

# 解決された問題

Apr 27, 2017

XenMobile 10.4では、次の問題が修正されています。解決済みのアップグレードツールの問題については、後述の「XenMobileアップグレードツール10.4」を参照してください。

注：バージョン10.4のリリース時点で、Worx Mobile AppsはXenMobile Appsに名前が変更されています。個別のXenMobileアプリの大部分も同様に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。

Windows Phoneのパブリックアプリケーションストアアプリを追加する場合、MicrosoftストアからURLを入力するとアップロードが失敗します。[CXM-13468]

構成によっては、XenMobile 9から10.3.6にアップグレードした後に、XenMobile 9で以前に登録されたデバイスがインストール済みのアプリを開いたり、WorxStoreから新しいアプリをダウンロードしたりできなくなります。アプリはWorx Homeから表示されなくなり、ユーザーはWorxStoreにアクセスできません。[CXM-13708]

特殊文字（小なり記号 (<)、大なり記号 (>)、アンパサンド (&) など）を含む定義済みのWiFiパスワードを使用してWiFiデバイスポリシーを作成すると、ユーザーはWiFiパスワードの入力を求められます。[CXM-13717]

iOSエンタープライズアプリをアップロードしようとするときに、アイコンサイズが1,000KBを上回っていると、「アイコンが見つかりません」というエラーが表示されます。[CXM-13729]

クラスタリングが有効なときに切断されているデバイスにデバイスワイプが送信されると、予期したとおりに、再接続されるたびにデバイスがワイプされます。ただし、デバイスが再登録されるか、異なるクラスターノードに接続した場合、デバイスはXenMobileにより再びワイプされます。[CXM-13793]

共有デバイス登録機能権限は、XenMobileサービス（クラウド）展開では管理者のRBACの役割でデフォルトで有効になっています。結果的に、Adminロールを持つユーザーに属しているすべてのデバイスは共有デバイスとして登録されます。[CXM-15203]

クライアント証明書認証を構成する場合、CAサーバーで [Require Server Name Indication] オプションが有効になっていると登録は失敗します。[CXM-15312]

XenMobileコンソールからGoogle Play Storeアプリを検索する場合、検索は登録されたデバイス上のAndroidオペレーティングシステムに基づいてアプリを返しません。たとえば、最小オペレーティングシステム要件が4.4のアプリが結果に示されません。[CXM-15653]

ローカルグループに割り当てられたローカルユーザーを作成した場合、およびローカルユーザーがWindows 10デバイスを使用して登録しようと試みた場合、登録は失敗します。[CXM-16895]

Citrix Launcherポリシーを作成するとユーザーはAndroidデバイスを登録できますが、ポリシー設定を変更すると、ポリシーで設定したパスワードを使用してCitrixを終了することができなくなります。回避策として、ポリシー設定にパスワードを挿入しなおしてポリシーを更新する必要があります。[CXM-17157]

XenMobileで [Enable ShareFile] オプションを無効にすると、Secure Mail for Androidで、ユーザーはいかなる種類の添付ファイルにもアクセスできません。[CXM-17887]

Rolling Patch 1を伴うXenMobile 10.3.6からXenMobile 10.4に更新する場合、ライセンスの種類が永続的だと、期限切れになり、エラーメッセージが表示されます。[CXM-17900]

XenMobile 10.3.6からXenMobile 10.4に更新する場合、ライセンスの種類が永続的でまだ有効でも、ライセンスが期限切れだ

というエラーメッセージが表示されます。[CXM-17987]

WindowsパブリックストアアプリのURLを手動で入力し、URLがU.S.ストアのURLではない場合、XenMobileコンソールはエラーを表示します。U.S.ストアのアプリURLを使用する場合、アップロードは成功します。[CXM-18013]

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

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

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

XenMobile NetScaler Connectorは、ActiveSyncを使用する同期ではSamsung 5.xデバイスを取得しません。[#613522]

AndroidのWiFiデバイスポリシーを認証方法802.1x EAPで作成すると、[パスワード] フィールドが必須ではなくなります。[#614932]

この修正により、セキュリティ上の脆弱性に関する問題が解決されます。詳しくは、セキュリティ情報 (<http://support.citrix.com/article/CTX207824>) を参照してください。

注：このセキュリティ修正を機能させるには、XenMobileサーバーを2回再起動して修正を有効にする必要があります。[#624347]

現時点では、XenMobileの **[Settings]** > **[Google Play Credentials]** ページの記載に従って電話に「\*##8255#\*##」と入力しても、Android IDを見つけることはできません。デバイスIDの検索には、Google PlayストアのデバイスIDアプリを使用してください。[#633854]

Windows Phoneを登録すると、Worx Homeの起動に失敗することがあります。[#633884]

Worx Storeに無効になったHDXアプリが表示されません。[#634110]

XenMobileサーバーは、ログファイルに誤ったユーザーデータを表示します。[#636754]

XenMobile 10.3.1から10.3.6に更新した後、Files policyプロパティのファイルの種類および目的フォルダーが、XenMobileコンソールに正しく表示されません。[#640334]

[VPP token max length] テキストボックスは256文字です。[#640692]

Windows PhoneユーザーがsAMAccountにデバイスを登録できません。[#640847]

登録されたユーザーをShareFile制御サブシステムから削除した後で、その登録されたユーザーが、XenMobileコンソールのユーザー監査ログファイルに表示されることがあります。[#641342]

XenMobile Server 10.1から10.3.xにアップグレードした後で<https://zdm/enrollmdm.html>をクリックすると、iOSプラットフォームがプラットフォームの選択肢に表示されません。[#641771]

iOSデバイスのためにWorx Homeを登録する場合、MDM登録は成功しても、MAM登録は失敗します。[#644892]

入れ子にされたグループを削除しても反映されません。[#647557]

[**Manage**] > [**Enrollment**] に2,000以上のエントリがある場合、 [**Export**] をクリックするとページが空白になり、レポートは生成されません。[#647855]

XenMobile管理者がXenMobileコンソールにアクセスしようとする、代わりにXenMobile Self-Help Portalに移動することがありました。この問題は、XenMobile管理者グループが役割ベースのアクセス制御を設定して作成されており、グループをあるActive Directory OUから別のActive Directory OUに移動した場合に起きることがあります。[#647987]

iOSアプリをアップロードすると、次のエラーが表示されて失敗します：アップロードされたモバイルアプリは無効です。アプリケーションアイコンが見つかりませんでした。[#649574]

XenMobileサーバーが、メモリ不足エラーで無応答になることがあります。[#650490]

クラスター化されたメッセージが原因の、デバイスワイプの問題。[#650555]

VPN Deviceポリシーを構成する場合、ポート番号を指定できません。[#650972]

クラスタリングを有効にしてXenMobileサーバーをアップグレードした後、いくつかのデッドロックが発生することがあります。サーバーが応答しなくなることがあります。[#651122]

デバイス削除の確認を求めてくるときに、XenMobileコンソールにシリアル番号の詳細が表示されません。[#651185]

XenMobileサーバー10.3.6上のSSOアカウントポリシーは予期したとおりに機能しません。ユーザーはずっとパスワードを求められます。[#651860]

XenMobile 10.3.6上で、VPPアプリに対してiPadアプリの関連付けを無効にできません。[#652280]

デリバリーグループをデバイスポリシーから削除しても、XenMobileに変更が保存されず、デリバリーグループがポリシーに割り当てられたままになります。[#652321]

SSOアカウントが短いFQDNを保存できません。[#652704]

ユーザーがAndroidデバイスからデバイス管理者権限を削除すると、XenMobileはMDX登録済みデバイスとMAM登録済みデバイスの両方の状態を「Orange/unmanaged」に変更し、ユーザーはすべてのMDXアプリにアクセスできなくなります。MAM状態は「Green/managed」のままでなければなりません。[#655180]

## XenMobileアップグレードツール10.4

最大または最小のオペレーティングシステムについてXenMobile 9.0のデバイス設定が10以上に設定され、これがMDXおよびエンタープライズアプリの除外デバイスの場合、アップグレード後に規則が適切に移行されません。表示されるべきアプリが表示されず、表示される必要がないアプリが表示されます。[#603412]

Microsoft SQL Serverは大文字小文字を区別して構成されている場合、表「Id\_Generator」が「id\_generator」として指定されるとアップグレードが失敗します。[#623300]

XenMobile 9からXenMobile 10にアップグレードすると、パーソナルホットスポットプライバシーの値の種類は、文字列ではなくブーリアン型になります。[#633337]

Active Directoryグループ名に「@」が含まれている場合、アップグレードは失敗します。[#633718]

Device Manager 9.0サーバーがローカルのPostgreSQLを使用してセットアップされており、このデータベースサーバーの参照としてローカルホストが使用されている場合、アップグレードは失敗します。この問題を解決するには、Device Manager 9.0サーバーでew-config.propertiesを編集して、すべてのローカルホスト参照をDevice ManagerデータベースサーバーのIPアド

レスで置き換えてから、アップグレード前の要件を実行してください。[#635023]

XenMobile 9.0では、LDAP接続パラメーターでユーザーの組織単位 (Organizational Unit : OU) を定義している場合、XenMobile 10へのアップグレード後に、ユーザーの組織単位に完全なルートコンテキストは追加されません。たとえば、「OU=MDMUsers,OU=SALES」は「OU=MDMUsers,OU=SALES,DC=citrite,DC=com」のようになりません。このため、XenMobile 10で、手動で更新する必要があります。[#635981]

アップグレード中、サポートバンドルをアップロードすると、「MAM set up failed, see the logs for details」というエラーメッセージが表示され、アップグレードツールは破損したMAMデータを保存します。[#638062]

Active Directoryグループ名に「.」が含まれている場合、デリバリーグループとして移行された役割はグループの関連付けを失います。[#647590]

App Controllerのプロキシ設定に「\」文字が含まれている場合、XenMobile 10.1サーバーを起動できず、サーバーが再起動し続け、「Starting main app...」というエラーメッセージが表示されます。[#647919]

XenMobile 9からXenMobile 10にアップグレードすると、アプリ構成がインストールを必要としない限り、有料のVPPアプリがXenMobile (Worx) Storeからインストールされません。[#668102]

ドメイン間の認証の構成で、XenMobile 9から10.3.6にアップグレードした後に、XenMobile 9で以前に登録されたデバイスがインストール済みのアプリを開いたり、Worx (XenMobile) Storeから新しいアプリをダウンロードしたりできなくなります。[CXM-13708]

XenMobile 9からXenMobile 10にアップグレードすると、インストールされたパブリックストアのアプリがXenMobile (Worx) Storeでサブスクリプション解除として表示されます。[CXM-17936]

データベース接続URLがlocalhostの場合、ew-config.propertiesを変更する必要がなくなります。

LDAPとActive Directoryまたはすべての子へのアクセスを制限してRBACの役割を構成していた場合、アップグレード後、XenMobileコンソールに管理者としてログオンしても同じ設定は選択されません。

# 既知の問題

Apr 27, 2017

XenMobile 10.4では、次の問題が修正されています。

Citrix Launcherを構成する場合、**[Just Once]** オプションは機能しません。**[Always]** オプションをクリックする必要があります。[CXM-13413]

場合により、ユーザーがAndroidデバイスを再登録すると、予期していない選択的なワイプが発生します。[CXM-13716]

XenMobileコンソールのパブリックアプリケーションを構成すると、XenMobile 10.4を更新後、Secure HubをWindows 10タブレットに展開しても、ユーザーはパブリックアプリケーションを表示できません。[CXM-16516]

MDMモードのCitrix Launcherで、ユーザーがXenMobile Storeを開くと、ホワイトリストに別のブラウザを追加していても、Storeはデフォルトのブラウザで開きます。[CXM-17097]

Citrix Launcherは、自己署名証明書のあるサーバーからロゴと背景画像をダウンロードできません。[CXM-17159]

XenMobileコンソールをInternet Explore 11ブラウザで使用している場合、新しいLDAP構成を追加できません。[CXM-18324]

## XenMobileアップグレードツール10.4

### データおよびポリシーの問題

アップグレード後、syslogサーバー構成データがXenMobileサーバーに移行されません。[#558539]

一部の制限ポリシー構成が10.1で廃止されました。このため、XenMobile 9からXenMobile 10.4へアップグレードすると、XenMobile 10.4ではすべての制限ポリシーを正常にWindows 10 Phoneに展開することができません。ただし、XenMobile 10.4でポリシー設定を表示して保存すると、ポリシーが正常に展開されます。[#608541]

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

XenMobile 9からXenMobile 10.4にアップグレードした後、WindowsデバイスがMAM+MDMモードでなくMDMモードになります。また、XenMobile Storeが開きません。回避策として、ユーザーは移行したデバイスを再登録できます。[CXM-18532]

### Google Playアプリ

Androidデバイス向けパブリックGoogle Playアプリをデフォルトのアイコンにしている場合、移行後に、デフォルトのアイコンがXenMobileコンソールに表示されません。画像を表示するには、アプリを編集して保存するか、[Check for Updates] をクリックする必要があります。[#557996]

### SQL Server

PostgreSQLデータベースを使用している場合は、アップグレード後にMAMデバイスを再登録できません。この問題を解決するには、XenMobileから該当するデバイスを削除して、ユーザーに登録通知を送信してください。[#632831]

### RBAC

アップグレード後に発生するRBAC設定に関する問題

- スーパー管理者の役割を構成していた場合、すべての権限がデフォルトで選択されます。アップグレード後、RBAC、登録、およびリリース管理の3つの権限のみが選択されます。
- カスタムスーパー管理者の役割を作成していた場合、すべてのスーパー権限がデフォルトで選択されます。アップグレード後、サポート権限設定はどれも選択されません。この問題を回避するには、アップグレード後にサポート権限を設定します。[#569350, #569395, #569423]

## Citrix Secure HubとCitrix Store

XenMobile 9からXenMobile 10.4へのアップグレード前に、WorxStoreにカスタム名があった場合、登録、Worx Homeへのアクセス、WorxStoreへのアクセスに関する問題が発生します。回避策としては、アップグレード前に、ストアをデフォルト設定の「**Store**」に変更します。前提条件の回避策について詳しくは、「[アップグレードツールの前提条件](#)」を参照してください。[#619458]

MAMのみのデバイスを使用するユーザーがXenMobile 9.0からXenMobile 10.4にアップグレードして、LDAPの[**User search by**] オプションを [**samAccountName**] に設定すると、Secure Hubへの認証を行うことができなくなります。[#628233]

## Android at Work

SAML証明書の拡張子は「.pem」でありXenMobileサーバーにインポートされないため、アップグレード後にAndroid for WorkでのSAMLログインが失敗します。[#631795]

この問題を解決するには、以下のように、XenMobileに適切なSAML証明書を配置してください。

1. XenMobile 9 App Controllerから、秘密キー ([AppController.example.com](#)) 付きでSAML証明書をエクスポートします。この証明書はPEM形式であり、拡張子は「.pem」です。

2. opensslコマンドを使用して、PEMファイルからPFXファイルを生成します。

```
openssl pkcs12 -export -out certificate.pfx -in certificate.pem
```

3. PFXファイルを、SAMLキーストアとしてXenMobile 10.3にインポートします。

4. SAML証明書をXenMobile 10.4から秘密キーを付けずにエクスポートして、Android for Workドメインにアップロードします。

# アーキテクチャ

Apr 27, 2017

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記録する必要があります。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Secure Hub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。

- 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、組織内または社外で作成されたモバイルアプリケーション（XenMobile Appなど）を安全にラップできます。アプリケーションをラップした後、XenMobileコンソールを使用してアプリケーションをXenMobileに追加し、ポリシー構成を必要に応じて変更します。また、アプリケーションカテゴリを追加したり、ワークフローを適用したり、アプリケーションをデリバリーグループに展開したりすることができます。「[MDX Toolkitについて](#)」を参照してください。
- StoreFront（オプション）。Receiverとの接続を介して、StoreFrontからWindowsベースのアプリケーションや仮想デスクトップへのアクセスを提供できます。
- ShareFile Enterprise（オプション）。ShareFileを展開する場合は、XenMobileからエンタープライズディレクトリ統合を有効にできます。これは、Security Assertion Markup Language (SAML) IDプロバイダーとして機能します。ShareFileのIDプロバイダーの構成について詳しくは、ShareFileサポートサイトを参照してください。

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

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

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は、「[クラスタリング](#)」を参照してください。

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

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

## モバイルデバイス管理 (MDM) モード

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

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

## MDM+MAMモード

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

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

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



# システム要件と互換性

Apr 27, 2017

その他の要件と互換性情報について詳しくは、次の記事を参照してください。

- [XenMobileの互換性](#)
- [サポート対象のデバイスプラットフォーム](#)
- [ポート要件](#)
- [スケーラビリティ](#)
- [ライセンス管理](#)
- [FIPS 140-2への準拠](#)
- [言語サポート](#)

XenMobile 10.4を使用するには、以下のシステム環境が必要です。

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

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

## NetScaler Gatewayのシステム要件

XenMobile 10.4と共にNetScaler Gatewayを使用するには、以下のシステム環境が必要です。

- 以下のいずれかのサーバーオペレーティングシステム
  - XenServer (サポートされるバージョン：6.5、7.0)
  - VMWare (サポートされるバージョン：ESXi 4.1、ESXi 5.1、ESXi 5.5、ESXi 6.0)
  - Hyper-V (サポートされるバージョン：Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2)
- 2つの仮想CPU
- 2GBのRAM
- 20GBのディスクスペース

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

## XenMobile 10.4のデータベース要件

XenMobileでは、次のいずれかのデータベースが必要です。

- Microsoft SQL Server

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

い)。

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

XenMobile 10.4は、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。

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

注：XenMobileで使用されるSQL Serverのサービスアカウントに、DBcreator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](#)

- PostgreSQL

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

注：XenMobileの全エディションがRemote PostgreSQL 9.5.2と9.3.11 for Windowsをサポートしますが、次の制限事項があります。

- サポートできるのは最大300台のデバイス

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

- クラスタリングはサポートしない

## StoreFrontの互換性

StoreFront 3.6

StoreFront 3.5

StoreFront 3.0

StoreFront 2.6

Web Interface 5.4

XenAppおよびXenDesktop 7.9

XenAppおよびXenDesktop 7.8

XenAppおよびXenDesktop 7.7

XenAppおよびXenDesktop 7.6

XenAppおよびXenDesktop 7.5

XenApp 6.5

## XenMobile 10.4のメールサーバーの要件

XenMobile 10.4では、以下のメールサーバーがサポートされます。

- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010

# ポート要件

Apr 27, 2017

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Citrix Secure Hub、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、「[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) アドレスなどのNetScalerが所有する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 (TCP とUDP)	DNS接続に使用されます。	NetScaler Gateway  XenMobile	DNSサーバー
80	NetScaler Gatewayは、2番目のファイアウォールを介してVPN接続を内部ネットワークリソースに渡します。これは、通常、ユーザーがNetScaler Gateway Plug-inでログオンした場合に起こります。	NetScaler Gateway	イントラネットWebサイト
80または8080	列挙、チケット機能、および認証に使用されるXMLおよびSecure Ticket Authority (STA) ポート。	StoreFrontおよびWeb Interface XMLのネットワークトラフィック	XenDesktopまたはXenApp
443	ポート443の使用を推奨します。	NetScaler Gateway STA	
123 (TCP とUDP)	ネットワークタイムプロトコル (Network Time Protocol : NTP) サービスに使用されます。	NetScaler Gateway  XenMobile	NTPサーバー

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。	インターネット	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。	インターネット	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。	インターネット	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コネクシオンに使用されます。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 デバイス インターネット	XenMobile
4443	管理者がブラウザーを使用してXenMobileコンソールにアクセスする場合に使用されます。	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、Secure Hub for Android、またはSecure Hub for Windows Phoneを介してアプリケーションストアからアプリケーションを公開するために使用されます。	XenMobile	Apple iTunes App Store (ax.itunes.apple.comおよび*.mzstatic.com)  Apple Volume Purchase Program (vpp.itunes.apple.com)  Windows Phoneの場合 : login.live.comおよび *.notify.windows.com  Google Play (play.google.com)
80また は443	XenMobileとNexmo SMS Notification Relay間の送信接続に使用されます。	XenMobile	Nexmo SMS Relay Server
389	セキュリティで保護されないLDAP接続に使用されます。	XenMobile	LDAP認証サーバーまたはActive Directory
443	AndroidおよびWindows Mobileの登録およびエージェント設定に使用されます。	インターネット	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	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)

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

## 自動検出サービスの接続のポート要件

このポート構成では、Secure Hub for Androidのバージョン10.2および10.3から接続するAndroidデバイスで、内部ネットワークからCitrix ADS (Auto Discovery Service : 自動検出サービス) にアクセスできるようになります。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Secure Hubで利用できることを保証します。Secure Hub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。

Secure Hub 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

# スケーラビリティとパフォーマンス

Apr 27, 2017

XenMobileインフラストラクチャの規模を理解することはXenMobileを展開し構成する方法を決定するうえで重要な役割を果たします。このトピックは、小規模から大規模なオンプレミスXenMobile 10.4エンタープライズ展開でパフォーマンスおよびスケーラビリティのインフラストラクチャ要件を判断するための、スケーラビリティテストのデータおよび手順で構成されています。

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

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

このトピックのデータは、10,000~60,000デバイスの規模の展開でテストされた結果です。テストは、既知のワークロードを使用したモバイルデバイスで構成されています。

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

テストでは、NetScaler Gateway 7500（最大10,000デバイスの展開）およびNetScaler Gateway 5550（10,000デバイスを超える展開）を使用しました。同様の、またはそれ以上の容量を持つNetScalerアプライアンスの場合は、同様のまたはそれ以上のスケーラビリティおよびパフォーマンスを提供することが予想されます。

この表では、スケーラビリティテストの結果をまとめています。

スケーラビリティ	最大 <b>60,000</b> デバイス	
ログインレート	既存ユーザーの再接続レート	毎時最大7,500デバイス
構成	NetScaler Gateway	MPX 7500、MPX 5550
	XenMobile Enterprise Editionのみです。	5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

## デバイスおよびハードウェア構成ごとのテスト結果

この表は、展開でテストされたデバイスおよびハードウェア構成のテスト結果を示します。

デバイスの数	10,000	30,000	45,000	60,000
既存デバイスの毎時再接続レート	833	3,750	5,625	7,500

<b>XenMobileサーバー - モード</b>	スタンドアロン	クラスター	クラスター	クラスター
<b>XenMobileサーバー - クラスター</b>	-		4	5
<b>XenMobileサーバー - 仮想アプライアンス</b>	メモリ = 12GBのRAM 仮想CPU = 4	メモリ = 16GBのRAM 仮想CPU = 6	メモリ = 24GBのRAM 仮想CPU = 8	メモリ = 24GBのRAM 仮想CPU = 8
<b>Active Directoryの要件 :</b>	メモリ = 8GBのRAM 仮想CPU = 4	メモリ = 16GBのRAM 仮想CPU = 4	メモリ = 16GBのRAM 仮想CPU = 4	メモリ = 16GBのRAM 仮想CPU = 4
<b>Microsoft SQL Server外部データベース</b>	メモリ = 32GBのRAM 仮想CPU = 16	メモリ = 32GBのRAM 仮想CPU = 12	メモリ = 48GBのRAM vCPUs = 4 (各4コア)	メモリ = 48GBのRAM vCPUs = 4 (各4コア)

45,000デバイスの展開では、SQL Serverはワーカースレッドの数を2,000に増やすように設定されています。60,000デバイスの展開では、SQL Serverはワーカースレッドの数を3,000に増やすように設定されています。(SQL Serverでワーカースレッドの数を設定する方法については、Microsoftの記事 ([max worker threadsサーバー構成オプションの構成](#)) を参照してください。)

## スケーラビリティプロファイル

以下の表は、このトピックのデータを得るために使用されたテストプロファイルについてまとめています。

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

XenMobileサーバーの構成	合計	ユーザーごと
ポリシー	20	20.

アプリ	270	50
パブリックアプリケーション	200	0
MDX	50	30
WebおよびSaaS	20	20
操作	50	
デリバリーグループ	20	
デリバリーグループあたりのActive Directoryグループ	10	

SQL	
データベースの数	1

### デバイス接続およびアプリケーションアクティビティ

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

テストは、通常よりも高い負荷条件にあるXenMobileサーバーノードの再接続間隔をシミュレーションします。この負荷条件は、デバイスの再接続によって、デバイスのすべての関連セキュリティポリシーが取得されるためです。以降の再接続では、変更されたポリシー、または新しいポリシーのみがiOSデバイスにプッシュされるため、XenMobileサーバーノードの負荷は軽減されます。

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

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

8時間のテスト間隔中、以下のアプリケーション関連のアクティビティが発生します。

- Secure Hubが一度起動し、対象アプリ一覧を表示します
- 2つのSAML Webアプリが起動します
- 4つのMAMアプリがダウンロードされます
- Secure Mailで使用する1つのSTAが生成されます
- 240のSTAチケットの検証は、マイクロVPN経由のSecure Mailの再接続イベントごとに、1つずつ実行されます。

## リファレンスアーキテクチャ

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

## 制限事項

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

- Windowsプラットフォームはテストしていません。
- ポリシーのプッシュは、iOSおよびAndroidデバイスでテストされました。
- 各XenMobileサーバーノードは最大10,000デバイスを同時にサポートします。

# ライセンス管理

Apr 27, 2017

XenMobileおよびNetScaler Gatewayにはライセンスが必要です。各エディションでどのXenMobile機能が利用できるかが表示されたデータシートは、この[PDF](#)を参照してください。

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

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

XenMobileのライセンスをダウンロードする前に、Citrixライセンスサーバーをインストールする必要があります。ライセンスファイルを生成するには、Citrixライセンスサーバーをインストールしたサーバー名が必要となります。XenMobileをインストールする場合、そのサーバーにはデフォルトでCitrixライセンスサーバーがインストールされます。または、既存のCitrixライセンスサーバー展開を使ってXenMobileのライセンスを管理できます。Citrixライセンスサーバーのインストール、展開、および管理について詳しくは、「[製品ライセンスの有効化](#)」を参照してください。

## 注意

バージョン10.4.xのXenMobileでは、Citrixライセンスサーバー11.12.1以降が必要です。それより古いバージョンのライセンスサーバーはXenMobile 10.4.xで動作しません。

## Important

XenMobileのノード（インスタンス）をクラスター化する場合は、リモートサーバー上でCitrixライセンスサーバーを使用する必要があります。

受け取ったすべてのライセンスファイルのコピーをローカルに保存しておくことをお勧めします。構成ファイルのバックアップコピーを保存すると、すべてのライセンスファイルもバックアップに含まれます。ただし、最初に構成ファイルをバックアップせずにXenMobileを再インストールする場合は、元のライセンスファイルが必要になります。

## XenMobileライセンスについての考慮事項

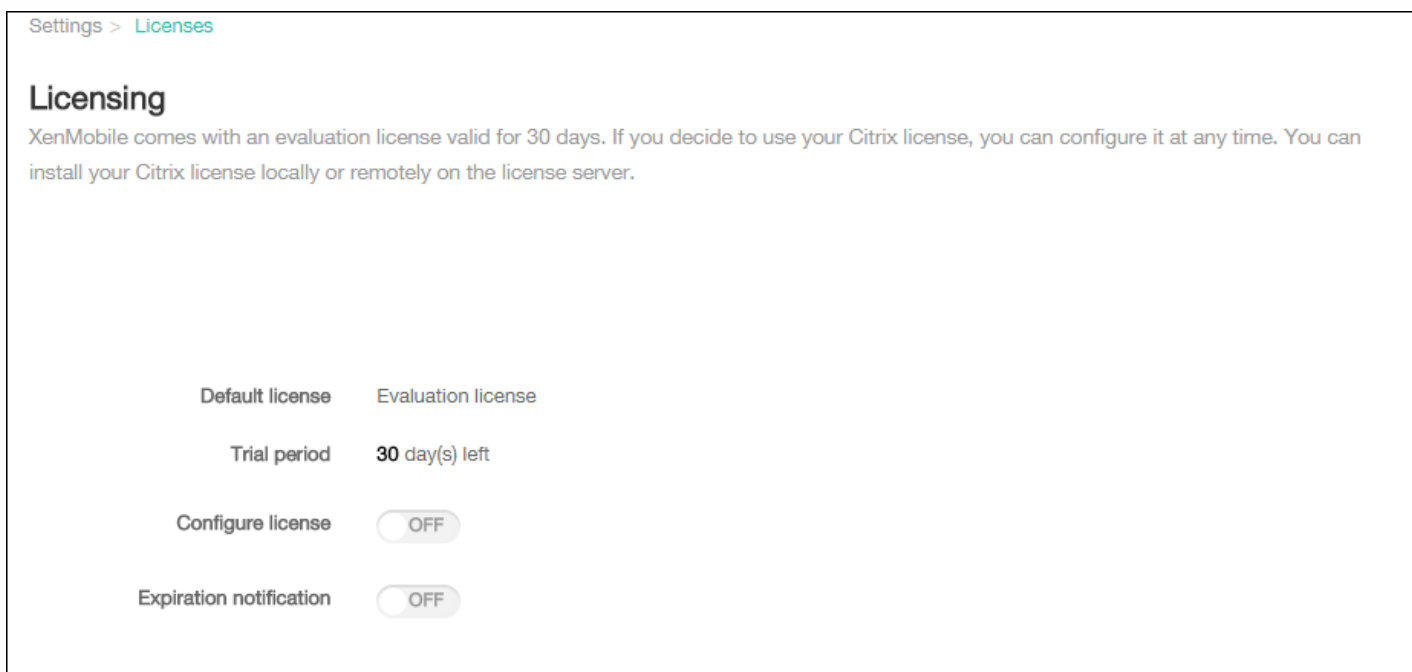
ライセンスがない場合、30日間は試用モードでXenMobileのすべての機能を実行することができます。この試用モードを使用できるのは、XenMobileのインストール時から30日間の1回限りです。有効なXenMobileライセンスを使用できるかどうかに関係なく、XenMobile Webコンソールへのアクセスはブロックされません。XenMobileコンソールで、試用期間の残り日数を参照できます。

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

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

XenMobileコンソールで [Licensing] ページを開くには

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



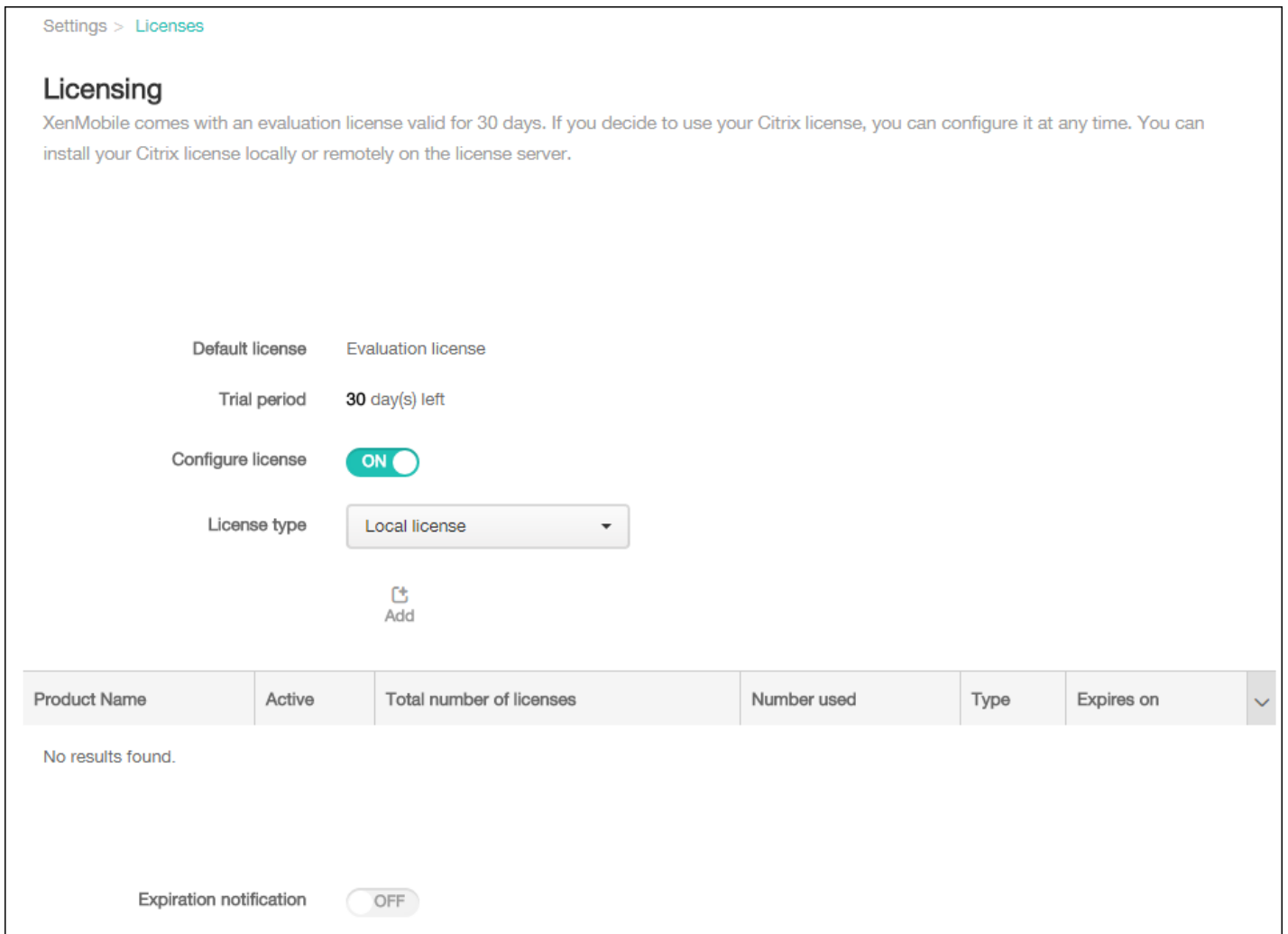
1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Licensing] をクリックします。[Licensing] ページが開きます。

ローカルライセンスを追加するには

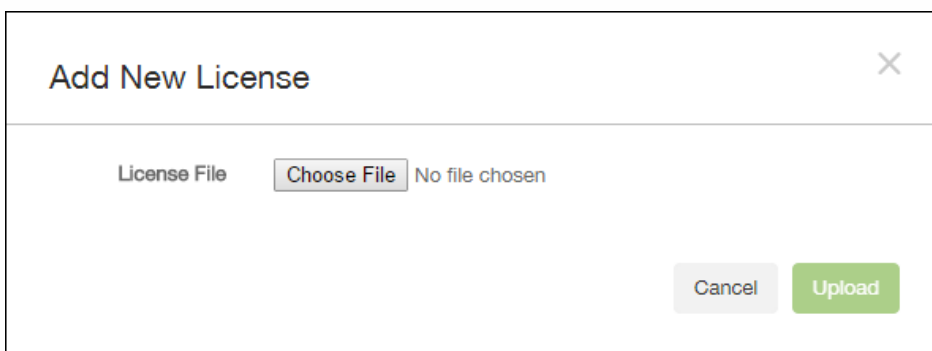
新しいライセンスを追加すると、表にライセンスが表示されます。最初に追加したライセンスは自動的にアクティブ化されません。カテゴリ (Enterpriseなど) および種類 (デバイスなど) が同じライセンスを複数追加した場合、表ではこれらのライセンスが1つの行として表示されます。この場合、[Total number of licenses] と [Number used] に、共通するライセンスの合計数が表示されます。[Expires on] の日付は、共通するライセンスのうち最も後の有効期限を示します。

ローカルライセンスの管理は、すべてXenMobileコンソールで行います。

1. ライセンス管理コンソールを介してSimple License Serviceから、またはCitrix.comのアカウントから直接、ライセンスファイル入手します。詳しくは、「[ライセンスファイルの入手](#)」を参照してください。
2. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
3. [Licensing] をクリックします。[Licensing] ページが開きます。
4. [Configure license] を [On] に設定します。[License type] ボックス、[Add] ボタン、[Licensing] の表が表示されます。[Licensing] の表には、XenMobileで使用したライセンスが表示されます。Citrixライセンスをまだ追加していない場合、この表は空白です。



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



6. [Add New License] ダイアログボックスで、[Choose File] をクリックし、ライセンスファイルの場所を参照します

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



License type

|

Product Name	Active	Total number of licenses	Number used	Type	Expires on
Citrix XenMobile Enterprise Edition[Device]	✓	15002	0	Retail	01-DEC-2015

Showing 1 - 1 of 1 items

Expiration notification

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

リモートライセンスを追加するには

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

1. **[Licensing]** ページで、**[Configure license]** を **[On]** に設定します。**[License type]** ボックス、**[Add]** ボタン、**[Licensing]** の表が表示されます。**[Licensing]** の表には、XenMobileで使用したライセンスが表示されます。Citrixライセンスをまだ追加していない場合、この表は空白です。

3. **[License type]** を **[Remote license]** に設定します。**[Add]** ボタンが、**[License server]** フィールドおよび**[Port]** フィールドと、**[Test Connectivity]** ボタンに置き換わります。

License type

License server\*

Port\*

Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

4. 次の設定を構成します。

- **License server** : リモートライセンスサーバーのIPアドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- **Port** : デフォルトポートをそのまま使用するか、ライセンスサーバーとの通信に使用するポート番号を入力します。

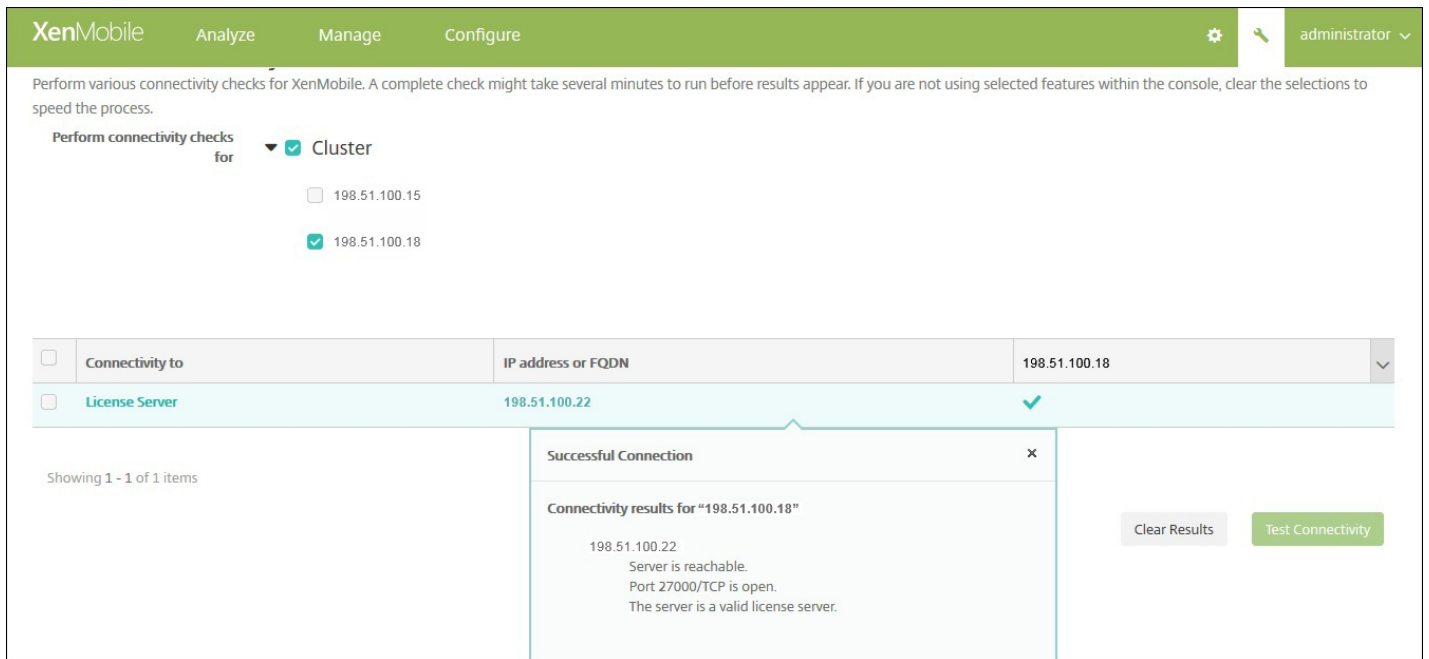
5. **[Test Connection]** をクリックします。接続が成功した場合、XenMobileはライセンスサーバーに接続し、使用可能なライセンスがライセンスの表に表示されます。ライセンスが1つのみの場合は、自動的にアクティブ化されます。

**[Text Connection]** をクリックすると、XenMobileで以下のことが確認されます。

- XenMobileがライセンスサーバーと通信できるか。

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

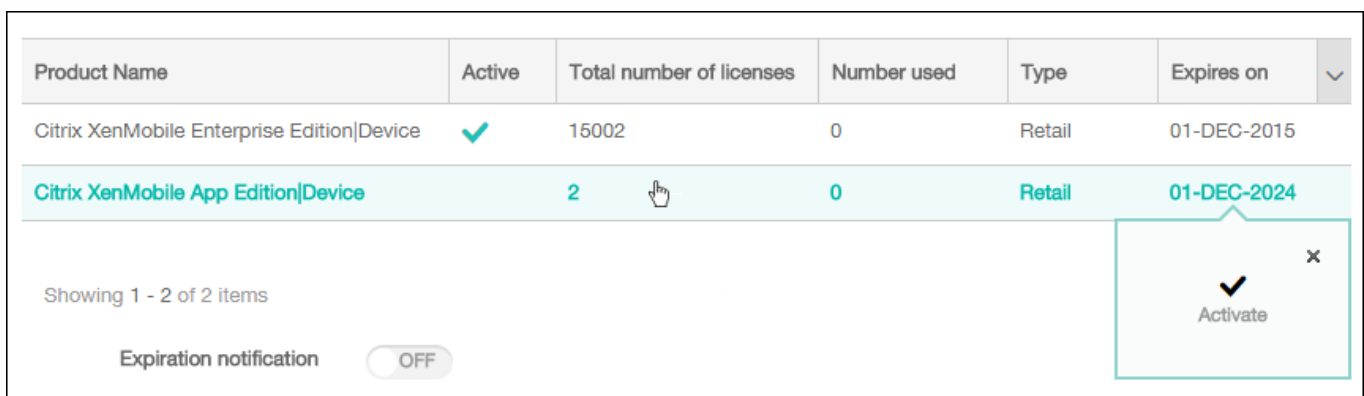
接続に失敗した場合は、表示されるエラーメッセージを確認し、必要な修正を加えてから、**[Test Connection]** をクリックします。



別のライセンスをアクティブ化するには

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

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



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

3. **[Activate]** をクリックします。選択したライセンスがアクティブ化されます。

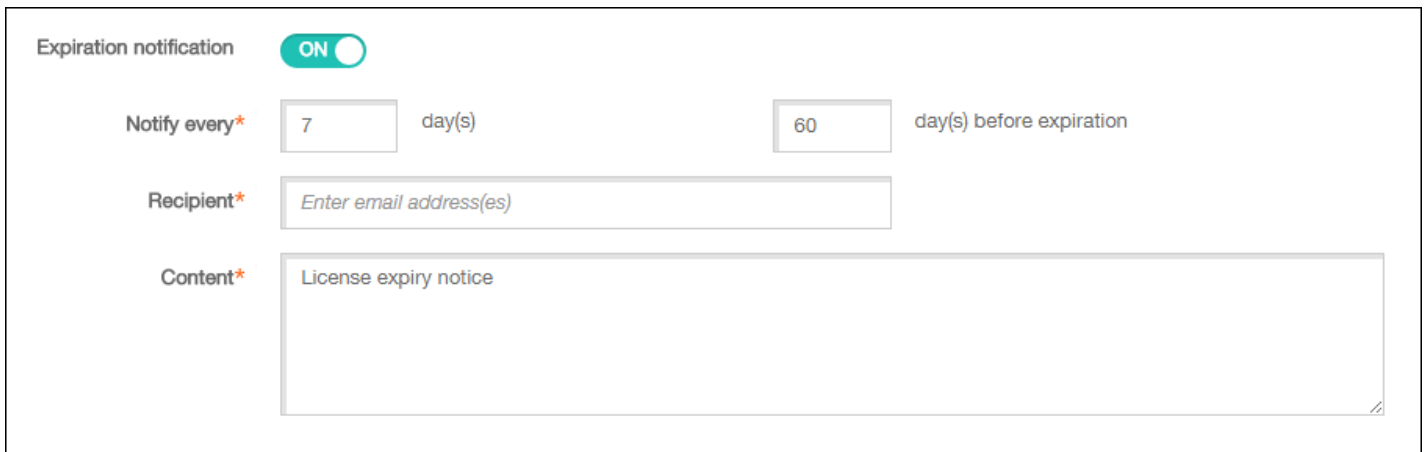
## Important

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

有効期限通知を自動化するには

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

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



The screenshot shows the configuration for 'Expiration notification'. At the top, there is a toggle switch labeled 'Expiration notification' which is turned 'ON'. Below this, there are three main fields:

- Notify every\***: A text input field containing the number '7', followed by the text 'day(s)'. To its right is another text input field containing the number '60', followed by the text 'day(s) before expiration'.
- Recipient\***: A text input field with the placeholder text 'Enter email address(es)'.
- Content\***: A large text area containing the text 'License expiry notice'.

