XenMobile Server 10

May 10, 2016

アプリケーションの追加

MDXポリシーの概要

自動化された操作

XenMobileクライアント設定

iOSデバイス用のカスタムWorx Storeブランド設定を作成するには

Worx HomおよびGoToAssistサポートオプションを作成するには

クライアントプロパティを追加、編集、または削除するには

クライアントプロパティリファレンス

XenMobileサーバー設定

XenMobileでのActiveSyncゲートウェイ

Google Play資格情報

iOSデバイス登録プログラム

iOS VPP

Mobile Service Provider

ネットワークアクセス制御

Samsung KNOX

サーバープロパティ

Syslog

XenAppおよびXenDesktopを構成するには

サポートとメンテナンス

接続確認の実行

XenMobileでのサポートバンドルの作成

デバッグログファイルを表示するには

ログ設定を構成するには

XenMobileでのログファイルの表示および分析

XenMobileコマンドラインインターフェイスオプション

XenMobile 10 API

XenMobile Mail Manager 10

アーキテクチャ

システム要件および前提条件

インストールおよび構成

ActiveSync IDによるメールポリシーの適用

アクセス制御規則

デバイス監視

XenMobile 10について

Oct 24, 2016

XenMobile 10は、App ControllerとXenMobile 9以前のバージョンのDevice Managerコンポーネントをユーザーデバイスやアプリを構成できる一元的な管理ツールに結合します。

注: Remote Supportクライアントは、Windows CEおよびSamsung Androidデバイス用XenMobile Cloudバージョン10.xでは利用できません。

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

新機能

このリリースで解決した問題については、http://support.citrix.com/article/CTX141722を参照してください。 XenMobile 10.0の既知の問題については、「既知の問題」を参照してください。

- **結合されたインフラストラクチャ。** モバイルデバイス管理（MDM）およびモバイルアプリ管理（MAM）が1つのサーバーインフラストラクチャに結合されています。
  - 必要となるセットアップ手順が少なくなるため、より早くXenMobileを展開できます。
  - 1つの仮想サーバーからアプリとデバイスを管理できます。
- **新しい一元的なXenMobileコンソール。**
  - 新しく設計された操作が簡単なユーザーインターフェイスにより、モビリティ環境全体の登録、展開、構成、およびトラブルシューティングといった管理タスクを簡素化しています。
  - また、アプリおよびデバイスのポリシー構成が簡素化されています。 使用できるすべてのデバイスプラットフォーム全体に対して1つのポリシーを構成できます。
- **同じコンソールのNetScaler Gatewayの統合。** モビリティ環境の一部である複数のシステムに対する自動接続性チェックを管理できます。
- **ビーコンサポートの廃止。** オプションがXenMobileコンソールに表示されますが、ビーコンはXenMobile 10でサポートされません。 NetScaler Gateway経由でXenMobileサーバーに接続するか、ファイアウォール内から直接XenMobileサーバーに接続することをお勧めします。
- **アプリ認証のサポートの強化。** デバイスと内部ネットワーク間、内部ネットワークとXenMobileサーバー間、およびXenMobileコンソール接続を安全に暗号化できます。
  - RSA Adaptive Authentication
  - FIPS 140.2高度暗号化のサポート

XenMobile 10の使用を開始する

まず、XenServer、VMware ESXi、またはHyper-Vといったハイパーバイザー上にXenMobile 10.0 Editionの仮想イメージをダウンロードおよびインストールして作業を開始し、ハイパーバイザーのコマンドラインコンソールでXenMobileの初期構成を実行します。 詳しくは、「システム要件」「インストール前のチェックリスト」および「XenMobileのインストール」を参照してください。

次に、初期構成の間にセットアップした管理者アカウントでWebベースのXenMobileコンソールを開きます。

次にコンソールで何をするかについては、「コンソールで始める」を参照してください。 最初の一連の推奨事項は、インストール手順実行中にスキップした可能性のある初期設定が対象になっています。

アーキテクチャの概要

Oct 24, 2016

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

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

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

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

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

以降のセクションでは、XenMobile展開のさまざまなリファレンスアーキテクチャについて説明します。 リファレンスアーキテクチャ図については、『XenMobile展開ハンドブック』の、「Reference Architecture for On-Premises Deployments」および「Reference Architecture for Cloud Deployments」を参照してください。 ポートの完全な一覧については、『XenMobileのポート要件」を参照してください。

実稼働環境では、スケーラビリティとサーバー冗長性を実現するために、XenMobileソリューションをクラスター構成で展開することをお勧めします。 また、NetScaler SSLオフロード機能を活用してXenMobileサーバーの負荷をさらに軽減し、スループットを高めることができます。 NetScalerで2つの負荷分散仮想IPアドレスを構成することによってXenMobile 10.xのクラスタリングをセットアップする方法について詳しくは、「XenMobile 10のクラスタリングの構成」を参照してください。

モバイルデバイス管理（MDM）モード

XenMobile MDM Editionでは、iOS、Android、Amazon、およびWindows Phoneのモバイルデバイス管理を使用できます（「XenMobile 10のサポート対象のデバイスプラットフォーム」参照）。 XenMobileのMDM機能のみを使用する場合、XenMobileをMDMモードで展開します。 たとえば、コーポレート発行のデバイスをMDMで管理して、デバイスポリシーやアプリを展開し、アセットインベントリを取得して、デバイスワイプなどのアクションをデバイスで実行できるようにする必要がある場合などです。

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

モバイルアプリケーション管理（MAM）モード

MAMではiOSおよびAndroidデバイスがサポートされますが、Windows Phoneデバイスはサポートされません（「XenMobile 10のサポート対象のデバイスプラットフォーム」参照）。 XenMobileのMAM機能のみを使用する予定で、MDM用に登録するデバイスがない場合は、XenMobileをMAMモード（MAM-onlyモードとも呼ばれます）で展開します。 たとえば、BYOモバイルデバイスのアプリとデータをセキュリティ保護する必要がある場合や、エンタープライズモバイルアプリを配信して、アプリのロックおよびデータのワイプを実行できるようにする必要がある場合などです。 デバイスをMDMに登録することはできません。

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

MDM+MAMモード

MDMモードとMAMモードを併用すると、iOS、Android、およびWindows Phone向けのモバイルデバイス管理に加えて、モバイルアプリとデータの管理を行うこともできます（「XenMobile 10のサポート対象のデバイスプラットフォーム」参照）。 XenMobileのMDM+MAM機能を使用する場合、XenMobileをENT（エンタープライズ）モードで展開します。 たとえば、コーポレート発行のデバイスをMDMで管理する必要がある場合や、デバイスポリシーやアプリを展開し、アセットインベントリを取得し、およびデバイスをワイプできるようにする必要がある場合です。 さらに、エンタープライズモバイルアプリを配信し、アプリのロックとデバイスのデータのワイプを実行できるようにする必要がある場合もあります。

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

XenMobile 10の展開規模

Oct 24, 2016

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

パフォーマンスとスケーラビリティのガイドライン

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

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

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

表1. XenMobile Enterpriseの登録

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

システム構成およびテスト結果

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

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

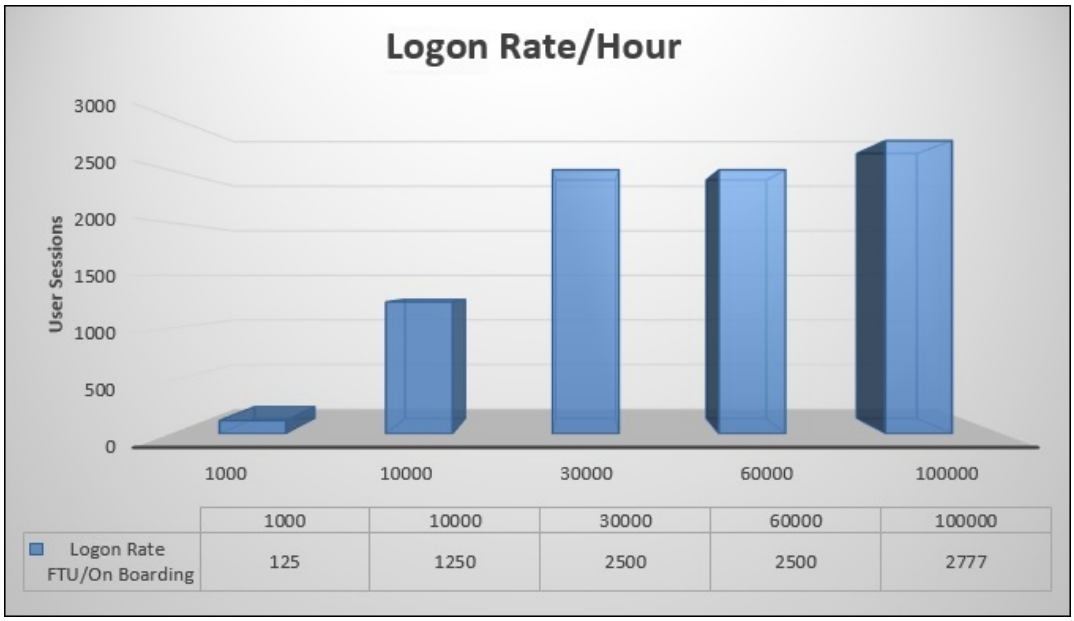
テスト結果の解析により、以下の結論が導かれました。

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

表2. XenMobile Enterpriseの登録スケーラビリティのテスト

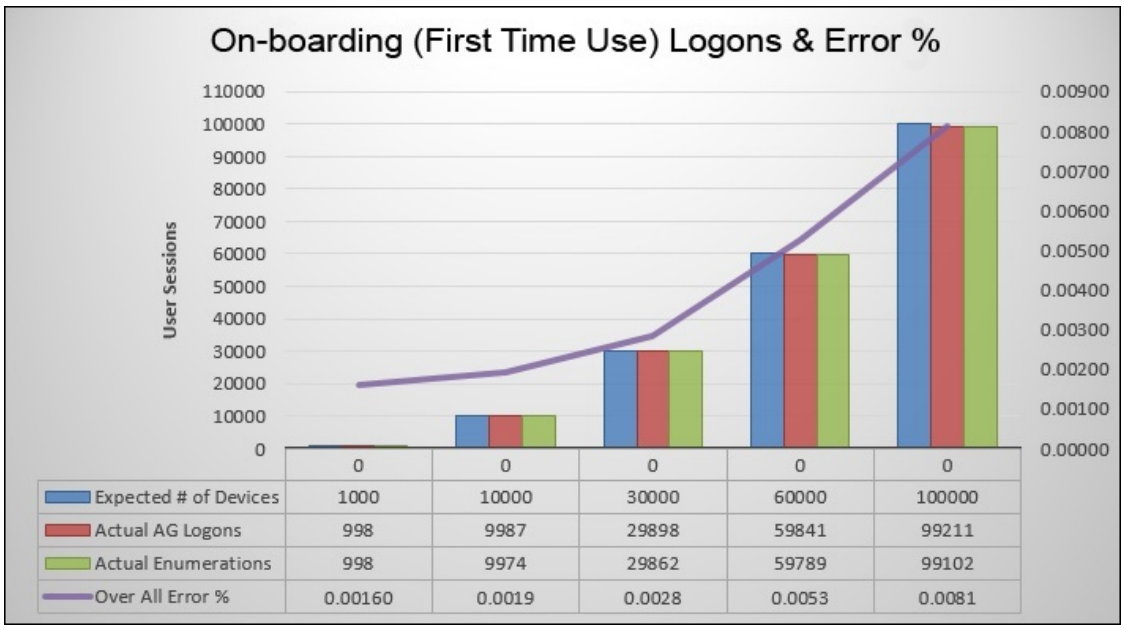
デバイスの数	1,000	10,000	30,000	60,000	100,000
ログオン数					
オンボーディング（FTU)	125	1,250	2,500	2,500	2,777
既存ユーザー	1,000	2,500	7,500	15,000	16,667
構成					
参照環境	VPX-XenMobile スタンドアロン	MPX-XenMobile スタンドアロン	MPX-XenMobile クラスター（3）	MPX-XenMobile クラスター（6）	MPX-XenMobileクラスター（10）
NetScaler Gateway	2GBのRAMを搭載したVPX 2つの仮想CPU	MPX-10500		MPX-20500	
XenMobile - モード	スタンドアロン	スタンドアロン	クラスター		
XenMobile - クラスター	-	-	3	6	10
XenMobile - 仮想アプライアンス	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	8GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU	16GBのRAMおよび4つの仮想CPU
データベース	外部				

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



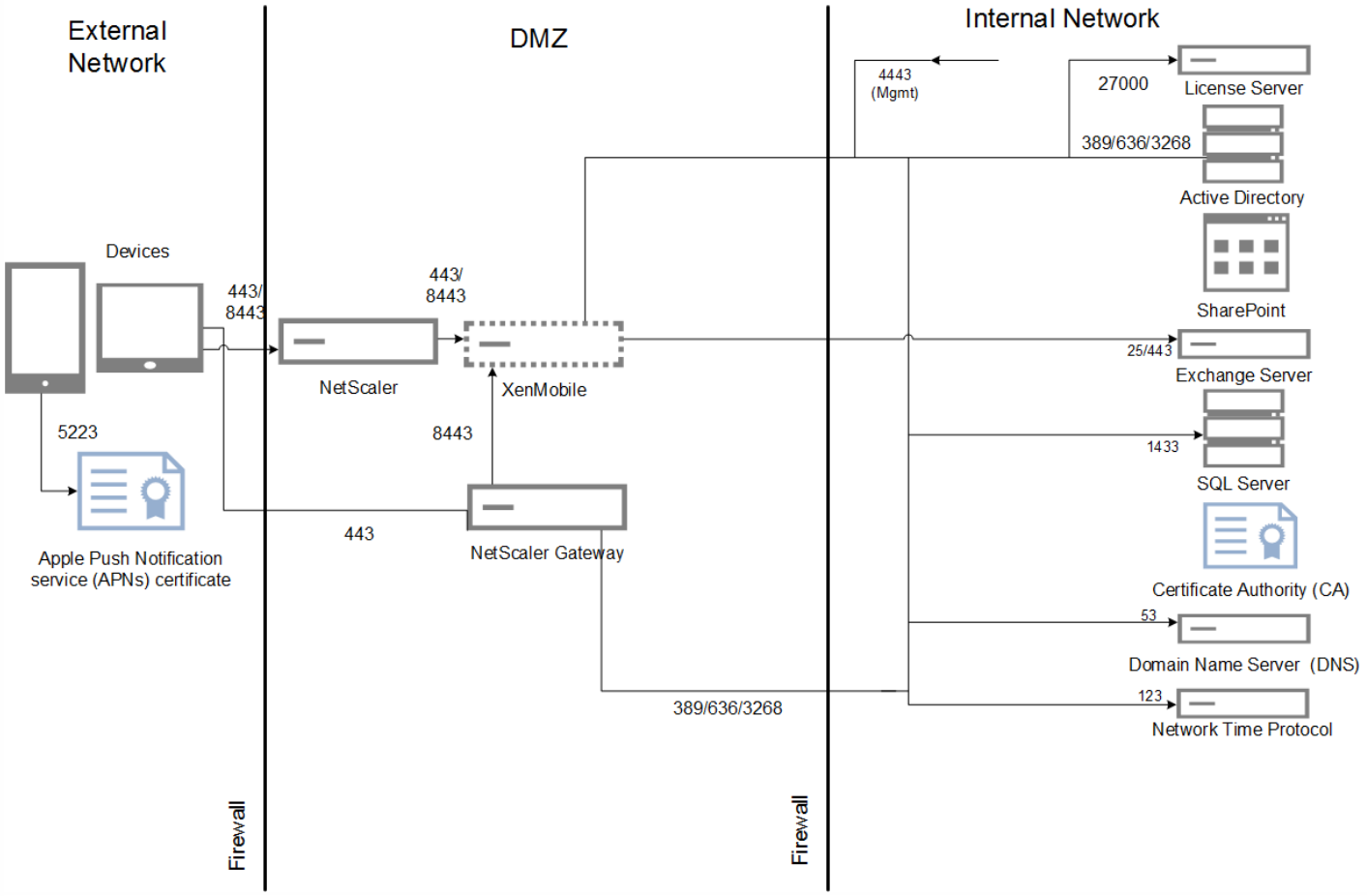
注：システム規模に対して推奨される数を超過する登録やログオンがあったりハードウェアの性能が不足していたりすると、以下の事象が発生します。

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

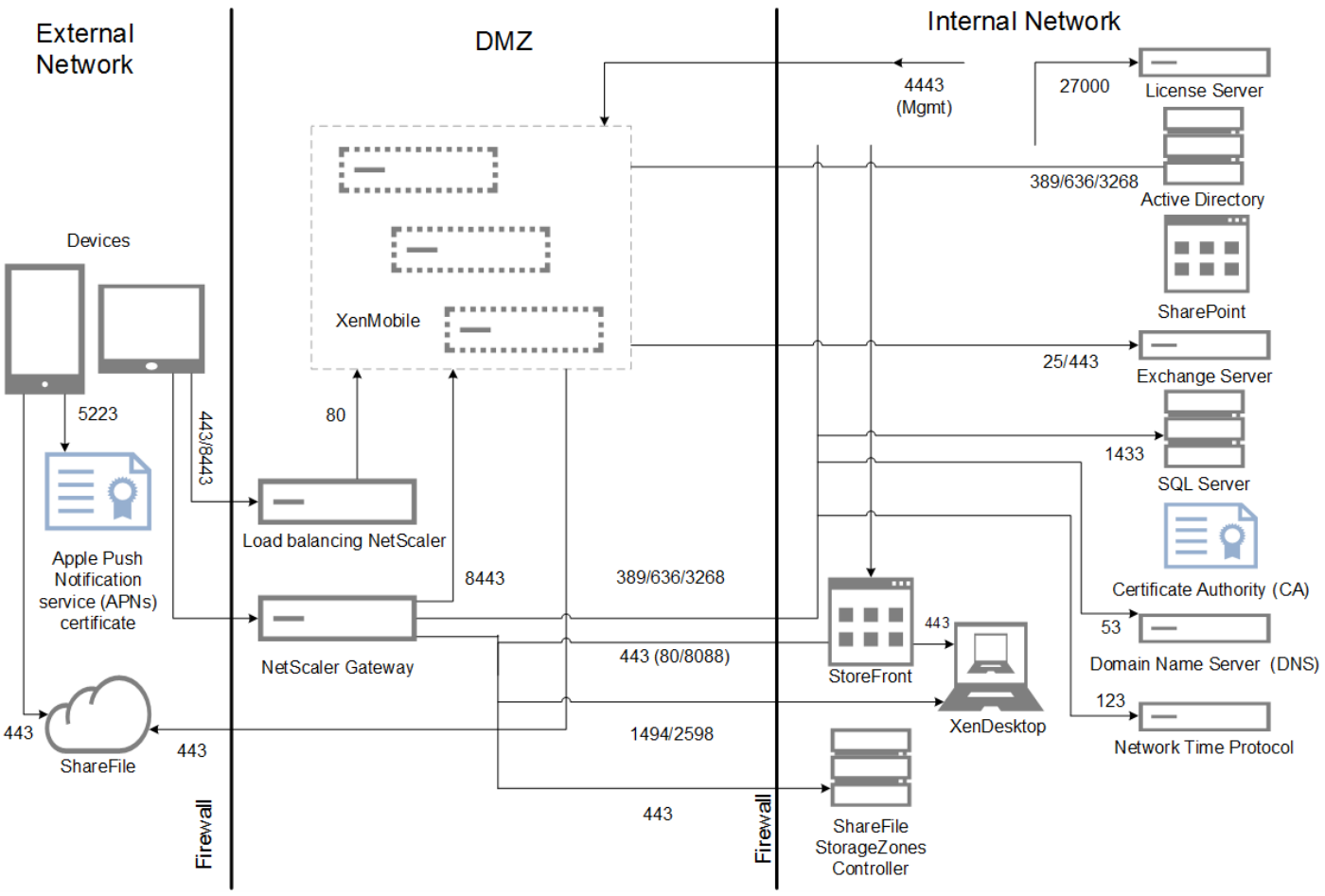


上の図のエラー率には各操作に対応する要求に対して発生する全体的なエラーが含まれており、ログオンに限定したものではありません。「終了基準」に定義するとおり、エラー率は各実行テストの許容可能な範囲に収まっています。

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



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



テスト方法

ベンチマークを確立するため、XenMobile Enterpriseに対してテストを実行しました。小規模および大規模な展開の両方を対象とし、測定には1,000～10,0000デバイスを使用しました。

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

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

ワークロード

ユーザーワークロードは以下のように定義されます。

表3ユーザーワークロードの定義

ユーザーセッ	各セッションのNetScaler Gatewayログオン、列挙、デバイス登録などが含まれます。

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

オンボーディング（FTU)ワークロード

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

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

ワークロードのパラメーターには以下が含まれました。

- デバイスあたり1件のデバイス登録
- デバイスあたり1件の列挙
- デバイスあたり14件のアプリの列挙
- デバイスあたり4件のWorx Storeの起動
- デバイスあたり4件のWeb/SaaSアプリのSSO
- デバイスあたり1件のMDXアプリのダウンロード
- 2件の必須アプリのダウンロード

既存ユーザーのワークロード

以下の表は既存ユーザーのワークロードを示します。このワークロードにより、WorxMailおよびWorxWebアプリを使用する人のユーザーがシミュレートされました。このシミュレーションを使用して、XenMobile構成内のNetScaler Gatewayポートのスケーラビリティを測定しました。WorxWebアプリについては、ユーザーは内部Webサイトにアクセスしました。この場合XenMobileのSSOはトリガーされません。このモードで含まれる操作は以下のとおりです。

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

WorxAppsの接続プロファイル

以下の表は既存ユーザーのワークロードパラメーターを示します。

表4WorxAppsの接続プロファイル

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

1.**セッションあたり**：8時間

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

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

注：接続の詳細を変更すると解析結果に影響があります。たとえば、ユーザーあたりの接続数を増やすと、サポートされるNetScaler Gatewayセッションの数は減少する可能性があります。

WorxMailおよびWorxWebのプロファイル

以下の図は、WorxMailおよびWorxWebのプロファイルの詳細を示します。

表5中程度のワークロードのWorxMailプロファイル

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

表6中程度のワークロードのWorxWebプロファイル

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

構成とパラメーター

以下の構成を使用してスケーラビリティテストを実行しました。

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

終了基準

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

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

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

ソフトウェアおよびハードウェアの詳細

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

表7XenMobileインフラストラクチャのコンポーネント

コンポーネント	バージョン
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0.0.62300
外部データベース	MS SQL Server 2008 R2 （128GBのRAM、300GBのディスクスペース、24の仮想CPU）

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

表8XenServerのハードウェア

ベンダー	GenuineIntel
モデル	Intel Xeon CPU — E5645 @ 2.40GHz（CPU数24）

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

このトピックまたは言及されている製品に関する追加的な製品情報および技術的な質問については、Citrix.comのXenMobileドキュメントサイトにアクセスして最新の製品ドキュメントを参照するか、Citrixの販売担当者にお問い合わせください。

XenMobile Cloudについて

Oct 24, 2016

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

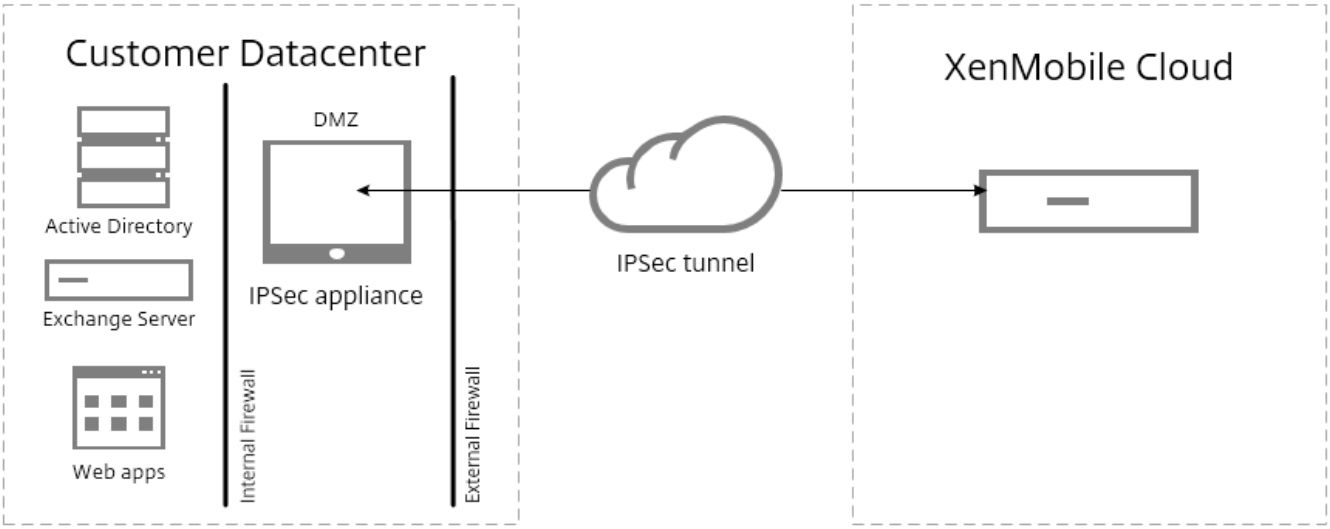
Cloud Operations管理者は、ネットワーク接続のメンテナンスと構成を行うだけでなく、NetScaler、XenApp、XenDesktop、StoreFront、ShareFileなどの各種のCitrix製品を統合します。 クラウド環境は、世界中にあるAmazonデータセンターでホストされ、高パフォーマンス、迅速な応答を実現し、サポートに対応します。

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

注意

- Remote Supportクライアントは、Windows CEおよびSamsung Androidデバイス用XenMobile Cloudバージョン10.xでは利用できません。
- XenMobile Cloudサーバー側のコンポーネントはFIPS 140-2に準拠していません。
- XenMobile Cloud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コンソールのサポートページでログをダウンロードできます。 システムログをダウンロードするには、［すべてダウンロード］をクリックしてください。 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。

次の図にXenMobile Cloudの基本アーキテクチャを示します。 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、「クラウド展開のリファレンスアーキテクチャ」についてのセクションを参照してください。



XenMobile Cloudアーキテクチャは、Citrix CloudBridgeをインストールおよび展開するか、データセンター内の既存のIPsecゲートウェイを使用することで、既存のインフラストラクチャに統合することができます。

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

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

XenMobile Cloudの役割

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

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

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

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

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

役割をユーザー（ユーザーレベルで）や、Active Directoryグループ（グループ内のすべてのユーザーが同じ権限を持つ）に割り当てることができます。 ユーザーが複数のActive Directoryグループに属している場合は、すべての権限が統合されてそのユーザーの権限が定義されます。 たとえば、ADGroupAのユーザーがマネージャーのデバイスを検索でき、ADGroupBのユーザーが従業員のデバイスをワイプできる場合、両方のグループに属するユーザーは、マネージャーおよび従業員のデバイスを

検索し、ワイプすることができます。

注：ローカルユーザーに割り当てることができる役割は1つだけです。

XenMobileのRBAC機能を使用すると、次のことを実行できます。

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

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

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

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

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

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

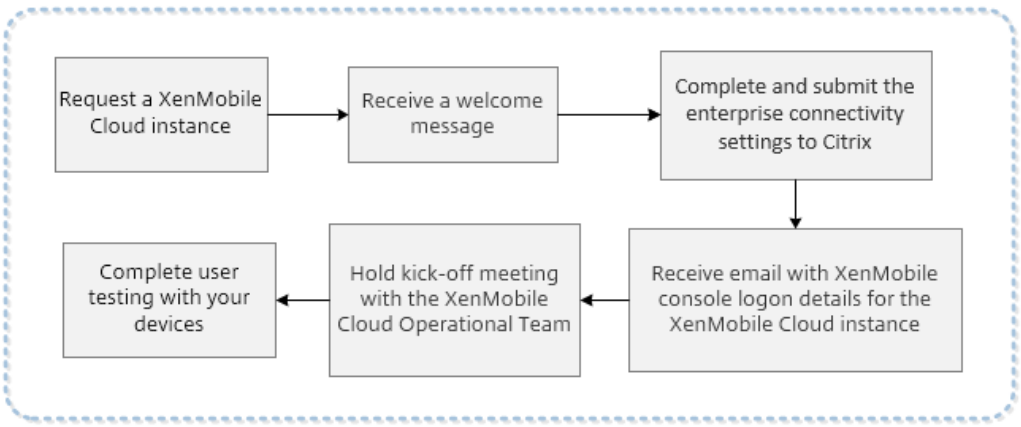
役割をカスタマイズする手順については、「RBACを使用した役割の構成」を参照してください。

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

XenMobile Cloudの前提条件および管理

May 10, 2016

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



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

XenMobile CloudのIPSecトンネルゲートウェイ

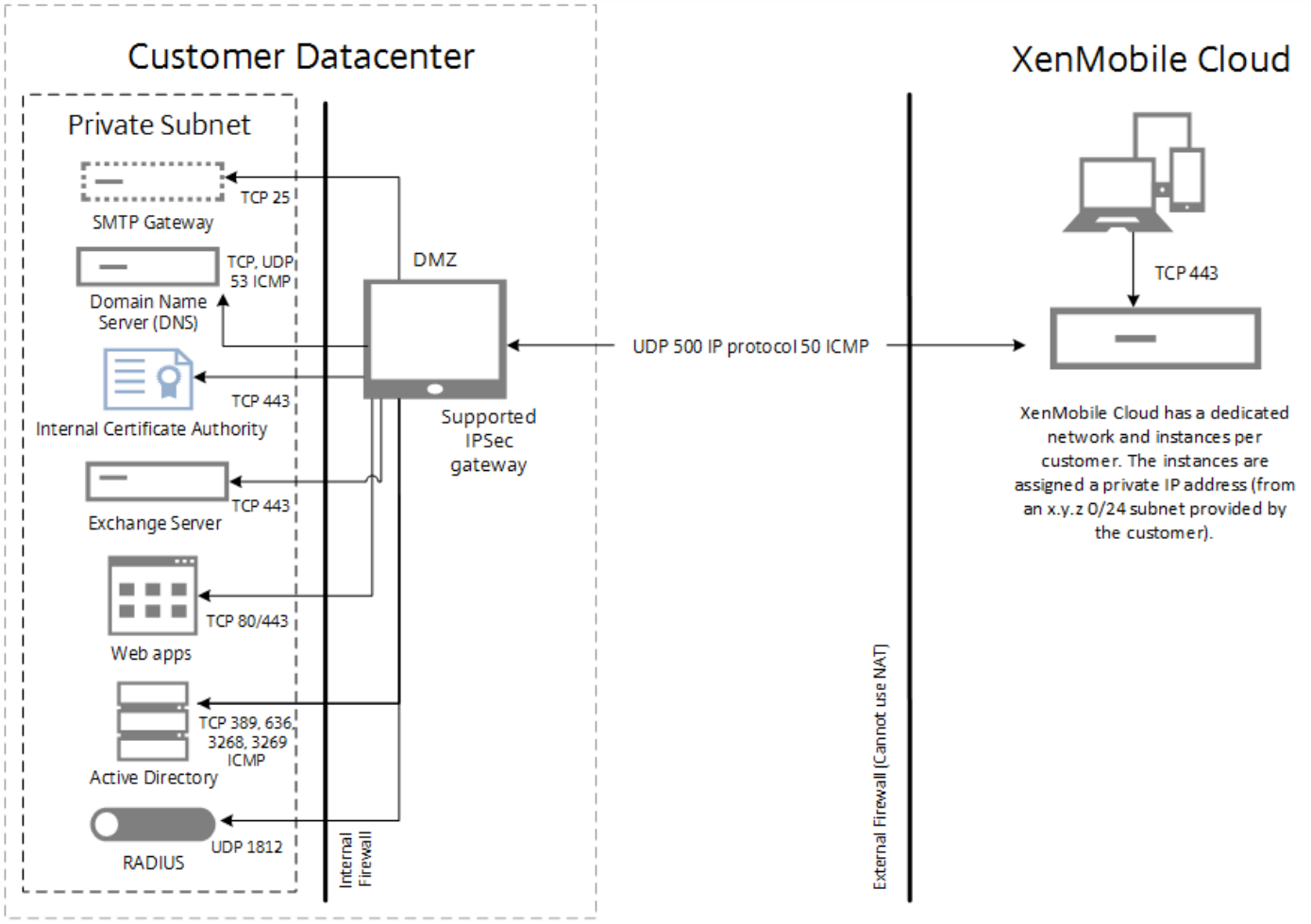
IPSecトンネルであるXenMobile Enterprise Connectorを使用して、Active Directoryなどの企業サービスにXenMobile Cloudインフラストラクチャを接続できます。

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

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

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

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



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

接続元	接続先	プロトコル	ポート	説明
外部（境界）ファイアウォール - 受信規則				
XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	UPD	500	IPSec IKE構成。
XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	IPプロトコルID	50	IPSec ESPプロトコル。

XenMobile Cloud（AWS）IPCSEC VPNのパブリックIPアドレス[1]	顧客のIPSecアプライアンス	ICMP		トラブルシューティング用（セットアップ後に削除可能）。
外部（境界）ファイアウォール – 送信規則				
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	UDP	500	IPSec IKE構成。
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	IPプロトコルID	50、51	IPSec ESPプロトコル。
顧客のDMZサブネット	XenMobile Cloud（AWS）IPSec VPNのパブリックIPアドレス[1]	ICMP		トラブルシューティング用（セットアップ後に削除可能）。
内部ファイアウォール – 受信規則				
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内の内部DNSサーバー	TCP、UPP、ICMP	53	DNS解決。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のActive Directoryドメインコントローラー	LDAP（TCP）	389、636 3268、3269	ドメインコントローラーに対するユーザーのActive Directory認証およびディレクトリクエリ用。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のActive Directoryドメインコントローラー	ICMP		トラブルシューティング用（セットアップ全体の完了後に削除可能）。
未使用でルーティング可能な顧客の/24サブネット[2]	顧客のデータセンター内のExchangeサーバー	SMTP（TCP）	25	オプション。XenMobileメール通知用。
未使用でルーティング可	顧客のデータセンター内	HTTP、	80、443	ActiveSyncトラフィックがデ

能な顧客の/24サブネット[2]	のExchangeサーバー	HTTPS（TCP）		バイスから（IPSecトンネル経由で）XenMobile Cloudインフラストラクチャを介してExchangeサーバーに送信される場合は、Exchange ActiveSyncが必要です。 ユーザーデバイスが、XenMobile IPSecトンネル経由でExchangeサーバーに接続する必要がなく、インターネット経由でパブリックなActiveSync FQDNと通信する場合は、これは不要です。
未使用でルーティング可能な顧客の/24サブネット[2]	イントラネット/Webサーバー、SharePointサーバーなどのアプリケーションサーバー	HTTP、HTTPS（TCP）	80、443	XenMobile IPSecトンネル経由の、イントラネットおよび/またはアプリケーションサーバーへのユーザーモバイルデバイスからのアクセス。 各アプリケーションサーバーを、アプリケーションにアクセスするために必要なポート番号（通常ポート80および/または443）と共にファイアウォール規則に追加する必要があります。
未使用でルーティング可能な顧客の/24サブネット[2]	PKIサーバー（オンプレミスPKIを使用する場合）	HTTPS（TCP）	443	オプション（XenMobile POCでは使用しません）： これは、XenMobile CloudインフラストラクチャとMicrosoft CAのようなオンプレミスPKIインフラストラクチャを統合して、XenMobileソリューションに証明書ベースの認証を設定するために活用できます。
未使用でルーティング可能な顧客の/24サブネット[2]	RADIUSサーバー	UDP	1812	オプション（XenMobile POCでは使用しません）： これは、XenMobileソリューションに2要素認証を設定する

				ために使用できます。
内部ファイアウォール – 送信規則				
顧客の内部サブネット。このサブネットからXenMobileコンソールを使用可能にする必要があります。	未使用でルーティング可能な顧客の/24サブネット[2]	TCP	4443	XenMobile Cloudインフラストラクチャ内のXenMobile App Controller（MAM）コンソール。

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

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

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

XenMobile Apple APNs証明書

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

WorxMail for iOSのプッシュ通知証明書

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

XenMobile MDX Toolkit

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

iOSアプリをラップする計画をしている場合は、必要なApple配布プロファイルを作成するためにApple開発者アカウントが必要です。 詳しくは、MDX Toolkitのシステム要件およびApple Developer Webサイトを参照してください。

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

Windows Phone登録のためのXenMobile自動検出

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

XenMobileコンソール

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

XenMobileデバイス登録

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

XenMobileサポート

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

XenMobile Cloudにおけるモバイルプラットフォームのサポート

May 10, 2016

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

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

Android

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

iOS

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

Windows

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

システム要件

Oct 24, 2016

XenMobile 10を使用するには、以下のシステム環境が必要です。

- 以下のいずれかのサーバーオペレーティングシステム
  - XenServer（サポートされるバージョン：6.2.x、6.1.x、または6.0.x）。詳細は「XenServer」を参照してください。
  - VMware（サポートされるバージョン：ESXi 5.5、ESXi 5.1、またはESXi 4.1）詳しくは「VMware」を参照してください。
  - Hyper-V（サポートされるバージョン：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2）。詳しくは「Hyper-V」を参照してください。
- デュアルコアプロセッサ
- 2つの仮想CPU
- 8GBのRAM
- 50GBのディスクスペース

10,000台のデバイスの場合は以下の構成が推奨されます。

- クアッドコアプロセッサ
- 8GBのRAM

NetScaler Gatewayのシステム要件

XenMobile 10と共にNetScaler Gatewayを使用するには、以下のシステム環境が必要です。

- XenServer、VMWare、またはHyper-V
- 2つの仮想CPU
- 2GBのRAM
- 20 GBのディスクスペース

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

XenMobile 10のデータベース要件

XenMobileリポジトリでは、以下のサポート対象バージョンのいずれかで稼動しているMicrosoft SQL Serverデータベースが必要です。

- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008

Citrix XenMobileはデータベース高可用性用に、SQL AlwaysOn可用性グループおよびSQLクラスタリングをサポートします。XenMobileデータベース高可用性用のデータベースミラーリングはサポートされていません。 MS SQL Cluster展開でActive/ActiveまたはActive Passiveモードのデータベース高可用性はサポートしません。

注：データベースがオフラインの場合、XenMobileサーバーもオフラインになるため、XenMobileサーバーによりデバイスからのいずれの接続も実行されません。

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

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

XenMobileの互換性

Oct 24, 2016

> **Important**
>
> 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。すべてではありませんが、ほとんどのXenMobileアプリの名称も変更されました。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（NetScaler Gatewayなど）のサポートされているバージョンと、Worxモバイル/XenMobileアプリをラップ、構成、および配布するために必要なMDX Toolkitのバージョンを示しています。

XenMobile 10.x

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

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 10.4の場合、XenMobile 10.3.6（このバージョンは完全版ではなくService Pack）およびXenMobile 10.3.5もサポートされます。

XenMobileのクライアントコンポーネントは以下の適合性の要件に従います。

- 最新バージョンのSecure HubおよびMDX Toolkitは最新およびその2つ前のバージョンまでのXenMobileサーバーと互換性があります。
- Secure Hubの最新バージョンとその前のバージョンは、最新バージョンのMDX ToolkitおよびXenMobileアプリと互換性があります。
- 最新バージョンのXenMobileアプリは最新のMDX Toolkitでテスト済みです。

新しい機能や修正された機能、およびポリシーの更新について最大限に活用するには、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。

新しい機能や修正された機能、およびポリシーの更新について最大限に活用するには、最新バージョンのMDX Toolkit、Worx Home、およびWorxモバイルアプリをインストールすることをお勧めし

MDX Toolkit for iOSおよびAndroidのバージョン	**Worx Home/Secure Hubのバージョン**	
	Android	**iOS**
10.4	10.4	10.4
10.3.10	10.3.10	10.3.10
10.3.9	10.3.9	10.3.9
10.3.6	10.3.8	10.3.8
10.3.5	10.3.6	10.3.6
10.3.1	10.3.5	10.3.5
10.2.1	10.3.1	10.3.1
10.0.7	10.3	
10.0.5	10.2.1	10.2.1
10.0.3	10.0.8	10.0.8
	10.0.3	10.0.3

MDX Toolkit for Windows Phone	**互換性のあるWorx Homeのバージョン***
10.0.7	10.0.3
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

*バージョン10.0.3より前のWorx Homeには互換性はありますがサポートされません。

> **注意**
>
> Windows Phone 10は、現在XenMobile 10と10.3.xでのみサポートされています。 XenMobile 10.1で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、CTX215497を参照してください。

XenMobile 10.x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 8.1/10[1]
Secure Hub	10.4	10.4	
Worx Home	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3.1 10.2.1 10.0.8 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.3 10.0.0
Secure Forms		10.4 10.3.10 10.3.9 10.3.8 10.3.6	
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
Worx Notes	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	

WorxTasks	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[2]	6.5	6.4	
ShareConnect	3.6	3.8	
ShareFile	4.9	4.7.1	

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

2 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
- Self Help Portal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。

XenMobile 9

XenMobile 9にはDevice Manager 9.0およびApp Controller 9.0が含まれます。

サポートされているNetScaler Gatewayのバージョン：

- 11.0.64
- 10.5.x.e
- 10.5.x MR
- 10.1.x.e
- 10.1.x MR

XenMobileのクライアントコンポーネントは一般的に以下の適合性の要件に従います。

- 最新バージョンのSecure HubおよびMDX Toolkitは最新およびその直前のバージョンのXenMobileサーバーに適合します。
- 最新バージョンのMDX Toolkitは最新のXenMobileアプリに適合します。
- 最近のいくつかのバージョンのMDX Toolkitは以下のバージョンのSecure Hubに適合します。

MDX Toolkit for iOSおよびAndroidのバージョン	**Worx Home/Secure Hubのバージョン***

	Android	iOS
10.4	10.4	10.4
10.3.6	10.3.6	10.3.6
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	
10.3	10.3	10.3
10.2.1	10.2.1	10.2.1
10.0.7	10.0.8	10.0.8
10.0.5	10.0.3	10.0.3
10.0.3		

MDX Toolkit （Windows Phone 10[1]	互換性のあるSecure Hub バージョン
10.4	10.4
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2	10.2

[1]XenMobile 9で、Windows 10の修正プログラムが必要です。こちらから入手できます。

MDX Toolkit for Windows Phone 8.1	互換性のあるSecure Hubのバージョン*
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2.1	10.2.1
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

*バージョン10.0.3より前のSecure Hubには互換性はありますがサポートされません。

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

アプリ	Android	iOS	Windows Phone 8.1
Secure Hub	10.4	10.4	
Worx Home	10.3.10	10.3.10	10.0.3

	10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3.1 10.2.1 10.0.3 10.0.0	10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2.1 10.0.8 10.0.3 10.0.0	10.0.0
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.7
Secure Notes	10.4	10.4	
WorxNotes*	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.0	
Secure Tasks	10.4	10.4	
WorxTasks	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7	

Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.7 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[1]	6.0.2	6.3.10	
ShareConnect	3.2	3.6	
ShareFile	4.6.5	4.5	

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

* MDX Toolkit 2.3および2.2.1はWorxNotes/Secure Notesをサポートしません。

サポート対象のデバイスプラットフォーム

Oct 24, 2016

XenMobileは次のプラットフォームを実行中のデバイスをサポートし、アプリケーションおよびデバイスの管理を含むエンタープライズモビリティを管理します。 プラットフォーム固有の制限事項やセキュリティ機能によっては、一部の機能がサポートされない場合があります。

Android 4.1やiOS 7のような、モバイルオペレーティングシステムの古いバージョンをサポートする方法については、Citrix Support Knowledge CenterのCTX204192を参照してください。

ここに記載したサポートされるデバイスプラットフォーム情報は、XenMobile Mail ManagerおよびXenMobile NetScaler Connectorにも適用されます。

> ## 注意
>
> - 最低限、主要オペレーティングシステムプラットフォームの最新バージョンおよび1つ前のバージョンをサポートします。 XenMobileの新しいバージョンには、以前のプラットフォームリリースで使用できない機能もあります。 ここでは、現在サポートされるオペレーティングシステムの詳細について説明します。 また、テスト済みのデバイスモデルについても説明します。 その他のデバイスモデルで問題が発生した場合は、Citrixサポートにお問い合わせください。
> - バージョン10.4リリースでは、WorxモバイルアプリはXenMobileアプリに名前が変更されました。 すべてではありませんが、XenMobileアプリの大半の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。

Android

XenMobile 10.4および10.3.x

すべてのモードでサポートされるオペレーティングシステム：Android 4.4.x、5.x、6.x、7

MDM-Onlyモードでサポートされるオペレーティングシステム：Android 4.1.x、4.2.x、4.3

Worx Home/Secure Hubは、x86ベースのAndroidデバイスでサポートされ、MDM機能を提供します。

MDXでラップされたWorxアプリ/XenMobileアプリは、Android x64ベースのデバイスではサポートされています。

上記のオペレーティングシステム上でXenMobile 10.3.xと10.4のテストに使用されたAndroidデバイスの例：

- Nexus 6、7、9、10
- Samsung Galaxy S4およびNote 3、4、5
- GalaxyタブレットP750
- Galaxy Tab-A
- Galaxy Tab 2 - S3、S4、S5
- HTC One
- Samsung Tab P750
- Samsung S6、S6 Edge、S7
- OnePlus X
- Xiaomi Mi 4
- Huawei Honor 6
- Huawei Ascend Mate 7

- HTC One M9
- Motorola Moto-X
- Sony Experia Z
- Note 2、3、4

XenMobile 10および10.1

すべてのモードでサポートされるオペレーティングシステム：4.4.x、5.x、6.x、7

MDM-Onlyモードでサポートされるオペレーティングシステム：4.1.x

Android 4.2および4.3はサポートされません。

Worx Homeは、x86ベースのAndroidデバイスでサポートされ、MDM機能を提供します。 アプリケーション管理は、ARMベースのプロセッサを装備したAndroidデバイスでのみ使用可能です。 MDXでラップされたアプリケーションは、Android x86ベースのデバイスではサポートされていません。

MDXでラップされたWorxアプリケーションは、Android x64ベースのデバイスでサポートされています。

上記に記載されたオペレーティングシステム上でXenMobile 10と10.1をテストする際に使用されたAndroidデバイスの例：

- Nexus 10、7、5、9
- Galaxy S4およびNote 2, 3
- Galaxy Tab 2、S3、S4、S5
- Moto X
- HTC One
- HTC Desire、LG
- Samsung Tab P750

SAFEおよびKNOX

互換性のあるSamsungデバイスでは、XenMobile 10.xはSamsung for Enterprise（SAFE）ポリシーとSamsung KNOXポリシーの両方をサポートし、拡張しています。 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。 Samsung KNOX APIを有効にするには、Samsung ELMキーの展開に加え、Samsung KNOX License Management System（KLMS）を使用してSamsung KNOXライセンスを購入する必要もあります。

HTC固有のポリシーについては、XenMobileはHTC APIバージョン0.5.0をサポートします。 Sony固有のポリシーの場合、XenMobileはSony Enterprise SDK 2.0をサポートします。

iOS

注：すべてのWorxアプリ/XenMobileアプリは、iOS 10のバージョン10.3.10以降と互換性があります。 モバイルまたはエンタープライズアプリをラップして、iOS 10との適切な互換性を確保するには、MDX Toolkit 10.3.10以降を使用する必要があります。 iOS 10にアップグレードすると、MDXアプリを起動するためにWorx Home 10.3.10以降（Secure Hub）にアップグレードする必要があります。 詳しくは、こちらのSupport Knowledge Centerの記事を参照してください。

XenMobile 10.3.xおよび10.4

- iOS 10
- iOS 9.x
- iOS 8.x（MDM-only環境のWorx Home/Secure Hubのみ）

XenMobile 10.3.xおよび10.4がサポートするiOSデバイスの例：

- iPhone 6、6+、6S、6S+、5s、5、5c
- iPad 2、3
- iPad Air、iPad Air -2、iPad Mini-3、iPad Mini-2
- iPad Pro
- Mac OS X
  - MacBook、Air、Mini、Mini Retina 10.9.5、10.10、10.11

XenMobile 10および10.1

- iOS 10
- iOS 9.x
- iOS 8.x（MDM-only環境のWorx Homeのみ）

XenMobile 10および10.1がサポートするiOSデバイスの例：

- iPhone 5、5s、5c、6、6+
- iPad2、3、Mini、Air、Air2、Mini Retina

Windows PhoneおよびWindowsタブレット

XenMobile 10.3.xおよび10.4

- Windows 10、8.1タブレット
  - XenMobileがMAM-Onlyモードのみである場合、Windows 10タブレットはサポートされません。
- WindowsタブレットSurface Pro 3、Surface 2、RT
- Windows Phone 10、8.1
  - Windows Phone 10は、XenMobileのダウンロードページから修正プログラムをダウンロードしてインストールする必要があります。
  - XenMobileがMAM-Onlyモードのみである場合、Windows 8.1および10はサポートされません。
- Windows Phone 8.1のWorx Homeとの互換性：
  - XenMobileがエンタープライズモードの場合Worx Home 10.0。
  - XenMobileがMDM-onlyモードの場合Worx Home 9.1.0。
- Windows 8.1 ProおよびEnterprise Edition（32ビットおよび64ビット）
- Windows RT 8.1
- Windows Mobile/CE
  - XenMobileがMAM-Onlyモードである場合、Windows CEはサポートされません。

XenMobile 10.3がサポートするWindowsデバイスの例：

- Windows タブレット 10、8.1
- Windows Phone 10、8.1
- HTC（Windows Phone 8.1）
- Nokia 920、925、1020、1520（Windows Phone 8.1）
- WindowsタブレットSurface Pro 3
- WindowsタブレットSurface 2
- WindowsタブレットRT

XenMobile 10および10.1

- Windows 10タブレット
- Windows Phone 8.1 / 10：
  - XenMobileがMAM-onlyモードのみである場合、Windows Phone 8.1はサポートされません。
  - Windows Phone 10は、XenMobile 10.3以降でサポートされています。
  - Windows Phone 10は、XenMobile 9でサポートされます。ただし、Support Knowledge Centerの記事に記載されたDevice Manager Rolling Patchをインストールする必要があります。 Windows phone用のWindows 10 Anniversary Update Version 1607のパッチも記録する必要があります。 詳しくは、Support Knowledge Centerの記事を参照してください。
- Windows Phone 8.1のWorx Homeとの互換性：
  - XenMobileがエンタープライズモードの場合Worx Home 10.0
  - XenMobileがMDM-onlyモードの場合Worx Home 9.0.3
- Windows 8.1 ProおよびEnterprise Edition（32ビットおよび64ビット）
- Windows RT 8.1
- Windows Mobile：XenMobile 10.1では、Windows Mobileデバイスはサポートされません。 Windows MobileまたはWindows CEを実行しているデバイスのユーザーは、XenMobile 9を引き続き使用する必要があります。

XenMobile 10および10.1がサポートするWindowsデバイスの例：

- Windows 8.1タブレット
- HTC（Windows Phone 8.1）
- Nokia 920、925、1020、1520（Windows Phone 8.1）
- WindowsタブレットSurface Pro 3
- WindowsタブレットSurface 2
- WindowsタブレットRT

Windows Phone 7の管理は、XenMobile Mail Managerによって提供されます。 詳しくは、「XenMobile Mail Managerのインストール」を参照してください。

Symbian

XenMobile 10.3.xおよび10.4

XenMobile 10.3.xおよび10.4では、Symbianはサポートされません。

XenMobile 10および10.1

XenMobile 10.1および10でサポートされているSymbianデバイスもあります。 XenMobile 10で、デバイス管理機能のみサポートされているSymbianデバイス：

- Symbian 3
- Symbian S60 5th Edition
- Symbian S60 3rd Edition、Feature Pack 2
- Symbian S60 3rd Edition、Feature Pack 1
- Symbian S60 3rd Edition
- Symbian S60 2nd Edition、Feature Pack 3
- Symbian S60 2nd Edition、Feature Pack 2

BlackBerry

BlackBerryデバイスの管理は、XenMobile Mail Managerによって提供されます。 詳しくは、「XenMobile Mail Managerのインストール」を参照してください。

ポート要件

Oct 24, 2016

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

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

ユーザーがWorx Home、Citrix Receiver、およびNetScaler Gateway Plug-inからNetScaler Gateway経由でXenMobile、StoreFront、XenDesktop、XenMobile NetScaler Connector、およびイントラネットWebサイトなどのそのほかの内部ネットワークリソースに接続できるようにするには、次のポートを開く必要があります。 NetScaler Gatewayについて詳しくは、NetScaler Gatewayドキュメントの「XenMobile環境の設定の構成」を参照してください。 NetScaler IP（NSIP）仮想サーバーIP（VIP）、サブネットIP（SNIP）アドレスのようなNetScaler所有IPアドレスについて詳しくは、NetScalerドキュメントの「NetScalerとクライアント/サーバーとの通信方法」を参照してください。

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

389	セキュリティで保護されないLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはMicrosoft Active Directory
443	Citrix ReceiverからStoreFrontへの接続またはReceiver for WebからXenAppおよびXenDesktopへの接続に使用されます。	Internet	NetScaler Gateway
	Web、モバイル、およびSaaSアプリケーションの配信のためのXenMobileへの接続に使用されます。	Internet	NetScaler Gateway
	XenMobileサーバーとの一般的なデバイス通信に使用されます。	XenMobile	XenMobile
	登録のためにモバイルデバイスからXenMobileへの接続に使用されます。	Internet	XenMobile
	XenMobileからXenMobile NetScaler Connectorへの接続に使用されます。	XenMobile	XenMobile NetScaler Connector
	XenMobile NetScaler ConnectorからXenMobileへの接続に使用されます。	XenMobile NetScaler Connector	XenMobile
	証明書認証のない展開でのコールバックURLに使用されます。	XenMobile	NetScaler Gateway
514	XenMobileとsyslogサーバー間の接続に使用されます。	XenMobile	Syslogサーバー
636	セキュリティで保護されるLDAP接続に使用されます。	NetScaler Gateway XenMobile	LDAP認証サーバーまたはActive Directory
1494	内部ネットワーク内のWindowsベースのアプリケーションへのICAコネクションに使用されます。 このポートは開いたままにしておくことをお勧めします。	NetScaler Gateway	XenAppまたはXenDesktop
1812	RADIUS接続に使用されます。	NetScaler Gateway	RADIUS認証サーバー
2598	セッション画面の保持を使用した内部ネット	NetScaler Gateway	XenAppまたはXenDesktop

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

デバイスを管理するXenMobileポートの開放

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

TCPポート	説明	接続元	接続先
25	XenMobile通知サービスのデフォルトのSMTPポート。SMTPサーバーで別のポートを使用する場合は、そのポートがファイアウォールによってブロックされないことを確認してください。	XenMobile	SMTPサーバー
80、443	Apple iTunes App Store（ax.itunes.apple.com）、Google Play（80を使用する必要があります）、またはWindows Phone StoreへのEnterprise App Store接続。 iOS上のCitrix Mobile Self-Serve、Worx Home for Android、またはWorx Home for Windows Phoneを介してアプリケーションストアからアプリケーションを公開するために使用されます。	XenMobile	Apple iTunes App Store（ax.itunes.apple.comおよび*.mzstatic.com） Apple Volume Purchase Program（vpp.itunes.apple.com） Windows Phoneの場合：login.live.comおよび*.notify.windows.com Google Play（play.google.com）
80または443	XenMobileとNexmo SMS Notification Relay間の送信接続に使用されます。	XenMobile	Nexmo SMS Relay Server
443	AutoDiscoveryサーバーへの発信接続のために使用されます。	XenMobile	https://discovery.mdm.zenprise.com
443	AndroidおよびWindows Mobileの登録およびエージェント設定に使用されます。	Internet	XenMobile
	AndroidおよびWindowsデバイス、XenMobile Webコンソール、およびMDM Remote Support Clientの登録およびエージェント設定に使用されます。	内部LANおよびWiFi	
1433	デフォルトで、リモートデータベースサーバーへの接続に使用されます（オプション）。	XenMobile	SQL Server
2195	iOSデバイスの通知およびデバイスポリシーのプッシュのためのgateway.push.apple.comへのApple Push Notification	XenMobile	インターネット（パブリックIPアドレス17.0.0.0/8を使用している

TCPポート	説明	接続元	接続先
2196	サービス（APNs）送信接続に使用されます。 iOSデバイスの通知およびデバイスポリシーのプッシュのためのfeedback.push.apple.comへのAPNs送信接続に使用されます。		APNsホスト）
5223	Wi-Fiネットワーク上のiOSデバイスから*.push.apple.comへのAPNs送信接続に使用されます。	WiFiネットワーク上のiOSデバイス	インターネット（パブリックIPアドレス17.0.0.0/8を使用しているAPNsホスト）
8443	iOSおよびWindows Phoneデバイスの登録に使用されます。	Internet	XenMobile
		LANおよびWiFi	

自動検出サービスの接続のポート要件

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

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

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

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

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

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

完全修飾ドメイン名	IPアドレス
	54.225.219.53
	54.243.185.79

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

FIPS 140-2への準拠

May 10, 2016

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

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

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

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

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

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

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

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

XenMobileの言語サポート

May 10, 2016

Citrix WorxアプリケーションおよびXenMobileコンソールは英語以外の言語での使用にも適応しています。これには、アプリケーションがユーザーの優先言語にローカライズされていない場合でも、英語以外の文字およびキーボード入力のサポートが含まれます。

Worxアプリケーションの言語サポート

次の表では、Worxアプリケーションでサポートしている言語について、○で示しています。

ユーザーインターフェイス言語	日本語	簡体字中国語	ドイツ語	フランス語	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
Apple iPhone/iPad												
Worx Home	○	○	○	○	○	○	○	○	○	○	○	○
WorxMail	○	○	○	○	○	○	○	○	○	○	○	○
WorxWeb	○	○	○	○	○	○	○	○	○	○	○	○
WorxNotes	○	○	○	○	○	○	○	○	○	○	○	○
WorxTasks	○	○	○	○	○	○	○	○	○	○	○	○
QuickEdit	○	○	○	○	○	○	○	○				
Androidスマートフォン/タブレット												
Worx Home	○	○	○	○	○	○	○	○	○	○	○	○
WorxMail	○	○	○	○	○	○	○	○	○	○	○	○
WorxWeb	○	○	○	○	○	○	○	○	○	○	○	○
WorxNotes	○	○	○	○	○	○	○	○	○	○	○	○
WorxTasks	○	○	○	○	○	○	○	○	○	○	○	○

QuickEdit	○	○	○	○	○	○	○	○			
Windows Phone											
Worx Home			○	○	○				○	○	○
WorxMail			○	○	○				○	○	○
WorxWeb			○	○	○				○	○	○

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

XenMobileコンソールの言語サポート

次の表では、ローカライズされているXenMobileコンソールの言語を○で示しています。

ユーザーインターフェイス言語	簡体字中国語	ドイツ語	フランス語	韓国語	ポルトガル語
XenMobileコンソール	○	○	○	○	○

右から左書きのサポート機能

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

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

インストール前のチェックリスト

May 10, 2016

このチェックリストを使用して、XenMobile 10をインストールするための前提条件と設定を記録できます。各タスクまたは注には、要件が適用されるコンポーネントまたは機能を示す列があります。インストール手順については、「XenMobileのインストール」を参照してください。

ネットワークの基本的な接続

以下はXenMobileソリューションに必要なネットワーク設定です。

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

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

ライセンス管理

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

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

証明書

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

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

ポート

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

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

データベース

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

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

Active Directoryの設定

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

XenMobileとNetScaler Gatewayの間の接続

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

✓	ファイルリポジトリURLを記録します。	XenMobile コンポーネント	設定の記録

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

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

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

既知の問題

May 10, 2016

XenMobile 10.0の既知の問題は次のとおりです。

このリリースで解決した問題については、http://support.citrix.com/article/CTX141722を参照してください。

- iOSデバイスをiOS 7からiOS 8に更新して再起動すると、Worx Homeでアイコンの代わりに灰色のプレースホルダーが表示される場合があります。 これはサードパーティ製品の問題です。 [#502879]
- 登録中、iOSデバイスでモバイルデバイス管理（MDM）プロファイルのインストール中またはインストール後に、エラーが発生する場合があります。 iOS 8.1を実行しているデバイスでは「Cocoa error 4097」と表示され、それより前のバージョンのiOSを実行しているデバイスでは「Profile cannot be decrypted」と表示されます。 この問題が発生した場合、登録を再試行する必要があります。 場合によっては、再試行が2回以上必要なことがあります。 [#507948]
- XenMobile 10では、USERグループクラスでcheckUserPasswordおよびaddGroup SOAPの呼び出しを行うことができません。 ユーザーAPIの変更は、データベースには反映されますが、デバイスのユーザーインターフェイスには反映されません。 [#511551、#511822]
- XenMobile Webコンソールから、デリバリーグループリソースの展開順序を変更することはできません。 展開順序を制御するには、XenMobileが使用する展開順序に合わせ、数値（1、2、3、...）、 大文字 アルファベット（A、B、C、...）、小文字アルファベット（a、b、c、...）の順序になるよう、リソース名を変更します。 たとえば、「24」で始まる名前のリソースは、「WM」で始まる名前のリソースより先に展開され、いずれも 「tw」で始まります。 [#512566]
- アダルトコンテンツフィルター制限が有効になっている場合は、Windows Phone 8.1デバイスのセーフサーチが無効化されて［標準］に設定されます。 [#513605]
- Windows 8.1タブレットのデバイスポリシーを展開するとき、デバイスからのポリシーの実行の確認をXenMobileで受信する前に、XenMobileコンソールの［Device details］の［Deployed］タブにポリシーが表示される場合があります。 [#514749]
- デバイスの再登録で、ユーザーが登録解除してから再登録するまでの時間が短すぎる場合、登録が失敗する場合があります。 [#516567]
- 場合によっては、ユーザーがWorx Homeで再登録するときに、XenMobileでキャッシュされたSSLセッションが表示され、登録画面がもう一度表示されることがあります。 この問題が発生した場合、再登録をもう一度実行する必要があります。 [#517301]
- 親ドメインおよび子ドメインに属するActive Directoryグループを対象にAND演算子を使用してデリバリーグループが定義されている場合、アプリケーション列挙が失敗します。 これを避けるには、デリバリーグループを定義するときにOR演算子を使用してください。 [#518084]
- XenMobileコンソールで設定またはポリシーを構成し、そこでファイル（証明書、PDF、フォントなど）をアップロードした場合、後でそのポリシーまたは設定の詳細を表示すると、ファイル名が表示されません。 [#519552]
- XenMobileは、iOSデバイスおよびAndroidデバイスのモバイルアプリケーション管理（MAM）モードでのPINによる認証をサポートしていません。 XenMobileコンソールでこのモードをデフォルトにして構成した場合、ユーザーはWorx Homeで資格情報を2回入力する必要があります。 [#519572]
- XenMobileコンソールで、AllUsersグループをデリバリーグループとして無効にすると、いずれのデリバリーグループにも属していないユーザーはデバイスを登録できませんが、 Self Help Portalにはログオンできます。 [#521393]
- Worx Home for Windows Phone 8.xは、モバイルデバイス管理モードでは、アプリケーションがオプションとして展開されている場合、公開ストアからのアプリケーションのみをサポートします。 これらのアプリケーションが必須としてデリバリーグループに追加されている場合、Worx Homeでは表示されません。 [#521524]
- ［Role-Based Access Control (RBAC) Role Info］ページを開くと、デフォルトのAdminテンプレートを編集できます。 ［RBAC template］ フィールドや そのほかのオプションを変更しても、これらの変更はAdminテンプレートに保存されません。 Adminテンプレートは、編集できないように設計されています。 [#521540]
- iOSデバイスで、ユーザーがWorx Homeに登録してShareFileアカウントを構成する場合、SAMLトークンのプロビジョニク

は同期しないことがあります。 この問題を解決するには、ユーザーがWorx Homeをサインオフしてからもう一度サインインし、その後でSAMLトークン要求を再度トリガーするためにShareFileアプリにログオンします。 [#521934]

- Androidを実行しているほとんどのデバイスでは、メニューアイコンをタップすると［Accept and Decline］メニューオプションが表示され、登録処理を続けることができます。 しかし、Samsung Tablet GT-P7510など、4.0より前のオペレーティングシステムを実行している一部のデバイスでは、デフォルト表示の［Terms and Conditions］ページでメニューアイコンが表示されず、登録処理を完了することができません。 回避策として、これらのデバイスを契約条件の展開から除外することができます。 [#524039]
- XenMobile コンソールの［Beacons］ページ（［Configure］>［Settings］>［More］>［Beacons］）でデフォルトのストア名を変更した場合、iOSデバイスのWorx HomeがWorx Storeに接続できません。 デフォルトの設定は［Store］です。この設定が変更されている場合、 ログオン に探索サービスが失敗してWorx Storeが見つかりません。 このエラーを回避するには、［Beacons］ページの［Store name］設定を［Store］のままにしておいてください。 [#523306]
- 負荷分散とSSLオフロードを伴うXenMobile構成では、SAMLアプリを構成すると、ユーザーがWorxWebをインストールしてサービスプロバイダー側開始のアプリを開く時にシングルサインオン（SSO）を実行するため、XenMobileサーバーに対するすべてのリファレンスがポート443の代わりにポート8443をポイントする必要があります。 [#528680]
- Samsung KNOXパスコードポリシーを作成するときに、［Lock device after (minutes of activity)］設定を構成すると、コンソールの設定は分単位で示されますが、サーバーのロックは秒単位で適用されます。 [#531204]
- XenMobile 10で、ユーザーとデバイスを認証するために独自のSAMLサービスおよびIDプロバイダーを構成することはできません。 [#530892]
- XenMobileコンソールで、BlackBerryデバイスまたはWindowsデバイスを1つだけ追加することはできません。 [#532844]
- シャープ記号（#）を含む名前の SAML アプリケーションを構成した場合、Worx Homeからのシングルサインオン（SSO）が機能せず、エラーメッセージが表示されます。 [#533078]
- XenMobileコンソールで汎用PKI（GPKI）エンティティを追加する場合、Web Services Description Language（WSDL）URLアダプター接続を構成中にテストすることができません。 [#533871]
- Windowsタブレットのパスワードポリシーがデバイスで直ちには有効にならず、 パスワードの 最小文字数に対する更新の適用でいくつか不整合が発生します。 これはサードパーティ製品の問題です。 [#534088]
- ユーザーがiOSデバイスをモバイルデバイス管理（MDM）モードで登録した場合、デバイスの検索と追跡を行うためのXenMobileコンソールの［Manage］>［Devices］ページで、［Security］オプションがすぐには表示されません。 このオプションは、少し遅れて表示されます。 [#534672]
- ピリオド（.）などの特殊文字を含む名前のStoreFront Delivery Controller表示名を構成すると、ユーザーがWorx HomeからXenAppでアプリケーションをサブスクライブしたり開いたりすることができません。「Cannot complete your request」というエラーメッセージが表示されます。 回避策としては、特殊文字を名前から削除します。 [#535497]
- アプリケーションを追加および構成するとき、XenMobileコンソールの［Excluded devices］フィールドに値を入力すると、iOS 8より前のiOSデバイスにおいて、アプリケーションがWorx Storeで表示されません。 回避策として、展開規則を構成してアプリケーションをインストール可能なデバイスを指定できます。 [#537631]
- デフォルトの443以外のポートでXenMobileとのNetScaler Gateway接続を構成すると、Windowsデバイス上のWorx Home同様に、iOSデバイスでモバイルアプリケーション管理（MAM）登録が失敗します。 [#537368]
- XenMobile 10のインストール時のCLIパスワード、および証明書に割り当てられるパスワードでは、$、@、"のような特殊文字は認識されません。特殊文字とその後に続く文字はすべて無視され、ログオンに失敗します。 インストール後は、特殊文字を含めるためにCLIパスワードを変更することはできません。 [#541997, #542436]
- XenMobileでiOSデバイス登録プログラムを構成しようとすると、無効なプロファイルエラーが発生します。 これはサードパーティ製品の問題です。 [#608213]

XenMobile Mail Manager 10.0の既知の問題は次のとおりです。

- XenMobile Mail Manager 10にアップグレードする間、インストールされたXenMobile Mail Managerのバージョンは常に8.5として表示されます。ただし、XenMobile Mail Managerのアップグレードは実行されます。[#539520]
- マイナースナップショットの“devices found”報告で混乱が生じることがあります。マイナースナップショットがメジャースナップショットの開始に引き続いて実行される場合、連続したマイナースナップショットの概要では同じデバイス

が“new”として報告されることがあります。

XenMobileのインストール

Oct 24, 2016

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

開始前：XenMobile展開を計画する場合は、多くの検討事項があります。 エンドツーエンドXenMobile環境の推奨事項、よくある質問、およびユースケースについては、『XenMobile展開ハンドブック』を参照してください。 「XenMobile 10のシステム要件」およびXenMobile 10インストール前のチェックリストについても参照してください。
注：XenMobileはハイパーバイザーの時刻を使用するため、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。

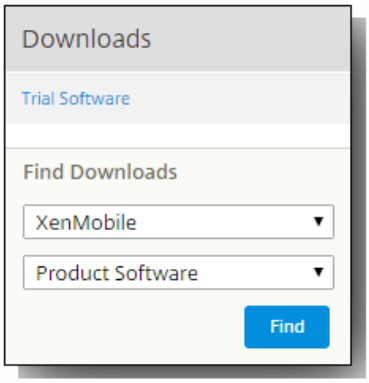
Hyper-Vの前提条件：XenMobileをHyper-Vにインストールする前に、以下を実行する必要があります。 詳しくは、Hyper-Vのドキュメントを参照してください。

- 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。

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

XenMobile製品ソフトウェアのダウンロード

Citrixの製品ソフトウェアは、CitrixのWebサイトからダウンロードできます。CitrixのWebサイトにログオンして、[ダウンロード] リンクをクリックします。次に、製品および種類を選択します。下の図は、XenMobileと製品ソフトウェアを一覧で選択したところを示しています。



[検索] をクリックすると、ダウンロード可能な製品の一覧が表示され、最新のバージョンが一覧の上位に表示されます。こ

の一覧で、ダウンロードするソフトウェアを選択します。

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. ［マイアカウント］をクリックしてログオンします。
3. ［ダウンロード］をクリックします。
4. ［ダウンロードの検索］の製品一覧で、［XenMobile］を選択します。
5. ［ダウンロードの検索］のダウンロードタイプ一覧で［ソフトウェア製品］をクリックして、［検索］をクリックします。
6. ［XenMobile Product Software］ページで、ダウンロードするXenMobile 10.0のエディションをクリックします。
7. ［XenMobile 10.0 Edition］ページで、XenServer、VMware、またはHyper-Vにインストールする適切なXenMobile仮想イメージの［ダウンロード］をクリックします。
8. 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. ［マイアカウント］をクリックしてログオンします。
3. ［ダウンロード］をクリックします。
4. ［ダウンロードの検索］の製品一覧で、［NetScaler Gateway］をクリックします。
5. ［ダウンロードの検索］のダウンロードタイプ一覧で［ソフトウェア製品］をクリックして、［検索］をクリックします。
   注：ここで［Virtual Appliances］をクリックしてNetScaler VPXをダウンロードすることもできます。この場合、対象のハイパーバイザーを選択するためのページが開きます。
6. ［NetScaler Gateway］ページで、［10.5(4)］を展開します。
7. 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。
8. ダウンロードするバージョンのアプライアンスソフトウェアのページで、適切な仮想アプライアンスの［ダウンロード］をクリックします。
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。

初回使用時のXenMobileの構成

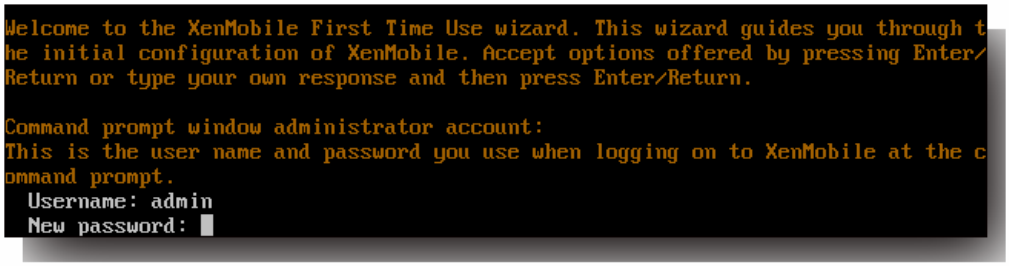
初回使用時のXenMobileの構成プロセスは2つの部分から成ります。

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

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

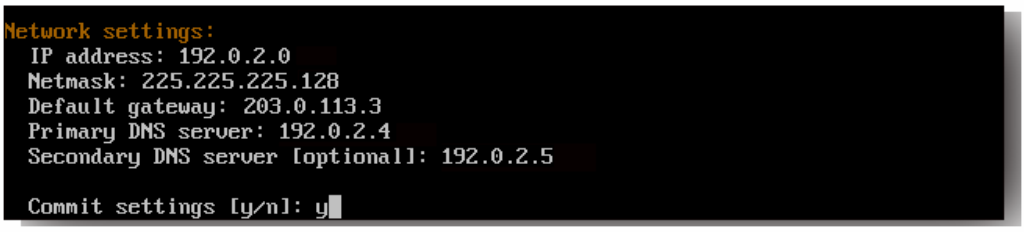
コマンドプロンプトウィンドウでのXenMobileの構成

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



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。

4. 次の情報を指定します。
   1. IPアドレス
   2. ネットマスク
   3. デフォルトゲートウェイ
   4. プライマリDNSサーバー
   5. セカンダリDNSサーバー（オプション）



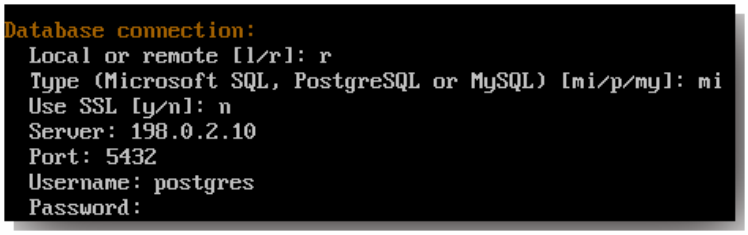
注：この図に示されているアドレスは使用されておらず、例示のみを目的としています。

5. 「y」を入力して、セキュリティを高めるためにランダムな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。書き込みを表示することはできません。

注：環境の拡張を意図していて、追加のサーバーを構成する場合は、自分のパスフレーズを指定する必要があります。ランダムなパスフレーズを選択した場合、パスフレーズを表示する方法はありません。

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

7. データベース接続を構成します。 データベースはローカルでもリモートでも構いません。[Local or remote]が表示されたら、「r」または「l」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。



   重要：デフォルトのPostgreSQL用ポートは5432です。

   注：この図に示されているアドレスは使用されておらず、例示のみを目的としています。
8. 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。

   重要：サーバーの再インストールを完了せずにFQDNを変更することはできません。

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

```
HTTP [80]: 80
HTTPS with certificate authentication [443]: 443
HTTPS with no certificate authentication [8443]: 8443
HTTPS for management [4443]: 4443
```

10. すべてのPKI（Public Key Infrastructure：公開キーのインフラストラクチャ）サーバー証明書のパスワードの入力を求めるメッセージが表示されます。各証明書に同じパスワードを使用するように選択することもできます。 XenMobile PKI機能について詳しくは、「XenMobileでの証明書のアップロード」を参照してください。
重要：XenMobileのノード（インスタンス）をまとめてクラスター化する場合は、後続ノードで同じパスワードを入力する必要があります。

```
The wizard will now generate an internal Public Key Infrastructure (PKI):
 - A root certificate
 - An intermediate certificate to issue device certificates during enrollment
 - An intermediate certificate to issue an SSL certificate
 - An SSL certificate for your connectors
  Do you want to use the same password for all the certificates of the PKI [y]:
  New password:
  Re-enter new password:
```

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。

11. 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。

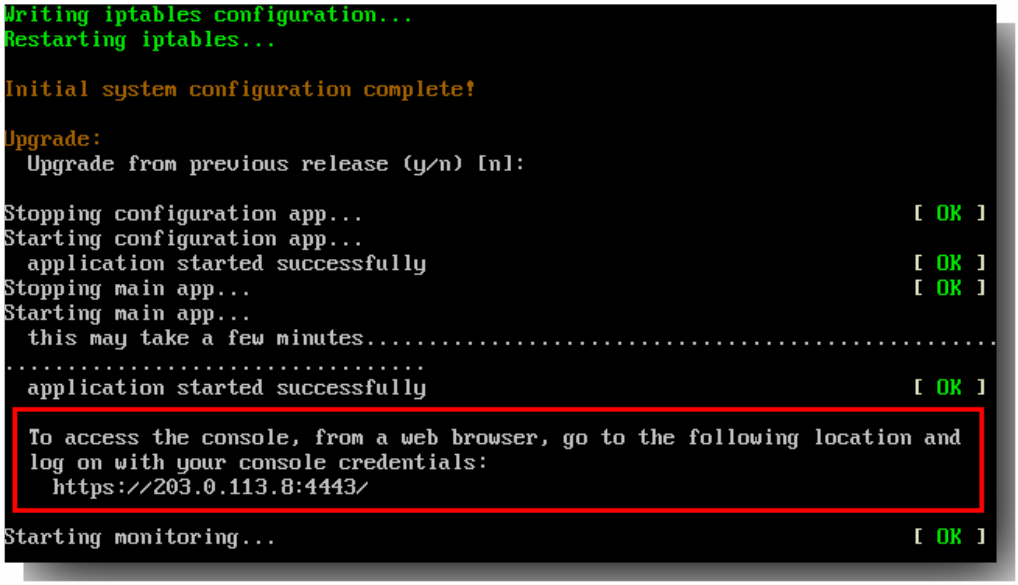
```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile cons
ole through a web browser.
  Username [administrator]: administrator
  Password:
  Re-enter new password:
```

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。

12. 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。

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

13. 画面に表示されたURL全体をコピーして、このXenMobile初期構成をWebブラウザーで続行します。



WebブラウザーでのXenMobileの構成

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

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

3. ［Get Started］ページで［Start］をクリックします。［Licensing］ページが開きます。
4. ライセンスを構成します。XenMobileには30日間有効な評価版ライセンスが付属しています。ライセンスの追加と構成、および有効期限切れ通知の構成について詳しくは、「XenMobileのライセンス」を参照してください。
   重要：XenMobileのノード（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。
5. ［Certificate］ページで、［Import］をクリックします。［Import］ダイアログボックスが開きます。

6. APNとSSLリスナー証明書をインポートします。 証明書の取り扱いについて詳しくは、「XenMobileでの証明書」を参照してください。
   注：SSLリスナー証明書では、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。
   注：NetScaler Gatewayはオプションの設定ですが、ページでのデータ入力後にそのページから移動するには、必須フィールドを消去するか入力する必要があります。
8. Active Directoryからのユーザーとグループにアクセスするため、LDAP構成を完了します。 LDAP接続の構成について詳しくは、「LDAP構成」を参照してください。
9. 通知サーバーを構成して、ユーザーにメッセージを送信できるようにします。 通知サーバー構成について詳しくは、「XenMobileでの通知」を参照してください。

XenMobileでのFIPSの構成

May 10, 2016

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

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

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

FIPSモードの構成

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

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

1. セットアップ時に**FIPSモード**を有効にします。

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

    a.CA証明書をコピーして貼り付けます。

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

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

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

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

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

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

証明書のインポート

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

SQLの前提条件

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

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

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

    b.SQL ServerでMMC.exeを開きます。

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

    d.［**OK**］をクリックします。

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

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

    g.［**グループ名またはユーザー名**］で［**追加**］をクリックします。

    h.前の手順でコピーしたSQLサービスアカウント名を入力します。

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

    j.**MMC**を閉じ、SQLサービスを開始します。

3. SQLサービスが正常に開始されたか確認します。

インターネットインフォメーションサービス（IIS）の前提条件

1. ルート証明書（base 64）をダウンロードします。

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

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

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

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

6. .cerがブロックされていないか確認します。

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

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

a.Server Managerを開きます。

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

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

d. **[次へ]** をクリックしてインストールを完了させます。

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

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

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

初期FIPS構成中のルート証明書のインポート

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

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

XenMobile 10 MDMアップグレードツール

May 10, 2016

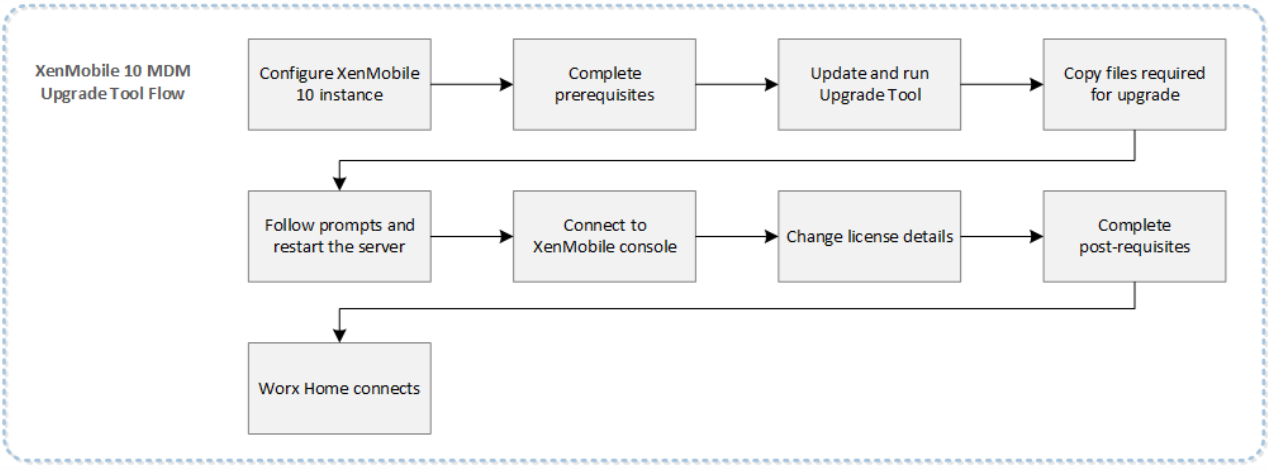
> ## 注意
>
> 最新バージョンのアップグレードツールを使用することをお奨めします。最新バージョンのアップグレードツールを使うと、1つのツール内でXenMobile 9.0環境のMAM、MDM、およびEnterpriseモードを更新できます。Citrix.comのダウンロードページで、アップグレードツールを入手できます。

XenMobile 10 MDMアップグレードツールを使用して、XenMobile 9.0からXenMobile 10にアップグレードします。このツールでは、XenMobile MDMエディションの展開からのアップグレードがサポートされます。

重要：このツールを使用してXenMobile App EditionまたはXenMobile Enterprise Editionからアップグレードすることは、サポートされません。同様に、このツールはXenMobile 8.6または8.7からXenMobile 10へのアップグレードには使用できません。さらに、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XenMobile 10に移行できません。
XenMobile 9.0セットアップが名前付きSQLインスタンスをベースとしたものである場合は、この状況に特化した次の手順を実行する必要があります。詳しくは、「名前付きSQLインスタンスのサポート」を参照してください。

アップグレードツールは、XenMobile 10仮想マシン内で構築されます。XenMobile 10の初回インストール中にコマンドラインコンソールを使用して1回のみのウィザードを有効にします。

次の図は、XenMobile 9.0からXenMobile 10に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。



XenMobile 10への移行を開始する前に、「前提条件」および「既知の問題」を参照してください。

アップグレードツールで実行される内容

XenMobile 10 MDMアップグレードツールでは、同じ完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）のXenMobile 9.0サーバーからXenMobile 10の新しいインスタンスに構成とユーザーデータが移行されます。

アップグレードを試行することも、完全な実稼働環境のアップグレードを実行することもできます。ツールで[Test

Drive］を選択すると、構成データのみがXenMobile 10に移行されます。デバイスとユーザーデータは移行されません。このオプションでは、実稼働環境に影響を与えずに、XenMobile 9.0とXenMobile 10を比較できます。

ツールで［Production Upgrade］を選択すると、構成、デバイス、およびユーザーデータがすべて移行されます。アップグレード後にXenMobile 10コンソールにログオンすると、XenMobile 9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。

注：これはインプレース移行ではありません。すべてのデータは、移動ではなく、XenMobile 10に*コピー*されます。XenMobile 10サーバーが実稼働に移行するまで、XenMobile 9.0のすべてのデータはそのまま保持されます。ユーザーが実稼働環境のXenMobile 10に接続した後で、何らかの理由でXenMobile 9.0に戻す場合は、そのユーザーはXenMobile 9.0に再登録する必要があります。
実稼働環境のアップグレードが成功した後で、XenMobile 10を実際の稼働環境に移行するには、次の操作を実行する必要があります。

1. DNSエントリを更新して、XenMobile 9.0のFQDNを、新しいXenMobile 10サーバーのIPアドレスにマップします。
2. NetScalerでXenMobile Device Managerサーバーの負荷を分散している場合は、XenMobile 9.0サービスをXenMobile 10サービスに切り替える必要があります。

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XenMobile 10に移行**されません**。

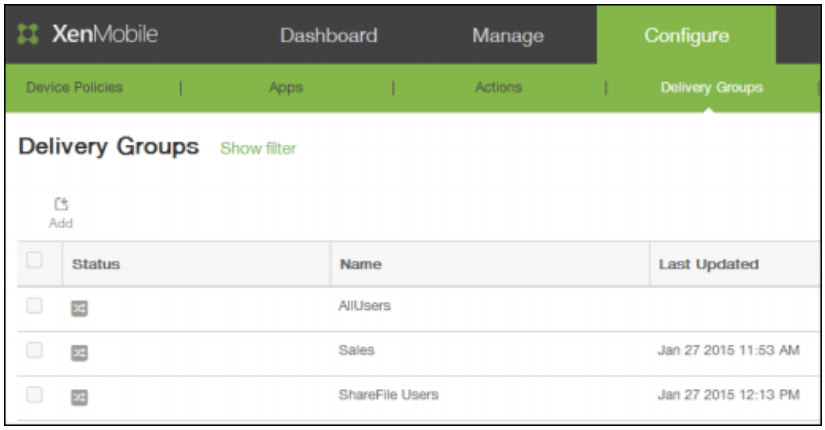
- ライセンス情報
- レポートのデータ
- 自動化された操作
- サーバーグループポリシーとそれに関連する展開
- MSPグループ
- Windows CEとWindows 8.0に関連するポリシーおよびパッケージ
- 使用していない展開パッケージ（展開パッケージにユーザーまたはグループが割り当てられていない場合など）
- migration.logファイル内に記述されている、そのほかの構成またはユーザーデータ
- CXM Web（Citrix WorxWebに置き換えられます）
- DLPポリシー（Citrix Sharefileに置き換えられます）
- カスタムのActive Directoryの属性
- 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移行されません。XenMobile 10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XenMobile 10に移行するには、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。XenMobile 10のコンソールへのアクセスの制限は、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。

XenMobile 10での次の変更点にも注意してください。

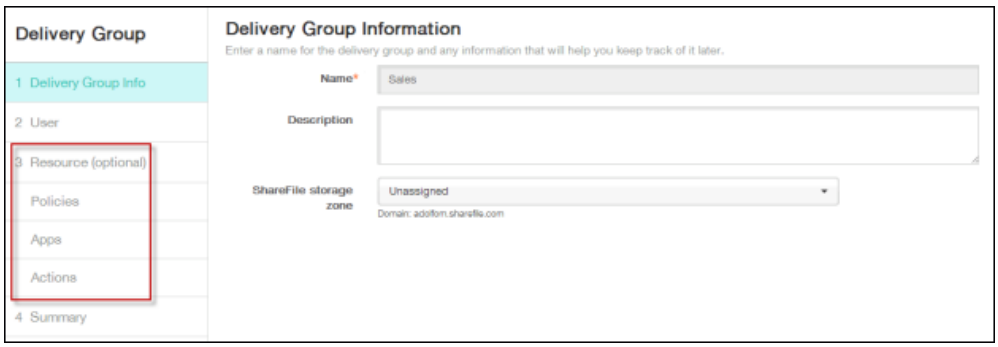
- XenMobile 10では、ローカルグループに割り当てられたActive Directoryユーザーはサポートされません。
- ローカルグループの階層はフラットです。

XenMobile 10での用語の変更

次の図に示すように、アップグレード後、Device Managerの展開パッケージはデリバリーグループと呼ばれます。詳しくは、「デリバリーグループの管理」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MDMポリシー、操作、およびアプリケーションを表示できます。

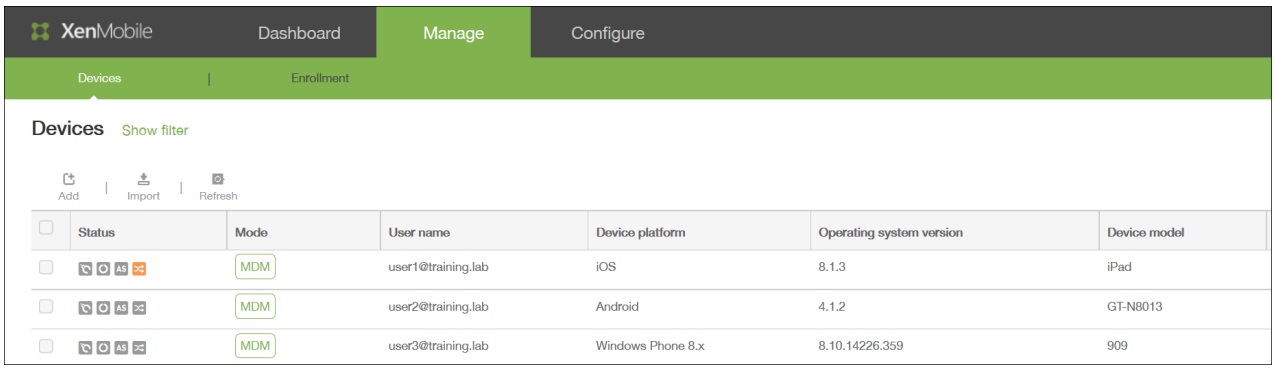


アップグレード後のデバイス登録

ユーザーは、XenMobile 10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、XenMobile 10サーバーに自動的に接続されます。

すぐにデバイスをXenMobile 10に接続する場合は、デバイスで、［WorxHome］［デバイス情報］［ポリシーの更新］を使用します。

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。



前提条件

May 10, 2016

XenMobile 10 MDMアップグレードツールを実行する前に、以下の前提条件を満たす必要があります。

Citrixライセンスサーバー

Citrixライセンスサーバー11.12.1（「Citrix Licensing」ページから取得可能）をインストールして、最新のV6 MDMのみのライセンスでサーバーを構成していることを確認します。サーバーに対して、ライセンスサーバーのポート27000および7279が開いていることを確認します。XenMobile Enterpriseモードへのユーザーのデバイスの意図しないアップグレードが実行されて、ライセンス違反が発生し、ユーザーにデバイスの再登録が強制されることを防ぐため、この手順は必須です。

データベース

移行は、同じ種類のデータベース間でのみ行うことができます。次に例を示します。

サポートされます

- PostgreSQLからPostgreSQL
- MSSQLからMSSQL

サポートされません

- MSSQLからPostgreSQL
- PostgreSQLからMSSQL

XenMobileは、データ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. 新しい行を追加します" hostall all[XMS address/external address]/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ファイルを見つけて開き、行
   "#listen_addresses = 'localhost'"

   を次のように変更します

   "listen_addresses = '*'"

   注：行にはコメントを付けないようにする必要があります。これは、XenMobile 9.0とXenMobile 10サーバーのIPのみに対してPostgreSQLデータベースへのアクセスを許可することで（listen_addresses = '10.x.x.1,10.x.x.2'制限できます。
6. 変更が反映されるようにPostgreSQLサービスを停止してから開始します。
7. XMSとデータベースがお互いに通信するか確認してください（これにより、データベースがリモート接続を受け付けることができるかもチェックされます）。

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 10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。

外部SSL証明書

外部SSL証明書が、「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。移行を開始する前に、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。

管理者アカウントユーザー名

XenMobile 10コンソールへのログオンに使用される管理者アカウントには、小文字のみを指定できます。アカウントに大文字が含まれていると、移行後にXenMobile 10コンソールにログインできません。すべて小文字で管理者のユーザーアカウントを作成し、すべての権限を有効にして、移行後にそのアカウントを使用してXenMobile 10コンソールにログオンできるようにします。

特殊文字を含む展開パッケージ名

特殊文字（!、$、()、#、%、+、*、~、?、|、{}、および[]）を含む、XenMobile 9.0の展開パッケージ名は移行しますが、移行後にXenMobile 10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、開き角かっこ（[）を含むローカルユーザーおよびローカルグループにより、XenMobile 10で登録招待状を作成するときに問題が発生します。移行前に、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。

XenMobile 9.0 Device Managerからのファイルのコピー

Device Managerがデフォルトの場所（C:\Program Files(x86)\Citrix\XenMobile Device Manager\tomcat）にインストールされている場合は、以下のファイルを一時フォルダーにコピーします。

C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\confフォルダーにある以下のファイル

- server.xml
- https.p12
- cacerts.pem.jks
- pki-ca-root.p12
- pki-ca-devices.p12
- pki-ca-servers.p12

注：Device Managerを実行していたサーバーでカスタムサーバーのSSLサーバー証明書（.p12）が使用されていた場合は、https.p12ではなく、その証明書を一時フォルダーにコピーします。
C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\webapps\zdm\WEB-INF\classes\フォルダーから、以下のファイルを同じ一時フォルダーにコピーします。

- ew-config.properties
- pki.xml
- variables.xml

上記のファイルをすべてコピーしたら、一時フォルダーを開き、ファイルを圧縮します。その一時フォルダーではなく、ファイルのみを圧縮します。圧縮されたファイルは、アップグレード中にアップロードされます。

既知の問題を理解し、すべての前提条件を満たしている場合に、アップグレードを開始します。詳しくは、「XenMobile 10 MDMアップグレードツールの有効化と実行」を参照してください。

既知の問題

May 10, 2016

XenMobile 10 MDMアップグレードツールの既知の問題は次のとおりです。

- XenMobileのロックアウト制限値は移行されません。移行後に、値を再設定します。[#545770]
- 役割ベースのアクセス制御（role-based access control：RBAC）の役割のオプションは正確に移行されません。移行後に、RBACの役割を確認して、必要な調整を行います。[#543183]
- ログの設定は移行されません。移行後に、XenMobileコンソールでログの設定を再構成します。[#541869]
- 複数のLDAP構成を持つ構成が移行され、その中にネストされたグループをサポートするLDAP構成が1つのみある場合、移行後に、構成したすべてのLDAPでネストされたグループのサポートが有効になります。さらに、すべてのLDAPサーバーで、サーバーの起動時にグループの同期が実行されます。[#540713]
- WebコンテンツフィルターのデバイスポリシーにHTTPまたはHTTPSのないURLが含まれる場合は、ユーザーがURLを編集して操作を取り消すと、URLが削除されます。移行後、すべてのURLにHTTPまたはHTTPSが含まれるようにし、編集操作の取り消しで削除されないようにします。[#540025]
- さまざまな規則を含む複数のパッケージにポリシー、アプリケーション、または操作が含まれる場合、展開規則が移行されません。これは意図された動作です。[#539517]
- XenMobile 9.0管理者のユーザー名に大文字が含まれる場合、移行に成功すると、その管理者はXenMobile 10コンソールにログオンできません。移行前に、すべて小文字で管理者のユーザーアカウントを作成し、すべての権限を有効にして、移行後にそのアカウントを使用してXenMobile 10コンソールにログオンできるようにします。[#547422]
- XenMobile 9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XenMobile 10に移行できません。[#549969]
- XenMobile 9.0で作成されたスーパー管理者の役割のいくつかの設定と割り当て権限は、XenMobile 10に移行されません。移行後に、XenMobile 10コンソールで、［Configure］、［Settings］、［Role Based Access Control］の順に選択し、XenMobile 10管理者の役割の権限を使用してXenMobile 9.0スーパー管理者の役割を再作成します。[#553079]

- XenMobile 9.0で作成された、特殊文字（:、!、$、()、#、%、+、*、~、?、|、{}、および[]）を含む展開パッケージ名は、移行後に編集できません。さらに、XenMobile 9.0で作成された、開き角かっこ（[）を含むローカルユーザーおよびローカルグループにより、XenMobile 10で登録招待状を作成するときに問題が発生します。移行前に、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。[#538639

XenMobile 10 MDMアップグレードツールの有効化および実行

May 10, 2016

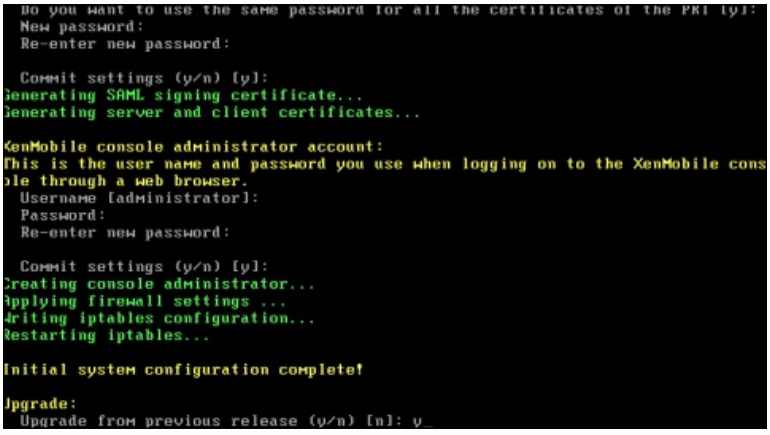
以下は、XenMobile 9.0からXenMobile 10にアップグレードする場合に実行する基本的な手順です。

1. コマンドラインコンソールを使用して、XenMobile 10インスタンスを構成します。
2. アップグレードツールのすべての前提条件を満たします。 詳しくは、 「前提条件」を参照してください。
3. アップグレードツールを最新バージョンに更新します。
   重要：システムの再起動後にブラウザーのキャッシュを消去します。
4. FirefoxまたはChromeでアップグレードツールを起動します。
5. XenMobile 9.0ファイルのコピーをアップグレードツールにアップロードします。
6. XenMobile 9.0の証明書パスワードを入力します。
7. アップグレードツールの実行を許可します。
8. XenMobile 10サーバーを再起動します。
9. XenMobile 10コンソールにログオンします。
10. XenMobile 10でライセンスを構成して、ユーザーの接続を許可します。
11. 実稼働環境のアップグレードの場合は、XenMobileの外部DNSを、新しいXenMobile 10サーバーを指すように変更します。
12. 実稼働環境のアップグレードで、負荷分散NetScalerを使用している場合は、XenMobile 9.0サーバーのIPを削除してXenMobile 10サーバーのIPを追加します。

XenMobile 10のインスタンスをインストールしてアップグレードツールを有効にするには

次の図に示すように、XenMobile 10の初期インストール中に、コマンドラインコンソールを使用してアップグレードツールを有効にします。

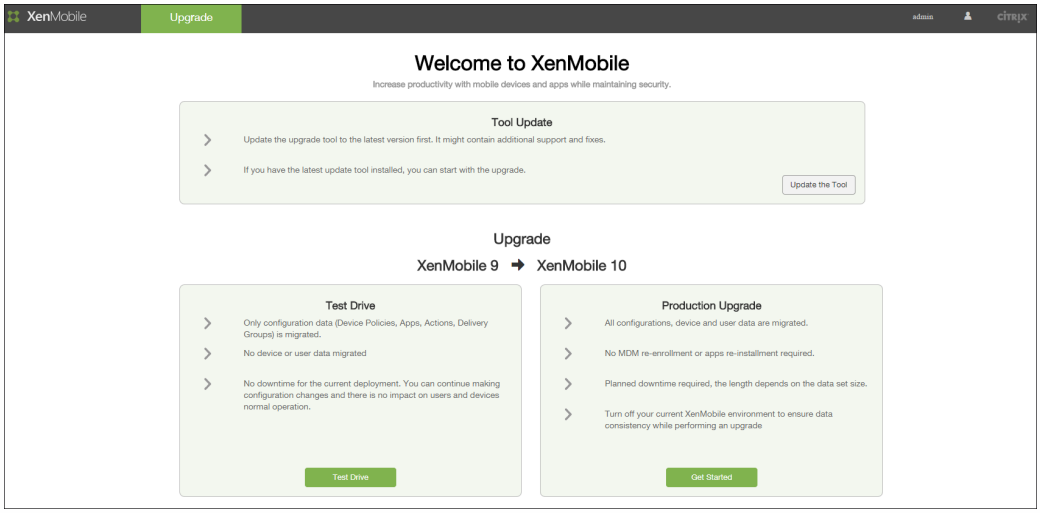
重要：システムのスナップショットを取得する場合は、XenMobile 10の初期構成の後で、アップグレードツールにアクセスする*前に*行います。



「**y**」を入力してアップグレードすると、XenMobile 10で1回のみのアップグレードツールが有効になります。次に、https:///uw/からアップグレードツールにアクセスします。

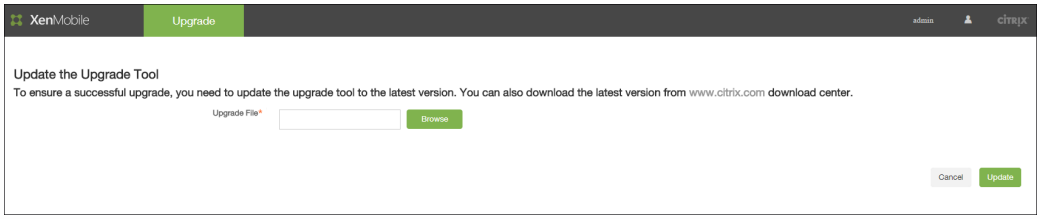
ヒント：アップグレードツールへのアクセスには、FirefoxまたはChromeを使用することをお勧めします。Internet Explorerは推奨されません。
新しいサーバーに移行する場合は、新しいサーバーのホスト名と、移行元のサーバーのホスト名が一致するようにします。

の一致により、Worx Homeが、XenMobile 9.0に接続していたときに使用されたホスト名を使用して、XenMobile 10に接続できるようになります。この方法により、ユーザーがXenMobile 10に再登録する必要がなくなります。



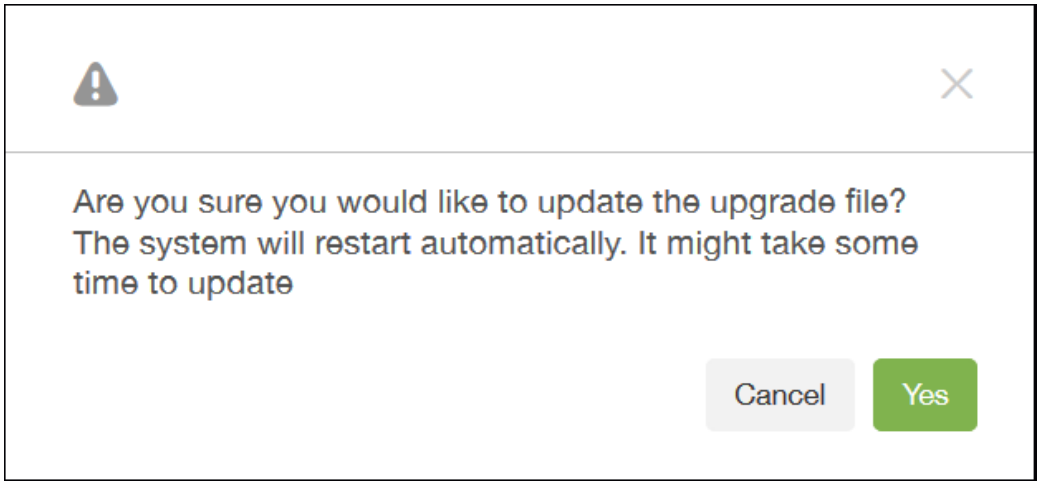
アップグレードツールをアップグレードして移行を開始するには

XenMobileのダウンロードページで、アップグレードツールに対する更新を見つけます。MDMの移行の場合は、Citrix.comからダウンロードした最新のツールを使用する必要があります。



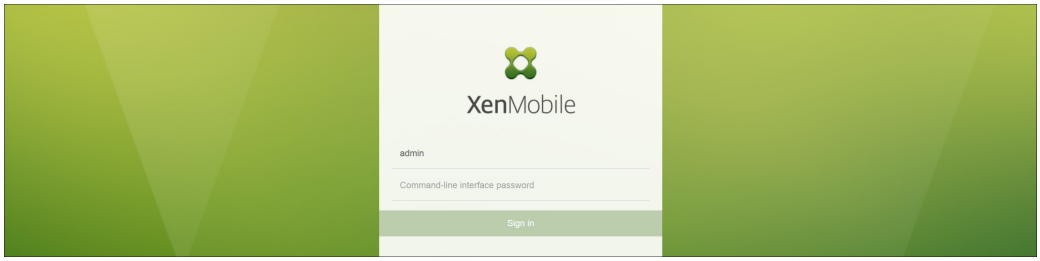
更新プロセスの開始を確認する次のメッセージが表示されます。

注：［Yes］をクリックした後、進行状況のインジケーターは表示されませんが、コマンドラインインターフェイスを監視して、システムの再起動の時間を確認できます。更新には、約30秒かかります。

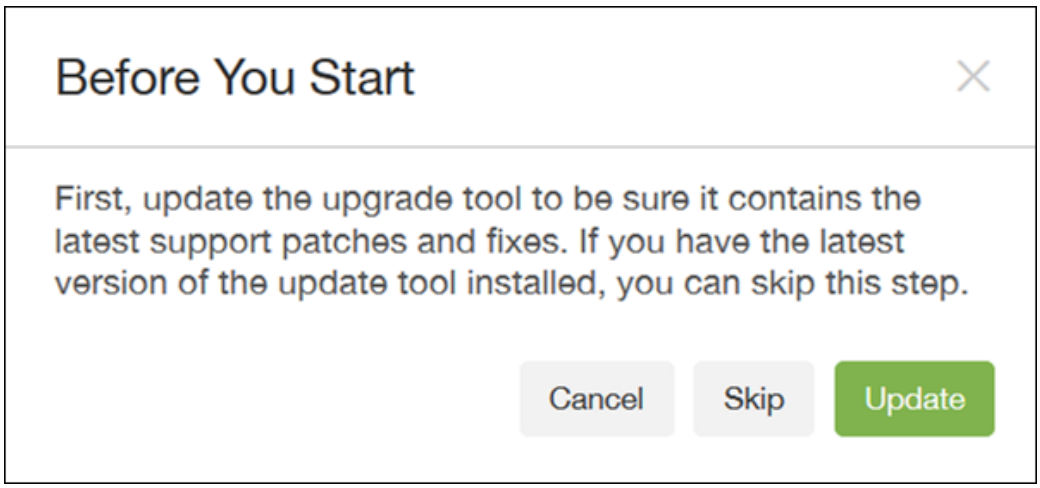


注：

- システムが再起動したら、アップグレードツールのURL（https:///uw）に再度アクセスする前に、ブラウザーのキャッシュを消去します。
- HTTPS通信のデフォルトポート（443）を使用しない場合、アップグレードツールのURLはhttps://:/uwになります。



アップグレードツールにログオンしたら、この場合はアップグレードツールを既に更新しているので、**[Skip]** をクリックできます。



［Test Drive］または［Production Upgrade］を選択して、移行に進みます。

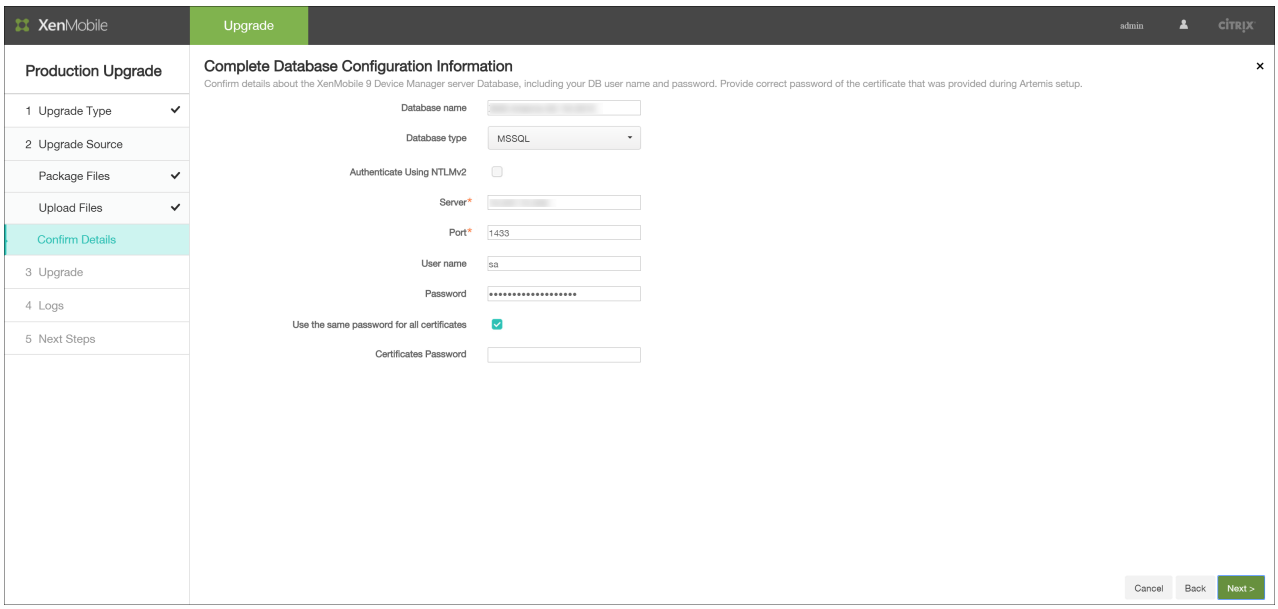
アップグレードツールが開くと、すべてのデータを移行するか、構成データのみを移行するかを選択できます。［Configuration Data only］を選択する場合は、ユーザーがデバイスを再登録する必要があります。［Next］をクリックして、前提条件として一時フォルダーにコピーして圧縮したファイルをアップロードします。

アップロードが完了したら、［Next］をクリックします。

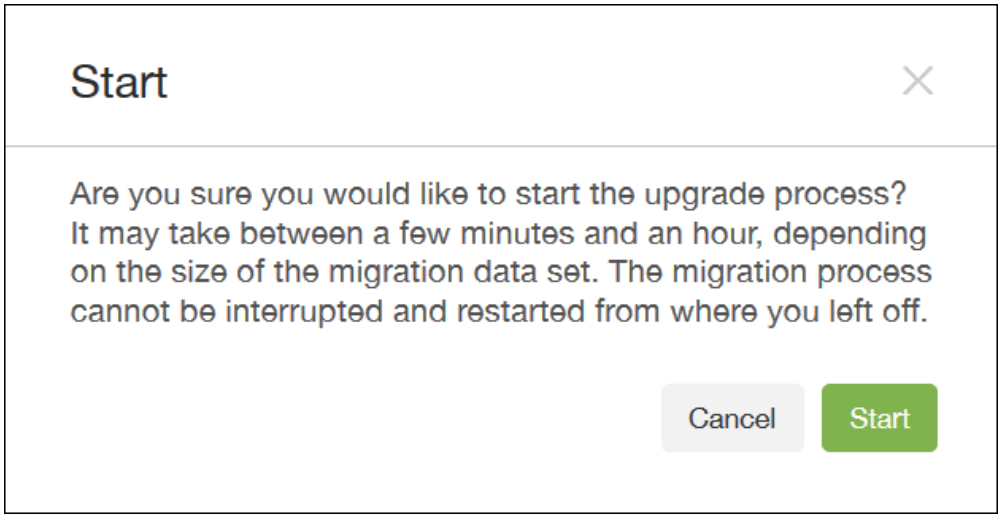
PostgreSQLデータベースの移行時に、サーバー名が「localhost」である場合は、「localhost」をサーバーのIPアドレスに変更する必要があります。

XenMobile 9.0 Device Managerから収集された情報が正しいことを確認します。証明書パスワードも入力する必要があります。

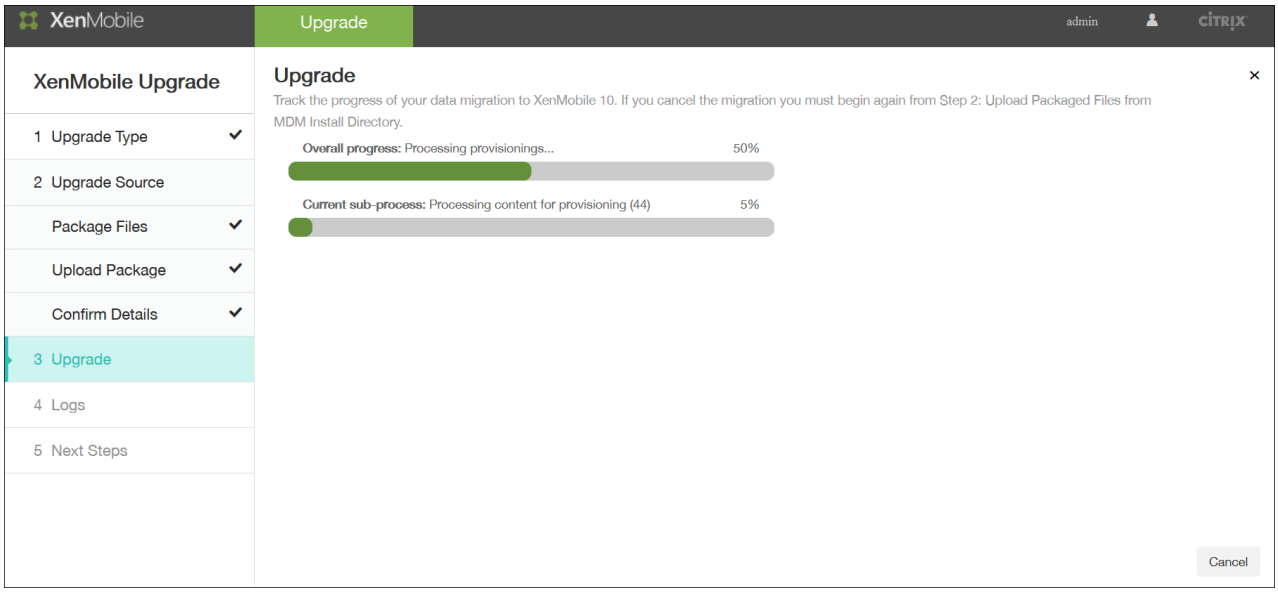
重要：すべての証明書パスワードを正しく入力する必要があります。正しく入力されない場合は移行が失敗します。

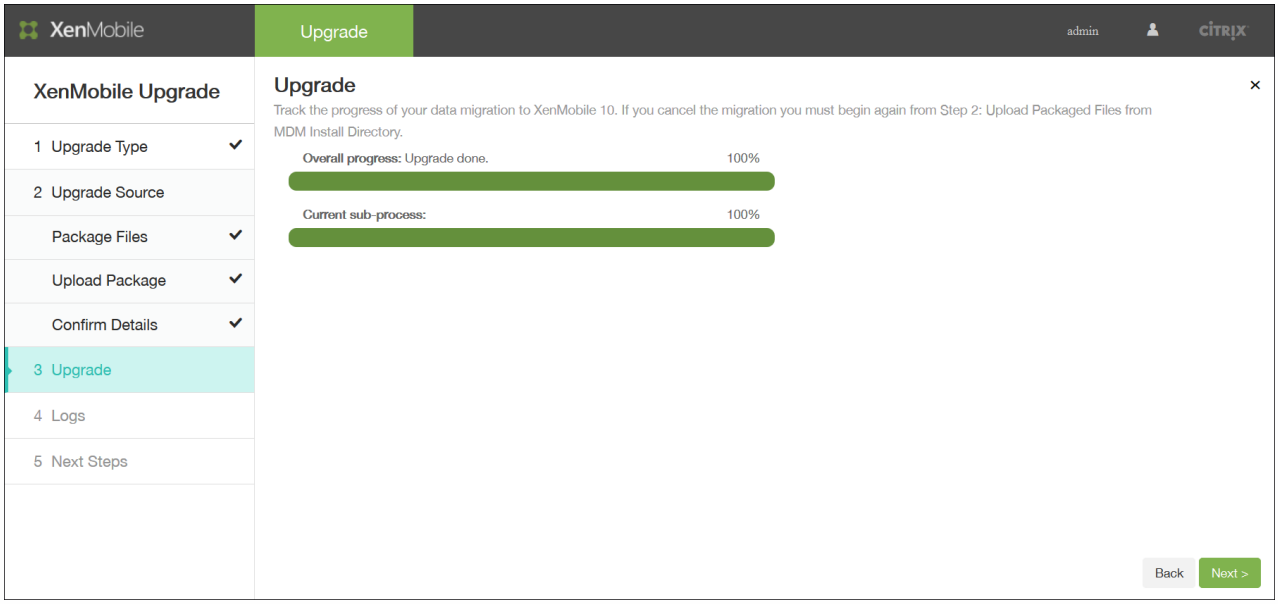


［Next］をクリックすると、次の確認メッセージが表示されます。



次に、［Upgrade］ページに進行状況のインジケーターが表示されるため、XenMobile 9.0からのデータの移行を追跡できます。



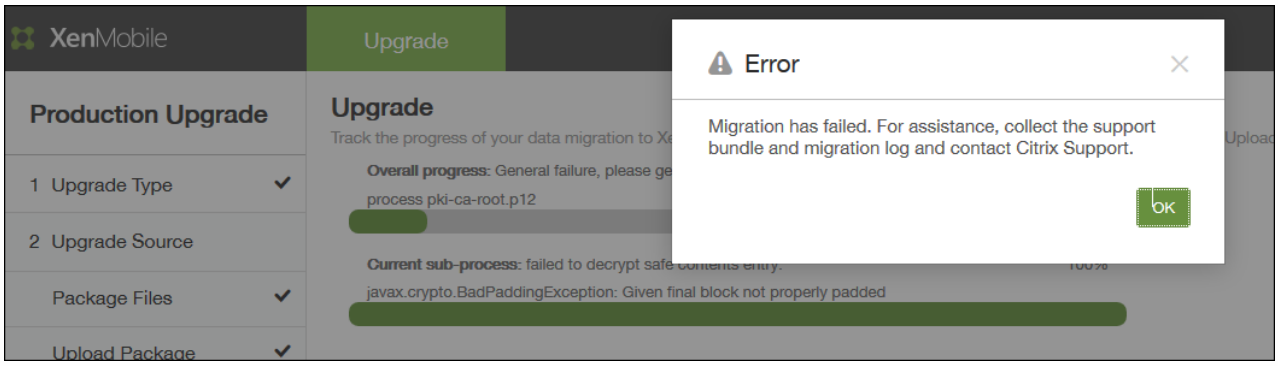


すべての必要なDevice Managerファイルを.zipフォルダーにコピーしていない場合は、アップグレードツールで不足しているファイルが表示されます。この場合、必要なファイルが追加されると、ツールが再開されます。

問題を解決できない場合は、XenMobileサポートバンドルを生成して、移行ログを収集し、Citrixテクニカルサポートに連絡するように求めるエラーメッセージが表示されます。

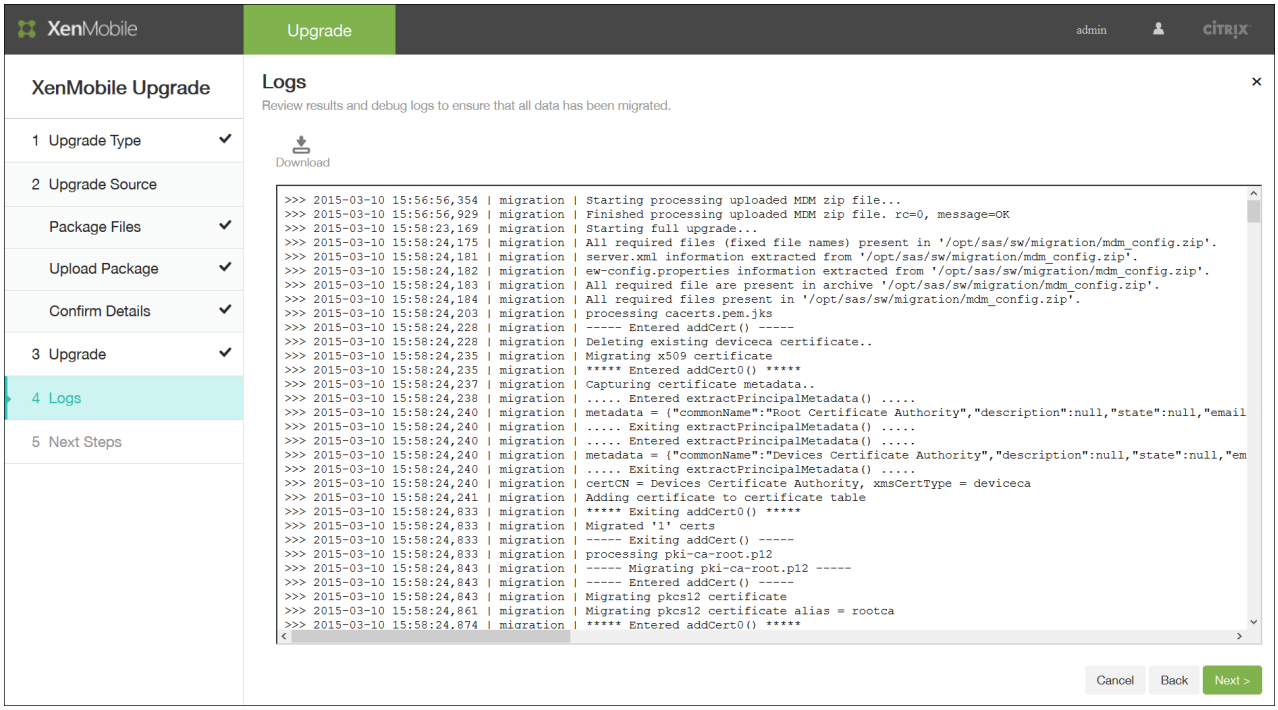
注：

- 移行が失敗した場合は、新しいXenMobile 10インスタンスをインポートして、移行を再度開始する必要があります。
- 移行が完了（パスまたは失敗）したら、［Back］を使用して情報を修正することはできません。新しいXenMobile 10インスタンスをインポートして、移行を再度開始する必要があります。



アップグレードツールログの表示

XenMobile 10へのアップグレード後、次の図に示すように、ダウンロードして確認できるログファイル（migration.log）が表示されます。ファイルを確認して、ポリシー、設定、ユーザーデータなどがXenMobile 10に移行されたかどうかを確認することをお勧めします。



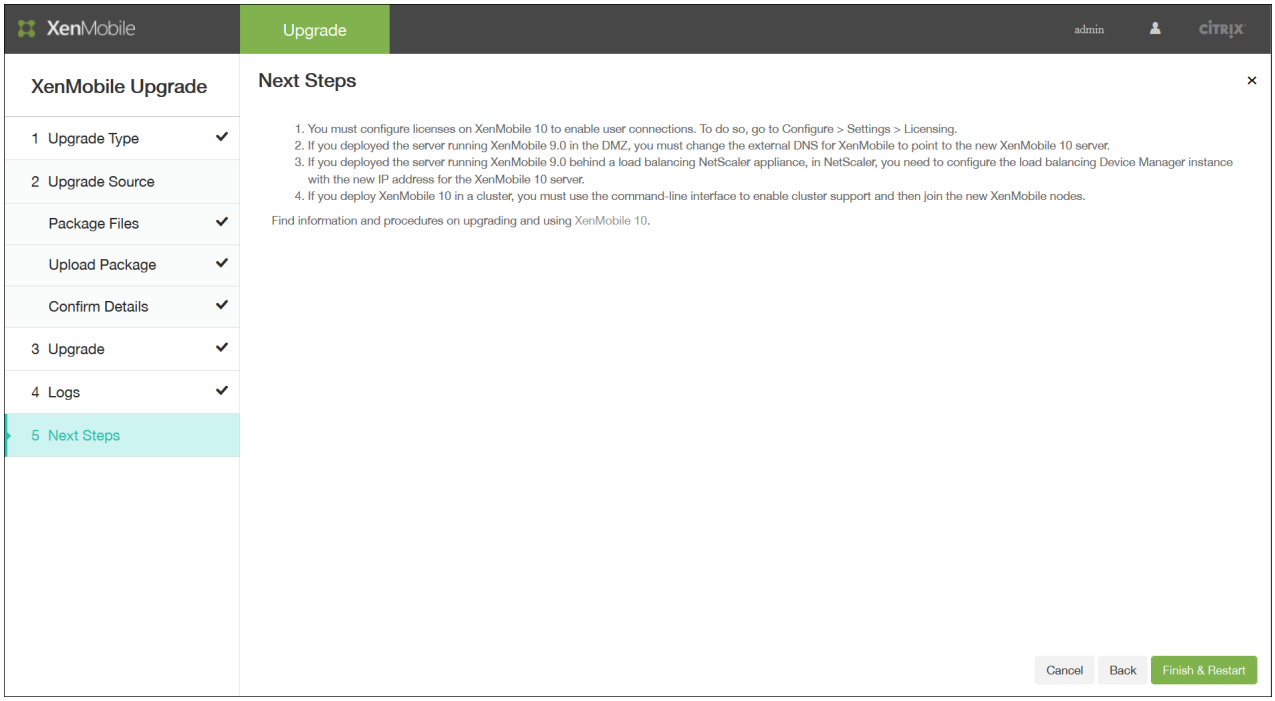
移行ログをダウンロードして確認したら、［Next］をクリックして、次の手順に移動します。詳しくは、「アップグレードツールのアップグレード後要件」を参照してください。

アップグレードツールのアップグレード後要件

May 10, 2016

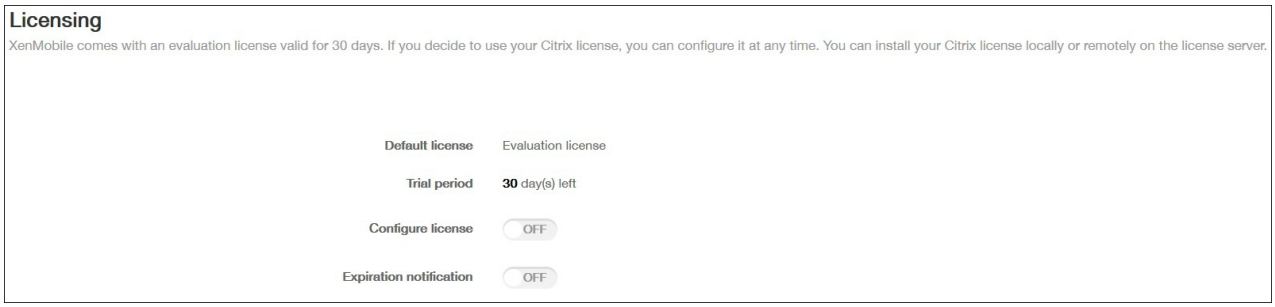
アップグレード後に、次に示すアップグレード後要件を満たしていることを確認します。一部はアップグレードツールの最後の画面にも表示されます。［Finish & Restart］をクリックすると、サーバーが再起動します。

注：管理者資格情報により、https://:4443を使用してXenMobileコンソールにログオンします。



ライセンス管理

XenMobile 10はCitrix V6ライセンスサーバーのみをサポートします。次の図に示すように、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忘れずに設定し、「Citrix Licensing」からライセンスファイルをダウンロードします。詳しくは、「XenMobileのライセンス」のトピックを参照してください。



XenMobile 10でライセンスを構成して、ユーザーの接続を有効にする必要があります。これを行うには、［**Configure**］、［**Settings**］、［**Licensing**］の順に選択します。スタンドアロンサーバーでXenMobile 10を実行している場合は、XenMobileコンソールにMDMのみのライセンスをアップロードできます。

DNS

注：このアップグレード後要件は、実稼働環境のアップグレードの場合に満たす必要があります。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 10サーバーを指すように変更する

必要があります。

負荷分散NetScalerのIPアドレス

注：このアップグレード後要件は、実稼働環境のアップグレードの場合に満たす必要があります。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、XenMobile 10サーバーの新しいIPアドレスで、NetScalerの負荷分散Device Managerインスタンスを構成する必要があります。

クラスタリング

XenMobile 10をクラスターで展開する場合は、コマンドラインインターフェイス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。同じIPアドレスの新しいXenMobile 10インスタンスを構成して、管理者ノードまたは最も古いノードに接続することで、XenMobile 9.0ノードのIPアドレスを再使用できます。

移行されなかった情報の更新

必要に応じて以下の情報を更新します。

- 自動化された操作
- サーバーグループポリシーとそれに関連する展開
- MSPグループ
- カスタムのActive Directoryの属性
- XenMobileのロックアウト制限値
- RBACの役割
- ログ設定
- HTTPまたはHTTPSが含まれないURL
- 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

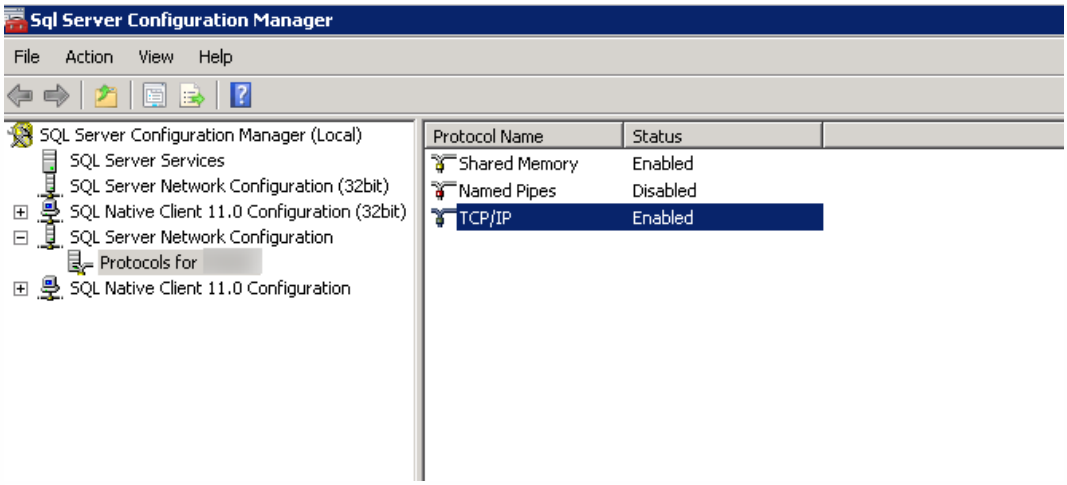
名前付きSQLインスタンスのサポート

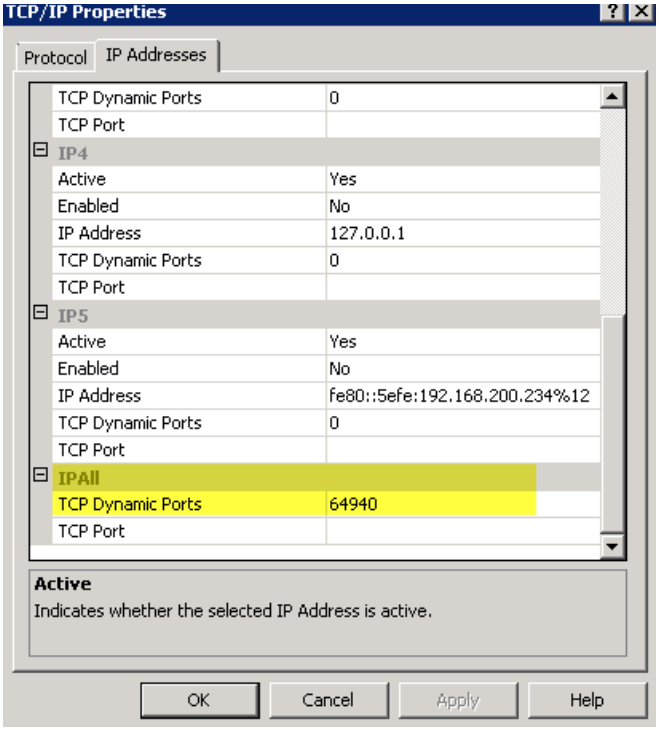
May 10, 2016

アップグレードツールを使用して、XenMobile 9.0からXenMobile 10.に、またXenMobile 9.0からXenMobile 10.1アップグレードできます。XenMobile 9セットアップが名前付きSQLインスタンスをベースとしたものである場合は、この状況に特化した次の手順を実行する必要があります。XenMobile 9環境が次の前提条件を満たす場合、このアーティクルの手順に従ってアップグレードを実行します。

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

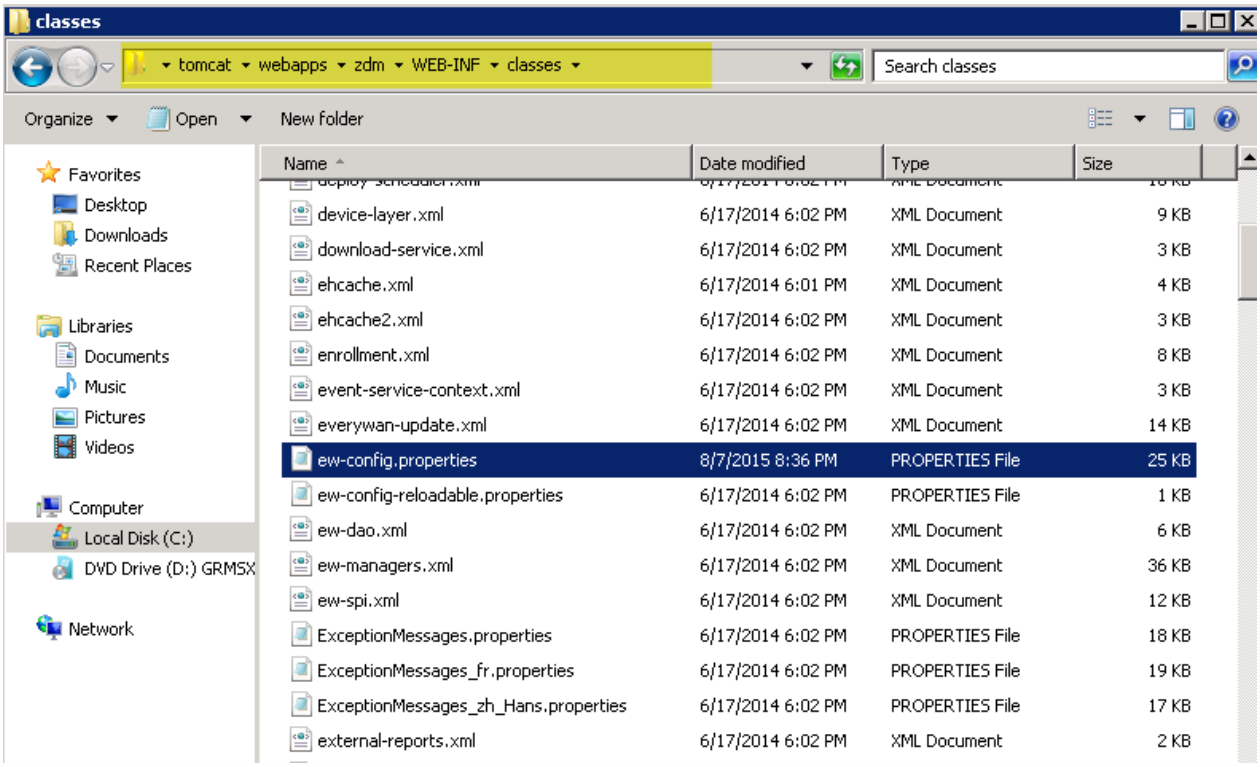
> ## 注意
>
> XenMobileはデータベースに対する持続的なアクセスを必要とするため、SQL Serverデータベースインスタンスは常時静的ポートで実行することをお勧めします。この接続は、通常ファイヤウォールを介して実行されます。その結果、ファイアウォールで適切なポートを開く必要があります。つまり、静的ポートで実行中のデータベースインスタンスが必要です。





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

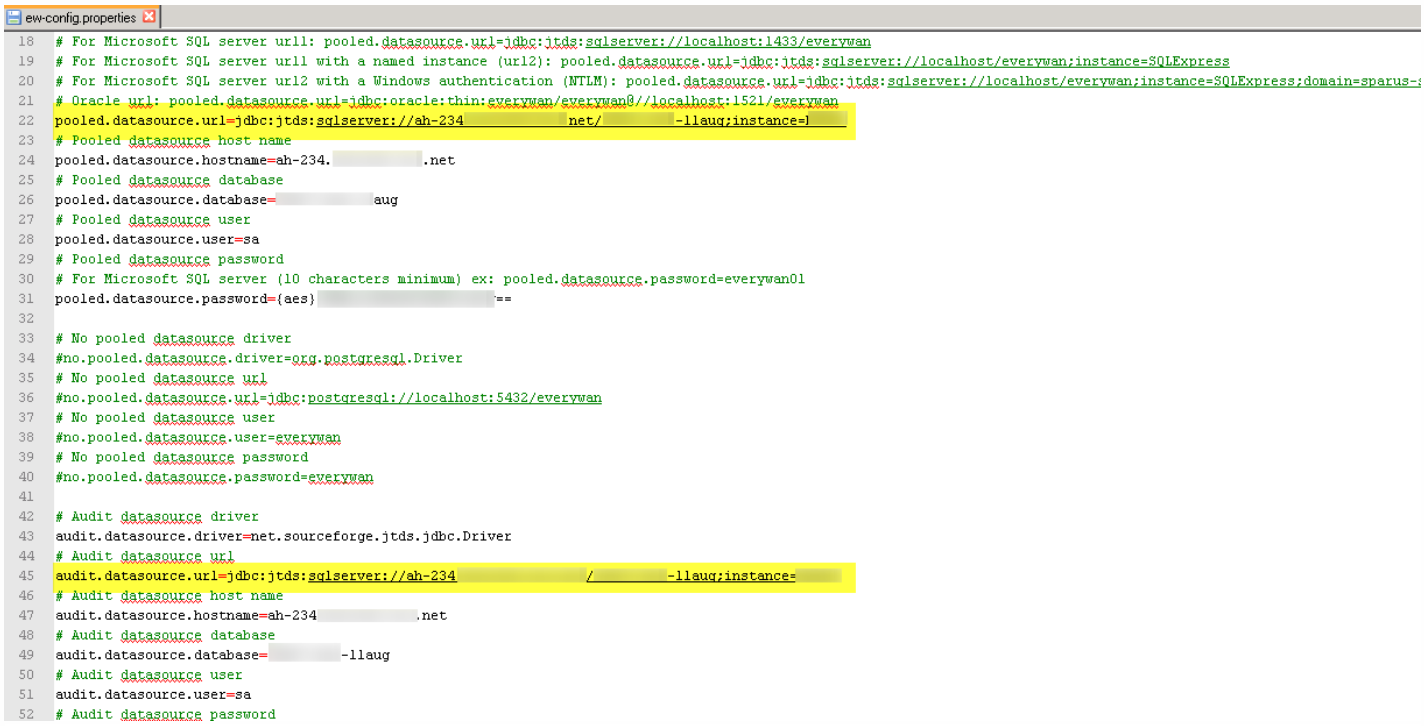
1. Device Managerインストールディレクトリにアクセスして、ew-config.propertiesファイルを開きます。このファイルは、tomcat/webapps/zdm/WEB-INF/classesにあります。



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

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

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



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

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

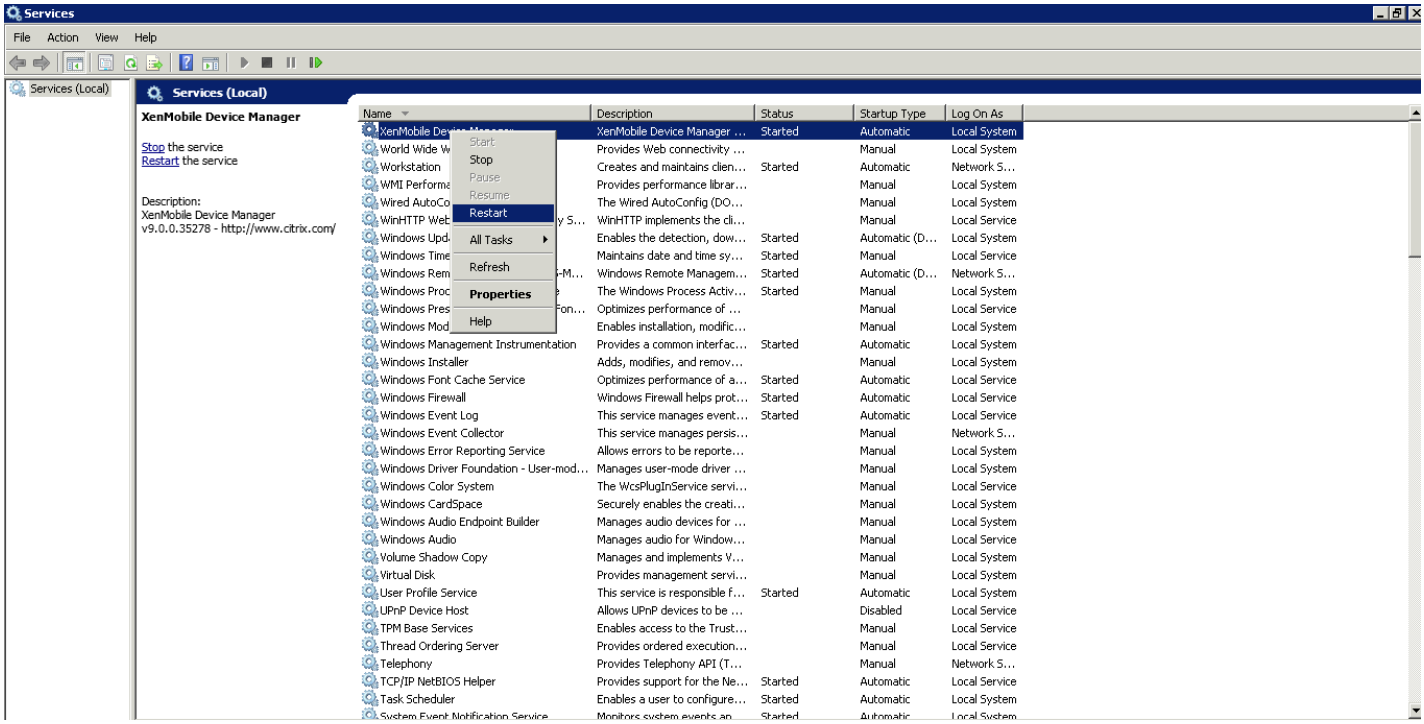
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

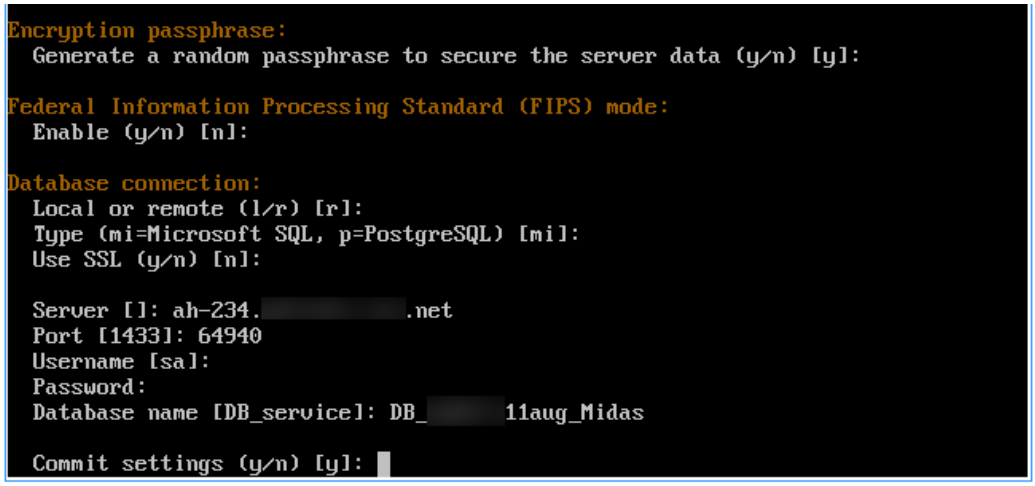
ew-config.properties

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

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

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

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



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



6. このアーティクルで説明する手順に従って、XenMobile環境のアップグレードを続けます。

- XenMobile 9.0 App EditionまたはEnterprise EditionからXenMobile 10.1にアップグレードするには、XenMobile Server App EditionおよびEnterprise Edition Upgrade Toolを使用します。詳しくは、「XenMobile 10.1アップグレードツールの有効化と実行」を参照してください。
- XenMobile 9.0 MDMエディションのみをXenMobile 10.1にアップグレードするには、「XenMobile 10 MDMアップグレードツール」を参照してください。

XenMobileコンソールでのXenMobileのアップグレード

May 10, 2016

XenMobileソフトウェアの新しいバージョンを入手できる場合は、新しいバージョンにアップグレードできます。XenMobileソフトウェア、サービスパック、およびシステムパッチの新しいバージョンをインストールするには、XenMobileコンソールの［Release Management］ページを使用します。

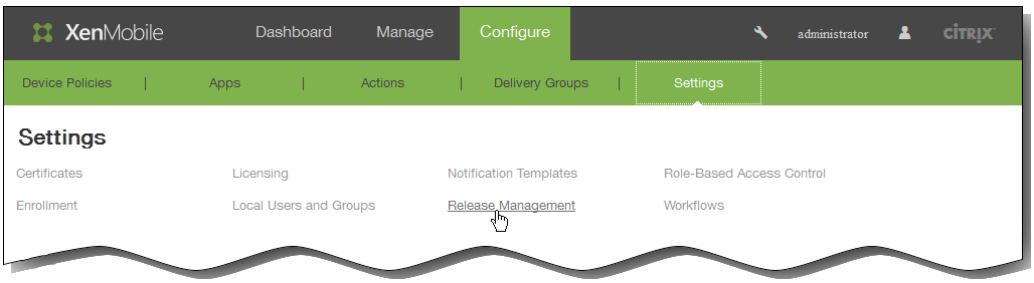
注：新しいバージョンや重要な更新が利用可能になるとCitrix.comに公開され、各ユーザーレコードの連絡先に通知が送信されます。

重要：

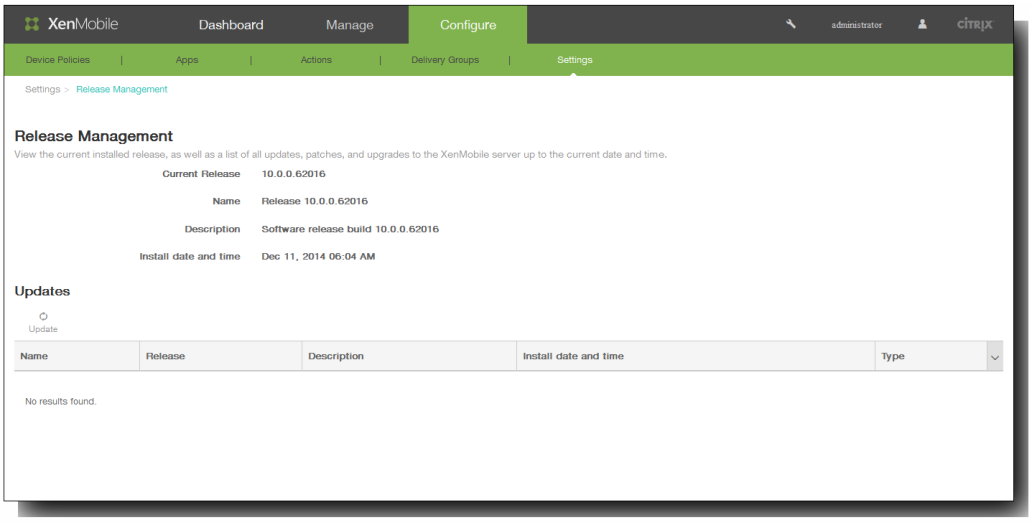
- XenMobileの更新をインストールする前に、仮想マシン（VM）の機能を使用して、システムのスナップショットを取得してください。
- システム構成データベースをバックアップしてください。
- MDMサーバーでSamsung KNOX認証を有効化しており、XenMobile 10.0へのアップグレードを計画している場合は、アップグレードの前に、新しいカスタムのKNOX認証ドメインを追加する必要があります。Samsung KNOX認証の有効化について詳しくは、「Samsung KNOX」を参照してください。新しい認証ドメインは次のとおりです。
  - 中国の地域 - china-attest-api.secb2b.com.cn
  - ヨーロッパ地域 - eu-attest-api.secb2b.com
  - US地域 - us-attest-api.secb2b.com

XenMobileをアップグレードするには

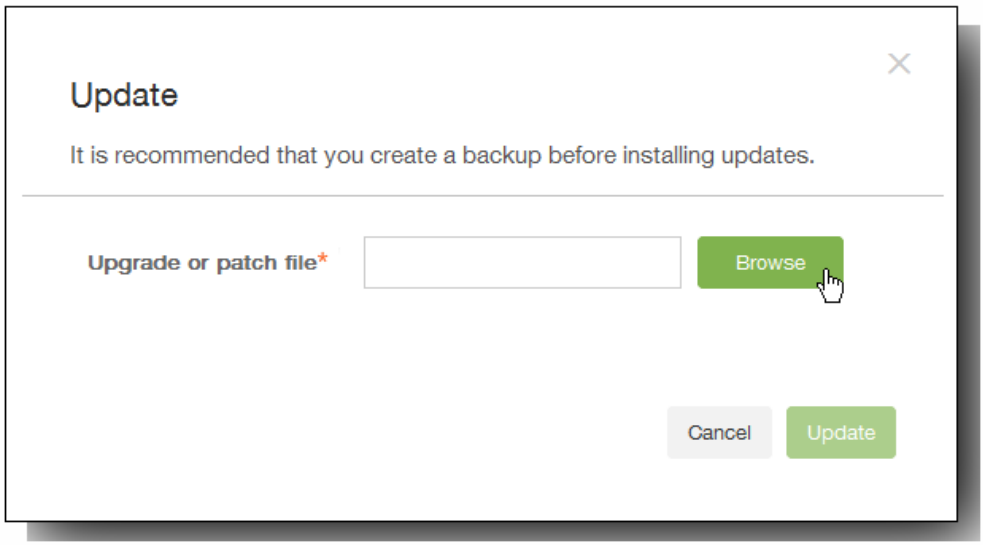
1. Citrix Webサイトのアカウントにログオンして、XenMobile Upgrade（.bin）ファイルを適切な場所にダウンロードします。
2. XenMobileコンソールで、［Configure］、［Settings］、［Release Management］の順にクリックします。



［Release Management］ページが開きます。このページには、現在インストールされているソフトウェアバージョンと、既にアップロードした更新、パッチ、およびアップグレードの一覧が表示されます。



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



4. ［Browse］をクリックし、Citrix.comからダウンロードしたXenMobileアップグレードファイルを保存した場所に移動して、そのファイルを選択します。
5. ［Update］をクリックし、メッセージが表示されたらXenMobileを再起動します。
注：更新プログラムをインストールした後に、XenMobileの再起動が不要な場合もあります。この場合は、更新プログラムのインストールが成功したことを示すメッセージが表示されます。ただし、XenMobileの起動が必要な場合は、コマン

ドラインを使用する必要があります。
重要：システムがクラスターモードで構成されている場合、以下の手順に従って各ノードを更新します。

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

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

XenMobile 10のクラスタリングの構成

Oct 24, 2016

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

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

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

前提条件

- 必要なXenMobileノードが完全に構成されていること
- 仮想IPアドレスの負荷分散用の2つの空きIPアドレス
- サーバー証明書
- NetScaler Gateway仮想IPアドレス用の1つの空きIPアドレス

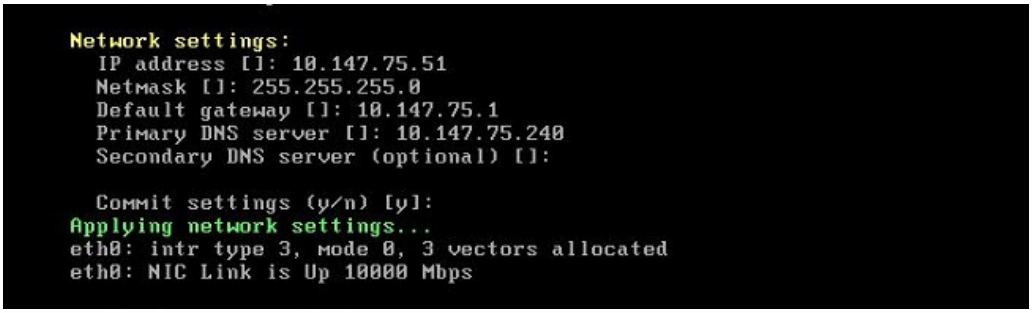
クラスター構成におけるXenMobile 10.xのリファレンスアーキテクチャ図については、「アーキテクチャの概要」を参照してください。

XenMobileクラスターノードのインストール

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

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

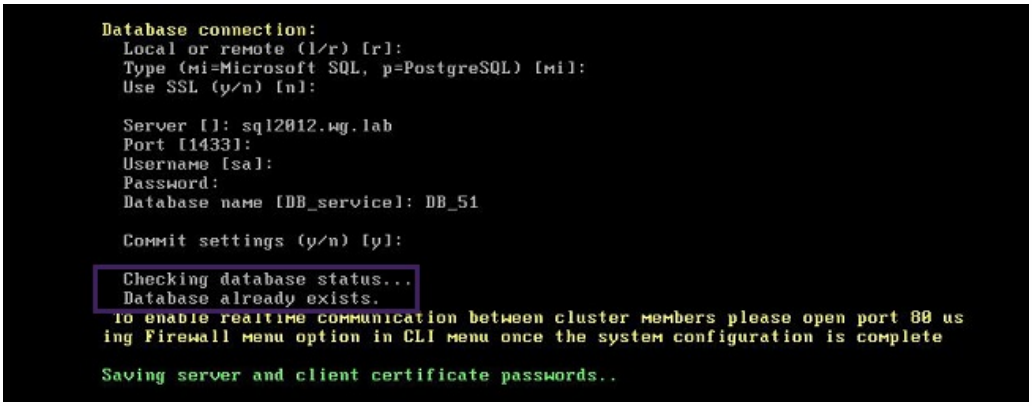
2. 次の図のようなネットワーク構成情報を指定します。



3. データ保護のためにデフォルトのパスワードを使用する場合、「**y**」と入力します。そうでない場合は「**n**」と入力して新しいパスワードを入力します。 **注：**クラスターに追加のノードを手動で追加する計画で、最初のXenMobile VMを複製しない予定の場合は、ここで新しいパスワードを手動で入力する必要があります。 連続するノードには同じパスコードが必要です。 一致するパスコードを使用しないと、第2ノードを追加するときに処理に失敗します。 失敗したときはVMを複製できますが、新しいパスワードを入力すると失敗を防ぐことができます。

4. FIPSを使用する場合は、「**y**」と入力します。そうでない場合は「**n**」と入力します。

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



6. 最初のVMに付与した証明書のものと同じパスワードを入力してください。

```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

  Server []: sql2012.wg.lab
  Port [1433]:
  Username [sa]:
  Password:
  Database name [DB_service]: DB_51

  Commit settings (y/n) [y]:

  Checking database status...
  Database already exists.
 To enable realtime communication between cluster members please open port 80 us
ing Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key In
frastructure (PKI) in first node
  Do you want to use the same password for all the certificates of the PKI [y]:
```

パスワードの入力が完了すると、2台目のノードでの初期構成が完了します。

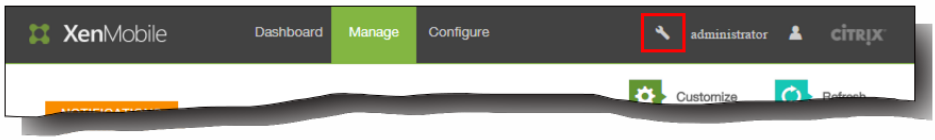
```
      Saving server and client certificate passwords..

      WARNING: Please enter the same passwords used to generate internal Public Key In
      frastructure (PKI) in first node
        Do you want to use the same password for all the certificates of the PKI [y]:
      y
        New password:
        Re-enter new password:
      Saving server and client certs password...

      Applying port listener configuration...
      Applying firewall settings ...
      Writing iptables configuration...
      Restarting iptables...

      Initial system configuration complete!
      Stopping configuration app...                                    [ OK ]
      Starting configuration app...
        this may take a few seconds.................................
        application started                                            [ OK ]
      Stopping main app...                                             [ OK ]
      Starting main app...
        this may take a few minutes....._
```

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

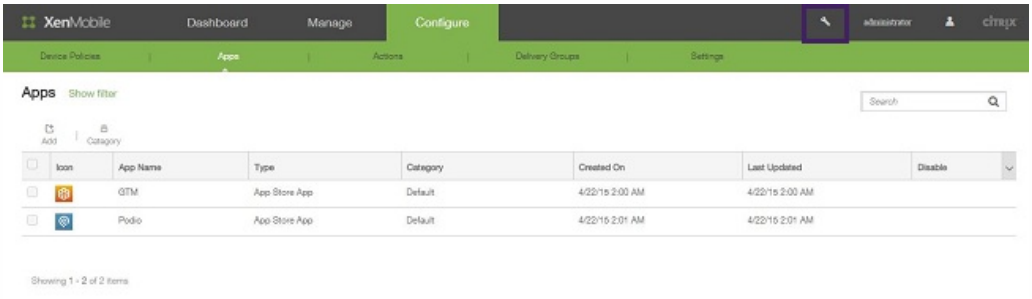
```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app...                                      [ OK ]
Starting configuration app...
  this may take a few seconds.......
  application started                                              [ OK ]
Stopping main app...                                               [ OK ]
Starting main app...
  this may take a few minutes.........................^[.....................
.....................................
  application started                                              [ OK ]

  To access the console, from a web browser, go to the following location and
  log on with your console credentials:
    https://10.147.75.59:4443/

Starting monitoring...                                             [ OK ]

xms51.wg.lab login:
```

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

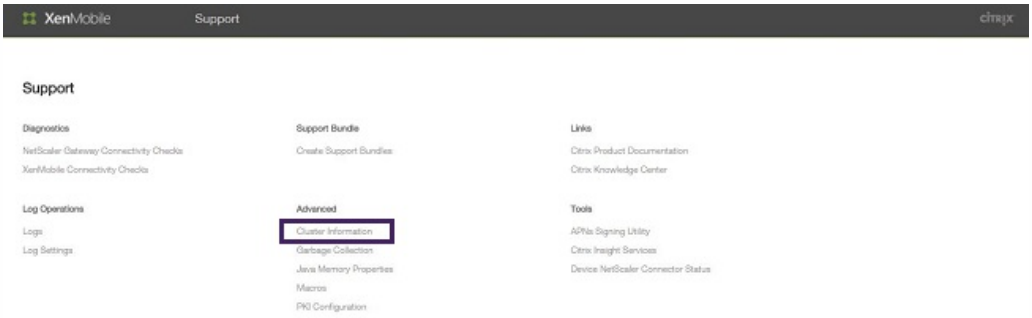
8. WebブラウザーでXenMobileコンソールを開くには、XenMobileの完全修飾ドメイン名（FQDN）を使用します。
9. ［Dashboard］で画面右上のツールアイコンをクリックします。



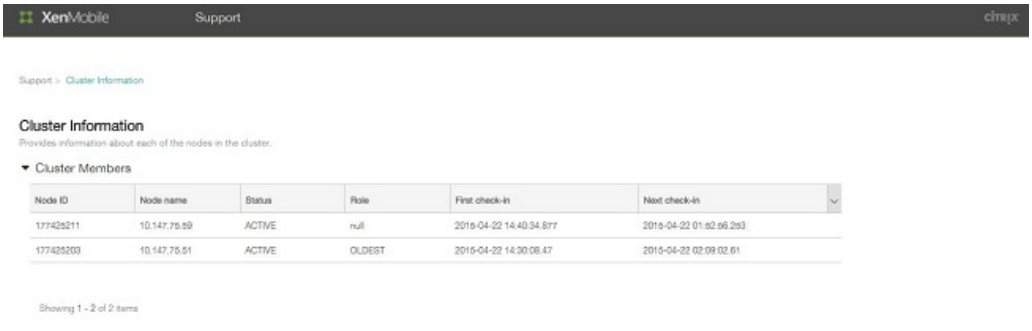
［Support］ページが開きます。



10. ［Advanced］の［クラスター情報］をクリックします。



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



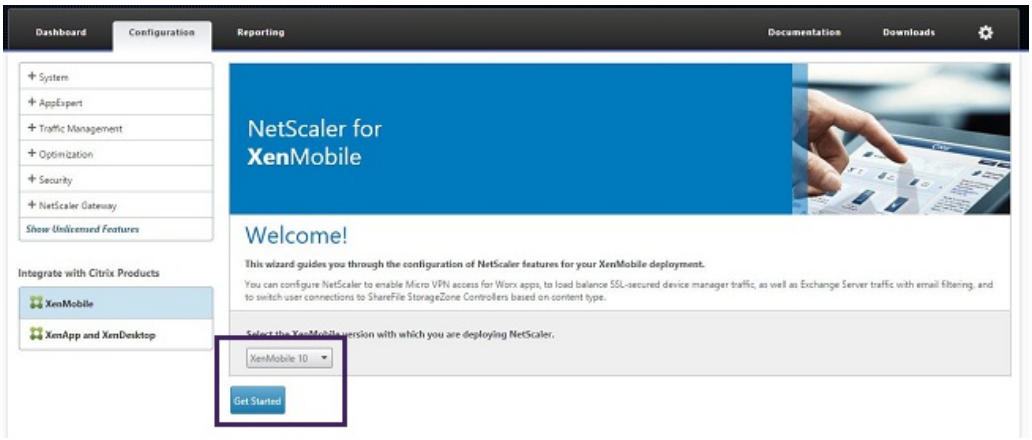
新しいノードがクラスターのメンバーになります。別のノードを追加する場合も、手順は同じです。

NetScalerでXenMobileクラスターの負荷分散を構成するには

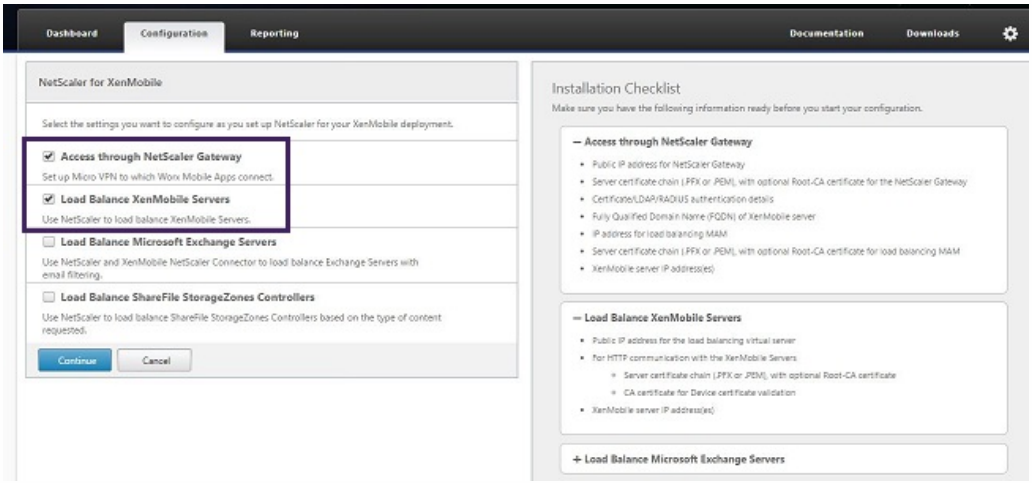
必要なノードをXenMobileクラスターのメンバーとして追加した後、クラスターにアクセスできるようにノードの負荷分散を行う必要があります。負荷分散を行うには、NetScaler 10.5.xで利用可能なXenMobileウィザードを実行します。ウィザードの実行によりXenMobileの負荷分散を行う手順は、以下のとおりです。

1. NetScalerにログオンします。

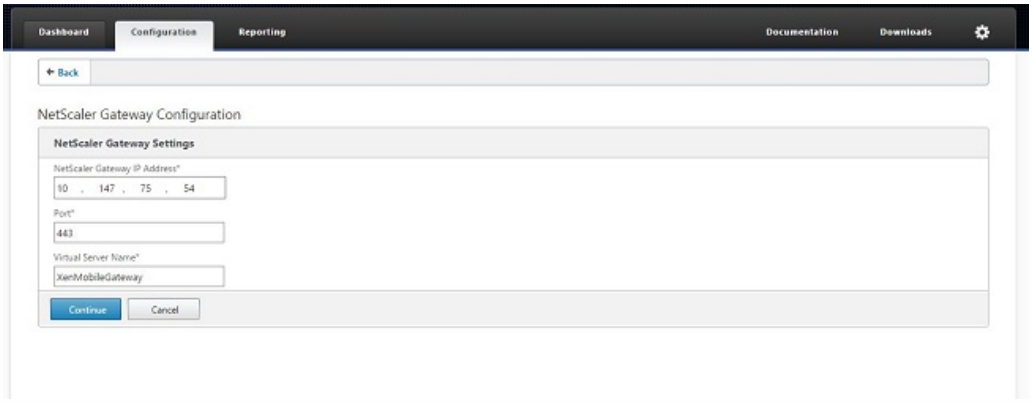
2. ［Configuration］タブで［XenMobile］をクリックし、［Get Started］をクリックします。



3. ［Access through NetScaler Gateway］チェックボックスと［Load Balance XenMobile Servers］チェックボックスをオンにし、［Continue］をクリックします。

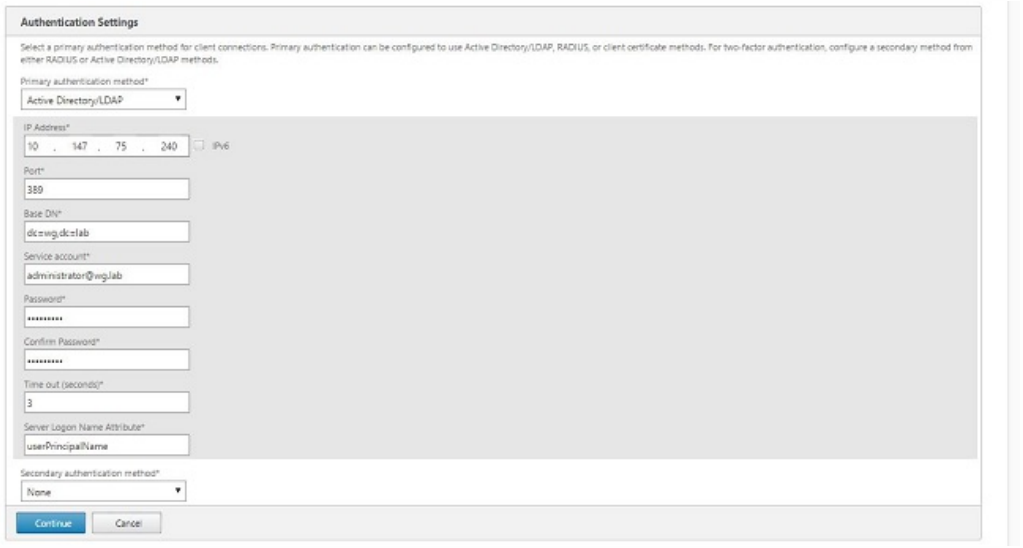


4. NetScaler GatewayのIPアドレスを入力し、［Continue］をクリックします。



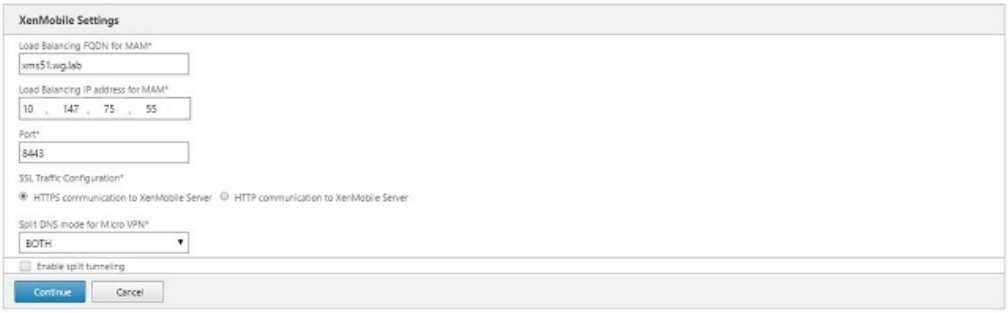
5. 以下のいずれかの方法でサーバー証明書をNetScaler Gatewayの仮想IPアドレスにバインドして[Continue］をクリックします。
   - ［Use existing certificate］で一覧からサーバーの証明書を選択します。
   - ［Install Certificate］タブをクリックして、新しいサーバーの証明書をアップロードします。

6. 認証サーバーの詳細を入力して、［Continue］をクリックします。



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

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

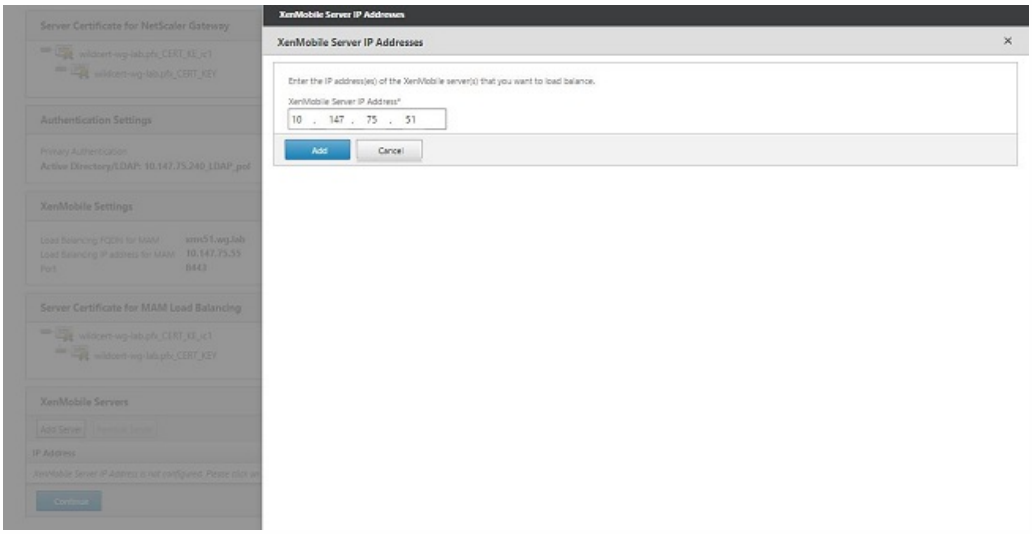


注：MAM負荷分散仮想IPアドレスのFQDNとXenMobileのFQDNが同じであることを確認してください。

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

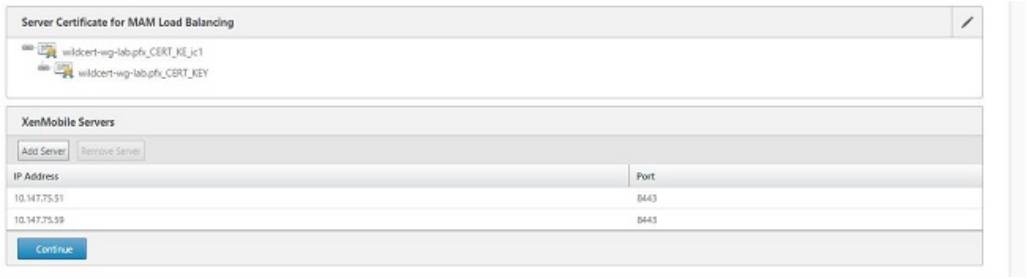
10. ［XenMobile Servers］の下で［Add Server］をクリックしてXenMobileノードを追加します。

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

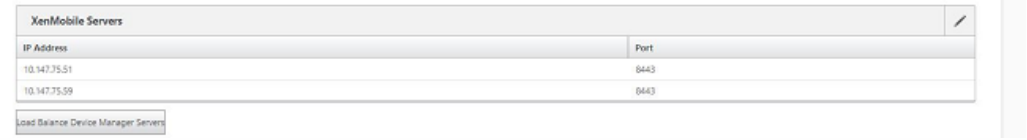


12. 手順10および11を繰り返して、XenMobileクラスターの一部であるXenMobileノードを追加します。追加したすべての

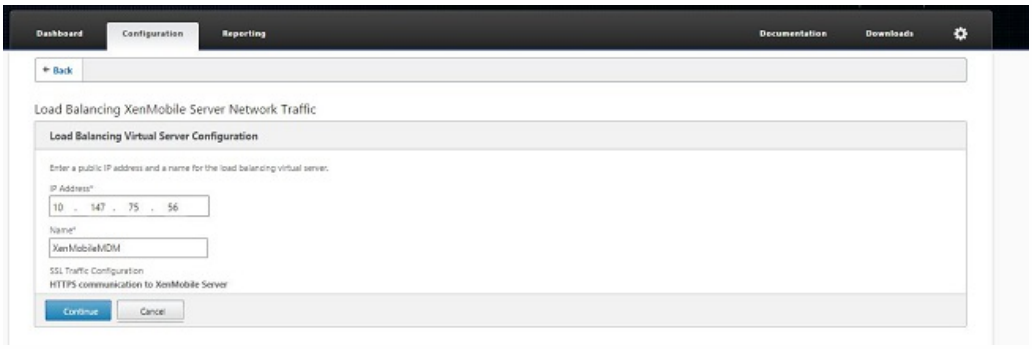
XenMobileノードが表示されます。［続ける］をクリックします。



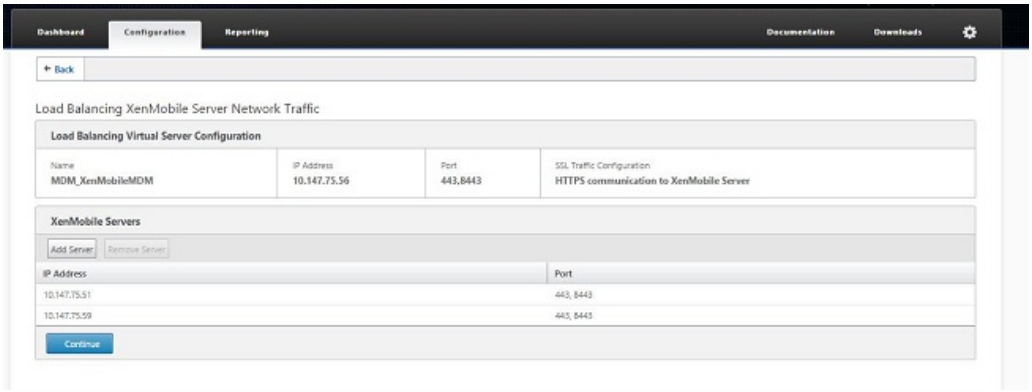
13. ［Load Balance Device Manager Servers］をクリックしてMDM負荷分散の構成を続行します。



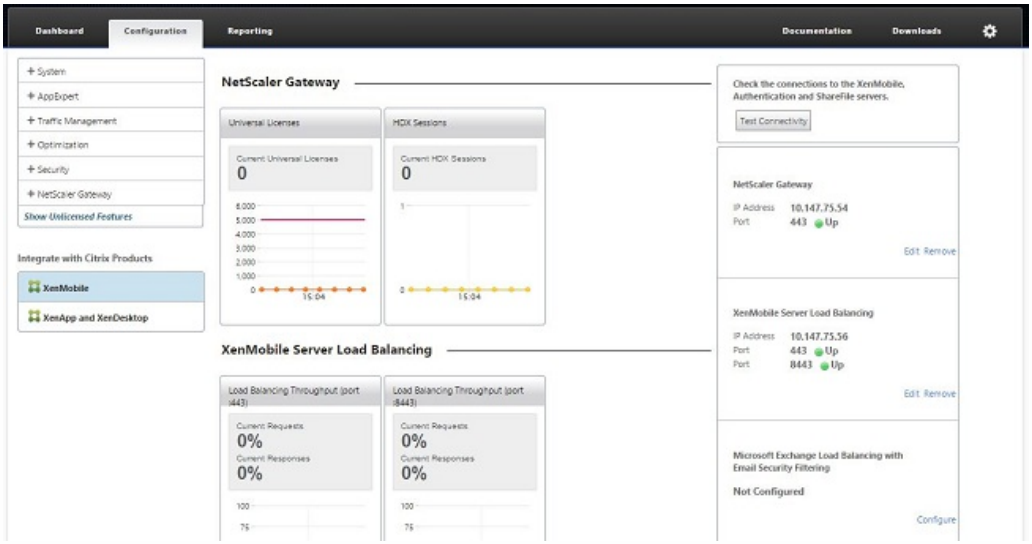
14. MDM負荷分散IPアドレス用に使用するIPアドレスを入力し、［Continue］をクリックします。



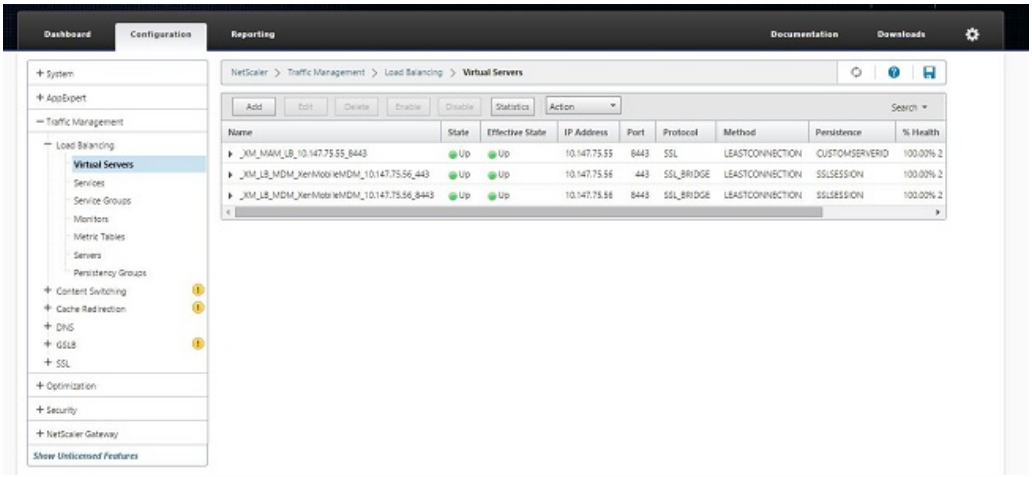
15. 一覧にXenMobileノードが表示されたら、［Continue］をクリックしてから［Done］をクリックして処理を完了します。



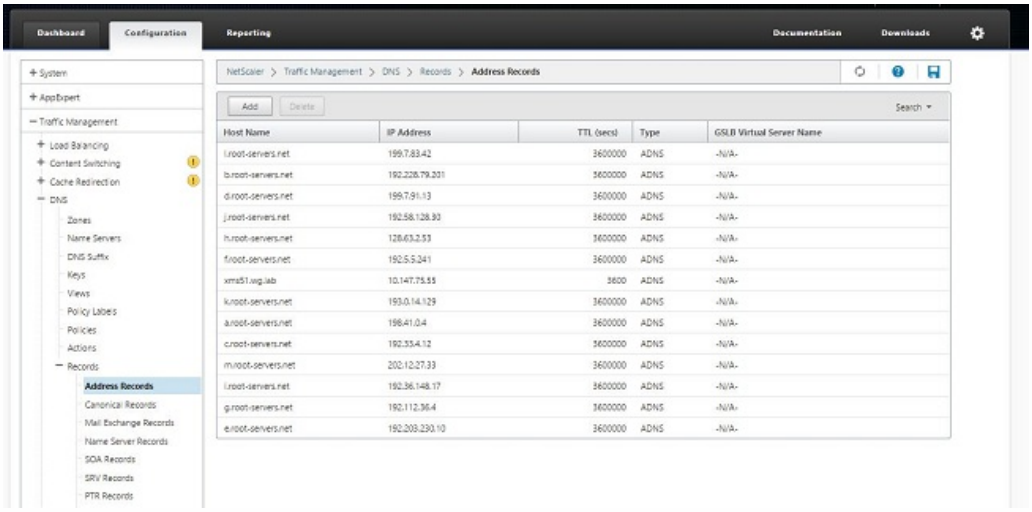
［XenMobile］ページに仮想IPアドレスのステータスが表示されます。



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



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

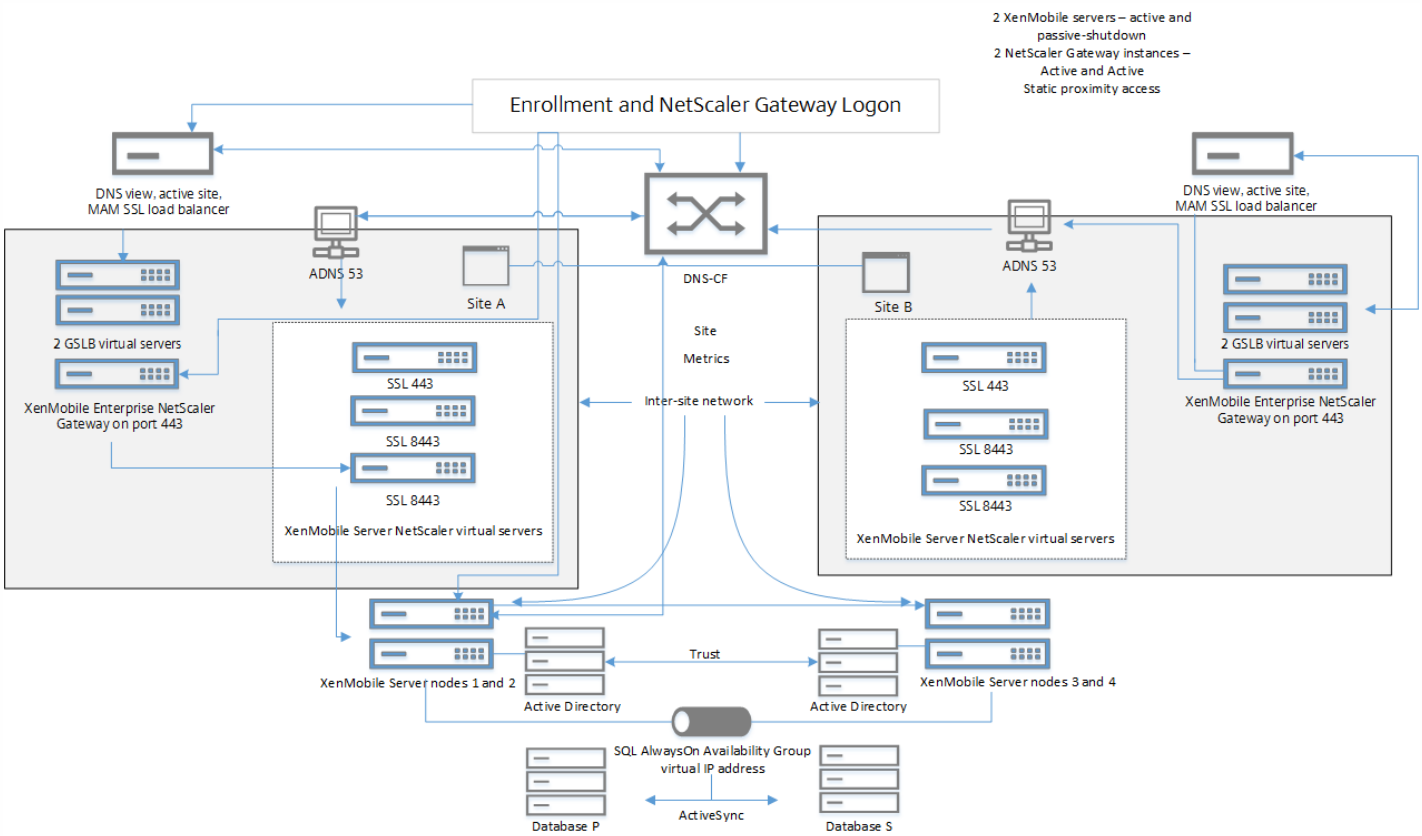


XenMobile障害回復ガイド

May 10, 2016

このガイドはPDFとして提供されており、XenMobile 10 Enterprise Editionでの障害回復用の展開環境の構成方法について説明しています。

次の図に、この障害回復用の展開環境のアーキテクチャを示します。この図はPDFとしてダウンロードすることもできます。



PDF XenMobile障害回復ガイド

PDF XenMobile障害回復のアーキテクチャ図

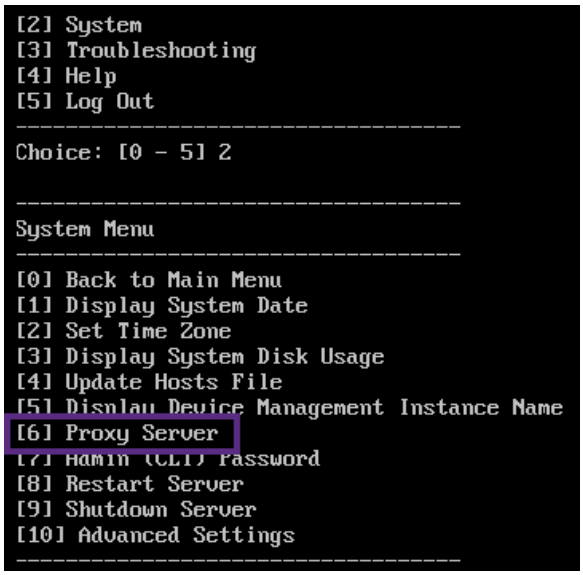
XenMobileでのプロキシサーバーの有効化

May 10, 2016

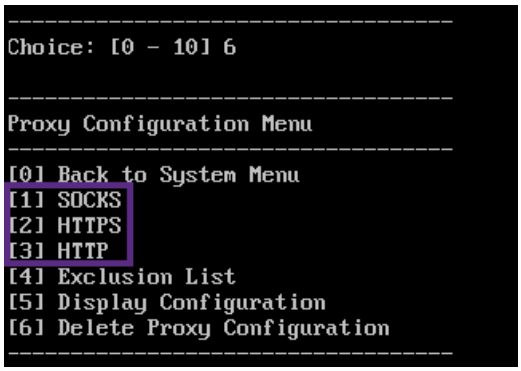
発信インターネットトラフィックを制御するために、そのトラフィックを発信するプロキシサーバーをXenMobileにセットアップできます。これを行うには、コマンドラインインターフェイス（CLI）でプロキシサーバーをセットアップする必要があります。プロキシサーバーのセットアップにはシステムの再起動が必要なことに注意してください。

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

2. ［System］メニューで、「**6**」と入力して［Proxy Server］メニューを選択します。



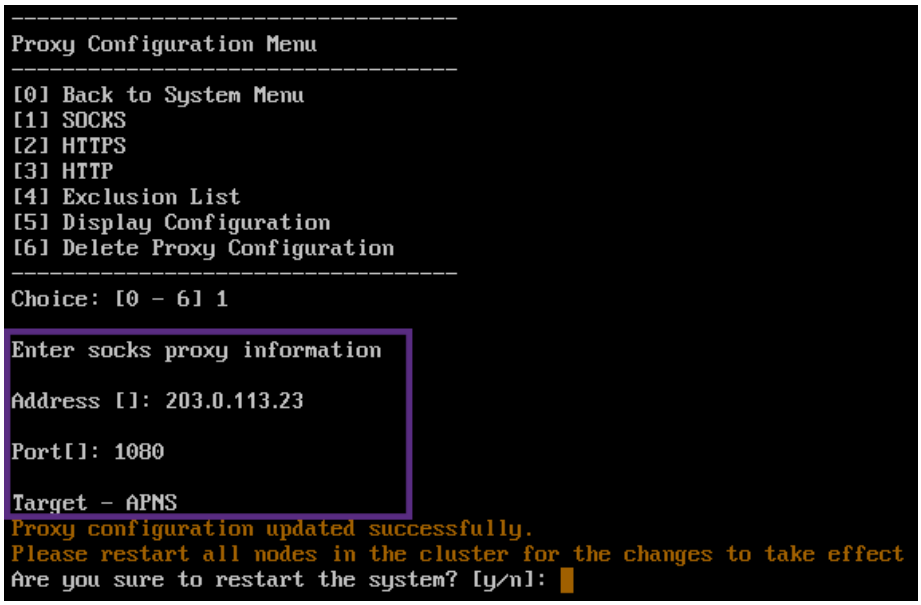
3. ［Proxy Configuration］メニューで、「**1**」と入力して［SOCKS］を選択するか、「**2**」と入力して［HTTPS］を選択するか、「**3**」と入力して［HTTP］を選択します。



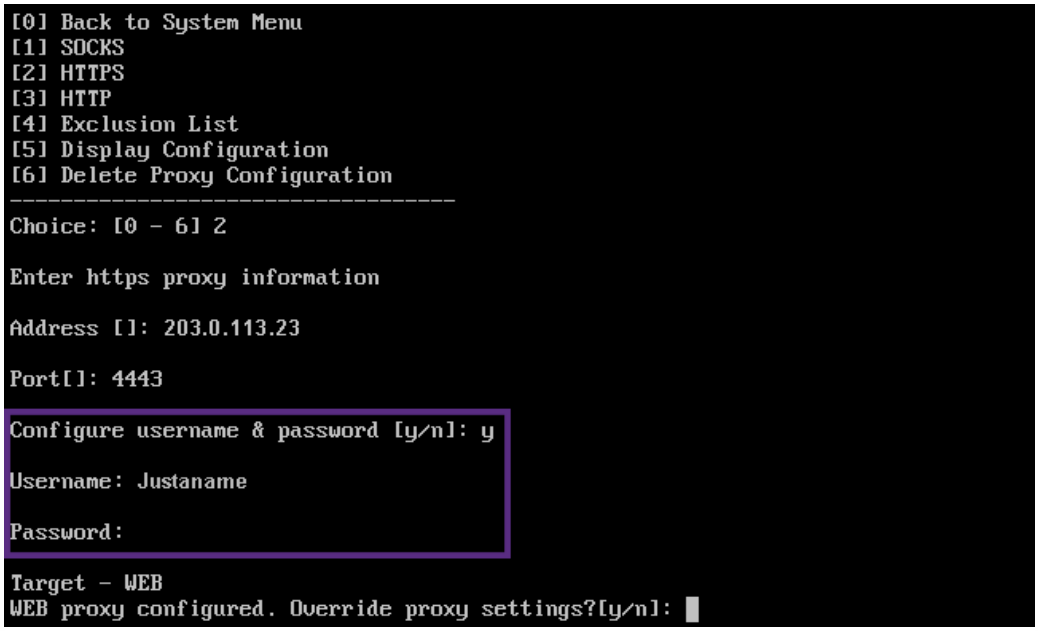
4. プロキシサーバーのIPアドレス、ポート番号、およびターゲットを入力します。プロキシサーバーの種類別の、サポートされるターゲットの種類については以下の表を参照してください。

プロキシの種類	サポートされるターゲット
SOCKS	APNS

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



5. HTTPまたはHTTPSプロキシサーバーに認証用のユーザー名およびパスワードを構成する場合は「**y**」と入力し、ユーザー名とパスワードを入力します。



6.「**y**」と入力してプロキシサーバーのセットアップを完了します。

ライセンス管理

May 10, 2016

XenMobile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、「Installing Licenses on NetScaler Gateway」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、「シトリックスのライセンスシステム」を参照してください。

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

XenMobileのライセンスをダウンロードする前に、Citrixライセンスサーバーをインストールする必要があります。ライセンスファイルを生成するには、Citrixライセンスサーバーをインストールしたサーバー名が必要となります。XenMobileをインストールする場合、そのサーバーにはデフォルトでCitrixライセンスサーバーがインストールされます。または、既存のCitrixライセンスサーバー展開を使ってXenMobileのライセンスを管理できます。Citrixライセンスサーバーのインストール、展開、および管理について詳しくは、「製品ライセンスの有効化」を参照してください。
注：XenMobile 10では、Citrixライセンスサーバー11.12.1以降が必要です。それより古いバージョンのライセンスサーバーはXenMobile 10で動作しません。
重要：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

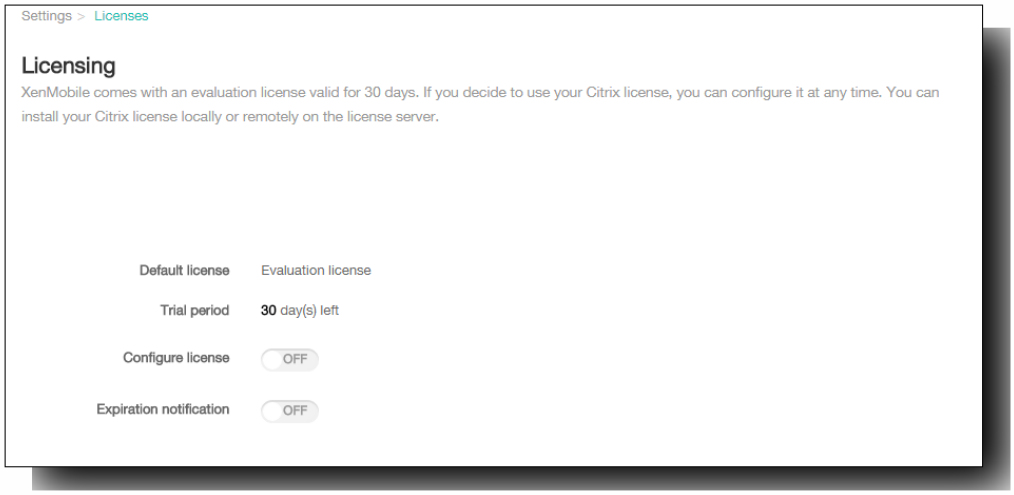
ライセンスがない場合、30日間は試用モードでXenMobileのすべての機能を操作することができます。この試用モードを使用できるのは、インストールから30日間の1回限りです。有効なXenMobileライセンスを使用できるかどうかに関係なく、XenMobile Webコンソールへのアクセスはブロックされません。

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の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が使用できなくなります。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コンソールで［Licensing］ページを開くには

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



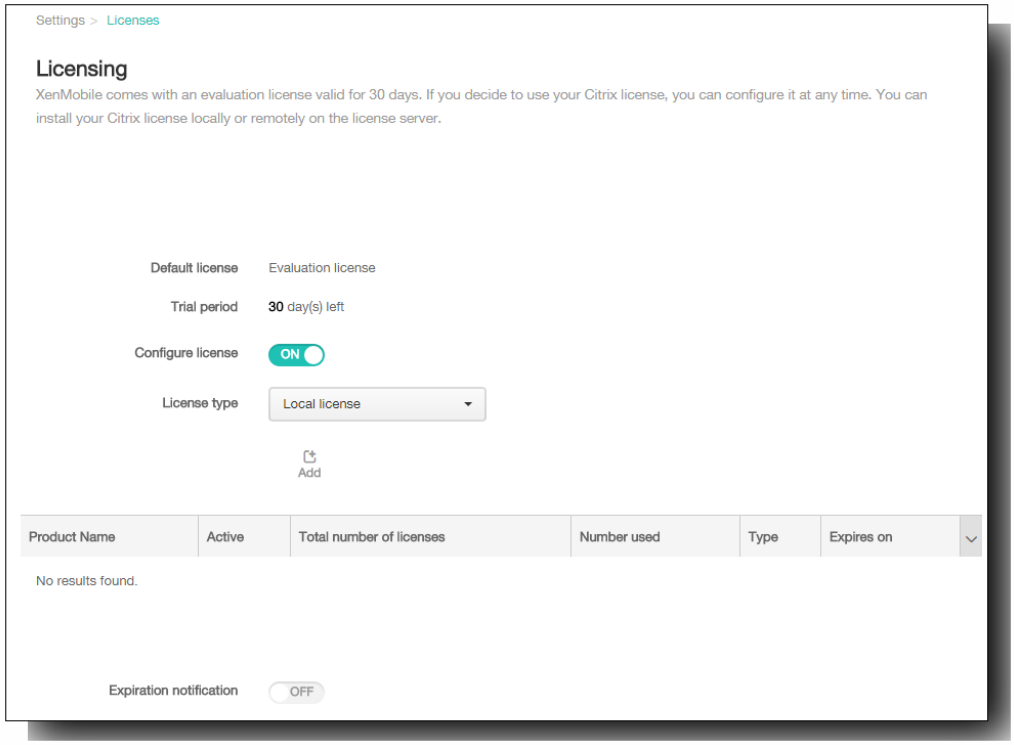
1. XenMobileコンソールで、［Configure］の［Settings］をクリックします。
2. ［Licensing］をクリックします。 ［Licensing］ページが開きます。

ローカルライセンスを追加するには

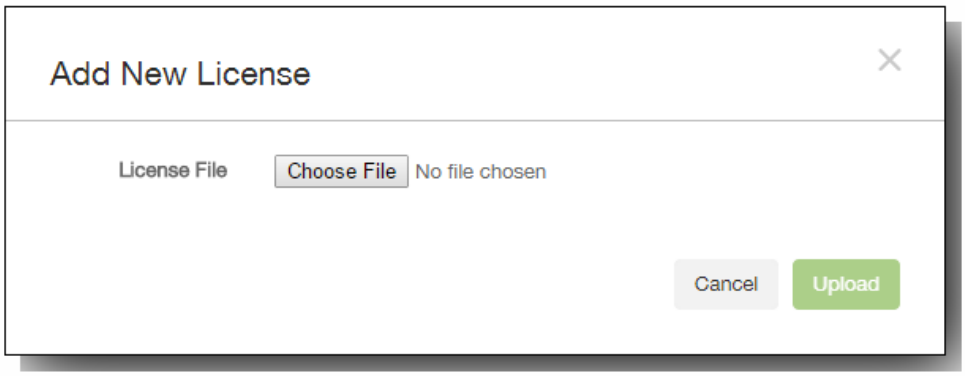
新しいライセンスを追加すると、表にライセンスが表示されます。最初に追加したライセンスは自動的にアクティブ化されます。カテゴリ（Enterpriseなど）および種類（デバイスなど）が同じライセンスを複数追加した場合、表ではこれらのライセンスが1つの行として表示されます。この場合、［Total number of license］と［Number used］に、共通するライセンスの合計数が表示されます。［Expires on］の日付は、共通するライセンスのうち最も後の有効期限を示します。

ローカルライセンスの管理は、すべてXenMobileコンソールで行います。

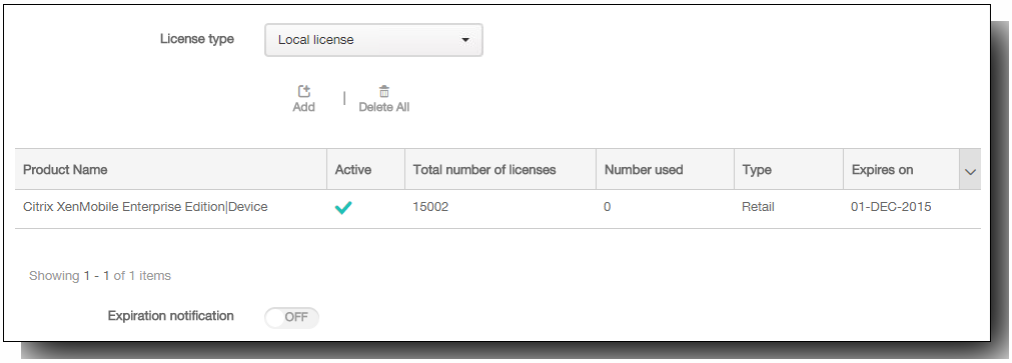
1. ライセンス管理コンソールを介してSimple License Serviceから、またはCitrix.comのアカウントから直接、ライセンスファイルを入手します。詳しくは、「ライセンスファイルの入手」を参照してください。
2. コンソールで、［Configure］、［Settings］、［Licenses］の順にクリックします。 ［Licensing］ページが開きます。
3. ［Configure license］を［On］に設定します。 ［License type］ボックス、［Add］ボタン、ライセンスの表が表示されます。ライセンスの表には、XenMobileで使用したライセンスが表示されます。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。



4. ［License type］が［Local license］に設定されていることを確認して、［Add］をクリックします。 ［Add New License］ダイアログボックスが開きます。



5. ［Add New License］ダイアログボックスで、［Choose File］をクリックし、ライセンスを参照して指定します
6. ［Upload］をクリックします。 ライセンスがローカルにアップロードされ、表に表示されます。

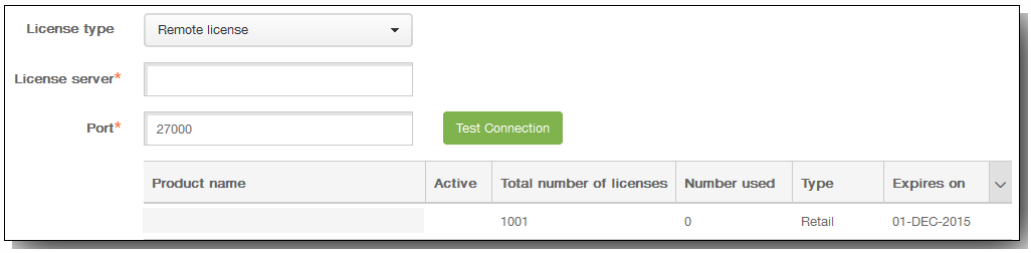


7. ライセンスが［License］ページの表に表示されたら、ライセンスをアクティブ化します。 この表で最初のライセンスの場合、ライセンスは自動的にアクティブ化されます。

リモートライセンスを追加するには

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

1. ［Licensing］ページで、［Configure license］を［On］に設定します。 ［License type］ボックス、［Add］ボタン、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ライセンスをだ追加していない場合、この表は空白です。
2. ［License type］を［Remote license］に設定します。 ［Add］ボタンが、［License server］フィールドおよび［Port］フィールドと、［Test Connectivity］ボタンに置き換わります。

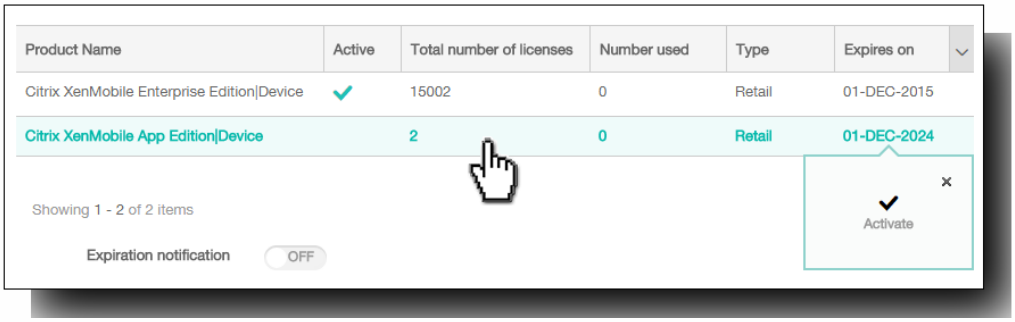


3. ［License server］ボックスに、リモートライセンスサーバーのIPアドレスまたは完全修飾ドメイン名（FQDN）を入力します。
4. ［Port］フィールドで、デフォルトポートをそのまま使用するか、ライセンスサーバーとの通信に使用するポート番号を入力します。
5. ［Test Connection］をクリックします。 接続が成功した場合、XenMobileはライセンスサーバーに接続し、使用可能なライセンスがライセンスの表に表示されます。接続が成功しなかった場合は、正しい情報を入力していることとすべての接続がアクティブであることを確認します。
   注：ライセンスが1つのみの場合は、自動的にアクティブ化されます。

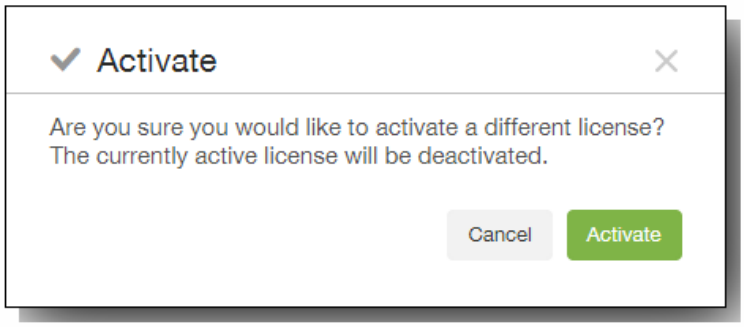
別のライセンスをアクティブ化するには

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

1. ［Licensing］ページのライセンスの表で、アクティブ化するライセンスの行をクリックします。 ［Activate］確認ボックスが、その行の横に表示されます。



2. ［Activate］をクリックします。 ［Activate］ダイアログボックスが開きます。

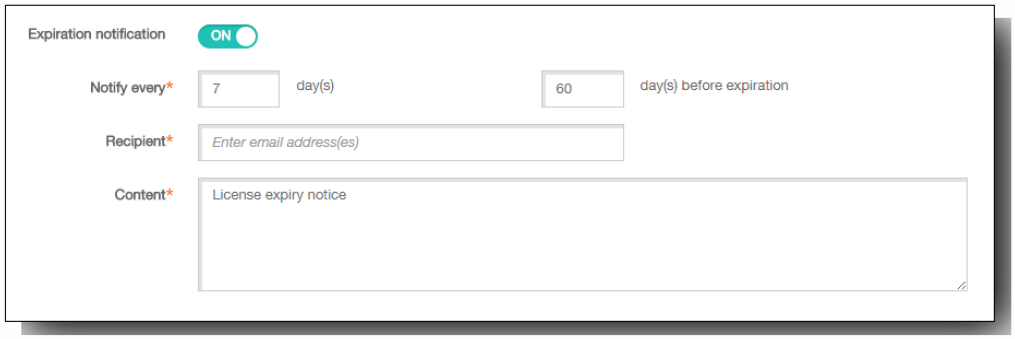


3. ［Activate］をクリックします。
   重要：選択したライセンスをアクティブ化すると、現在アクティブなライセンスは非アクティブになります。
   選択したライセンスがアクティブ化されます。

有効期限通知を自動化するには

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

1. ［Licensing］ページで、［Expiration notification］を［On］に設定します。 通知に関連するフィールドが新たに表示されます。



2. ［Notify every］に以下を入力します。

- 通知が送信される頻度（7日ごとなど）。
- 通知の送信を開始する時期（ライセンス有効期限の60日前など）。

3. ［Recipient］フィールドに、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。
4. ［Content］フィールドに、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。
5. ［Save］をクリックします。 有効期限の残りが指定日数になると、指定した受信者への、この手順で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繰り返されます。

XenMobileコンソールの概要

May 10, 2016

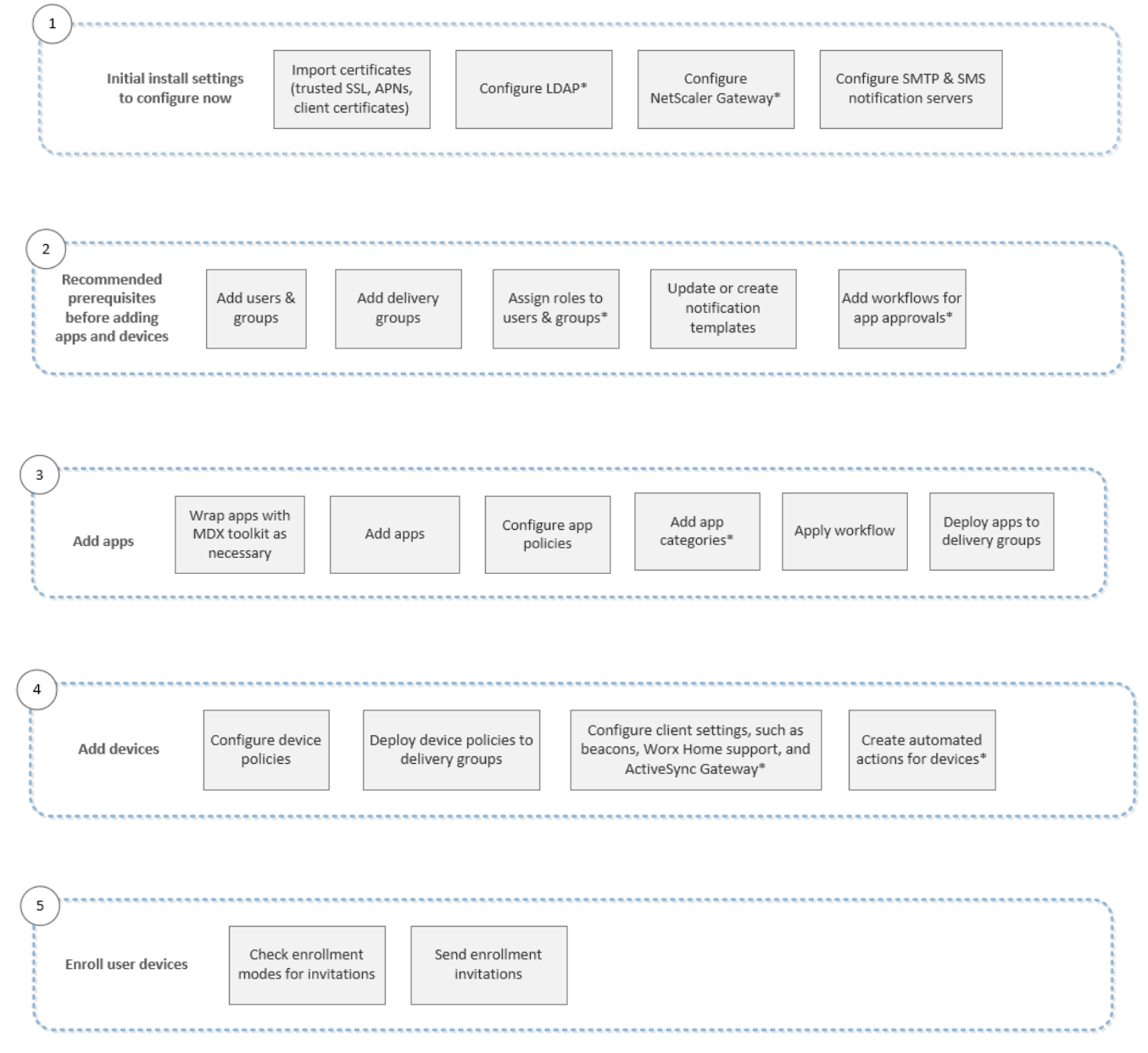
XenMobileコンソールは、XenMobile 9以前のバージョンのApp ControllerコンポーネントとDevice Managerコンポーネントをまとめた、XenMobile 10の統合管理ツールです。ここでの説明は、XenMobileがインストール済みで、コンソールで作業できる状態になっていることが前提となっています。XenMobileをインストールする必要がある場合は、「XenMobileのインストール」を参照してください。

