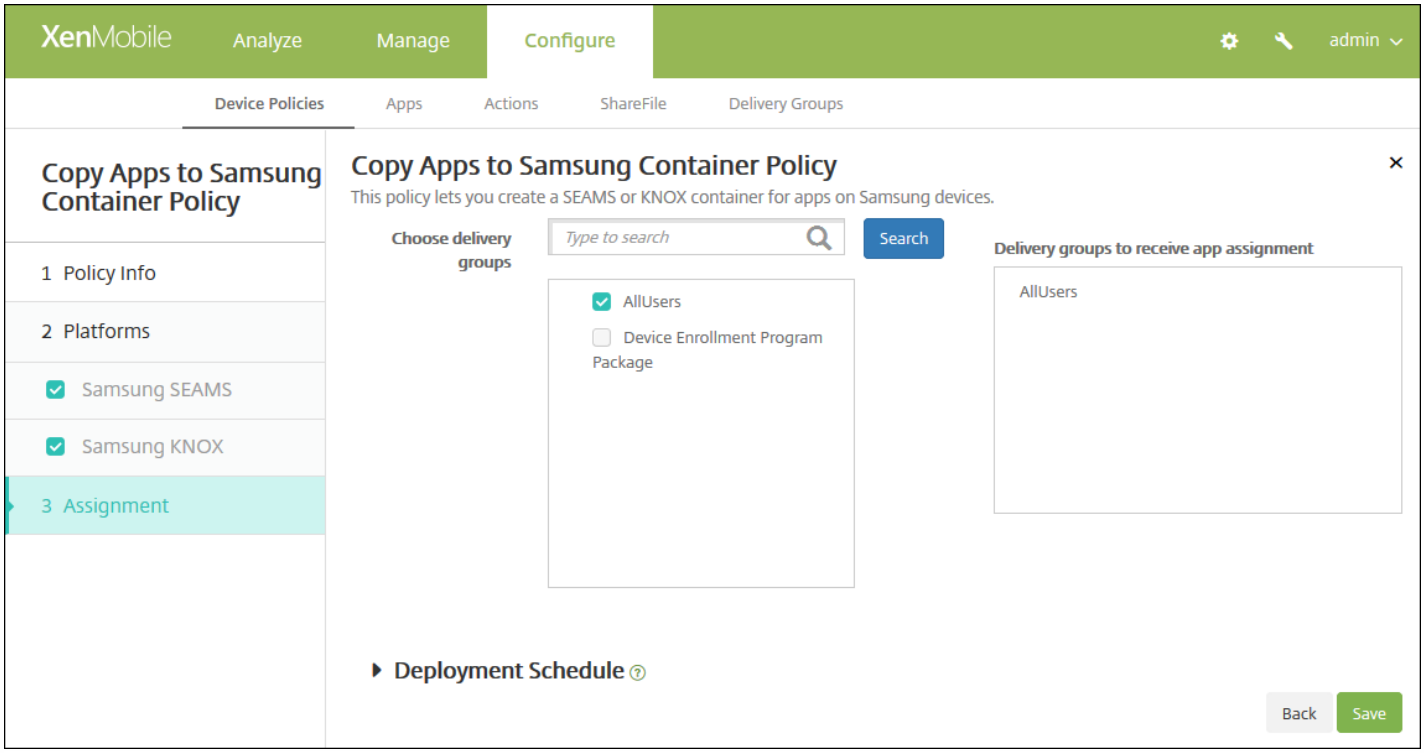
- **New app**：一覧に追加するアプリケーションごとに、 **[Add]** をクリックして以下の操作を行います。
  - パッケージIDを入力します。たとえば、LacingArtアプリの場合、「lacingart」と入力します。
  - **[Save]** または **[Cancel]** をクリックします。

    注： 既存のアプリを削除するには、その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. 展開規則を構成します。

9. **[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。



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。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。 [オフ] を選択した場合、そのほかのオプション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 [すぐに] 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。
- [展開状態] の横の [接続するたび] をクリックするか、 [以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、 [接続するたび] です。
- [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 [オフ] 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。

12. [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。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

Defenderデバイスポリシー

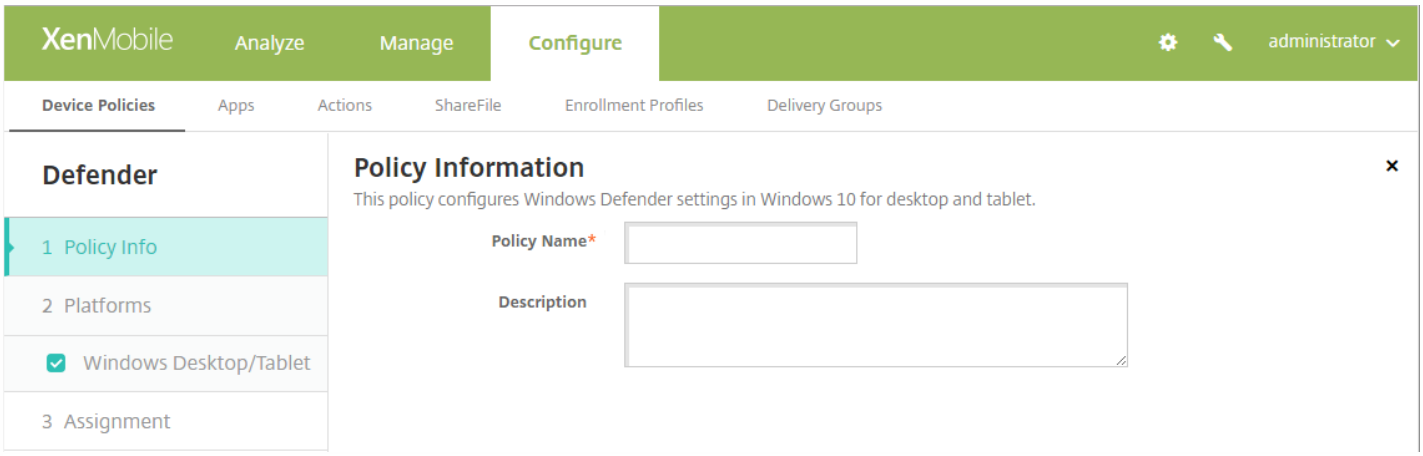
Feb 27, 2017

Windows Defenderは、Windows 10に搭載されたマルウェア対策ソフトです。XenMobileデバイスポリシーとDefenderを使ってデスクトップやタブレットのWindows 10のMicrosoft Defenderポリシーを構成できます。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

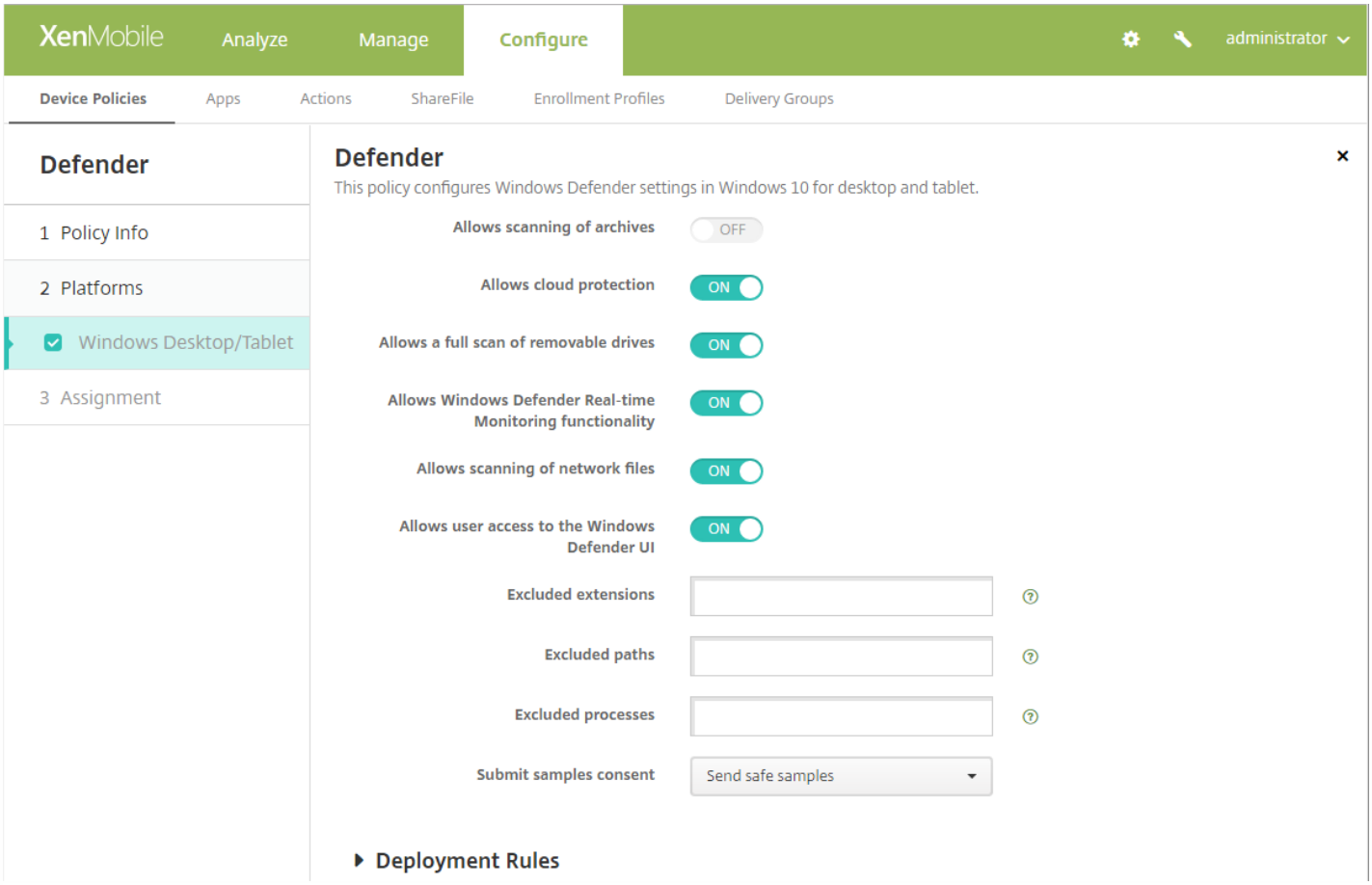
3. まず「**Defender**」と入力し、検索結果でその名前をクリックします。**[Defender ポリシー情報]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**： 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. **[次へ]** 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。

- **アーカイブのスキャンを許可する**：Defenderがアーカイブされたファイルをスキャンすることを許可するか禁止するか。デフォルトは［**オフ**］です。
- **クラウド保護を許可する**：Defenderがマルウェアの活動についてMicrosoftに情報を送信することを許可するか禁止するか。デフォルトは［**オン**］です。
- **リムーバブルドライブのスキャンを許可する**：DefenderがUSBメモリなどのリムーバブルドライブをスキャンすることを許可するか禁止するか。デフォルトは［**オン**］です。
- **Windows Defenderのリアルタイム監視機能を許可する**：デフォルトは［**オン**］です。
- **ネットワークファイルのスキャンを許可する**：Defenderがネットワークファイルをスキャンすることを許可するか禁止するか。デフォルトは［**オン**］です。
- **ユーザーに Windows DefenderのUIへのアクセスを許可する**：ユーザーがWindows Defenderのユーザーインターフェイスにアクセスできるかどうかを指定します。この設定はユーザーデバイスを再起動しないと有効になりません。この設定が［**オフ**］の場合、ユーザーにWindows Defenderの通知は配信されません。デフォルトは［**オン**］です。
- **除外された拡張子**：リアルタイムスキャンと定期スキャンから除外する拡張子。拡張子を区切るには、「|」文字をを使用します。例、「lib|obj」。
- **除外されたパス**：リアルタイムスキャンと定期スキャンから除外するパス。パスを区切るには、「|」文字をを使用します。例、「C:\Example|C:\Example1」。
- **除外された処理**：リアルタイムスキャンと定期スキャンから除外するプロセス。プロセスを区切るには、「|」文字をを使用します。例、「C:\Example.exe|C:\Example1.exe」。
- **サンプルの提出に同意する**：不正かどうか判断するためにさらなる分析が必要な可能性のあるファイルをMicrosoftに送信するか否かを制御します。オプション：［**常に確認する**］、［**安全なサンプルを送信する**］、［**送信しない**］、［**すべて**

のサンプルを送信する]。デフォルトは、[安全なサンプルを送信する]です。

6. 展開規則を構成します。

7. [次へ]をクリックします。[Defender]割り当てページが開きます。

8. [デリバリーグループを選択]の横に、デリバリーグループを入力して検索します。ポリシーをグループに割り当てるには、一覧でグループを選択します。選択したグループが[アプリ割り当てを受信するためのデリバリーグループ]一覧に表示されます。

9. [Deployment Schedule]を展開して以下の設定を構成します。

- [展開]の横の[オン]をクリックすると展開がスケジュールされ、[オフ]をクリックすると展開が行われません。デフォルトのオプションは[オン]です。[オフ]を選択した場合、他のオプションは適用されません。
- [展開スケジュール]の横の[すぐに]または[あとで]をクリックします。デフォルトのオプションは[すぐに]です。
- [あとで]をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態]の横の[接続するたび]をクリックするか、[以前の展開が失敗した場合のみ]をクリックします。デフォルトのオプションは、[接続するたび]です。
- [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[オフ]です。

10. [Save]をクリックしてポリシーを保存します。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

デバイス正常性構成証明デバイスポリシー

Feb 27, 2017

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。

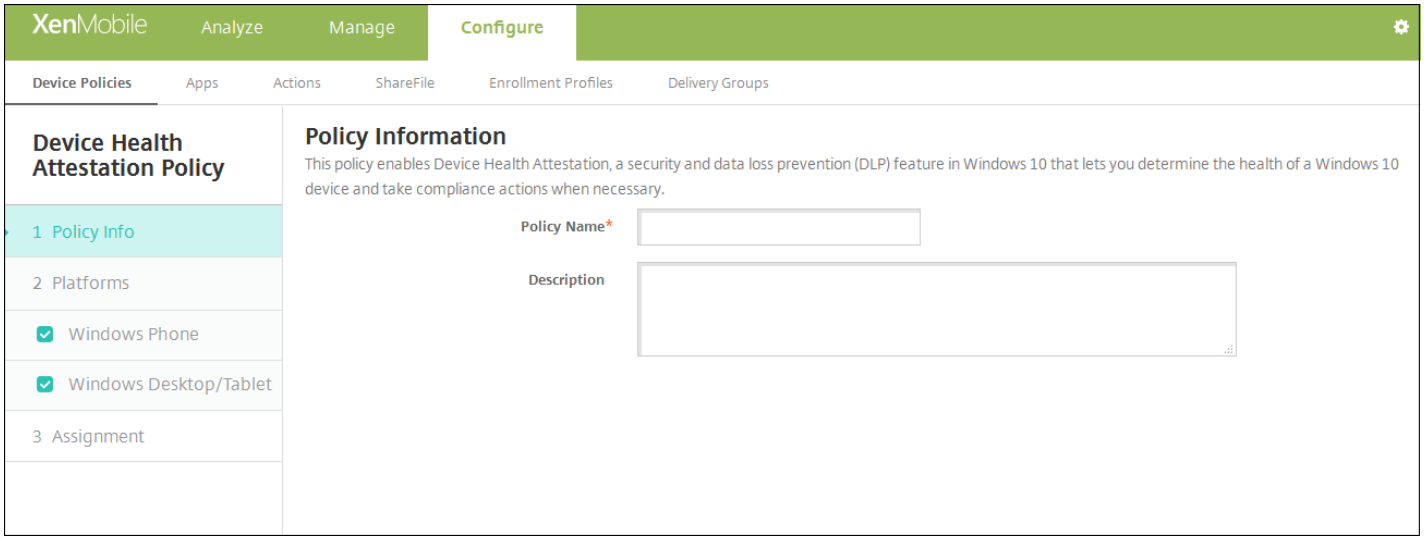
- AIKの有無
- Bit Lockerの状態
- ブートデバッグが有効化されているかどうか
- ブートマネージャーのバージョン
- コードの整合性チェックが有効化されているかどうか
- コード整合性のバージョン
- DEP ポリシー
- ELAMドライバーが起動されているかどうか
- 発行元
- カーネルのデバッグが有効化されているかどうか
- PCR
- リセット回数
- 再起動の回数
- セーフモードが有効化されているかどうか
- SBCPハッシュ
- セキュアブートが有効化されているかどうか
- テスト署名が有効化されているかどうか
- VSMが有効であること。
- WinPEが有効であること。

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、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. 新しいポリシーを追加するには **[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。



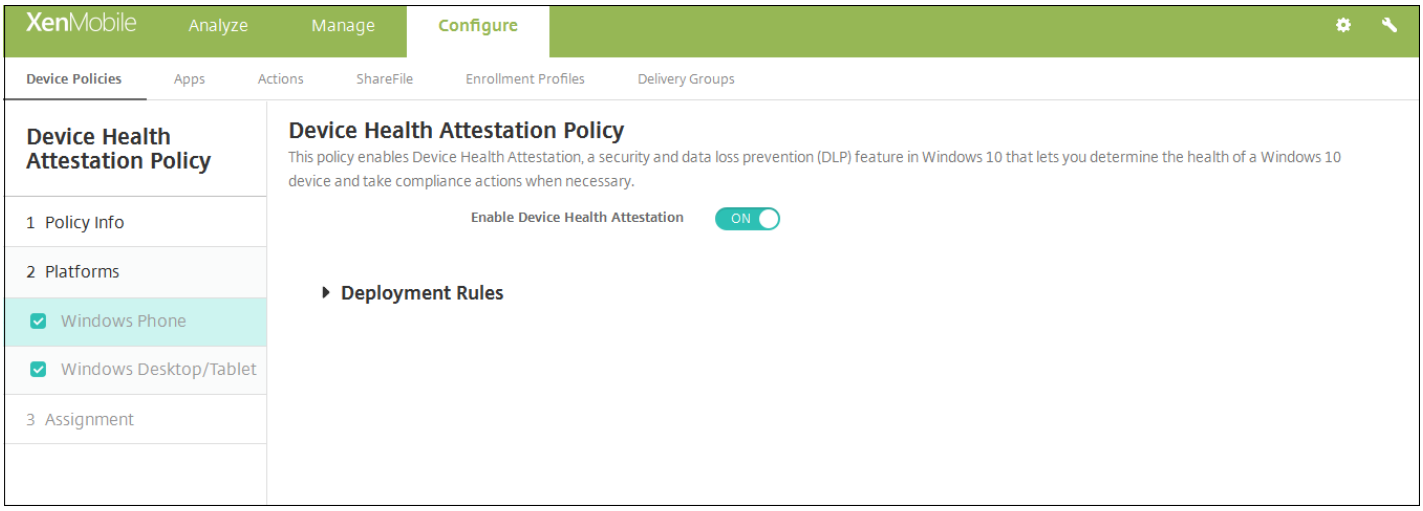
4. [Policy Information] ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. [次へ] をクリックします。 [Policy Platforms] ページが開きます。

6. [プラットフォーム] で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

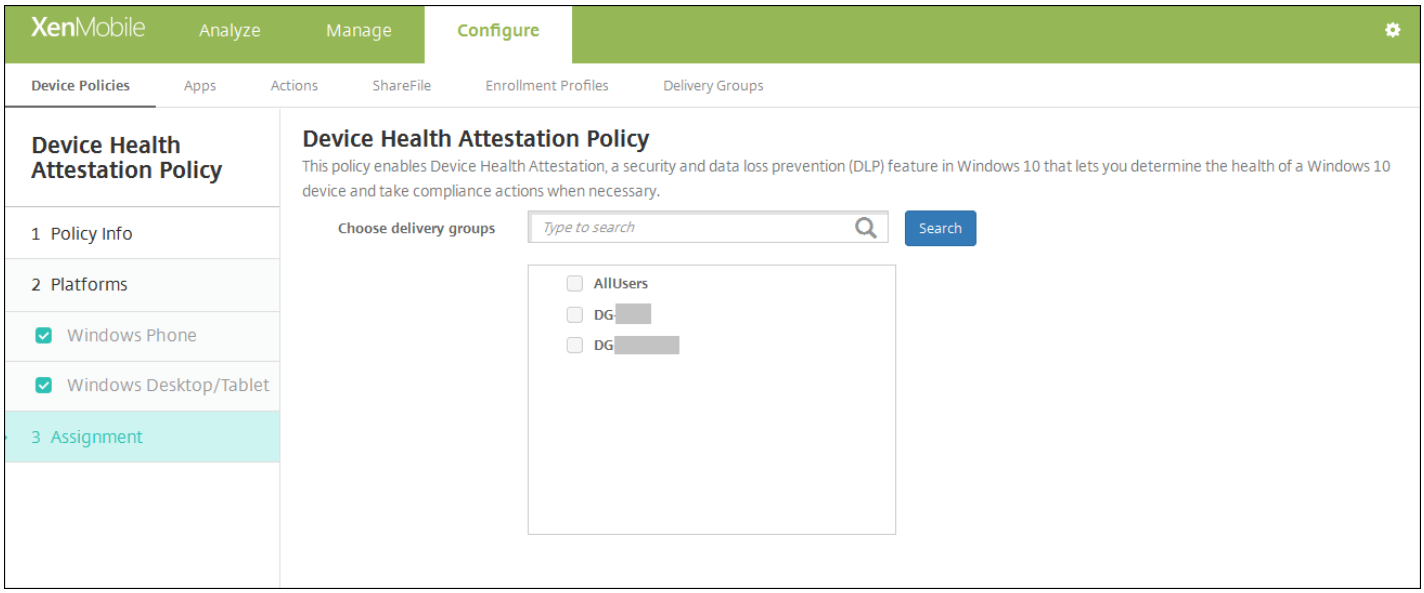


選択したプラットフォームごとに、次の設定を構成します。

- **Enable Device Health Attestation**：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. 展開規則を構成します。

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. **[デリバリーグループを選択]** 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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

デバイス名デバイスポリシー

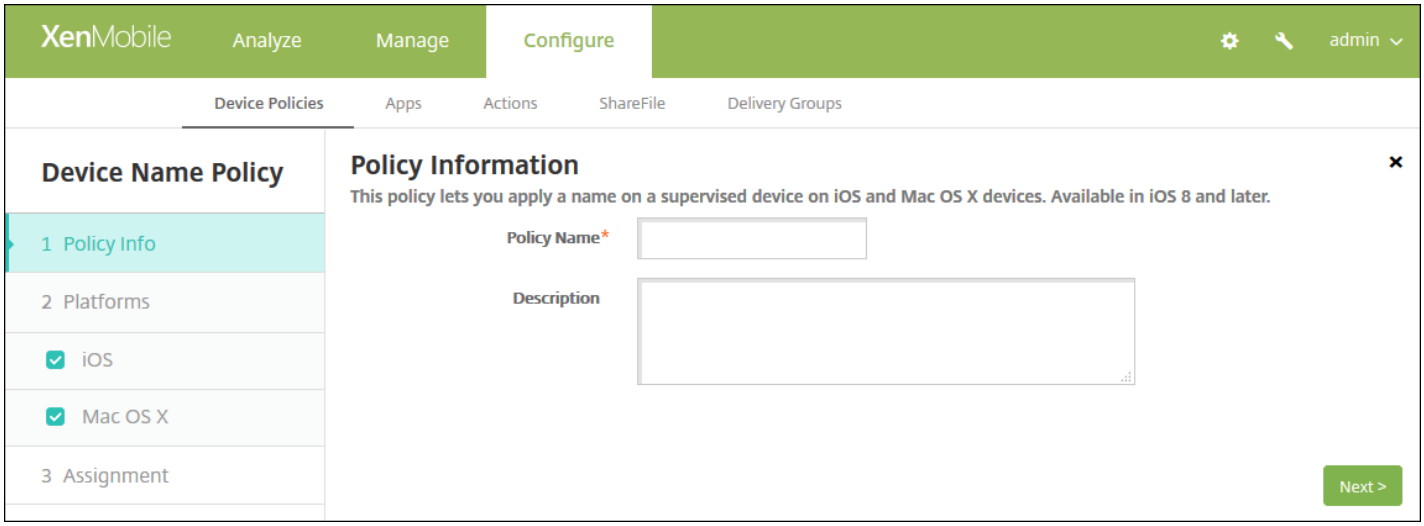
Feb 27, 2017

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番号として設定するには、${device.serialnumber}を使用します。デバイス名をユーザー名とドメインの組み合わせとして設定するには、${user.username}@example.comを使用します。マクロについて詳しくは、「XenMobileのマクロ」を参照してください。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[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。



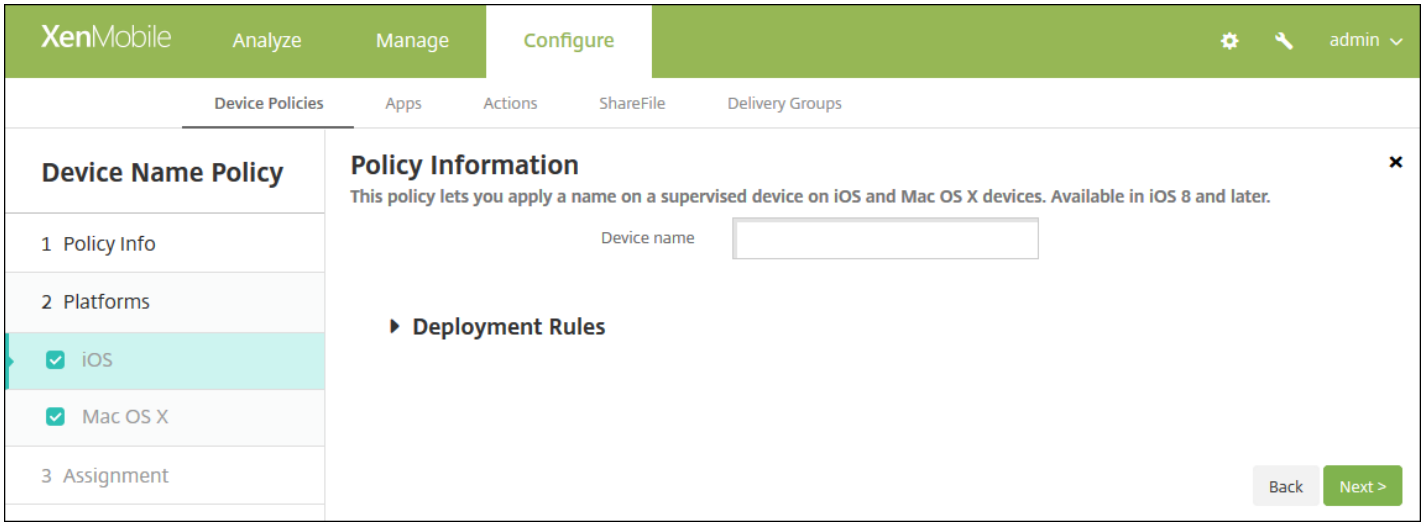
4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[Policy Platforms]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

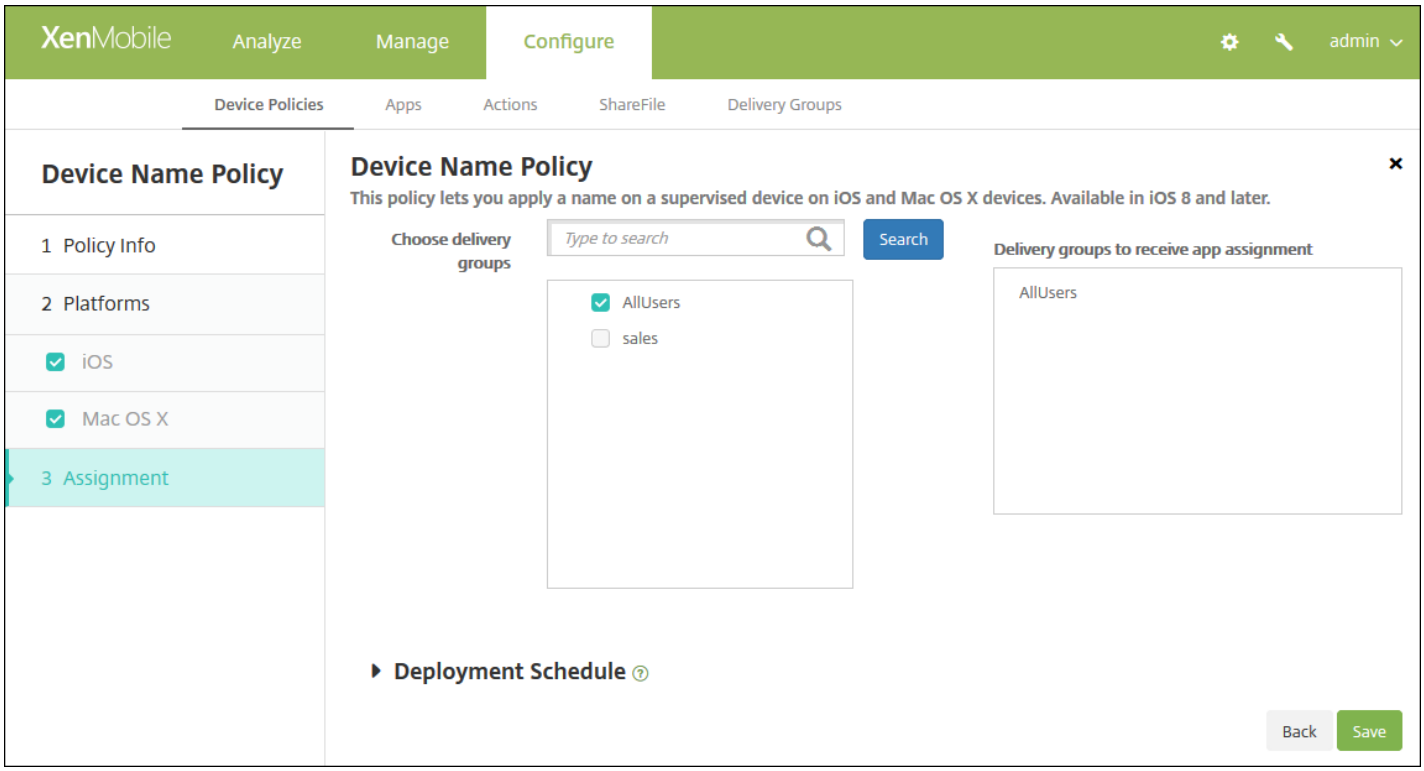


選択したプラットフォームに、次の設定を構成します。

- **デバイス名**：マクロ、複数のマクロの組み合わせ、またはマクロとテキストの組み合わせを入力して、各デバイスに一意の名前を付けます。たとえば、デバイス名を各デバイスのシリアル番号に設定するには、${device.serialnumber}を使用します。デバイス名にユーザーの名前を含めるには、${device.serialnumber} ${ user.username}を使用します。

7. 展開規則を構成します。

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. [デリバリーグループを選択] 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. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

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、**[常時接続に対する展開]** 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

Feb 27, 2017

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。

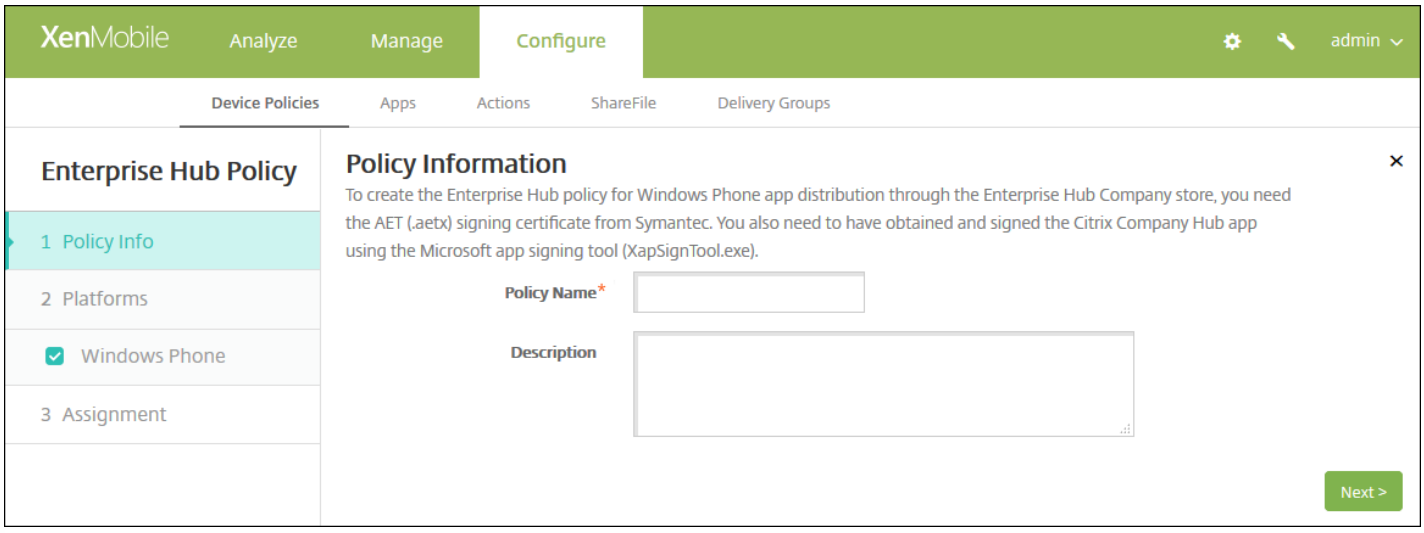
- SymantecからのAET（.aetx）署名証明書
- Microsoftのアプリケーション署名ツール（XapSignTool.exe）を使用して署名されたCitrix Company Hubアプリケーション

注： XenMobileでは、Windows Phone Secure Hubの1つのモードについて、1つのEnterprise Hubポリシーだけがサポートされています。たとえば、Windows Phone Secure Hub for XenMobile Enterprise Editionをアップロードするために、複数のEnterprise Hubポリシーをさまざまなバージョンの Work Home for XenMobile Enterprise Edition用に作成する必要はありません。デバイスの登録中に最初のEnterprise Hubポリシーを展開するだけです。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。 **[新しいポリシーの追加]** ダイアログボックスが開きます。

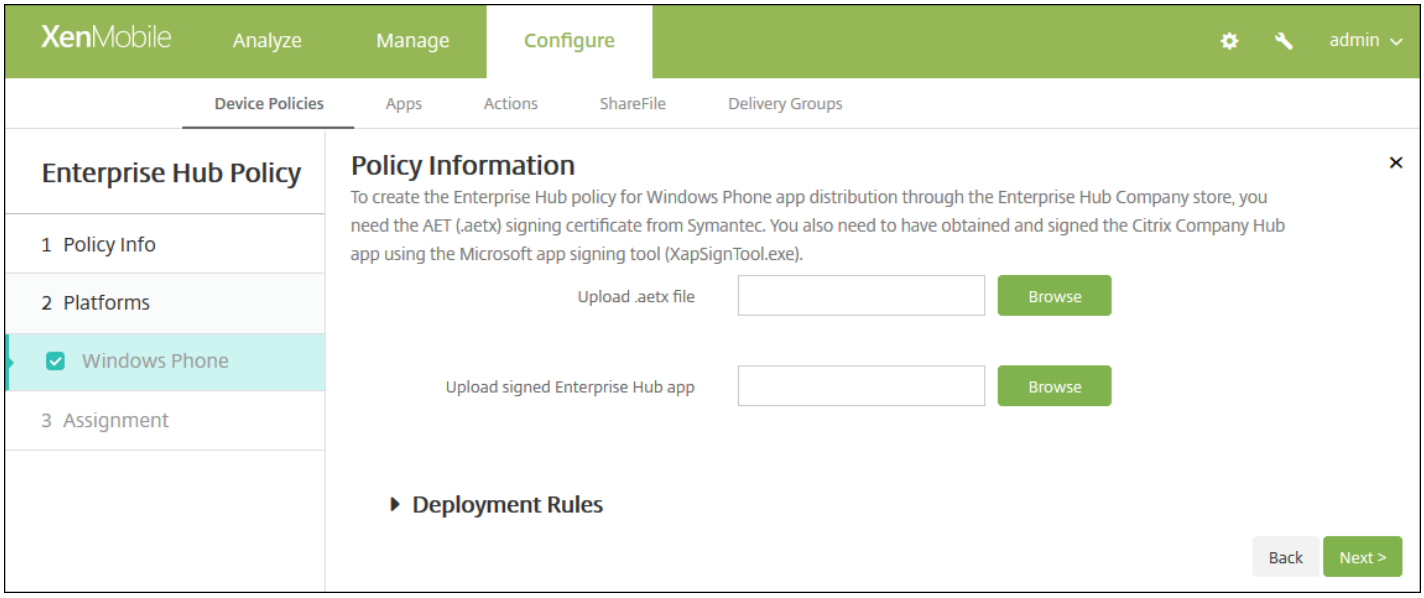
3. **[More]** をクリックした後、 **[XenMobile agent]** の下の **[Enterprise Hub]** をクリックします。 **[Enterprise Hub Policy]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：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。

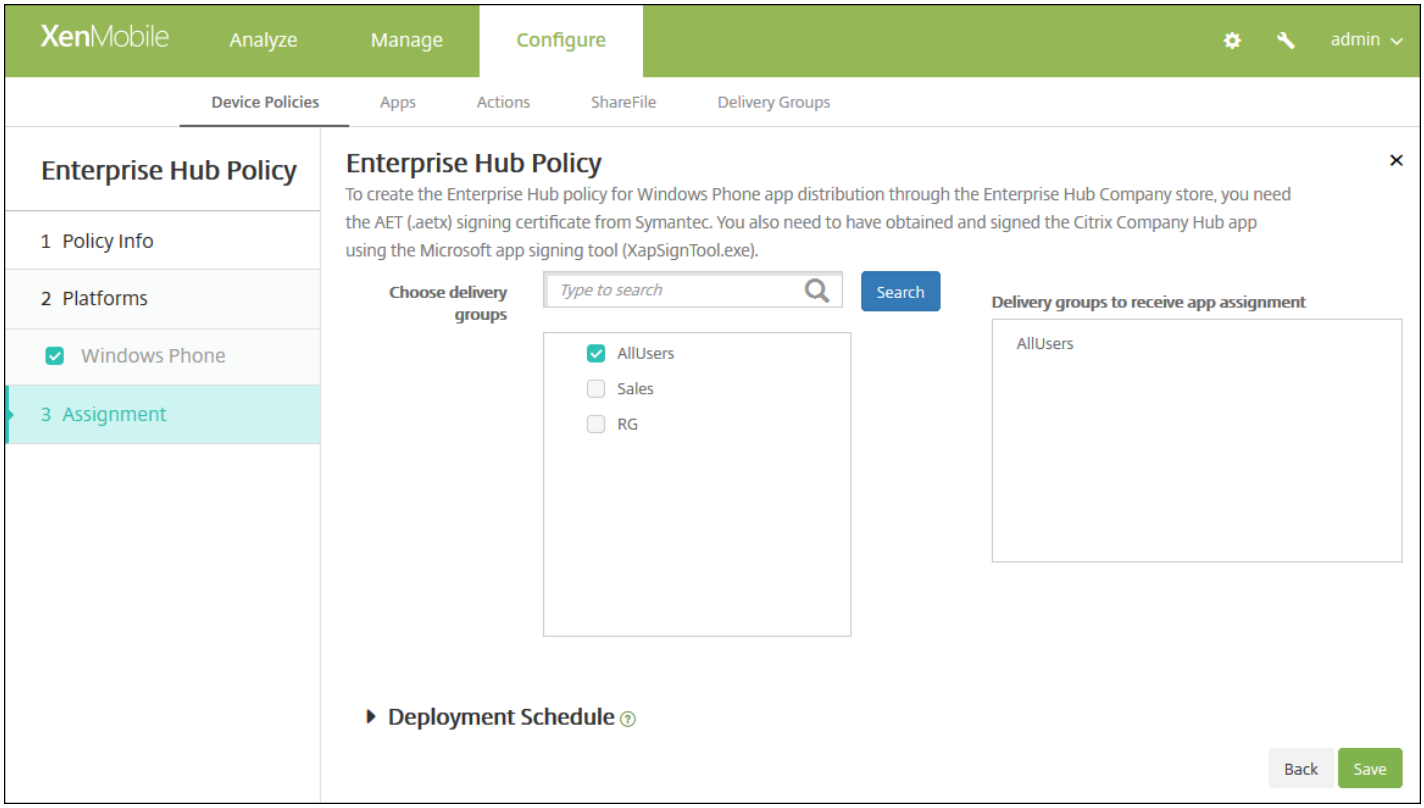


6. 次の設定を構成します。

- **.aetxファイルのアップロード：** [ブラウザー] をクリックして.aetxファイルの場所へ移動し、そのファイルを選択します。
- **署名済みエンタープライズ ハブ アプリをアップロード:** [ブラウザー] をクリックしてエンタープライズ ハブ アプリの場所へ移動し、そのアプリを選択します。

7. 展開規則を構成します。

8. [次へ] をクリックします。 [エンタープライズハブポリシー] 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. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

フォントデバイスポリシー

Feb 27, 2017

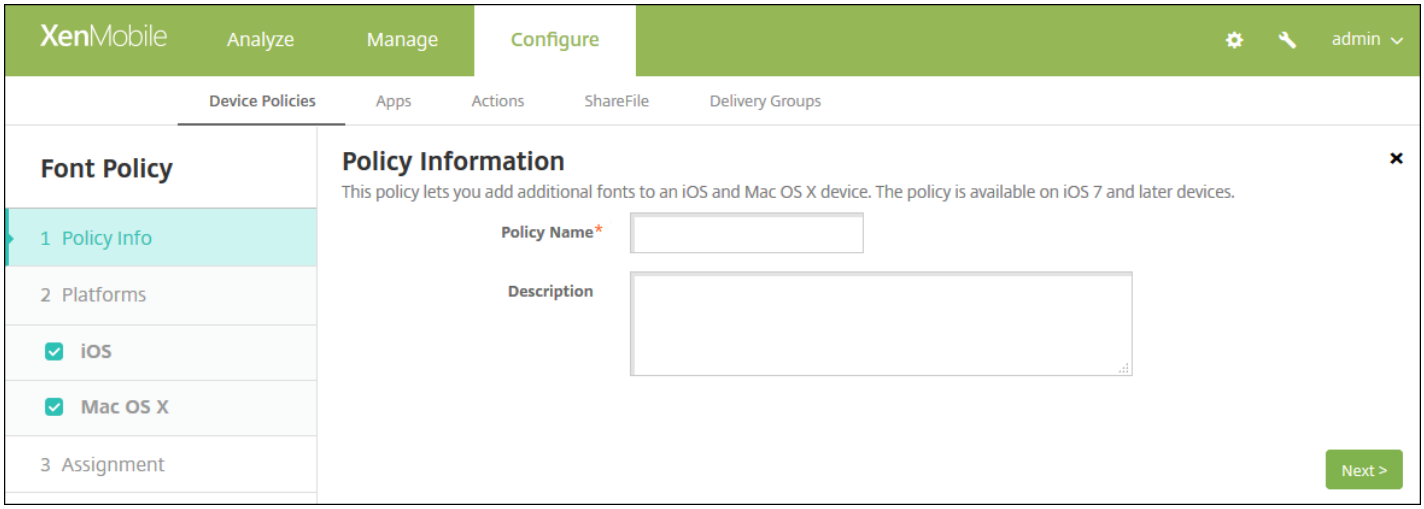
XenMobileでデバイスポリシーを追加して、追加フォントをユーザーのiOSデバイスおよびMac OS Xデバイスに追加することができます。フォントはTrueType（.ttf）またはOpenType（.oft）である必要があります。フォントコレクション（.ttcまたは.otc）はサポートされません。

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、**[構成]の[デバイスポリシー]**をクリックします。**[デバイスポリシー]**ページが開きます。

2. **[追加]**をクリックします。**[新しいポリシーの追加]**ダイアログボックスが開きます。

3. **[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。



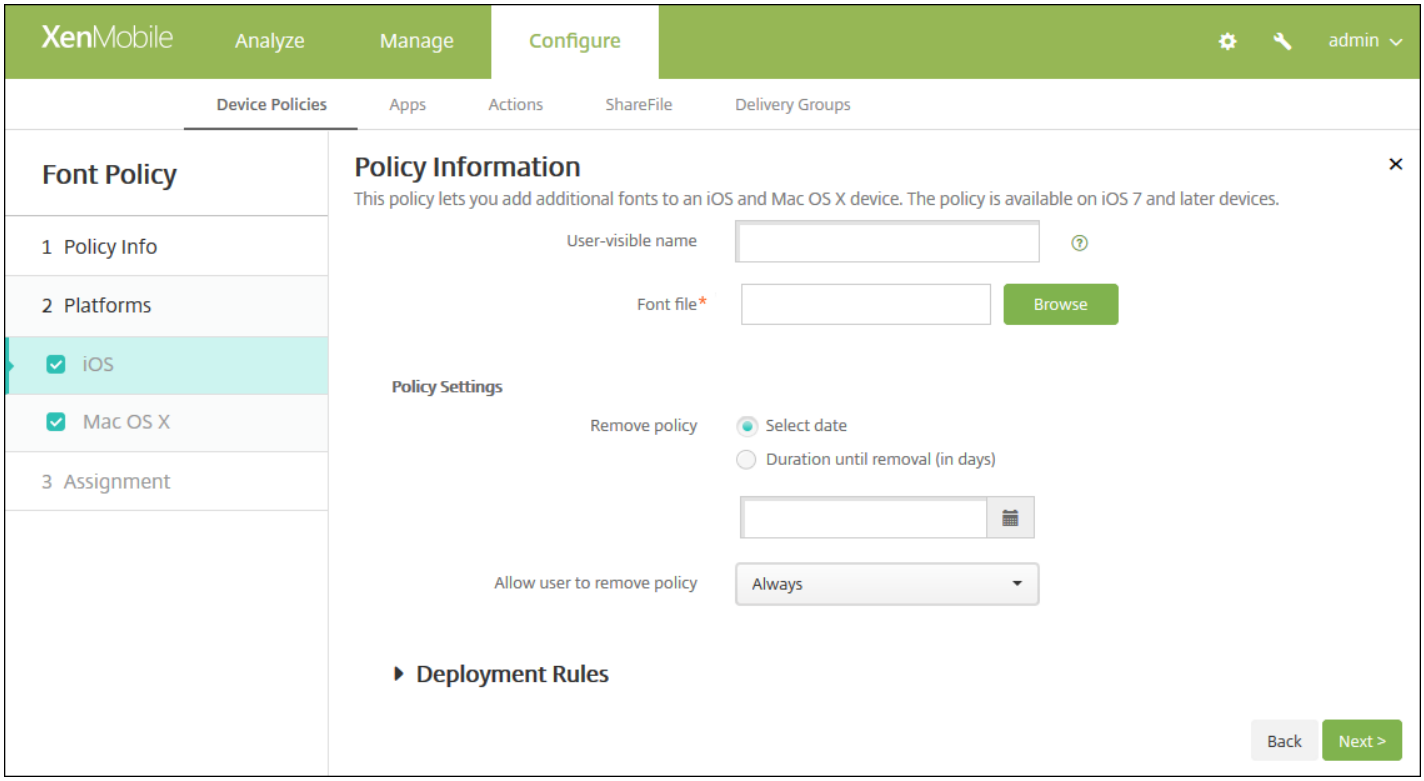
4. **[ポリシー情報]**ペインで、以下の情報を入力します。

- **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. **[次へ]**をクリックします。**[プラットフォーム]**ページが開きます。

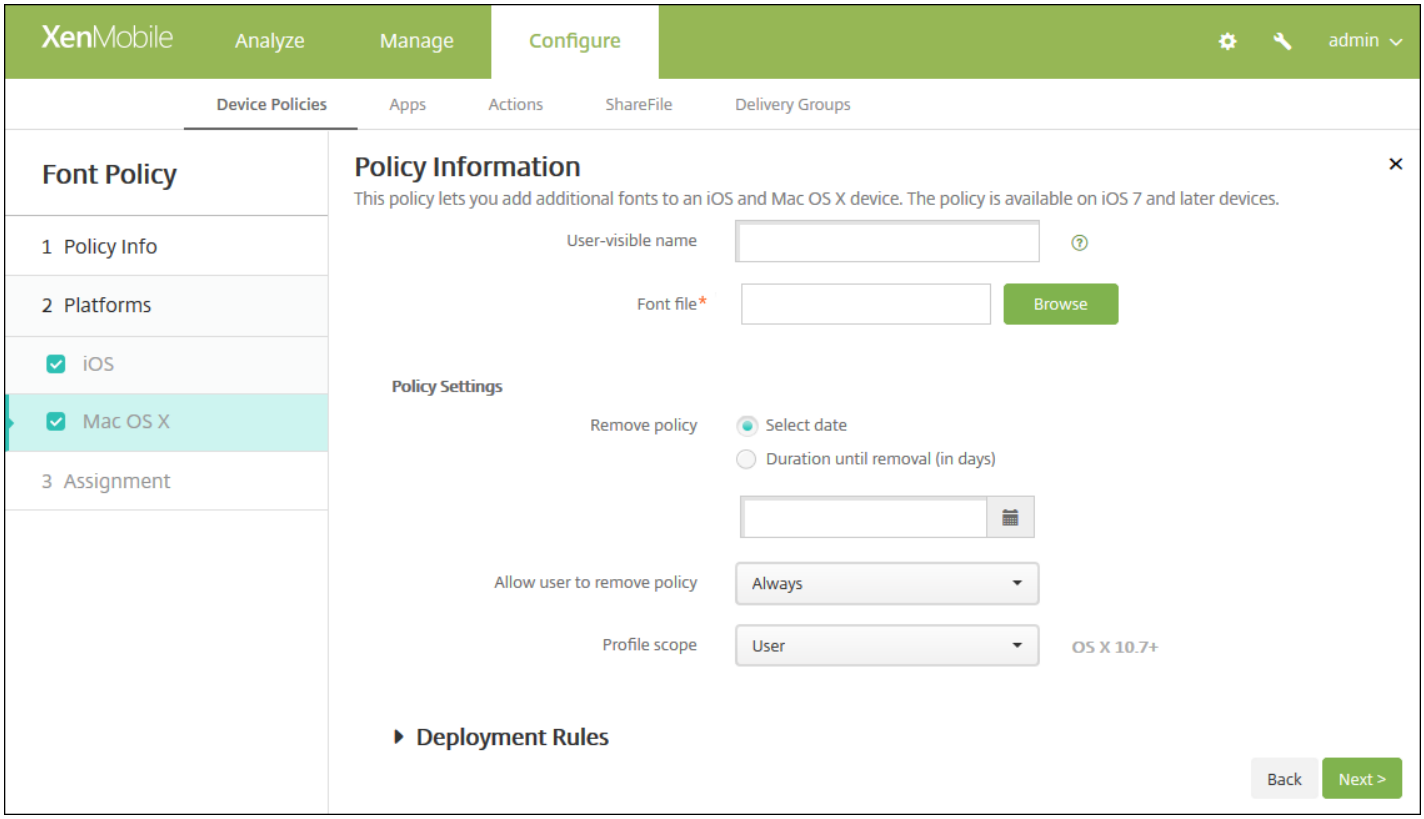
6. **[プラットフォーム]**で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



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。

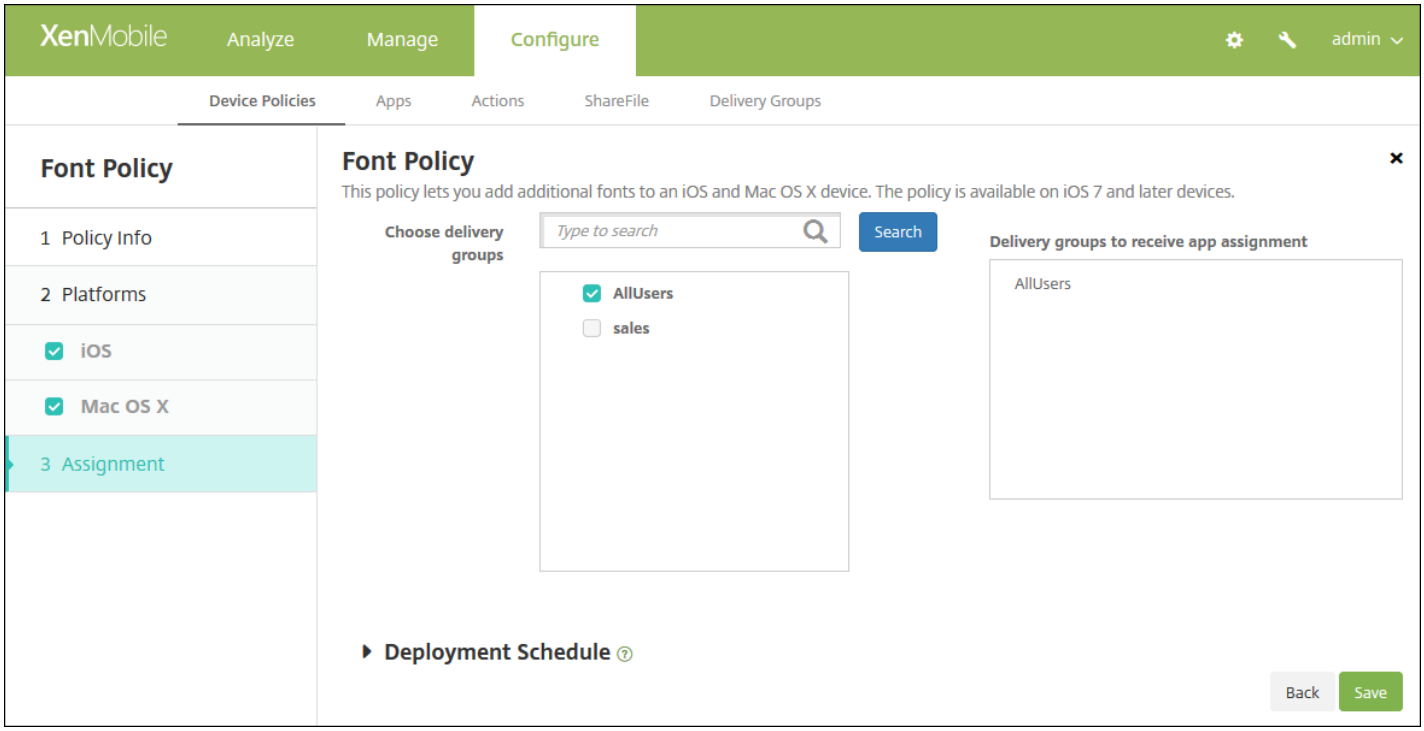


次の設定を構成します。

- 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。

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] の一覧に表示されます。

10. [展開スケジュール] を展開して以下の設定を構成します。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[オフ] 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 [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、[以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

注：

- このオプションは、[設定] の [サーバープロパティ] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[常時接続に対する展開] は適用されません。

11. [保存] をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

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

Feb 27, 2017

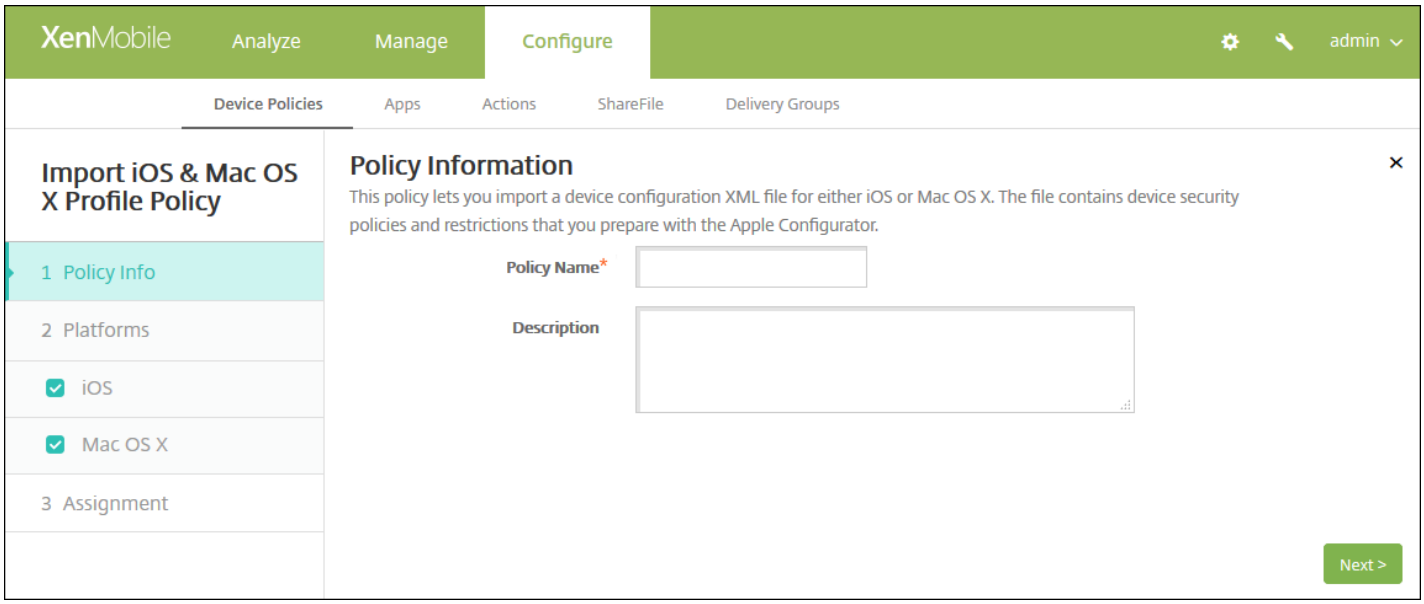
iOSおよびOS Xデバイス用のデバイス構成MXLファイルをXenMobileにインポートできます。XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。

この記事で説明するように、Apple Configuratorを使用してiOSデバイスを監視モードにできます。Apple Configuratorの使用による構成ファイルの作成について詳しくは、Appleの「Configurator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. **[追加]** をクリックします。 **[新しいポリシーの追加]** ダイアログボックスが開きます。

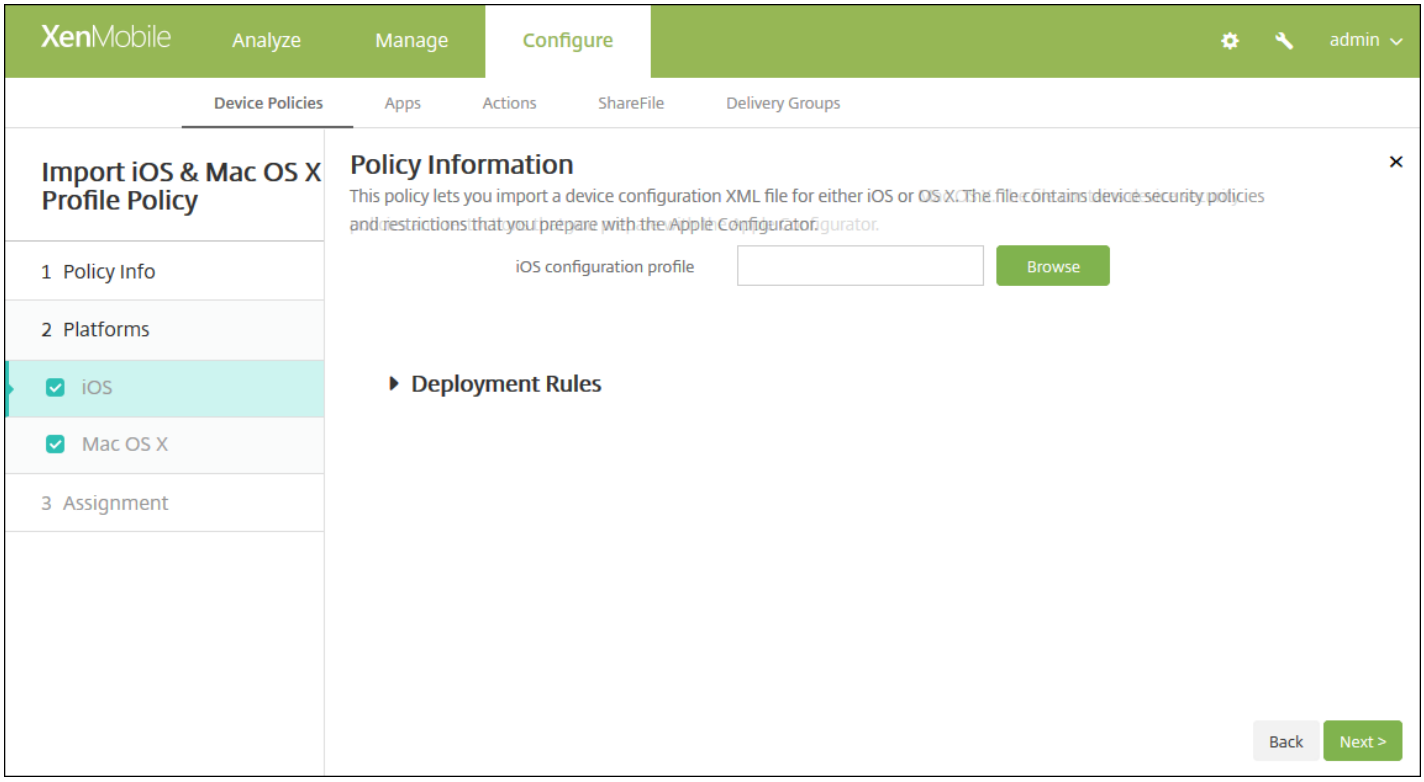
3. **[More]** を展開した後、 **[Custom]** の下の **[Import iOS & Mac OS X Profile]** をクリックします。 **[Import iOS & Mac OX X Profile Policy]** 情報ページが開きます。



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。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

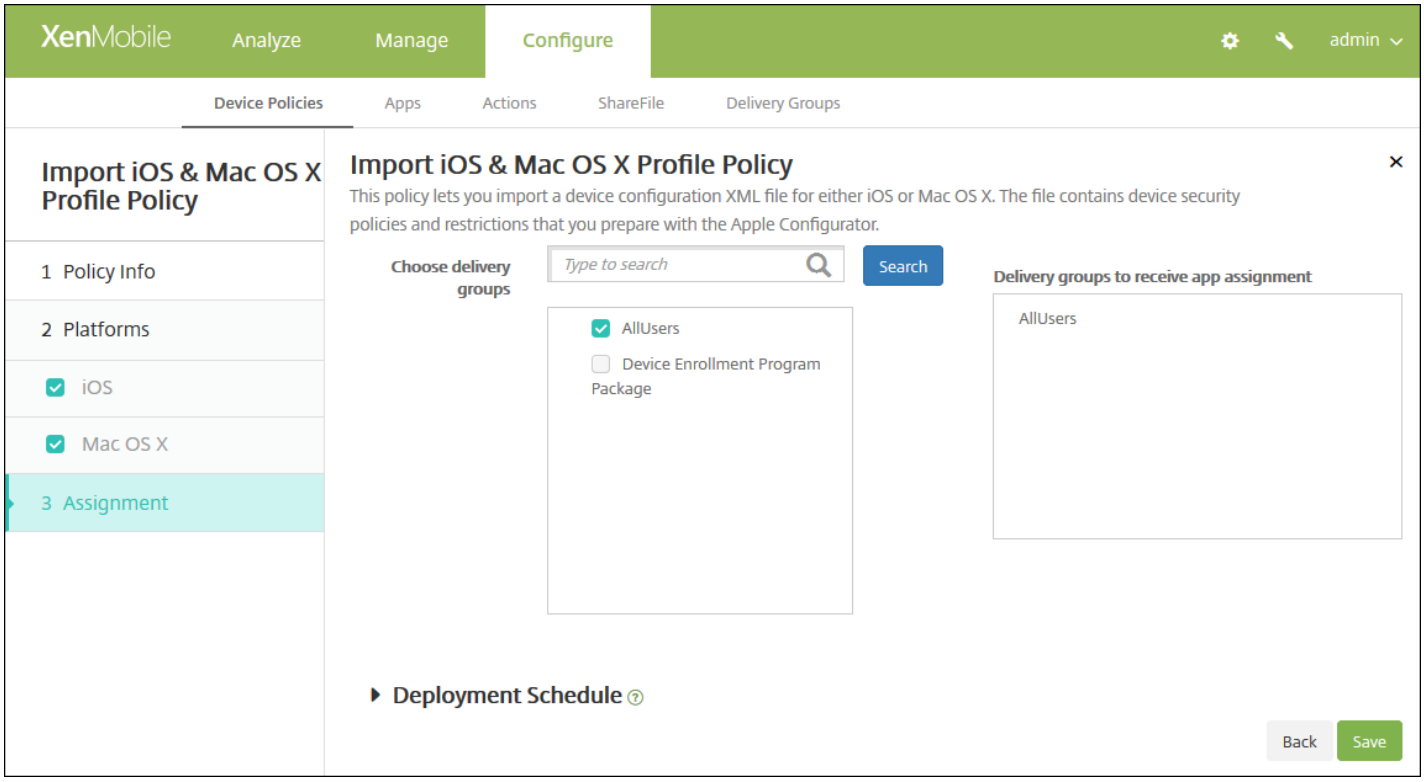
1つのプラットフォームの設定の構成が完了したら、手順8.を参照してプラットフォームの展開規則を設定します。 ではありません。

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構成プロファイル**または**Mac OS X 構成プロファイル**: **[ブラウザー]** をクリックしてインポートする構成ファイルの場所へ移動し、そのファイルを選択します。

8. 展開規則を構成します。

9. **[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。



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。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、[オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[オフ] を選択した場合、そのほかのオプションを構成する必要はありません。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、[以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

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。

12. [Save] をクリックしてポリシーを保存します。

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：

a. **[Supervision]** コントロールを **[On]** に切り替えます。構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。

b. 必要に応じてデバイスの名前を指定します。

c. 最新バージョンのiOSをインストールする場合、［iOS］ボックスの一覧で **[Latest]** を選択します。

5. デバイスの監視の準備が整ったら、 **[Prepare]** をクリックします。

Samsung SAFEのキオスクデバイスポリシー

Feb 27, 2017

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、**[キオスクモード]** を **[無効化]** 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

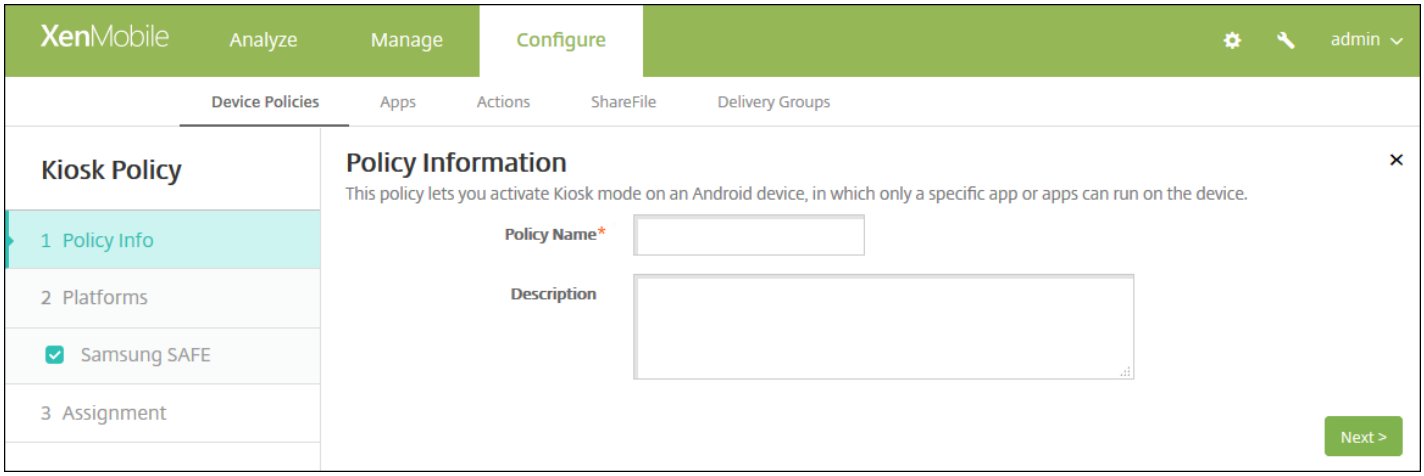
注：

- 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、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

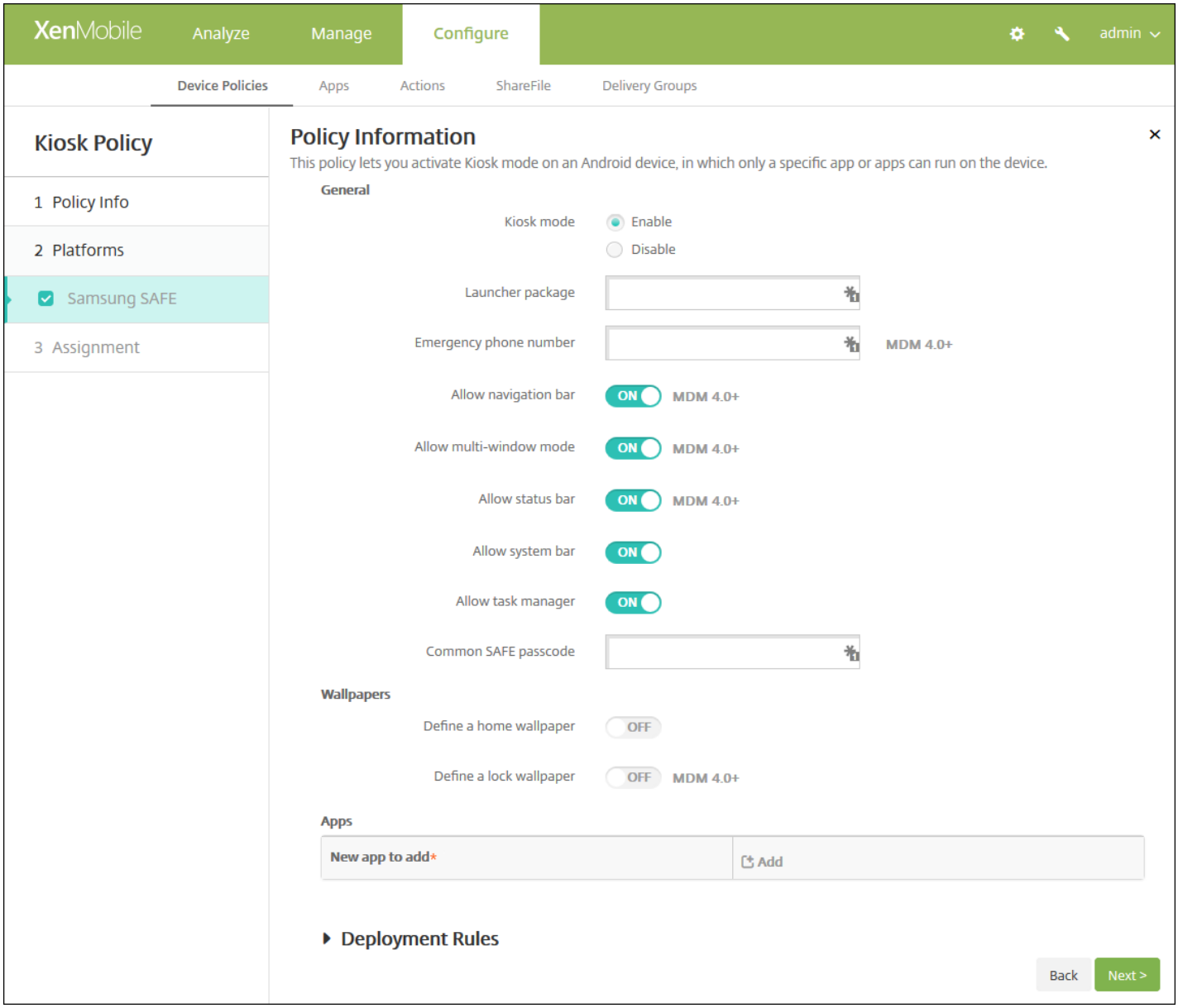
3. **[詳細]** を展開した後、**[セキュリティ]** の下の **[キオスク]** をクリックします。**[キオスクポリシー]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[Samsung SAFE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。

- **キオスクモード**：［**有効化**］または［**無効化**］を選択します。デフォルトは［**有効化**］です。［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。
- **ナビゲーションバーを許可**：キオスクモードのときに、ユーザーにナビゲーションバーを表示して使用できるようにするかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは［**オン**］です。
- **マルチウィンドウモードを許可**：キオスクモードのときに、ユーザーが複数のウィンドウを使用できるようにするかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは［**オン**］です。
- **ステータスバーを許可**：キオスクモードのときに、ユーザーにステータスバーを表示するかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは［**オン**］です。

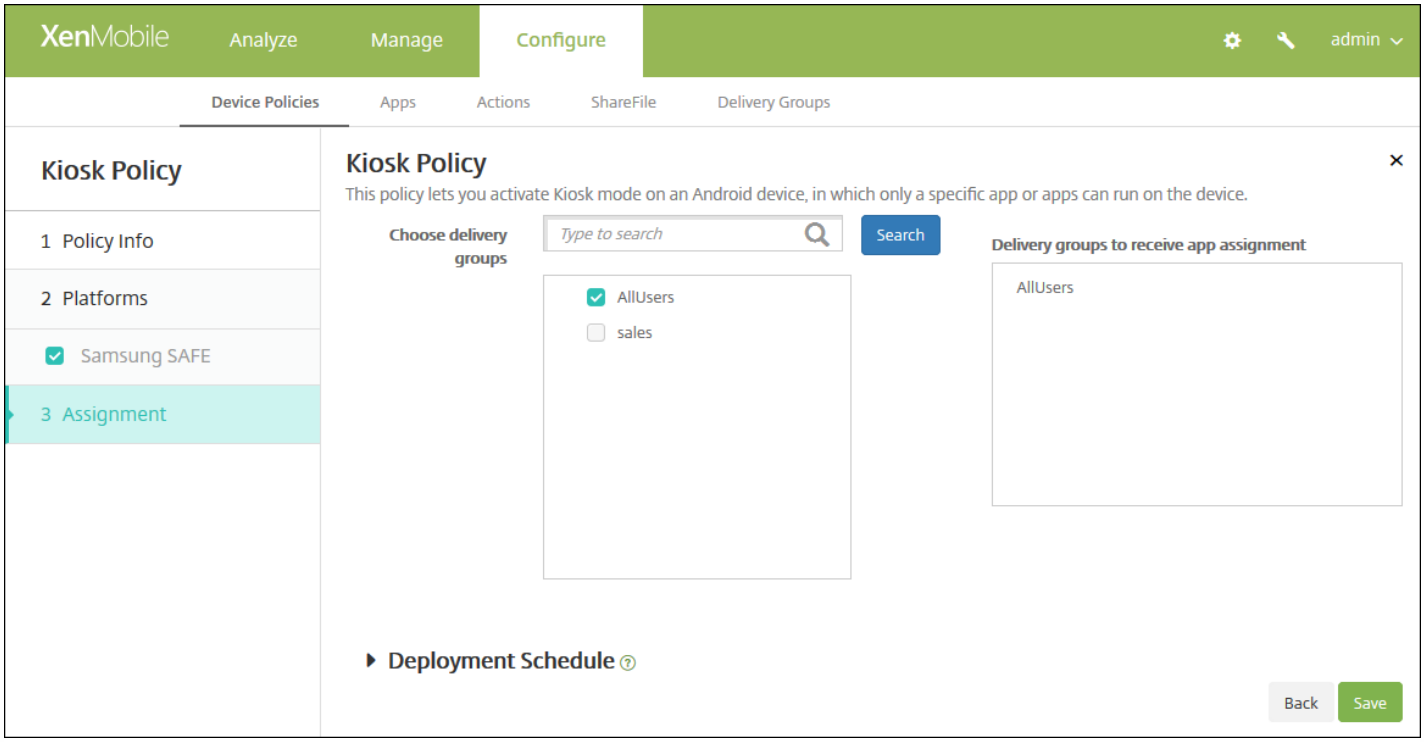
- **システムバーを許可**：キオスクモードのときに、ユーザーにシステムバーを表示するかどうかを選択します。デフォルトは［**オン**］です。
- **タスクマネージャーを許可**：キオスクモードのときに、ユーザーにタスクマネージャーを表示して使用できるようにするかどうかを選択します。デフォルトは［ON］です。
- **Common SAFE passcode**： すべてのSamsung SAFEデバイスを対象とする汎用パスコードポリシーを設定した場合、オプションとして、このフィールドにパスコードを入力します。
- **壁紙**
  - **ホーム画面の壁紙を定義**：キオスクモードのときに、ホーム画面でカスタムイメージを使用するかどうかを選択します。デフォルトは［**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［**オフ**］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。
  - **追加する新規アプリ**：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を追加するか、［**Cancel**］をクリックしてアプリ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. 展開規則を構成します。

8. ［**次へ**］をクリックします。［**キオスクポリシー**］割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

位置情報デバイスポリシー

Mar 24, 2017

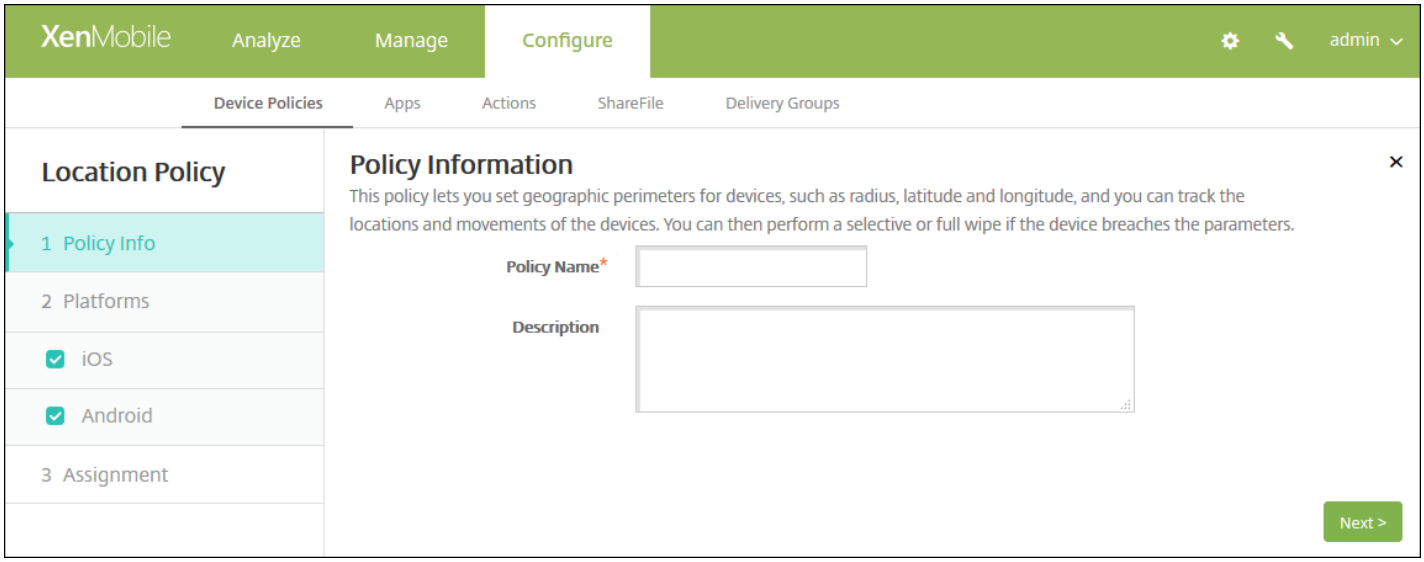
XenMobileで位置情報デバイスポリシーを作成して、地理的な境界を適用することができます。定義された境界（*ジオフェンス*とも呼ばれます）の外にユーザーが出た場合、XenMobileでは特定のアクションを実行できます。たとえば、定義された境界の外にユーザーが出た場合に、警告メッセージを表示するようにポリシーを構成できます。また、境界違反時にユーザーの企業データを即時または一定の時間が経過してからワイプするように構成することもできます。デバイスの追跡と検索の有効化などのセキュリティ操作について詳しくは、「デバイス」の「セキュリティの操作を実行する」セクションを参照してください。

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、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[場所]** をクリックします。**[場所ポリシー]** 情報ページが開きます。



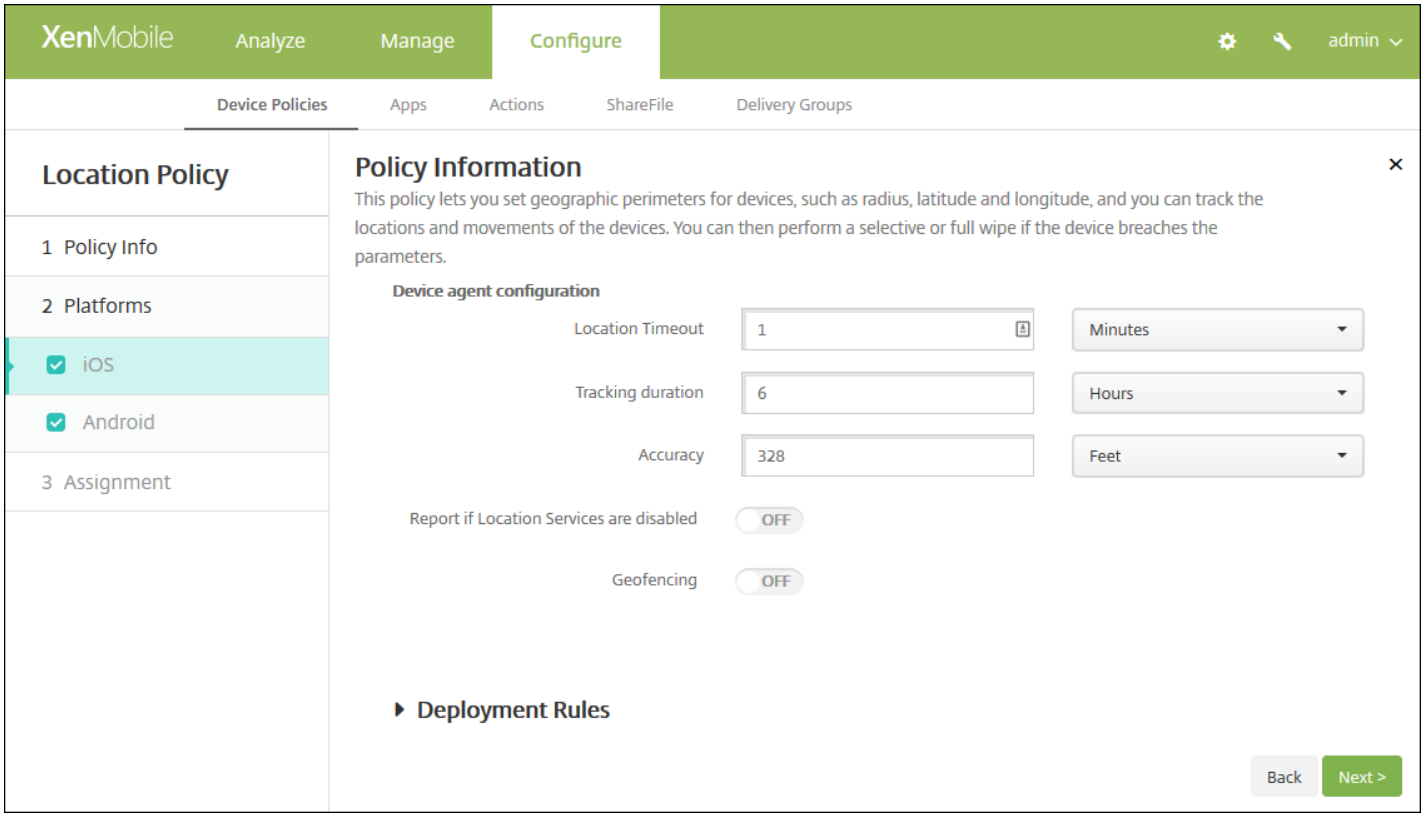
4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。**[プラットフォーム]** ページが開きます。

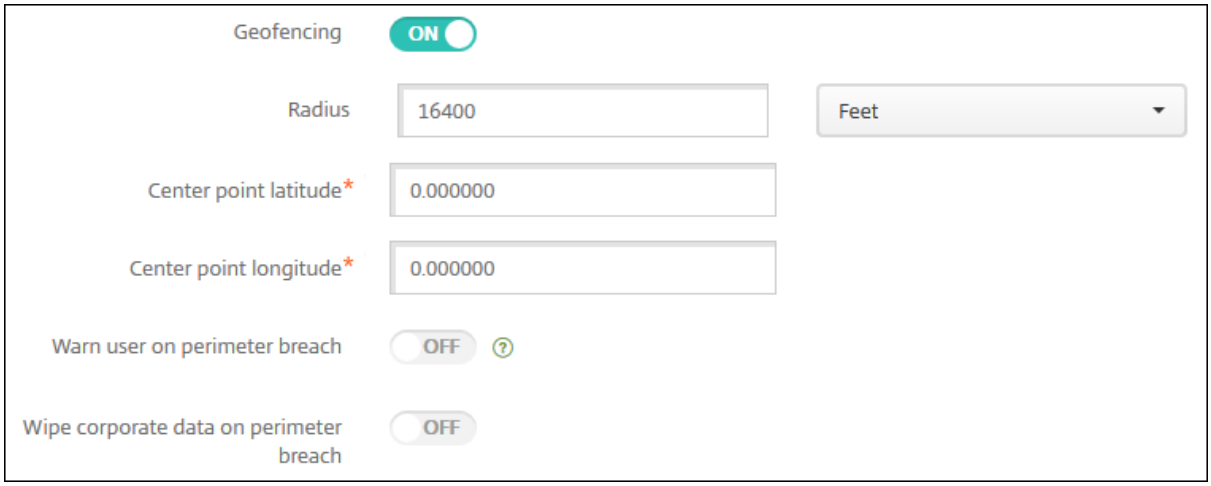
6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



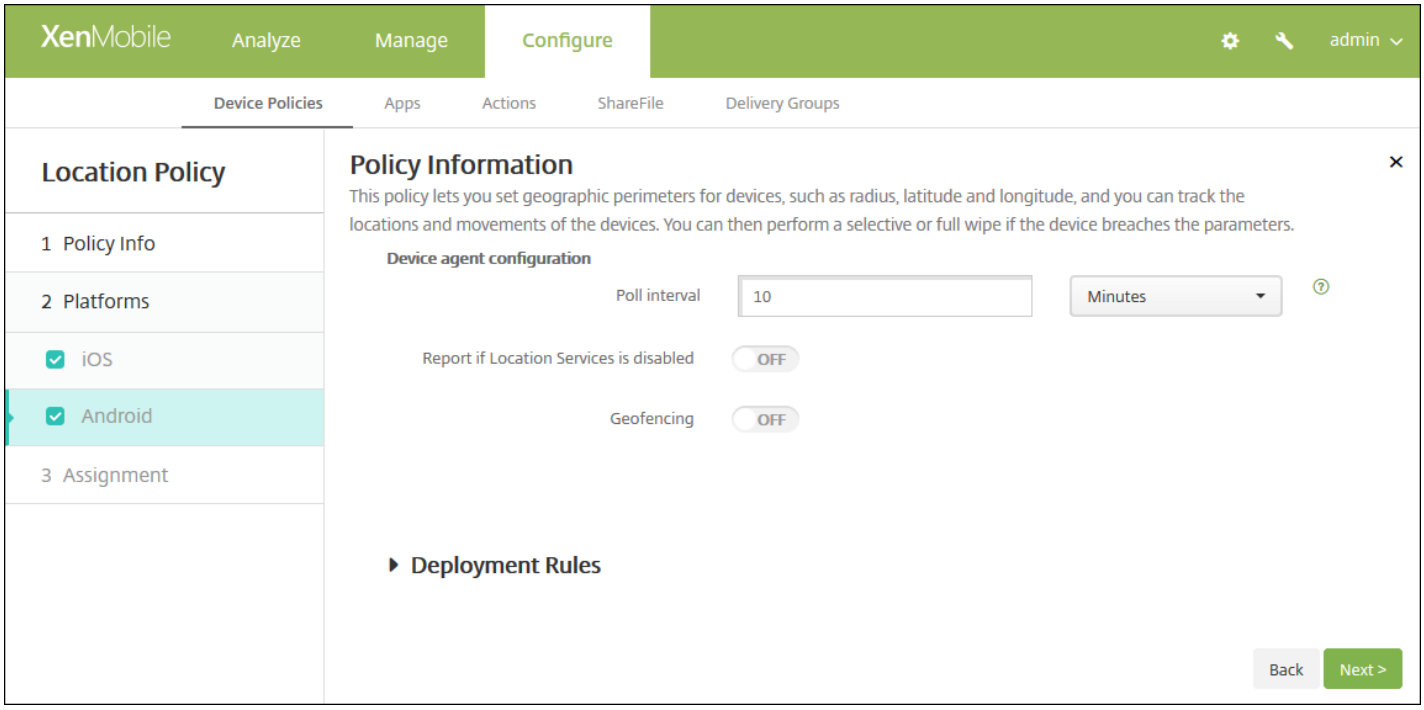
次の設定を構成します。

- **位置タイムアウト**：数値を入力して、ボックスの一覧で **[秒]** または **[分]** を選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、60～900秒または1～15分です。デフォルトは1分です。
- **追跡期間**：数値を入力して、ボックスの一覧で **[時間]** または **[分]** を選択し、XenMobileがデバイスを追跡する時間を設定します。有効な値は、1～6時間または10～360分です。デフォルトは6時間です。
- **精度**：数値を入力して、ボックスの一覧で **[メートル]**、**[フィート]**、**[ヤード]** のいずれかを選択し、XenMobileがデバイスを追跡する精度を設定します。有効な値は、10～5000ヤード、10～5000m、または30～15000フィートです。デフォルトは328フィートです。
- **位置情報サービスが無効の場合は報告**：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。デフォルトは **[オフ]** です。
- **ジオフェンシング**

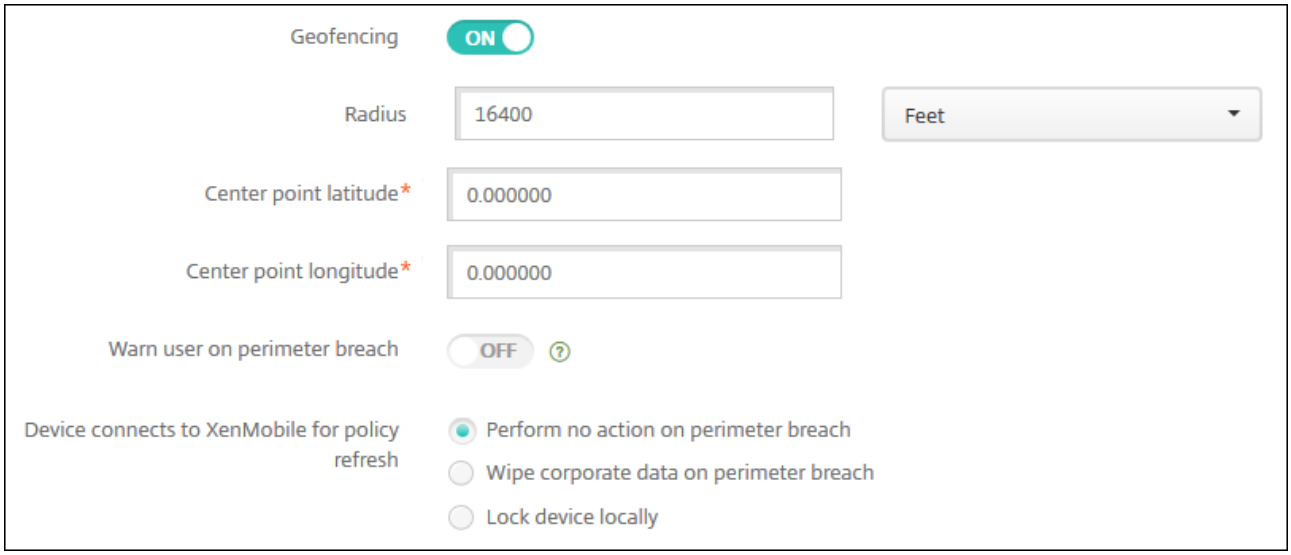


［ジオフェンシング］を選択した場合は、次の設定を構成します。

- **半径**：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。有効な半径の値は次のとおりです。
  - 164～164000フィート
  - 50～50000m
  - 54～54680ヤード
  - 1～31マイル
- **中心点の緯度**：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- **中心点の経度**：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- **境界違反についてユーザーに警告**：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［**オフ**］です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- **境界違反時に企業データをワイプ**：ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。デフォルトは［**オフ**］です。このオプションを有効にすると、［**ローカルワイプを延期**］フィールドが表示されます。
  - 数値を入力し、一覧から［**秒**］または［**分**］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。



- **ポーリング間隔**：数値を入力して、ボックスの一覧で［**分**］、［**時間**］、または［**日**］を選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1～1440分、1～24時間、または任意の日数です。デフォルトは10分です。この値を10分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- **位置情報サービスが無効の場合は報告**：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。デフォルトは［**オフ**］です。
- **ジオフェンシング**

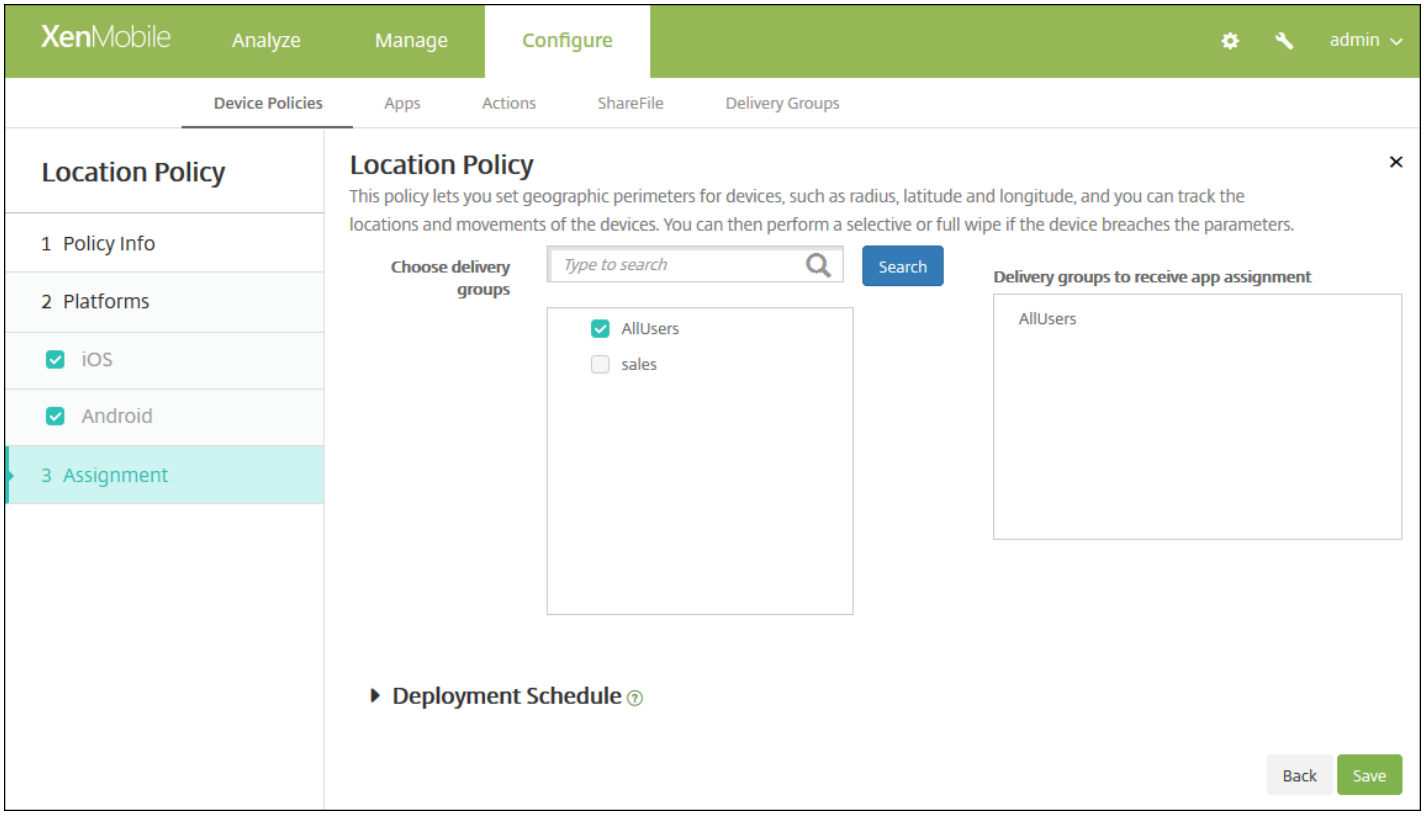


［ジオフェンシング］を選択した場合は、次の設定を構成します。

- **半径**：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。有効な半径の値は次のとおりです。
  - 164～164000フィート
  - 1～50km
  - 50～50000m
  - 54～54680ヤード
  - 1～31マイル
- **中心点の緯度**：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- **中心点の経度**：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- **境界違反についてユーザーに警告**：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは**［オフ］**です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- **ポリシー更新のためデバイスをXenMobileに接続**：ユーザーが境界の外に出た場合のオプションを以下から選択します。
  - **境界違反時に何も実行しない**：何もしません。これがデフォルトの設定です。
  - **境界違反時に企業データをワイプ**：指定時間後に企業データをワイプします。このオプションを有効にすると、**［ローカルワイプを延期］**フィールドが表示されます。
    - 数値を入力し、一覧から［秒］または［分］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。
  - **ロックを延期**：指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、**［ロックを延期］**フィールドが表示されます。
    - 数値を入力し、一覧から［秒］または［分］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

7. 展開規則を構成します。

8. **［次へ］**をクリックします。**［場所ポリシー］**割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

管理対象ドメインデバイスポリシー

Feb 27, 2017

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。

iOS 8以降の監視対象デバイスの場合、URLまたはサブドメインを指定して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御します。iOS 9.3以降の監視対象デバイスの場合、Safariにパスワードを保存できるURLを指定します。

iOSデバイスを監視モードに設定する手順については、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」を参照してください。

ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。

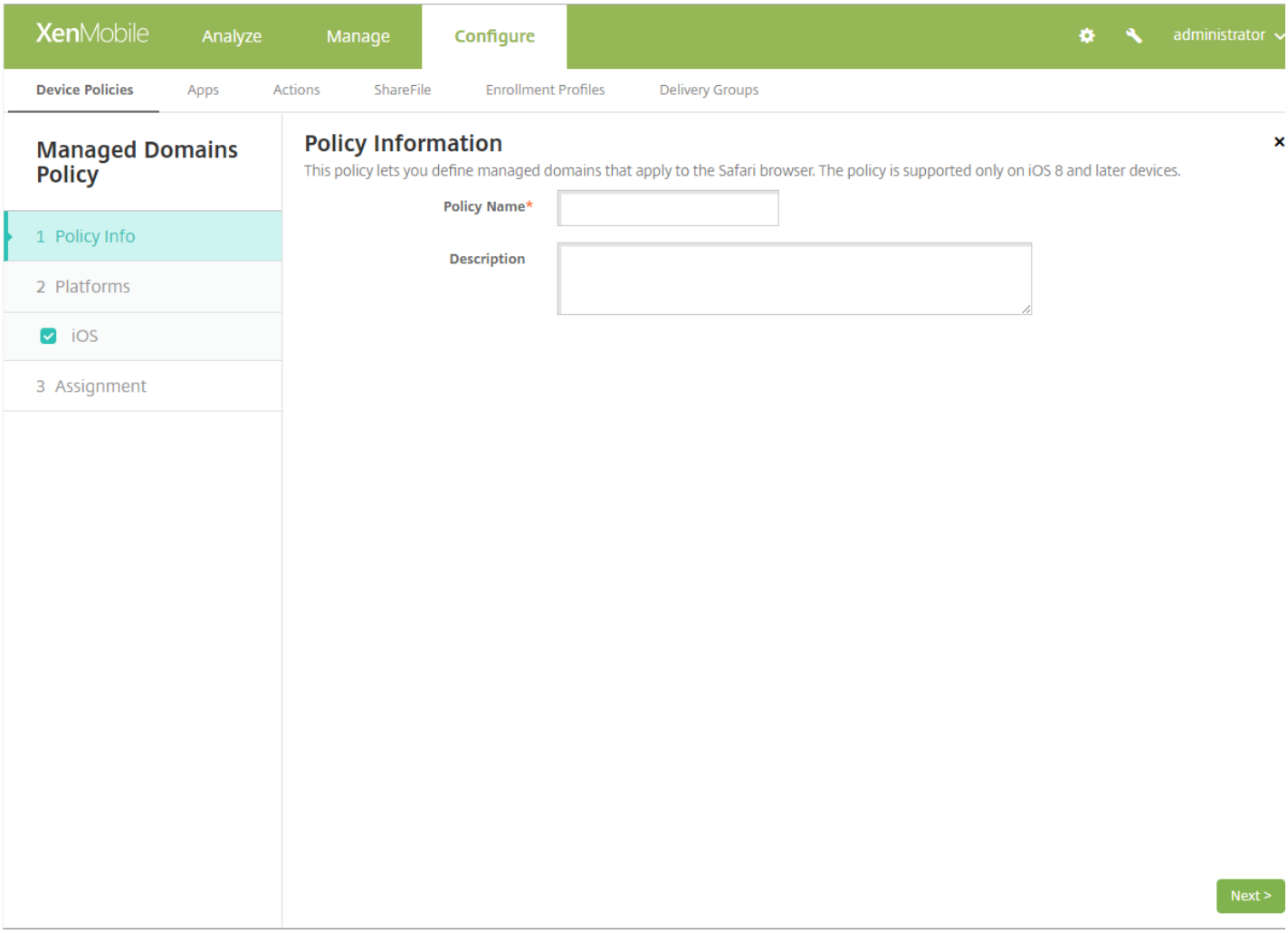
ドキュメント、添付ファイルなど、ダウンロードしたものなどのアイテムの場合： ユーザーがSafariを使用して、管理対象Webドメイン一覧に含まれているWebドメインから取得したアイテムを開く場合、適切な社内アプリケーションによってアイテムが開かれます。アイテムが管理対象Webドメイン一覧にあるWebドメインから取得されたものでない場合、ユーザーは社内アプリケーションでアイテムを開くことができません。 ユーザーは各自の非管理対象アプリケーションを使用する必要があります。

監視対象デバイスの場合（Safari のパスワード自動入力ドメインを指定していない場合でも）： デバイスがエフェメラルマルチユーザーとして構成されている場合、ユーザーはパスワードを保存できません。ただし、デバイスがエフェメラルマルチユーザーとして構成されていない場合は、ユーザーはすべてのパスワードを保存できます。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[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。

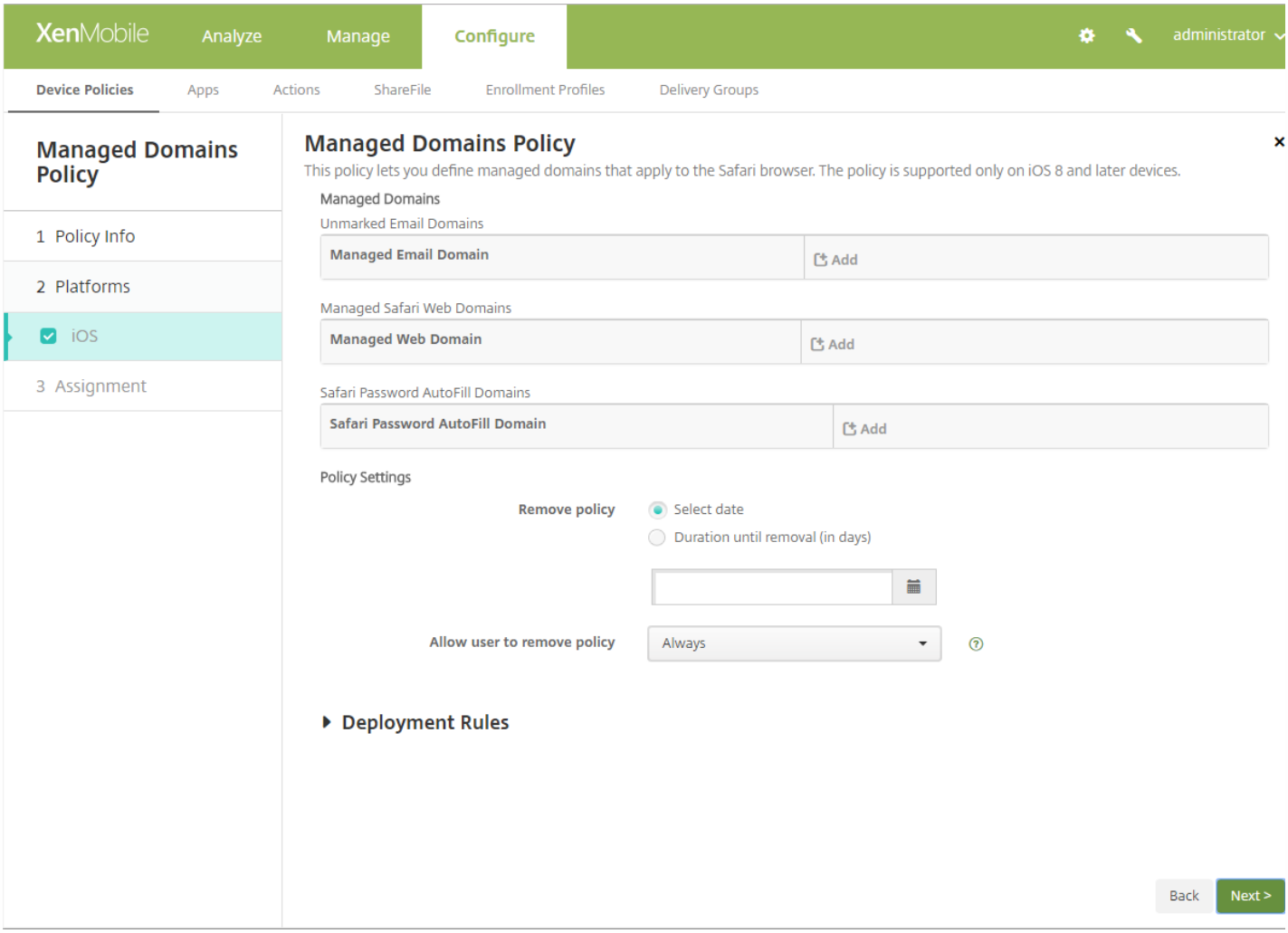
3. **[More]** を展開した後、 **[Security]** の下の **[Managed domains]** をクリックします。 **[Managed Domains Policy]** 情報ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：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。
  - **管理対象のSafari Webドメイン**： 一覧に含めるWebドメインごとに、［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。
  - **Safariのパスワードオートフィルドメイン**:
    一覧に含める自動入力ドメインごとに、［**追加**］をクリックして以下の操作を行います。
    - **Safariのパスワードオートフィルドメイン**: 自動入力ドメインを入力します。
    - ［**保存**］をクリックして自動入力ドメインを保存するか、［**キャンセル**］をクリックして操作を取り消します。

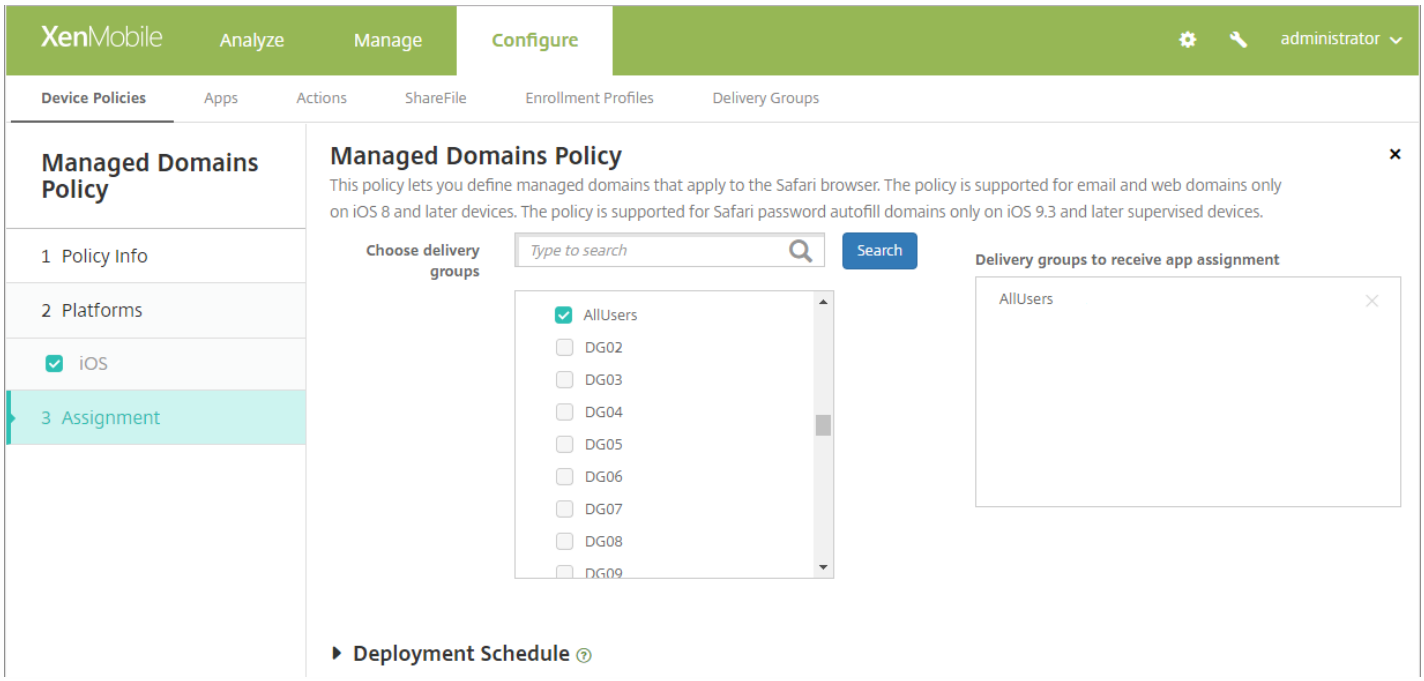
      注： 既存のドメインを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

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、［保存］をクリックして変更した項目を保存するか、［キャンセル］をクリックします。

- **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. 展開規則を構成します。

8. ［Next］をクリックします。［割り当て］ページが開きます。



9. ［デリバリーグループを選択］の横に、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［アプリ割り当てを受信するためのデリバリーグループ］一覧に表示されます。

10. ［展開スケジュール］を展開して以下の設定を構成します。

- ［展開］の横の［オン］をクリックすると展開がスケジュールされ、［オフ］をクリックすると展開が行われません。デフォルトのオプションは［オン］です。［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。
- ［展開スケジュール］の横の［すぐに］または［あとで］をクリックします。デフォルトのオプションは［すぐに］です。
- ［あとで］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［展開状態］の横の［接続するたび］をクリックするか、［以前の展開が失敗した場合のみ］をクリックします。デフォルトのオプションは、［接続するたび］です。
- ［常時接続に対する展開］の横の［オン］または［オフ］をクリックします。デフォルトのオプションは［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、**［常時接続に対する展開］**は適用されません。

11. **［保存］**をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

プロファイル削除デバイスポリシー

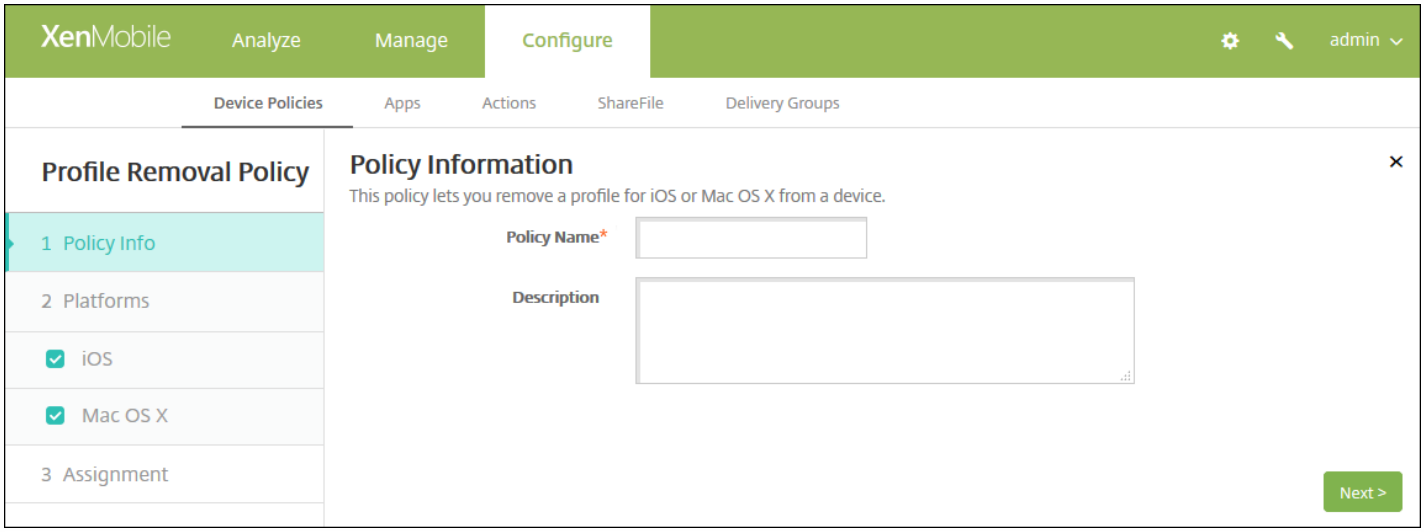
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** 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、 **[Removal]** で **[Profile Removal]** をクリックします。 **[Profile Removal Policy]** ページが開きます。



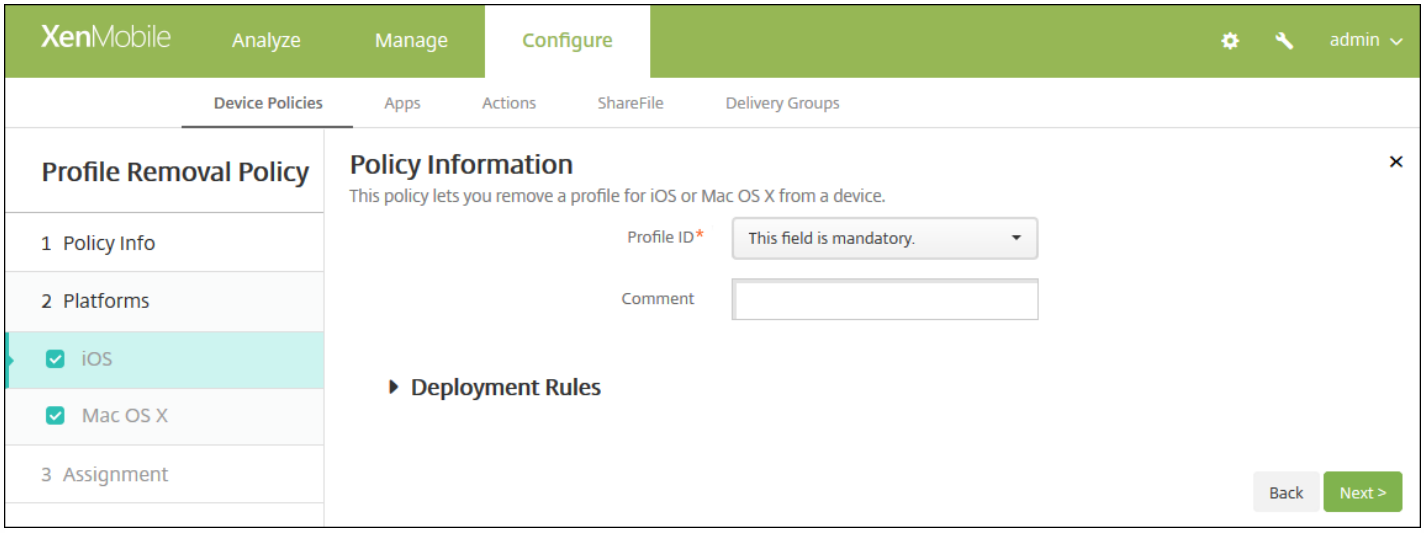
4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[プラットフォーム]** ページが開きます。

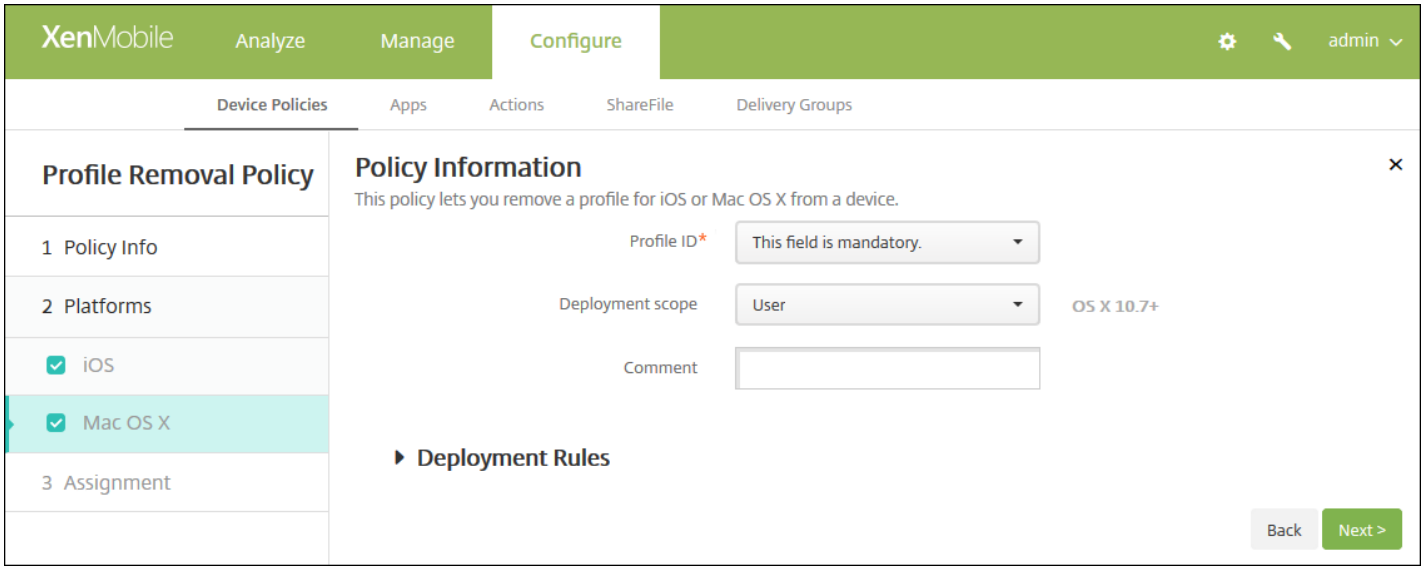
6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。



次の設定を構成します。

- **Profile ID**： 一覧から、アプリケーションプロファイルIDを選択します。このフィールドは必須です。
- **Comment**： 任意でコメントを入力します。

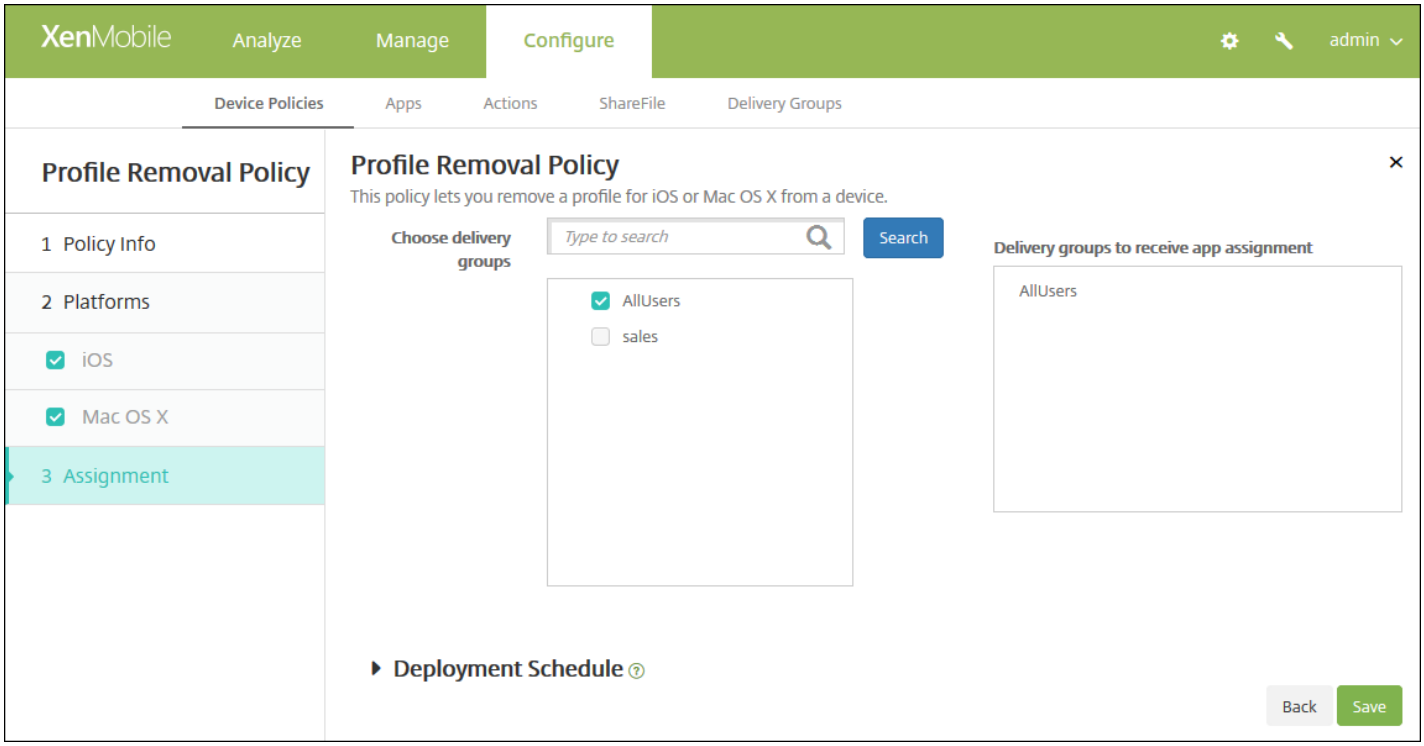


次の設定を構成します。

- **Profile ID**： 一覧から、アプリケーションプロファイルIDを選択します。このフィールドは必須です。
- **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OS X 10.7以降でのみ使用できます。
- **Comment**： 任意でコメントを入力します。

7. 展開規則を構成します。

8. [Next] をクリックします。 [App Uninstall Policy] 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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 **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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. **[保存]** をクリックします。

プロビジョニングプロファイルデバイスポリシー

Feb 27, 2017

iOSエンタープライズアプリを開発しコード署名するときは、通常は、iOSデバイスで実行するアプリにAppleが求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。

プロビジョニングプロファイルの主な問題は、Apple Developer Portalで生成されてから1年で期限が切れるので、ユーザーによって登録されたすべてのiOSデバイス上のすべてのプロビジョニングファイルの期限を追跡する必要があることです。期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信する、プロビジョニングプロファイルをWebポータルに置いてダウンロードとインストールを可能にする、という2つの方法があります。これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Webポータルにアクセスして適切なプロファイルをダウンロードしインストールすることを求めたりするので、エラーが発生する傾向があります。

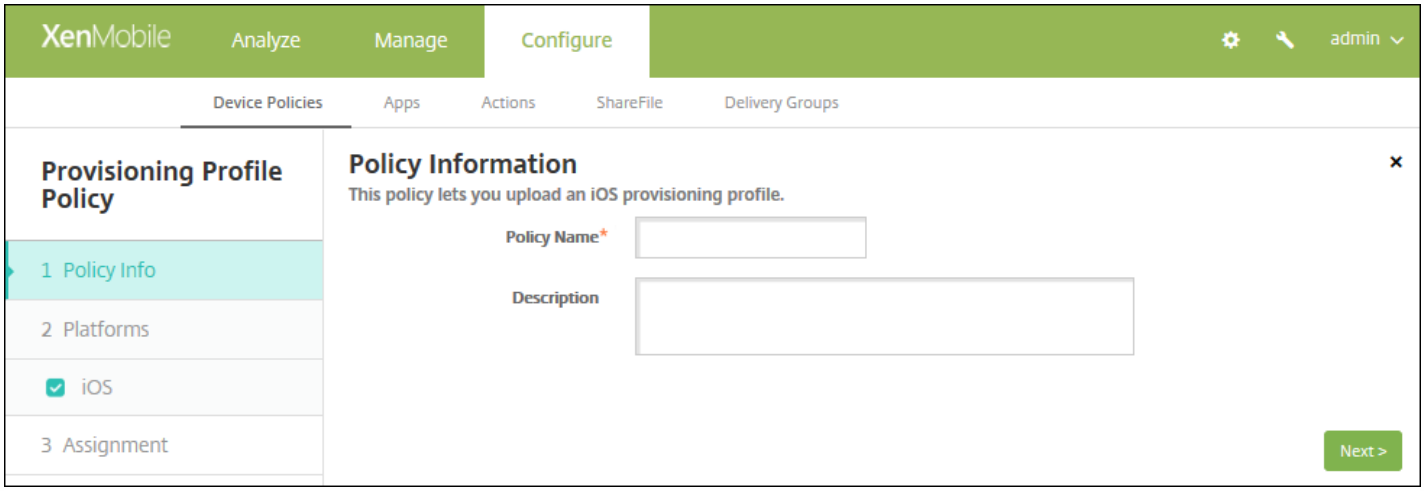
このプロセスをユーザーが意識しないで済むように、XenMobileではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。

プロビジョニングプロファイルポリシーを作成するには、プロビジョニングプロファイルのファイルを作成する必要があります。詳しくは、Apple Developerサイトのプロビジョニングプロファイルの作成に関するページを参照してください。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[Add]** をクリックします。 **[Add a New Policy]** ページが開きます。

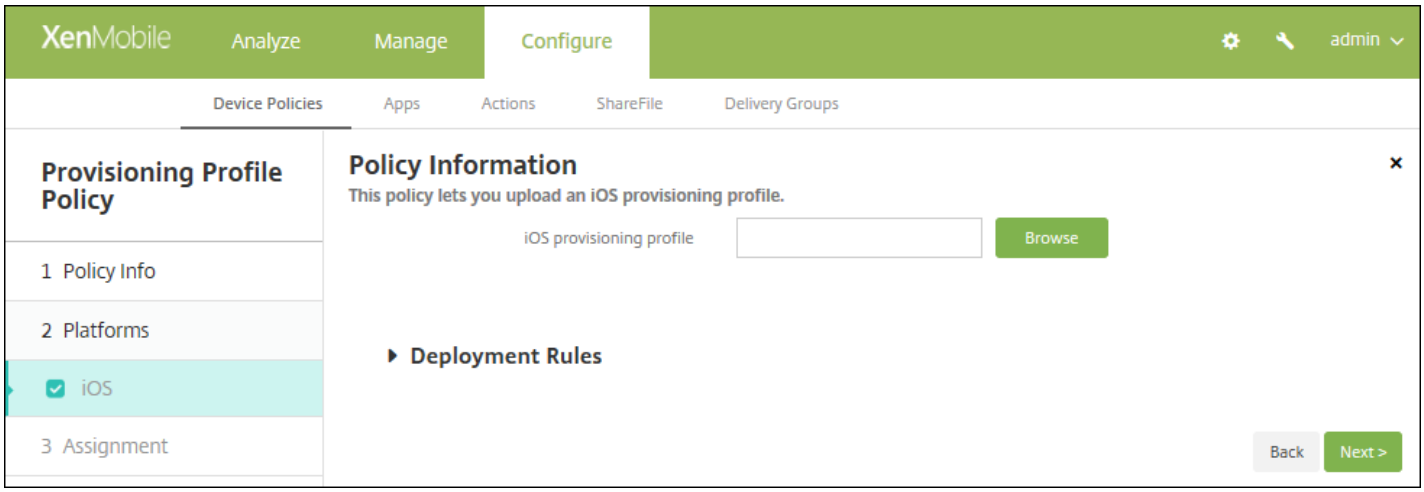
3. **[More]** を展開し、 **[Apps]** の下の **[Provisioning Profile]** をクリックします。 **[Provisioning Profile Policy]** 情報ページが開きます。



4. **[ポリシー情報]** 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。

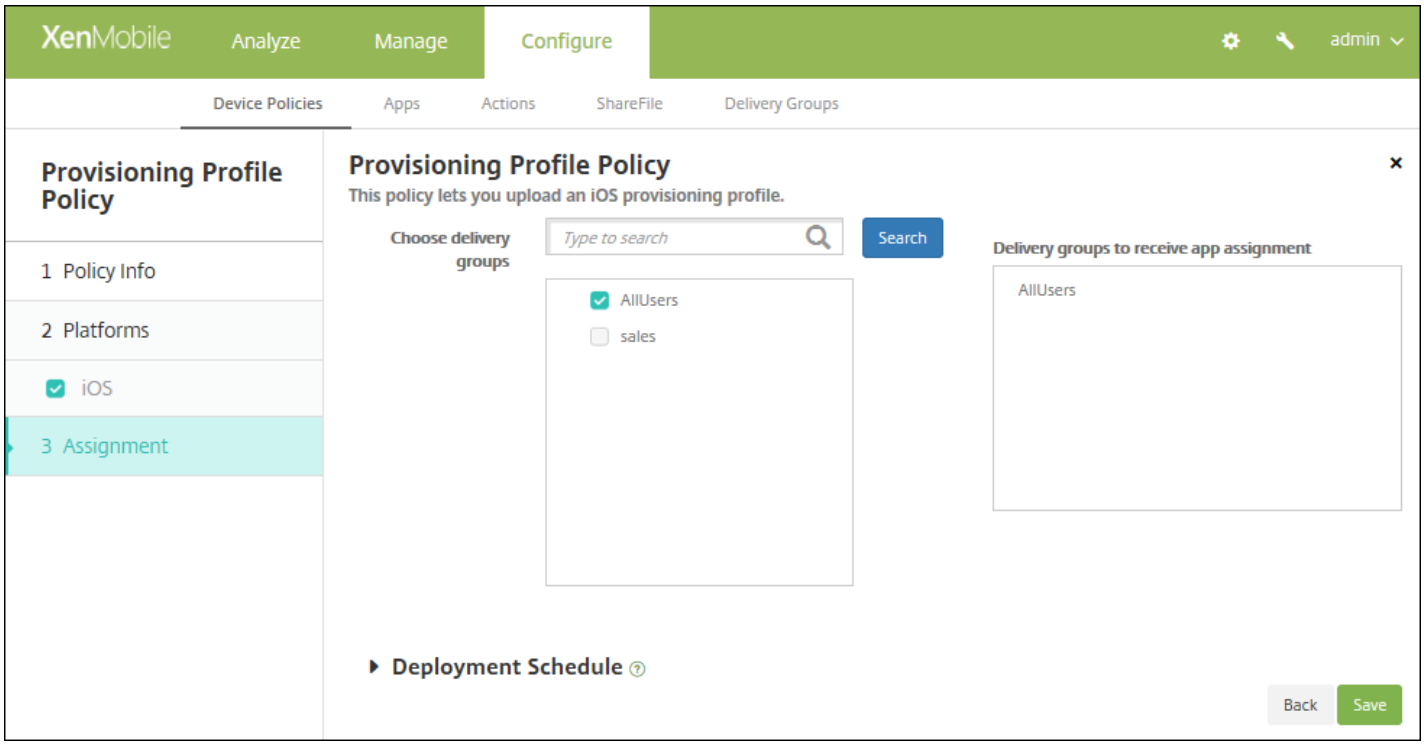


6. 次の設定を構成します。

- **iOSプロビジョニングプロファイル**: **[参照]** をクリックしてインポートするプロビジョニングプロファイルファイルの場所へ移動し、そのファイルを選択します。

7. 展開規則を構成します。

8. **[次へ]** をクリックします。 **[プロビジョニングプロファイルポリシー]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- ［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［**オン**］です。［**オフ**］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。
- ［**展開スケジュール**］の横の［**すぐに**］または［**あとで**］をクリックします。デフォルトのオプションは［**すぐに**］です。
- ［**あとで**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［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、［**接続するたび**］です。
- ［**常時接続に対する展開**］の横の［**オン**］または［**オフ**］をクリックします。デフォルトのオプションは［**オフ**］です。

注：

- このオプションは、［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、［**常時接続に対する展開**］は適用されません。

11. ［**保存**］をクリックします。

プロファイル削除デバイスポリシー

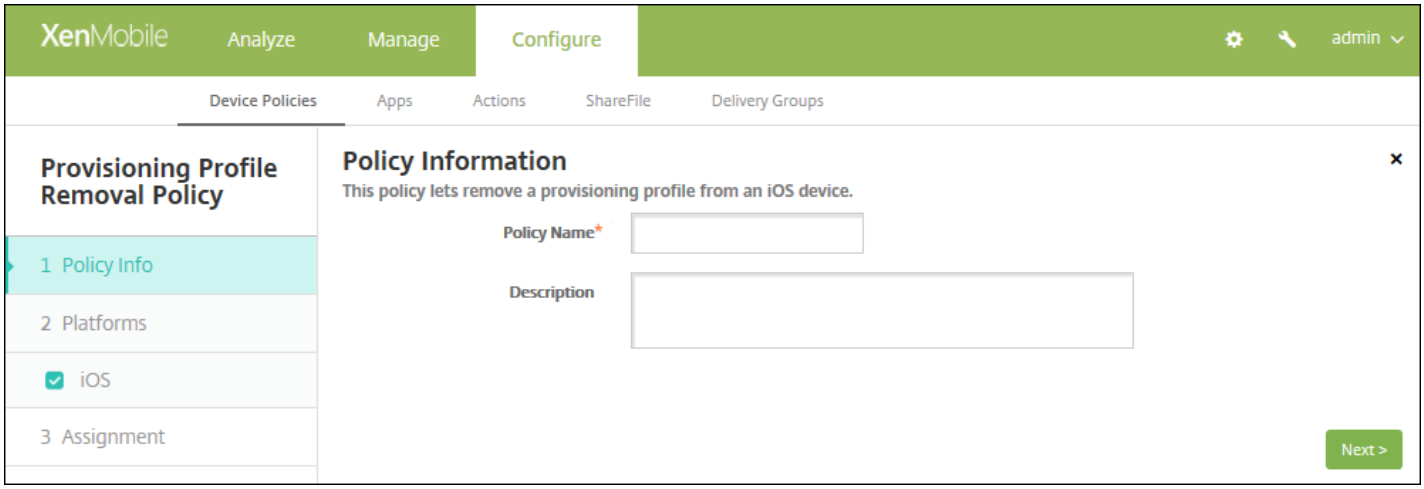
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。

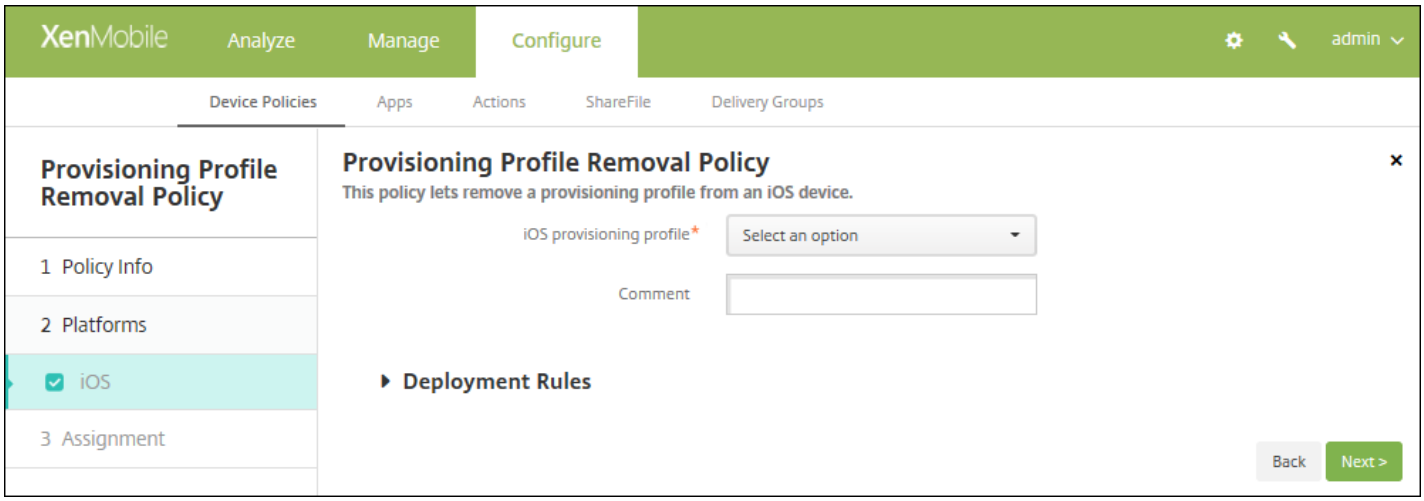
3. **[More]** を展開し、**[Removal]** で **[Provisioning Profile Removal]** をクリックします。**[Provisioning Profile Removal Policy]** 情報ページが開きます。



4. **[ポリシー情報]** 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。

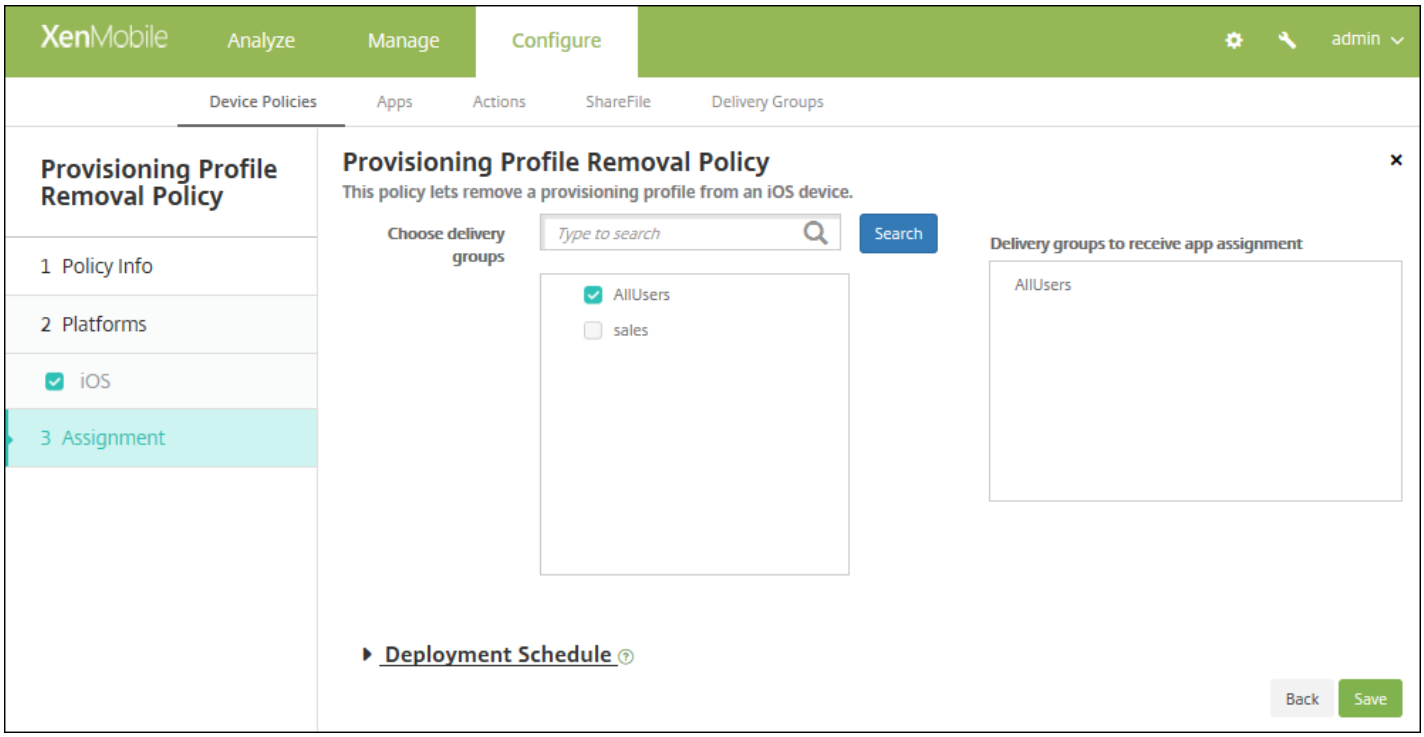


6. 次の設定を構成します。

- **iOS プロビジョニング プロファイル**: 一覧から削除するプロビジョニングプロファイルを選択します。
- **コメント**： 必要に応じてコメントを追加します。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Provisioning Profile Removal Policy]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[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、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

プロキシデバイスポリシー

Feb 27, 2017

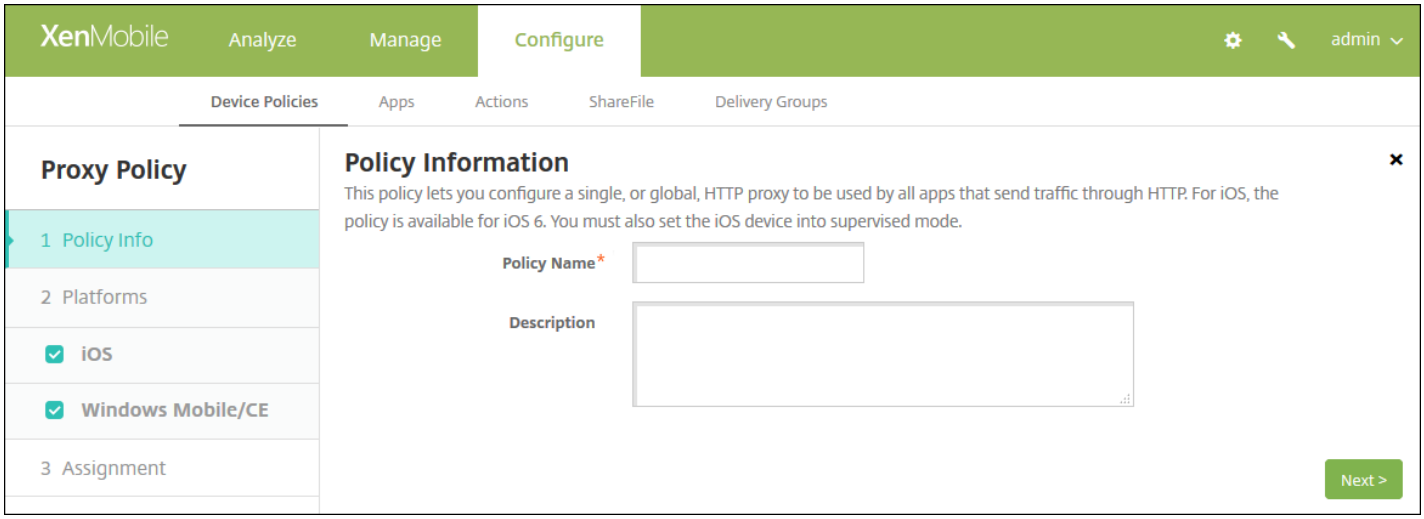
XenMobileでデバイスポリシーを追加して、Windows Mobile/CEおよびiOS 6.0以降を実行しているデバイスのグローバルHTTPプロキシ設定を指定できます。グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。

注： このポリシーを展開する前に、グローバルHTTPプロキシを設定するすべてのiOSデバイスを必ず監視モードに設定してください。詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

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. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[More]** をクリックした後、**[Network access]** の下の **[Proxy]** をクリックします。**[Proxy 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。

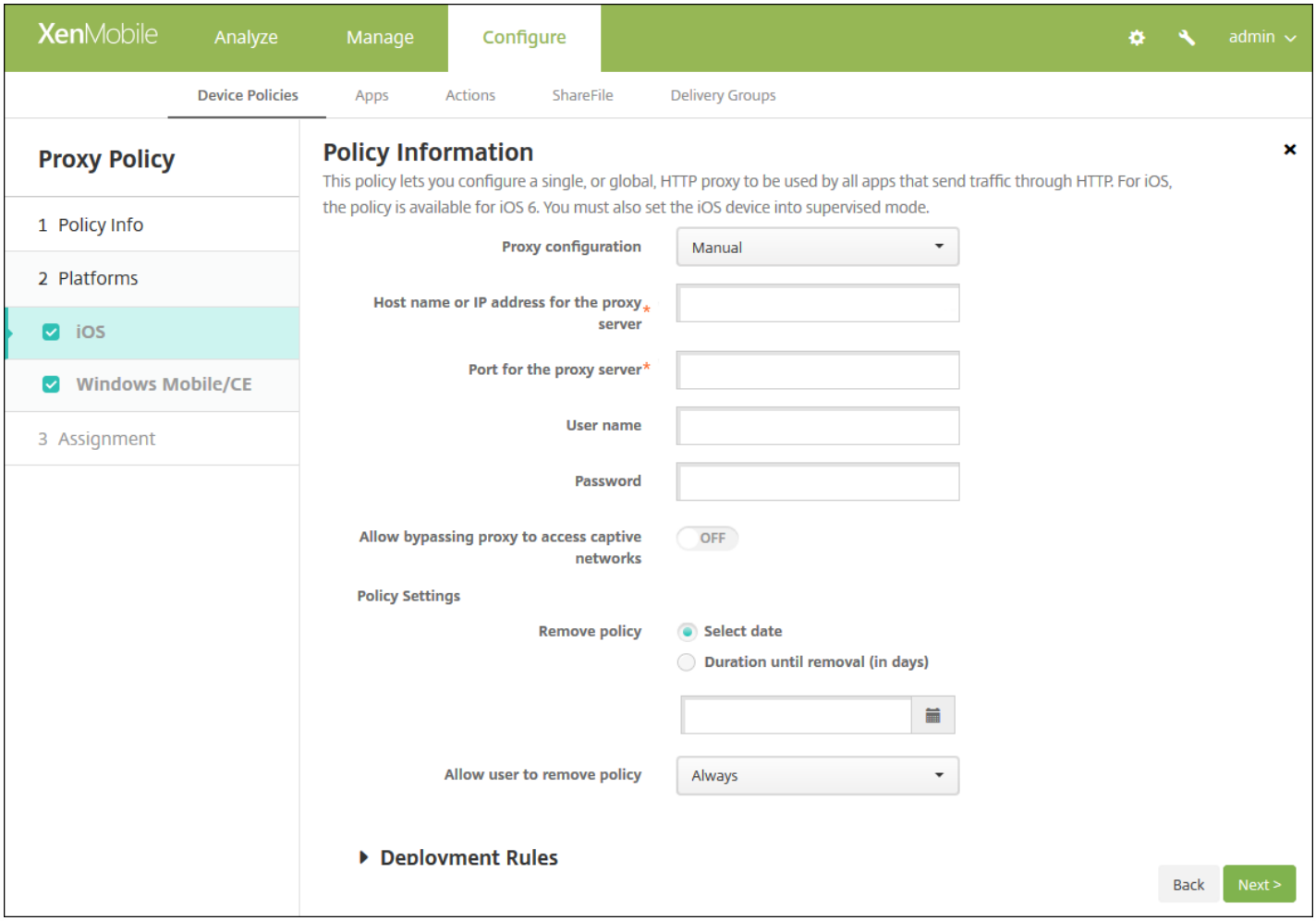
- **Policy Name**： ポリシーの説明的な名前を入力します。
- **Description**： 任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。**[Policy Platforms]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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



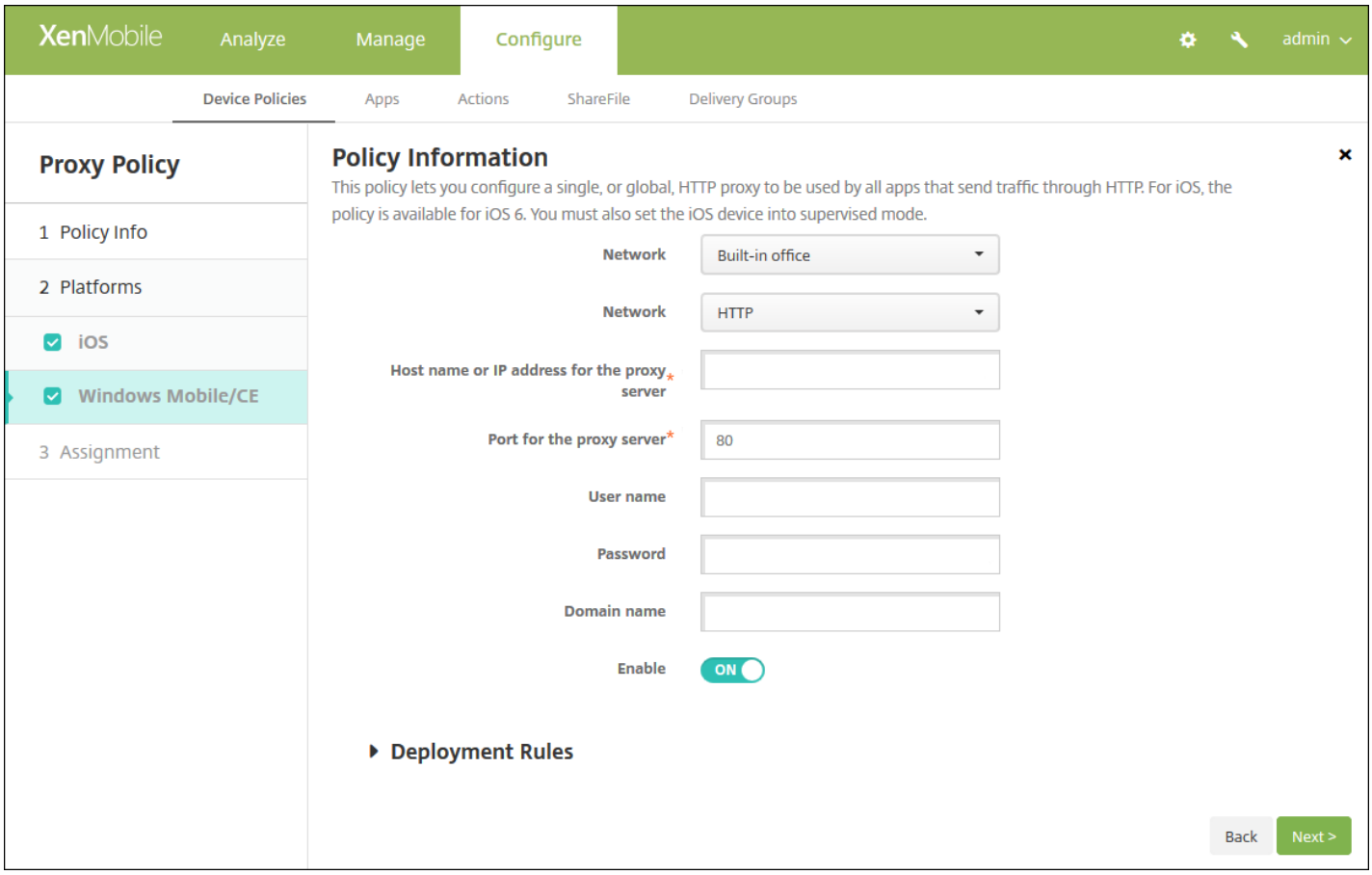
次の設定を構成します。

- **Proxy configuration**：ユーザーのデバイスでのプロキシの構成方法に関して、一覧から［**Manual**］または［**Automatic**］を選択します。
  - ［**手動**］を選択した場合は、次の設定を構成します。
    - **プロキシサーバーのホスト名または IP アドレス**：プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
    - **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。
    - **Proxy PAC URL**：プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達不能である場合は直接接続を許可**：PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは［**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。
- **キャプティブネットワークへのアクセスのためにプロキシのバイパスを許可**：キャプティブネットワークにアクセスするためにプロキシをバイパスすることを許可するかどうか選択します。デフォルトは［**OFF**］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。