2. 次の設定を構成します。

- **Notify every** : 以下を入力します。
  - 通知が送信される頻度 (7日ごとなど)。
  - 通知の送信を開始する時期 (ライセンス有効期限の60日前など)。
- **Recipient** : 自分またはライセンス担当者のメールアドレスを入力します。
- **Content** : 受信者への有効期限通知メッセージの内容を入力します。

3. **[Save]** をクリックします。有効期限の残りが設定した日数になると、**[Recipient]** に入力した受信者への、**[Content]** に入力したテキストを含むメールメッセージの送信が開始されます。設定した頻度で通知が送信されます。

# FIPS 140-2への準拠

Apr 27, 2017

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

**重要：** FIPSサポートを利用できるのは、XenMobileサーバーがオンプレミスにインストールされている場合のみです。XenMobile FIPSモードは、初回インストール時にのみ有効化できます。

**注：** HDXアプリケーションが使用されない限り、XenMobileモバイルデバイス管理のみ、XenMobileモバイルアプリケーション管理のみ、およびXenMobileエンタープライズはすべてFIPSに準拠しています。

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

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、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のドキュメントの「**FIPS**」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。

# 言語サポート

Apr 27, 2017

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

ここでは、XenMobile 10.4でサポートされる言語を示します。

## XenMobileコンソールおよび自己ヘルプポータル

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

## XenMobileアプリ

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

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

## iOSまたはAndroid

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

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

## Windows :

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

右書きの言語のサポート

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

	<b>iOS</b>	<b>Android</b>
Secure Hub	○	○
Secure Mail	○	○
Secure Web	○	○
Secure Tasks	○	○
Secure Notes	○	○
QuickEdit	○	○

# インストールと構成

Apr 27, 2017

以下の点に注意してください。

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

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

インストール手順は、この記事で後述している『[XenMobileのインストール](#)』を参照してください。

## インストール前チェックリスト

### ネットワークの基本的な接続

以下はXenMobileソリューションに必要なネットワーク設定です。

•	前提条件または設定	コンポーネントまたは機能	設定の記録
	リモートユーザーが接続する完全修飾ドメイン名 (Fully Qualified Domain Name : FQDN) を記録します。	XenMobile NetScaler Gateway	
	パブリックおよびローカルIPアドレスを記録します。  ネットワークアドレス変換 (Network Address Translation : NAT) を設定するためのファイアウォールの構成にはこれらのIPアドレスが必要です。	XenMobile NetScaler Gateway	
	サブネットマスクを記録します。	XenMobile NetScaler Gateway	
	DNS IPアドレスを記録します。	XenMobile NetScaler Gateway	
	WINSサーバーのIPアドレスを記録します (該当する場合)。	NetScaler Gateway	



NetScaler Gatewayのホスト名を調べて記録します。  注：これはFQDNではありません。FQDNは、仮想サーバーにバインドされ、ユーザーが接続する署名されたサーバー証明書に含まれます。NetScaler Gatewayのインストールウィザードを使用してホスト名を構成できます。	NetScaler Gateway	
XenMobileのIPアドレスを記録します。  XenMobileのインスタンスを1つインストールする場合は、IPアドレスを1つ予約します。  クラスターを構成する場合は、必要なすべてのIPアドレスを記録します。	XenMobile	
<ul style="list-style-type: none"> <li>NetScaler Gateway上で構成された1つのパブリックIPアドレス</li> <li>NetScaler Gateway用の1つの外部DNSエントリ</li> </ul>	NetScaler Gateway	
WebプロキシサーバーのIPアドレス、ポート、プロキシホストの一覧、および管理者のユーザー名とパスワードを記録します。ネットワークにプロキシサーバーを展開する場合は、これらの設定はオプションです（該当する場合）。  注：Webプロキシのユーザー名を構成するときには、sAMAccountNameまたはユーザープリンシパル名（User Principal Name : UPN）のいずれかを使用できます。	XenMobile  NetScaler Gateway	
デフォルトゲートウェイのIPアドレスを記録します。	XenMobile  NetScaler Gateway	
システムIP（NSIP）アドレスとサブネットマスクを記録します。	NetScaler Gateway	
サブネットIP（SNIP）アドレスとサブネットマスクを記録します。	NetScaler Gateway	
NetScaler Gatewayの仮想サーバーIPアドレスとFQDNを証明書から記録します。  複数の仮想サーバーを構成する必要がある場合は、証明書からすべての仮想IPアドレスとFQDNを記録します。	NetScaler Gateway	
ユーザーがNetScaler Gatewayを通してアクセスできる内部ネットワークを記録します。  例：10.10.0.0/24  分割トンネリングが [On] に設定されているとき、ユーザーがSecure HubまたはNetScaler Gateway Plug-inと接続するときにアクセスする必要のあるすべての内部ネットワークおよびネッ	NetScaler Gateway	

	トワークセグメントを入力します。		
	XenMobileサーバー、NetScaler Gateway、外部Microsoft SQL Server、およびDNSサーバーの間のネットワーク接続が到達可能であることを確認します。	XenMobile NetScaler Gateway	


## ライセンス管理

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

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

## 証明書

XenMobileおよびNetScaler Gatewayは、ほかのCitrix製品およびアプリケーションと接続するため、およびユーザーデバイスから接続するために、証明書が必要です。詳しくは、XenMobileのドキュメントの「[証明書および認証](#)」を参照してください。

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

## ポート

XenMobileコンポーネントと通信できるように、ポートを開く必要があります。

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

## データベース

データベース接続を構成する必要があります。XenMobileリポジトリでは、サポート対象バージョン (Microsoft SQL Server

2014、SQL Server 2012、SQL Server 2008 R2、SQL Server 2008) のいずれかで稼動しているMicrosoft SQL Serverデータベースが必要です。Citrixでは、Microsoft SQLをリモートで使用することをお勧めします。XenMobileにはPostgreSQLが付属しており、ローカルまたはリモートで、テスト環境においてのみ使用する必要があります。

•	前提要件	コンポーネント	設定の記録
	<p>Microsoft SQL ServerのIPアドレスとポート。</p> <p>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。</p>	XenMobile	

## Active Directoryの設定

•	前提要件	コンポーネント	設定の記録
	<p>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。</p> <p>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。</p>	XenMobile NetScaler Gateway	
	Active Directoryドメイン名を記録します。	XenMobile NetScaler Gateway	
	<p>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。</p> <p>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。</p>	XenMobile NetScaler Gateway	
	<p>ユーザーベースDNを記録します。</p> <p>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。</p>	XenMobile NetScaler Gateway	
	<p>グループベースDNを記録します。</p> <p>これはグループが置かれるディレクトリのレベルです。</p> <p>NetScaler GatewayおよびXenMobileは、Active Directoryのクエリにこれを使用します。</p>	XenMobile NetScaler Gateway	

## XenMobileとNetScaler Gatewayの間の接続

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

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

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

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

# XenMobileのインストール

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

## 注意

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

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

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

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

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

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

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

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

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

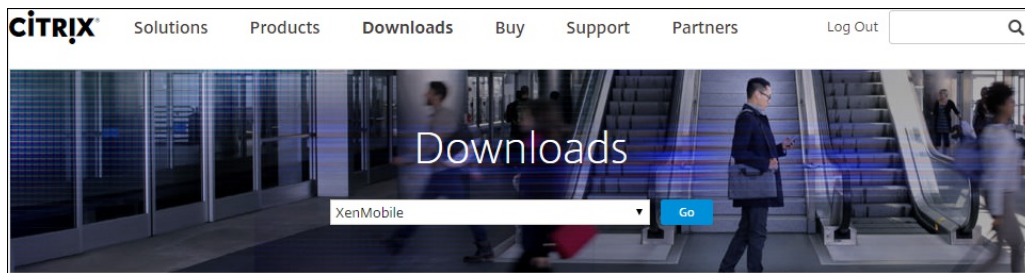
## XenMobile製品ソフトウェアのダウンロード

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

## XenMobileのソフトウェアをダウンロードするには

1. [CitrixのWebサイト](#)にアクセスします。

2. [Search] ボックスの横の [Log on] をクリックしてアカウントにログオンします。
3. [Downloads] タブをクリックします。
4. [Downloads] ページの製品一覧で、 [XenMobile] を選択します。



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

## NetScaler Gatewayのソフトウェアをダウンロードするには

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

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

### 初回使用時のXenMobileの構成

初回使用時のXenMobileの構成プロセスは2つの部分から成ります。

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

## 注意

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

## コマンドプロンプトウィンドウでのXenMobileの構成

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

### 重要：

コマンドプロンプトで作成する管理者アカウント、公開キー基盤 (PKI) サーバー証明書、およびFIPSのパスワードを作成または変更すると、XenMobileでは以下の規則をActive Directoryユーザーを除くすべてのユーザーに適用します。Active DirectoryユーザーのパスワードはXenMobileの外部で管理されます。

- パスワードは8文字以上にして、以下の複雑度の条件のうち3つ以上を満たす必要があります。
  - 大文字 (A~Z)
  - 小文字 (a~z)
  - 数字 (0~9)
  - 特殊文字 (!、#、\$、%など)

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the initial configuration of XenMobile. Accept options offered by pressing Enter/Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the command prompt.
Username: admin
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。

4. 以下の情報を入力して「y」を入力し、設定を確定します。
  1. XenMobileサーバーのIPアドレス
  2. ネットマスク
  3. デフォルトゲートウェイ。DMZのデフォルトゲートウェイのIPアドレスです。
  4. プライマリDNSサーバー。DNSサーバーのIPアドレスです。
  5. セカンダリDNSサーバー (オプション)

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

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

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

- 「y」を入力して、セキュリティを高めるためにランダムな暗号化パスワードを生成するか、「n」を入力して独自のパスワードを指定します。Citrixでは、「y」を入力してランダムなパスワードを生成することをお勧めします。このパスワードは、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ワードのハッシュが、データの暗号化と復号化でキーを取得するときに使用されます。このパスワードを表示することはできません。

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

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

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

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

- 以下の情報を入力してデータベース接続を構成します。

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

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



4. XenMobileをホストするサーバーの完全修飾ドメイン名 (FQDN) を入力します。この1つのホストサーバーで、デバイス管理サービスとアプリケーション管理サービスの両方を提供します。
  5. データベースのポート番号がデフォルトのポート番号と異なる場合は入力します。デフォルトのMicrosoft SQL用ポートは1433で、PostgreSQL用のポートは5432です。
  6. データベース管理者のユーザー名を入力します。
  7. データベース管理者のパスワードを入力します。
  8. データベース名を入力します。
  9. **Enter**キーを押してデータベース設定を確定します。
8. オプションとして、「y」を入力してXenMobileノードまたはインスタンスのクラスター化を有効にします。

```
Cluster:
Please press y to enable cluster? [y/n]: y
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu, once the system configuration is complete.
```

**重要** : XenMobileクラスターを有効にする場合は、クラスターメンバー間のリアルタイム通信を有効にするために、システム構成を完了した後でポート80を必ず開放してください。この操作は、すべてのクラスターノード上で完了する必要があります。

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

```
XenMobile hostname:
Hostname: justan.example.com
```

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

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

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

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

**重要** : XenMobileのノード (イン

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

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

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

15. **Enter**キーを押して設定を確定します。
16. Webブラウザを使用して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 console through a web browser.
Username [administrator]: administrator
Password:
Re-enter new password:
```

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

17. **Enter**キーを押して設定を確定します。最初のシステム構成が保存されます。

18. この処理がアップグレードであるかどうかを確認するメッセージが表示されたら、新規インストールであるため、「n」を入力します。

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

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

Initial system configuration complete!

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

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

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

Starting monitoring... [ OK ]
```

## Webブラウザでの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ブラウザでその処理を完了します。

1. Webブラウザで、コマンドプロンプトウィンドウ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。



# XenMobile

User name

Password

Sign in

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

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

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

注：この手順ではサーバーを再起動する必要があります。

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

注：

- 組織の内部ネットワーク（またはイントラネット）の境界にNetScaler Gatewayを展開して、内部ネットワークのサーバー、アプリケーション、およびそのほかのネットワークリソースへの安全な単一のアクセスポイントを提供できます。この展開では、すべてのリモートユーザーが、内部ネットワークの任意のリソースにアクセスする前に、NetScaler Gatewayに接続する必要があります。
- NetScaler Gatewayはオプションの設定ですが、ページでのデータ入力後にそのページから移動するには、必須フィールドを消去するか入力する必要があります。

8. Active Directoryからのユーザーとグループにアクセスするため、LDAP構成を完了します。LDAP接続の構成について詳しくは、「[LDAP構成](#)」を参照してください。

9. 通知サーバーを構成して、ユーザーにメッセージを送信できるようにします。通知サーバー構成について詳しくは、次を参照してください。 [通知](#)。

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

# XenMobileでのFIPSの構成

Apr 27, 2017

XenMobileの米国の情報処理標準（FIPS : Federal Information Processing Standards）モードは、すべての暗号化操作に対してFIPS 140-2証明済みライブラリのみを使用するようにサーバーを構成して、米国政府のカスタマーをサポートします。XenMobileサーバーをFIPSモードでインストールすると、すべての静止データおよびXenMobileクライアントとサーバーの間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SSL通信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. 初期セットアップ時に**FIPSモード**を有効にします。
2. SQL Server用のルートCA証明書をアップロードします。SQL Serverで公開証明書ではなく自己署名SSL証明書を使用した場合は、このオプションについては【はい】を選択して、次のいずれかを実行します。
  - a. CA証明書をコピーして貼り付けます。
  - b. CA証明書をインポートします。CA証明書をインポートするには、XenMobileサーバーからHTTP URLを介してアクセスできるWebサイトに証明書を送信する必要があります。詳しくは、この記事で後述している「[証明書のインポート](#)」セクションを参照してください。
3. SQL Serverのサーバー名とポート番号、SQL Serverにログインするための資格情報、およびXenMobileに対して作成するデータベース名を指定します。

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

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

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

## 証明書のインポート

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

## SQLの前提条件

1. XenMobileからSQLインスタンスの接続をセキュリティで保護し、SQL Serverのバージョンは2012または2014が必要です。接続の保護については、「[How to enable SSL encryption for an instance of SQL Server by using Microsoft Management Console](#)」を参照してください。
2. サービスが適切に再開しない場合は、**Services.msc**を開いて次のようにチェックします。
  - a. SQL Serverサービスで使用されたログオンアカウント情報をコピーします。  
SQL ServerでMMC.exeを起動します。
  - c. [ファイル] > [スナップインの追加と削除] の順に選択し、証明書アイテムをダブルクリックして証明書スナップインを追加します。ウィザードの2つのページでコンピューターアカウントとローカルコンピューターを選択します。
  - d. [OK] をクリックします。
  - e. [証明書 (ローカルコンピューター)] > [個人] > [証明書] の順に選択し、インポートされたSSL証明書を探します。
  - f. インポートされた証明書を右クリックして[すべてのタスク] > [秘密キーの管理] の順に選択します。
  - g. [グループ名またはユーザー名] で [追加] をクリックします。
  - h. 前の手順でコピーしたSQLサービスアカウント名を入力します。
  - i. [フルコントロールを許可] オプションをクリアします。デフォルトでは、サービスアカウントにはフルコントロールと読み取り権限のどちらもが付与されますが、秘密キーの読み取りだけが必要です。
  - j. MMCを閉じ、SQLサービスを開始します。
3. SQLサービスが正常に開始されたか確認します。

## インターネットインフォメーションサービス (IIS) の前提条件

1. ルート証明書 (base 64) をダウンロードします。
2. ルート証明書をIISサーバー上のデフォルトのサイト (C:\inetpub\wwwroot) にコピーします。
3. デフォルトサイトに対して [認証] チェックボックスをオンにします。
4. [匿名] を [有効] に設定します。
5. [要求追跡の失敗] 規則チェックボックスをオンにします。
6. .cerがブロックされていないか確認します。

7. ローカルサーバーのInternet Explorerブラウザで.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に表示されます。

8. ルート証明書がInternet Explorerブラウザに表示されない場合、ASPがIISで有効化されているかを次のようにして確認します。

a. Server Managerを開きます。

[管理] > [役割と機能の追加] の順に移動します。

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

[次へ] をクリックしてインストールを完了させます。

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

詳しくは、[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://<IISサーバーの完全修飾ドメイン名>cert.cer
- サーバー：SQLサーバーの完全修飾ドメイン名
- ポート：1433
- ユーザー名：データベースを作成できるサービスアカウント (domain\username) 。
- パスワード：サービスアカウントのパスワード。
- データベース名：選択した名前。

# クラスタリングの構成

Apr 27, 2017

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

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

モバイルデバイス管理 (MDM) 負荷分散仮想IPアドレスおよびモバイルアプリケーション管理 (MAM) 負荷分散仮想IPアドレスの完全修飾ドメイン名 (FQDN) は登録FQDNと同一の、XenMobileサーバーのFQDNです。

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

## 前提条件

- 必要なXenMobileノードが完全に構成されていること
- MDM負荷分散用の1つのパブリックIPアドレス
- MAM負荷分散用のRFC 1918で定義された範囲の1つのプライベートIPアドレス
- サーバー証明書
- NetScaler Gateway仮想IPアドレス用の1つの空きIPアドレス

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

## XenMobileクラスターノードのインストール

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

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

```
*****
*           Citrix XenMobile           *
*   (in First Time Use mode)         *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through t
he initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password: _
```

2. 次の図のようなネットワーク構成情報を指定します。

```

Network settings:
IP address []: 10.147.75.51
Netmask []: 255.255.255.0
Default gateway []: 10.147.75.1
Primary DNS server []: 10.147.75.240
Secondary DNS server (optional) []:

Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps

```

3. データ保護でデフォルトのパスワードを使用する場合は「y」と入力します。デフォルト以外のパスワードを使用する場合は「n」と入力して、新しいパスワードを入力します。

```

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

```

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。

```

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

```

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.

```

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_service1]: DB_51

Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..

```

6. 最初のVMに付与した証明書のも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 [1]: 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 using 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 Infrastructure (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 Infrastructure (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..... [ OK ]
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: |
```

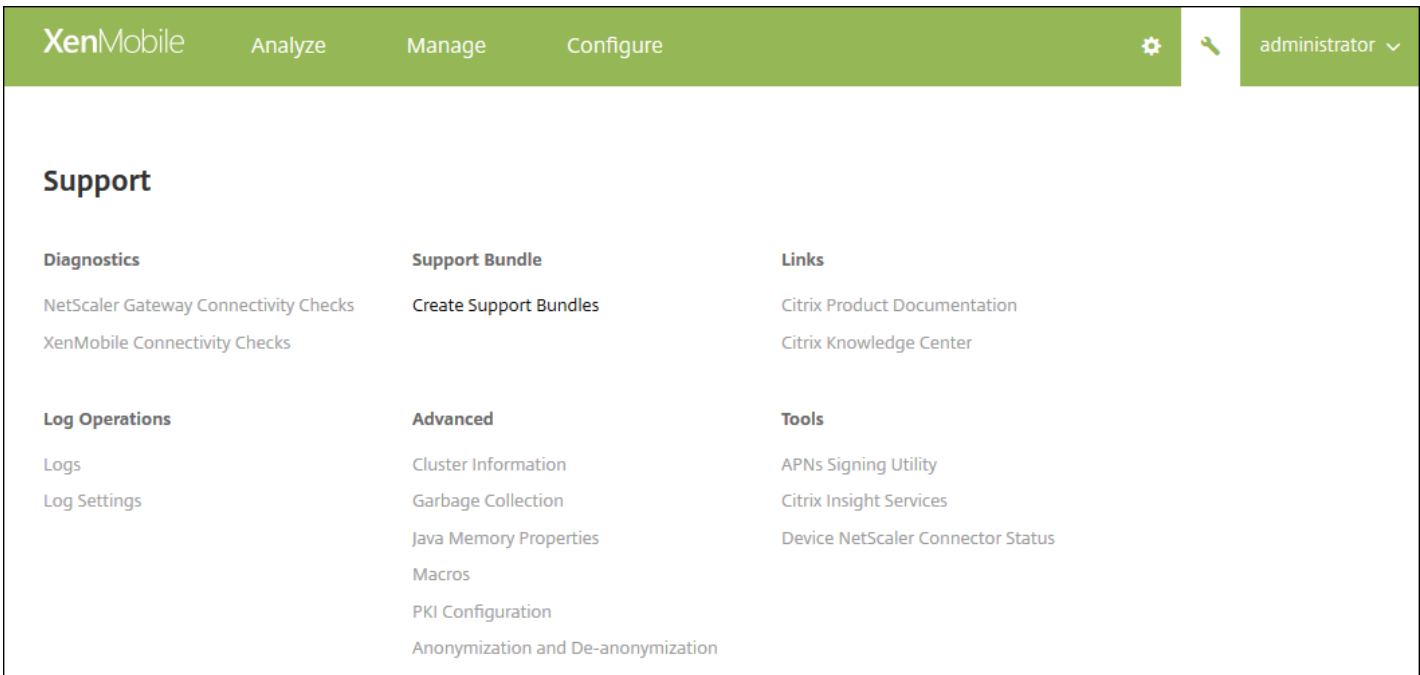
注：ログオンダイアログボックスは最初のVMのログオンダイアログボックスと同じです。同じであるため、両方のVMで同じデータベースサーバーを使用していることが確認できます。

- 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. XenMobileコンソールで、右上のレンチアイコンをクリックします。



[Support] ページが開きます。

- 10. [Advanced] の [Cluster Information] 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。

Node ID	Node name	Status	Role	First check-in	Next check-in
177425211		ACTIVE	null	2019-04-22 14:40:34.877	2019-04-22 01:52:56.293
177425208		ACTIVE	OLDEST	2019-04-22 14:30:06.47	2019-04-22 02:09:02.61

別のノードを追加する場合も、手順は同じです。ノードに追加された最初のクラスターには、**OLDEST**という役割が割り当てられています。その後追加されたクラスターの役割には、**NONE**または**null**が表示されます。

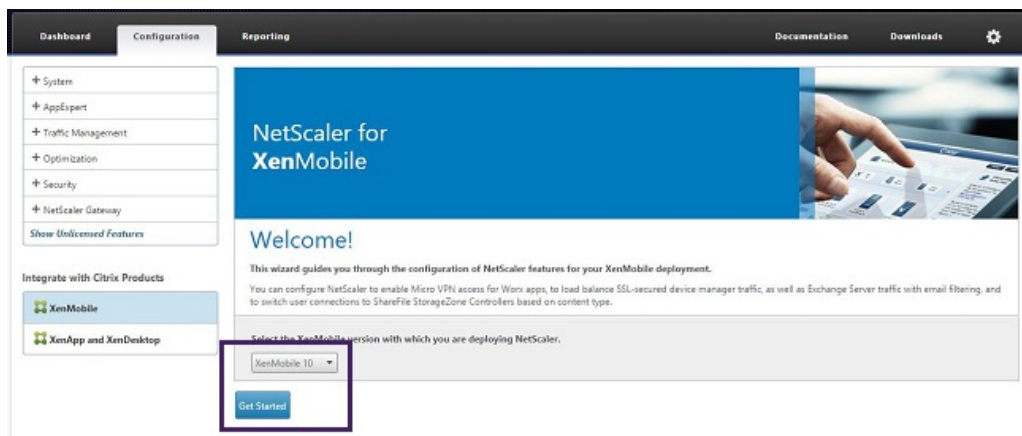
### NetScalerでXenMobileクラスターの負荷分散を構成するには

必要なノードをXenMobileクラスターのメンバーとして追加した後、クラスターにアクセスできるようにノードの負荷分散を行う必要があります。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。

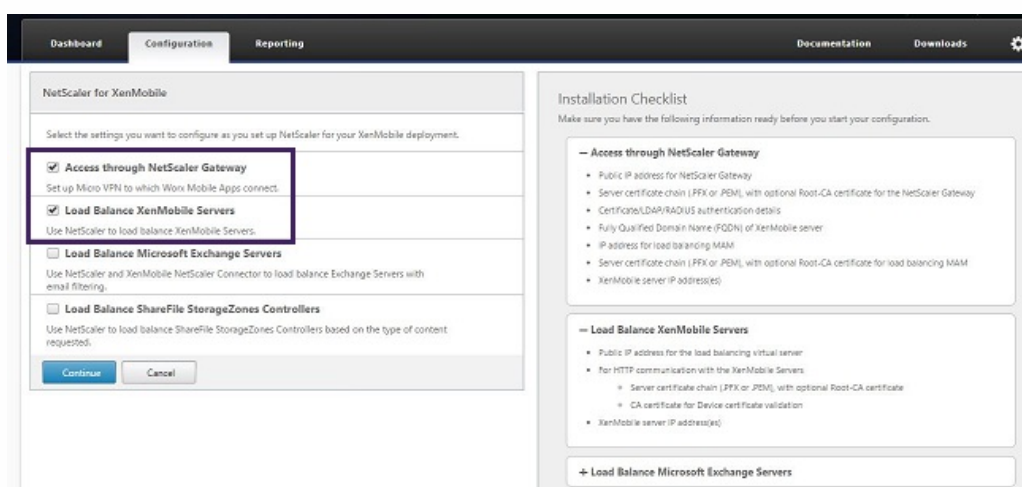
1. NetScalerにログオンします。



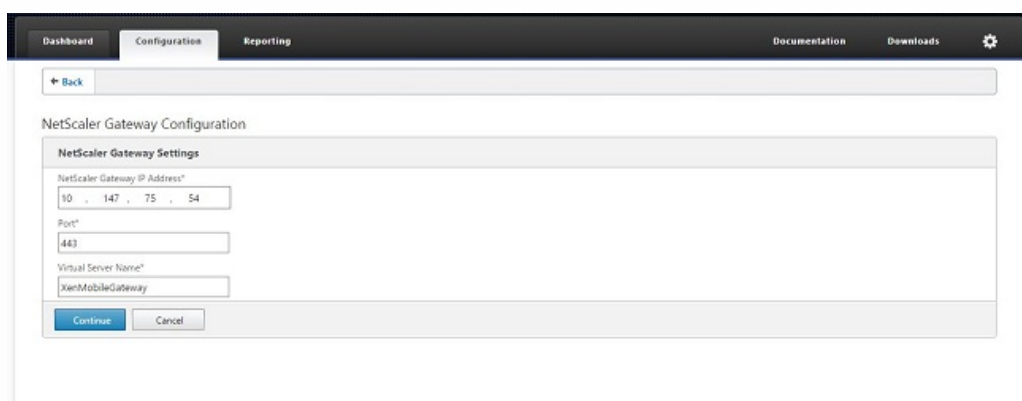
2. [Configuration] タブで [XenMobile] をクリックし、 [Get Started] をクリックします。



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する。
  - [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する。

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一であることを確認してください。

7. [XenMobile settings] の下の [Load Balancing FQDN for MAM] に入力し、[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が同一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クラスターに含まれるXenMobileノードを追加します。追加したすべてのXenMobileノードが表示されます。 [Continue] 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。

XenMobile Servers	
IP Address	Port
10.147.75.51	8443
10.147.75.59	8443

Load Balance Device Manager Servers

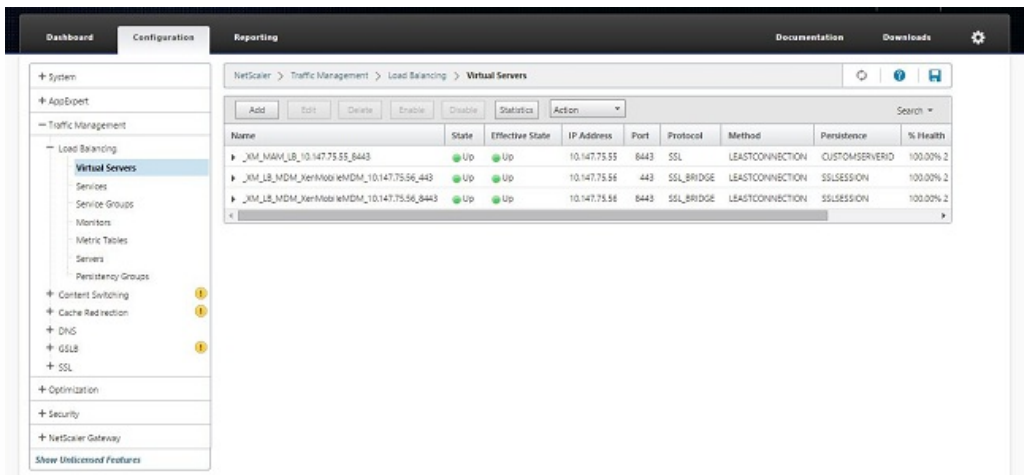
- MDM負荷分散IPアドレス用に使用するIPアドレスを入力し、[Continue] をクリックします。

- 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。

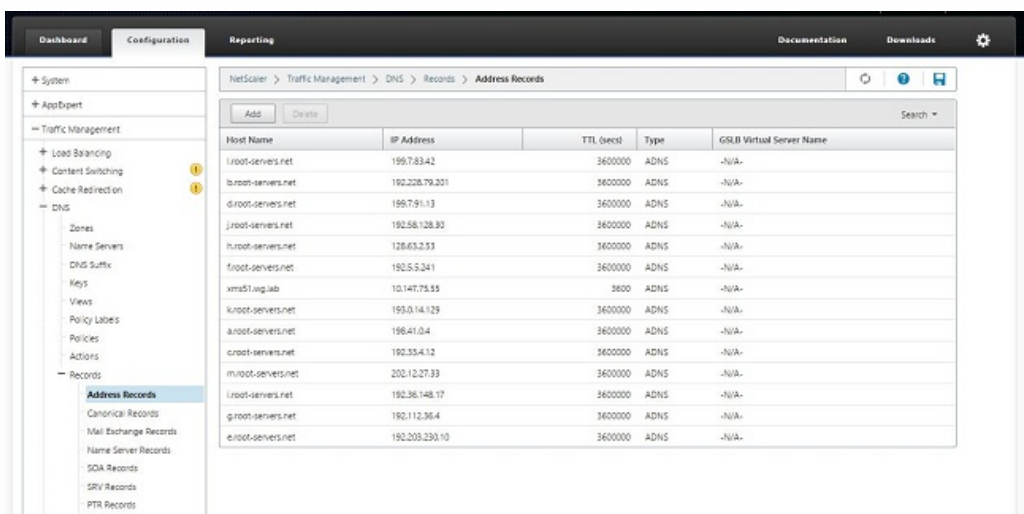
XenMobile Servers	
IP Address	Port
10.147.75.51	443, 8443
10.147.75.59	443, 8443

[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。

- 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。





# 障害回復ガイド

Apr 27, 2017

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

# プロキシサーバーの有効化

Apr 27, 2017

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

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

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] Admin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

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。

```
Choice: [0 - 10] 6
-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
```

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

```

-----
Proxy Configuration Menu
-----
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 1
Enter socks proxy information
Address [1]: 203.0.113.23
Port[1]: 1080
Target - APNS
Proxy configuration updated successfully.
Please restart all nodes in the cluster for the changes to take effect
Are you sure to restart the system? [y/n]: █

```

5. 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。

```
[0] Back to System Menu
[1] SOCKS
[2] HTTPS
[3] HTTP
[4] Exclusion List
[5] Display Configuration
[6] Delete Proxy Configuration
-----
Choice: [0 - 6] 2

Enter https proxy information
Address [1]: 203.0.113.23
Port[1]: 4443
Configure username & password [y/n]: y
Username: Justaname
Password:
Target - WEB
WEB proxy configured. Override proxy settings?[y/n]: █
```

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。

# サーバープロパティ

Apr 27, 2017

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

使用されることが多いプロパティについて詳しくは、XenMobile仮想ハンドブックの [Server Properties](#)」を参照してください。

## サーバープロパティ定義

### Add Device Always

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

### Audit Log Cleanup Execution Time

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

### Audit Log Cleanup Interval (in Days)

XenMobileサーバーが監査ログを保持する日数。デフォルトは**1**です。

### Audit Logger

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

### Audit Log Retention (in Days)

XenMobileサーバーが監査ログを保持する日数。デフォルトは**7**です。

### Certificate Renewal in Seconds

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

### Connection Timeout to Microsoft Certification Server

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

### Deploy Log Cleanup (in Days)

XenMobileサーバーが展開ログを保持する日数。デフォルトは**7**です。

### Disable SSL Server Verification

**True**の場合、次の条件がすべて満たされていると、SSLサーバー証明書確認が無効になります：XenMobileサーバーで証明書ベースの認証を有効にしている、Microsoft CAサーバーが証明書の発行元である、XenMobileサーバーによってルートが信頼されていない内部CAが証明書に署名している。デフォルトは**True**です。

### Enable Console

**True**の場合、自己ヘルプポータルコンソールへのユーザーアクセスが可能になります。デフォルトは**true**です。

### Hibernateによる診断統計ログの有効化/無効化

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

### Enable Notification Trigger

Secure Hubクライアントの通知を有効または無効にします。値**true**は通知を有効にします。デフォルトは**true**です。

### Full Pull of ActiveSync Allowed and Denied Users

ActiveSyncデバイスのベースラインを取得するPowerShellコマンドを実行するときに、XenMobileがドメインからの応答を待機する秒数です。デフォルトは**28800**秒です。

### Identifies if telemetry is enabled or not

利用統計情報（カスタマーエクスペリエンス向上プログラム、すなわちCEIP）が有効かどうかを指定します。XenMobileをインストールするかアップグレードすると、CEIPにオプトインすることができます。XenMobileが15回連続でアップロードに失敗した場合、利用統計情報は無効になります。デフォルトは**false**です。

### Inactivity Timeout in Minutes

**WebServices timeout type**サーバープロパティが**INACTIVITY\_TIMEOUT**の場合、このプロパティは、XenMobileサーバーのパブリックAPIを使用してXenMobileコンソールやサードパーティ製アプリケーションにアクセスした非アクティブな管理者がログアウトされるまでの分数を定義します。タイムアウトが**0**の場合、非アクティブなユーザーはログインしたままになります。デフォルトは**5**です。

### iOS Device Management Enrollment Auto-Install Enabled

**true**の場合、このプロパティはデバイスの登録中に必要なユーザー操作の量を削減します。ユーザーは**[Root CA install]**（必要に応じて）および**[MDM Profile install]**をクリックする必要があります。

### iOS Device Management Enrollment First Step Delayed

ユーザーがデバイス登録中に資格情報を入力すると、このプロパティの値は、ルートCAをインストールするメッセージを表示する前に待機する時間を指定します。ネットワーク遅延またはスピードの問題がない限り、このプロパティを編集しないことをお勧めします。編集する場合は、5000ミリ秒（5秒）を超える値を設定しないでください。デフォルトは**1000**ミリ秒（1秒）です。

### iOS Device Management Enrollment Last Step Delayed

デバイスの登録中、このプロパティの値はMDMプロファイルのインストールからデバイスでエージェントを開始する

までの待機時間を指定します。ネットワーク遅延またはスピードの問題がない限り、このプロパティを編集しないことをお勧めします。編集する場合は、5000ミリ秒（5秒）を超える値を設定しないでください。デフォルトは**1000**ミリ秒（1秒）です。

### iOS Device Management Identity Delivery Mode

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

### iOS Device Management Identity Key Size

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

### iOS Device Management Identity Renewal Days

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

### iOS MDM APNS Private Key Password

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

### iOS MDM APNS Private Key Password

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

### MAM\_MACRO\_SUPPORT

MAM-only展開のXenMobileサーバーを、AndroidまたはiOSデバイスを持ち、電子メール資格情報でSecure Hubに登録するユーザーがSecure Mailに自動的に登録されるように構成します。これは、ユーザーが追加情報を入力する必要がないか、Secure Mailに登録する追加手順を実行する必要がないことを意味します。このカスタムキーを追加し、デフォルト値**True**を使用して、自動電子メール登録を有効化します。クライアントプロパティENABLE\_CREDENTIAL\_STOREおよびSEND\_LDAP\_ATTRIBUTESも必要です。

Secure Mailを初めて使用する場合、Secure MailはSecure Hubからユーザーの電子メールアドレス、ドメインおよびユーザーIDを取得します。Secure Mailは、電子メールアドレスを使用して自動検出します。ドメインとユーザーIDを使用してExchange Serverが識別されます。Exchange Serverによって、Secure Mailのユーザー自動認証が行われます。パスワードをパススルーしないようにポリシーが設定されている場合、ユーザーはパスワードの入力を求められますが、ユーザーは何も追加情報を入力する必要がありません。

### NetScaler Single Sign-On

**False**の場合、NetScalerからXenMobileサーバーへのシングルサインオン実行中にXenMobileコールバック機能が無効にされます。コールバック機能は、NetScaler Gateway構成にコールバックURLが含まれる場合に、NetScaler GatewayセッションIDの確認に使用されます。デフォルトは**False**です。

### Number of consecutive failed uploads

カスタマーエクスペリエンス向上プログラム（CEIP）アップロード中の連続失敗回数を表示します。アップロードが失敗した場合、XenMobileがこの値を増やします。アップロードが15回失敗すると、XenMobileによってCEIP（利用統計

情報)が無効化されます。詳しくは、サーバープロパティ **Identifies if telemetry is enabled or not** を参照してください。アップロードが成功した場合、XenMobileによってこの値は**0**にリセットされます。

### Number of Users Per Device

モバイルデバイス管理 (MDM : Mobile Device Management) に同じデバイスを登録できるユーザーの最大数。この値が**0**の場合、同一デバイスを登録できるユーザー数は無制限です。デフォルトは**10**です。

### Pull of Incremental Change of Allowed and Denied Users

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

### Read Timeout to Microsoft Certification Server

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

### REST Web Services

REST Web Serviceを有効または無効にします。デフォルトは**true**です。

### Session Log Cleanup (in Days)

XenMobileサーバーがセッションログを保持する日数。デフォルトは**7**です。

### サーバーモード

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

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

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

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



サーバーモードは、ライセンスがアクティブ化または削除されるたびに、そしてサーバープロパティでサーバーモードが変更されるときにサーバーログに追加されます。ログファイルの作成と表示については、「[ログ](#)」および「[XenMobileでのログファイルの表示および分析](#)」を参照してください。

## Static Timeout in Minutes

**WebServices timeout type**サーバープロパティが**STATIC\_TIMEOUT**の場合、このプロパティは、XenMobileサーバーのパブリックAPIを使用してXenMobileコンソールやサードパーティ製アプリケーションにアクセスした管理者がログアウトされるまでの分数を定義します。デフォルトは**60**です。

## Trigger Agent Message Suppression

Secure Hubクライアントのメッセージを有効または無効にします。値**false**はメッセージを有効にします。デフォルトは**true**です。

## Trigger Agent Sound Suppression

Secure Hubクライアントのサウンドを有効または無効にします。値**false**はサウンドを有効にします。デフォルトは**true**です。

## Unauthenticated App Download for Android Devices

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

## Unauthenticated App Download for Windows Devices

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

## Use ActiveSync ID to Conduct an ActiveSync Wipe Device

**True**の場合、XenMobile Mail Managerは、ActiveSync識別子をasWipeDeviceメソッドの引数として使用します。デフォルトは**false**です。

## Users only from Exchange

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

## WebServices Timeout Type

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

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

## XAM One-Time Ticket

ワンタイム認証トークン (OTT) がアプリケーションをダウンロードするのに有効なミリ秒の数字です。このプロパティは、未認証のアプリのダウンロードを許可するかを指定するプロパティ**Unauthenticated App download for Android**および**Unauthenticated App download for Windows**とともに使用されます。デフォルトは**3600000**です。

## XenMobile MDM Self Help Portal console max inactive interval (minutes)

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

# サーバープロパティを追加、編集、または削除するには

XenMobileで、サーバーにプロパティを適用できます。変更を行った後、すべてのノードでXenMobileを再起動し、変更を確定して有効化する必要があります。

## 注意

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

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

<input type="checkbox"/>	Display name	Key	Value	Default value	Description
<input type="checkbox"/>	NetScaler Gateway Client Cert Issuing Throttling Interval	ag.client.cert.throttling.minutes	30	30	Throttling interval for issuance of NetScaler Gateway client certificates.
<input type="checkbox"/>	Number of consecutive failed uploads.	ceip.consecutive.upload.failures	0	0	
<input type="checkbox"/>	Sharefile byPath API fields	com.citrix.sharefile.bypath.fields	odata.metadata, id, url	odata.metadata, id, url	Comma separated set of fields (case-sensitive) that need to be extracted from the complete sharefile byPath API response
<input type="checkbox"/>	Sharefile configuration type : ENTERPRISE/CONNECTORS/NONE	com.citrix.sharefile.config.type	ENTERPRISE	NONE	Sharefile configuration type . Possible values being ENTERPRISE or CONNECTORS or NONE
<input type="checkbox"/>	Connection Timeout	CONNECTION_TIMEOUT	5	5	Session inactivity timeout, in minutes, after which the TCP connection to a device will be closed (by default 5 minutes).
<input type="checkbox"/>	Identifies if telemetry is enabled or not.	console.ceip.participate	true	false	
<input type="checkbox"/>	Length of Inactivity Before Device Is Disconnected	device.inactivity.days.threshold	7	7	Length of inactivity (in days) before the device is disconnected.
<input type="checkbox"/>	User-Defined Device Properties 1	device.properties.userDefined1			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 2	device.properties.userDefined2			User-defined device properties.
<input type="checkbox"/>	User-Defined Device Properties 3	device.properties.userDefined3			User-defined device properties.

サーバープロパティを追加するには

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

The screenshot shows the XenMobile interface for adding a new server property. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure', along with a settings icon and a user profile 'admin'. The breadcrumb trail is 'Settings > Server Properties > Add New Server Property'. The main heading is 'Add New Server Property'. The form contains four fields: 'Key' (a dropdown menu with 'Select an option' and a help icon), 'Value\*' (a text input field), 'Display name\*' (a text input field), and 'Description' (a larger text area). At the bottom right, there are 'Cancel' and 'Save' buttons.

2. 次の設定を構成します。

- **キー**：一覧で、適切なキーを選択します。キーでは大文字と小文字が区別されます。変更を行う前にCitrixのサポート担当者にお問い合わせるか、特殊キーを要求する必要があります。

- **値**：選択したキーに応じて値を入力します。
- **表示名**：[サーバープロパティ]の表に表示される、新しいプロパティ値の名前を入力します。
- **説明**：任意で、新しいサーバープロパティの説明を入力します。

3. [Save] をクリックします。

サーバープロパティを編集するには

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

注：サーバープロパティの横にあるチェックボックスをオンにすると、サーバープロパティ一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、項目の右側にオプションメニューが表示されます。

2. [Edit] をクリックします。[Edit New Server Property] ページが開きます。

The screenshot shows the 'Edit New Server Property' page in the XenMobile interface. The breadcrumb trail is 'Settings > Server Properties > Edit New Server Property'. The form contains the following fields:

- Key**: ag.client.cert.throttling.mi
- Value\***: 30
- Display name\***: NetScaler Gateway Client
- Description**: Throttling interval for issuance of NetScaler Gateway client certificates.

At the bottom right, there are 'Cancel' and 'Save' buttons.

3. 必要に応じて以下の情報を変更します。

- **Key**：このフィールドは変更できません。
- **Value**：プロパティの値です。

- **Display Name** : プロパティの名前です。
- **Description** : プロパティの説明です。

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

サーバープロパティを削除するには

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

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

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

# コマンドラインインターフェイスオプション

Apr 27, 2017

以下のように、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。

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

CLIを使用して、さまざまな構成タスクやトラブルシューティングを実行できます。以下は、CLIの第一レベルメニューです。

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

## 構成オプション

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

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

## [1] Network

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

Applying network settings...

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

## [2] Firewall

```
-----
```

```

Configure which services are enabled through the firewall.