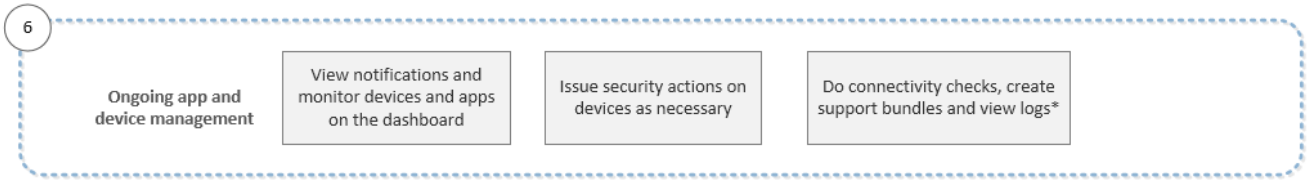
XenMobileコンソールは、Firefox、Chrome、Internet Explorerのそれぞれ最新の2つのバージョンでサポートされます。

コンソールで次にどこへ進めばよいかを確認できるよう、以下の図に、アプリケーションおよびデバイスの継続的な管理を準備するための推奨されるワークフローを示しています。最初の一連の推奨事項は、インストール手順実行中にスキップした可能性のある初期設定が対象になっています。

ヒント：各行をクリックするとトピックが開き、詳細や手順へのリンクを確認できます。

注：アスタリスクが付いている項目はオプションです。



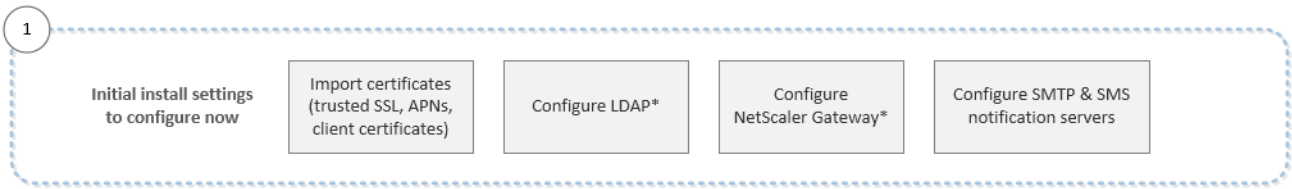


初期設定のワークフロー

May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。初期構成画面に戻ることはできないため、インストール構成の一部をその時点でスキップした場合は、コンソールで以下の設定を構成できます。ユーザー、アプリケーション、デバイスの追加を開始する前に、これらのインストール設定を完了することを考慮する必要があります。開始するには、**[Configure]**の**[Settings]**をクリックします。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

注：アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下のeDocsトピックスを参照してください。

- XenMobileでの証明書
- LDAP構成
- NetScaler GatewayとXenMobile
- XenMobileでの通知

コンソールの前提条件のワークフロー

May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

このワークフローは、アプリケーションとデバイスを追加する前に構成する、推奨される前提条件を示しています。
注：アスタリスクが付いている項目はオプションです。

各設定の詳細と具体的な手順については、以下のeDocsトピックスを参照してください。

- ユーザーアカウント、役割、および登録設定の構成
- XenMobileでのデリバリーグループの管理
- XenMobileでRBACを使用してカスタムの役割を作成または更新するには
- XenMobileで通知テンプレートを作成または更新するには
- 登録モードを構成してSelf Help Portalを有効化するには
- ワークフローを作成および管理するには

アプリケーションの追加のワークフロー

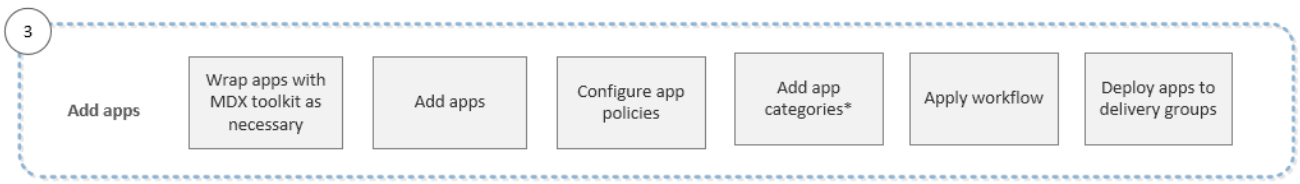
May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

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

注：アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下のeDocsトピックスを参照してください。

- MDX Toolkitによるアプリのラップ
- XenMobileへのアプリケーションの追加
- iOS、Android、およびWindows Phone 8.1用のMDXポリシーの概要
- アプリケーションカテゴリを追加するには
- ワークフローを作成および管理するには
- XenMobileでのデリバリーグループの管理

デバイスの追加のワークフロー

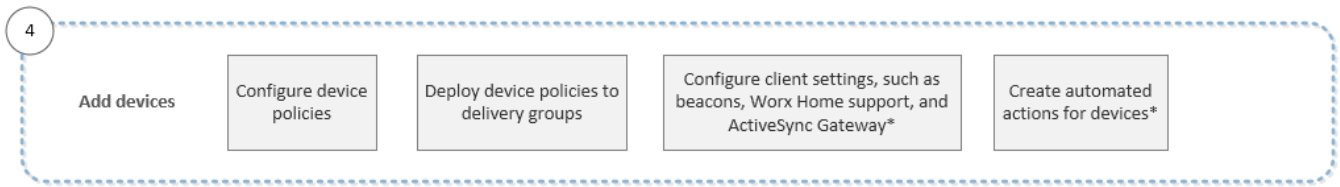
May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。次に、「アプリケーションの追加のワークフロー」に従ってアプリケーションを追加できます。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

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

注：アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下のeDocsトピックスを参照してください。

- XenMobileでのデバイスの追加およびデバイスの詳細の表示
- プラットフォーム別のXenMobileデバイスポリシー
- XenMobileでのデリバリーグループの管理
- XenMobileクライアント設定の構成
- XenMobileでの自動化された操作の作成

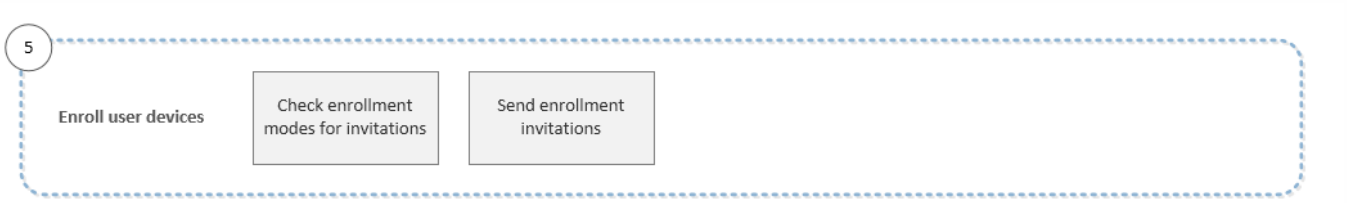
ユーザーデバイスの登録のワークフロー

May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。次に、「アプリケーションの追加のワークフロー」に従ってアプリを追加し、「デバイスの追加のワークフロー」に従ってデバイスを追加および登録できます。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

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



各設定の詳細と具体的な手順については、以下のeDocsトピックスを参照してください。

- ユーザーアカウント、役割、および登録設定の構成
- 登録モードを構成してSelf Help Portalを有効化するには

アプリケーションおよびデバイスの継続的な管理のワークフロー

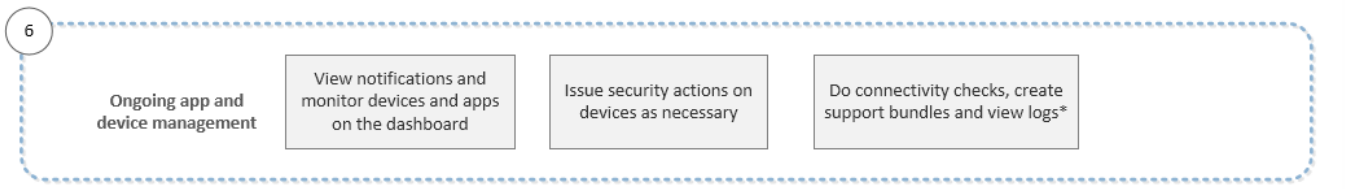
May 10, 2016

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。インストール構成の一部をその時点でスキップした場合は、推奨される初期設定を「初期設定のワークフロー」で確認できます。

次に、「コンソールの前提条件のワークフロー」に従って、アプリケーションとデバイスを追加する前のいくつかの前提条件を構成できます。次に、「アプリケーションの追加のワークフロー」に従ってアプリケーションを追加し、「デバイスの追加のワークフロー」に従ってデバイスを追加および登録できます。最初の4つのワークフローが完了した後、「ユーザーデバイスの登録のワークフロー」に従ってユーザーデバイスを登録します。ワークフロー全体を確認するには、「XenMobileコンソールの概要」を参照してください。

この6番目で最後のワークフローは、コンソールで実行可能であり推奨される、アプリケーションおよびデバイスの継続的な管理作業を示しています。

注：アスタリスクが付いている項目はオプションです。



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

XenMobileコンソールのフィルターおよび表

May 10, 2016

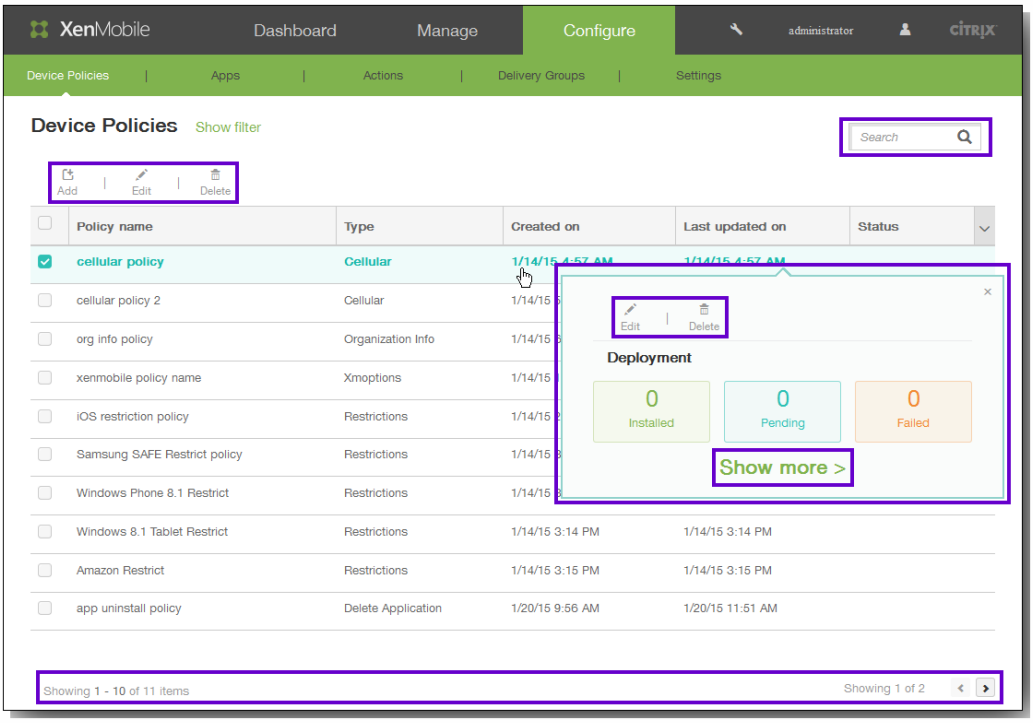
フィルターと表は、XenMobileコンソールのすべてのタブ（［Devices］、［Enrollment］、［Device Policies］、［Apps］、［Actions］、［Delivery Groups］）にあります。フィルターでは、コンソールのいずれかの領域の情報を絞り込み、表示する情報を的確に見つけることができます。表では、クリックによって、表内の情報に対するアクションを実行するためのオプションを表示できます。

XenMobileコンソールの表でオプションを表示するには

コンソールの表の情報に対するアクションを実行するためのさまざまなオプションを、いくつかの異なる方法で表示できます。

- 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できます。
- 複数のポリシーの横にあるチェックボックスをオンにして、それらのポリシーすべてを一度に削除できます。
- 一覧でポリシーをクリックして、その項目の右側にオプションメニューを表示できます。［Show More］をクリックすると、構成に関する詳細の一覧が表示されます。
- ポリシー名の全体または一部を［Search］ボックスに入力して、一覧に表示されるポリシーの数を絞り込むことができます。

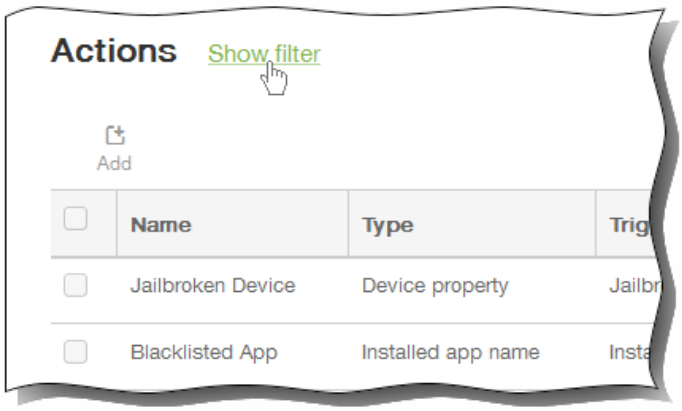
次の図は、コンソールの［Device Policies］領域でオプションがどのように表示されるかを示しています。一覧に表示される項目は1ページにつき10項目のみです。ページの右下の三角をクリックして、前後のページに移動します。



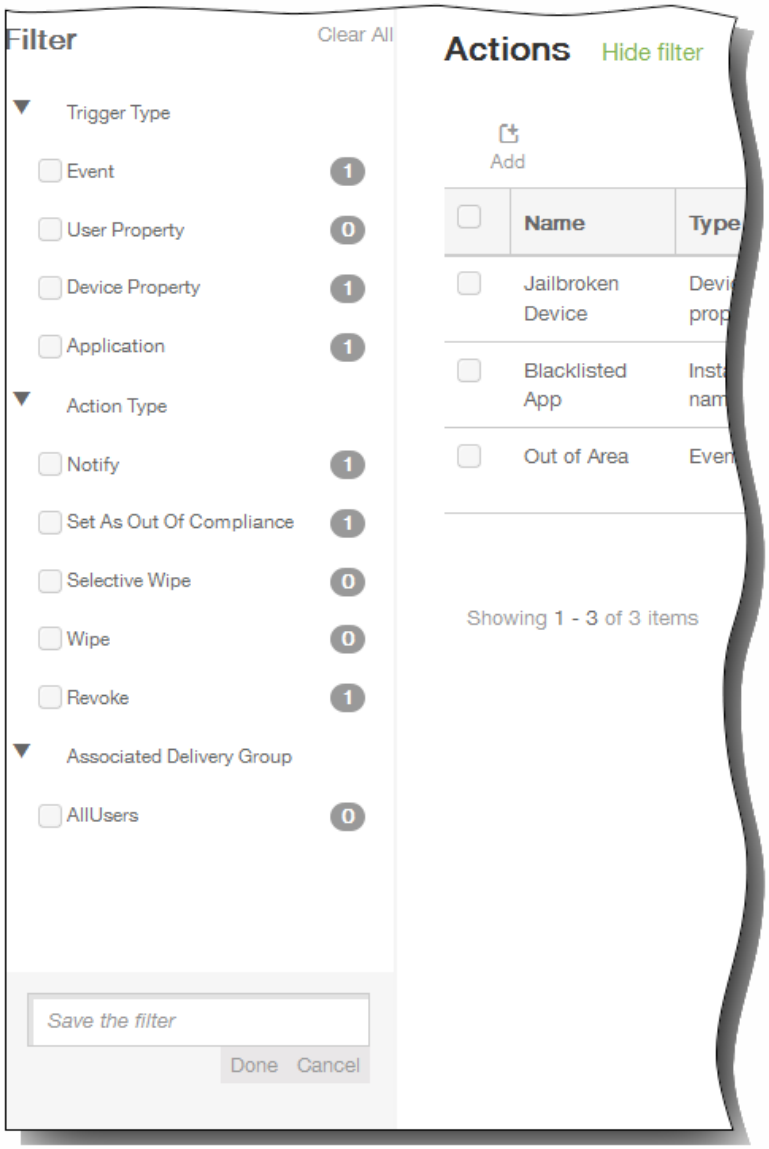
XenMobileコンソールで情報をフィルターするには

コンソールの［Devices］、［Enrollment］、［Device Policies］、［Apps］、［Actions］、［Delivery Groups］などの領域で特定の一部の情報を表示する場合、選択した条件に基づいて一覧をフィルタリングできます。次の手順では、例として［Actions］ページを使用していますが、コンソールのどのページでもフィルタリングの手順は同じです。

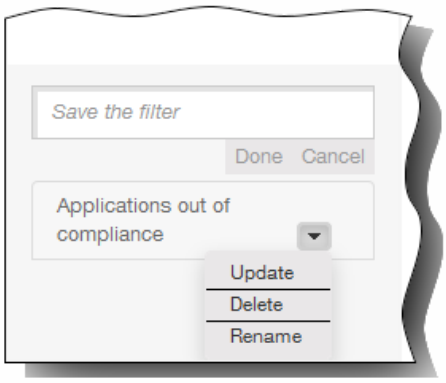
1. ［Actions］ページで、［Show Filter］をクリックします。



フィルターパネルが開き、条件の一覧が表示されます。この条件を使用して、[Actions] 一覧をフィルタリングできます。各条件の右に表示されている数字は、その条件に含まれるアクションの数を表しています。



2. フィルターの左にある三角をクリックしすると、そのフィルターで使用できるオプションが表示されます。
3. 使用するフィルター条件を選択します。 ［Actions］一覧が、選択した条件に一致するアクションに絞り込まれます。
4. 次のいずれかを行います。
   - ［Hide Filter］をクリックして、フィルターされた一覧に対する操作を続けます。
   - ［Clear All］をクリックして、完全な一覧に戻します。
5. 選択した条件をカスタムフィルターとして保存する場合は、［Filter］パネルの下部にある［Save the filter］フィールドに説明的な名前を入力して、 ［Done］をクリックします。 フィルターを保存しない場合は、［Cancel］をクリックします。



6. フィルターを保存すると、［Filter］パネルの下部でそのフィルターを選択できます。
   注：フィルター名の右の三角をクリックすると、そのフィルターを新しい条件または変更した条件で更新したり、フィルターを削除したり、フィルター名を変更したりすることができます。

通知

May 10, 2016

XenMobileでの通知は以下の目的で利用できます。

- 多くのシステム関連機能に関して、選択したグループのユーザーに連絡します。また、iOSデバイスを持つすべてのユーザー、コンプライアンスを満たしていないデバイスのユーザー、個人所有のデバイスを持つすべてのユーザーなど、特定のユーザーを対象にこれらの通知を行うこともできます。
- ユーザーとデバイスを登録します。
- コンプライアンスに関する問題が原因で、ユーザーのデバイスが社内ドメインからブロックされようとしているときや、デバイスがジェイルブレイクまたはルート化されたときなど、特定の条件が満たされた場合に（自動化された操作を使用して）ユーザーに自動的に通知します。自動化された操作について詳しくは、「XenMobileでの自動化された操作の作成」を参照してください。

XenMobileで通知を送信するには、ゲートウェイおよび通知サーバーを構成する必要があります。XenMobileで通知サーバーを設定して、SMTP（簡易メール転送プロトコル：Simple Mail Transfer Protocol）サーバーやショートメッセージサービス（SMS）のゲートウェイサーバーを構成し、電子メールやテキスト（SMS）通知をユーザーに送信することができます。通知では、SMTPまたはSMSの2種類のチャネル経由でメッセージを送信できます。

- SMTPはコネクション型のテキストベースプロトコルで、通常はTCP（Transmission Control Protocol）経由で、メール送信者がコマンド文字列を発行して必要なデータを供給し、メール受信者と通信します。SMTPセッションは、SMTPクライアント（メッセージの送信者）から送信されたコマンドと、コマンドに対応する、SMTPサーバーからの応答によって構成されます。
- SMSは、電話、Web、またはモバイル通信システムのテキストメッセージサービスコンポーネントです。標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

また、XenMobileでキャリアSMSゲートウェイを設定して、電話会社のSMSゲートウェイ経由で送信される通知を構成することもできます。電話会社はSMSゲートウェイを使用して、通信ネットワークと相互にSMSメッセージを送受信します。これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

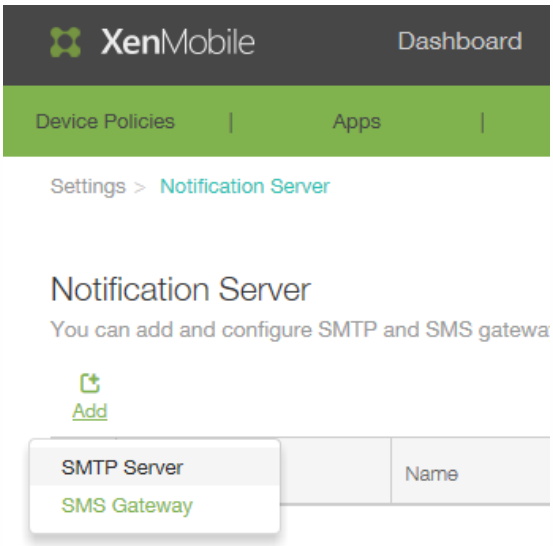
このトピックの手順では、SMTPサーバー、SMSゲートウェイ、キャリアSMSゲートウェイの追加について説明します。

SMTPサーバーおよびSMSゲートウェイを構成するには

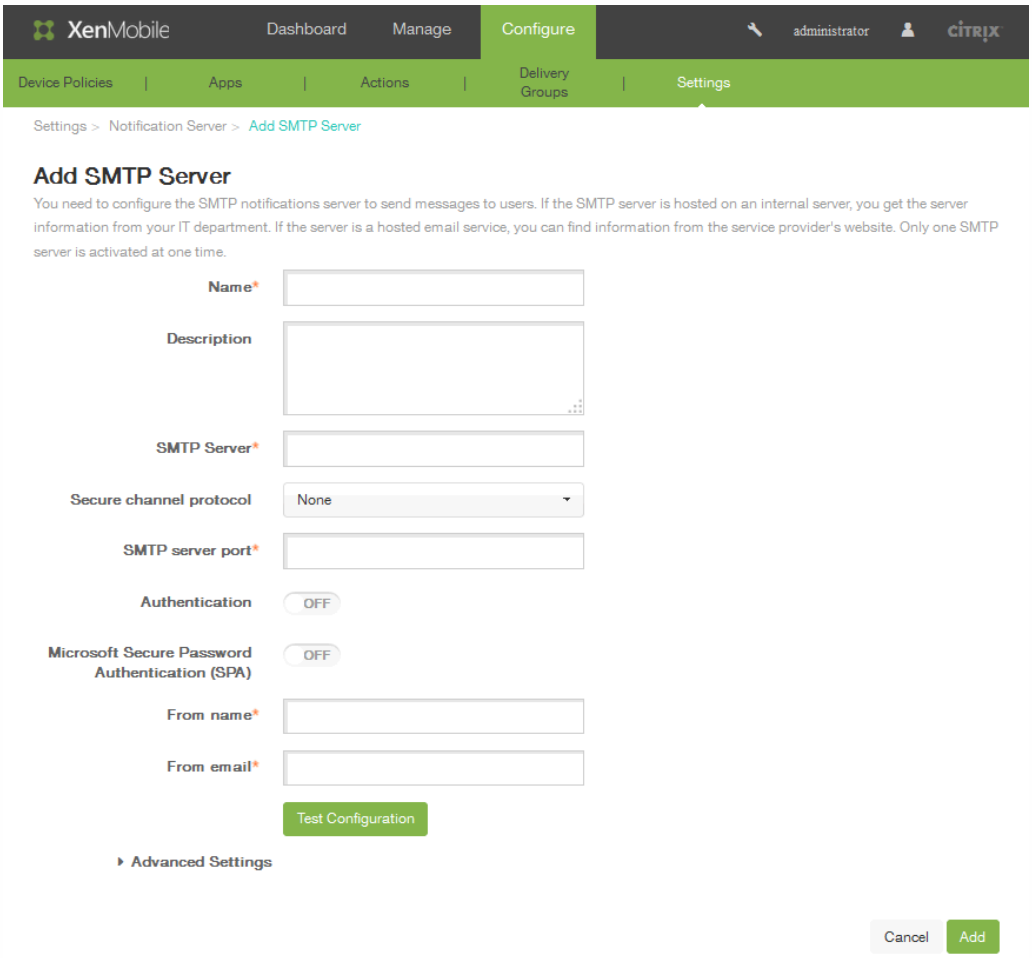
前提条件

- SMSゲートウェイを構成する前に、システム管理者に問い合わせてサーバー情報を確認してください。SMSサーバーが社内サーバーでホストされているか、ホストされている電子メールサービスに含まれているかを確認することが重要です。後者の場合は、サービスプロバイダーのWebサイトからの情報が必要です。
- メッセージをユーザーに送信するためのSMTP通知サーバーを構成する必要があります。サーバーが社内サーバーでホストされている場合は、システム管理者に構成情報を問い合わせてください。サーバーが、ホストされている電子メールサービスの場合は、サービスプロバイダーのWebサイトで適切な構成情報を確認してください。
- SMTPサーバーとSMSサーバーは、それぞれ一度に1つのみがアクティブになります。
- 通知を正しく送信するには、ネットワークのDMZ内のXenMobileからポート25を開き、内部ネットワークのSMTPサーバーにポイントバックする必要があります。

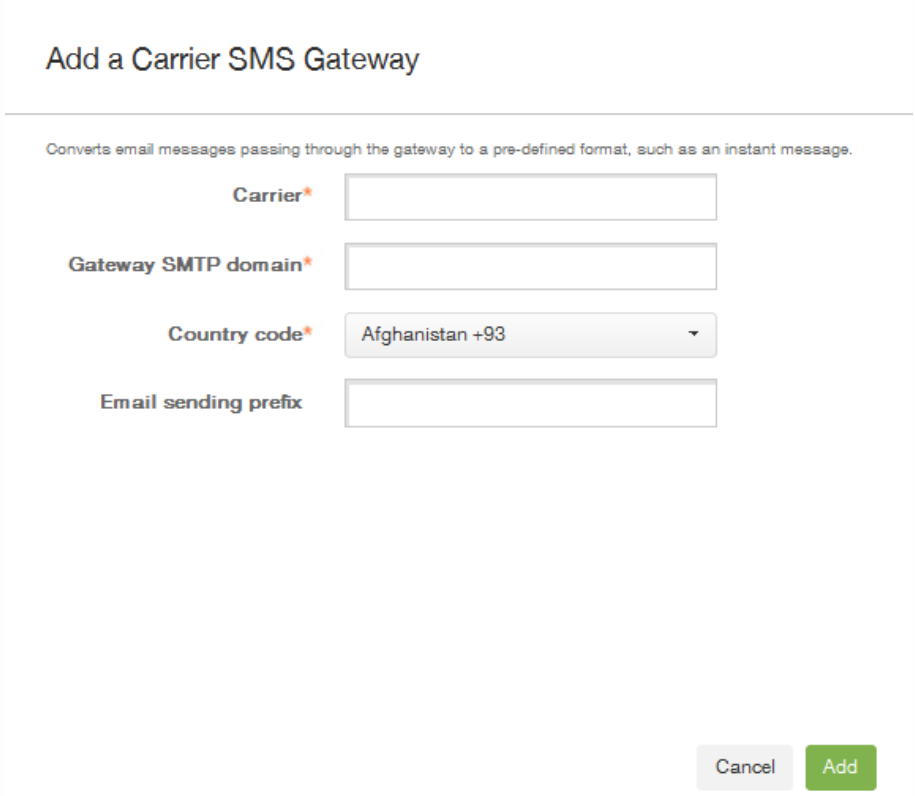
1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Notification Server］の順にクリックします。
   ［Notification Server］構成ページが開きます。



2. ［Add］をクリックし、［SMTP Server］または［SMS Gateway］をクリックして、以下の選択ごとに後続の手順に従います。
   - SMTPサーバーを追加するには、手順3.～6.に従います。
   - SMSゲートウェイを追加するには、手順7.～9.に従います。
3. SMTPサーバーを追加するために［SMTP Server］をクリックした場合、［Add SMTP Server］ページが開きます。



4. 次の設定を構成します。
   - Name：このSMTPサーバーアカウントに関連付ける名前を入力します。
   - Description：任意で、サーバーの説明を入力します。
   - SMTP Server：サーバーのホスト名を入力します。ホスト名には、完全修飾ドメイン名（FQDN）またはIPを指定できます。
   - Secure channel protocol：（サーバーが安全な認証を使用するよう構成されている場合）一覧から、サーバーが使用する適切なセキュアチャネルプロトコル（［SSL］、［TLS］、または［None］）をクリックします。デフォルトでは、このフィールドは［None］に設定されています。
   - SMTP server port：SMTPサーバーが使用するポートを入力します。デフォルトでは、ポートは25に設定されています。SMTP接続でSSLセキュアチャネルプロトコルを使用する場合、ポートは465に設定されます。
   - Authentication：［ON］または［OFF］を選択します。デフォルトでは、この機能は無効になっています。
   - Microsoft Secure Password Authentication（SPA）：SMTPサーバーがSPAを使用している場合は、［ON］をクリックします。デフォルトでは、この機能は無効になっています。
   - From Name：クライアントがこのサーバーから通知メールを受信したとき、メールの送信者として表示される名前を入力します。たとえば、「Corporate IT」です。
   - From email：SMTPサーバーによって送信された通知に、メール受信者が返信する場合に使用されるメールアドレスを入力します。
   - Test Configuration：クリックすると、テストのメール通知が送信されます。
5. ［Advanced Settings］を展開して以下の設定を構成します。
   - Number of SMTP retries：SMTPサーバーからのメッセージの送信が失敗した場合に再試行する回数を入力します。デフォルトでは、このフィールドは5に設定されています。
   - SMTP Timeout：SMTP要求送信時に待機する時間（秒）を入力します。送信しているメッセージが、タイムアウトに起因して失敗し続ける場合には、この値を大きくします。この値を小さくするとタイムアウト回数が多くなり、配信されないメッセージが増える場合があるため、注意してください。デフォルトでは、このフィールドは30秒に設定されています。
   - Maximum number of SMTP recipients：SMTPサーバーによって送信される各メールメッセージの最大受信者数を入力します。デフォルトでは、この値は100に設定されています。
6. SMTPサーバーを構成したら、**［Add］**をクリックします。
7. SMSゲートウェイを構成するには、［Notification Server］構成ページで、［Add］をクリックして［SMS Gateway］をクリックします。
   ［Add SMS Gateway］ページが開きます。



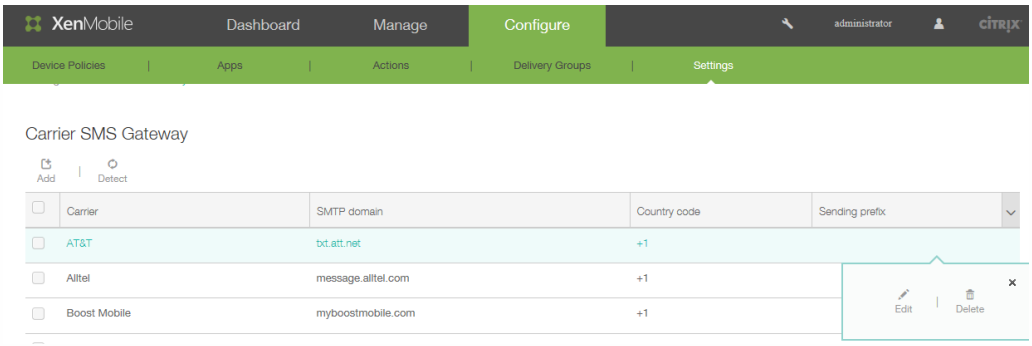
注：XenMobileはNexmo SMSメッセージのみをサポートします。Nexmoメッセージを使用するためのアカウントがまだない場合は、Webサイトにアクセスしてアカウントを作成してください。

8. 次の設定を構成します。
   - Name：SMSゲートウェイ構成を識別します。
   - Description：任意で、構成の説明を入力します。
   - Key：アカウントをアクティブ化するときにシステム管理者から提供された、数値形式の識別子を入力します。
   - Secret：パスワードを紛失した場合や盗まれた場合にアカウントへのアクセスに使用する、システム管理者から提供されたシークレットを入力します。
   - Virtual Phone Number：このフィールドは、北米の電話番号（プレフィックスが+1）への送信時に使用されます。Nexmo仮想電話番号を入力する必要があります。そのほかの場合は、意味のあるラベルまたは名前を入力します。仮想電話番号はNexmoのWebサイトで購入できます。
   - HTTPS：NexmoへのSMS要求の伝送にHTTPSを使用する場合はオンにします。
   - Country Code：一覧から、組織内受信者のデフォルトのSMS国コードプレフィックスを選択します。このフィールドは常に+記号で始まります。
   - Test Configuration：クリックすると、現在の構成を使用してテストメッセージが送信されます。認証エラーや仮想電話番号エラーなど、接続エラーが直ちに検出されて表示されます。メッセージは、携帯電話間で送信された場合と同様の所要時間で受信されます。
9. ［Add］をクリックします。

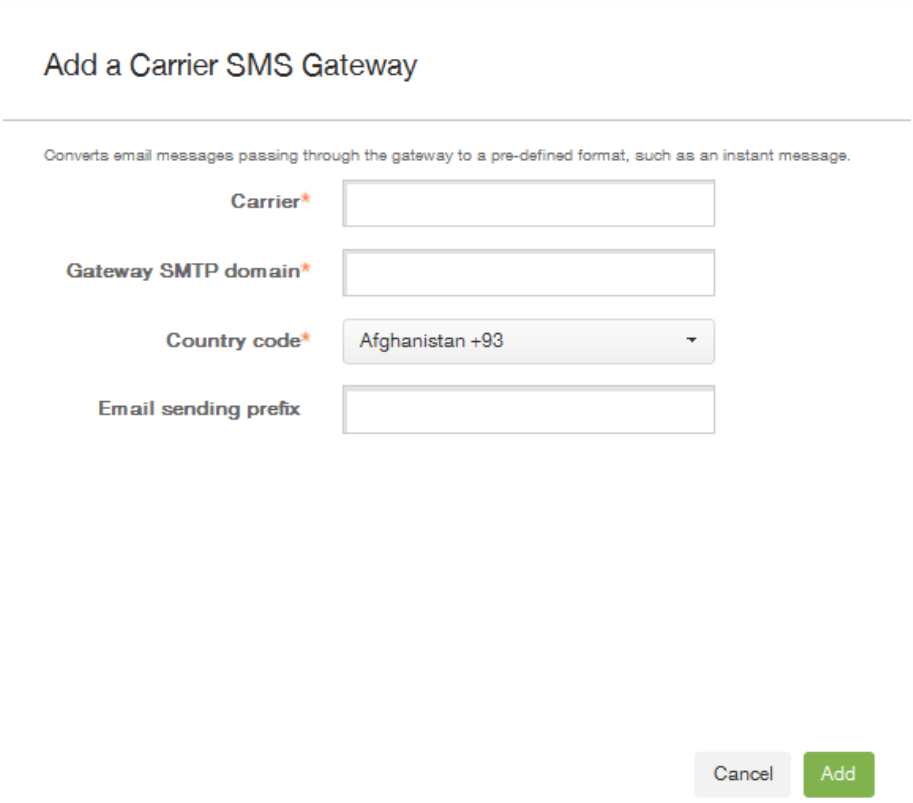
キャリアSMSゲートウェイを追加するには

XenMobileでキャリアSMSゲートウェイを設定して、電話会社のSMSゲートウェイ経由で送信される通知を構成できます。電話会社はショートメッセージサービス（SMS）ゲートウェイを使用して、通信ネットワークと相互にSMSメッセージを送受信します。これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Carrier SMS Gateway］の順にクリックします。 ［Carrier SMS Gateway］構成ページが開きます。



2. 新しい電話会社を追加するには［Add］をクリックします。 ゲートウェイを自動的に検出するには［Detect］をクリックします。 ［Add a Carrier SMS Gateway］ダイアログボックスが開きます。



3. 以下の情報を入力します。XenMobileはNexmo SMSメッセージのみをサポートします。Nexmoメッセージを使用するためのアカウントがまだない場合は、Webサイトにアクセスしてアカウントを作成してください。
   1. Carrier：電話会社の名前を入力します。
   2. Gateway SMTP domain：SMTPゲートウェイに関連付けられたドメインを入力します。
   3. Country code：一覧から、電話会社の国コードを選択します。
   4. Email sending prefix：任意で、メール送信プレフィックスを指定します。

証明書

Oct 24, 2016

XenMobileでは証明書を使用し、セキュリティで保護された接続を作成してユーザーを認証します。

XenMobileには、サーバーへの通信フローを保護するためにインストール中に生成される自己署名SSL（Secure Sockets Layer）証明書がデフォルトで含まれています。 このSSL証明書を、既知のCA（Certificate Authority：証明機関）からの信頼されるSSL証明書に置き換えることをお勧めします。

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

XenMobileでiOSデバイスを登録して管理するには、AppleのApple Push Notification service（APNs）証明書を設定および作成する必要があります。 手順については、「APN証明書の要求」を参照してください。

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

XenMobileコンポーネント	**証明書の形式**	**必要な証明書の種類**
NetScaler Gateway	PEM（BASE64） PFX（PKCS#12）	SSL、ルート NetScaler Gatewayによって自動的にPFXがPEMに変換されます。
XenMobileサーバー	PEMまたは PFX（PKCS#12）	SSL、SAML、APNS XenMobileはインストール処理中に完全なPKIも生成します。 XenMobileサーバーは、拡張子が.pemの証明書をサポートしません。 openssslコマンドを使用して、PEMファイルからPFXファイルを生成します。 openssl pkcs12 -export -out certificate.pfx -in certificate.pem
StoreFront	PFX（PKCS#12）	SSL、ルート

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

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

認証用のクライアント証明書の構成

NetScaler Gatewayでは、クライアント証明書を使用した認証がサポートされます。 NetScaler Gatewayにログオンするユー

ザーを、仮想サーバーに提示されるクライアント証明書の属性に基づいて認証することもできます。 クライアント証明書認証は、2要素認証を提供するために、LDAPやRADIUSなどのほかの種類の認証と一緒に使用することもできます。

クライアント側の証明書の属性でユーザーを認証するには、仮想サーバー上のクライアント認証が有効になっており、クライアント証明書を要求するように構成されている必要があります。 さらに、NetScaler Gateway上でルート証明書をその仮想サーバーにバインドする必要があります。

Netscaler Gatewayによるデバイス認証は、随意CAによって取得した証明書に対してはサポートされません。

NetScaler Gatewayにログオンしたユーザーの認証後、そのユーザー名の情報が証明書の特定フィールドから抽出されます。通常、このフィールドはSubject:CNです。 ユーザー名の抽出に成功すると、ユーザーの認証が完了します。 SSL（Secure Sockets Layer）ハンドシェイク時に有効な証明書が提供されなかったりユーザー名の抽出に失敗したりすると、認証に失敗します。

クライアント証明書に基づいて認証するには、デフォルトの認証の種類としてクライアント証明書を指定します。 また、「証明書アクション」を作成して、クライアントのSSL証明書に基づいた認証時の動作を定義することもできます。

XenMobile PKI

XenMobile PKI（Public Key Infrastructure：公開キーのインフラストラクチャ）の統合機能を使用して、デバイスで使用するセキュリティ証明書の配布とライフサイクルを管理できます。

XenMobileはインストール処理中に、デバイス認証用の内部PKIを作成します。

外部PKIを使用して証明書をデバイスに発行し、構成ポリシーで使用することや、NetScaler Gatewayに対するクライアント認証で使用することもできます。

このPKIシステムの主要機能はPKIエンティティです。PKIエンティティは、バックエンドコンポーネントをPKI処理用にモデル化します。このコンポーネントは、Microsoft、RSA、Entrust、Symantex、OpenTrust PKIなどの企業インフラストラクチャの一部です。PKIエンティティはバックエンドの証明書の発行と失効を処理します。PKIエンティティは証明書のステータスに関する認証済みの情報源です。XenMobile構成には、通常1つのバックエンドPKIコンポーネントにつき1つのPKIエンティティのみが含まれます。

PKIシステムの2つ目の機能は資格情報プロバイダーです。資格情報プロバイダーとは、証明書の発行とライフサイクルの特定の構成を指します。資格情報プロバイダーは、証明書の形式（サブジェクト、キー、アルゴリズム）および証明書の更新または失効の条件（該当する場合）などを管理します。資格情報プロバイダーは処理をPKIエンティティに委任します。つまり、資格情報プロバイダーはPKI処理が実行されるタイミングやそのときに使用するデータを管理しますが、PKIエンティティはそれらの処理の実行方法を管理します。通常、XenMobile構成では、1つのPKIエンティティに多くの資格情報プロバイダーが含まれます。

XenMobile証明書の管理

XenMobile環境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把握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のSSL証明書
SAML証明書（ShareFile用）

上記の証明書およびその他の内部リソース（StoreFrontやプロキシサーバーなど）用のルート証明書および中間CAの証明書
iOSデバイス管理用のAPN証明書
XMS WorxHome通知用の内部APN証明書
PKIに接続するためのPKIユーザー証明書

MDX Toolkit
Apple Developer証明書
Appleプロビジョニングプロファイル（アプリケーションごと）
Apple APN証明書（WorxMailで使用）
Androidキーストアファイル
Windows Phone – Symantec証明書

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

XenMobile証明書の有効期限ポリシー

証明書の有効期限が切れると、証明書が無効になり、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。

WorxMailのAPN証明書

Appleプッシュ通知サービス（APNs）証明書は毎年有効期限が切れるため、期限切れ前に新しいAppleプッシュ通知サービス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、WorxMailプッシュ通知に一貫性がなくなります。 また、アプリのプッシュ通知を送信することもできなくなります。

iOSデバイス管理用のAPN証明書

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

Apple Push Certificates Portalにログオンして、APN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。

よろしくお願いします。

Appleプッシュ通知サービス」

MDX Toolkit（iOS配布証明書）

物理的iOSデバイス（Apple App Storeのアプリケーション以外）上で実行する任意のアプリケーションにプロビジョニングプロファイルおよび対応する配布証明書で署名する必要があります。

既存のiOS Developer for Enterprise証明書とプロビジョニングプロファイルは、iOS 9と互換性がない場合があります。 詳しくは、「iOS 9用のWorx Appのラップ」を参照してください。

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 **[Settings]** をクリックして、 **[Configure]** をクリックします。
2. APN証明書、SSL証明書、リスナー証明書、ルート証明書、中間証明書を含むすべての証明書が有効であることを確認してください。

Androidキーストア

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

SymantecのWindows Phone用エンタープライズ証明書

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ユーザーは登録や同社が公開し署名したアプリのインストール、Windows phoneにインストールされた会社のアプリの起動ができなくなります。

NetScaler

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

期限の切れたNetScaler証明書を使用すると、Worx Storeへの登録やアクセス、WorxMail使用中のExchangeサーバーへの接続、HDXアプリの表示や起動ができません（期限の切れた証明書の種類によります）。

Expiry MonitorおよびCommand Centerによって、NetScaler証明書の記録を確認でき、証明書の有効期限が切れると通知が送

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

XenMobileでの証明書のアップロード

May 10, 2016

証明書はXenMobileサーバーで機能上使用されます。XenMobileへの証明書のアップロードは、XenMobileコンソールの［Certificates］領域で行います。これらの証明書には、CA（Certificate Authority：証明機関）証明書、RA（Registration Authority：登録機関）証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとして［Certificates］領域を使用することができます。これは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。

アップロードする各証明書は、［Certificates］の表で1つのエンティティとして表され、その内容がまとめられています。証明書が必要なPKI統合コンポーネントを構成するときに、サーバー証明書の一覧からコンテキスト依存の条件を満たすサーバー証明書を選択するよう求めるメッセージが表示されます。たとえば、XenMobileをMicrosoft CAと統合するように構成する場合があります。Microsoft CAへの接続はクライアント証明書を使用して認証されます。

秘密キーの要件

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

コンソールへの証明書のアップロード

CAが要求に署名するために使用するCA証明書（秘密キーなし）とクライアント認証用のSSLクライアント証明書（秘密キーあり）をアップロードできます。Microsoft CAエンティティを構成する場合は、CA証明書を指定する必要があります。CA証明書であるすべてのサーバー証明書の一覧から選択できます。同様に、クライアント認証を構成する場合は、XenMobileが秘密キーを持っているすべてのサーバー証明書の一覧から選択できます。

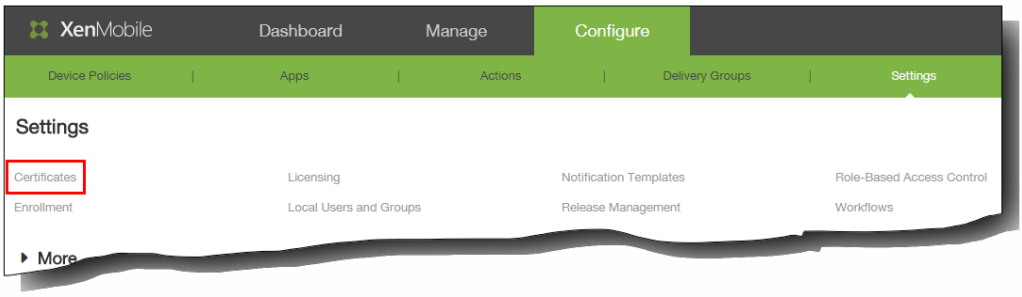
XenMobileは、証明書の以下の入力形式をサポートします。

- PEMまたはDERでエンコードされた証明書ファイル
- PEMまたはDERでエンコードされた秘密キーファイルが関連付けられたPEMまたはDERでエンコードされた証明書ファイル
- PKCS#12キーストア（P12。WindowsのPFXとも呼ばれます）

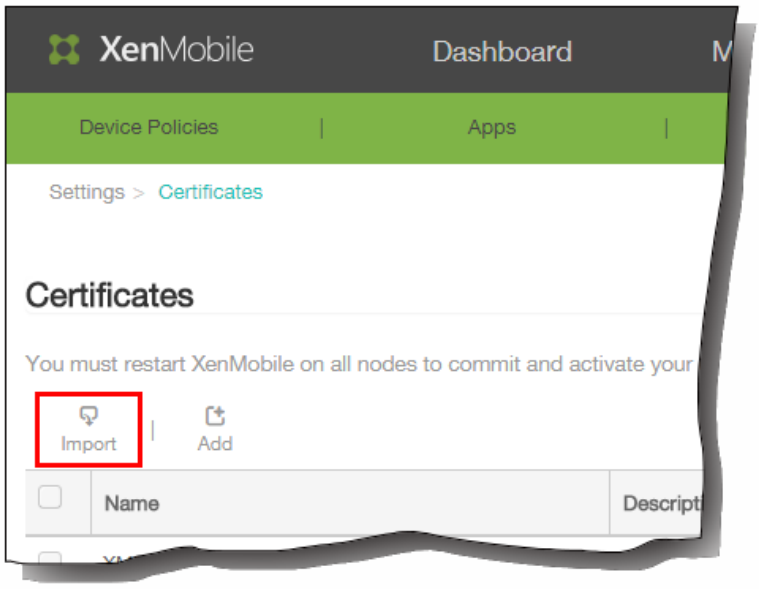
キーストアをインポートするには

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

1. XenMobileコンソールで、［Configure］、［Settings］、［Certificates］の順にクリックします。

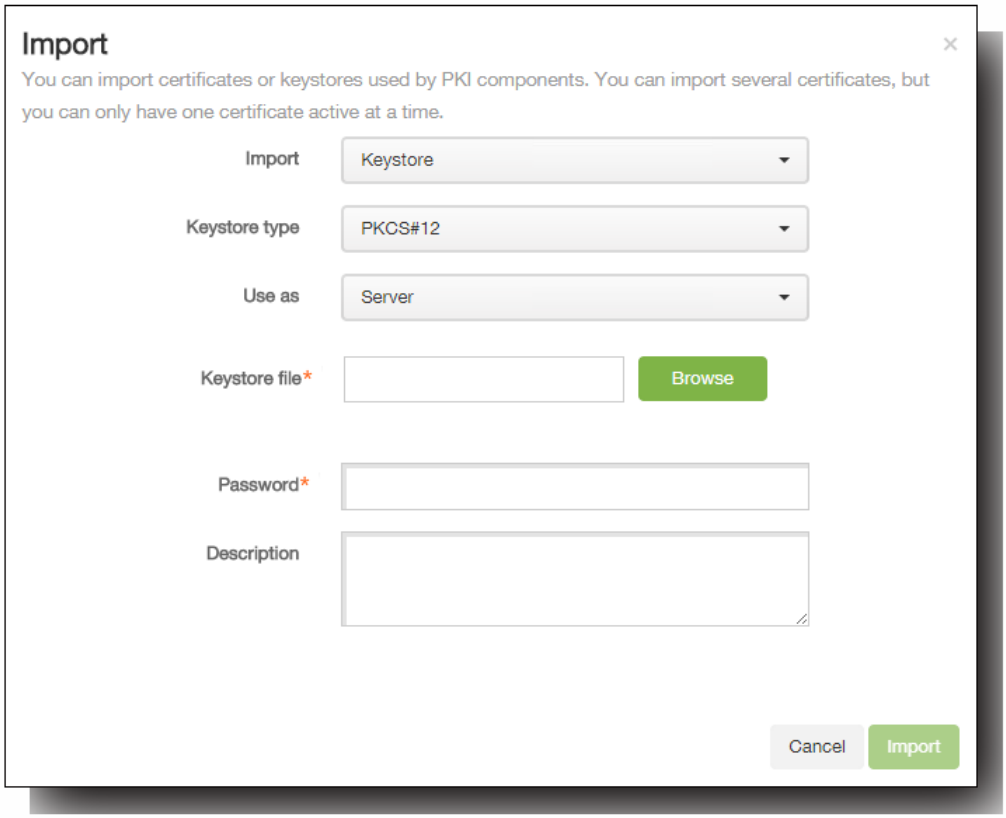


2. ［Certificates］ページで、［Import］をクリックします。



［Import］ダイアログボックスが開きます。

3. ［Import］ダイアログボックスの［Import］の一覧から、［Keystore］を選択します。



［Import］ダイアログボックスが、前の図に示されているように、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。

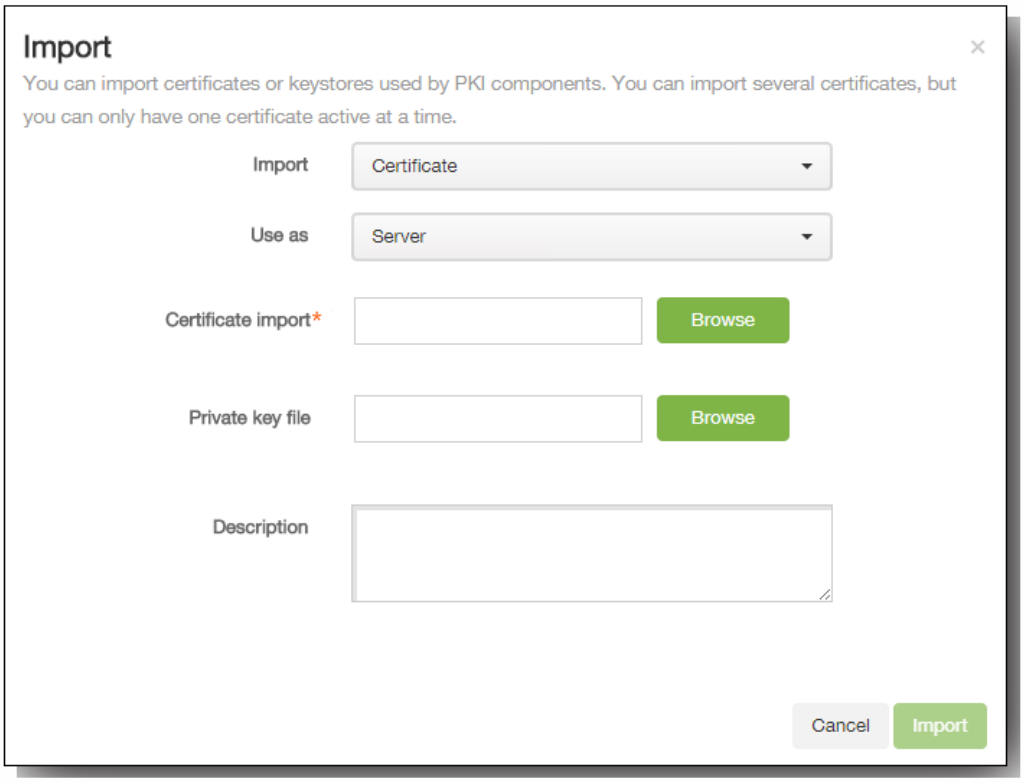
4. ［Keystore type］の一覧から、［PKCS#12］を選択します。
5. ［Use as］の一覧から、キーストアの使用方法を選択します。 以下の種類から選択できます。
   - **Server**。サーバー証明書はXenMobileサーバーで機能上使用される証明書で、XenMobile Webコンソールにアップロードされます。サーバー証明書には、CA証明書、RA証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。これは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。
   - **SAML**。Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Webサイト、およびアプリケーションへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
   - **APNs**。AppleのApple Push Notificationサービス（APNs）証明書を使用すると、Apple Push Networkを使用してモバイルデバイスを管理できます。
   - **SSL Listener**。SSL（Secure Sockets Layer）リスナーは、XenMobileにSSL暗号化アクティビティを通知します。
6. インポートするキーストアを参照して指定します。
7. ［Password］ボックスに、証明書に割り当てられたパスワードを入力します。
8. 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。
9. ［Import］をクリックします。キーストアが［Certificates］の表に追加されます。

証明書をインポートするには

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

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

1. XenMobileコンソールで、［Configure］、［Settings］、［Certificates］の順にクリックします。
2. ［Certificates］ページで、［Import］をクリックします。［Import］ダイアログボックスが開きます。
3. ［Import］ダイアログボックスの［Import］の一覧から、まだ選択していない場合は［Certificate］を選択します。



［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。

4. ［Use as］の一覧から、キーストアの使用方法を選択します。 以下の種類から選択できます。
   - **Server**。サーバー証明書はXenMobileサーバーで機能上使用される証明書で、XenMobile Webコンソールにアップロードされます。サーバー証明書には、CA証明書、RA証明書、およびインフラストラクチャのほかのコンポーネントでのクライアント認証用の証明書が含まれます。また、デバイスに展開する証明書のストレージとしてサーバー証明書を使用することができます。このオプションは特に、デバイスで信頼性を確立するために使用されるCAに適用されます。
   - **SAML**。Security Assertion Markup Language（SAML）証明書を使用すると、サーバー、Webサイト、およびアプリケーションへのシングルサインオン（Single Sign-On：SSO）アクセスを提供できます。
   - **SSL Listener**。SSL（Secure Sockets Layer）リスナーは、XenMobileにSSL暗号化アクティビティを通知します。
5. インポートする証明書を参照して指定します。
6. 任意で、証明書の秘密キーファイルを参照して指定します。 秘密キーは、証明書と組み合わせて暗号化と復号化で使用されます。
7. 任意で、証明書の説明を入力します。この説明は、ほかの証明書と区別するときに役立ちます。
8. ［Import］をクリックします。証明書が［Certificates］の表に追加されます。

証明書の更新

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

証明書を最も効果的に更新するには、XenMobileコンソールで［Configure］、［Settings］、［Certificates］の順にクリックすると開く、［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。

PKIエンティティ

May 10, 2016

XenMobileのPKI（Public Key Infrastructure：公開キーのインフラストラクチャ）エンティティ構成は、実際のPKI処理（発行、失効、状態情報）を実行するコンポーネントを表します。これらのコンポーネントはXenMobileに対して内部（この場合は随意と呼ばれます）、またはそれらが企業インフラストラクチャの一部である場合はXenMobileに対して外部になります。

XenMobileは次の種類のPKIエンティティをサポートします。

- 随意CA（Certificate Authority：証明機関）
- 汎用PKIs（GPKIs）
- Microsoft Certificate Services

XenMobileでは、次のCAサーバーがサポートされます。

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

共通のPKI概念

種類に関係なく、すべてのPKIエンティティには以下の機能のサブセットがあります。

- 署名：証明書署名要求（CSR）に基づく新しい証明書の発行
- フェッチ：既存の証明書とキーペアの回収
- 失効：クライアント証明書の失効

CA証明書

PKIエンティティを構成するときに、XenMobileに、そのエンティティにより発行される（またはそのエンティティから回収される）証明書の署名者になるCA証明書を示す必要があります。1つの同じPKIエンティティから、複数の異なるCAが署名した、（フェッチされたか、または新たに署名された）証明書が返されることがあります。これらのCAそれぞれの証明書を、PKIエンティティ構成の一部として提供する必要があります。これを行うため、証明書をXenMobileにアップロードして、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

汎用PKI（Generic PKI：GPKI）プロトコルは、さまざまなPKIソリューションとの統一された連携を目的としてSOAP Webサービスレイヤーで実行される独自のXenMobileプロトコルです。GPKIプロトコルは、以下の3つの基本PKI処理を定義します。

- 署名：アダプターはCSRを取得し、それらの要求をPKIに送信して、新しい署名入り証明書を返すことができます。
- フェッチ：アダプターは既存の証明書とキーペア（入力パラメーターによる）をPKIから取得できます。
- 失効：アダプターはPKIで特定の証明書を失効させることができます。

GPKIプロトコルの受信側はGPKIアダプターです。GPKIアダプターによって、基本処理がそのアダプターが作成された特定の種類のPKIに変換されます。つまり、RSA用のGPKIアダプターと、もう1つEnTrust用のGPKIアダプターなどがあります。

GPKIアダプターは、SOAP Webサービスのエンドポイントとして、自己記述型のWeb Services Description Language（WSDL）定義を公開します。GPKI PKIエンティティの作成は、URLを通じてまたはファイルそのものをアップ

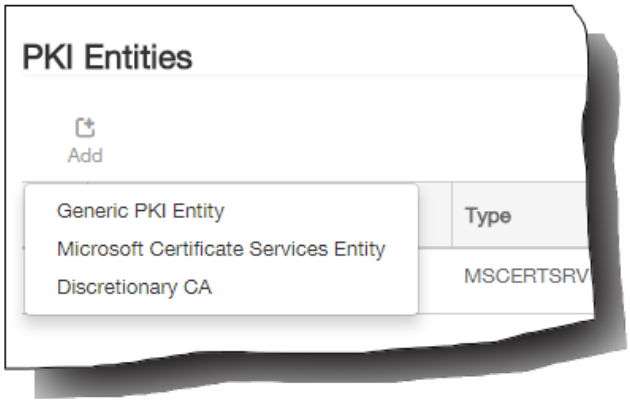
ロードして、XenMobileにそのWSDL定義を提供することを意味します。

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

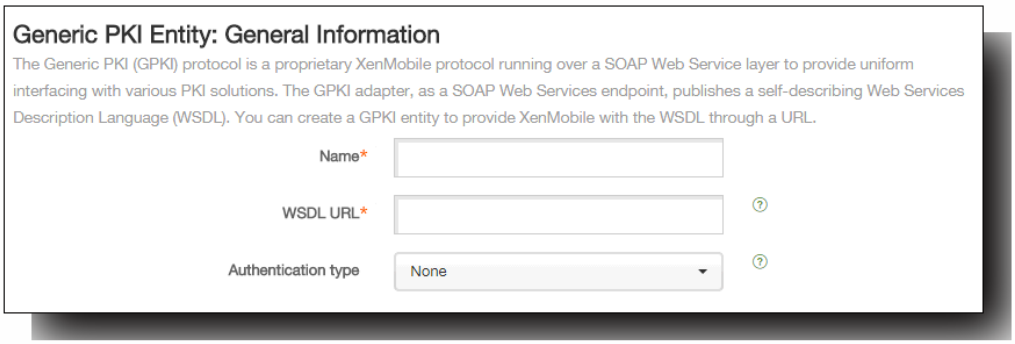
ユーザーパラメーターは、特定の処理についてGPKIアダプターで定義されるパラメーターで、XenMobileに値を提供する必要があります。アダプターがサポートする処理（アダプターの機能）と各処理に必要なパラメーターは、XenMobileによりWSDLファイルを解析して決定されます。選択した場合、SSLクライアント認証によってXenMobileとGPKIアダプターの間の接続が保護されます。

汎用PKIを追加するには

1. XenMobileコンソールで、［Configure］、［Settings］、［More］、［PKI Entities］の順にクリックします。
2. ［PKI Entities］ページで、［Add］をクリックします。
   追加できるPKIエンティティの種類を示す一覧が表示されます。



3. ［Generic PKI Entity］をクリックします。
   ［Generic PKI Entity: General Information］ページが開きます。



4. ［Generic PKI Entity: General Information］ページで、以下を行います。
   1. Name：PKIエンティティの説明的な名前を入力します。
   2. 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。
   3. Authentication type：一覧から、使用する認証方法を選択します。
      - なし

- HTTP Basic：アダプターへの接続に必要なユーザー名とパスワードを指定します。
- Client certificate：正しいSSLクライアント証明書を選択します。

4. ［Next］をクリックします。
   ［Generic PKI Entity: Adapter Capabilities］ページが開きます。

5. ［Generic PKI Entity: Adapter Capabilities］ページで、アダプターに関連付けられた機能とパラメーターを確認して、［Next］をクリックします。
   ［Generic PKI Entity: Issuing CA Certificates］ページが開きます。

6. ［Generic PKI Entity: Issuing CA Certificates］ページで、エンティティで使用する証明書を選択します。
   注：エンティティからは、異なるCAによって署名された証明書が返される場合がありますが、特定の証明書プロバイダーから取得される証明書の署名は、すべて同じCAによって行われる必要があります。したがって、資格情報プロバイダー設定を構成するときに［Distribution］ページで、ここで構成したいずれかの証明書を選択してください。
7. ［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。

Microsoft Certificate Services

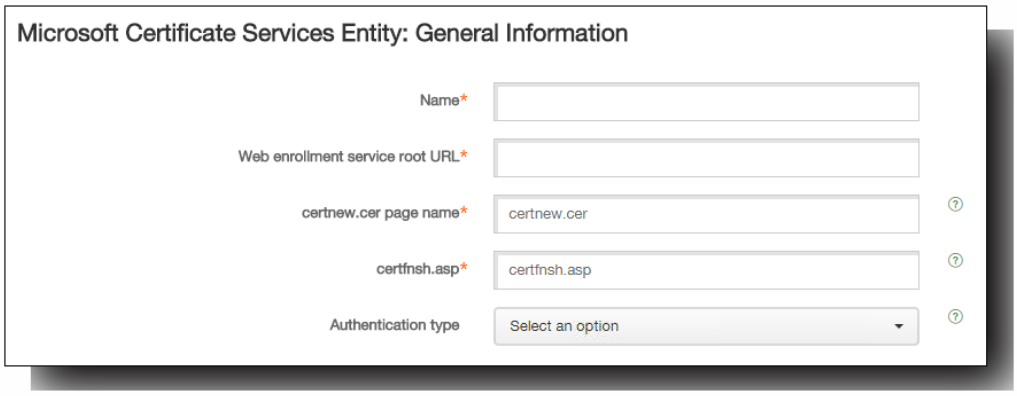
XenMobileは、Web登録インターフェイスを通じてMicrosoft Certificate Servicesと連携します。XenMobileはそのインターフェイスを使用した新しい証明書の発行（GPKI署名機能と同等の機能）のみをサポートします。

XenMobileでMicrosoft CA PKIエンティティを作成するには、Certificate ServicesのWebインターフェイスのベースURLを指定する必要があります。選択した場合、SSLクライアント認証によって、XenMobileとCertificate ServicesのWebインターフェイスとの間の接続が保護されます。

Microsoft Certificate Servicesエンティティを追加するには

1. XenMobileコンソールで、［Configure］、［Settings］、［More］、［PKI Entities］の順にクリックします。
2. ［PKI Entities］ページで、［Add］をクリックします。
   追加できるPKIエンティティの種類を示す一覧が表示されます。

3. ［Microsoft Certificate Services Entity］をクリックします。
   ［Microsoft Certificate Services Entity: General Information］ページが開きます。



4. ［Microsoft Certificate Services Entity: General Information］ページで、以下を行います。
   1. Name：新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意の名前にする必要があります。
   2. Web enrollment service root URL：Microsoft CA Web登録サービスのベースURL（https://192.0.2.13/certsrv/など）を入

力します。URLには、HTTPまたはHTTP-over-SSLを使用します。
3. certnew.cer page name：certnew.cerページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
4. 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。
5. Authentication type：一覧から、使用する認証方法を選択します。
   - なし
   - HTTP Basic：接続に必要なユーザー名とパスワードを指定します。
   - Client certificate：正しいSSLクライアント証明書を選択します。
   - ［Next］をクリックします。
     ［Microsoft Certificate Services Entity: Templates］ページが開きます。このページで、Microsoft CAがサポートするテンプレートの内部名を指定します。資格情報プロバイダーを作成するとき、ここで定義したテンプレートを一覧て選択します。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。

5. ［Microsoft Certificate Services Entity: Templates］ページで［Add］をクリックし、テンプレートの名前を入力して、［Save］をクリックします。追加する各テンプレートについて、この手順を繰り返します。
6. ［Next］をクリックします。
   ［Microsoft Certificate Services Entity: HTTP parameters］ページが開きます。このページで、Microsoft Web登録インターフェイスに対するHTTP要求にXenMobileが挿入するカスタムパラメーターを指定します。これは、カスタマイズしたスクリプトをCAで実行している場合にのみ使用できます。

7. ［Microsoft Certificate Services Entity: HTTP parameters］ページで［Add］をクリックし、追加するHTTPパラメーターの名前と値を入力して、［Next］をクリックします。
   ［Microsoft Certificate Services Entity: CA Certificates］ページが開きます。このページでは、システムでこのエンティティを通じて取得される証明書の署名者をXenMobileに通知するよう要求されます。CA証明書が更新された場合は、そのCA証明書をXenMobileで更新すると、変更がエンティティに透過的に適用されます。

8. ［Microsoft Certificate Services Entity: CA Certificates］ページで、このエンティティで使用する証明書を選択します。
9. ［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。

随意CA

随意CAは、CA証明書と関連の秘密キーをXenMobileに提供したときに作成されます。XenMobileは、管理者が指定したパラメーターに従って、証明書の発行、失効、および状態情報を内部で処理します。

随意CAを構成するときに、そのCAに対してOCSP（Online Certificate Status Protocol）サポートをアクティブにするオプションがあります。OCSPサポートを有効にした場合に限り、CAは発行する証明書にid-pe-authorityInfoAccess拡張を追加して、以下の場所にあるXenMobileの内部OSCPレスポンダーを指し示します。

https://server/instance/ocsp
OCSPサービスを構成するときに、該当の随意エンティティのOCSP署名証明書を指定する必要があります。CA証明書そのものを署名者として使用できます。CA秘密キーの不必要な漏えいを防ぐ場合（推奨）は、CA証明書で署名された、委任OCSP署名証明書を作成し、id-kp-OCSPSigning extendedKeyUsage拡張を含めます。

XenMobile OCSPレスポンダーサービスは、基本のOCSP応答と要求の以下のハッシュアルゴリズムをサポートします。

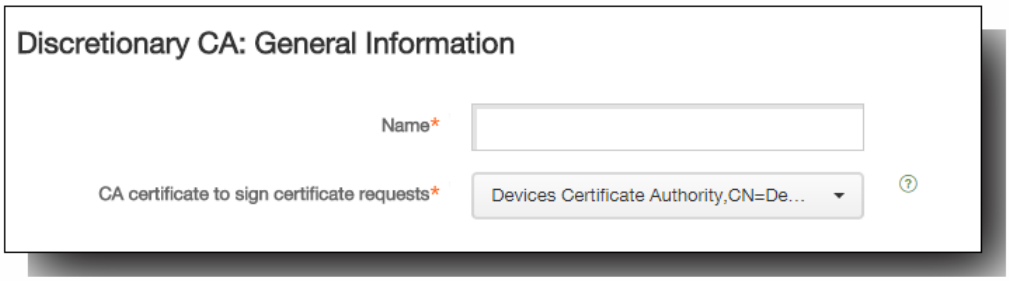
- SHA-1
- SHA-224
- SHA-256

- SHA-384
- SHA-512

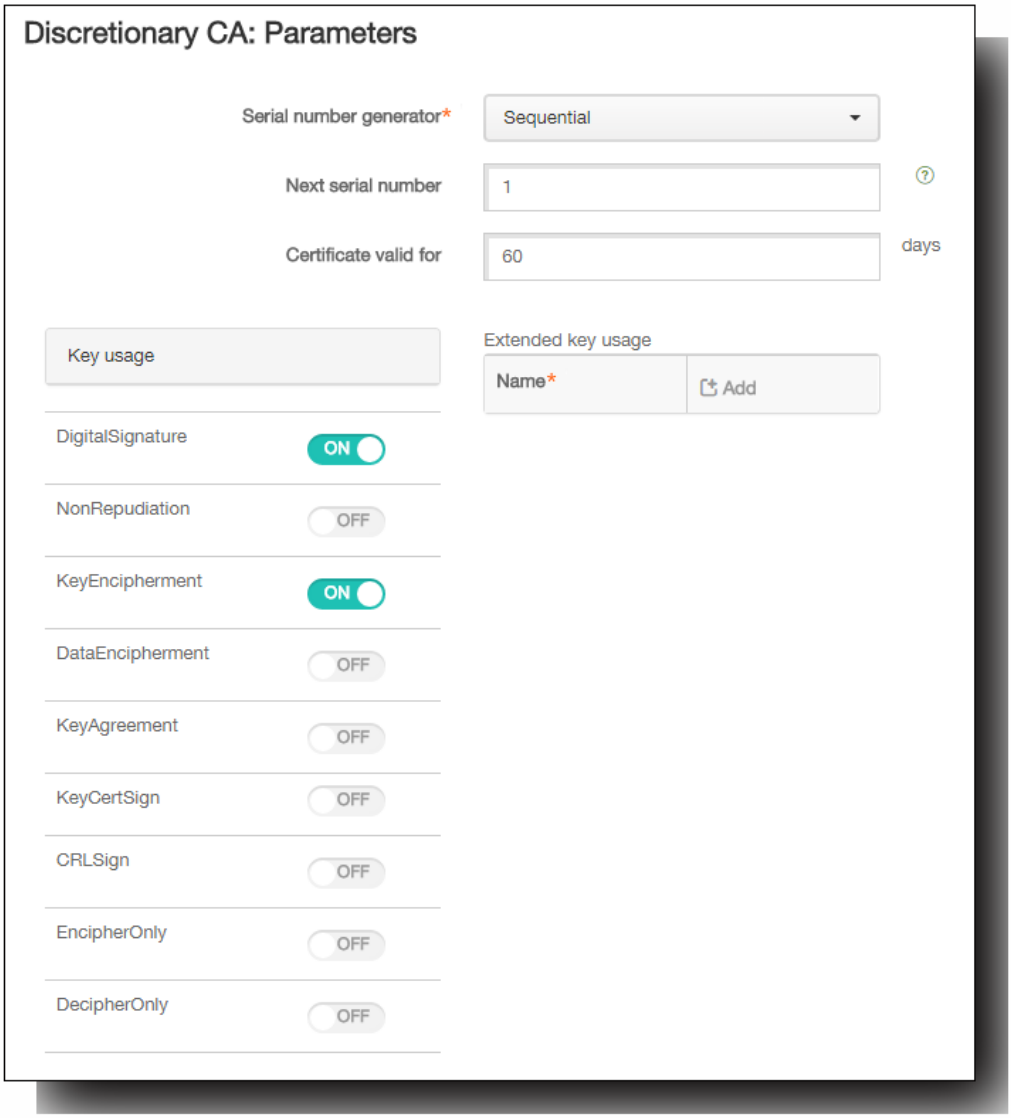
応答はSHA-256および署名証明書キーアルゴリズム（DSA、RSAまたはECDSA）で署名されます。

随意CAを追加するには

1. XenMobileコンソールで、［Configure］、［Settings］、［More］、［PKI Entities］の順にクリックします。
2. ［PKI Entities］ページで、［Add］をクリックします。
   追加できるPKIエンティティの種類を示す一覧が表示されます。
3. ［Discretionary CA］をクリックします。
   ［Discretionary CA: General Information］ページが開きます。



4. ［Discretionary CA: General Information］ページで、以下を行います。
   1. Name：随意CAの説明的な名前を入力します。
   2. CA certificate to sign certificate requests：一覧から、証明書要求に署名するために使用する随意CAの証明書を選択します。この証明書一覧は、［Configure］、［Settings］、［Certificates］でXenMobileにアップロードした、秘密キーのあるCA証明書から生成されます。
   3. ［Next］をクリックします。
      ［Discretionary CA: Parameters］ページが開きます。



5. ［Discretionary CA: Parameters］ページで、以下を行います。
   1. 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。
   2. Next serial number：値を入力して、次に発行される番号を指定します。
   3. Certificate valid for：証明書の有効期間（日数）を入力します。
   4. 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。
   5. 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。
   6. ［Next］をクリックします。
      ［Discretionary CA: Distribution］ページが開きます。

6. ［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および保存されます。この分散モードはSCEPを使用し、keyUsage keyEncryptionによるRA暗号化証明書とKeyUsage digitalSignatureによるRA署名証明書が必要

です。暗号化と署名で同じ証明書を使用できます。

7. [Next] をクリックします。
   [Discretionary CA: Online Certificate Status Protocol (OCSP)] ページが開きます。

8. [Discretionary CA: Online Certificate Status Protocol (OCSP)] ページで、以下を行います。
   1. 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。
   2. 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、[Configure]、[Settings]、[Certificates] でXenMobileにアップロードしたCA証明書から生成されます。
9. [保存] をクリックします。
   [PKI Entities] の表に随意CAが表示されます。

資格情報プロバイダー

May 10, 2016

資格情報プロバイダーは、XenMobileシステムのさまざまな部分で使用する実際の証明書の構成です。資格情報プロバイダーは、証明書がデバイス構成の一部であるかスタンドアロン（デバイスにそのままプッシュされる）であるかに関係なく、証明書のソース、パラメーター、およびライフサイクルを定義します。

デバイス登録によって証明書のライフサイクルは制約されます。つまり、登録前に証明書は発行されませんが、登録の一部として一部の証明書が発行される場合があります。また、1回の登録のコンテキスト内で内部PKIから発行された証明書は、登録が失効すると失効します。管理関係が終了すると、証明書の有効性は維持されません。

1つの資格情報プロバイダーの構成を複数の場所で使用し、1つの構成によって任意の数の証明書を同時に管理することができます。この場合、この全体は展開リソースおよび展開上にあります。たとえば、資格情報プロバイダーPが構成Cの一部としてデバイスDに展開された場合、Dに展開される証明書はPの発行設定によって決まります。同様に、Cが更新されるときにDの更新設定が適用され、Cが削除されたりDが失効したりしたときにはDの失効設定も適用されます。

この点を考慮し、XenMobileの資格情報プロバイダーの構成では以下を行います。

- 証明書のソースを決定します。
- 証明書を取得するときに使用する方法を決定します。新しい証明書に署名するか、既存の証明書とキーペアをフェッチ（回復）します。
- 発行または回復のパラメーターを決定します。キーサイズ、キーアルゴリズム、識別名、証明書拡張などの証明書署名要求（Certificate Signing Request：CSR）パラメーターがあります。
- 証明書をデバイスに配信する方法を決定します。
- 失効条件を決定します。管理関係が失われるとすべての証明書がXenMobileで失効しますが、構成によっては、関連付けられたデバイス構成が削除された場合など、以前の失効を指定する場合もあります。また、条件によっては、XenMobileで関連付けられた証明書の失効がバックエンドのPKI（Public Key Infrastructure：公開キーのインフラストラクチャ）に送信されることがあります。つまりXenMobileでの証明書の失効によってPKIでも証明書が失効する場合があります。
- 更新設定を決定します。特定の資格情報プロバイダーを通じて取得された証明書は、期限が近くなると自動的に更新されるか、それとは別に、期限が近づくと通知が発行されます。

使用できる各種構成オプションの範囲は、主に、資格情報プロバイダーに対して選択したPKIエンティティの種類と発行方法によって異なります。

証明書の発行方法

証明書は2つの方法で取得でき、これを発行方法と呼びます。

- 署名。 この方法では、新しい秘密キーを作成し、CSRを作成してCA（Certificate Authority：証明機関）に送信し、署名してもらいます。 XenMobileは、3種類のPKIエンティティによる署名方法をサポートします（MS証明書サービスエンティティ、汎用PKI、任意CA）。
- フェッチ。 この方法におけるXenMobileのための発行は、既存のキーペアの回復を意味します。 XenMobileは汎用PKIによるフェッチ方法のみをサポートします。

資格情報プロバイダーは署名またはフェッチのうちいずれかの発行方法を使用します。 選択した方法は使用可能な構成オプションに影響します。 特に、CSR構成と分散配信は、発行方法が署名の場合にのみ使用できます。 フェッチされた証明書は常にPKCS#12としてデバイスに送信されます（署名方法の集中配信モードと同じ）。

証明書の配信

XenMobileでの証明書の配信には、集中と分散の2つのモードがあります。分散モードはSCEP（Simple Certificate Enrollment Protocol）を使い、クライアントがこのプロトコルをサポートする状況でのみ使用できます（iOSのみ）。場合によっては分散モードが必須となります。

資格情報プロバイダーで分散（SCEPを使用した）配信をサポートするには、特別な構成手順として、RA（Registration Authority：登録機関）証明書の設定が必要です。RA証明書が必要なのは、SCEPプロトコルを使用する場合、XenMobileが実際

のCAに対する代理（登録機関）と同様に機能し、XenMobileはそのような役割を果たす権限があることをクライアントに証明する必要があるためです。その権限は、XenMobileに前述の証明書を提供することにより確立されます。

RA署名とRA暗号化の2つの異なる証明書の役割が必要です（1つの証明書で両方の要件を満たすことができます）。これらの役割には以下の制約があります。

- RA署名証明書には、X.509キー使用法デジタル署名が必要です。
- RA暗号化証明書には、X.509キー使用法キーの暗号化が必要です。

資格情報プロバイダーのRA証明書を構成するには、それらの証明書をXenMobileにアップロードし、資格情報プロバイダーでそれらの証明書にリンクします。

資格情報プロバイダーに証明書の役割について構成されている証明書がある場合、分散配信のみをサポートするとみなされます。各資格情報プロバイダーは、集中モードを優先するか、分散モードを優先するか、または分散モードを必要とするように構成できます。実際の結果はコンテキストに応じて異なります。コンテキストが分散モードをサポートしないにもかかわらず、資格情報プロバイダーに分散モードが必要な場合、展開は失敗します。同様に、コンテキストに分散モードが必要な場合でも、資格情報プロバイダーが分散モードをサポートしていなければ、展開は失敗します。ほかのすべての場合、優先設定が適用されます。

次の表は、XenMobile全体におけるSCEP分散を示しています。

コンテキスト	SCEPのサポート	SCEPの必要
iOSプロファイルサービス	はい	はい
iOSモバイルデバイス管理登録	はい	いいえ
iOS構成プロファイル	はい	いいえ
SHTP登録	いいえ	いいえ
SHTPの構成	いいえ	いいえ
Windows Phone登録	いいえ	いいえ
Windows Phoneの構成	いいえ	いいえ

証明書の失効

失効には以下の3つの種類があります。

- **内部失効**。内部失効はXenMobileで維持されている証明書の状態に影響します。この状態は、XenMobileに提示された証明書をXenMobileで評価するとき、または一部の証明書のOCSP状態に関する情報をXenMobileから提供する必要がある場合に考慮されます。資格情報プロバイダー構成により、さまざまな条件下でこの状態がどのように影響を受けるかが決まります。たとえば、資格情報プロバイダーでは、そのプロバイダーを通じて取得した証明書がデバイスから削除されたとき、失効済みのフラグが立てられるよう指定する場合があります。
- **外部に伝達される失効**。失効XenMobileとも呼ばれるこの種類の失効は、外部のPKIから取得した証明書に適用されます。資

格情報プロバイダー構成で定義された条件下で、証明書がXenMobileで内部失効すると、その証明書はPKIでも失効します。失効を実行するための呼び出しを行うには、失効対応GPKI（General PKI：汎用PKI）エンティティが必要です。

- **外部で誘導される失効**。失効PKIとも呼ばれるこの種類の失効も、外部のPKIから取得した証明書のみに適用されます。XenMobileで特定の証明書の状態が評価されるたびに、その状態についてPKIに照会されます。PKIで証明書が失効している場合、XenMobileで証明書が内部失効します。このメカニズムではOCSPプロトコルが使用されます。

これらの3つの種類は排他的ではなく、同時に適用されます。内部失効は外部失効または独立した検出により生じ、その結果、内部失効が外部失効を発生させる可能性があります。

証明書の書き換え

証明書の書き換えとは、既存の証明書の失効と別の証明書の発行を両方行うことです。

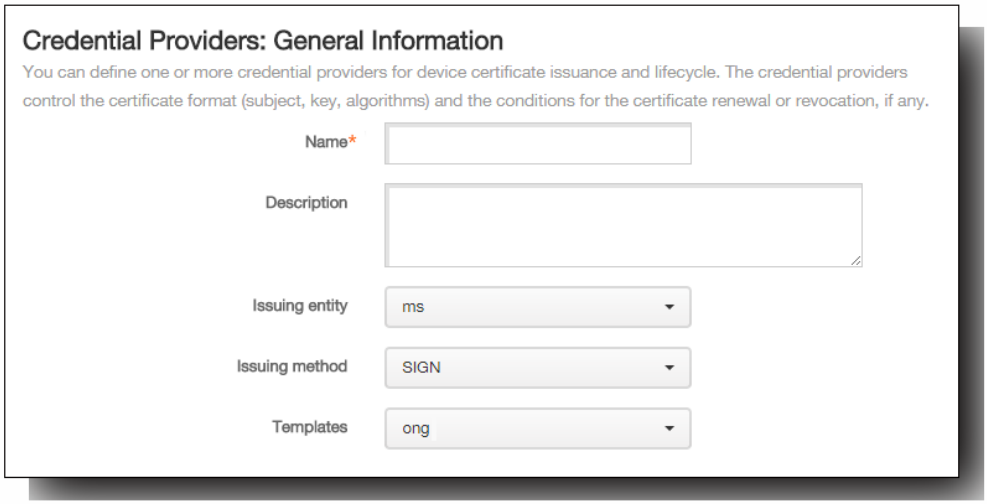
XenMobileでは、発行が失敗した場合にサービスが途絶えるのを防ぐため、以前の証明書が失効する前にまず新しい証明書の取得を試行します。（SCEP対応の）分散配信を使用する場合、失効は証明書がデバイスに正しくインストールされてから一度だけ発生します。使用しない場合、新しい証明書がデバイスに送信される前に、インストールの成否に関係なく失効が発生することになります。

失効の構成では、特定の期間を日単位で指定する必要があります。デバイスが接続されると、証明書のNotAfterの日付からこの指定した期間を引いて、現在の日付より後になっているかどうかがサーバーによって検証されます。現在の日付より後になっている場合、書き換えが試行されます。

資格情報プロバイダーを作成するには

資格情報プロバイダーの構成は、主に、資格情報プロバイダーに対して選択した発行エンティティや発行方法により異なります。内部エンティティを使用する資格情報プロバイダー（随意など）と、外部エンティティを使用する資格情報プロバイダー（Microsoft CAやGPKIなど）に区別することができます。随意エンティティの発行方法は常に署名です。つまり、各発行操作で、XenMobileはエンティティに対して選択されたCA証明書で新しいキーペアに署名します。キーペアがデバイスまたはサーバーのどちらで生成されるかは、選択した分散方法によって異なります。

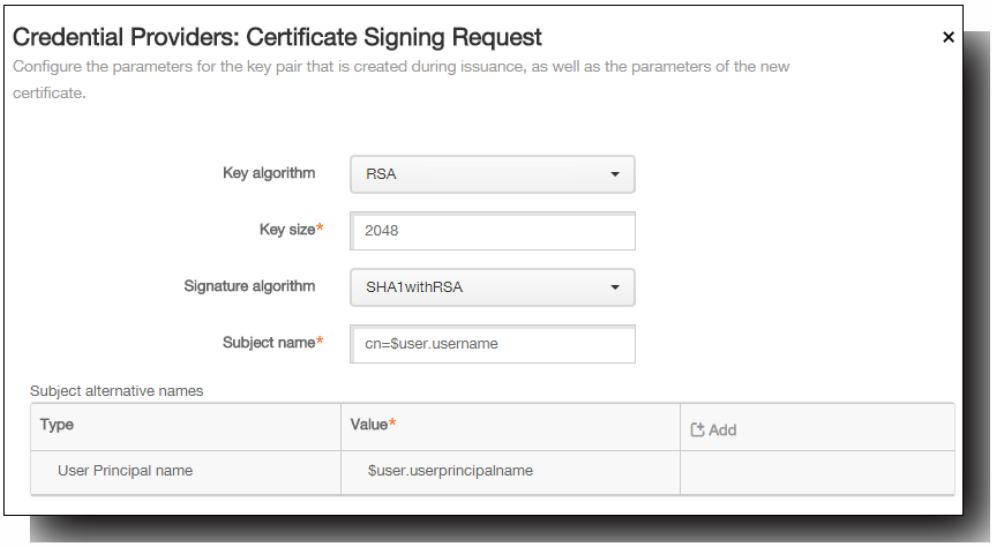
1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Credential Providers］の順にクリックします。
2. ［Credential Providers］ページで、［Add］をクリックします。
   ［Credential Providers: General Information］ページが開きます。



3. ［Credential Providers: General Infomation］ページで、以下を指定します。
   1. Name：新しいプロバイダー構成の一意の名前を入力します。この名前はXenMobileコンソールのほかの部分で構成を参照

するために後で使用されます。

2. Description：資格情報プロバイダーの説明です。このフィールドはオプションですが、後でこの資格情報プロバイダーの詳細を思い出すときに説明が役立ちます。
3. Issuing entity：証明書発行エンティティを選択します。
4. Issuing method： ［Sign］または［Fetch］をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。
5. テンプレート一覧が使用できる場合は、資格情報プロバイダーのテンプレートを選択します。
   注：これらのテンプレートは、［Configure］、［Settings］、［More］、［PKI Entities］の順にクリックすると開くページで、Microsoft証明書サービスエンティティが追加されている場合に使用可能になります。
6. ［Next］をクリックします。
   ［Credential Providers: Certificate Signing Request］ページが開きます。



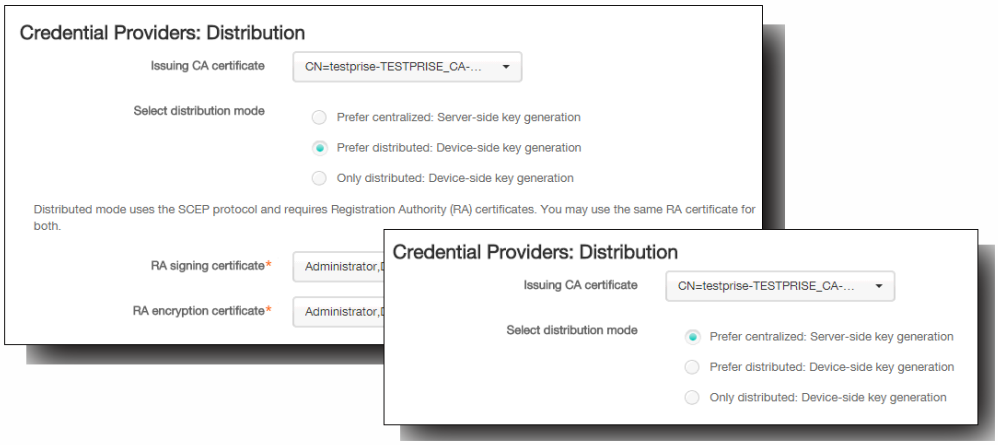
4. ［Credential Providers: Certificate Signing Request］ページで、以下を指定します。
   1. Key algorithm：新しいキーペアのキーアルゴリズムを選択します。使用可能な値は［RSA］、［DSA］、および［ECDSA］です。
   2. Key size：キーペアのサイズ（ビット単位）を入力します。これは必須フィールドです。
      注：許可される値はキーの種類によって異なります。たとえば、DSAキーの最大サイズは1024ビットです。基になるハードウェアおよびソフトウェアに依存する偽陰性を回避するため、XenMobileではキーのサイズが強制されません。資格情報プロバイダーの構成を実稼働環境でアクティブにする前に、必ずテスト環境でテストしてください。
   3. Signature algorithm：新しい証明書の値を選択します。値はキーアルゴリズムによって異なります。
   4. Subject name：新しい証明書のサブジェクトの識別名（Distinguished Name：DN）を入力します。次に例を示します。CN=${user.username},OU=${user.department},O=${user.companyname},C=${user.c}\endquotation. これは必須フィールドです。
   5. ［Subject alternative names］の表に新しいエントリを追加するには、［Add］をクリックします。別名の種類を選択して、2つ目の列に値を入力します。
      注：サブジェクト名と同様に、値フィールドでXenMobileマクロを使用できます。
   6. ［Next］をクリックします。
      ［Credential Providers: Distribution］ページが開きます。

5. ［Credential Providers: Distribution］ページで、以下を行います。
   1. ［Issuing CA certificate］の一覧から、提供されたCA証明書を選択します。資格情報プロバイダーは随意CAエンティティを使用するため、資格情報プロバイダーのCA証明書は常にエンティティそのものに構成されているCA証明書になります。

ここでは外部エンティティを使用する構成との整合性のために示されます。

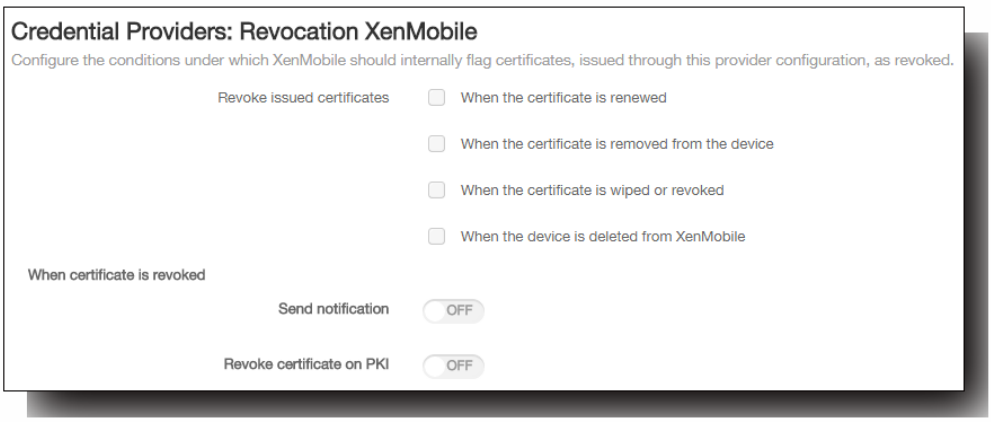
2. ［Select distribution mode］で、次のいずれかのキーの生成および配布方法をクリックします。
   - Prefer centralized: Server-side key generation。この集中管理オプションをお勧めします。このオプションはXenMobileでサポートされるすべてのプラットフォームをサポートし、NetScaler Gateway認証を使用する場合は必須です。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
   - Prefer distributed: Device-side key generation。ユーザーデバイス上で秘密キーが生成および保存されます。この分散モードはSCEPを使用し、keyUsage keyEncryptionによるRA暗号化証明書とKeyUsage digitalSignatureによるRA署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。
   - Only distributed: Device-side key generation。このオプションは［Prefer distributed: Device-side key generation］と同じように動作しますが、「Prefer」ではなく「Only」であるため、デバイス側でのキー生成が失敗した場合または使用できない場合にはオプションを使用できない点が異なります。

   ［Prefer distributed: Device-side key generation］または［Only distributed: Device-side key generation］を選択する場合は、RA署名証明書とRA暗号化証明書も選択する必要があります。これらの証明書のための新しいフィールドが表示されます。



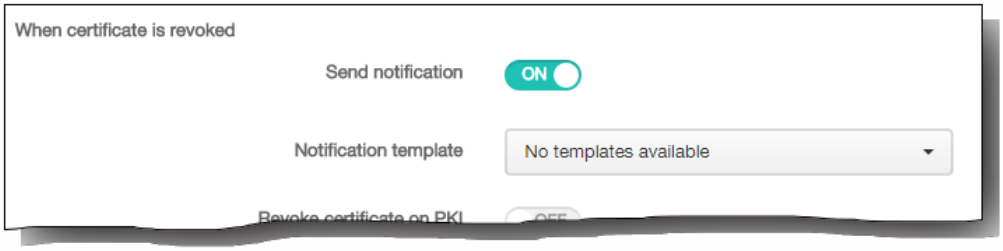
3. ［Prefer distributed: Device-side key generation］または［Only distributed: Device-side key generation］を選択した場合は、［RA signing certificate］の一覧からRA署名証明書を選択し、［RA encryption certificate］の一覧からRA暗号化証明書を選択します。両方に同じ証明書を使用できます。
4. ［Next］をクリックします。

   ［Credential Providers: Revocation XenMobile］ページが開きます。このページで、XenMobileがこのプロバイダー構成により発行された証明書に内部で失効のフラグを設定する条件を構成します。

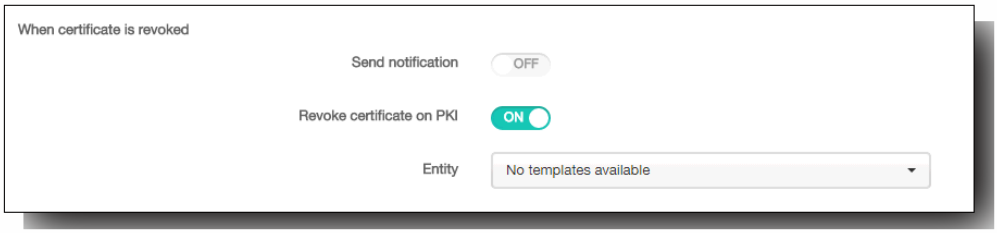


6. ［Credential Providers: Revocation XenMobile］ページで、以下を行います。
   1. ［Revoke issued certificates］で、証明書がいつ失効するかを示すいずれかのオプションを選択します。

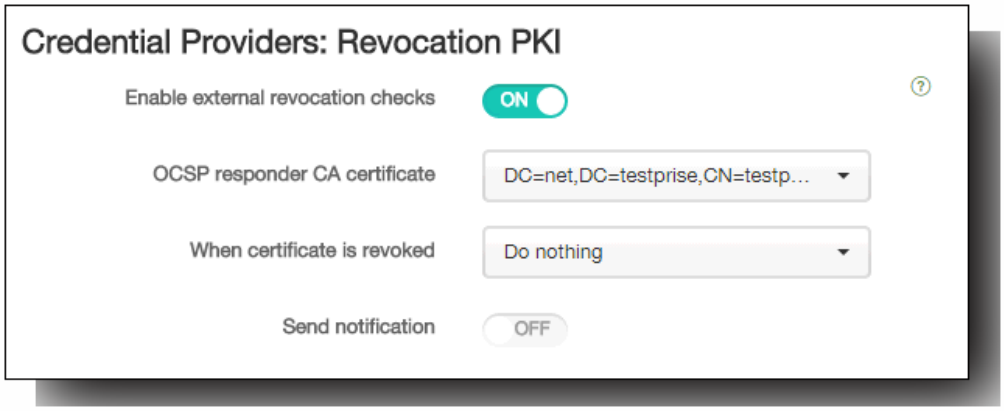
2. 証明書が失効したときにXenMobileから通知を送信する場合は、［Send notification］の値を［On］に設定して、通知テンプレートを選択します。



3. XenMobileで証明書が失効したときに、PKIでも証明書を失効させる場合は、［Revoke certificate on PKI］を［On］に設定し、［Entity］の一覧からテンプレートを選択します。［Entity］の一覧には、失効機能で使用できるすべてのGPKIエンティティが表示されます。XenMobileで証明書が失効すると、［Entity］の一覧から選択したPKIに、失効呼び出しが送信されます。



4. ［Next］をクリックします。
［Credential Providers: Revocation PKI］ページが開きます。このページで、証明書が失効したときにPKIで行うアクションを特定します。また、通知メッセージを作成するオプションもあります。

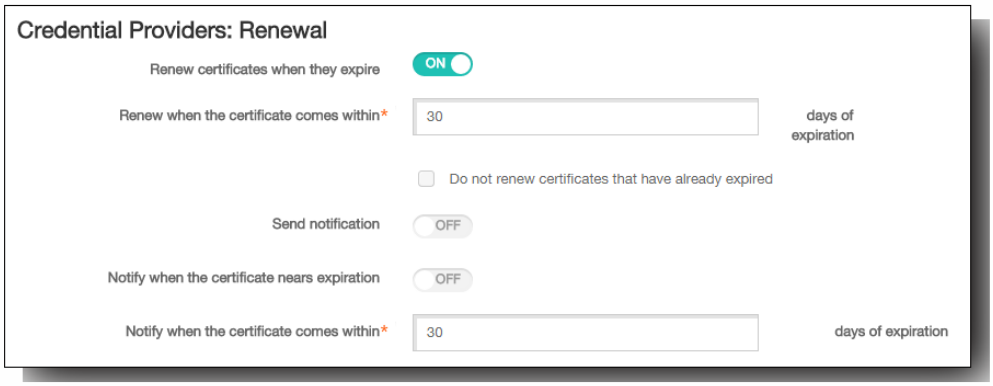


7. PKIで証明書を失効させる場合は、［Credential Providers: Revocation PKI］ページで以下を行います。
    1. ［Enable external revocation checks］の設定を［On］に変更します。
    失効PKIに関連する追加のフィールドが表示されます。
    2. ［OCSP responder CA certificate］の一覧から、証明書のサブジェクトの識別名（Distinguished Name：DN）を選択します。

注：DNフィールドの値には、XenMobileマクロを使用できます。例：CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation

3. ［When certificate is revoked］の一覧から、証明書が失効したときにPKIエンティティで行う次のいずれかのアクションを選択します。
   - Do nothing（何もしない）
   - Renew the certificate（明書を更新する）
   - Revoke and wipe the device（デバイスを取り消してワイプする）
4. 証明書が失効したときにXenMobileから通知を送信する場合は、［Send notification］の値を［On］に設定します。2つの通知オプションから選択できます。
   - ［Select notification template］を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［Notification template］の一覧にあります。
   - ［Enter notification details］を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。
5. ［Next］をクリックします。
   ［Credential Providers: Renewal］ページが開きます。このページで、XenMobileを構成して次のことを実行できます。
   - 証明書の更新、（オプション）証明書更新時の通知の送信（更新に関する通知）、および（オプション）既に期限が切れた証明書の操作からの除外
   - 期限が近い証明書に関する通知の発行（更新前の通知）

8. 証明書が失効したら更新する場合は、［Credential Providers: Renewal］ページで以下を行います。
   1. ［Renew certificates when they expire］を［On］に設定します。
      追加のフィールドが表示されます。



   2. ［Renew when the certificate comes within］フィールドに、期限の何日前に更新を行うかを入力します。
   3. 任意で、［Do note renew certificates that have already expired］（既に期限が切れている証明書を更新しない）チェックボックスをオンにします。
      注：この場合の「already expired（既に期限が切れている）」とは、証明書のNotAfterが過去の日付であることを意味し、証明書が失効しているという意味ではありません。XenMobileでは、内部で失効した証明書は更新されません。
   4. 証明書が更新されたときにXenMobileから通知を送信する場合は、［Send notification］を［On］に設定します。2つの通知オプションから選択できます。
      - ［Select notification template］を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［Notification template］の一覧にあります。
      - ［Enter notification details］を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。
   5. 証明書の期限が近いときにXenMobileから通知を送信する場合は、［Notify when certificate nears expiration］を［On］に設定します。

2つの通知オプションから選択できます。

- ［Select notification template］を選択した場合は、カスタマイズ可能な事前作成済み通知メッセージを選択できます。これらのテンプレートは、［Notification template］の一覧にあります。
- ［Enter notification details］を選択した場合は、独自の通知メッセージを作成できます。受信者のメールアドレスやメッセージの指定のほかに、通知が送信される頻度を設定できます。

6. ［Notify when the certificate comes within］フィールドで、証明書の期限の何日前に通知を送信するかを入力します。

9. ［Save］をクリックします。
資格情報プロバイダーが［Credential Provider］の表に追加されます。

APN証明書の要求

May 10, 2016

XenMobileでiOSデバイスを登録して管理するには、AppleのApple Push Notificationサービス（APN）証明書を設定および作成する必要があります。 ここでは、APN証明書を要求するための以下の基本的な手順の概要を説明します。

- Windows Server 2012 R2またはWindows 2008 R2 ServerとMicrosoftインターネットインフォメーションサービス（IIS）、またはMacコンピューターを使用して、CSR（Certificate Signing Request：証明書署名要求）を生成します。
- CSRにCitrixの署名を受けます。
- AppleのAPN証明書を要求します。
- 証明書をXenMobileにインポートします。

注：

- AppleのAPN証明書を使用すると、Apple Push Networkを使用してモバイルデバイスを管理できます。 証明書を失効させると、過失であっても故意であっても、デバイスを管理できなくなります。
- iOS Developer Enterprise Programを使用してMobile Device Managerプッシュ証明書を作成した場合は、既存の証明書をApple Push Certificates Portalに移行するためのアクションが必要になることがあります。

手順の概要を説明するトピックを以下に示します。この順番で実行してください。

手順1	IISでCSRを作成する MacでCSRを作成する	Windows Server 2012 R2またはWindows 2008 R2 ServerとMicrosoft IIS、またはMacコンピューターを使用してCSRを生成します。 この方法を使用することをお勧めします。
手順2	CSRに署名するには	XenMobile APNs CSR署名Webサイト（MyCitrix IDが必要）で、CitrixにCSRを送信します。 モバイルデバイス管理の署名証明書を使用して署名された.plist形式のファイルが返送されます。
手順3	署名済みのCSRをAppleに送信する	署名入りCSRをApple Push Certificate Portal（Apple IDが必要）でAppleに送信し、AppleのAPNs証明書をダウンロードします。
手順4	Microsoft IISを使用して.pfx APN証明書を作成するには Macコンピューターで.pfx APN証明書を作成するには OpenSSLを使用して.pfx APN証明書を作成する	（IIS、Mac、またはSSLで）APN証明書をPCKS #12（.pfx）証明書としてエクスポートします。
手順5	APN証明書をXenMobileにインポートする	証明書をXenMobileにインポートします。

Apple MDMプッシュ通知の移行情報

iOS Developer Enterprise Programで作成されたモバイルデバイス管理（MDM）プッシュ通知は、Apple Push Certificates Portalに移行されています。 この移行により、新しいMDMプッシュ通知の作成と既存のMDMプッシュ通知の更新、失効、およびダウンロードが影響を受けます。 そのほかの（MDM以外の）APN証明書には影響がありません。

MDMプッシュ通知がiOS Developer Enterprise Programで作成された場合、次の状況が当てはまります。

- 証明書が自動的に移行されます。
- ユーザーに影響を与えずに証明書をApple Push Certificates Portalで更新できます。
- 既存の証明書を失効またはダウンロードするには、iOS Developer Enterprise Programを使用する必要があります。

有効期限が近づいているMDMプッシュ通知がない場合は、何もする必要はありません。 有効期限が近づいているMDMプッシュ通知がある場合は、MDMソリューションプロバイダーに問い合わせてください。 次に、iOS Developer Programエージェントログを Apple IDと共にApple Push Certificates Portalに置きます。

すべての新しいMDMプッシュ通知は、Apple Push Certificates Portalで作成される必要があります。 iOS Developer Enterprise Programでは、com.apple.mgmtを含むBundle Identifier（APNsトピック）を持つApp IDを作成できなくなります。

注：証明書の作成に使用されたApple IDの記録をとる必要があります。 さらに、Apple IDは個人IDではなく会社IDでなければなりません。

Microsoft IISを使用してCSRを作成するには

iOSデバイスのAPNs証明書要求を生成するには、まずCSR（Certificate Signing Request：証明書署名要求）を作成します。 Windows 2012 R2またはWindows 2008 R2 Serverでは、Microsoft IISを使用してCSRを生成できます。

1. Microsoft IISを開きます。
2. IISのサーバー証明書アイコンをクリックします。
3. ［サーバー証明書］ウィンドウで、**［証明書の要求の作成］**をクリックします。
4. 適切な識別名（Distinguished Name：DN）を入力して**［次へ］**をクリックします。
5. ［暗号化サービスプロバイダー］で**［Microsoft RSA SChannel Cryptographic Provider］**を選択して、ビット長として**［2048］**を選択し、**［次へ］**をクリックします。
6. ファイル名を入力してCSRを保存する場所を指定し、**［完了］**をクリックします。

MacコンピューターでCSRを作成するには

1. Mac OS Xを実行するMacコンピューターの**［アプリケーション］**>**［ユーティリティ］**で、キーチェーンアクセスアプリケーションを起動します。
2. **［キーチェーンアクセス］**メニューを開いて**［環境設定］**を選択します。
3. **［証明書］**タブをクリックして、**［OCSP］**および**［CRL］**のオプションを**［切］**に変更し、［環境設定］ウィンドウを閉じます。
4. **［キーチェーンアクセス］**メニューで、**［証明書アシスタント］**>**［認証局に証明書を要求］**の順に選択します。
5. 証明書アシスタントにより、次の情報の入力を求められます。
   1. **ユーザのメールアドレス**。 証明書の管理を担当する個人または役割アカウントのメールアドレス。
   2. **通称**。 証明書の管理を担当する個人または役割アカウントの通称。
   3. **CAのメールアドレス**。 認証局のメールアドレス。
6. **［ディスクに保存］**をクリックし、**［鍵ペア情報を指定］**チェックボックスをオンにして、**［続ける］**をクリックします。
7. CSRファイルの名前を入力してコンピューターにファイルを保存し、**［保存］**を選択します。
8. **［鍵のサイズ］**で［2048ビット］を選択し、アルゴリズムに**［RSA］**を選択してから**［続ける］**をクリックします。 APN

証明書プロセスの一環としてCSRファイルをアップロードする準備ができました。

9. 証明書アシスタンスによるCSRプロセスが完了してから**[完了]**をクリックします。

OpenSSLを使用してCSRを作成するには

Windows 2012 R2またはWindows 2008 R2 ServerとMicrosoftインターネットインフォメーションサービス（IIS）、またはMacコンピューターを使用して、Apple Push Notificationサービス（APNs）証明書のためにAppleに送信するCSR（Certificate Signing Request：証明書署名要求）を生成できない場合は、OpenSSLを使用することができます。

注：OpenSSLを使用してCSRを作成するには、まず、OpenSSLのWebサイトからOpenSSLをダウンロードしてインストールする必要があります。

1. OpenSSLをインストールしたコンピューターで、コマンドプロンプトまたはシェルから次のコマンドを実行します。
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. 証明書の名前に関する次のメッセージが表示されます。 要求された情報を入力します。
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.

   Country Name (2 letter code) [AU]:US
   State or Province Name (full name) [Some-State]:CA
   Locality Name (eg, city) []:RWC
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Customer
   Organizational Unit Name (eg, section) []:Marketing
   Common Name (eg, YOUR name) []:John Doe
   Email Address []:john.doe@customer.com

3. 次のメッセージが表示されたら、CSRの秘密キーのパスワードを入力します。
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:

4. 結果のCSRをCitrixに送信します。

署名済みのCSRがメールで返送されてきます。

CSRに署名するには

証明書をAppleに送信する前に、Citrixの署名を受けてXenMobileで使用できるようにする必要があります。

1. ブラウザーで、XenMobile APNs CSR署名Webサイトに移動します。
2. **[Upload the CSR]**をクリックします。
3. 証明書に移動して選択します。
   注：証明書は.pem/txt形式である必要があります。

4. XenMobile APN CSR署名ページで、**[Sign]**をクリックします。 CSRが署名されて、構成されているダウンロードフォルダーに自動的に保存されます。

署名入りCSRをAppleに送信してAPN証明書を取得するには

署名入りCSR（Certificate Signing Request：証明書署名要求）をCitrixから受け取ったら、それをAppleに送信してAPN証明書を取得する必要があります。

注：一部のユーザーから、Apple Push Portalへのログイン時の問題が報告されています。 代わりの手段として、手順1でidentity.apple.comリンクにアクセスする前に、Apple Developer Portal（http://developer.apple.com/devcenter/ios/index.action）にログオンしても構いません。

1. Webブラウザーで、https://identity.apple.com/pushcertに移動します。
2. **[証明書識別情報を作成]**をクリックします。
3. Appleで初めて証明書を作成する場合は **[利用規約を読みました。内容に同意します。]** チェックボックスをオンにして、 **[同意します]** をクリックします。
4. **[ファイルの選択]** をクリックし、コンピューター上の署名入りCSRを指定して **[アップロード]** をクリックします。アップロードが成功したことを示す確認メッセージが表示されます。
5. **[ダウンロード]** をクリックして、.pem証明書を取得します。
   注：Internet Explorerを使用していて、ファイル拡張子がない場合は、 **[キャンセル]** を2回クリックして、次のウィンドウからダウンロードします。

Microsoft IISを使用して.pfx APN証明書を作成するには

XenMobileでAppleのAPN証明書を使用するには、Microsoft IISで証明書要求を完成させて、証明書をPCKS #12（.pfx）ファイルとしてエクスポートし、このAPN証明書をXenMobileにインポートする必要があります。

重要：このタスクには、CSRを生成するために使用したサーバーと同じIISサーバーを使用する必要があります。

1. Microsoft IISを開きます。
2. サーバー証明書アイコンをクリックします。
3. **[サーバー証明書]** ウィンドウで、 **[証明書の要求の完了]** をクリックします。
4. AppleのCertificate.pemファイルを指定します。 フレンドリ名または証明書名を入力して **[OK]** をクリックします。
5. 手順4で指定した証明書を選択して **[エクスポート]** をクリックします。
6. .pfx証明書の場所とファイル名およびパスワードを指定して **[OK]** をクリックします。
   注：XenMobileのインストール中にこの証明書のパスワードが必要になります。
7. .pfx証明書をXenMobileがインストールされるサーバーにコピーします。
8. 管理者または **[About]** タブにアクセスできるユーザーとしてXenMobileコンソールにサインインします。
9. **[About]** タブをクリックし、 **[Update APNs Certificate]** をクリックします。
10. **[Update APNs Certificate]** ダイアログボックスで、コンピューターにあるAPNs証明書の.pfxファイルを指定して新しいパスワードを入力します。
11. **[Load APNs Certificate]** をクリックします。
12. **[Update]** をクリックします。

Macコンピューターで.pfx APN証明書を作成するには

1. Mac OS Xを実行する、CSRの生成に使用したものと同じMacコンピューターで、Appleから受け取ったProduction identity（.pem）証明書を見つけます。
2. 証明書ファイルをダブルクリックして、ファイルをキーチェーンにインポートします。
3. 特定のキーチェーンへの証明書の追加を確認するメッセージが表示された場合は、デフォルトの選択されたログインキーチェーンを維持して **[OK]** をクリックします。 新たに追加された証明書が証明書の一覧に表示されます。
4. 証明書をクリックして、 **[File]** メニューの **[Export]** をクリックして、証明書のPCKS #12（.pfx）証明書へのエクスポー

トを開始します。
5. XenMobileサーバーで使用するために証明書ファイルに一意の名前を付けて、証明書を保存するフォルダーの場所を選択し、.pfxファイル形式を選択して［保存］をクリックします。
6. パスワードを入力して証明書をエクスポートします。 一意で強力なパスワードを使用することをお勧めします。 また、後で使用および参照するために証明書とパスワードを安全に保管するようにします。
7. キーチェーンアクセスアプリケーションによって、ログインパスワードまたは選択したキーチェーンを確認するメッセージが表示されます。 パスワードを入力して、［OK］をクリックします。 XenMobileサーバーで保存された証明書を使用する準備ができました。
   注：CSRを生成して証明書のエクスポートプロセスを完了した元のコンピューターとユーザーアカウントを保持しない場合は、ローカルシステムの個人キーと公開キーを保存するかエクスポートすることをお勧めします。 そうしなければ、再利用のためのAPN証明書へのアクセスは無効になり、CSRおよびAPNsプロセス全体を繰り返す必要があります。

OpenSSLを使用して.pfx APNs証明書を作成するには

OpenSSLを使用してCSR（Certificate Signing Request：証明書署名要求）を作成した後、OpenSSLを使用して.pfx APNs証明書を作成することもできます。

1. コマンドプロンプトまたはシェルで次のコマンドを実行します。
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12
2. .pfx証明書ファイルのパスワードを入力します。 このパスワードは、証明書をXenMobileにアップロードするときに再び使用するので覚えておいてください。
3. .pfx証明書ファイルの場所を確認し、XenMobileコンソールを使用してアップロードできるようにXenMobileサーバーにコピーします。

APN証明書をXenMobileにインポートするには

新しいAPN証明書を要求して受け取ったら、そのAPN証明書をXenMobileにインポートして、最初の証明書として追加するか、既存の証明書を置き換えます。

1. XenMobileコンソールに管理者としてサインオンします。
2. ［Configure］、［Settings］、［Certificates］の順にクリックします。
3. ［Certificates］ページで、［Import］をクリックします。 ［Import］ダイアログボックスが開きます。
4. コンピューターの.p12ファイルを指定します。
5. パスワードを入力して、［Import］をクリックします。

XenMobileの証明書について詳しくは、「証明書」セクションを参照してください。

APN証明書を更新するには

APN証明書を更新するには、新しい証明書を作成する場合と同じ手順を実行する必要があります。 その後、Apple Push Certificates Portalにアクセスして、新しい証明書をアップロードします。 ログオンすると、既存の証明書（または、前のApple Developersアカウントからインポートされた証明書）が表示されます。 証明書を更新する場合は、証明書を作成する場合との唯一の違いとして、Certificates Portalで［Renew］をクリックします。 Certificates Portalにアクセスするには、このサイトの開発者アカウントが必要です。

注：APN証明書の有効期限を調べるには、［Configure］＞［Settings］＞［Certificates］の順にクリックします。 ただし、証明書の有効期限が切れていても証明書を失効させないでください。

1. Microsoftインターネットインフォメーションサービス（Internet Information Services：IIS）を使用してCSRを生成します。
2. XenMobile APNs CSR署名Webサイトで、新しいCSRをアップロードして［Sign］をクリックします。

3. 署名済みのCSRをApple Push Certificate PortalでAppleに送信します。
4. **[Renew]** をクリックします。
5. Microsoft IISを使用してPCKS #12（.pfx）APN証明書を生成します。
6. 新しいAPN証明書をXenMobileに更新するには、**[Configure]** 、 **[Settings]** 、 **[Certificates]** の順に選択します。
7. **[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。

NetScaler GatewayとXenMobile

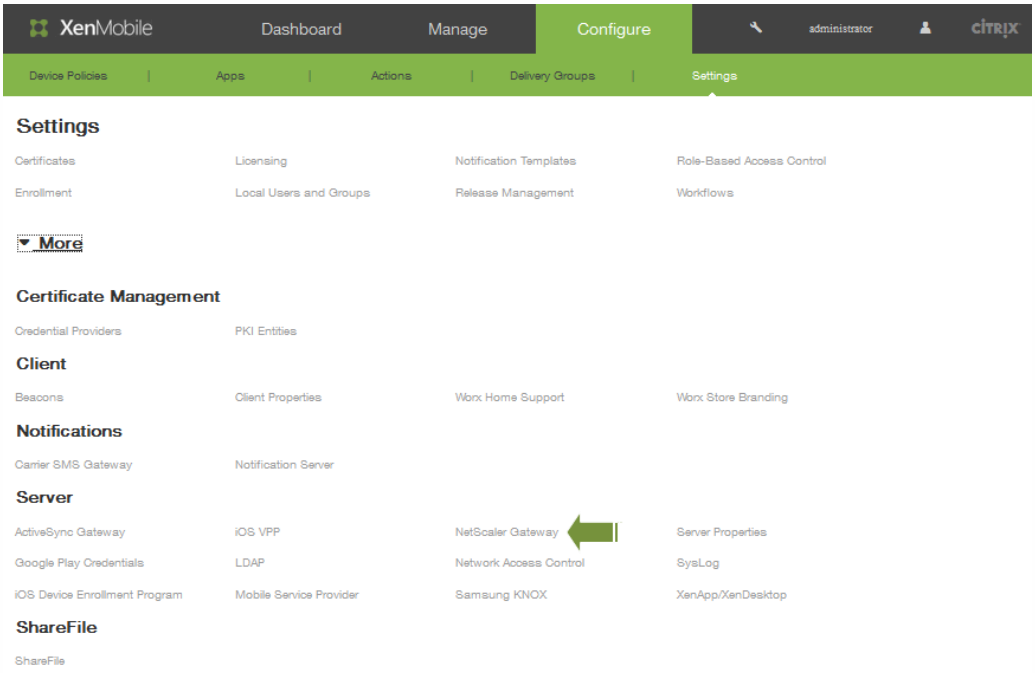
May 10, 2016

XenMobileを使用してNetScaler Gatewayを構成すると、リモートデバイスで内部ネットワークにアクセスするための認証メカニズムが確立されます。この機能を利用すると、モバイルデバイス上のアプリケーションからNetScaler Gatewayへのマイクロ VPNを作成し、イントラネット内にある社内サーバーにアクセスすることができます。NetScaler Gatewayの構成はXenMobileコンソールで行います。

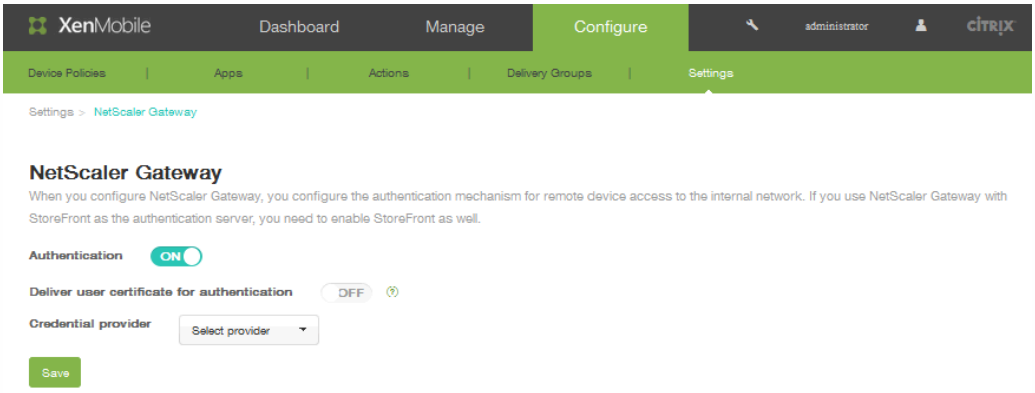
注：NetScalerでXenMobile用にNetScaler Gatewayを設定する方法について詳しくは、「XenMobile環境の設定の構成」を参照してください。

NetScaler Gatewayを構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［NetScaler Gateway］の順にクリックします。



2. ［Authentication］で［ON］を選択します。



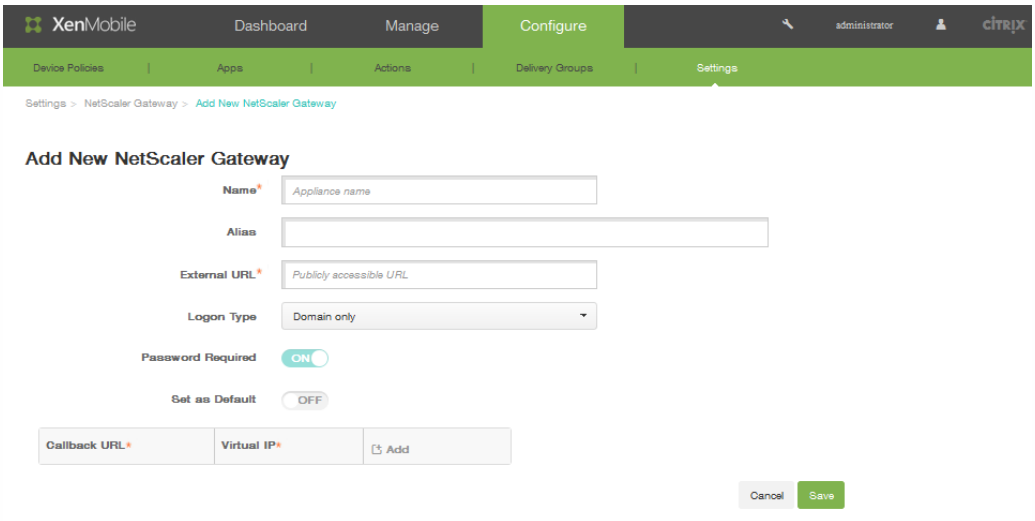
3. XenMobileでWorx Homeと認証証明書を共有し、NetScaler Gatewayでクライアント証明書認証の処理を行うようにする

には、［Deliver user certificate for authentication］で［ON］を選択します。

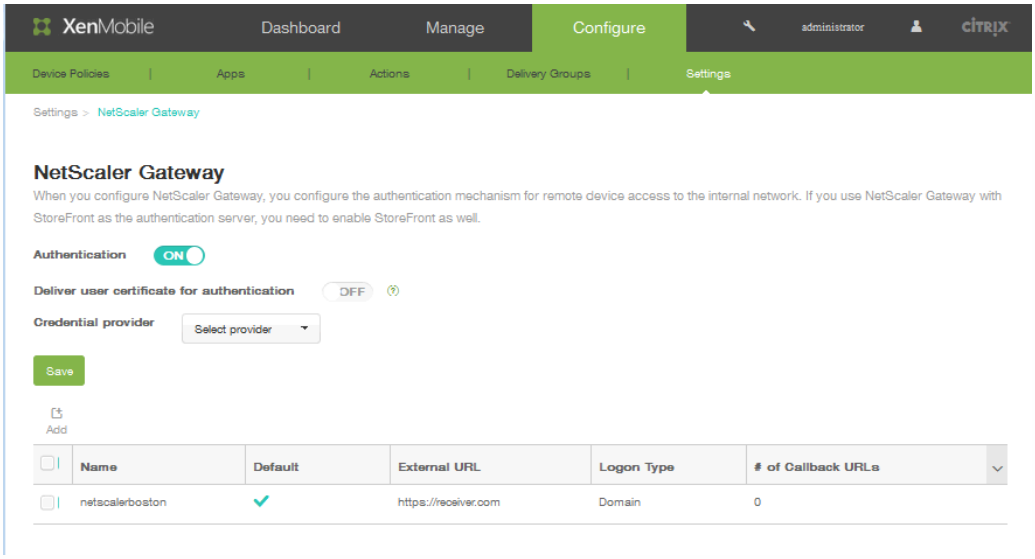
4. ［Credential Provider］の一覧から、資格情報プロバイダーを選択します。詳しくは、「資格情報プロバイダー」を参照してください。
5. ［Save］をクリックします。

新しいNetScaler Gatewayインスタンスを追加するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［NetScaler Gateway］の順にクリックします。
2. 表の上の［Add］をクリックします。［Add New NetScaler Gateway］ページが開きます。

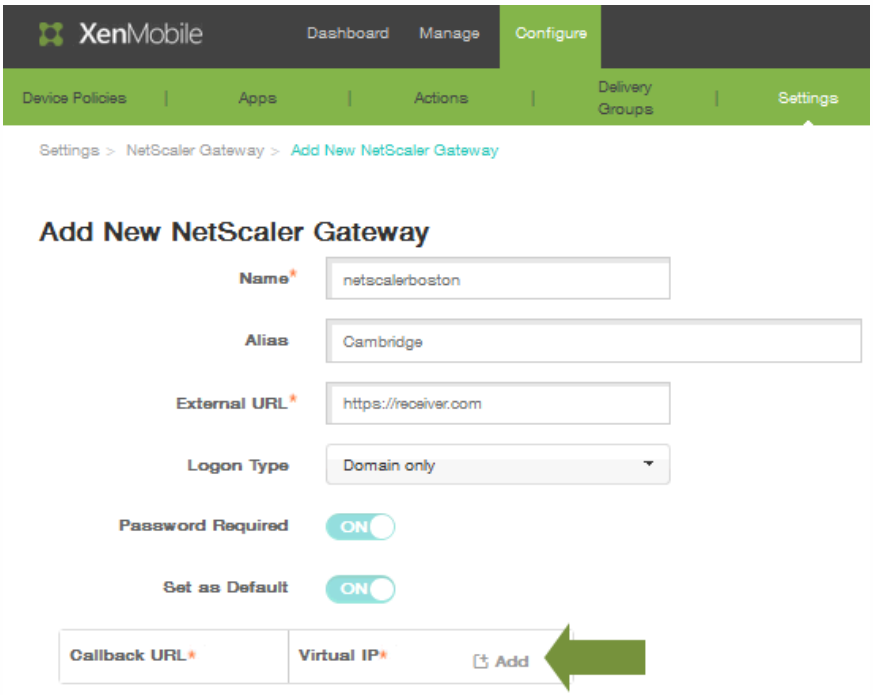


3. ［Name］ボックスに、NetScaler Gatewayインスタンスの名前を入力します。
4. ［Alias］ボックスに、オプションでエイリアスを入力します。
5. ［External URL］ボックスに、NetScaler Gatewayの、パブリックにアクセスできるURLを入力します。たとえば、https://receiver.comなどです。
6. ［Logon Type］の一覧から、ログオンの種類を選択します。種類には、［Domain only］、［Security token only］、［Domain and security token］、［Certificate］、［Certificate and domain］、［Certificate and security token］があります。デフォルトでは、ログオンの種類は**［Domain only］**に設定されています。複数のドメインがある場合は、**［Domain only］**が機能せず、**［Certificate and domain］**を使用する必要があります。［Domain only］など一部のオプションでは、［Password］フィールドを変更できません。このログオンの種類の場合、このフィールドは常に［ON］です。また、［Password Required］フィールドのデフォルト値は、選択した［Logon Type］に基づいて変化します。
7. パスワード認証を必須にするには、**［Password Required］**で［ON］を選択します。
8. このNetScaler Gatewayをデフォルトとして使用するには、**［Set as Default］**で［ON］を選択します。
9. **［Save］**をクリックします。新しいNetScaler Gatewayが追加され、表に表示されます。表で名前をクリックして、インスタンスを編集または削除できます。



NetScaler Gatewayインスタンスを追加した後、コールバックURLを追加したり、NetScaler Gateway VPN仮想IPアドレスを指定したりすることができます。 **注**：この設定はオプションですが、特にXenMobileサーバーがDMZに配置されている場合に、セキュリティ強化のために構成できます。

1. ［NetScaler Gateway］画面の表でNetScaler Gatewayを選択し、 **［Add］**をクリックします。
2. ［Add New NetScaler Gateway］ページのコールバックURL一覧表で、［Add］をクリックします。



3. **コールバックURL**を指定します。 このフィールドは完全修飾ドメイン名（FQDN）を表し、要求元がNetScaler Gatewayであることを検証します。

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

LDAP構成

May 10, 2016

XenMobileでは、LDAP（Lightweight Directory Access Protocol）に準拠している1つまたは複数のディレクトリ（Active Directoryなど）への接続を構成することができます。そしてこのLDAP構成を使用して、グループ、ユーザーアカウント、関連するプロパティをインポートします。LDAPは、オープンソースで特定のベンダーに依存しないアプリケーションプロトコルであり、インターネットプロトコル（IP）ネットワーク経由で分散ディレクトリ情報サービスへのアクセスや管理を行うためのものです。ディレクトリ情報サービスは、ネットワークで使用可能な、ユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。LDAPは一般的に、シングルサインオン（SSO）をユーザーに提供するために利用されます。SSOでは（ユーザーごとに）1つのパスワードを複数のサービスで共有します。ユーザーは、会社のWebサイトに一度ログオンすれば、社内イントラネットに自動的にログインできます。

LDAPの動作

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

XenMobileでLDAP接続を構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［LDAP］の順にクリックします。
   ［LDAP］構成ページが開きます。

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

3. 次の設定を構成します。
   - Directory type：適切なディレクトリの種類をクリックします。デフォルトでは、Microsoft Active Directoryが選択されています。
   - Primary server：LDAPで使用するプライマリサーバーを入力します。IPアドレスまたは完全修飾ドメイン名（FQDN）を入力できます。
   - Secondary server：任意で、セカンダリサーバーのIPアドレスまたはFQDNを入力します（構成されている場合）。
   - Port：LDAPサーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていないLDAP接続用のポート番号389に設定されています。セキュリティ保護されたLDAP接続ではポート番号636、Microsoftのセキュリティ保護されていないLDAP接続では3268、Microsoftのセキュリティ保護されたLDAP接続では3269を使用します。
   - Domain name：ドメイン名を入力します。
   - User base DN：Active Directory内でのユーザーの位置を固有の識別子で入力します。構文の例には、「ou=users, dc=example, or dc=com」などがあります。
   - Group base DN：「cn=groupname」のように指定される、グループのベースDNグループ名を入力します。たとえば、「cn=users, dc=servername, dc=net」で、「cn=users」はグループ名です。DNおよびサーバー名は、Active Directoryを実行しているサーバーの名前を表します。
   - User ID：Active Directoryアカウントに関連付けられたユーザーIDを入力します。
   - Password：ユーザーに関連付けられたパスワードを入力します。
   - ［Domain alias］：ドメイン名のエイリアスを入力します。
   - XenMobile Lockout Limit：ログオンの試行失敗回数として、0～999の数を入力します。このフィールドを0に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
   - XenMobile Lockout Time：ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、0～99999の数を入力します。このフィールドを0に設定すると、ロックアウト後にユーザーが待機する必要はなくなります。
   - Global Catalog TCP Port：グローバルカタログサーバーのTCPポート番号を入力します。デフォルトでは、TCPポート番号は3268に設定されています。SSL接続では、ポート番号3269を使用します。

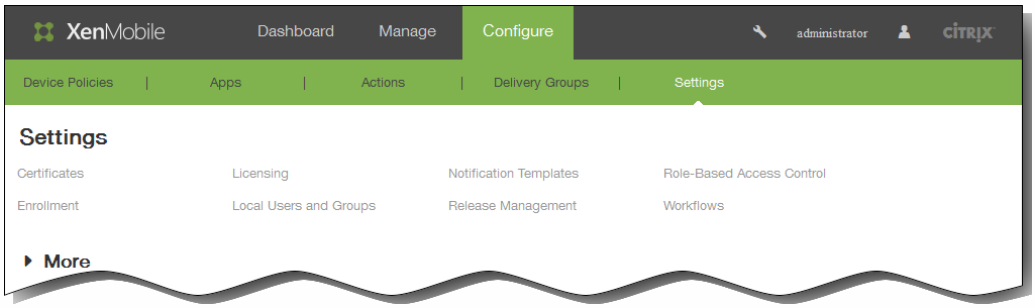
- Global Catalog Root Context：任意で、Active Directoryでのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準のLDAP検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- User search by：一覧から、［userPrincipalName］または［sAMAccountName］を選択します。
- Use secure connection：セキュリティ保護された接続を有効化するには、［YES］をクリックします。

4. ［Save］をクリックします。

ユーザーアカウント、役割、および登録設定

May 10, 2016

XenMobileでは、XenMobileコンソールの［Settings］ページで、ユーザーとグループ、ユーザーとグループの役割、登録モード、および招待状を構成します。



［Settings］ページでは以下の操作を実行できます。

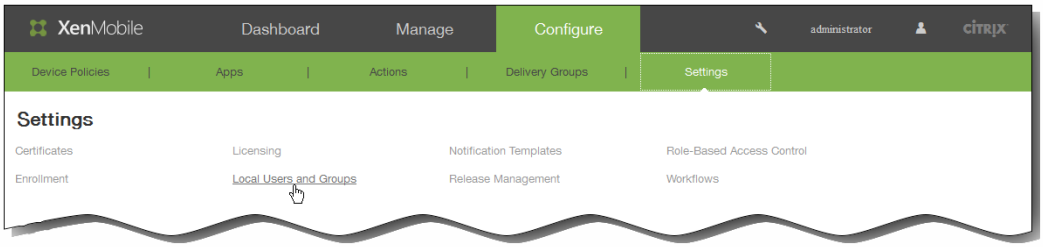
- ［Local Users and Groups］をクリックして、ユーザーアカウントを手動で追加するか、.csvプロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理します。詳しくは、以下のセクションを参照してください。
  - XenMobileでローカルユーザーを追加、編集、または削除するには
  - .csvプロビジョニングファイルとプロビジョニングファイル形式を使用してユーザーアカウントをインポートするには
  - XenMobileでグループを追加または削除するには
- ［Enrollment］をクリックして、最大7つのモードを構成します。それぞれに独自のセキュリティレベルを設定し、ユーザーがデバイスを登録するときや登録招待状を送信するときに必要ないくつかの手順を指定します。詳しくは、以下のセクションを参照してください。
  - 登録モードを構成してSelf Help Portalを有効化するには
  - XenMobileでユーザー登録の自動検出を有効化するには
- ［Role-Based Access Control］をクリックして、権限の定義済みセットである役割をユーザーとグループに割り当てます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。詳しくは、以下のセクションを参照してください。
  - XenMobileでRBACを使用してカスタムの役割を作成または更新するには
- ［Notification Templates］をクリックして、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用する通知テンプレートを指定します。Worx Home、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。詳しくは、以下のセクションを参照してください。
  - XenMobileで通知テンプレートを作成または更新するには

XenMobileでローカルユーザーを追加、編集、または削除するには

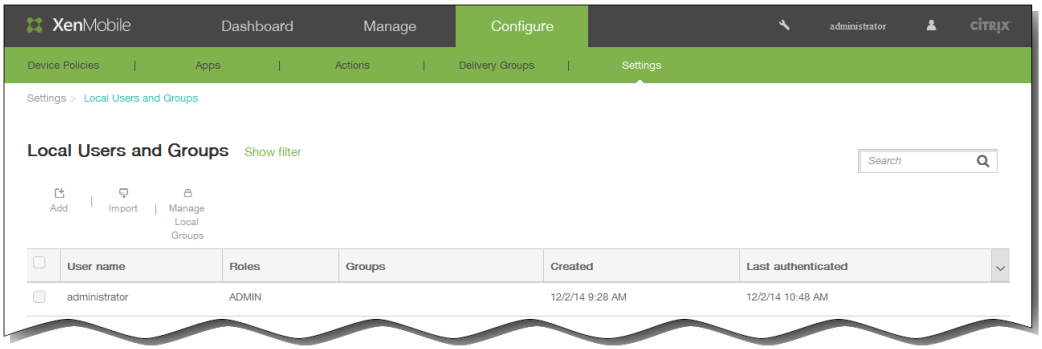
May 10, 2016

ローカルユーザーアカウントをXenMobileに手動で追加したり、プロビジョニングファイルを使用してアカウントをインポートしたりすることができます。プロビジョニングファイルからユーザーをインポートする手順については、「.csvプロビジョニングファイルを使用してユーザーアカウントをインポートするには」を参照してください。

1. XenMobileコンソールで、［Configure］、［Settings］、［Local Users and Groups］の順にクリックします。



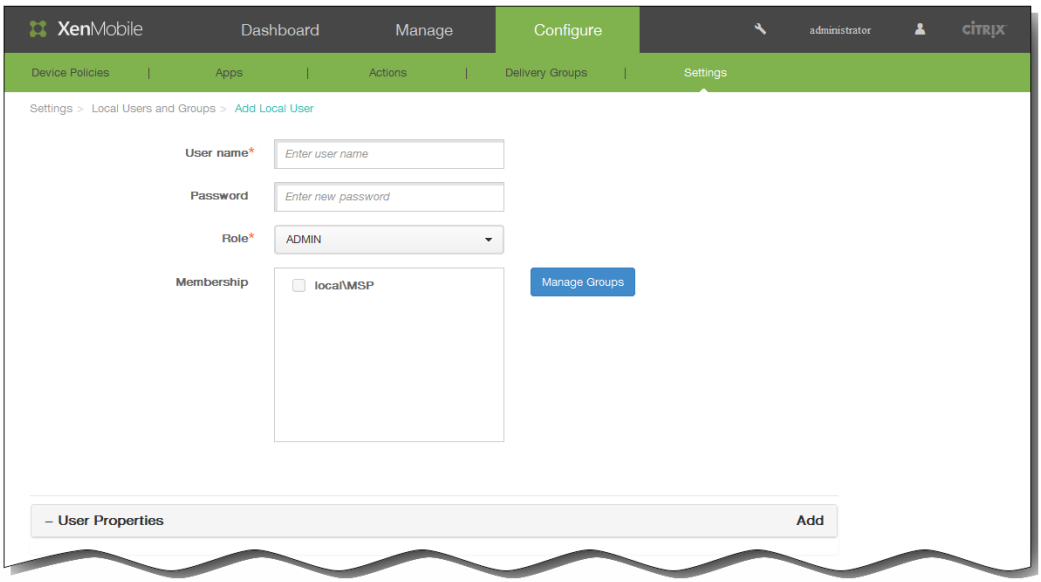
［Local Users and Groups］ページが開きます。



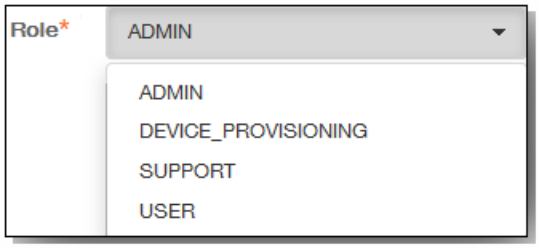
ローカルユーザーを追加するには

この手順では、一度に単一のユーザーを追加します。複数のユーザーを追加するには、「csvプロビジョニングファイルを使用してユーザーアカウントをインポートするには」を参照してください。

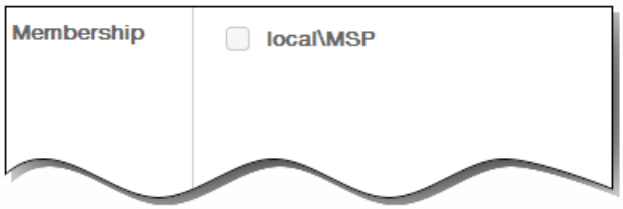
1. ［Local Users and Groups］ページで、［Add］をクリックします。［Add Local User］ページが開きます。



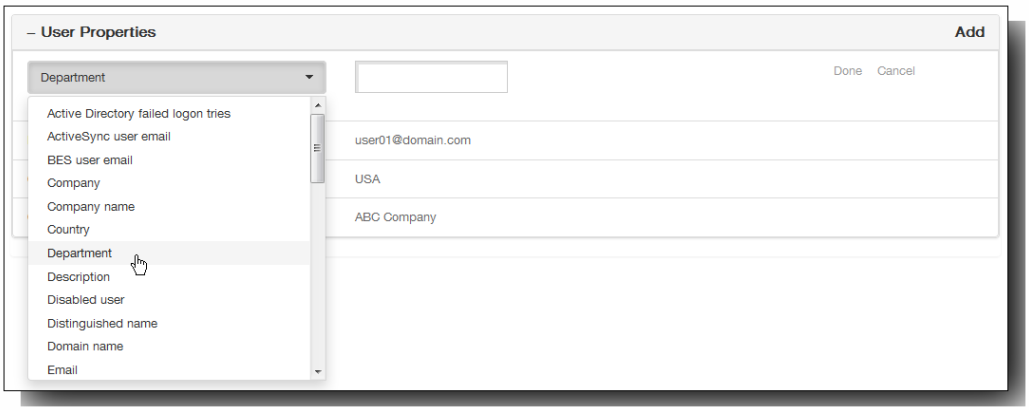
2. 以下の情報を入力して、新しいローカルユーザーを追加します。
   1. User name：ユーザーの名前を入力します。 これは必須フィールドです。
   2. Password：任意で、ユーザーのパスワードを入力します。
   3. Role：［Role］の一覧で、ユーザーの役割を選択します。 役割について詳しくは、「XenMobileでRBACを使用してカスタムの役割を作成または更新するには」を参照してください。



   4. Membership：［Membership］の一覧で、ユーザーを追加するグループをクリックします。

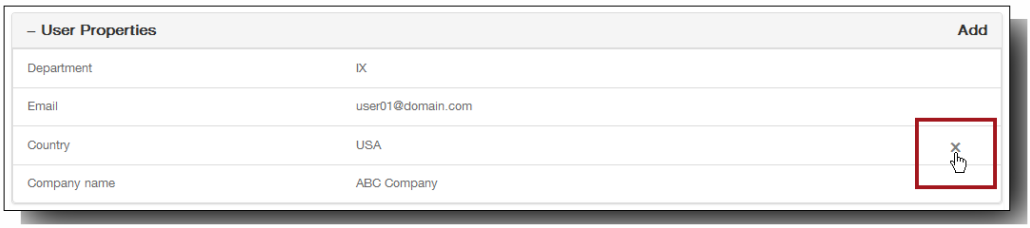


3. 任意でユーザープロパティを追加するには、次の手順に従います。
   1. ［User Properties］の横の［Add］をクリックします。
   2. ［User Properties］の一覧で、プロパティを選択します。
   3. 一覧の横のフィールドに、ユーザープロパティ属性を入力します。



4. ［Done］をクリックしてユーザープロパティを保存するか、［Cancel］をクリックして操作を取り消します。
5. 追加するほかのプロパティについて手順b.、c.、およびd.を繰り返します。

4. 任意でユーザープロパティを編集するには、次の手順に従います。
   1. 編集するユーザープロパティをクリックします。
   2. ユーザープロパティ属性を変更します。
   3. ［Done］をクリックして編集を保存するか、［Cancel］をクリックして編集を取り消します。
5. 任意でユーザープロパティを削除するには、次の手順に従います。
   1. 削除するユーザープロパティが含まれる行の上にマウスポインターを置きます。
   2. 行の右側に表示される［X］をクリックします。

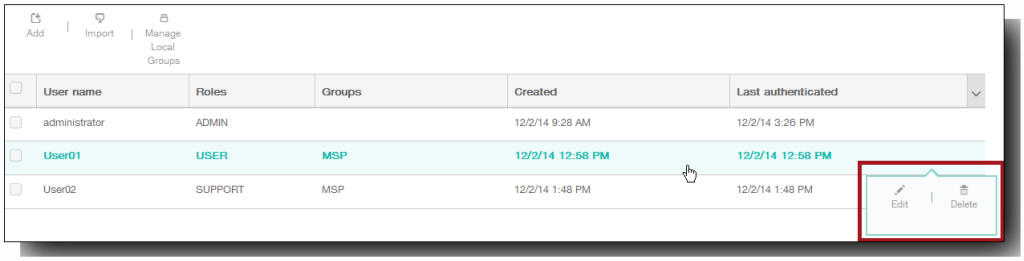


プロパティがすぐに削除されます。

6. ［Save］をクリックして、新しいユーザーを保存します。

ローカルユーザーを編集するには

1. ［Local Users and Groups］ページのユーザー一覧で、ユーザーをクリックして選択します。



［Edit Local User］ページが開きます。

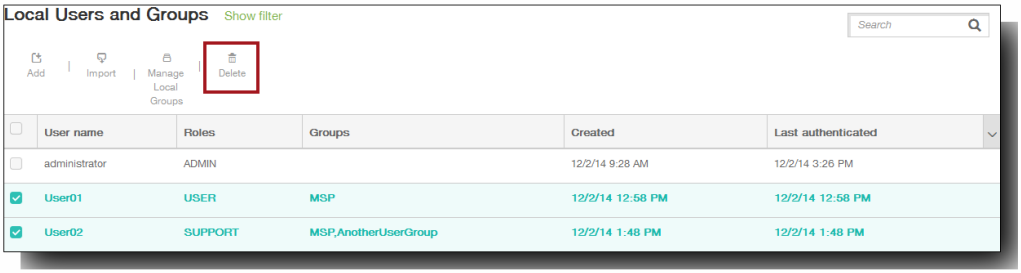
2. 必要に応じて以下の情報を変更します。
   1. User name：ユーザーの名前を入力します。 これは必須フィールドです。

2. Password：任意で、ユーザーのパスワードを入力します。
3. Role：［Role］の一覧で、ユーザーの役割を選択します。
4. Membership：［Membership］の一覧で、ユーザーを追加するグループをクリックします。
5. User properties：新しいユーザープロパティを追加するか、既存のユーザープロパティを編集します。

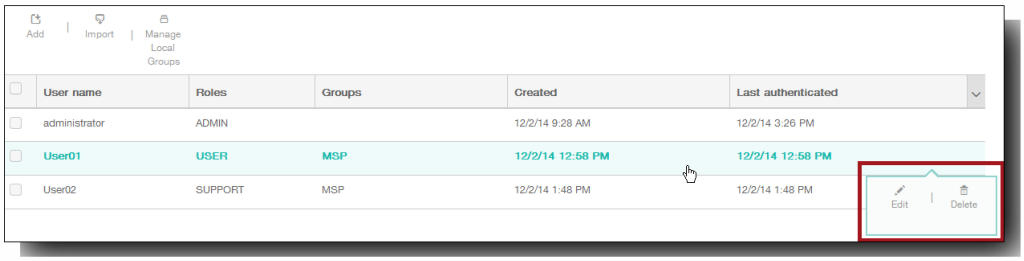
3. ［Save］をクリックして変更を保存します。

ローカルユーザーを削除するには

1. ［Local Users and Groups］ページのユーザー一覧で、次のいずれかを実行します。
   - 削除するユーザーの横のチェックボックスをオンにして、［Delete］をクリックします。



   - 削除するユーザーの行をクリックして、右に表示されるメニューで［Delete］をクリックします。



確認ダイアログボックスが開きます。［Delete］をクリックして操作を確認し、ユーザーを削除します。
重要：この操作を元に戻すことはできません。

ユーザーアカウントのインポート

May 10, 2016

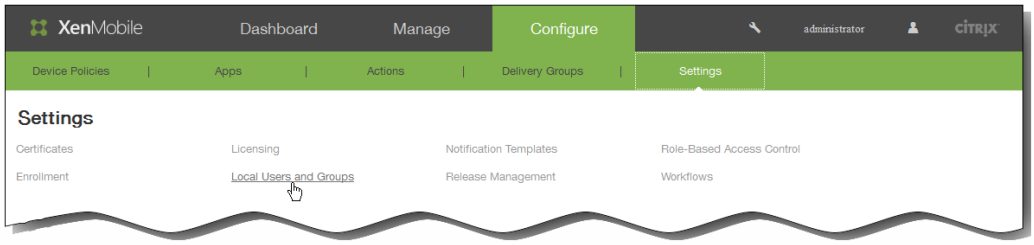
ユーザーアカウントやプロパティを、プロビジョニングファイルと呼ばれる.csvファイルからインポートできます。このファイルは手動で作成できます。プロビジョニングファイルの形式について詳しくは、「プロビジョニングファイル形式」を参照してください。

注：

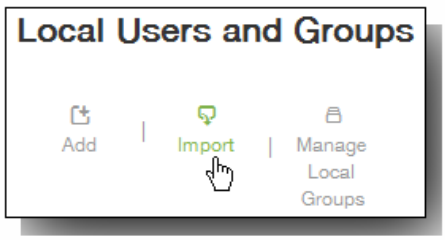
- LDAPディレクトリからユーザーをインポートする場合は、インポートファイルの中でユーザー名と共にドメイン名を使用します。たとえば、username@domain.comのように指定します。この構文を使用すると、インポートの速度が遅くなる余分なルックアップを行わずに済みます。
- XenMobileの内部ユーザーディレクトリにユーザーをインポートする場合は、インポートプロセスの速度を上げるため、デフォルトのドメインを無効にします。内部ユーザーのインポートが完了した後で、デフォルトドメインを再び有効にできます。
- ローカルユーザーはユーザープリンシパル名（User Principal Name：UPN）形式で指定できますが、管理対象ドメインは使用しないことをお勧めします。たとえば、example.comが管理されている場合、このUPN形式のローカルユーザー「user@example.com」を作成しないでください。

プロビジョニングファイルを準備した後、以下の手順に従ってファイルをXenMobileにインポートします。

1. XenMobileコンソールで、［Configure］、［Settings］、［Local Users and Groups］の順にクリックします。

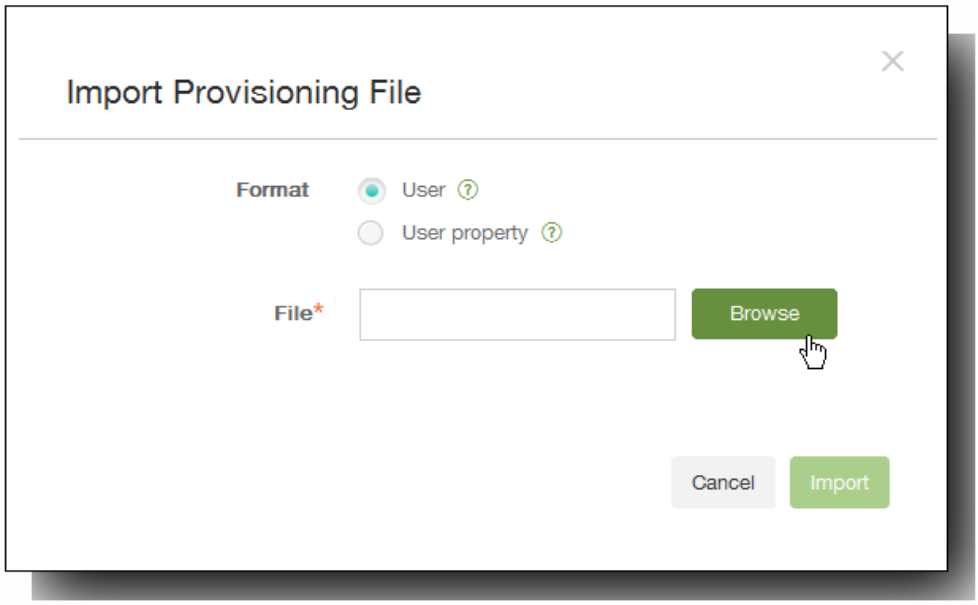


2. ［Local Users and Groups］ページで［Import］をクリックします。



［Import Provisioning File］ダイアログボックスが開きます。

3. ［Import Provisioning File］ダイアログボックスで、インポートするプロビジョニングファイルの形式を選択します。



4. ［File］の横の［Browse］をクリックし、プロビジョニングファイルの場所へ移動して、［Import］をクリックします。

プロビジョニングファイル形式

May 10, 2016

手動で作成し、XenMobileへのユーザーアカウントとプロパティのインポートに使用するプロビジョニングファイルは、次の形式である必要があります。

- ユーザープロビジョニングファイルフィールド：user;password;role;group1;group2
- ユーザー属性プロビジョニングファイルフィールド：user;propertyName1;propertyValue1;propertyName2;propertyValue2

注：

- プロビジョニングファイル内では、フィールドをセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。たとえば、プロパティpropertyV;test;1;2の入力はプロビジョニングファイルではpropertyV\;test\;1\;2;prop 2となります。
- 役割として有効な値は、定義済みの役割のUSER、ADMIN、SUPPORT、DEVICE_PROVISIONINGのほか、自分で定義した追加の役割です。
- ピリオド文字（.）は、グループ階層を作成するための区切り文字として使用します。したがって、グループ名にピリオドを使用することはできません。
- 属性プロビジョニングファイル内のプロパティ属性は小文字にする必要があります。データベースでは、大文字と小文字が区別されます。

ユーザープロビジョニングファイルの内容例

このエントリuser01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01は、次の意味です。

- User: user01
- パスワード：pwd;01
- 役割：USER
- グループ：
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

ユーザー属性プロビジョニングファイルの内容例

このエントリuser01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 valueは、次の意味です。

- User: user01
- プロパティ1：
  - 名前：propertyN
  - 値：propertyV;test;1;2
- プロパティ2：
  - 名前：prop 2
  - 値：prop 2 value

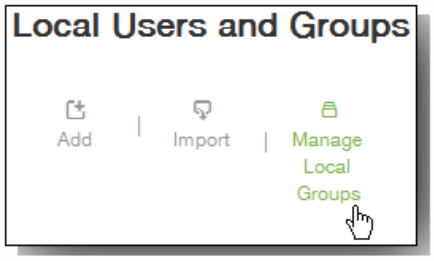
グループの追加または削除

May 10, 2016

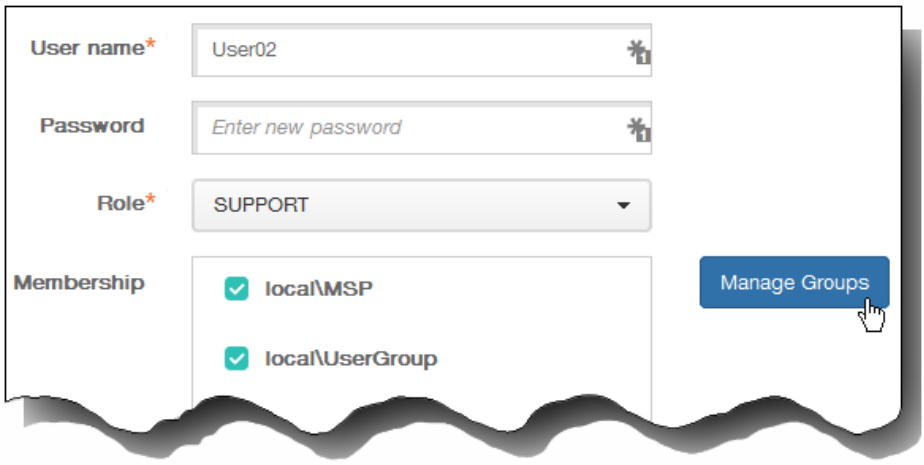
グループの管理は、XenMobileコンソールの［Manage Groups］ダイアログボックスで行います。このダイアログボックスは、［Local Users and Groups］ページ、［Add Local User］ページ、または［Edit Local User］ページからアクセスできます。グループ編集コマンドはありません。グループを削除する場合、グループを削除してもユーザーアカウントには影響しない点に注意してください。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリケーションやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

ローカルグループを追加するには

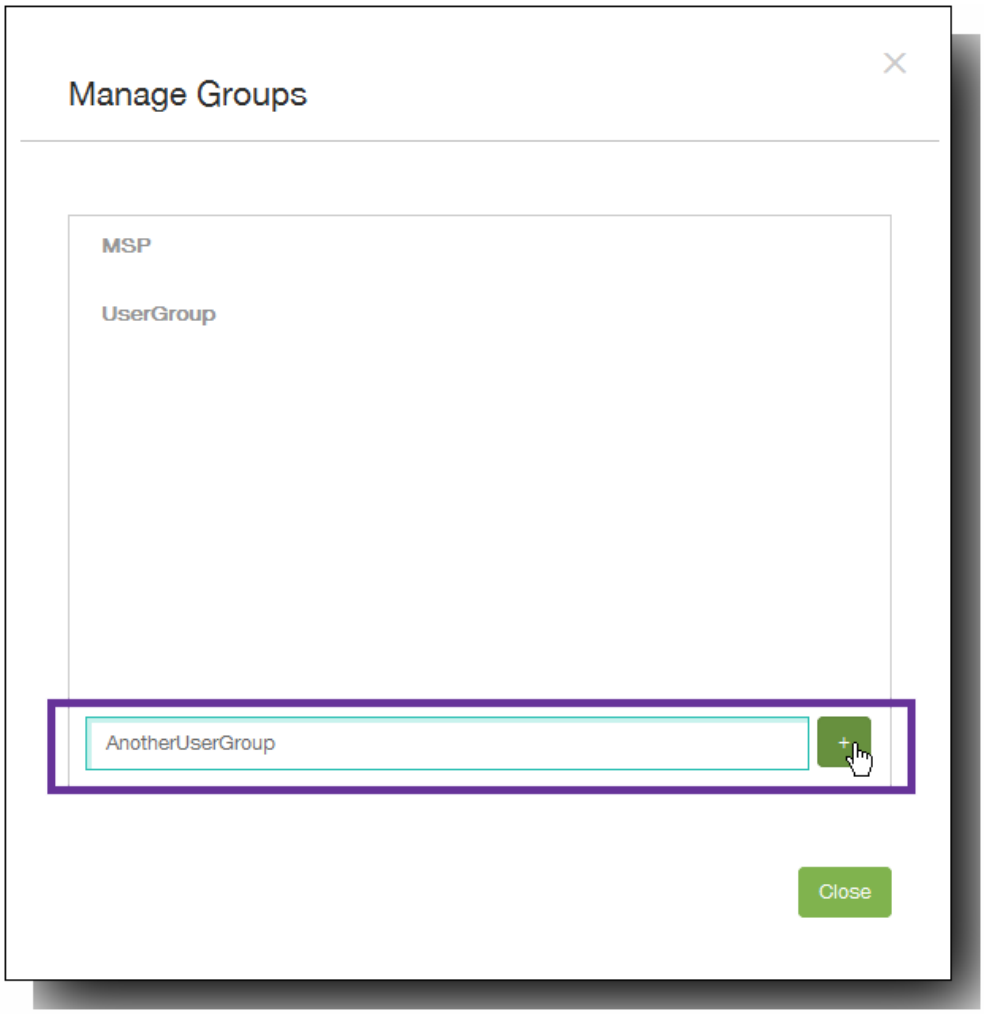
1. 次のいずれかを行います。
   - ［Local Users and Groups］ページで、［Manage Local Groups］をクリックします。



   - ［Add Local User］ページまたは［Edit Local User］ページで、［Manage Groups］をクリックします。



   ［Manage Groups］ダイアログボックスが開きます。
2. グループの一覧の下で、新しいグループ名を入力してプラス記号（+）をクリックします。



ユーザーグループが一覧に追加されます。

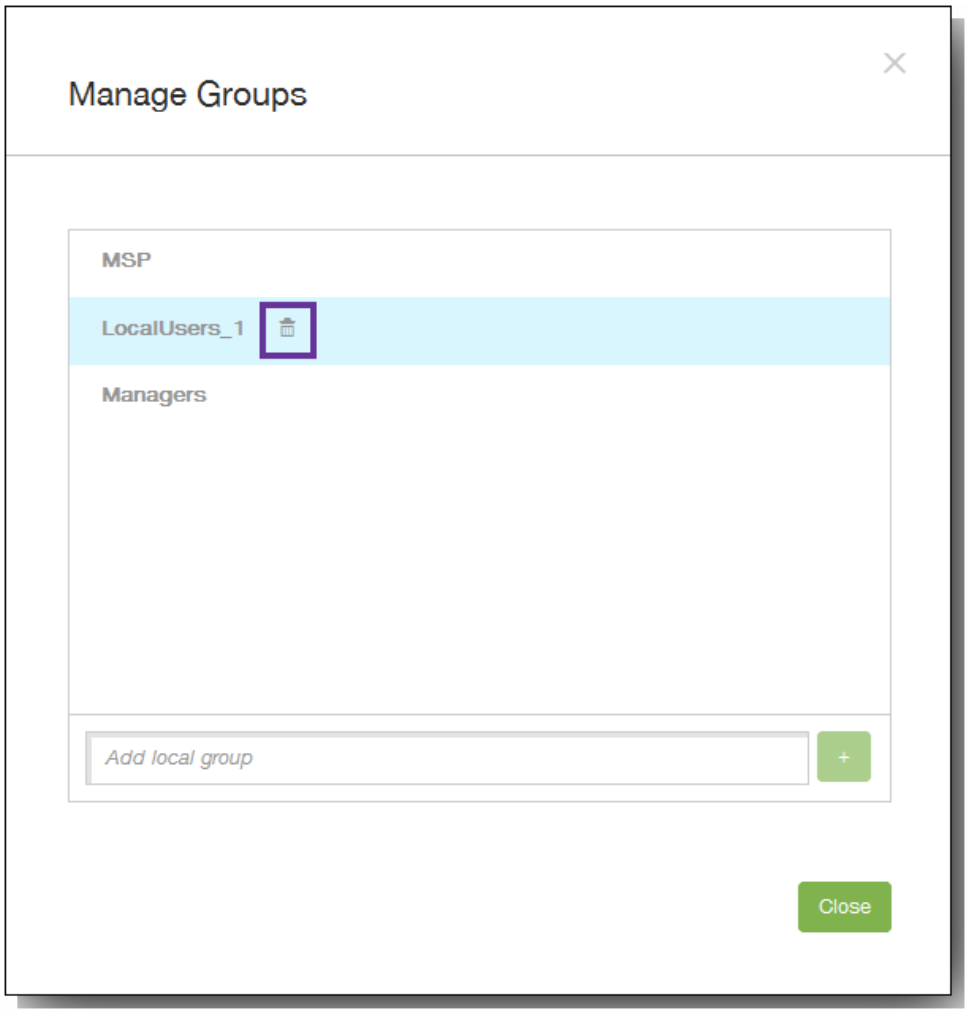
3. ［閉じる］をクリックします。

グループを削除するには

注：グループを削除してもユーザーアカウントには影響ありません。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられているデリバリーグループによって提供されているアプリケーションやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

1. 次のいずれかを行います。
   - ［Local Users and Groups］ページで、［Manage Local Groups］をクリックします。
   - ［Add Local User］ページまたは［Edit Local User］ページで、［Manage Groups］をクリックします。

   ［Manage Groups］ダイアログボックスが開きます。
2. ［Manage Groups］ダイアログボックスで、削除するグループを選択します。



3. グループ名の右側のごみ箱アイコンをクリックします。 確認ダイアログボックスが開きます。
4. ［Delete］をクリックして操作を確認し、グループを削除します。
   重要：この操作を元に戻すことはできません。
5. ［Manage Groups］ダイアログボックスで、［Close］をクリックします。

登録モードを構成してSelf Help Portalを有効化するには

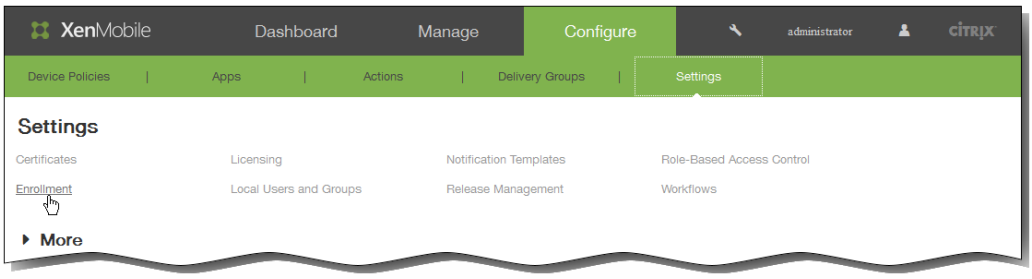
May 10, 2016

デバイス登録モードを構成して、ユーザーがデバイスをXenMobileに登録できるようにします。XenMobileには7つのモードがあり、それぞれに独自のセキュリティレベルと、ユーザーがデバイスを登録するときに行う必要がある手順があります。一部のモードはSelf Help Portalで使用可能にすることができます。ユーザーはSelf Help Portalにログオンして、デバイスを登録できる登録リンクを生成したり、登録招待状を自分に送信したりすることができます。

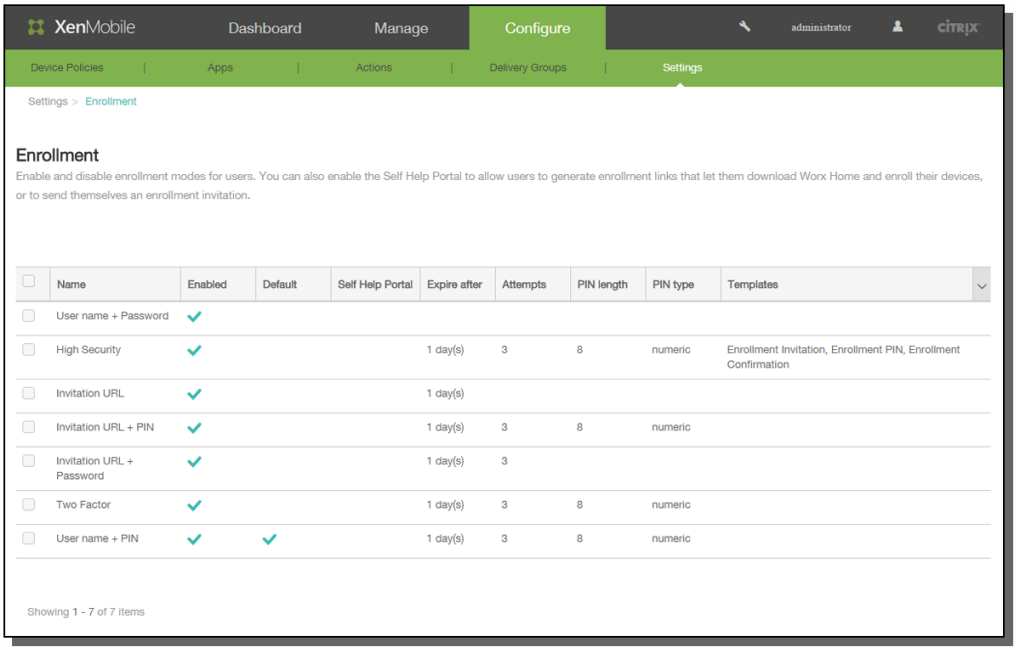
登録モードの構成は、XenMobileコンソールで［Settings］の［Enrollment］ページから行います。登録招待状の送信は、XenMobileコンソールで［Manage］の［Enrollment］ページから行います（「XenMobileへのユーザーとデバイスの登録」を参照してください）。

注：カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「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。

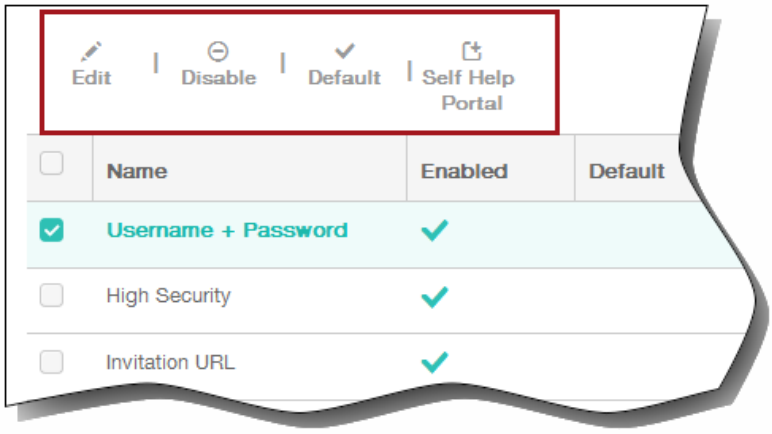
1. XenMobileコンソールで、［Configure］、［Settings］、［Enrollment］の順にクリックします。

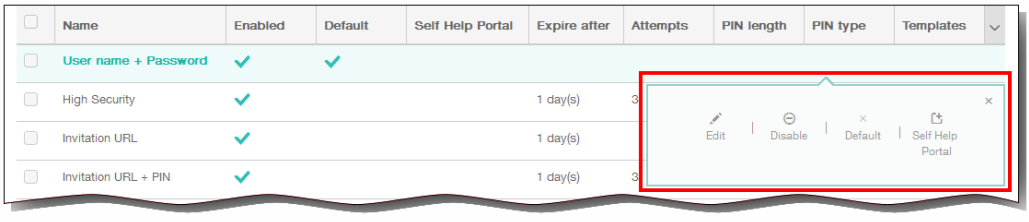


［Enrollment］ページが開き、すべての使用可能な登録モードの表が表示されます。



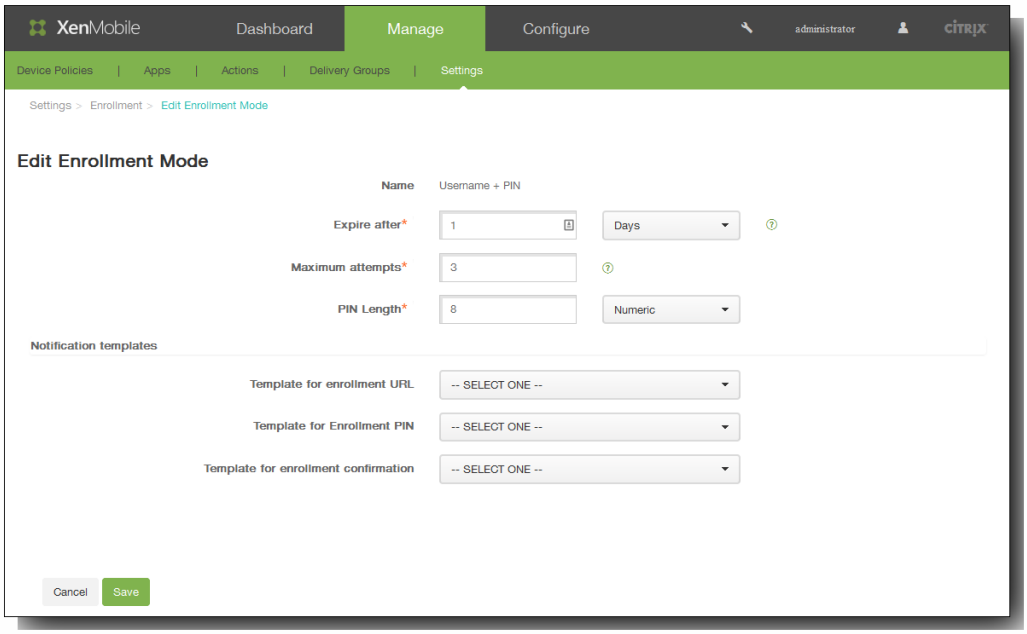
2. 一覧で登録モードを選択し、モードを編集してデフォルトに設定したり、モードを削除したり、ユーザーがSelf Help Portalからアクセスできるようにしたりします。
   注：登録モードの横にあるチェックボックスをオンにすると、登録モード一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。



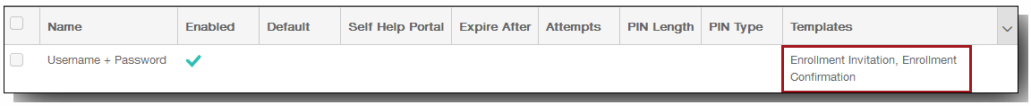


登録モードを編集するには

1. ［Enrollment］の一覧で登録モードを選択し、［Edit］をクリックします。 選択したモードによって、以下の図と異なるオプションが表示される場合があります。



2. 必要に応じて以下の情報を変更します。
   1. Expire after：ユーザーがデバイスを登録できなくなる、有効期限を入力します。
      注：0を入力すると、招待状は期限切れになりません。
   2. Days：［Expire after］ボックスに入力した有効期限に応じて、［Days］または［Hours］を選択します。
   3. Maximum attempts：登録処理からロックアウトされるまでにユーザーが実行できる登録の試行回数を入力します。
      注：「0」を入力すると、無制限に試行できます。
   4. PIN length：生成されるPINの桁数または文字数を入力します。
   5. Numeric：PINの種類として、［Numeric］または［Alphanumeric］を選択します。
3. ［Notification templates］で、必要に応じて以下の設定を変更します。
   1. Template for enrollment URL：登録URLに使用するテンプレートを選択します。 たとえば、登録招待状テンプレートではテンプレートの構成方法に応じて、デバイスをXenMobileに登録できる電子メールまたはSMSをユーザーに送信します。 通知テンプレートについて詳しくは、「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。
   2. Template for enrollment confirmation：登録が成功したことをユーザーに通知するときに使用するテンプレートを選択します。
4. ［Save］をクリックして変更を保存します。

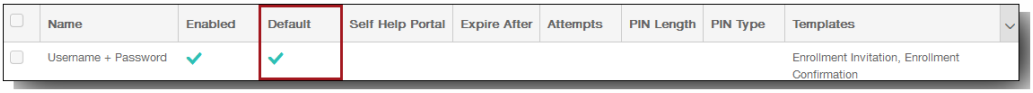


登録モードをデフォルトとして設定するには

登録モードをデフォルトとして設定すると、別の登録モードを選択しない限り、そのモードがすべてのデバイス登録要求に対して使用されます。デフォルトとして設定されている登録モードがない場合は、デバイス登録ごとに登録の要求を作成する必要があります。

注：デフォルトの登録モードとして設定できるのは、［Username + Passwords］、［Two Factor］、［Username + PIN］のいずれかのみです。

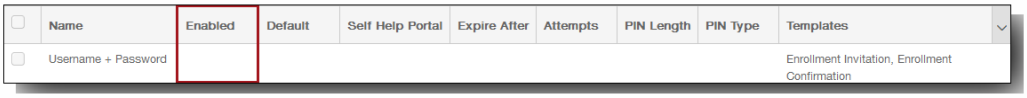
1. ［Username + Passwords］、［Two Factor］、［Username + PIN］のいずれかを選択し、デフォルトの登録モードとして設定します。
   注：デフォルトとして設定するには、選択したモードが有効化されている必要があります。
2. ［Default］をクリックします。 これにより、選択したモードがデフォルトになります。ほかの登録モードがデフォルトとして設定されていた場合、そのモードはデフォルトでなくなります。



登録モードを無効化するには

登録モードを無効化すると、その登録モードは、グループ登録招待状でもSelf Help Portalでも使用できなくなります。ある登録モードを無効化して別の登録モードを有効化することで、ユーザーがデバイスを登録できる方法を変更できます。

1. 登録モードを選択します。
   注：デフォルトの登録モードは無効化できません。デフォルトの登録モードを無効化するには、登録モードのデフォルト状態をまず解除する必要があります。
2. ［Disable］をクリックします。 登録モードが有効でなくなります。



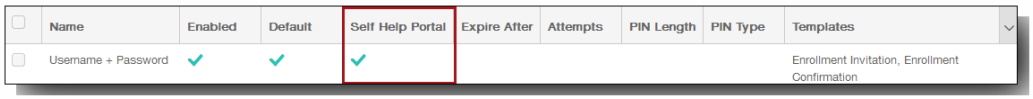
Self Help Portalで登録モードを有効化するには

Self Help Portalで登録モードを有効化すると、ユーザーが個別にデバイスをXenMobileに登録できます。

注：

- Self Help Portalで登録モードを使用できるようにするには、登録が有効化され、通知テンプレートにバインドされている必要があります。
- Self Help Portalでは、登録モードを一度に1つのみ有効化できます。

1. 登録モードを選択します。
2. ［Self Help Portal］をクリックします。 選択した登録モードをSelf Help Portalでユーザーが使用できるようになります。Self Help Portalで既に有効化されていたモードがあった場合、ユーザーはそれを使用できなくなります。



RBACを使用した役割の構成

May 10, 2016

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

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

- **Administrator**。システムへのフルアクセスが許可されます。
- **Provisioning**。管理者が、Device Provisioningツールによってすべてのデバイスをグループとしてプロビジョニングする場合に使用します。
- **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してカスタマイズし、これらの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することもできます。

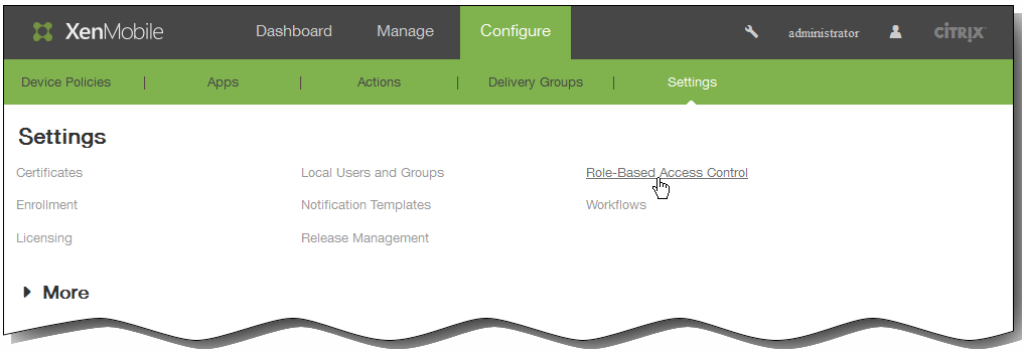
役割をローカルユーザーに（ユーザーレベルで）割り当てることや、Active Directoryグループに割り当てることができます（そのグループ内のすべてのユーザーが同じ権限を持ちます）。ユーザーが複数のActive Directoryグループに属している場合は、すべての権限が統合されてそのユーザーの権限が定義されます。たとえば、ADGroupAのユーザーがマネージャーのデバイスを検索でき、ADGroupBのユーザーが従業員のデバイスをワイプできる場合、両方のグループに属するユーザーは、マネージャー*および*従業員のデバイスを検索し、ワイプすることができます。

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。

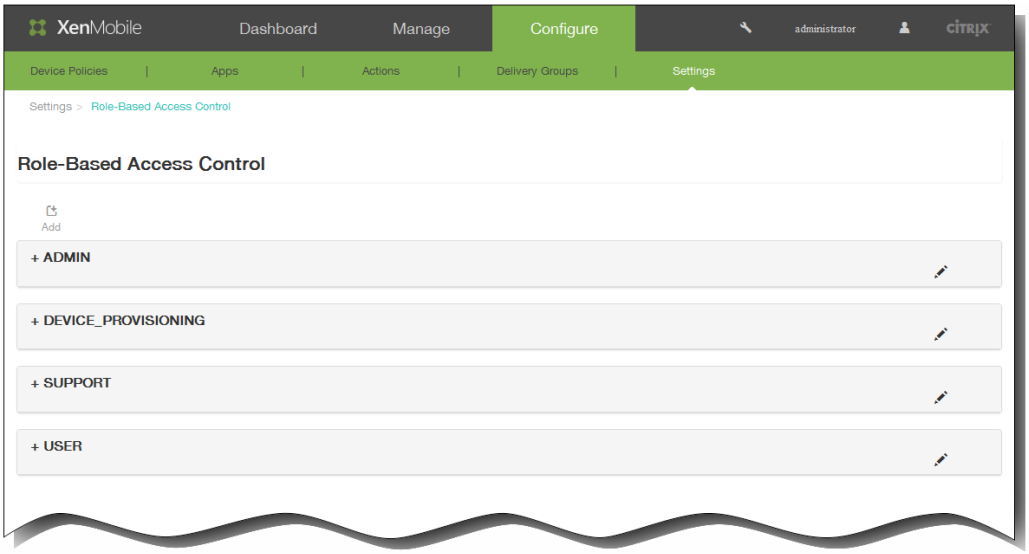
XenMobileのRBAC機能を使用すると、次のことを実行できます。

- 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。

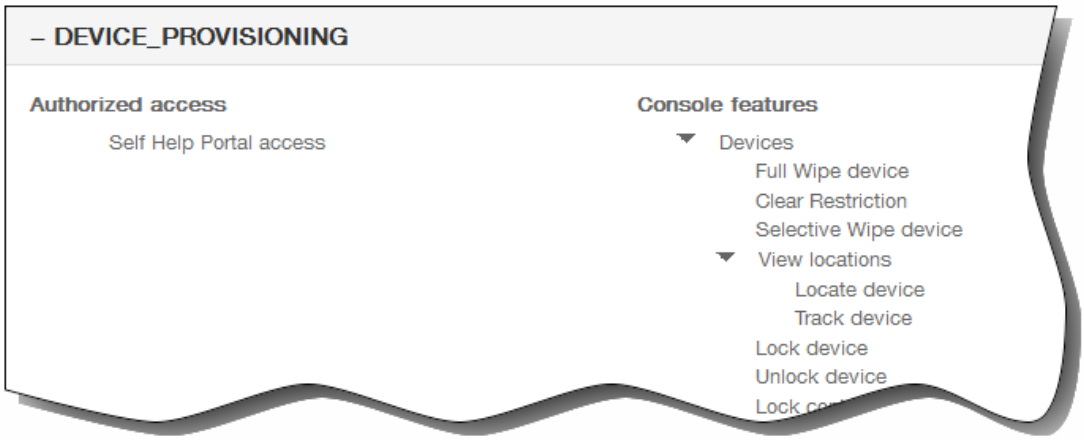
1. XenMobileコンソールで、［Configure］、［Settings］、［Role-Based Access Control］の順にクリックします。



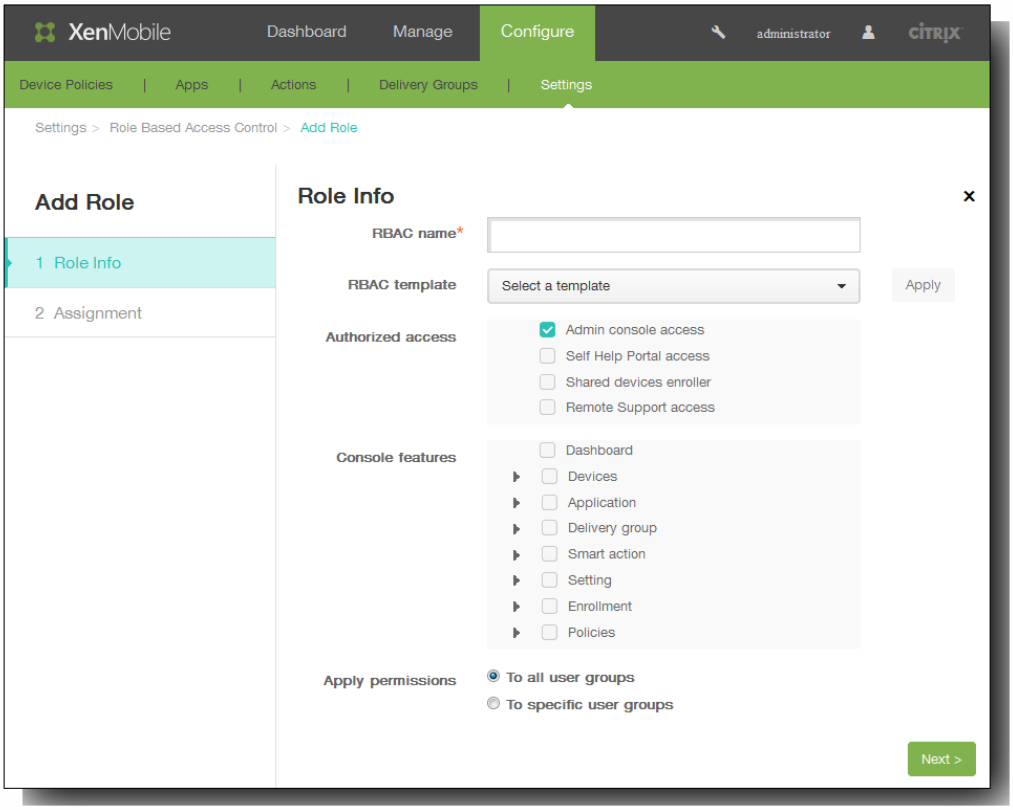
［Role］ページが開き、4つのデフォルトのユーザー役割と、以前に追加した役割が表示されます。



注：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。

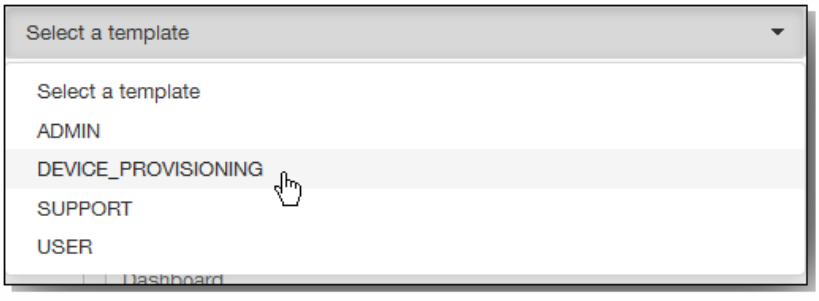


2. ［Add］をクリックして新しいユーザー役割を追加したり、既存の役割の右にあるペンアイコンをクリックして役割を編集したり、以前定義した役割の右にあるごみ箱アイコンをクリックして役割を削除したりします。 デフォルトのユーザー役割を削除することはできません。
   - ［Add］またはペンアイコンをクリックすると、［Add Role］ページまたは［Edit Role］ページが開きます。



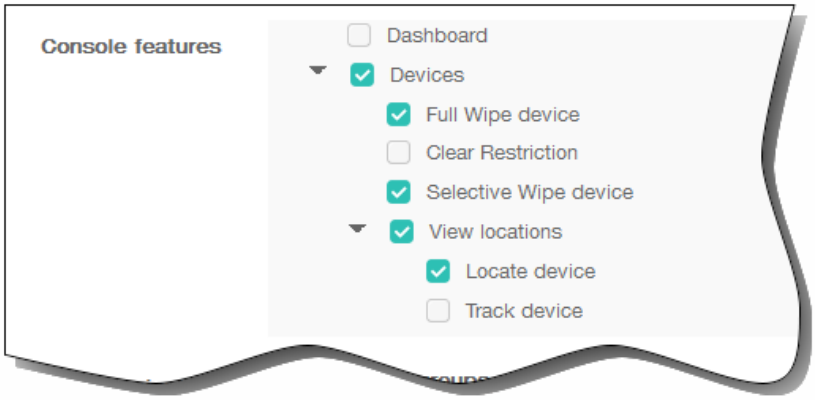
- ごみ箱アイコンをクリックすると、確認ダイアログボックスが開きます。[Delete] をクリックすると、選択した役割が削除されます。

3. 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。
   1. 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。
   2. RBAC template：新しい役割の開始点とするテンプレートを選択するか、既存の役割のための新しいテンプレートを選択します。
      注：RBACテンプレートは、デフォルトのユーザー役割と以前定義した役割です。これらによって、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。

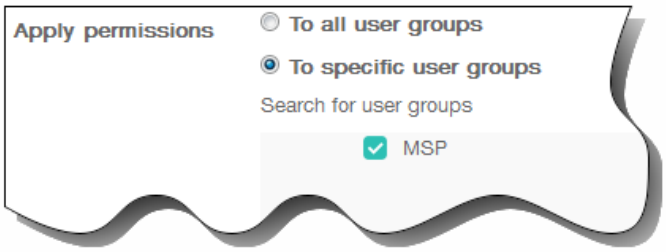


- [Apply] をクリックして、選択したテンプレートで定義済みのアクセス権と機能権限を、[Authorized access] および [Console features] にあるチェックボックスに反映させます。
- [Authorized access] および [Console features] にあるチェックボックスをオンまたはオフにして、役割をカスタ

マイズします。
注：［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読み取り専用アクセスを許可できます。そのオプションの書き込み/更新アクセスを許可するには、最上位レベルより下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、［Clear Restrictions］オプションに対するユーザーアクセスは読み取り専用アクセスのみです。

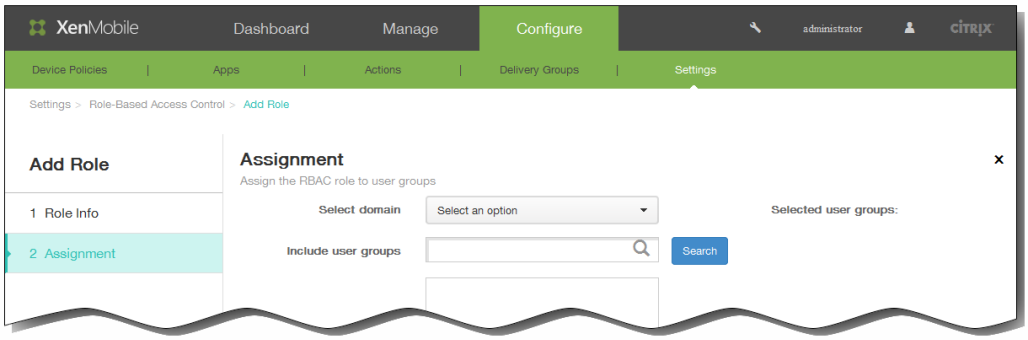


3. Apply permissions：選択した権限を適用するグループを選択します。



［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。

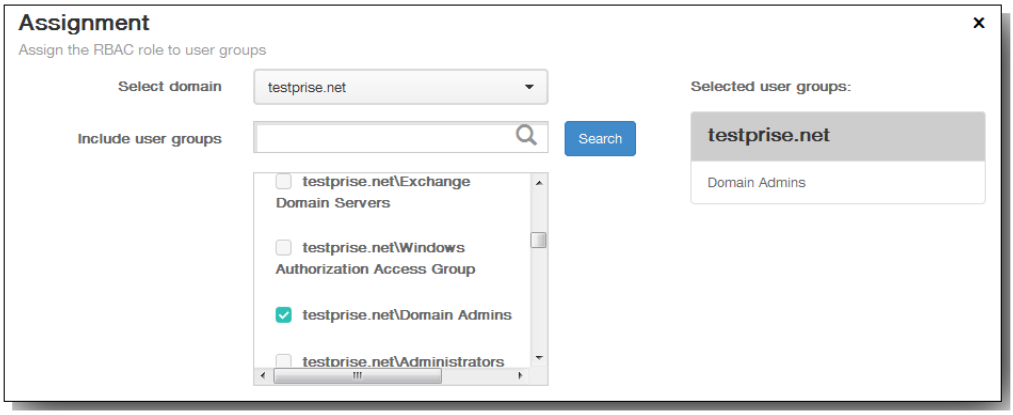
4. ［Next］をクリックします。 ［Assignment］ページが開きます。



5. 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、［Save］をクリックします。
   1. Select domain：一覧から、ドメインを選択します。
   2. 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。

3. 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、検索ボックスの右にある選択済みグループの一覧にグループが表示されます。



［Selected user groups］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。

- ［Search］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
- グループ名の全体または一部を検索ボックスに入力して［Search］をクリックし、ユーザーグループの一覧を絞り込みます。

［Selected user groups］の一覧に含まれるユーザーグループは、結果一覧内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、削除する各グループの横のチェックボックスをオフにします。

XenMobileでユーザー登録の自動検出を有効化するには

Oct 24, 2016

自動検出を使用するとユーザーの登録処理が簡単になります。 ユーザーは、ネットワークユーザー名とActive Directoryパスワードを使用してデバイスを登録できます。XenMobileサーバーの詳細を入力する必要はありません。 ユーザーは、ユーザー名をユーザープリンシパル名（User Principal Name：UPN）形式で入力します（たとえば、user@mycompany.com）。

AutoDiscoveryサービスポータル（https://xenmobiletools.citrix.com）にアクセスして、自動検出を有効にできます。 AutoDiscoveryサービスポータルについて詳しくは、「XenMobile AutoDiscovery Connectorサービス」を参照してください。

一部の限られた事例では、自動検出を有効化する場合にCitrixサポートへの連絡が必要な場合があります。 そうするために、以下の手順に従って展開の情報をCitrixテクニカルサポートチームに通知できます。また、Windowsデバイスの場合はSSL証明書も送信する必要があります。 Citrixでこの情報を受け取った後、ユーザーがデバイスを登録するときに、ドメイン情報が抽出されてサーバーアドレスにマップされます。 この情報はXenMobileデータベースで管理され、ユーザーが登録するときにこれにアクセスして使用できます。

1. Autodiscoveryサービスポータル（https://xenmobiletools.citrix.com）で自動検出を有効にできない場合は、Citrixサポートポータルでテクニカルサポートケースを作成して、以下の情報を入力します。
   - ユーザーが登録時に使用するアカウントを含むドメイン。
   - XenMobileサーバーの完全修飾ドメイン名（FQDN）。
   - XenMobileのインスタンス名。 デフォルトでは、インスタンス名はdmであり、大文字と小文字が区別されます。
   - ユーザーIDのタイプ。UPNまたはメールのいずれかにできます。 デフォルトでは、タイプはUPNです。
   - デフォルトポート8443からポート番号を変更した場合は、iOS登録に使用されるポート。
   - デフォルトポート443からポート番号を変更した場合は、XenMobileサーバーが接続を受け入れるポート。
   - XenMobile管理者のメールアドレス（オプション）。
2. Windowsデバイスを登録する場合は、以下を実行します。
   1. enterpriseenrollment.<mycompany>.comの公式に署名された非ワイルドカードSSL証明書を取得します。ここで、<mycompany>.comはユーザーが登録時に使用するアカウントを含むドメインです。 要求に.pfx形式のSSL証明書とパスワードを添付します。
   2. DNSで正規名（CNAME）レコードを作成し、SSL証明書のアドレス（enterpriseenrollment.mycompany.com）をautodisc.zc.zenprise.comにマップします。 ユーザーがWindowsデバイスを登録するときにUPNを使用する場合、XenMobileサーバーの詳細を提供するだけでなく、Citrix登録サーバーはXenMobileサーバーの有効な証明書を要求するようにデバイスに指示します。

詳細情報および証明書（該当する場合）がCitrixサーバーに追加されると、テクニカルサポートケースが更新されます。これで、ユーザーは自動検出による登録を開始できます。

注：複数のドメインを使用して登録する場合、マルチドメイン証明書を使用することもできます。マルチドメイン証明書には、以下の構造が含まれている必要があります。

- 対応するプライマリドメインを指定する、SubjectDNおよびCN（たとえば、enterpriseenrollment.mycompany1.com）。
- 残りのドメインの適切なSAN（たとえば、enterpriseenrollment.mycompany2.com、enterpriseenrollment.mycompany3.comなど）。

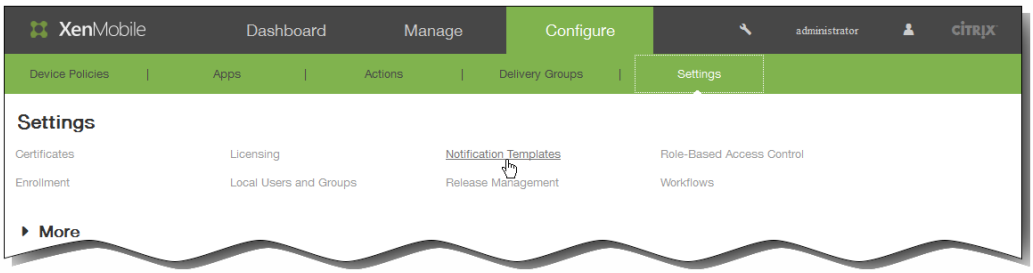
通知テンプレートの作成および更新

May 10, 2016

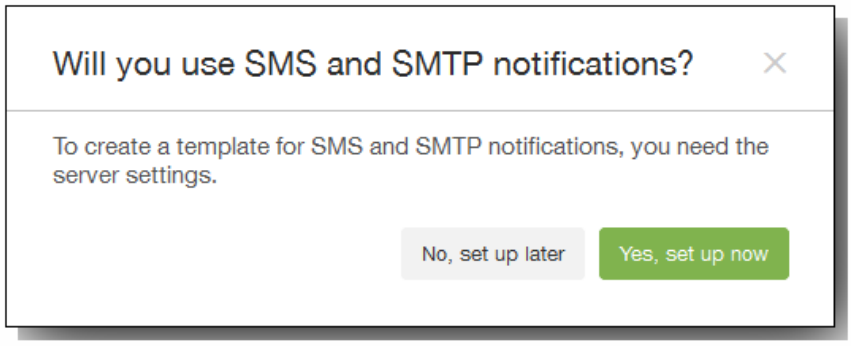
XenMobileで通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Worx Home、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。

注：SMTPまたはSMSチャネルを使用してユーザーに通知を送信する場合は、アクティブ化する前にチャネルを設定する必要があります。通知テンプレートを追加するときにチャネルがまだ設定されていないと、チャネルを設定するよう求めるメッセージが表示されます。詳しくは、「XenMobileでの通知」を参照してください。

1. XenMobileコンソールで、［Configure］、［Settings］、［Notification Templates］の順にクリックします。

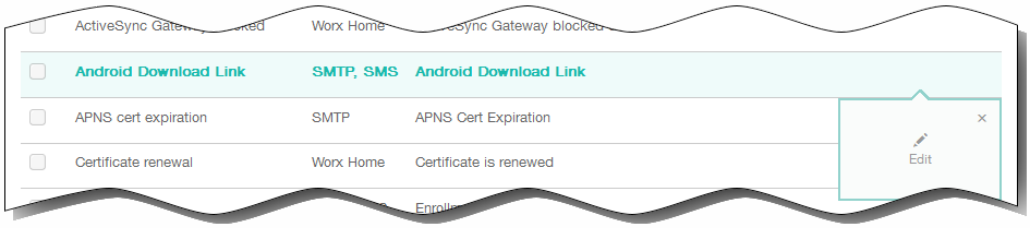


2. 次のいずれかを行います。
   - 新しい通知テンプレートを追加するには［Add］をクリックします。SMSゲートウェイまたはSMTPサーバーが設定されていない場合、SMSおよびSMTP通知に関するメッセージが表示されます。SMTPサーバーまたはSMSゲートウェイを今すぐ設定するか後で設定するかを選択できます。詳しくは、「XenMobileでの通知」を参照してください。.
     注：SMSまたはSMTPサーバーを今すぐ設定することを選択した場合は、［Configure］、［Settings］、［Notification Server］の順にクリックすると開くページにリダイレクトされます。使用するチャネルを設定した後、［Configure］、［Settings］、［Notification Template］の順にクリックすると開くページに戻って、通知テンプレートの追加または変更を続けることができます。
     重要：SMSまたはSMTPサーバーの設定を後で行うことを選択した場合、通知テンプレートの追加または編集のときにこれらのチャネルをアクティブ化することはできません。つまり、ユーザー通知の送信にこれらのチャネルを使用することができません。

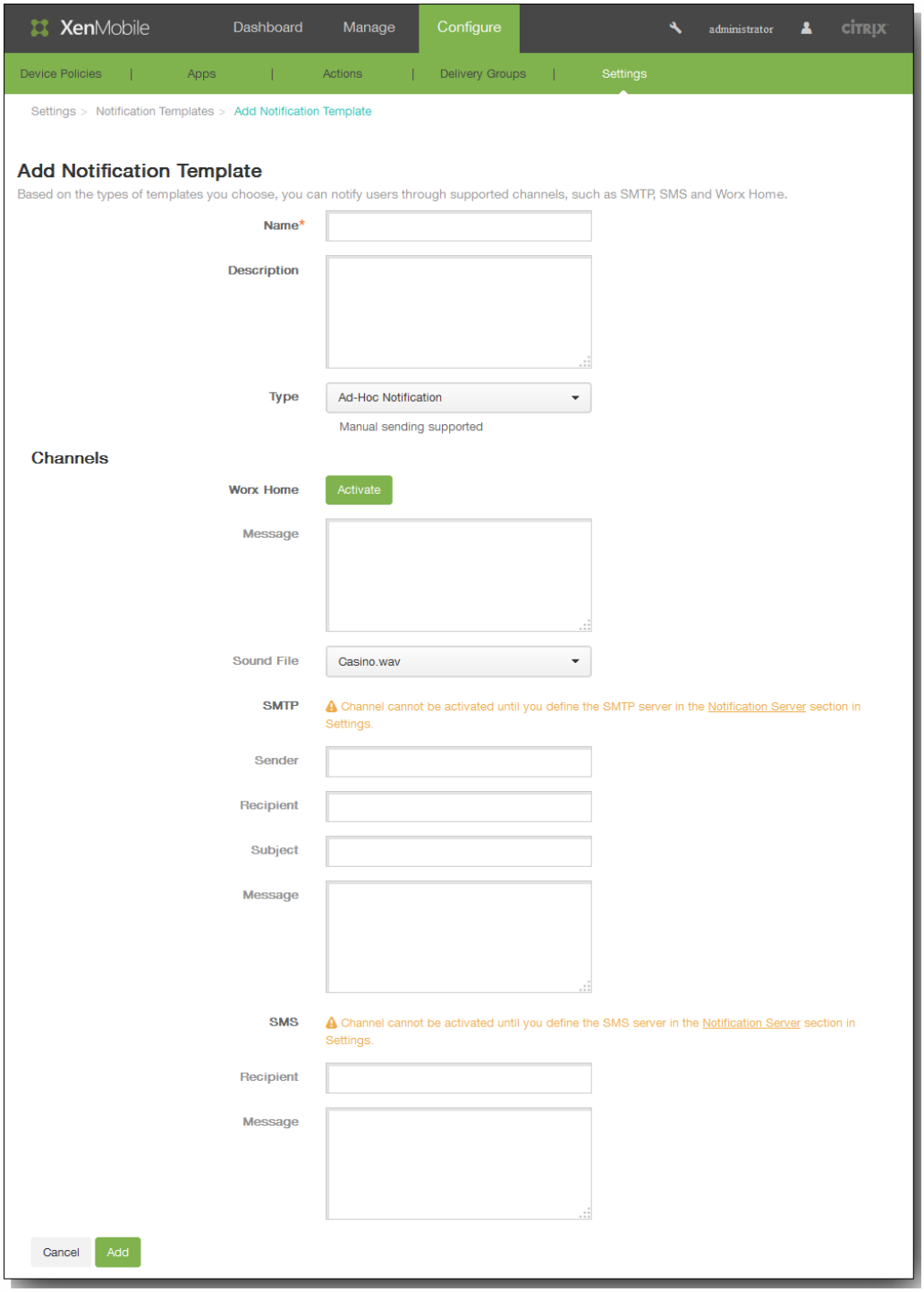


   - 編集または削除する既存のテンプレートを選択します。使用するオプションをクリックします。
     注：
     - 自分で追加した通知テンプレートのみを削除できます。定義済みの通知テンプレートは削除できません。

- 通知テンプレートの横にあるチェックボックスをオンにすると、通知テンプレート一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。
- XenMobileには、システム内のすべてのデバイスに対してXenMobileが自動的に応答する個別の種類のイベントを反映した、定義済みの通知テンプレートが多数用意されています。



テンプレートを追加するために［Add］をクリックした場合、［Add Notification Template］ページが開きます。



3. ［Add Notification Template］ページ（または、既存の通知を編集する場合は［Edit Notification Template］ページ）で、以下の情報を入力または変更します。
   1. Name：テンプレートの説明的な名前を入力します。
   2. Description：テンプレートの説明を入力します。
   3. Type：通知の種類を選択します。 選択した種類でサポートされるチャネルのみが表示されます。
      注：テンプレートの種類の一部では、種類の下に［Manual sending supported］が表示されます。これは、このテンプレートが［Dashboard］および［Devices］ページの［Notifications］一覧に表示され、手動でユーザーに通知を送信できることを意味します。いずれのチャネルの場合も、［Subject］フィールドまたは［Message］フィールドに以下のマクロが使われているテンプレートでは、手動送信は使用できません。

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

注意：定義済みテンプレートである［APNS Cert Expiration］テンプレートは1つだけ使用できます。つまり、この種類の新しいテンプレートは追加できません。

4. Channels：この通知で使用される各チャネルの情報を入力または変更します。 一部またはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。
   - Worx Homeを選択した場合、iOSデバイスおよびAndroidデバイスのみが通知を受信し、通知はデバイスの通知トレイに表示されます。
   - SMSを選択した場合、SIMカードが搭載されたデバイスのユーザーのみが通知を受信します。
   - SMTPを選択した場合、ほとんどのユーザーはメールアドレスを使って登録するため、ほとんどのユーザーがメッセージを受信します。

   Worx Home
   1. Activate：クリックして通知チャネルを有効にします。
   2. Message：ユーザーに送信されるメッセージを入力します。 Worx Homeを使用する場合、このフィールドは必須です。
   3. Sound File：ユーザーが通知を受信したときに再生される通知音を選択します。

   SMTP
   1. ［Activate］をクリックして、通知チャネルを有効にします。
      重要：SMTP通知は、SMTPサーバーが既に設定されている場合にのみ有効化できます。詳しくは、「XenMobileでの通知」を参照してください。.
   2. Sender：任意で、通知の送信者（名前、メールアドレス、またはその両方）を入力します。
   3. Recipient：このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMTP受信者アドレスに送信されるようにするためのマクロが事前設定されています。 テンプレートのマクロは変更しないでください。 アドレスをセミコロン（;）で区切って追加することにより、ユーザー以外の受信者（社内の管理者など）を追加することもできます。 アドホック通知を送信するには、このページで個別に受信者を入力するか、［Manage］の［Devices］ページでデバイスを選択して、そこから通知を送信します。 詳しくは、「XenMobileでのデバイスの追加およびデバイスの詳細の表示」を参照してください。
   4. Subject：通知の説明的な件名を入力します。 SMTPを使用する場合、このフィールドは必須です。
   5. Message：ユーザーに送信されるメッセージを入力します。

   SMS
   1. ［Activate］をクリックして、通知チャネルを有効にします。
      重要：SMTP通知は、SMTPサーバーが既に設定されている場合にのみ有効化できます。詳しくは、「XenMobileでの通知」を参照してください。.
   2. Recipient：このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMTP受信者アドレスに送信されるようにするためのマクロが事前設定されています。 テンプレートのマクロは変更しないでください。 アドホック通知を送信するには、個別に受信者を入力するか、［Manage］の［Devices］ページでデバイスを選択します。 詳しくは、「XenMobileでのデバイスの追加およびデバイスの詳細の表示」を参照してください。
   3. Message：ユーザーに送信されるメッセージを入力します。 SMSを使用する場合、このフィールドは必須です。
      重要：SMS通知は、SMSゲートウェイが既に設定されている場合にのみ有効化できます。詳しくは、「XenMobileでの通知」を参照してください。.
5. ［Add］をクリックして新しいテンプレートを追加するか、［Save］をクリックして編集を保存します。すべてのチャネルが正しく構成されている場合、［Notification Templates］ページに、SMTP、SMS、Worx Homeの順に表示されます。正しく構成されていないチャネルがあれば、正しく構成されているチャネルの後に表示されます。

デリバリーグループの管理

May 10, 2016

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 8.1、Windows 8.1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。

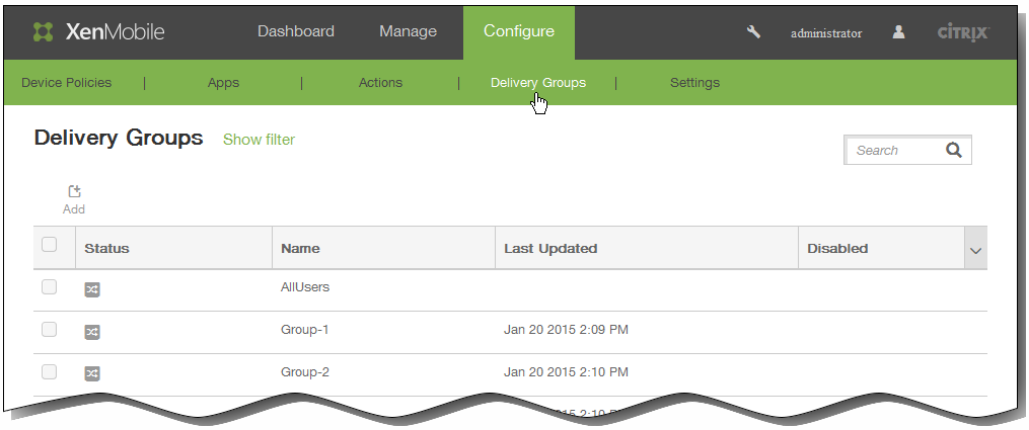
デフォルトのAllUsersデリバリーグループは、XenMobileをインストールして構成するときに作成されます。このグループには、すべてのローカルユーザーとActive Directoryユーザーが含まれます。AllUsersグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

XenMobileでデリバリーグループを追加、編集、無効化、有効化、展開、削除することで、ポリシー、アプリケーション、アクションをどのようにユーザーに展開するかを管理できます。これらのアクションのそれぞれについて、このトピックの次の節以降で説明します。

- デリバリーグループを追加するには
- デリバリーグループを編集するには
- AllUsersデリバリーグループを有効化および無効化するには
- 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を削除するには

デリバリーグループの管理を開始するには、次の手順に従って［Delivery Groups］ページを開きます。

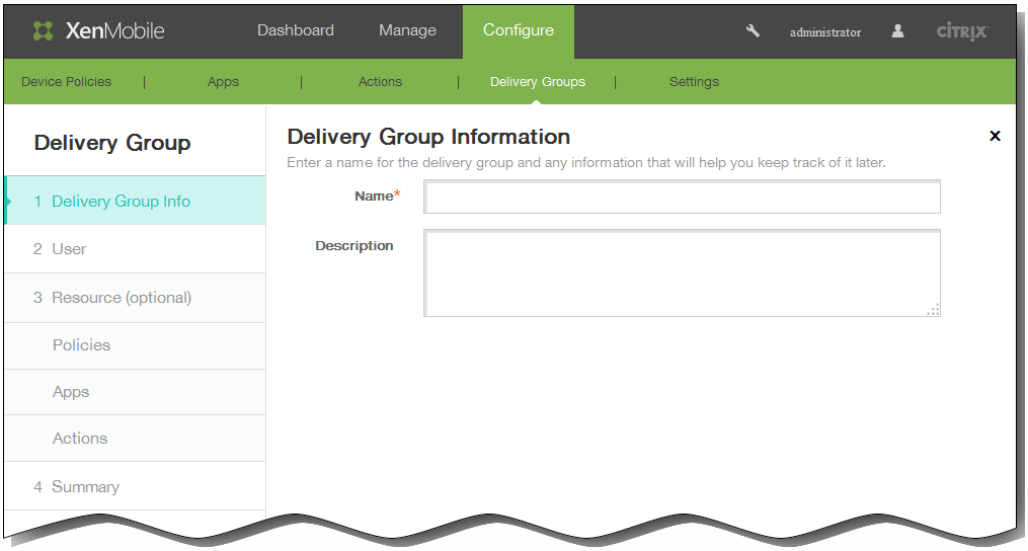
1. XenMobileコンソールで、［Configure］の［Delivery Groups］をクリックします。



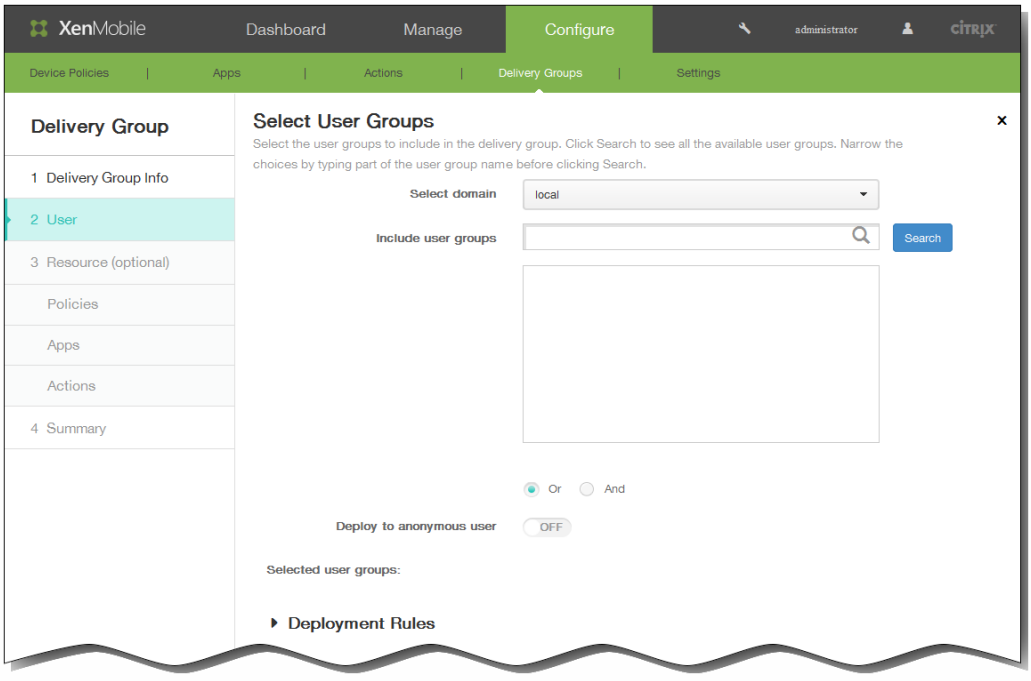
［Delivery Groups］ページが開きます。次に、実行するアクションに関する特定のeDocsトピックを参照します。