Windows Mobile/CEの設定の構成



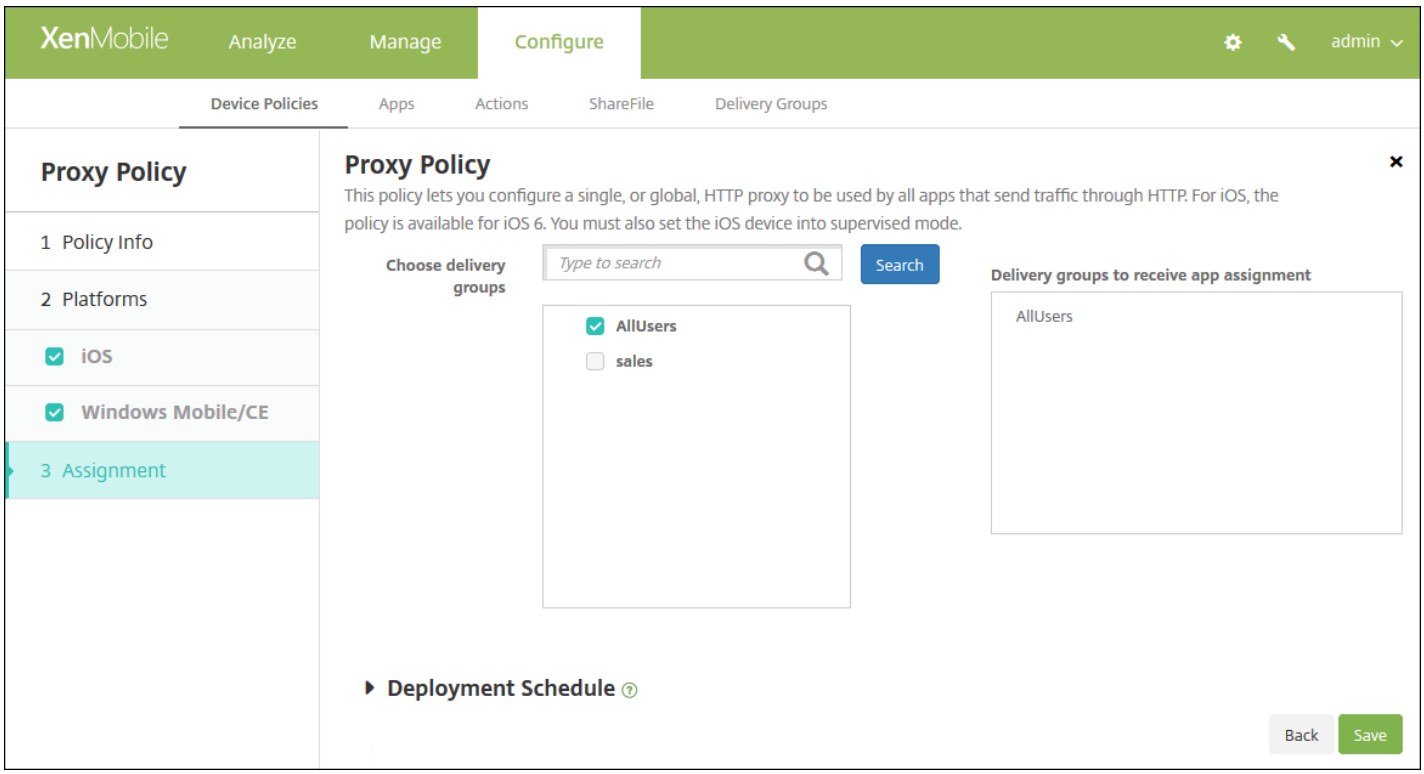
次の設定を構成します。

- **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。選択できるオプションは以下のとおりです。
  - User-defined office
  - User-defined Internet
  - Built-in office
  - Built-in Internet
- **Network**： 一覧から、使用するネットワーク接続プロトコルを選択します。デフォルトは［**HTTP**］です。選択できるオプションは以下のとおりです。
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **Hostname 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。デフォルトは**80**です。
- **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。
- **Domain name**： 任意で、ユーザー名を入力します。
- **Enable**： プロキシを有効にするかどうかを選択します。デフォルトは**[オン]**です。

7. 展開規則を構成します。

8. **[Next]**をクリックします。**[Proxy 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. **[展開スケジュール]**を展開して以下の設定を構成します。

- **[展開]**の横の**[オン]**をクリックすると展開がスケジュールされ、**[オフ]**をクリックすると展開が行われません。デフォルトのオプションは**[オン]**です。**[オフ]**を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]**の横の**[すぐに]**または**[あとで]**をクリックします。デフォルトのオプションは**[すぐに]**です。
- **[あとで]**をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]**の横の**[接続するたび]**をクリックするか、**[以前の展開が失敗した場合のみ]**をクリックします。デフォルトのオプションは、**[接続するたび]**です。
- **[常時接続に対する展開]**の横の**[オン]**または**[オフ]**をクリックします。デフォルトのオプションは**[オフ]**です。

注：

- このオプションは、**[設定]**の**[サーバープロパティ]**において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]**は適用されません。

11. **[保存]** をクリックします。

レジストリデバイスポリシー

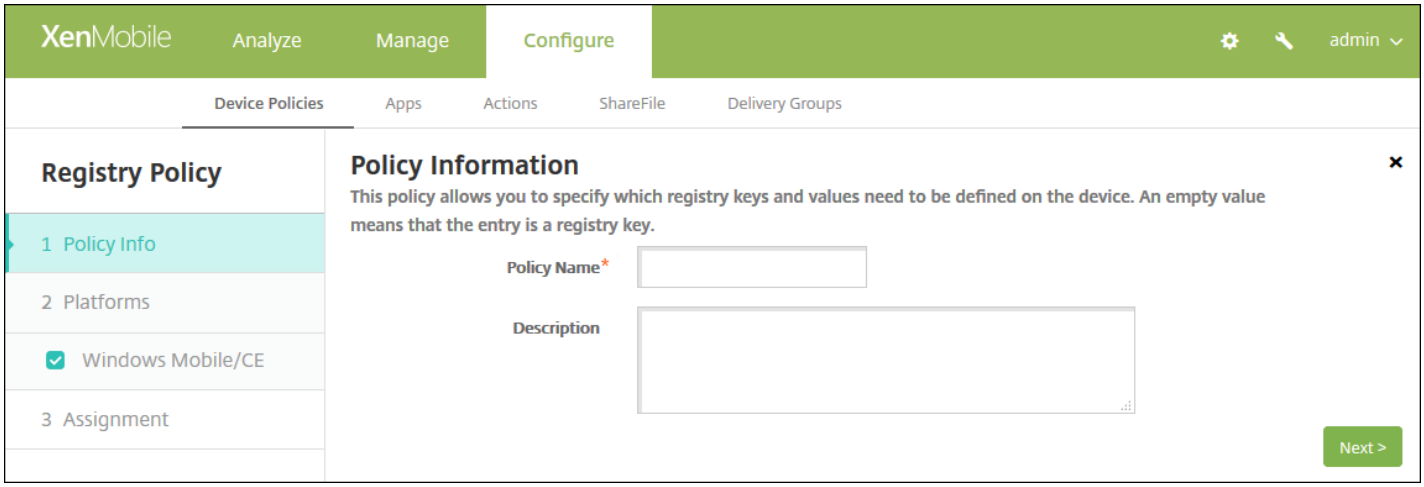
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

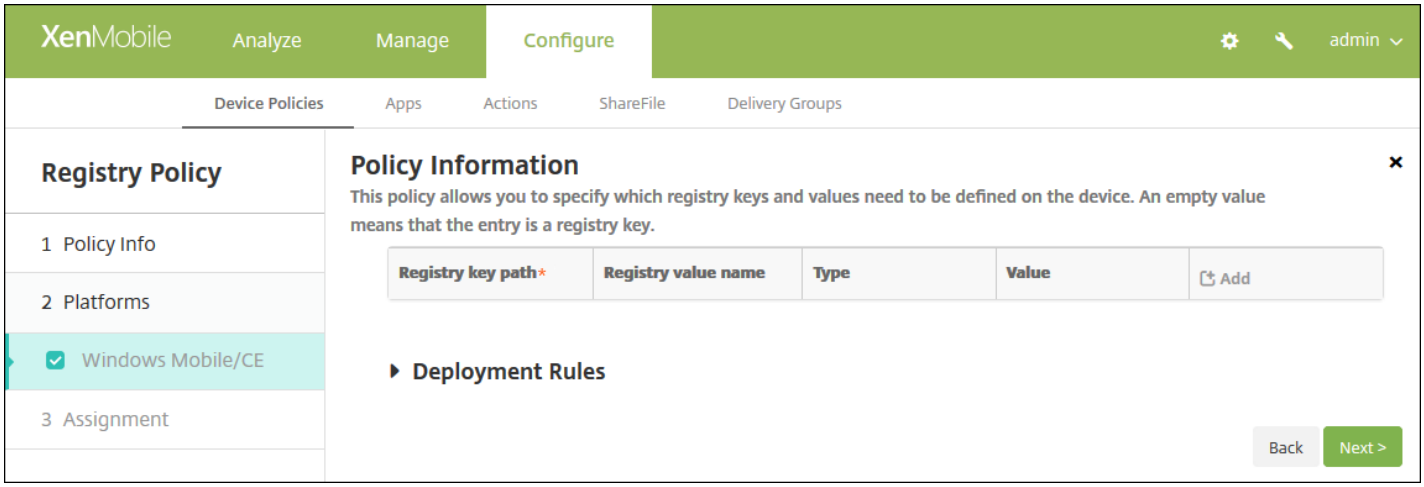
3. **[More]** を展開した後、**[Custom]** の下の **[Registry]** をクリックします。**[Registry Policy]** 情報ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：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。

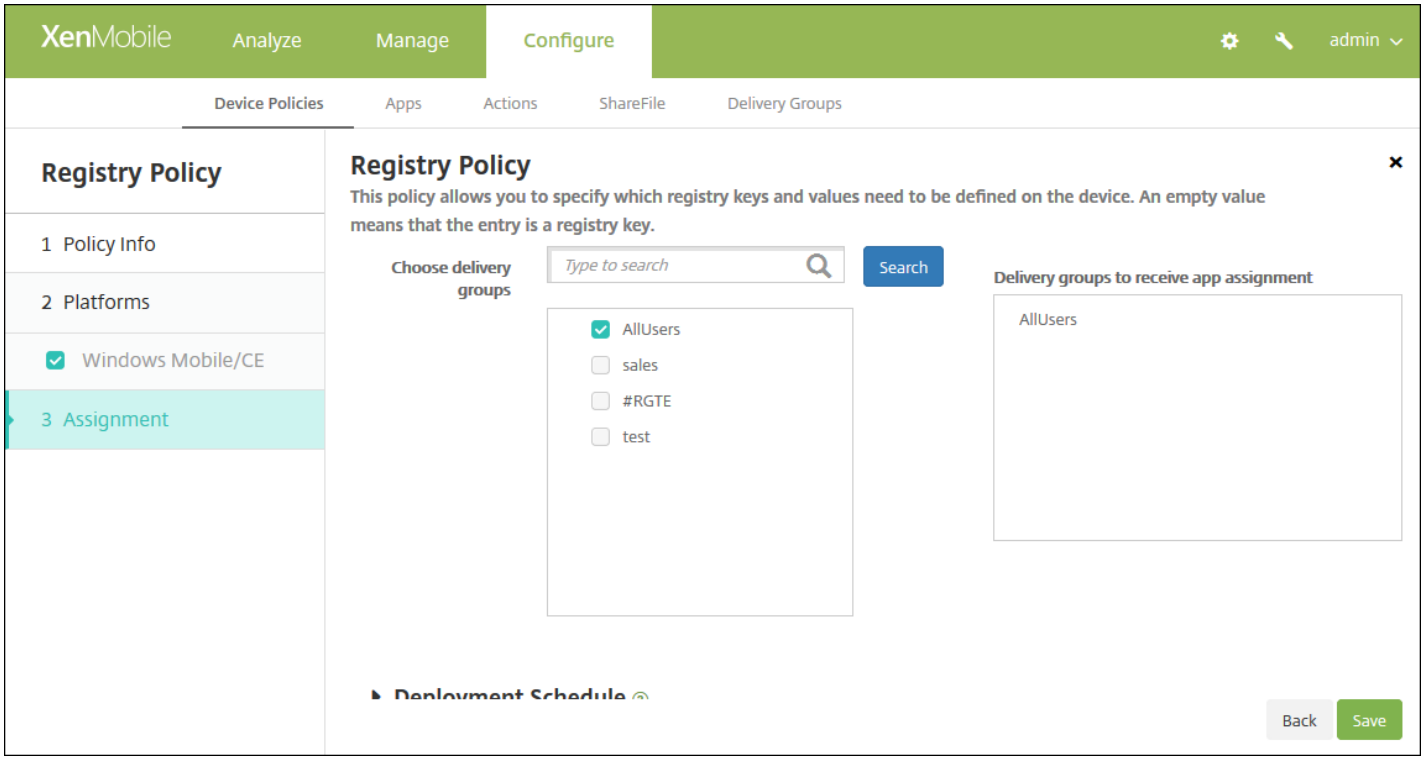
- 追加するレジストリキーまたはレジストリキーと値のペアごとに、**[Add]** をクリックして以下の操作を行います。
- **Registry key path**：レジストリキーのフルパスを入力します。たとえば、「*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows*」と入力して、HKEY_LOCAL_MACHINEルートキーからWindowsキーまでのルートを指定します。
- **Registry value name**：レジストリキー値の名前を入力します。たとえば、「*ProgramFilesDir*」と入力して、レジストリキーのパスHKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersionに値の名前を追加します。このフィールドを空白のままにすると、レジストリキーと値のペアではなく、レジストリキーを追加することになります。
- **Type**：一覧から、値のデータの種類を選択します。デフォルトは **[DWORD]** です。選択できるオプションは以下のとおりです。
  - **DWORD**：32ビットの未署名の整数
  - **String**：あらゆる文字列
  - **Extended string**：%TEMP%や%USERPROFILE%のような環境変数を含めることができる文字列値
  - **Binary**：あらゆる任意のバイナリデータ
- **Value**：［Registry value name］に関連付ける値を入力します。たとえば、ProgramFilesDirの値を指定するには、「*C:\Program Files*」と入力します。
- レジストリキー情報を保存する場合は **[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：既存のレジストリキーを削除するには、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。

  既存のキーをレジストリ編集するには、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。 **[Registry Policy]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

制限デバイスポリシー

Feb 27, 2017

制限デバイスポリシーでは、ユーザーデバイスの特定の機能（カメラなど）を許可または制限します。また、セキュリティ制限、メディアコンテンツの制限、ユーザーがインストールできる（できない）アプリ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。

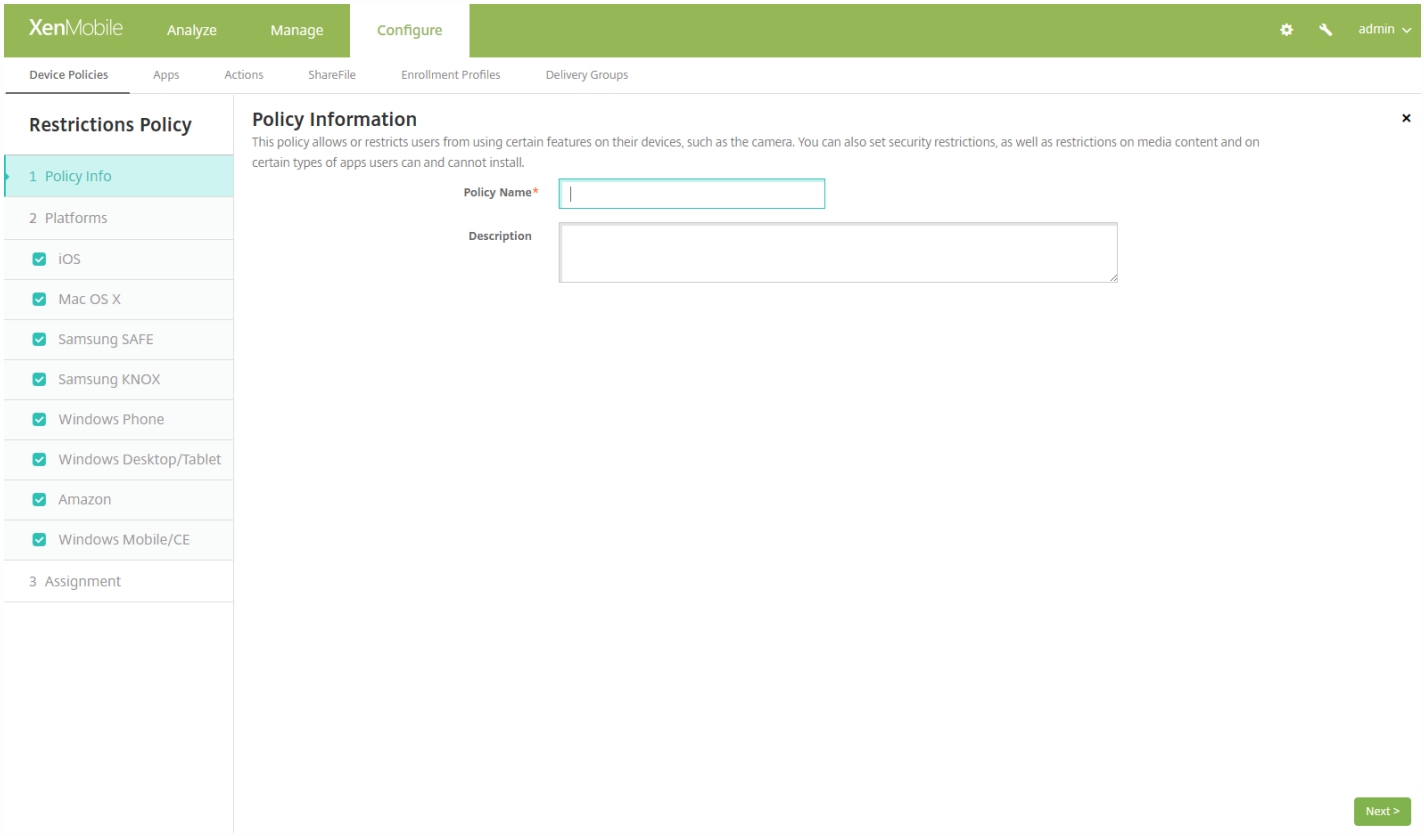
ヒント：オプションで **[オン]** を選択した場合、ユーザーが該当する操作を実行、または該当する機能を使用できるようになります。次に例を示します。

- **カメラ**。 **オン**の場合、ユーザーはデバイスでカメラを使用できます。**オフ**の場合、ユーザーはデバイスでカメラを使用できません。
- **スクリーンショット**。 **オン**の場合、ユーザーはデバイスでスクリーンショットを取得できます。**オフ**の場合、ユーザーはデバイスでスクリーンショットを取得できません。

1. XenMobileコンソールで、 **[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。 **[新しいポリシーの追加]** ページが開きます。

3. **[制限]** をクリックします。制限の **[ポリシー情報]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**： 任意で、ポリシーの説明を入力します。

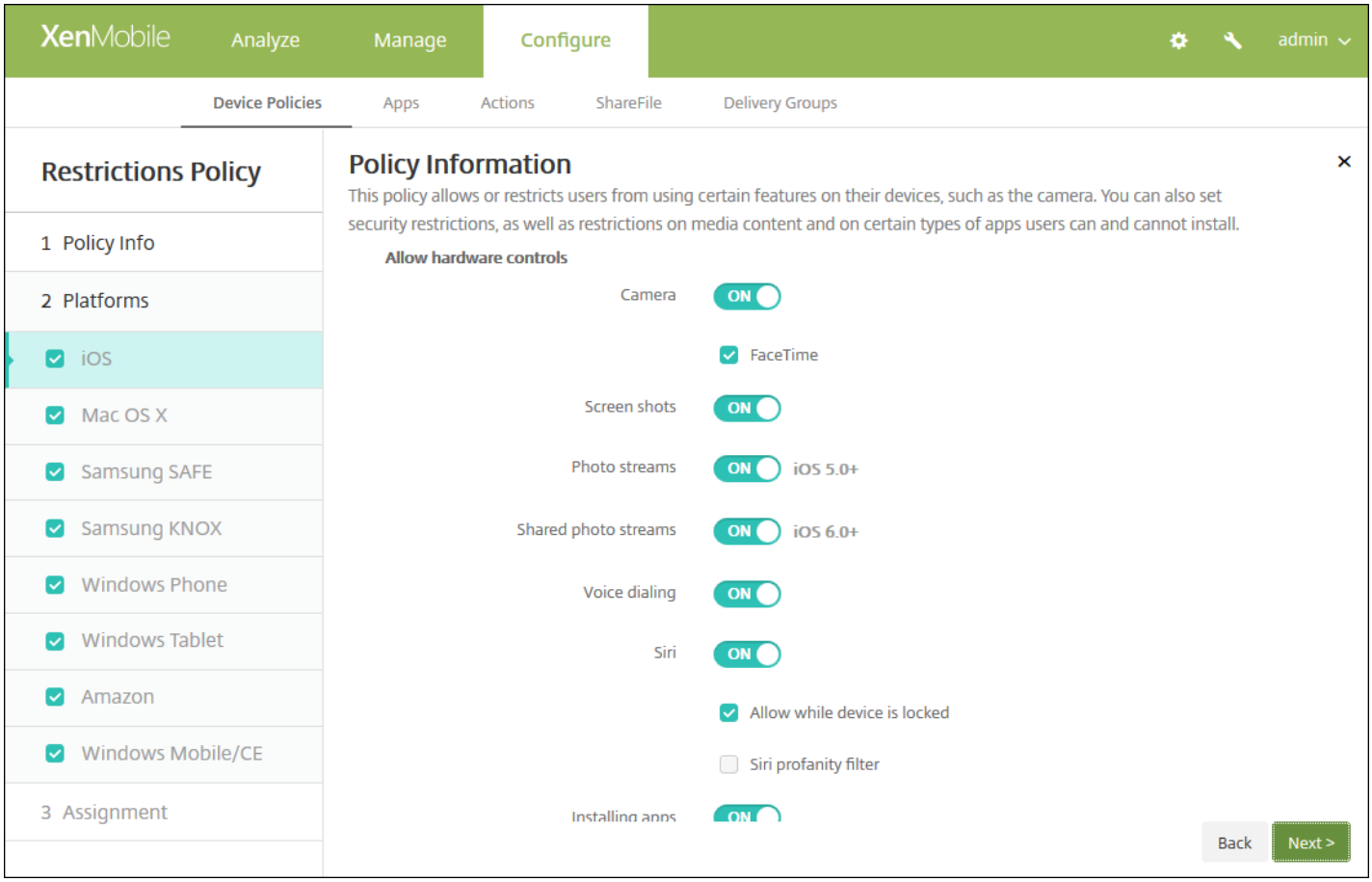
4. **[次へ]** をクリックします。 **[ポリシープラットフォーム]** ページが開きます。

5. **[プラットフォーム]** の下で、追加するプラットフォームをオンにします。このとき、選択したプラットフォームごとにポリシー情報を変更できます。以下のセクションで、制限する機能をクリックすると、設定が **[オフ]** に変わります。特に注記がない場合は、デフォルト設定で機能は有効です。

選択したプラットフォーム：
iOSの場合はこちらの設定を構成します。
Mac OS Xの場合はこちらの設定を構成します。
Samsung SAFEの場合はこちらの設定を構成します。
Samsung KNOXの場合はこちらの設定を構成します。
Windows Phoneの場合はこちらの設定を構成します。
Windows Tabletの場合はこちらの設定を構成します。
Amazonの場合はこちらの設定を構成します。
Windows Mobile/CEの場合はこちらの設定を構成します。

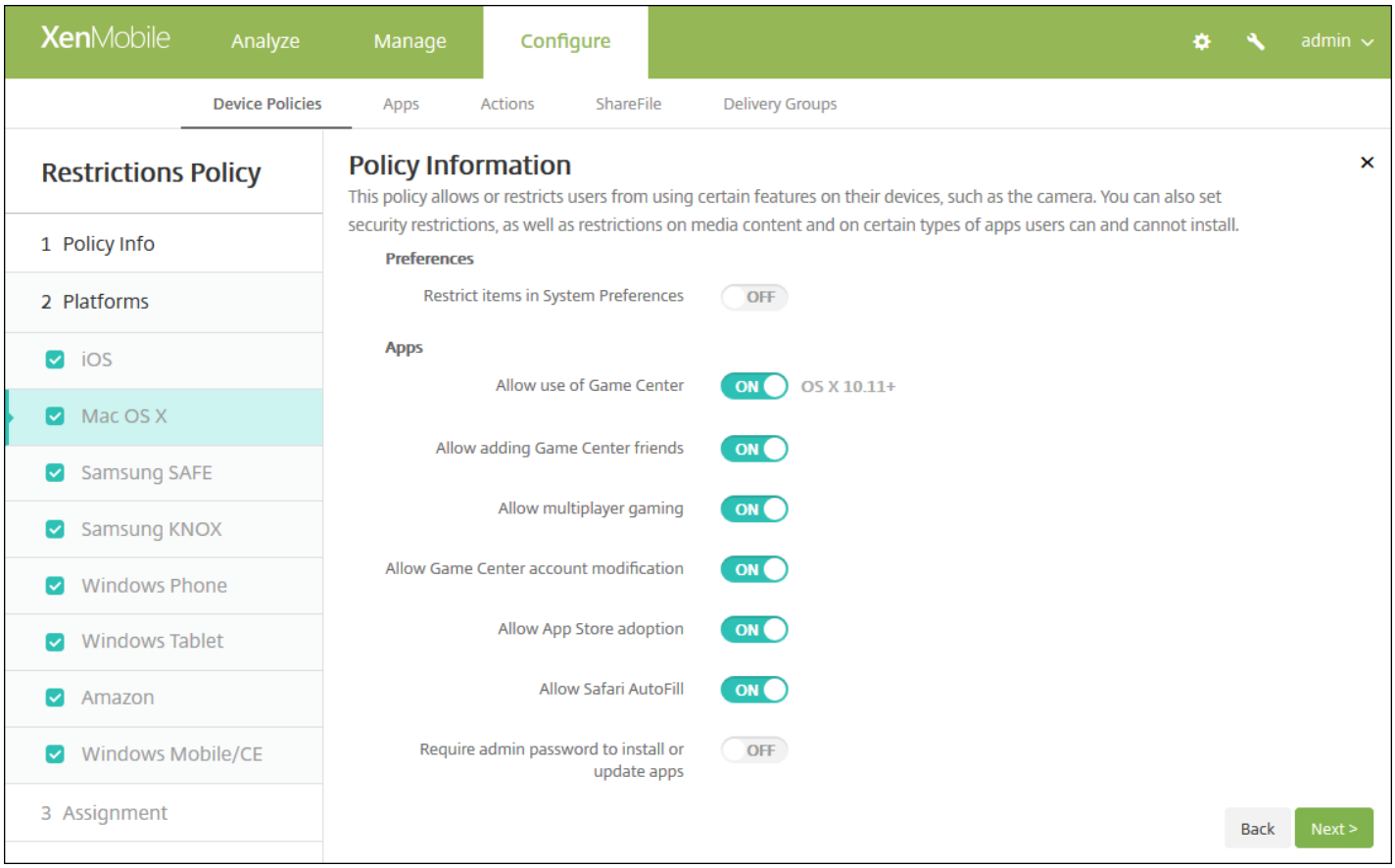
プラットフォームに対する制限の設定が完了した後の、プラットフォームの展開規則の設定方法については、このトピックの後半にある手順7を参照してください。

［iOS］を選択した場合は、次の設定を構成します。



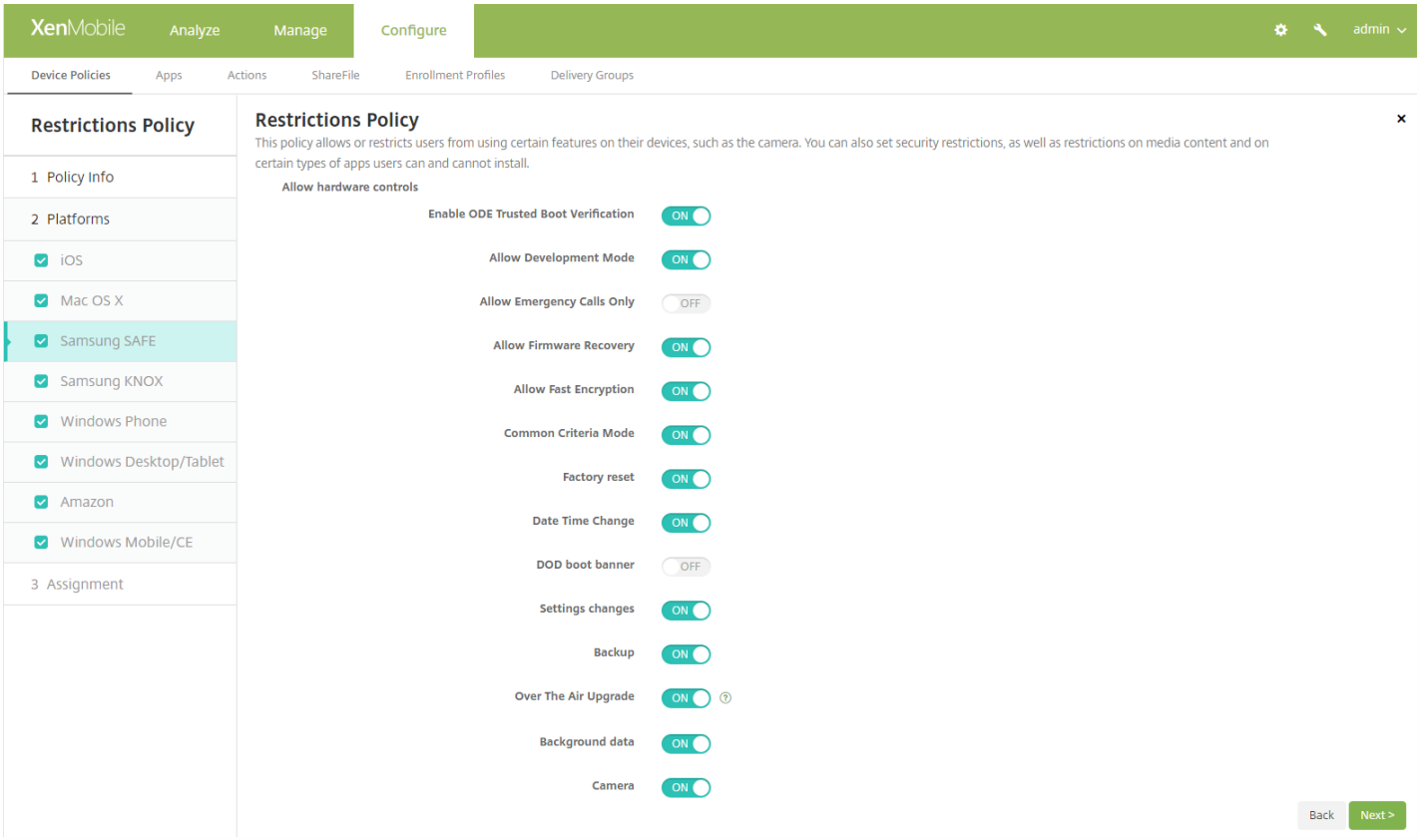
iOSの設定

Mac OS Xの設定の構成



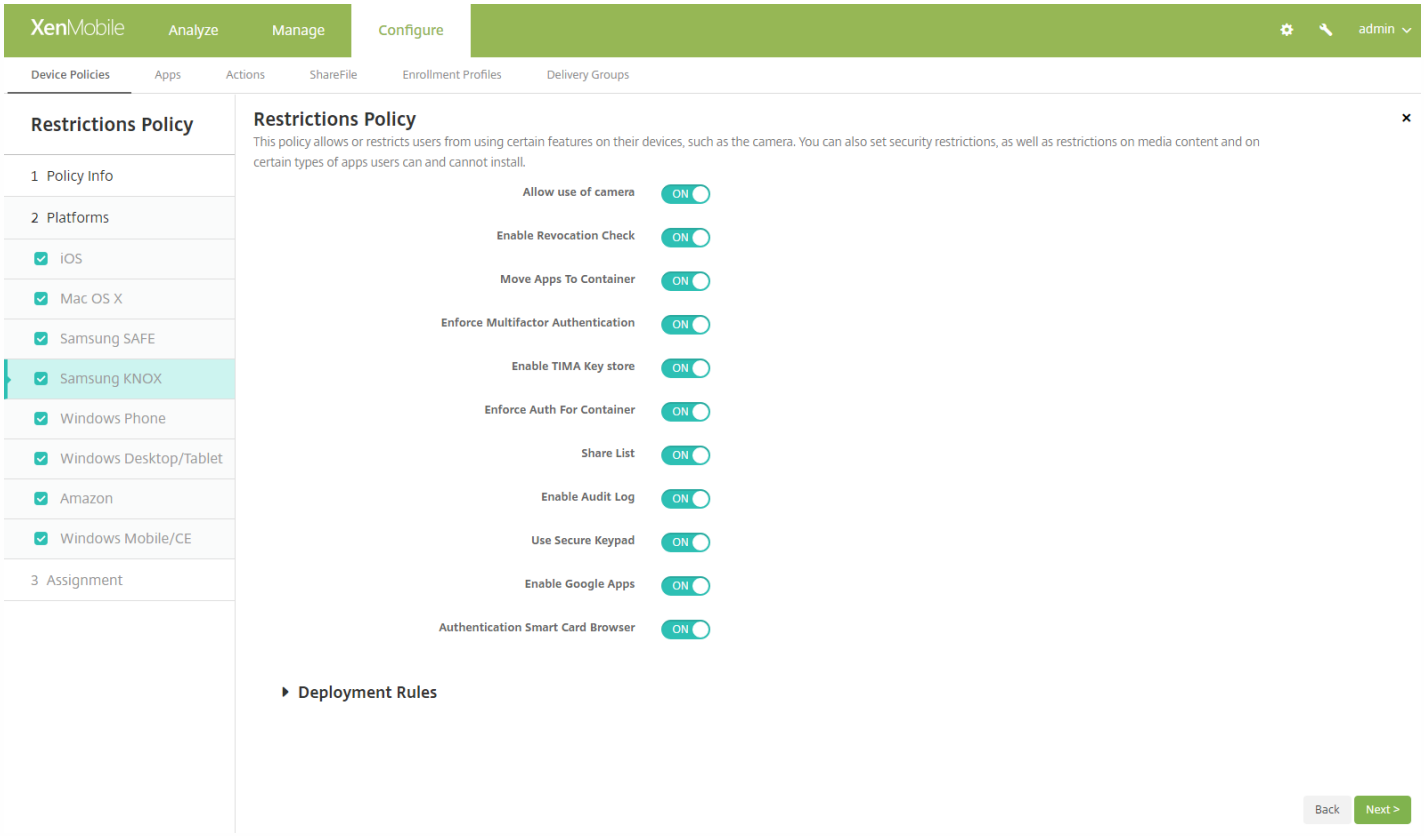
Mac OS Xの設定

Samsung SAFEの設定の構成



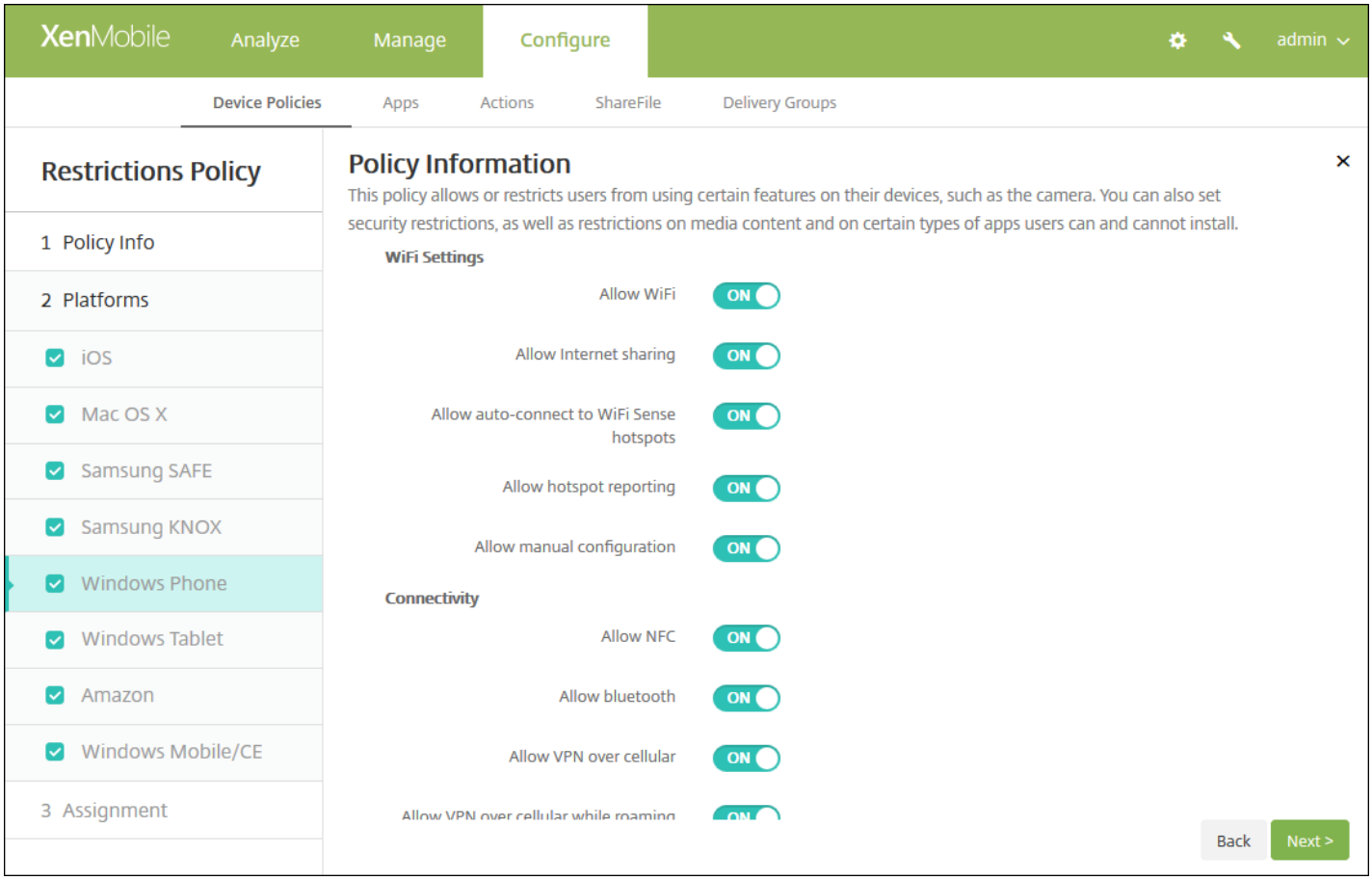
Samsung SAFEの設定

Samsung KNOXの設定の構成



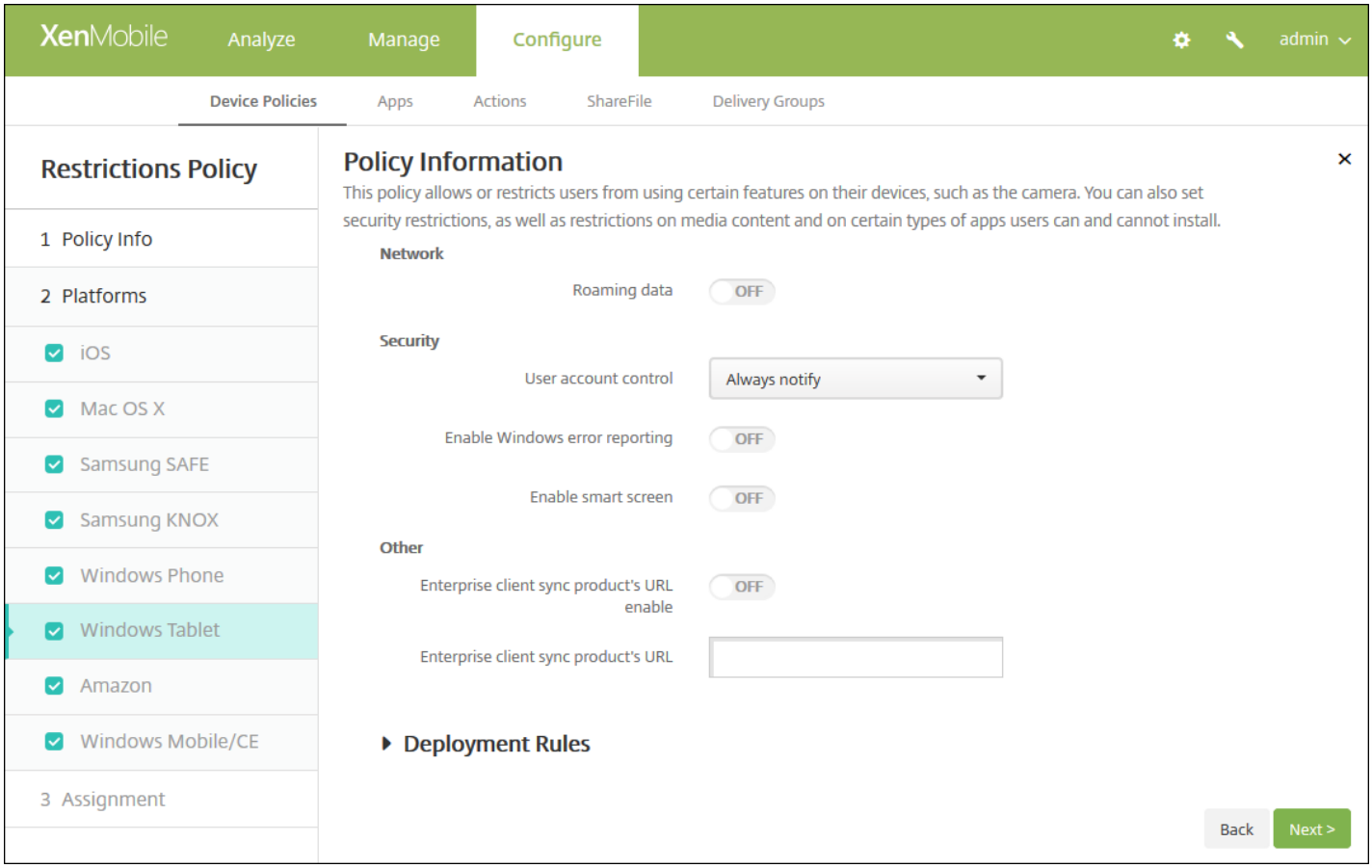
Samsung KNOXの設定

Windows Phoneの設定の構成



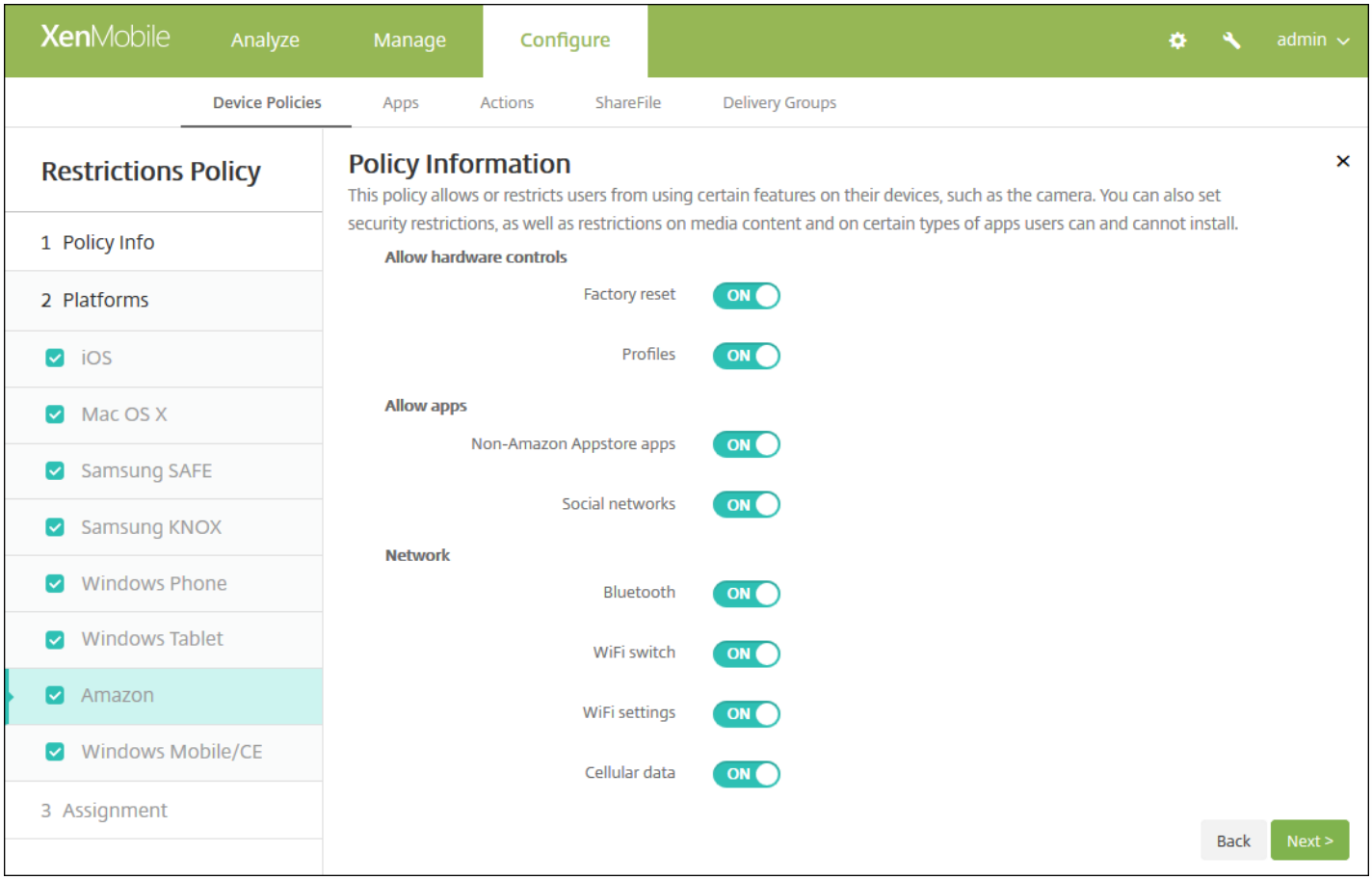
Windows Phoneの設定

Windowsデスクトップ/タブレットの設定の構成



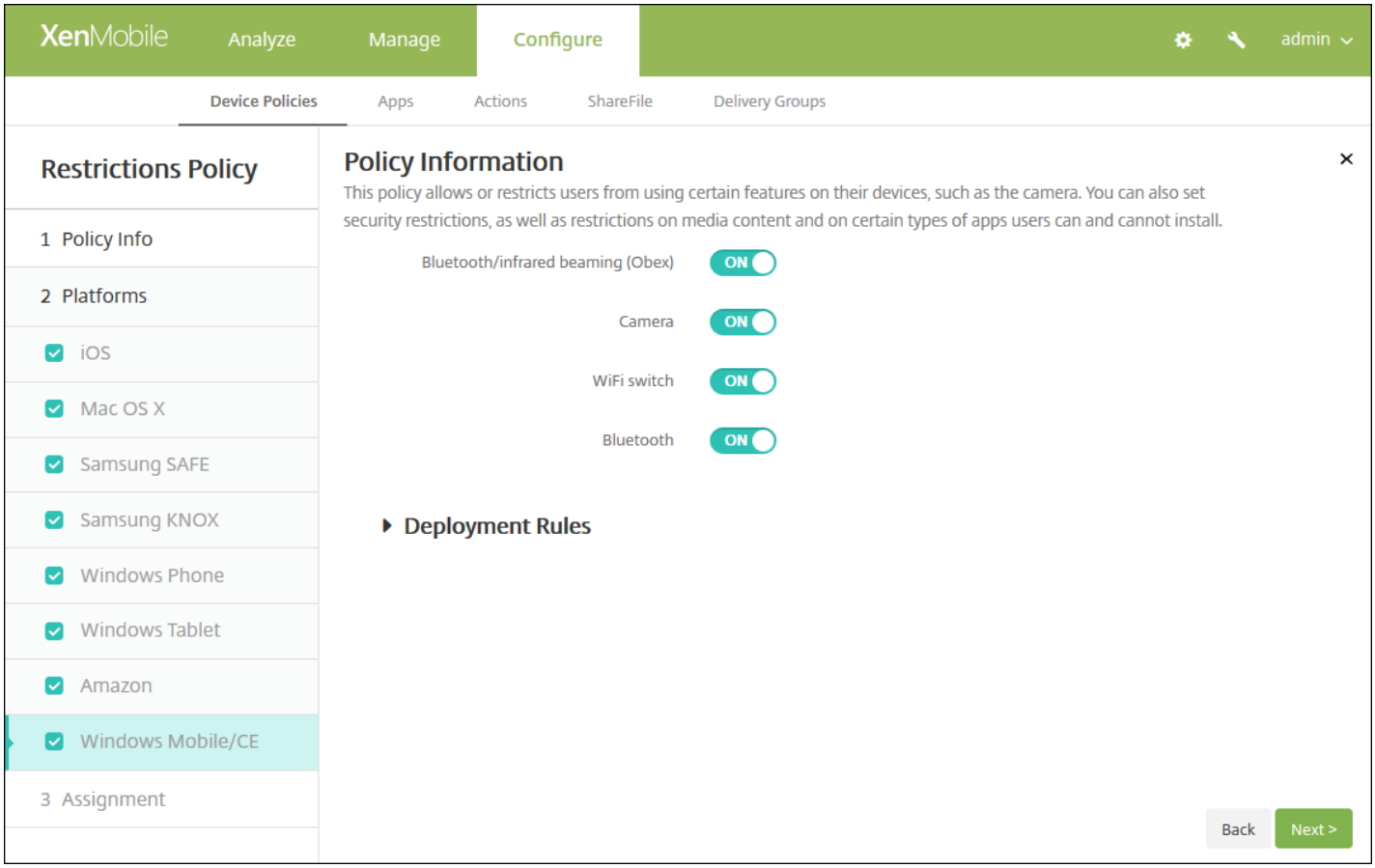
Windowsデスクトップ/タブレットの設定

Amazonの設定の構成



Amazonの設定

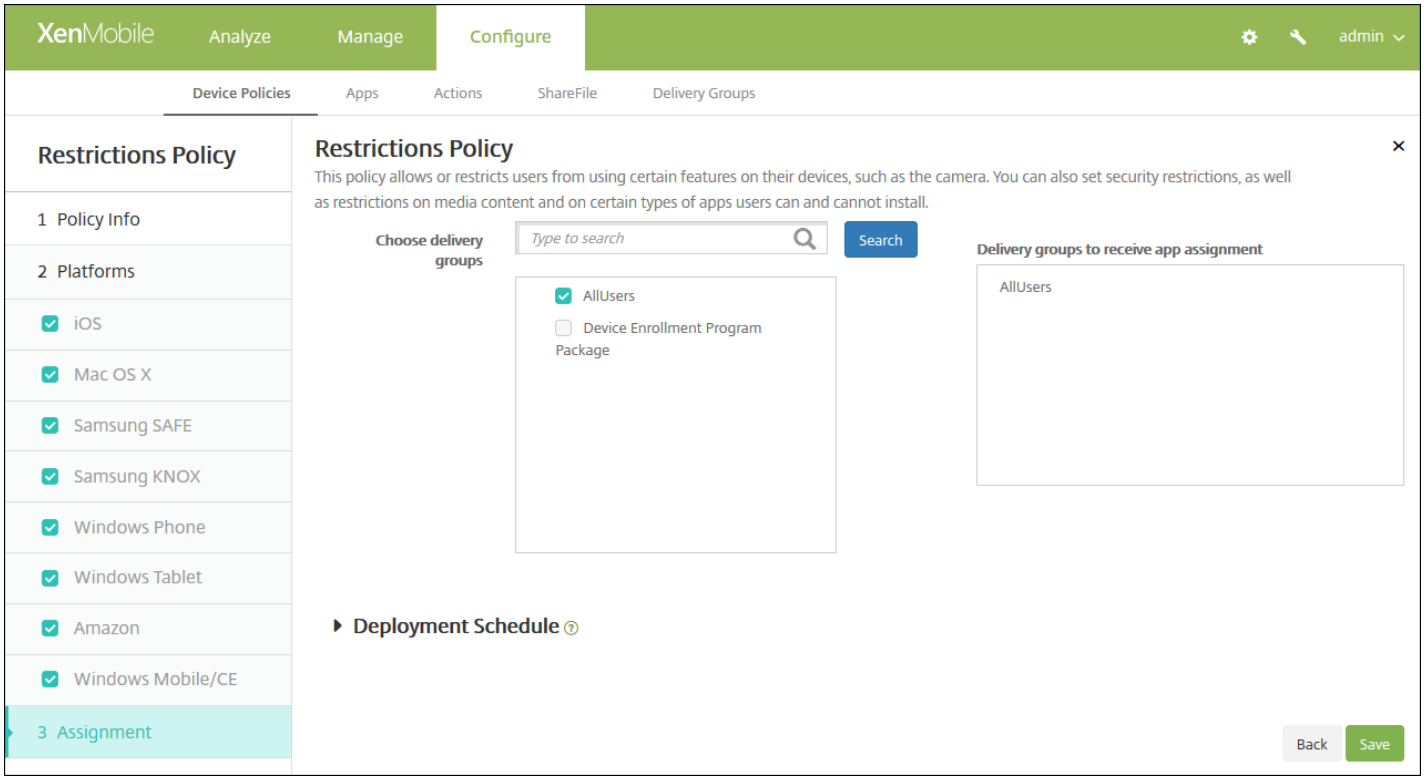
Windows Mobile/CEの設定の構成



Windows Mobile/CEの設定

7. 展開規則を構成します。

8. **[次へ]** をクリックします。 **[制限ポリシー]** 割り当てページが表示されます。



9. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** を選択した場合、そのほかのオプション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 **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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。

10. **[Save]** をクリックしてポリシーを保存します。

ローミングデバイスポリシー

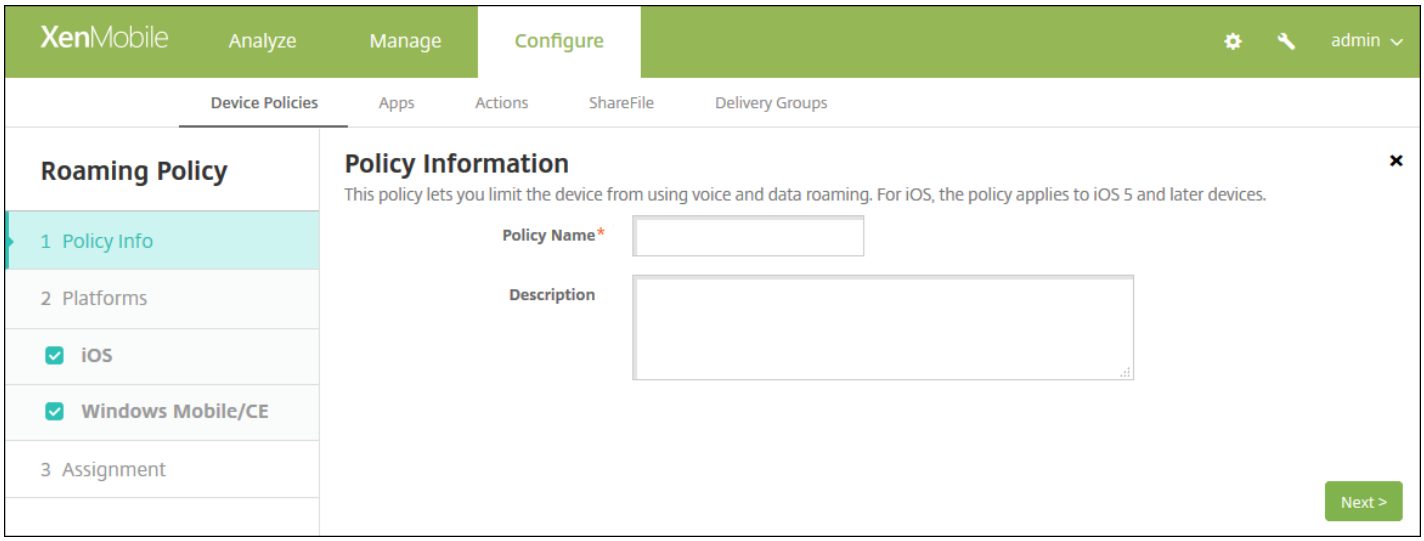
Feb 27, 2017

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、データローミングも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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[More]** をクリックした後、**[Network access]** の下の **[Roaming]** をクリックします。**[Roaming Policy]** 情報ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

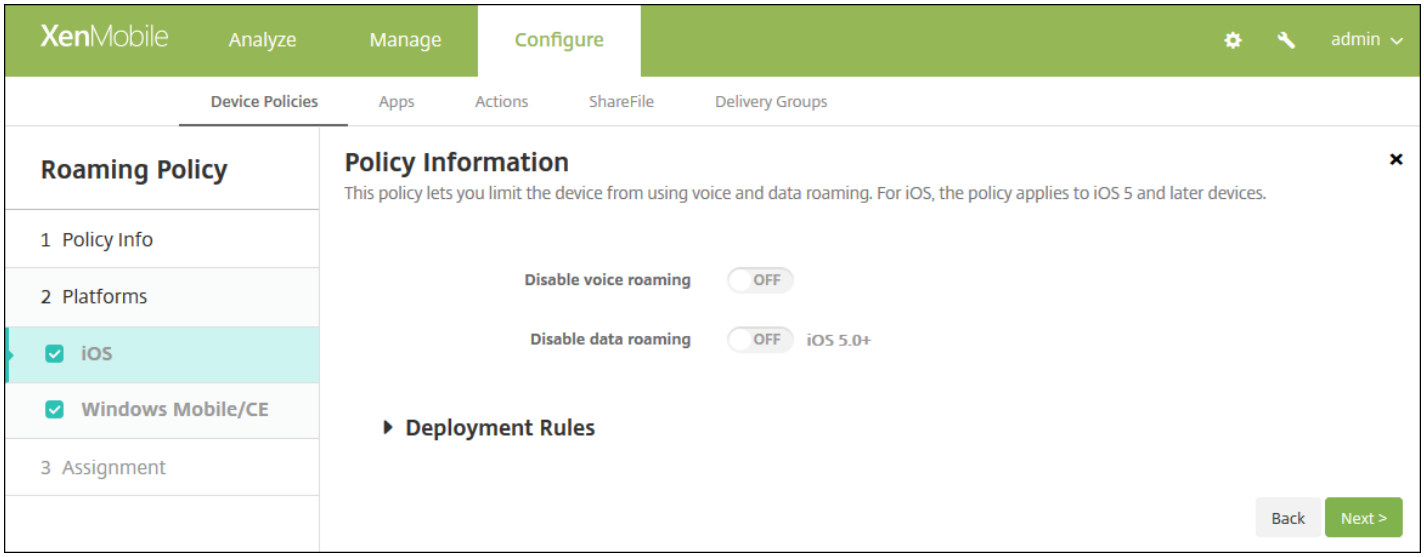
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。**[プラットフォーム]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

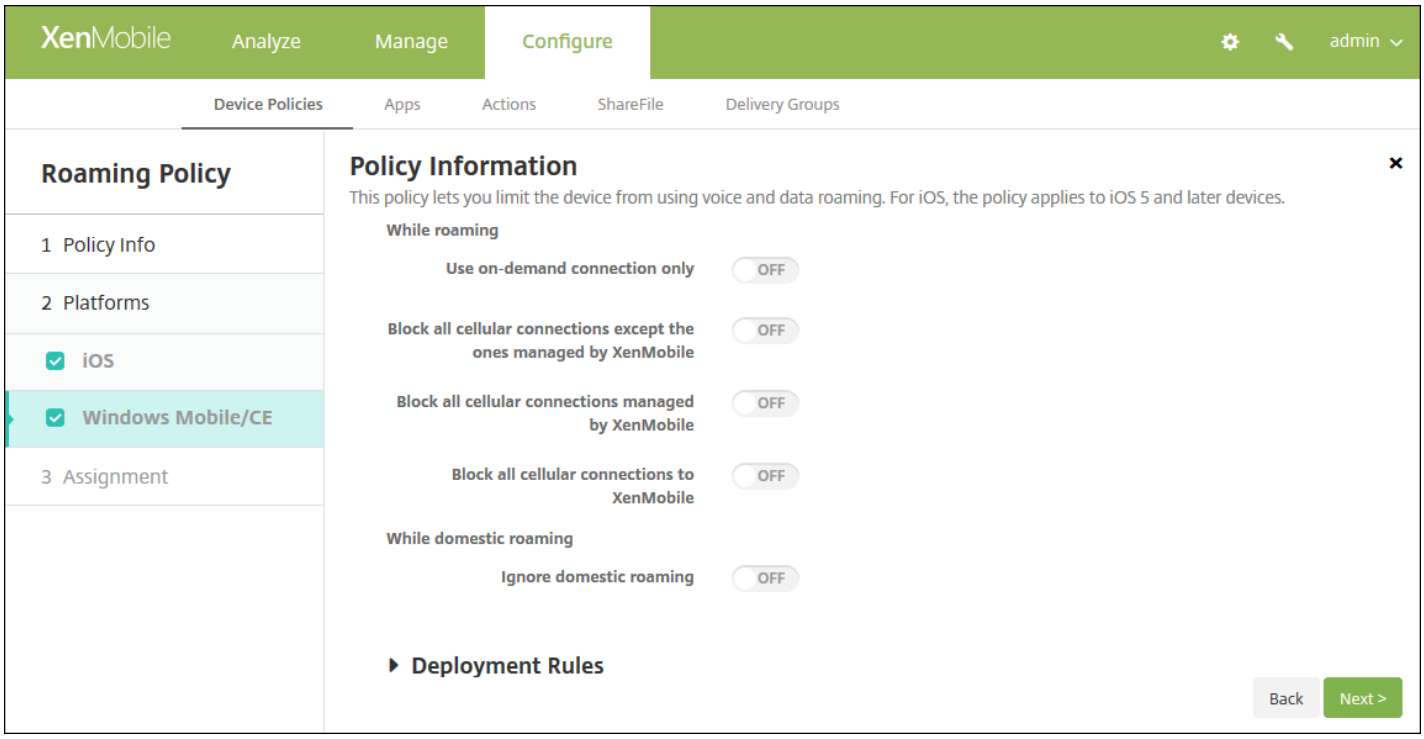
iOSの設定の構成



次の設定を構成します。

- **Disable voice roaming**： 音声通話ローミングを無効にするかどうかを選択します。このオプションを有効にした場合、データローミングは自動的に無効になります。デフォルトは **[OFF]** で、音声通話ローミングを許可します。
- **Disable data roaming**：データローミングを無効にするかどうかを選択します。このオプションは、音声通話ローミングが有効になっている場合にのみ使用できます。デフォルトは **[OFF]** で、データローミングを許可します。

Windows Mobile/CEの設定の構成



次の設定を構成します。

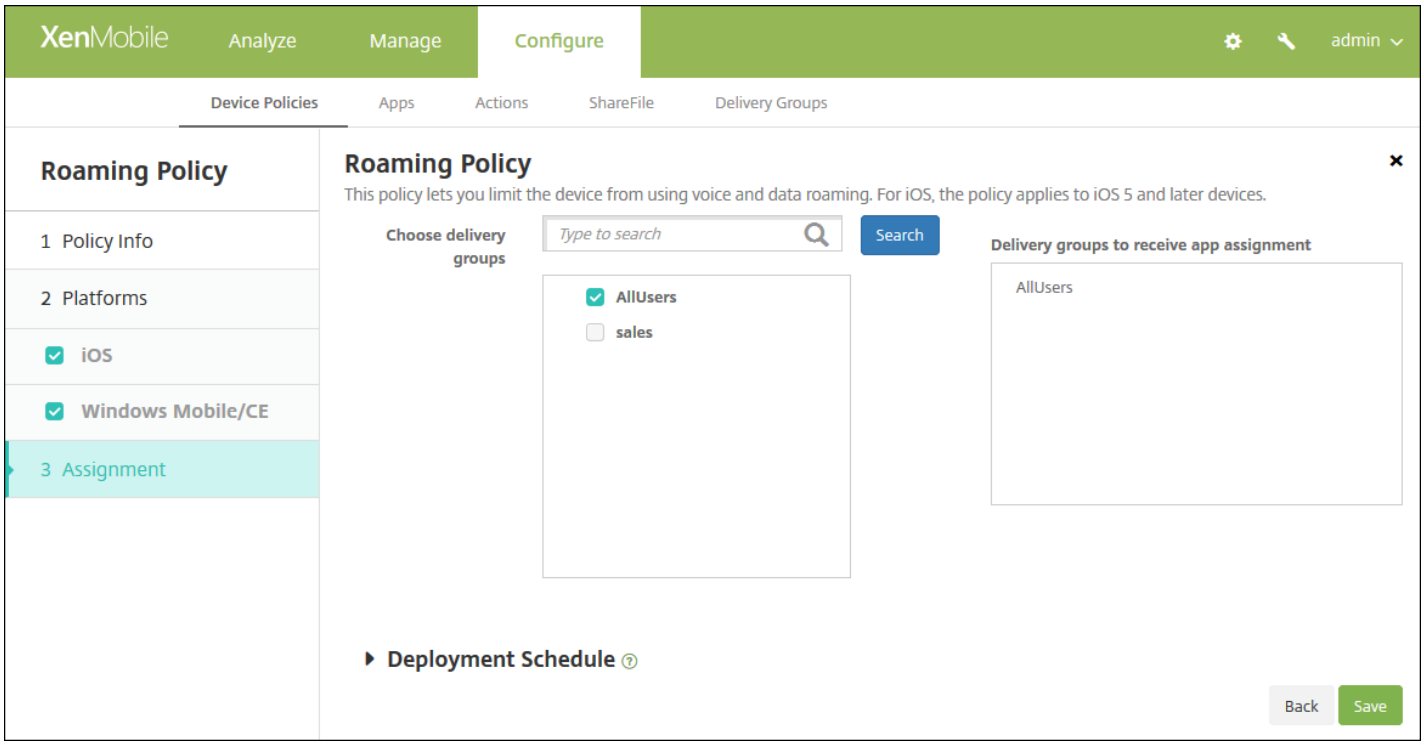
- ローミング中

- **Use on-demand connection only**： ユーザーがデバイスで接続を手動でトリガーする場合、またはモバイルアプリケーションが強制接続を要求する場合のみ（Exchange Serverに相応の設定があらかじめされている場合のプッシュ型のメール要求など）、デバイスはXenMobileに接続します。このオプションにより、デフォルトデバイス接続スケジュールポリシーは一時的に無効化される点に注意してください。
- **Block all cellular connections except the ones managed by XenMobile**： XenMobileアプリケーショントンネルまたはそのほかのXenMobileデバイス管理タスクで公式に宣言されているデータトラフィックを除き、ほかのデータはデバイスによって送受信されません。たとえば、このオプションではデバイスのWebブラウザーを使用したインターネットへの接続がすべて無効化されます。
- **Block all cellular connections managed by XenMobile**： XenMobileトンネルを使用して転送されるすべてのアプリケーションデータ（XenMobile Remote Supportを含む）がブロックされます。ただし、純粋なデバイス管理に関連するデータトラフィックはブロックされません。
- **Block all cellular connections to XenMobile**： この場合、USB、Wi-Fi、またはデフォルトのモバイル事業者のモバイルネットワークを通じてデバイスが再接続されるまで、デバイスとXenMobile間のトラフィックの転送は発生しません。

- **国内ローミング中**
  - **Ignore domestic roaming**： ユーザーが国内でローミングしている間はデータがブロックされません。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Roaming Policy]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[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 **[オン]** です。 **[オフ]** 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 **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[保存]** をクリックします。

Samsung MDMライセンスキーデバイスポリシー

Feb 27, 2017

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。

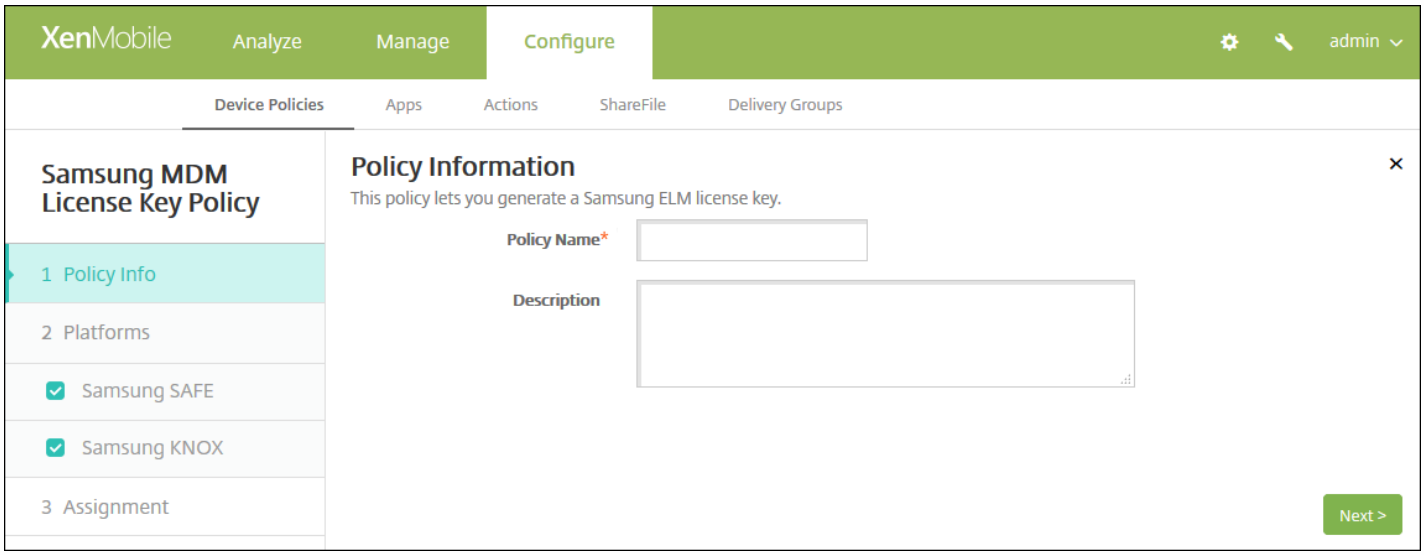
SAFEのポリシーおよび制限を展開する前に、組み込みのSamsung Enterprise License Management（ELM）キーをデバイスに展開することによってSAFE APIを有効にする必要があります。また、Samsung KNOX APIを有効にするには、Samsung ELMキーの展開に加え、Samsung KNOX License Management System（KLMS）を使用してSamsung KNOXワークスペースライセンスを購入する必要があります。Samsung KLMSはモバイルデバイス管理（MDM：Mobile Device Management）ソリュー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。

Secure Hub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。

1. XenMobileコンソールで、**[構成]**の**[デバイスポリシー]**をクリックします。**[デバイスポリシー]**ページが開きます。

2. **[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**[Samsung MDM License Key]**をクリックします。**[Samsung MDM License Key Policy]**情報ページが開きます。



4. **[ポリシー情報]**ペインで、以下の情報を入力します。

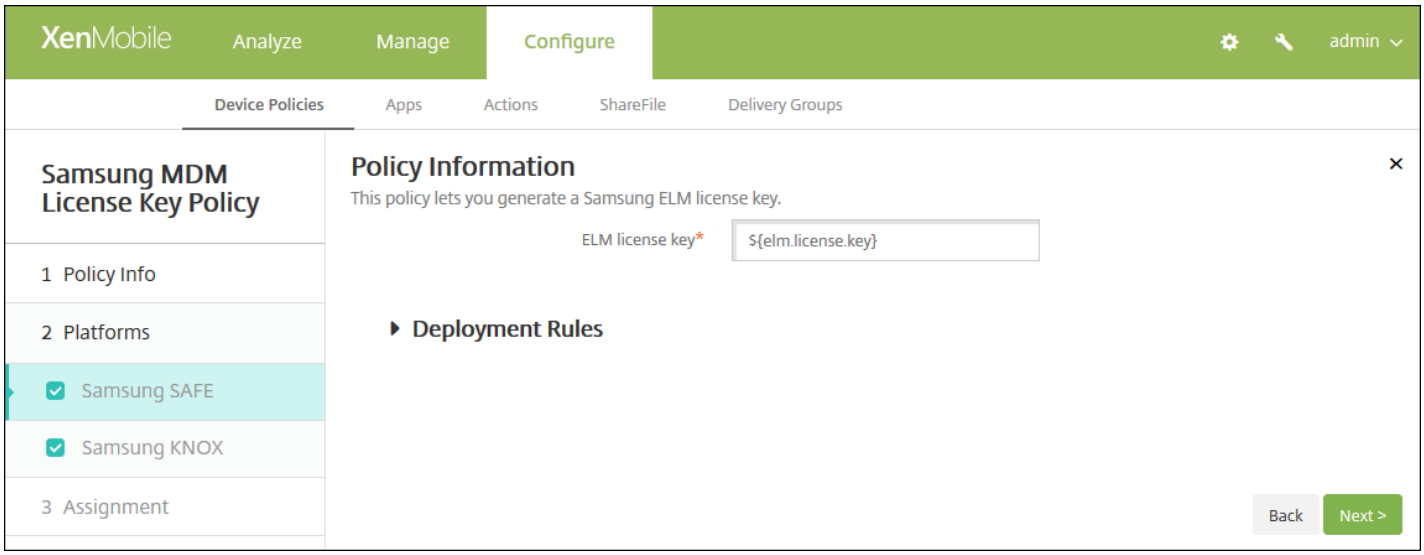
- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]**をクリックします。**[Platforms]**ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

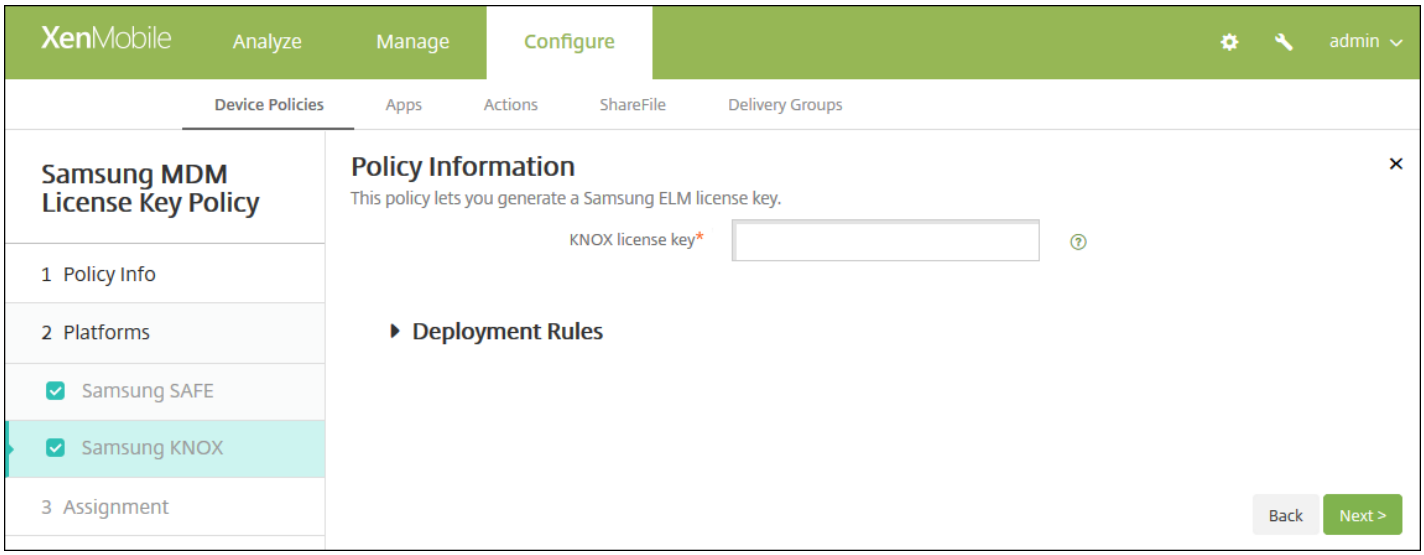
Samsung SAFEの設定の構成



次の設定を構成します。

- **ELM License key**：このフィールドには、既にELMライセンスキーを生成するマクロが入力されています。このフィールドが空白の場合は、「${elm.license.key}」というマクロを入力します。

Samsung KNOXの設定の構成

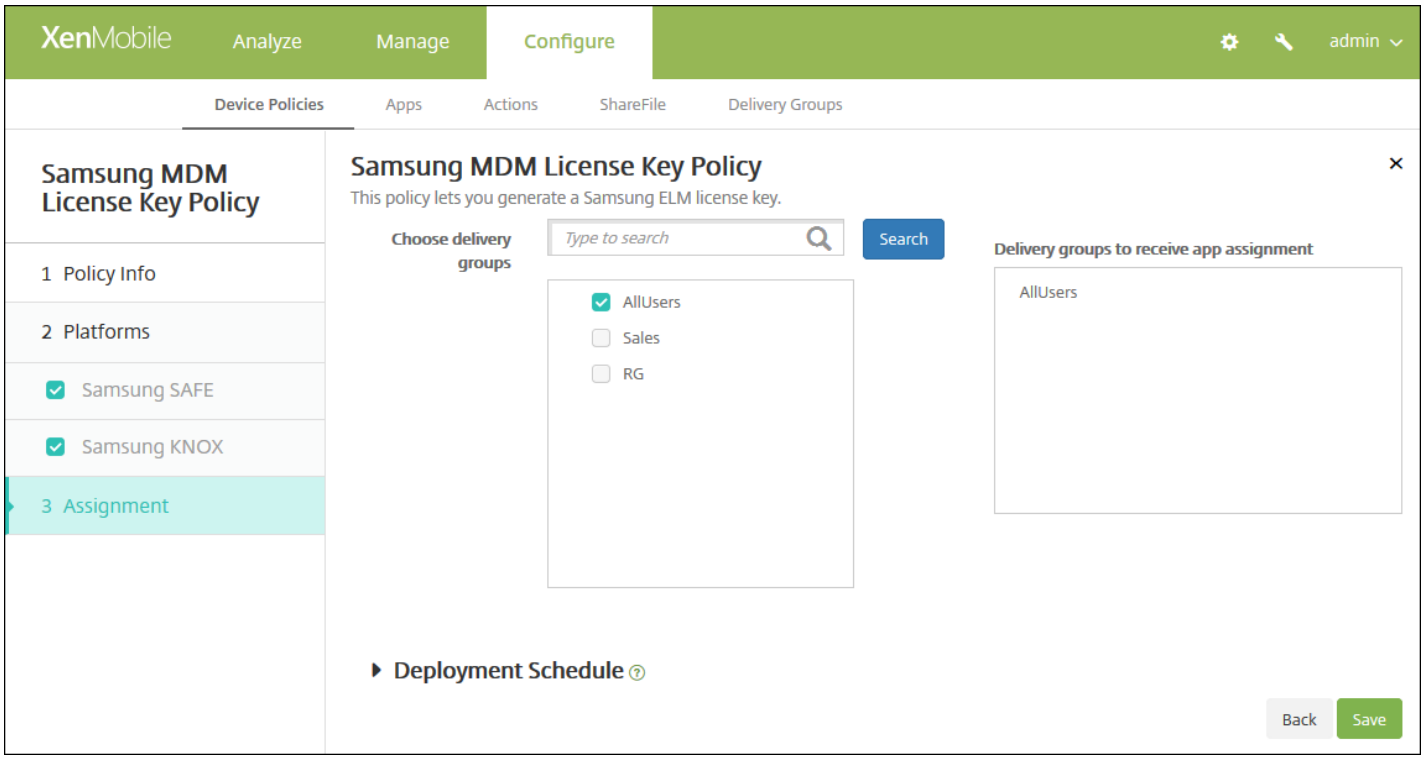


次の設定を構成します。

- **KNOX License key**：Samsungから取得したKNOXライセンスキーを入力します。

7. 展開規則を構成します。

8. **[次へ]** をクリックします。 **[Samsung MDMライセンスキーポリシー]** 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. **[展開スケジュール]** 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 **[オン]** です。 **[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[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 **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

Samsung SAFEのファイアウォールデバイスポリシー

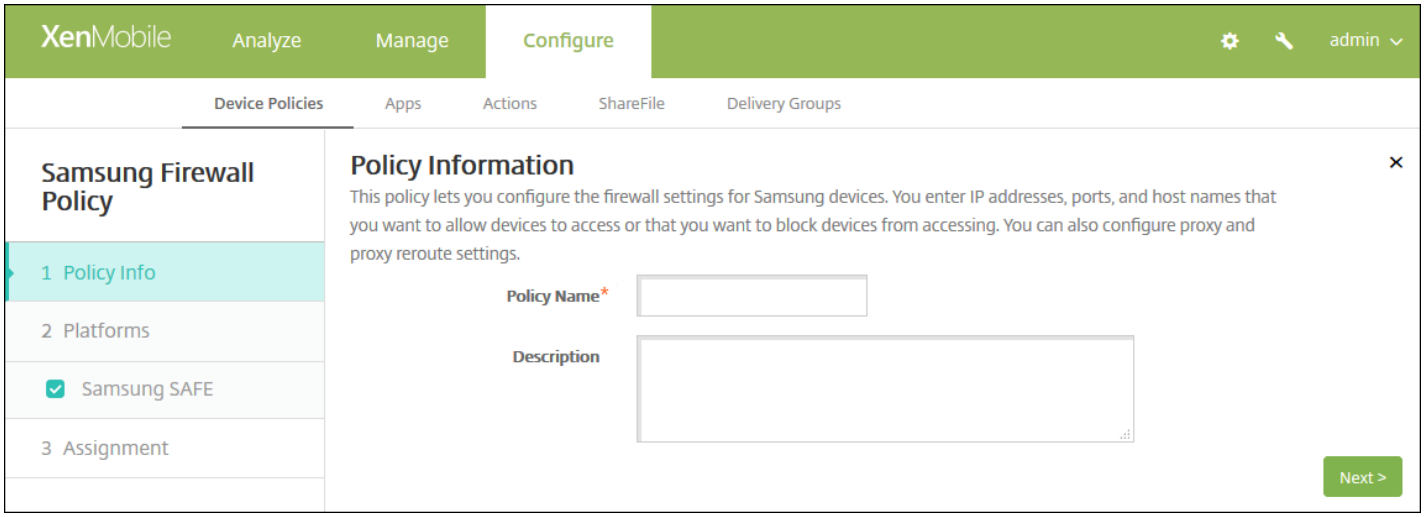
Feb 27, 2017

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

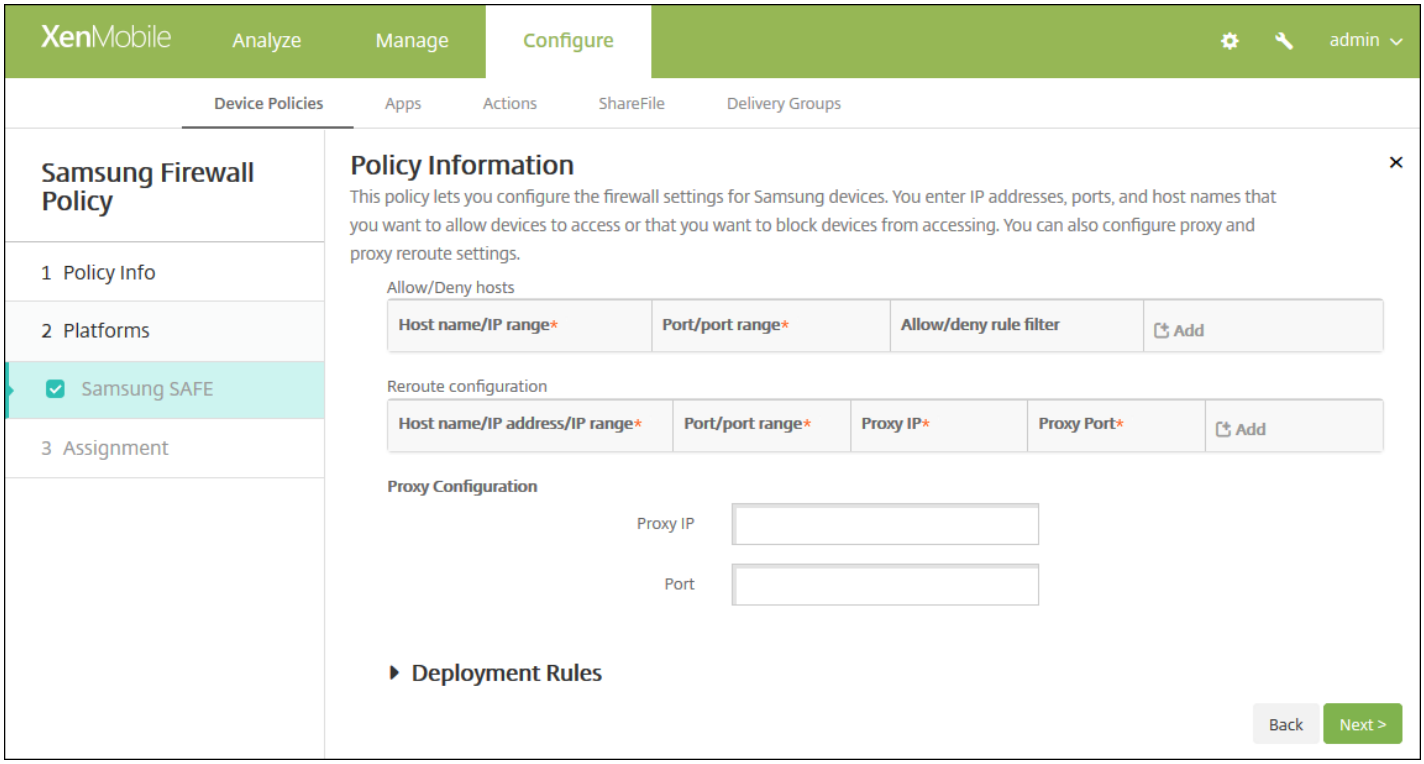
3. **[More]** をクリックした後、**[Network access]** の下の **[Samsung Firewall]** をクリックします。**[Samsung ファイアウォール ポリシー]** ページが開きます。



4. **[ポリシー情報]** 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]** 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。

- **ホストを許可/禁止**
  - アクセスを許可または拒否するホストごとに、**[Add]** をクリックして以下の操作を行います。
    - **Host name/IP range**： ポリシーを適用するサイトのホスト名またはIPアドレスの範囲を入力します。
    - **Port/port range**： ポートまたはポートの範囲を入力します。
    - **Allow/deny rule filter**： サイトへのアクセスを許可する場合は［ホワイトリスト］を選択し、サイトへのアクセスを拒否する場合は［ブラックリスト］を選択します。
    - **[Save]** または **[Cancel]** をクリックします。
- **経路変更構成**
  - 構成するプロキシごとに、**[Add]** をクリックして以下の操作を行います。
    - **Host name/IP range**： プロキシ再ルーティングのホスト名またはIPアドレスの範囲を入力します。
    - **Port/port range**： ポートまたはポートの範囲を入力します。
    - **Proxy IP**： プロキシIPアドレスを入力します。
    - **Proxy port**： プロキシのポート番号を入力します。
    - **[Save]** または **[Cancel]** をクリックします。

    注： 既存のアイテムを削除するには、その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。

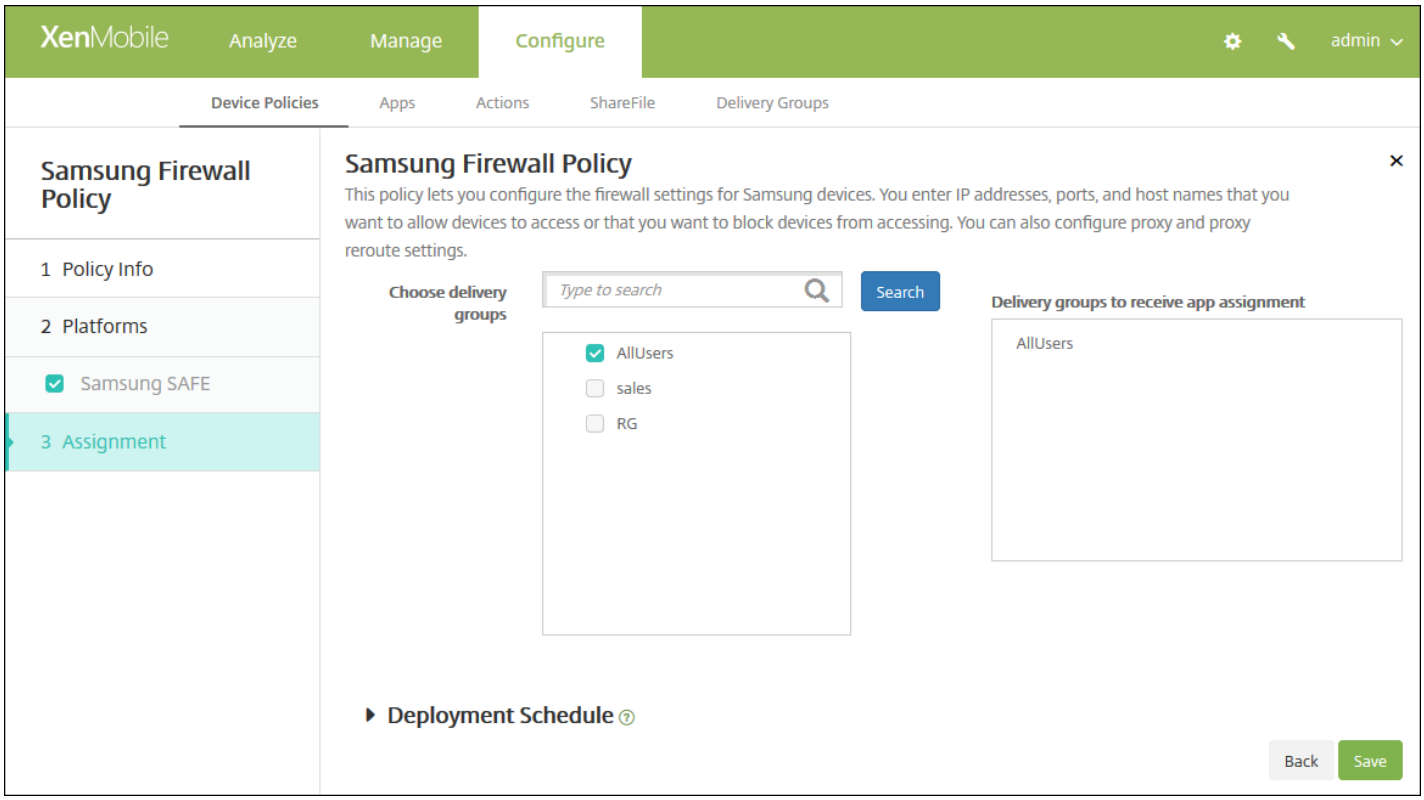
    既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、 **[Save]** をクリックして変更した項目を保存するか、 **[Cancel]** をクリックして項目を変更せずそのままにします。

- **ポート構成**
  - **Proxy IP**： プロキシサーバーの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。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Samsung Firewall Policy]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

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、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

SCEPデバイスポリシー

Feb 27, 2017

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。

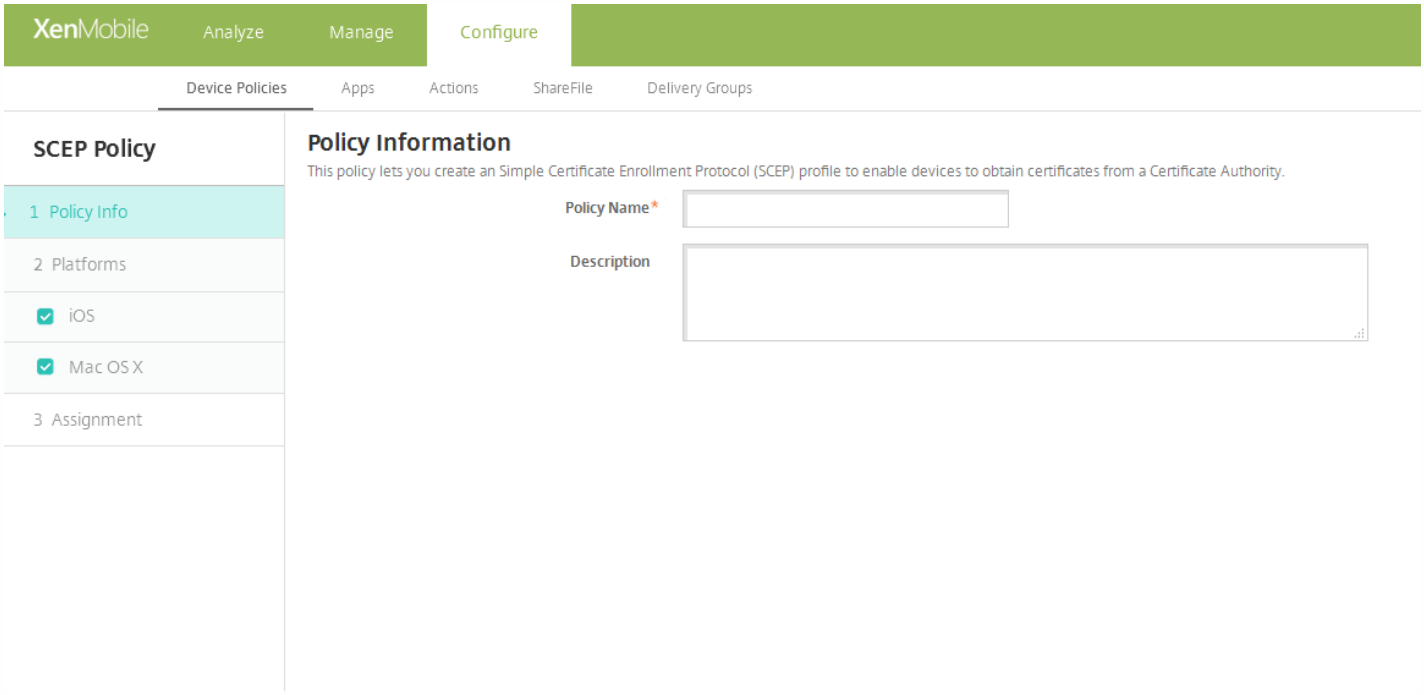
iOSの設定

Mac OS Xの設定

1. XenMobileコンソールで、**[構成]の[デバイスポリシー]**をクリックします。**[デバイスポリシー]**ページが開きます。

2. **[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**[SCEP]**をクリックします。**[SCEP Policy]**情報ページが開きます。



4. **[ポリシー情報]**ペインで、以下の情報を入力します。

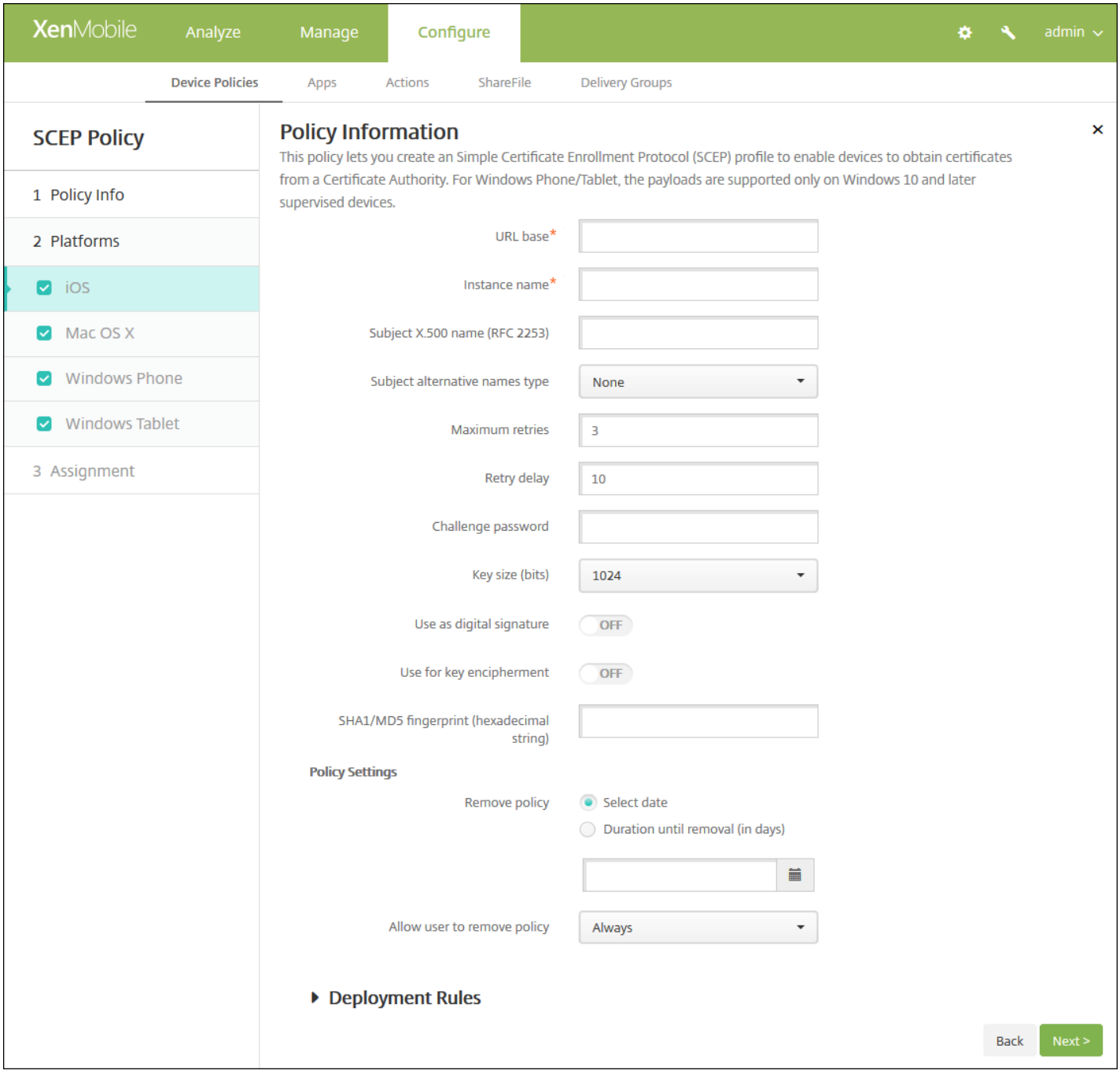
- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]**をクリックします。**[プラットフォーム]**ページが開きます。

6. **[プラットフォーム]**で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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



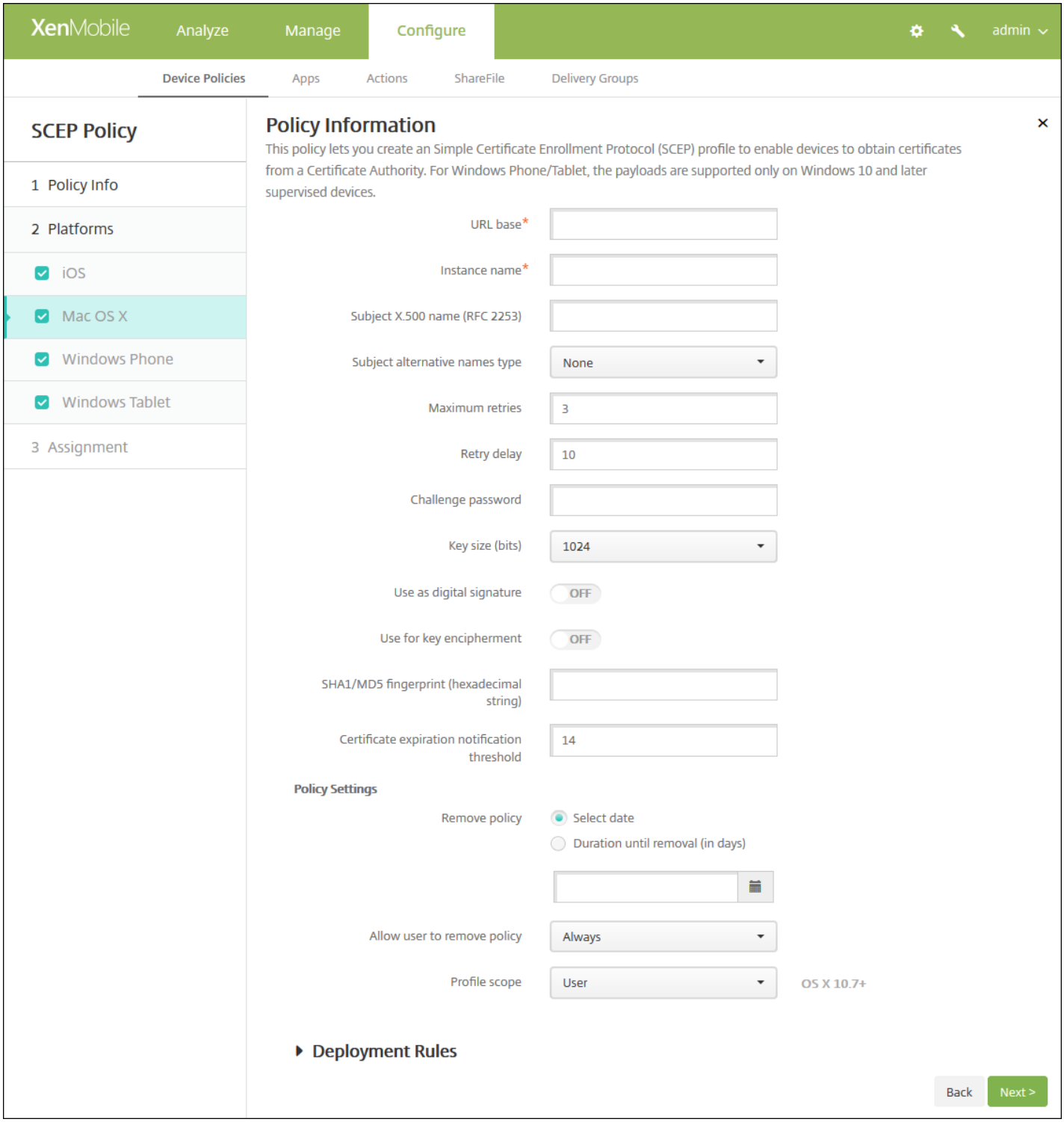
次の設定を構成します。

- **URL base**：HTTPまたはHTTPSを介したSCEP要求の送信先を定義するSCEPサーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するためにHTTPSを使用してください。これは必須の手順です。
- **Instance name**：SCEPサーバーで認識される文字列を入力します。たとえば、example.orgのようなドメイン名です。CAに複数のCA証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **Subject X.500 name (RFC 2253)**：オブジェクト識別子（OID）と値の配列として示されるX.500の名前の表現を入力しま

す。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]」のように解釈されます。OIDはドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。

- **［Subject alternative names type］**：一覧から、代替名の種類を選択します。SCEPポリシーは、CAが証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。**［None］**、**［RFC 822 name］**、**［DNS name］**、**［URI］**のいずれかを指定できます。
- **最大再試行回数**： SCEPサーバーがPENDING応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは**3**です。
- **再試行の遅延**： 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは**10**です。
- **チャレンジパスワード**： 事前共有シークレットを入力します。
- **［Key size（bits）］**：一覧から、**1024**または**2048**のいずれかのキーサイズ（ビット）を選択します。デフォルトは**1024**です。
- **Use as digital signature**：デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合（証明書がCAによって発行されたかどうかを確認する場合など）、公開キーを使ってハッシュを復号化する前に、SCEPサーバーではデジタル署名に証明書を使用できるかどうかが確認されます。
- **Use for key encipherment**：キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかが最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5 fingerprint (hexadecimal string)**：CAでHTTPが使われている場合、このフィールドを使って、CA証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CAの応答の信頼性を確認するためにデバイスで使われます。SHA1またはMD5のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。
- **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。

- **URL base**：HTTPまたはHTTPSを介したSCEP要求の送信先を定義するSCEPサーバーのアドレスを入力します。秘密キーは証明書署名要求（Certificate Signing Request：CSR）と一緒には送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するためにHTTPSを使用してください。これは必須の手順です。
- **Instance name**：SCEPサーバーで認識される文字列を入力します。たとえば、example.orgのようなドメイン名です。CAに複数のCA証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。

- **Subject X.500 name (RFC 2253)**：オブジェクト識別子（OID）と値の配列として示されるX.500の名前の表現を入力します。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]」のように解釈されます。OIDはドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
- **［Subject alternative names type］**：一覧から、代替名の種類を選択します。SCEPポリシーは、CAが証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。**［None］**、**［RFC 822 name］**、**［DNS name］**、**［URI］**のいずれかを指定できます。
- **最大再試行回数**： SCEPサーバーがPENDING応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは**3**です。
- **再試行の遅延**： 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは**10**です。
- **チャレンジパスワード**： 事前共有シークレットを入力します。
- **［Key size（bits）］**：一覧から、**1024**または**2048**のいずれかのキーサイズ（ビット）を選択します。デフォルトは**1024**です。
- **Use as digital signature**：デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合（証明書がCAによって発行されたかどうかを確認する場合など）、公開キーを使ってハッシュを復号化する前に、SCEPサーバーではデジタル署名に証明書を使用できるかどうかが確認されます。
- **Use for key encipherment**：キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかが最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5 fingerprint (hexadecimal string)**：CAでHTTPが使われている場合、このフィールドを使って、CA証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CAの応答の信頼性を確認するためにデバイスで使われます。SHA1またはMD5のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。
- **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。

7. 展開規則を構成します。

8. **［次へ］**をクリックします。**［SCEPポリシー］**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. **［展開スケジュール］**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**［オン］**です。**［オフ］**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［すぐに］です。
- **［あとで］**をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。

- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[常時接続に対する展開]** は適用されません。

11. **[Save]** をクリックしてポリシーを保存します。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

ストレージ暗号化デバイスポリシー

Feb 27, 2017

XenMobileでストレージ暗号化デバイスポリシーを作成して、内部ストレージと外部ストレージを暗号化したり、デバイスによっては、ユーザーがデバイスでストレージカードを使用できないようにしたりします。

Samsung SAFE、Windows Phone、Android Sonyデバイスに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

Samsung SAFEの設定

Windows Phoneの設定

Android Sonyの設定

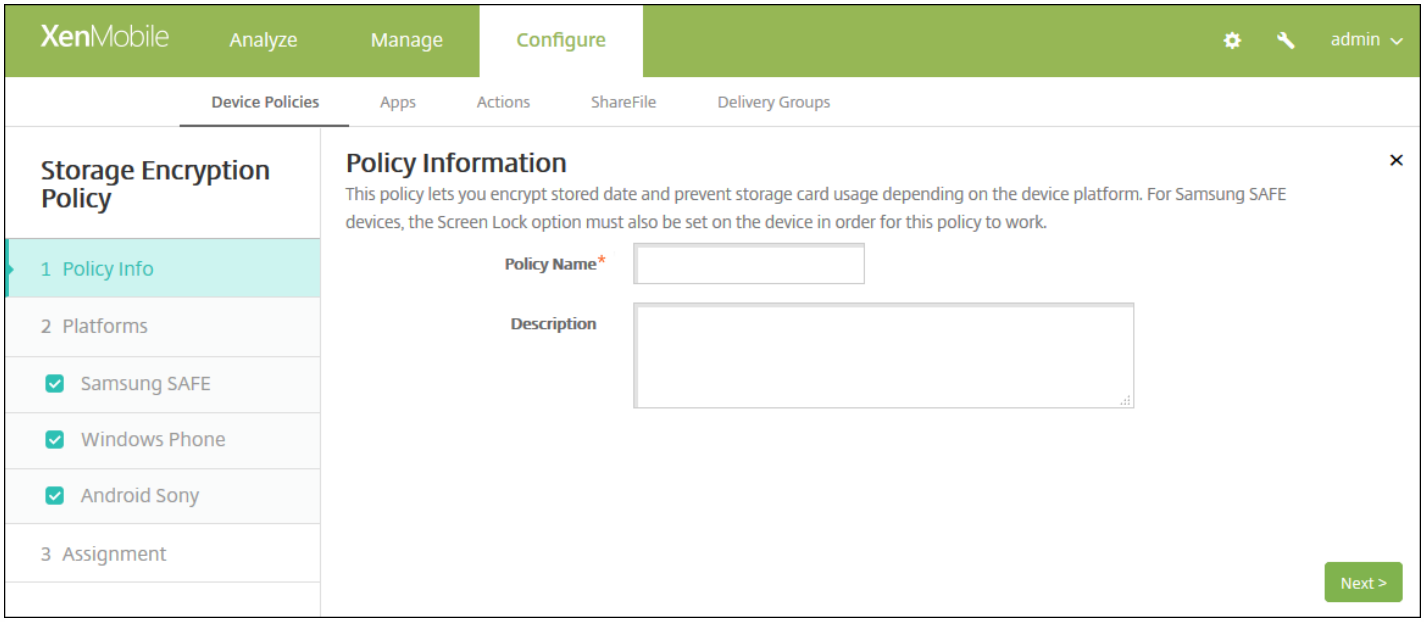
注：Samsung SAFEデバイスの場合は、このポリシーを構成する前に、次の要件が満たされていることを確認します。

- ユーザーのデバイスで画面のロックオプションを設定する必要があります。
- ユーザーのデバイスがコンセントに接続され、80%充電されている必要があります。
- 数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。

1. XenMobileコンソールで、**[構成]の[デバイスポリシー]**をクリックします。**[デバイスポリシー]**ページが開きます。

2. **[追加]**をクリックします。**[新しいポリシーの追加]**ダイアログボックスが開きます。

3. **[More]**をクリックした後、**[Security]**の下の**[Storage Encryption]**をクリックします。**[Storage Encryption Policy]**情報ページが開きます。



4. **[ポリシー情報]**ペインで、以下の情報を入力します。

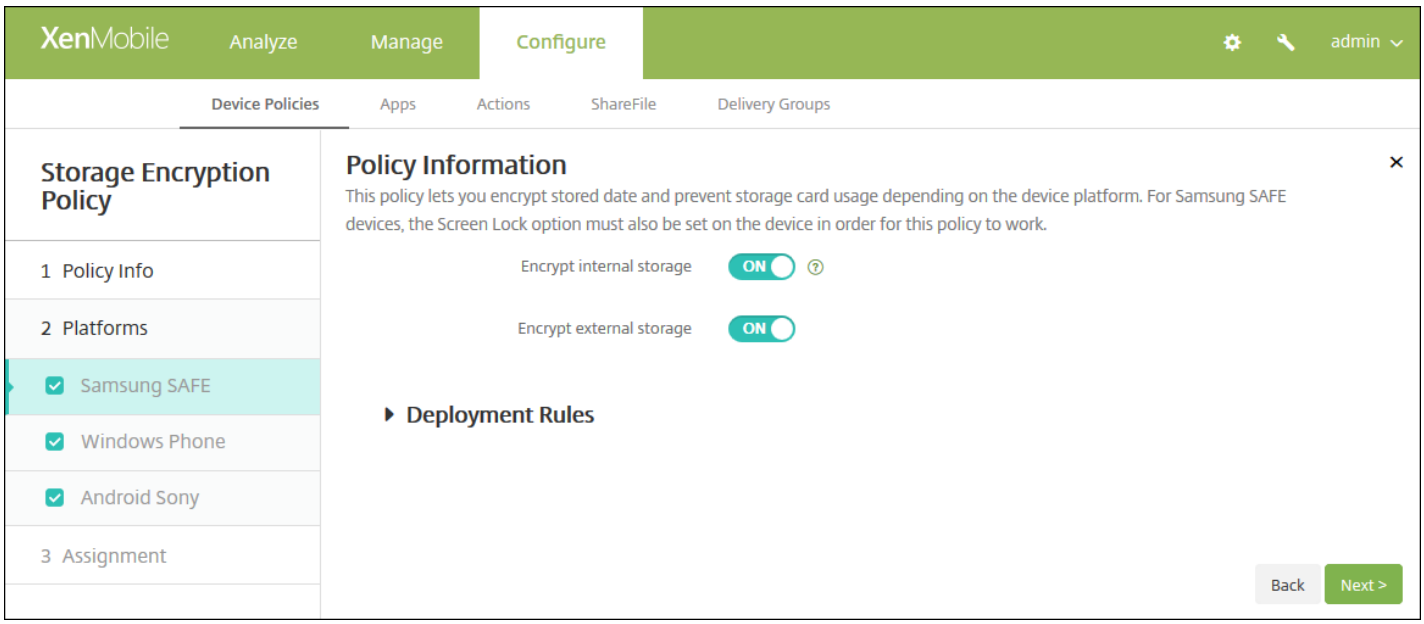
- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. [次へ] をクリックします。 [**Policy Platforms**] ページが開きます。

6. [**プラットフォーム**] で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

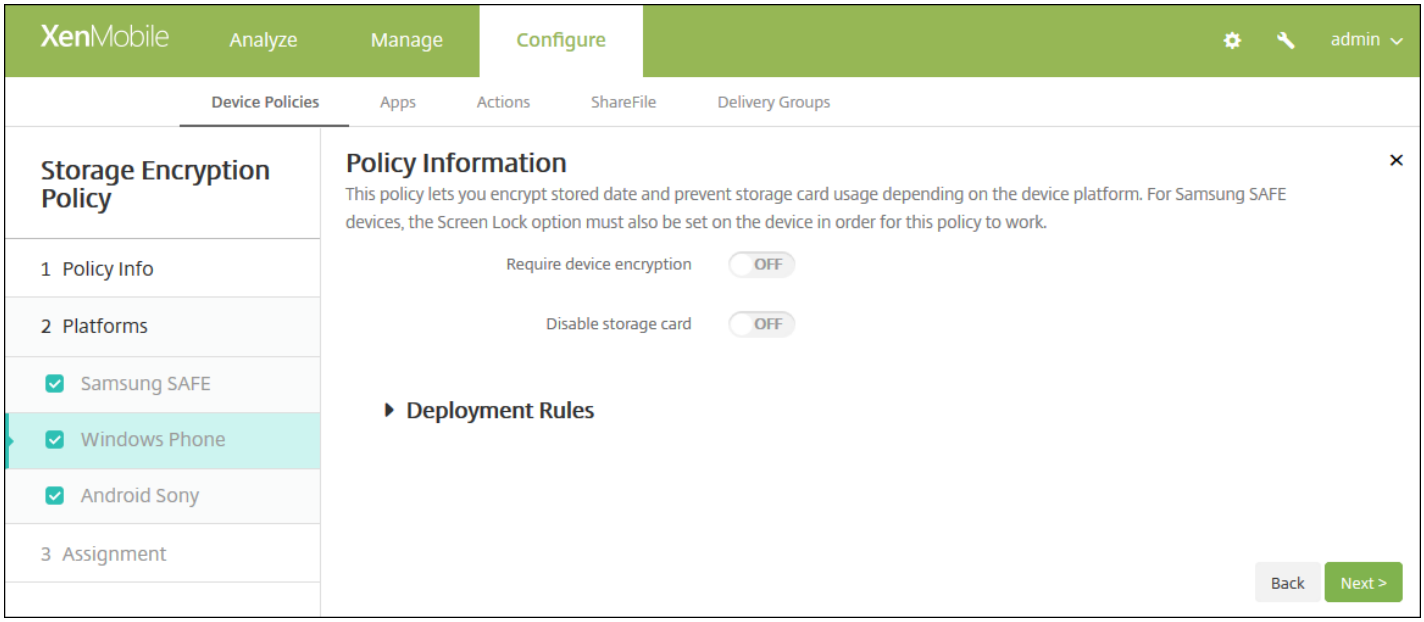
Samsung SAFEの設定の構成



次の設定を構成します。

- **Encrypt internal storage** : ユーザーのデバイスの内部ストレージを暗号化するかどうかを選択します。内部ストレージには、デバイスのメモリと内部ストレージが含まれます。デフォルトは [**ON**] です。
- **Encrypt external storage** : ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。デフォルトは [**ON**] です。

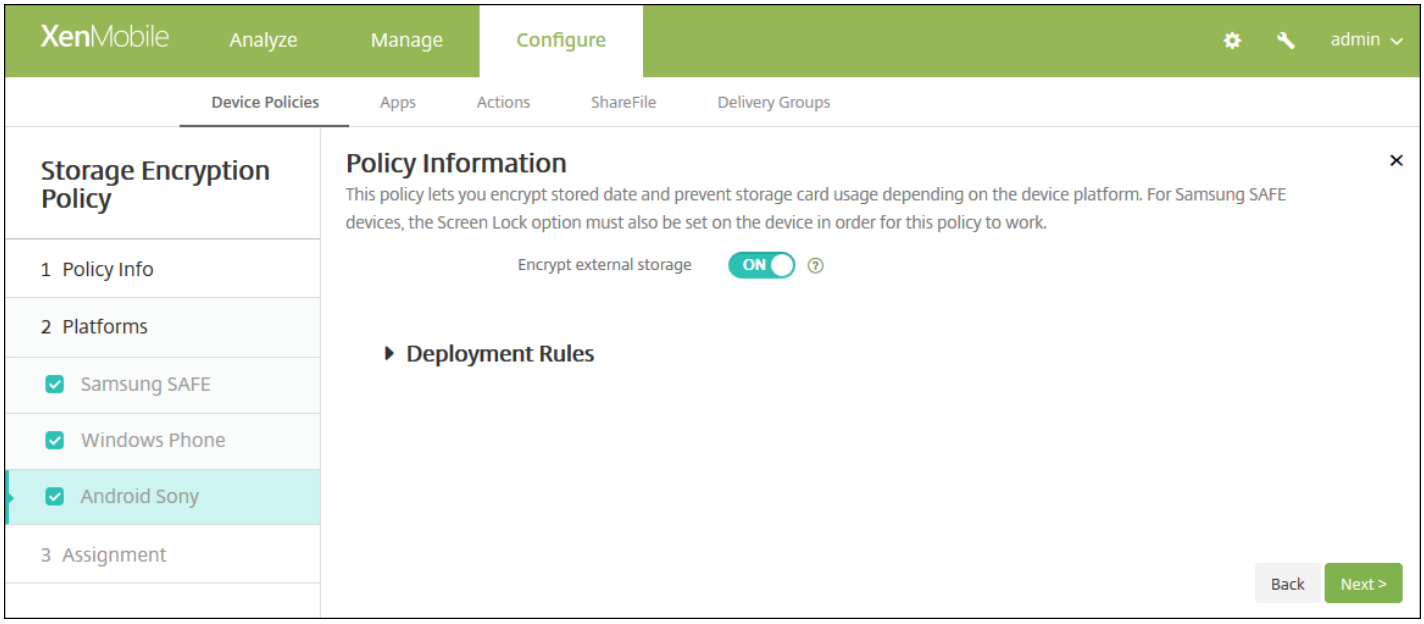
Windows Phoneの設定の構成



次の設定を構成します。

- **Require device encryption**：ユーザーのデバイスを暗号化するかどうかを選択します。デフォルトは**[OFF]**です。
- **Disable storage card**：ユーザーがデバイスでストレージカードを使用できないようにするかどうかを選択します。デフォルトは**[OFF]**です。

Android Sonyの設定の構成

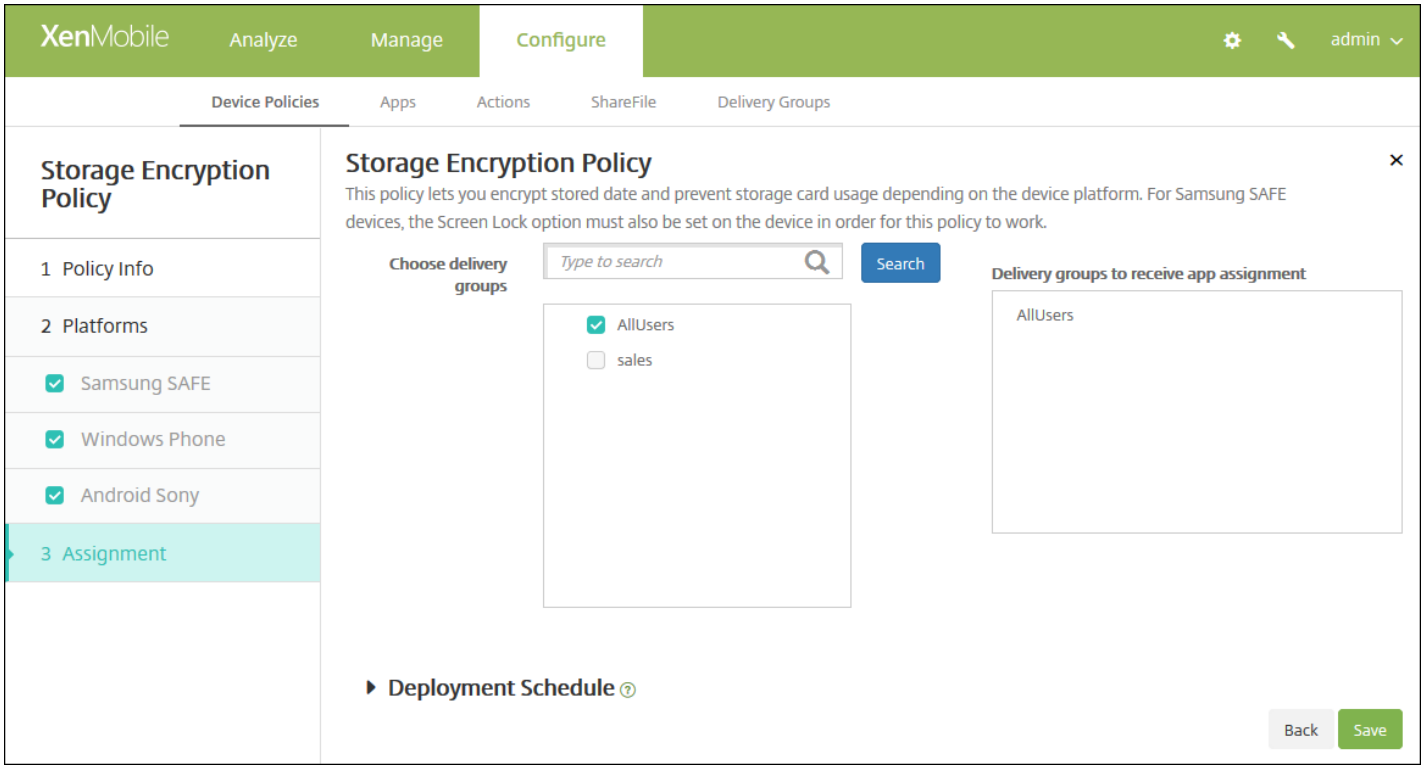


次の設定を構成します。

- **Encrypt external storage**：ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。デフォルトは**[ON]**です。

7. 展開規則を構成します。

8. **[次へ]** をクリックします。 **[ストレージ暗号化ポリシー]** 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. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

ストアデバイスポリシー

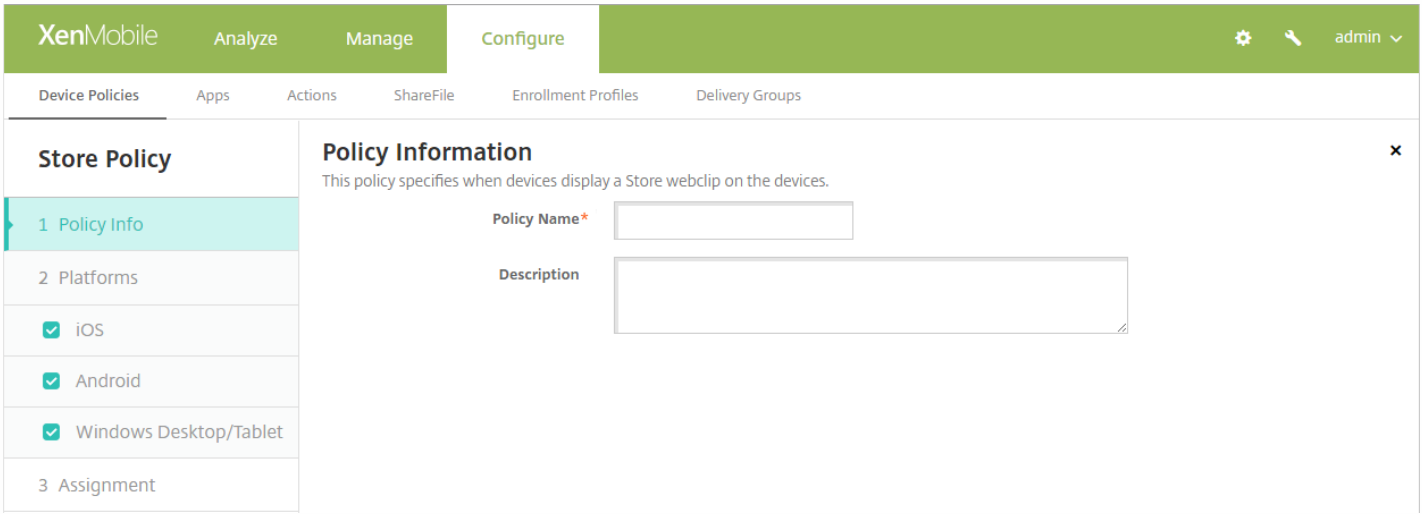
Feb 27, 2017

XenMobileでポリシーを作成して、iOS、Android、またはWindowsタブレットデバイスのホーム画面でXenMobile Storeの Webクリップを表示するかどうかを指定できます。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

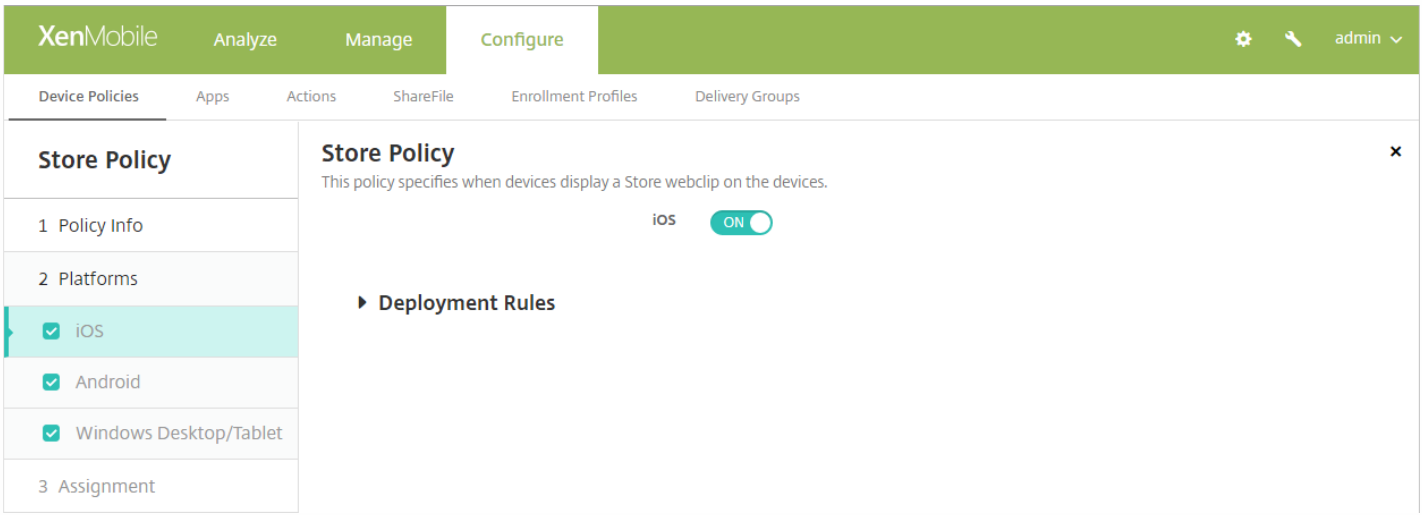
3. **[More]** を展開した後、**[Apps]** の下の **[Store]** をクリックします。**[Store Policy]** ページが開きます。



4. **[ポリシー情報]** 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. **[次へ]** をクリックします。**[プラットフォーム]** ページが開きます。



6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

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XenMobile Store Webクリップを表示するかどうかを選択します。デフォルトは **[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. 展開規則を構成します。

9. **[Next]** をクリックします。 **[XenMobile Store Policy]** 割り当てページが表示されます。

10. **[デリバリーグループを選択]** 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 **[アプリ割り当てを受信するためのデリバリーグループ]** の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。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

12. **[Save]** をクリックします。

サブスクライブされたカレンダーデバイスポリシー

Feb 27, 2017

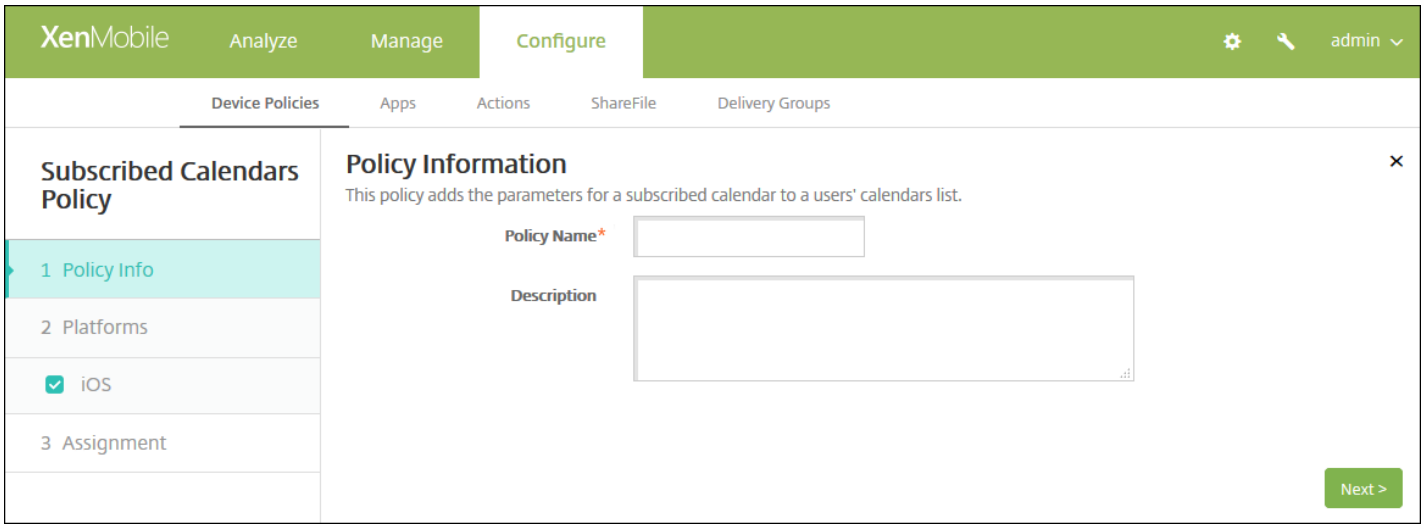
XenMobileでデバイスポリシーを追加して、サブスクライブされたカレンダーをユーザーのiOSデバイスのカレンダー一覧に追加することができます。サブスクライブできる公開カレンダーの一覧は、www.apple.com/downloads/macosx/calendarsにあります。

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。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

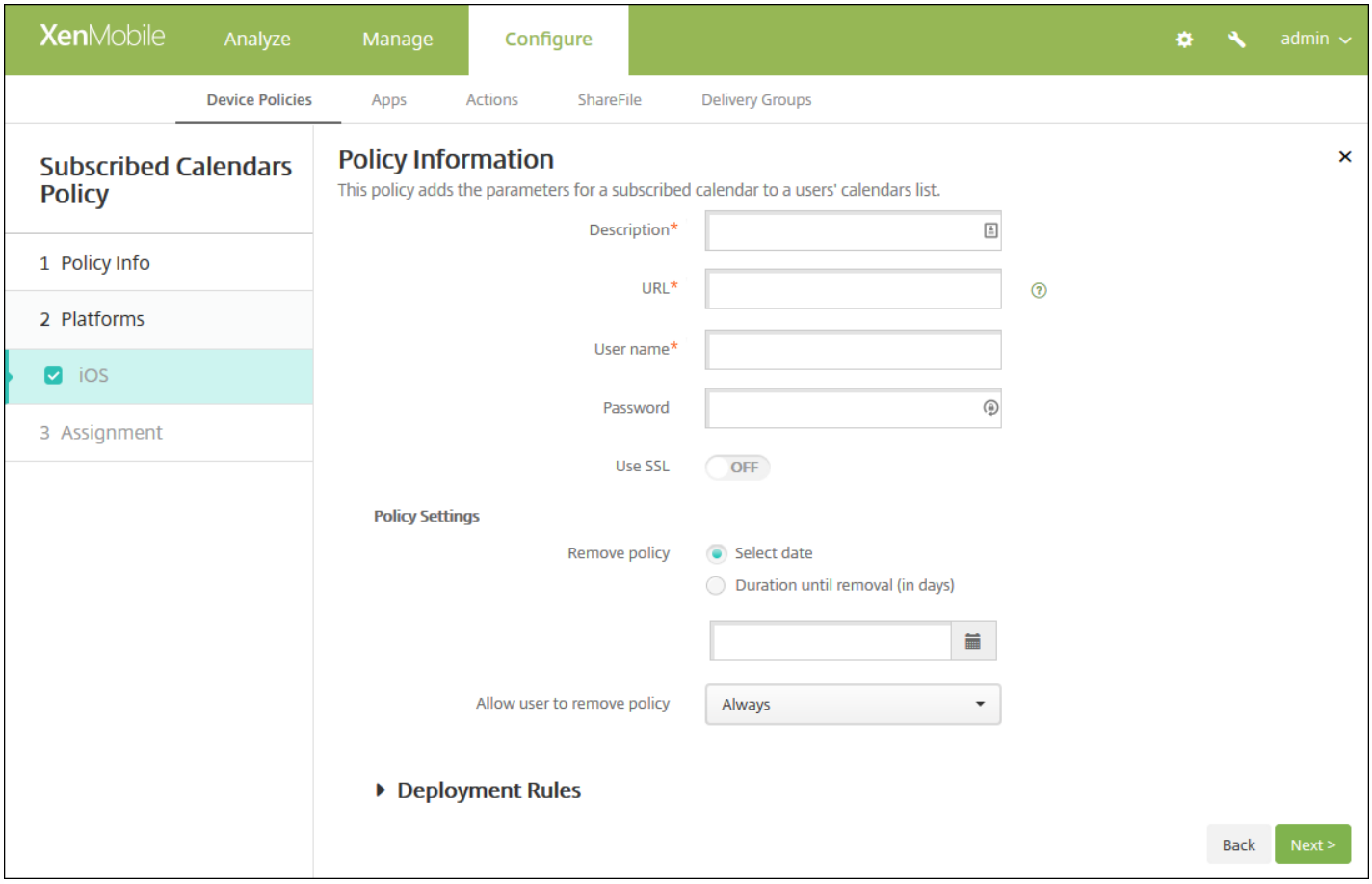
3. **[More]** をクリックした後、**[End user]** の下の **[Subscribed Calendars]** をクリックします。**[Subscribed Calendars Policy]** ページが開きます。



4. **[ポリシー情報]** 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。

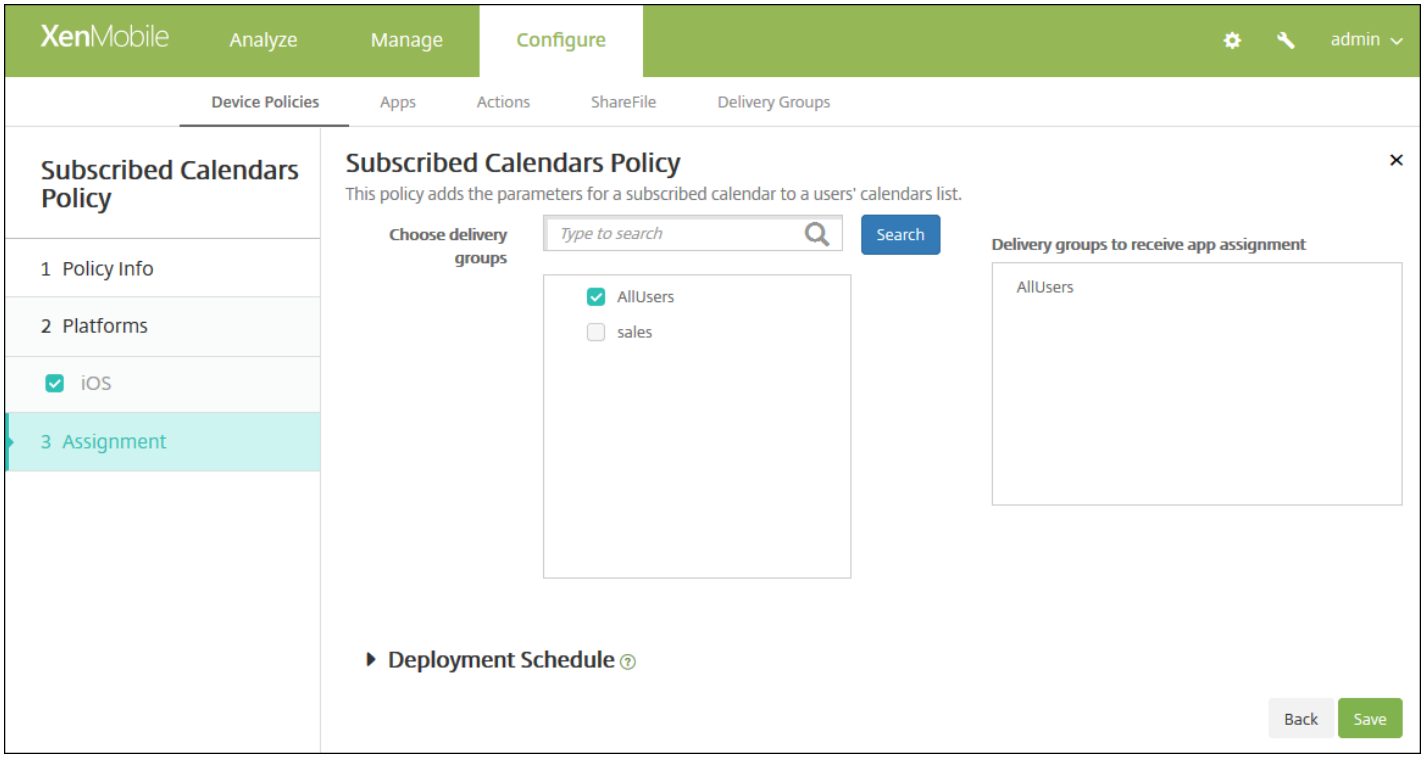


6. 次の設定を構成します。

- **Description**： カレンダーの説明を入力します。このフィールドは必須です。
- **URL**： カレンダーのURLを入力します。iCalendarファイル（.ics）へのwebcal:// URLまたはhttp://リンクを入力してください。このフィールドは必須です。
- **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**： カレンダーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは、［Off］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。

7. 展開規則を構成します。

8. **［Next］**をクリックします。**［Subscribed Calendars 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. **[展開スケジュール]** 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 **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

VPNデバイスポリシー

May 07, 2017

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

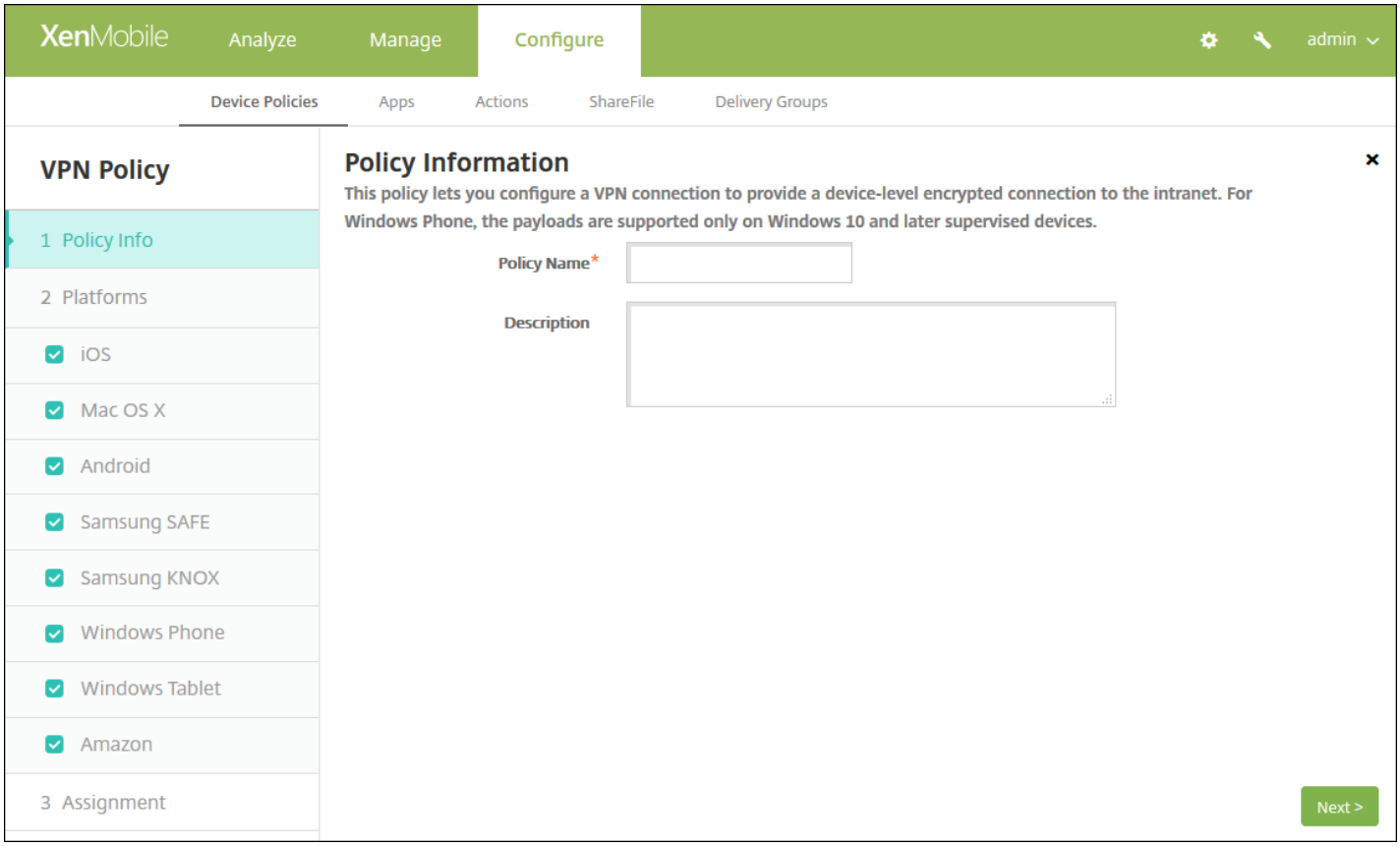
Windowsタブレットの設定

Amazonの設定

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[VPN]** をクリックします。**[VPNポリシー]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

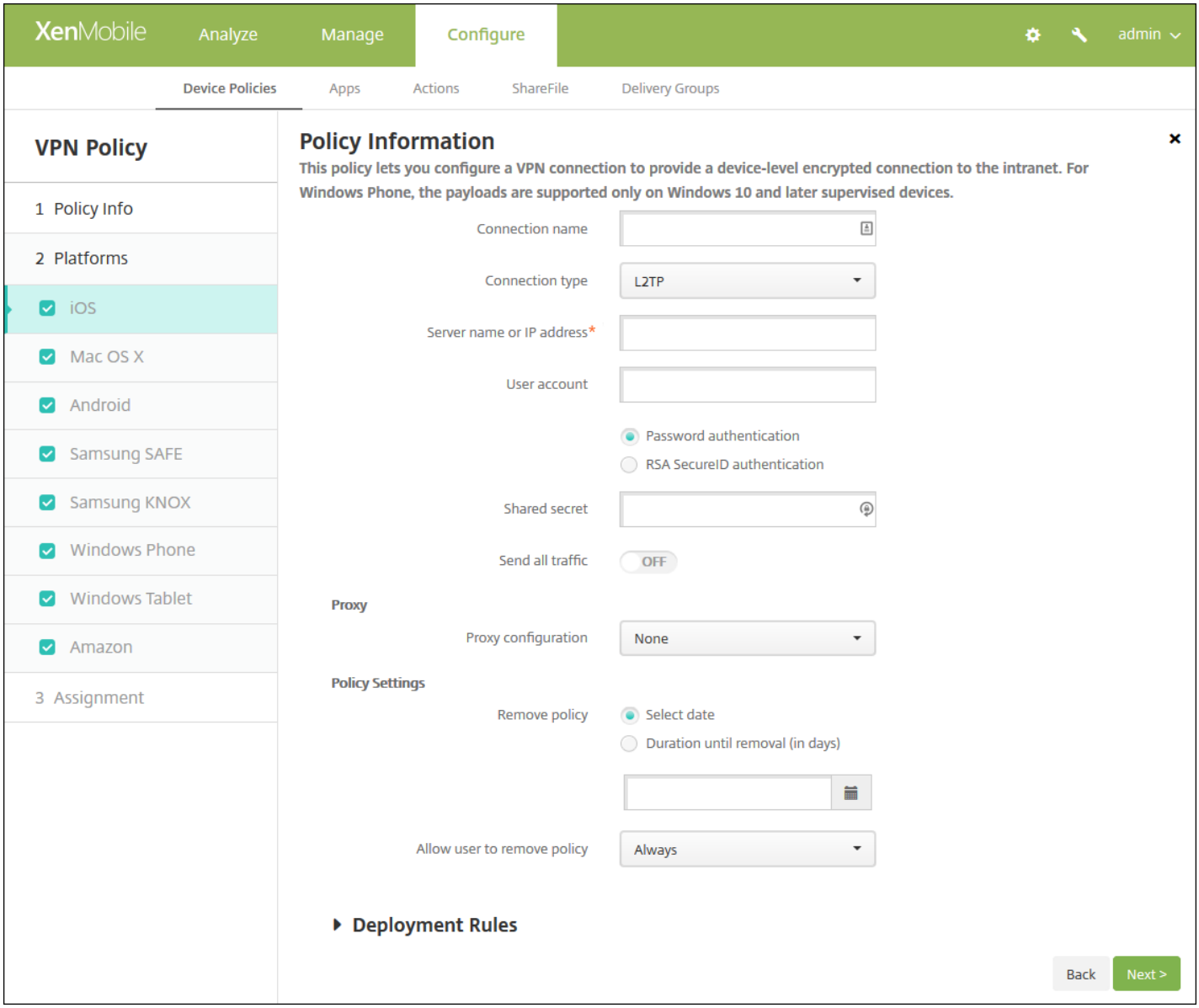
- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[ポリシープラットフォーム]** ページが開きます。 **[ポリシープラットフォーム]** 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. **[プラットフォーム]** 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。

- **接続名**：接続名を入力します。
- **接続の種類**：一覧から、この接続において使用するプロトコルを選択します。デフォルトは**[L2TP]**です。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証。
  - **PPTP**：Point-to-Pointトンネリング。
  - **IPSec**：社内VPN接続
  - **Cisco AnyConnect**：Cisco AnyConnect VPNクライアント
  - **Juniper SSL**：Juniper Networks SSL VPNクライアント
  - **F5 SSL**：F5 Networks SSL VPNクライアント
  - **SonicWALL Mobile Connect**：iOS用Dell統合VPNクライアント
  - **Ariba VIA**：Aruba Networks仮想インターネットアクセスクライアント
  - **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
  - **カスタムSSL**：カスタムSSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