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

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

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

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

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

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

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

```

### [3] Database

```

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

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

```

### [4] Listener Ports

```

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

```

## [Clustering] オプション

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

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

### [1] Show Cluster Status

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75  status: ACTIVE  role: OLDEST
node: 10.207.87.77  status: ACTIVE  role: NONE
node: 10.207.87.88  status: ACTIVE  role: NONE
```

### [2] Enable/disable cluster

クラスタリングの有効化を選択すると、次のメッセージが表示されます。

クラスタメンバー間でリアルタイム通信を有効にするには、CLIメニューの [Firewall] オプションでポート80を開きます。また、[Firewall] 設定の [Access white list] でアクセス制限を構成します。

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。

クラスタリングの無効化を選択しました。ポート80へのアクセスは必要ありません。無効にしてください。

### [3] Cluster member white list

```
Current White List:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction

Please enter hosts or networks to be white listed:
```

### [4] Enable or disable SSL offload

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

[Enabling SSL offload] は全ユーザーにポート80を開きます。また、[Firewall] 設定の [Access white list] でアクセス制限を構成します。



## [5] Display Hazelcast Cluster

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

Hazelcast Cluster Members :

[IP addresses listed]

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

[System] オプション

[System] メニューから、さまざまなシステムレベルの情報の表示、サーバーの再起動またはシャットダウン、[Advanced] 設定へのアクセスを実行できます。

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
```

## [12] Advanced Settings

```
***** WARNING *****
Please only modify these options if you are
in contact with Citrix Support
*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] Reset SSL Certificate
[4] Reset pki.xml
[5] Server Tuning
-----
```

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

[Troubleshooting] オプション

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

```
-----  
Troubleshooting Menu  
-----
```

```
[0] Back to Main Menu  
[1] Network Utilities  
[2] Logs  
[3] Support Bundle  
-----
```

### [1] Network Utilities

```
-----  
Network Menu  
-----
```

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

### [2] Logs

```
-----  
Logs Menu  
-----
```

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

### [3] Support Bundle

```
-----  
Support Bundle Menu  
-----
```

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

# XenMobileコンソールの導入ワークフロー

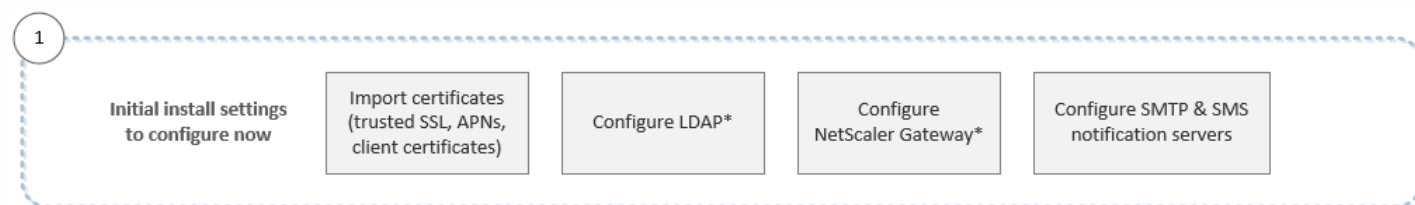
Apr 27, 2017

XenMobileコンソールは、XenMobileの統合管理ツールです。ここでの説明は、XenMobileがインストール済みで、コンソールで作業できる状態になっていることが前提となっています。XenMobileをインストールする必要がある場合は、「[XenMobileのインストール](#)」を参照してください。XenMobileコンソールのブラウザーサポートについて詳しくは、「[XenMobileの互換性](#)」の「[ブラウザーサポート](#)」を参照してください。

## 初期設定のワークフロー

最初にコマンドラインコンソールでXenMobileの構成を完了したら、次にXenMobileコンソールのダッシュボードが開きます。初期構成画面に戻ることはできないため、インストール構成の一部をその時点でスキップした場合は、コンソールで以下の設定を構成できます。ユーザー、アプリケーション、デバイスの追加を開始する前に、これらのインストール設定を完了することを考慮する必要があります。設定を開始するには、コンソールの右上にある歯車アイコンをクリックします。

注：アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントの記事やそのサブ記事を参照してください。

- [認証](#)
- [NetScaler GatewayとXenMobile](#)
- [通知](#)

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

Android :

- Google Play資格情報を作成します。詳しくは、Google Playの[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、「[Android at Work](#)」を参照してください。
- Googleでのドメイン名を検証します。詳しくは、[Verify your domain for 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、[Android for Workのヘルプ](#)を参照してください。

iOS :

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

Windows :

- Microsoft Windowsストア開発者アカウントを作成します。詳しくは、[Microsoft Windows Dev Center](#)を参照してください。
- Microsoft Windowsストア発行元IDを入手します。詳しくは、[Microsoft Windows Dev Center](#)を参照してください。
- Symantecからエンタープライズ証明書を購入します。詳しくは、[Microsoft Windows Dev Center](#)を参照してください。
- Windows Phoneの登録のためにXenMobile自動検出を活用したい場合は、パブリックなSSL証明書を利用できるようにします。詳しくは、「[XenMobile Autodiscoveryサービス](#)」を参照してください。
- アプリケーション登録トークン (AET) を作成します。詳しくは、[Microsoft Windows Dev Center](#)を参照してください。

### コンソールの前提条件のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



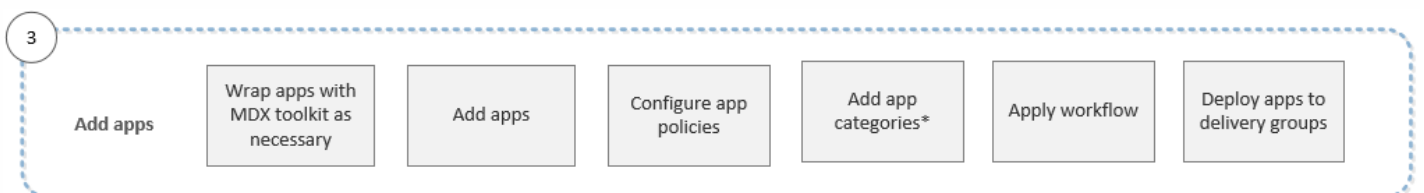
各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントの記事やそのサブ記事を参照してください。

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

### アプリケーションの追加のワークフロー

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

注：アスタリスクが付いている項目はオプションです。



各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントの記事やそのサブ記事を参照してください。

- [MDX Toolkitについて](#)
- [アプリケーションの追加](#)
- [MDXポリシーの概要](#)
- [ワークフローの作成および管理](#)
- [リソースの展開](#)

## デバイスの追加のワークフロー

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

注：アスタリスクが付いている項目はオプションです。

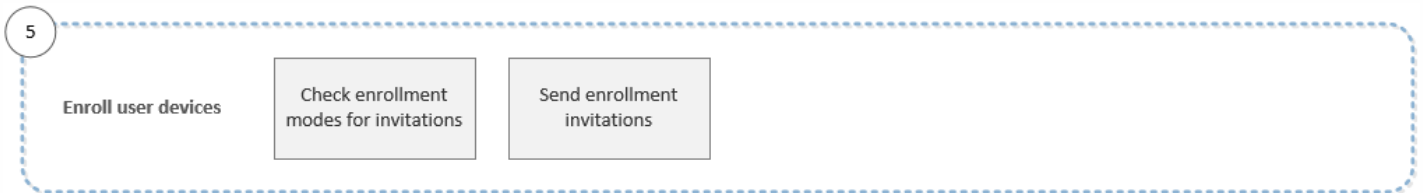


各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントの記事やそのサブ記事を参照してください。

- [デバイス](#)
- [サポート対象のデバイスプラットフォーム](#)
- [リソースの展開](#)
- [モニターとサポート](#)
- [自動化された操作](#)

## ユーザーデバイスの登録のワークフロー

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



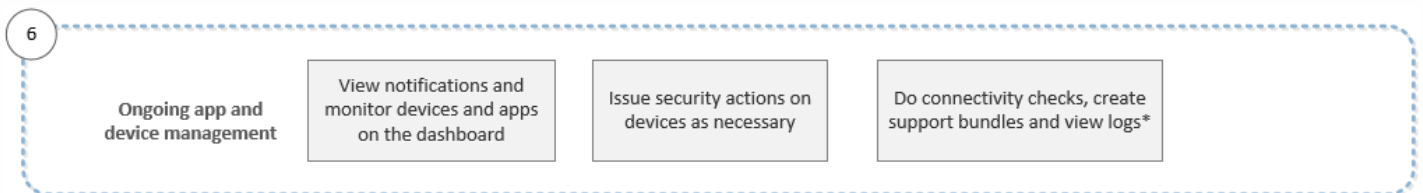
各設定の詳細と具体的な手順については、以下のCitrix製品ドキュメントを参照してください。

- [ユーザーアカウント、役割、および登録](#)
- [通知](#)

## アプリケーションおよびデバイスの継続的な管理のワークフロー

このワークフローでは、コンソールで実行可能であり推奨される、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行います。

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、[モニターとサ](#)

ポート」およびそのサブ記事を参照してください。

# 認証

Apr 27, 2017

XenMobileの動作では、複数のコンポーネントが認証に関与します。

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

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

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

一要素、または二要素による方法の概要など、認証を構成する方法を決定する場合に検討すべき情報について詳しくは、『[Deployment Handbook](#)』の[Authentication](#)に関するトピックを参照してください。

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

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

## 証明書

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

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

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

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

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

XenMobileコンポーネント	証明書の形式	必要な証明書の種類
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL、ルート NetScaler Gatewayによって自動的にPFXがPEMに変換されます。
XenMobileサーバー	.p12 (Windowsベースのコンピューターの.pfx)	SSL、SAML、APNS XenMobileはインストール処理中に完全なPKIも生成します。
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。

### XenMobileでの証明書のアップロード

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

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

### 秘密キーの要件

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



## コンソールへの証明書のアップロード

コンソールに証明書をアップロードする場合、主に2つのオプションがあります。

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

CAが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。

### キーストアをインポートするには

設計上、セキュリティ証明書のリポジトリであるキーストアには、複数のエントリが含まれていることがあります。このため、キーストアから読み込むときに、読み込むエントリを識別するエ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、常に1つだけであるため、キーストアの種類としてPKCS#12を選択した場合、エイリアスフィールドは表示されません。

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

XenMobile Analyze Manage Configure admin

Settings > Certificates

### Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key	▼
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓	
<input type="checkbox"/>	*.agsag.com		⚠ Expired	2013-10-23	2015-10-23	SSL Listener	✓	
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA		
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate		
<input type="checkbox"/>	APSP:3623302e-7c6e-4df8-aa91		🕒 22 days left	2015-09-30	2016-09-29	APNs	✓	

Showing 1 - 5 of 5 items

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

4. 次の設定を構成します。

- **Import** : ボックスの一覧から、 [**Keystore**] を選択します。 [**Import**] ダイアログボックスが、使用可能なキーストアオプションを反映した表示に変わります。

**Import** ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file\***  **Browse**

**Password\***

**Description**

**Cancel** **Import**

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

## 証明書をインポートするには

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

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

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

証明書を最も効率よく更新するには、XenMobileコンソールで右上の歯車アイコンをクリックして**[Settings]** ページを開き、**[Certificates]** をクリックします。**[Import]** ダイアログボックスで、新しい証明書をインポートします。

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

# 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用のSSL証明書

SAML証明書 (ShareFile用)

前記証明書およびその他の内部リソース (StoreFront/Proxyなど) 用のルートおよび中間CA証明書

iOSデバイス管理用のAPNs証明書

XenMobileサーバーのSecure Hub通知用の内部APNs証明書

PKIに接続するためのPKIユーザー証明書

#### **MDX Toolkit**

Apple Developer証明書

Appleプロビジョニングプロファイル (アプリケーションごと)

Apple APNs証明書 (Citrix Secure Mail用)

Android KeyStoreファイル

Windows Phone – Symantec証明書

#### **NetScaler**

MDM FQDN用のSSL証明書

Gateway FQDN用のSSL証明書

ShareFile SZC FQDN用のSSL証明書

Exchangeでの負荷分散用のSSL証明書 (オフロード構成)

StoreFrontでの負荷分散用のSSL証明書

前記証明書用のルートおよび中間CA証明書

#### **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。

#### **Citrix Secure MailのAPN証明書**

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

#### **iOSデバイス管理用のAPN証明書**

XenMobileでiOSデバイスを登録して管理するには、AppleのAPN (Apple Push Notification) サービス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、「[APNs証明書](#)」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。

よろしくお願いたします。

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。

有効なiOS配布証明書があるかを確認するには、以下の操作を行います。

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

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

1. XenMobileコンソールで、**[Settings]**、**[Certificates]** の順にクリックします。
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、Storeへの登録やアクセス、Secure Mail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用のSSL証明書

Gateway FQDN用のSSL証明書

ShareFile SZC FQDN用のSSL証明書

Exchangeでの負荷分散用のSSL証明書（オフロード構成）

StoreFrontでの負荷分散用のSSL証明書

前記証明書用のルートおよび中間CA証明書

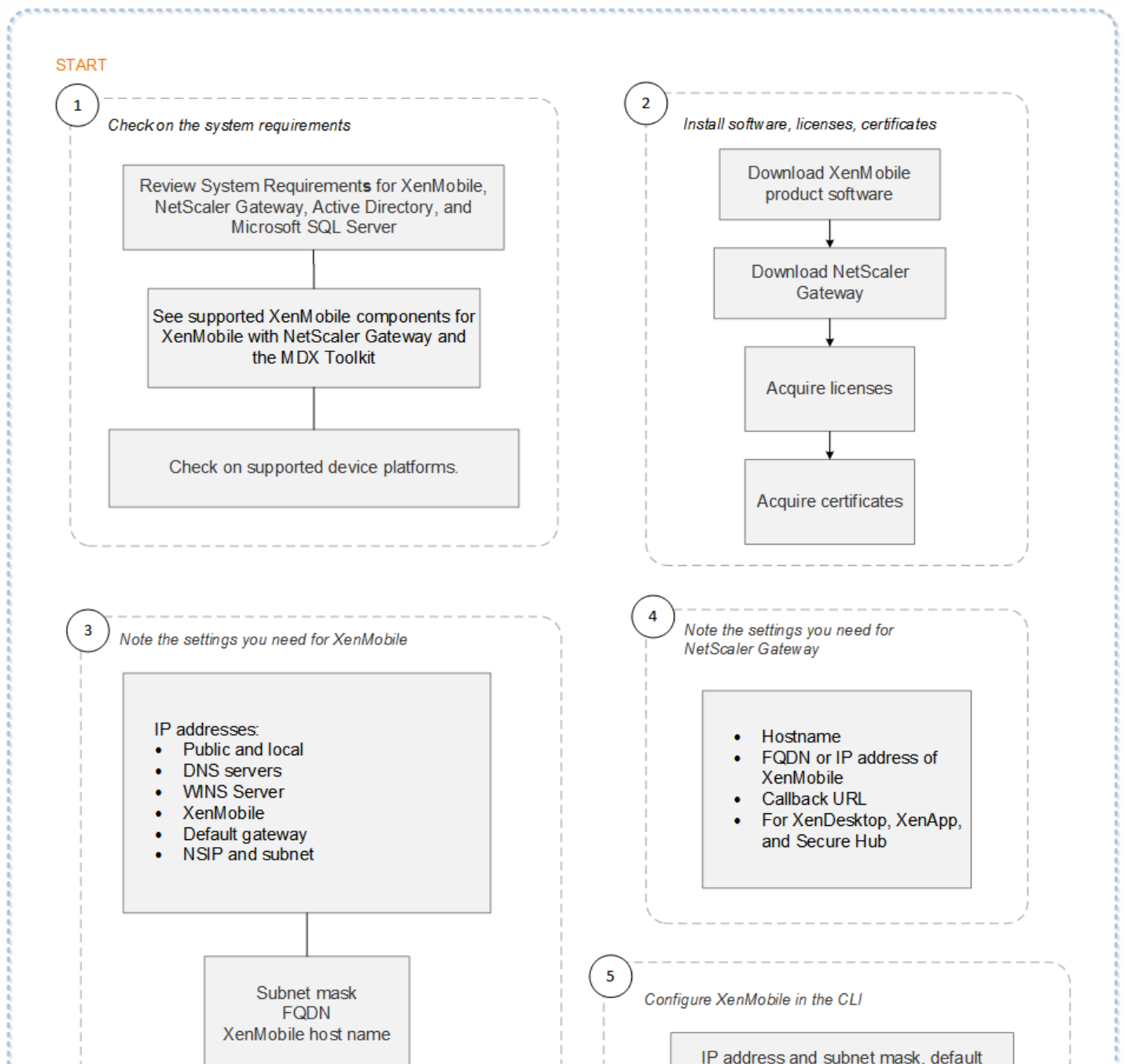
# NetScaler GatewayとXenMobile

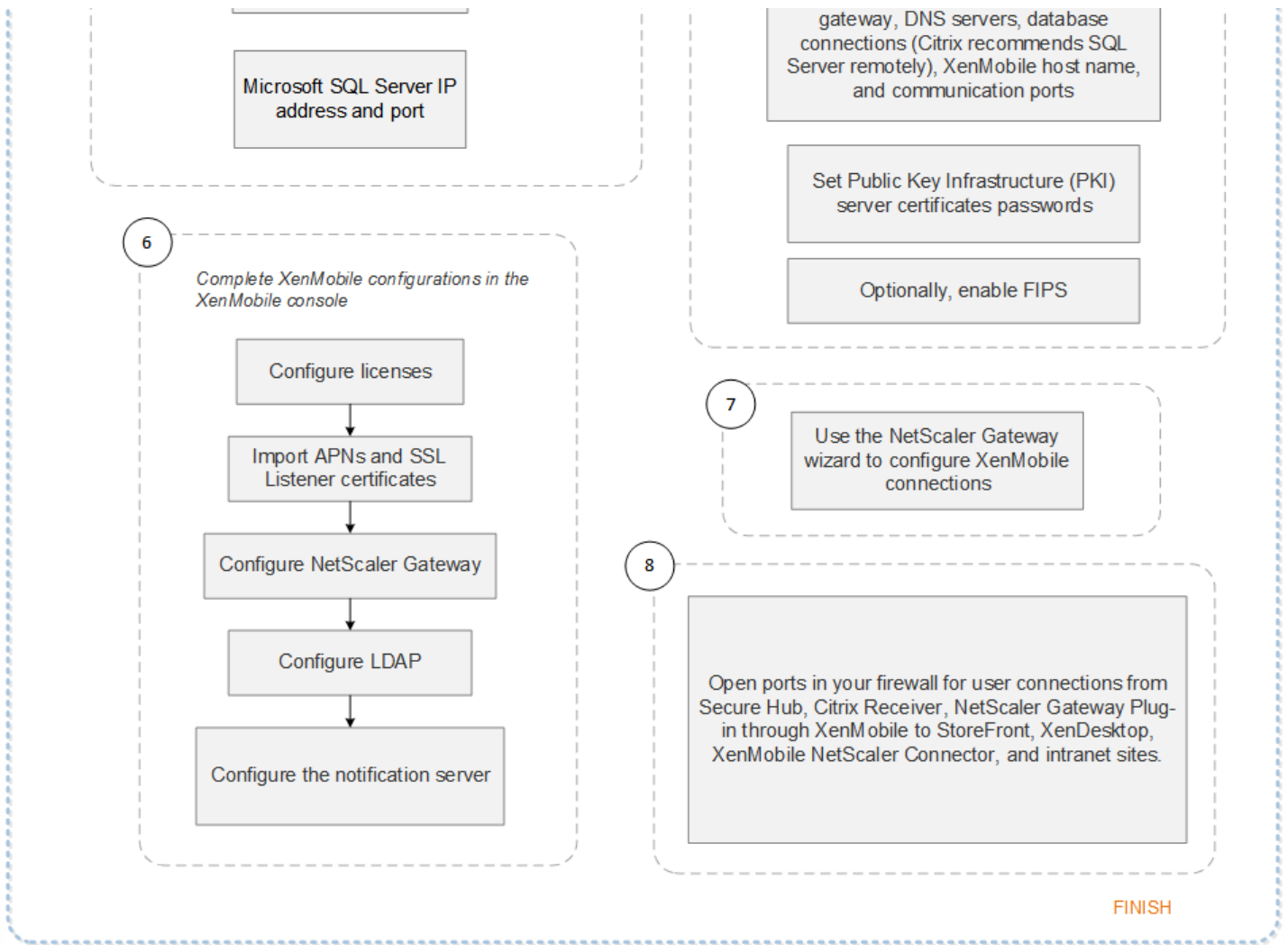
Apr 27, 2017

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、この記事の説明に従って、XenMobileコンソールで行います。

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

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





1

- システム要件と互換性

2

- インストールと構成

3

- インストール前チェックリスト

4



- インストール前チェックリスト

5

- コマンドプロンプトウィンドウでのXenMobileの構成

6

- WebブラウザでのXenMobileの構成

7

- XenMobile環境の設定の構成

8

- ポート

このフローチャートは、PDF形式でも入手できます。

 [XenMobile展開のフローチャート](#)

NetScaler Gatewayを構成するには

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

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway

## NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication  ON

Deliver user certificate for authentication  OFF ?

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs	▼
<input type="checkbox"/>	ag186	<input checked="" type="checkbox"/>	https://mb186.agsag.com	Domain	0	
<input type="checkbox"/>	agdumy	<input type="checkbox"/>	https://10.199.225.200	Domain	0	

Showing 1 - 2 of 2 items

次の設定を構成します。

- **Authentication** : 暗号化を有効にするかどうかを選択します。デフォルトは **[ON]** です。
- **Deliver user certificate for authentication** : XenMobileでSecure Hubと認証証明書を共有し、NetScaler Gatewayでクライアント証明書認証を処理できるようにするかどうかを選択します。デフォルトは **[OFF]** です。
- **Credential Provider** : ボックスの一覧で、使用する資格情報プロバイダーを選択します。詳しくは、[資格情報プロバイダー](#)を参照してください。

6. **[Save]** をクリックします。

新しいNetScaler Gatewayインスタンスを追加するには

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

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway > Add New NetScaler Gateway

### Add New NetScaler Gateway

Name\*

Alias

External URL\*

Logon Type

Password Required

Set as Default

Callback URL*	Virtual IP*	<input type="button" value="Add"/>
---------------	-------------	------------------------------------

4. 次の設定を構成します。

- **[Name]** : NetScaler Gatewayインスタンスの名前を入力します。
- **[Alias]** : 任意で、エイリアスを入力します。
- **External URL** : NetScaler Gatewayの、パブリックにアクセスできるURLを入力します。たとえば、https://receiver.com などです。
- **Logon type** : 一覧から、ログオンの種類を選択します。種類には、**[Domain only]**、**[Security token only]**、**[Domain and security token]**、**[Certificate]**、**[Certificate and domain]**、**[Certificate and security token]** があります。デフォルトは **[Domain only]** です。

複数のドメインを使用している場合、**[Domain only]** は無効です。**[Certificate and domain]** を使用する必要があります。**[Domain only]** など一部のオプションでは、**[Password]** フィールドを変更できません。

このログオンの種類の場合、このフィールドは常に **[ON]** です。また、**[Password Required]** フィールドのデフォルト値は、選択した **[Logon Type]** に基づいて変化します。

**[Certificate and security token]** を使用する場合、NetScaler GatewayでSecure Hubがサポートされるようにするには、追加の設定が必要となります。詳しくは、「[Configuring XenMobile for Certificate and Security Token Authentication](#)」を参照してください。

- **Password Required** : パスワード認証を必須にするかどうかを選択します。デフォルトは **[ON]** です。
- **Set as Default** : このNetScaler Gatewayをデフォルトとして使用するかどうかを選択します。デフォルトは **[OFF]** です。

5. **[Save]** をクリックします。新しいNetScaler Gatewayが追加され、表に表示されます。表で名前をクリックして、イン

スタンスを編集または削除できます。

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

1. [NetScaler Gateway] 画面の表でNetScaler Gatewayを選択し、**[Add]** をクリックします。**[Add New NetScaler Gateway]** ページが開きます。
2. コールバックURLが一覧表示されている表で、**[Add]** をクリックします。
3. コールバックURLを指定します。このフィールドは完全修飾ドメイン名 (FQDN) を表し、要求元がNetScaler Gatewayであることを検証します。コールバックURLは、XenMobileサーバーから接続できるIPアドレスに解決する必要がありますが、外部NetScaler Gateway URLである必要はありません。
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。

# ドメインまたはドメイン+セキュリティトークン認証

Apr 27, 2017

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

LDAPは、オープンソースで特定のベンダーに依存しないアプリケーションプロトコルであり、インターネットプロトコル (IP) ネットワーク経由で分散ディレクトリ情報サービスへのアクセスや管理を行うためのものです。ディレクトリ情報サービスは、ネットワークで使用可能な、ユーザー、システム、ネットワーク、サービス、およびアプリケーションに関する情報を共有するために使用されます。LDAPは一般的に、シングルサインオン (SSO) をユーザーに提供するために利用されます。SSOでは (ユーザーごとに) 1つのパスワードを複数のサービスで共有します。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。

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セッションを開きます。次に、クライアントは操作要求をサーバーに送信し、サーバーは適切な認証で応答します。

XenMobileでLDAP接続を追加するには

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Server] の下の [LDAP] をクリックします。[LDAP] ページが開きます。このページでは、LDAP準拠のディレクトリを [Add]、[Edit]、[Delete] することができます。

The screenshot shows the XenMobile configuration interface for LDAP. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure. On the right, there is a gear icon and a user profile 'admin'. Below the navigation, the breadcrumb is 'Settings > LDAP'. The main heading is 'LDAP' with a sub-heading: 'Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.' There is a toggle for 'Support nested groups' set to 'NO'. Below this is an 'Add' button with a plus icon. A table lists the configured LDAP directory:

<input type="checkbox"/>	Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default	
<input type="checkbox"/>	Microsoft Active Directory	agsag.com	10.199.225.101:389	dc=agsag,dc=com	dc=agsag,dc=com	✓	▼

Showing 1 - 1 of 1 items

LDAP準拠のディレクトリを追加するには

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

Settings &gt; LDAP &gt; Add LDAP

## Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	<input type="text" value="Microsoft Active Directory"/>	?
Primary server*	<input type="text" value="IP Address or FQDN"/>	
Secondary server	<input type="text" value="IP Address or FQDN"/>	
Port*	<input type="text" value="389"/>	
Domain name*	<input type="text"/>	
User base DN*	<input type="text" value="dc=example,dc=com"/>	?
Group base DN*	<input type="text" value="dc=example,dc=com"/>	?
User ID*	<input type="text"/>	
Password*	<input type="password"/>	
Domain alias*	<input type="text"/>	
XenMobile Lockout Limit	<input type="text" value="0"/>	?
XenMobile Lockout Time	<input type="text" value="1"/>	?
Global Catalog TCP Port	<input type="text" value="3268"/>	?
Global Catalog Root Context	<input type="text" value="dc=example,dc=com"/>	?
User search by	<input type="text" value="userPrincipalName"/>	
Use secure connection	<input type="radio" value="NO"/>	

Cancel

Save

2. 次の設定を構成します。

- **Directory type** : 一覧から、適切なディレクトリの種類を選択します。デフォルトは [Microsoft Active Directory] です。
- **Primary server** : LDAPで使用するプライマリサーバーを入力します。IPアドレスまたは完全修飾ドメイン名 (FQDN) を入力できます。
- **Secondary server** : セカンダリサーバーが構成されている場合、任意でセカンダリサーバーのIPアドレスまたはFQDNを入力します。このサーバーは、プライマリサーバーが使用できない場合に使用するフェイルオーバーサーバーです。

- **Port** : LDAPサーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていないLDAP接続用のポート番号389に設定されています。セキュリティ保護されたLDAP接続ではポート番号636、Microsoftのセキュリティ保護されていないLDAP接続では3268、Microsoftのセキュリティ保護されたLDAP接続では3269を使用します。
- **Domain name** : ドメイン名を入力します。
- **User base DN** : Active Directory内でのユーザーの位置を一意的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** : Active Directoryのグループの場所を入力します。たとえば、cn=users、c=domain、dc=netの場合、cn=usersはグループのコンテナ名でdcはActive Directoryのドメインコンポーネントです。
- **User ID** : Active Directoryアカウントに関連付けられたユーザーIDを入力します。
- **Password** : ユーザーに関連付けられたパスワードを入力します。
- **Domain alias** : ドメイン名のエイリアスを入力します。
- **XenMobile Lockout Limit** : ログオンの試行失敗回数として、0~999の数値を入力します。このフィールドを「0」に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
- **XenMobile Lockout Time** : ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、0~99999の数値を入力します。このフィールドを「0」に設定すると、ロックアウト後にユーザーが待機する必要はなくなります。
- **Global Catalog TCP Port** : グローバルカタログサーバーのTCPポート番号を入力します。デフォルトでは、TCPポート番号は3268に設定されています。SSL接続では、ポート番号3269を使用します。
- **Global Catalog Root Context** : 任意で、Active Directoryでのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準のLDAP検索に加えて、実際のドメイン名を指定することなく任意のドメインを検索できます。
- **User search by** : 一覧から、[userPrincipalName] または [sAMAccountName] を選択します。デフォルトは [userPrincipalName] です。
- **Use secure connection** : セキュリティ保護された接続を使用するかどうかを選択します。デフォルトは[NO] です。

3. [Save] をクリックします。

LDAP準拠のディレクトリを編集するには

1. [LDAP] の表で、編集するディレクトリ選択します。

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

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

Settings > LDAP > Add LDAP

### Edit LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	10.61	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	.net	
User base DN*	dc=.dc=.net	ⓘ
Group base DN*	dc=.dc=.net	ⓘ
User ID*	administrator@.net	
Password*		
Domain alias*	.net	
XenMobile Lockout Limit	0	ⓘ
XenMobile Lockout Time	1	ⓘ
Global Catalog TCP Port	3268	ⓘ
Global Catalog Root Context	dc=example,dc=com	ⓘ
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

3. 必要に応じて以下の情報を変更します。

- **Directory type** : 一覧から、適切なディレクトリの種類を選択します。
- **Primary server** : LDAPで使用するプライマリサーバーを入力します。IPアドレスまたは完全修飾ドメイン名 (FQDN) を入力できます。
- **Secondary server** : 任意で、セカンダリサーバーのIPアドレスまたはFQDNを入力します (構成されている場合)。
- **Port** : LDAPサーバーで使用するポート番号を入力します。デフォルトでは、セキュリティ保護されていないLDAP接続用のポート番号389に設定されています。セキュリティ保護されたLDAP接続ではポート番号636、Microsoftのセキュリティ保護されていないLDAP接続では3268、Microsoftのセキュリティ保護されたLDAP接続では3269を使用します。
- **Domain name** : このフィールドは変更できません。
- **User base DN** : Active Directory内でのユーザーの位置を一意的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servernameは、Active Directoryを実行しているサーバーの名前を表します。
- **User ID** : Active Directoryアカウントに関連付けられたユーザーIDを入力します。
- **Password** : ユーザーに関連付けられたパスワードを入力します。
- **Domain alias** : ドメイン名のエイリアスを入力します。
- **XenMobile Lockout Limit** : ログオンの試行失敗回数として、0~999の数値を入力します。このフィールドを「0」に設定すると、ユーザーがログオンの試行失敗によってロックアウトされることはなくなります。
- **XenMobile Lockout Time** : ロックアウト制限を超えた後にユーザーが待機する必要がある分数を表す、0~99999の数値を入力します。このフィールドを「0」に設定すると、ロックアウト後にユーザーが待機する必要はなくなります。
- **Global Catalog TCP Port** : グローバルカタログサーバーのTCPポート番号を入力します。デフォルトでは、TCPポート番号は3268に設定されています。SSL接続では、ポート番号3269を使用します。
- **Global Catalog Root Context** : 任意で、Active Directoryでのグローバルカタログ検索を有効にしたときに使用する、グローバルルートコンテキスト値を入力します。この検索では、標準のLDAP検索に加えて、実際のドメイン名を指定するこ



となく任意のドメインを検索できます。

- **User search by** : 一覧から、 [userPrincipalName] または [sAMAccountName] を選択します。
- **Use secure connection** : セキュリティ保護された接続を使用するかどうかを選択します。

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

LDAP準拠のディレクトリを削除するには

1. [LDAP] の表で、削除するデバイスを選択します。

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

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

## ドメイン+セキュリティトークン認証の構成

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

ユーザービリティを最適化するためにこの構成をCitrix PINおよびActive Directoryパスワードキャッシュと組み合わせて、ユーザーがActive Directoryのユーザー名とパスワードを繰り返し入力する必要がないようにすることができます。登録、パスワード失効、およびアカウントのロックアウトの場合は、ユーザー名とパスワードを入力する必要があります。

LDAP設定の構成

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

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

The screenshot shows the XenMobile configuration page for LDAP. The 'Support nested groups' toggle is set to 'NO'. Below this, there are icons for 'Add', 'Edit', and 'Delete'. A table lists the configured LDAP directory:

Directory Type	Domain Name	Server:Port	User Base DN	Group Base DN	Default
<input checked="" type="checkbox"/> Microsoft Active Directory	xmlab.net	10.207.86.51:389	dc=xmlab,dc=net	dc=xmlab,dc=net	<input checked="" type="checkbox"/>

3. [Port] が636であることを確認します (セキュリティで保護されたLDAP接続の場合)。セキュリティで保護されたMicrosoft LDAP接続の場合は3269です。

4. [Use secure connection] を [Yes] に変更します。

XenMobile Analyze Manage Configure admin

Port\* 636

Domain name\* .net

User base DN\* dc=.net

Group base DN\* dc=.net

User ID\* administrator@.net

Password\*

Domain alias\* .net

XenMobile Lockout Limit 0

XenMobile Lockout Time 1

Global Catalog TCP Port 3269

Global Catalog Root Context dc=example,dc=com

User search by userPrincipalName

Use secure connection

Cancel Save

## NetScaler Gateway設定の構成

次の手順では、NetScaler GatewayインスタンスをすでにXenMobileに追加してあると想定しています。NetScaler Gatewayインスタンスを追加するには、「[新しいNetScaler Gatewayインスタンスを構成するには](#)」を参照してください。

1. [Settings] で [NetScaler Gateway] をクリックします。
2. [NetScaler Gateway] を選択して [編集] をクリックします。
3. [Logon Type] で [Domain and security token] を選択します。

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway > Add New NetScaler Gateway

### Add New NetScaler Gateway

Name\* THAG

Alias

External URL\* https://ag-bm1.xs.citrix.com

Logon Type Domain and security token

Password Required

Set as Default

Callback URL*	Virtual IP*	Add
---------------	-------------	-----

Cancel Save

## Worx PINとユーザーパスワードキャッシュの有効化

Worx PINとユーザーパスワードキャッシュを有効化するには、**[Settings] > [Client Properties]** に移動し、チェックボックス **[Enable Worx PIN Authentication]** および **[Enable User Password Caching]** を選択します。詳しくは、「[クライアントプロパティ](#)」を参照してください。

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

NetScaler Gatewayセッションのプロファイルおよびポリシーを、XenMobileで使用される仮想サーバー用に構成します。詳しくは、NetScaler Gatewayのドキュメントの「[Configuring Domain and Security Token Authentication for XenMobile](#)」を参照してください。

# クライアント証明書、または証明書とドメイン認証の組み合わせ

Apr 27, 2017

XenMobileのデフォルト構成は、ユーザー名とパスワードによる認証です。登録およびXenMobile環境へのアクセスのセキュリティを強化するには、証明書ベースの認証の使用を考慮してください。XenMobile環境では、この構成が、最適なSSO機能とNetScalerでの2要素認証によって提供されるセキュリティが結びついている、セキュリティおよびユーザーエクスペリエンスの最高の組み合わせです。

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

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

非常にセキュアな環境で、パブリックまたはセキュリティが確保されていないネットワークでの組織外のLDAP資格情報の使用が組織に対する主要なセキュリティの脅威とみなされる場合には、クライアント証明書とセキュリティトークンを使用する2要素認証が選択肢になります。詳しくは、「[Configuring XenMobile for Certificate and Security Token Authentication](#)」を参照してください。

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

## Microsoftサーバーの場合

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

## XenMobileサーバーの場合

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

NetScaler Gatewayで、NetScaler Gatewayドキュメントの「[Configuring Client Certificate or Client Certificate and Domain Authentication](#)」の説明に従って構成します。

## 前提条件

- クライアント証明書認証およびSSL Offloadを使用するWindows Phone 8.1デバイスの場合、NetScaler内の両方の負荷分散仮想サーバー上のポート443に対するSSLセッション再利用を無効にする必要があります。そうするには、vserver上でポー

ト443に対して次のコマンドを実行します。