デリバリーグループを追加するには

1. ［Delivery Groups］ページで、［Add］をクリックします。 ［Delivery Group Information］ページが開きます。



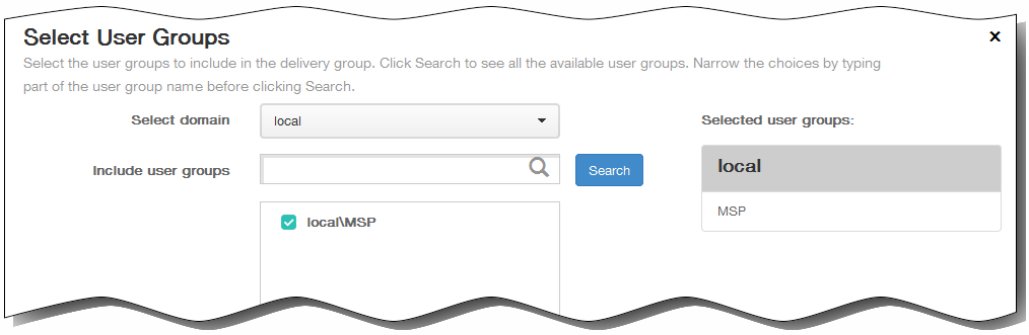
2. ［Delivery Group Information］ペインで、以下の情報を入力します。
   1. Name：デリバリーグループの説明的な名前を入力します。
   2. Description：任意で、デリバリーグループの説明を入力します。
3. ［Next］をクリックします。 ［Delivery Group User］ページが開きます。



4. ［Select User Groups］ペインで、以下の情報を入力します。
   1. 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。
   2. Include user groups：次のいずれかを行います。

- ［Search］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
- グループ名の全体または一部を検索ボックスに入力して［Search］をクリックし、ユーザーグループの一覧を絞り込みます。

3. ユーザーグループの一覧で、追加するグループを選択します。 選択したグループが［Selected user groups］一覧に表示されます。



［Selected user groups］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。

- ［Search］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
- グループ名の全体または一部を検索ボックスに入力して［Search］をクリックし、ユーザーグループの一覧を絞り込みます。

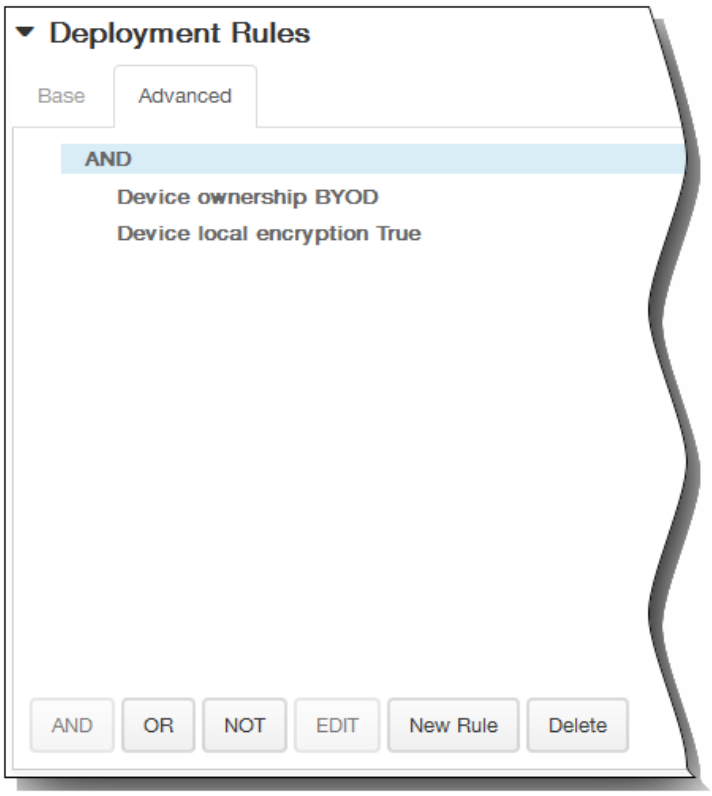
［Selected user groups］の一覧に含まれるユーザーグループは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除する各グループの横のチェックボックスをオフにします。

4. Or/And：リソースが展開されるユーザーがいずれかのグループに属していればよいか（［Or］）、すべてのグループに属している必要があるか（［And］）を選択します。
5. Deploy to anonymous user：デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。
   注：認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

5. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

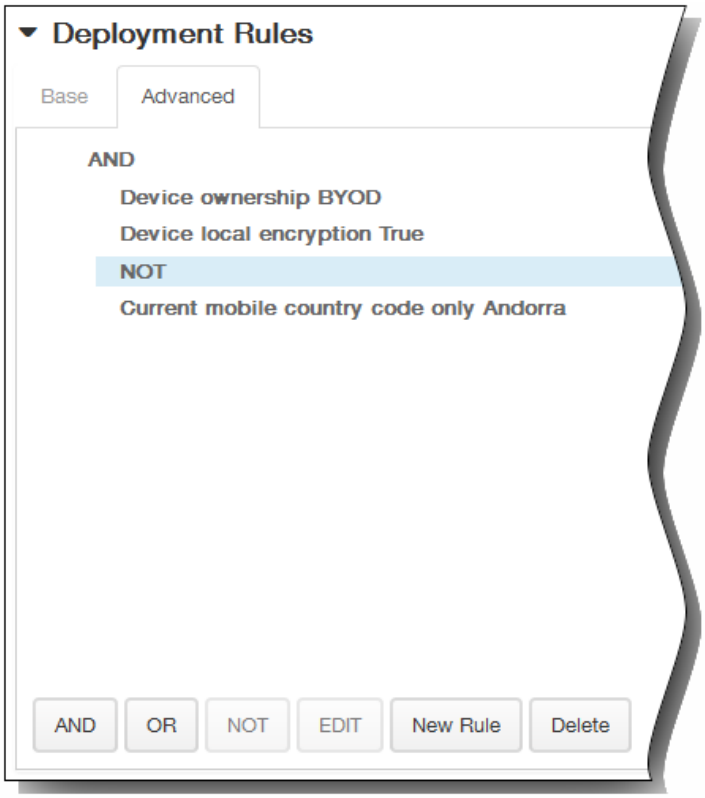
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
   1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。

2. ［Advanced］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。

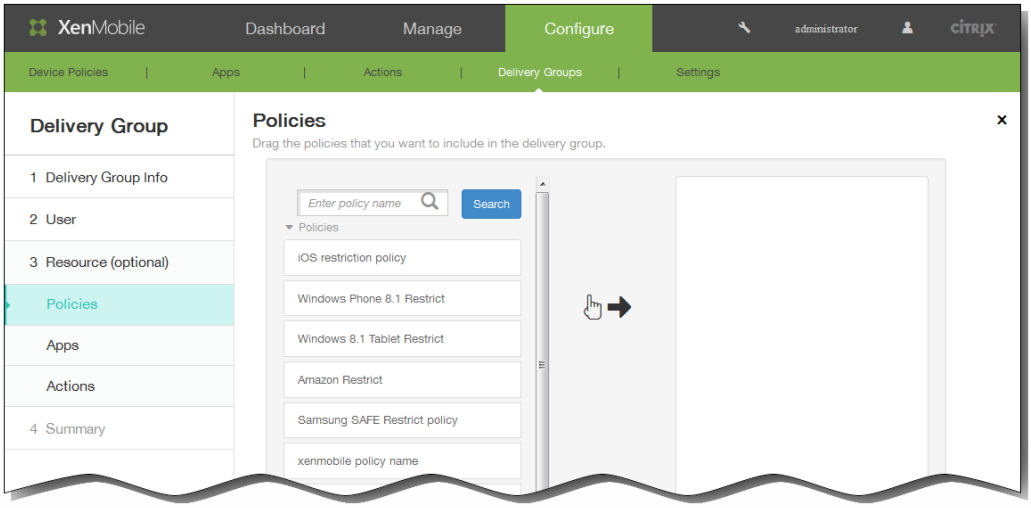


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。

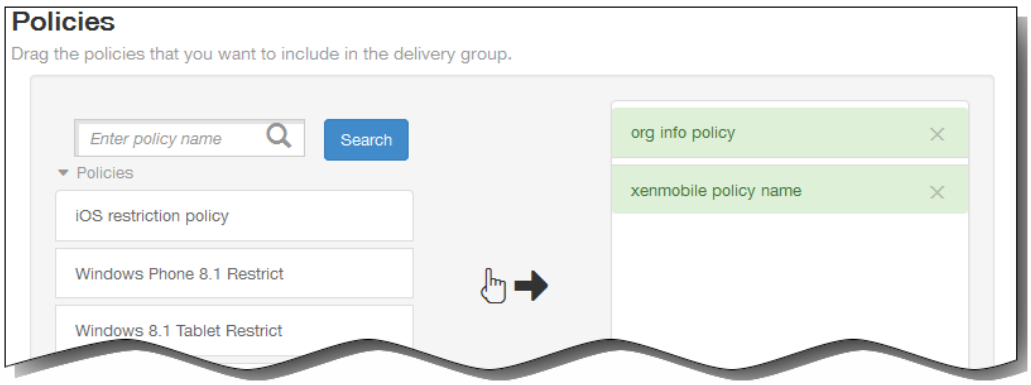


6. ［Next］をクリックします。 ［Delivery Group Resources］ページが開きます。オプションとして、このページでデリバリーグループのポリシー、アプリケーション、アクションを追加します。この手順をスキップするには、［Delivery Group］の［Summary］をクリックしてデリバリーグループ構成の概要情報を表示します。スキップしない場合は、以下の操作を行います。
注：リソースをスキップするには、［Resources (optional)］で追加するリソースをクリックし、そのリソースの手順に従います。
ポリシーを追加するには



1. 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るか、ポリシーの一覧を限定するため、検索ボックスにポリシー名の全体または一部を入力して［Search］をクリックします。

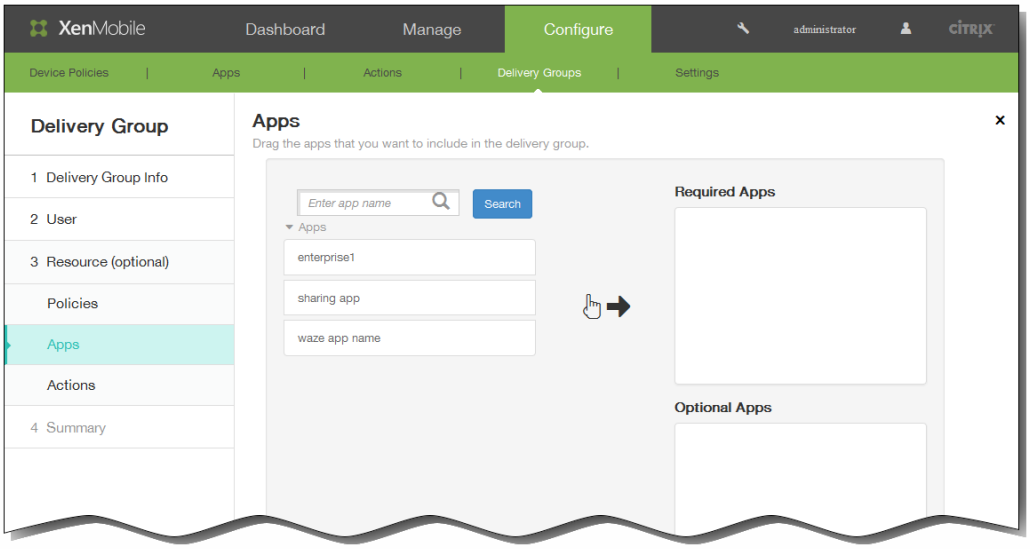
2. ポリシーをクリックして、右側のボックス内へドラッグします。
3. 手順a.およびb.を繰り返して、ポリシーをさらに追加します。



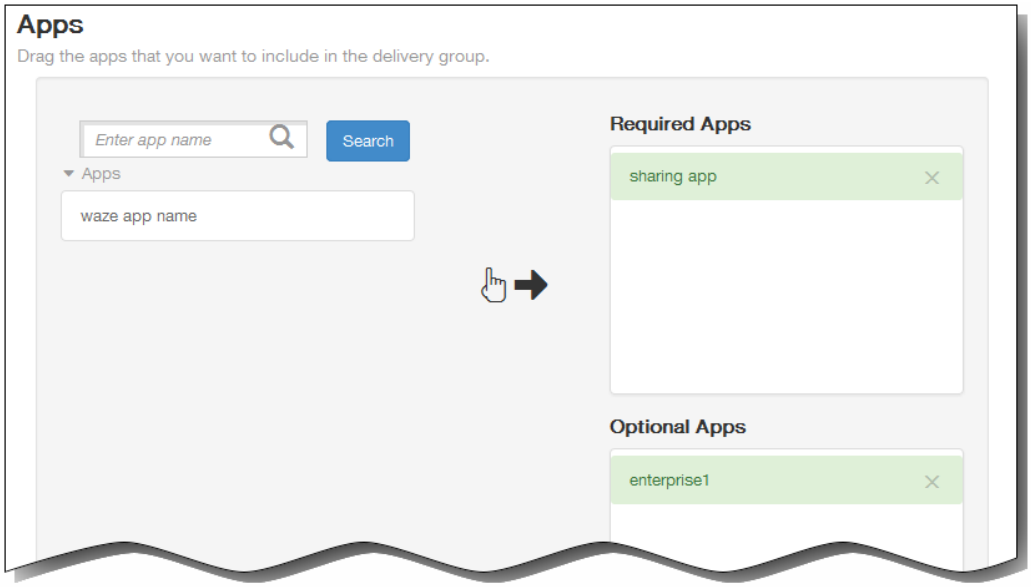
ポリシーリソースを削除するには、ポリシー名の横にある［X］をクリックします。

4. ［Next］をクリックして、［Apps］リソースページに移動します。 リソースをそれ以上追加しない場合は、［Delivery Group］の［Summary］をクリックします。 ［Apps］リソースページが開くか、［Summary］ページが開きます。

アプリケーションを追加するには



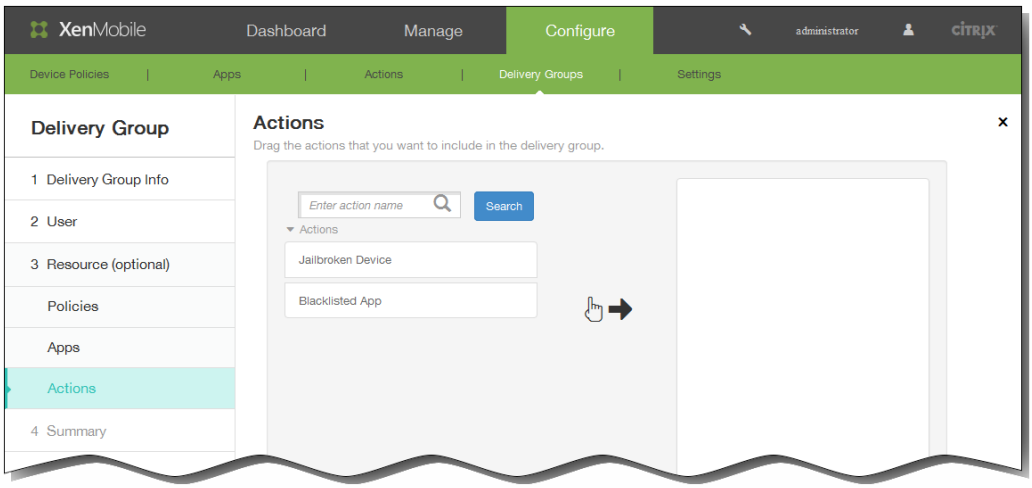
1. 使用可能なアプリケーションの一覧をスクロールして追加するアプリケーションを見つけるか、アプリケーションの一覧を限定するため、検索ボックスにアプリケーション名の全体または一部を入力して［Search］をクリックします。
2. アプリケーションをクリックして、［Required Apps］ボックス内または［Optional Apps］ボックス内へドラッグします。
3. 手順a.およびb.を繰り返して、アプリケーションをさらに追加します。



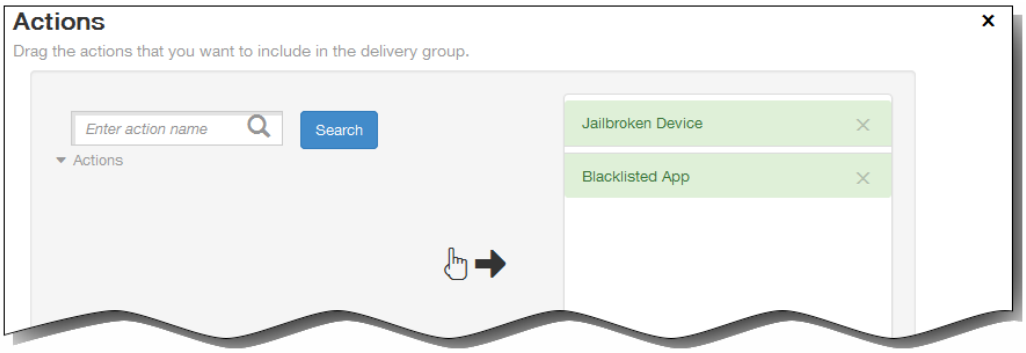
アプリケーションリソースを削除するには、アプリケーション名の横にある［X］をクリックします。

4. ［Next］をクリックして、［Actions］リソースページに移動します。 リソースをそれ以上追加しない場合は、［Delivery Group］の［Summary］をクリックします。 ［Actions］リソースページが開くか、［Summary］ページが開きます。

アクションを追加するには

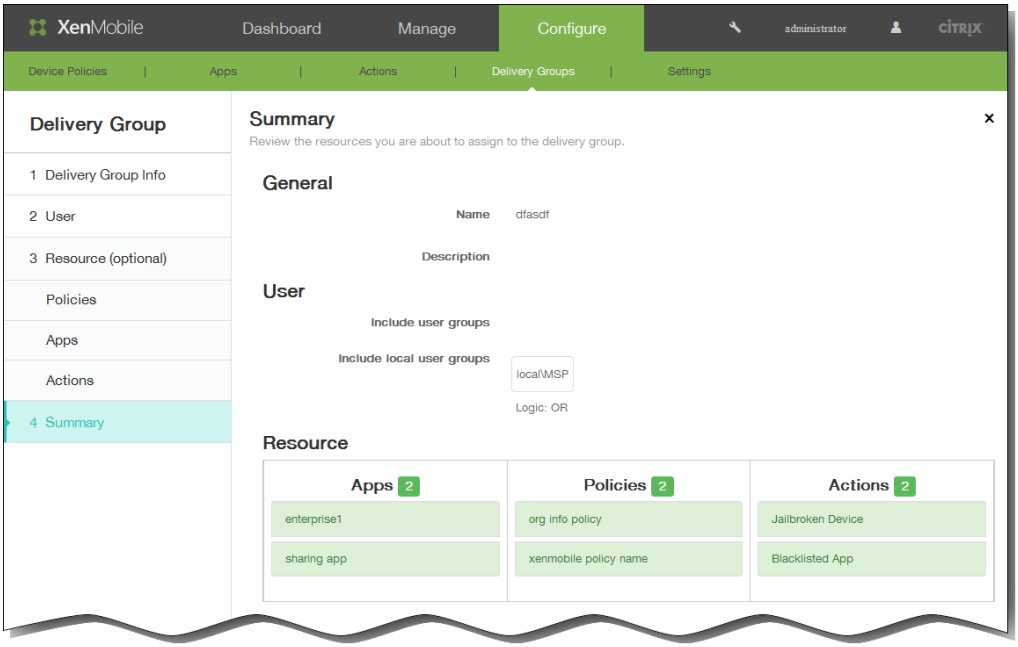


1. 使用可能なアクションの一覧をスクロールして追加するアクションを見つけるか、アクションの一覧を限定するため、検索ボックスにアクション名の全体または一部を入力して［Search］をクリックします。
2. アクションをクリックして、右側のボックス内へドラッグします。
3. 手順a.およびb.を繰り返して、アクションをさらに追加します。



アクションリソースを削除するには、アクション名の横にある［X］をクリックします。

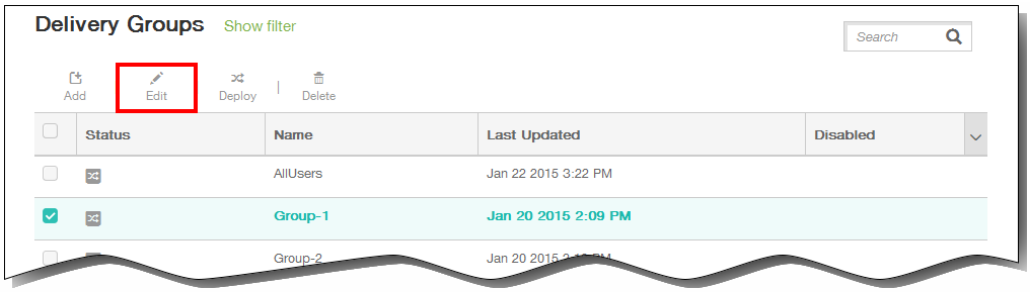
4. ［Next］をクリックします。 ［Summay］ページが開きます。

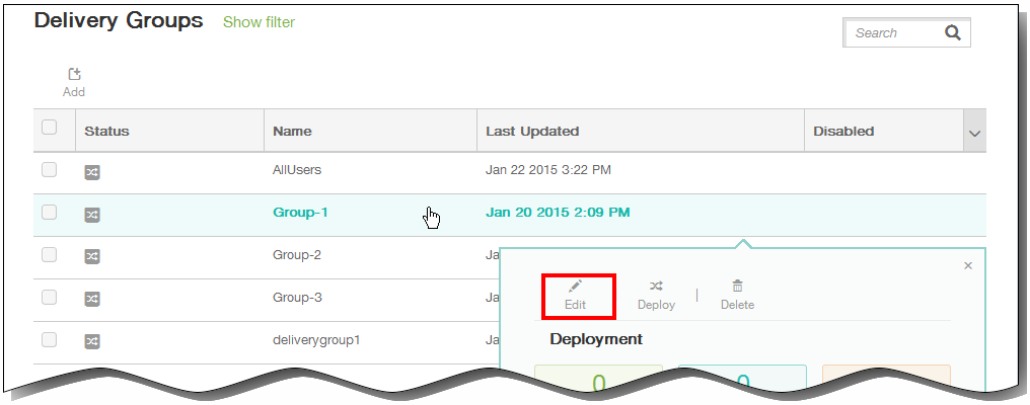


7. ［Summary］ページで、デリバリーグループに対して構成したオプションを確認します。 構成の調整が必要な場合は、 ［Back］をクリックして前のページに戻ります。
8. ［Save］をクリックして、デリバリーグループを保存します。

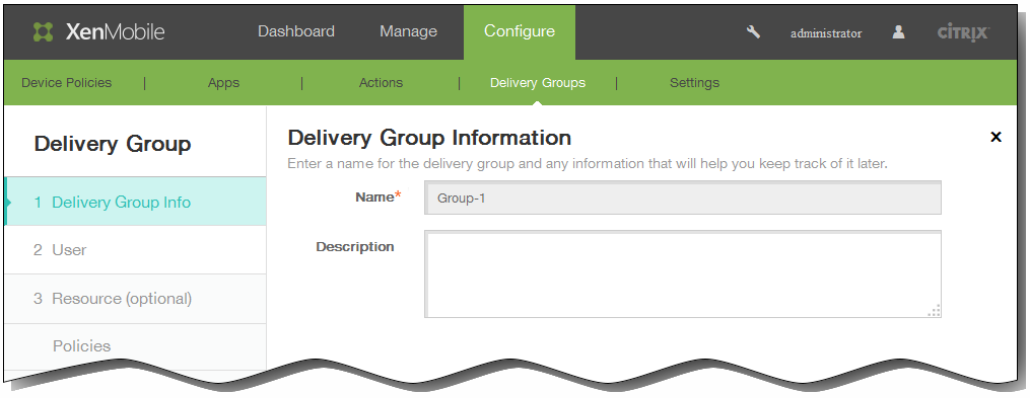
デリバリーグループを編集するには

1. ［Delivery Groups］ページで、デリバリーグループ名の横にあるチェックボックスをオンにするか、デリバリーグループ名を含む行をクリックして、デリバリーグループを選択します。
2. ［Edit］をクリックします。
   注：デリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に[Edit］コマンドが表示されます。

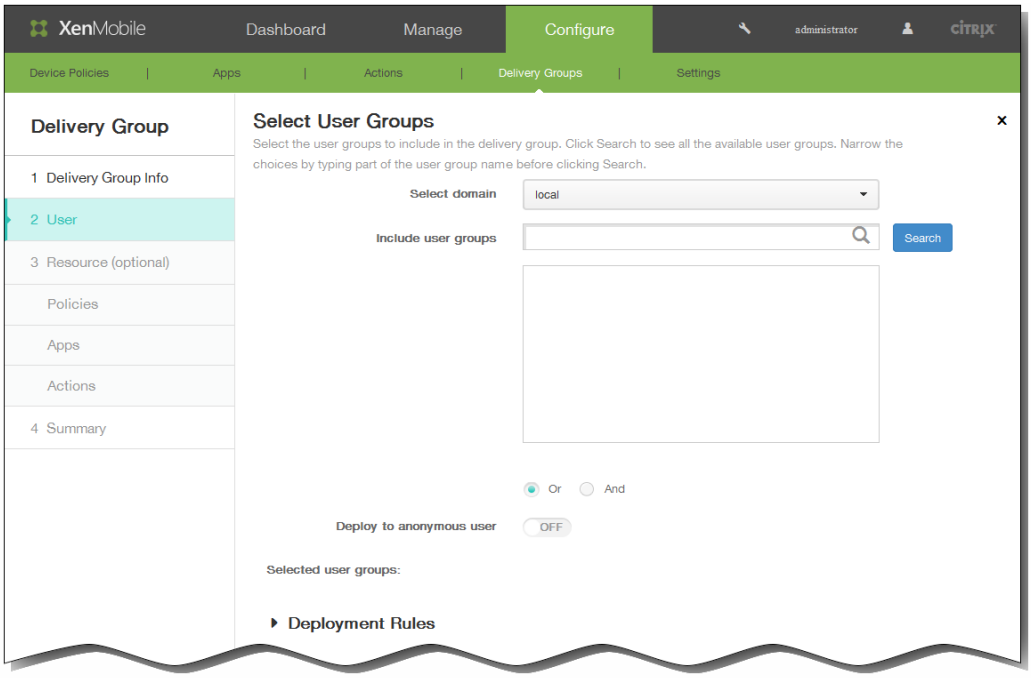




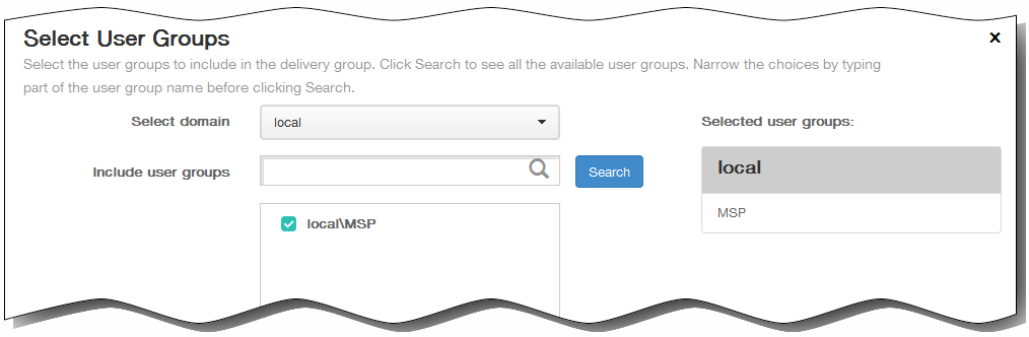
［Delivery Group Information］編集ページが開きます。



3. ［Description］ボックスに説明を追加するか、または既存の説明を変更します。
   注：既存のグループの名前は変更できません。
4. ［Next］をクリックします。 ［Select User Groups］ページが開きます。

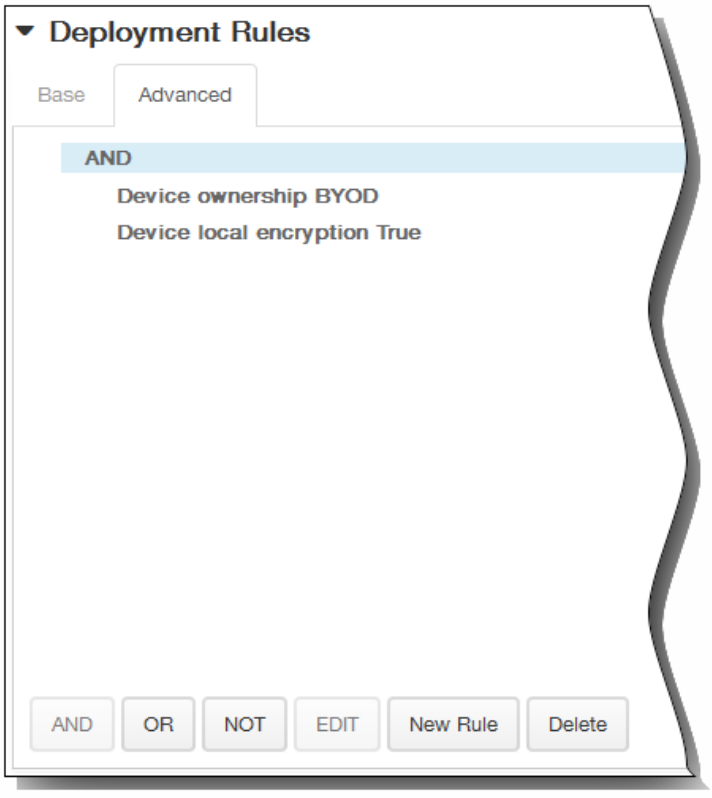


5. ［Select User Groups］ペインで、以下の情報を入力または変更します。
   1. Select domain：一覧から、ユーザーを選択するドメインを選択します。
   2. Include user groups：次のいずれかを行います。
      - ［Search］をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
      - グループ名の全体または一部を検索ボックスに入力して［Search］をクリックし、ユーザーグループの一覧を絞り込みます。
   3. ユーザーグループの一覧で、追加するグループを選択します。 選択したグループが［Selected user groups］一覧に表示されます。



   注：ユーザーグループを削除するには、［Search］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［Search］をクリックすると、一覧に表示されるユーザーグループ数を絞り込むことができます。
   4. Or/And：展開対象のユーザーがいずれかのグループに属していればよいか（［Or］）、すべてのグループに属している必要があるか（［And］）を選択します。
   5. Deploy to anonymous user：デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。
      注：認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。
6. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

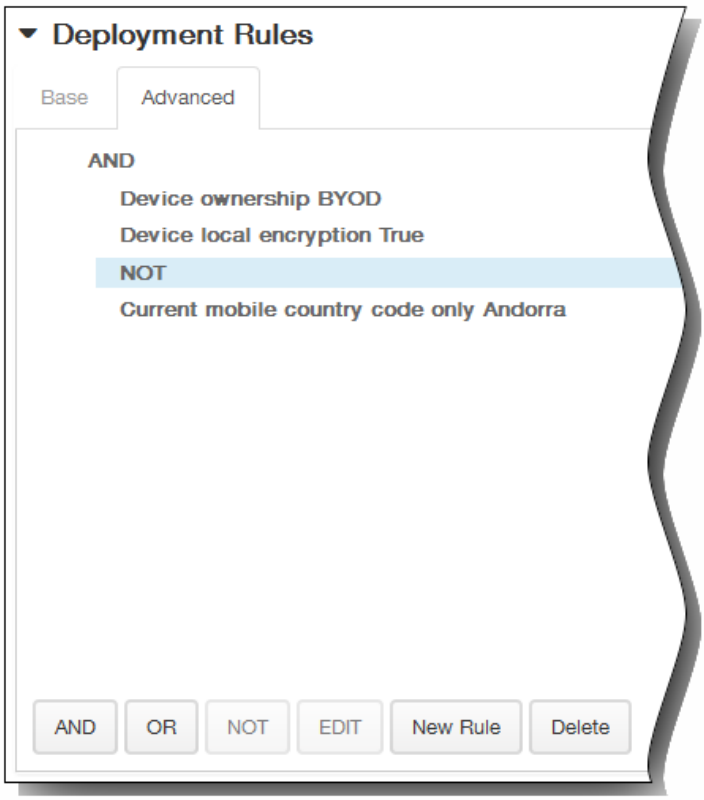


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。

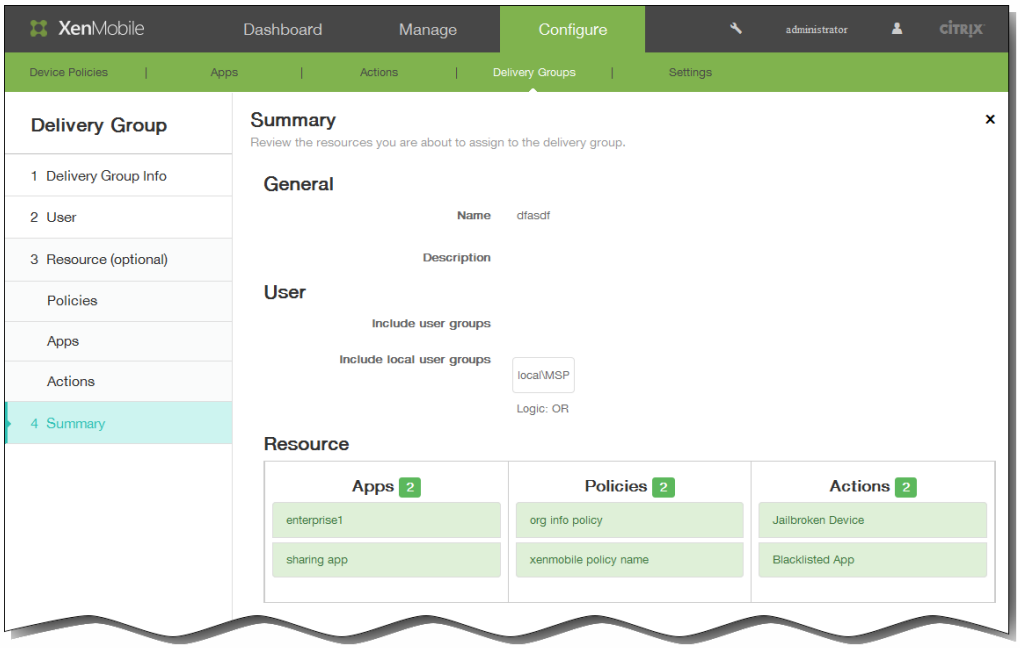
いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



7. ［Next］をクリックします。［Delivery Group Resources］ページが開きます。このページでポリシー、アプリケーション、アクションを追加または削除します。この手順をスキップするには、［Delivery Group］の［Summary］をクリックしてデリバリーグループ構成の概要情報を表示します。
リソースの変更が完了したら、［Next］をクリックするか、［Delivery Group］の［Summary］をクリックします。

次のリソースページが開くか、［Summary］ページが開きます。

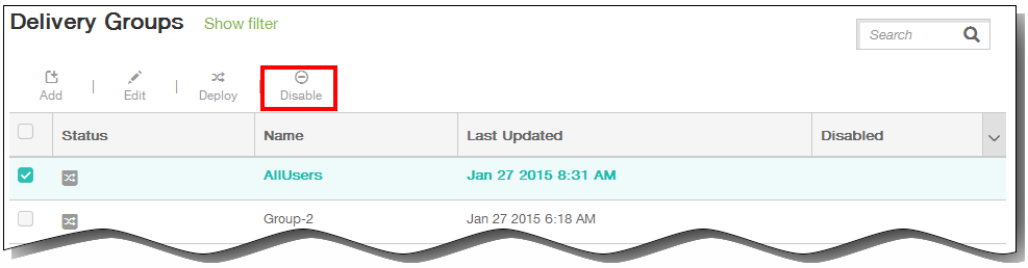


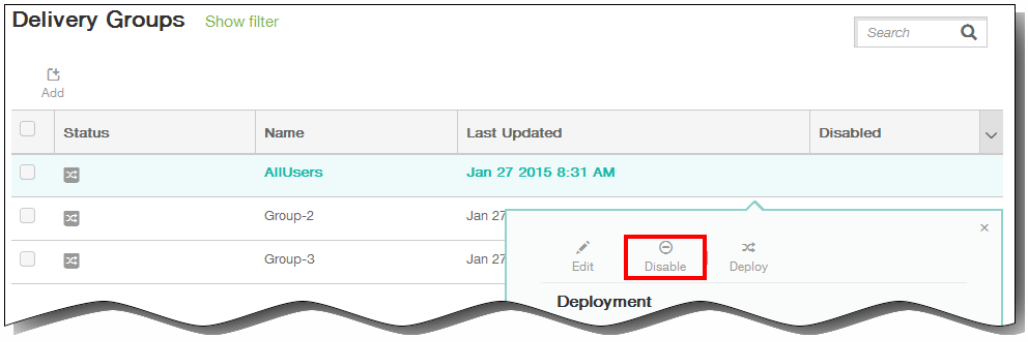
8. ［Summary］ページで、変更した内容を確認します。 構成の調整が必要な場合は、［Back］をクリックして前のページに戻ります。
9. ［Save］をクリックして変更を保存します。

AllUsersデリバリーグループを有効化および無効化するには

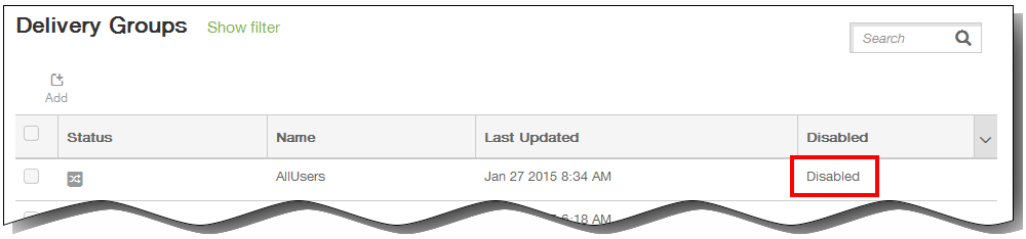
注：AllUsersは、有効化または無効化することができる唯一のデリバリーグループです。

1. ［Delivery Groups］ページで、［AllUsers］の横にあるチェックボックスをオンにするか、［AllUsers］を含む行をクリックして、AllUsersデリバリーグループを選択します。 次に、以下のいずれかを行います。
   注：［AllUsers］を選択した方法に応じて、AllUsersデリバリーグループの上または右側に［Enable］または［Disable］コマンドが表示されます。





- AllUsersデリバリーグループを無効化するには、［Disable］をクリックします。このコマンドは、［AllUsers］が有効（デフォルト）になっている場合にのみ使用できます。
  デリバリーグループの表の［Disabled］の見出しの下に、［Disabled］が表示されます。



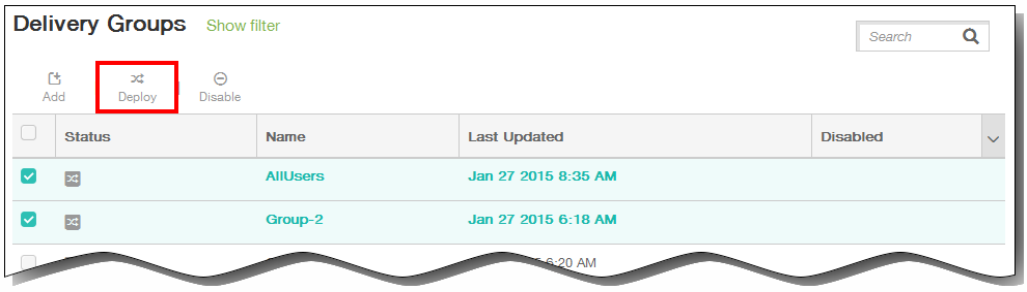
- AllUsersデリバリーグループを有効化するには、［Enable］をクリックします。このコマンドは、［AllUsers］が現在無効になっている場合にのみ使用できます。
  デリバリーグループの表の［Disabled］の見出しの下の［Disabled］の表示が消えます。

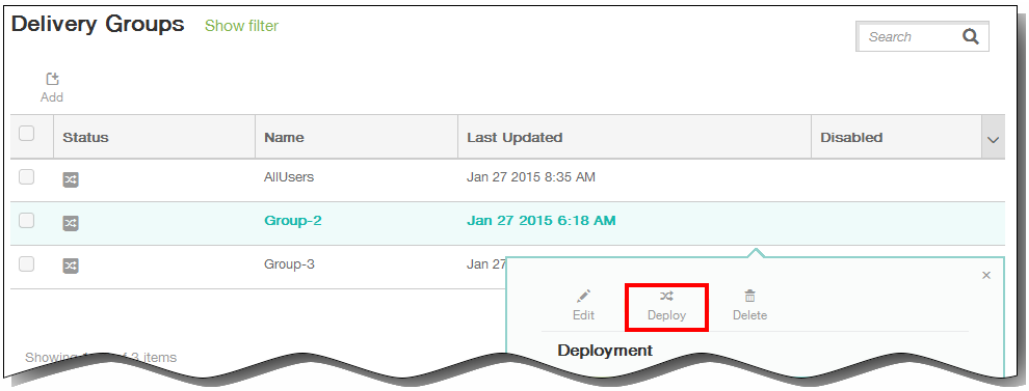
デリバリーグループに展開するには

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 8.1、Windows 8.1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。

注：ユーザーのAndroidデバイスで、Worx Storeの［Updated Available］の一覧に更新されたアプリケーションが表示されるようにするには、最初にアプリケーションインベントリポリシーをユーザーのデバイスに展開しておく必要があります。

1. ［Delivery Groups］ページで、次のいずれかを行います。
   - 複数のデリバリーグループ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. ［Deploy］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[Deploy］コマンドが表示されます。



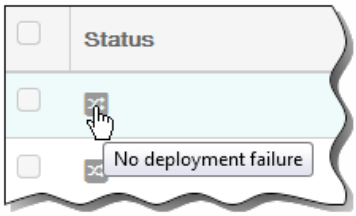


［Deploy Devices］ダイアログボックスが開きます。

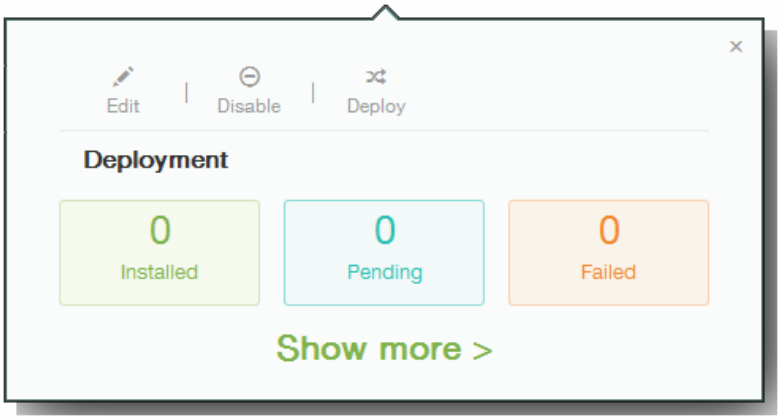
3. アプリケーション、ポリシー、アクションを展開するグループが一覧にあることを確認して、［Deploy］をクリックします。 デバイスプラットフォームとスケジュール設定ポリシーに基づいて、選択したグループにアプリケーション、ポリシー、アクションが展開されます。

［Delivery Groups］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［Status］の見出しの下で、展開エラーを示す展開アイコンを確認します。



- デリバリーグループを含む行をクリックし、［Installed］（インストール済み）、［Pending］（保留中）、［Failed］（失敗）の展開を示すオーバーレイを表示します。



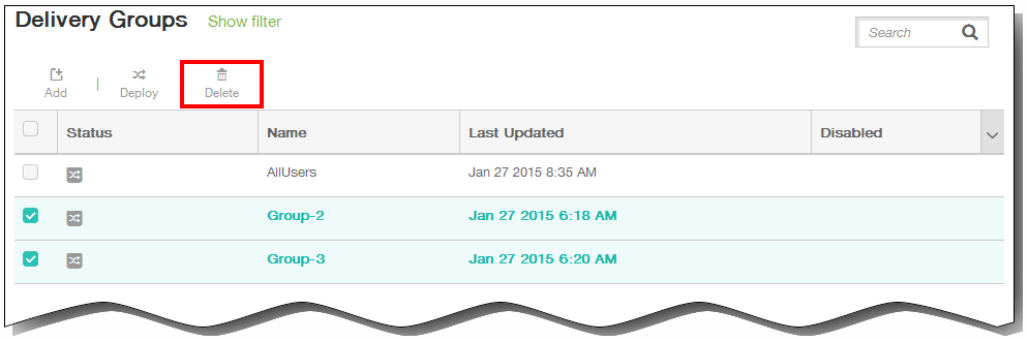
デリバリーグループを削除するには

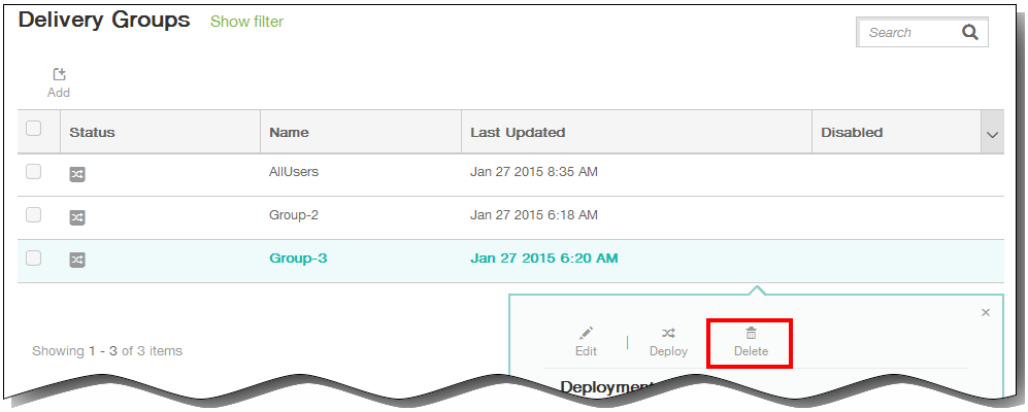
注：AllUsersデリバリーグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

1. ［Delivery Groups］ページで、次のいずれかを行います。
   - 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。

- 1つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行をクリックします。

2. ［Delete］をクリックします。
注：1つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に[Delete］コマンドが表示されます。





［Delete］ダイアログボックスが開きます。

3. ［Delete］ダイアログボックスで［Delete］をクリックします。
重要：このアクションを元に戻すことはできません。

ユーザーとデバイスの登録

May 10, 2016

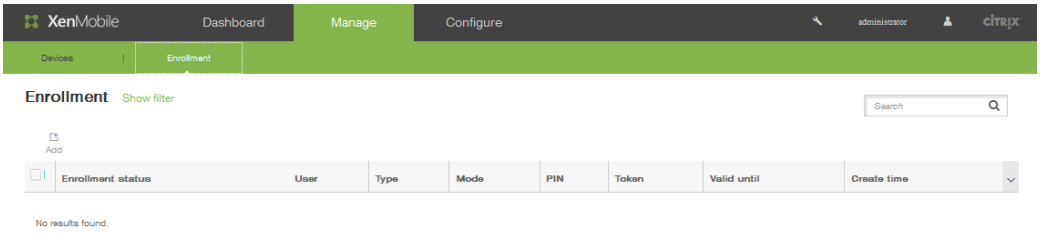
ユーザーデバイスをリモートで安全に管理するには、ユーザーデバイスをXenMobileに登録する必要があります。XenMobile クライアントソフトウェアがユーザーデバイスにインストールされ、ユーザーのIDが認証され、XenMobileとユーザーのプ ファイルがインストールされます。デバイスの登録後、XenMobileコンソールで、ポリシーの適用、アプリケーションの展開、データのデバイスへのプッシュ、紛失または盗難されたデバイスのロック、ワイプ、および捜索などのデバイス管理タスクを実行できます。

ユーザーを登録するには、Active Directory接続をまだ確立していない場合はまずユーザーをXenMobileに追加する必要があります。このセクションのトピックでは、ユーザーの登録に必要なこれ以降の手順について説明します。

- 登録モードの構成（デフォルト、SHP）。
- 通知サーバーの構成（SMTPおよびSMS）。
- 登録通知テンプレートの構成。
- 登録通知の送信。

注：iOSデバイスユーザーを登録する前に、APNS証明書を要求する必要があります。詳しくは、「XenMobileでの証明書」を参照してください。

ユーザーとデバイスの構成オプションにアクセスするには、XenMobileコンソールで[**Manage**]の[**Enrollment**]をクリックします。



Androidデバイス

May 10, 2016

1. AndroidデバイスでGoogle PlayストアまたはAmazonアプリストアに移動して、Citrix Worx Homeアプリケーションをダウンロードしてからアプリケーションをタップします。
2. インストールを求めるメッセージが表示されたら、［次へ］をクリックし、［インストール］をクリックします。
3. インストールが完了したら、［開く］をタップします。
4. 会社の資格情報（組織のXenMobileサーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールアドレスなど）を入力し、［次へ］をクリックします。
5. ［デバイス管理者を有効にしますか］画面で、［有効にする］をタップします。
6. 会社のパスワードを入力し、［サインオン］をタップします。
7. XenMobileの構成方法によっては、Worx PINの作成を求められる場合があります。Worx PINは、Worx Homeやそのほかのworx準拠アプリ（WorxMail、WorxWeb、ShareFileなど）へのサインオンに使用できます。 ［Worx PINの作成］画面で、6つの数字からなるPINを入力します。
8. PINを再入力します。

これでAndroidデバイスが登録されました。Worx Storeをタップして、コーポレートアプリストアやWorx準拠アプリ（WorxMail、WorxWeb、ShareFileなど）にアクセスできます。

Androidデバイスを登録解除および再登録するには

Updated: 2015-02-12

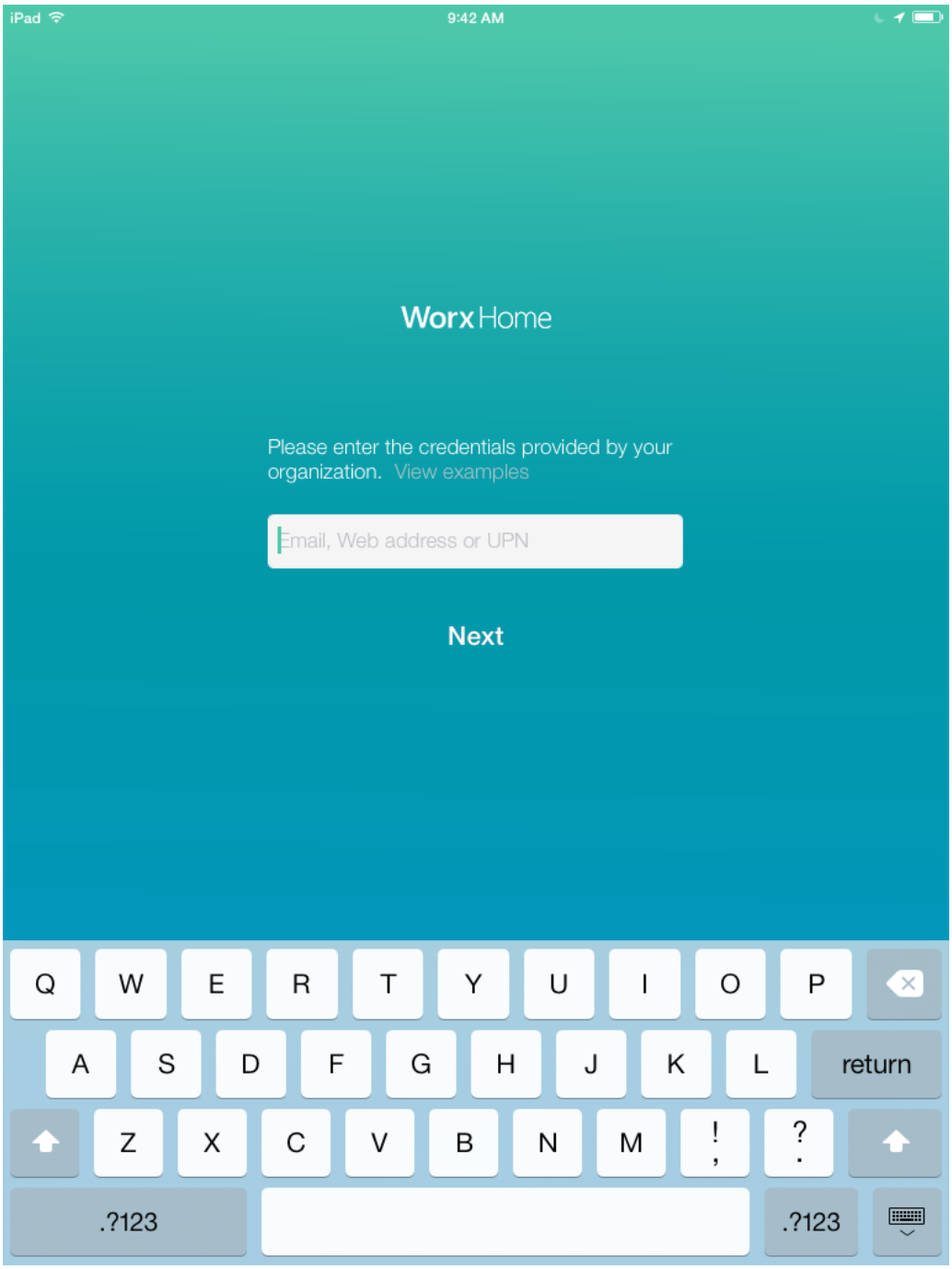
デバイスを再登録する前に、そのデバイスの登録がまず解除されます。登録が解除されてから再登録されるまでの間、そのデバイスはXenMobileコンソールのデバイスインベントリー一覧には表示されますが、XenMobileで管理されなくなります。デバイスがXenMobileで管理されていない間は、そのデバイスを追跡したり、デバイスのコンプライアンスを監視したりすることができません。

1. Worx Homeアプリケーションをタップして開きます。
2. アプリケーションウィンドウの左上にある［設定］アイコンをタップします。
3. ［Re-Enroll］をタップします。 デバイスの再登録を確認するメッセージが表示されます。
4. ［OK］をタップします。 これにより、デバイスの登録が解除されます。
5. 画面の指示に従って、デバイスを再登録します。

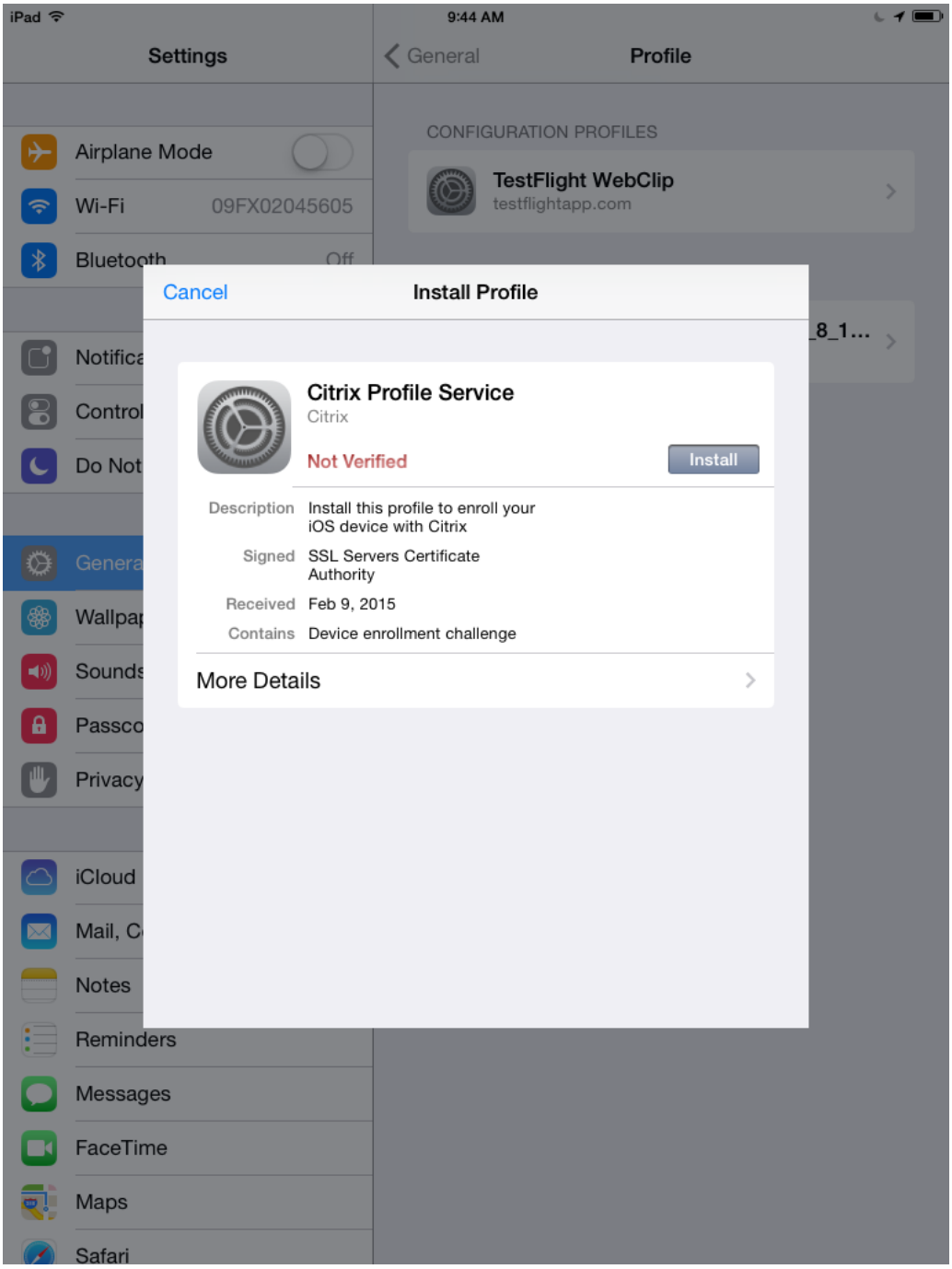
iOSデバイス

May 10, 2016

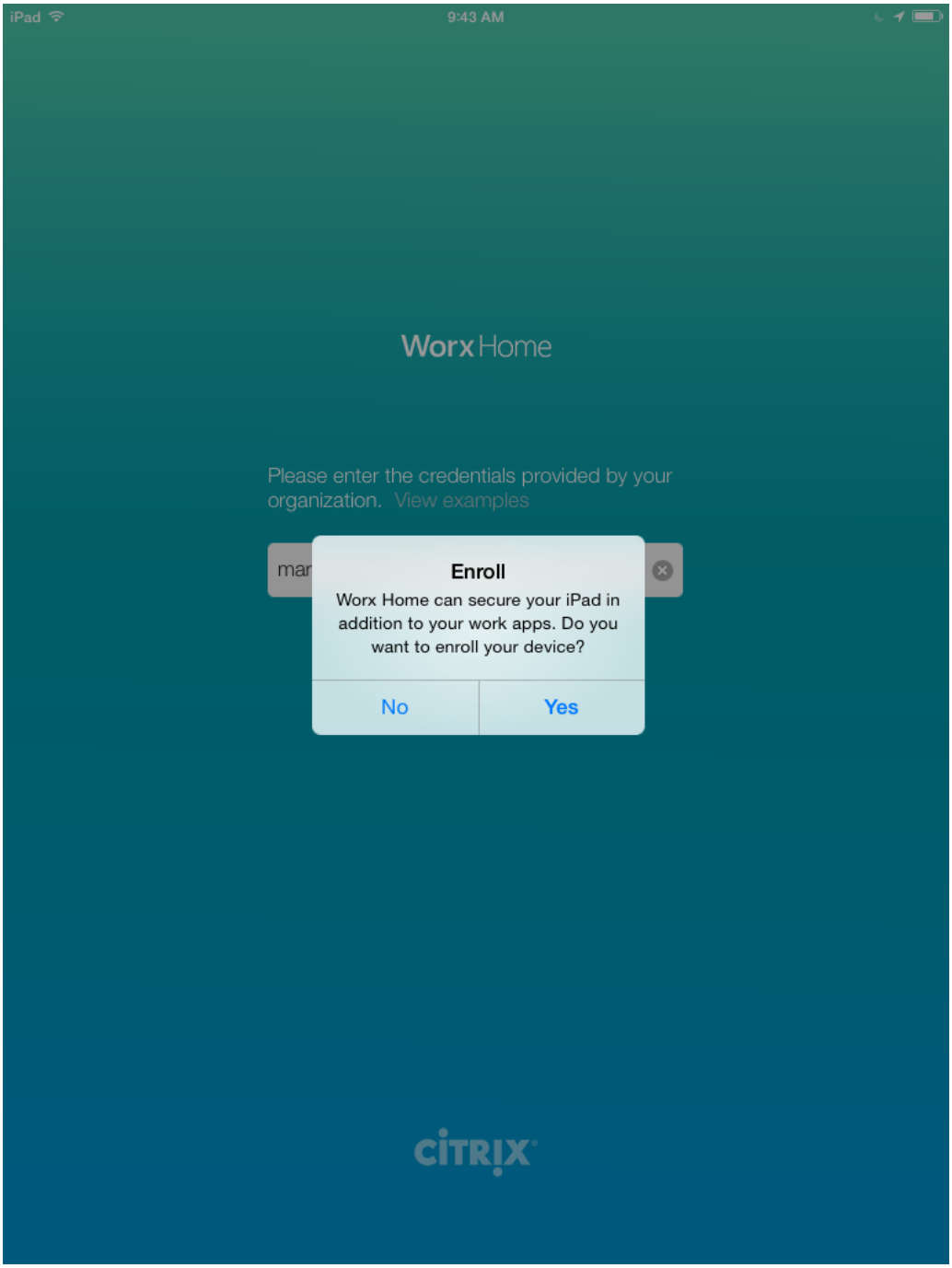
1. Worx Homeアプリをデバイスのapple iTunes App Storeからダウンロードした後、アプリをデバイスにインストールします。
2. iOSデバイスのホーム画面で、Worx Homeアプリをタップします。
3. Worx Homeアプリが開いたら、会社のXenMobileサーバー名、ユーザープリンシパル名（User Principal Name：UPN）、メールなどの会社の資格情報を入力し、［次へ］をクリックします。



4. ユーザー名とパスワードを入力します。 ブラウザーが起動して登録処理が開始されます。
5. ［インストール］をタップして、Citrix Profileサービスをインストールします。



6. 警告メッセージのプロンプトが表示される場合は、［インストール］をタップします。
7. デバイスにパスコードが構成されている場合、プロファイルをインストールするにはパスコードの入力を求められます。
8. ［インストール］をタップします。
9. プロファイルのインストールが終了したら、［完了］をタップして会社のプロファイルのインストールプロセスを完了します。
10. Worx Homeが表示されたら、［はい］をタップして、Worx Homeが現在の場所を使用できるようにします。



11. XenMobileの構成方法によっては、Worx PINの作成を求められる場合があります。Worx PINは、Worx Homeやそのほかの Worx準拠アプリ（WorxMail、WorxWeb、ShareFileなど）へのサインオンに使用できます。 Worx PINは2回入力する必要があります。 Worx Homeが開きます。 その後、Worx Storeにアクセスし、iOSデバイスにインストールできるアプリを確認することができます。
12. ［Worx Store］をタップし、企業アプリストアを開きます。
13. 登録の後でアプリをユーザーデバイスに自動的にプッシュするようにXenMobileを構成している場合は、アプリのインストールを求めるメッセージがユーザーに表示されます。 ［インストール］をタップしてアプリをインストールします。

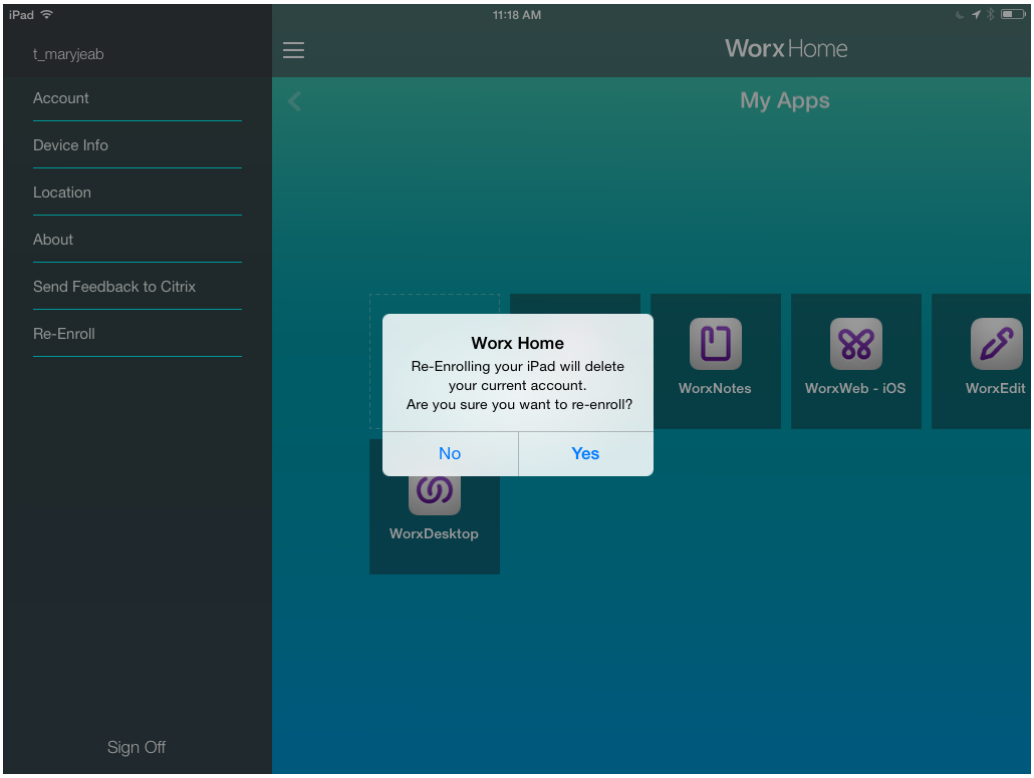
iOSデバイスを再登録するには

Updated: 2015-02-13

デバイスを再登録する場合、そのデバイスの登録がまず解除されます。登録が解除されてから再登録されるまでの間、そのデ

バイスはXenMobileコンソールのデバイスインベントリー覧には表示されますが、XenMobileで管理されなくなります。デバイスがXenMobileで管理されていない間は、そのデバイスを追跡したり、デバイスのコンプライアンスを監視したりすることができません。

1. Worx Homeアプリケーションをタップして開きます。
2. アプリケーションウィンドウの左上にある［設定］アイコンをタップします。
3. ［再登録］をタップします。 デバイスの再登録を確認するメッセージが表示されます。



4. ［はい］をタップします。 これにより、デバイスの登録が解除されます。
5. 画面の指示に従って、デバイスを再登録します。

XenMobileへのWindowsデバイスの登録

May 10, 2016

XenMobileは、以下のWindowsオペレーティングシステムを実行しているデバイスの登録をサポートしています。

- Windows
- Windows Phone

WindowsおよびWindows Phoneのユーザーはデバイスから直接登録します。

ユーザー登録のため自動検出を構成して、WindowsおよびWindows Phoneデバイスの管理を有効にする必要があります。

> ## 注意
>
> Windowsデバイスを登録するには、SSLリスナー証明書が公開証明書である必要があります。 自己署名SSL証明書をアップロード済みの場合、登録が失敗します。

自動検出なしでWindows 8.1デバイスを登録するには

ユーザーは、Windows RT 8.1、およびWindows 8.1 ProとWindows 8.1 Enterprise（32ビットと64ビット）の両方を実行しているデバイスを登録できます。Windows 8.1デバイスの管理を有効にするには、自動検出を構成することをお勧めします。詳しくは、「ユーザー登録のためにXenMobileで自動検出を有効にするには」を参照してください。

1. デバイスで使用可能なWindows Updateをすべて確認し、インストールします。 この手順は、Windows 8からWindows 8.1にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。
2. チャームメニューで［設定］をタップし、［PC設定の変更］、［ネットワーク］、［社内ネットワーク］の順にタップします。
3. 会社のメールアドレスを入力し、［オンにする］をタップします。 ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します（例：foo@mydomain.com）。これによって既知のMicrosoftの制限を回避できます。［Connecting to a service］ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。デバイスがXenMobileサーバーを自動的に検出し、登録処理が開始されます。
4. パスワードを入力します。 XenMobileのユーザーグループのメンバーであるアカウントに関連付けられたパスワードを使用します。
5. デバイスの管理に同意することを通知する［IT管理者によるアプリやサービスの管理を許可する］ダイアログボックスで、［オンにする］をタップします。

自動検出なしでWindows 8.1デバイスを登録するには

自動検出なしでWindows 8.1デバイスを登録することができます。しかし、自動検出を構成するようお勧めします。自動検出なしで登録すると希望するURLに接続する前にポート80を呼び出すことになるため、実稼働環境でのベストプラクティスとはみなせません。このような処理は、テスト環境や概念実証展開でのみ使用するようにしてください。

1. デバイスで使用可能なWindows Updateをすべて確認し、インストールします。 この手順は、Windows 8からWindows 8.1にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。
2. チャームメニューで［設定］をタップし、［PC設定の変更］、［ネットワーク］、［社内ネットワーク］の順にタップします。
3. 会社のメールアドレスを入力します。
4. ［サーバーアドレスを自動検出する］がオンになっている場合、タップしてオフにします。

5. ［サーバーの入力］アドレスフィールドに、「https://*serverfqdn:8443/serverInstance*/Discovery.svc」という形式でサーバーアドレスを入力します。未認証のSSL接続に8443以外のポートが使用される場合、このアドレスの8443の箇所にそのポート番号を指定します。
6. パスワードを入力します。
7. デバイスの管理に同意することを通知する［IT管理者によるアプリやサービスの管理を許可する］ダイアログボックスで、［オンにする］をタップします。

Windows Phone 8.1デバイスを登録するには

Updated: 2015-2-11

XenMobileでWindows Phone 8.1デバイスを登録するには、ユーザーはActive Directoryまたは内部ネットワークのメールアドレスおよびパスワードを入力する必要があります。自動検出がセットアップされていない場合、ユーザーはXenMobileサーバーのサーバーWebアドレスも必要です。以下の手順に従って、デバイスを登録します。

注：Windows Phoneの業務用ストアを介してアプリケーションを展開する場合は、ユーザーが登録する前に、（署名済みのCitrix Worx Home Windows Phone 8アプリケーションを使って）Enterprise Hubポリシーを構成します。

1. Window 8.1 Phoneのメイン画面で［設定］アイコンをタップします。
2. ［ワークスペース］をタップします。
3. ［ワークスペース］画面で、［アカウントを追加］をタップします。
4. 次の画面でメールアドレスとパスワードを入力し、［サインイン］をタップします。 ドメインに自動検出が構成されている場合、以降のいくつかの手順で求められる情報は自動的に抽出されます。 手順8.に進みます。 ドメインに自動検出が構成されていない場合、次の手順に進みます。 ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します（例：foo@mydomain.com）。これによって既知のMicrosoftの制限を回避できます。［Connecting to a service］ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。
5. 次の画面でXenMobileサーバーのWebアドレスを、「https://://wpe」のように入力します。 たとえば、https://mycompany.mdm.com:8443/zdm/wpeなどです。 注：実際の実装に合わせてポート番号を選択する必要がありますが、iOSの登録に使用したポートと同じポートを使用してください。
6. ユーザー名とドメインを介して認証が検証される場合、ユーザー名とドメインを入力し、次に［サインイン］をタップします。
7. 証明書に関する問題を通知する画面が表示された場合、そのエラーは自己署名入り証明書の使用が原因です。 サーバーが信頼できる場合、［続行］をタップします。 信頼できない場合は、［キャンセル］をタップします。
8. アカウントを追加すると、［業務用アプリをインストール］というオプションが表示されます。 管理者が業務用アプリストアを構成済みの場合、このオプションをオンにして、［完了］をタップします。 このオプションをクリアした場合、業務用アプリストアを受信するには、再登録が必要になります。
9. ［アカウントが追加されました］画面で［完了］をタップします。
10. サーバーへの接続を強制的に実行するには、［最新の情報に更新］アイコンをタップします。 デバイスを手動でサーバーに接続できない場合、XenMobileは再接続を試行します。 XenMobileは3分ごとに5回連続でデバイスに接続し、その後は2時間ごとに接続します。この接続頻度は、［Server properties］にある［Windows WNS Heartbeat Interval］で変更できます。登録が完了したら、Worx Homeはバックグラウンドで登録を実行します。インストールが完了してもそれについては何も通知されません。［すべてのアプリ］画面からWorx Homeを開きます。

Symbianデバイス

May 10, 2016

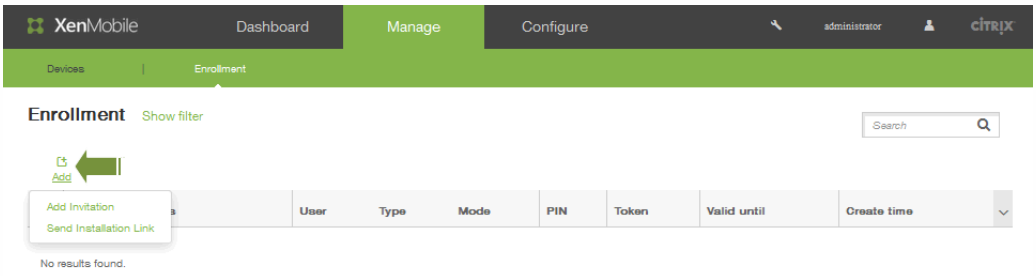
1. 組織のXenMobile Webアドレスを参照します。 Webアドレスはhttps://.domain.com//setupという形式になります。
   注：Thawte、VeriSignなど、信頼される認証機関が発行した証明書がある場合のみ、HTTPSプレフィックスを使用できます。
2. ［Install］画面で［OK］をタップします。
3. XenMobileエージェントのインストール先として、［Phone Memory］をタップします。
4. インストールが完了したら、［Yes］をタップして、XenMobileを開きます。
5. ［Security Details］画面で［OK］をタップし、XenMobileから電話へのアクセスを許可します。
6. サーバーコードの最初の4桁を「2831」と入力し、［OK］をタップします。
7. ［Control Request Accepted］画面で［OK］をタップします。
8. XenMobileサーバーのユーザー名とパスワード、サーバー名、ポート、インスタンス名を入力し、［OK］をタップします。 接続情報が表示されます。
9. ［Options］をタップしてサーバーの接続詳細情報を確認し、［Close］をタップしてセットアップを終了します。

XenMobileでの登録招待状の送信

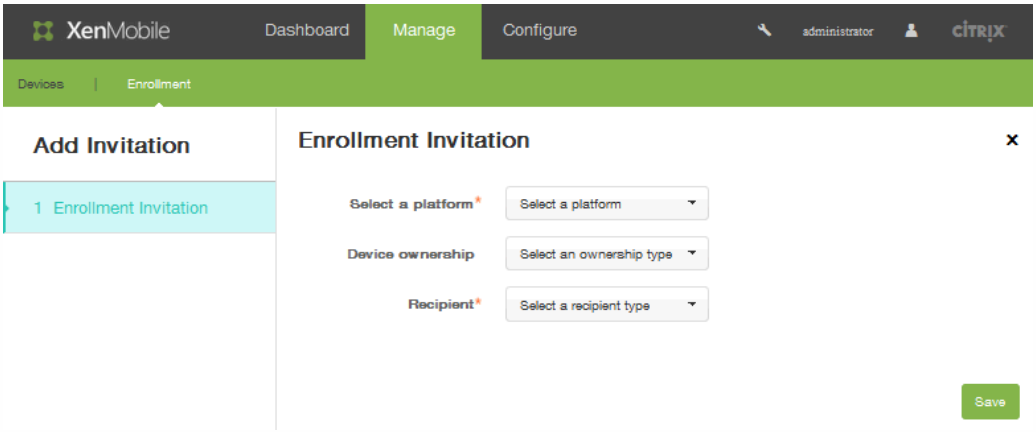
May 10, 2016

XenMobileコンソールで、iOSデバイスおよびAndroidデバイスを使用しているユーザーに登録招待状を送信できます。

1. XenMobileコンソールで、［Manage］の［Enrollment］をクリックします。
2. ［Enrollment］画面で、［Add］をクリックします。 招待状の追加またはインストールリンクの送信を行うオプションを示すメニューが表示されます。



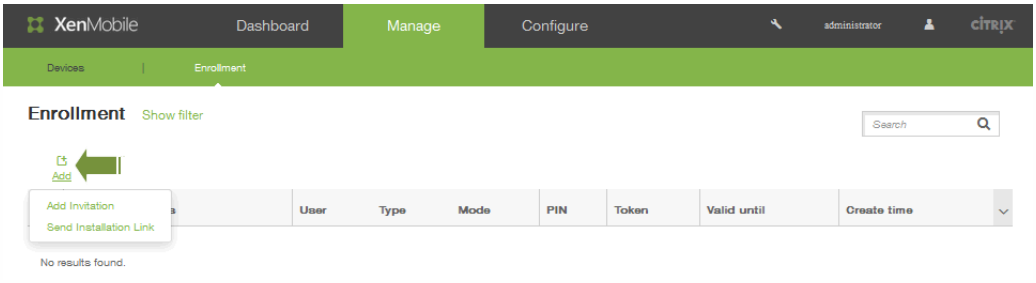
3. ［Add Invitation］をクリックします。 ［Enrollment Invitation］画面が開きます。



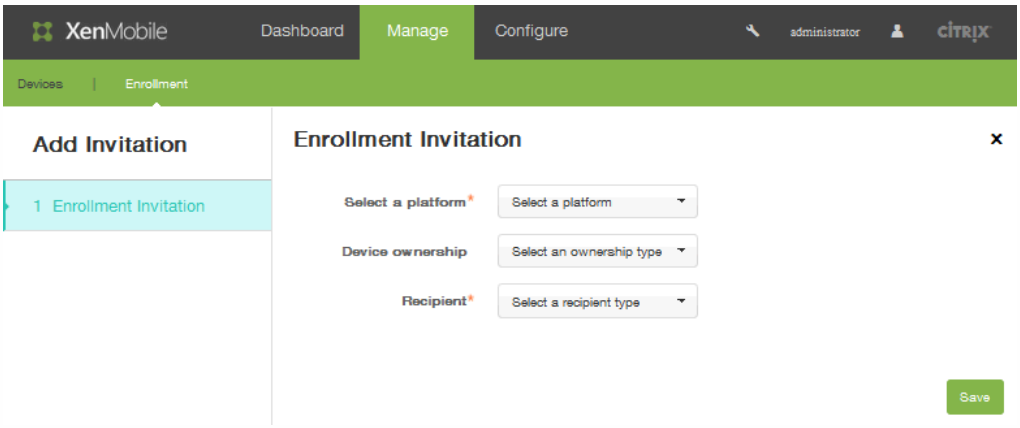
4. ［Select a platform］の一覧から、［iOS］または［Android］を選択します。
5. ［Device ownership］の一覧から、［Corporate］または［Employee］を選択します。
6. ［Recipient］の一覧から、［User］または［Group］を選択します。 ユーザーを受信者として選択すると、インターフェイスが変わり、追加の構成オプションが表示されます。以下のトピックの手順に従って、選択した受信者の種類に応じた招待状設定を完了します。

登録招待状をユーザーに送信するには

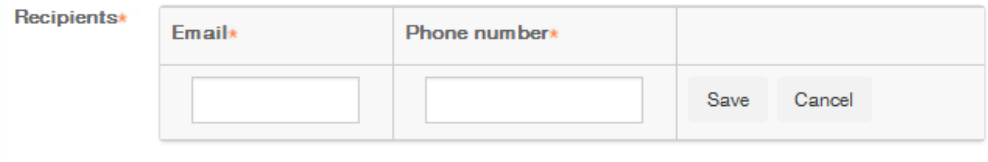
1. XenMobileコンソールで、［Manage］の［Enrollment］をクリックします。
2. ［Enrollment］画面で、［Add］をクリックします。 招待状の追加またはインストールリンクの送信を選択できるメニューが表示されます。



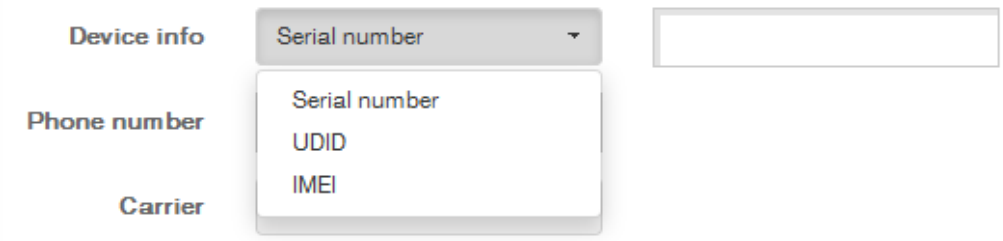
3. ［Add Invitation］をクリックします。 ［Enrollment Invitation］画面が開きます。



4. ［Select a platform］の一覧から、［iOS］または［Android］を選択します。
5. ［Device ownership］の一覧から、［Corporate］または［Employee］を選択します。
6. ［Recipient］の一覧から、［User］を選択します。 インターフェイスが変わり、ユーザー登録関連の構成オプションが表示されます。



7. ［User name］にユーザー名を入力します。 ユーザーは、XenMobileサーバーのローカルユーザー、またはActive Directoryのユーザーとして存在している必要があります。ローカルユーザーの場合、通知を送信するため、ユーザーの電子メールプロパティが設定されていることを確認します。Active Directoryユーザーの場合、LDAPが構成されていることを確認します。
8. ［Device info］の一覧から、［Serial number］、［UDID］、［IMEI］のいずれかを選択します。 オプションを選択すると、インターフェイスが変わり、デバイスに応じて値を入力できるフィールドが表示されます。

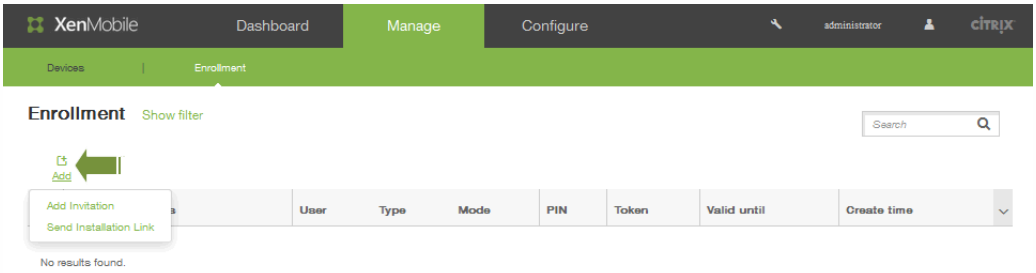


9. ［Phone number］に、オプションでユーザーの電話番号を入力します。
10. ［Carrier］の一覧から、ユーザーの電話番号を関連付ける電話会社を選択します。

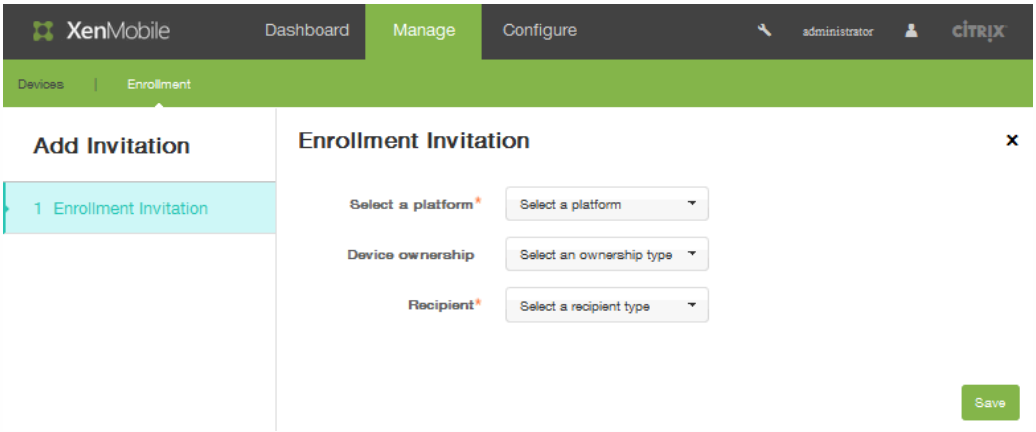
11. ［Enrollment mode］の一覧から、［User name + Password］（デフォルト）、［High Security］、［Invitation URL］、［Invitation URL + PIN］、［Invitation URL + Password］、［Two Factor］、［User name + PIN］のいずれかを選択します。
12. ［Template for agent download］の一覧では、プラットフォームの種類に基づいてオプションが決まります。 たとえば、手順1でプラットフォームとして［iOS］を選択した場合、オプションとして［iOS Download Link］が表示されます。
13. ［Template for enrollment URL］の一覧から、［Enrollment Invitation］を選択します。
14. ［Template for enrollment confirmation］の一覧から、［Enrollment Confirmation］を選択します。 登録招待状は一定期間が過ぎると期限切れになります。［Expire after］フィールドは、登録の期限を示します。［Maximum Attempts］フィールドは、登録処理を行う回数の上限を示します。
15. ［Send invitation］で、［ON］をクリックします。
16. ［Save］をクリックします。

登録招待状をグループに送信するには

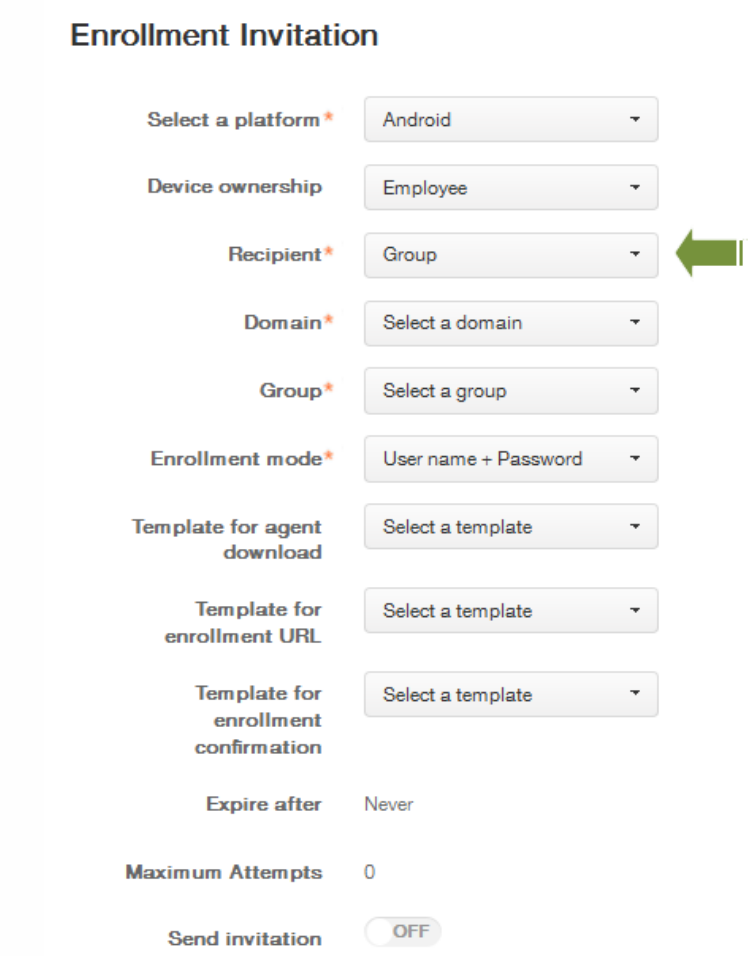
1. XenMobileコンソールで、［Manage］の［Enrollment］をクリックします。
2. ［Enrollment］画面で、［Add］をクリックします。 招待状の追加またはインストールリンクの送信を選択できるメニューが表示されます。



3. ［Add Invitation］をクリックします。 ［Enrollment Invitation］画面が開きます。



4. ［Select a platform］の一覧から、［iOS］または［Android］を選択します。
5. ［Device ownership］の一覧から、［Corporate］または［Employee］を選択します。
6. ［Recipient］の一覧から、［Group］を選択します。 インターフェイスが変わり、グループ登録の構成オプションが表示されます。

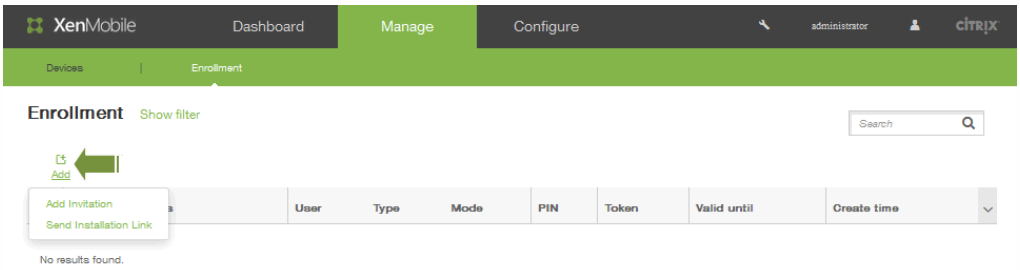


7. ［Domain］で、受信者のグループが存在するドメインを選択します。
8. ［Group］で、登録通知を送信するグループを選択します。
9. ［Enrollment mode］の一覧から、［User name + Password］（デフォルト）、［High Security］、［Invitation URL + PIN］、［Invitation URL + Password］、［Two Factor］、［User name + PIN］のいずれかを選択します。
10. ［Template for agent download］の一覧では、プラットフォームの種類に基づいてオプションが決まります。 たとえば、手順1.で［iOS］を選択した場合は、［iOS Download Link］がオプションとして表示されます。
11. ［Template for enrollment URL］の一覧から、［Enrollment Invitation］を選択します。
12. ［Template for enrollment confirmation］の一覧から、［Enrollment Invitation］を選択します。 登録招待状は一定期間が過ぎると期限切れになります。［Expire after］フィールドは、登録の期限を示します。［Maximum Attempts］フィールドは、登録処理を行う回数の上限を示します。
13. ［Send invitation］で［ON］をクリックすると、選択したグループに登録招待状が送信されます。
14. ［Save］をクリックします。

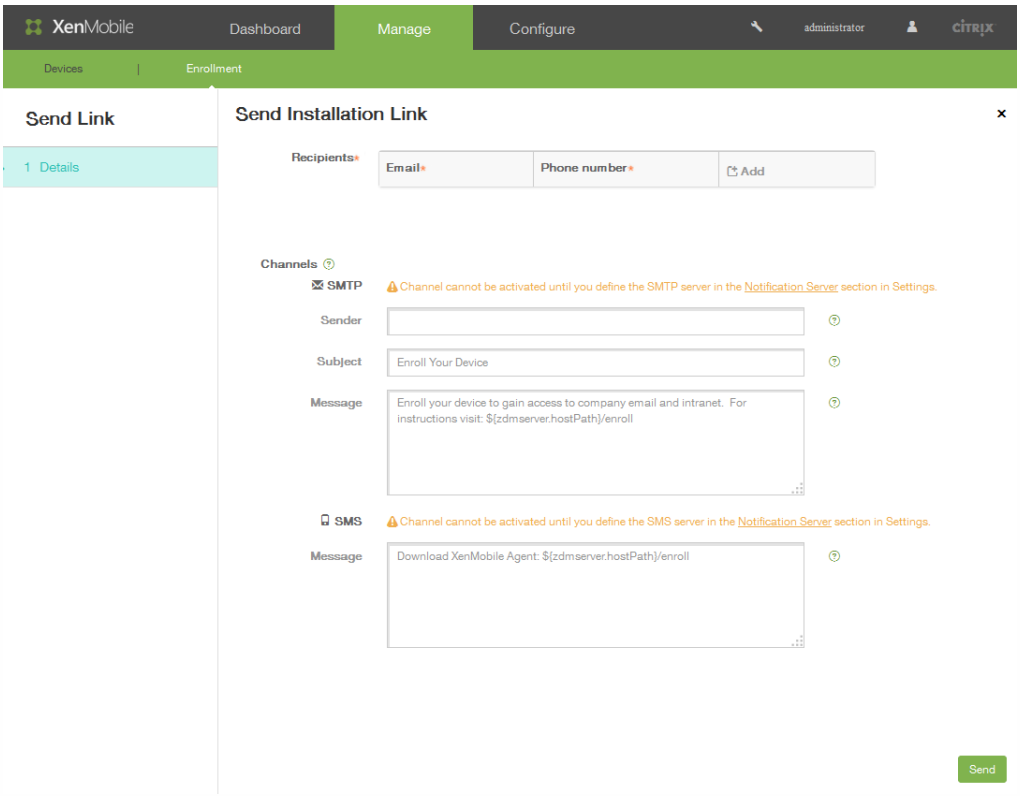
登録インストールリンクを送信するには

登録インストールリンクを送信する前に、通知サーバー（［Configure］、［Settings］、［Notification Server］の順にクリックします）でチャネル（SMTPまたはSMS）を構成する必要があります。詳しくは、「XenMobileでの通知」を参照してください。

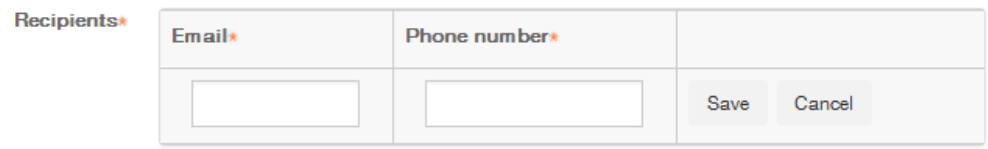
1. XenMobileコンソールで、［Manage］の［Enrollment］をクリックします。
2. ［Enrollment］画面で、［Add］をクリックします。 招待状の追加またはインストールリンクの送信を選択できるメニューが表示されます。



3. ［Send Installation Link］をクリックします。 インターフェイスが変わり、［Send Installation Link］オプションが表示されます。



4. ［Recipient］で、［Add］をクリックして、インストール登録リンクの送信先の受信者を指定します。 ［Recipient］フィールドが展開され、メールアドレスと電話番号を追加できます。



5. ［Email］ボックスに、登録招待状リンクを受け取るユーザーのメールアドレスを、［Phone number］ボックスにそのユーザーの電話番号を入力します。 これらのフィールドは必須です。
6. ［Channels］で、登録インストールリンクの送信に使用する適切なチャネルを選択します。 通知はSMTPまたはSMSで送信されます。 注： ［Configure］、［Settings］、［Notification Server］の順に選択してサーバー設定を構成するまでは、これらのチャネル（SMTPまたはSMS）を有効化できません。詳しくは、「XenMobileへのアプリケーションの追加」を参照してください。
7. ［SMTP］フィールドを構成する場合は、［Sender］を指定します。 これはオプションのフィールドで、SMTPメッセー

ジの差出人フィールドで使用されます。 ここで送信者を指定しなかった場合は、［Settings］の［Notification Server］フィールドで指定されている値が使用されます。

8. SMTP通知の場合、オプションで［Subject］を指定します。 たとえば、「enroll your device」などです。
9. 受信者へ送信されるメッセージの内容として使用する［Message］を指定します。 たとえば、「Enroll your device to gain access to company email and intranet.」などです。
10. 通知をSMSで送信するには、受信者へ送信されるメッセージを入力します。 SMSベースの通知の場合、このフィールドは必須です。 **注**：北米の場合、160文字を超えるSMSメッセージは複数のメッセージとして配信されます。
11. ［Send］をクリックします。

> ## 注意
>
> お使いの環境でSAMAccountNameが使用されている場合、ユーザーが招待状を受け取りリンクをクリックすした後、ユーザー名を編集して認証を完了する必要があります。 たとえば、SAMAccountName@*domainname*.com.から*domainname*を削除する必要があります。

展開規則の構成

Oct 24, 2016

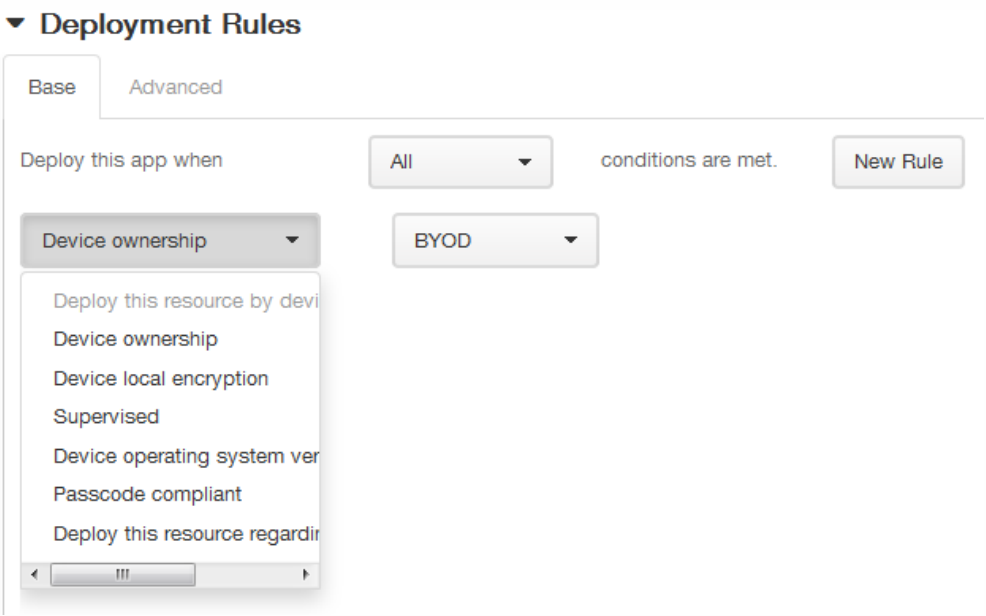
ここでは、以下の内容について説明します。

- 展開規則 - パッケージの展開結果に影響を与えるパラメーターです。
- 展開スケジュール - XenMobileからパッケージがデバイスにプッシュされるタイミングを指定するオプションです。

展開規則の構成

パッケージの展開結果に影響を与えるパラメーターを必要に応じていくつでも設定できます。

たとえば、特定のオペレーティングシステムバージョン、特定のハードウェアプラットフォーム、またはそのほかの組み合わせに基づいてパッケージを展開することができます。このウィザードには、基本的な規則エディターと高度な規則エディターが用意されています。高度な規則エディターの概観は自由形式のエディターです。次の図は、アプリケーションを追加または編集するときに使用できる［Deployment Rules］画面を示しています。



基本的な展開規則は、あらかじめ定義されたテストと、その結果のアクションで構成されています。 可能であれば、テスト例に結果があらかじめ組み込まれます。 たとえば、ハードウェアプラットフォームに基づくパッケージ展開では、既知のプラットフォームがすべて結果のテストに組み込まれ、規則の作成時間が大幅に短縮されてエラーが発生する可能性も低くなります。

［New rule］をクリックしてパッケージに規則を追加します。

注：規則ビルダーには各テストに固有の詳細情報が含まれています。

新しい規則を作成するには、規則テンプレートを選択し、条件の種類を選択して、規則をカスタマイズします。 規則のカスタマイズには説明の変更も含まれます。 設定の構成が完了したら、その規則をパッケージに追加します。

規則は、必要に応じていくつでも追加できます。 すべての規則に一致した場合にパッケージが展開されます。

[Advanced] タブをクリックすると、 **[Advanced Rule Editor]** が表示されます。

このモードでは、規則間の関係を指定できます。 使用できる演算子は、**AND**、**OR**、および**NOT**です。

展開スケジュールの構成

XenMobileでは、操作、アプリ、デバイスポリシーに対して指定する展開スケジュールを使用して、これらのアイテムの展開を制御できます。 展開が即座に実行されるか、特定の日時に実行されるか、展開条件に従って実行されるかを指定できます。 構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

展開スケジュールオプションを変更しない場合、展開は接続のたびに即座に行われます。 展開スケジュールのオプションは次のとおりです。

Deploy：デフォルトでは **[ON]** です。 展開を行わない場合は、この設定を **[OFF]** に変更します。

Deployment Schedule：デフォルトでは **[Now]** です。 展開の時間を指定するには、 **[Later]** を選択してから日付を選択し、時刻を入力します。

Deployment condition：デフォルトでは **[On every connection]** です。 展開を制限するには、この設定を **[Only when previous deployment has failed]** に変更します。

Deploy for always-on connection：デフォルトでは **[OFF]** です。 iOSおよびWindows Mobileデバイスの場合：デバイスの **[Connection Scheduling Policy]** オプションを **[Always]** に設定した場合は、 **[Deploy for always-on connections]** を **[ON]** に変更する必要があります。 Androidデバイスの場合：XenMobileの **[Background Deployment]** サーバープロパティでは、Androidデバイスに展開される各ポリシーに対して **[Deploy for always-on connections]** を **[ON]** に設定する必要があります。

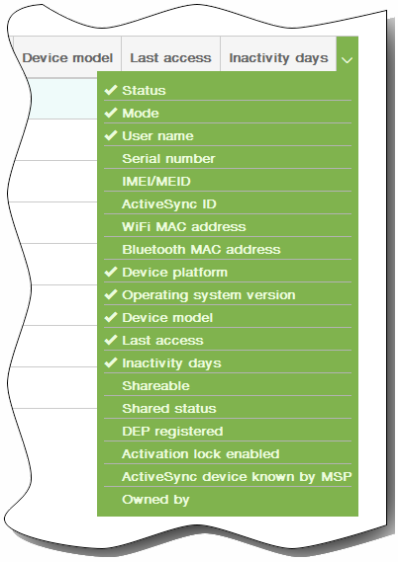
デバイスの追加およびデバイスの詳細の表示

May 10, 2016

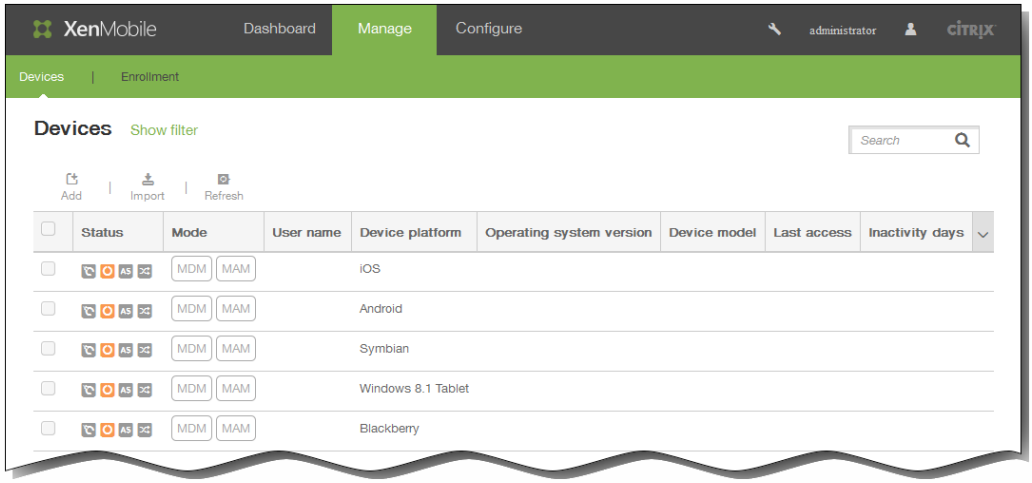
XenMobileコンソールサーバーのリポジトリデータベースには、モバイルデバイスの一覧が保存されます。各モバイルデバイスは、一意のシリアル番号またはIMEI（International Mobile Station Equipment Identity）/MEID（Mobile Equipment Identifier）識別番号のいずれか、またはその両方によって定義されます。XenMobileコンソールにデバイスを追加するには、手動でデバイスを追加するか、ファイルからデバイスの一覧をインポートします。「デバイスプロビジョニングファイル形式」を参照してください。

コンソールの［Devices］ページには、各デバイスとその情報の一覧を示す表があり、状態（ジェイルブレイクされていないデバイス、管理されていないデバイス、Active Sync Gateway使用不可、展開エラーがない）、モード（MDM、MAM）、ユーザー名、デバイスプラットフォーム、オペレーティングシステムバージョン、デバイスのモデル、最終アクセス、操作が行われていない日数が示されます。

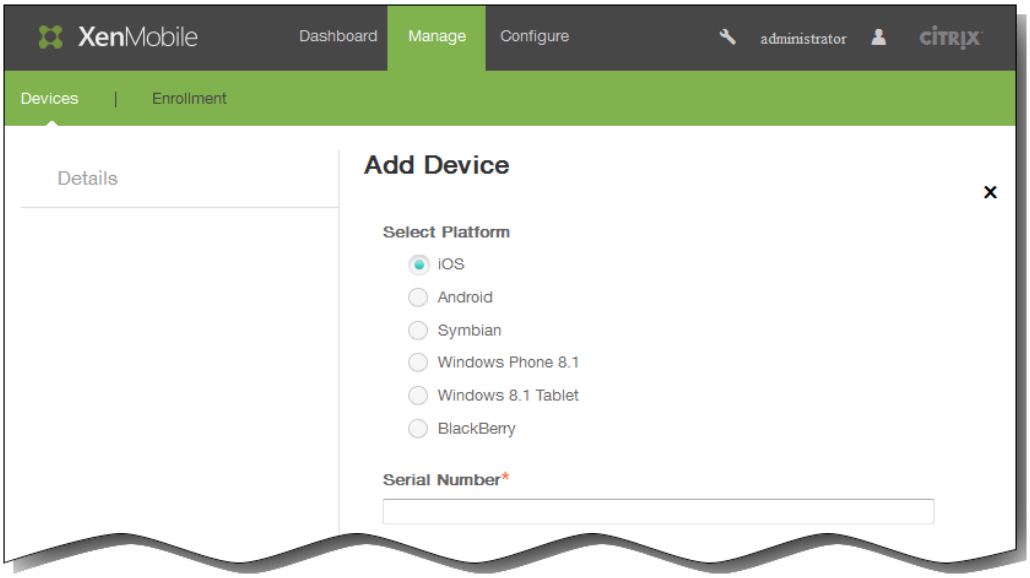
注：これらはデフォルトの見出しです。末尾の見出しの下向き矢印をクリックし、表示する見出しをオンにしたり表示しない見出しをオフにしたりして、表に示される内容をカスタマイズできます。



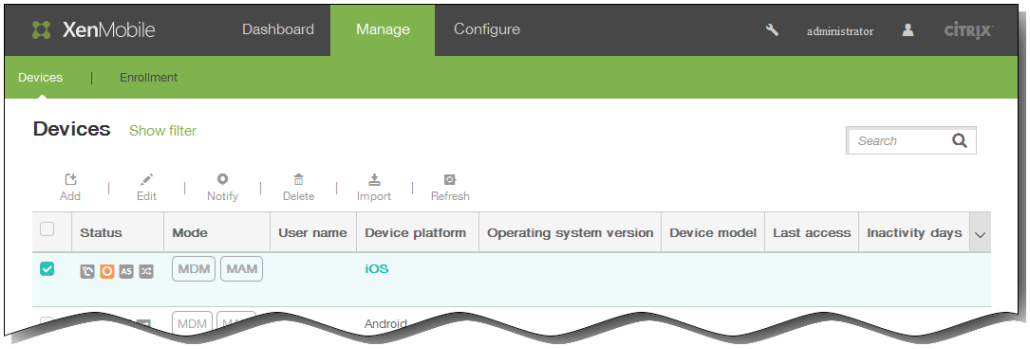
［Add］をクリックして手動で新しいデバイスを追加するか、［Import］をクリックしてプロビジョニングファイルをインポートすることができます。表を更新するには、［Refresh］をクリックします。



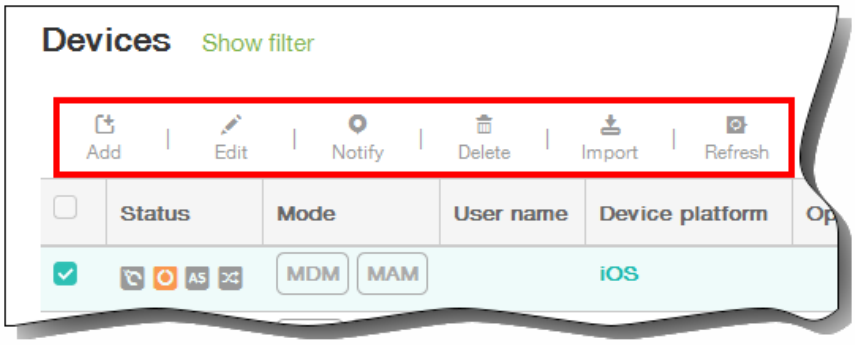
1. XenMobileコンソールで［Manage］［Devices］の順にクリックして、［Add］をクリックします。［Add Device］ページが開きます。

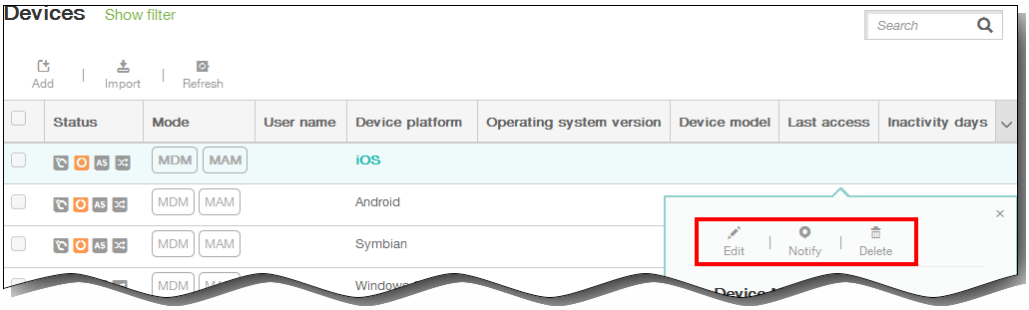


2. ［Select platform］で、［iOS］、［Android］、［Symbian］、［Windows Phone 8.1］、［Windows 8.1 Tablet］、［BlackBerry］のいずれかをクリックします。
3. 次の情報を入力します。
   1. iOS：［Serial Number］ボックスにシリアル番号を入力します。
   2. Android：［Serial Number］ボックスにシリアル番号を、［IMEI/MEID］ボックスにIMEIまたはMEIDを入力します。
   3. Symbian：［IMEI/MEID］ボックスにIMEIまたはMEIDを入力します。
   4. Windows Phone 8.1：［Serial Number］ボックスにシリアル番号を、［IMEI/MEID］ボックスにIMEIまたはMEIDを入力します。
   5. Windows 8.1 Tablet：［Serial Number］ボックスにシリアル番号を、［IMEI/MEID］ボックスにIMEIまたはMEIDを入力します。
   6. BlackBerry：［Serial Number］ボックスにシリアル番号を、［IMEI/MEID］ボックスにIMEIまたはMEIDを入力します。
4. ［Add］をクリックします。［Devices］の表に示される一覧の一番下に、追加したデバイスが表示されます。
5. 追加したデバイスを一覧で選択して表示されるメニューで［Edit］をクリックし、デバイスの詳細を表示して確認します。

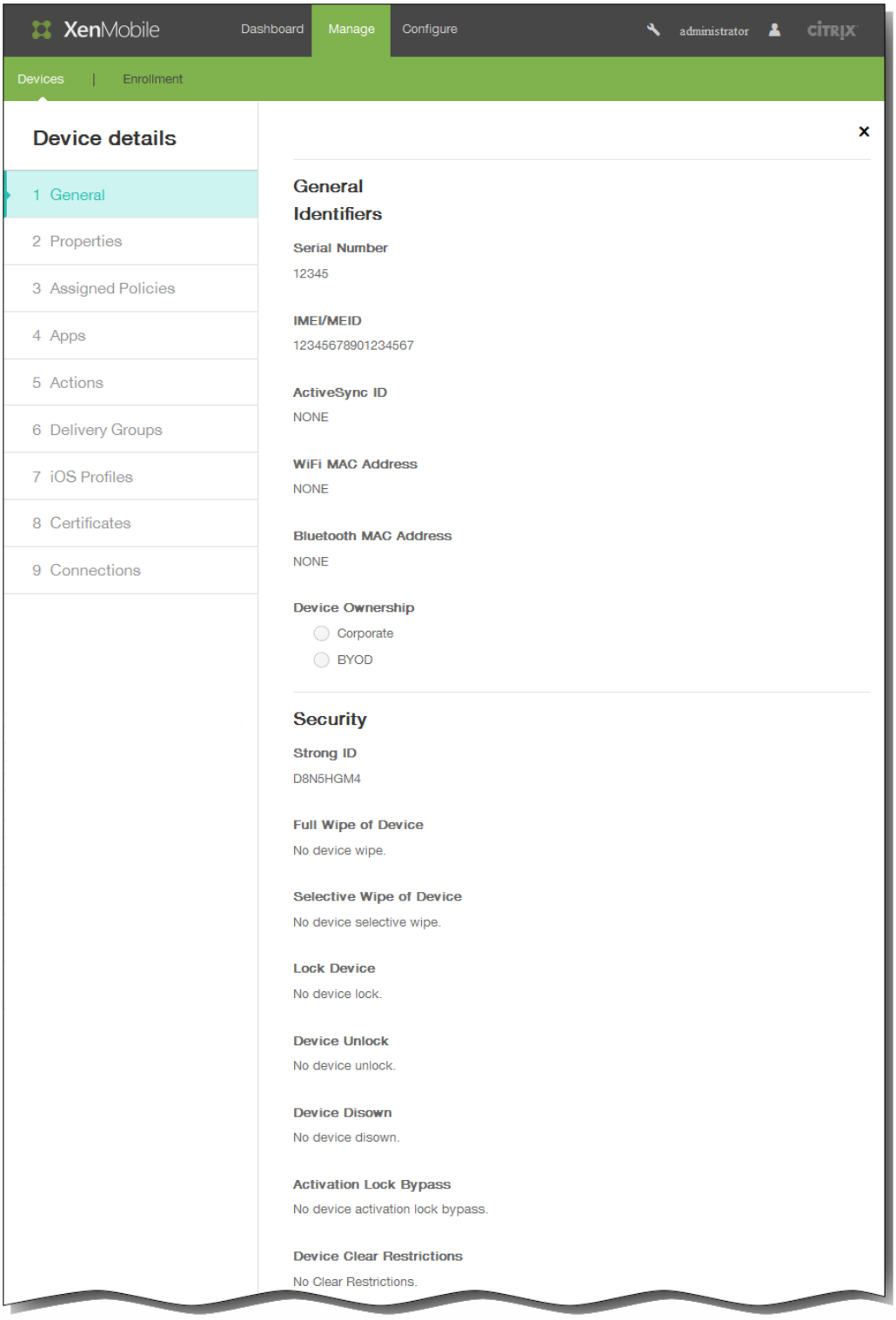


注：デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。

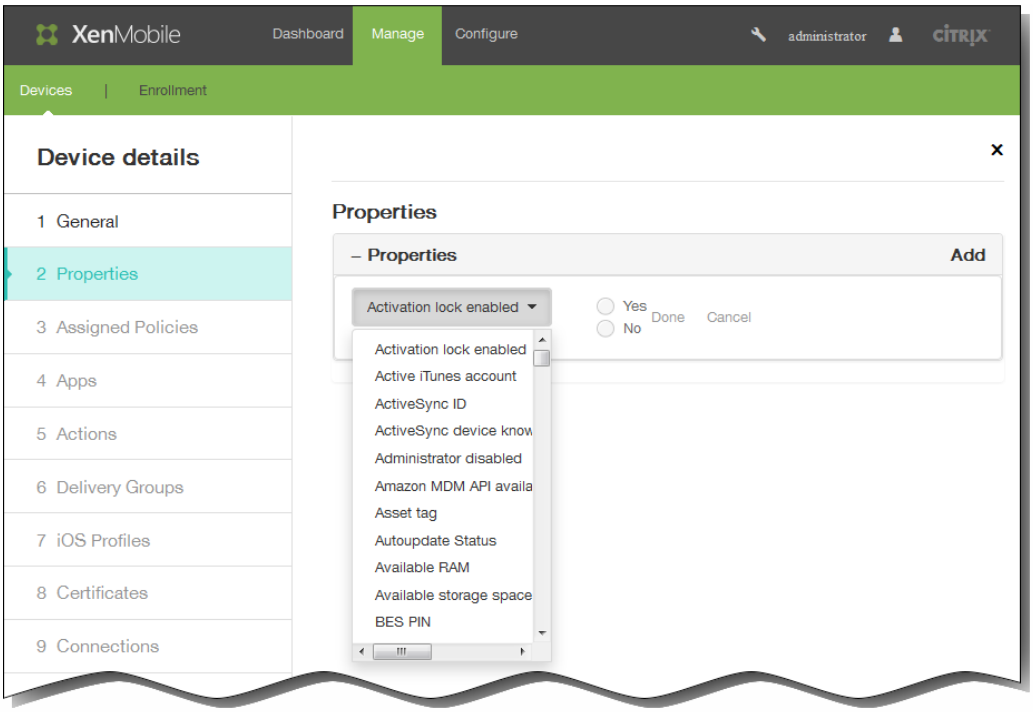




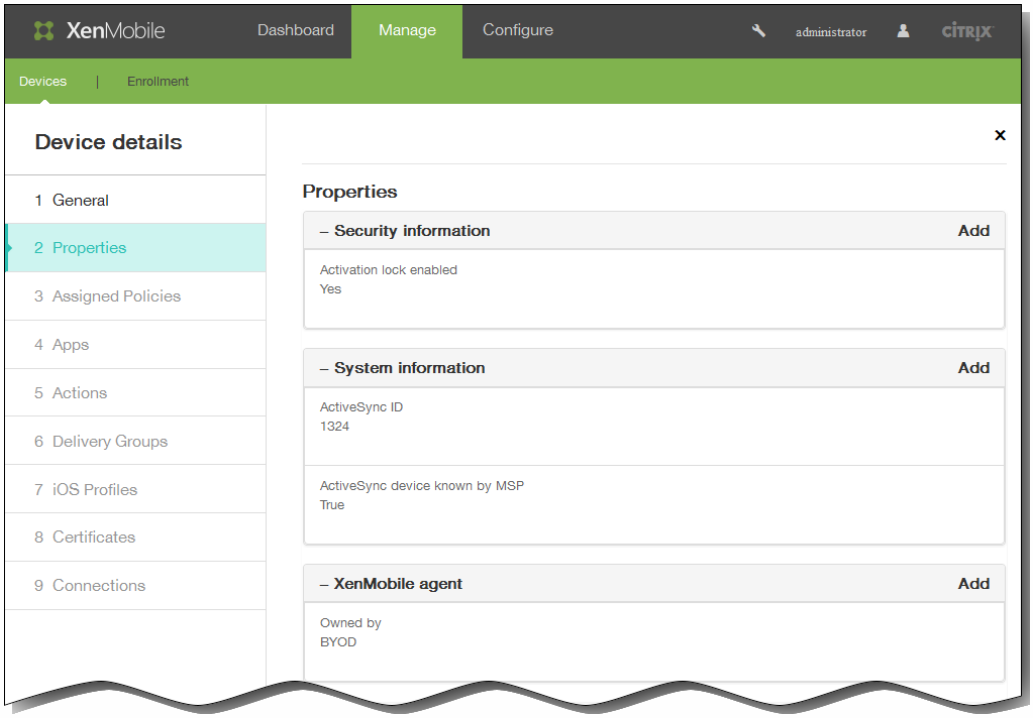
6. ［General Identifiers］の下に表示される、［Serial Number］、［IMEI/MEID］、［ActiveSync ID］、［WiFi MAC Address］、［Bluetooth MAC Address］、［Device Ownership］（［Corporate］または［BYOD］）の各情報（正確なパラメーター一覧は、プラットフォームの種類によって異なります）を確認します。



7. ［Security］の下に表示される、［Strong ID］、［Full Wipe of Device］、［Selective Wipe of Device］、［Lock Device］、［Device Unlock］、［Device Disown］、［Activation Lock Bypass］、［Device Clear Restrictions］の各情報（正確なパラメーター一覧は、プラットフォームの種類によって異なります）を確認します。
8. ［Next］をクリックしてプロパティを追加します。
9. ［Properties］ページで［Add］をクリックして、デバイスに対してプロビジョニングできるプロパティの一覧を表示します。 使用可能なプロパティー覧のボックスが表示されます。



10. 一覧から、プロビジョニングするプロパティを選択して、値を設定します。 たとえば前述の図では、プロパティ［Activation lock enabled］が選択されており、［Yes］または［No］のいずれかの値を設定できます。
11. プロパティを構成したら、［Done］をクリックします。
12. プロビジョニングするプロパティごとに手順9.～11.を繰り返し、［Next］をクリックします。
    注：プロパティを追加すると、すべて［Properties］の下に表示されます。後で［Properties］ページに戻ると、プロパティが複数のカテゴリに分かれています。



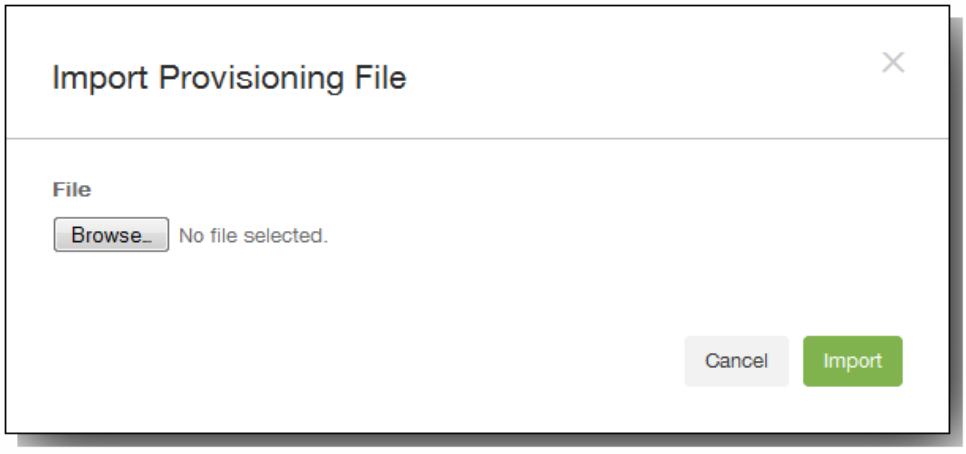
［**Assigned Policies**］以降のすべてのセクションには、デバイスの概要情報が含まれています。

- Assigned Policies：展開済み、保留中、失敗のポリシー数を含む、割り当て済みポリシー数が表示されます。各ポリシーの名前、種類、最新展開の情報も表示されます。
- Apps：インストール済み、保留中、失敗のアプリケーション数を含む、最新のインベントリ時点のアプリケーション数が表示されます。
  - ［Installed］については、名前、所有権、バージョン、作成者、サイズ、インストール済み、識別子、種類の各情報が表示されます。
  - ［Pending］および［Failed］のアプリケーションについては、名前、最新展開、識別子、種類の各情報が表示されます。
- Actions：展開済み、保留中、失敗のアクション数を含む、アクション数が表示されます。各アクションの名前および最新展開の情報が表示されます。
- Delivery Groups：成功、保留中、失敗のデリバリーグループ数が表示されます。各アクションのデリバリーグループと時刻の情報が表示されます。また、デリバリーグループの状態、アクション、所有者、日付などのさらに詳細な情報も表示されます。
- iOS Profiles（iOSデバイスのみ）：名前、種類、組織、説明など、最新のiOSプロファイルインベントリが表示されます。
- Certificates：有効な証明書と期限切れまたは失効した証明書の数が表示され、種類、プロバイダー、発行者、シリアル番号、有効期間の開始日および終了日の情報も表示されます。
- Connections：最初の接続状態と最後の接続状態が表示されます。各接続のユーザー名、最後から2番目の認証、最後の認証が表示されます。
- TouchDown（Androidデバイスのみ）：最後のデバイス認証と最後のユーザー認証の情報が表示されます。それぞれ該当するポリシー名とポリシー値が表示されます。

13. ［Save］をクリックします。

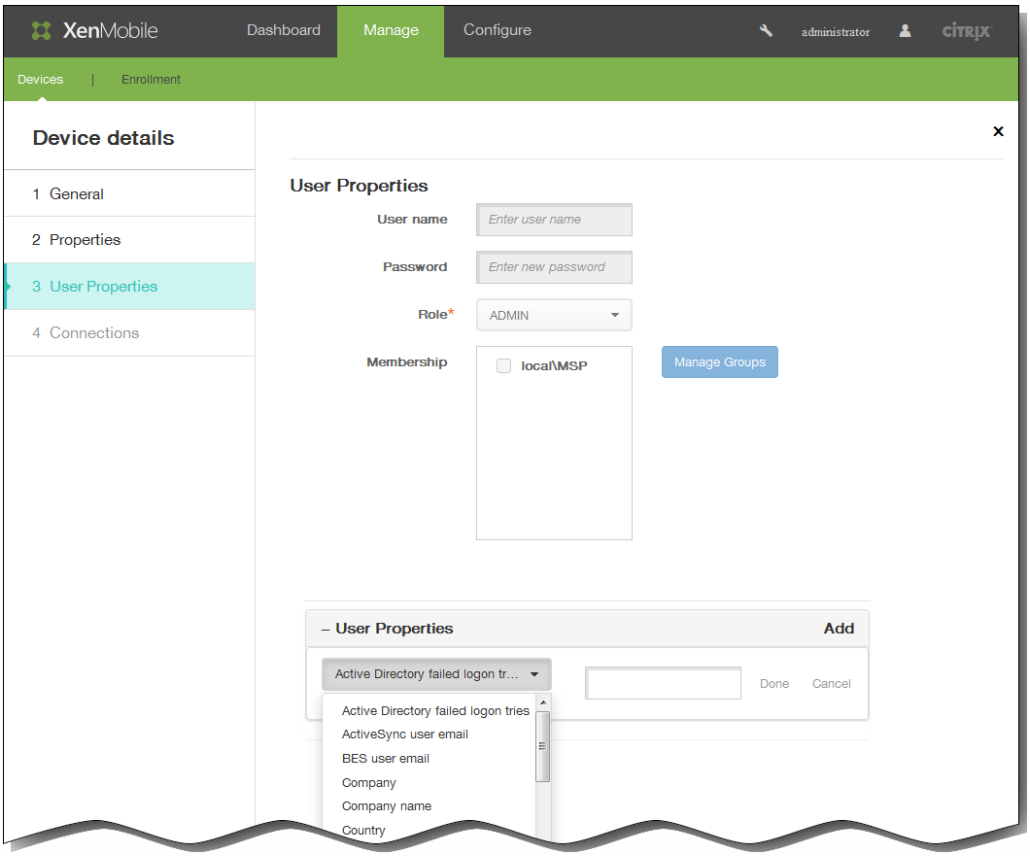
モバイル事業者やデバイス製造元が提供するファイルをインポートしたり、独自のデバイスプロビジョニングファイルを作成したりすることができます。「デバイスプロビジョニングファイル形式」を参照してください。

1. ［Devices］の表の上にあるメニューで、［Import］をクリックします。［Import Provisioning File］ダイアログボックスが開きます。



2. ［Browse］をクリックしてファイルの場所へ移動し、インポートするファイルを選択します。
3. ［Import］をクリックします。インポートされたファイルが［Devices］の表に追加されます。

1. 編集するデバイスを選択し、［Edit］をクリックします。 ［Device Details］ページが開きます。
2. ［General Identifiers］で変更できるフィールドは［Device Ownership］のみで、［Corporate］または［BYOD］に設定できます。
3. ［Next］をクリックします。 ［Properties］ページが開きます。
4. ［Properties］ページで、プロパティを必要に応じて追加、編集、または削除します。
   - プロパティを編集するには、プロパティを選択して設定を変更し、［Done］または［Cancel］をクリックします。
   - プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の［X］をクリックします。項目が直ちに削除されます。
5. ［Next］をクリックします。 次に開くページは、選択したデバイスによって異なります。デバイスによって、［User Properties］が開く場合と、［Assigned Properties］が開く場合があります。
6. ［User Properties］が開いた場合は、以下の手順に従ってユーザープロパティを追加、編集、または削除します。 ［Assigned Properties］が開いた場合は、残りのページにデバイスの概要情報が表示されます。 これらのページについて詳しくは、「デバイスを手動で追加するには」を参照してください。



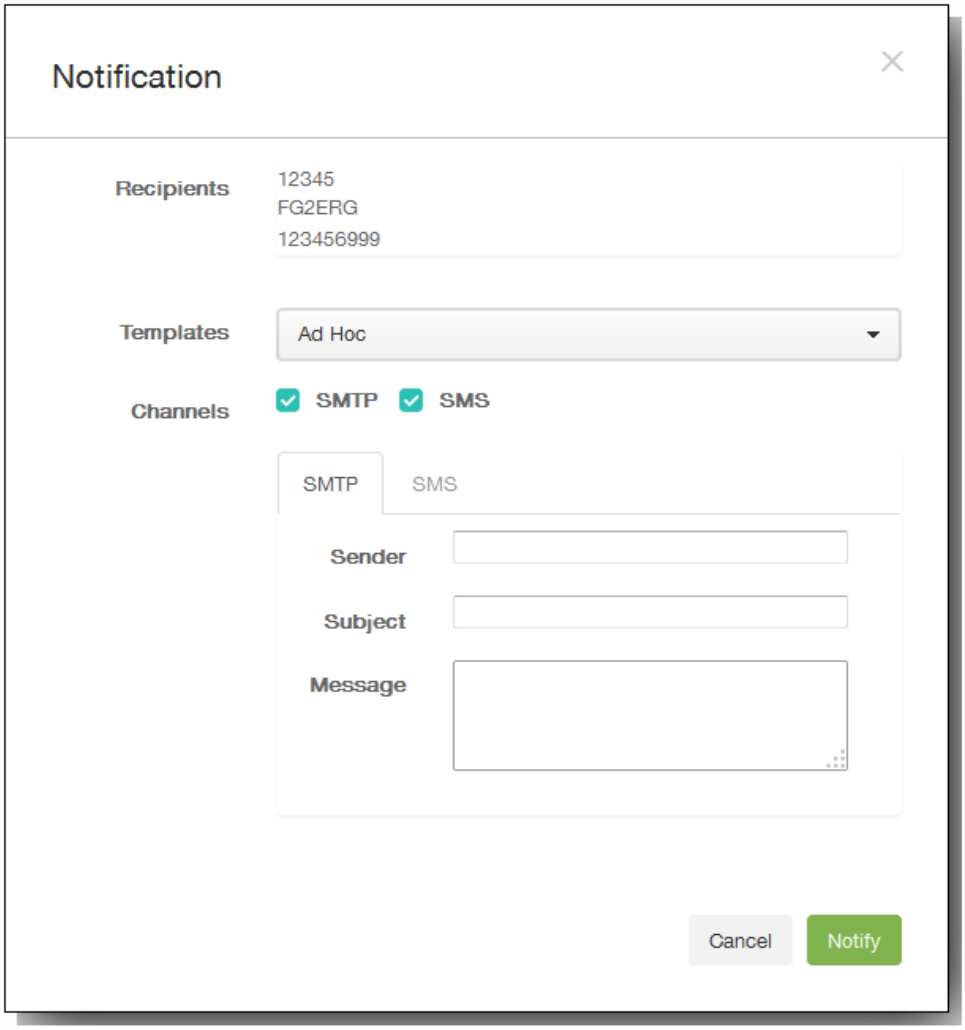
注：［User Properties］ページの上側の部分は編集できません。

- ユーザープロパティを追加するには、［Add］をクリックします。
  - 一覧から、追加するプロパティを選択してプロパティの値を入力し、［Done］または［Cancel］をクリックします。追加する各プロパティについて、この手順を繰り返します。
- プロパティを編集するには、プロパティを選択して設定を変更し、［Done］または［Cancel］をクリックします。
- プロパティを削除するには、項目の上にマウスカーソルを置いて、右側の［X］をクリックします。項目が直ちに削除されます。

7. 以降の各ページで［Next］をクリックして、概要情報を表示します。
8. 最後のページで［Save］をクリックして、デバイスの変更を保存します。

［Devices］ページで、デバイスに通知を送信できます。通知について詳しくは、「XenMobileで通知テンプレートを作成または更新するには」を参照してください。

1. 通知を送信するデバイスを選択します。
2. ［Notify］をクリックします。［Notification］ダイアログボックスが開きます。［Recipients］に、通知を受信するすべてのデバイスの一覧が表示されます。



3. 次の情報を構成します。
   1. Templates：一覧から、送信する通知の種類を選択します。
      ［Ad Hoc］を選択した場合を除き、［Subject］フィールドおよび［Message］フィールドには、選択したテンプレートで構成済みのテキストが入力されます。
   2. Channels：メッセージの送信方法を選択します。デフォルトは［SMTP］
      —および
      ［SMS］です。
      ［SMTP］タブと［SMS］タブをクリックすると、それぞれのメッセージ形式を表示できます。
   3. Sender：オプションで送信者を入力します。

4. Subject：アドホックメッセージの場合、件名を入力します。
5. Message：アドホックメッセージの場合、メッセージを入力します。

4. ［Notify］をクリックします。

1. ［Devices］の表で、削除するデバイスを選択します。
2. ［Delete］をクリックします。 確認ダイアログボックスが開きます。もう一度［Delete］をクリックします。
   重要：この操作を元に戻すことはできません。

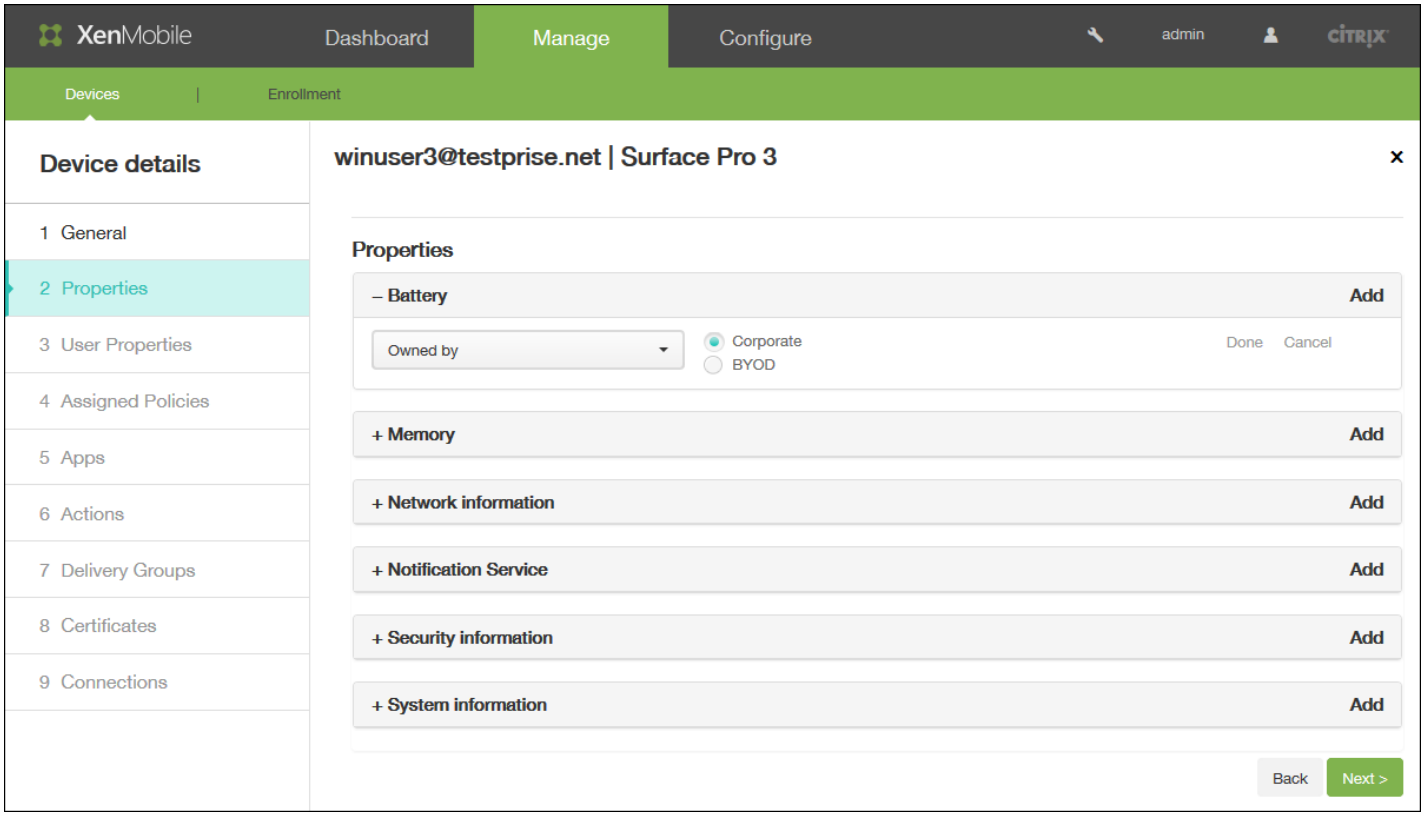
ユーザーデバイスの手動タグ付け

May 10, 2016

次の3通りの方法で、XenMobileのデバイスに手動でタグ付けすることができます。

- 招待状に基づく登録処理中に、デバイスにタグ付けします。
- Self Help Portal登録処理中に、デバイスにタグ付けします。
- デバイスプロパティとしてデバイス所有権を追加することで、デバイスにタグ付けします。

組織所有または個人所有のいずれかとして、デバイスにタグ付けするオプションが用意されています。Self Help Portalを使ってデバイスを自己登録するときに、組織所有または個人所有のいずれかとして、デバイスにタグを付けることもできます。次の図で示すように、［**Owned by**］という名前のプロパティを追加し、［**Corporate**］あるいは［**BYOD**］（個人所有）のいずれかを選択して、XenMobileコンソールの［**Devices**］タブからデバイスにプロパティを追加することにより手動でデバイスにタグ付けすることもできます。



デバイスプロビジョニングファイル形式

May 10, 2016

多くのモバイル事業者やデバイス製造元は、認証済みモバイルデバイスの一覧を提供しています。この一覧を使用すると、モバイルデバイスの長い一覧を手動で入力する必要がなくなります。XenMobileは、Android、iOS、Windowsの3種類のサポート対象デバイスすべてに共通のインポートファイル形式をサポートしています。

手動で作成し、XenMobileへのデバイスのインポートに使用するプロビジョニングファイルは次の形式である必要があります。

- SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

注：

- ファイルの文字セットはUTF-8を指定してください。
- プロビジョニングファイル内では、フィールドをセミコロン（;）で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字（\）を使ってエスケープする必要があります。たとえば、プロパティpropertyV;test;1;2の入力はプロビジョニングファイルではpropertyV\;test\;1\;2;prop 2となります。
- SerialNumberはIMEIが指定されない場合に必須です。
- SerialNumberiOSデバイスの識別子であるため、iOSデバイスではSerialNumberが必須です。
- IMEIはSerialNumberが指定されない場合に必須です。
- OperatingSystemFamilyで有効な値はWINDOWS、ANDROID、またはiOSです。

デバイスプロビジョニングファイル内で、以下の各行がデバイスを示しています。

1050BF3F51730108161006551059039l;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F51730108161006551059039 2;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F51730108161006551059039 3;35244201625379903;iOS;test;

4050BF3F51730108161006551059039 3;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

最初のエントリは以下を意味しています。

- SerialNumber：1050BF3F5173010816100655105903 91
- IMEI：15244201625379901
- OperatingSystemFamily：WINDOWS
- ProertyName：propertyN
- PropertyValue：propertyV\;test\;1\;2;prop 2

XenMobileのマクロ

May 10, 2016

XenMobileでは、強力なマクロが提供されています。マクロにはいろいろな用途がありますが、たとえば、プロファイル、ポリシー、通知、または登録テンプレートのテキストフィールドにユーザーまたはデバイスのプロパティデータを設定できます（一部の操作の場合）。マクロを使用すると、単一のポリシーを構成して大きなユーザーベースに展開し、各対象ユーザーに固有の値を表示させることができます。たとえば、何千人ものユーザーがいるExchangeプロファイルにユーザーのメールボックスの値を事前に設定できます。

この機能は現在、iOSおよびAndroidデバイスの構成とテンプレートの場合にのみ使用できます。

以下のユーザーマクロは常に使用できます。

- loginname（ユーザー名＋domainname)
- username（loginnameドメイン名を除去したもの、ある場合）
- domainname（ドメイン名またはデフォルトドメイン）

以下の管理者が定義するプロパティも使用できる場合があります。

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox

- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname（前に説明したプロパティを上書きします）

さらに、ユーザーがLDAPなどの認証サーバーを使用して認証されている場合、そのストアでユーザーに関連付けられているすべてのプロパティを使用できます。

マクロの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。

デバイスポリシー

May 10, 2016

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

新しいポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定のデリバリーグループを作成します。
- 必要なCA証明書をインストールします。

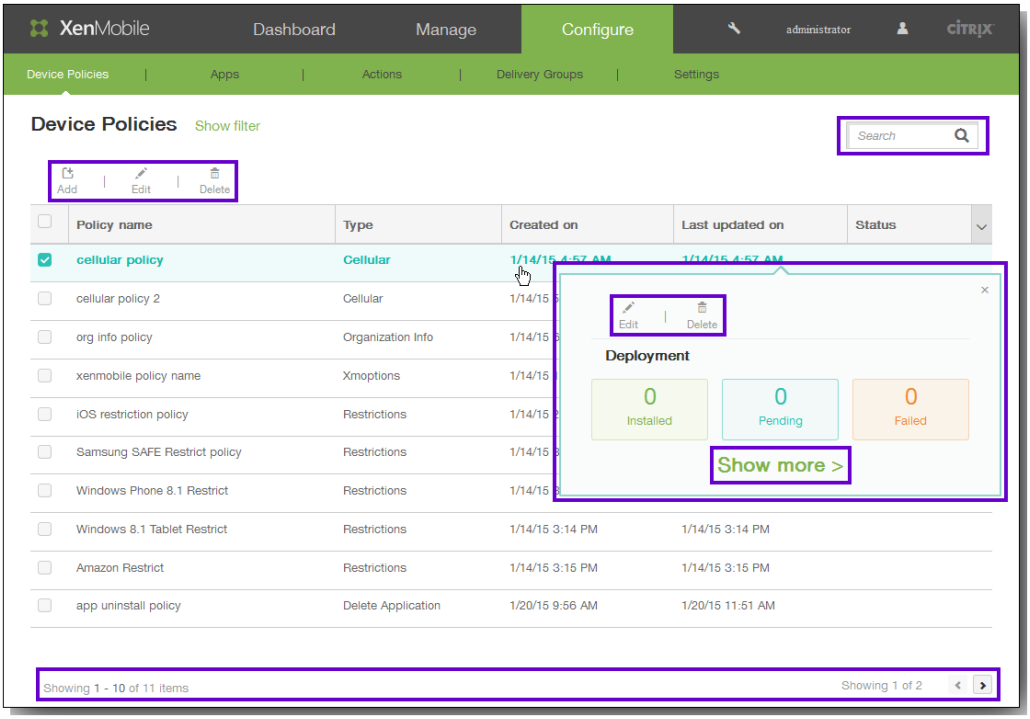
デバイスポリシーの基本的な作成手順は次のとおりです。

1. ポリシーの名前と説明を指定します。
2. 1つまたは複数のプラットフォームを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

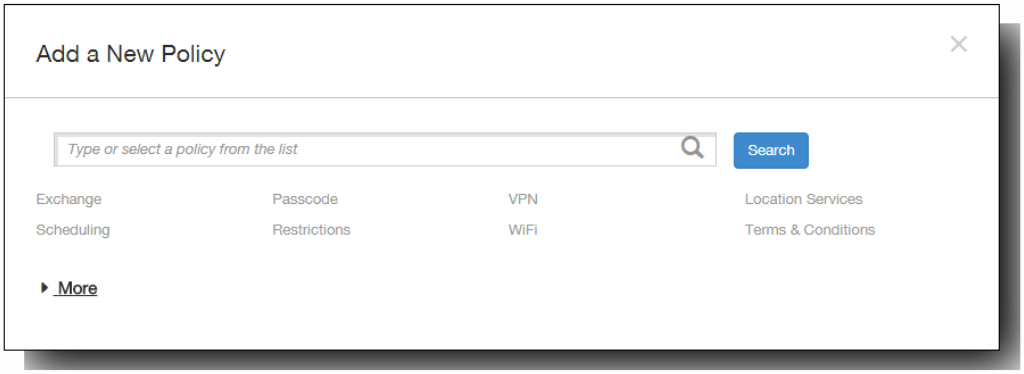
デバイスポリシーの操作は、XenMobileコンソールの［Device Policies］ページで行います。［Device Policies］ページにアクセスするには、［Configure］の［Device Policies］をクリックします。このページで新しいポリシーを追加したり、既存のポリシーの状態を確認したり、ポリシーを編集または削除したりすることができます。

［Device Policies］ページには、現在のポリシーをすべて示す表があります。

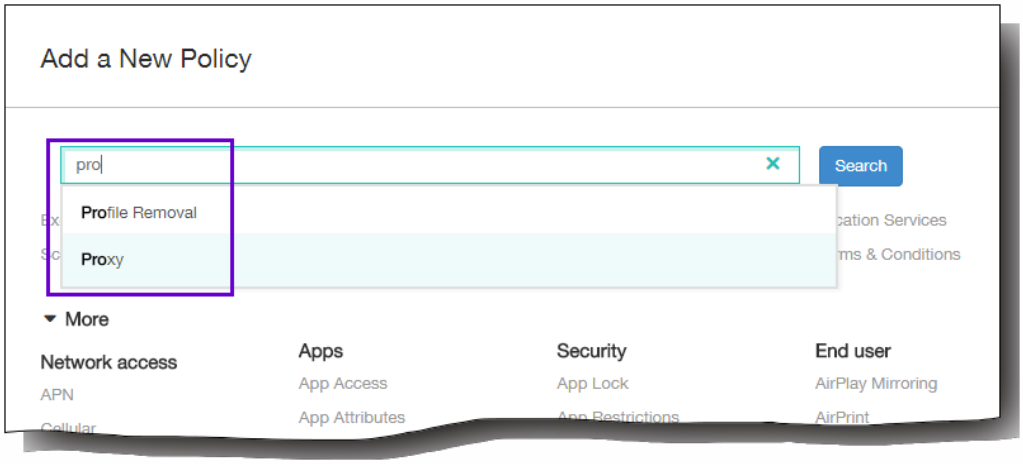
［Device Policies］ページでポリシーを編集または削除するには、ポリシーの横のチェックボックスをオンにしてポリシー一覧の上に表示されるオプションメニューを使用するか、一覧内でポリシーをクリックして項目の右側に表示されるオプションメニューを使用します。［Show More］をクリックすると、ポリシーの詳細が表示されます。



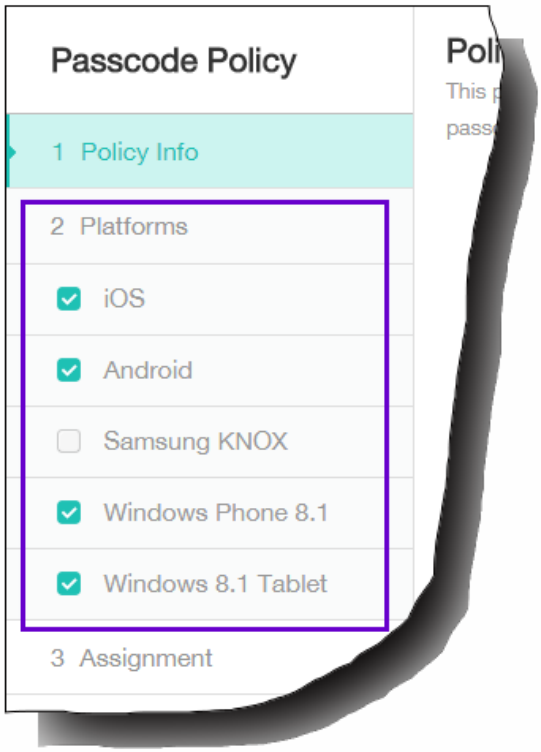
1. ［Device Policies］ページで、［Add］をクリックします。
［Add a New Policy］ダイアログボックスが開きます。［More］を展開するとほかのポリシーを表示できます。



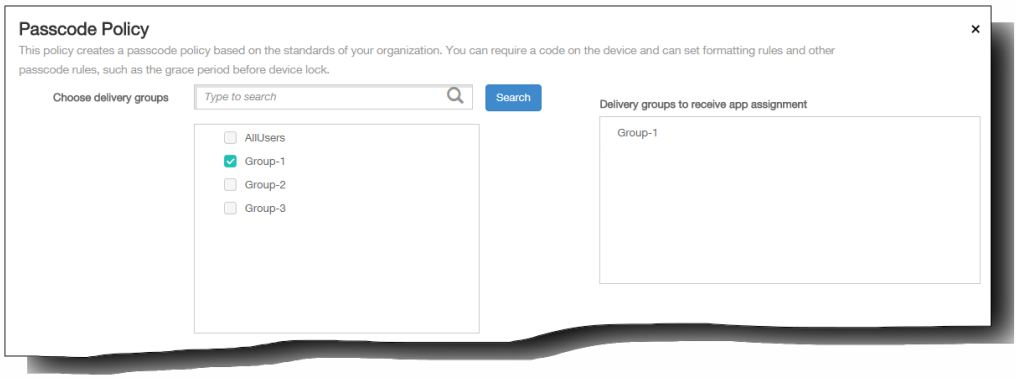
2. 追加するポリシーを検索するには、次のいずれかを実行します。
   - ポリシーをクリックします。
   選択したポリシーの［Policy Information］ページが開きます。
   - 検索フィールドにポリシーの名前を入力します。入力すると一致候補が表示されます。一覧の中に目的のポリシーがあれば、それをクリックします。選択したポリシーのみがダイアログボックス内に残ります。それをクリックして、そのポリシーの［Policy Information］ページを開きます。
   重要：選択したポリシーが［More］領域の中にある場合、［More］を展開した場合にのみ表示されます。



3. ポリシーに含めるプラットフォームを選択します。選択したプラットフォームの構成ページが手順5.で表示されます。
   注： ポリシーでサポートされるプラットフォームのみが一覧に表示されます。



4. ［Policy Information］ページで必要な情報を入力して、［Next］をクリックします。［Policy Information］ページにはポリシー名などの情報が集約されているため、ポリシーの識別や追跡に役立ちます。このページはすべてのポリシーで類似ています。
5. プラットフォームページの入力を完了します。手順3.で選択した各プラットフォームのページが開きます。これらのページはポリシーごとに異なります。各ポリシーはプラットフォームによって異なる場合があります。すべてのポリシーがすべてのプラットフォームでサポートされるわけではありません。［Next］をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、［Assignment］ページに移動します。
6. ［Assignments］ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、［Delivery groups to receive app assignment］ボックスにそのグループが表示されます。
   注： ［Delivery groups to receive app assignment］ボックスは、デリバリーグループを選択するまで表示されません。



7. ［Save］をクリックします。
   ポリシーが［Device Policies］の表に追加されます。

1. **［Device Policies］**の表で、編集または削除するポリシーの横のチェックボックスをオンにします。
2. ［Edit］または［Delete］をクリックします。
   - ［Edit］をクリックした場合、いずれかまたはすべての設定を編集できます。
   - ［Delete］をクリックした場合、確認ダイアログボックスで、もう一度［Delete］をクリックします。

プラットフォーム別のXenMobileデバイスポリシー

May 10, 2016

次の表は、Amazon、iOS、Android、Samsung SAFE、Samsung KNOX、Symbian、Windows Phone 8.1、およびWindows 8.1タブレットデバイスに対してXenMobile 10.0で追加および構成できるデバイスポリシーを示しています。デバイスポリシーの追加と構成は、XenMobileコンソールの［Configure］の［Device Policies］をクリックすると開くページで実行できます。

注：Android Sonyはストレージ暗号化ポリシーのみをサポートします。Android HTCはExchangeポリシーのみをサポートします。

デバイスポリシー	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
共通								
Exchange		○	○	○	○		○	
スケジュール設定			○			○		
パスコード		○	○		○		○	○
制限事項	○	○		○			○	○
VPN	○	○	○	○	○			○
WiFi		○	○				○	○
位置情報サービス		○	○					
契約条件	○	○	○	○	○	○	○	○
Network access								
APN		○	○		○			
移動体通信			○					
個人用ホットスポット		○						
プロキシDHCP		○						

デバイスポリシー	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
移動		○			○			
Samsungファイアウォール				○				
トンネル			○					

	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
カスタム								
カスタムXML						○	○	○
iOSプロファイルのインポート		○						
削除								
プロファイル削除		○						
Apps								
アプリケーションアクセス		○	○			○		
アプリケーション属性		○						
アプリケーション構成		○						
アプリケーションインベントリ		○	○		○	○	○	○
アプリケーションのアンインストール		○	○		○			○
アプリケーションのアンインストール制限	○			○				
ファイル			○					

	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
Samsungブラウザーホームページ				○	○			○
サイドローディングキー								
証明書署名								○
Webクリップ		○	○					○
Worx Store		○	○					○

	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
セキュリティ								
アプリケーションロック		○	○					
アプリケーション制限					○			
連絡先（CardDAV）		○						
資格情報		○	○					○
キオスク				○				
管理対象ドメイン		○						
SCEP		○						
Samsung MDMライセンスキー				○	○			
ストレージ暗号化			○	○			○	
Webコンテンツフィルター		○						
XenMobileエージェント								
エンタープライズハブ							○	

デバイスポリシー	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1タブレット
XenMobileオプション			○			○		
XenMobileのアンインストール			○					
エンドユーザー								
AirPlayミラー化		○						
AirPrint		○						
カレンダー（CalDav）		○						
フォント		○						
LDAP		○						
MDMオプション		○						
メール		○						
組織情報		○						
SSOアカウント		○						
サブスクライブされたカレンダー		○						

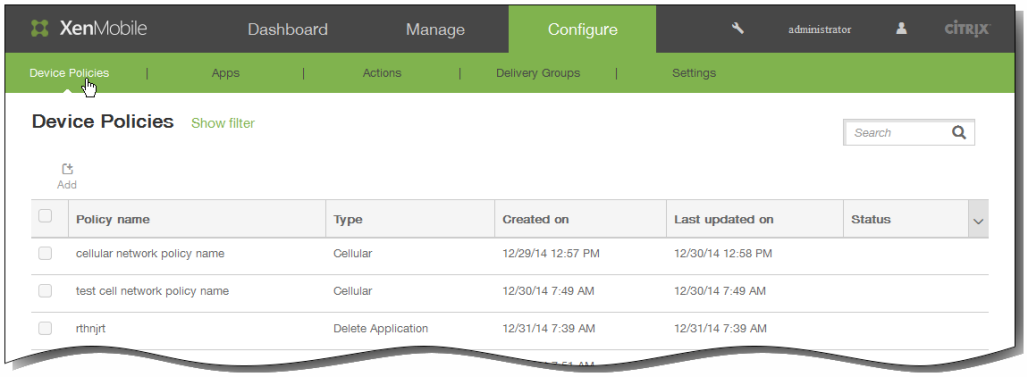
アプリケーションアクセスデバイスポリシーを追加するには

May 10, 2016

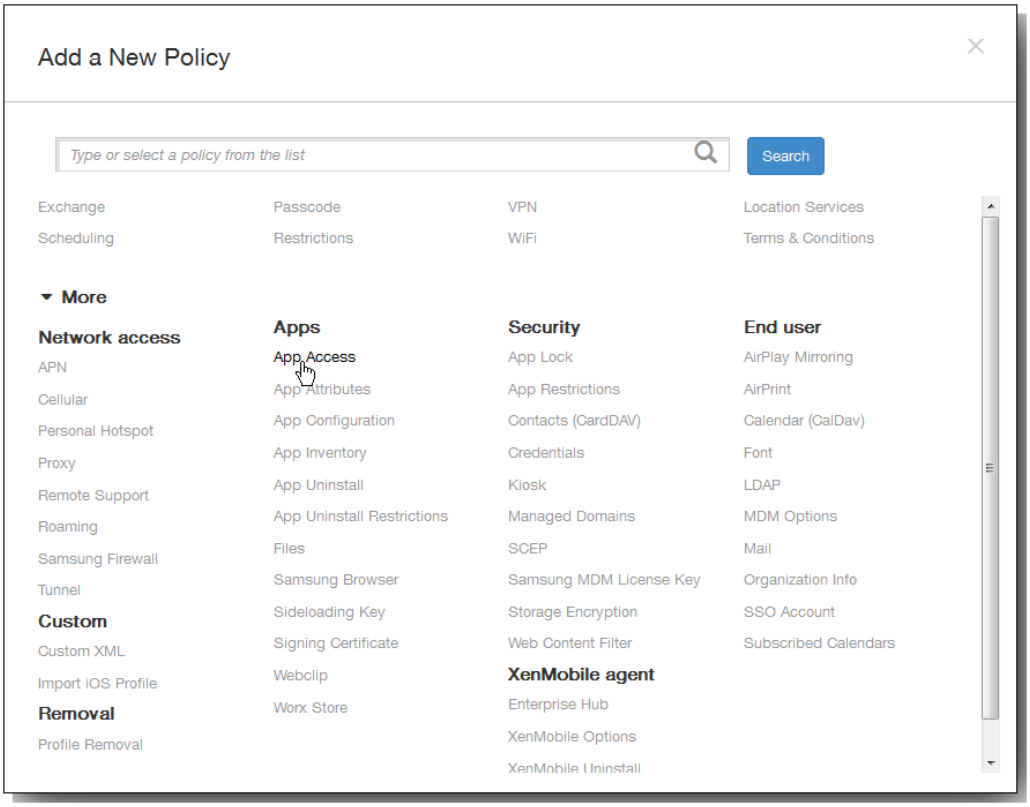
XenMobileのアプリケーションアクセスデバイスポリシーでは、デバイスへのインストールが必須のアプリケーション、デバイスにインストール可能なアプリケーション、デバイスへのインストールが禁止されるアプリケーションの一覧を定義できます。次に、そのアプリケーション一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。アプリケーションアクセスポリシーは、iOS、Android、Symbianデバイスに対して作成できます。

アクセスポリシーは一度に1種類のみ構成できます。必須アプリケーション、推奨アプリケーション、禁止アプリケーションのいずれかの一覧のポリシーを追加できますが、同じアプリケーションアクセスポリシー内に混在させることはできません。一覧の種類ごとにポリシーを作成する場合、XenMobileでどのポリシーがどのアプリケーション一覧に適用されるかがわかるようにするため、各ポリシーの名前付けに注意することをお勧めします。

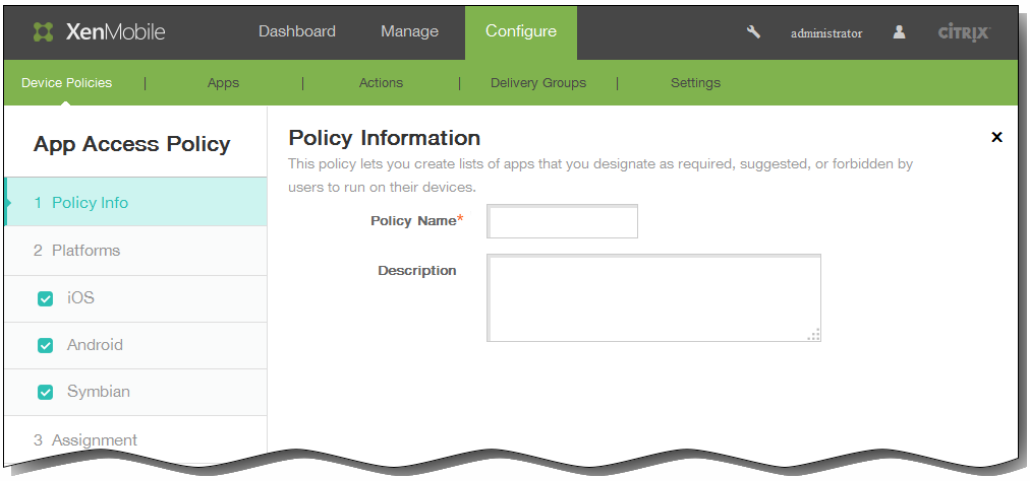
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。



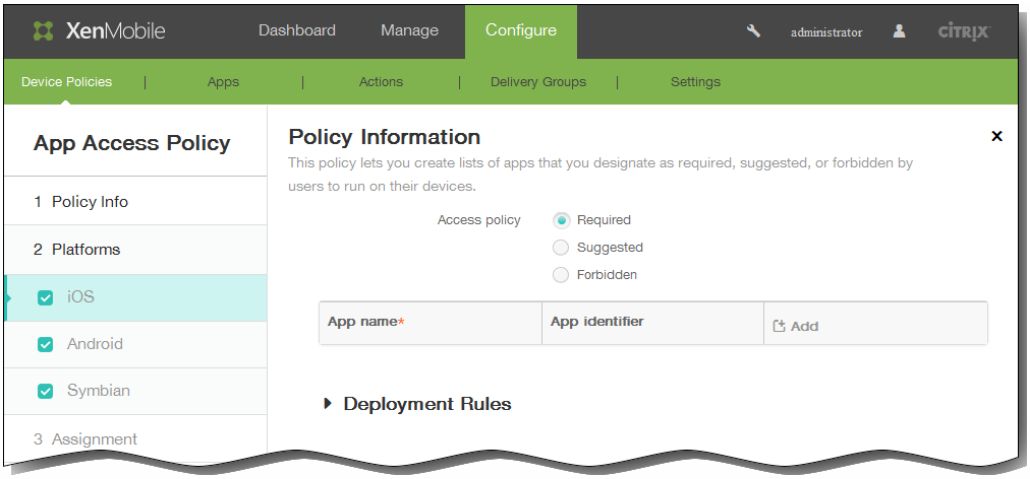
2. ［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］、［App Access］の順にクリックします。 ［App Access Policy］情報ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォーム構成ページが開きます。



6. ［Platforms］の下で、追加するプラットフォームをオンにして、プラットフォームごとに以下の操作を行います。
   1. Access policy：［Required］、［Suggested］、［Forbidden］のいずれかをクリックします。 デフォルトは［Required］です。
   2. 1つまたは複数のアプリケーションを一覧に追加するには、［Add］をクリックして以下の操作を行います。
      1. App name：アプリケーション名を入力します。
      2. App Identifier：任意で、アプリケーション識別子を入力します。
      3. ［Save］または［Cancel］をクリックします。
      4. 追加するカスタムキーごとに手順i.～iii.を繰り返します。

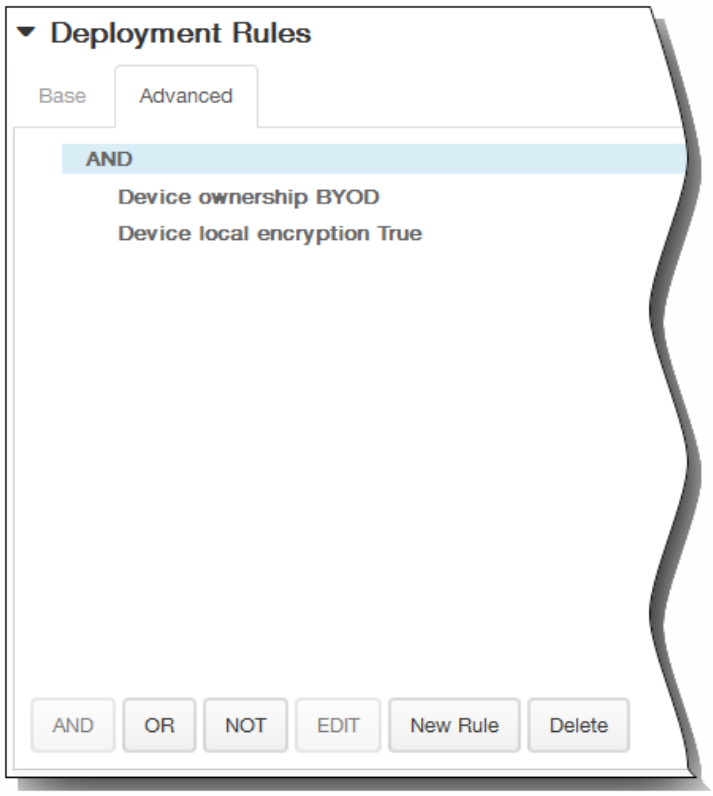
      注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

      既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

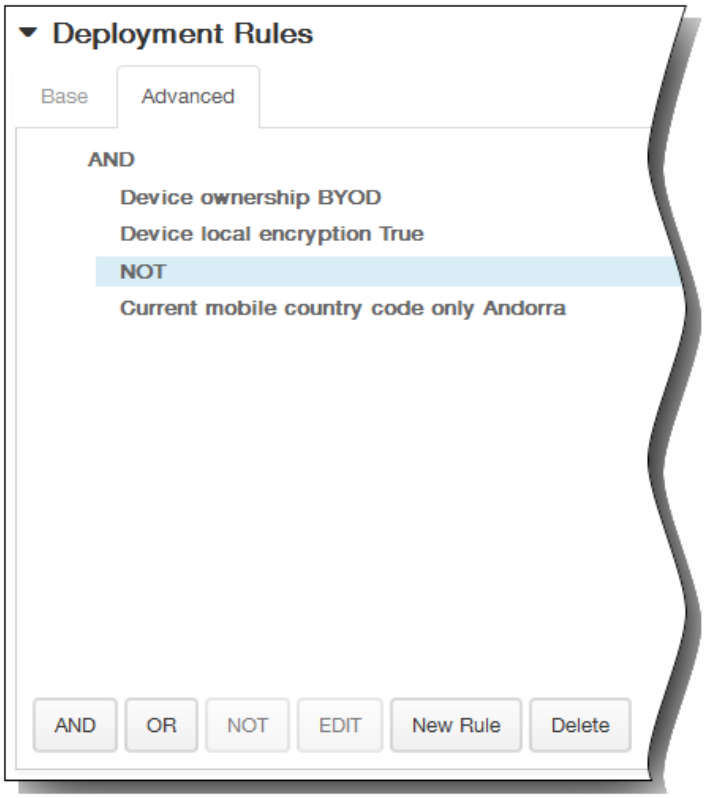
   1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
      1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
      2. ［New Rule］をクリックして条件を定義します。
      3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
      4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。

2. ［Advanced］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。

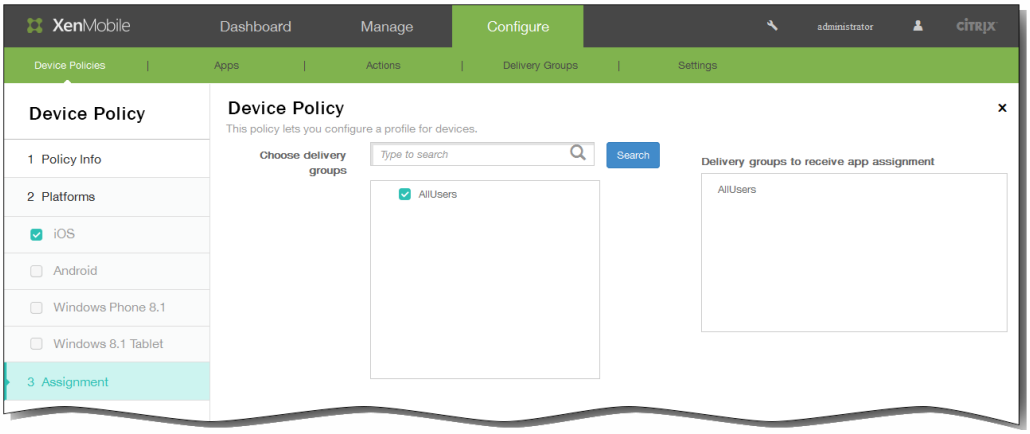


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 次のプラットフォームのページまたはポリシーの［Assignment］ページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



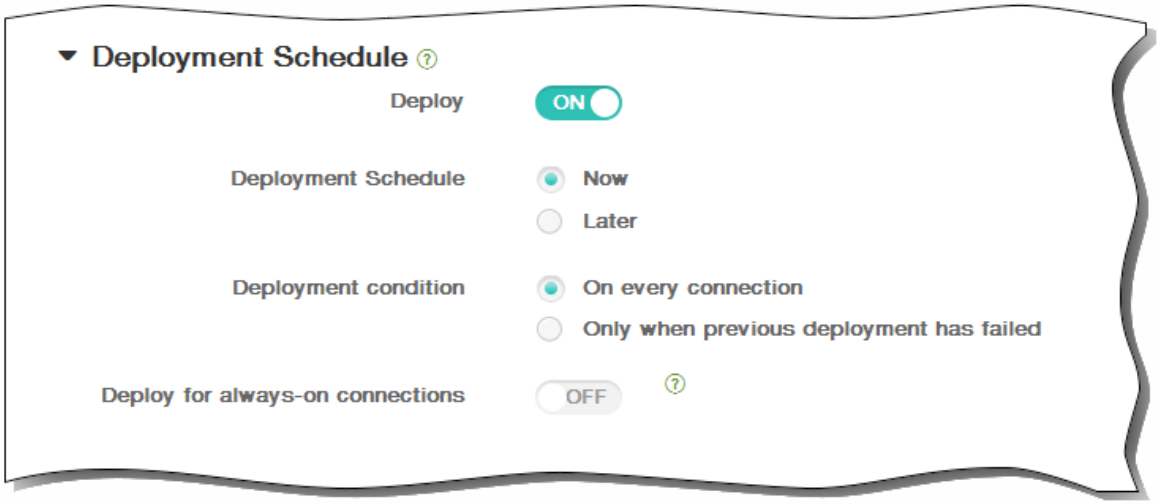
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

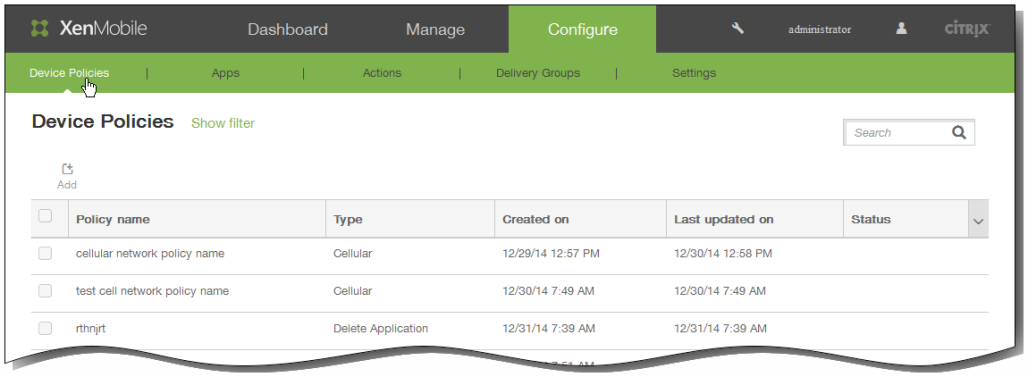
アプリケーションインベントリデバイスポリシーを追加するには

May 10, 2016

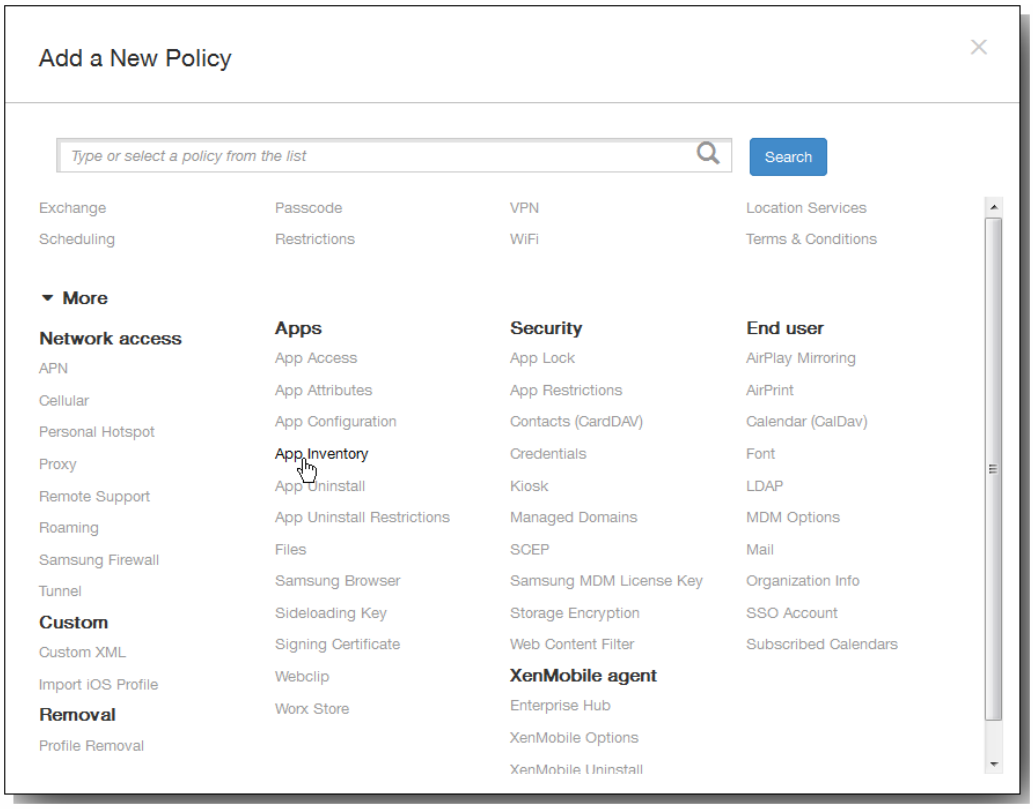
XenMobileのアプリケーションインベントリポリシーにより、管理されているデバイスのアプリケーションのインベントリを収集できます。その後、インベントリは、それらのデバイスに展開されたアプリケーションアクセスポリシーと比較されます。この方法で、アプリケーションのブラックリスト（アプリケーションアクセスポリシーで禁止）またはホワイトリスト（アプリケーションアクセスポリシーで必須）に表示されるアプリケーションを検出し、それに応じた操作を実行することができます。

重要： ユーザーのAndroidデバイスで、Worx Storeの［Updates Available］の一覧に更新されたアプリケーションが表示されるようにするには、最初にこのポリシーをユーザーのデバイスに展開しておく必要があります。

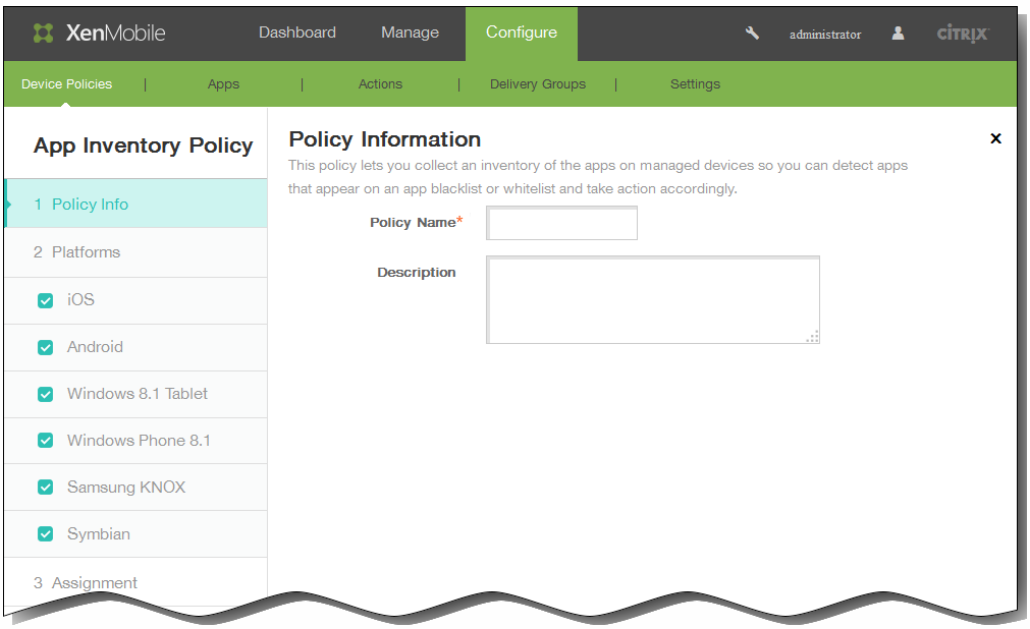
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



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



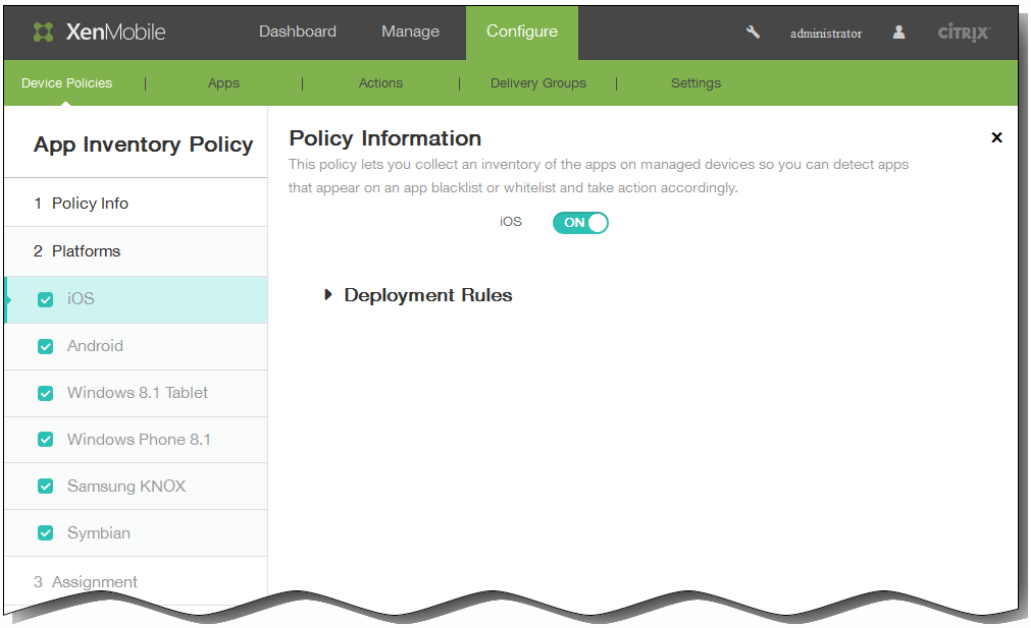
3. ［More］の［App Inventory］をクリックします。 ［App Inventory Policy］ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。

注： ［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラット

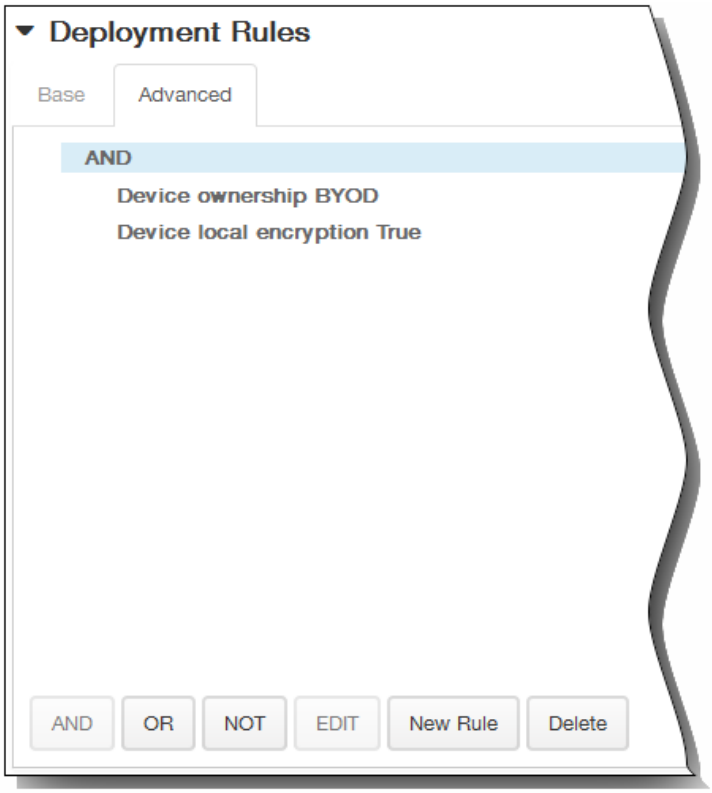
フォーム構成パネルが開きます。



追加するプラットフォームをオンにして、プラットフォームごとに以下の操作を行います。

6. 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. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

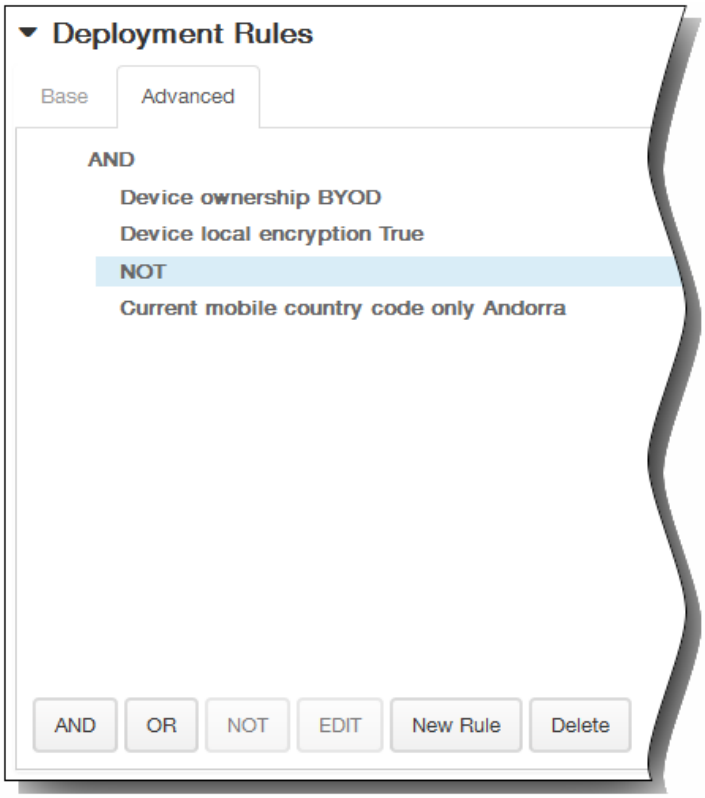
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
   1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］タブをクリックし、ブール値オプションを使用して規則を組み合わせます。



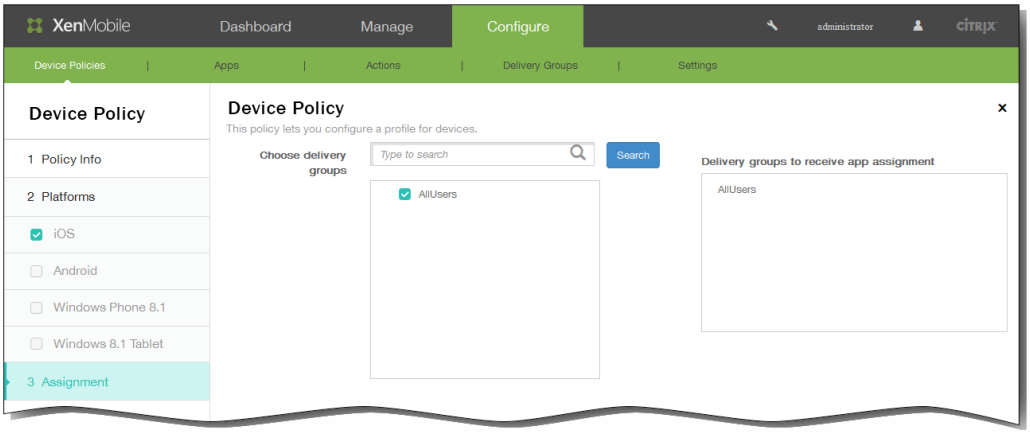
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 次のプラットフォームのページが開くか、ポリシーの［Assignment］ページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



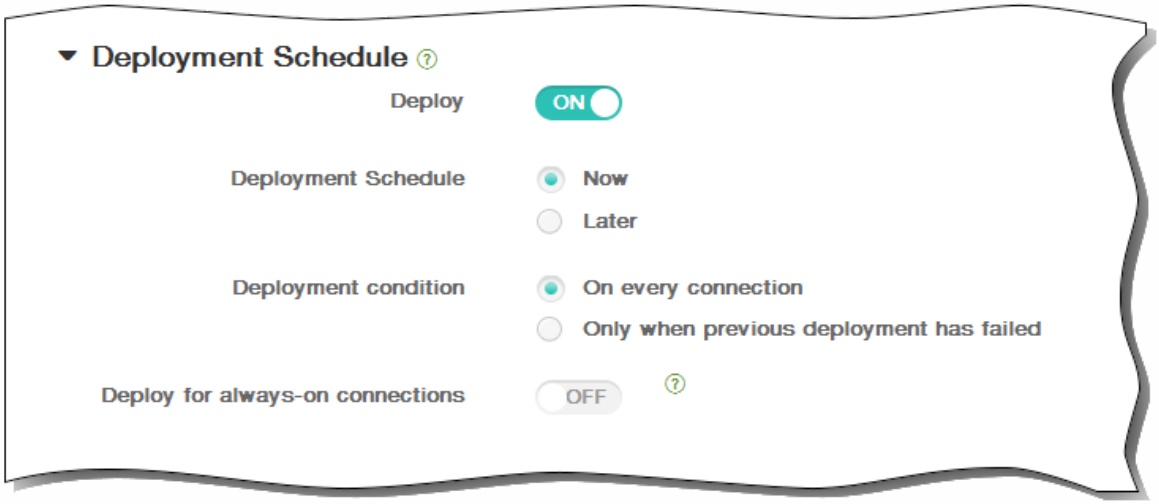
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

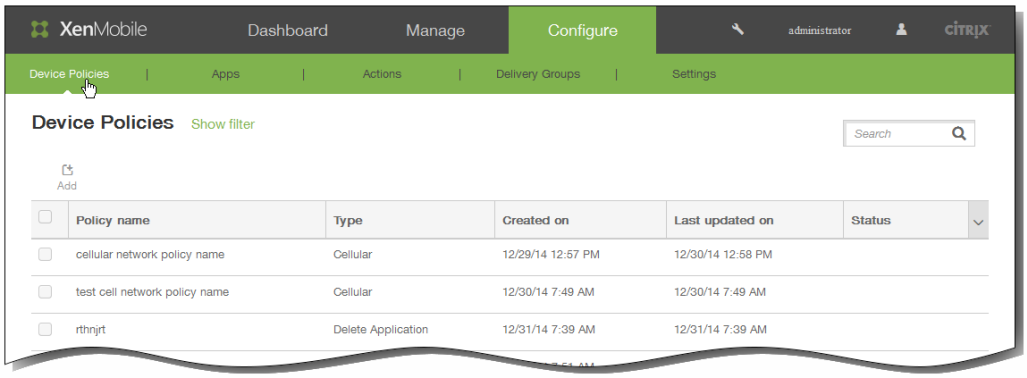
Androidのアプリトンネルデバイスポリシーを追加するには

May 10, 2016

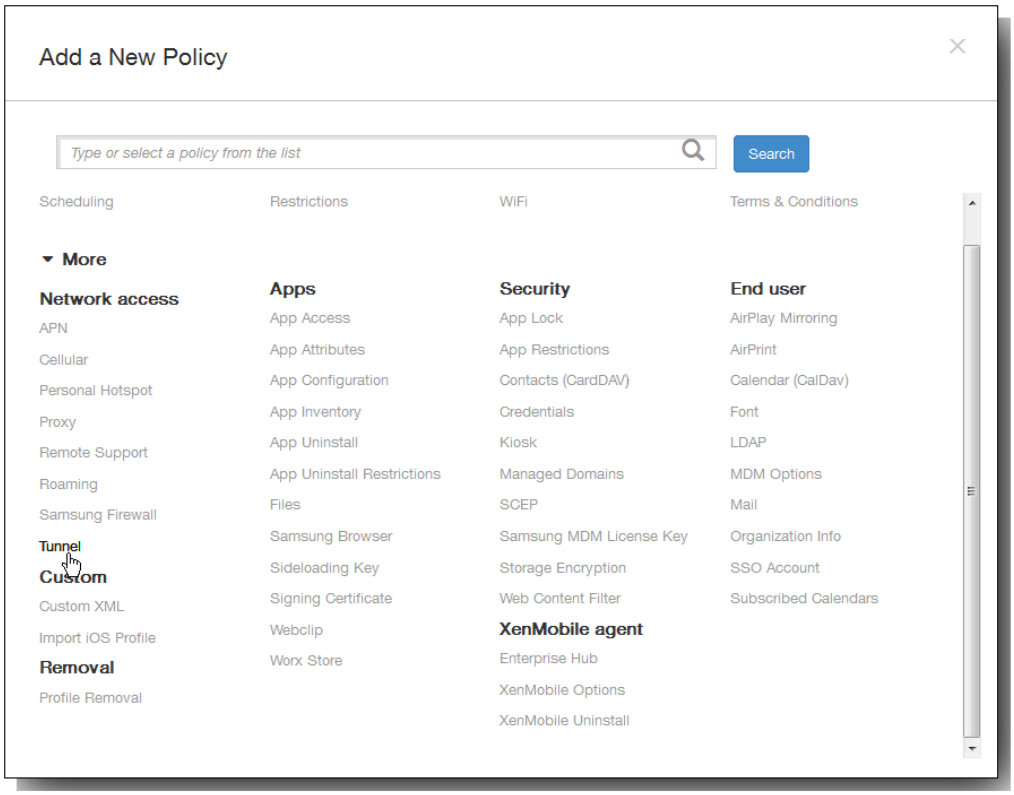
アプリトンネルは、モバイルアプリケーションのサービスの継続性およびデータ転送の信頼性を向上させるように設計されています。アプリトンネルは、モバイルデバイスアプリケーションのクライアントコンポーネントとアプリケーションサーバコンポーネント間のプロキシパラメーターを定義します。また、アプリトンネルを使用して、デバイスへのリモートサポートンネル（管理のサポートに使用）も作成できます。

注：このポリシーで定義したトンネルを使用して送信されるアプリケーショントラフィックは、XenMobileを経由してから、アプリケーションを実行するサーバーにリダイレクトされます。

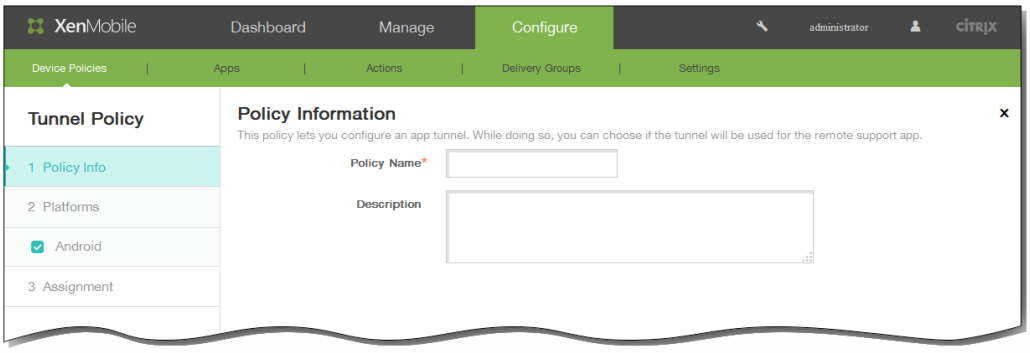
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



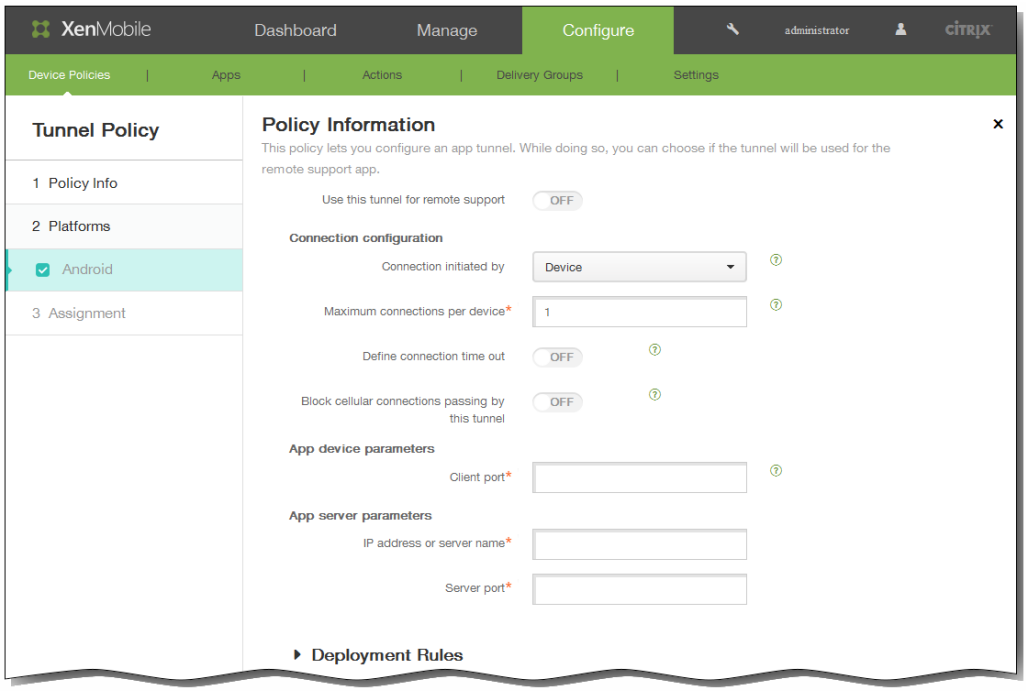
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Network access］の下の［Tunnel］をクリックします。 ［Tunnel Policy］ページが開きます。



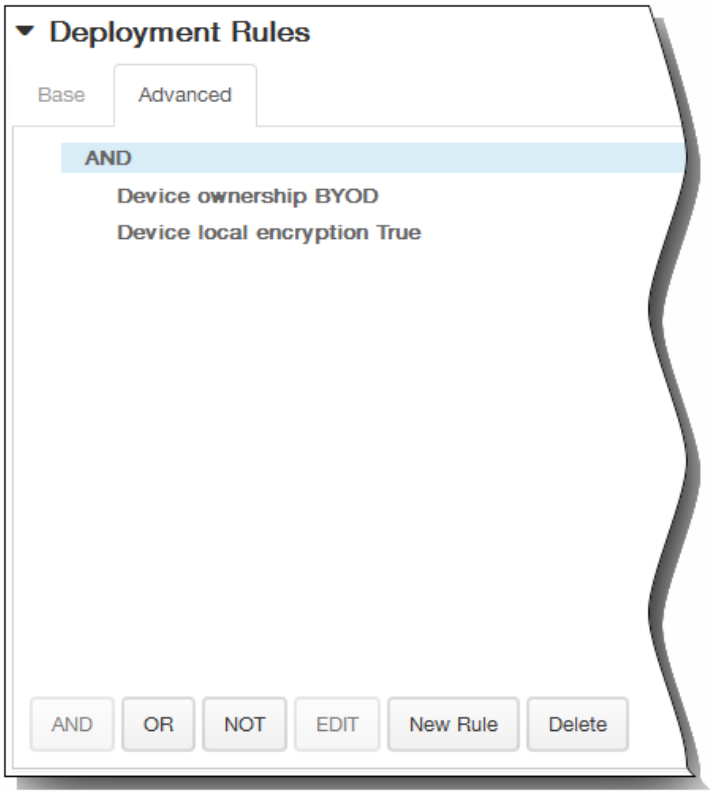
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Android Policy］プラットフォームページが開きます。



6. ［Use this tunnel for remote support］で、トンネルをリモートサポートで使用するかどうかを選択します。
   注：リモートサポートを選択するかどうかによって、構成手順が異なります。
   リモートサポートを**選択しない**場合、以下の手順を実行します。
   1. Connection initiated by：一覧から［Device］または［Server］を選択して、接続の開始元を指定します。
   2. 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。
   3. Define connection time out：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
   4. Connection time out：［Define connection time out］を［On］に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
   5. Block cellular connections passing by this tunnel：ローミング中、このトンネルをブロックするかどうかを選択します。
      注：WiFiおよびUSB接続はブロックされません。
   6. Client port：クライアントのポート番号を入力します。 ほとんどの場合、この値はサーバーポートと同じです。
   7. 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。
   8. Server port：サーバーのポート番号を入力します。

   リモートサポートを**選択する**場合、以下の手順を実行します。
   1. Use this tunnel for remote support：［On］に設定します。
   2. Define connection time out：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
   3. Connection time out：［Define connection time out］を［On］に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
   4. Use SSL connection：このトンネルで、安全なSSL接続を使用するかどうかを選択します。
   5. Block cellular connections passing by this tunnel：ローミング中、このトンネルをブロックするかどうかを選択します。
      注：WiFiおよびUSB接続はブロックされません。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

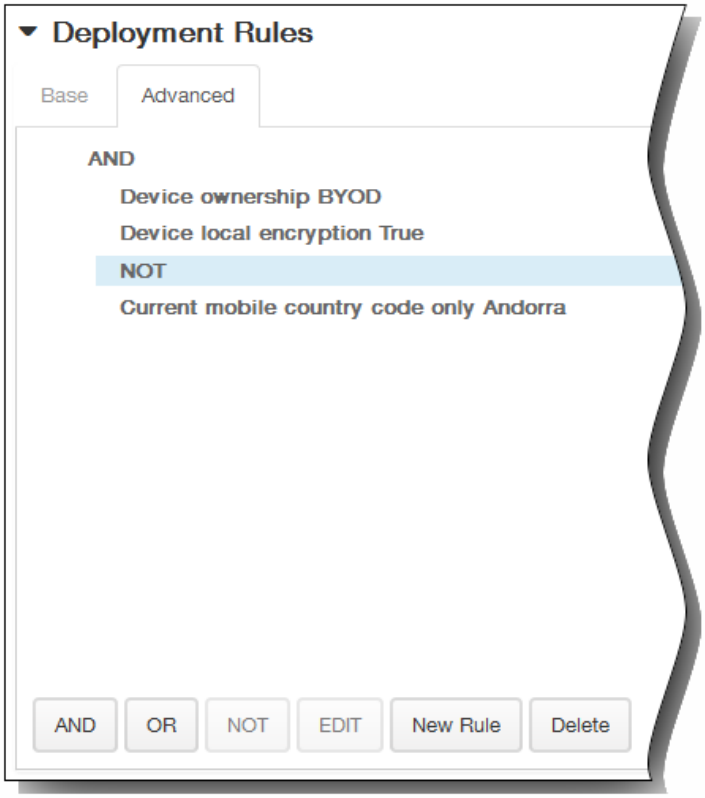


［Base］タブで選択した条件が表示されます。

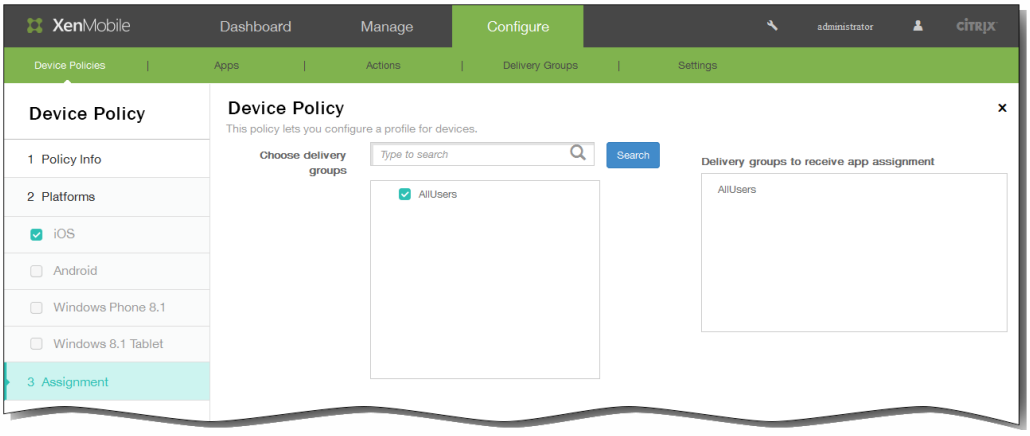
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Tunnel Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

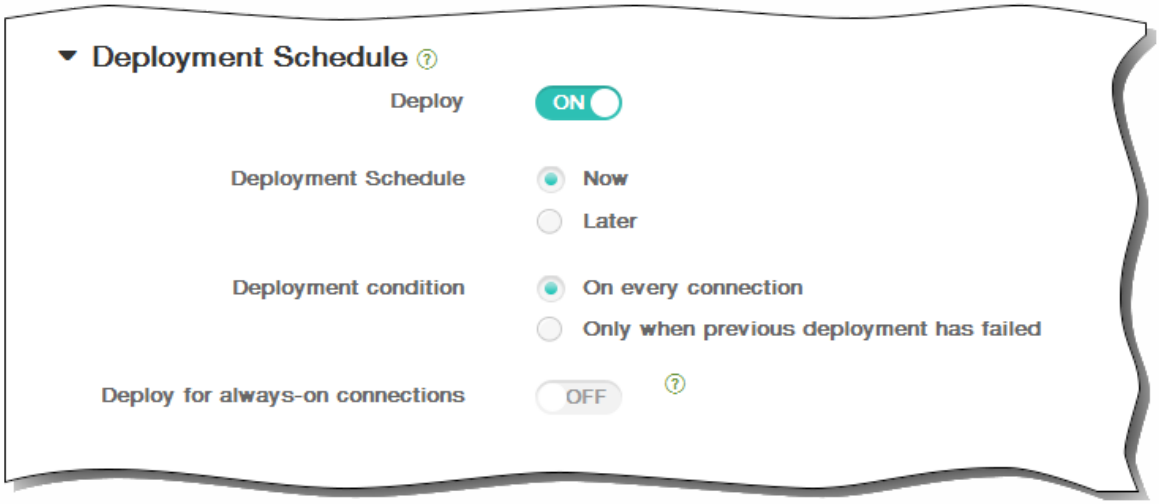


10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

カスタムXMLデバイスポリシー

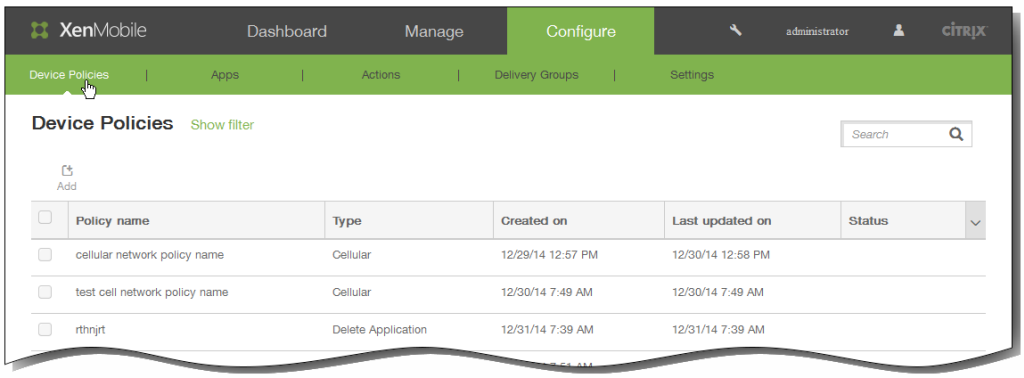
May 10, 2016

Windows Phone 8.1、Windows 8.1タブレット、Symbianデバイスの以下の機能をカスタマイズする場合、XenMobileでカスタムXMLポリシーを作成できます。

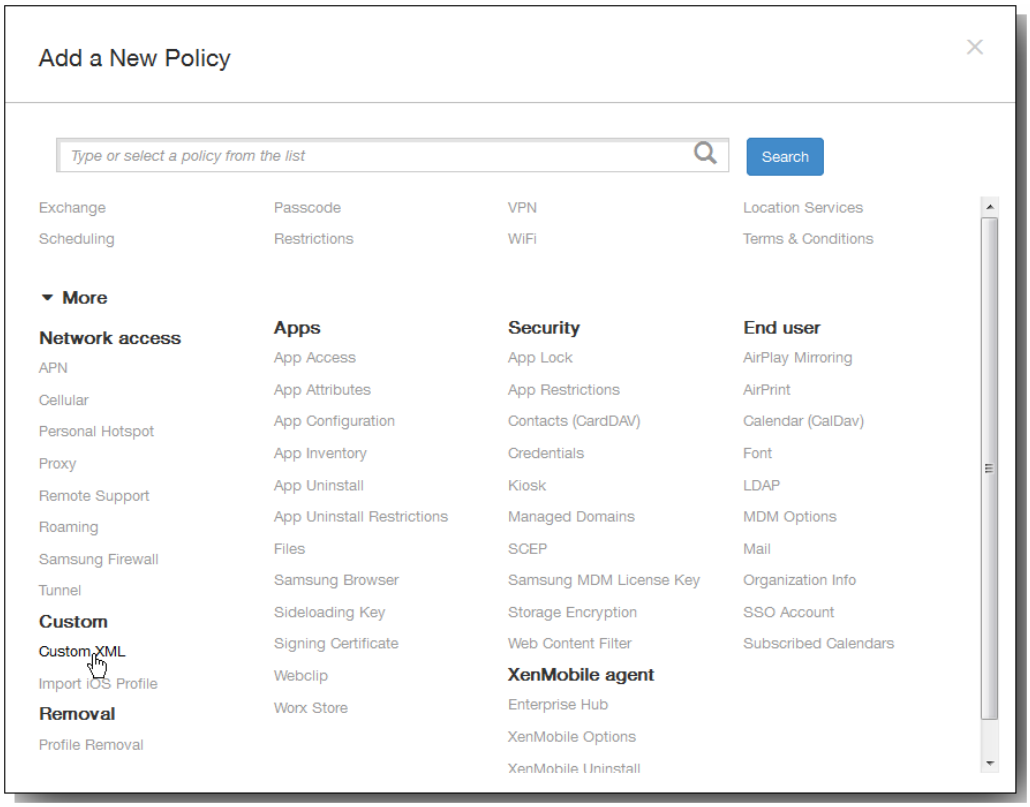
- プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。
- デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。
- ソフトウェアのアップグレード。アプリケーションやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。
- 障害管理。デバイスからのエラーおよび状態レポートの受信などです。

Windows 8.1でOpen Mobile Alliance Device Management（OMA DM）APIを使用して、カスタムXML構成を作成します。OMA DM APIを使用したカスタムXMLの作成については、このトピックでは扱いません。OMA DM APIの使用について詳しくは、Microsoft Developer Networkサイトの「OMA Device Management」を参照してください。

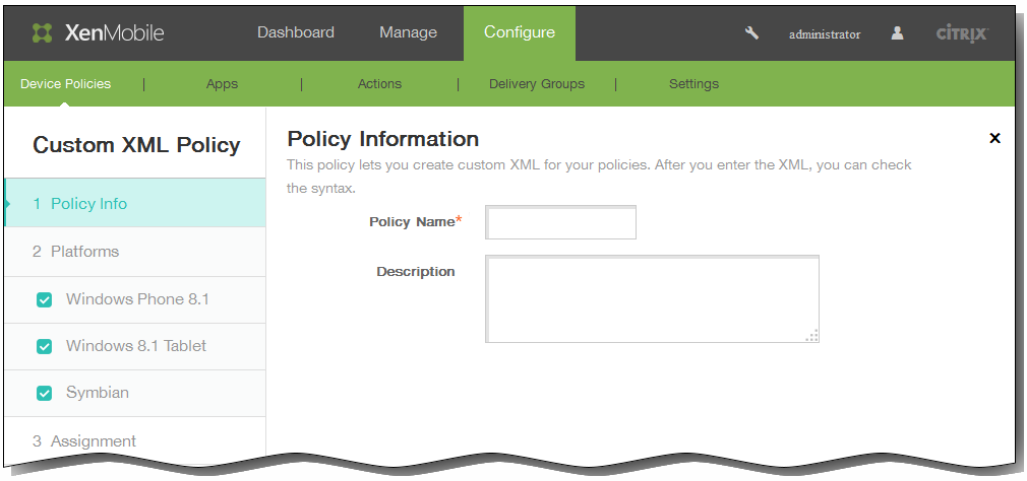
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



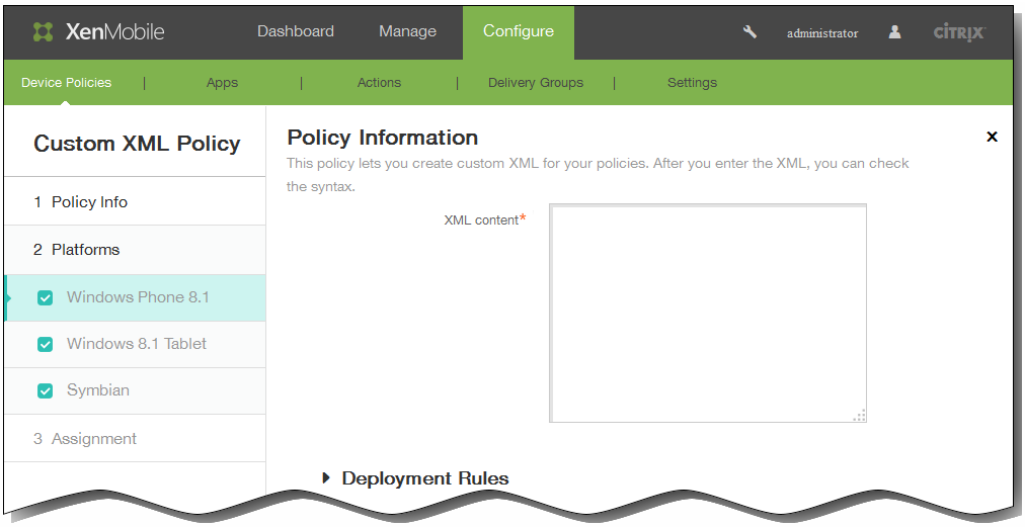
2. 新しいポリシーを追加するには［Add］をクリックします。［Add New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Custom］の下の［Custom XML］をクリックします。 ［Custom XML Policy］情報ページが開きます。