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

IKEv2プロトコルの構成

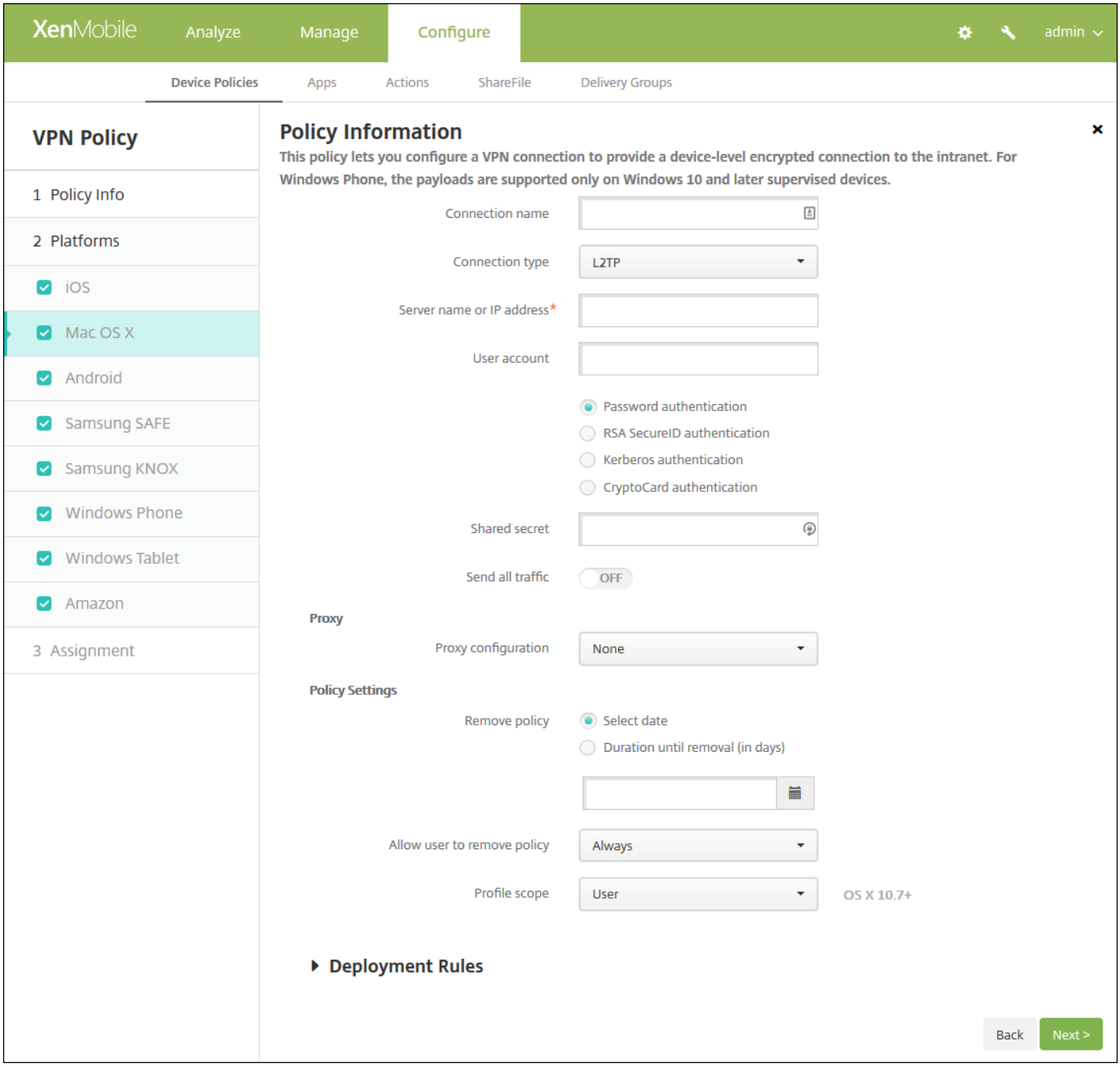
Citrix VPNプロトコルの構成

カスタムSSLプロトコルの構成

［オンデマンドにVPNを有効化］オプションの構成

- **プロキシDHCP**
  - **プロキシ構成**： 一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。デフォルトは**[なし]**です。
    - **[手動]**を有効にした場合は、次の設定を構成します。
      - **プロキシサーバーのホスト名またはIPアドレス**: プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
      - **プロキシサーバーのポート**： プロキシサーバーのポート番号を入力します。このフィールドは必須です。
      - **ユーザー名**： 任意で、プロキシサーバーのユーザー名を入力します。
      - **パスワード**： オプションのプロキシサーバーパスワードを入力します。
    - **[自動]**を選択した場合は、次の設定を構成します。
      - **プロキシサーバーURL**： プロキシサーバーのURLを入力します。このフィールドは必須です。
- **ポリシー設定**
  - **[ポリシー設定]**の下の**[ポリシーの削除]**の横にある、**[日付を選択]**または**[削除までの期間 (日) を指定]**をクリックします。
  - **[日付を選択]**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[ユーザーにポリシーの削除を許可]**の一覧で、**[常に]**、**[パスワードが必要]**、**[許可しない]**のいずれかを選択します。
  - **[パスワードが必要]**を選択した場合、**[パスワードを削除]**の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **接続名**： 接続名を入力します。
- **接続の種類**：一覧から、この接続において使用するプロトコルを選択します。デフォルトは［L2TP］です。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証。
  - **PPTP**：Point-to-Pointトンネリング。
  - **IPSec**：社内VPN接続
  - **Cisco 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Del統合VPNクライアント

- **Ariba VIA**：Aruba Networks仮想インターネットアクセスクライアント
- **Citrix VPN**：Citrix VPNクライアント
- **カスタムSSL**：カスタムSSL（Secure Socket Layer）

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

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

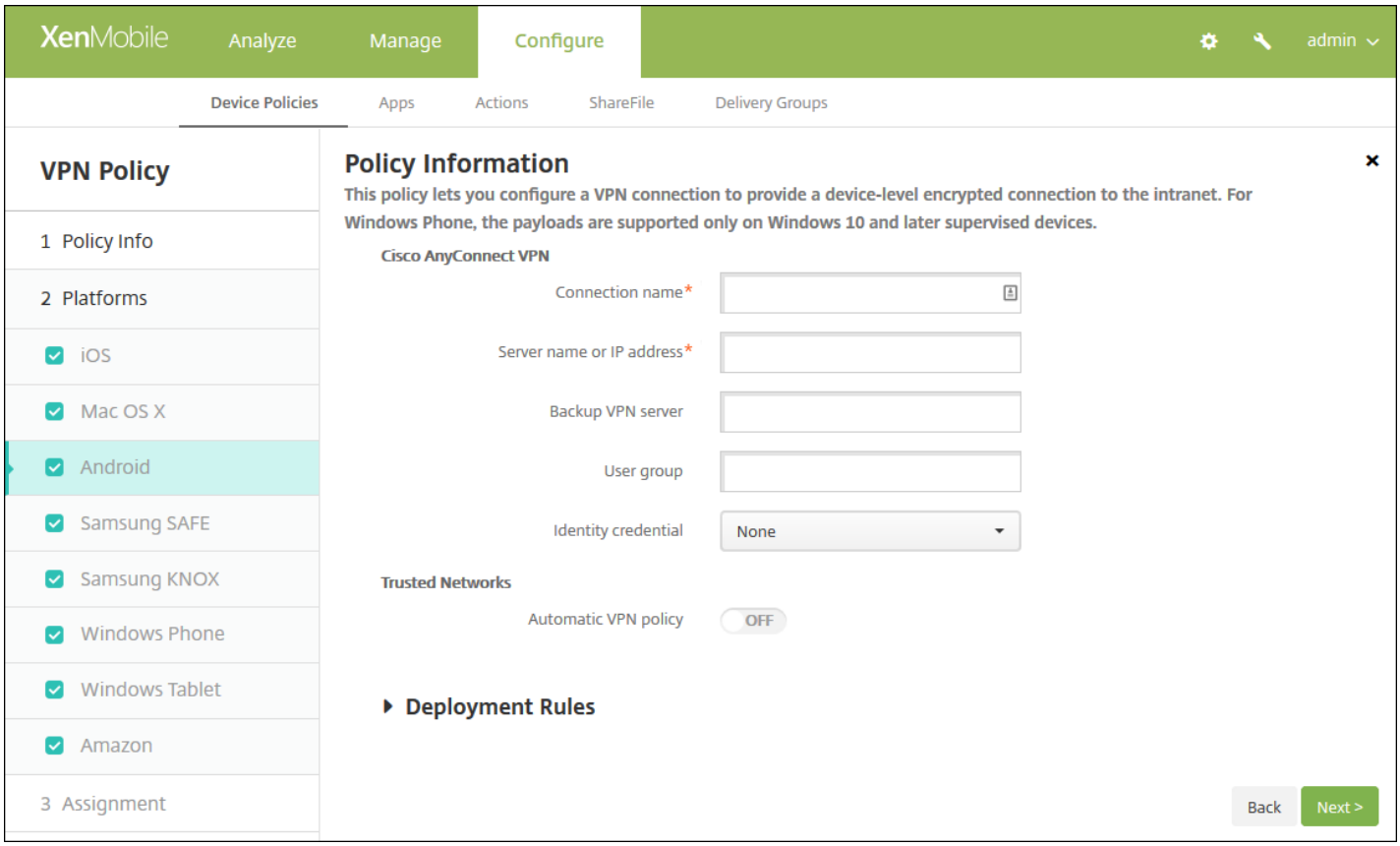
Citrix VPNプロトコルの構成

カスタムSSLプロトコルの構成

［オンデマンドにVPNを有効化］オプションの構成

- **プロキシDHCP**
  - **プロキシ構成**：一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。デフォルトは**［なし］**です。
    - **［手動］**を有効にした場合は、次の設定を構成します。
      - **プロキシサーバーのホスト名またはIPアドレス**：プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
      - **プロキシサーバーのポート**：プロキシサーバーのポート番号を入力します。このフィールドは必須です。
      - **ユーザー名**：任意で、プロキシサーバーのユーザー名を入力します。
      - **パスワード**：オプションのプロキシサーバーパスワードを入力します。
    - **［自動］**を選択した場合は、次の設定を構成します。
      - **プロキシサーバーURL**：プロキシサーバーのURLを入力します。このフィールドは必須です。
- **ポリシー設定**
  - **［ポリシー設定］**の下の**［ポリシーの削除］**の横にある、**［日付を選択］**または**［削除までの期間 (日) を指定］**をクリックします。
  - **［日付を選択］**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **［ユーザーにポリシーの削除を許可］**の一覧で、**［常に］**、**［パスワードが必要］**、**［許可しない］**のいずれかを選択します。
  - **［パスワードが必要］**を選択した場合、**［パスワードを削除］**の横に必要なパスワードを入力します。
  - **［プロファイルの対象］**の横にある、**［ユーザー］**または**［システム］**を選択します。デフォルトは**［ユーザー］**です。このオプションは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。

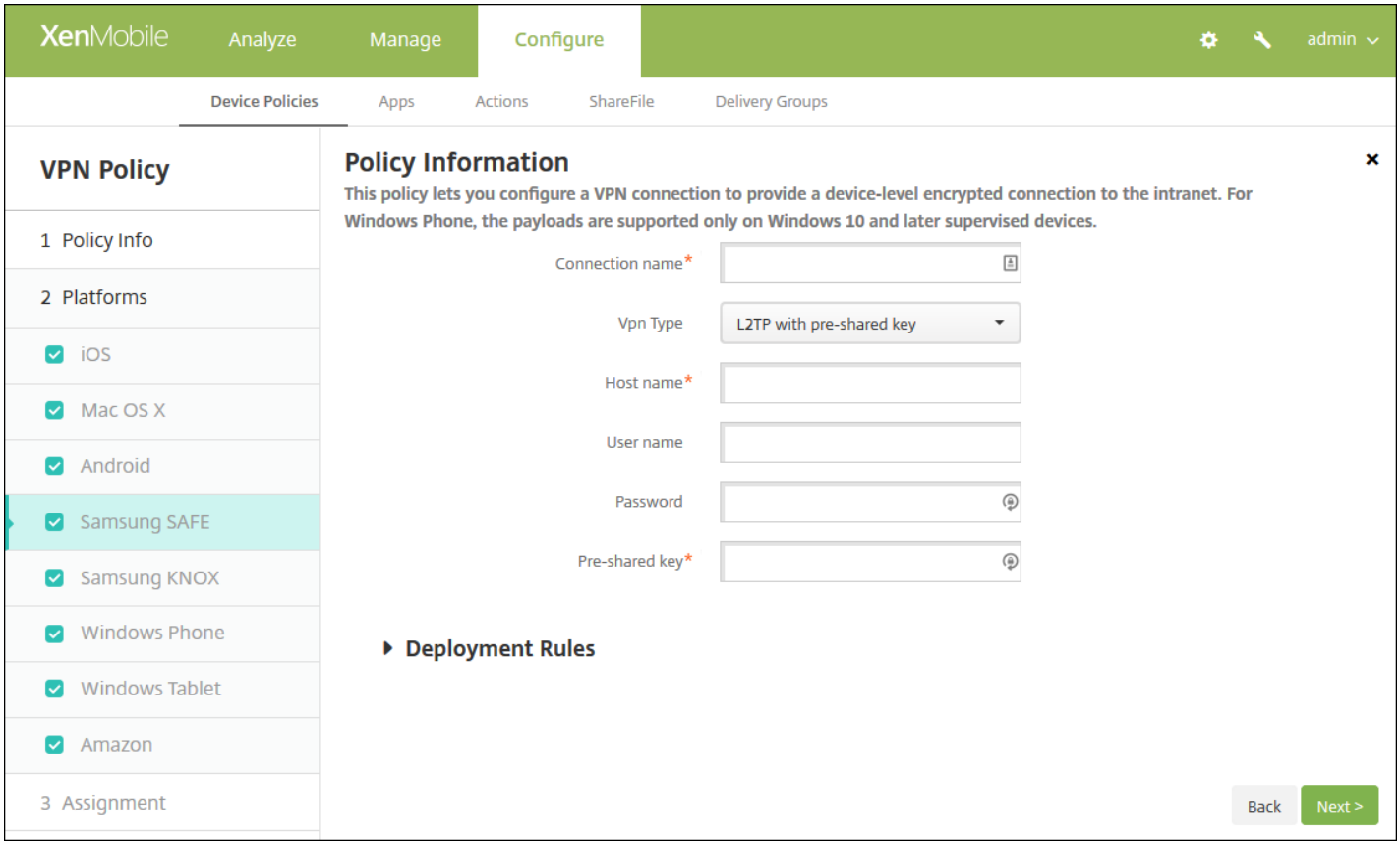
- **Cisco AnyConnect VPN**
  - **接続名**： Cisco AnyConnect VPN接続の名前を入力します。このフィールドは必須です。
  - **サーバー名またはIPアドレス**： VPNサーバーの名前またはIPアドレスを入力します。このフィールドは必須です。
  - **バックアップVPNサーバー**： バックアップVPNサーバー情報を入力します。
  - **ユーザーグループ**： ユーザーグループ情報を入力します。
  - **ID資格情報**： 一覧で、ID資格情報を選択します。
- **信頼されたネットワーク**
  - **自動VPNポリシー**： このオプションを有効または無効にして、VPNが信頼されたネットワークまたは信頼されていないネットワークにどのように反応するかを設定できます。有効にした場合は、次の設定を構成します。
    - **信頼されたネットワークポリシー**: 一覧から、目的のポリシーを選択します。デフォルトは **[切断]** です。選択できるオプションは以下のとおりです。
      - **切断**： クライアントにより、信頼できるネットワーク圏内のVPN接続が終了されます。これがデフォルトの設定です。
      - **接続**： クライアントにより、信頼できるネットワーク圏内のVPN接続が開始されます。
      - **何もしない**： クライアントによるアクションはありません。
      - **一時停止**： 信頼できるネットワーク圏外でVPNセッションが確立された後、信頼済みとして構成されたネットワークにユーザーがアクセスすると、VPNセッションが（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。
    - **信頼されていないネットワークポリシー**: 一覧から、目的のポリシーを選択します。デフォルトは **[接続]** です。選

択できるオプションは以下のとおりです。
  - **接続**： クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。
  - **何もしない**： クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。このオプションにより、［常時VPNに接続］が無効化されます。
- **信頼されたドメイン**： クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるドメインサフィックスごとに、**［追加］**をクリックして以下の操作を行います。
  - **ドメイン**： 追加するドメインを入力します。
  - **［保存］**をクリックしてドメインを保存するか、**［キャンセル］**をクリックして操作を取り消します。
- **信頼されたサーバー**： クライアントが信頼できるネットワーク圏内にある場合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、**［追加］**をクリックして以下の操作を行います。
  - **サーバー**： 追加するサーバーを入力します。
  - **［保存］**をクリックしてサーバーを保存するか、**［キャンセル］**をクリックして操作を取り消します。

    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**［削除］**をクリックし、項目をそのままにするには**［キャンセル］**をクリックします。

    既存の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、**［保存］**をクリックして変更した項目を保存するか、**［キャンセル］**をクリックして項目を変更せずそのままにします。

Samsung SAFEの設定の構成



次の設定を構成します。

- **接続名**： 接続名を入力します。
- **Vpn 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、事前共有キーを使用するL2TPです。選択できるオプションは以下のとおりです。
  - **事前共有キーを使用するL2TP**： レイヤー2トンネリングプロトコルと事前共有キー認証。これがデフォルトの設定です。
  - **証明書を使用するL2TP**：レイヤー2トンネリングプロトコルと証明書。
  - **PPTP**：Point-to-Pointトンネリング。
  - **エンタープライズ**： 社内VPN接続。Version 2.0よりも前のSAFEバージョンに適用されます。
  - **一般**： 一般的なVPN接続。Version 2.0以降のSAFEバージョンに適用されます。

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

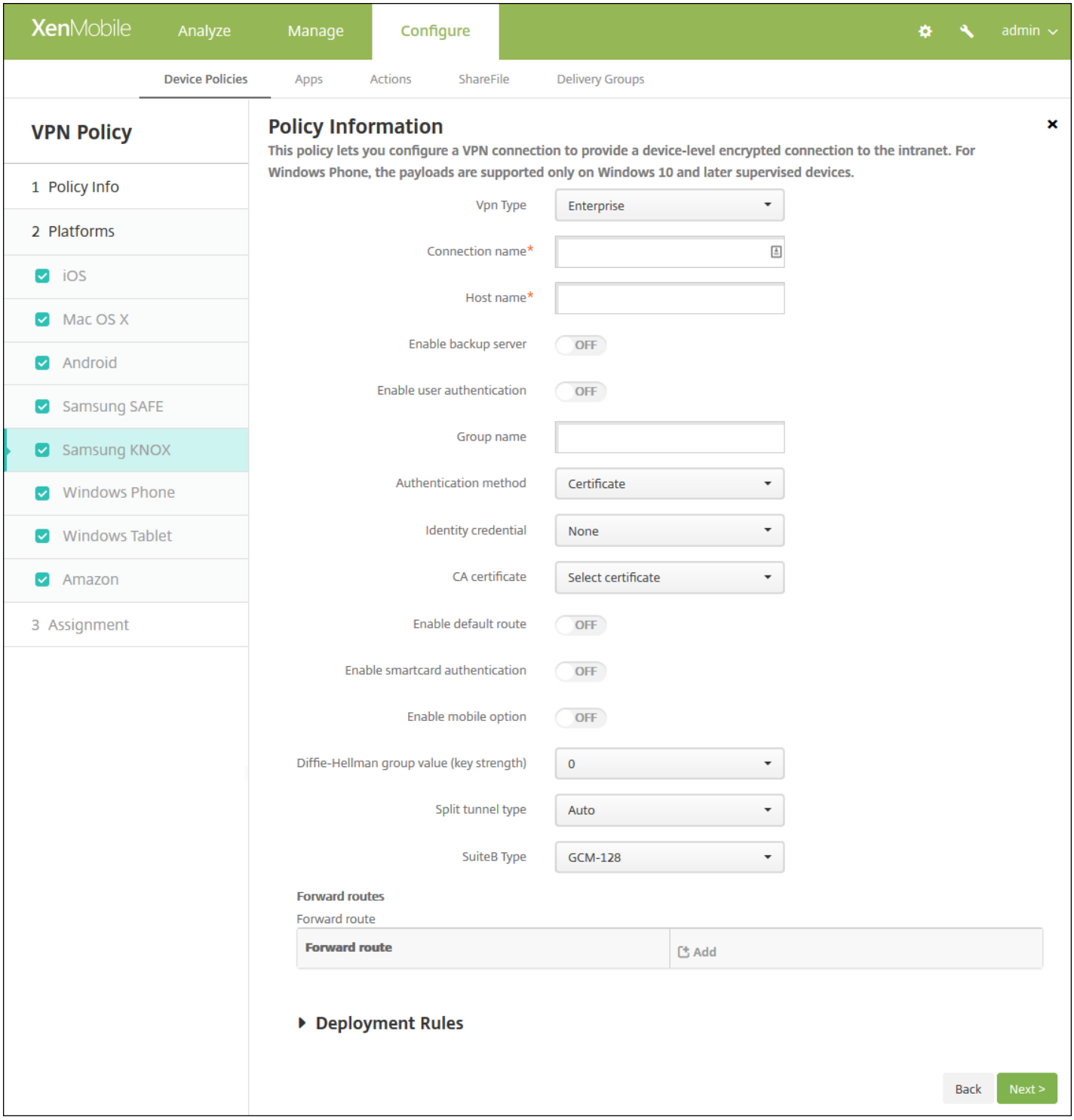
[証明書を使用するL2TP] プロトコルの構成

PPTPプロトコルの構成

エンタープライズプロトコルの構成

汎用プロトコルの構成

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。

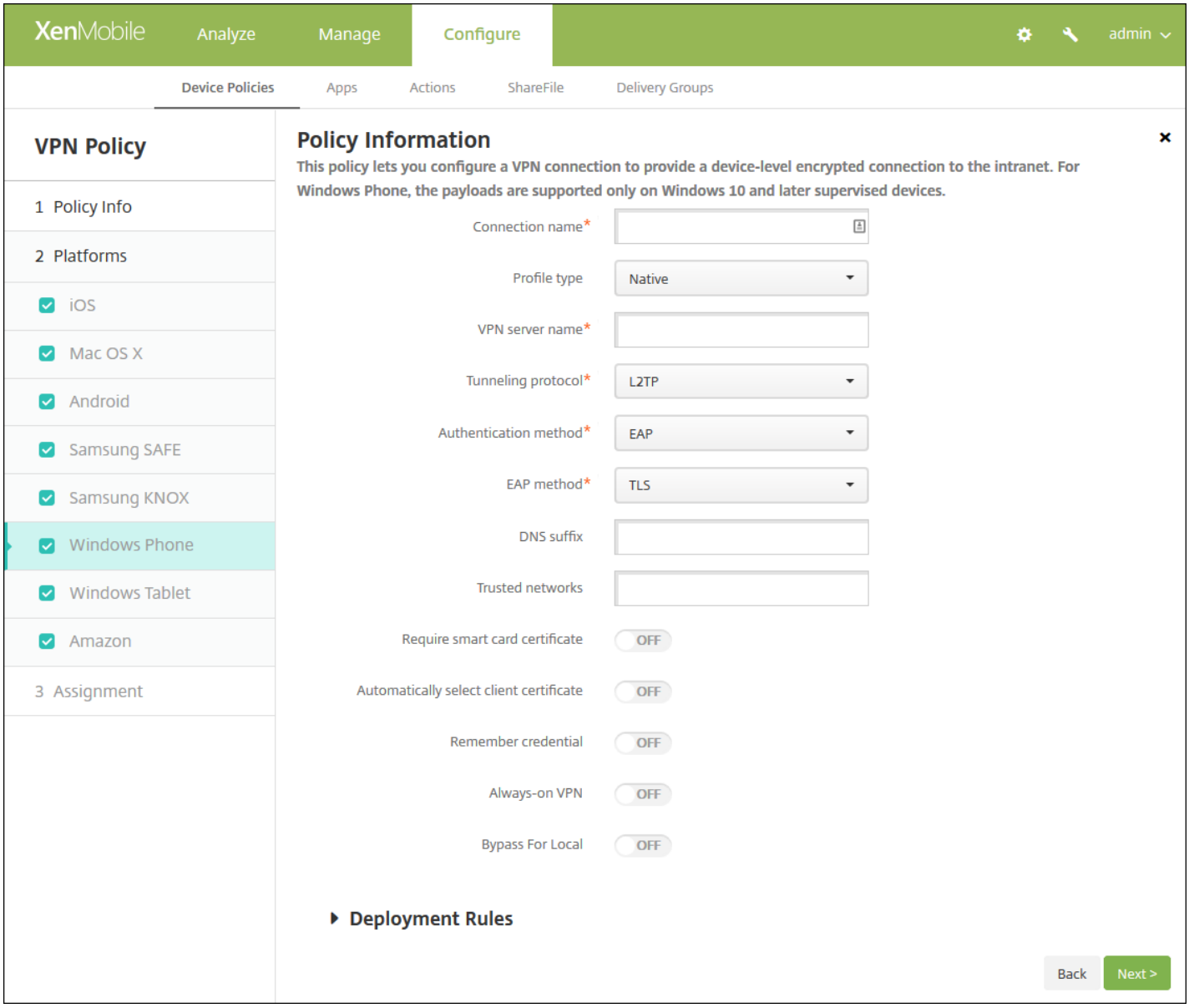
- **VPNの種類**： 一覧で、構成するVPN接続の種類として、**[エンタープライズ]**（Version 2.0より前のKNOXバージョンに適用）または**[汎用]**（Version 2.0以降のKNOXバージョンに適用）をクリックします。デフォルトは**[エンタープライズ]**です。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

エンタープライズプロトコルの構成

汎用プロトコルの構成

Windows Phoneの設定の構成



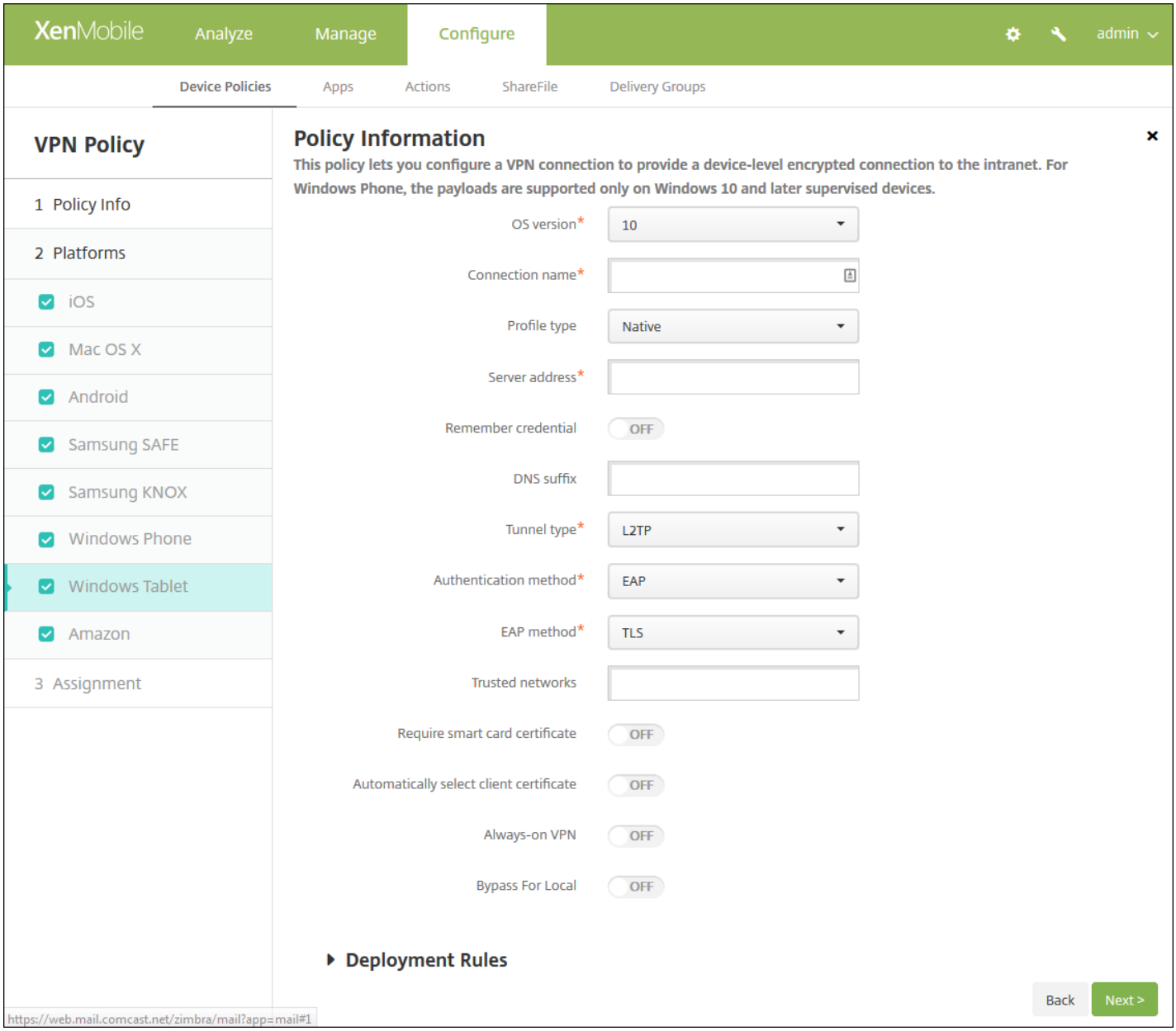
注：これらの設定は、Windows 10以降の監視対象Windows Phoneでのみサポートされます。

次の設定を構成します。

- **接続名**：接続の名前を入力します。このフィールドは必須です。
- **プロファイルの種類**：一覧から、［**ネイティブ**］または［**プラグイン**］を選択します。デフォルトは［**ネイティブ**］です。次のセクションでは、各オプションの設定について説明します。
- ［**ネイティブ**］**プロファイルの種類設定の構成**：以下の設定は、ユーザーのWindows Phoneに組み込まれているVPNに適用されます。
  - **VPNサーバー名**：VPNサーバーの完全修飾ドメイン名またはIPアドレスを入力します。このフィールドは必須です。
  - **トンネリングプロトコル**：一覧から、使用するVPNトンネルの種類を選択します。デフォルトは［**L2TP**］です。選択で

きるオプションは以下のとおりです。
  - **L2TP**：レイヤー2トンネリングプロトコルと事前共有キー認証。
  - **PPTP**：Point-to-Pointトンネリング。
  - **IKEv2**：インターネットキー交換バージョン2
- **認証方法**：一覧から、使用する認証方法を選択します。デフォルトは **[EAP]** です。選択できるオプションは以下のとおりです。
  - **EAP**：拡張認証プロトコル。
  - **MSChapV2**：相互認証にMicrosoftのチャレンジハンドシェイク認証を使用します。トンネルの種類に［IKEv2］を選択した場合、このオプションは使用できません。［MSChapV2］を選択すると、 **[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メソッド**：一覧から、使用するEAP方法を選択します。デフォルトは **[TLS]** です。［MSChapV2］認証が有効になっている場合、このフィールドは使用できません。選択できるオプションは以下のとおりです。
  - **TLS**：Transport Layer Security
  - **PEAP**：保護された拡張認証プロトコル
- **DNS Suffix**：DNSサフィックスを入力します。
- **信頼できるネットワーク**：アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- **スマートカード証明書を要求**：スマートカード証明書を必須とするかどうかを選択します。デフォルトは［オフ］です。
- **クライアント証明書を自動的に選択**：認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。デフォルトは［オフ］です。［スマートカード証明書を要求］が有効になっている場合、このオプションは使用できません。
- **資格情報を保存**：資格情報をキャッシュするかどうかを選択します。デフォルトは［オフ］です。有効にすると、可能な場合に資格情報がキャッシュされます。
- **常時VPNに接続**： VPNを常にオンにするかどうかを選択します。デフォルトは［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
- **ローカル用バイパス**：ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。
- **プラグインプロトコルの種類を構成**: 以下の設定は、Windows Storeから取得し、ユーザーのデバイスにインストールしたVPNプラグインに適用されます。
  - **サーバーアドレス**： VPNサーバーのURL、ホスト名またはIPアドレスを入力します。
  - **クライアントアプリID**: VPNプラグインのパッケージファミリ名を入力します。
  - **プラグインプロファイルXML**: 使用するカスタムVPNプラグインプロファイルの場所に［ブラウザー］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サフィックス**：DNSサフィックスを入力します。
  - **信頼できるネットワーク**：アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - **資格情報を保存**：資格情報をキャッシュするかどうかを選択します。デフォルトは［オフ］です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **常時VPNに接続**： VPNを常にオンにするかどうかを選択します。デフォルトは［オフ］です。有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
  - **ローカル用バイパス**：ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

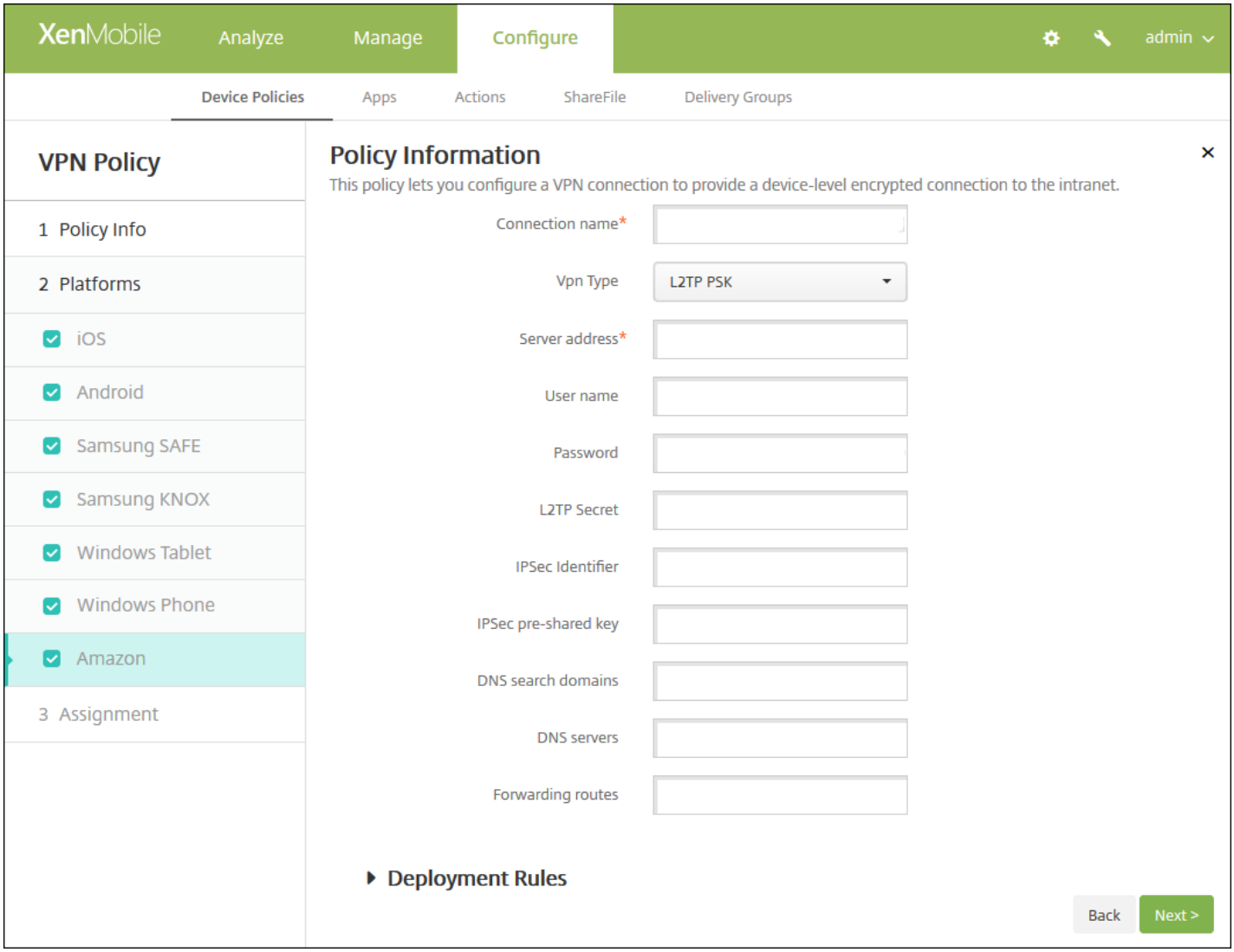
Windowsタブレットの設定の構成



次の設定を構成します。

Windows 10の設定の構成

Amazonの設定の構成



次の設定を構成します。

- **接続名**：接続の名前を入力します。
- **VPNの種類**： 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ハイブリッドRSA**： インターネットプロトコルセキュリティとハイブリッドRSA認証。
  - **PPTP**：Point-to-Pointトンネリング。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

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

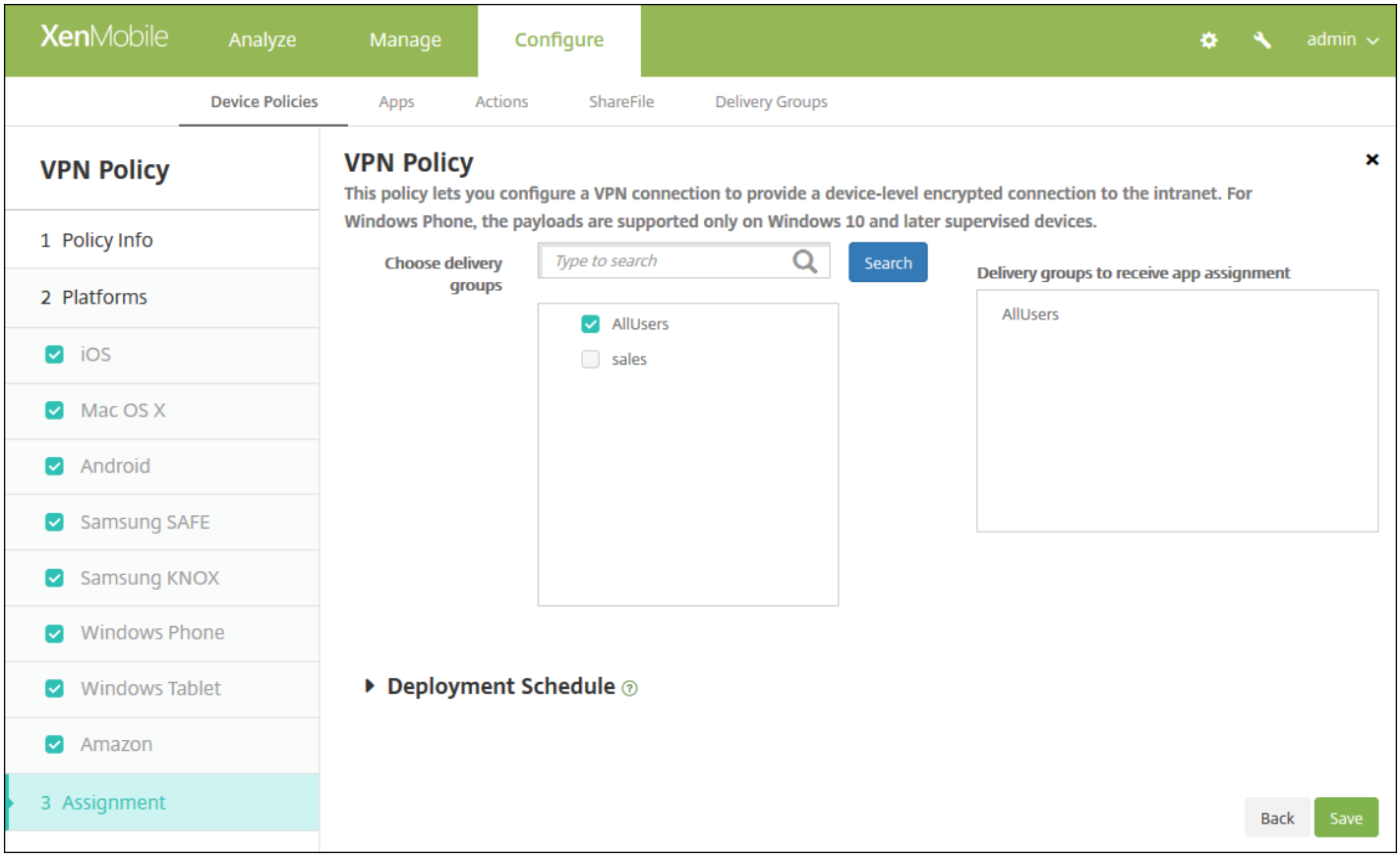
IPSEC AUTH RSAの設定の構成

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. **[次へ]** をクリックします。 **[VPNポリシー]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** の一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

壁紙デバイスポリシー

Feb 27, 2017

.pngファイルまたは.jpgファイル追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。iOS 7.1.2以降で使用できます。iPadおよびiPhoneで異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。

次の表に、Apple社がiOSデバイス用に推奨しているイメージサイズを示します。

デバイス		イメージサイズ（ピクセル）
iPhone - なし。	**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、 **[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

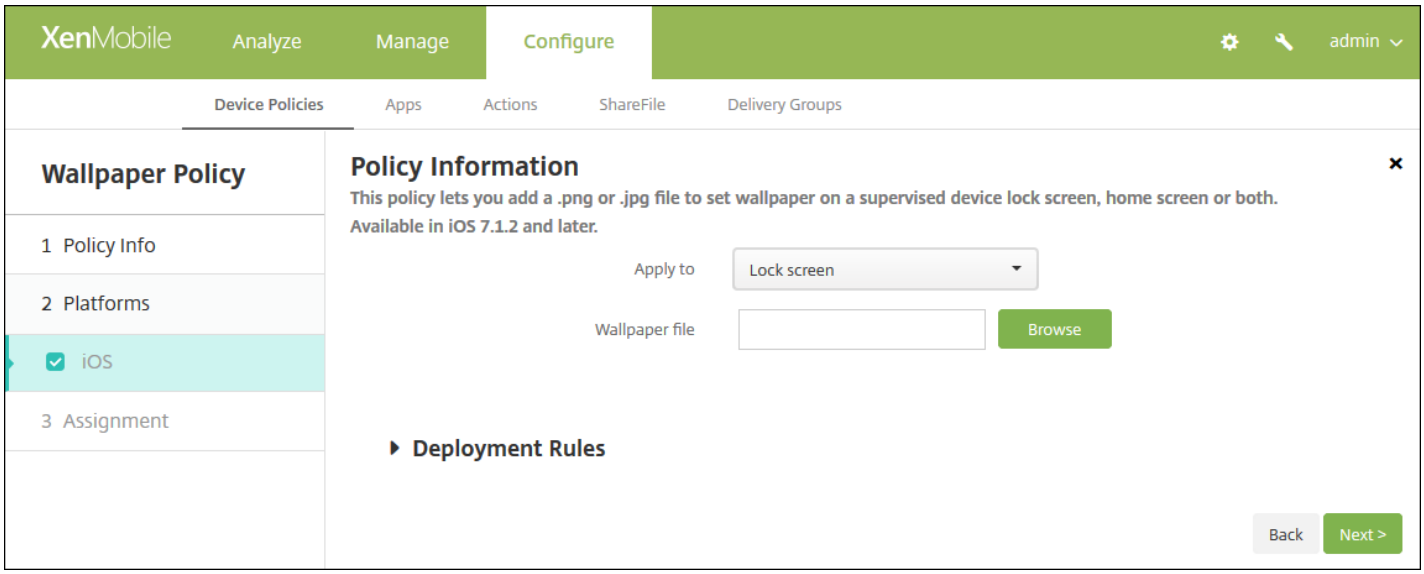
2. **[追加]** をクリックします。 **[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[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. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[Policy Platforms]** ページが開きます。

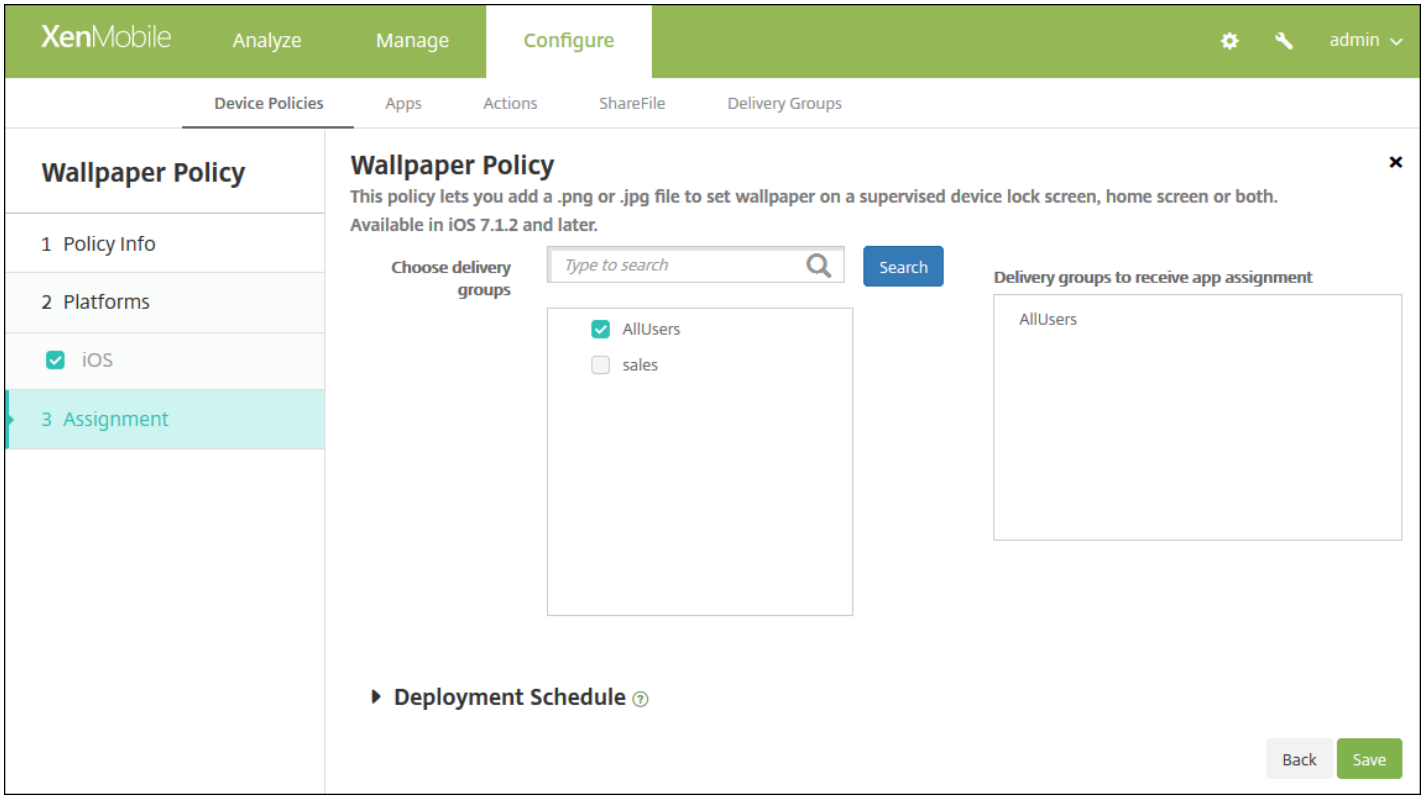


次の設定を構成します。

- **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. 展開規則を構成します。

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. **[デリバリーグループを選択]** 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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[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、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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. **[保存]** をクリックします。

Webコンテンツフィルターデバイスポリシー

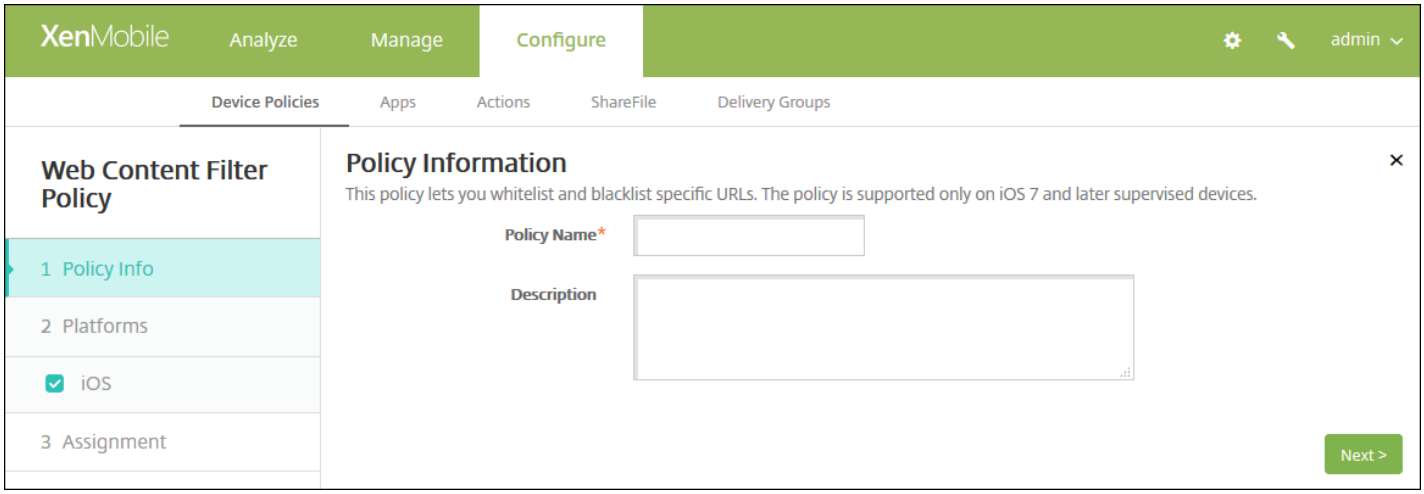
Feb 27, 2017

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デバイスを監視モードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスを監視モードにするには」を参照してください。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。

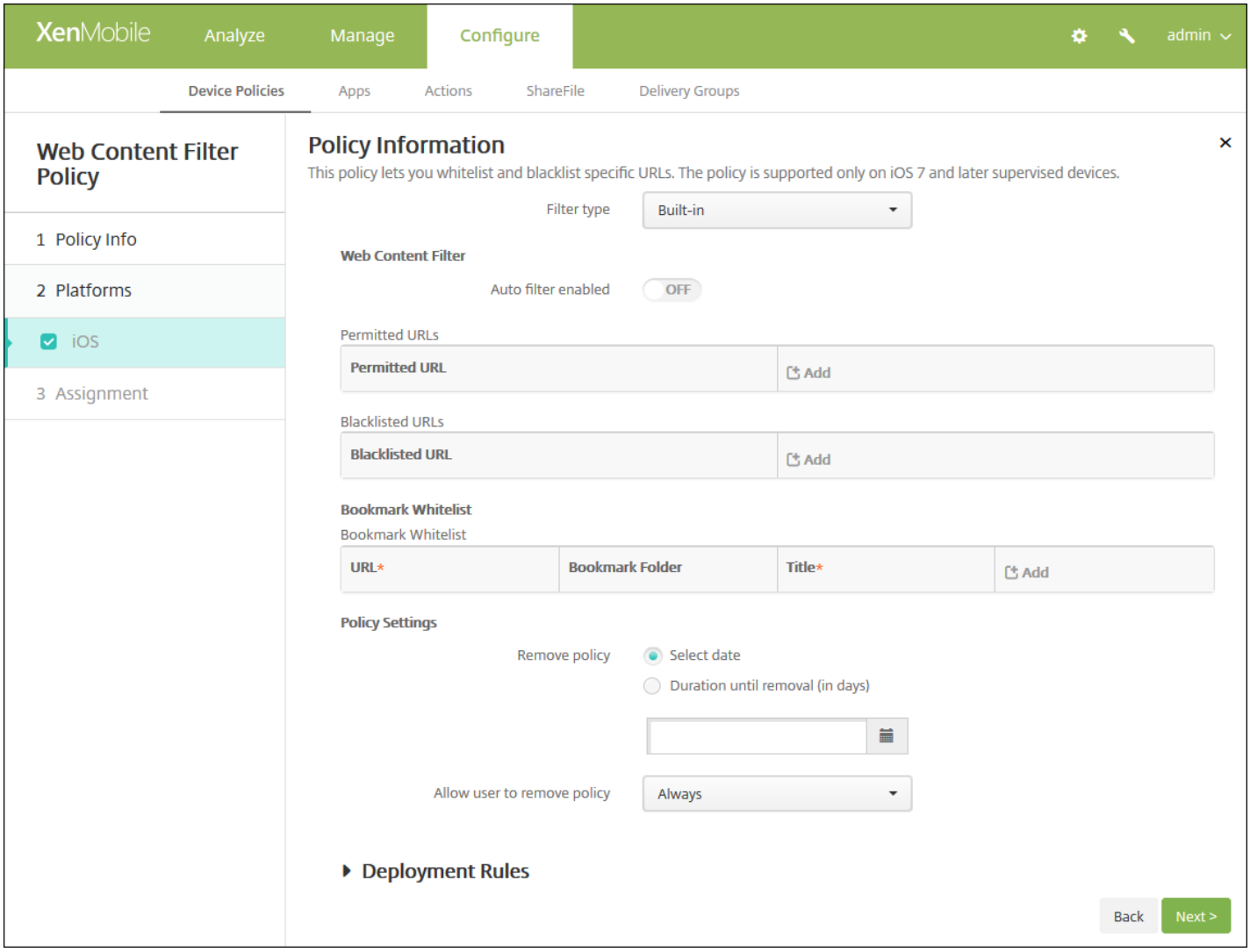
3. **[More]** をクリックした後、**[Security]** の下の **[Web Content Filter]** をクリックします。**[Web Content Filter Policy]** ページが開きます。



4. **[ポリシー情報]** 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。

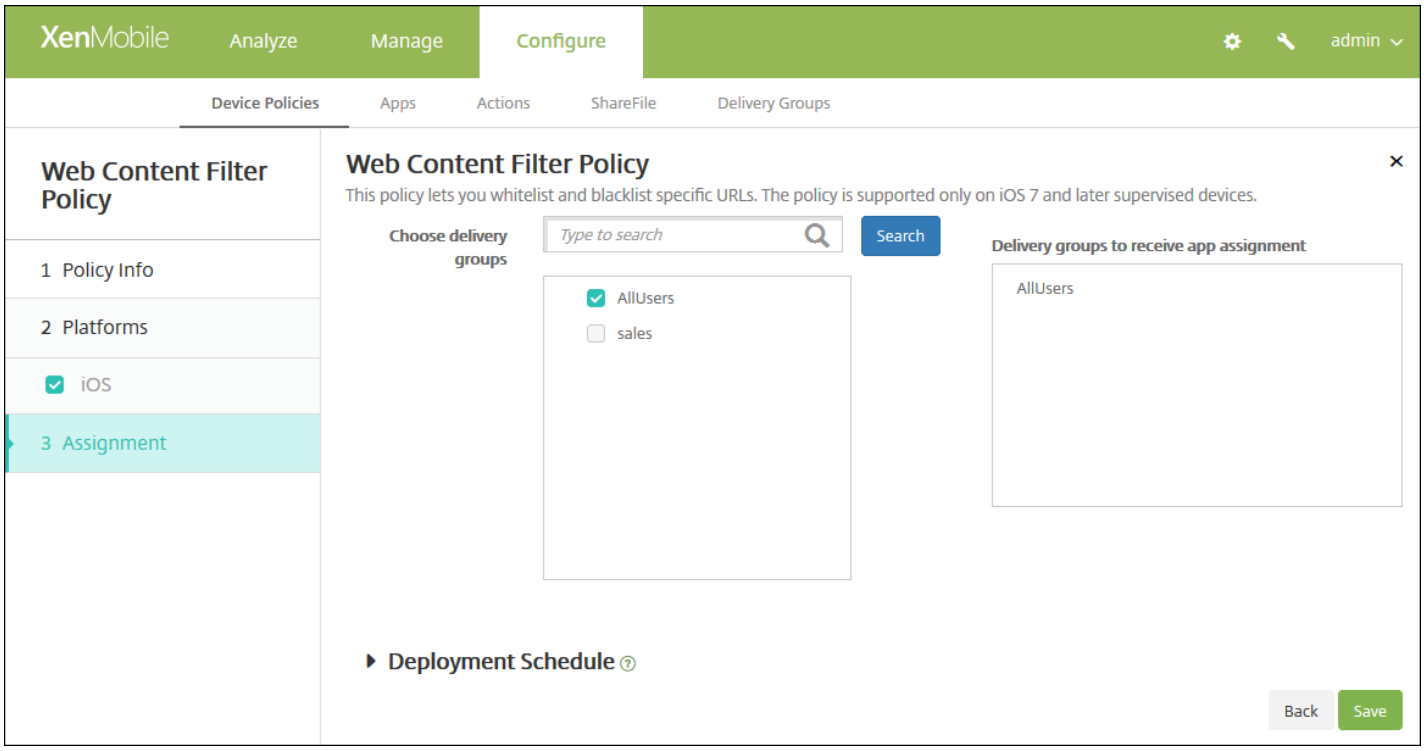
組み込みフィルターの種類の設定

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. 展開規則を構成します。

8. ［**次へ**］をクリックします。［**Webコンテンツフィルターポリシー**］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. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** を選択した場合、そのほかのオプション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 **[すぐに]** 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。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

e feel your pain.

' is not here. The link might be misspelled or outdated.

arch or navigate for the content
d retry the link

vestigate

Feedback link at the bottom of Docs.citrix.com to tell us about it

WiFiデバイスポリシー

Apr 24, 2017

[構成] > [デバイスポリシー] ページを使用して、XenMobileで新しいWi-Fiデバイスポリシーを作成するか、既存のWi-Fiデバイスポリシーを編集します。Wi-Fiポリシーでは、次の各項目を定義することでユーザーデバイスのWi-Fiネットワークへの接続方法を管理できます。

- 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
- その他のWi-F関連事項

以下のプラットフォームで、ユーザーに対するWi-Fiの設定を構成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

iOSの設定

Mac OS Xの設定

Androidの設定（Android for Work対応デバイスを含む）

Windows Phoneの設定

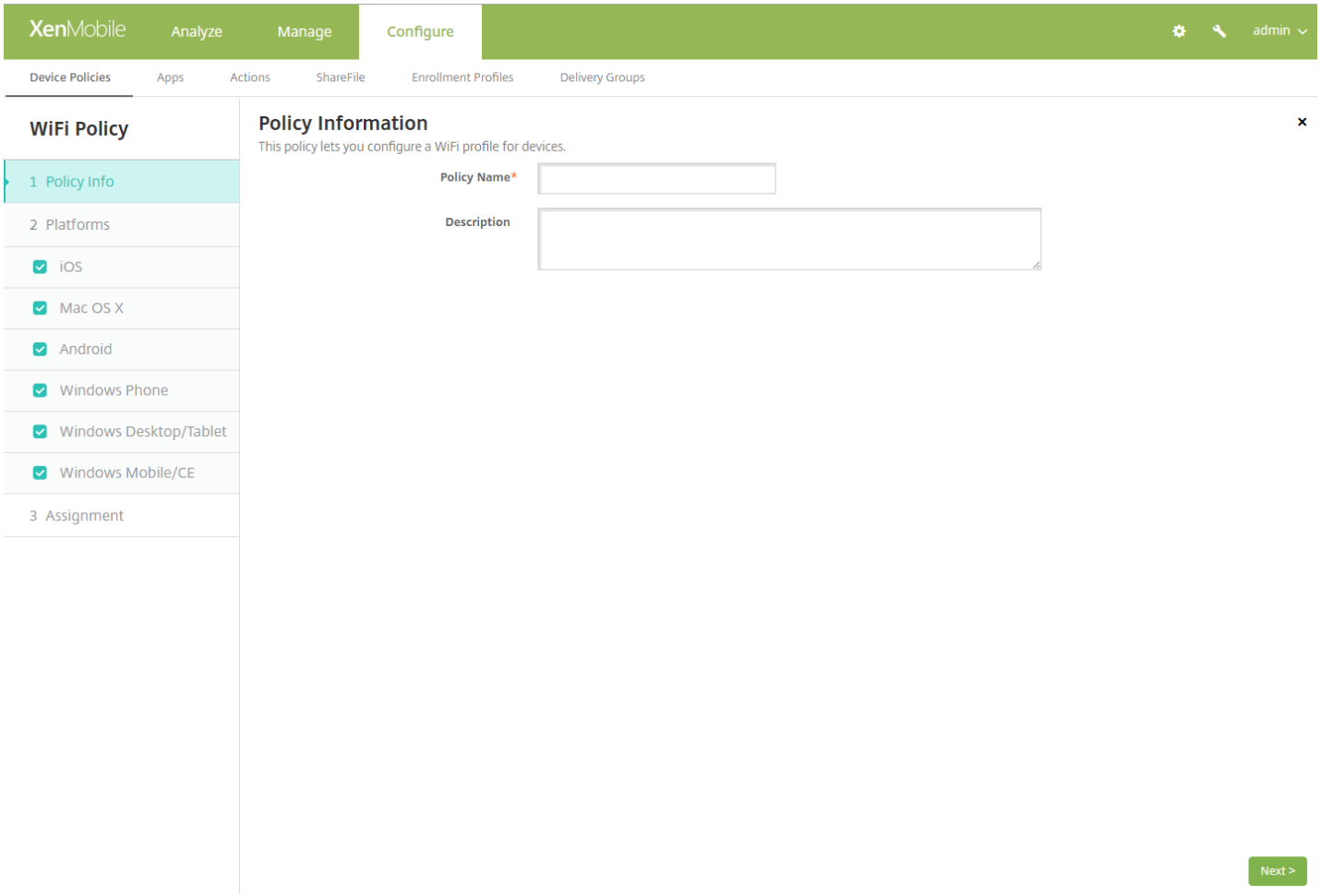
Windowsデスクトップ/タブレットの設定

> ## Important
>
> ポリシーを作成する前に、以下の手順を完了してください。
>
> - 使用する予定のデリバリーグループを作成します。
> - ネットワークの名前と種類を確認します。
> - 使用する予定の認証またはセキュリティの種類を確認します。
> - 必要な場合、プロキシサーバーの情報を確認します。
> - 必要なCA証明書をインストールします。
> - 必要な共有キーを取得します。
> - 証明書に基づいた認証のためにPKIエンティティを作成します。
> - 資格情報プロバイダーを構成します。
>
> 詳しくは、「認証」とそのサブ記事を参照してください。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

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



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

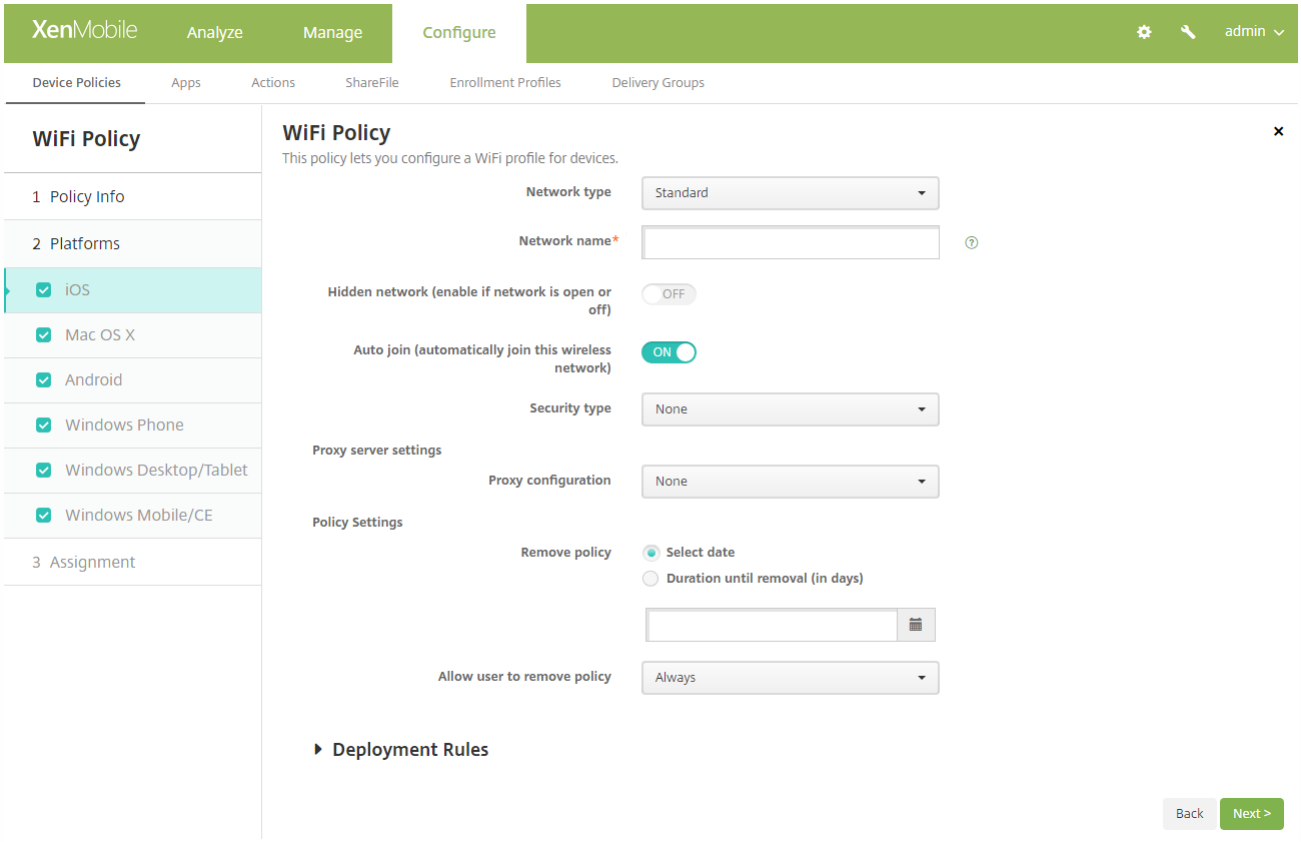
- **ポリシー名**： ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。 **[プラットフォーム]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7を参照してその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。

- **ネットワークの種類**： 一覧で、 **[標準]** 、 **[従来のホットスポット]** 、または **[Hotspot 2.0]** を選択して、使用するネットワークの種類を設定する必要があります
- **Network Name**：デバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **隠しネットワーク（ネットワークが開いているか、オフの場合は有効）**： ネットワークを非表示にするかどうかを選択します。
- **自動参加（このワイヤレスネットワークに自動的に参加）**： ネットワークに自動で参加するかどうかを選択します。デフォルトは**[オン]** です。
- **セキュリティの種類**： 一覧で、使用するセキュリティの種類を選択します。**Hotspot 2.0**には適用されません。
  - None - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2パーソナル
  - 任意 (パーソナル)
  - WEPエンタープライズ
  - WPA/WPA-2エンタープライズ： Windows 10の最新リリースでは、WPA-2エンタープライズを使用するにはSCEPを構成する必要があります。構成後、XenMobileから証明書をデバイスに送信してWi-Fiサーバーを認証することができます。SCEPを構成するには、 **[設定] > [資格情報プロバイダー]** の［ディストリビューション］ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。
  - 任意（エンタープライズ）

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

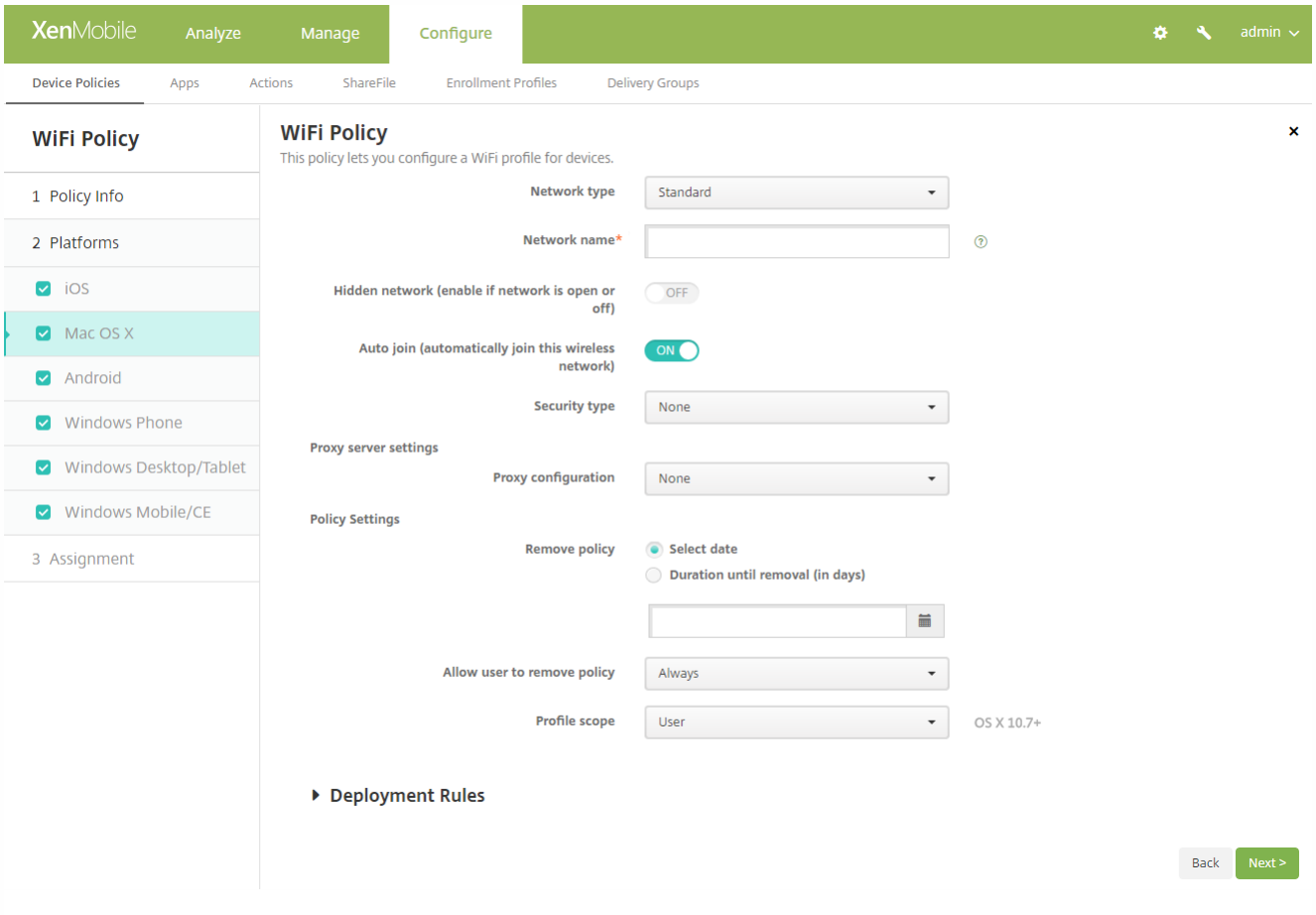
WPA、WPAパーソナル、任意（パーソナル）

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、Any (Enterprise)

- **プロキシサーバーの設定**
  - **プロキシ構成**： 一覧から、 **[なし]** 、 **[手動]** 、または **[自動]** を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は **[なし]** で、そのほかの構成は不要です。
  - **[手動]** を有効にした場合は、次の設定を構成します。
    - **ホスト名/IPアドレス**： プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **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。
    - **パスワード**： プロキシサーバーに認証するオプションのパスワードを入力します。
  - **[自動]** を有効にした場合は、次の設定を構成します。
    - **サーバーURL**： プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達不能である場合は直接接続を許可**： PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは**[オン]** です。このオプションはiOS 7.0以降でのみ使用できます。

- **ポリシー設定**
  - **[ポリシーの削除]** の横にある **[日付を選択]** または **[削除までの期間（日）を指定]** を選択します。
  - **[日付を選択]** を選択した場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[ユーザーにポリシーの削除を許可]** ボックスの一覧で、 **[常に]** 、 **[パスワードが必要です]** 、 **[許可しない]** のいずれかを選択します。
  - **[パスワードが必要です]** を選択した場合、 **[削除パスワード]** の横に必要なパスワードを入力します。

Mac OS Xの設定の構成



次の設定を構成します。

- **ネットワークの種類**： 一覧で、 **[標準]** 、 **[従来のホットスポット]** 、または **[Hotspot 2.0]** を選択して、使用するネットワークの種類を設定する必要があります
- **Network Name**：デバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。**Hotspot 2.0**には適用されません。
- **隠しネットワーク（ネットワークが開いているか、オフの場合は有効）**： ネットワークを非表示にするかどうかを選択します。
- **自動参加（このワイヤレスネットワークに自動的に参加）**： ネットワークに自動で参加するかどうかを選択します。デフォルトは**[オン]** です。
- **セキュリティの種類**： 一覧で、使用するセキュリティの種類を選択します。**Hotspot 2.0**には適用されません。
  - None - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2パーソナル
  - 任意 (パーソナル)
  - WEPエンタープライズ
  - WPA/WPA2エンタープライズ
  - 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。

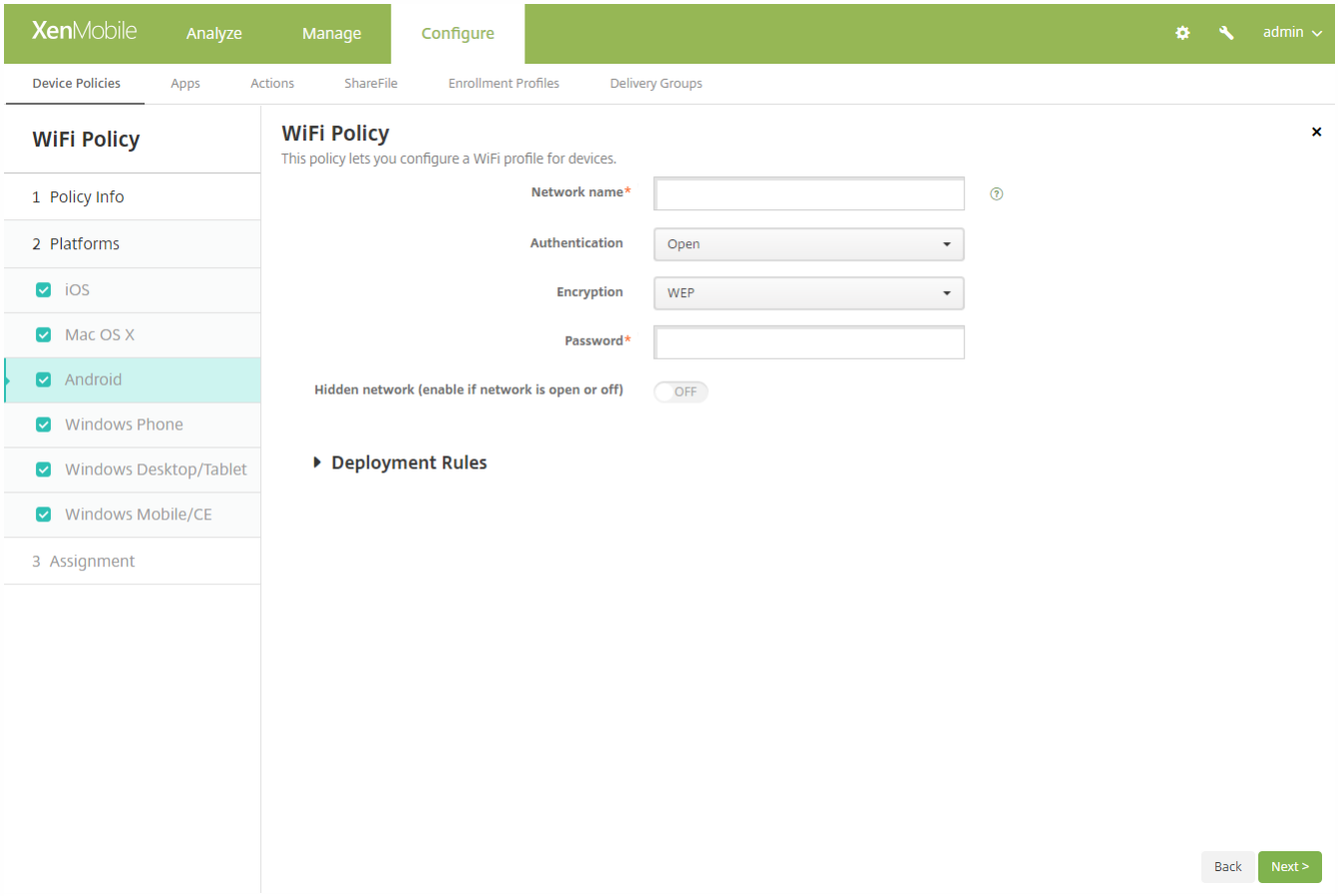
WPA、WPAパーソナル、WPA-2パーソナル、任意（パーソナル）

WEPエンタープライズ、WPAエンタープライズ、WPA2エンタープライズ、任意（エンタープライズ）

- **ログインウィンドウ構成として使用**: ユーザーの認証に、ログインウィンドウで入力したものと同じ資格情報を使用するかどうかを選択します。
- **プロキシサーバーの設定**
  - **プロキシ構成**： 一覧から、 **[なし]** 、 **[手動]** 、または **[自動]** を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は **[なし]** で、そのほかの構成は不要です。
  - **[手動]** を有効にした場合は、次の設定を構成します。
    - **ホスト名/IPアドレス**： プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **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。
    - **パスワード**： プロキシサーバーに認証するオプションのパスワードを入力します。
  - **[自動]** を有効にした場合は、次の設定を構成します。
    - **サーバーURL**： プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達不能である場合は直接接続を許可**： PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは**[オン]** です。このオプションはiOS 7.0以降でのみ使用できます。
- **ポリシー設定**
  - **[ポリシーの削除]** の横にある **[日付を選択]** または **[削除までの期間（日）を指定]** を選択します。

- **[日付を選択]** を選択した場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- **[ユーザーにポリシーの削除を許可]** ボックスの一覧で、 **[常に]** 、 **[パスワードが必要です]** 、 **[許可しない]** のいずれかを選択します。
- **[パスワードが必要です]** を選択した場合、 **[削除のパスワード]** の横に必要なパスワードを入力します。
- **[プロファイルの対象]** の横にある、 **[ユーザー]** または **[システム]** を選択します。デフォルトは **[ユーザー]** です。このオプションは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。

- **ネットワーク名**： 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。
- **認証**： 一覧で、Wi-Fi接続に使用するセキュリティの種類を選択します。
  - オープン
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

  以下では、上記の接続の種類ごとに、構成するオプションを示します。

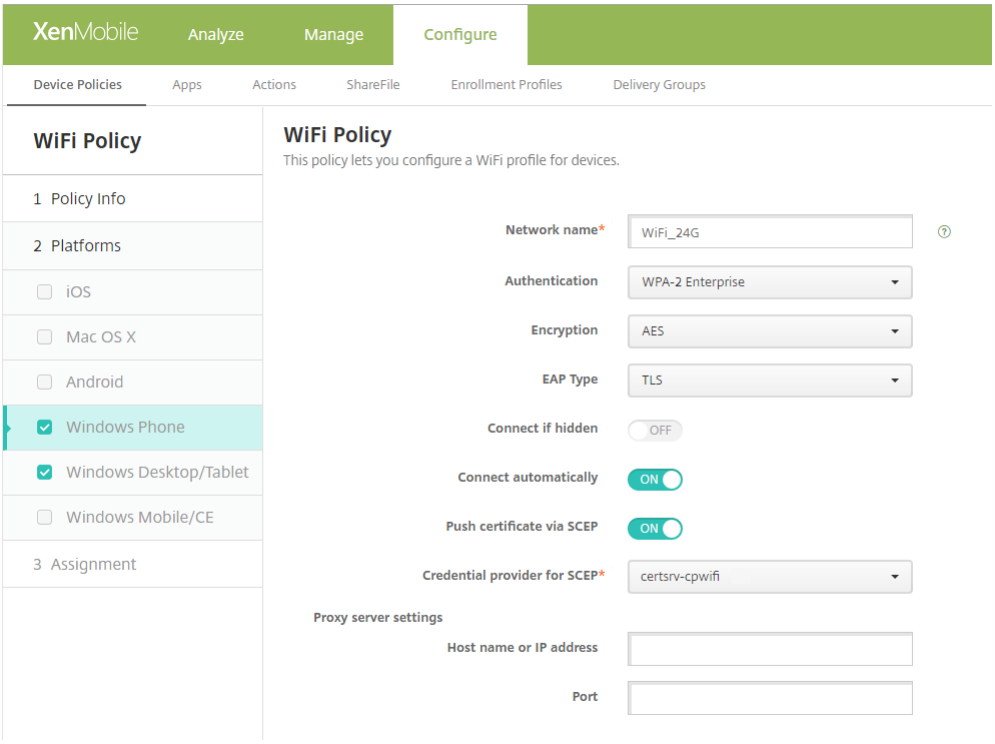
オープン、共有

WPA、WPA-PSK、WPA2、WPA2-PSK

802.1x

- **隠しネットワーク（ネットワークが開いているか、オフの場合は有効）**： ネットワークを非表示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。

- **ネットワーク名**：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。
- **認証**：一覧で、Wi-Fi接続に使用するセキュリティの種類を選択します。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPA-2エンタープライズ：Windows 10の最新リリースでは、WPA-2エンタープライズを使用するにはSCEPを構成する必要があります。SCEPを構成すると、XenMobileから証明書をデバイスに送信してWi-Fiサーバーを認証することができます。SCEPを構成するには、**[Settings] > [Credential Providers]** の **[Distribution]** ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

    以下では、上記の接続の種類ごとに、構成するオプションを示します。

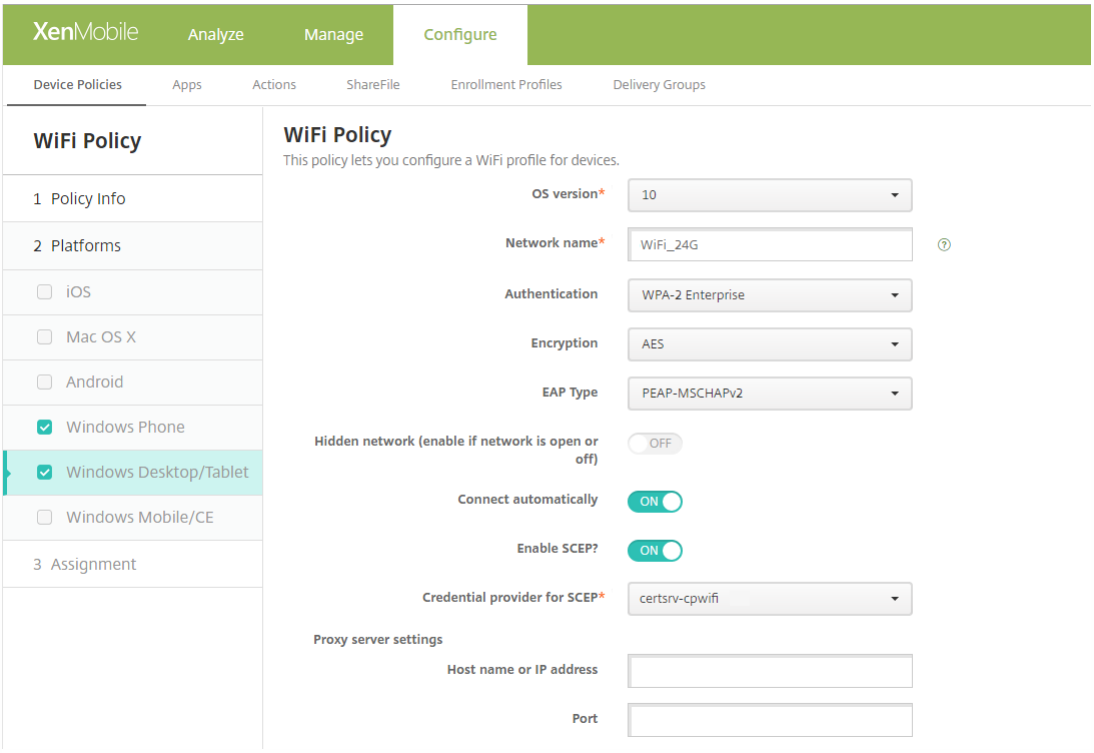
オープン

WPAパーソナル、WPA-2パーソナル

WPA-2エンタープライズ

- **プロキシサーバーの設定**
  - **ホスト名またはIPアドレス**：プロキシサーバーの名前またはIPアドレスを入力します。
  - **Port**：プロキシサーバーのポート番号を入力します。

Windowsデスクトップ/タブレットの設定の構成



次の設定を構成します。

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。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPAエンタープライズ
  - WPA-2エンタープライズ：Windows 10の最新リリースでは、WPA-2エンタープライズを使用するにはSCEPを構成する必要があります。SCEPを構成すると、XenMobileから証明書をデバイスに送信してWi-Fiサーバーを認証することができます。SCEPを構成するには、 **[Settings] > [Credential Providers]** の **[Distribution]** ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

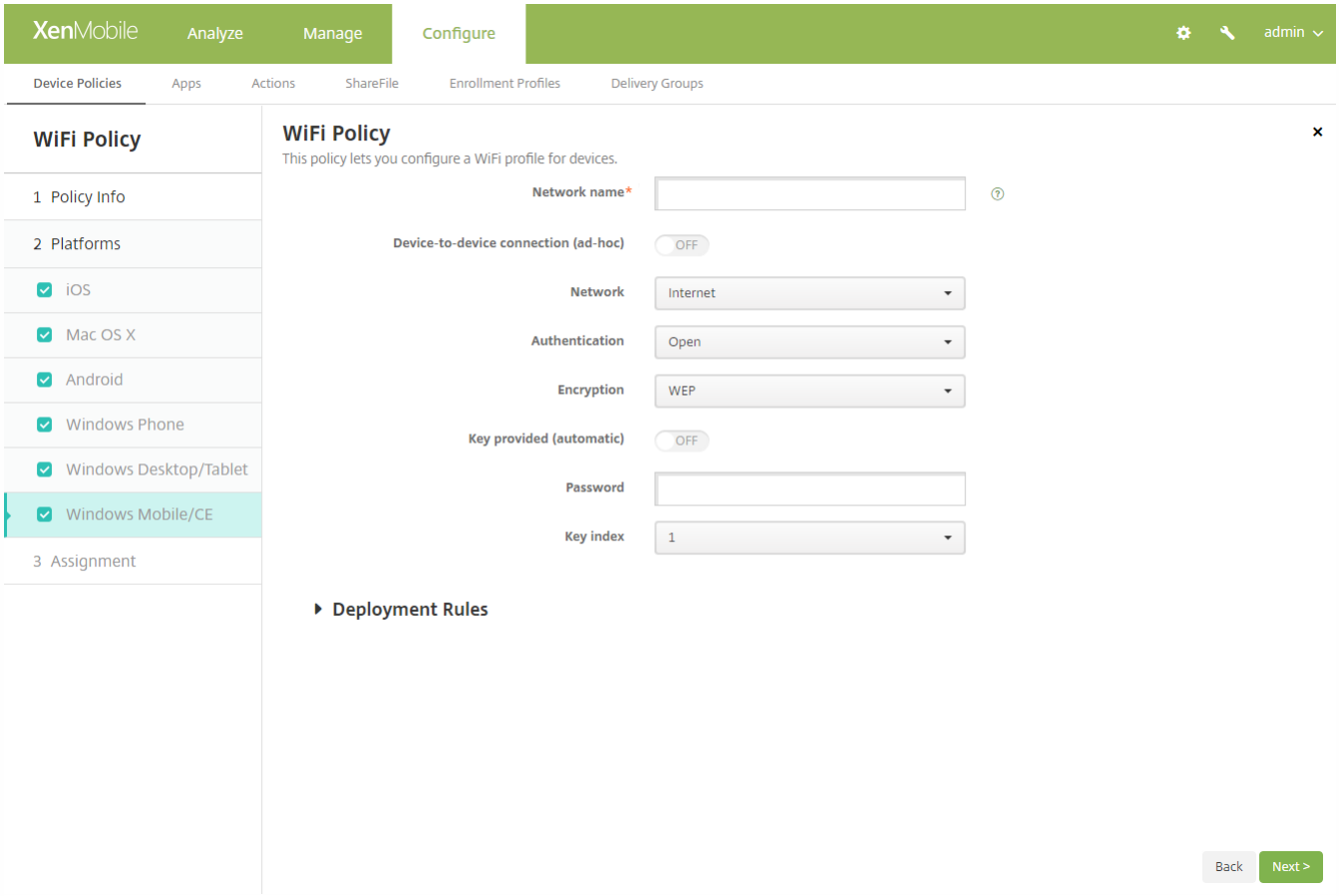
    以下では、上記の接続の種類ごとに、構成するオプションを示します。

オープン

WPAパーソナル、WPA-2パーソナル

WPA-2エンタープライズ

Windows Mobile/CEの構成



次の設定を構成します。

- **ネットワーク名**： 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。
- **デバイス間接続（アドホック）**： 2つのデバイスが直接接続できるようにします。デフォルトは**[オフ]**です。
- **ネットワーク**： デバイスを外部インターネットソースに接続するか、オフィスのイントラネットに接続するかを選択します。
- **認証**： 一覧で、Wi-Fi接続に使用するセキュリティの種類を選択します。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPA-2エンタープライズ

以下では、上記の接続の種類ごとに、構成するオプションを示します。

オープン

WPAパーソナル、WPA-2パーソナル

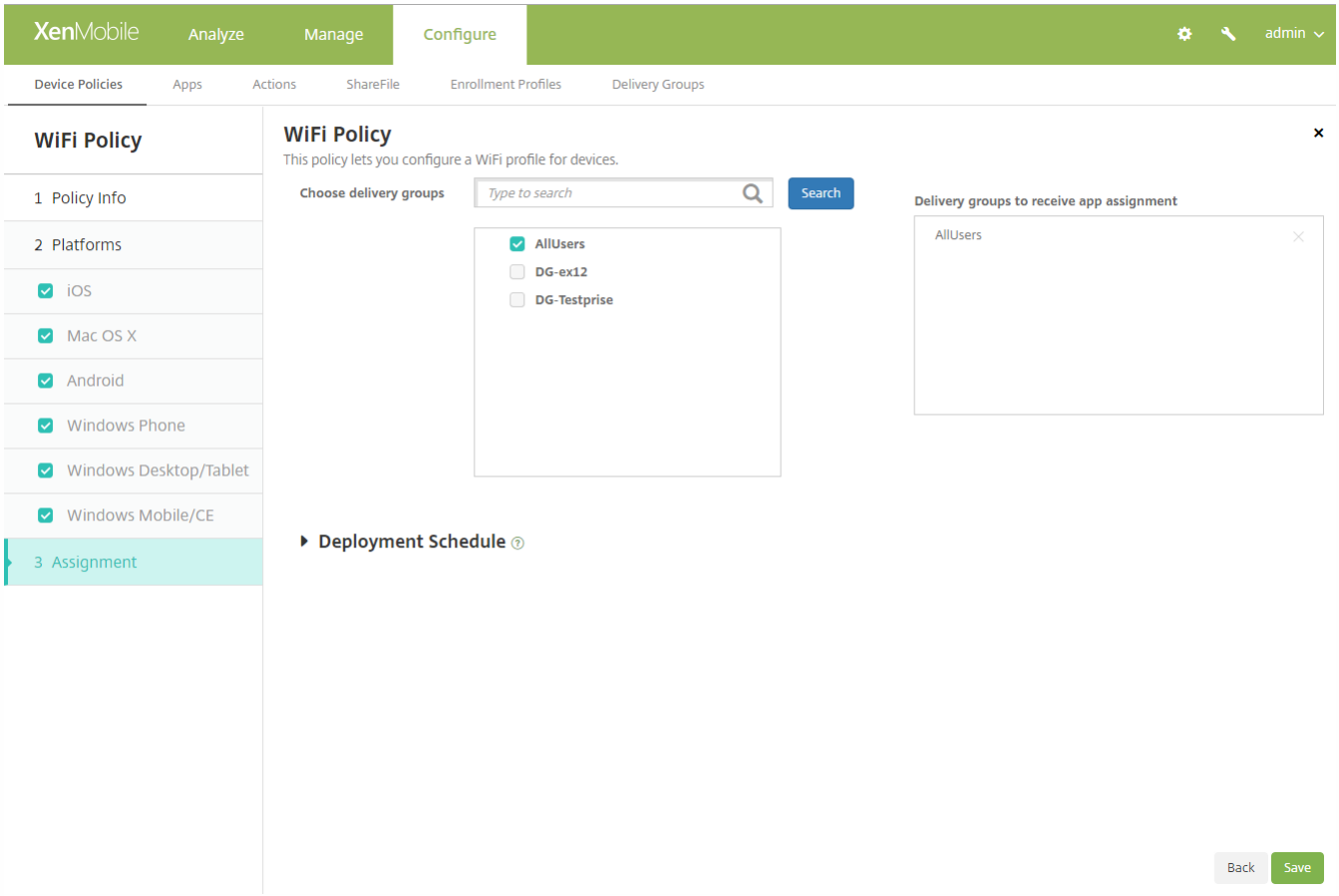
WPA-2エンタープライズ

- **入力されたキー（自動）**： キーを自動で入力するかどうかを選択します。デフォルトは**[オフ]**です。
- **パスワード**： このフィールドにパスワードを入力します。
- **キーインデックス**： キーインデックスを選択します。使用可能なオプションは、**[1]**、**[2]**、**[3]**、**[4]**です。

7. 展開規則を構成します。

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。［Wi-Fiポリシー**割り当て**］ページが開きます。
8. **[Next]**をクリックします。［Wi-Fiポリシー**割り当て**］ページが開きます。
8. **[Next]**をクリックします。［Wi-Fiポリシー**割り当て**］ページが開きます。



9. **[デリバリーグループを選択]** の横に、デリバリーグループを入力して検索するか、1つまたは複数のグループを選択します。選択したグループが**[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは**[オン]** です。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[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、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

Windows CE証明書デバイスポリシー

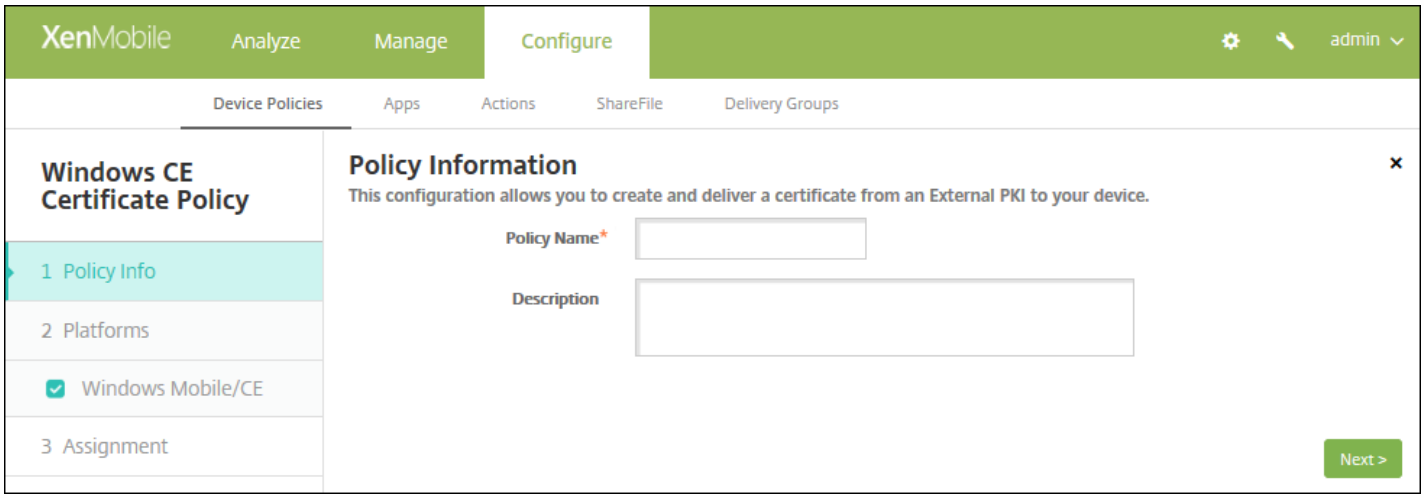
Feb 27, 2017

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、**[構成]** の **[デバイスポリシー]** をクリックします。 **[デバイスポリシー]** ページが開きます。

2. **[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。

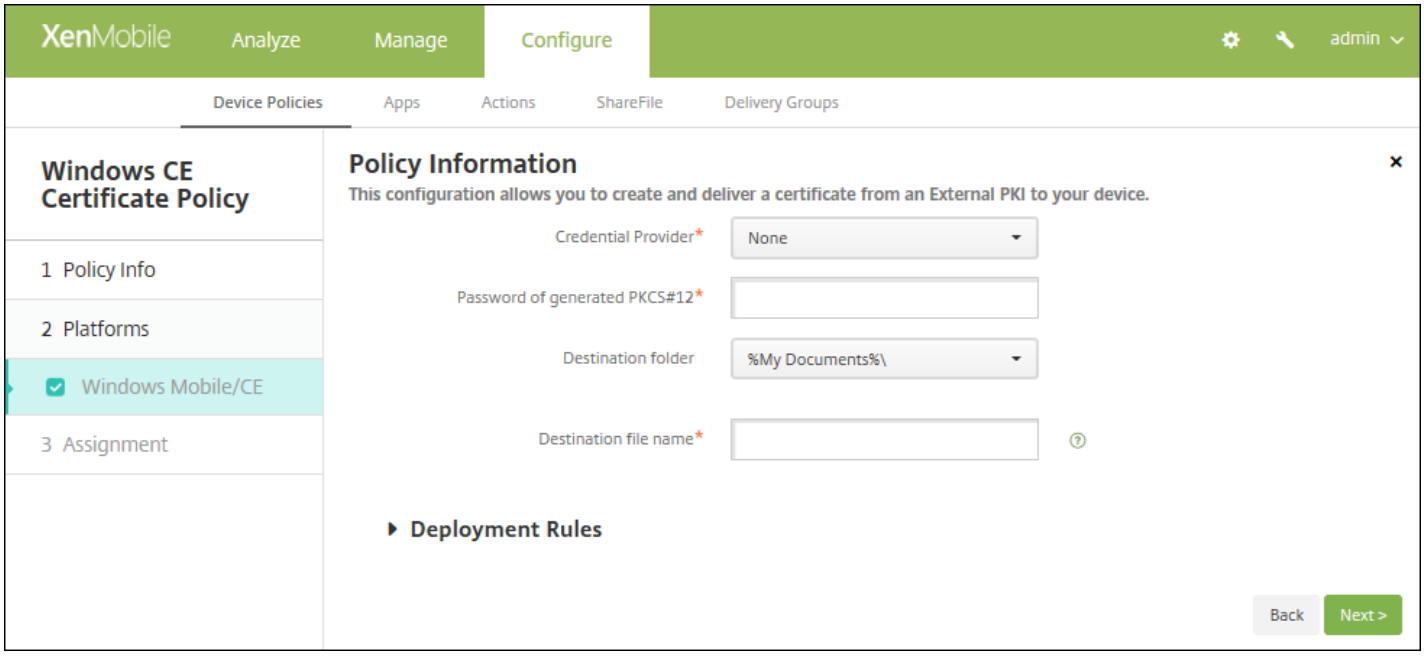
3. **[More]** を展開した後、 **[Security]** の下の **[Windows CE Certificate]** をクリックします。 **[Windows CE Certificate Policy]** 情報ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

- **ポリシー名**：ポリシーの説明的な名前を入力します。
- **説明**：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。

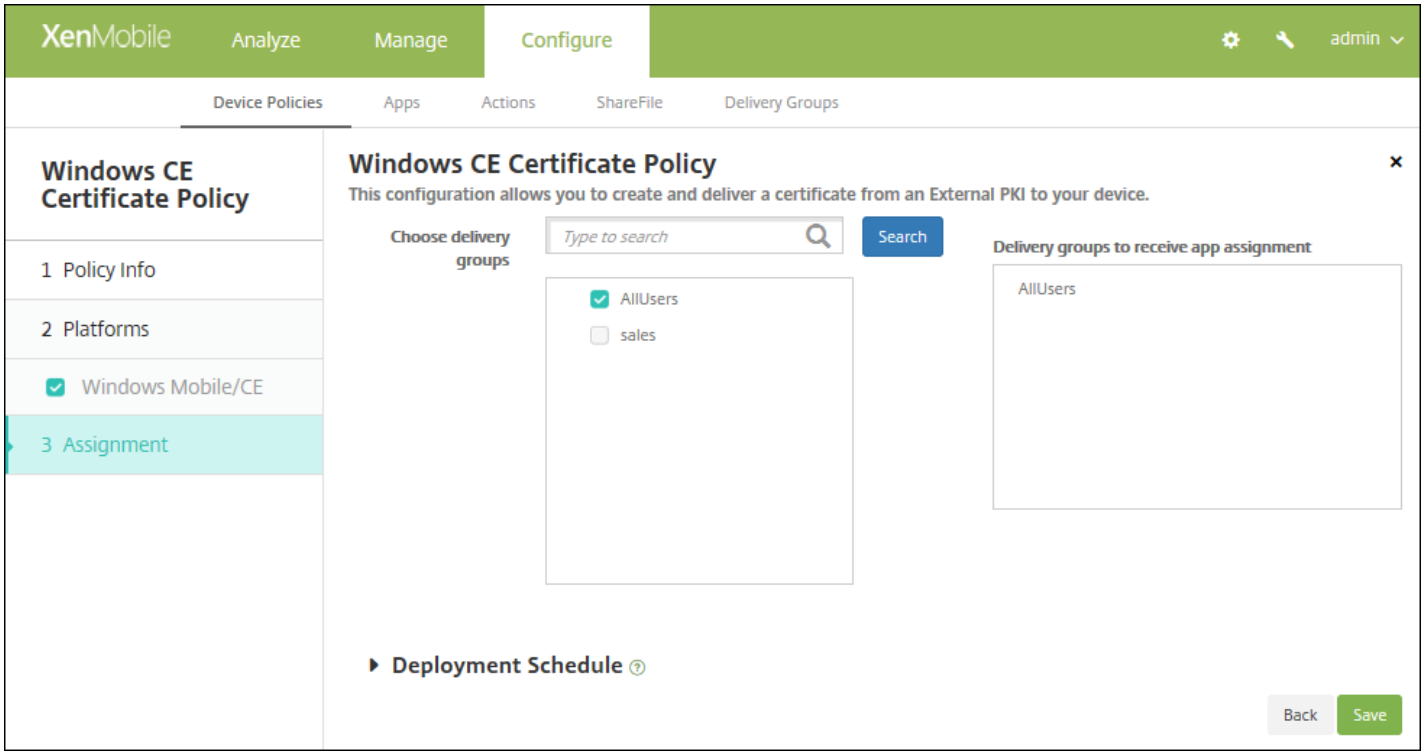


6. 次の設定を構成します。

- **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. 展開規則を構成します。

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. **[デリバリーグループを選択]** 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. **[展開スケジュール]** 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 **[オン]** です。**[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、[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、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

XenMobileオプションデバイスポリシー

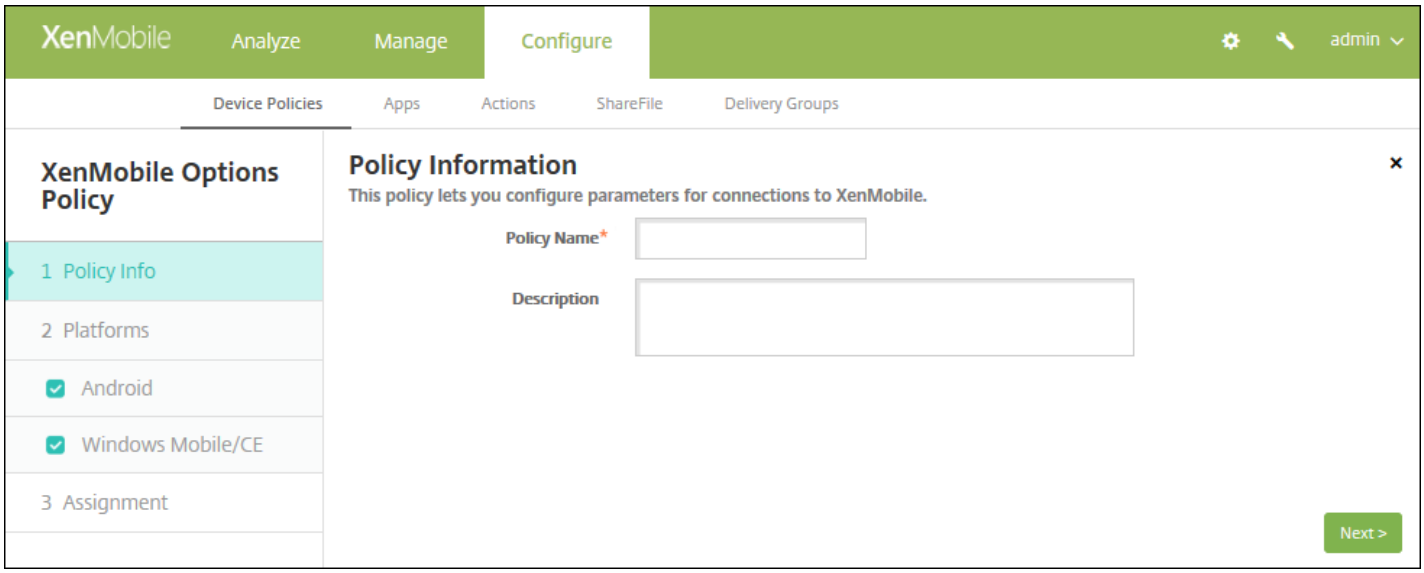
Feb 27, 2017

XenMobileオプションポリシーを追加して、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのSecure Hubの動作を構成します。

1. XenMobileコンソールで、**[構成]** の **[デバイスポリシー]** をクリックします。**[デバイスポリシー]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[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オプションポリシー]** ページが開きます。



4. **[ポリシー情報]** ペインで、以下の情報を入力します。

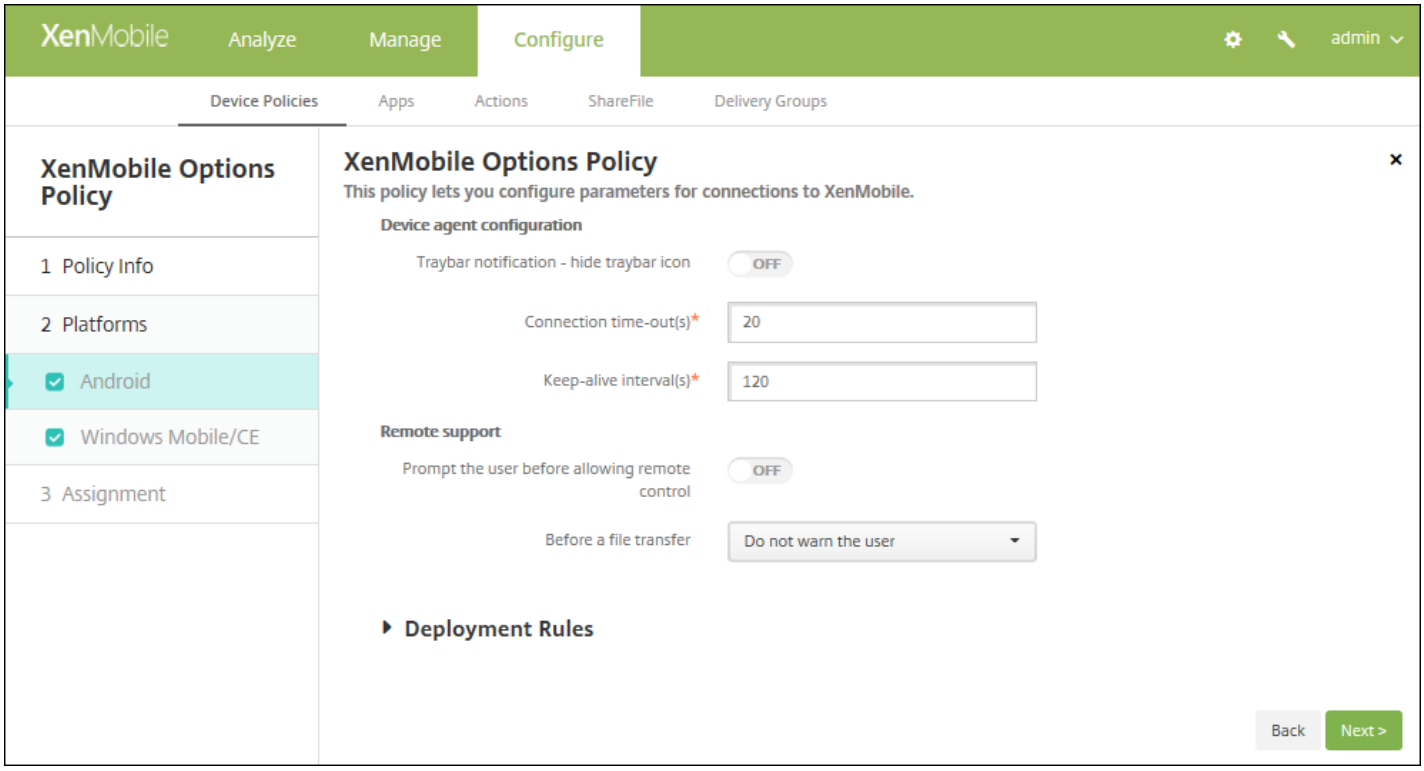
- **ポリシー名**：ポリシーの名前を入力します。
- **説明**：任意で、ポリシーの説明を入力します。

5. **[次へ]** をクリックします。**[Policy Platforms]** ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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。

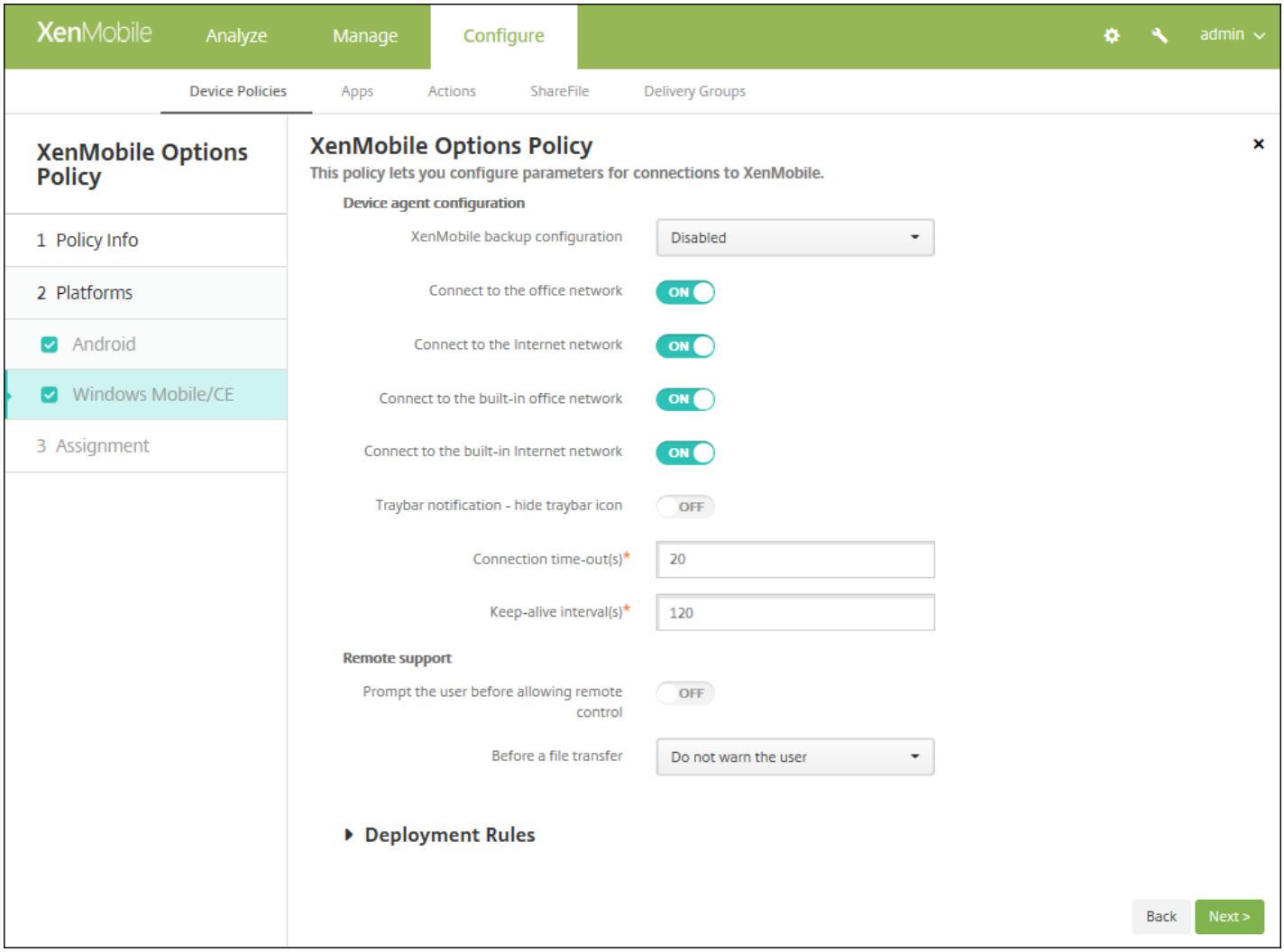
Androidの設定の構成



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**： Remote Supportの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは **[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、 **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



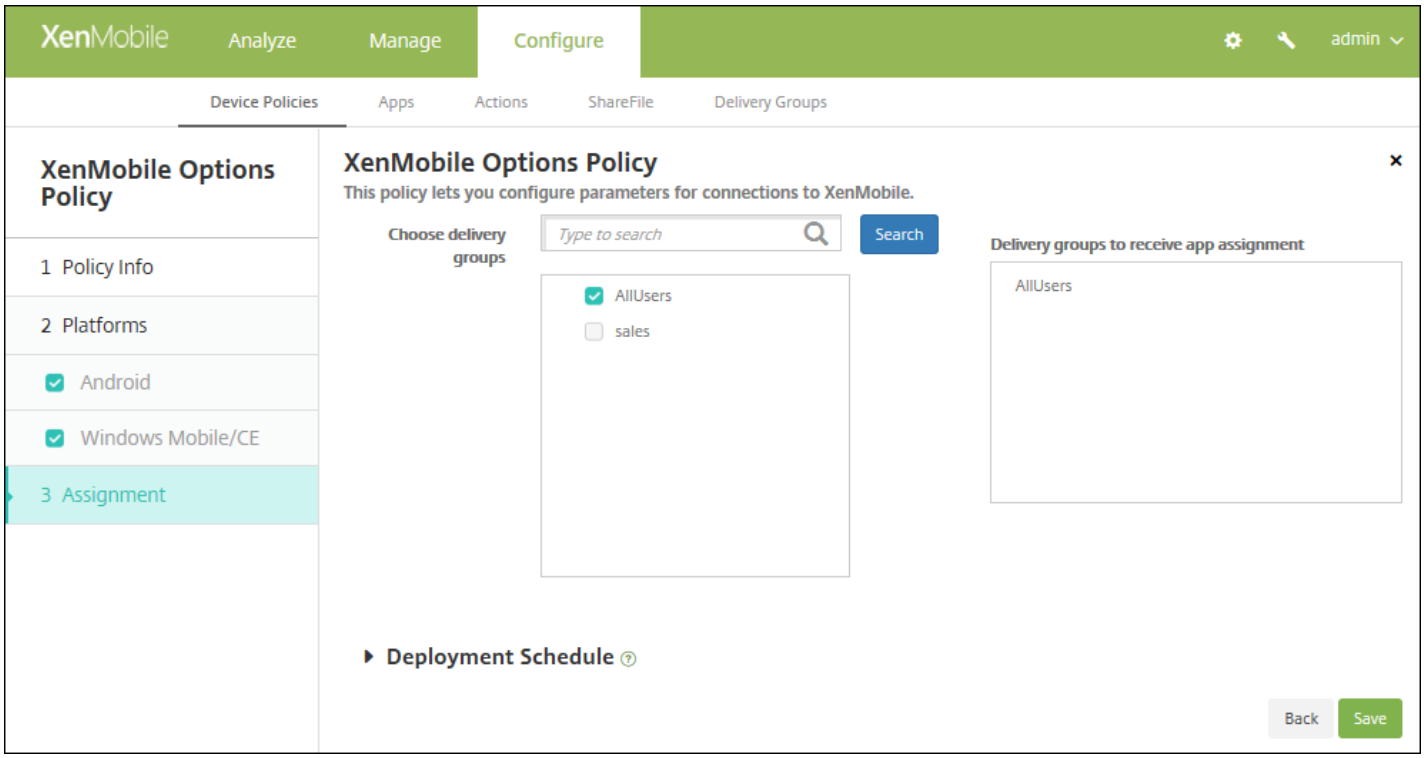
次の設定を構成します。

- **デバイス エージェント構成**
  - **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。
    - 無効
    - XenMobileインストール後の初回接続時
    - 各デバイスの再起動後の初回接続時
  - **オフィス ネットワークに接続**
  - **インターネット ネットワークに接続**
  - **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。

- リモート サポート
  - **Prompt the user before allowing remote control**： Remote Supportの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは［**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、 **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. ［**デリバリーグループを選択**］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［**アプリ割り当てを受信するためのデリバリーグループ**］一覧に表示されます。

10. ［**展開スケジュール**］を展開して以下の設定を構成します。

- ［**展開**］の横の［**オン**］をクリックすると展開がスケジュールされ、［**オフ**］をクリックすると展開が行われません。デフォルトのオプションは［**オン**］です。［**オフ**］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。
- ［**展開スケジュール**］の横の［**すぐに**］または［**あとで**］をクリックします。デフォルトのオプションは［**すぐに**］です。
- ［**あとで**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**展開状態**］の横の［**接続するたび**］をクリックするか、［**以前の展開が失敗した場合のみ**］をクリックします。デフォルトのオプションは、［**接続するたび**］です。
- ［**常時接続に対する展開**］の横の［**オン**］または［**オフ**］をクリックします。デフォルトのオプションは［**オフ**］です。

注：

- このオプションは、［**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、**[常時接続に対する展開]**は適用されません。

11. **[保存]**をクリックします。

XenMobileアンインストールデバイスポリシー

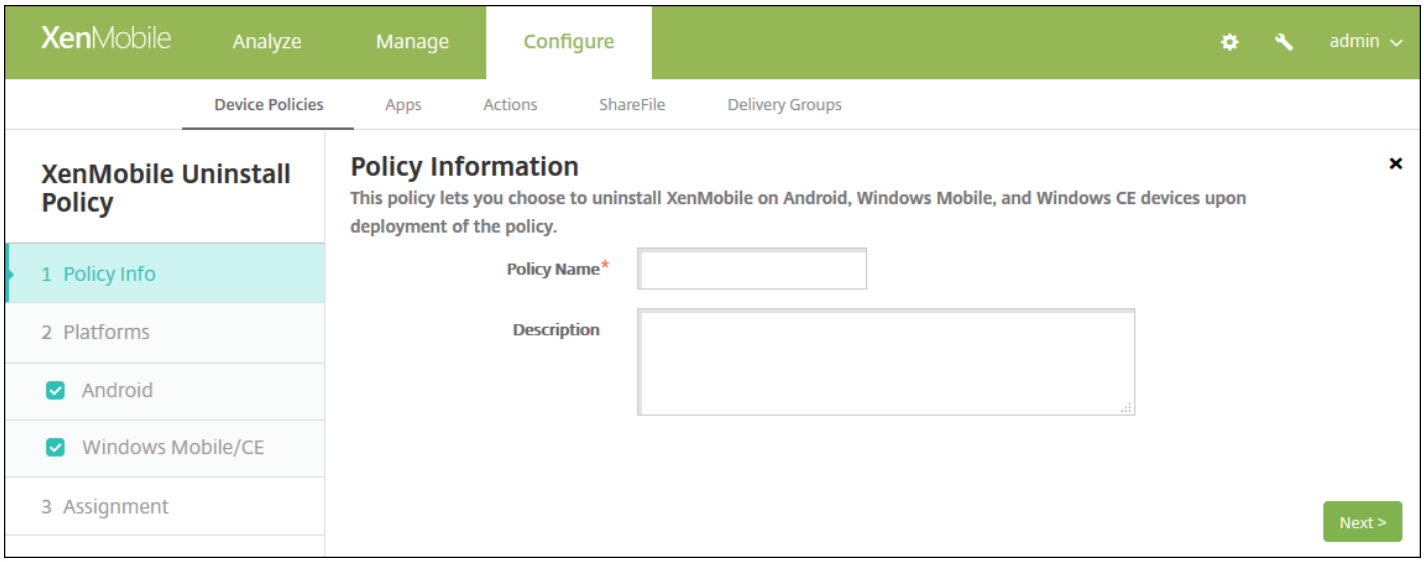
Feb 27, 2017

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、**[構成]** の **[デバイスポリシー]** をクリックします。**[Device Policies]** ページが開きます。

2. **[追加]** をクリックします。**[新しいポリシーの追加]** ダイアログボックスが開きます。

3. **[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. **[ポリシー情報]** ペインで、以下の情報を入力します。

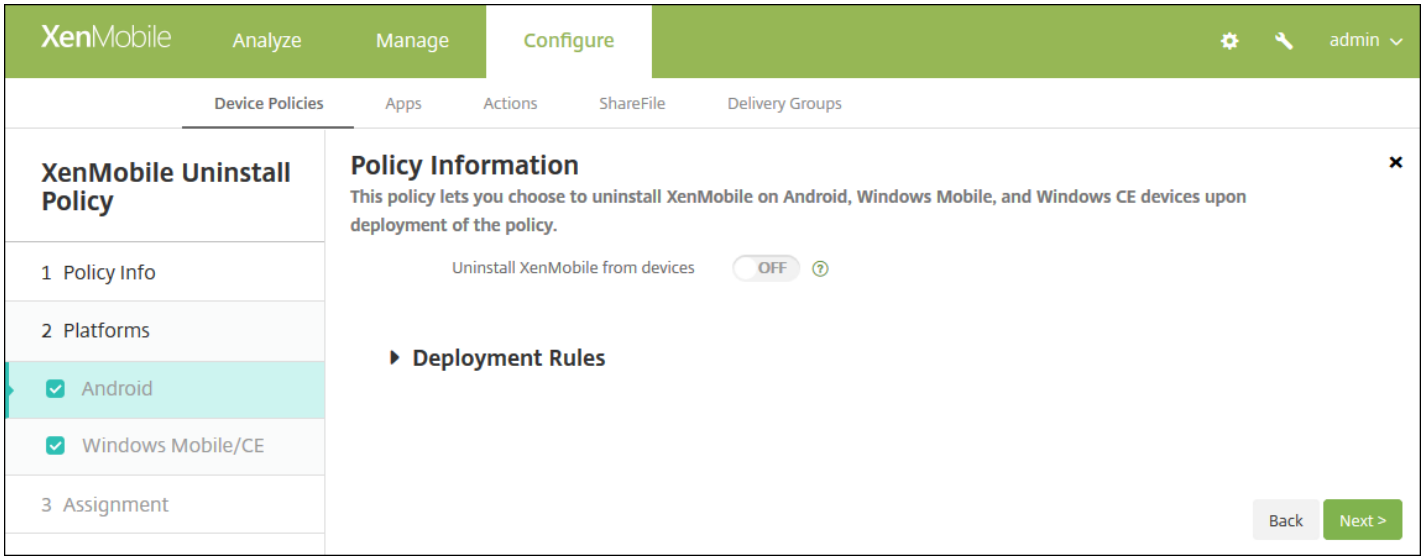
- **Policy Name**：ポリシーの説明的な名前を入力します。
- **Description**：任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。**[Policy Platforms]** 情報ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順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

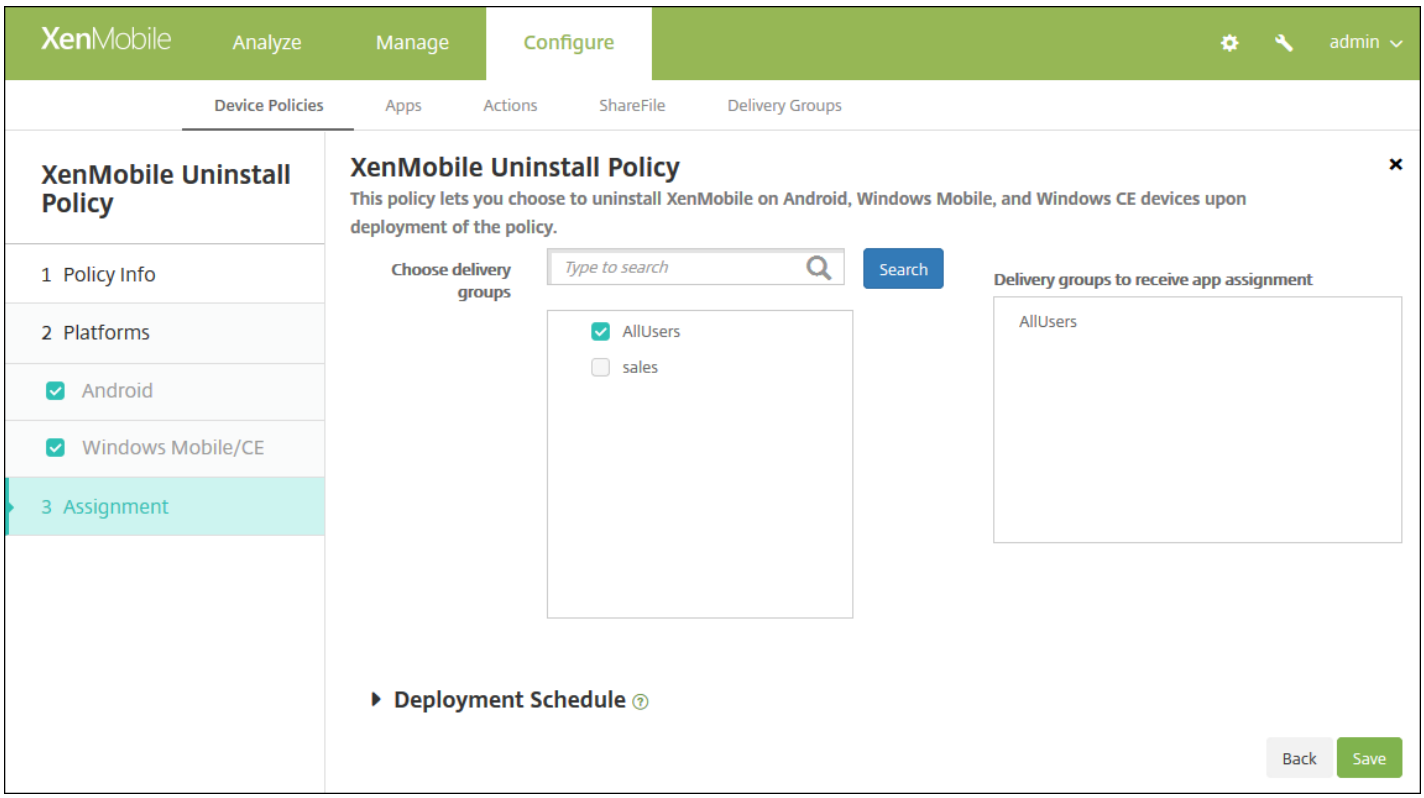


選択したプラットフォームごとに、次の設定を構成します。

- **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. 展開規則を構成します。

8. **[次へ]** をクリックします。 **[XenMobileアンインストールポリシー]** 割り当てページが開きます。



9. **[デリバリーグループを選択]** の横に、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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。**[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、**[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

アプリケーションの追加

May 10, 2017

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。
- **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。
- **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、デバイスに展開する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ないインストールのことです。アプリは、バックグラウンドで自動的にインストールされます。サイレントインストールを実装するには、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デバイスを監視モードにします。詳しくは、「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」を参照してください。
> - Androidアプリの場合、Samsung for Enterprise（SAFE）またはKNOXポリシーをデバイスで有効にします。
>   このためには、Samsung MDMライセンスキーデバイスポリシーを設定して、Samsung ELMおよびKNOXライセンスキーを生成します。詳しくは、「Samsung MDMライセンスキーデバイスポリシー」を参照してください。

モバイルおよびMDXアプリケーションのしくみ

XenMobileでは、Secure Hub、Secure Mail、Secure WebなどのXenMobile Appsを含むiOS、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。XenMobile 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。

XenMobile Apps for iOSおよびAndroidを配布するには、Citrixからパブリックストアで MDXファイルをダウンロードし、これらのファイルをXenMobileコンソールにアップロードし（**[構成] > [アプリ]**）、必要に応じてMDXポリシーを更新してから、MDXファイルをパブリックアプリケーションストアにアップロードします。詳しくは、この記事の「MDXアプリケーションの追加」を参照してください。

XenMobile Apps for Windowsを配布するには、Citrixからアプリファイルをダウンロードし、MDX Toolkitでラッピングしてから、XenMobileコンソールにアップロードします。必要に応じてMDXポリシーを変更して、デリバリーグループ経由でユーザーデバイスにアプリを配信します。詳しくは、XenMobile Appsドキュメントの「Public App Store Delivery of XenMobile Apps」を参照してください。

Citrixは、Citrixのロジックおよびポリシーでios、Android、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す。ユーザーアカウントの作成や管理用のテンプレートを構成することもできます。XenMobileには、Security Assertion Markup Language（SAML）コネクタが含まれています。SAMLコネクタは、SSOおよびユーザーアカウント管理用のSAMLプロトコルをサポートするWebアプリ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。

詳しくは、「WebおよびSaaSアプリケーションの追加」を参照してください。

エンタープライズアプリケーションのしくみ

エンタープライズ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Secure Hub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と、XenMobileはそのアプリケーションコネクタを作成します。詳しくは、この記事の「エンタープライズアプリケーションの追加」を参照してください。

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。詳しくは、この記事の「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。

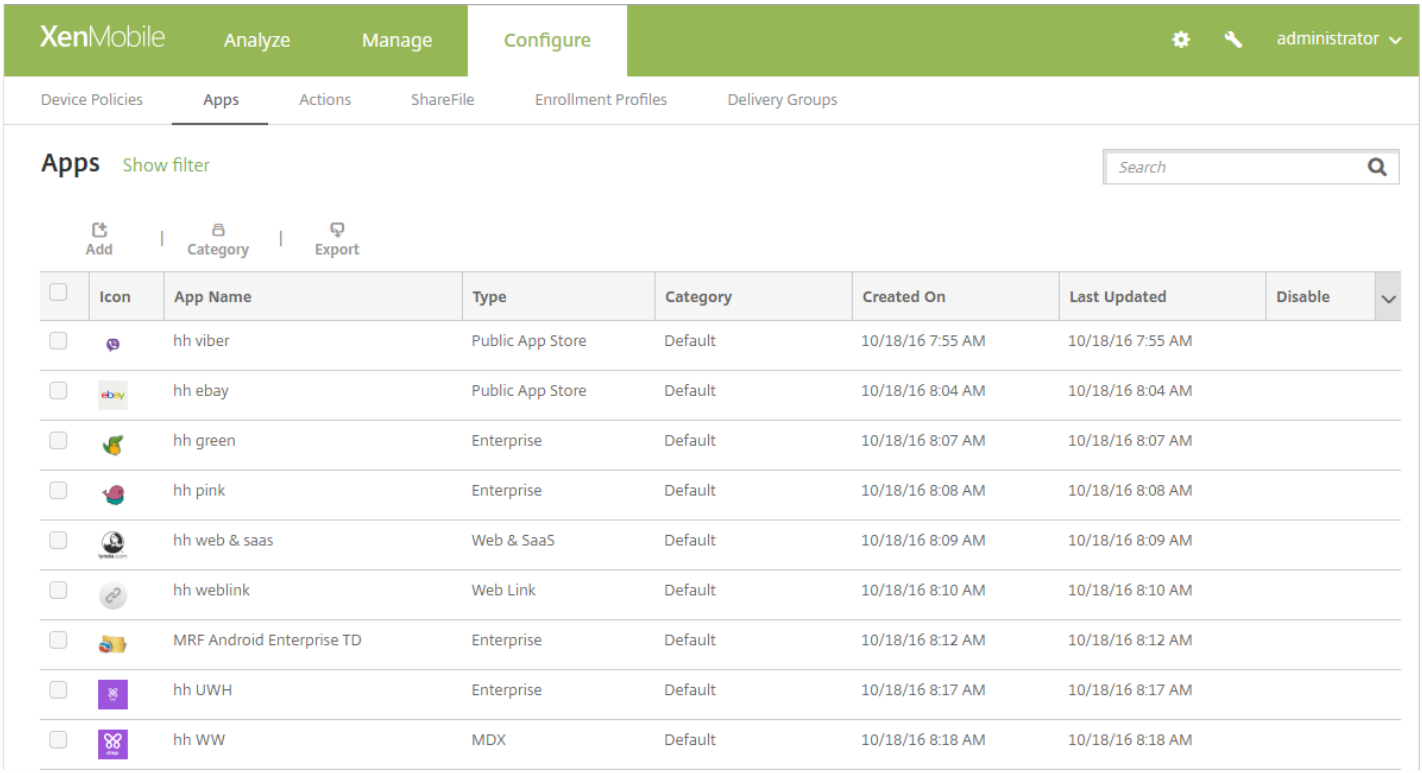
Webリンクのしくみ

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XenMobile Storeにアイコンとして表示されます。ユーザーがSecure Hubを使ってログオンすると、リンクは使用可能なアプリ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。詳しくは、この記事の「Webリンクアプリケーションの追加」を参照してください。

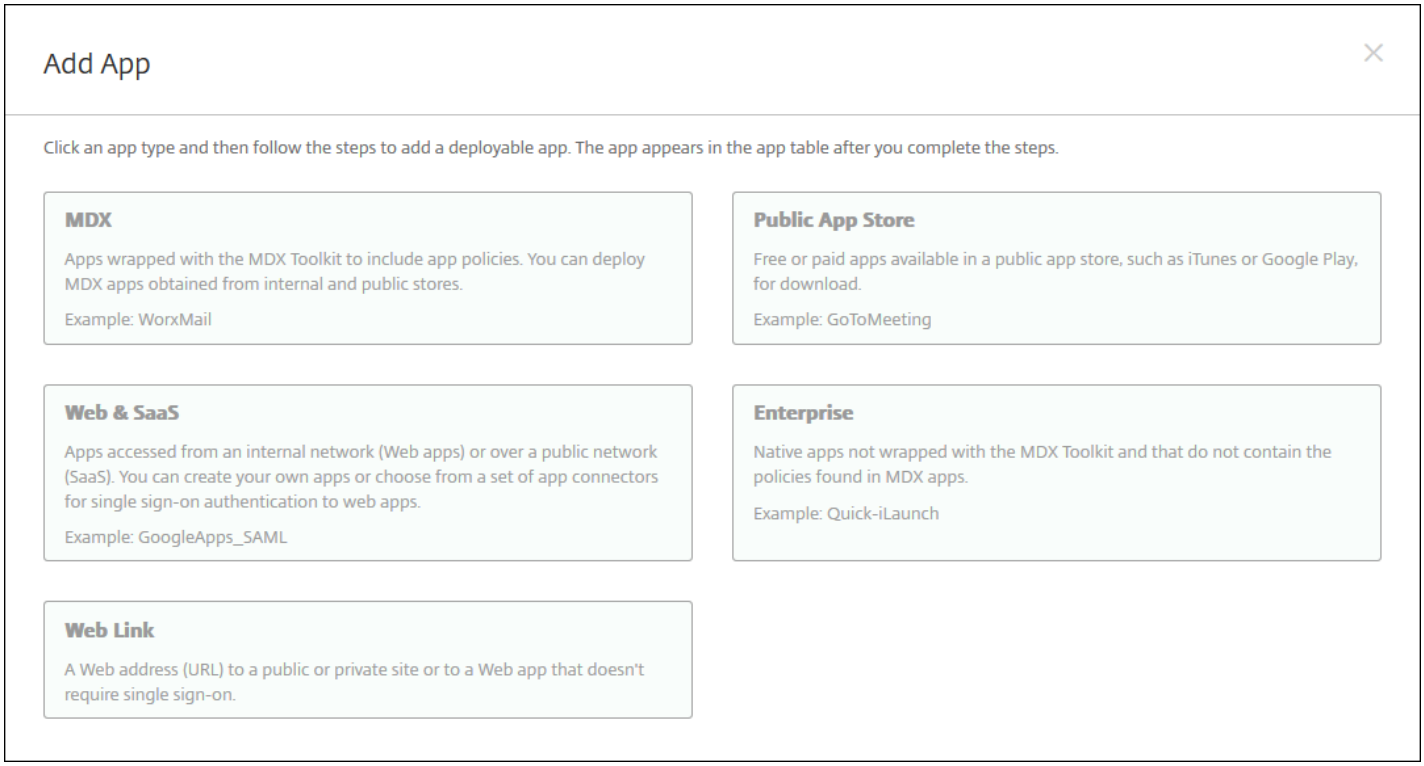
MDXアプリケーションの追加

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、「MDXポリシーの概要」を参照してください。このトピックでは、ポリシーの詳細についても説明しています。

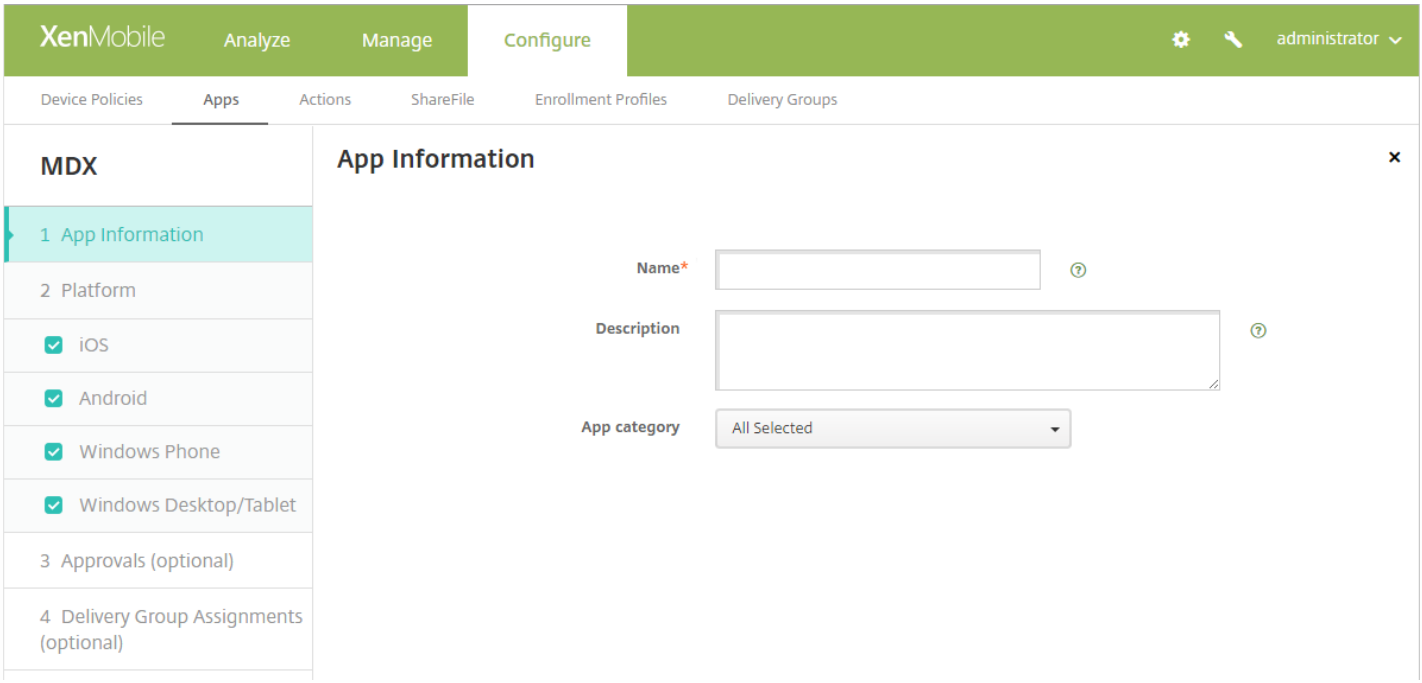
1. XenMobileコンソールで、**[構成]**の**[アプリ]**をクリックします。**[アプリ]**ページが開きます。



2. **[追加]** をクリックします。 **[アプリの追加]** ダイアログボックスが開きます。



3. **[MDX]** をクリックします。 **[MDXアプリケーション情報]** 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。

- **名前**： 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、**[アプリ]** の表の **[アプリ名]** 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、「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. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順11を参照してプラットフォームの展開規則を設定します。

7. **[アップロード]** をクリックしてアップロードする.mdxファイルの場所へ移動し、そのファイルを選択します。

- iOS VPP B2Bアプリケーションを追加する場合は、**[お使いのアプリケーションは VPP B2Bアプリケーションですか?]** をクリックして、 一覧から使用するB2B VPPアカウントを選択します。

8. **[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。

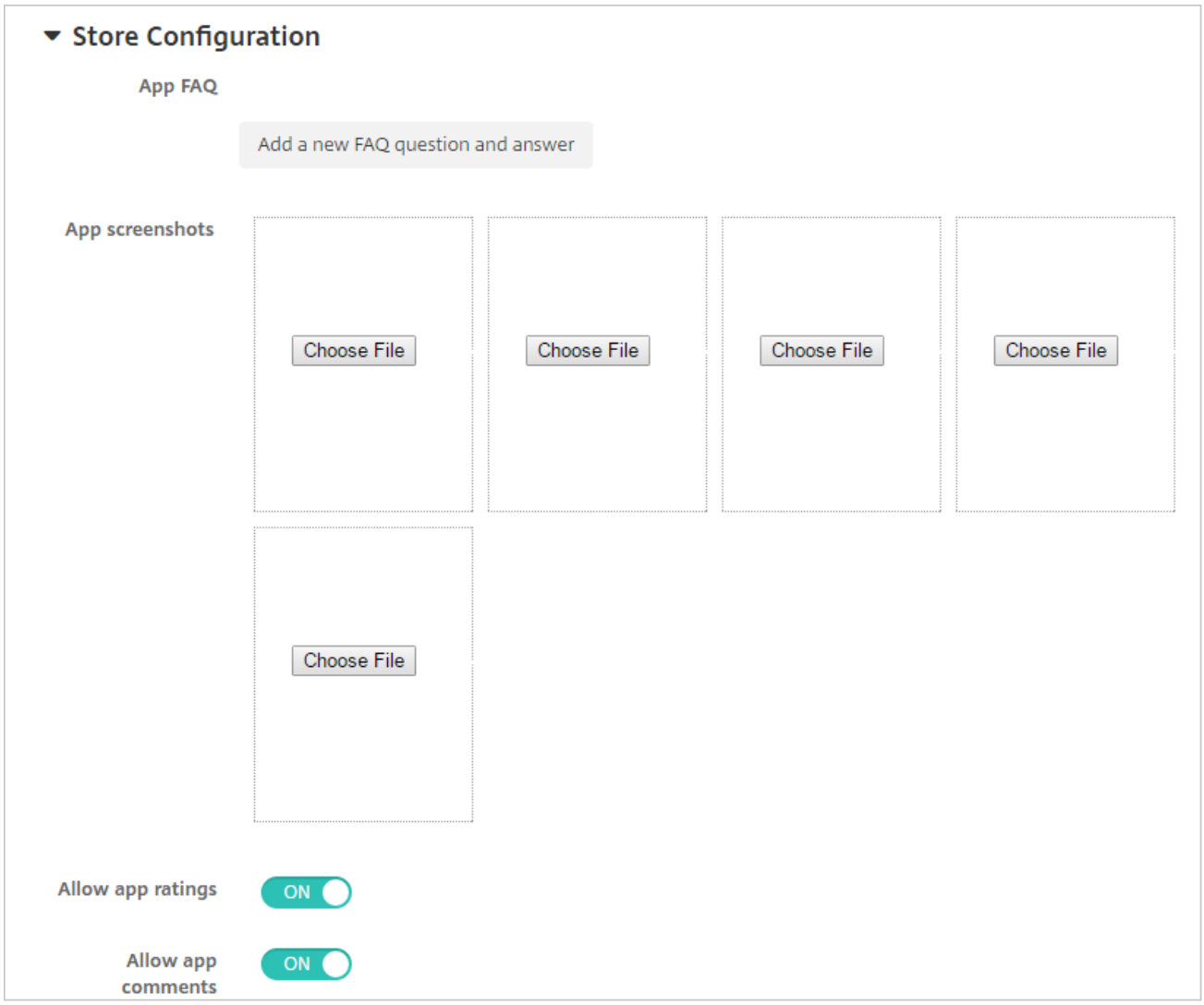
- **File name**：アプリケーションに関連付けられているファイル名を入力します。
- **App Description**：アプリケーションの説明を入力します。
- **App version**：任意で、アプリケーションのバージョン番号を入力します。
- **Minimum OS version**：任意で、アプリケーションを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
- **Maximum OS version**：任意で、アプリケーションを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバ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以降で利用できます。

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、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、「MDXポリシーの概要」を参照してください。

11. 展開規則を構成します。

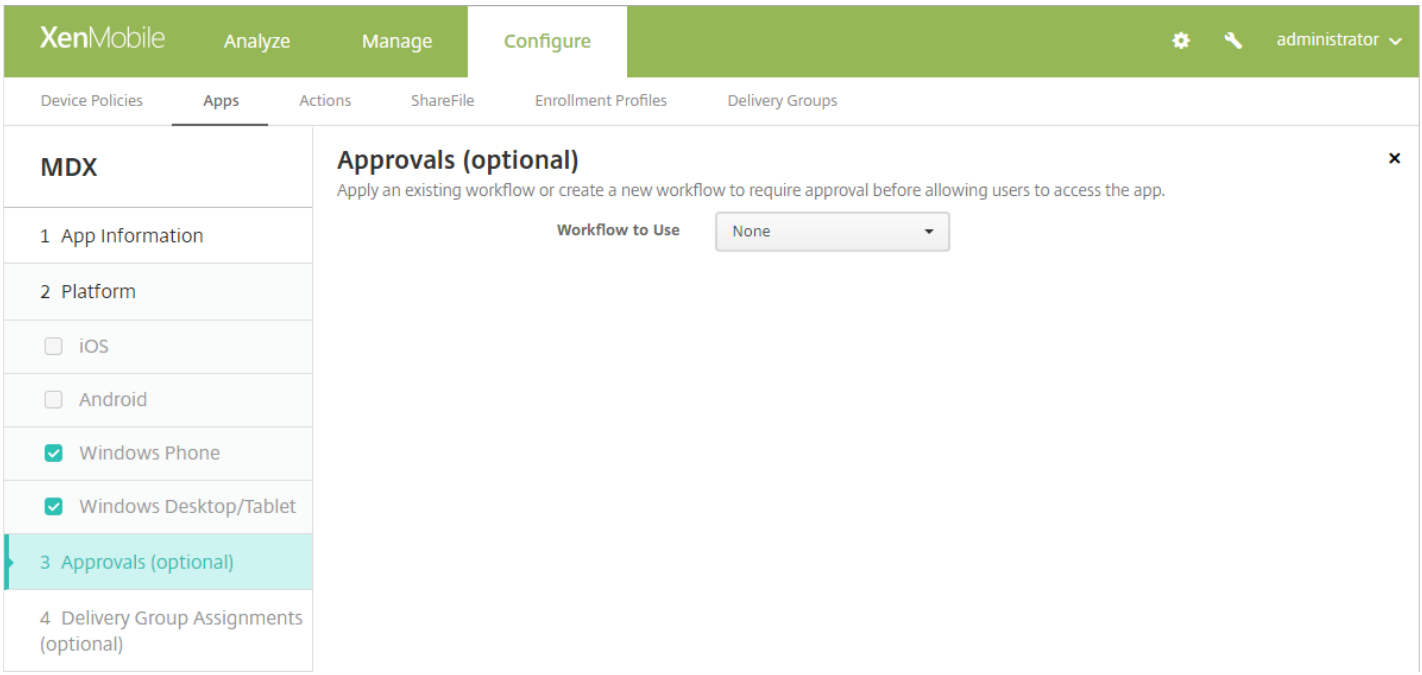
12.［**XenMobile Store Configuration**］を展開します。



任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリ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XenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **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. **[次へ]**をクリックします。**[承認]**ページが開きます。



ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順15に進みます。

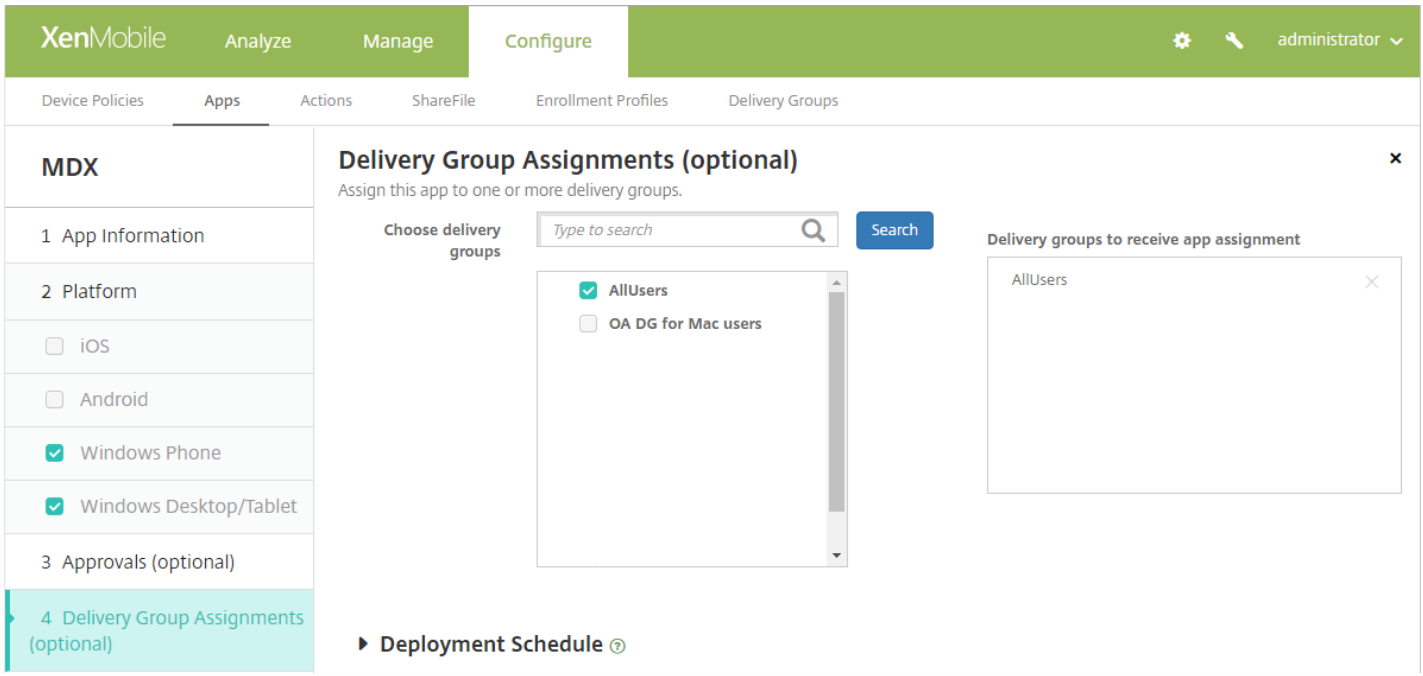
ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **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。
- **[新しいワークフローの作成]**を選択した場合は、次の設定を構成します。詳しくは、「ワークフローの作成および管理」を参照してください。
  - **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。
  - **メール承認テンプレート**： 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **マネージャー承認のレベル**： 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［1つのレベル］です。選択できるオプションは以下のとおりです。

- 不必要
- 1つのレベル
- 2つのレベル
- 3つのレベル

- **Active Directoryドメインの選択**： 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を検索**： 検索フィールドに、追加で必要なユーザーの名前を入力して、**[検索]** をクリックします。名前はActive Directoryで取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[選択した追加の必須承認者]** の一覧に表示されます。
  - **[選択した追加の必須承認者]** の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して **[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. **[次へ]** をクリックします。 **[デリバリーグループ割り当て]** ページが開きます。



15. **[デリバリーグループを選択]** の横に、アプリ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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

16. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- ［展開スケジュール］の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**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、**[接続するたび]** です。

- **[常時接続に対する展開]**の横の**[オン]**または**[オフ]**をクリックします。デフォルトのオプションは**[オフ]**です。

注：

- このオプションは、**[設定]**の**[サーバープロパティ]**において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]**は適用されません。