```
set ssl vserver sessReuse DISABLE
```

注：SSLセッション再利用を無効にすると、NetScalerで提供される最適化の一部が無効になり、NetScaler上のパフォーマンスが低下することがあります。

- Exchange ActiveSyncに対して証明書ベースの認証を構成するには、この[Microsoftのブログ](#)を参照してください。
- プライベートサーバー証明書を使用してExchange ServerへのActiveSyncトラフィックを保護する場合は、モバイルデバイスがすべてのルート証明書および中間証明書を持っていることを確認してください。これらの証明書がない場合、Secure Mailでのメールボックス設定時に、証明書ベースの認証が失敗します。Exchange IIS Consoleコンソールでは、次のことが必要です。
  - XenMobileをExchangeと使用するためのWebサイトを追加し、Webサーバー証明書をバインドします。
  - ポート9443を使用します。
  - そのWebサイトに対して、Microsoft-Server-ActiveSync用とEWS用に、2つのアプリケーションを追加する必要があります。それらの両方のアプリケーションに対して、[SSL Settings] で [Require SSL] を選択します。
- 最新のMDX Toolkitを使用してiOS、AndroidおよびWindows Phone用のSecure Mailがラップされていることを確認します。

## 証明書のスナップインのMicrosoft管理コンソールへの追加

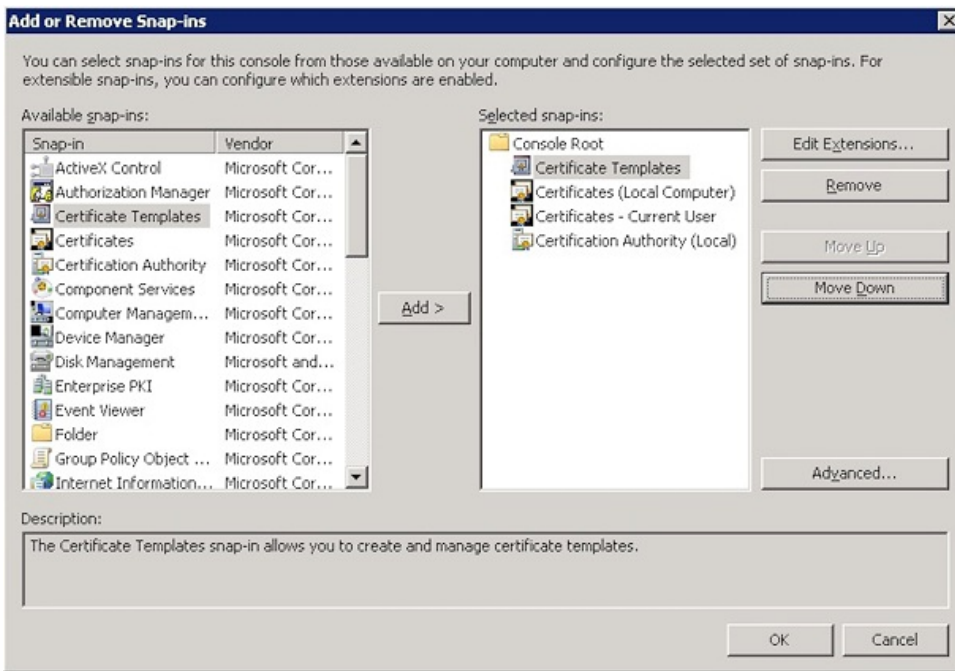
1. コンソールを開いて、[Add/Remove Snap-Ins] をクリックします。
2. 次のスナップインを追加します。

証明書テンプレート

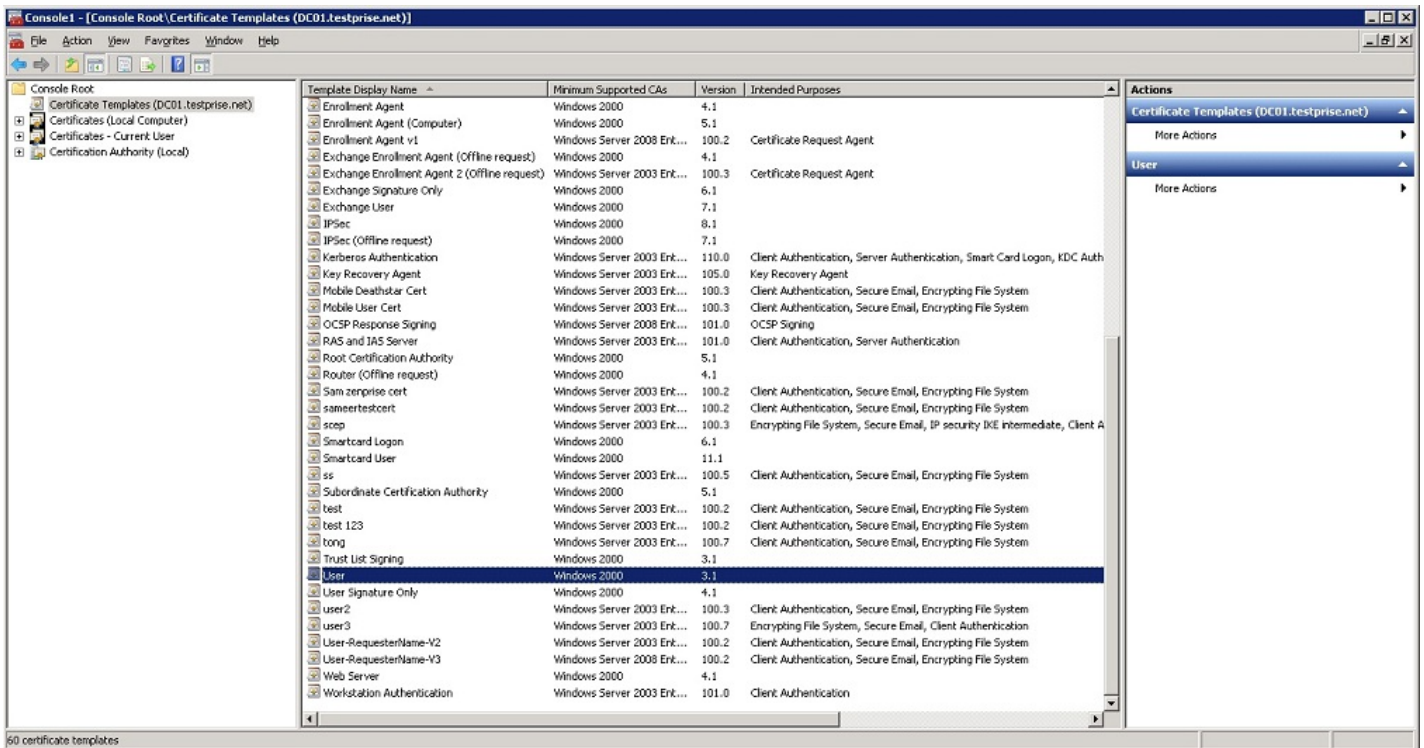
証明書 (ローカルコンピューター)

証明書 - 現在のユーザー

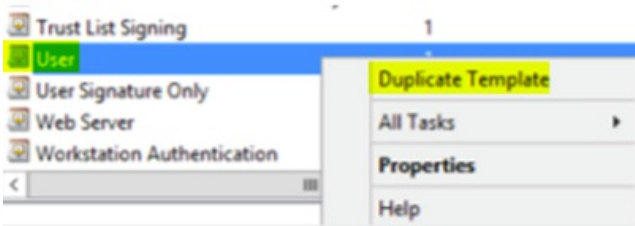
証明機関 (ローカル)



3. [証明書テンプレート] を展開します。



4. [ユーザー] テンプレートと [テンプレートの複製] を選択します。

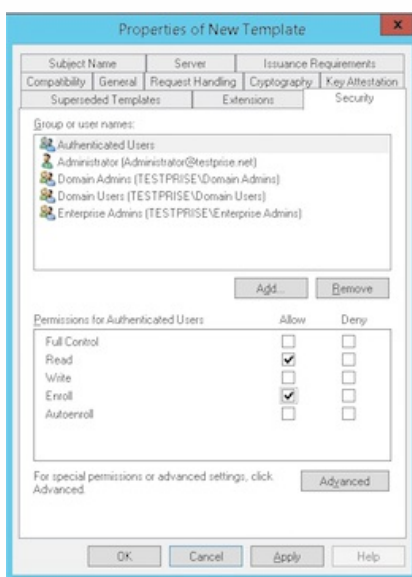


5. [テンプレート] の表示名を入力します。

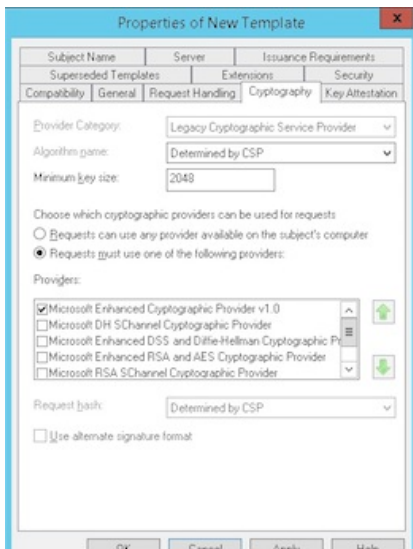
**重要**：必要な場合以外は、[Active Directoryの証明書を発行する] チェックボックスを選択しないでください。このオプションが選択されると、すべてのユーザークライアント証明書がActive Directoryで発行/作成され、Active Directory データベースを圧迫する可能性があります。

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

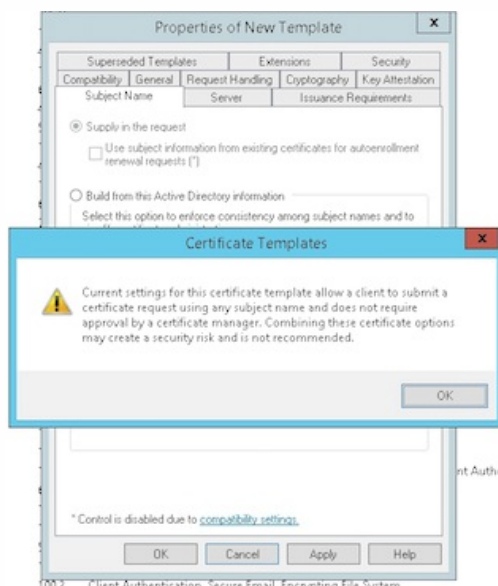
7. [セキュリティ] で、認証ユーザーの [許可] 列の [登録] オプションを選択します。



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



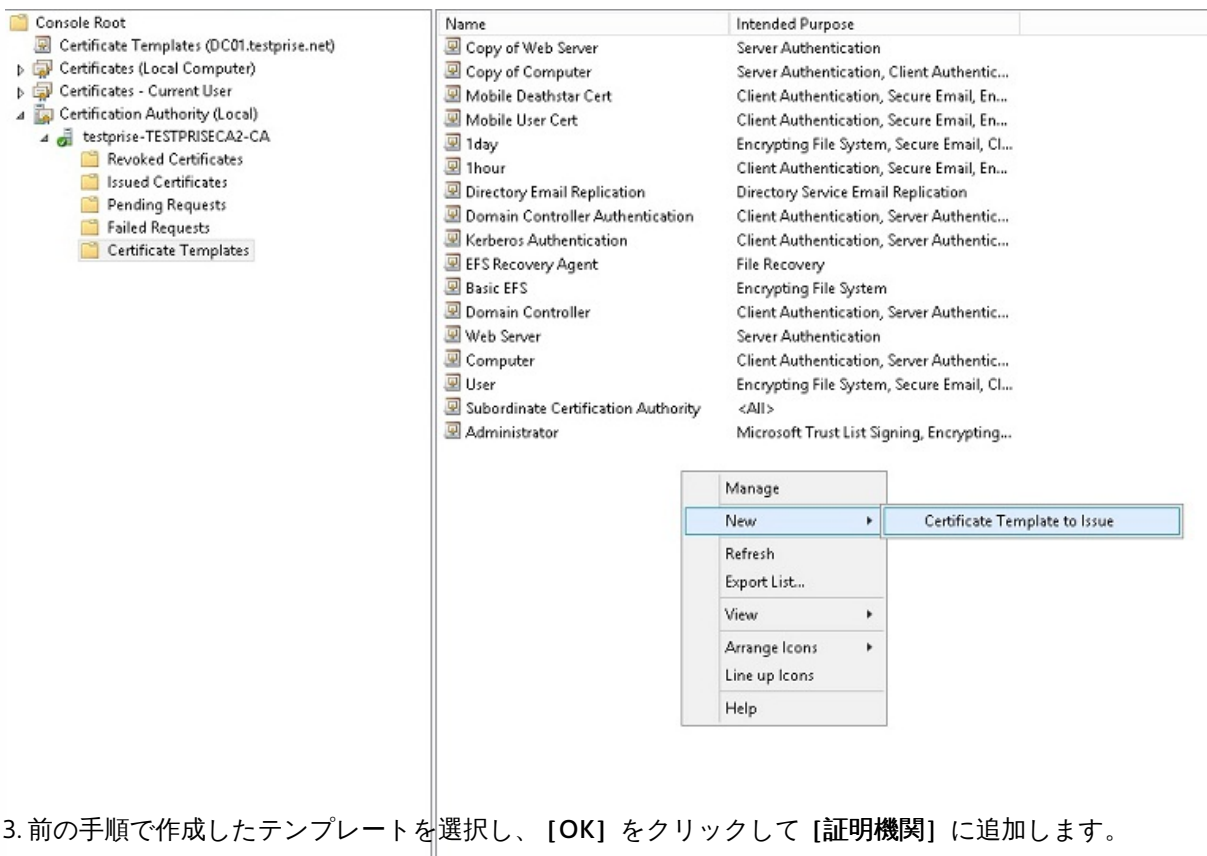
9. [サブジェクト名] で、[要求に含まれる] を選択します。変更を適用して、保存します。



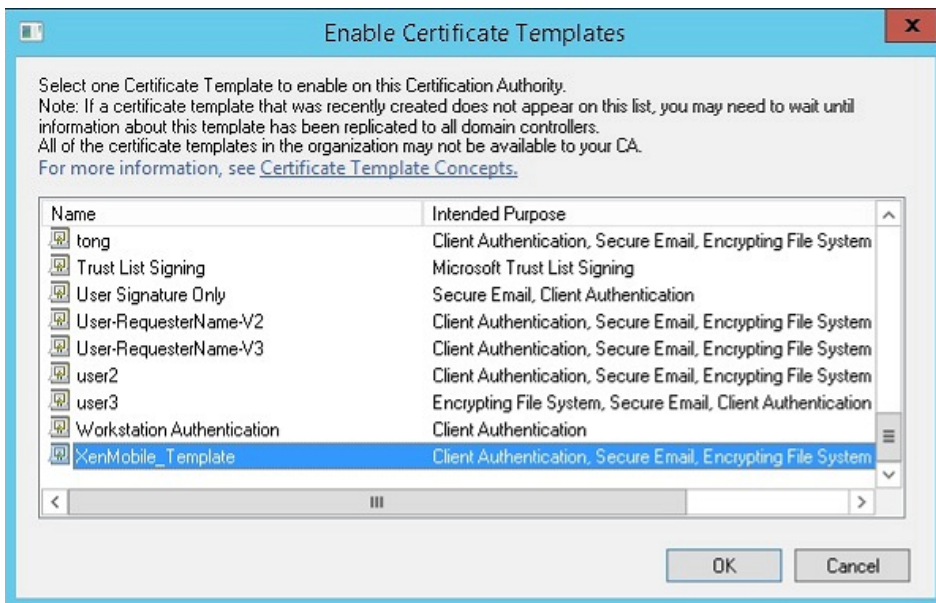
## 証明機関 (CA) へのテンプレートの追加

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





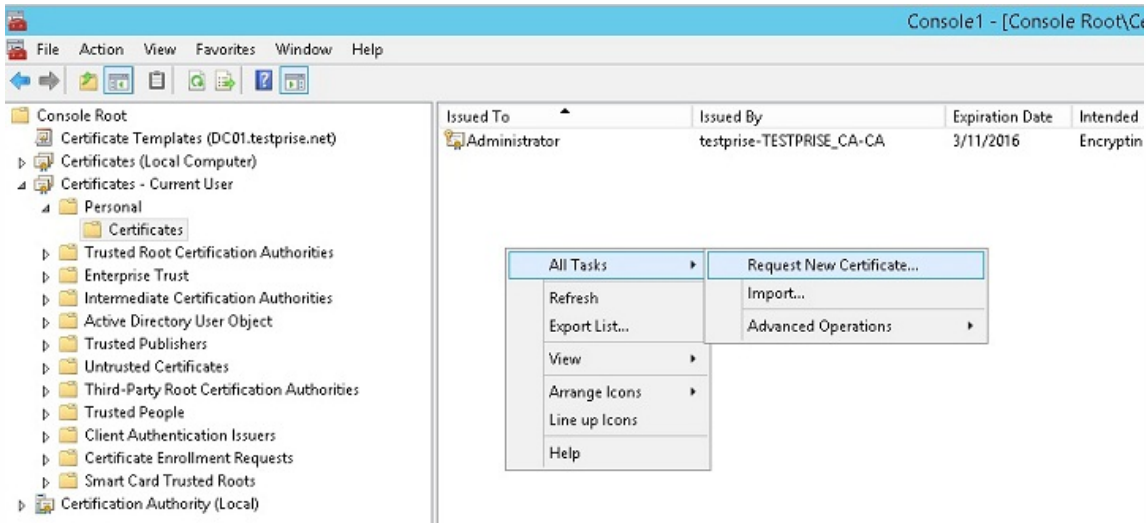
3. 前の手順で作成したテンプレートを**選択**し、**[OK]** をクリックして **[証明機関]** に追加します。



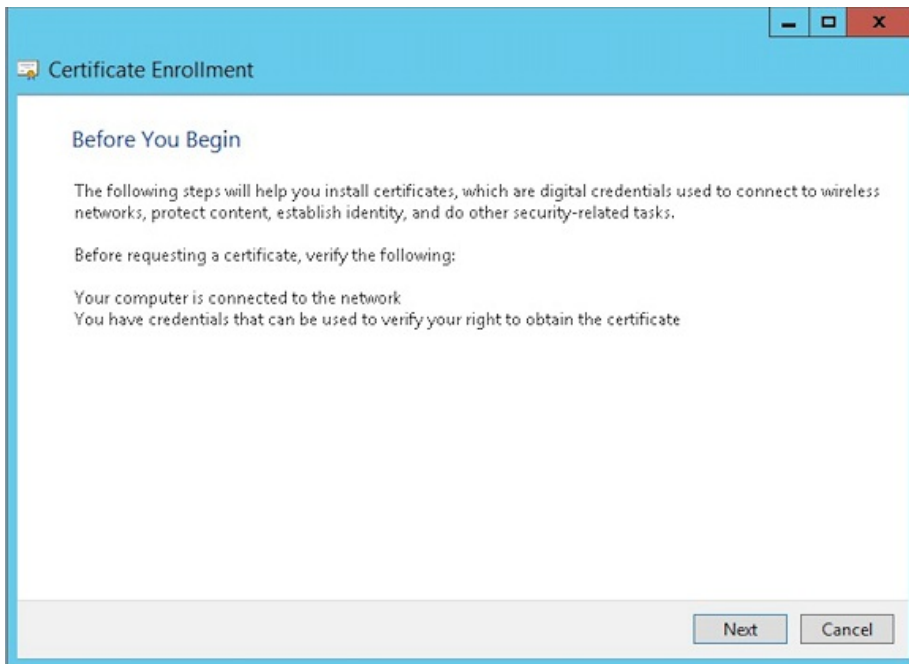
## CAサーバーからのPFX証明書の作成

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

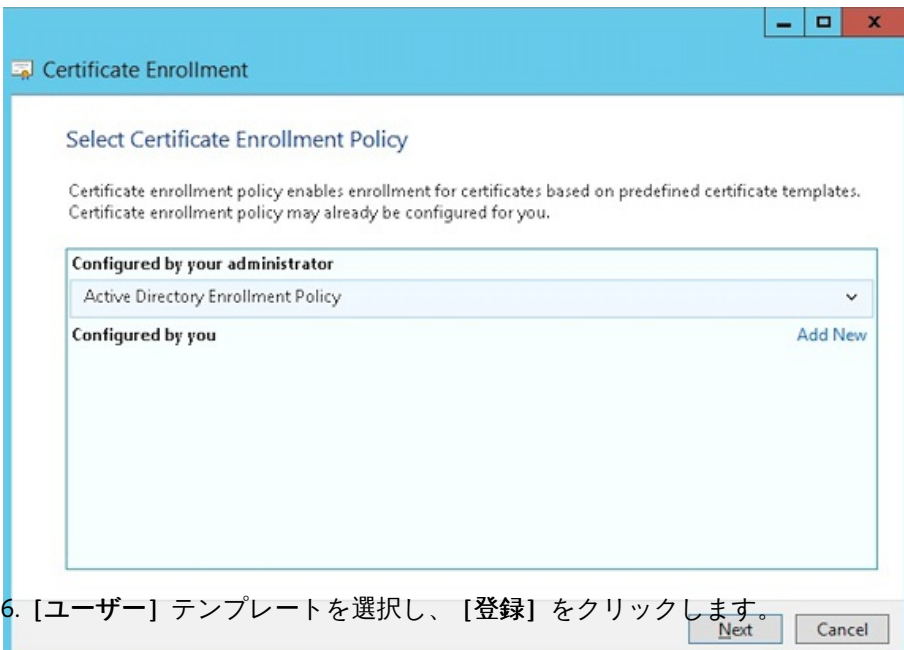
3. 右ペインで右クリックし、[新しい証明書の要求] をクリックします。



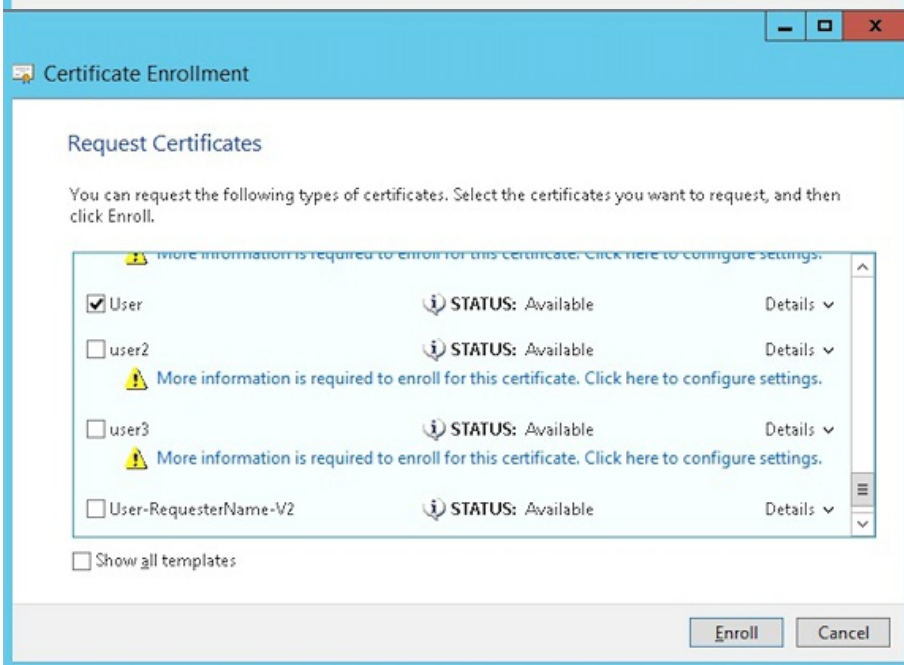
4. [証明書の登録] 画面が開きます。[次へ] をクリックします。



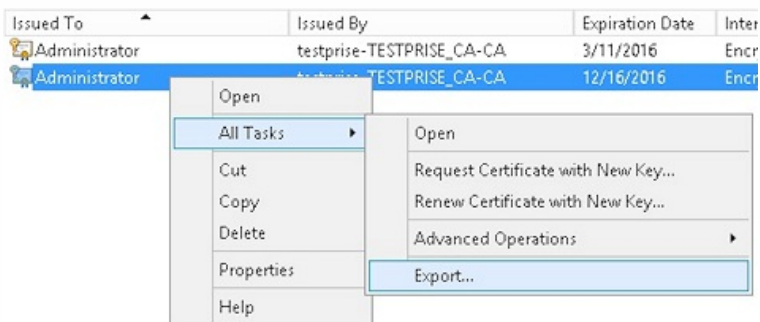
5. [Active Directory登録ポリシー] を選択して [次へ] をクリックします。



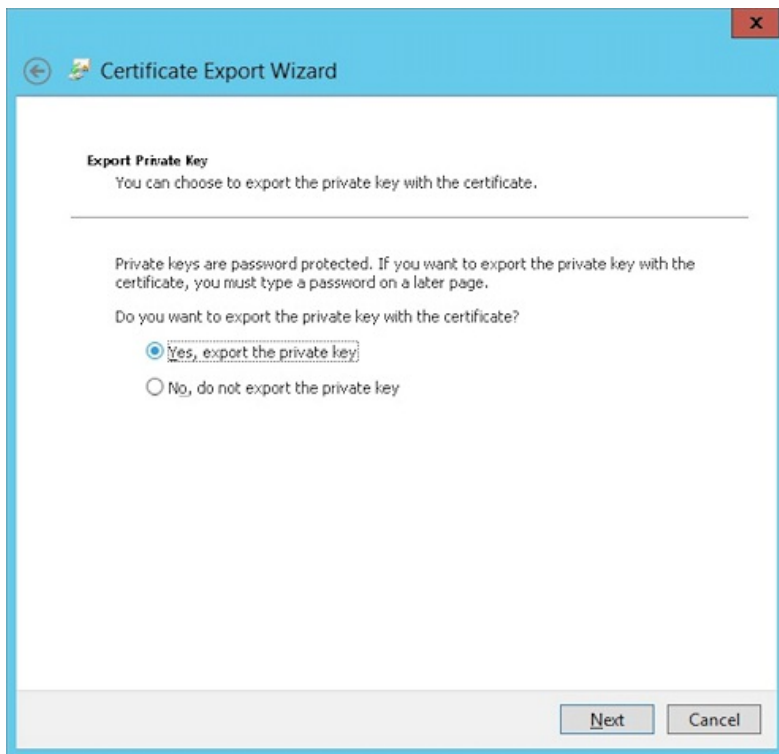
6. [ユーザー] テンプレートを選択し、[登録] をクリックします。



7. 前の手順で作成した.pfxファイルをエクスポートします。



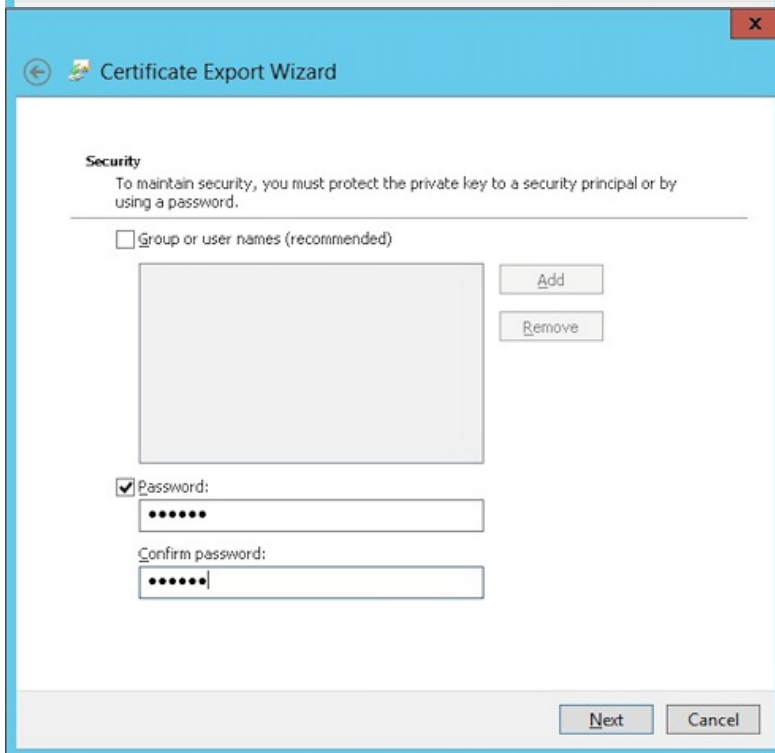
8. [はい、秘密キーをエクスポートします] をクリックします。



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



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



11. 証明書をローカルのハードドライブに保存します。

## XenMobileへの証明書のアップロード

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] 画面が表示されます。
2. [Certificates] をクリックしてから、[Import] をクリックします。

3. 以下のパラメーターを入力します。

- **Import** : Keystore
- **Keystore type** : PKCS#12
- **Use as** : Server
- **Key File Name** : [参照] をクリックして、前の手順で作成した.pfx証明書を選択します。
- **Password** : 証明書と一緒に作成したパスワードを入力します。

**Import** ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

**Import** Keystore

**Keystore type** PKCS#12

**Use as** Server

**Keystore file\***  **Browse**

**Password\***

**Description**

**Cancel** **Import**

4. [Import] をクリックします。

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

## 証明書に基づいた認証のためのPKIエンティティの作成

1. [Settings] で、[More]、[Certificate Management]、[PKI Entities] の順に移動します。

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

3. 以下のパラメーターを入力します。

- **Name** : 任意の名前を入力します
- **Web enrollment service root URL** : https://RootCA-URL/certsrv/  
Be sure to add the last slash (/) in the URL path.

- certnew.cerページ名 : certnew.cer (デフォルト値)
- certfnsh.asp : certfnsh.asp (デフォルト値)
- Authentication type : クライアント証明書。
- SSL client certificate : XenMobileクライアント証明書を発行するために使用するユーザー証明書を選択します。

Settings > PKI Entities > Microsoft Certificate Services Entity

**Microsoft Certificate Services Entity**

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

### Microsoft Certificate Services Entity: General Information

Name\*

Web enrollment service root URL\*

certnew.cer page name\*  ⓘ

certfnsh.asp\*  ⓘ

Authentication type  ⓘ

SSL client certificate  ⓘ

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

**Microsoft Certificate Services Entity**

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

### Microsoft Certificate Services Entity: Templates

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates*	Add
XMTemplate	<input type="button" value="Add"/>

5. HTTPパラメーターをスキップし、[CA Certificates] をクリックします。

6. 環境内で関連するルートCA証明書の名前を選択します。このルートCA証明書は、XenMobileクライアント証明書からインポートされたチェーンの一部です。

**Microsoft Certificate Services Entity**

- 1 General
- 2 Templates
- 3 HTTP Parameters
- 4 CA Certificates

### Microsoft Certificate Services Entity: CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input checked="" type="checkbox"/>	training-AD-CA	14508232713118666452725886249131	02/22/2013	02/22/2023

7. [Save] をクリックします。

## 資格情報プロバイダーの構成

1. [Settings] で、 [More] 、 [Certificate Management] 、 [Credential Providers] の順に移動します。

2. [Add] をクリックします。

3. [General] で、次のパラメーターを入力します。

- Name : 任意の名前を入力します。
- Description : 任意の説明を入力します。
- Issuing entity : 前に作成したPKIエンティティを選択します。
- Issuing method : SIGN
- Templates : PKIエンティティに追加されたテンプレートを選択します。

Credential Providers	Credential Providers: General Information
1 General	<p>You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.</p> <p><b>Name*</b> <input type="text" value="XenMobile_PKI"/></p> <p><b>Description</b> <input type="text" value="XenMobile PKI Configuration"/></p> <p><b>Issuing entity</b> <input type="text" value="MS PKI"/></p> <p><b>Issuing method</b> <input type="text" value="SIGN"/></p> <p><b>Templates</b> <input type="text" value="XMTemplate"/></p>
2 Certificate Signing Request	
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. [Certificate Signing Request] をクリックしてから、次のパラメーターを入力します。

- Key algorithm : RSA
- Key size : 2048
- Signature algorithm : SHA1withRSA
- Subject name : cn=\$user.username

[Subject Alternative Names] の [Add] をクリックしてから、次のパラメーターを入力します。

- Type : ユーザープリンシパル名
- Value : \$user.userprincipalname



5. **[Distribution]** をクリックし、次のパラメーターを入力します。

- **Issuing CA certificate** : 署名済みのXenMobileクライアント証明書の発行CAを選択します。
- **Select distribution mode** : **[Prefer centralized: Server-side key generation]** を選択します。

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

7. **[Renewal]** をクリックします。

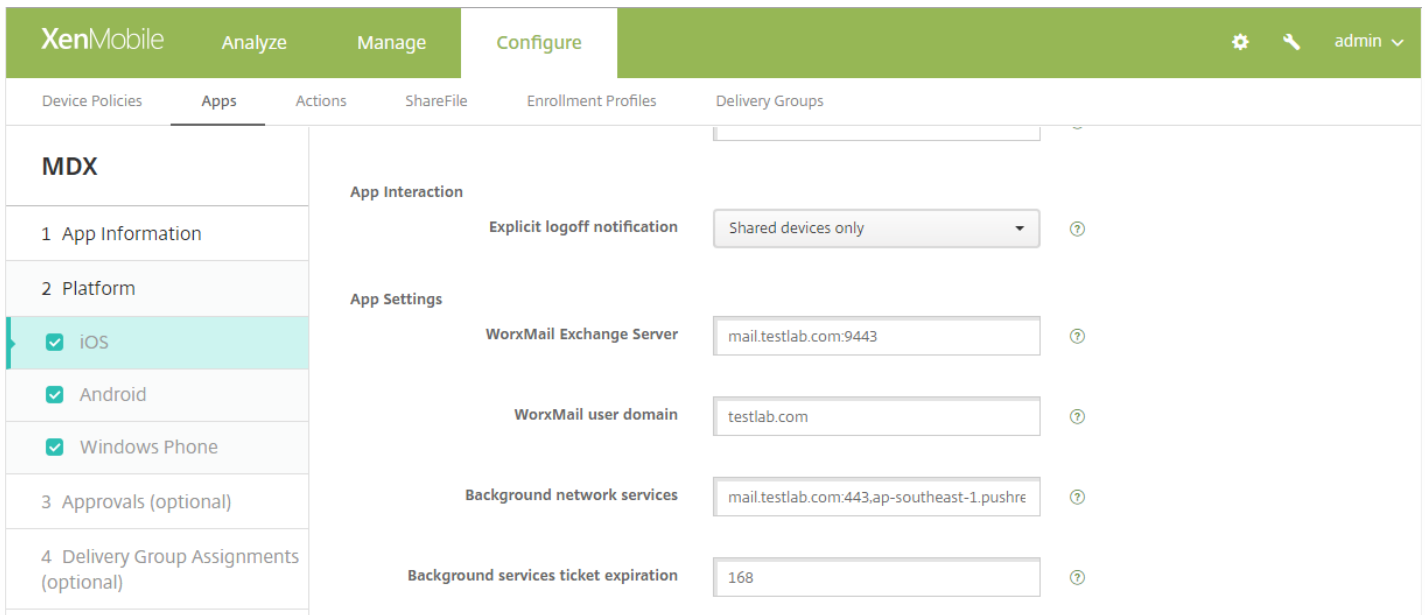
8. **[Renew certificates when they expire]** で **[ON]** を選択します。

9. そのほかの設定はすべてそのままにするか、必要な変更を加えます。

10. **[Save]** をクリックします。

## 証明書ベースの認証を使用するようにSecure Mailを構成する

XenMobileにSecure Mailを追加する場合、必ず **[App Settings]** でExchangeの設定を構成してください。



## XenMobileでのNetScaler証明書の配信の構成

1. XenMobileコンソールにログオンして、右上の歯車アイコンをクリックします。[Settings] 画面が表示されます。
2. [Server] の下の [NetScaler Gateway] をクリックします。
3. NetScaler Gatewayがまだ追加されていない場合、[Add] をクリックして、次のように設定を指定します。
  - External URL : `https://YourNetScalerGatewayURL`
  - Logon Type : Certificate
  - Password Required : OFF
  - Set as Default : ON
4. [Deliver user certificate for authentication] で [On] を選択します。

XenMobile Analyze Manage Configure admin

Settings > NetScaler Gateway

## NetScaler Gateway

When you configure NetScaler Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use NetScaler Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication

**Deliver user certificate for authentication**  ?

Credential provider

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
--------------------------	------	---------	--------------	------------	--------------------

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

6. ユーザープリンシパル名 (UPN) の代替としてユーザー証明書のsAMAccount属性を使用する場合、XenMobileでLDAPコネクタを次のように構成します： [Settings] > [LDAP] に移動し、ディレクトリを選択して [Edit] をクリックし、[User search by] で [sAMAccountName] を選択します。

XenMobile Analyze Manage Configure admin

User base DN\*  ?

Group base DN\*  ?

User ID\*

Password\*

Domain alias\*

XenMobile Lockout Limit  ?

XenMobile Lockout Time  ?

Global Catalog TCP Port  ?

Global Catalog Root Context  ?

User search by

Use secure connection  NO

# Windows Phone 8.1および10デバイス用のEnterprise Hubポリシーの作成

Windows Phoneデバイスの場合、Enterprise Hubデバイスポリシーを作成して、AETXファイルおよびSecure Hubクライアントを配信する必要があります。

## 注意

AETXファイルとSecure Hubファイルの両方で、証明書プロバイダーからの同じエンタープライズ証明書と、Windowsストア開発者アカウントからの同じ発行元IDが使用されてい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。
2. [Add] をクリックした後、[More] > [XenMobile Agent] の下の [Enterprise Hub] をクリックします。
3. ポリシーに名前を付けた後で、エンタープライズハブに対して適切なAETXファイルと署名されたSecure Hubアプリを選択します。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Device Policies' tab is active, showing a list of policies on the left and a 'Policy Information' section on the right. The 'Enterprise Hub Policy' is selected in the list. The 'Policy Information' section contains the following text: 'To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe)'. Below this text are two input fields with 'Browse' buttons. The first is labeled 'Upload .aetx file' and the second is labeled 'Upload signed Enterprise Hub app'.

4. ポリシーをデリバリーグループに割り当て、保存します。

## クライアント証明書構成のトラブルシューティング

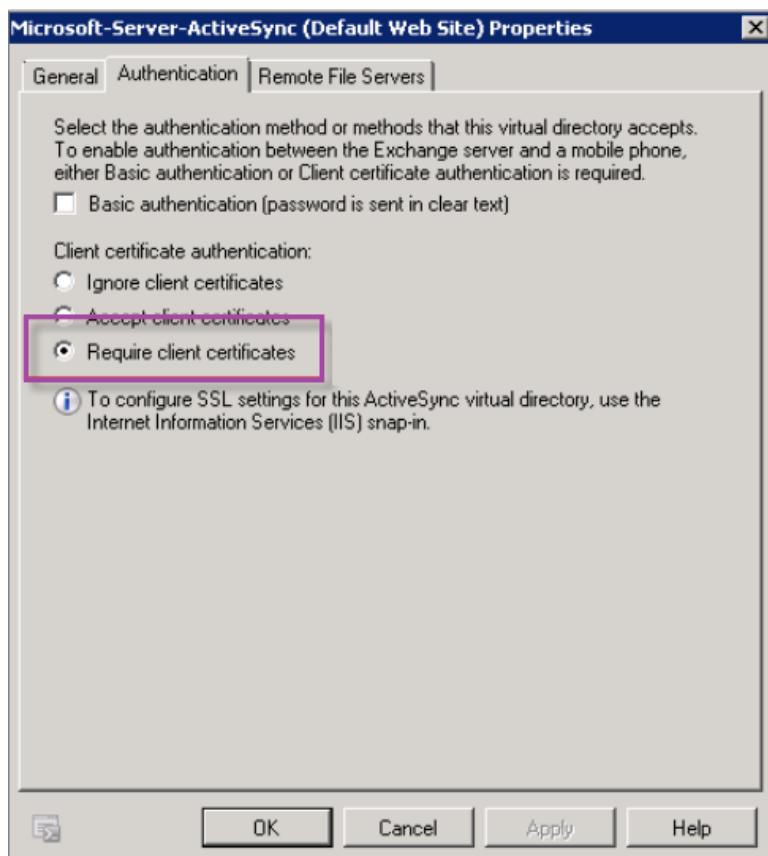
先行する構成とNetScaler Gatewayの構成が成功すると、ユーザーワークフローは次のようになります。

1. ユーザーがモバイルデバイスを登録します。
2. XenMobileがユーザーにCitrix PINを作成するよう求めます。
3. ユーザーがXenMobile Storeにリダイレクトされます。
4. ユーザーがiOS、AndroidまたはWindows Phone 8.1用のSecure Mailを起動した場合、XenMobileはユーザーのメールボックス

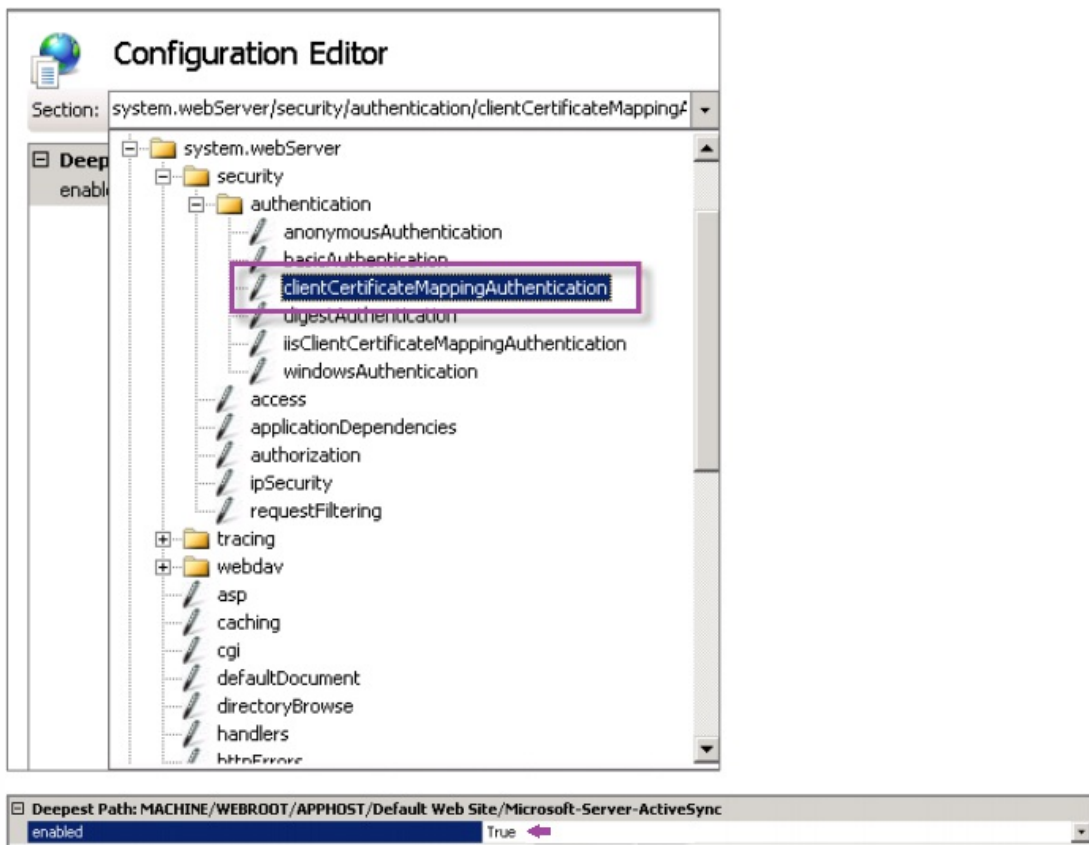
スを構成するための適切な資格情報を求めません。その代わりに、Secure MailはSecure Hubからのクライアント証明書を要求し、認証のためにMicrosoft Exchange Serverに送信します。ユーザーがSecure Mailを起動したときにXenMobileで資格情報を求められた場合は、構成を確認してください。

ユーザーはSecure Mailをダウンロードしてインストールできるが、Secure Mailでメールボックス構成時に構成を完了できない場合：

1. Microsoft Exchange Server ActiveSyncがプライベートSSLサーバー証明書を使用してトラフィックを保護している場合、ルート証明書または中間証明書がモバイルデバイスにインストールされていることを確認してください。
2. ActiveSyncに対して選択された認証の種類が [Require client certificates] であることを確認します。



3. Microsoft Exchange Serverで、Microsoft-Server-ActiveSyncサイトのクライアント証明書マッピング認証が有効になっていることを確認します（デフォルトでは無効）。オプションは、 [Configuration Editor] > [Security] > [Authentication] にあります。



注： [True] を選択したら、必ず [Apply] をクリックして変更を反映してください。

4. XenMobileコンソールでNetScaler Gateway設定を確認します：「XenMobileでNetScaler証明書の配信を構成するには」の説明に従って、 [Deliver user certificate for authentication] が [ON] で、 [Credential provider] で適切なプロファイルが選択されていることを確認してください。

クライアント証明書がモバイルデバイスに配信されたかどうかを判定するには：

1. XenMobileコンソールで、 [Manage] > [Devices] と移動して、デバイスを選択します。
2. [Edit] または [Show More] をクリックします。
3. [Delivery Groups] セクションに移動し、このエントリを検索します。

NetScaler Gateway資格情報： 要求された資格情報、 CertId=

クライアント証明書ネゴシエーションが有効かどうか確認するには：

1. このnetshコマンドを実行して、 IIS WebサイトにバインドされたSSL証明書構成を表示します。

```
netsh http show sslcert
```

2. [Negotiate Client Certificate] の値が [Disabled] の場合、次のコマンドを実行して有効化します。

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={app_id} certstorename=store_name
```

```
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

たとえば、次のように設定します：

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da appid=  
{4dc3e181-e14b-4a21-b022-59fc669b0914} certstorename=ExampleCertStoreName  
verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
clientcertnegotiation=Enable
```

XenMobileを介してWindows Phone 8.1デバイスにルート証明書または中間証明書を配信できない場合：

- 電子メールを介してWindows Phone 8.1デバイスにルート証明書または中間証明書 (.cer) ファイルを送信し、直接インストールします。

Secure MailがWindows Phone 8.1に正常にインストールされない場合：

- Enterpriseハブデバイスポリシーを使用して、XenMobile経由でアプリケーション登録トークン (.AETX) ファイルが配信されていることを確認します。
- アプリケーション登録トークンが、Secure MailのラップおよびSecure Hubアプリの署名に使用された証明書プロバイダーからのエンタープライズ証明書と同じものを使用して作成されたことを確認します。
- Secure Hub、Secure Mail、アプリケーション登録トークンのラップと署名に同一の発行者IDが使用されていることを確認します。

# PKIエンティティ

Apr 27, 2017

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

XenMobileは次の種類のPKIエンティティをサポートします。

- 任意 CA (Certificate Authority : 証明機関)
- 汎用PKIs (GPKIs)
- Microsoft 証明書サービス

XenMobileでは、次のCAサーバーがサポートされます。

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

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

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

## CA証明書

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

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

- sign : 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。
- fetch : 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。
- revoke : アダプターはPKIで特定の証明書を失効させることができます。

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

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



ドして、XenMobileにそのWSDL定義を提供することを意味します。

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

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

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

2. **[PKI Entities]** ページで、**[Add]** をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. **[Generic PKI Entity]** をクリックします。

**[Generic PKI Entity: General Information]** ページが開きます。

4. **[Generic PKI Entity: General Information]** ページで、以下を行います。

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

5. **[Next]** をクリックします。

**[Generic PKI Entity: Adapter Capabilities]** ページが開きます。

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

**[Generic PKI Entity: Issuing CA Certificates]** ページが開きます。

7. **[Generic PKI Entity: Issuing CA Certificates]** ページで、エンティティで使用する証明書を選択します。

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

8. **[Save]** をクリックします。

**[PKI Entities]** の表にエンティティが表示されます。

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。

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

2. **[PKI Entities]** ページで、**[Add]** をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. **[Microsoft Certificate Services Entity]** をクリックします。

**[Microsoft Certificate Services Entity: General Information]** ページが開きます。

4. **[Microsoft Certificate Services Entity: General Information]** ページで、以下を行います。

- **Name** : 新しいエンティティの名前を入力します。この名前は後でそのエンティティを参照するために使用します。エンティティ名は一意的な名前にする必要があります。
- **Web enrollment service root URL** : Microsoft CA Web登録サービスのベースURL (<https://192.0.2.13/certsrv/>など) を入力します。URLには、HTTPまたはHTTP-over-SSLを使用します。
- **certnew.cer page name** : certnew.cerページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- **certfnsh.asp** : certfnsh.aspページの名前。何らかの理由で名前を変更した場合を除き、デフォルト名を使用します。
- **Authentication type** : 一覧から、使用する認証方法を選択します。
- なし
- **HTTP Basic** : 接続に必要なユーザー名とパスワードを指定します。
- **Client certificate** : 正しいSSLクライアント証明書を選択します。

5. **[Next]** をクリックします。

**[Microsoft Certificate Services Entity: Templates]** ページが開きます。このページで、Microsoft CAがサポートするテンプレートの内部名を指定します。資格情報プロバイダーを作成するとき、ここで定義したテンプレートを一覧で選択します。このエンティティを使用するすべての資格情報プロバイダーが、このようなテンプレートを1つだけ使用します。

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

6. **[Microsoft Certificate Services Entity: Templates]** ページで **[Add]** をクリックし、テンプレートの名前を入力して、**[Save]** をクリックします。追加する各テンプレートについて、この手順を繰り返します。

7. **[Next]** をクリックします。

**[Microsoft Certificate Services Entity: HTTP parameters]** ページが開きます。このページで、Microsoft Web登録インターフェイスに対するHTTP要求にXenMobileが挿入するカスタムパラメーターを指定します。これは、カスタマイズしたスクリプトをCAで実行している場合にのみ使用できます。

8. **[Microsoft Certificate Services Entity: HTTP parameters]** ページで **[Add]** をクリックし、追加するHTTPパラメーターの名前と値を入力して、**[Next]** をクリックします。

[Microsoft Certificate Services Entity: CA Certificates] ページが開きます。このページでは、システムでこのエンティティを通じて取得される証明書の署名者をXenMobileに通知するよう要求されます。CA証明書が更新された場合は、そのCA証明書をXenMobileで更新すると、変更がエンティティに透過的に適用されます。

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

10. [Save] をクリックします。

[PKI Entities] の表にエンティティが表示されます。

XenMobileは、サードパーティ証明機関でのみ証明書失効一覧 (CRL) をサポートします。Microsoft CAが構成されている場合、XenMobileはNetScalerを使用して失効を管理します。クライアント証明書ベースの認証を構成する場合、NetScale証明書失効一覧 (CRL) 設定を構成する必要があるかどうか検討します。[Enable CRL Auto Refresh]。この手順を使用すると、MAM-onlyモードのデバイスのユーザーがデバイス上の既存の証明書を使用して認証することができなくなります。ユーザー証明書が失効してもユーザーによる生成が制限されるわけではないので、XenMobileは新しい証明書を再発行します。この設定は、CRLが期限切れのPKIエンティティを確認する場合、PKIエンティティのセキュリティを強化します。

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

任意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OCSPレスポンスを指し示します。

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

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

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

1. XenMobileコンソールで、右上の歯車アイコンをクリックした後、[More] の [PKI Entities] をクリックします。

2. [PKI Entities] ページで、[Add] をクリックします。

追加できるPKIエンティティの種類を示す一覧が表示されます。

3. [Discretionary CA] をクリックします。

[Discretionary CA: General Information] ページが開きます。

4. [Discretionary CA: General Information] ページで、以下を行います。

- **Name** : 随意CAの説明的な名前を入力します。
- **CA certificate to sign certificate requests** : 一覧から、証明書要求に署名するために使用する随意CAの証明書を選択します。この証明書一覧は、[Configure]、[Settings]、[Certificates] でXenMobileにアップロードした、秘密キーのあるCA証明書から生成されます。

5. [Next] をクリックします。

[Discretionary CA: Parameters] ページが開きます。

6. [Discretionary CA: Parameters] ページで、以下を行います。

- **Serial number generator** : 随意CAは発行する証明書のシリアル番号を生成します。一覧で[Sequential] または [Non-sequential] を選択して、番号の生成方法を指定します。
- **Next serial number** : 値を入力して、次に発行される番号を指定します。
- **Certificate valid for** : 証明書の有効期間 (日数) を入力します。
- **Key usage** : 適切なキーを [On] に設定して、随意CAが発行する証明書の目的を指定します。設定すると、CAによる証明書の発行がそれらの目的に限定されます。
- **Extended key usage** : 追加パラメーターを追加するには、[Add] をクリックし、キー名を入力して [Save] をクリックします。

7. Nextをクリックします。

[Discretionary CA: Distribution] ページが開きます。

8. [Discretionary CA: Distribution] ページで、配布モードを選択します。

- **Centralized: server-side key generation**. この集中管理オプションをお勧めします。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
- **Distributed: device-side key generation**. ユーザーデバイス上で秘密キーが生成されます。この分散モードはSCEPを使用し、keyUsage keyEncryptionによるRA暗号化証明書とKeyUsage digitalSignatureによるRA署名証明書が必要です。暗号化と署名で同じ証明書を使用できます。

9. Nextをクリックします。

[Discretionary CA: Online Certificate Status Protocol (OCSP)] ページが開きます。

[Discretionary CA: Online Certificate Status Protocol (OCSP)] ページで、以下を行います。

- このCAが署名する証明書にAuthorityInfoAccess (RFC2459) 拡張を追加する場合は、[Enable OCSP support for this CA] を [On] に設定します。この拡張は、CAのOCSPレスポンス (<https://server/instance/ocsp>) を指し示します。
- OCSPサポートを有効にした場合は、OSCP署名CA証明書を選択します。この証明書一覧は、XenMobileにアップロードしたCA証明書から生成されます。

10. [Save] をクリックします。

[PKI Entities] の表に随意CAが表示されます。

# 資格情報プロバイダー

Apr 27, 2017

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。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に展開された場合、Pの発行設定によってDに展開される証明書が決まり、Cが更新されるときにPの更新設定が適用され、Cが削除されたりDが失効するときにはPの失効設定が適用されます。

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があります。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。

証明書は2つの方法で取得でき、これを発行方法と呼びます。

- 署名。この方法では、新しい秘密キーを作成し、CSRを作成してCA（Certificate Authority : 証明機関）に送信し、署名してもらいます。XenMobileでは3つのPKIエンティティ（MS証明書サービスエンティティ、汎用PKI、随意CA）の署名方法がサポートされています。
- フェッチ。この方法における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でのみフェッチの方法をサポートします。

資格情報プロバイダーは署名またはフェッチの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）。

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説明する必要があります。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が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せん。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	なし
iOS構成プロファイル	はい	なし
SHTP登録	なし	なし
SHTPの構成	なし	なし
Windows PhoneおよびWindowsタブレットの登録	なし	なし
Windows PhoneおよびWindowsタブレットの構成	なし。ただし、Windows Phone 8.1 および最新のWindows 10リリースでサポートされるWi-Fiデバイスポリシーを除く。	なし