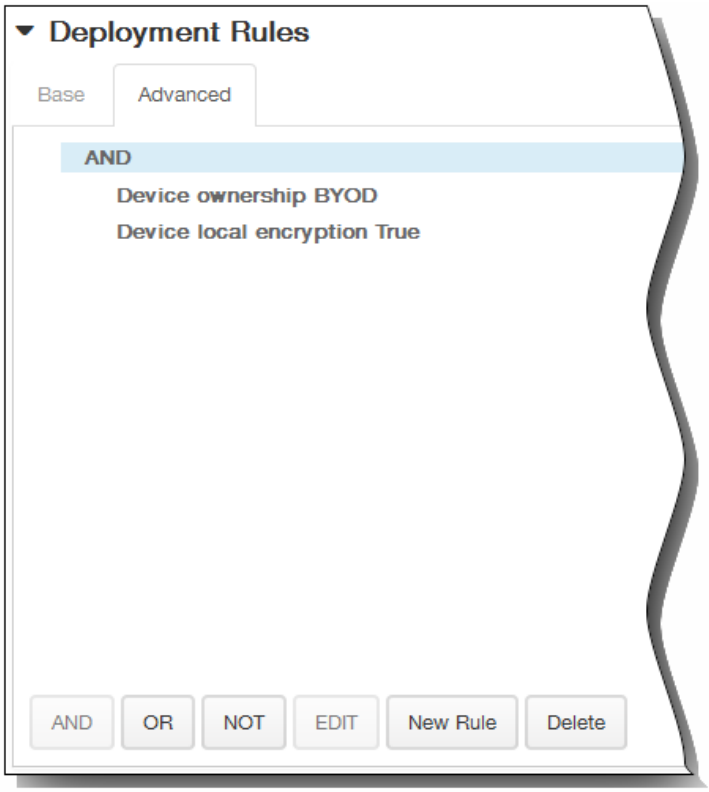


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はWindows Phone 8.1プラットフォーム構成パネルが開きます。



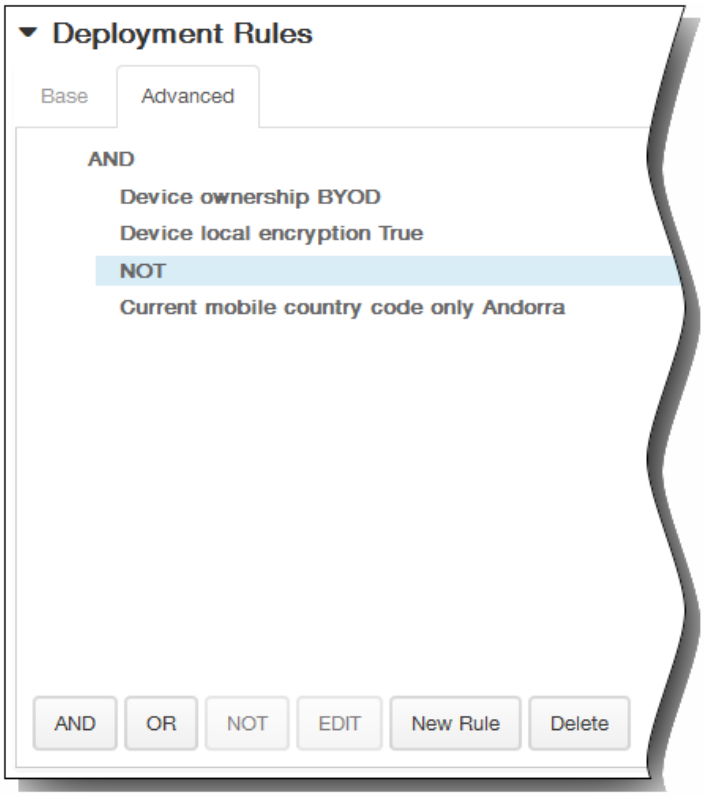
6. ［Platforms］の下で、追加するプラットフォームのみがオンになるようにします。
7. ［XML content］ボックスに、ポリシーに追加するカスタムXMLコードを入力します。 コンテンツが長い場合は、ソースファイルからコードをコピーして貼り付けることができます。
8. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
    1. 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［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



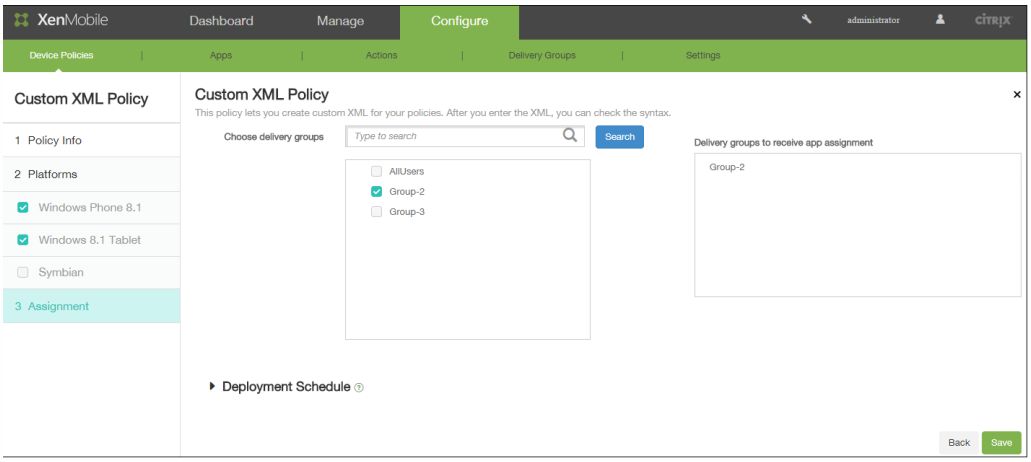
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



9. ［Next］をクリックします。 XenMobileでXMLコンテンツの構文がチェックされます。構文エラーがある場合、コンテンツボックスの下に表示されます。続行するにはエラーを修正する必要があります。
構文エラーがない場合は、［Custom XML Policy］割り当てページが開きます。

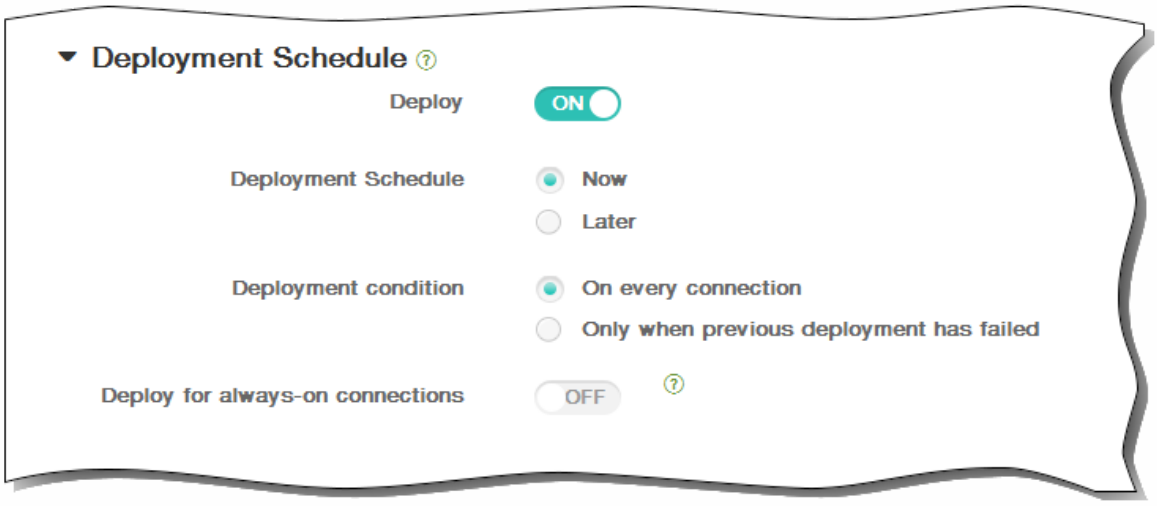
10. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



11. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。

3. ［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。
4. ［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。
5. ［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。

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。



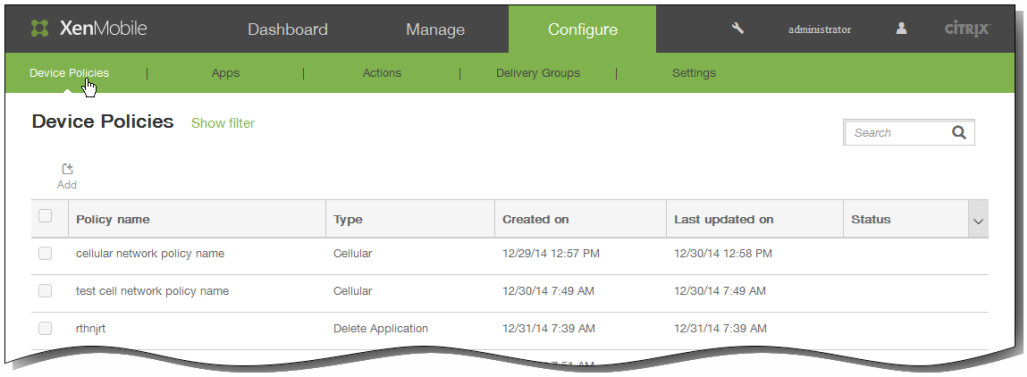
12. ［Save］をクリックしてポリシーを保存します。

アプリケーションアンインストールデバイスポリシー

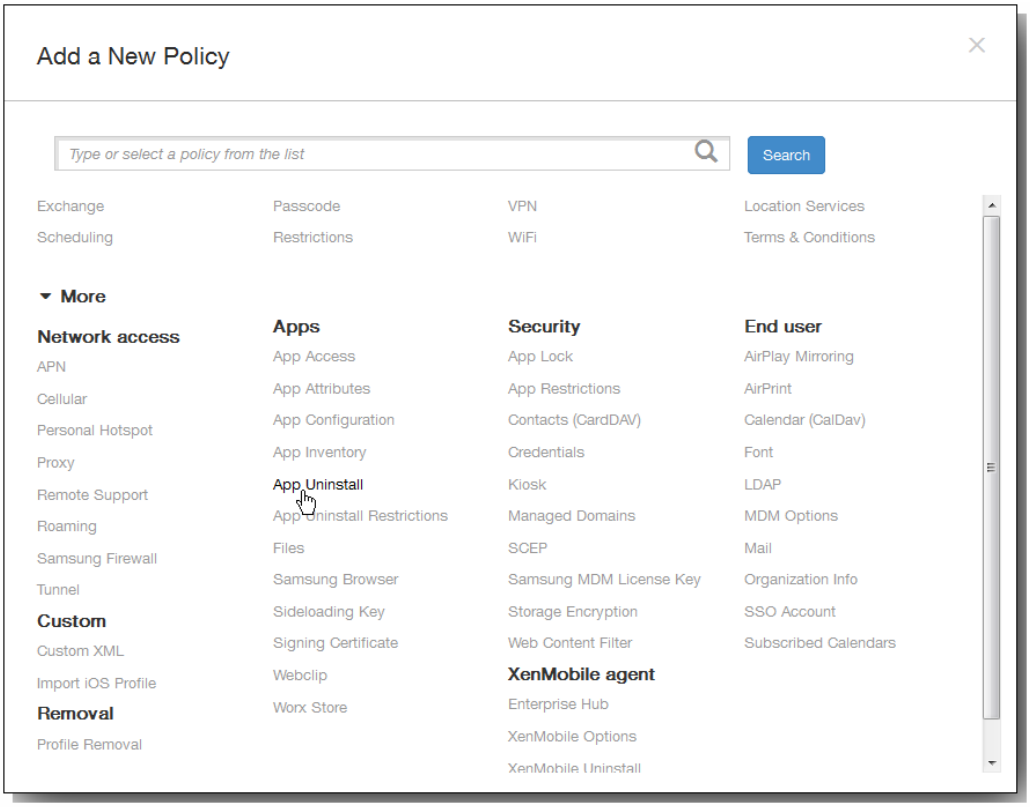
May 10, 2016

iOS、Android、Samsung KNOX、およびWindows 8.1タブレット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。

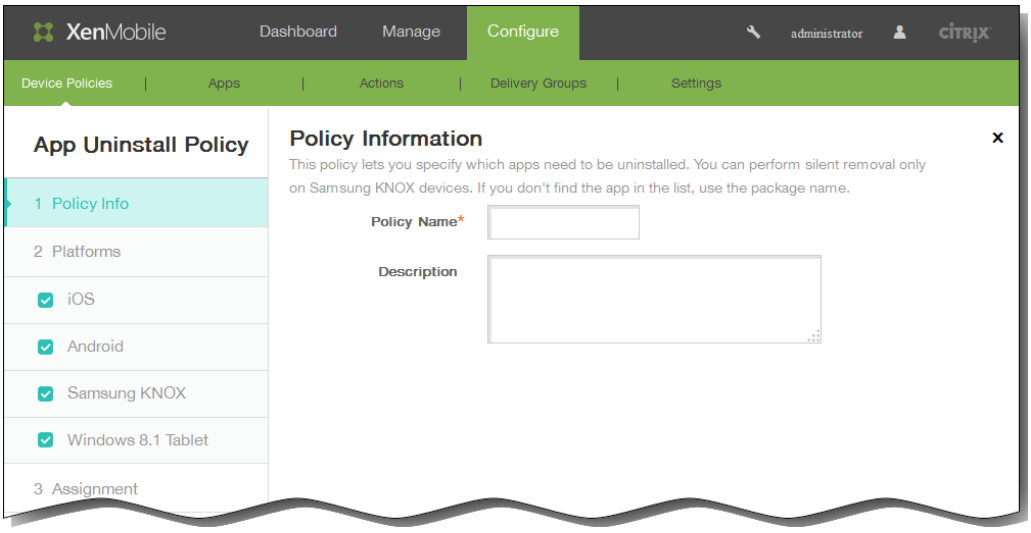
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。［Device Policies］ページで、［Add］をクリックします。



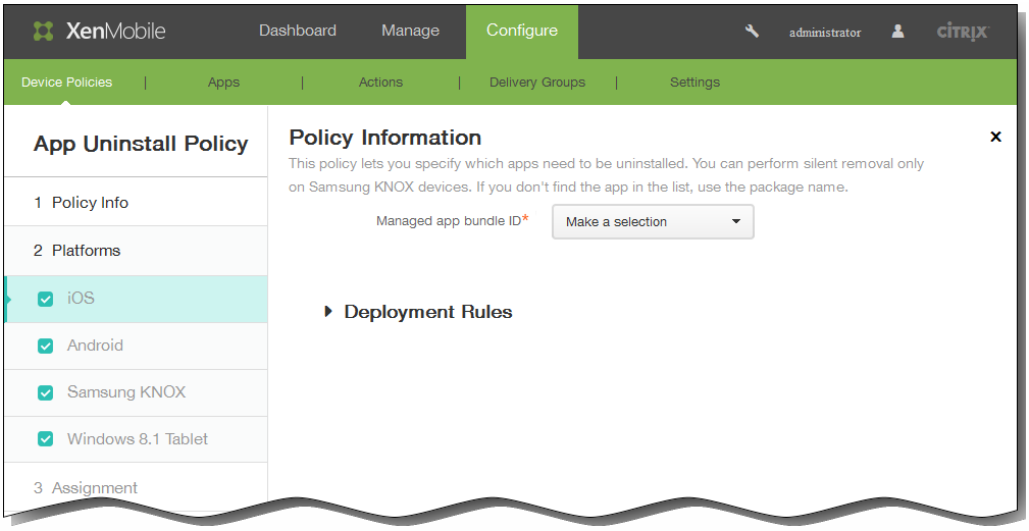
2. ［Add a New Policy］ダイアログボックスで、［More］をクリックして、［Apps］の下の［App Uninstall］をクリックします。



3. ［App Uninstall Policy］情報ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
   3. ［Next］をクリックします。

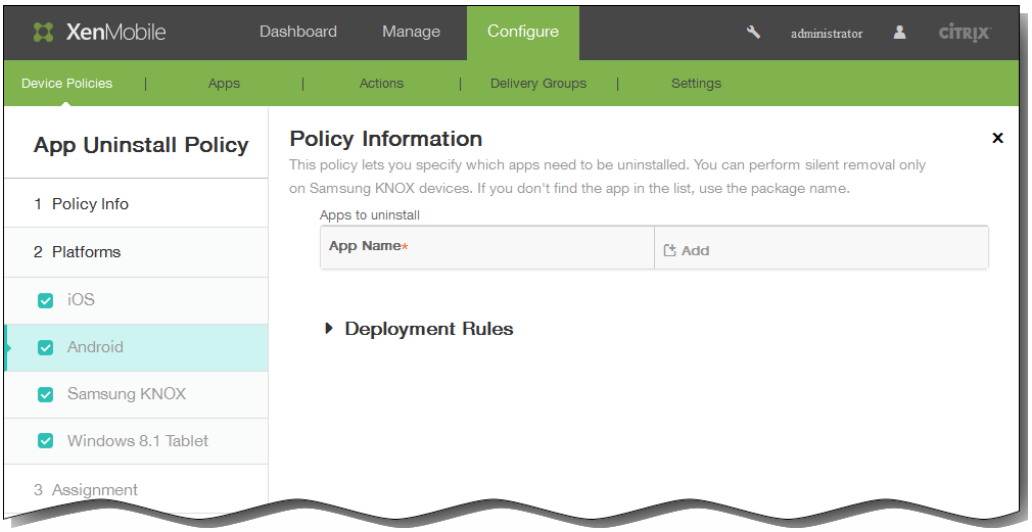


4. ［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォーム構成パネルが開きます。 ［Platforms］の下で、追加するプラットフォームをオンにして、追加しないプラットフォームをオフにします。



5. 選択したプラットフォームに基づいて、次の設定を構成します。
   1. ［iOS］を選択した場合は、［Managed app bundle ID］ボックスの一覧で、既存のアプリケーションを選択するか、［Add new］をクリックします。

      注：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。
   2. ［Android］、［Samsung KNOX］、または［Windows 8.1 Tablet］を選択した場合は、以下の手順に従います。



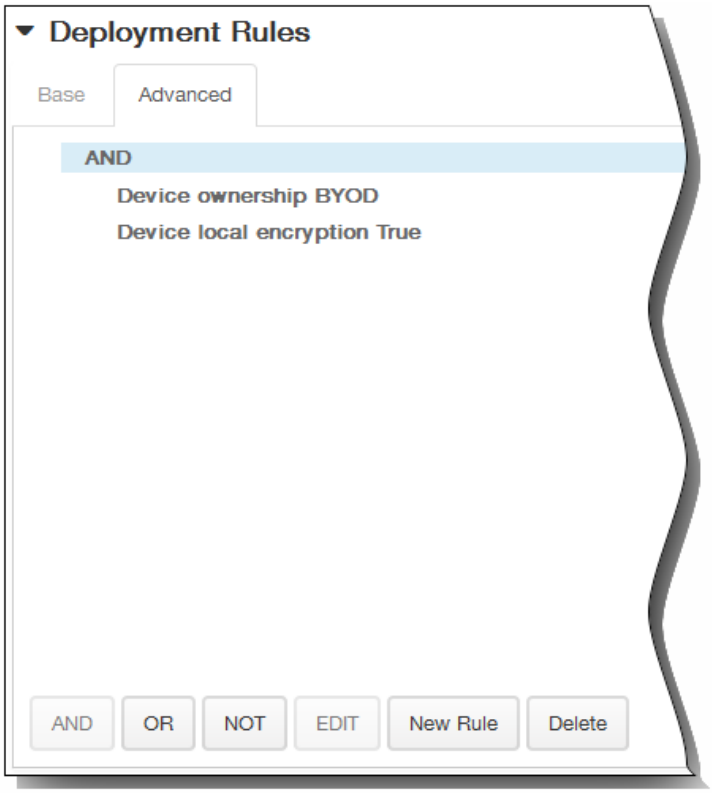
［Apps to uninstall］の下で［Add］をクリックして、以下の操作を行います。

1. App name：一覧で既存のアプリケーションを選択するか、［Add new］をクリックして新しいアプリケーション名を入力します。
   注：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。
2. ［Add］をクリックしてアプリケーションを追加するか、［Cancel］をクリックしてアプリケーションの追加を取り消します。

3. 追加するカスタムキーごとに手順i.およびii.追加するアプリケーションごとに手順i.およびii.を繰り返します。
   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。

6. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

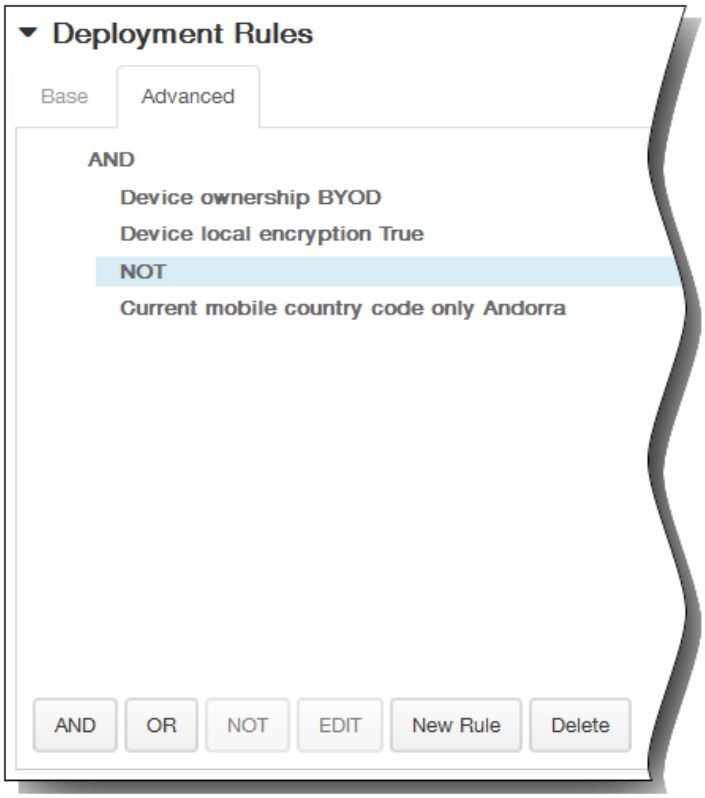
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
   1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］タブをクリックし、ブール値オプションを使用して規則を組み合わせます。



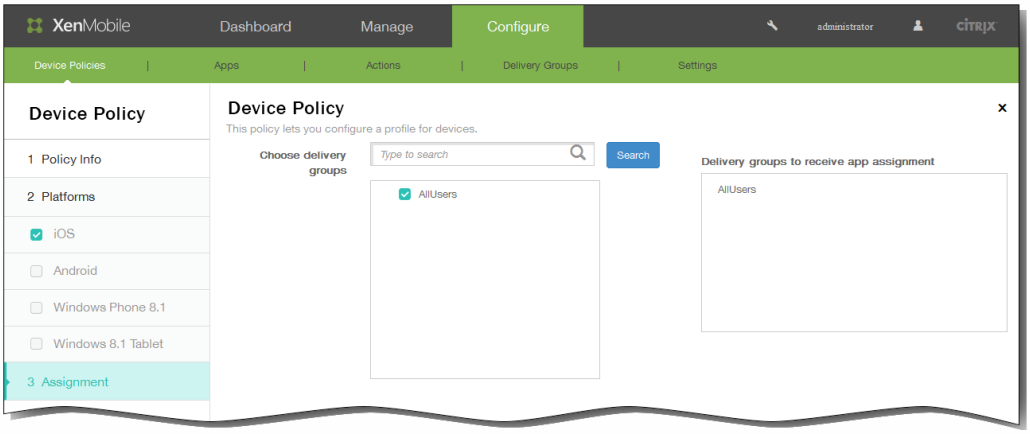
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



7. ［Next］をクリックします。 ［App Uninstall 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右側の［Delivery groups to receive app assignment］一覧に表示されます。



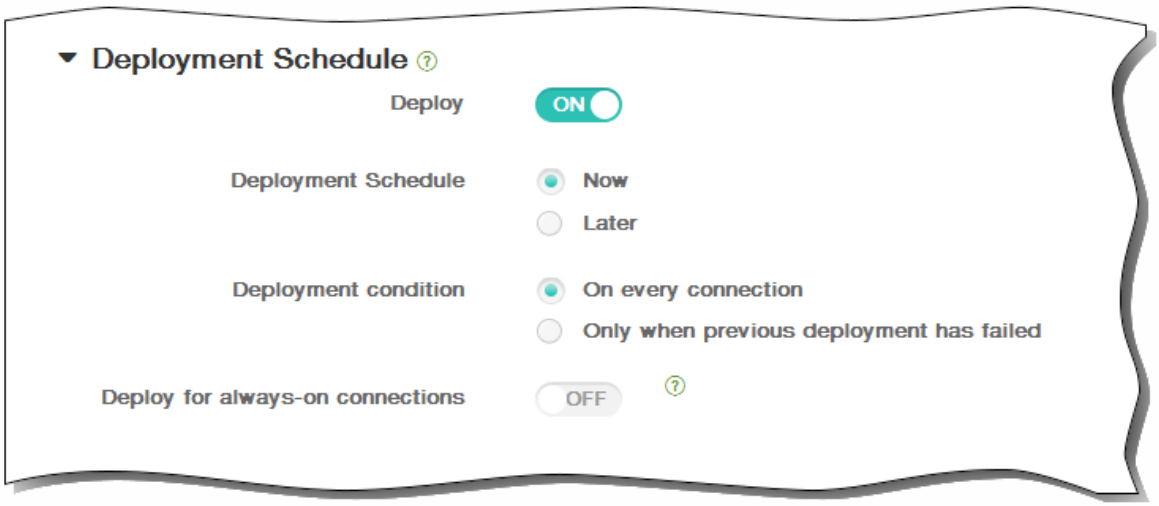
9. ［Deployment Schedule］を展開して以下の設定を構成します。
   1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
   2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
   3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
   4. ［Deployment 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。

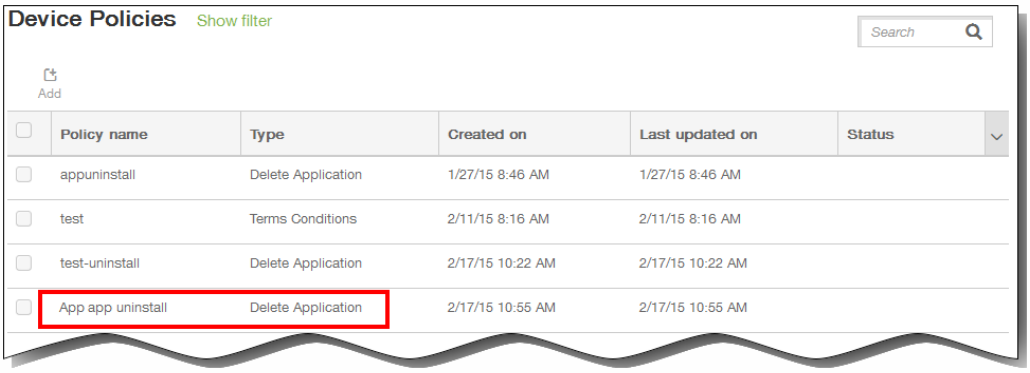
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



10. ［Save］をクリックしてポリシーを保存します。 ［Device Policies］ページに表示される、追加したポリシーの［Type］列には、［Delete Application］と表示されます。

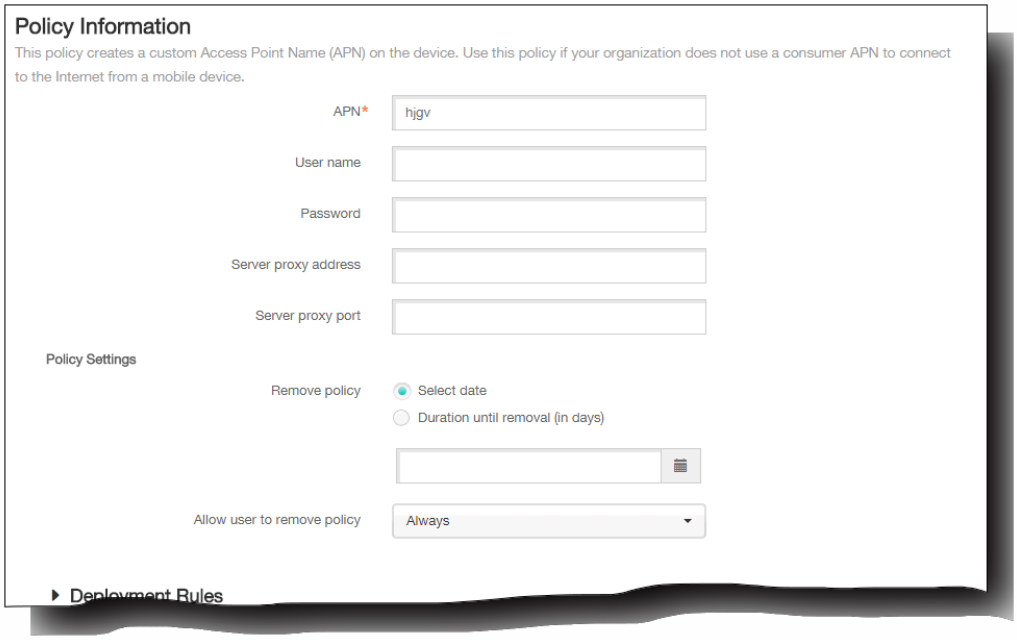


APNポリシーを追加するには

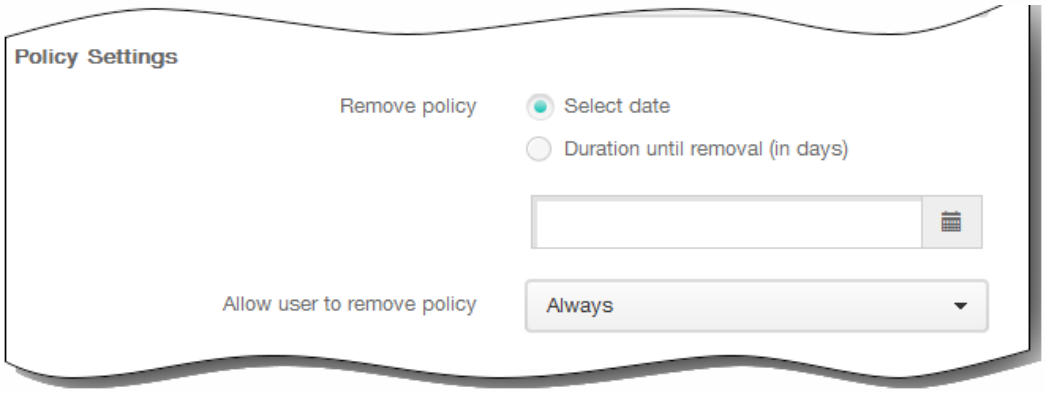
May 10, 2016

このポリシーを使用して、iOS、Android、またはSamsung KNOXデバイスのカスタムアクセスポイント名（APN）を構成できます。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。

1. XenMobileコンソールで、［Configure］、［Device Policies］、［Add］の順にクリックします。
2. ［Add a New Policy］ページで［More］をクリックして、［Network Access］の下の［APN］をクリックします。
3. ポリシーに含めるプラットフォームを選択します。 選択したプラットフォームの構成ページが手順5.で表示されます。
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。 最初のプラットフォームの情報ページが開きます。
6. iOSプラットフォームを選択した場合は、［iOS Platform Information］ページで、以下の操作を行います。

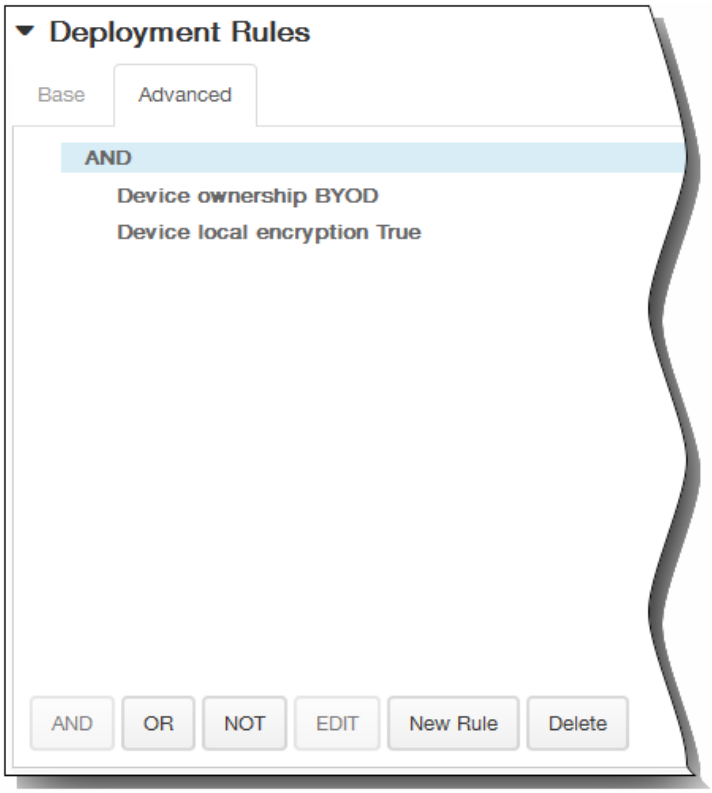


   1. APN。 アクセスポイントの名前を入力します。
   2. User name。 このAPNのユーザー名を指定する文字列です。 ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
   3. Password。 このAPNのユーザーのパスワードです。 難読化のために、パスワードはエンコードされます。 ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
   4. Server proxy address。 APNプロキシのIPアドレスまたはURLです。
   5. Server proxy port。 APNプロキシのポート番号です。
7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

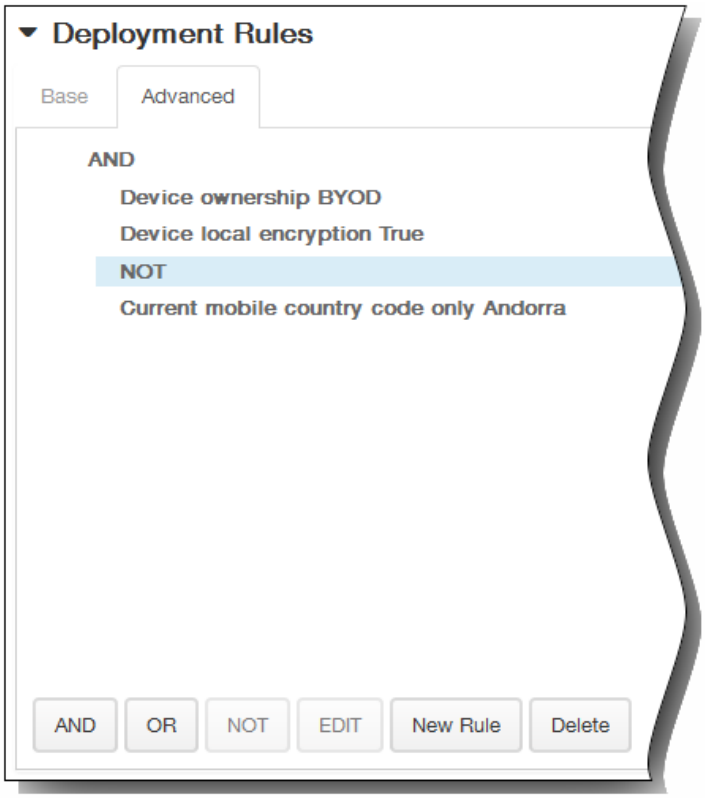
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



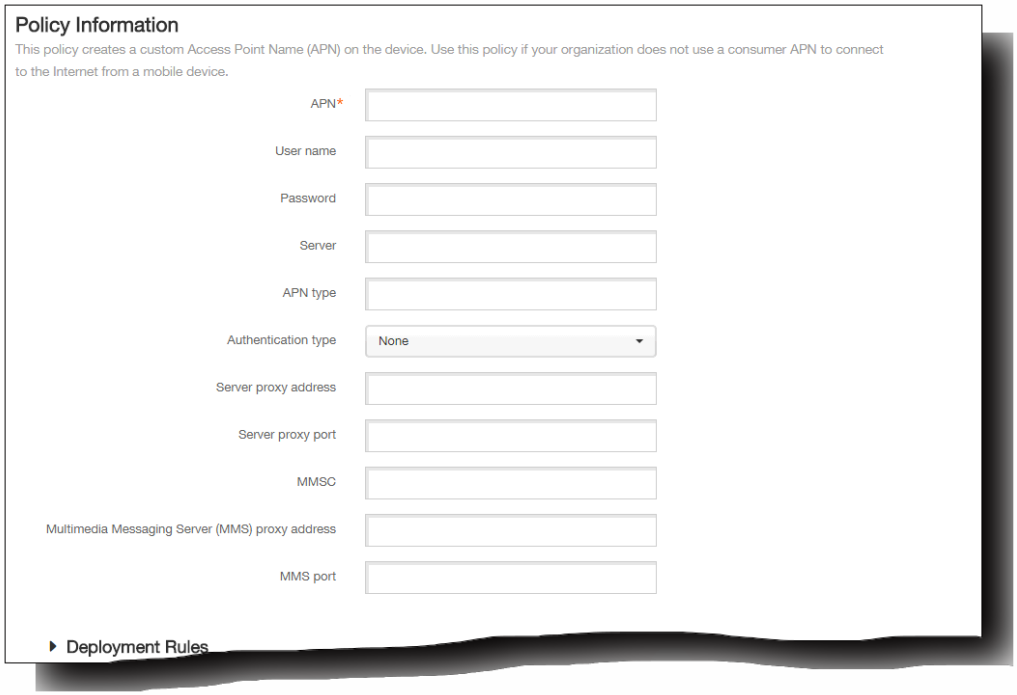
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. AndroidまたはSamsung KNOXプラットフォームを選択した場合は、プラットフォームの情報ページで、以下の操作を行います。



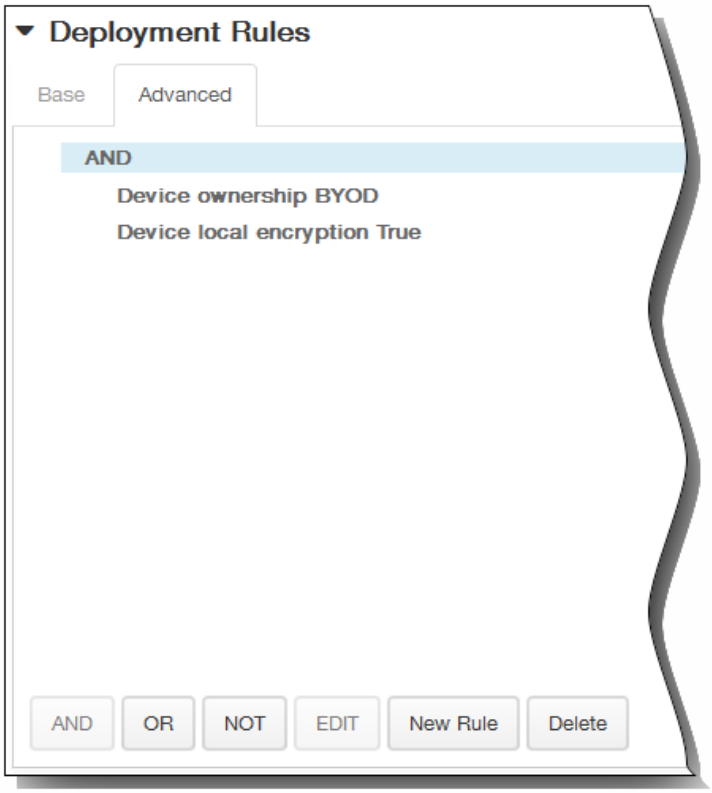
1. APN。 アクセスポイントの名前を入力します。
2. User name。 このAPNのユーザー名を指定する文字列です。 ユーザー名がない場合、デバイスでは、プロファイルのイ

ンストール中に文字列の入力が求められます。

3. Password。 このAPNのユーザーのパスワードです。 難読化のために、パスワードはエンコードされます。 ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
4. Server。 この設定はスマートフォンより前のもので、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。
5. 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。
6. Authentication type。 ［PAP］、［CHAP］、［PAP or CHAP］のいずれかにする必要があります。 デフォルトは［None］です。
7. Server proxy address。 APNプロキシのIPアドレスまたはURLです。
8. Server proxy port。 APNプロキシのポート番号です。
9. MMSC。 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）。
10. Multimedia Messaging Server (MMS) proxy address。 これは、MMSトラフィック用のHTTPプロキシサーバーです。
11. MMS port。 MMSプロキシによって使用されるポートです。

13. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

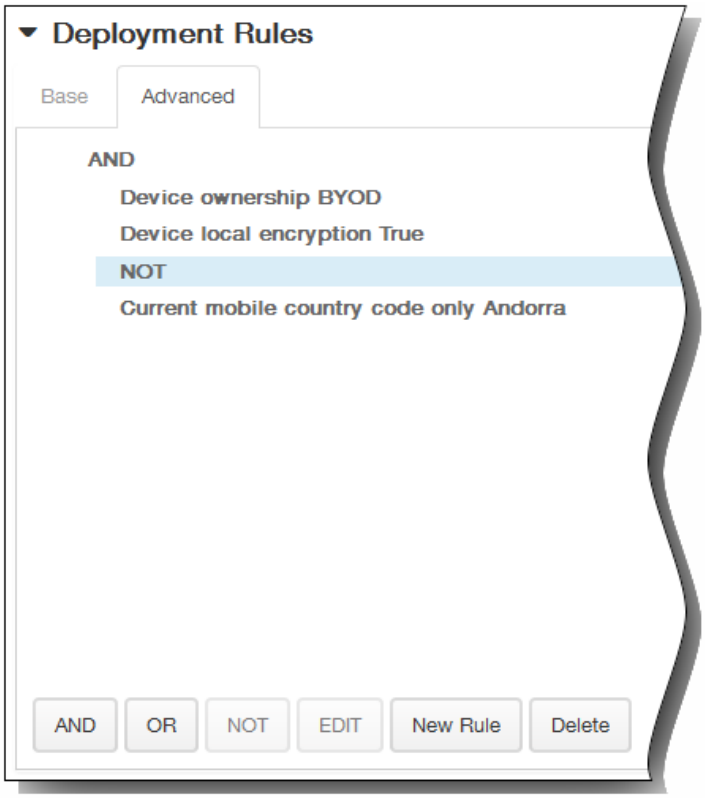
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
   1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］タブをクリックし、ブール値オプションを使用して規則を組み合わせます。



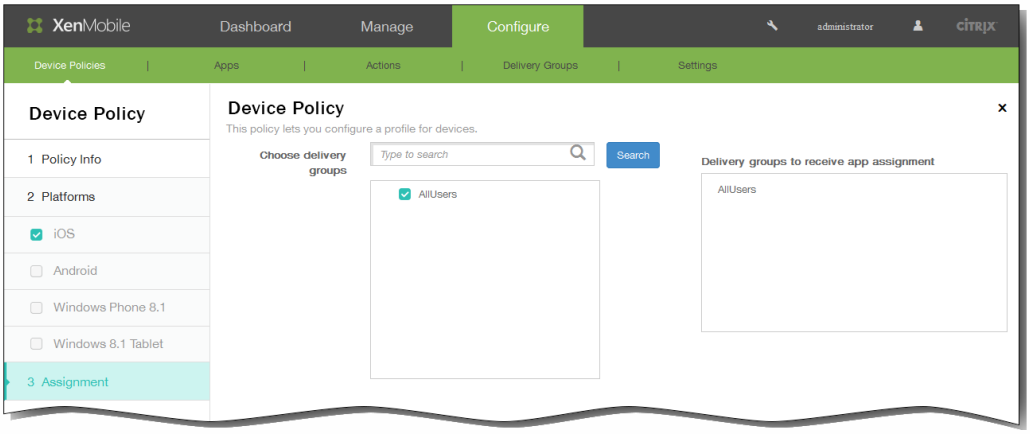
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



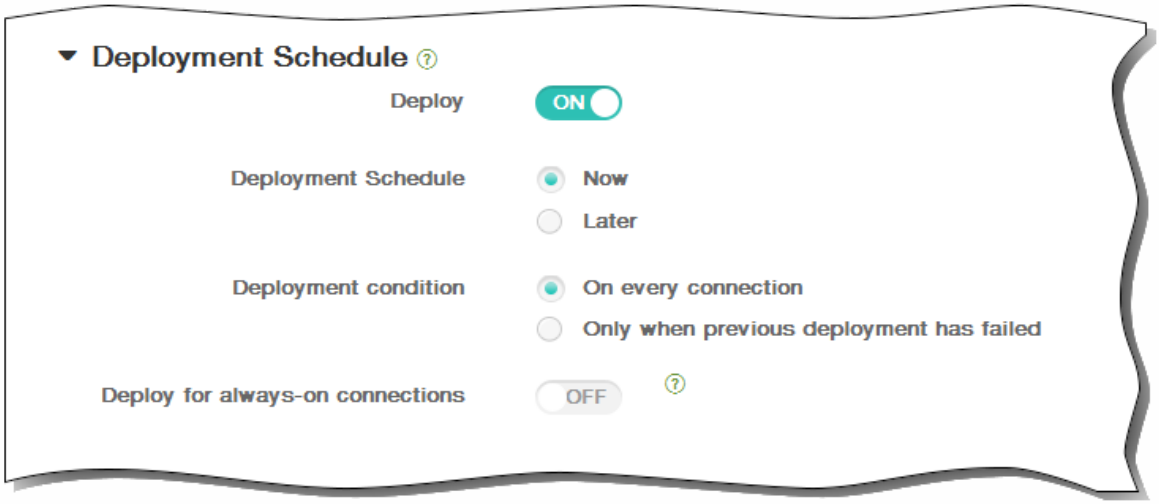
14. AndroidおよびSamsung KNOXプラットフォームを両方選択した場合は、手順8.を繰り返して［Samsung KNOX Platform Information］ページで必要な項目を入力し、［Next］をクリックします。 ［APN Policy Assignment］ページが開きます。
15. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



16. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。

3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



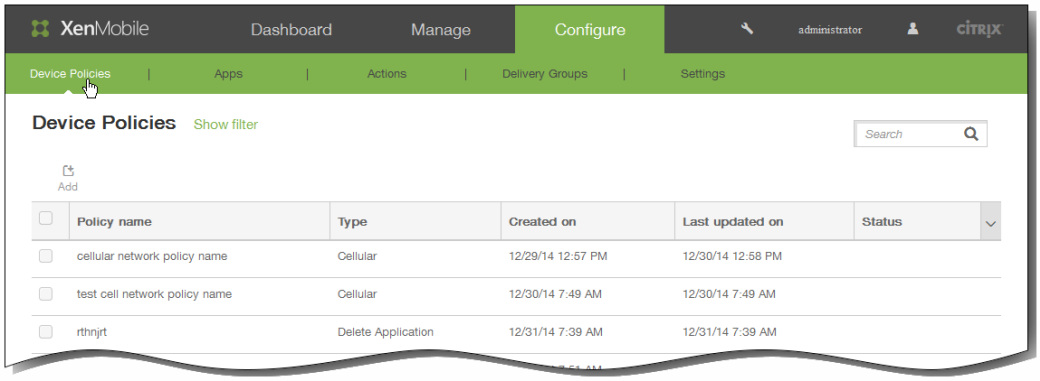
17. ［Save］をクリックしてポリシーを保存します。

iOSのモバイルデバイスポリシーを追加するには

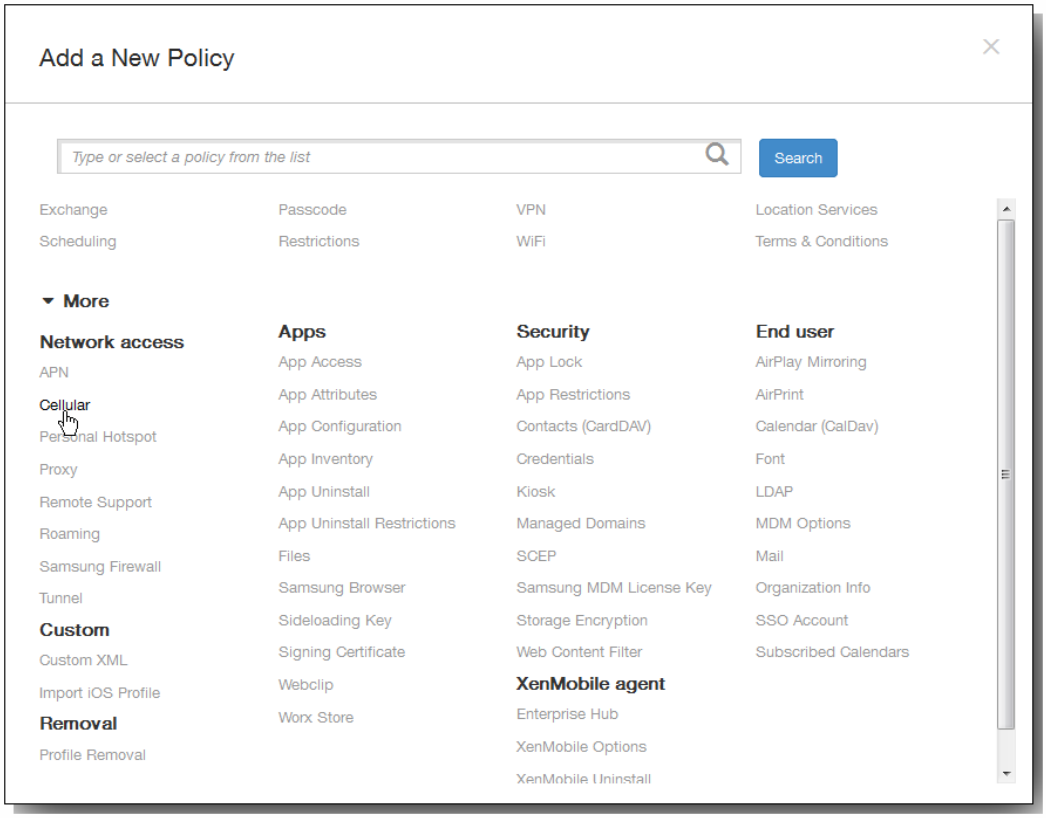
May 10, 2016

このポリシーを使用すると、iOSデバイスのモバイルネットワーク設定を構成できます。

1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。

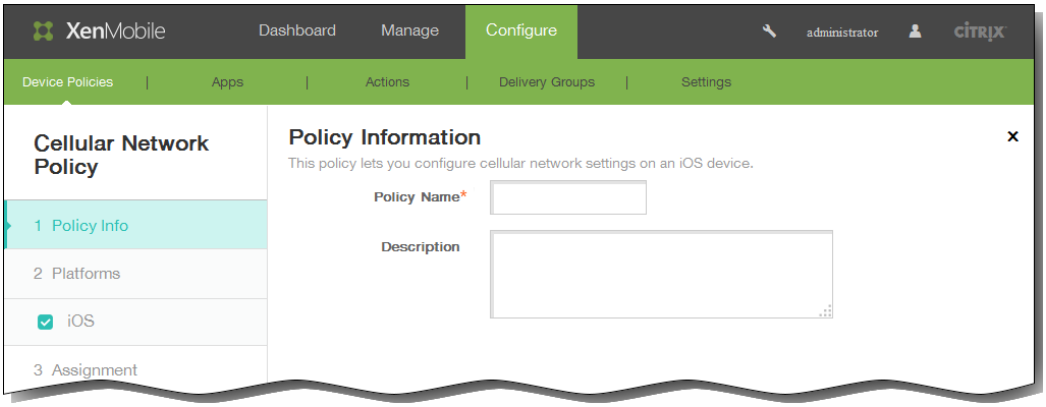


2. ［Add］をクリックします。
［Add a New Policy］ページが開きます。

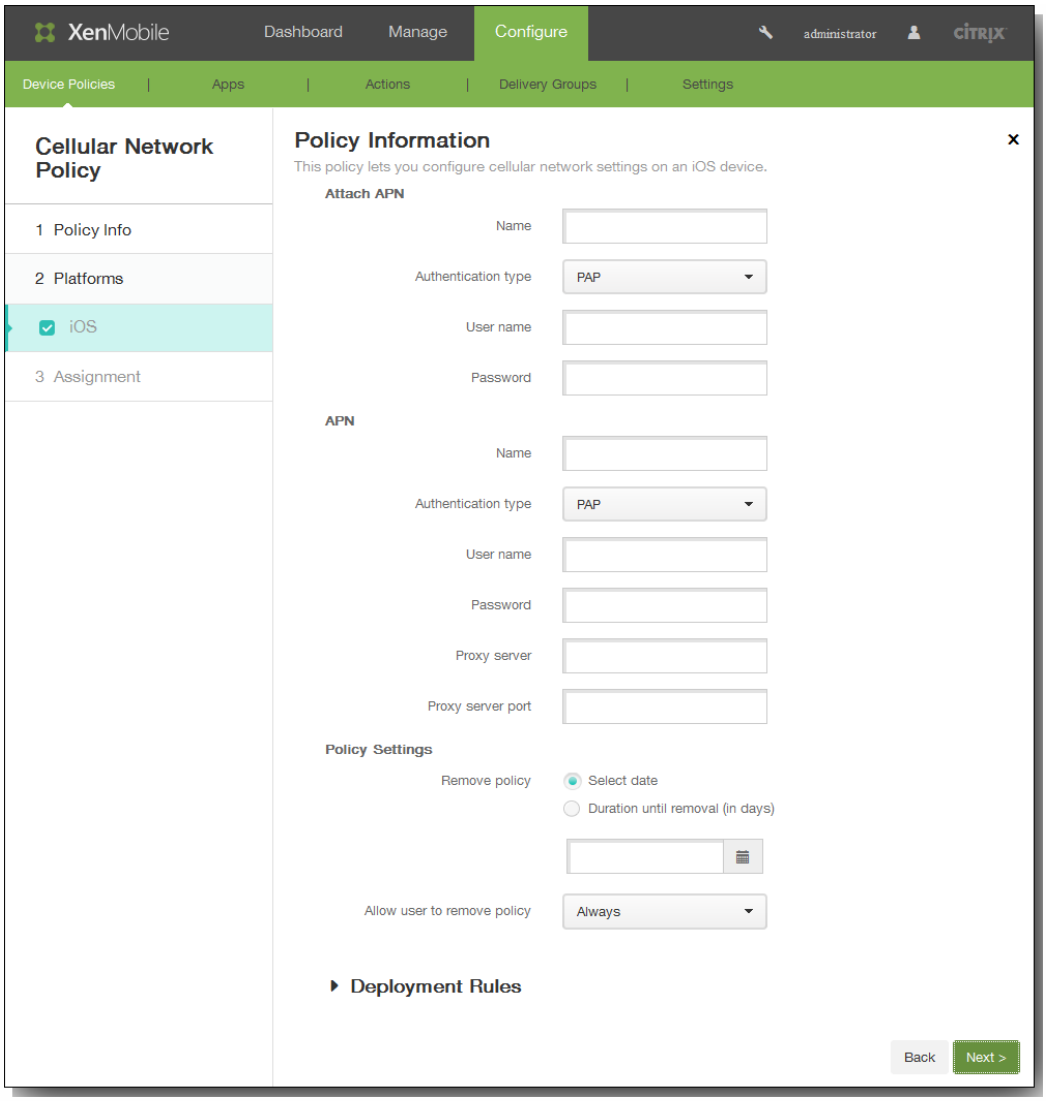


3. ［Add a New Policy］ページで［More］をクリックして、［Network Access］の下の［Cellular］をクリックします。

［Cellular Network Policy］情報ページが開きます。



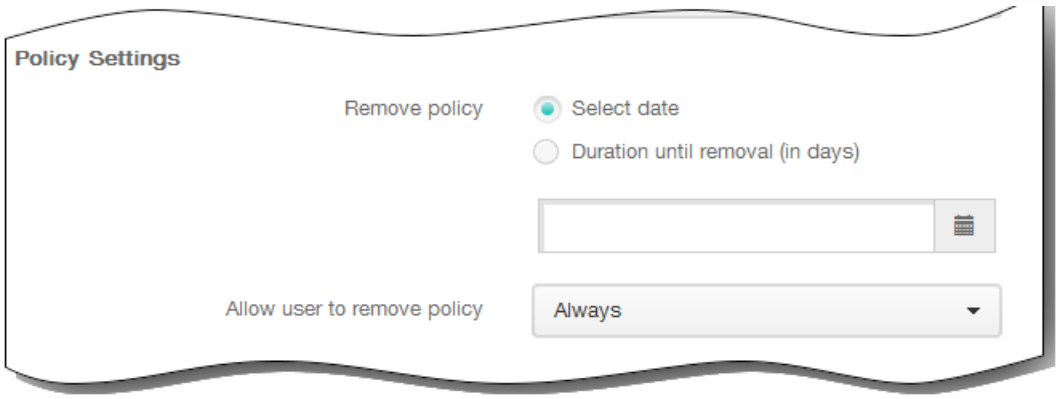
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform Information］ページが開きます。



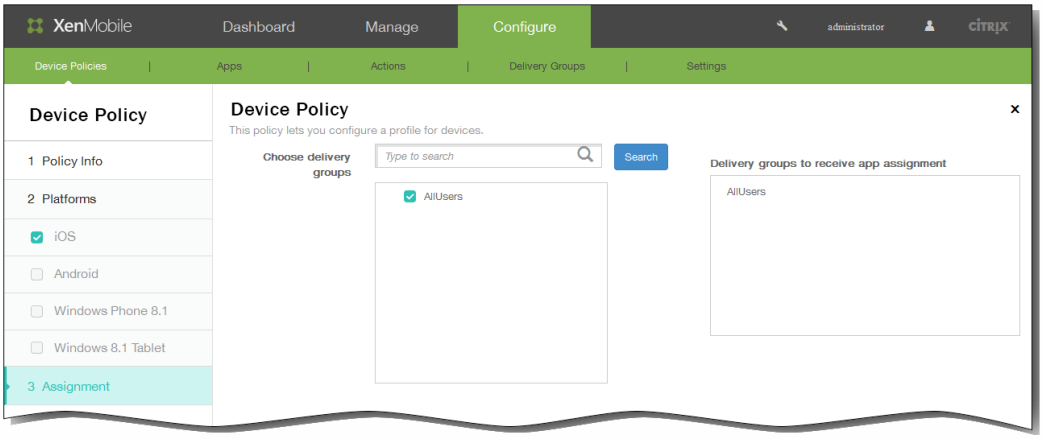
6. ［iOS Platform Information］ページの **［Attach APN］** の下で、以下の情報を入力します。
   1. Name：この構成の名前を入力します。
   2. Authentication type：一覧から、［CHAP］（Challenge-Handshake Authentication Protocol：チャレンジハンドシェイク認証プロトコル）または［PAP］（Password Authentication Protocol：パスワード認証プロトコル）のいずれかを選択します。 デフォルトは［PAP］です。
   3. User name：認証に使用するユーザー名を入力します。
   4. Password：認証に使用するパスワードを入力します。

   ［APN］ の下で以下を入力します。
   1. 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。
   2. 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。
   3. User name：認証に使用するユーザー名を入力します。
   4. Password：認証に使用するパスワードを入力します。
   5. Proxy server：プロキシサーバーのネットワークアドレスを入力します。
   6. Proxy server port：プロキシサーバーのポートを入力します。
7. ［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。
8. ［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。

9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。

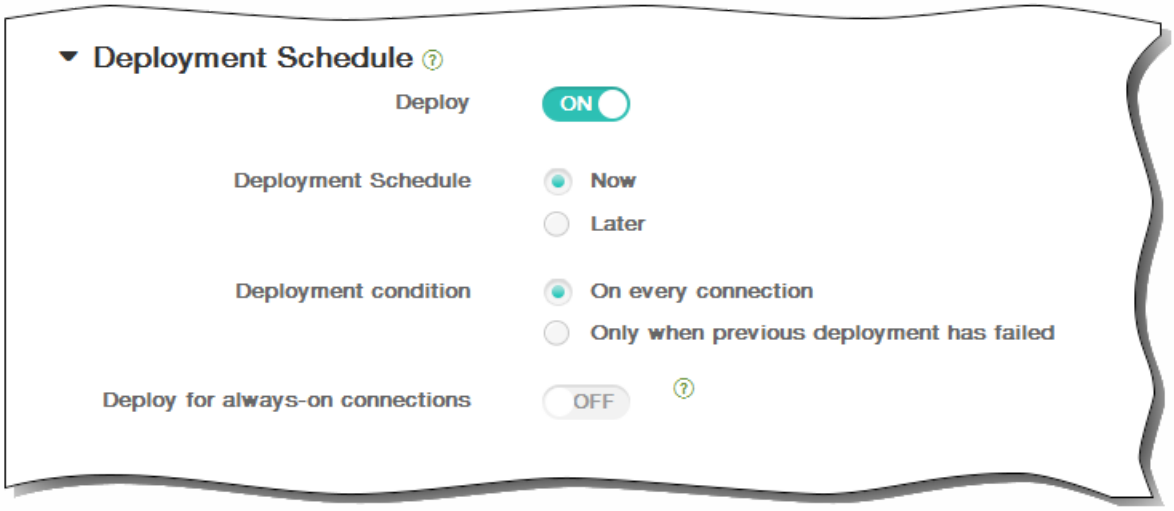


11. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



12. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［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。
    4. ［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。
    5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
    注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



13. ［Save］をクリックしてポリシーを保存します。

Windows Phone 8.1のEnterprise Hubデバイスポリシーを追加するには

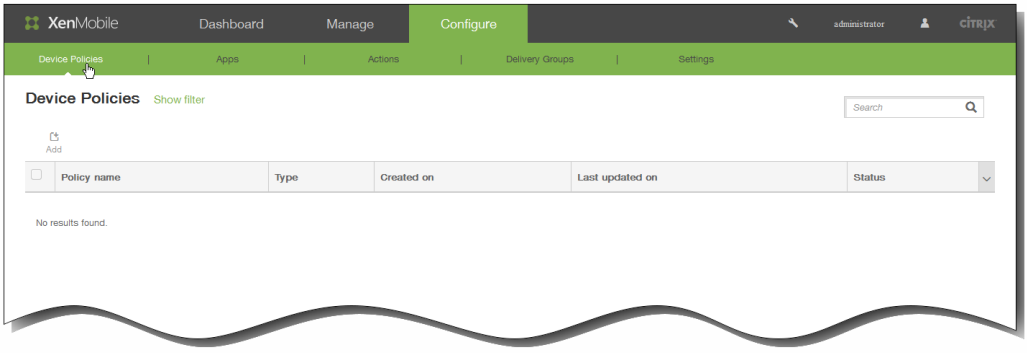
May 10, 2016

Windows Phone 8.1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。

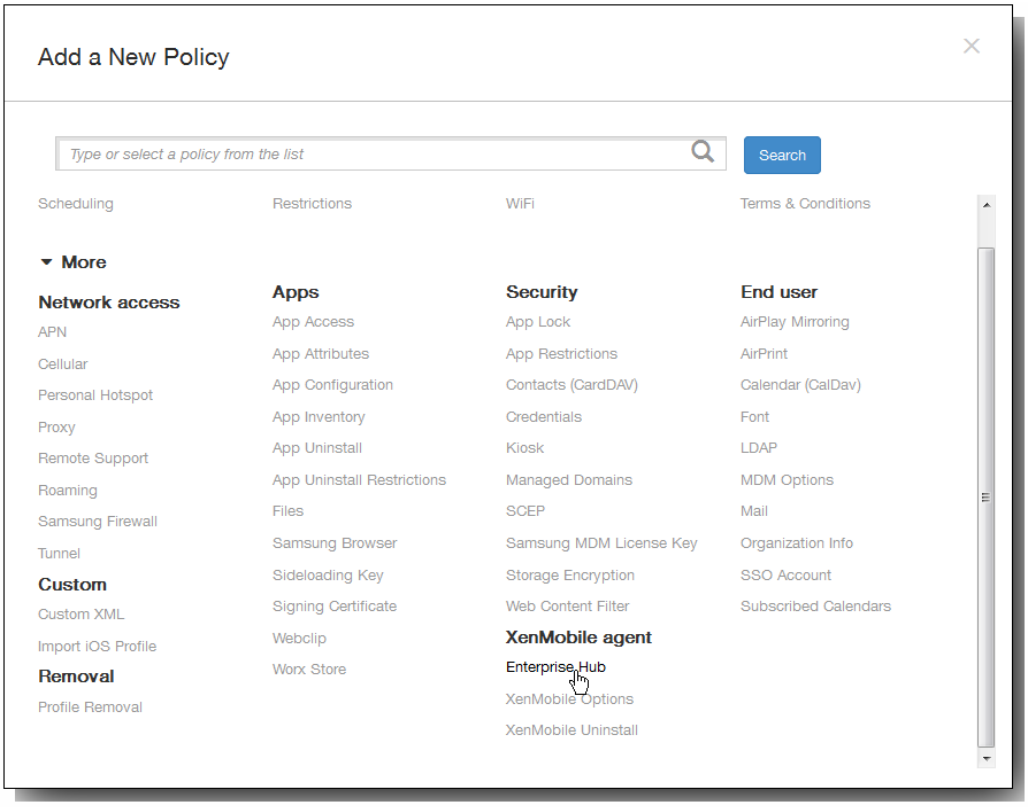
このポリシーを作成するには以下が必要です。

- 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

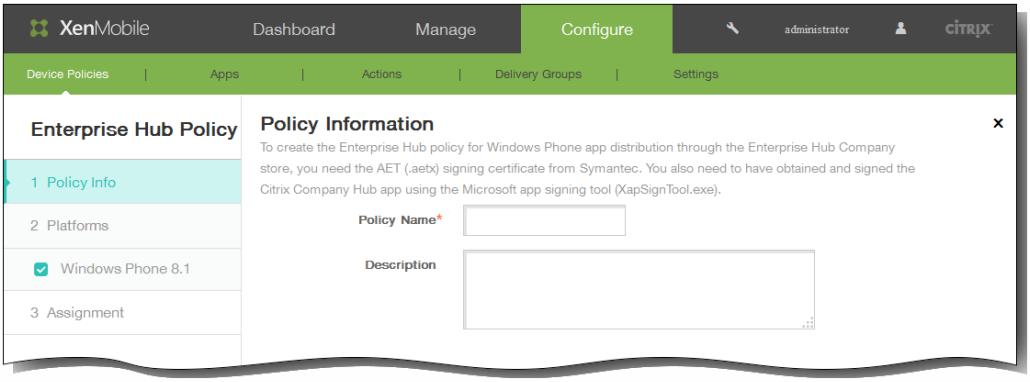
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



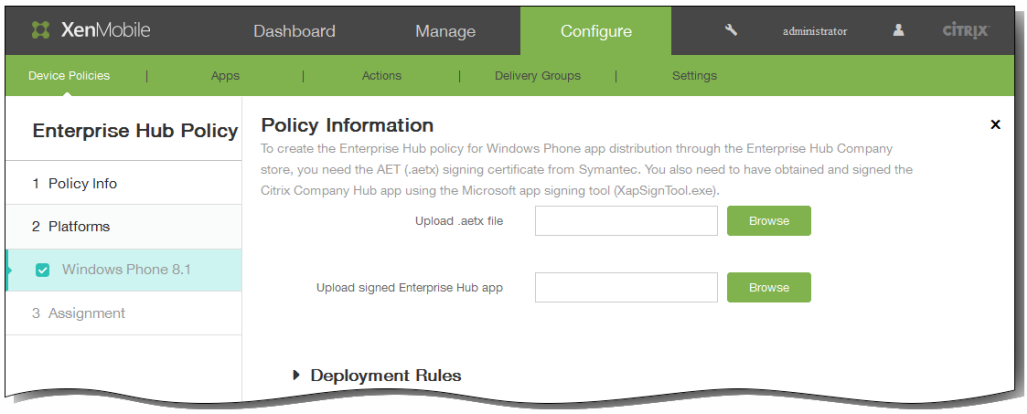
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



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

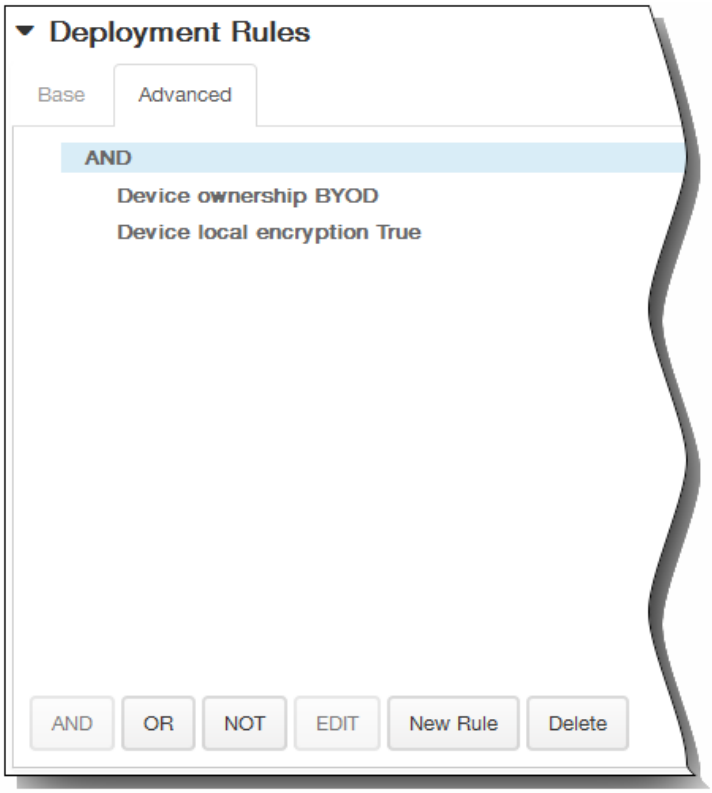


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：必要に応じて、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Windows Phone 8.1］プラットフォームページが開きます。



6. 次の設定を構成します。
   1. Upload .aetx file：.aetxファイルの場所を参照して、ファイルを選択します。
   2. Upload signed Enterprise Hub app：Enterprise Hubアプリケーションの場所を参照して、アプリケーションを選択します。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

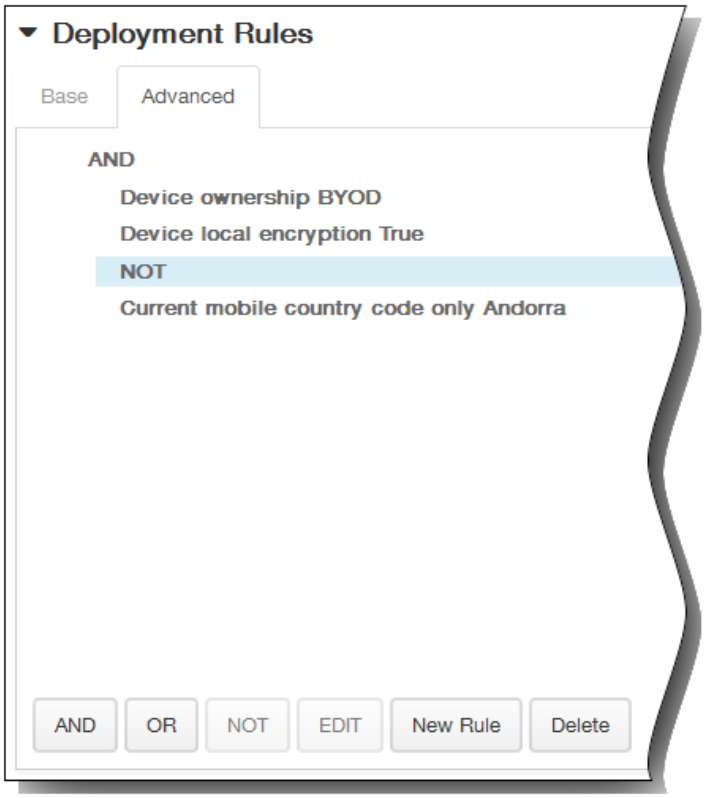
   1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
      1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
      2. ［New Rule］をクリックして条件を定義します。
      3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
      4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
   2. ［Advanced］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。



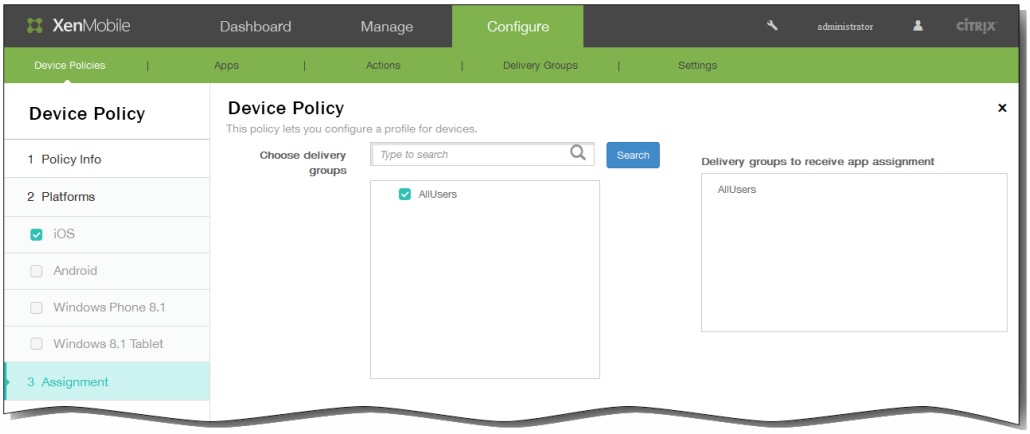
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Enterprise Hub Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



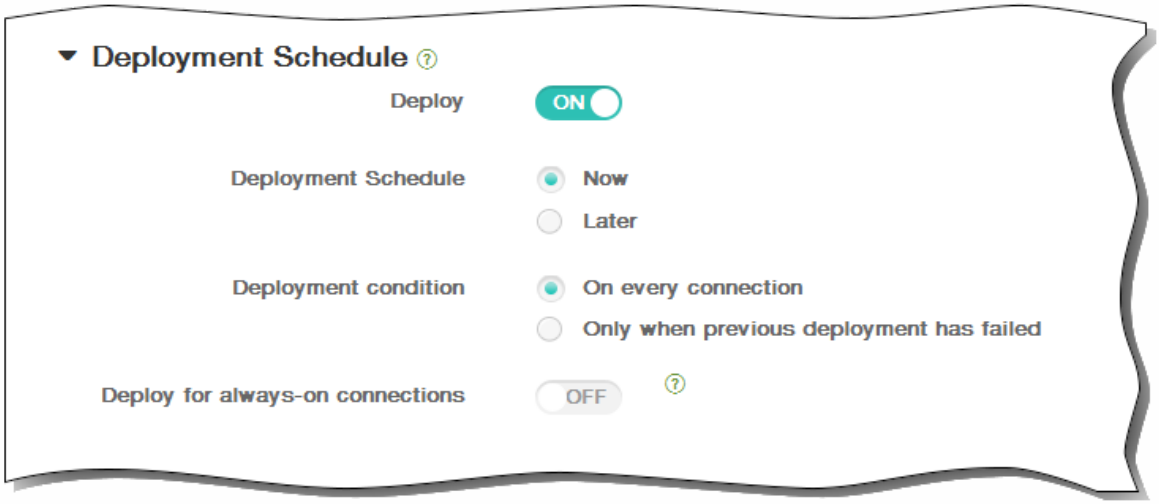
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

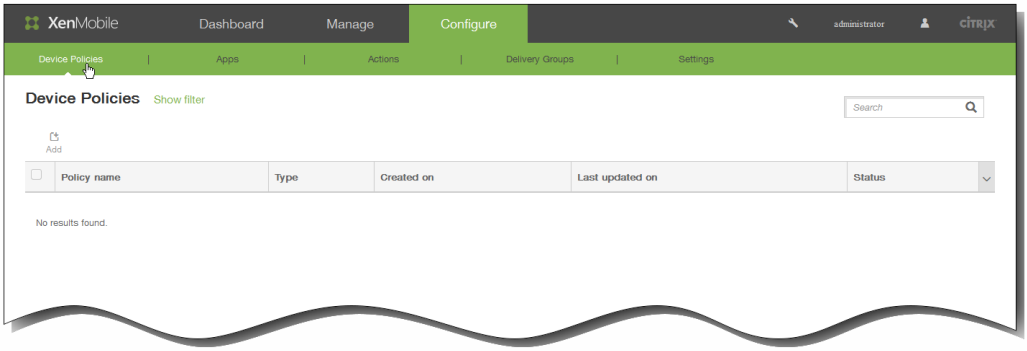
Microsoft Exchange ActiveSyncデバイスポリシー

May 10, 2016

Exchange ActiveSyncデバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchangeでホストされている会社のメールにアクセスできるようにすることができます。iOS、Android HTC、Android TouchDown、Samsung SAFE、Samsung KNOX、Windows Phone 8.1に対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、以下のトピックで説明しています。

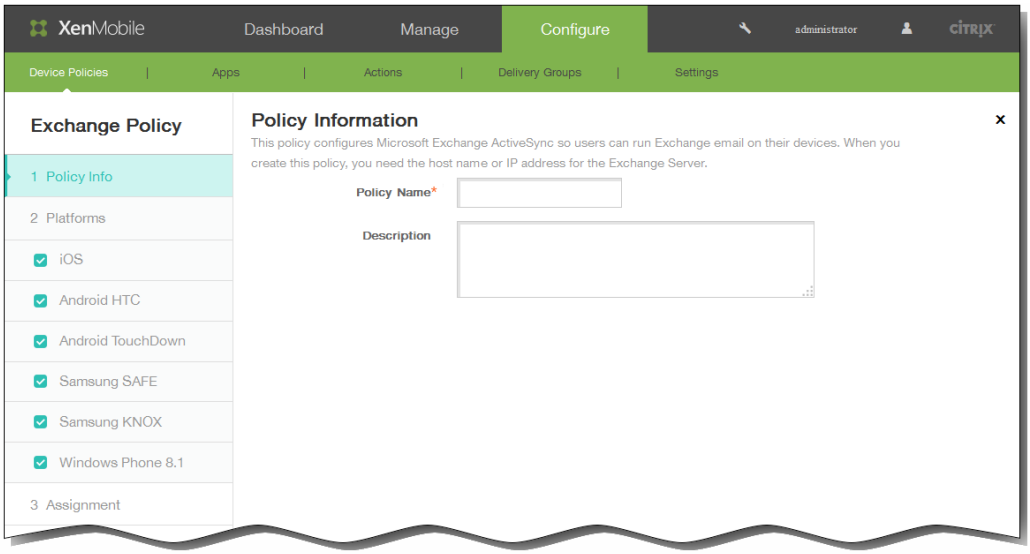
このポリシーを作成するには、事前にExchange Serverのホスト名またはIPアドレスを把握しておく必要があります。

1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。

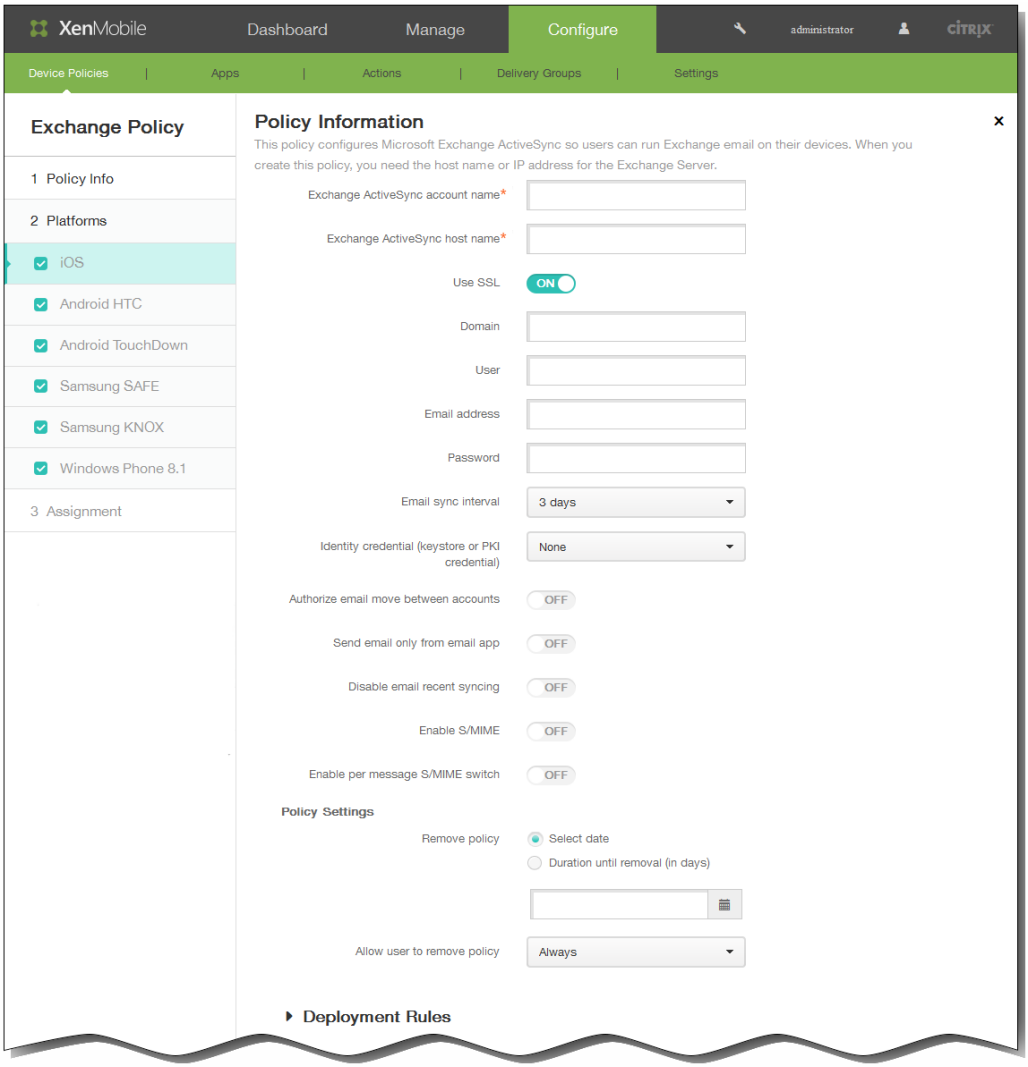


2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add New Policy］ダイアログボックスが開きます。

3. ［Exchange］をクリックします。 ［Exchange Policy］情報ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォーム構成パネルが開きます。



6. ［Platforms］の下で、追加するプラットフォームをオンにします。
   - ［iOS］を選択した場合は、次の設定を構成します。

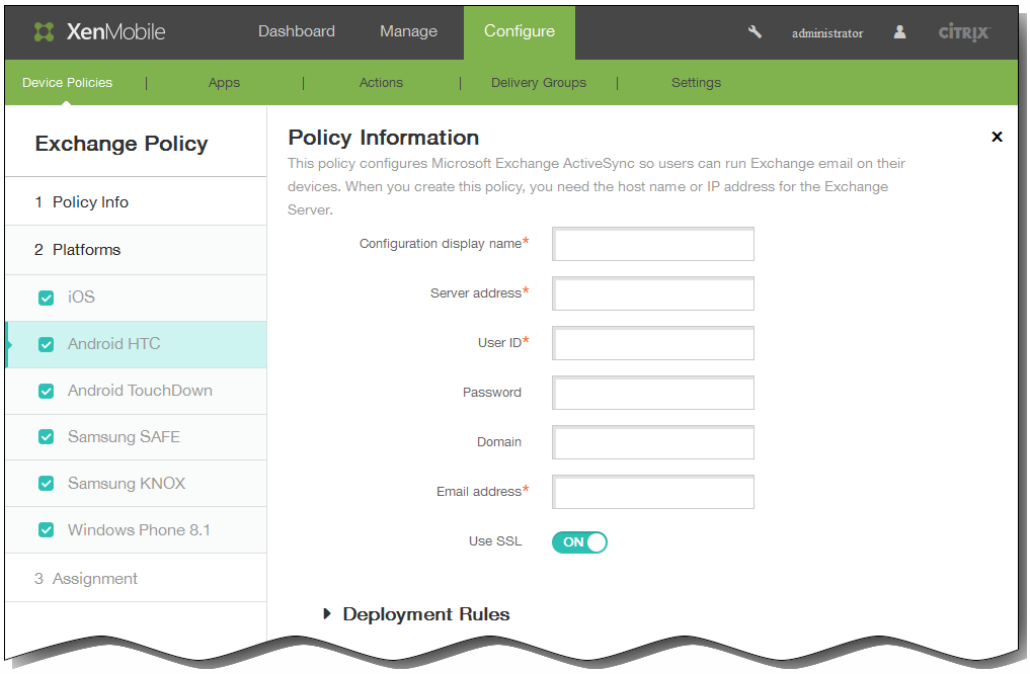
     Configuration display name：ユーザーのデバイスで表示される、このポリシーの名前を入力します。

     Server address：Exchange Serverのホスト名またはIPアドレスを入力します。

     User ID：Exchangeユーザーアカウントのユーザー名を指定します。
     注：このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
     Password：任意で、Exchangeユーザーアカウントのパスワードを入力します。

     Domain：Exchange Serverがあるドメインを入力します。
     注：このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
     Email address：ユーザーの完全なメールアドレスを指定します。
     注：このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
     Use SSL：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは［On］です。

- ［Android HTC］を選択した場合は、次の設定を構成します。



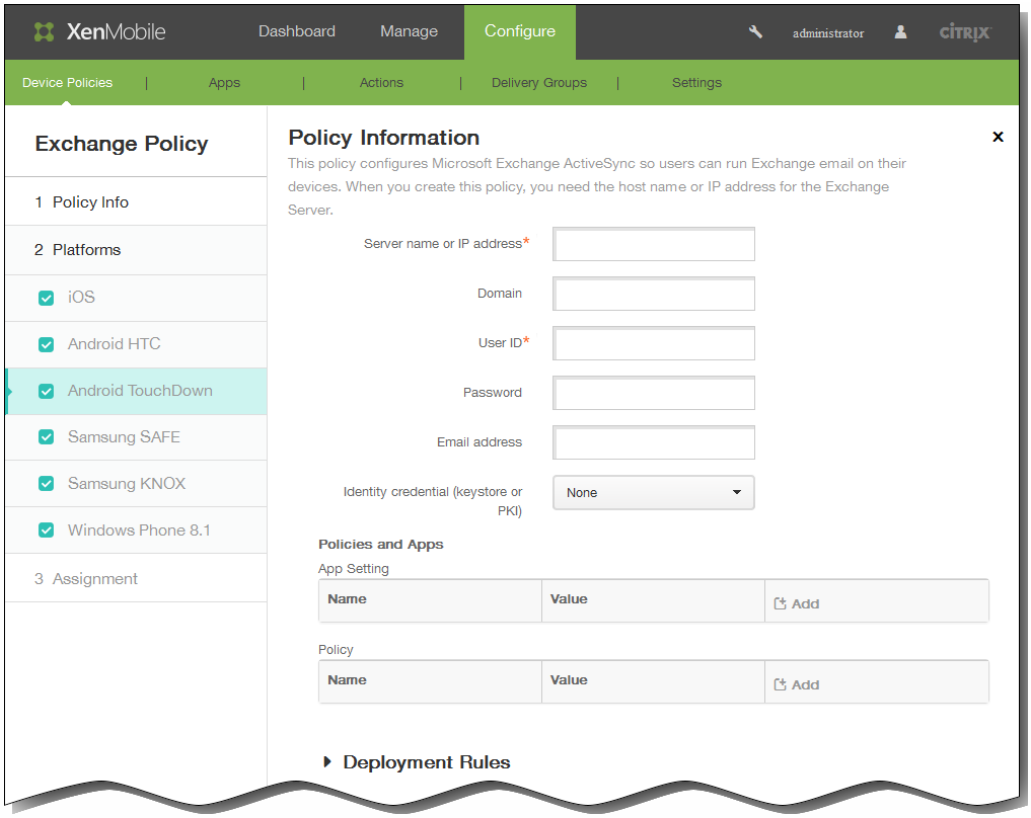
Configuration display name：ユーザーのデバイスで表示される、このポリシーの名前を入力します。

Server address：Exchange Serverのホスト名またはIPアドレスを入力します。

User ID：Exchangeユーザーアカウントのユーザー名を指定します。
注：このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
Password：任意で、Exchangeユーザーアカウントのパスワードを入力します。

Domain：Exchange Serverがあるドメインを入力します。
注：このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
Email address：ユーザーの完全なメールアドレスを指定します。
注：このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
Use SSL：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは［On］です。

- ［Android TouchDown］を選択した場合は、次の設定を構成します。



Server name or IP address：Exchange Serverのホスト名またはIPアドレスを入力します。

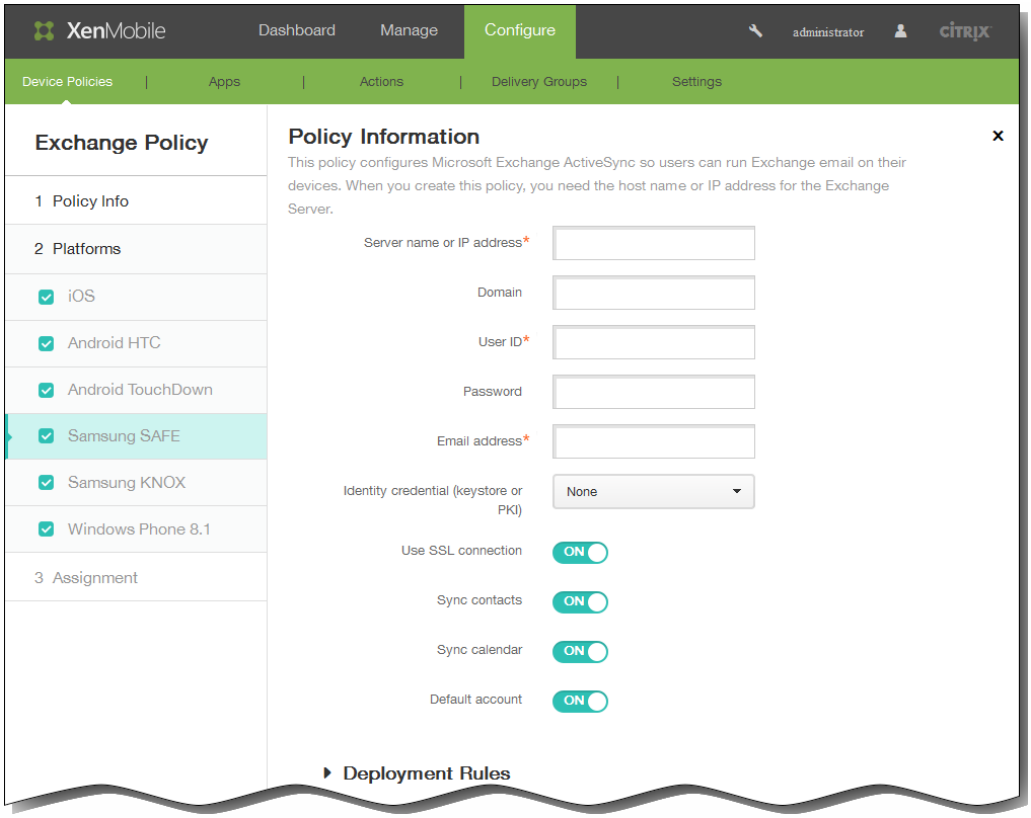
Domain：Exchange Serverがあるドメインを入力します。
注：このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
User ID：Exchangeユーザーアカウントのユーザー名を指定します。
注：このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
Password：任意で、Exchangeユーザーアカウントのパスワードを入力します。

Email address：ユーザーの完全なメールアドレスを指定します。
注：このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
Identity credential（keystore or PKI）：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。

App Setting：オプションで、このポリシーのTouchDownアプリケーション設定を追加します。

Policy：オプションで、このポリシーのTouchDownポリシーを追加します。

- ［Samsung SAFE］または［Samsung KNOX］を選択した場合は、次の設定を構成します。



Server name or IP address：Exchange Serverのホスト名またはIPアドレスを入力します。

Domain：Exchange Serverがあるドメインを入力します。
注：このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
User ID：Exchangeユーザーアカウントのユーザー名を指定します。
注：このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
Password：任意で、Exchangeユーザーアカウントのパスワードを入力します。

Email address：ユーザーの完全なメールアドレスを指定します。
注：このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
Identity credential（keystore or PKI）：XenMobileのIDプロバイダーを構成している場合、オプションとして、ボックスの一覧でID資格情報を選択します。このフィールドは、Exchangeでクライアント証明書認証が必要な場合にのみ必要です。

Use SSL connection：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは［On］です。

Sync contacts：デバイスとExchange Serverの間でユーザーのアドレス帳を同期できるようにするかどうかを選択します。デフォルトは［On］です。

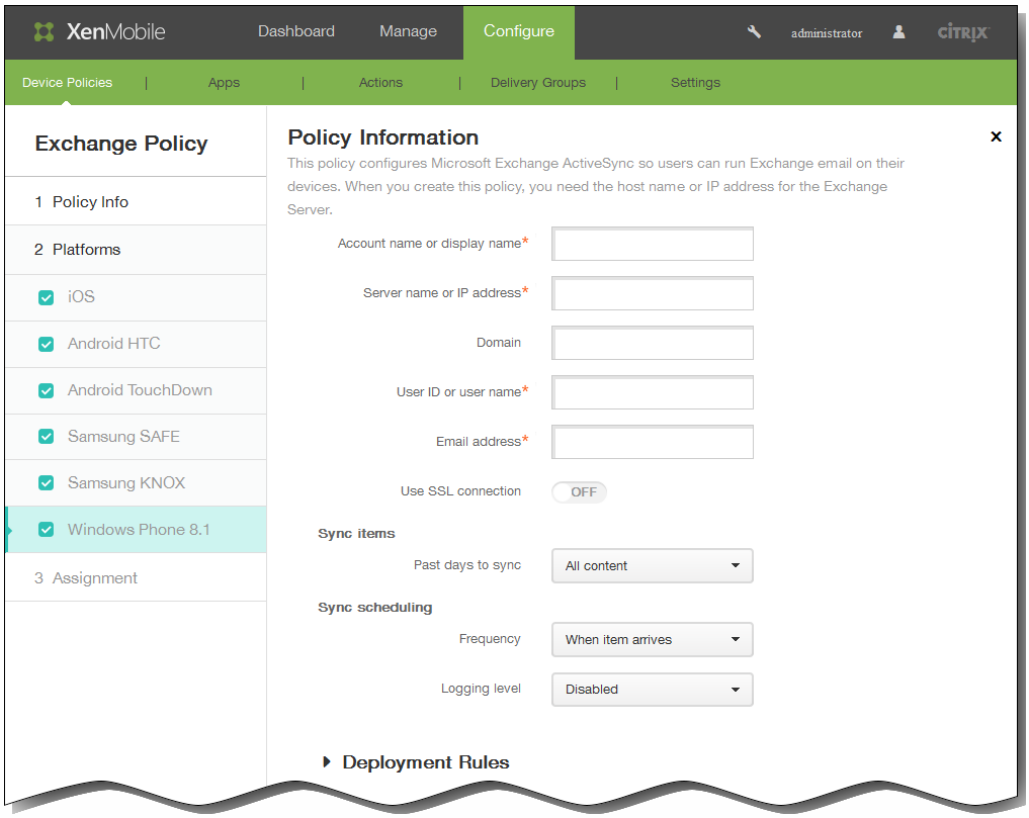
Sync calendar：デバイスとExchange Serverの間でユーザーのカレンダーを同期できるようにするかどうかを選択します。デフォルトは［On］です。

Default account：ユーザーのExchangeアカウントをデバイスから送信するメールのデフォルトにするかどうかを選択

します。デフォルトは［On］です。

- ［Windows Phone 8.1］を選択した場合は、次の設定を構成します。

  注：このポリシーを使ってユーザーパスワードを設定することはできません。ユーザーはポリシーがプッシュされた後に、デバイスでパラメーターを設定する必要があります。



Account name or display name：Exchange ActiveSyncアカウント名を入力します。

Server name or IP address：Exchange Serverのホスト名またはIPアドレスを入力します。

Domain：Exchange Serverがあるドメインを入力します。
注：このフィールドでシステムマクロ${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
User ID or user name：Exchangeユーザーアカウントのユーザー名を指定します。
注：このフィールドでシステムマクロ${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
Email address：ユーザーの完全なメールアドレスを指定します。
注：このフィールドでシステムマクロ${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
Use SSL connection：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは［Off］です。

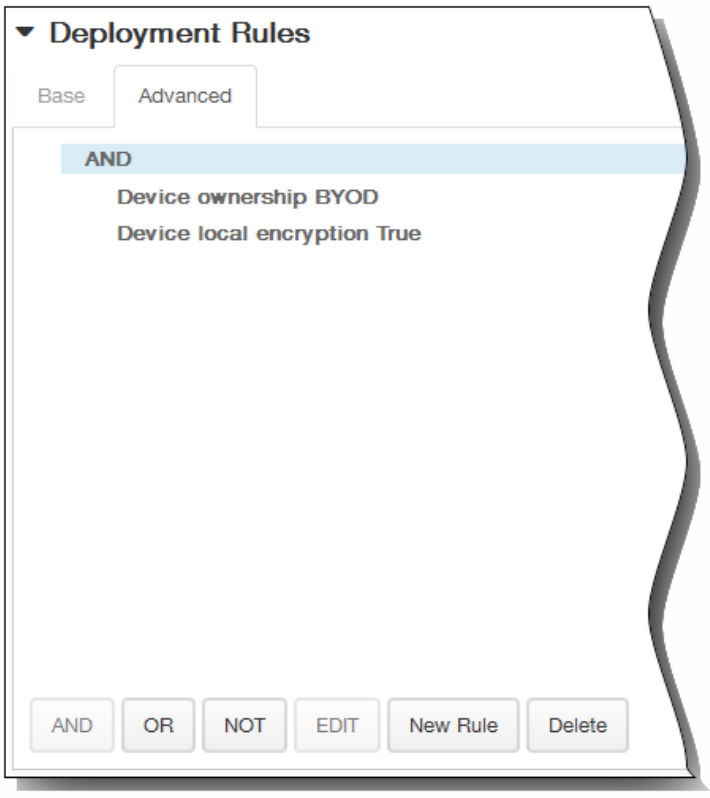
Past days to sync：ボックスの一覧で、デバイス上のすべてのコンテンツをExchange Serverと過去にさかのぼって同期する日数を選択します。

Frequency：ボックスの一覧で、Exchange Serverからデバイスへ送信されるデータの同期に使用するスケジュールを選択します。

Logging level：ボックスの一覧で、［Disabled］、［Basic］、または［Advanced］を選択して、Exchangeのアクティビティをログ記録する詳細レベルを指定します。

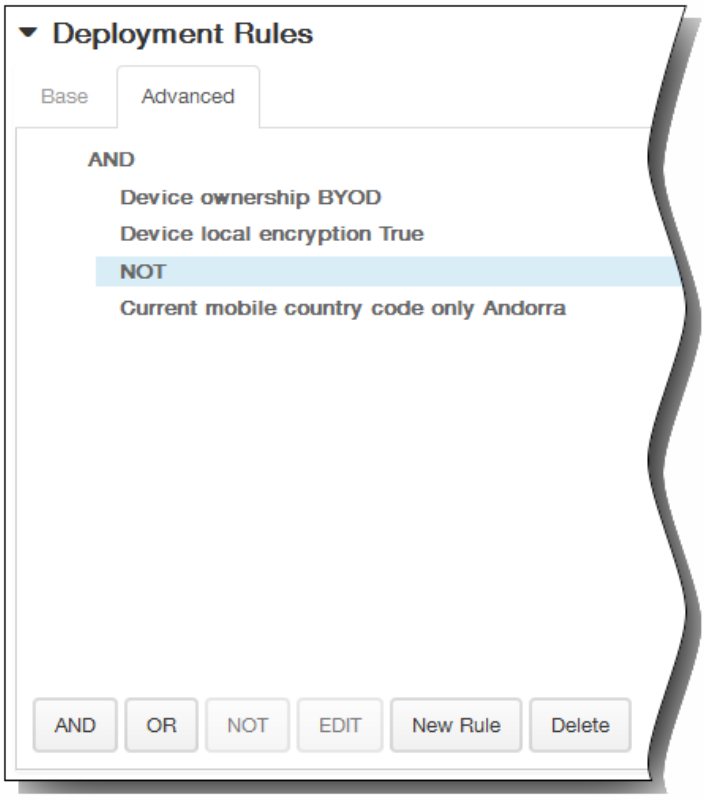
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

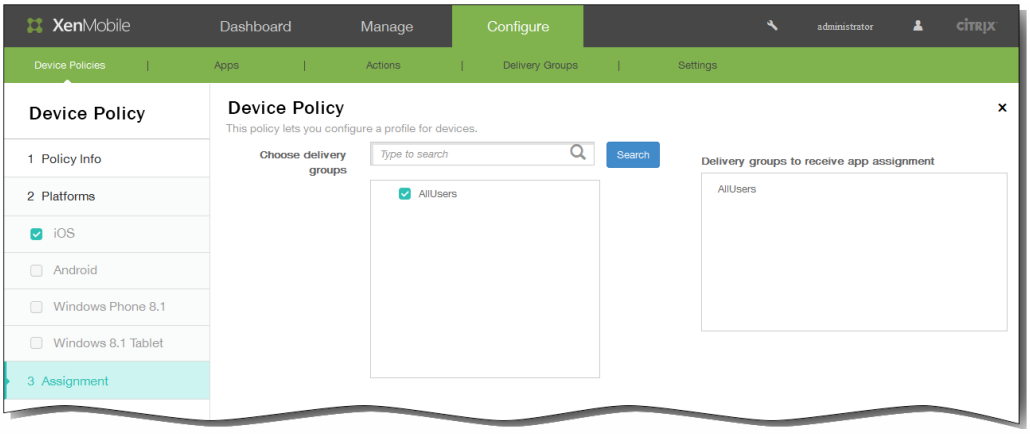


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



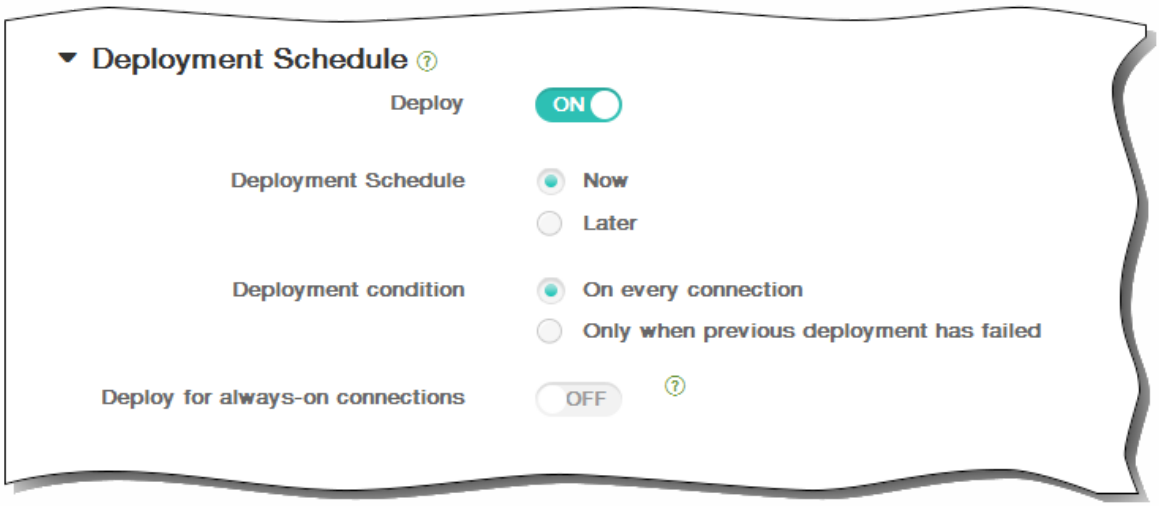
8. ［Next］をクリックします。［Exchange Policy Assignment］ページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［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。
    4. ［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。
    5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

    注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

    注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックします。

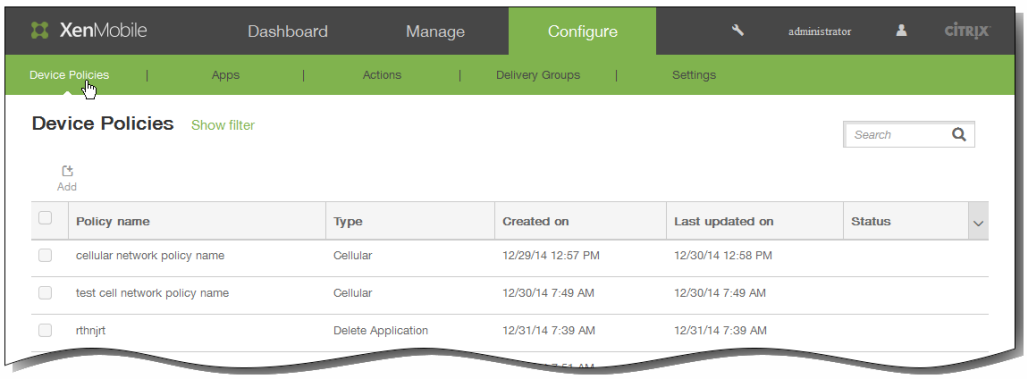
位置情報デバイスポリシー

May 10, 2016

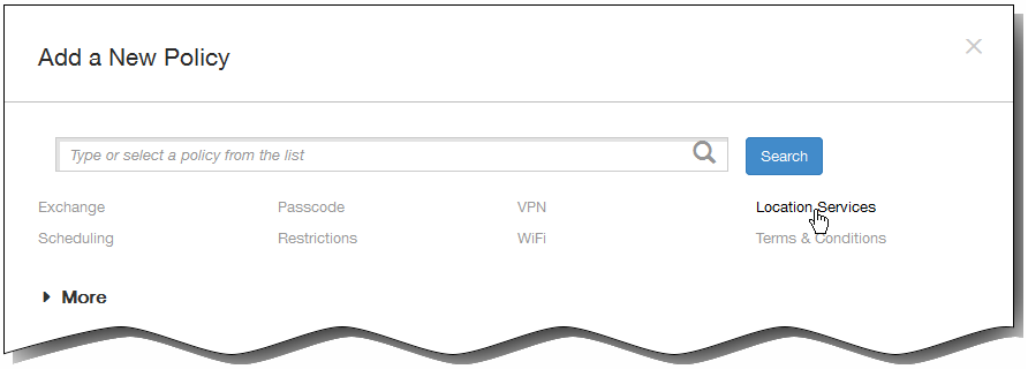
XenMobileで位置情報デバイスポリシーを作成して、地理的な境界を適用したり、ユーザーのデバイスの位置や移動を追跡したりすることができます。定義された境界（ジオフェンス）の外にユーザーが出た場合、XenMobileで選択的ワイプまたは完全なワイプを直ちに実行することができます。また、許可された場所にユーザーが戻ることができるように、一定の時間が経過してから実行することもできます。

位置情報デバイスポリシーは、iOSおよびAndroidに対して作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

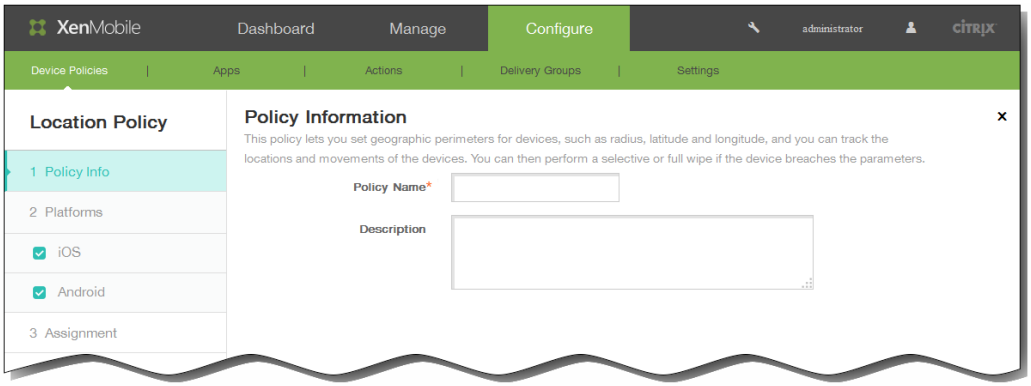
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



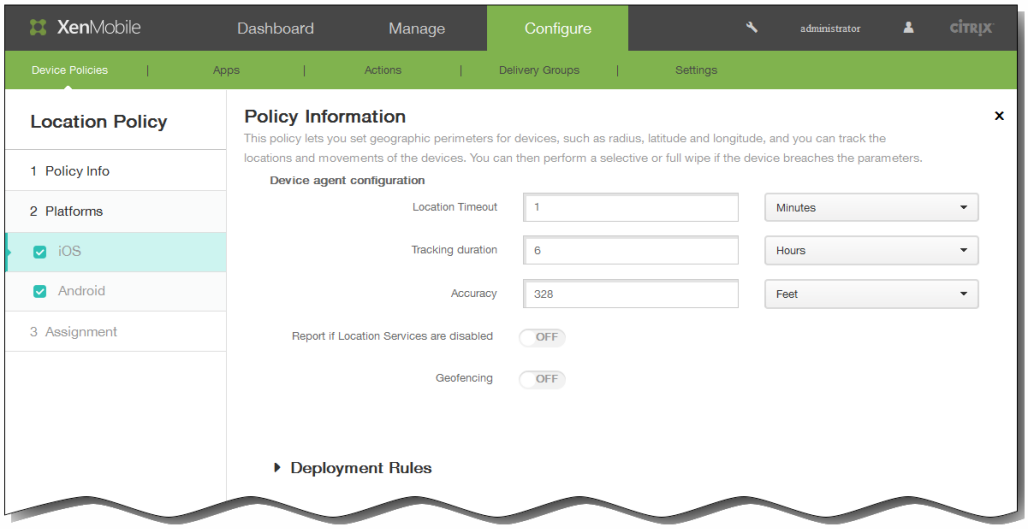
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add New Policy］ダイアログボックスが開きます。



3. ［Location Services］をクリックします。 ［Location Policy］情報ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときは両方のプラットフォームがオンになっており、最初はiOSプラットフォーム構成パネルが開きます。



6. ［Platforms］の下で、追加するプラットフォームをオンにします。
   - ［iOS］を選択した場合は、次の設定を構成します。
     Location timeout：数値を入力して、ボックスの一覧で［Seconds］または［Minutes］を選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、60～900秒または1～15分です。デフォルトは1分です。

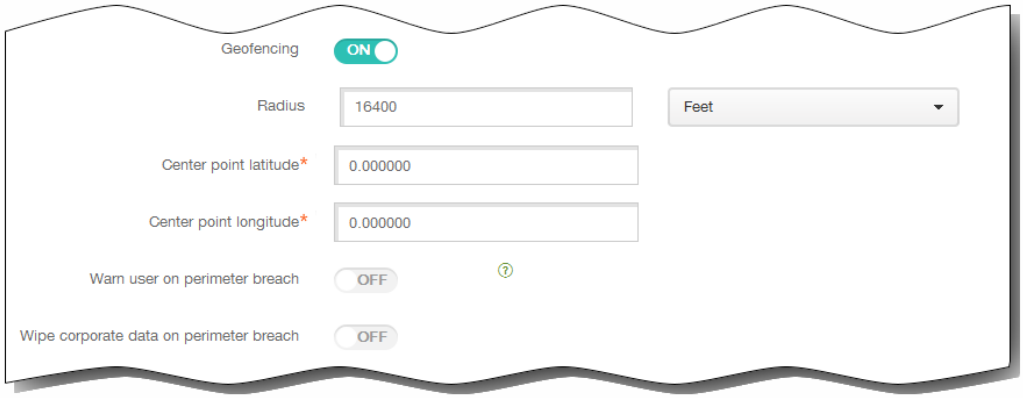
     Tracking duration：数値を入力して、ボックスの一覧で［Hours］または［Minutes］を選択し、XenMobileがデバイスを追跡する時間を設定します。有効な値は、1～6時間または10～360分です。デフォルトは6時間です。

     Accuracy：数値を入力して、ボックスの一覧で［Meters］、［Feet］、［Yards］のいずれかを選択し、XenMobileがデバイスを追跡する精度を設定します。有効な値は、10～5000ヤード、10～5000m、または30～15000フィートです。デフォルトは328フィートです。

     Report if Location Services are disabled：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信す

るかどうかを選択します。デフォルトは［OFF］です。

Geofencing：このオプションをオンにして、以下の設定を構成します。

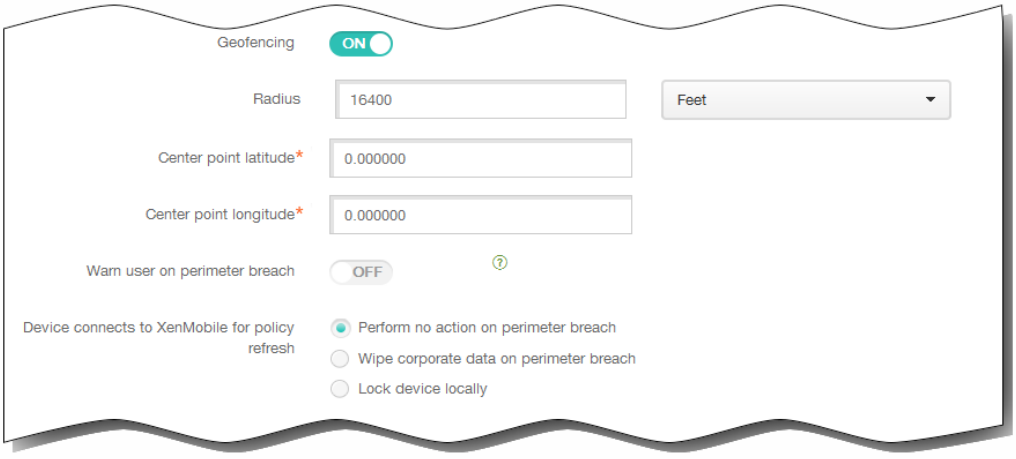


- Radius：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。
  有効な半径の値は次のとおりです。
  - 164～164000フィート
  - 1～50km
  - 50～50000m
  - 54～54680ヤード
  - 1～31マイル
- Center point latitude：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- Center point longitude：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- Warn user on perimeter breach：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［OFF］です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- Wipe corporate data on perimeter breach：ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。デフォルトは［OFF］です。
  このオプションを有効にすると、［Delay on local wipe］フィールドが表示されます。

  数値を入力し、一覧から［Seconds］または［Minutes］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

- ［Android］を選択した場合は、次の設定を構成します。
  Poll interval：数値を入力して、ボックスの一覧で［Minutes］、［Hours］、［Days］のいずれかを選択し、XenMobileがデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1～1440分、1～24時間、または任意の日数です。デフォルトは10分です。
  注：この値を10分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
  Report if Location Services are disabled：GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。デフォルトは［OFF］です。

  Geofencing：このオプションをオンにして、以下の設定を構成します。



- Radius：数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。
  有効な半径の値は次のとおりです。
  - 164～164000フィート
  - 1～50km
  - 50～50000m
  - 54～54680ヤード
  - 1～31マイル
- Center point latitude：緯度（37.787454など）を入力して、ジオフェンスの中心点の緯度を定義します。
- Center point longitude：経度（122.402952など）を入力して、ジオフェンスの中心点の経度を定義します。
- Warn user on perimeter breach：定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは［OFF］です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- Device connects to XenMobile for policy refresh：ユーザーが境界の外に出た場合のオプションを以下から1つ選択します。
  - Perform no action on perimeter breach：何もしません。これがデフォルトの設定です。
  - Wipe corporate data on perimeter breach：指定した時間が経過すると、企業データがワイプされます。
    このオプションを有効にすると、［Delay on local wipe］フィールドが表示されます。

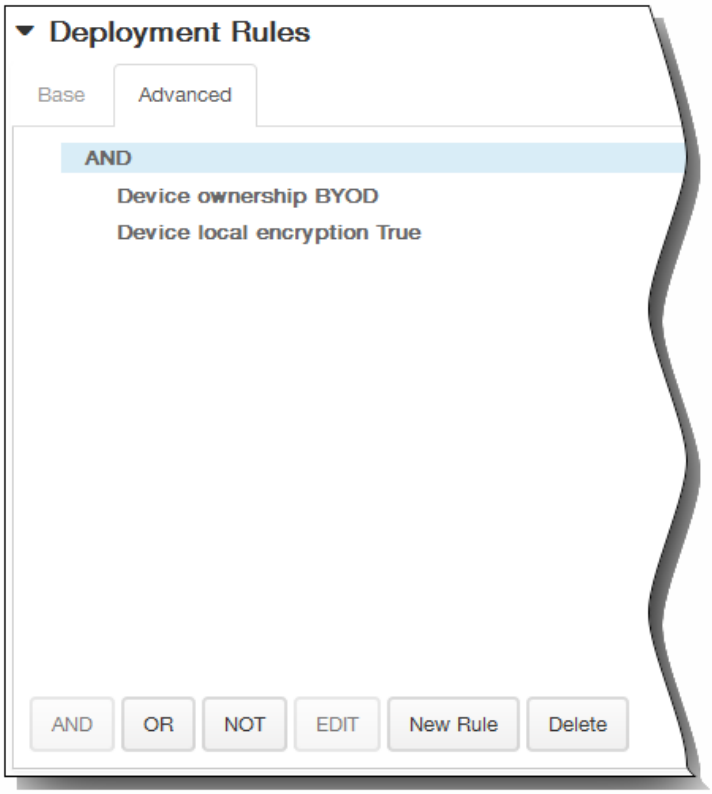
    数値を入力し、一覧から［Seconds］または［Minutes］を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

  - Delay on lock：指定した時間が経過すると、ユーザーのデバイスがロックされます。
    このオプションを有効にすると、［Delay on lock］フィールドが表示されます。

    数値を入力し、一覧から［Seconds］または［Minutes］を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

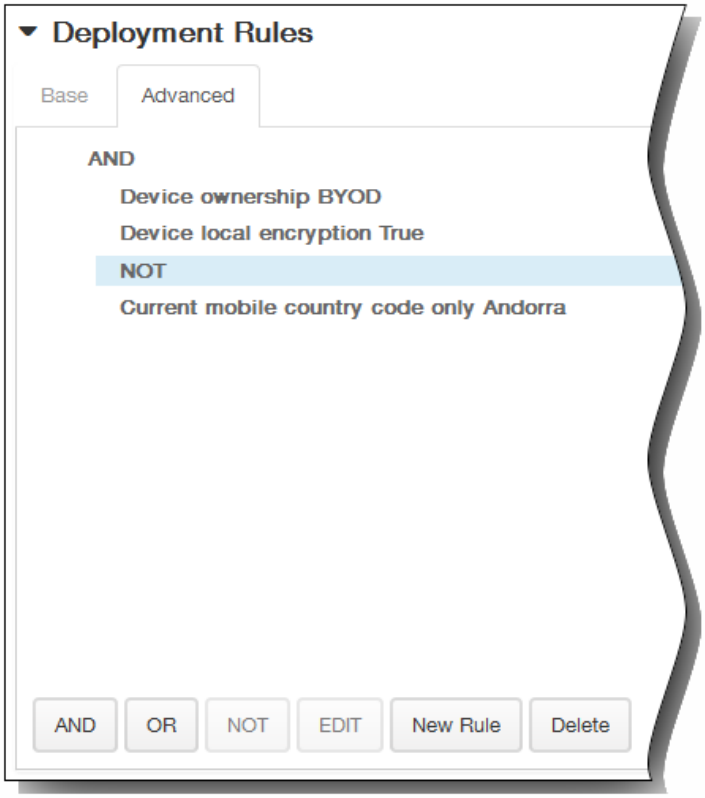


［Base］タブで選択した条件が表示されます。

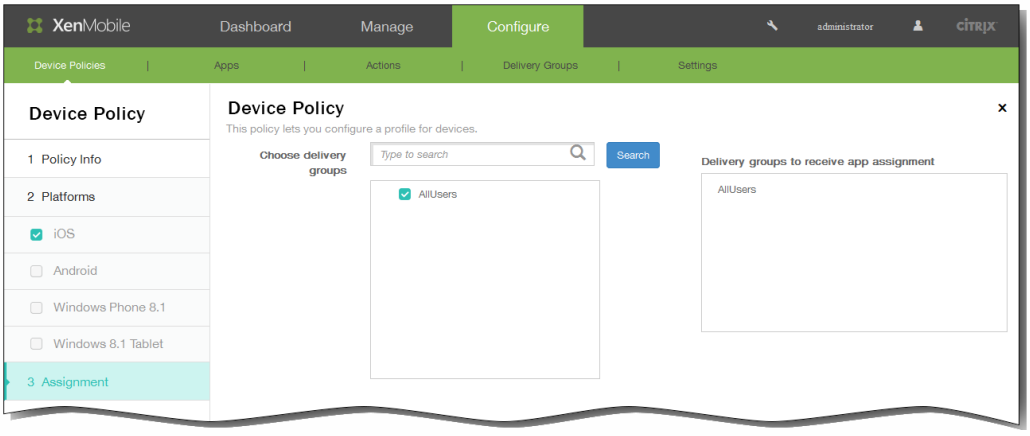
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Location Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

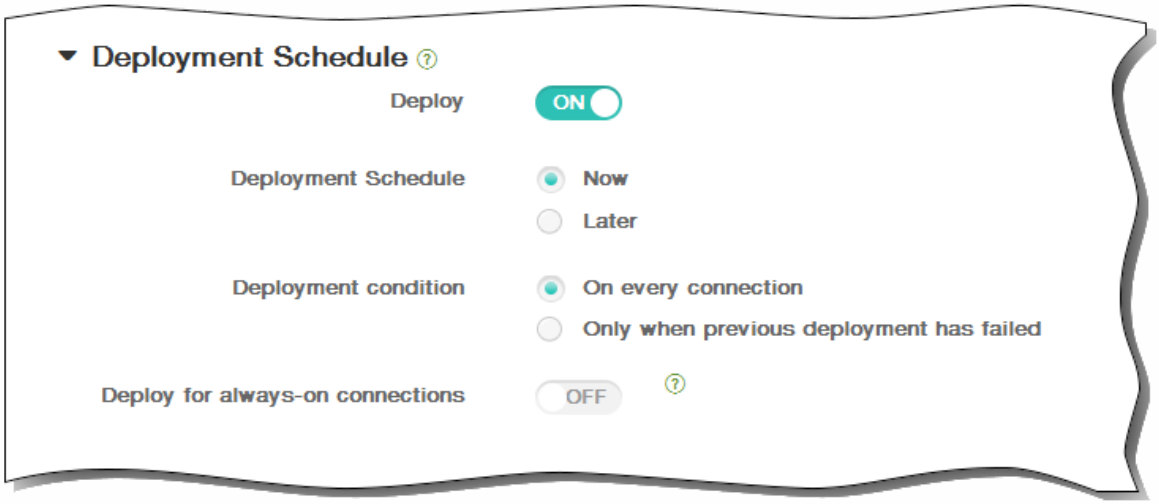


10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



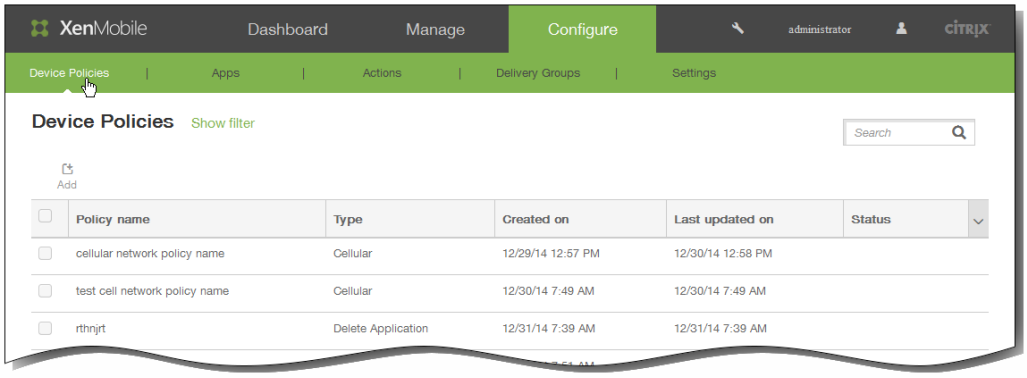
11. ［Save］をクリックしてポリシーを保存します。

接続スケジュールデバイスポリシー

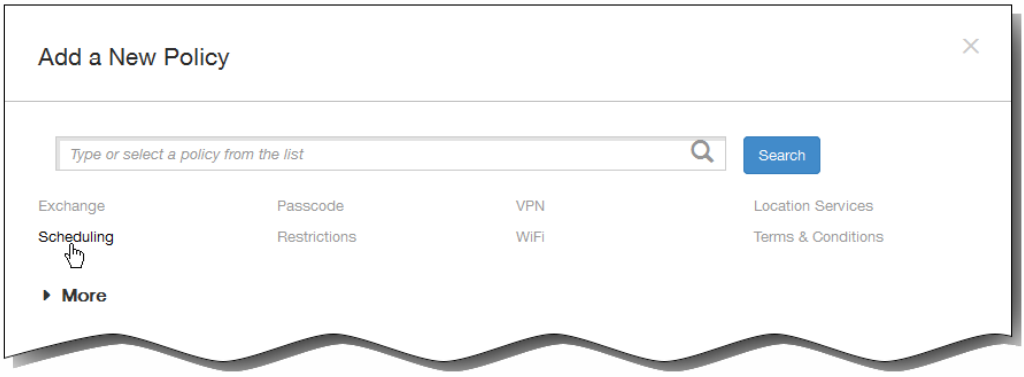
May 10, 2016

接続スケジュールポリシーを作成して、ユーザーのAndroidデバイスおよびSymbianデバイスをXenMobileに接続する方法と時間を管理します。ユーザーが手動でデバイスを接続するか、デバイスが永続的に接続されたままにするか、定義した期間内にデバイスが接続されるようにするかを指定できます。

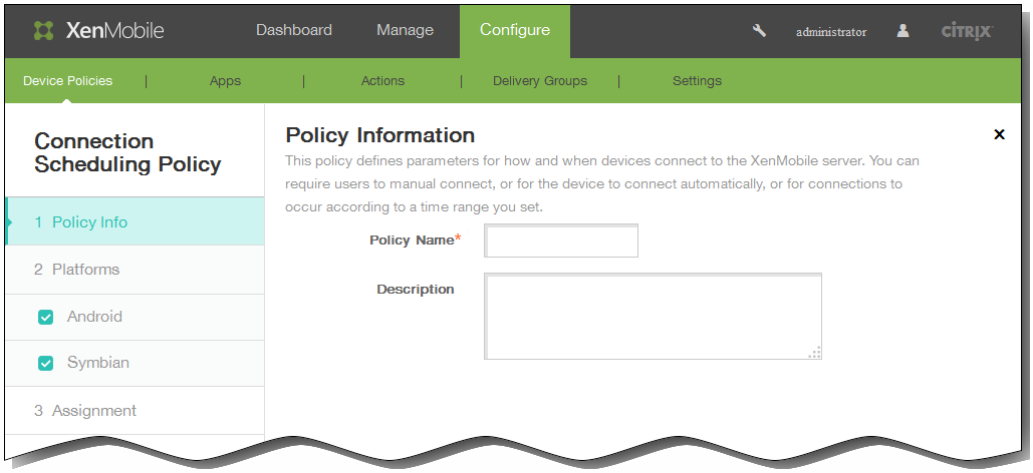
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



2. 新しいポリシーを追加するには［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. ［Scheduling］をクリックします。 ［Connection Scheduling Policy］情報ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注： ［Policy Platforms］ページが開いたときは両方のプラットフォームがオンになっており、最初はAndroidプラットフォーム構成パネルが開きます。
6. ［Platforms］の下で、追加するプラットフォームをオンにします。
7. 選択したプラットフォームそれぞれに対して次の設定を構成します: ［Require devices to connect］：このスケジュールに対して設定するオプションをクリックします。
   - Always：接続のオンライン状態を永続的に維持します。ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobileサーバーへの再接続を試行し、一定の間隔でコントロールパケットを送信することによって接続を監視します。
     このオプションはバッテリーを消耗し、ネットワークトラフィックを大量に発生させるためお勧めしません。
   - Never：手動で接続します。ユーザーがデバイス上のXenMobileから接続を開始する必要があります。
   - Every：指定された間隔で接続されます。定義した分数後にデバイスが自動的に接続されます。
     このオプションを選択すると、［Connect every N minutes］フィールドが表示されます。このフィールドに、デバイスが再接続されるまでの分数を入力する必要があります。デフォルトは20です。
   - Define schedule：ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobileサーバーへの再接続を試行し、定義した期間中、一定の間隔でコントロールパケットを送信することによって接続を監視します。次の節では接続期間の定義方法について説明します。
     接続期間を定義するには

     以下のオプションを有効にすると時間軸が表示されます。これを使用して必要な期間を定義できます。特定の時間内に永続的な接続を必要とするオプション、または特定の期間内に1回の接続を必要とするオプションのいずれか、またはその両方を有効にできます。時間軸の各四角は30分間であるため、毎平日の8:00 AM～9:00 AMに接続が必要な場合は、時間軸で毎平日の［8 AM］と［9 AM］の間の2つの四角をクリックします。

     たとえば、次の図の2つの時間軸では、毎平日の8:00 AM～9:00 AMに永続的な接続、土曜日の12:00 AM～日曜日の1:00 AMに永続的な接続、毎平日の5:00 AM～8:00 AMまたは10:00 AM～11:00 PMに1回以上の接続が必要です。

Maintain permanent connection during these hours：定義した期間中、ユーザーのデバイスが接続されている必要があります。

Require a connection within each of these ranges：定義した期間内に1回以上、ユーザーのデバイスが接続される必要があります。

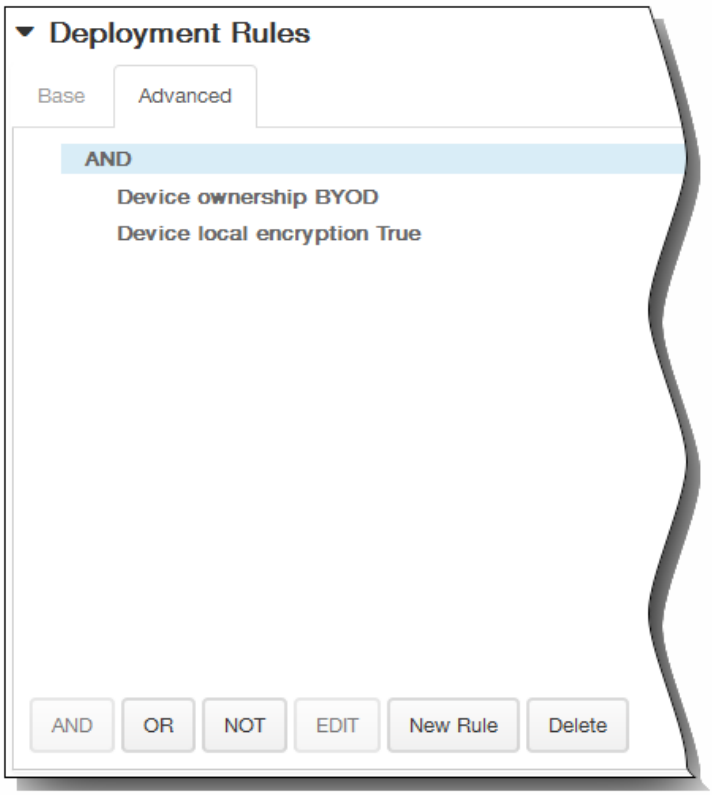
Use local device time rather than UTC：定義した期間を、UTC（Coordinated Universal Time：協定世界時）ではなくローカルデバイスの時間に同期させます。

8. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。

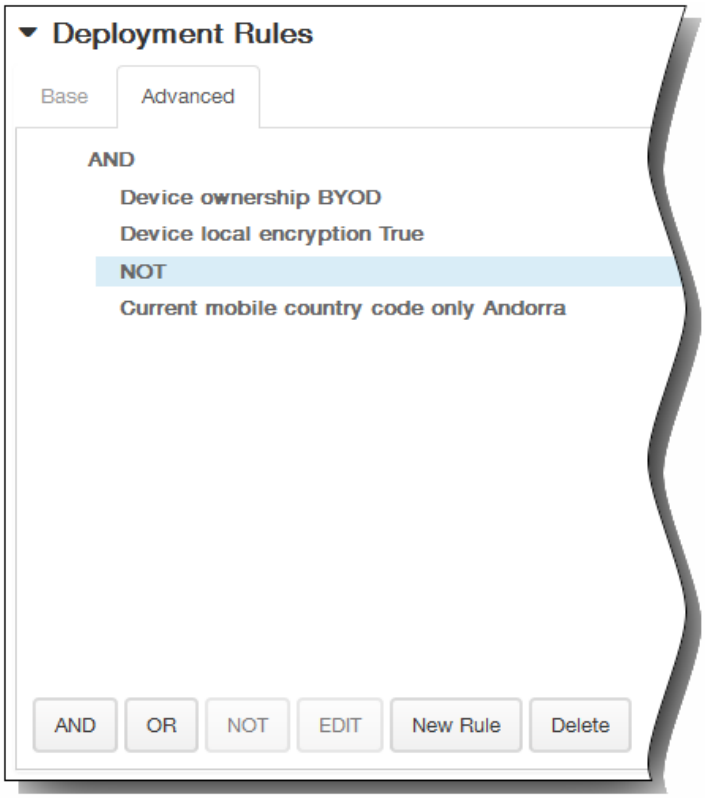
2. ［New Rule］をクリックして条件を定義します。
3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。

2. ［Advanced］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。

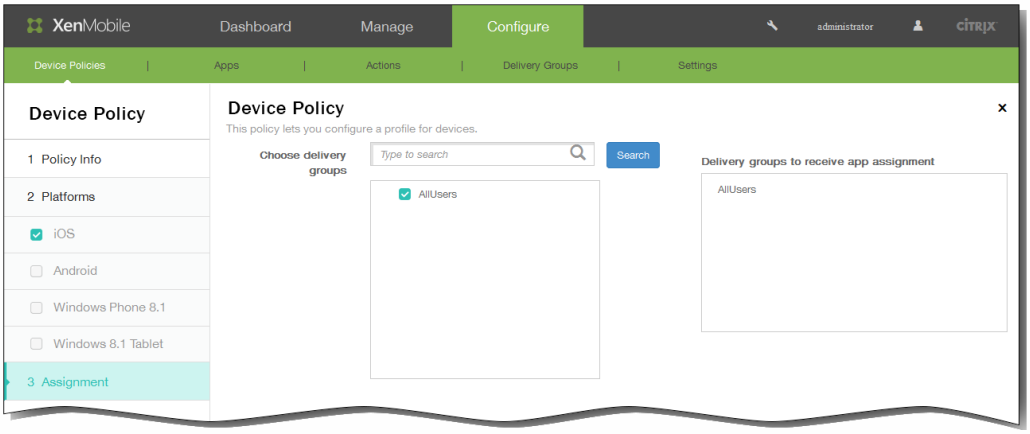


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



9. ［Next］をクリックします。 ［Connection Scheduling Policy］割り当てページが開きます。
10. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



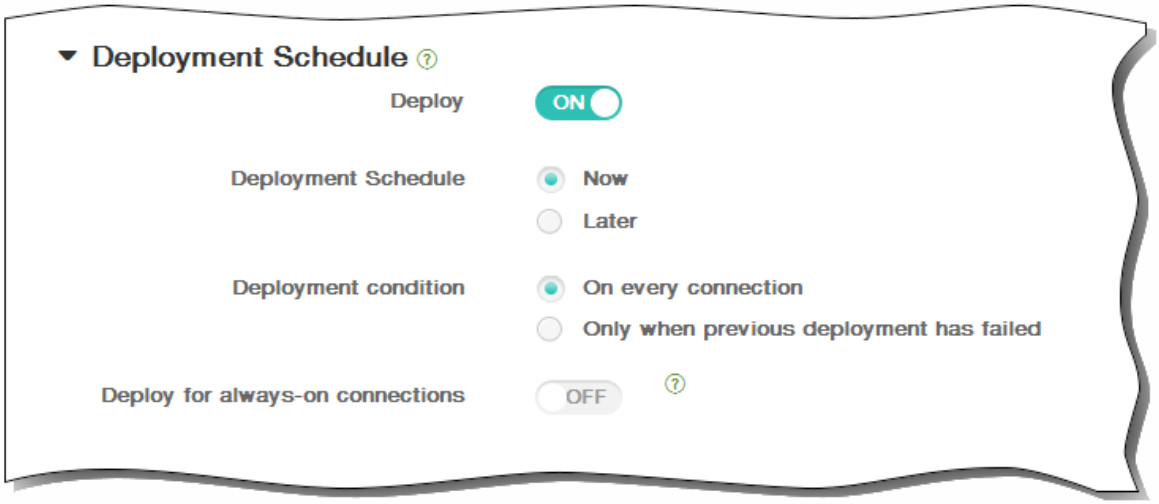
11. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



12. ［Save］をクリックしてポリシーを保存します。

iOSのAirPlayミラーリングデバイスポリシーを追加するには

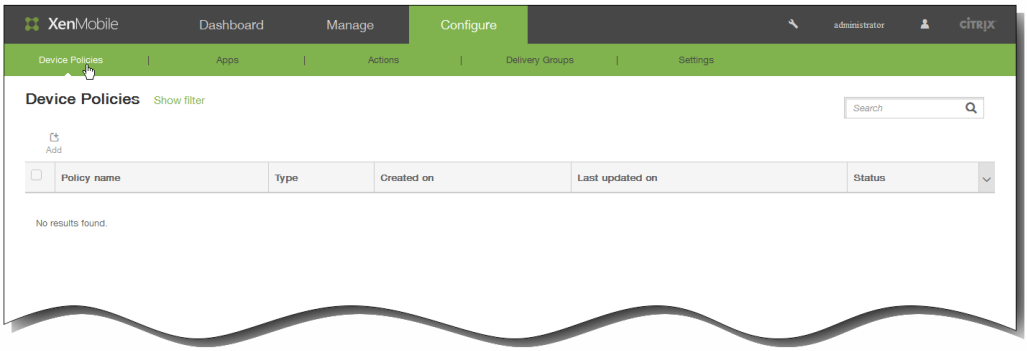
May 10, 2016

Apple AirPlay機能を使用すると、Apple TVを介してiOSデバイスからTV画面にコンテンツをワイヤレスでストリーム配信したり、デバイス上の表示をTV画面またはほかのMacコンピューターに正確にミラーリングしたりすることができます。

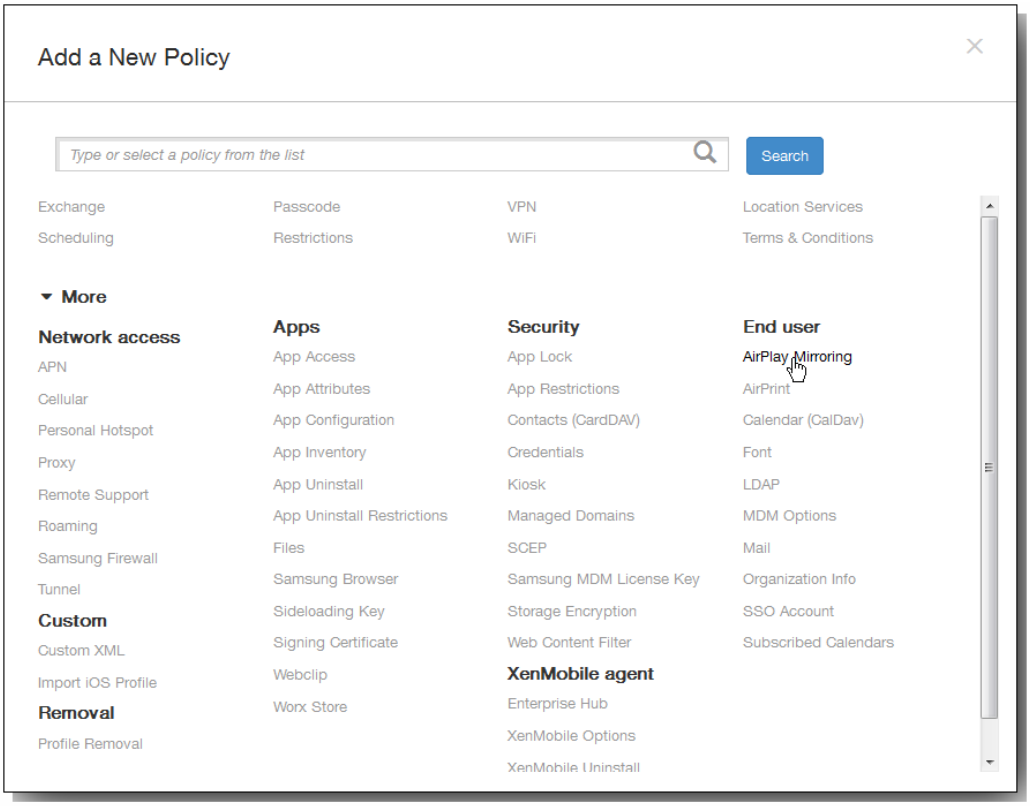
XenMobileでデバイスポリシーを追加して、特定のAirPlayデバイス（Apple TVやほかのMacコンピューターなど）をユーザーのiOSデバイスに追加することができます。また、デバイスを監視対象デバイスのホワイトリストに追加して、ユーザーをホワイトリストにあるAirPlayデバイスのみに限定するオプションもあります。デバイスをSupervisedモードに設定する方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

注：続行する前に、追加するすべてのデバイスのデバイスIDとパスワードがあることを確認してください。

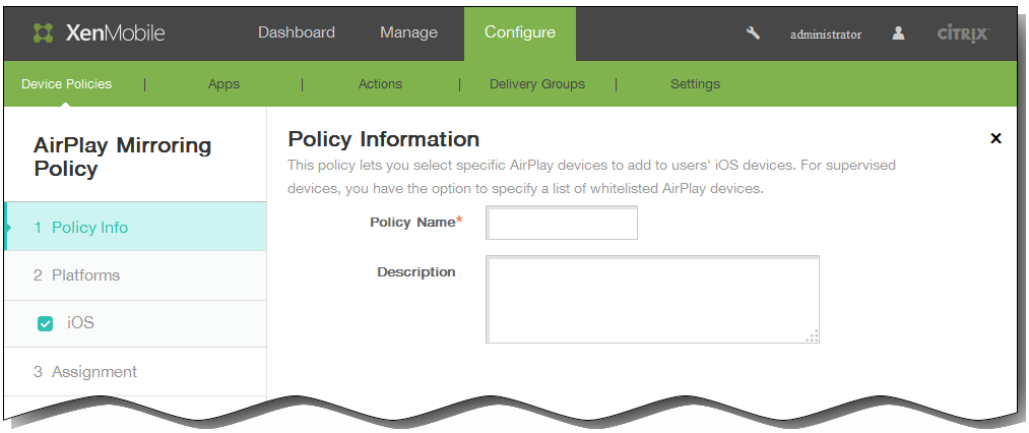
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



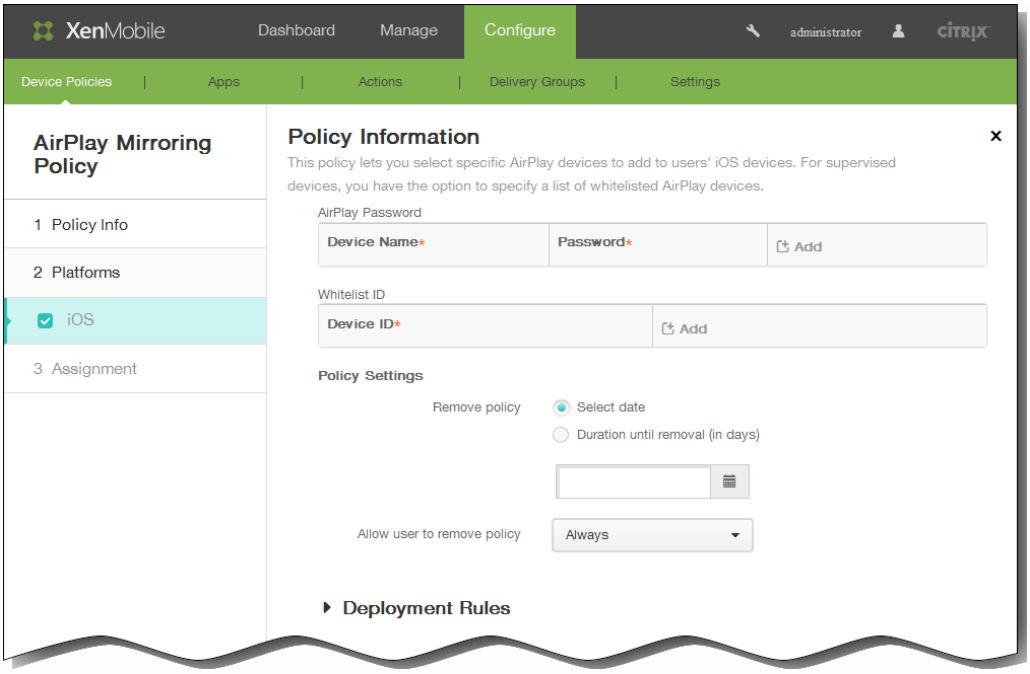
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［End user］の下の［AirPlay Mirroring］をクリックします。 ［AirPlay Mirroring Policy］ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。

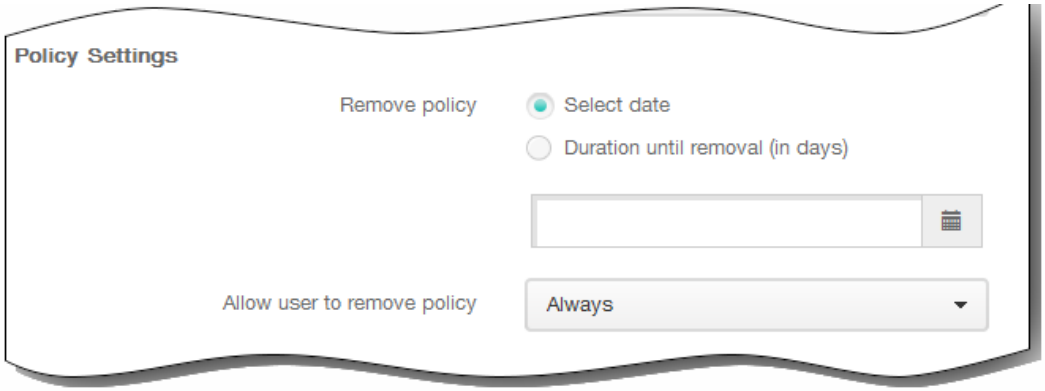


6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. AirPlay Password：［Add］をクリックして、以下の操作を行います。
      1. Device ID：デバイスIDを「xx:xx:xx:xx:xx::xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
      2. Password：任意で、デバイスのパスワードを入力します。
      3. ［Add］をクリックしてデバイスを追加するか、［Cancel］をクリックしてデバイスの追加を取り消します。
      4. 追加するカスタムキーごとに手順i.～iii.を繰り返します。
   2. Whitelist ID：監視対象デバイスをホワイトリストにIDがあるデバイスのみに限定するには、［Add］をクリックして以下の操作を行います。
      注：この一覧は、監視対象ではないデバイスでは無視されます。
      1. Device ID：デバイスIDを「xx:xx:xx:xx:xx:xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
      2. ［Add］をクリックしてデバイスを追加するか、［Cancel］をクリックしてデバイスの追加を取り消します。
      3. 追加するカスタムキーごとに手順iおよびiiを繰り返します。

      注：既存のデバイスを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

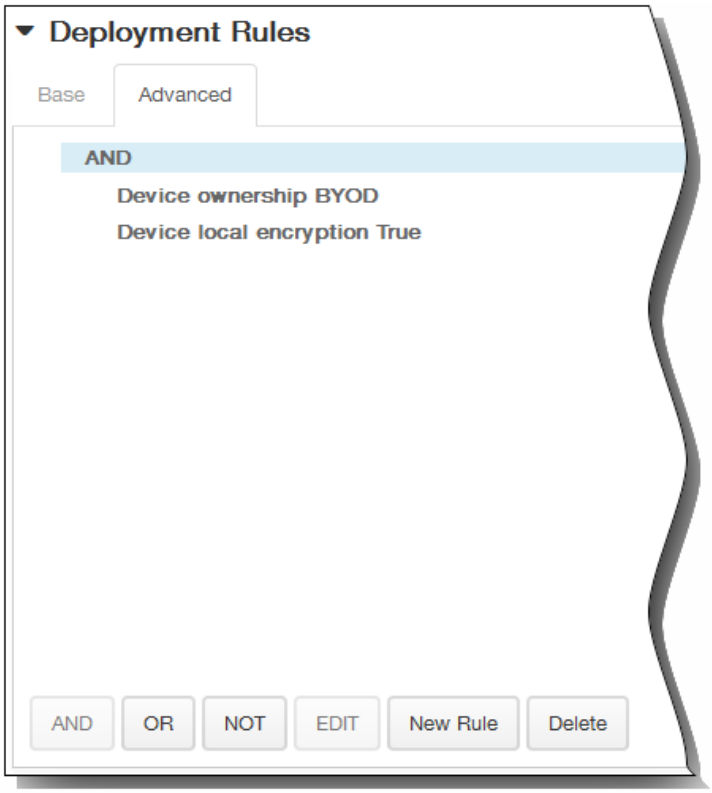
      既存のデバイスを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

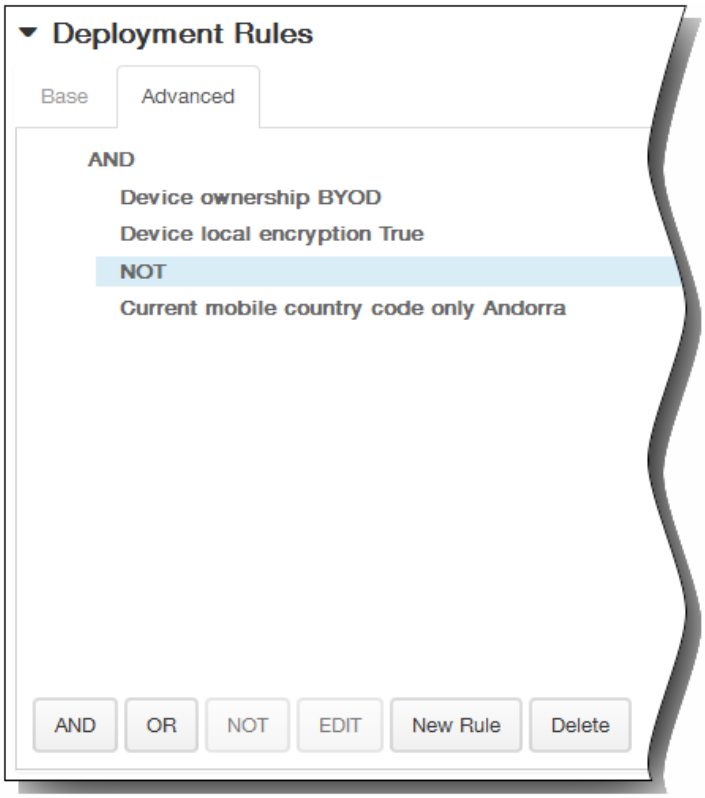
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



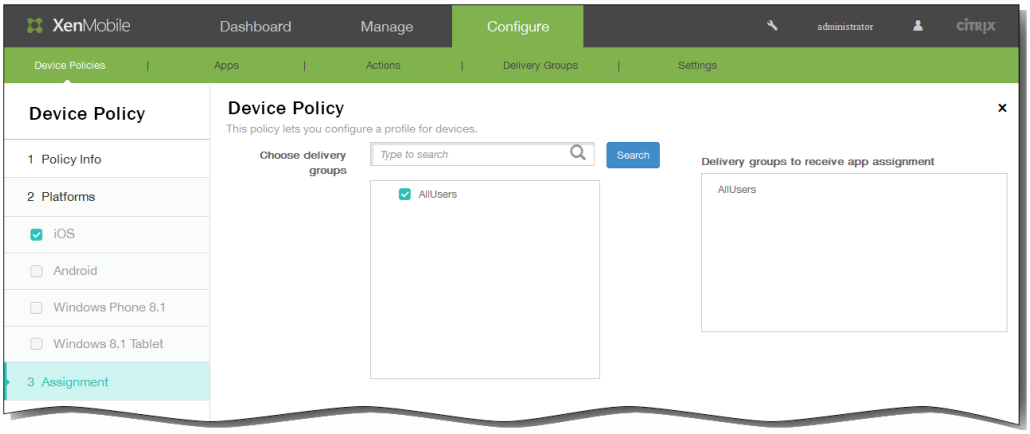
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［AirPlay Mirroring Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



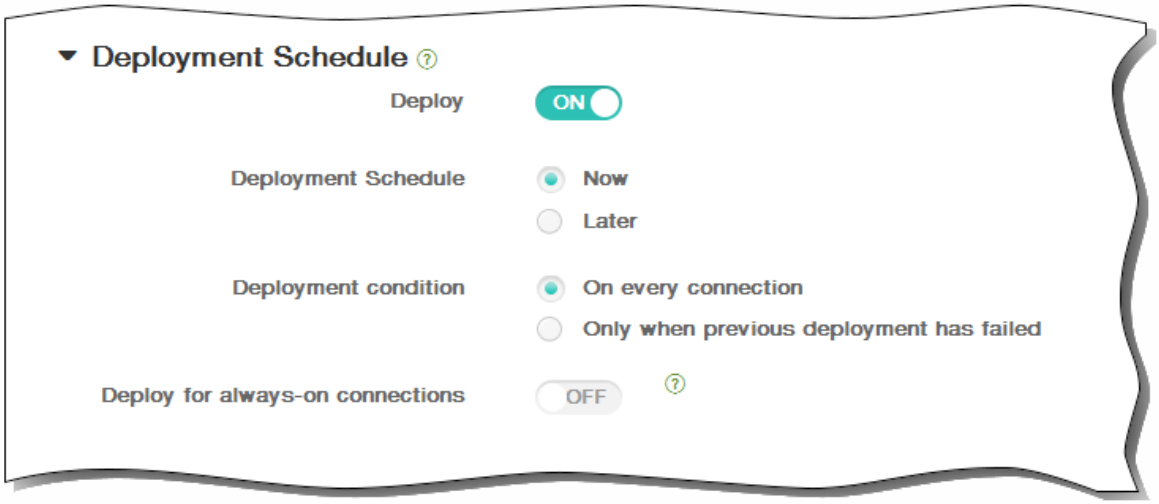
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



15. ［Save］をクリックしてポリシーを保存します。

iOSのAirPrintデバイスポリシーを追加するには

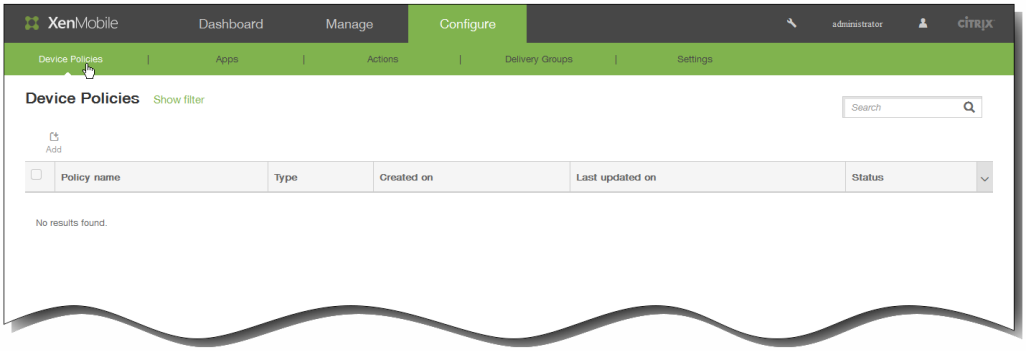
May 10, 2016

XenMobileでデバイスポリシーを追加して、AirPrintプリンターをユーザーのiOSデバイスのAirPrintプリンター一覧に追加できます。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。

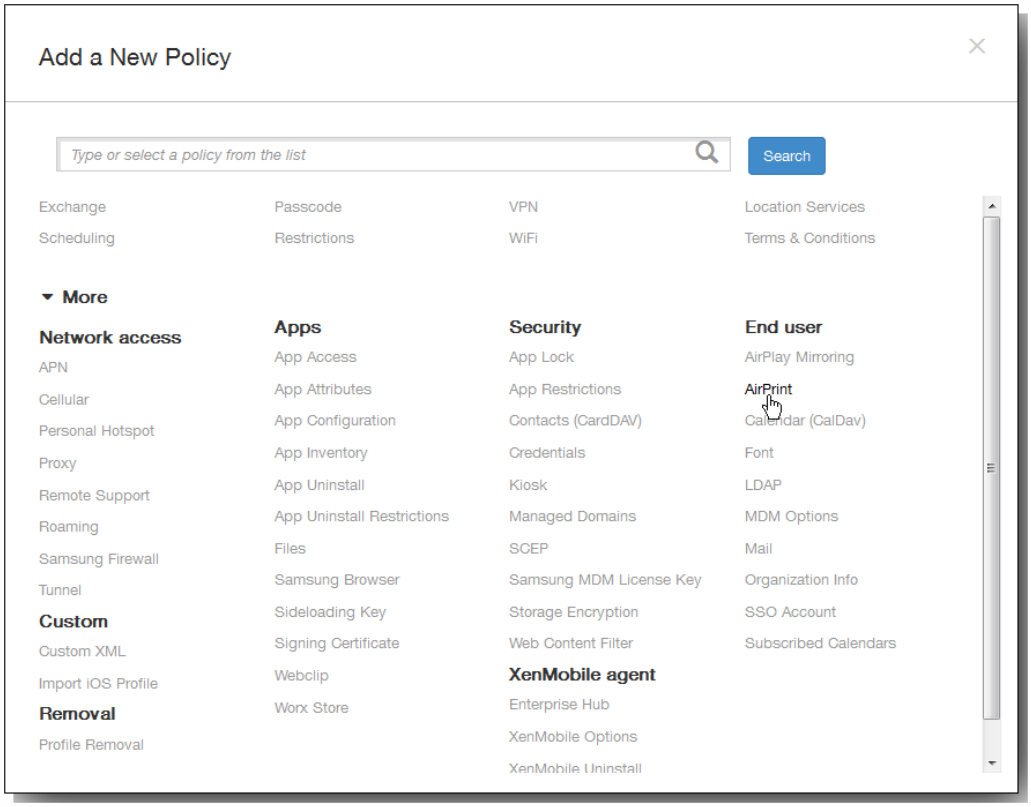
注：

- このポリシーはiOS 7.0以降に適用されます。
- 各プリンターのIPアドレスとリソースパスがあることを確認してください。

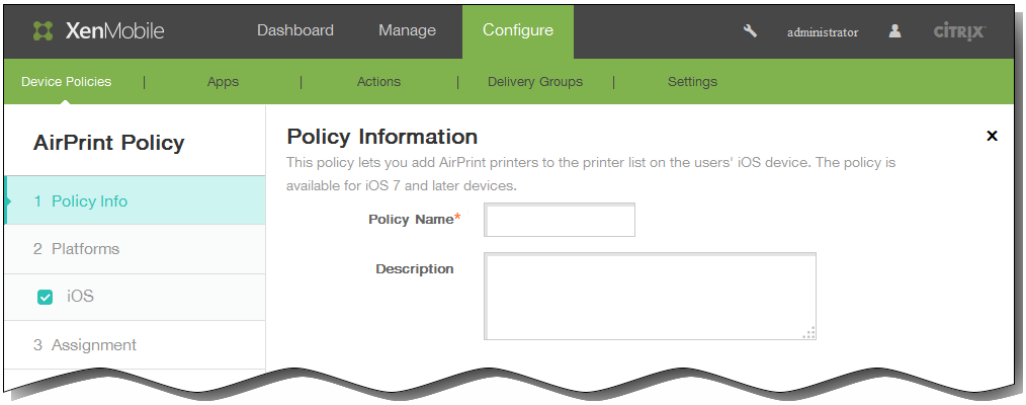
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



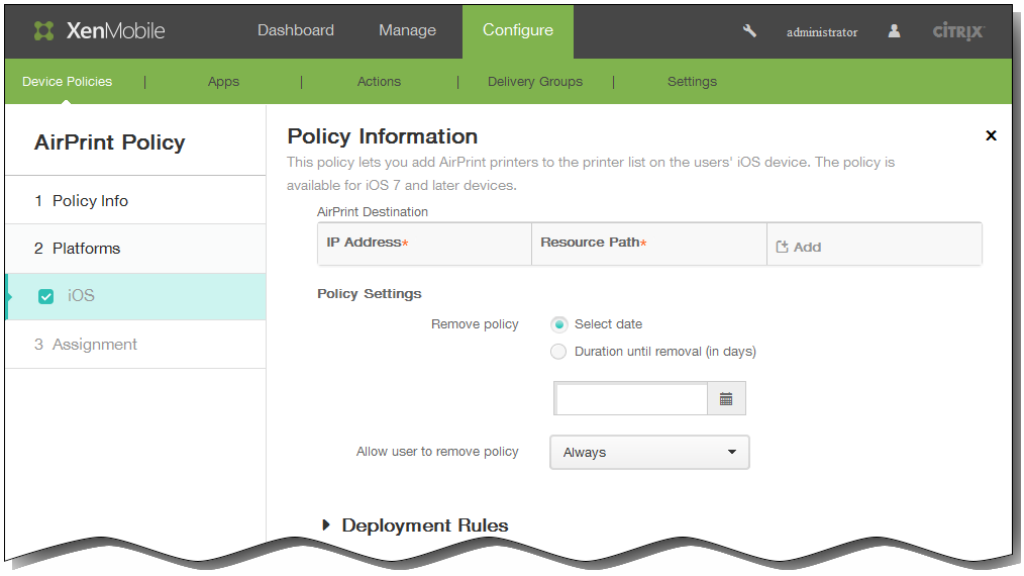
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［End user］の下の［AirPrint］をクリックします。 ［AirPrint Policy］ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。



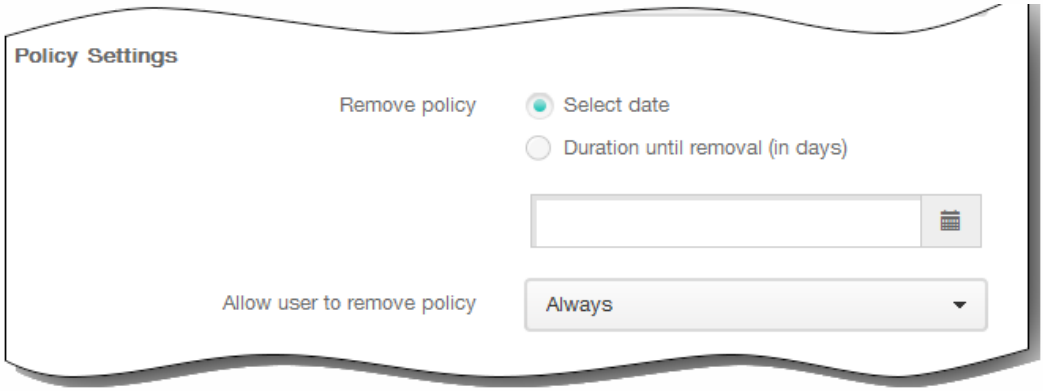
6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. AirPrint Destination：［Add］をクリックして、以下の操作を行います。
      1. IP Address：AirPrintプリンターのIPアドレスを入力します。
      2. Resource Path：プリンターに関連付けられているリソースパスを入力します。この値は、_ipps.tcp Bonjourレコードのパラメーターに対応します。たとえば、printers/Canon_MG5300_series or printers/Xerox_Phaser_7600。
      3. ［Add］をクリックしてプリンターを追加するか、［Cancel］をクリックしてプリンターの追加を取り消します。
      4. 追加するカスタムキーごとに手順i.～iii.を繰り返します。

      注：既存のプリンターを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

      既存のプリンターを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリック

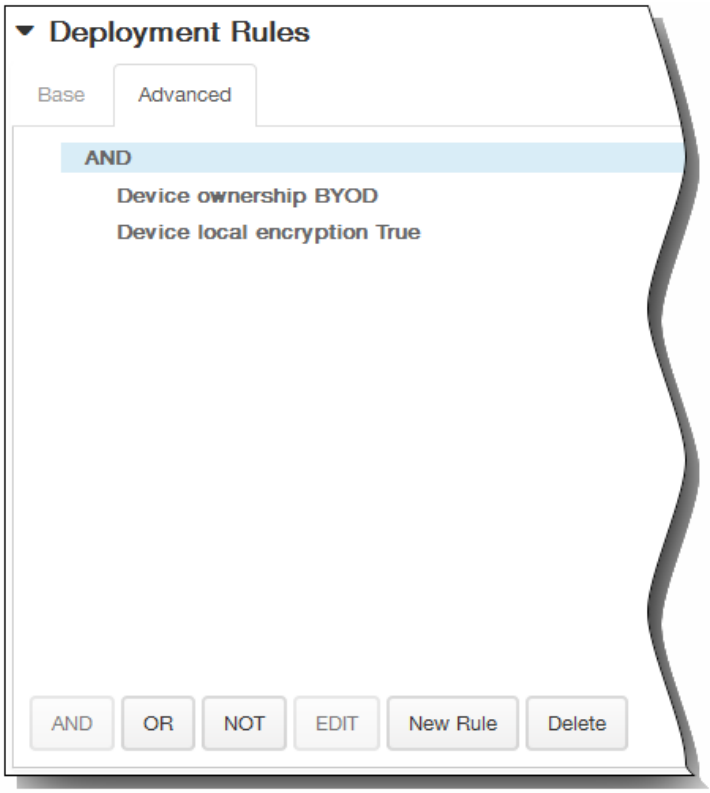
します。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



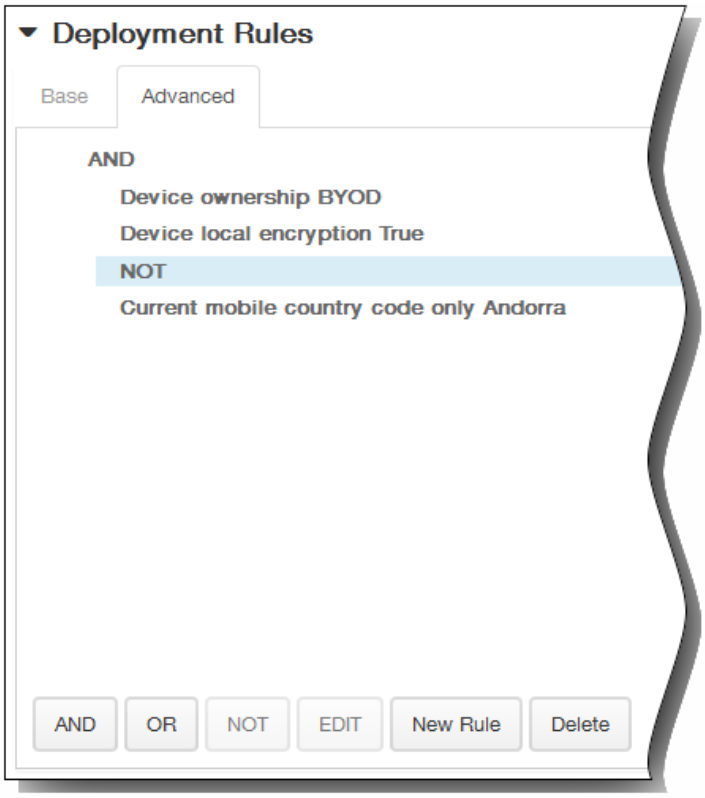
11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
    1. 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［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

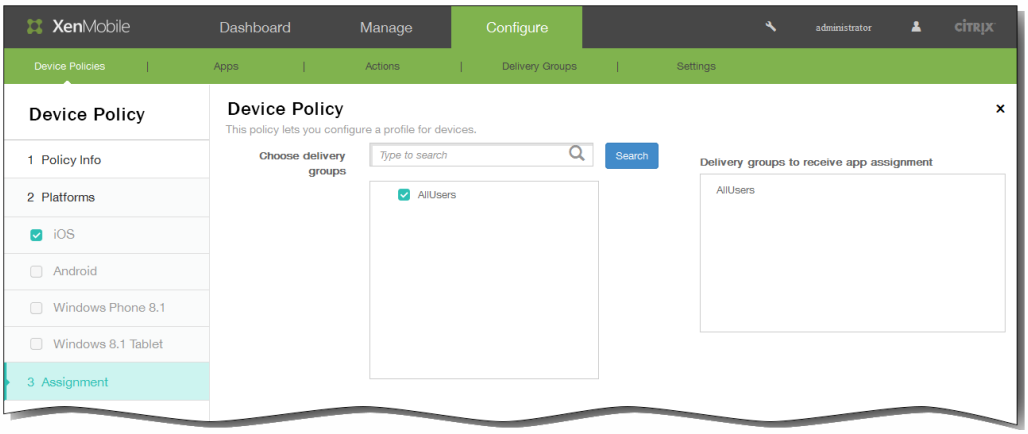


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［AirPrint Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



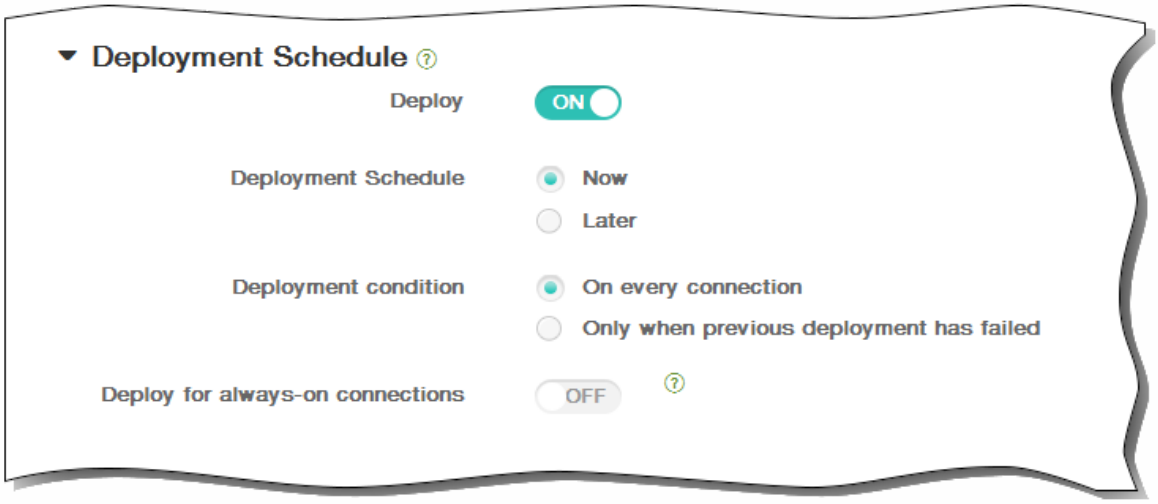
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



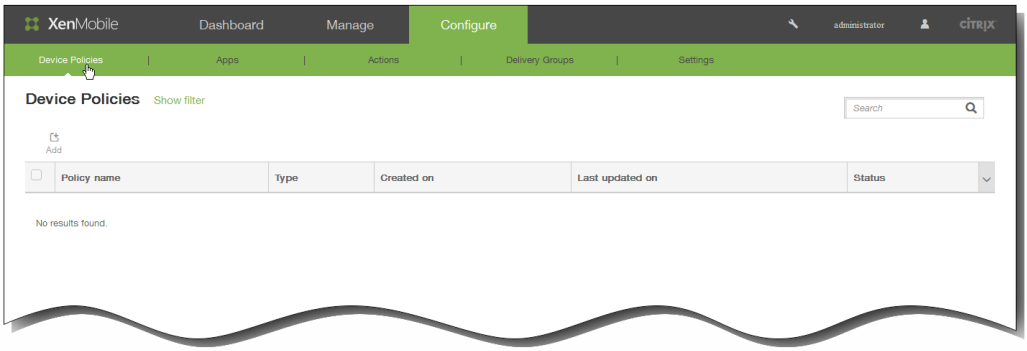
15. ［Save］をクリックしてポリシーを保存します。

iOSのカレンダー（CalDav）デバイスポリシーを追加するには

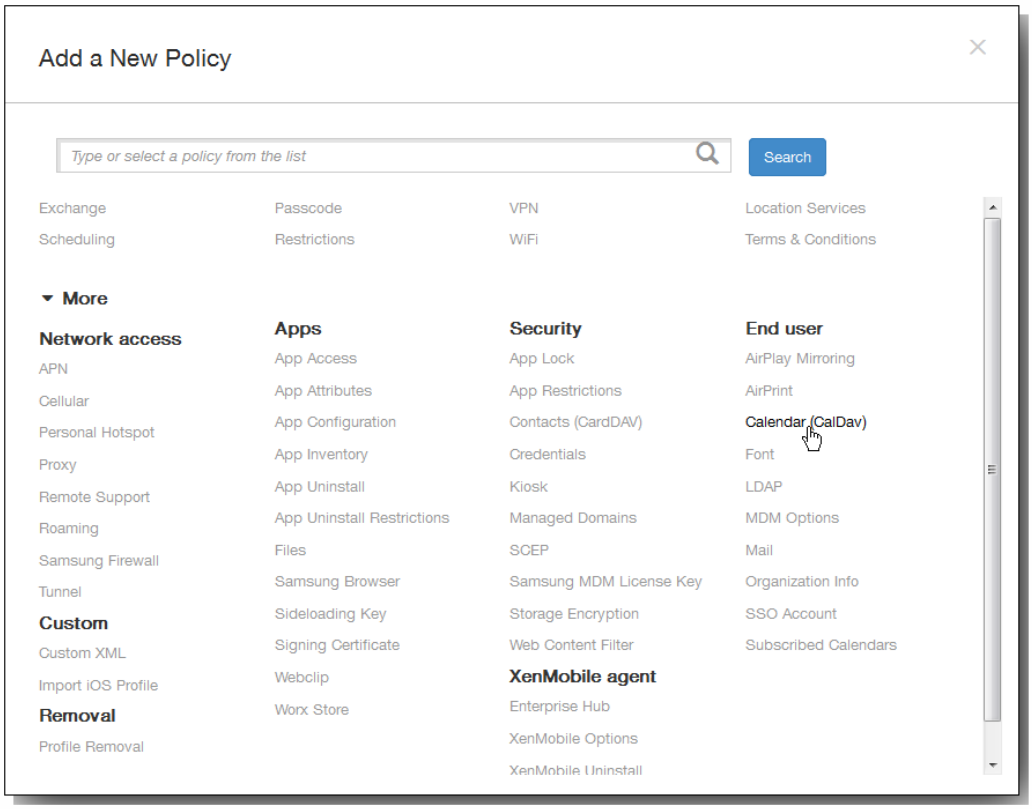
May 10, 2016

XenMobileでデバイスポリシーを追加して、iOSカレンダー（CalDAV）アカウントをユーザーのiOSデバイスに追加し、CalDAVをサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。

1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。

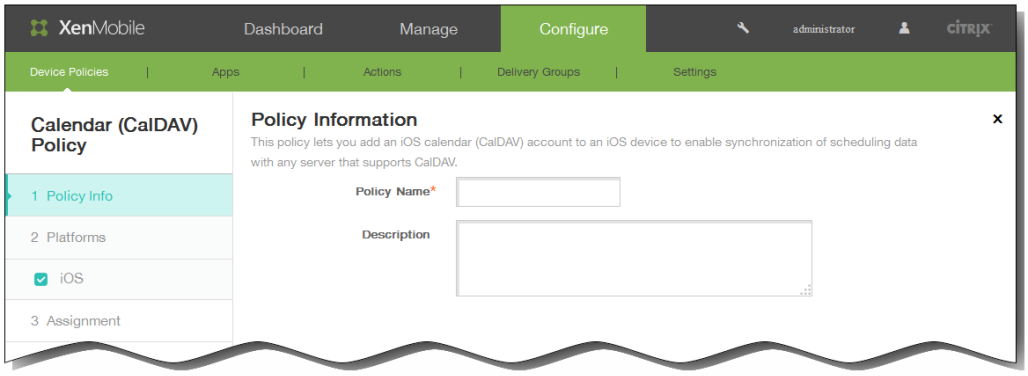


2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。

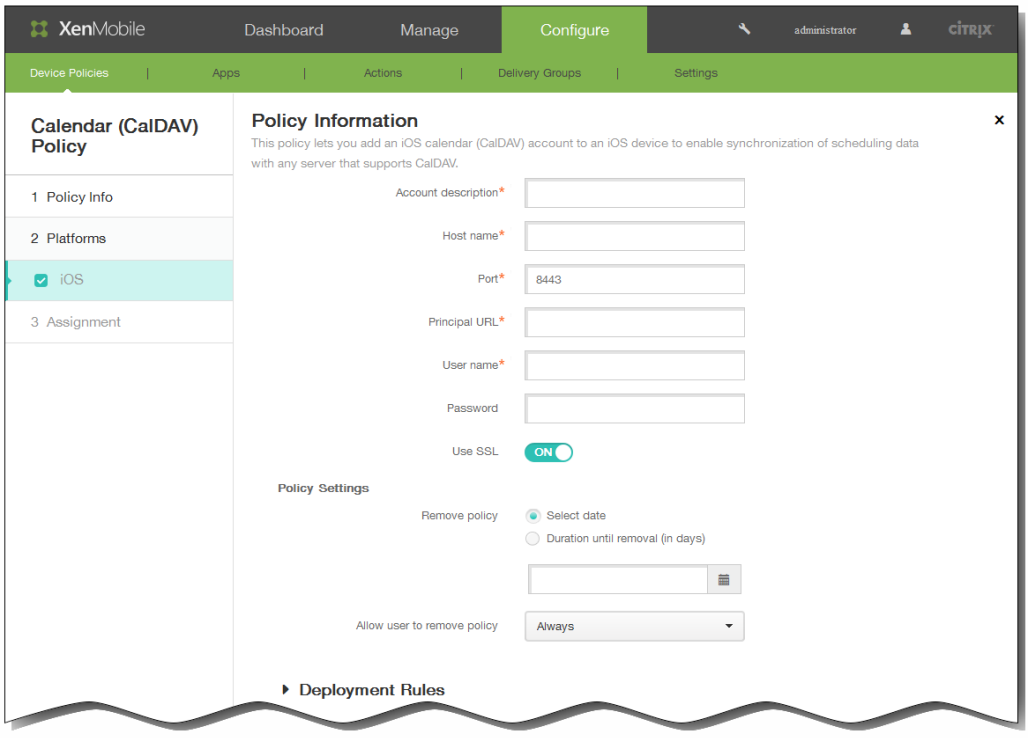


3. ［More］をクリックした後、［End user］の下の［Calendar（CalDAV）］をクリックします。

［Calendar（CalDAV）Policy］ページが開きます。



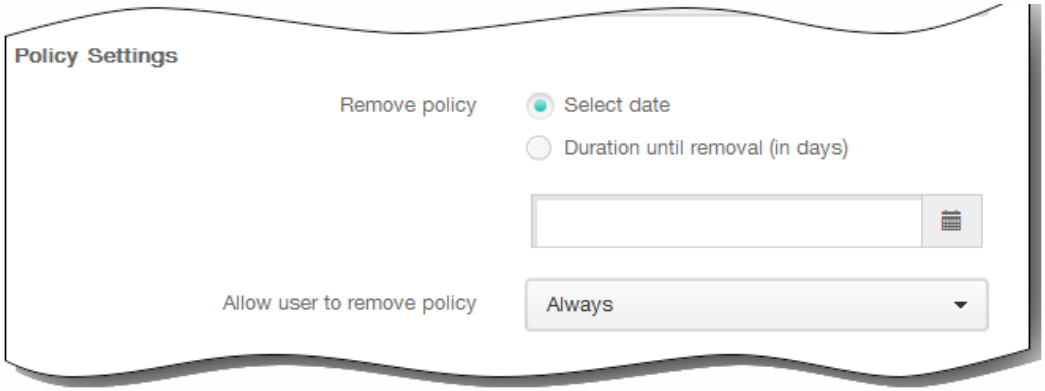
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform Information］ページが開きます。



6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. 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。
   2. Host name：CalDAVサーバーのアドレスを入力します。 このフィールドは必須です。
   3. Port：CalDAVサーバーへの接続用ポートを入力します。 このフィールドは必須です。 デフォルトは8443です。
   4. 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。
   5. 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。
   6. Password：任意で、ユーザーのパスワードを入力します。

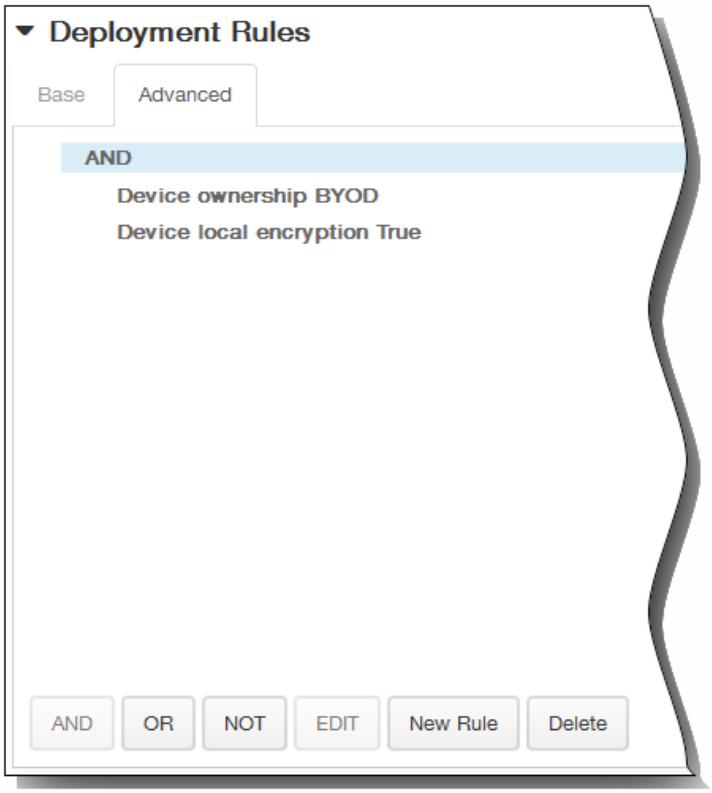
7. Use SSL：CalDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［On］です。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



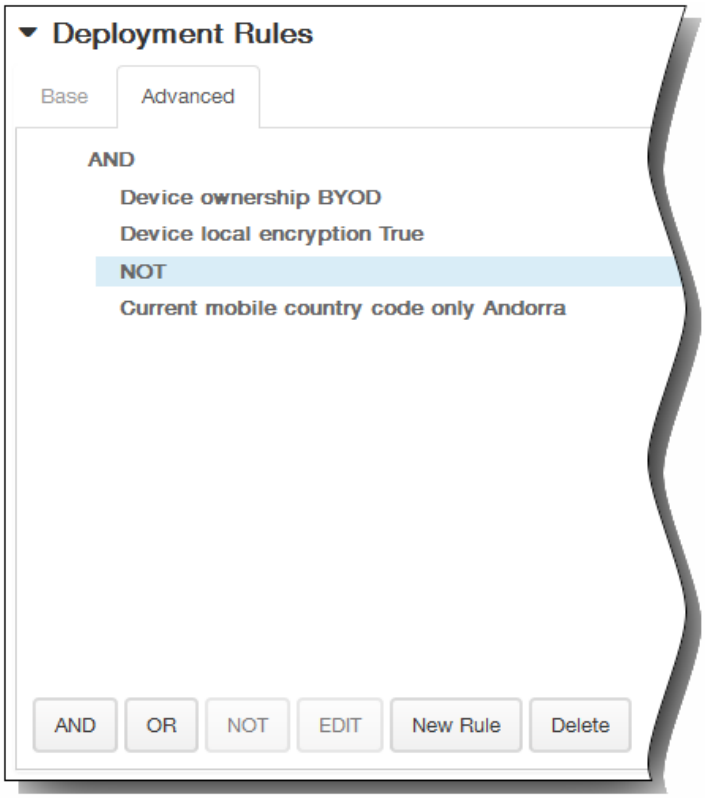
11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
    1. 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［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

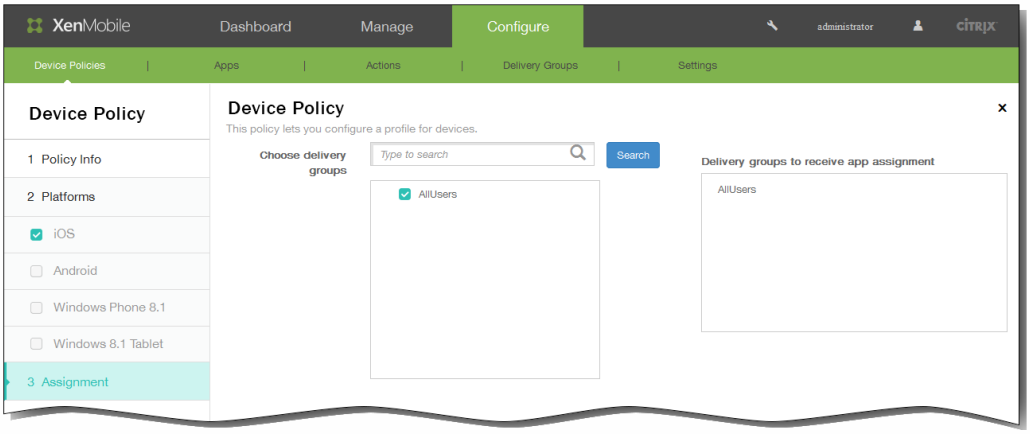


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［Calendar（CalDAV）Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



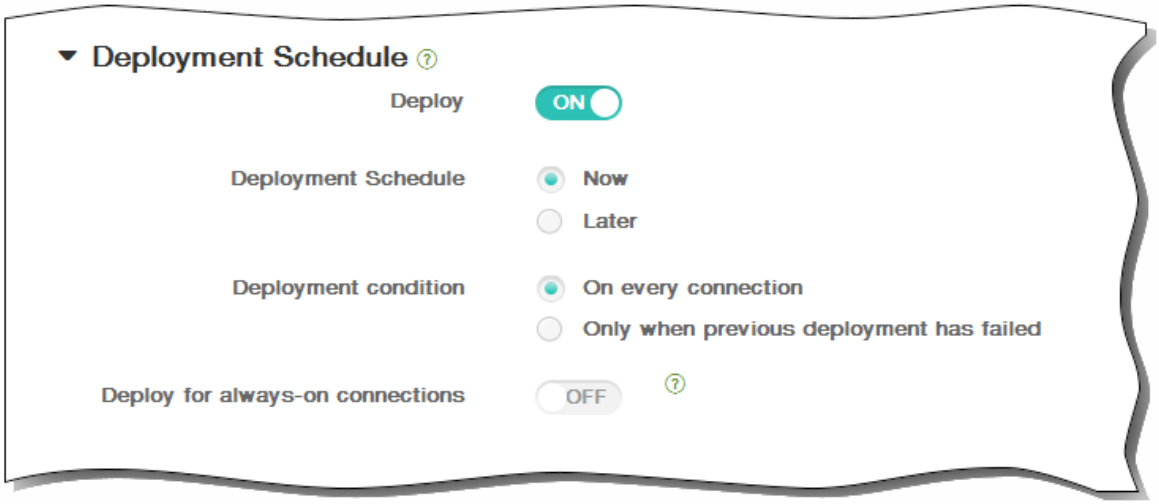
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



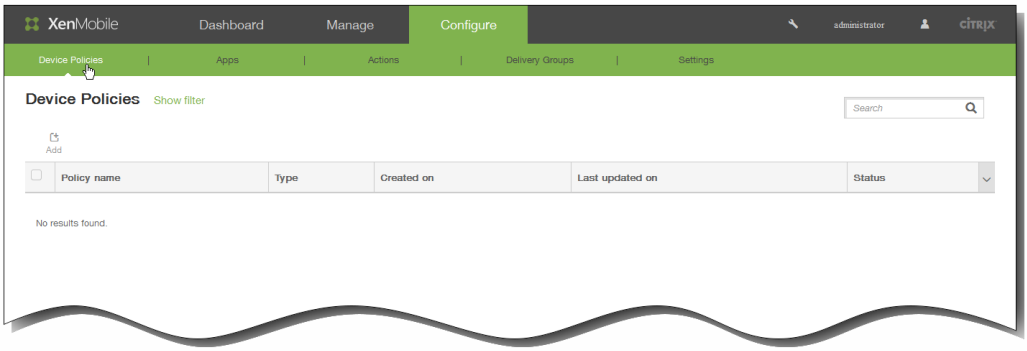
15. ［Save］をクリックしてポリシーを保存します。

iOSの連絡先（CardDAV）デバイスポリシーを追加するには

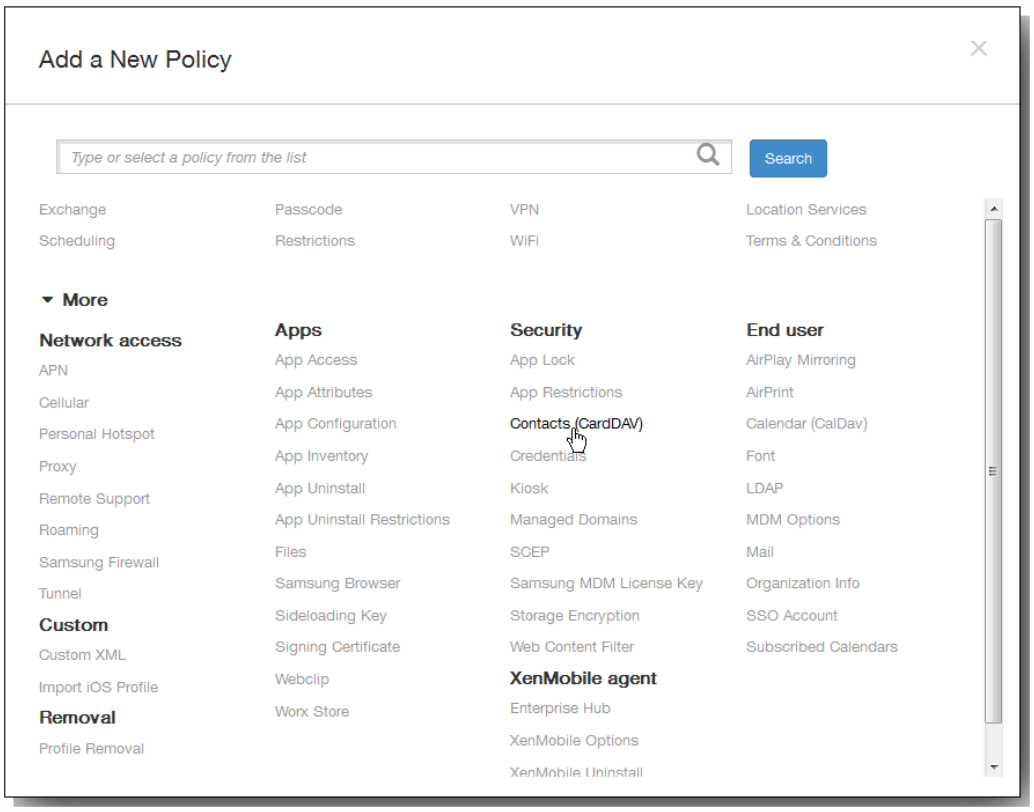
May 10, 2016

XenMobileでデバイスポリシーを追加して、iOS連絡先（CardDAV）アカウントをユーザーのiOSデバイスに追加し、CardDAV をサポートするサーバーとそのデバイスの連絡先データを同期することができます。

1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。

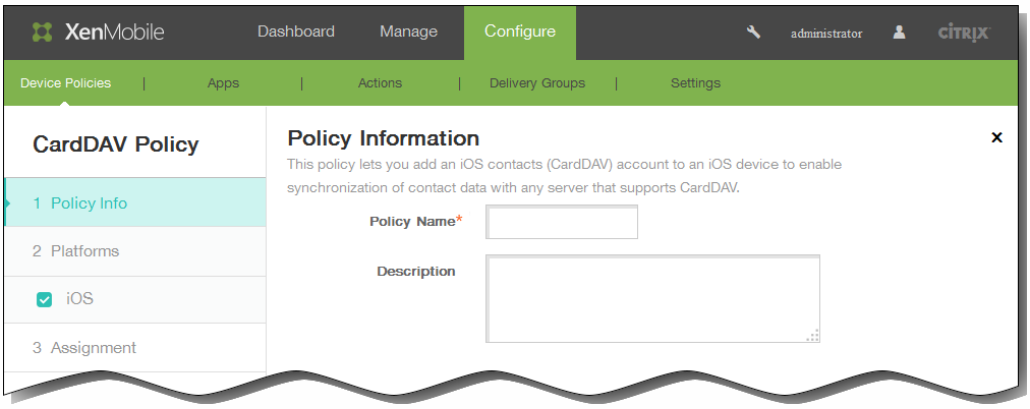


2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。

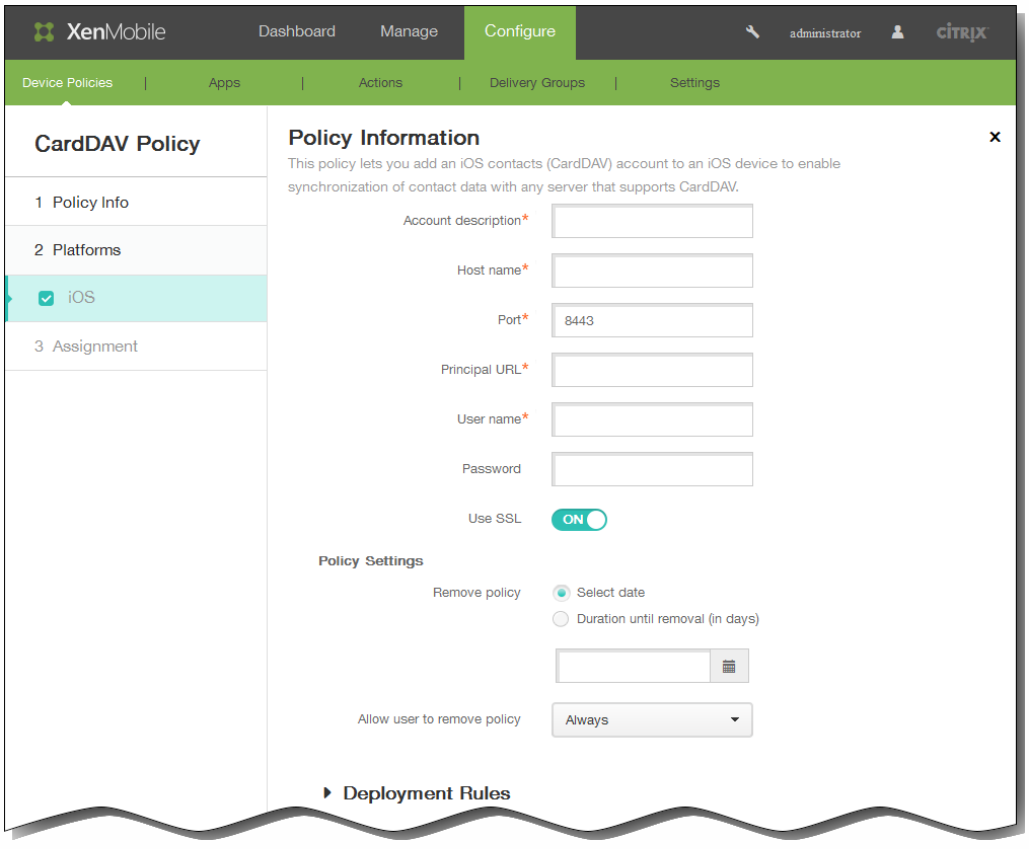


3. ［More］をクリックした後、［Security］の下の［Contacts CardDAV］をクリックします。 ［CardDAV Policy］ページが

開きます。



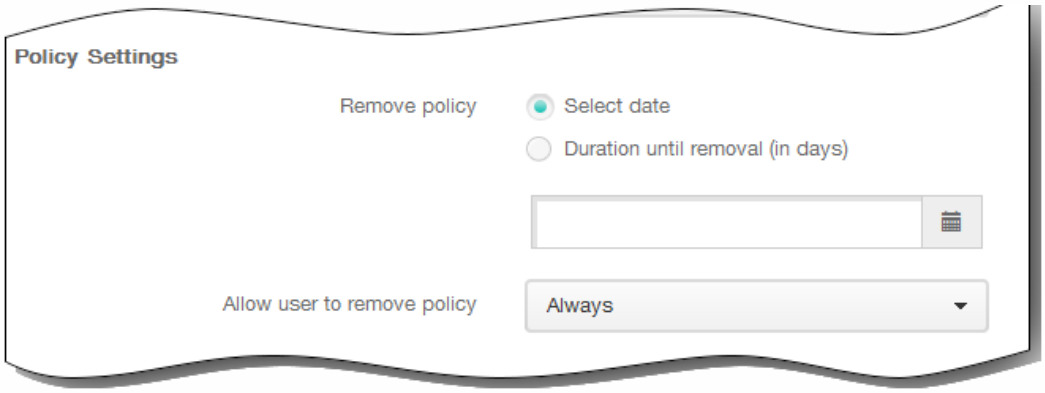
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform Information］ページが開きます。



6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. 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。
   2. 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。
   3. 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。

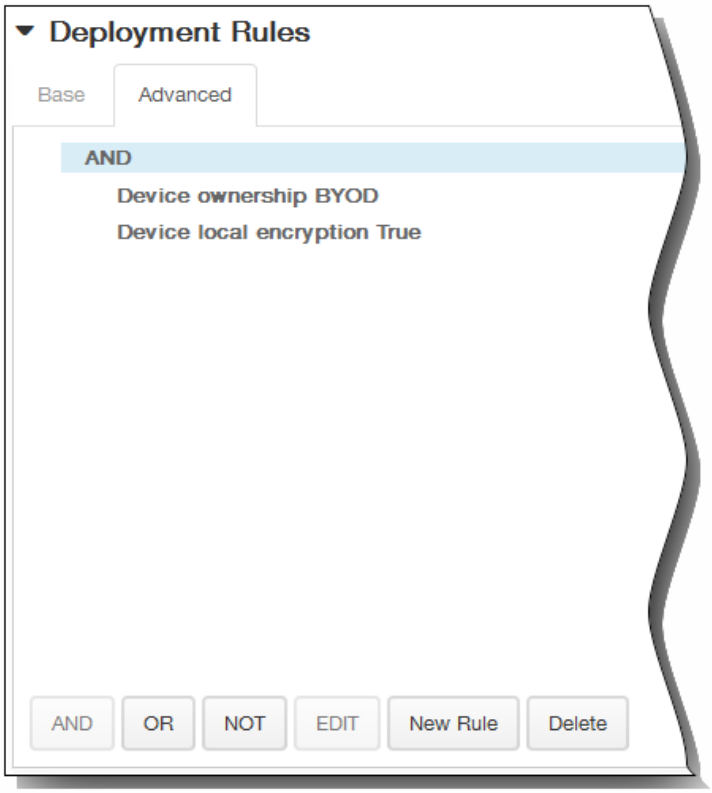
4. Principal URL：ユーザーのカレンダーに対するベースURLを入力します。
5. User name：ユーザーのログオン名を入力します。 このフィールドは必須です。
6. Password：任意で、ユーザーのパスワードを入力します。
7. Use SSL：CardDAVサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［ON］です。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

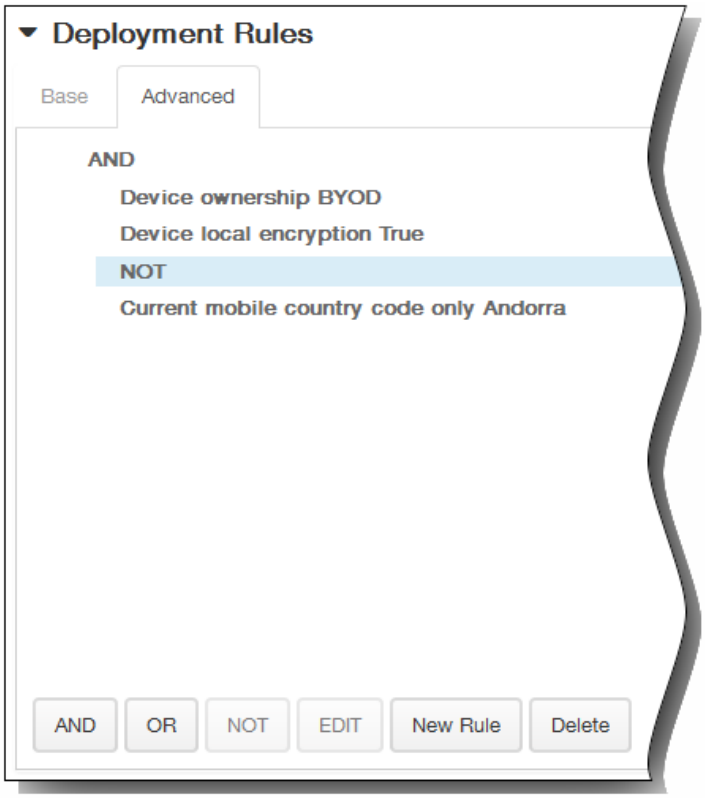
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



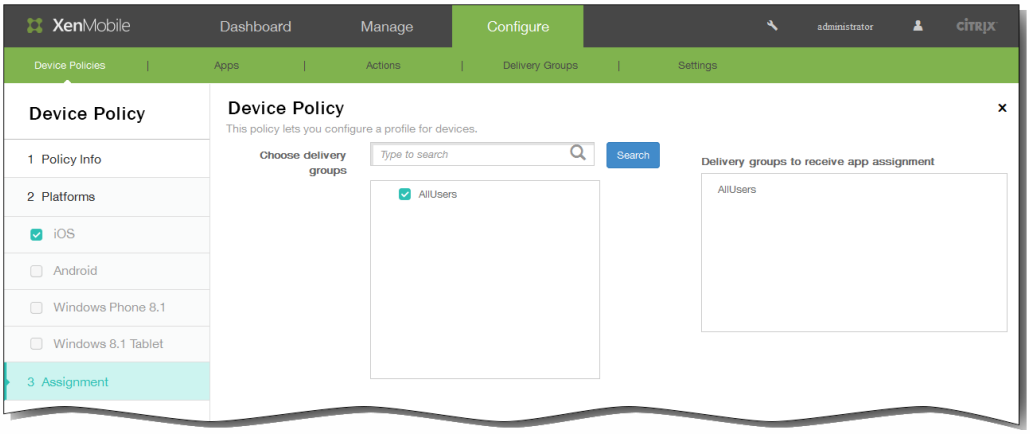
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［CardDAV Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



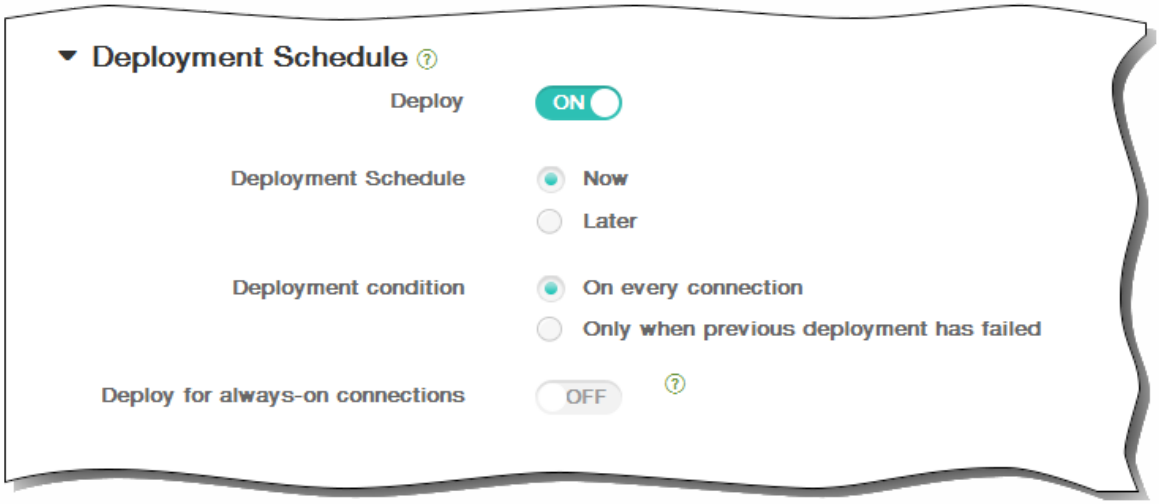
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



15. ［Save］をクリックしてポリシーを保存します。

資格情報デバイスポリシー

May 10, 2016

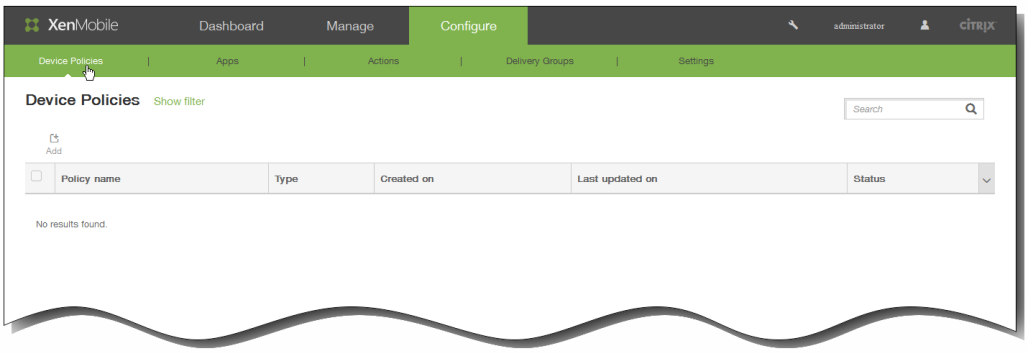
XenMobileで資格情報デバイスポリシーを作成し、XenMobileのPKI構成（PKIエンティティ、キーストア、資格情報プロバイダー、サーバー証明書など）を使用した統合認証を有効にすることができます。資格情報について詳しくは、「XenMobileでの証明書」を参照してください。

資格情報ポリシーは、iOS、Android、Windows 8.1タブレットデバイスに対して作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

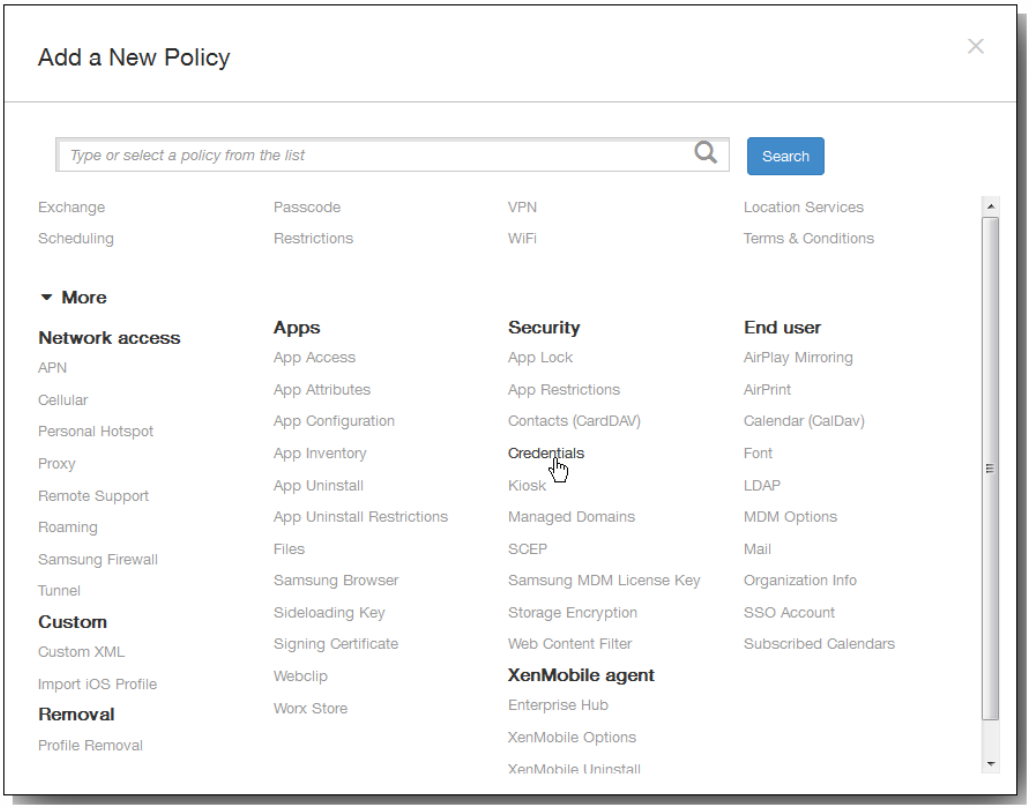
このポリシーを作成する前に以下の情報が必要です。

- 各プラットフォームで使用する予定の資格情報と、証明書およびパスワード。

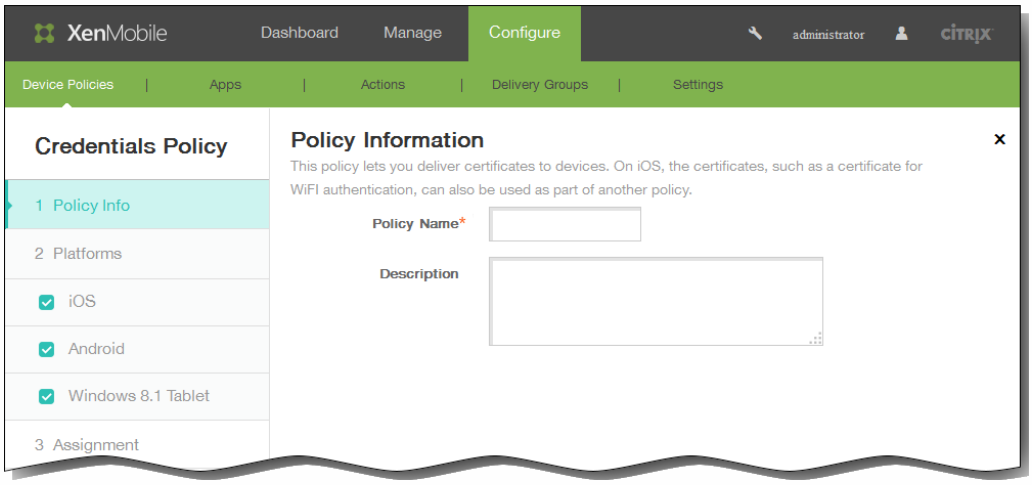
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