17. **[保存]**をクリックします。

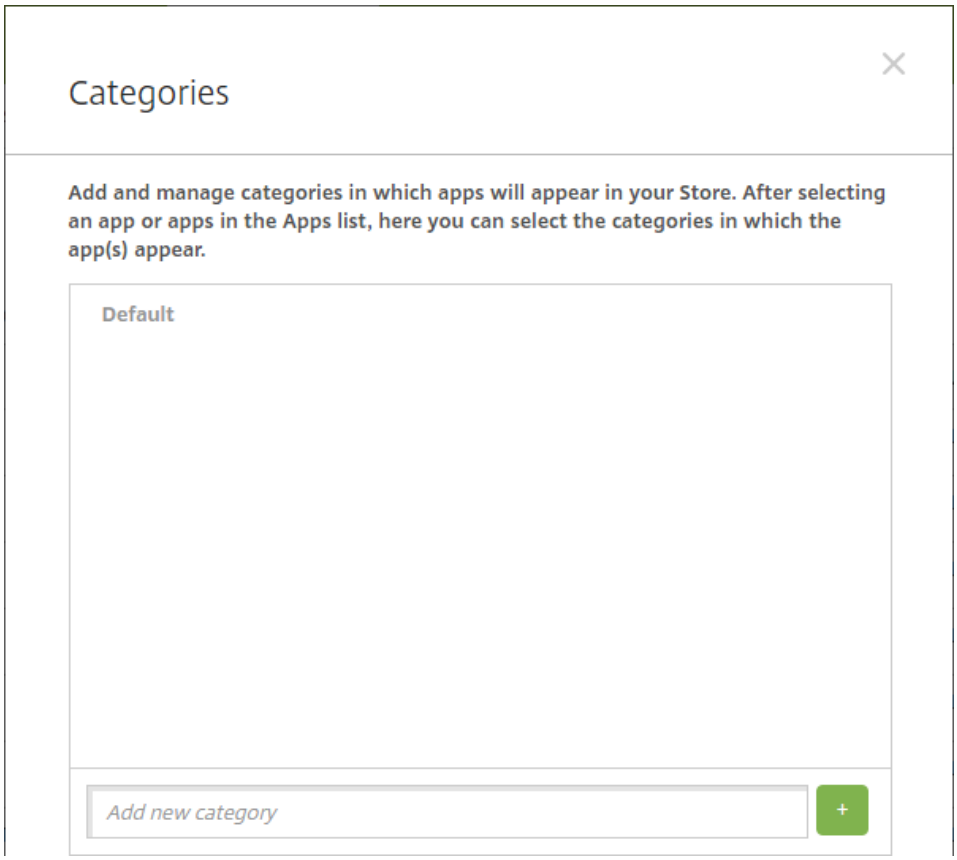
アプリケーションカテゴリの作成

ユーザーがSecure Hub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**[アプリ]**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。

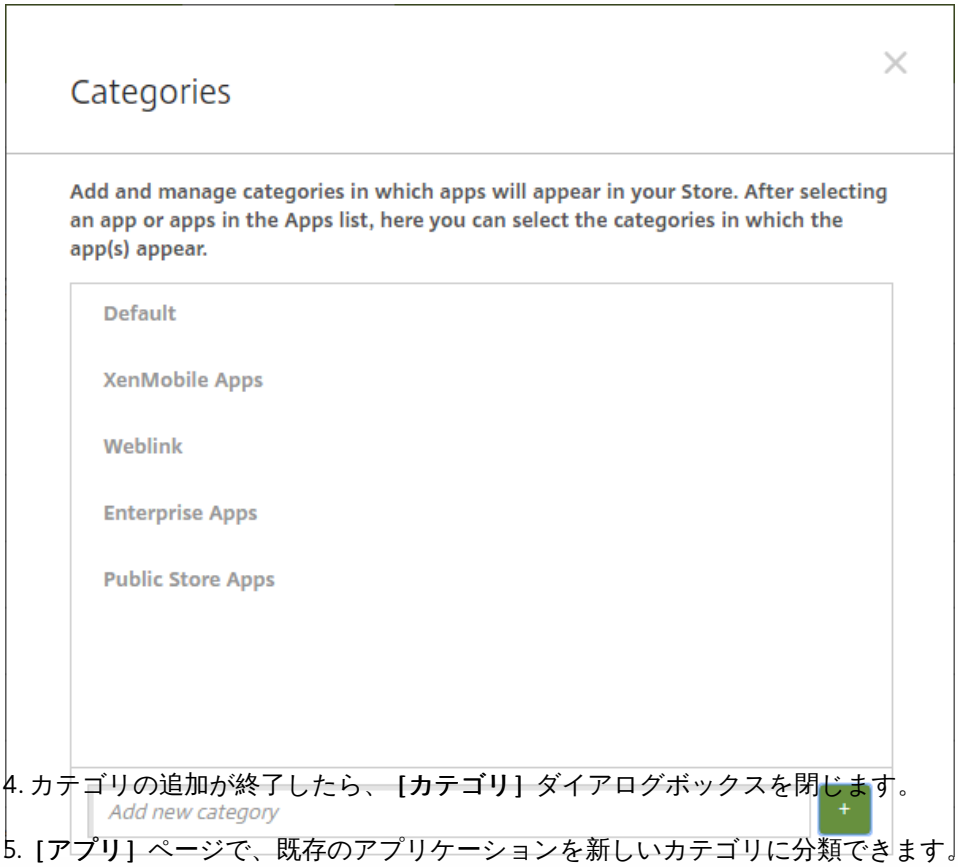
1. XenMobileコンソールで、**[構成]**の**[アプリ]**をクリックします。**[アプリ]**ページが開きます。

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、**[カテゴリ]** ダイアログボックスに表示されます。



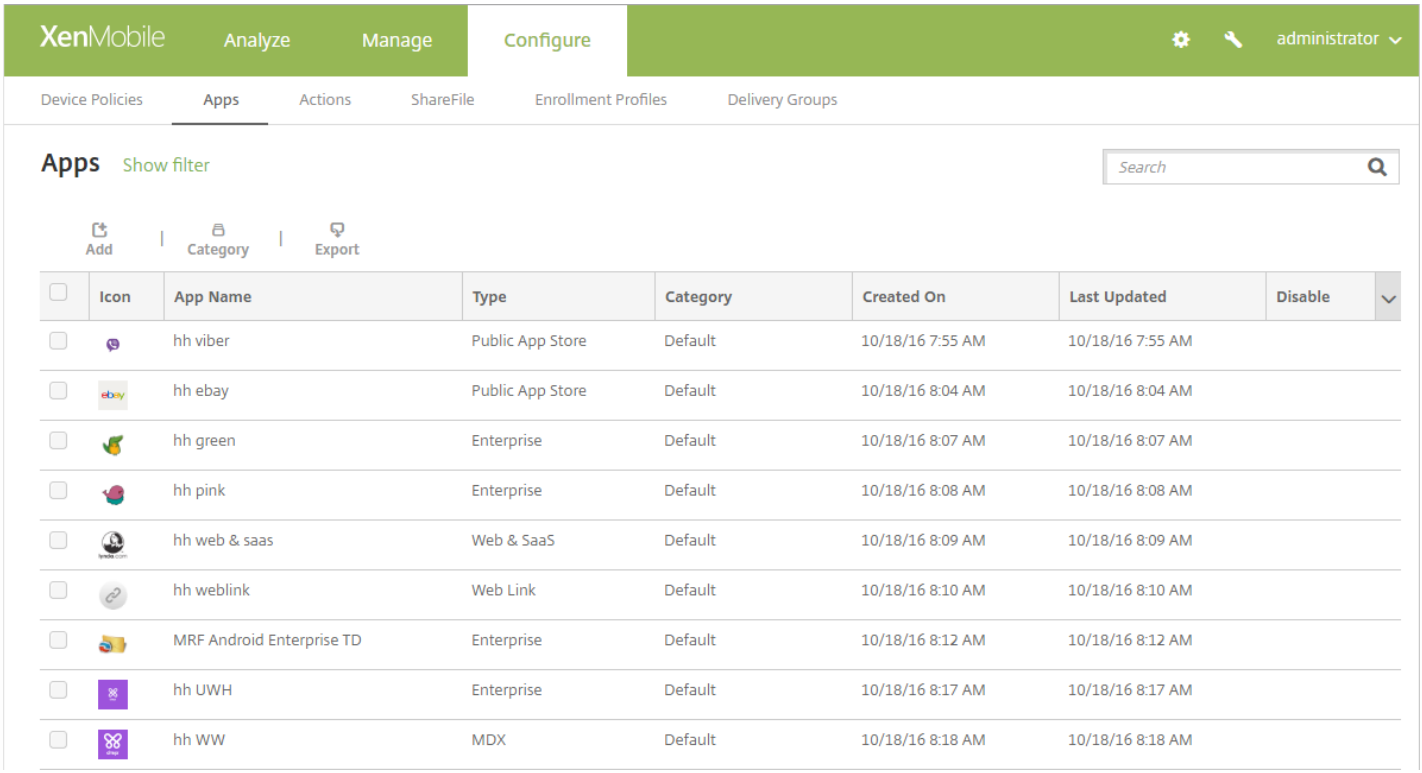
4. カテゴリの追加が終了したら、**[カテゴリ]** ダイアログボックスを閉じます。
5. **[アプリ]** ページで、既存のアプリケーションを新しいカテゴリに分類できます。

- 分類するアプリケーションを選択します。
- **[編集]** をクリックします。**[アプリケーション情報]** ページが開きます。
- **[アプリケーションカテゴリ]** の一覧で、新しいカテゴリのチェックボックスをオンにしてカテゴリを適用します。既存のカテゴリでアプリ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。
- **[デリバリーグループ割り当て]** タブをクリックするか、後続の各ページで **[次へ]** をクリックして、残りのアプリ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。
- **[デリバリーグループ割り当て]** のページの **[保存]** をクリックして新しいカテゴリを適用します。新しいカテゴリがアプリケーションに適用され、**[アプリ]** の表に表示されます。

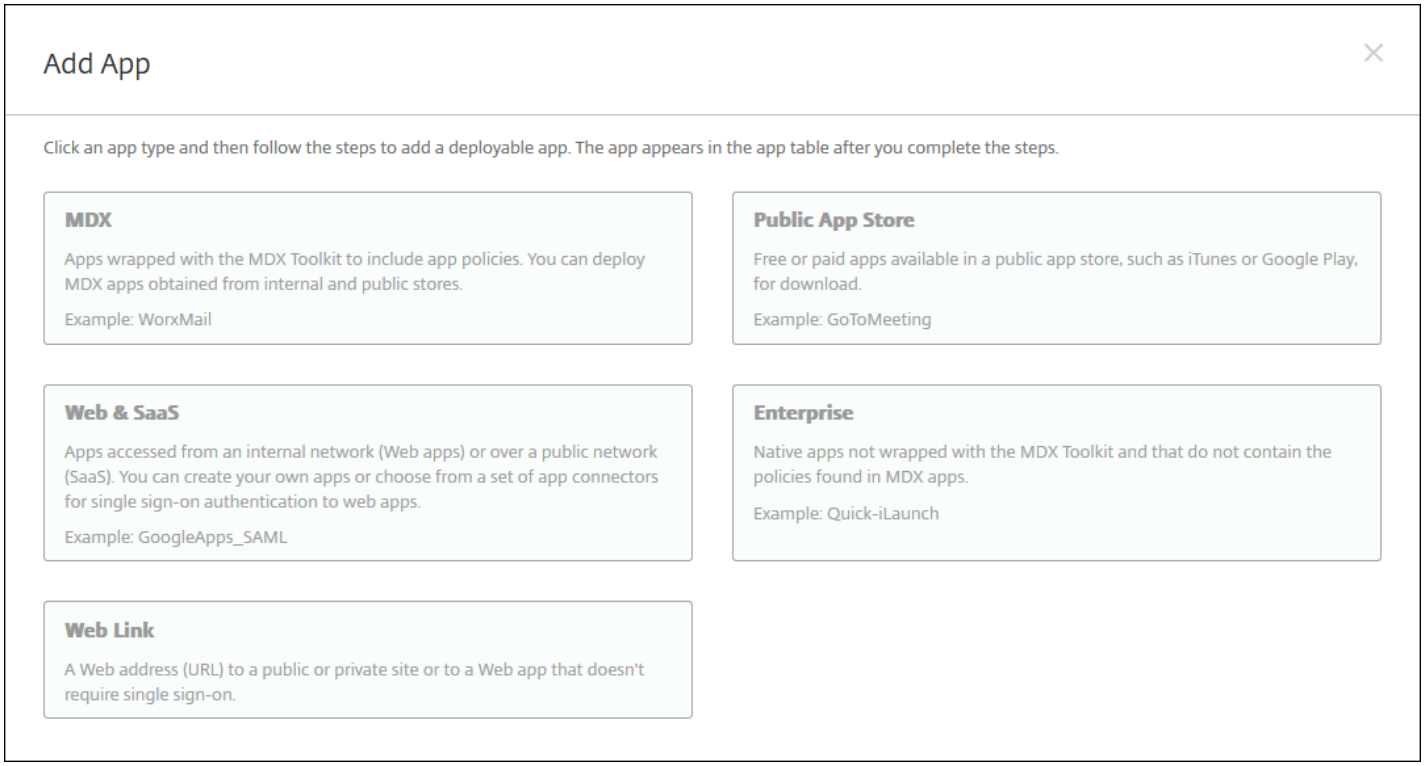
パブリックアプリケーションストアのアプリケーションの追加

iTunesやGoogle Playなどのパブリックアプリケーションストアで入手できる無料または有料のアプリケーションをXenMobileに追加できます。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。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。

1. XenMobileコンソールで、**[構成]** の **[アプリ]** をクリックします。**[アプリ]** ページが開きます。



2. **[追加]** をクリックします。 **[アプリの追加]** ダイアログボックスが開きます。



3. **[商用アプリケーションストア]** をクリックします。 **[アプリケーション情報]** 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。

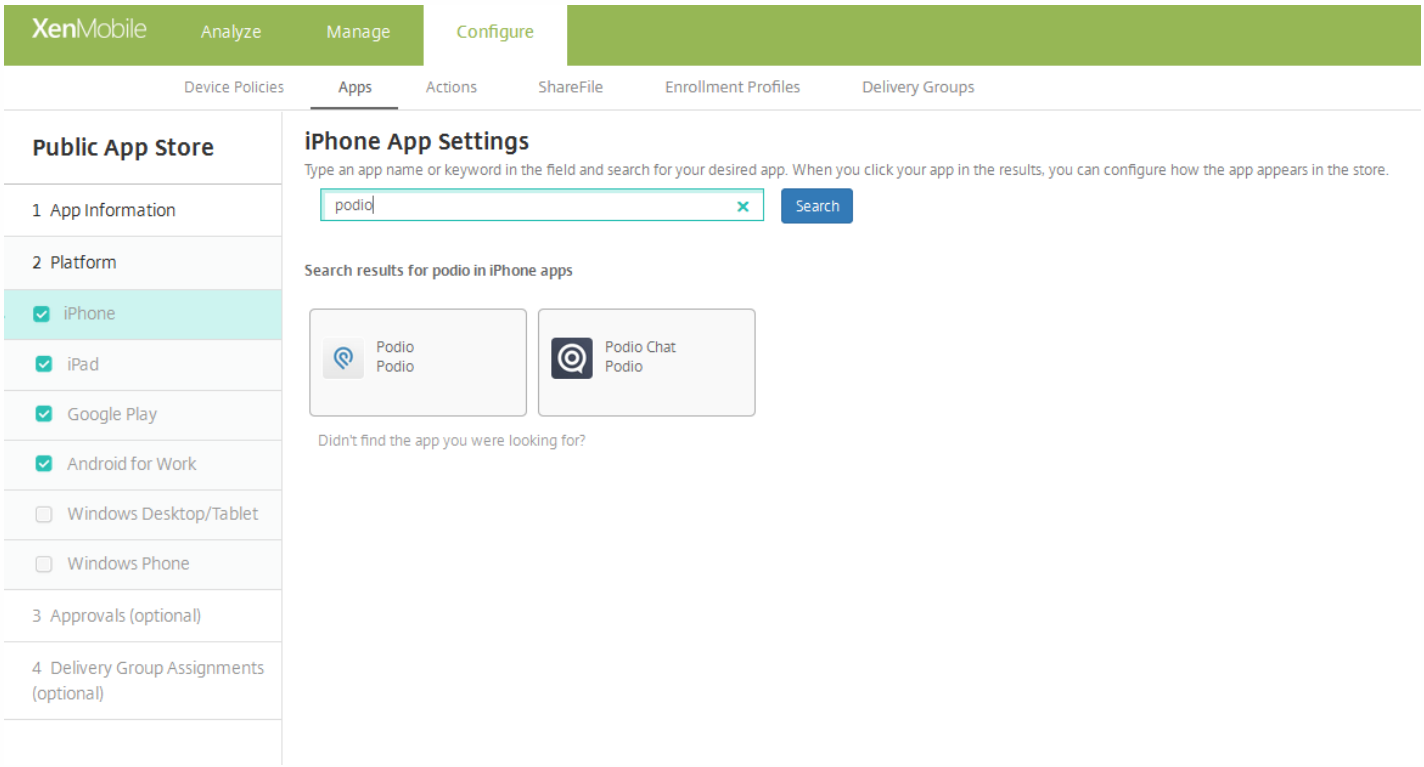
- **名前**： アプリケーションの説明的な名前を入力します。 この情報は、**[アプリ]** の表の **[アプリ名]** の下に表示されます。
- **Description**：任意で、アプリケーションの説明を入力します。
- **App category**： 任意で、一覧から、アプリを追加するカテゴリを選択します。 アプリケーションカテゴリについて詳しくは、「アプリケーションカテゴリの作成」を参照してください。

5. **[Next]** をクリックします。 **[App Platforms]** ページが開きます。

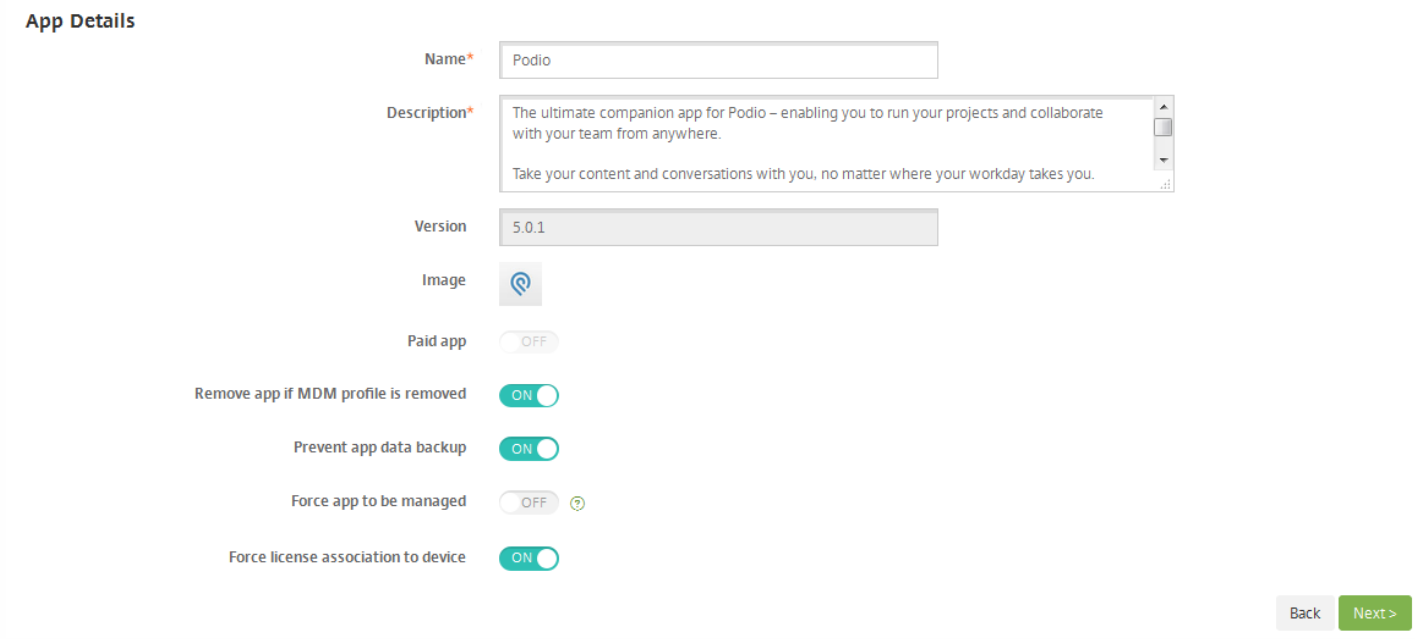
6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10を参照してプラットフォームの展開規則を設定します。

7. 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。

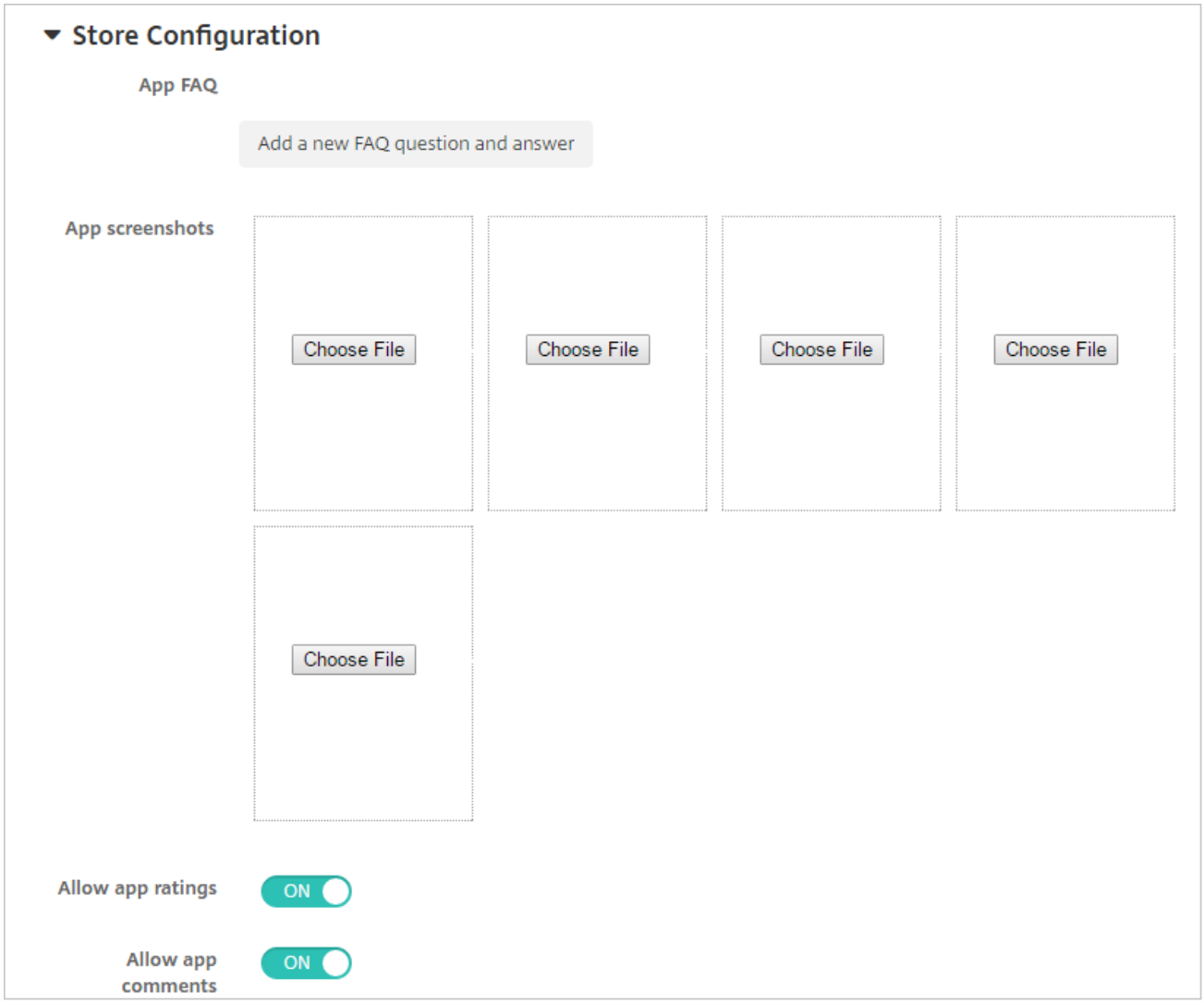


9. 次の設定を構成します。

- 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。
- **MDMプロファイルが削除されたらアプリケーションを削除します**: MDMプロファイルが削除された場合にアプリ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［**オン**］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［**オン**］です。
- **管理されるアプリケーション**：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以降で利用できます。
- **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. 展開規則を構成します。

11. ［**XenMobile Store構成**］を展開します。

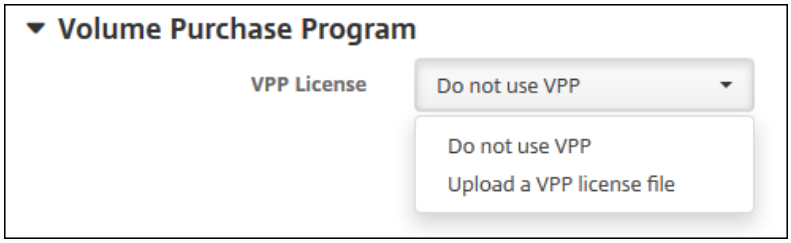


任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **アプリケーションの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。
  - **アプリケーションスクリーンショット**：アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **アプリケーション評価を許可**：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。
  - **アプリケーションコメントを許可**：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**［一括購入］**を展開します。

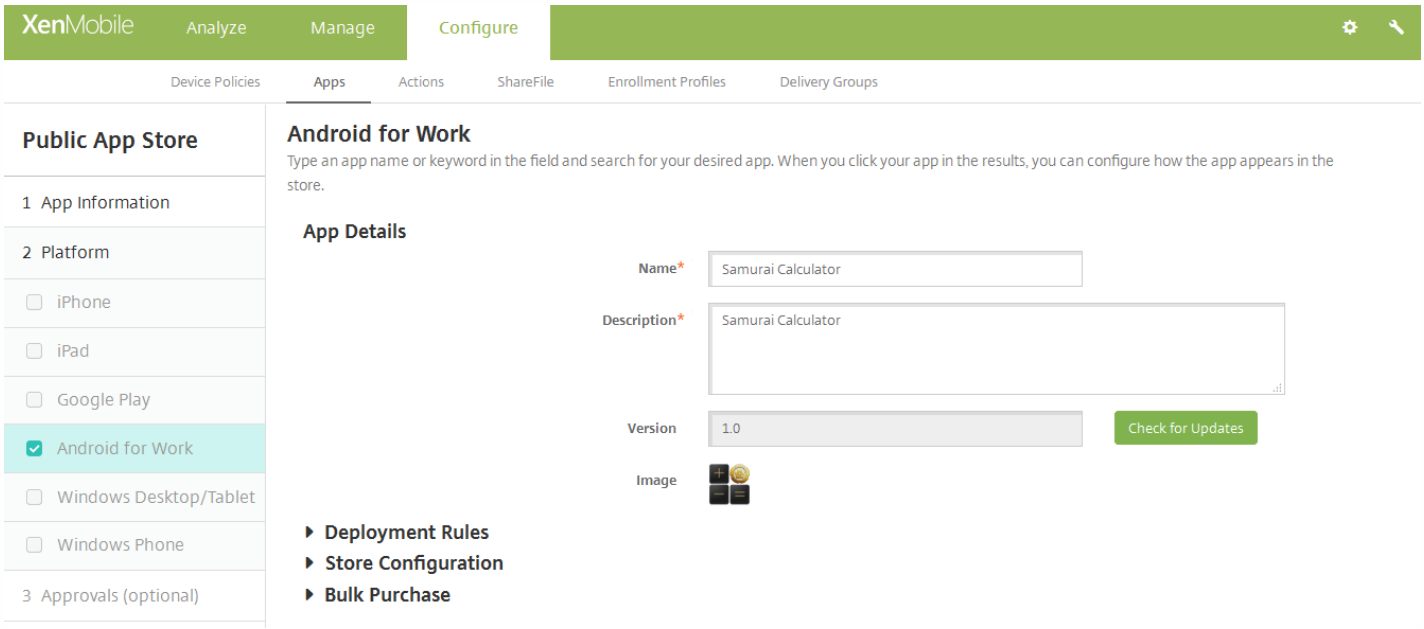
このVolume Purchase Programについて、次の手順に従います。



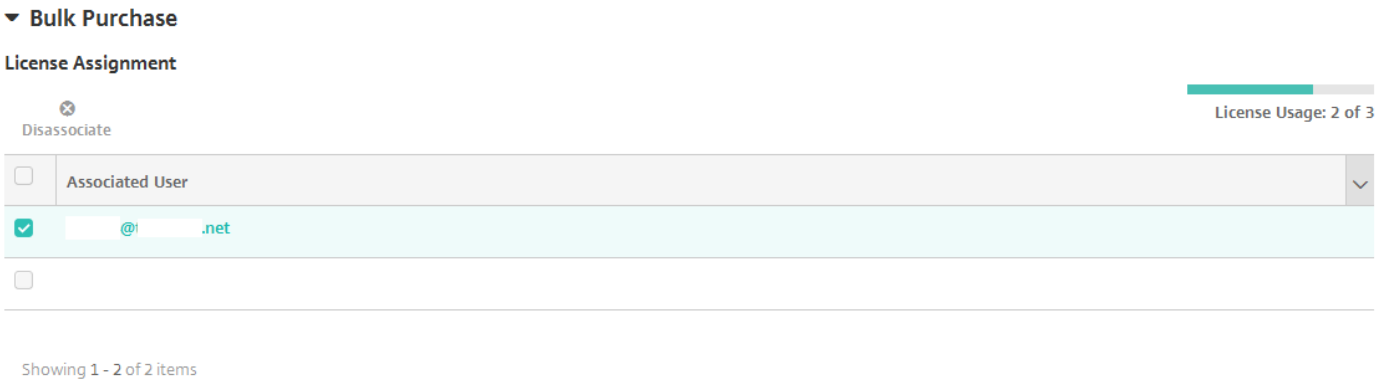
a. XenMobileでアプリケーションのVPPライセンスを適用できるようにする場合は、**[VPPライセンス]** の一覧から、 **[VPPライセンスファイルをアップロードする]** を選択します。

b. ダイアログボックスが開いたら、ライセンスをインポートします。

Android for Workの一括購入の場合は、 **[一括購入]** セクションを展開します。



［ライセンス割り当て］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 **[割り当て解除]** をクリックすると、そのユーザーへのライセンスの割り当てが終了し、別のユーザー向けにライセンスを空けることができます。ただし、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。



13. **[次へ]** をクリックします。 **[承認]** ページが開きます。

ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、次の手順に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **使用するワークフロー**：一覧から既存のワークフローを選択するか、**[新しワークフローの作成]** をクリックします。デフォルトは **[なし]** です。
- **[新しワークフローの作成]** を選択した場合は、次の設定を構成します。
  - **名前**：ワークフローの固有の名前を入力します。
  - **説明**： 任意で、ワークフローの説明を入力します。
  - **メール承認テンプレート**： 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **マネージャー承認のレベル**： 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは **[1つのレベル]** です。選択できるオプションは以下のとおりです。
    - 不必要
    - 1つのレベル
    - 2つのレベル
    - 3つのレベル
  - **Active Directoryドメインの選択**： 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **追加の必須承認者を検索**： 検索フィールドに、追加で必要なユーザーの名前を入力して、**[検索]** をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[選択した追加の必須承認者]** の一覧に表示されます。
    - **[選択した追加の必須承認者]** の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
    - **[選択した追加の必須承認者]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

14. **[次へ]** をクリックします。 **[デリバリーグループ割り当て]** ページが開きます。

15. **[デリバリーグループを選択]** の横に、アプリ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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

16. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、**[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、**[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構

成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[常時接続に対する展開]**は適用されません。

17. **[保存]**をクリックします。

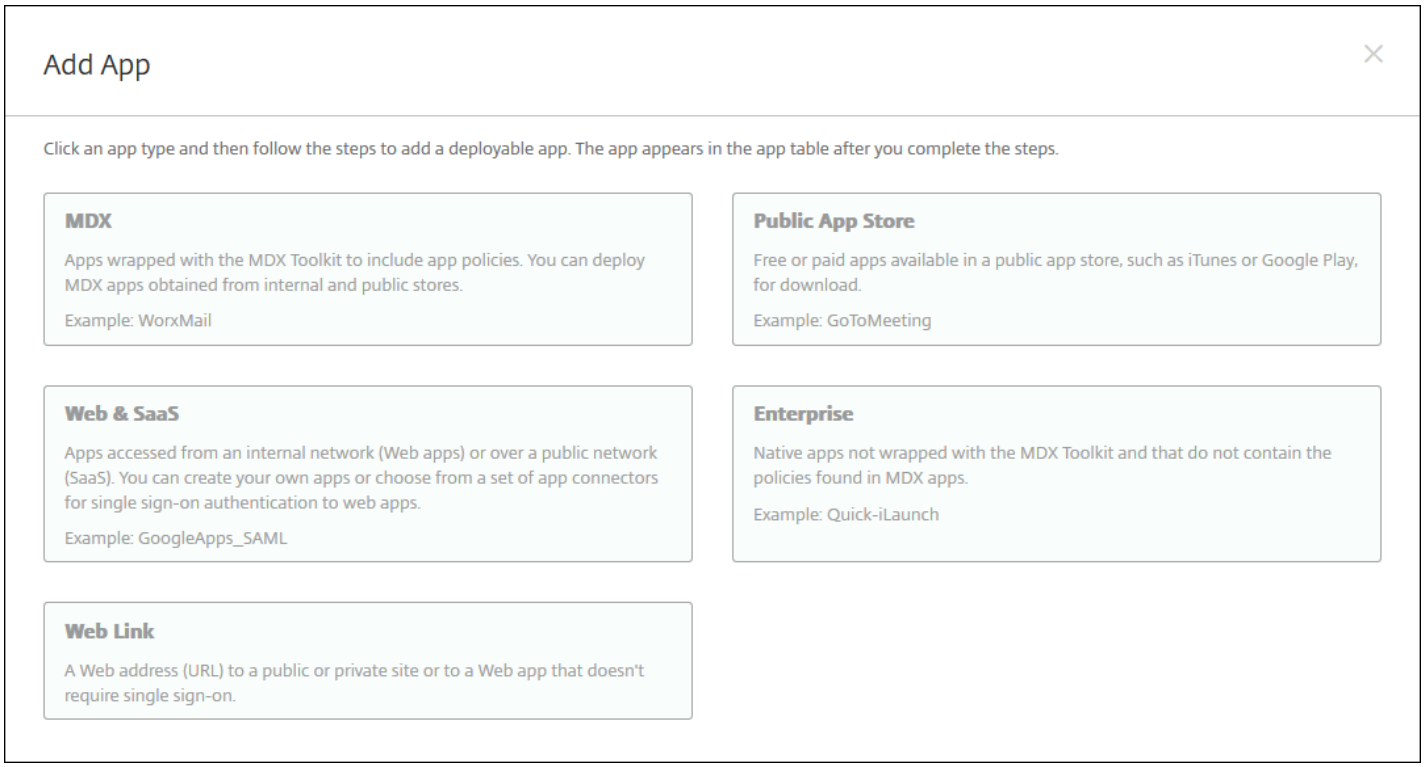
WebまたはSaaSアプリケーションの追加

XenMobileコンソールを使用して、モバイル、エンタープライズ、Web、SaaS（Software as a Service）アプリケーションへのSSO（Single Sign-On：シングルサインオン）認証をユーザーに提供できます。アプリケーションの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」を参照してください。WebアプリまたはSaaSアプリを追加すると、XenMobileで独自のコネクタを構築することもできます。

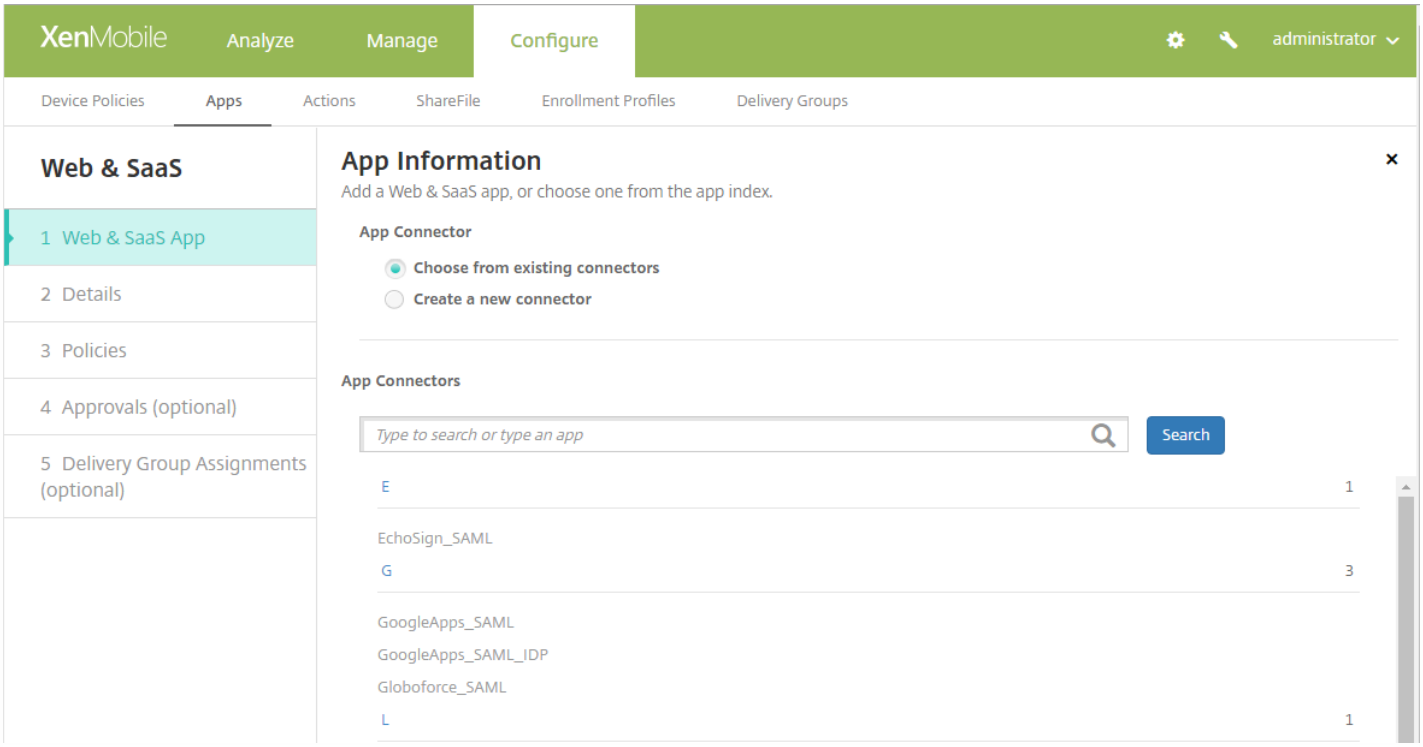
アプリケーションがSSOのみに対応している場合に、前記の設定の構成を完了してその設定を保存すると、アプリケーションがXenMobileコンソールの**[アプリ]**タブに表示されます。

1. XenMobileコンソールで、**[構成]**の**[アプリ]**をクリックします。**[アプリ]**ページが開きます。

2. **[追加]**をクリックします。**[アプリの追加]**ダイアログボックスが開きます。



3. **[WebおよびSaaS]**を選択します。**[アプリケーション情報]**ページが開きます。



4. 既存のまたは新しいアプリケーションコネクタは、以下のように構成します。

既存のアプリケーションコネクタを構成するには

[アプリケーション情報] ページで、上のように **[既存のコネクタから選択します]** が既に選択されています。 **[アプリケーションコネクタ]** 一覧で、使用するコネクタを選択します。アプリケーションコネクタの情報が表示されます。

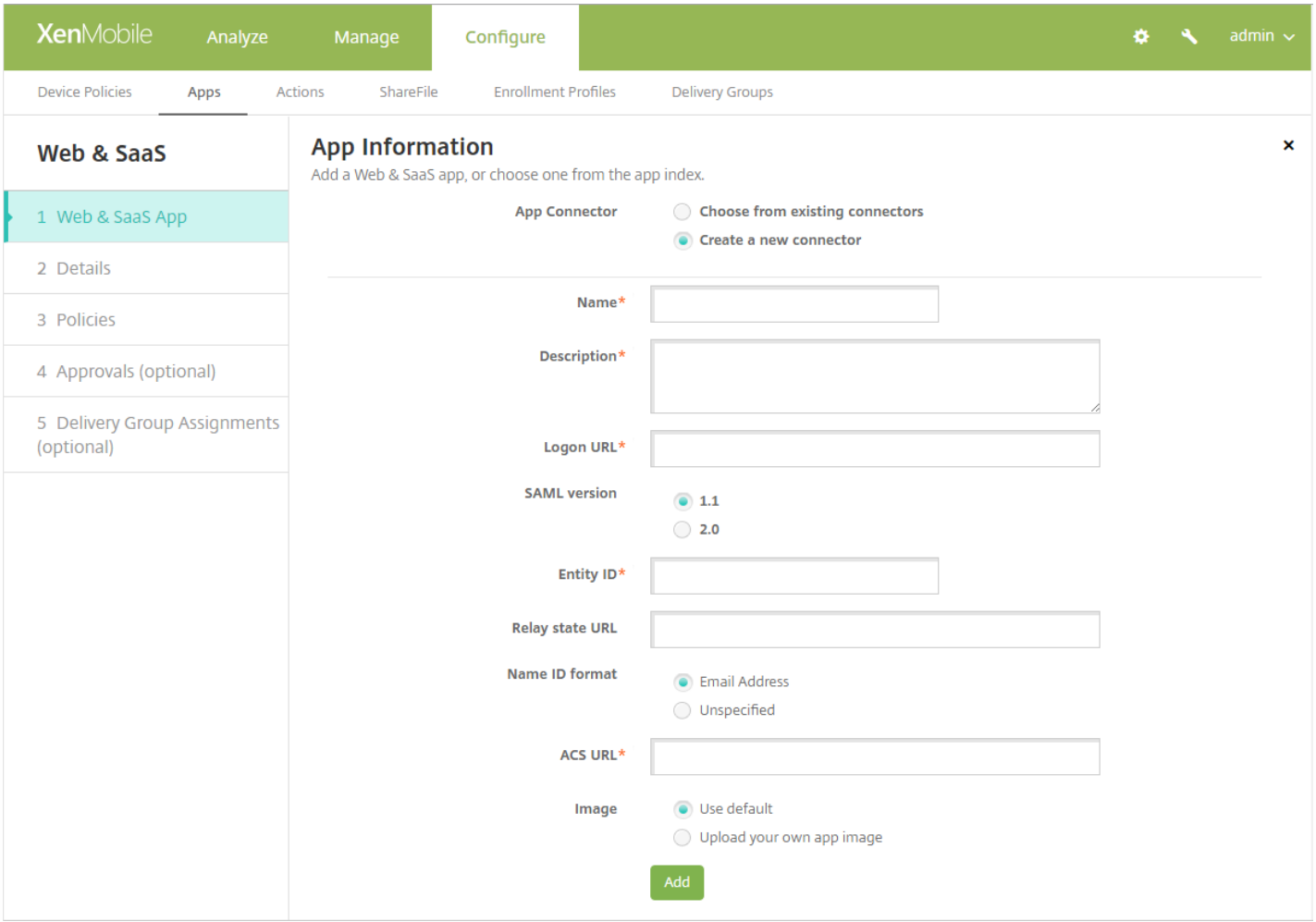
次の設定を構成します。

- **アプリ名**： 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- **アプリの説明**: 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL**： 事前に入力されているURLをそのまま使用するか、アプリケーションの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。
- **ドメイン名**：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。
- **アプリケーションは内部ネットワークでホストされます**: 内部ネットワークのサーバーでアプリ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 **[オン]** 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 **[オフ]** です。
- **アプリケーションカテゴリ**： 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。
- **ユーザーアカウントのプロビジョニング**: アプリケーションのユーザーアカウントを作成するかどうかを選択します。Globalforce_SAMLコネクタを使用している場合は、このオプションを有効にして、シームレスなSSO統合が行われるようにする必要があります。
- **[ユーザーアカウントのプロビジョニング]** を有効にした場合は、次の設定を構成します。
  - **サービスアカウント**
    - **ユーザー名**： アプリ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。
    - **パスワード**： 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。
  - **ユーザーアカウント**

- **ユーザー権利の終了時**：一覧から、ユーザーがアプリ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。選択できるオプションは以下のとおりです。
  - アカウントの無効化
  - アカウントの維持
  - アカウントを削除
- **ユーザー名規則**
  - 追加するユーザー名の規則ごとに、以下の操作を行います。
    - **ユーザー属性**： 一覧から、規則に追加するユーザー属性を選択します。
    - **長さ（文字）**： 一覧から、ユーザー名の規則で使用するユーザー属性の文字数を選択します。デフォルトは**[すべて]**です。
    - **規則**： 追加した各ユーザー属性が、ユーザー名の規則に自動的に追加されます。
- **パスワード要件**
  - **長さ**： ユーザーパスワードの最小文字数を入力します。デフォルトは**8**です。
- **パスワードの有効期限**
  - **有効期間（日）**： パスワードの有効期間（日数）を入力します。有効な値は**0**～**90**です。デフォルトは90です。
  - **有効期限が切れた後にパスワードを自動的にリセット**： 有効期限が切れたときにパスワードを自動的にリセットするかどうかを選択します。デフォルトは**[オフ]**です。このフィールドを有効にしないと、ユーザーパスワードの有効期限が切れたときにアプリケーションを開くことができなくなります。

新しいアプリケーションコネクタを構成するには

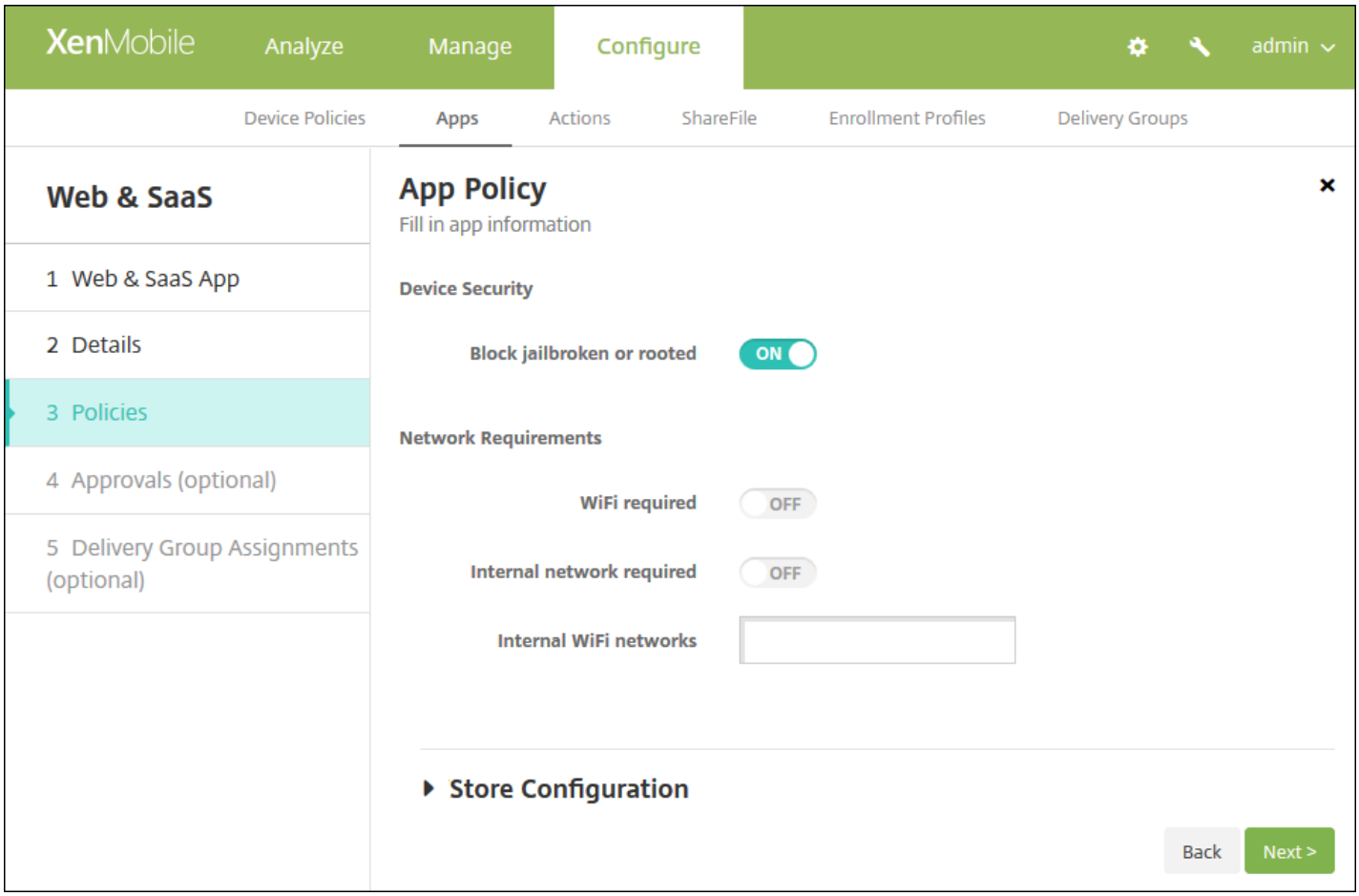
[アプリケーション情報]ページで、**[新しいコネクタの作成]**を選択します。アプリケーションコネクタのフィールドが表示されます。



次の設定を構成します。

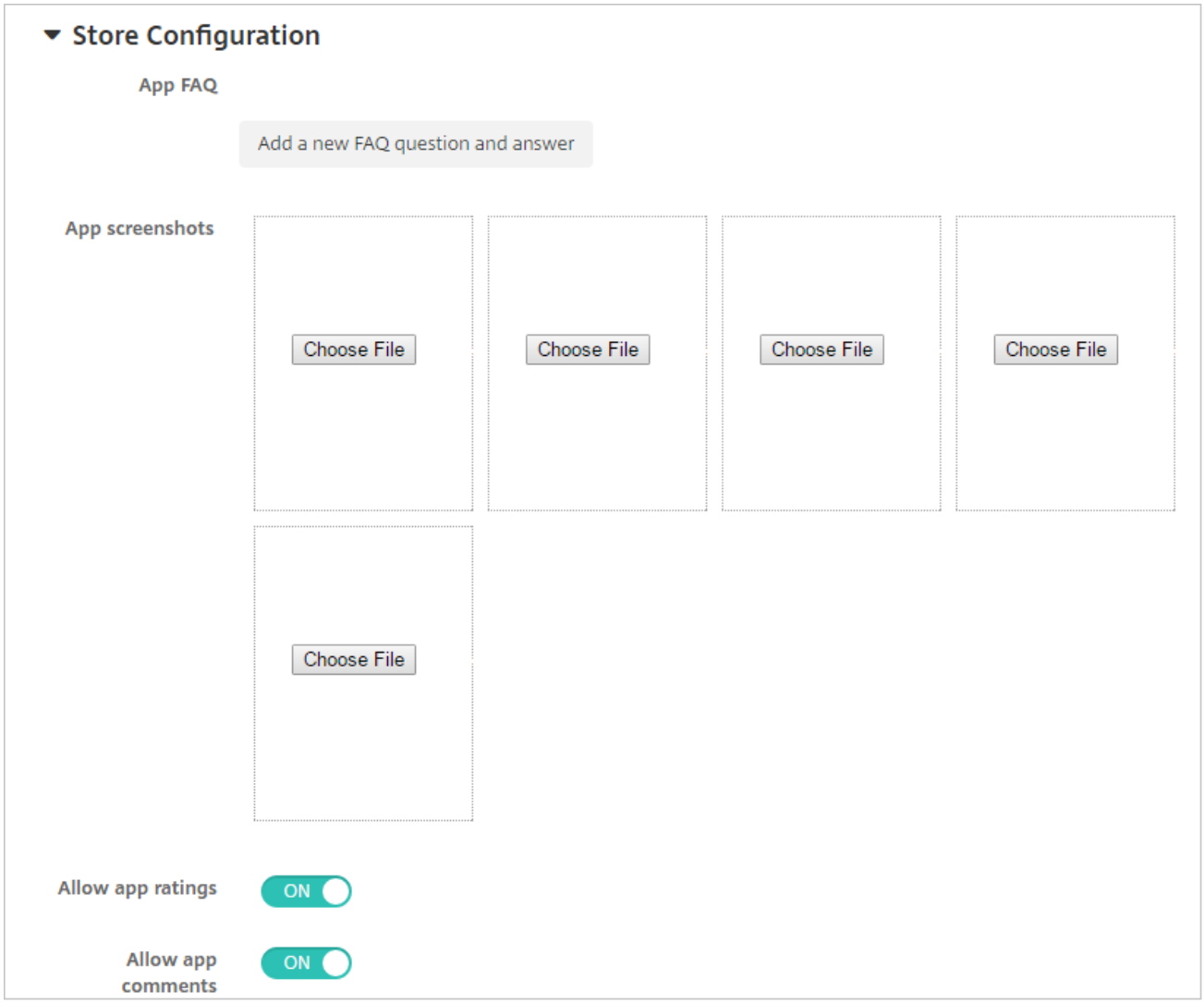
- **名前**： 接続名を入力します。このフィールドは必須です。
- **説明**： コネクタの説明を入力します。このフィールドは必須です。
- **ログオンURL**： ユーザーがサイトにログオンするときに使用するURLを入力するか、コピーして貼り付けます。たとえば、追加するアプリにログオンページがある場合、Webブラウザーを開いてアプリのログオンページに移動します。「http://www.example.com/logon」などです。このフィールドは必須です。
- **SAMLのバージョン**： **1.1**または**2.0**を選択します。デフォルトは**1.1**です。
- **エンティティID**： SAMLアプリケーションのIDを入力します。
- **リレー状態URL**： SAMLアプリケーションのWebアドレスを入力します。リレーステートURLはアプリケーションからの応答URLです。
- **名前ID形式**： **[メールアドレス]**または**[未指定]**を選択します。デフォルトは**[メールアドレス]**です。
- **ACS URL**：IDプロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービスURL（ACS URL）を入力します。ACS URLでは、ユーザーがシングルサインオン機能を使用できます。
- **イメージ**： デフォルトのCitrixイメージを使用するのか、独自のアプリ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［デフォルトを使用］です。
  - 独自のイメージをアップロードする場合は、**[参照]**をクリックしてアップロードするファイルの場所に移動し、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。
  - 完了したら、**[追加]**をクリックします。**[詳細]**ページが開きます。

5. [次へ] をクリックします。 [アプリのポリシー] ページが開きます。



- 次の設定を構成します。
  - デバイスセキュリティ
    - **ジェイルブレークまたはRoot化をブロックします**: 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 [**オン**] です。
  - ネットワーク要件
    - **WiFiが必要です**： 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。
    - **内部ネットワークが必要です**： 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 [**オフ**] です。
    - **内部WiFiネットワーク**： [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。

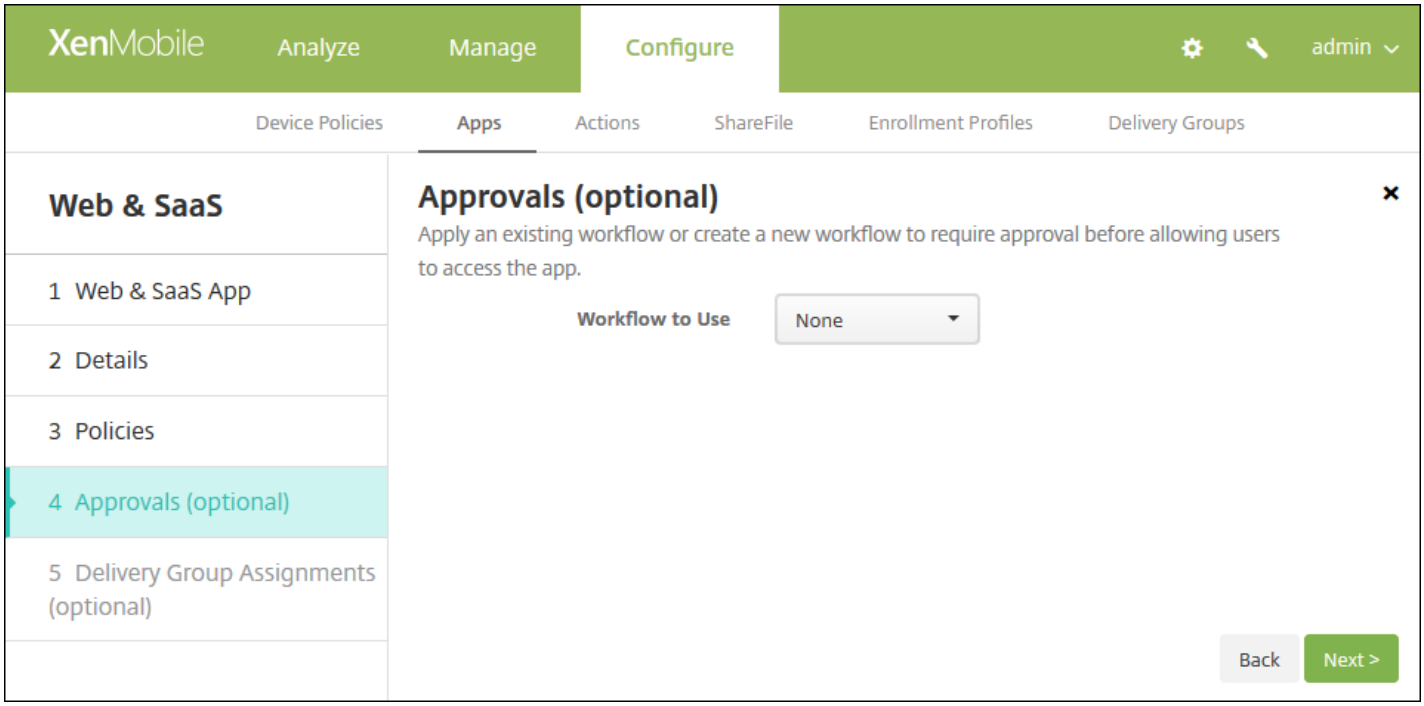
6. [**XenMobile Store構成**] を展開します。



任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリ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。
  - **アプリケーションの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。
  - **アプリケーションスクリーンショット**：アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **アプリケーション評価を許可**：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。
  - **アプリケーションコメントを許可**：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. **[次へ]** をクリックします。 **[承認]** ページが開きます。

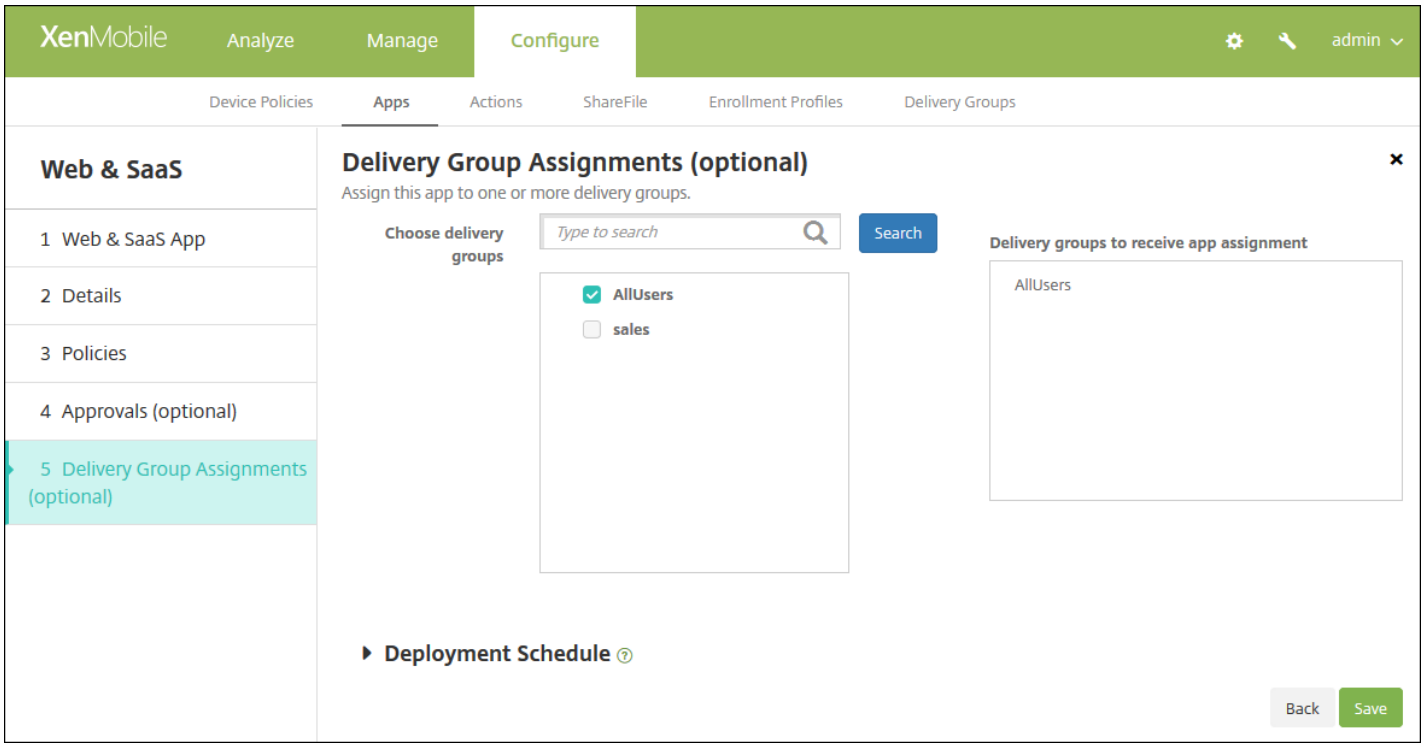


ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順8に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **使用するワークフロー**：一覧から既存のワークフローを選択するか、**[新しワークフローの作成]**をクリックします。デフォルトは**[なし]**です。
- **[新しワークフローの作成]**を選択した場合は、次の設定を構成します。
  - **名前**：ワークフローの固有の名前を入力します。
  - **説明**：任意で、ワークフローの説明を入力します。
  - **メール承認テンプレート**：一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **マネージャー承認のレベル**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは**[1つのレベル]**です。選択できるオプションは以下のとおりです。
    - 不必要
    - 1つのレベル
    - 2つのレベル
    - 3つのレベル
  - **Active Directoryドメインの選択**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **追加の必須承認者を検索**：検索フィールドに、追加で必要なユーザーの名前を入力して、**[検索]**をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが**[選択した追加の必須承認者]**の一覧に表示されます。
    - **[選択した追加の必須承認者]**の一覧からユーザーを削除するには、次のいずれかを行います。
      - **[検索]**をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して**[検索]**をクリックし、検索結果を絞り込みます。
      - **[選択した追加の必須承認者]**の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

8. **[次へ]** をクリックします。 **[デリバリーグループ割り当て]** ページが開きます。



9. **[デリバリーグループを選択]** の横に、アプリ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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

10. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** 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。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注：

- このオプションは、 **[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[常時接続に対する展開]** は適用されません。

11. **[保存]** をクリックします。

エンタープライズアプリケーションの追加

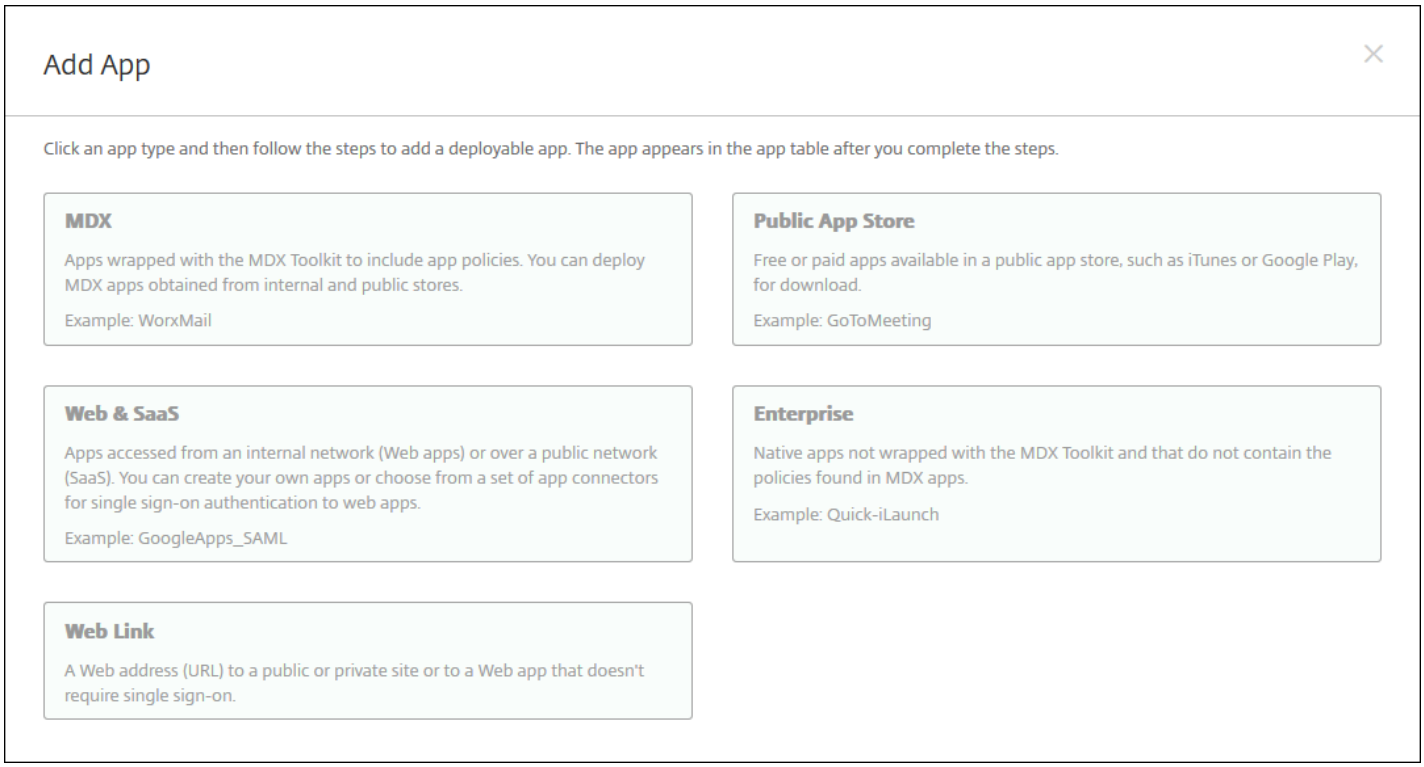
XenMobileのエンタープライズアプリケーションとは、MDX Toolkitでラップされておらず、MDXアプリケーションに関連付

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 **[アプリ]** タブで行うことができます。エンタープライズアプリケーションは、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。

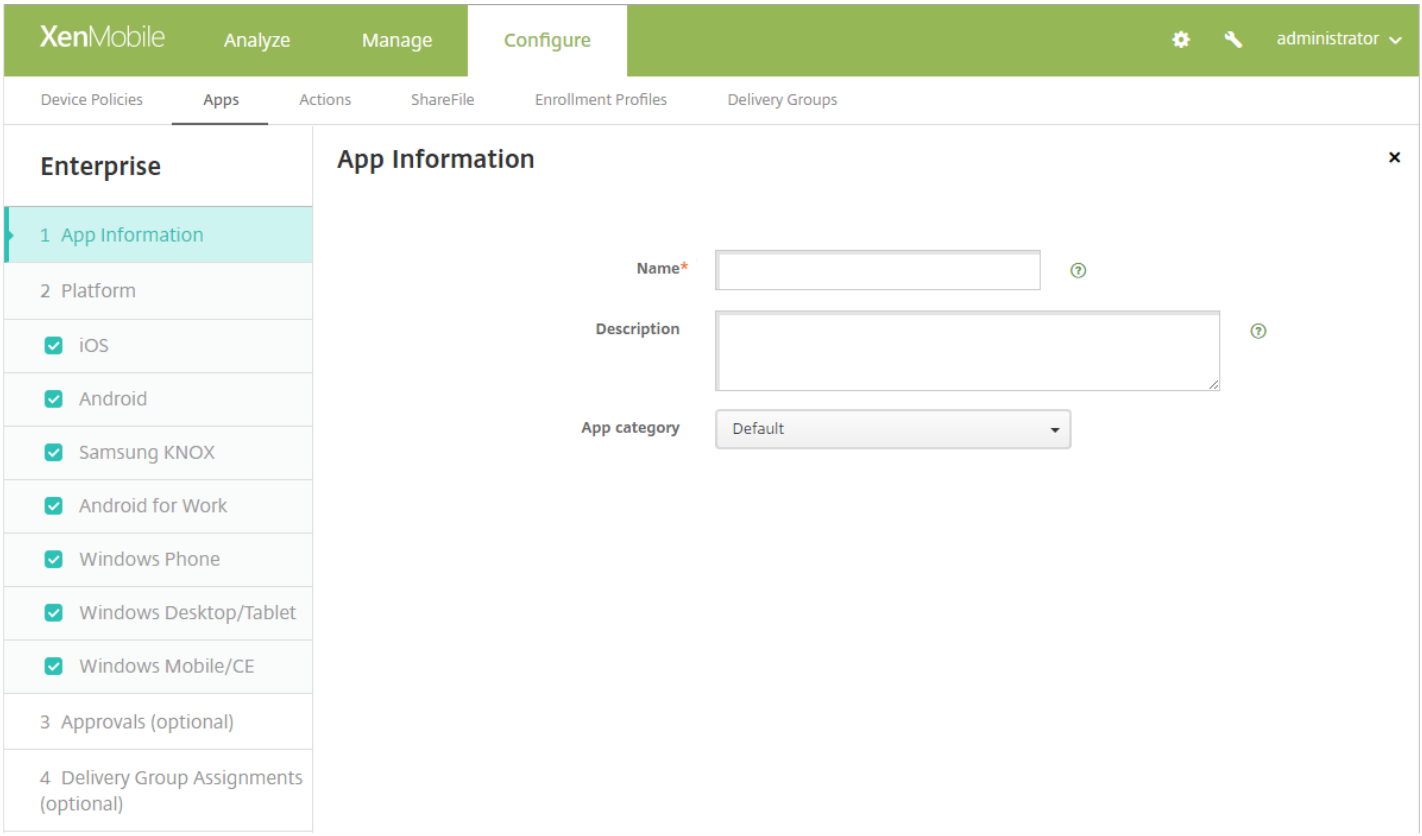
- iOS（.ipaファイル）
- Android（.apkファイル）
- Samsung KNOX（.apkファイル）
- Android for Work（.apkファイル）
- Windows Phone（.xapまたは.appxファイル）
- Windowsタブレット（.appxファイル）
- Windows Mobile/CE（.cabファイル）

1. XenMobileコンソールで、 **[構成]** の **[アプリ]** をクリックします。 **[アプリ]** ページが開きます。

2. **[追加]** をクリックします。 **[アプリの追加]** ダイアログボックスが開きます。



3. **[エンタープライズ]** をクリックします。 **[アプリケーション情報]** 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。

- **名前**： 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、［アプリ］の表の［アプリ名］の下に表示されます。
- **説明**： 任意で、アプリケーションの説明を入力します。
- **アプリケーションカテゴリ**： 任意で、一覧から、アプリを追加するカテゴリを選択します。 アプリ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. **[次へ]** をクリックします。**アプリのプラットフォーム**ページが開きます。

6. **[プラットフォーム]** で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、**[参照]** をクリックしてアップロードするファイルの場所に移動し、そのファイルを選択します。

8. **[次へ]** をクリックします。プラットフォームのアプリケーション情報ページが開きます。

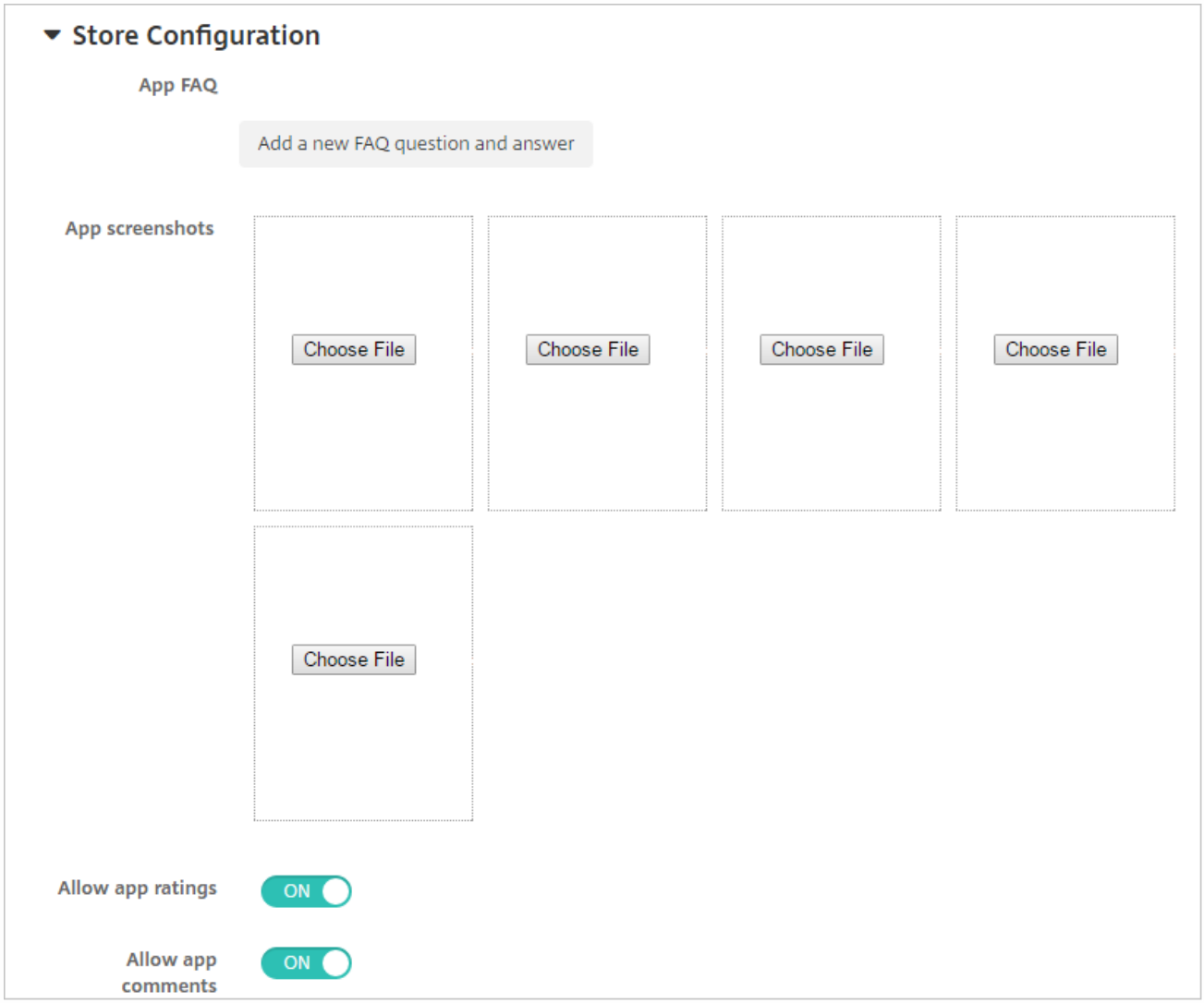
9. プラットフォームの種類について、以下の設定を構成します。

- **ファイル名**： 任意で、アプリケーションの名前を新たに入力します。
- **アプリの説明**：任意で、アプリケーションの説明を新たに入力します。
- **アプリのバージョン**： このフィールドは変更できません。
- **最小OSバージョン**：任意で、アプリ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。

- **最大OSバージョン**： 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。
- **除外するデバイス**：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。
- **MDMプロファイルが削除されたらアプリケーションを削除します**: MDMプロファイルが削除された場合にデバイスからアプリ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。
- **アプリケーションデータのバックアップを阻止します**: 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［**オン**］です。
- **管理されるアプリケーション**：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。この設定は、iOS 9.xデバイスに適用されます。

10. 展開規則を構成します。

11. ［**XenMobile Store構成**］を展開します。

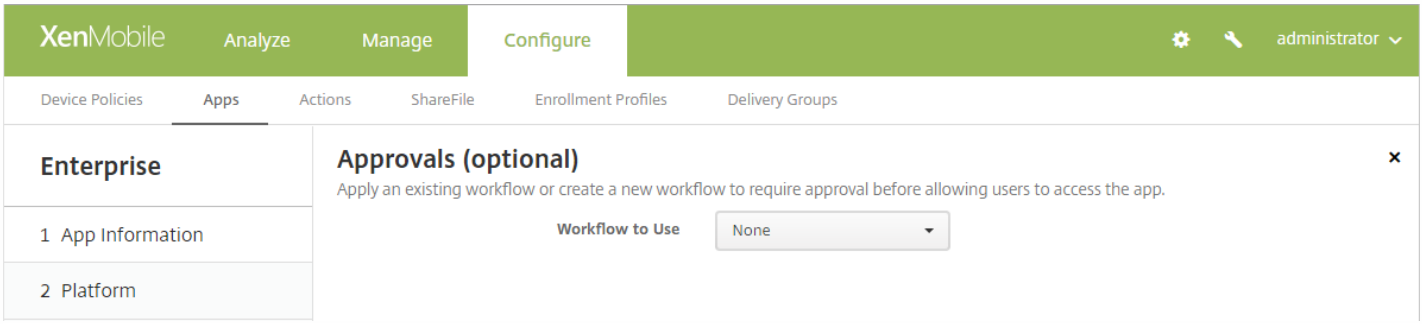


任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **アプリケーションの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。

- **アプリケーションスクリーンショット**：アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
- **アプリケーション評価を許可**：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［**オン**］です。
- **アプリケーションコメントを許可**：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［**オン**］です。

12. ［**次へ**］をクリックします。［**承認**］ページが開きます。

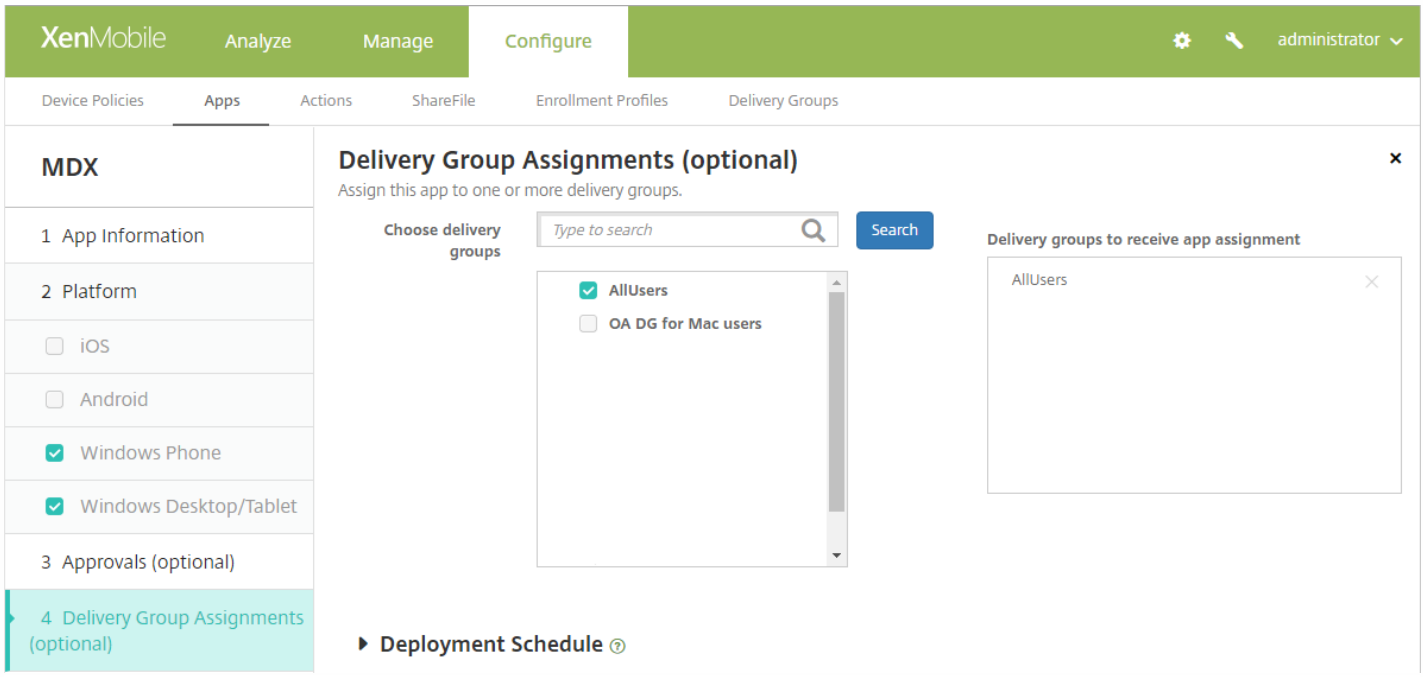


ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順13に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **使用するワークフロー**：一覧から既存のワークフローを選択するか、［**新しいワークフローの作成**］をクリックします。デフォルトは［**なし**］です。
- ［**新しいワークフローの作成**］を選択した場合は、次の設定を構成します。
  - **名前**：ワークフローの固有の名前を入力します。
  - **説明**：任意で、ワークフローの説明を入力します。
  - **メール承認テンプレート**：一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **マネージャー承認のレベル**：一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［**1つのレベル**］です。選択できるオプションは以下のとおりです。
    - 不必要
    - 1つのレベル
    - 2つのレベル
    - 3つのレベル
  - **Active Directoryドメインの選択**：一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **追加の必須承認者を検索**：検索フィールドに、追加で必要なユーザーの名前を入力して、［**検索**］をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが［**選択した追加の必須承認者**］の一覧に表示されます。
    - ［**選択した追加の必須承認者**］の一覧からユーザーを削除するには、次のいずれかを行います。
      - ［**検索**］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して［**検索**］をクリックし、検索結果を絞り込みます。
      - ［**選択した追加の必須承認者**］の一覧に含まれるユーザーは、検索結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

13. [次へ] をクリックします。 [デリバリーグループ割り当て] ページが開きます。



14. [デリバリーグループを選択] の横に、アプリ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 [アプリ割り当てを受信するためのデリバリーグループ] 一覧に表示されます。

15. [展開スケジュール] を展開して以下の設定を構成します。

- [展開] の横の [オン] をクリックすると展開がスケジュールされ、 [オフ] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。 [オフ] 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。
- [展開スケジュール] の横の [すぐに] または [あとで] をクリックします。デフォルトのオプションは [すぐに] です。
- [あとで] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [展開状態] の横の [接続するたび] をクリックするか、 [以前の展開が失敗した場合のみ] をクリックします。デフォルトのオプションは、 [接続するたび] です。
- [常時接続に対する展開] の横の [オン] または [オフ] をクリックします。デフォルトのオプションは [オフ] です。

注：

- このオプションは、 [設定] の [サーバープロパティ] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 [常時接続に対する展開] は適用されません。

16. [保存] をクリックします。

Webリンクの追加

XenMobileで、パブリックサイトやプライベートサイト、またはシングルサインオン（SSO）を必要としないWebアプリケーションのWebアドレス（URL）を設置できます。

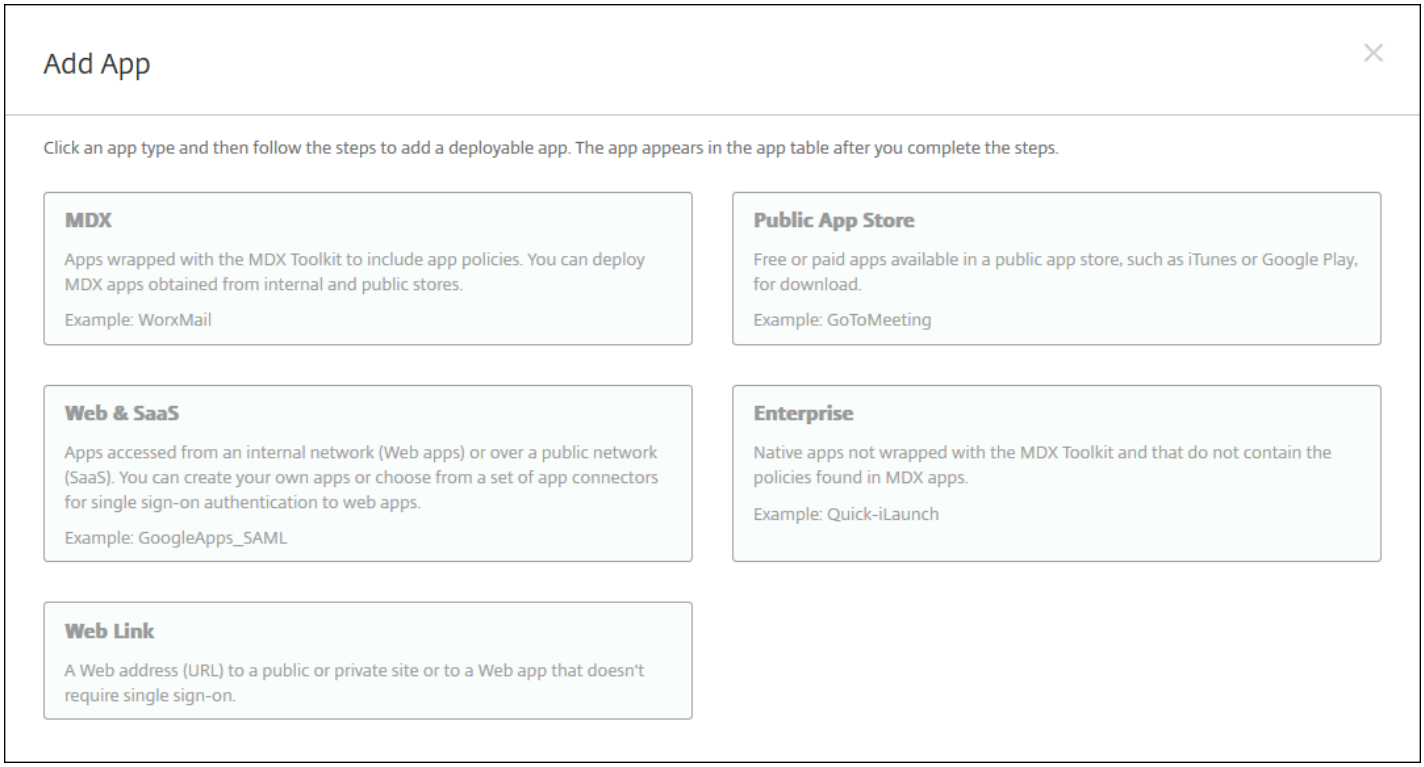
Webリンクの構成は、XenMobileコンソールの［アプリ］タブで行うことができます。Webリンクの構成が完了すると、リンクは［アプリ］の表の一覧にリンクアイコンとして表示されます。ユーザーがSecure Hubを使ってログオンすると、リンクに使用可能なアプリケーションおよびデスクトップの一覧と共に表示されます。

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、［構成］の［アプリ］をクリックします。［アプリ］ページが開きます。

2. ［追加］をクリックします。［アプリの追加］ダイアログボックスが開きます。



3. ［Webリンク］をクリックします。［アプリケーション情報］ページが開きます。

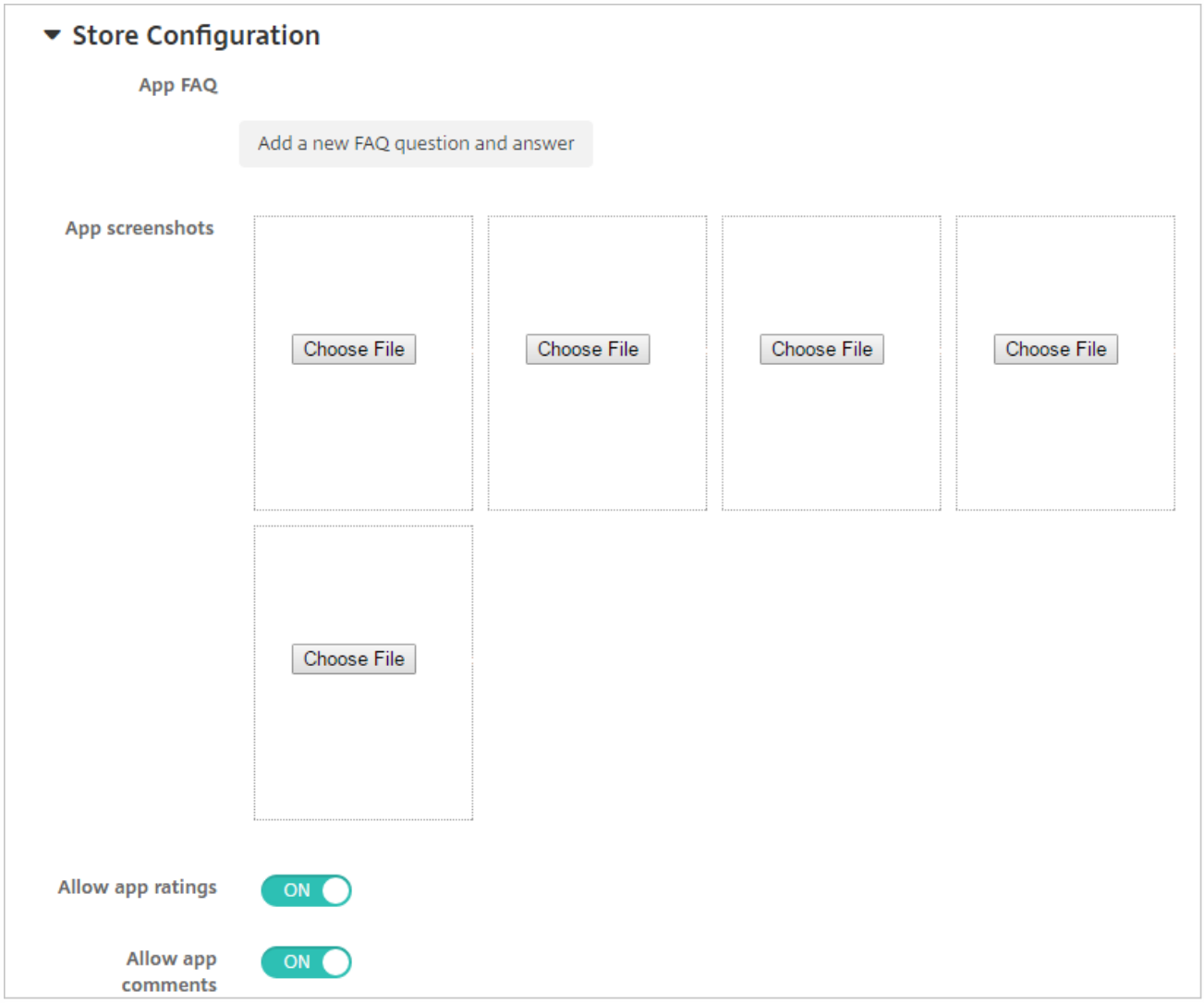
4. 次の設定を構成します。

- **アプリ名**： 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- **アプリの説明**: 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL**： 事前に入力されているURLをそのまま使用するか、アプリケーションの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。
- **アプリケーションは内部ネットワークでホストされます**: 内部ネットワークのサーバーでアプリ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［**オン**］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［**オフ**］です。

- **アプリケーションカテゴリ**： 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。
- **イメージ**： デフォルトのCitrixイメージを使用するのか、独自のアプリ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［デフォルトを使用］です。
  - 独自のイメージをアップロードする場合は、［**参照**］をクリックしてアップロードするファイルの場所に移動し、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. ［**XenMobile Store構成**］を展開します。



任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリ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。
  - **アプリケーションの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。
  - **アプリケーションスクリーンショット**：アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。

- **アプリケーション評価を許可**：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［**オン**］です。
- **アプリケーションコメントを許可**：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［**オン**］です。

6. ［**次へ**］をクリックします。［**デリバリーグループ割り当て**］ページが開きます。

7. ［**デリバリーグループを選択**］の横に、アプリ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［**アプリ割り当てを受信するためのデリバリーグループ**］一覧に表示されます。

8. ［**展開スケジュール**］を展開して以下の設定を構成します。

- ［**展開**］の横の［**オン**］をクリックすると展開がスケジュールされ、［**オフ**］をクリックすると展開が行われません。デフォルトのオプションは［**オン**］です。［**オフ**］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。
- ［**展開スケジュール**］の横の［**すぐに**］または［**あとで**］をクリックします。デフォルトのオプションは［**すぐに**］です。
- ［**あとで**］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- ［**展開状態**］の横の［**接続するたび**］をクリックするか、［**以前の展開が失敗した場合のみ**］をクリックします。デフォルトのオプションは、［**接続するたび**］です。
- ［**常時接続に対する展開**］の横の［**オン**］または［**オフ**］をクリックします。デフォルトのオプションは［**オフ**］です。

注：

- このオプションは、［**設定**］の［**サーバープロパティ**］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［**常時接続に対する展開**］は適用されません。

9. ［**保存**］をクリックします。

Microsoft 365アプリの有効化

MDXコンテナを開いて、Secure Mail、Secure Web、およびShareFileがMicrosoft Office 365アプリにドキュメントやデータを転送するようにできます。詳しくは、「Office 365アプリとのセキュアな対話式操作の許可」を参照してください。

ワークフローの作成および管理

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

XenMobileを初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

XenMobileの次の2つの方法でワークフローを構成できます。

- XenMobileコンソールの［ワークフロー］ページ。［ワークフロー］ページでは、アプリケーションの構成で使用する複数

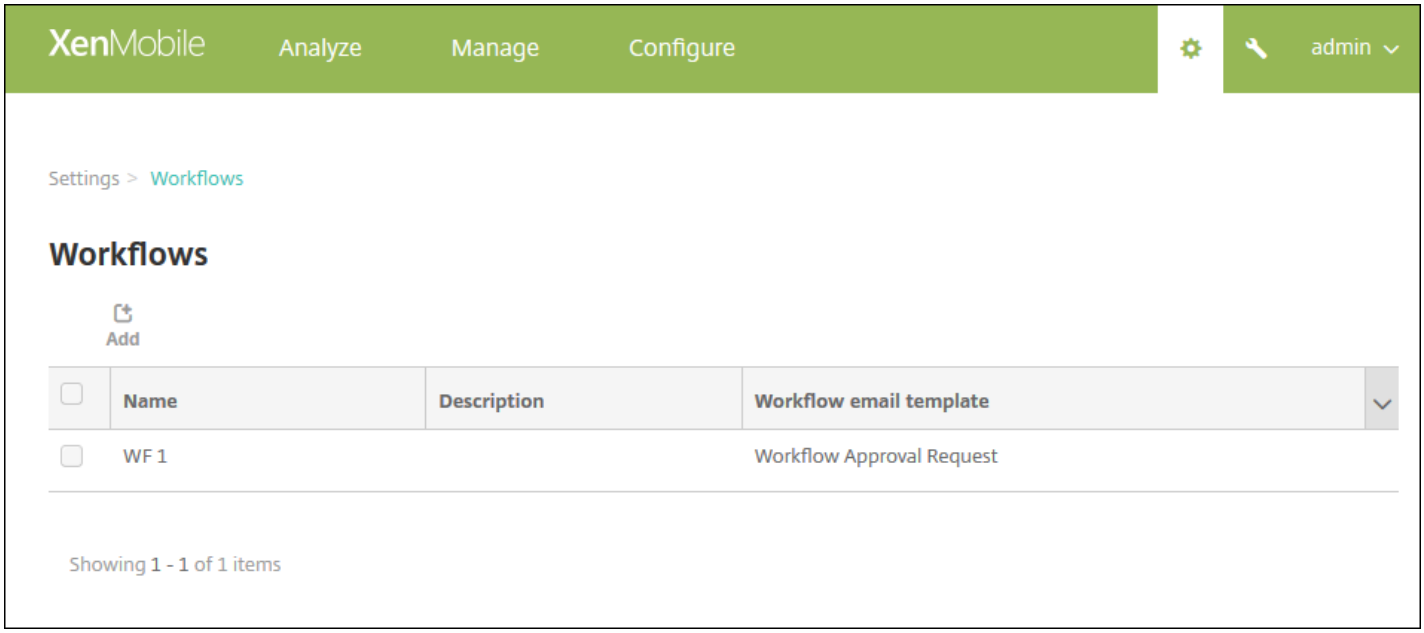
のワークフローを構成できます。［ワークフロー］ページでワークフローを構成するとき、アプリケーションを構成するときのワークフローを選択できます。

- 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。

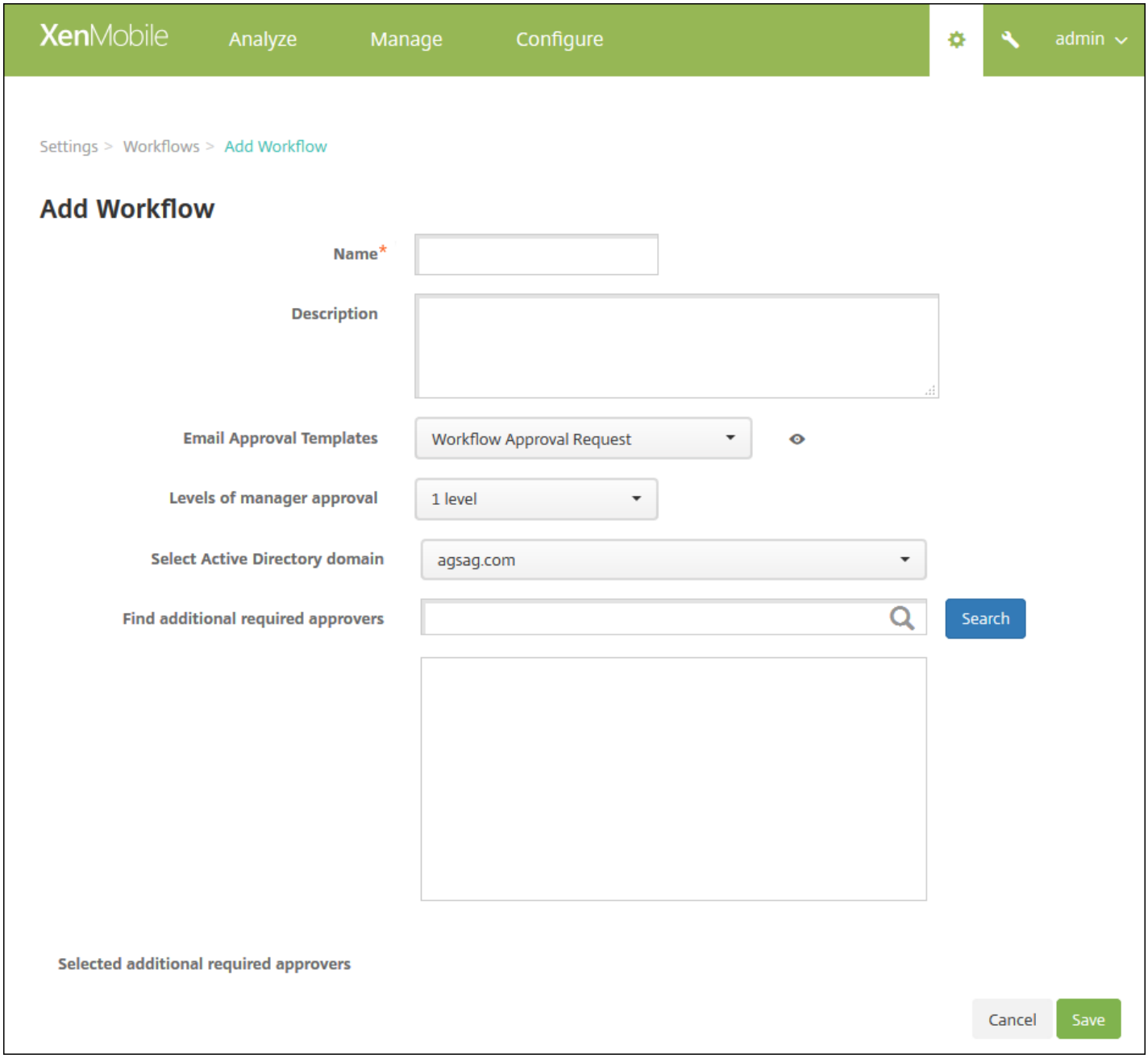
ユーザーアカウントの管理者承認を最大3レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、ユーザーの名前またはメールアドレスを使用して追加のユーザーを検索し選択することができます。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

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

2. **[ワークフロー]** をクリックします。**[ワークフロー]** ページが開きます。

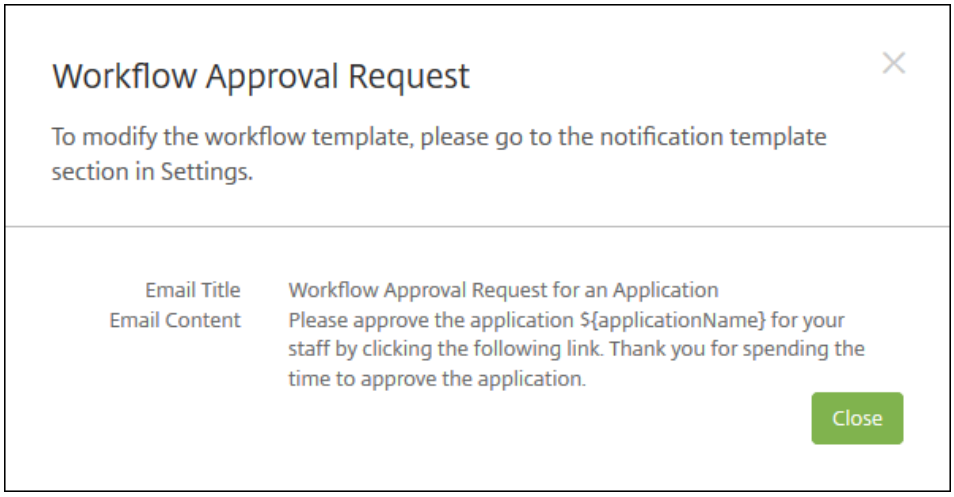


3. **[追加]** をクリックします。**[ワークフローの追加]** ページが開きます。



4. 次の設定を構成します。

- **名前**： ワークフローの固有の名前を入力します。
- **説明**： 任意で、ワークフローの説明を入力します。
- **メール承認テンプレート**： 一覧から、割り当てる電子メール承認テンプレートを選択します。電子メールテンプレートの作成は、XenMobileコンソールの［設定］の［通知テンプレート］セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、以下のダイアログボックスが表示されます。



- **マネージャー承認のレベル**： 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［1つのレベル］です。選択できるオプションは以下のとおりです。
  - 不必要
  - 1つのレベル
  - 2つのレベル
  - 3つのレベル
- **Active Directoryドメインの選択**： 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
- **追加の必須承認者を検索**： 検索フィールドに、追加で必要なユーザーの名前を入力して、［検索］をクリックします。名前はActive Directoryで取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが**［選択した追加の必須承認者］**の一覧に表示されます。
  - **［選択した追加の必須承認者］**の一覧からユーザーを削除するには、次のいずれかを行います。
    - **［検索］**をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して**［検索］**をクリックし、検索結果を絞り込みます。
    - **［選択した追加の必須承認者］**の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

5. **［保存］**をクリックします。作成したワークフローが**［ワークフロー］**ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリ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. **［ワークフロー］**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、**［削除］**をクリックします。確認ダイアログボックスが開きます。もう一度**［削除］**をクリックします。

重要：この操作を元に戻すことはできません。

アプリコネクタの種類

Feb 27, 2017

次の表に、WebアプリまたはSaaSアプリを追加する場合にXenMobile内で使用できるコネクタとコネクタの種類を示します。 WebまたはSaaSアプリを追加すると、新しいコネクタを追加することもできます。

この表は、各コネクタがユーザーアカウント管理をサポートするかどうかについて示します。ユーザーアカウント管理がサポートされる場合、管理者は新しいアカウントを自動的に作成したり、ワークフローを使って作成したりできます。

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
EchoSign_SAML	はい	はい
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	はい	はい
GoogleApps_SAML_IDP	はい	はい
Lynda_SAML	はい	はい
Office365_SAML	はい	はい
Salesforce_SAML	はい	はい
Salesforce_SAML_SP	はい	はい
SandBox_SAML	はい	
SuccessFactors_SAML	はい	
ShareFile_SAML	はい	
ShareFile_SAML_SP	はい	
WebEx_SAML_SP	はい	はい

MDXまたはエンタープライズアプリケーションのアップグレード

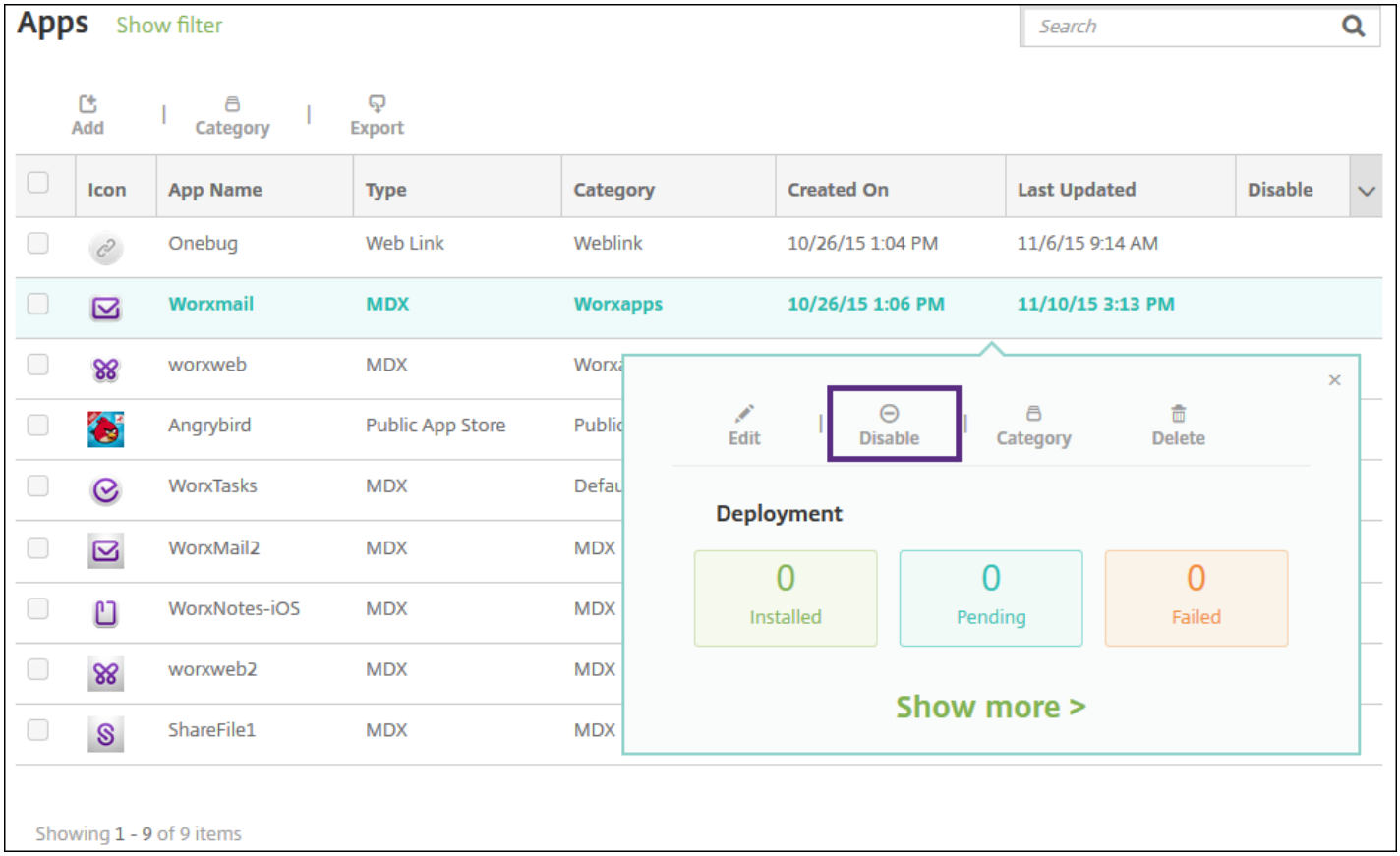
Feb 27, 2017

XenMobileでMDXまたはエンタープライズアプリケーションをアップグレードするには、XenMobileコンソールでアプリケーションを無効にしてから、アプリケーションの新しいバージョンをアップロードします。

1. XenMobileコンソールで、**[構成] > [アプリ]** の順にクリックします。**[アプリ]** ページが開きます。

2. 管理対象デバイス（モバイルデバイス管理でXenMobileに登録されたデバイス）の場合は、スキップして手順3に進みます。非管理対象デバイス（エンタープライズアプリケーション管理の目的のみでXenMobileに登録されたデバイス）の場合は、次の手順に従います。

- **[アプリ]** の表で、アプリ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、**[無効化]** をクリックします。



- 確認のダイアログボックスで **[無効化]** をクリックします。アプリケーションの **[無効化]** 列に「*無効*」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。

3. **[アプリ]** 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。

4. 表示されるメニューで、 **[編集]** 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、 **[アプリケーション情報]** ページが開きます。

5. 次の設定を構成します。

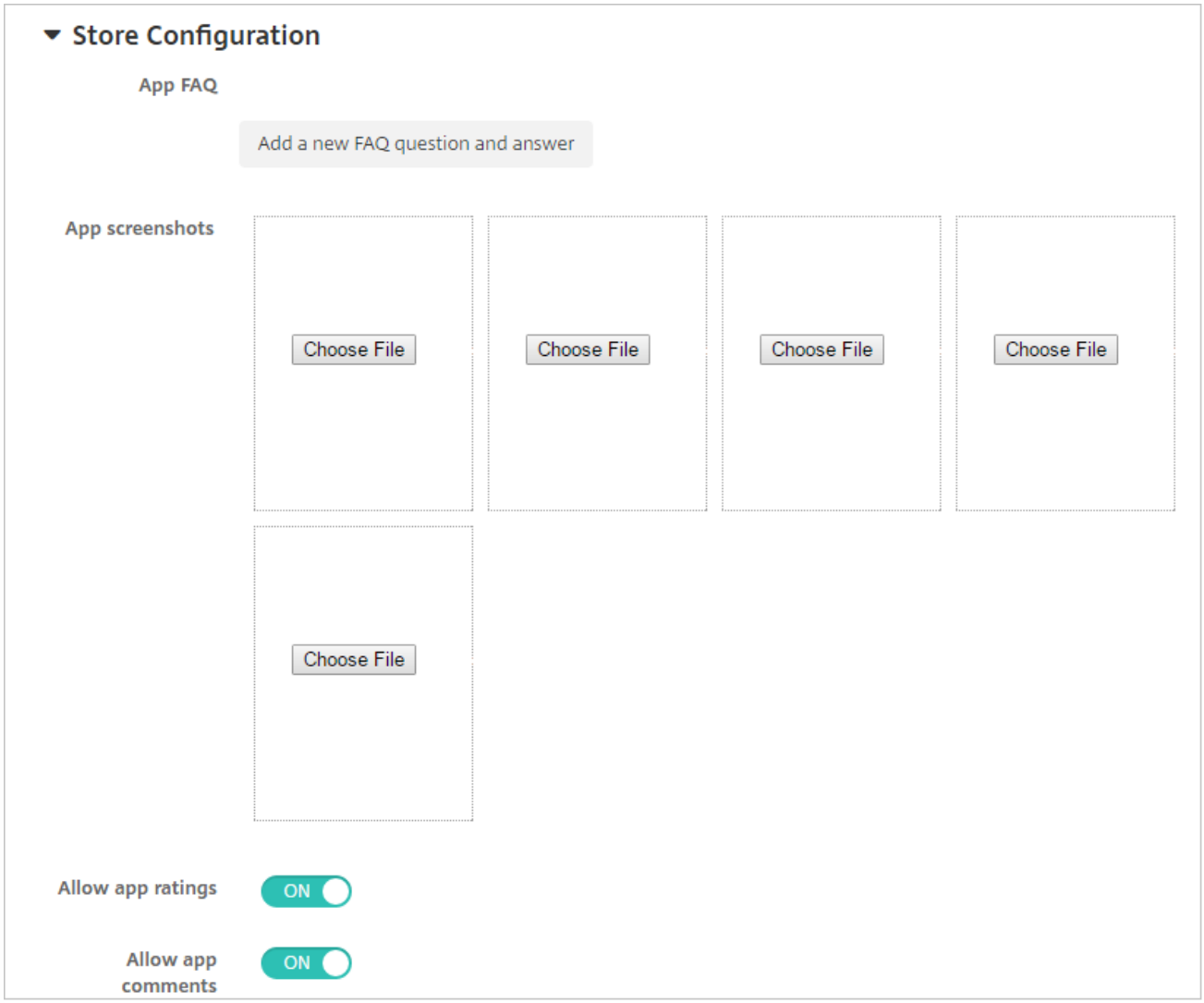
- **Name**： 任意で、アプリケーション名を変更します。
- **Description**： 任意で、アプリケーションの説明を変更します。
- **App category**： 任意で、アプリケーションのカテゴリを変更します。

6. **[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。

- **[アップロード]** をクリックしてアップロードするファイルの場所に移動し、置き換えるファイルを選択します。アプリケーションがXenMobileにアップロードされます。
- 任意で、プラットフォームのアプリ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XenMobile Storeの構成（手順8を参照）を行います。

7. 展開規則を構成します。

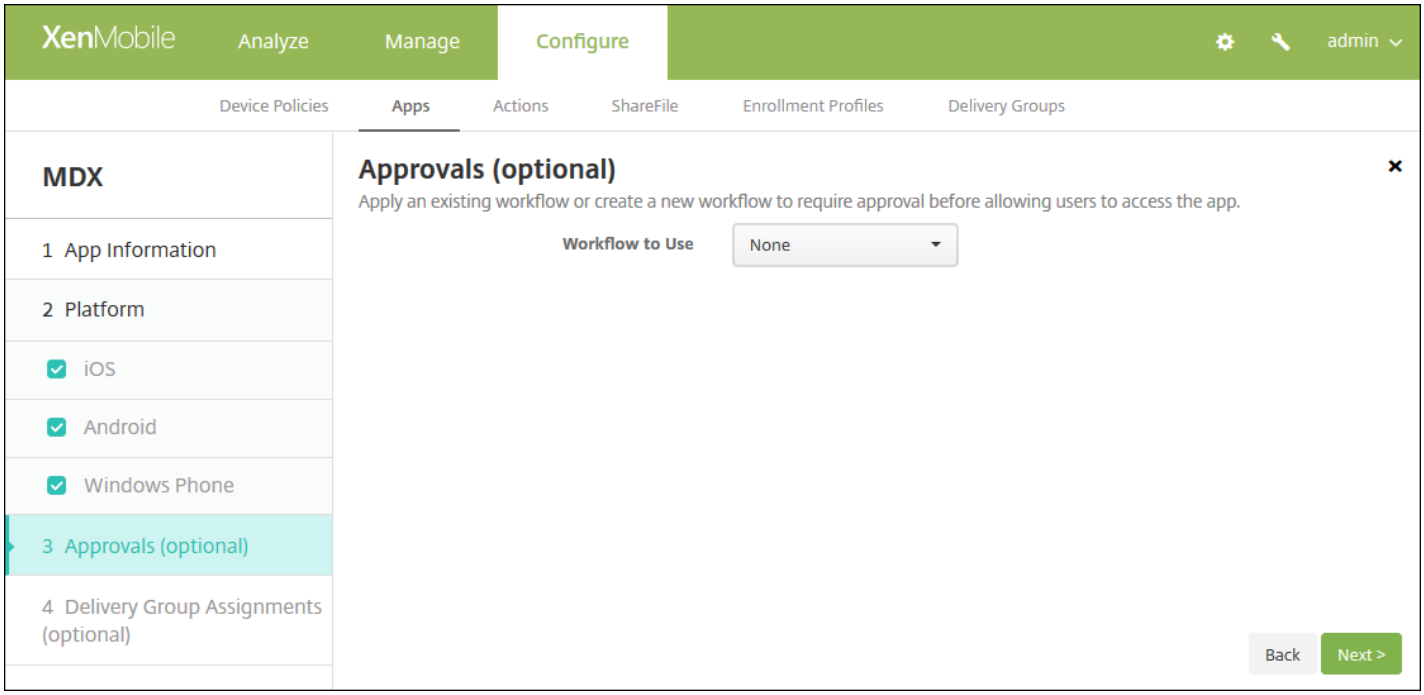
8. **[Store Configuration]** を展開します。



任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリ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XenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **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。

9. **[次へ]** をクリックします。 **[承認]** ページが開きます。



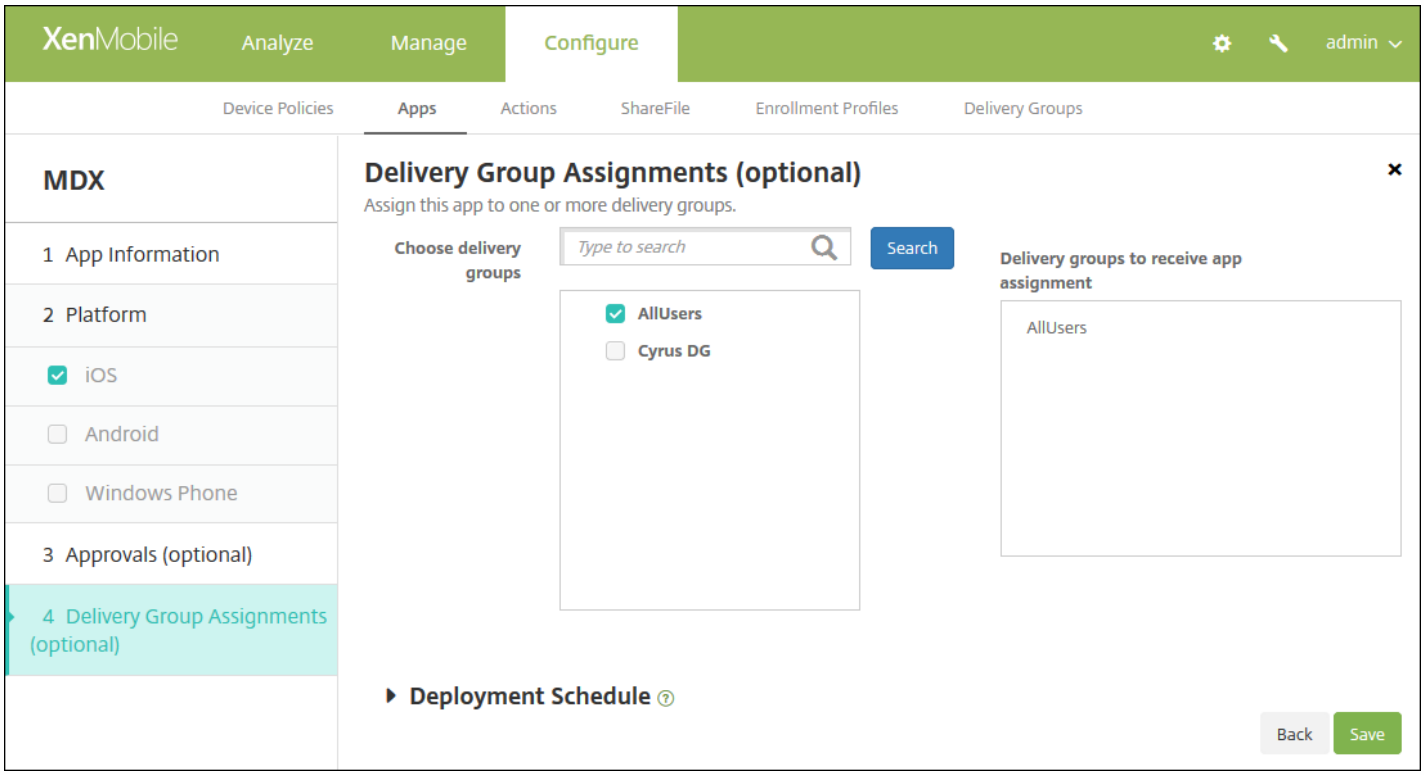
10. ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順11に進みます。

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。
  - **メール承認テンプレート**： 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **マネージャー承認のレベル**： 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは［**1つのレベル**］です。 選択できるオプションは以下のとおりです。
    - 不必要
    - 1 level
    - 2 levels
    - 3 levels
  - **Active Directoryドメインの選択**： 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **追加の必須承認者を検索**： 検索フィールドに、追加で必要なユーザーの名前を入力して、［**検索**］をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが［**選択した追加の必須承認者**］の一覧に表示されます。
  - ［選択した追加の必須承認者］の一覧からユーザーを削除するには、次のいずれかを行います。
    - ［**検索**］をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して［**検索**］をクリックし、検索結果を絞り込みます。
    - ［**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。

11. **[次へ]** をクリックします。 **[デリバリーグループ割り当て]** ページが開きます。



12. **[デリバリーグループを選択]** 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 **[アプリ割り当てを受信するためのデリバリーグループ]** 一覧に表示されます。

13. **[展開スケジュール]** を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[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、 **[接続するたび]** 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 **[オフ]** 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、 **[常時接続]** の展開は適用されません。

14. **[保存]** をクリックします。 **[アプリ]** ページが開きます。

15. 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。

- **[アプリ]** 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**[有効化]** をクリックします。
- 確認ダイアログボックスが表示されたら、**[有効化]** 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。

MDXアプリケーションポリシーの概要

Feb 27, 2017

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のMDXアプリケーションポリシーの一覧については、MDX Toolkitのドキュメントの「MDXアプリケーションポリシーの概要」を参照してください。

XenMobile StoreおよびCitrix Secure Hubのブランド設定

Feb 27, 2017

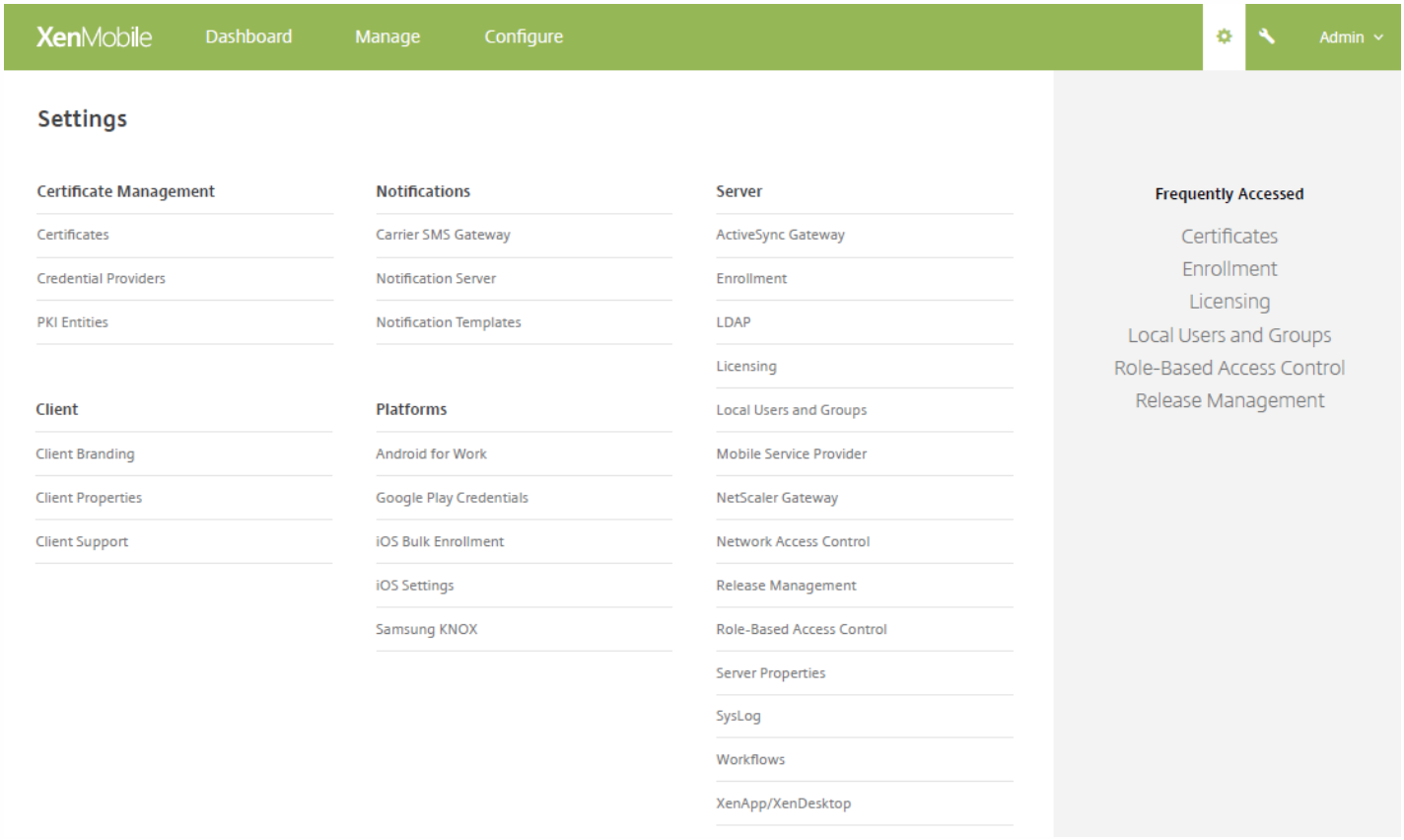
ストアにアプリを表示する方法を設定してロゴを追加し、Secure HubとXenMobile Storeをブランド化できます。このブランド設定機能は、iOSおよびAndroidデバイスで利用できます。

注： 始める前に、カスタム画像を準備してアクセスできるようにしてください。

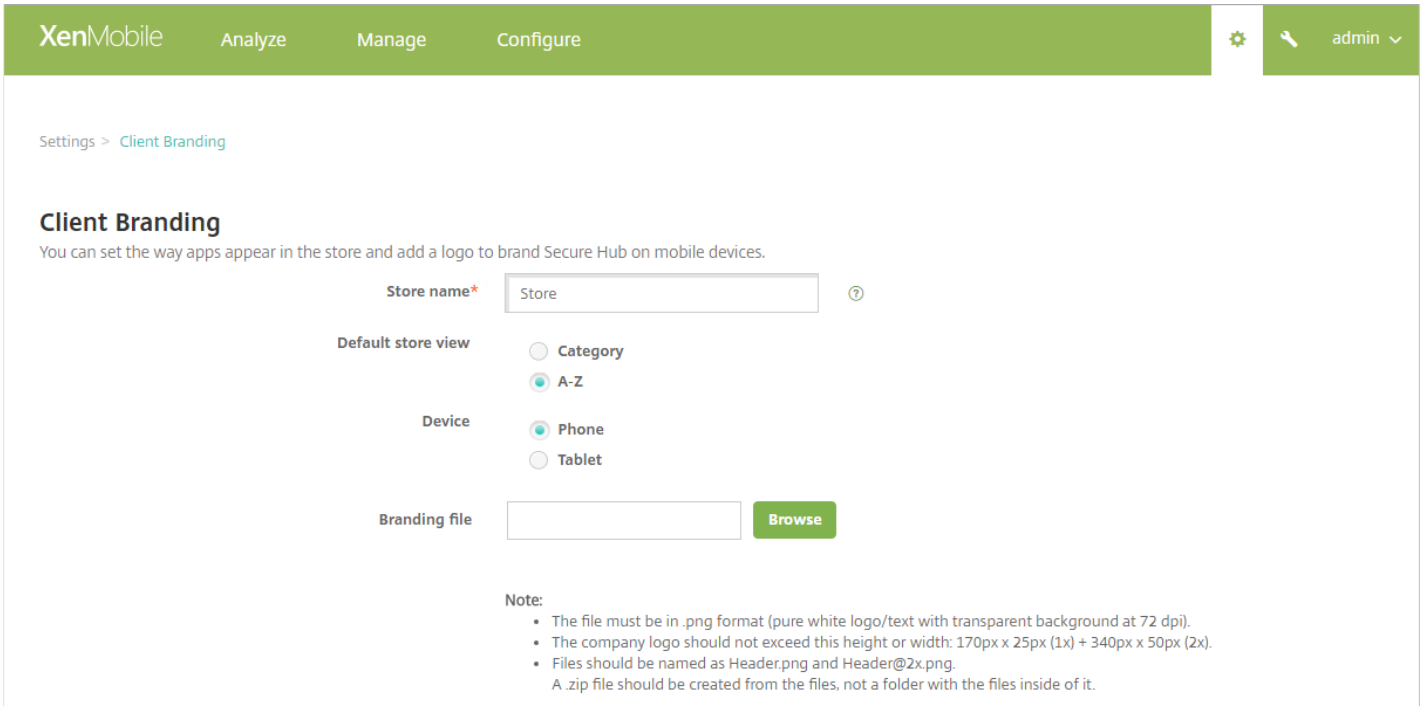
カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および340px×50px（2x）を超過しないようにする必要があります。
- ファイルの名前はHeader.pngおよびHeader@2x.pngにします。
- ファイルを含むフォルダーではなく、ファイルから.zipファイルを作成します。

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



2. **[クライアント]** で **[クライアントブランド化]** をクリックします。**[クライアントブランド化]** ページが開きます。



次の設定を構成します。

- **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。
- **デフォルトストアビュー**：［カテゴリ］または［A~Z］を選択します。デフォルトは［A~Z］です。
- **デバイス**：［電話］または［タブレット］を選択します。デフォルトは［電話］です。
- **ブランド化するファイル**：［参照］をクリックしてブランド設定に使用するイメージまたはイメージの.zipファイルの場所に移動し、ファイルを選択します。

3. ［保存］をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、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。

Citrix Launcher

Feb 27, 2017

Citrix Launcherを使用すると、XenMobileによって展開されたAndroidデバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix LauncherのSecure Hub管理でサポートされるAndroidの最小バージョンは、Android 4.0.3です。**Launcher構成**ポリシーを追加すると、次のCitrix Launcher機能を制御できます。

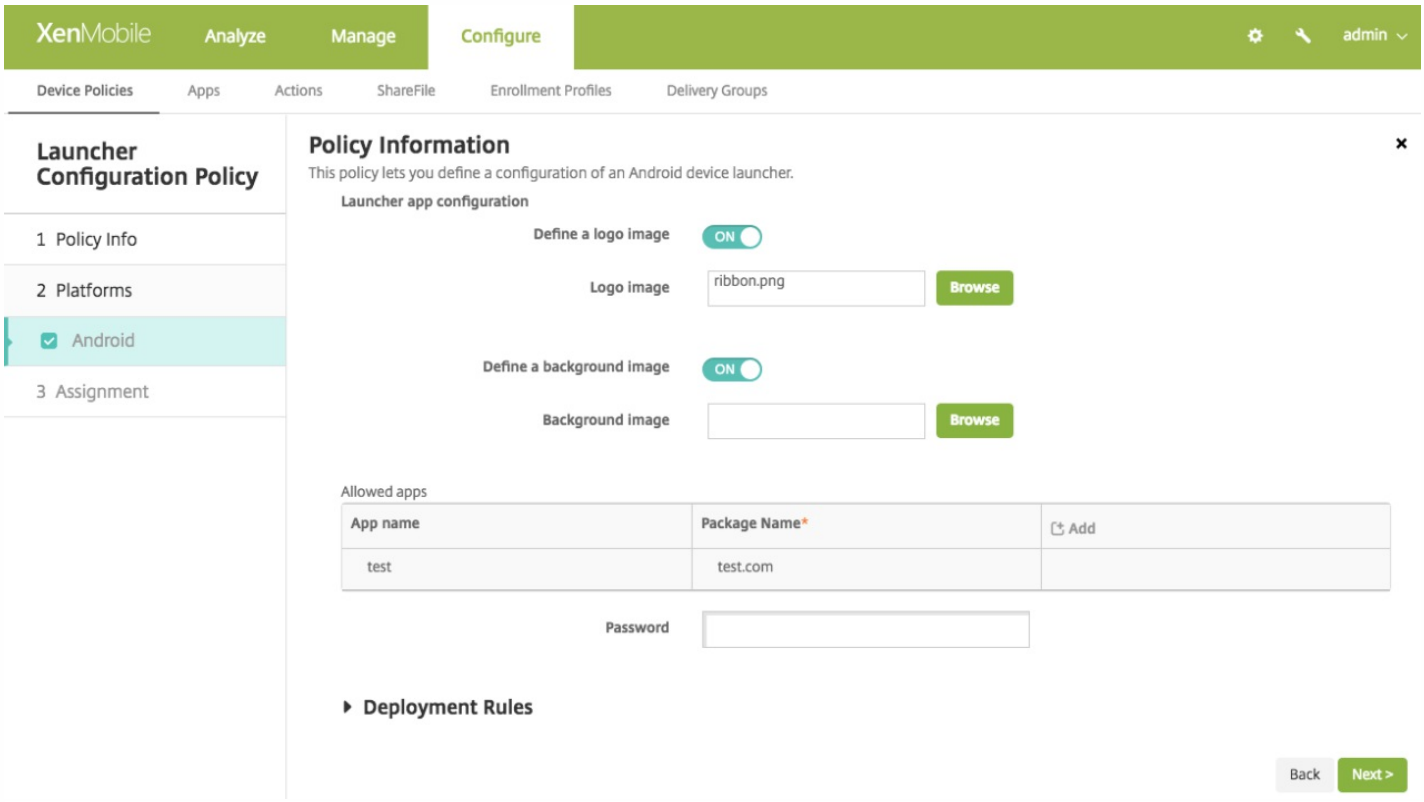
- ユーザーは管理者が指定したアプリにのみアクセスできるようにAndroidデバイスを管理する。
- Citrix Launcherアイコンのカスタムロゴ画像と、Citrix Launcherのカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

Citrix Launcherを使用するとそれらのデバイスレベルの制約を適用できますが、ランチャーは、WiF設定、Bluetooth設定、およびデバイスパスコード設定などのデバイス設定への組み込みのアクセス権をユーザーに付与します。Citrix Launcherは、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Citrix LauncherをAndroidデバイスに提供するには、次の一般的な手順に従います。

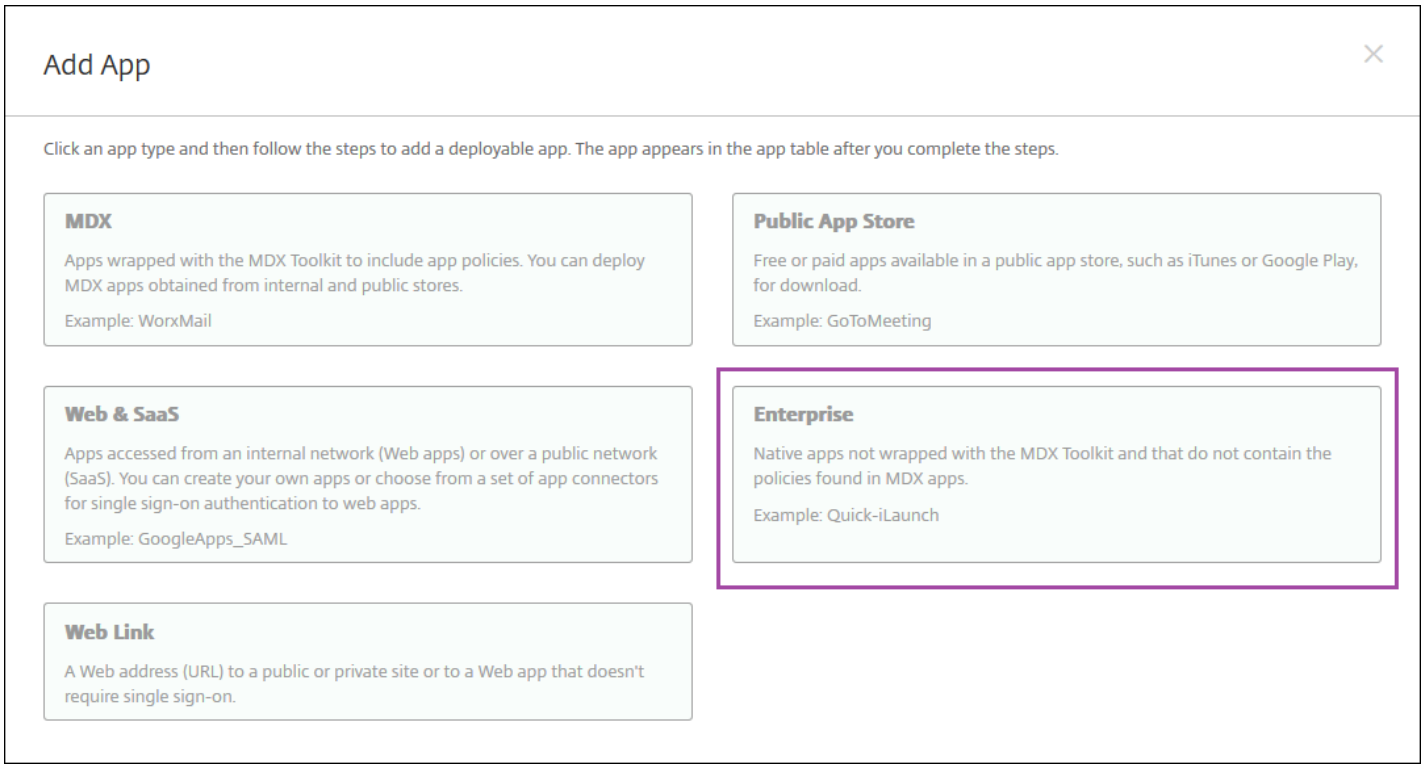
1. Citrix LauncherアプリをXenMobileエディションのCitrix XenMobileダウンロードページからダウンロードします。ファイル名はCitrixLauncher.apkです。ファイルはすぐにXenMobileにアップロードできる状態で、ラッピングを必要としません。

2. デバイスポリシー**Launcher Configuration Policy**を追加します。**[Configure] > [Device Policies]**の順にクリックして、**[Add]**をクリックし、**[Add a New Policy]**ダイアログボックスに「**Launcher**」と入力を開始します。詳しくは、「Launcher Configurationポリシー」を参照してください。



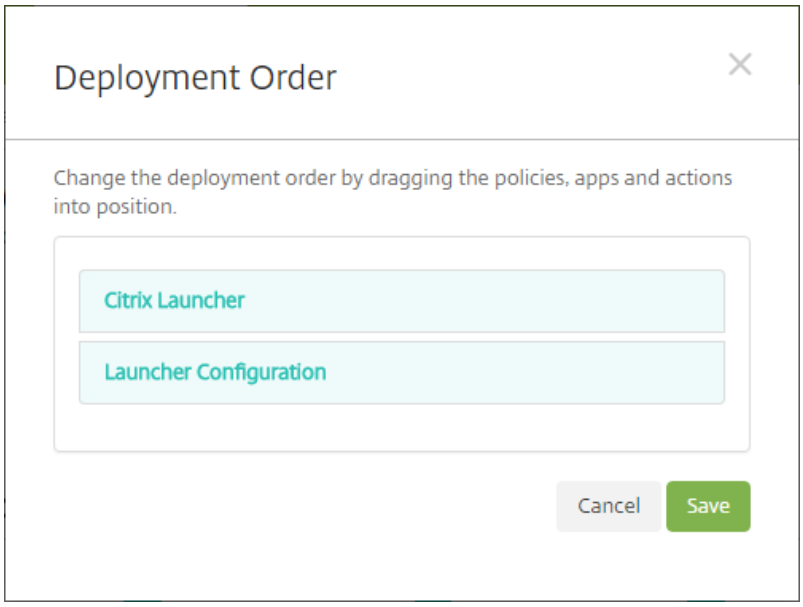
3. Citrix Launcherアプリをエンタープライズアプリとして XenMobileに追加します。**[構成] > [アプリ]**で、**[追加]**をクリックし、続いて**[エンタープライズ]**をクリックします。詳しくは、「エンタープライズアプリケーションの追加」を参

照してください。



4. **[Configure] > [Delivery groups]** で次のように構成して、Citrix Launcherのデリバリーグループを作成します。

- **[Policiesシー]** ページで、 **[Launcher Configuration Policy]** を追加します。
- **[アプリ]** ページで、**Citrix Launcher**を **[必須アプリ]** にドラッグします。
- **[概要]** ページで **[展開順]** をクリックして、**Citrix Launcher**アプリが**Launcher構成**ポリシーよりも先であることを確認します。



詳しくは、「リソースの展開」を参照してください。

iOS Volume Purchase Planの設定

Apr 04, 2017

AppleのiOS Volume Purchase Program（VPP）を使用すると、iOSアプリのライセンスを管理することができます。VPPソリューションを利用すると、組織のアプリケーションやそのほかの大量なデータの検索、購入、配布の処理が簡単になります。

VPPではXenMobileを使用してパブリックアプリケーションストアのアプリを配布することができます。VPPは、XenMobile Apps、またはMDX Toolkitを使用してラップしたアプリではサポートされていません。VPPではパブリックストアから入手したXenMobileアプリを配布することはできますが、展開は最適化されません。この制約に対処するには、XenMobileサーバーとSecure Hubストアをさらに強化する必要があります。VPP経由のXenMobileパブリックストアアプリの展開に関する既知の問題と想定される解決策の一覧は、Citrix Knowledge Centerのこちらのトピックを参照してください。

VPPによって、適用可能なアプリをデバイスに直接配布できます。また、引き換え可能なコードを使用してユーザーにコンテンツを割り当てることができます。XenMobileで、iOS VPPに固有の設定を構成できます。

XenMobileは、VPPライセンスをAppleから定期的に再インポートしてライセンスにすべての変更を反映させています。こうした変更にはVPPからインポートしたアプリを手動で削除する場合も含まれます。デフォルトで、XenMobileはVPPライセンスベースラインを最小で720分ごとに更新します。このベースライン間隔をサーバープロパティの［VPP ベースライン間隔］（vpp.baseline）で変更することができます。詳しくは、「サーバープロパティ」を参照してください。

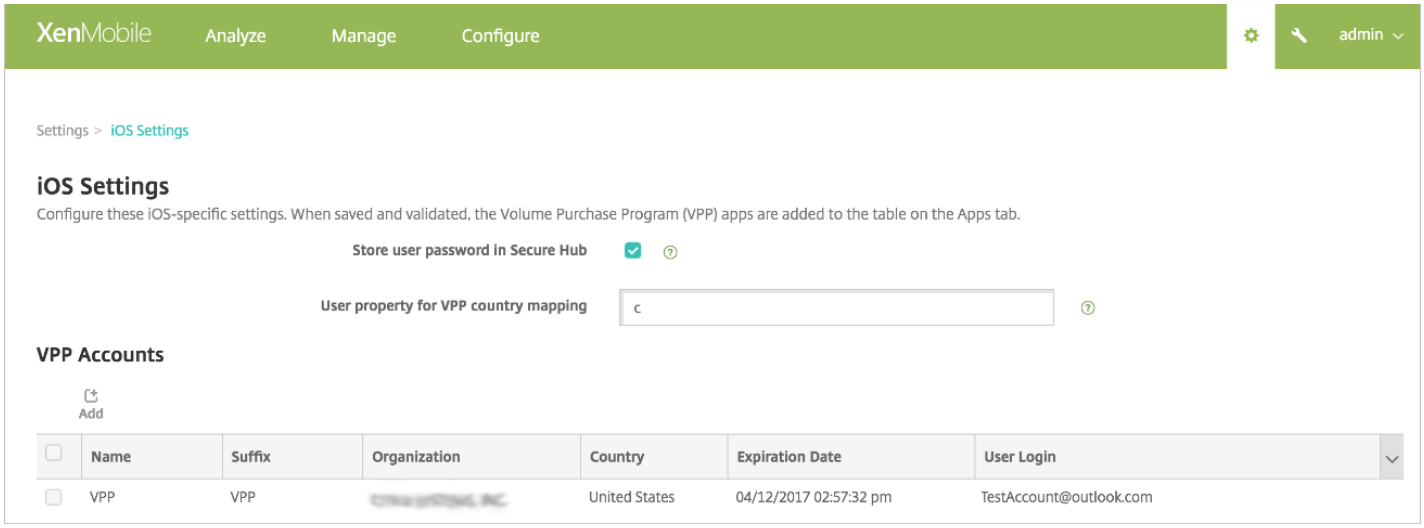
このトピックは、管理されたライセンスでVPPを使用して、XenMobileでアプリを配布できるようにする方法について説明します。現在引き換えコードを使用中で、管理された配布に変更する場合は、Apple社のサポートドキュメントのMigrate from redemption codes to managed distribution with the Volume Purchase Programを参照してください。

iOS VPPについて詳しくは、http://www.apple.com/business/vpp/を参照してください。VPPに登録するには、https://deploy.apple.com/qforms/open/register/index/avsにアクセスしてください。iTunesのVPPストアにアクセスするには、https://vpp.itunes.apple.com/?l=enに移動してください。

XenMobileでiOS VPP設定を保存すると、購入したアプリケーションがXenMobileコンソールの**[構成] > [アプリ]** ページに表示されます。

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

2. **[プラットフォーム]** で **[iOS設定]** をクリックします。**[iOS設定]** 構成ページが開きます。



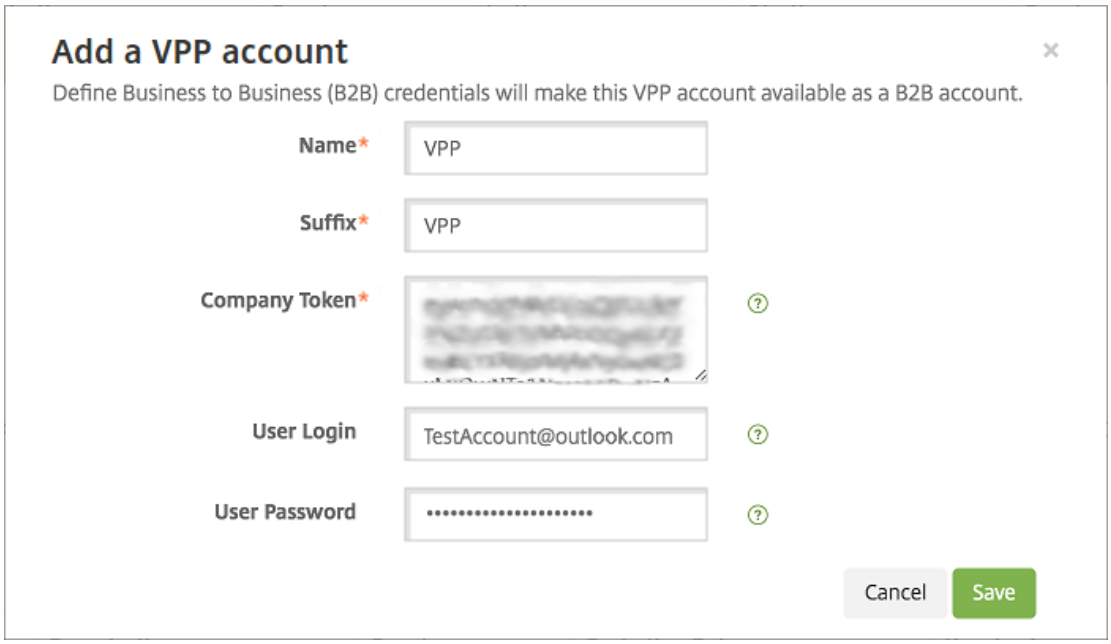
3. 次の設定を構成します。

- **Secure Hubのユーザーパスワードを保存する**: XenMobile認証用のユーザー名とパスワードをSecure Hubに保存するかどうかを選択します。デフォルトでは、この安全な方法で情報を保存します。
- **VPP国マッピングのユーザープロパティ**: ユーザーが国固有のアプリ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コードが日本用の場合、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アカウント

- 追加するVPPアカウントごとに、**[追加]** をクリックします。**[VPPアカウントの追加]** ダイアログボックスが開きます。



追加するアカウントごとに、次の設定を構成します。

注：Apple Configurator 1を使用している場合、次の手順でライセンスファイルをアップロードします。**[構成] > [アプリ]**、プラットフォームページの順に移動し、**[Volume Purchase Program]** を展開します。

- **名前**：VPPアカウント名を入力します。
- **サフィックス**：VPPアカウントを介して取得したアプリケーションに表示されるサフィックスを入力します。たとえば、「**VPP**」と入力すると、Secure Mailアプリはアプリ一覧で「**Secure Mail - VPP**」と表示されます。
- **会社トークン**：Appleから取得したVPPサービストークンを入力するか、コピーして貼り付けます。トークンを取得するには、Apple VPPポータルの **[Account Summary]** ページで **[Download]** をクリックし、VPPファイルを生成してダウンロードします。このファイルには、サービストークンのほかに、国コードや有効期限などの他の情報も含まれます。ファイルを安全な場所に保存します。
- **ユーザーログイン**：任意で、カスタムB2Bアプリケーションのインポートに使用する、認証済みVPPアカウントの管理者名を入力します。
- **ユーザーパスワード**：VPPアカウントの管理者パスワードを入力します。