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

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックした後、[More] の [Credential Providers] をクリックします。

2. [Credential Providers] ページで、[Add] をクリックします。

[Credential Providers: General Information] ページが開きます。

3. [Credential Providers: General Information] ページで、以下を指定します。

- **Name**：新しいプロバイダー構成の一意の名前を入力します。この名前はXenMobileコンソールのほかの部分で構成を参照するために後で使用されます。
- **Description**：資格情報プロバイダーの説明です。このフィールドはオプションですが、後でこの資格情報プロバイダーの詳細を思い出すときに説明が役立ちます。
- **Issuing entity**：証明書発行エンティティを選択します。
- **Issuing method**：[Sign] または [Fetch] をクリックして、構成されたエンティティから証明書を取得するために使用する方法を選択します。クライアント証明書認証の場合は、[Sign] を使用します。
- テンプレート一覧が使用できる場合は、資格情報プロバイダーのテンプレートを選択します。

4. [Next] をクリックします。

注：これらのテンプレートは、[Settings]、[More]、[PKI Entities]の順にクリックすると開くページで、Microsoft 証明書サービスエンティティが追加されている場合に使用可能になります。

[Credential Providers: Certificate Signing Request] ページが開きます。

5. [Credential Providers: Certificate Signing Request] ページで、以下を指定します。

- **Key algorithm**：新しいキーペアのキーアルゴリズムを選択します。使用可能な値は[RSA]、[DSA]、および[ECDSA]です。
- **Key size**：キーペアのサイズ（ビット単位）を入力します。これは必須フィールドです。  
注：許可される値はキーの種類によって異なります。たとえば、DSAキーの最大サイズは1024ビットです。基になるハードウェアおよびソフトウェアに依存する偽陰性を回避するため、XenMobileではキーのサイズが強制されません。資格情報プロバイダーの構成を実稼働環境でアクティブにする前に、必ずテスト環境でテストしてください。
- **署名アルゴリズム**：新しい証明書の値を選択します。値はキーアルゴリズムによって異なります。
- **Subject name**：新しい証明書のサブジェクトの識別名（Distinguished Name：DN）を入力します。例：  
CN=\${user.username}, OU=\${user.department}, O=\${user.companyname}, C=\${user.c}\endquotation これは必須フィールドです。

たとえば、クライアント証明書認証には次の設定を使用します。

キーアルゴリズム：RSA

キーサイズ：2048ビット

署名アルゴリズム：SHA1withRSA

Subject name: cn=\${user.username}

6. [Subject alternative names] の表に新しいエントリを追加するには、[Add] をクリックします。別名の種類を選択して、2つ目の列に値を入力します。

クライアント証明書認証では、次のように指定します。

Type：User Principal name

Value：\${user.userprincipalname}

注：サブジェクト名と同様に、値フィールドでXenMobileマクロを使用できます。

7. [Next] をクリックします。

[Credential Providers: Distribution] ページが開きます。

8. [Credential Providers: Distribution] ページで、以下を行います。

- [Issuing CA certificate] の一覧から、提供されたCA証明書を選択します。資格情報プロバイダーは随意CAエンティティを使用するため、資格情報プロバイダーのCA証明書は常にエンティティそのものに構成されているCA証明書になります。ここでは外部エンティティを使用する構成との整合性のために示されます。
- [Select distribution mode] で、次のいずれかのキーの生成および配布方法をクリックします。
  - **Prefer centralized: Server-side key generation**。この集中管理オプションをお勧めします。このオプションはXenMobileでサポートされるすべてのプラットフォームをサポートし、NetScaler Gateway認証を使用する場合は必須です。サーバー上で秘密キーが生成および保存され、ユーザーデバイスに配布されます。
  - **優先分散：デバイス側のキー生成**。ユーザーデバイス上で秘密キーが生成および保存されます。この分散モードはSCEI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、暗号化と署名で同じ証明書を使用できます。



- **Only distributed: Device-side key generation.** このオプションは [Prefer distributed: Device-side key generation] と同じように動作しますが、「Prefer」ではなく「Only」であるため、デバイス側でのキー生成が失敗した場合または使用できない場合にはオプションを使用できない点が異なります。

[Prefer distributed: Device-side key generation] または [Only distributed: Device-side key generation] を選択した場合は、[RA signing certificate] の一覧からRA署名証明書を選択し、[RA encryption certificate] の一覧からRA暗号化証明書を選択します。両方に同じ証明書を使用できます。これらの証明書のための新しいフィールドが表示されます。

9. [Next] をクリックします。

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

12. [Credential Providers: Revocation XenMobile] ページで、以下を行います。

- [Revoke issued certificates] で、証明書がいつ失効するかを示すいずれかのオプションを選択します。
- 証明書が失効したときにXenMobileから通知を送信する場合は、[Send notification] の値を [On] に設定して、通知テンプレートを選択します。
- XenMobileで証明書が失効したときに、PKIでも証明書を失効させる場合は、[Revoke certificate on PKI] を [On] に設定し、[Entity] の一覧からテンプレートを選択します。[Entity] の一覧には、失効機能で使用できるすべてのGPKIエンティティが表示されます。XenMobileで証明書が失効すると、[Entity] の一覧から選択したPKIに、失効呼び出しが送信されます。

13. [Next] をクリックします。

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

14. PKIで証明書を失効させる場合は、[Credential Providers: Revocation PKI] ページで以下を行います。

- [Enable external revocation checks] の設定を [On] に変更します。失効PKIに関連する追加のフィールドが表示されません。
- [OCSP responder CA certificate] の一覧から、証明書のサブジェクトの識別名 (Distinguished Name : DN) を選択します。注 : DNフィールドの値には、XenMobileマクロを使用できます。例 : CN=\${user.username}, OU=\${user.department}, O=\${user.companyname}, C=\${user.c}\endquotation
- [When certificate is revoked] の一覧から、証明書が失効したときにPKIエンティティで行う次のいずれかのアクションを選択します。

Do nothing (何もしない)

Renew the certificate (明書を更新する)

Revoke and wipe the device (デバイスを取り消してワイプする)

- 証明書が失効したときにXenMobileから通知を送信する場合は、[Send notification] の値を [On] に設定します。

2つの通知オプションから選択できます。

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

15. [Next] をクリックします。

[Credential Providers: Renewal] ページが開きます。このページで、XenMobileを構成して次のことを実行できます。

- 証明書の更新、(オプション) 証明書更新時の通知の送信 (更新に関する通知)、および (オプション) 既に期限が切れた証明書の操作からの除外
- 期限が近い証明書に関する通知の発行 (更新前の通知)

16. 証明書が失効したら更新する場合は、[Credential Providers: Renewal] ページで以下を行います。[Renew certificates when they expire] を [On] に設定します。

追加のフィールドが表示されます。

- [Renew when the certificate comes within] フィールドに、期限の何日前に更新を行うかを入力します。
- 任意で、[Do not renew certificates that have already expired] (既に期限が切れている証明書を更新しない) チェックボックスをオンにします。注：この場合の「already expired (既に期限が切れている)」とは、証明書のNotAfterが過去の日付であることを意味し、証明書が失効しているという意味ではありません。XenMobileでは、内部で失効した証明書は更新されません。

17. 証明書が更新されたときにXenMobileから通知を送信する場合は、[Send notification] を [On] に設定します。2つの通知オプションから選択できます。

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

18. 証明書の期限が近いときにXenMobileから通知を送信する場合は、[Notify when certificate nears expiration] を [On] に設定します。2つの通知オプションから選択できます。

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

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

20. [Save] をクリックします。

資格情報プロバイダーが [Credential Provider] の表に追加されます。

# APNs証明書

Apr 27, 2017

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の署名を受け取ります。
- 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	<a href="#">IISでCSRを作成する</a> <a href="#">MacでCSRを作成する</a>	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	<a href="#">CSRに署名するには</a>	<a href="#">XenMobile APNs CSR署名Webサイト</a> （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	<a href="#">署名済みのCSRをAppleに送信する</a>	署名入りCSRを <a href="#">Apple Push Certificate Portal</a> （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	<a href="#">Microsoft IISを使用して.pfx APN証明書を作成するには</a> <a href="#">Macコンピューターで.pfx APN証明書を作成するには</a> <a href="#">OpenSSLを使用して.pfx APN証明書を作成する</a>	（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	<a href="#">APN証明書をXenMobileにインポートする</a>	証明書をXenMobileにインポートします。

---

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お問い合わせください。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。

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. [Server Certificates] ウィンドウで、[Create Certificate Request] 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。

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. 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。

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。

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 (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。代替りの手段として、手順1で [identity.apple.com](http://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。

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PKCS #12 (.pfx) ファイルとしてエクスポートし、このAPN証明書をXenMobileにインポートする必要があります。

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

1. Microsoft IISを開きます。
2. サーバー証明書アイコンをクリックします。
3. [サーバー証明書] ウィンドウで、[証明書の要求の完了] をクリックします。
4. AppleのCertificate.pemファイルを指定します。フレンドリ名または証明書名を入力して [OK] をクリックします。
5. 手順4で指定した証明書を選択して [エクスポート] をクリックします。
6. .pfx証明書の場所とファイル名およびパスワードを指定して [OK] をクリックします。  
注：XenMobileのインストール中にこの証明書のパスワードが必要になります。
7. .pfx証明書をXenMobileがインストールされるサーバーにコピーします。
8. XenMobileコンソールに管理者としてサインオンします。
9. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
10. [Certificates] をクリックします。[Certificates] ページが開きます。
11. [Import] をクリックします。[Import] ダイアログボックスが開きます。
12. [Import] メニューから、[Keystore] を選択します。
13. [Use as] から、[APNs] を選択します。
14. [Keystore] ファイルで、[Browse] をクリックしてインポートするキーストアファイルの場所に移動し、そのファイルを選択します。
15. [Password] ボックスに、証明書に割り当てられたパスワードを入力します。
16. [Import] をクリックします。

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

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

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Certificates] をクリックします。[Certificates] ページが開きます。
3. [Import] をクリックします。[Import] ダイアログボックスが開きます。
4. [Import] メニューから、[Keystore] を選択します。
5. [Use as] から、[APNs] を選択します。
6. コンピューターの.p12ファイルを指定します。
7. パスワードを入力して、[Import] をクリックします。

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

APN証明書を更新するには、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。証明書を更新する場合、組織名とApple IDは必ず同じものを使用してください。

注：APN証明書の有効期限を調べるには、XenMobileコンソールで **[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PKCS #12 (.pfx) APN証明書を生成します。
6. XenMobileコンソールで新しいAPN証明書を更新します。コンソールの右上にある歯車アイコンをクリックします。 **[Settings]** ページが開きます。
7. **[Certificates]** をクリックします。 **[Certificates]** ページが開きます。
8. **[Import]** をクリックします。 **[Import]** ダイアログボックスが開きます。
9. **[Import]** メニューから、 **[Keystore]** を選択します。
10. **[Use as]** から、 **[APNs]** を選択します。
11. コンピューターの.p12ファイルを指定します。
12. パスワードを入力して、 **[Import]** をクリックします。



# ShareFileでのSAMLによるシングルサインオン

Apr 27, 2017

XenMobileとShareFileを構成し、セキュリティアサーションマークアップランゲージ (SAML) を使用して、MDXツールキットでラップされたShareFile Mobileアプリはもちろん、Webサイト、Outlook Plug-in、SyncクライアントなどのラップされていないShareFileクライアントへのシングルサインオンアクセス (SSO) を提供することができます。

- **ラップされているShareFileアプリの場合。** ShareFile Mobileアプリを介してShareFileにログオンするユーザーは、ユーザー認証のためにSecure Hubにリダイレクトされ、SAMLトークンを取得します。認証が成功した後で、ShareFile MobileアプリからShareFileにSAMLトークンが送信されます。最初のログオンの後は、ユーザーはSSOを介してShareFile Mobileアプリにアクセスし、毎回ログオンしなくてもSecure MailのメールにShareFileからドキュメントを添付できます。
- **ラップされていないShareFileクライアントの場合:** WebブラウザーまたはほかのShareFileクライアントを介してShareFileにログオンするユーザーは、ユーザー認証のためにXenMobileにリダイレクトされ、SAMLトークンを取得します。認証が成功した後で、SAMLトークンがShareFileに送信されます。最初のログオンの後は、毎回ログオンしなくてもユーザーはSSOを介してShareFileクライアントにアクセスできます。

リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の、[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およびShareFileアプリにSSOを構成する前に、以下の前提条件を満たす必要があります。

- MDX Toolkit Version 9.0.4移行 (ShareFile Mobileアプリ用)
- 適切なShareFile Mobileアプリ：
  - ShareFile for iPhoneバージョン3.0.x
  - ShareFile for iPadバージョン2.2.x
  - ShareFile for Androidバージョン3.2.x
- Secure Hub 9.0 (ShareFile Mobileアプリケーション用) - 必要に応じて、iOSまたはAndroidバージョンをインストールします。
- ShareFile管理者アカウント

XenMobileおよびShareFileに接続できることを確認します。

ShareFileのためにSAMLを設定する前に、以下のようにShareFileアクセス情報を入力します。

1. XenMobile Webコンソールで、**[Configure]** の **[ShareFile]** をクリックします。 **[ShareFile]** 構成ページが開きます。

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure (selected). On the right, there are icons for settings and search, and a user dropdown menu showing 'administrator'. Below the navigation, there are sub-tabs: Device Policies, Apps, Actions, ShareFile (selected), and Delivery Groups.

The main content area is titled 'ShareFile' and contains the following settings:

- Domain\***: A text input field containing 'subdomain.sharefile.com'.
- Assign to delivery groups**: A search interface with a text input field containing 'Type to search', a search icon, and a blue 'Search' button.
- ShareFile Administrator Account Logon**: A section with two text input fields: 'User name\*' containing 'Enter user name' and 'Password\*' containing 'Enter new password'.
- User account provisioning**: A toggle switch currently set to 'OFF'.

At the bottom right, there are 'Cancel' and 'Save' buttons.

2. 次の設定を構成します。

- **Domain** : ShareFileサブドメイン名を入力します。たとえば、「example.sharefile.com」です。
- **Assign to delivery groups** : ShareFileと共にSSOを使用するデリバリーグループを選択または検索します。
- **ShareFile 管理者アカウント ログオン**
  - **User name** : ShareFile管理者のユーザー名を入力します。このユーザーには管理特権が必要です。
  - **Password** : ShareFile管理者のパスワードを入力します。
  - **User account provisioning** : XenMobileでユーザープロビジョニングを有効にする場合はこのオプションをオンにします。ユーザープロビジョニングにShareFile User Management Toolを使用する計画である場合は無効のままにします。

注：選択した役割にShareFileアカウントを持たないユーザーが含まれる場合も、[User account provisioning] が有効であればそのユーザーに自動的にShareFileアカウントがプロビジョニングされます。構成をテストするために、メンバーが少ない役割を使用することをお勧めします。これにより、多くのユーザーがShareFileアカウントを持たない可能性を避けることができます。

3. [Save] をクリックします。

以下の手順がiOSおよびAndroidのアプリおよびデバイスに当てはまります。

1. MDX ToolkitでShareFileモバイルアプリケーションをラップします。MDX Toolkitによるアプリケーションのラップについて詳しくは、「[MDX Toolkitによるアプリケーションのラップ](#)」を参照してください。
2. XenMobileコンソールで、ラップされたShareFileモバイルアプリをアップロードします。MDXアプリをアップロードする方法について詳しくは、「[MDXアプリケーションをXenMobileに追加するには](#)」を参照してください。
3. 上記の手順で構成した管理者のユーザー名とパスワードでShareFileにログオンしてSAML設定を検証します。
4. ShareFileおよびXenMobileが同じタイムゾーンで構成されていることを確認します。

注：構成したタイムゾーンに関して、XenMobileに正しい時刻が表示されていることを確認してください。正しい時刻が表示されていない場合は、SSOエラーが発生している可能性があります。

## ShareFile Mobileアプリを検証する

1. まだ行っていない場合は、ユーザーデバイスにSecure Hubをインストールして構成します。
2. XenMobile StoreからShareFile Mobileアプリをダウンロードしてインストールします。
3. ユーザー名やパスワードの入力を求められずにShareFileが開始されます。

## Secure Mailによる検証

1. まだ行っていない場合は、ユーザーデバイスにSecure Hubをインストールして構成します。
2. XenMobile StoreからSecure Mailをダウンロード、インストール、および設定します。
3. 新規メールを開いて [Attach from ShareFile] をタップします。メールに添付できるファイルがユーザー名とパスワードを入力しなくても表示されます。

Webサイト、Outlook Plug-in、SyncクライアントなどのラップされていないShareFileクライアントへのアクセスを構成するには、以下のようにNetScaler Gatewayを構成して、SAML IDプロバイダーとしてのXenMobileの使用をサポートする必要があります。

- ホームページのリダイレクトを無効にする。
- ShareFileのセッションポリシーとプロファイルを作成する。
- NetScaler Gateway仮想サーバーにポリシーを構成する。

## ホームページのリダイレクトを無効にする

構成されたホームページの代わりに本来要求された内部URLをユーザーが見られるように、/cginfraパスから送られる要求に対するデフォルトの動作を無効にする必要があります。

1. XenMobileのログオンに使用されるNetScaler Gateway仮想サーバーの設定を編集します。NetScaler 10.5で、[Other Settings] に移動して [Redirect to Home Page] チェックボックスをオフにします。

2. [ShareFile] の下にXenMobileの内部サーバー名およびポート番号を入力します。

3. [AppController] の下にXenMobileのURLを入力します。

この構成により、/cginfraパスを介して入力したURLに対する要求が承認されます。

## ShareFileのセッションポリシーと要求プロファイルを作成する

以下の設定を構成してShareFileセッションポリシーと要求プロファイルを作成します。

1. NetScaler Gateway構成ユーティリティの左側のナビゲーションペインで、[NetScaler Gateway]、[Policies]、[Session] の順にクリックします。
2. 新しいセッションポリシーを作成します。[Policies] タブで [Add] をクリックします。
3. [Name] ボックスに「ShareFile\_Policy」と入力します。
4. [+] をクリックして新しい操作を作成します。[Create NetScaler Gateway Session Profile] ページが開きます。

**Configure NetScaler Gateway Session Profile**

Configure NetScaler Gateway Session Profile

Name  
Sharefile\_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Accounting Policy  
[Dropdown]

Override Global  
 Display Home Page

Home Page  
none

URL for Web-Based Email  
[Text Box]

Split Tunnel\*  
OFF

Session Time-out (mins)  
1

Client Idle Time-out (mins)  
[Text Box]

Clientless Access\*  
Allow

Clientless Access URL Encoding\*  
Obscure

Clientless Access Persistent Cookie\*  
DENY

Plug-in Type\*  
Windows/MAC OS X

Single Sign-on to Web Applications

Credential Index\*  
PRIMARY

KCD Account  
[Text Box]

次の設定を構成します。

- Name : 「ShareFile\_Profile」と入力します。
- [Client Experience] タブをクリックし、以下の設定を構成します。
  - Home Page : 「none」と入力します。
  - Session Time-out (mins) : 「1」と入力します。
  - Single Sign-on to Web Applications : この設定を選択します。
  - Credential Index : 一覧で [PRIMARY] をクリックします。
- [Published Applications] タブをクリックします。

Configure NetScaler Gateway Session Profile

Name  
Sharefile\_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Override Global

ICA Proxy\*  
ON

Web Interface Address  
https://xms.citrix.lab:8443

Web Interface Address Type\*  
IPV4

Web Interface Portal Mode\*  
NORMAL

Single Sign-on Domain  
citrix

Citrix Receiver Home Page

Account Services Address

OK Close

次の設定を構成します。

- ICA Proxy : 一覧で [ON] を選択します。
- Web Interface Address : XenMobileサーバーのURLを入力します。
- Single Sign-on Domain : Active Directoryドメイン名を入力します。

注 : WNetScaler Gatewayセッションプロファイルを構成するとき、 [Single Sign-on Domain] に入力するドメインサフィックスをLDAPに定義するXenMobileドメインエイリアスと一致させる必要があります。

5. [Create] をクリックしてセッションプロファイルを定義します。
6. [Expression Editor] をクリックします。

Back

Create NetScaler Gateway Session Policy

Name\*  
Sharefile\_Policy

Action\*  
Sharefile\_Profile

Expression\*  
Operators Saved Policy Expressions

Create Close

Add Expression

Select Expression Type: General

Flow Type  
REQ

Protocol  
HTTP

Qualifier  
HEADER

Operator  
CONTAINS

Value\*  
NSC\_FSRD

Header Name\*  
COOKIE

Length

Offset

Done Cancel

Expression Editor  
Clear

次の設定を構成します。

- Value : 「NSC\_FSRD」と入力します。
- Header Name : 「COOKIE」と入力します。

- [Done] をクリックします。

7. [Create] をクリックしてから、[Close] をクリックします。

## NetScaler Gateway仮想サーバーにポリシーを構成する

以下の設定をNetScaler Gateway仮想サーバーに構成します。

1. NetScaler Gateway構成ユーティリティの左側のナビゲーションペインで、[NetScaler Gateway] の [Virtual Servers] をクリックします。
2. [Details] ペインでNetScaler Gateway仮想サーバーをクリックします。
3. [Edit] をクリックします。
4. [Configured policies] の [Session policies] をクリックし、[Add binding] をクリックします。
5. [ShareFile\_Policy] を選択します。
6. 以下の図に示すように、このポリシーの優先順位が一覧表示されるほかのポリシーよりも高くなるように、選択したポリシーに対して自動生成される [Priority] の番号を最も小さい数に変更します。

Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Ci...	AC_AG_PLG_10.217.232.36_A_

7. [Done] をクリックして、NetScaler構成を保存します。

以下の手順に従って、ShareFile構成のための内部アプリ名を見つけます。

1. 「<https://4443/OCA/admin/>」にアクセスしてXenMobile管理ツールにログインします。「OCA」は必ず大文字で入力してください。
2. [View] の一覧で、[Configuration] をクリックします。

**Login**  
 CITRIX® Please enter the login credentials to access the system

User Name

Password

Domain

View

3. [Applications] の [Applications] をクリックし、 [Display Name] が「ShareFile」のアプリの [Application Name] を記録します。

Application Name	Display Name	Description
activedirectory	activedirectory	
AmericanExpress	AmericanExpress	Online access to world-class card, financial, insu...
Fidelity	Fidelity	Your Personal Investing Resource
LinkedIn	LinkedIn	Business-oriented social networking site
ShareFile_SAML	ShareFile	Online storage for business
MobileApp11	ShareFile_220	ShareFile 2.2.0
MobileApp13	ShareFile_iPhone_303	ShareFile 3.0.3

### ShareFile.comのSSO設定を変更する

1. ShareFileアカウント (https://sharefile.com) にShareFile管理者としてログオンします。
2. ShareFileのWebインターフェイスで [Admin] をクリックし、 [Configure Single Sign-on] を選択します。
3. [Login URL] を以下のように編集します。

[Login URL] は「https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile\_SAML\_SP&reqtype=1」のように表示されているはずですが。

Home Manage Users Send a File Request a File Admin My Settings Apps

Basic Settings

Enable SAML:

ShareFile Issuer / Entity ID: \*

Your IDP Issuer / Entity ID:

X.509 Certificate: \*

Login URL: \*

Logout URL:



- NetScaler Gateway仮想サーバーの外部FQDNおよび「/cginfra/https/」をXenMobileサーバーのFQDNの前に挿入し、XenMobileサーバーのFQDNの後に「8443」を追加します。

これで、URLは「https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\_SAML\_SP&reqtype=1」のようになるはずですが。

- パラメーター&app=ShareFile\_SAML\_SPを、「ShareFileでのSAMLによるシングルサインオン」の手順3で確認したShareFile内部アプリ名に変更します。デフォルトで内部名は「ShareFile\_SAML」ですが、構成を変更するたびに数字が内部名に付加されます（ShareFile\_SAML\_2、ShareFile\_SAML\_3など）。

これで、URLは「https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\_SAML&reqtype=1」のようになるはずですが。

- 「&nssso=true」をURLの最後に追加します。

これで、変更したURLは「https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile\_SAML&reqtype=1&nssso=true」のようになるはずですが。

**重要**：XenMobileコンソールでShareFileアプリを編集または再作成したりShareFile設定を変更したりするたびに、内部アプリ名に新しい番号が付加されます。これは、ShareFile WebサイトでログインURLも更新して、更新されたアプリ名を反映する必要があるということを意味します。

4. [Optional Settings] の下の [Enable Web Authentication] チェックボックスをオンにします。

The image shows a configuration window titled "Optional Settings". It contains several fields and checkboxes:

- Require SSO Login:**  ?
- SSO IP Range:**  ?
- SP-Initiated SSO certificate:** HTTP Redirect with no signature ?
- Enable Web Authentication:**  ? (This checkbox is highlighted with a red box in the original image)
- SP-Initiated Auth Context:** User Name and Password Minimum ?
- Active Profile Cookies:**  ?

At the bottom, there are two buttons: **Save** (with a green checkmark icon) and **Cancel**.

以下の操作を実行して構成を検証します。

1. ブラウザーでhttps://sharefile.com/saml/loginにアクセスします。

NetScaler Gatewayのログオンフォームにリダイレクトされます。リダイレクトされない場合は前の構成設定を検証します。

2. NetScaler Gatewayおよび構成したXenMobile環境のユーザー名とパスワードを入力します。

.sharefile.comにあるShareFileフォルダーが表示されます。ShareFileフォルダーが表示されない場合は、正しいログオン資格情報を入力したかどうか確認します。

# Microsoft Azure Active Directoryサーバー設定

Apr 27, 2017

Windows 10が実行されているデバイスを、AzureをActive Directory認証の統合手段として使用して登録します。管理者は、以下のいずれかの方法を用いてWindows 10デバイスをMicrosoft Azure ADに統合できます。

- 初めてデバイスの電源を入れたときに、特別な設定をすることなくAzure AD統合の一部としてMDMに登録する。
- デバイスを構成したあとに、[Windows Settings] ページからAzure AD統合の一部としてMDMに登録する。この機能は、Windows 10 Phoneでは使用できません。
- 個人用デバイスでワークアカウントを追加する場合にAzure AD統合の一部としてMDMに登録する。

XenMobileとMicrosoft Azureを統合するには、Microsoft Azure Active Directoryのプレミアムライセンスが必要です。ライセンスは、Windows 10デバイスを使用するユーザーがAzure ADを使用して登録できるようにMDMとAzure ADの統合を有効化するために必要です。プレミアムライセンスの取得について詳しくは、「[Microsoft Azure](#)」を参照してください。価格について詳しくは、「[Azure Active Directoryの価格](#)」を参照してください。

WindowsデバイスユーザーがAzureを使用して登録するには、管理者がXenMobileでMicrosoft Azureサーバーの設定を構成し、さらにWindowsデバイス用の契約条件デバイスポリシーを設定する必要があります。ここでは、Microsoft Azureの設定の構成方法について説明します。Windowsデバイスの契約条件デバイスポリシーの構成については、「[契約条件デバイスポリシー](#)」を参照してください。

XenMobileでMicrosoft Azureサーバーの設定を構成する前に、Azure ADポータルにログオンして、以下の操作を行う必要があります。

1. カスタムドメインを登録して、ドメインを検証します。詳しくは、「[Azure Active Directoryへの独自のドメイン名の追加](#)」を参照してください。
2. ディレクトリ統合ツールを使用して、オンプレミスのディレクトリをAzure Active Directoryに拡張します。詳しくは、「[ディレクトリ統合](#)」を参照してください。
3. MDMをAzure ADの信頼できるパーティーにします。そのためには、[Azure Active Directory]、[Applications] の順にクリックして、[Add] をクリックします。ギャラリーから [Add an application] を選択します。[MOBILE DEVICE MANAGEMENT] に移動して、[On-premise MDM application] を選択し、設定を保存します。
4. アプリケーションで、XenMobileサーバー検出、使用条件エンドポイント、およびAPP ID URIを以下のように構成します。
  - MDM検出URL : <https://:8443/zdm/wpe>
  - MDM契約条件URL : <https://:8443/zdm/wpe/tou>
  - APP ID URI : <https://:8443/>
5. 手順3で作成したオンプレミスMDMアプリケーションを選択し、[Manage devices for these users] オプションを有効にして、すべてのユーザーまたは特定のユーザーグループに対してMDM管理を有効にします。

また、XenMobileコンソールで設定を構成するには、Microsoft Azureアカウントの以下の情報を記録しておく必要があります。

- App ID URI - XenMobileを実行しているサーバーのURL
- Tenet ID - [Azure application settings] ページに記載
- Client ID - アプリケーションの一意の識別子
- Key - [Azure application settings] ページに記載

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

XenMobile Analyze Manage Configure

Settings > Microsoft Azure

### Microsoft Azure

Integrate XenMobile with Microsoft Azure to let devices running Windows 10 enroll with Azure as a federated means of Active Directory authentication. You derive the values to enter here from your Azure directory settings. Note that you must also configure a Terms & Conditions device policy for Windows; otherwise, users cannot enroll with Azure.

App ID URI\*

Tenant ID\*  ?

Client ID\*

Key\*  ?

Cancel Save

3. 次の設定を構成します。

- **App ID URI** : Azure設定の構成時に入力した、XenMobileを実行しているサーバーのURLを入力します。
- **Tenant ID** : [Azure application settings] ページから値をコピーします。ブラウザのアドレスバーに表示されている、数字と文字から成る部分をコピーします。たとえば、  
<https://manage.windowsazure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...>とある場合、テナントIDは「*abc123-abc123-abc123*」です。
- **Client ID** : [Azure Configure] ページから値をコピーして貼り付けます。これはアプリケーションの一意の識別子です。
- **Key** : [Azureアプリケーション設定] ページから値をコピーします。[Keys] の下で、一覧から期間を選択し、設定を保存します。キーは、コピーしてこのフィールドに貼り付けることができます。キーは、Microsoft Azure ADでアプリケーションがデータを読み取ったり書き込んだりする場合に必要です。

4. [Save] をクリックします。

## Important

ユーザーがWindowsデバイスでAzure ADに参加する場合、XenMobileで構成されたXenMobile StoreおよびWebリンクデバイスポリシーについては、ローカルユーザーではなくAzure ADユーザーのみが使用できます。ローカルユーザーがこれらのデバイスポリシーを使用するには、次の手順を実行する必要があります。

1. [Settings] > [About] > [Join Azure AD] で、Azureユーザーの代わりにAzure ADに参加します。
2. Windowsからサインアウトし、Azure ADアカウントを使用してサインインします。



# アップグレード

Apr 27, 2017

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

XenMobileのアップグレードには次の選択肢があります。

- **XenMobile 9.0からXenMobile 10.4にアップグレードする。**  
XenMobile 10.4内蔵のXenMobileアップグレードツールを使用します。詳しくは、このセクションの記事を参照してください。  
アップグレードツールは、XenMobile 9のすべてのエディション（MDM、AppおよびEnterprise）をサポートします。  
解決された問題と既知の問題については、「[解決された問題](#)」および「[既知の問題](#)」を参照してください。  
以前のアップグレードツールを、Citrix.comで入手することはできませんのでご注意ください。
- **XenMobile 10.3.xからXenMobile 10.4にアップグレードする。**  
XenMobileコンソールで **[Release Management]** ページを使用します。詳しくは、この記事の手順を参照してください。  
XenMobile 10.3.xのインストールには、アップグレードツールは使用しません。
- **XenMobile 10またはXenMobile 10.1からXenMobile 10.4にアップグレードする。**  
まず、XenMobileコンソールの **[Release Management]** ページを使用して、XenMobile 10またはXenMobile 10.1からXenMobile 10.3にアップグレードします。次に、XenMobileコンソールの **[Release Management]** ページを使用して、XenMobile 10.3からXenMobile 10.4にアップグレードします。詳しくは、この記事の手順を参照してください。これらのインストールには、アップグレードツールは使用しません。

XenMobileサーバーのバージョン	リリース番号	アップグレード先	リリース番号	アップグレードパス	リリースアップデートの入手場所
XenMobile Server 9 (Rolling Patch インストール済み)	9.0.0_97106	XenMobileサーバー-10.4	10.4.0.116	XenMobile Server 9からXenMobile Server 10.4	<a href="#">ダウンロード</a> 。Rolling Patchの必須コンポーネントです。 XenMobile 10.4用のアップグレードツールはXenMobile Serverに内蔵されています。
XenMobile Server 10またはXenMobile Server 10.1	10.1.0.63030	XenMobileサーバー-10.3	10.3.0.824	XenMobile 10またはXenMobile 10.1からXenMobile 10.3にアップグレード	<a href="#">ダウンロード</a>
XenMobileサーバー-10.3.x	10.3.x	XenMobileサーバー-10.4	10.4.0.116	XenMobile 10.3.xからXenMobile 10.4にアップグレード	<a href="#">ダウンロード</a>

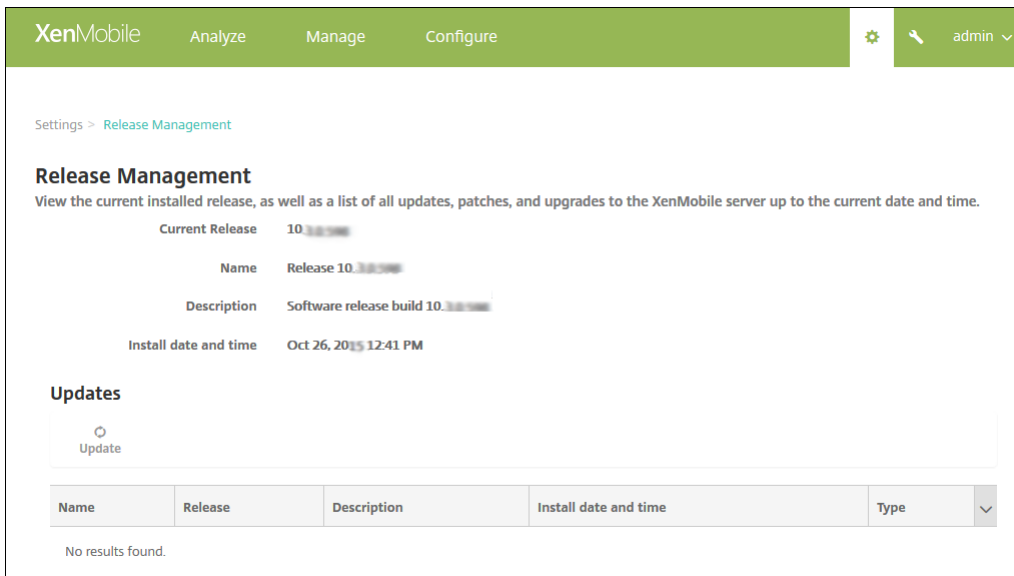
10.4.0?
10.4.0?

## 前提条件

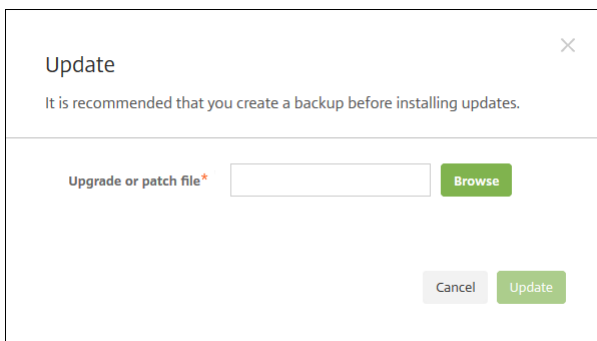
- XenMobileの更新をインストールする前に、仮想マシン（VM）の機能を使用して、システムのスナップショットを取得してください。
- システム構成データベースをバックアップしてください。
- 更新するバージョンに関しては、「システム要件」を参照してください。XenMobile 10.4について詳しくは、[必要なシステム環境](#)を参照してください。

クラスター展開の場合、このトピックの最後にある手順を参照してください。

1. Citrix Webサイトのアカウントにログインして、XenMobile Upgrade (.bin) ファイルを適切な場所にダウンロードします。
2. XenMobileコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。
3. **[Release Management]** をクリックします。 **[Release Management]** ページが開きます。



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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## クラスター化されたXenMobile展開にアップグレードするには

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

1. [Settings] > [Release Management] から、すべてのノードでbinファイルをアップロードします。
2. まずアップグレードするもの以外のすべてのノードをシャットダウンします。ノードをシャットダウンするには、[System Menu] をコマンドラインインターフェイスで使います。
3. まだ実行されているノードをアップグレードします。
3. アップグレードされたノードでこのサービスが実行中かチェックしてください。
4. 他のノードを1つずつ起動します。

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



# アップグレードツールの前提条件

Apr 27, 2017

XenMobile 9.0からXenMobile 10.4にアップグレードするには、XenMobile 10.4内蔵アップグレードツールを使用します。

アップグレードツールは次のものをサポートします。

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

XenMobile 9.0でマルチテナントコンソール（Multi-Tenant Console : MTC）が有効化されている場合は、MTCをスタンドアロンのXenMobile 10.4展開に移行できます。XenMobile 10ではMTCはサポートされないため、アップグレードしたインスタンスは個別に管理する必要があります。この記事の前提条件を完了したら、「[MTCテナントサーバーからXenMobile 10.4へのアップグレード](#)」を参照してください。

XenMobile 10.4は、NetScaler Gatewayのバージョン11.1.x、11.0.x、および10.5.xをサポートしています。

XenMobile 10.4内蔵のアップグレードツールは、NetScaler Gatewayのバージョン10.1.xもサポートしています。NetScaler Gateway 10.1をXenMobile 10.4とともに使用することはサポートされていません。ただし、XenMobile 10.4内蔵のアップグレードツールを使用して、NetScaler Gateway 10.1の展開をアップグレードできます。その後で、NetScaler Gatewayをサポートされている最新バージョンにアップグレードすることをお勧めします。

## Important

アップグレード処理は複雑です。アップグレードを開始する前に、必ず、この記事の説明に従って**既知の問題**を確認し、アップグレードを計画し、前提条件をすべて完了します。また、この**ブログ**にある前提条件のチェックリストは、アップグレードを計画する助けになります。

アップグレードツールの実行後、すべてのアップグレード後要件を完了していることを確認します。

前提条件を完了していない場合、アップグレードが失敗することがあります。その場合は、コマンドラインコンソールで新しいXenMobile 10.4インスタンスを構成し、アップグレードツールを再起動する必要があります。

次の段階でアップグレードすることをお勧めします。

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

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

2. 体験版アップグレードで、構成データ（たとえばLDAP、ポリシー、およびアプリ）が正しくアップグレードされたことを確認します。テストデバイスを確認します。

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

## 体験版アップグレードと実稼働環境のアップグレードについて

XenMobile 10.4アップグレードツールを使用して、まずアップグレードをテストし、続いて実稼働環境を完全にアップグレードします。

### 体験版アップグレードを選択する場合：

アップグレードツールが実稼働環境の構成データで体験版アップグレードを実行して、実稼働環境に影響を与えずにXenMobile 9.0とXenMobile 10.4を比較できます。体験版アップグレードでは構成データのみがテストされます。デバイスデータ（XenMobile Enterprise Edition展開の場合）またはユーザーデータはテストされません。

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

### アップグレードを選択する場合：

アップグレードツールはまずすべての構成、デバイス、およびユーザーデータをXenMobile 9.0から、同じ完全修飾ドメイン名（Fully Qualified Domain Name：FQDN）を持つXenMobile 10.4の新しいインスタンスにコピーします。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。

アップグレード後にXenMobile 10.4コンソールにログオンすると、アップグレードでXenMobile 9.0から移動されたすべてのユーザーおよびデバイスデータが表示されます。

## アップグレードツールで実行されない内容

アップグレードツールを使用した場合、次の情報はXenMobile 10.4にアップグレードされません。

- ライセンス情報
- レポートのデータ
- サーバークループのポリシーおよび関連する展開（XenMobile 10.4でサポートされません）。
- Managed Service Provider（MSP）グループ
- Windows 8.0に関連するポリシーおよびパッケージ
- 使用していない展開パッケージ（展開パッケージにユーザーまたはグループが割り当てられていない場合など）
- アップグレードログファイル内に記述されている、そのほかの構成またはユーザーデータ
- CXM Web（Citrix Secure Webに置き換えられます）
- DLPポリシー（Citrix Sharefileに置き換えられます）
- カスタムのActive Directoryの属性
- 複数のブランド設定ポリシーを構成している場合、ブランド設定ポリシーはアップグレードされません。XenMobile 10.4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 10.4にアップグレードするには、XenMobile 9.0のブランド設定ポリシーを1つに維持する必要があります。
- コンソールへのアクセスの制限に使用される、XenMobile 9.0のauth.jspファイル内の設定。XenMobile 10.4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。
- Syslogサーバーの構成
- XenMobile 9.0で構成されたフォーム入力コネクタ（XenMobile 10.1でサポートされません）

## XenMobileの変更

- アップグレードツールでは、ローカルグループに割り当てられたActive Directoryユーザーはアップグレードされません。

後からActive Directoryユーザーをローカルグループに割り当てることができます。

- XenMobile 10では、入れ子になったローカルグループはサポートされていません。XenMobile 9からアップグレードすると、ローカルグループの階層がフラット化されます。
- 次の図に示すように、Device Managerの展開パッケージはXenMobileではデリバリーグループと呼ばれます。詳しくは、「[リソースの展開](#)」を参照してください。

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Configure', 'Delivery Groups' is highlighted. The main content area displays a table of Delivery Groups with columns for Status, Name, Last Updated, and Disabled. There are 'Add' and 'Export' buttons above the table. A search bar is also present.

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		<input type="checkbox"/>
<input type="checkbox"/>		Domain users	Jun 13 2016 5:10 PM	<input type="checkbox"/>
<input type="checkbox"/>		Sales	Apr 13 2016 12:50 PM	<input type="checkbox"/>

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

The screenshot shows the XenMobile interface with the 'Configure' tab selected. Under 'Configure', 'Delivery Groups' is highlighted. A sidebar on the left shows a list of options for a Delivery Group, with '1 Delivery Group Info' selected. The main content area displays the 'Delivery Group Information' form, which includes fields for Name and Description.

**Delivery Group Information** ×

Enter a name for the delivery group and any information that will help you keep track of it later.