2. 新しいポリシーを追加するには［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。

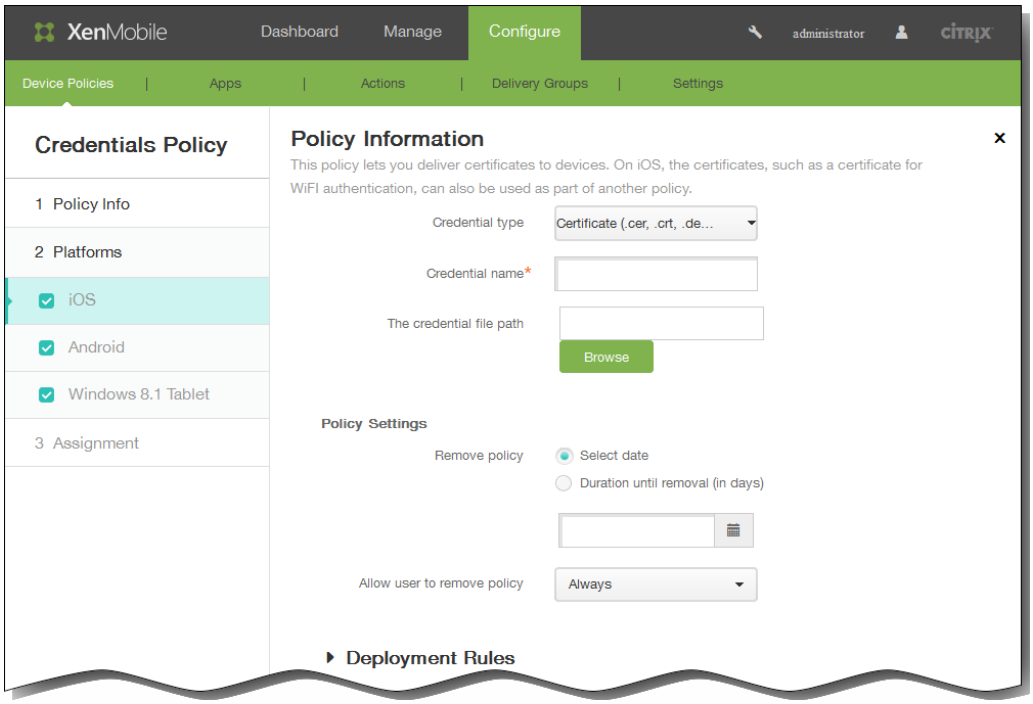


3. ［More］をクリックした後、［Security］の下の［Credentials］をクリックします。 ［Credentials Policy］情報ページが開きます。

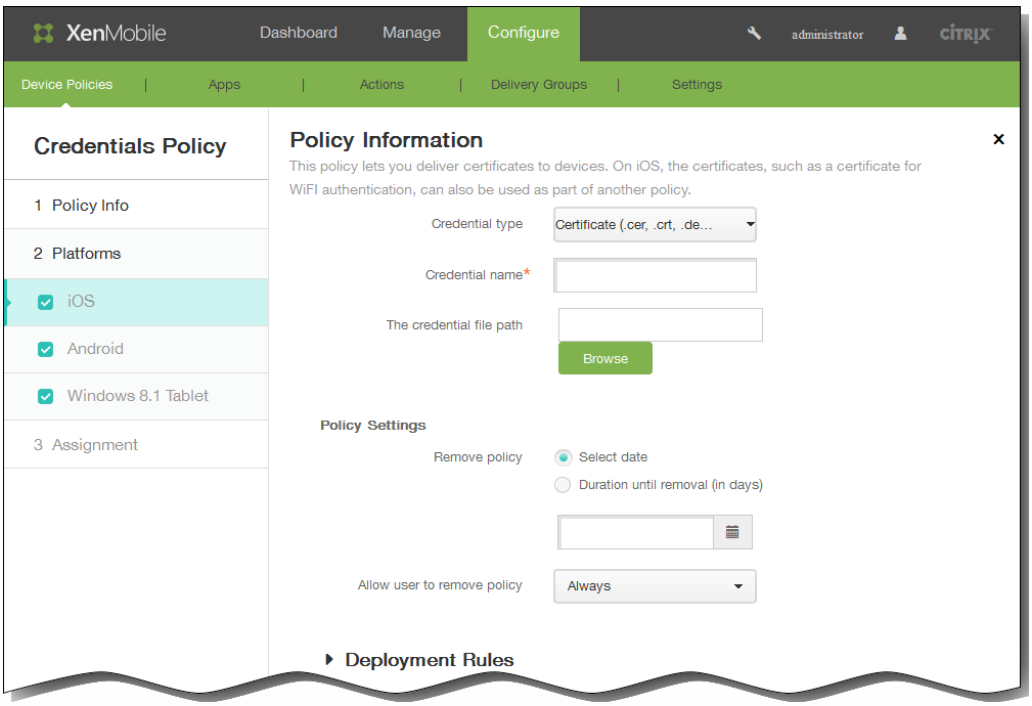


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。

注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォーム構成パネルが開きます。



6. ［Platforms］の下で、追加するプラットフォームをオンにします。
   - ［iOS］を選択した場合は、次の設定を構成します。



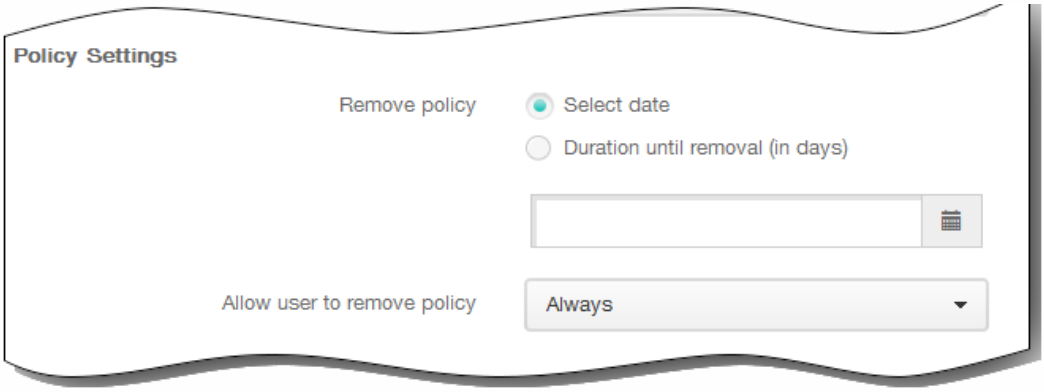
Credential type：ボックスの一覧で、このポリシーで使用する資格情報の種類を選択します。

選択した資格情報に応じて以下の情報を入力します。

- **証明書**
  - Credential name：資格情報の固有の名前を入力します。
  - The credential file path：［Browse］をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。

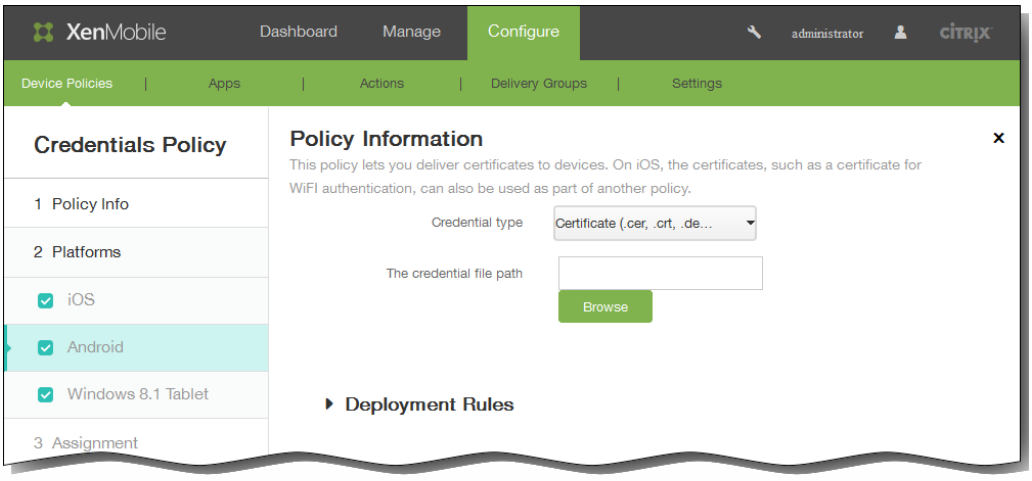
- **キーストア**
  - Credential name：資格情報の固有の名前を入力します。
  - The credential file path：［Browse］をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - Password：資格情報のキーストアパスワードを入力します。
- **サーバー証明書**
  - Server certificate：ボックスの一覧で、使用する証明書を選択します。
- **資格情報プロバイダー**
  - Credential provider：ボックスの一覧で、資格情報プロバイダーの名前を選択します。

ポリシー設定



1. ［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。
2. ［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。
3. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
4. ［Password required］を選択した場合、［Removal password］の横に必要なパスワードを入力します。

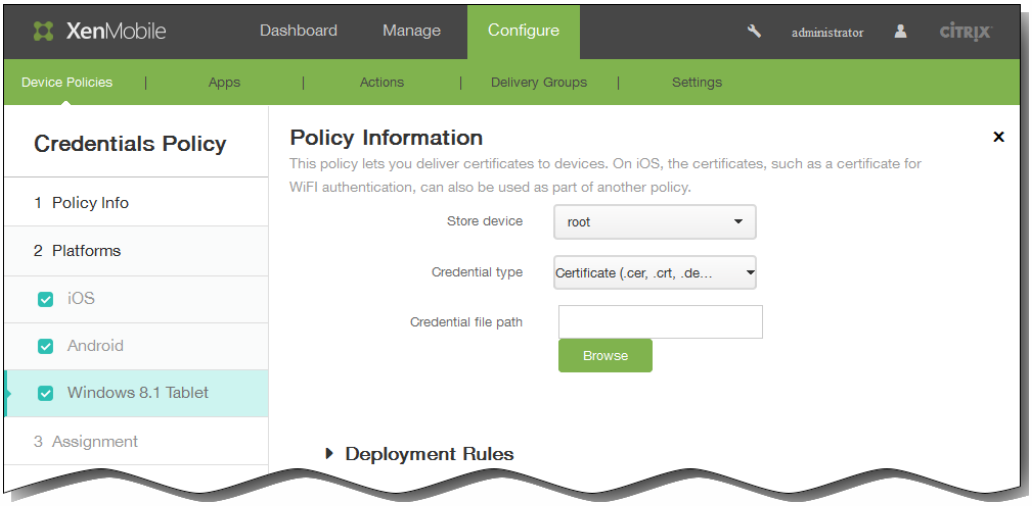
- ［Android］を選択した場合は、次の設定を構成します。



Credential type：ボックスの一覧で、このポリシーで使用する資格情報の種類を選択します。

選択した資格情報に応じて以下の情報を入力します。

- **証明書**
  - Credential name：資格情報の固有の名前を入力します。
  - The credential file path：［Browse］をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
- **キーストア**
  - Credential name：資格情報の固有の名前を入力します。
  - The credential file path：［Browse］をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - Password：資格情報のキーストアパスワードを入力します。
- **サーバー証明書**
  - Server certificate：ボックスの一覧で、使用する証明書を選択します。
- **資格情報プロバイダー**
  - Credential provider：ボックスの一覧で、資格情報プロバイダーの名前を選択します。
- ［Windows 8.1 Tablet］を選択した場合は、次の設定を構成します。



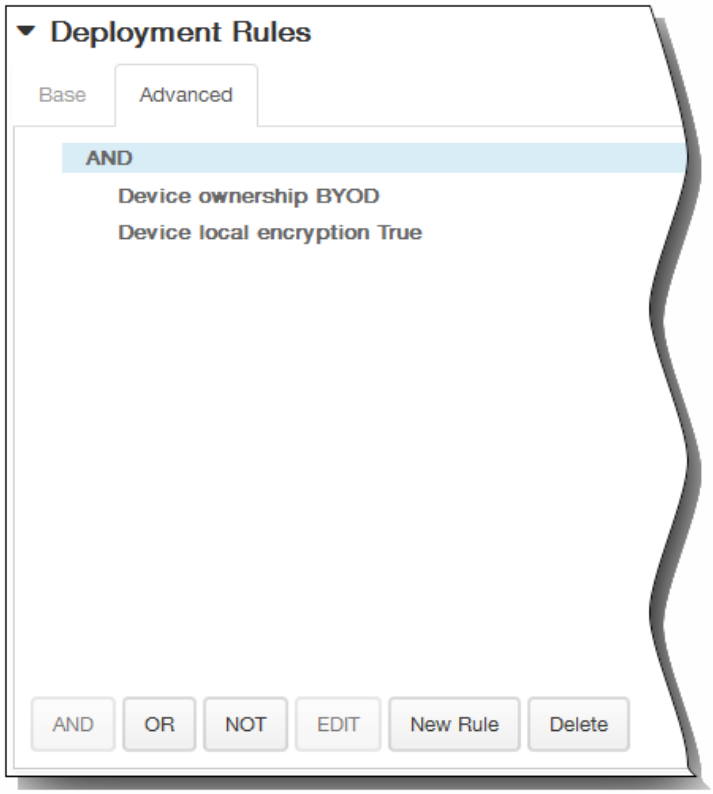
Store device：資格情報の証明書ストアの場所に応じて、ボックスの一覧で［root］、［My］、［CA］のいずれかを選択します。［My］を選択すると、証明書はユーザーの証明書ストアに保存されます。

Credential type：Windows 8.1タブレットの場合、資格情報の種類は証明書のみです。

The credential file path：［Browse］をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。

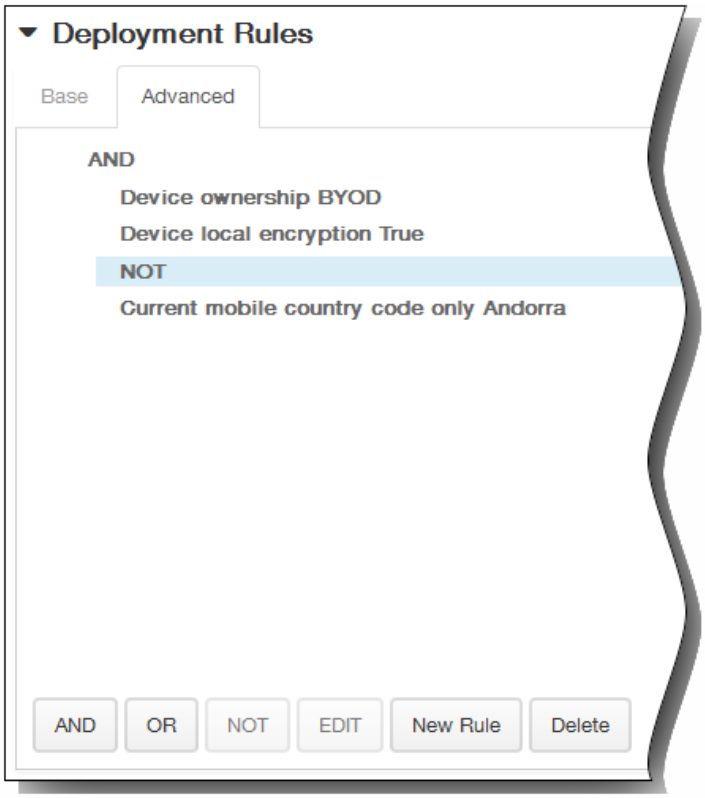
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

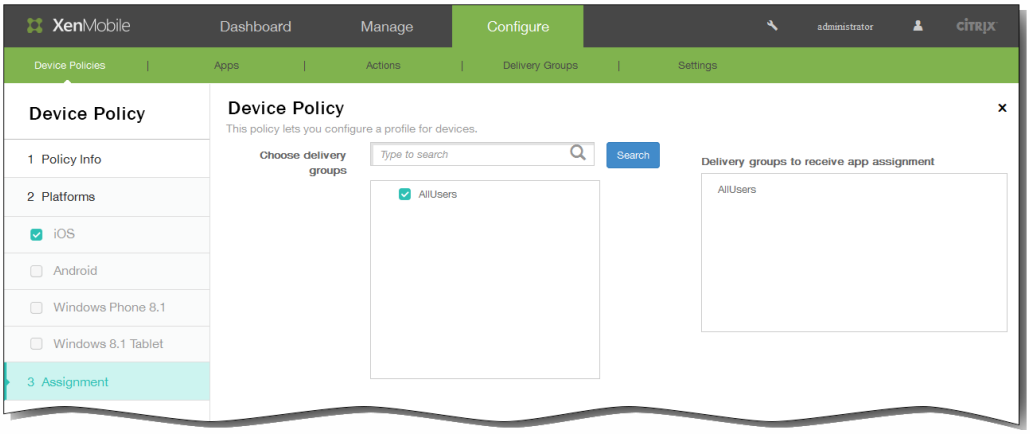


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Credentials Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



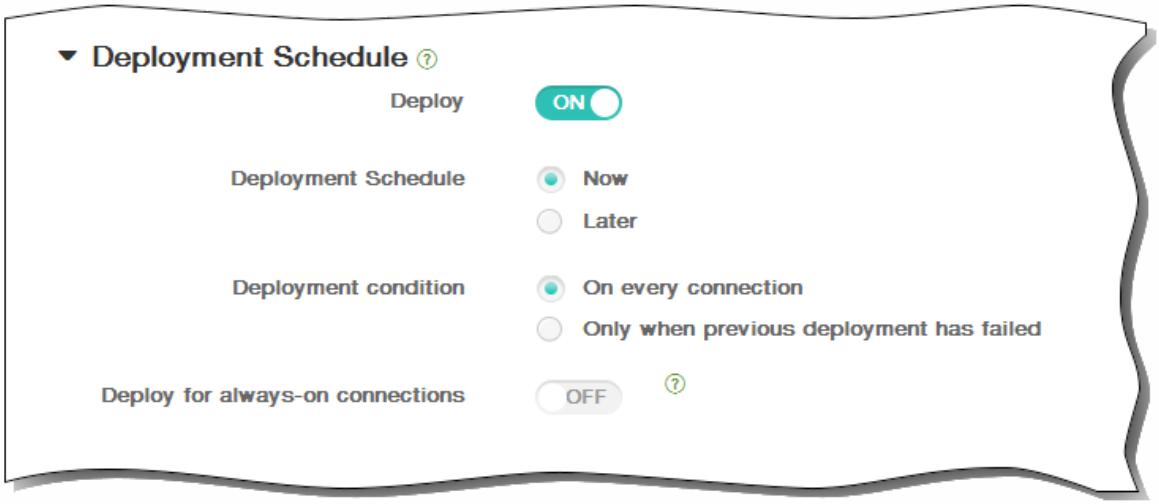
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

Samsung SAFEのキオスクデバイスポリシーを追加するには

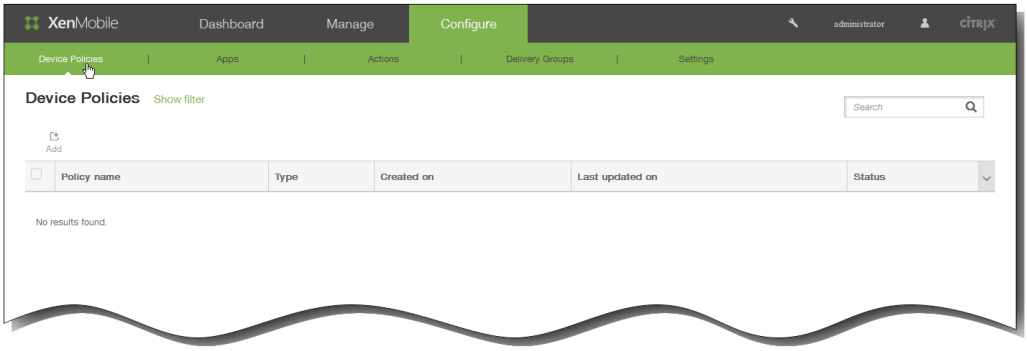
May 10, 2016

XenMobileでキオスクポリシーを作成して、特定のアプリケーションのみをSamsung SAFEデバイスで使用できるように指定することができます。このポリシーは、特定の種類またはクラスのアプリケーションのみを実行するように設計されているコーポレートデバイスで役立ちます。また、このポリシーを使用して、デバイスがキオスクモードのときのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。

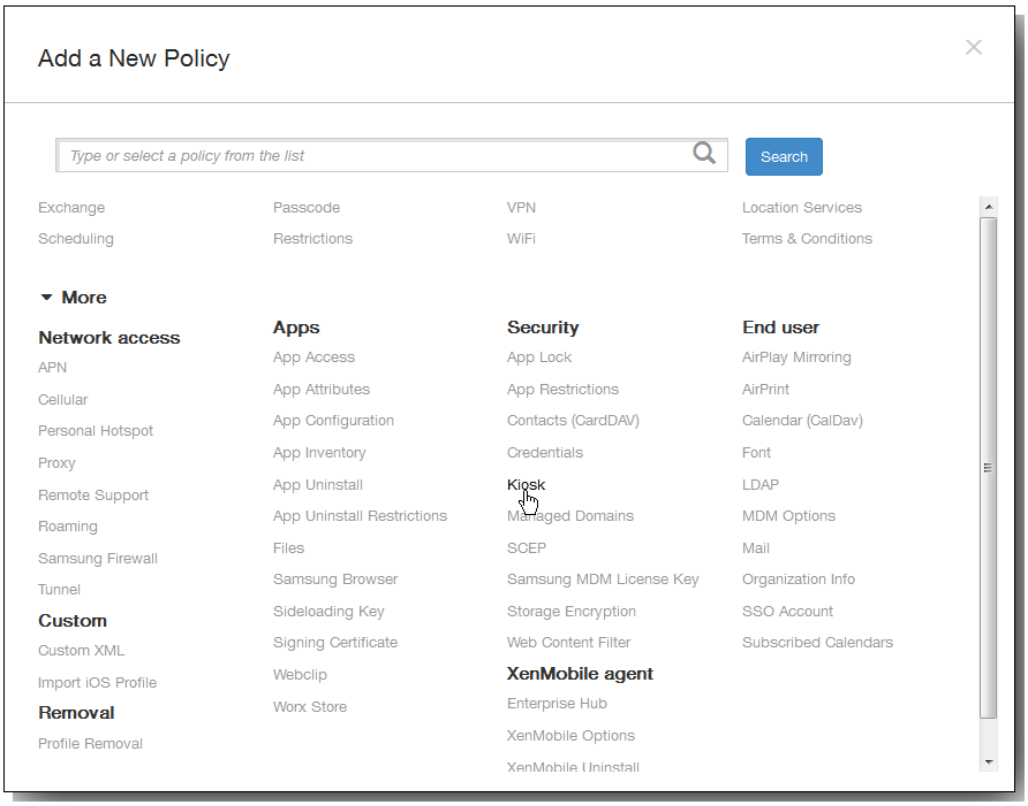
注：

- 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API 4.0以降にのみ適用されます。

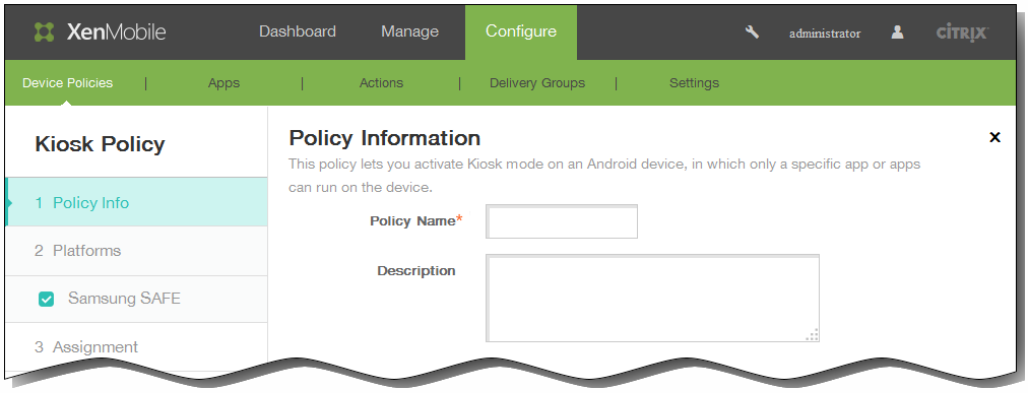
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



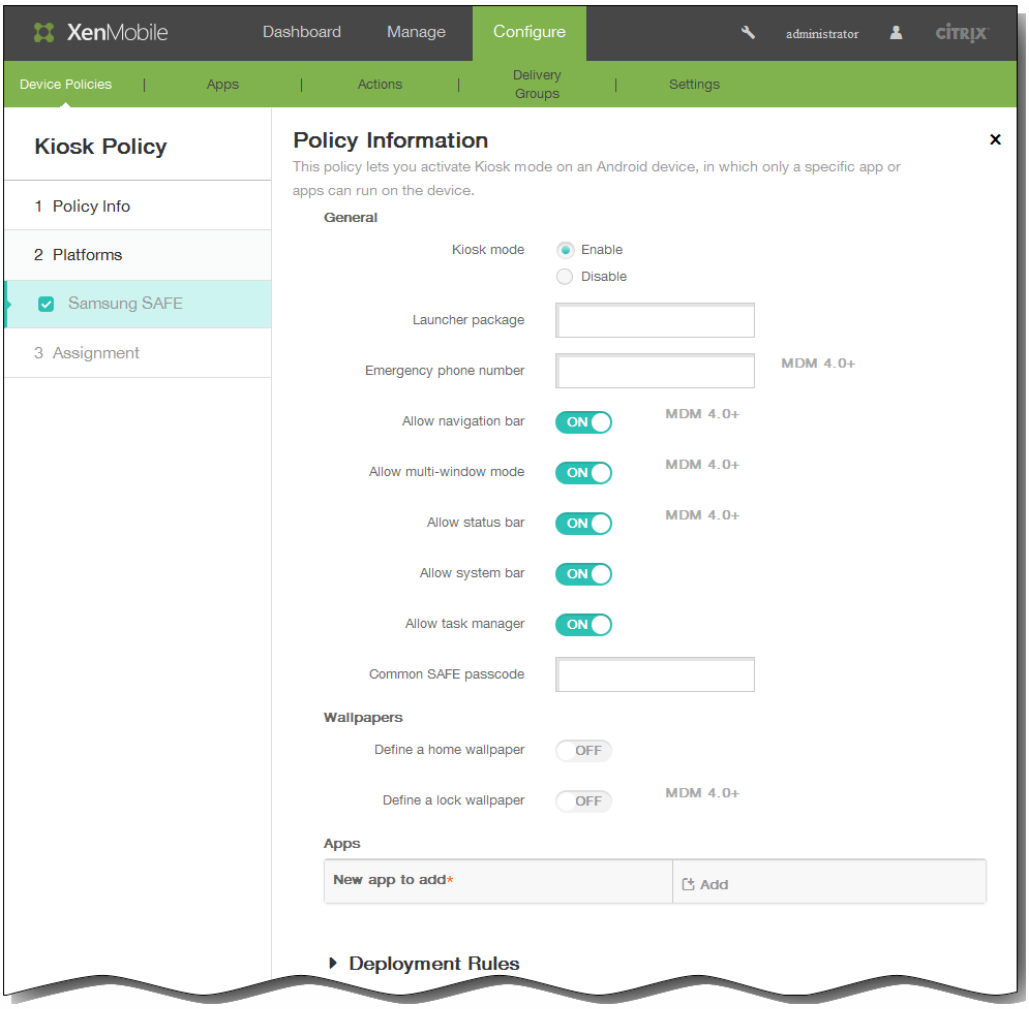
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Security］の下の［Kiosk］をクリックします。 ［Kiosk Policy］ページが開きます。



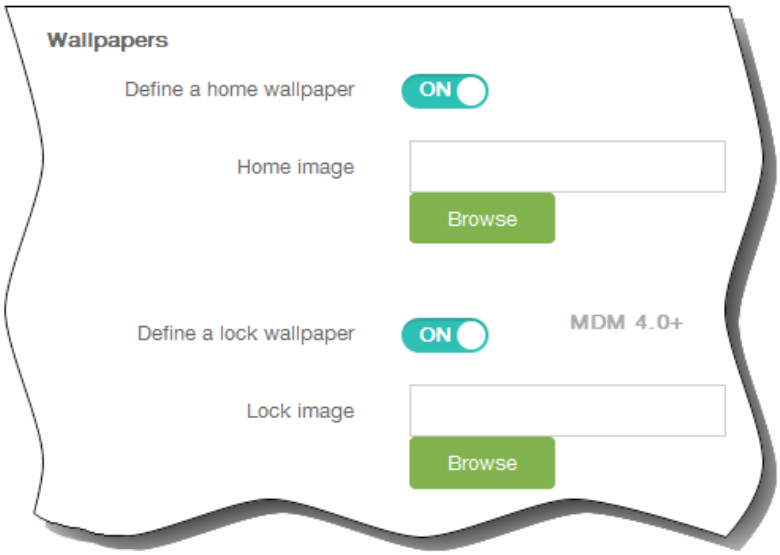
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Samsung SAFE Platform］情報ページが開きます。



6. ［Samsung SAFE Platform］情報ページで、以下の情報を入力します。
   1. Kiosk mode：［Enable］または［Disable］をクリックします。 デフォルトは［Enable］です。 ［Disable］をクリックすると、以下のオプションはすべて表示されなくなります。
   2. 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。
   3. 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。 Samsungモバイルデバイス管理API 4.0以降にのみ適用されます。
   4. Allow navigation bar：キオスクモードのときに、ユーザーがナビゲーションバーを表示して使用できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。
   5. Allow multi-window mode：キオスクモードのときに、ユーザーが複数のウィンドウを使用できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。
   6. Allow status bar：キオスクモードのときに、ユーザーがステータスバーを表示できるようにするかどうかを選択します。 MDM 4.0以降にのみ適用されます。
   7. Allow system bar：キオスクモードのときに、ユーザーがシステムバーを表示できるようにするかどうかを選択します。
   8. Allow task manager：キオスクモードのときに、ユーザーがタスクマネージャーを表示して使用できるようにするかどうかを選択します。
   9. 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。
   10. Define a home wallpaper：キオスクモードのときに、ホーム画面でカスタムイメージを使用するかどうかを選択しま

す。 デフォルトは［OFF］です。

11. Define a lock wallpaper：キオスクモードのときに、ロック画面でカスタムイメージを使用するかどうかを選択します。 デフォルトは［OFF］です。 MDM 4.0以降にのみ適用されます。 壁紙に関する上記のオプションが有効になっている場合、カスタムイメージを選択するフィールドが表示されます。［Browse］をクリックしてイメージの場所に移動し、選択することができます。



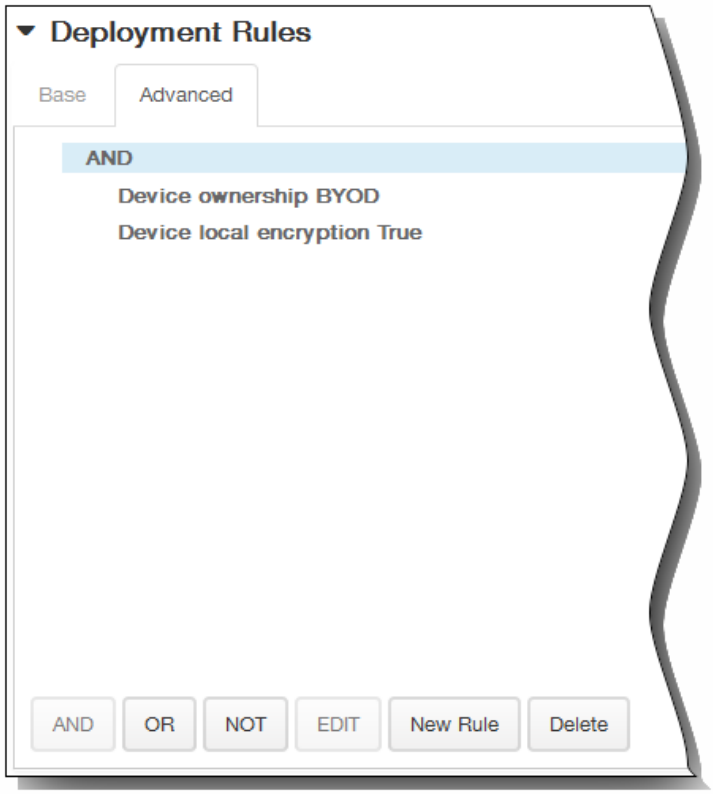
12. Apps：［Add］をクリックして、以下の操作を行います。
    1. New app to add：追加するアプリケーションの完全な名前を入力します。たとえば、「com.android.calendar」を入力すると、ユーザーがAndroidのカレンダーアプリケーションを使用できます。
    2. ［Add］をクリックしてアプリケーションを追加するか、［Cancel］をクリックしてアプリケーションの追加を取り消します。
    3. 追加するカスタムキーごとに手順iおよびii.を繰り返します。

    注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。

    既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

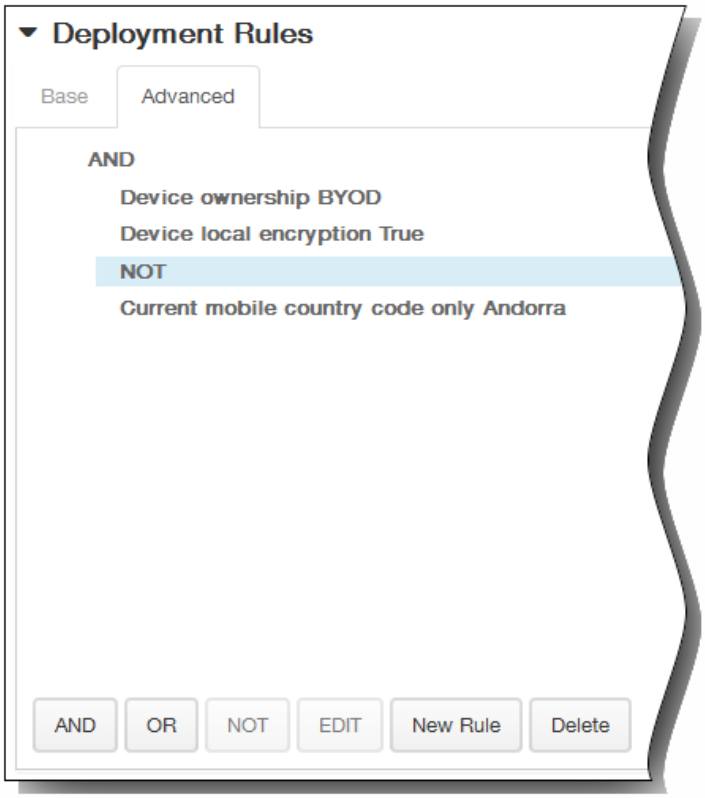
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



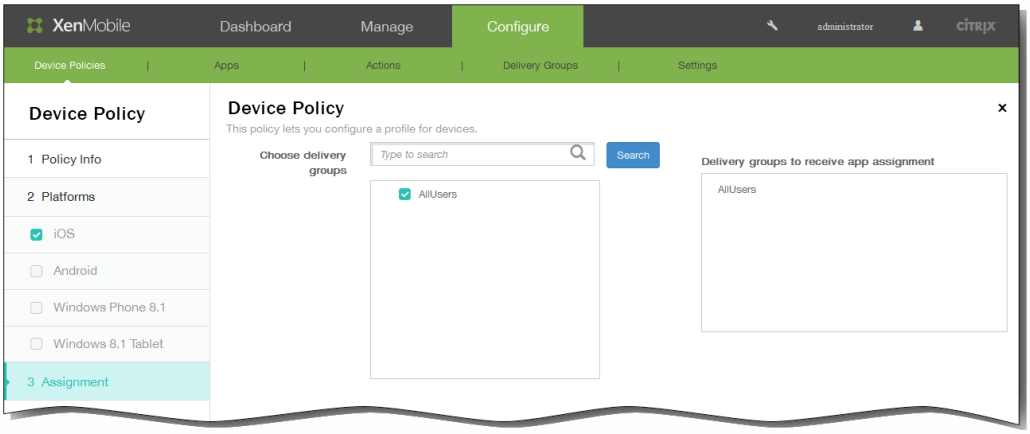
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
    1. ［AND］、［OR］、または［NOT］をクリックします。
    2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
    いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

    3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
    この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Kiosk Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



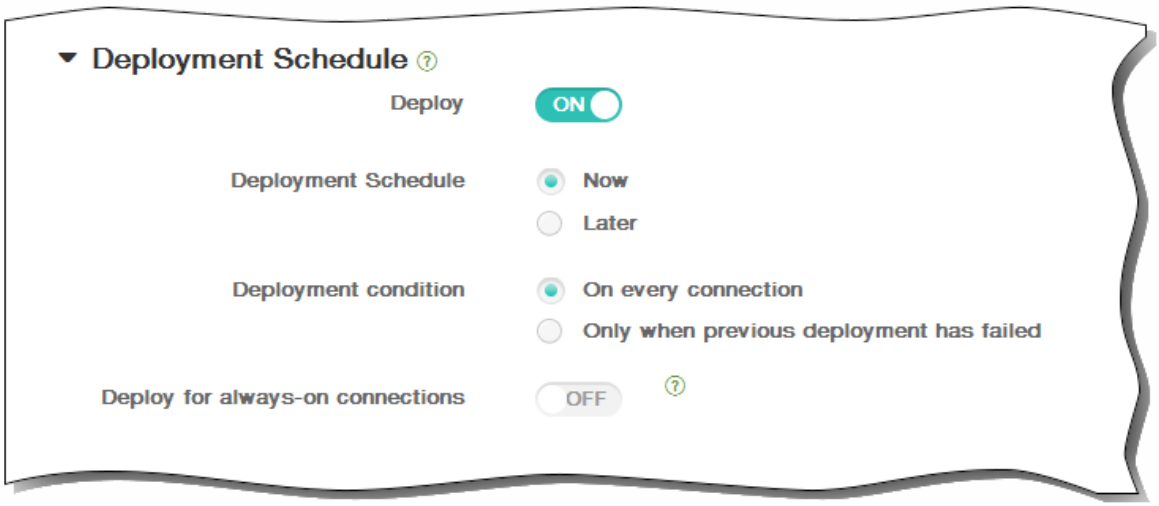
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

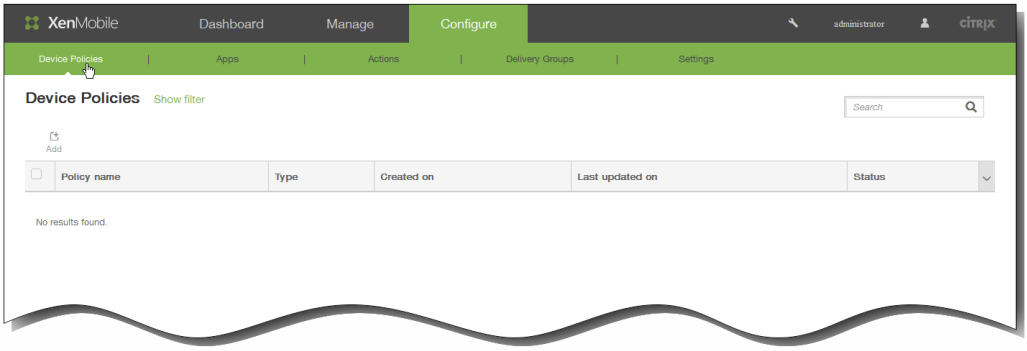
iOSのフォントデバイスポリシーを追加するには

May 10, 2016

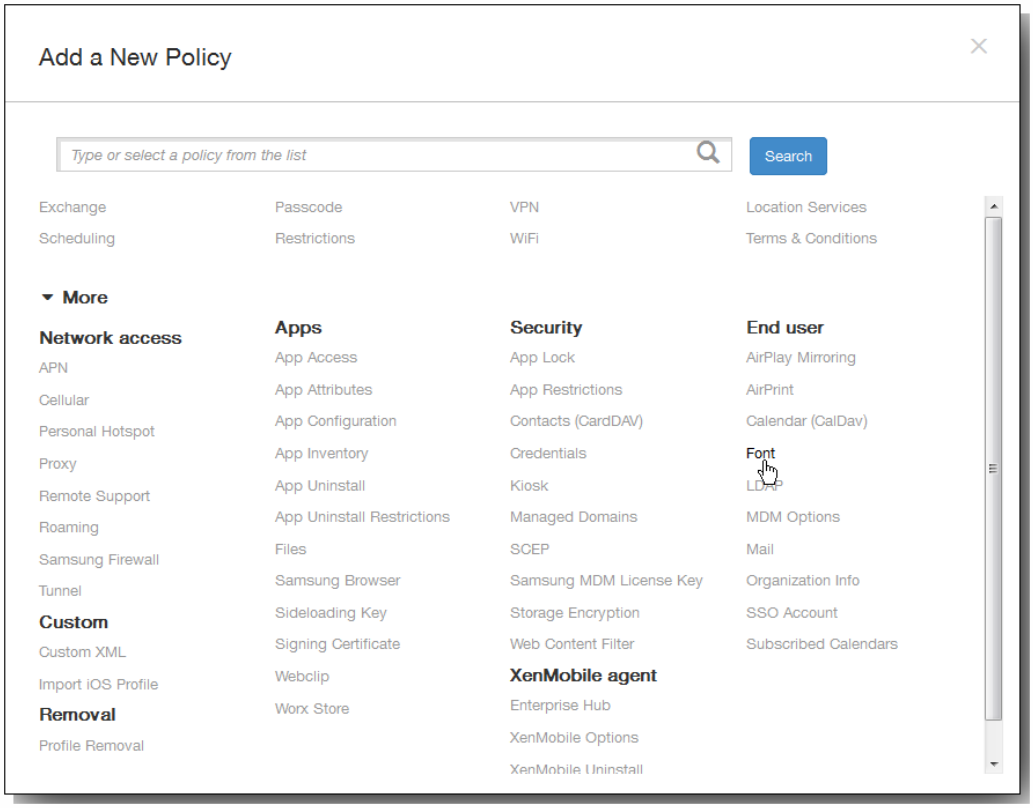
XenMobileでデバイスポリシーを追加して、追加フォントをユーザーのデバイスに追加することができます。フォントはTrueType（.ttf）またはOpenType（.oft）である必要があります。フォントコレクション（.ttcまたは.otc）はサポートされません。

注：このポリシーはiOS 7.0以降にのみ適用されます。

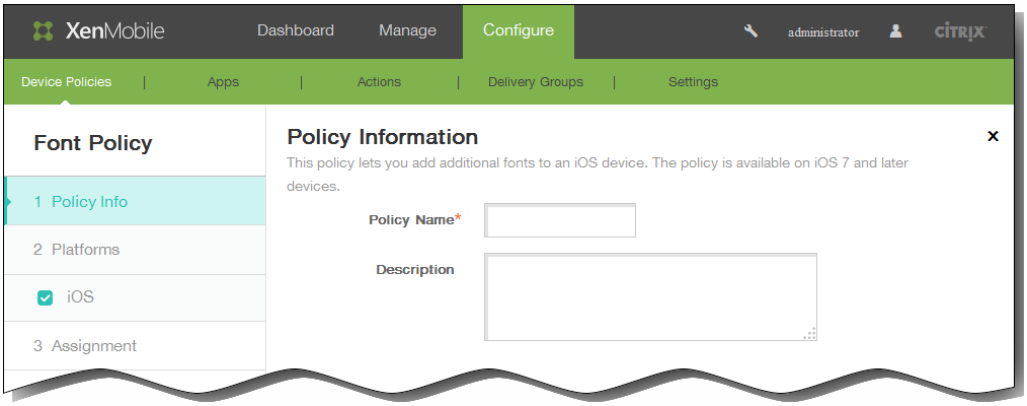
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



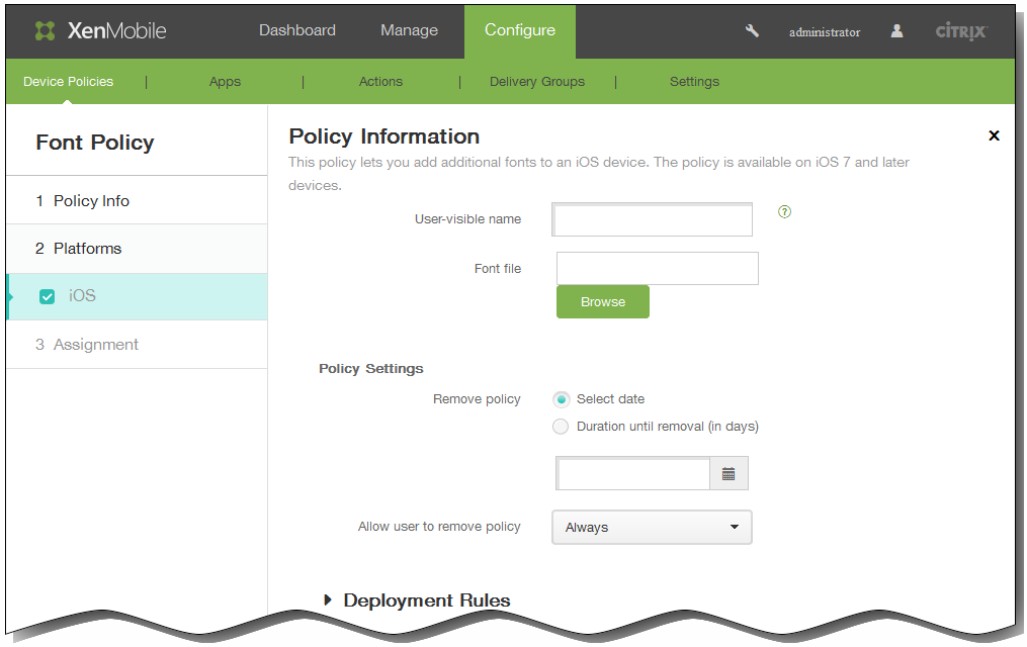
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



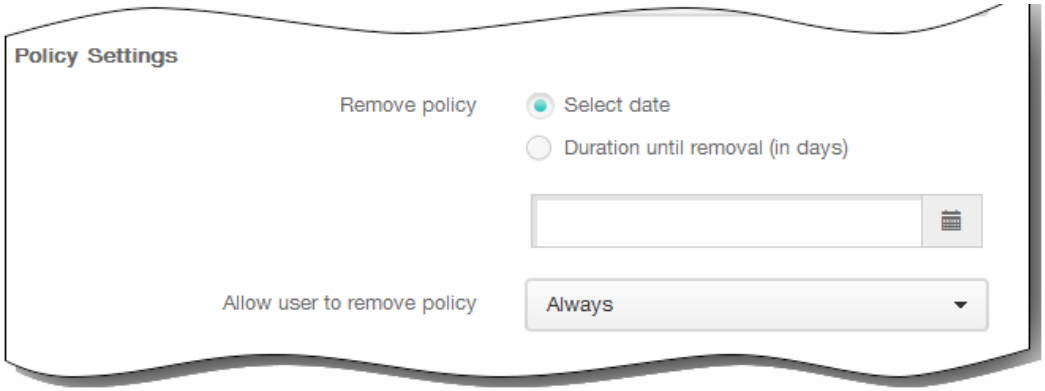
3. ［More］をクリックした後、［End user］の下の［Font］をクリックします。 ［Font Policy］ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。

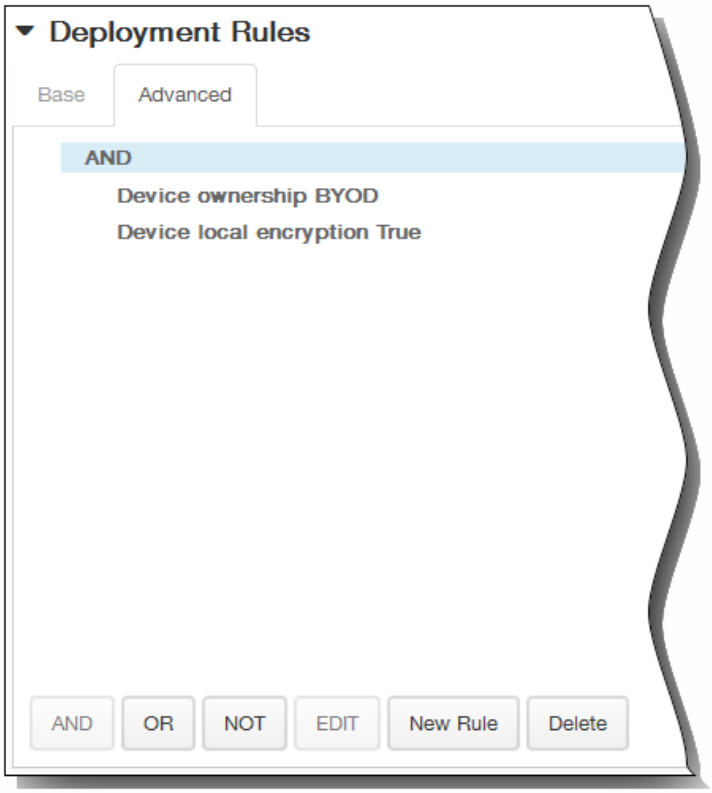


6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. User-visible name：ユーザーのフォント一覧に表示される名前を入力します。
   2. Font file：［Browse］をクリックしてファイルの場所に移動し、ユーザーのデバイスに追加するフォントファイルを選択します。
7. ［Policy Settings］の下の［Remove policy］の横にある、［Select date］または［Duration until removal (in days)］をクリックします。
8. ［Select date］をクリックした場合、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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

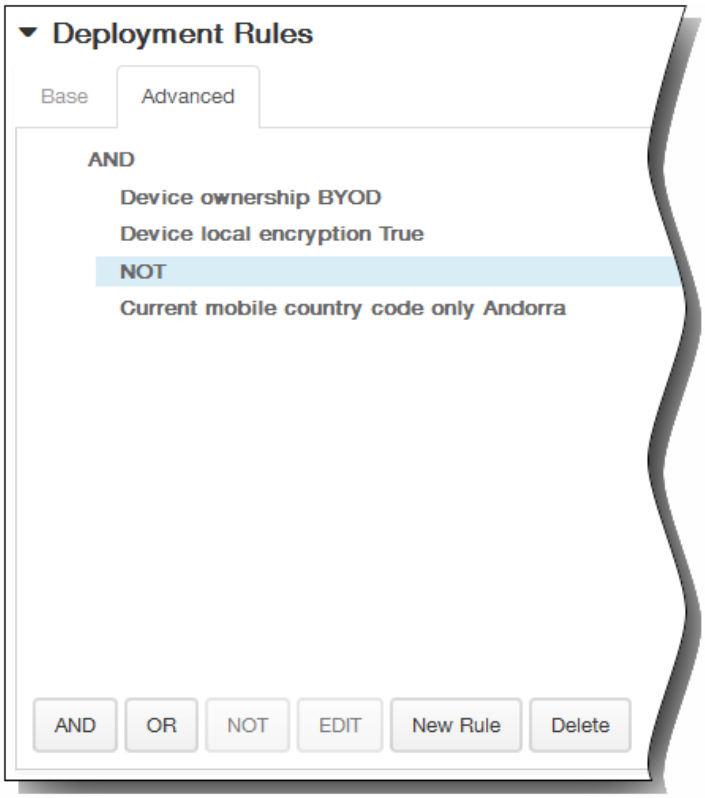
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



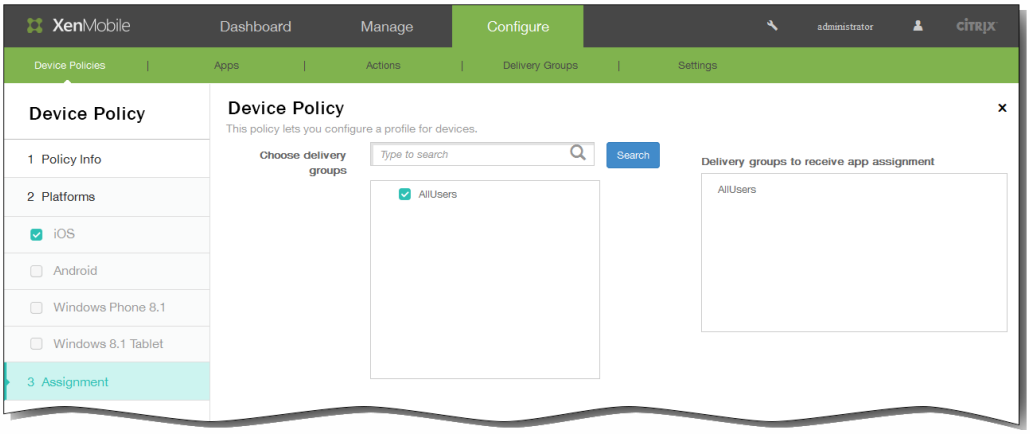
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［Font Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



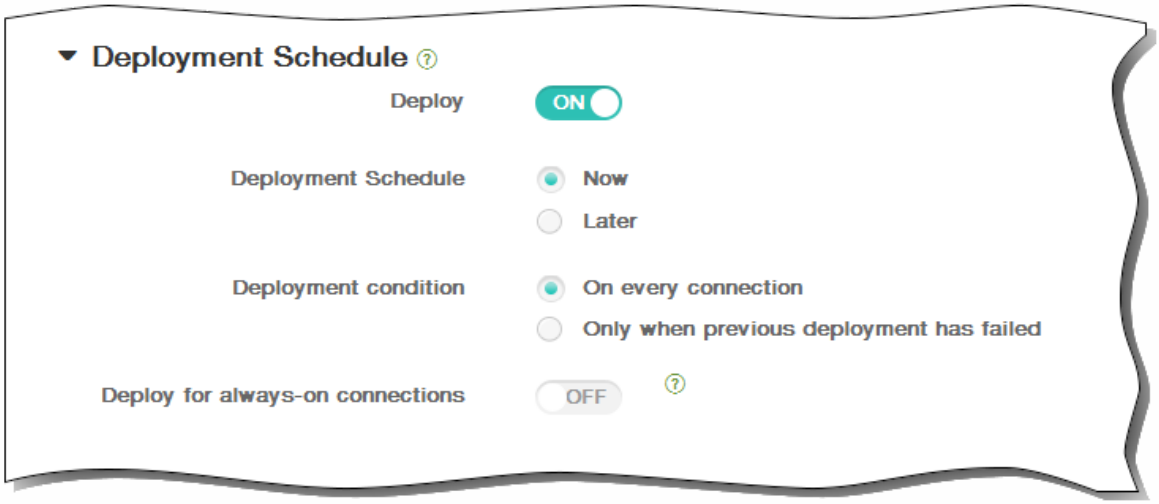
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



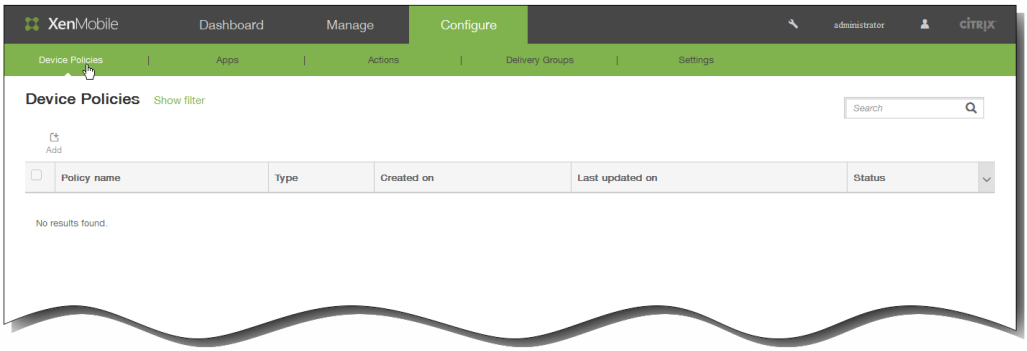
15. ［Save］をクリックしてポリシーを保存します。

iOSの組織情報デバイスポリシーを追加するには

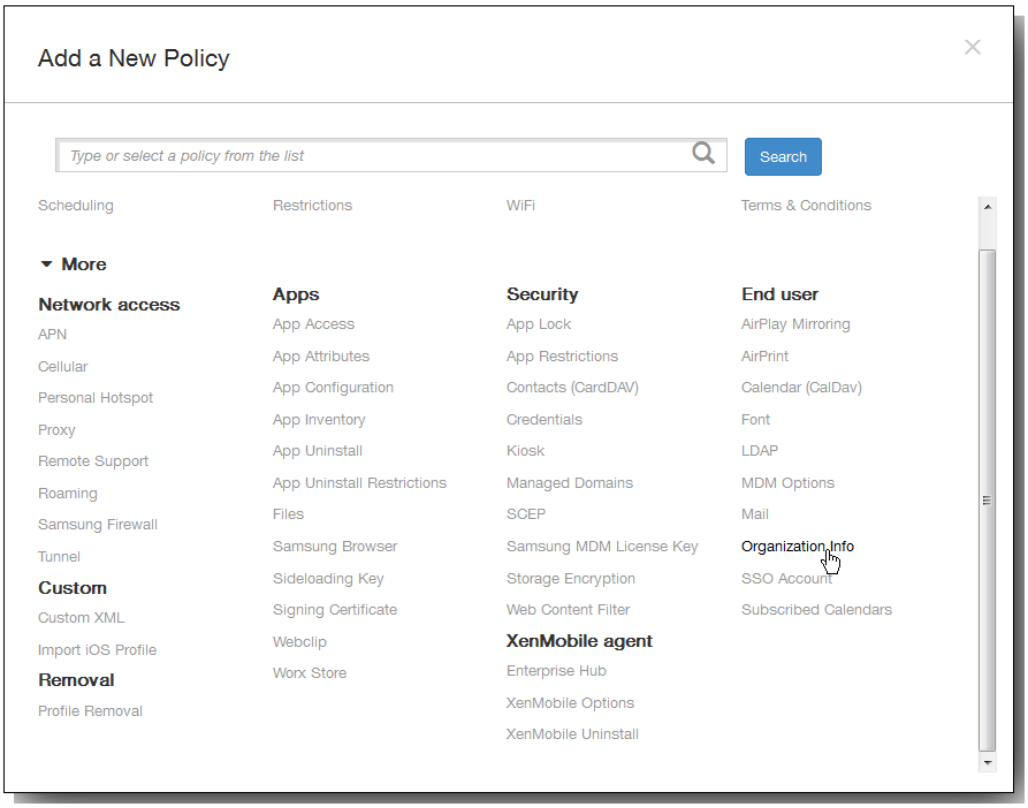
May 10, 2016

XenMobileでデバイスポリシーを追加して、XenMobileからiOSデバイスにプッシュされるアラートメッセージ用の組織情報を指定できます。このオプションはiOS 7以降のデバイスで使用できます。

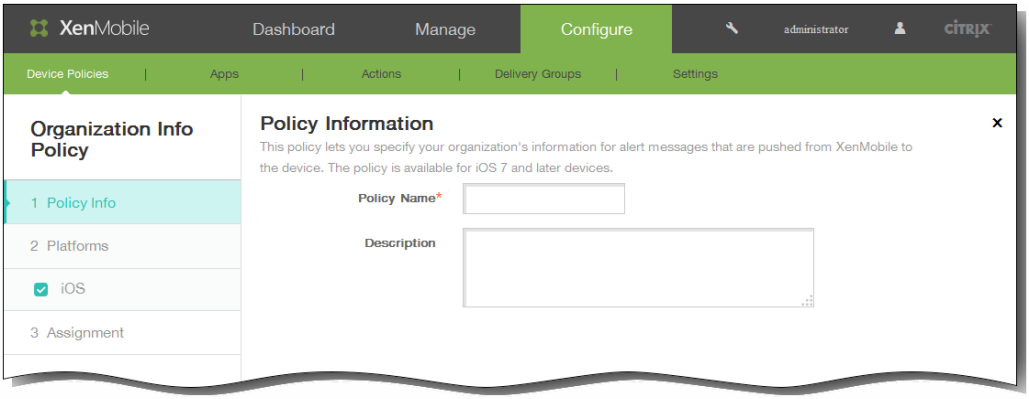
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



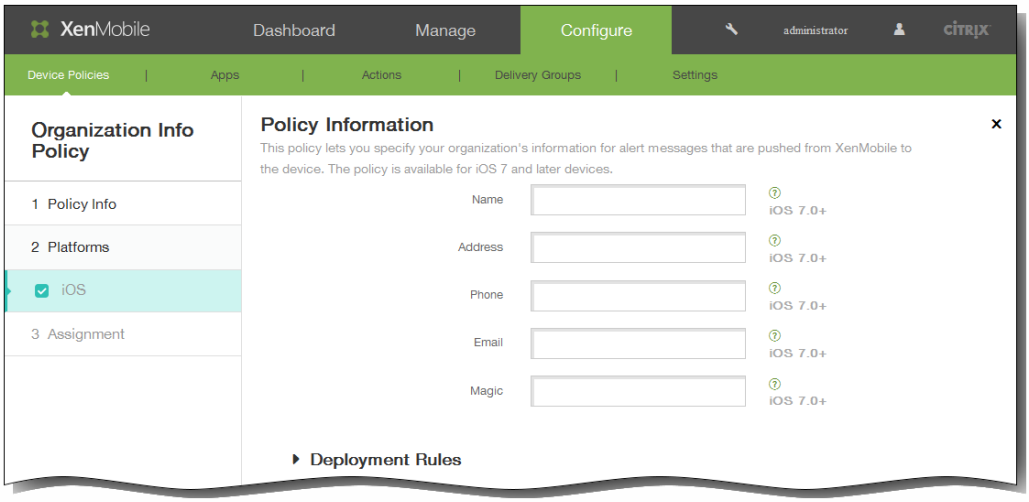
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［End user］の下の［Organization info］をクリックします。 ［Organization Info Policy］ページが開きます。

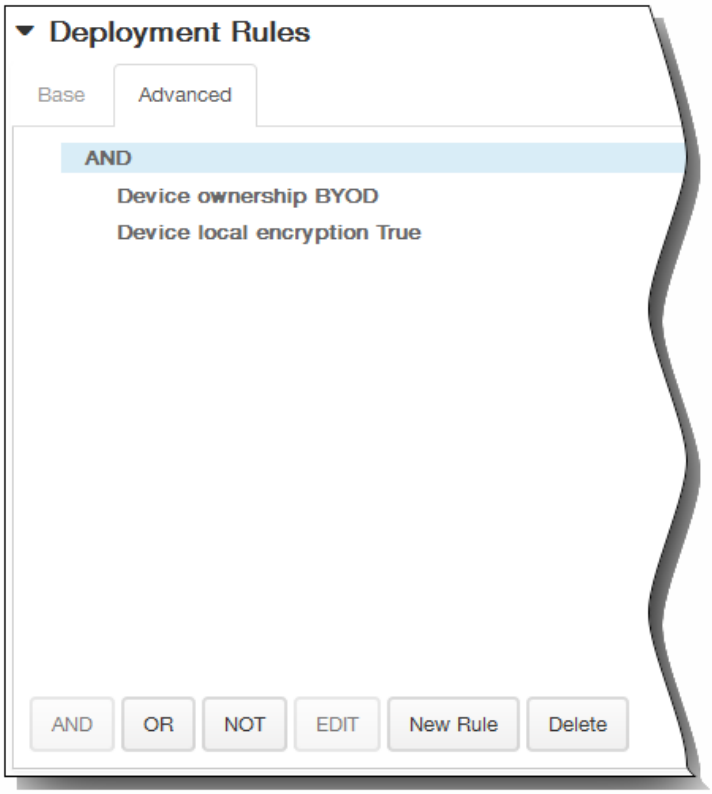


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：必要に応じて、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform Information］ページが開きます。



6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. Name：XenMobileを実行している組織の名前を入力します。
   2. Address：組織のアドレスを入力します。
   3. Phone：組織のサポート電話番号を入力します。
   4. Email：サポートメールアドレスを入力します。
   5. Magic：組織が管理しているサービスについて説明する語句を入力します。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

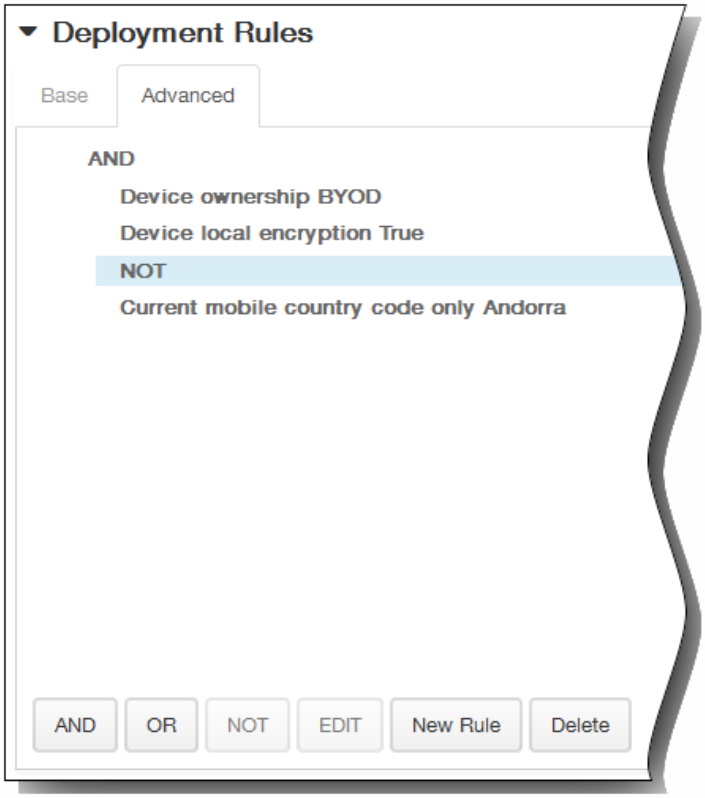


［Base］タブで選択した条件が表示されます。

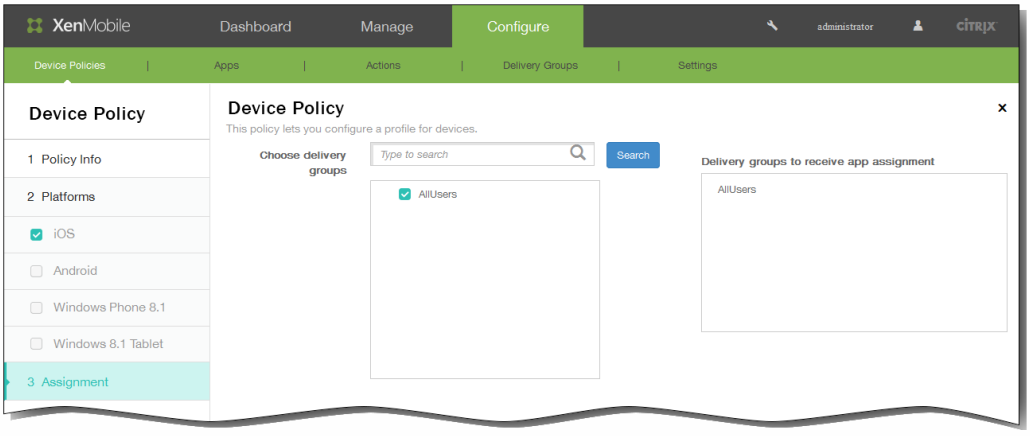
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Organization Info Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

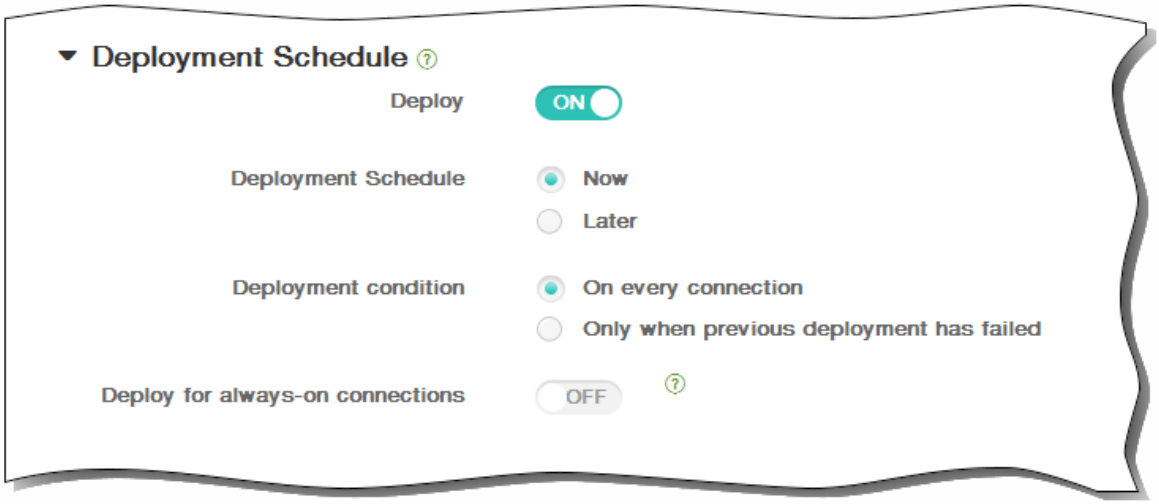


10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

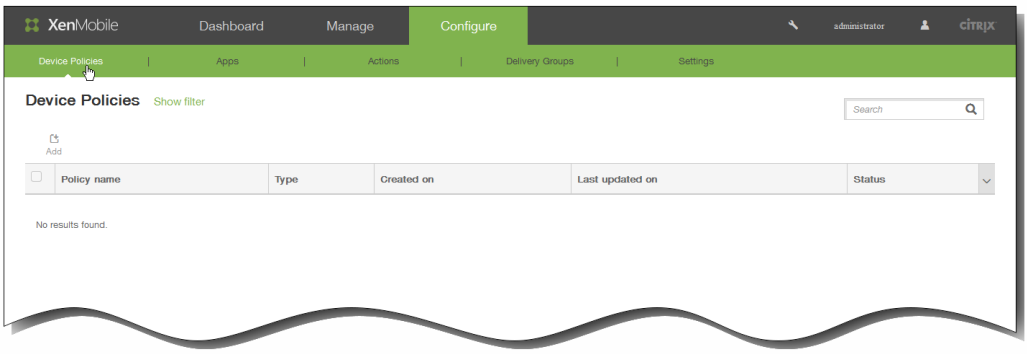
iOSのLDAPデバイスポリシーを追加するには

May 10, 2016

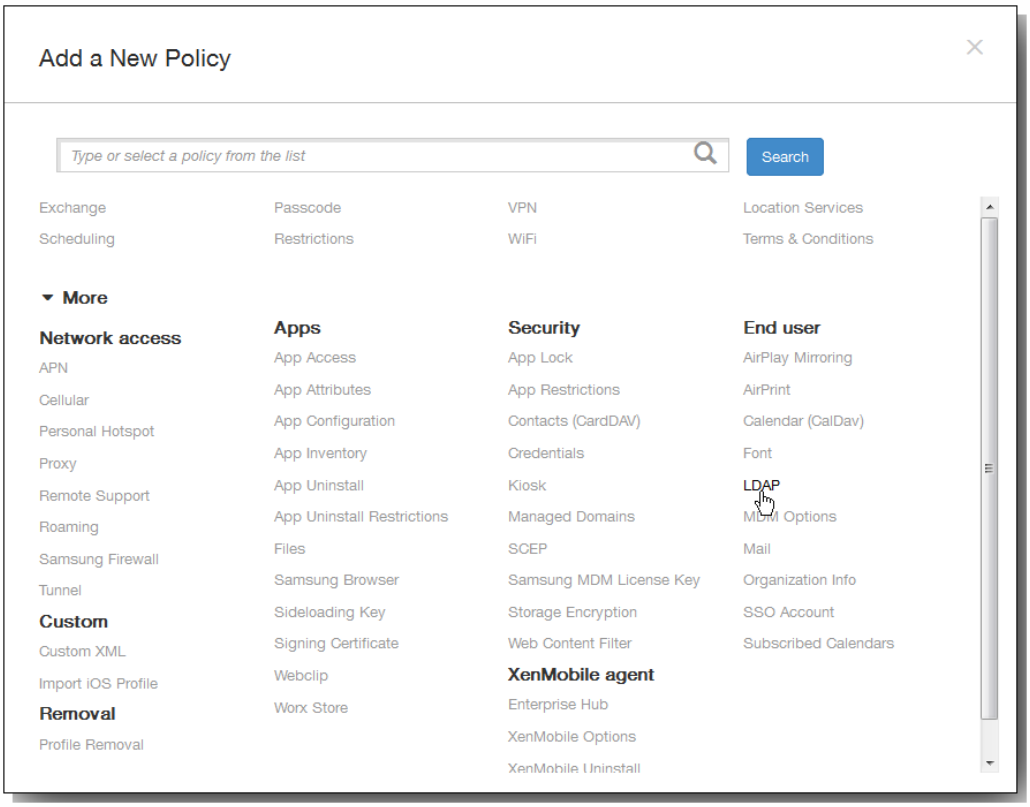
XenMobileでiOSデバイスのLDAPポリシーを作成して、必要なアカウント情報など、使用するLDAPサーバーに関する情報を指定できます。また、LDAPサーバーの照会に使用するLDAP検索ポリシーのセットが提供されます。

このポリシーを構成するには、LDAPホスト名が必要です。

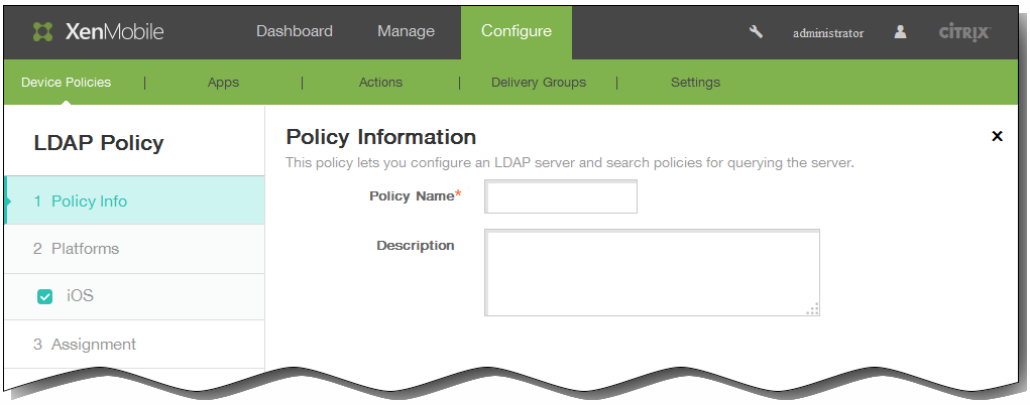
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



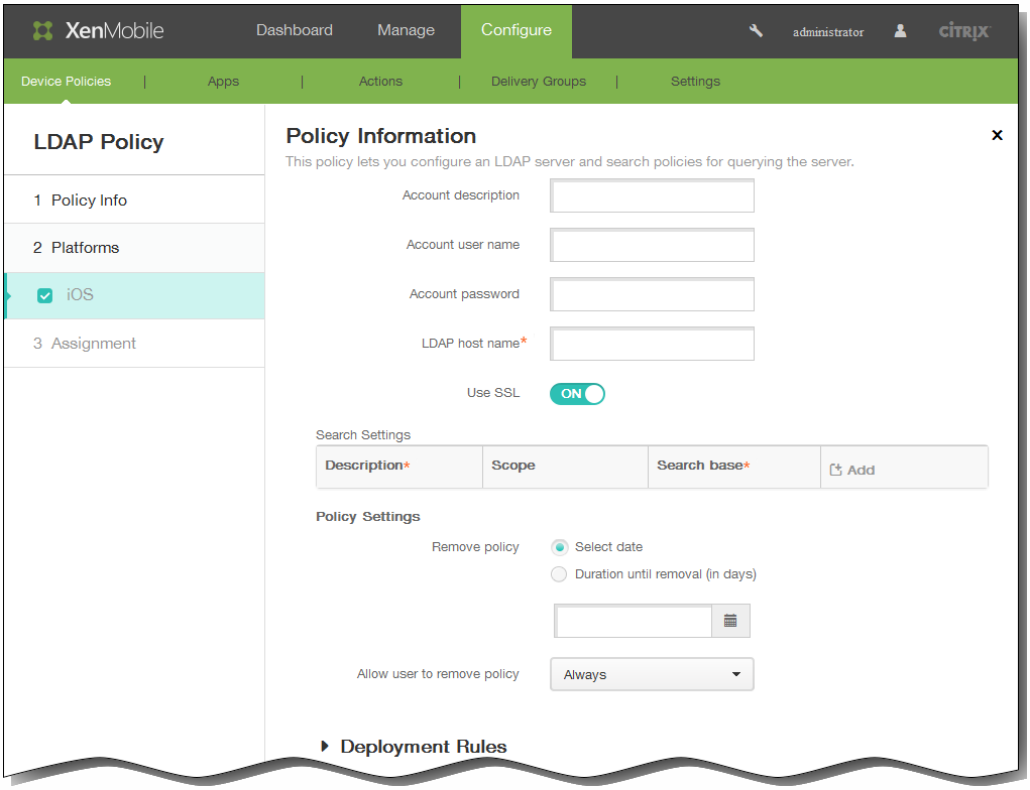
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［End user］の下の［LDAP］をクリックします。 ［LDAP Policy］ページが開きます。



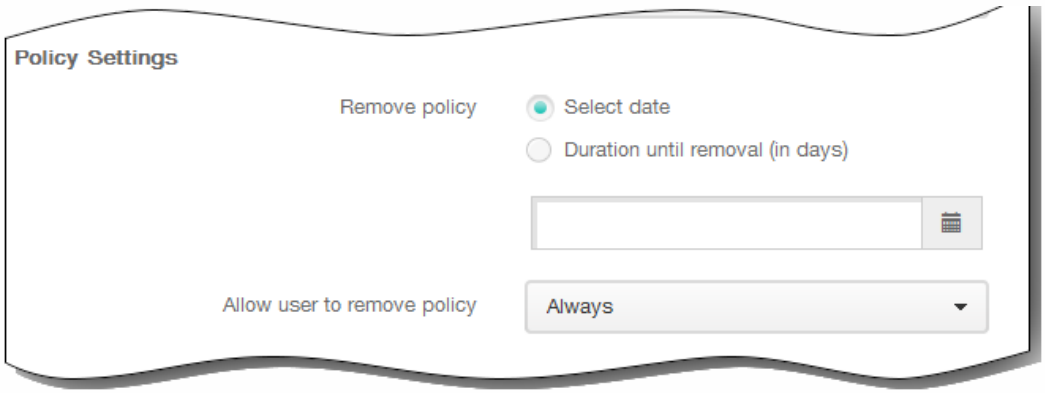
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform］情報ページが開きます。



6. ［iOS Platform］情報ページで、以下の情報を入力します。
   1. Account description：オプションで、アカウントの説明を入力します。
   2. Account user name：オプションで、ユーザー名を入力します。
   3. Account password：オプションで、パスワードを入力します。 これは、暗号化されたプロファイルに対してのみ使用します。
   4. LDAP host name：LDAPサーバーのホスト名を入力します。 このフィールドは必須です。

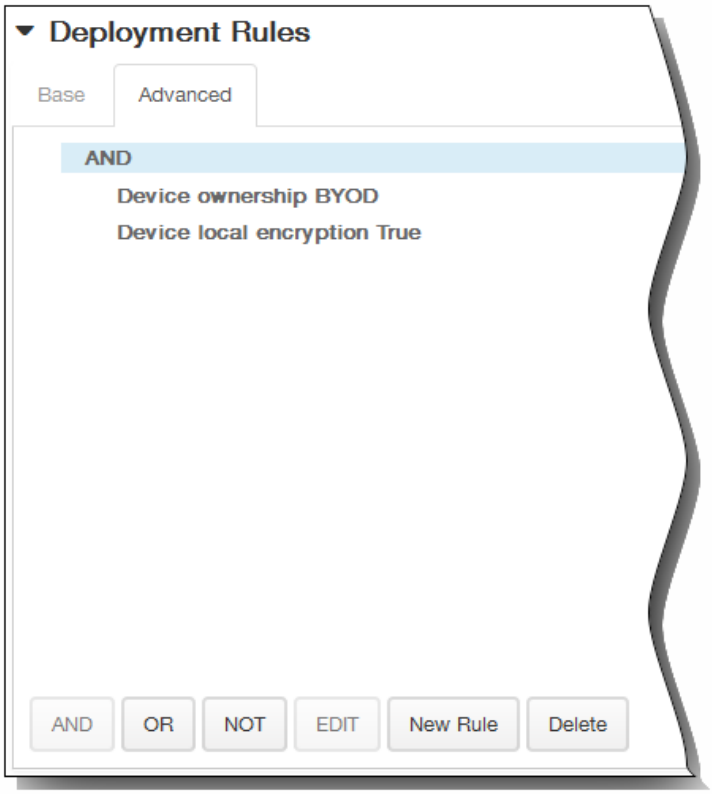
5. Use SSL：LDAPサーバーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［ON］です。
6. ［Search Settings］：［Add］をクリックして、以下の操作を行います。
   注：必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも1つ入力してください。
   1. ［Description］：検索設定の説明を入力します。このフィールドは必須です。
   2. Scope：ボックスの一覧で［Base］、［One level］、［Subtree］のいずれかを選択して、LDAPツリーをどの深さまで検索するかを定義します。デフォルトは［Base］です。
      - ［Base］を選択すると、［Search base］で参照されているノードを検索します。
      - ［One level］を選択すると、［Base］を選択した場合の検索対象ノードとその1つ下のレベルを検索します。
      - ［Subtree］を選択すると、［Base］を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
   3. Search base：検索の開始位置とするノードへのパスを入力します。たとえば、ou=peopleまたは0=example corpと入力します。このフィールドは必須です。
   4. ［Add］をクリックして検索設定を追加するか、［Cancel］をクリックして検索設定の追加を取り消します。
   5. 追加するカスタムキーごとに手順i.～iv.を繰り返します。

   注：既存の検索設定を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには［Delete］をクリックし、項目をそのままにするには［Cancel］をクリックします。
   既存の検索設定を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。
7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

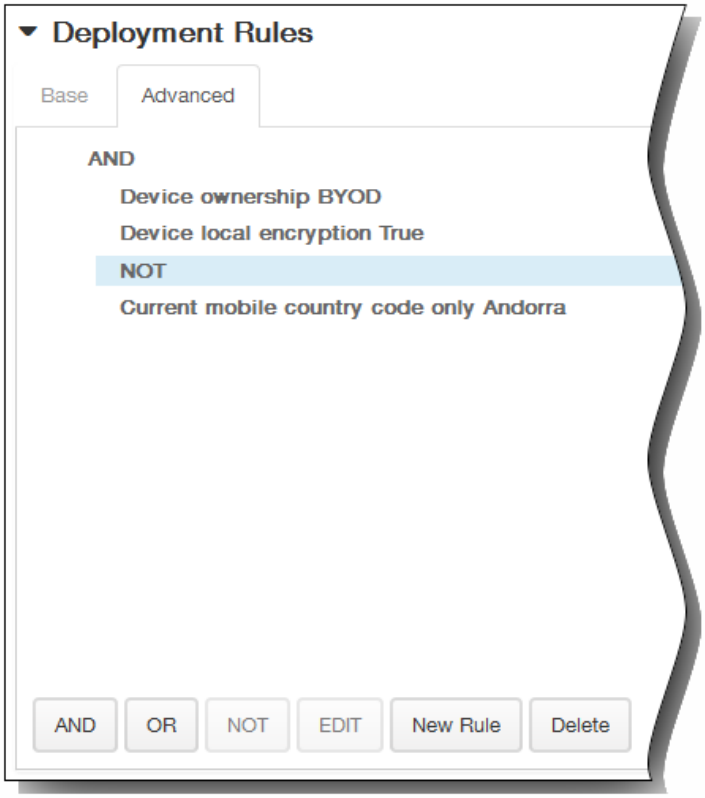


［Base］タブで選択した条件が表示されます。

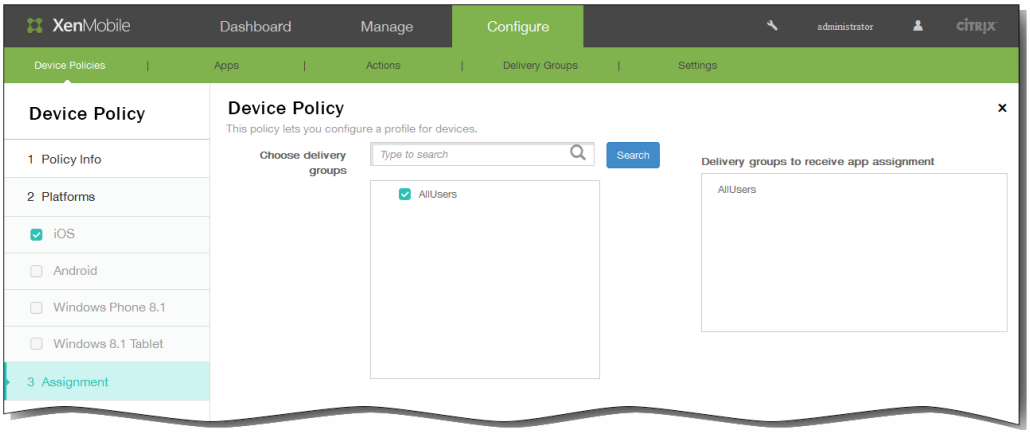
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［LDAP Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

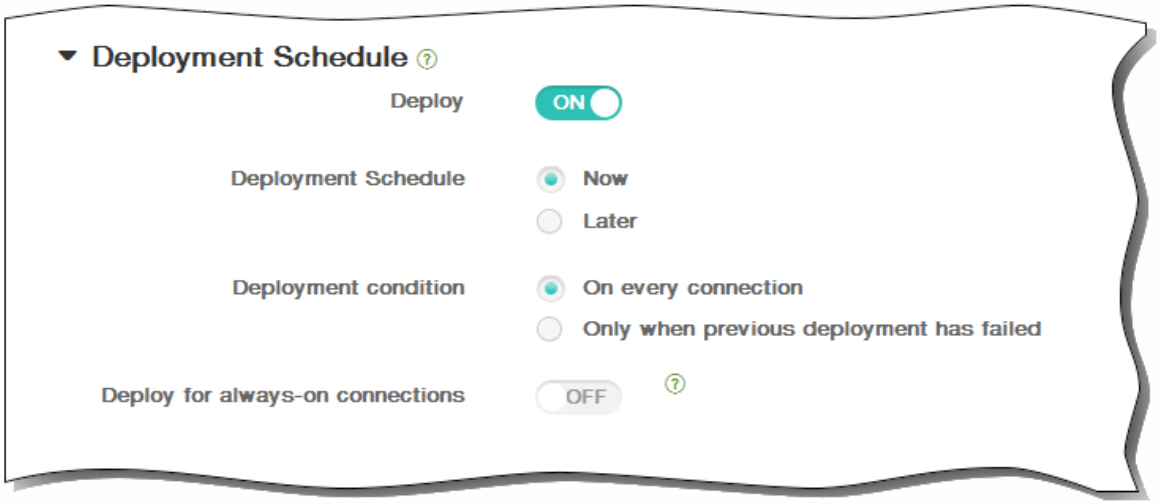


14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



15. ［Save］をクリックしてポリシーを保存します。

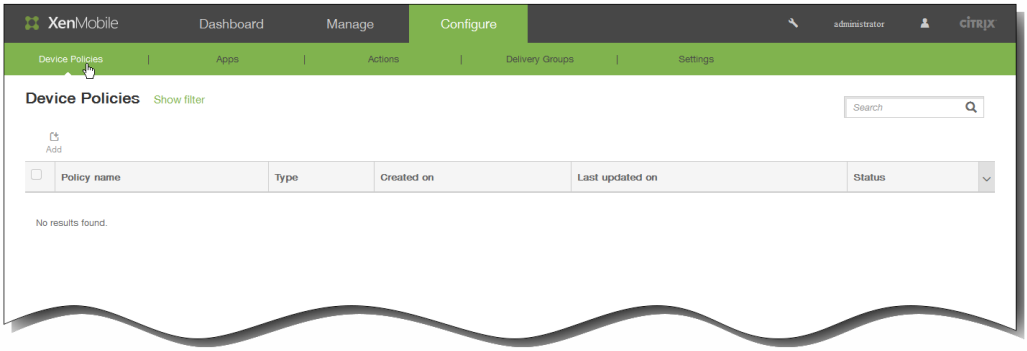
iOSのシングルサインオンアカウントデバイスポリシーを追加するには

May 10, 2016

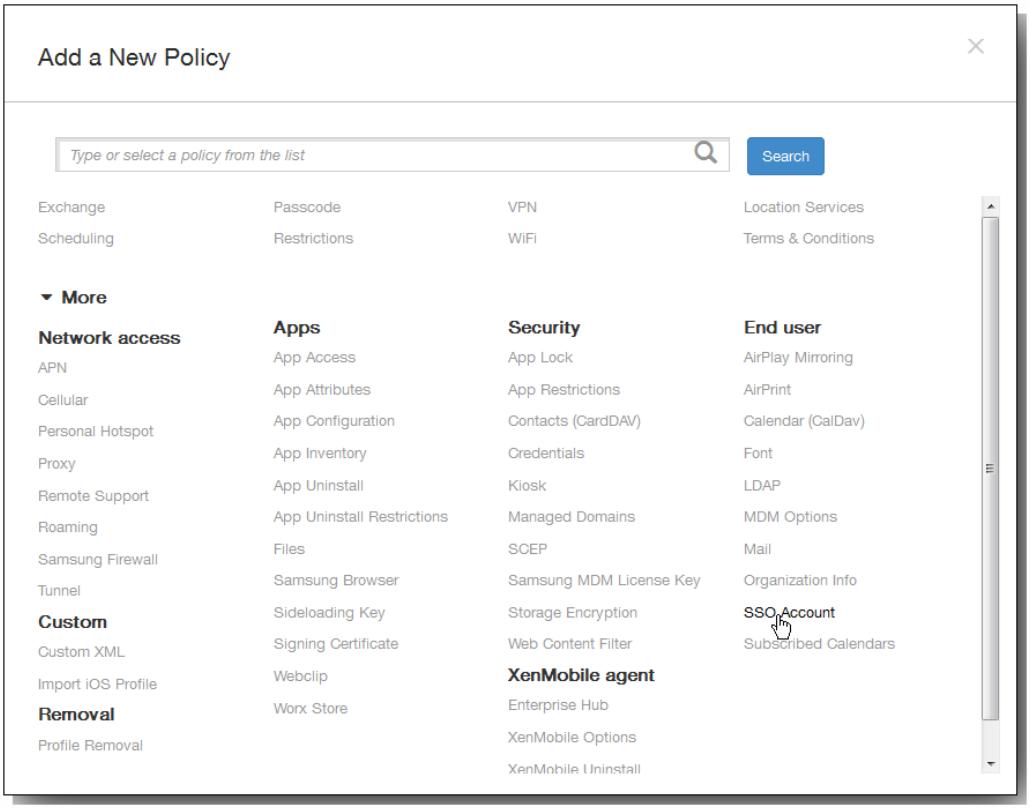
XenMobileでシングルサインオン（SSO）アカウントを作成して、ユーザーが1回サインオンするだけで、さまざまなアプリケーションからXenMobileおよび社内リソースにアクセスすることができるようにします。デバイスに資格情報を保存する必要はありません。SSOアカウントエンタープライズユーザーの資格情報は、App Storeからのアプリケーションを含む複数のアプリケーションで使用されます。このポリシーは、Kerberos認証バックエンドで動作するように設計されています。

注：このポリシーはiOS 7.0以降にのみ適用されます。

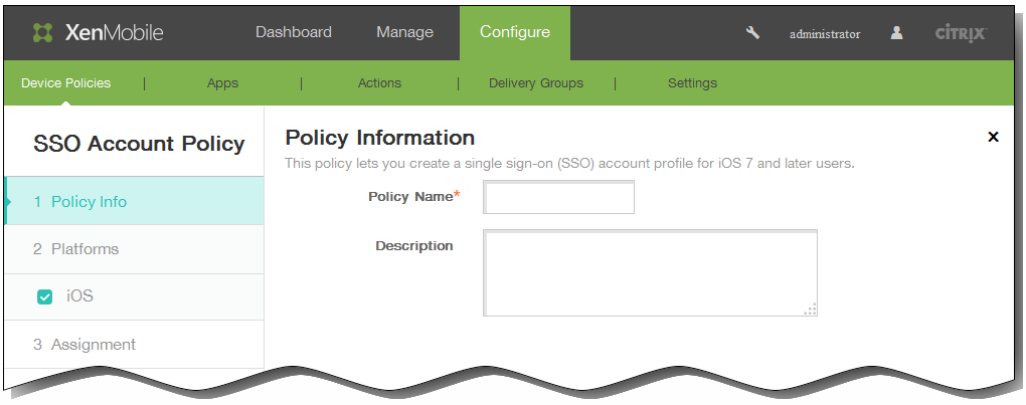
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



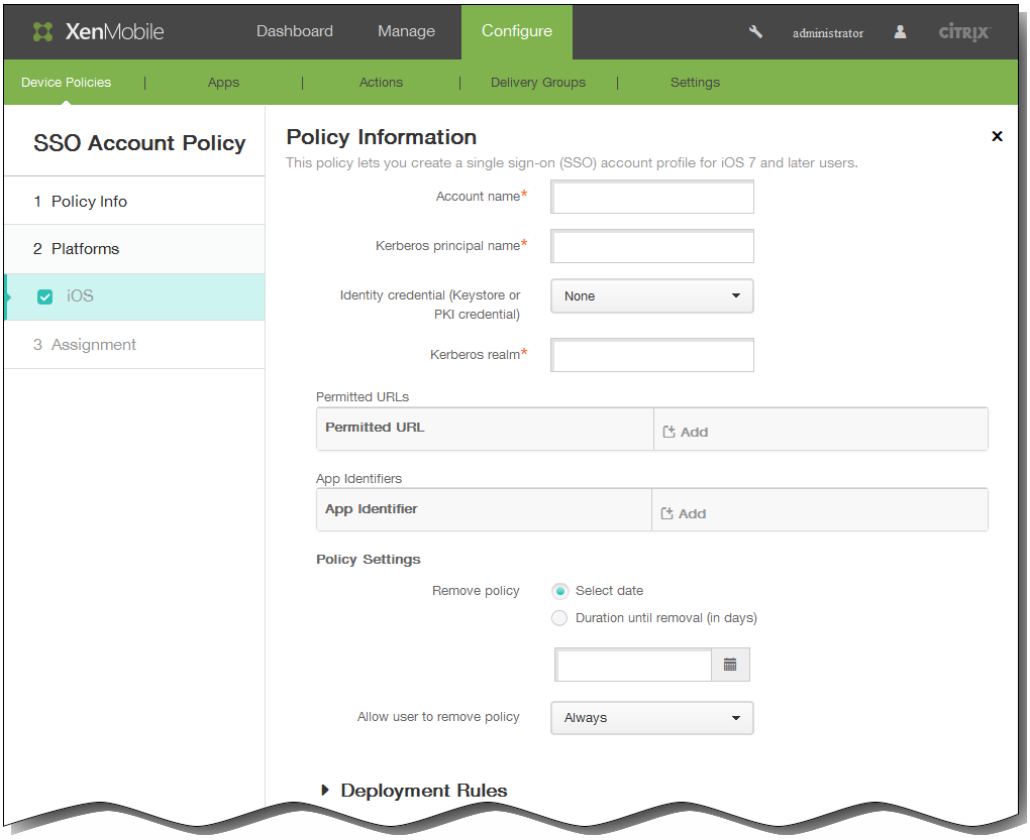
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［End user］の下の［SSO Account］をクリックします。 ［SSO Account Policy］ページが開きます。



4. ［SSO Account Policy］情報ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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. ［iOS Platform］情報ページで、以下の情報を入力します。
   1. Account name：ユーザーのデバイスで表示されるKerberos SSOアカウント名を入力します。 このフィールドは必須です。
   2. Kerberos principal name：Kerberosプリンシパル名を入力します。 このフィールドは必須です。
   3. Identity credential（Keystore or PKI credential）：一覧から、オプションとして、ID資格情報を選択します。これを使用して、Kerberos資格情報をユーザー操作なしで更新できます。
   4. Kerberos realm：このポリシーのKerberosレルムを入力します。 これは通常、ドメイン名をすべて大文字にしたものです（例：EXAMPLE.COM）。 このフィールドは必須です。
   5. Permitted URLs：［Add］をクリックして、以下の操作を行います。
      1. Permitted URL：ユーザーがiOSデバイスからアクセスしたときにSSOを要求するURLを入力します。
         たとえば、ユーザーがサイトを参照しようとし、WebサイトがKerberosチャレンジを開始した場合、そのサイトがURL一覧にないと、iOSデバイスは、前のKerberosログオンでデバイスにキャッシュされている可能性があるKerberoトークンの提供によるSSOを試行しません。URLのホスト部分が正確に一致する必要があります。たとえば、http://shopping.apple.comは有効ですが、http://*.apple.comは有効ではありません。また、Kerberosがホストの一致に基づいてアクティブ化されない場合でも、URLは標準のHTTP呼び出しにフォールバックします。これは、URLにKerberosを使用するSSOだけが構成されている場合であっても、標準パスワードチャレンジやHTTPエラーなどを含むほとんどすべてのことを意味する可能性があります。

      2. ［Add］をクリックしてURLを追加するか、［Cancel］をクリックしてURLの追加を取り消します。
      3. 追加するアプリケーションIDごとに手順iおよびii繰り返します。
   6. App Identifiers：［Add］をクリックして、以下の操作を行います。
      1. App Identifier：このログインを使用できるアプリケーションのアプリケーションIDを入力します。
         注：アプリケーションIDを追加しなかった場合、このログインは**すべて**のアプリケーションIDに一致します。
      2. ［Add］をクリックしてアプリケーションIDを追加するか、［Cancel］をクリックしてアプリケーションIDの追加を

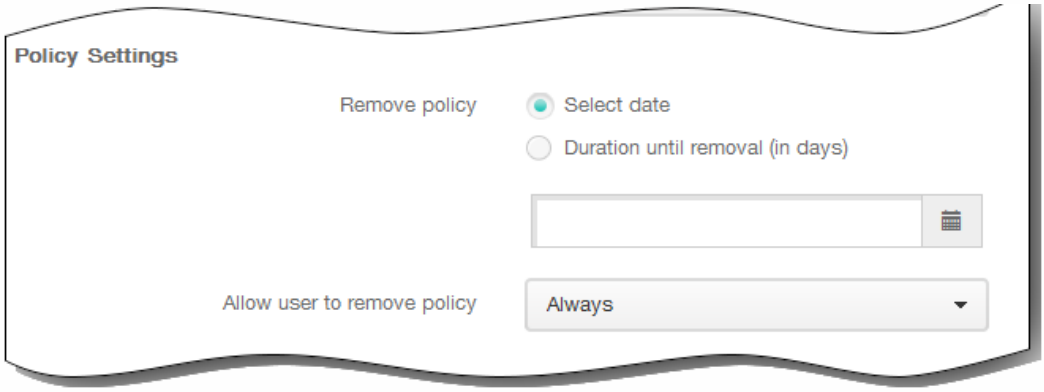
取り消します。

3. 追加するアプリケーションIDごとに手順i.およびii.繰り返します。

注：既存のURLまたはアプリケーションID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。

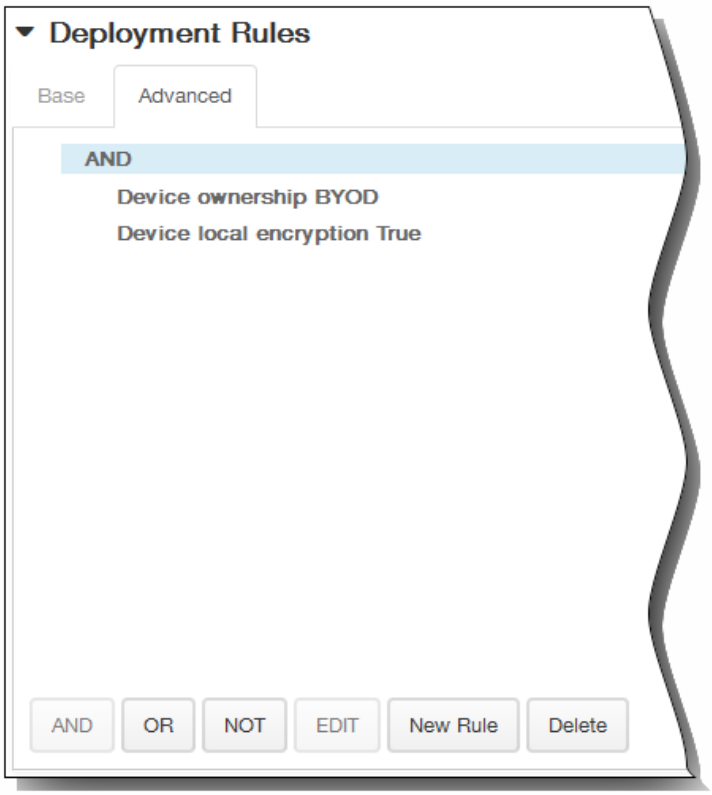
既存のURLまたはアプリケーションIDを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、［Save］をクリックして変更した項目を保存するか、［Cancel］をクリックして項目を変更せずそのままにします。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



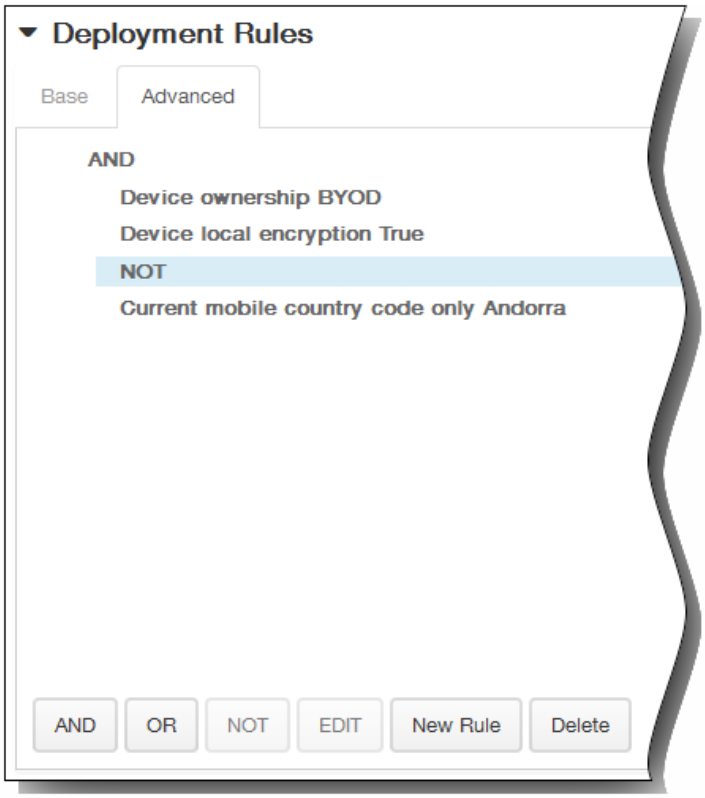
11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
    1. 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［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

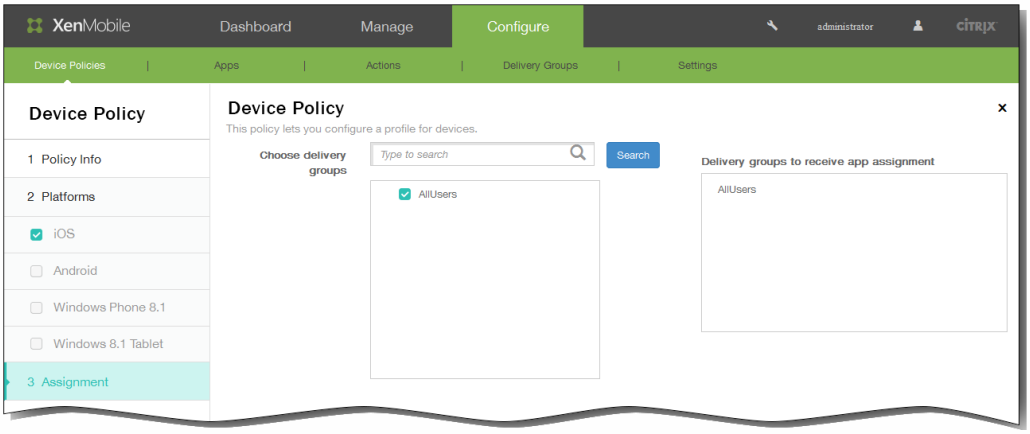


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［SSO Account Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



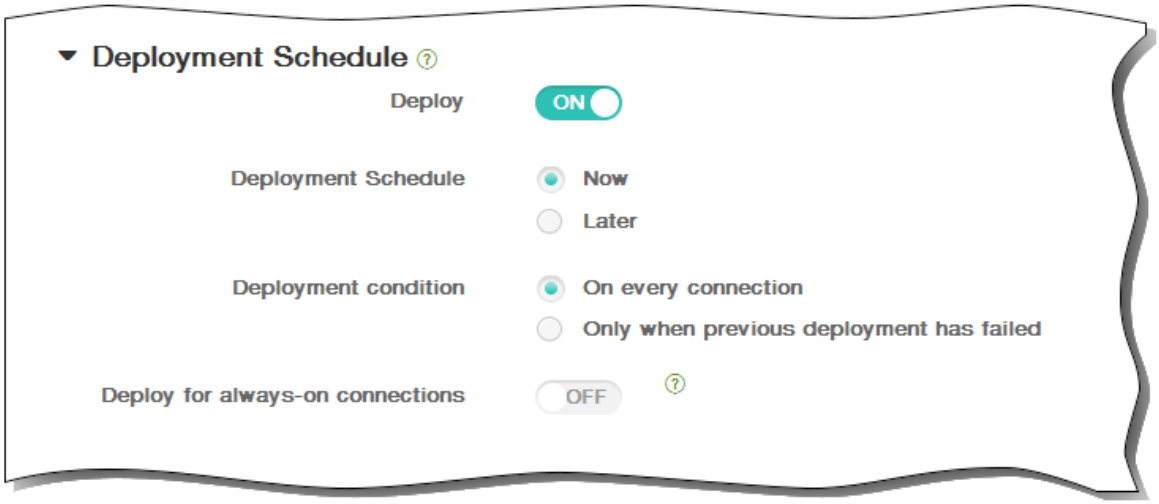
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



15. ［Save］をクリックしてポリシーを保存します。

iOSのサブスクライブされたカレンダーデバイスポリシーを追加するには

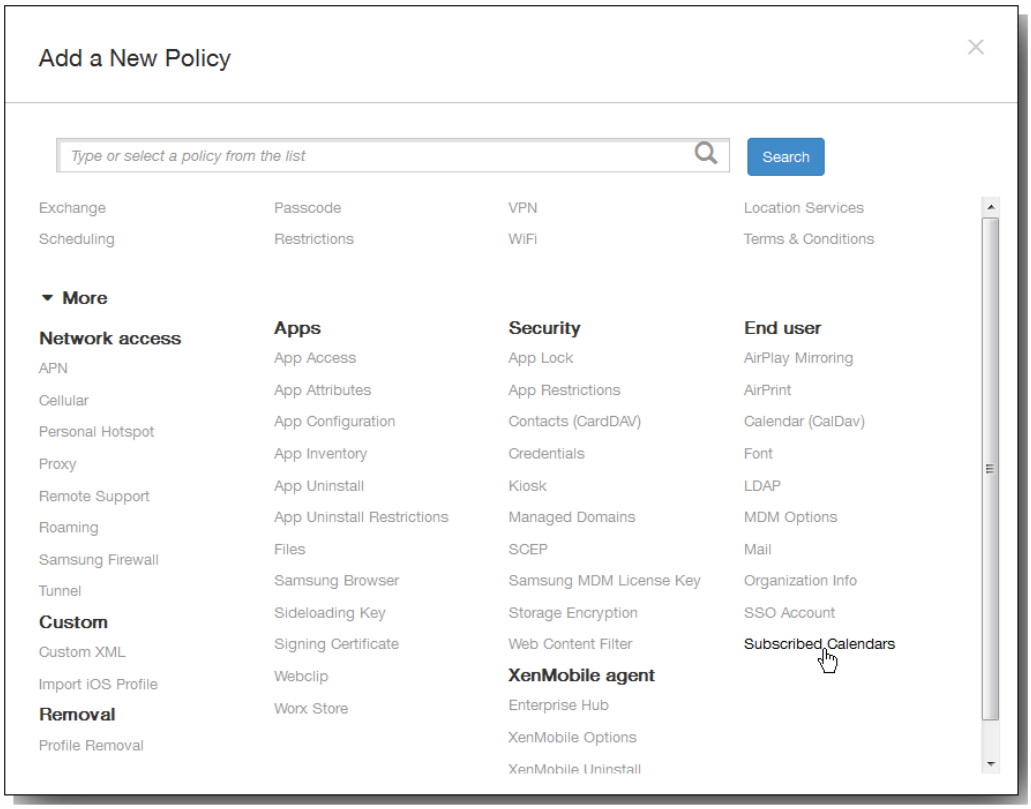
May 10, 2016

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。

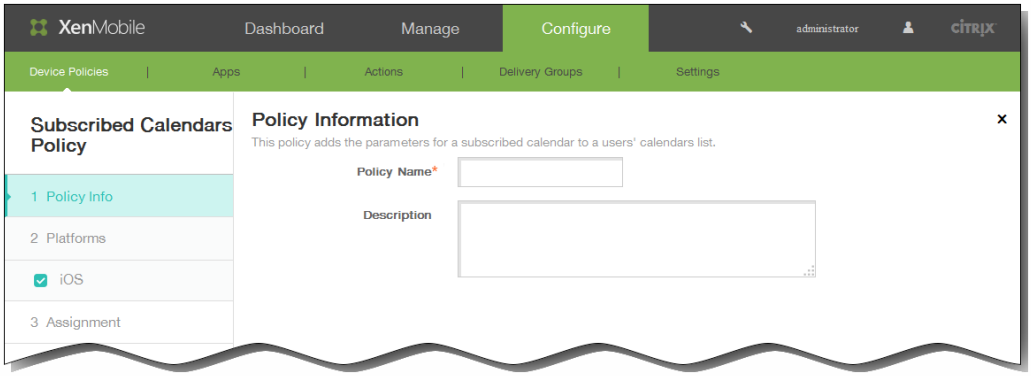
注：ユーザーのデバイスのサブスクライブされたカレンダー一覧にカレンダーを追加するには、そのカレンダーをサブスクライブ済みである必要があります。

1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。

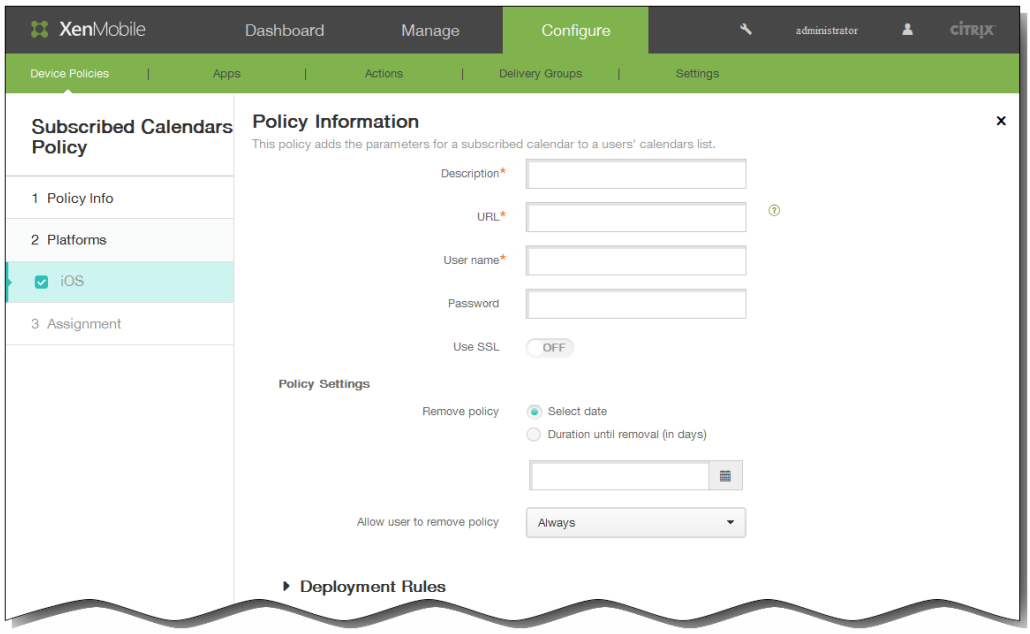
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［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。

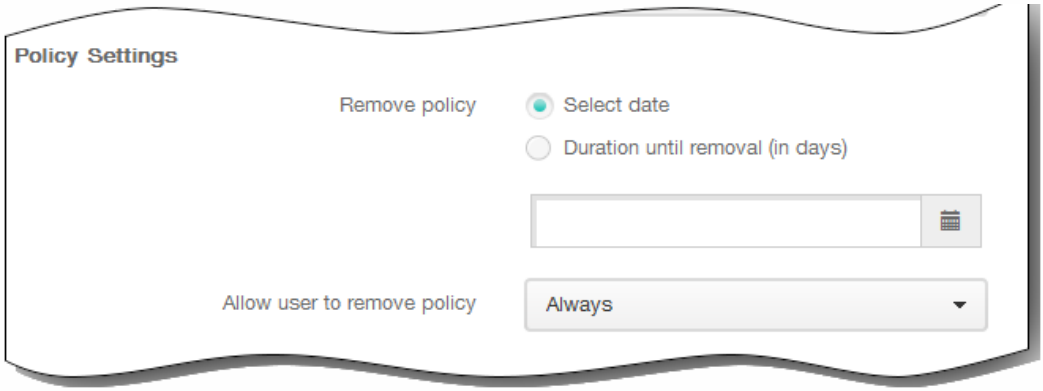


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［iOS Platform Information］ページが開きます。



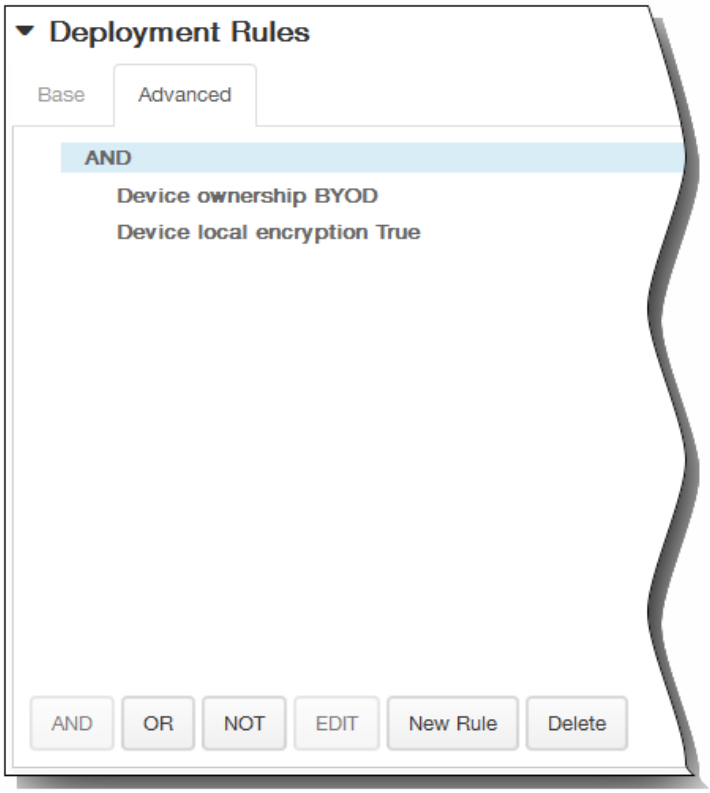
6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. Description：カレンダーの説明を入力します。 このフィールドは必須です。
   2. URL：カレンダーのURLを入力します。 iCalendarファイル（.ics）へのwebcal://URLまたはhttp://リンクを入力できます。 このフィールドは必須です。
   3. User name：ユーザーのログオン名を入力します。 このフィールドは必須です。
   4. Password：任意で、ユーザーのパスワードを入力します。
   5. Use SSL：カレンダーに対してSSL（Secure Socket Layer）接続を使用するかどうかを選択します。 デフォルトは［Off］です。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

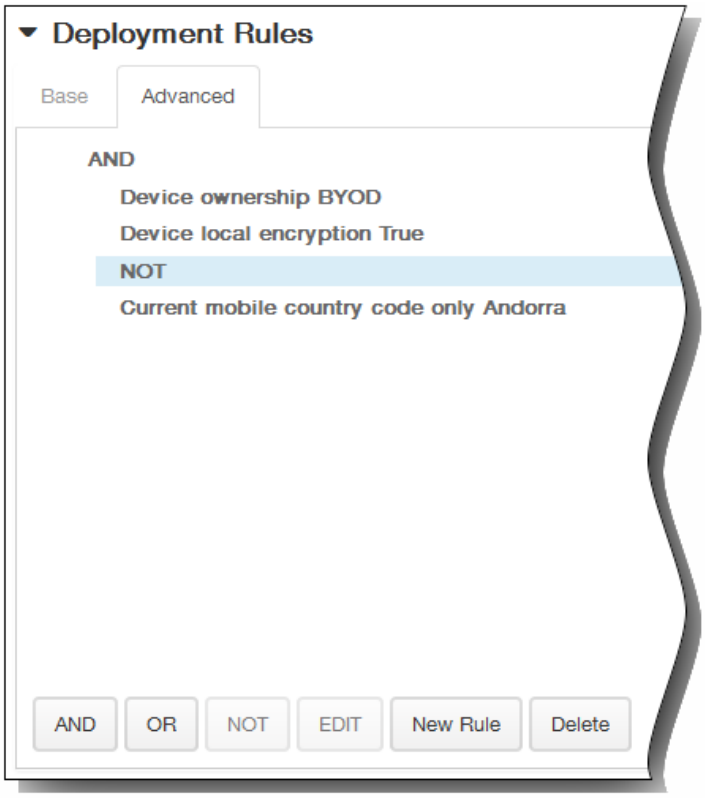
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



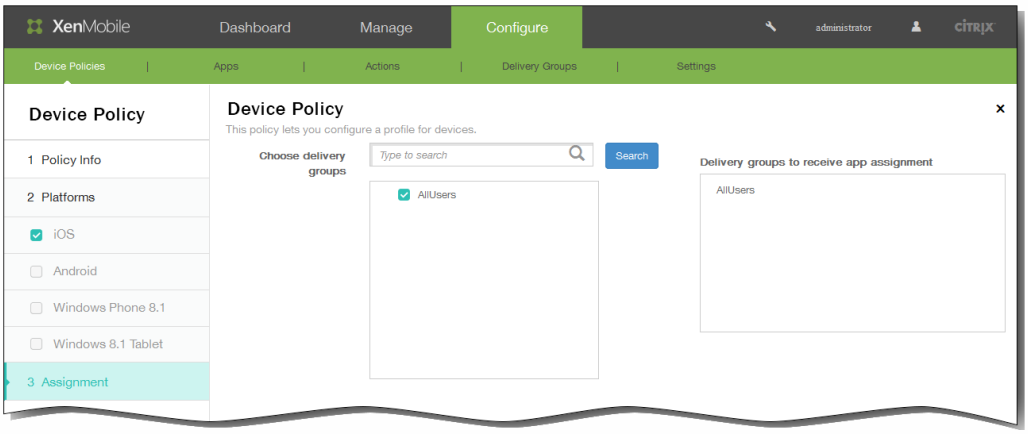
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［Subscribed Calendars Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



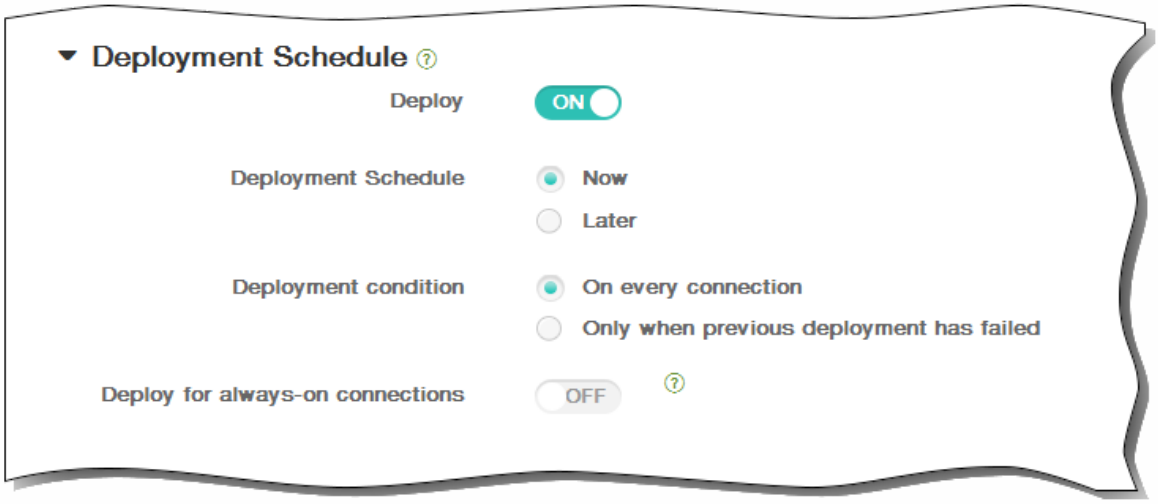
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



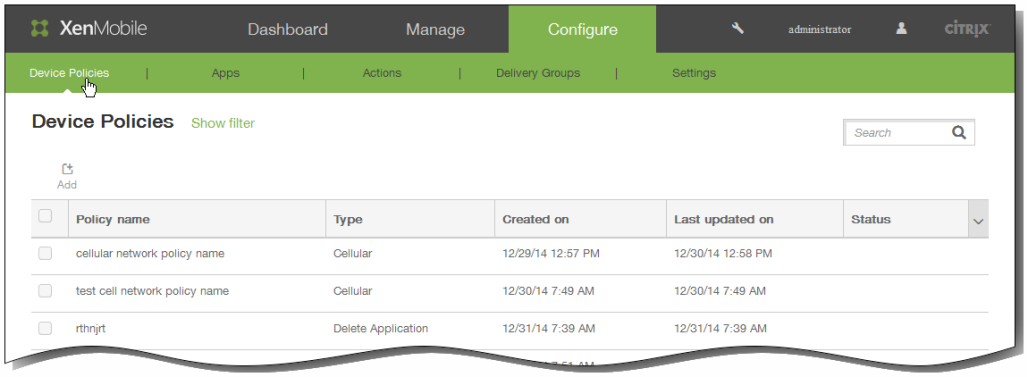
15. ［Save］をクリックしてポリシーを保存します。

パスコードデバイスポリシー

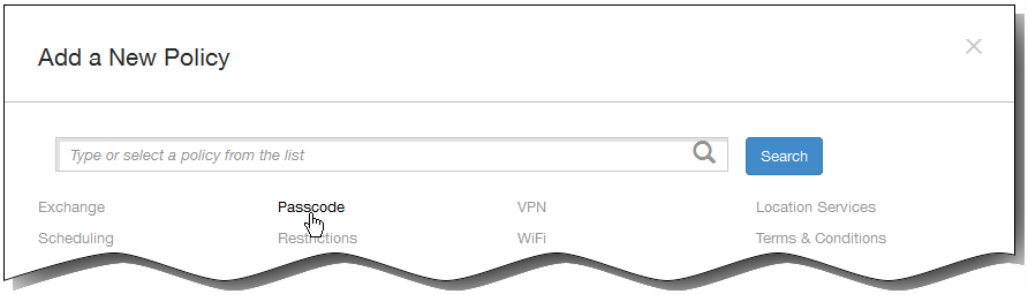
May 10, 2016

組織の基準に基づいて、XenMobileでパスコードポリシーを作成します。ユーザーのデバイスでパスコードを要求し、さまざまな形式およびパスコード規則を設定することができます。iOS、Android、Samsung KNOX、Windows Phone 8.1、Windows 8.1タブレットに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

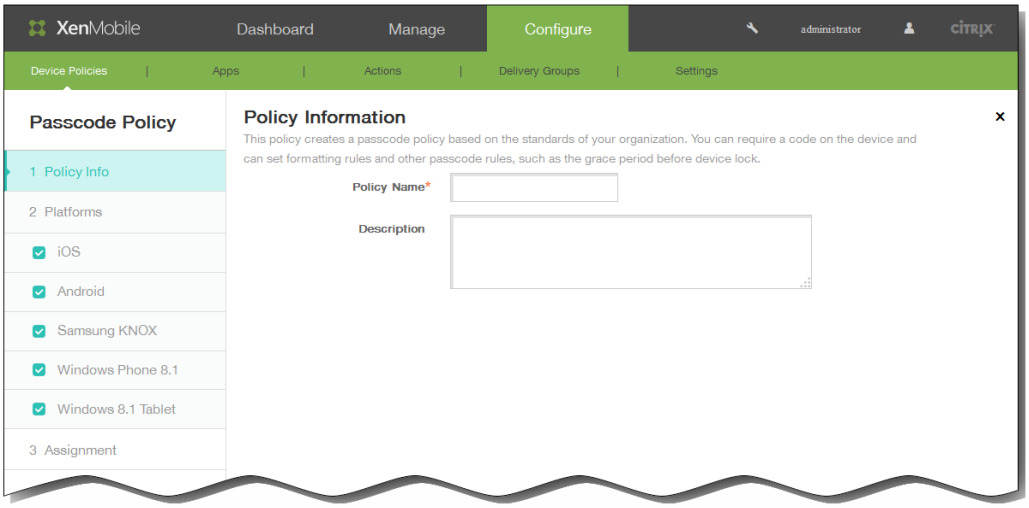
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。新しいポリシーを追加するには［Add］をクリックします。



2. ［Add New Policy］ページで、［Passcode］をクリックします。

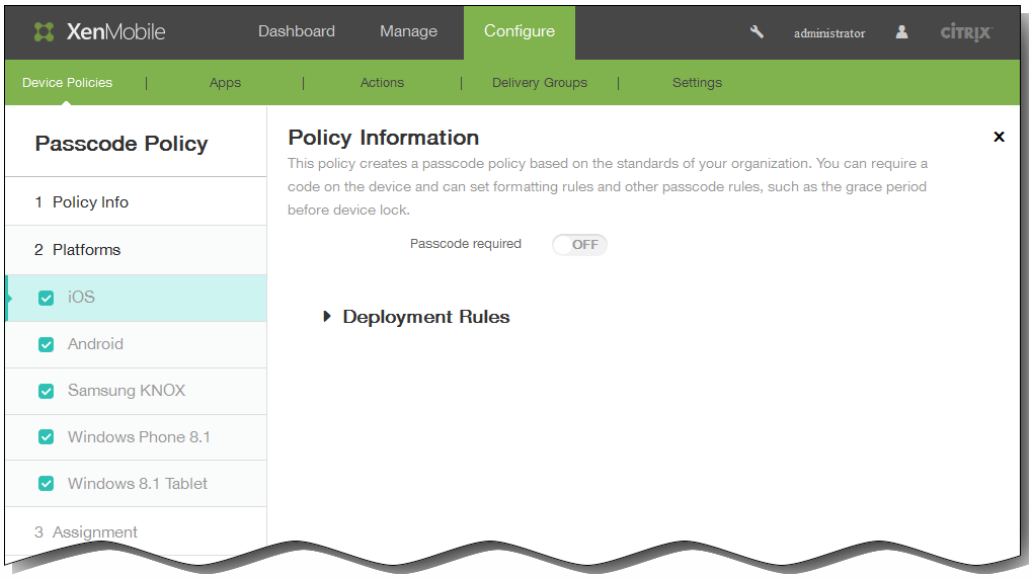


3. ［Policy Information］ペインで、以下の情報を入力します。

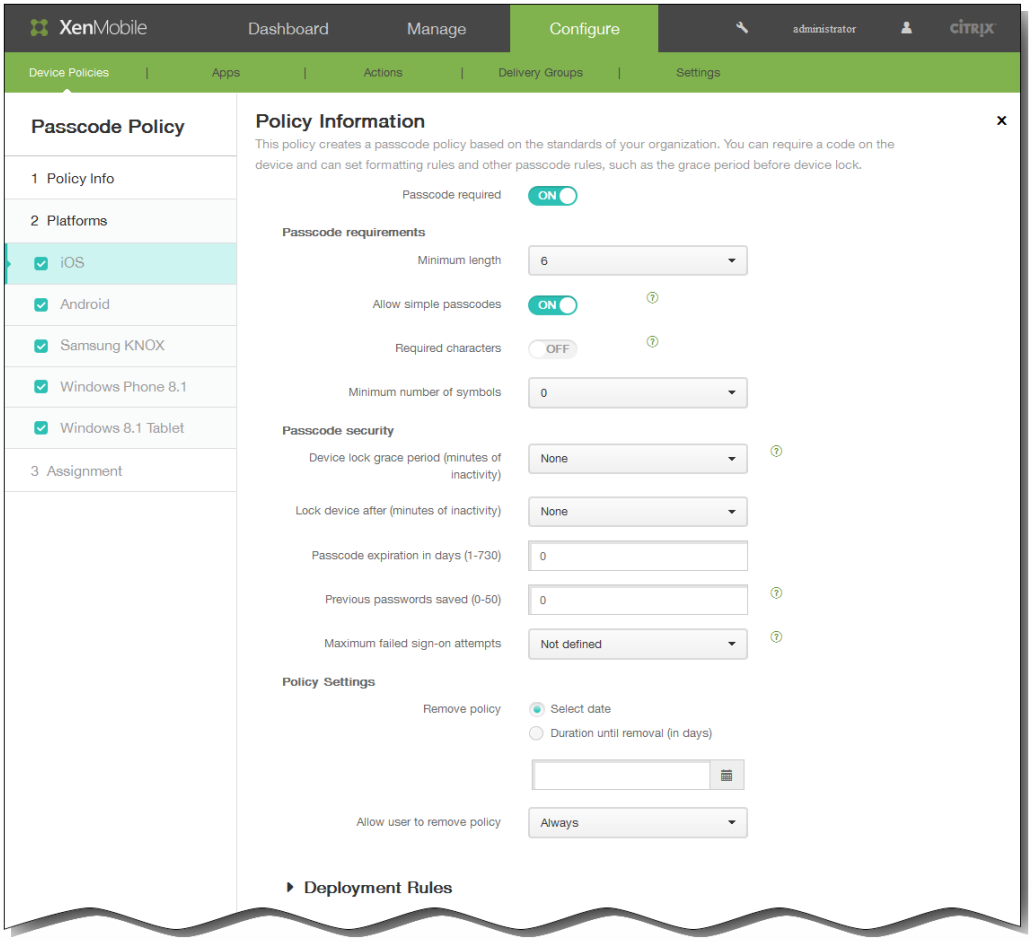


1. Policy Name：ポリシーの説明的な名前を入力します。
2. Description：任意で、ポリシーの説明を入力します。
3. ［次へ］をクリックします。
4. ［Platforms］の下で、このポリシーを構成するプラットフォームをオンにします。

注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォーム構成パネルが開きます。



- ［iOS］を選択した場合は、次の設定を構成します。



Passcode required：このオプションをオンにするとパスコードが必須になり、iOSのパスコードデバイスポリシーの構成オプションが表示されます。 ページが展開され、パスコード要件、パスコードセキュリティ、ポリシー設定を構成できます。

パスコード要件

Minimum length：一覧から、パスコードの最小文字数を選択します。 デフォルトは6です。

Allow simple passcodes：簡単なパスコードを許可するかどうかを選択します。 簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。 デフォルトは［ON］です。

Required characters：パスコードに文字を1つ以上含める必要があるかどうかを選択します。 デフォルトは[OFF］です。

Minimum number of symbols：一覧から、パスコードに含める必要がある記号の数を選択します。

パスコードセキュリティ

Device lock grace period（minutes of inactivity）：一覧から、ユーザーがパスコードを入力してデバイスのロックを解除することが必要になるまでの時間を選択します。 デフォルトは［None］です。

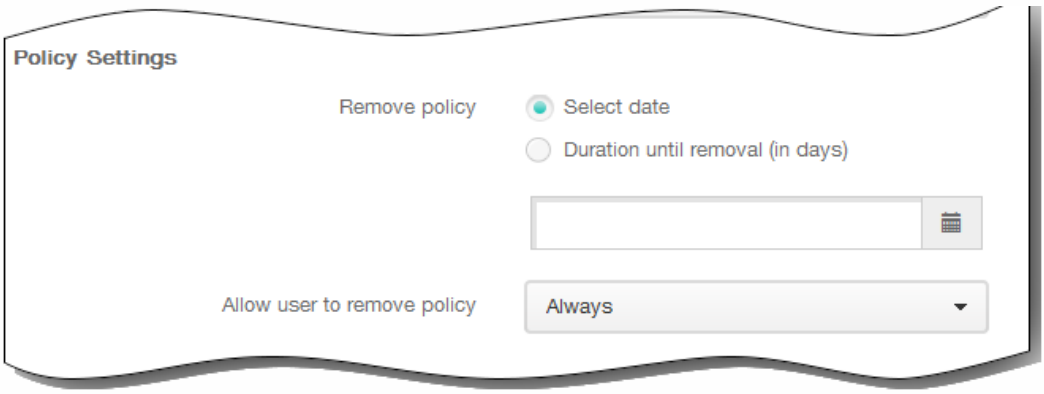
Lock device after（minutes of inactivity）：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。 デフォルトは［None］です。

Passcode expiration in days（1-730）：パスコードを有効期限切れにするまでの日数を入力します。 有効な値は1～730です。 デフォルトは0で、パスコードの有効期限がないことを意味します。

Previous passwords saved（0-50）：保存する使用済みパスワードの数を入力します。 ユーザーはこの一覧にあるパスワードを使用できません。 有効な値は0～50です。 デフォルトは0で、ユーザーがパスワードを再使用できることを意味します。

サインオン失敗回数の上限：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。 デフォルトは［Not defined］です。

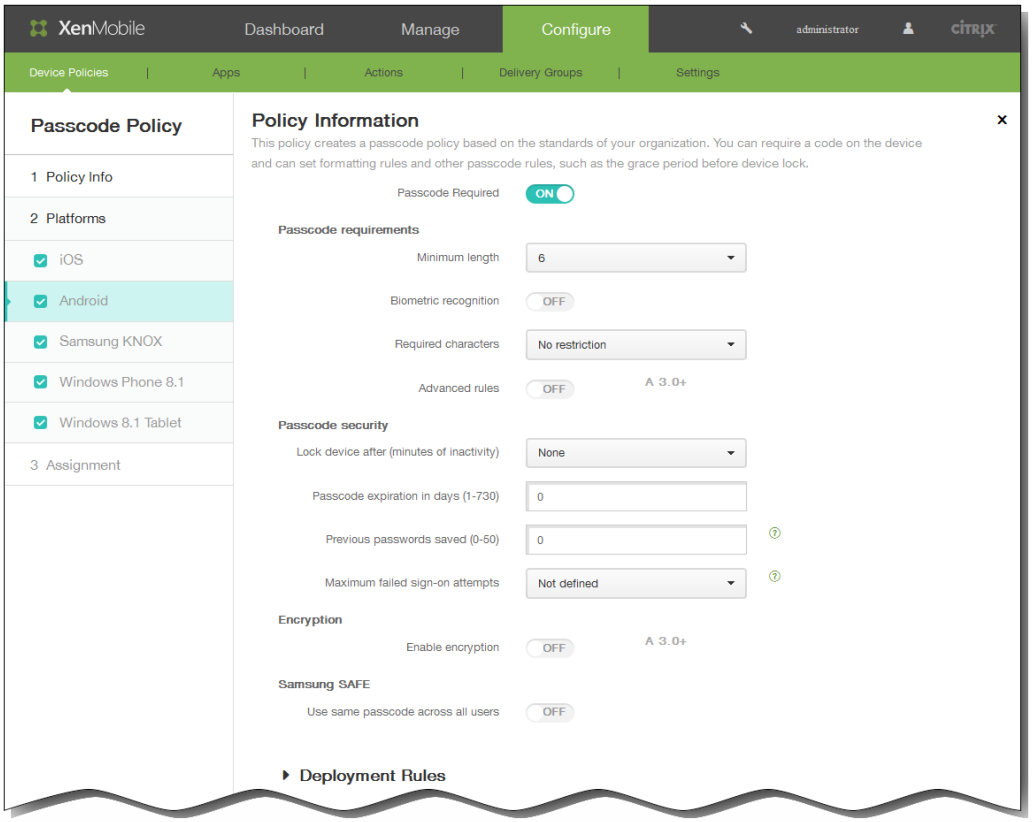
ポリシー設定



1. ［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。
2. ［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。
3. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
4. ［Password required］を選択した場合、［Removal password］の横に必要なパスワードを入力します。

- ［Android］を選択した場合は、次の設定を構成します。

  注：Androidのデフォルト設定は［OFF］です。 ページが展開され、パスコード要件、パスコードセキュリティ、暗号化、Samsung SAFEの設定を構成できます。



パスコード要件

Minimum length：一覧から、パスコードの最小文字数を選択します。 デフォルトは6です。

Biometric recognition：生体認証を有効にするかどうかを選択します。 このオプションを有効にした場合、[Required characters] フィールドは非表示になります。 デフォルトは [OFF] です。

Required characters：一覧から [No Restriction] 、 [Both numbers and letters] 、 [Numbers only] 、 [Letters only] のいずれかを選択して、パスワードの作成方法を構成します。 デフォルトは[No restriction] です。

Advanced rules：詳細なパスコード規則を適用するかどうかを選択します。 このオプションはAndroid 3.0以降で使用できます。 デフォルトは [OFF] です。

[Advanced rules] を [ON] に設定した場合、以下のボックスの一覧のそれぞれで、パスコードに含める必要がある文字、記号、または数字の数を、種類ごとに選択します。

- Symbols：記号の最小使用数
- Letters：文字の最小使用数
- Lowercase letters：小文字の最小使用数
- Uppercase letters：大文字の最小使用数
- Numbers or symbols：数字または記号の最小使用数
- Numbers：数字の最小使用数

パスコードセキュリティ

Lock device after（minutes of inactivity）：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。 デフォルトは [None] です。

Passcode expiration in days（1-730）：パスコードを有効期限切れにするまでの日数を入力します。 有効な値は1～730です。 デフォルトは0で、パスコードの有効期限がないことを意味します。

Previous passwords saved（0-50）：保存する使用済みパスワードの数を入力します。 ユーザーはこの一覧にあるパスワードを使用できません。 有効な値は0～50です。 デフォルトは0で、ユーザーがパスワードを再使用できることを意味します。

サインオン失敗回数の上限：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。 デフォルトは［Not defined］です。

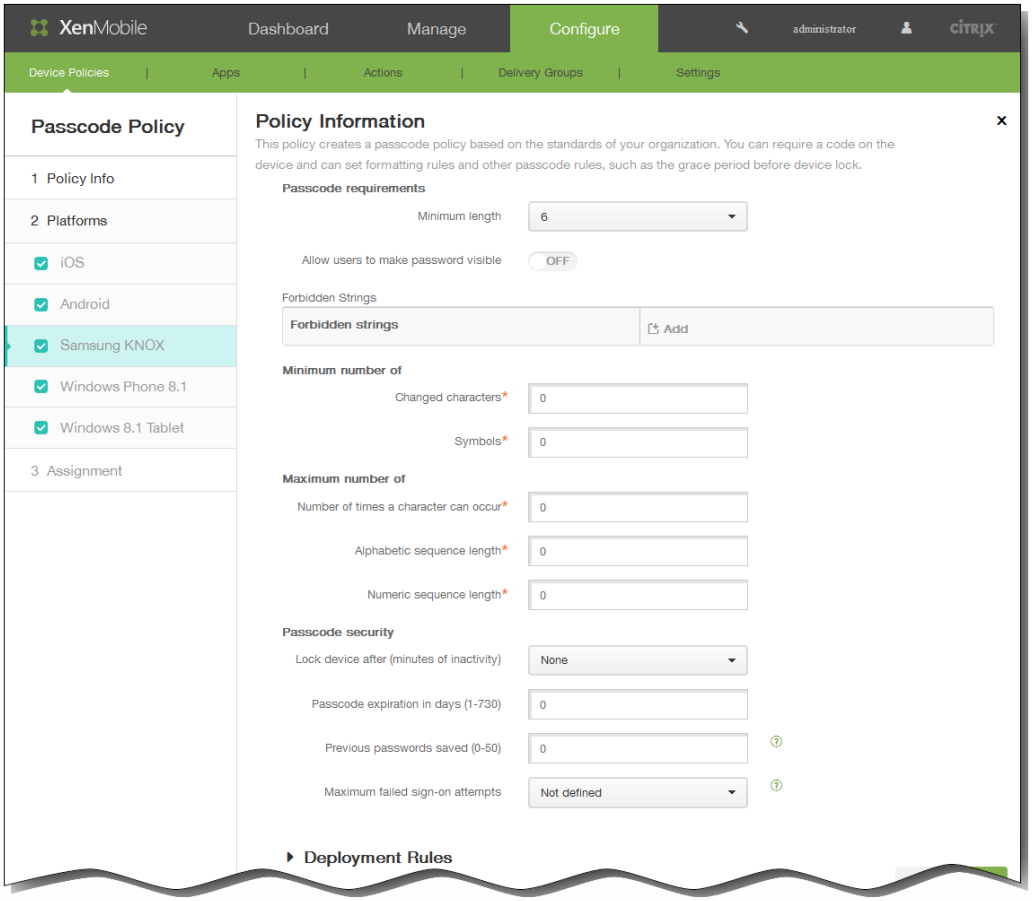
Encryption

Enable encryption：暗号化を有効にするかどうかを選択します。 このオプションはAndroid 3.0以降で使用できます。 このオプションは、［Passcode required］設定にかかわらず使用できます。

Use same passcode across all users：すべてのユーザーに対して同じパスコードを使用するかどうかを選択します。 このオプションはSamsung SAFEデバイスにのみ適用され、［Passcode required］設定にかかわらず使用できます。 デフォルトは［OFF］です。

このオプションを有効にした場合、表示されるフィールドに、必要なパスコードを入力します。

- ［Samsung KNOX］を選択した場合は、次の設定を構成します。



パスコード要件

Minimum length：一覧から、パスコードの最小文字数を選択します。

Allow users to make password visible：ユーザーがパスワードを表示できるようにするかどうかを選択します。

- Forbidden strings：禁止文字列を作成して、「password」、「pwd」、「welcome」、「123456」、「111111」などの類推しやすく安全ではない文字列をユーザーが使用できないようにします。 次のいずれかを行います。
  - **禁止文字列を追加するには**
    1. ［Add］をクリックします。
    2. 禁止文字列を入力します。
    3. ［Save］をクリックして文字列を保存するか、［Cancel］をクリックして文字列の追加を取り消します。
    4. 追加するカスタムキーごとに手順i. ～iii. を繰り返します。
  - **禁止文字列を編集するには**
    1. Previous passwords saved（0-50）：保存する使用済みパスワードの数を入力します。 ユーザーはこの一覧にあるパスワードを使用できません。 有効な値は0～50です。 デフォルトは0で、ユーザーがパスワードを再使用できることを意味します。
    1. 編集する文字列の上にマウスポインターを置きます。
    2. 項目の右側のペンアイコンをクリックします。
    3. 文字列を変更します。
    4. ［Save］をクリックして文字列を保存するか、［Cancel］をクリックして文字列の変更を取り消します。

最小数

Changed characters：ユーザーが前のパスコードから変更する必要がある文字数を入力します。 デフォルトは0です。

Symbols：パスコードに含める必要がある記号の最小数を入力します。 デフォルトは0です。

最大数

Number of times a character can occur：パスコード内に1つの文字を繰り返し使用できる最大回数を入力します。 デフォルトは0です。

Alphabetic sequence length：パスコードに含まれる、連続するアルファベットの最大文字数を入力します。 デフォルトは0です。

Numeric sequence length：パスコードに含まれる、連続する数字の最大文字数を入力します。 デフォルトは0です。

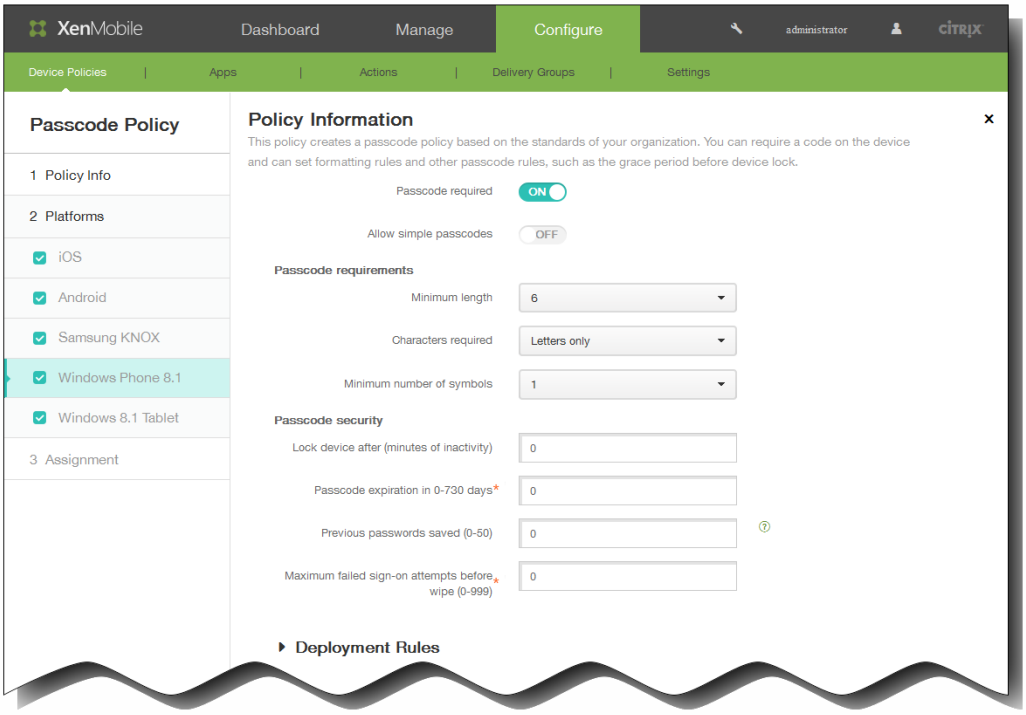
パスコードセキュリティ

Lock device after（minutes of inactivity）：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。 デフォルトは［None］です。
注：このフィールドのラベルは「minutes of inactivity」（非アクティブの分数）となっていますが、実際には指定した*秒*数が経過した後にロックが適用されます。
Passcode expiration in days（1-730）：パスコードを有効期限切れにするまでの日数を入力します。 有効な値は1～730です。 デフォルトは0で、パスコードの有効期限がないことを意味します。

Previous passwords saved（0-50）：保存する使用済みパスワードの数を入力します。 ユーザーはこの一覧にあるパスワードを使用できません。 有効な値は0～50です。 デフォルトは0で、ユーザーがパスワードを再使用できることを意味します。

Maximum failed sign-on attempts：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはロックされます。 デフォルトは［Not defined］です。

- ［Windows Phone 8.1］を選択した場合は、次の設定を構成します。



Passcode required：Windows Phone 8.1デバイスでパスコードを要求しない場合、このオプションを選択します。 デフォルト設定は［ON］で、パスコードを要求します。 ページが折りたたまれ、以下のオプションは表示されなくなります。 パスコード要件をオフにしない場合、以下の設定の構成を続けます。

Allow simple passcodes：簡単なパスコードを許可するかどうかを選択します。 簡単なパスコードとは、文字の繰り返しや連続する文字を使用したパスコードのことです。 デフォルトは［OFF］です。

パスコード要件

Minimum length：一覧から、パスコードの最小文字数を選択します。 デフォルトは6です。

Characters required：一覧から［Numeric or alphanumeric］、［Letters only］、［Numbers only］のいずれかを選択して、パスワードの作成方法を構成します。 デフォルトは［Letters only］です。

Minimum number of symbols：一覧から、パスコードに含める必要がある記号の数を選択します。 デフォルトは1です。

パスコードセキュリティ

Lock device after（minutes of inactivity）：一覧から、デバイスを非アクティブにしておくことができる時間を選択します。この時間が過ぎると、デバイスはロックされます。 デフォルトは0です。

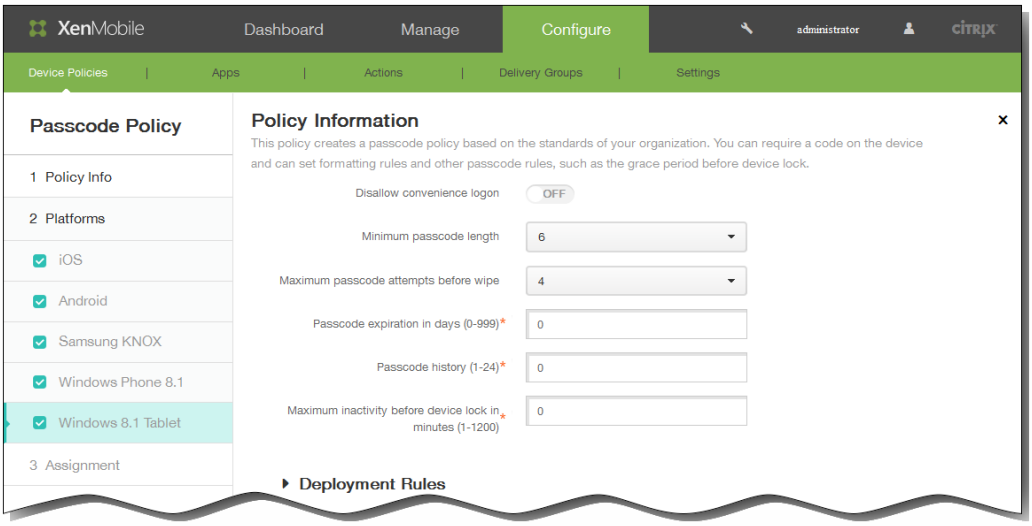
Passcode expiration in 0-730 days：パスコードを有効期限切れにするまでの日数を入力します。 有効な値は1～730です。 デフォルトは0で、パスコードの有効期限がないことを意味します。

Previous passwords saved（0-50）：保存する使用済みパスワードの数を入力します。 ユーザーはこの一覧にあるパスワードを使用できません。 有効な値は0～50です。 デフォルトは0で、ユーザーがパスワードを再使用できることを意

味します。

Maximum failed sign-on attempts before wipe（0-999）：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、企業データがデバイスからワイプされます。 デフォルトは0です。

- ［Windows 8.1 Tablet］を選択した場合は、次の設定を構成します。



Disallow convenience logon：ユーザーがピクチャーパスワードまたは生体認証ログオンを使用してデバイスにアクセスできるようにするかどうかを選択します。 デフォルトは［OFF］です。

Miniumum passcode length：一覧から、パスコードの最小文字数を選択します。 デフォルトは6です。

Maximum passcode attempts before wipe：一覧から、ユーザーが正常なサインインの前に失敗できる回数を選択します。この回数を超えると、デバイスはワイプされます。 デフォルトは4です。

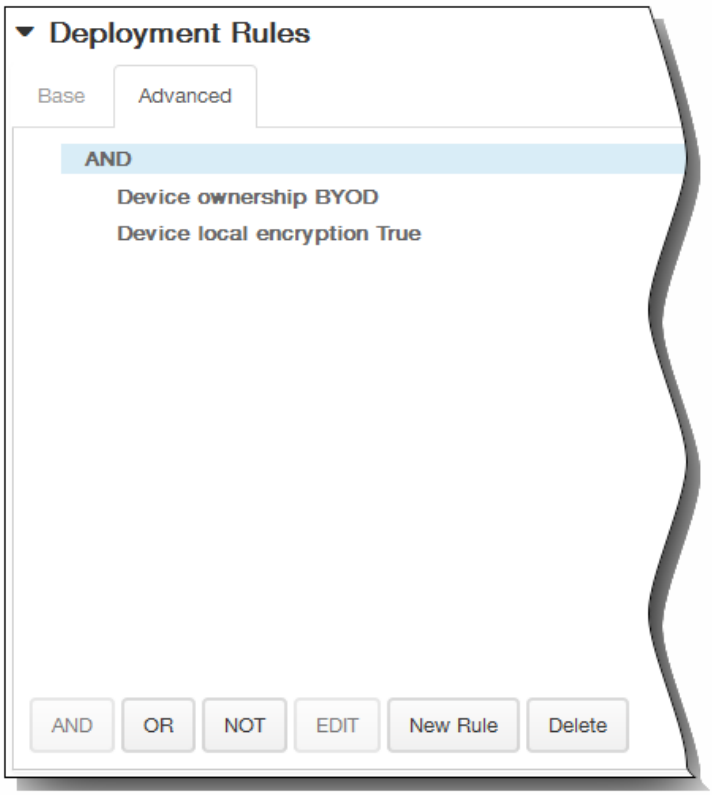
Passcode expiration in days（0-999）：パスコードを有効期限切れにするまでの日数を入力します。 有効な値は1～999です。 デフォルトは0で、パスコードの有効期限がないことを意味します。

Passcode history:（1-24）：保存する使用済みパスコードの数を入力します。 ユーザーはこの一覧にあるパスコードを使用できません。 有効な値は1～24です。 このフィールドには1～24の数値を入力する必要があります。

Maximum inactivity before device lock in minutes（1-1200）：デバイスを非アクティブにしておくことができる時間（分）を入力します。この時間が過ぎると、デバイスはロックされます。 有効な値は1～1200です。 このフィールドには1～1200の数値を入力する必要があります。

5. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。 必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

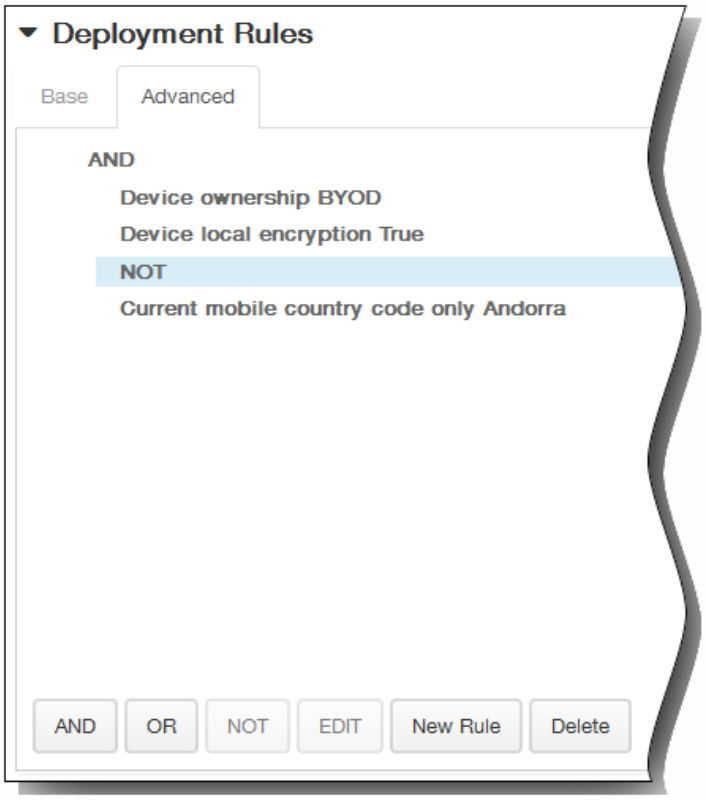


［Base］タブで選択した条件が表示されます。

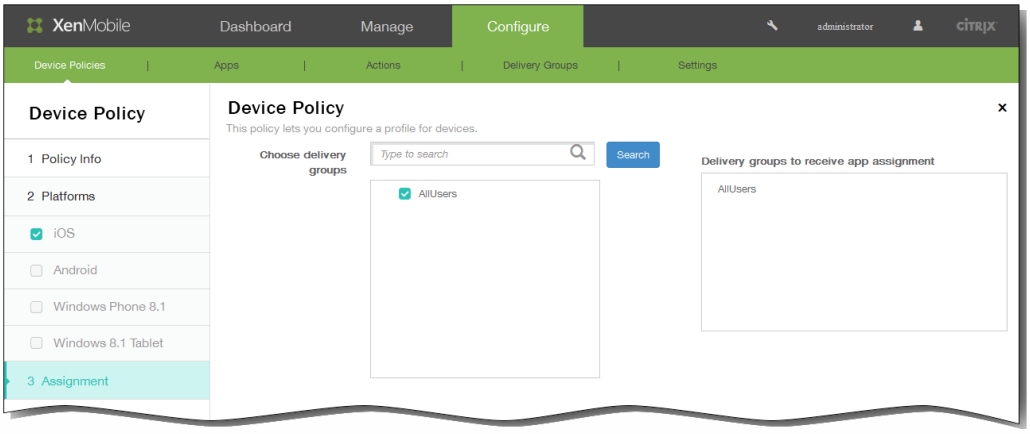
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追

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

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。

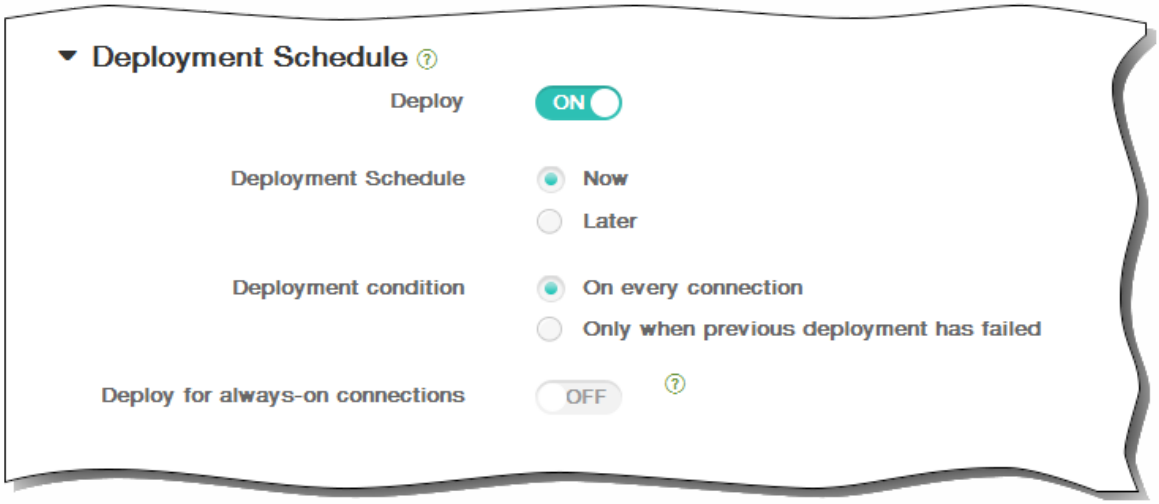


6. ［次へ］をクリックします。［Passcode Policy］割り当てページが開きます。
7. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



8. ［Deployment Schedule］を展開して以下の設定を構成します。
   1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
   2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
   3. ［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。
   4. ［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。
   5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
      注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。 常時接続オプションは、iOSデバイスでは使用できません。

   注：構成した展開スケジュールはすべてのプラットフォームについて同一です。 すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



9. ［Save］をクリックします。

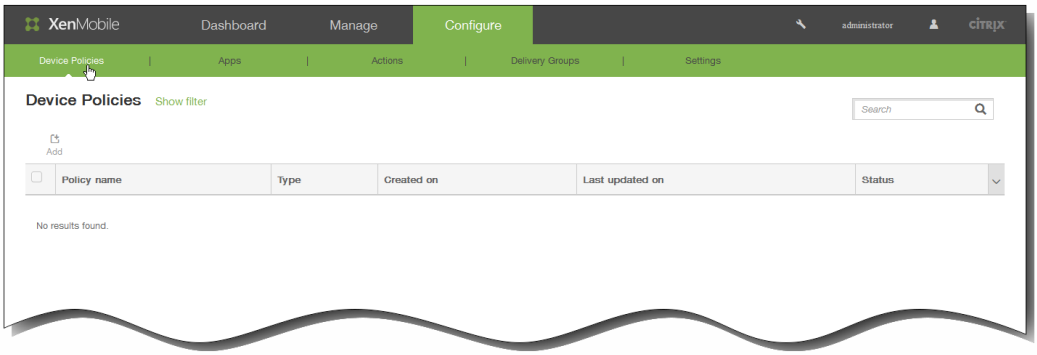
iOSのプロキシデバイスポリシーを追加するには

May 10, 2016

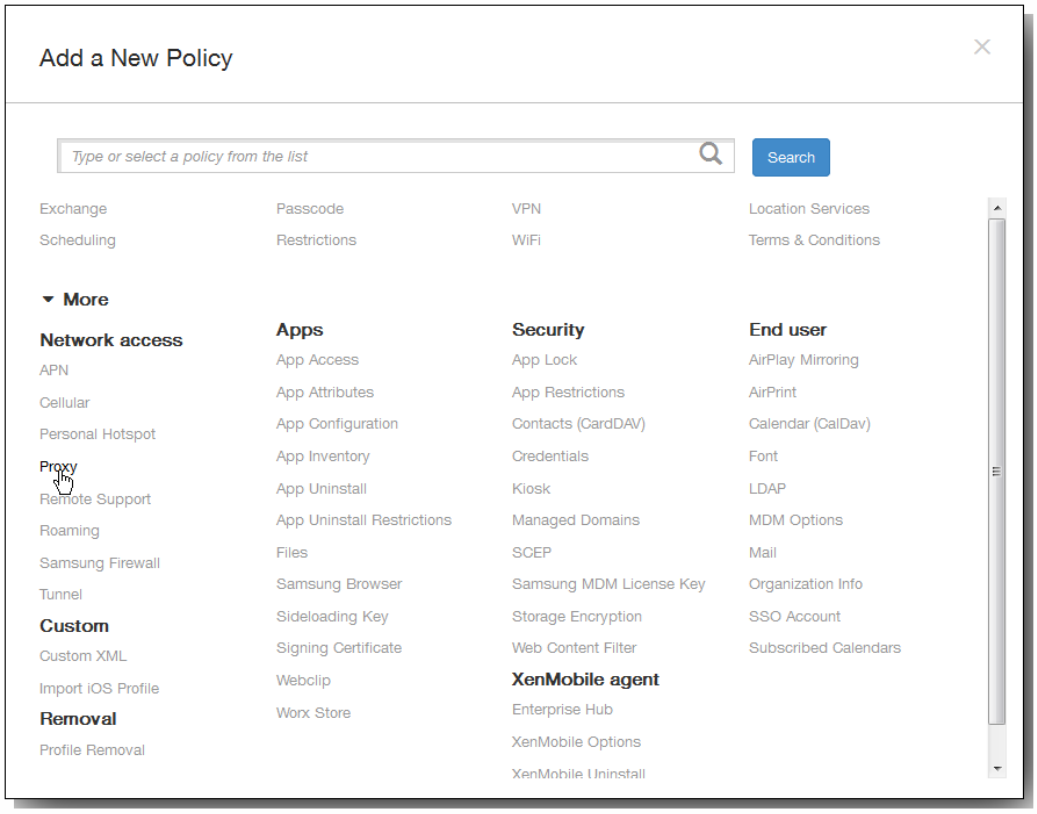
XenMobileでデバイスポリシーを追加して、iOS 6.0以降を実行しているデバイスのグローバルHTTPプロキシ設定を指定できます。グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。

注：このポリシーを展開する前に、グローバルHTTPプロキシを設定するすべてのiOSデバイスを必ずSupervisedモードに設定してください。詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

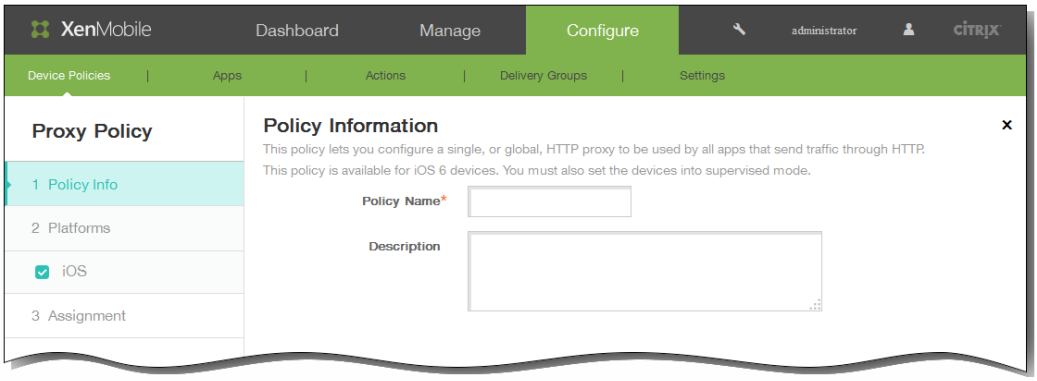
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



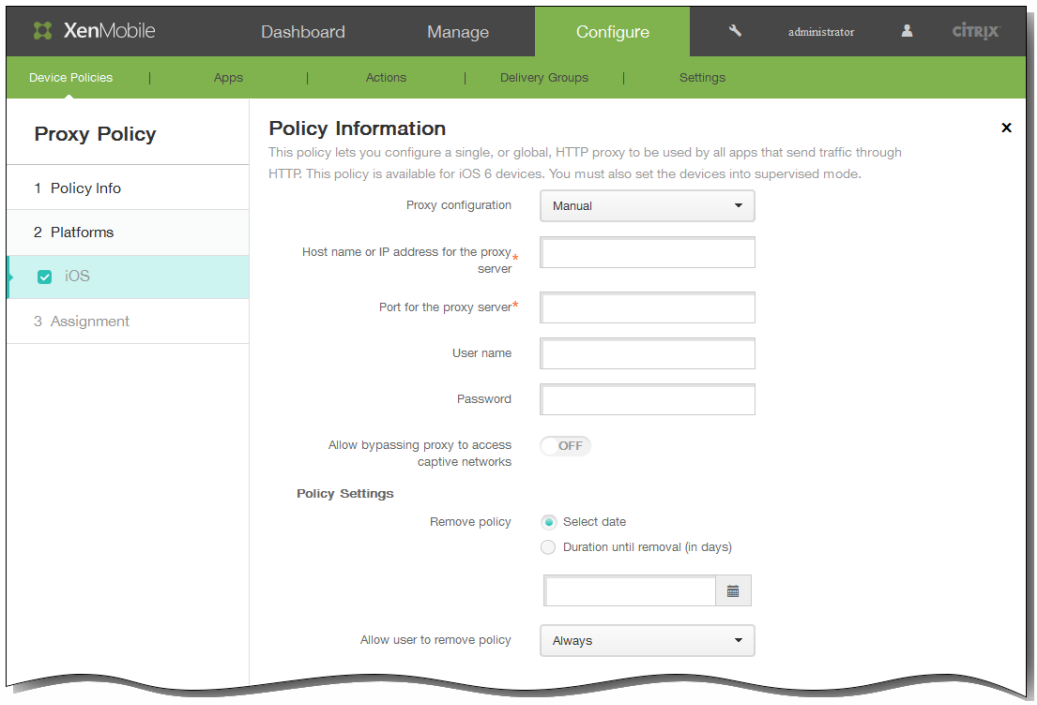
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［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。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。

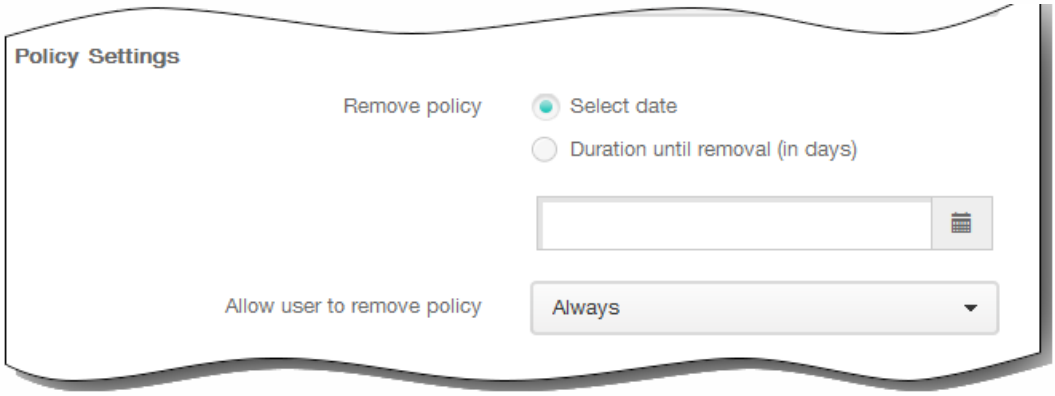


6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. Proxy configuration：ユーザーのデバイスでのプロキシの構成方法に応じて、一覧から［Manual］または［Automatic］を選択します。 次の表は、各プロキシ構成で使用できるオプションの一覧です。各セルは、そのオプションが適用されない（-）、必須、オプション（任意）のいずれかを示しています。

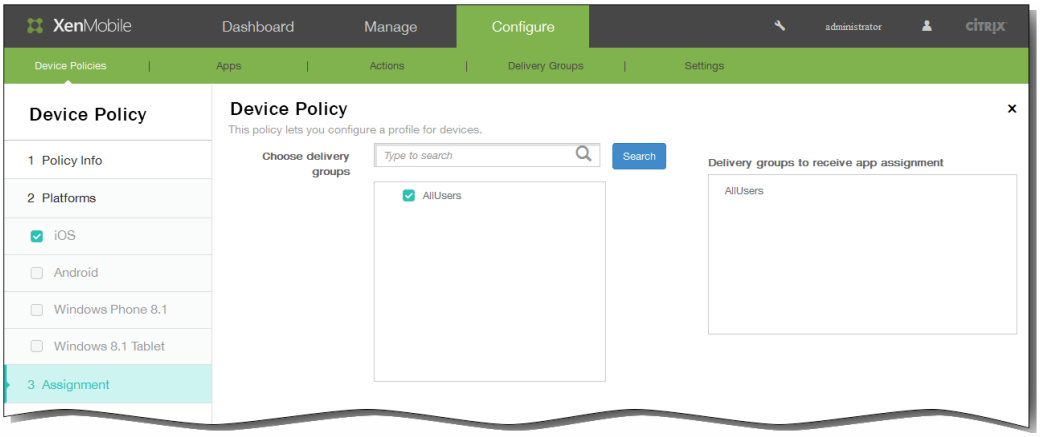
	Manual	Automatic
Host name or IP addrss for the proxy server	必須	–
Port for the proxy server	必須	–
ユーザー名	任意	–
Password	任意	–
Proxy PAC URL	–	任意
Allow direct connection if PAC is unreachable	–	OFF

2. Allow bypassing proxy to access captive networks：プロキシを使用せずにキャプティブネットワークにアクセスできるようにするかどうかを選択します。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。

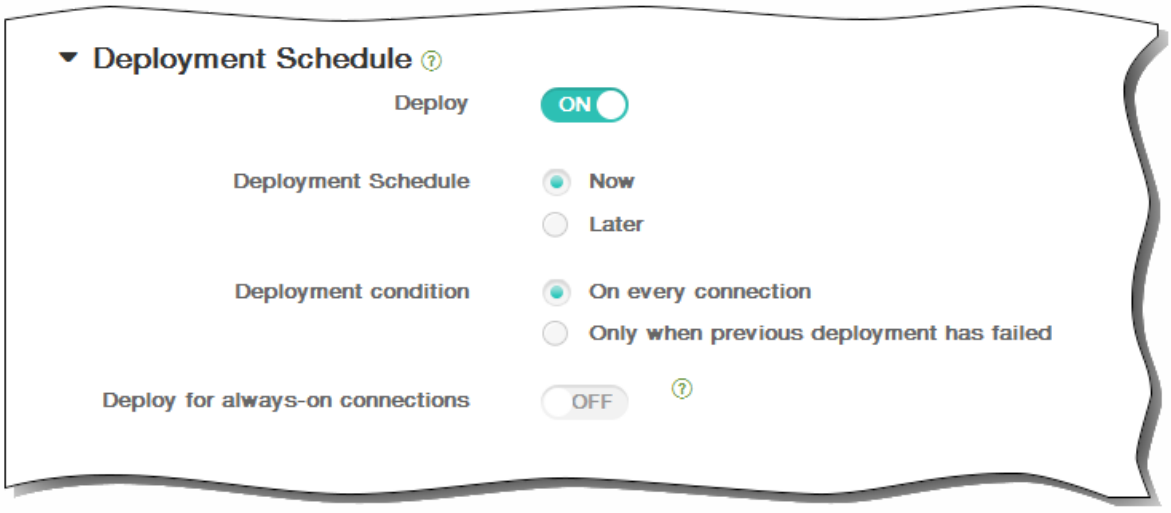


11. ［Next］をクリックします。［Proxy Policy］割り当てページが開きます。
12. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



13. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［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。
    4. ［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。
    5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
    注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



14. ［Save］をクリックしてポリシーを保存します。

Samsung KNOXのリモートサポートデバイスポリシーを追加するには

May 10, 2016

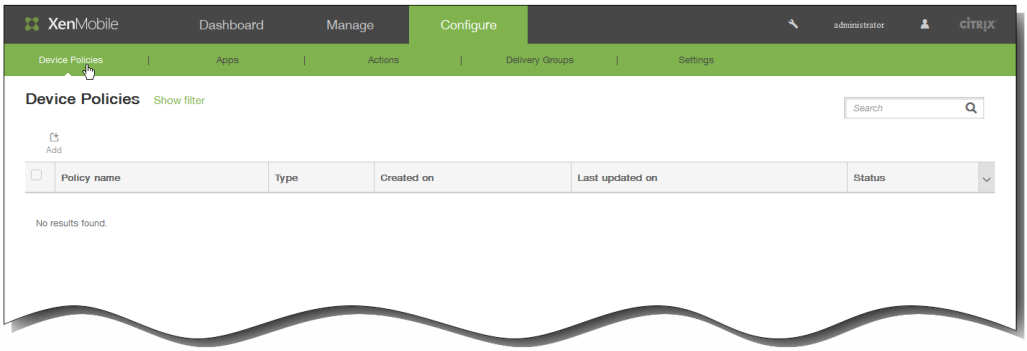
XenMobileでリモートサポートポリシーを作成して、ユーザーのSamsung KNOXデバイスへのリモートアクセスを行うことができます。次の2種類のサポートを構成できます。

- ［Basic］は、システム情報、実行中のプロセス、タスクマネージャー（メモリ使用率とCPU使用率）、インストールされているソフトウェアフォルダーの内容など、デバイスに関する診断情報を表示できます。
- ［Premium］は、色の制御（メインウィンドウまたは独立した浮動ウィンドウ）、ヘルプデスクとユーザーの間のVoIP（Voice-over-IP）セッションの確立、設定の構成、ヘルプデスクとユーザーの間のチャットセッションの確立など、デバイスの画面をリモート制御できます。

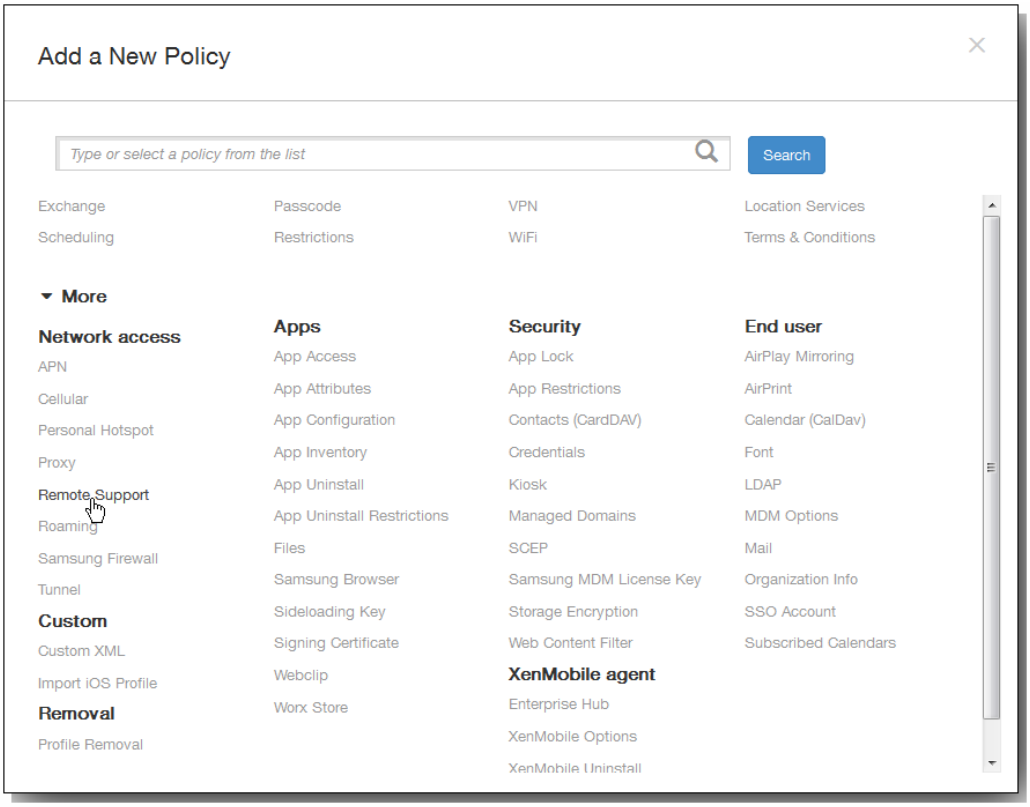
注：このポリシーを実装するには、次の手順を実行する必要があります。

- XenMobile Remote Supportアプリケーションを環境にインストールします。
- リモートサポートアプリトンネルを構成します。詳しくは、「Androidのアプリトンネルデバイスポリシーを追加するには」を参照してください。
- このトピックの説明に従ってSamsung KNOXのリモートサポートデバイスポリシーを構成します。
- アプリトンネルリモートサポートポリシーと、Samsung KNOXのリモートサポートポリシーの両方をユーザーのデバイスに展開します。

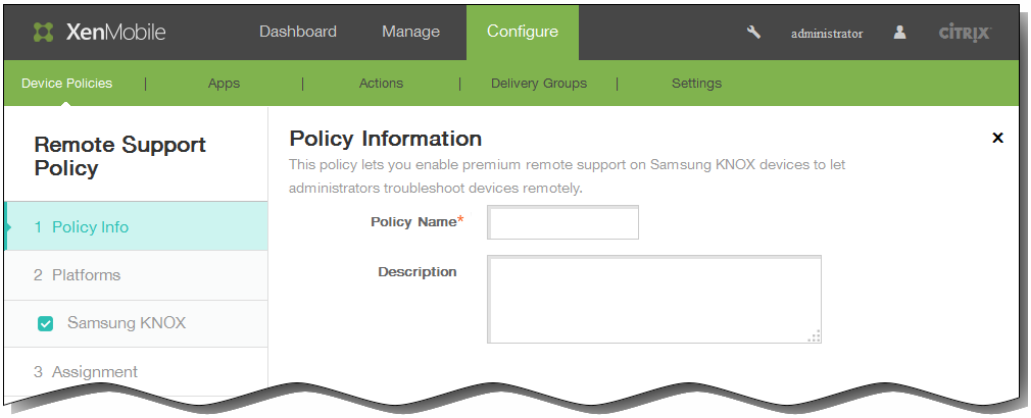
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



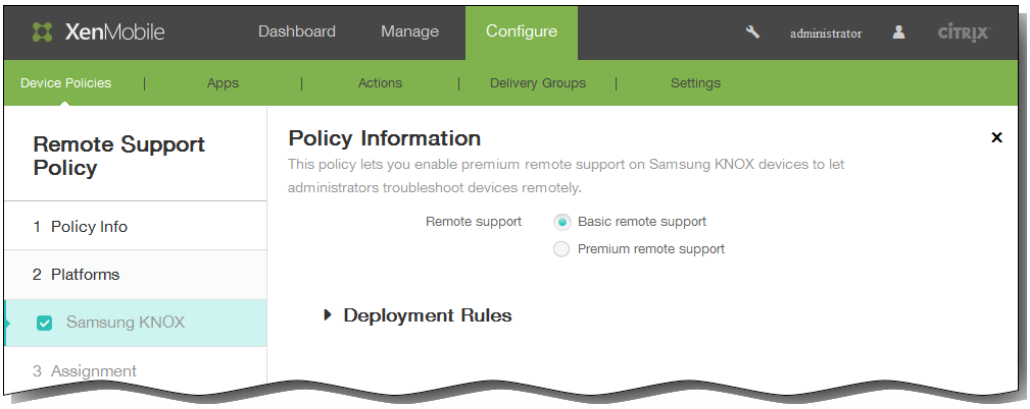
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Network access］の下の［Remote Support］をクリックします。 ［Remote Support Policy］ページが開きます。

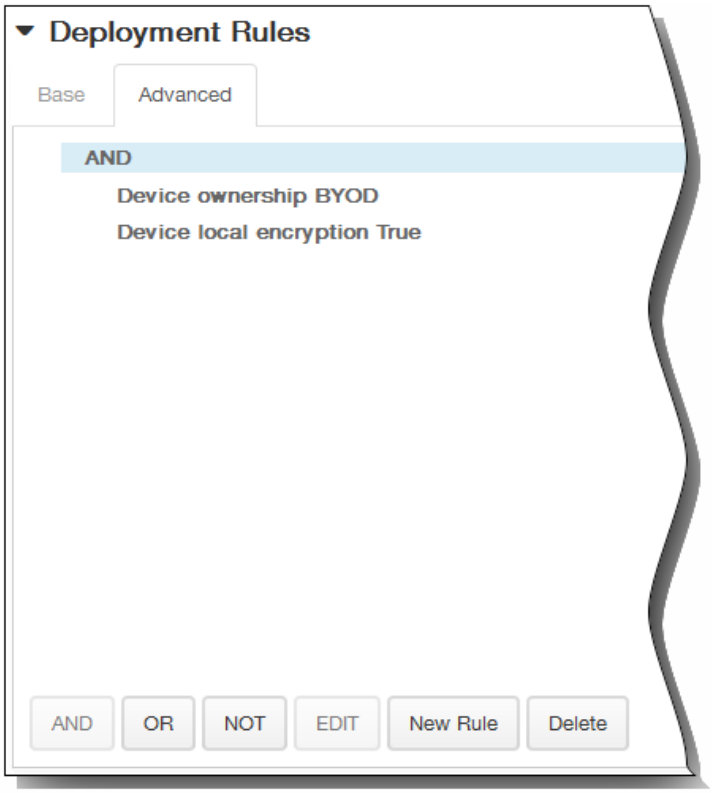


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Samsung KNOX］プラットフォーム情報ページが開きます。



6. ［Samsung KNOX］プラットフォーム情報ページで、以下の情報を入力します。
   1. Remote support：［Basic remote support］または［Premium remote support］をクリックします。 デフォルトは［Basic remote support］です。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

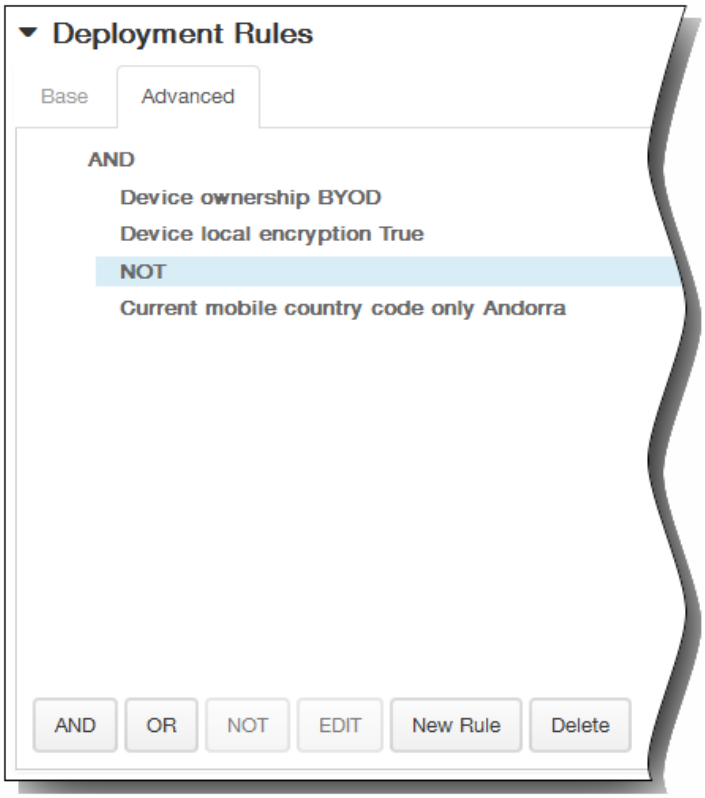
   1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
      1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
      2. ［New Rule］をクリックして条件を定義します。
      3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
      4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
   2. ［Advanced］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。



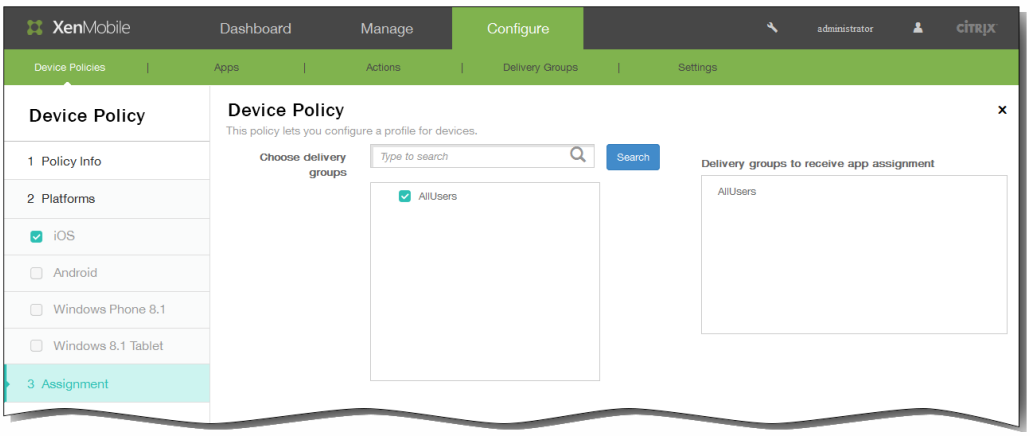
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Remote Support Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



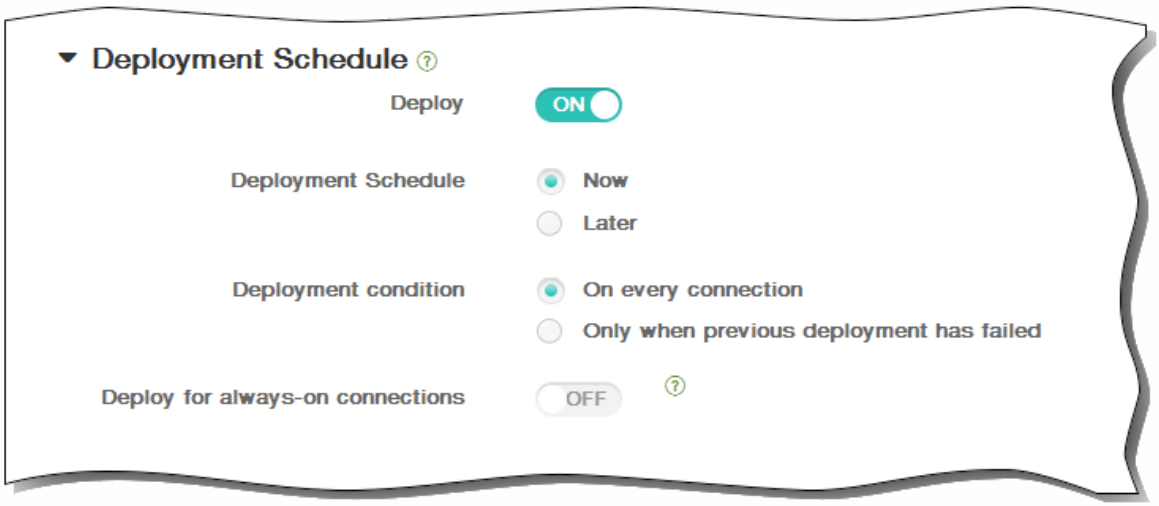
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

制限デバイスポリシー

May 10, 2016

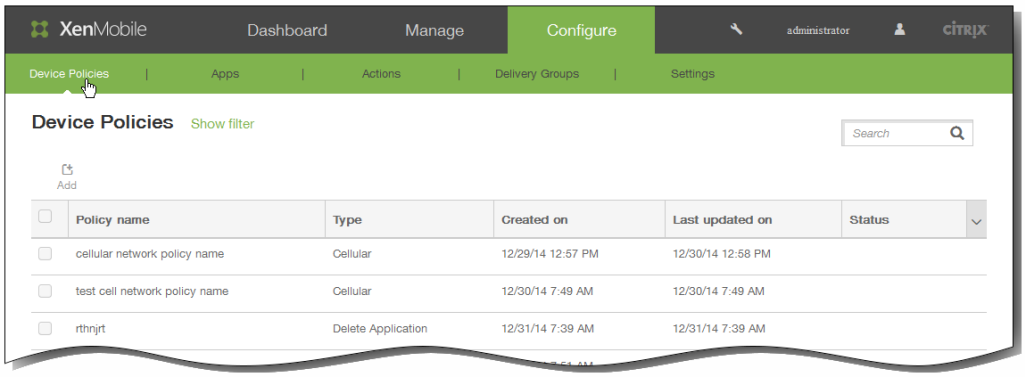
XenMobileでデバイスポリシーを追加して、ユーザーのデバイス、電話、タブレットなどの特定の機能を制限できます。デバイス制限ポリシーは、iOS、Samsung SAFE、Windows 8.1タブレット、Windows Phone 8.1、Amazonの各プラットフォームに対して構成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

このデバイスポリシーでは、デバイスの特定の機能（カメラなど）をユーザーが使用することを許可または制限します。また、セキュリティ制限、メディアコンテンツの制限、ユーザーがインストールできる（できない）アプリケーションの種類の制限を設定できます。ほとんどの制限設定は、デフォルトでは［ON］（
— 許可
）に設定されています。主な例外としては［Security - Force］機能があり、この機能はデフォルトで[OFF］（
— 制限
）に設定されています。
ヒント：
— ON
を選択したオプションは、ユーザーが操作を実行、または機能を使用できる ことを意味します。次に例を示します。

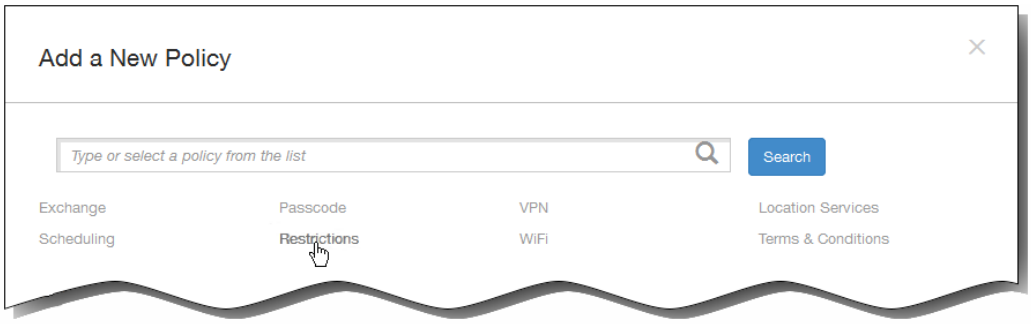
- ［Camera］。［ON］の場合、ユーザーはデバイスでカメラを使用できます。［OFF］の場合、ユーザーはデバイスでカメラを使用できません。
- **［Screen shots］**。［ON］の場合、ユーザーはデバイスでスクリーンショットを取得できます。［OFF］の場合、ユーザーはデバイスでスクリーンショットを取得できません。

注：iOSの制限オプションの中には、特定のiOSバージョンにのみ適用されるものがあります（該当する場合、XenMobileコンソールのページにこれらのバージョンが注記されています）。また、デバイスがSupervisedモードになっている場合にのみ適用されるオプションもあります。たとえば、AirDropの許可またはブロックはiOS 7以降を実行しているデバイスのみでサポートされています。また、フォトストリームの許可またはブロックは、iOS 5以降を実行しているデバイスでサポートされています。iOSデバイスをSupervisedモードに設定する手順については、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

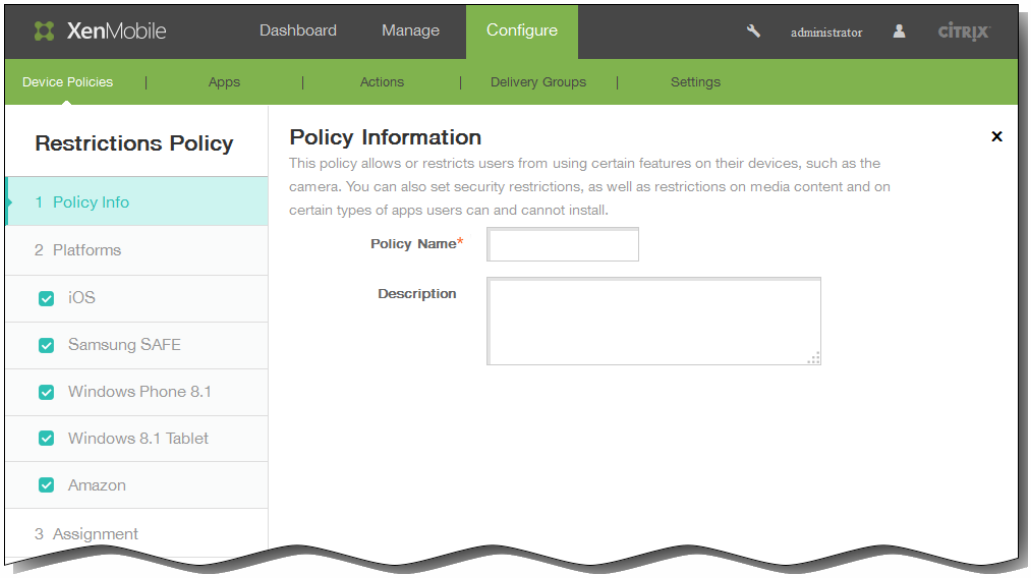
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



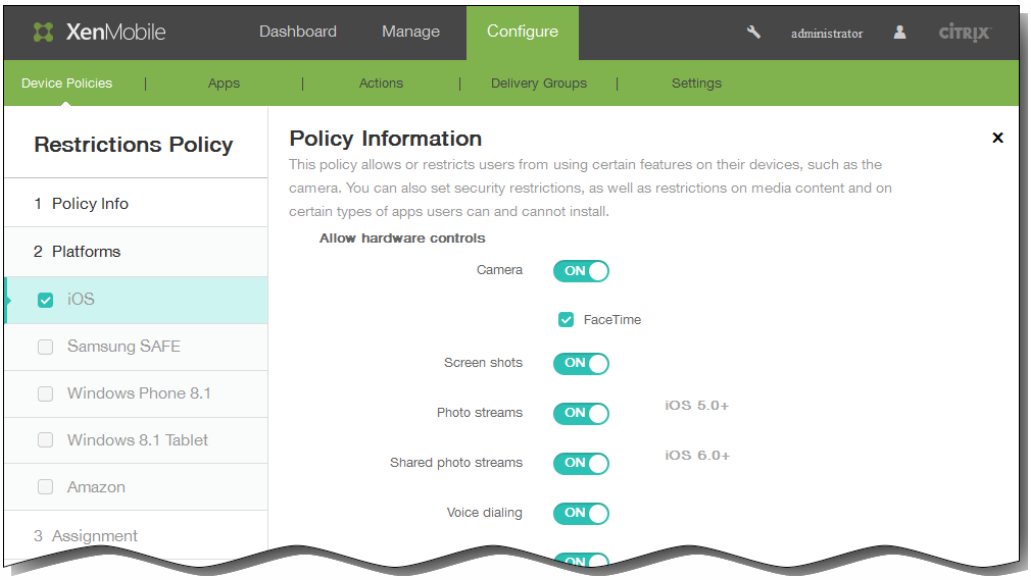
2. ［Add］をクリックします。［Add a New Policy］ページが開きます。



3. ［Restrictions］をクリックします。
［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。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Platforms］の下で、追加するプラットフォームをオンにします。 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します。クリックすると設定が［OFF］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。
   - ［iOS］を選択した場合は、次の設定を構成します。



- Allow hardware controls：

  Camera、FaceTime

  Screen shots

  Photo streams（iOS 5.0以降で使用できます）

  Shared photo streams（iOS 6.0以降で使用できます）

  Voice dialing

  Siri：
  - Allow while device is locked：このオプションをデフォルトのオンのままにするか、チェックボックスをオフにします。
  - Siri profanity filter：このオプションをデフォルトのオフのままにするか、チェックボックスをオンにしますデフォルトでは、この機能を制限します。

  Installing apps

- Allow apps：

  YouTube

  iTunes Store

  In-app purchases: Require iTunes password for purchases：このオプションをデフォルトのオフのままにするか、チェックボックスをオンにします（iOS 5.0以降で使用できます）。デフォルトでは、この機能を制限します。

  Safari：
  - Autofill：このオプションをデフォルトのオンのままにするか、チェックボックスをオフにします。
  - Force fraud warning：このオプションをデフォルトのオフのままにするか、チェックボックスをオンにしますデフォルトでは、この機能を制限します。
  - Enable JavaScript：このオプションをデフォルトのオンのままにするか、チェックボックスをオフにします。
  - Block pop-ups：このオプションをデフォルトのオフのままにするか、チェックボックスをオンにしますデフォルトでは、この機能を制限します。

［Accept cookies］で、次のいずれかをクリックします。

- Always
- Never
- From visited sites only
  デフォルトのオプションは［Always］です。

- Network - Allow iCloud actions：

  Documents and data sync（iOS 5.0以降で使用できます）

  Device backup（iOS 5.0以降で使用できます）

  Automatic sync while roaming

  iCloud keychain（iOS 7.0以降で使用できます）

- Security - Force：

  Encrypted backups（デフォルトは［OFF］です）

  Limited ad tracking（iOS 7.0以降で使用できます。デフォルトは［OFF］です）

  Passcode on first Airplay pairing（iOS 7.0以降で使用できます。デフォルトは［OFF］です）

- Security - Allow：

  Accepting untrusted SSL certificates（iOS 5.0以降で使用できます）

  Automatic update to certificate trust settings（iOS 7.0以降で使用できます）

  Documents from managed apps in unmanaged apps

  Documents from unmanaged apps in managed apps

  Diagnostic submission to Apple

  Touch ID to unlock device（iOS 7.0以降で使用できます）

  Passbook notifications when locked（iOS 6.0以降で使用できます）

  Handoff（iOS 8.0以降で使用できます）

  iCloud sync for managed apps（iOS 8.0以降で使用できます）

  Backup for enterprise books（iOS 8.0以降で使用できます）

  Notes and highlights sync for enterprise books（iOS 8.0以降で使用できます）

- Supervised only settings - Allow：

  Internet results in Spotlight（iOS 8.0以降で使用できます）

  Erase all content and settings（iOS 8.0以降で使用できます）

  Configuring restriction（iOS 8.0以降で使用できます）

Installing configuration profiles（iOS 6.0以降で使用できます）

AirDrop（iOS 7.0以降で使用できます）

iMessage（iOS 6.0以降で使用できます）

Siri user-generated content（iOS 7.0以降で使用できます）

iBooks（iOS 6.0以降で使用できます）

Removing apps（iOS 7.0以降で使用できます）

Game Center（iOS 6.0以降で使用できます）
- Add friends：このオプションをデフォルトのオンのままにするか、チェックボックスをオフにします。
- Multiplayer gaming：このオプションをデフォルトのオンのままにするか、チェックボックスをオフにします。

Modifying account settings（iOS 7.0以降で使用できます）

Modifying app cellular data settings（iOS 7.0以降で使用できます）

Modifying Find My Friends settings（iOS 7.0以降で使用できます）

Pairing with non-Configurator hosts（iOS 7.0以降で使用できます）

Single App bundle ID：［App name］に、アプリケーションを1つ以上入力します。

- Security - Show in lock screen：

  Control Center（iOS 7.0以降で使用できます）

  Notification（iOS 7.0以降で使用できます）

  Today view

- Media content - Allow：

  Explicit music, podcasts, and iTunes U material

  Explicit sexual content in iBooks（iOS 6.0以降で使用できます）

  Ratings region：一覧から国を選択します。デフォルトは［United States］です。

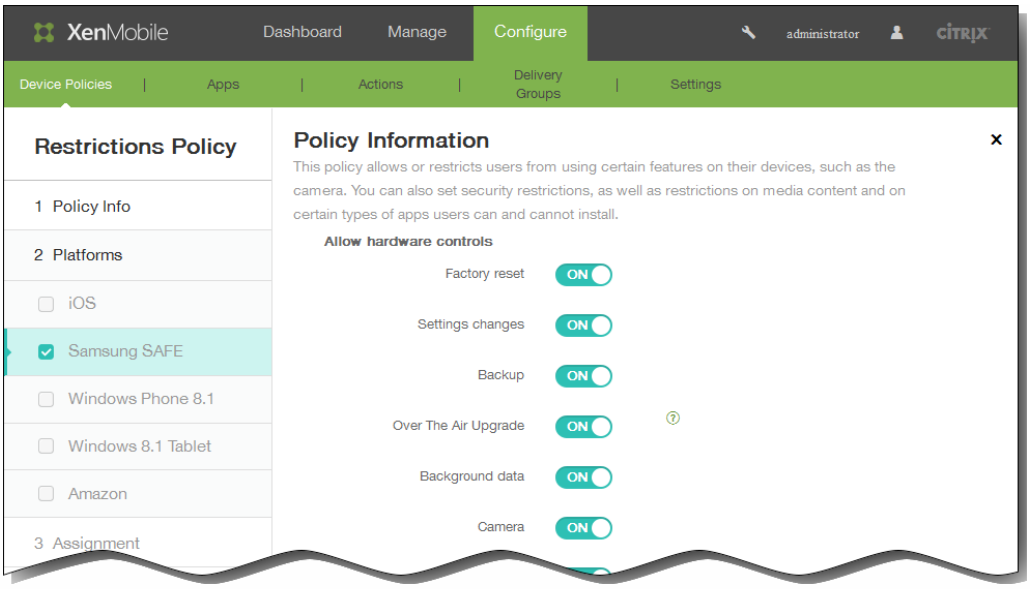
  Movies：［Allow all movies］、［Block movies］、［G］、［PG］、［PG-13］、［R］、［NC-17］のいずれかのオプションをクリックします。デフォルトは［Allow all movies］です。

  TV Shows：［Allow all TV shows］、［Block TV shows］、［TV-Y］、［TV-Y7］、［TV-G］、［TV-PG］、［TV-PG14］、［TV-MA］のいずれかのオプションをクリックします。デフォルトは［Allow all TV Shows］です。

  Apps：［Allow all apps］、［Block apps］、［4+］、［9+］、［12+］、［17+］のいずれかのオプションをクリックします。デフォルトは［Allow all apps］です。

- ［Samsung SAFE］を選択した場合は、次の設定を構成します。

  注：一部のオプションは、Samsungモバイルデバイス管理API 4.0以降でのみ使用できます。該当するものには「（MDM 4.0以降）」と表記しています。



- ［Allow hardware controls］で以下を設定します。

  Factory Reset

  Settings changes

  Backup

  Over The Air Upgrade（MDM 4.0以降）

  Background data

  Camera

  Clipboard

  Clipboard share（MDM 4.0以降）

  Home key

  Microphone

  Mock location

  NFC (Near Field Communication)（MDM 4.0以降）

  Power off（MDM 4.0以降）

  Screenshot

  SD card

  Voice Dialer（MDM 4.0以降）

  SBeam（MDM 4.0以降）

  SVoice（MDM 4.0以降）

- ［Allow apps］で以下を設定します。

  Browser

  YouTube

  GooglePlay/Marketplace

  Allow No-Google Play apps

  Stop system app（MDM 4.0以降）

- ［Network］で以下を設定します。

  Bluetooth、Tethering

  WiFi、Tethering, Direct（MDM 4.0以降）

  Tethering

  Cellular data

  Allow roaming。デフォルトは［OFF］です。

  Only secure connections

  Android beam（MDM 4.0以降）

  Audio record（MDM 4.0以降）

  Video record（MDM 4.0以降）

  Location services

  Limit by day（MB）：ユーザーが利用できる、1日あたりのMB数を入力します。デフォルトは0で、この機能を無効にします（MDM 4.0以降）。

  Limit by week（MB）：ユーザーが利用できる、1週間あたりのMB数を入力します。デフォルトは0で、この機能を無効にします（MDM 4.0以降）。

  Limit by month（MB）：ユーザーが利用できる、1か月あたりのMB数を入力します。デフォルトは0で、この機能を無効にします（MDM 4.0以降）。

- ［Allow USB actions］で以下を設定します。

  Debugging

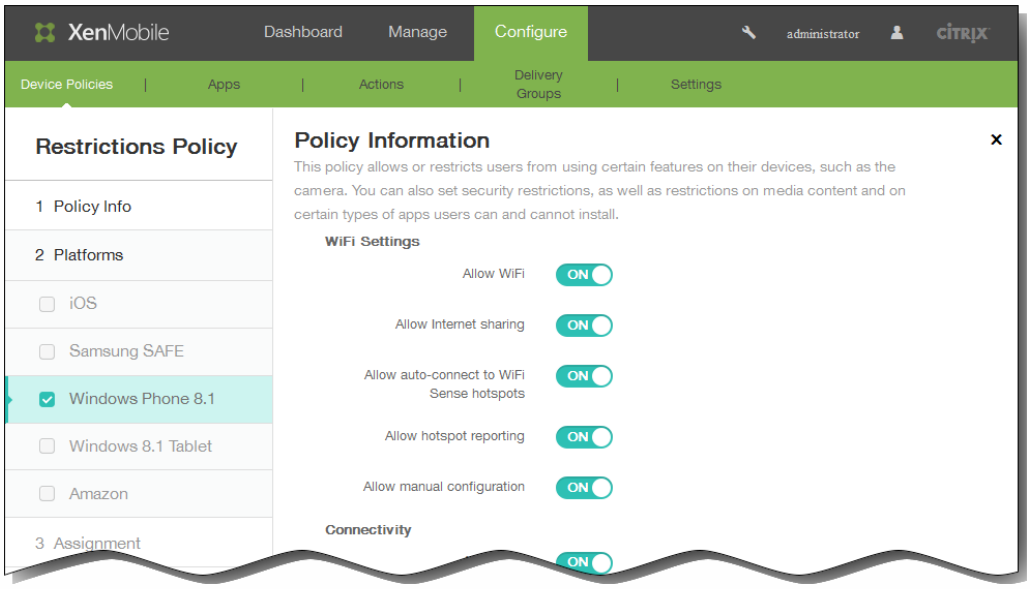
  Host storage

  Mass storage

  Kies media player

  Tethering

- ［Windows Phone 8.1］を選択した場合は、次の設定を構成します。



- WiFi Settings :

  Allow WiFi

  Allow Internet sharing

  Allow auto-connect to WiFiSense hotspots

  Allow hotspot reporting

  Allow manual configuration

- Connectivity :

  Allow NFC (Near Field Communication)

  Allow bluetooth

  Allow VPN over cellular

  Allow VPN over cellular while roaming

  Allow USB connection

  Allow cellular data roaming

- Accounts :

  Allow Microsoft account connection

  Allow non-Microsoft email

- Search :

  Allow search to use location

Filter adult content（デフォルトは［OFF］です）

Allow Bing Vision to store images

- System :

  Allow storage card

  Allow location services

  Allow use of camera

  Telemetry：［Allowed］、［Not Allowed］、［Allowed except for secondary data request］のいずれかの設定をクリックしますデフォルトは［Allowed］です。

- Security :

  Allow manual root certificate installation

  Require device encryption（デフォルトは［OFF］です）

  Allow copy and paste

  Allow screen capture

  Allow voice recording

  Allow Save As of Office files

  Allow action center notifications

  Allow Cortana

  Allow sync of device settings

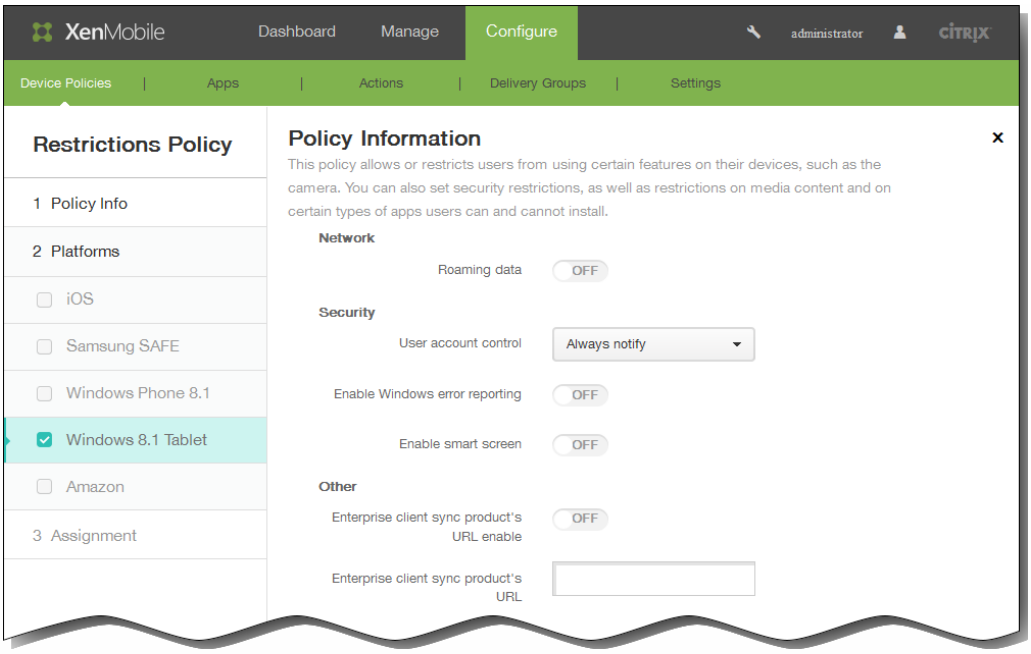
- Apps :

  Allow store access

  Allow developer unlock

  Allow web browser access

- ［Windows 8.1 Tablet］を選択した場合は、次の設定を構成します。



- Network：

  Roaming data

- Security：

  User account control：一覧から、［Always notify］、［Notify app changes］、［Notify app changes (no dim)］、［Never notify］のいずれかの設定を選択します。デフォルトは［Always notify］です。