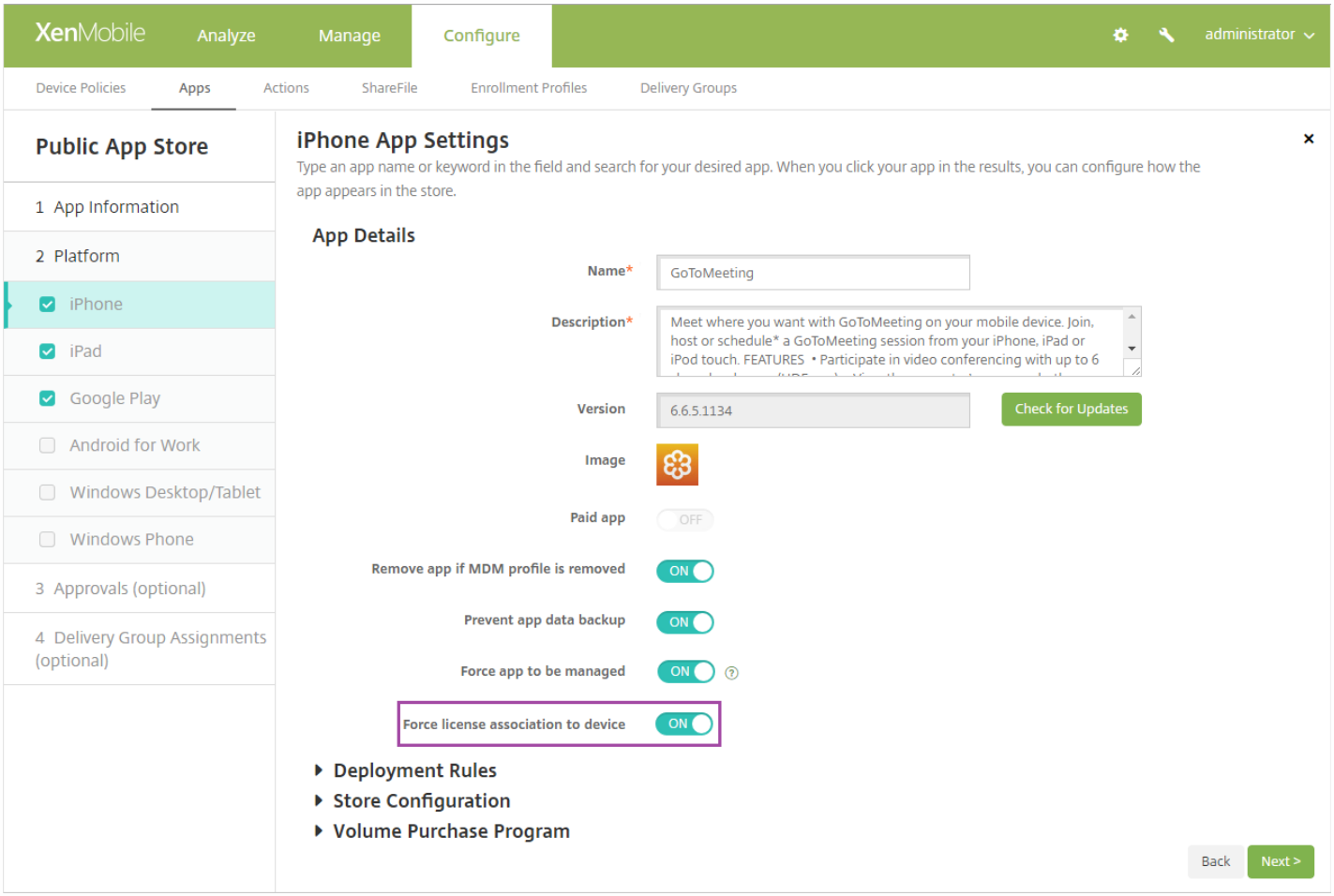
5. **[保存]** をクリックしてダイアログボックスを閉じます。

6. **[保存]** をクリックしてiOS設定を保存します。

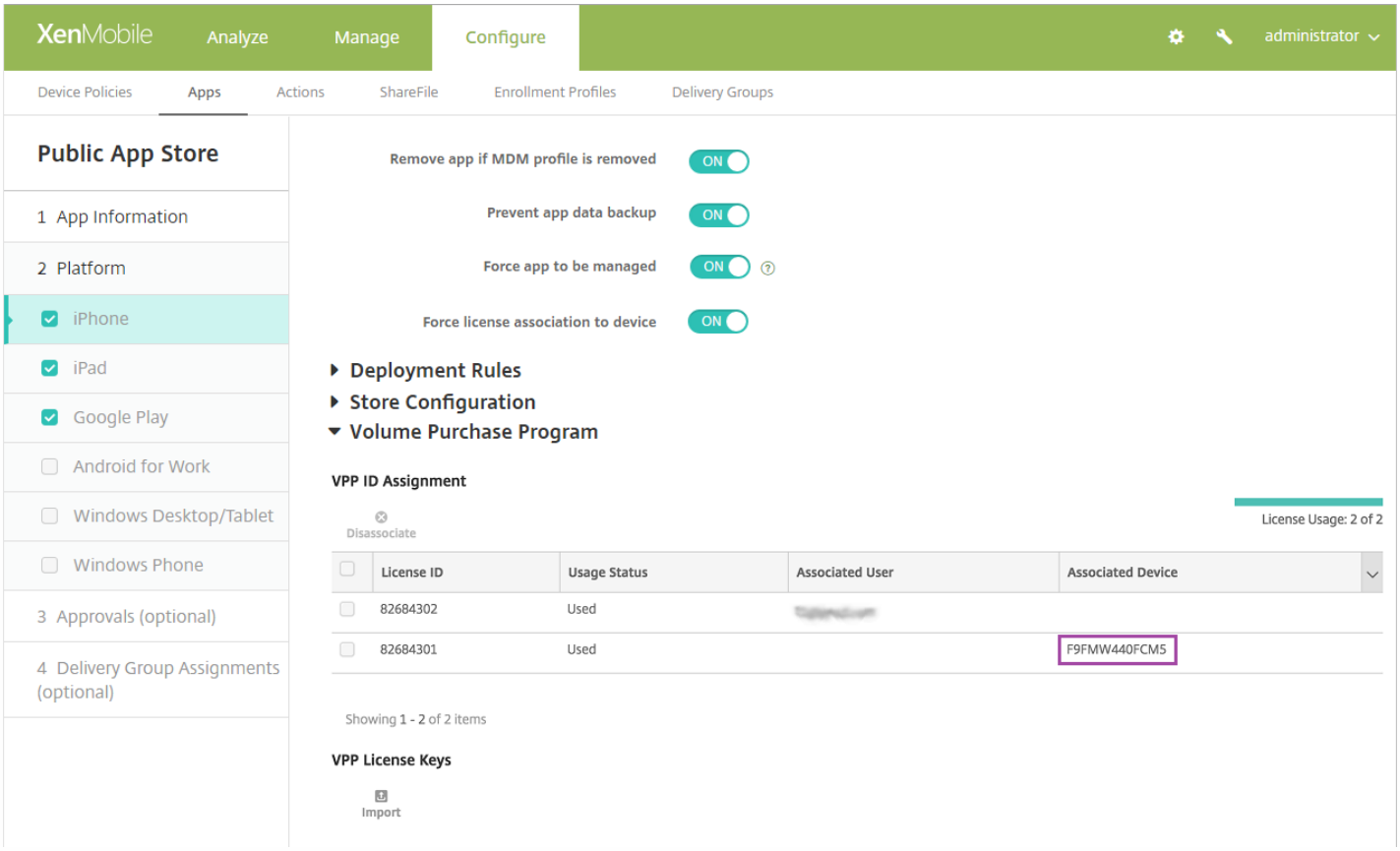
アプリを **[構成] > [アプリ]** ページの一覧に追加することを伝えるメッセージが表示されます。このページで、VPPアカウントのアプリ名に前述の構成で指定したサフィックスが含まれていることを確認してください。

VPPアプリ設定を構成し、VPPアプリのデリバリーグループおよびデリバリーポリシー設定を調整できるようになりました。この構成を完了すると、ユーザーはデバイスを登録できるようになります。以下は、この手順で検討する事項です。

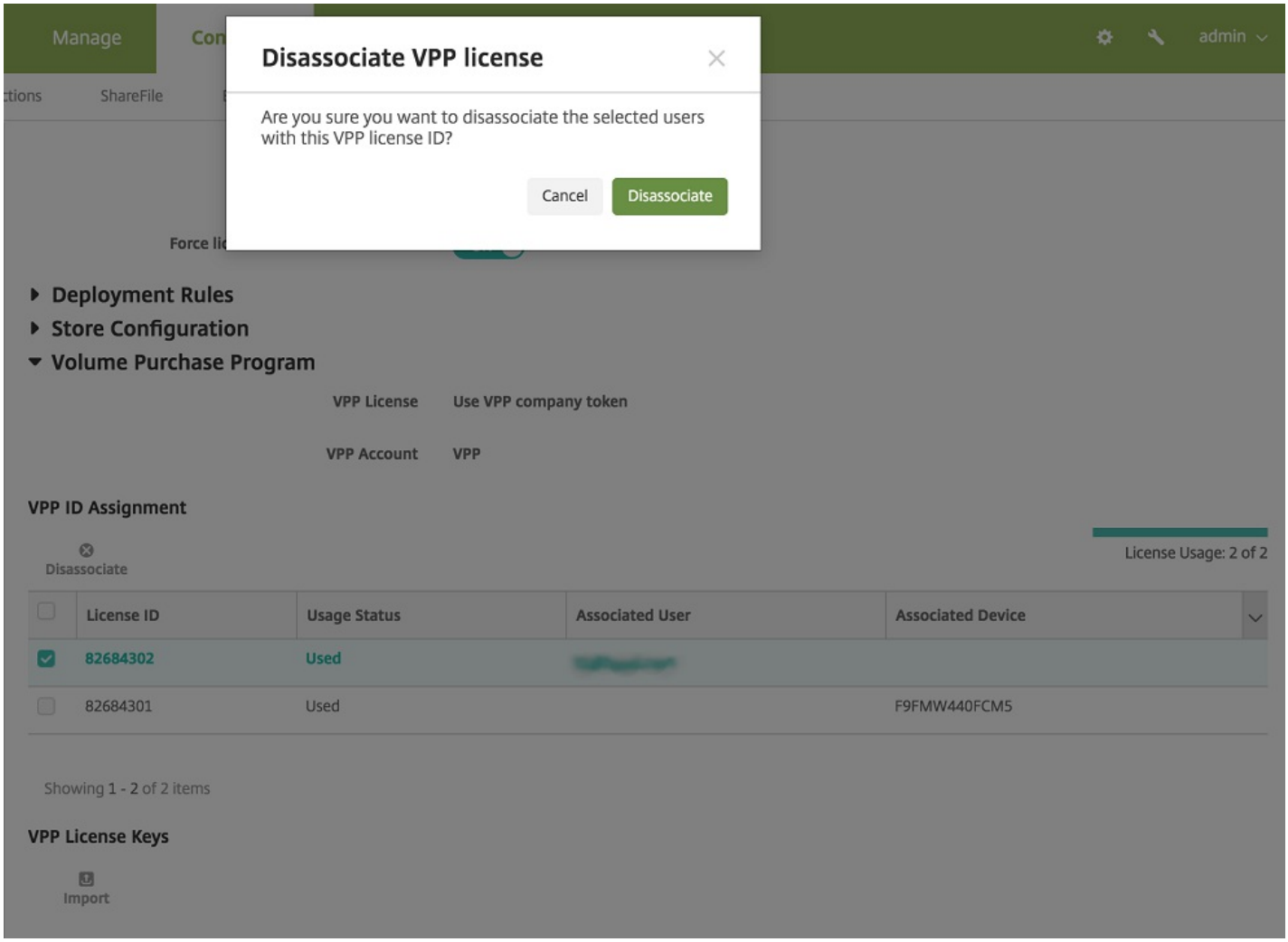
- VPPアプリ設定（ **[構成] > [アプリ]** ）を構成すると、 **[デバイスへの強制ライセンス割り当て]** が有効になります。監視対象デバイスでApple VPPおよびDEPを使用する利点は、XenMobileがアプリをデバイスレベル（ユーザーレベルではなく）で割り当てることができるようになることです。このため、Apple IDデバイスを使用する必要がありません。また、VPPプログラム参加の招待状がユーザーに送信されることもありません。ユーザーは各自のiTunesアカウントにサインインせずにアプリをダウンロードできます。



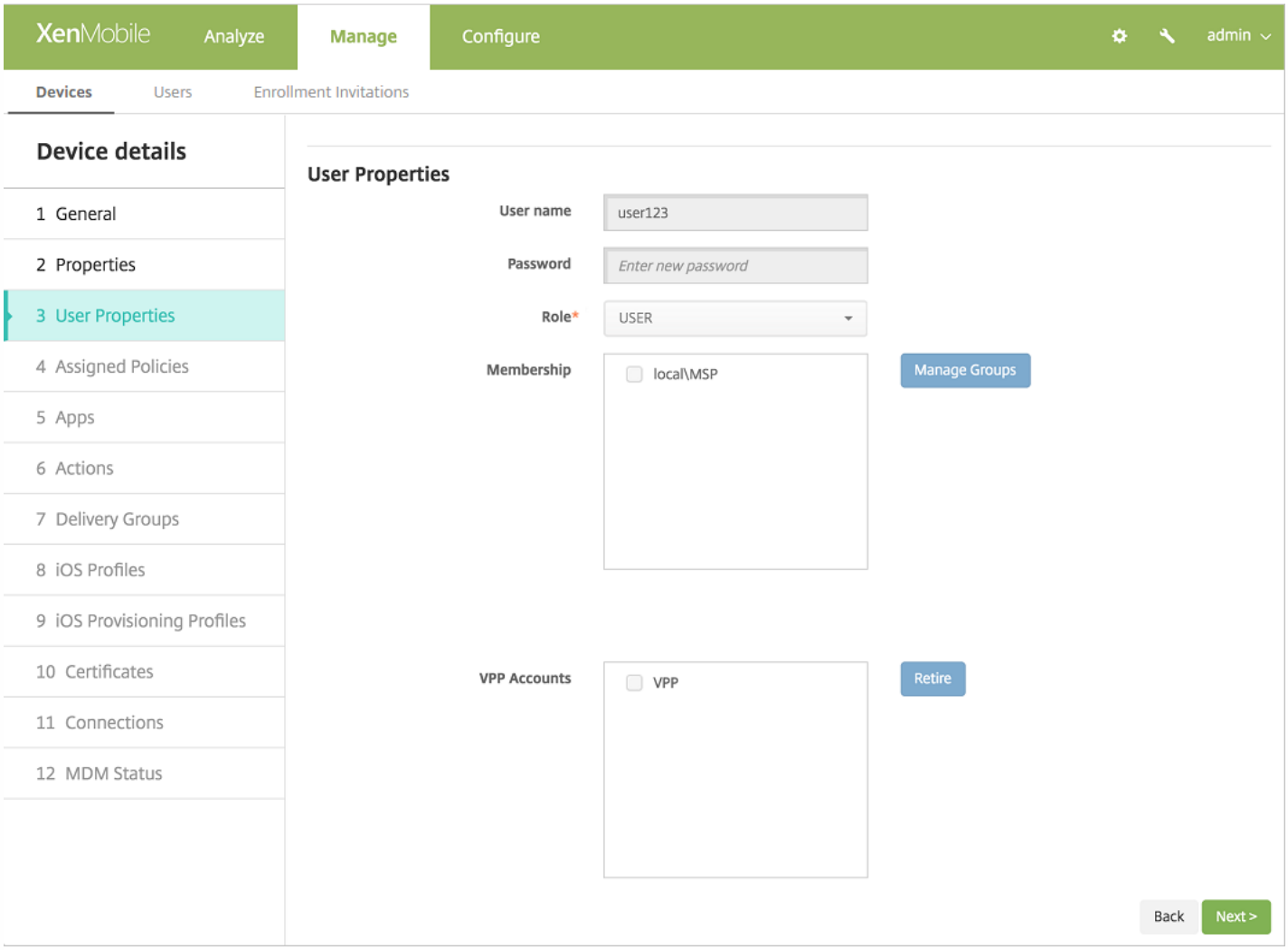
アプリのVPP情報を表示するには、 **[Volume Purchase Program]** を展開します。 **[VPP ID割り当て]** の表で、ライセンスがデバイスに関連付けられていることにご注意ください。デバイスのシリアル番号は **[割り当てられたデバイス]** 列に表示されます。ユーザーがトークンを削除して再度インポートすると、シリアル番号ではなく「**非表示**」と表示されます。これはApple社のプライバシー制限によるものです。



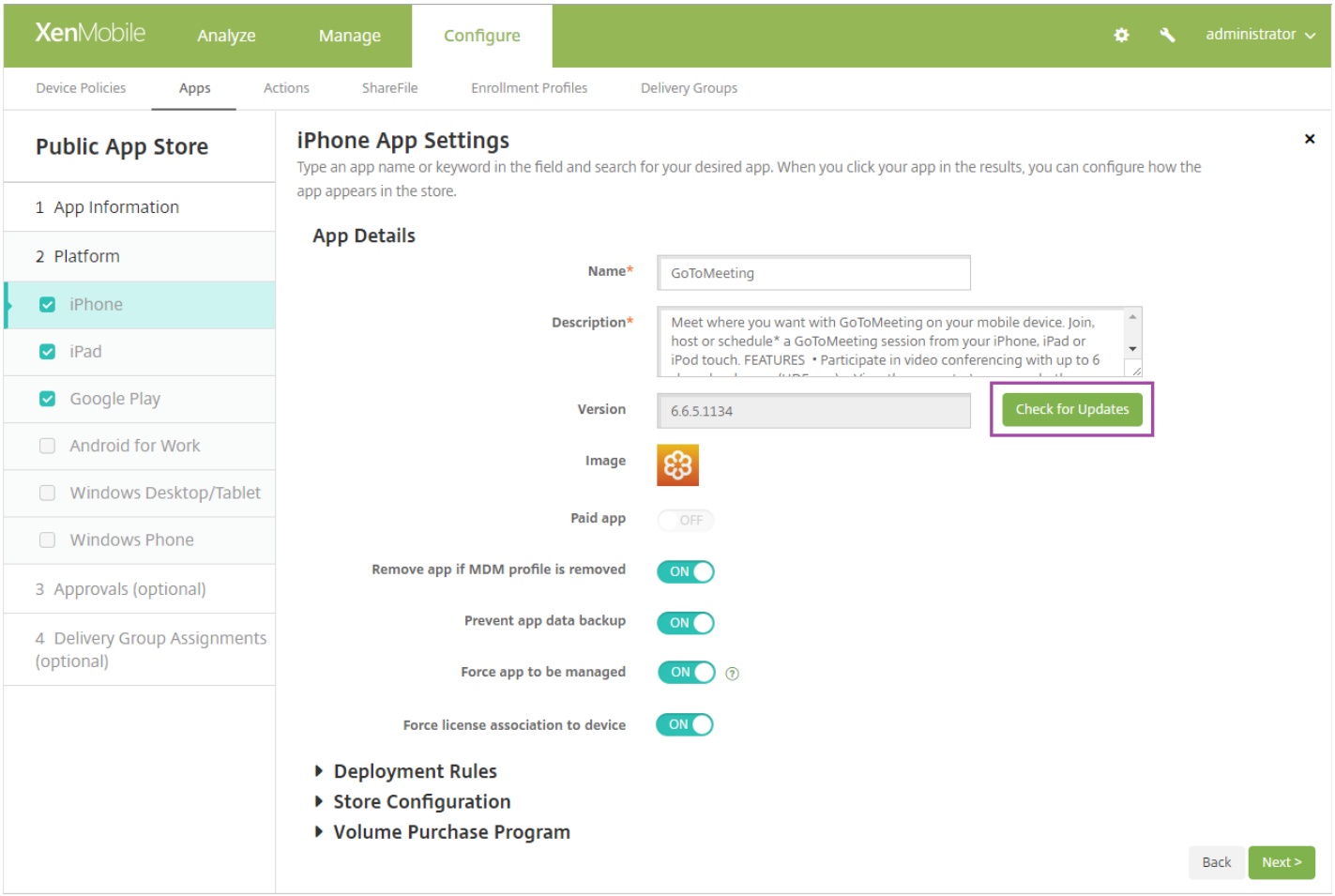
ライセンスの関連付けを解除するには、該当ライセンスの行を選択して**[割り当て解除]**をクリックします。



VPPライセンスをユーザーに関連付けると、XenMobileはユーザーをVPPアカウントに統合し、ユーザーのiTunes IDをVPPアカウントに関連付けます。ユーザーのiTunes IDがユーザーの会社やXenMobileサーバーに表示されることはありません。Apple社はユーザーのプライバシーを確保するために、透過的に関連付けを作成します。ユーザーアカウントからすべてのライセンスの関連付けを解除することで、VPPプログラムからユーザーを削除できます。ユーザーを削除するには、 **[管理] > [デバイス]** にアクセスします。



- アプリをデリバリーグループに割り当てると、XenMobileはデフォルトでアプリを任意アプリとして認識します。XenMobileで確実にアプリがデバイスに展開されるようにするには、**[構成] > [デリバリーグループ]** に移動します。**[アプリ]** ページでアプリを **[必須アプリ]** 一覧に移動します。
- パブリックアプリケーションストアのアプリの更新が使用可能で、アプリがVPP経由でプッシュされる場合、ユーザーが更新をチェックして適用するまで、このアプリは自動的にデバイスで更新されません。Secure Hub（ユーザーではなくデバイスに割り当てられている場合）の更新をプッシュするには、次の手順を実行します。プラットフォームページの **[構成] > [アプリ]** で、**[更新プログラムのチェック]** をクリックして更新を適用します。



Citrix Secure Hubを介したXenAppおよびXenDesktop

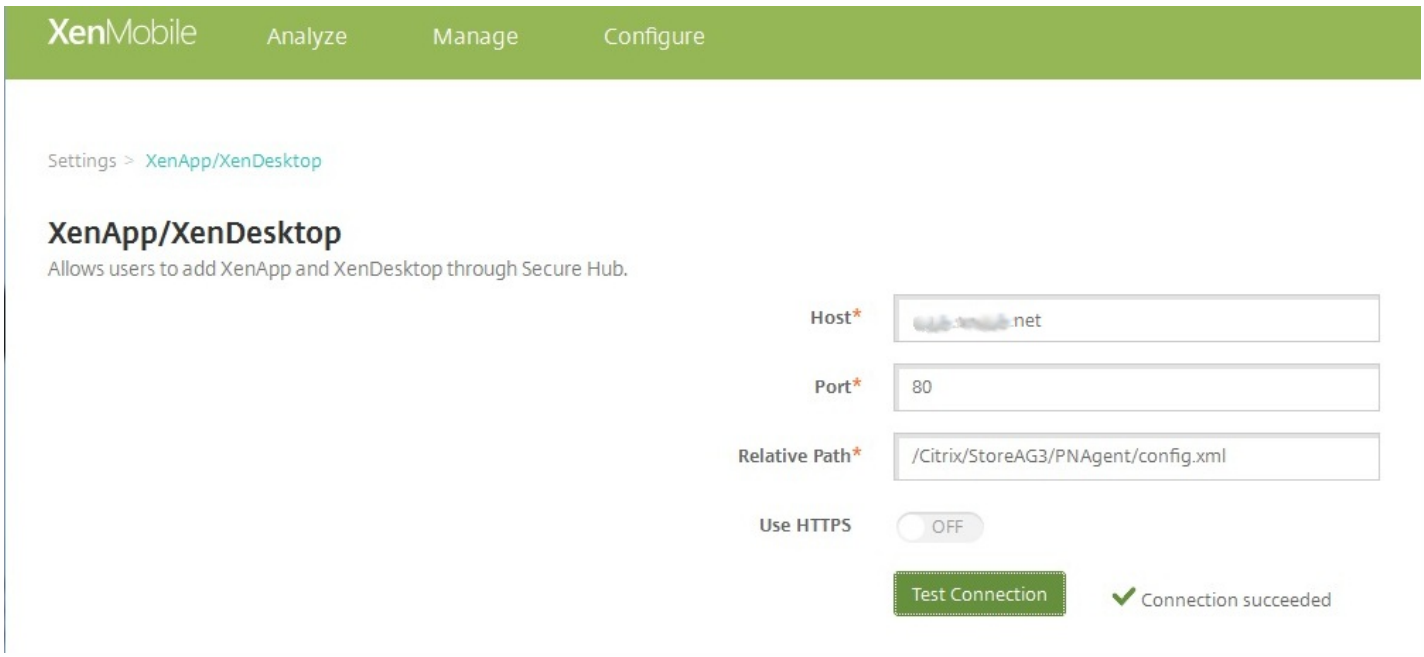
Feb 27, 2017

XenMobileでは、XenAppおよびXenDesktopからアプリケーションを収集して、XenMobile Storeでモバイルデバイスユーザーがそのアプリ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、XenMobile Store内から直接アプリケーションをサブスクライブして、Secure Hubから起動します。アプリケーションを起動するために、Citrix Receiverをユーザーのデバイスにインストールする必要があります。ただし、構成する必要はありません。

この設定を構成するには、Web InterfaceサイトまたはStoreFrontの完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）またはIPアドレスと、ポート番号が必要です。

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックします。**[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。

- **ホスト：** Web InterfaceサイトまたはStoreFrontの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
- **ポート：** Web InterfaceサイトまたはStoreFrontのポート番号を入力します。デフォルトは80です。
- **相対パス：** パスを入力します。たとえば、「/Citrix/PNAgent/config.xml」と入力します。
- **HTTPSの使用：** Web InterfaceサイトまたはStoreFrontとクライアントデバイスの間で安全な認証を有効にするかどうかを選択します。デフォルトは**[オフ]**です。

4. **[接続のテスト]**をクリックして、指定したXenAppおよびXenDesktopサーバーにXenMobileが接続できることを確認します。

5. **[保存]**をクリックします。

ShareFileをXenMobileと使用する

Apr 24, 2017

XenMobileには、ShareFileと統合するために次の２つのオプションがあります。 ShareFile EnterpriseとStorageZoneコネクタです。ShareFile EnterpriseまたはStorageZoneコネクタと統合するにはXenMobile Enterprise Editionが必要です。

ShareFile Enterprise

XenMobile Enterprise Editionの場合、XenMobileでShareFile Enterpriseアカウントにアクセスできるよう構成可能です。この構成により以下の機能が実現します。

- モバイルユーザーがファイル共有やファイル同期、StorageZoneコネクタなどの完全なShareFile機能セットにアクセスできます。
- ShareFileでXenMobileアプリユーザーのシングルサインオン認証やADベースのユーザーのアカウントプロビジョニング、総合的なアクセス制御ポリシーが可能になります。
- XenMobileコンソールからShareFileの構成、サービスレベル監視、ライセンス使用状況の監視が可能になります。

ShareFile Enterpriseに関するXenMobileの構成について詳しくは、「ShareFileでのSAMLによるシングルサインオン」を参照してください。

StorageZone コネクタ

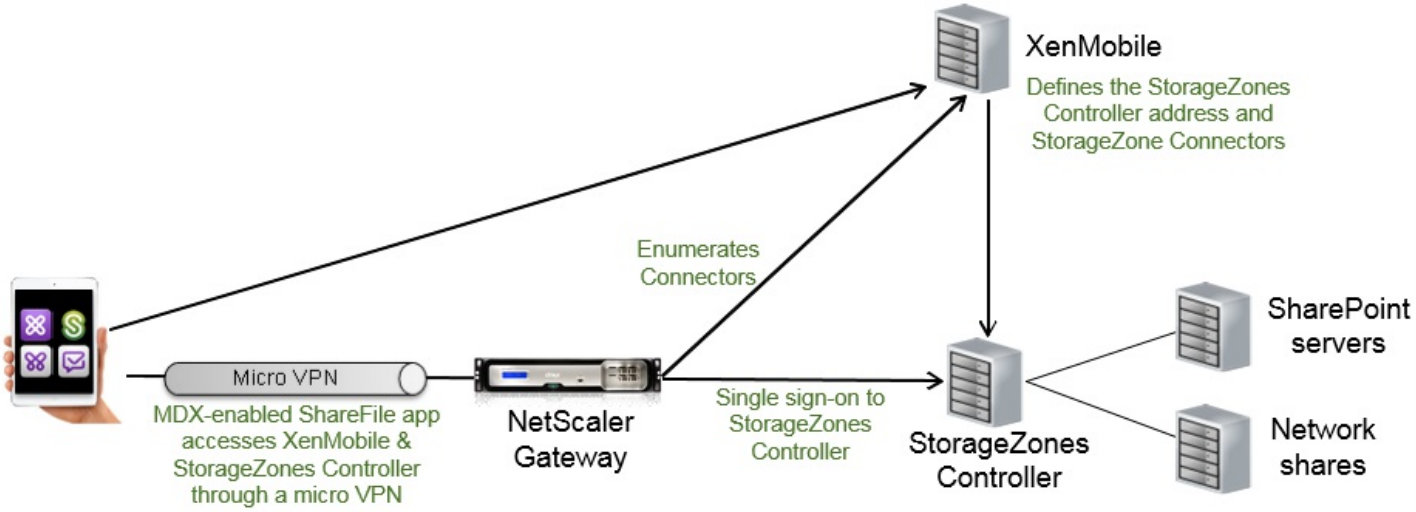
XenMobileを、XenMobileコンソールで作成したStorageZoneコネクタだけにアクセスできるように構成することも可能です。この構成により以下の機能が実現します。

- SharePointサイトやネットワークファイル共有などの既存のオンプレミスのストレージリポジトリに安全にモバイルアクセスできます。
- ShareFileサブドメインの設定やShareFileに対するユーザーのプロビジョニング、ShareFileデータのホストが不要になります。
- ShareFile XenMobile Apps for iOSおよびAndroidでデータにモバイルアクセスできます。Microsoft Officeドキュメントを編集できます。モバイル デバイスから Adobe PDF ファイルのプレビューおよび注釈もできます
- 社内ネットワーク外へのユーザー情報漏洩に対するセキュリティ規制に準拠します。
- XenMobileコンソールでStorageZoneコネクタを簡単に設定できます。XenMobileでShareFileの全機能を後から使うことになった場合は、XenMobileコンソールで構成を変更できます。
- XenMobile Enterprise Editionは必要です。

XenMobileとStorageZoneコネクタのみとの統合の場合、次のようになります。

- ShareFileは、NetScaler Gatewayへのシングルサインオン構成を使用してStorageZones Controllerに対する認証を行います。
- ShareFileコントロールプレーンが使用されないため、XenMobileでのSAML経由での認証は行われません。

次の図は、XenMobileとStorageZoneコネクタを組み合わせて使う高度なアーキテクチャを示しています。



要件

- 各コンポーネントの最小バージョンは次のとおりです。
  - XenMobile Server 10.5（オンプレミス）
  - ShareFile for iOS（MDX）5.3
  - ShareFile for Android（MDX）5.3
  - ShareFile StorageZones Controller 5.0

    この記事では、ShareFile StorageZones Controller 5.0の構成方法を説明します。
- StorageZones Controllerを実行するサーバーがシステム要件を満たしていることを確認してください。この要件については、ShareFile StorageZones Controllerのドキュメントの「System requirements」で次のセクションを参照してください。
  - StorageZones Controller
  - StorageZone Connector for SharePoint
  - StorageZone Connector for Network File Shares

    StorageZones for ShareFile DataおよびRestricted StorageZonesに関する要件は、XenMobileとStorageZone Connectorsのみとの統合には適用されません。

    XenMobileでは、Documentumコネクタはサポートされません。
- PowerShellスクリプトを実行するには
  - スクリプトは、32ビット（x86）バージョンのPowerShellで実行します。

インストール作業

StorageZones Controllerのインストールと設定を行うには、次の作業を記載順に実行します。これらの手順は、XenMobileとStorageZoneコネクタのみとの統合に固有のものです。以下の記事の一部は、StorageZones Controllerのドキュメントのものです。

1.StorageZones Controller用のNetScalerの構成

NetScalerをStorageZones ControllerのDMZプロキシとして使用できます。

2.SSL証明書のインストール

StorageZones Controllerで標準ゾーンをホストする場合、SSL証明書が必要になります。StorageZones Controllerで制限付きゾーンをホストし内部アドレスを使用する場合は、SSL証明書は必要ありません。

3.サーバーの準備

StorageZoneコネクタに対してIISとASP.NETを設定する必要があります。

4.StorageZones Controllerのインストール

5.StorageZoneコネクタのみで使用するStorageZones Controllerの準備

6.StorageZonesのプロキシサーバーの指定

StorageZones Controllerのコンソールで、StorageZones Controllerのプロキシサーバーを指定できます。プロキシサーバーは他の方法で指定することもできます。

7.委任のためにStorageZones Controllerを信頼するようにドメインコントローラーを構成する

ネットワーク共有上またはSharePointサイト上のNTLMかKerberos認証をサポートするようにドメインコントローラーを構成します。

8.StorageZoneへのセカンダリStorageZones Controllerの追加

高可用性を実現するようにStorageZoneを構成するには、2つ以上のStorageZones ControllerをStorageZoneに接続します。

StorageZones Controllerのインストール

1. StorageZones Controllerソフトウェアをダウンロードしてインストールします。

a. ShareFileのダウンロードページ（http://www.citrix.com/downloads/sharefile.html）でログオンして、最新のStorageZones Controllerインストーラーをダウンロードします。

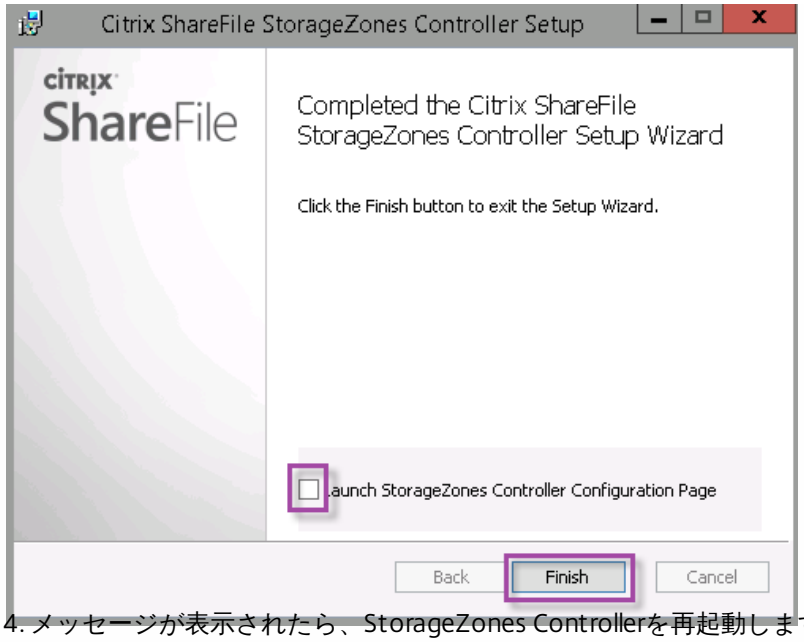
b. StorageZones Controllerをインストールすると、サーバーのデフォルトのWebサイトがStorageZones Controllerのインストールパスに変更されます。デフォルトのWebサイトで**匿名認証**を有効にします。

2. StorageZones Controllerをインストールするサーバー上でStorageCenter.msiを実行します。

ShareFile StorageZones Controller Setupウィザードが起動します。

3. プロンプトに従ってインストールを進めます。

- インターネットインフォメーションサービス（IIS：Internet Information Services）がデフォルトの場所にインストールされている場合、**［Destination Folder］**ページの設定はデフォルトのままにします。IISがデフォルトの場所以外にインストールされている場合は、IISのインストール先を指定します。
- インストールが完了したら、**［Launch StorageZones Controller Configuration Page］**チェックボックスをオフにして**［Finish］**をクリックします。



4. メッセージが表示されたら、StorageZones Controllerを再起動します。

5. インストールが成功したかテストするために、http://localhost/にアクセスします。インストールが成功している場合、ShareFileのロゴが表示されます。

ShareFileのロゴが表示されない場合は、ブラウザーのキャッシュを削除してもう一度アクセスしてください。

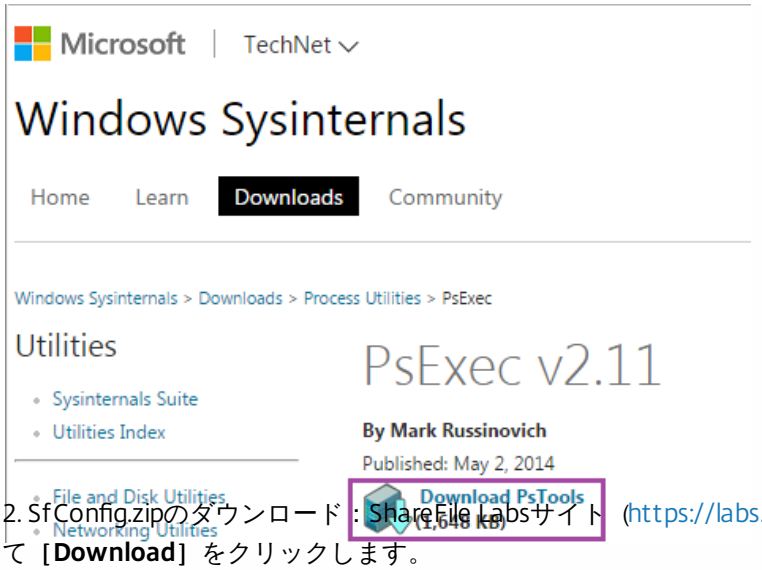
> **Important**
>
> StorageZones Controllerを複製する予定がある場合は、StorageZones Controllerの構成に進む前にディスクイメージをキャプチャします。

StorageZoneコネクタのみで使用するStorageZones Controllerの準備

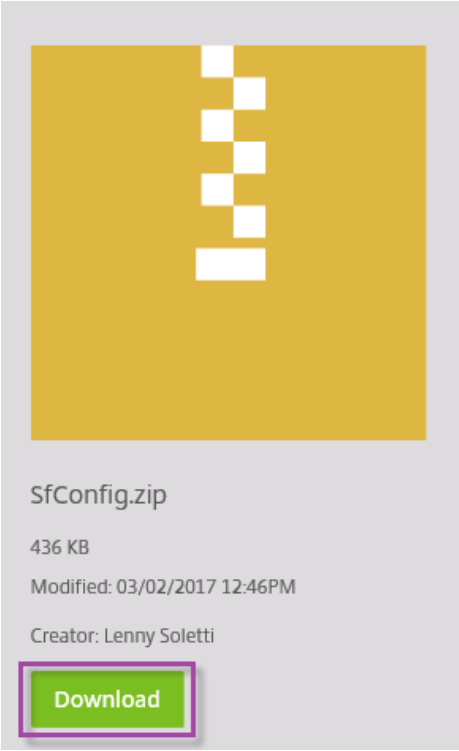
StorageZoneコネクタのみと統合する場合、StorageZones Controllerの管理コンソールは使用しません。これは、管理コンソールではこのソリューションに必要ないShareFileの管理者アカウントが求められるためです。このため、PowerShellスクリプトを実行して、使用するStorageZones Controllerの準備をShareFileコントロールプレーンを用いずに行います。このスクリプトでは次の操作が行われます。

- プライマリStorageZones Controllerとしての現在のStorageZones Controllerの登録。後で、このプライマリStorageZones Controllerにセカンダリ StorageZones Controllerを追加できます。
- ゾーンの作成およびゾーンのパスフレーズの設定

1. StorageZone ControllerサーバーでのPsExecツールのダウンロード：MicrosoftWindows Sysinternalsにアクセスし［**PsToolsのダウンロード**］をクリックします。ダウンロードしたツールをCドライブのルートに展開します。

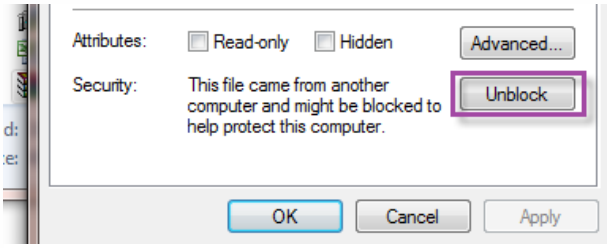


2. SfConfig.zipのダウンロード：ShareFile Labsサイト（https://labs.sharefile.com/d-sf083d50048a4e408）にアクセスして［**Download**］をクリックします。

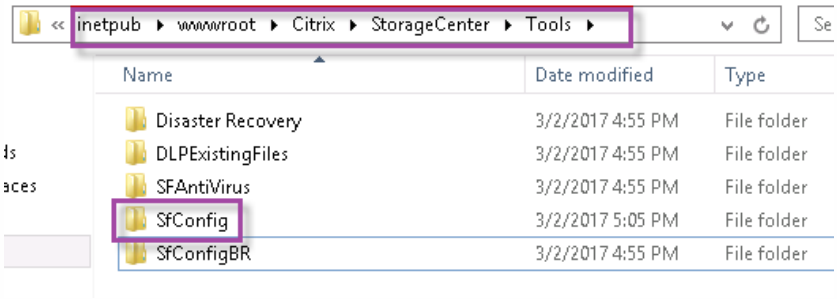


3. SfConfig.zipをC:\inetpub\wwwroot\Citrix\StorageCenter\Toolsに保存します。

4. SfConfig.zipを右クリックして［**プロパティ**］を選択し、［**ブロックの解除**］をクリックしてセキュリティブロックを解除します。



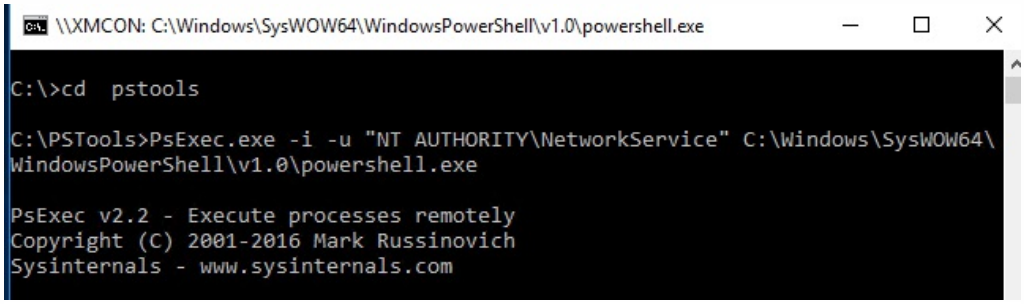
5. SfConfig.zipをC:\inetpub\wwwroot\Citrix\StorageCenter\Toolsに展開します。



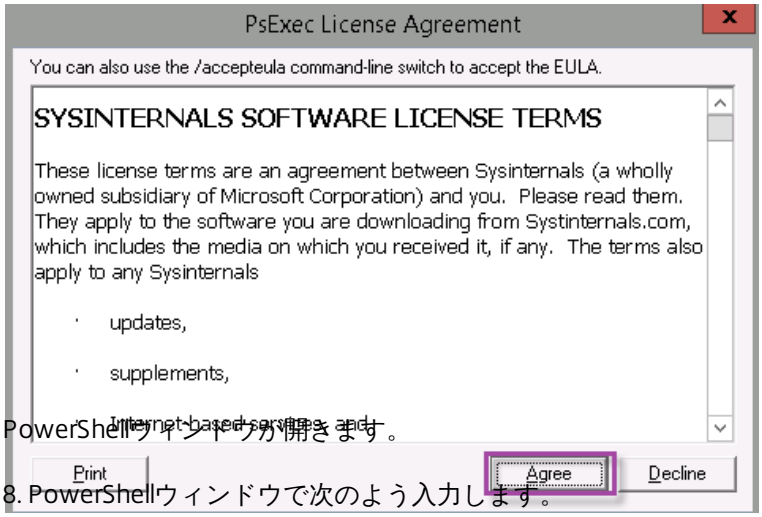
6. PsExecツールの実行：管理者ユーザーとしてコマンドプロンプトを開き、次のように入力します。

-command コピー

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



7. メッセージが表示されたら、［**Agree**］をクリックしてSysinternalsツールを実行します。



PowerShellウィンドウが開きます。

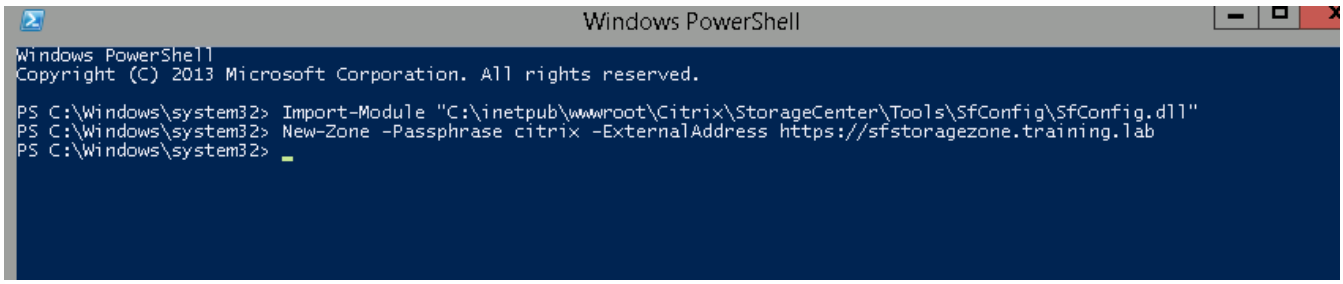
8. PowerShellウィンドウで次のよう入力します。

```
-command
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone  -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

各オプションの意味は次のとおりです。

Passphrase：サイトに割り当てるパスフレーズを指定します。このパスフレーズはメモしておいてください。StorageZones Controllerでパスフレーズを回復することはできません。パスフレーズを失くすと、StorageZonesの再インストール、StorageZoneへのStorageZones Controllerの追加、サーバー障害時のStorageZoneの復旧を行えなくなります。

ExternalAddress：StorageZones Controllerサーバーの外部完全修飾ドメイン名を指定します。



これで、プライマリStorageZones Controllerの準備ができました。

該当する場合は、XenMobileにログインしてStorageZoneコネクタを作成する前に以下の構成を行います。

StorageZonesのプロキシサーバーの指定

委任のためにStorageZones Controllerを信頼するようにドメインコントローラーを構成する

StorageZoneへのセカンダリStorageZones Controllerの追加

StorageZoneコネクタを作成する場合は、「XenMobileでStorageZonesコントローラ接続を定義する」を参照してください。

StorageZoneへのセカンダリStorageZones Controllerの追加

高可用性を実現するようにStorageZoneを構成するには、2つ以上のStorageZones ControllerをStorageZoneに接続します。ゾーンにセカンダリStorageZones Controllerを追加するには、2台目のサーバーにStorageZones Controllerをインストールします。その後、インストールしたStorageZones Controllerを、プライマリStorageZones Controllerのゾーンに追加します。

1. プライマリサーバーに追加するStorageZones Controllerサーバーで、PowerShellウィンドウを開きます。

2. PowerShellウィンドウで次のよう入力します。

Join-Zone -Passphrase -PrimaryController

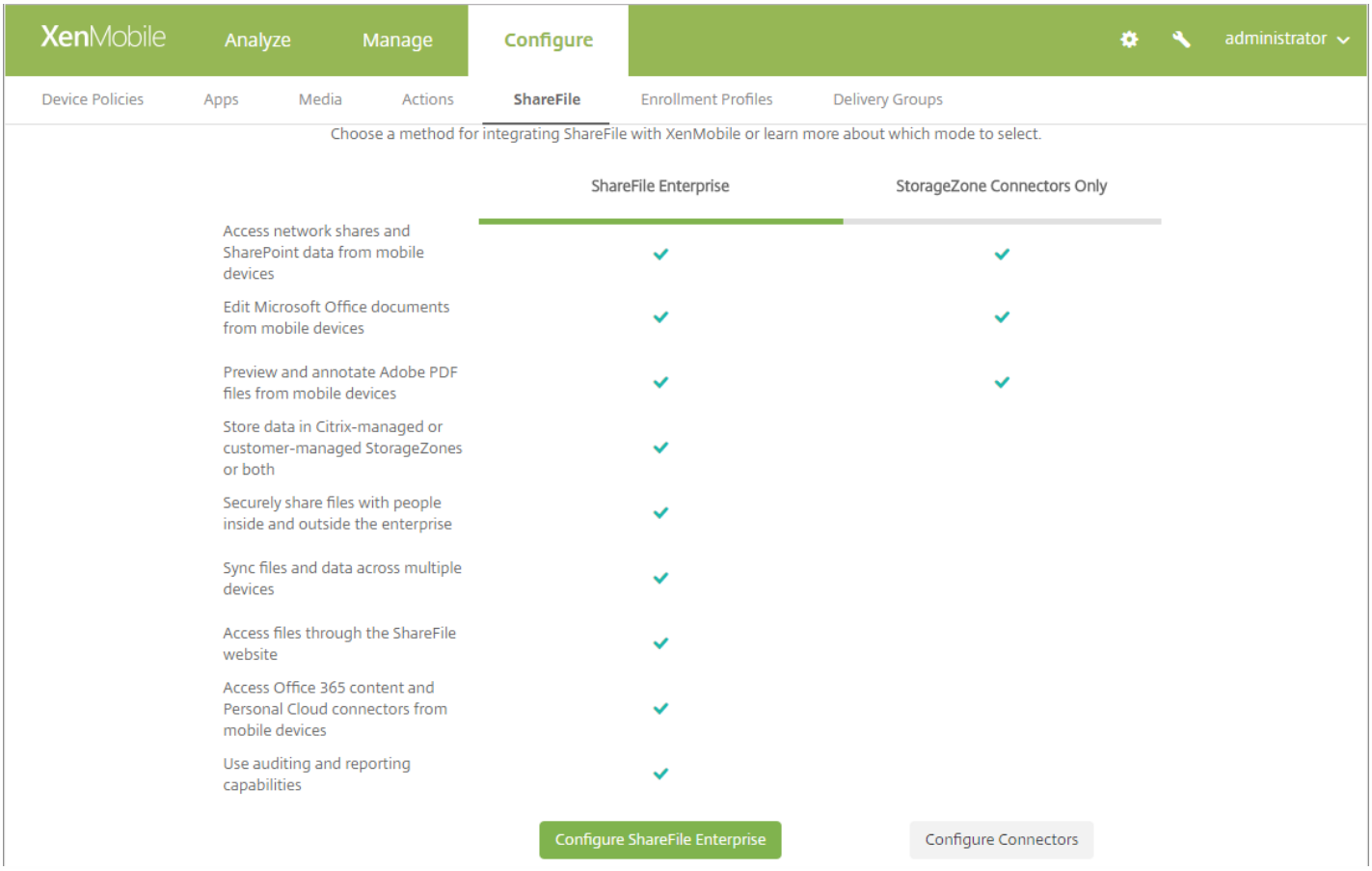
次に例を示します。

Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210

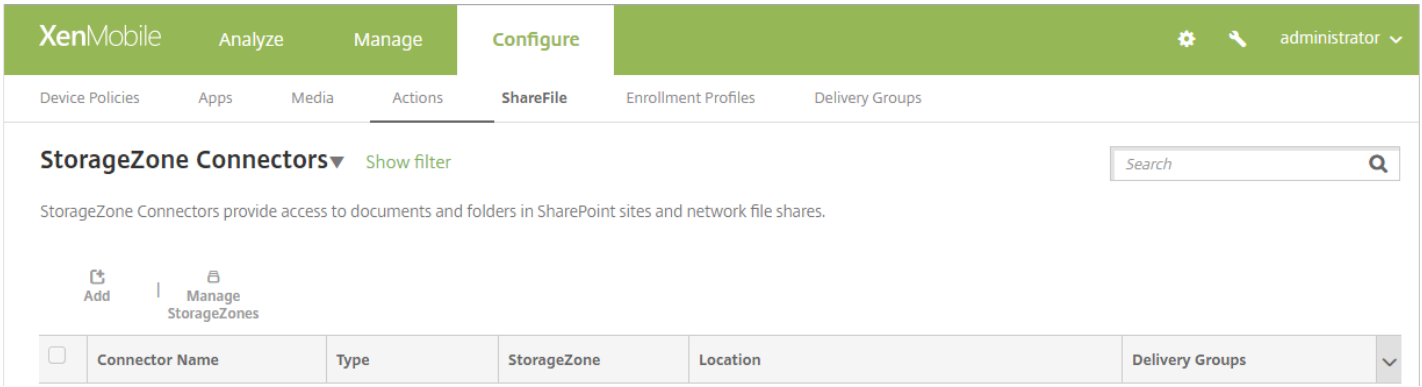
XenMobileでStorageZonesコントローラ接続を定義する

StorageZonesコネクタを追加する前に、StorageZonesコネクタに対して有効なStorageZonesコントローラごとに接続情報を構成します。このセクションの説明通りにStorageZonesコントローラを定義してください。つまり、コネクタを追加する場合の手順は以下の通りです。

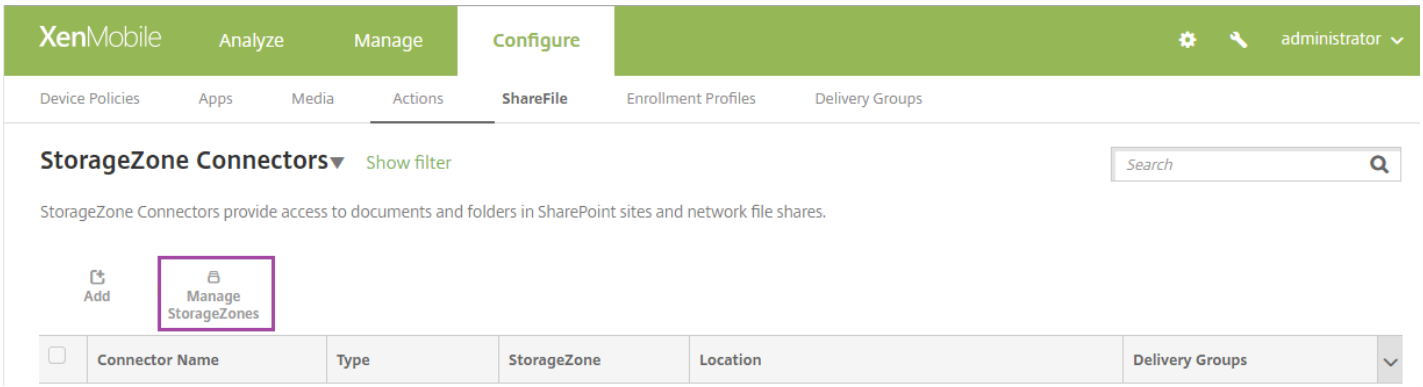
初めて**[構成] > [ShareFile]**の順にアクセスすると、XenMobileをShareFile Enterpriseと組み合わせた場合とStorageZoneコネクタと組み合わせた場合との差異の要約が表示されます。



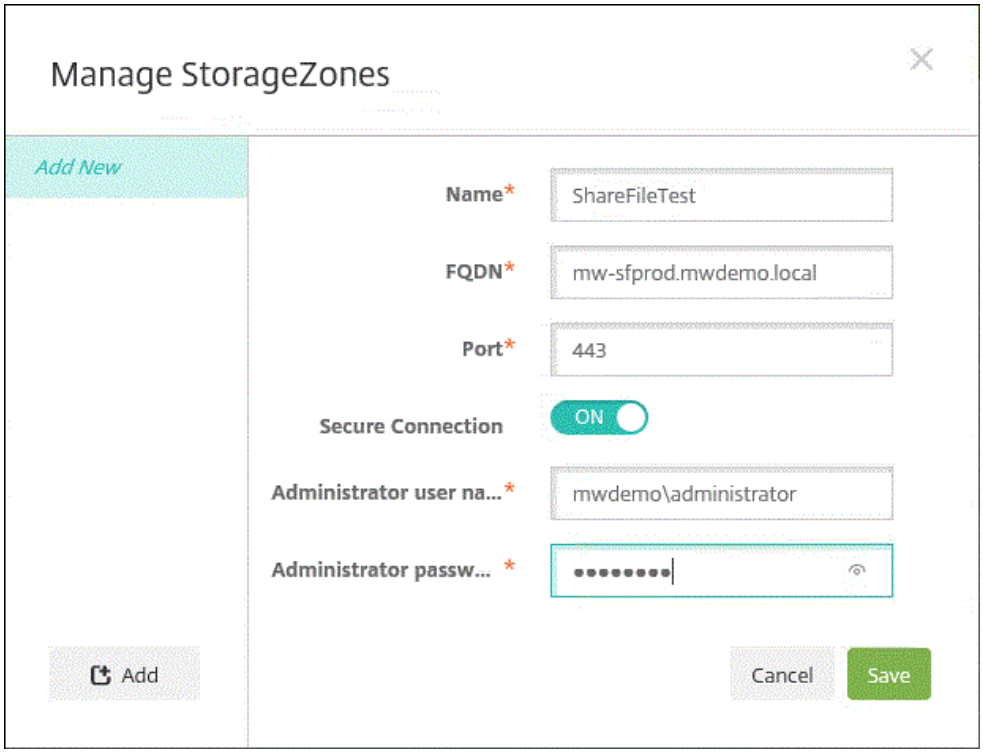
[コネクタの構成] をクリックしてこの記事の構成手順を進めます。



1. [構成] > [ShareFile] で、 [StorageZonesの管理] をクリックします。



2. [StorageZonesの管理] で接続情報を追加します。



- **名前**： StorageZoneの説明的な名前で、XenMobileでStorageZoneを識別するのに使用されます。名前に空白や特殊文字は含めないでください。
- **［FQDN］および［ポート］**：XenMobileサーバーからアクセス可能なStorageZones Controllerの完全修飾ドメイン名（FQDN）とポート番号。
- **セキュリティで保護された接続**：StorageZones Controllerとの接続にSSLを使用する場合は、デフォルト設定の［オン］を使用します。接続にSSLを使用しないのであれば、この設定を［オフ］に変更します。
- **［管理者ユーザー名］**と**［管理者パスワード］**：管理者サービスアカウントのユーザー名（domain\admin形式）とパスワード。または、StorageZones Controllerの読み取り権限と書き込み権限を持つユーザーアカウントを指定します。

3. **［保存］**をクリックします。

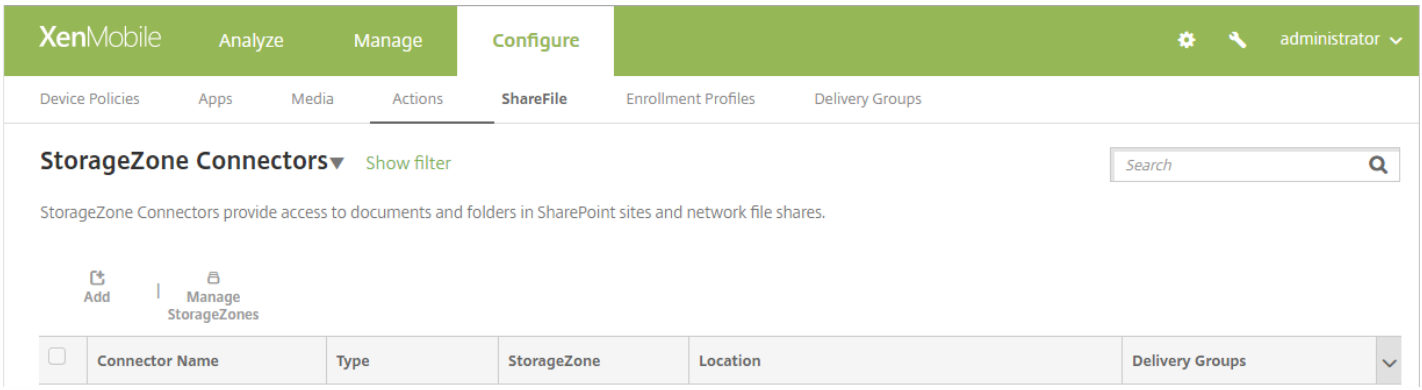
4. 接続をテストするために、XenMobileサーバーがポート443でStorageZones Controllerの完全修飾ドメイン名に接続できることを確認します。

5. 別のStorageZonesコントローラ接続を設定するには、**［StorageZonesの管理］**の**［追加］**ボタンをクリックします。

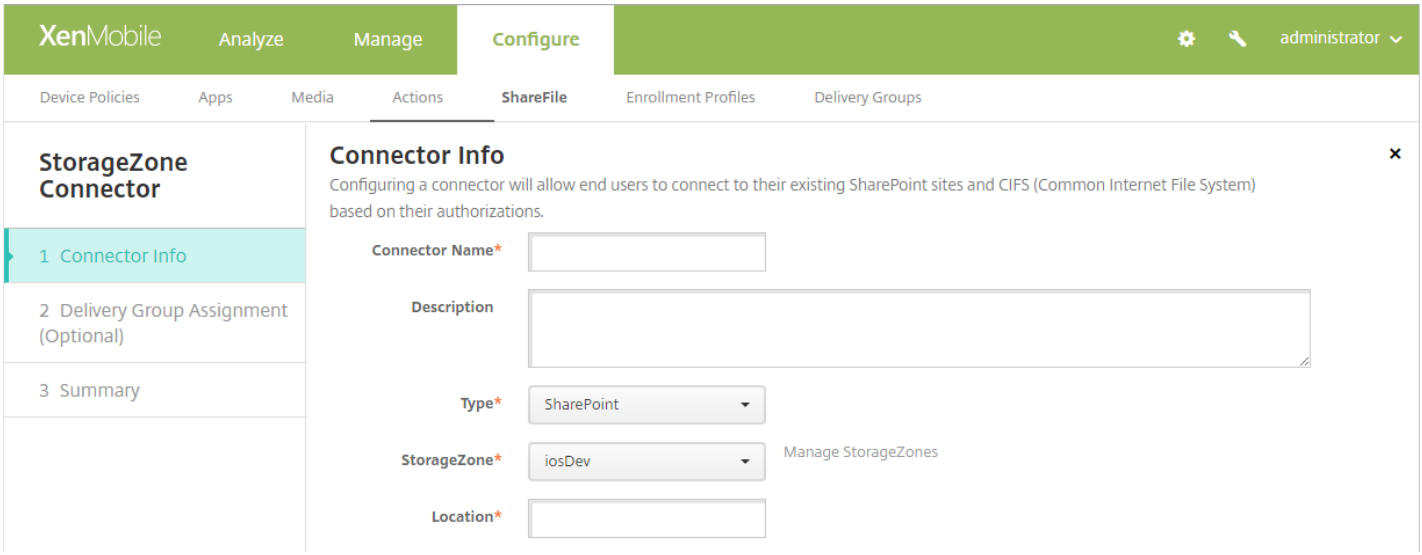
StorageZonesコントローラの接続情報を編集したり、削除するには、**［StorageZonesの管理］**で接続名を選択します。次に、**［編集］**または**［削除］**をクリックします。

XenMobileにStorageZoneコネクタを追加する

1. **［構成］＞［ShareFile］**の順にアクセスし、**［追加］**をクリックします。

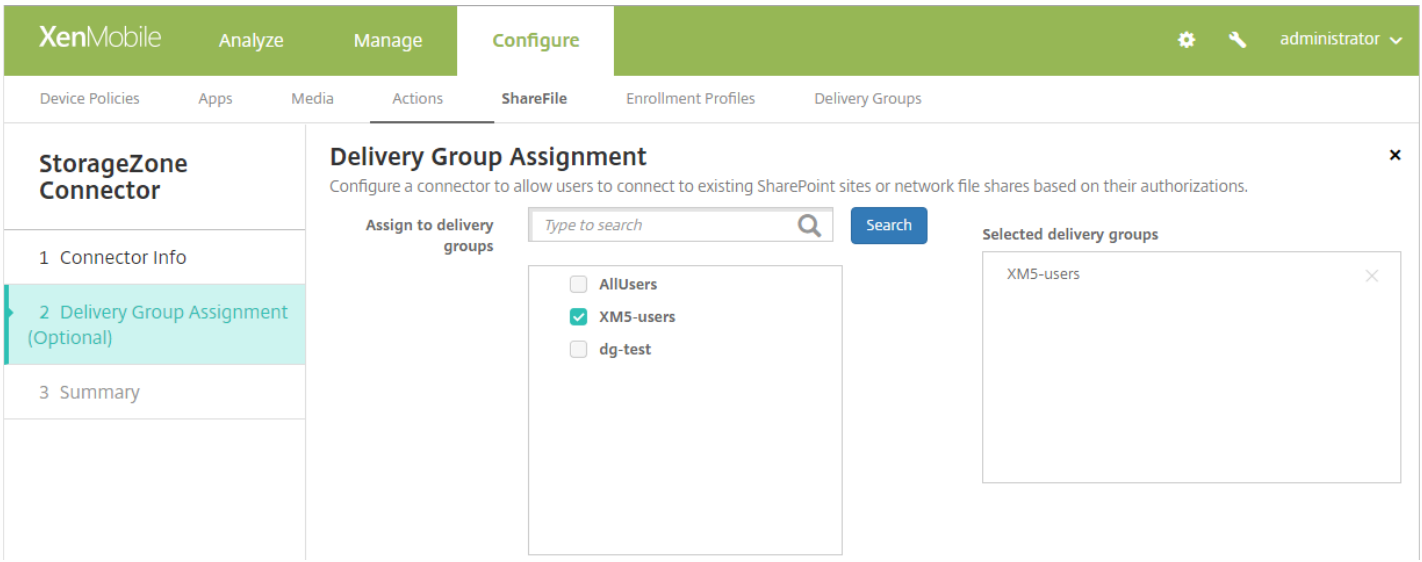


2. **［コネクタ情報］**ページで、以下の設定を構成します。



- **コネクタ名**： XenMobileでStorageZoneコネクタを識別する名前。
- **説明**： コネクタについての任意のメモ。
- **種類**： **[SharePoint]** または **[ネットワーク]** を選択します。
- **StorageZone**： コネクタに割り当てられたStorageZoneを選択します。StorageZoneが一覧に表示されていない場合は、 **[StorageZones の管理]** をクリックしてStorageZonesコントローラを設定します。
- **場所**： SharePointの場合、SharePointのルートレベルのサイト、サイトコレクション、またはドキュメントライブラリのURLをhttps://sharepoint.company.com形式で指定します。ネットワーク共有の場合、UNC（Uniform Naming Convention：汎用命名規則）パスの完全修飾ドメイン名を\\server\share形式で指定します。

3. **[デリバリーグループ割り当て]** ページで、任意で、コネクタをデリバリーグループに割り当てます。あるいは、**[構成] > [デリバリーグループ]** を使ってコネクタをデリバリーグループに関連付けることもできます。



4. **[概要]** ページで構成したオプションを確認できます。構成を修正する場合は、**[戻る]** をクリックします。

5. **[保存]** をクリックしてコネクタを保存します。

6. コネクタをテストします。

a. ShareFileクライアントをラップする場合は、次の操作を行います。

- Network accessポリシーを **[内部ネットワークへトンネル]** に設定します。

  この操作モードでは、ShareFileクライアントからのネットワークトラフィックがすべてXenMobile MDXフレームワークによりインターセプトされます。インターセプトされたトラフィックは、アプリ固有のMicro VPNによりNetScaler Gateway経由でリダイレクトされます。

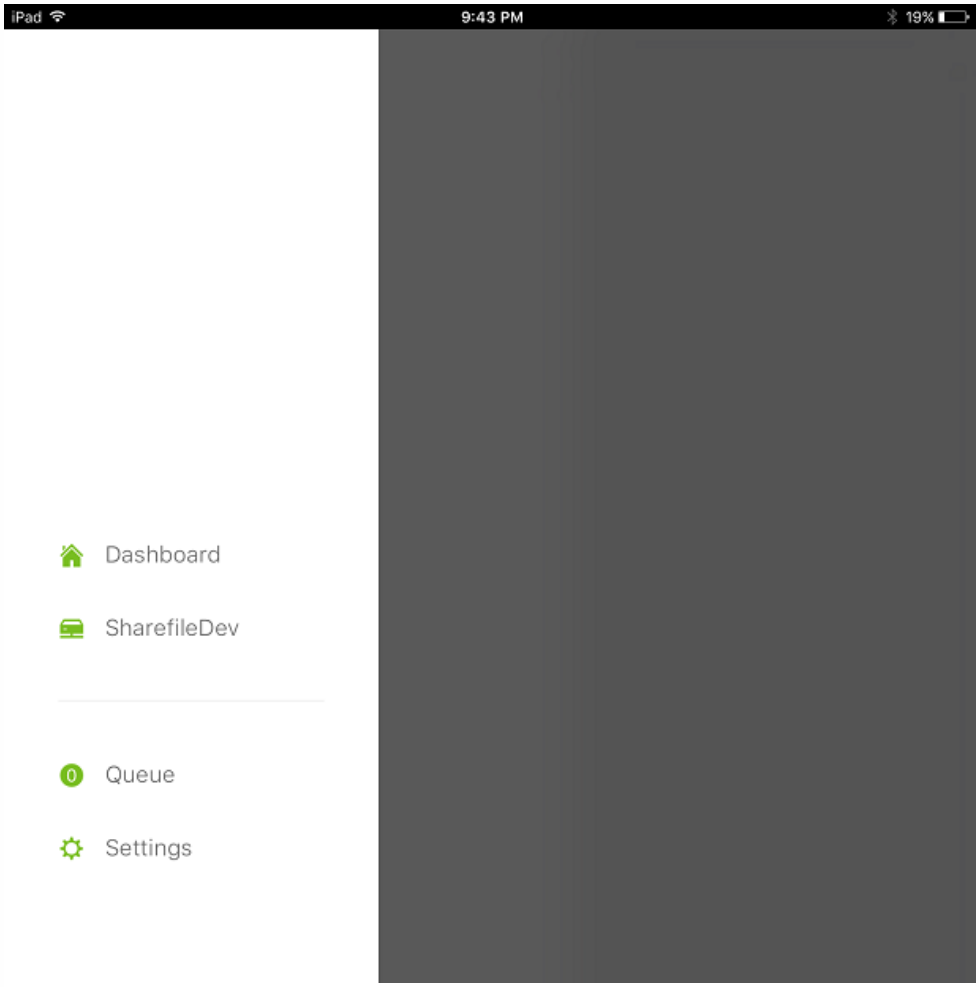
- Preferred VPN modeポリシーを **[セキュアブラウズ]** に設定します。

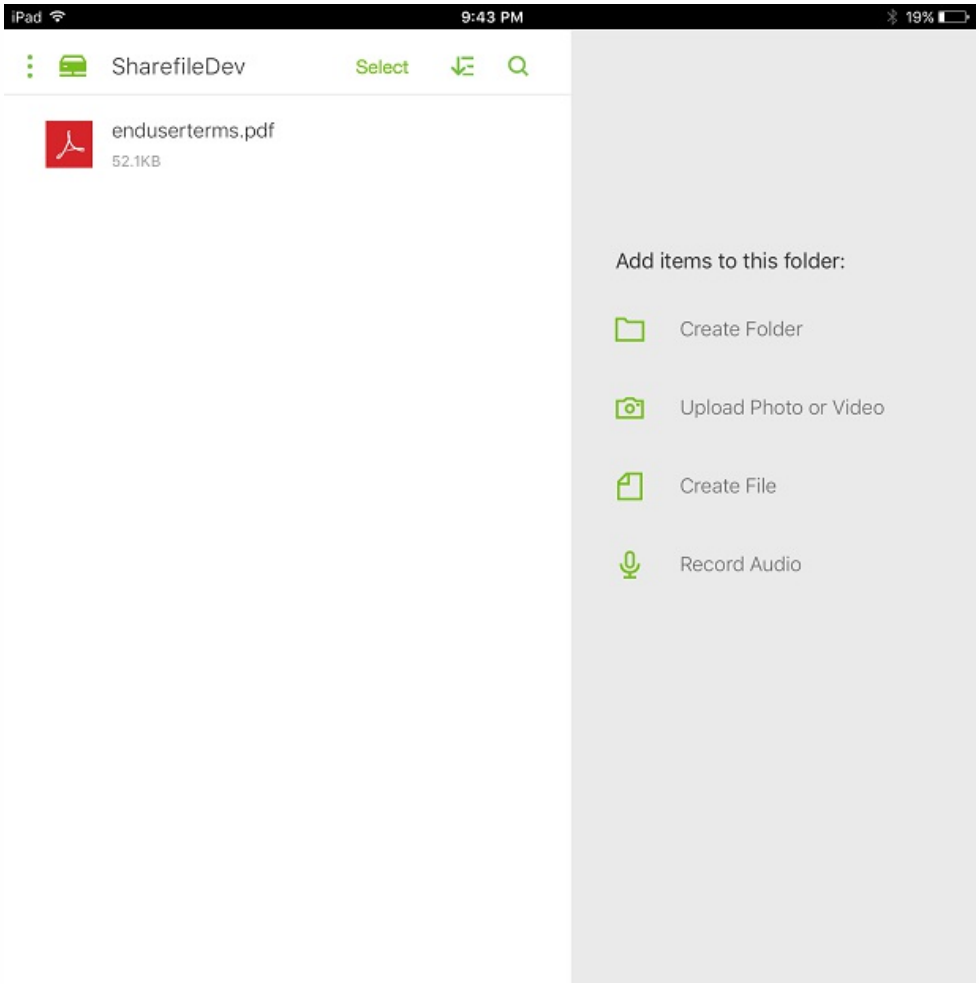
  このトンネルモードでは、MDXアプリからのSSL/HTTPトラフィックがMDXフレームワークによって終了されます。その後、ユーザーに代わってMDXにより内部接続に対する新しい接続が開始されます。このポリシー設定では、MDXフレームワークが、Webサーバーから発行された認証チャレンジを検出してそれに応答できます。

b. ShareFile クライアントをXenMobileに追加します。詳しくは、「To add ShareFile clients to XenMobile」を参照してください。

c. サポート対象のデバイスで、ShareFileおよびコネクタへのシングルサインオンを確認します。

次の例のSharefileDevはコネクタの名前です。

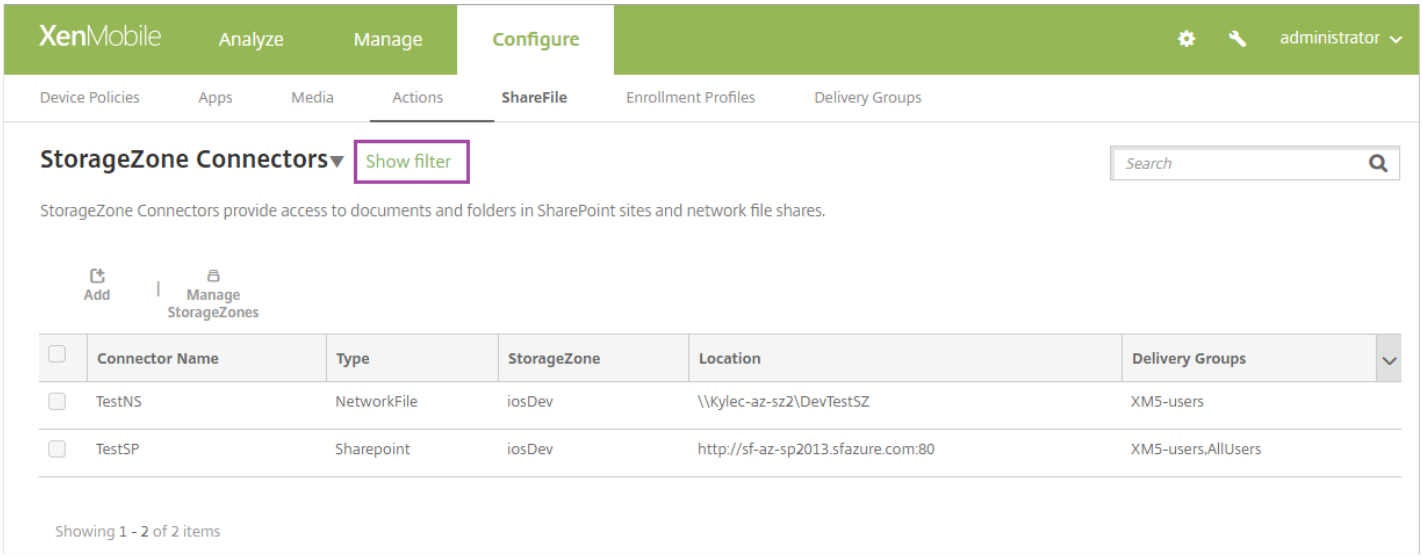




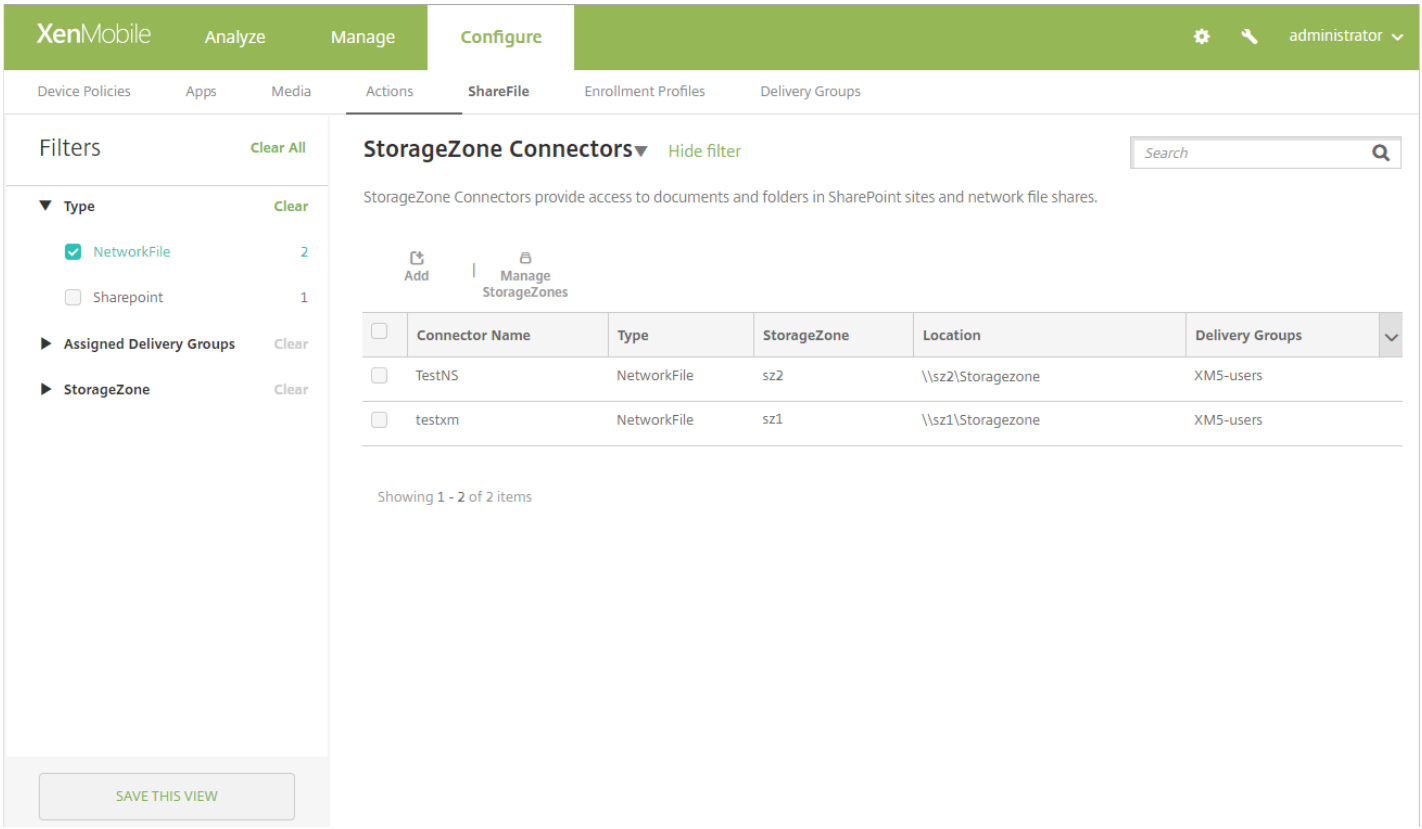
StorageZoneコネクター一覧をフィルターする

StorageZoneコネクター一覧は、コネクタの種類、割り当てられたデリバリーグループ、StorageZoneによってフィルターできます。

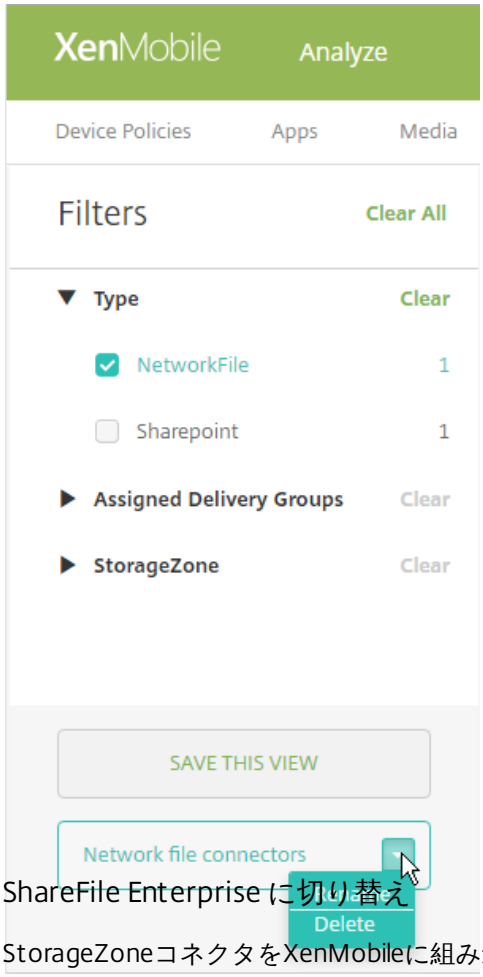
1. **[構成] > [ShareFile]** の順にアクセスし、**[フィルターを表示]** をクリックします。



2. フィルターの見出しを展開して、項目を選択します。フィルターを保存するには、**[このビューを保存]** をクリックして、フィルター名を入力し **[保存]** をクリックします。



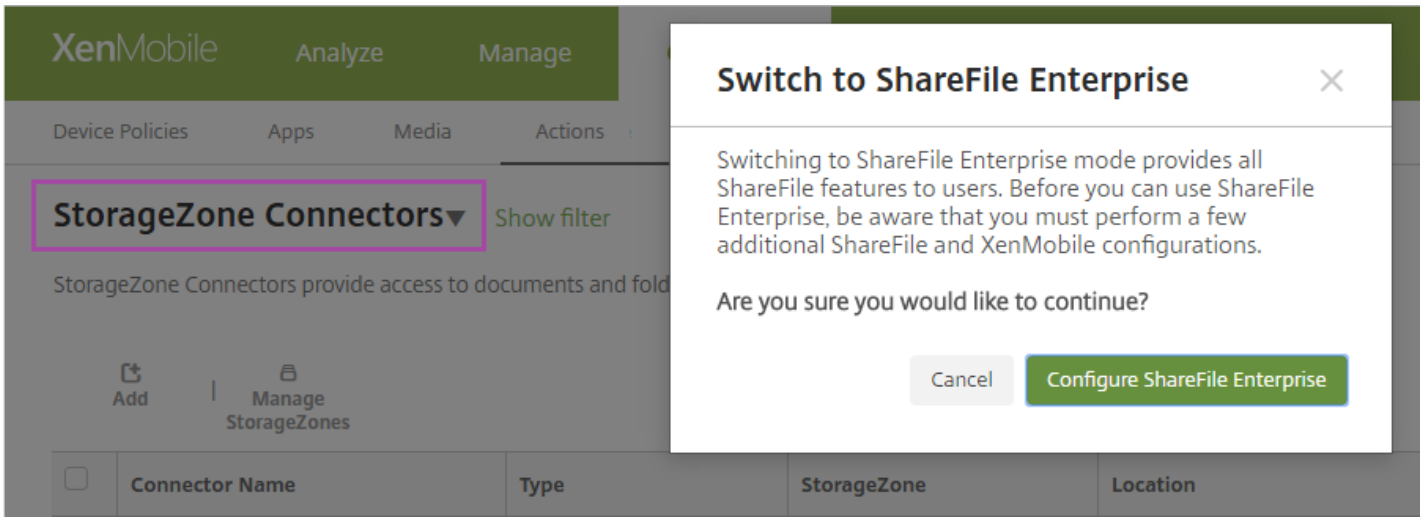
3. フィルターの名前を変更したり削除するには、フィルター名の横の矢印アイコンをクリックします。



ShareFile Enterpriseに切り替え

StorageZoneコネクタをXenMobileに組み込んだ後で、完全なShareFile Enterprise機能セットに切り替えられます。ShareFile Enterprise機能セットを使用するには、XenMobile Enterprise Editionが必要です。XenMobileは、既存のStorageZoneコネクタの統合設定を保持しています。

［構成］ > ［ShareFile］の順にアクセスし、**［StorageZoneコネクタ］**ドロップダウンメニューを選択して、**［ShareFile Enterpriseの構成］**をクリックします。



ShareFile Enterpriseの構成については、「ShareFileでのSAMLによるシングルサインオン」を参照してください。

HDXアプリ向けSmartAccess

Feb 27, 2017

この機能により、デバイスプロパティ、デバイスのユーザープロパティ、デバイスにインストールされたアプリケーションに基づいてHDXへのアクセスを制御できます。この機能を使用するには、そのデバイスをコンプライアンス違反に指定するよう自動化された操作を設定して、そのデバイスのアクセスを拒否します。この機能を使用するHDXアプリをXenAppとXenDesktopに構成するには、コンプライアンス違反のデバイスへのアクセスを拒否するSmartAccessポリシーを使います。XenMobileは、署名された暗号化タグを使って、StoreFrontにデバイスの状態を伝えます。次にStoreFrontは、アプリのアクセス制御ポリシーに基づいてアクセスを許可または拒否します。

この機能を使用するには、展開に次の製品が必要です。

- XenAppおよびXenDesktop 7.6
- StoreFront 3.7または3.8
- StoreFrontサーバーからHDXアプリを収集するよう構成されたXenMobileサーバー
- タグの署名や暗号化に使用されるSAML証明書が設定されたXenMobileサーバー秘密キーなしの同じ証明書をStoreFrontサーバーにアップロードします。

この機能を使い始める手順は次のとおりです。

- XenMobileサーバーの証明書をStoreFrontストアに設定します
- 必要とされるSmartAccessポリシーに少なくとも１つのXenApp とXenDesktopデリバリーグループを設定します
- XenMobileに自動化された操作を設定します

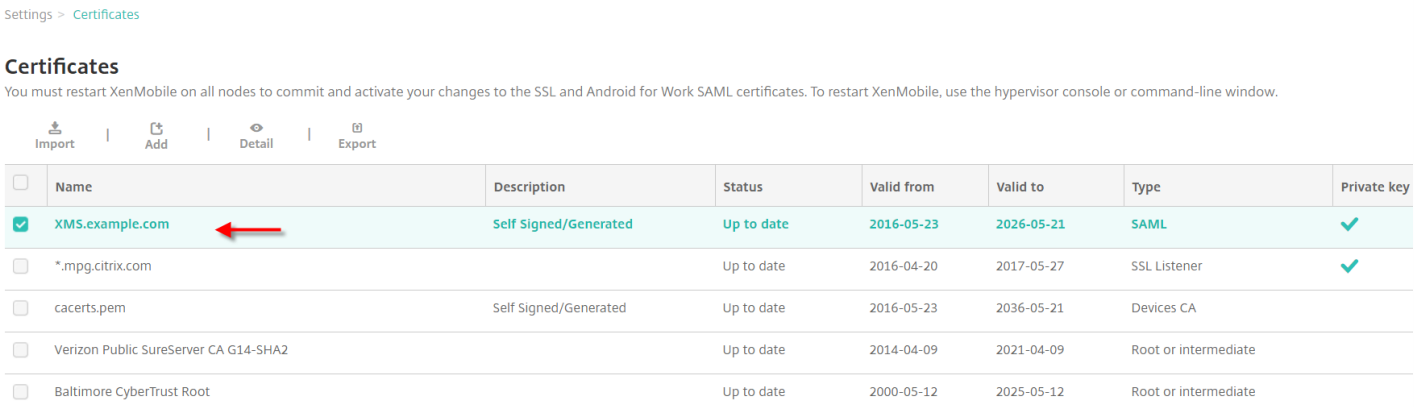
XenMobileサーバーの証明書をエクスポートし、構成して、StoreFrontストアにアップロードする

SmartAccessは、署名された暗号化タグを使ってXenMobileとStoreFrontサーバー間で通信します。この通信を有効にするには、XenMobileのサーバー証明書をStoreFrontストアに追加します。

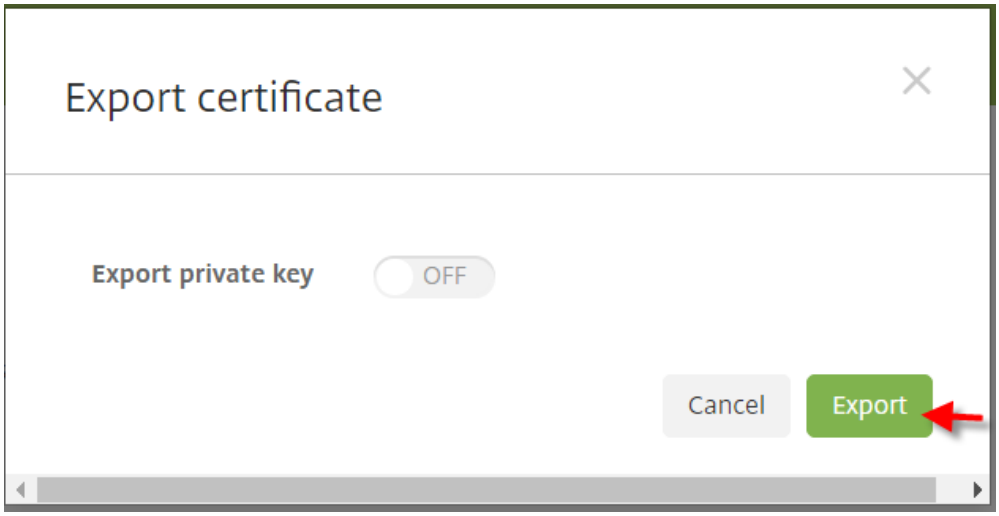
SAML証明書をXenMobileサーバーからエクスポートする

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

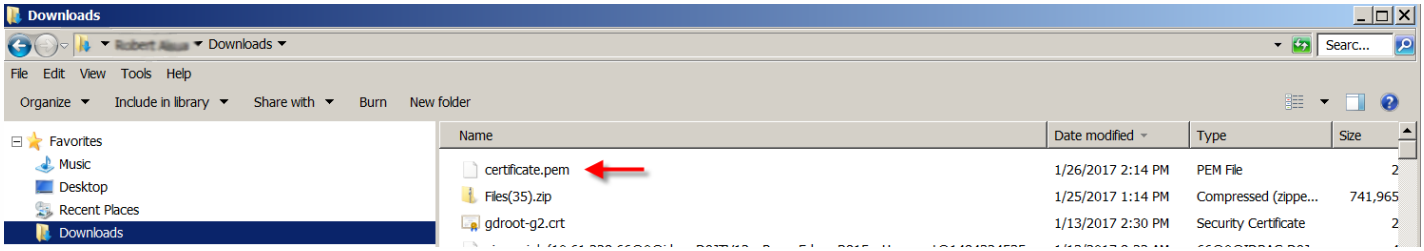
2. XenMobileサーバーのSAML証明書を指定します。



3. **[機密キーをエクスポート]** が **[オフ]** に設定されていることを確認します。**[エクスポート]** をクリックして、証明書をダウンロードディレクトリにエクスポートします。

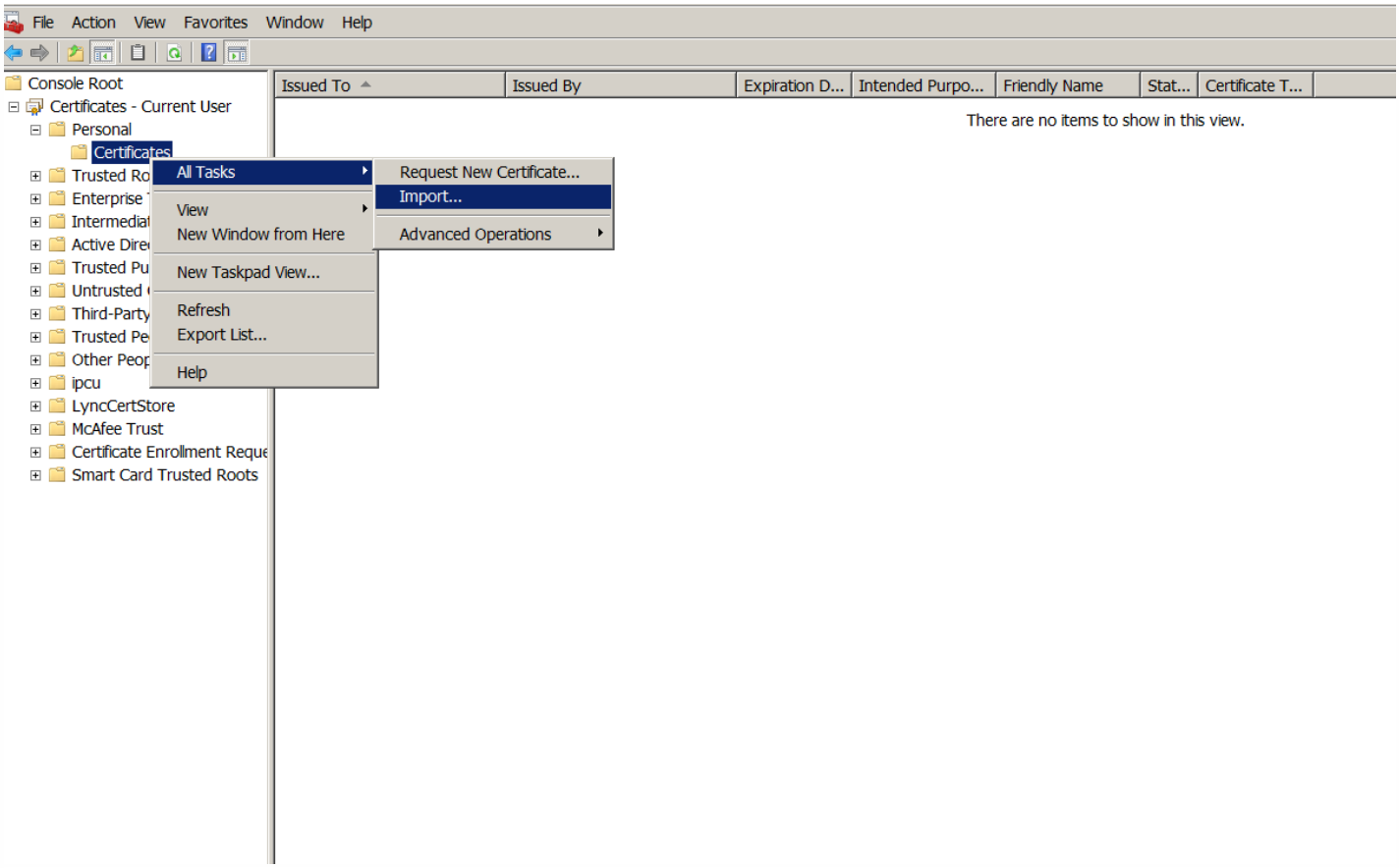


4. ダウンロードディレクトリで証明書を指定します。証明書はPEM形式です。



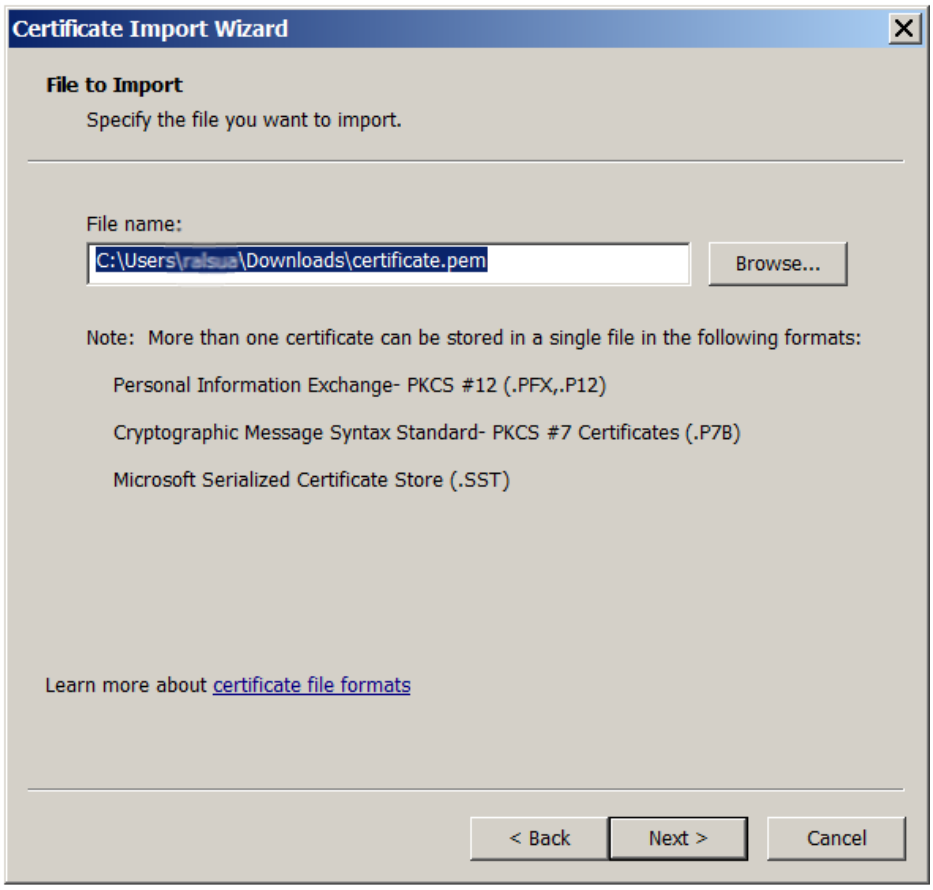
証明書をPEMからCERに変換する

1. Microsoft 管理コンソール（MMC）を開き、右クリックして **[証明書] > [すべてのタスク] > [インポート]** の順に選択します。

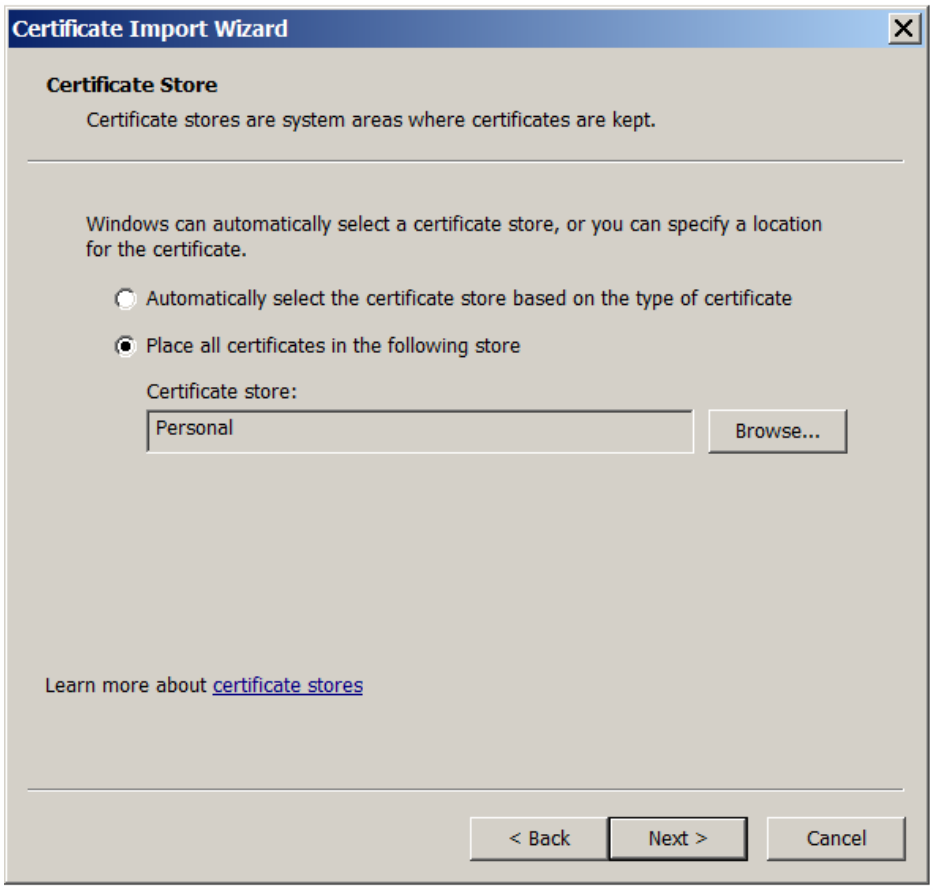


2. [証明書のインポートウィザード] ページが開いたら、**[次へ]** をクリックします。

3. ダウンロードディレクトリで証明書を参照します。

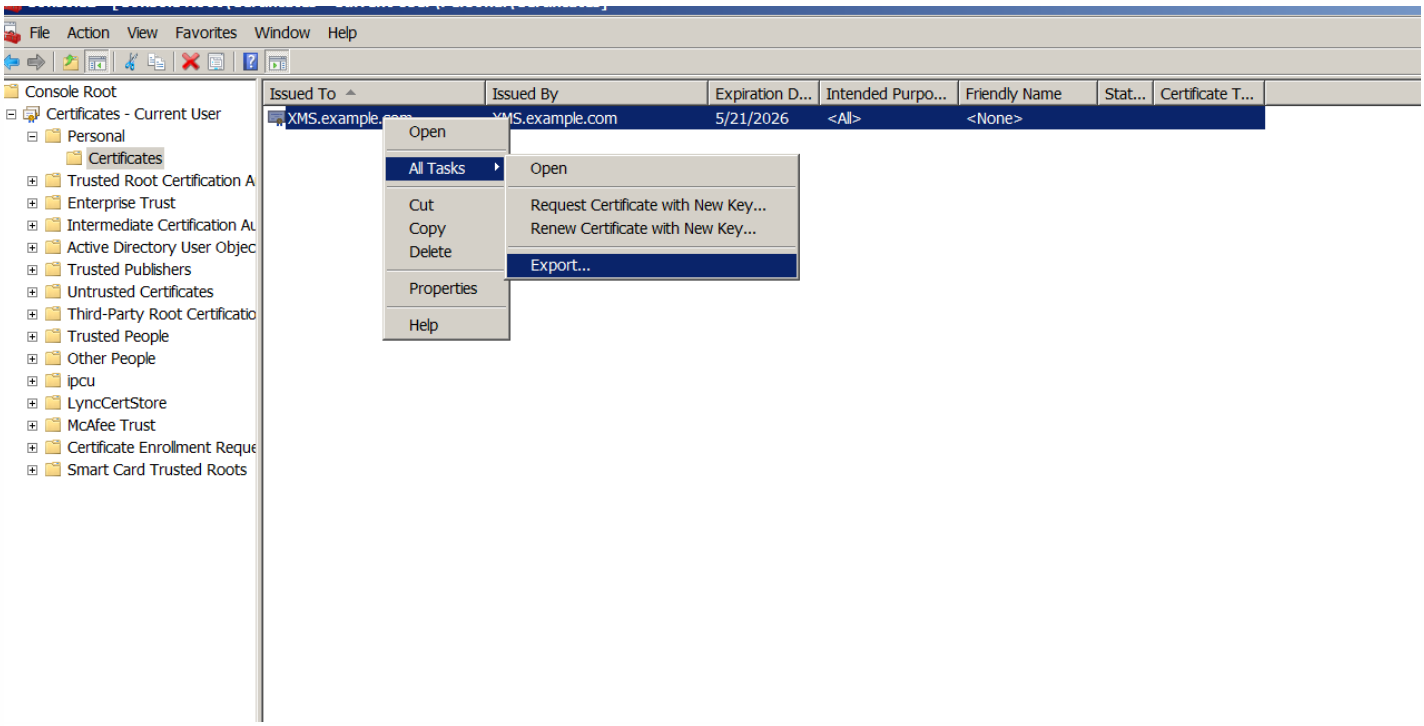


4. **[証明書をすべて次のストアに配置する]** を選択し、証明書ストアとして **[個人]** を選択します。 **[次へ]** をクリックします。



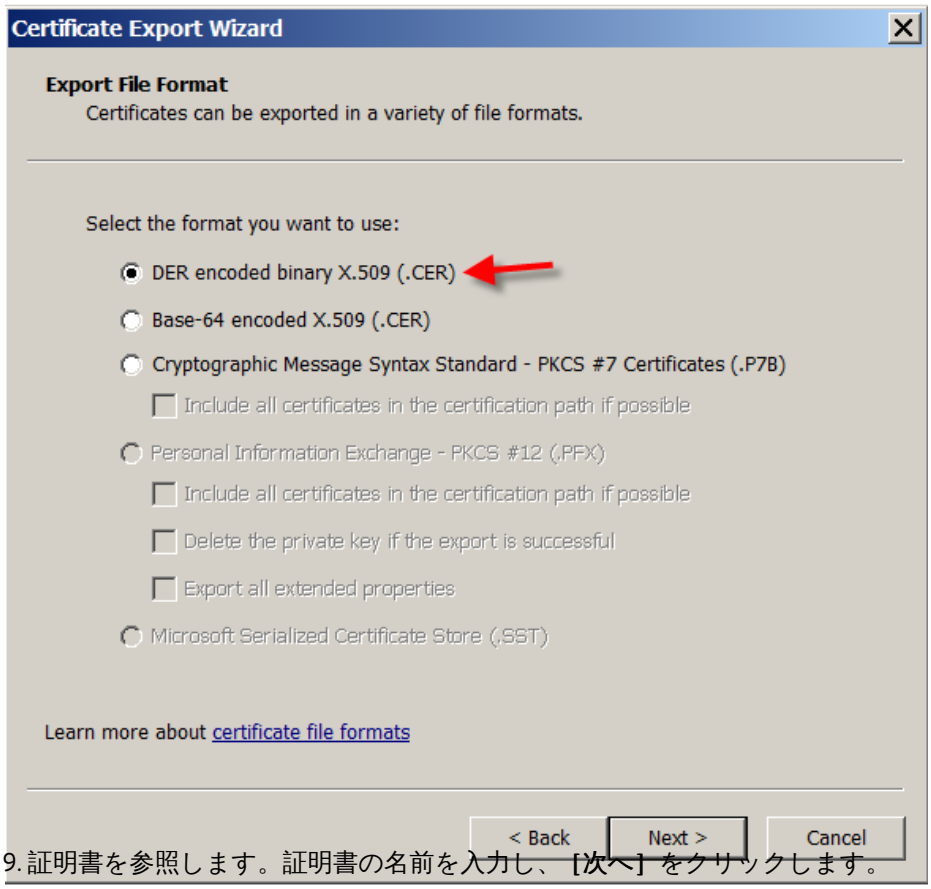
5. 選択を確認して［**完了**］をクリックします。［**OK**］をクリックして、確認画面を閉じます。

6. MMCで、証明書を右クリックし、［**すべてのタスク**］**>**［**エクスポート**］の順に選択します。

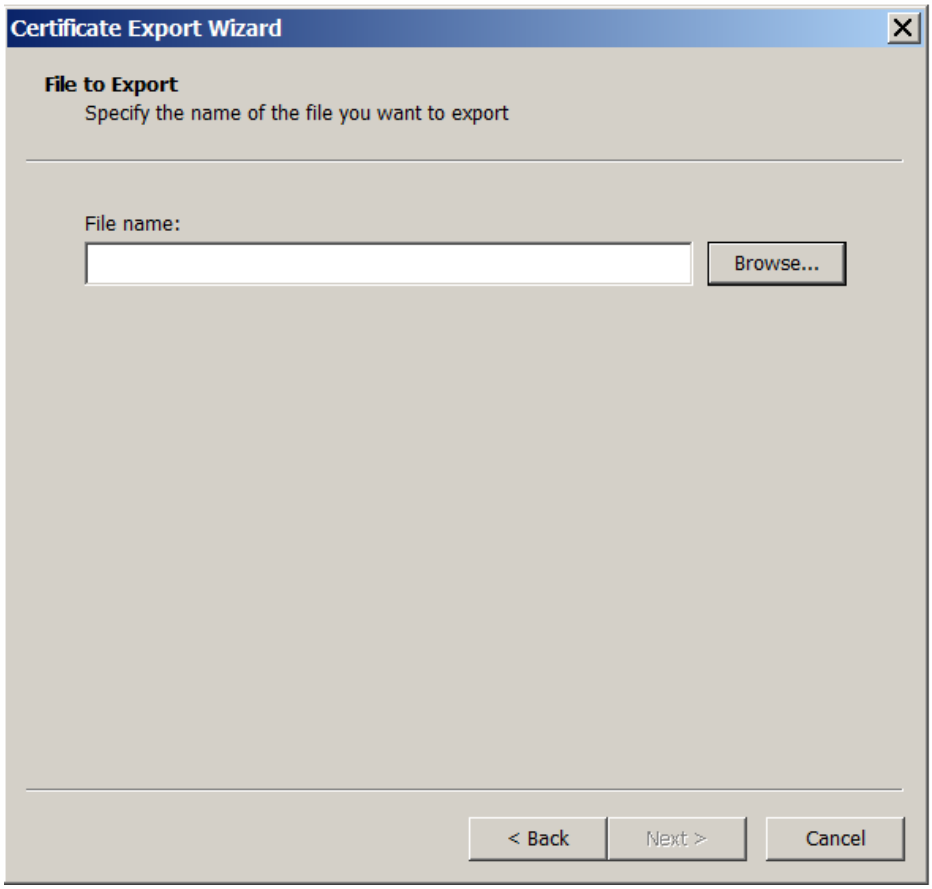


7. ［証明書のエクスポートウィザード］ページが開いたら、［**次へ**］をクリックします。

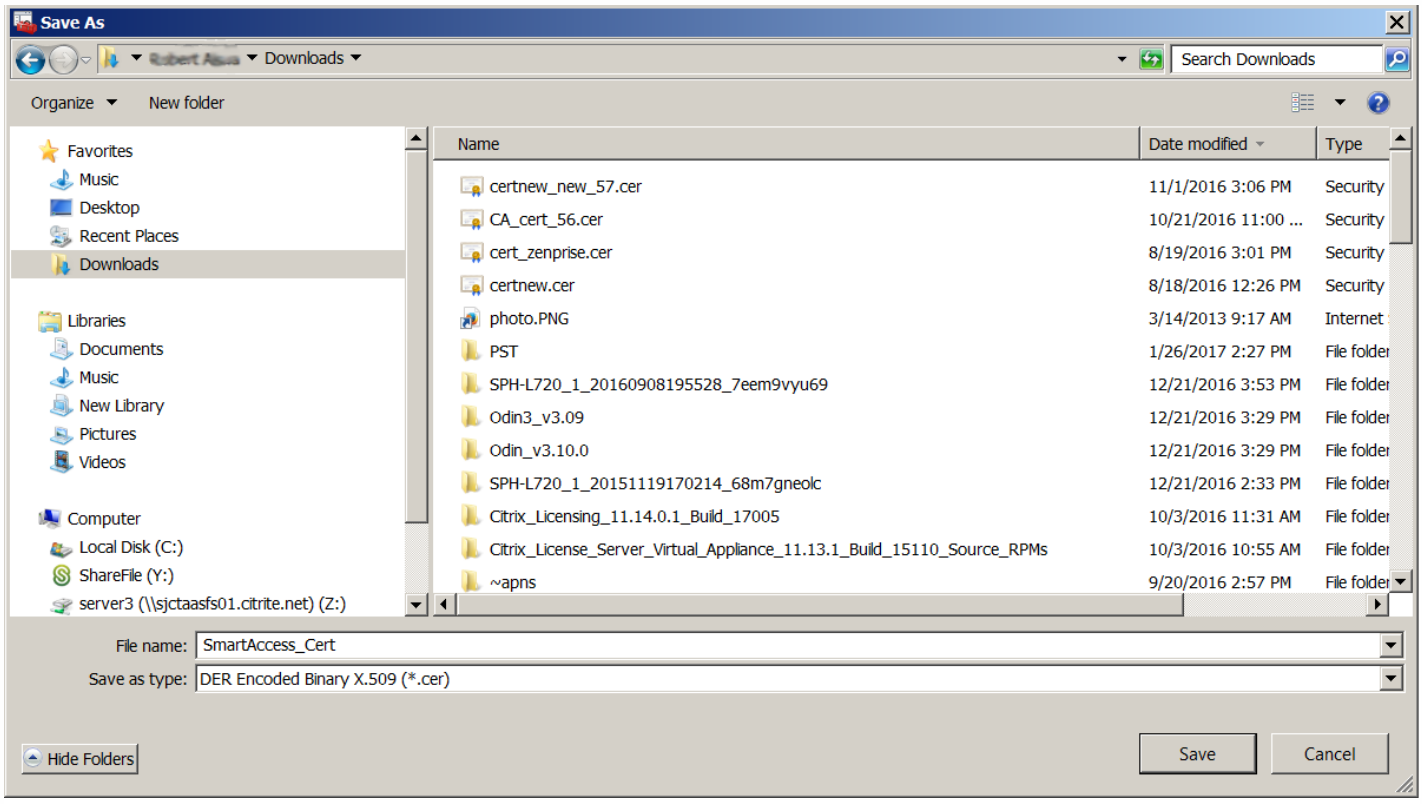
8. [**DER encoded binary X.509 (.CER)**] 形式を選択します。 [**次へ**] をクリックします。



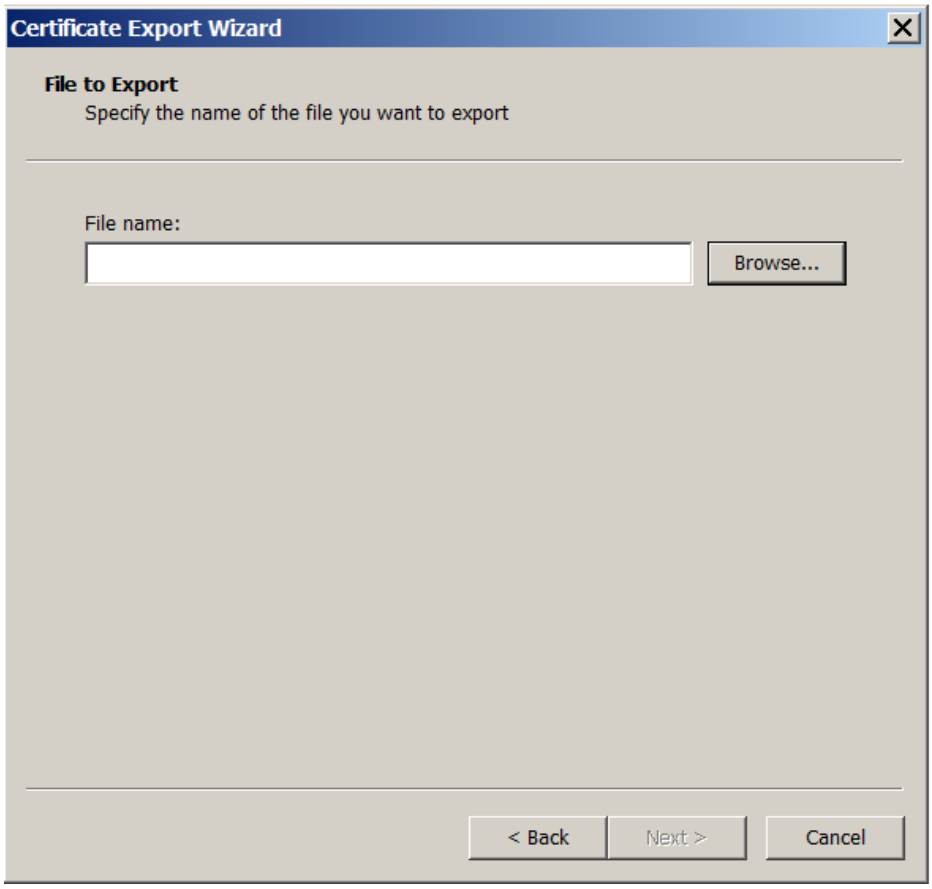
9. 証明書を参照します。証明書の名前を入力し、[次へ] をクリックします。



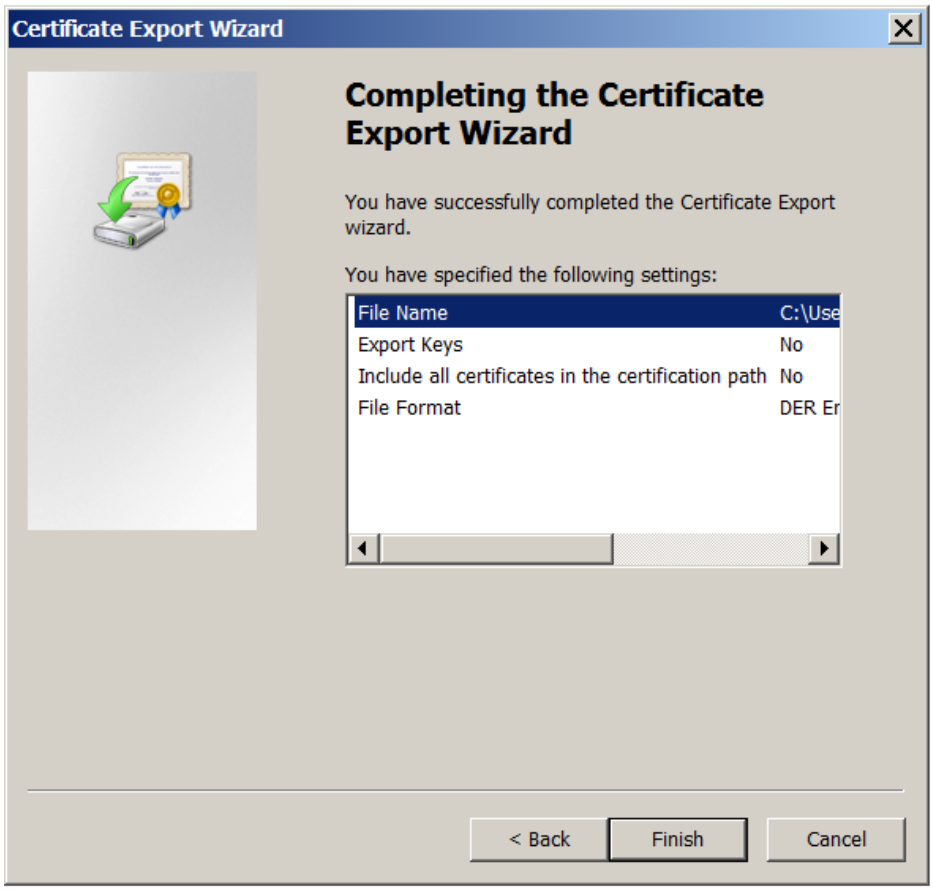
10. 証明書を保存します。



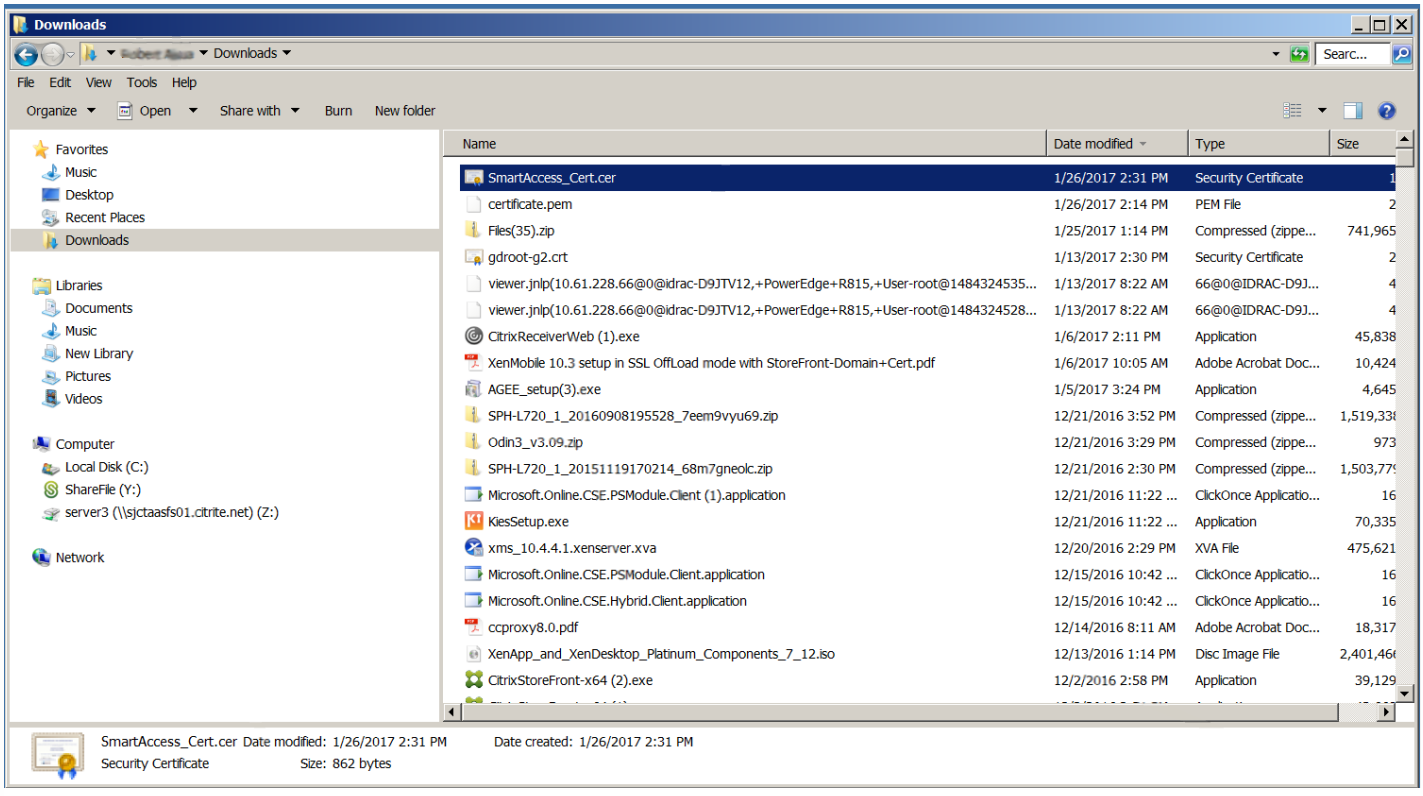
11. 証明書を参照して、 **[次へ]**



12. 選択を確認して **[完了]** をクリックします。 **[OK]** をクリックして、確認画面を閉じます。



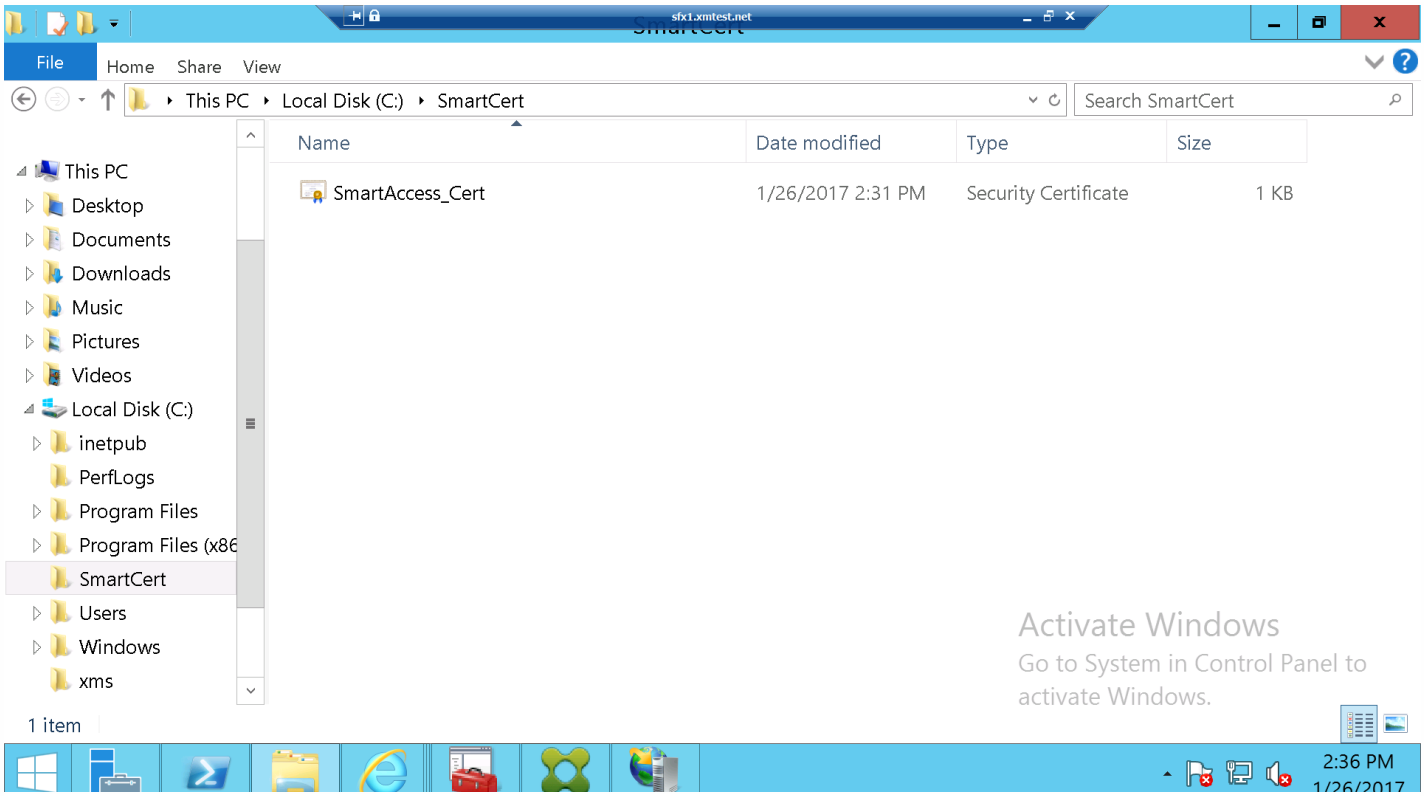
13. ダウンロードディレクトリで証明書を指定します。証明書がCER形式であることに注意してください。



証明書をStoreFrontサーバーにコピーする

1. StoreFrontサーバー側で、**SmartCert**という名前のフォルダーを作成します。

2. 証明書を**SmartCert**フォルダーにコピーします。

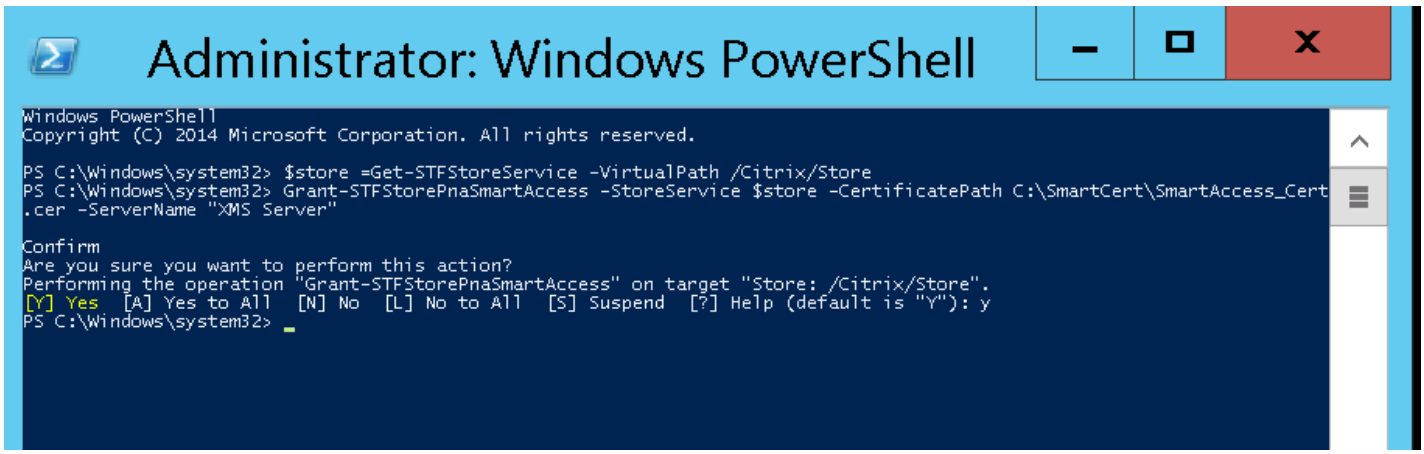


StoreFrontストアに証明書を設定する

StoreFrontサーバーで、次のとおりPowerShellコマンドを実行し、変換されたXenMobileサーバー証明書をストアに設定します。

-command コピー

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath “C:\xms\xms.cer” –ServerName “XMS server”
```



StoreFrontストアに既存の証明書が存在する場合は、次のPowerShellコマンドを実行して証明書を無効にします。

```
-command

Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

あるいは、次のいずれかのPowerShellコマンドをStoreFrontサーバーで実行してStoreFrontストアの既存の証明書を無効にすることもできます。

- サーバー名で無効化：

```
-command

$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server”
```

- 拇印で無効化：

```
-command

$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “1094821dec7834d5d42 bb456329efe4fca86c60b”
```

- サーバーオブジェクトで無効化：