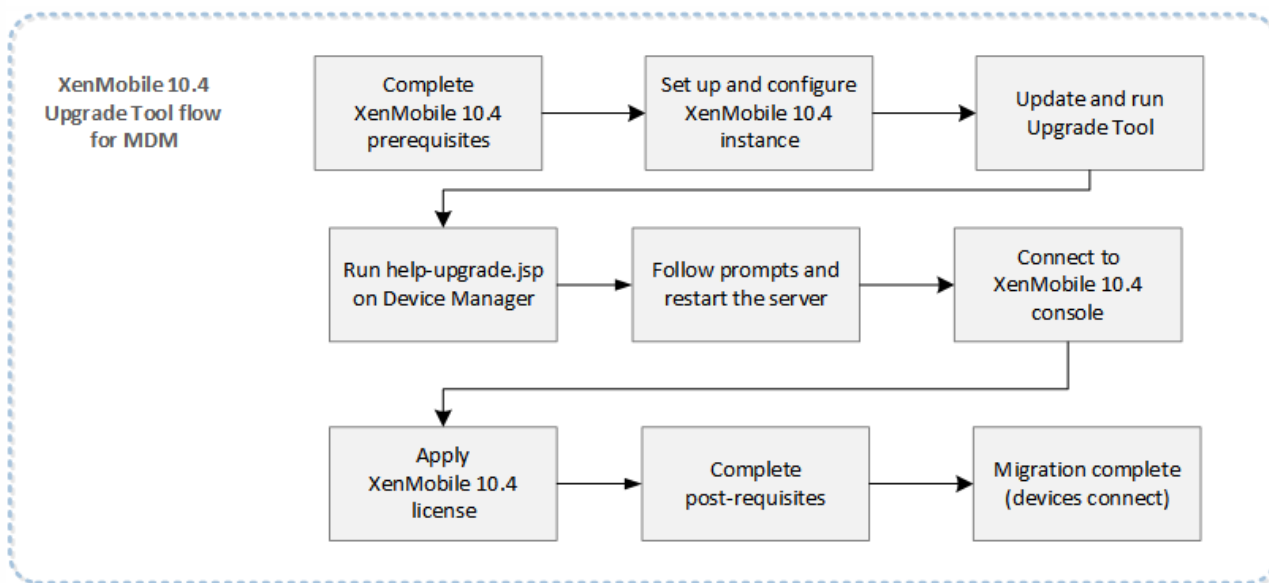
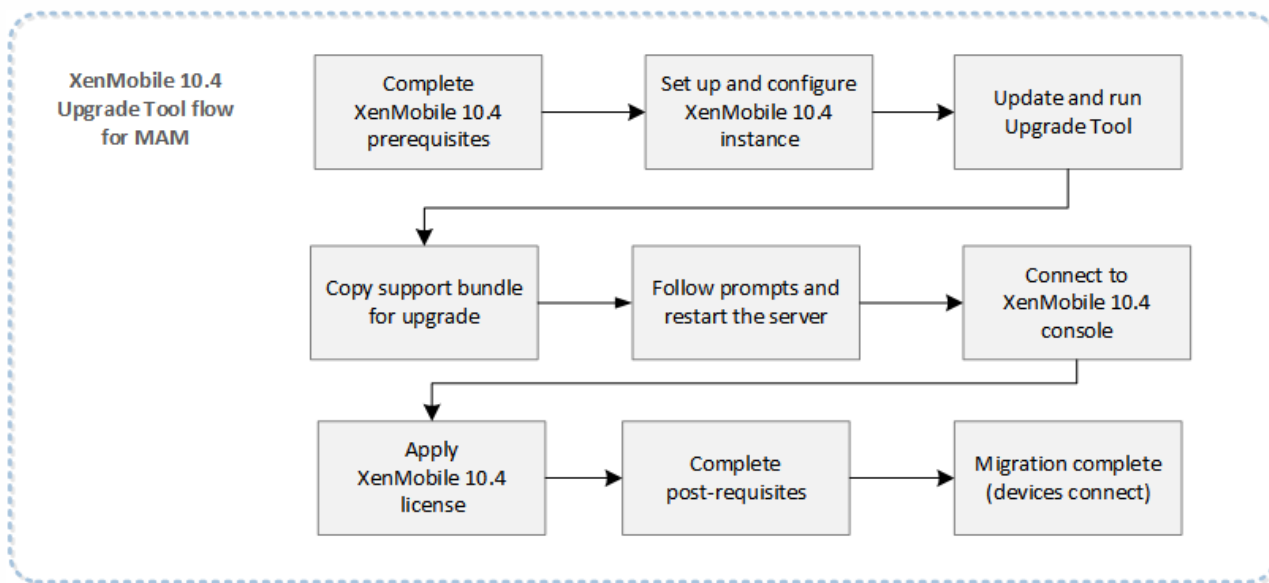
**Name**

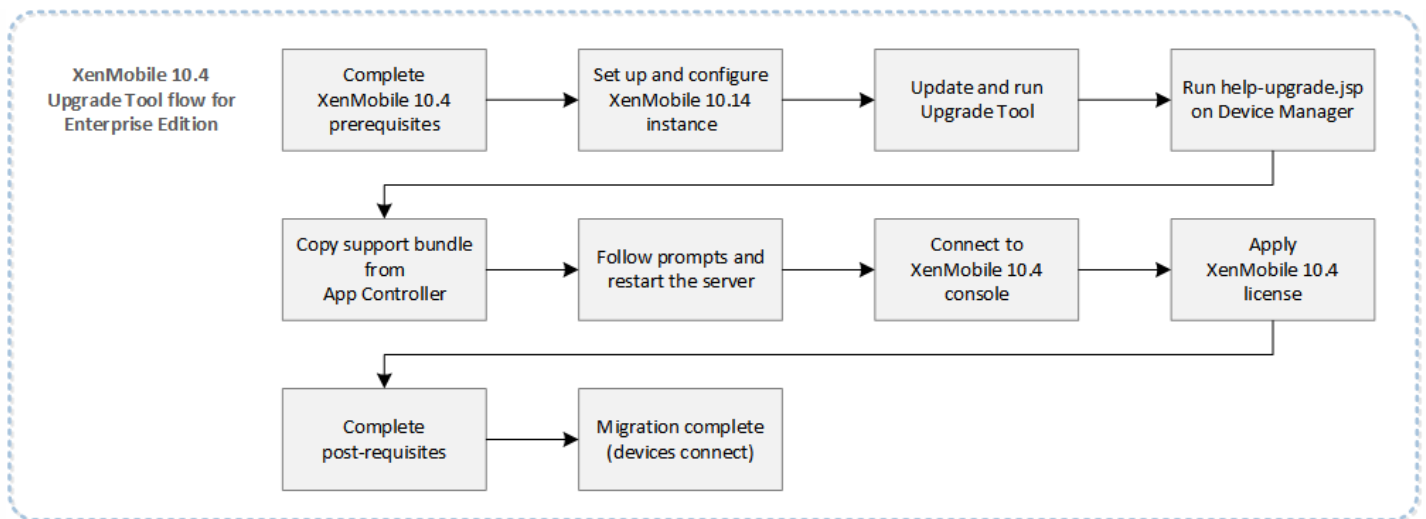
**Description**

**Delivery Group**

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile
- Enrollment Profile
- 4 Summary

次の図は、XenMobile 9.0からXenMobile 10.4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。





Windows PhoneがEnterpriseモードで登録されており、Worx Home 9.xを使用している場合、XenMobile 9.0 Enterprise環境のXenMobile 10.4へのアップグレードでは以下の手順が推奨されます。

1. Device Manager上のWorx HomeをWorx Home 10.2にアップグレードしてから、Worx Home 10.2を展開します。
2. ユーザーデバイスから手動でWorx Home 9.xをアンインストールします。
3. ユーザーに、Windows PhoneでDownload Hubにアクセスして、Device Managerで展開したWorx Home 10.2をインストールするように伝えます。
4. この記事で説明した前提条件の完了後、「[XenMobileアップグレードツールの有効化および実行](#)」の説明に従って、XenMobile 10.4へアップグレードします。
5. 「[アップグレードツールのアップグレード後要件](#)」の説明に従って、デバイスを接続するようにNetScalerを変更します。

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

App Controller管理コンソールで、[Settings] > [Release Management] の順にクリックします。[Update] をクリックして、ダウンロードしたパッチファイルを選択します。[Upload] をクリックしてApp Controllerを再起動します。

登録済みのWindowsデバイスがアップグレード後も動作するように、XenMobile 9をXenMobile 10.4にアップグレードする前にカスタムストア名をデフォルト値に戻す必要があります。詳しくは、<http://support.citrix.com/article/CTX214553>を参照してください。

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

## Beacons [Edit](#)

Store name: \*

Default store view:

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

- **NetScaler** : NetScalerをアップグレードする前に、NetScaler構成ファイル (ns.conf) のコピーを必ず保存してください。Netscalerの現在のリリースには、使いやすいクイック展開ユーティリティと、NetScalerとXenMobileを統合する手順が順を追って表示されるNetScaler for XenMobileウィザードが含まれています。詳しくは、「[XenMobile環境の設定の構成](#)」および「[FAQ: XenMobile 10 and NetScaler 10.5 Integration](#)」を参照してください。
- **ファイアウォールのポート** : 新しいXenMobile 10.4サーバーのIPに対して開放するファイアウォールのポートはXenMobile 9.0サーバーのIPに対して開放するポートと同様です。XenMobile 10.4のポートの要件については、「[ポート要件](#)」を参照してください。
- **LDAPサーバー** : 新しいXenMobile 10.4サーバーが1つまたは複数のLDAPサーバーに接続していることを確認します。サーバーを再起動するとき、アップグレード後のLDAPサーバーへの有効なルートがある必要があります。

次の表は、実行できるデータベースの移行オプションを示しています。システム要件については、[XenMobile 10.4のデータベース要件](#)」を参照してください。

XenMobile 9.0から

XenMobile 10.4へ

### Enterprise Edition

#### App Controller

#### MDM

ローカルのPostgreSQL

ローカルのPostgreSQL

ローカルのPostgreSQL

ローカルのPostgreSQL

MS SQL

MS SQL

ローカルのPostgreSQL

リモートのPostgreSQL

リモートのPostgreSQL

### App Edition

ローカルのPostgreSQL

ローカルのPostgreSQL

ローカルのPostgreSQL

リモートのPostgreSQL

ローカルのPostgreSQL

MS SQL

## MDM Edition

ローカルのPostgreSQL

ローカルのPostgreSQL

MS SQL

MS SQL

リモートのPostgreSQL

リモートのPostgreSQL

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

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

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

1. ファイルpg\_hba.confを開き、次の行を検索します。

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

2. すべてのIPアドレスを許可するには、この行を次のように変更します。

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

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

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

3. ファイルを保存します。
4. サービスを停止してから開始します。
5. postgresql.confファイルを開き、次の行を検索します。

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

6. 行を次のように変更します。

```
listen_addresses = '*'
```

7. PostgreSQLサービスを停止して起動し、変更を適用します。

カスタムポートがデータベースソリューションに割り当てられている場合、XenMobile 9.0 Device Managerのファイアウォール保護でそのポートが許可されて開いている必要があります。こうすることで、XenMobile 10.4がデータベースに接続し、必要な情報を移行できるようになります。

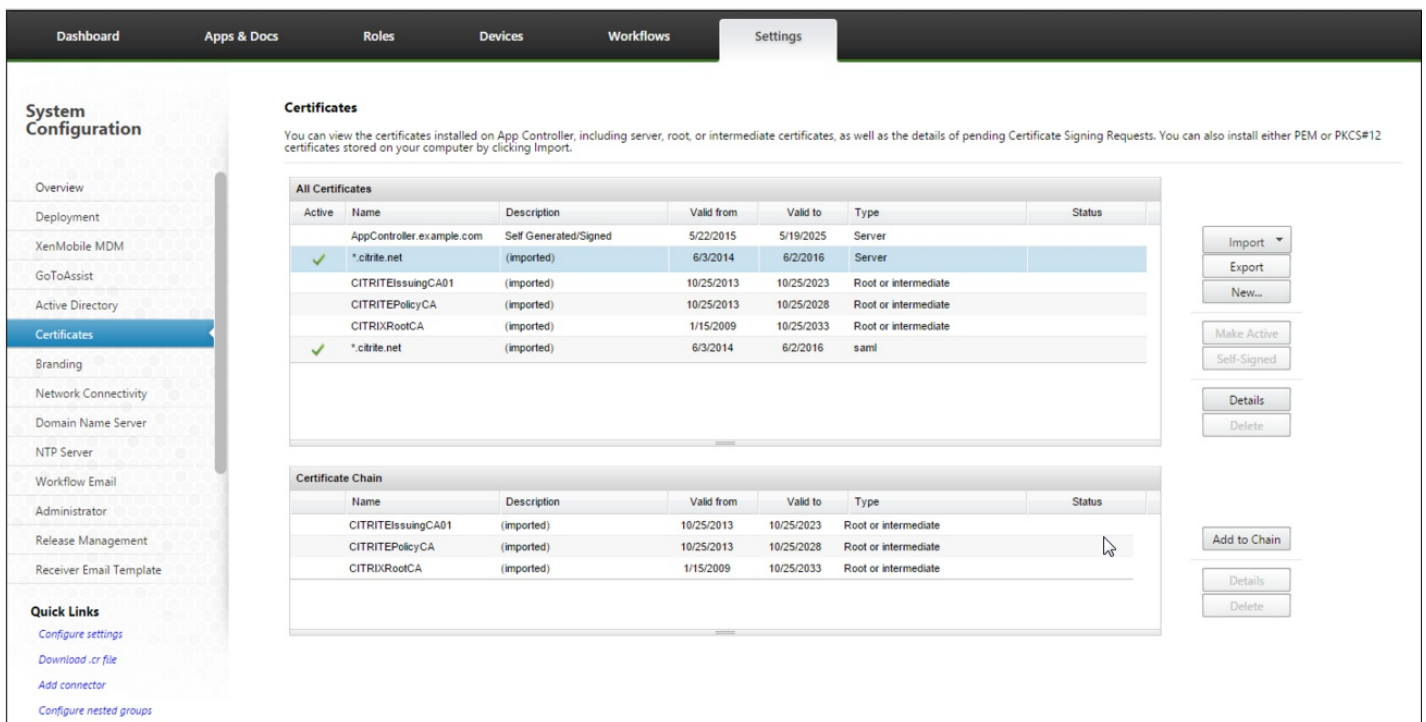
特殊文字 (!、\$, (), #、%、+、\*、~、?、|、{}、および[]) を含むXenMobile 9.0の展開パッケージ名はアップグレードされ

ますが、アップグレード後にXenMobile 10.4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。アップグレード前に、展開パッケージ名からすべての特殊文字を削除して、ローカルユーザーおよびローカルグループの名前から開き角かっこを削除します。

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

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

1. XenMobile 9.0 App Controllerにログオンして **[Certificates]** をクリックします。
2. 証明書一覧でエクスポートするサーバー証明書をクリックし、**[エクスポート]** をクリックします。



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



The screenshot shows the Citrix System Configuration interface. The 'Certificates' section is active, displaying a list of certificates and a 'Certificate Chain' table. An 'Export Certificate' dialog box is open, prompting for a password and confirmation password.

**System Configuration**

- Overview
- Deployment
- XenMobile MDM
- GoToAssist
- Active Directory
- Certificates**
- Branding
- Network Connectivity
- Domain Name Server
- NTP Server
- Workflow Email
- Administrator
- Release Management
- Receiver Email Template

**Quick Links**

- [Configure settings](#)
- [Download .cr file](#)
- [Add connector](#)
- [Configure nested groups](#)

**Certificates**

You can view the certificates installed on App Controller, including server, root, or intermediate certificates, as well as the details of pending Certificate Signing Requests. You can also install either PEM or PKCS#12 certificates stored on your computer by clicking Import.

**All Certificates**

Active	Name	Description	Status
	AppController.example.com	Self Ge	
✓	*.citrix.net	(import	
	CITRITeIssuingCA01	(import	intermediate
	CITRITePolicyCA	(import	intermediate
	CITRIXRootCA	(import	intermediate
✓	*.citrix.net	(import	

**Export Certificate**

Password: \* [.....]

Confirm Password: \* [.....]

Buttons: Ok, Close

**Certificate Chain**

Name	Description	Valid from	Valid to	Type	Status
CITRITeIssuingCA01	(imported)	10/25/2013	10/25/2023	Root or intermediate	
CITRITePolicyCA	(imported)	10/25/2013	10/25/2028	Root or intermediate	
CITRIXRootCA	(imported)	1/15/2009	10/25/2033	Root or intermediate	

Buttons: Import, Export, New..., Make Active, Self-Signed, Details, Delete, Add to Chain, Details, Delete

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

# XenMobileアップグレードツールの有効化および実行

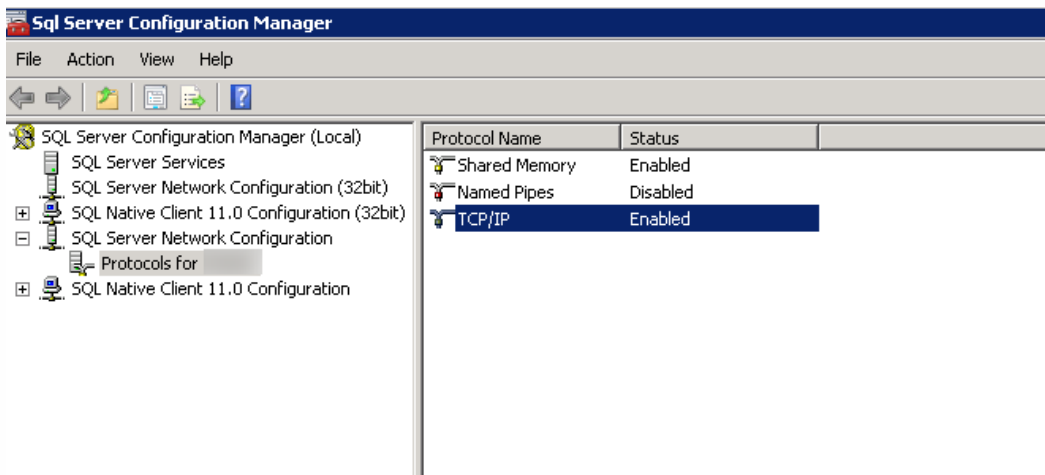
Apr 27, 2017

XenMobile 9環境が次の前提条件を満たす場合、アップグレードの前にこのセクションの手順を実行します。

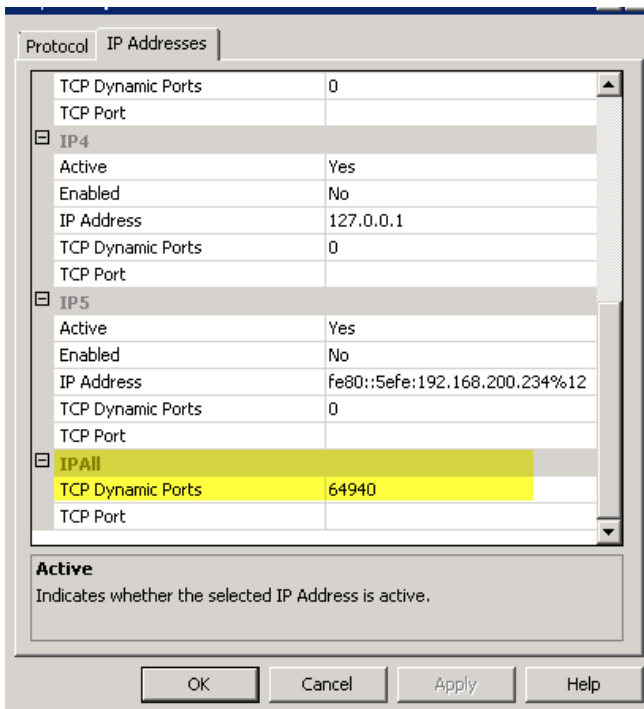
- XenMobile 9 MDM EditionまたはEnterprise Editionには外部SQL Serverデータベースがあります。
- 非デフォルトの名前付きインスタンスでSQL Serverデータベースが実行されます。
- SQL Server名前付きインスタンスが静的または動的TCPポートをリスンします。次の図にあるように、名前付きインスタンスのTCP/IPプロトコルのIPアドレスを見て、この前提条件を確認できます。

## 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、通常ファイア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。

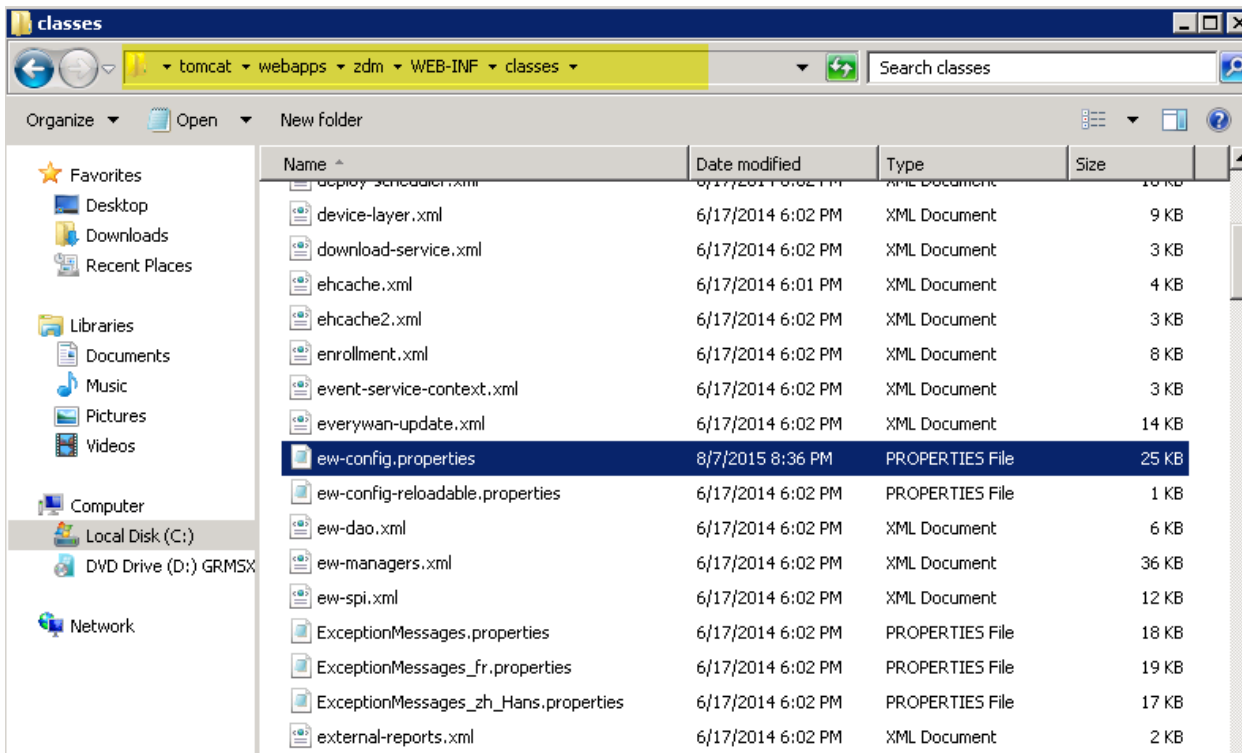


TCP/IP Properties ? | X



## 事前アップグレード手順

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:jt ds:sqlserver:///;instance=

audit.datasource.url=jdbc:jt ds:sqlserver:///;instance=

```
ew-config.properties
18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jt ds:sqlserver://localhost:1433/everwyan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jt ds:sqlserver://localhost/everwyan;instance=SQLEXPRESS
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jt ds:sqlserver://localhost/everwyan;instance=SQLEXPRESS;domain=sparus-
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everwyan/everwyan@//localhost:1521/everwyan
22 pooled.datasource.url=jdbc:jt ds:sqlserver://ah-234 .net/ -llaug;instance=
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234. .net
25 # Pooled datasource database
26 pooled.datasource.database=-llaug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everwyan01
31 pooled.datasource.password={aes} ==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/everwyan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everwyan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everwyan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jt ds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jt ds:sqlserver://ah-234 / -llaug;instance=
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234 .net
48 # Audit datasource database
49 audit.datasource.database=-llaug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password
```

3. 前のURLからインスタンス名を削除して、ポートおよびSQL Server FQDN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:jt ds:sqlserver:// :64940/

audit.datasource.url=jdbc:jt ds:sqlserver:// :64940/

## 注意

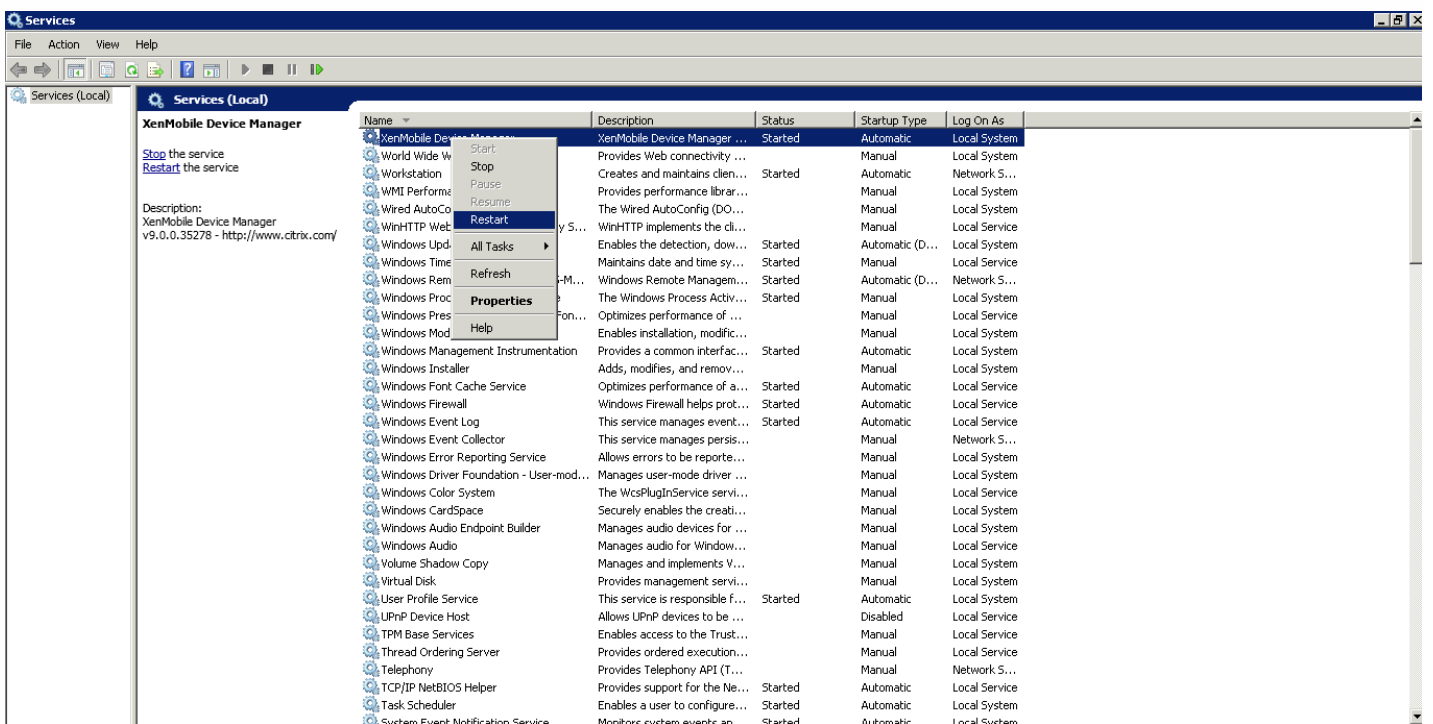
ew-config.propertiesファイルで加える変更内容のバックアップ、コピー、またはメモの作成をお勧めします。この情報は、アップグレードに失敗した場合に有用です。

```

18 # For Microsoft SQL server url1: pooled.datasource.url=jdbc:jtds:sqlserver://localhost:1433/verywan
19 # For Microsoft SQL server url1 with a named instance (url2): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress
20 # For Microsoft SQL server url2 with a Windows authentication (NTLM): pooled.datasource.url=jdbc:jtds:sqlserver://localhost/verywan;instance=SQLExpress;domain=sparus-s
21 # Oracle url: pooled.datasource.url=jdbc:oracle:thin:everywan/everywan@localhost:1521/verywan
22 pooled.datasource.url=jdbc:jtds:sqlserver://ah-234. net: -llaug
23 # Pooled datasource host name
24 pooled.datasource.hostname=ah-234. .net
25 # Pooled datasource database
26 pooled.datasource.database=-llaug
27 # Pooled datasource user
28 pooled.datasource.user=sa
29 # Pooled datasource password
30 # For Microsoft SQL server (10 characters minimum) ex: pooled.datasource.password=everywan01
31 pooled.datasource.password=(aes) ==
32
33 # No pooled datasource driver
34 #no.pooled.datasource.driver=org.postgresql.Driver
35 # No pooled datasource url
36 #no.pooled.datasource.url=jdbc:postgresql://localhost:5432/verywan
37 # No pooled datasource user
38 #no.pooled.datasource.user=everywan
39 # No pooled datasource password
40 #no.pooled.datasource.password=everywan
41
42 # Audit datasource driver
43 audit.datasource.driver=net.sourceforge.jtds.jdbc.Driver
44 # Audit datasource url
45 audit.datasource.url=jdbc:jtds:sqlserver:// -inc.net: -llaug
46 # Audit datasource host name
47 audit.datasource.hostname=ah-234. .net
48 # Audit datasource database
49 audit.datasource.database=-llaug
50 # Audit datasource user
51 audit.datasource.user=sa
52 # Audit datasource password

```

4. Device Managerサービスを再起動します。Device Managerインスタンスの再起動後、デバイス接続を更新します。



5. 新しいXenMobile 10.x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である場合、静的ポートに変換することをお勧めします。アップグレード時に、データベースセットアップの以下の部分が表示されたら、新しいXenMobileサーバーで静的ポートを構成します。

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

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

これで、アップグレードを実行できるようになりました。

システムがクラスターモードで構成されている場合：

1. まずアップグレードするもの以外のすべてのノードをシャットダウンします。ノードをシャットダウンするには、**[Settings]** をコマンドラインインターフェイスで使用します。
2. 次の「アップグレードツールを有効にして実行するには」に従って、実行中のノードをアップグレードします。
3. 最初のアップグレードが予期したとおりにアップグレードされたことを確認した後、残りのノードの各々を1つずつ再結合します。再結合するには：

- a. ノードを再起動します。
- b. メッセージが表示された場合、ノードをアップグレードしないでください。
- c. クラスターデータベースにノードを結合します。

クラスターに再結合されたノードは、XenMobileにより自動的にアップグレードされます。

4. 各ノードをクラスターに再結合した後、各ノード上ですべてのアップグレード後要件のタスクを実行します。

XenMobile 10.4を初めてインストールするときにコマンドラインインターフェイス（CLI）からアップグレードツールを有効にします。

## Important

システムのスナップショットを取得する場合は、XenMobile 10.4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。

1. CLIで、管理者のユーザー名、パスワード、およびネットワーク設定を入力します。
2. 「y」と入力して設定を確定します。

```
*****
*      Citrix XenMobile      *
*      (in First Time Use mode)  *
*****

Welcome to the XenMobile First Time Use wizard. This wizard guides you through the
initial configuration of XenMobile. Accept options offered by pressing Enter/
Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the c
ommand prompt.
Username: admin
New password:
Re-enter new password:

Network settings:
IP address [1]: 10.207.87.35
Netmask [1]: 255.255.254.0
Default gateway [1]: 10.207.86.1
Primary DNS server [1]: 10.207.86.50
Secondary DNS server (optional) [1]: 10.207.86.51

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

3. 「y」と入力してアップグレードします。

## 注意

ここで「y」を選択しない場合、新しいXenMobile 10.4のインスタンスをコマンドラインコンソールで構成し、アップグレードツールを再開する必要があります。

4. ランダムなパスフレーズを生成するかどうかと、任意でFIPSを有効にするかどうかを選択します。データベース接続情報を入力します。

5. 「y」と入力して設定を確定します。

```
Commit settings (y/n) [y]:
Applying network settings...

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

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

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

Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:
Server [1]: sql01.xmlab.net
Port [1433]:
Username [sa]: xmsadmin
Password:
Database name [DB_service]: migdemo

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

XenMobileによりデータベースが初期化されます。

```
Checking database status...
Database does not exist.
Initializing database...
```

6. サーバーのクラスター化を有効にするかどうかを選択します。XenMobileの完全修飾ドメイン名 (FQDN) を入力します。以下の点に注意してください。

- XenMobile Enterprise Editionの展開では、FQDNはXenMobile 9.0 MDMのFQDNと同じです。
- MAMの展開では、FQDNはXenMobile 9.0 App ControllerのFQDNと同じです。
- MDMの展開では、FQDNはXenMobile 9.0 Device ManagerのFQDNと同じです。

## Important

9.0環境用と10.4環境用のFQDNは一致していなければなりません。

```
Cluster:
Please press y to enable cluster? [y/n]: y
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu, once the system configuration is complete.

Xenmobile Server FQDN:
Hostname []: migdemo.xs.citrix.com

Commit settings (y/n) [y]:
Applying fqdn settings...
```

7. 「y」と入力して設定を確定します。

8. 通信ポートを設定します。

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

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

9. 「y」と入力して設定を確定します。

10. すべての証明書に同じパスワードを使用するかどうかを選択し、証明書に使用するパスワードを入力します。

11. 「y」と入力して設定を確定します。



```
Applying port listener configuration...

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
- A Node Identification certificate for cluster node client auth
Do you want to use the same password for all the certificates of the PKI [y]:
New password:
Re-enter new password:

Commit settings (y/n) [y]:
Generating SAML signing certificate...
Generating server and client certificates...

XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]:
```

12. XenMobileコンソール管理者のユーザー名とパスワードを入力します。

13. 「y」と入力して設定を確定します。

XenMobile 10.4で1回のみアップグレードツールが有効になります。

```
Re-enter new password:

Commit settings (y/n) [y]: y
Creating console administrator...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

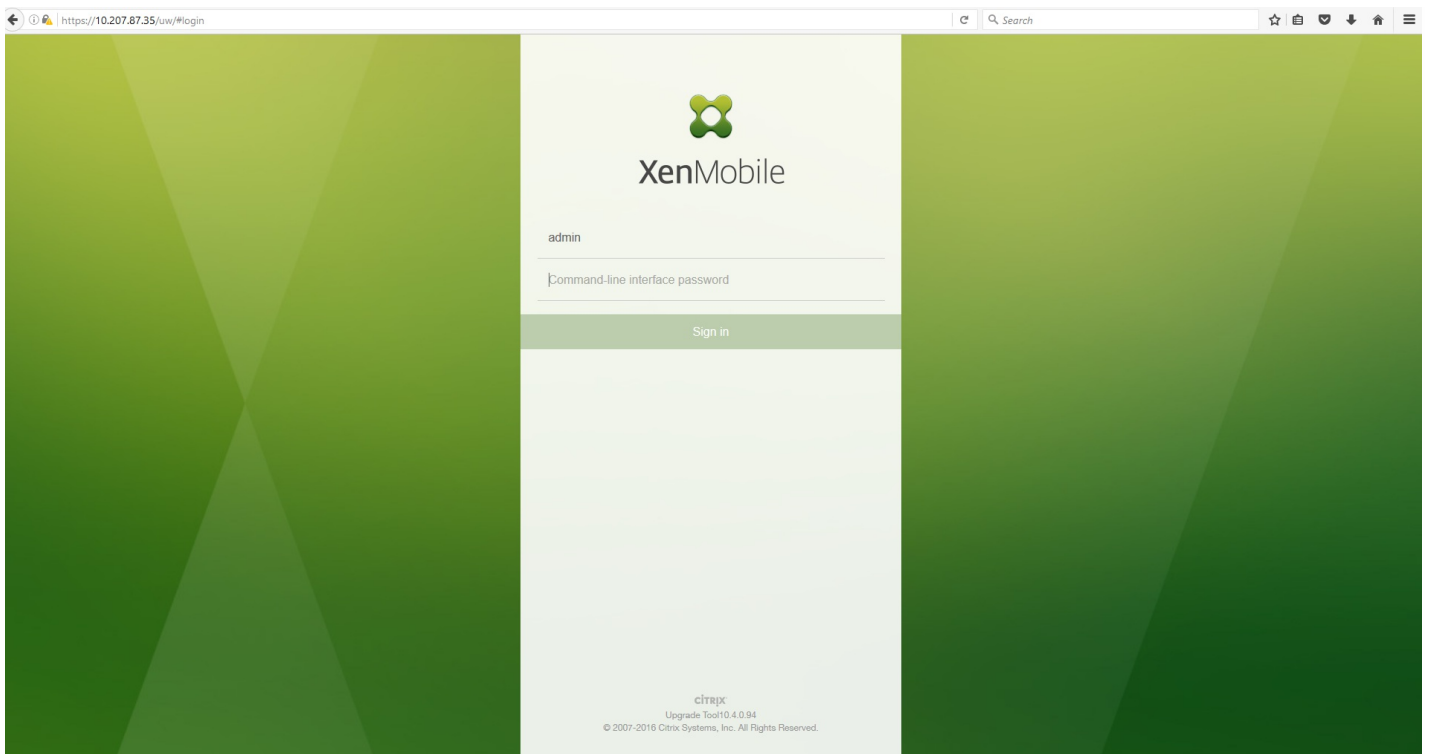
Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds.....
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  not ready to start yet [ OK ]

To complete the upgrade process, from a web browser, go to the following
location and log on with your command prompt credentials:
https://10.207.87.35/uw/

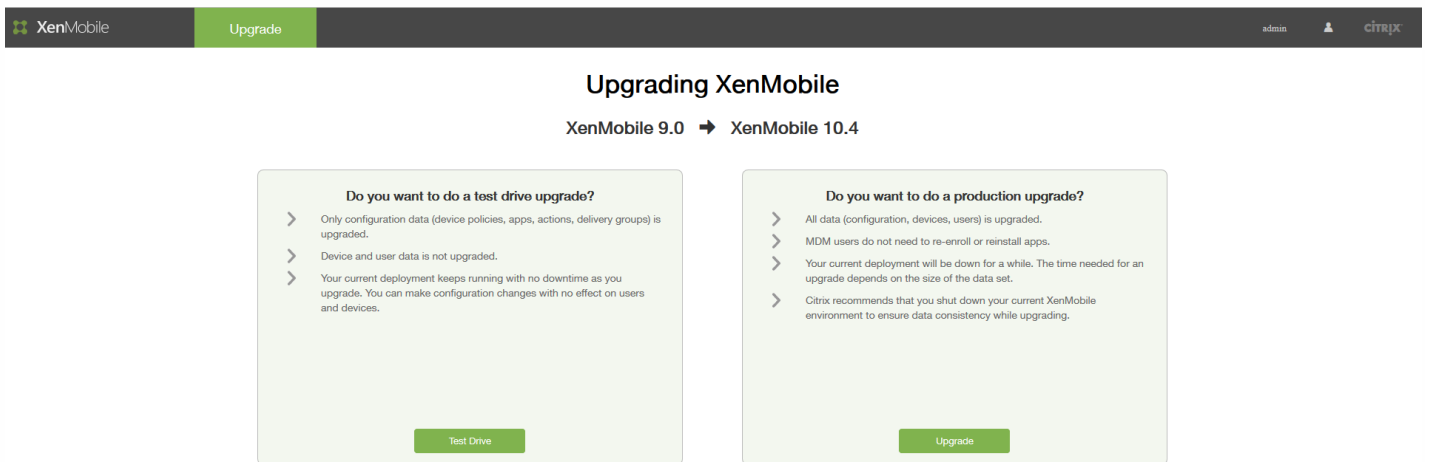
Starting monitoring... [ OK ]

migdemo.xs.citrix.com login:
```

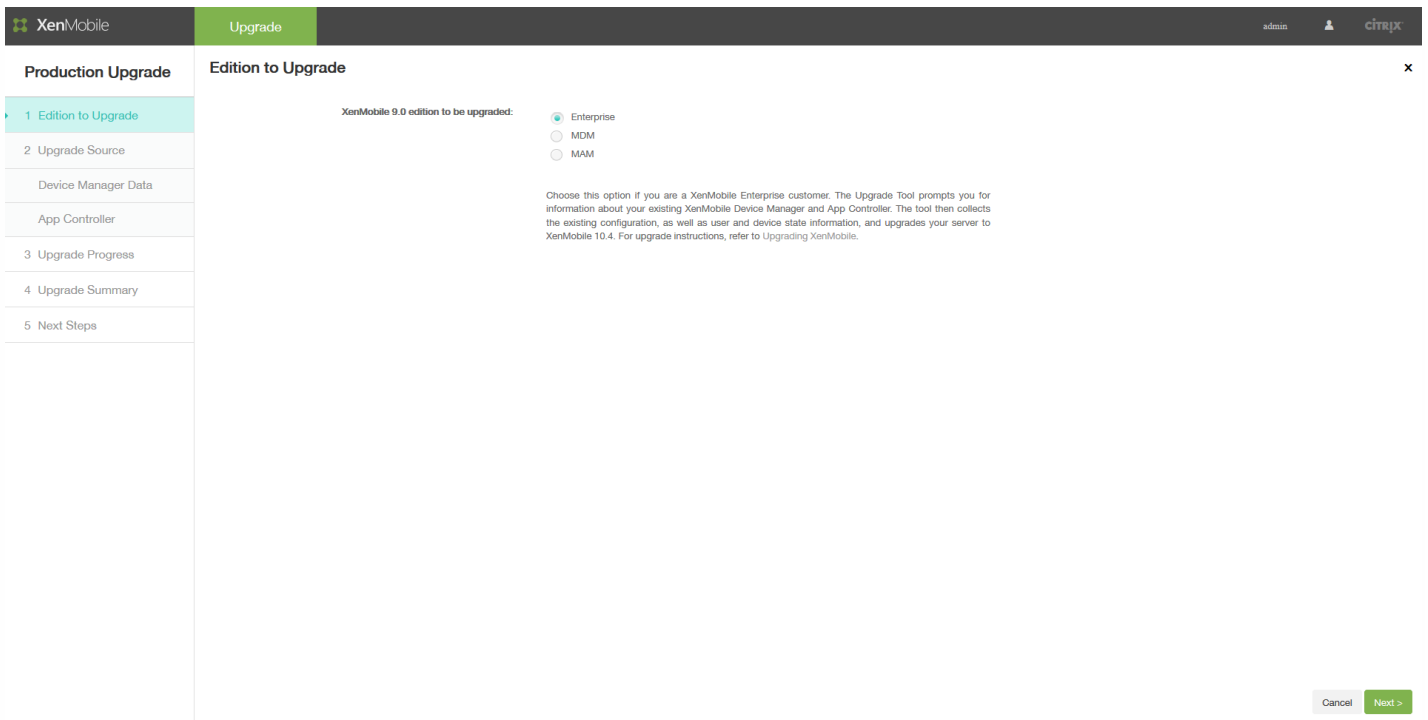
14. Webブラウザに「https://uw/」と入力してアップグレードツールにアクセスし、CLIを使用して指定した資格情報を使用してログインします。



15. これで、体験版アップグレードと実稼働環境のアップグレードを選択できるようになりました。以下の手順は、実稼働環境のアップグレードの場合のものです。【Upgrading XenMobile】ページで、【Upgrade】をクリックします。



16. 【Edition to Upgrade】ページで、お使いのエディションを選択します。次の画面例は、Enterpriseエディションを選択した状態を示しています。



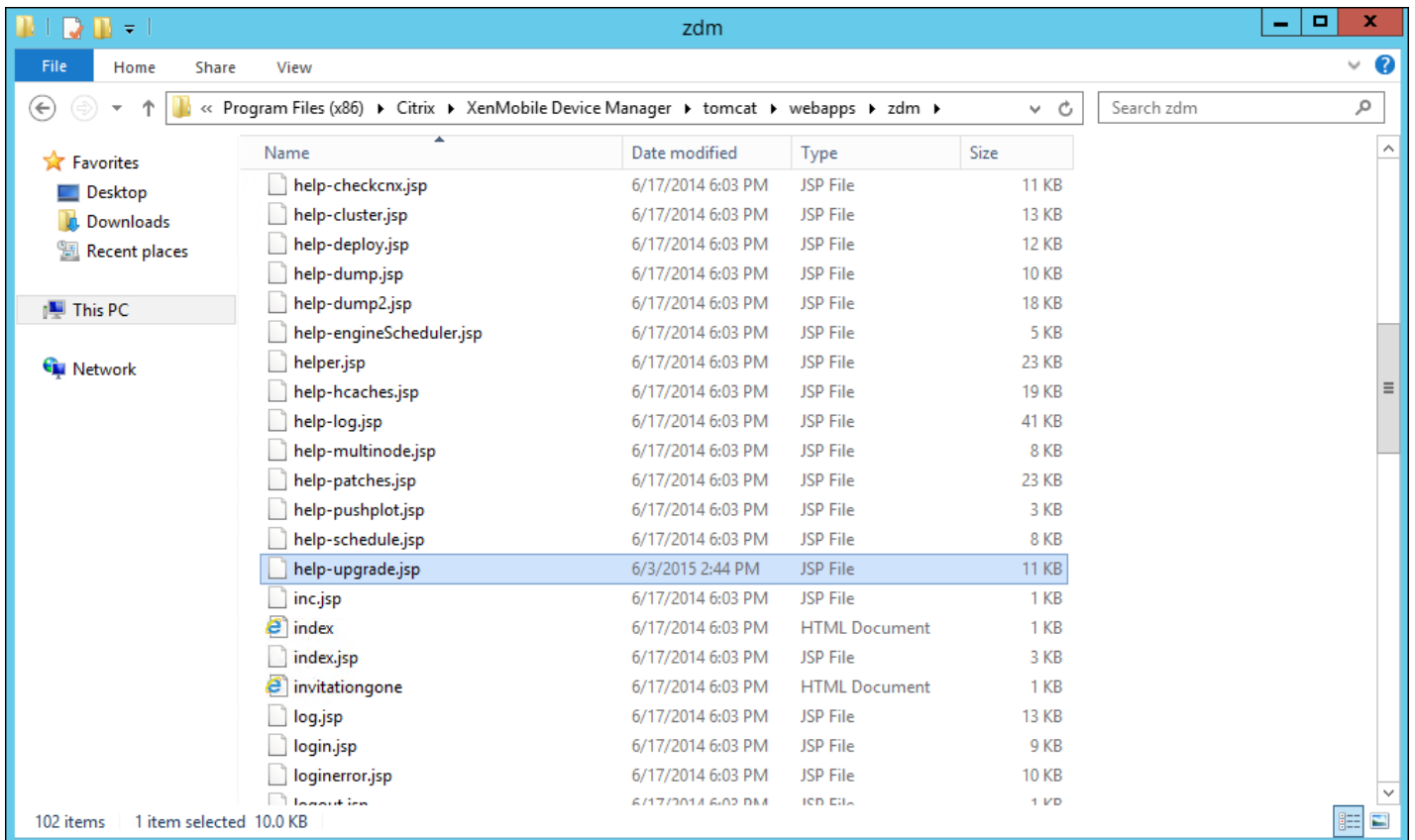
17. [Next] をクリックします。

EnterpriseまたはMDMエディションをアップグレードする場合、[Device Manager] ページが表示されます。手順18~22を実行して、このページを完了します。

MAMエディションをアップグレードする場合は、手順23にスキップして [App Controller] ページを完了します。

18. 既存のXenMobile 9.0 Device Managerのデータを移行するために必要なファイルを収集します。また、データベースURLおよびユーザー名をコピーして、 [Device Manager] ページに貼り付けます。

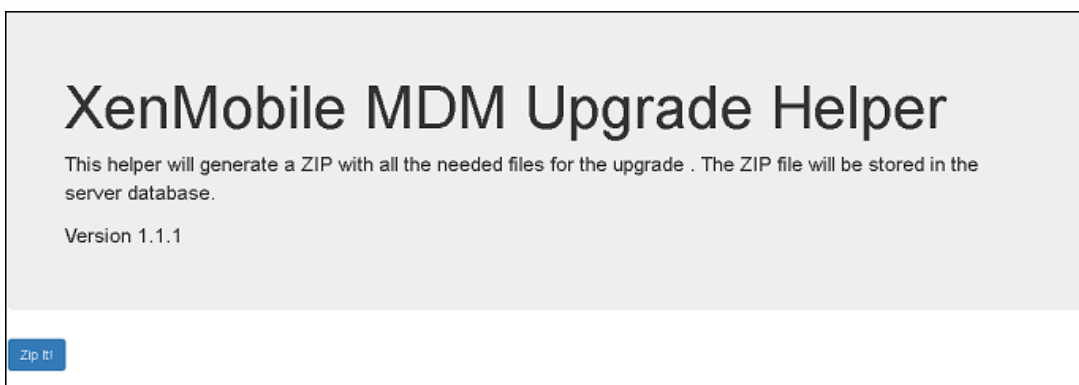
- a. [Device Manager] ページの手順1のリンクをクリックして、help-upgrade.zipファイルをダウンロードして保存します。
- b. help-upgrade.jspファイルを既存のXenMobile 9.0 Device Managerの\tomcat\webapps\zdmに展開します。



c. ブラウザーウィンドウでXenMobile 9.0サーバーにログインします。

d. 別のブラウザータブで「<https://localhost/zdm/help-upgrade.jsp>」と入力します。これにより [XenMobile MDM Upgrade Helper] ページが開きます。ここでXenMobile 10.4へのアップグレードに必要なXenMobile 9.0のすべてのファイルを収集してzipファイルに圧縮します。zipファイルは展開した場所からサーバーデータベースに保存されます。

e. [Zip it] をクリックし、画面の指示に従ってアップグレードに必要なファイルを収集します。



19. [Result] のURLをコピーして、アップグレードツールの [Device Manager] ページにある [Database URL] フィールドに貼り付けます。次に、ユーザー名をコピーして、 [Device Manager] ページに貼り付けます。

# XenMobile MDM Upgrade Helper

This helper will generate a ZIP with all the needed files for the upgrade . The ZIP file will be stored in the server database.