  Enable Windows error reporting

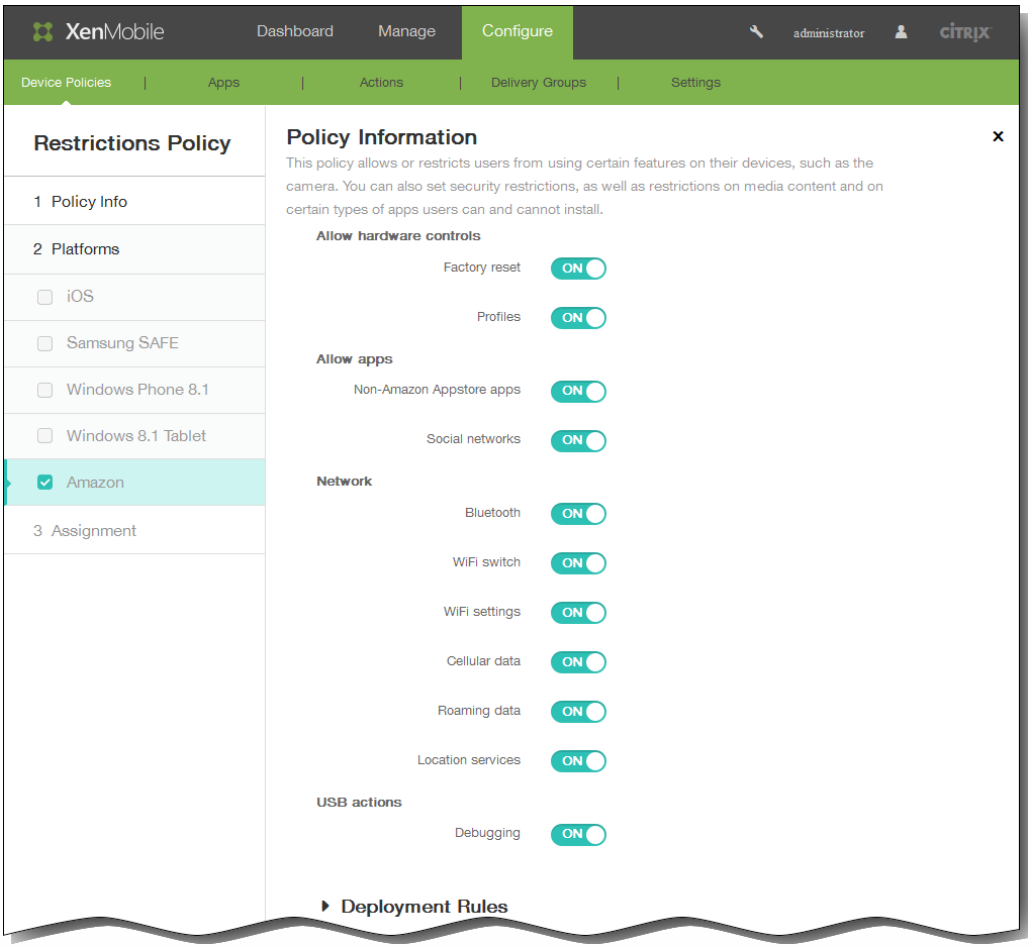
  Enable smart screen

- Other：

  Enterprise client sync product's URL enable

  Enterprise client sync product's URL：有効なURLアドレスを入力します。

- ［Amazon］を選択した場合は、次の設定を構成します。



- Allow hardware controls：

  Factory reset

  Profiles

- Allow apps：

  Non-Amazon Appstore apps

  Social networks

- Network：

  Bluetooth

  WiFi switch

  WiFi settings

  Cellular data

  Roaming data

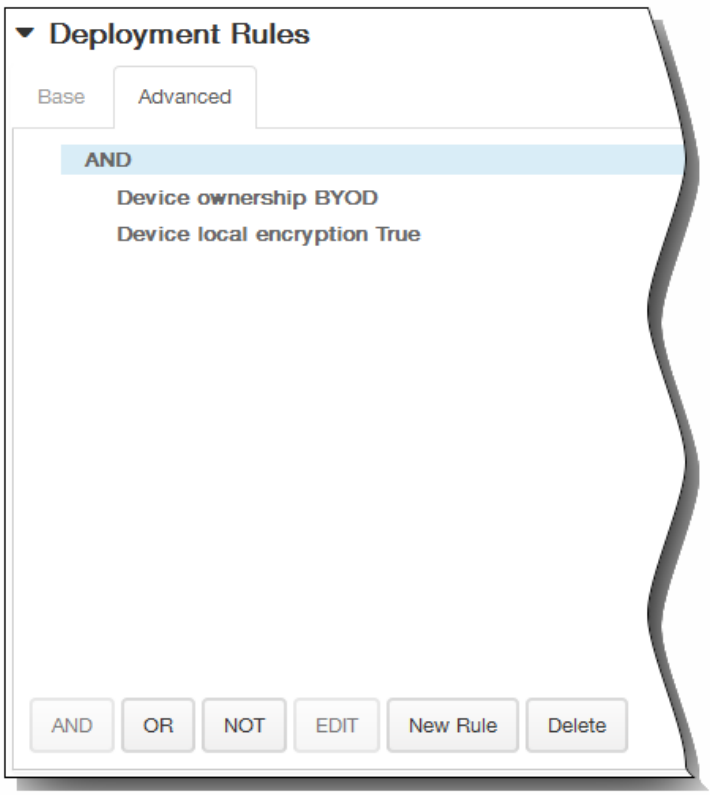
  Location services

- USB actions：

  Debugging

6. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

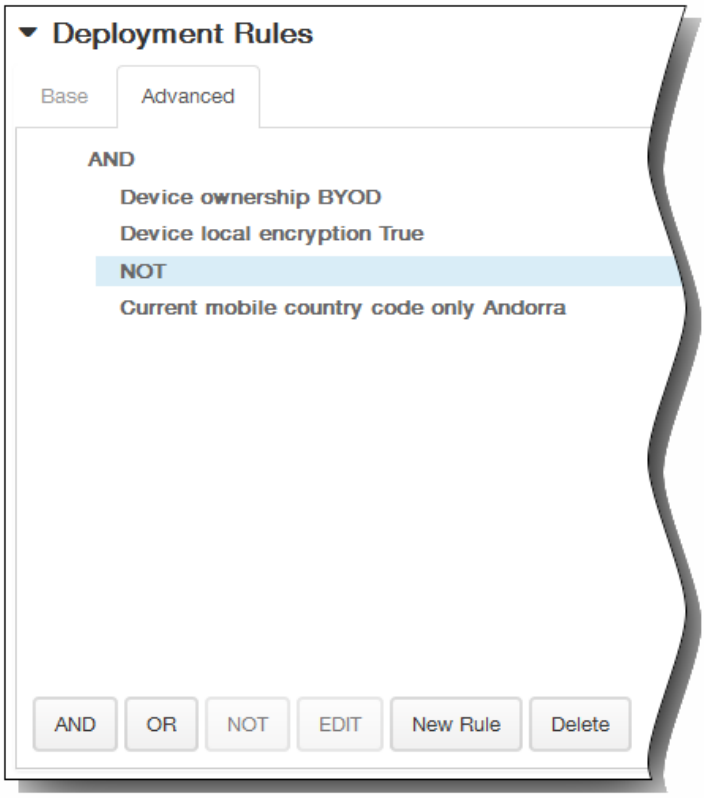
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
   1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］タブをクリックし、ブール値オプションを使用して規則を組み合わせます。



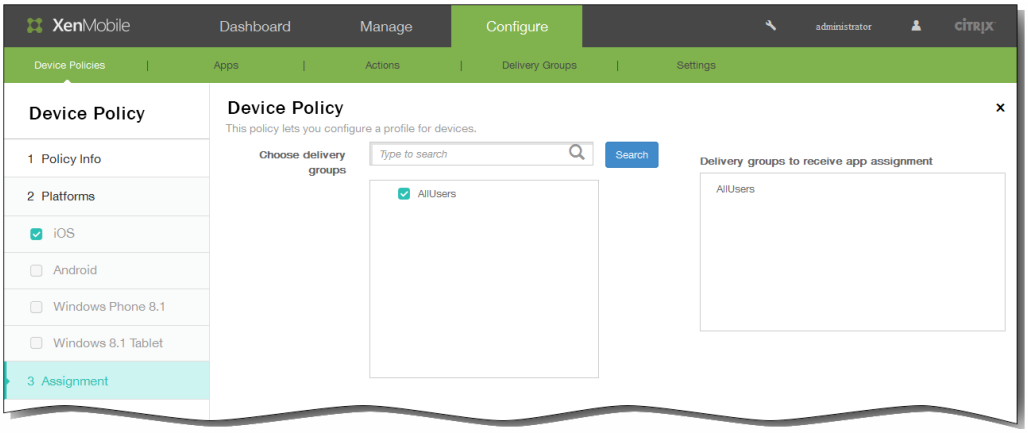
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
    1. ［AND］、［OR］、または［NOT］をクリックします。
    2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
       いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

    3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
       この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。

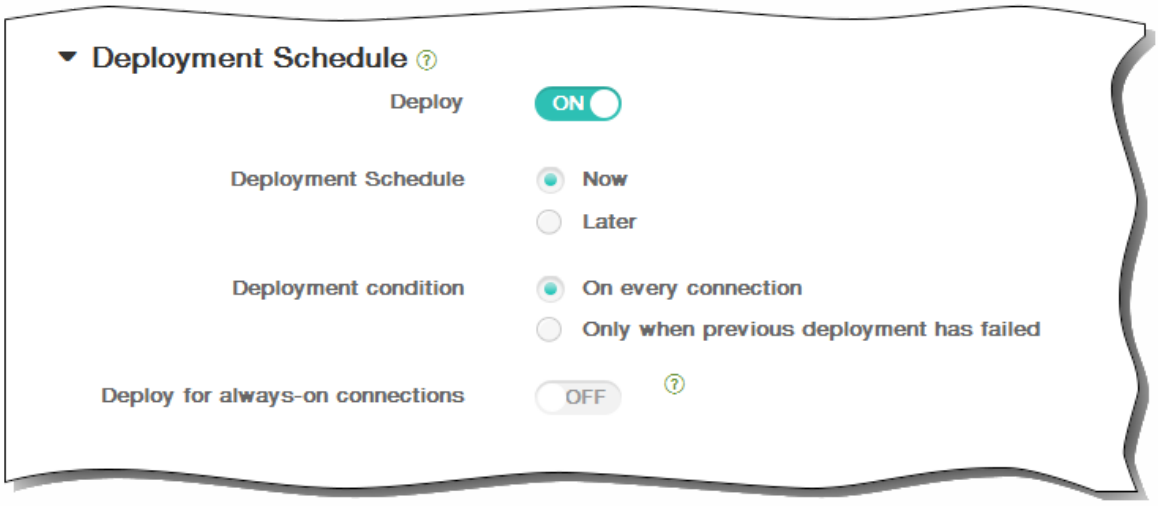


7. 1つまたは複数のプラットフォームについて設定の構成を完了して［Next］をクリックすると、［Assignment］ページが開きます。
8. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



9. ［Deployment Schedule］を展開して以下の設定を構成します。
   1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
   2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
   3. ［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。
   4. ［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。
   5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
      注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

   注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



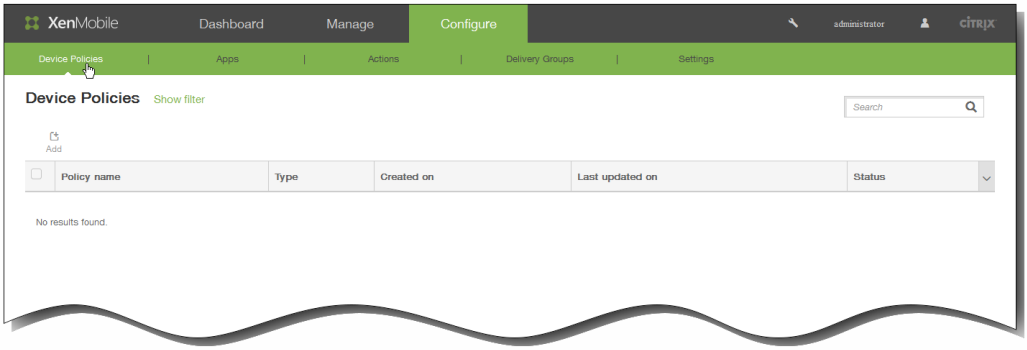
10. ［Save］をクリックしてポリシーを保存します。

iOSのローミングデバイスポリシーを追加するには

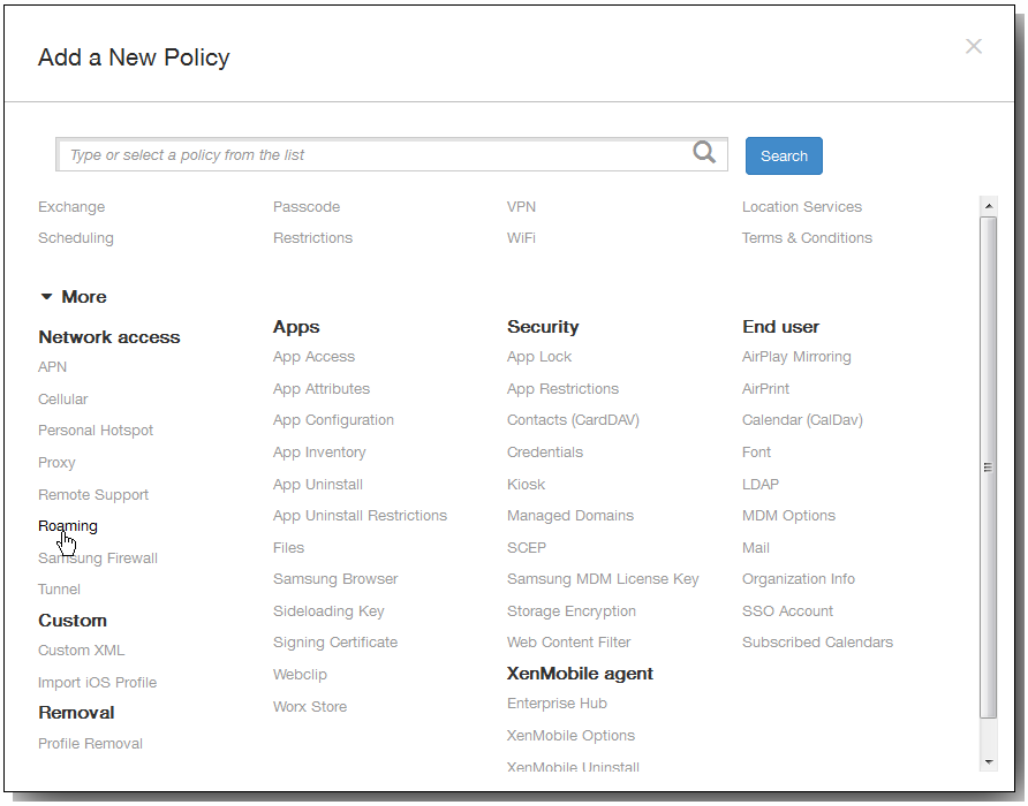
May 10, 2016

XenMobileでデバイスポリシーを追加して、ユーザーのiOSデバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。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。

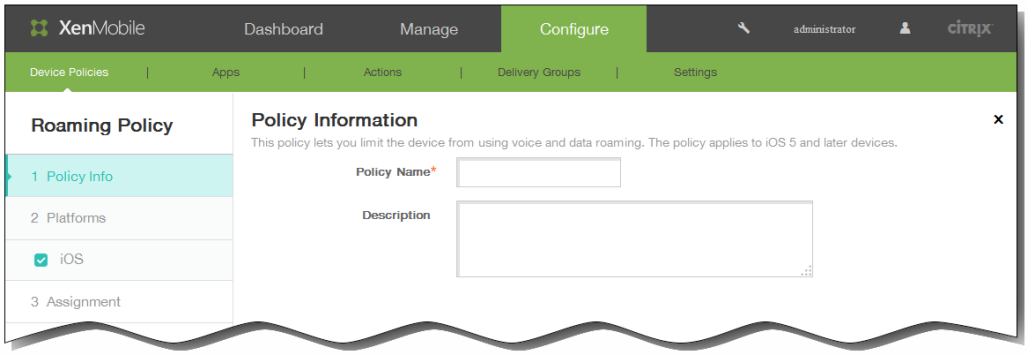
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



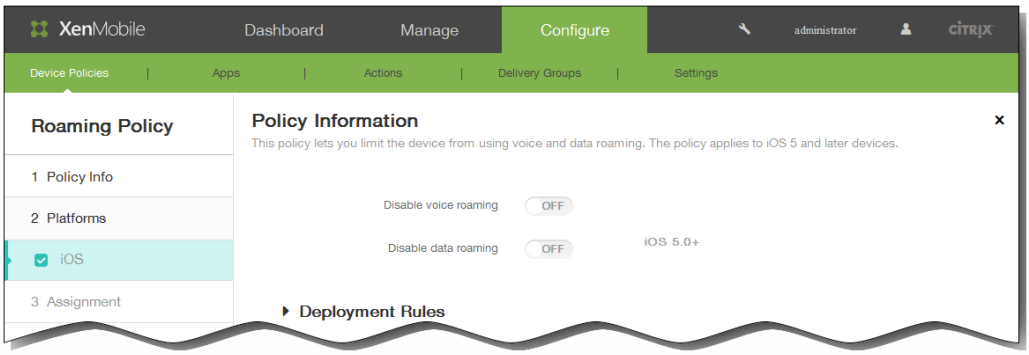
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Network access］の下の［Roaming］をクリックします。 ［Roaming Info 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。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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。



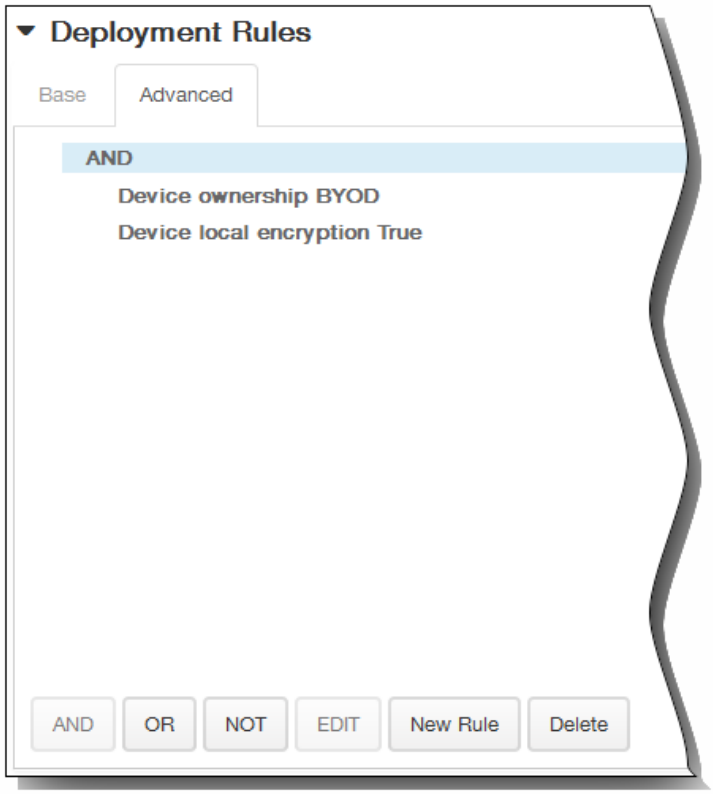
6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. Disable voice roaming：音声通話ローミングを無効にするかどうかを選択します。 このオプションを有効にした場合、データローミングは自動的に無効になります。 デフォルトは［OFF］で、音声通話ローミングを許可します。
   2. Disable data roaming：データローミングを無効にするかどうかを選択します。 このオプションは、音声通話ローミングが有効になっている場合にのみ使用できます。 デフォルトは［OFF］で、データローミングを許可します。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

   1. 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。
      1. 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［All］です。

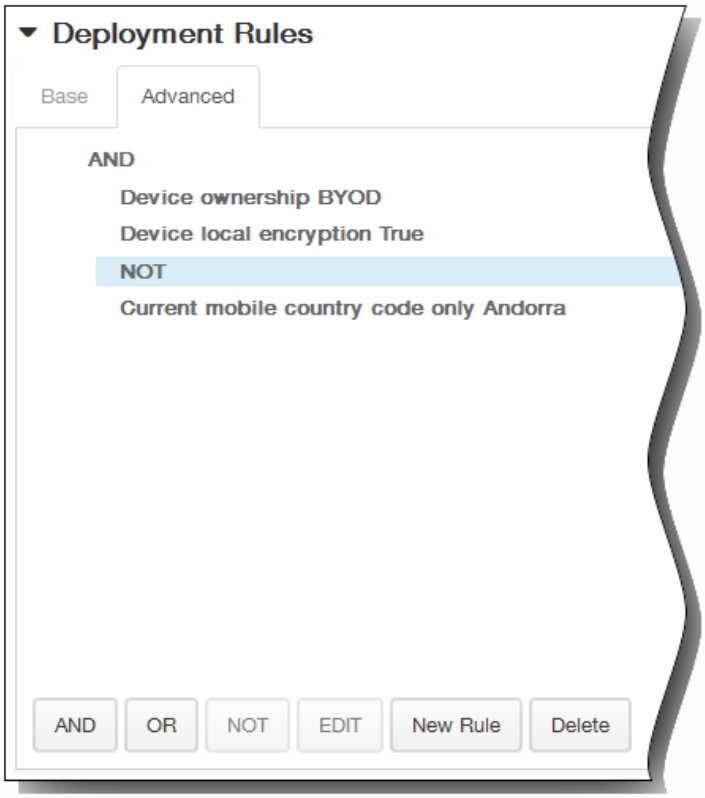
2. ［New Rule］をクリックして条件を定義します。
3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。

2. ［Advanced］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。

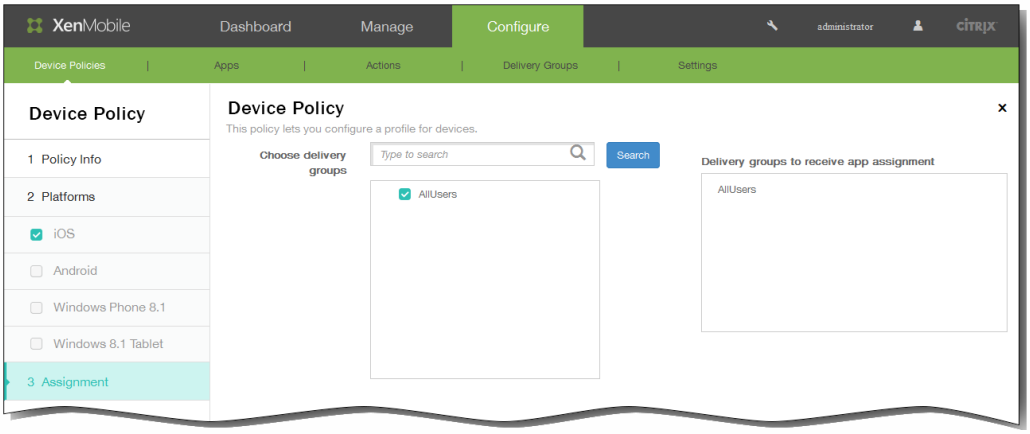


［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。
   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Roaming Info Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



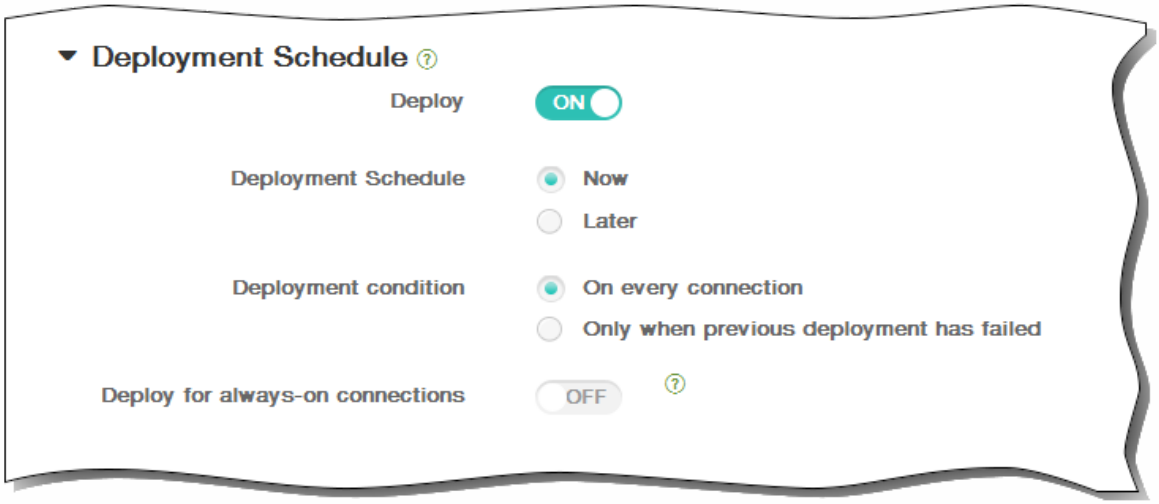
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



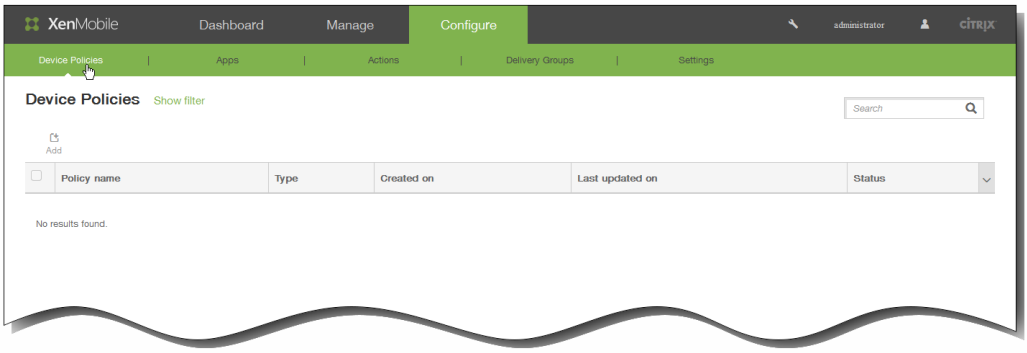
11. ［Save］をクリックしてポリシーを保存します。

iOSのSCEPデバイスポリシーを追加するには

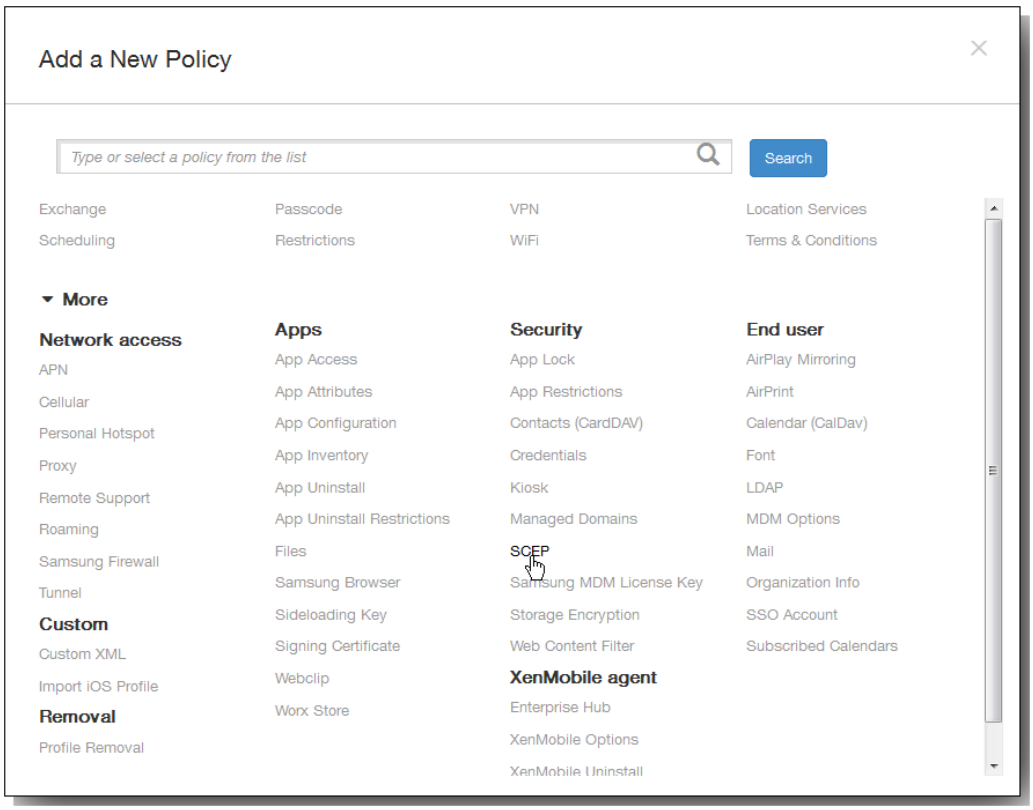
May 10, 2016

このポリシーでiOS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。

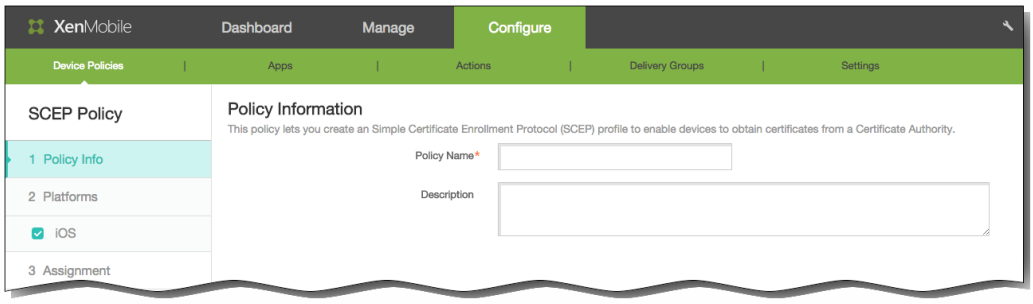
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。
   ［Device Policies］ページが開きます。



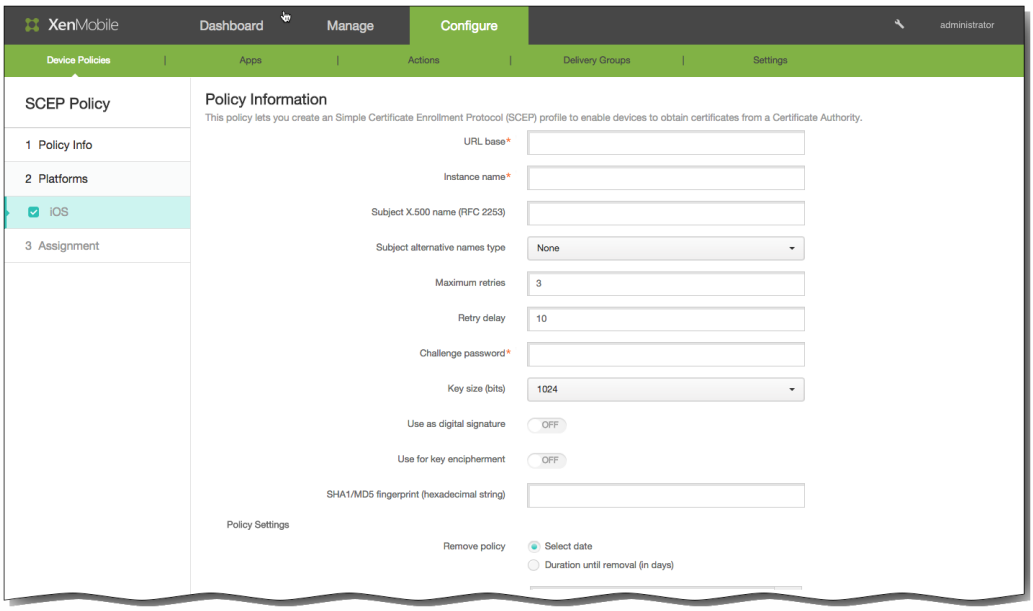
2. ［Add］をクリックします。
   ［Add a New Policy］ページが開きます。



3. ［Add a New Policy］ページで［More］をクリックした後、［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。



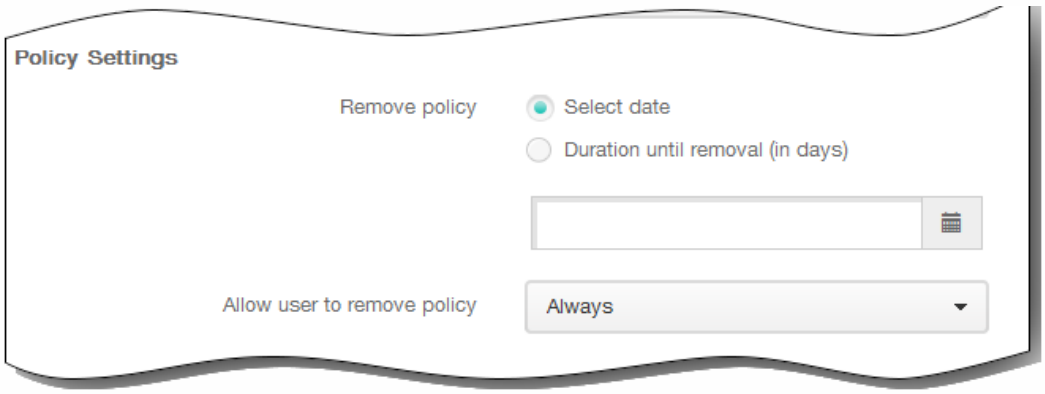
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。
   ［iOS Platform Information］ページが開きます。



6. ［iOS Platform Information］ページで、以下の情報を入力します。
   1. 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。
   2. 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。

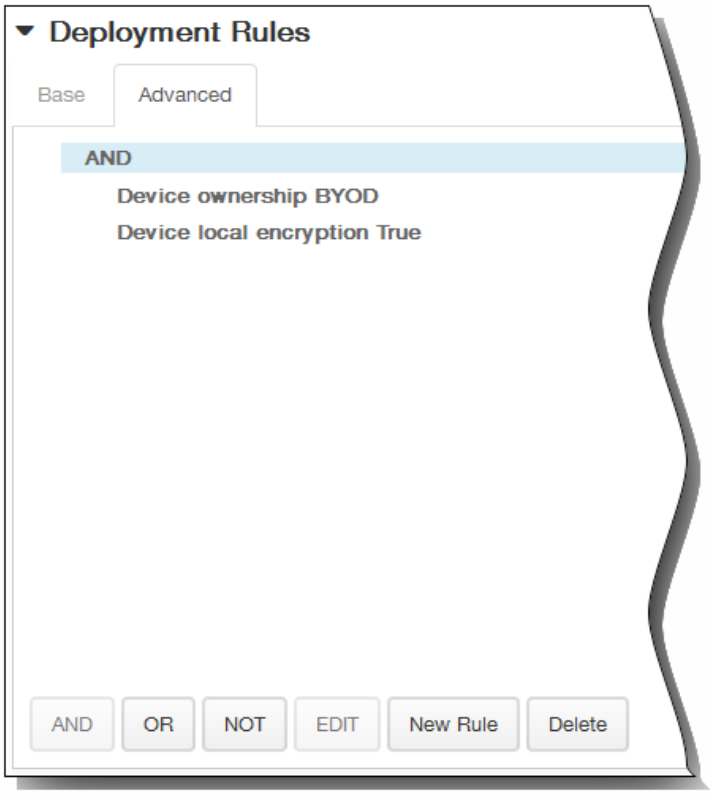
3. Subject X.500 name (RFC 2253)：オブジェクト識別子（OID）と値の配列として示されるX.500の名前の表現を入力します。 たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]」のように解釈されます。 OIDはドット付き数値として表すことができ、略語は国（C）、地域（L）、州（ST）、組織（O）、組織単位（OU）、共通名（CN）を表しています。
4. ［Subject alternative 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。
5. Maximum retries：ユーザーが誤ったパスワードを入力した場合に再試行できる回数を入力します。 デフォルトは3です。
6. Retry delay：ユーザーの再試行が最大数を超えた後、ロックアウトが適用される期間を入力します。 デフォルトは10てす。
7. Challenge password：事前共有シークレットを入力します。 これは必須の手順です。
8. ［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。
9. 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。
10. 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。
11. 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。

7. ［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。
8. ［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。
9. ［Allow user to remove policy］の一覧で、 ［Always］、 ［Password required］、 ［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

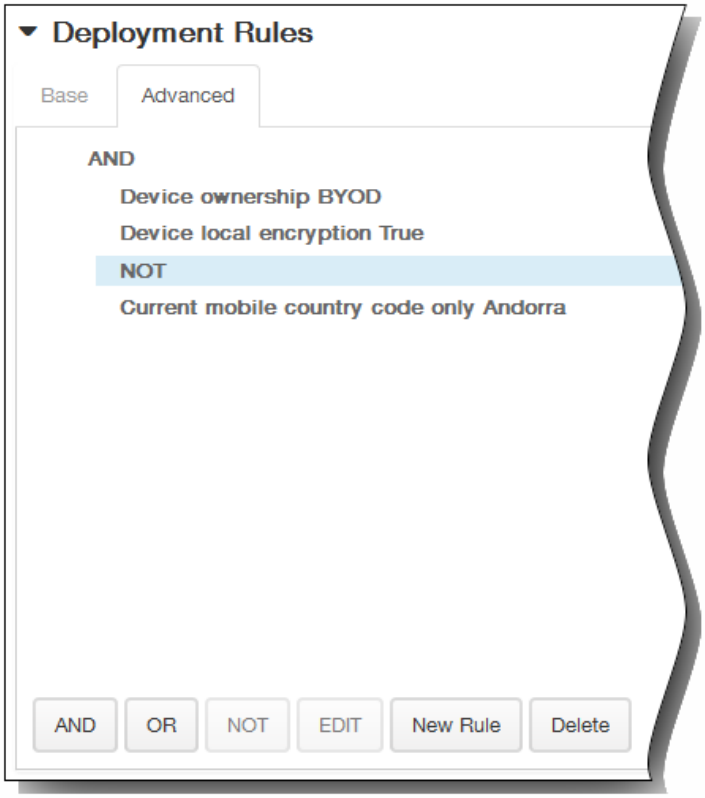


［Base］タブで選択した条件が表示されます。

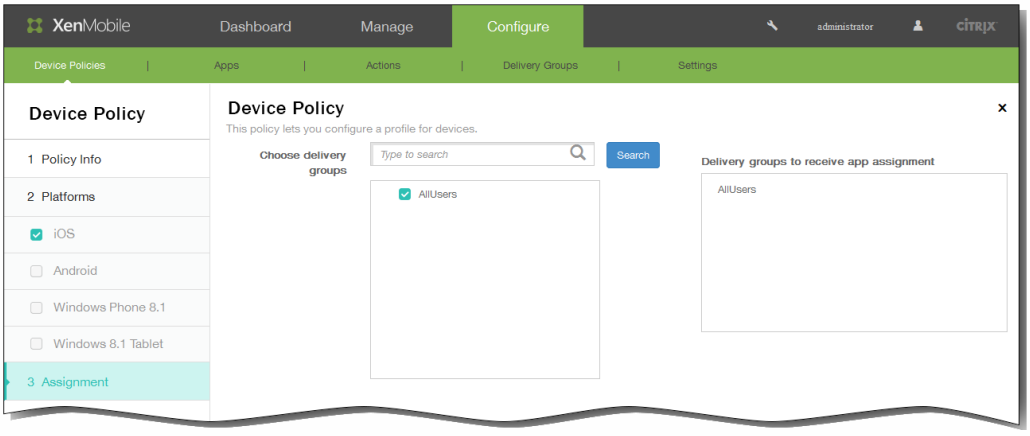
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［SCEP Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

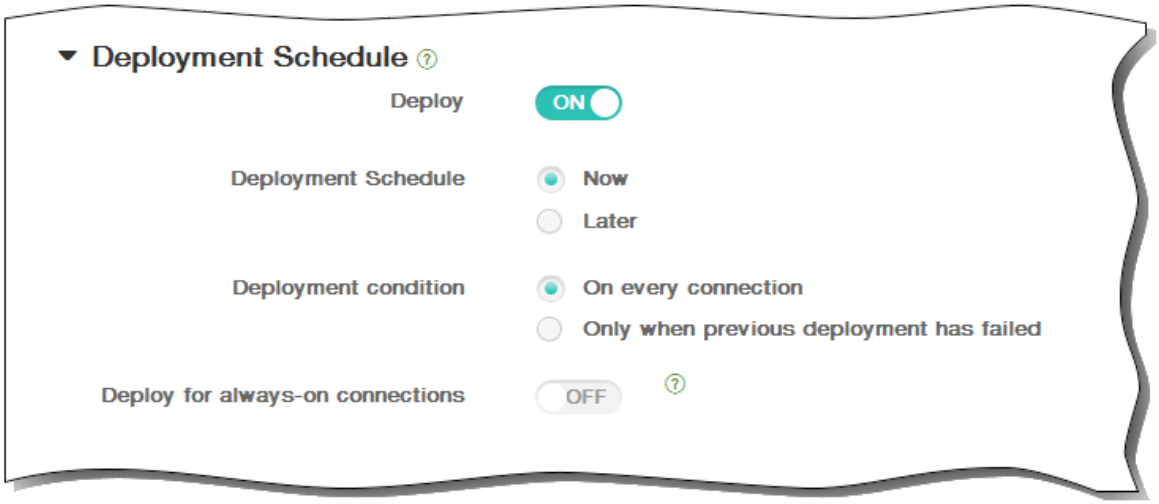


14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



15. ［Save］をクリックしてポリシーを保存します。

Samsung MDMライセンスキーデバイスポリシー

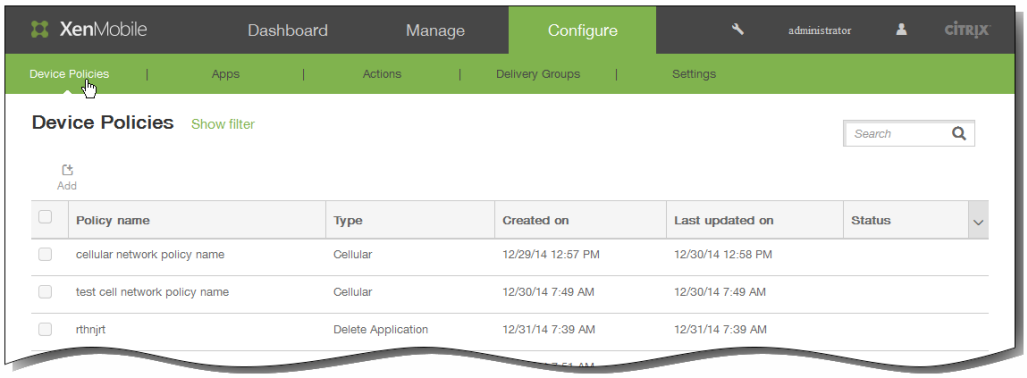
May 10, 2016

XenMobileはSamsung for Enterprise（SAFE）およびSamsung KNOXポリシーの両方をサポートし、拡張しています。SAFEは、モバイルデバイス管理（MDM：Mobile Device Management）ソリューションとの統合を通じてビジネス向けのセキュリティおよび機能拡張を提供するソリューションファミリーです。Samsung KNOXは、企業向けにより高いセキュリティで保護されたAndroidプラットフォームを提供する、SAFEプログラム内のソリューションです。

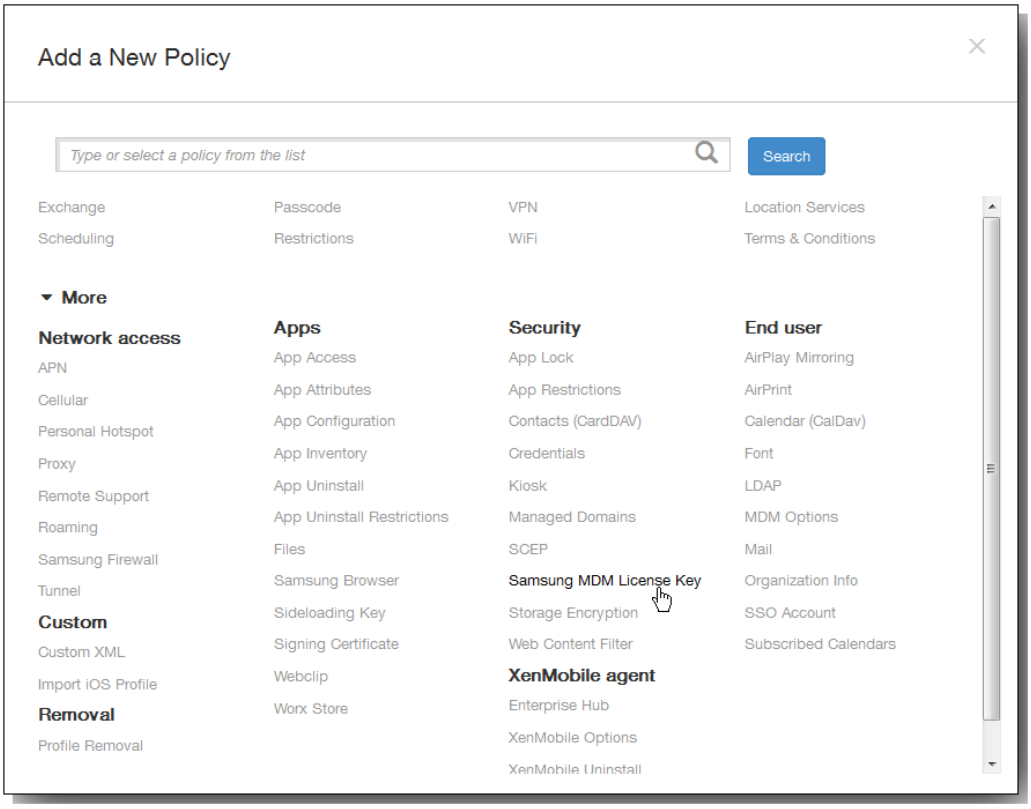
SAFEのポリシーおよび制限を展開する前に、組み込みのSamsung Enterprise License Management（ELM）キーをデバイスに展開することによってSAFE APIを有効にする必要があります。また、Samsung KNOX APIを有効にするには、Samsung ELMキーの展開に加え、Samsung KNOX License Management System（KLMS）を使用してSamsung KNOXライセンスを購入する必要もあります。Samsung KLMSはモバイルデバイス管理（MDM：Mobile Device Management）ソリューションに有効なライセンスをプロビジョニングし、モバイルデバイスでSamsung KNOX APIをアクティブ化できるようにします。これらのライセンスはSamsungから取得する必要があり、Citrixからは提供されません。

Worx HomeをSamsung ELMキーと共に展開し、SAFEおよびSamsung KNOX APIを有効にする必要があります。SAFE APIが有効になっていることは、デバイスプロパティをチェックすることで確認できます。Samsung ELMキーが展開されると、［Samsung MDM API available］設定が［True］に設定されます。

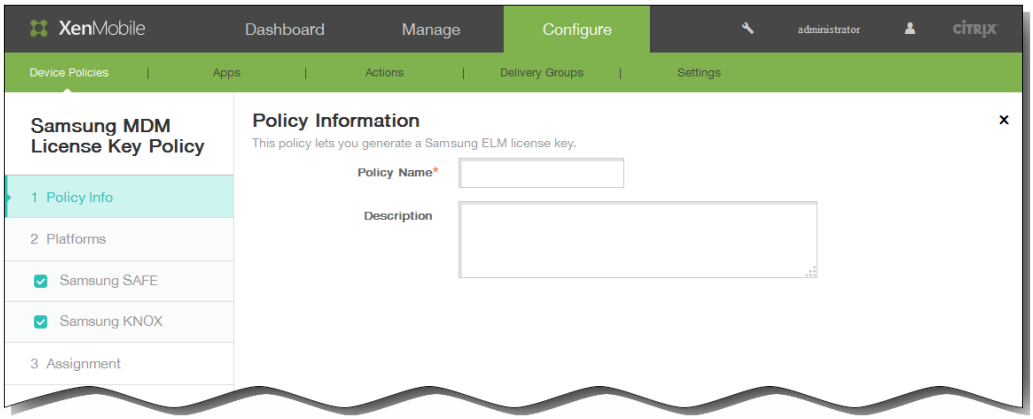
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



2. 新しいポリシーを追加するには［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。

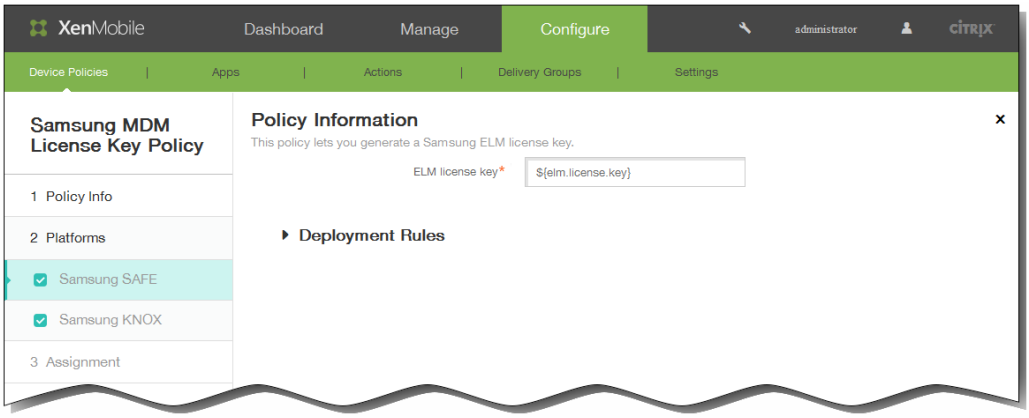


3. ［More］をクリックした後、［Security］の下の［Samsung MDM Licence Key］をクリックします。 ［Samsung MDM Licence Key Policy］情報ページが開きます。



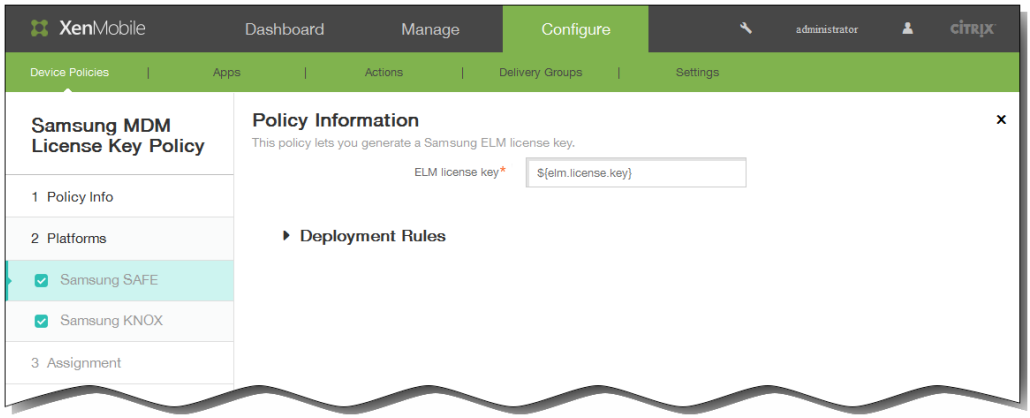
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。

注：［Policy Platforms］ページが開いたときは両方のプラットフォームがオンになっており、最初はSamsung SAFEプラットフォーム構成パネルが開きます。

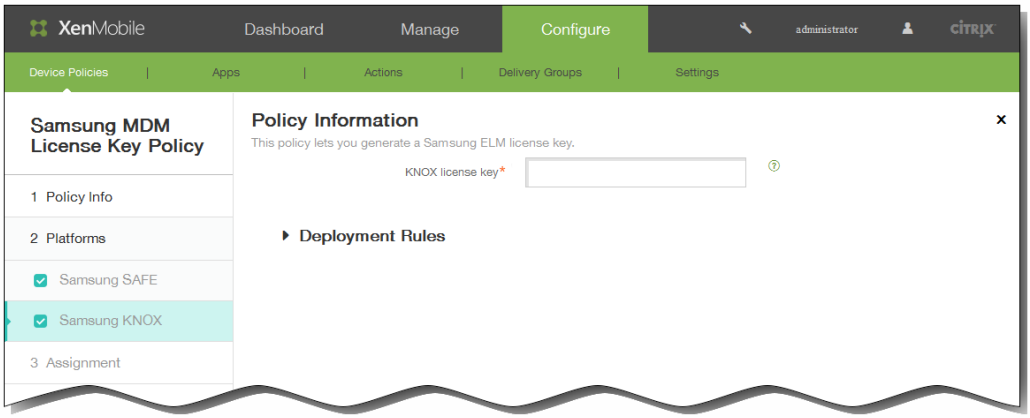


6. ［Platforms］の下で、このポリシーを作成するSamsungプラットフォームをオンにします。 このポリシーに追加しないプラットフォームがオンになっている場合はオフにします。

- Samsung SAFEを選択した場合は、ELMライセンスキーを生成するために［ELM license key］にマクロ「${elm.license.key}」を入力します。このフィールドには既にマクロが入力されています。

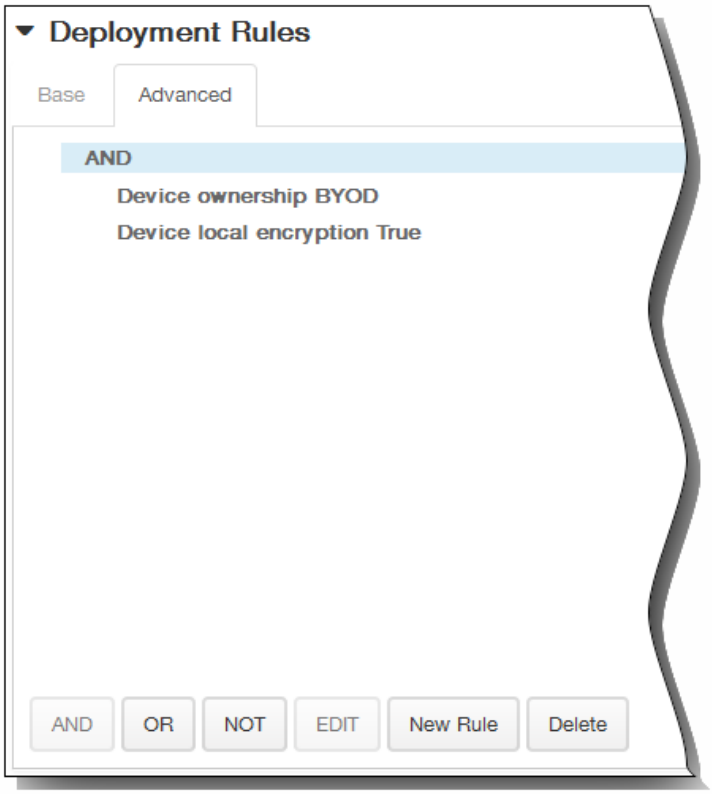


- Samsung KNOXを選択した場合は、［KNOX license key］に25桁のKNOXライセンスキーを入力します。



7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

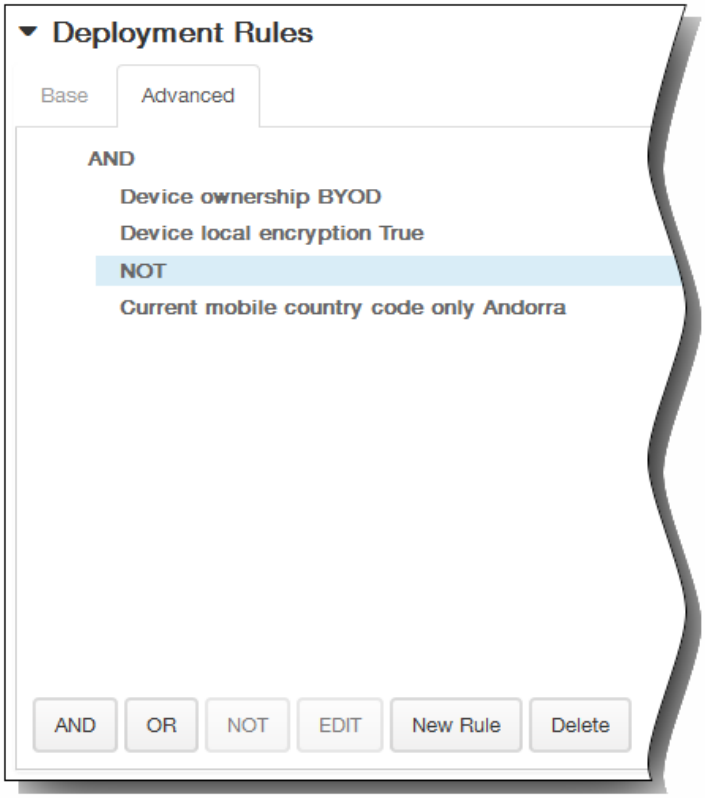


［Base］タブで選択した条件が表示されます。

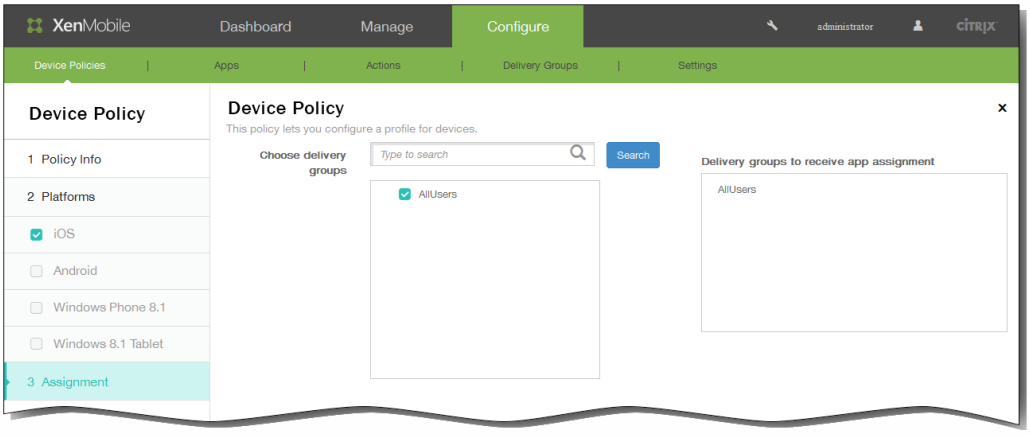
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件

を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Samsung MDM License Key Policy］ページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。

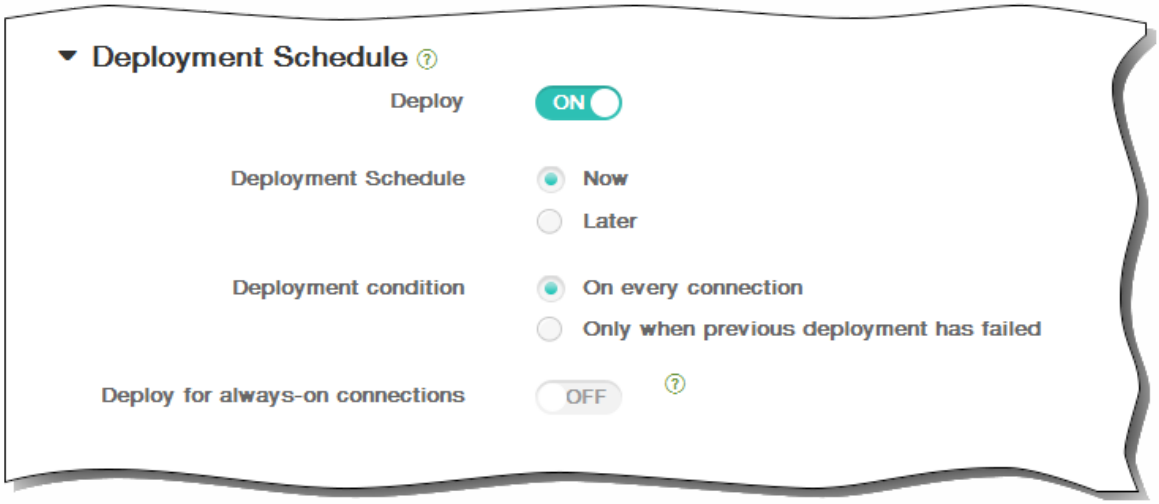


10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はあり

ません。

2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
3. ［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。
4. ［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。
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



11. ［Save］をクリックしてポリシーを保存します。

ストレージ暗号化デバイスポリシー

May 10, 2016

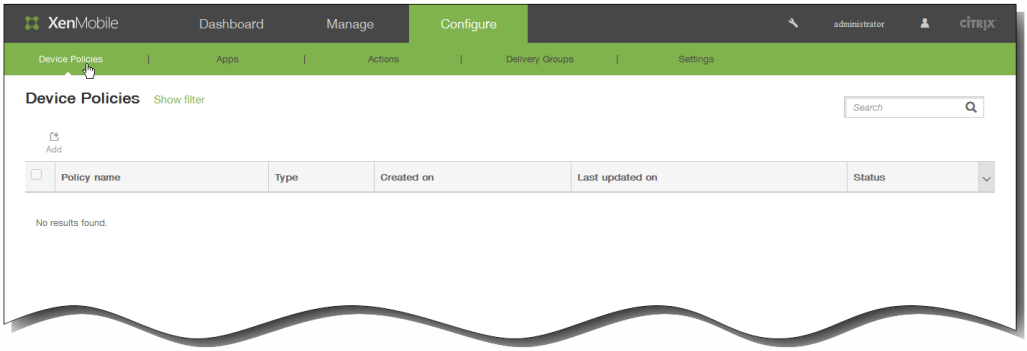
XenMobileでストレージ暗号化デバイスポリシーを作成して、内部ストレージと外部ストレージを暗号化したり、デバイスによっては、ユーザーがデバイスでストレージカードを使用できないようにしたりします。

Samsung SAFE、Windows 8.1タブレット、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、以下の手順で説明しています。

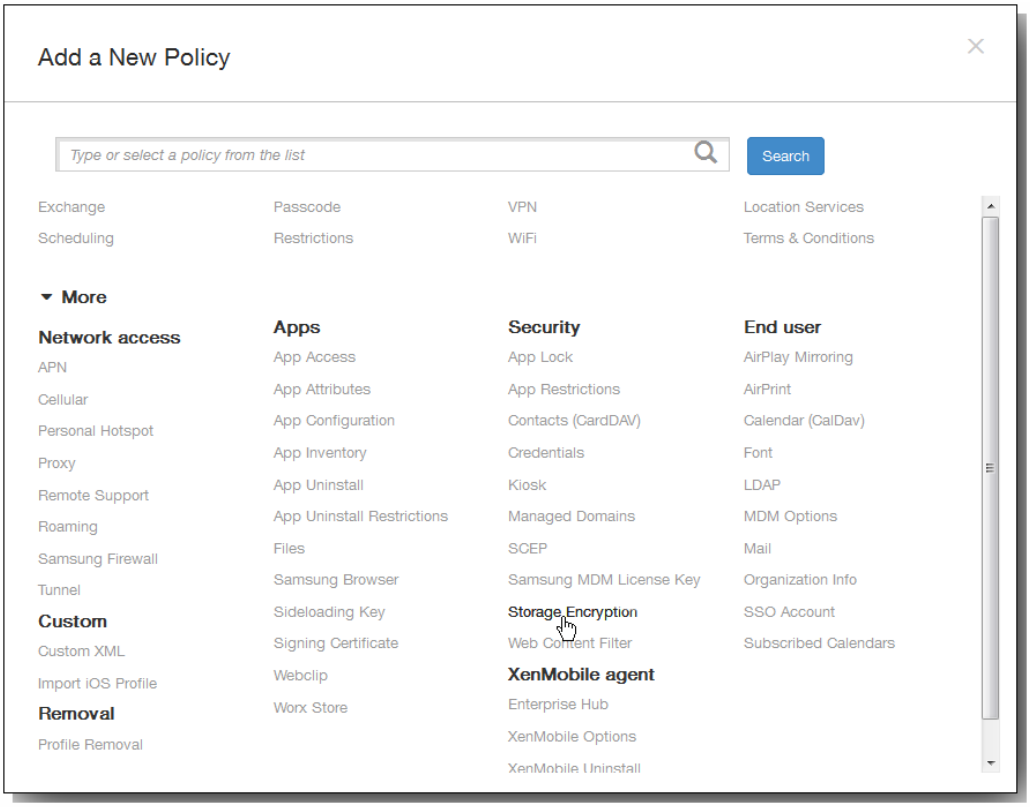
注：Samsung SAFEデバイスの場合は、このポリシーを構成する前に、次の要件が満たされていることを確認します。

- 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。

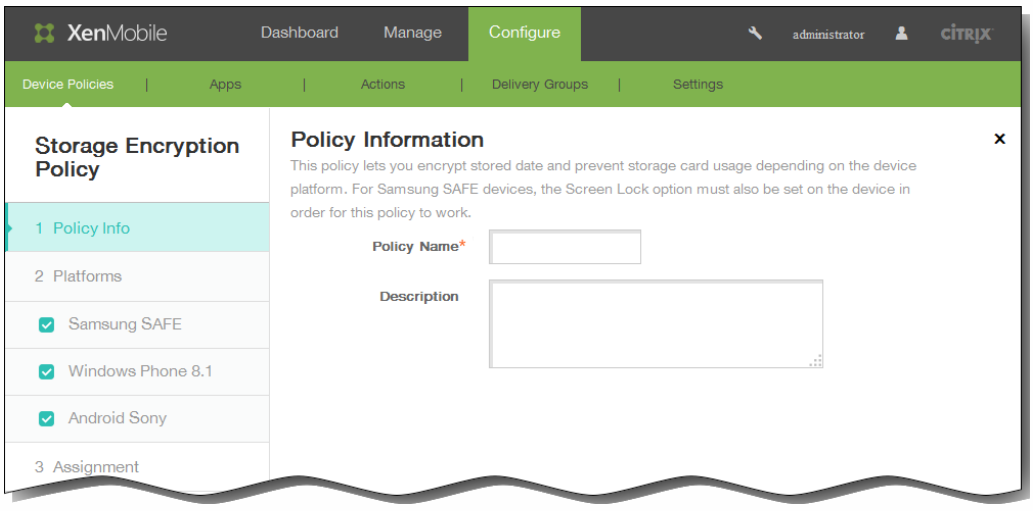
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



2. 新しいポリシーを追加するには［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。



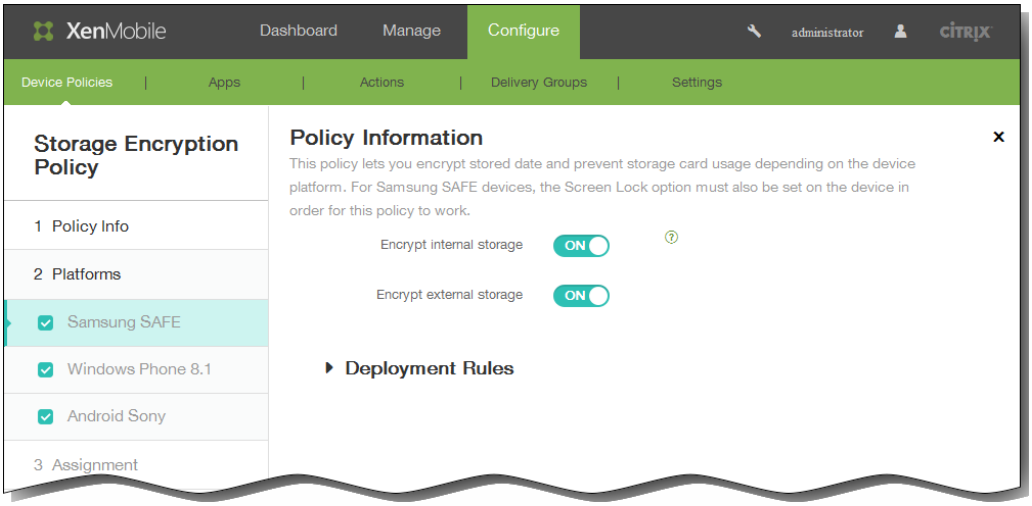
3. ［More］をクリックした後、［Security］の下の［Storage Encryption］をクリックします。 ［Storage Encryption Policy］情報ページが開きます。



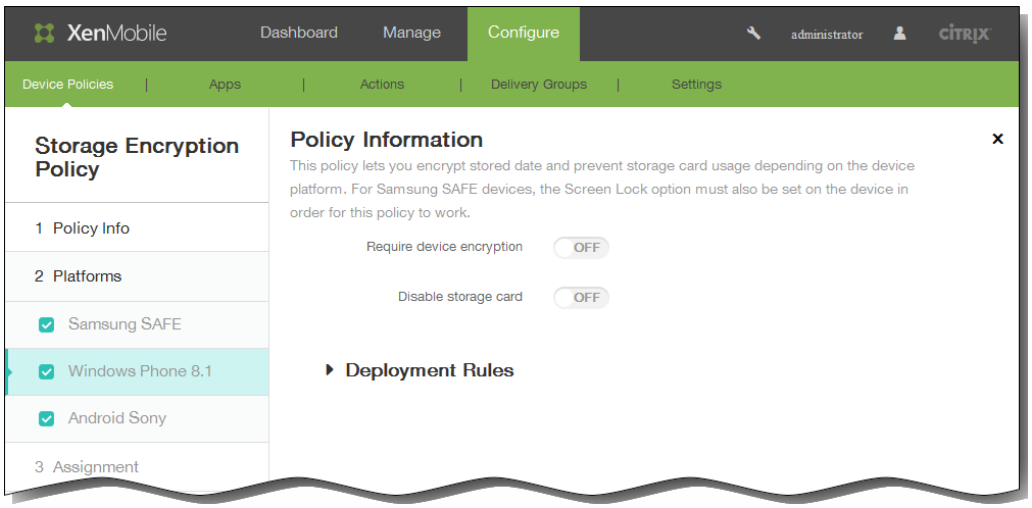
4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときはすべてのプラットフォームがオンになっており、最初はSamsung SAFEプラットフォーム構成パネルが開きます。
6. ［Platforms］の下で、このポリシーを構成するプラットフォームをオンにします。 これが構成する唯一のプラットフォ-

ムである場合は、ほかの選択されているプラットフォームをすべてオフにします。

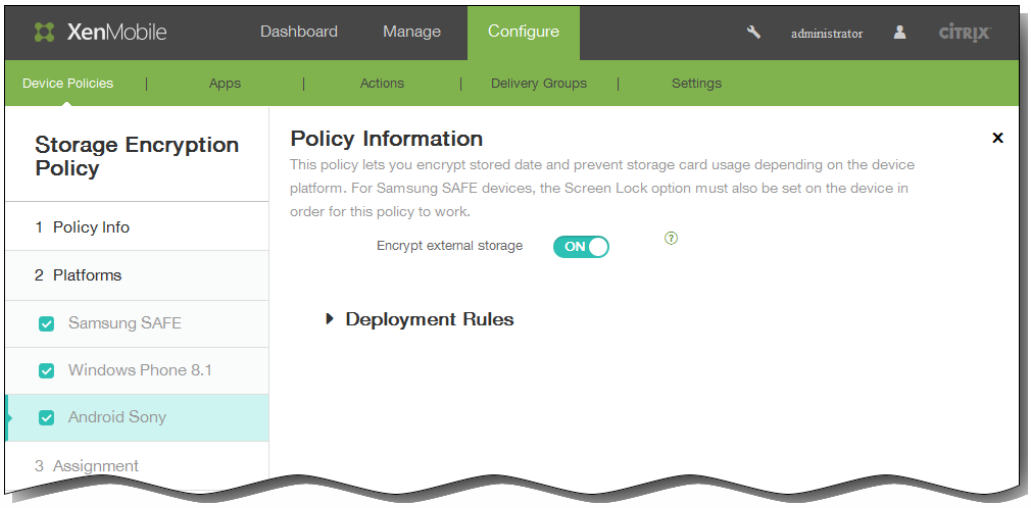
- ［Samsung SAFE］を選択する場合は、次を指定します。
  - Encrypt internal storage：ユーザーのデバイスの内部ストレージを暗号化するかどうかを選択します。内部ストレージには、デバイスのメモリと内部ストレージが含まれます。デフォルトは［ON］です。
  - Encrypt external storage：ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。デフォルトは［ON］です。



- ［Windows Phone 8.1］を選択する場合は、次を指定します。
  - 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。

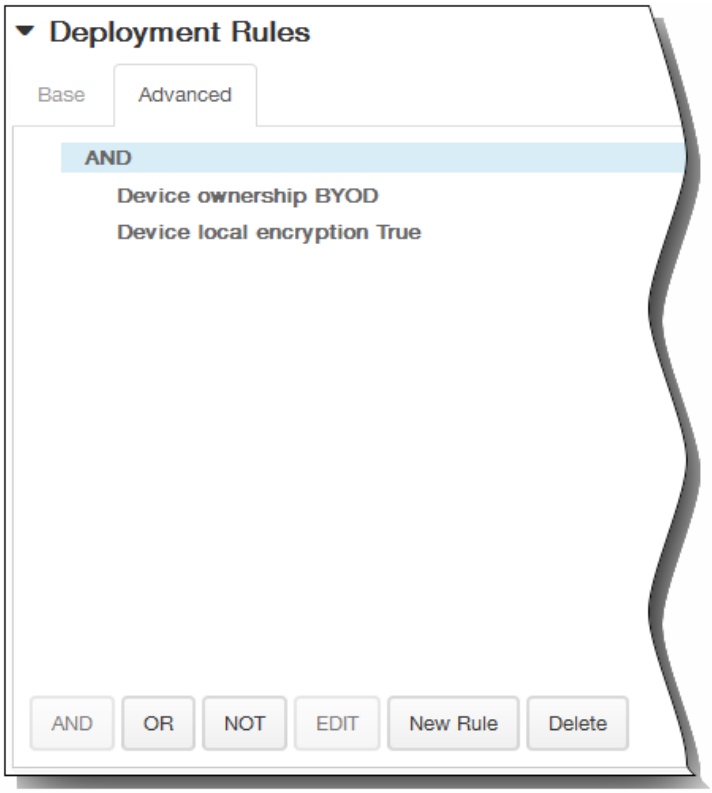


- ［Android Sony］を選択する場合は、［Encrypt external storage］で、ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。デフォルトは［ON］です。



7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

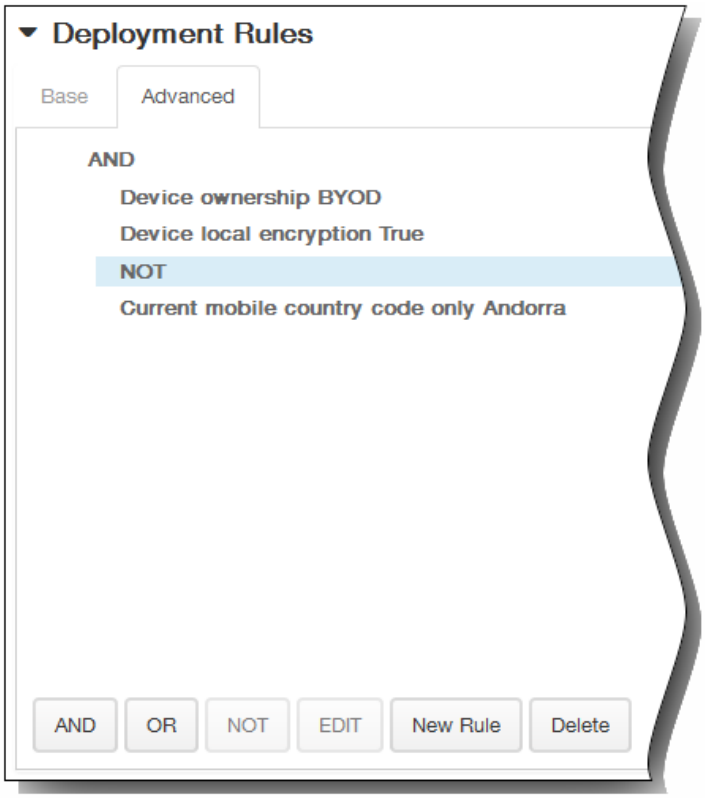
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



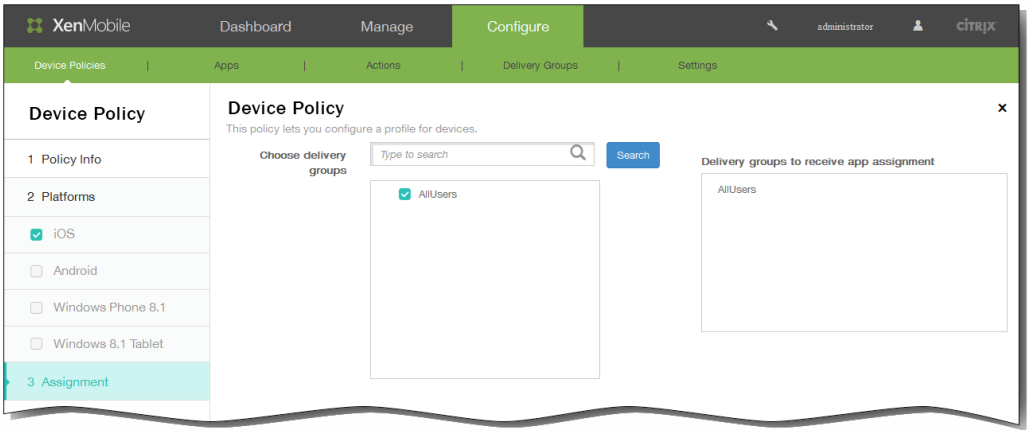
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Storage Encryption Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



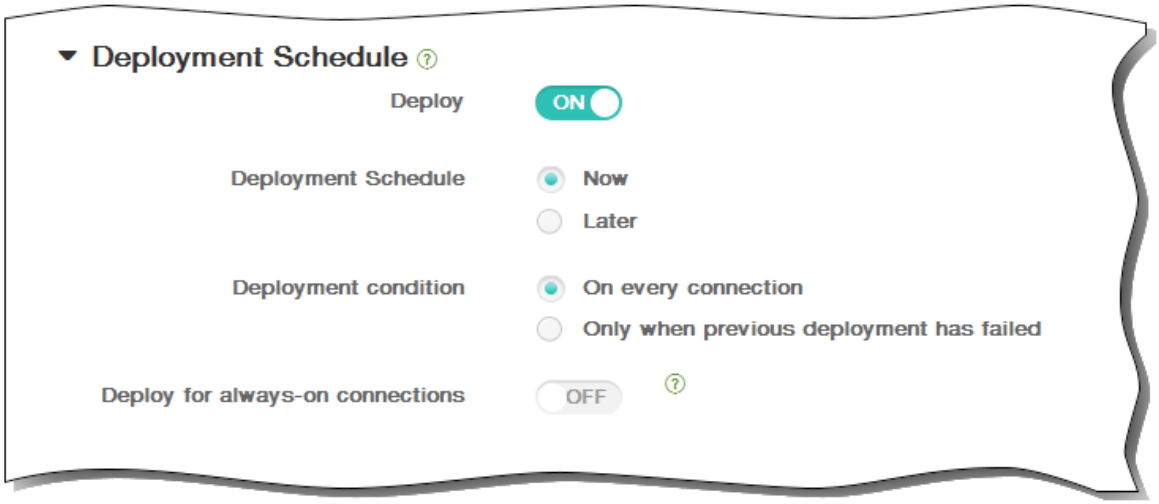
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



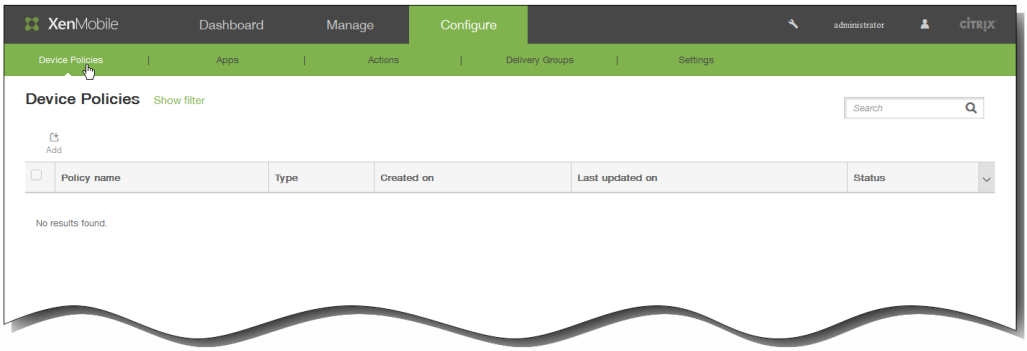
11. ［Save］をクリックしてポリシーを保存します。

iOSのWebコンテンツデバイスポリシーを追加するには

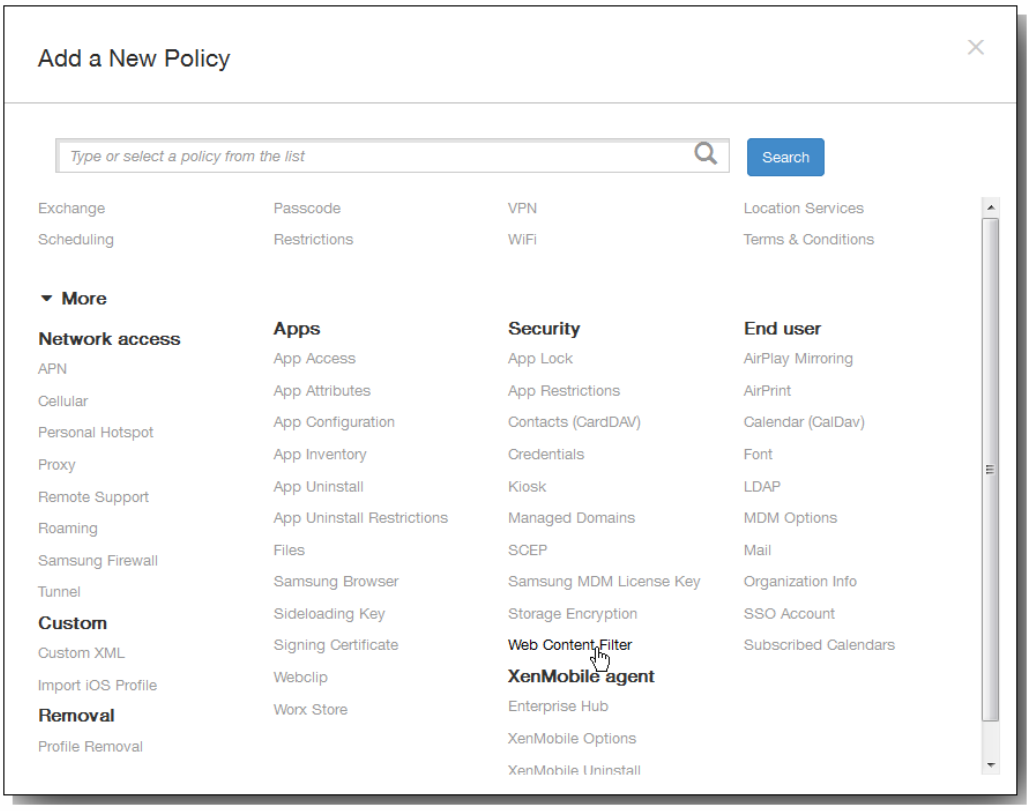
May 10, 2016

XenMobileでデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトとAppleのオートフィルター機能を組み合わせて使用して、iOSデバイスでWebコンテンツをフィルタリングできます。このポリシーはiOS 7.
以降のSupervisedモードのデバイスでのみ使用できます。iOSデバイスをSupervisedモードにする方法について詳しくは、「Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには」を参照してください。

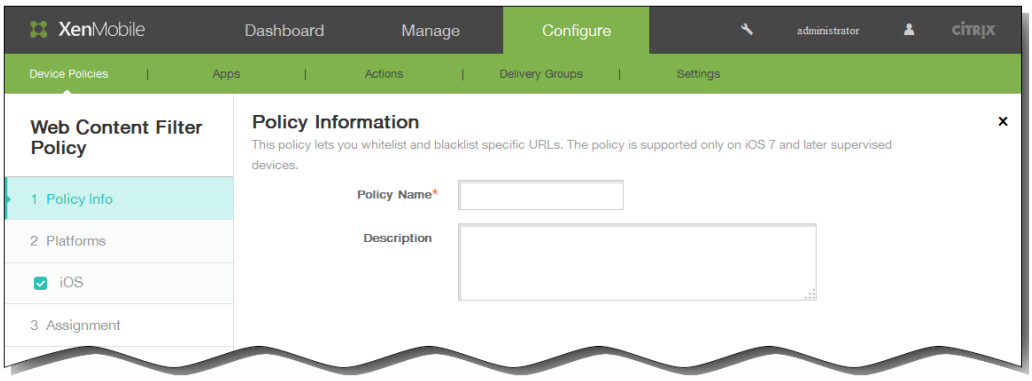
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。 ［Device Policies］ページが開きます。



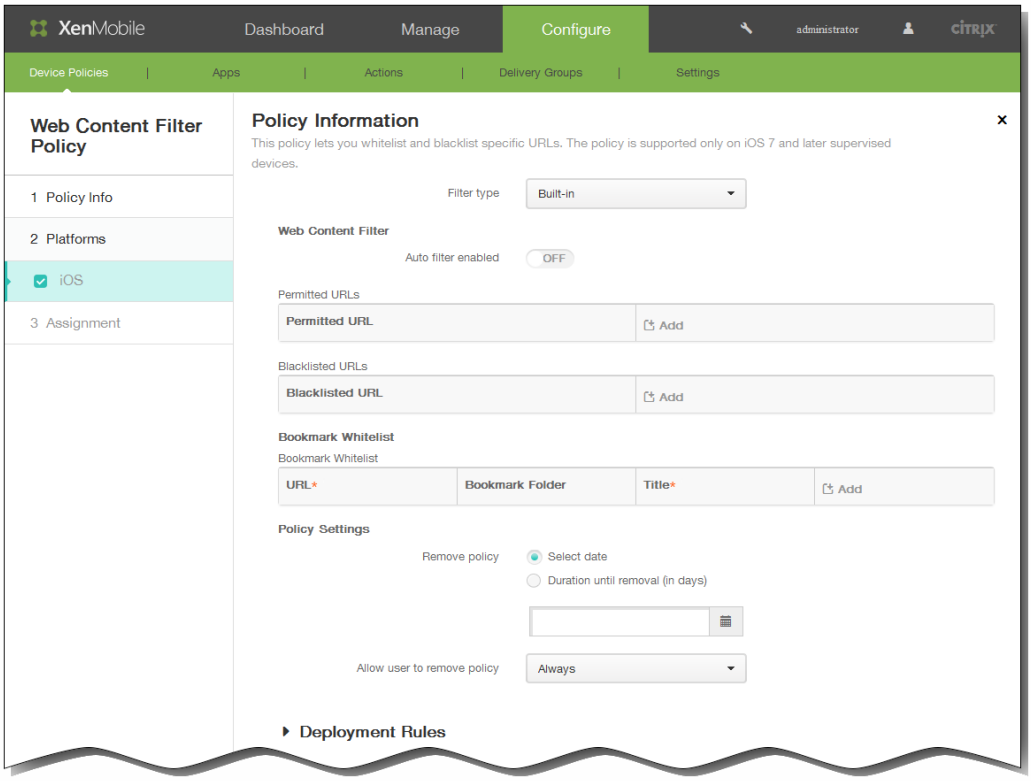
2. 新しいポリシーを追加するには［Add］をクリックします。 ［Add a New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Security］の下の［Web Content Filter］をクリックします。 ［Web Content Filter Policy］ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. 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. ［iOS Platform Information］ページの［Filter type］の一覧から次のいずれかを実行し、選択したオプションに応じて、このトピックの後で説明する手順に従います。
   - フィルターの種類をデフォルトの［Built-in］（組み込み）のままにします。
   - ［Plug-in］を選択して、プラグインのフィルターを構成します。

組み込みのフィルターを構成するには

1. Auto filter enabled：Appleのオートフィルター機能を使用して、Webサイトの不適切なコンテンツを分析するかどうかを選択します。 デフォルトは［OFF］です。
2. Permitted URLs：この一覧は、［Auto filter enabled］が［OFF］に設定されている場合は無視されます。［Auto filter enabled］が［ON］に設定されている場合、この一覧に含まれる項目は、オートフィルターがアクセスを許可しているかどうかにかかわらず常にアクセスできます。
   Webサイトをホワイトリストに追加するには、［Add］をクリックして次の操作を実行します。

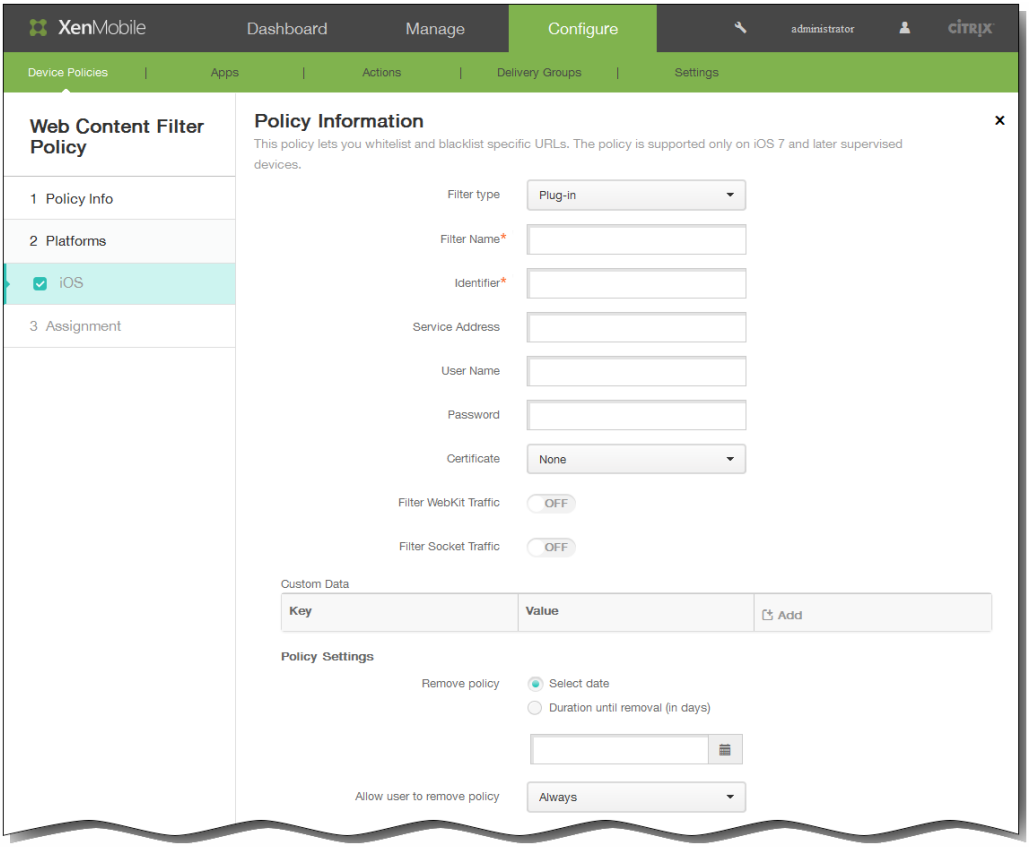
   i. 許可するWebサイトのURLを入力します。Webアドレスの前には、http://またはhttps://を付ける必要があります。
   ii. Webサイトをホワイトリストに保存する場合は［Save］をクリックし、保存しない場合は［Cancel］をクリックします。
   iii. 追加するカスタムキーごとに手順i.およびii.を繰り返します。
3. Blacklisted URLs：この一覧に含まれる項目は常にブロックされます。
   Webサイトをブラックリストに追加するには、［Add］をクリックして次の操作を実行します。

   i. ブロックするWebサイトのURLを入力します。Webアドレスの前には、http://またはhttps://を付ける必要があります。
   ii. Webサイトをブラックリストに保存する場合は［Save］をクリックし、保存しない場合は［Cancel］をクリックします。
   iii. 追加するカスタムキーごとに手順i.およびii.を繰り返します。
4. Bookmark whitelist：ユーザーは、この一覧に含まれるサイトのみにアクセスできます。
   Webサイトをブックマークするには、［Add］をクリックして次の操作を実行します。

   i. URL：ブックマークするWebサイトのURLを入力します。Webアドレスの前には、http://またはhttps://を付ける必要があります。このフィールドは必須です。
   ii. Bookmark folder：任意で、ブックマークフォルダー名を入力します。このフィールドを空白のままにすると、ブックマークはデフォルトのブックマークディレクトリに追加されます。
   iii. Title：Webサイトの説明的なタイトルを入力します。たとえば、http://google.comというURLに対して「Google」と入力します。
   iv. Webサイトをブラックリストに保存する場合は［Save］をクリックし、保存しない場合は［Cancel］をクリックします。
   v. 追加するカスタムキーごとに手順i.～iv.を繰り返します。
   注：既存のWebサイトを削除するには、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Webサイトを編集するには、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。

5. 手順7.を参照して、組み込みフィルターの構成を完了します。

プラグインのフィルターを構成するには



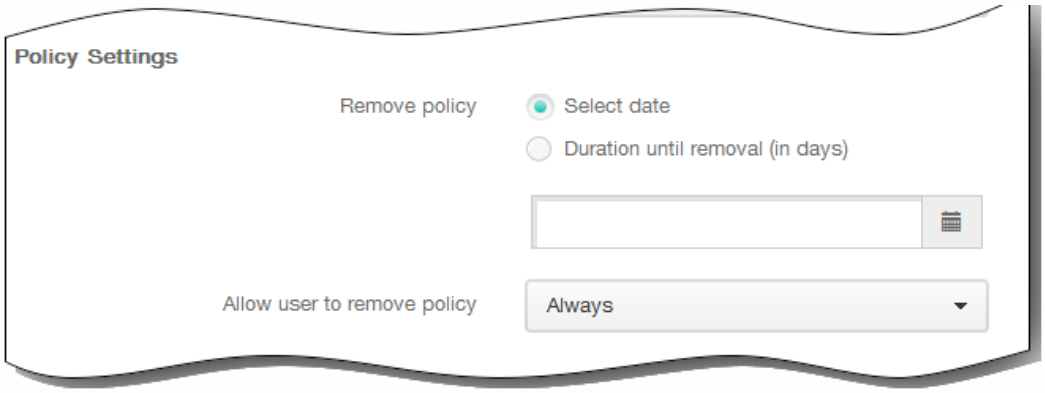
1. Filter name：フィルターの固有の名前を入力します。
2. Identifier：フィルタリングサービスを提供するプラグインのバンドルIDを入力します。
3. Service address：任意で、サーバーアドレスを入力します。 有効な形式は、IPアドレス、ホスト名、またはURLです。
4. User name：任意で、サービスのユーザー名を入力します。
5. Password：任意で、サービスのパスワードを入力します。
6. Certificate：一覧から、オプションとして、サービスでユーザーを認証するために使用するID証明書を選択します。 デフォルトは［None］です。
7. Filter WebKit traffic：WebKitトラフィックをフィルタリングするかどうかを選択します。
8. Filter Socket traffic：ソケットトラフィックをフィルタリングするかどうかを選択します。
9. Custom Data：［Add］をクリックして次の操作を実行し、Webコンテンツフィルターにカスタムデータを追加します。
   1. Key：カスタムキーを入力します。
   2. Value：カスタムキーの値を入力します。
   3. カスタムキーを保存する場合は［Save］をクリックし、保存しない場合は［Cancel］をクリックします。
   4. 追加するカスタムキーごとに手順i.～iii.を繰り返します。

   注：既存の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。

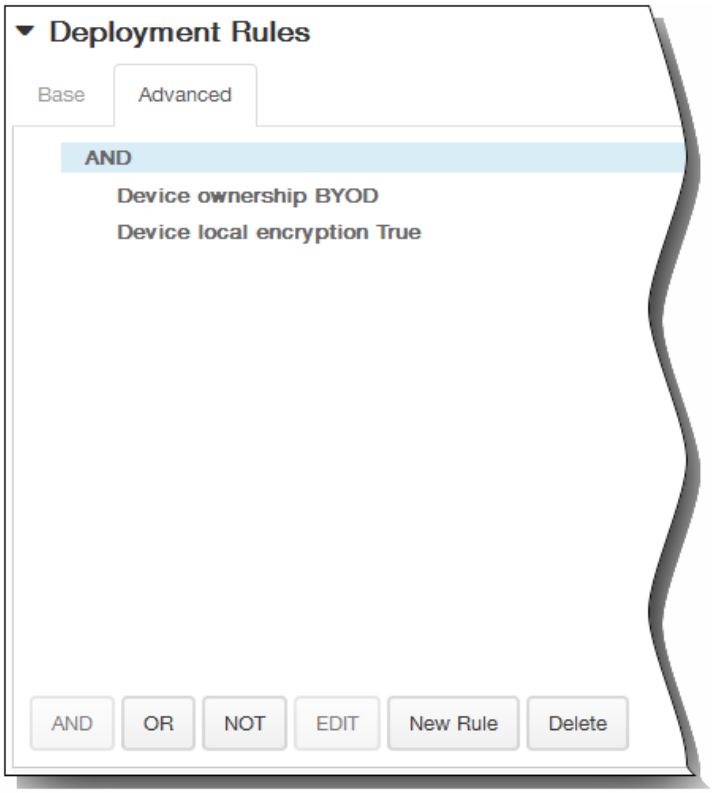
7. ［Policy Settings］の下の［Remove policy］の横にある、［Select date］または［Duration until removal (in days)］をクリックします。

8. ［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。
9. ［Allow user to remove policy］の一覧で、［Always］、［Password required］、［Never］のいずれかを選択します。
10. ［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。



11. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

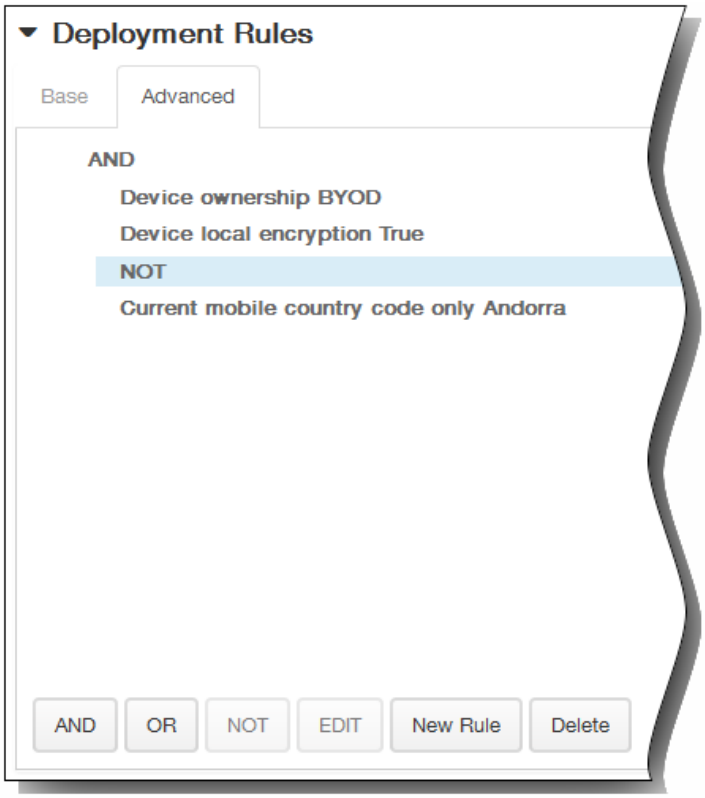
1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
    1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
    2. ［New Rule］をクリックして条件を定義します。
    3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
    4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。



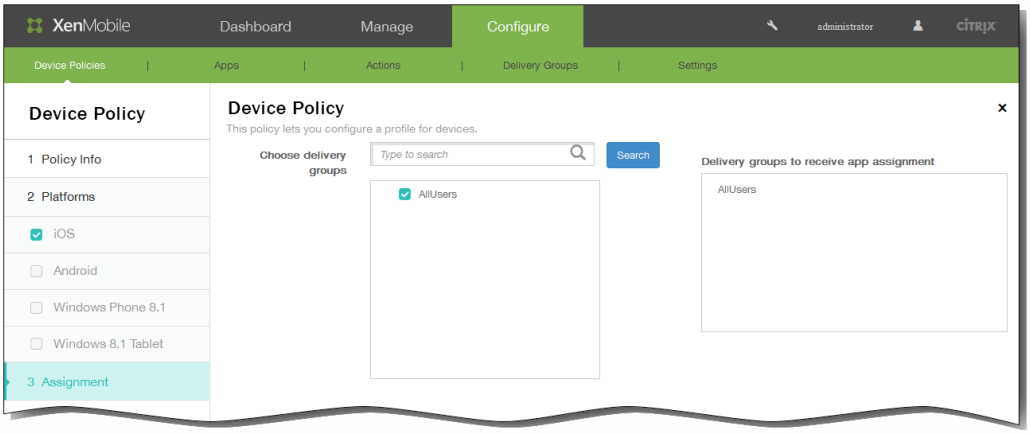
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



12. ［Next］をクリックします。 ［Web Content Filter Policy］割り当てページが開きます。
13. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



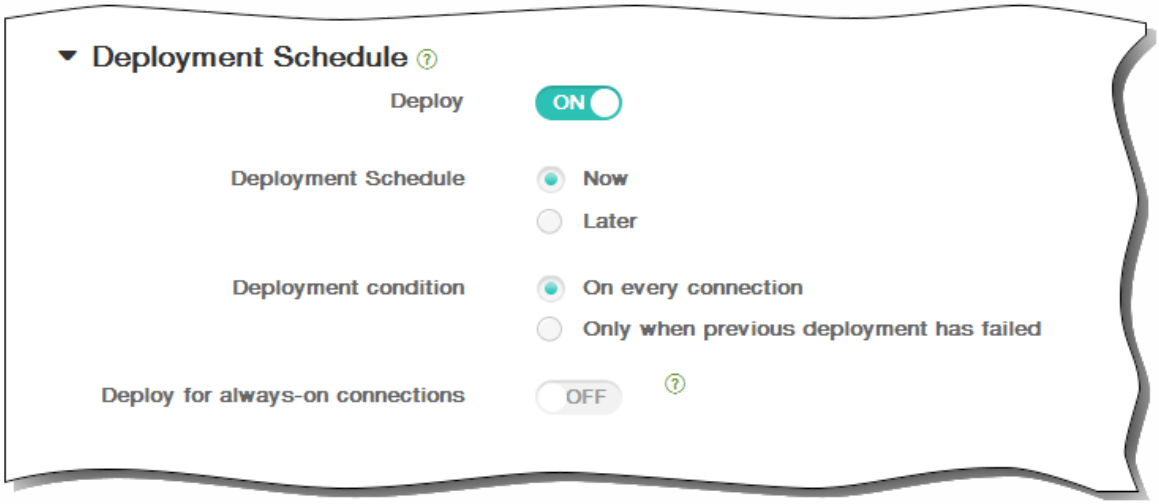
14. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



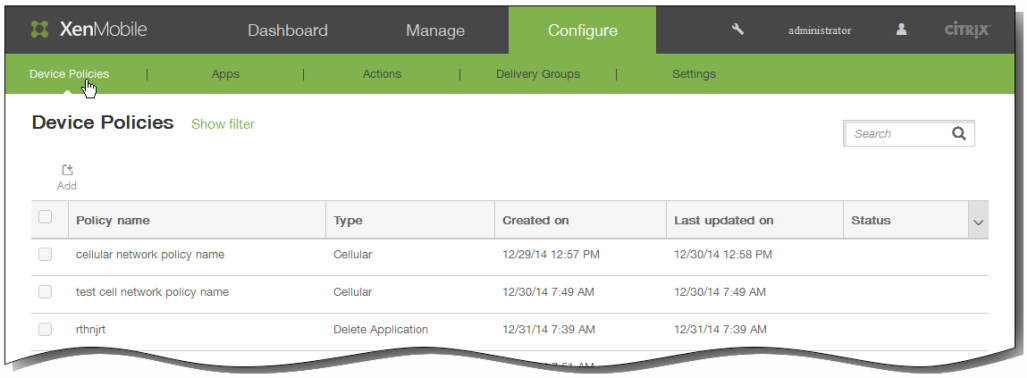
15. ［Save］をクリックしてポリシーを保存します。

Samsungブラウザーデバイスポリシー

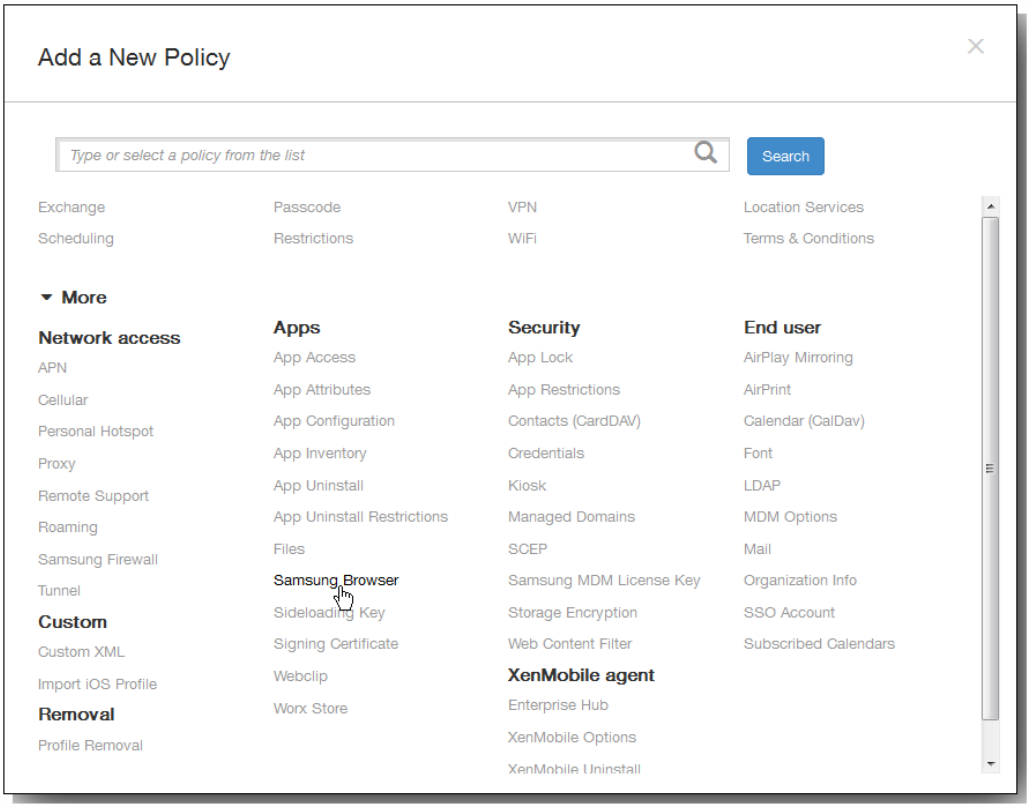
May 10, 2016

Samsung SAFEおよびSamsung KNOXデバイスのSamsungブラウザーデバイスポリシーを作成して、ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、ユーザーのデバイスで使用できるブラウザー機能を制限したりすることができます。ブラウザーを完全に無効にすることや、ポップアップ、JavaScript、Cookie、オートフィル、不正Webサイト警告の適用の有無を有効または無効にすることができます。

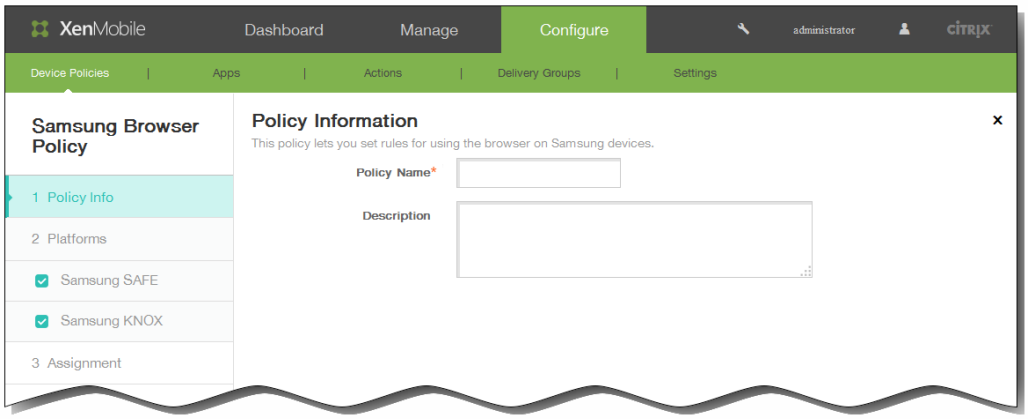
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



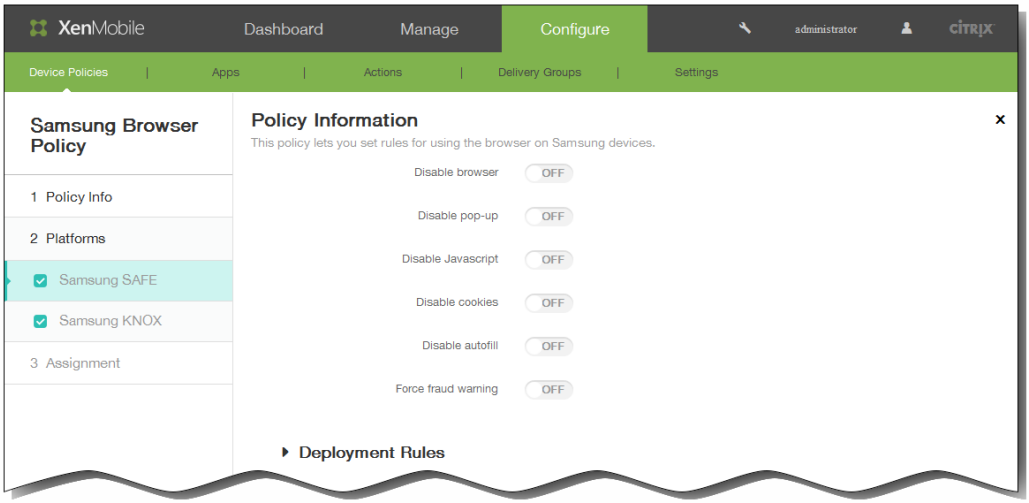
2. 新しいポリシーを追加するには［Add］をクリックします。［Add New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Apps］の下の［Samsung Browser］をクリックします。 ［Samsung Browser Policy］情報ページが開きます。



4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。 ［Policy Platforms］ページが開きます。
   注：［Policy Platforms］ページが開いたときは両方のプラットフォームがオンになっており、最初はSamsung SAFEプラットフォーム構成パネルが開きます。

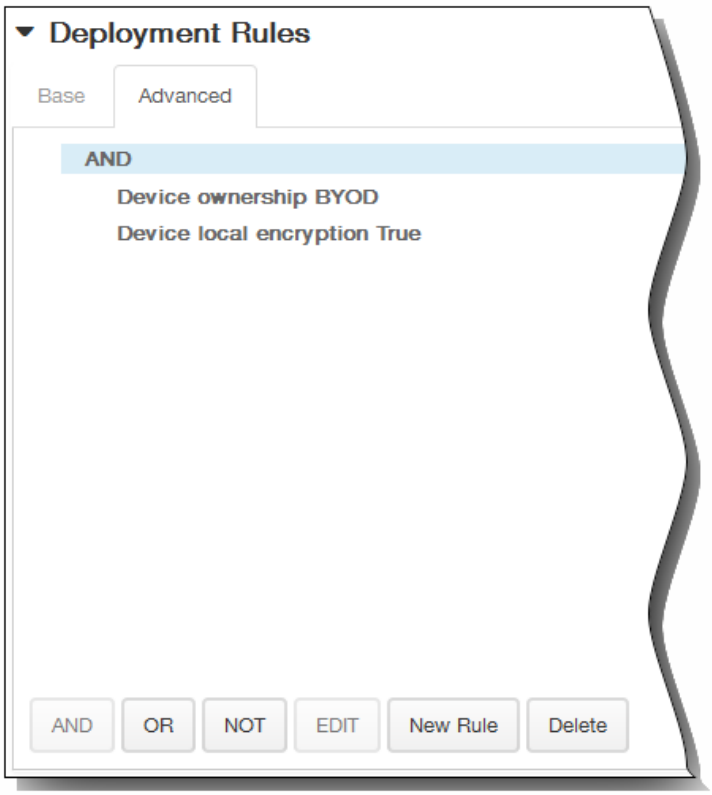


6.
7. ［Platforms］の下で、追加するSamsungプラットフォームをオンにします。 1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにして、次の設定を構成します。
   1. Disable browser：ユーザーのデバイスでSamsungブラウザーを完全に無効にするかどうかを選択します。 デフォルトは［OFF］で、ユーザーはブラウザーを使用できます。 ブラウザーを無効にした場合、以下のオプションは表示されなくなります。
   2. Disable pop-up：ブラウザーでポップアップメッセージを許可するかどうかを選択します。
   3. Disable Javascript：ブラウザーでJavaScriptの実行を許可するかどうかを選択します。
   4. Disable cookies：Cookieを許可するかどうかを選択します。
   5. Disable autofill：ユーザーがブラウザーのオートフィル機能をオンにできるかどうかを選択します。

6. Force fraud warning：ユーザーが不正な、または信頼できないWebサイトを参照したときに、警告メッセージを表示するかどうかを選択します。

8. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

1. 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。
   1. 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［All］です。
   2. ［New Rule］をクリックして条件を定義します。
   3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
   4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
2. ［Advanced］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。

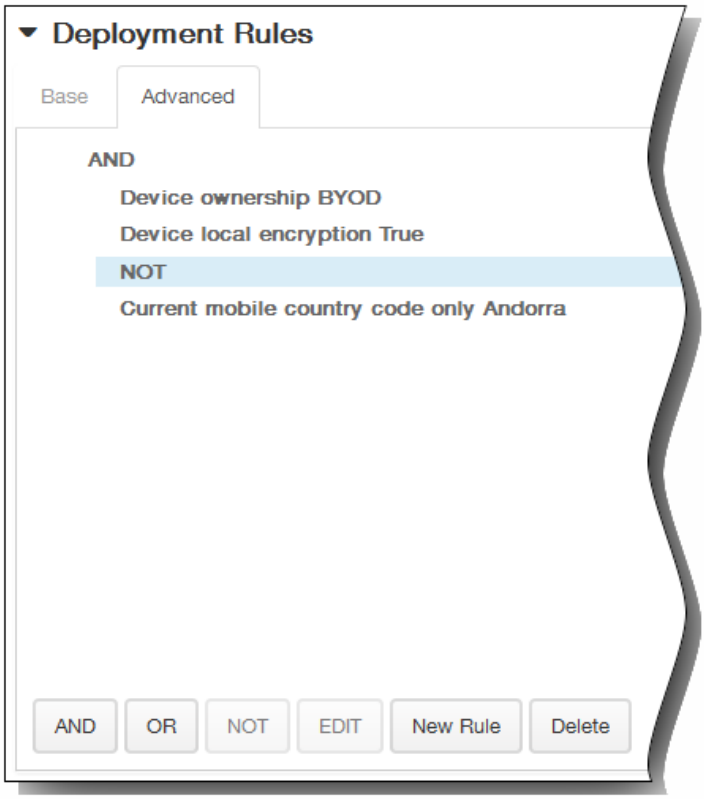


［Base］タブで選択した条件が表示されます。

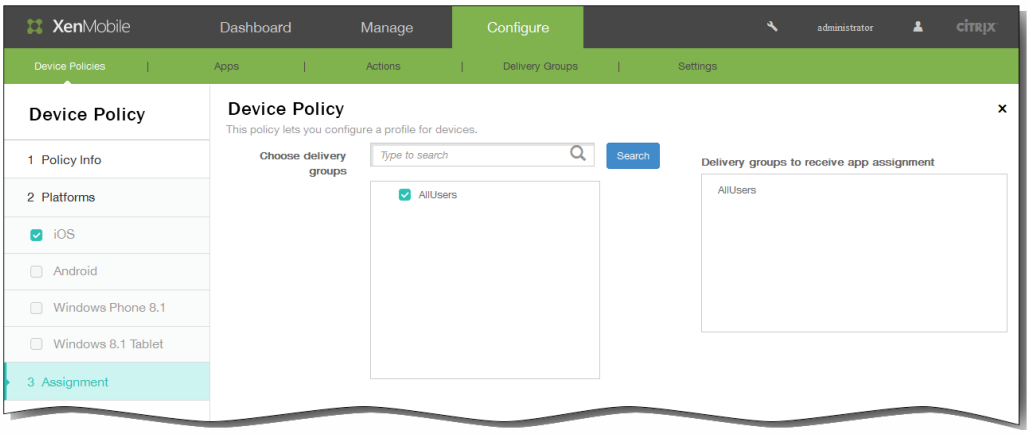
3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。

1. ［AND］、［OR］、または［NOT］をクリックします。
2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
   いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
   この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。

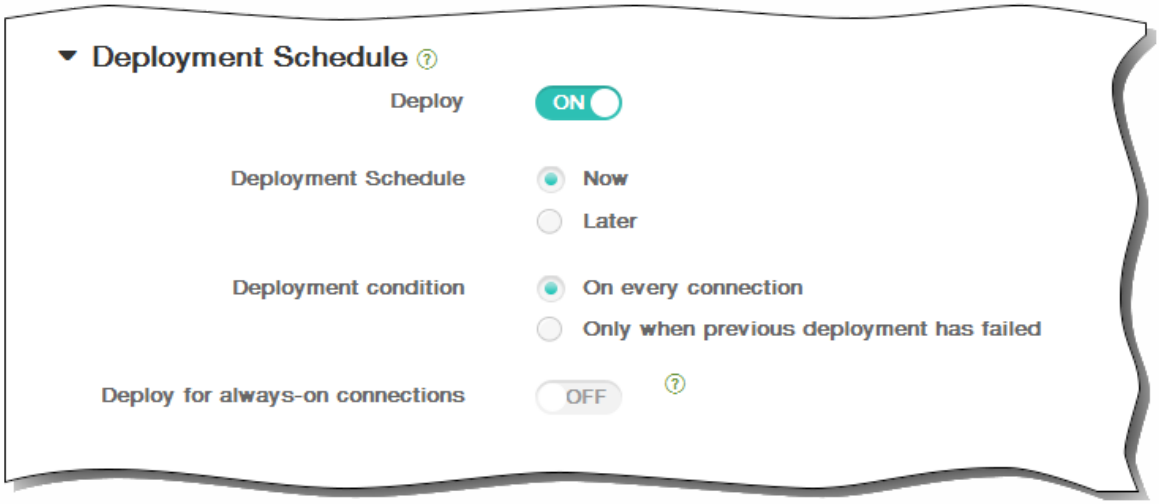


9. ［Next］をクリックします。 ［Samsung Browser Device Policy］ページが開きます。
10. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



11. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［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。
    4. ［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。
    5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。
    注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

    注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。



12. ［Save］をクリックしてポリシーを保存します。

Windows 8.1タブレットのサイドローディングキーデバイスポリシーを追加するには

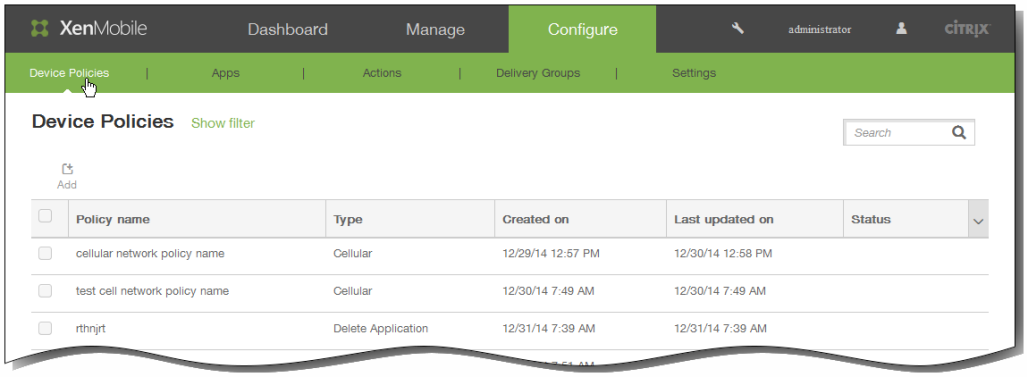
May 10, 2016

XenMobileのサイドローディングにより、Windows Storeから購入していないアプリケーションをWindows 8.1デバイスに展開できます。最もよくある場合として、会社用に開発し、Windowsストアで公開したくないアプリケーションをサイドロードします。アプリケーションをサイドロードするには、サイドローディングキーとキーアクティブ化を構成して、アプリケーションをユーザーのデバイスに展開します。

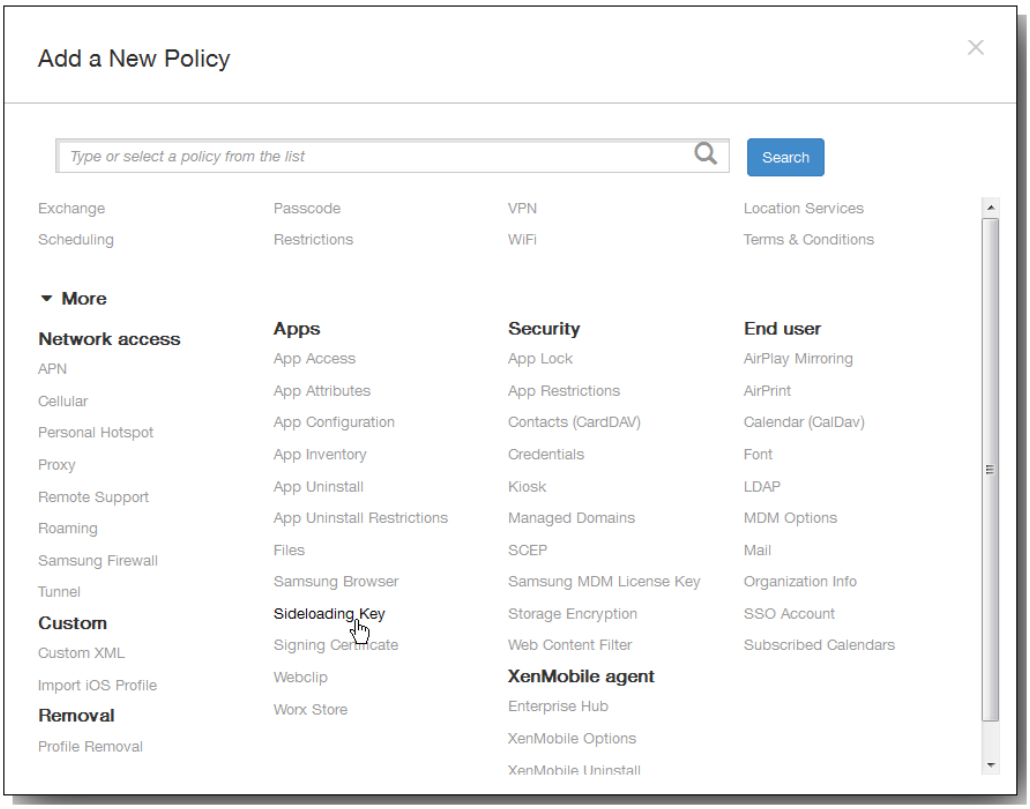
このポリシーを作成する前に以下の情報が必要です。

- サイドローディングプロダクトキー。Microsoftボリュームライセンスサービスセンターにサインインして取得します。
- キーアクティブ化。サイドローディングプロダクトキーを取得した後に、コマンドラインを使用して作成します。

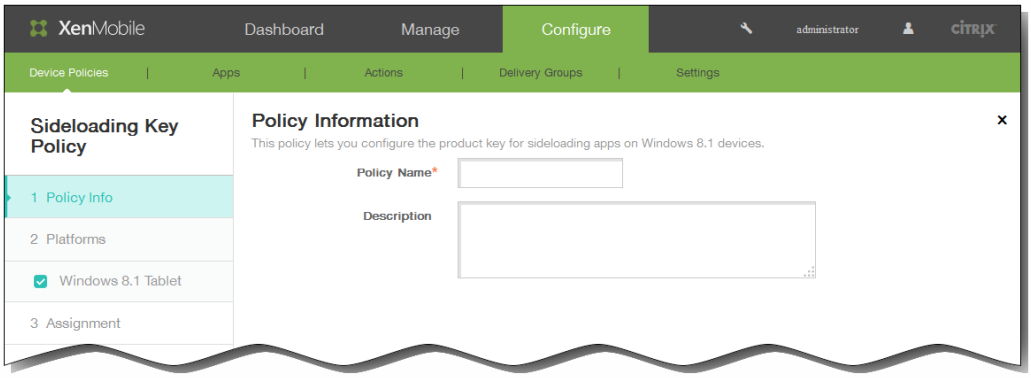
1. XenMobileコンソールで、［Configure］の［Device Policies］をクリックします。［Device Policies］ページが開きます。



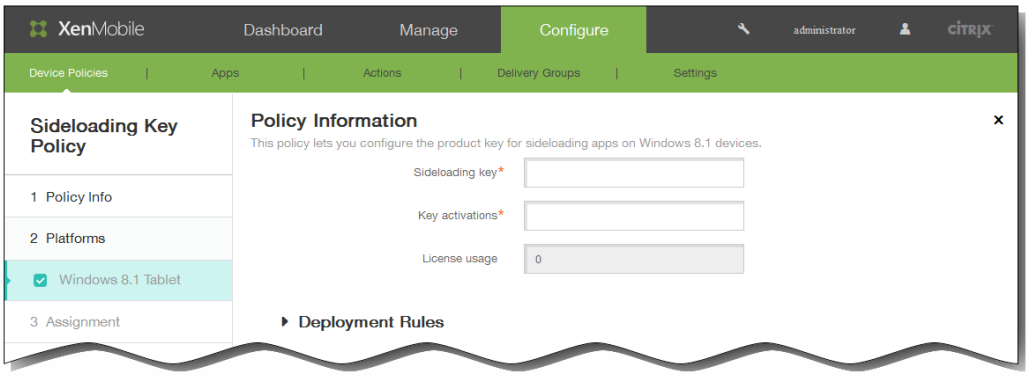
2. ［Add］をクリックします。［Add New Policy］ダイアログボックスが開きます。



3. ［More］をクリックした後、［Apps］の下の［Sideloading Key］をクリックします。 ［Sideloading Key Policy］ページが開きます。

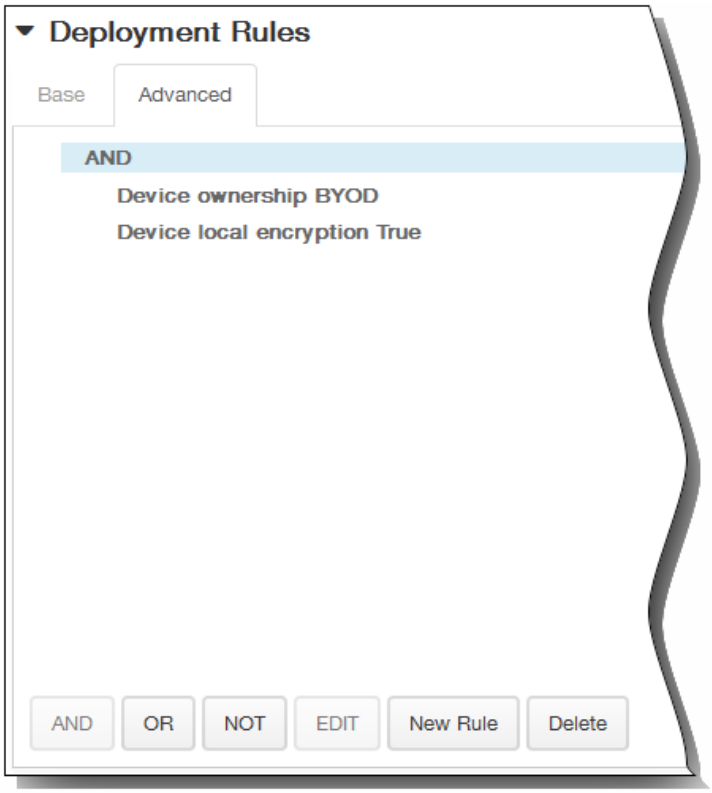


4. ［Policy Information］ペインで、以下の情報を入力します。
   1. Policy Name：ポリシーの説明的な名前を入力します。
   2. Description：任意で、ポリシーの説明を入力します。
5. ［Next］をクリックします。
   ［Windows 8.1 Tablet Platform］情報ページが開きます。



6. 次の設定を構成します。
   1. Sideloading key：Microsoftボリュームライセンスサービスセンターで取得したサイドローディングキーを入力します。
   2. Key activations：サイドローディングキーから作成したキーアクティブ化を入力します。
   3. License usage：この値は、登録されたタブレットの数に基づき、XenMobileによって計算されます。 このフィールドは変更できません。
7. ［Deployment Rules］を展開して以下の設定を構成します。デフォルトでは［Base］タブが表示されます。

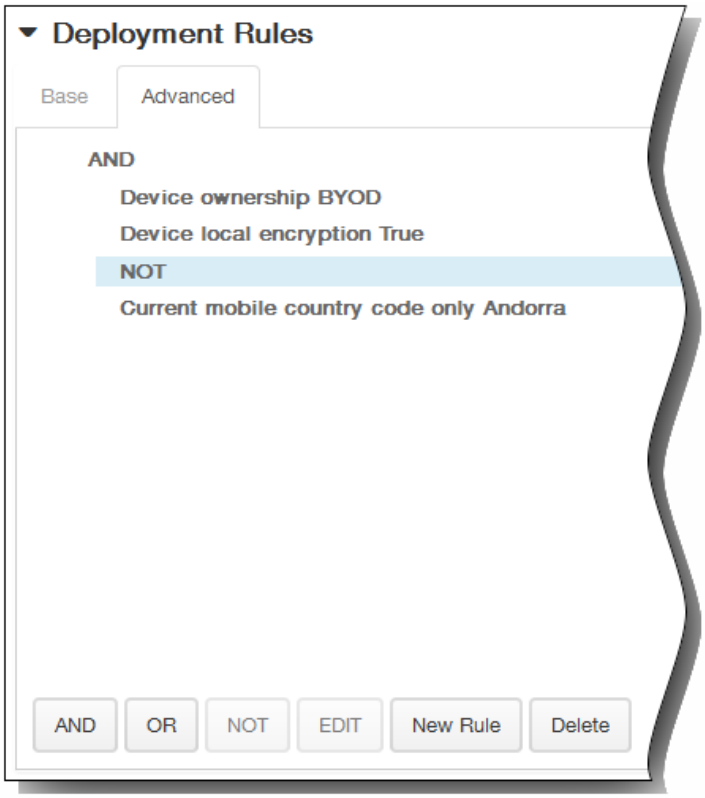
   1. 一覧から、ポリシーをいつ展開するかを決定するオプションを選択します。
      1. すべての条件が満たされたときにポリシーを展開するか、いずれかの条件が満たされたときにポリシーを展開するかを選択できます。デフォルトのオプションは［All］です。
      2. ［New Rule］をクリックして条件を定義します。
      3. 前述の図に示されているように、一覧から［Device ownership］や［BYOD］などの条件を選択します。
      4. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。必要なだけいくつでも条件を追加できます。
   2. ［Advanced］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。



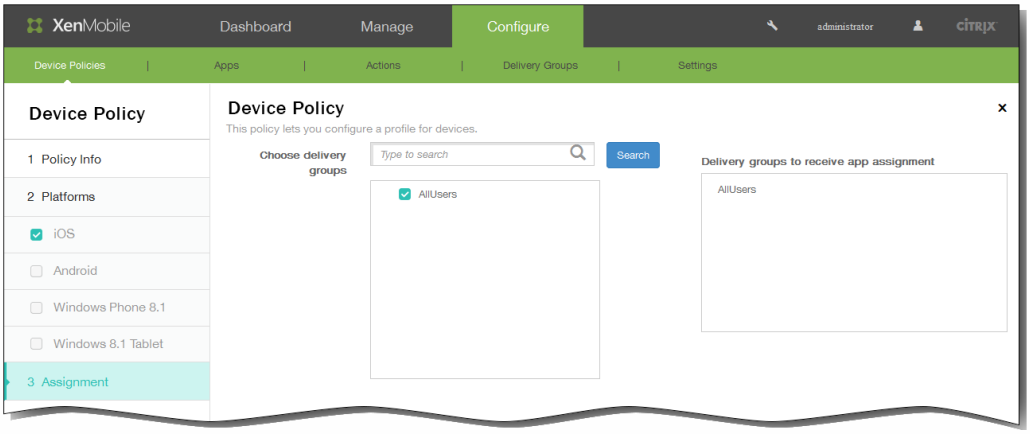
［Base］タブで選択した条件が表示されます。

3. さらに高度なブール値ロジックを使用して、規則を組み合わせたり、編集したり、追加したりすることができます。
   1. ［AND］、［OR］、または［NOT］をクリックします。
   2. 表示される一覧で、規則に追加する条件を選択して右側のプラス記号（+）をクリックすると、その条件が規則に追加されます。
      いつでも、条件をクリックして選択し、［EDIT］をクリックして条件を変更したり、［Delete］をクリックして条件を削除したりすることができます。

   3. 条件をさらに追加する場合は、［New Rule］をもう一度クリックします。
      この例では、デバイスの所有権がBYOD、デバイスのローカル暗号化がTrueであり、デバイスのモバイル国コードをAndorraのみにすることができません。



8. ［Next］をクリックします。 ［Sideloading Key Policy］割り当てページが開きます。
9. ［Choose delivery groups］の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。 選択したグループが右側の［Delivery groups to receive app assignment］一覧に表示されます。



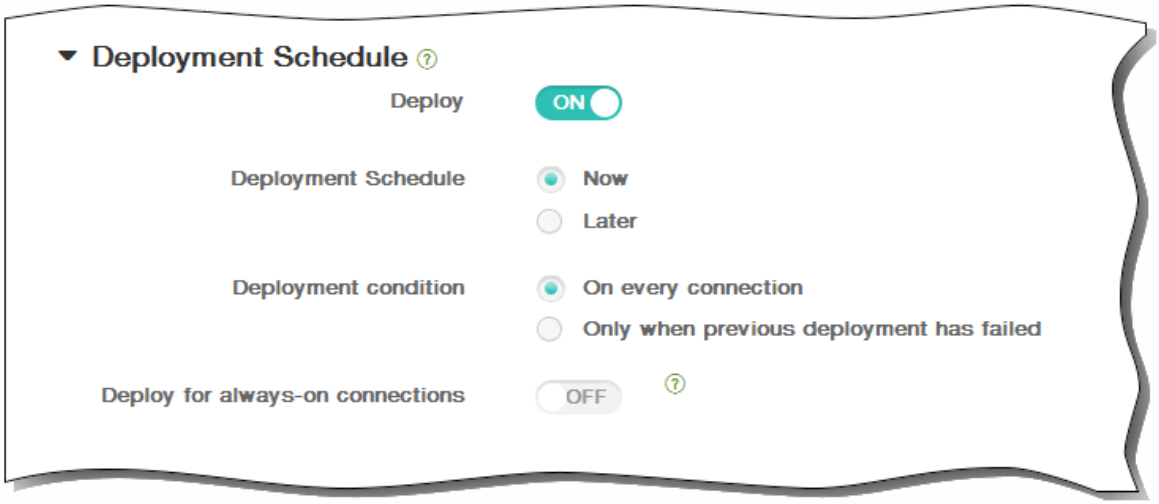
10. ［Deployment Schedule］を展開して以下の設定を構成します。
    1. ［Deploy］の横の［ON］をクリックすると展開がスケジュールされ、［OFF］をクリックすると展開が行われません。 デフォルトのオプションは［ON］です。 ［OFF］を選択した場合、そのほかのオプションを構成する必要はありません。
    2. ［Deployment schedule］の横の［Now］または［Later］をクリックします。 デフォルトのオプションは［Now］です。
    3. ［Later］をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
    4. ［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。

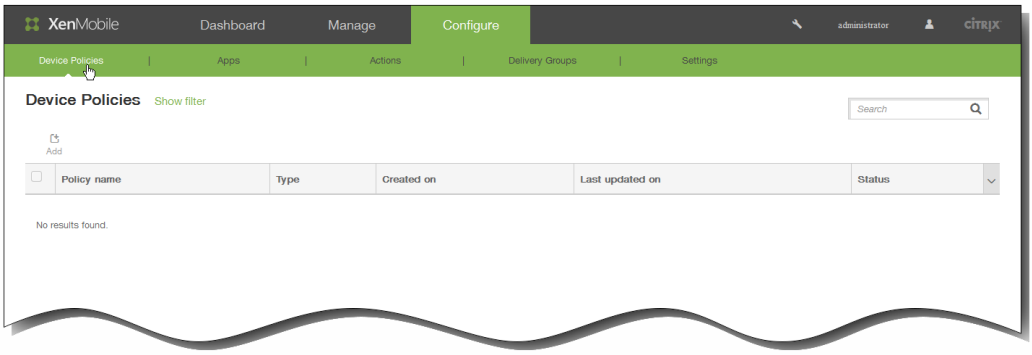
5. ［Deploy for always-on connection］の横の［ON］または［OFF］をクリックします。 デフォルトのオプションは［OFF］です。

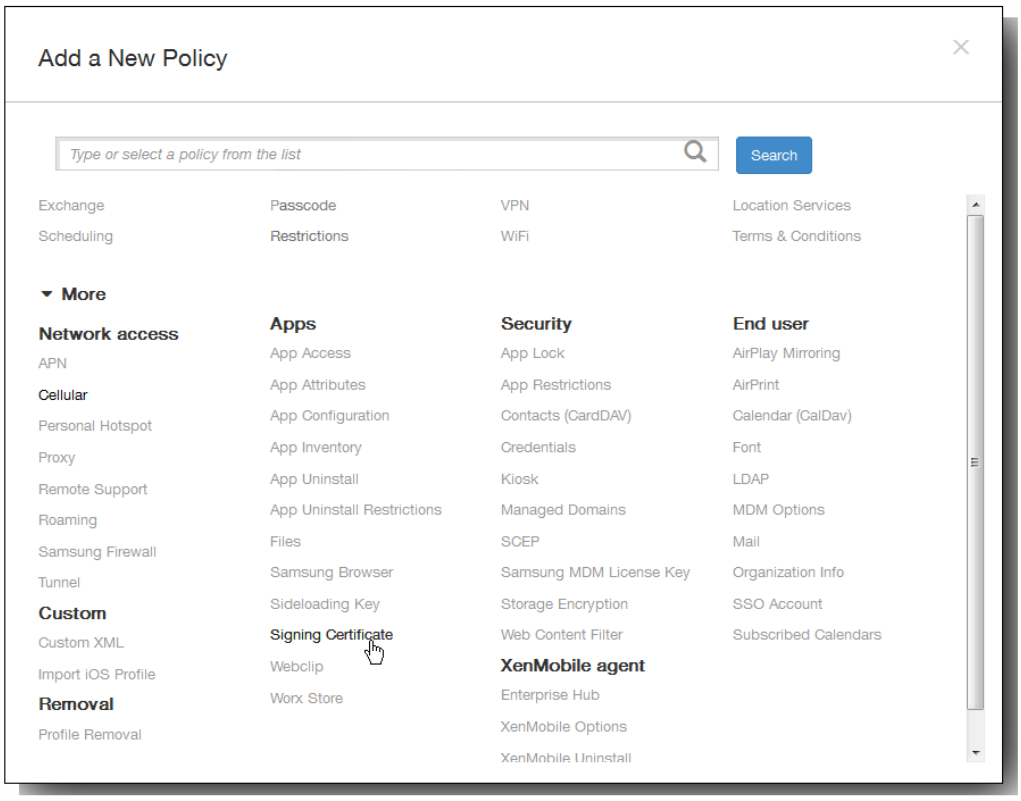
   注：このオプションは、［Settings］の［Server Properties］において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

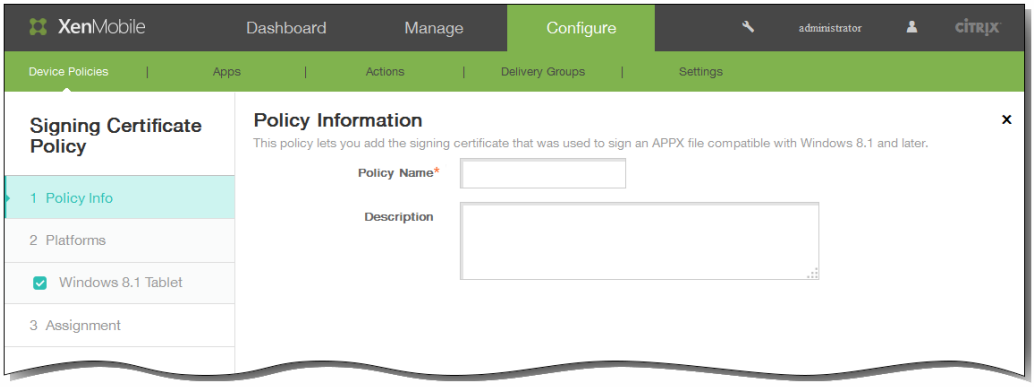
注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、［Deploy for always on connection］は適用されません。

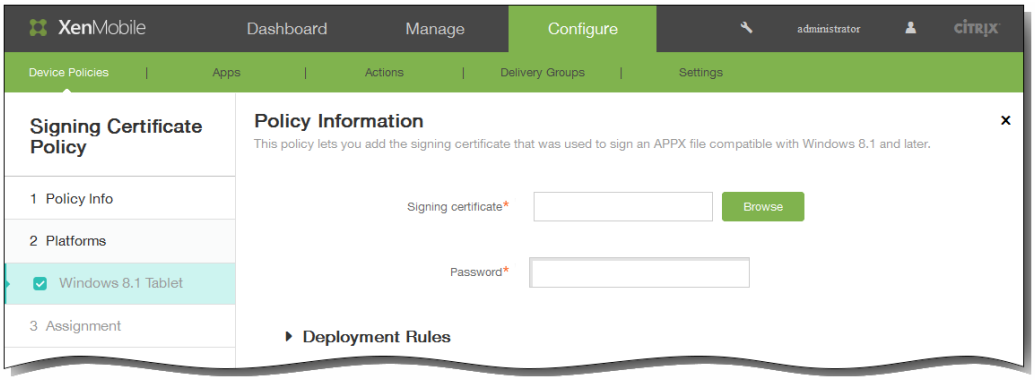


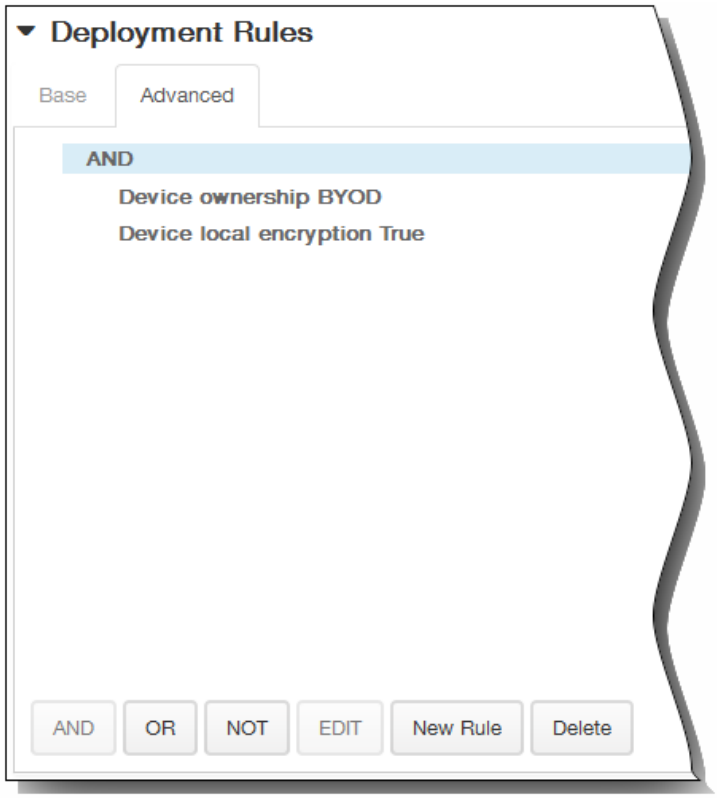
Windows 8.1タブレットの署名証明書デバイスポリシーを追加するには

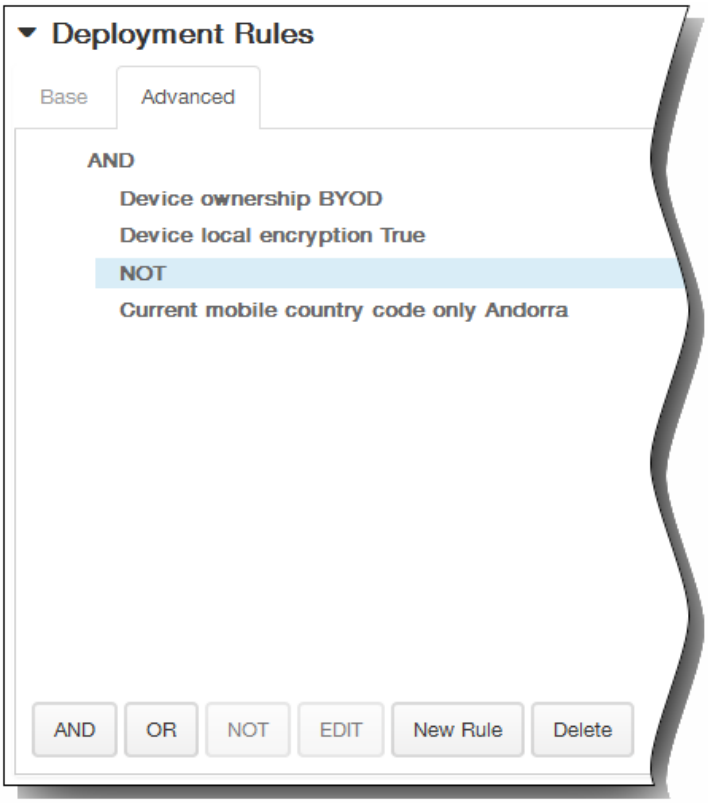


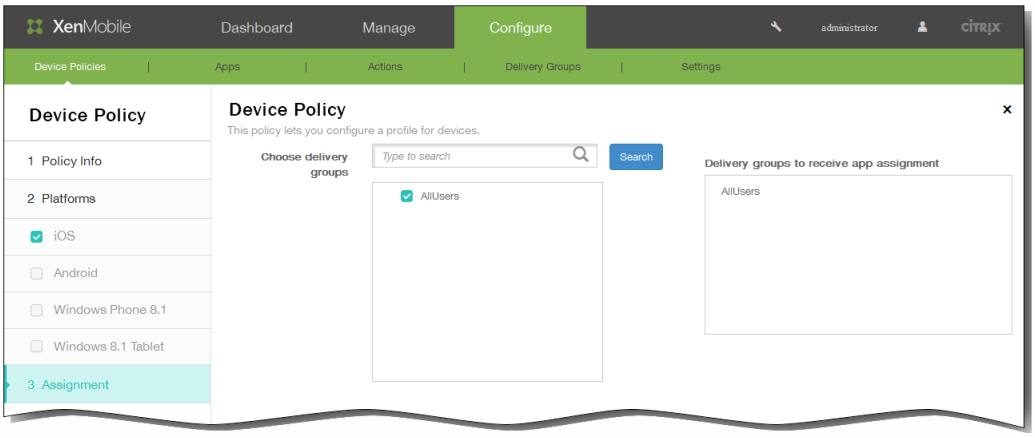


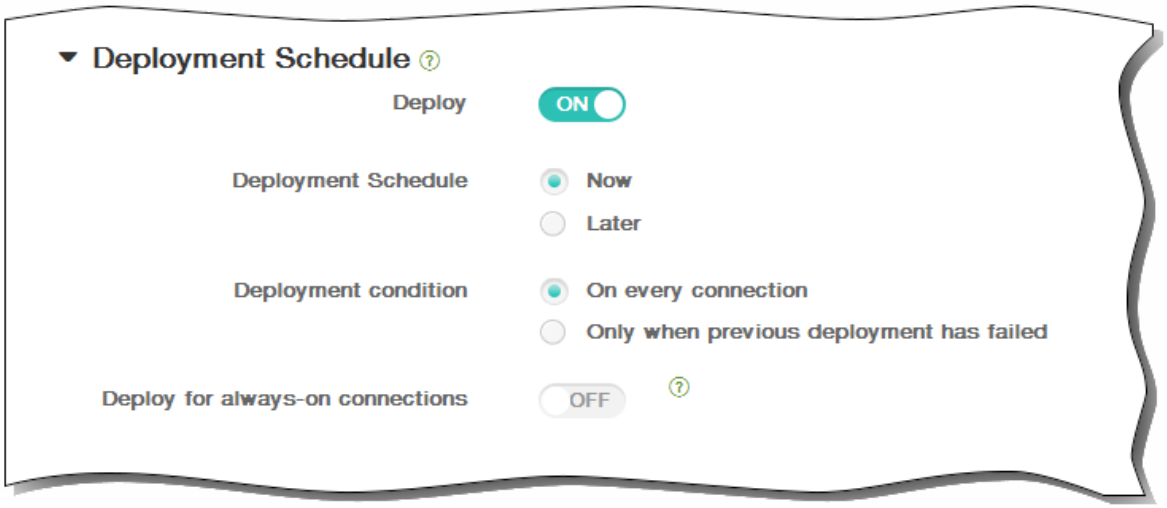




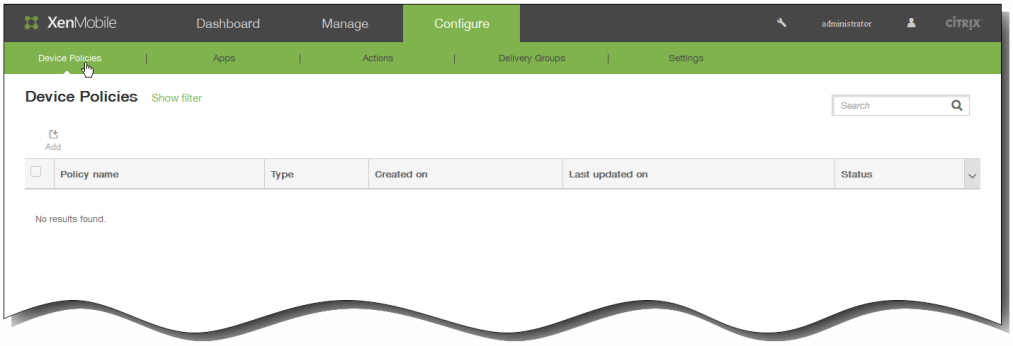


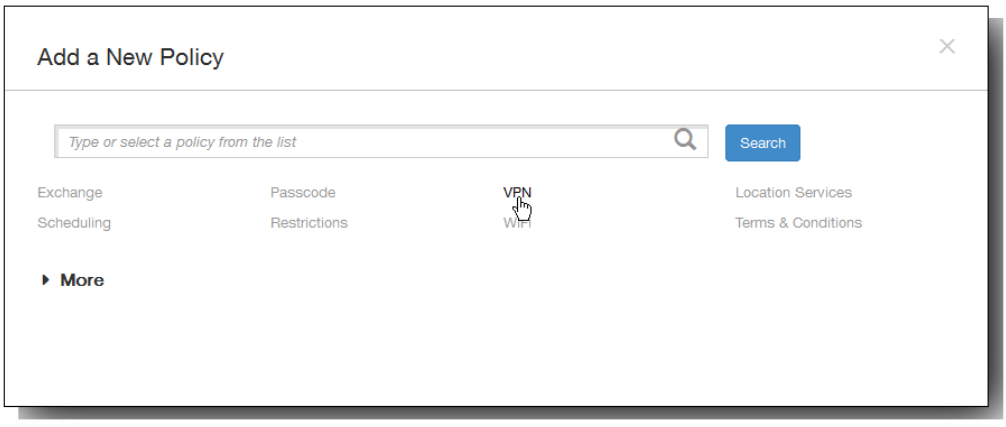


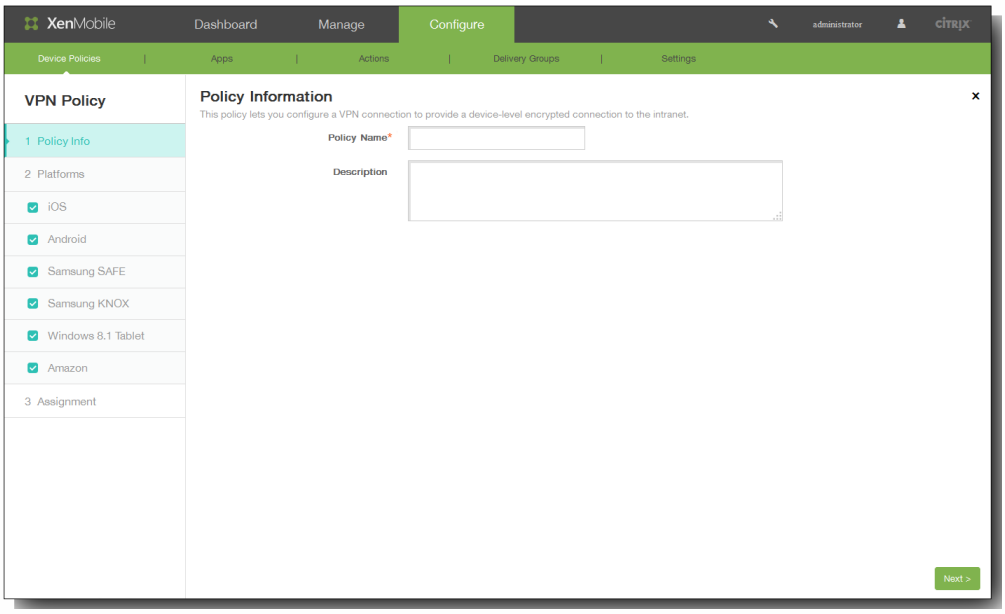


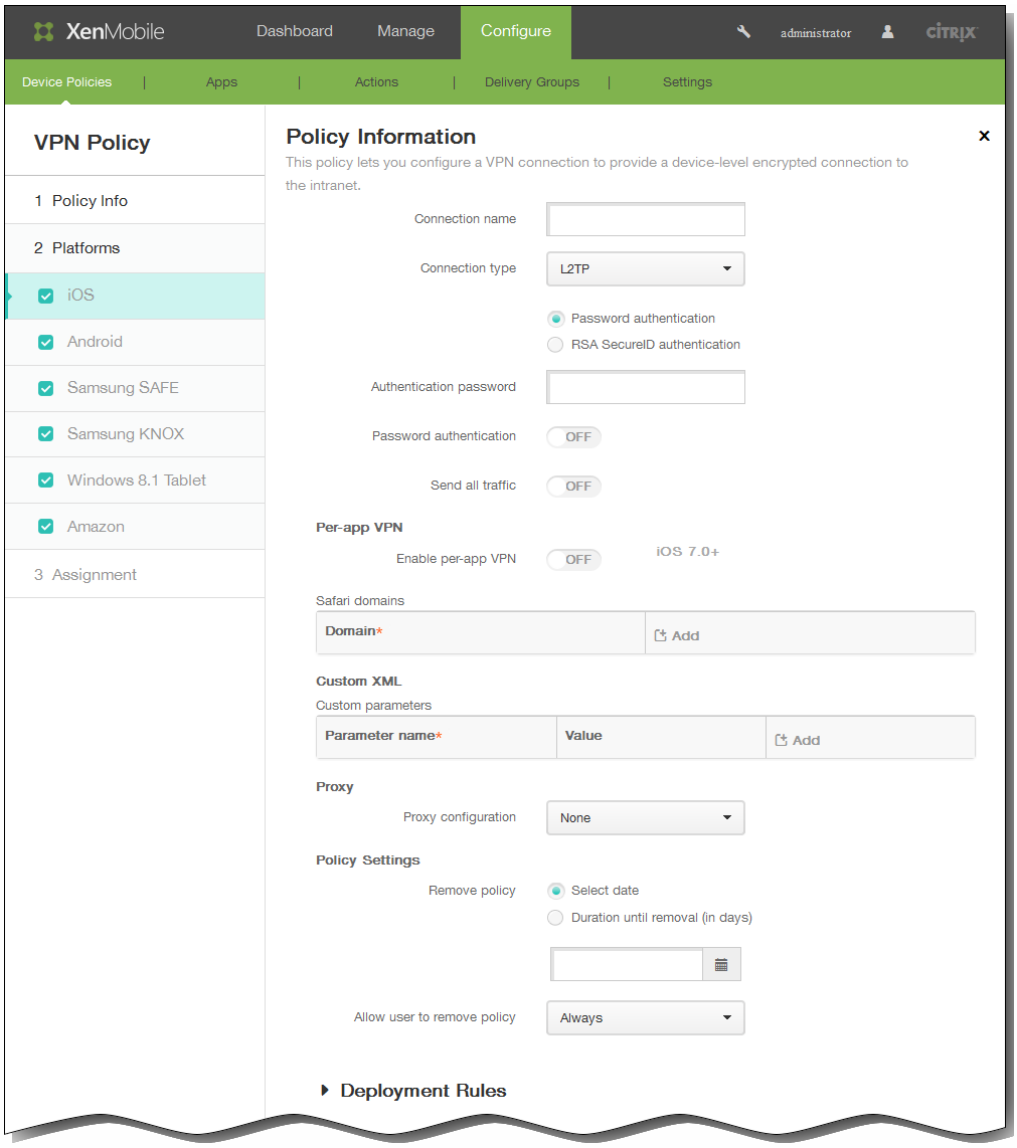


VPNデバイスポリシー

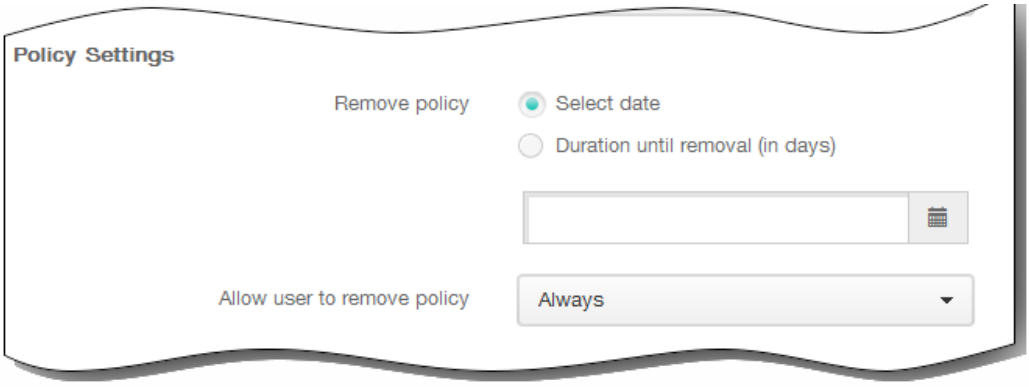


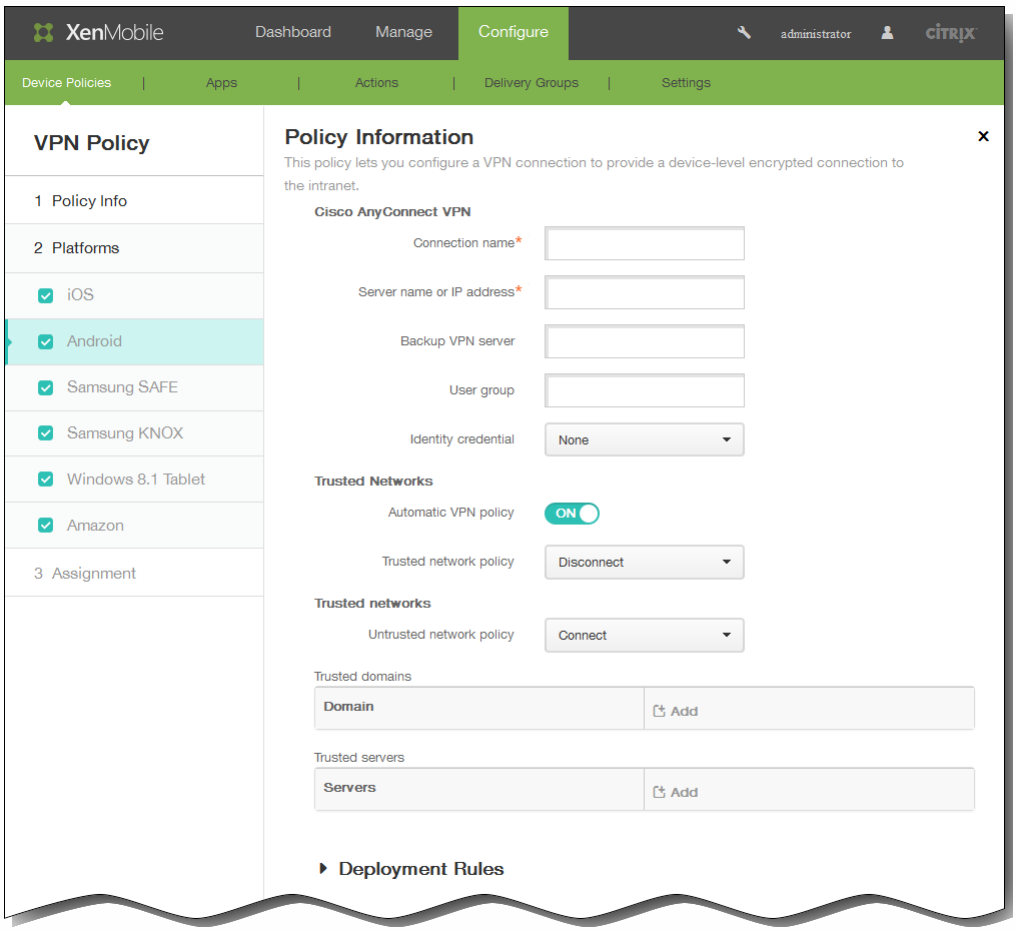




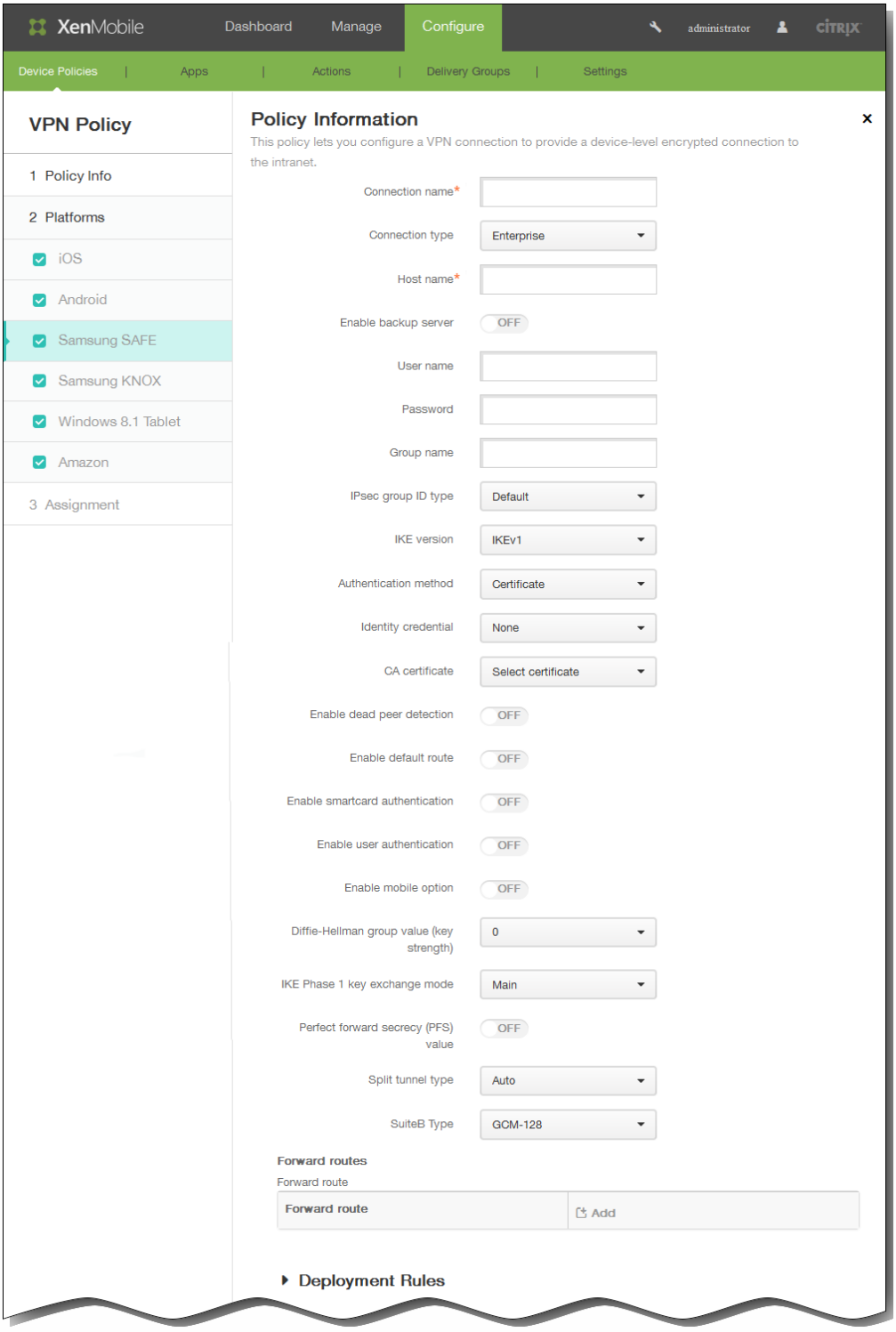


-
-
-
-
-
-
-
-
-
-

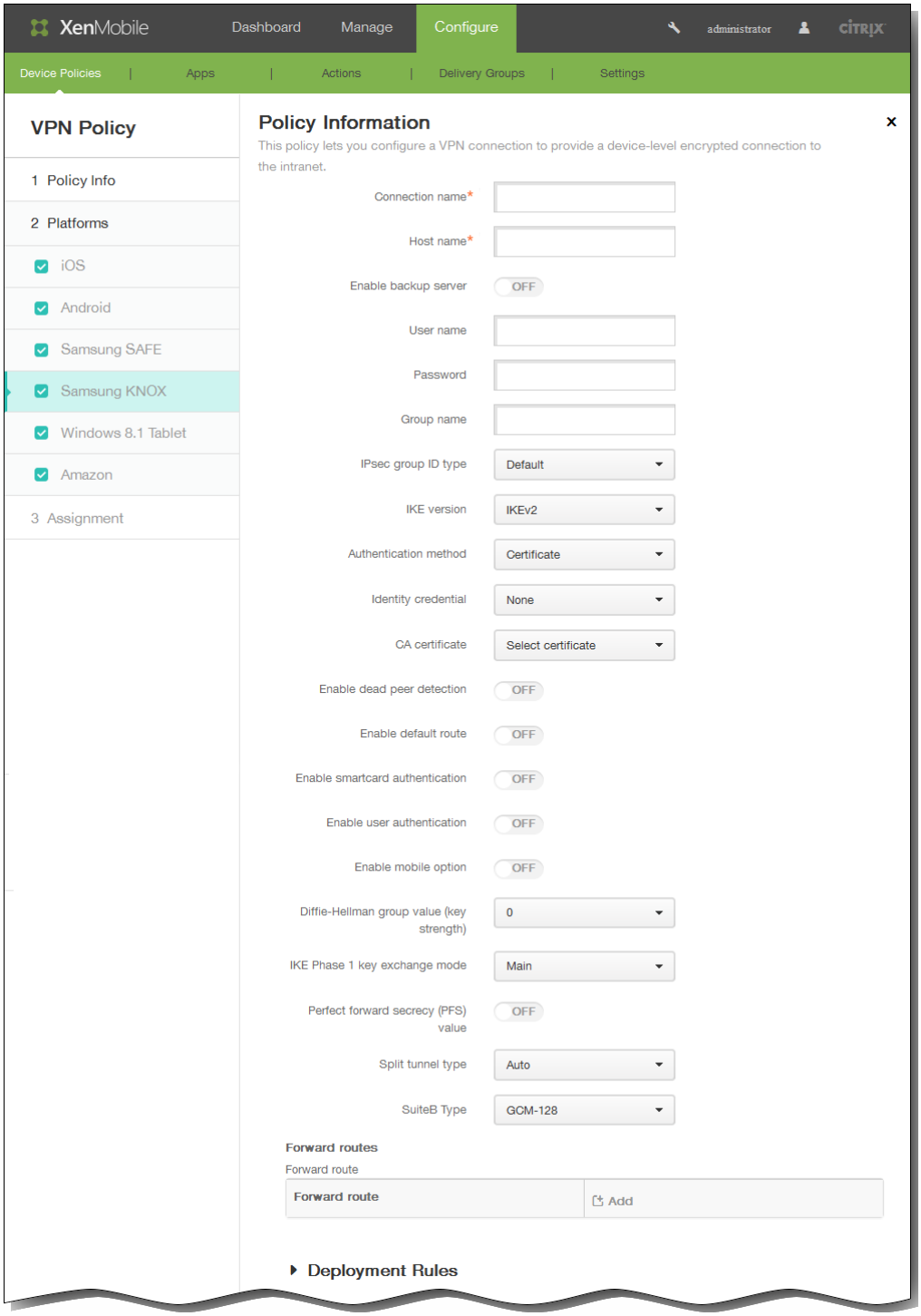




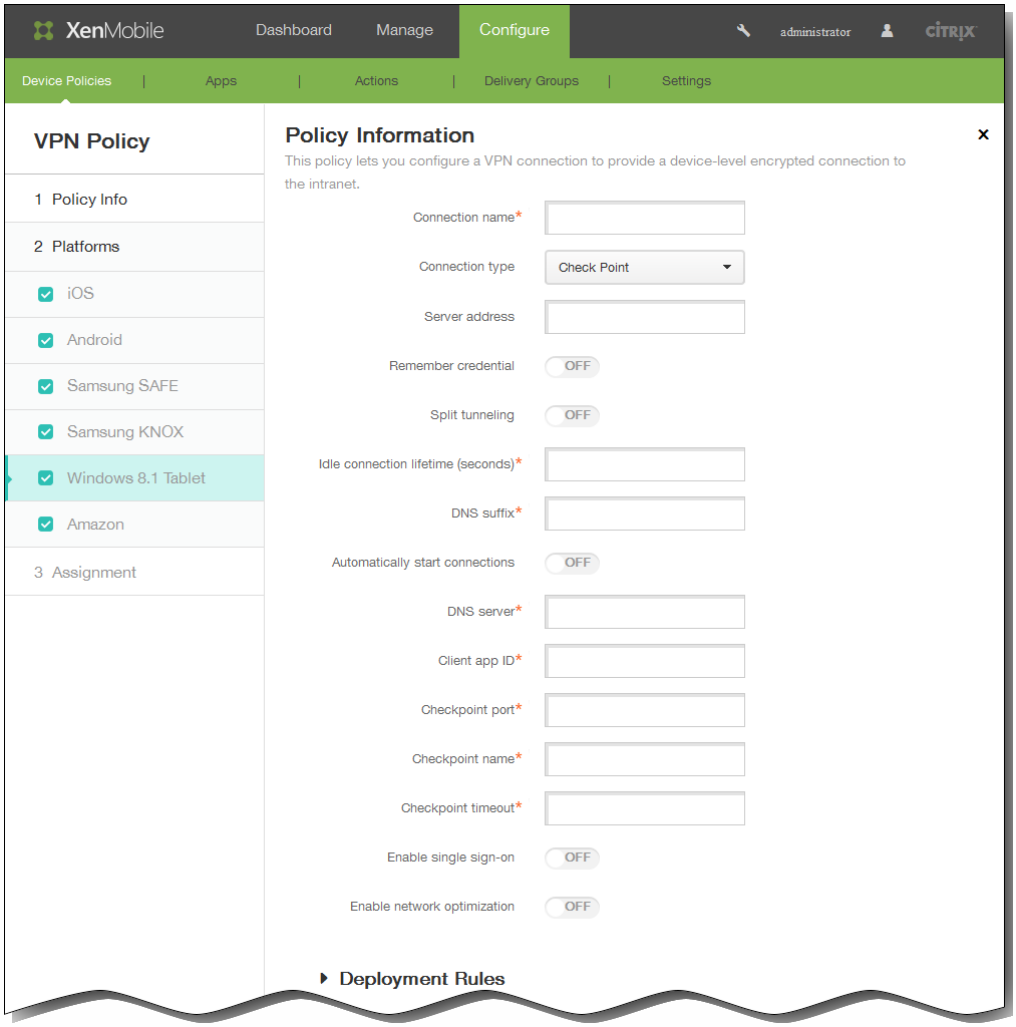
-
-



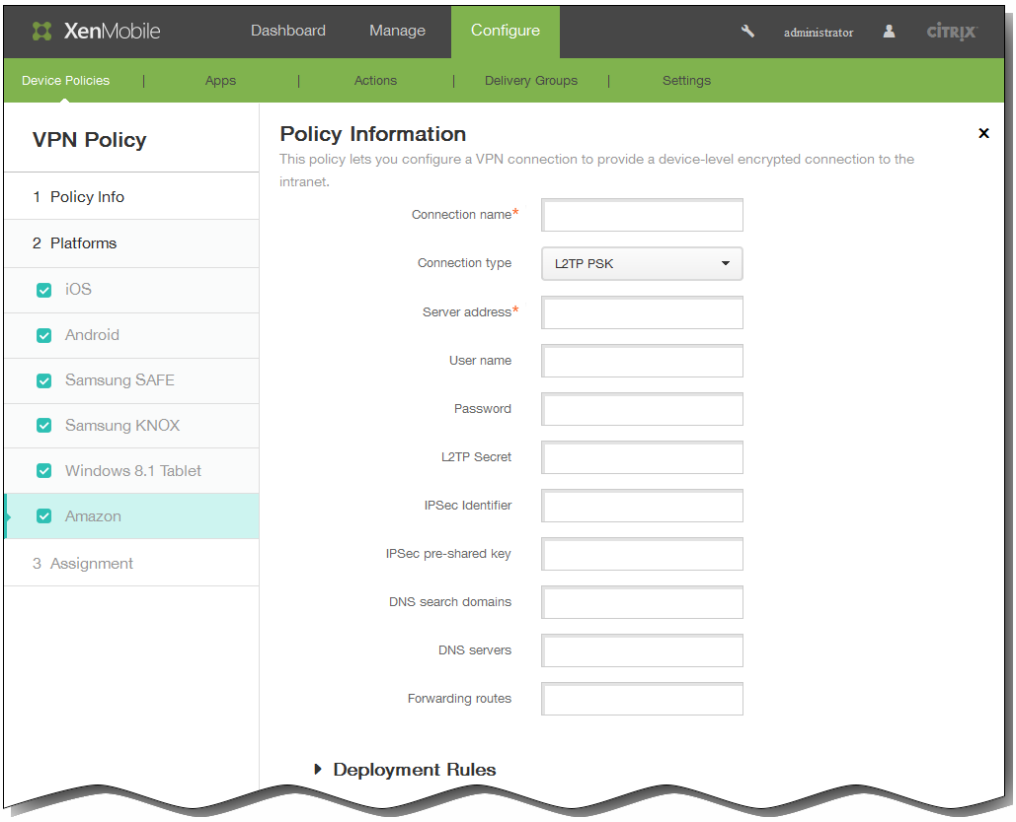
-
-
-
-



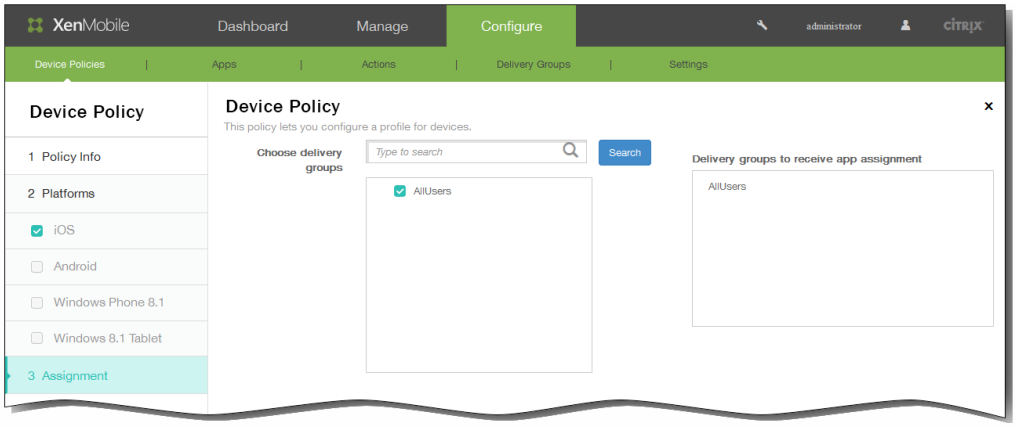
-
-
-
-
-

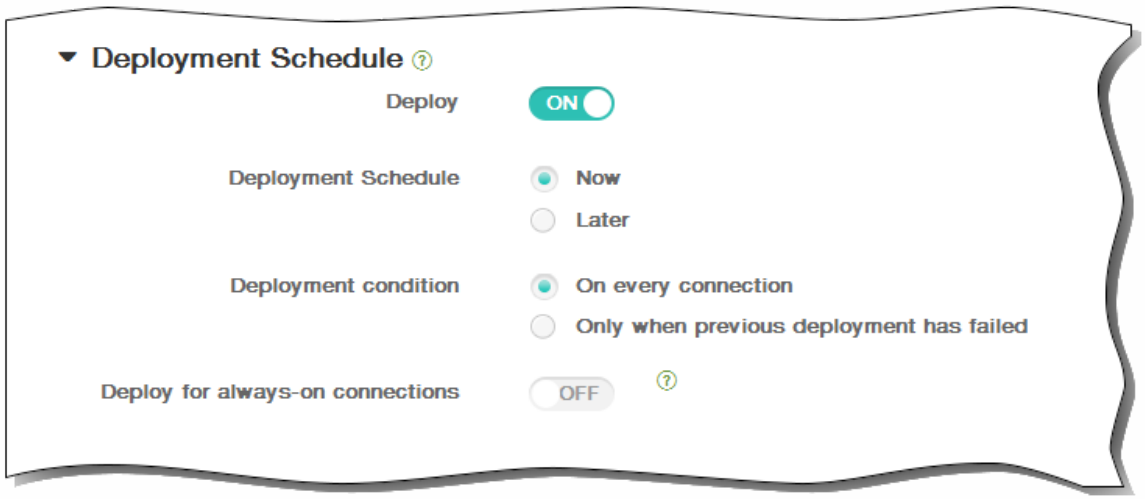


-
-
-
-
-



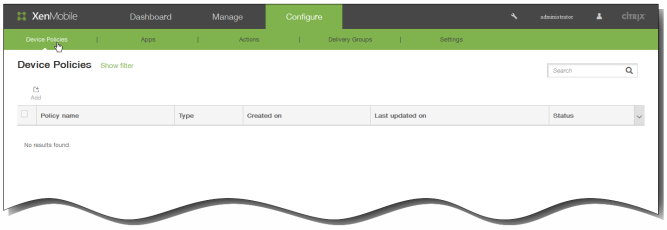
-
-
-
-
-
-

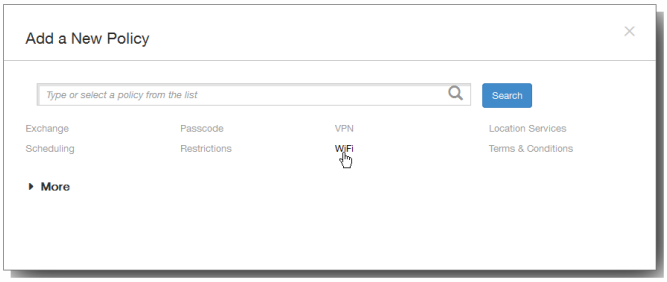


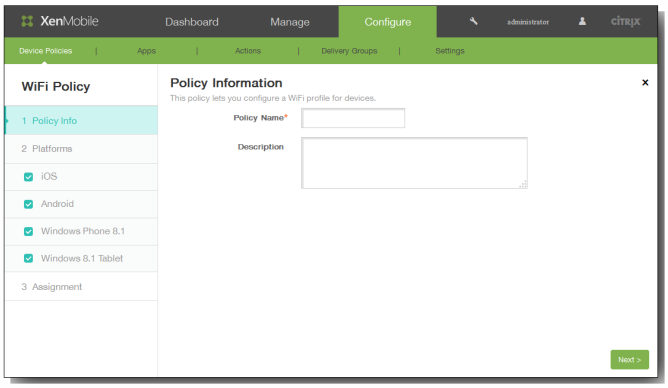


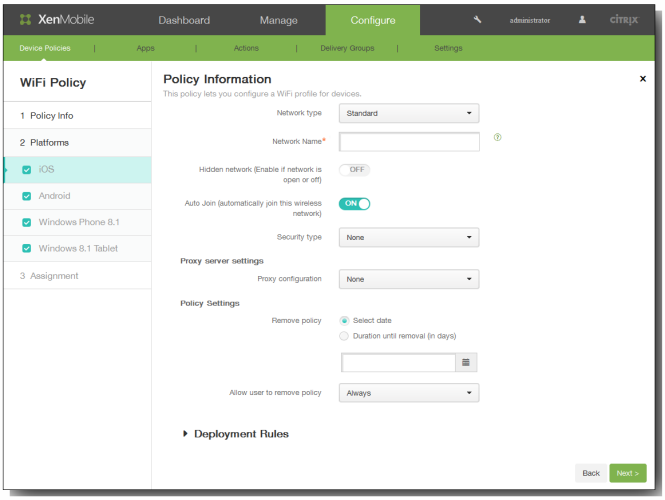
WiFiデバイスポリシー

-
-
-
-
-
-

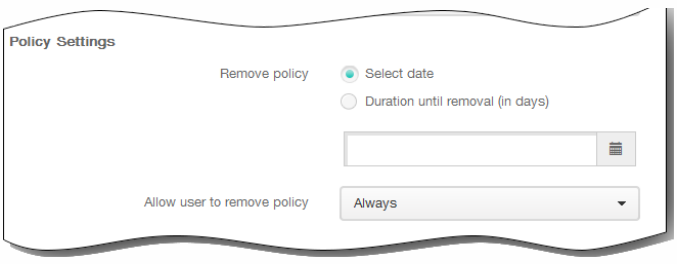


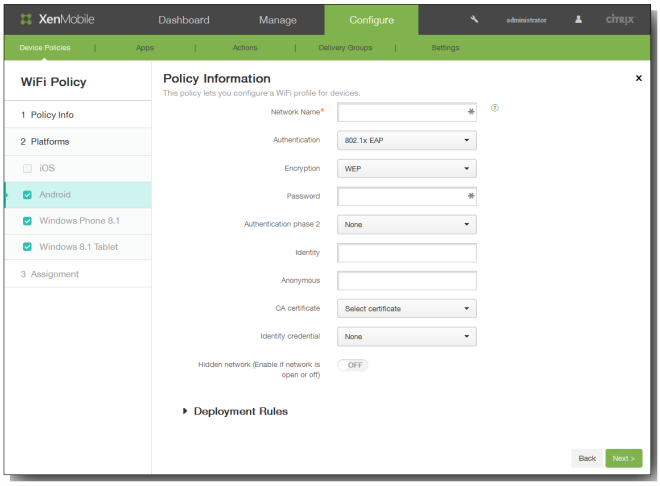




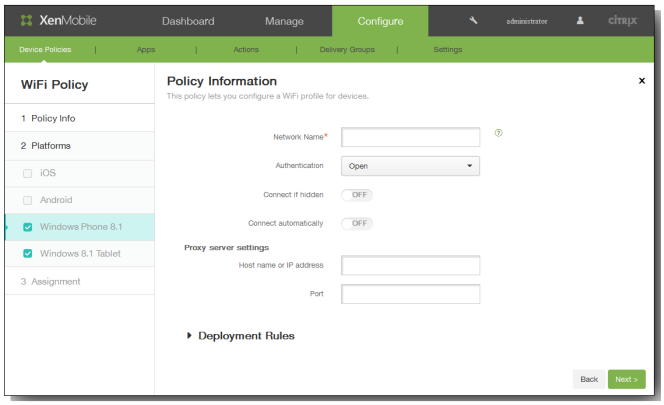


-
-
-
-
-
-
-

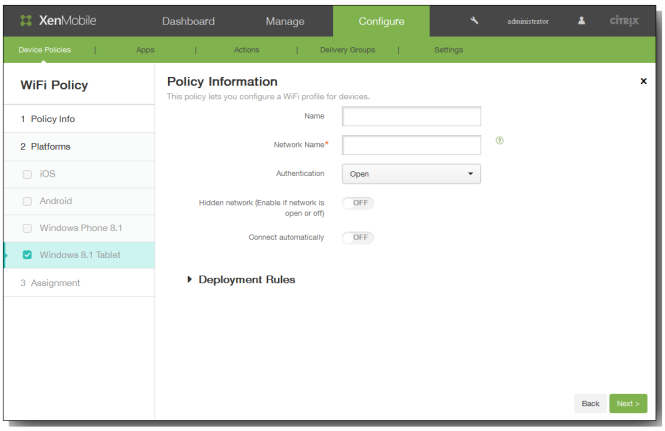




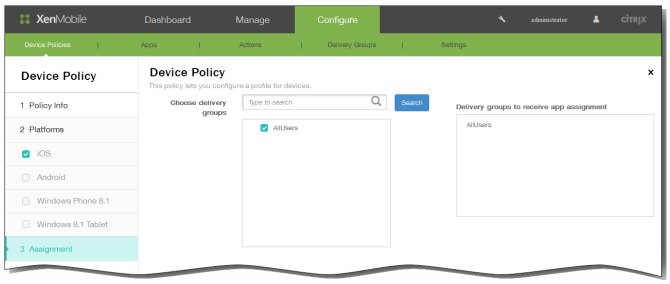
-
-
-
-
-
-
-

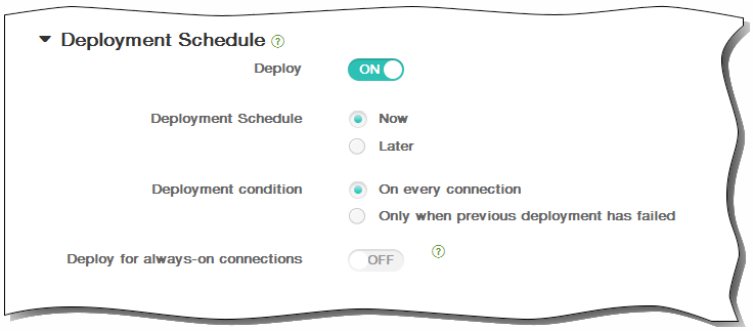


-
-
-
-

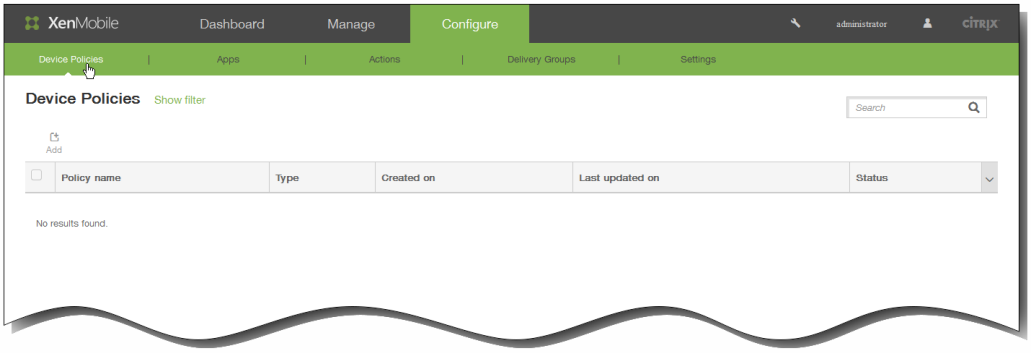


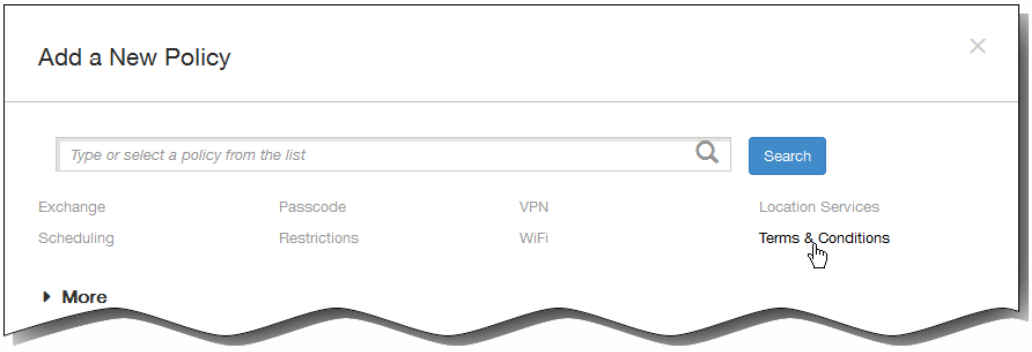
-
-
-
-
-

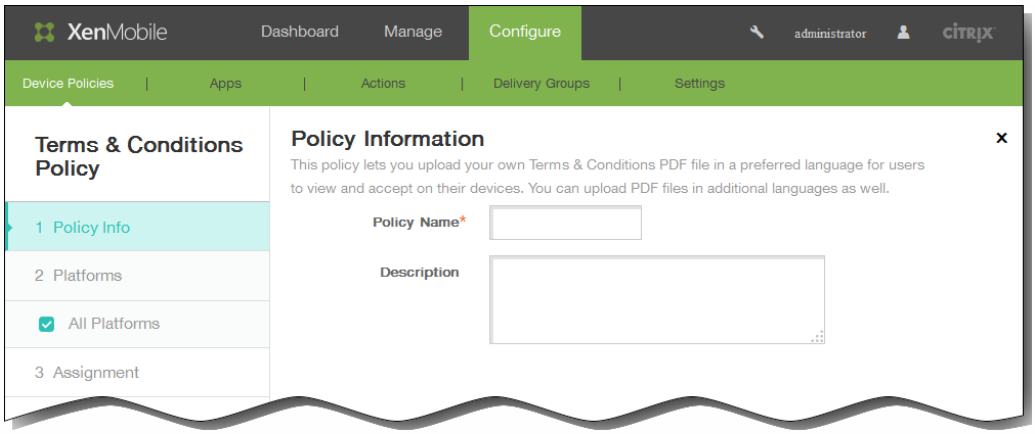


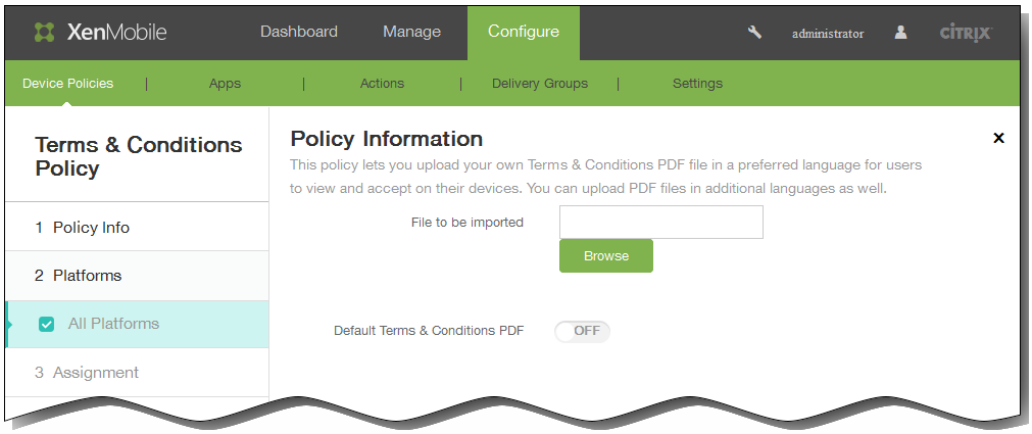


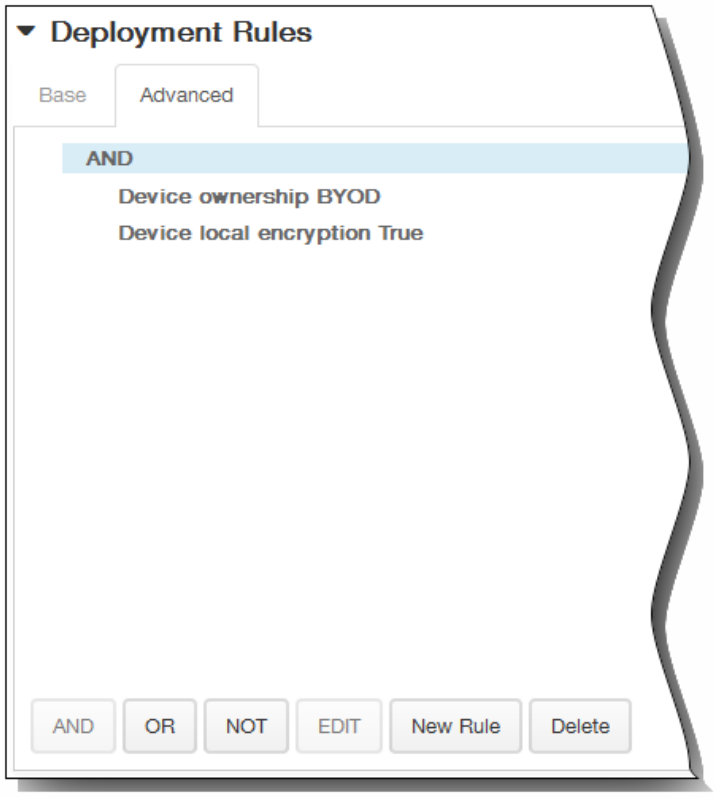
すべてのプラットフォームの契約条件デバイスポリシーを追加するには

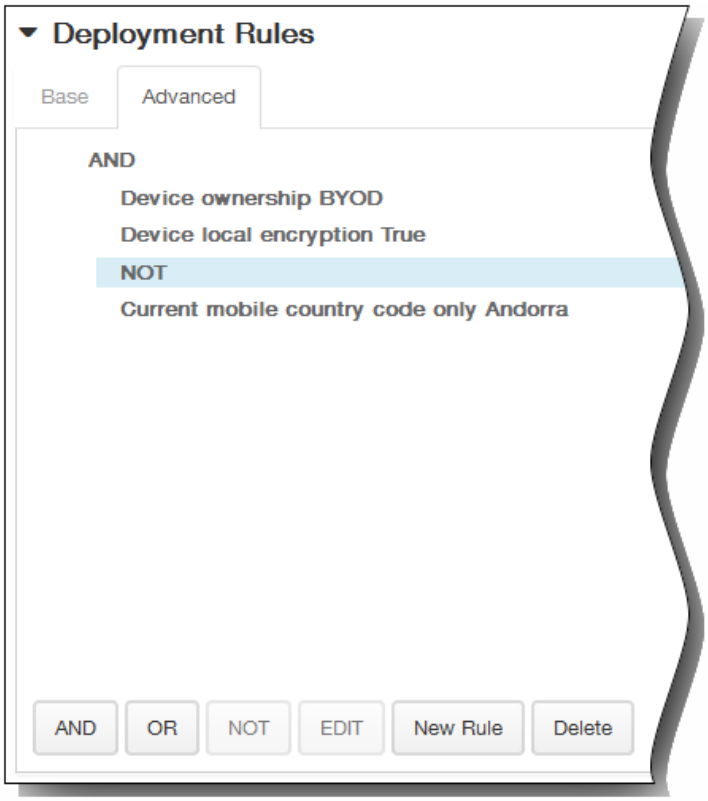


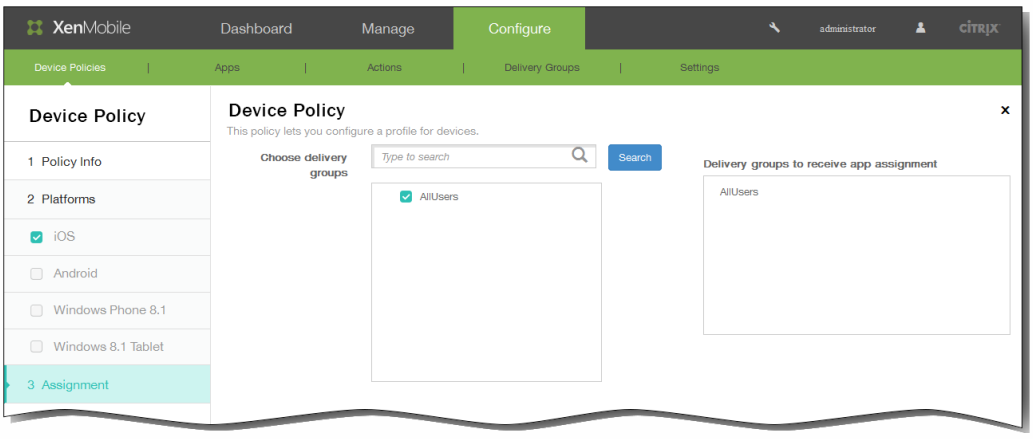


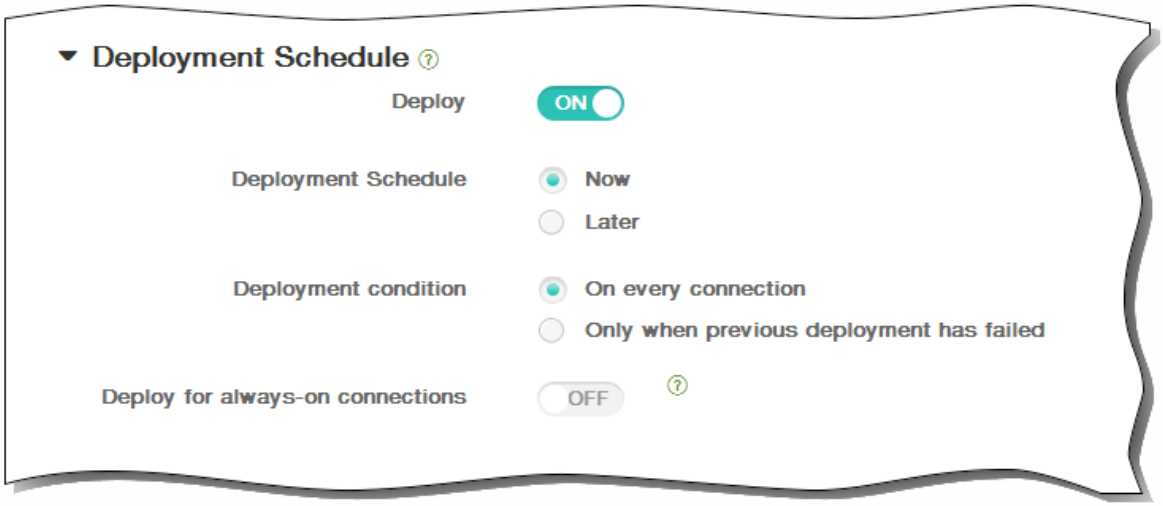




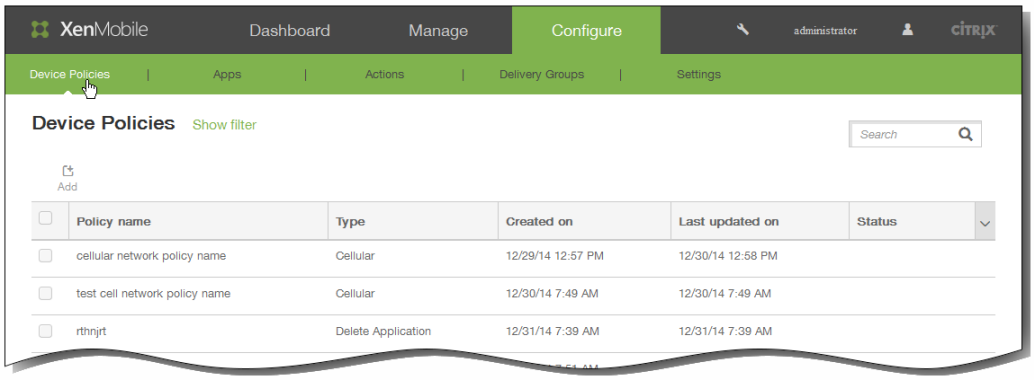


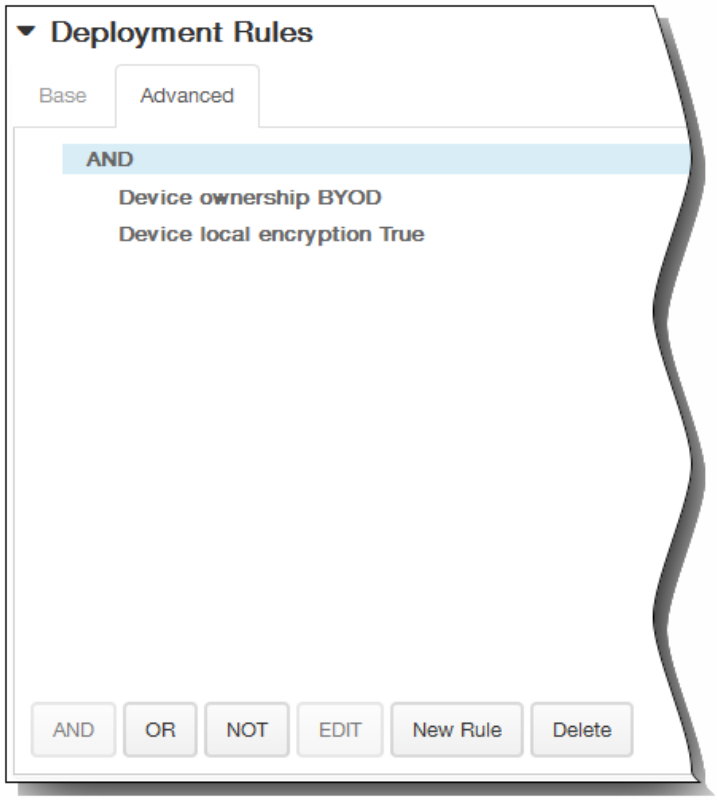


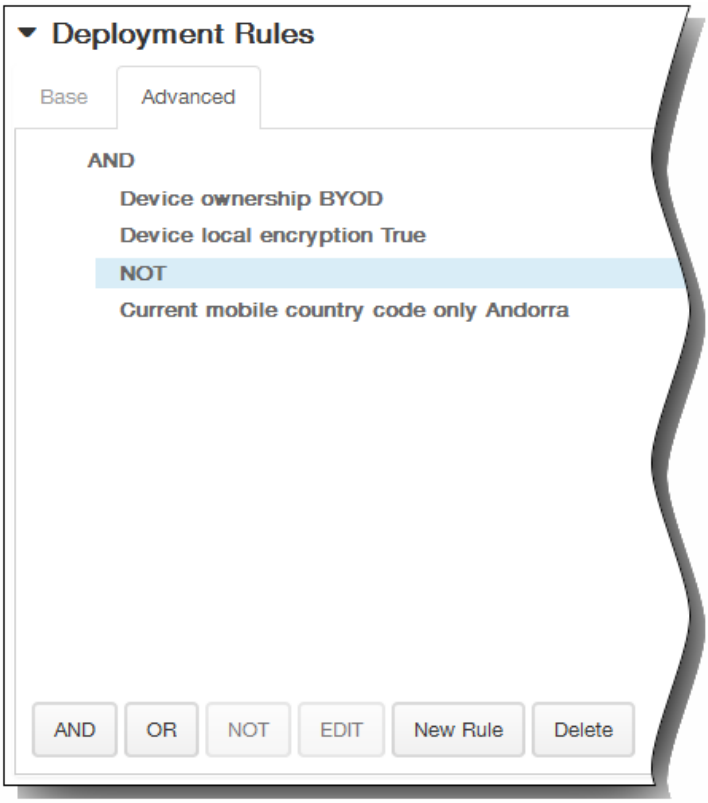


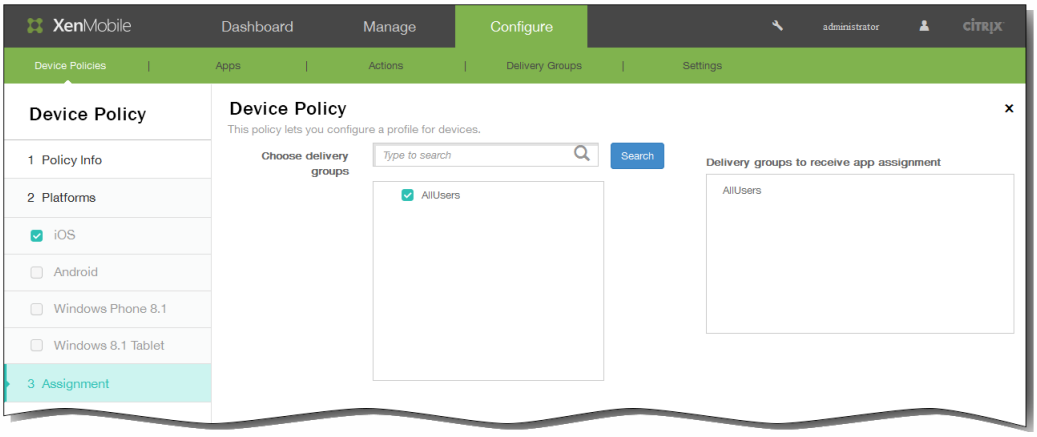


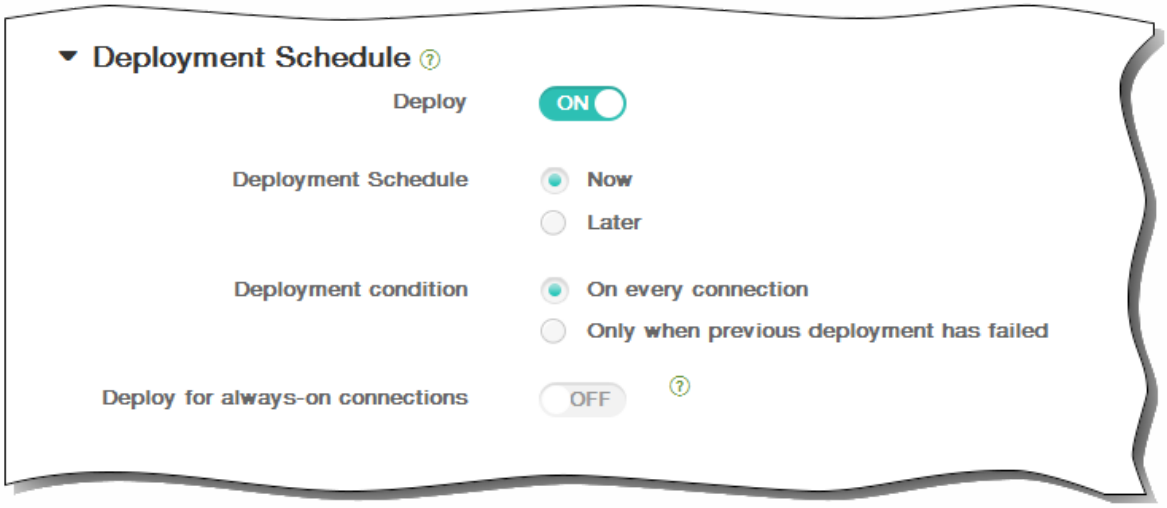
Worx Storeデバイスポリシーを追加するには



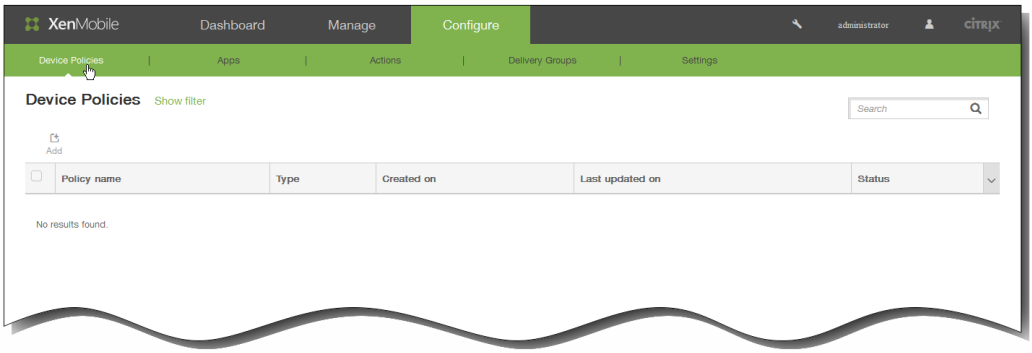


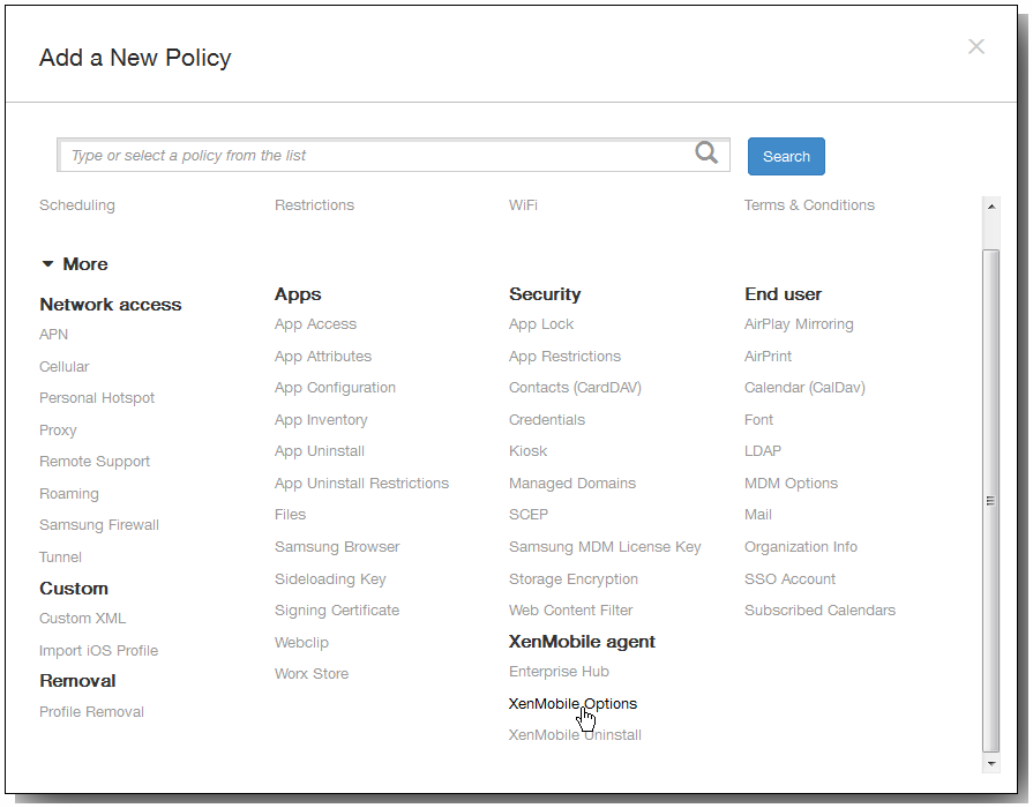


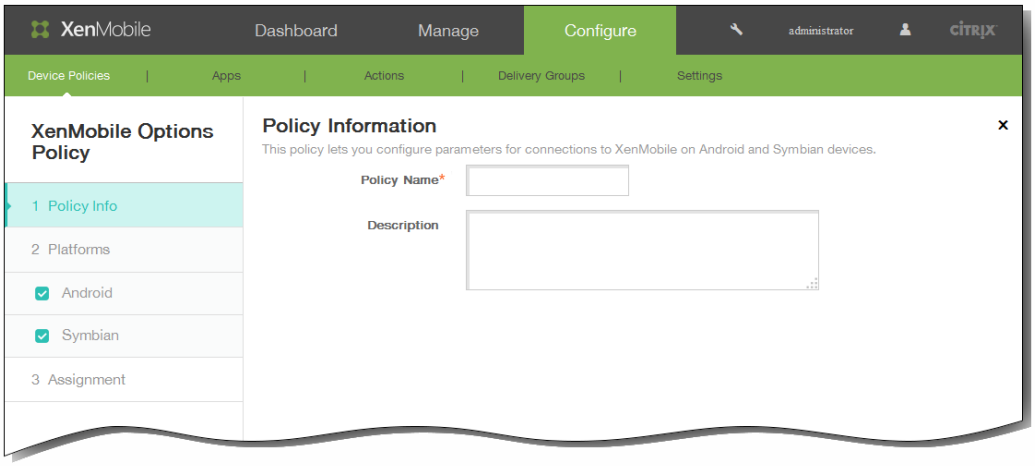


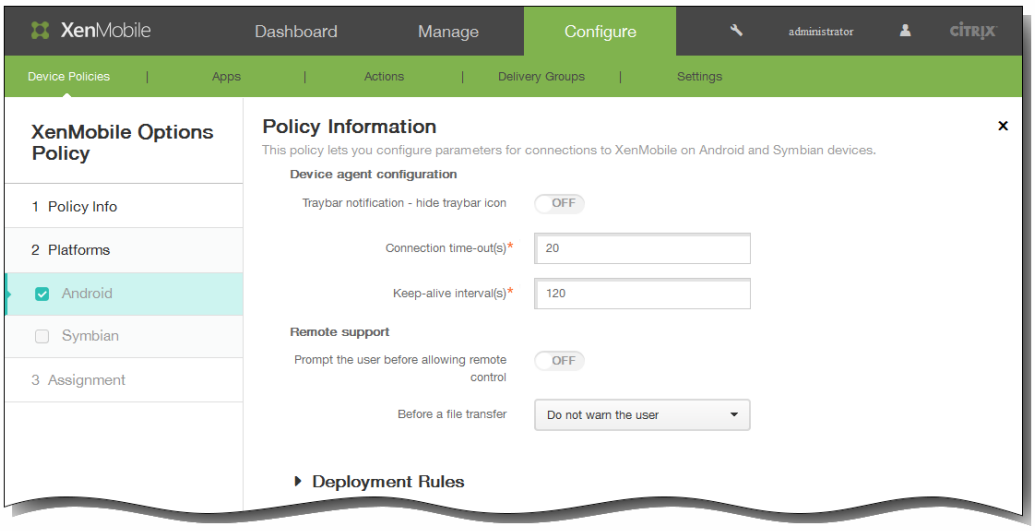


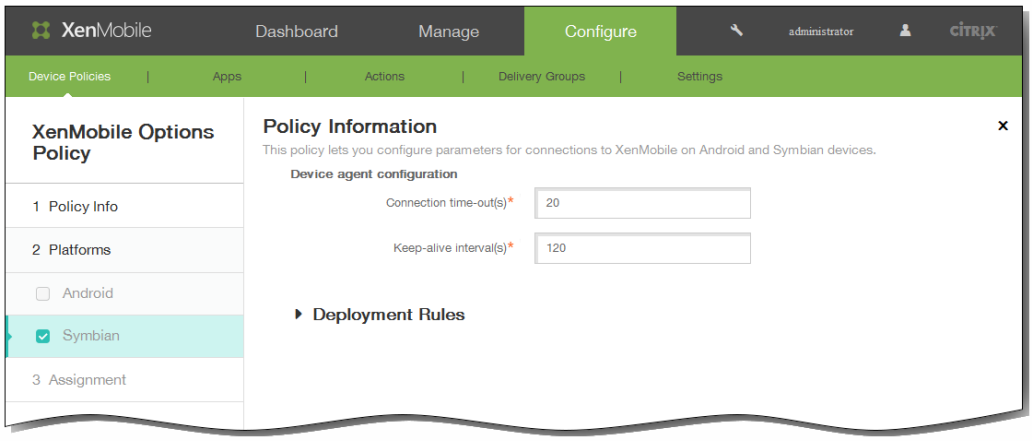
XenMobileオプションデバイスポリシー

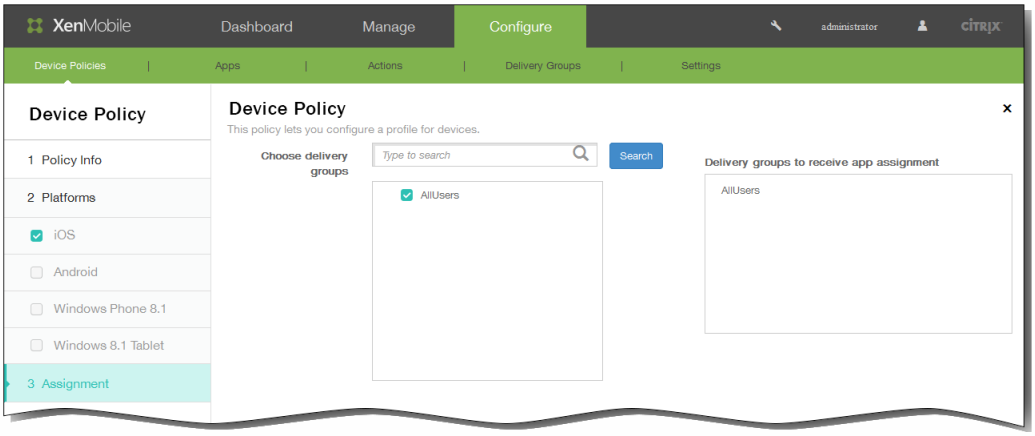


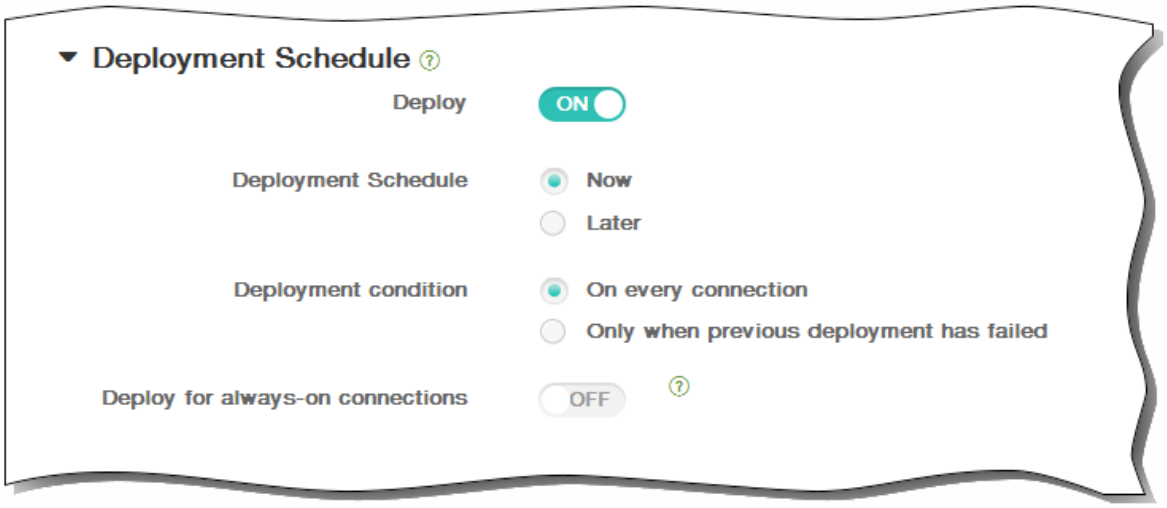




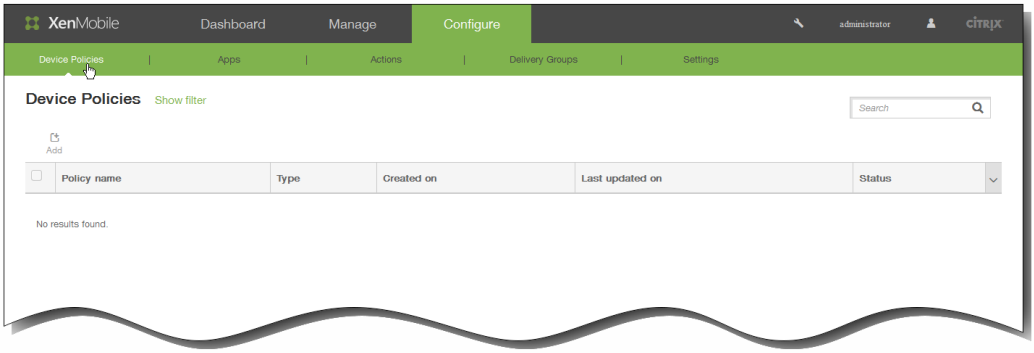


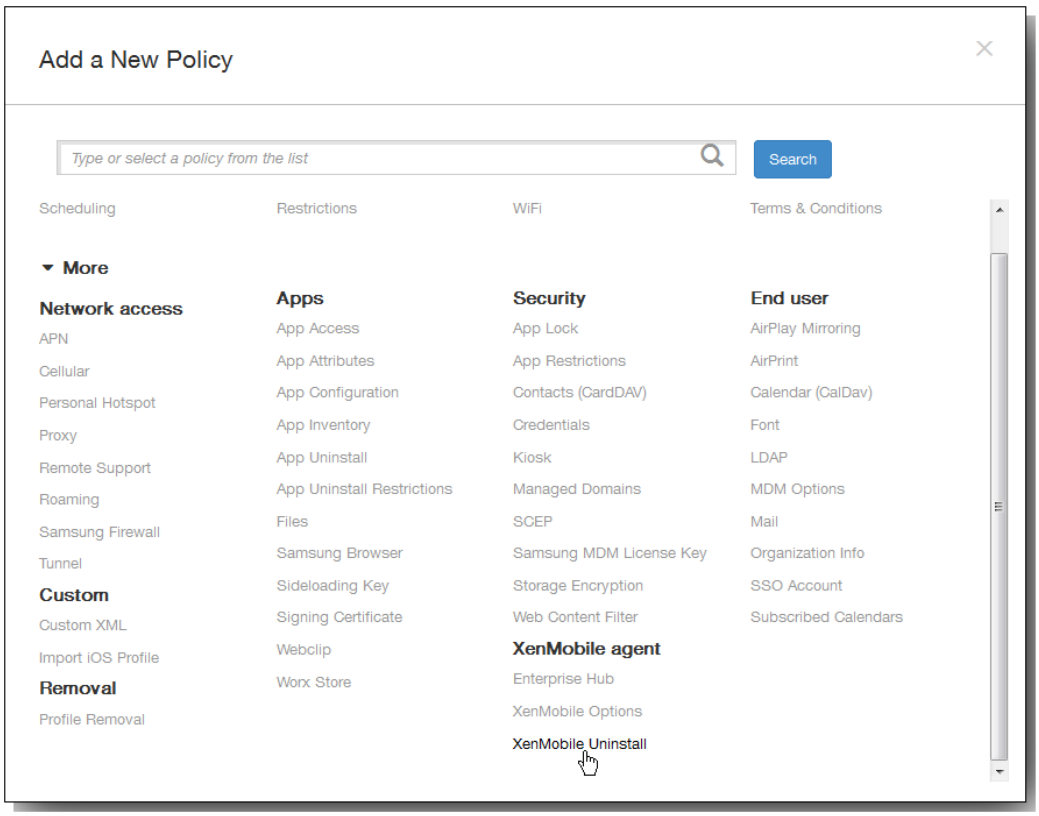


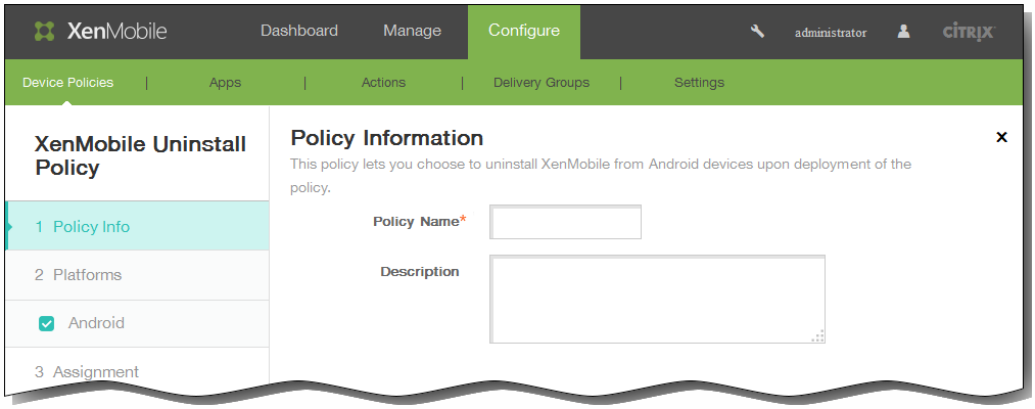


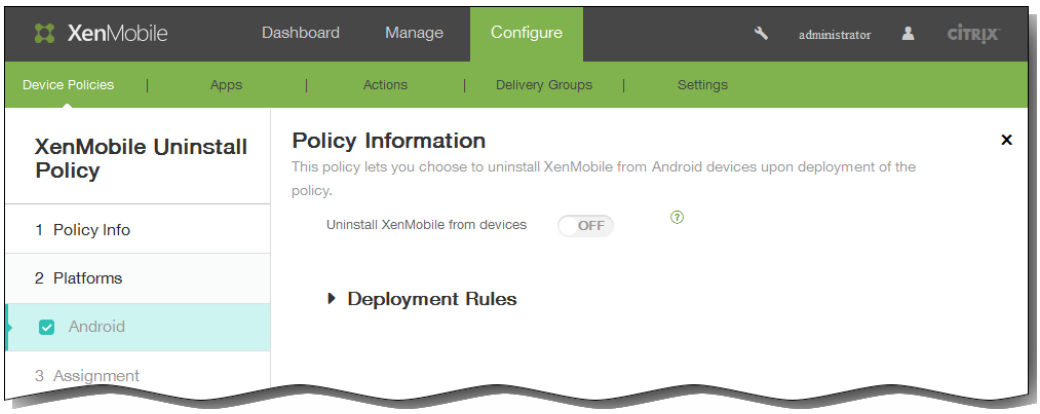


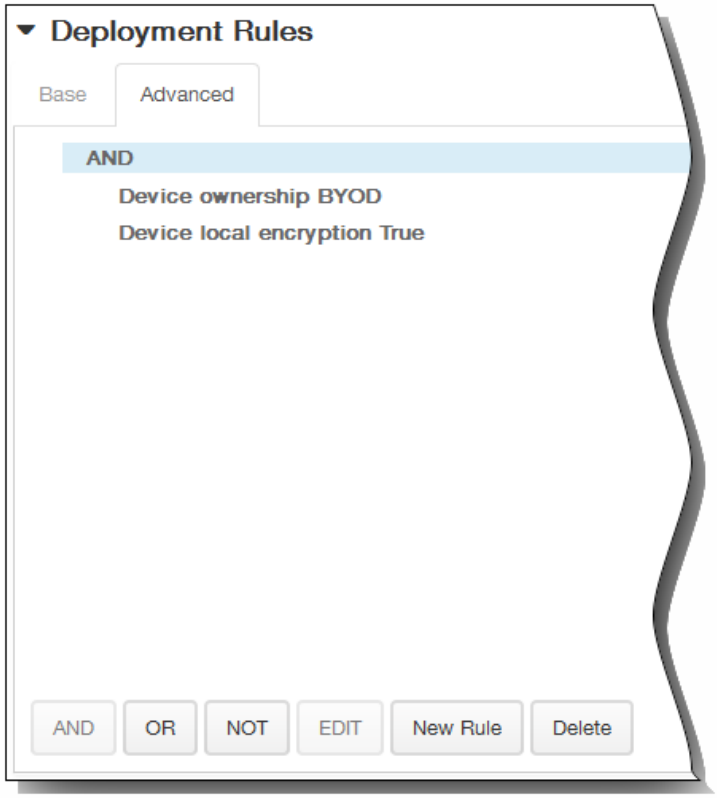
AndroidのXenMobileアンインストールデバイスポリシーを追加するには