```
-command
```

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess –StoreService $store

Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

XenAppとXenDesktopのSmartAccessポリシーの設定

必要なSmartAccessポリシーをHDXアプリを配信するデリバリーグループに追加するための手順は次のとおりです。

1. XenAppとXenDesktopサーバーで、Citrix Studioを開きます。

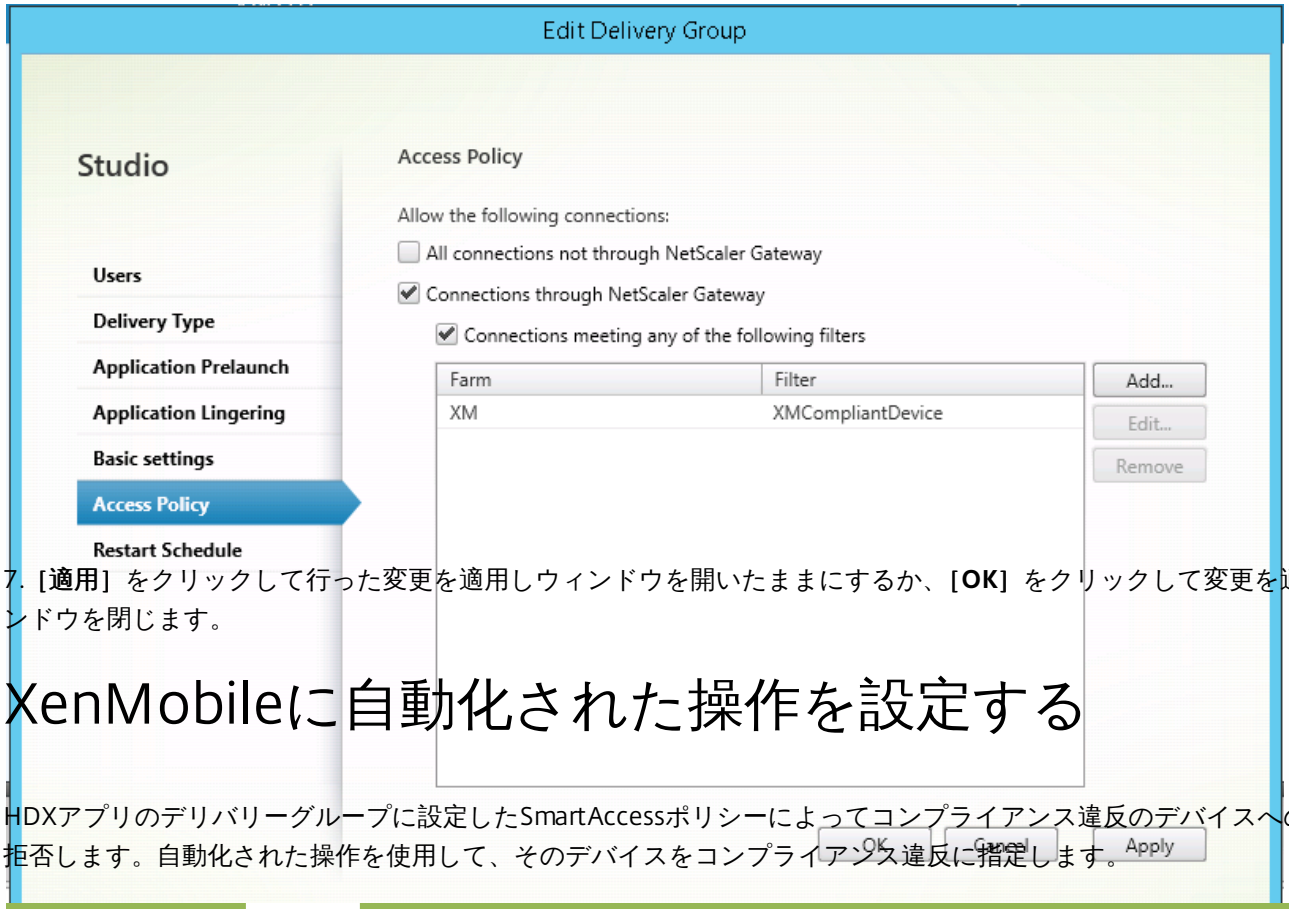
2. Studioのナビゲーションペインで **[デリバリーグループ]** を選択します。

3. アプリを配信するグループまたはアクセス制御したいアプリを選択します。**[操作]** ペインの **[デリバリーグループの編集]** を選択します。

4. **[アクセスポリシー]** ページで、 **[NetScaler Gatewayを経由する接続]** チェックボックスと **[次のフィルターのいずれかに一致する接続]** チェックボックスをオンにします。

5. **[Add]** をクリックします。

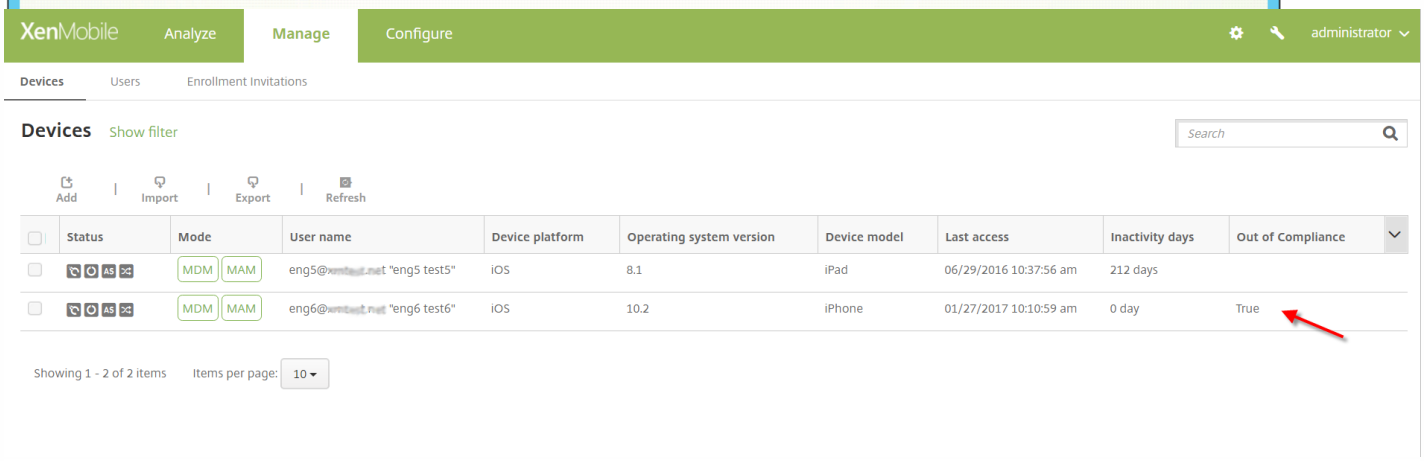
6.**Farm**が**XM**で**Filter**が**XMCompliantDevice**のアクセスポリシーを追加します。



7. **[適用]** をクリックして行った変更を適用しウィンドウを開いたままにするか、**[OK]** をクリックして変更を適用しウィンドウを閉じます。

XenMobileに自動化された操作を設定する

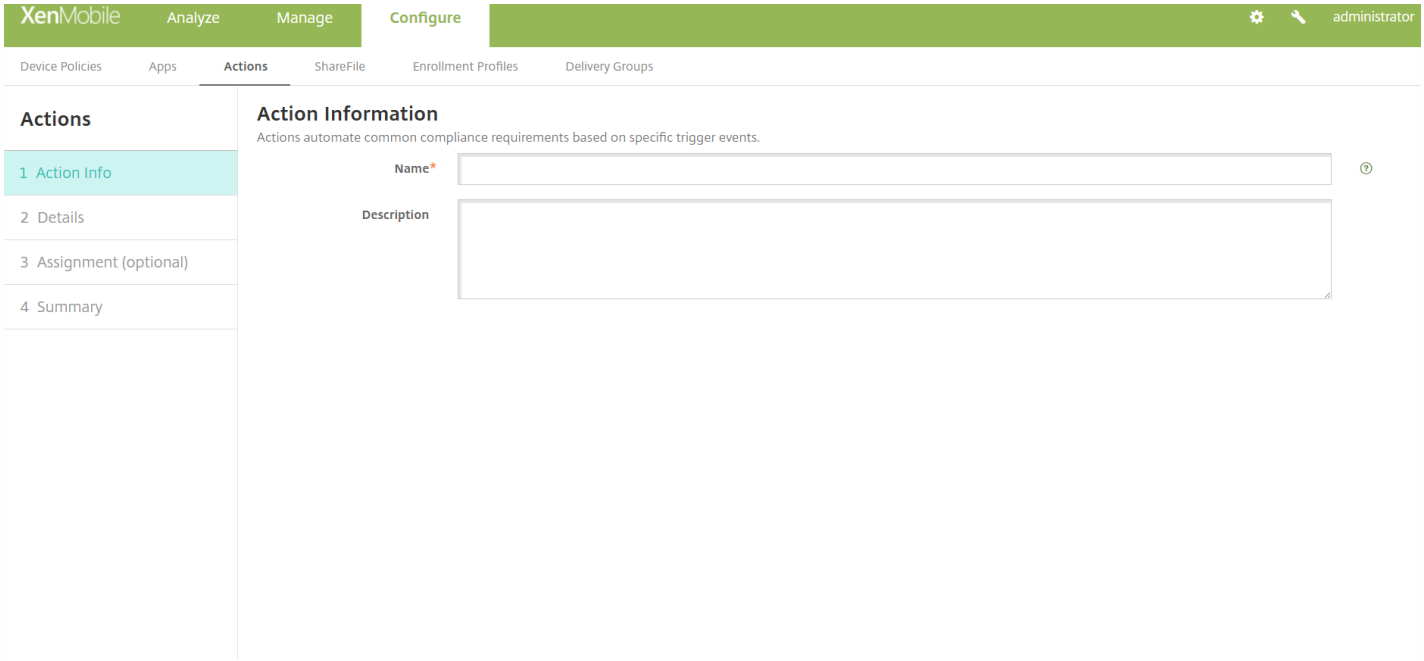
HDXアプリのデリバリーグループに設定したSmartAccessポリシーによってコンプライアンス違反のデバイスへのアクセスを拒否します。自動化された操作を使用して、そのデバイスをコンプライアンス違反に指定します。



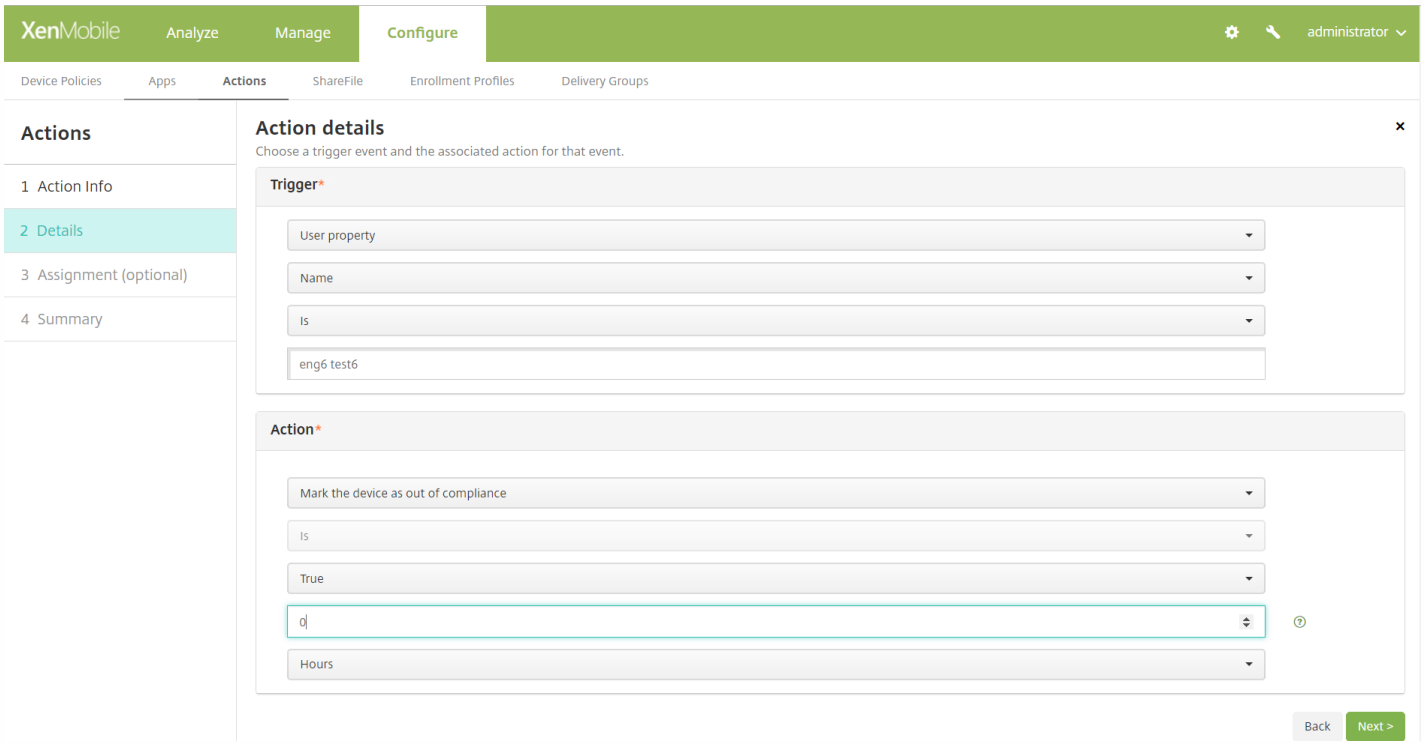
1. XenMobileコンソールで、**[構成]** > **[操作]** をクリックします。**[操作]** ページが開きます。

2. 操作を追加するには **[追加]** をクリックします。**[アクション情報]** ページが開きます。

3. **[アクション情報]** ページで、操作の名前と説明を入力します。



4. **[次へ]** をクリックします。 **[アクションの詳細]** ページが開きます。次の例では、デバイスのユーザープロパティ名が**eng5**または**eng6**の場合に、直ちにコンプライアンス違反に指定するトリガーが作成されます。



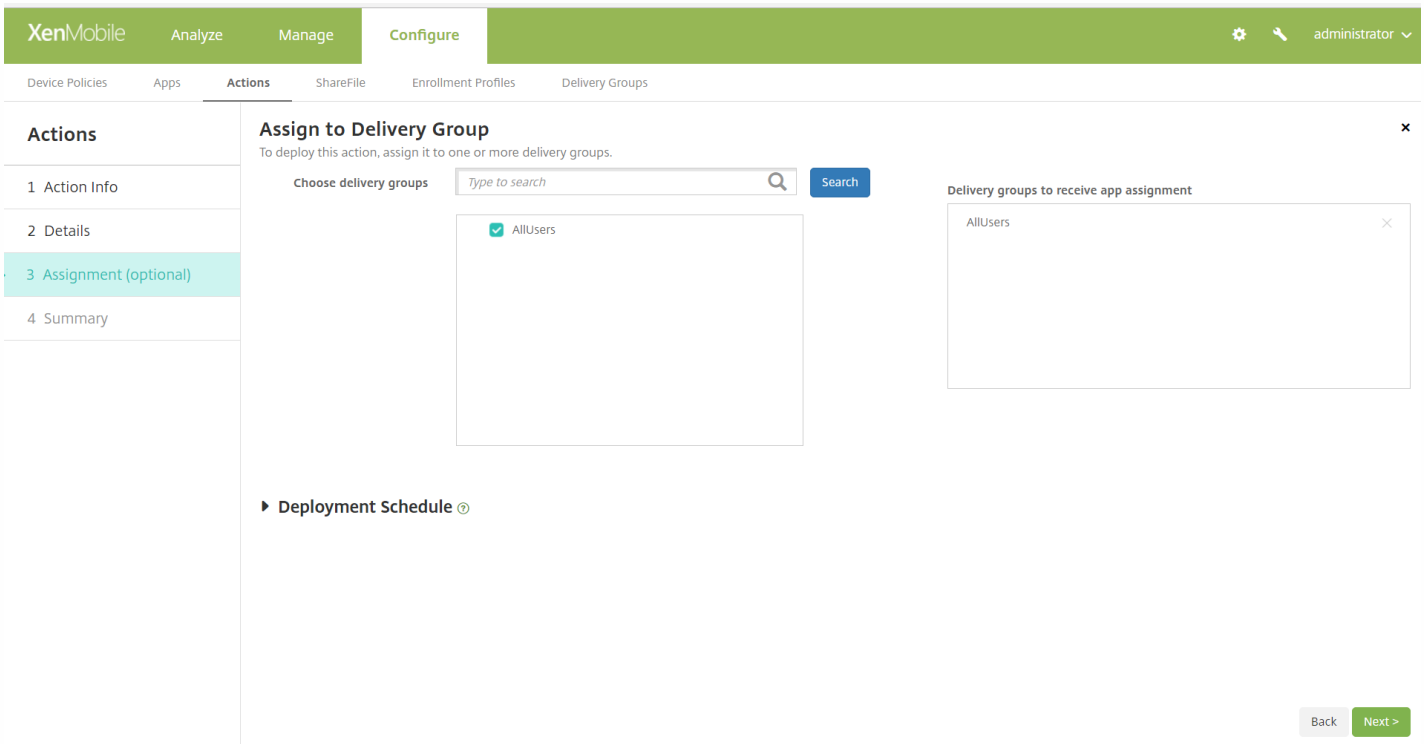
5. **[トリガー]** 一覧で **[デバイスプロパティ]** 、 **[ユーザープロパティ]** 、 **[インストール済みアプリ名]** から選択します。SmartAccessは、イベントトリガーをサポートしていません。

6. **[アクション]** 一覧で次のように設定します。

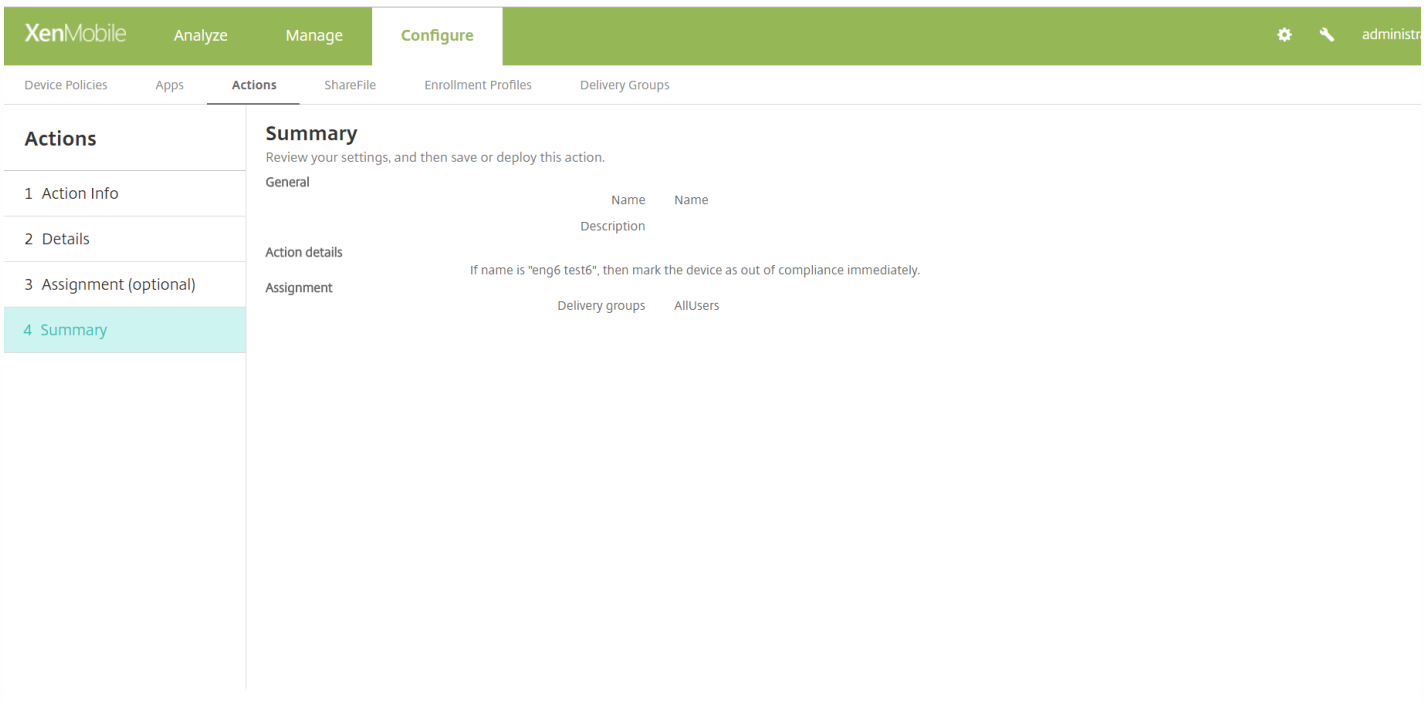
- **[コンプライアンス違反としてデバイスをマーク]** を選択。

- =を選択。
- 真を選択。
- トリガー条件に合致した場合に、直ちにデバイスをコンプライアンス違反に指定するよう操作を設定するために、タイムフレームを**0**に設定。

7. XenMobileデリバリーグループまたはこの操作を適用するグループを選択します。



8. アクションの概要を確認します。

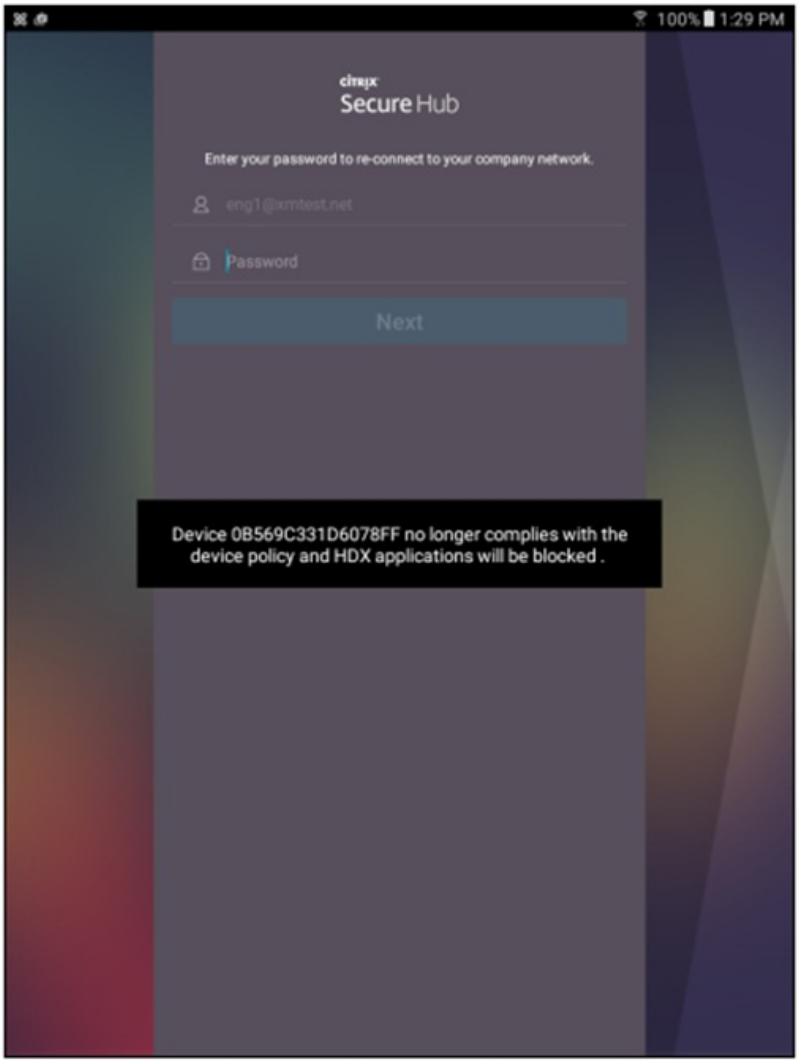


9. **[次へ]** をクリックし、 **[保存]** をクリックします。

デバイスがコンプライアンス違反に指定されると、HDXアプリは、Secure Hubストアに表示されなくなります。ユーザーがプリケーションのサブスクライブから外れたからです。デバイスに通知はされませんし、Secure HubストアにもそのHDXアプリが以前公開されていたことを示す情報は何も表示されません。

ユーザーにデバイスがコンプライアンス違反に指定されたことを通知したい場合は、通知を作成してから、その通知を送信する自動化された操作を設定します。

この例では、デバイスがコンプライアンス違反に指定されたときに、次の通知を作成して送信します。「デバイスのシリア番号または電話番号がデバイスポリシーに準拠しなくなりましたので、HDXアプリケーションがブロックされます」。



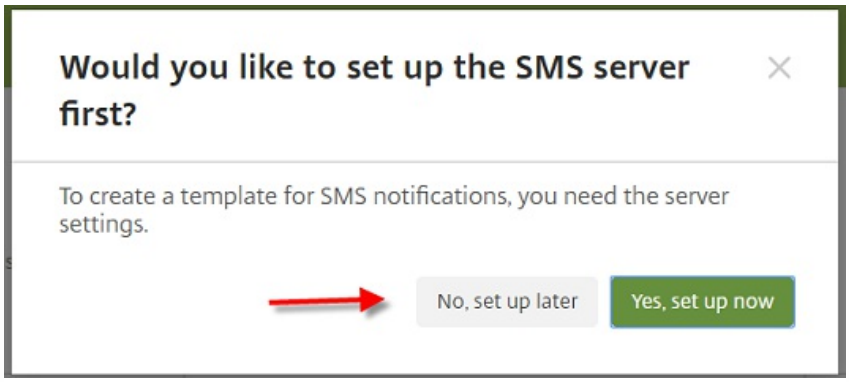
デバイスがコンプライアンス違反に指定されたときに、ユーザーに表示される通知を作成する

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

2. **[通知テンプレート]** をクリックします。 **[通知テンプレート]** ページが開きます。

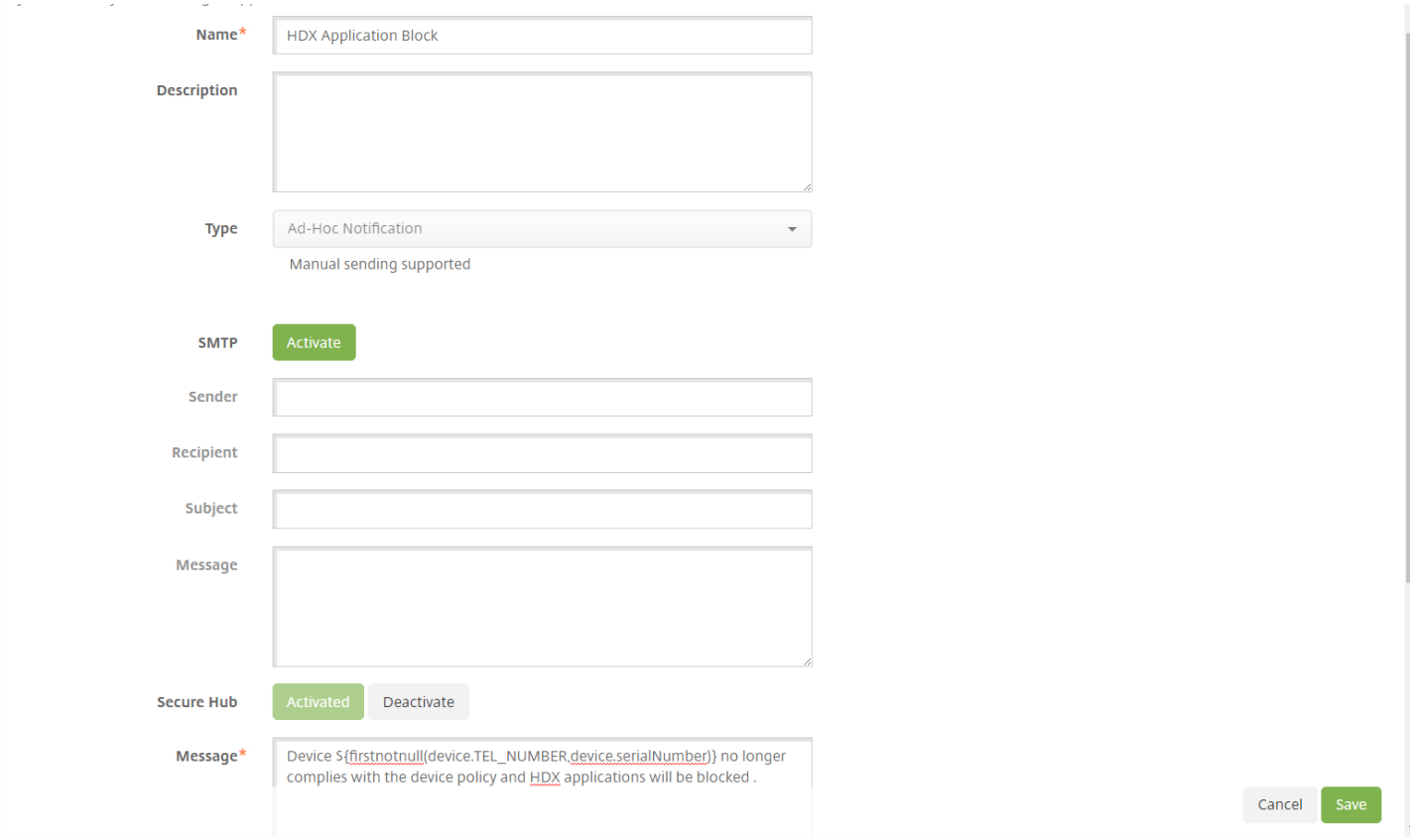
3. **[追加]** をクリックして、 **[通知テンプレート]** ページに追加します。

4. まずSMSサーバーを設定することを求めるメッセージが表示されたら、**[いいえ、あとでセットアップする]** をクリックします。



5. 次の設定を構成します。

- **名前**： HDX Application Block
- **説明**： デバイスがコンプライアンス違反になった場合のエージェント通知
- **種類**： Ad-Hoc Notification
- **Secure Hub**： アクティブ
- **メッセージ**： デバイス ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} がデバイスポリシーに準拠しなくなりましたので、HDXアプリケーションがブロックされます。



6. **[保存]** をクリックします。

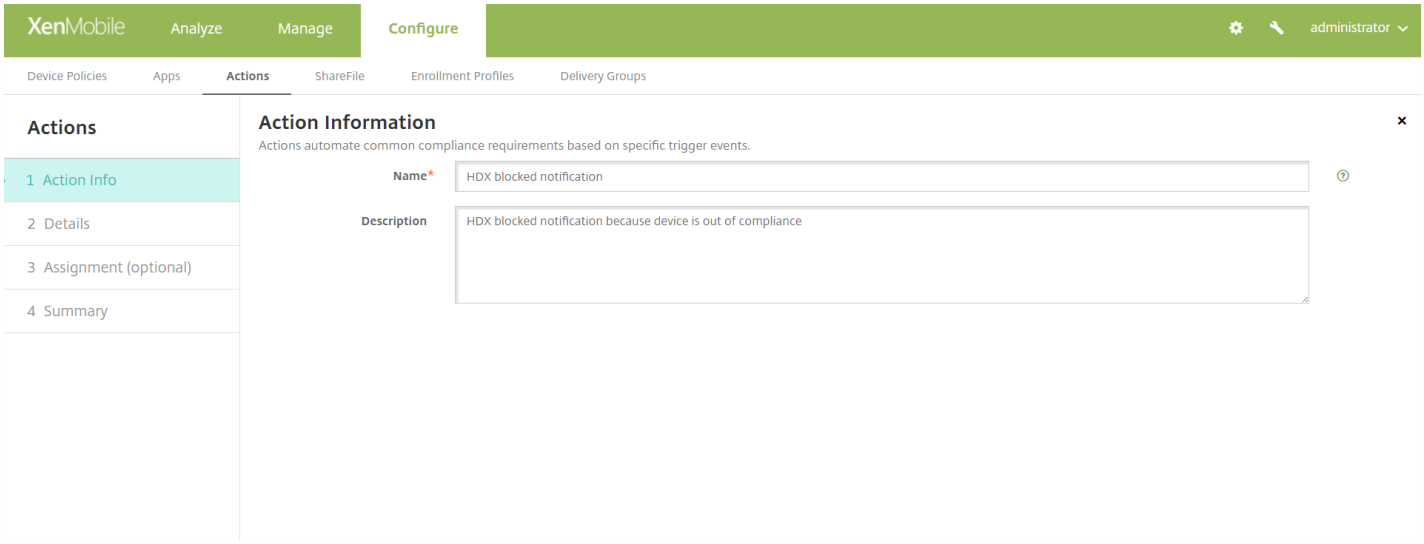
デバイスがコンプライアンス違反に指定されたときに、通知を送信する操作を設定する

1. XenMobileコンソールで、**[構成] > [操作]** をクリックします。**[操作]** ページが開きます。

2. 操作を追加するには **[追加]** をクリックします。**[アクション情報]** ページが開きます。

3. **[アクション情報]** ページで、操作の名前と説明を入力します。

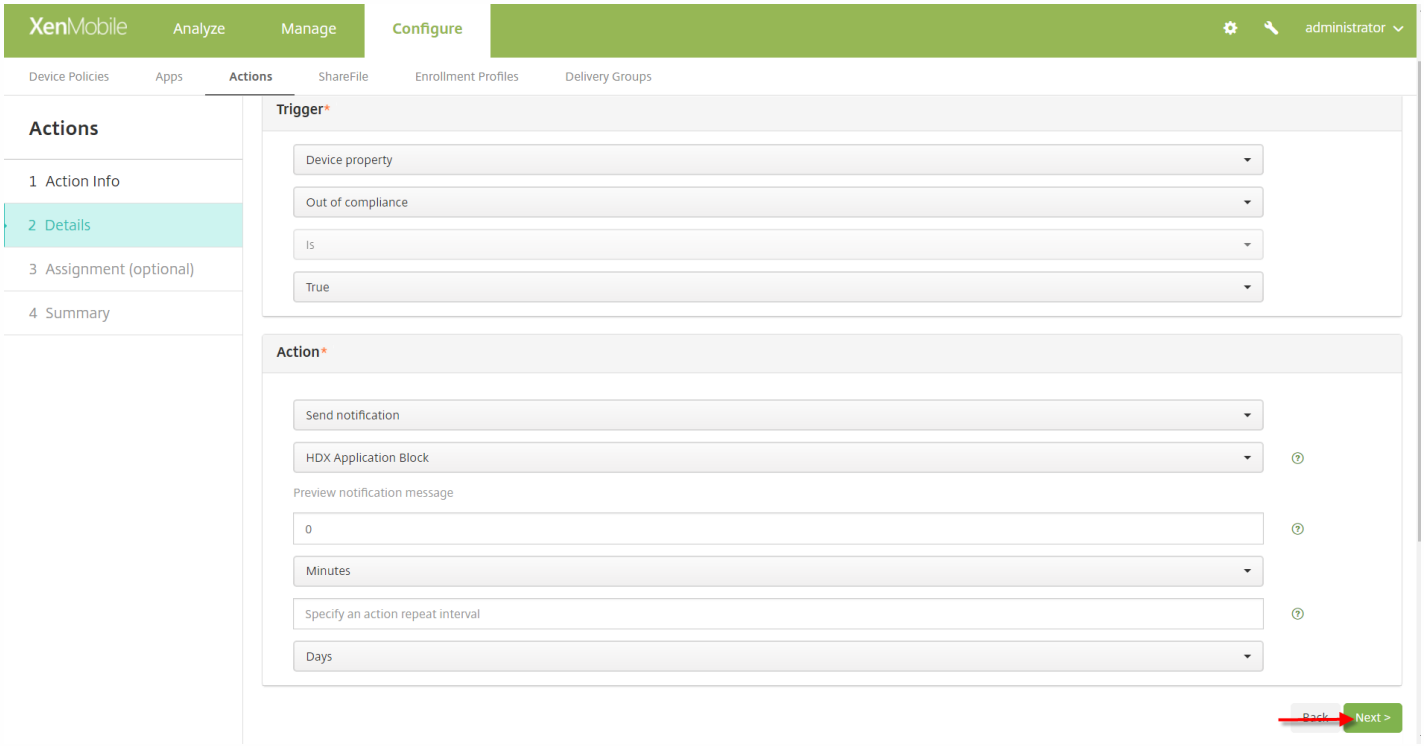
- 名前： HDX blocked notification
- **説明**： デバイスがコンプライアンス違反になったため、HDXがブロックされた通知



4. **[次へ]** をクリックします。 **[アクションの詳細]** ページが開きます。

5. **[トリガー]** 一覧で次のように設定します。

- **[デバイスプロパティ]** を選択。
- **[コンプライアンス違反]** を選択。
- **=**を選択。
- **真**を選択。

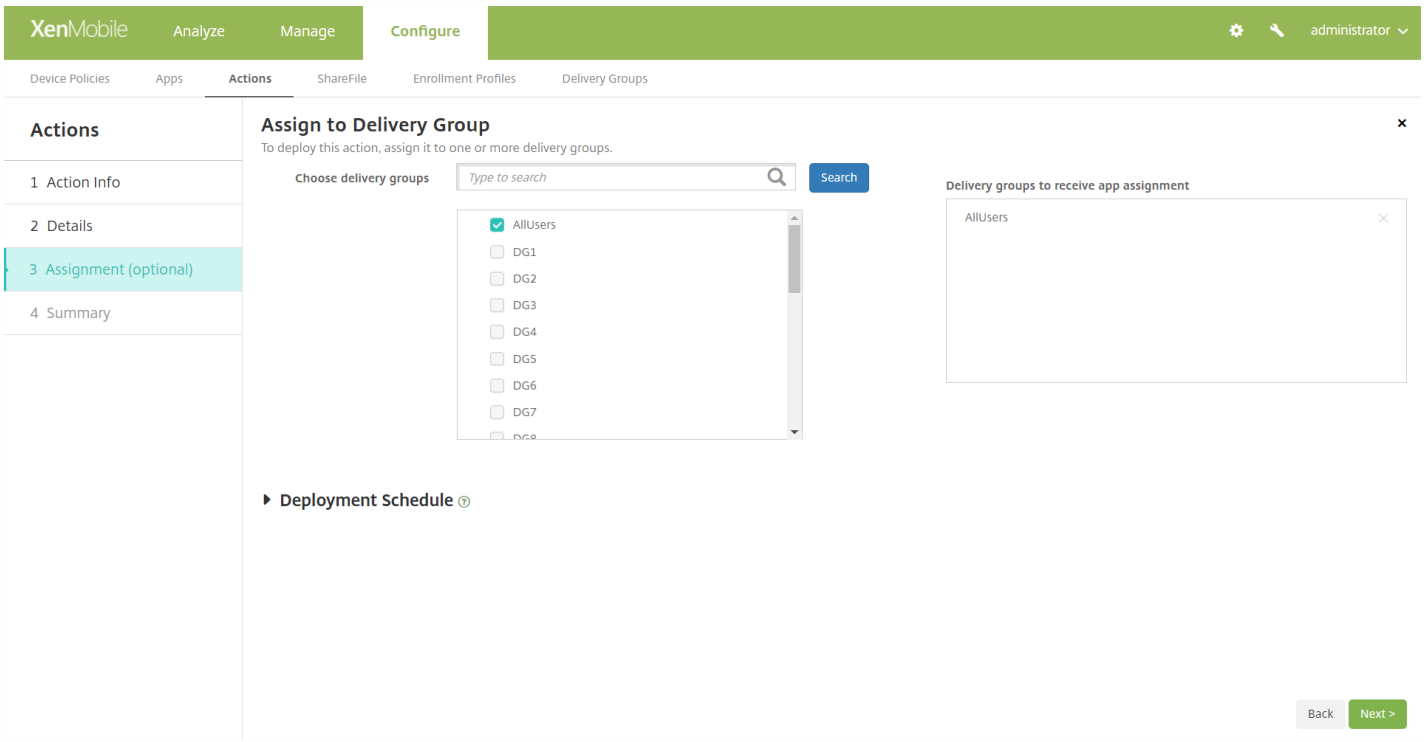


6. **[アクション]** 一覧で、トリガーに一致したときに実行される操作を指定します。

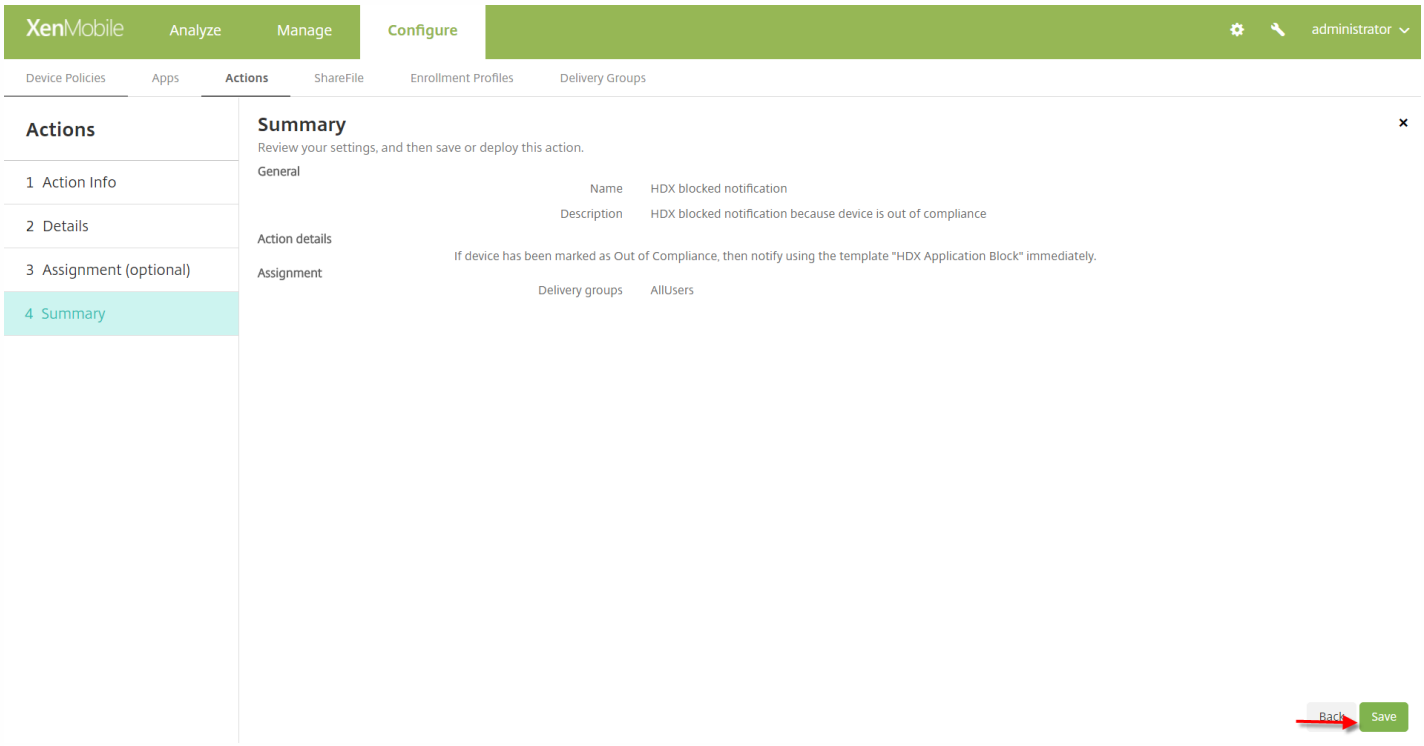
- **[通知を送信]** を選択。

- 作成した通知の［**HDX Application Block**］を選択。
- **0**を選択。この値を0に設定すると、通知はトリガー条件に合致したら直ちに送信されます。

7. XenMobileデリバリーグループまたはこの操作を適用するグループを選択します。この例では、**AllUsers**を選択します。



8. アクションの概要を確認します。



9. **[次へ]** をクリックし、 **[保存]** をクリックします。

自動化された操作の設定について詳しくは、「自動化された操作」を参照してください。

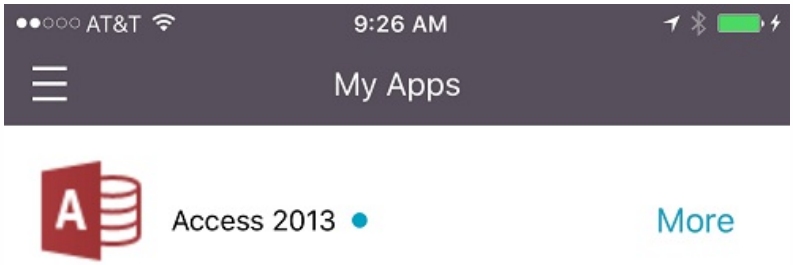
HDXアプリへのアクセス権の回復方法

ユーザーは、デバイスがコンプライアンス準拠状態に戻ればHDXアプリへのアクセスを再び許可されます。

1. デバイス上で、Secure Hubストアにアクセスし、ストアのアプリを更新します。

2. ブロックされたアプリに移動し、 **[追加]** をタップします。

アプリが追加されると、［マイアプリ］の横に青い点を付けて表示され、新しくインストールされたアプリであることを示します。



リソースの展開

Feb 27, 2017

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デバイスに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、デバイスプロパティで指定された展開規則を使って、ポリシー、アプリ、操作、デリバリーグループをフィルターします。たとえば、ドメイン名が特定の値に一致した場合、展開規則が展開パッケージをプッシュするよう指定できます。
- **展開スケジュール：** XenMobileでは、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。

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
アクション	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。

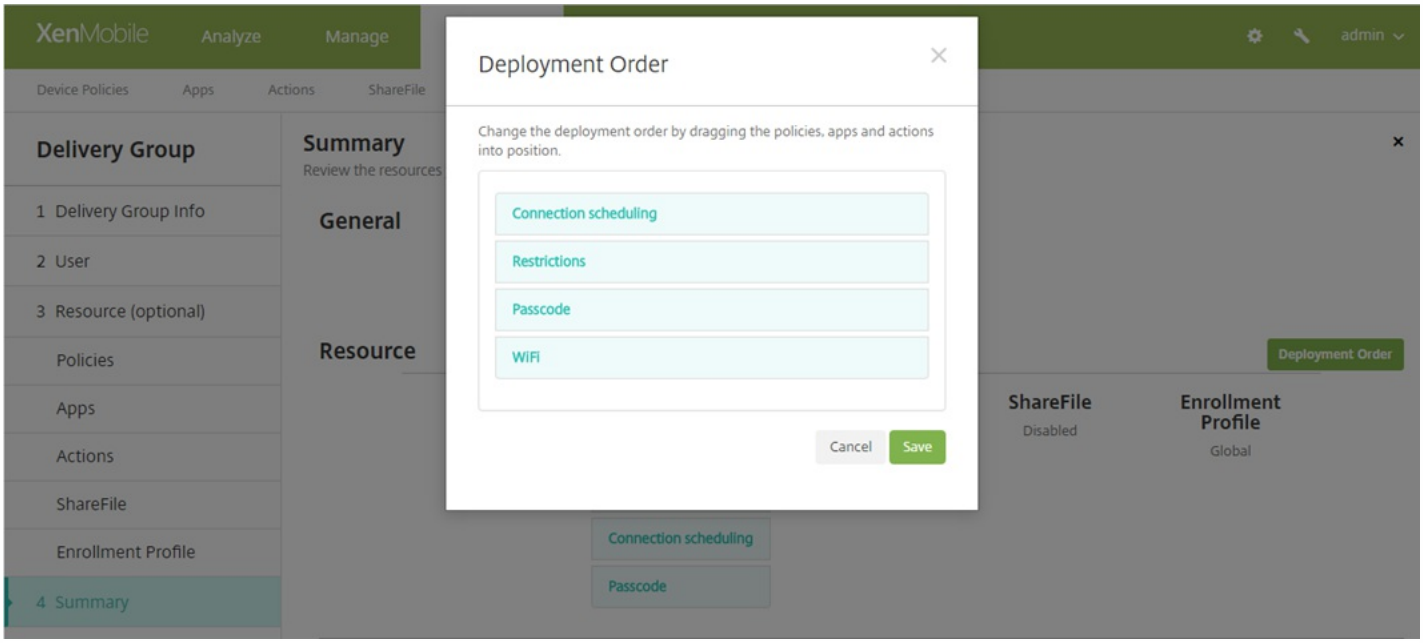
    c. 並べ替え中、デリバリーグループのリソースにユーザー定義の展開順が指定されている場合、その順序を保持します。そうでない場合は、デリバリーグループ内でリソースをリソース名で並べ替えることができます。

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 Manager1： リソースの順序が**未指定**で、**WiFi**ポリシーおよび**Passcode**ポリシーを含みます。
- デリバリーグループ、Account Manager2： リソースの順序が**指定**されていて、**Connection scheduling**ポリシー、**Restrictions**ポリシー、**Passcode**ポリシー、**WiFi**ポリシーを含みます。この事例では、**WiFi**ポリシーの前に**パスコード**ポリシーを配信するように指定されます。

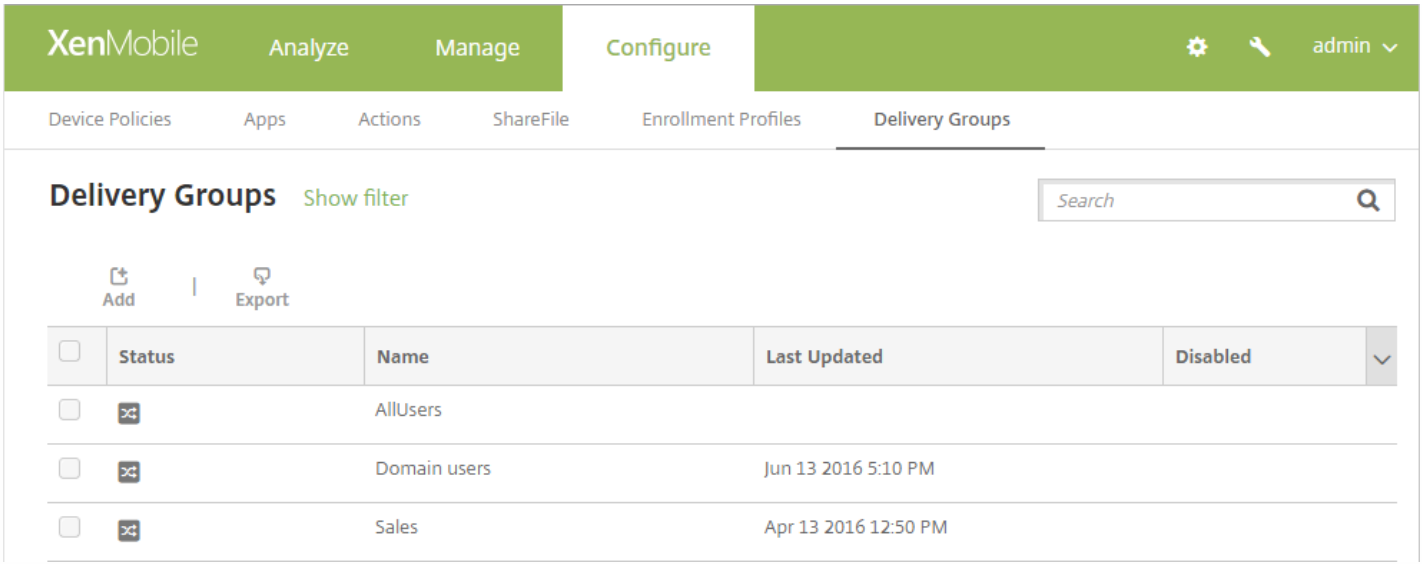


計算アルゴリズムが名前のみを基準に展開グループを順序づけた場合、XenMobileはデリバリーグループAccount Manager 1から開始して、次の順序で展開を実行します。 **WiFi**ポリシー、**パスコード**ポリシー、**接続のスケジューリング**ポリシー、**制限**ポリシー。XenMobileは、Account Manager 2デリバリーグループの重複する**パスコード**および**WiFi**を無視します。

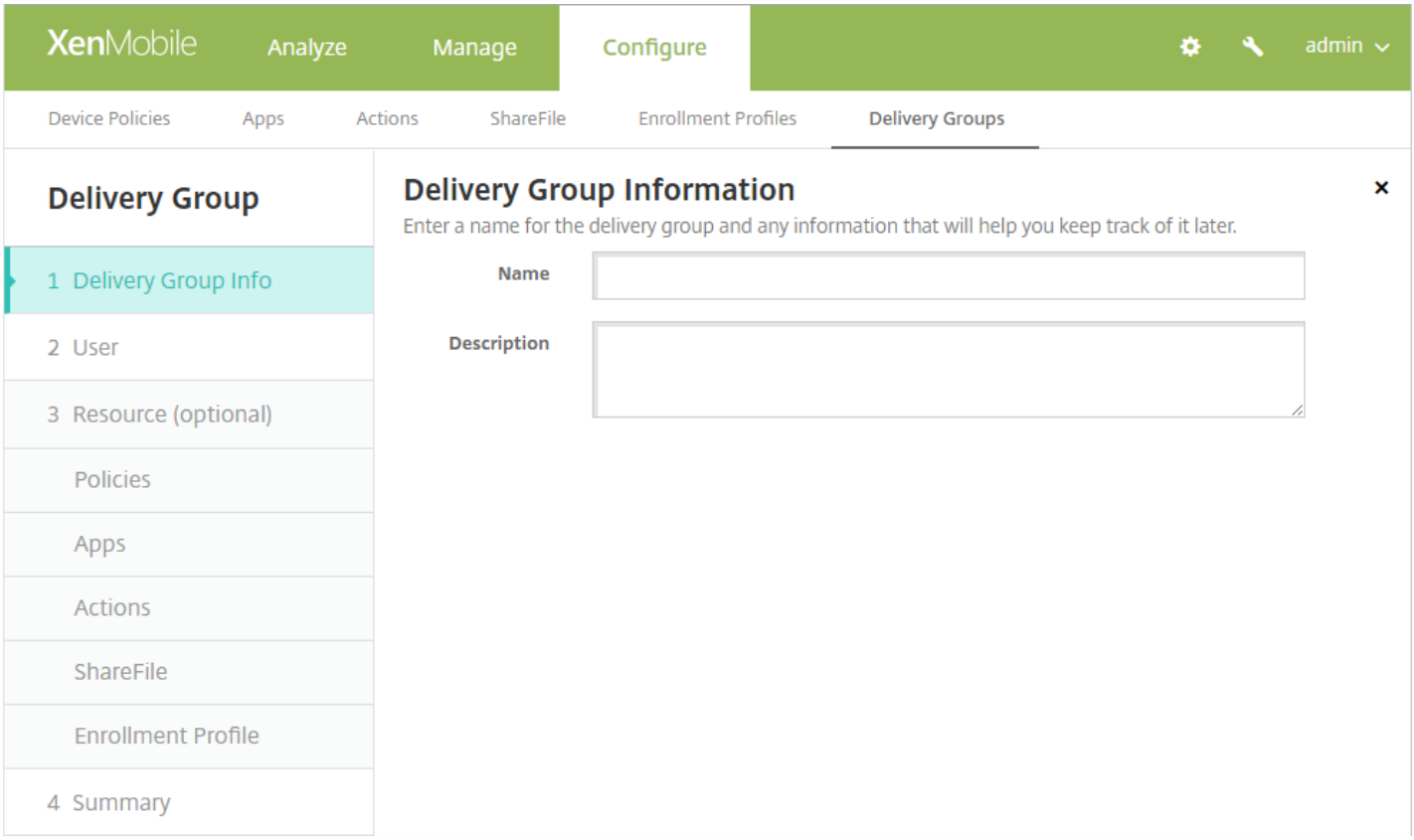
ただし、Account Manager 2グループには管理者が指定した展開順序があるため、計算アルゴリズムは、Account Manager 2デリバリーグループからのリソースを、Account Manager 1デリバリーグループからのものより一覧で上位に配置します。結果的に、XenMobileはポリシーを次の順序で展開します。 **Connection scheduling**、**Restrictions**、**Passcode**、**WiFi**。XenMobileは、Account Manager 1デリバリーグループからのポリシー**WiFi**および**パスコード**を無視します。重複しているためです。このアルゴリズムは、XenMobile管理者によって指定された順序を優先します。

デリバリーグループを追加するには

1. XenMobileコンソールで、 **[構成] > [デリバリーグループ]** の順にクリックします。 **[デリバリーグループ]** ページが開きます。



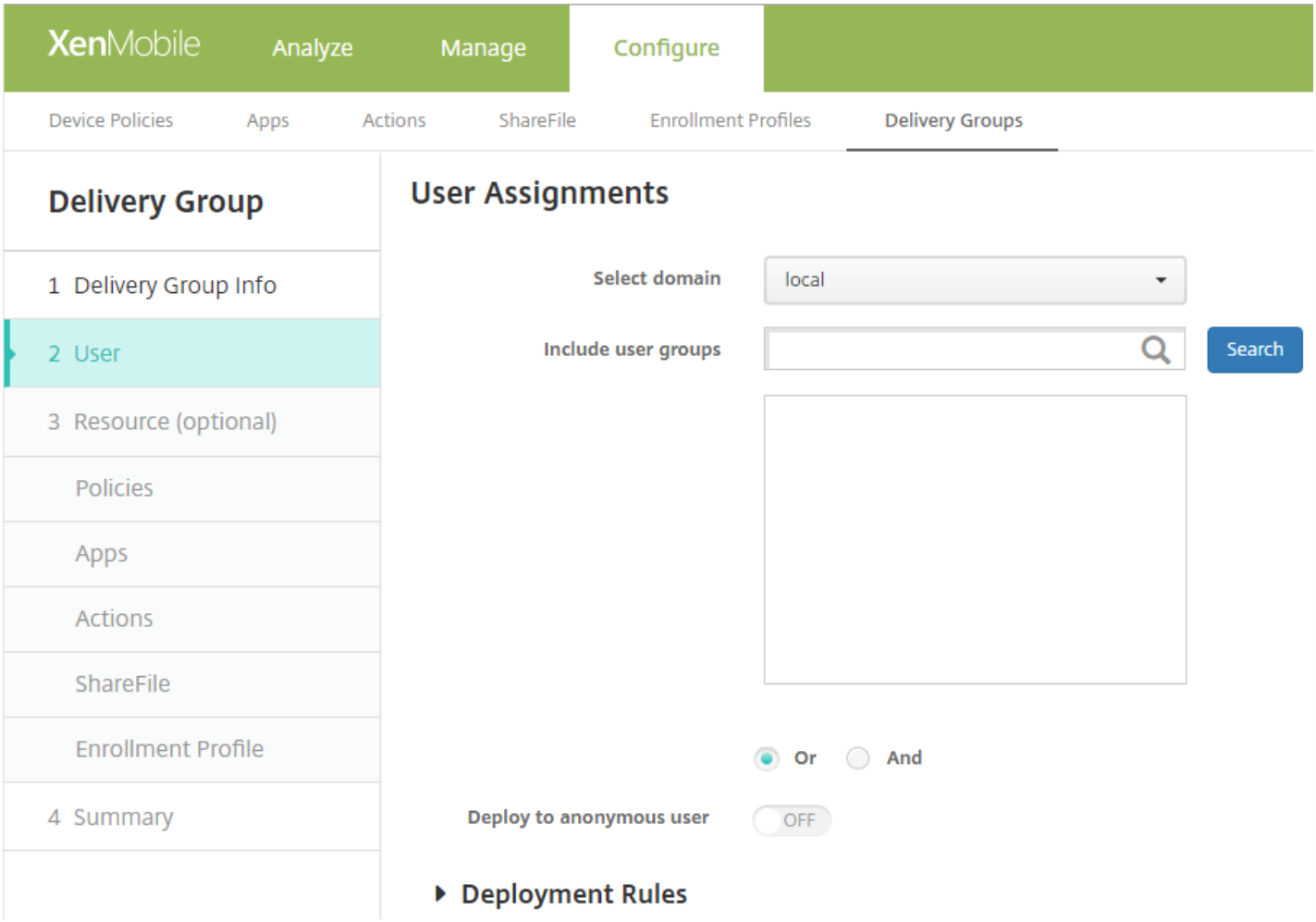
2. **[デリバリーグループ]** ページで、 **[追加]** をクリックします。 **[デリバリーグループ情報]** ページが開きます。



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。

- **名前**： 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]** をクリックします。 **[ユーザー割り当て]** ページが開きます。



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します。選択したグループが**[選択したユーザーグループ]** 一覧に表示されます。
  - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - グループ名の全体または一部を検索ボックスに入力して **[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。
    - **[選択したユーザーグループ]** の一覧からユーザーグループを削除するには、次のいずれかを行います。
      - **[選択したユーザーグループ]** の一覧で、削除する各グループの横にある **[X]** をクリックします。
      - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
      - グループ名の全体または一部を検索ボックスに入力して **[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
- **または/および**： 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（［または］）、すべてのグループに属している必要があるか（［および］）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。

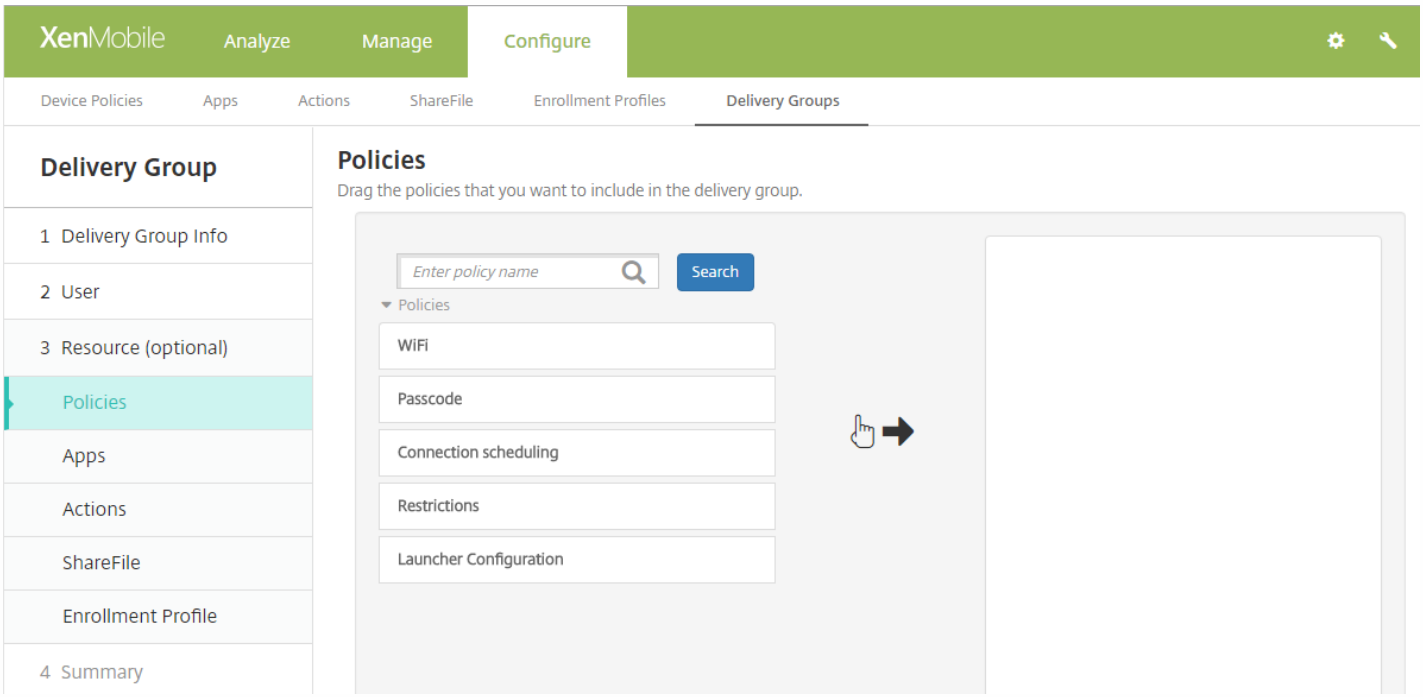
  注： 認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

6. 展開規則を構成します。

デリバリーグループに任意のリソースを追加するには

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。リソースの追加をスキップするには、 **[Summary]** をクリックします。

ポリシーの追加



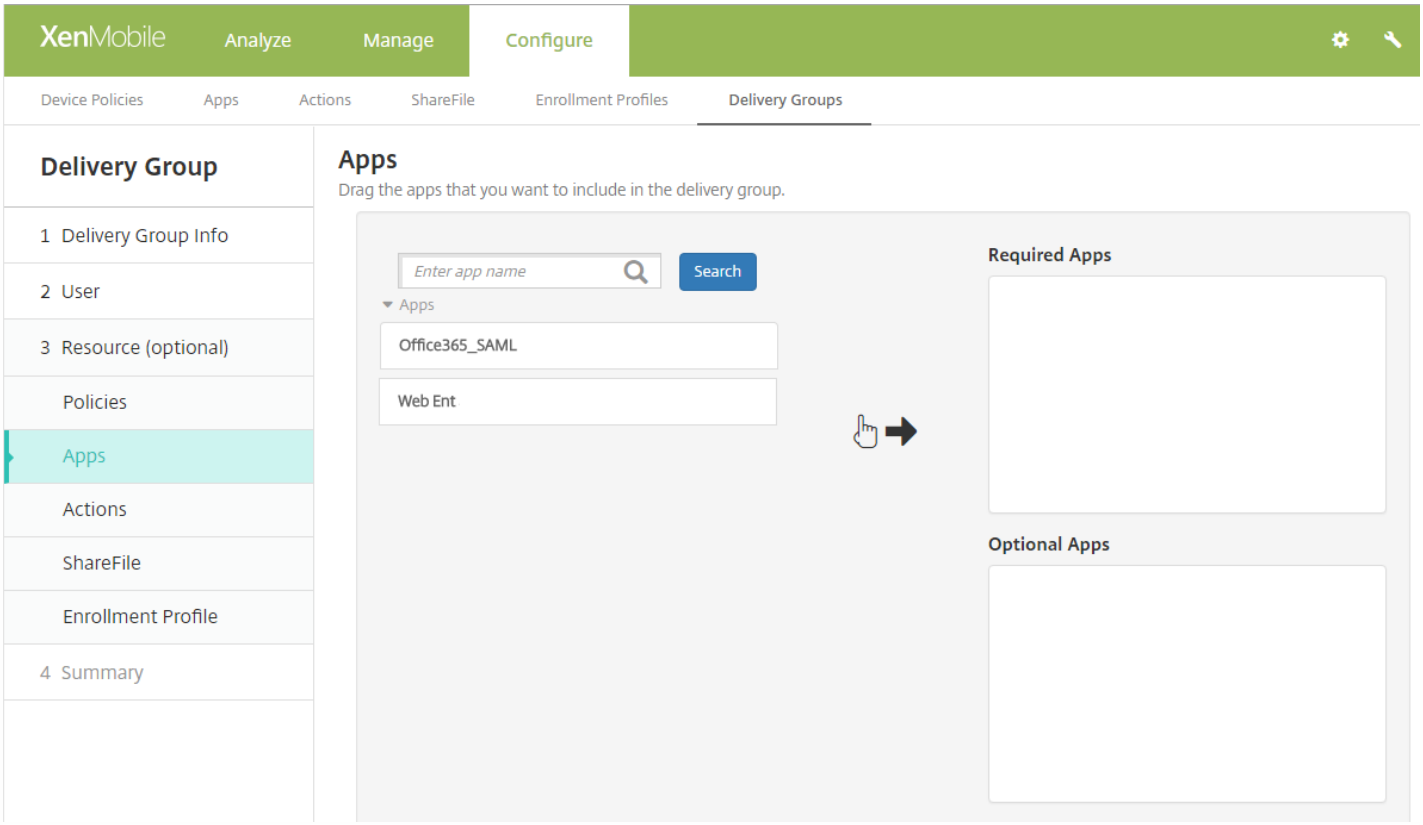
1. 追加するポリシーごとに、以下の操作を行います。

- 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**[検索]** をクリックします。
- 追加するポリシーをクリックして、右側のボックス内へドラッグします。

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



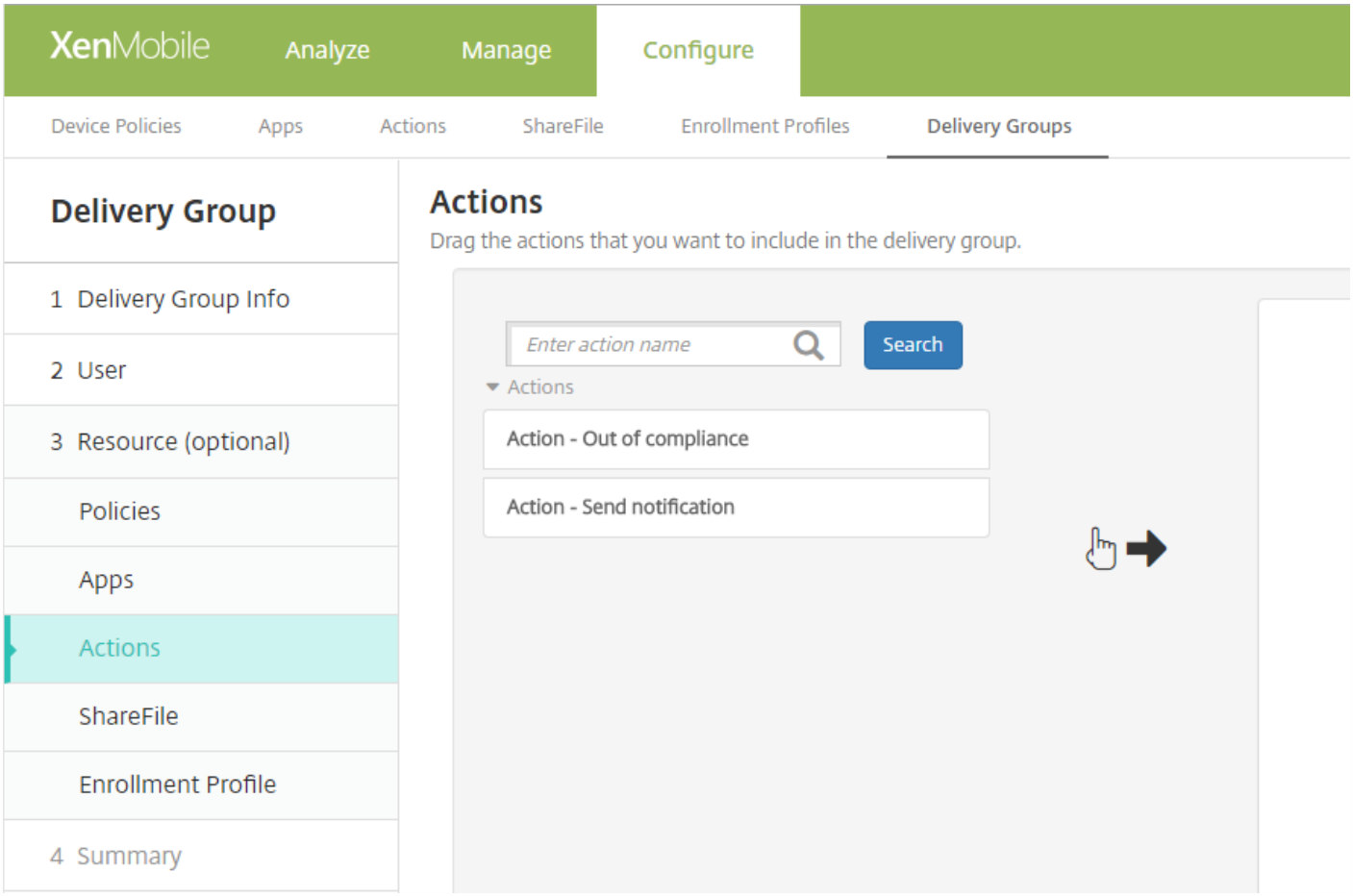
1. 追加するアプリケーションごとに、以下の操作を行います。

- 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**[検索]** 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、**[必須アプリ]** ボックス内または **[任意アプリ]** ボックス内へドラッグします。

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. **[次へ]** をクリックします。 **[操作]** ページが開きます。

操作の追加



1. 追加する操作ごとに、以下の操作を行います。

- 使用可能な操作の一覧をスクロールして、追加するアクションを見つけます。
- または、操作の一覧を絞り込むため、検索ボックスに操作名の全体または一部を入力して**[検索]**をクリックします。
- 追加する操作をクリックして、右側のボックス内へドラッグします。

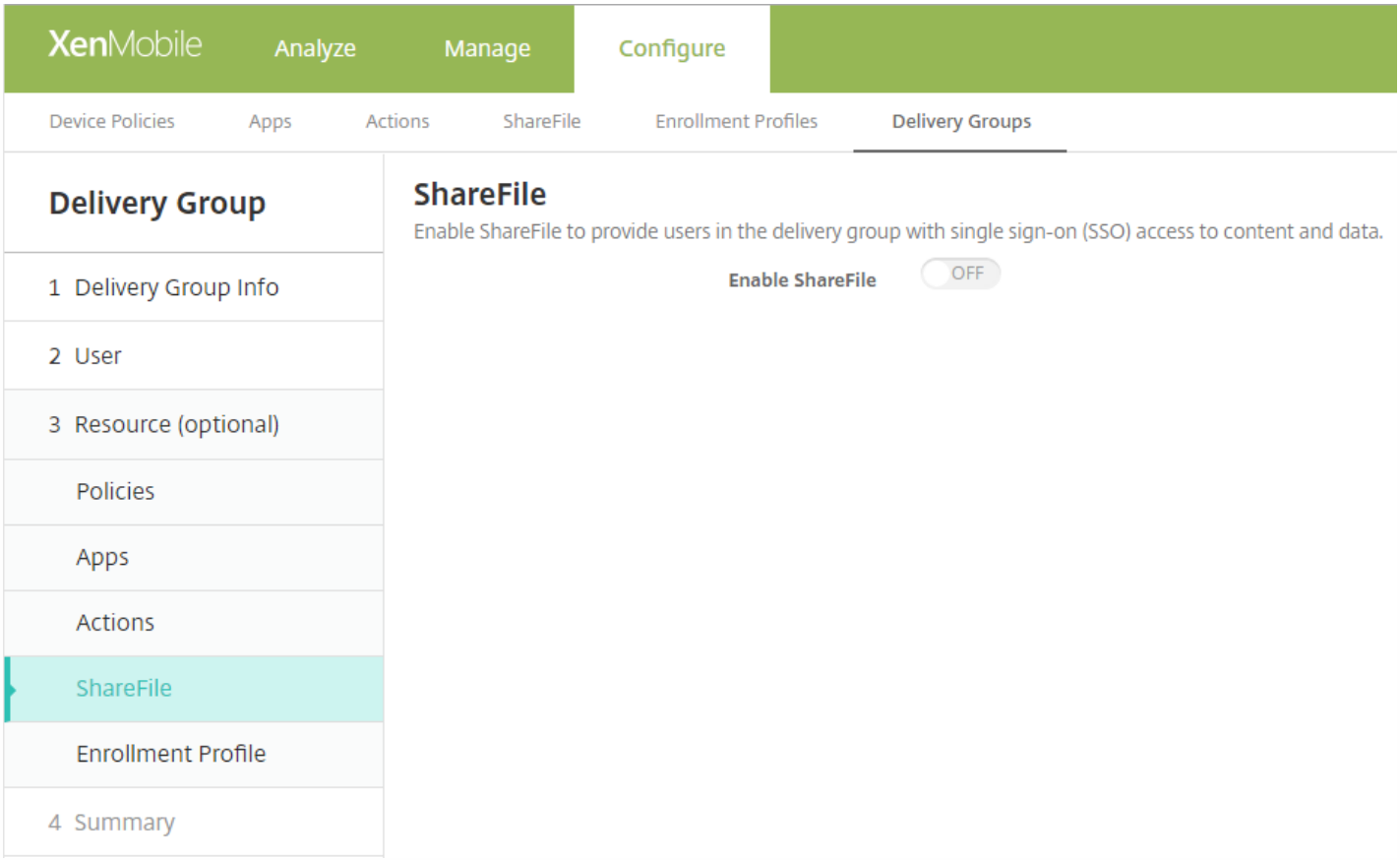
注： 操作を削除するには、右側のボックス内の操作名の横にある**[X]**をクリックします。

2. **[次へ]**をクリックします。**[ShareFile]**ページが開きます。

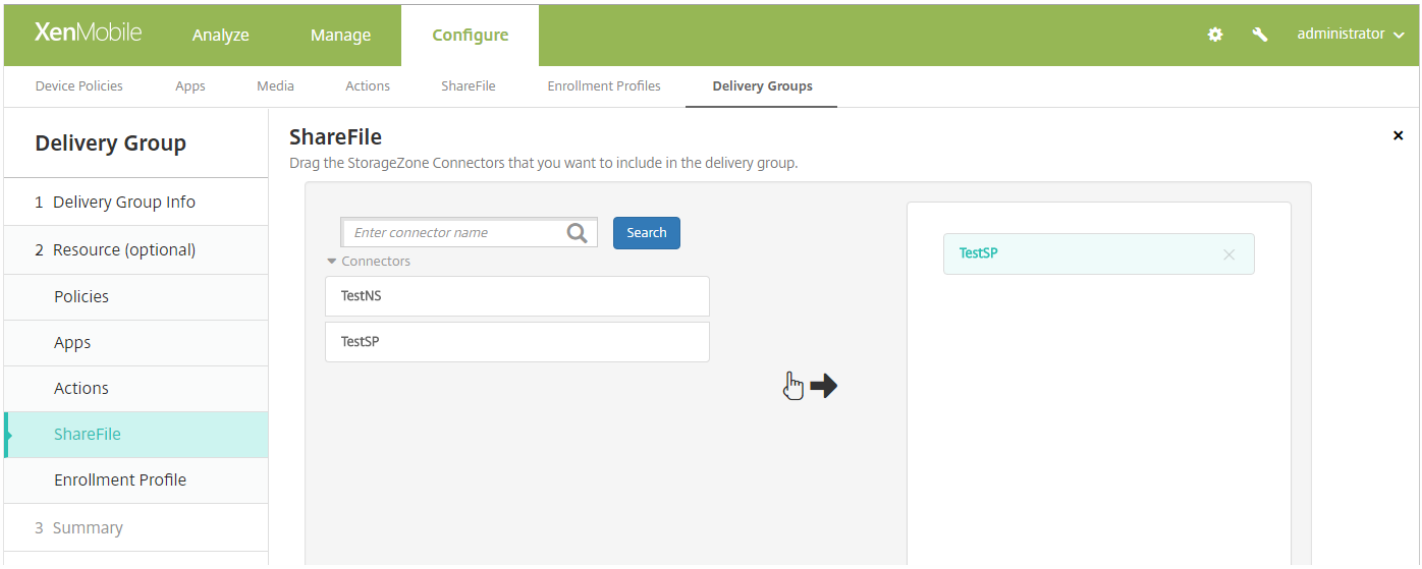
ShareFile構成の適用

ShareFileページの表示は、XenMobile（**[構成] > [ShareFile]**）をShareFile Enterprise用に構成したか、StorageZoneコネクタ用に構成したかによって異なります。

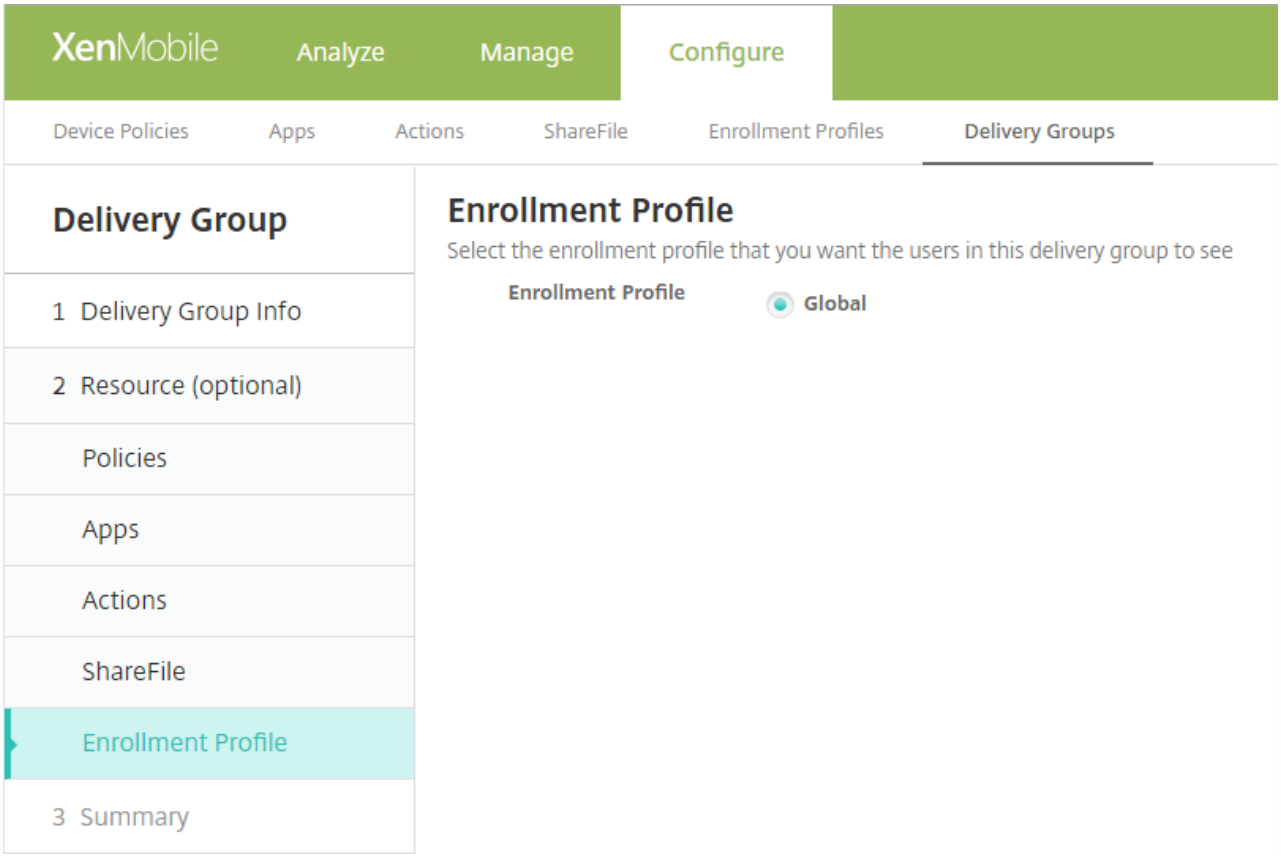
ShareFile EnterpriseをXenMobileと組み合わせて使用するように構成した場合、**[ShareFile の有効化]**を**[オン]**に設定して、デリバリーグループがShareFileのコンテンツとデータにシングルサインオンでアクセスできるようにします。



StorageZoneコネクタをXenMobileと組み合わせて使用するように構成した場合、StorageZoneコネクタを選択してデリバリーグループに含めます。



登録プロファイル

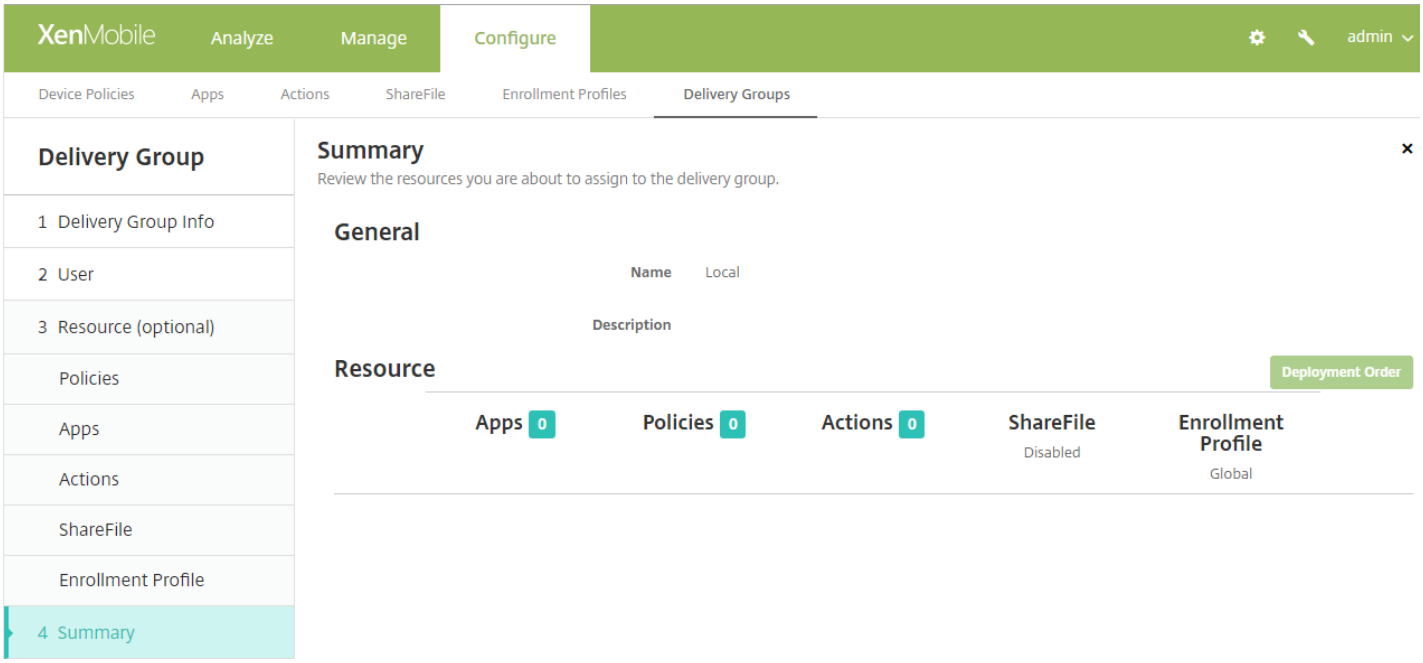


1. 次の設定を構成します。

- **登録プロファイル**：登録プロファイルを選択します。登録プロファイルを作成するには、「デバイス登録の制限」を参照してください。

2. **[Next]** をクリックします。**[概要]** ページが開きます。

構成したオプションの確認および展開順序の変更



［**概要**］ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。［概要］ページには、リソースがカテゴリ別に表示されます。展開順序を反映してはいません。

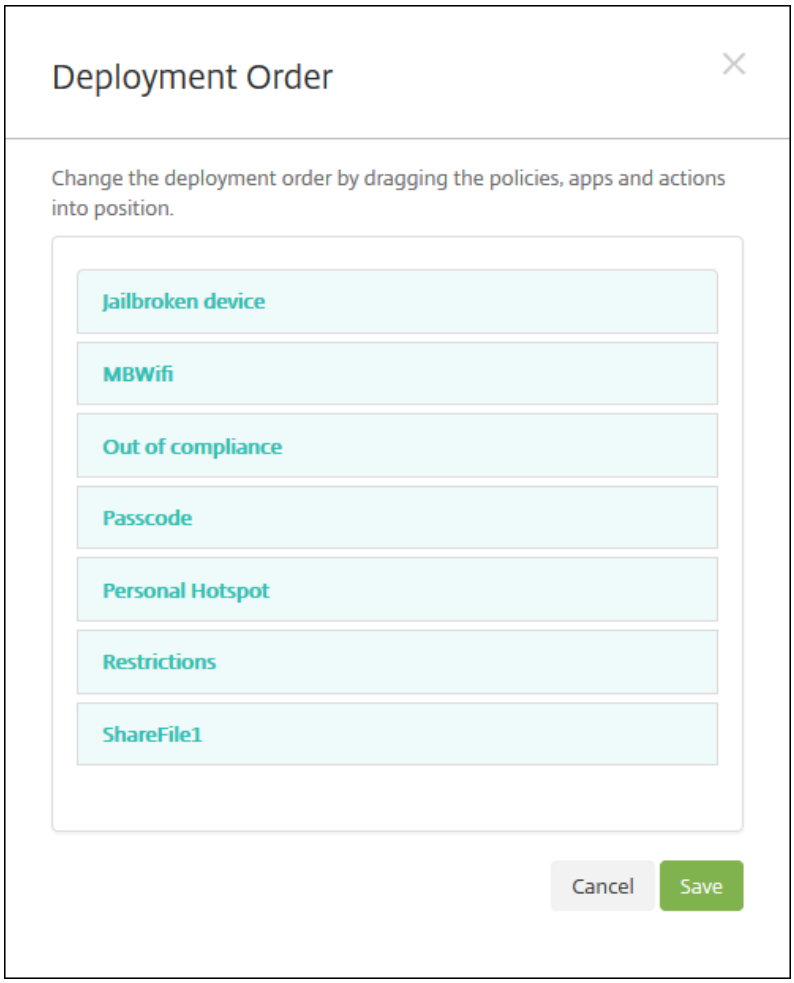
1. 構成の調整が必要な場合は、［**戻る**］をクリックして前のページに戻ります。

2. 展開順序を表示するか、展開順序を並べ替えるには、［**展開順**］をクリックします。

3. ［**Save**］をクリックして、デリバリーグループを保存します。

展開順を変更するには

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. **[保存]** をクリックして、展開順序を保存します。

デリバリーグループを編集するには

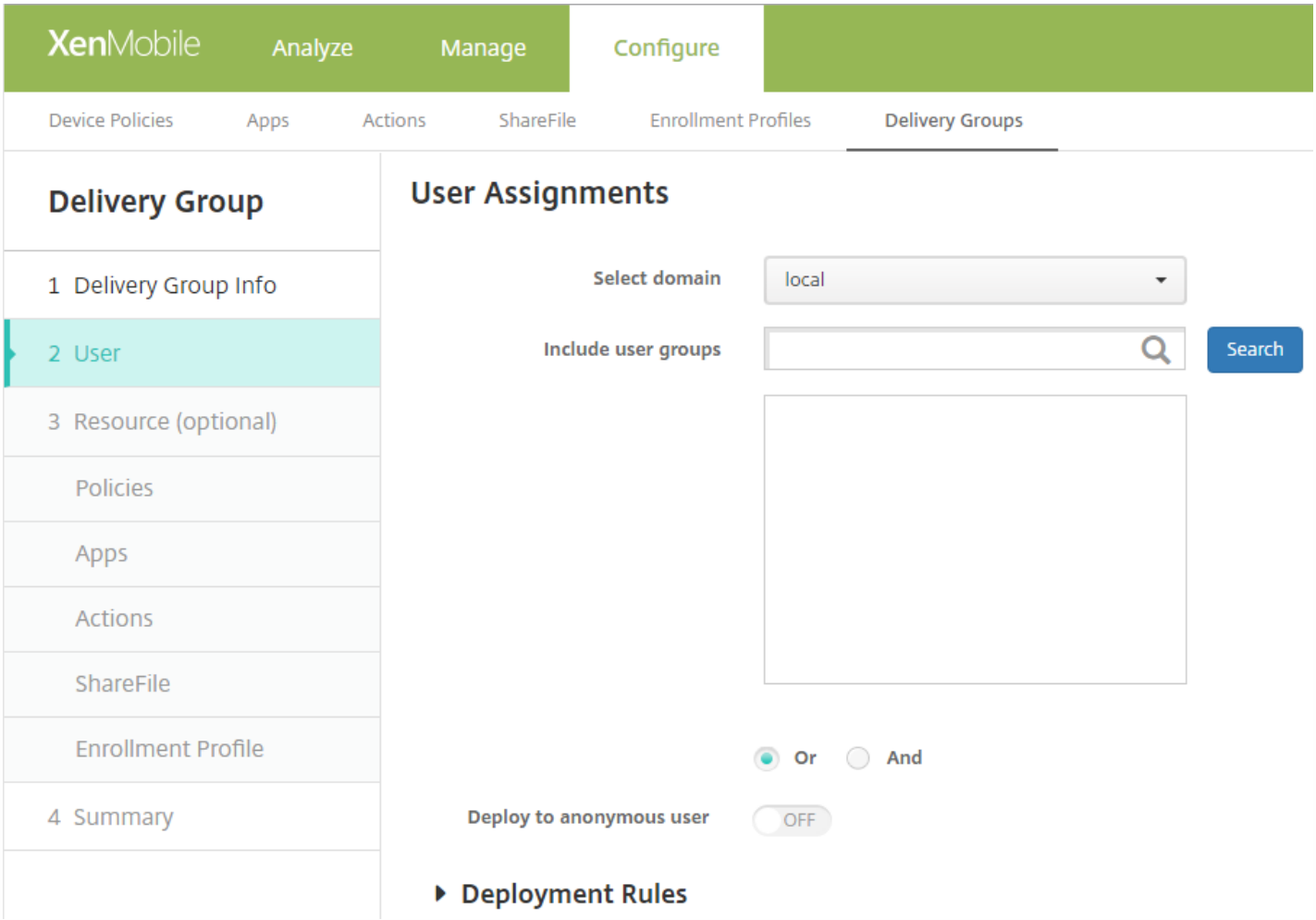
1. **[デリバリーグループ]** ページで、デリバリーグループ名の横にあるチェックボックスをオンにするかデリバリーグループ名を含む行をクリックして、編集するデリバリーグループを選択し、 **[編集]** をクリックします。 **[デリバリーグループ情報]** 編集ページが開きます。

> **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**[編集]** コマンドが表示されます。

2. **[説明]** 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. **[次へ]** をクリックします。 **[ユーザー割り当て]** ページが開きます。



4. **[ユーザーグループの選択]** ページで、以下の情報を入力または変更します。

- **ドメインを選択**： 一覧から、ユーザーを選択するドメインを選択します。
- **ユーザーグループを含める**： 次のいずれかを行います。
  - ユーザーグループの一覧で、追加するグループを選択します。選択したグループが**[選択したユーザーグループ]** 一覧に表示されます。
  - **[検索]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - グループ名の全体または一部を検索ボックスに入力して **[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。

    注： ユーザーグループを削除するには、**[検索]** をクリックして、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 **[検索]** 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。

- **または/および**： 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（［または］）、すべてのグループに属している必要があるか（［および］）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。

5. **[展開規則]** 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. **[次へ]** をクリックします。 **[デリバリーグループリソース]** ページが開きます。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、 **[デリバリーグループ]** の **[概要]** をクリックしてデリバリーグループ構成の概要情報を表示します。

7. リソースの変更が完了したら、 **[次へ]** をクリックするか、 **[デリバリーグループ]** の **[概要]** をクリックします。

8. **[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。

9. 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。

10. リソースの展開順序を並べ替えるには **[展開順]** をクリックします。展開順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。

AllUsersデリバリーグループを有効化および無効化するには

> **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. **[デリバリーグループ]** ページで、 **[AllUsers]** の横にあるチェックボックスをオンにするか、［AllUsers］を含む行をクリックして、AllUsersデリバリーグループを選択します。次に、以下のいずれかを行います。

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 **[有効]** または **[無効]** 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、 **[無効]** をクリックします。このコマンドは、［AllUsers］が有効（デフォルト）になっている場合にのみ使用できます。 **デリバリーグループの表の [無効] の見出しの下に、 [無効]** が表示されます。
- AllUsersデリバリーグループを有効化するには、 **[有効]** をクリックします。このコマンドは、［AllUsers］が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 [無効] の見出しの下の［無効]** の表示が消えます。

デリバリーグループに展開するには

デリバリーグループへの展開とは、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、XenMobile Storeの［更新可能］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。

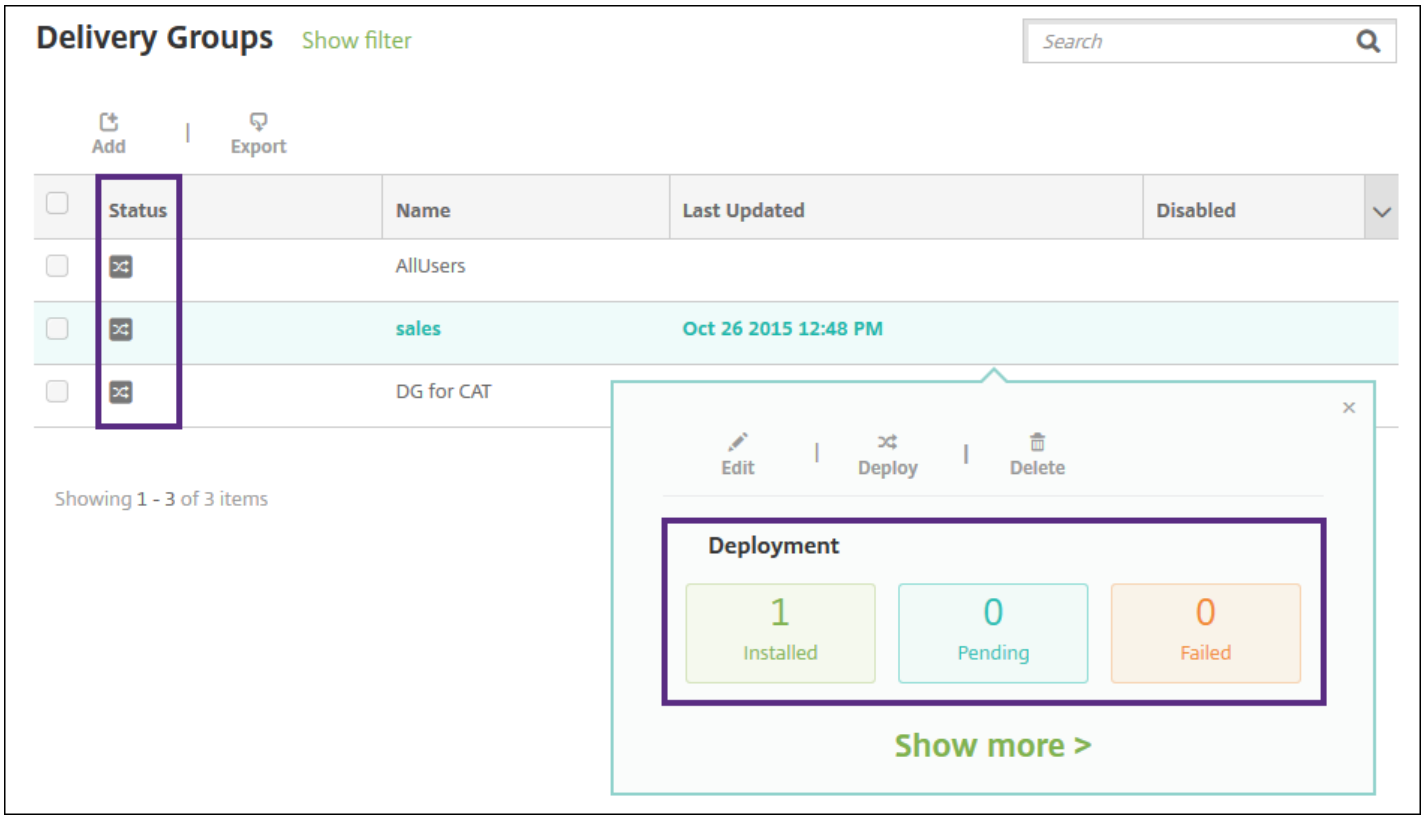
2. **[展開]** をクリックします。

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、アクションを展開するグループが一覧にあることを確認して、[展開] をクリックします。デバイスプラットフォームとスケジュール設定ポリシーに基づいて、選択したグループにアプリケーション、ポリシー、アクションが展開されます。

[デリバリーグループ] ページで、次のいずれかの方法により展開ステータスを確認できます。

- デリバリーグループの [状態] の見出しの下で、展開エラーを示す展開アイコンを確認します。
- デリバリーグループを含む行をクリックし、[インストール済み] 、 [保留] 、 [失敗] の展開を示すオーバーレイを表示します。



デリバリーグループを削除するには

> **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. [デリバリーグループ] ページで、次のいずれかを行います。

- 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。
- 1つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

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

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**[削除]** コマンドが表示されます。

3. **[削除]** 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。

［Delivery Groups］の表をエクスポートするには

1. **[デリバリーグループ]** の表の上にある **[エクスポート]** をクリックします。XenMobileによって **［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。

マクロ

Feb 27, 2017

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（ユーザー名とドメイン名）
- username（loginnameから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（前述の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。

自動化された操作

Feb 27, 2017

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。

ユーザーのデバイスがコンプライアンス不遵守状態になった後で、デバイスがコンプライアンス遵守状態になるようユーザーがデバイスを修正した場合、デバイスをコンプライアンス遵守状態にリセットするパッケージを展開するようポリシーを構成する必要があります。

自動的に発生する効果は、次の範囲から設定します。

- デバイスに選択的ワイプまたは完全なワイプを実行する。
- デバイスをコンプライアンス不遵守に設定する。
- 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。

この記事では、XenMobileでの自動化された操作の追加、編集、フィルターの方法、およびアプリロックおよびアプリワイプ操作をMAM-onlyモード用に構成する方法について説明します。

> ## 注意
>
> 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。次を参照してください。XenMobileでの通知。また、続行する前に使用予定の通知テンプレートを設定します。通知テンプレートの設定について詳しくは、「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. XenMobileコンソールで、**［構成］** > **［操作］** をクリックします。**［アクション］** ページが開きます。

2. **［アクション］** ページで、次のいずれかを行います。

- 新しい操作を追加するには **［追加］** 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。

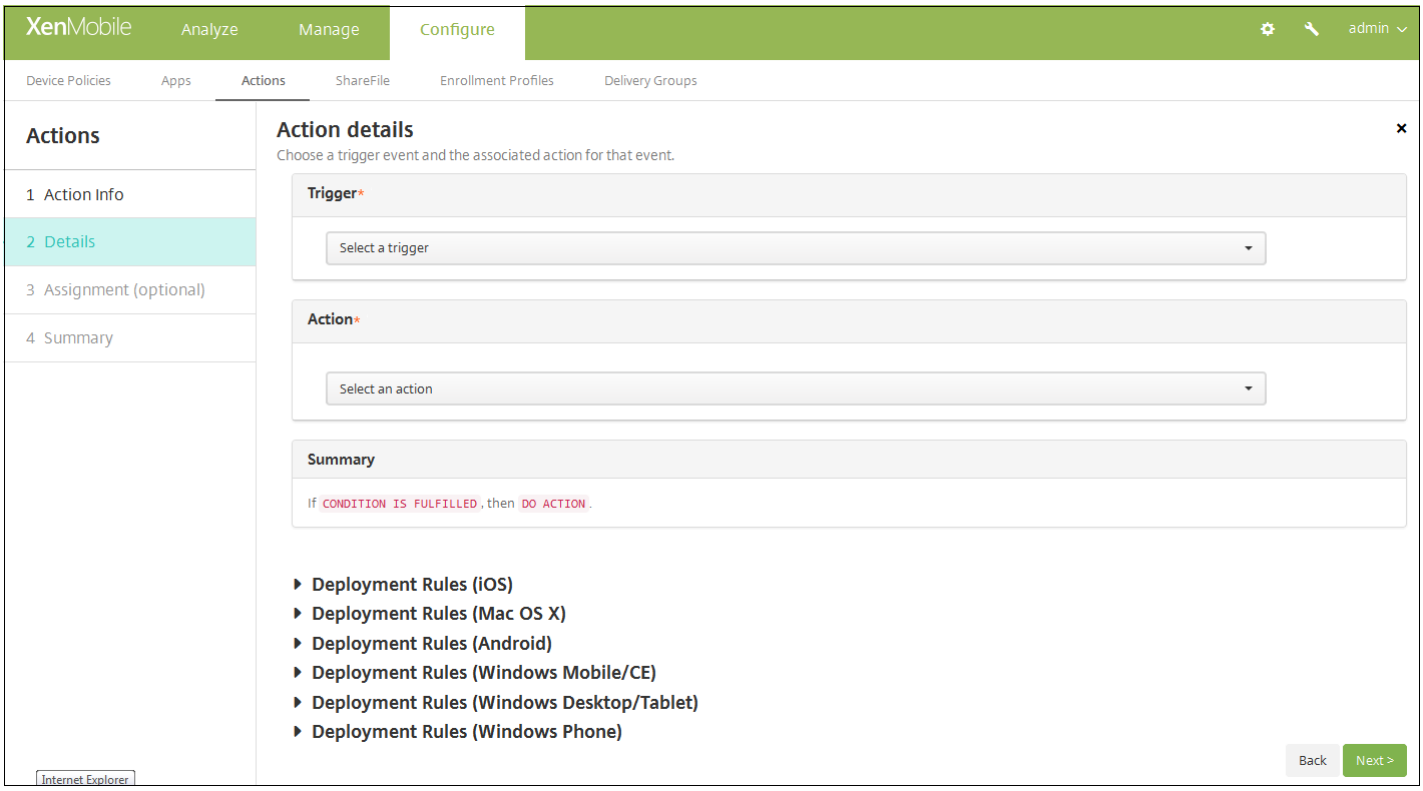
3. **［アクション情報］** ページが開きます。

4. **［アクション情報］** ページで、次の情報を入力または変更します。

- **名前**： 操作を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. **[次へ]** をクリックします。 **[アクションの詳細]** ページが開きます。

注： 次の例は**イベント**トリガーの設定方法を示しています。別のトリガーを選択した場合、この図で示されているものとは異なるオプションになります。



6. **[アクションの詳細]** ページで、次の情報を入力または変更します。

- **[トリガー]** 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。
  - **イベント**： 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. **[アクション]** の一覧で、トリガーの条件が満たされたときに実行される操作をクリックします。**[通知を送信]** 以外では、トリガーの原因となった問題をユーザーが解決できる期間を選択します。その期間内に問題が解決されない場合は、選択した操作が実行されます。実行できるアクションは次のとおりです。

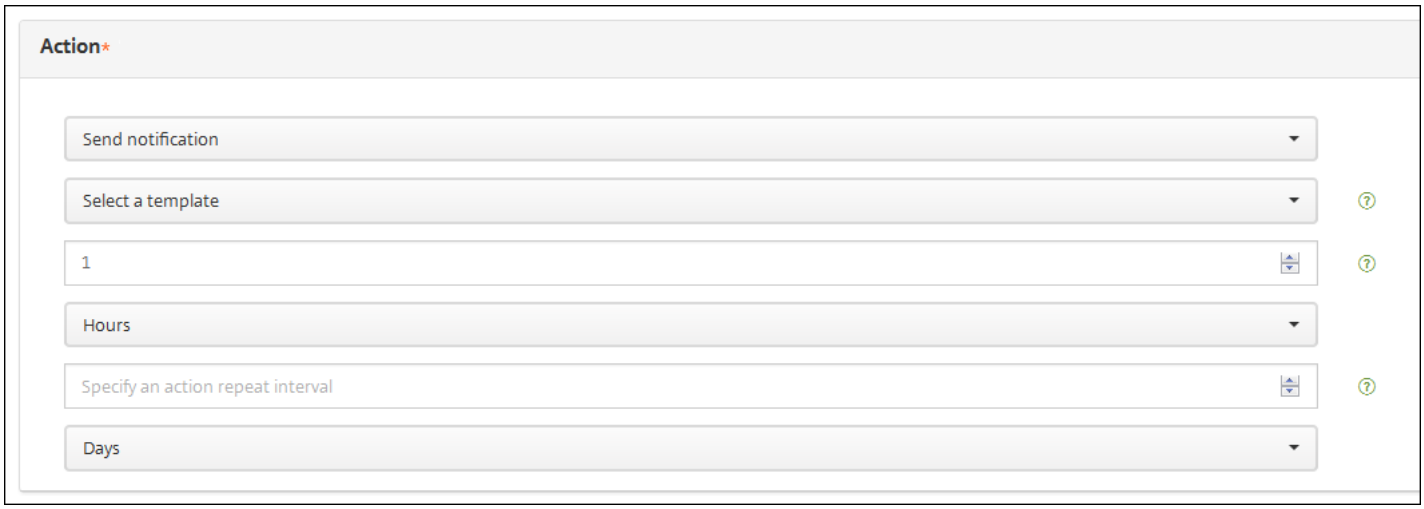
- **Selectively wipe the device**： 個人のデータとアプリケーションは残して、企業のすべてのデータとアプリケーションをデバイスから消去します。

- **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。デバイスに装備されている場合、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。詳しくは、この記事で後述する「MAM-onlyモードでのアプリロックとアプリワイプ操作」を参照してください。
- **アプリワイプ**： Androidでは、これによりユーザーのXenMobileアカウントが削除されます。iOSでは、これにより、ユーザーがXenMobile機能にアクセスするために必要な暗号キーが削除されます。詳しくは、この記事で後述する「MAM-onlyモードでのアプリロックとアプリワイプ操作」を参照してください。
- **コンプライアンス違反としてデバイスをマーク**: コンプライアンス違反としてデバイスを設定します。
- **Send notification**： ユーザーへのメッセージの送信します。

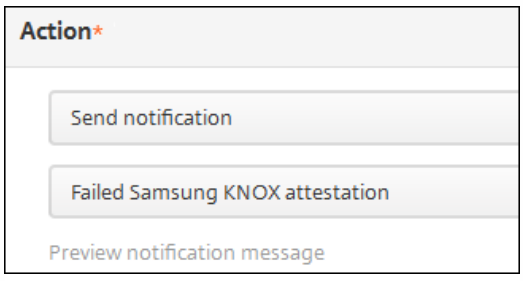
[Send notification] を選択すると、以降の手順で通知の送信方法について説明します。

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した通知テンプレートが表示されます（通知の種類に既にテンプレートが存在する場合）。テンプレートがない場合、テンプレートの構成を促す次のメッセージが表示されます：このイベントの種類にテンプレートがありません（No template for this event type.） **[設定]** の**通知テンプレート**でテンプレートを作成します。

注： ユーザーに通知するには、XenMobileがメッセージを送信できるように、［設定］で通知サーバー（SMTPおよびSMS）を構成している必要があります。次を参照してください。 XenMobileでの通知。また、続行する前に使用予定の通知テンプレートを設定します。通知テンプレートの設定について詳しくは、「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、 **[通知メッセージをプレビュー]** をクリックして通知をプレビュー表示できます。



10. 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. **[概要]** で、意図したとおりに、自動化された操作を作成したことを確認します。

12. 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。

13. 展開規則を構成します

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、 **[次へ]** をクリックします。 **[アクション]** 割り当てページが開きます。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. **[デリバリーグループを選択]** 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 **[アプリ割り当てを受信するためのデリバリーグループ]** の一覧に表示されます。

16. ［展開スケジュール］を展開して以下の設定を構成します。

- **[展開]** の横の **[オン]** をクリックすると展開がスケジュールされ、 **[オフ]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[オフ]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[展開スケジュール]** の横の **[すぐに]** または **[あとで]** をクリックします。デフォルトのオプションは **[すぐに]** です。
- **[あとで]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[展開状態]** の横の **[接続するたび]** をクリックするか、 **[以前の展開が失敗した場合のみ]** をクリックします。デフォルトのオプションは、 **[接続するたび]** です。
- **[常時接続に対する展開]** の横の **[オン]** または **[オフ]** をクリックします。デフォルトのオプションは **[オフ]** です。

注： このオプションは、**[設定]** の **[サーバープロパティ]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

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、**[常時接続に対する展開]** は適用されません。

17. **[次へ]** をクリックします。**[概要]** ページが開きます。ここで操作の構成を確認できます。

18. **[保存]** をクリックして操作を保存します。

MAM-onlyモードでのアプリロックとアプリワイプ操作

XenMobile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できます。4つのカテゴリは、Event、Device property、User property、Installed app nameです。

自動でアプリのワイプまたはロックを構成するには

1. XenMobileコンソールで、**[Configure]** の **[Actions]** をクリックします。

2. **[Actions]** ページで、**[Add]** をクリックします。

3. **[Action Information]** 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. **[Action Details]** ページで、目的のトリガーを選択します。

5. **[Action]** でアクションを選択します。

この段階で、以下の条件に注意してください。

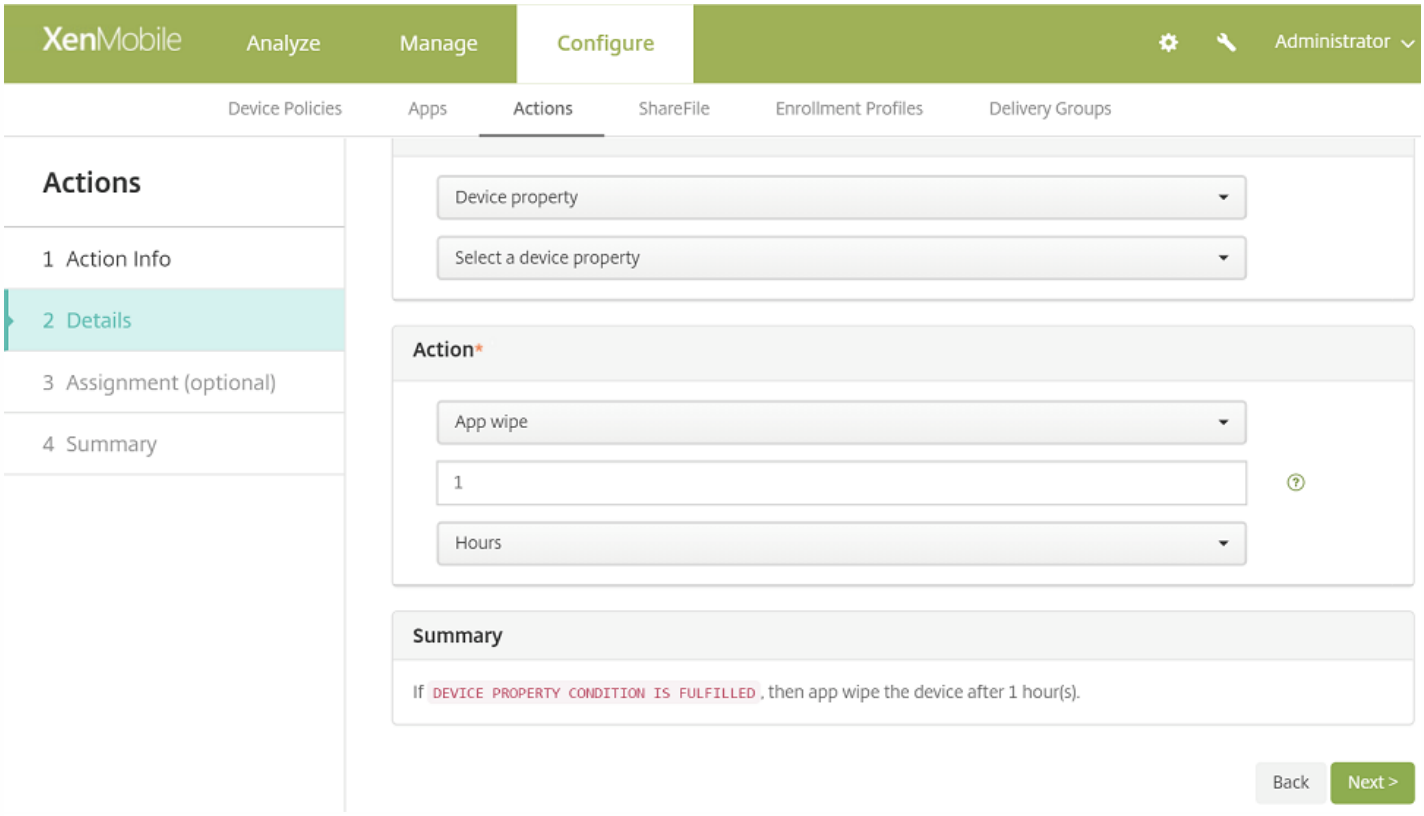
トリガーの種類が**Event** で、値が**Active Directory disabled user**ではない場合、**[App wipe]** および **[App lock]** アクションは表示されません。

トリガーの種類が**デバイスプロパティ**で値が**MDMの紛失モードが有効になっています**である場合、次のアクションが表示されます。

- デバイスを選択的にワイプ
- デバイスを完全にワイプ
- デバイスを取り消す

各オプションでは、自動で1時間の遅延が設定されていますが、遅延の期間は分単位、時間単位、日数単位を選択できます。遅延によって、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を使用した役割の構成」を参照してください。

> **注意**
>
> トリガーを**event**に設定すると、繰り返し間隔は自動的に最小1時間となります。通知を生成するには、デバイスはポリシーの更新を実行して、サーバーと同期する必要があります。通常、ユーザーのサインオン時、またはSecure Hubでポリシーを手動で更新すると、デバイスはサーバーと同期します。
>
> Active DirectoryデータベースとXenMobileとの同期を許可するアクションが実行される前に、さらに約1時間、遅延を追加できます。



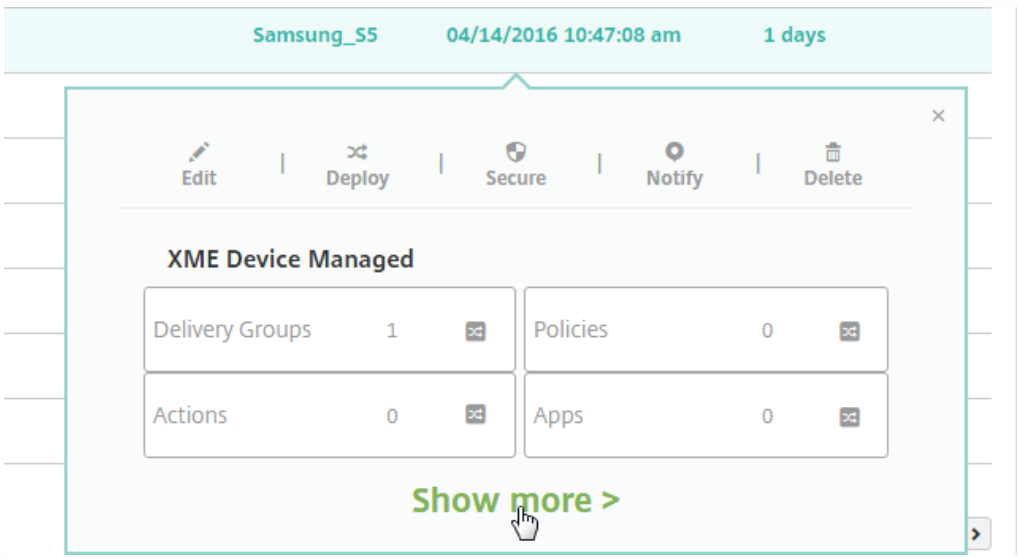
6. 展開規則を構成して、［**Next**］をクリックします。

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、［**Next**］をクリックします。

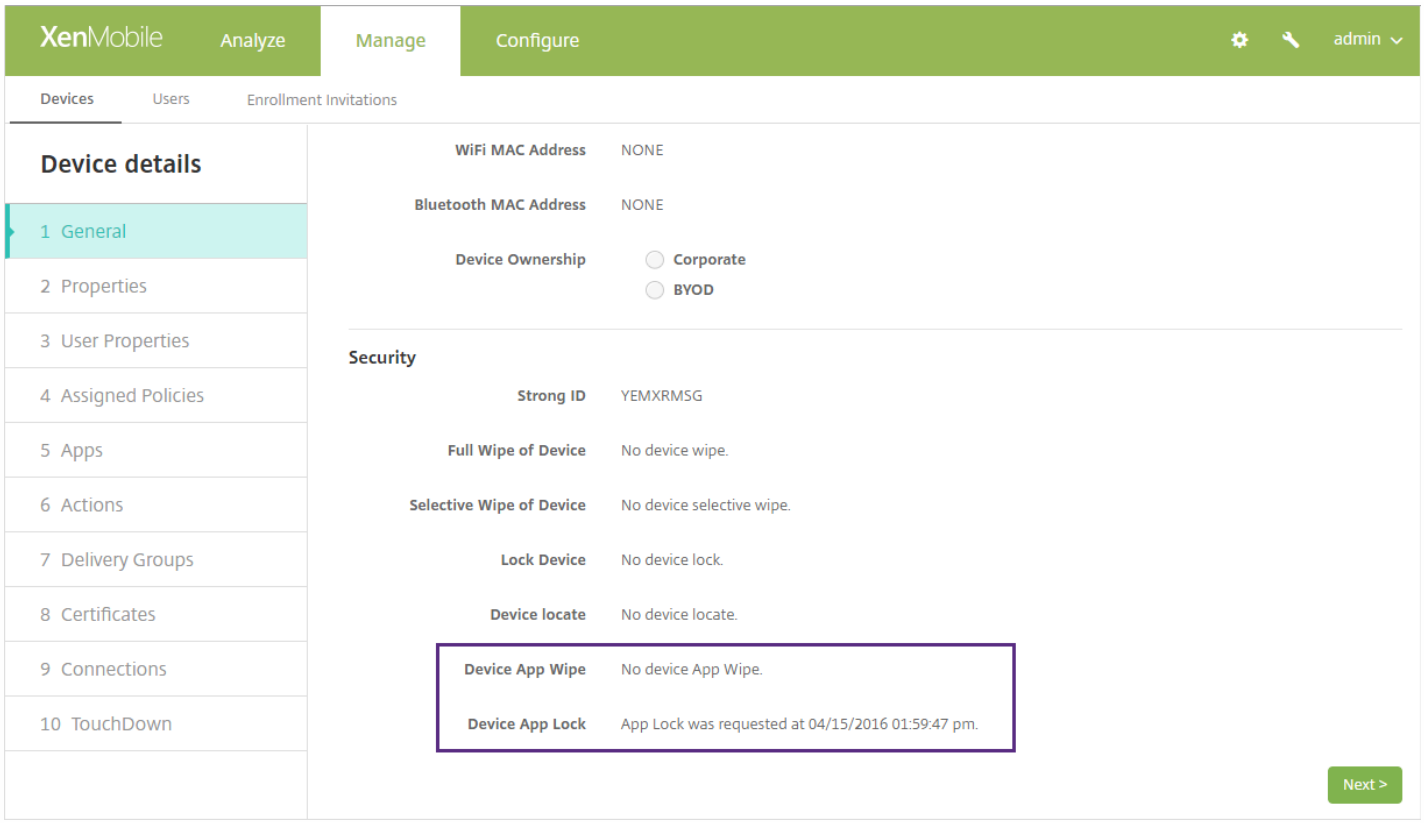
8. ［**Save**］をクリックします。

アプリロックとアプリワイプの状態を確認するには

1. ［**Manage**］**>** ［デ**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。



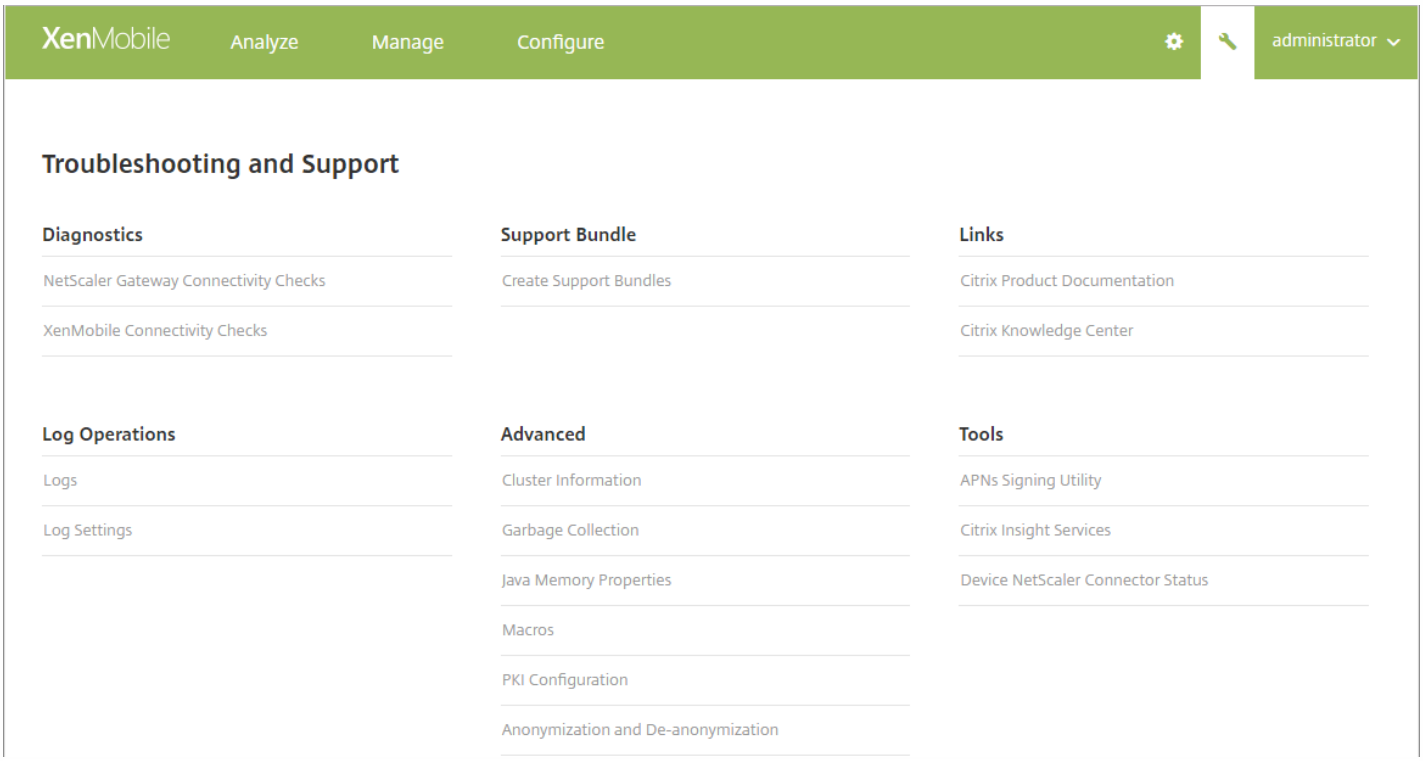
モニターとサポート

May 10, 2017

XenMobileダッシュボードとXenMobileサポートページを使用して、XenMobile Serverの監視およびトラブルシューティングができます。XenMobileサポートページを使用して、サポートに関連するいくつか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、「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。

［サポート］ページが開きます。

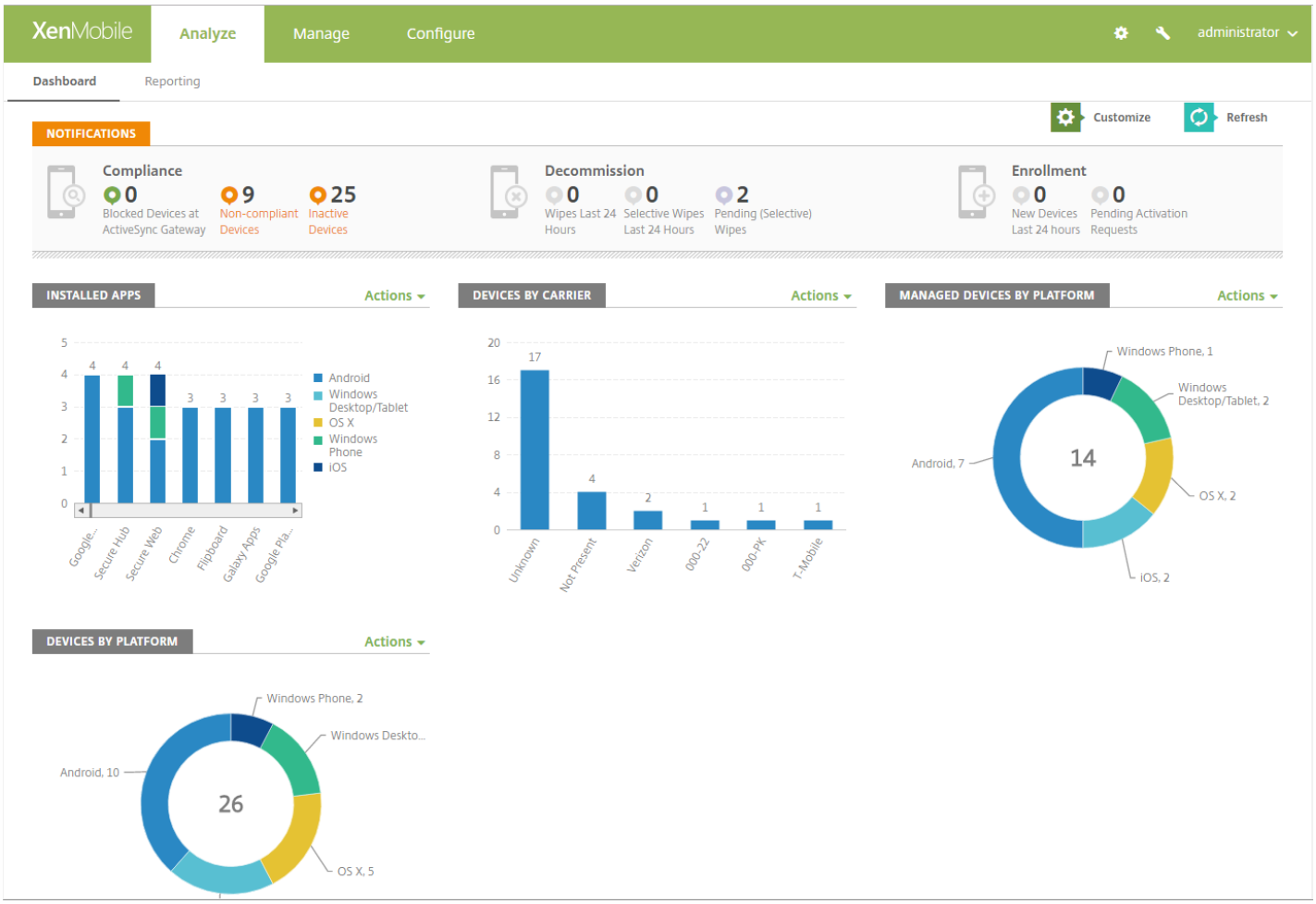


［XenMobileサポート］ページを使用して以下を行います。

- 診断へのアクセス
- サポートバンドルの作成
- 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

XenMobileコンソールのダッシュボードにアクセスして、情報を一目で確認することもできます。この情報を使用して、ウ

ジェットで問題や成功をすみやかに確認できます。

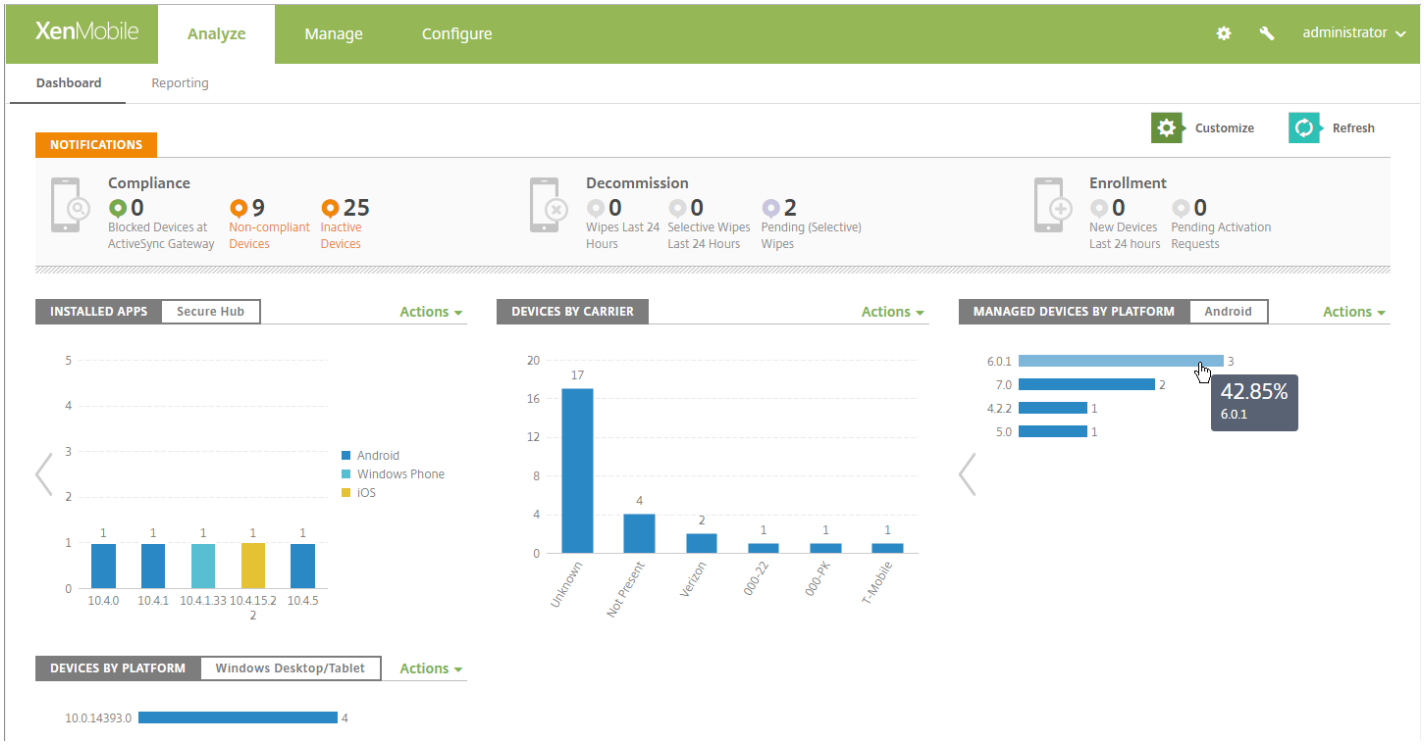


ダッシュボードは、XenMobileコンソールにサインオンすると最初に表示される画面です。コンソールの別の場所からダッシュボードにアクセスするには、［**分析**］をクリックします。ページのレイアウトを編集したり表示されるウィジェットを編集するには、ダッシュボードの［**カスタマイズ**］をクリックします。

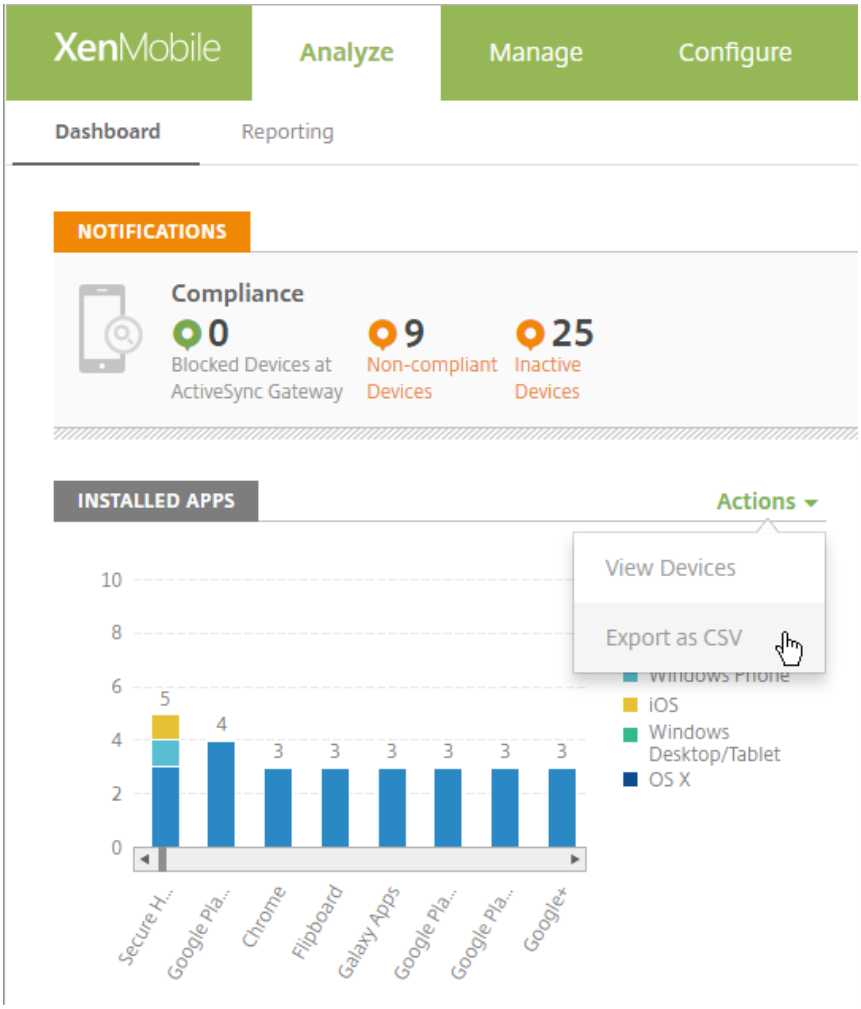
- **マイダッシュボード**：最大4つのダッシュボードを保存できます。ダッシュボードを個別に編集し、保存したダッシュボードを選択してそれぞれを表示することができます。
- **レイアウトスタイル**: この行では、ダッシュボードに表示するウィジェットの数とレイアウトを選択することができます。
- **ウィジェット選択**：ダッシュボードに表示する情報を選択することができます。
  - **通知**：左側の数字の上のチェックボックスをオンにして、ウィジェットの上に通知バーを追加します。このバーには、準拠デバイス数、非アクティブデバイス数、24時間以内にワイプまたは登録されたデバイス数が表示されます。
  - **プラットフォームごとのデバイス**：プラットフォームごとの管理対象デバイス数と管理対象外デバイス数が表示されます。
  - **キャリアごとのデバイス**：キャリアごとの管理対象デバイス数と管理対象外デバイス数が表示されます。各バーをクリックすると、プラットフォームごとの内訳が表示されます。
  - **プラットフォームにより管理されているデバイス**: プラットフォームごとの管理対象デバイス数が表示されます。
  - **プラットフォームにより管理されていないデバイス**: プラットフォームごとの管理対象外デバイス数が表示されます。このグラフに表示されるデバイスにはエージェントがインストールされている場合がありますが、特権が失効またはワイプされています。

- **ActiveSyncゲートウェイ状態ごとのデバイス**：ActiveSyncゲートウェイの状態ごとにグループ化されたデバイス数が表示されます。この情報では拒否、許可、または不明の状態が表示されます。各バーをクリックするとプラットフォームごとの内訳が表示されます。
- **所有権ごとのデバイス**：所有権の状態ごとにグループ化されたデバイス数が表示されます。この情報ではコーポレート所有、従業員所有、または不明の所有権状態が表示されます。
- **Android TouchDownライセンス状態**：TouchDownライセンスがあるデバイス数が表示されます。
- **失敗したデリバリーグループ展開**：失敗した展開の合計数がパッケージごとに表示されます。展開に失敗したパッケージのみが表示されます。
- **ブロックされた理由ごとのデバイス**：ActiveSyncでブロックされたデバイス数が表示されます。
- **インストール済みアプリ**：このウィジェットを使用して、アプリ名を入力すると、グラフにはそのアプリに関する情報が表示されます。
- **VPPアプリライセンス使用状況**：Apple Volume Purchase Programアプリのライセンス使用状況に関する統計データが表示されます。

各ウィジェットでは個々の部分をクリックして、さらに情報をドリルダウンできます。



[操作] のドロップダウンをクリックして、情報を.csvファイルとしてエクスポートすることもできます。



レポート

Feb 27, 2017

XenMobileには、以下の事前定義されたレポートが用意されており、アプリケーションおよびデバイスの展開を分析できます。

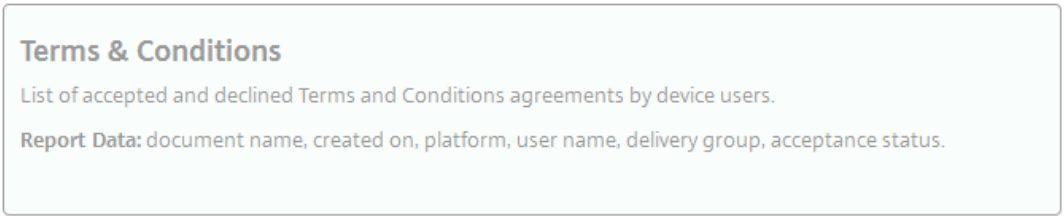
- **デバイスとユーザーを基準とするアプリ**: ユーザーのデバイスにある管理対象アプリを一覧表示します。このレポートには、デバイスにインストールされている個人用アプリは含まれません。
- **使用条件**：使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。
- **上位25のアプリ**：ほとんどのユーザーのデバイスに存在している上位25のアプリケーションを一覧表示します。
- **ジェイルブレイク/Root化されたデバイス**: Root化済みのiOSデバイスおよびジェイルブレイクされたAndroidデバイスを一覧表示します。
- **上位10のアプリ**：失敗した展開：展開に失敗したアプリケーションを10個まで一覧表示します。
- **非アクティブデバイス**: 指定した時間範囲内でアクティブでなかったデバイスを一覧表示します。
- **種類とカテゴリを基準とするアプリ**: 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。
- **デバイス登録**: すべての登録済みデバイスを一覧表示します。
- **プラットフォームを基準とするアプリ**: 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。
- **ユーザーがデバイスごとにブラックリストに登録したアプリ**: ユーザーのデバイスでブラックリストに登録されているアプリを一覧表示します。
- **デバイスとアプリ**: 管理対象アプリケーションを実行しているデバイスを一覧表示します。

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。

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。

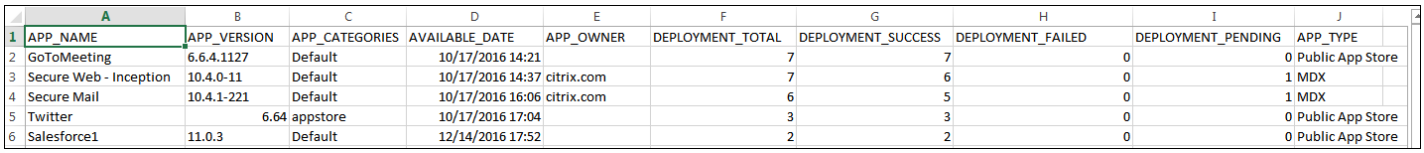
各レポートの種類には、以下のように、レポートが収集する情報の説明および具体的なレポートデータが含まれます。



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。

次の図は、Top 25 AppsをMicrosoft Excelで表示した例です。



	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store

Important

カスタムレポートの作成にSQL Serverを使用することは可能ですが、お勧めしません。この方法でSQL Serverデータベースを使用すると、XenMobile展開環境で予期しない結果になることがあります。このレポート作成方法を実行する場合は、SQLクエリが読み取り専用アカウントで実行されるようにしてください。

Mobile Service Provider

Feb 27, 2017

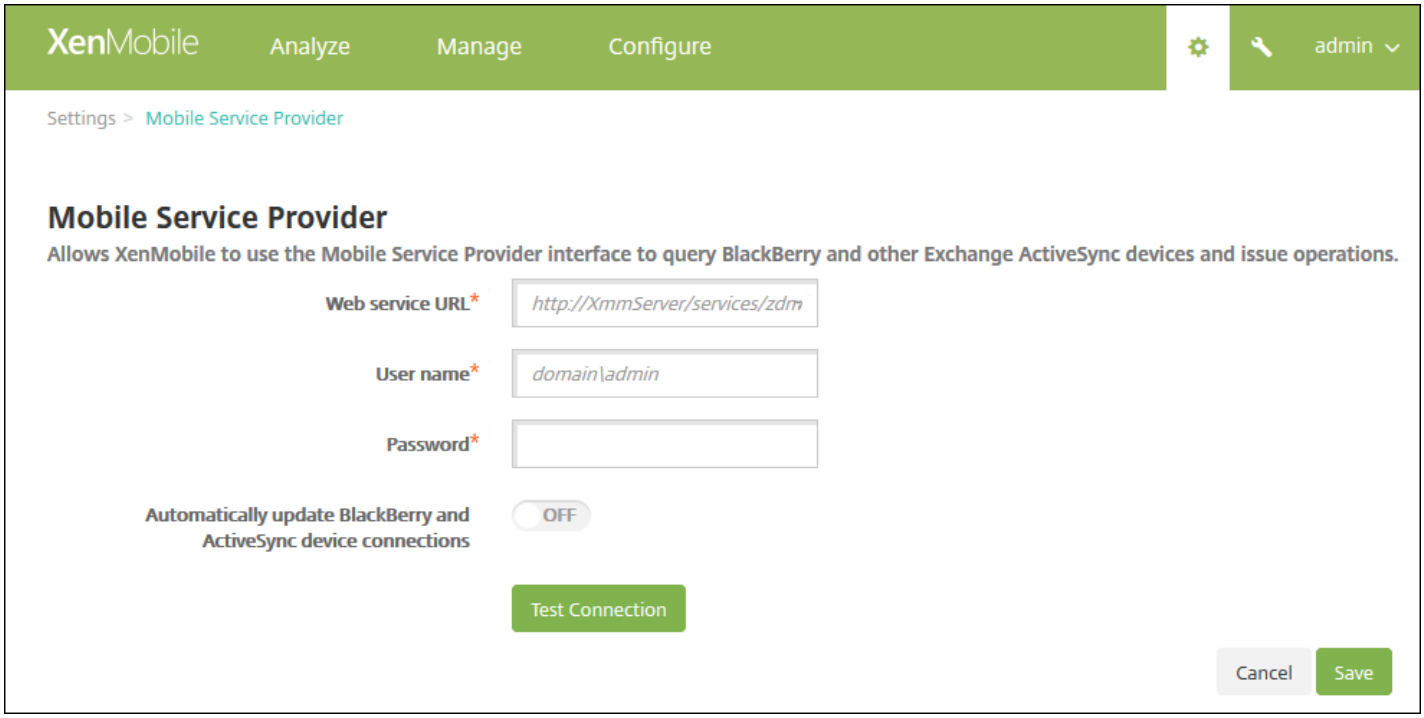
XenMobileでMobile Service Providerインターフェイスの使用を有効にして、BlackBerryやExchange ActiveSyncデバイスに対してクエリを実行したり、操作を発行したりできます。

たとえば、組織に1,000ユーザーが存在し、各ユーザーが1つまたは複数のデバイスを使用するとします。すべてのユーザーに対して、管理のためにデバイスをXenMobileに登録する必要があることを通知した後、XenMobileコンソールはユーザーが登録したデバイスの数を表示します。この設定を構成することで、Exchange Serverに接続しているデバイスの数を判断できます。これによって、次の操作を実行できます。

- ほかにデバイスを登録する必要のあるユーザーがいるかどうかを確認する。
- Exchange Serverに接続するユーザーデバイスにコマンド（データワイプなど）を発行する。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。**[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サービスURL**：WebサービスのURL（http://XmmServer/services/xdmserviceなど）を入力します。
- **ユーザー名**：「ドメイン\ユーザー」の形式でユーザー名を入力します。
- **パスワード**：パスワードを入力します。
- **BlackBerryおよびActiveSyncデバイス接続を自動的に更新**：デバイス接続を自動的に更新するかどうかを選択します。デフォルトは**[オフ]**です。
- **[接続のテスト]**をクリックして、接続を検証します。

4. **[Save]**をクリックします。

Syslog

Apr 13, 2017

XenMobile Server（オンプレミスのみ）を構成して、ログファイルをシステムログ（syslog）サーバーに送信できます。サーバーのホスト名またはIPアドレスが必要です。

Syslogは、監査モジュール（アプライアンス上で実行）とサーバー（リモートシステムで実行可能）の2つのコンポーネントを使用する、標準ロギングプロトコルです。Syslogプロトコルでは、データ転送でユーザーデータプロトコル（UDP）を使用します。管理者イベントとユーザーイベントが記録されます。

サーバーを構成して、以下の種類の情報を収集できます。

- XenMobileで実行されたアクションの記録が含まれるシステムログ
- XenMobileのシステムアクティビティの時系列の記録が含まれる監査ログ

syslogサーバーがアプライアンスから収集したログ情報は、メッセージ形式でログファイルに保存されます。通常、これらのメッセージには次の情報が含まれています。

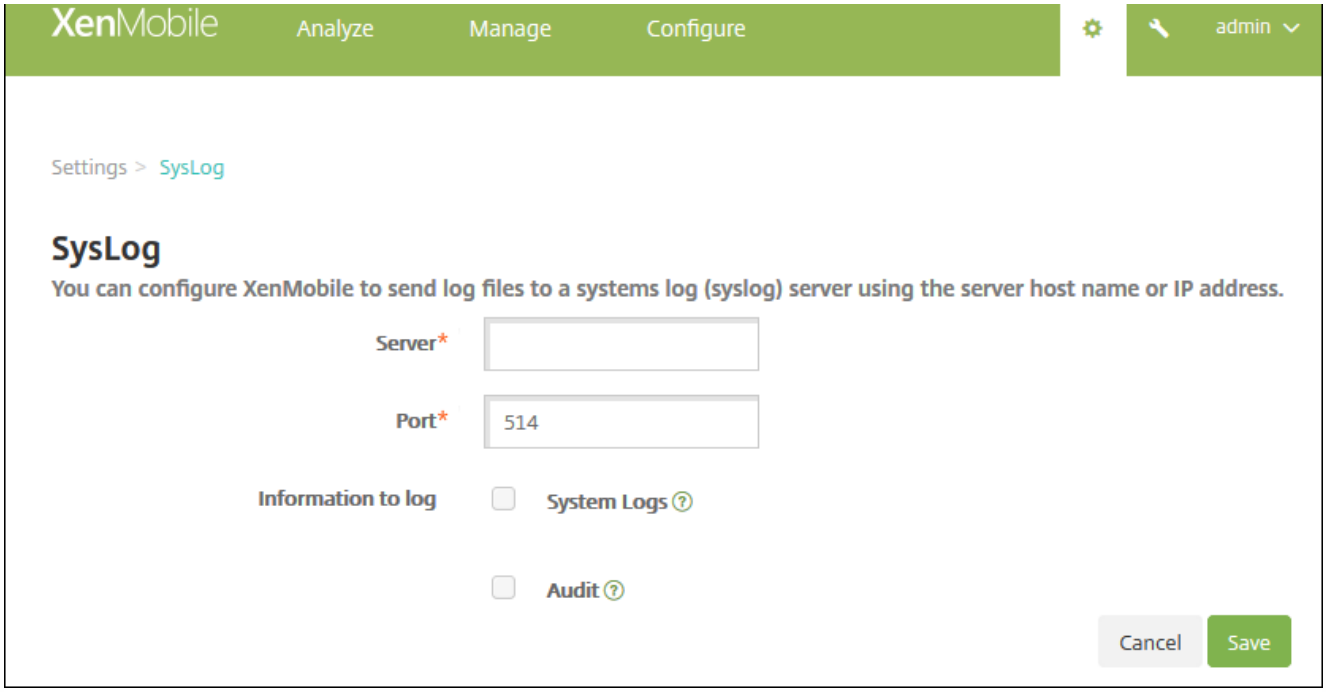
- ログメッセージを生成したアプライアンスのIPアドレス
- タイムスタンプ
- メッセージの種類
- イベントに関連付けられたログレベル（重要、エラー、通知、警告、情報、デバッグ、アラート、または緊急）
- メッセージの情報

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サービス（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、XenMobile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、**［すべてダウンロード］**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。