Version 1.1.1

ZIP successfully stored in database !

## Result

jdbc:mysql://server:/ copy

username=admin copy

20 アップグレードツールで次の操作を行います。

- パスワードを入力して、 **[Validate Connection]** をクリックします。
- 各証明書のパパスワードを入力して、 **[Validate Password]** をクリックします。

XenMobile Upgrade

Production Upgrade

1 Edition to Upgrade ✓

2 Upgrade Source

Device Manager Data

App Controller

3 Upgrade Progress

4 Upgrade Summary

5 Next Steps

Device Manager

Follow these steps to collect the files you need to move your XenMobile 9.0 Device Manager data to XenMobile 10.4.

- Download the latest [help-upgrade.jsp](#).
- Add the downloaded file to this location (-MDM\_Install\_Path>tomcat/webapps/zdm) on your existing XenMobile 9.0 Device Manager.
- Open your browser on the XenMobile 9.0 Device Manager and then access the following URL: <https://cxdm FQDN or IP>/zdm/help-upgrade.jsp>. Keep that page open throughout the upgrade process, as you will need to refer to it more than once.
- From the Upgrade Helper page that displays, copy the database URL and user name into the fields below. After you complete your entries, click Validate Connection. If the connection validates, continue with certificate validation.

Database URL \*

User name

Password

✓

Use the same password for all certificates

Root certificate password

Server certificate password

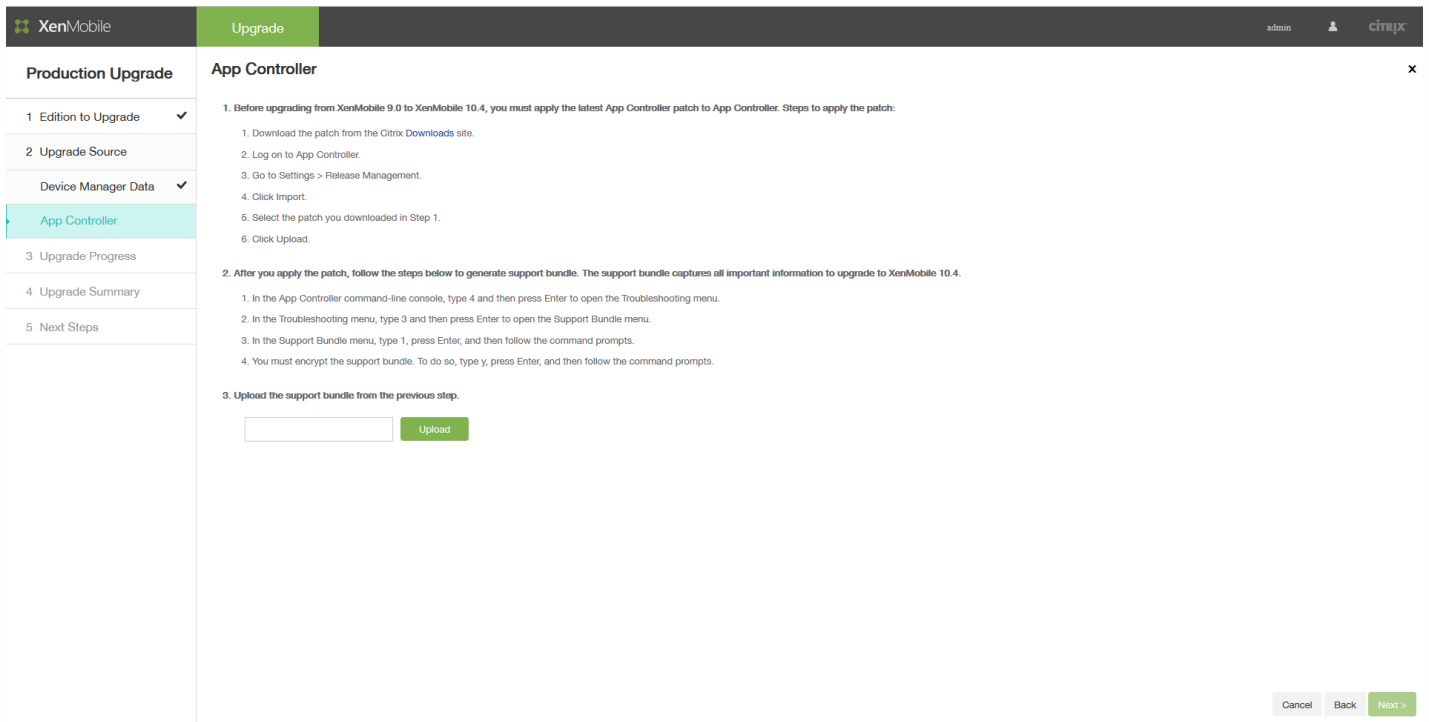
✓

21. **[Next]** をクリックします。

22. ew-config.propertiesファイルを変更した場合、XenMobile 9 MDM上でxdmサービスを再起動し、<https://localhost/zdm/help-upgrade.jsp>に移動してzipを再実行します。そうするとew-config.propertiesファイルが再度読み込まれ、移行に備えてXenMobile MDM 9データベースに保存されます。

23. 次に、App Controllerにアップグレードパッチを適用してから、サポートバンドルを生成してアップロードします。ま

ず、 [App Controller] ページのセクション1の手順に従ってApp Controllerをアップグレードします。



The screenshot shows the XenMobile Upgrade interface. The top navigation bar includes 'XenMobile', 'Upgrade', and 'admin'. The left sidebar lists 'Production Upgrade' steps: 1. Edition to Upgrade, 2. Upgrade Source, Device Manager Data, App Controller (selected), 3. Upgrade Progress, 4. Upgrade Summary, and 5. Next Steps. The main content area is titled 'App Controller' and contains two sections of instructions. Section 1, 'Before upgrading from XenMobile 9.0 to XenMobile 10.4, you must apply the latest App Controller patch to App Controller. Steps to apply the patch:', lists six steps: 1. Download the patch from the Citrix Downloads site, 2. Log on to App Controller, 3. Go to Settings > Release Management, 4. Click Import, 5. Select the patch you downloaded in Step 1, and 6. Click Upload. Section 2, 'After you apply the patch, follow the steps below to generate support bundle. The support bundle captures all important information to upgrade to XenMobile 10.4.', lists four steps: 1. In the App Controller command-line console, type 4 and then press Enter to open the Troubleshooting menu, 2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu, 3. In the Support Bundle menu, type 1, press Enter, and then follow the command prompts, and 4. You must encrypt the support bundle. To do so, type y, press Enter, and then follow the command prompts. Below these instructions is an 'Upload' button. At the bottom right, there are 'Cancel', 'Back', and 'Next >' buttons.

25. [App Controller] ページのセクション2の手順を続行します。

a. App Controllerのコマンドラインコンソールで「4」と入力してEnterキーを押すと、 [Troubleshooting] メニューが開きます。

```
AppController 9.0.0.973502, 2015-05-26
-----
Main Menu
-----
[0] Express Setup
[1] High Availability
[2] Clustering
[3] System
[4] Troubleshooting
[5] Help
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] █
```

[Troubleshooting] メニューで「3」と入力してEnterキーを押すと、 [Support Bundle] メニューが開きます。

```
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] 3
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----
Choice: [0 - 4] █
```

c. [Support Bundle] メニューで「1」と入力してEnterキーを押し、コマンドプロンプトの指示に従います。

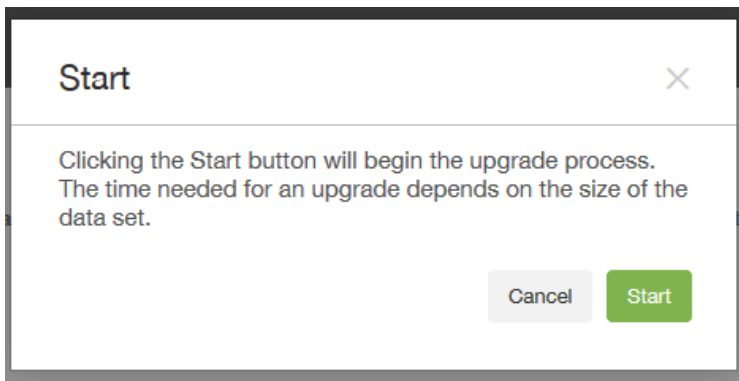
注：サポートバンドルは暗号化する必要があります。

```
[6] Log Out
-----
Choice: [0 - 6] 4
-----
Troubleshooting Menu
-----
[0] Back to Main Menu
[1] Network Utilities
[2] Logs
[3] Support Bundle
-----
Choice: [0 - 3] 3
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
-----
Choice: [0 - 4] 1
```

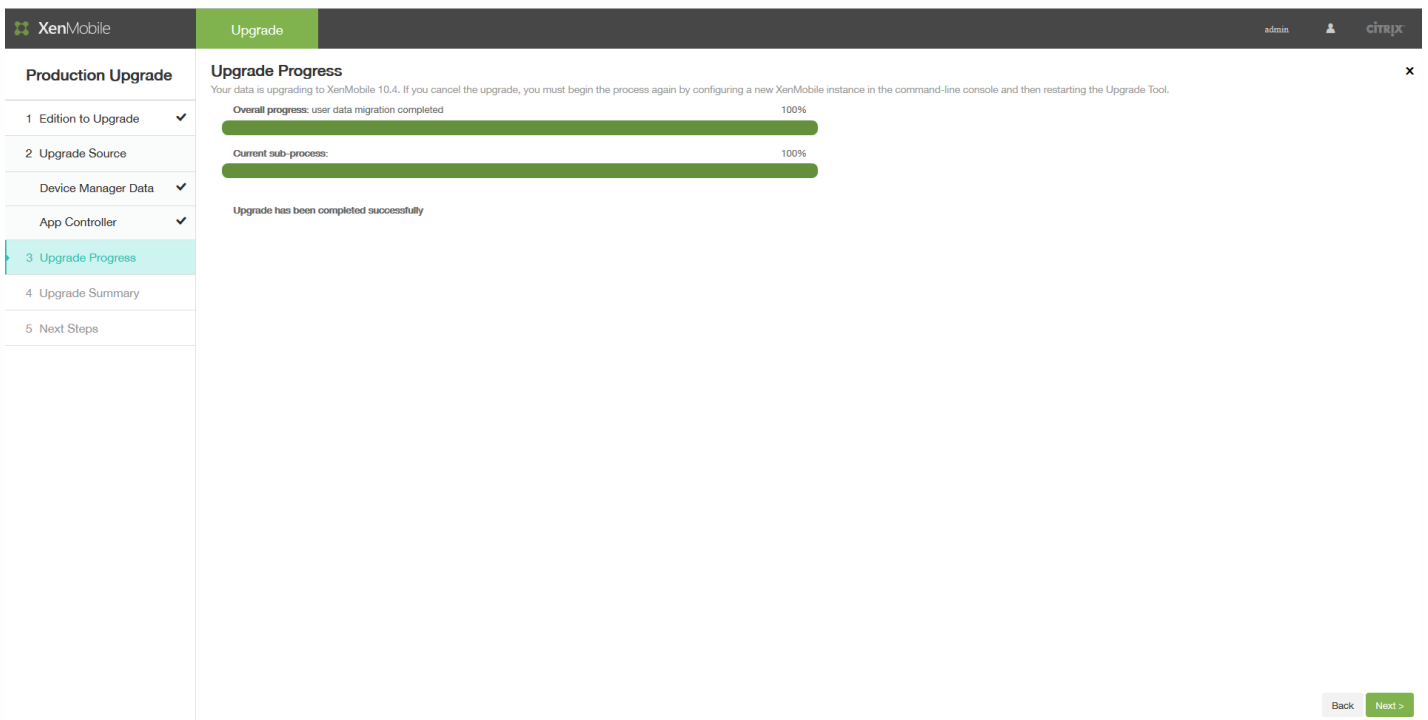
26. [App Controller] ページのセクション3で、サポートバンドルを指定して[Upload] をクリックします。

アップグレードツールにより収集したファイル（XenMobile Enterprise EditionとXenMobile MAM Editionの場合）およびサポートバンドルが処理されます。ユーザー数が多いとこの手順に15分以上かかる場合があります。

27. [Next] をクリックします。[Start] 確認ダイアログボックスが開きます。



28. [Start] をクリックします。[Upgrade Progress] ページには、XenMobile 9.0からのデータアップグレードの進行状況を示すインジケータが表示されます。アップグレードが完了すると進行状況のインジケータが100%になり、[Next] ボタンが有効になります。



## 注意

アップグレードが失敗した場合、ログでエラーの原因を確認することができます。そして、新しいXenMobile 10.4インスタンスをインポートして、アップグレード処理を再度開始する必要があります。Webブラウザの [戻る] ボタンをクリックして前のページに戻り、情報を修正することはできません。

アップグレードが正常に完了すると、[Upgrade Progress] ページにその旨が表示されます。

29. [Next] をクリックします。[Upgrade Summary] ページが開きます。

EnterpriseまたはMAMエディションをアップグレードする場合、[Upgrade Summary] ページに次のように表示されることがあります。



**XenMobile** Upgrade admin citrix

**Production Upgrade** Upgrade Summary

Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Upgrade log

1 Edition to Upgrade	✓
2 Upgrade Source	
Device Manager Data	✓
App Controller	✓
3 Upgrade Progress	✓
4 Upgrade Summary	
5 Next Steps	

Devices Upgraded	5
Apps Upgraded	46
Users Upgraded	323
Delivery Groups Upgraded	12
Policies Upgraded	44
Smart Actions Upgraded	0

Cancel Back Next >

MDMエディションをアップグレードする場合、[Upgrade Summary] ページに次のように表示されることがあります。

**XenMobile** Upgrade admin citrix

**Production Upgrade** Upgrade Summary

Review the upgrade results and debug logs to ensure that all data upgraded successfully to XenMobile 10.4. Be sure to download the log before continuing.

Upgrade log

1 Edition to Upgrade	✓
2 Upgrade Source	
App Controller	✓
3 Upgrade Progress	✓
4 Upgrade Summary	
5 Next Steps	

Devices Upgraded	604
Apps Upgraded	23
Users Upgraded	316
Delivery Groups Upgraded	5

Cancel Back Next >

30. [Upgrade log] アイコンをクリックしてログをダウンロードします。このページから移動する前に必ずログをダウンロードしてください。

ログを確認して、ポリシー、設定、ユーザーデータなどがXenMobile 10.4にアップグレードされたかどうかを確認することをお勧めします。

31. アップグレードログをダウンロードしたら、[Next] をクリックします。[Next Steps] ページが開きます。

The screenshot shows the XenMobile Upgrade interface. The top navigation bar includes the XenMobile logo, the 'Upgrade' tab, and user information (admin, Citrix). The main content area is divided into two columns. The left column, titled 'Production Upgrade', contains a list of steps: 1. Edition to Upgrade, 2. Upgrade Source, Device Manager Data, App Controller, 3. Upgrade Progress, 4. Upgrade Summary, and 5. Next Steps (highlighted in light blue). The right column, titled 'Next Steps', contains a list of instructions: 1. You must configure licenses on XenMobile 10.4 to enable user connections. To do so, go to Configure > Settings > Licensing. 2. If you deployed the server running XenMobile 9.0 in the DMZ, you must change the external DNS for XenMobile to point to the new XenMobile 10.4 server. 3. If you deployed the server running XenMobile 9.0 behind a load balancing NetScaler appliance, in NetScaler, you must configure the load balancing Device Manager instance with the new IP address for the XenMobile 10.4 server. 4. If you deploy XenMobile 10.4 in a cluster, you must use the command-line interface to enable cluster support and then join the new XenMobile nodes. Below this list is a 'Note' section with a warning icon, stating: 'Please collect support bundle from a newly upgraded XenMobile server before restarting it: 1. In the command-line console, type 3 and then press Enter to open the Troubleshooting menu. 2. In the Troubleshooting menu, type 3 and then press Enter to open the Support Bundle menu. 3. In the Support Bundle menu, type 2, press Enter to Generate support bundle. Restart the server. Go to Manage > Device and make sure all devices have been upgraded properly before making any NetScaler changes.' At the bottom right of the interface are three buttons: 'Cancel', 'Back', and 'Finish & Restart'.

上記手順について詳しくは、「[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

Apr 27, 2017

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

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

1. XenMobileでライセンスを構成して、ユーザーの接続を有効にします詳しくは、[手順](#)を参照してください。
2. XenMobile 9.0を実行しているサーバーをDMZに展開していた場合は、XenMobileの外部DNSを、新しいXenMobile 10.4サーバーを指すように変更します。
3. 負分散NetScalerアプライアンスを活用してXenMobile 9.0を実行しているサーバーを展開した場合は、NetScalerを以下のように変更します。
  - a. 新しい負分散仮想サーバーをアップグレード用に構成します。詳しくは、[手順](#)を参照してください。
  - b. App ControllerサーバーのFQDNがアップグレード用の新しいロードバランサーをポイントするようにアドレスレコードを構成します。詳しくは、[手順](#)を参照してください。
  - c. 新しいXenMobile 10.1サーバーのIPアドレスを参照するように、Device Manager負分散仮想サーバーを変更します。詳しくは、[手順](#)を参照してください。
  - d. 新しいXenMobileサーバーのFQDNを参照するようにNetScaler Gatewayを変更します。詳しくは、[手順](#)を参照してください。
  - e. 次のタスクは以下の場合にのみ必要です。
    - NetScaler for XenMobileウィザード9を、NetScaler 11.1、11.0または10.5とともに使用する場合、または
    - NetScaler Gateway 10.1を使用している場合（非推奨）、または
    - NetScaler for XenMobileウィザードを使用しないでNetScaler for XenMobile 10.5以降を構成した場合。

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

[SSLブリッジのMDM構成に基づいて、新しいMAM負分散仮想サーバーを作成する](#)

[SSLオフロードのMDM構成に基づいて、新しいMAM負分散仮想サーバーを作成する](#)

4. XenMobile 10.4をクラスターで展開する場合は、XenMobile 10.4のコマンドラインインターフェイス（CLI）を使用してクラスターのサポートを有効にし、新しいXenMobileノードに接続する必要があります。XenMobile CLIのヘルプは、「[\[Clustering\] メニューオプション](#)」を参照してください。

- 5 環境の必要に応じて、残りのアップグレード後要件を完了します。

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

XenMobile 10.4はCitrix V6ライセンスサーバーのみをサポートします。次のように、XenMobile 10.4コンソールでローカルまたはリモートのライセンス構成を設定してユーザーの接続を有効にする必要があります。

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

2. アップグレードされたXenMobile 10.4コンソールにログオンして、<https://:4443>に移動します。

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

[Settings] > [Licensing] の順に移動します。

Settings > Licensing

### Licensing

XenMobile comes with an evaluation license valid for 30 days. If you decide to use your Citrix license, you can configure it at any time. You can install your Citrix license locally or remotely on the license server.

License type: Remote license

License server\*: lic1.xmlab.net

Port\*: 27000

Test Connection

Product name	Status	Active	Total number of licenses	Number used	Type	Expires on
--------------	--------	--------	--------------------------	-------------	------	------------

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

## Important

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

XenMobile Enterprise EditionをXenMobile 10.4に実稼働環境でアップグレードした後は、XenMobile 9.0 App ControllerのFQDNに対して新しい負荷分散仮想サーバーを構成する必要があります。それには、NetScaler Gateway構成ツールを使用します。

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

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

Dashboard Configuration Reporting Documentation Downloads

Traffic Management / Load Balancing / Virtual Servers

## Virtual Servers

<input type="checkbox"/>	Name	State	Effective State	IP Address	Port
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443

2. [Add] をクリックします。

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

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Virtual Server

### Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address. You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name\*

Protocol\*

IP Address Type\*

IP Address\*

Port\*

▶ More

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

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

Dashboard Configuration Reporting Documentation Downloads

## ← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

### Basic Settings

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	● UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

### Services and Service Groups

- No Load Balancing Virtual Server Service Binding >
- No Load Balancing Virtual Server ServiceGroup Binding >**

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

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

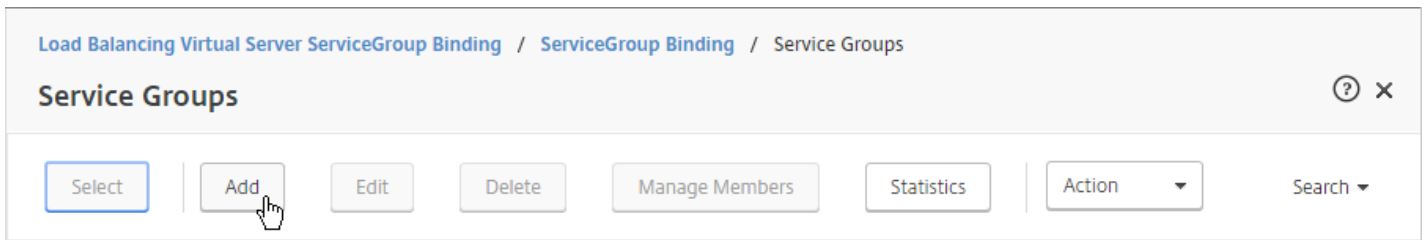
### ServiceGroup Binding

Select Service Group Name\*

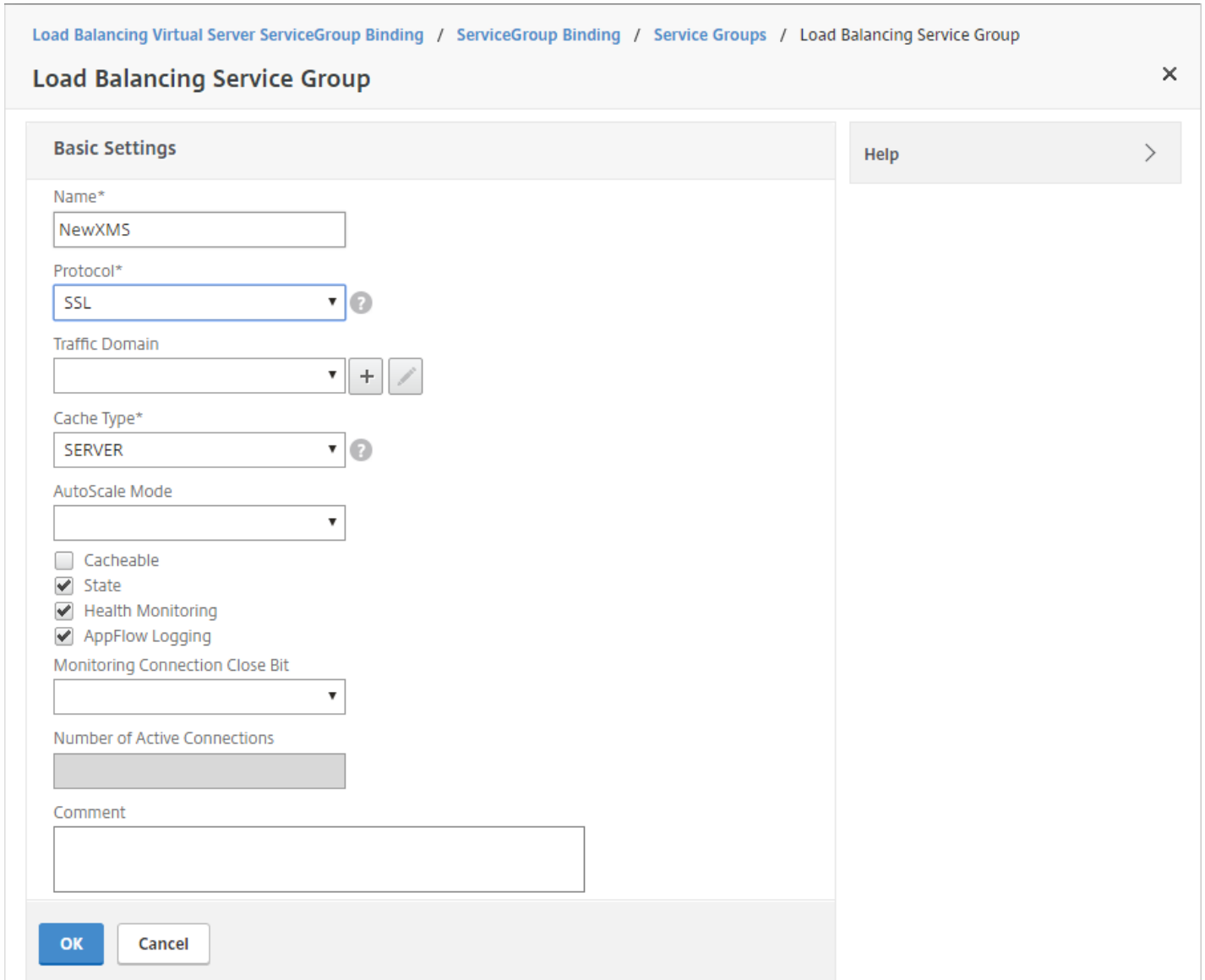
Click to select > + ✎

Bind Close

6. 新しいサービスグループを作成するには [Add] をクリックします。



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



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

## Load Balancing Service Group

## Basic Settings

Name	NewXMS	Cache Type	SERVER
Protocol	SSL	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

## Service Group Members

No Service Group Member

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

- IP Address/IP Address Range : XenMobile 10.4サーバーのIPアドレスを入力します。
- Port : 8443に設定します。
- Server ID : XenMobile 9.0のクラスター化環境からXenMobile 10.4のクラスター化環境に移行する場合は、現在のXenMobileサーバーのサーバーノードIDを入力します。サーバーノードIDを確認するには、XenMobile 10.4サーバーのコマンドラインインターフェイス (CLI) にログオンして「1」と入力し、[Clustering] メニューを開きます。CLIでは、サーバーノードIDは「Current Node ID」と表示されます。

```

-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----
Choice: [0 - 5] 1
Current Node ID: 181356771

```



Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding / Service Groups / Load Balancing Service Group / Service Group Members Binding / Create Service Group

### Create Service Group Member

IP Based
  Server Based

IP Address/IP Address Range\*

10 . 207 . 87 . 38  IPv6 -

Port\*

8443

Weight

1

Server Id

181356771

Hash Id


12345

State

10. [Create] をクリックして [Done] をクリックします。


Load Balancing Virtual Server ServiceGroup Binding / Load Balancing Service Group

### Load Balancing Service Group

**Basic Settings** 

Name	<b>NewXMS</b>	Cache Type	<b>SERVER</b>
Protocol	<b>SSL</b>	Cacheable	<b>NO</b>
State	<b>ENABLED</b>	Health Monitoring	<b>YES</b>
Effective State	<b>UP</b>	AppFlow Logging	<b>ENABLED</b>
Traffic Domain	<b>0</b>	Monitoring Connection Close Bit	<b>NONE</b>
Comment		Number of Active Connections	<b>0</b>
		AutoScale Mode	<b>DISABLED</b>

**Service Group Members**

1 Service Group Member 

11. [Done] をクリックして、 [OK] をクリックします。

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

Load Balancing Virtual Server ServiceGroup Binding / ServiceGroup Binding

### ServiceGroup Binding

Select Service Group Name\*

NewXMS > + ✎

Bind Close

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

Dashboard Configuration Reporting Documentation Downloads

## Load Balancing Virtual Server

Load Balancing Virtual Server | Export as a Template

#### Basic Settings

Name	MigrationLB	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	UP	Range	1
IP Address	192.168.1.10	Redirection Mode	IP
Port	443	RHI State	PASSIVE
Traffic Domain	0	AppFlow Logging	ENABLED
		Redirect From Port	
		HTTPS Redirect URL	

#### Services and Service Groups

- No Load Balancing Virtual Server Service Binding >
- 1 Load Balancing Virtual Server ServiceGroup Binding >

#### Certificate

- No Server Certificate >
- No CA Certificate >

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

SSL Virtual Server Server Certificate Binding / Server Certificate Binding

### Server Certificate Binding

Select Server Certificate\*

Click to select > +

Server Certificate for SNI

Bind Close

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

	Name	Common Name	Issuer Name
<input type="radio"/>	ns-sftrust-certificate	XXXXXXXXXXXX	XXXXXXXXXXXX
<input type="radio"/>	ns-server-certificate	XXXXXXXXXXXX	XXXXXXXXXXXX
<input type="radio"/>	xs-full	XXXXXXXXXXXX.com	XXXXXXXXXXXX
<input type="radio"/>	xmlab-server	XXXXXXXXXXXX.net	XXXXXXXXXXXX

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

Select Server Certificate\*

xmlab-server > +

Server Certificate for SNI

Bind Close

## ← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings	
Name	MigrationLB
Protocol	SSL
State	● UP
IP Address	192.168.1.10
Port	443
Traffic Domain	0
Listen Priority	-
Listen Policy Expression	NONE
Range	1
Redirection Mode	IP
RHI State	PASSIVE
AppFlow Logging	ENABLED
Redirect From Port	
HTTPS Redirect URL	

Services and Service Groups	
No	Load Balancing Virtual Server Service Binding >
1	Load Balancing Virtual Server ServiceGroup Binding >

Certificate	
1	Server Certificate >
No	CA Certificate >

17. 更新ボタンをクリックしてサーバーが実行中であることを確認します。

Traffic Management / Load Balancing / Virtual Servers

### Virtual Servers

↻ ? 🔗

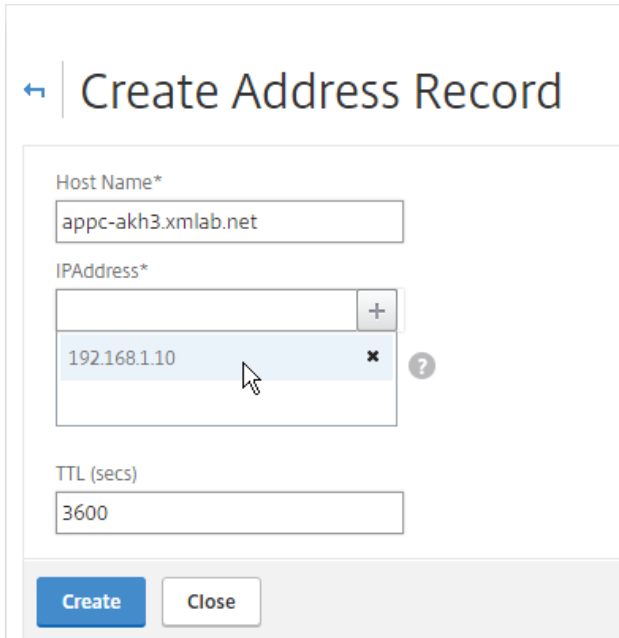
Add Edit Delete Enable Disable Statistics Action ▾ Search ▾

<input type="checkbox"/>	Name	State	Effective State	IP Address	Port	Protocol	Method
<input type="checkbox"/>	MigrationLB	● UP	● UP	192.168.1.10	443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_MAM_LB_192.168.2.10_8443	● UP	● UP	192.168.2.10	8443	SSL	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_443	● UP	● UP	172.16.30.38	443	SSL_BRIDGE	LEASTCONNECT
<input type="checkbox"/>	_XM_LB_MDM_XenMobileMDM_172.16.30.38_8443	● UP	● UP	172.16.30.38	8443	SSL_BRIDGE	LEASTCONNECT

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

## 注意

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



← Create Address Record

Host Name\*  
appc-akh3.xmlab.net

IPAddress\*  
192.168.1.10

TTL (secs)  
3600

Create Close

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 10.4サーバーの新しいIPアドレスで、NetScalerの負荷分散XenMobile 9.0 Device Managerインスタンスを構成する必要があります。

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

### NetScaler 11.1の場合

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

The screenshot shows the NetScaler Gateway dashboard with the following components:

- Navigation Bar:** Dashboard, Configuration, Reporting, Documentation, Downloads.
- Left Sidebar:** Search bar, System menu (AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway, Authentication), Integrate with Citrix Products (Unified Gateway, XenMobile, XenApp and XenDesktop), and Show Unlicensed Features.
- Dashboard Content:**
  - NetScaler Gateway:** Includes a connectivity check box, Universal Licenses (0), HDX Sessions (0), and a table for XenMobile Server Load Balancing (IP: 172.16.30.37, Port 443 UP, Port 8443 UP).
  - XenMobile Server Load Balancing:** Shows two throughput graphs (port :443 and port :8443) and two load balancing request/response rate graphs (both at 0%).
  - Microsoft Exchange Load Balancing with Email Security Filtering:** Not Configured.

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

This is a close-up of the XenMobile Server Load Balancing widget. It displays the following information:

- XenMobile Server Load Balancing**
- IP Address: 172.16.30.38
- Port: 443 ● UP
- Port: 8443 ● UP
- Buttons: Edit, Remove

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

The screenshot shows the configuration page for 'Load Balancing XenMobile Server Network Traffic'. It contains the following sections:

- Load Balancing Virtual Server Configuration:**

Name	MDM_XenMobileMDM	IP Address	172.16.30.38	Port	443,8443	Communication with XenMobile Server	HTTPS
------	------------------	------------	--------------	------	----------	-------------------------------------	-------
- XenMobile Servers:**

IP Address	Port
10.207.87.37	443, 8443
- Buttons:** Done

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

← Load Balancing XenMobile Server Network Traffic

**Load Balancing Virtual Server Configuration**

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

**XenMobile Servers**

Add Server Remove Server

<input type="checkbox"/>	IP Address	Port
<input type="checkbox"/>	10.207.87.37	443,8443

Continue

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

← Load Balancing XenMobile Server Network Traffic

**Load Balancing Virtual Server Configuration**

Name	IP Address	Port	Communication with XenMobile Server
MDM_XenMobileMDM	172.16.30.38	443,8443	HTTPS

**XenMobile Servers**

Add Server Remove Server

<input checked="" type="checkbox"/>	IP Address	Port
<input checked="" type="checkbox"/>	10.207.87.37	443,8443

Continue

5. [Add Server] をクリックして新しいXenMobile 10.4サーバーのIPアドレスを追加します。

**XenMobile Server IP Addresses**

Enter the IP address of the XenMobile server that you want to load balance.

XenMobile Server IP Address\*

Add Cancel

# NetScaler のバージョン 11.0 または 10.5

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

The screenshot shows the NetScaler Configuration page. The left sidebar has a menu with categories like System, AppExpert, Traffic Management, Optimization, Security, NetScaler Gateway, and Authentication. Under 'Integrate with Citrix Products', 'XenMobile' is highlighted. The main content area is titled 'Dashboard' and includes 'NetScaler Gateway' and 'Device Manager Load Balancing' sections. The 'NetScaler Gateway' section shows 'Universal Licenses' at 0 and 'HDX Sessions' at 1. The 'Device Manager Load Balancing' section shows two ports (443 and 8443) both as 'Up'.

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

This is a close-up of the 'Device Manager Load Balancing' configuration card. It displays the IP Address as 10.217.232.39 and two ports: 443 (Up) and 8443 (Up). There are 'Edit' and 'Remove' links at the bottom right of the card.

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



## Load Balancing Device Manager Network Traffic

Load Balancing Virtual Server Configuration		
Name	IP Address	Port
MDM_XenMobileMDM	10.217.232.39	443,8443

Device Manager Server IP Addresses		
IP Address	Port	State
10.207.72.216	443, 8443	● Up

Done

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

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	● Up

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

Device Manager Server IP Addresses		
<input type="button" value="Add Server"/>	<input type="button" value="Remove Server"/>	<input type="button" value="Add from existing servers"/>
IP Address	Port	State
10.207.72.216	443, 8443	● Up

5. [Add Server] をクリックして新しいXenMobile 10.4サーバーのIPアドレスを追加します。

Device Manager Server IP Addresses	
Enter the IP address(es) of the device manager server(s) that you want to load balance. If the server IP address is already added to the NetScaler, click <b>Add from existing servers</b> to select the device manager server IP.	
Device Manager Server IP Address*	
<input type="text" value="10 . 207 . 87 . 38"/>	
<input type="button" value="Add"/>	<input type="button" value="Cancel"/>

この時点で、NetScaler GatewayはApp Controller FQDNをポイントしています。新しいXenMobile 10.4のFQDNをポイントするように、NetScalerを変更する必要があります。XenMobile 10.4は、ポート443ではなくポート8443でリッスンします。NetScaler for XenMobileウィザード9を使用してNetScalerを設定する場合、次の表の例に示すように、FQDNにポート番号を含める必要があります。

### XenMobile Enterprise Edition

新しいXenMobile 10.4のFQDNを参照するように、App ControllerのFQDNをXenMobile 9.0のDevice ManagerのFQDNにポート8443を続けたものに変更します。次の表は、一例です。

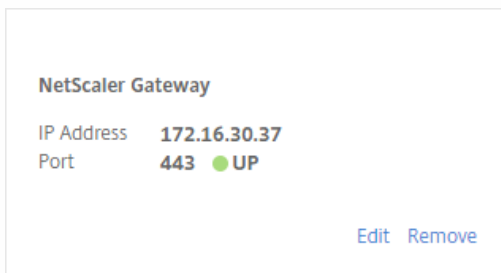
XenMobile 9.0 のコンポーネント	コンポーネントのFQDN	XenMobile 10.4 Enterprise EditionのFQDN
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	-
NetScaler Gateway	access.example.com	-

### XenMobile App Edition

新しいXenMobile 10.4のFQDNを参照するように、App ControllerのFQDNをXenMobile 9.0のApp ControllerのFQDNにポート8443を続けたものに変更します。次の表は、一例です。

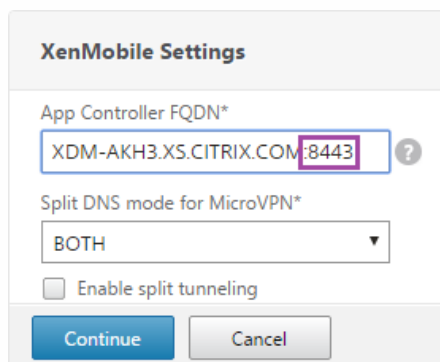
XenMobile 9.0 のコンポーネント	コンポーネントのFQDN	XenMobile 10.4 Enterprise EditionのFQDN
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	-

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



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

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



**XenMobile Settings**

App Controller FQDN\*

XDM-AKH3.XS.CITRIX.COM:8443 ?

Split DNS mode for MicroVPN\*

BOTH

Enable split tunneling

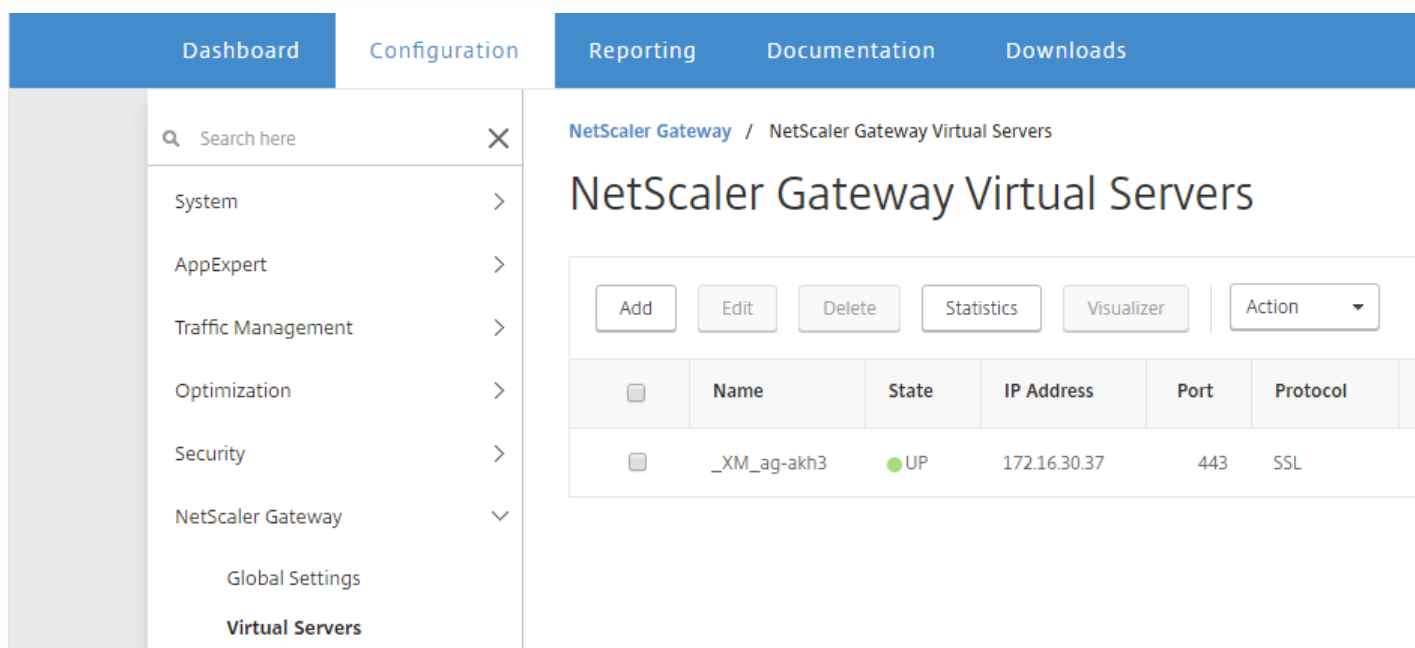
Continue Cancel

4. [Continue]、[Finish] の順にクリックします。

次に、DNSを更新して、Secure Ticket Authorityを実行しているサーバーのFQDNを、XenMobile Server 10.4のIPアドレスに解決する必要があります。アップグレード後要件の変更の後、Secure Ticket Authority ServerがNetScalerにバインドされていないのに [VPN Virtual Server STA Server Binding] の一覧に表示されることがあります。

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

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



Dashboard Configuration Reporting Documentation Downloads

Search here

System >

AppExpert >

Traffic Management >

Optimization >

Security >

NetScaler Gateway >

Global Settings

Virtual Servers

NetScaler Gateway / NetScaler Gateway Virtual Servers

## NetScaler Gateway Virtual Servers

Add Edit Delete Statistics Visualizer Action

<input type="checkbox"/>	Name	State	IP Address	Port	Protocol
<input type="checkbox"/>	_XM_ag-akh3	UP	172.16.30.37	443	SSL

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

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

Published Applications
No Next HOP Server
1 STA Server
No Url

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

### VPN Virtual Server STA Server Binding

Add Binding
Unbind

<input type="checkbox"/>	Secure Ticket Authority Server	Secure Ticket Authority Server Address Type
<input checked="" type="checkbox"/>	https://XDM-AKH3.XS.CITRIX.COM:8443	IPV4

Close

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

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

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

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

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

1. XenMobile 10.4コンソールで、 [Settings] > [Server Properties] の順に選択します。

2. [Add] をクリックして、フィールドに次のように値を指定します。

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

Settings > Server Properties > Add New Server Property

## Add New Server Property

Key	Custom Key	?
Key*	host.name.uselowercase	
Value*	true	
Display name*	Use lowercase for host name	
Description		

3. XenMobileサーバーを再起動します。

必要に応じて以下の情報を更新します。

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

アップグレードする前、前提条件の手順の1つは、カスタムのCitrix Store名をそのデフォルト値に戻すよう変更することでした。その前提条件を実行しなかった場合は、次のいずれかのアップグレード後要件の手順に従ってから、XenMobile Server 10.4を使用することができます。

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

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

ユーザーは、実稼働環境でのXenMobile 10.4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 10.4サーバーに自動的に接続されます。ただし、デバイスを再接続する前にユー

ザーが再認証を求められる可能性があります。

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

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage' (which is highlighted), and 'Configure'. Below these are sub-tabs: 'Devices', 'Users', and 'Enrollment'. The 'Devices' section is active, showing a 'Show filter' link. Below the navigation are icons for 'Add', 'Import', 'Export', and 'Refresh'. The main content is a table with the following columns: 'Status', 'Mode', 'User name', 'Device platform', and 'Operating system version'. There are two rows of device data.