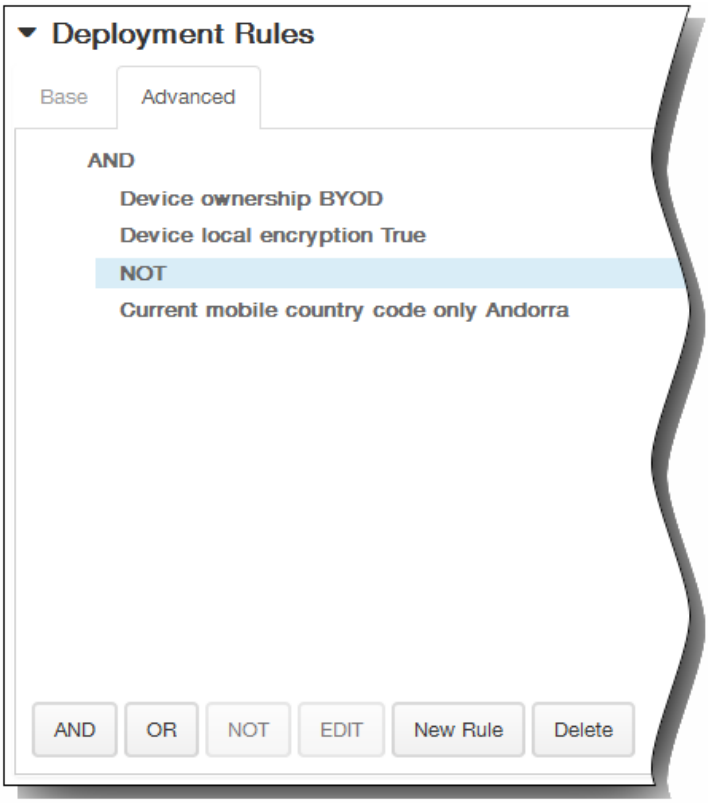


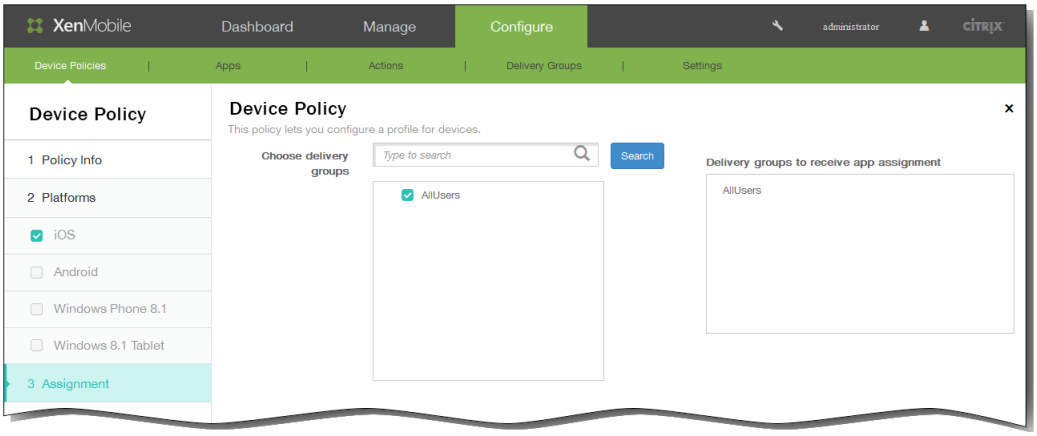


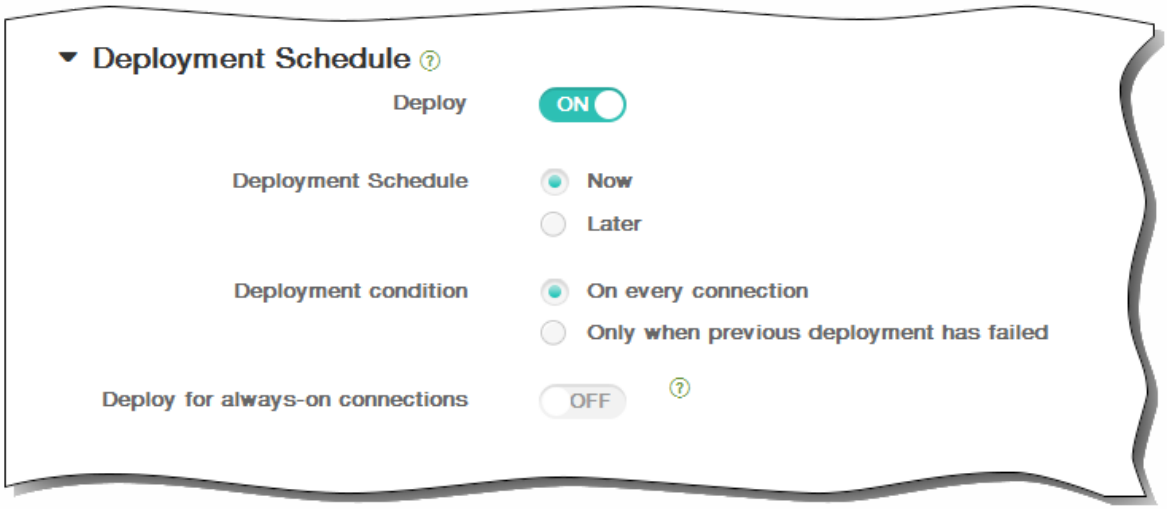












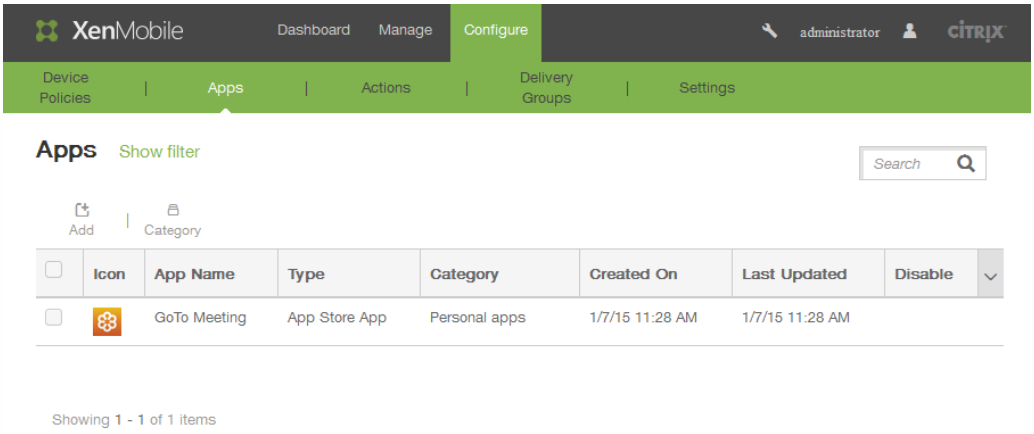
Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには

> Important

アプリケーションの追加

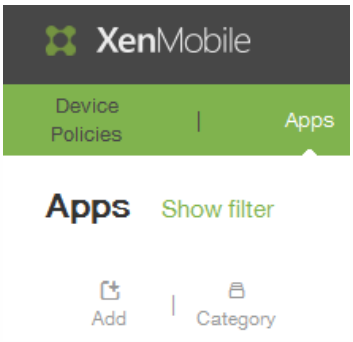
-
-
-
-
-
-
-

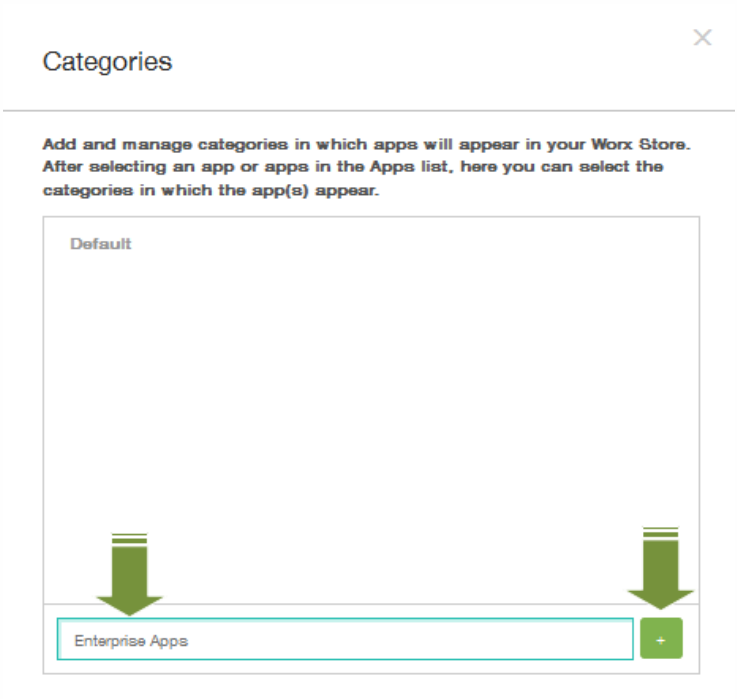
-
-
-
-

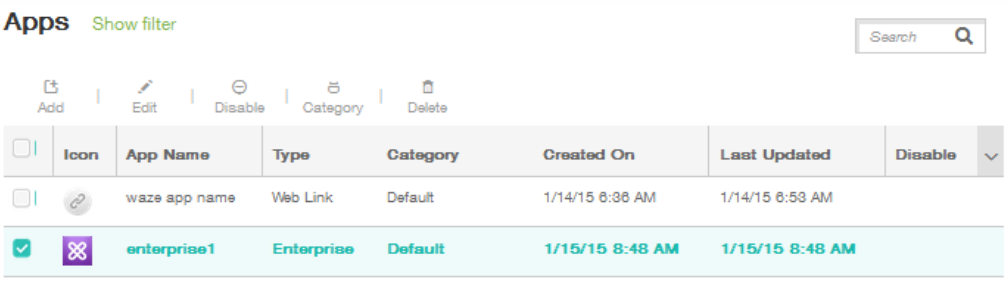


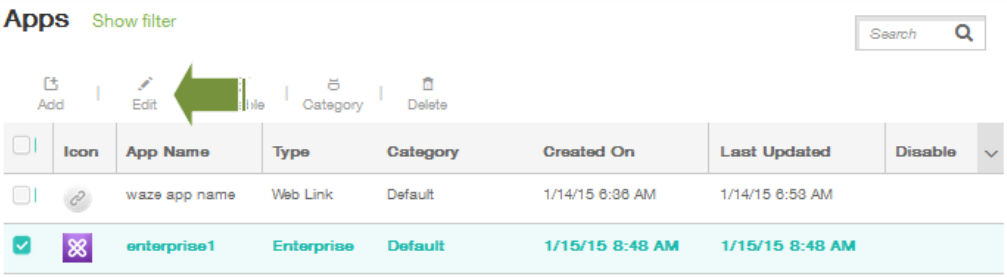
-
-
-
-
-

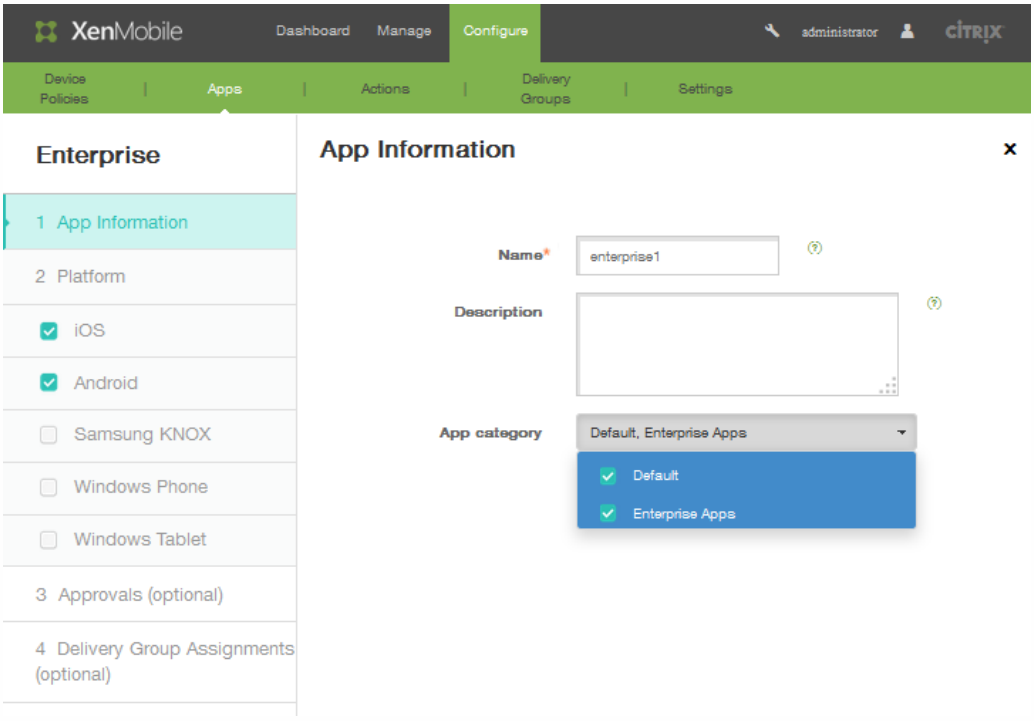
アプリケーションカテゴリを追加するには

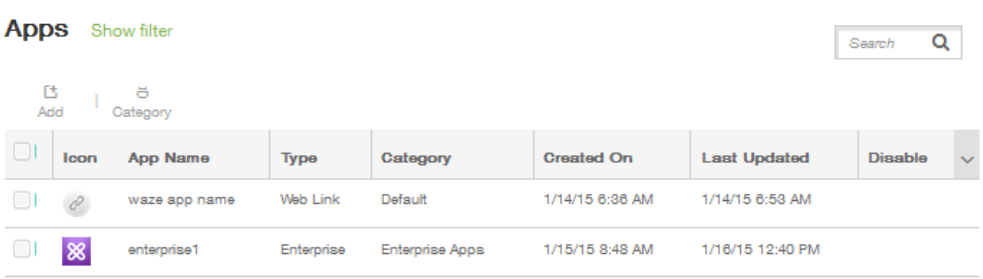




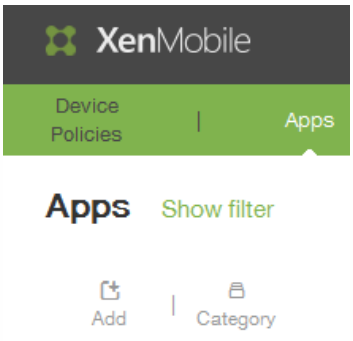


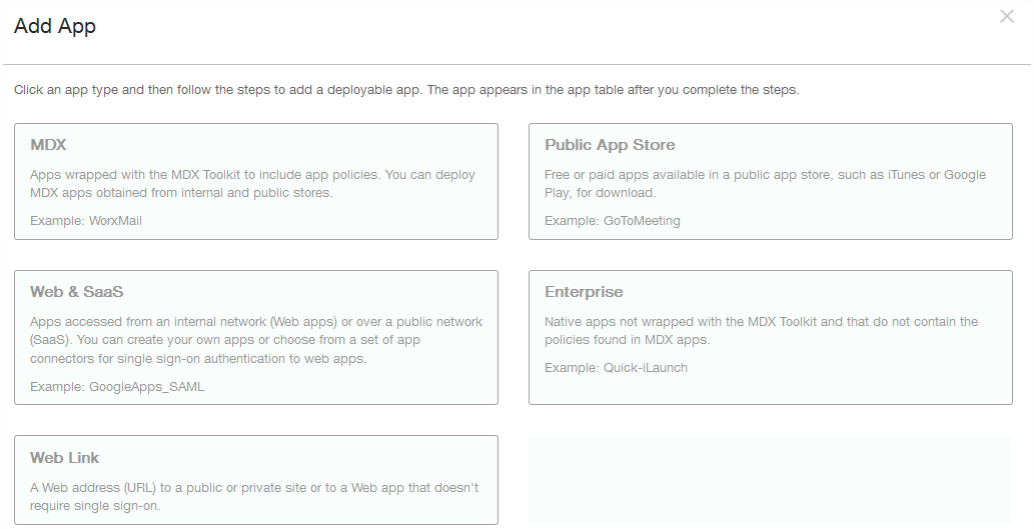


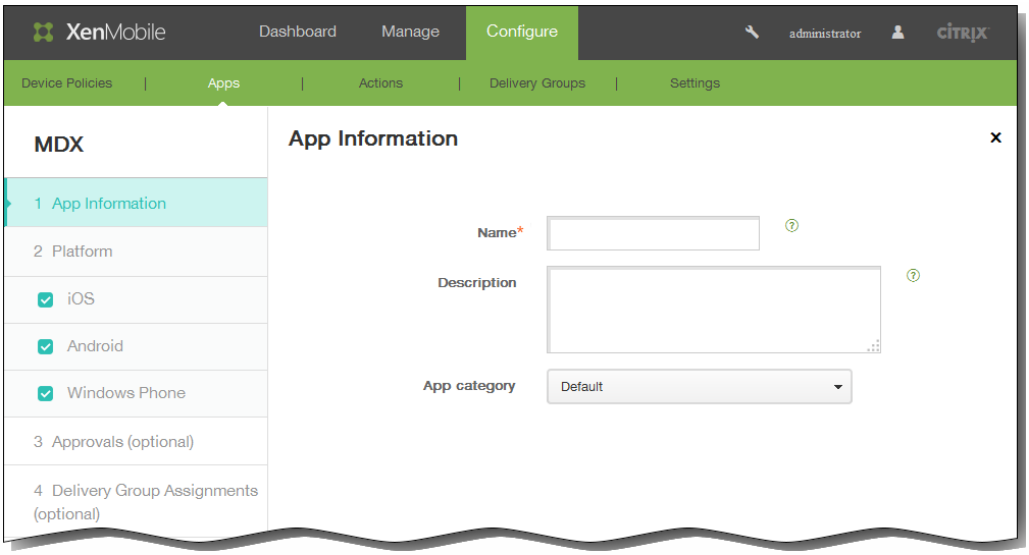


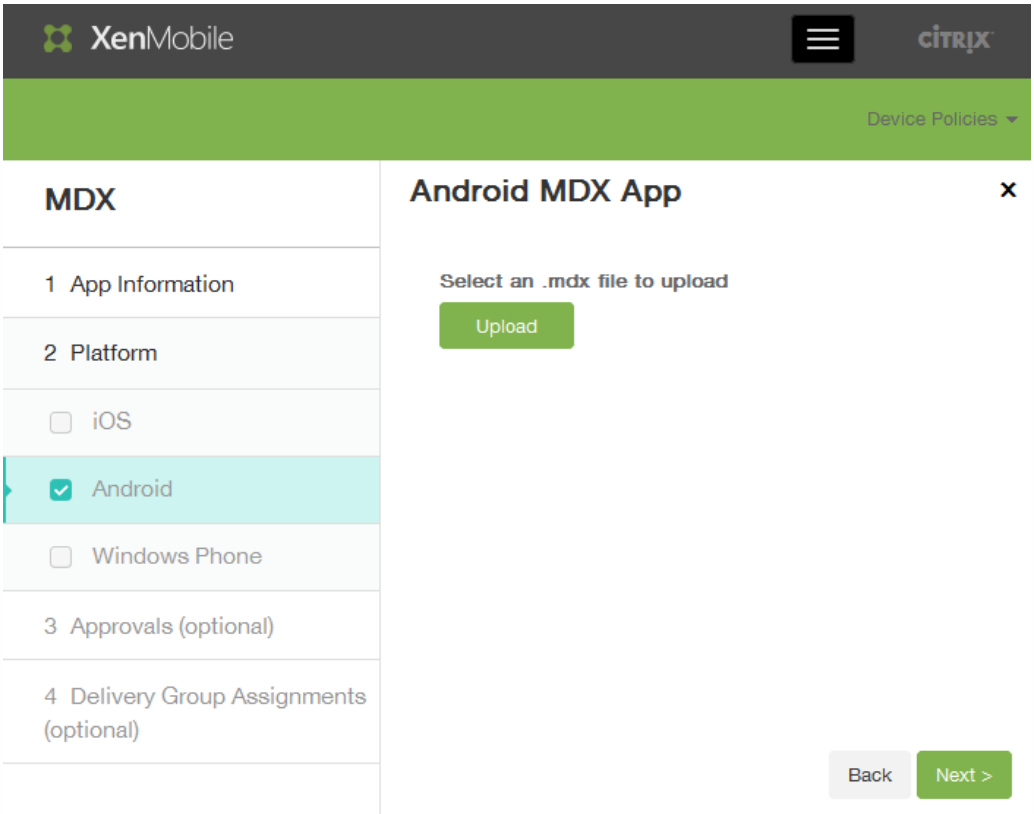


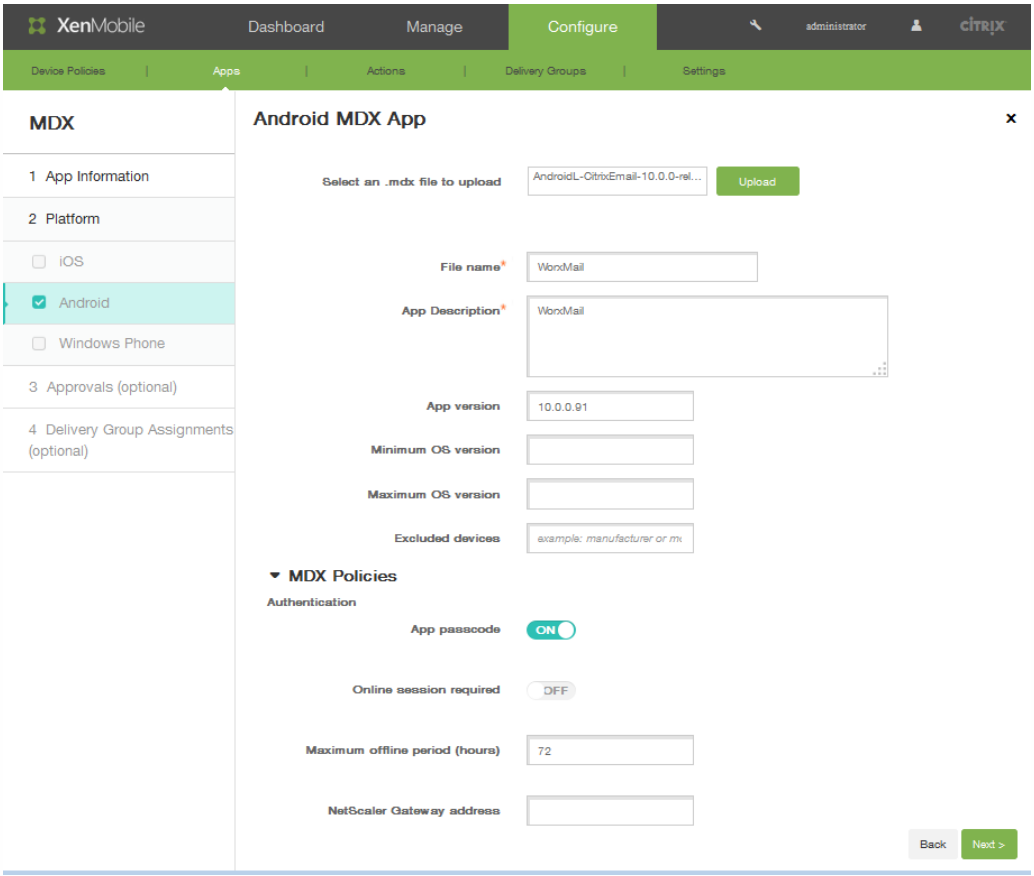
MDXアプリケーションをXenMobileに追加するには

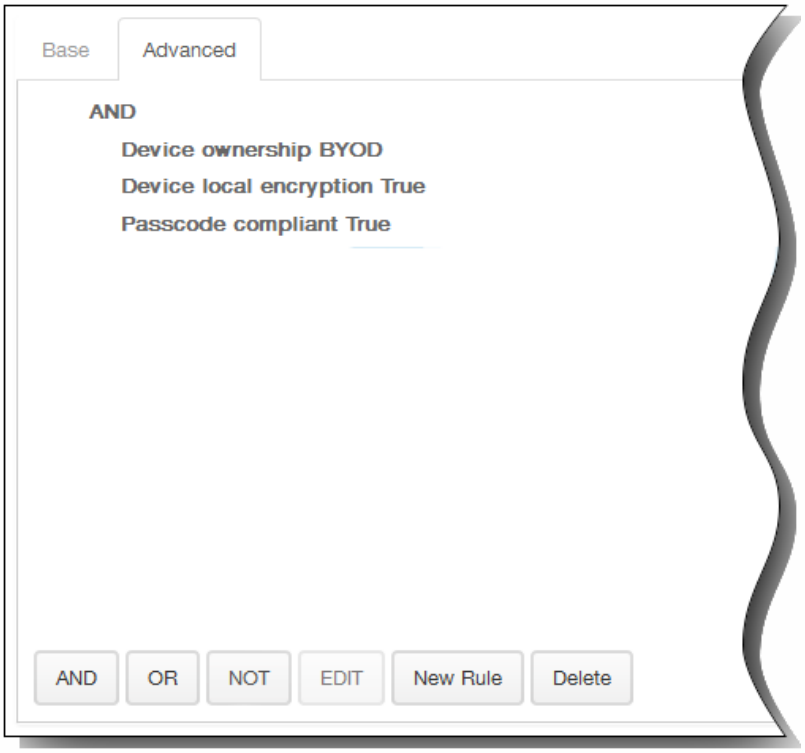


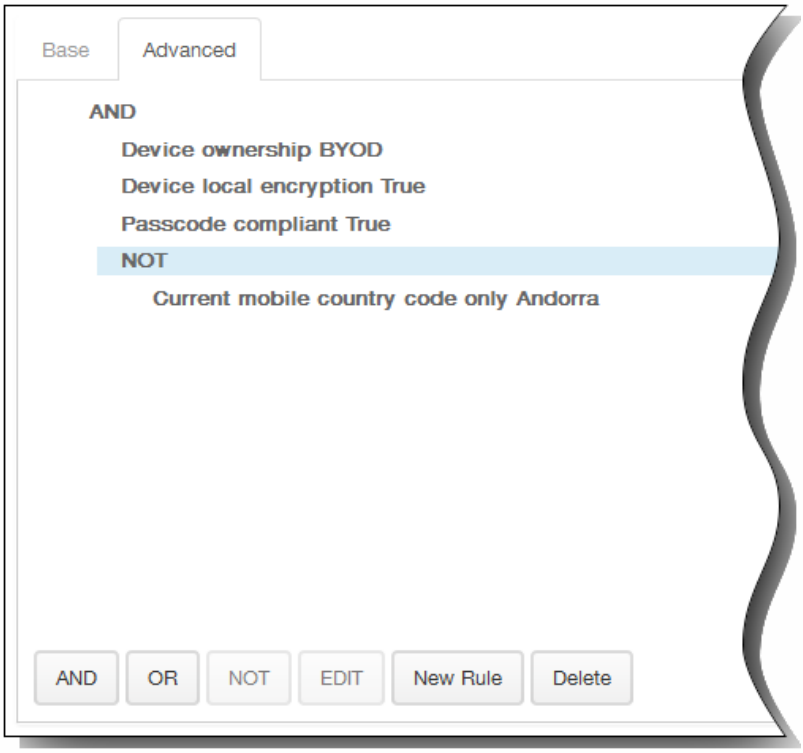


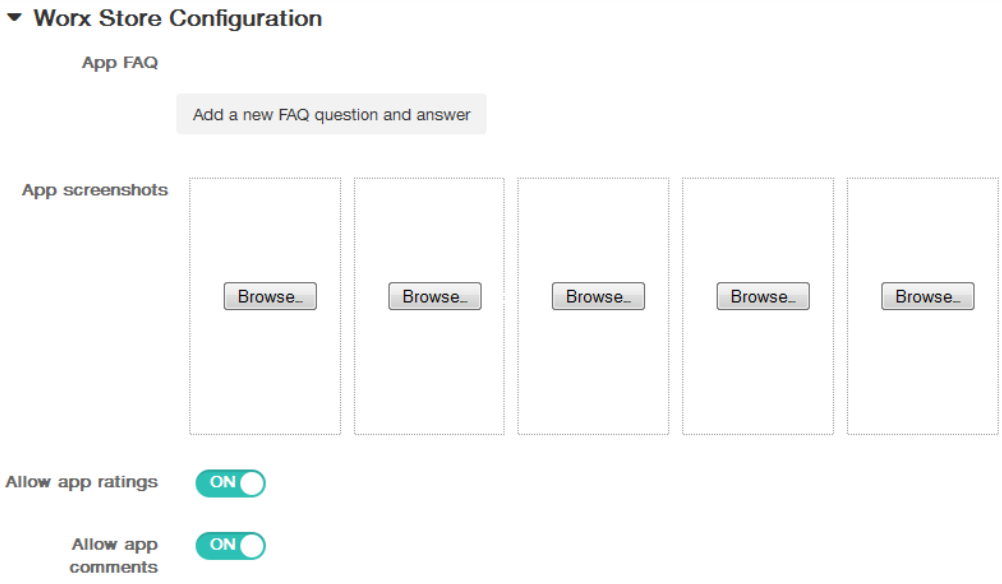


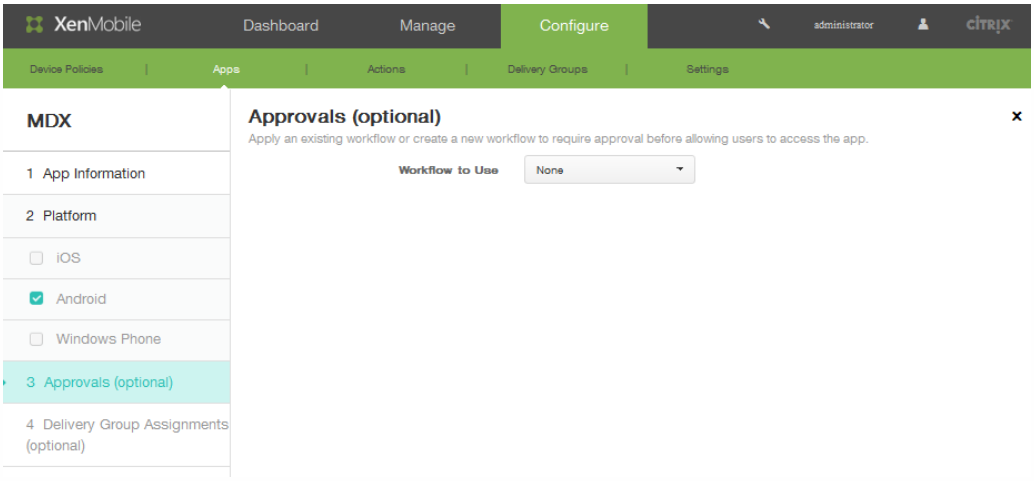


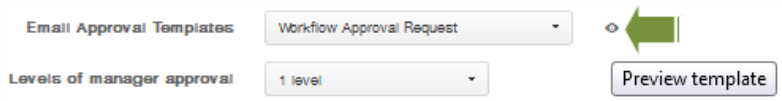


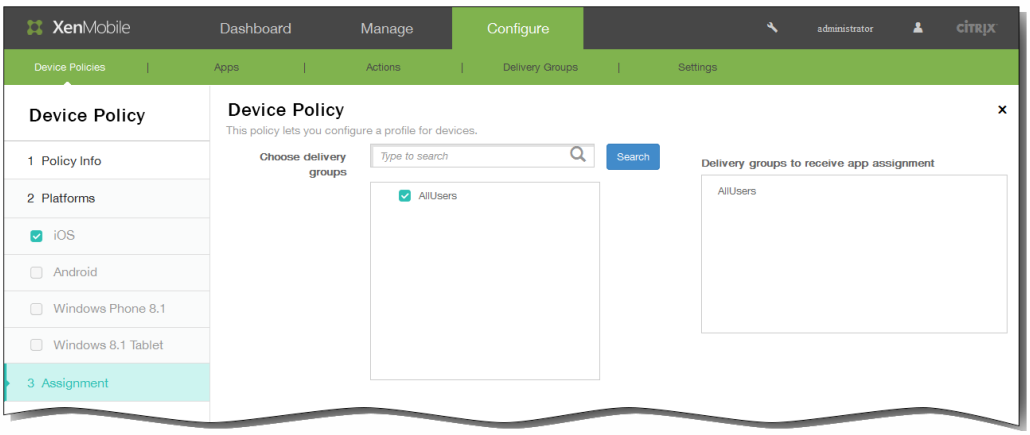


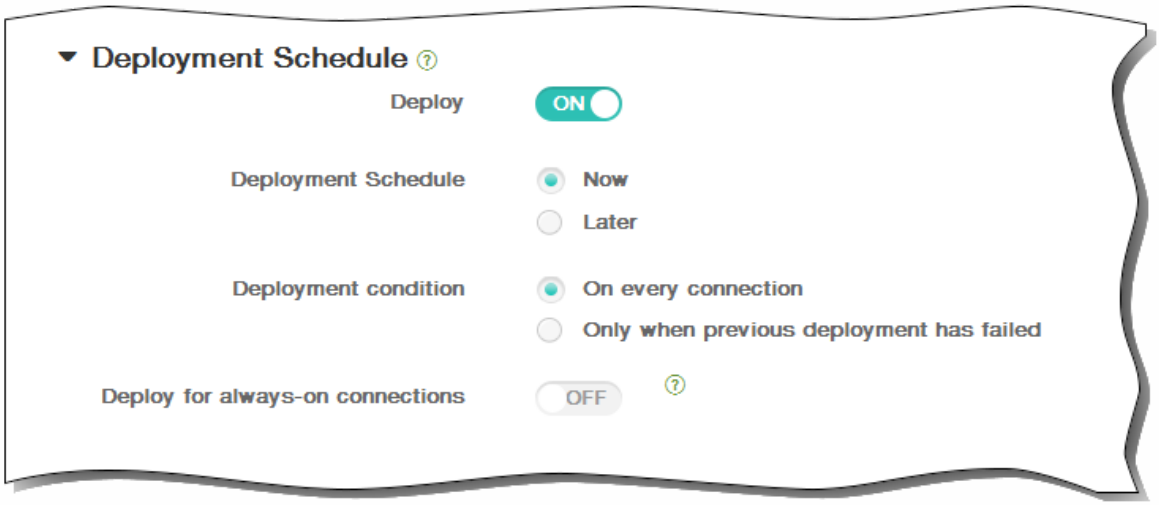




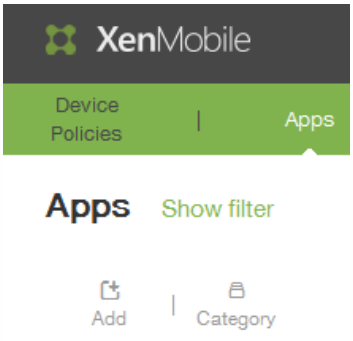


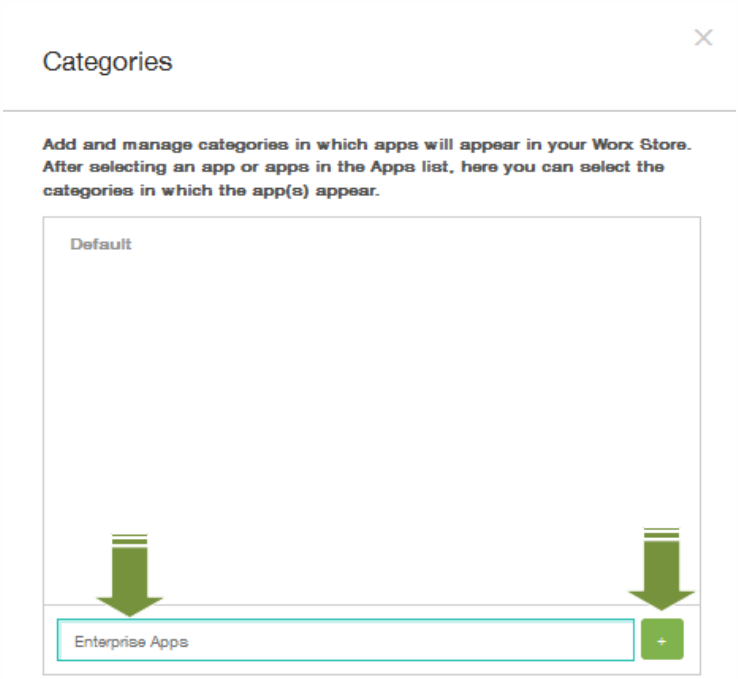


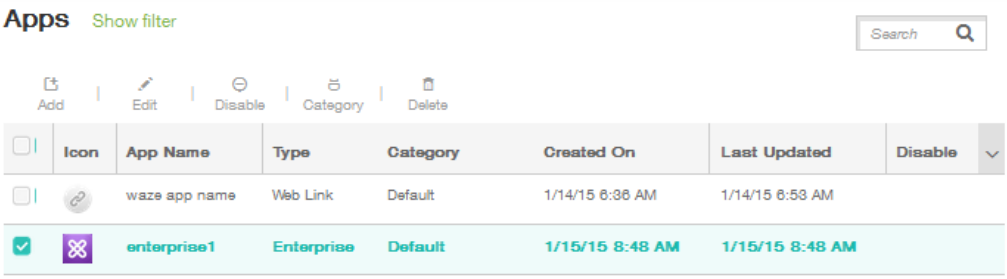


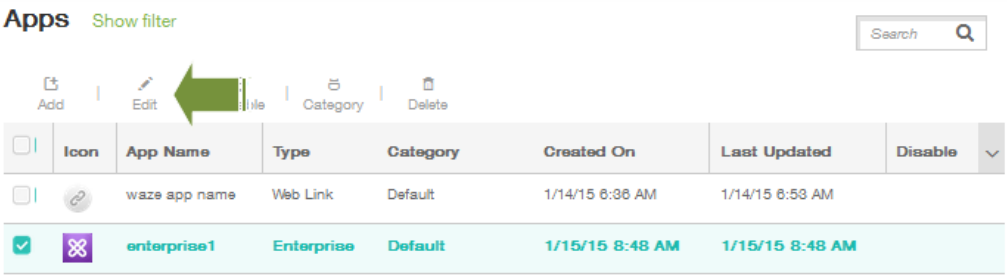


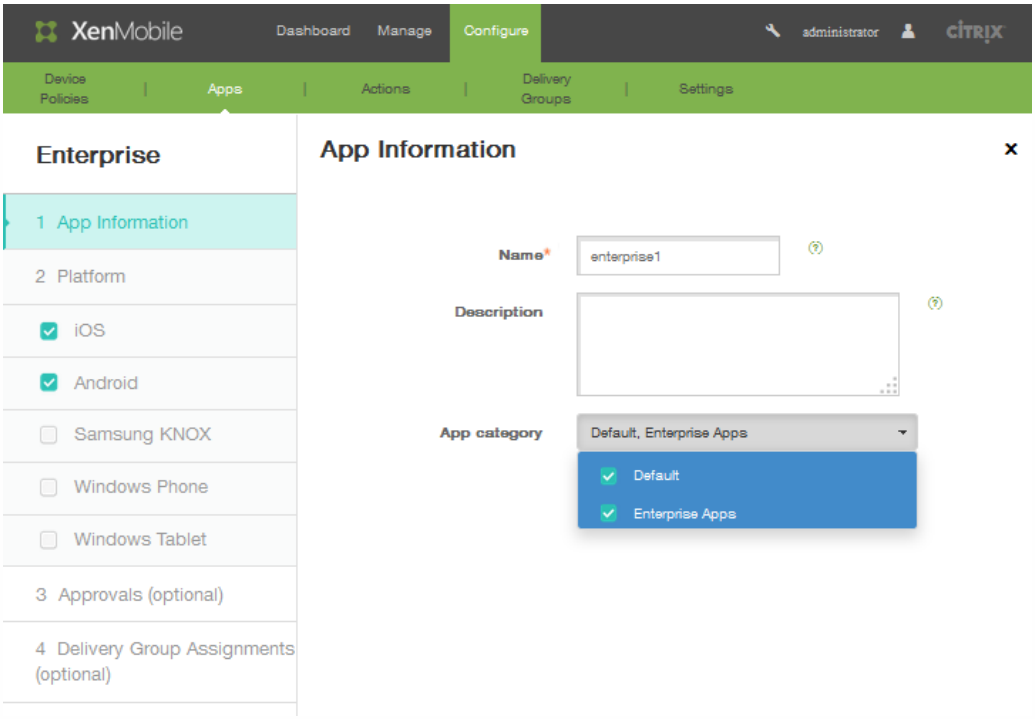
XenMobileでのアプリケーションカテゴリの作成

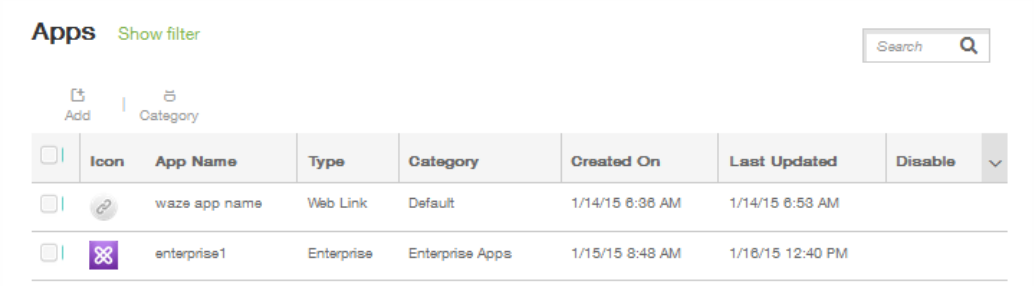




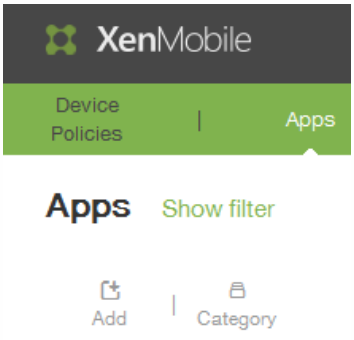


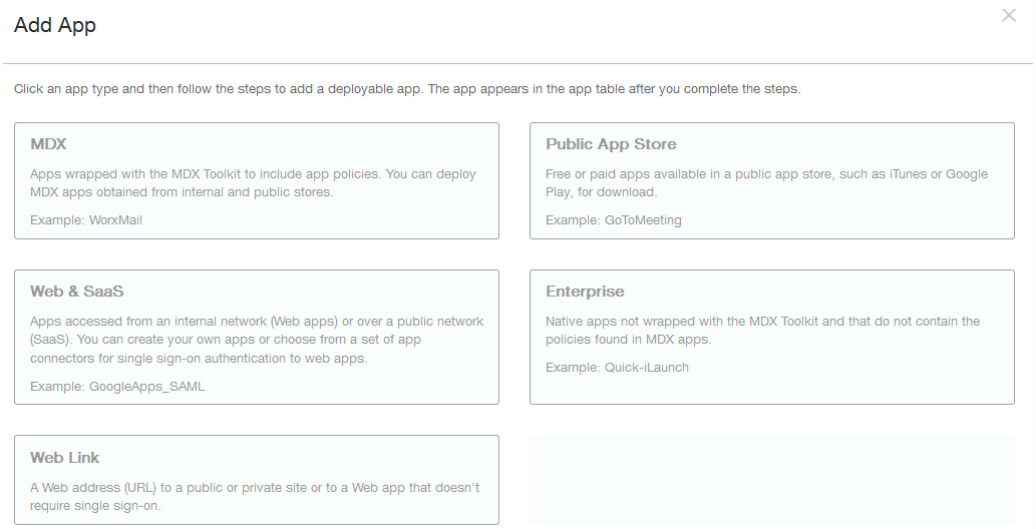


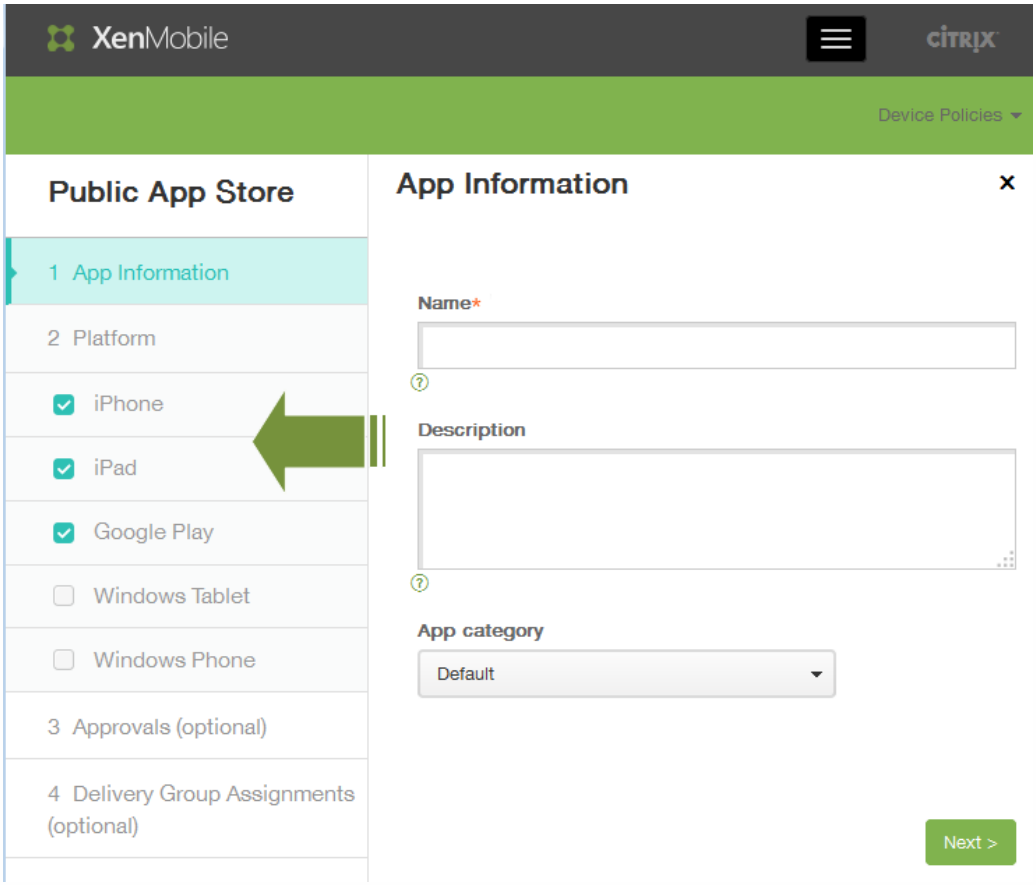


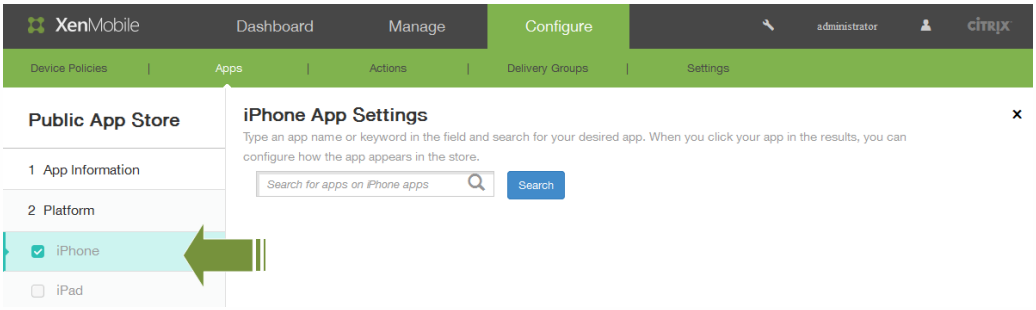


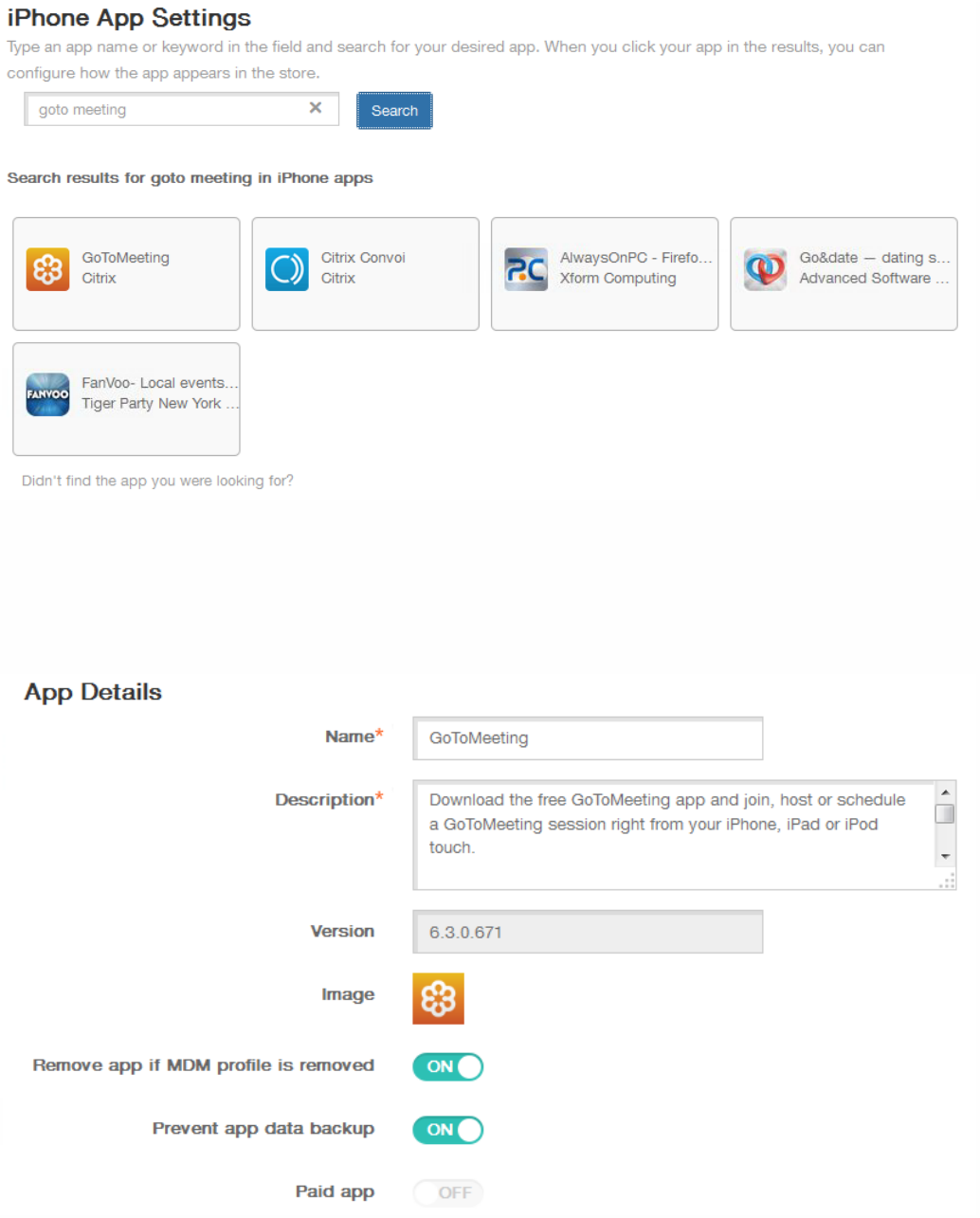
パブリックアプリケーションストアのアプリケーションをXenMobileに追加するには

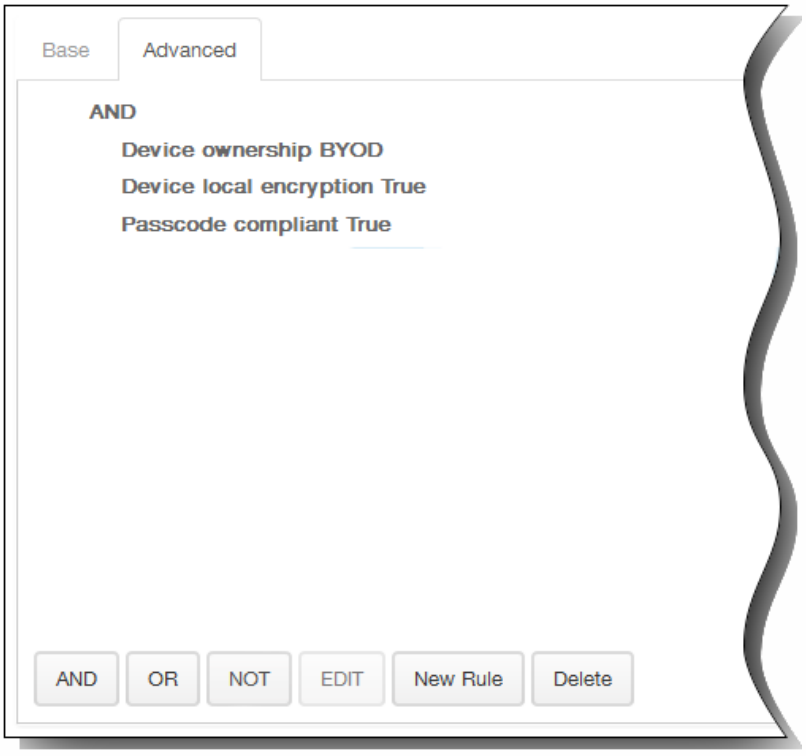


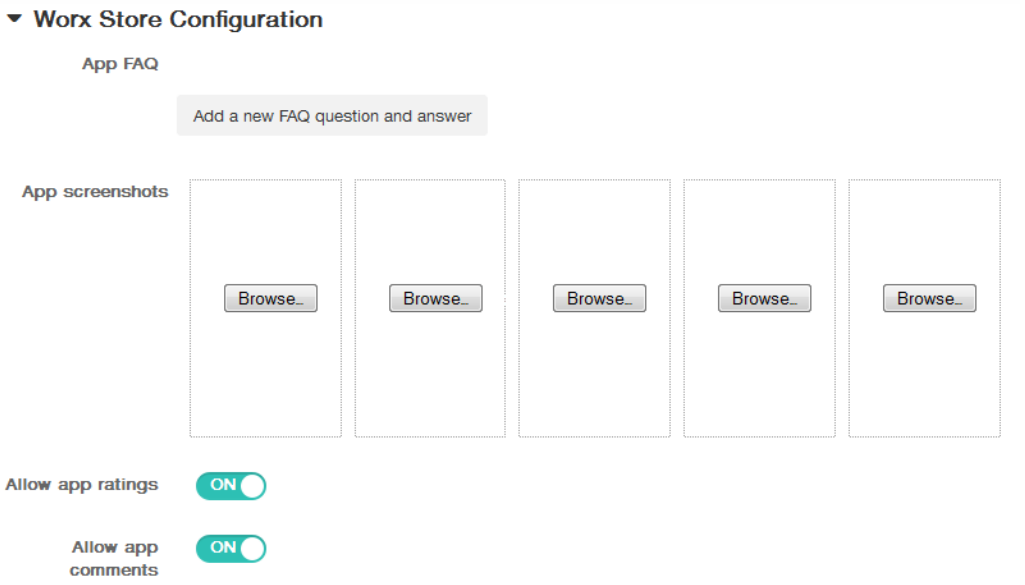


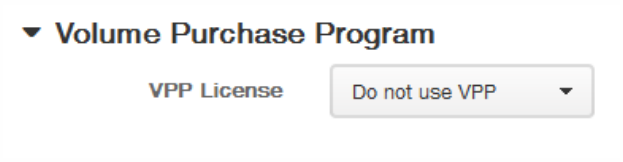


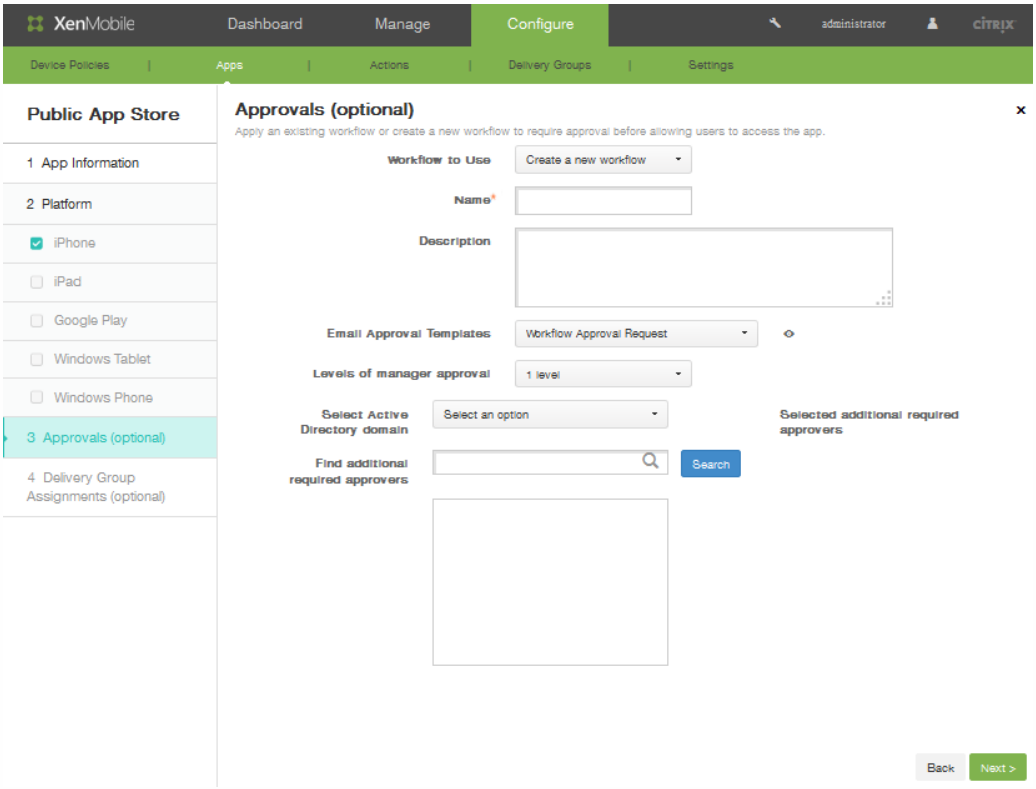


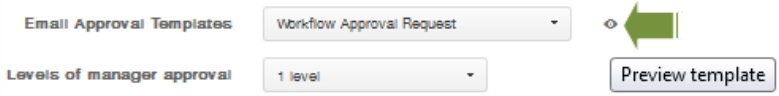


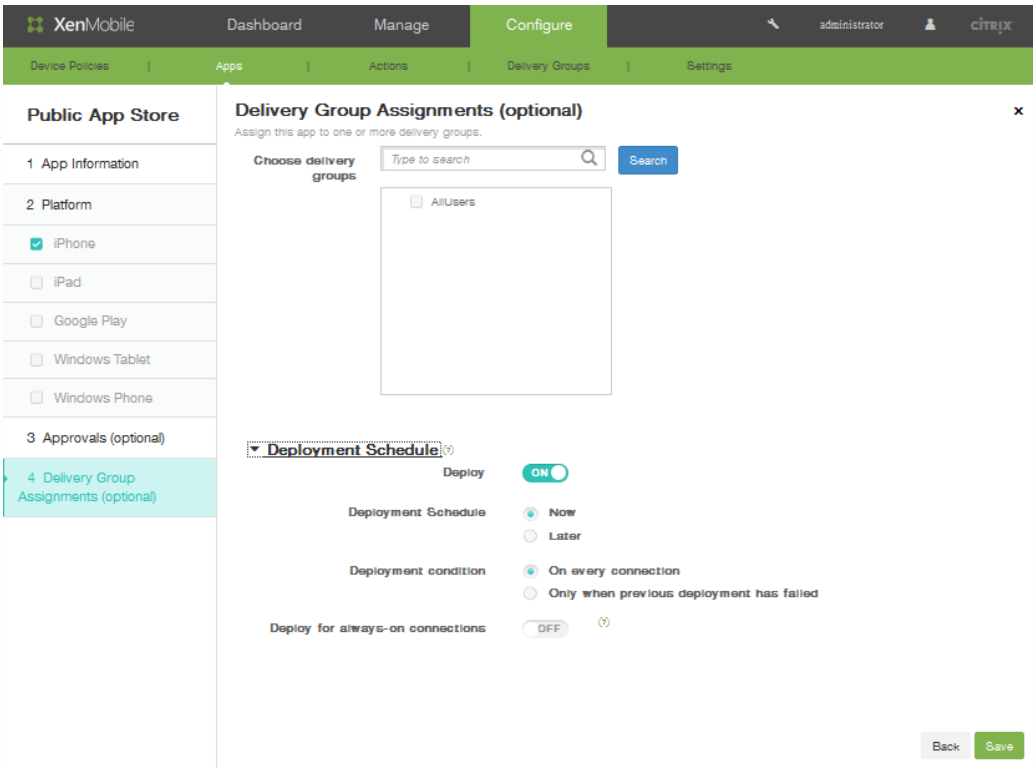








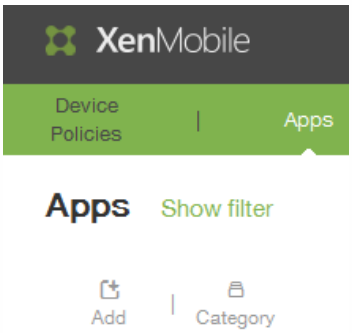


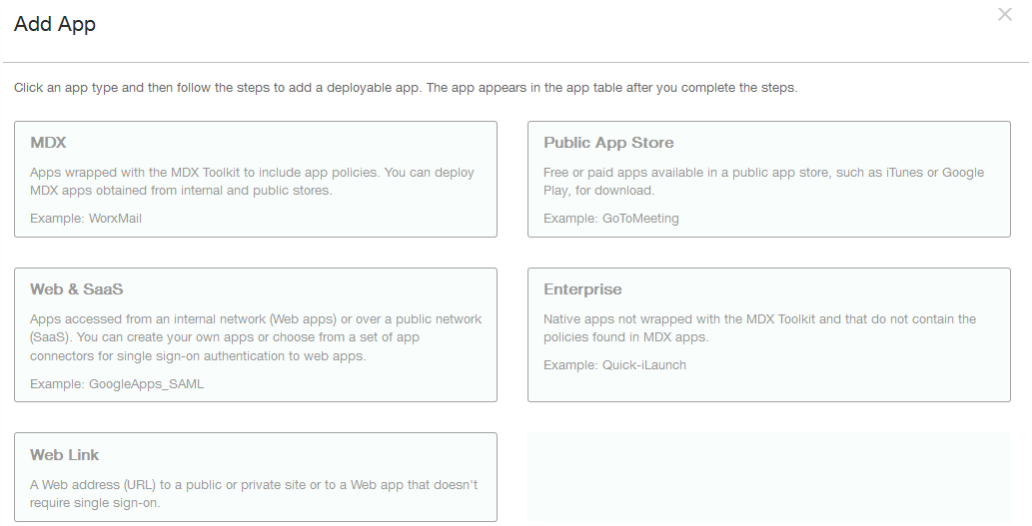


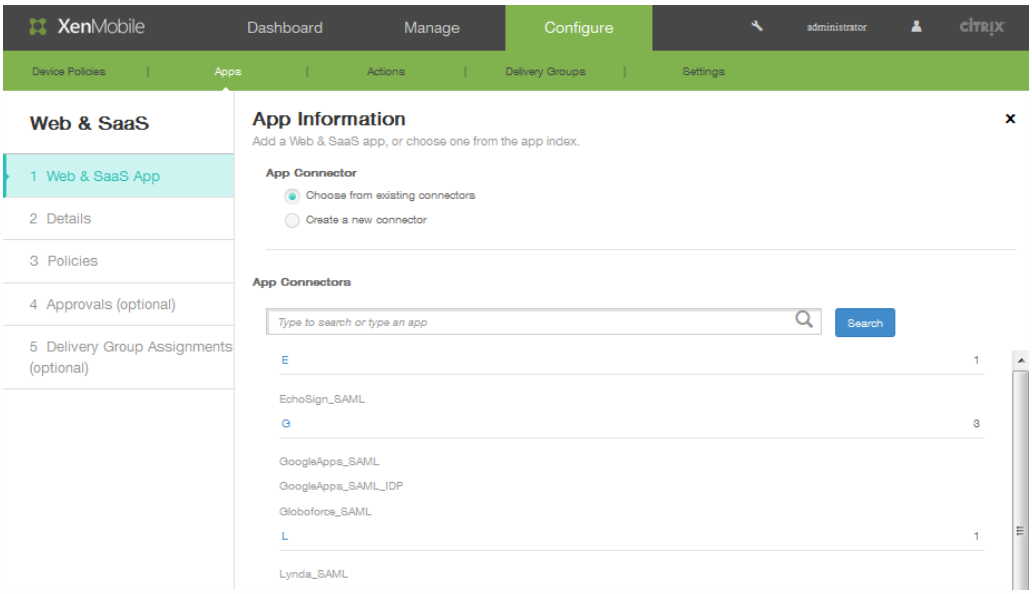
WebおよびSaaSアプリケーションをXenMobileに追加するには

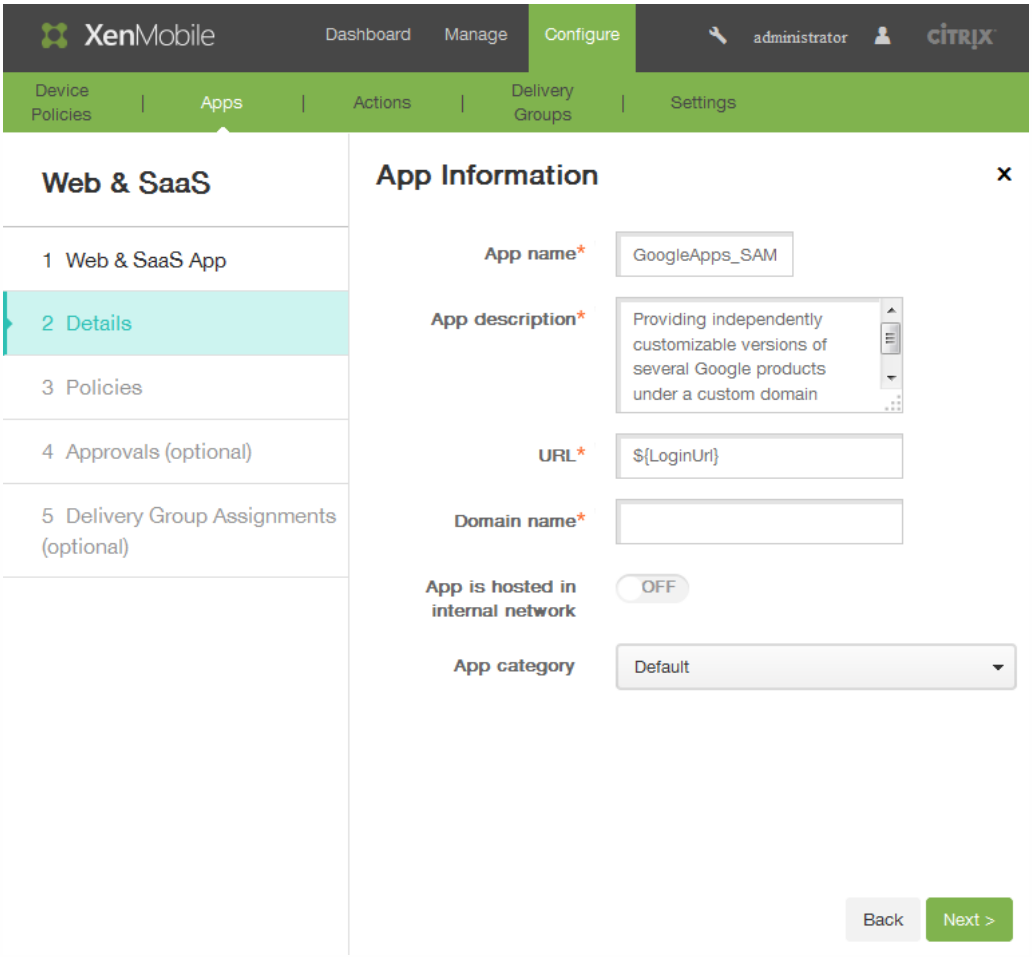
-
-
-
-
-
-
-
-

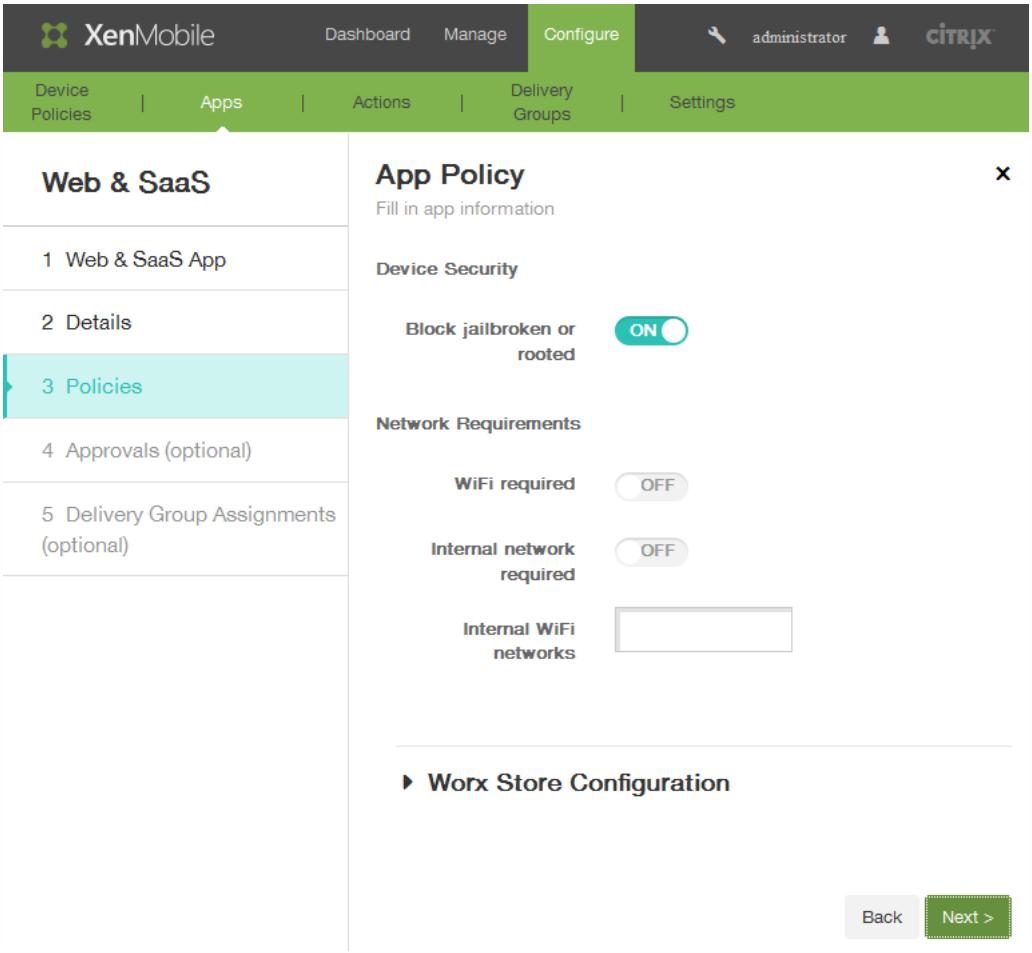
XenMobileでアプリケーションコネクタを追加するには

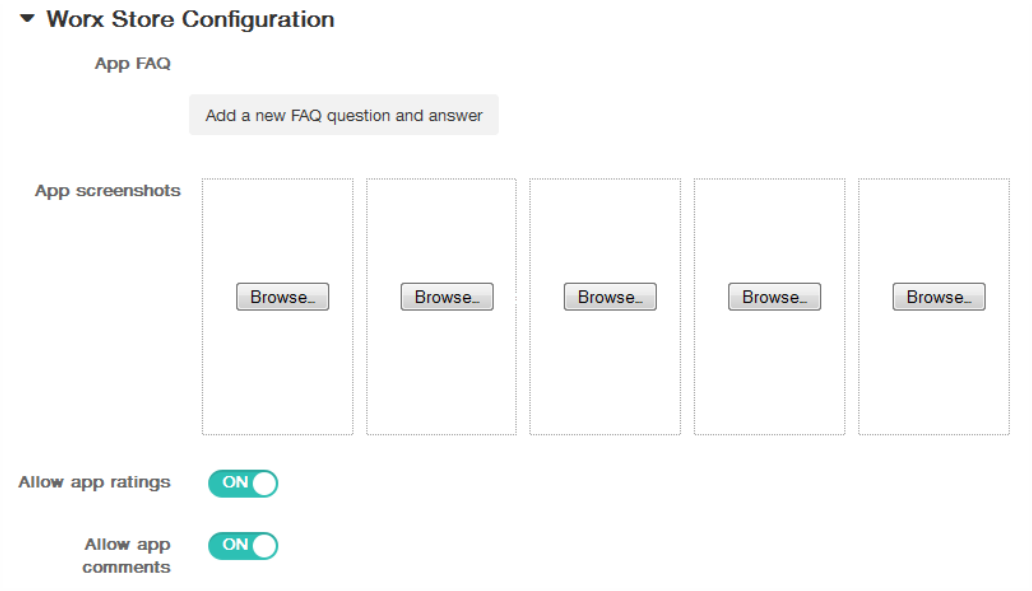


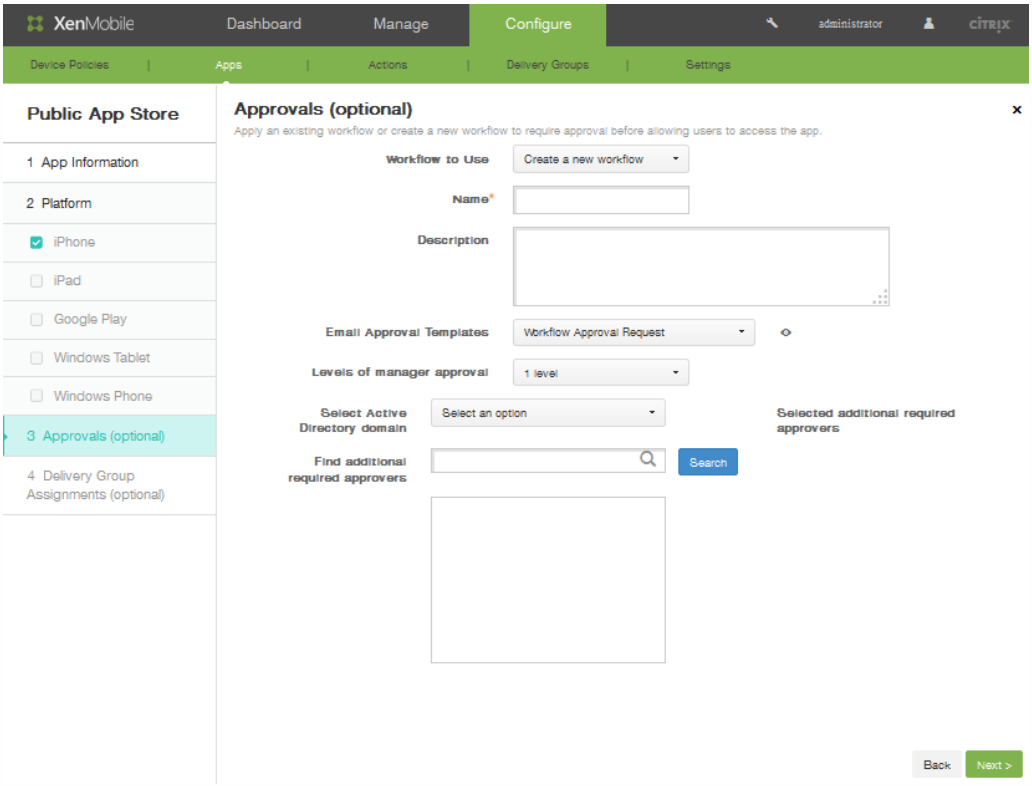


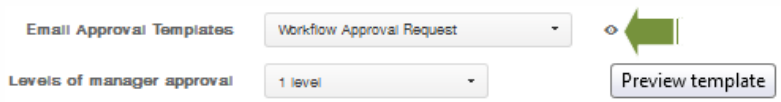


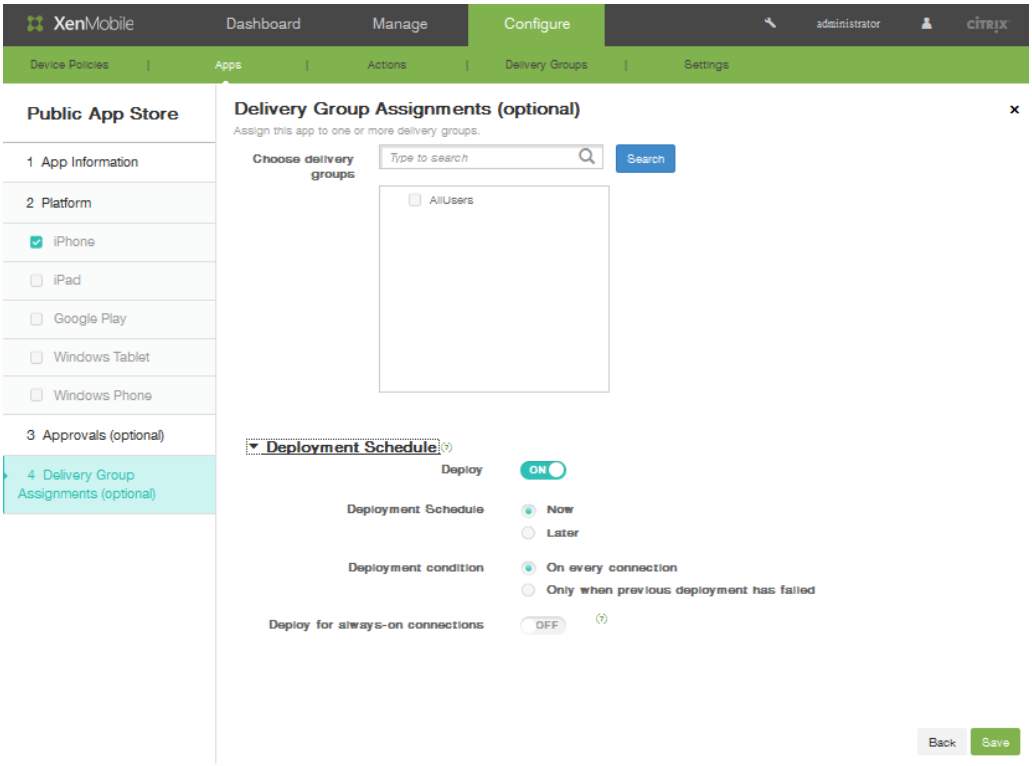


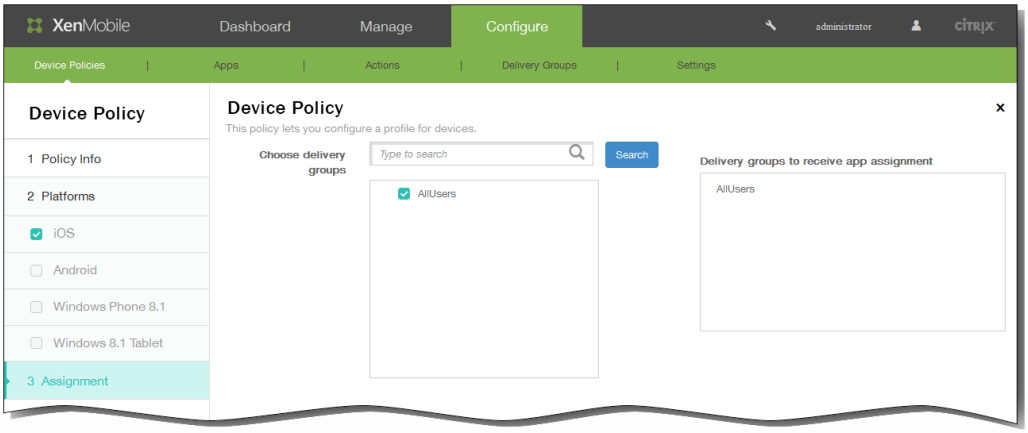


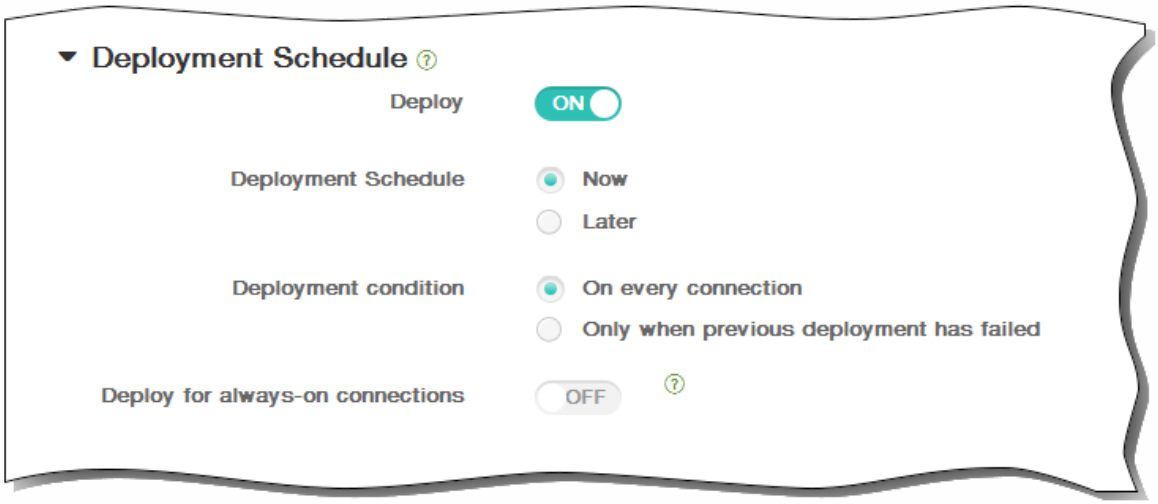










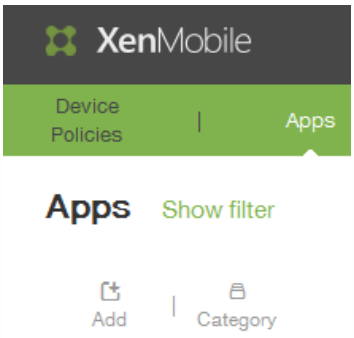


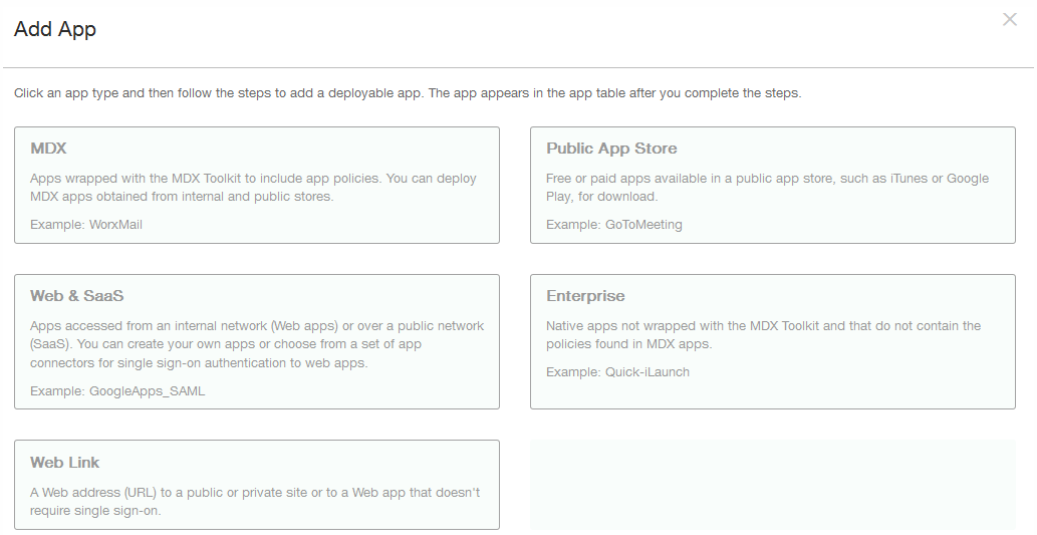
Application Connectorの種類の一覧

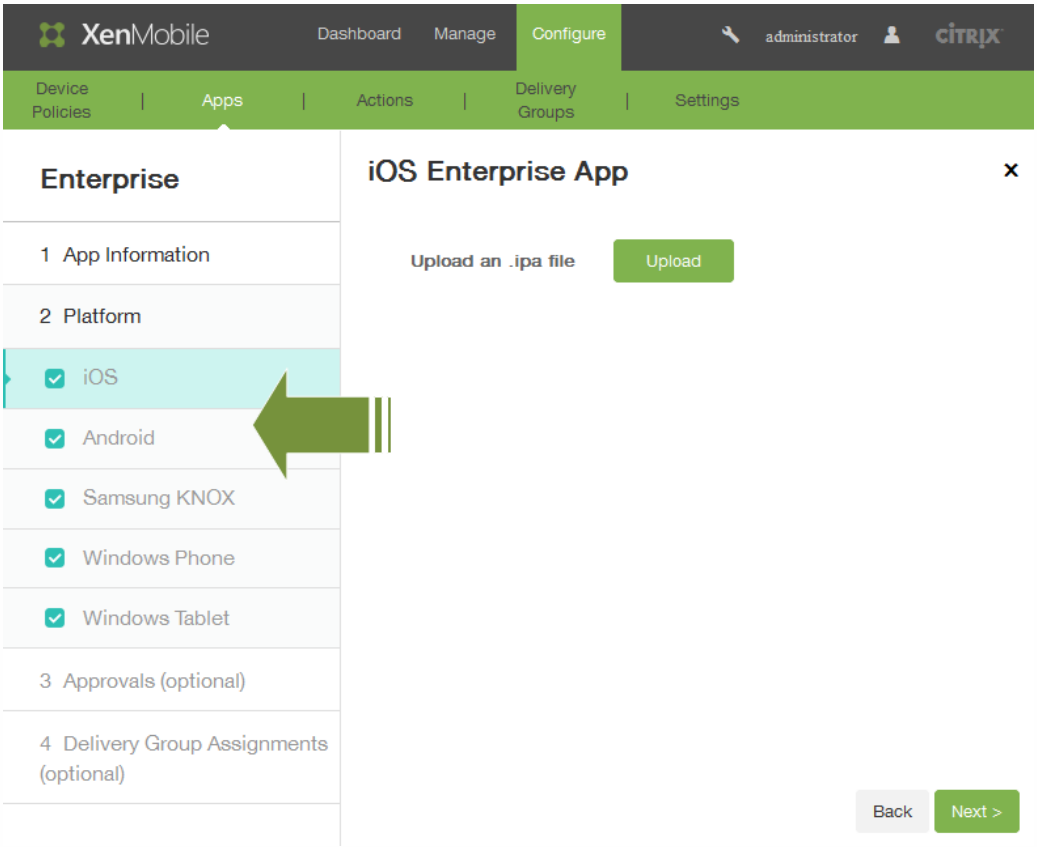
エンタープライズアプリケーションをXenMobileに追加するには

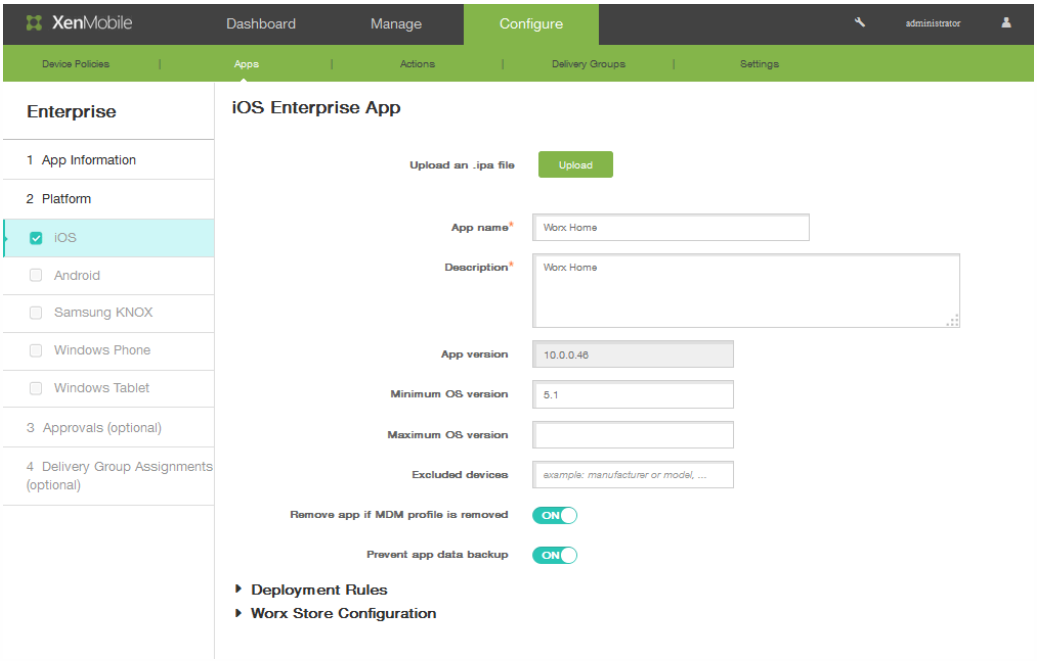
-
-
-
-
-

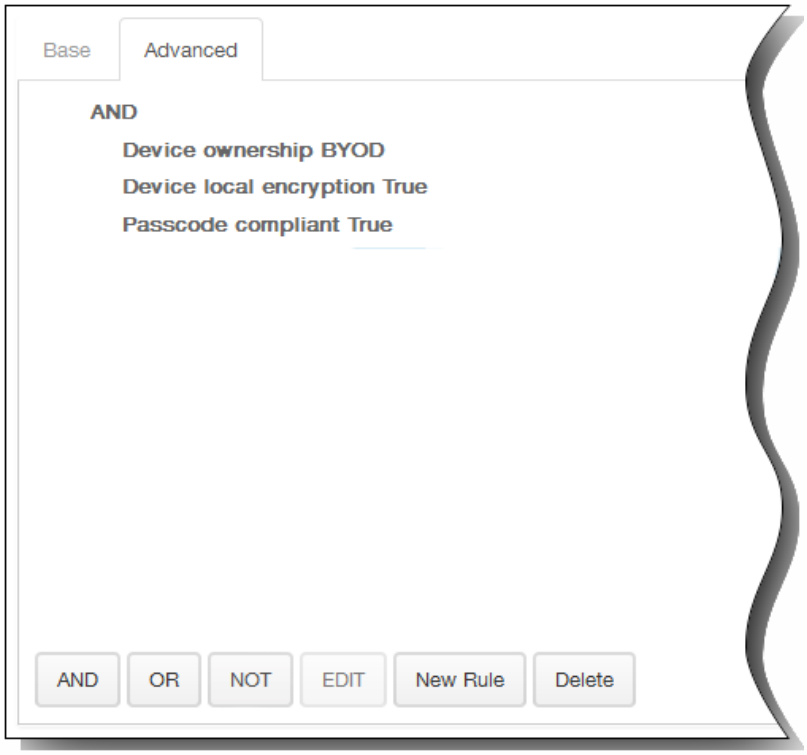
エンタープライズアプリケーションを作成するには

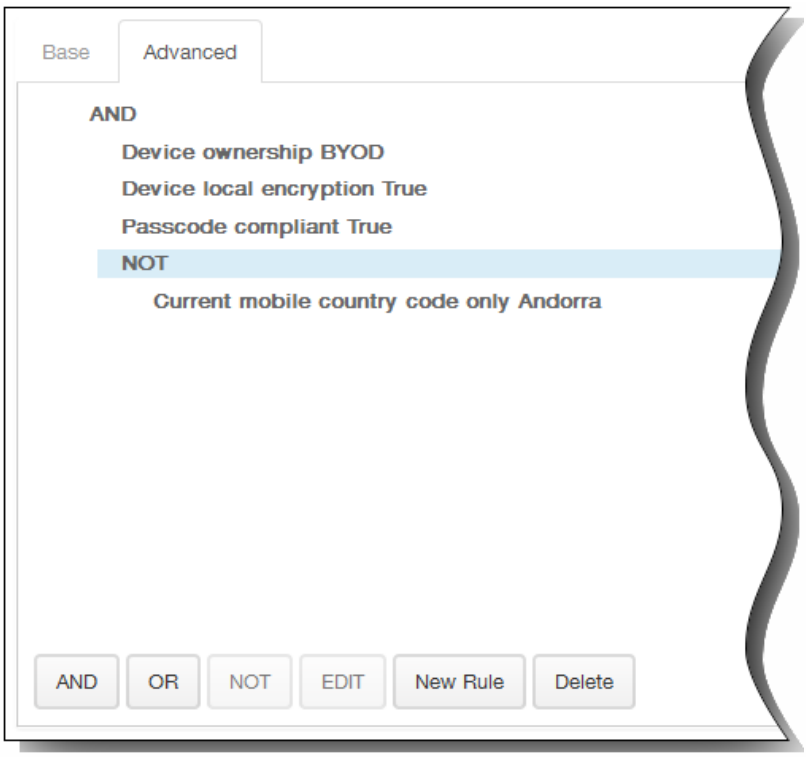


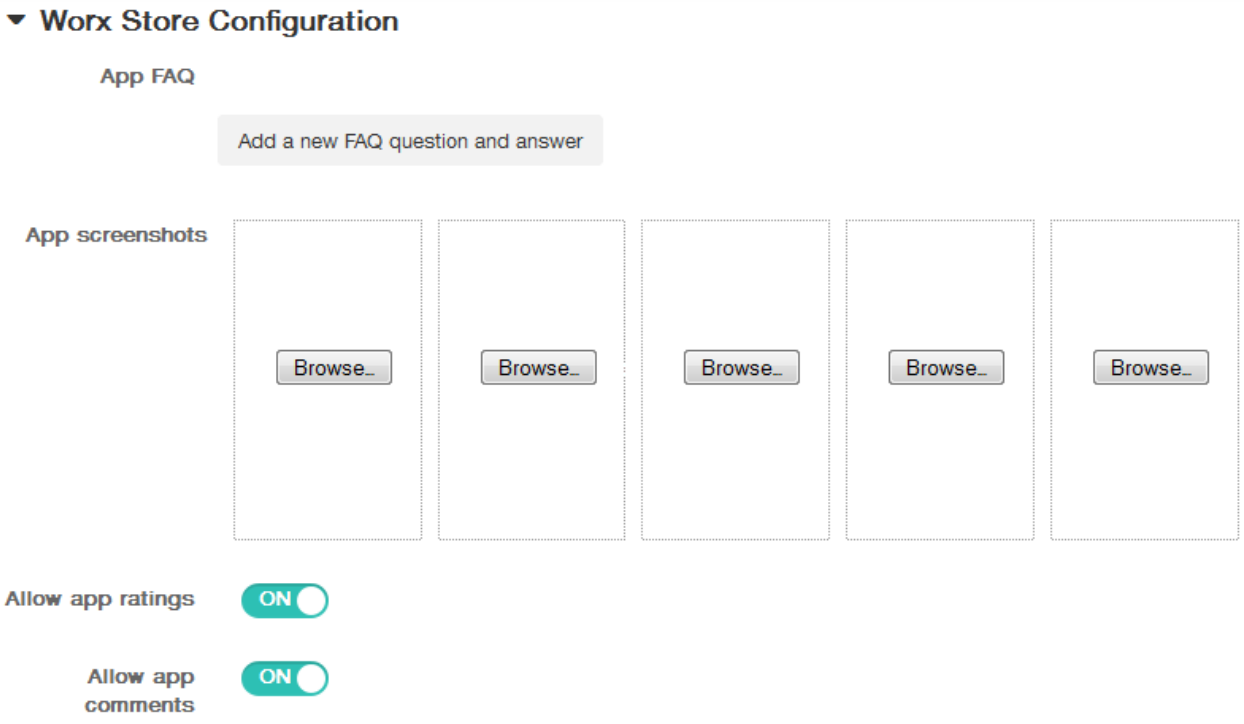


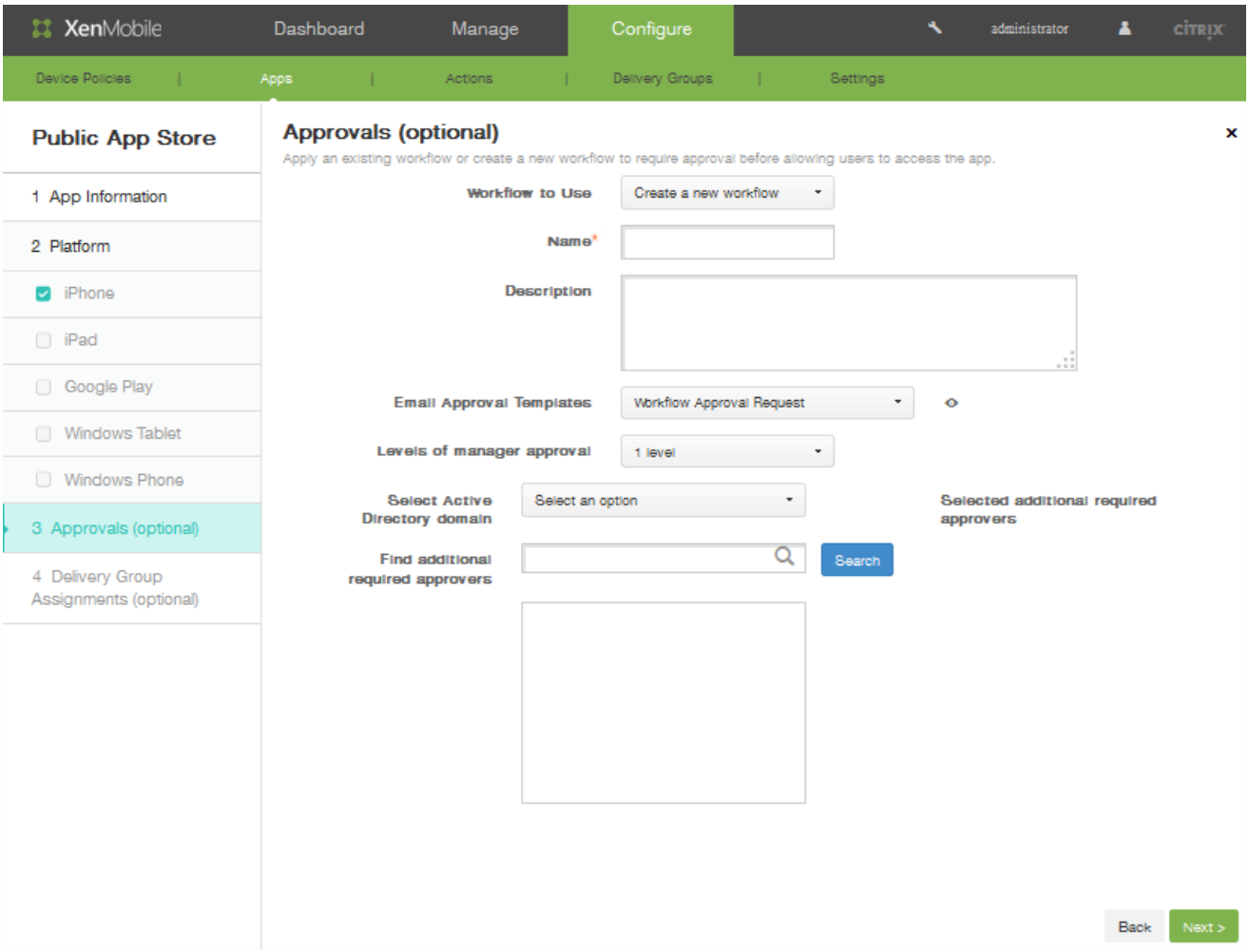


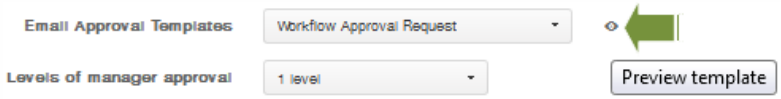


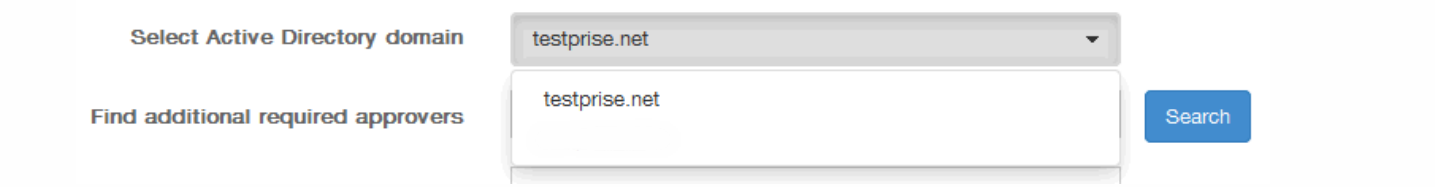


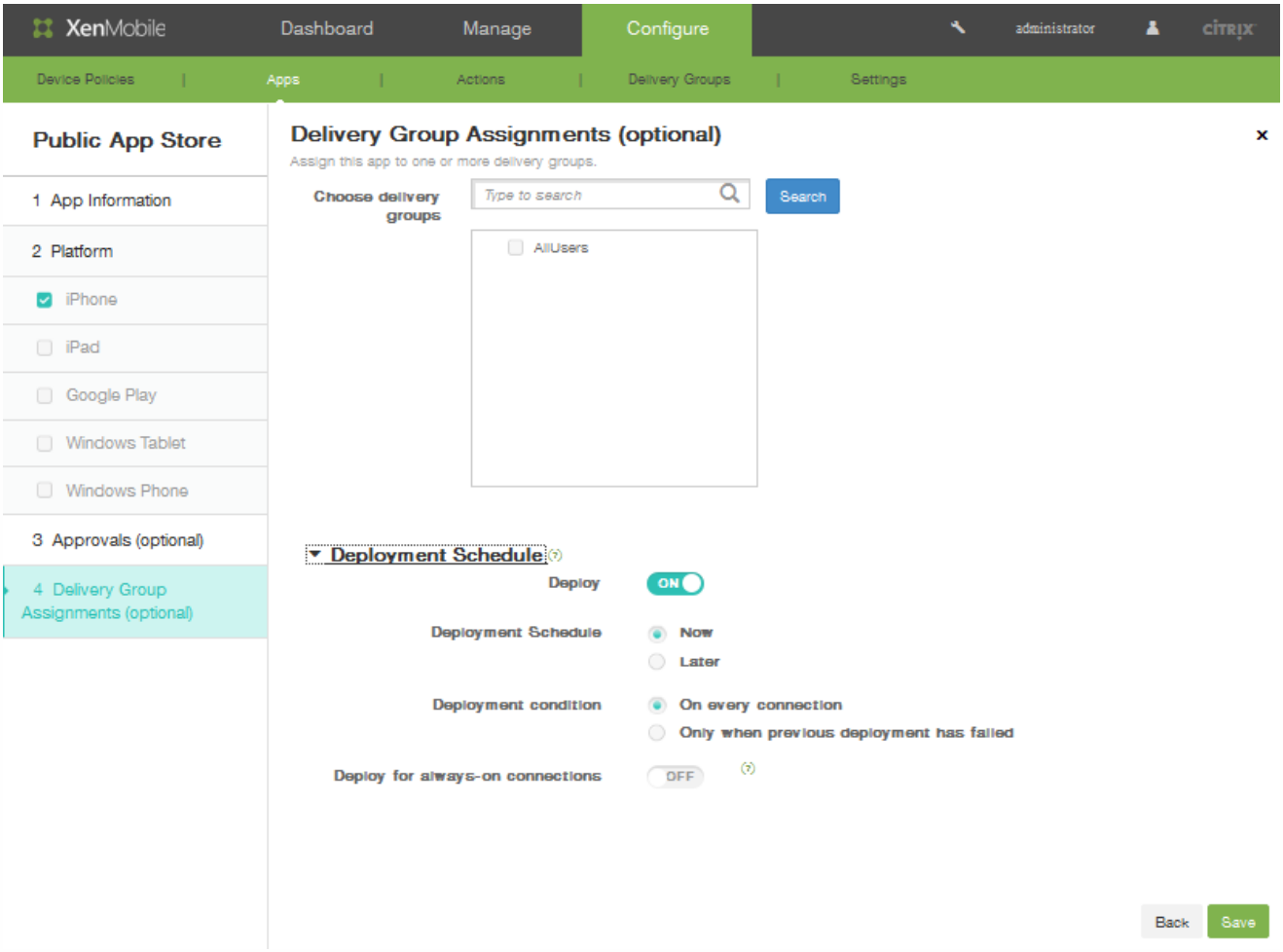






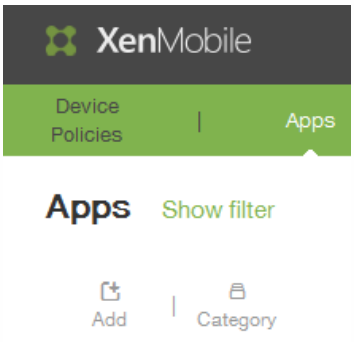


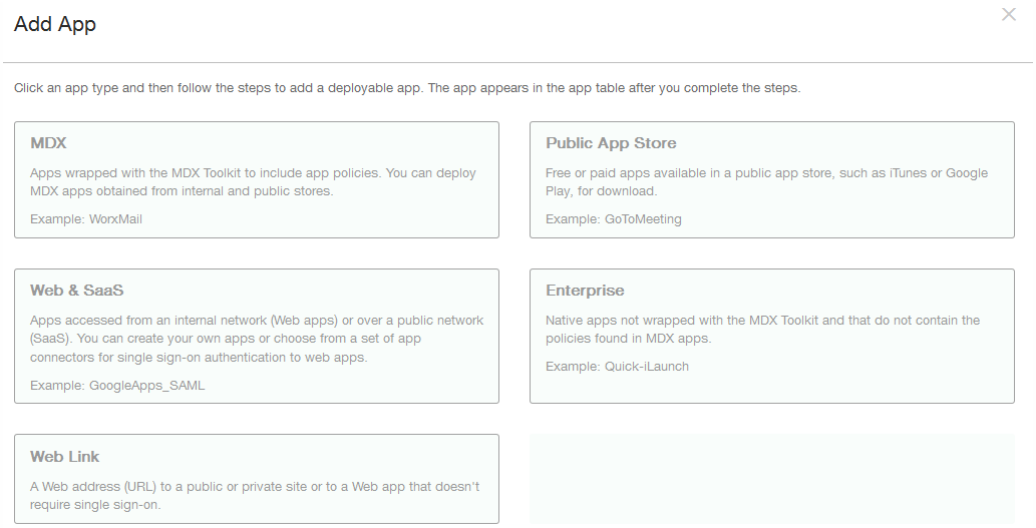


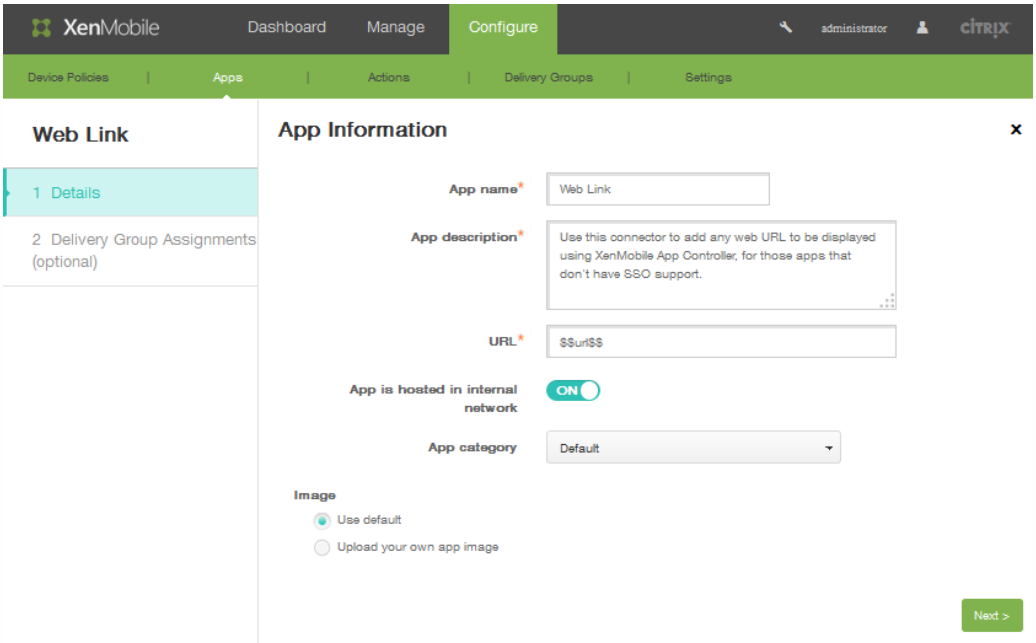


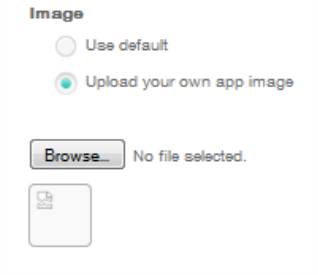
Webリンクアプリケーションを XenMobile に追加するには

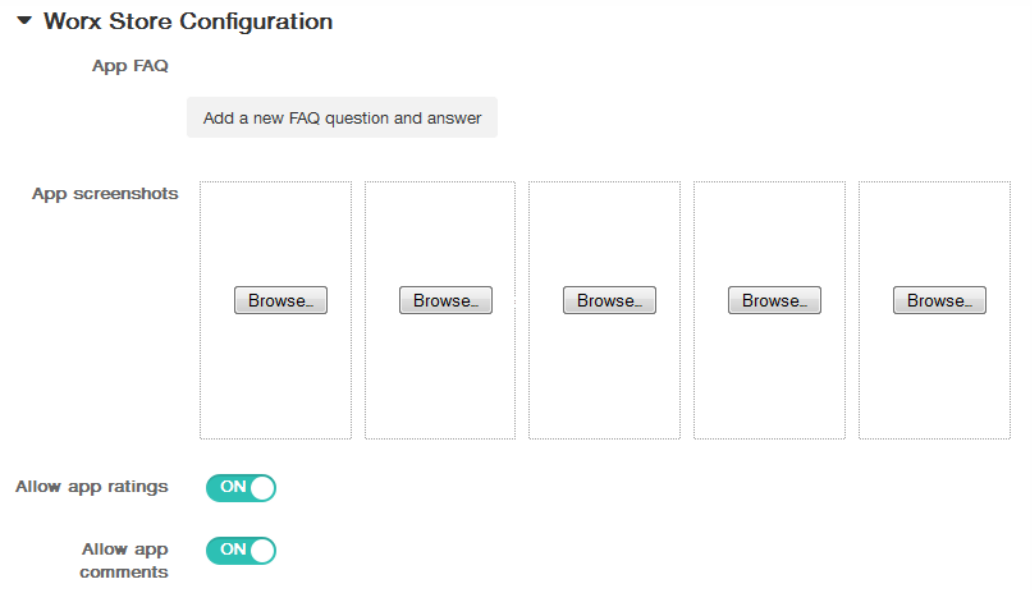
-
-
-
-
-
-

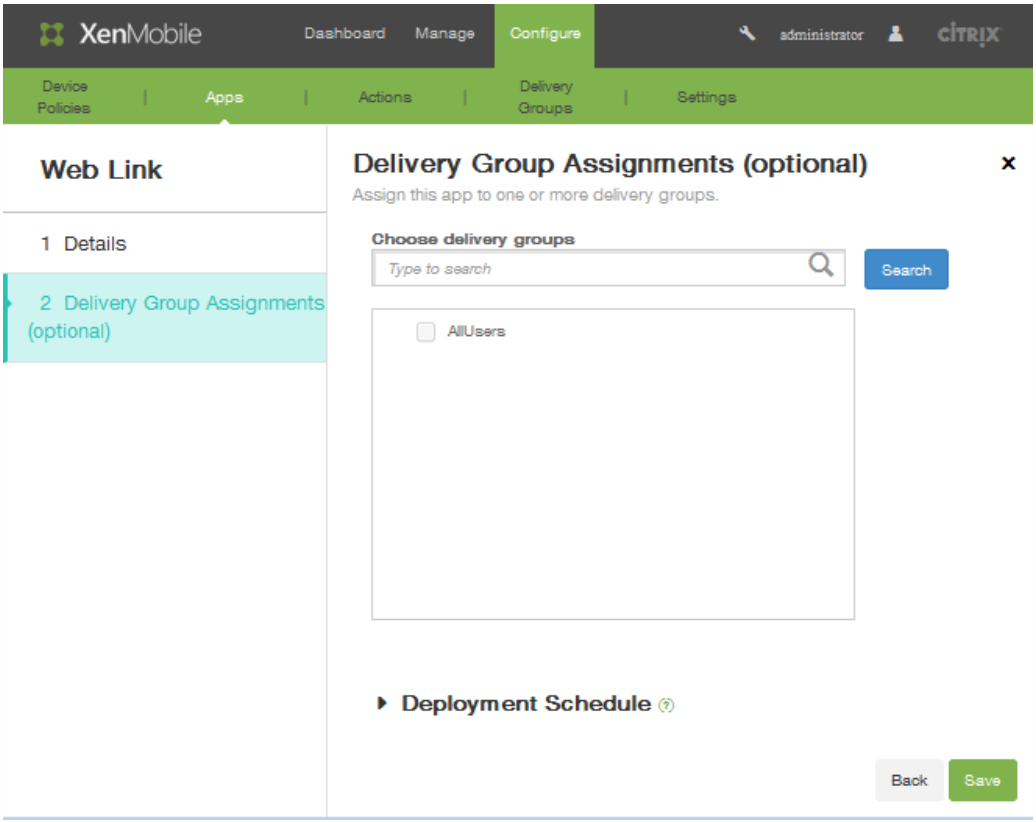


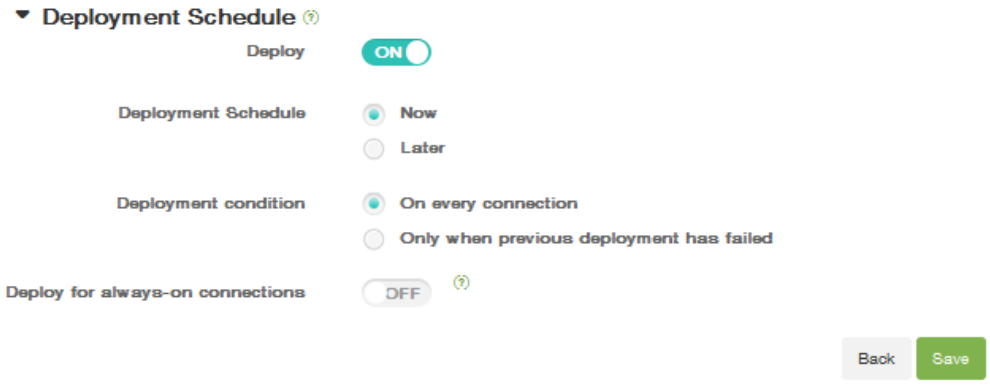






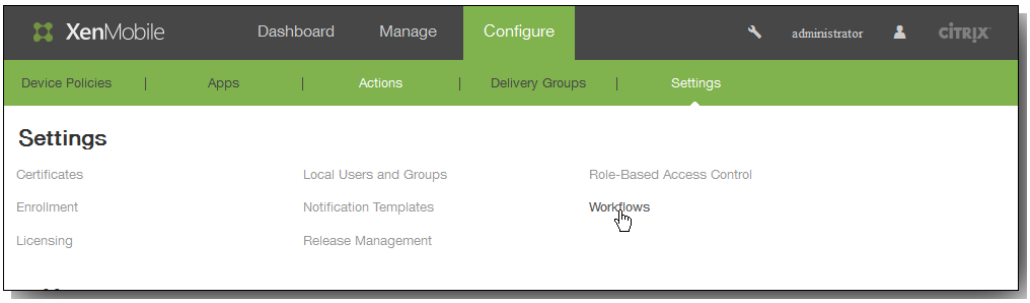


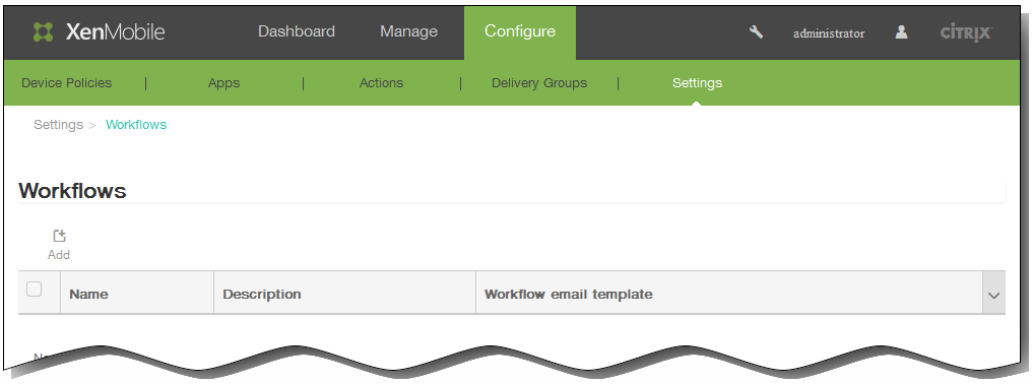


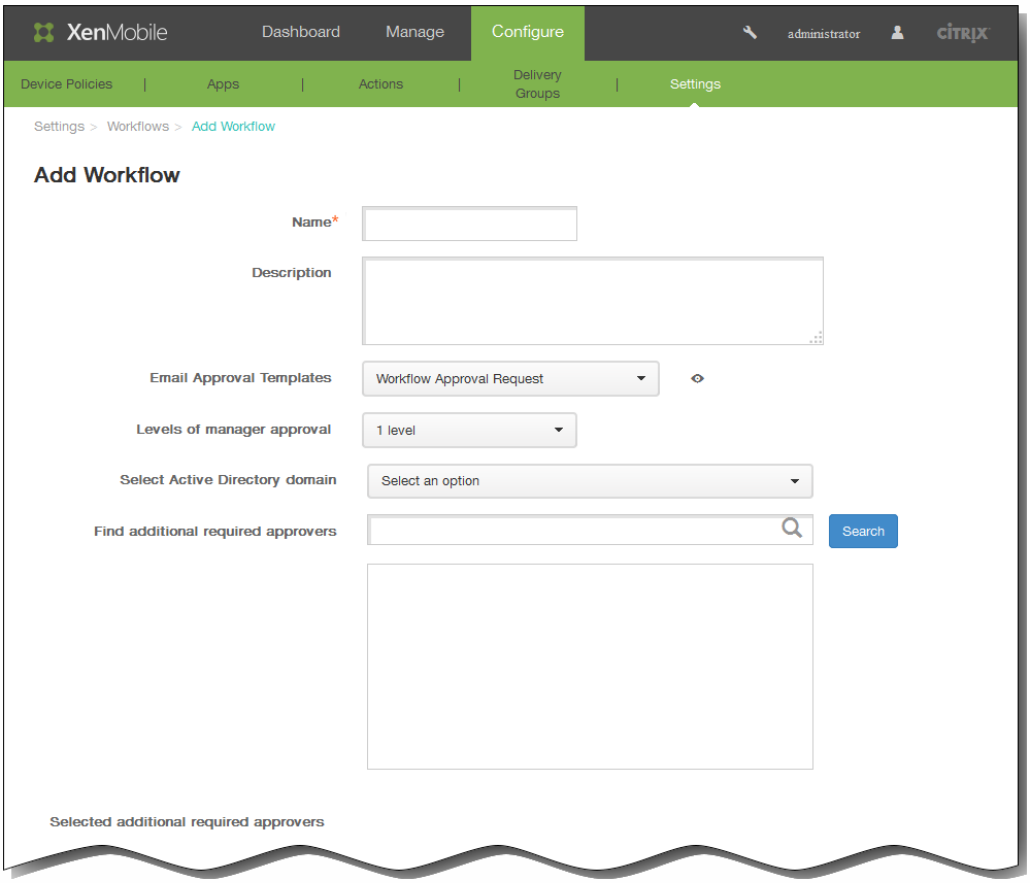


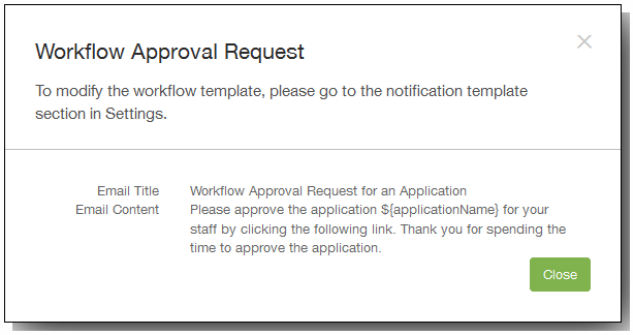
ワークフローを作成および管理するには

-
-





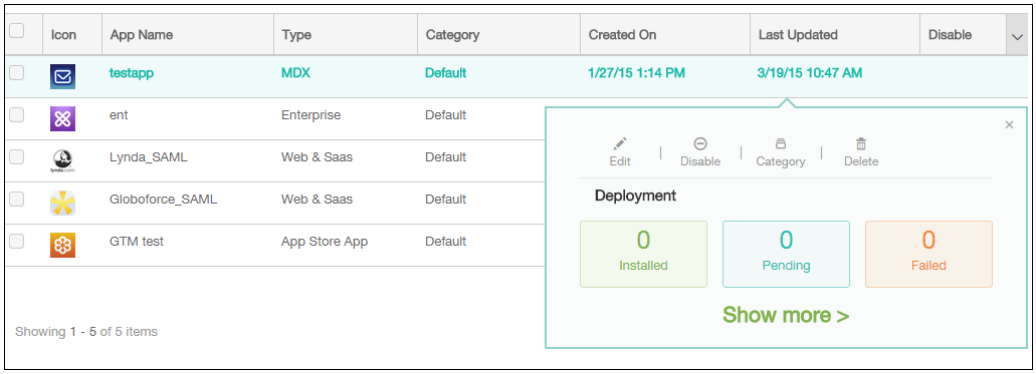


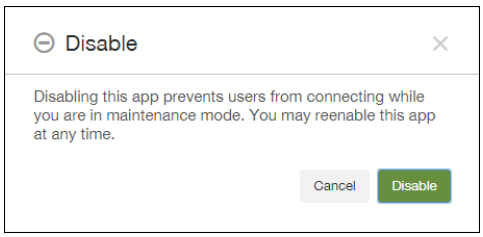


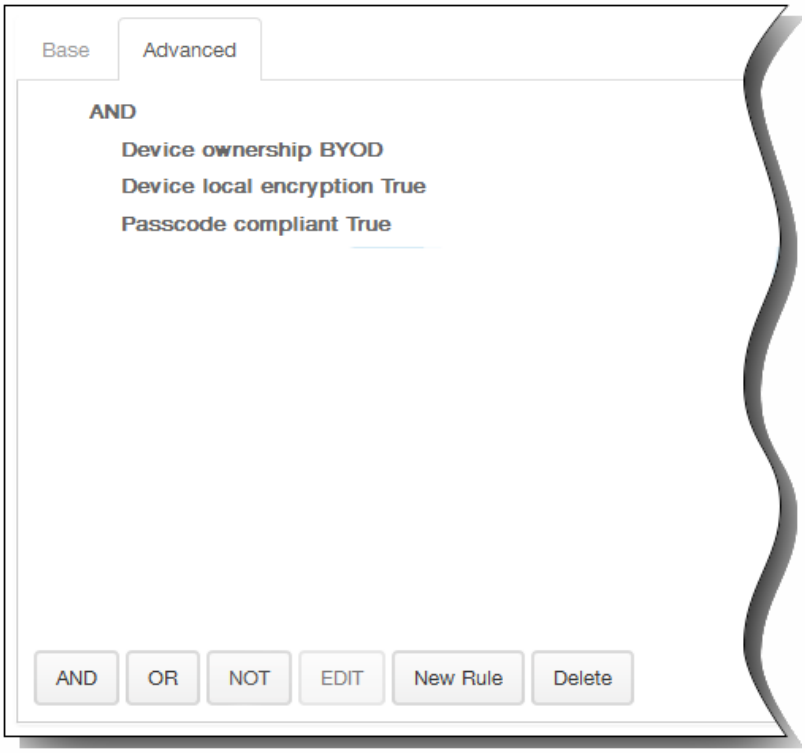
-
-

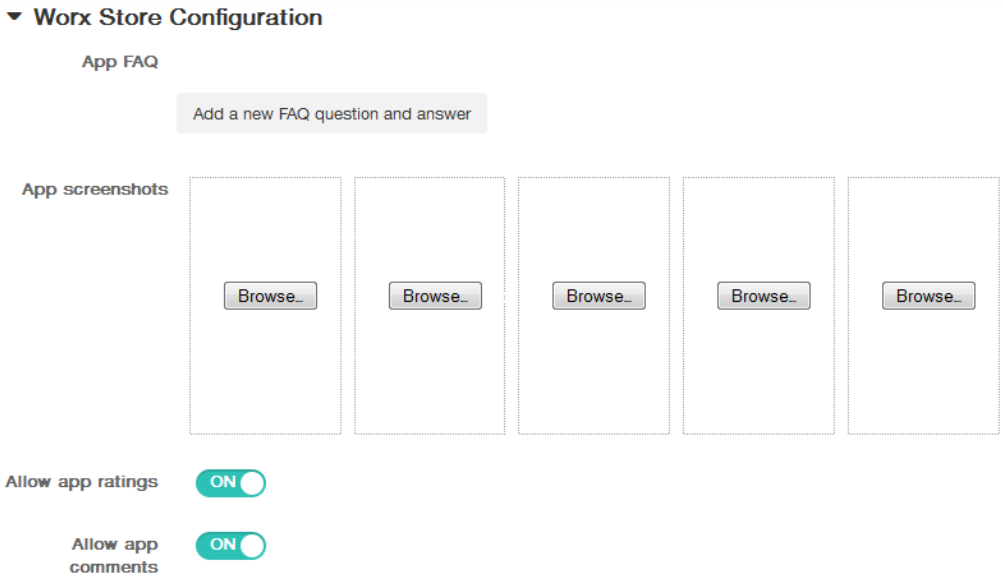
ワークフローの詳細の表示および削除を行うには

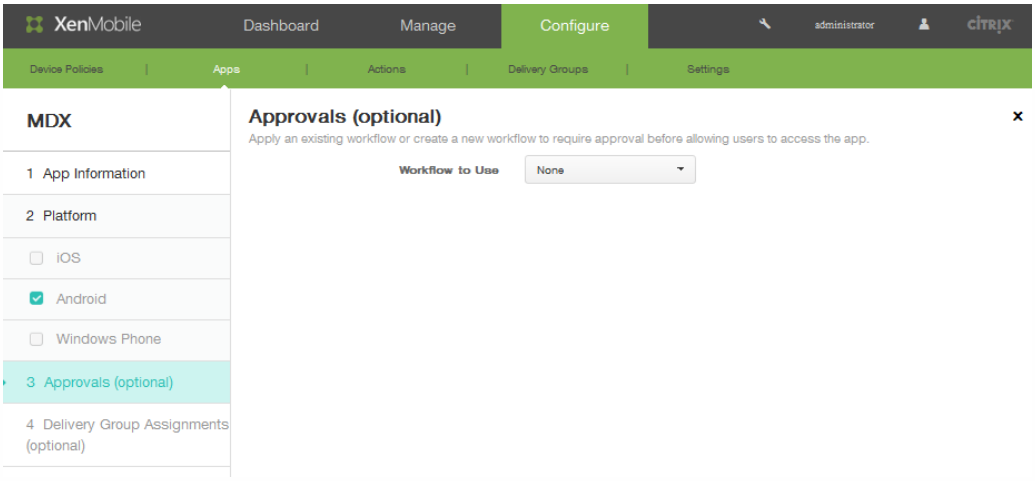
XenMobileでのアプリケーションのアップグレード

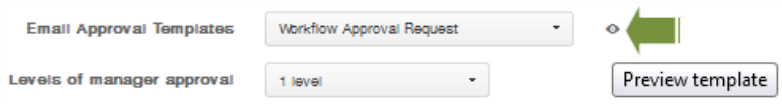


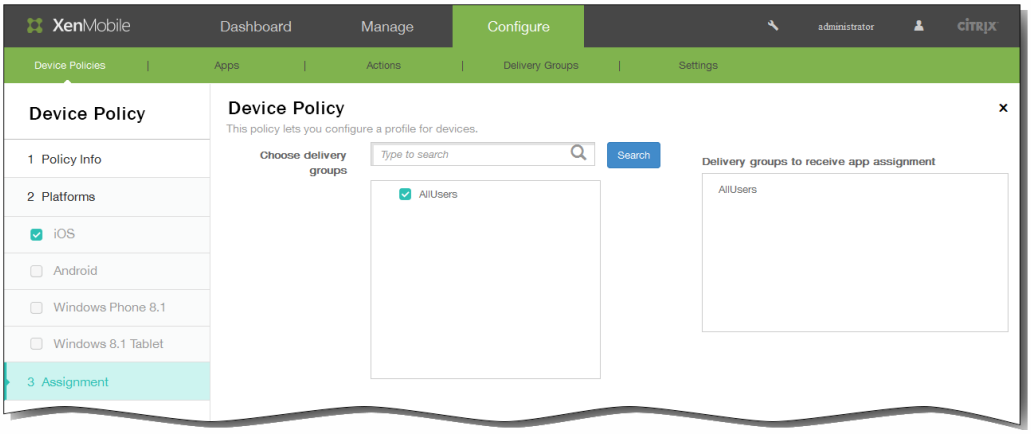


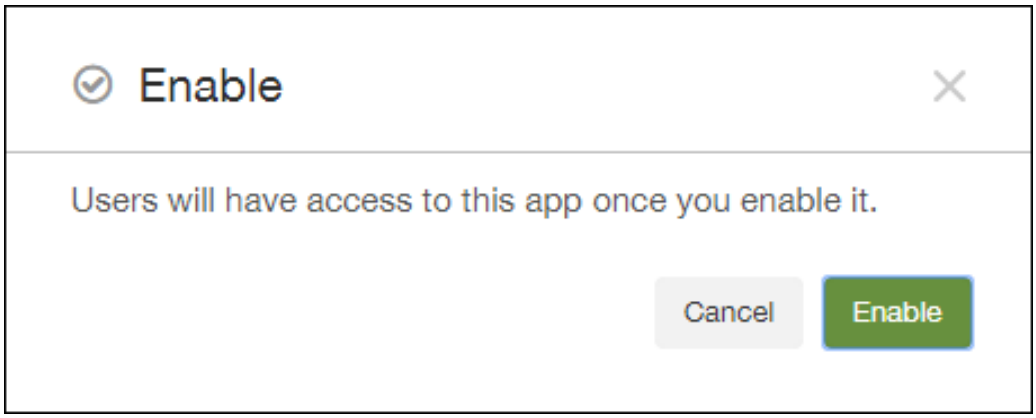








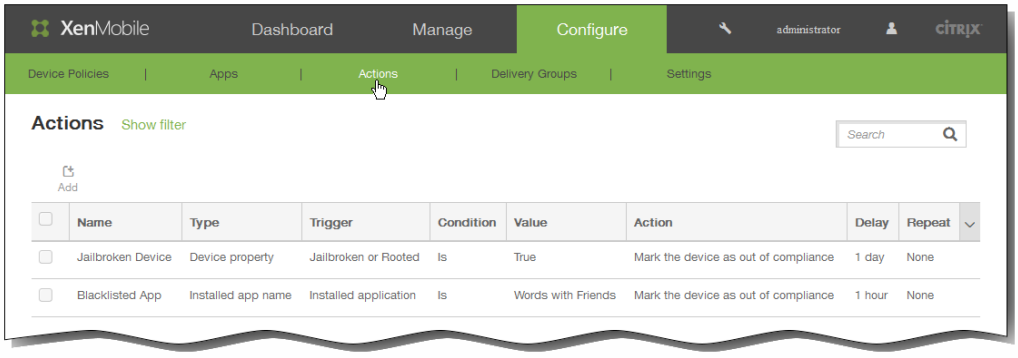




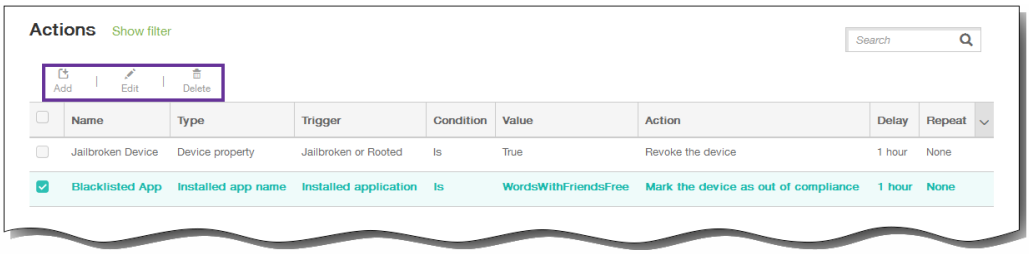
MDXアプリケーションポリシーの概要

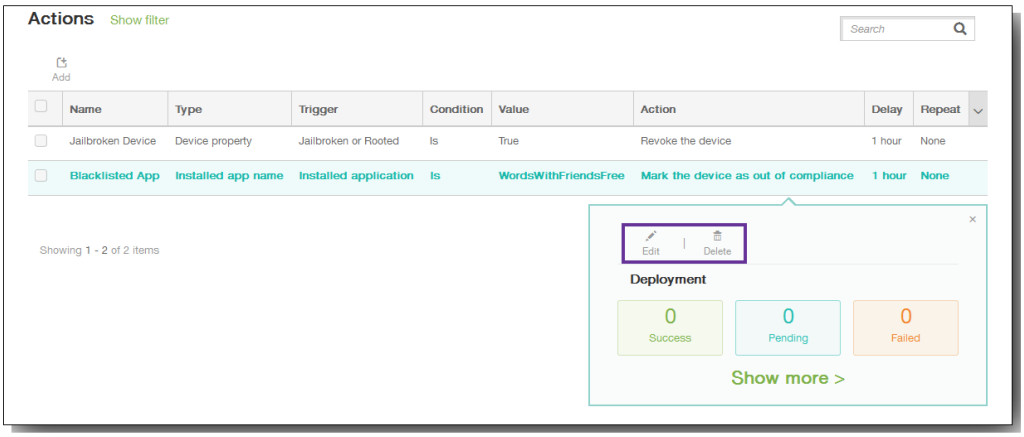
自動化された操作

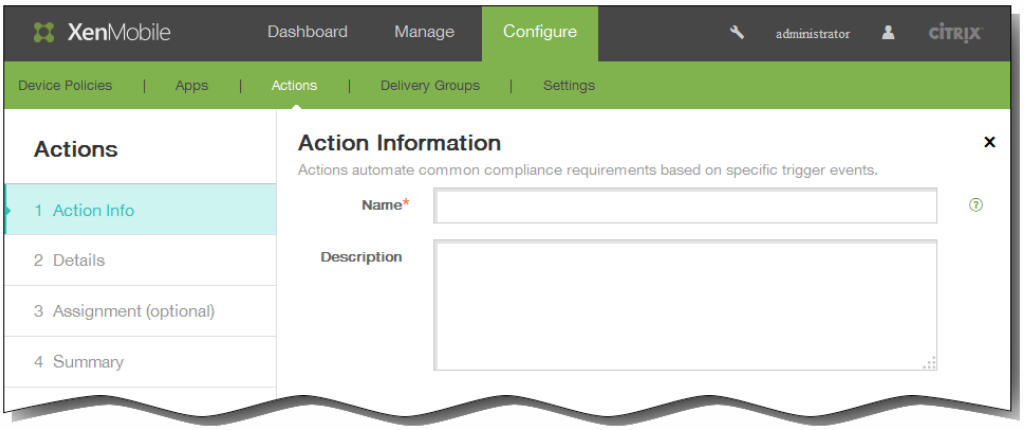
-
-
-
-

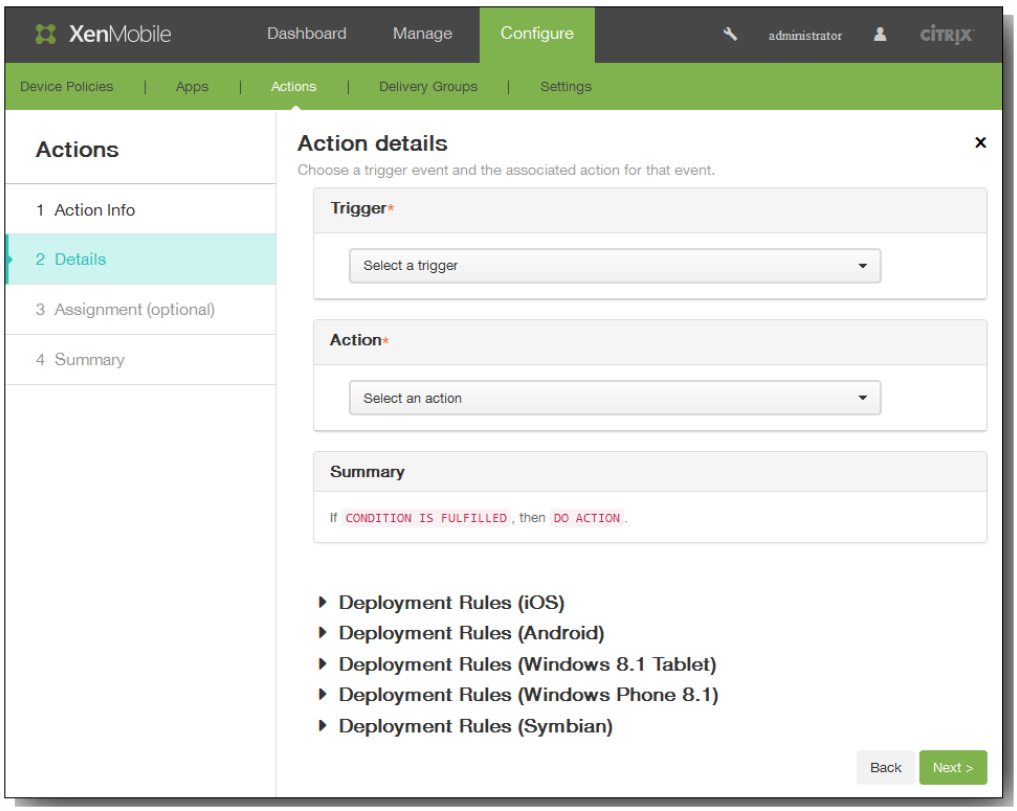


-
-

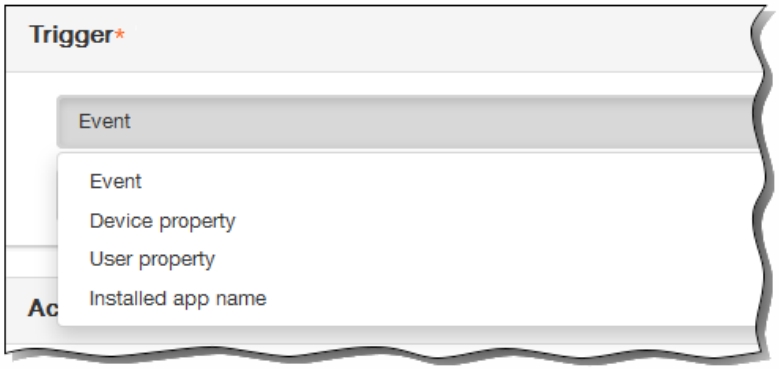


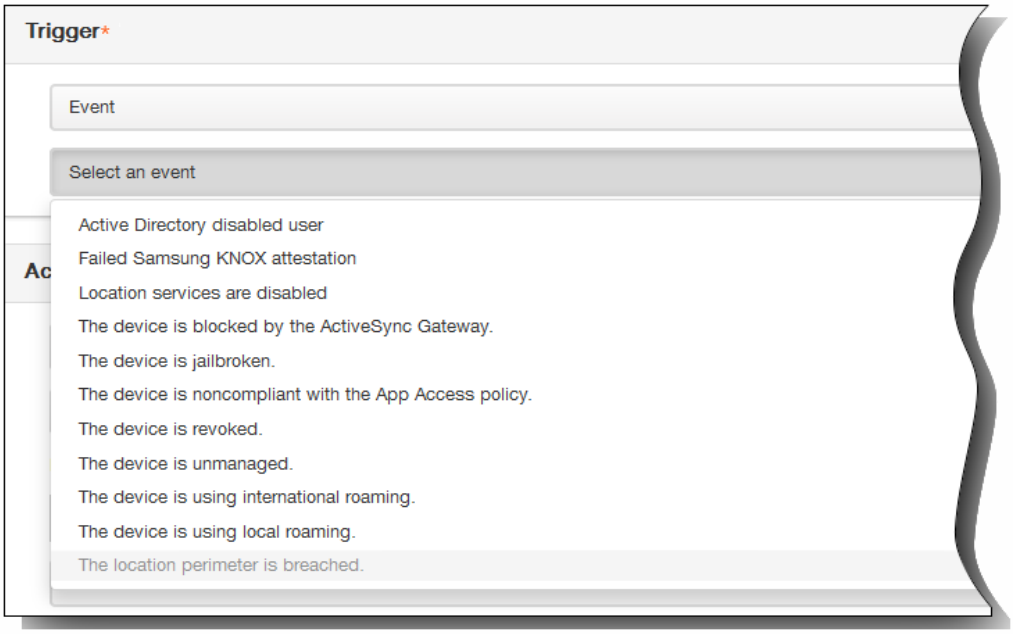


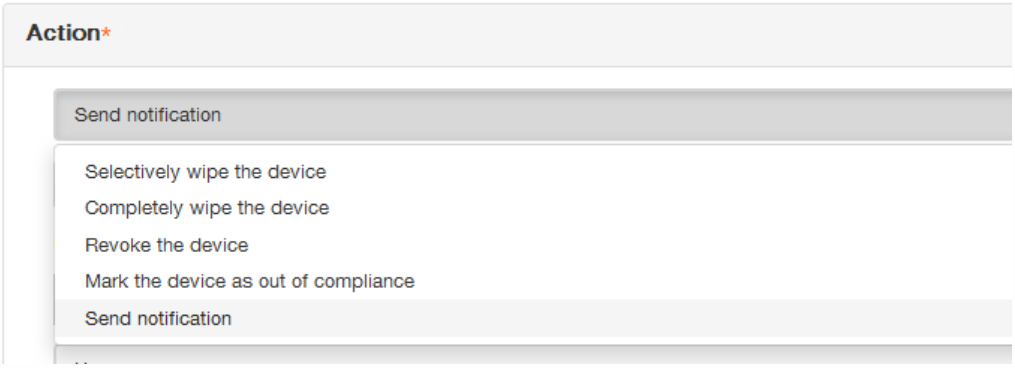


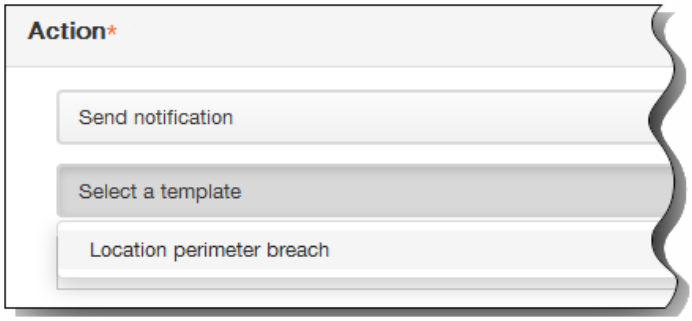


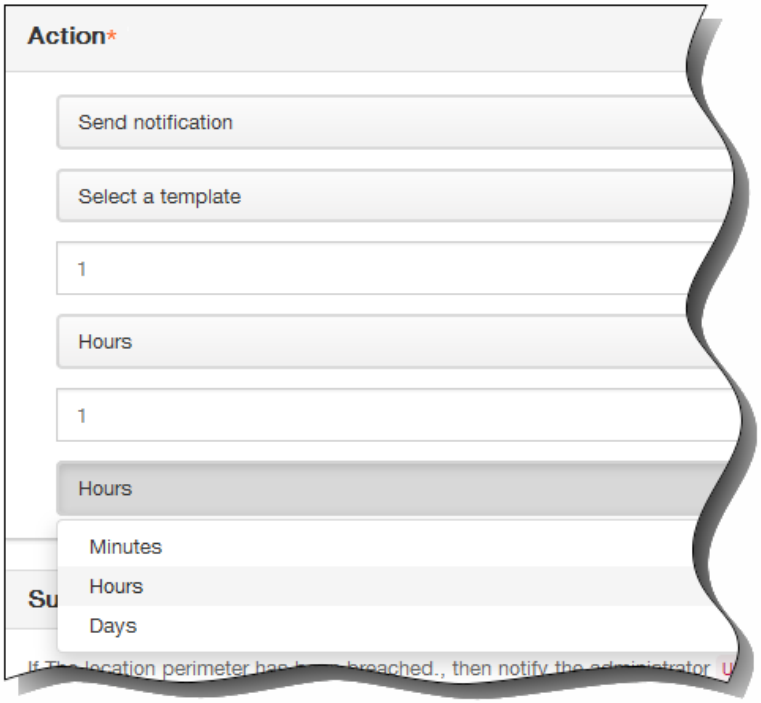
-
-
-
-

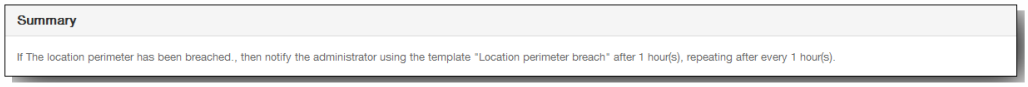


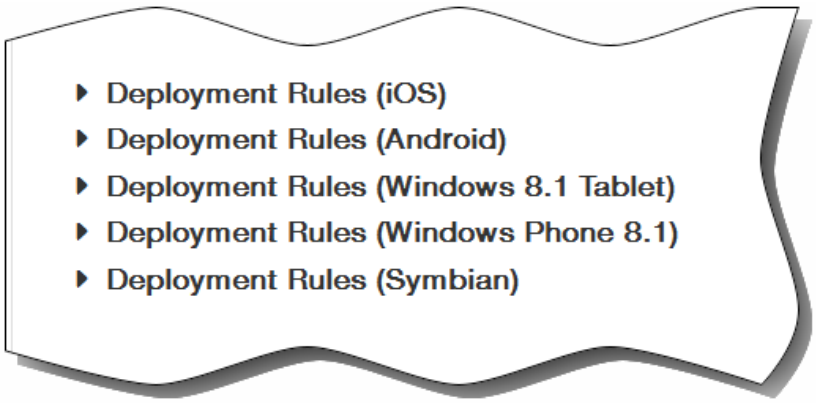


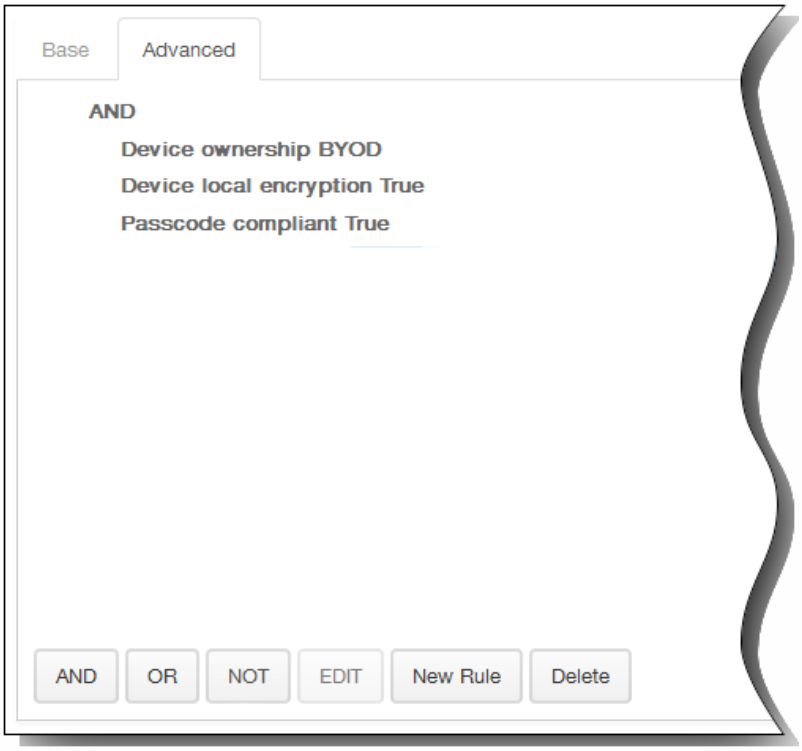


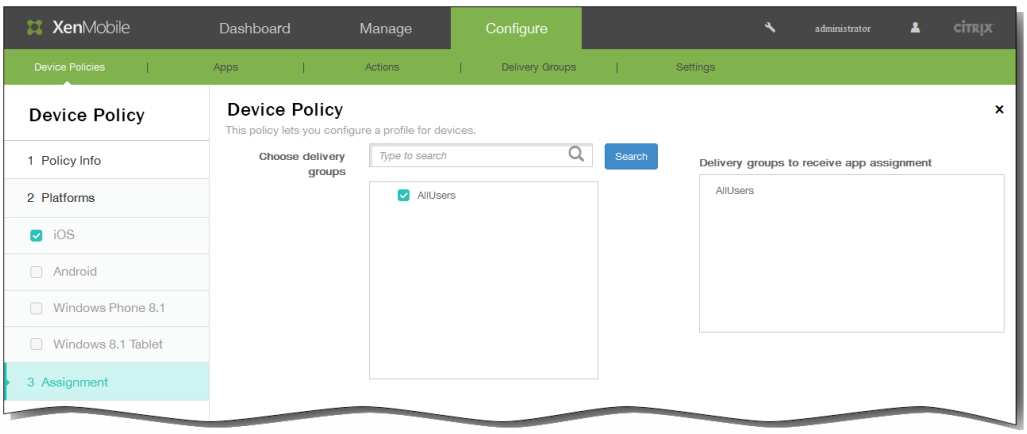


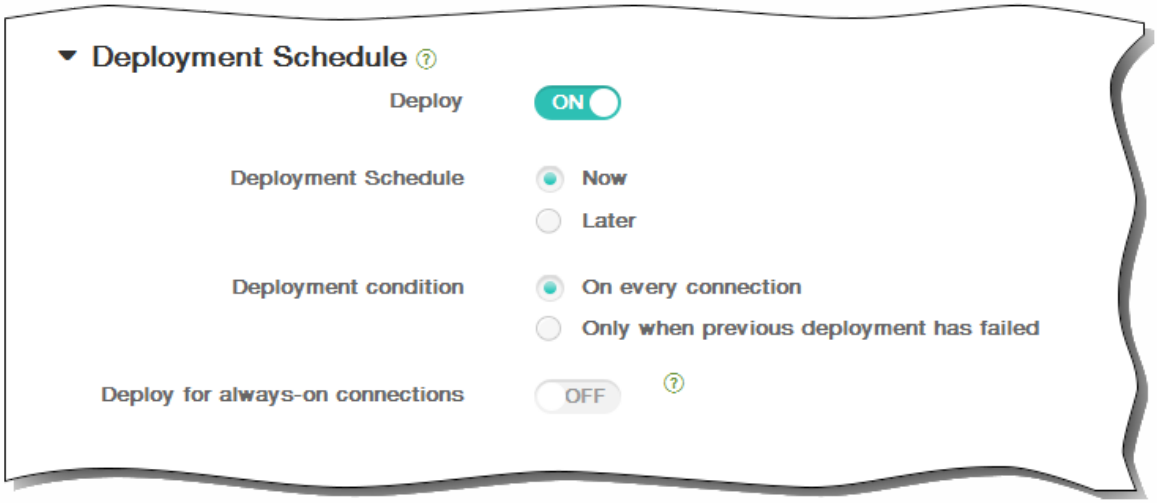


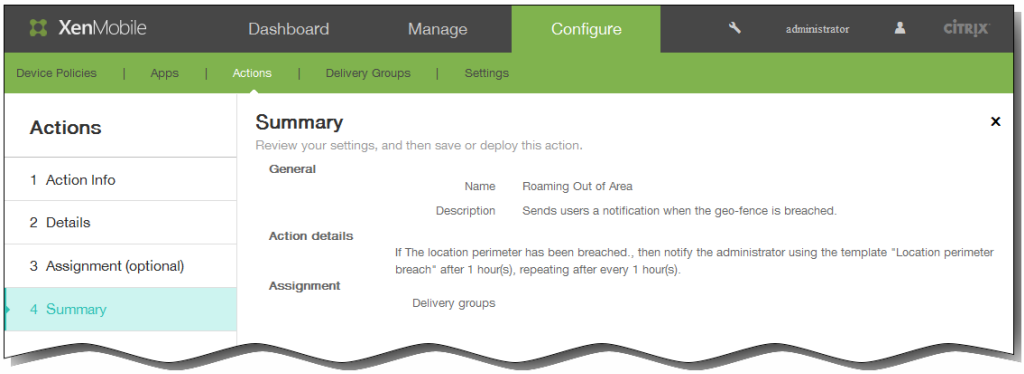












XenMobileクライアント設定

May 10, 2016

XenMobile Webコンソールで、XenMobileクライアント設定を構成できます。

1. XenMobileコンソールで［Configure］をクリックして、［Settings］をクリックします。
   ［Settings］ページが開きます。
2. ［More］をクリックします。
3. **［Client］**で、構成するオプションをクリックします。

iOSデバイス用のカスタムWorx Storeブランド設定を作成するには

Oct 24, 2016

ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、iOSおよびAndroidのモバイルデバイス上でWorx HomeおよびWorxStoreをブランド化することができます。

注：始める前に、カスタム画像を準備してアクセスできるようにしてください。

- ファイル名は.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、［Configure］、［Settings］、［More］、［Worx Store Branding］の順にクリックします。
2. ［Default store view］の横で、［Category］または［A-Z］を選択します。
3. ［Device option］の横で、［Phone］または［Tablet］を選択します。
4. ［Branding file］の横の［Browse］をクリックしてブランド設定に使用する画像または画像の.zipファイルを選択し、［Save］をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、展開する必要があります。

Worx HomおよびGoToAssistサポートオプションを作成するには

May 10, 2016

1. XenMobileコンソールで、［Configure］、［Settings］、［More］、［Worx Home Support］の順にクリックします。
2. ［Worx Home Support］ページで、以下のフィールドの値を入力します。
    1. Support email (IT help desk)
    2. Support phone (IT help desk)
    3. Token for GoToAssist chat
    4. GoToAssist support ticket email

作成したWorx Homeサポート情報は、XenMobileコンソールの［Client Properties］一覧で、関連付けられた各キー（SUPPORT_EMAIL、SUPPORT_PHONE、GTA_CHAT、GTA_TICKET）に表示されます。

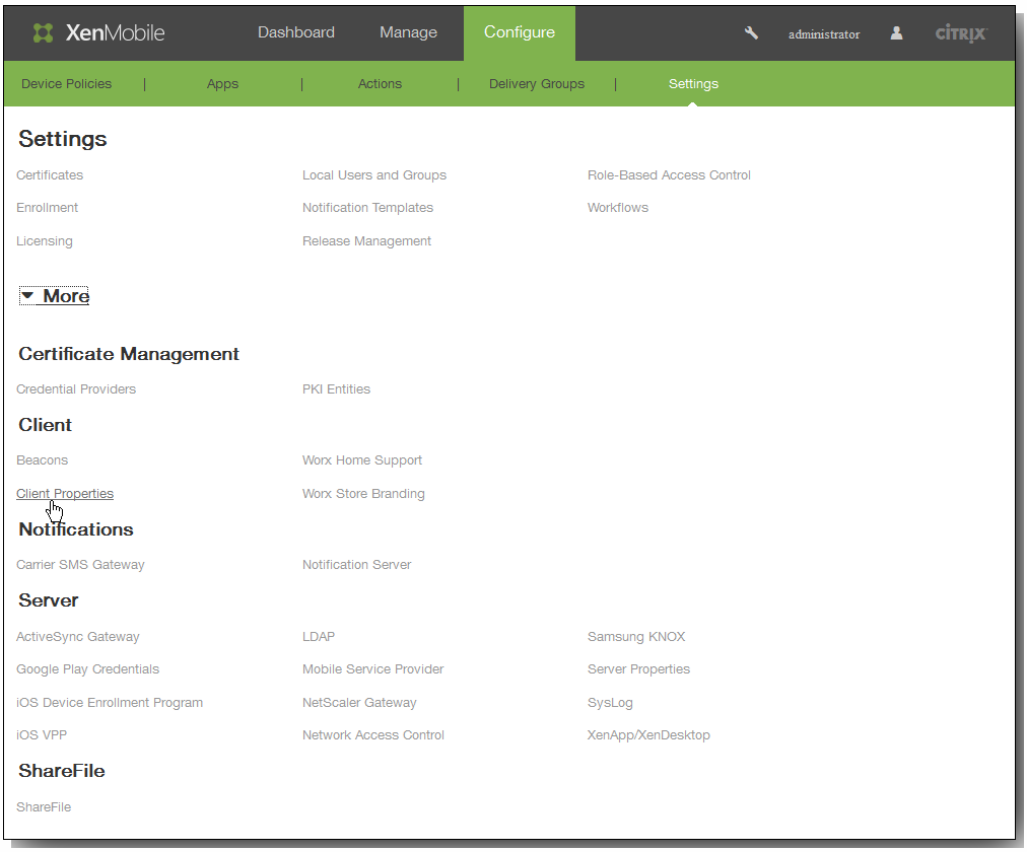
クライアントプロパティを追加、編集、または削除するには

May 10, 2016

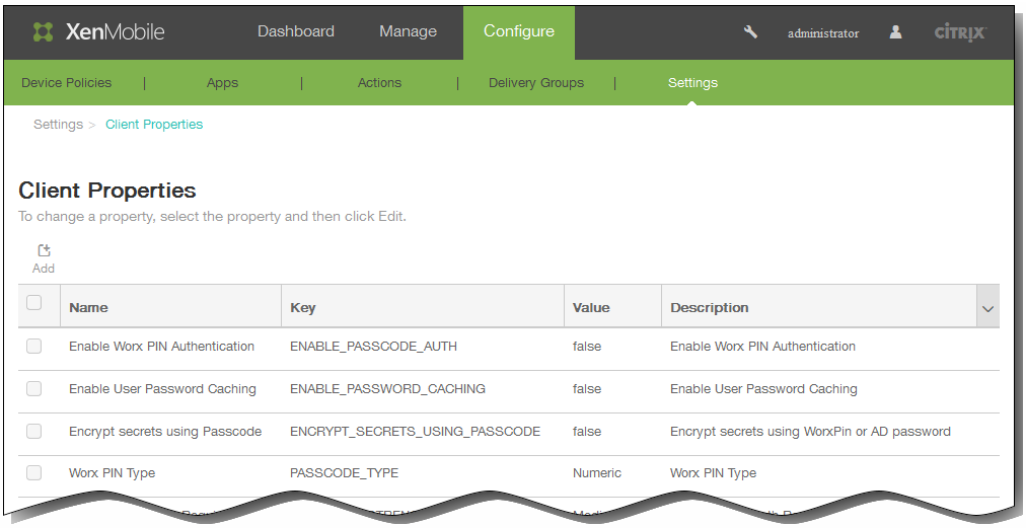
クライアントプロパティには、ユーザーのデバイスのWorx Homeに直接提供される情報が含まれています。これらのプロパティは、Worx PINなどの詳細設定を構成するときに使用されます。クライアントプロパティはCitrixサポートから取得します。

注：クライアントプロパティは、クライアントアプリケーション（特にWorx Home）のリリースごとに変更されます。

1. XenMobileコンソールで、［Configure］、［Settings］、［More］、［Client Properties］の順にクリックします。

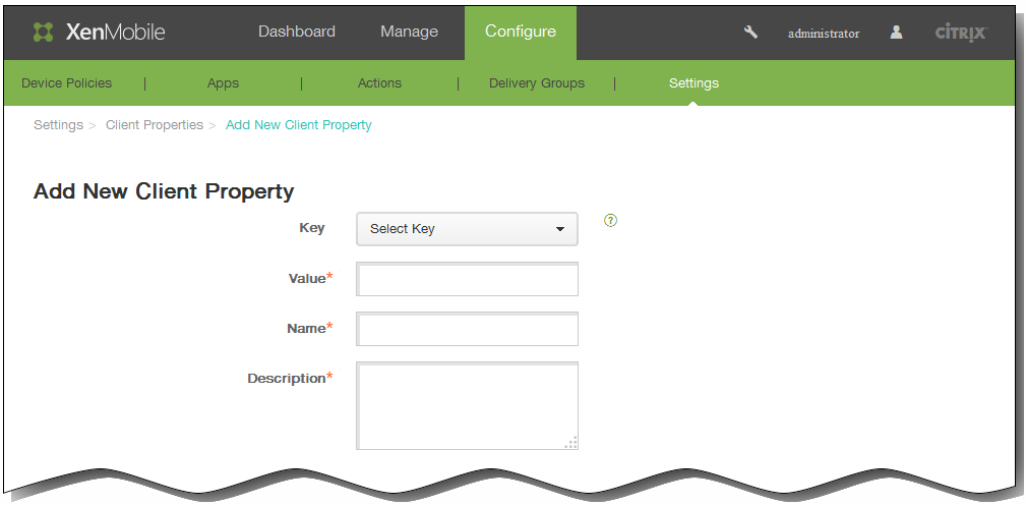


［Client Properties］ページが開きます。このページでは、クライアントプロパティを追加、編集、または削除できます。



クライアントプロパティを追加するには

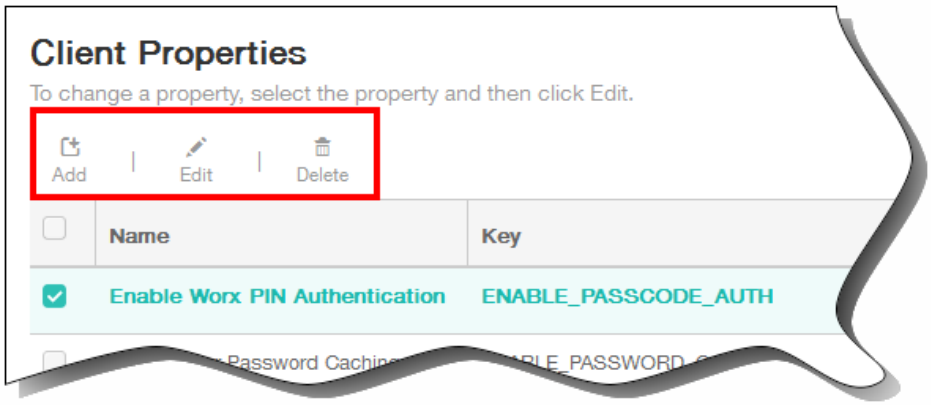
1. ［Client Properties］ページで、［Add］をクリックします。［Add New Client Property］ページが開きます。

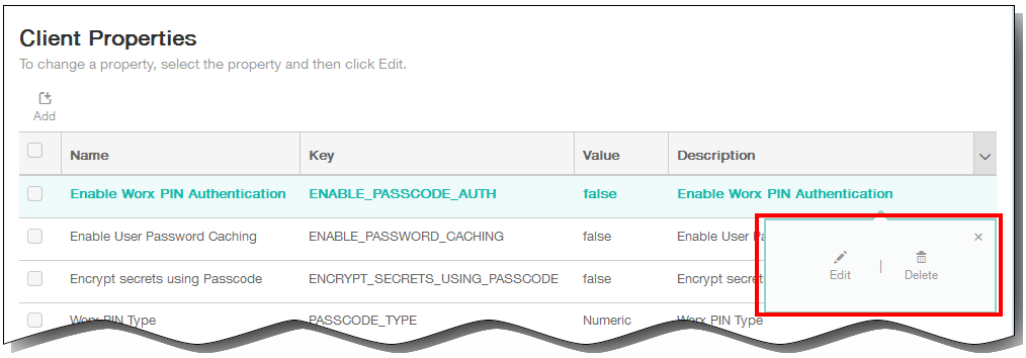


2. ［Add New Client Property］ページで、以下の情報を入力します。
   注：すべてのフィールドが必須です。
   1. Key：一覧から、追加するプロパティキーを選択します。
      重要：変更を行う前にCitrixのサポート担当者に問い合わせるか、変更を行うための特殊キーを要求してください。
   2. Value：選択したプロパティの値を入力します。
   3. Name：プロパティの名前を入力します。
   4. Description：プロパティの説明を入力します。

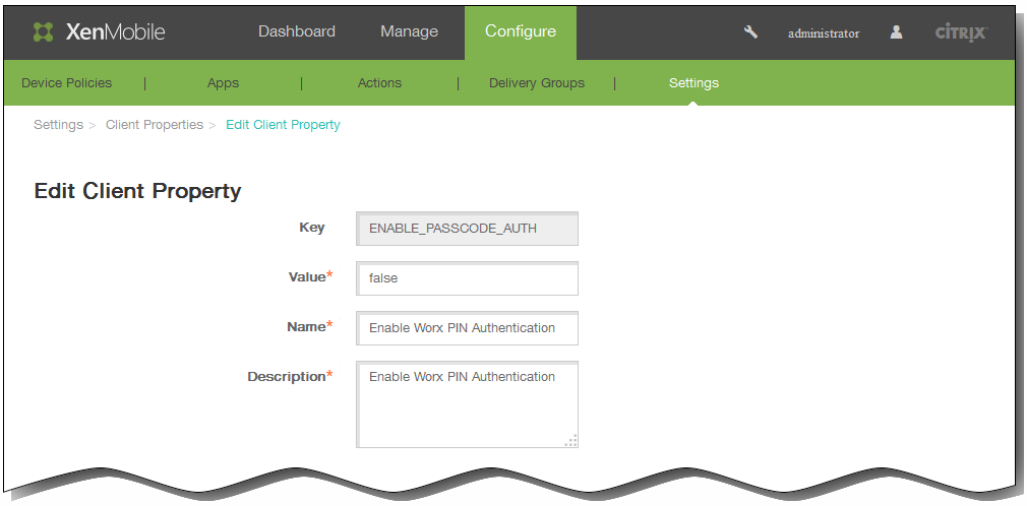
クライアントプロパティを編集するには

1. ［Client Properties］の表で、編集するクライアントプロパティを選択します。
   注：クライアントプロパティの横にあるチェックボックスをオンにすると、クライアントプロパティ一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。





2. ［Edit］をクリックします。 ［Edit Client Property］ページが開きます。



3. 必要に応じて以下の情報を変更します。
   1. Value：選択したプロパティの値です。
   2. Name：プロパティの名前です。
   3. Description：プロパティの説明です。

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

クライアントプロパティを削除するには

1. ［Client Properties］の表で、削除するクライアントプロパティを選択します。
   注：各プロパティの横のチェックボックスをオンにして、削除するプロパティを複数選択できます。
2. ［Delete］をクリックします。 確認ダイアログボックスが開きます。もう一度 [Delete］をクリックします。

クライアントプロパティリファレンス

Oct 24, 2016

次に、XenMobileの定義済みクライアントプロパティとそのデフォルトの設定を示します。

ENABLE_PASSCODE_AUTH

表示名：Enable Worx PIN Authentication

このキーを使用すると、Worx PIN機能を有効にできます。 ユーザーは、Worx PINまたはパスコードにより、Active Directoryパスワードの代わりに使用するPINを定義するように求められます。 ENABLE_PASSWORD_CACHINGが有効になっているとき、またはXenMobileで証明書認証を使用しているときは、この設定が自動的に有効になります。

ユーザーがオフライン認証を実行している場合、Worx PINがローカルで検証されて、要求したアプリやコンテンツへのアクセスがユーザーに許可されます。 ユーザーがオンライン認証を実行している場合、Worx PINまたはパスコードを使用してActive Directoryパスワードまたは証明書がロック解除されて、XenMobileとの認証を実行するために送信されます。

設定可能な値：trueまたはfalse

デフォルト値：false

ENABLE_PASSWORD_CACHING

表示名：Enable User Password Caching

このキーを使用すると、ユーザーのActive Directoryパスワードをモバイルデバイス上にローカルにキャッシュできます。 このキーをtrueに設定すると、ユーザーはWorx PINまたはパスコードを設定するように求められます。 このキーをtrueに設定する場合は、ENABLE_PASSCODE_AUTHキーをtrueに設定する必要があります。

設定可能な値：trueまたはfalse

デフォルト値：false

ENCRYPT_SECRETS_USING_PASSCODE

表示名：Encrypt secrets using Passcode

このキーでは、機密データをプラットフォームベースのネイティブな格納場所（iOSキーチェーンなど）ではなく、モバイルデバイスのSecret Vaultに格納できます。 この構成キーにより、重要な成果物を強力に暗号化できますが、ユーザーエントロピー（ユーザーだけが知るユーザーが生成するランダムなPINコード）も追加されます。

ユーザーデバイスのセキュリティを強化するために、このキーを有効にすることをお勧めします。

注：このキーを有効にすると、Worx PINでの認証を求められる回数が大幅に増えるため、ユーザーエクスペリエンスに影響します。

設定可能な値：trueまたはfalse

デフォルト値：false

PASSCODE_TYPE

表示名：Worx PIN Type

このキーで、数字のWorx PINまたは英数字のWorxパスコードのいずれをユーザーが定義できるようにするのかを定義します。 ［Numeric］を選択した場合、ユーザーは数字のWorx PINのみを定義できます。 ［Alphanumeric］を選択した場合、ユーザーは文字と数字を組み合わせたWorxパスコードを使用できます。

Note:設定を変更すると、ユーザーは、次回認証を求められたときに、新しいWorx PINまたはパスコードを設定するように求められます。

設定可能な値：NumericまたはAlphanumeric

デフォルト値：Numeric

PASSCODE_EXPIRY

表示名：Worx PIN Expiry Requirement

このキーで、Worx PINまたはパスコードが有効な期間（日単位）を定義します。この期間を過ぎると、ユーザーはWorx PINまたはパスコードを変更する必要があります。 この設定を変更すると、ユーザーの現在のWorx PINまたはパスコードの有効期限が切れた場合のみ、新しい値が設定されます。

設定可能な値：1～99

デフォルト値：90

PASSCODE_HISTORY

表示名：Worx PIN History

このキーで、Worx PINまたはパスコードの変更時にユーザーが再利用できない、以前に使用したWorx PINまたはパスコードの個数を定義します。 この設定を変更すると、ユーザーがWorx PINまたはパスコードを次回再設定したときに新しい値が設定されます。

設定可能な値：1～99

デフォルト値：5

PASSCODE_MAX_ATTEMPTS

表示名：Worx PIN Maximum Attempts

このキーで、完全認証が必要になる前に、ユーザーが誤ったWorx PINまたはパスコードを入力できる回数を定義します。 完全認証に成功した後で、ユーザーは新しいWorx PINまたはパスコードを作成するように求められます。

設定可能な値：正の整数

デフォルト値：15

INACTIVITY_TIMER

表示名：Inactivity Timer

このキーで、ユーザーがデバイスを非アクティブにした後で、Worx PINまたはパスコードの入力を求められずにアプリにアクセスする時間（分単位）を定義します。 MDXアプリでこの設定を有効にするには、 ［App Passcode］設定を［On］に設定する必要があります。 ［App Passcode］設定を［Off］に設定すると、ユーザーは完全認証を実行するよ

うWorx Homeにリダイレクトされます。 この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。 **注**：iOSでは、Inactivity TimerはMDXアプリだけでなくWorx Homeへのアクセスにも対応します。

設定可能な値：正の整数

デフォルト値：15

PASSCODE_STRENGTH

表示名：Worx PIN Strength Requirement

このキーで、Worx PINまたはパスコードの強度を定義します。 この設定を変更すると、ユーザーは、次回認証を求められたときに、新しいWorx PINまたはパスコードを設定するように求められます。

設定可能な値：Low、Medium、またはStrong

デフォルト値：Medium

次の表は、PASSCODE_TYPEで選択する設定に基づいた、各強度設定のパスワード規則を示しています。

パスコードの強度	数字パスコードの規則	英数字パスコードの規則
低	すべての数字を任意の順序で使用できます。	1つ以上の数字と1つ以上の文字が含まれている必要があります。 **使用不可**：AAAaaa、aaaaaa、abcdef **使用可**：aa11b1、Abcd1#、Ab123~、aaaa11、aa11aa
中（デフォルト設定）	1.すべての数字を同じにすることはできません。 たとえば、444444は使用できません。 2.すべての数字を連続した数字にすることはできません。 たとえば、123456や654321は使用できません。 **使用可**：444333、124567、136790、555556、788888	パスコード強度「Low」の規則に加えて、以下の規則が適用されます。 1.文字およびすべての数字を同じにすることはできません。 たとえば、aaaa11、aa11aa、またはaaa111は使用できません。 2.連続した文字および連続した数字は使用できません。 たとえば、abcd12、bcd123、123abc、xy1234、xyz345、またはcba123は使用できません。 **使用可**：aa11b1、aaa11b、aaa1b2、abc145、xyz135、sdf123、ab12c3、a1b2c3、Abcd1#、Ab123~
Strong	Worx PINのパスコード強度「Medium」と同じです。	パスコードに1つ以上の数字、1つ以上の特殊記号、1つ以上の大文字、および1つ以上の小文字が含まれている必要があります。 **使用不可**：abcd12、Abcd12、dfgh12、jkrtA2 **使用可**：Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#

ENABLE_CRASH_REPORTING

表示名：Enable Crash reporting

このキーでは、Worx AppsのCrashlyticsを使用するクラッシュの報告を有効または無効にします。

設定可能な値：trueまたはfalse

デフォルト値：true

DISABLE_LOGGING

表示名：Disable logging

このキーでは、ユーザーが自分のデバイスのログを収集およびアップロードする機能を無効にできます。 Worx Homeおよびすべてのインストール済みMDXアプリのロギングが無効になります。 ユーザーは［Support］ページから任意のアプリにログを送信することはできません。メール作成ダイアログボックスは開きますが、ログは添付されません。ロギングが無効になっているというメッセージが追加されます。 ユーザーのデバイスに対する効果に加えて、Worx HomeおよびMDXアプリのXenMobileコンソールでログ設定を変更することはできません。

このキーをtrueに設定すると、Worx Homeによって［Block application logs］が［true］に設定され、新しいポリシーが適用されたときにMDXアプリのロギングが停止します。

設定可能な値：trueまたはfalse

Default value：false（ロギングは有効です）

XenMobileサーバー設定

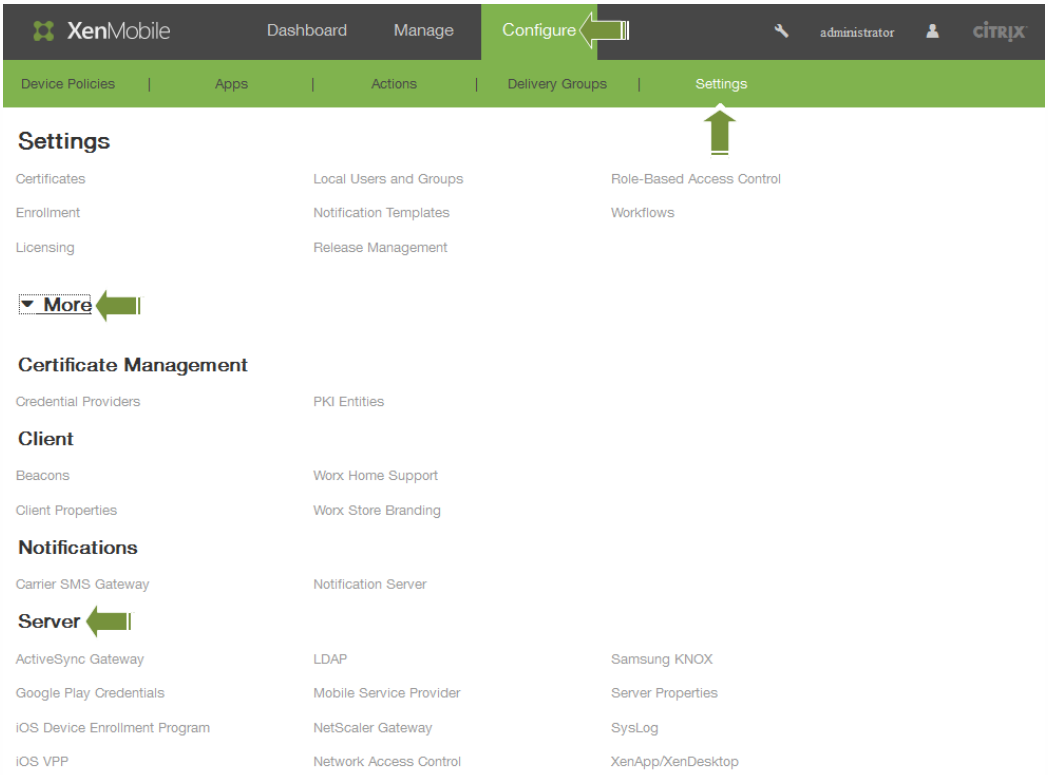
May 10, 2016

XenMobile Webコンソールで、XenMobileサーバー設定を構成できます。

サーバー構成には次のオプションがあります。

ActiveSync Gateway	iOS VPP	NetScaler Gateway	サーバープロパティ
Google Play資格情報	LDAP	ネットワークアクセス制御	Syslog
iOSデバイス登録プログラム	Mobile Service Provider	Samsung KNOX	XenApp/XenDesktop

1. XenMobileコンソールで［Configure］をクリックして、［Settings］をクリックします。
   ［Settings］ページが開きます。



2. ［More］をクリックします。
3. **［Server］**で、構成するオプションをクリックします。

XenMobileでのActiveSyncゲートウェイ

May 10, 2016

ActiveSyncは、Microsoftが開発したモバイルデータ同期プロトコルです。 ActiveSyncは、ハンドヘルドデバイスやデスクトップ（またはラップトップ）コンピューターとデータを同期します。 XenMobileでActiveSyncゲートウェイの規則を構成できます。 これらの規則に基づいて、デバイスのActiveSyncデータへのアクセスを許可または拒否することができます。 たとえば、［不足必須アプリ］の規則をアクティブ化すると、XenMobileは［アプリ アクセス ポリシー］の必須アプリを確認し、必須アプリが不足している場合は、ActiveSyncデータへのアクセスを拒否します。

XenMobileでは、次の規則がサポートされます。

匿名デバイス：デバイスが匿名モードではないかを確認します。 これは、デバイスが再接続を試みたとき、XenMobileがユーザーを再認証できない場合に確認のために使用します。

Samsung KNOX 構成証明に失敗しました：デバイスが、Samsung KNOX構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ：デバイス上に［アプリアクセスポリシー］で定義された禁止アプリがないかを確認します。

暗示的許可および拒否：これは、［ActiveSync ゲートウェイ］のデフォルトの操作です。その他のフィルター規則条件を満たしていないすべてのデバイスのデバイス一覧を作成し、リストに基づいて接続を許可または拒否します。 一致する規則がなければ、デフォルトは［暗黙的な許可］になります。

非アクティブ デバイス：［サーバー プロパティ］のデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。

不足必須アプリ：デバイスに［アプリ アクセス ポリシー］で定義された必須アプリの不足がないかを確認します。

非推奨アプリ：デバイスに［アプリ アクセス ポリシー］で定義された非推奨アプリがないかを確認します。

非準拠パスワード：ユーザーパスワードが正しいかを確認します。 XenMobileが、iOSおよびAndroidデバイス上で、現在デバイスにあるパスワードがデバイスに送られたパスコードポリシーに準拠しているかを確認します。 たとえばiOSの場合、ユーザーはXenMobileがデバイスにパスコードを送ってから60分以内に、パスワードを設定する必要があります。 さもなければ、ユーザーがパスワードを設定する前に、パスコードが非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス外かどうかを確認します。 このプロパティは通常、自動化された操作によって変更されたり、XenMobile APIを使用するサードパーティによって変更されたりします。

失効状態：デバイスの証明書が失効していないかを確認します。 証明書が失効したデバイスは、再度認証されるまで再登録できません。

ルート化された Android およびジェイルブレークした iOS デバイス：AndroidまたはiOSデバイスがジェイルブレークされていないかを確認します。

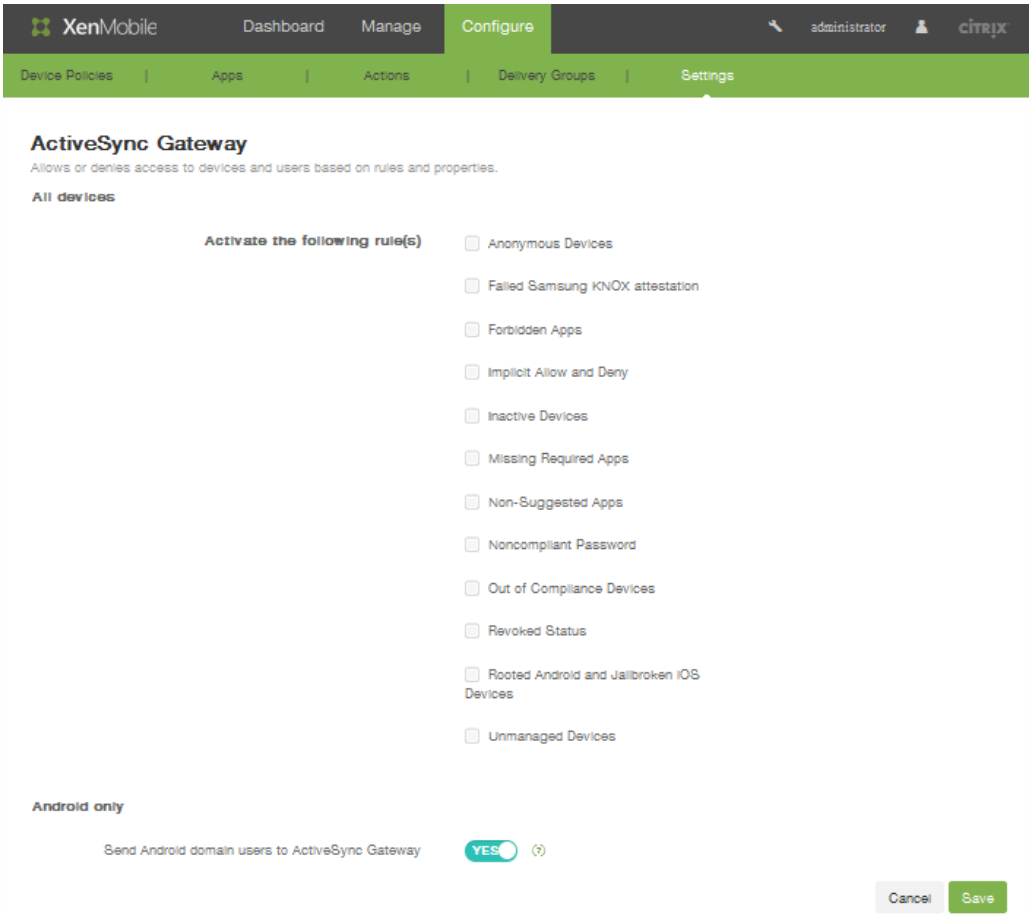
非管理デバイス：デバイスがまだXenMobileの管理下にあるかを確認します。 たとえば、MAMモードで実行されているデバイス、あるいは登録されていないデバイスは、管理下にありません。

Android ドメイン ユーザーを ActiveSync Gateway に送信：［はい］をクリックすることで、XenMobileによって、Androidデバイスの情報がActiveSyncゲートウェイに送信されるようにします。 このオプションを有効にすると、Androidデバイスユーザーの ActiveSync識別子がXenMobileにない場合でも、XenMobileによってAndroidデバイスの情報がActiveSyncゲー

トウェイに送信されます。

XenMobileでActiveSyncゲートウェイを構成するには

1. XenMobileコンソールで、**[構成] > [設定] > [詳細] > [ActiveSync ゲートウェイ]** の順にクリックします。**[ActiveSync ゲートウェイ]** 構成ページが開きます。



2. **[Activate the following rules]** で、有効にする規則を1つまたは複数オンにします。
3. **[Android-only]** の **[Android ドメイン ユーザーを ActiveSync Gateway に送信]** で **[はい]** をクリックし、XenMobileによってAndroidデバイスの情報がSecure Mobile Gatewayに送信されるようにします。
4. **[保存]** をクリックします。

Google Play資格情報

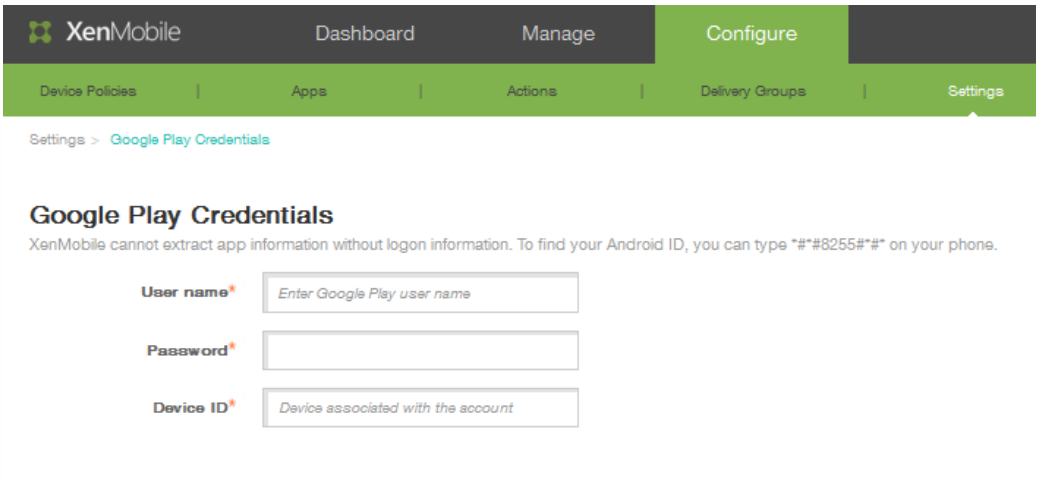
May 10, 2016

XenMobileでは、Google Play資格情報を使用してデバイスのアプリケーション情報を抽出します。

注：Android IDを確認するには、お使いの電話機で「*#*#8255#*#*」を入力します。
重要：XenMobileでアプリケーション情報の抽出を有効にするには、安全でない接続を許可するようにGmailアカウントを構成する必要があります。手順については、Googleサポートサイトを参照してください。

XenMobileを構成してGoogle Play資格情報を使用するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Google Play Credentials］の順にクリックします。
   ［Google Play Credentials］構成画面が開きます。



2. ［User name］ボックスに、Google Playアカウントに関連付けられた名前を入力します。
3. ［Password］ボックスにユーザーパスワードを入力します。
4. ［Device ID］ボックスにAndroid IDを入力します。
   Android IDを確認するには、お使いの電話機で「*#*#8255#*#*」を入力します。
5. ［Save］をクリックします。

iOSデバイス登録プログラム

May 10, 2016

XenMobileで、iOSデバイスを実行しているモバイルデバイス用のiOSデバイス登録プログラムを設定できます。この機能を使用すると、デバイスの設定アシスタントのエクスペリエンスをカスタマイズするプロファイルについてiOSデバイスがAppleサーバーに通知し、それを特定のデバイスに割り当てることができます。

XenMobileでiOSデバイス登録プログラムを構成するには

続行する前に、deploy.apple.comでApple DEPアカウントを作成しておく必要があります。DEPアカウントの作成後、仮想MDMサーバーをセットアップしてXenMobileとAppleの通信を許可します。これを実行するには、XenMobile公開キーをAppleにアップロードする必要があります。Appleが公開キーを受信したら、XenMobileにインポートするサーバートークンが返されます。次の手順に従って、XenMobileとApple間での通信を確立します。

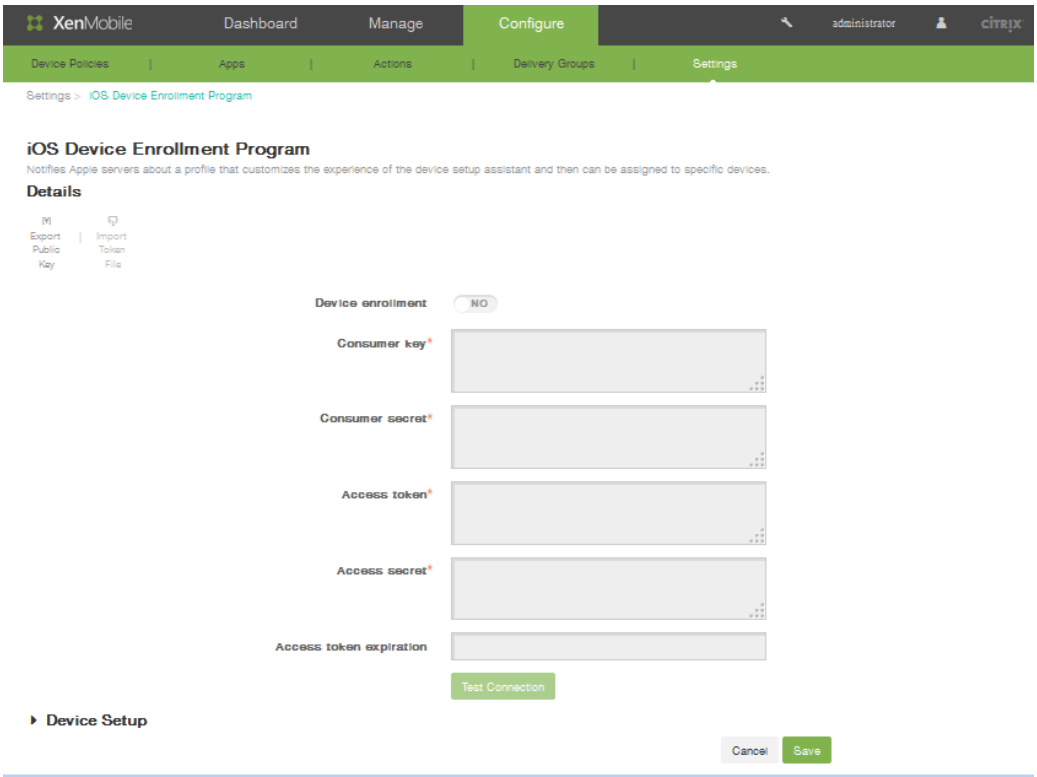
1. 公開キーを取得してAppleにアップロードするには、**[Settings] > [More]** の順に選択して **[iOS Device Enrollment Program]** ページで、 **[Export Public Key]** をクリックしてファイルをコンピューターに保存します。

2. deploy.apple.comにアクセスして、DEPアカウントにログインし、MDMサーバーのセットアップ手順に従います。この処理の一部として、Appleによりサーバートークンが提供されます。

3. **[iOS Device Enrollment Program]** ページで **[Device enrollment]** を **[Yes]** に設定し、 **[Import Token File]** をクリックしてAppleサーバートークンをXenMobileに追加します。

4. トークンファイルがXenMobileにアップロードされると、 **[Server tokens]** フィールドに値が自動的に入ります。

5. **[Test Connectivity]** をクリックして、XenMobileとAppleが通信できるか確認します。接続テストに失敗したら、すべてに必要なポートが開いているか確認します。ほとんどの場合で、これが障害の原因です。XenMobileで開く必要があるポートについて詳しくは、「ポート要件」を参照してください。



[Details] で、次の設定を構成してDEP構成を完了します。

- Device enrollment：［YES］をクリックします。
- Consumerkey：コンシューマーキーを入力します。
- Consumer secret：コンシューマーシークレットを入力します。
- Access token：アクセストークンを指定します。
- Access secret：アクセストークンのシークレットを入力します。
- Access token expiration：任意で、アクセストークンの有効期限を指定します。
- ［Test Connection］をクリックして、接続を検証します。

- ［Device Setup］を展開して以下の設定を構成します。
  - Business unit：事業単位に関連付けられた名前を入力します。
  - Support phone number：サポートの電話番号を入力します。
  - Support email address：任意で、サポートメールアドレスを入力します。
  - Unique service ID：任意で、一意のサービスIDを含めます。

- ［Device Settings］で、iOSデバイス登録プログラムに関連付けられた以下のデバイス設定を構成します。
  - Allow or deny pairing：［Allow］をクリックして、iTunesやApple ConfiguratorなどのAppleツールによるデバイスの管理を有効にします。

> ## 注意
>
> ペアリングを許可し、Apple Configuratorを使用する場合、**[Supervised mode]** で **[YES]** を選択します。

- - Device profile removal：リモートで削除できるプロファイルをデバイスで使用する場合は、［Allow］をクリックします。
  - Require device enrollment：ユーザーが登録処理をスキップできないようにするには、このチェックボックスをオンにします。

- ［Device Setup Steps］で、次の設定を構成します。
  - Locationservices：［Set up］をクリックしてデバイスが位置情報を共有できるようにするか、［Skip］をクリックしてデバイスが位置情報を共有できないようにします。
  - Restore from backup：［Set up］をクリックしてデバイスでバックアップファイルからデータを復元できるようにします。
  - Apple and iCloud：［Set up］をクリックしてデバイスでApple IDおよびiCloudを使用できるようにします。
  - Terms and Conditions：［Set up］をクリックします。
  - Passcode：デバイス登録でパスコードを使用するには、［Set up］をクリックします。
  - Siri：［Set up］をクリックしてデバイスでSiriを使用できるようにします。
  - Touch ID：［Set up］をクリックしてデバイスでTouch IDを使用します。
  - Apple Pay：［Set up］をクリックしてデバイスでApple Payを有効にします。
  - Zoom：［Set up］をクリックしてズームを有効にします。
  - Diagnostics：［Set up］をクリックしてデバイスで診断を共有できるようにします。