- **サーバー**： syslogサーバーのIPアドレスまたは完全修飾ドメイン名（FQDN）を入力します。
- **ポート**： ポート番号を入力します。デフォルトのポートは、514です。
- **ログを記録する情報**： **[システムログ]** チェックボックスおよび **[監査]** チェックボックスをオンまたはオフにします。
  - システムログには、XenMobileで実行されたアクションが含まれます。
  - 監査ログには、XenMobileのシステムアクティビティの時系列の記録が含まれます。

4. **[Save]** をクリックします。

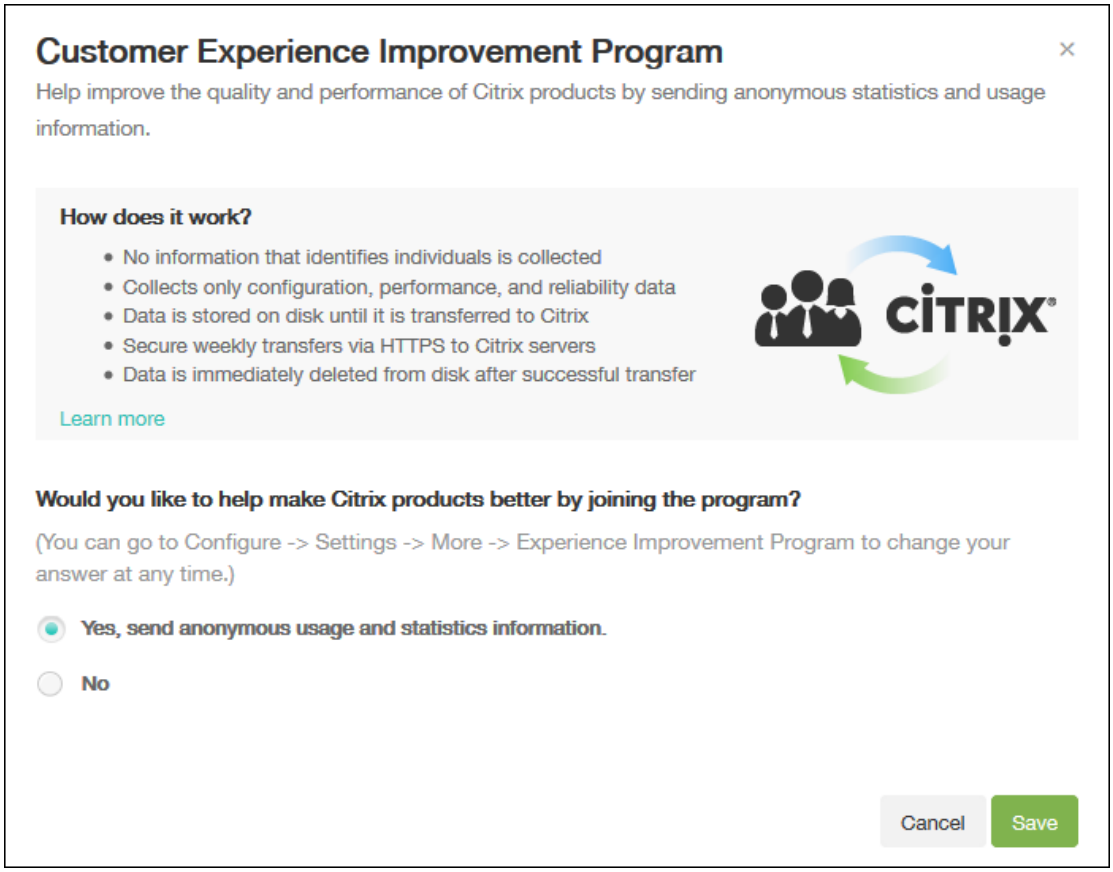
カスタマーエクスペリエンス向上プログラム

Feb 27, 2017

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。

CEIPで参加を選択する

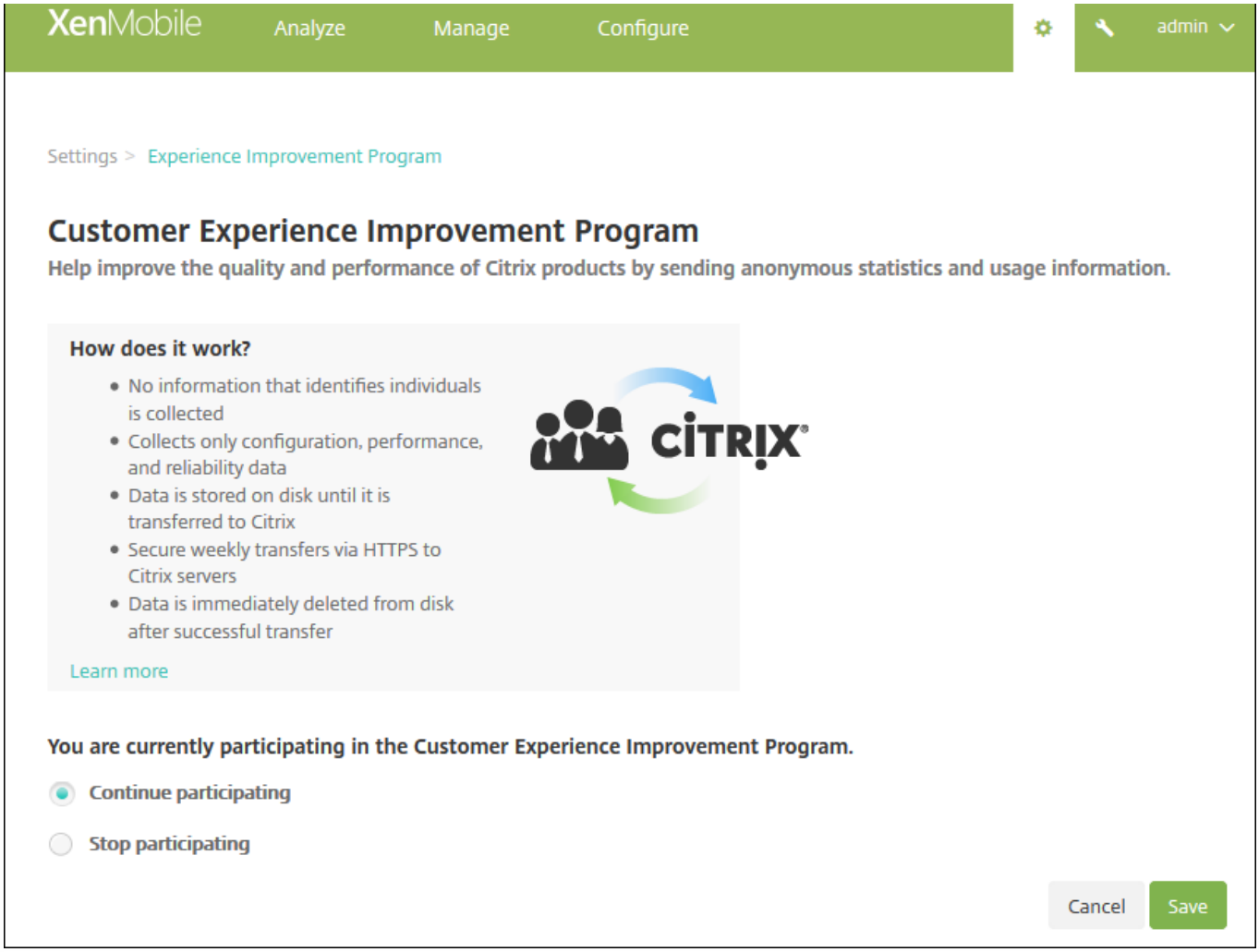
XenMobileの初回インストール時、または更新時に、参加を促す以下のダイアログボックスが開きます。



CEIP参加設定の変更

1. CEIP参加設定を変更するには、XenMobileコンソールで右上の歯車アイコンをクリックして**[設定]**ページを開きます。

2. **[サーバー]**の下で**[エクスペリエンス向上プログラム]**をクリックします。**[カスタマーエクスペリエンス向上プログラム]**ページが開きます。表示される実際のページは、現在CEIPに参加しているかどうかによって異なります。



3. 現在CEIPに参加していて、中止を希望する場合、 **[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. **[保存]** をクリックします。

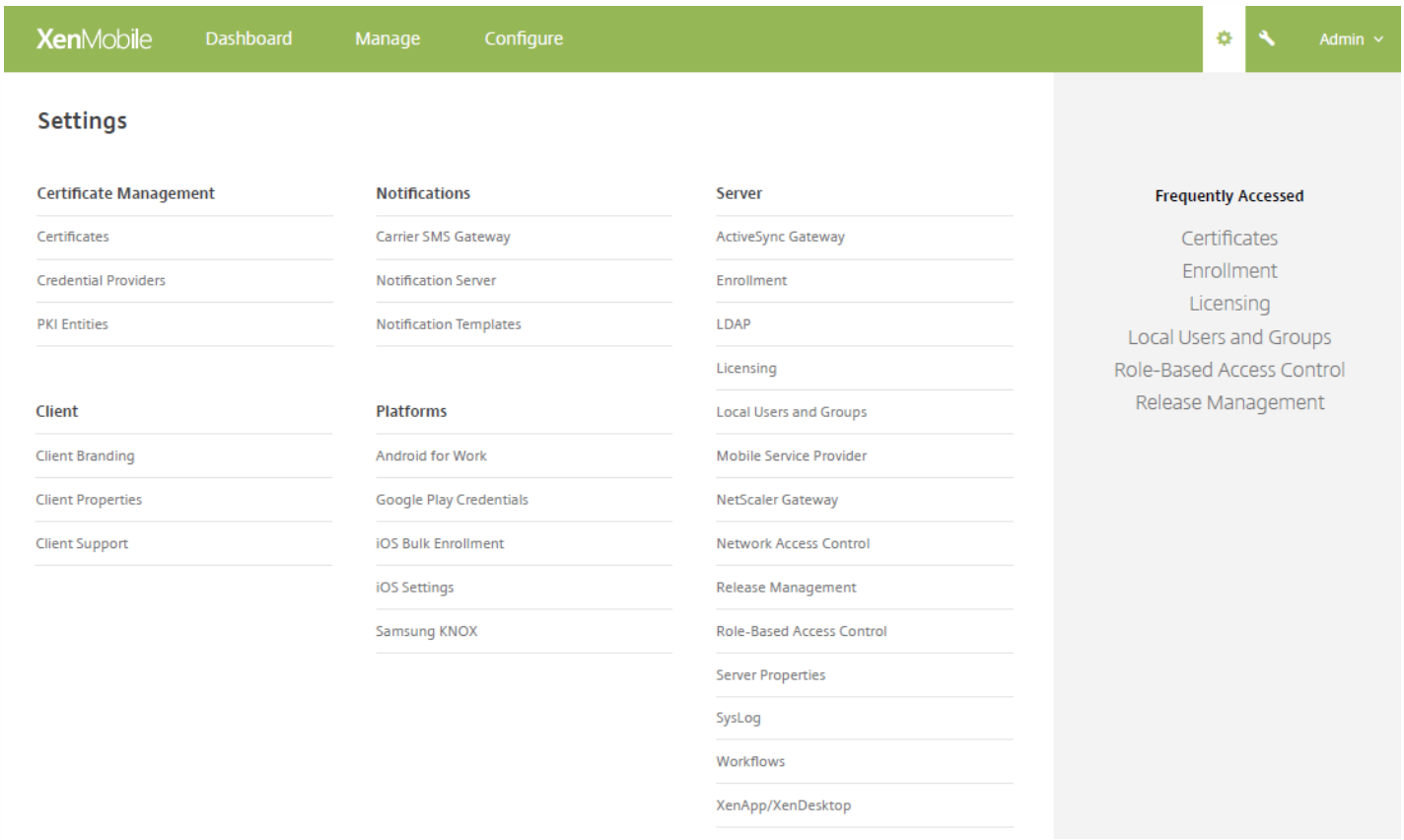
サポートオプションとリモートサポート

Apr 26, 2017

サポートスタッフへの問い合わせ用のメールアドレスをユーザーに提供できます。ユーザーがデバイスからサポートを要求すると、このメールアドレスが表示されます。

ユーザーがデバイスからヘルプデスクにログを送信する方法も構成できます。ログを直接送信するか、メールで送信するように構成できます。

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



2. [**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。

- **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、[Store logs on ShareFile]の設定が表示されます。[Store logs on ShareFile]を有効にすると、ログはShareFileに直接送信されます。このオプションを有効にしない場合、ログはXenMobileに送信されてからヘルプデスクにメール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。サーバーの問題に関するログの送信にクライアントのメールを使用しない場合は、このオプションを無効にすることができます。ただし、このオプションを無効にすると、サーバーに問

題があってもログが送信されません。
- [**by email**] を有効にすると、ログの送信では常にクライアントのメールが使用されます。

4. [**Save**] をクリックします。

リモートサポート

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。

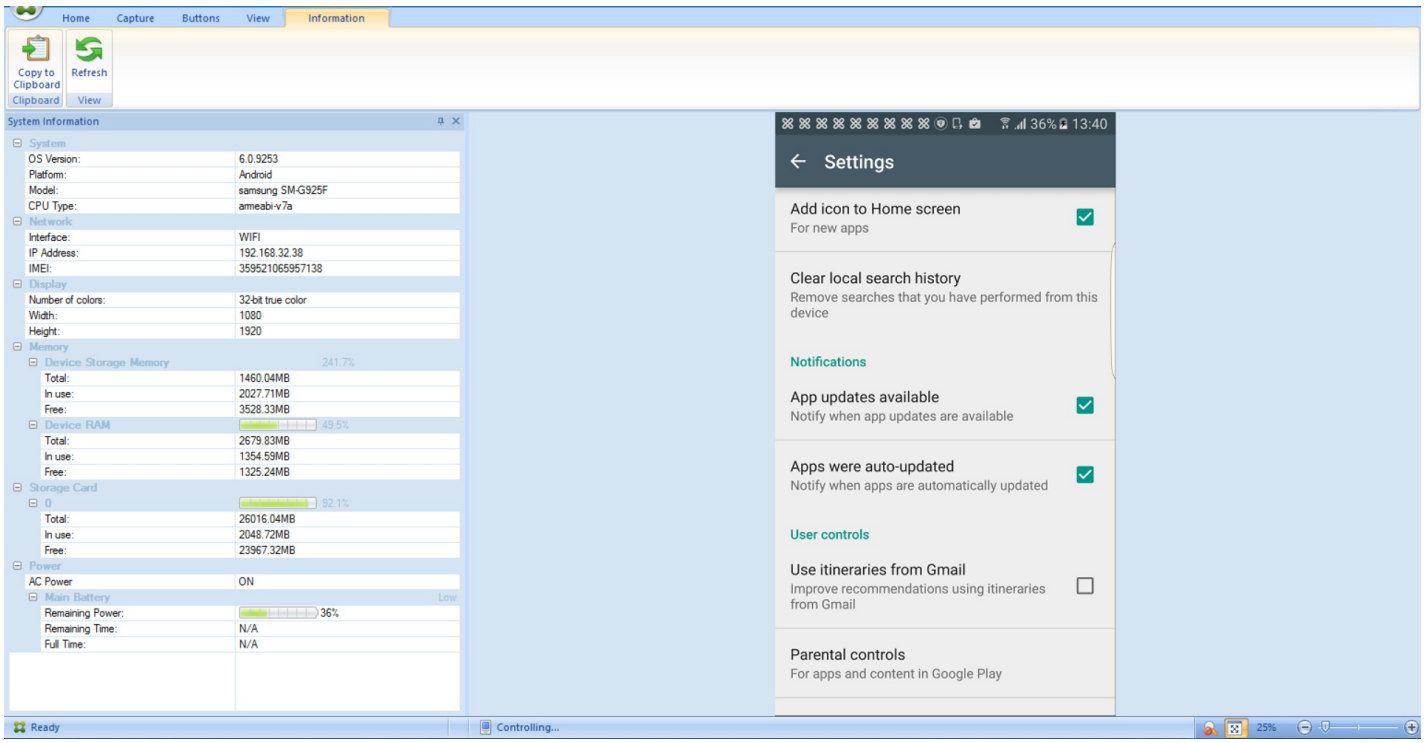
Remote Supportは、すべてのWindows MobileデバイスおよびAndroidのSamsung SAFEデバイスおよびSamsung以外のデバイスで使用できます。Remote Support Clientは、Windows CEデバイスおよびSamsung Androidデバイス向けのXenMobile Service Version 10.xでは使用できません。

画面のキャストはSamsung KNOXでのみサポートされています。

iOSデバイスのリモート制御はサポートされていません。

リモート制御セッション時の動作は次のようになります。

- ユーザーのモバイルデバイスには、リモート制御セッションがアクティブであることを示すアイコンが表示されます。
- Remote Supportアプリケーションウィンドウが開いて、［Remote Contorol］ウィンドウに制御対象デバイスが表示されます。



Remote Supportで、次のことを実行できます。

- ユーザーデバイスにリモートでサインオンし、デバイスの画面を制御する。ユーザーはヘルプデスク担当者による画面の動を確認できるため、ユーザーのトレーニングとしても役に立つことがあります。
- リアルタイムでリモートデバイス内を移動して修復する。構成の変更、オペレーティングシステムの問題のトラブルシューティング、問題があるアプリケーションやプロセスの無効化または終了を行うことができます。

- ネットワークアクセスの無効化、不正プロセスの停止、アプリまたはマルウェアの削除をリモートに実行することで、ほかのモバイルデバイスに脅威が広がる前に、その脅威を隔離して封じこめる。
- ユーザーがデバイスを見つけられるように、デバイスの着信音や電話の発信をリモートで有効にする。デバイスを見つけることができなかった場合は、重要なデータが侵害されないように、デバイスにワイプを実行できます。

Remote Supportでは、サポート担当者に次の機能も提供されます。

- 1つまたは複数のXenMobileインスタンスについて、接続しているすべてのデバイスの一覧を表示する。
- デバイスのモデル、オペレーティングシステムのレベル、IMEI（International Mobile Station Equipment Identity：国際移動体装置識別番号）、シリアル番号、メモリおよびバッテリーの状態、接続状態などのシステム情報を表示する。
- XenMobileのユーザーおよびグループを表示する。
- アクティブなプロセスの表示や停止、およびモバイルデバイスの再起動を行うためのデバイスタスクマネージャーを実行する。
- モバイルデバイスと中央ファイルサーバー間の双方向のリモートファイル転送を実行する。
- 1つまたは複数のモバイルデバイスに対するソフトウェアプログラムの一括ダウンロードおよびインストール。
- デバイスのレジストリキーのリモートからの構成。
- 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Windowsベースのコンピューターにインストールします。ポートの要件については、「ポート要件」を参照してください。

サポートされるプラットフォームは、以下のとおりです。

- Intel Xeon/Pentium 4-1GHz以上のワークステーションクラス
- 512MB以上のRAM
- 100MB以上の空きディスク領域

以下のオペレーティングシステムがサポートされています。

- Microsoft Windows 2003 Server Standard EditionまたはEnterprise Edition SP1以降
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2以降
- Microsoft Windows Vista SP1以降
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Remote Supportソフトウェアをインストールするには

1. Remote Support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。
   Remote Supportのファイル名はXenMobileRemoteSupport-9.0.0.35265.exeです。

3. Remote Supportインストーラーをダブルクリックし、表示されるインストールウィザードの指示に従います。

コマンドラインからRemote Supportをインストールするには：

次のコマンドを実行します。

RemoteSupport.exe /S

*RemoteSupport*にはインストールプログラムの名称を指定します。次に例を示します。

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。

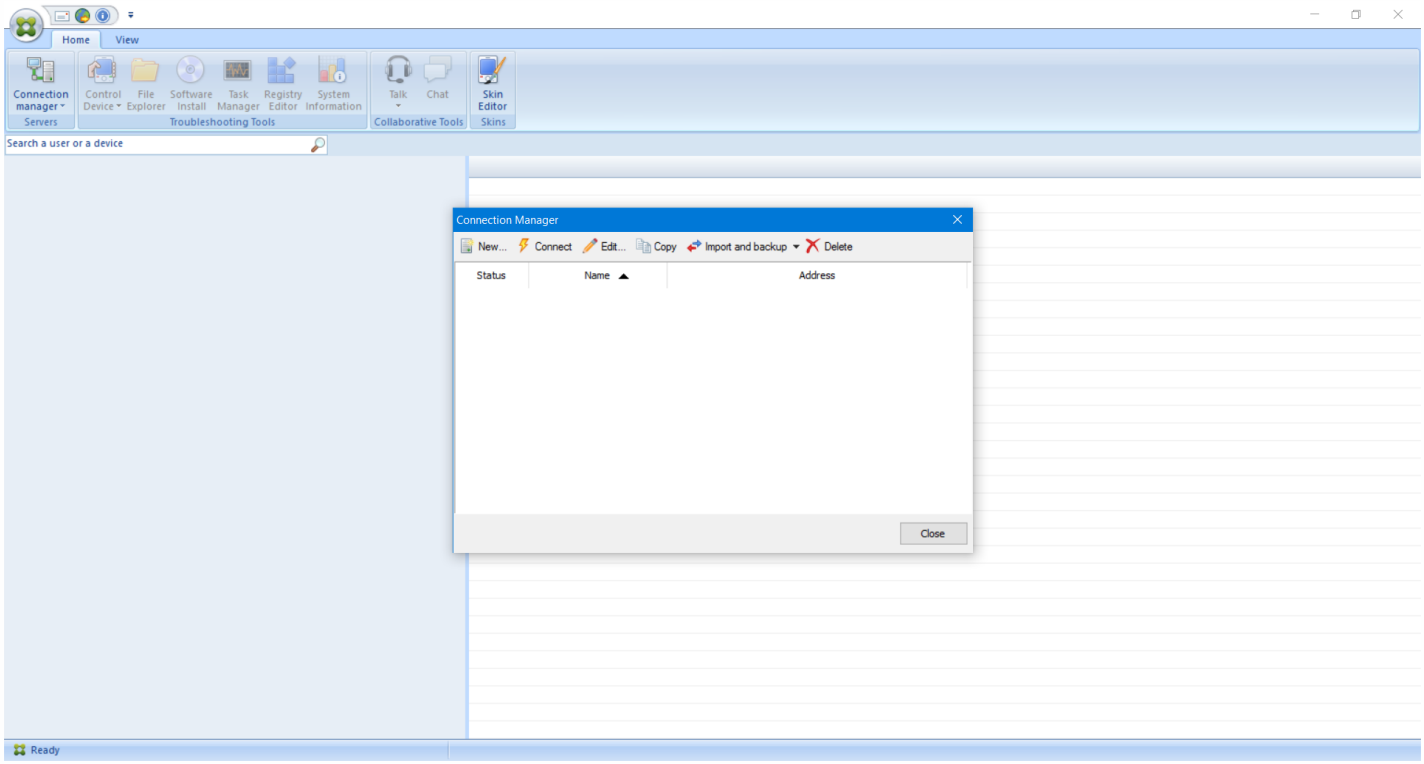
- /S：デフォルトのパラメーターを使用してRemote Supportソフトウェアをインストールします。
- /D=dir:。カスタムのインストールディレクトリを指定します。

Remote SupportをXenMobileに接続するには

管理対象デバイスへのリモートサポート接続を確立するには、Remote Supportからの接続を、該当のデバイスを管理する1つまたは複数のXenMobile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MDMポリシーで定義したアプリトンネル上で実行されます。Remote SupportをXenMobileに接続するには、アプリトンネルを定義します。詳しくは、「アプリケーショントンネリングデバイスポリシー」を参照してください。

1. Remote Supportソフトウェアを起動し、XenMobileの資格情報を使用してサインオンします。

2. [**Connection Manager**]で、 [**New**]をクリックします。



3. [**Connection Configuration**]ダイアログボックスの [**Server**]タブで、次の値を入力します。

a. **[Configuration name]** に構成エントリの名前を入力します。

b. **[Server IP address or name]** にXenMobileサーバーのIPアドレスまたはDNS名を入力します。

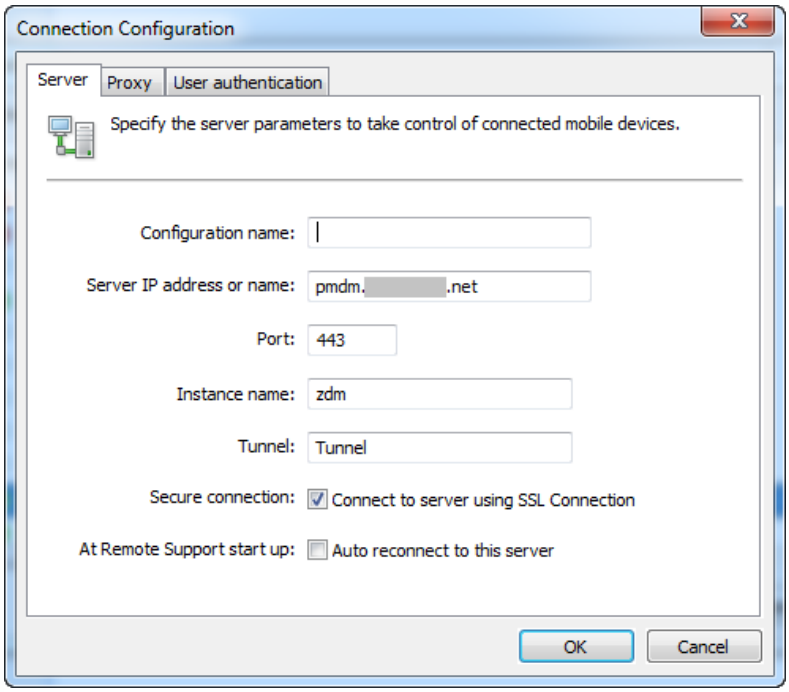
c. **[Port]** に、XenMobileサーバー構成で定義されているTCPポート番号を入力します。

d. XenMobileがマルチテナント環境に含まれている場合は、**[Instance name]** にインスタンス名を入力します。

e. **[Tunnel]** にトンネルポリシーの名前を入力します。

f. **[Connect to server using SSL Connection]** チェックボックスをオンにします。

g. Remote Supportアプリケーションが起動するたびに、構成したXenMobile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。

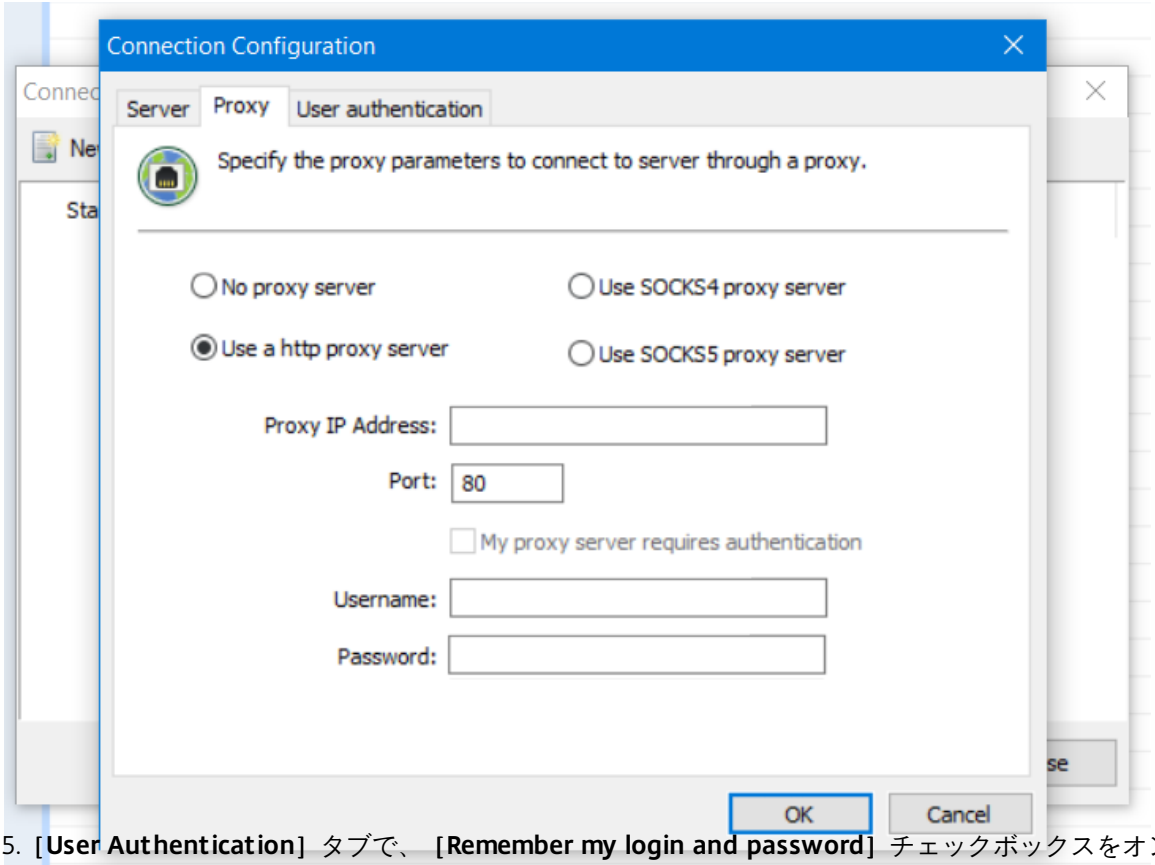
a. **[Proxy IP Address]** に、プロキシサーバーのIPアドレスを入力します。

b. **[Port]** に、プロキシで使用するTCPポート番号を入力します。

c. プロキシサーバーでトラフィックの許可に認証が必要な場合は、**[My proxy 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。

e. **[Password]** に、プロキシサーバーで認証するパスワードを入力します。



5. [**User Authentication**] タブで、 [**Remember my login and password**] チェックボックスをオンにして資格情報を入力します。

6. [**OK**] をクリックします。

XenMobileに接続するには、作成した接続をダブルクリックし、この接続用に構成したユーザー名とパスワードを入力します。

Samsung KNOXデバイスでリモートサポートを有効にするには

XenMobileでRemote Supportポリシーを作成して、Samsung KNOXデバイスへのリモートアクセスを行うことができます。次の2種類のサポートを構成できます。

- **基本**：デバイスに関する診断情報を表示できます。たとえば、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率とCPU使用率）、およびインストールされているソフトウェアフォルダーの内容などです。
- **プレミアム**：デバイスの画面をリモートで制御できます。たとえば、ウィンドウの色の制御、ヘルプデスクとユーザー間のVoIPセッションの確立、ヘルプデスクとユーザー間でのチャットセッションの確立などを行うことができます。

  プレミアムサポートでは、XenMobileコンソールでSamsung MDMライセンスキーのデバイスポリシーを構成する必要があります。このポリシーを構成する場合は、**Samsung KNOX**プラットフォームのみを選択してください。Samsung SAFEプラットフォームについては、XenMobileへの登録時にELMキーが自動でSamsungデバイスに展開されます。このため、このポリシーでSamsung SAFEプラットフォームは選択しないでください。詳しくは、「Samsung MDMライセンスキー」を参照してください。

リモートサポートポリシーの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コンソールで定義したXenMobileユーザーグループが表示されます。デフォルトでは、現在接続されているユーザーが含まれているグループのみが表示されます。ユーザーエントリの横に、各ユーザーのデバイスが表示されます。

1. すべてのユーザーを表示するには、左側の列の各グループを展開します。
   XenMobile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。制御対象デバイスは次の方式で操作できます。

- デバイス画面のメインウィンドウまたは別の浮動ウィンドウを制御する（色の制御を含む）。
- ヘルプデスクとユーザー間のボイスオーバーIP（VoIP）セッションを確立する。VoIP設定を構成します。
- ユーザーとのチャットセッションを確立する。
- デバイスのタスクマネージャーにアクセスして、メモリの使用率、CPUの使用率、実行中のアプリケーションなどのアイテムを管理する。
- モバイルデバイスのローカルディレクトリを探索する。ファイルを転送する。
- Windows Mobileデバイス上のデバイスレジストリを編集する。
- デバイスシステム情報およびインストールされているすべてのソフトウェアを表示する。
- XenMobileサーバーとモバイルデバイスの接続状態を更新する。

接続確認

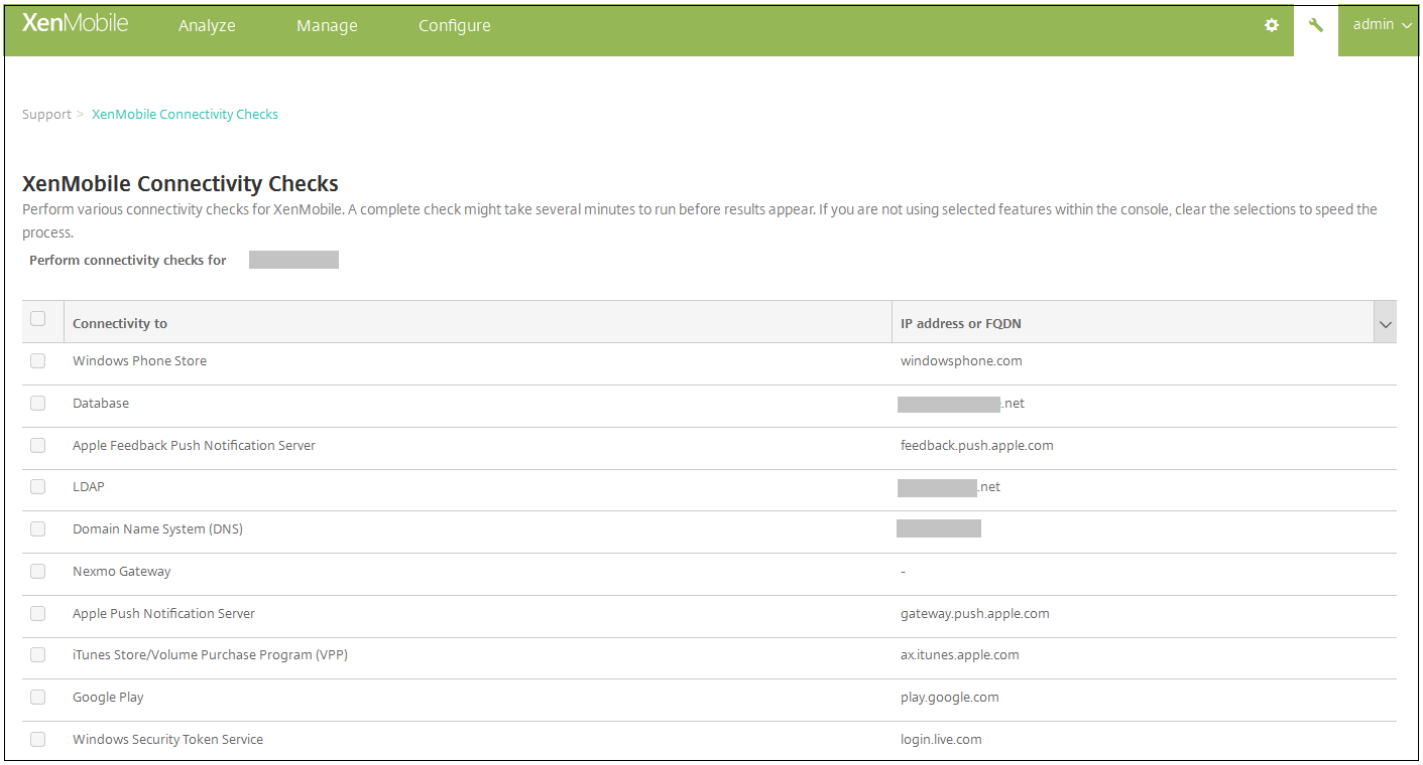
Feb 27, 2017

XenMobileの［**サポート**］ページで、NetScaler GatewayおよびそのほかのサーバーやXenMobileの接続を確認できます。

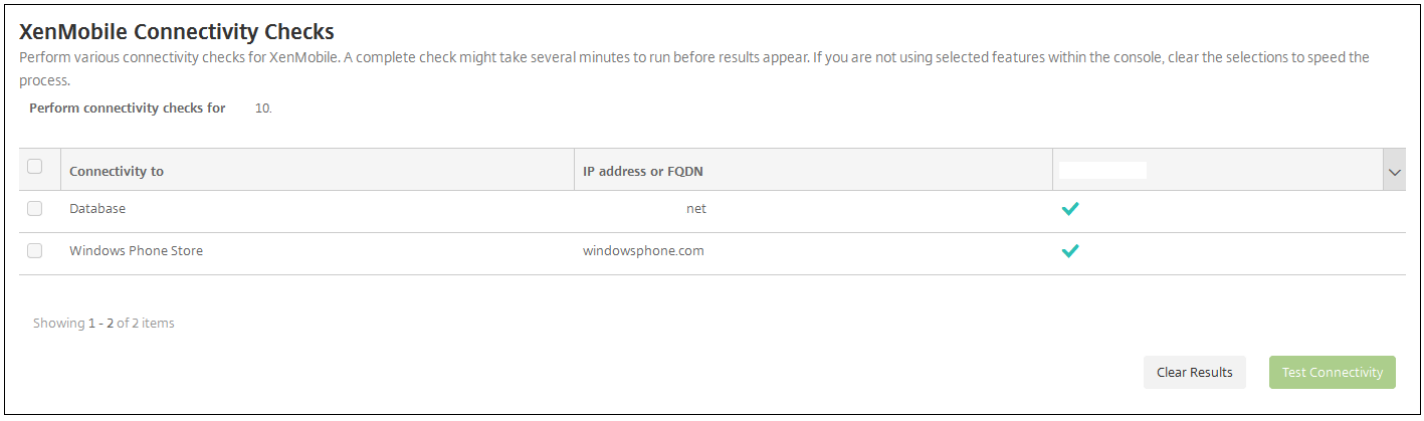
XenMobileの接続確認の実行

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。

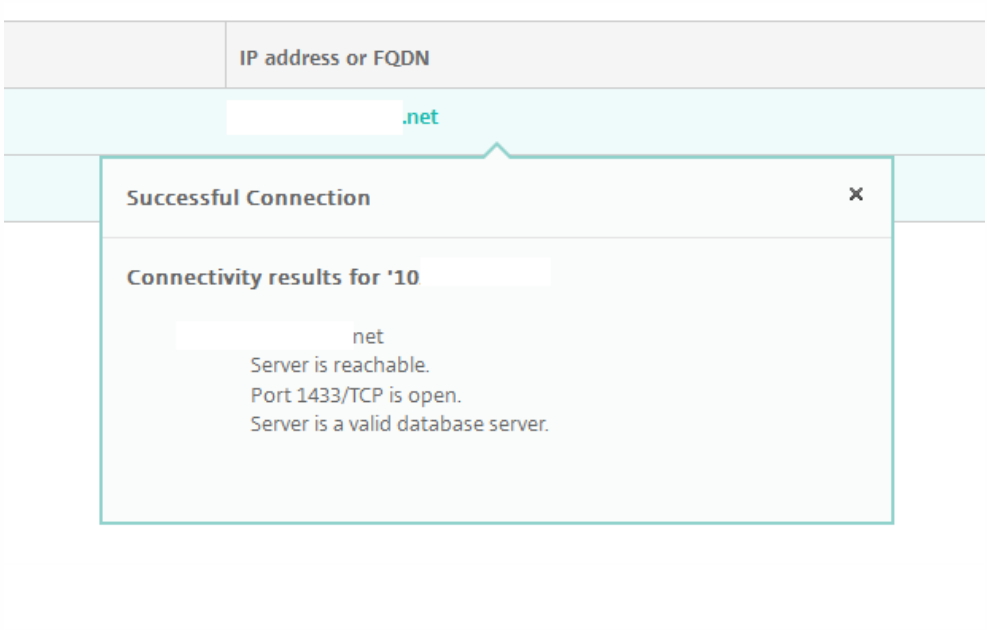
2. ［**診断**］の下の［**XenMobile接続性チェック**］をクリックします。［**XenMobile接続性チェック**］ページが開きます。XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。



2. 接続テストに含めるサーバーをオンにして、［**接続性をテスト**］をクリックします。［テスト結果］ページが開きます。

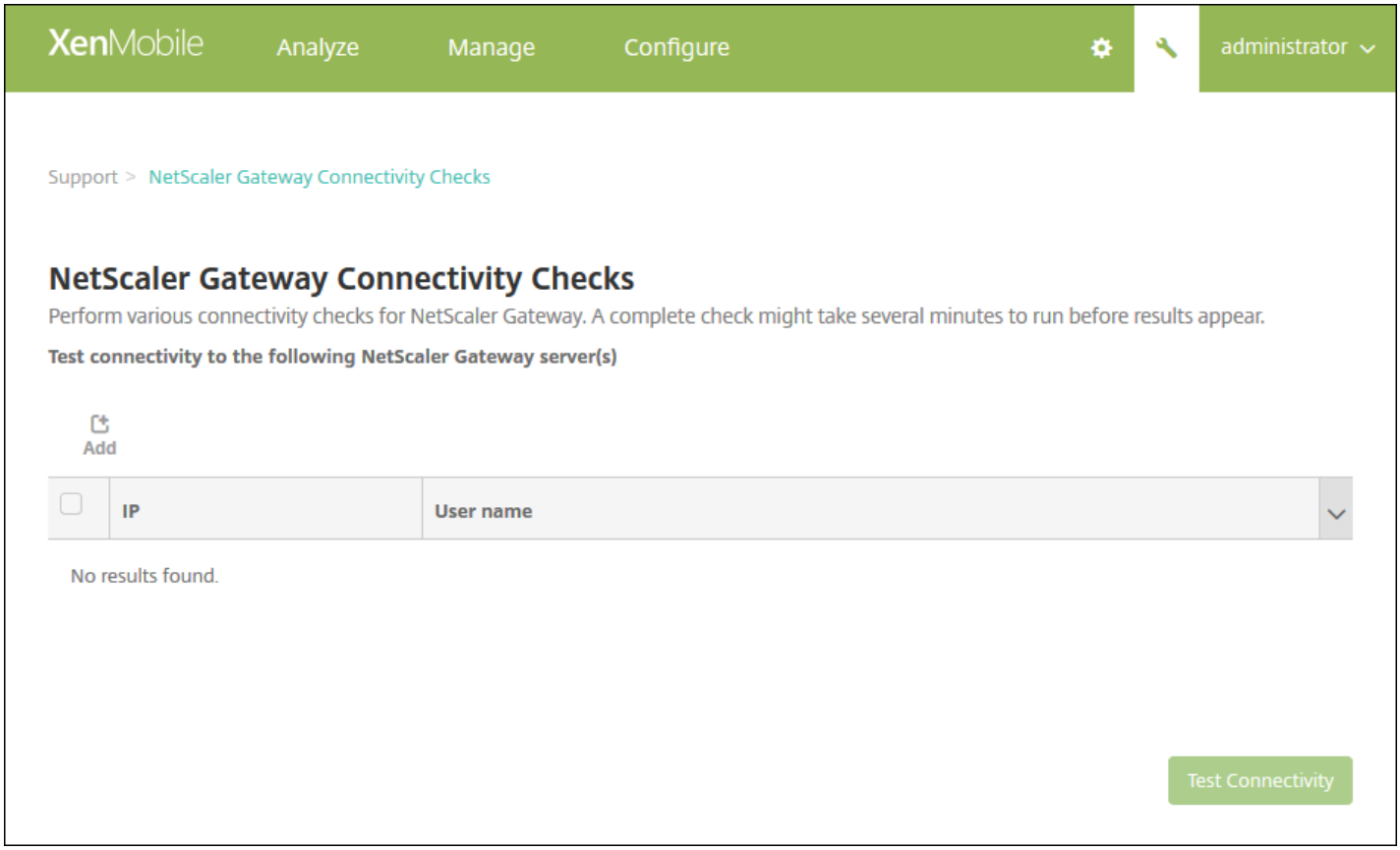


3. ［テスト結果］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

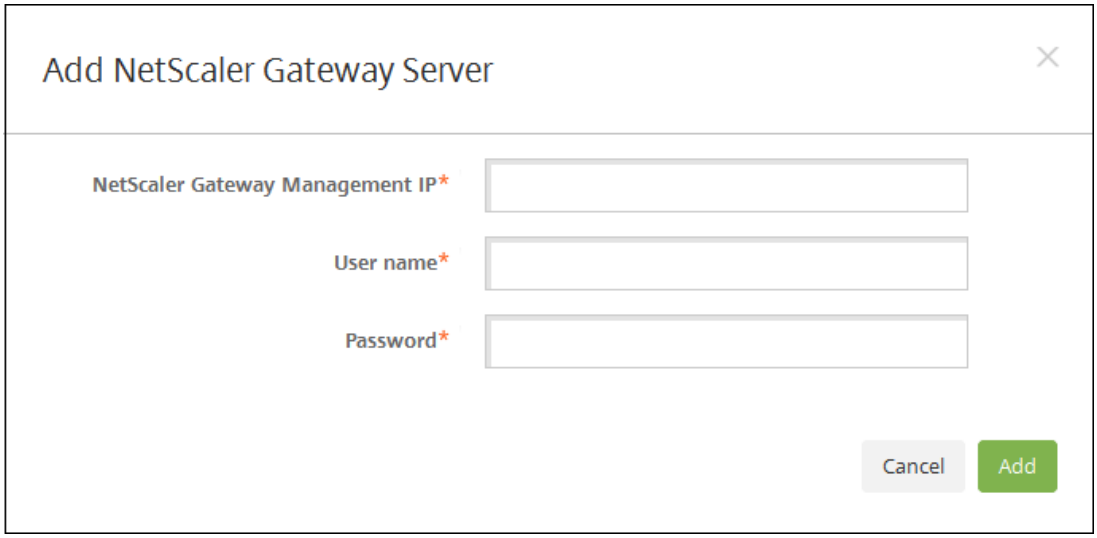


NetScaler Gatewayの接続確認の実行

1. **［サポート］**ページで、**［診断］**の下の**［NetScaler Gateway接続性チェック］**をクリックします。**［NetScaler Gateway接続性チェック］**ページが開きます。NetScaler Gatewayサーバーが追加されていない場合、表は空白です。



2. **［追加］**をクリックします。**［NetScaler Gatewayサーバーの追加］**ダイアログボックスが開きます。



3. **[NetScaler Gateway管理IP]** ボックスに、テストするNetScaler Gatewayを実行しているサーバーのIPアドレスを入力します。

注： 既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、IPアドレスは入力されています。

4. このNetScaler Gatewayの管理者資格情報を入力します。

注： 既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、ユーザー名は入力されています。

5. **[追加]** をクリックします。NetScaler Gatewayが、 **[NetScaler Gateway接続性チェック]** ページの表に追加されます。

6. NetScaler Gatewayサーバーを選択して、 **[接続性をテスト]** をクリックします。［テスト結果］の表に結果が表示されます。

7. ［テスト結果］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

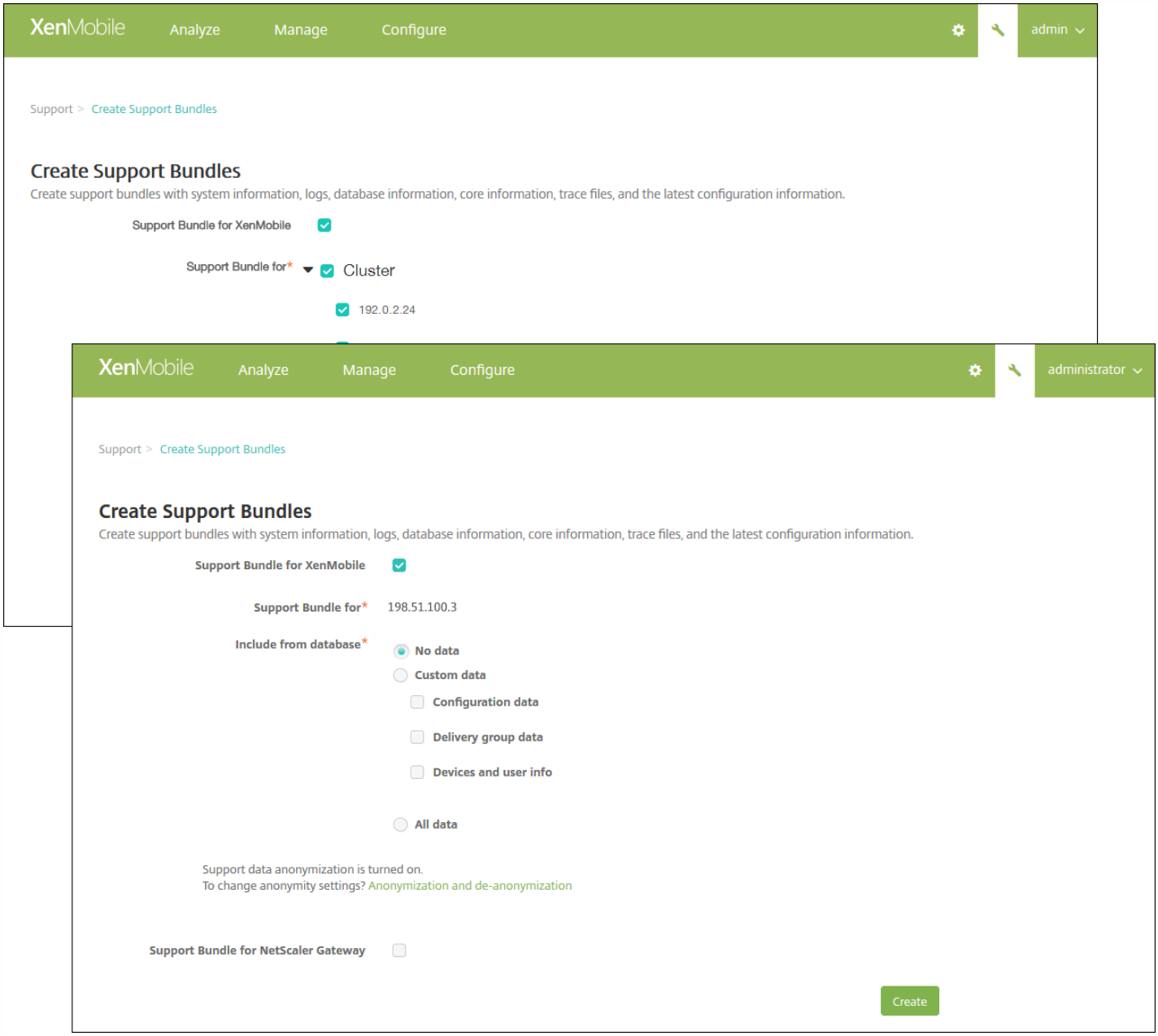
サポートバンドル

Feb 27, 2017

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。**[サポート]** ページが開きます。

2. **[サポート]** ページで、 **[サポートバンドルの作成]** をクリックします。 **[サポートバンドルの作成]** ページが開きます。XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。



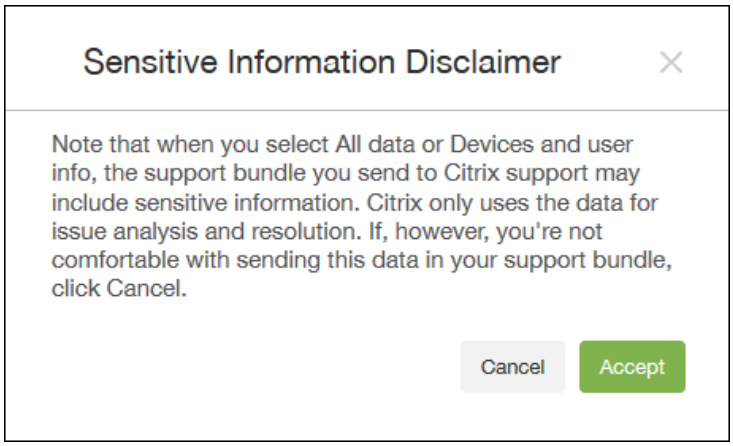
3. **[XenMobileのサポートバンドル]** チェックボックスがオンになっていることを確認します。

4. XenMobile環境内にクラスターノードがある場合は、**[サポートバンドルの対象]** ですべてのノードを選択するか、データの取得先にするノードの組み合わせを選択できます。

5. **[データベースから包含]** で、次のいずれかを実行します。

- **[データなし]** をクリックします。
- **[カスタムデータ]** をクリックして、次のいずれかまたはすべてをオンにします（デフォルトでは、すべてのオプションが選択されています）。
  - **構成データ**： 証明書構成とデバイスマネージャーポリシーを含めます。
  - **デリバリーグループデータ**： アプリ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。
  - **デバイスおよびユーザー情報**： 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。
- **[すべてのデータ]** をクリックします。

注： **[デバイスおよびユーザー情報]** または **[すべてのデータ]** を選択し、かつこれが初めて作成するサポートバンドルである場合は、 **[機密情報に関する免責事項]** ダイアログボックスが開きます。免責事項を読み、**[承諾]** または **[キャンセル]** をクリックします。 **[キャンセル]** をクリックした場合は、サポートバンドルをCitrixにアップロードできません。**[承諾]** をクリックした場合は、サポートバンドルをCitrixにアップロードでき、次回デバイスやユーザーデータを含むサポートバンドルを作成するときに免責事項が表示されなくなります。

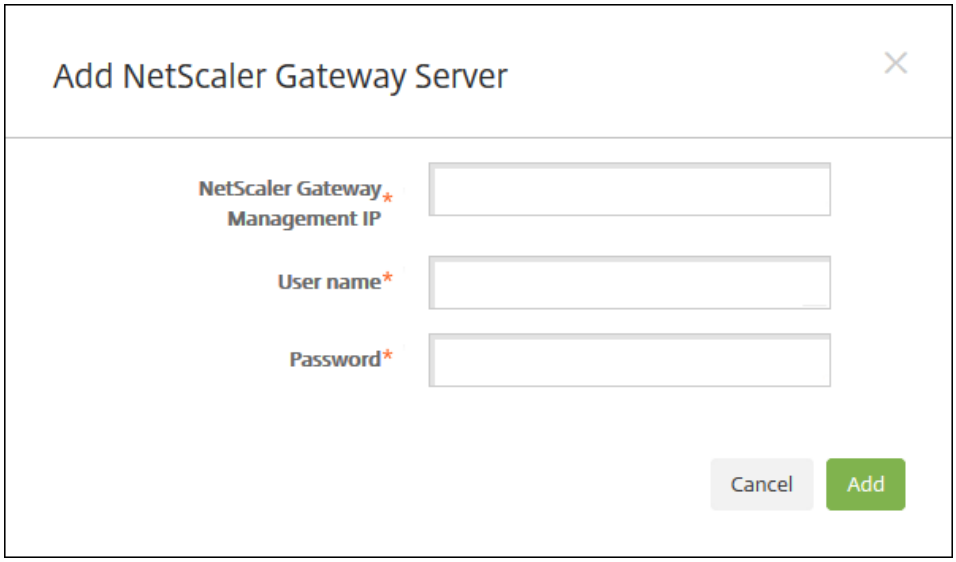


6. **[Support data anonymization is turned on]** オプションのデフォルト設定はデータの匿名化で、機密性の高いユーザー、サーバー、ネットワークのデータをサポートバンドルで匿名化します。

この設定を変更するには、 **[Anonymization and de-anonymization]** を選択します。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。

7. NetScaler Gatewayからのサポートバンドルを含める場合は、 **[NetScaler Gatewayのサポートバンドル]** チェックボックスをオンにして以下を行います。

a. **[追加]** をクリックします。 **[NetScaler Gatewayサーバーの追加]** ダイアログボックスが開きます。



b. **[NetScaler Gateway管理IP]** ボックスに、サポートバンドルデータの取得先にするNetScaler GatewayのNetScaler管理IPアドレスを入力します。

注： 既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、IPアドレスは入力されています。

c. **[ユーザー名]** ボックスと **[パスワード]** ボックスに、NetScaler Gatewayを実行しているサーバーへのアクセスに必要なユーザー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. **[追加]** をクリックします。新しいNetScaler Gatewayサポートバンドルが表に追加されます。

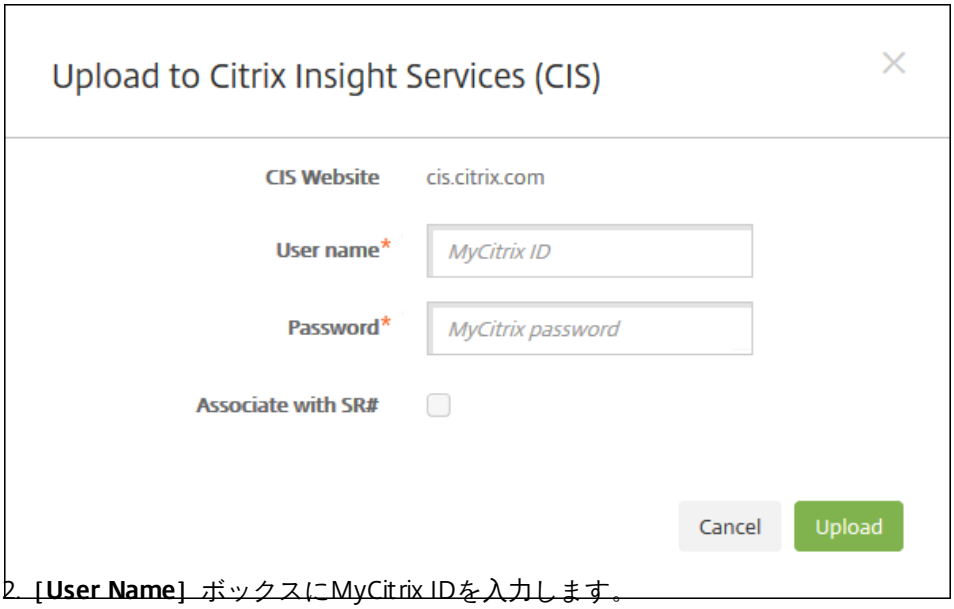
8. 手順7を繰り返し、ほかのNetScaler Gatewayサポートバンドルを追加します。

9. **[作成]** をクリックします。サポートバンドルが作成され、**[CISへアップロード]** と **[クライアントへダウンロード]** の2つの新しいボタンが表示されます。

Citrix Insight Servicesへのサポートバンドルのアップロード

サポートバンドルを作成した後、Citrix Insight Services（CIS）にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。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. **[サポートバンドルの作成]** ページで、 **[CISへアップロード]** をクリックします。 **[Citrix Insight Services（CIS）へのアップロード]** ダイアログボックスが開きます。



2. [**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。

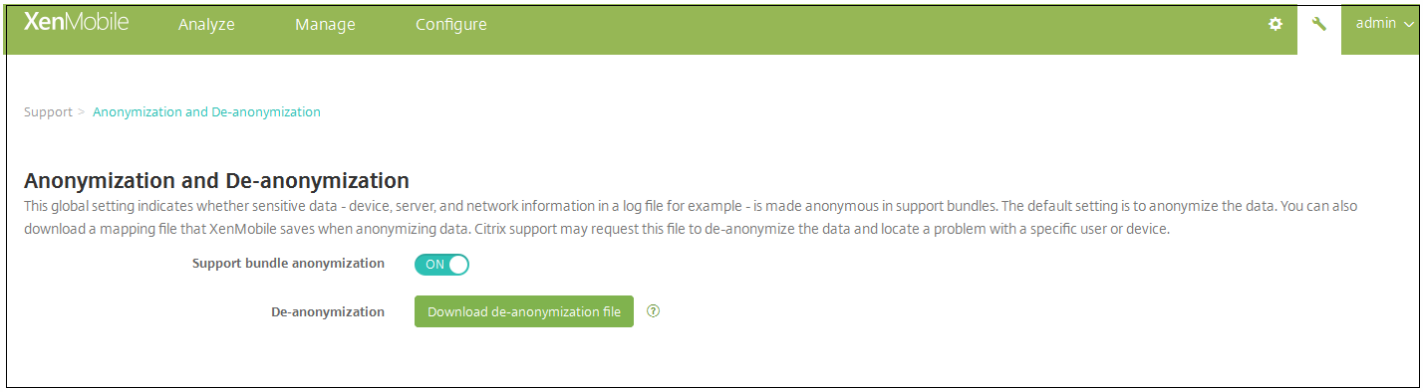
サポートバンドルのデータの匿名化

Feb 27, 2017

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

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。**［サポート］**ページが開きます。

2. **［サポート］**ページで、**［詳細］**の下の**［匿名化および匿名化解除］**をクリックします。**［匿名化および匿名化解除］**ページが開きます。



3. **［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。

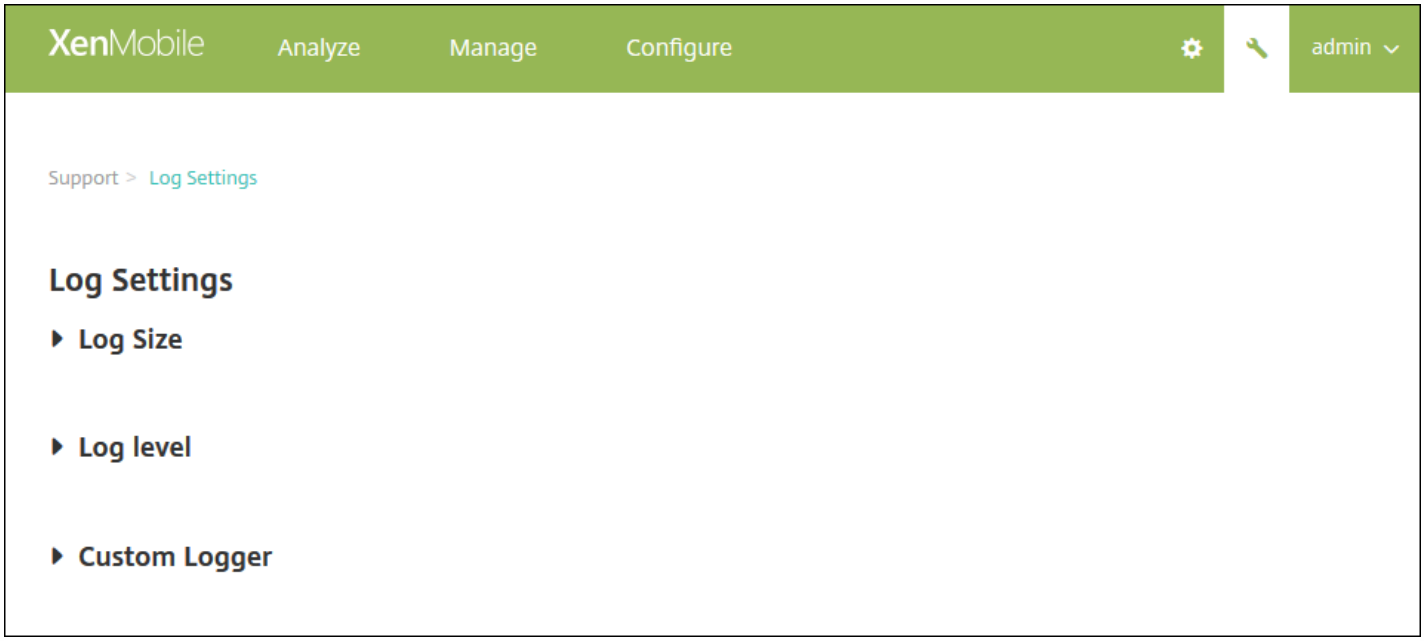
ログ

Feb 27, 2017

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。

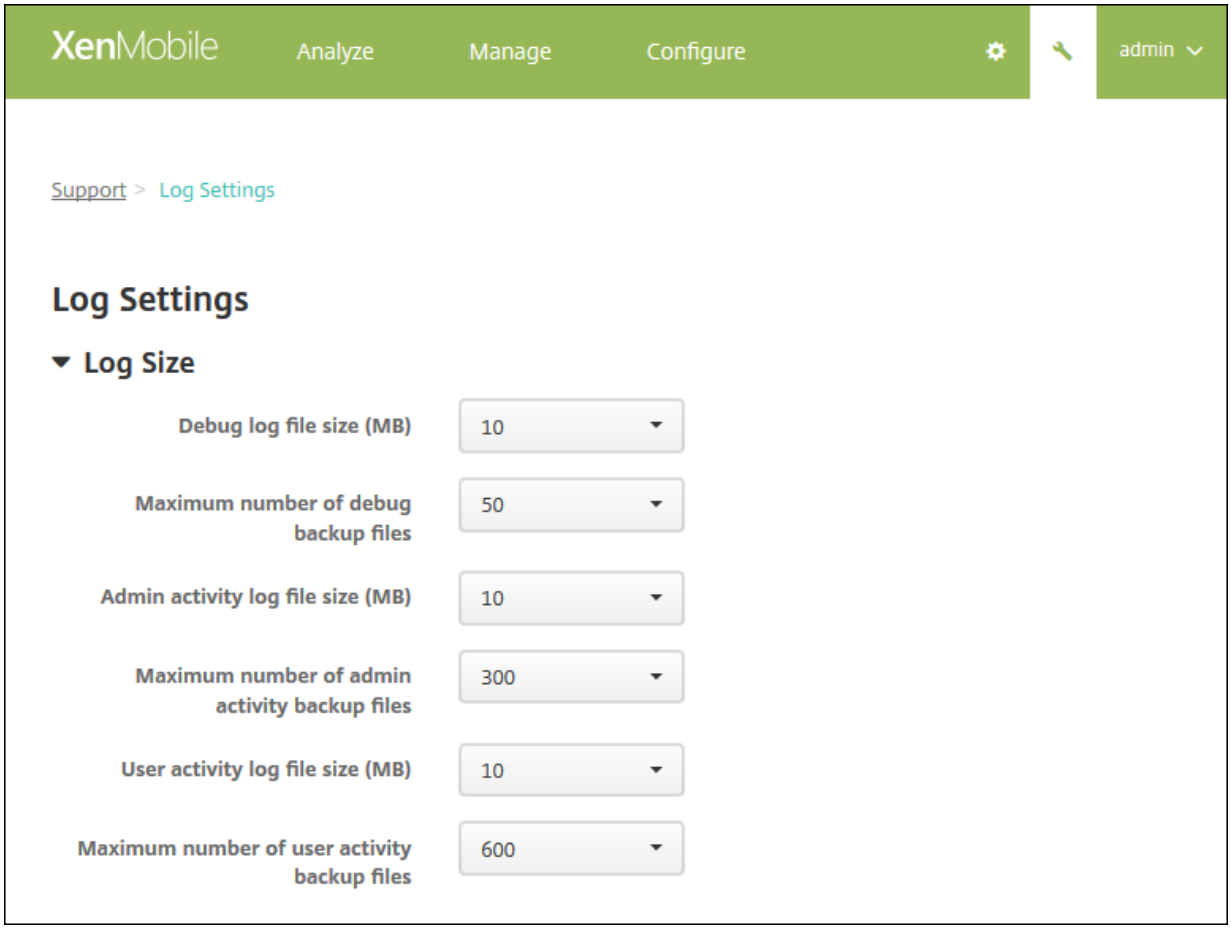


[Log Settings]ページでは、以下のオプションにアクセスできます。

- **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。



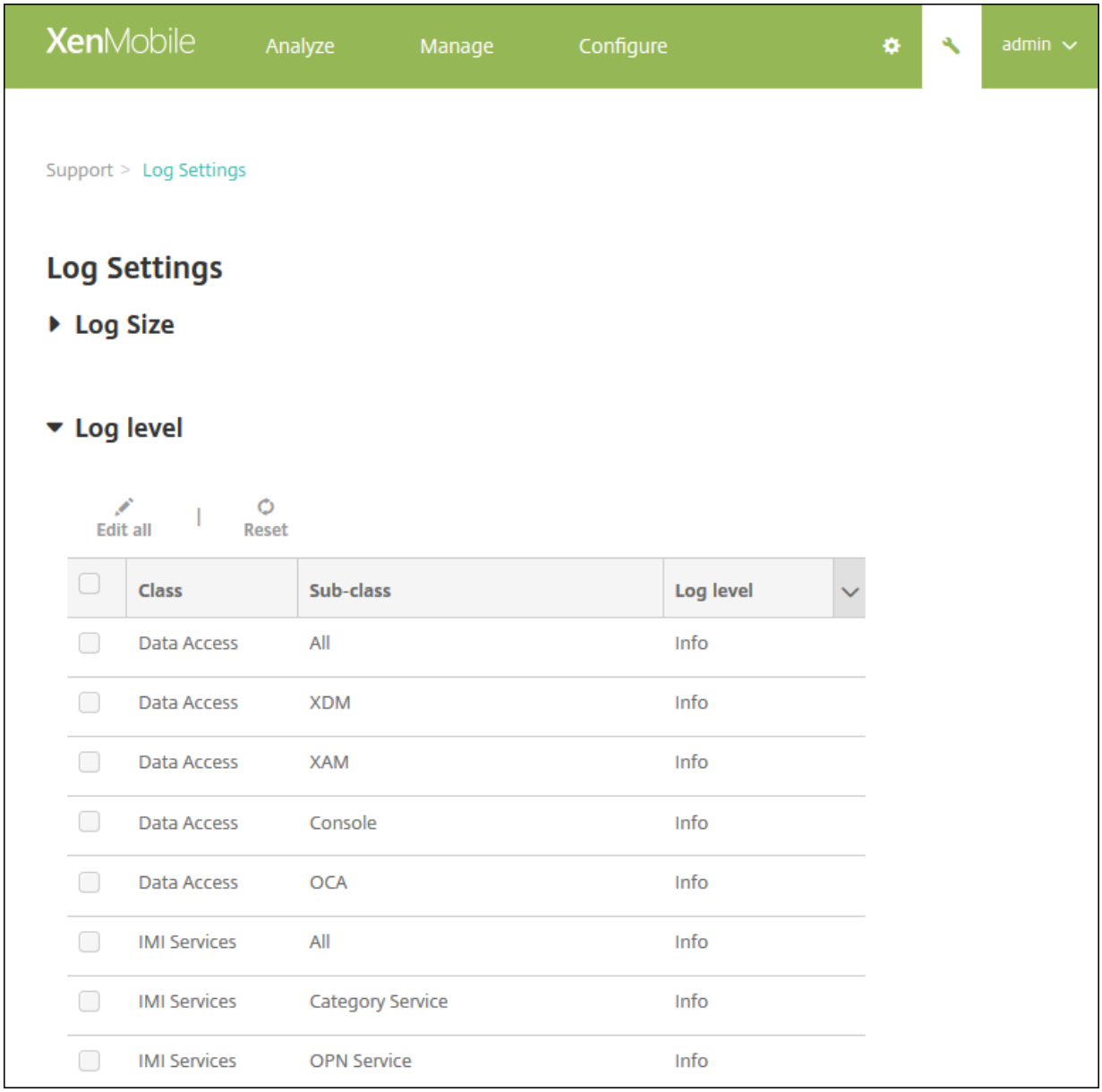
2. 次の設定を構成します。

- **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。

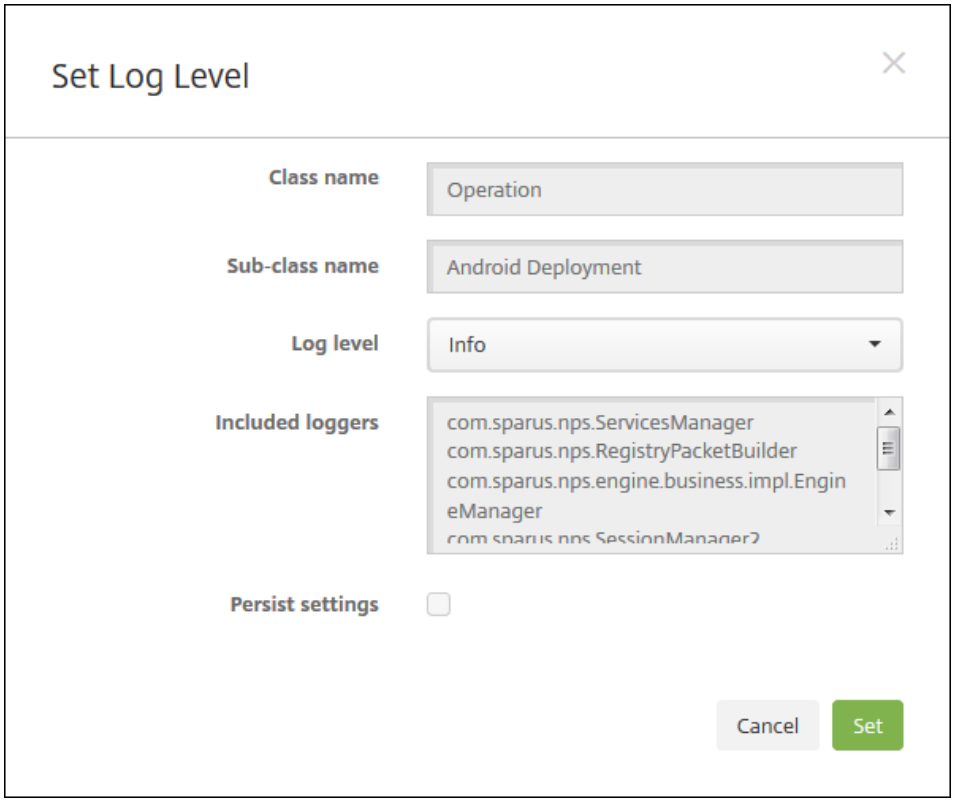
1. **［Log Settings］**ページで**［Log level］**を展開します。すべてのログクラスの表が表示されます。



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。

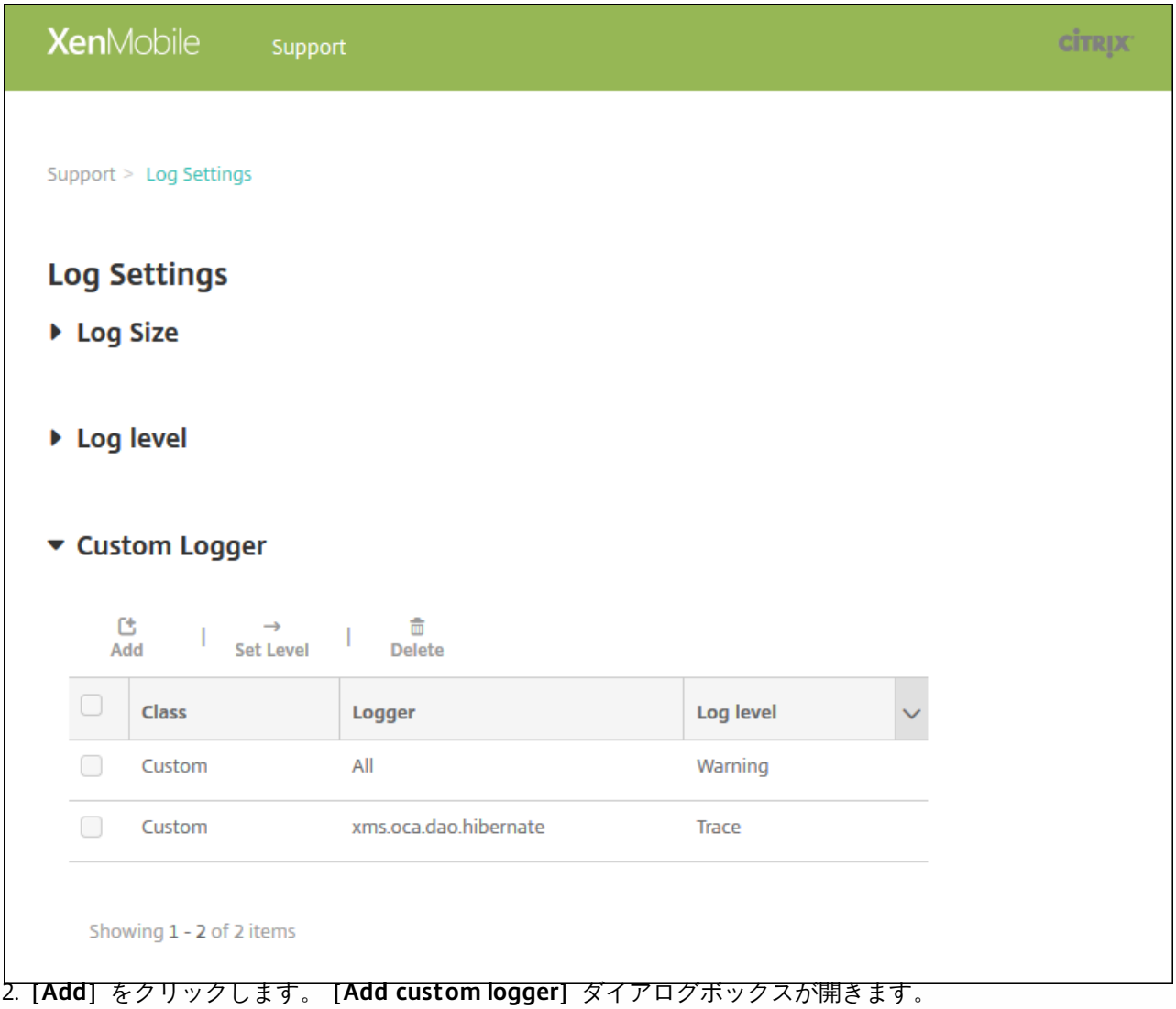


- **Class Name**：すべてのクラスのログレベルを変更する場合はこのフィールドに［All］と表示されます。そうでない場合は個別のクラス名が表示されます。編集できません。
- **Sub-class name**：すべてのクラスのログレベルを変更する場合はこのフィールドに［All］と表示されます。そうでない場合は個別のクラスのサブクラス名が表示されます。編集できません。
- **Log level**：一覧でログレベルをクリックします。サポートされるログレベルは以下のとおりです。
  - 重大
  - エラー
  - 警告
  - 詳細
  - デバッグ
  - トレース
  - 電源 - オフ
- **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。

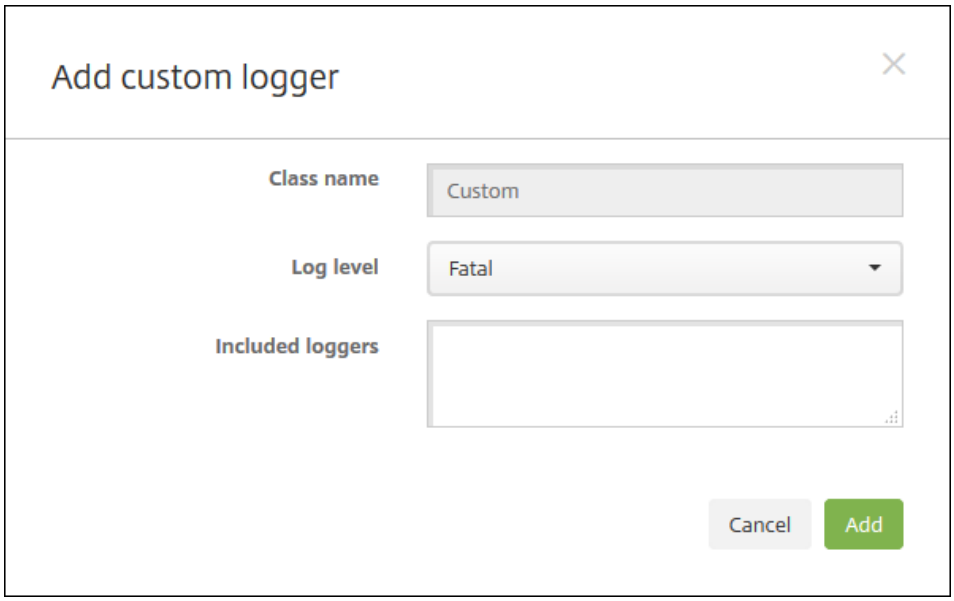
3. **[Set]** をクリックして変更を確定します。

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。



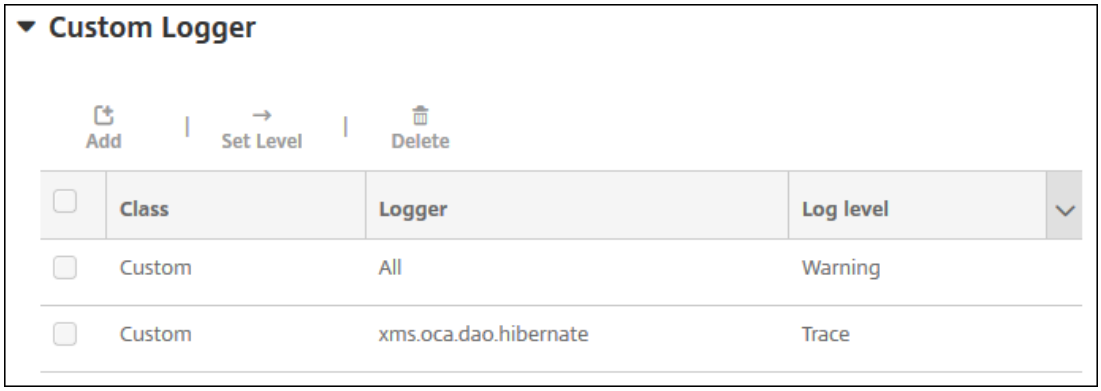
2. [**Add**] をクリックします。 [**Add custom logger**] ダイアログボックスが開きます。



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。
  - 重大
  - エラー
  - 警告
  - 詳細
  - デバッグ
  - トレース
  - 電源 - オフ
- **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。

3. ［**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 Analyzerツール

Apr 10, 2017

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。

XenMobile Serverをポイントするようにこのツールを構成するとともに、サーバーの展開の種類、モバイルプラットフォーム、認証の種類、ユーザーの資格情報などの情報の入力を行います。設定が完了するとツールはサーバーに接続し、構成の問題をチェックするために環境をスキャンします。XenMobile Analyzerで問題が検出されると、ツールにより問題を修正するための推奨事項が示されます。

ここでは次のことについて説明します。

- XenMobile Analyzerへのアクセスと起動
- 環境チェックの実行
- NetScalerチェックの実行
- 環境チェックのスケジュールの追加
- その他の有益なチェックの実行

主な機能

- 安全なクラウドベースのマイクロサービスによりXenMobile関連の問題すべてのトラブルシューティングを行うことができます。
- 正確な推奨事項によりXenMobileの構成に関する問題を解決できます。
- サポートへの問い合わせ件数を低減しXenMobile環境のトラブルシューティングを迅速化します。
- XenMobile Serverの各種リリースに対してゼロデイのサポートを行います。
- ヘルスチェックのスケジュールを毎日または週ごとで設定できます。
- NetScalerの構成をチェックします。
- イントラネットサイトへのSecure Webの到達可能性をテストします。
- Secure Mail Autodiscoveryサービスのチェックを行います。
- ShareFileへのシングルサインオン（SSO：Single Sign-on）をチェックします。

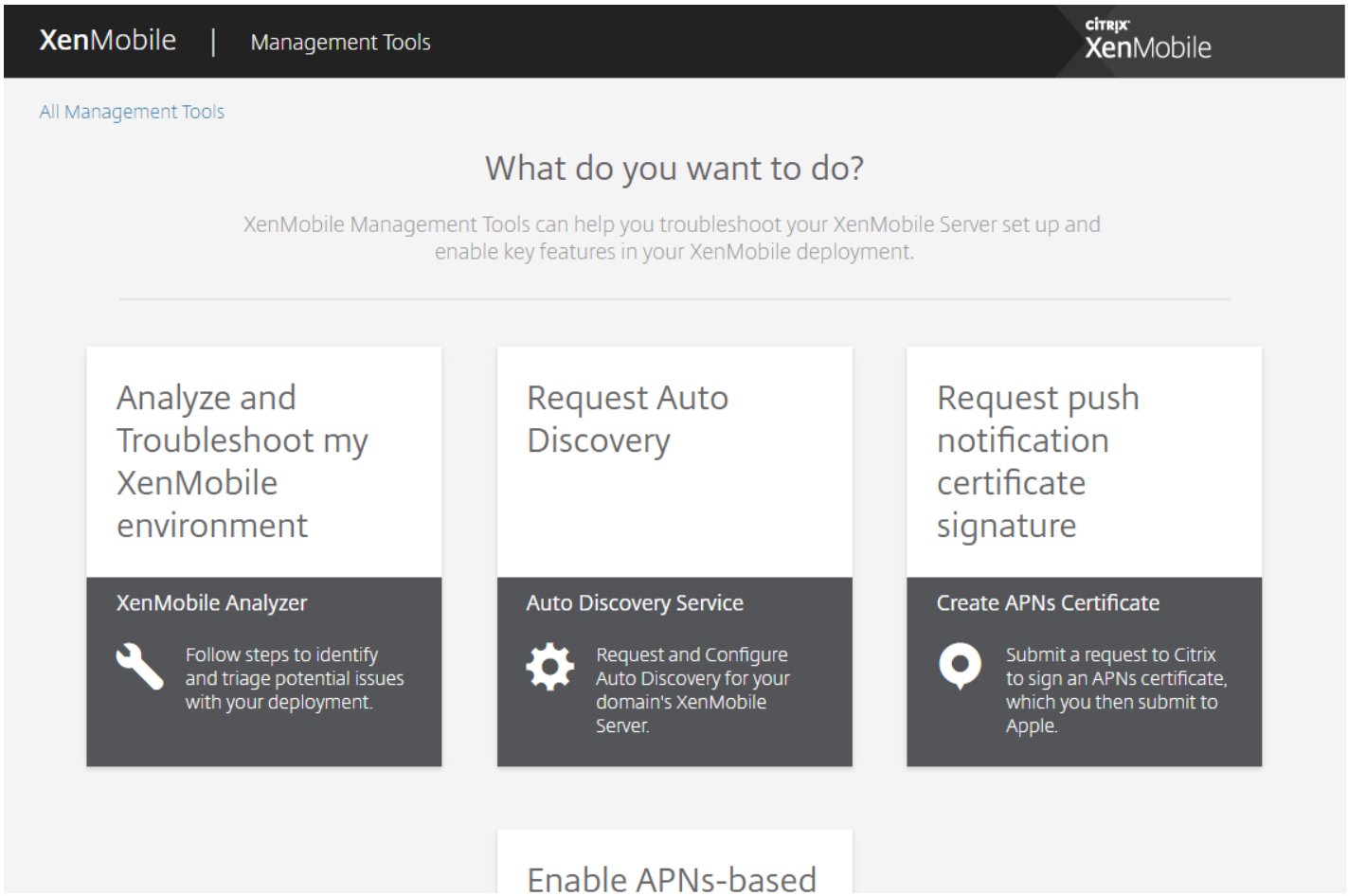
XenMobile Analyzerへのアクセスと起動

前提条件

製品	サポートされるバージョン
XenMobile Server	10.3.0以降
NetScaler Gateway	10.5以降
クライアント登録シミュレーション	iOSまたはAndroid

My Citrix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**

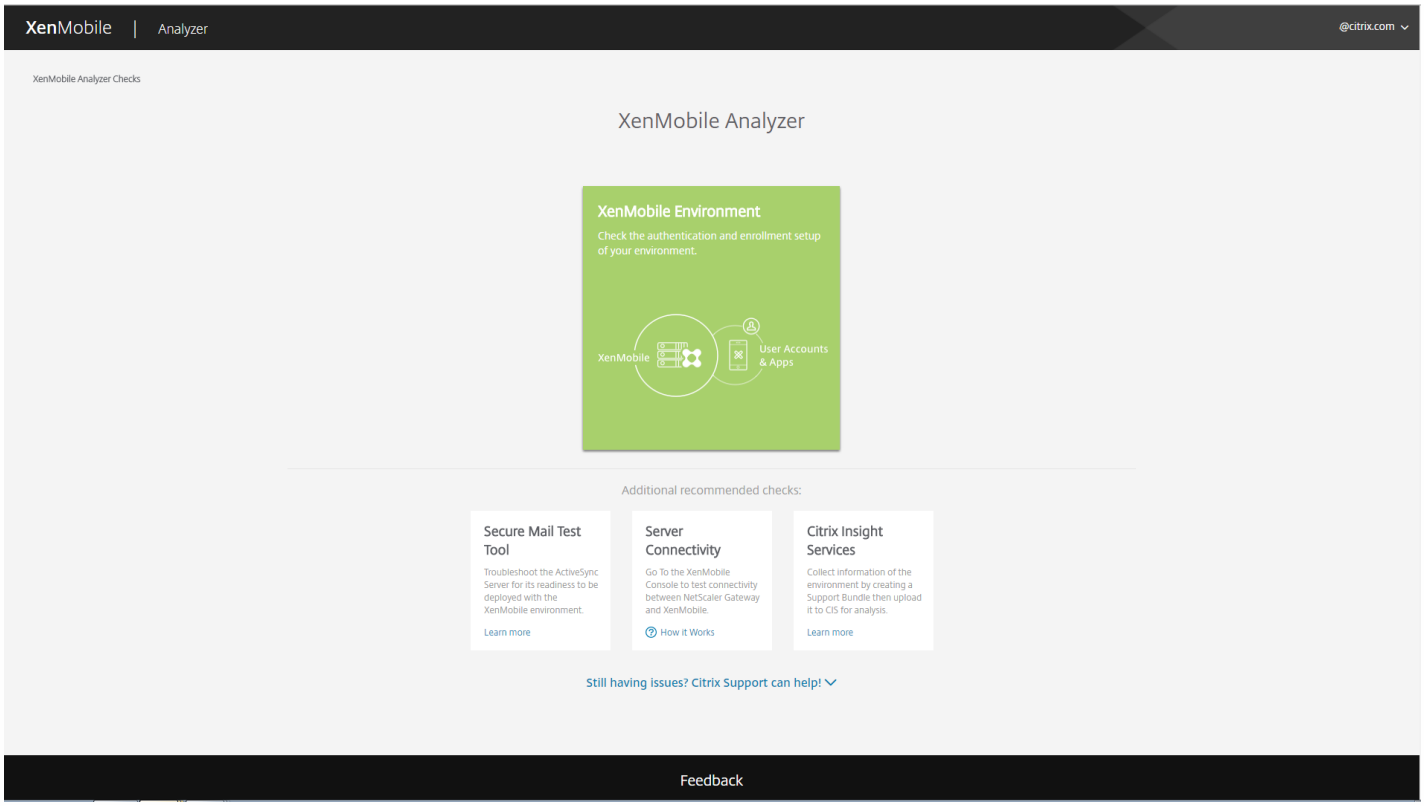
Environment] をクリックします。



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つのオプションがあります。これらのオプションにより、すべてのユーザーの負担を減らすことができます。

使用できるオプションは、次のとおりです。

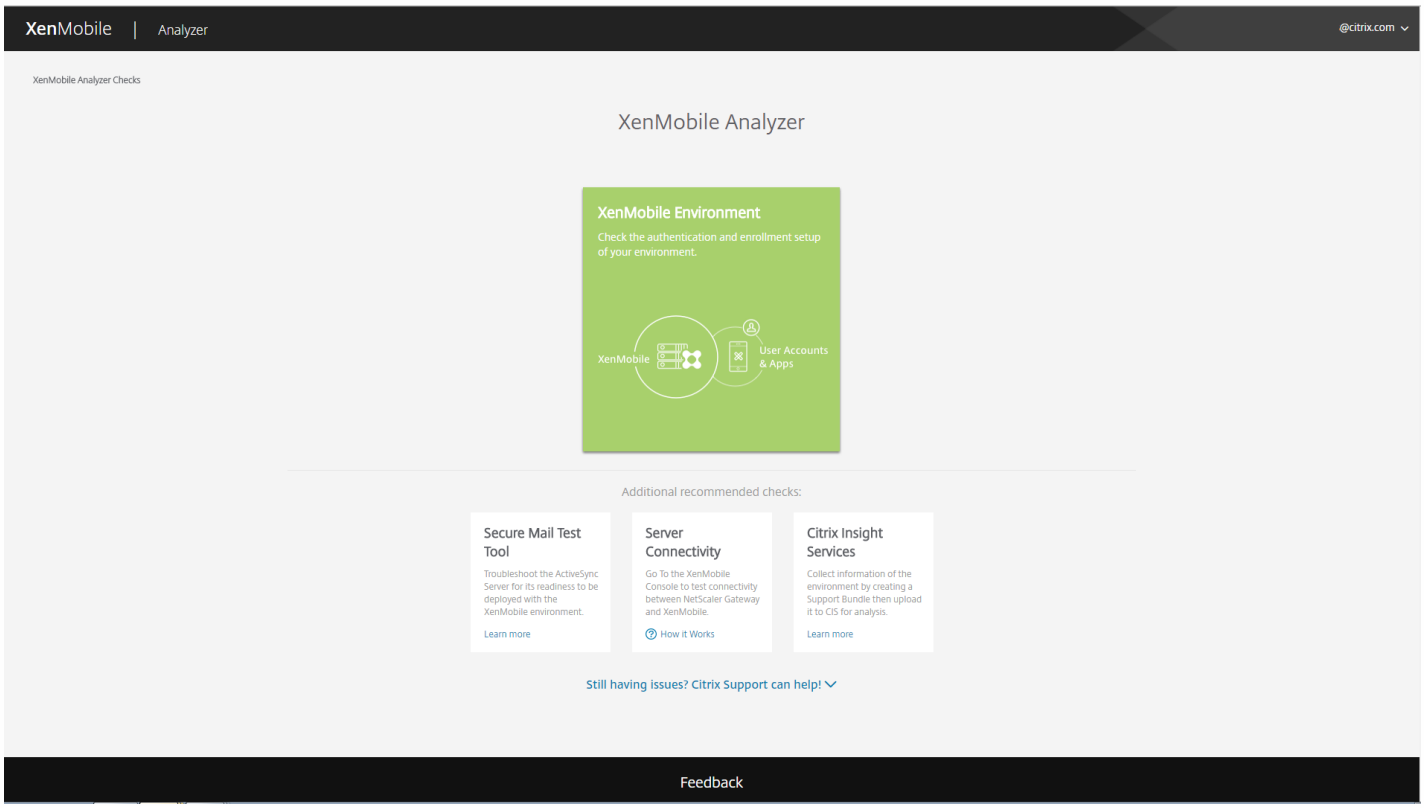
- **環境チェック** - この手順では、設定に問題がないかどうかをチェックするテストを設定します。また、デバイス、ユーザー登録、および認証に関する問題についての推奨事項も示されます。
- **NetScalerチェック** - この手順では、XenMobile展開向けのNetScalerの構成が準備できているかをチェックします。
- **詳細診断** - この手順では、環境チェックで見逃された可能性のある問題を見つけるための、Citrix Insight Servicesの使用に関する情報が提供されます。
- **Secure Mailの用意** - この手順では、XenMobile Exchange 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で、XenMobile環境へのActiveSyncサーバーの展開の準備に関するトラブルシューティングを行います。
- **サーバー接続チェック** - この手順では、サーバーの接続性をテストする方法が示されます。
- **Citrixサポートへの問い合わせ** - この手順では、依然として問題が発生する場合にCitrixサポートケースを登録するためのサイトのリンクが表示されます。



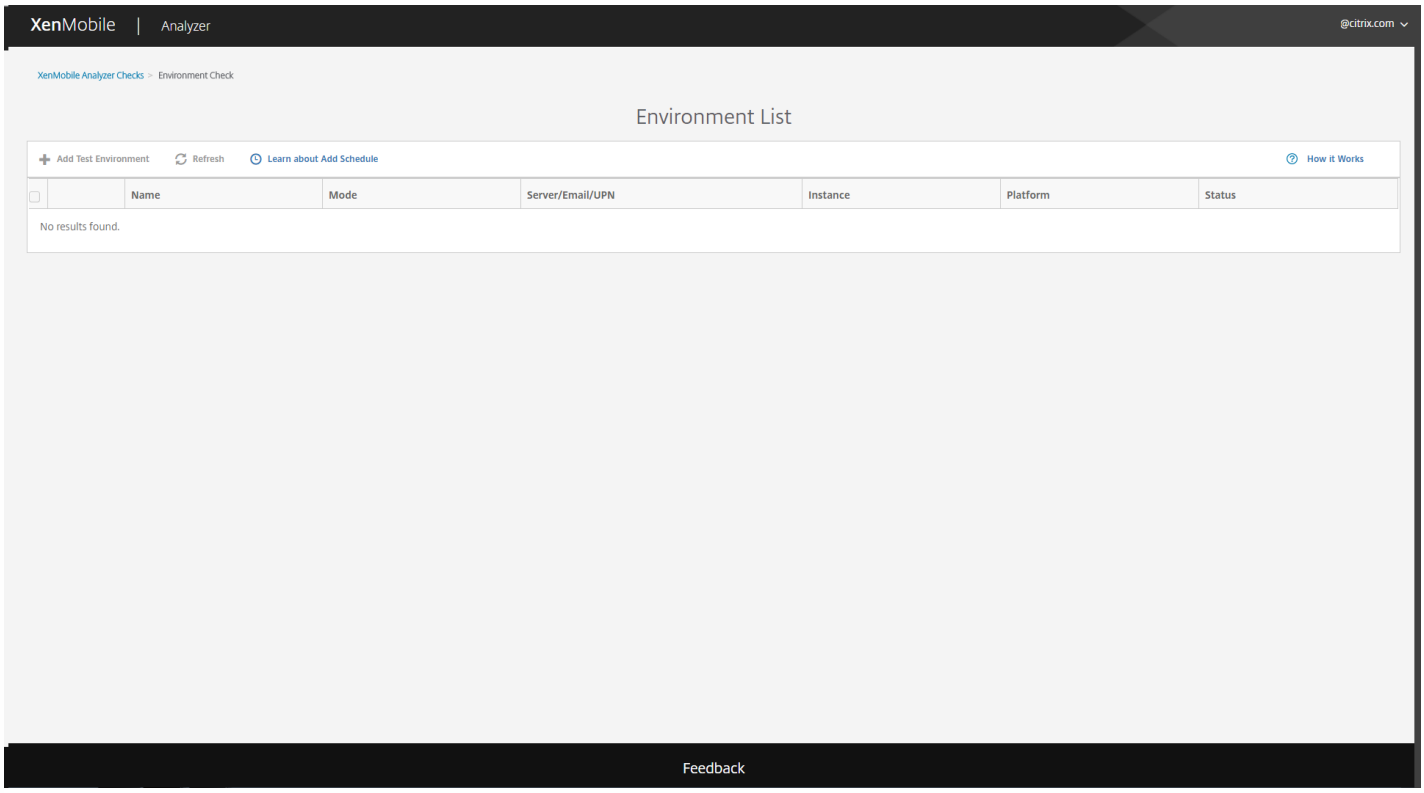
以下のセクションで、これらのオプションについてより詳しく説明します。

環境チェックの実行

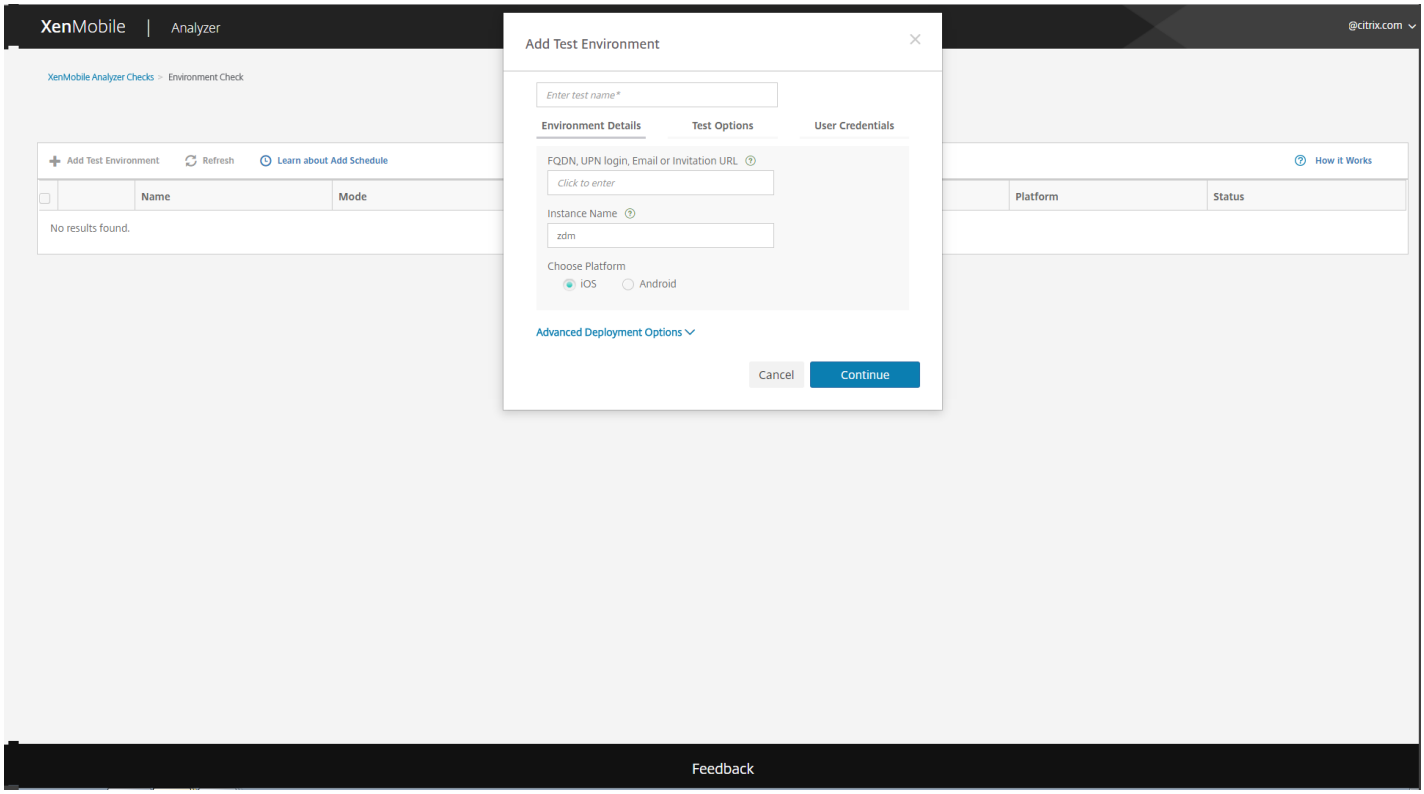
1. XenMobile Analyzerにログオンし、**[Environment Checks]** をクリックします。



2. [**Add Test Environment**] をクリックします。



3. 新しい [**Add Test Environment**] ダイアログボックスで、以下の操作を行います。



a. 今後テストを特定できるように、テストの一意の名前を入力します。

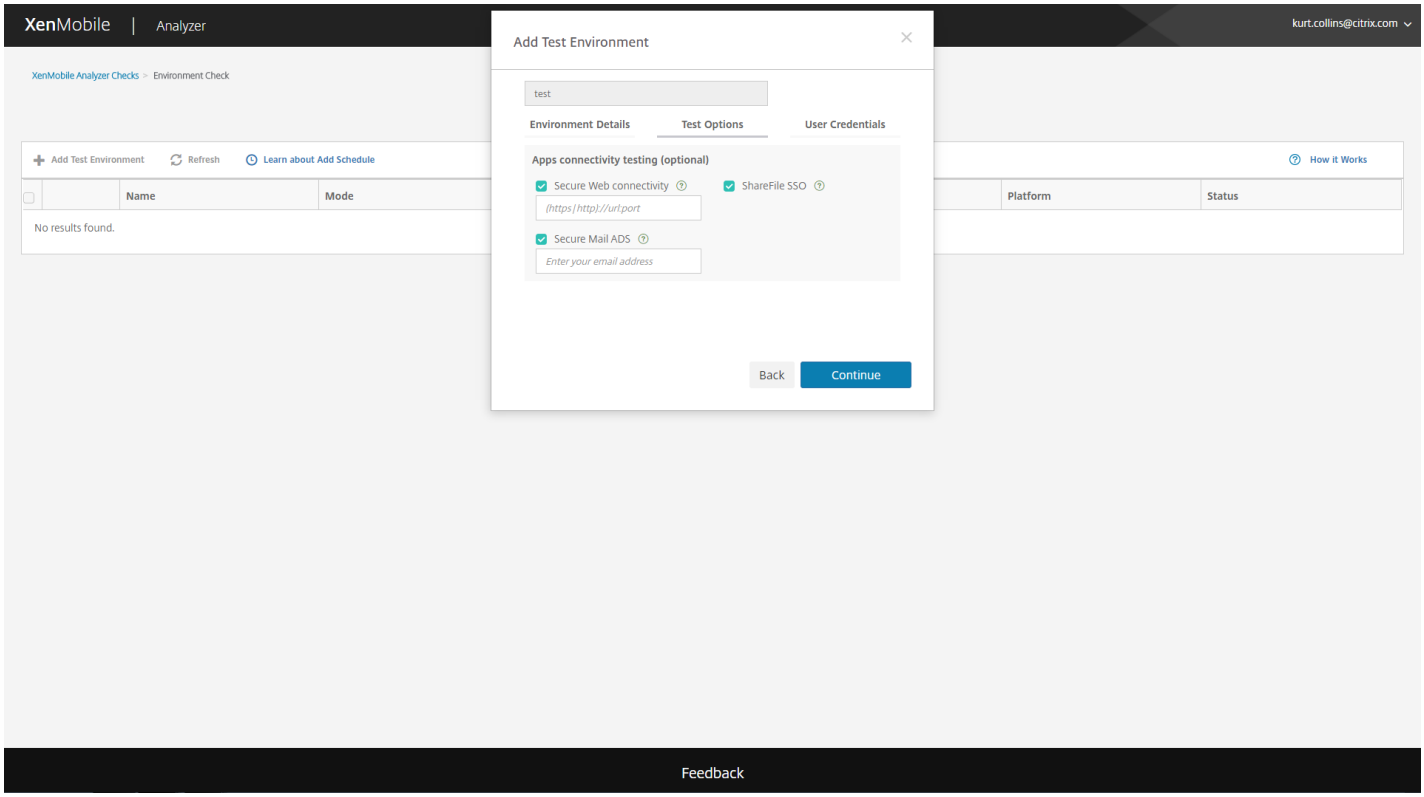
b. ［**FQDN, UPN login, Email or URLInvitation**］フィールドで、サーバーへのアクセスに使用する情報を入力します。

c. カスタムインスタンスを使用している場合は、［**Instance Name**］にその値を入力します。

d. ［**Choose Platform**］で、テスト用のプラットフォームとして**iOS**または**Android**を選択します。

e. ［**Advanced Deployment Options**］を展開すると、［**Deployment Mode**］ボックスの一覧で、使用するXenMobile展開モードを選択できます。使用できるオプションは［**Enterprise（MDM + MAM）**］、［**App Management（MAM）**］、［**Device Managment（MDM）**］です。

4. ［**Continue**］をクリックします。



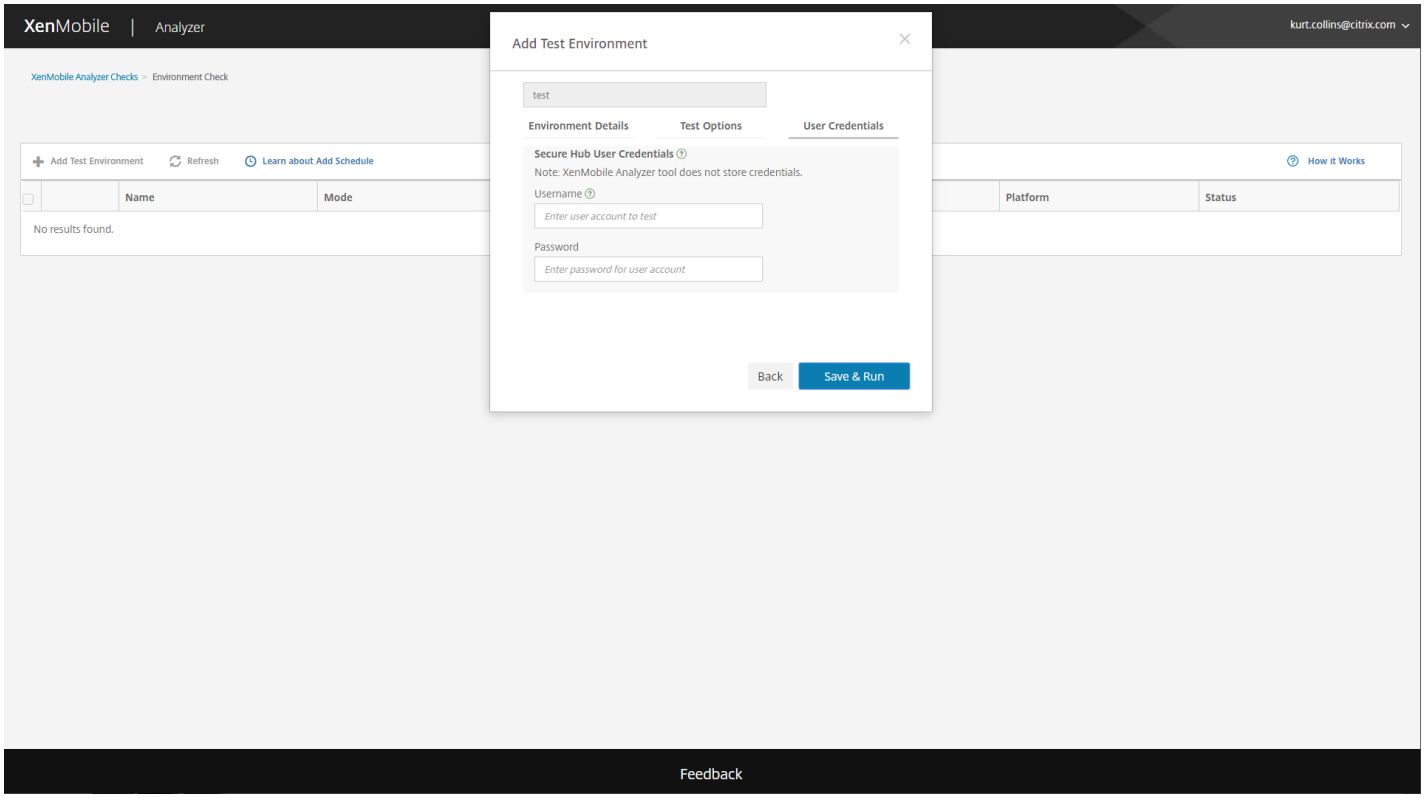
5. 実行するアプリケーションレベルのテストを選択します。次のテストの1つ以上を選択できます。

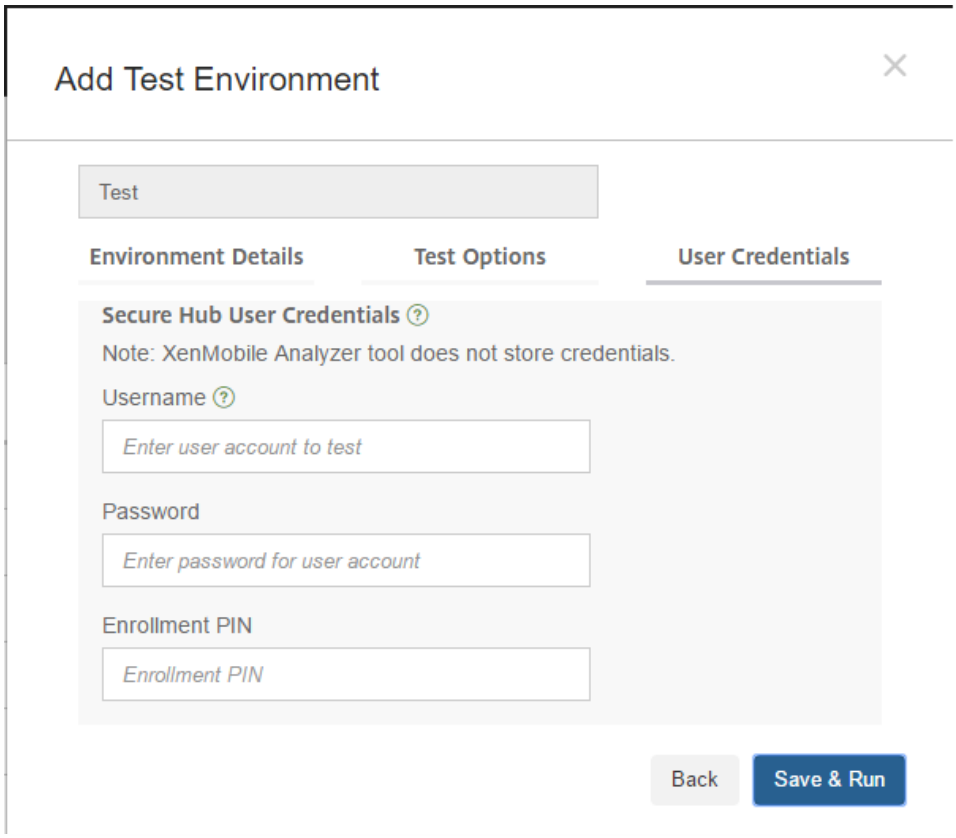
a.**Secure Webの接続**。イントラネットのURLを指定します。ツールにより、入力したURLへの到達可能性がテストされます。このテストでは、イントラネットのURLへの接続時にSecure Webアプリで生じる可能性のある、接続に関する問題が検出されます。

b. **Secure Mail ADS**。ユーザーの電子メールIDを指定します。このIDを使用して、XenMobile環境にあるMicrosoft Exchange Serverの自動検出機能がテストされます。Secure Mail Auto Discovery関連の問題があるかどうかが検出されます。

c.**ShareFile SSO**：この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。

6. [**Continue**] をクリックします。





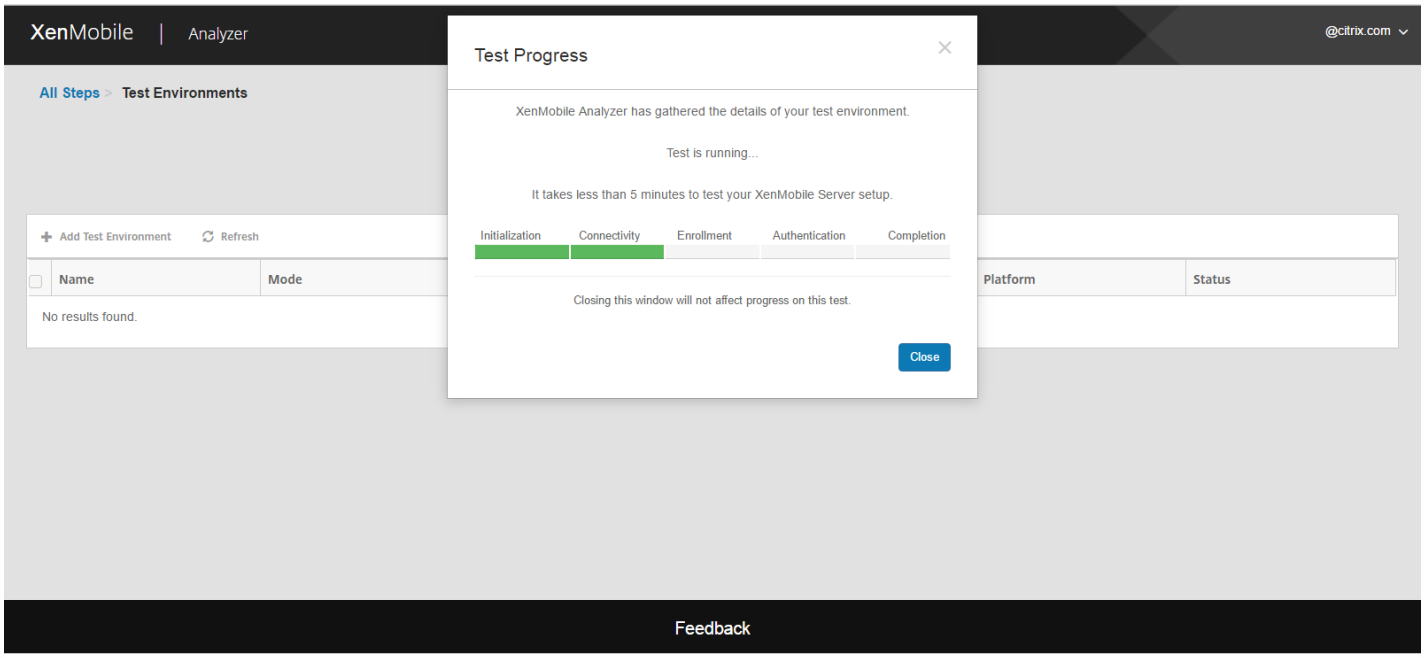
7. サーバーのセットアップによっては［User Credentials］の入力フィールドが異なる表示になることがあります。この

フィールドには、［**Username**］のみ、［**Username**］と［**Password**］、または［**Username**］、［**Password**］、および［**Enrollment PIN**］があります。

8. この情報を入力後、［**Save & Run**］をクリックしてテストを開始します。

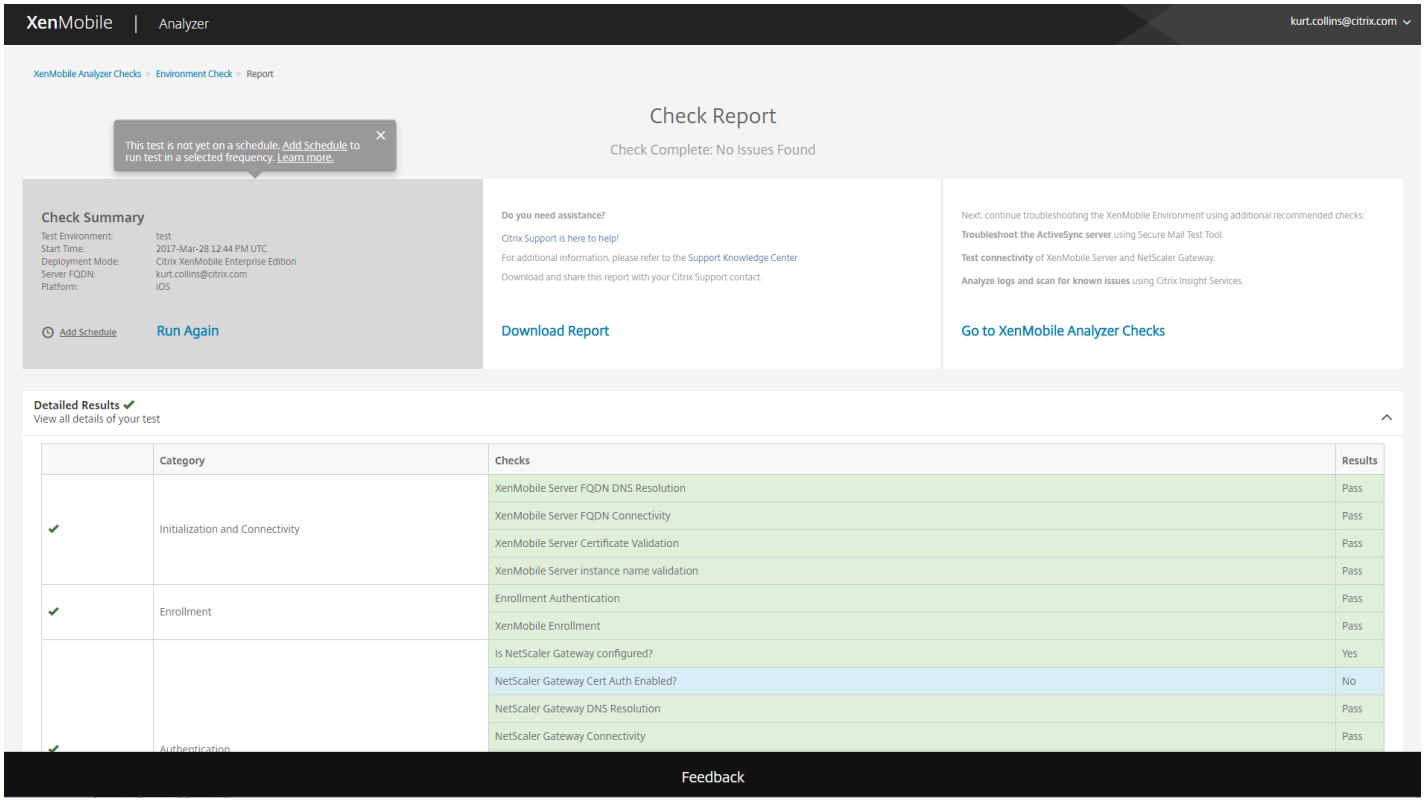
進行状況が表示されます。この進行状況を示すダイアログボックスは開いたままにしても、閉じても構いません。どちらの場合でもテストは続行されます。

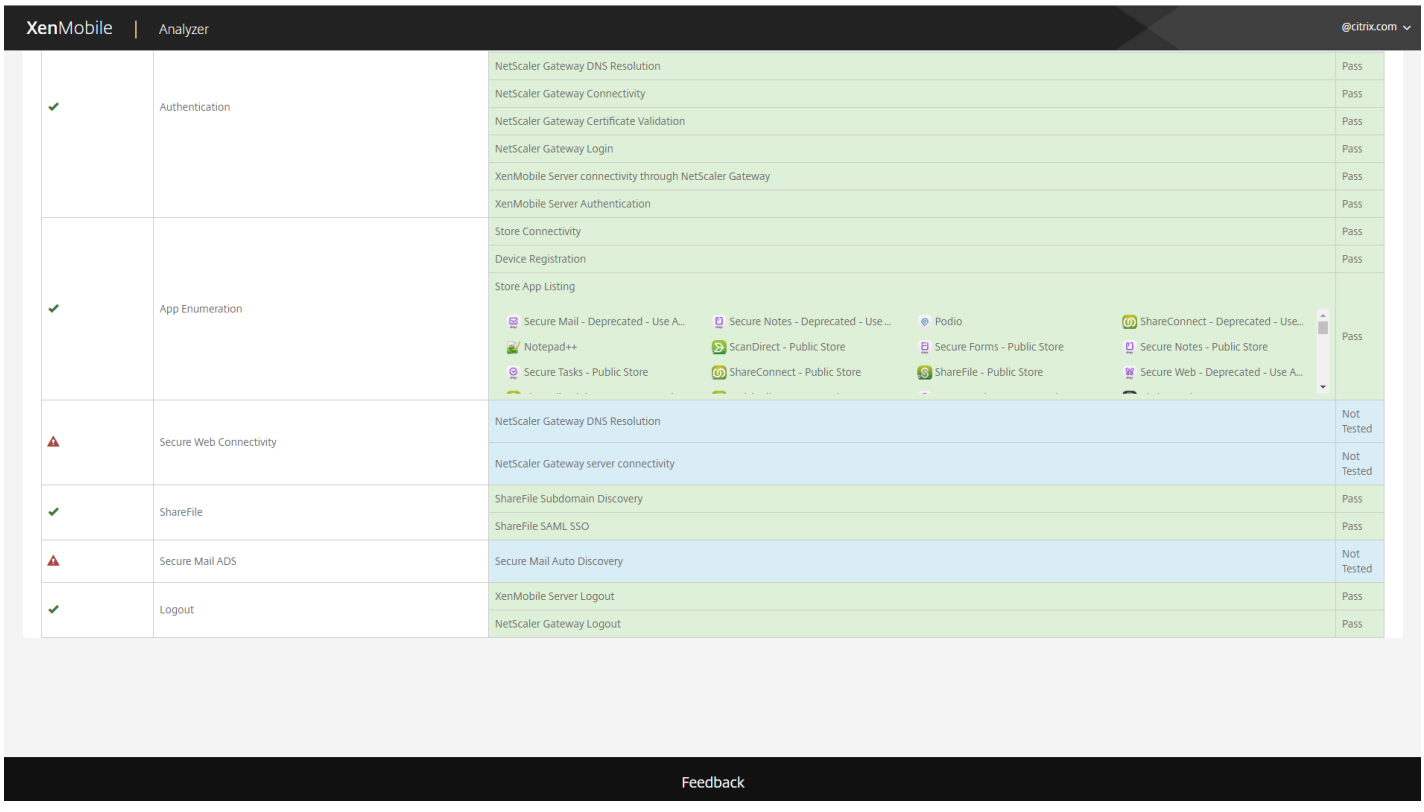
問題なく完了したテストは緑色で表示されます。失敗したテストは赤色で表示されます。



8. 進行状況を示すダイアログボックスを閉じた後、［**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。

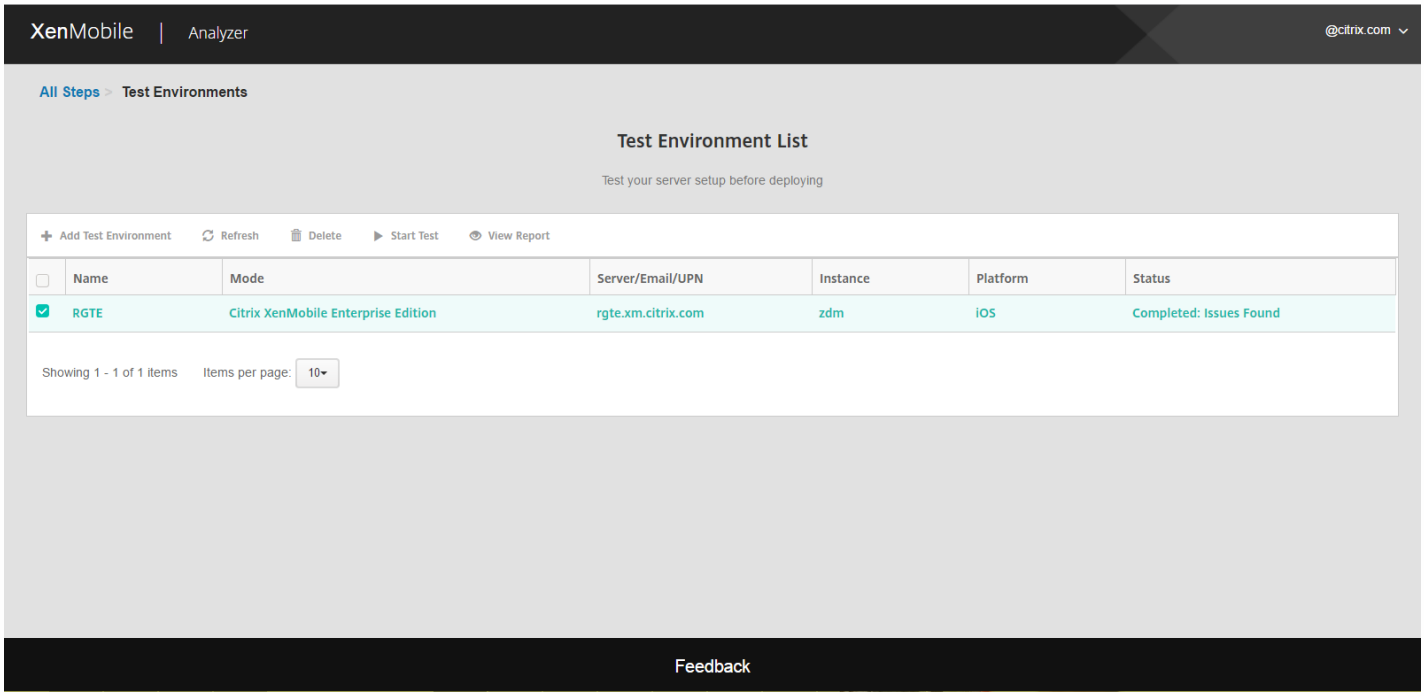
a. レポートをダウンロードするには、［**Download Report**］をクリックします。

b. テスト環境の一覧に戻るには、［**Environment Check**］をクリックします。

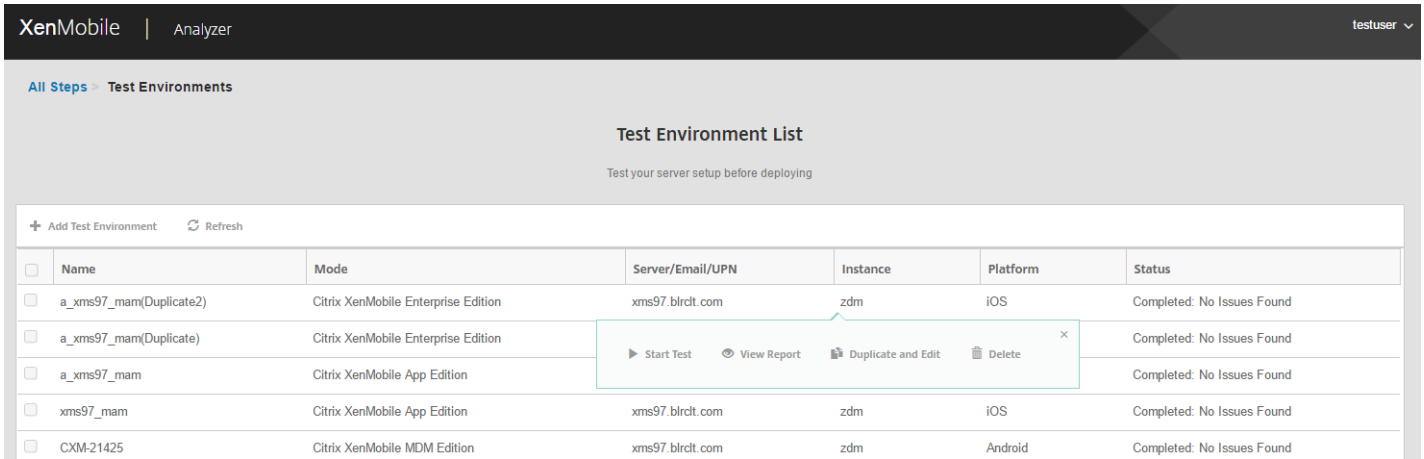
c. 同じテストをもう一度実行するには、［**Run Again**］をクリックします。

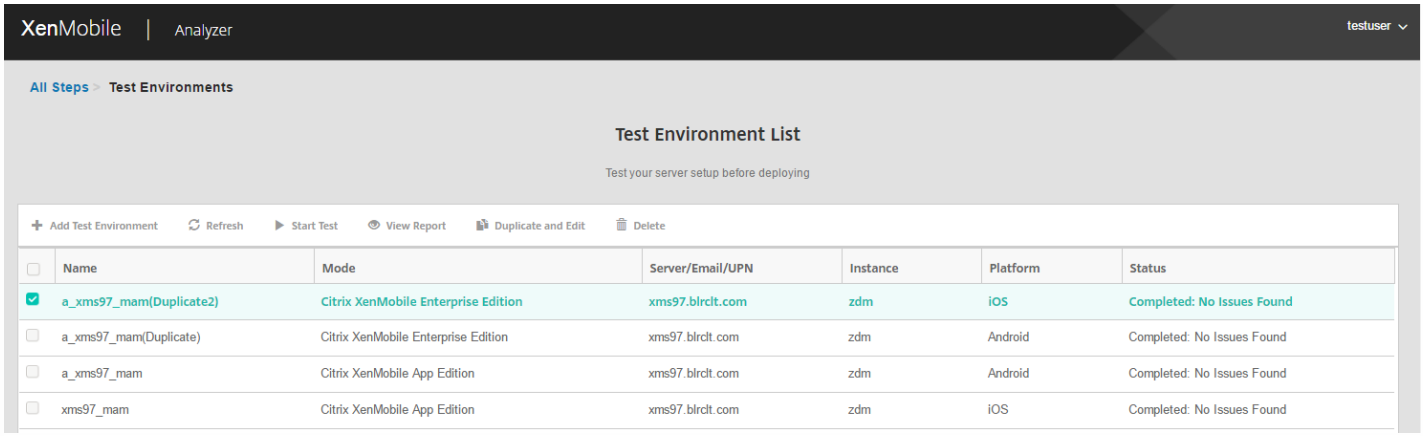
d. 別のテストをもう一度実行するには、［**Test Environments**］に戻って再実行するテストを選択し、［**Start Test**］をクリックします。

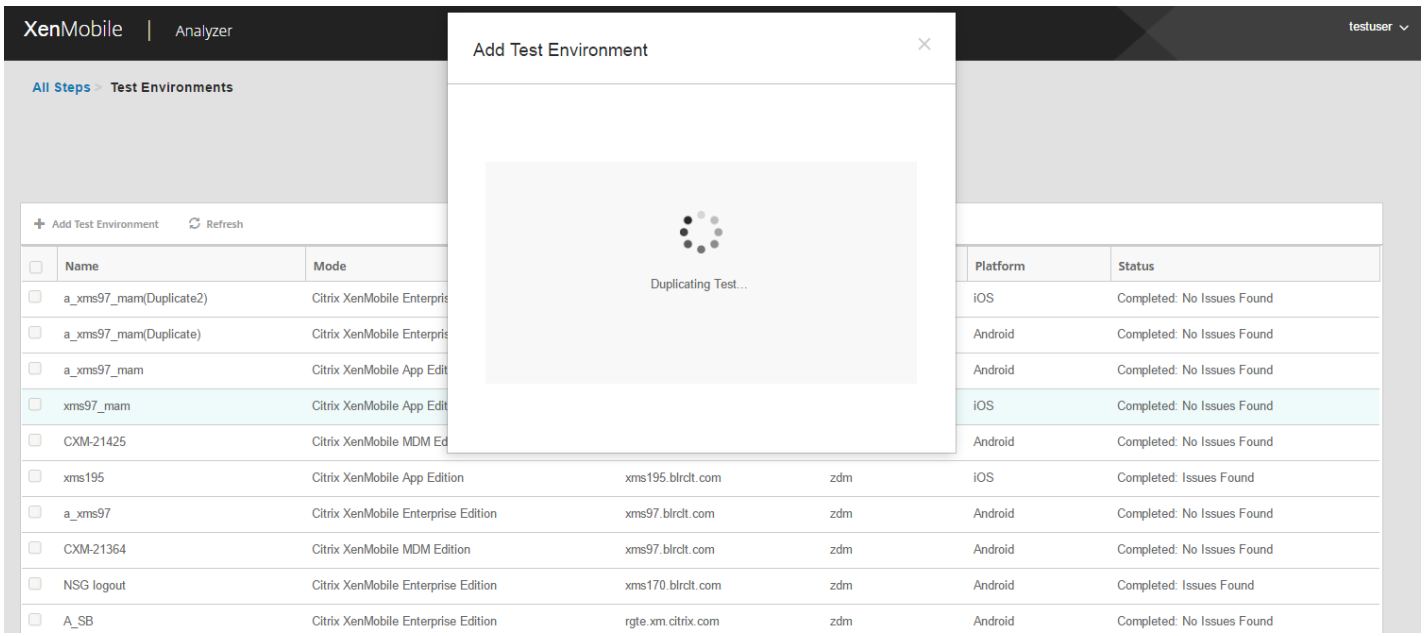
e. XenMobile Analyzerの別のオプションを選択するには、［**Go To XenMobile Analyzer Checks**］をクリックします。

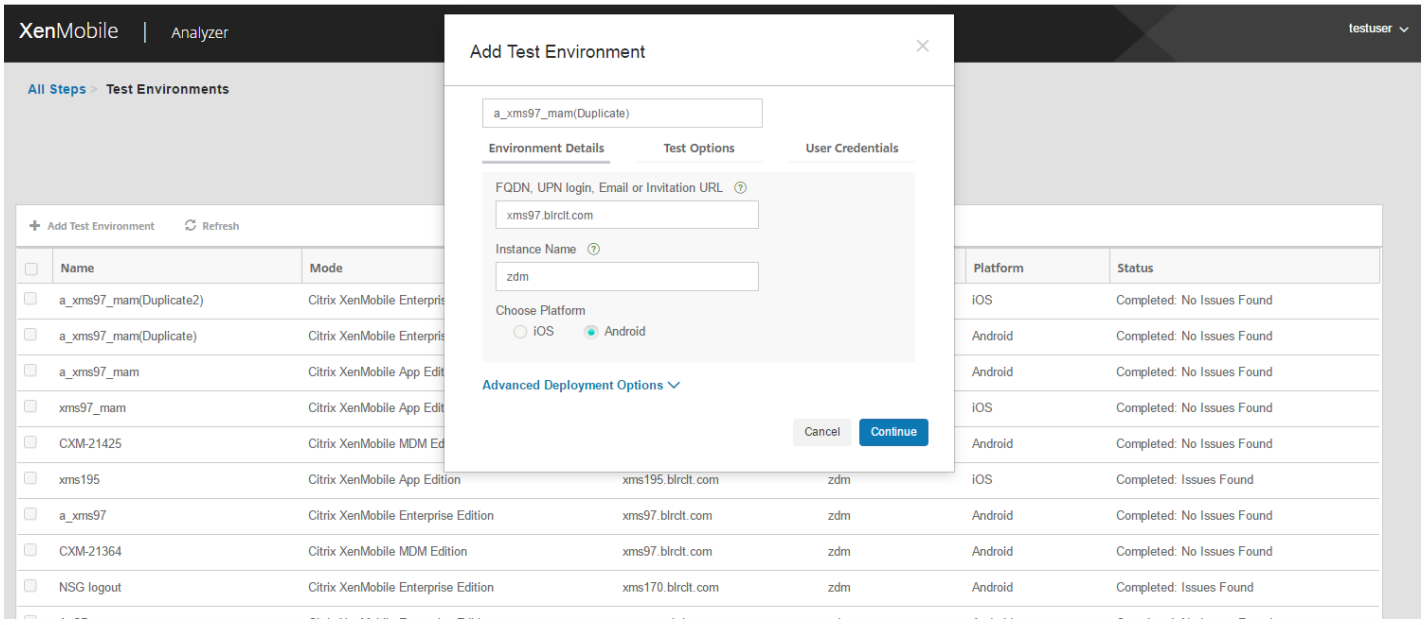


10. ［Test Environments］ページで、テストをコピーし、編集できます。このためには、テストを選択し、**［Duplicate and Edit］**をクリックします。選択したテストのコピーが作成され、［Add Test Environment］ダイアログが開いて新しいテストを変更できるようになります。





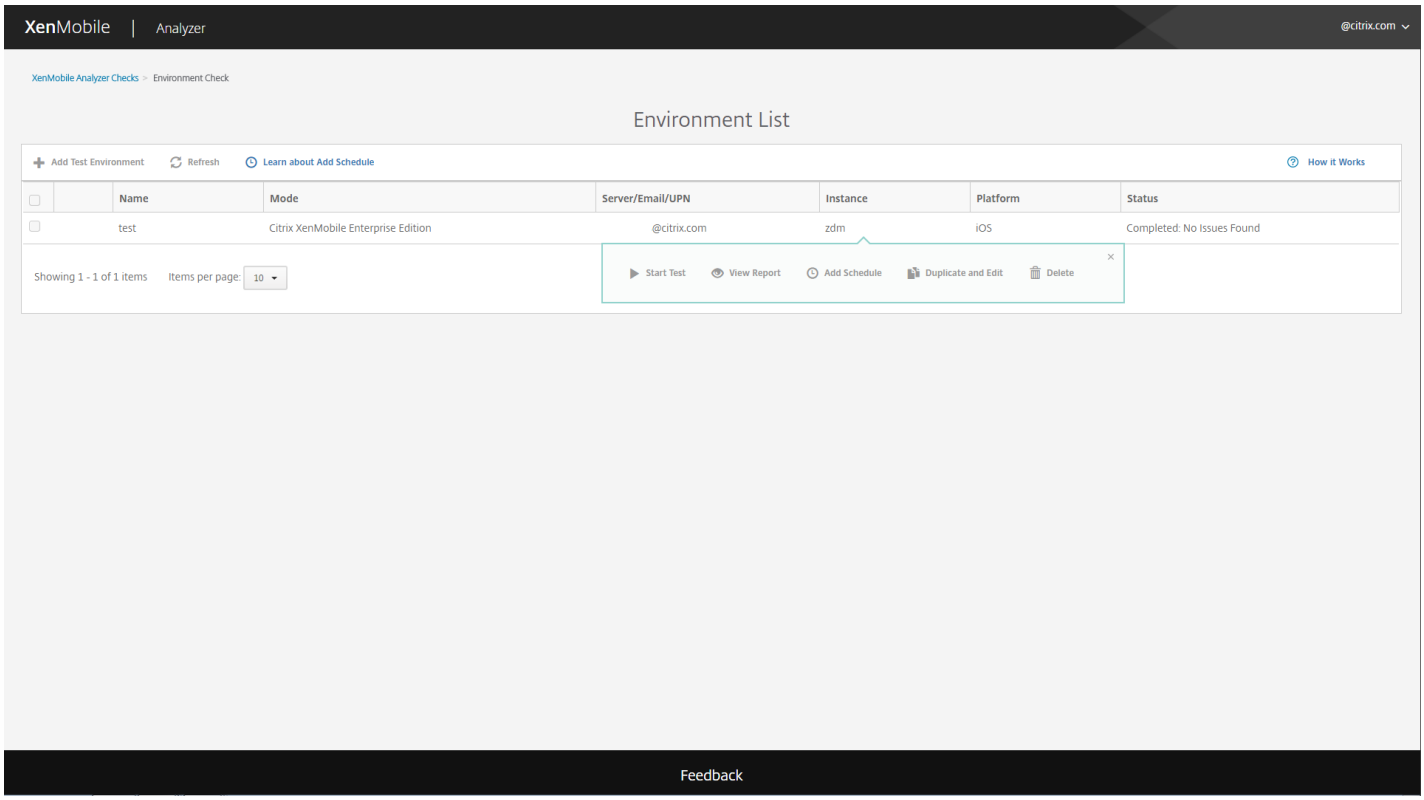




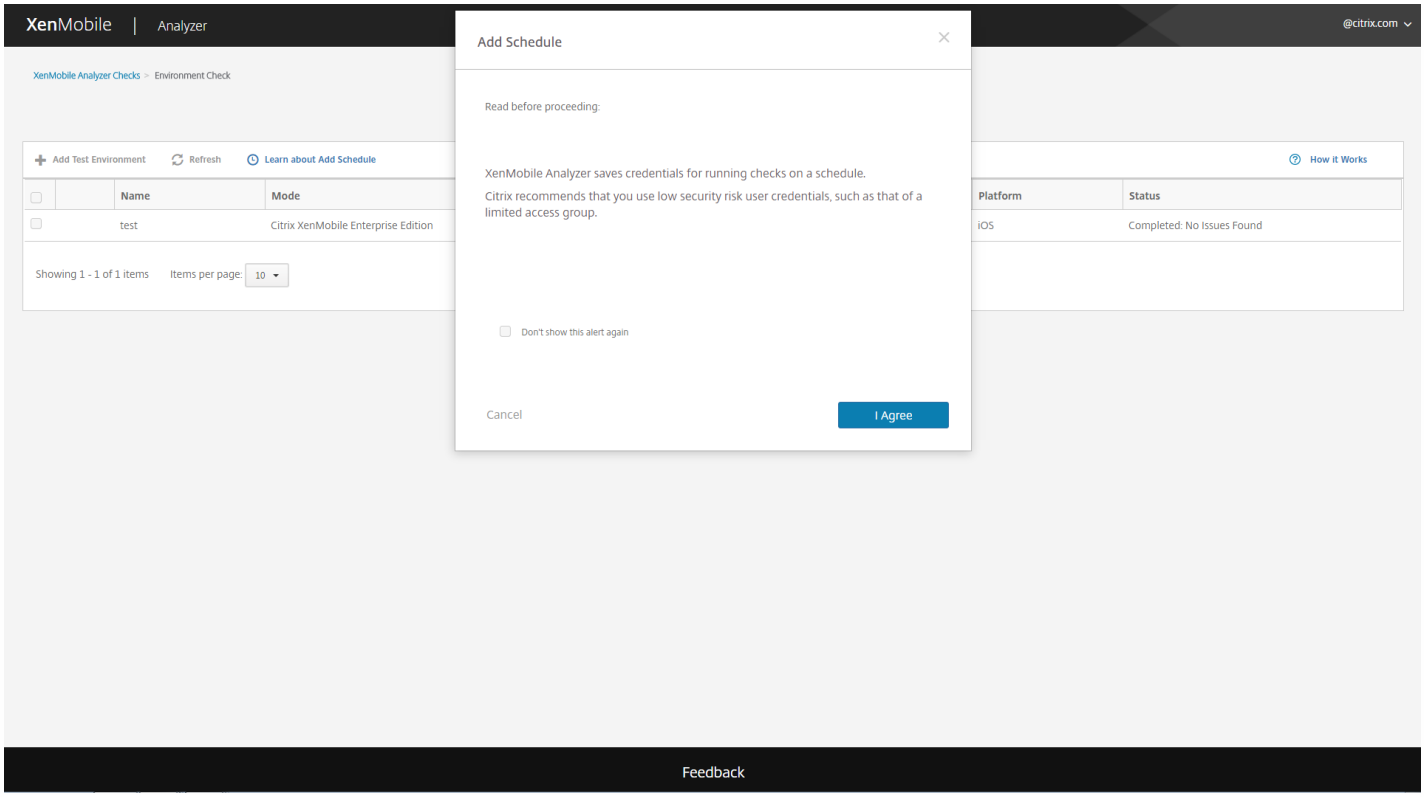
環境チェックのスケジュールの追加

テストは、スケジュールに基づいて自動で実行し、構成した一覧のユーザーに結果を送信するように構成できます。

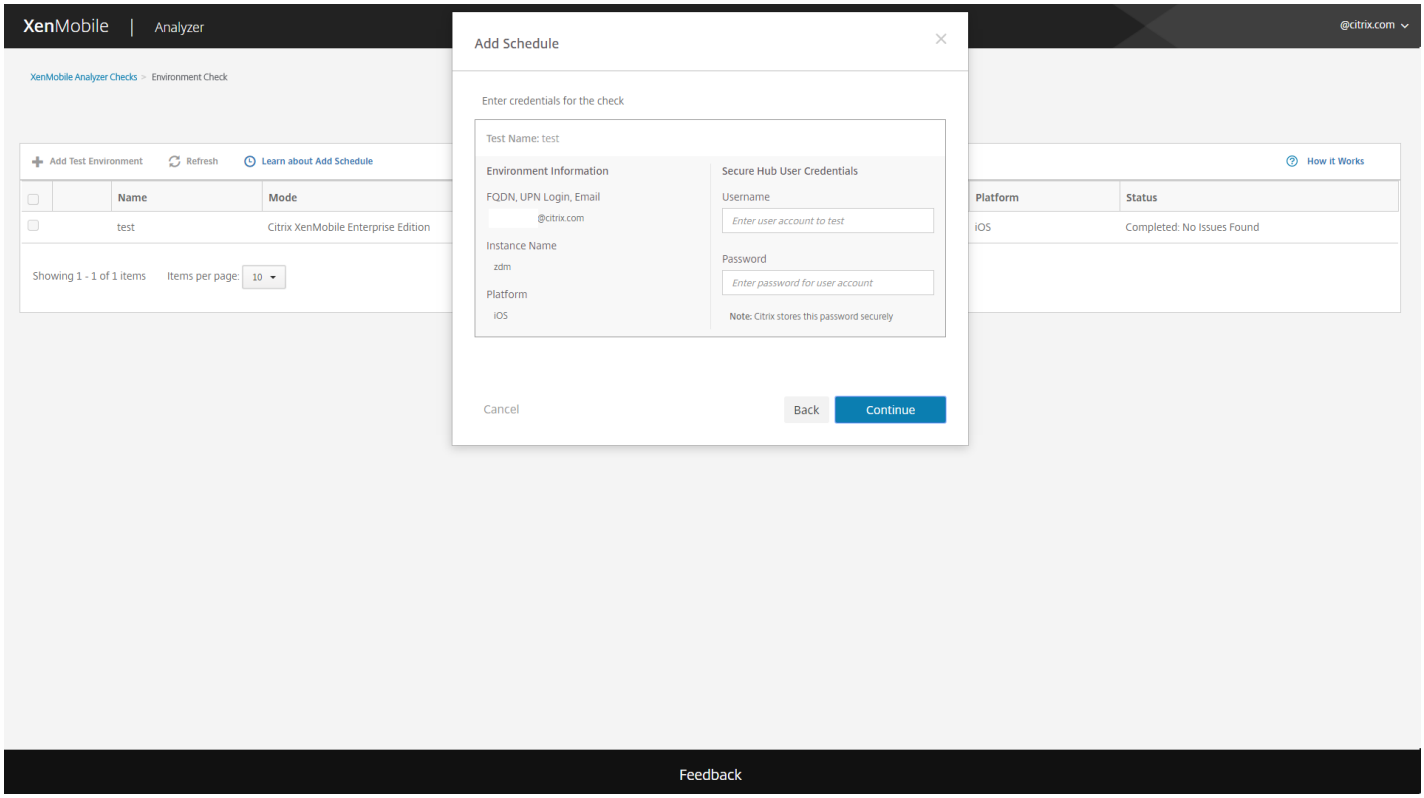
1. [**Environment List**] ページでスケジュールを設定する環境を選択し、 [**Add Schedule**] をクリックします。



2. [**Add Schedule**] ウィンドウに、スケジュールに基づいてテストを実行するためにXenMobile Analyzerに資格情報が保存されることを警告するメッセージが表示されます。スケジュールによるテストの実行には、アクセスが制限されたアカウントを使用することをお勧めします。 [**I Agree**] をクリックして続行します。

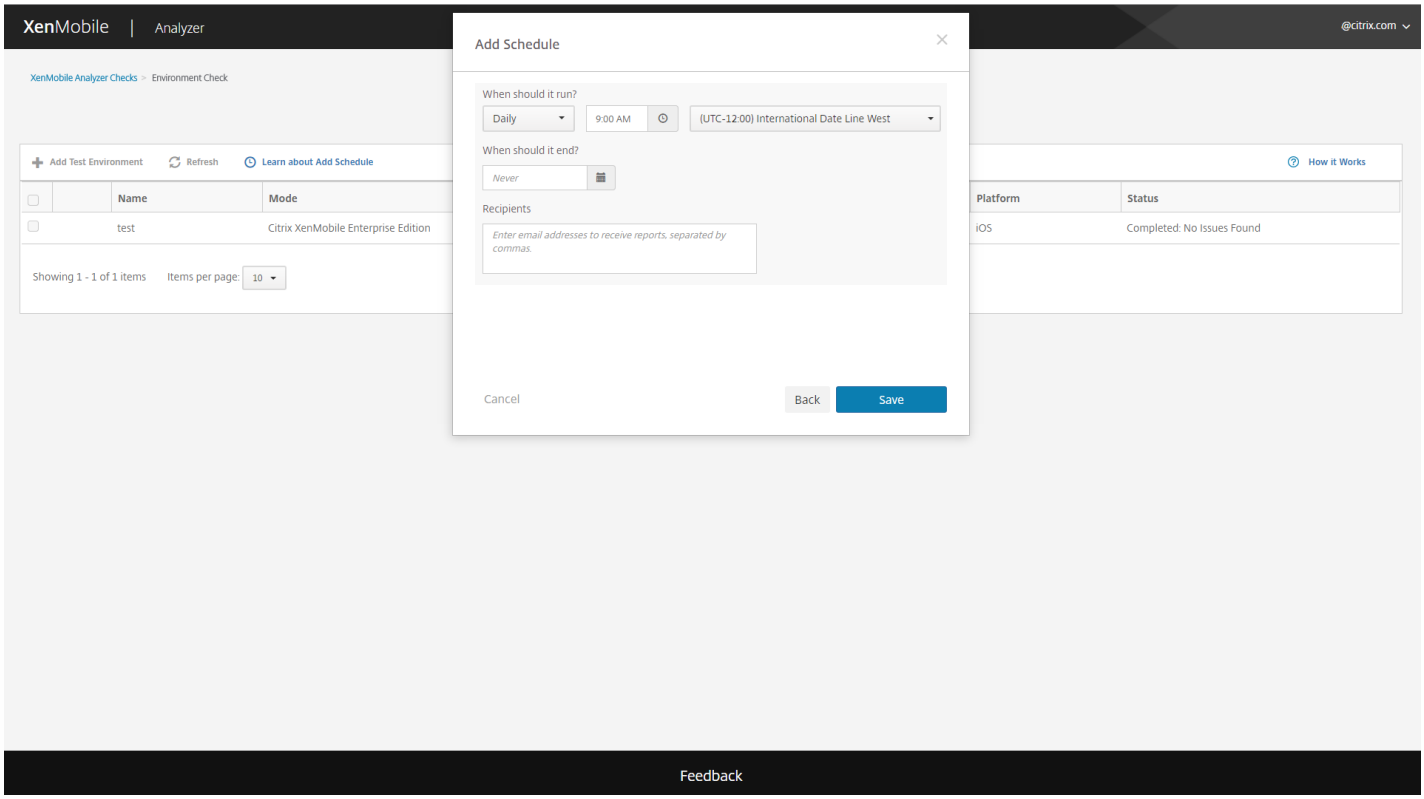


3. テストを実行する**ユーザー名**と**パスワード**を入力します。

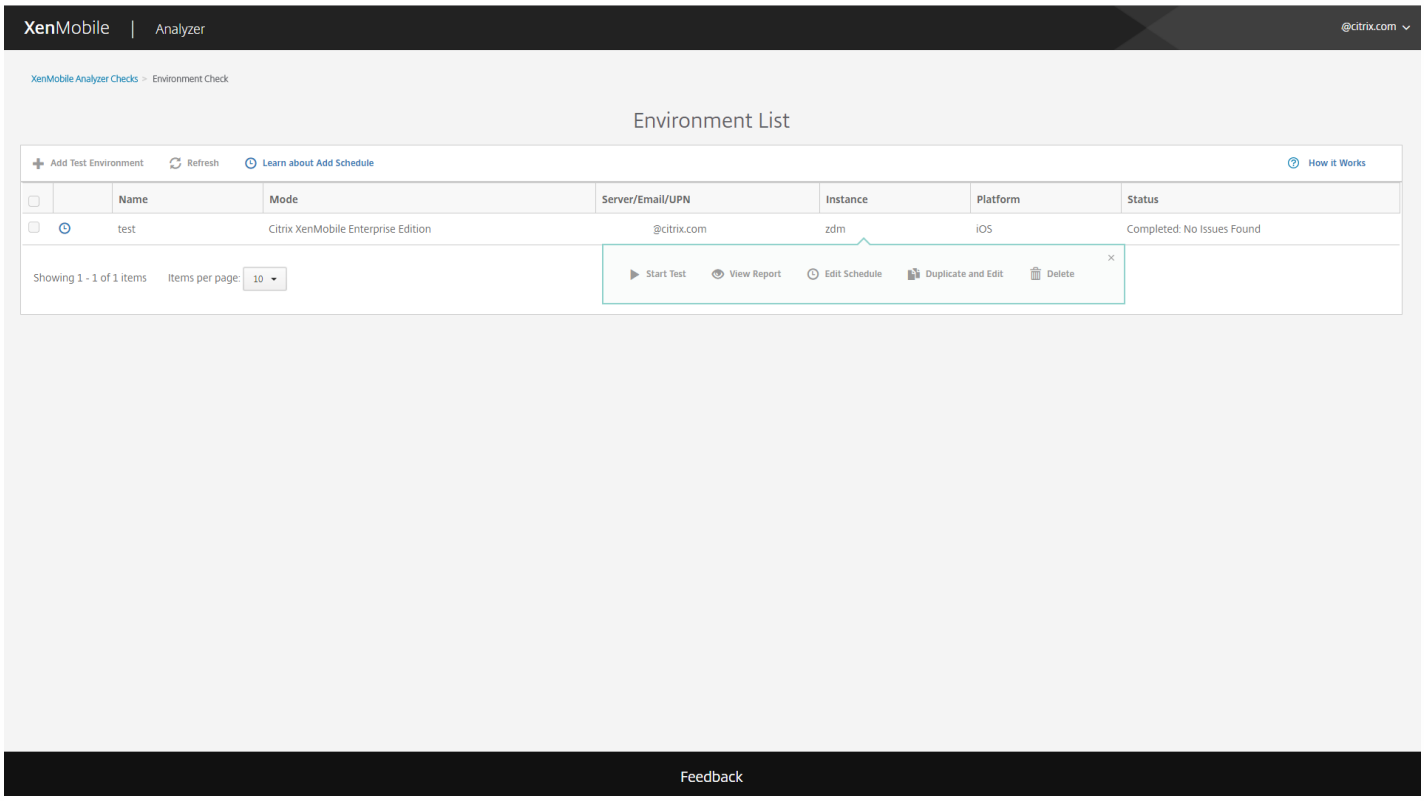


4. テストを実行するスケジュールを構成します。ドロップダウンから [**Daily**] または [**Weekly**] を選択します。テストを実行する時刻とタイムゾーンを選択します。カレンダーを使用して、スケジュールしたテストの実行を停止する日

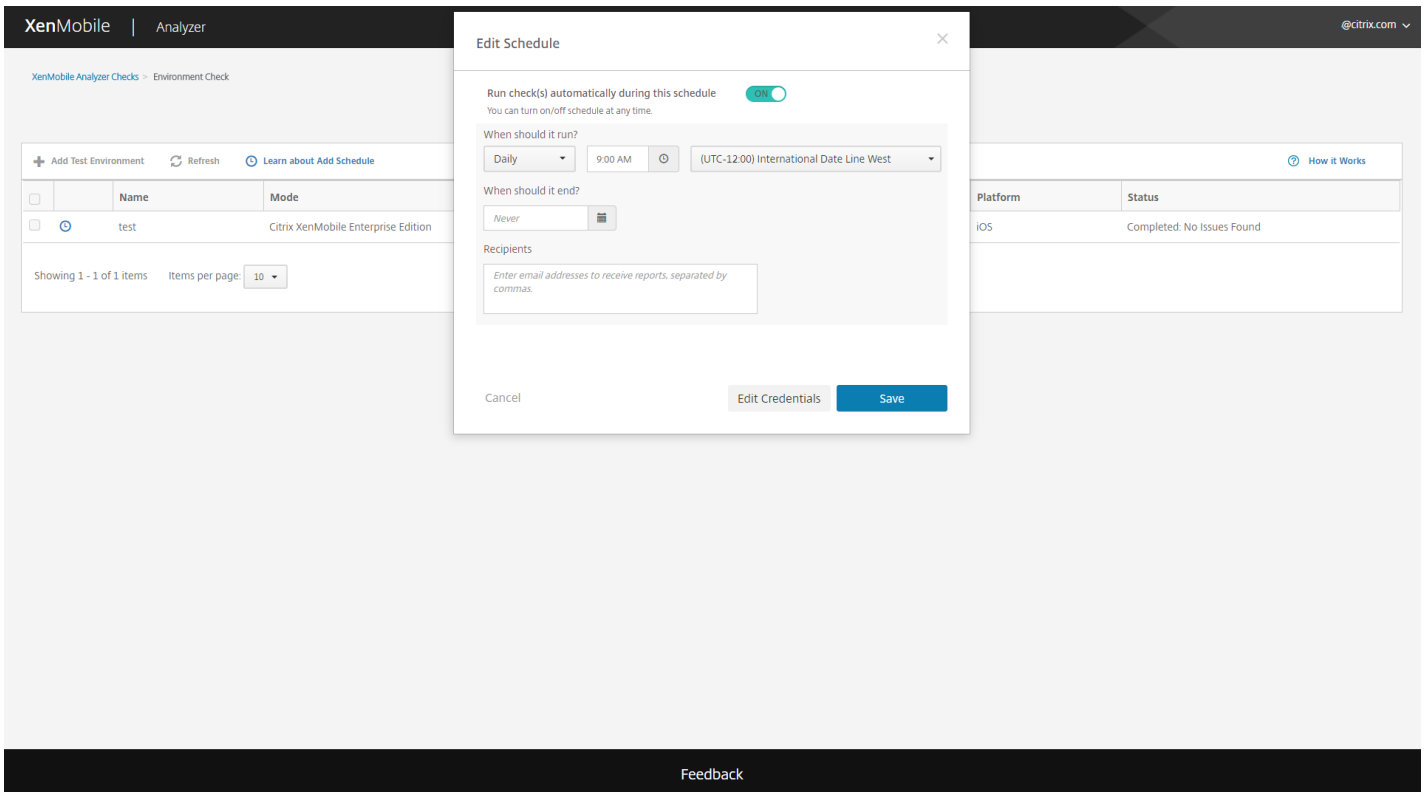
付を選択します。テストを無期限に実行する場合は空白のままにします。レポートを送信するメールアドレスの一覧を、コンマで区切って入力します。［**Save**］をクリックします。



5. テストの左側に、スケジュールが構成されていることを示す時計アイコンが表示されます。テストの実行タイミングを変更するには、テストを選択して［**Edit Schedule**］をクリックします。



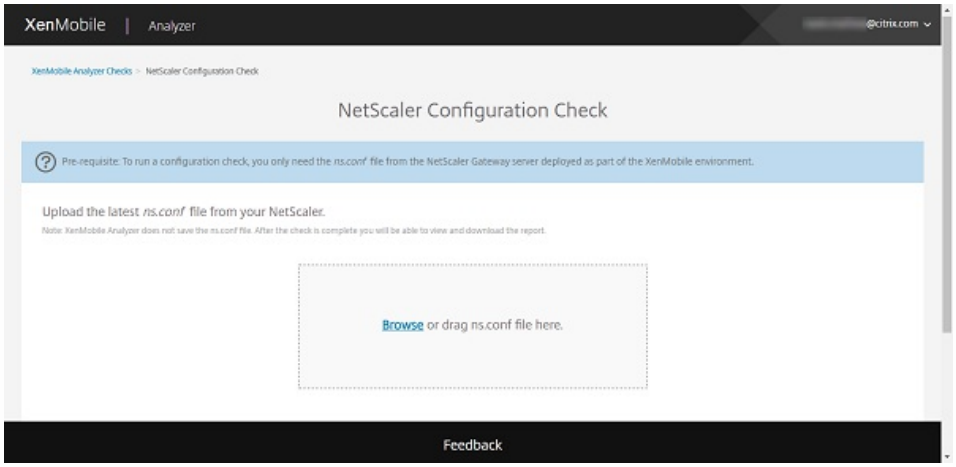
6. 表示されたウィンドウで、テストの実行タイミングを変更できます。最上部にあるスイッチをクリックして、テストを無効にすることもできます。変更が完了したら［**Save**］をクリックします。



NetScalerチェックの実行

1. XenMobile Analyzerにログオンして［**NetScaler Configuration**］をクリックします。

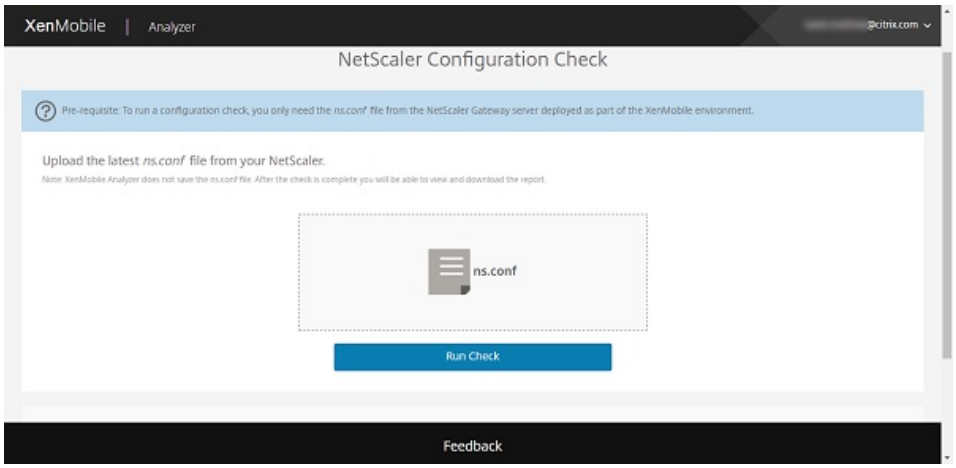
2. NetScalerインスタンスの最新のns.confファイルをアップロードします。アップロードは、ns.confファイルをアップロードボックスにドラッグするか、［**Browse**］をクリックしてファイルを追加することにより行います。最新のns.confファイルのダウンロード方法について詳しくは、Support Knowledge Centerを参照してください。



注意

XenMobile Analyzerにns.confファイルは保存されません。チェックが完了すると、レポートを表示およびダウンロードできるようになります。

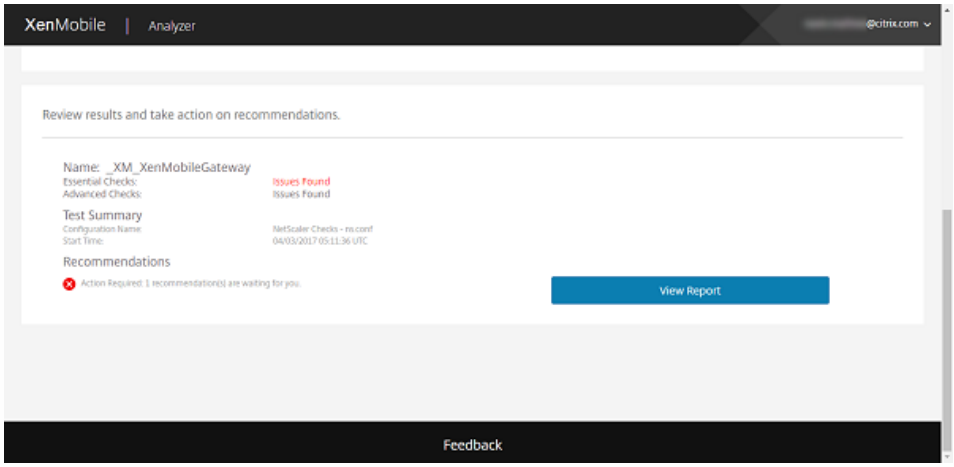
3. [**Run Check**] をクリックします。



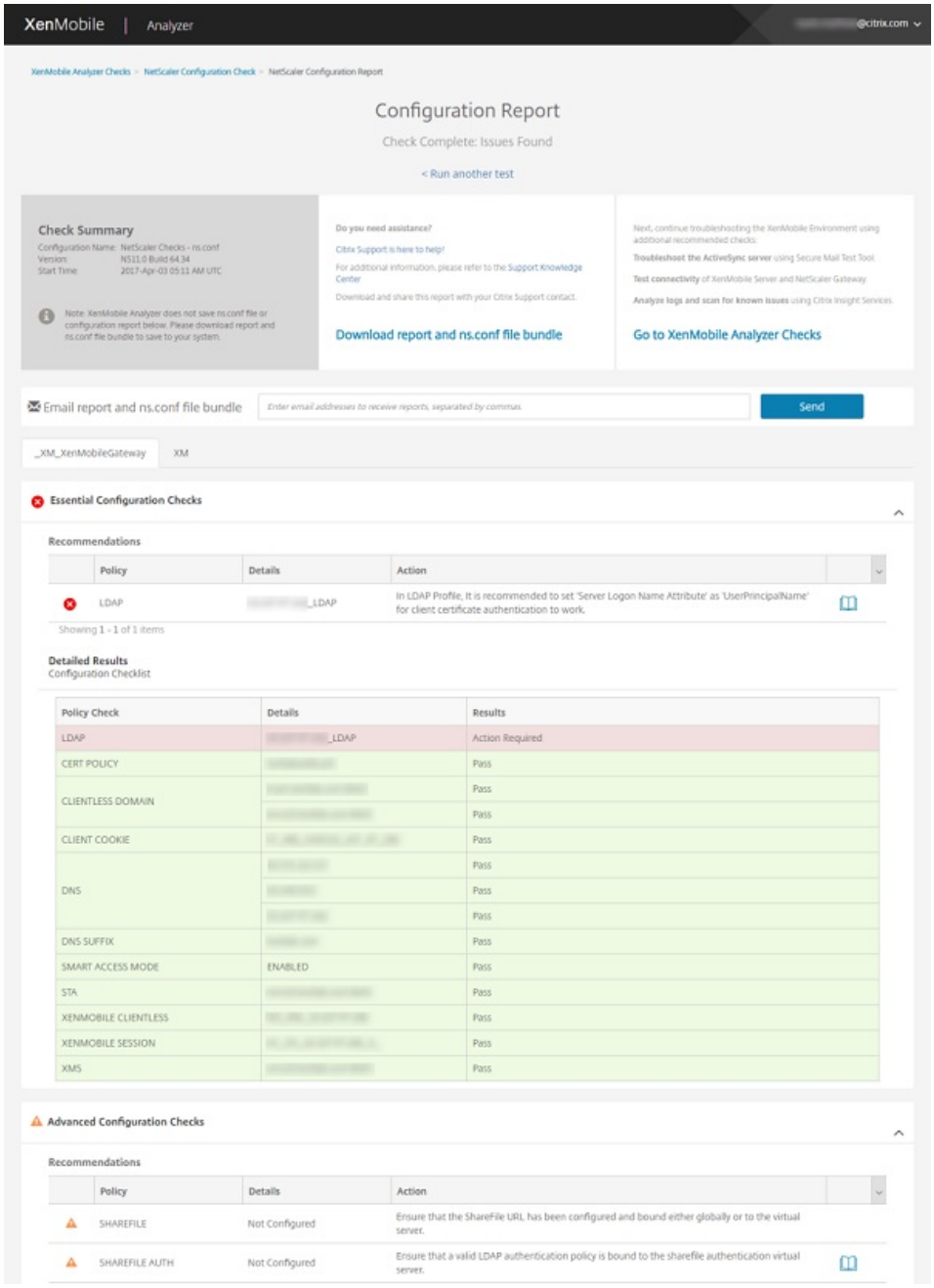
2種類の構成チェックが実行されます。

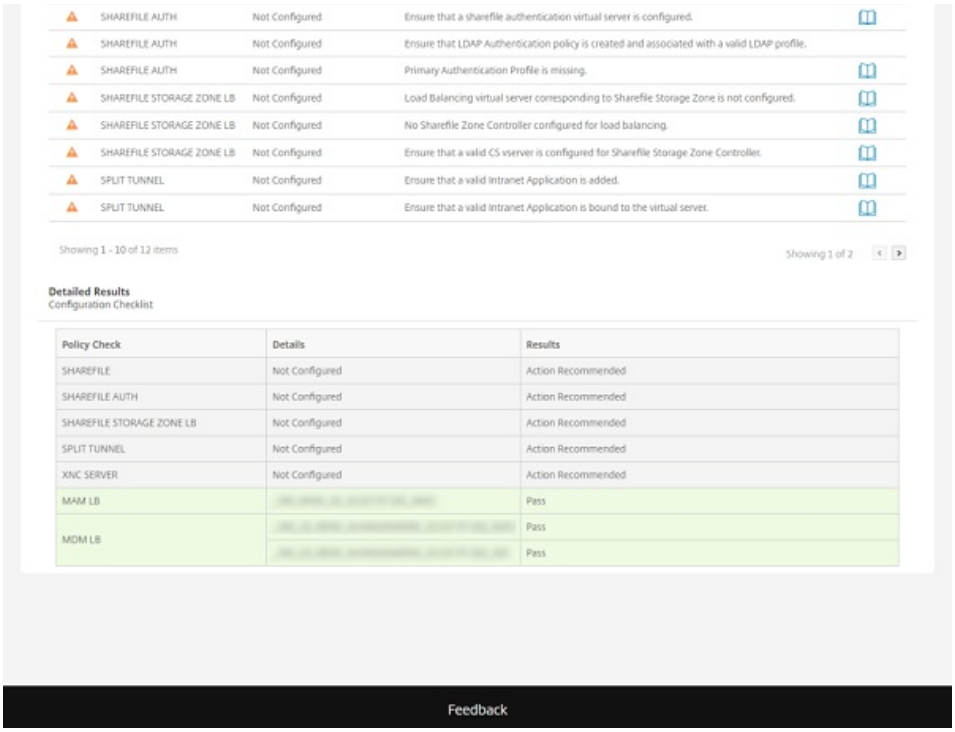
- 必須チェックでは、XenMobileを正常に展開するために不可欠なコンポーネントを確認します。
- 詳細チェックでは、必須ではないもののXenMobileの展開を補助するコンポーネントを確認します。

4. NetScalerの必須チェックおよび詳細チェックに基づく推奨事項を確認するには、[**View Report**] をクリックします。



[**Configuration Report**] ページが開きます。





注意

XenMobile Analyzerでは、NetScalerウィザードを使用して構成されたゲートウェイサーバーがサポートされます。NetScaler Gatewayインスタンスのタイトルにはすべて、「_XM_*展開時にユーザーが指定した名前」という名前が付けられます。

必須構成チェックに合格すると、全体の状態が成功になります。

必須構成チェックに失敗すると、［Recommendations］テーブルに**ポリシー**、**詳細**、**結果（必要なアクション）**が一覧表示されます。

詳細構成チェックに失敗すると、［Recommendations］テーブルに**ポリシー**、**詳細**、**結果（推奨されるアクション）**が一覧表示されます。

［**Configuration Report**］ページには次のオプションが用意されています。

a. 詳細を表示するには、［**Essential Configuration Checks**］または［**Advanced Configuration Checks**］（または展開アイコン）をクリックします。

b. 別のNetScaler構成チェックを実行するには、［**Run another test**］をクリックします。

c. トラブルシューティングツールおよび分析ツールを表示するには、［**Go to XenMobile Analyzer Checks**］をクリックします。

d. 結果のレポートをダウンロードするには［**Download report and ns.conf file bundle**］をクリックします。また

は、［**Email report and ns.conf bundle**］にメールアドレスを入力して、［**Send**］をクリックします。

その他の有益なチェックの実行

XenMobile Analyzerの環境チェック手順では直接操作してテストを実行しますが、その他のオプションでは役立つ情報が提供されます。これらの各オプションでは、XenMobile環境を正しく設定するために使用できる他のツールの情報が提供されます。

- **詳細診断**：環境に関する情報を収集して、Citrix Insight Servicesにアップロードします。このツールによってデータが分析され、環境に合ったレポートが推奨される解決方法とともに提供されます。
- **Secure Mailの用意**：XenMobile Exchange ActiveSync Testアプリケーションをダウンロードして実行します。このアプリケーションでは、XenMobile環境への展開についてのActiveSyncサーバーのトラブルシューティングを行います。アプリケーションを実行した後に、レポートを確認したり他のユーザーと共有したりできます。
- **サーバー接続チェック**：XenMobile Server、認証サーバー、およびShareFileサーバーへの接続を確認するための手順が示されます。
- **Citrixサポートへの問い合わせ**：他のすべての手順が失敗した場合に、Citrixサポートでサポートチケットを作成できます。

既知の問題

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、一覧に表示されるアプリの数がクライアントによって異なることがあります。
- Secure Webの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。
- Secure Hubの共有デバイス認証機能は使用できません。
- Secure Webテストは入力されたURLへの接続をチェックするだけで、関連サイトへの認証はチェックしません。

解決された問題

以下のXenMobile Analyzerの問題は解決されました。

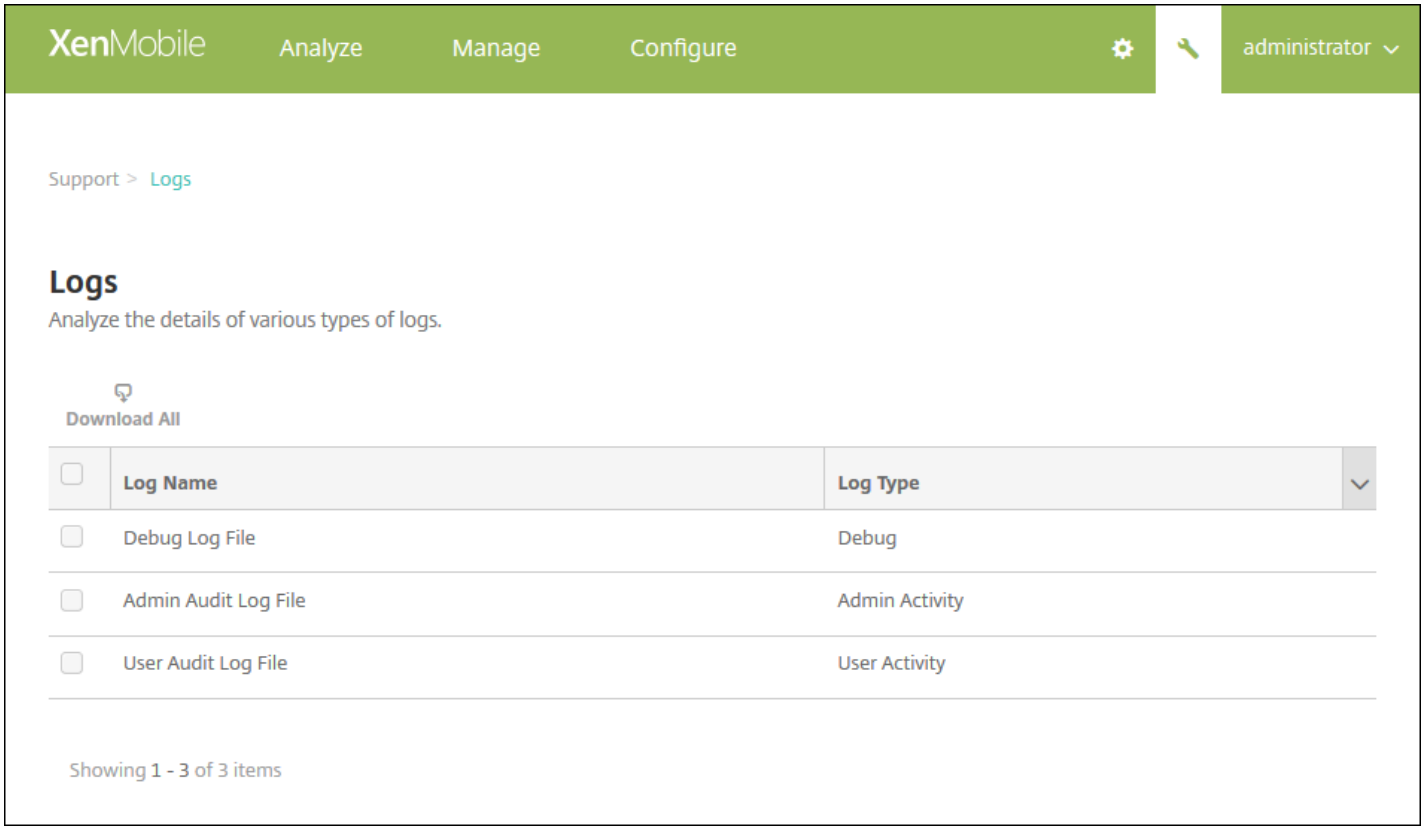
- 登録招待を使用してチェックを実行すると、テストは成功しますが登録招待は受理されません。

XenMobileでのログファイルの表示および分析

Feb 27, 2017

1. XenMobileコンソールで、右上のレンチアイコン（）をクリックします。**[サポート]** ページが開きます。

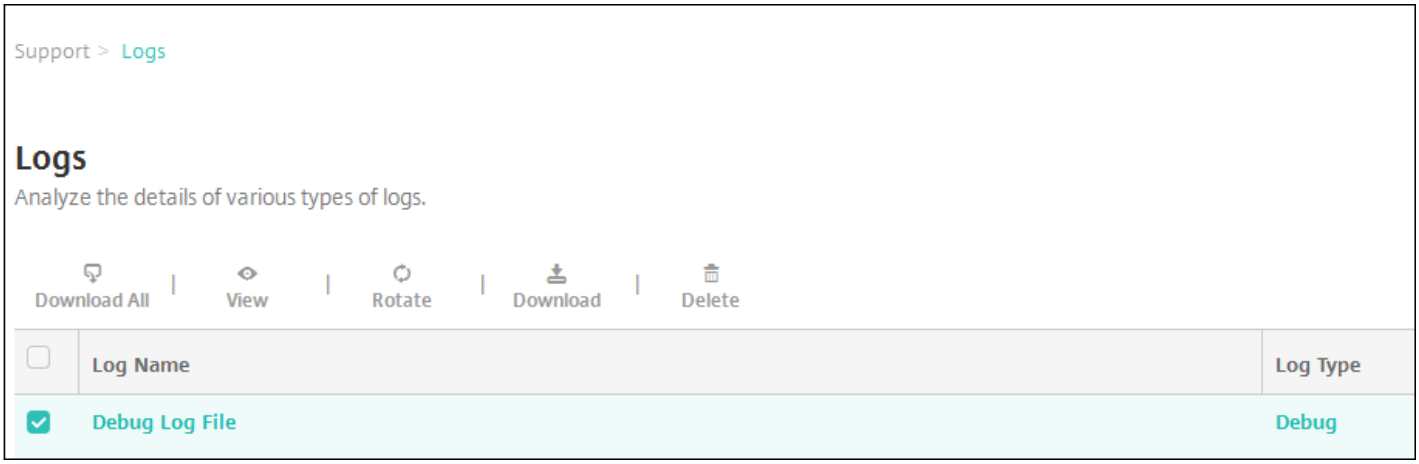
2. **[ログの操作]** の下の **[ログ]** をクリックします。 **[ログ]** ページが開きます。表に個別のログが表示されます。



3. 表示するログをオンにします。

- デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrixのサポート担当者向けの有用な情報が含まれています。
- 管理監査ログファイルには、XenMobileコンソール上の活動についての監査情報が含まれています。
- ユーザー監査ログファイルには構成済みユーザーに関連する情報が含まれています。

4. 表の上にあるアクションを使用して、すべてダウンロード、表示、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。

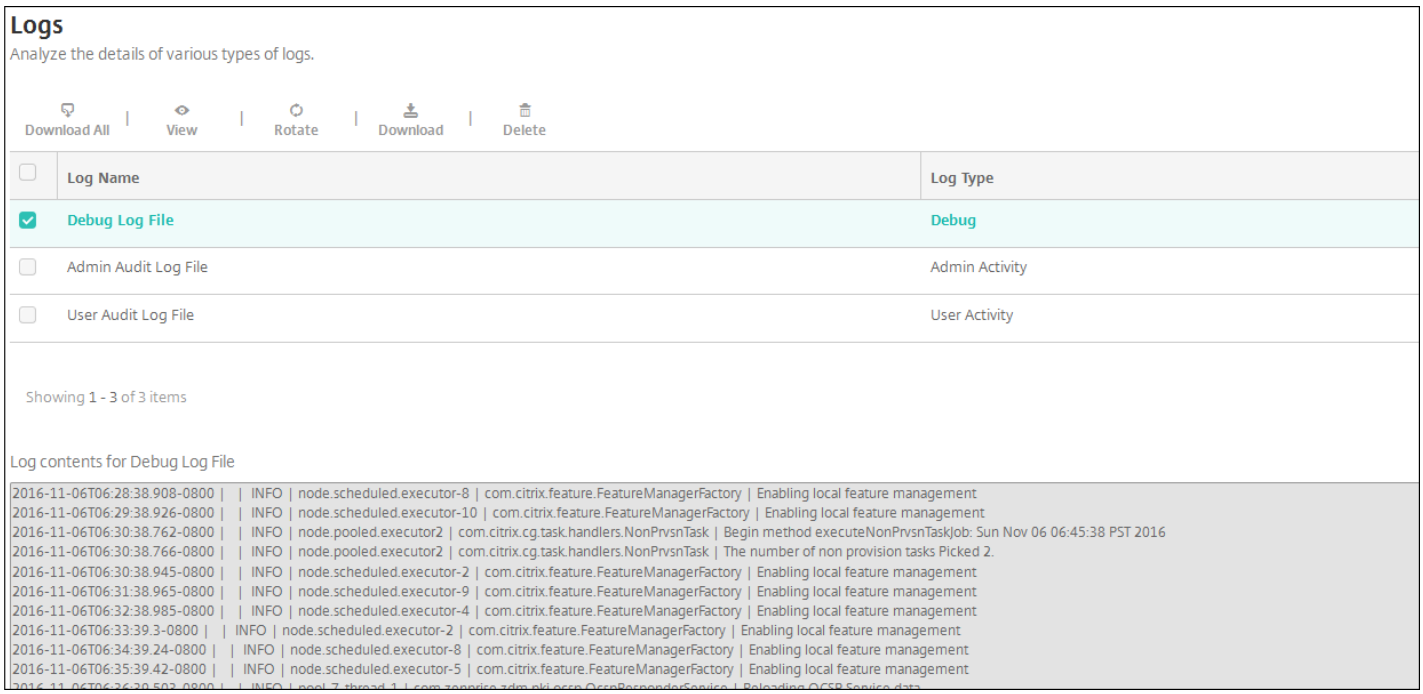


注：

- 複数のログファイルを選択した場合は、**[すべてダウンロード]**と**[交換]**のみを使用できます。
- XenMobileサーバーをクラスター化している場合は、接続しているサーバーのログのみを表示できます。ほかのサーバーのログを表示するには、ダウンロードオプションのいずれかを使用します。

5. 次のいずれかを行います。

- **すべてダウンロード**：システム上に存在するすべてのログ（デバッグ、管理監査、ユーザー監査、サーバーのログなど）をダウンロードします。
- **表示**：表の下に選択したログの内容を表示します。
- **交換**：現在のログファイルをアーカイブし、ログエントリを取得するための新しいファイルを作成します。ログファイルをアーカイブするときに、ダイアログボックスが開きます。［交換］をクリックして続行します。
- **ダウンロード**：選択されている単一の種類のログファイルのみをダウンロードします。アーカイブ済みの同じ種類のログもダウンロードされます。
- **削除**：選択したログファイルを完全に削除します。



REST API

Feb 27, 2017

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。

REST APIへのアクセスに必要な権限

REST APIへのアクセスには、以下の権限のうち1つが必要です。

- 役割ベースのアクセス構成の一部として設定されたパブリックAPIアクセス権限（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。

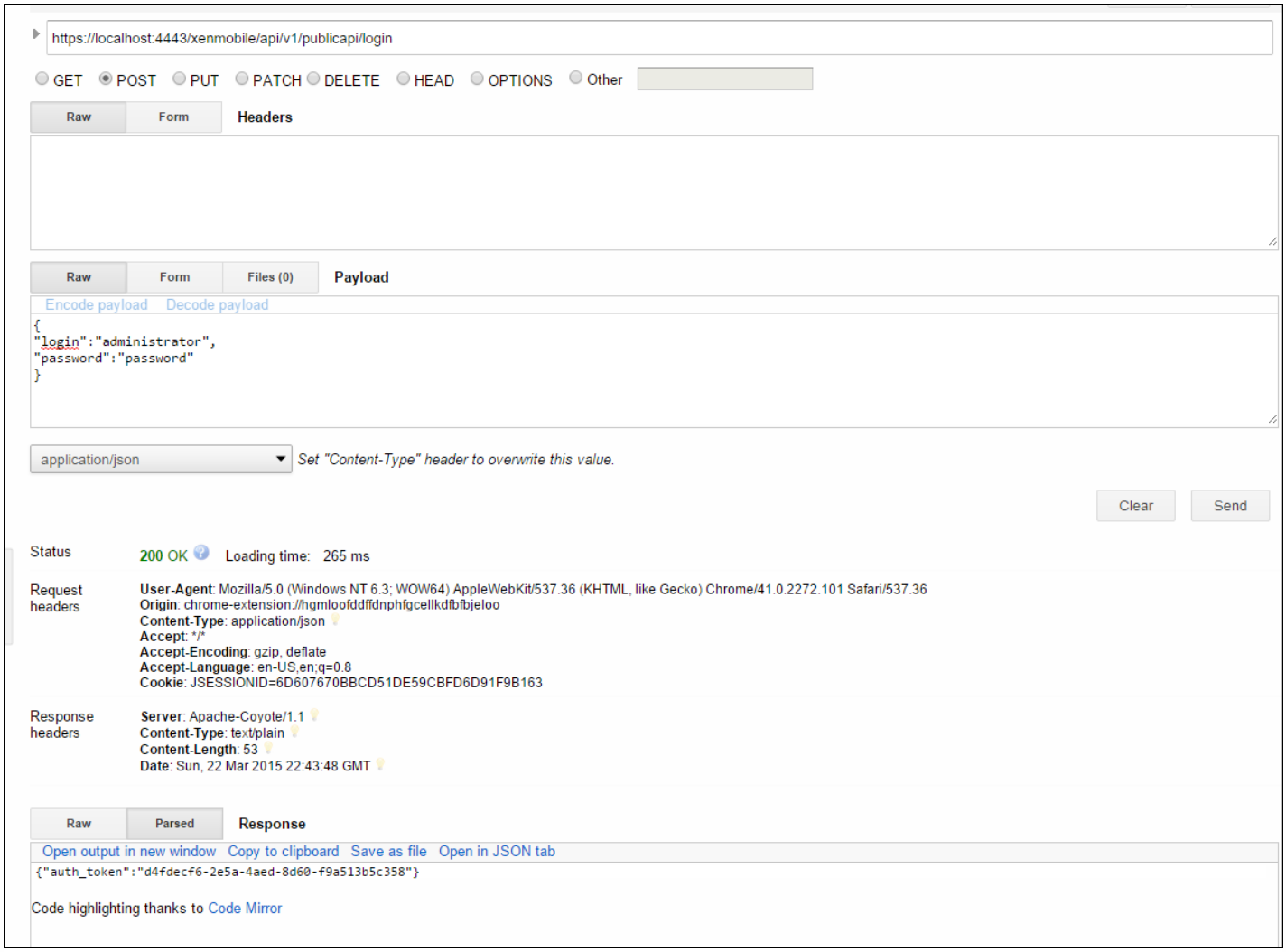
ログオン

URL：https://<ホスト名>:<ポート番号>/xenmobile/api/v1/authentication/login

要求: { "login":"administrator", "password":"password" }

メソッドの種類: POST

Content type：application/json



XenMobile Mail Manager 10のアーキテクチャ

Feb 27, 2017

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。無視可能と構成されていないエラーがメジャースナップショットにより戻された場合、スナップショットの結果は放棄されます。

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。無視するエラーそれぞれに対して、IgnorableErrors子ノードをPowerShellノードに追加します。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ユーティリティ一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。

認証

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。以前、XenMobile Mail Manager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［構成］ウィンドウで［パイプライン化の無効化］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]

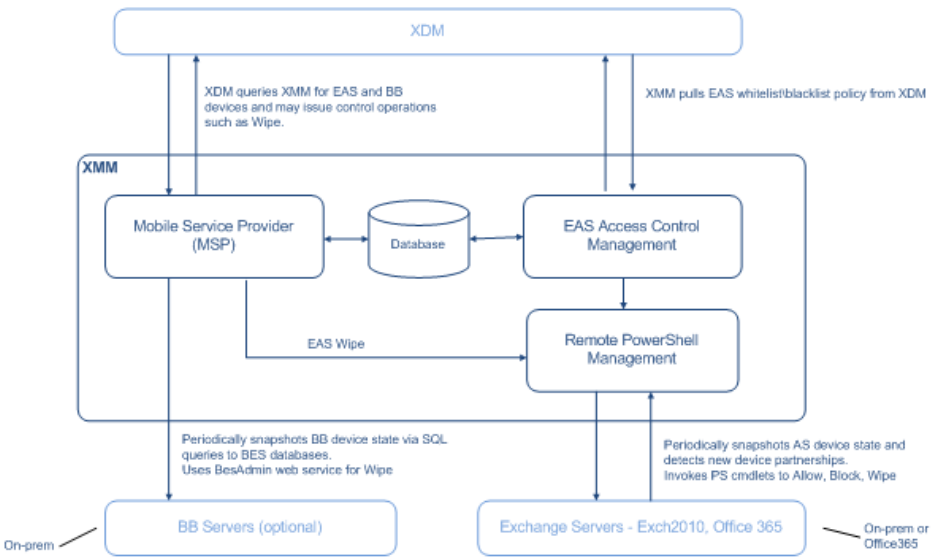
パイプライン化が無効化されたサポートシナリオで（XenMobile Mail Managerコンソールの［Configuration］ウィンドウで［Disable Pipelining］オプションを選択）、詳細スナップショットと簡易スナップショットのどちらのために環境が構成されているかに関係なく、詳細スナップショット用のデータが収集されなくなりました。詳細スナップショット用のデータが収集されるのは、環境が詳細スナップショット用に構成されているときだけになりました。 [#586092]

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]

アーキテクチャ

Feb 27, 2017

次の図に、XenMobile Mail Managerの主要コンポーネントを示します。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、「Reference Architecture for On-Premises Deployments」についてのセクション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

Feb 27, 2017

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 2012 R2、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 2016、SQL Server 2012、SQL Server 2012 Express LocalDB、またはSQL Server Express 2008
- 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

デバイスのメールクライアント

すべてのメールクライアントが、デバイスに関して一貫して同じActiveSync IDを返すわけではありません。XenMobile Mail Managerは、各デバイスに対して一意のActiveSync IDを前提とするため、デバイスごとに一意の同じActiveSync IDを一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントはテスト済みで、エラーなく実行できます。

- HTCのネイティブメールクライアント
- Samsungのネイティブメールクライアント
- iOSのネイティブメールクライアント
- Touchdown for Smartphones

XenMobile Mail Managerの前提条件

- 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、Set-AdServerSettings -ViewEntireForest $trueを実行するための権限が付与されている必要があります。
- 指定された資格情報には、リモートシェルを介して、Exchange Serverに接続する権限が与えられている必要があります。デフォルトでは、Exchangeをインストールしたユーザーがこの権限を持ちます。
- Microsoft TechNetサポート技術情報「about_Remote_Requirements」によれば、リモート接続を確立してリモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。ブログ記事You Don't Have to Be An Administrator to Run Remote PowerShell Commandsに記載されているように、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、Exchange Serverで次のPowerShellコマンドを実行する管理者にとって必要なのは、WinRM QuickConfigだけです。
- Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。Exchange 2010の場合、1人のユーザーに許可されている同時接続数のデフォルトは18です。接続数の上限に達すると、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。

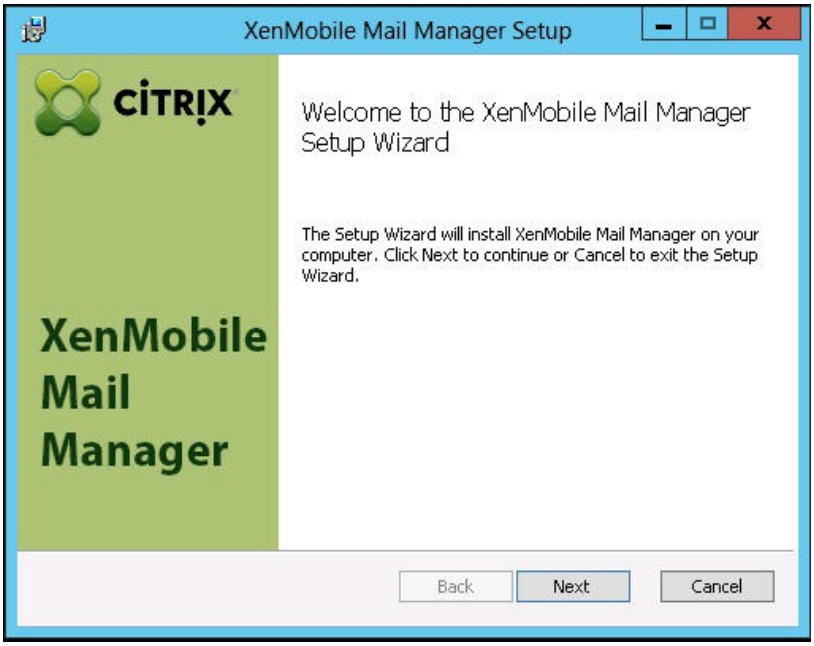
Office 365 Exchangeの要件

- **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
- **特権**。指定された資格情報には、リモートシェルを介して、Office 365サーバーに接続する権限が与えられている必要があります。デフォルトでは、Office 365のオンライン管理者には、必要な権限が備えられています。
- **調整ポリシー**。Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。Office 365の場合、1人のユーザーに許可されている同時接続数のデフォルトは3です。接続数の上限に達すると、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。

インストールと構成

Feb 27, 2017

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。

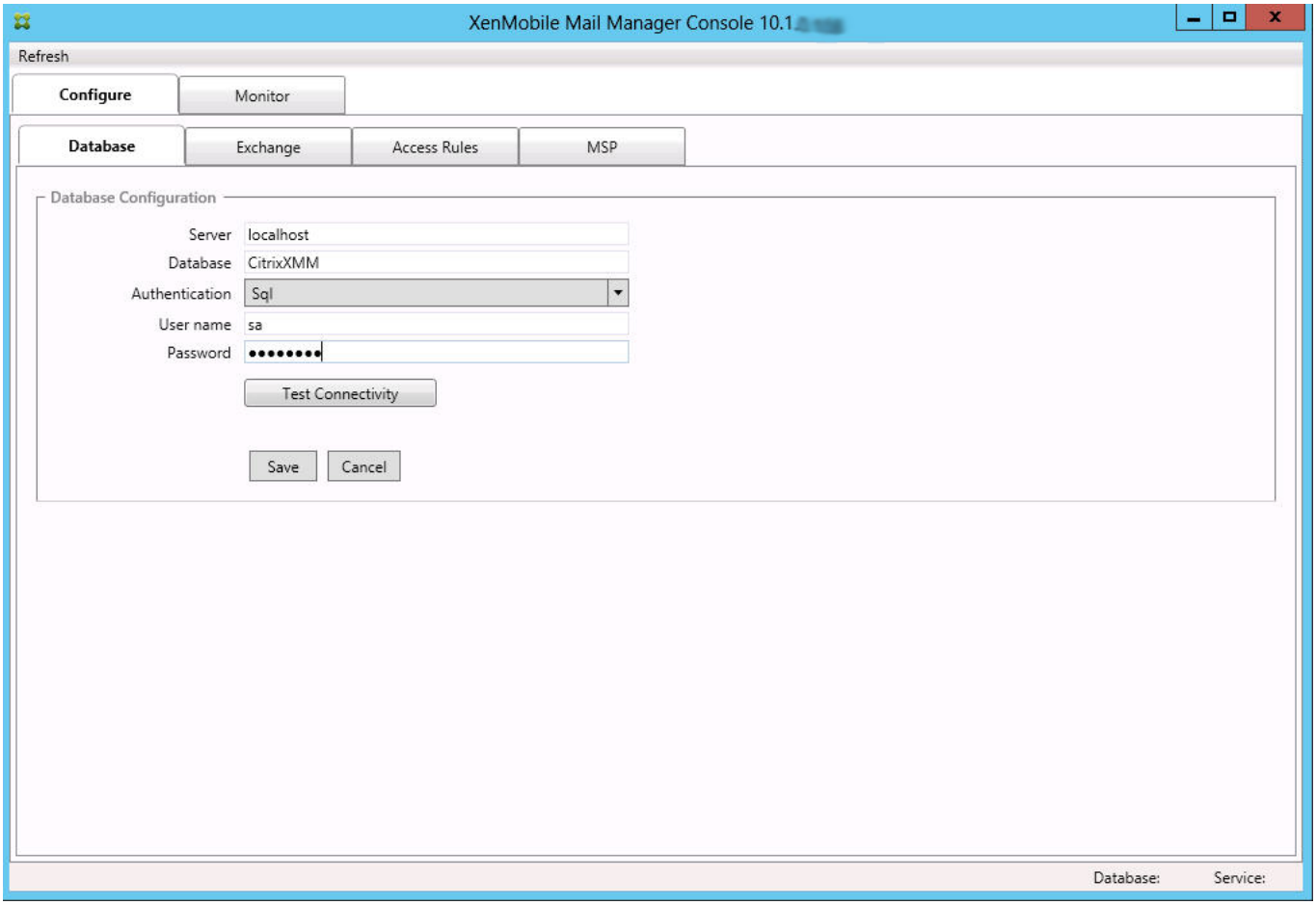


2. セットアップウィザードの最後の画面で、［**Launch the Configure utility**］をオンのままにしておきます。または、［**Start**］メニューの［**XenMobile Mail Manager**］を選択します。

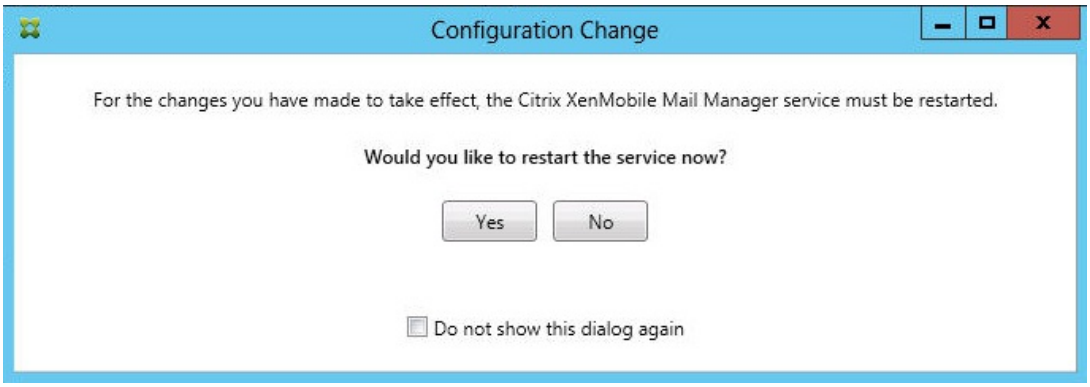
3. 次のデータベースプロパティを構成します。
    1. ［**Configure**］の［**Access Rules**］タブを選択します。
    2. SQL Serverの名前（デフォルトはlocalhost）を入力します。
    3. データベースはデフォルトのCitrixXmmのままにします。
    4. SQLに使用される次のいずれかの認証モードを選択します。

- **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。

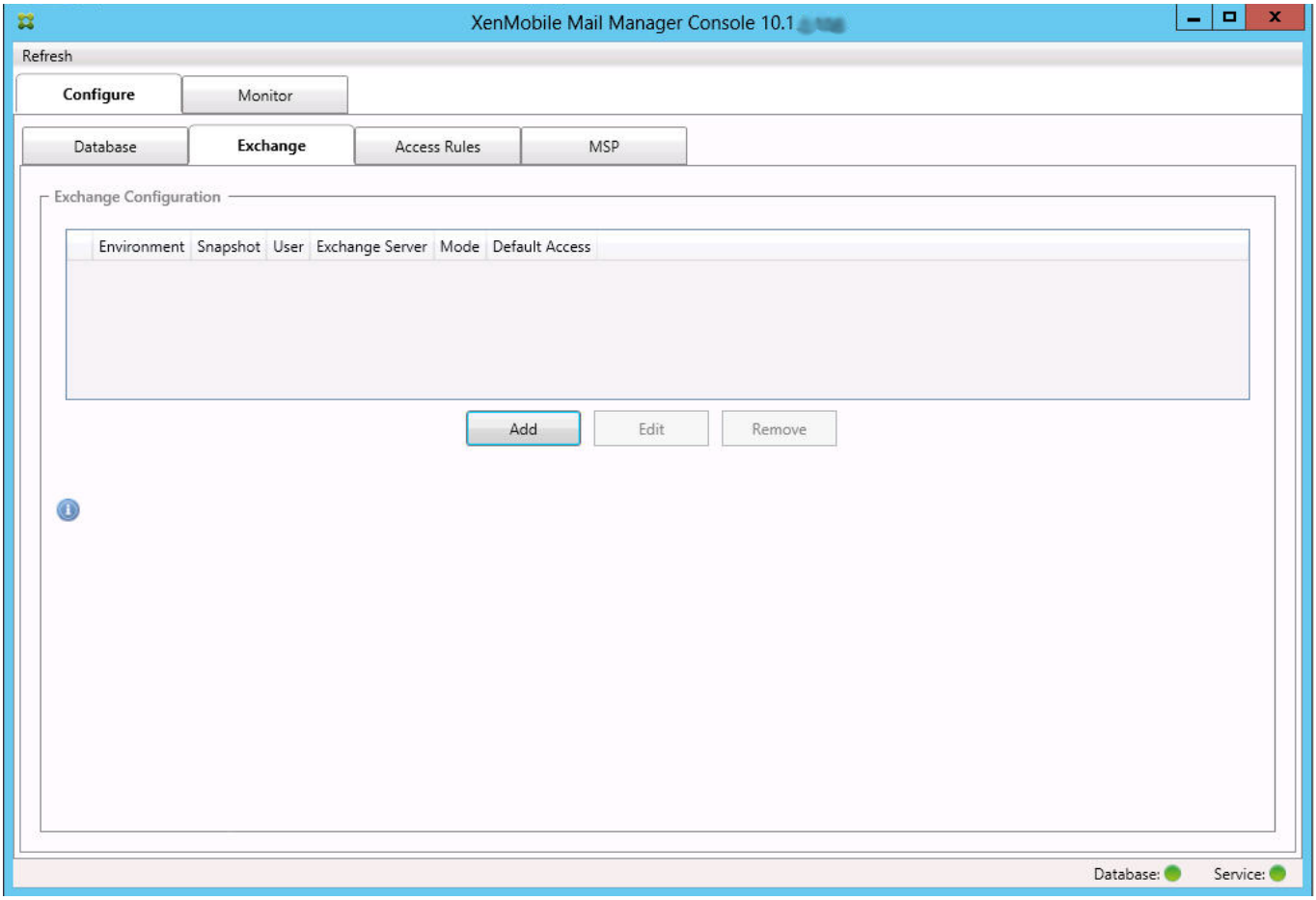
5. **［Test Connectivity］**をクリックしてSQL Serverに接続できることを確認し、**［Save］**をクリックします。



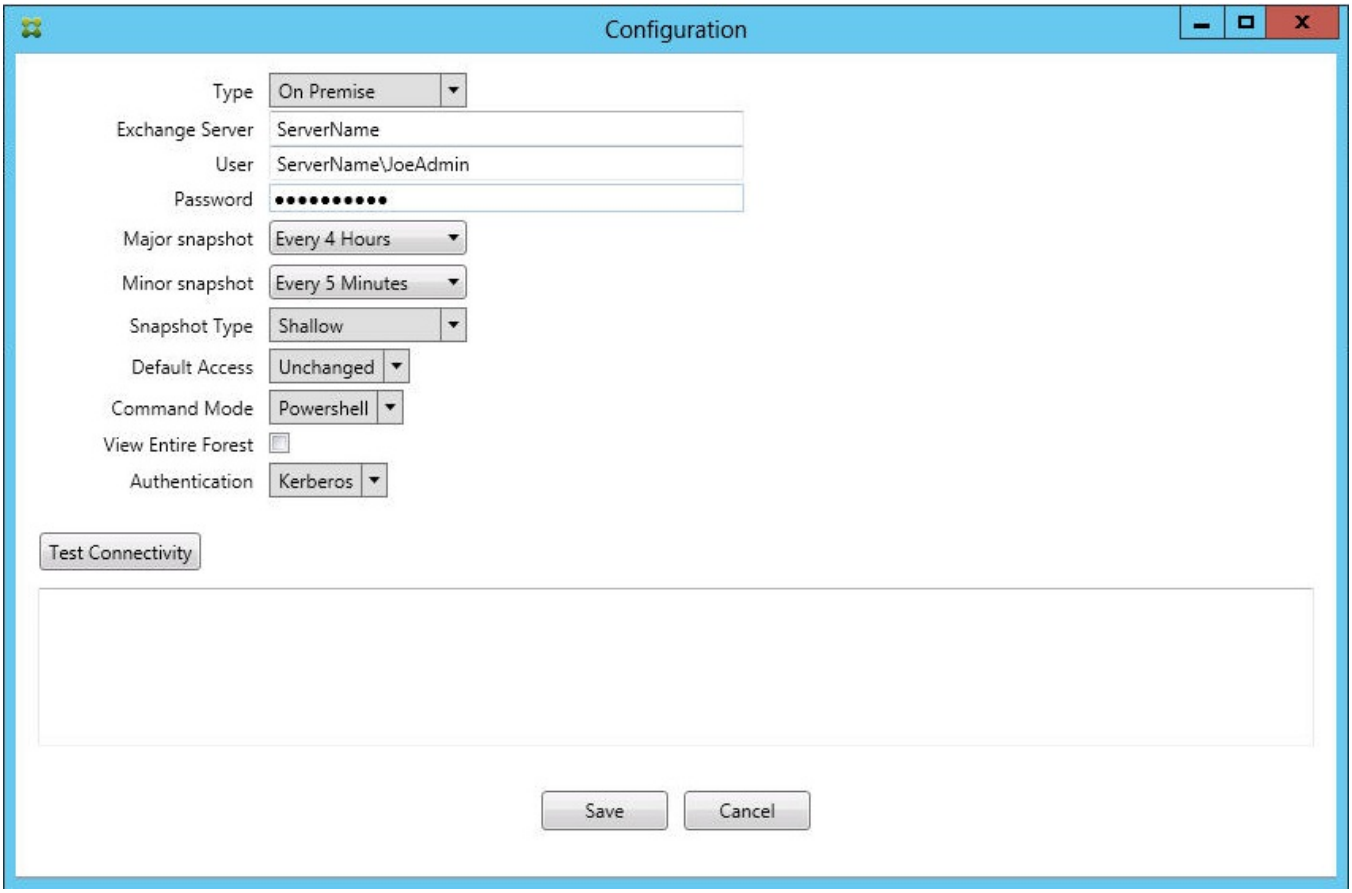
4. サービスの再起動を求めるメッセージが表示されます。**［Yes］**をクリックします。



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。



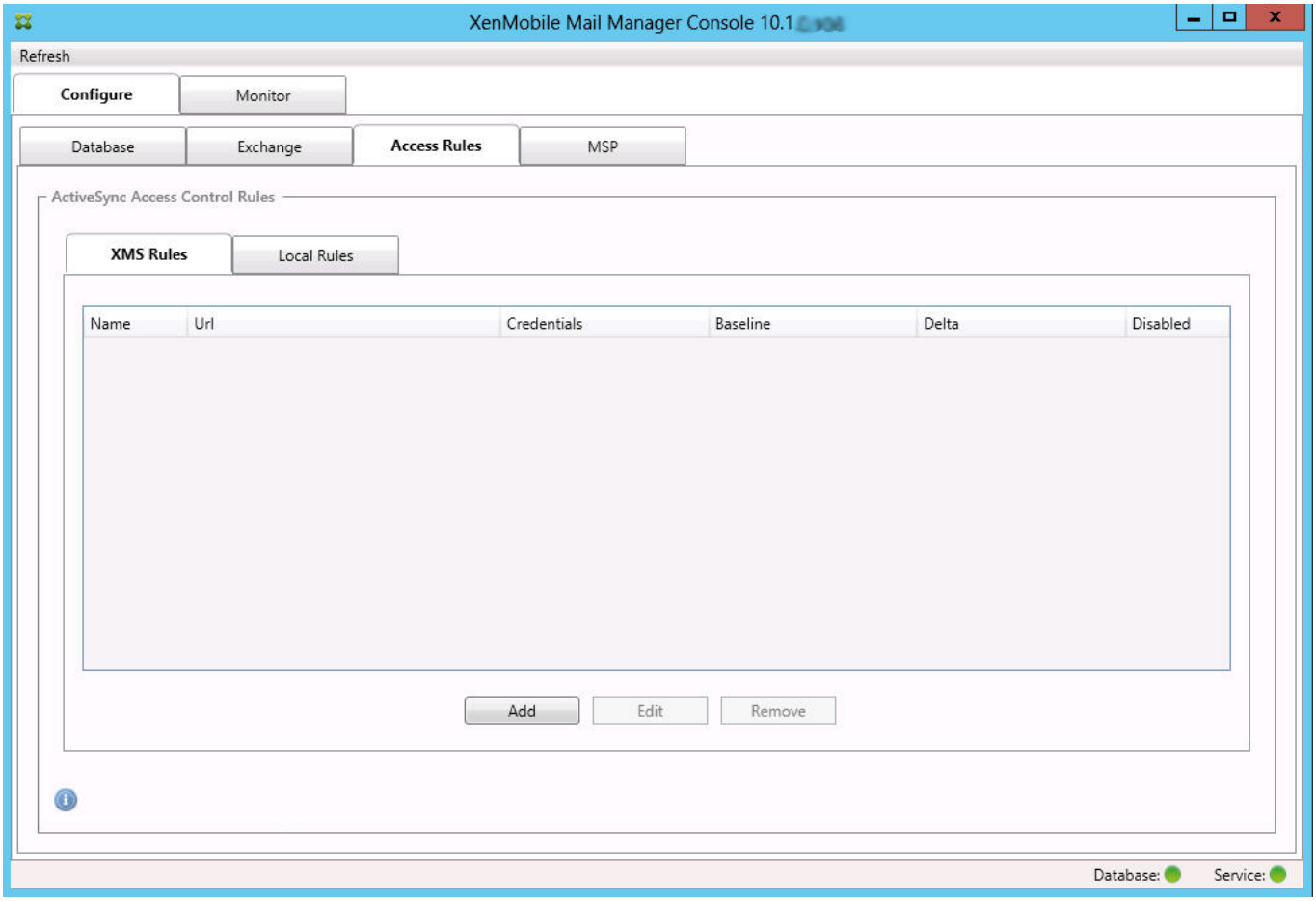
3. **[追加]**をクリックします。
4. Exchange Server環境の種類として、 **[On Premise]**または**[Office 365]**を選択します。



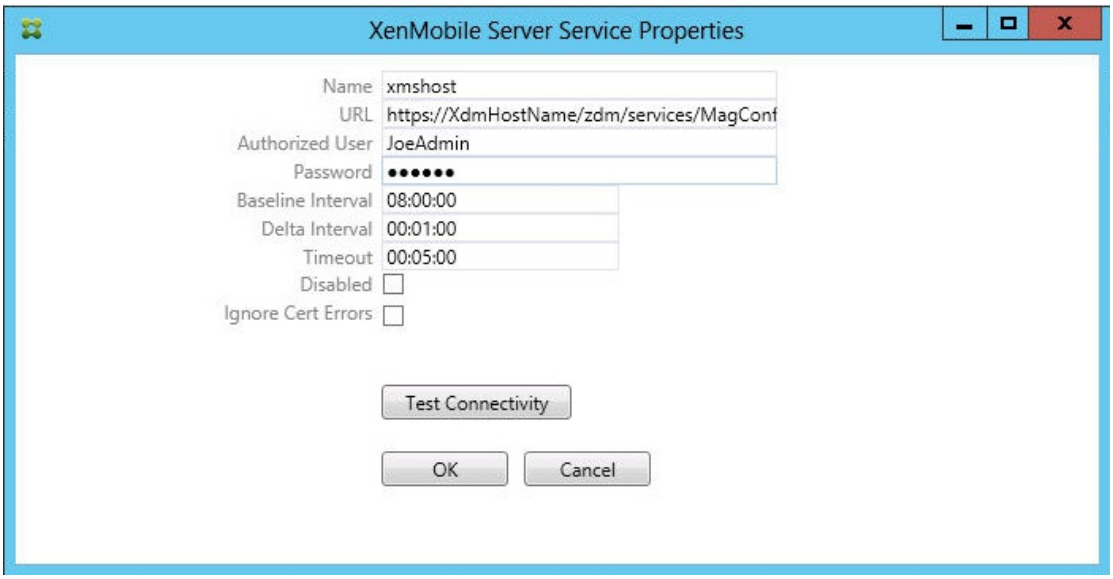
5. **［On Premise］**を選択した場合は、リモートPowerShellコマンド用に使用するExchange Serverの名前を入力します。
6. 要件セクション内で指定されているとおりの、Exchange Serverに対する適切な権限を持つWindows IDのユーザー名を入力します。
7. ユーザーのパスワードを**［Password］**ボックスに入力します。
8. メジャースナップショットを実行するスケジュールを選択します。メジャースナップショットにより、すべてのExchange ActiveSyncパートナーシップが検出されます。
9. マイナースナップショットを実行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の選択： **［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の選択： **［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 コマンドモード］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、**［フォレスト全体の表示］**を選択します。

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。

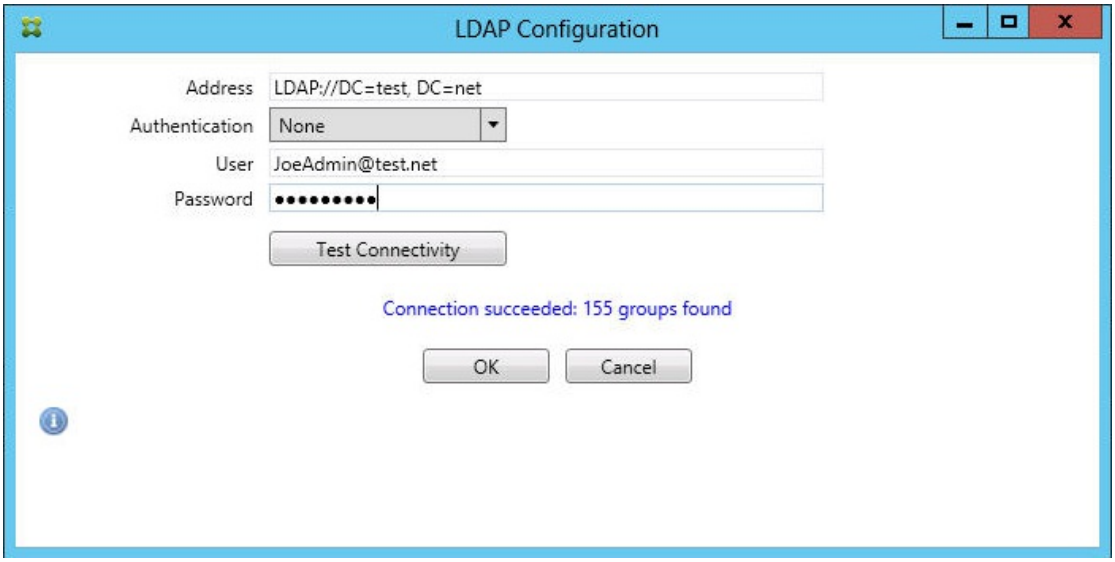


3. **[Add]** をクリックします。



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。

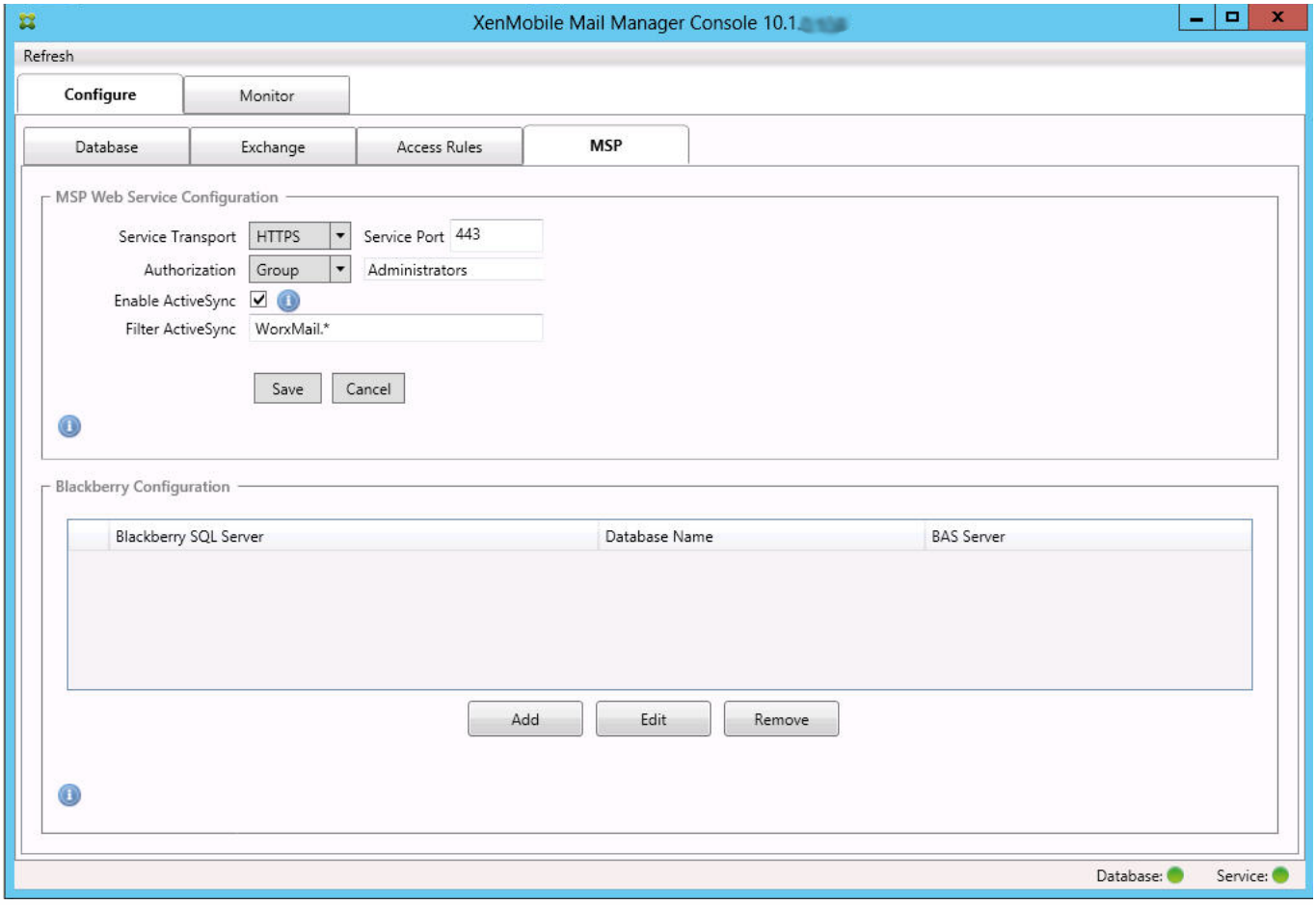
7. **[Local Rules]** タブをクリックします。
   1. Active Directoryのグループに対して使用するローカル規則を作成する場合は、**[Configure LDAP]** をクリックし、LDAP接続プロパティを構成します。



   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を使用します。したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。
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。

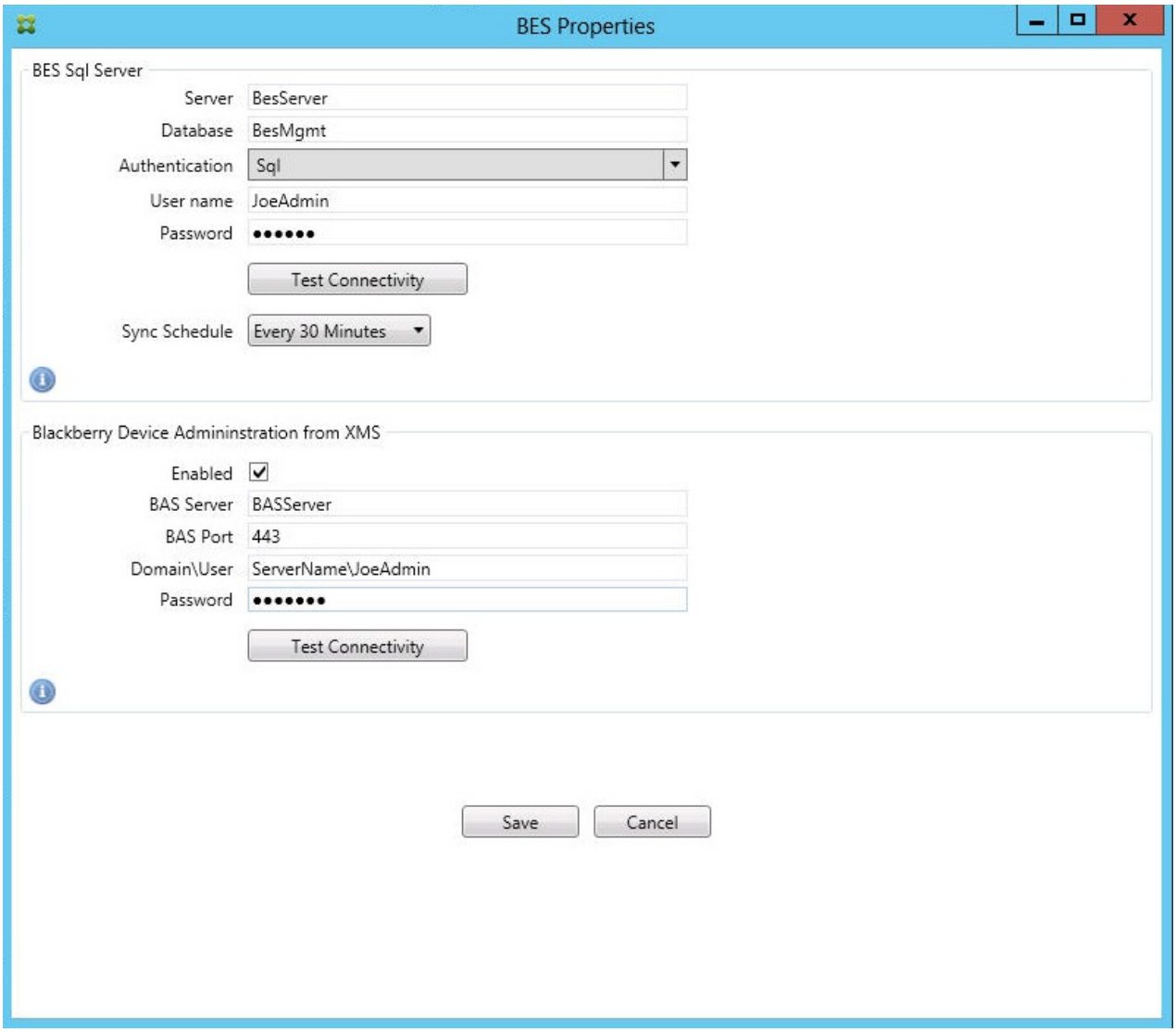
8. Mobile Service Providerを構成します。
   注：Mobile Service Providerはオプションであり、Mobile Service Providerインターフェイスを使用して非管理対象デバイスを照会するようにXenMobileがさらに構成されている場合にのみ必要です。
   1. ［**Configure**］> ［**MSP**］タブをクリックします。



   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。
   XenMobileサーバーでActiveSyncクエリが有効の場合は、Exchange Server（1つまたは複数）のスナップショットの種類を［**Deep**］に設定する必要があります。これにより、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「Secure Mail.*」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。

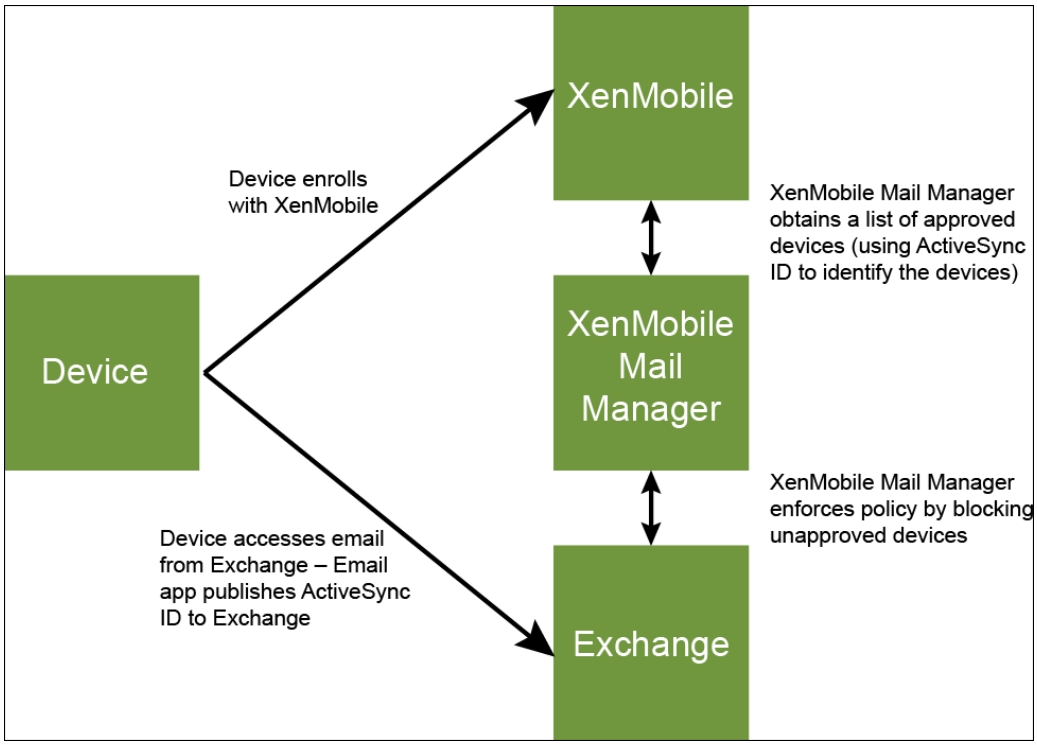
7. **[Test Connectivity]** をクリックして、SQL Serverへの接続を確認します。
   注： [Windows Integrated] を選択している場合、このテストでは、XenMobile Mail Managerサービスのユーザーでは
   なく、現在ログオンしているユーザーが使用されるため、SQL認証が正確にテストされません。
8. XenMobileからのBlackBerryデバイスのリモートでのワイプやResetPasswordをサポートする場合
   は、 **[Enabled]** チェックボックスをオンにします。
   1. BESの完全修飾ドメイン名（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

Feb 27, 2017

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とも呼ばれ、デバイスを一意に識別するために使用されます。Secure Hubでは同様の識別子を取得し、デバイスが登録されるとXenMobileにこの識別子を送信します。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
り、静的なポリシーを［デフォルトで禁止］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

Feb 27, 2017

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（XDM規則とも呼ばれます）、およびデフォルトのアクセス規則の3種類の規則があります。

ローカル規則：ローカル規則は最も優先されます。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］>［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XenMobile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
- XenMobileサーバー規則
- デフォルトのアクセス規則

一致が検出されると、評価は停止します。たとえば、ローカル規則が特定のデバイスと一致すると、そのデバイスはXenMobileサーバー規則またはデフォルトのアクセス規則に対して評価されません。このことは、特定の種類の規則内でも当てはまります。たとえば、ローカル規則一覧で、特定のデバイスに対して複数の一致がある場合、最初の一致が見つかるとすぐに評価は停止します。

デバイスプロパティが変更されたとき、デバイスが追加または削除されたとき、または規則自体が変更されたときは、現在定義されている一連の規則が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：

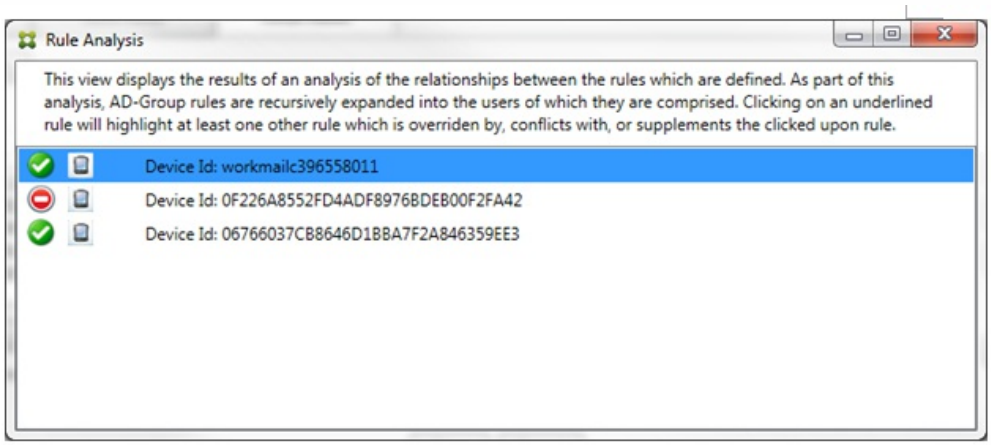
- **上書き規則**。同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- **競合規則**。同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- **補足規則**。正規表現の規則が複数あるので、2つ（またはそれ以上）の正規表現を1つの正規表現の規則に結合できるか、またはそれらの機能が重複していない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

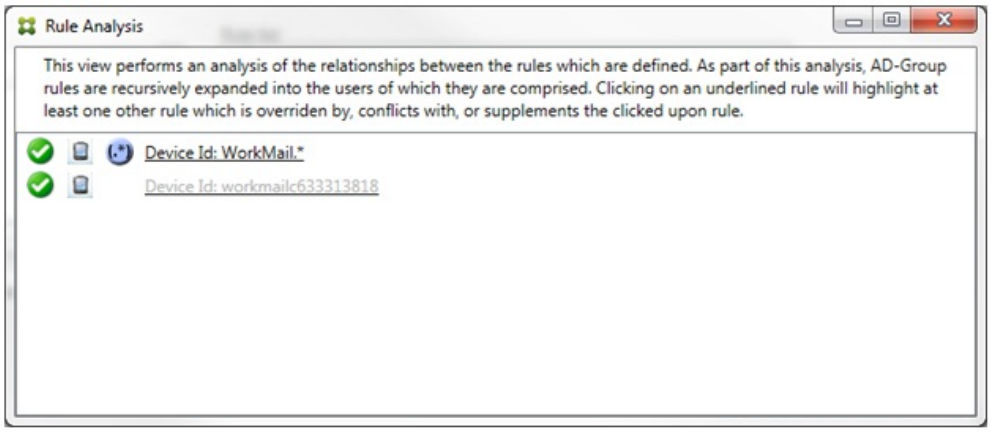
競合、上書き、または補足がない場合、［Rule Analysis］ダイアログボックスに下線付きのエントリは表示されません。どの

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。

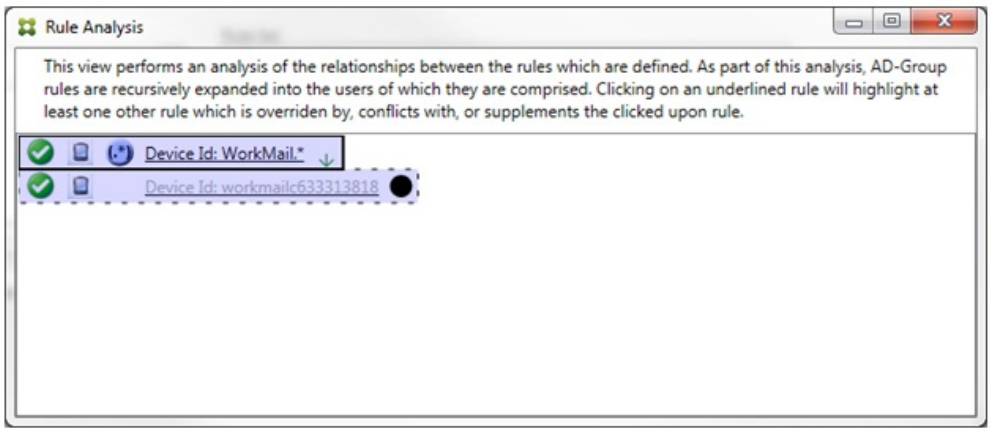
［Rule Analysis］ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。



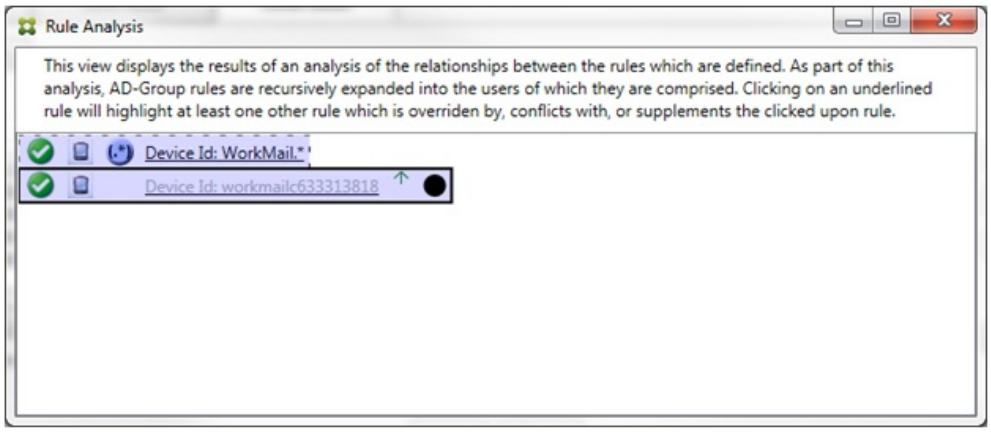
上書きが発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。1つまたは複数の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。上書きされた規則をクリックして、その規則を上書きした規則を確認できます。規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます。



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。

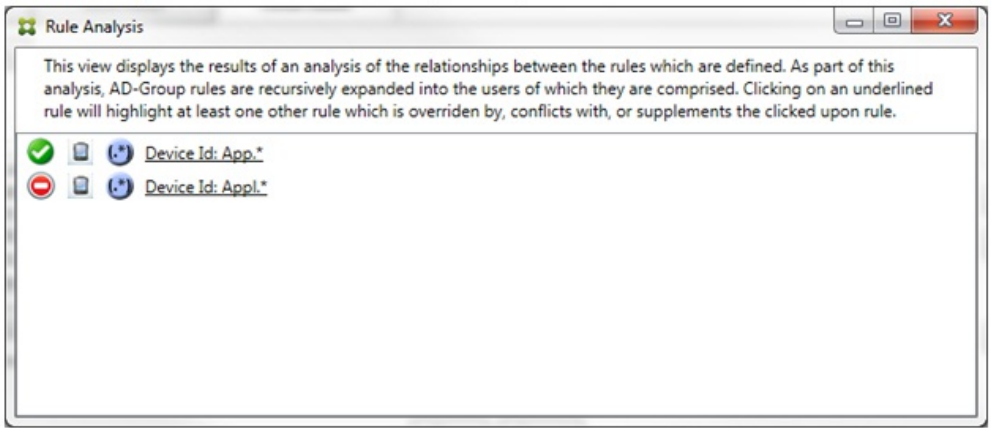


この例では、正規表現の規則WorkMail.*がプライマリ規則（実線の罫線で表示）で、通常の規則workmailc633313818が補助規則（破線の罫線で表示）です。補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります。

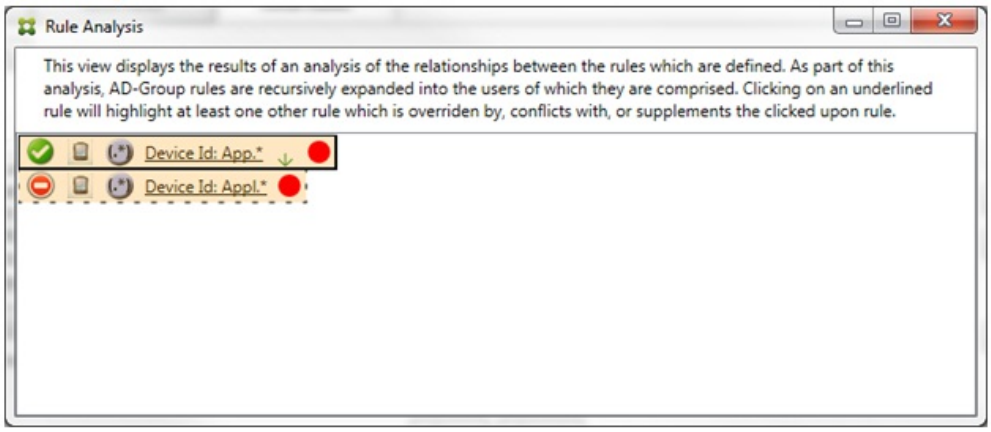


上記の例では、正規表現の規則WorkMail.*が補助規則（破線の罫線で表示）で、通常の規則workmailc633313818がプライマリ規則（実線の罫線で表示）です。このシンプルな例では、大きな違いはありません。より複雑な例については、このトピックで後述する複雑な式の例を参照してください。多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

競合が発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。競合している規則は赤色の点で示されます。相互に競合のみが発生している規則は、2つ以上の正規表現の規則が定義されている場合に限り発生します。ほかのすべての競合のシナリオでは、競合のみではなく、上書きも発生します。シンプルな例で説明すると、いずれかの規則をクリックする前は、次のようにダイアログボックスが表示されます。

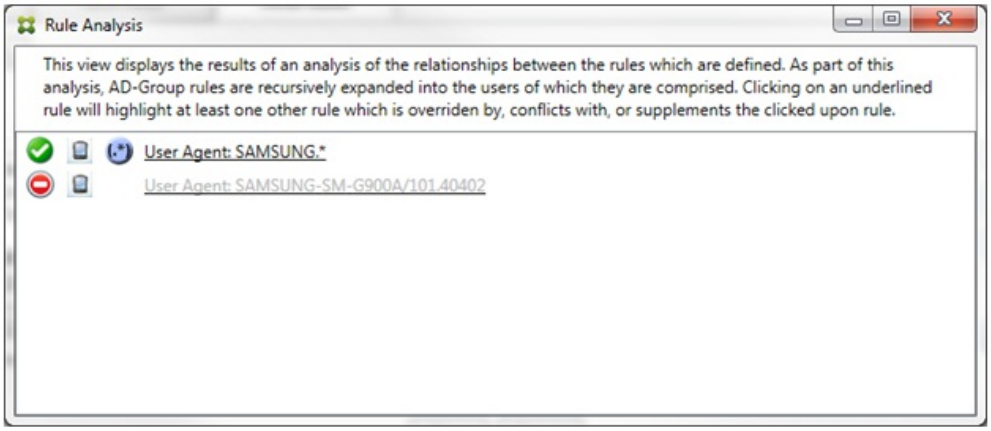


2つの正規表現の規則を確認すると、最初の規則で「App」がデバイスIDに含まれるすべてのデバイスを許可し、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスを拒否することがわかります。さらに、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは決して拒否されません。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



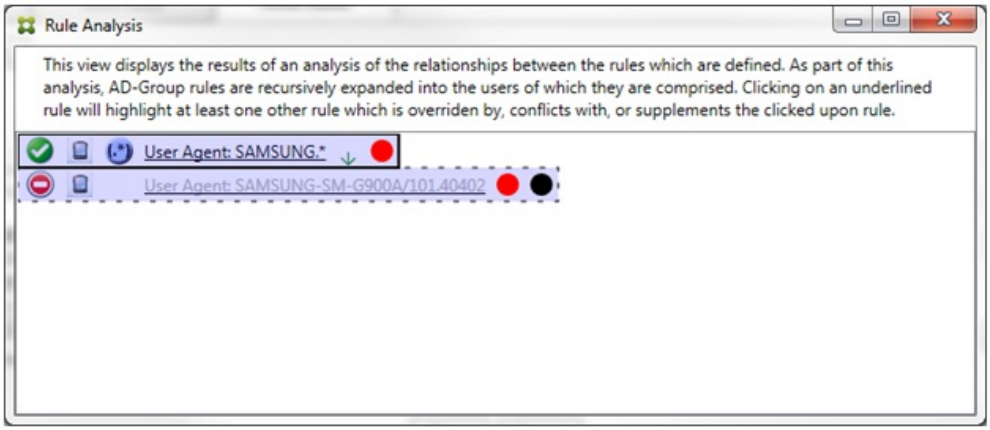
前述のシナリオでは、プライマリ規則（正規表現の規則App.*）と補助規則（正規表現の規則Appl.*）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

競合と上書きの両方を含むシナリオでは、プライマリ規則（正規表現の規則App.*）と補助規則（正規表現の規則Appl.*）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。



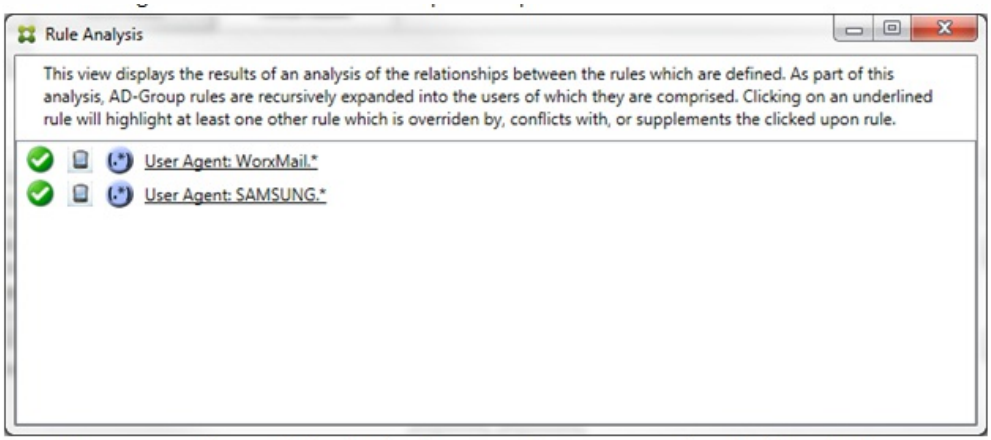
上記の例では、最初の規則（正規表現の規則SAMSUNG.*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。2つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

正規表現の規則をクリックすると、ダイアログボックスの表示は次のようになります。

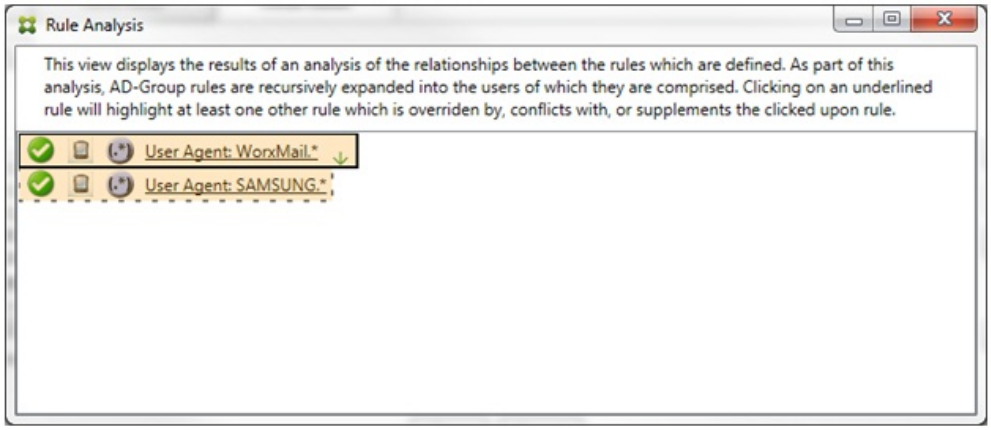


プライマリ規則（正規表現の規則SAMSUNG.*）の末尾には赤色の点が付けられて、アクセス状態が1つまたは複数の補助規則と競合していることが示されます。補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には、アクセス状態がプライマリ規則と競合していることを示す赤色の点に加えて、その規則が上書きされて非アクティブであることを示す黒点が付けられます。

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。



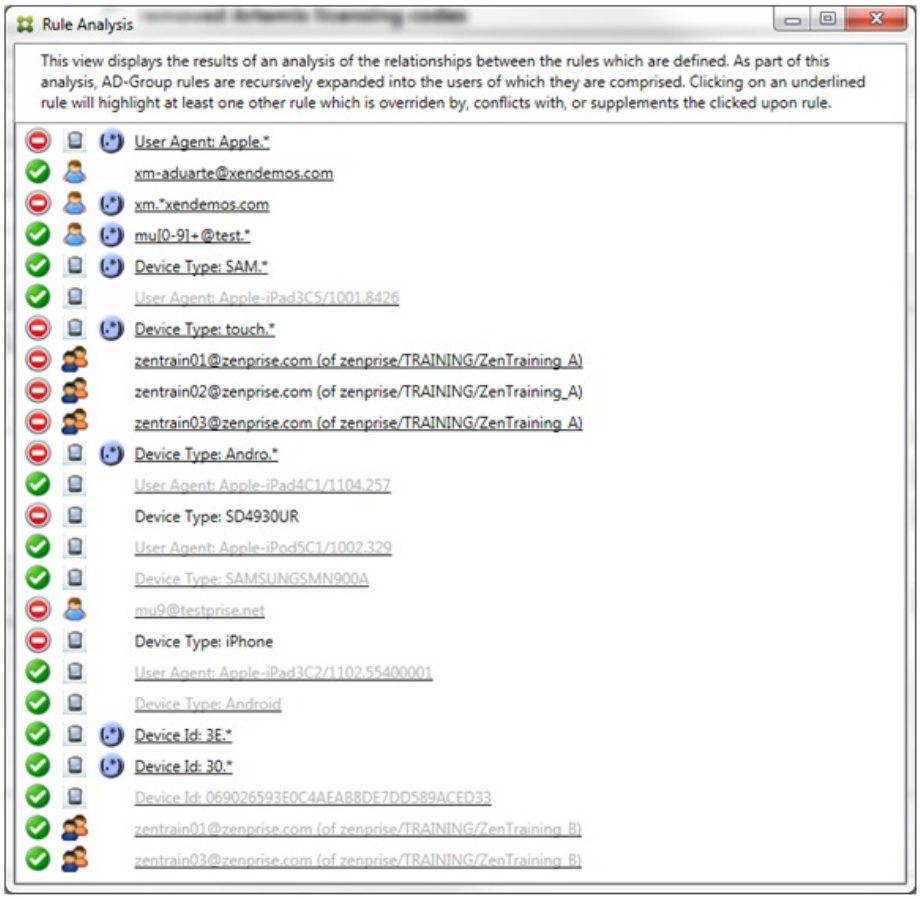
目視で確認すると、両方の規則が正規表現の規則で、両方ともXenMobile Mail Managerの［ActiveSync device ID］フィールドに適用されていることが容易にわかります。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



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

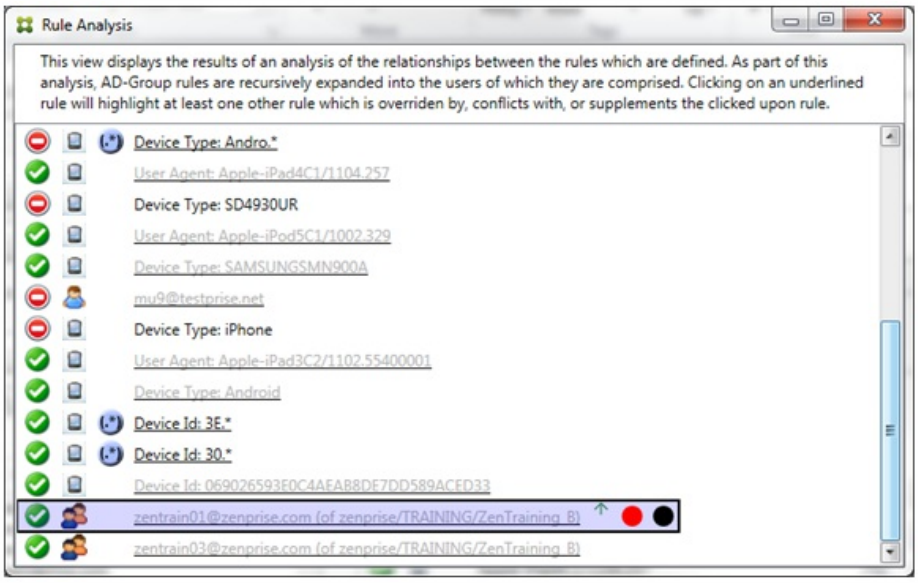
発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。次の図では、ほとんどのアイテムに下線が付けられています。多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。同様に、(.*)アイコンで示される多数の正規表現の規則も一覧に含まれています。



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。

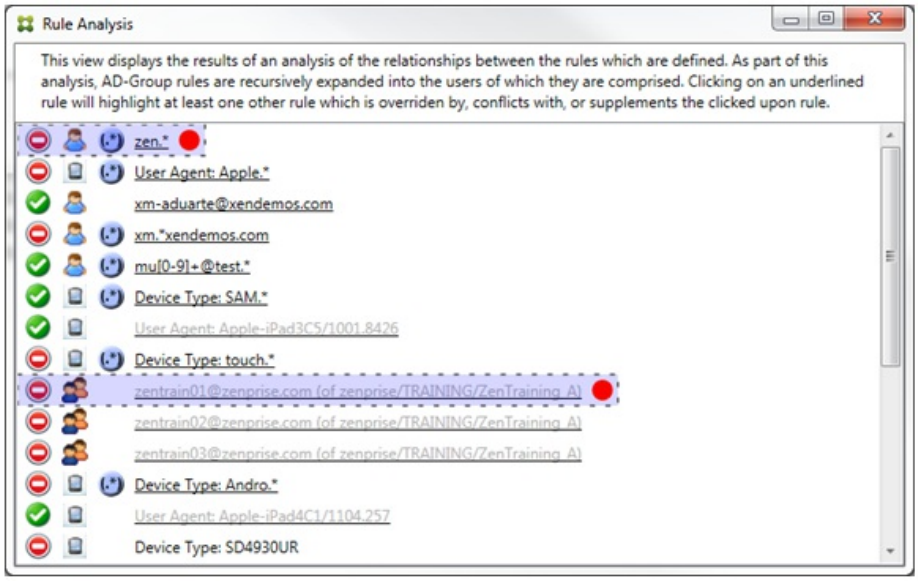


このプライマリ規則（zentrain01@zenprise.comがメンバーとして属するADグループ規則zenprise/TRAINING/ZenTraining B）

には、次の特性があります。

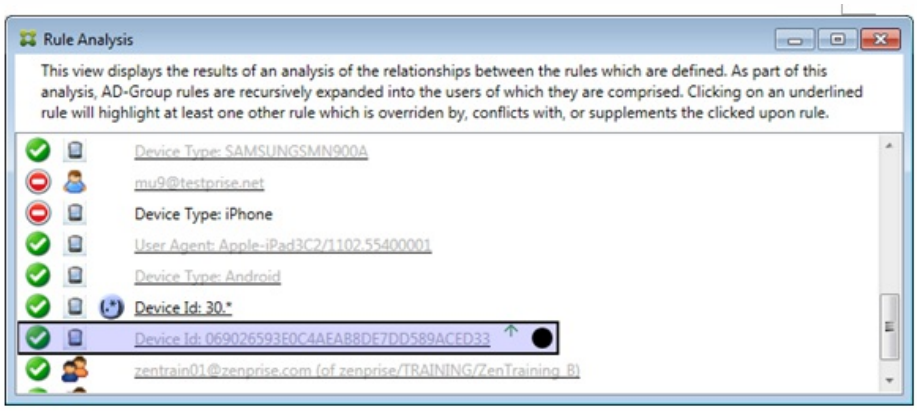
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（すべての補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、1つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます。



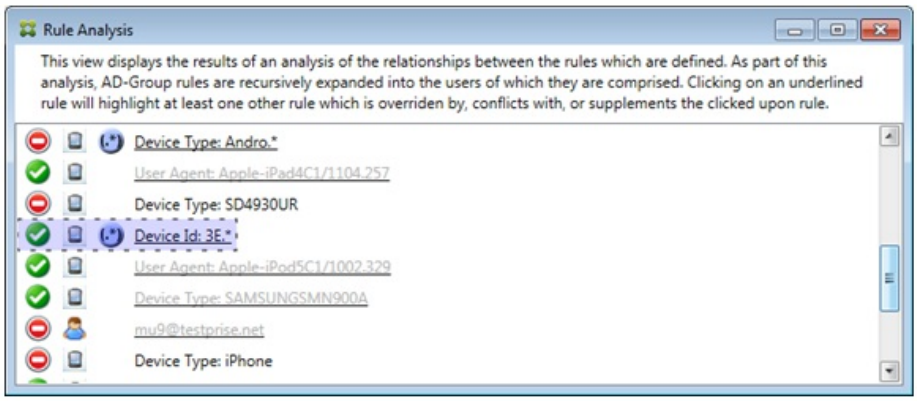
この場合、プライマリ規則を上書きする2つの補助規則（正規表現の規則zen.*と通常の規則zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)）があります。後者の補助規則の場合、Active Directoryグループ規則ZenTraining Aにユーザーzentrain01@zenprise.comが含まれる一方で、Active Directoryグループ規則ZenTraining Bにもユーザーzentrain01@zenprise.comが含まれることになります。ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、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。

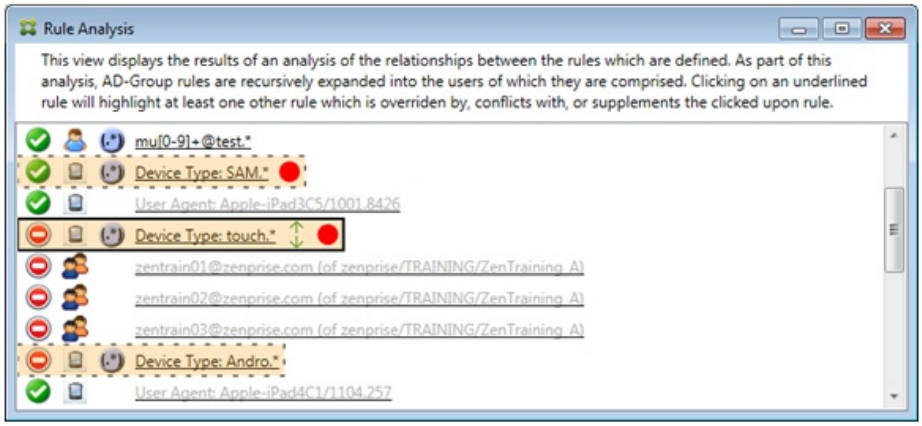


この場合、単一の補助規則（正規表現のActiveSyncデバイスIDの規則3E.*）がプライマリ規則を上書きします。正規表現3E.*が069026593E0C4AEAB8DE7DD589ACED33に一致するので、プライマリ規則は評価されません。

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。



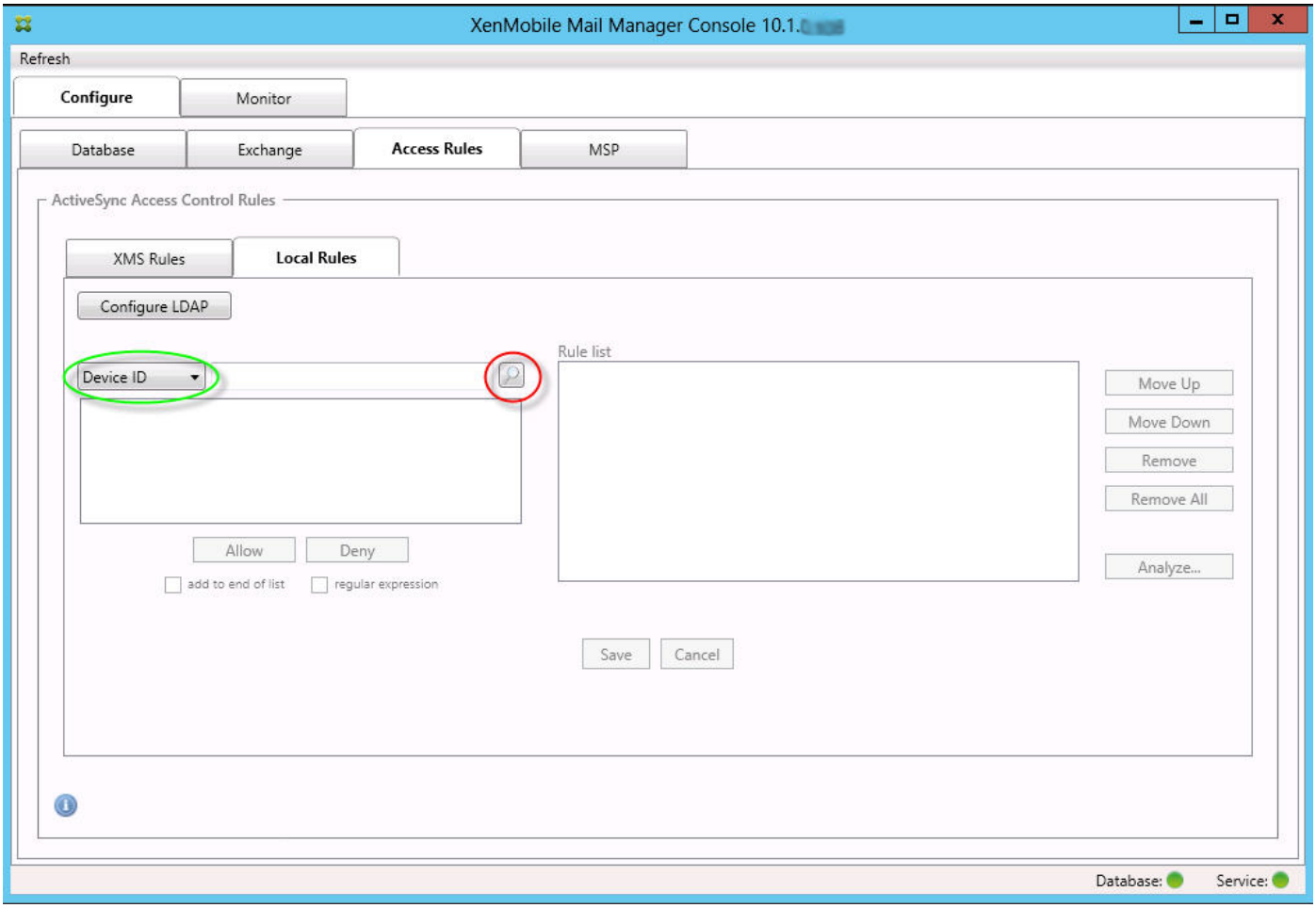
規則の高度な分析方法

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。

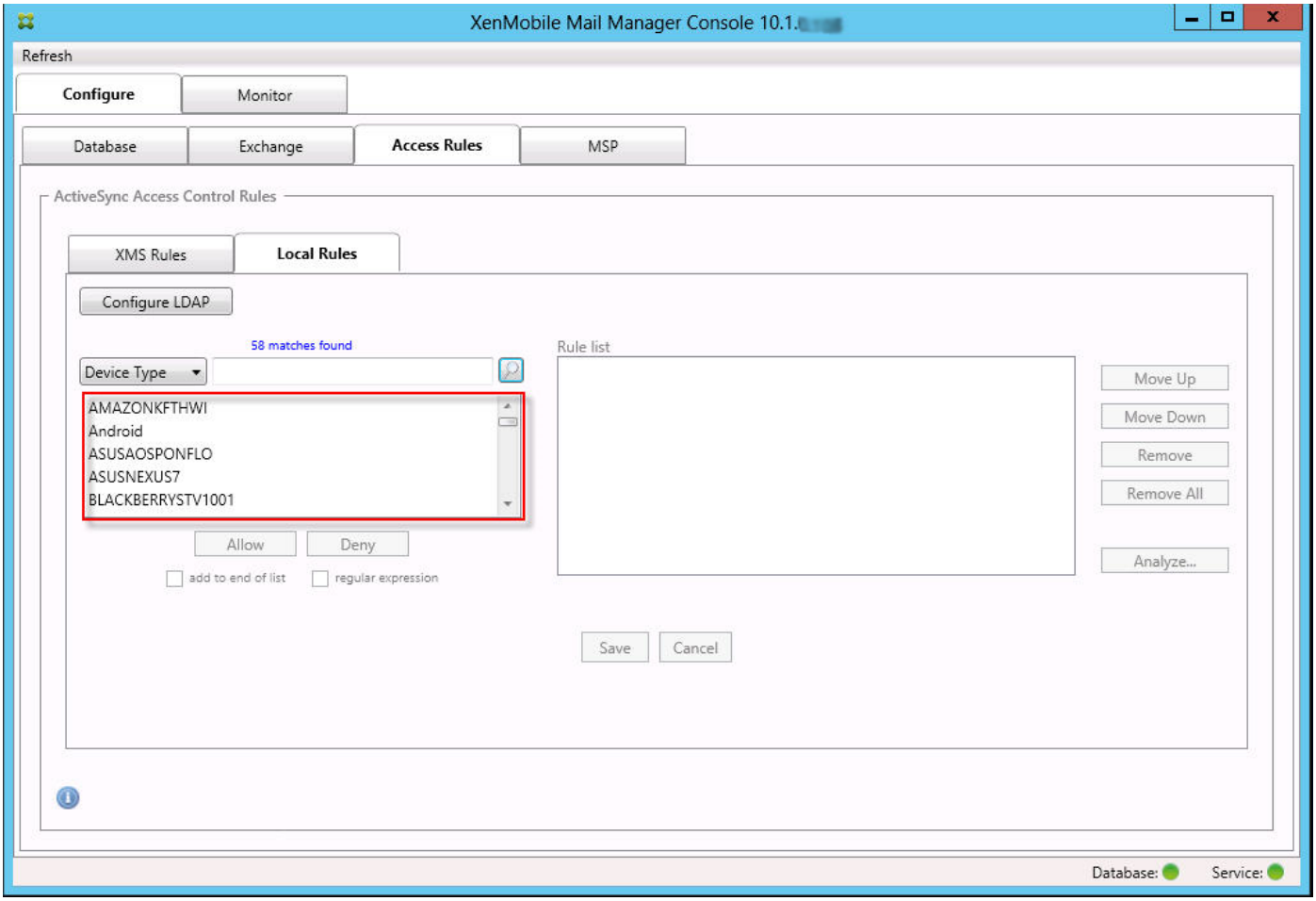
この例では、規則の関係に含まれる上書きされた規則が示されています。この規則は、通常のActiveSyncデバイスの種類の規則Androidです。この規則は上書きされ（淡色のフォントで示され、横に黒点が付けられています）、プライマリ規則（正規表現のActiveSyncデバイスの種類の規則Andro.*。この規則は、クリック前は補助規則でした）のアクセスと競合しています。前述の例では、その時点でのプライマリ規則（正規表現のActiveSyncデバイスの種類の規則touch.*）の観点からは関係しなかったので、通常のActiveSyncデバイスの種類の規則Androidは補助規則として表示されていませんでした。

通常の式のローカル規則を構成するには

1. ［Access Rules］タブをクリックします。

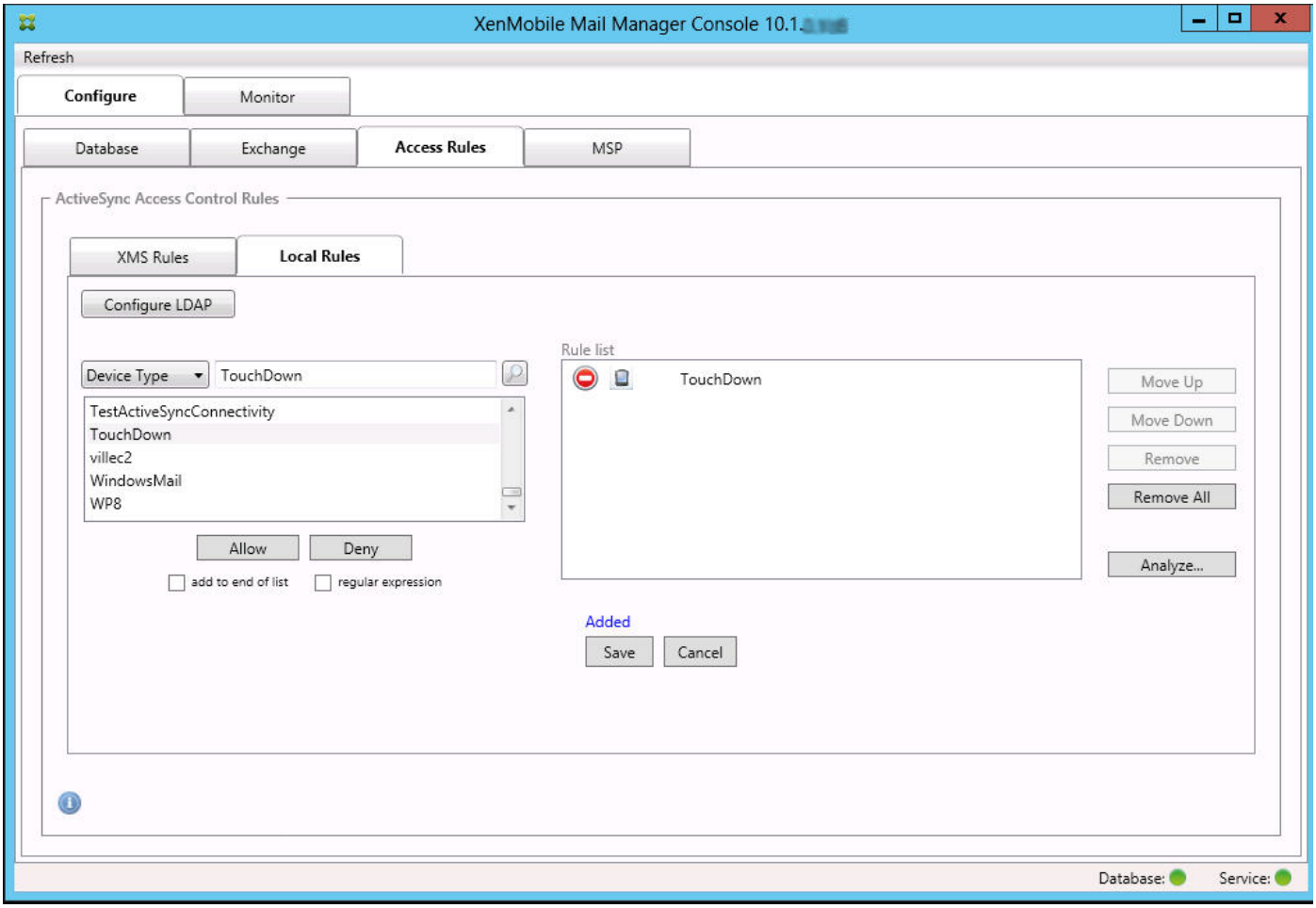


2. ［Device ID］一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 表示されたリストボックスでいずれかのアイテムをクリックして、次のいずれかのオプションをクリックします。
   - 許可を選ぶと、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。
   - 禁止を選ぶと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。

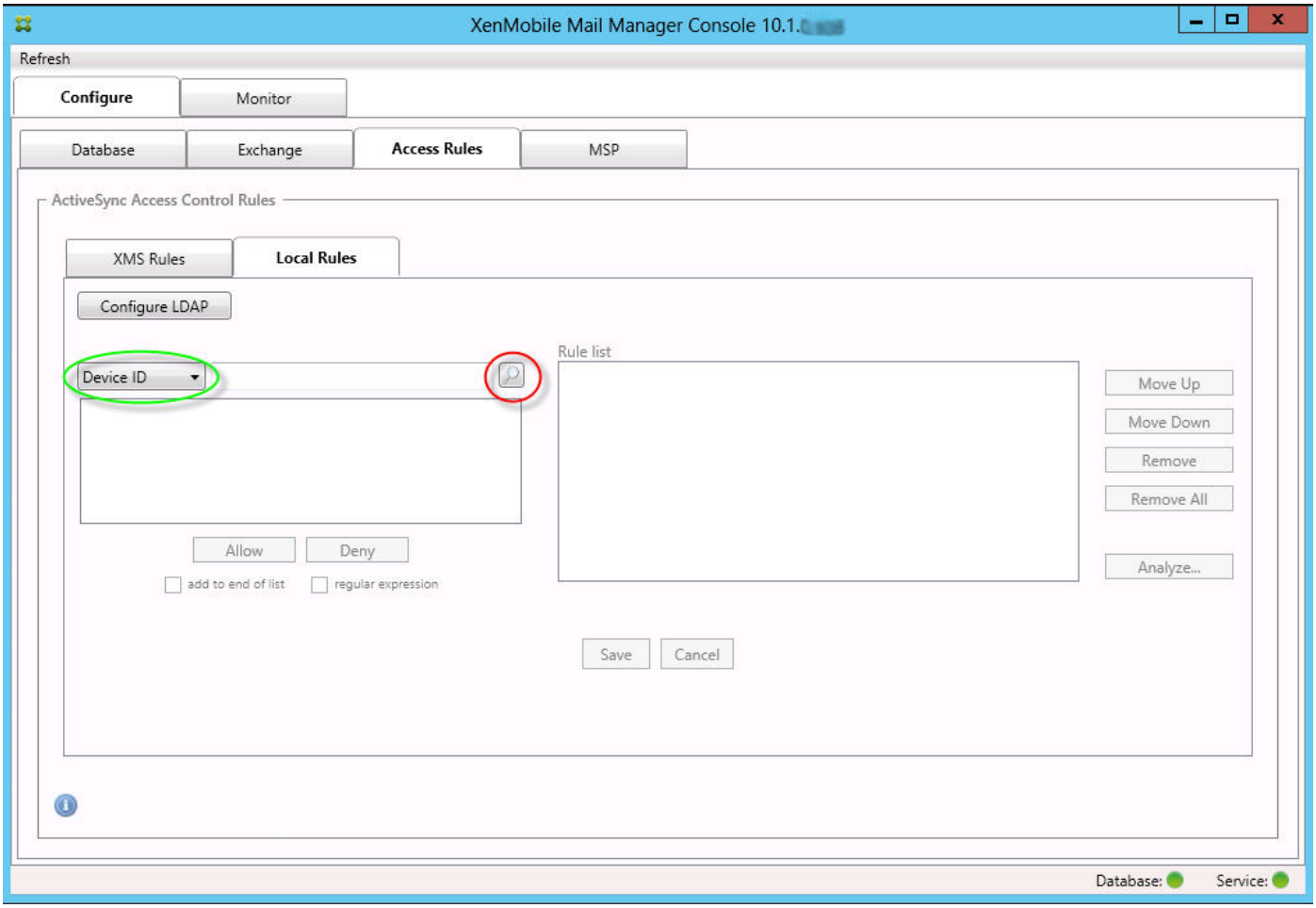


正規表現を追加するには

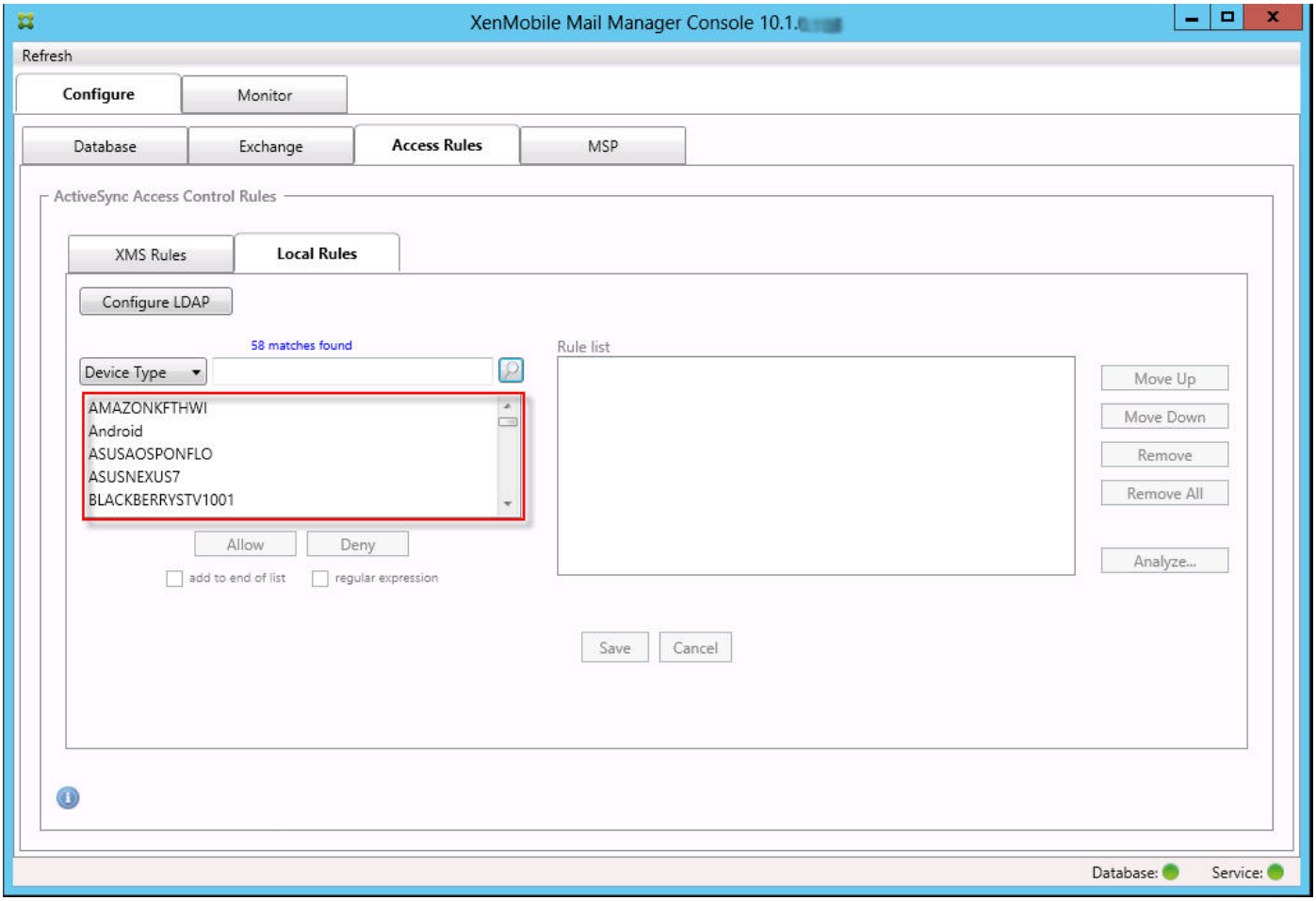
正規表現のローカル規則は、横に表示されるアイコン（(.*)）で識別できます。正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

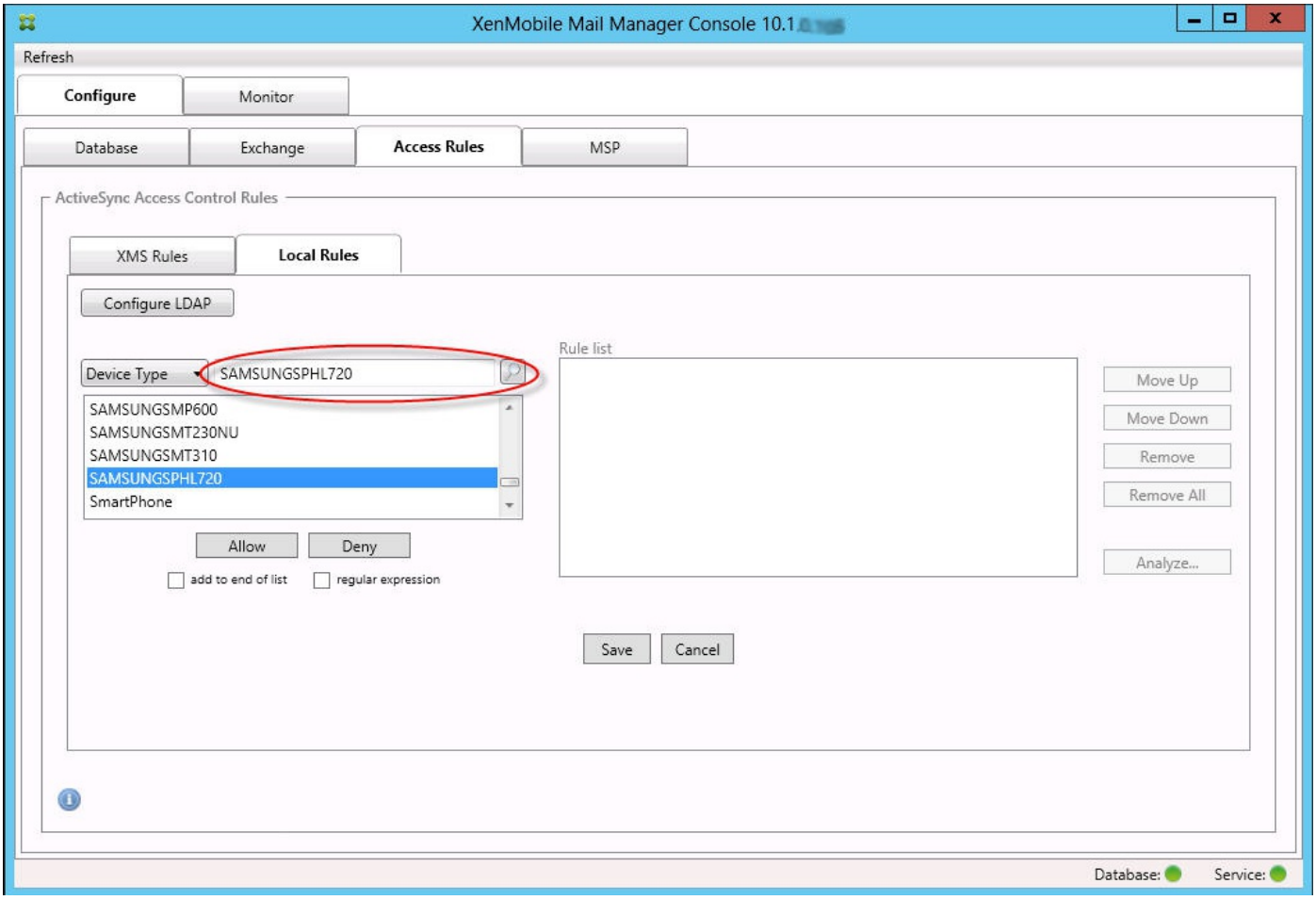
1. ［Access Rules］タブをクリックします。



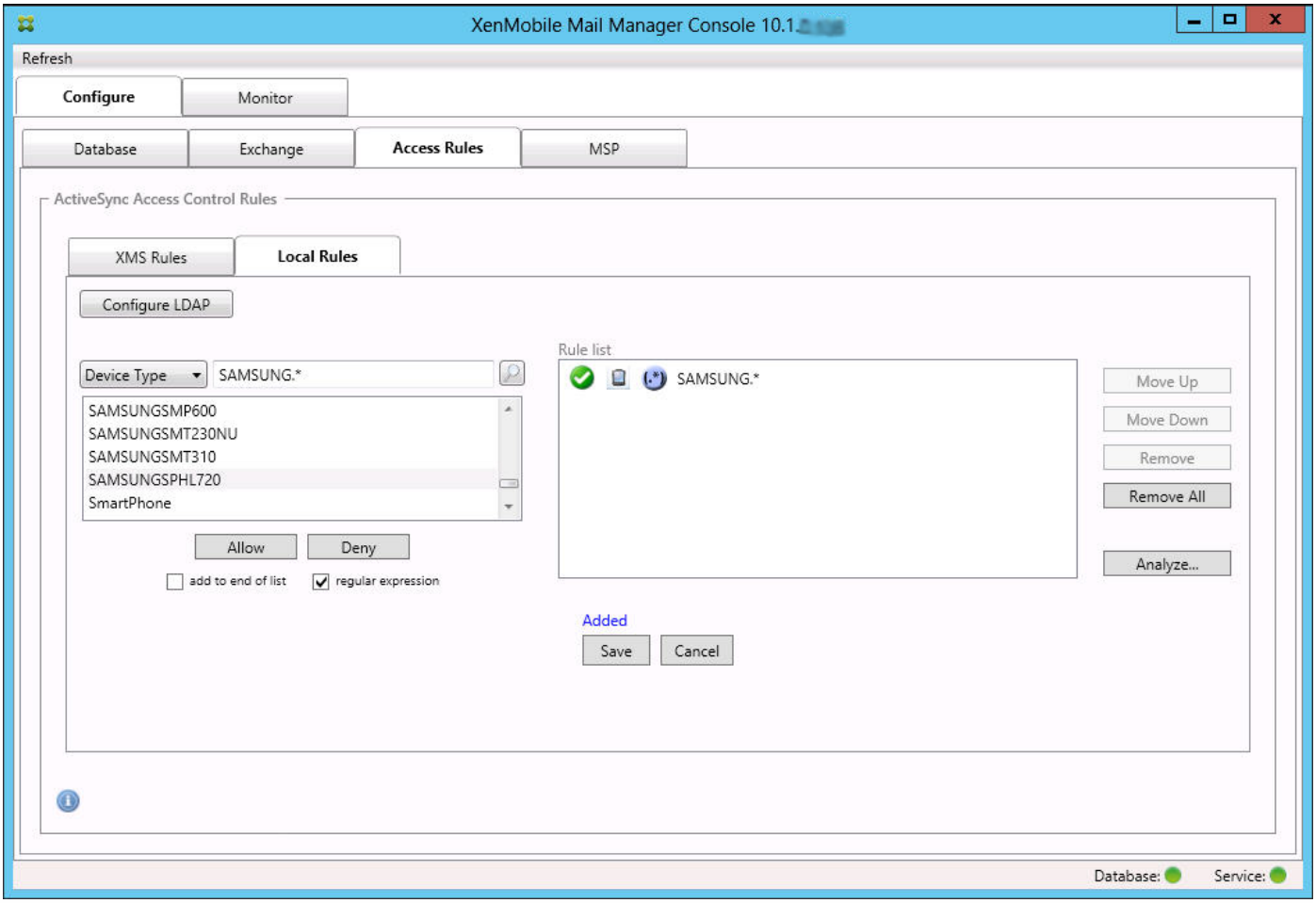
2. ［Device ID］一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 結果一覧でいずれかのアイテムをクリックします。この例では、SAMSUNGSPHL720が選択され、[Device Type]に隣接するテキストボックスに表示されています。

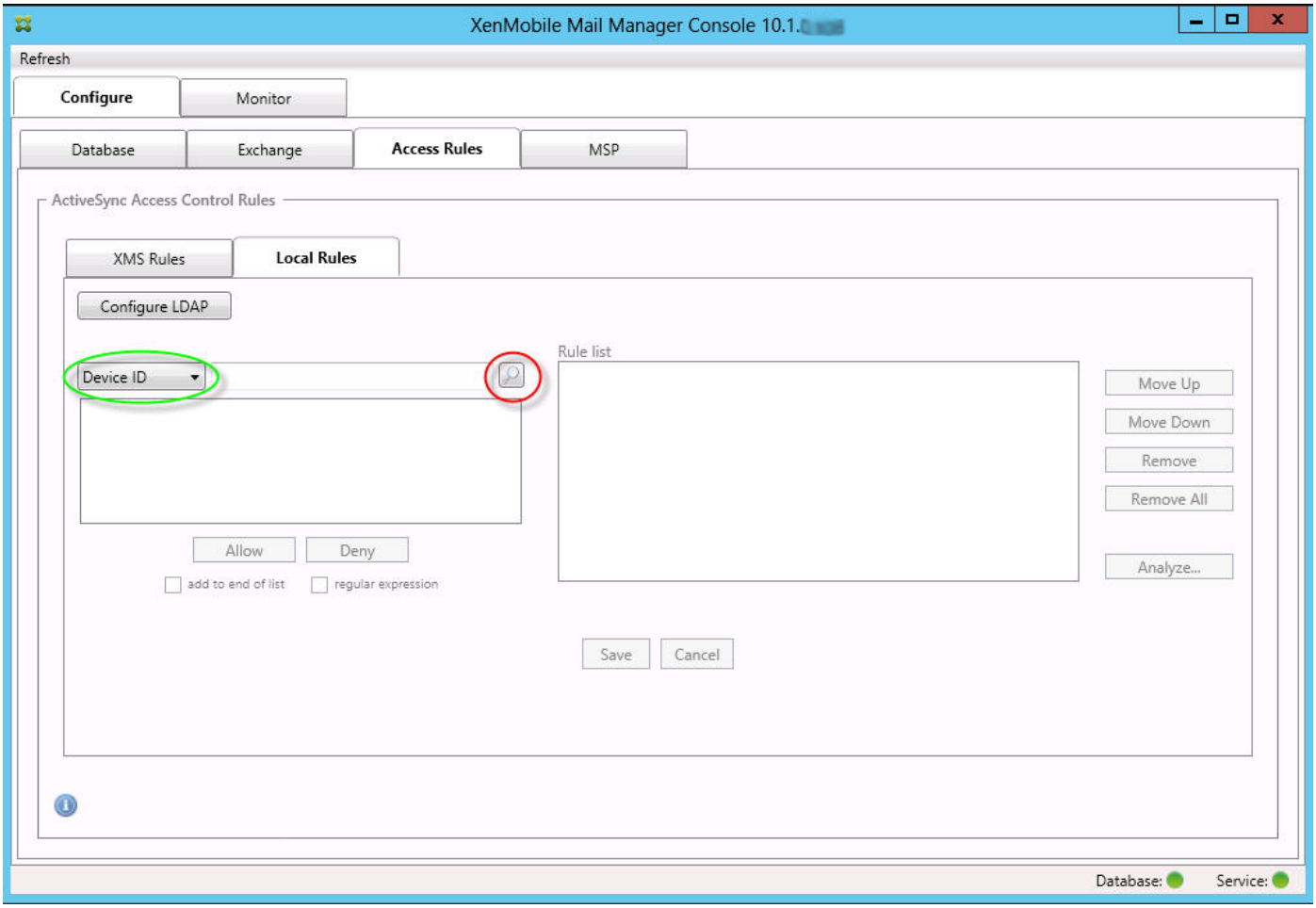


5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。
   1. 選択済みアイテムのテキストボックス内をクリックします。
   2. SAMSUNGSPHL720からSAMSUNG.*にテキストを変更します。
   3. ［regular expression］チェックボックスをオンにします。
   4. ［Allow］をクリックします。

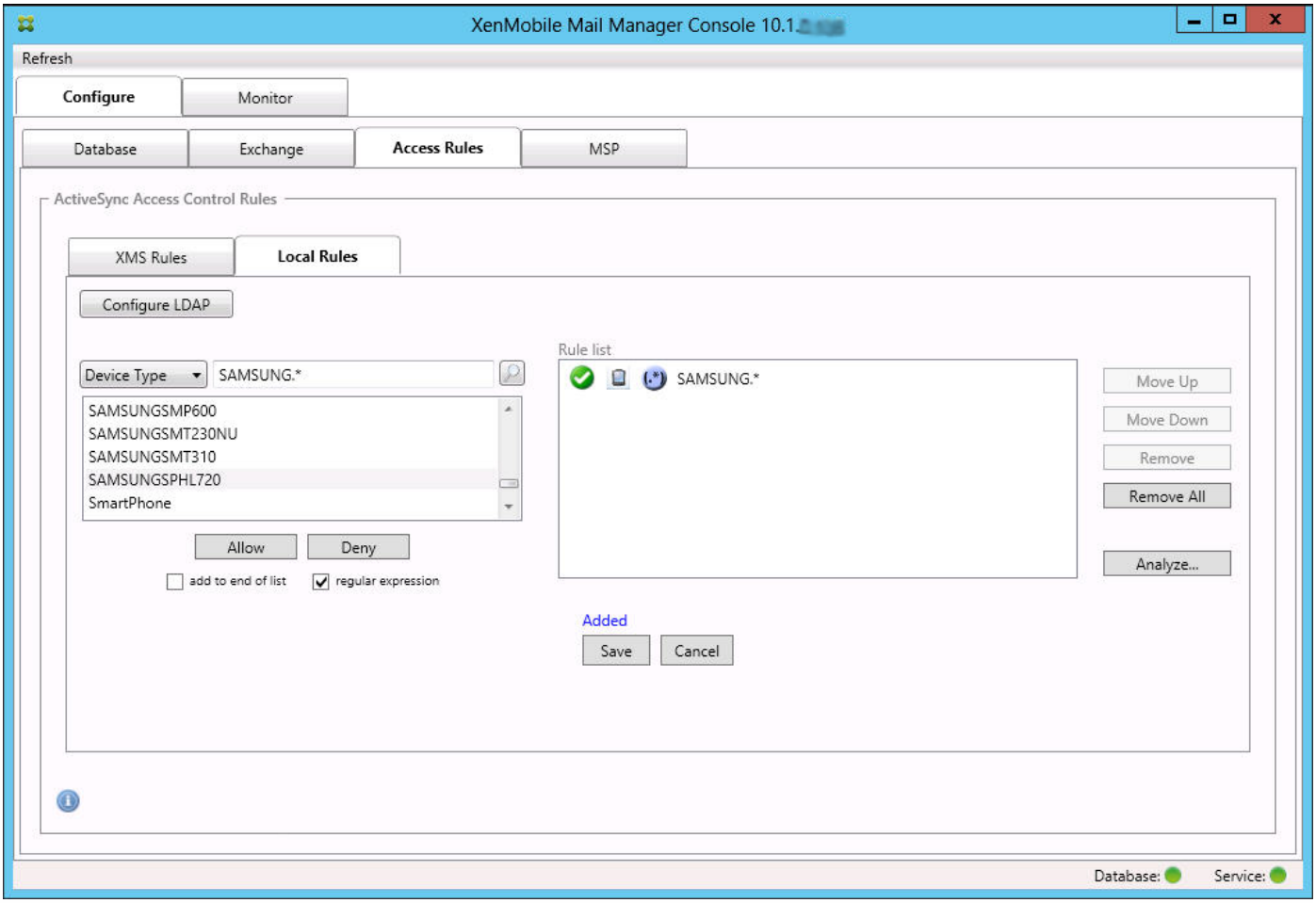


アクセス規則を作成するには

1. ［Local Rules］タブをクリックします。
2. 正規表現を入力するには、［Device ID］一覧と選択済みアイテムのテキストボックスの両方を使用する必要があります。



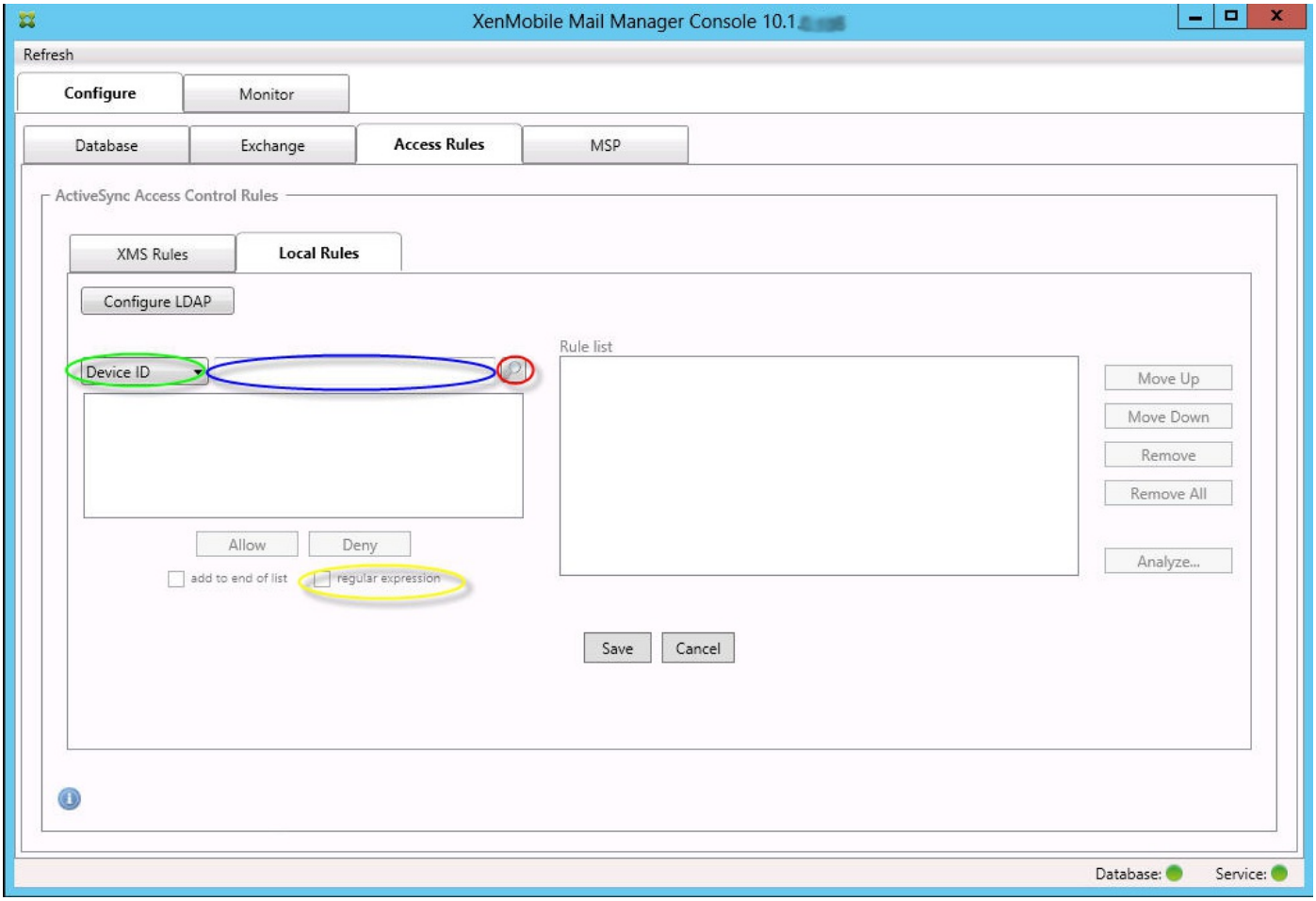
3. 照合するフィールドを選択します。この例では［Device Type］を使用します。
4. 正規表現を入力します。この例ではsamsung.*を使用します。
5. ［regular expression］チェックボックスをオンにして、［Allow］または［Deny］をクリックします。この例では、［Allow］を選択し、最終結果は次のようになります。



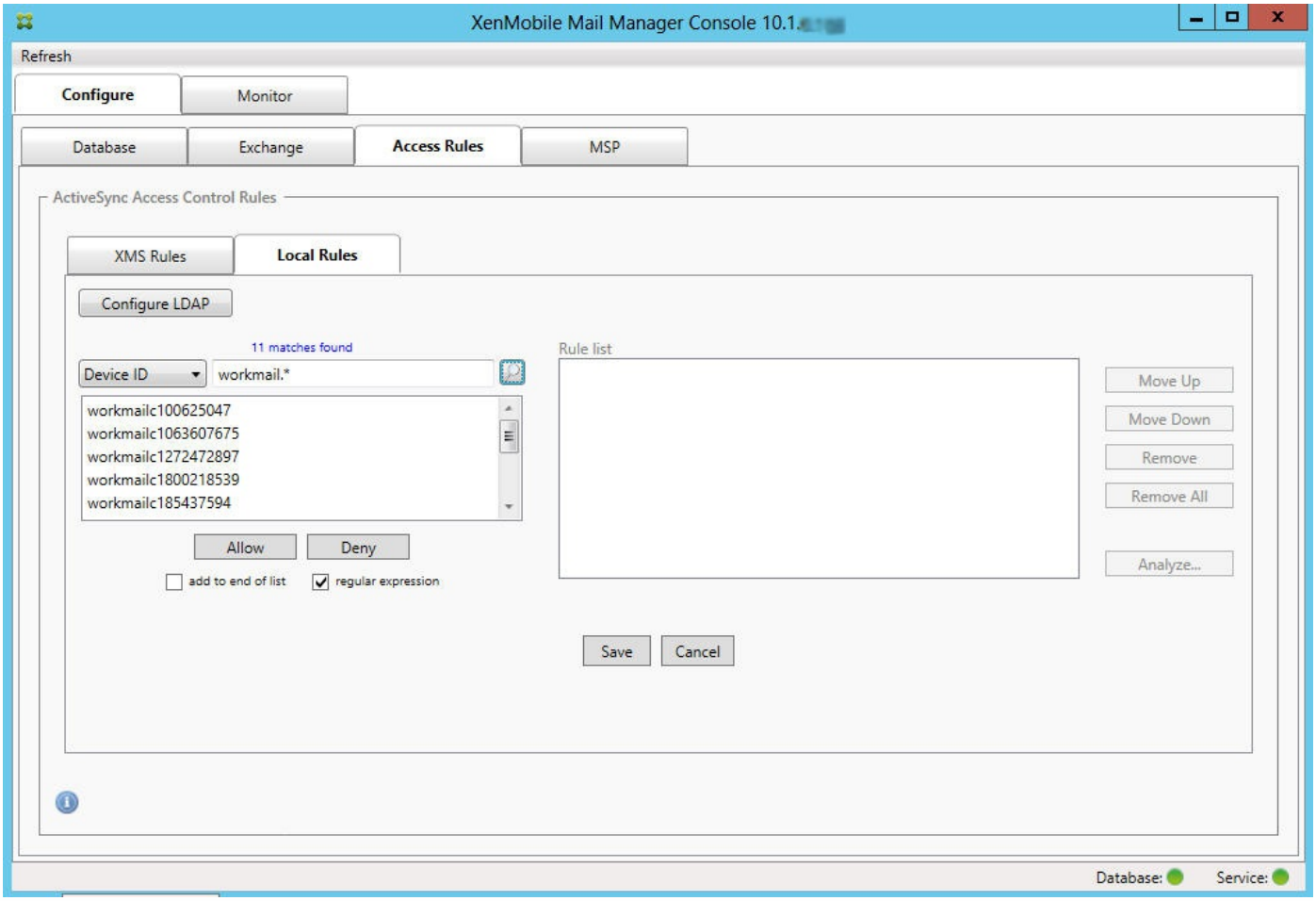
デバイスを検出するには

［regular expression］チェックボックスをオンにして、特定の式に一致する特定のデバイスの検索を実行できます。この機能は、メジャースナップショットが正常に完了している場合にのみ利用できます。正規表現の規則を使用しない場合でも、この機能を使用できます。たとえば、ActiveSyncデバイスIDにテキスト「workmail」が含まれるすべてのデバイスを検出するとします。これを行うには、以下の手順に従います。

1. ［Access Rules］タブをクリックします。
2. デバイスの照合フィールドセレクターが［Device ID］（デフォルト）に設定されていることを確認します。



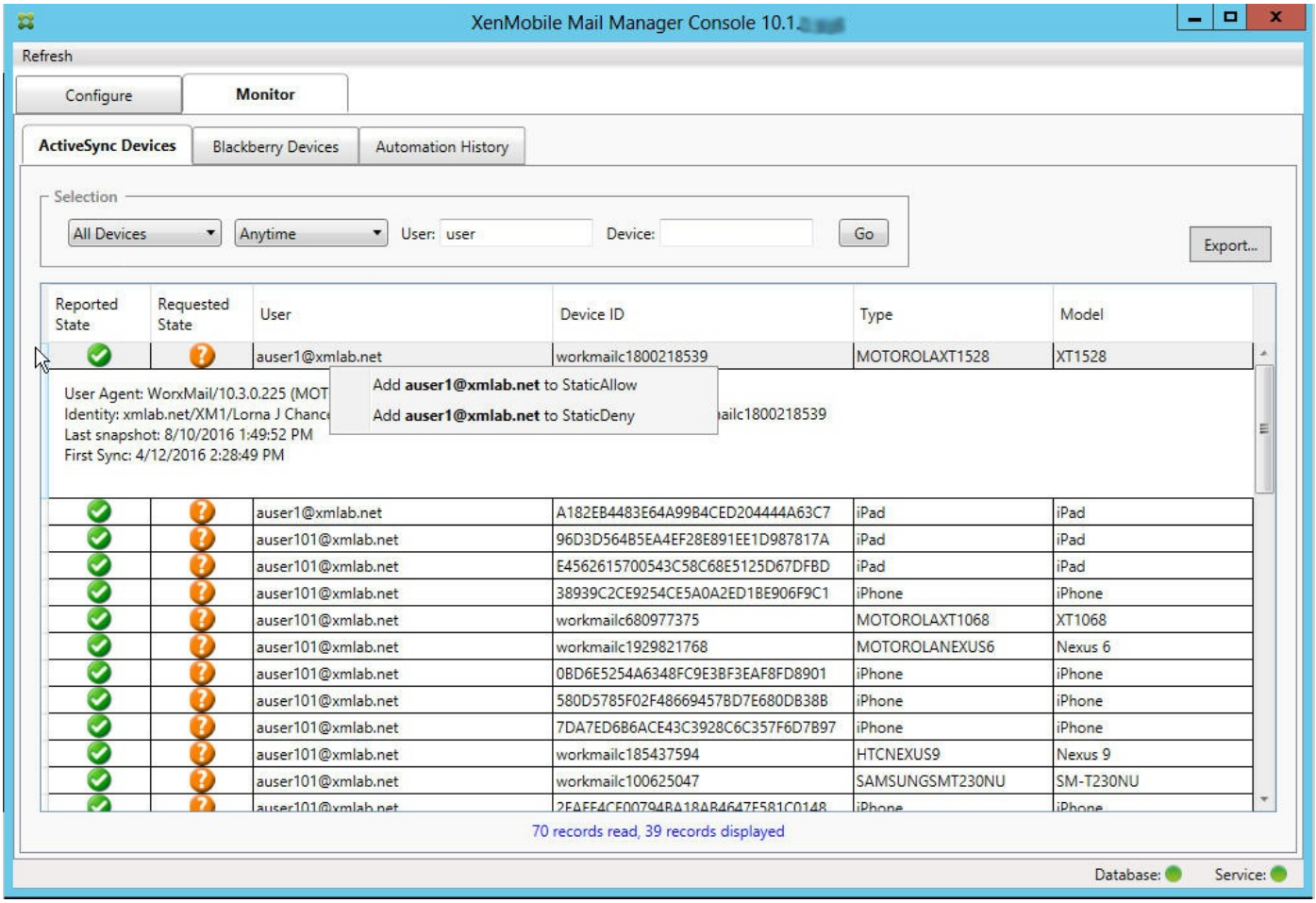
3. 選択済みアイテムのテキストボックス内（上記の図に青色で示されています）をクリックし、「workmail.*」と入力します。
4. ［regular expression］チェックボックスをオンにして、虫眼鏡アイコンをクリックし、次の図に示すように一致を表示します。



個々のユーザー、デバイス、またはデバイスの種類を静的規則に追加するには

［ActiveSync Devices］タブで、ユーザー、デバイスID、またはデバイスの種類に基づく静的規則を追加できます。

1. ［ActiveSync Devices］タブをクリックします。
2. 一覧で、ユーザー、デバイス、またはデバイスの種類を右クリックして、選択内容を許可するか、または拒否するかを選択します。
   次の図は、user1を選択したときの許可/拒否オプションを示しています。



デバイス監視

Feb 27, 2017

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

Feb 27, 2017

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

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。

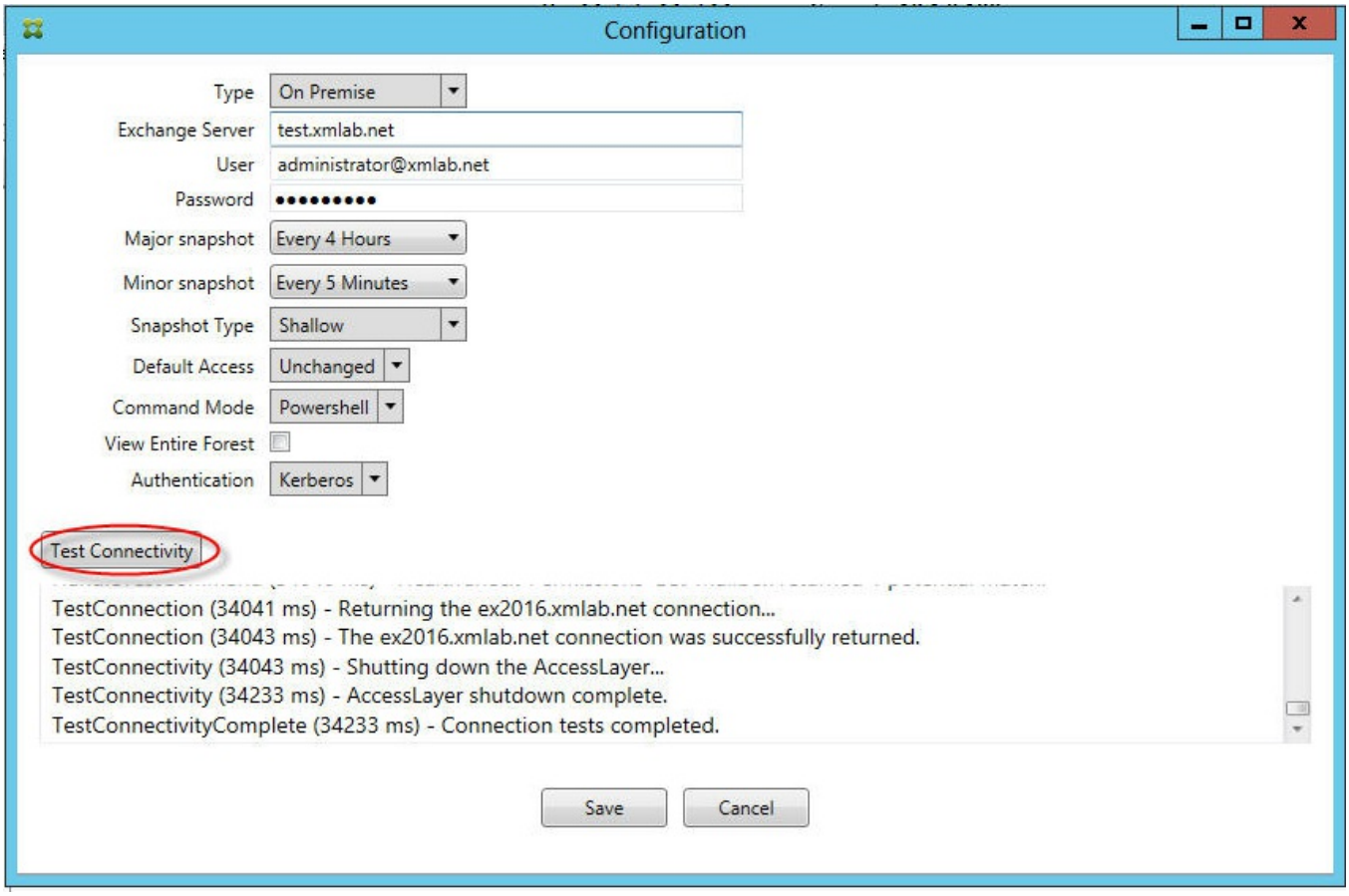
- XenMobile Mail ManagerサービスがSQL Serverにアクセスできない。これは、次の問題が原因である可能性があります。
  - SQL Serverサービスが実行されていない。
  - 認証に失敗した。
    ［Windows Integrated authentication］が構成されている場合、XenMobile Mail Managerサービスのユーザーアカウントは、許可されたSQLログオンである必要があります。XenMobile Mail Managerサービスのアカウントは、デフォルトではローカルシステムですが、ローカルの管理者権限を持つ任意のアカウントに変更できます。［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。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。



トラブルシューティングツール

Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

トラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

XenMobile NetScaler Connector

Feb 27, 2017

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、「Reference Architecture for On-Premises Deployments」についてのセクションを参照してください。

高度な設定

Sep 15, 2017

オンプレミスXenMobileのActive Directoryとのやり取り

Siddartha Vuppala , | Sep 15, 2017

この記事では、XenMobileサーバーとActive Directoryのやり取りについて説明します。XenMobileサーバーとActive Directoryのやり取りは、インラインとバックグラウンドの両方で行われます。以下のセクションでは、Active Directoryとのやり取りを伴うインライン操作およびバックグラウンド操作の詳細について説明します。

> ## 注意
>
> この記事ではやり取りの概要のみを示し、細かい詳細については扱いません。XenMobileコンソールでのActive DirectoryとLDAPの構成方法について詳しくは、「ドメインまたはドメイン+セキュリティトークン認証」を参照してください。

インラインでのやり取り

XenMobileサーバーは、管理者が構成するLDAP設定を使用してActive Directoryとの通信を行います。この設定により、ユーザーとグループに関する情報が取得されます。XenMobileサーバーとActive Directory間のやり取りが生じる操作を次に示します。

1. **LDAP構成。**Active Directory自体を構成するため、Active Directoryとのやり取りが行われます。XenMobileサーバーはActive Directoryで構成情報の認証を行うことで、構成情報の検証を試みます。この認証は、インターネットプロトコル、ポート、および指定のサービスアカウントの資格情報を使用して行われます。バインドが成功すれば、接続は適切に構成されています。

2. **グループベースのやり取り。**

   a. 役割ベースのアクセス制御（RBAC）時およびデリバリーグループの定義の作成時における1つ以上のグループの検索。XenMobileサーバーの管理者が、XenMobileコンソールで検索テキストを入力します。XenMobileサーバーにより、指定した文字列の一部が含まれるすべてのグループについて選択したドメインが検索されます。次に、XenMobileサーバーは検索で見つかったグループのobjectGUID属性、sAMAccountName属性、識別名属性を取得します。

   > ## 注意
   >
   > この情報は、XenMobileサーバーのデータベースには格納されません。

   b. RBACおよび展開グループの定義の追加または更新。XenMobileサーバーの管理者が上記の検索結果に基づいて目的のActive Directoryグループを選択し、展開グループの定義に追加します。XenMobileサーバーにより、Active Directory内で指定したグループが1度に1つずつ検索されます。XenMobileサーバーはobjectGUID属性を検索し、メンバーシップ情報を含む選択した属性を取得します。グループのメンバーシップ情報により、取得したグループとXenMobileサーバーデータベースの既存のユーザーまたはグループ間のメンバーシップが特定されます。グループのメンバーシップを変更すると、影響を受けるユーザーメンバーに関わるRBACおよび展開グループが確認され、ユーザーの権利割り当てが行われます。

   > ## 注意

展開グループの定義を変更すると、影響を受けるユーザーのアプリまたはポリシーの使用権が変更される場合があります。

c.**ワンタイムPIN（OTP）による招待**。XenMobileサーバー管理者が、XenMobileサーバーデータベースに存在するActive Directoryグループの一覧からグループを選択します。このグループのすべてのユーザーが、直接的および間接的にActive Directoryから取得されます。前の手順で特定されたユーザーに対して、OTP招待状が送られます。

注意

上記3つのやり取りは、XenMobileサーバーの構成変更によりグループベースのやり取りが開始されることを示しています。構成に変更がない場合、これらのやり取りではActive Directoryとの通信は行われません。また、定期的にバックグラウンドジョブでグループ側の変更を取得する必要もありません。

3. **ユーザーベースのやり取り。**

a. ユーザー認証。ユーザー認証のワークフローでは、Active Directoryと2種類のやり取りが行われます。

- 指定した資格情報によるユーザーの認証
- XenMobileサーバーデータベースへの選択したユーザー属性（objectGUID、識別名、sAMAccountName、グループのダイレクトメンバーシップなど）の追加または更新。グループのメンバーシップを変更すると、アプリ、ポリシー、アクセス資格の再評価が行われます。

ユーザーは、デバイスとXenMobileサーバーコンソールのどちらからでも認証を行うことができます。どちらの場合でも、Active Directoryとのやり取りの動作は同じです。

b. App Storeへのアクセスおよび更新。ストアを更新すると、ダイレクトグループメンバーシップを含むユーザー属性が更新されます。この処理により、ユーザー資格の再評価が可能になります。

c. デバイスのチェックイン。管理者は、定期的にXenMobileコンソールでデバイスのチェックインを構成します。デバイスのチェックインが行われるたびに、ダイレクトグループメンバーシップを含む対応するユーザー属性が更新されます。こうしたチェックインにより、ユーザー資格の再評価が可能になります。

d. グループ単位でのOTPによる招待。XenMobileサーバー管理者が、XenMobileサーバーデータベースに存在するActive Directoryグループの一覧からグループを選択します。ユーザーメンバーが直接的および間接的（入れ子構造の場合）にActive Directoryから取得され、XenMobileサーバーデータベースに保存されます。前の手順で特定されたユーザーメンバーに対して、OTP招待状が送られます。

e. ユーザー単位でのOTPによる招待。管理者が、XenMobileコンソールで検索テキストを入力します。XenMobileサーバーによりActive Directoryに対する紹介が行われ、入力したテキストに一致するユーザーレコードが返されます。次に、管理者がOTP招待状の送信先となるユーザーを選択します。ユーザーへの招待状の送信前に、XenMobileサーバーがActive Directoryからユーザーの詳細を取得してデータベースの該当する情報を更新します。

バックグラウンドでのやり取り

Active Directoryとのインライン通信で1つわかることは、XenMobileサーバーの構成が変更されるとグループベースのやり取りが行われるということです。構成に変更がない場合、グループについてActive Directoryとの通信は行われません。

こうしたやり取りではバックグラウンドジョブにより、Active Directoryと定期的に同期して変更内容を対象のグループに反映する必要があります。

Active Directoryをのやり取りを行うバックグラウンドジョブを次に示します。

1. **グループ同期ジョブ**。このジョブの目的は、対象のグループについて一度に1グループずつActive Directoryに照会し、識別名属性またはsAMAccountName属性の変更がないか確認することです。このActive Directoryに対する検索クエリでは、対象グループのobjectGUIDを使用して識別名属性とsAMAccountName属性の現在の値を取得します。対象グループの識別名またはsAMAccountNameの値の変更結果で、データベースが更新されます。

   > **注意**
   >
   > このジョブでは、ユーザーのグループメンバーシップ情報は更新されません。

2. **入れ子グループの同期ジョブ**。このジョブでは、対象グループの入れ子構造の変更内容が反映されます。XenMobileサーバーでは、対象グループの直接メンバーと間接メンバーの両方が資格を得ることができます。ユーザーのダイレクトメンバーシップは、ユーザーベースのインラインでのやり取りの際に更新されます。このジョブはバックグラウンドで実行され、間接メンバーシップを追跡します。間接メンバーシップとは、対象グループのメンバーであるグループにユーザーが属している状態を指します。

   このジョブでは、XenMobileサーバーデータベースからActive Directoryグループのリストを取得します。Active Directoryのグループは、展開グループかRBAC定義のどちらかに含まれます。このリストの各グループについて、XenMobileサーバーがグループのメンバーを取得します。グループのメンバーは、ユーザーとグループの両方を表す識別名をリスト化したものです。XenMobileサーバーはActive Directoryに対して別のクエリを実行し、対象グループのユーザーメンバーのみを取得します。これら2つのリストの差を取ると、対象グループのグループメンバーのみが残ります。メンバーグループへの変更結果がデータベースに反映されます。階層内のすべてのグループについて、同じ手順が繰り返されます。

   入れ子構造を変更すると、影響を受けるユーザーに対して資格の変更処理が行われます。

3. **無効なユーザーのチェック**。このジョブは、XenMobile管理者が無効なユーザーをチェックする操作を作成した場合のみ実行されます。このジョブはグループ同期ジョブの範囲内で実行されます。このジョブでは、Active Directoryに対してクエリを実行し、対象ユーザーの無効化状態を一度に1ユーザーずつ確認します。

よくある質問と回答

オンプレミスXenMobileのActive Directoryとのやり取り

Siddartha Vuppala , | Sep 15, 2017

この記事では、XenMobileサーバーとActive Directoryのやり取りについて説明します。XenMobileサーバーとActive Directoryのやり取りは、インラインとバックグラウンドの両方で行われます。以下のセクションでは、Active Directoryとのやり取りを伴うインライン操作およびバックグラウンド操作の詳細について説明します。

> ### 注意
>
> この記事ではやり取りの概要のみを示し、細かい詳細については扱いません。XenMobileコンソールでのActive DirectoryとLDAPの構成方法について詳しくは、「ドメインまたはドメイン+セキュリティトークン認証」を参照してください。

インラインでのやり取り

XenMobileサーバーは、管理者が構成するLDAP設定を使用してActive Directoryとの通信を行います。この設定により、ユーザーとグループに関する情報が取得されます。XenMobileサーバーとActive Directory間のやり取りが生じる操作を次に示します。

1. **LDAP構成。**Active Directory自体を構成するため、Active Directoryとのやり取りが行われます。XenMobileサーバーはActive Directoryで構成情報の認証を行うことで、構成情報の検証を試みます。この認証は、インターネットプロトコル、ポート、および指定のサービスアカウントの資格情報を使用して行われます。バインドが成功すれば、接続は適切に構成されています。

2. **グループベースのやり取り。**

   a. 役割ベースのアクセス制御（RBAC）時およびデリバリーグループの定義の作成時における1つ以上のグループの検索。XenMobileサーバーの管理者が、XenMobileコンソールで検索テキストを入力します。XenMobileサーバーにより、指定した文字列の一部が含まれるすべてのグループについて選択したドメインが検索されます。次に、XenMobileサーバーは検索で見つかったグループのobjectGUID属性、sAMAccountName属性、識別名属性を取得します。

   > ### 注意
   >
   > この情報は、XenMobileサーバーのデータベースには格納されません。

   b. RBACおよび展開グループの定義の追加または更新。XenMobileサーバーの管理者が上記の検索結果に基づいて目的のActive Directoryグループを選択し、展開グループの定義に追加します。XenMobileサーバーにより、Active Directory内で指定したグループが1度に1つずつ検索されます。XenMobileサーバーはobjectGUID属性を検索し、メンバーシップ情報を含む選択した属性を取得します。グループのメンバーシップ情報により、取得したグループとXenMobileサーバーデータベースの既存のユーザーまたはグループ間のメンバーシップが特定されます。グループのメンバーシップを変更すると、影響を受けるユーザーメンバーに関わるRBACおよび展開グループが確認され、ユーザーの権利割り当てが行われます。

   > ### 注意

展開グループの定義を変更すると、影響を受けるユーザーのアプリまたはポリシーの使用権が変更される場合があります。

c.**ワンタイムPIN（OTP）による招待**。XenMobileサーバー管理者が、XenMobileサーバーデータベースに存在するActive Directoryグループの一覧からグループを選択します。このグループのすべてのユーザーが、直接的および間接的にActive Directoryから取得されます。前の手順で特定されたユーザーに対して、OTP招待状が送られます。

注意

上記3つのやり取りは、XenMobileサーバーの構成変更によりグループベースのやり取りが開始されることを示しています。構成に変更がない場合、これらのやり取りではActive Directoryとの通信は行われません。また、定期的にバックグラウンドジョブでグループ側の変更を取得する必要もありません。

3. **ユーザーベースのやり取り。**

a. ユーザー認証。ユーザー認証のワークフローでは、Active Directoryと2種類のやり取りが行われます。

- 指定した資格情報によるユーザーの認証
- XenMobileサーバーデータベースへの選択したユーザー属性（objectGUID、識別名、sAMAccountName、グループのダイレクトメンバーシップなど）の追加または更新。グループのメンバーシップを変更すると、アプリ、ポリシー、アクセス資格の再評価が行われます。

ユーザーは、デバイスとXenMobileサーバーコンソールのどちらからでも認証を行うことができます。どちらの場合でも、Active Directoryとのやり取りの動作は同じです。

b. App Storeへのアクセスおよび更新。ストアを更新すると、ダイレクトグループメンバーシップを含むユーザー属性が更新されます。この処理により、ユーザー資格の再評価が可能になります。

c. デバイスのチェックイン。管理者は、定期的にXenMobileコンソールでデバイスのチェックインを構成します。デバイスのチェックインが行われるたびに、ダイレクトグループメンバーシップを含む対応するユーザー属性が更新されます。こうしたチェックインにより、ユーザー資格の再評価が可能になります。

d. グループ単位でのOTPによる招待。XenMobileサーバー管理者が、XenMobileサーバーデータベースに存在するActive Directoryグループの一覧からグループを選択します。ユーザーメンバーが直接的および間接的（入れ子構造の場合）にActive Directoryから取得され、XenMobileサーバーデータベースに保存されます。前の手順で特定されたユーザーメンバーに対して、OTP招待状が送られます。

e. ユーザー単位でのOTPによる招待。管理者が、XenMobileコンソールで検索テキストを入力します。XenMobileサーバーによりActive Directoryに対する紹介が行われ、入力したテキストに一致するユーザーレコードが返されます。次に、管理者がOTP招待状の送信先となるユーザーを選択します。ユーザーへの招待状の送信前に、XenMobileサーバーがActive Directoryからユーザーの詳細を取得してデータベースの該当する情報を更新します。

バックグラウンドでのやり取り

Active Directoryとのインライン通信で1つわかることは、XenMobileサーバーの構成が変更されるとグループベースのやり取りが行われるということです。構成に変更がない場合、グループについてActive Directoryとの通信は行われません。

こうしたやり取りではバックグラウンドジョブにより、Active Directoryと定期的に同期して変更内容を対象のグループに反映する必要があります。

Active Directoryをのやり取りを行うバックグラウンドジョブを次に示します。

1. **グループ同期ジョブ**。このジョブの目的は、対象のグループについて一度に1グループずつActive Directoryに照会し、識別名属性またはsAMAccountName属性の変更がないか確認することです。このActive Directoryに対する検索クエリでは、対象グループのobjectGUIDを使用して識別名属性とsAMAccountName属性の現在の値を取得します。対象グループの識別名またはsAMAccountNameの値の変更結果で、データベースが更新されます。

   > **注意**
   >
   > このジョブでは、ユーザーのグループメンバーシップ情報は更新されません。

2. **入れ子グループの同期ジョブ**。このジョブでは、対象グループの入れ子構造の変更内容が反映されます。XenMobileサーバーでは、対象グループの直接メンバーと間接メンバーの両方が資格を得ることができます。ユーザーのダイレクトメンバーシップは、ユーザーベースのインラインでのやり取りの際に更新されます。このジョブはバックグラウンドで実行され、間接メンバーシップを追跡します。間接メンバーシップとは、対象グループのメンバーであるグループにユーザーが属している状態を指します。

   このジョブでは、XenMobileサーバーデータベースからActive Directoryグループのリストを取得します。Active Directoryのグループは、展開グループかRBAC定義のどちらかに含まれます。このリストの各グループについて、XenMobileサーバーがグループのメンバーを取得します。グループのメンバーは、ユーザーとグループの両方を表す識別名をリスト化したものです。XenMobileサーバーはActive Directoryに対して別のクエリを実行し、対象グループのユーザーメンバーのみを取得します。これら2つのリストの差を取ると、対象グループのグループメンバーのみが残ります。メンバーグループへの変更結果がデータベースに反映されます。階層内のすべてのグループについて、同じ手順が繰り返されます。

   入れ子構造を変更すると、影響を受けるユーザーに対して資格の変更処理が行われます。

3. **無効なユーザーのチェック**。このジョブは、XenMobile管理者が無効なユーザーをチェックする操作を作成した場合のみ実行されます。このジョブはグループ同期ジョブの範囲内で実行されます。このジョブでは、Active Directoryに対してクエリを実行し、対象ユーザーの無効化状態を一度に1ユーザーずつ確認します。

よくある質問と回答

- デフォルトでは、バックグラウンドジョブの実行頻度はどのようになっていますか?
- なぜグループ同期ジョブが必要なのですか?
- グループ同期ジョブは無効化できますか?
- なぜ入れ子グループによる処理中のバックグラウンドジョブが必要なのですか?
- 入れ子グループによる処理中のジョブは無効化できますか?