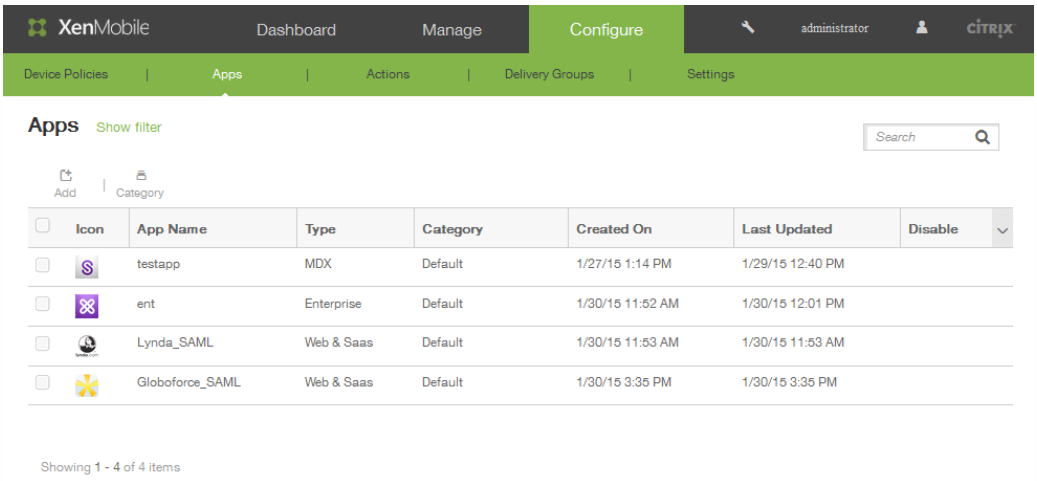
- ［Save］をクリックします。

iOS VPP

May 10, 2016

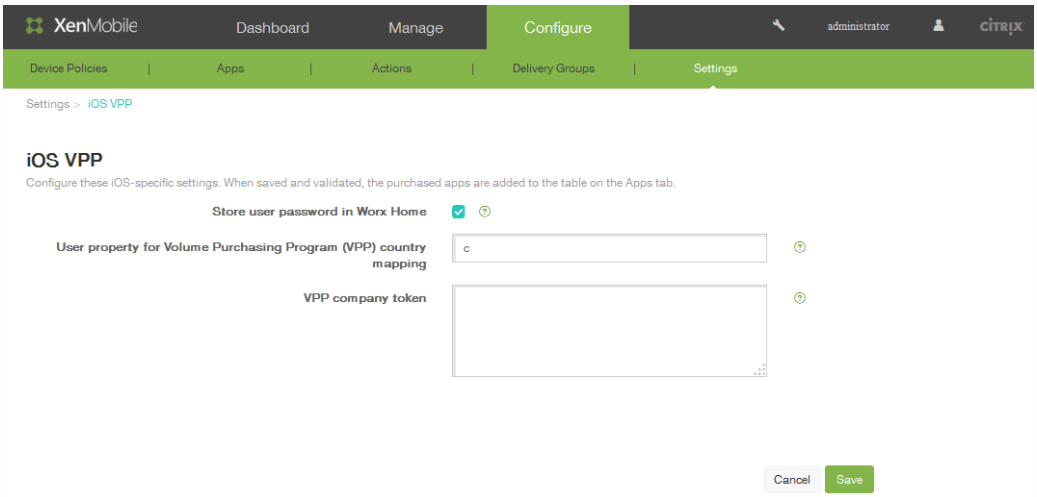
XenMobileで、iOS Volume Purchase Plan（VPP）に固有の設定を構成できます。iOS VPPを利用すると、組織のアプリケーションやそのほかの大量なデータの検索、購入、配布の処理が簡単になります。VPPは、組織のコンテンツニーズを管理するためのシンプルでスケーラブルなソリューションを提供します。

XenMobileでiOS VPP設定を保存して検証すると、購入したアプリケーションがXenMobileコンソールの［Apps］タブの表に追加されます。



XenMobileでiOS VPPを構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［iOS VPP］の順にクリックします。［iOS VPP］構成画面が開きます。

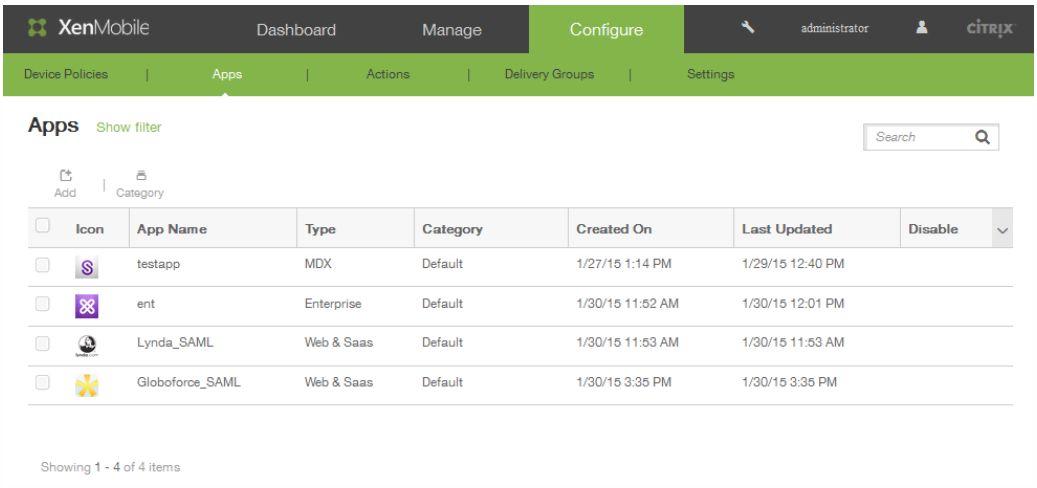


2. ［Store user password in Worx Home］の横のチェックボックスをオンにすると、XenMobile認証用のユーザー名とパス

ワードがWorx Homeに安全に保存されます。

3. ［User property for Volume Purchasing Program (VPP) country mapping］に、ユーザーが国固有のアプリケーションストアからアプリケーションをダウンロードできるようにするコードを入力します。
このマッピングはVPPのプロパティプールの選択に使用されます。たとえば、ユーザープロパティが米国で、アプリケーションのVPPコードが日本で配布されている場合、そのユーザーはそのアプリケーションをダウンロードすることはできません。国マッピングコードについて詳しくは、VPPプラン管理者に問い合わせてください。

4. ［VPP company token］に、ユーザーが会社ベースのアカウントを使ってApple App Storeで何かを購入したときに生成される、VPPサービストークンを表すトークンを入力します。このトークンはVPPライセンスを検証するために使用されます。たとえば、ビジネス向けのApple VPPアカウントがある場合は、https://vpp.itunes.comにアクセスして **［Business］** をクリックし、Apple VPPアカウントの資格情報でログインして適切な情報を取得します。
5. ［Save］をクリックします。［Apps］の表に次のように情報が表示されます。



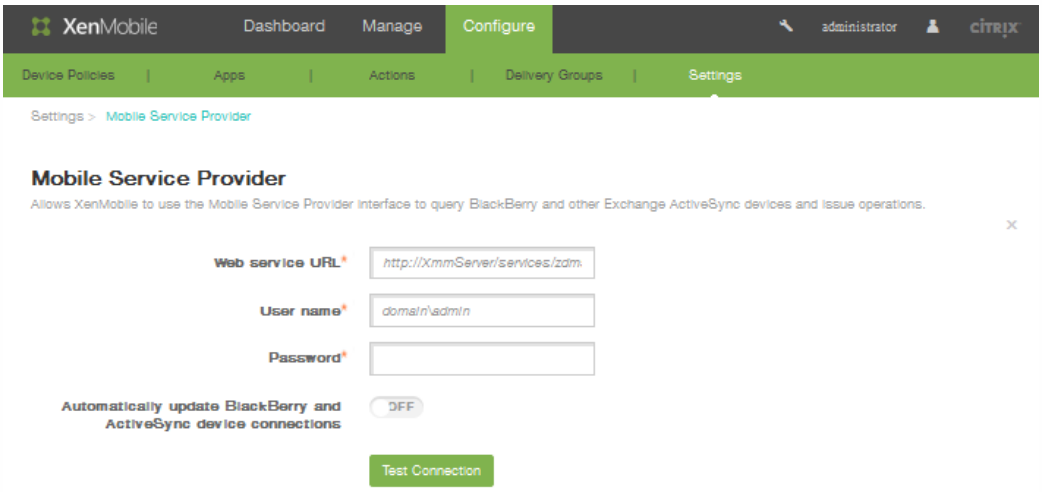
Mobile Service Provider

May 10, 2016

XenMobileでMobile Service Providerインターフェイスの使用を有効にして、BlackBerryやそのほかのExchange ActiveSyncデバイスに対してクエリを実行したり、操作を発行したりすることができます。

Mobile Service Providerを構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Mobile Service Provider］の順にクリックします。
   ［Mobile Service Provider］構成ページが開きます。



2. ［Web service URL］ボックスに、WebサービスのURL（http://XmmServer/services/xdmserviceなど）を入力します。
3. ［User name］ボックスに、domain\adminの形式でユーザー名を入力します。
4. ［Password］にパスワードを入力します。
5. ［Automatically update BlackBerry and ActiveSync device connections］で、このオプションを有効にする場合は［ON］をクリックします。デフォルトでは、［OFF］になっています。
6. ［Test connection］をクリックして、接続を検証します。
7. ［Save］をクリックします。

ネットワークアクセス制御

May 10, 2016

XenMobileで、Cisco ISEなどのNAC（Network Access Control：ネットワークアクセス制御）アプライアンスをネットワークで設定する場合は、フィルターで規則またはプロパティに基づいてデバイスをNACに準拠または非準拠として設定することができます。 XenMobileの管理対象デバイスが指定された条件を満たしておらず、その結果［Not Compliant］としてマークされている場合、そのデバイスはNACアプライアンスによりネットワーク上でブロックされます。

XenMobileコンソールの一覧で、デバイスを非準拠として設定する条件を1つまたは複数選択します。

XenMobileは、次のNACコンプライアンスフィルターをサポートします。

匿名デバイス：デバイスが匿名モードではないかを確認します。 これは、デバイスが再接続を試みたとき、XenMobileがユーザーを再認証できない場合に確認のために使用します。

Samsung KNOX 構成証明に失敗しました：デバイスが、Samsung KNOX構成証明サーバーのクエリに失敗していないかを確認します。

禁止アプリ：デバイス上に［アプリアクセスポリシー］で定義された禁止アプリがないかを確認します。

暗示的許可および拒否：これは、［ActiveSync ゲートウェイ］のデフォルトの操作です。その他のフィルター規則条件を満たしていないすべてのデバイスのデバイス一覧を作成し、リストに基づいて接続を許可または拒否します。 一致する規則がなければ、デフォルトは［暗黙的な許可］になります。

非アクティブ デバイス：［サーバー プロパティ］のデバイスの［非アクティブな日数のしきい値］に定義された期間、非アクティブであったかを確認します。

不足必須アプリ：デバイスに［アプリ アクセス ポリシー］で定義された必須アプリの不足がないかを確認します。

非推奨アプリ：デバイスに［アプリ アクセス ポリシー］で定義された非推奨アプリがないかを確認します。

非準拠パスワード：ユーザーパスワードが正しいかを確認します。 XenMobileが、iOSおよびAndroidデバイス上で、現在デバイスにあるパスワードがデバイスに送られたパスコードポリシーに準拠しているかを確認します。 たとえばiOSの場合、ユーザーはXenMobileがデバイスにパスコードを送ってから60分以内に、パスワードを設定する必要があります。 さもなければ、ユーザーがパスワードを設定する前に、パスコードが非準拠になる可能性があります。

コンプライアンス外デバイス：［コンプライアンス外デバイス］プロパティに基づいて、デバイスがコンプライアンス外かどうかを確認します。 このプロパティは通常、自動化された操作によって変更されたり、XenMobile APIを使用するサードパーティによって変更されたりします。

失効状態：デバイスの証明書が失効していないかを確認します。 証明書が失効したデバイスは、再度認証されるまで再登録できません。

ルート化された Android およびジェイルブレークした iOS デバイス：AndroidまたはiOSデバイスがジェイルブレークされていないかを確認します。

非管理デバイス：デバイスがまだXenMobileの管理下にあるかを確認します。 たとえば、MAMモードで実行されているデバイス、あるいは登録されていないデバイスは、管理下にありません。

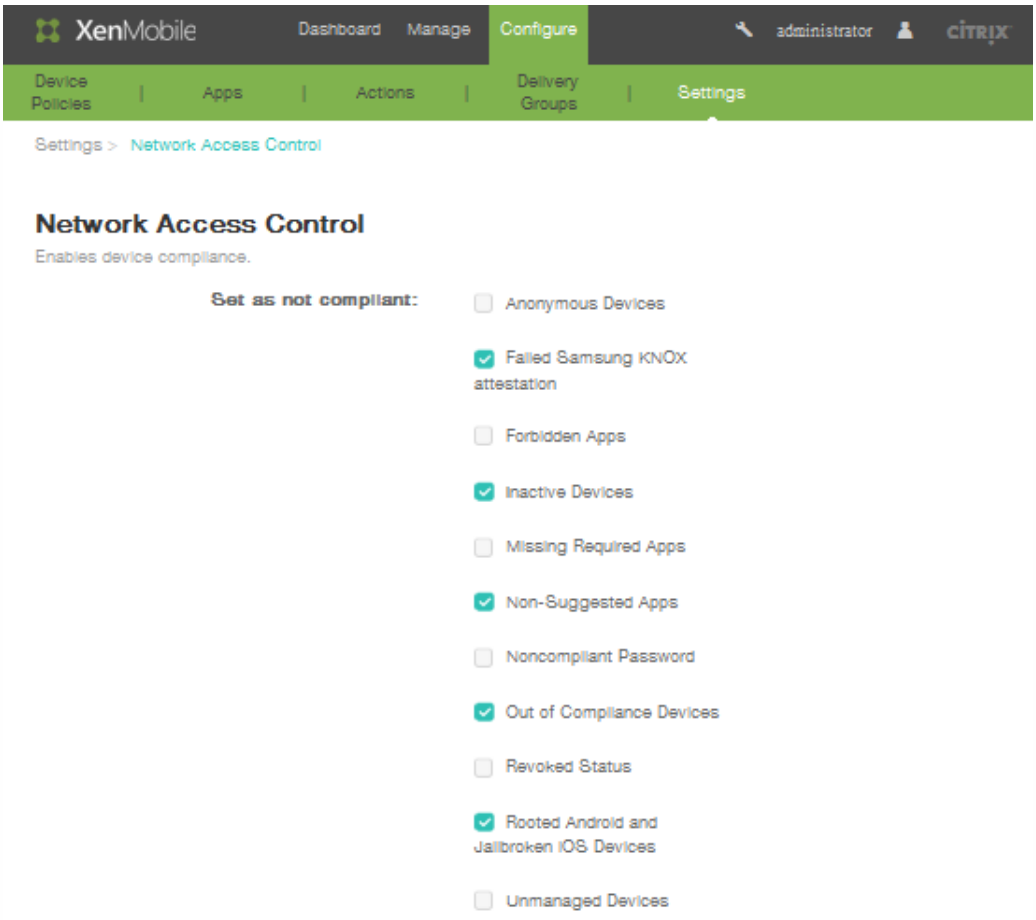
Android ドメイン ユーザーを ActiveSync Gateway に送信：［はい］をクリックすることで、XenMobileによって、Androidデバイスの情報がActiveSyncゲートウェイに送信されるようにします。 このオプションを有効にすると、Androidデ

イスユーザーのActiveSync識別子がXenMobileにない場合でも、XenMobileによってAndroidデバイスの情報がActiveSyncゲートウェイに送信されます。

> **注意**
>
> ［Implicit Compliant］または［Not Compliant］フィルターは、XenMobileによる管理対象デバイスでのみデフォルト値を設定します。たとえば、ブラックリストに入っているアプリケーションがインストールされているデバイスや、登録されていないデバイスは［Not-Compliant］としてマークされ、NACアプライアンスによりネットワークからブロックされます。

XenMobileでネットワークアクセス制御を構成するには

1. XenMobile Webコンソールで、**［構成］> ［設定］> ［詳細］> ［ネットワーク アクセス制御］**の順にクリックします。**［ネットワーク アクセス制御］**構成ページが開きます。



2. **［非準拠として設定］**フィルターで有効にしたい項目のチェックボックスを選択します。
3. **［保存］**をクリックします。

Samsung KNOX

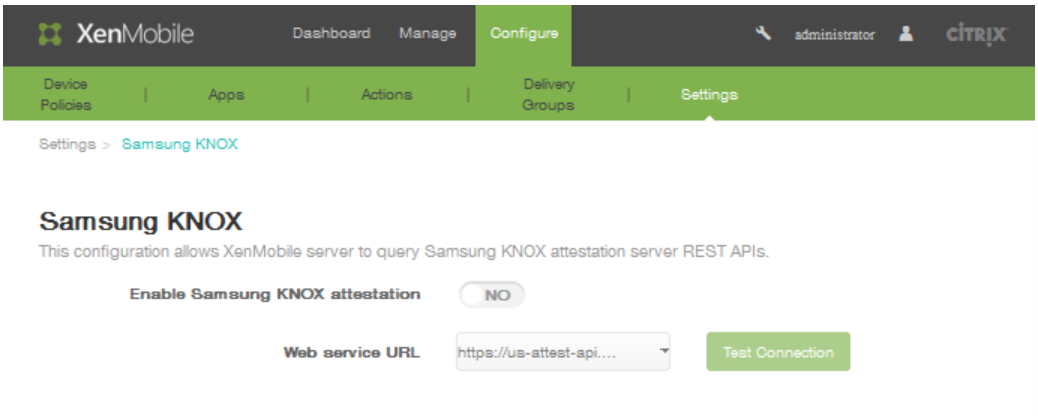
May 10, 2016

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

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

Samsung KNOX認証を有効化するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Samsung KNOX］の順にクリックします。［Samsung KNOX］構成ページが開きます。



2. ［Enable Samsung KNOX attestation］で［**YES**］をクリックします。
3. 手順2.で［YES］をクリックすると、［**Web service URL**］オプションが有効になります。一覧から、適切な認証サーバーを選択します。
4. ［**Test Connection**］をクリックして、接続を検証します。
5. ［**Save**］をクリックします。

サーバープロパティ

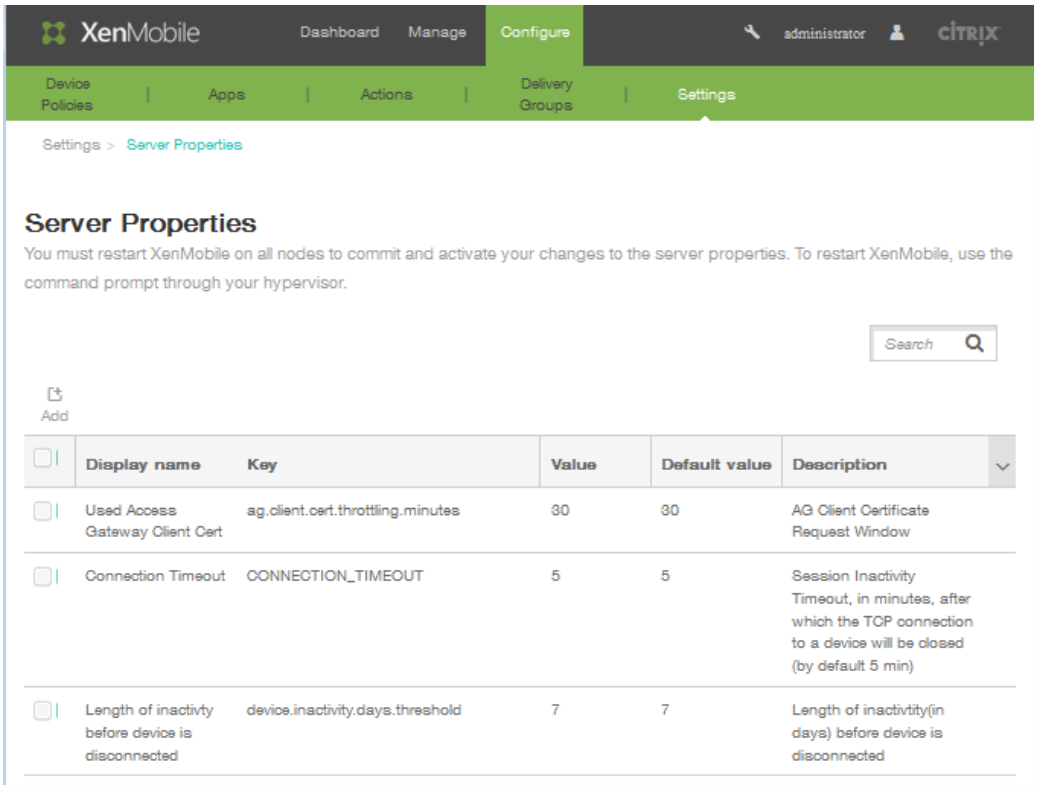
May 10, 2016

XenMobileで、サーバーにプロパティを適用できます。変更を行った後、すべてのノードでXenMobileを再起動し、変更を確定して有効化する必要があります。

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

XenMobileでサーバープロパティを構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Server Properties］の順にクリックします。［Server Properties］構成ページが開きます。



2. 次のいずれかを行います。
   - 新しいサーバープロパティを追加するには［Add］をクリックします。
   - 表で既存のプロパティをクリックして選択し、表示されるメニューで［Edit］をクリックします。
3. 手順2.で［Add］をクリックした場合は、以下のフィールドを構成します。

- Key：一覧から、適切なキーを選択します。
  注：キーでは大文字と小文字が区別されます。変更を行う前にCitrixのサポート担当者に問い合わせるか、特殊キーを要求する必要があります。

- **Value**：選択したキーに応じて値を入力します。
- **Display name**：［Server Properties］の表に表示される、新しいプロパティ値の名前を入力します。
- **Description**：任意で、新しいサーバープロパティの説明を入力して、［Save］をクリックします。

Syslog

May 10, 2016

XenMobileを構成して、ログファイルをシステムログ（syslog）サーバーに送信できます。サーバーのホスト名またはIPアドレスが必要です。

Syslogは、監査モジュール（アプライアンス上で実行）とサーバー（リモートシステムで実行可能）の2つのコンポーネントを使用する、標準ロギングプロトコルです。Syslogプロトコルでは、データ転送でユーザーデータプロトコル（UDP）を使用します。

サーバーを構成して、以下の種類の情報を収集できます。

- システムログには、XenMobileで実行されたアクションが示されます。
- 監査ログには、XenMobileのシステムアクティビティの記録が時系列で示されます。

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。

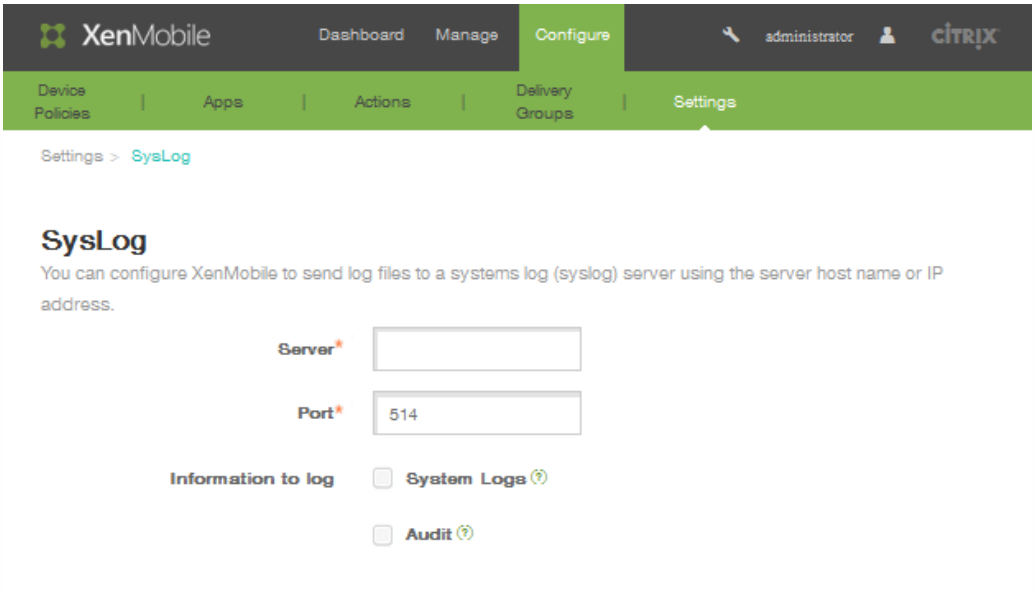
- ログメッセージを生成したアプライアンスのIPアドレス
- タイムスタンプ
- メッセージの種類
- イベントに関連付けられたログレベル（重要、エラー、通知、警告、情報、デバッグ、アラート、または緊急）
- メッセージの情報

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 Cloud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コンソールのサポートページでログをダウンロードできます。システムログをダウンロードするには、［すべてダウンロード］をクリックしてください。詳しくは、「XenMobileでのログファイルの表示および分析」を参照してください。

XenMobileでsyslogサーバーを構成するには

1. XenMobile Webコンソールで、［Configure］、［Settings］、［More］、［Syslog］の順にクリックします。
   ［Syslog］構成ページが開きます。



2. ［Name］ボックスに、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。
3. ［Port］ボックスにポート番号を入力します。デフォルトのポート番号は、514です。
4. ［Information to log］で、［System Logs］チェックボックスおよび［Audit］チェックボックスをオンまたはオフにします。
   - システムログには、XenMobileで実行されたアクションが示されます。
   - 監査ログには、XenMobileのシステムアクティビティの記録が時系列で示されます。
5. **［Save］**をクリックします。

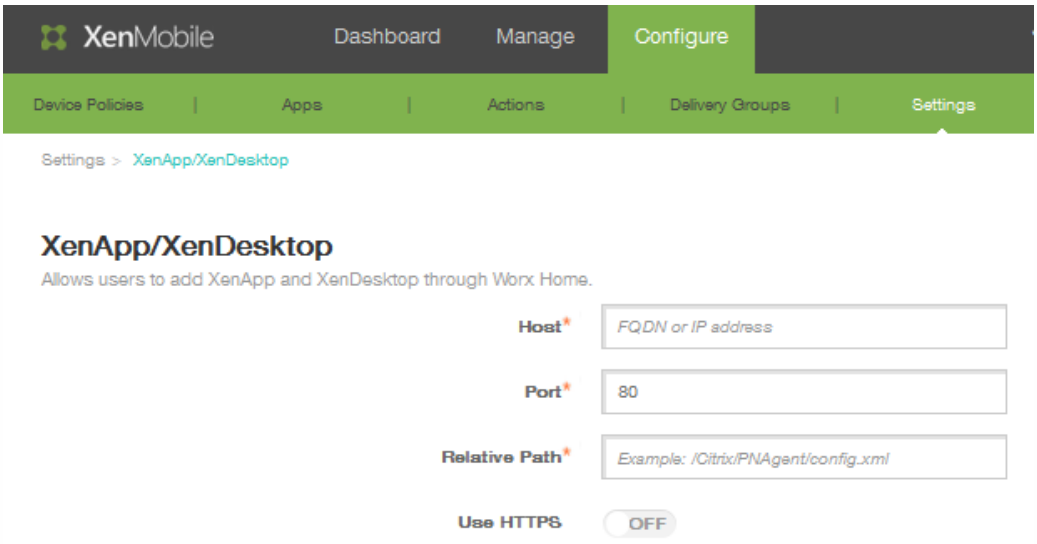
XenAppおよびXenDesktopを構成するには

May 10, 2016

XenMobileでは、XenAppおよびXenDesktopからアプリケーションを収集して、Worx Storeでモバイルデバイスユーザーがそのアプリケーションを使用できるようにすることができます。ユーザーは、Worx Store内から直接アプリケーションをサブスクライブして、Worx Homeから起動します。アプリケーションを起動するために、Receiverをユーザーのデバイスにインストールする必要があります。ただし、構成する必要はありません。

この設定を構成するには、StoreFrontまたはWeb Interfaceサイト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、**［Configure］>［Settings］>［More］>［XenApp/XenDesktop］**の順にクリックします。
   ［XenApp/XenDesktop］構成ページが開きます。



2. ［Host］ボックスに、StoreFrontまたはWeb Interfaceサイト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。
3. ［Port］ボックスに、StoreFrontまたはWeb Interfaceサイトのポート番号を入力します。デフォルトは80です。
4. ［Relative Path］ボックスにパスを入力します。たとえば、「/Citrix/Store/PNAgent/config.xml」と入力します。
5. ［Use HTTPS］で［ON］を選択して、StoreFrontまたはWeb Interfaceサイトとクライアントデバイスの間の安全な認証を有効にします。デフォルトは［OFF］です。
6. **［Save］**をクリックします。

XenMobileのサポートおよび保守

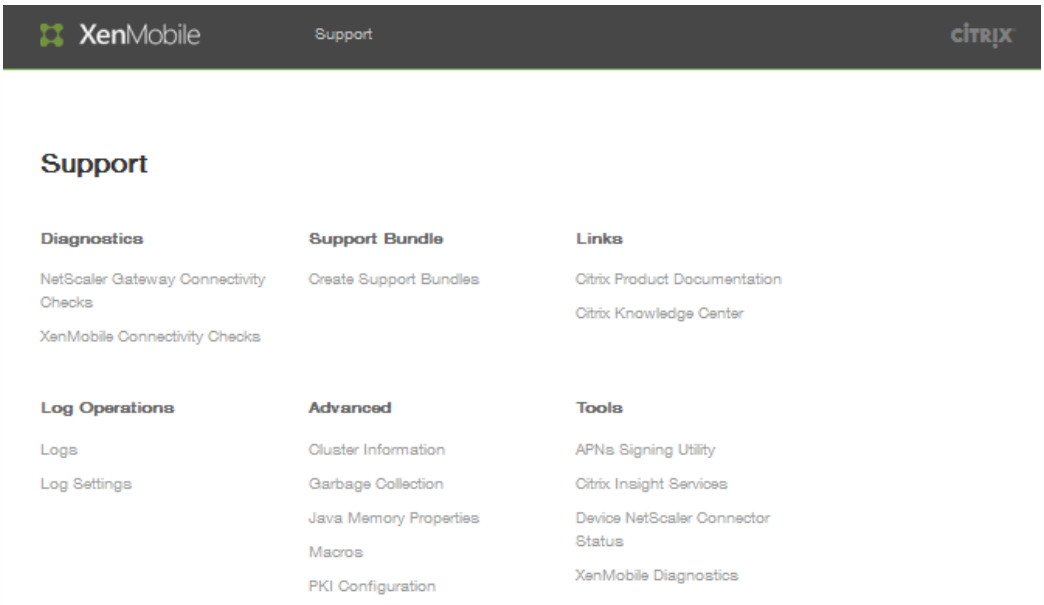
Oct 24, 2016

［XenMobile Support］ページを使用して、サポートに関連する多くの情報とツールにアクセスします。 また、コマンドラインインターフェイスからもアクションを実行できます。 詳しくは、「XenMobileコマンドラインインターフェイスオプション」を参照してください。

［Support］ページにアクセスするには

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。

ブラウザーの別のタブで、［Support］ページが開きます。



［XenMobile Support］ページを使用して以下を行います。

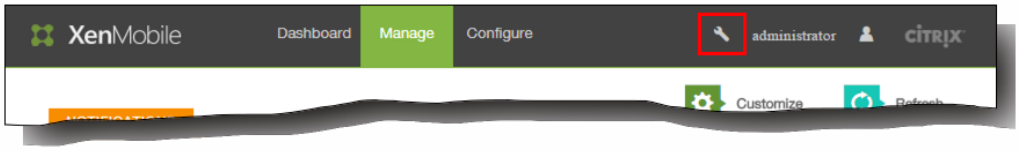
- 診断へのアクセス
- サポートバンドルの作成
- Citrixの製品ドキュメントおよびKnowledge Centerへのリンクへのアクセス
- ログ操作へのアクセス
- 一連の詳細情報および構成オプションからの選択
- 一連のツールおよびユーティリティへのアクセス

接続確認の実行

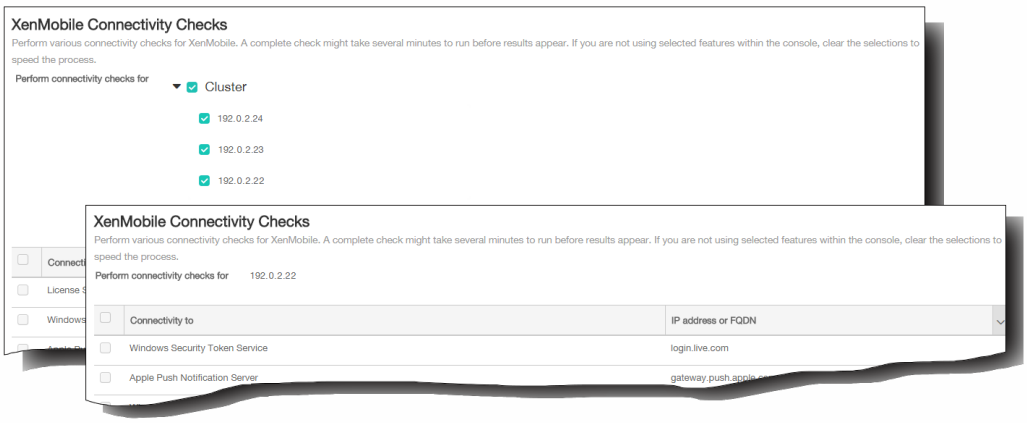
May 10, 2016

［XenMobile Support］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。［Support］ページにアクセスするには、以下を実行します。

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。 このレンチアイコンは、XenMobileコンソールのどのページにもあります。ユーザー名とパスワードの入力を求められる可能性があります。



ブラウザーの新しいタブで、［XenMobile Support］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。



XenMobileの接続確認の実行

1. ［Support］ページで、［XenMobile Connectivity Checks］をクリックします。 ［XenMobile Connectivity Checks］ページが開きます。
2. 接続テストに含めるサーバーをオンにして、［Test Connectivity］をクリックします。 結果が表示されます。
3. ［Test Results］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

NetScaler Gatewayの接続確認の実行

1. ［Support］ページで、［NetScaler Gateway Connectivity Checks］をクリックします。 ［NetScaler Gateway Connectivity Checks］ページが開きます。
2. ［Add］をクリックします。 ［Add NetScaler Gateway Server］ダイアログボックスが開きます。
3. ［NetScaler Gateway Management IP］ボックスに、テストするNetScaler Gatewayを実行しているサーバーのIPアドレスを入力します。
   注：既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、IPアドレスは入力されています。
4. このNetScaler Gatewayの管理者資格情報を入力します。
   注：既に追加されているNetScaler Gatewayサーバーの接続確認を実行する場合、ユーザー名は入力されています。

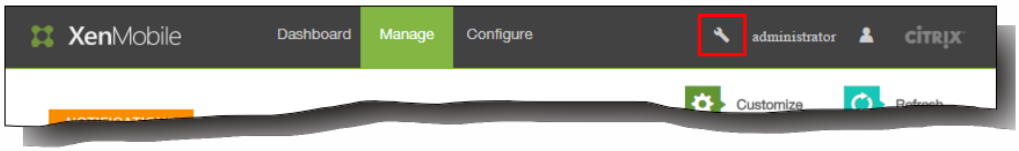
5. ［Add］をクリックします。 NetScaler Gatewayが、［NetScaler Gateway Connectivity Checks］ページの表に追加されます。
6. ［Test Connectivity］をクリックします。 ［Test Results］の表に結果が表示されます。
7. ［Test Results］の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

XenMobileでのサポートバンドルの作成

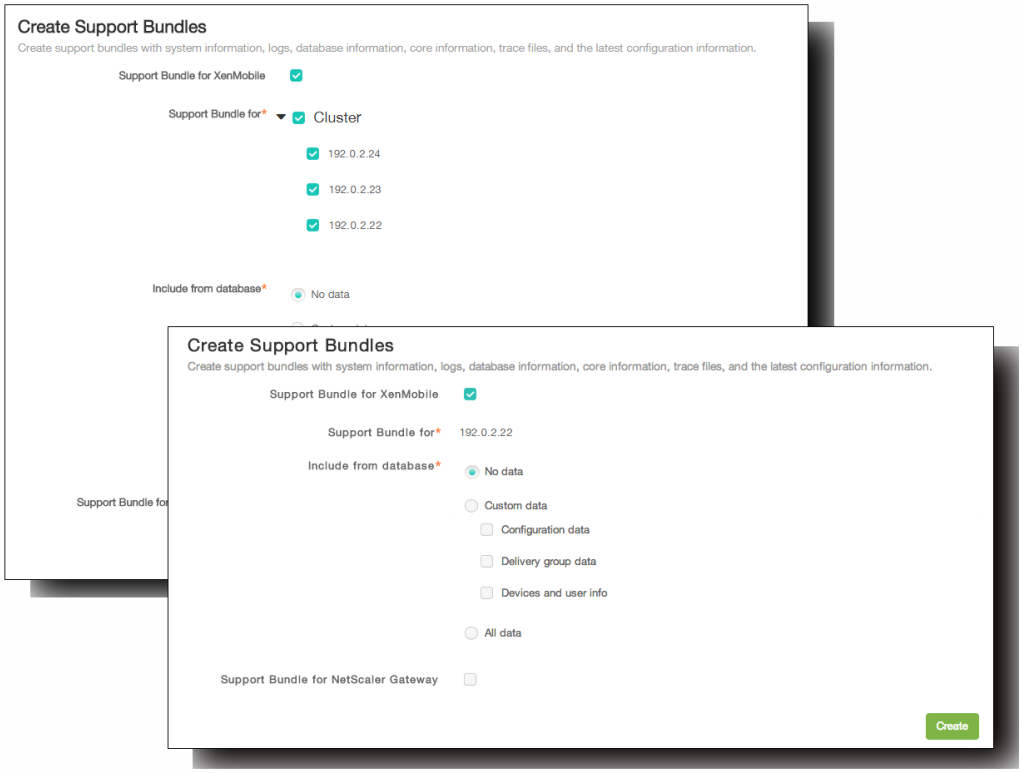
May 10, 2016

Citrixに問題を報告する場合や問題をトラブルシューティングする場合、サポートバンドルを作成してCitrix Insight Services（CIS）にアップロードできます。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。 このレンチアイコンは、XenMobileコンソールのどのページにもあります。
   注：ユーザー名とパスワードの入力を求められる可能性があります。



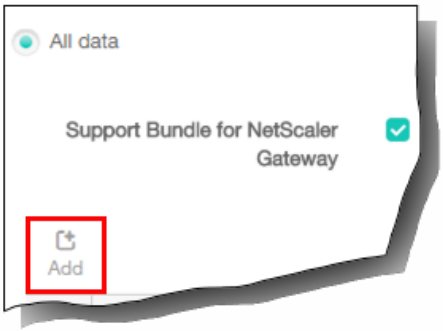
   ブラウザーの新しいタブで、［XenMobile Support］が開きます。
2. ［Support］ページで、［Create Support Bundles］をクリックします。 ［Create Support Bundles］ページが開きます。
   XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。



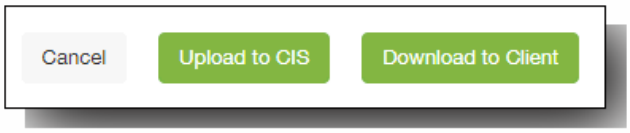
3. ［Support Bundle for XenMobile］チェックボックスがオンになっていることを確認します。
4. XenMobile環境内にクラスターノードがある場合は、［Support Bundle for］ですべてのノードを選択するか、データを取得するノードの組み合わせを選択できます。
5. ［Include from Database］で、次のいずれかを実行します。
   - ［No data］をクリックします。

- ［Custom data］をクリックして、次のいずれかまたはすべてをオンにします。
  - ［Configuration data］。証明書構成とデバイスマネージャーポリシーを含めます。
  - ［Delivery group data］。アプリケーションの種類やアプリケーションデリバリーポリシー詳細など、アプリケーションのデリバリーグループの情報を含めます。
  - ［Devices and user info］。デバイスポリシー、アプリケーション、アクション、デリバリーグループを含めます。
- ［All data］をクリックします。

6. NetScaler Gatewayからのサポートバンドルを含める場合は、［Support Bundle for NetScaler Gateway］をオンにして以下を行います。
   1. ［Add］をクリックします。



   ［Add NetScaler Gateway Server］ダイアログボックスが開きます。
   2. ［NetScaler Gateway Management IP］ボックスに、サポートバンドルを取得する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。
   3. ［User name］ボックスと［Password］ボックスに、NetScaler Gatewayを実行しているサーバーへのアクセスに必要なユーザー資格情報を入力します。
   注：既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、ユーザー名は入力されています。
   4. ［Add］をクリックします。 新しいNetScaler Gatewayサポートバンドルが表に追加されます。
   5. 必要に応じて手順6.を繰り返し、ほかのNetScaler Gatewayサポートバンドルを追加します。
7. ［Create］をクリックします。 サポートバンドルが作成され、［Upload to CIS］と［Download to Client］の2つの新しいボタンが表示されます。



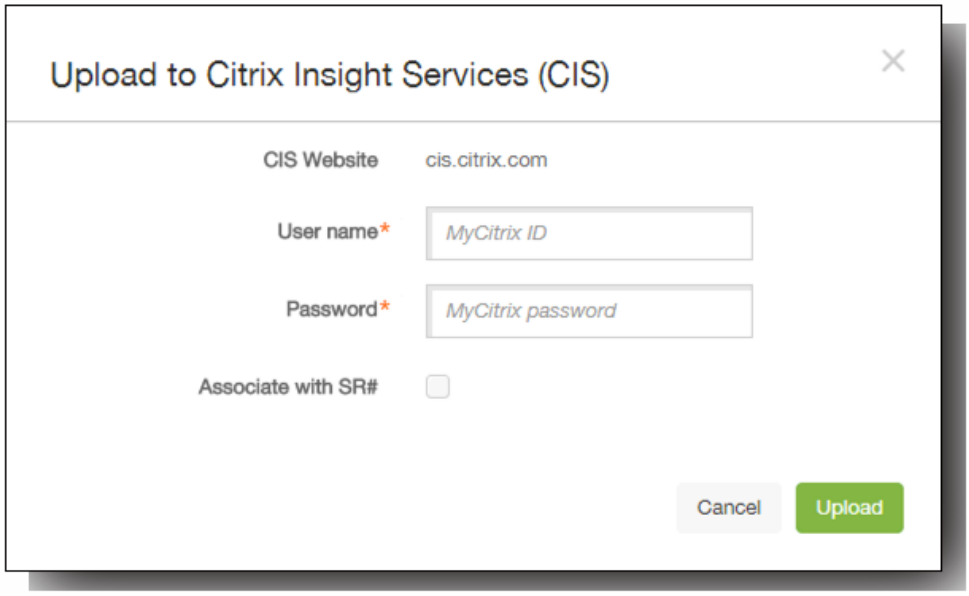
「**Citrix Insight Servicesへのサポートバンドルのアップロード**」または「**コンピューターへのサポートバンドルのダウンロード**」の手順に進みます。

Citrix Insight Servicesへのサポートバンドルのアップロード

サポートバンドルを作成した後、Citrix Insight Services（CIS）にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。以下の手順は、CISにバンドルをアップロードする方法を示しています。

1. ［Create Support Bundles］ページで、［Upload to CIS］をクリックします。 ［Upload to Citrix Insight Services (CIS)］ダ

イアログボックスが開きます。



2. ［User Name］ボックスにMyCitrix IDを入力します。
3. ［Password］ボックスにMyCitrixパスワードを入力します。
4. このバンドルを既存のサービスリクエスト番号に関連付ける場合は、［Associate with SR#］チェックボックスをオンにし、新たに表示される2つのフィールドで以下を実行します。
   1. ［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。
   2. ［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。 サポートバンドルがCISに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。

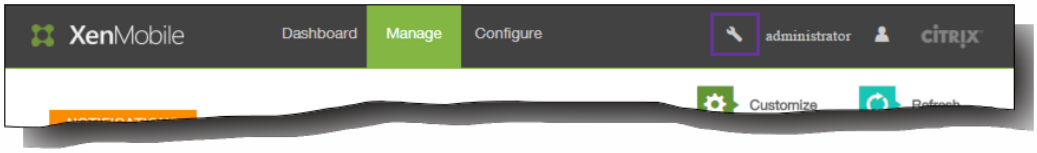
［Create Support Bundles］ページで、［Download to Client］をクリックします。バンドルがコンピューターにダウンロードされます。

デバッグログファイルを表示するには

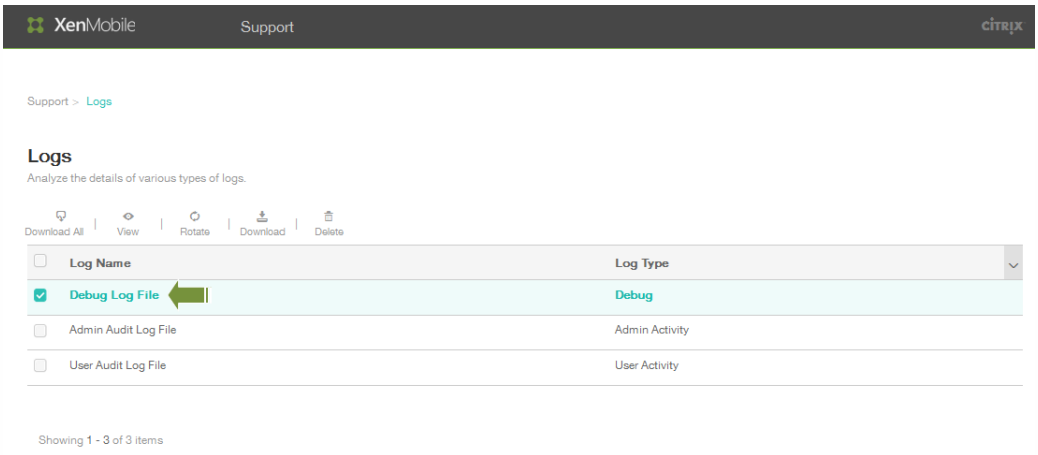
May 10, 2016

Citrixに問題を報告する場合や問題をトラブルシューティングする場合、サポートバンドルを作成してCitrix Insight Services（CIS）にアップロードできます。

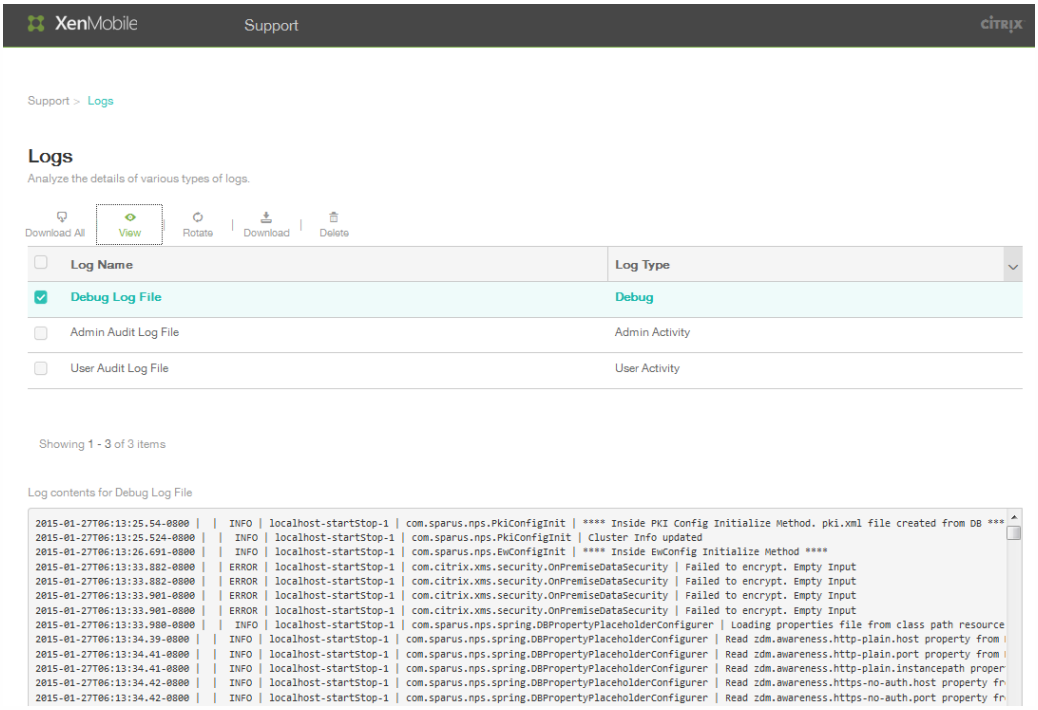
1. XenMobileコンソールで、右上のレンチアイコンをクリックします。 このレンチアイコンは、XenMobileコンソールのどのページにもあります。



2. ［Support］ページで、［Logs］をクリックします。 ［Logs］画面が開きます。



3. ［Debug Log File］を選択してから［View］をクリックして、ログの内容を表示します。



ログファイルを分析したら、［Download File］を使用してデータを保存するか、［Delete］をクリックしてデータベースからログの内容を削除します。

ログ設定を構成するには

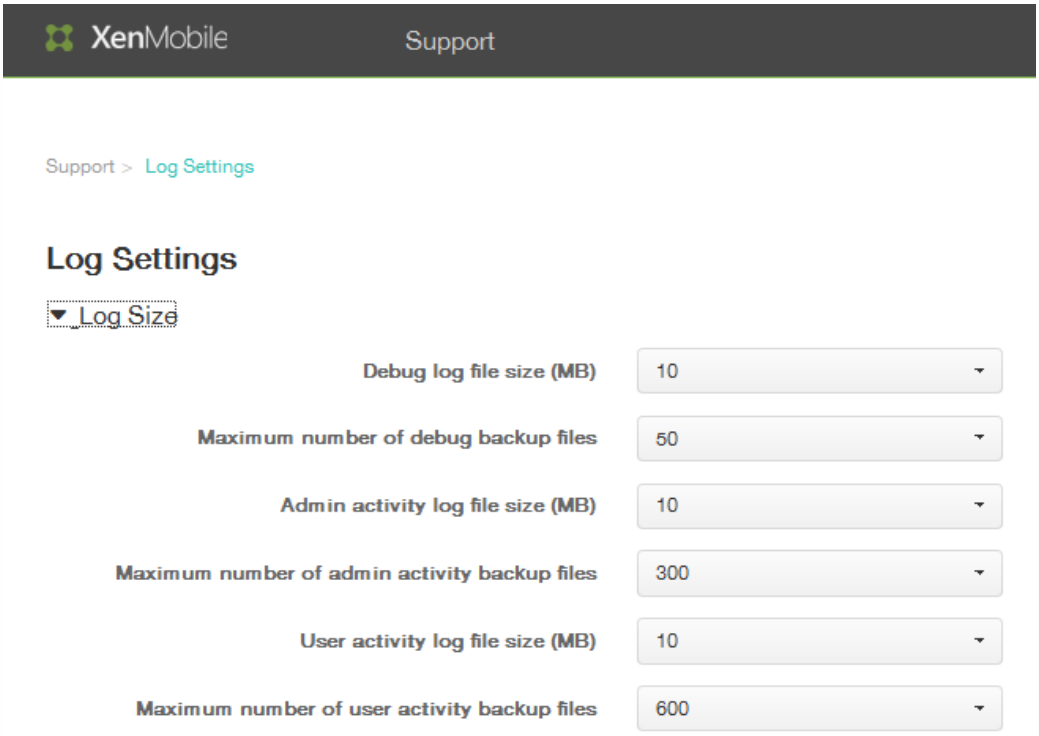
May 10, 2016

ログ設定を構成して、XenMobileで生成されるログの出力をカスタマイズすることができます。XenMobileコンソールで、［Support］の［Log Settings］をクリックして次のオプションにアクセスします。

- 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、クラス名、サブクラス名、ログレベルを変更するか、設定を保持します。
- 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. ［Support］の［Log Settings］をクリックして、［Log Size］を展開します。

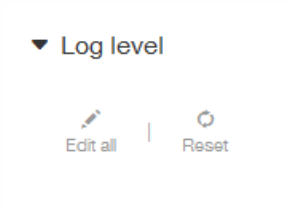


2. ［Debug log file size（MB）］ボックスの一覧で、サイズ（5～20MB）を選択して、デバッグファイルの最大サイズを変更します。 デフォルトでは、ファイルのサイズは10MBに設定されています。
3. ［Maximum number of debug backup files］ボックスの一覧で、デバッグファイルの数（5～300）を選択して、サーバーで保持されるデバッグファイルの最大数を変更します。 デフォルトでは、サーバーに50件のバックアップファイルが保持されます。
4. ［Admin activity log］ボックスの一覧で、サイズ（5～20MB）を選択します。 デフォルトでは、ファイルのサイズは10MBに設定されています。
5. ［Maximum number of admin backup files］ボックスの一覧で、サーバーで保持される管理者アクティビティバックアップファイルの最大数として、デバッグファイルの数（5～300）を選択します。 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。

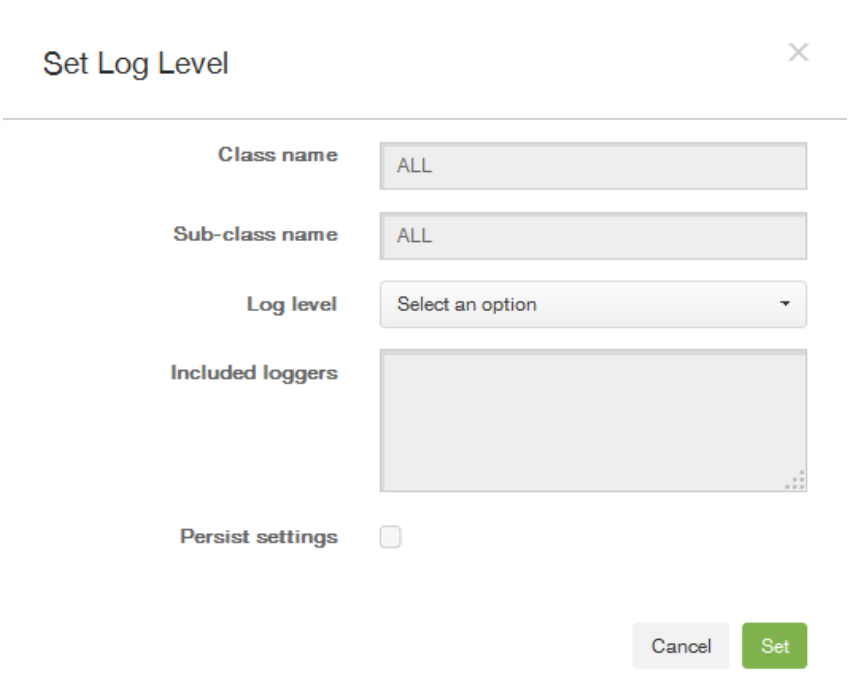
6. ［User activity log size］ボックスの一覧で、サイズ（5～20MB）を選択します。 デフォルトでは、ファイルのサイズは10MBに設定されています。
7. ［Maximum number of admin backup files］ボックスの一覧で、サーバーで保持される管理者アクティビティバックアップファイルの最大数として、デバッグファイルの数（5～300）を選択します。 デフォルトでは、サーバーに300件のバックアップファイルが保持されます。

［Log Level］のオプションを構成するには

1. ［Support］の［Log Settings］をクリックして、［Log level］を展開し、構成オプションを表示します。 ［Edit all］をクリックして、ログレベルの要素を構成します。



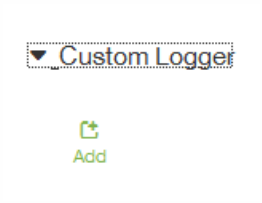
［Set Log Level］画面が開きます。



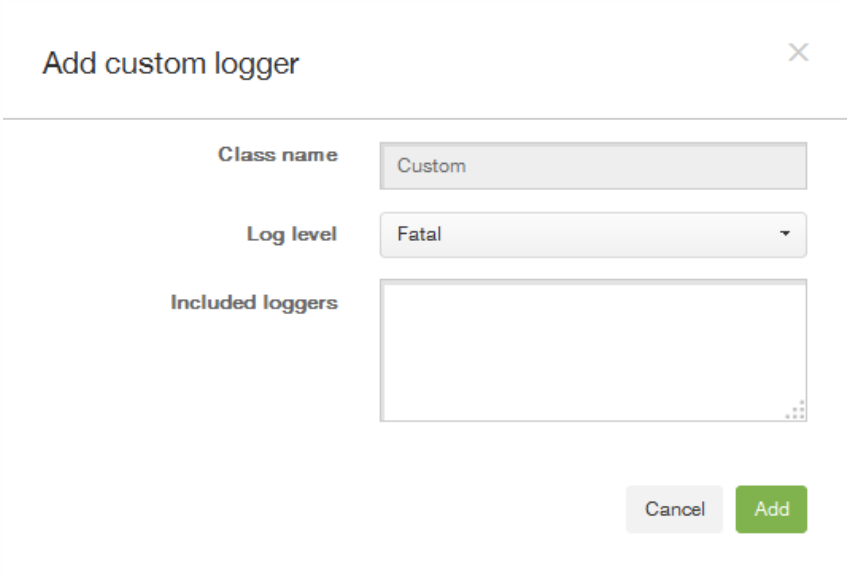
2. ［Class Name］ボックスにクラス名を入力します。 デフォルトでは、このフィールドは[All］に設定されています。
3. ［Sub-class name］ボックスにサブクラス名を入力します。 デフォルトでは、このフィールドは[All］に設定されています。
4. ［Log level］ボックスの一覧で、ログレベルを選択します。 サポートされるログレベルには、［Fatal］、［Error］、［Warning］、［Info］、［Debug］、［Trace］、［Off］などがあります。 ［Included Loggers］フィールドに、構成されている各クラスに対して、現在構成されているログレベルが表示されます。
5. ログレベルの設定を保持する場合は、［Persist settings］チェックボックスをオンにします。
6. ［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. カスタムロガーを追加するには、［Add］をクリックします。



［Add custom logger］画面が開きます。

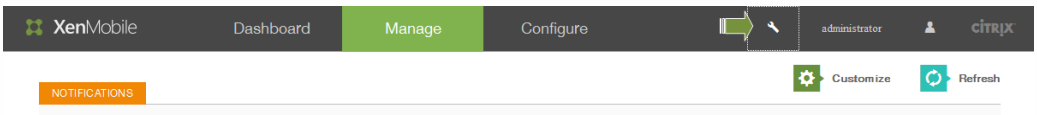


2. ［Class name］ボックスにクラス名を指定します。
3. ［Log level］ボックスの一覧で、ログレベルを選択します。 サポートされるログレベルには、［Fatal］、［Error］、［Warning］、［Info］、［Debug］、［Trace］、［Off］などがあります。 ［Included Loggers］フィールドに、構成されている各クラスに対して、現在構成されているログレベルが表示されます。
4. ［Add］をクリックします。

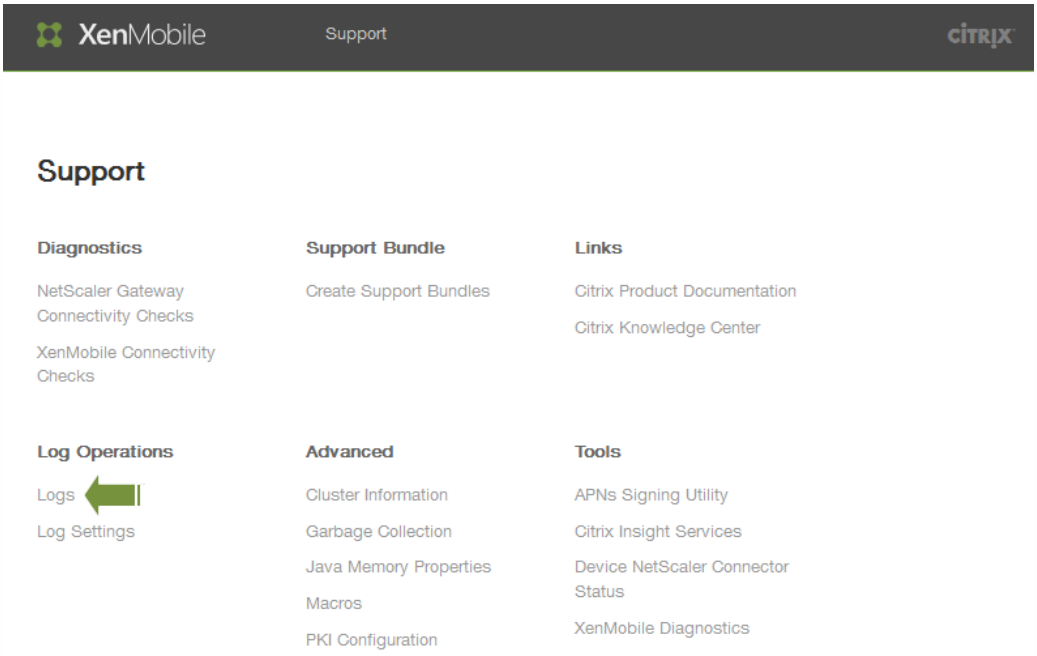
XenMobileでのログファイルの表示および分析

May 10, 2016

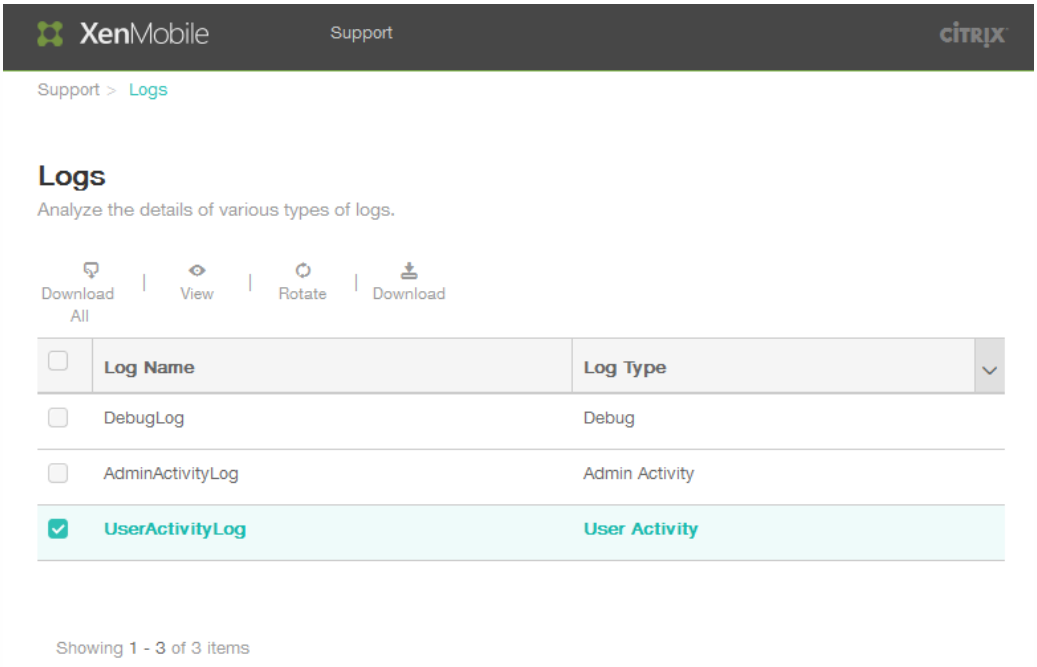
1. XenMobileコンソールで、右上のレンチアイコン（ ）をクリックします。 ブラウザーの新しいウィンドウで、［Support］ページが開きます。



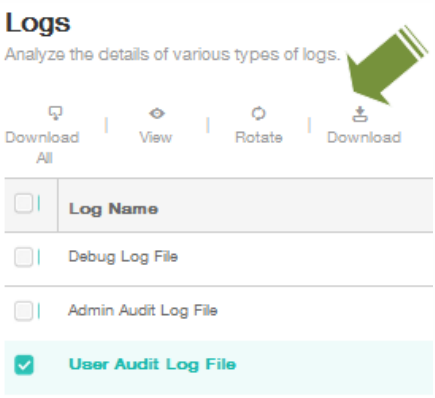
2. ［Log Operations］の下の**［Logs］**をクリックします。 **［Logs］**画面が開きます。表に個別のログが表示されます。



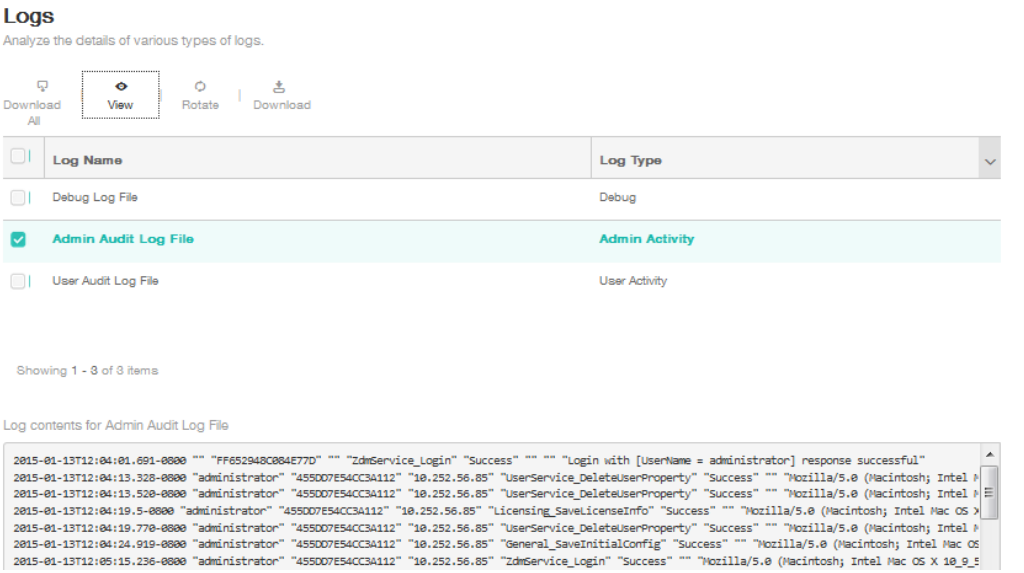
3. 表示するログをオンにします。 デバッグログには、Citrixのサポート担当者用の役立つ情報が含まれています。エラーメッセージやサーバー関連のアクションなどの有用な情報が含まれています。 ユーザーアクティビティログには、各構成済みユーザーに関連する情報が表示されます。 **［Logs］**画面が開きます。表に個別のログが表示されます。



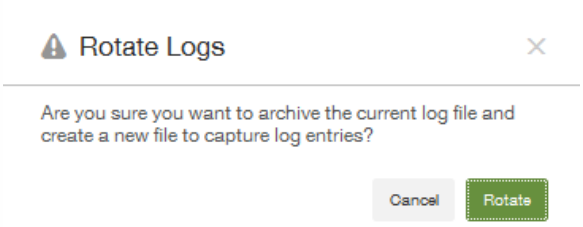
4. 表の上にあるアクションを使用して以下を行います。
   - Download All：システム上に存在するすべてのログ（デバッグログ、ユーザー/管理者アクティビティログ、サーバーログなど）をダウンロードします。［Download］をクリックすると、オンにしたログのみを保存できます（アーカイブされているログもダウンロードされます）。



   - View：表の下にログの内容を表示します。



- Delete：選択したログファイルを完全に削除します。
- Rotate：現在のログファイルをアーカイブし、ログエントリを取得するための新しいファイルを作成します。ログファイルをアーカイブするときに、ダイアログボックスが開きます。［Rotate］をクリックして続行します。



XenMobileコマンドラインインターフェイスオプション

May 10, 2016

XenMobileをインストールしたハイパーバイザー（Citrix XenServer、Microsoft Hyper-V、VMware ESXi）で、以下のコマンドラインインターフェイス（CLI）オプションにいつでもアクセスできます。

以下は［Main menu］（メインメニュー）から選択できるオプションで、［Configuration］、［Clustering］、［System］、［Troubleshooting］の4つのオプションがメニューの最初に表示されます。

Main menu

---

[0] Configuration

[1] Clustering

[2] System

[3] Troubleshooting

[4] Help

[5] Log Out

Choice: [0 - 5]

［Configuration］メニューオプション

メインメニューから［Configuration］オプションを選択すると、次のメニューが表示されます。

[0] Back to Main Menu

[1] Network

[2] Firewall

[3] Database

[4] Listener Ports

Choice: [0 - 4]

［Network］オプションを選択した場合は、変更を保存するために再起動を求めるメッセージが表示されます。

［Firewall］オプションを選択した場合は、以下のメッセージが表示されます。

Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:

- comma separated list of hosts or networks

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

- enter c as value to clear list

HTTPサービス

Port: 80

Enable access (y/n) [y]:

Management HTTPS service

Port: 4443

Enable access (y/n) [y]:

SSHサービス

Port [22]:

Enable access (y/n) [y]:

Access white list []:

Management API (for initial staging) HTTPS service

Port [30001]:

Enable access (y/n) [y]:

Access white list []:

Remote support tunnel

Port [8081]:

Enable access (y/n) [n]:

［Database］オプションを選択した場合は、以下のメッセージが表示されます。

Type: [mi]

Use SSL (y/n) [y]:

Upload Root Certificate (y/n) [y]:

Copy or Import (c/i) [c]:

［Clustering］メニューオプション

メインメニューから［Clustering］オプションを選択すると、次のメニューが表示されます。

[0] Back to Main Menu

[1] Show Cluster Status

[2] Enable/Disable cluster

[3] Cluster member white list

[4] Enable or Disable SSL offload

[5] Display Hazelcast Cluster

Choice: [0 - 5]

クラスタリングの有効化を選択すると、次のメッセージが表示されます。

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

クラスタリングの無効化を選択すると、次のメッセージが表示されます。

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

クラスタリングが無効になっている場合に［Cluster member white list］を選択すると、次のメッセージが表示されます。

Cluster is disabled.Please enable it.

クラスタリングを有効にした場合は、次のオプションが表示されます。

Current White List:

- comma separated list of hosts or network

- e.g. 10.20.5.3, 10.20.6.0/24

- an empty value means no access restriction

Please enter hosts or networks to be white listed:

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

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

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

Hazlecast Cluster Members:

[IP address listed]

NOTE: If an configured node is not part of the cluseter, please reboot that node.

［System］メニューオプション

メインメニューから［System］オプションを選択すると、次のメニューが表示されます。

```
------------------------------

[0] Back to Main Menu

[1] Display System Date

[2] Set Time Zone

[3] Display System Disk Usage

[4] Update Hosts File

[5] Proxy Server

[6] Admin (CLI) Password

[7] Restart Server

[8] Shutdown Server

[9] Advanced Settings

------------------------------

Choice: [0 - 9]
```

［Troubleshooting］メニューオプション

メインメニューから［Troubleshooting］オプションを選択すると、次のメニューが表示されます。

```
------------------------------

[0] Back to Main Menu

[1] Network Utilities

[2] Logs

[3] Support Bundle

------------------------------

Choice: [0 - 3]
```

［Network Utilities］オプションを選択した場合は、次のメニューが表示されます。

```
------------------------------

[0] Back to Troubleshooting Menu
```


[1] Network Information

[2] Show Routing Table

[3] Show Address Resolution Protocol (ARP) Table

[4] PING

[5] Traceroute

[6] DNS Lookup

[7] Network Trace

Choice: [0 - 7]

［Logs］オプションを選択した場合は、次のメニューが表示されます。

Logs Menu

---

[0] Back to Troubleshooting Menu

[1] Display Log File

Choice: [0 - 1]

XenMobile 10 API

May 10, 2016

XenMobile 10でのモバイルデバイス管理には、以下のWebサービスAPIを使用できます。XenMobile用のAPIおよびSDKは、XenMobile Developer Communityのサイトでダウンロードできます。

Web Service Definition Language（WSDL）名	呼び出し
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

Web Service Definition Language（WSDL）名	呼び出し
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice

Web Service Definition Language（WSDL）名	呼び出し
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	createOTP
	getAvailableEnrollmentModes
	getOtpInfo
	triggerNotification

XenMobile Mail Manager 10

May 10, 2016

XenMobile Mail Managerには、XenMobileの機能を拡張する以下の機能が備わっています。

- Exchange ActiveSync（EAS）デバイスに対するダイナミックアクセス制御。EASデバイスのExchangeサービスに対するアクセスを自動的に許可または禁止できます。
- Exchangeが提供するEASデバイスパートナーシップ情報にアクセスする機能のXenMobileへの提供。
- モバイルデバイスでEASワイプを実行する機能のXenMobileへの提供。
- Blackberryデバイスに関する情報にアクセスしたり、ワイプやパスワードリセットなどの制御操作を実行したりする機能のXenMobileへの提供。

以下は、XenMobile Mail Manager 10.0の現在のリリースの既知の問題と解決された問題です。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。

既知の問題

- XenMobile Mail Manager 10にアップグレードする間、インストールされたXenMobile Mail Managerのバージョンは常に8.5として表示されます。ただし、XenMobile Mail Managerのアップグレードは実行されます。[#539520]
- マイナースナップショットの“devices found”報告で混乱が生じることがあります。マイナースナップショットがメジャースナップショットの開始に引き続いて実行される場合、連続したマイナースナップショットの概要では同じデバイスが“new”として報告されることがあります。

解決された問題

PowerShellまたはExchangeの管理

特定のMicrosoft Exchange環境（主にOffice 365）では、帯域幅を効果的に制限するXenMobile Mail Managerに制限が課され、アプリケーションがPowerShell要求またはコマンドを発行できなくなります。現在では、Exchange構成タブで代わりのPowerShellコマンドレットパスウェイを使用できます。これにより、XenMobile Mail Managerが代替スナップショットモードになります。このモードでは、元のデータパスが回避されます。

新しいフラグで、Microsoft Office 365以外の環境の**AllowRedirection**フラグを公開できます。Microsoft Exchange構成タブを使用してこのフラグを有効化します。

規則の管理

LDAPローカル規則で、大規模なActive Directory環境の整理されていない数のグループがサポートされるようになりました。

XenMobileではWorxMailクライアントのデバイス情報が重複します。この問題を解決するには、XenMobile Mail ManagerのManaged Service Provider（MSP）の部分で正規表現のサポートを有効にする必要があります。こうすることで、XenMobileに返されるレコードセットがフィルタリングされます。フィルターに一致するデバイスはXenMobileに返されません。

MSP

BlackBerry Enterprise Server（BES）から削除されるユーザーがローカルデータベースから削除されるようになりました。

UI

永続的プロセスが実行されているシナリオで、進行状況のダイアログボックスクラスを使用できるようになりました。このようなプロセスでは、XenMobile Mail Managerからユーザーにフィードバックが送信され、取り消す機会が提供されます（該

当する場合）。

新しいMicrosoft Exchangeインスタンスのデフォルト値が *[Shallow]* に設定されるようになりました。

インストーラー

Zenpriseを参照するコンポーネントがXenMobile Mail Managerを反映するように変更されました。

インストールパスが見つからない場合、インストーラーがハングします。

インストール後に、サポートバイナリおよびスクリプトがSupportフォルダーに配置されるようになりました。

Windowsの［スタート］メニューで、XenMobile Mail Managerのショートカットが\Citrix\XenMobile Mail Managerフォルダーに配置されるようになりました。

サポート

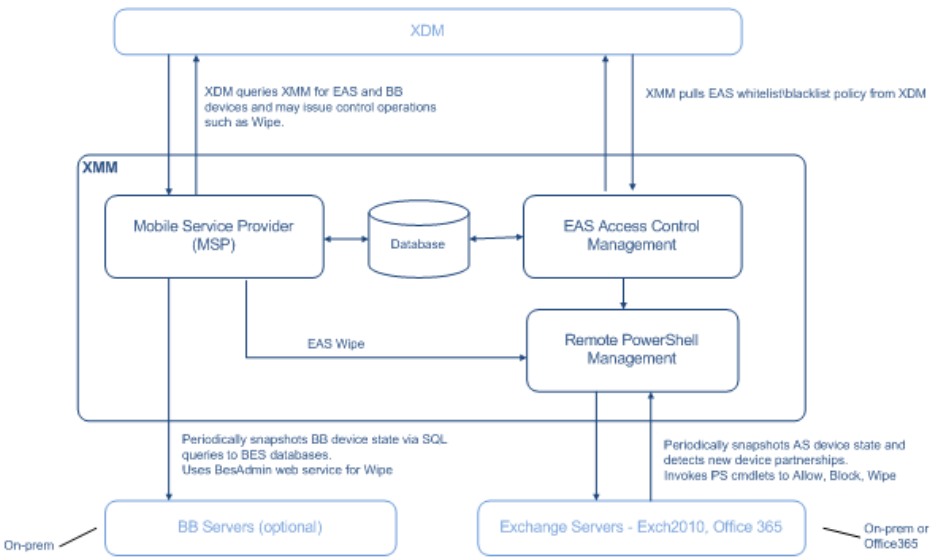
サポートモデルでは、config.xmlファイルの追加によってトラブルシューティング機能を有効化できます。このファイルを使用して、Citrixが問題をトラブルシューティングするのに役立てることができます。このリリースのXenMobile Mail Managerでは、この機能はMicrosoft Exchange構成の［追加］と［編集］の画面にのみ適用されます。
注：Shiftキーを押しながら構成ユーティリティを開いて、このトラブルシューティング機能を有効化することもできます。
ログ記録機能

PowerShellから返されるエラーメッセージに、関連するGUIDが含まれるようになりました。この値を使用して、[Snapshot History］詳細タブに表示される内容を制御します。

アーキテクチャ

Oct 24, 2016

次の図は、XenMobile Mail Managerの主要コンポーネントを示しています。 リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の、「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

May 10, 2016

XenMobile Mail Managerを使用するには、以下のシステム環境が必要です。

- Windows Server 2008 R2（英語ベースのサーバーであることが必須）
- Microsoft SQL Server 2008、SQL Server 2012、SQL Server Express 2008、SQL Server 2012、またはMicrosoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5。
- Blackberry Enterprise Service, version 5（オプション）

Microsoft Exchange Serverのサポートされる最小バージョン

- Microsoft Office 365
- Exchange Server 2013
- Exchange Server 2010 SP2

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 V4、V3、およびV2
- 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の役割ベースのアクセス制御（Role-Based Access Control：RBAC）については、このドキュメントでは扱いません。最小限の情報として、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ることのみを取り上げます。
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- フォレスト全体を表示するようにXenMobile Mail Managerが構成されている場合は、次のコマンドレットを実行するための権限が付与されている必要があります。Set-AdServerSettings -ViewEntireForest $true
- 指定された資格情報には、リモートシェルを介して、Exchange Serverに接続する権限が与えられている必要があります。デフォルトでは、Exchangeをインストールしたユーザーがこの権限を持ちます。
- https://technet.microsoft.com/ja-jp/library/dd315349.aspxに記載されているように、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。http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx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、必要なのはExchange Serverで次のPowerShellコマンドを実行する管理者のみです。WinRM QuickConfig.
- Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可される

PowerShellの同時接続数が制御されます。Exchange 2010の場合、1人のユーザーに許可されている同時接続数のデフォルトは18です。接続数の上限に達すると、XenMobile Mail ManagerはExchange Serverに接続できなくなります。PowerShe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

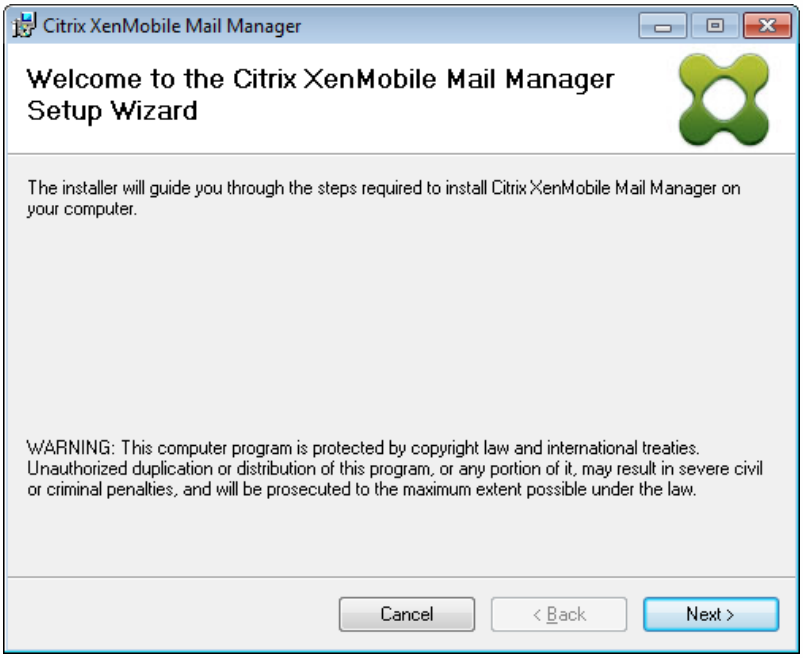
- **権限**。Exchangeの役割ベースのアクセス制御（Role-Based Access Control：RBAC）については、このドキュメントでは扱いません。最小限の情報として、Exchangeの構成UIで指定される資格情報を使用してOffice 365に接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセスが付与される必要があることのみを取り上げます。
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- 指定された資格情報には、リモートシェルを介して、Office 365サーバーに接続する権限が与えられている必要があります。デフォルトでは、Office 365のオンライン管理には、必要な権限が備えられています。
- Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。Office 365の場合、1人のユーザーに許可されている同時接続数のデフォルトは3です。接続数の上限に達すると、XenMobile Mail ManagerはExchange Serverに接続できなくなります。PowerShellの同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShellによるリモート管理に関連する、Exchangeの調整ポリシーについて調べてください。

インストールおよび構成

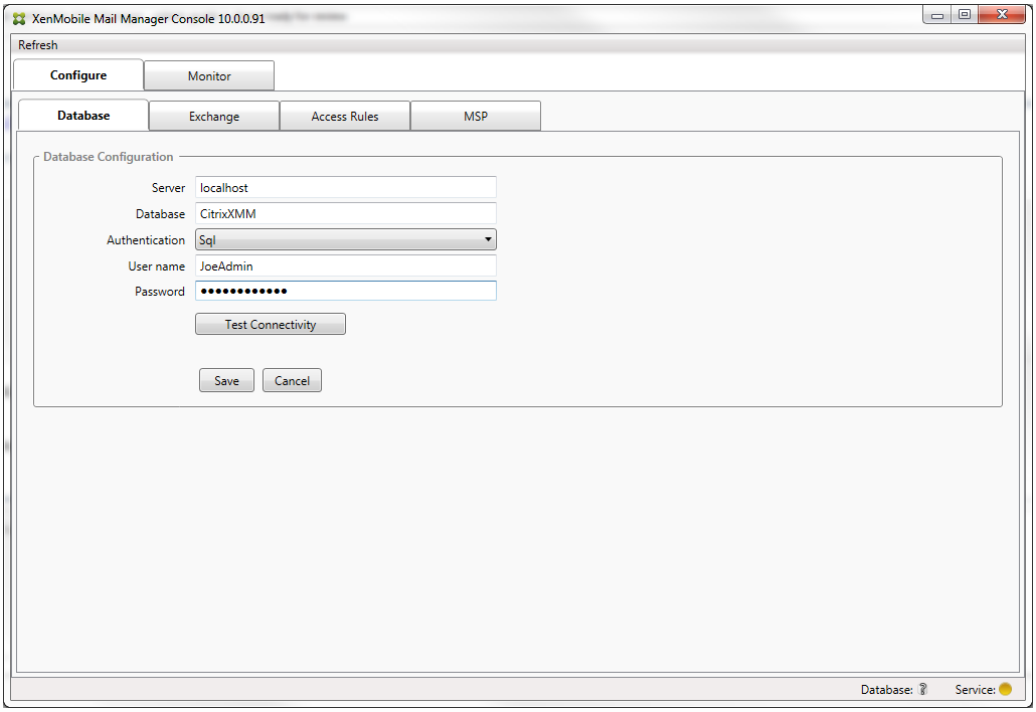
May 10, 2016

XenMobile Mail Managerをインストールして構成するには、次の手順に従います。開始する前に、システム要件と前提条件を確認してください。詳しくは「XenMobile Mail Managerのシステム要件および前提条件」を参照してください。

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。

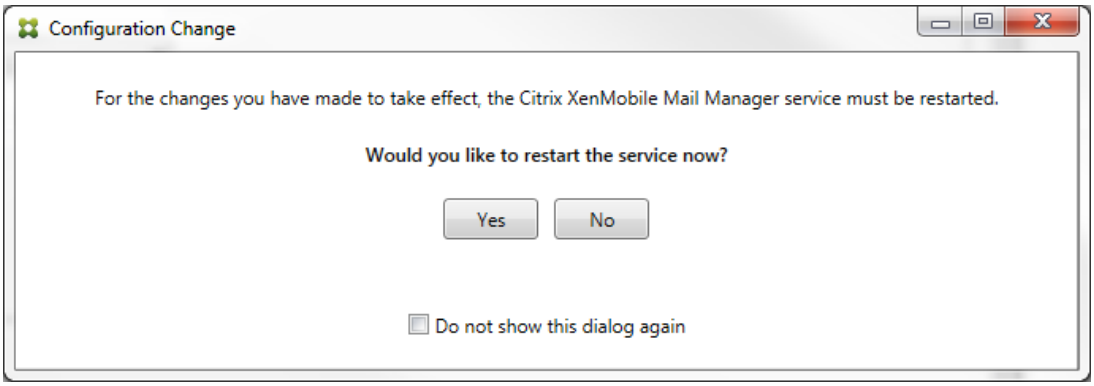


2. ［スタート］メニューの［XenMobile Mail Manager］を選択します。
3. 次のデータベースプロパティを構成します。
    1. ［Configure］の［Access Rules］タブを選択します。
    2. SQL Serverの名前（デフォルトはlocalhost）を入力します。
    3. データベースはデフォルトのCitrixXmmのままにします。
    4. SQLに使用される次のいずれかの認証モードを選択します。
        - Sql。有効なSQLユーザーのユーザー名とパスワードを入力します。
        - Windows Integrated。このオプションを選択した場合、XenMobile Mail Managerサービスのログオン資格情報を、SQL Serverにアクセスするための権限を持つWindowsアカウントに変更する必要があります。これを行うには、［コントロールパネル］、［管理ツール］、［サービス］の順に選択し、XenMobile Mail Managerサービスエントリをクリックし、［ログオン］タブをクリックします。
          注：BlackBerryデータベース接続に対しても［Windows Integrated］を選択している場合は、ここで指定されているWindowsアカウントにBlackBerryデータベースへのアクセスも付与する必要があります。

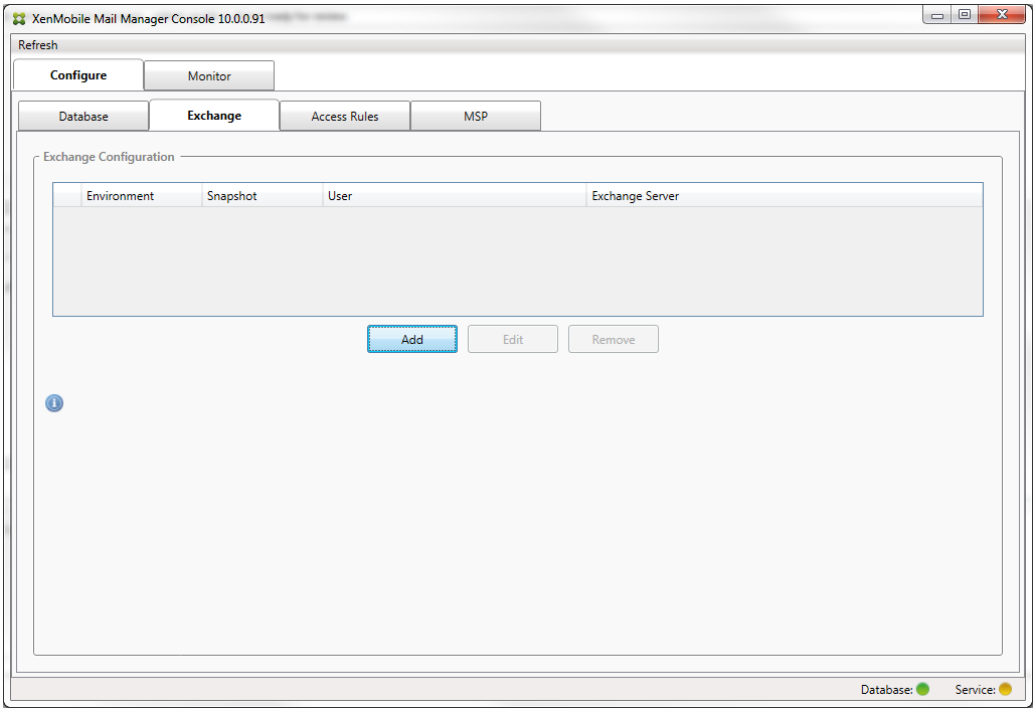


5. ［Test Connectivity］をクリックしてSQL Serverに接続できることを確認し、［Save］をクリックします。

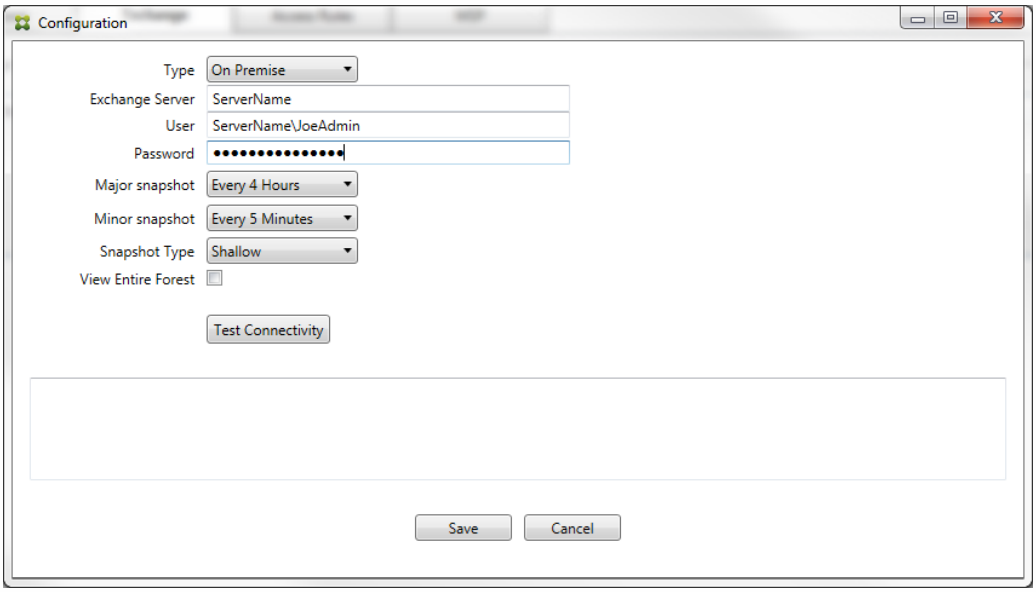
4. サービスの再起動を求めるメッセージが表示されます。［Yes］をクリックします。



5. 1つまたは複数のExchange Serverを構成します。
    1. 単一のExchange環境を管理している場合は、単一のサーバーを指定する必要があるのみです。 複数のExchange環境を管理している場合は、Exchange環境ごとに単一のExchange Serverを指定する必要があります。
    2. ［Configure］の［Exchange］タブをクリックします。



3. ［Add］をクリックします。
4. Exchange Server環境の種類として［On Premise］または［Office 365］を選択します。

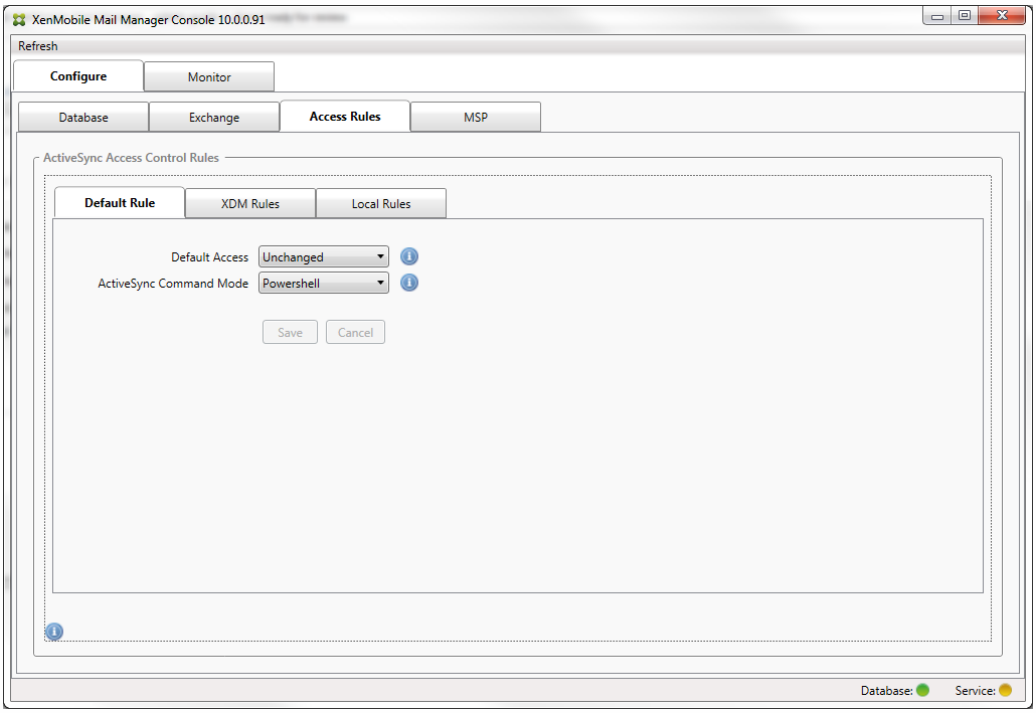


5. ［On Premise］を選択した場合は、リモートPowerShellコマンド用に使用するExchange Serverの名前を入力します。
6. 要件セクション内で指定されているとおりの、Exchange Serverに対する適切な権限を持つWindows IDのユーザー名を入力します。
7. ユーザーのパスワードを［Password］ボックスに入力します。
8. メジャースナップショットを実行するスケジュールを選択します。 メジャースナップショットにより、すべてのExchange ActiveSyncパートナーシップが検出されます。
9. マイナースナップショットを実行するスケジュールを選択します。 マイナースナップショットにより、新しく作成されたExchange ActiveSyncパートナーシップが検出されます。
10. スナップショットの種類として、［Deep］または［Shallow］を選択します。 通常、簡易スナップショットははるかに高速で、XenMobile Mail ManagerのExchange ActiveSyncアクセス制御機能をすべて実行するには十分です。詳細ス

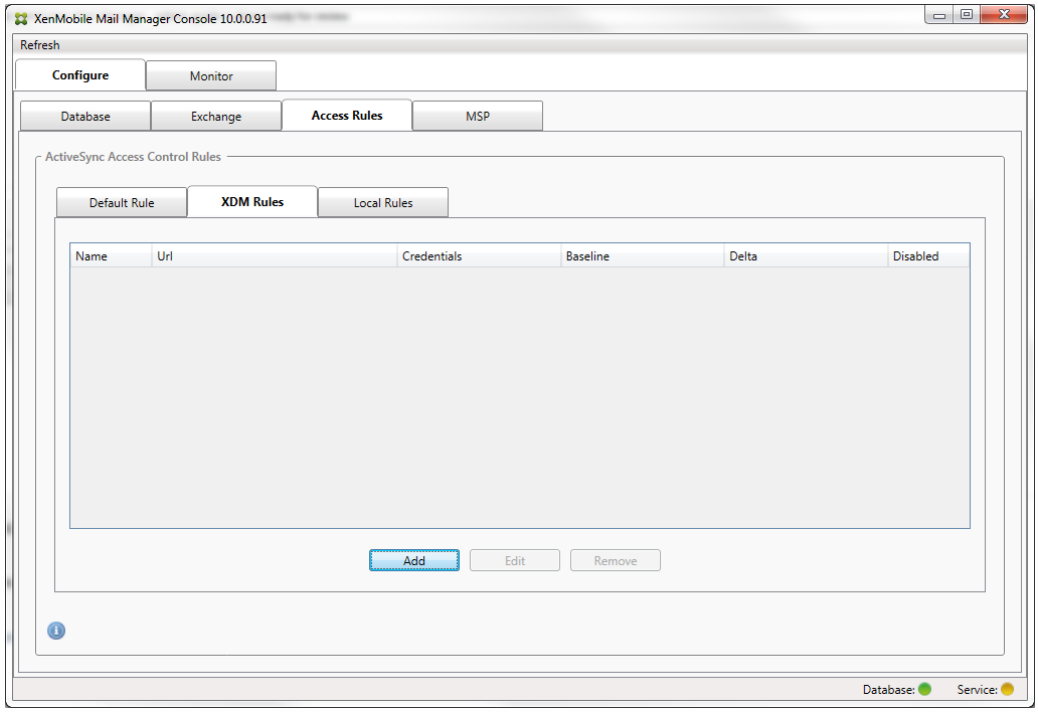
ナップショット（XenMobileで、非管理対象デバイスを照会できます）は、処理にかかる時間が著しく長くなることがあり、Mobile Service ProviderがActiveSyncに対して有効にされている場合にのみ必要です。

11. ［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。
12. 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。

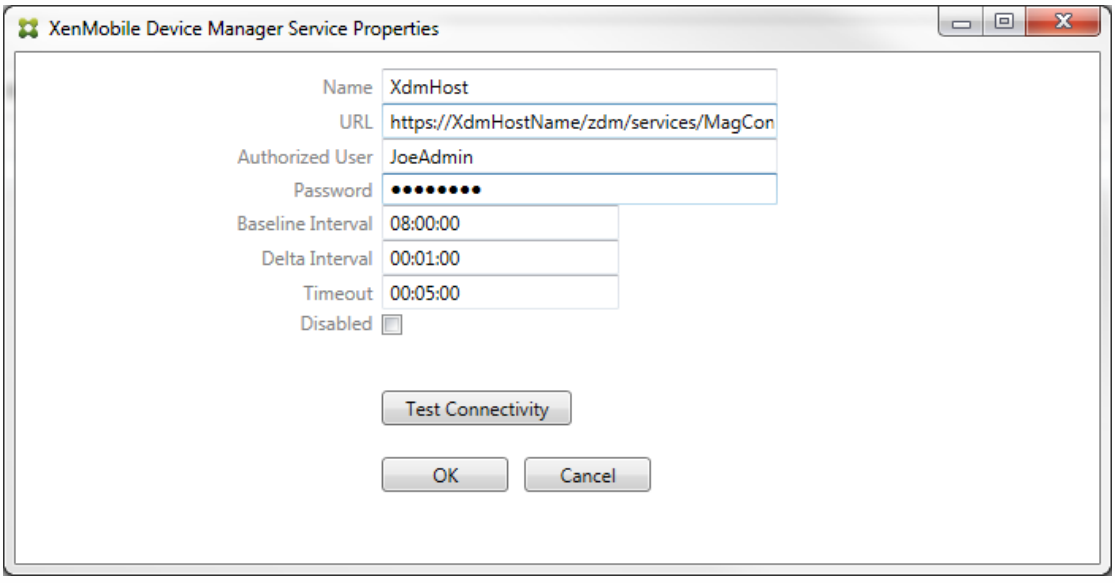
6. アクセス規則を構成します。
    1. ［Configure］の［Access Rules］タブをクリックします。



    2. ［Default Access］で、［Allow］、［Block］、または［Unchanged］を選択します。これにより、明示的なXenMobileまたはローカル規則で特定されたものを除くすべてのデバイスの処理方法が制御されます。［Allow］を選択した場合は該当するすべてのデバイスに対するActiveSyncアクセスが許可され、［Block］を選択した場合はアクセスが拒否され、［Unchanged］を選択した場合は変更されません。
    3. ［ActiveSync Command Mode］で、［PowerShell］または［Simulation］を選択します。
        - ［PowerShell］モードでは、XenMobile Mail ManagerはPowerShellコマンドを発行し、目的のアクセス制御を有効にします。
        - ［Simulation］モードでは、XenMobile Mail ManagerはPowerShellコマンドを発行しませんが、想定しているコマンドと結果をデータベースに記録します。［Simulation］モードでは、PowerShellモードを有効にした場合の結果を［Monitor］タブを使って確認できます。
    4. ［Save］をクリックします。
7. ［XDM Rules］タブをクリックします。



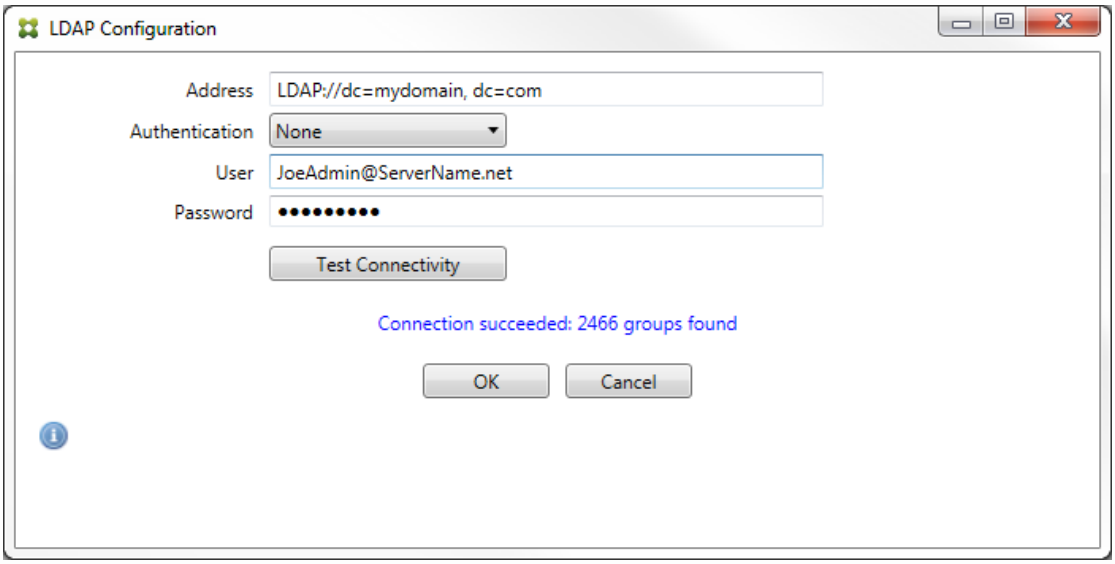
1. ［Add］をクリックします。
2. XDM規則の名前（XdmHostなど）を入力します。



3. 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。
4. サーバーで認証されているユーザーを入力します。
5. そのユーザーのパスワードを入力します。
6. ［Baseline Interval］、［Delta Interval］、および［Timeout］はデフォルト値のままにします。
7. ［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。
8. ［OK］をクリックします。

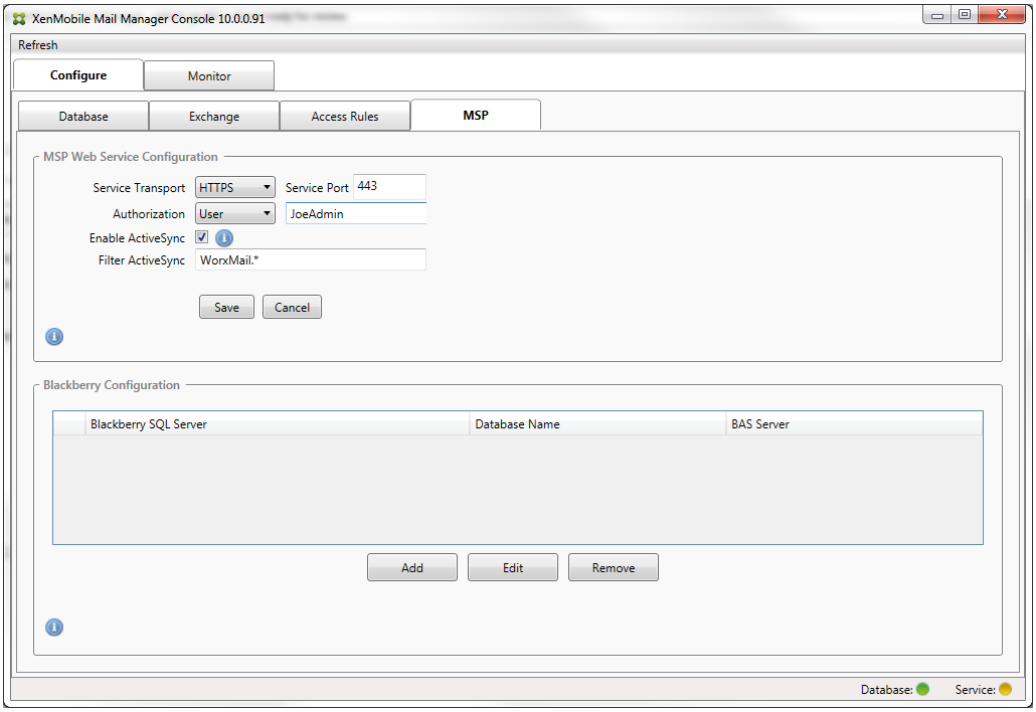
8. ［Local Rules］タブをクリックします。

1. Active Directoryのグループに対して使用するローカル規則を作成する場合は、［Configure LDAP］をクリックし、LDAP接続プロパティを構成します。



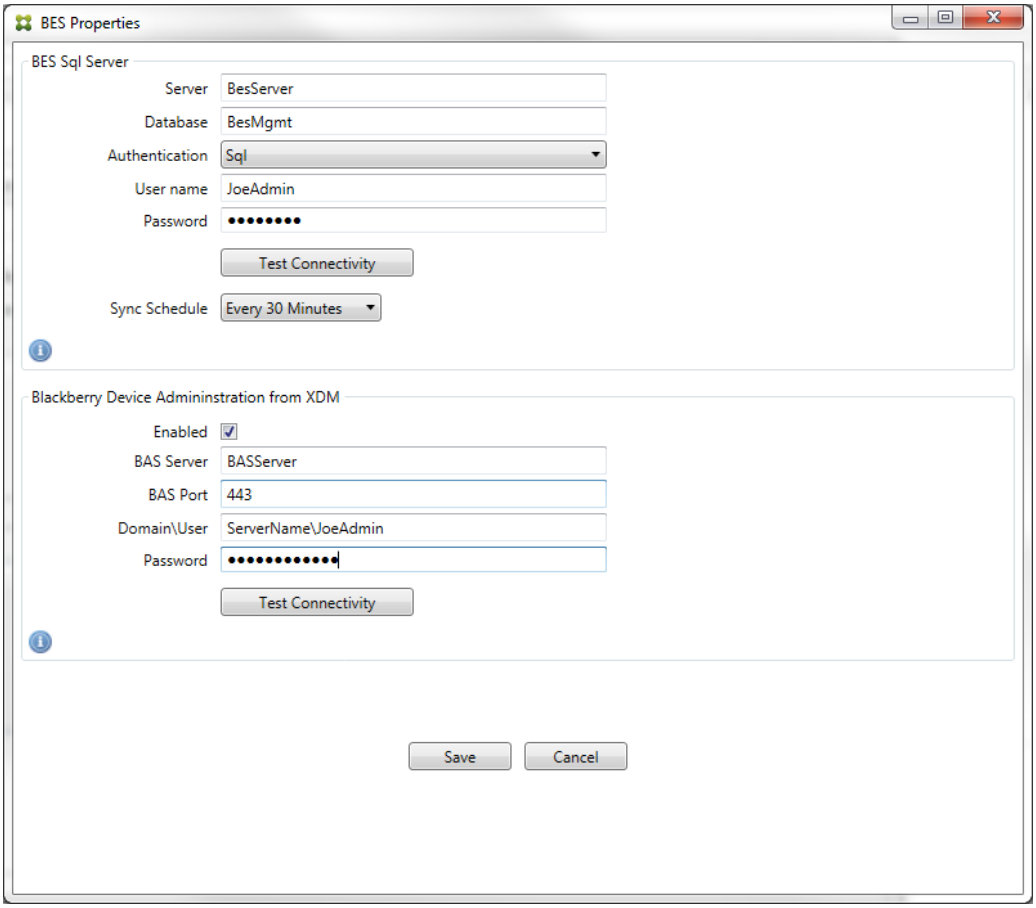
2. ［ActiveSync Device ID］、［Device Type］、［AD Group］、［User］、またはデバイスの［UserAgent］に基づいてローカル規則を追加できます。 一覧で、適切な種類を選択します。 詳しくは「XenMobile Mail Managerのアクセス制御規則」を参照してください。
3. テキストボックスにテキストまたはテキストフラグメントを入力します。 必要に応じて、クエリボタンをクリックしてフラグメントに一致するエンティティを表示します。
   注：グループ以外のすべての種類の場合、システムはスナップショットで見つかったデバイスに依存しています。したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。
4. テキスト値を選択し、［Allow］または［Deny］をクリックして右側の［Rule List］ペインに追加します。 ［Rule List］ペインの右側にあるボタンを使用して、規則の順序を変更したり、規則を削除したりすることができます。指定したユーザーおよびデバイスに対して、規則は表示順に評価され、上位の規則（より上部に近い規則）に一致すると以降の規則が無効になるので、順序は重要です。たとえば、すべてのiPadデバイスを許可する規則とユーザー「Matt」をブロックする下位の規則がある場合、MattのiPadは許可されます。この理由は、「iPad」規則の効果の優先度が「Matt」規則よりも高いからです。
5. 規則一覧内の規則の分析を実行して、上書き、競合、または補足構造の可能性を検出する場合は、［Analyze］をクリックします。
6. ［Save］をクリックします。

9. 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］の［MSP］タブをクリックします。



2. Mobile Service Providerサービスのサービストランスポートの種類（［HTTP］または［HTTPS］）を設定します。
3. Mobile Service Providerサービスのサービスポート（通常、80または443）を設定します。
   注：ポート443を使用する場合は、IISのこのポートにバインドされたSSL証明書が必要です。
4. 承認グループまたはユーザーを設定します。 これにより、XenMobileからMobile Service Providerサービスに接続できるユーザーまたは一連のユーザーが設定されます。
5. ActiveSyncクエリを有効または無効に設定します。
   注：XenMobileサーバーでActiveSyncクエリが有効の場合は、Exchange Server（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WorxMail.*に一致するActiveSyncデバイスは、XenMobileに送信されません。 必要に応じてこの動作を変更するには、［Filter ActiveSync］フィールドを変更します。
   注：空白は、すべてのデバイスがXenMobileに転送されることを意味します。
7. ［Save］をクリックします。

10. 任意で、1つまたは複数のBlackBerry Enterprise Server（BES）を構成します。
    1. ［Add］をクリックします。
    2. BES SQL Serverのサーバー名を入力します。



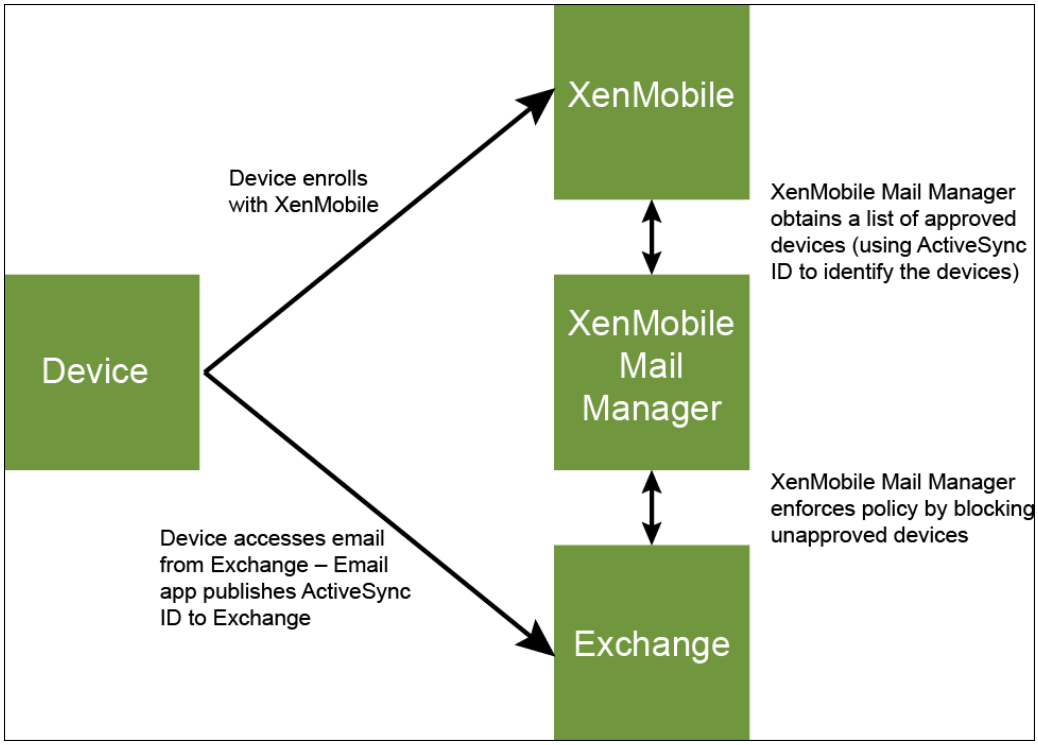
3. BES管理データベースのデータベース名を入力します。
4. 認証モードを選択します。 ［Windows Integrated authentication］を選択する場合、XenMobile Mail Managerサービスのユーザーアカウントが、BES SQL Serverへの接続に使用するアカウントになります。
   注：XenMobile Mail Managerデータベース接続に対しても［Windows Integrated］を選択している場合は、ここで指定したWindowsアカウントにXenMobile Mail Managerデータベースへのアクセスも付与する必要があります。
5. ［SQL authentication］を選択する場合は、ユーザー名とパスワードを入力します。
6. ［Sync Schedule］を設定します。 これは、BES SQL Serverへの接続とデバイス更新のチェックに使用するスケジュールです。
7. ［Test Connectivity］をクリックして、SQL Serverへの接続をテストします。
   注：［Windows Integrated］を選択している場合、このテストでは、XenMobile Mail Managerサービスのユーザーではなく、現在ログオンしているユーザーが使用されるため、SQL認証が正確にテストされません。
8. XenMobileからのBlackBerryデバイスのリモートでのワイプやResetPasswordをサポートする場合は、［Enabled］チェックボックスをオンにします。
   1. BESの完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を入力します。
   2. 管理者Webサービスで使用するBESポートを入力します。
   3. BESサービスに必要な完全修飾ユーザー名とパスワードを入力します。
   4. ［Test Connectivity］をクリックして、BESへの接続をテストします。
   5. ［Save］をクリックします。

ActiveSync IDによるメールポリシーの適用

May 10, 2016

企業のメールポリシーによっては、特定のデバイスで企業メールを使用することが認められない場合があります。このポリシーに従うには、そのようなデバイスから従業員が企業メールにアクセスできないようにする必要があります。XenMobile Mail ManagerおよびXenMobileを連携させ、そのようなメールポリシーを適用することができます。XenMobileで企業メールアクセスのポリシーを設定し、未承認のデバイスがXenMobileに登録されたときにXenMobile Mail Managerでポリシーを適用します。

デバイス上のメールクライアントはデバイスIDを使用してExchange Server（またはOffice 365）にクライアントの存在を通知します。このIDはActiveSync IDとしても知られており、デバイスを一意に識別するために使用されます。Worx Homeでは同様の識別子を取得し、デバイスが登録されるとXenMobileにこの識別子を送信します。XenMobile Mail Managerで2つのデバイスIDを比較することによって、特定のデバイスに企業メールへのアクセスを許可するかどうかが判定されます。次の図は、この概念を示しています。



デバイスがExchangeに公開したIDと異なるActiveSync IDがXenMobileからXenMobile Mail Managerに送信されると、XenMobile Mail ManagerからExchangeに対してそのデバイスに対する処理を指示できません。

ほとんどのプラットフォームでActiveSync IDのマッチングは確実に動作しますが、一部のAndroidの実装で、デバイスが送信するActiveSync IDとメールクライアントがExchangeに通知するIDが異なることが判明しています。この問題を緩和するため、次のことを実行できます。

- Samsung SAFEプラットフォームでは、デバイスのActiveSync構成をXenMobileからプッシュします。
- ほかのすべてのAndroidプラットフォームでは、XenMobileからTouchdownアプリとTouchdown ActiveSync構成の両方をXenMobileからプッシュします。

ただし、これにより従業員がAndroidデバイスにTouchdown以外のメールクライアントをインストールすることを防げるわけではありません。企業メールアクセスポリシーの適切な適用を保証するために、セキュリティについて防御的なスタンスをとり、静的なポリシーを［Deny by default］に設定することでXenMobile Mail Managerでメールを禁止するように構成することができます。これは、従業員がAndroidデバイスにTouchdown以外のメールクライアントを構成し、ActiveSync IDの検出が適切に動作しない場合は、従業員は企業メールへのアクセスを拒否されるということを意味します。

アクセス制御規則

May 10, 2016

XenMobile Mail Managerでは、Exchange ActiveSyncデバイスのアクセス制御を動的に構成するための、規則に基づく手法が提供されます。XenMobile Mail Managerのアクセス制御規則は、一致式と目的のアクセス状態（許可またはブロック）の2つで構成されます。特定のExchange ActiveSyncデバイスに対して規則を評価して、その規則がデバイスに適用されるかどうか、またはデバイスと一致するかどうかを判別できます。一致式にはいくつかの種類があります。たとえば、規則は、特定のデバイスの種類のすべてのデバイス、特定のExchange ActiveSyncデバイスID、特定のユーザーのすべてのデバイスと一致するなどの条件を指定できます。
規則一覧の規則を追加、削除、および並べ替えているときに［Cancel］をクリックすると、規則一覧が最初に開いたときの状態に戻ります。［Save］をクリックしない限り、構成ツールを閉じるとこのウィンドウに対して加えた変更が失われます。

XenMobile Mail Managerには、ローカル規則、XDM規則、およびデフォルトのアクセス規則の3種類の規則があります。

ローカル規則：ローカル規則が最も優先されます。デバイスがローカル規則と一致すると、規則の評価は停止します。XDM規則とデフォルトのアクセス規則は参照されません。ローカル規則は、［Configure］、［Access Rules］の順にクリックし、［Local Rules］タブから、XenMobile Mail Managerに対してローカルに構成されます。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。

XDM規則：XDM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XDM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XDM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XDM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XDM規則のいずれにも一致しないすべてのデバイスのアクセス状態は、XenMobile Mail Managerによって変更されません。ExchangeによってデバイスがQuarantineモードになっている場合、アクションは実行されません。たとえば、Quarantineモードからデバイスを削除する方法は、ローカル規則またはXDM規則で隔離を明示的に上書きすることのみです。

規則の評価について

ExchangeからXenMobile Mail Managerに報告されるデバイスごとに、次のように優先度の高い順に規則が評価されます。

- ローカル規則

- デフォルトのアクセス規則
- XDM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XDM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。

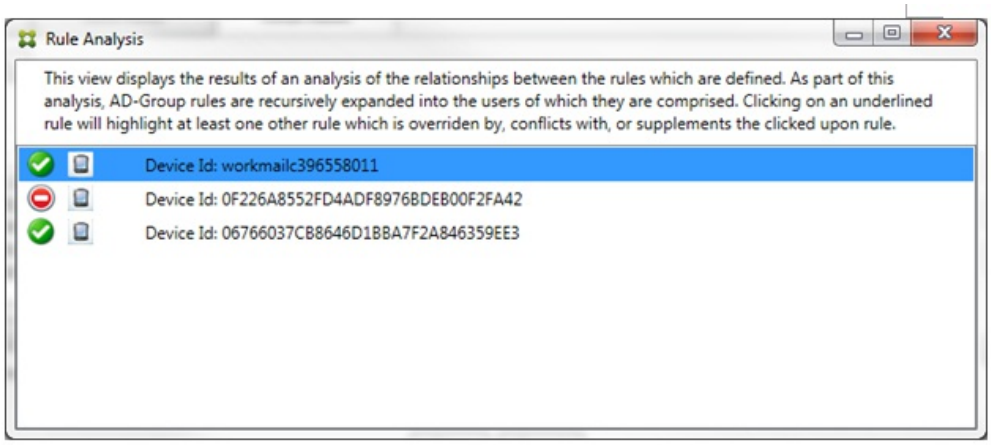
分析は、同じフィールドに対して複数の規則が定義されている場合に特に便利です。規則間の関係をトラブルシューティングできます。規則フィールドの観点から分析を実行します。たとえば、ActiveSyncデバイスID、ActiveSyncデバイスの種類、ユーザー、ユーザーエージェントなどの照合されるフィールドに基づくグループで規則が分析されます。

規則の用語：

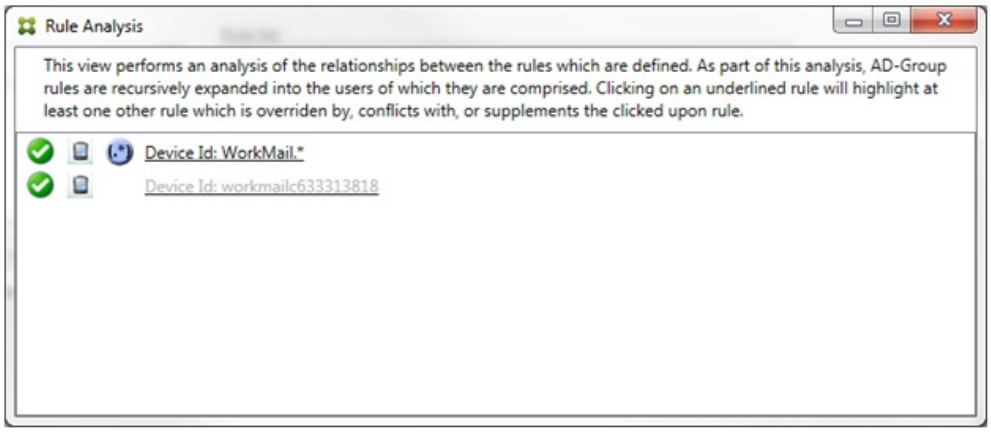
- **上書き規則**。同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- **競合規則**。同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- **補足規則**。正規表現の規則が複数あるので、2つ（またはそれ以上）の正規表現を1つの正規表現の規則に結合できるか、またはそれらの機能が重複していない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

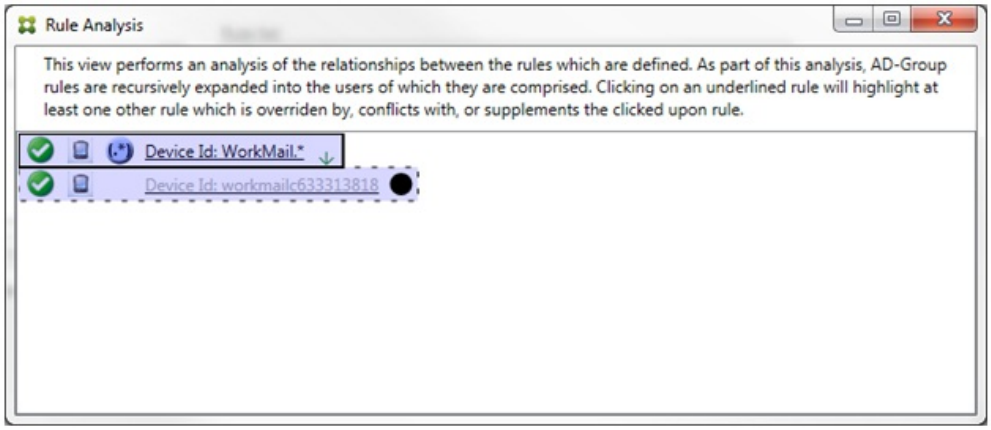
競合、上書き、または補足がない場合、［Rule Analysis］ダイアログボックスに下線付きのエントリは表示されません。どのアイテムをクリックしても影響はありません。通常の選択済みアイテムの表示になります。



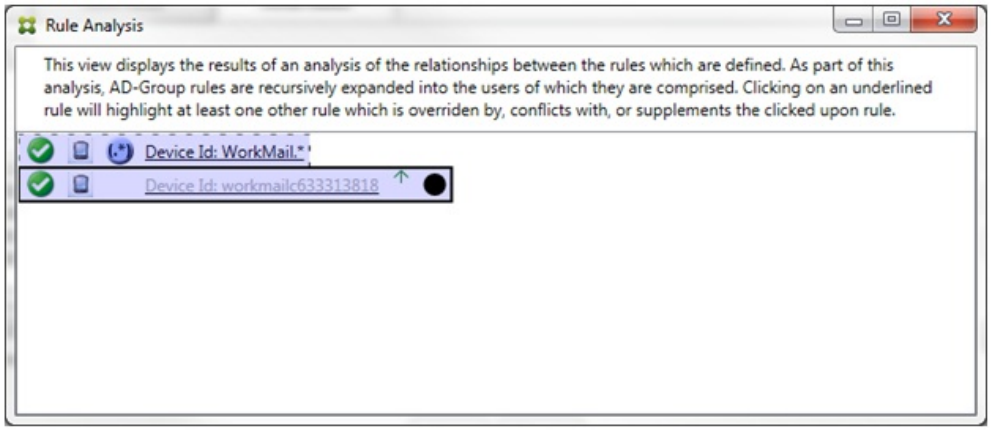
上書きが発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。1つまたは複数の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。上書きされた規則をクリックして、その規則を上書きした規則を確認できます。規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます。



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。

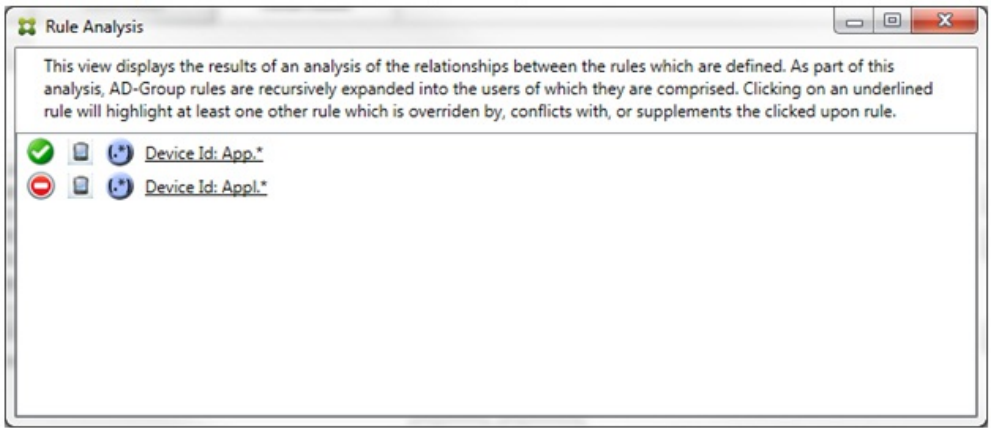


この例では、正規表現の規則WorkMail.*がプライマリ規則（実線の罫線で表示）で、通常の規則workmailc633313818が補助規則（破線の罫線で表示）です。補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります。

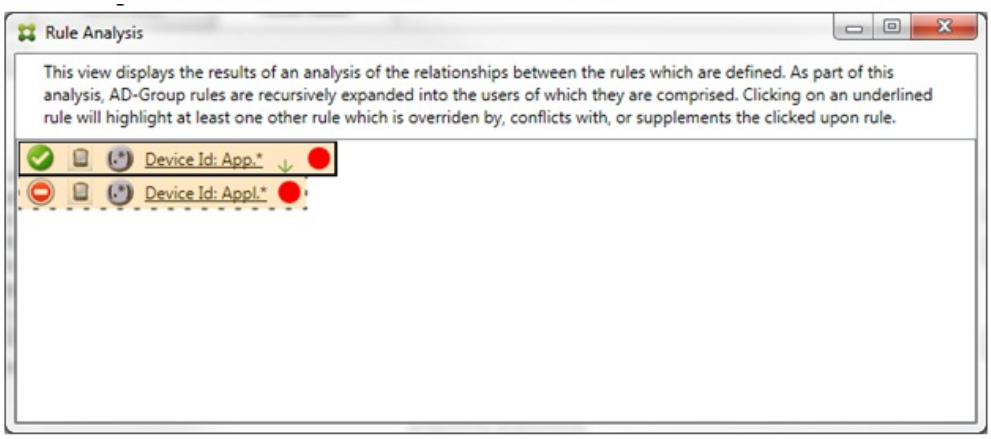


上記の例では、正規表現の規則WorkMail.*が補助規則（破線の罫線で表示）で、通常の規則workmailc633313818がプライマリ規則（実線の罫線で表示）です。このシンプルな例では、大きな違いはありません。より複雑な例については、このトピックで後述する複雑な式の例を参照してください。多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

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。

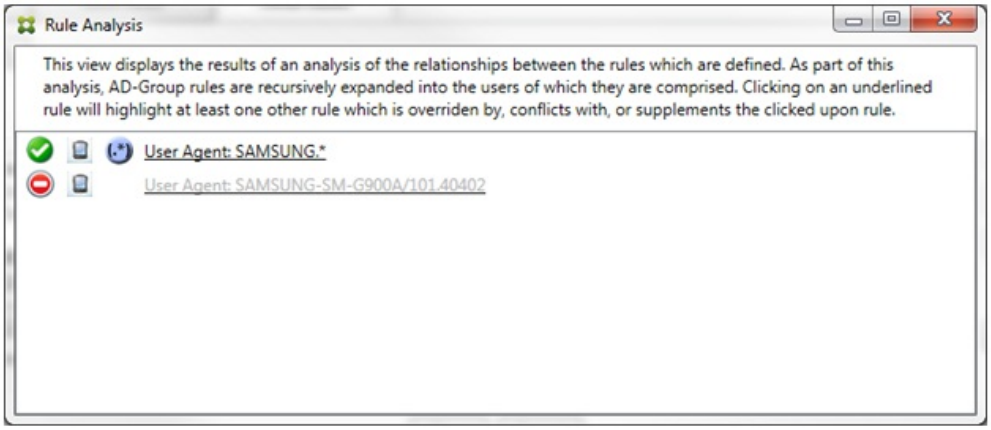


2つの正規表現の規則を確認すると、最初の規則で「App」がデバイスIDに含まれるすべてのデバイスを許可し、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスを拒否することがわかります。さらに、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは決して拒否されません。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



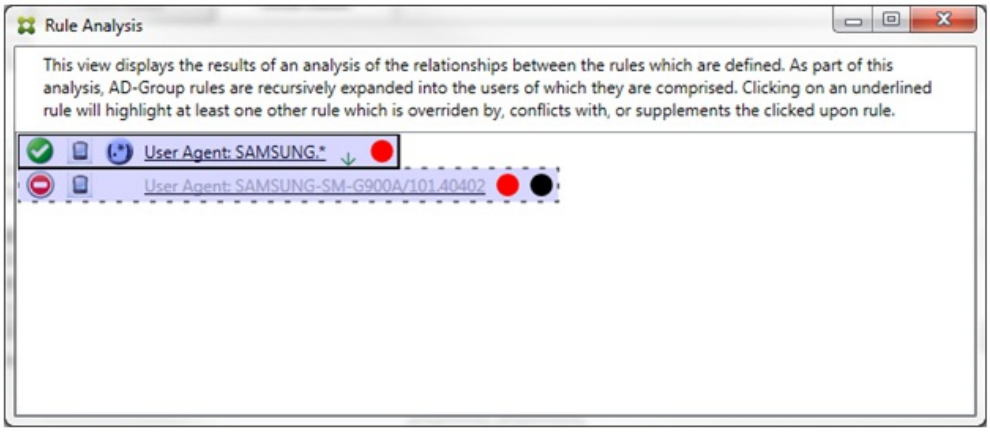
前述のシナリオでは、プライマリ規則（正規表現の規則App.*）と補助規則（正規表現の規則Appl.*）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

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。



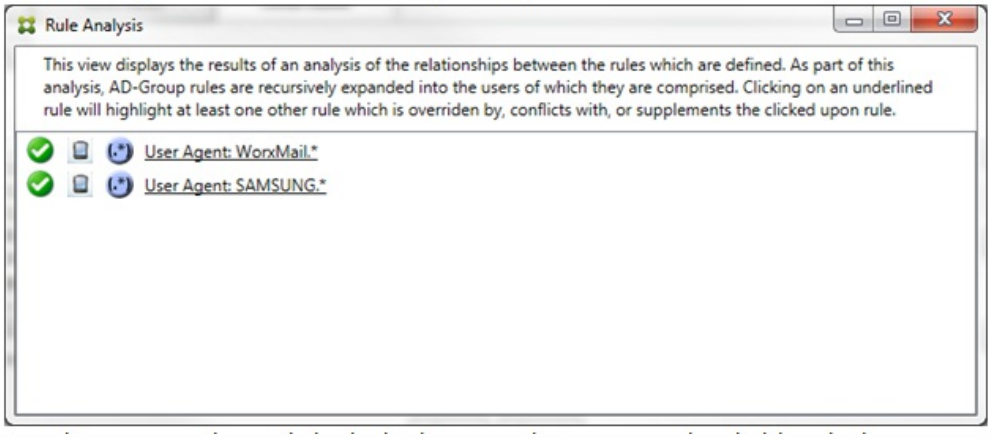
上記の例では、最初の規則（正規表現の規則SAMSUNG.*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。2つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

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。

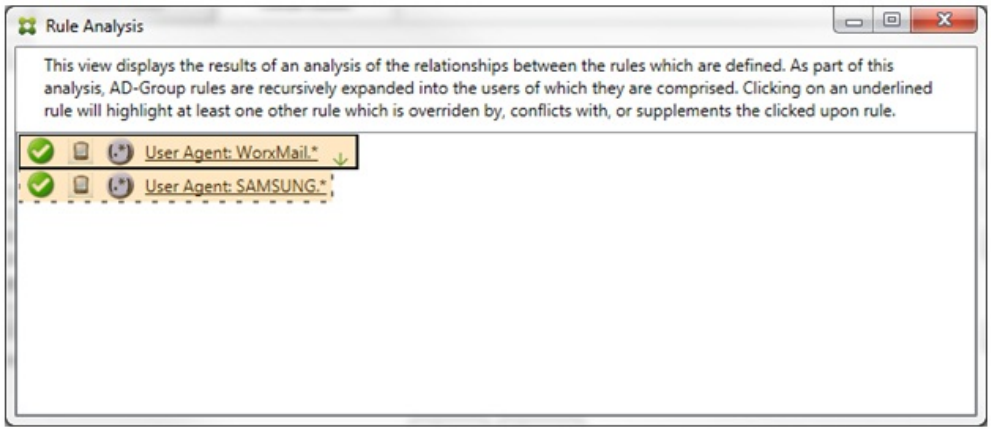


プライマリ規則（正規表現の規則SAMSUNG.*）の末尾には赤色の点が付けられて、アクセス状態が1つまたは複数の補助規則と競合していることが示されます。補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には、アクセス状態がプライマリ規則と競合していることを示す赤色の点に加えて、その規則が上書きされて非アクティブであることを示す黒点が付けられます。

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。



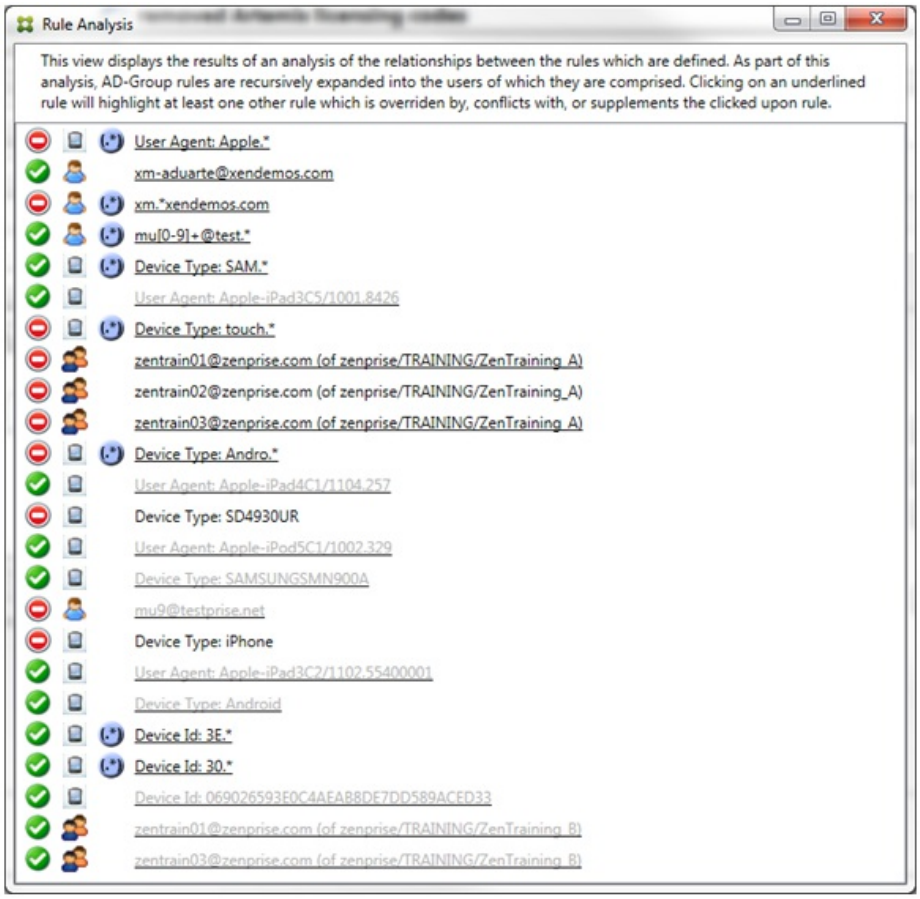
目視で確認すると、両方の規則が正規表現の規則で、両方ともXenMobile Mail Managerの［ActiveSync device ID］フィールドに適用されていることが容易にわかります。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



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

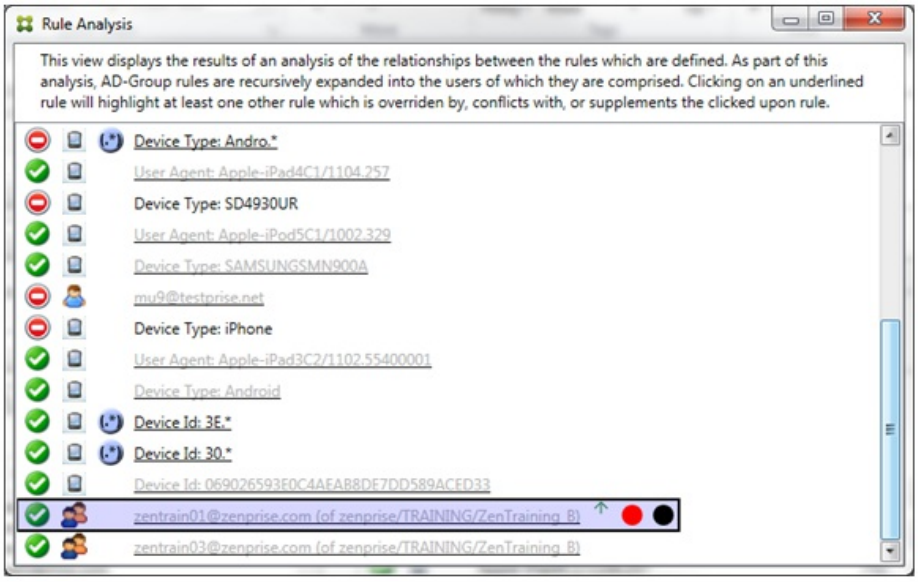
発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。次の図では、ほとんどのアイテムに下線が付けられています。多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。同様に、(.*)アイコンで示される多数の正規表現の規則も一覧に含まれています。



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。

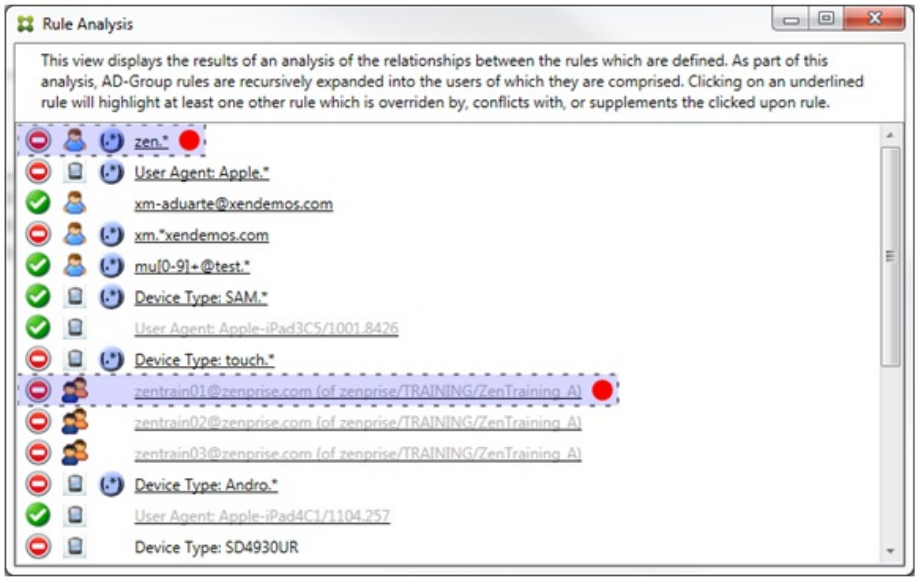
例1：この例では、zentrain01@zenprise.comが上書きされた理由を調べます。



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。

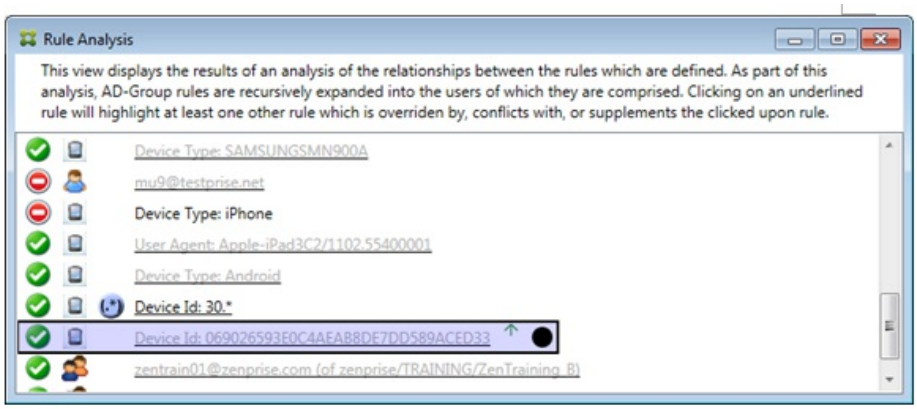
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている（すべての補助規則がこの規則より上に表示されていることを示します）。
- 末尾に、1つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます。



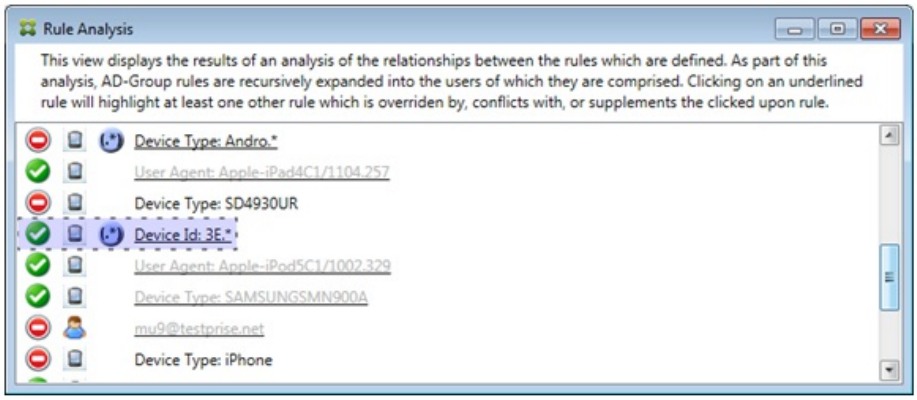
この場合、プライマリ規則を上書きする2つの補助規則（正規表現の規則zen.*と通常の規則zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)）があります。後者の補助規則の場合、Active Directoryグループ規則ZenTraining Aにユーザーzentrain01@zenprise.comが含まれる一方で、Active Directoryグループ規則ZenTraining Bにもユーザーzentrain01@zenprise.comが含まれることになります。ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、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。



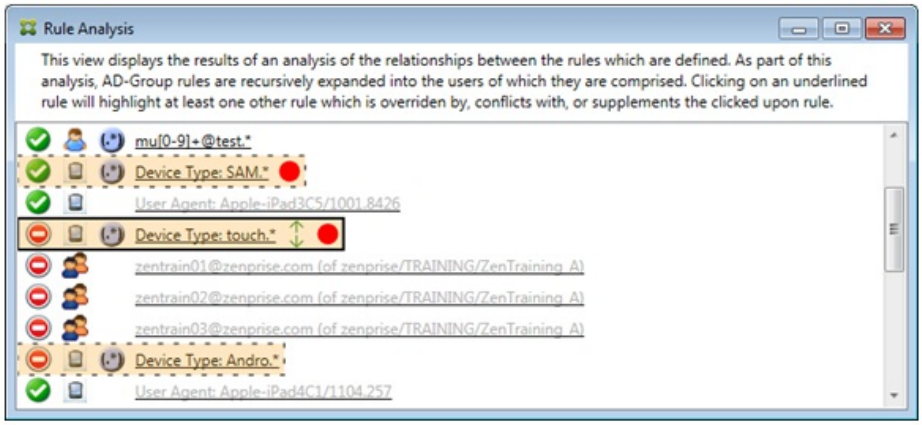
この場合、単一の補助規則（正規表現のActiveSyncデバイスIDの規則3E.*）がプライマリ規則を上書きします。正規表現3E.*が069026593E0C4AEAB8DE7DD589ACED33に一致するので、プライマリ規則は評価されません。

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。



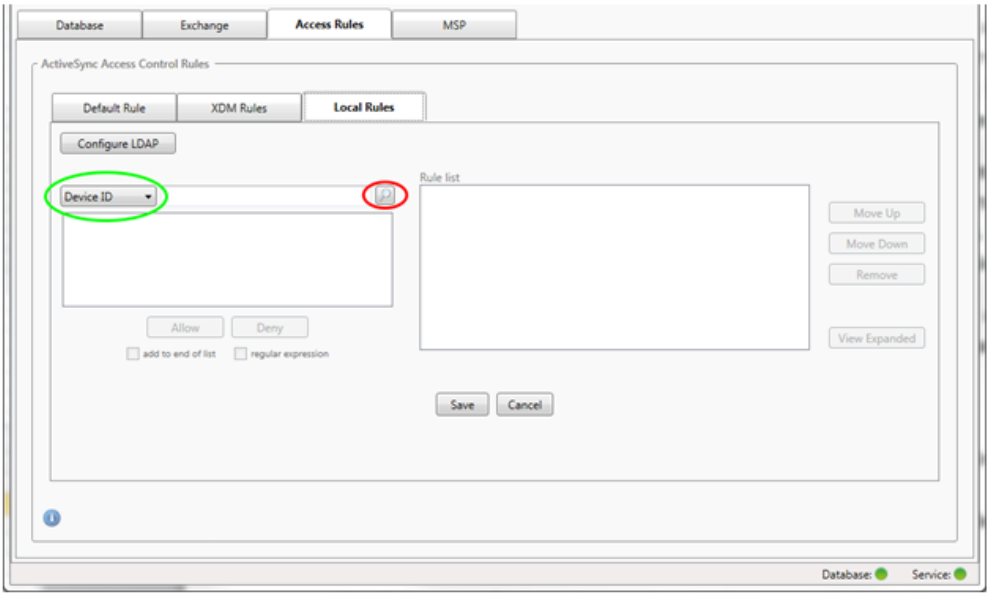
規則の高度な分析方法

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。

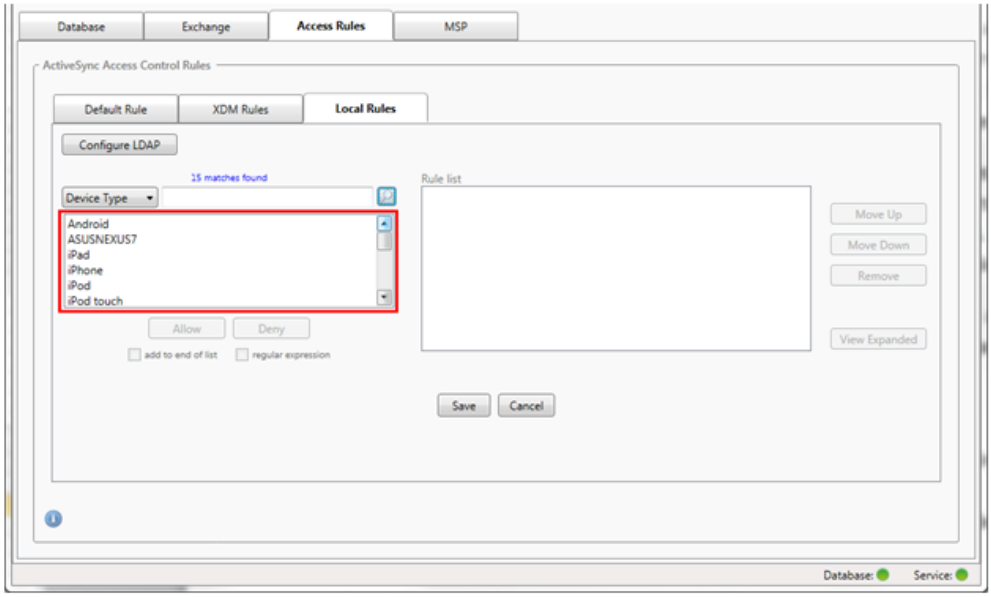
この例では、規則の関係に含まれる上書きされた規則が示されています。この規則は、通常のActiveSyncデバイスの種類の規則Androidです。この規則は上書きされ（淡色のフォントで示され、横に黒点が付けられています）、プライマリ規則（正規表現のActiveSyncデバイスの種類の規則Andro.*。この規則は、クリック前は補助規則でした）のアクセスと競合しています。前述の例では、その時点でのプライマリ規則（正規表現のActiveSyncデバイスの種類の規則touch.*）の観点からは関係しなかったので、通常のActiveSyncデバイスの種類の規則Androidは補助規則として表示されていませんでした。

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。

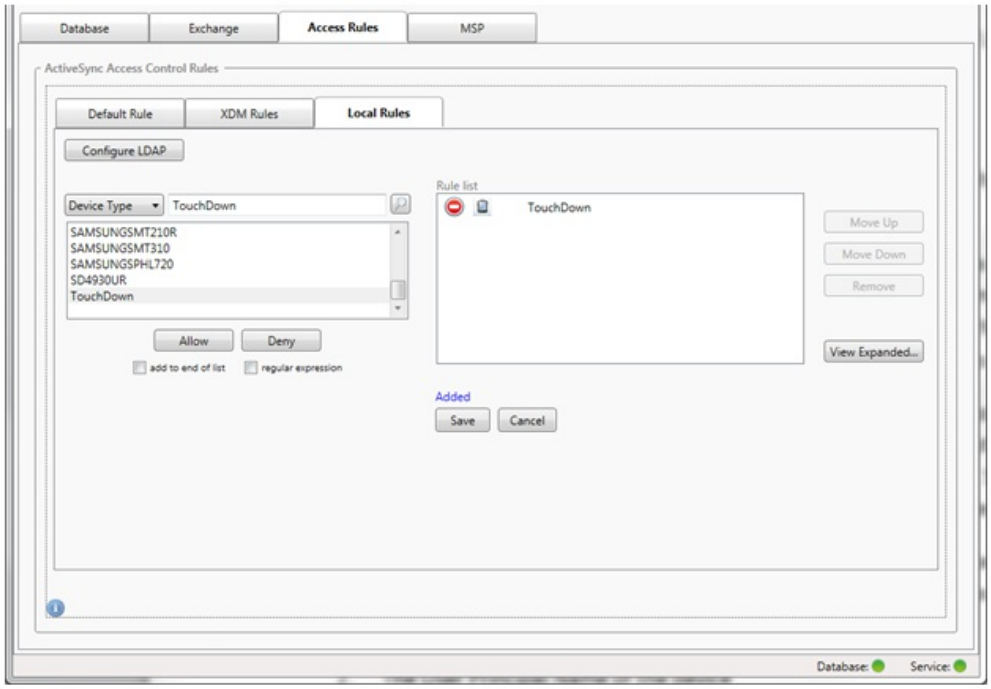


2. ［Device ID］一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。 この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



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。
   - Allow：すべての一致するデバイスに対して、ActiveSyncトラフィックを許可するようにExchangeが構成されます。
   - Deny：すべての一致するデバイスに対して、ActiveSyncトラフィックを拒否するようにExchangeが構成されます。

   この例では、デバイスの種類がTouchDownであるすべてのデバイスのアクセスが拒否されます。

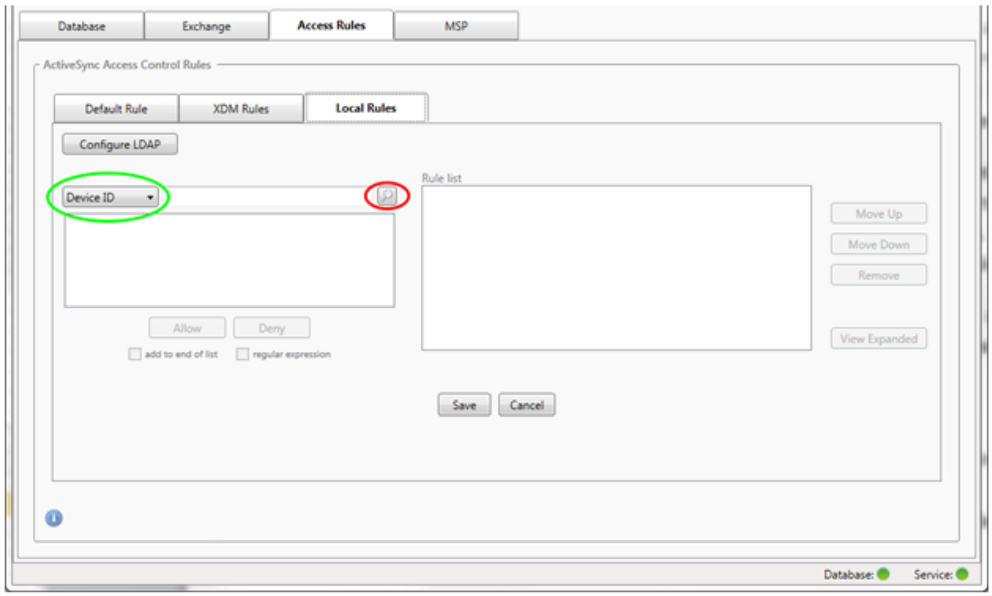


正規表現を追加するには

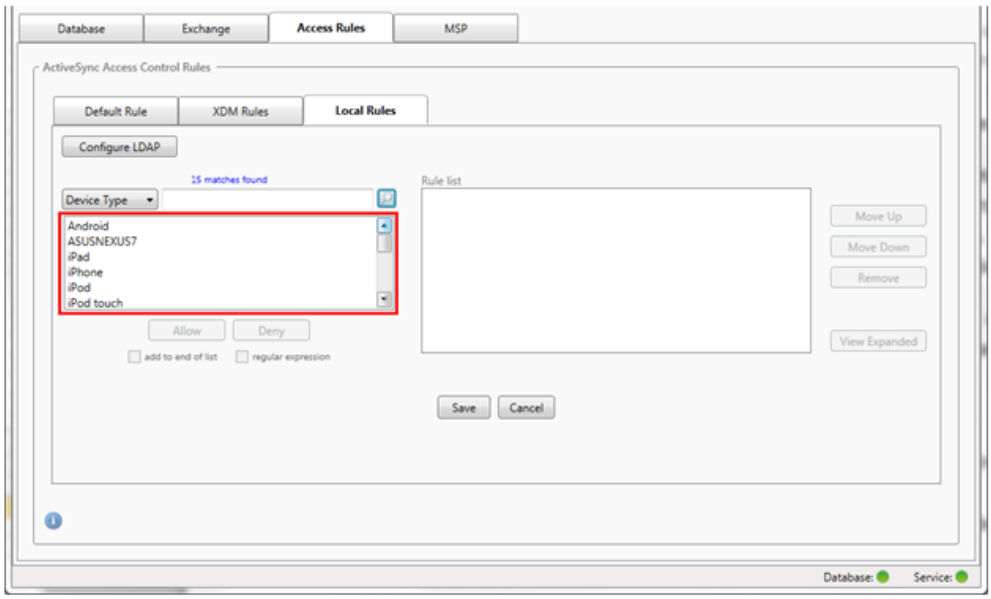
正規表現のローカル規則は、横に表示されるアイコン（(.*)）で識別できます。正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

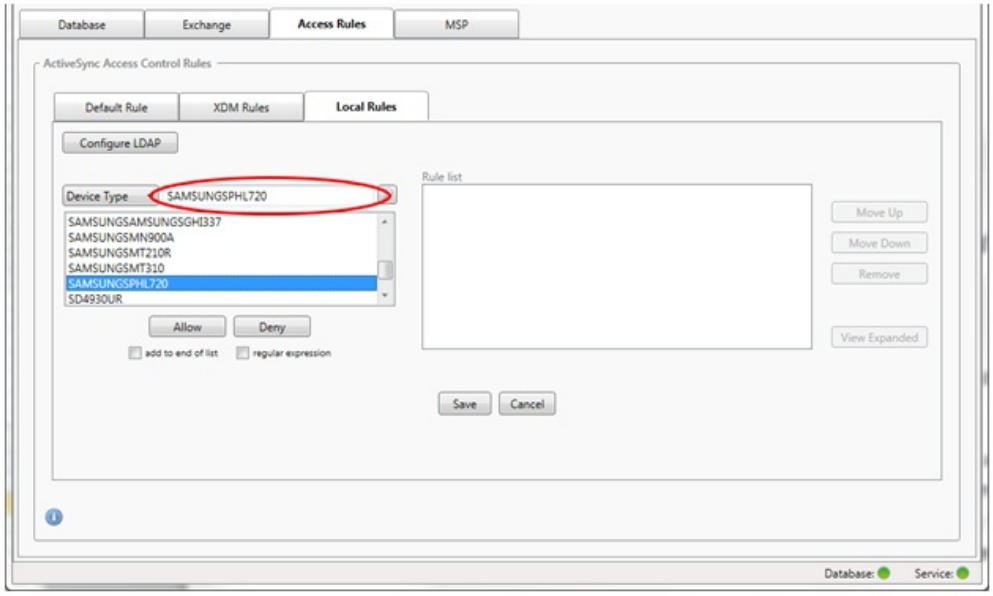
1. ［Access Rules］タブをクリックします。



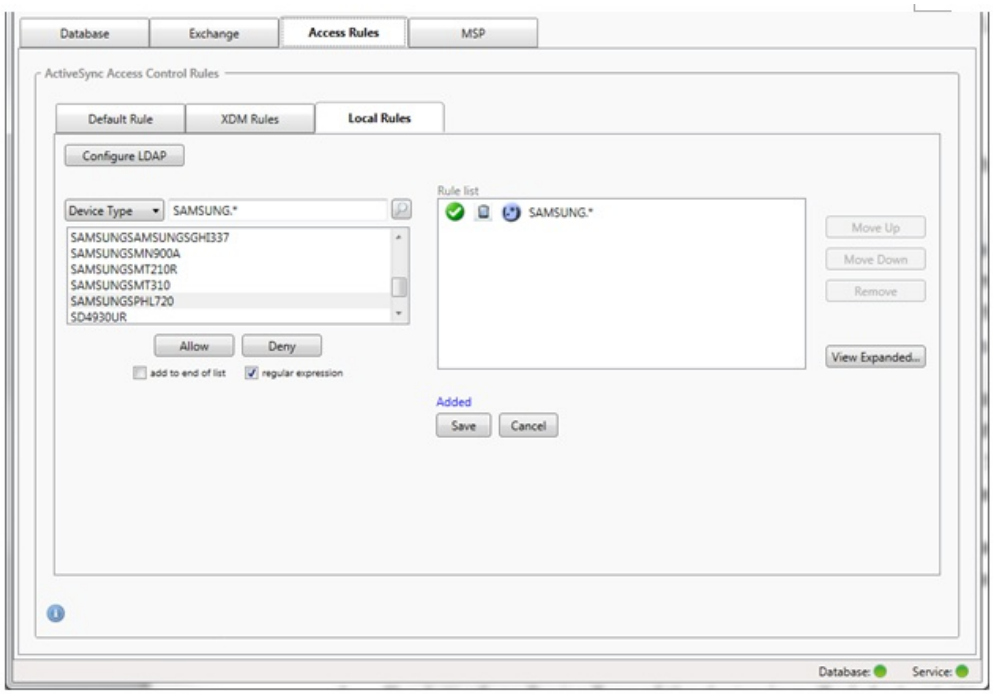
2. ［Device ID］一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。 この例では、［Device Type］フィールドが選択され、下のリストボックスに選択肢が表示されています。



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。

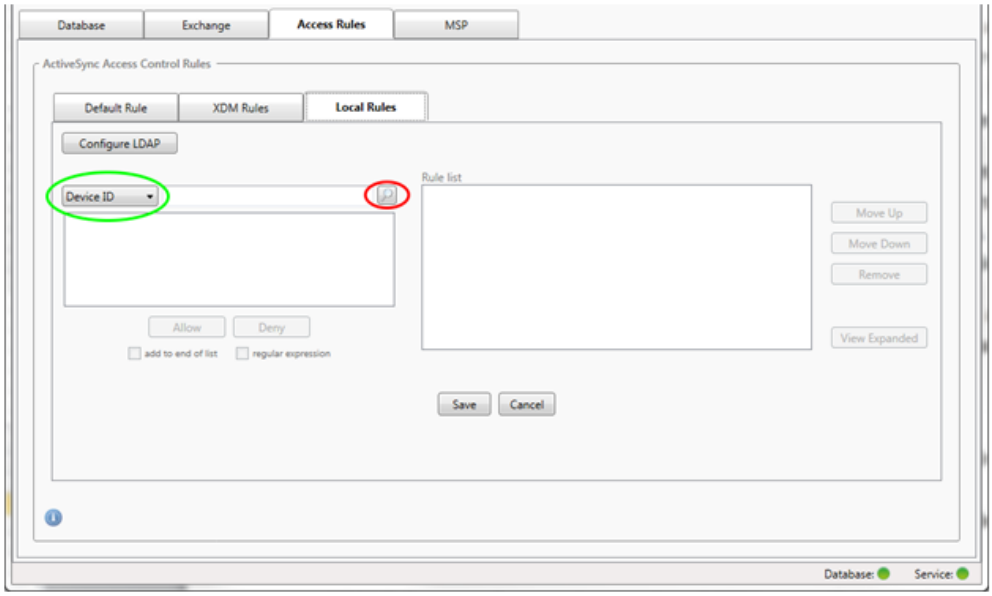


5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。
   1. 選択済みアイテムのテキストボックス内をクリックします。
   2. SAMSUNGSPHL720からSAMSUNG.*にテキストを変更します。
   3. [regular expression]チェックボックスをオンにします。
   4. [Allow]をクリックします。

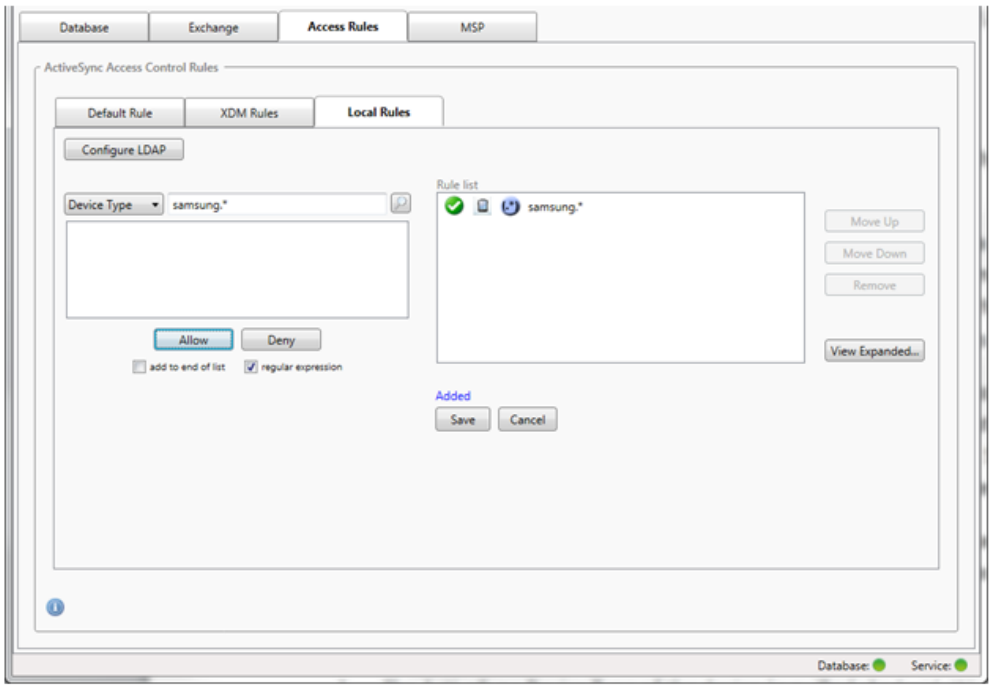


アクセス規則を作成するには

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。



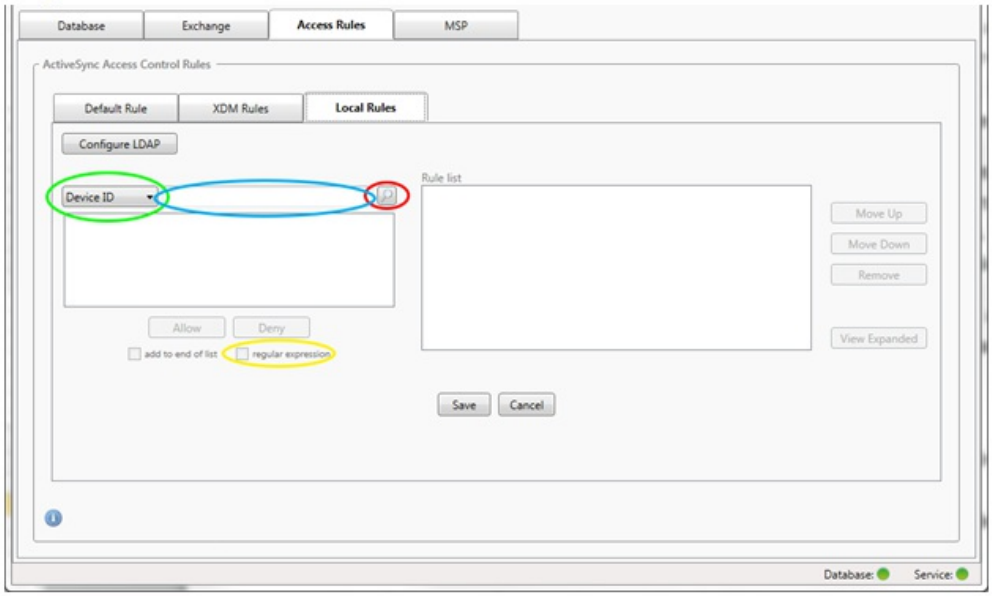
3. 照合するフィールドを選択します。 この例では［Device Type］を使用します。
4. 正規表現を入力します。 この例では次の文字列を使用します：samsung.*
5. ［regular expression］チェックボックスをオンにして、［Allow］または［Deny］をクリックします。 この例では、［Allow］を選択し、最終結果は次のようになります



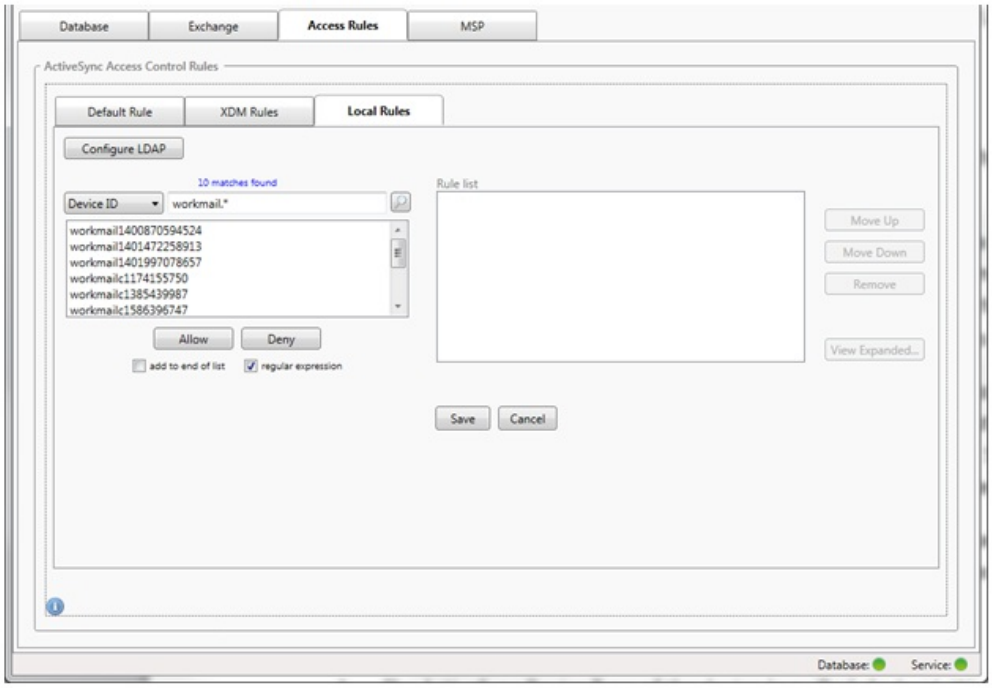
デバイスを検出するには

［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。



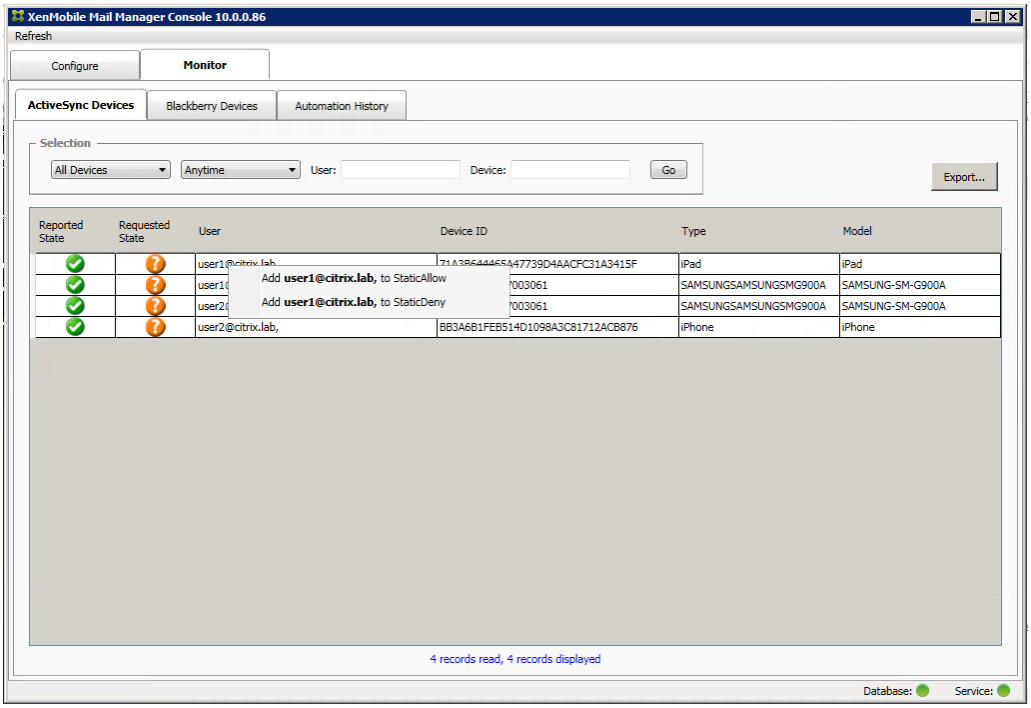
3. 選択済みアイテムのテキストボックス内（上記の図に青色で示されています）をクリックし、workmail.*と入力します。
4. ［regular expression］チェックボックスをオンにして、虫眼鏡アイコンをクリックし、次の図に示すように一致を表示します。



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

May 10, 2016

XenMobile Mail Managerの［Monitor］タブでは、検出されたExchange ActiveSyncデバイスおよびBlackBerryデバイスと、これまで自動で発行されたPowerShellコマンドの履歴を参照できます。［Monitor］タブには、次の3つのタブがあります。

- ActiveSync Devices：
  - ［Export］をクリックして、表示されているActiveSyncデバイスパートナーシップをエクスポートできます。
  - ［User］、［Device ID］、または［Type］列を右クリックし、許可またはブロックから適切な規則の種類を選択して、ローカル（静的）規則を追加できます。
  - 展開した行を折りたたむには、Ctrlキーを押しながらその行をクリックします。
- Blackberry Devices
- Automation History

［Configure］タブにはすべてのスナップショットの履歴が表示されます。スナップショットの履歴には、スナップショットの作成時刻、作成にかかった時間、検出されたデバイス数、発生したすべてのエラーが表示されます。

- ［Exchange］タブで、目的のExchange Serverの情報アイコンをクリックします。
- ［MSP］タブで、目的のBlackBerry Serverの情報アイコンをクリックします。

トラブルシューティングおよび診断

May 10, 2016

XenMobile Mail Managerでは、エラーなどの動作情報がログファイル（\log\XmmWindowsService.log）に記録されます。また、Windowsイベントログに、重要なイベントが記録されます。

一般的なエラーを以下に示します。

XenMobile Mail Managerサービスが起動しない

ログファイルとWindowsイベントログでエラーを確認します。一般的な原因は次のとおりです。

- XenMobile Mail ManagerサービスがSQL Serverにアクセスできない。これは、次の問題が原因である可能性があります。
  - SQL Serverサービスが実行されていない。
  - 認証に失敗した。
    ［Windows Integrated authentication］が構成されている場合、XenMobile Mail Managerサービスのユーザーアカウントは、許可されたSQLログオンである必要があります。XenMobile Mail Managerサービスのアカウントは、デフォルトではローカルシステムですが、ローカルの管理者権限を持つ任意のアカウントに変更できます。［SQL authentication］が構成されている場合、SQLログオンがSQLで適切に構成されている必要があります。
- Mobile Service Provider（MSP）に対して構成されたポートが使用できない。システムのほかのプロセスで使用されていないリッスンポートを選択する必要があります。

XenMobileがMSPに接続できない

XenMobile Mail Managerコンソールの［Configure］の［MSP］タブで、MSPサービスポートとトランスポートが適切に構成されていることを確認します。承認グループまたはユーザーが適切に設定されていることを確認します。
HTTPSが構成されている場合は、有効なSSLサーバー証明書がインストールされている必要があります。IISがインストールされている場合は、証明書のインストールにIISマネージャーを使用できます。IISがインストールされていない場合、証明書のインストールについて詳しくは、https://msdn.microsoft.com/ja-jp/library/ms733791.aspxを参照してください。

XenMobile Mail Managerには、MSPサービスへの接続をテストするためのユーティリティプログラムが含まれています。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。

XenMobile NetScaler Connector

Oct 24, 2016

XenMobile NetScaler Connectorは、モバイルデバイスからの社内メール、カレンダー、および連絡先へのアクセスを制御するソリューションです。 XenMobile NetScaler Connectorを使うと、顧客はXenMobileからNetScalerに準拠デバイスの一覧を送信することにより、どのモバイルデバイスが企業のExchange Serverとの同期を許可されているのかを制御できます。

XenMobileを使用すると、モバイルアプリケーション、ネットワーク、およびデータを完全に保護して、エンドツーエンドのセキュリティおよびコンプライアンスを確保できます。 NetScalerを使用すると、エンタープライズおよびクラウドサービスの配信を最適化、保護、および制御できます。 これら2つのCitrix製品はスケール機能を提供し、アプリケーションに対する高可用性を確実にして、モビリティ展開および管理コストを削減すると同時にセキュリティを維持します。

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。

XenMobileでは、ジェイルブレイクされたデバイスを検出したり、特定のアプリケーションを検出したりする高レベルのポリシーがあるコンプライアンスに基づいて、デバイスのホワイトリスト（承認済み）およびブラックリスト（禁止）ポリシーを提供します。 XenMobile NetScaler Connectorのローカルルールは一般的に、特定のオーバーライドが必要とされる場合にXenMobileルールを増やすために使用されます。たとえば、特定のオペレーティングシステムのバージョンを使ってすべてのデバイスをブロックする場合などです。

XenMobile NetScaler Connectorの主な機能は次のとおりです。

- **HTTP ActiveSync要求のアクセス制御**。 XenMobile NetScaler Connectorでは、モバイルデバイスがExchange Serverに対して行うHTTP ActiveSync要求を制御できます。 XenMobile NetScaler Connectorでフィルターを作成し、指定した規則および条件に基づいて、ユーザーデバイスを許可またはブロックできます。 XenMobile NetScaler Connectorで規則を設定した場合、XenMobileでその規則を有効または無効にすることにより、デバイスが組織内のメールにアクセスする機能を管理できます。
- **リモート構成**。 XenMobileでは、XenMobile NetScaler Connectorで使用するベースライン間隔およびデルタ間隔を制御できます。
- **Logging**。 XenMobile NetScaler Connector構成ユーティリティの［**Log**］タブで、許可またはブロックされているデバイスに加えて、特定のユーザーデバイスの暗号化が要求レベルでいつ有効化されたかを確認できます。

XenMobile NetScaler Connectorにより、次の機能が提供されます。

- **アクセスを許可またはブロックするフィルターベースのルール**。 XenMobile NetScaler Connectorでは、組織のルールに対して、NetScalerを介してルーティングされた特定のクライアント要求が評価されます。 評価の結果として、アクセスが*許可*または*ブロック*されます。許可の状態では、クライアントがMicrosoft Exchange 2010 クライアントアクセスサーバー（Client Access Server：CAS）に接続することが許可され、ブロックの状態では、クライアント要求が拒否され、Exchange CASへのアクセスが許可されません。 XenMobileコンソールの設定と組み合わせて、コンプライアンス条件（ブラックリストに登録されたアプリがデバイスにインストールされている場合、デバイスがジェイルブレイク済みかどうかなど）に基づいて、Exchange ActiveSyncメールからデバイスユーザーへのアクセスを防ぐことができます。
- **2階層のフィルターモデル**。 最初の階層では、着信したHTTP要求がパス固有の情報に基づいて解析されます。 2番目の階層では、ユーザーまたはデバイス固有の情報に基づいてフィルターします。 両方の階層を構成することができます。
- **構成ファイルに格納されたフィルター規則**。 組織内のユーザーアカウントおよびデバイスに関連する特定のフィルター規則は、ゲートウェイのXML構成ファイルに格納されます。

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。

XenMobile NetScaler Connectorの展開

May 10, 2016

XenMobile NetScaler Connectorでは、NetScalerを使用して、XenMobileによる管理対象デバイスとXenMobile間の通信をプロキシ接続したり、負荷分散したりできます。 XenMobile NetScaler ConnectorとXenMobile間の通信は定期的に行われ、ポリシーが同期されます。 XenMobile NetScaler ConnectorとXenMobileをまとめて、または別々にクラスター化したり、NetScalerによって負荷を分散したりできます。

XenMobile NetScaler Connectorのコンポーネント

XenMobile NetScaler Connectorは、以下の4つのコンポーネントで構成されます。

- XenMobile NetScaler Connectorサービス。 このサービスでは、NetScalerによって呼び出されるREST Webサービスのインターフェイスが提供され、デバイスからのActiveSync要求が承認されるかどうかが決定されます。
- XenMobile構成サービス。 このサービスでは、Device Managerとの通信が行われ、Device Managerポリシーの変更がXenMobile NetScaler Connectorと同期されます。
- XenMobile通知サービス。 このサービスによって、Device Managerへの承認されていないデバイスのアクセスが通知されるため、Device Managerでは、デバイスがブロックされた理由をユーザーに通知するなどの、適切な処置を施すことができます。
- XenMobile NetScaler構成ユーティリティ。 このアプリケーションを使用すると、管理者はXenMobile NetScaler Connectorを構成して監視することができます。

XenMobile NetScaler Connectorのリッスンアドレスをセットアップするには

XenMobile NetScaler ConnectorがNetScalerから要求を受信してActiveSyncトラフィックを承認できるようにするには、XenMobile NetScaler ConnectorがNetScaler Webサービス呼び出しをリッスンするポートを指定する必要があります。

1. ［Start］メニューの［XenMobile NetScaler configuration utility］を選択します。
2. ［Web Service］タブをクリックし、XenMobile NetScaler Connector Webサービスのリッスンアドレスを入力します。 HTTPとHTTPSの両方またはいずれかを選択できます。 XenMobile NetScaler ConnectorがXenMobileと共存している場合（同じサーバーにインストールされている場合）、XenMobileと競合しないポート値を選択します。
3. この値を構成した後、［Save］をクリックして、［Start Service］をクリックし、Webサービスを起動します。

XenMobile NetScaler Connectorでデバイスのアクセス制御ポリシーを構成するには

管理対象デバイスに適用するアクセス制御ポリシーを構成するには、次の操作を実行します。

1. XenMobile NetScaler構成ユーティリティで、［Path Filters］タブをクリックします。
2. 最初の行の［Microsoft-Server-ActiveSync is for ActiveSync］を選択し、［Edit］をクリックします。
3. ［Policy］の一覧から、目的のポリシーを選択します。 XenMobileポリシーが含まれるポリシーの場合、［Static + ZDM: Permit Mode］または［Static + ZDM: Block Mode］を選択します。 これらのポリシーでは、ローカル（または、静的）規則とXenMobileの規則が組み合わされます。 ［Permit Mode］では、規則によって明示的に特定されないすべてのデバイスがActiveSyncへのアクセスを許可されます。 ［Block Mode］では、そのようなデバイスがブロックされます。
4. ポリシーを設定したら、［Save］をクリックします。

XenMobileとの通信を構成するには

このタスクでは、XenMobile NetScaler ConnectorおよびNetScalerと共に使用する、XenMobileサーバー（構成プロバイダーともいいます）の名前およびプロパティを指定します。

注：このタスクでは、XenMobileサーバーがインストールされていて、構成済みであることを前提としています。

1. XenMobile NetScaler Connector構成ユーティリティで、［Config Providers］タブをクリックし、［Add］をクリックします。
2. この展開で使用するXenMobileサーバーの名前およびURLを入力します。 マルチテナント展開で複数のXenMobileサーバーがある場合は、この名前は各サーバーインスタンスで固有である必要があります。 たとえば、［Name］に「XMS、
3. ［Url］に、XenMobile GlobalConfig Provider（GCP）のWebアドレス（通常はhttps://DeviceManagerHost/zdm/services/MagConfigServiceという形式）を入力します。 MagConfigServiceの名前は大文字と小文字が区別されます。
4. ［Password］に、XenMobile WebサーバーでのHTTP基本認証に使用するパスワードを入力します。
5. ［Managing Host］に、XenMobile NetScaler Connectorをインストールしたサーバーの名前を入力します。
6. ［Baseline Interval］で、新しく更新された動的規則のセットがXenMobileから取得される期間を指定します。
7. ［Request Timeout］で、サーバー要求のタイムアウト間隔を指定します。
8. ［Config Provider］で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
9. ［Events Enabled］で、デバイスがブロックされたときにSecure Mobile GatewayからXenMobileに通知する場合はこのオプションを有効にします。 Device Managerの自動化された操作でSecure Mobile Gatewayの規則を使用する場合、このオプションが必要です。
10. サーバーを構成したら、［Test Connectivity］をクリックして、XenMobileサーバーへの接続をチェックします。
11. 接続が確立したら、［Save］をクリックします。

冗長性およびスケーラビリティのためのXenMobile NetScaler Connectorの展開

XenMobile NetScaler ConnectorおよびXenMobile展開のスケーラビリティを向上させるには、XenMobile NetScaler Connectorのインスタンスを複数のWindowsサーバーにインストールして同じXenMobileインスタンスを参照させ、NetScalerを使用してこれらのサーバーの負荷を分散します。

XenMobile NetScaler Connectorの構成には次の2つのモードがあります。

- 非共有モードでは、XenMobile NetScaler Connectorの各インスタンスがXenMobileサーバーと通信し、結果として生成されるポリシーの独自のプライベートコピーを保持します。 たとえば、XenMobileサーバーのクラスターがある場合、XenMobile NetScaler Connectorインスタンスを各XenMobileサーバーで実行すると、XenMobile NetScaler Connectorにより、ローカルXenMobileからポリシーが取得されます。
- 共有モードでは、XenMobile NetScaler Connectorの1つのノードがプライマリノードに指定され、このノードとXenMobileとの通信が行われます。 Windowsネットワーク共有またはWindows（または、サードパーティの）レプリケーションによって、結果として生成される構成がほかのノード間で共有されます。

XenMobile NetScaler Connectorの構成全体は、単一のフォルダー（数個のXMLファイルから構成されます）にあります。 XenMobile NetScaler Connectorの処理によって、このフォルダー内のファイルに加えられた変更が検出され、構成が自動的に再ロードされます。 共有モードのプライマリノードに対するフェイルオーバーはありません。 ただし、システムでは、前回の正常な構成がXenMobile NetScaler Connectorの処理にキャッシュされるため、プライマリサーバーが数分間停止（たとえば、再起動のために）しても許容されます。

XenMobile NetScaler Connectorのシステム要件

Oct 24, 2016

XenMobile NetScaler Connectorでは、NetScalerアプライアンスで構成されたSSLブリッジを介してNetScalerとの通信が行われます。SSLブリッジを使用すると、アプライアンスですべてのセキュアなトラフィックをXenMobileに直接ブリッジすることができます。 XenMobile NetScaler Connectorは、専用のサーバーまたはXenMobileと同じサーバーにインストールできます。 XenMobile NetScaler Connectorには、次の最小システム構成が必要です。

コンポーネント	条件
コンピューターとプロセッサ	Pentium III 733MHz以上のプロセッサ。 Pentium III 2.0GHz以上のプロセッサ（推奨）
NetScaler	ソフトウェアバージョン10を備えたNetScalerアプライアンス
メモリ	1ギガバイト（GB）
ハードディスク	150MBのハードディスクスペースがある、NTFSでフォーマットしたローカルパーティション
オペレーティングシステム	Microsoft Windows Server 2008 R2、Microsoft Windows Server 2008 SP2（推奨）
そのほかのデバイス	ホストオペレーティングシステムと互換性があるネットワークアダプター（内部ネットワークとの通信用）
表示	VGA以上の解像度のモニター

XenMobile NetScaler Connectorのホストコンピューターには、次の最小ハードディスクスペースが必要です。

- Application。 10～15MB（推奨値は100MB）
- Logging。 1GB（推奨値は20GB）

XenMobile NetScaler Connectorのプラットフォームのサポートについて詳しくは、「XenMobileのサポート対象のデバイスプラットフォーム」を参照してください。

XenMobile NetScaler Connectorのインストール

May 10, 2016

XenMobile NetScaler Connectorは、専用のサーバーまたはXenMobileをインストールしたサーバーにインストールできます。

次の場合は、XenMobile NetScaler Connectorを専用のサーバー（XenMobileとは別のサーバー）にインストールすることを検討してください。

- XenMobileサーバーがクラウドにリモートでホストされている場合（物理的な場所）。
- XenMobile NetScaler Connectorが、XenMobileサーバーの再起動の影響を受けないようにする場合（可用性）。
- サーバーのすべてのシステムリソースをXenMobile NetScaler Connector用に使用する場合（パフォーマンス）。

XenMobile NetScaler ConnectorがサーバーにかけるCPU負荷は管理対象デバイスの数によって異なりますが、XenMobile NetScaler ConnectorがXenMobileと同じサーバーに展開されている場合は、一般的な目安として、追加のCPUコアを1つプロビジョニングします。 多数のデバイス（50,000個以上）がある場合に、クラスター環境がないときは、追加のコアが必要になることがあります。 XenMobile NetScaler Connectorのメモリサイズは、追加メモリを保証するのに十分ではありません。

XenMobile NetScaler Connectorをインストール、アップグレード、またはアンインストールするには

May 10, 2016

1. 管理者アカウントでXncInstaller.exeを実行して、XenMobile NetScaler Connector（XNC）をインストールするか、既存のXenMobile NetScaler Connectorをアップグレードまたは削除できます。
2. 画面の指示に従って、インストール、アップグレード、またはアンインストールを完了します。

XenMobile NetScaler Connectorをインストールした後、XenMobileの構成サービスおよび通知サービスを手動で再起動する必要があります。

XNCをアンインストールするには

May 10, 2016

1. 管理者アカウントでXncInstaller.exeを実行します。
2. 画面の指示に従って、アンインストールを完了します。

XenMobile NetScaler Connectorの管理

May 10, 2016

XenMobile NetScaler Connectorで、デバイスの状態、アプリケーションのブラックリストやホワイトリスト、そのほかのさまざまな条件に基づいて、管理対象デバイスからのActiveSync接続要求を許可またはブロックするアクセス制御規則を作成できます。

XenMobile NetScaler Connector構成ユーティリティを使用して、社内のメールポリシーを適用する動的および静的規則を作成し、コンプライアンス基準に違反しているユーザーをブロックすることができます。 また、Exchange Serverを経由して管理対象デバイスに送信されるすべての添付ファイルを暗号化して、管理対象デバイスで権限のあるユーザーのみが添付ファイルを表示できるようにメールの添付ファイル暗号化をセットアップすることができます。

XenMobile NetScaler Connectorのセキュリティモデルの選択

May 10, 2016

許可モデル（［Permit Mode］）

あらゆる規模の組織にとって、モバイルデバイスを適切に展開するには、セキュリティモデルの確立が不可欠です。 一部の保護または隔離されたネットワーク制御を使用して、ユーザー、コンピューター、またはデバイスへのアクセスをデフォルトで許可することは珍しくありませんが、必ずしも適切な方法ではありません。 ITセキュリティを管理する各組織では、モバイルデバイスのセキュリティに対して多少異なったアプローチまたは組織に合わせたアプローチをとっている場合があります。

モバイルデバイスのセキュリティについても、同じことが言えます。 多くのモバイルデバイスおよびその種類、ユーザーごとのモバイルデバイス数、利用できる多数のオペレーティングシステムプラットフォームおよびアプリケーションを考慮すると、許可モデルの使用はお勧めできません。 多くの組織では、制限モデルの使用が最適な選択となります。

XenMobile NetScaler ConnectorとXenMobileの統合で許可される構成シナリオは次のとおりです。

許可セキュリティモデルは、デフォルトでアクセスがすべて許可または付与されているという前提で動作します。 規則またはフィルターの使用時のみ、ブロックされたり、制限が適用されたりします。 許可セキュリティモデルは、モバイルデバイスに対するセキュリティ上の懸念が比較的に低い組織に適しており、必要な場合にのみ（ポリシー規則が失敗した場合）、アクセスを拒否する制限制御を適用します。

制限モデル（［Block Mode］）

制限セキュリティモデルは、デフォルトでアクセスが許可または付与されていないという前提に基づきます。 セキュリティチェックポイントを通過するすべてのデータがフィルターおよび検査され、アクセスを許可する規則をパスしない限り、アクセスが拒否されます。 制限セキュリティモデルは、モバイルデバイスに対するセキュリティ上の条件が比較的に厳しい組織に適しています。 このモードでは、アクセスを許可するすべての規則をパスした場合にのみ、ネットワークサービスの使用機能へのアクセスが許可されます。

XenMobile NetScaler Connectorの構成

May 10, 2016

［Active Sync Service ID］、［Device type］、［User Agent］（デバイスのオペレーティングシステム）、［Authorized user］、［ActiveSync Command］といったプロパティに基づいて、ActiveSync要求を選択的にブロックまたは許可するようにXenMobile NetScaler Connectorを構成できます。

デフォルトの構成では、静的グループと動的グループの組み合わせがサポートされています。 静的グループは、SMG Controller Configurationユーティリティを使用して保守します。 静的グループは、特定のユーザーエージェントを使用するすべてのデバイスなど、デバイスの既知のカテゴリで構成される場合があります。

動的グループは、ゲートウェイ構成プロバイダーと呼ばれる外部ソースによって保守され、XenMobile NetScaler Connectorによって定期的に収集されます。 XenMobileを使用して、許可されたデバイスとユーザーおよびブロックされたデバイスとユーザーのグループをXenMobile NetScaler Connectorにエクスポートできます。

ポリシーとは、アクション（許可またはブロック）が関連付けられた各グループの順序指定された一覧と、グループメンバーの一覧のことです。 ポリシーには、任意の数のグループを含めることができます。 ポリシー内のグループの順序は重要です。これは、1つの一致が見つかると、グループのアクションが実行され、以降のグループは評価されないからです。

メンバーにより、要求のプロパティに一致する方法が定義されます。 デバイスIDなどの単一のプロパティ、またはデバイスの種類およびユーザーエージェントなどの複数のプロパティに一致することが可能です。

XenMobile NetScaler Connectorのポリシーモードの構成

May 10, 2016

XenMobile NetScaler Connectorは、次の6つのモードで実行できます。

- Allow All。 このポリシーモードでは、XenMobile NetScaler Connectorを経由するすべてのトラフィックのアクセスが許可されます。 そのほかのフィルター規則は使用されません。
- Deny All。 このポリシーモードでは、XenMobile NetScaler Connectorを経由するすべてのトラフィックのアクセスがブロックされます。 そのほかのフィルター規則は使用されません。
- Static Rules: Block Mode。 このポリシーモードでは、最後に暗黙的な拒否ステートメントまたはブロックステートメントを使って静的規則が実行されます。 ほかのフィルター規則によって許可または許容されないデバイスは、XenMobile NetScaler Connectorでブロックされます。
- Static Rules: Permit Mode。 このポリシーモードでは、最後に暗黙的な許容ステートメントまたは許可ステートメントを使って静的規則が実行されます。 ほかのフィルター規則によってブロックまたは拒否されないデバイスは、XenMobile NetScaler Connectorで許可されます。
- Static + ZDM Rules: Block Mode。 このポリシーモードでは、最初に静的規則が実行され、最後に暗黙的な拒否ステートメントまたはブロックステートメントを使ってXenMobileから動的規則が実行されます。 デバイスは、定義済みのフィルターおよびDevice Managerの規則に基づいて許容または拒否されます。 定義済みのフィルターおよび規則に一致しないデバイスはブロックされます。
- Static + ZDM Rules: Permit Mode。 このポリシーモードでは、最初に静的規則が実行され、最後に暗黙的な許容ステートメントまたは許可ステートメントを使ってXenMobileから動的規則が実行されます。 デバイスは、定義済みのフィルターおよびXenMobileの規則に基づいて許容または拒否されます。 定義済みのフィルターおよび規則に一致しないデバイスは許可されます。

XenMobile NetScaler Connectorの処理によって、XenMobileから受け取ったiOSモバイルデバイスおよびWindowsベースのモバイルデバイス用の一意のActiveSync IDに基づいて、動的規則が許容またはブロックされます。 Androidデバイスの場合、製造元によって動作が異なり、一部のAndroidデバイスでは、一意のActiveSync IDが直ちに提供されません。 代わりに、XenMobileによりAndroidデバイスのユーザーID情報が送信され、許容するかブロックするかを決定します。 その結果、ユーザーが1台のAndroidデバイスしか持っていない場合でも、許容およびブロック機能が正常に動作します。 ユーザーが複数のAndroidデバイスを持っている場合は、Androidデバイスを明確に区別できないため、すべてのデバイスが許可されます。 ゲートウェイはその場合にも、ActiveSyncID（既知の場合）に基づいてこれらのデバイスを静的にブロックするように構成できます。また、デバイスの種類またはユーザーエージェントに基づいてブロックするようにゲートウェイを構成することもできます。

ポリシーモードを指定するには、SMG Controller Configurationユーティリティで次の操作を実行します。

1. ［Path Filters］タブをクリックし、［Add］をクリックします。
2. ［Path Properties］ダイアログボックスの［Policy］ドロップダウンリストからポリシーモードを選択し、［Save］をクリックします。

［Policies］タブで規則を確認できます。 規則は、XenMobile NetScaler Connectorで最上位から順に処理されます。 ［Allow］が設定されたポリシーは緑のチェックマークで示されます。 ［Deny］が設定されたポリシーは中央に線が入った赤い丸で示されます。 画面を更新して、最近更新された規則を表示するには、［Refresh］をクリックします。 config.xmlファイル内の規則の順序を変更することもできます。

規則をテストするには、［Simulator］タブをクリックします。 フィールドに値を指定します。 これらの値をログから取得することもできます。 ［Allow］または［Block］が指定された結果メッセージが表示されます。

静的規則を構成するには

May 10, 2016

ActiveSync接続のHTTP要求のISAPIフィルターによって読み取られる値を使用して静的規則を入力する必要があります。 静的規則を使用すると、XenMobile NetScaler Connectorで次の条件に基づいてトラフィックを許可またはブロックすることができます。

- User。 XenMobile NetScaler Connectorでは、承認されたユーザー値と、デバイスの登録時に取得された名前構造が使用されます。 これは通常、LDAP経由でActive Directoryに接続されたXenMobileを実行しているサーバーによって参照されるdomain\usernameに示されています。 XenMobile NetScaler Connector構成ユーティリティ内の［Log］タブには、XenMobile NetScaler Connectorを経由して渡される値の構造を決定する必要がある場合、または値の構造が異なる場合に、その値が表示されます。
- Deviceid (ActiveSyncID)。 接続されたデバイスのActiveSyncIDとも呼ばれます。 この値は、通常、XenMobile コンソールの特定のデバイスプロパティページ内にあります。 また、XenMobile NetScaler Connector構成ユーティリティの［Log］タブから、この値を確認できます。
- DeviceType。 XenMobile NetScaler Connectorでは、デバイスがiPhone、iPad、またはそのほかの種類のデバイスかどうかを特定し、その条件に基づいてデバイスを許可またはブロックできます。 ほかの値の場合と同じように、XenMobile NetScaler Connector構成ユーティリティを使用して、ActiveSync接続のために処理中の接続済みデバイスの種類をすべて表示できます。
- UserAgent。 使用するActiveSyncクライアントの情報が含まれます。 ほとんどの場合、指定された値は、モバイルデバイスプラットフォームのオペレーティングシステムの特定のビルドおよびバージョンに対応します。

サーバーで実行中のXenMobile NetScaler Connector構成ユーティリティによって、静的規則は常に管理されます。

1. SMG Controller Configurationユーティリティで、［Static Rules］タブをクリックし、［Add］をクリックします。
2. ［Static Rule Properties］ダイアログボックスで、条件として使用する値を指定します。 たとえば、ユーザー名を入力して（「AllowedUser」など）から［Disabled］チェックボックスをオフにして、アクセスを許可するユーザーを指定します。
3. ［Save］をクリックします。 これで、静的規則が有効になりました。 また、正規表現を使用して値を定義できますが、config.xmlファイルで規則処理モードを有効化する必要があります。

動的な規則を構成するには

May 10, 2016

動的な規則はDevice Managerのデバイスポリシーおよびプロパティによって定義され、ポリシー違反またはプロパティ設定の有無に基づいて、XenMobile NetScaler Connectorの動的フィルターをトリガーできます。 XenMobile NetScaler Connectorのフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。 デバイスが条件に合致すると、デバイスは［Device List］に置かれます。 この［Device List］は、許可一覧およびブロック一覧のどちらでもありません。 これは、定義した条件に合致するデバイスの一覧です。 次の構成オプションでは、XenMobile NetScaler Connectorを使用して［Device List］のデバイスを許可または拒否するかどうかを定義できます。

注：これらの動的規則は、XenMobile Webコンソールで構成する必要があります。

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

2. **[Server]** の下の **[ActiveSync Gateway]** をクリックします。 ［ActiveSync Gateway］ページが開きます。

3. **[Activate the following rules]** で、有効にする1つまたは複数のルールをオンにします。

4. Androidのみ、 **[Send Android domain users to ActiveSync Gateway]** で **[YES]** をクリックし、XenMobileによってAndroidデバイスの情報がSecure Mobile Gatewayに送信されるようにします。 このオプションを有効にすると、Androidデバイスユーザーの ActiveSync識別子がXenMobileにない場合でも、XenMobileによってAndroidデバイスの情報がXenMobile NetScaler Connectorに送信されます。

XenMobile NetScaler ConnectorのXMLファイルを編集してカスタムポリシーを構成するには

May 10, 2016

XenMobile NetScaler Connector構成ユーティリティの［Policies］タブで、デフォルトの構成の基本ポリシーを確認できます。 カスタムポリシーを作成する場合、XenMobile NetScaler ConnectorのXML構成ファイル（config\config.xml）を編集できます。

1. ファイル内のPolicyListセクションに移動し、新しいPolicy要素を追加します。
2. 追加の静的グループや追加のGCPをサポートするグループなどの新しいグループも必要な場合は、新しいGroup要素をGroupListセクションに追加します。
3. 必要に応じて、GroupRef要素を並べ替えることにより、既存のポリシー内のグループの順序を変更できます。

XenMobile NetScaler Connector XMLファイルの構成

May 10, 2016

XenMobile NetScaler Connectorでは、XML構成ファイルを使用して、XenMobile NetScaler Connectorのアクションが指示されます。 このファイルにより、ほかのエントリと同様に、グループファイルと、HTTP要求を評価するときにフィルターにより実行される関連アクションが指定されます。 デフォルトでは、このファイルにはconfig.xmlという名前が付けられ、..\Program Files\Citrix\XenMobile NetScaler Connector\config\に配置されます。

GroupRefノードにより、論理的なグループ名（デフォルトでは、AllowGroupとDenyGroup）が定義されます。
注：GroupRefListノードに表示されるGroupRefノードの順序は重要です。
GroupRefノードのID値により、特定のユーザーアカウントまたはデバイスを一致させるために使用するメンバーの論理的なコンテナーまたはコレクションが特定されます。 アクションの属性により、コレクション内の規則に一致するメンバーをフィルターで処理する方法が指定されます。 たとえば、AllowGroupセットの規則に一致するユーザーアカウントまたはデバイスは「パス」（Exchange CASへのアクセスが許可される）し、DenyGroupセットの規則に一致するユーザーアカウントまたはデバイスは「拒否」（Exchange CASへのアクセスが許可されない）されます。

特定のユーザーアカウント/デバイスまたはその組み合わせが両方のグループの規則に一致する場合、優先する規則を使用して要求の結果が指定されます。 優先順位は、config.xmlファイルのGroupRefノードの最上位から最下位へと至る順序で表されています。 GroupRefノードは優先度によりランク付けされています。 許可グループの特定条件の規則は、拒否グループの同じ条件の規則よりも常に優先されます。

さらに、config.xmlにより、グループノードが定義されます。 これらのノードによって、論理的なコンテナー、つまりAllowGroupおよびDenyGroupが外部XMLファイルとリンクされます。 外部ファイルに格納されたエントリは、フィルター規則の基礎を形成します。
注：このリリースでは、外部XMLファイルのみがサポートされています。
デフォルトのインストールでは、構成に2つのXMLファイル（allow.xmlとdeny.xml）が実装されます。

XenMobileからポリシーをインポートするには

May 10, 2016

1. XenMobile NetScaler構成ユーティリティで、［Config Providers］タブをクリックし、［Add］をクリックします。
2. ［Config Providers］ダイアログボックスの［Name］に、XenMobileサーバーでのHTTP基本認証に使用する、管理者権限を持つユーザー名を入力します。
3. ［Url］に、XenMobile Gateway Configuration Service（GCS）のWebアドレス（通常はhttps://xdmHost/xdm/services/MagConfigServiceという形式）を入力します。 MagConfigServiceの名前は大文字と小文字が区別されます。
4. ［Password］に、XenMobileサーバーでのHTTP基本認証に使用するパスワードを入力します。
5. ［Test Connectivity］をクリックし、ゲートウェイから構成プロバイダーへの接続をテストします。接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い合わせてください。
6. 接続が成功した場合、［Disabled］チェックボックスをオフにし、［Save］をクリックします。
7. ［Managing Host］で、ローカルホストコンピューターのDNS名をデフォルトのままにします。1つのアレイ内で複数のForefront Threat Management Gateway（TMG）が構成されている場合、この設定を使用して、XenMobileとの通信を調整します。

設定を保存してから、GCSを開きます。

XenMobile NetScaler Connectorへの接続を構成するには

May 10, 2016

XenMobile NetScaler Connectorでは、セキュリティで保護されたWebサービスを介してXenMobileおよびそのほかのリモート構成プロバイダーとの通信が行われます。

1. XenMobile NetScaler Connector構成ユーティリティで、［Config Providers］タブをクリックし、［Add］をクリックします。
2. ［Config Providers］ダイアログボックスの［Name］に、XenMobileサーバーでのHTTP基本認証に使用する、管理者権限を持つユーザー名を入力します。
3. ［Url］に、XenMobile GCSのWebアドレス（通常はhttps://ZdmHost/zdm/services/MagConfigServiceという形式）を入力します。 MagConfigServiceの名前は大文字と小文字が区別されます。
4. ［Password］に、XenMobileサーバーでのHTTP基本認証に使用するパスワードを入力します。
5. ［Managing Host］に、XenMobile NetScaler Connectorのサーバー名を入力します。
6. ［Baseline Interval］で、新しく更新された動的規則のセットがDevice Managerから取得される期間を指定します。
7. ［Delta interval］で、動的規則の更新が取得される期間を指定します。
8. ［Request Timeout］で、サーバー要求のタイムアウト間隔を指定します。
9. ［Config Provider］で、構成プロバイダーのサーバーインスタンスによってポリシー構成を提供するかどうかを選択します。
10. ［Events Enabled］で、デバイスがブロックされたときにXenMobile NetScaler ConnectorからXenMobileに通知する場合はこのオプションを有効にします。 XenMobileの自動化された操作でXenMobile NetScaler Connectorの規則を使用する場合、このオプションが必要です。
11. ［Save］をクリックし、［Test Connectivity］をクリックして、ゲートウェイから構成プロバイダーへの接続をテストします。 接続に失敗した場合、ローカルファイアウォールの設定が接続を許可していることをチェックするか、管理者に問い合わせてください。
12. 接続が成功した場合、［Disabled］チェックボックスをオフにし、［Save］をクリックします。

新しい構成プロバイダーを追加すると、XenMobile NetScaler Connectorにより、このプロバイダーに関連付けられた1つまたは複数のポリシーが自動的に作成されます。 これらのポリシーは、config\policyTemplates.xmlのNewPolicyTemplateセクションに含まれているテンプレート定義によって定義されます。 このセクション内で定義される各ポリシー要素に対して、新しいポリシーが作成されます。 ポリシー要素がスキーマ定義に適合していて、標準の置換文字列（中かっこで囲まれた）が変更されていない場合、演算子を使用して、ポリシー要素を追加、削除、または変更できます。 次に、プロバイダーの新しいグループを追加し、ポリシーを更新してこの新しいグループを含めます。

XenMobile NetScaler Connectorのフィルターの選択

May 10, 2016

XenMobile NetScaler Connectorのフィルターは、指定のポリシー違反またはプロパティ設定についてデバイスを解析することにより機能します。 デバイスが条件に合致すると、デバイスは［Device List］に置かれます。 この［Device List］は、許可一覧およびブロック一覧のどちらでもありません。 これは、定義された条件に合ったデバイスの一覧です。 XenMobile内では、XenMobile NetScaler Connectorで次のフィルターを使用できます。

- Blacklisted Apps。 ブラックリストポリシーによって定義されたデバイスの一覧およびブラックリスト内のアプリの存在に基づいて、デバイスが許可または拒否されます。
- Whitelisted Apps only。 ホワイトリストポリシーによって定義されたデバイスの一覧およびホワイトリスト内にないアプリの存在に基づいて、デバイスが許可または拒否されます。
- Unmanaged Devices。 XenMobileデータベース内のすべてのデバイスの一覧が作成されます。 Mobile Application Gatewayは、ブロックモードで展開する必要があります。
- Rooted Android /Jailbroken iOS Devices。 ルートされていることを示すフラグが付けられたすべてのデバイスの一覧が作成され、ルートされた状態に基づいてデバイスが許可または拒否されます。
- Out of Compliance Devices。 独自の内部ITコンプライアンス条件に合致するデバイスが拒否または許可されます。 コンプライアンスは、Out of Complianceという名前のデバイスプロパティによって定義される任意の設定であり、TrueまたはFalseのいずれかになるブール型のフラグです （このプロパティを手動で作成して値を設定するか、デバイスが特定の条件に合致する場合、または合致しない場合は、自動化された操作を使用してデバイス上でこのプロパティを作成できます）。
  - Out of Compliance = True。 デバイスが、IT部門によって設定されたコンプライアンス基準およびポリシー定義に合致しない場合、デバイスはコンプライアンス違反になります。
  - Out of Compliance = False。 デバイスが、IT部門によって設定されたコンプライアンス基準およびポリシー定義に合致する場合、デバイスはコンプライアンスに準拠しています。
- Noncompliant password。 デバイスでパスコードが設定されていないすべてのデバイスの一覧が作成されます。
- Revoked Status。 取り消されたすべてのデバイスの一覧が作成され、取り消された状態に基づいてデバイスが許可または拒否されます。
- Inactive devices。 XenMobileとの通信が特定の期間に行われていないため、非アクティブだと見なされたデバイスの一覧が作成され、それに従ってデバイスが許可または拒否されます。
- Anonymous Devices。 XenMobileに登録されているが、ユーザーのIDが不明なデバイスが許可または拒否されます。 たとえばこのユーザーは、登録されているがActive Directoryパスワードの有効期限が切れている、または不明な資格情報を使って登録されている場合があります。
- Implicit Allow/Deny。 そのほかのフィルタールール条件に合致しないすべてのデバイスの一覧が作成され、この一覧に基づいてデバイスが許可または拒否されます。 ［Implicit Allow/Deny］オプションを使用すると、［Devices］タブにあるXenMobile NetScaler Connectorの状態が確実に有効化され、デバイスのXenMobile NetScaler Connectorの状態が表示されます。 また、［Implicit Allow/Deny］オプションにより、選択されていないほかのすべてのXenMobile NetScaler Connectorフィルターが制御されます。 たとえば、［Blacklists Apps］は、XenMobile NetScaler Connectorによって拒否（ブロック）されます。その一方で、［Implicit Allow/Deny］オプションが［Allow］に設定されているので、ほかのすべてのフィルターは許可されます。

XenMobile NetScaler ConnectorでActiveSyncトラフィックをシミュレートするには

May 10, 2016

XenMobile NetScaler Connectorを使用して、ポリシーと共にActiveSyncトラフィックがどのようになるかシミュレートすることができます。 XenMobile NetScaler Connector構成ユーティリティで、［Simulations］タブをクリックします。 構成した規則にしたがってポリシーがどのように適用されるかが表示されます。

XenMobile NetScaler Connectorの監視

May 10, 2016

XenMobile NetScaler Connector構成ユーティリティでは、Secure Mobile Gatewayによって許可またはブロックされる、Exchange Server経由のすべてのトラフィックを表示するために使用できる詳細なログ記録が提供されます。

認証のためにNetScalerによってXenMobile NetScaler Connectorに転送されるActiveSync要求の履歴を確認するには、［Log］タブを使用します。

また、XenMobile NetScaler Connector Webサービスが実行されていることを確認するには、XenMobile NetScaler Connectorサーバー上のブラウザーにURL（http:///services/ActiveSync/Version）をロードします。 このURLをロードした結果、製品バージョンが文字列で返される場合は、Webサービスが応答しています。