Status	Mode	User name	Device platform	Operating system version
	MDM MAM	us1user1@...net "us1 user1"	Android	5.0.2
	MDM MAM	us3user3@...net "us3 user3"	iOS	8.4.1

# MTCテナントサーバーからXenMobile 10.4へのアップグレード

Apr 27, 2017

XenMobile 9.0 MDMまたはEnterprise EditionでMulti-Tenant Console (MTC) が有効になっている場合、MTCで管理されているXenMobile 9インスタンスをスタンドアロンのXenMobile 10.4インスタンスに移行できます。XenMobile 10ではMTCはサポートされないため、アップグレードしたインスタンスは個別に管理する必要があります。

1. ネットワークアドレス変換 (NAT) をすべてのMTCクライアントの前に構成していることを確認します。
2. XenMobile 10のインスタンスをインストールします。
3. MTCテナントでポートマッピングが有効化されていない場合は、以下を実行します。
  - a. 証明書を使用するHTTPS通信を許可するXenMobile 10サーバーポート (通常はポート443) と、証明書を使用しないHTTPS通信を許可するXenMobile 10サーバーポート (8443) が、XenMobileインスタンスで使用するポートと一致していることを確認します。
  - b. 新しい管理用ポートを構成します。
  - c. ポートマッピングが有効化されている場合、XenMobileサーバーがリスンするポートではなく、XenMobileサーバーにマッピングされているポートを使用します。
4. XenMobileサーバーの起動時に、インスタンス名 (zdm) を使用します。
5. アップグレードツールをコマンドラインインターフェイス (CLI) から有効にする場合、アップグレードのプロンプトに [Yes] と答える必要があります。
6. アップグレードするサーバーから、C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classesにある以下のファイルをコピーします。
  - ew-config.properties
  - pki.xml
  - variables.xml
7. C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant nameにある以下のファイルをコピーします。
  - cacerts.pem.jks
  - https.p12
  - pki-ca-devices.p12
  - pki-ca-root.p12
  - pki-ca-servers.p12
8. C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xmlのコピーを作成して、以下の手順の説明に従って変更します。
9. ポート80を除いて、server.xmlのそのほかのテナントによって使用されているポートコネクタをすべて削除します。
10. 使用されるポートコネクタで、以下の範囲内のすべてのファイルパスからインスタンス名を削除します。

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\https.p12"

新しい場所

C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xmlをコピーして変更します。

11. 以下の範囲内のファイルパスで、手順10を繰り返します。

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\cacerts.pemjks"

新しい場所

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pemjks"

12. 手順6～8でコピーしたファイルで.zipファイルを作成します。

13. XenMobile 10.4サーバーのIPアドレスを、`https://ipAddress:port/uw/?cloudMode`のように開きます。ここで`port`は、証明書を持つHTTPS接続です。アップグレードウィザードが開きます。

14. アップグレードウィザードで説明される手順に従って、[MDM] または [Enterprise] を選択します。

**MDM**アップグレードの場合、ウィザードにより.zipファイルのアップロードを求められます。また、データベースが正しいことを確認し、CA証明書のパスワードを入力する必要があります。

**Enterprise**アップグレードの場合、ウィザードにより、App Controllerのサポートバンドルをアップロードするよう求められます。

15. XenMobileサーバーが再起動した後、XenMobileサーバーのIPアドレスの後に管理ポート番号が続くアドレスで、XenMobileコンソールにサインオンします。

16. 新しいサーバーをポイントするように、NATを変更します。

17. XenMobileサーバーが使用するポートを許可するために必要なファイアウォールの変更を行います。



# ユーザーアカウント、役割、および登録

Apr 27, 2017

XenMobileで、ユーザーアカウントおよびグループとそれらの役割を構成します。登録モードおよび招待状も構成します。XenMobileコンソールの **[Manage]** タブおよび **[Settings]** ページで、これらの設定を構成します。

**[Manage]** タブから、以下の操作を実行できます。

- **[Users]** をクリックして、ユーザーアカウントを手動で追加するか、.csvプロビジョニングファイルを使用してアカウントをインポートし、ローカルグループを管理します。詳しくは、次のページを参照してください。
  - [ローカルユーザーアカウントを追加、編集、または削除するには](#)
  - [.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](#)

ワークフローを使用して、ユーザーアカウントの作成および削除を管理することもできます。この記事の後段、[ワークフローの作成および管理](#)で説明します。

- **[Enrollment]** をクリックして、最大7つのモードを構成します。**[Enrollment]** をクリックして、最大7つのモードを構成します。それぞれに独自のセキュリティレベルを設定し、ユーザーがデバイスを登録するときや登録招待状を送信するときに必要ないくつかの手順を指定します。詳しくは、次のページを参照してください。
  - [登録モードを構成してSelf Help Portalを有効化するには](#)
  - [XenMobileでのユーザー登録の自動検出の有効化](#)

**[Settings]** ページでは以下の操作を実行できます。

- **[役割ベースのアクセス制御]** をクリックして、権限の定義済みセットである役割をユーザーとグループに割り当てます。これらの権限によって、システム機能に対するユーザーのアクセスレベルを制御します。詳しくは、次のページを参照してください。
  - [RBACを使用した役割の構成](#)
- **[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。Secure Hub、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。詳しくは、次のページを参照してください。
  - [通知テンプレートの作成および更新](#)

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

1. XenMobileコンソールで、**[Manage]** > **[Users]** の順にクリックします。**[Users]** ページが開きます。

XenMobile					
Analyze		Manage		Configure	
Devices		Users		Enrollment	
<b>Users</b> <a href="#">Show filter</a>					
Add Local User		Import Local Users		Manage Local Groups	
Export					
<input type="checkbox"/>	User name	First name	Last name	Roles	Groups
<input type="checkbox"/>	us1user1@net	us1	user1	USER	net\Domain Users
<input type="checkbox"/>	us3user3@net	us3	user3	USER	net\Domain Users

ローカルユーザーアカウントを追加するには

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

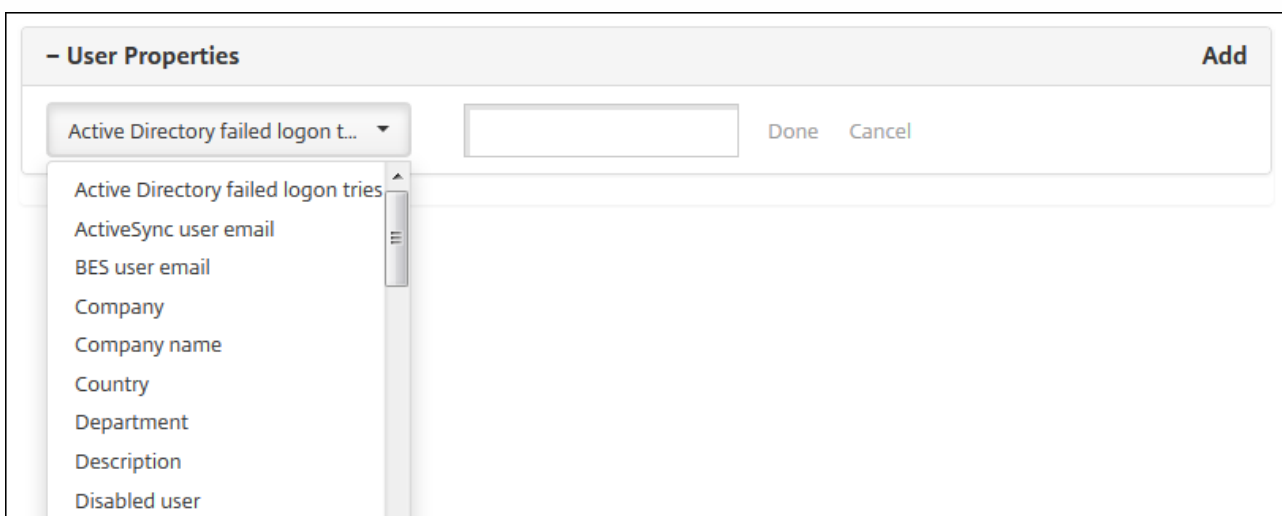
XenMobile					
Analyze		Manage		Configure	
Devices		Users		Enrollment	
<b>Add Local User</b> <span style="float: right;">✕</span>					
<b>User name*</b>	<input type="text" value="Enter user name"/>				
<b>Password</b>	<input type="password" value="Enter new password"/>				
<b>Role*</b>	ADMIN <span style="float: right;">▼</span>				
<b>Membership</b>	<input type="checkbox"/> local\MSP <span style="float: right; margin-left: 20px;"><a href="#">Manage Groups</a></span>				
- User Properties					<a href="#">Add</a>
					<input type="button" value="Cancel"/> <input type="button" value="Save"/>

2. 次の設定を構成します。

- **User name** : ユーザーの名前を入力します。このフィールドは必須です。名前にはスペースや大文字、小文字を含めることができます。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Role** : 一覧から、ユーザーの役割を選択します。役割について詳しくは、「[RBACを使用した役割の構成](#)」を参照してください。選択できるオプションは以下のとおりです。
  - 管理者
  - DEVICE\_PROVISIONING
  - サポート
  - USER
- **Membership** : 一覧から、ユーザーを追加するグループを選択します。
- **User Properties** : 任意でユーザープロパティを追加します。追加するユーザープロパティごとに、**[Add]** をクリックして以下の操作を行います。
  - **User Properties** : 一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
  - **[Done]** をクリックしてユーザープロパティを保存するか、**[Cancel]** をクリックして操作を取り消します。

注: 既存のユーザープロパティを削除するには、プロパティが含まれる行の上にマウスポインターを置き、右側の **[X]** をクリックします。プロパティがすぐに削除されます。

既存のユーザープロパティを編集するには、プロパティを選択して変更を加えます。**[Done]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。



3. **[Save]** をクリックします。

ローカルユーザーアカウントを編集するには

1. **[Users]** ページのユーザー一覧で、ユーザーをクリックして選択してから **[Edit]** をクリックします。 **[Edit Local User]** ページが開きます。

The screenshot shows the 'Edit Local User' form in the XenMobile console. The form includes the following elements:

- User name\***: Text input field containing 'Freida Cat'.
- Password**: Text input field with placeholder text 'Enter new password'.
- Role\***: Dropdown menu currently set to 'USER'.
- Membership**: A list box containing 'local\MSP' with a checked checkbox. A 'Manage Groups' button is located to the right of this list.
- User Properties**: A section with an 'Add' button and a table of properties. One property is visible: 'ActiveSync user email' with the value 'freida.cat@example.com'.
- Buttons**: 'Cancel' and 'Save' buttons are located at the bottom right of the form.

2. 必要に応じて以下の情報を変更します。

- **User name** : ユーザー名は変更できません。
- **Password** : ユーザーパスワードを変更または追加します。
- **Role** : 一覧から、ユーザーの役割を選択します。
- **Membership** : 一覧から、ユーザーアカウントを追加または編集するグループを選択します。ユーザーアカウントをグループから削除するには、グループ名の横にあるチェックボックスをオフにします。
- **User properties** : 次のいずれかを行います。
  - 変更するユーザープロパティごとに、プロパティを選択して変更を加えます。[Done] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。
  - 追加するユーザープロパティごとに、[Add] をクリックして以下の操作を行います。
    - **User Properties** : 一覧からプロパティを選択し、プロパティの横のフィールドにユーザープロパティ属性を入力します。
    - [Done] をクリックしてユーザープロパティを保存するか、[Cancel] をクリックして操作を取り消します。
  - 削除する既存のユーザープロパティごとに、プロパティが含まれる行の上にマウスポインターを置き、右側の [X] をクリックします。プロパティがすぐに削除されます。

3. [Save] をクリックして変更を保存するか、[Cancel] をクリックしてユーザーを変更せずそのままにします。

#### ローカルユーザーアカウントを削除するには

1. [Users] ページのユーザーアカウント一覧で、ユーザーアカウントをクリックして選択します。

注：各ユーザーアカウントの横のチェックボックスをオンにして、削除するユーザーアカウントを複数選択できます。

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

3. [Delete] をクリックしてユーザーアカウントを削除するか、[Cancel] をクリックして操作を取り消します。

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

注：

- ローカルユーザーの場合は、インポートファイル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のように指定します。この形式で作成またはインポートしたローカルユーザーがXenMobileの管理されたドメインにある場合、以下に注意してください。ユーザーは、関連するLDAP資格情報を使用して登録することはできません。
- XenMobileの内部ユーザーディレクトリにユーザーアカウントをインポートする場合は、インポートプロセスの速度を上げるため、デフォルトのドメインを無効にします。ドメインを無効にすると登録にも影響があるため、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する必要があります。
- ローカルユーザーはユーザープリンシパル名 (User Principal Name : UPN) 形式で指定できますが、管理対象ドメインは使わないことをお勧めします。example.comが管理されている場合、このUPN形式のローカルユーザー「user@example.com」を作成しないでください。

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

1. XenMobileコンソールで、[Manage] > [Users] の順にクリックします。[Users] ページが開きます。

2. [Import Local Users] をクリックします。[Import Provisioning File] ダイアログボックスが開きます。

Import Provisioning File

Format  User ?  
 User property ?

File\*

3. インポートするプロビジョニングファイルの形式として、[User] または [Property] を選択します。
4. [Browse] をクリックして使用するプロビジョニングファイルの場所へ移動し、そのファイルを選択します。
5. [Import] をクリックします。

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

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

注 :

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

#### ユーザープロビジョニングファイルの内容例

エン트리 user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01の意味は以下のとおりです。

- User : user01
- Password : pwd;01
- Role : USER
- Groups :

- myGroup.users01
- myGroup.users02
- myGroup.users.users.users01

別の例として、「AUser0;1.password;USER;ActiveDirectory.test.net」の意味は次のとおりです。

- User : AUser0
- Password : 1.password
- Role : USER
- Group : ActiveDirectory.test.net

#### ユーザー属性プロビジョニングファイルの内容例

エン트리user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 valueの意味は以下のとおりです。

- User : user01
- プロパティ1 :
  - name : propertyN
  - value : propertyV;test;1;2
- Property 2 :
  - name : prop 2
  - value : prop2 value

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コンソールの [Settings] の [Enrollment] ページから行います。

登録招待状の送信は、[Manage] の [Enrollment] ページから行います。詳しくは、「[登録招待状の送信](#)」を参照してください。

注：カスタム通知テンプレートを使用する予定の場合は、登録モードを構成する前にテンプレートを設定しておく必要があります。通知テンプレートについて詳しくは、「[通知テンプレートの作成または更新](#)」を参照してください。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Enrollment] をクリックします。[Enrollment] ページが開き、すべての使用可能な登録モードの表が表示されます。デフォルトでは、すべての登録モードが有効です。
3. 一覧で登録モードを選択し、モードを編集してデフォルトに設定したり、モードを無効にしたり、ユーザーがSelf Help Portalからアクセスできるようにします。

注：登録モードの横のチェックボックスを選択すると、登録モード一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

Settings &gt; Enrollment

## Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Work Home and enroll their devices, or to send themselves an enrollment invitation.



<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▾
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

### 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。[Edit Enrollment Mode] ページが開きます。選択したモードによって、異なるオプションが表示される場合があります。



XenMobile Analyze Manage Configure   admin ▾

Settings > Enrollment > Edit Enrollment Mode

## Edit Enrollment Mode

	Name	High Security
Expire after*	<input type="text" value="1"/>	Days 
Maximum attempts*	<input type="text" value="3"/>	
PIN Length*	<input type="text" value="8"/>	Numeric ▾

Notification templates

Template for enrollment URL	<input type="text" value="-- SELECT ONE --"/>
Template for Enrollment PIN	<input type="text" value="-- SELECT ONE --"/>
Template for enrollment confirmation	<input type="text" value="-- SELECT ONE --"/>

2. 必要に応じて以下の情報を変更します。

- **Expired after** : ユーザーがデバイスを登録できなくなる、有効期限を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。  
注 : 「0」を入力すると、招待状は期限切れになりません。
- **Days** : 一覧から、**[有効期限]** ボックスに入力した有効期限に応じて、**[日]** または **[時間]** を選択します。
- **Maximum attempts** : 登録処理からロックアウトされるまでにユーザーが実行できる登録の試行回数を入力します。この値は、ユーザーおよびグループの登録招待状構成ページに表示されます。  
注 : 「0」を入力すると、無制限に試行できます。
- **PIN length** : 生成されるPINの桁数または文字数を入力します。
- **Numeric** : 一覧から、PINの種類として、**[Numeric]** または **[Alphanumeric]** を選択します。
- **通知テンプレート** :
  - **Template for enrollment URL** : 一覧から、登録URLに使用するテンプレートを選択します。たとえば、登録招待状テンプレートではテンプレートの構成方法に応じて、デバイスをXenMobileに登録できる電子メールまたはSMSをユーザーに送信します。通知テンプレートについて詳しくは、「[通知テンプレートおよび作成または更新](#)」を参照してください。
  - **Template for enrollment PIN** : 一覧から、登録PINに使用するテンプレートを選択します。
  - **Template for enrollment confirmation** : 一覧から、登録が成功したことをユーザーに通知するときに使用するテンプレートを選択します。

3. [Save] をクリックします。

#### 登録モードをデフォルトとして設定するには

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適用して使用されます。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、[ユーザー名およびパスワード]、[2要素]、[ユーザー名およびPIN] のいずれかのみです。

1. [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。

グループの管理は、XenMobileコンソールの [Manage Groups] ダイアログボックスで行います。このダイアログボックスは、[Users] ページ、[Add Local User] ページ、または [Edit Local User] からアクセスできます。グループ編集コマンドはありません。

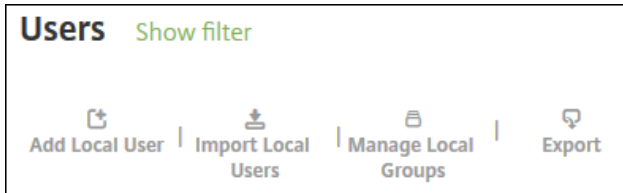
グループを削除する場合、グループを削除してもユーザーアカウントには影響しない点に注意してください。グループを削除しても、そのグループとユーザーの関連付けが削除されるだけです。また、ユーザーは、そのグループに関連付けられてい

デリバリーグループによって提供されているアプリケーションやプロファイルにアクセスできなくなります。ただし、そのほかのグループ関連付けはそのまま保持されます。ほかのローカルグループに関連付けられていないユーザーは、最上位レベルで関連付けられます。

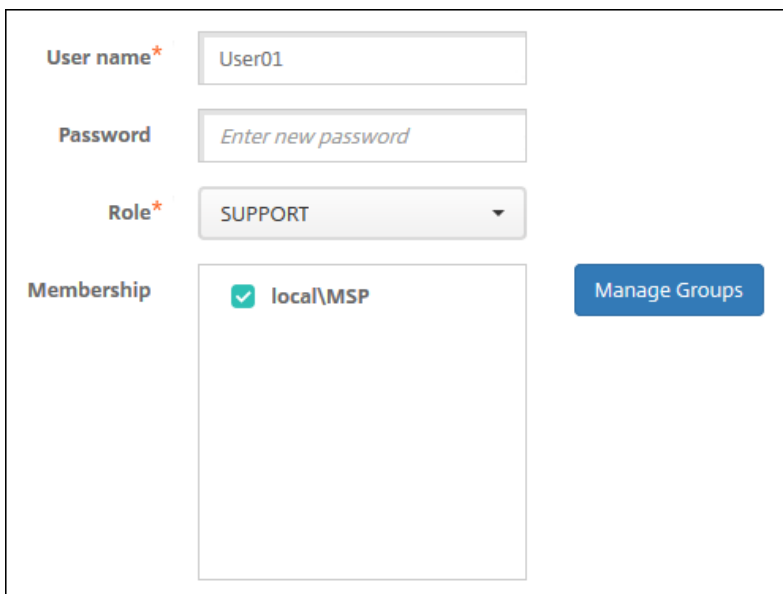
ローカルグループを追加するには

1. 次のいずれかを行います。

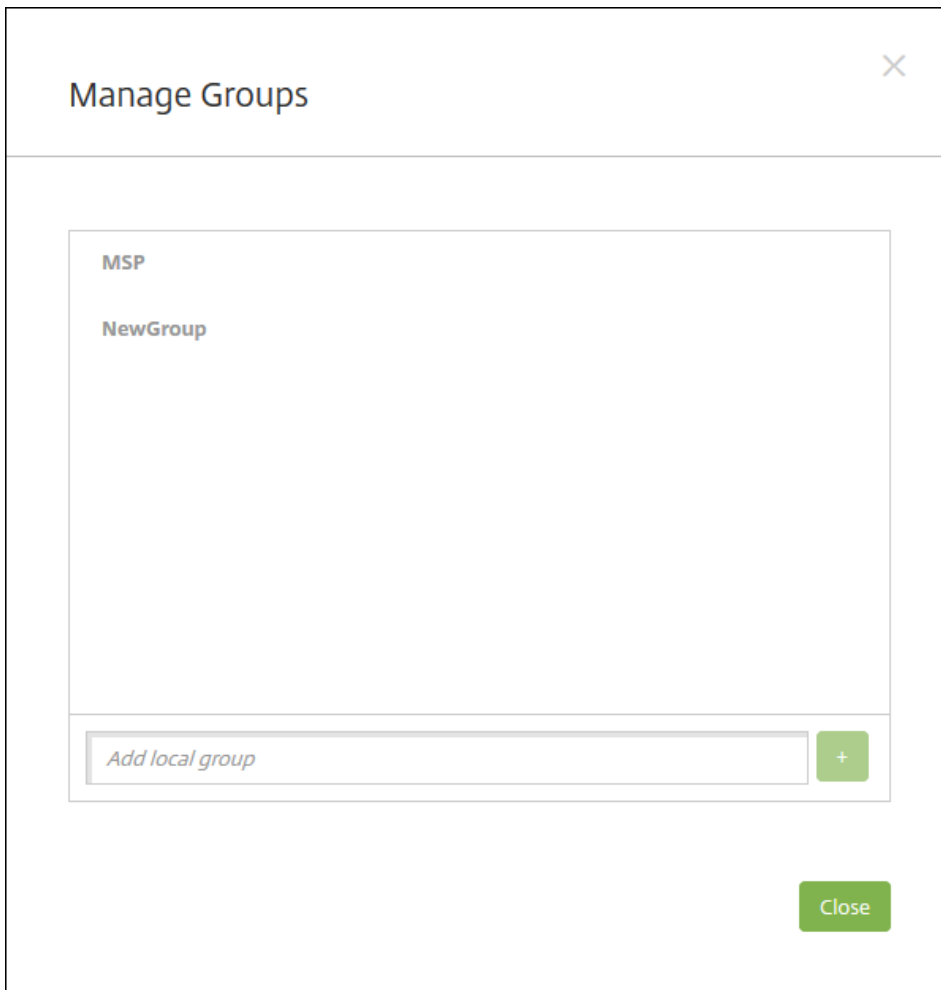
- [Users] ページで、[Manage Local Groups] をクリックします。



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

A screenshot of the 'Add Local User' or 'Edit Local User' form. It contains several input fields: 'User name\*' with the value 'User01', 'Password' with the placeholder 'Enter new password', and 'Role\*' with a dropdown menu showing 'SUPPORT'. Below these is a 'Membership' section with a list containing 'local\MSP' which has a checked checkbox. To the right of the membership list is a blue button labeled 'Manage Groups'.

[Manage Group] ダイアログボックスが開きます。



2. グループの一覧の下で、新しいグループ名を入力してプラス記号 (+) をクリックします。ユーザーグループが一覧に追加されます。

3. [Close] をクリックします。

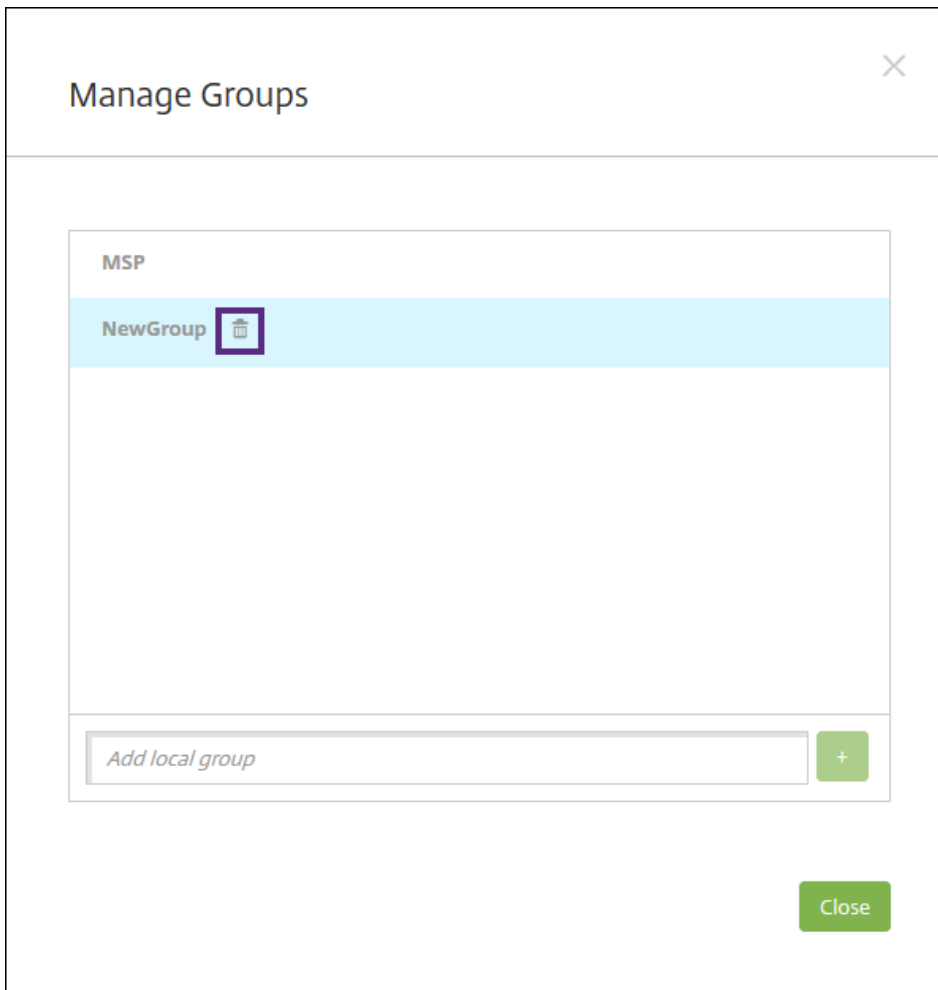
#### グループを削除するには

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

1. 次のいずれかを行います。

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

[Manage Groups] ダイアログボックスが開きます。



2. [Manage Groups] ダイアログボックスで、削除するグループを選択します。
3. グループ名の右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。
4. [Delete] をクリックして操作を確認し、グループを削除します。

**重要：** この操作を元に戻すことはできません。

5. [Manage Groups] ダイアログボックスで、[Close] をクリックします。

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

XenMobileを初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。

XenMobileの次の2つの方法でワークフローを構成できます。

- XenMobileコンソールの [Workflows] ページ。 [Workflows] ページでは、アプリケーションの構成で使用する複数のワークフローを構成できます。 [Workflows] ページでワークフローを構成するとき、アプリケーションを構成するときワークフローを選択できます。

- アプリケーションコネクタを構成するとき、アプリケーションで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。「[XenMobileへのアプリケーションの追加](#)」を参照してください。

ユーザーアカウントの管理者承認を最大3レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、ユーザーの名前またはメールアドレスを使用して追加のユーザーを検索し選択することができます。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。

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

2. [Workflows] をクリックします。[ワークフロー] ページが開きます。

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

4. 次の設定を構成します。

- **Name** : ワークフローの固有の名前を入力します。
- **Description** : 任意で、ワークフローの説明を入力します。
- **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。電子メールテンプレートの作成は、XenMobileコンソールの [Settings] の [Notification Templates] セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、構成中のテンプレートのプレビューが表示されます。
- **マネージャー承認のレベル** : 一覧から、このワークフローに必要なマネージャー承認のレベル数を選択します。デフォルトは [1 level] です。選択できるオプションは以下のとおりです。
  - Not Needed
  - 1 level
  - 2 levels
  - 3 levels
- **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
- **Find additional required approvers** : 検索フィールドに、追加に必要なユーザーの名前を入力して、[Search] をクリックします。名前はActive Directoryで取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが [Selected additional required approvers] の一覧に表示されます。
  - [Selected additional required approvers] の一覧からユーザーを削除するには、次のいずれかを行います。
    - [検索] をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して [Search] をクリックし、検索結果を絞り込みます。
    - [Selected additional required approvers] の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

5. [Save] をクリックします。作成したワークフローが [Workflows] ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリケーションを表示したり、ワークフローを削除したりできます。ワークフローを作成した後でワークフローを編集することはできません。承認レベルまたは承認者が異なるワークフローが必要な場合は、別のワークフローを作成する必要があります。

ワークフローの詳細の表示および削除を行うには

1. [Workflows] ページの既存のワークフロー一覧で特定のワークフローを選択します。選択するには、表の列をクリックするか、ワークフローの横のチェックボックスを選択します。

2. ワークフローを削除するには、[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[削除] をク

リックします。

**重要**：この操作を元に戻すことはできません。

# RBACを使用した役割の構成

Apr 27, 2017

定義済みの役割ベースのアクセス制御 (Role-Based Access Control : RBAC) の各役割には、一定のアクセス権と機能権限が関連付けられています。このトピックでは、これらの権限で実行できる内容について説明します。組み込みの役割ごとのデフォルト権限に関する完全な一覧は、[Role-Based Access Control Defaults](#)からダウンロードしてください。

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

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

Adminの役割

Device Provisioningの役割

Supportの役割

ユーザーロール

## RBACを使用した役割の構成

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

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

- **Administrator**。システムへのフルアクセスが許可されます。
- **Device Provisioning**。Windows CEデバイスで基本的なデバイス管理へのアクセスが許可されます。
- **Support**。リモートサポートへのアクセスが許可されます。
- **User**。デバイスを登録でき、Self Help Portalにアクセスできるユーザーが使用します。

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

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

注：ローカルユーザーに割り当てることができる役割は1つだけです。

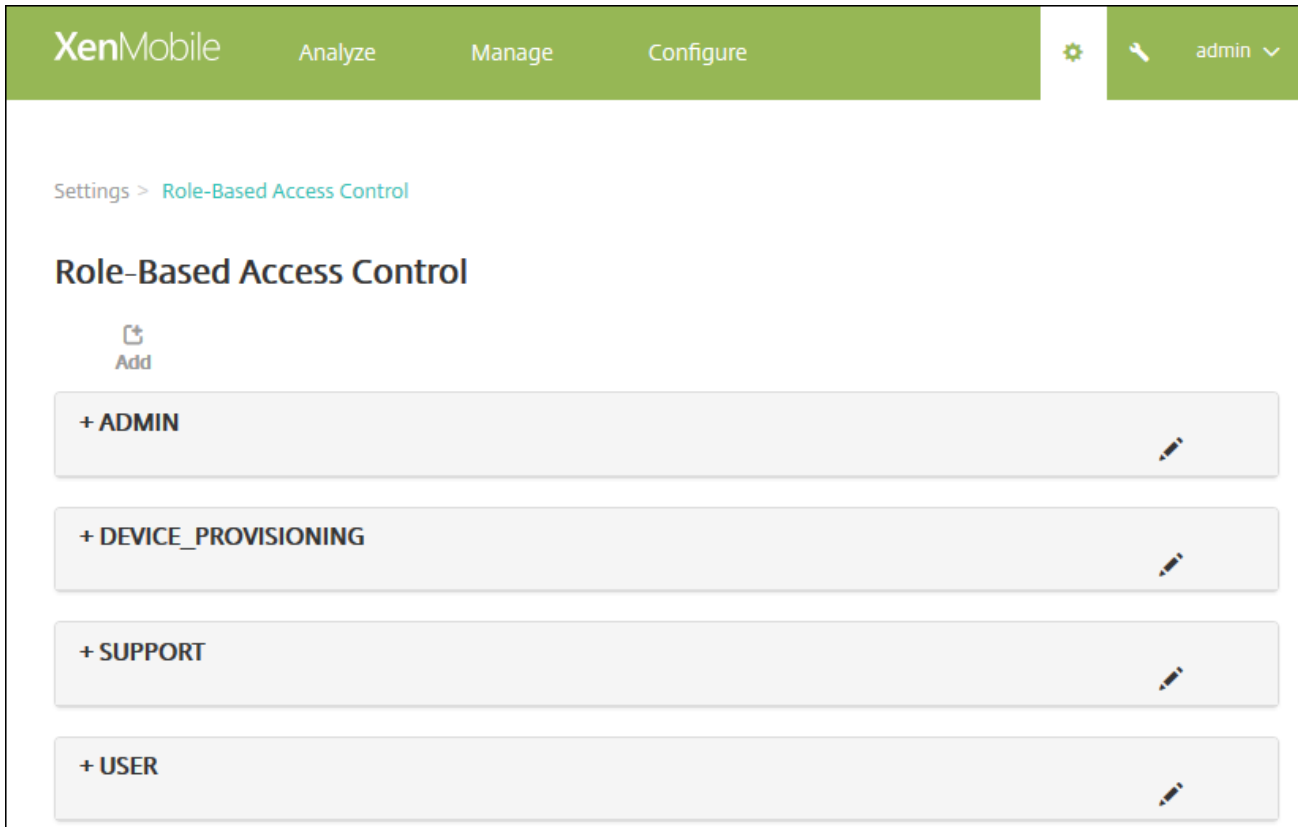
XenMobileのRBAC機能を使用すると、次のことを実行できます。



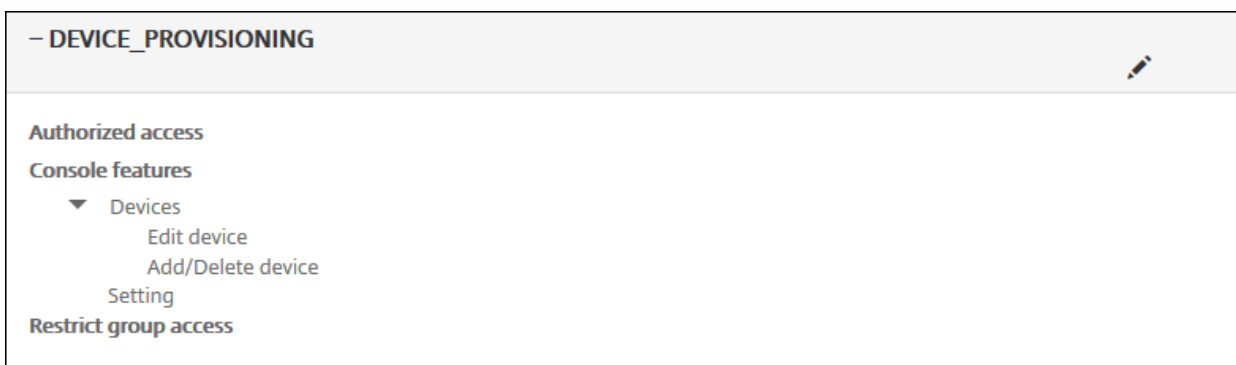
- 新しい役割を作成する。
- 役割にグループを追加する。
- ローカルユーザーを役割に関連付ける。

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

2. [Role-Based Access Control] をクリックします。[Role-Based Access Control] ページが開き、4つのデフォルトのユーザー役割と、以前に追加した役割が表示されます。



役割の横のプラス記号 (+) をクリックすると、次の図のように役割が展開され、その役割のすべての権限が表示されます。



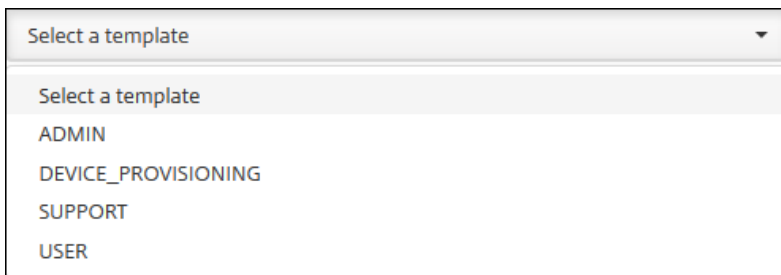
3. [Add] をクリックして新しいユーザー役割を追加したり、既存の役割の右にあるペンアイコンをクリックして役割を編集したり、以前定義した役割の右にあるごみ箱アイコンをクリックして役割を削除したりします。デフォルトのユーザー役割を削除することはできません。

- [Add] またはペンアイコンをクリックすると、[Add Role] ページまたは [Edit Role] ページが開きます。
- ごみ箱アイコンをクリックすると、確認ダイアログボックスが開きます。[Delete] をクリックすると、選択した役割が削除されます。

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

- **RBAC name** : 新しいユーザー役割の説明的な名前を入力します。既存の役割の名前は変更できません。
- **RBAC template** : 任意で、新しい役割の開始点とするテンプレートを選択します。既存の役割を編集する場合、テンプレートは選択できません。

RBACテンプレートは、デフォルトのユーザー役割です。RBACテンプレートによって、その役割に関連付けられているユーザーがシステムの機能に対して持つアクセス権を定義します。RBACテンプレートを選択すると、[Authorized Access] および [Console Features] フィールドで、その役割に関連付けられているすべての権限を参照できます。テンプレートの使用はオプションです。[Authorized Access] および [Console Features] フィールドで、役割に割り当てるオプションを直接選択することができます。



5. [RBAC template] フィールドの右にある [Apply] をクリックして、選択したテンプレートで定義されているアクセス権と機能権限を、[Authorized access] および [Console features] にあるチェックボックスに反映させます。

XenMobile Analyze Manage Configure admin

Settings > Role-Based Access Control > Add Role

### Add Role

- 1 Role Info
- 2 Assignment

### Role Info

RBAC name\*

RBAC template: DEVICE\_PROVISIONING Apply

Authorized access

- Admin console access
- Self Help Portal access
- Shared devices enroller
- Remote Support access
- Public api access

Console features

- Dashboard
- ▶  Devices
- ▶  App
- ▶  Delivery group
- ▶  Smart action
- ▶  Support
- ▶  Setting
- ▶  Enrollment

Apply permissions

- To all user groups
- To specific user groups

Next >

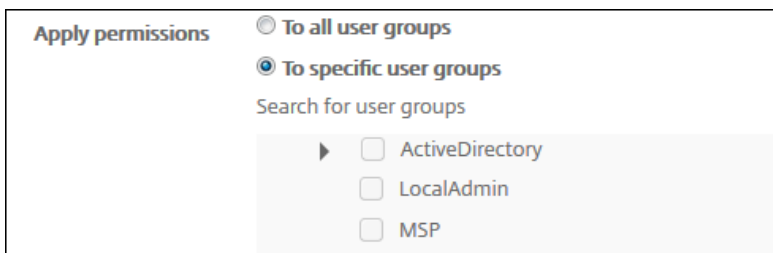
6. [Authorized access] および [Console Features] にあるチェックボックスをオンまたはオフにして、役割をカスタマイズします。

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

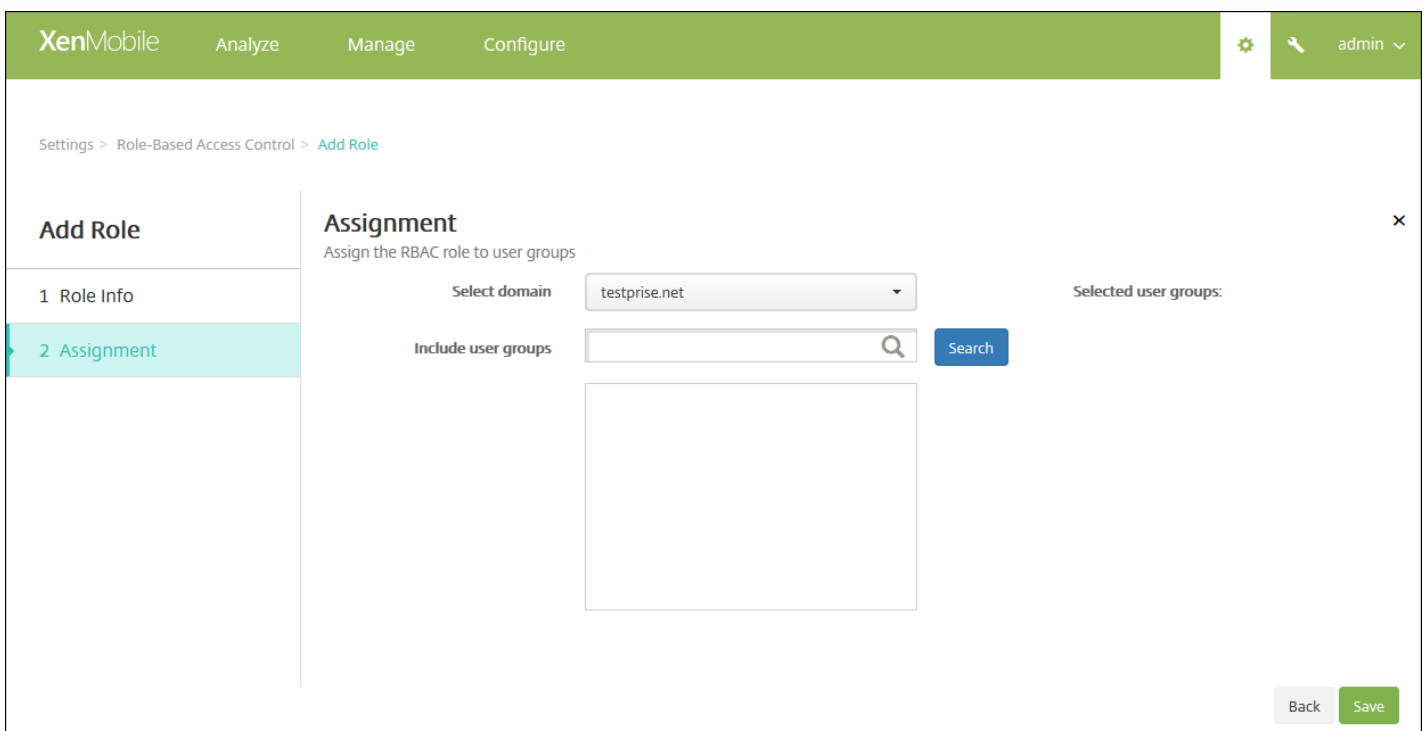
Console features

- Dashboard
- ▼  Devices
  - Full Wipe device
  - Clear Restriction
  - Selective Wipe device
  - ▶  View locations
  - Lock device

7. **Apply permissions** : 選択した権限を適用するグループを選択します。[To specific user groups] をクリックするとグループの一覧が開き、1つまたは複数のグループを選択できます。



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



9. ユーザーグループに役割を割り当てるための次の情報を入力します。

- **Select domain** : 一覧から、ドメインを選択します。
- **Include user groups** : [Search] をクリックして使用可能なすべてのグループの一覧を表示するか、グループ名の全体または一部を入力してその名前を持つグループのみに一覧を絞り込みます。
- 表示された一覧で、役割を割り当てるユーザーグループを選択します。ユーザーグループを選択すると、[Selected user groups] の一覧にグループが表示されます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. On the right, there is a user profile 'admin'. Below the navigation bar, the breadcrumb trail reads 'Settings > Role-Based Access Control > Add Role'. The main content area is titled 'Add Role' and has two tabs: '1 Role Info' and '2 Assignment', with '2 Assignment' being the active tab. The 'Assignment' section is titled 'Assignment' and has the subtitle 'Assign the RBAC role to user groups'. It contains a 'Select domain' dropdown menu set to 'testprise.net' and an 'Include user groups' search box containing the text 'user'. To the right of the search box is a blue 'Search' button. Below the search box is a list of user groups with checkboxes: 'testprise.net\Remote Desktop Users' (checked), 'testprise.net\Performance Monitor Users' (checked), and 'testprise.net\Performance Log Users' (unchecked). To the right of this list is a 'Selected user groups:' panel showing 'testprise.net' as the domain and two selected groups: 'Remote Desktop Users' and 'Performance Monitor Users', each with an 'X' icon for removal. At the bottom right of the page are 'Back' and 'Save' buttons.

注： [Selected user groups] の一覧からユーザーグループを削除するには、ユーザーグループ名の横にある [X] をクリックします。

10. [Save] をクリックします。

# 通知

Apr 27, 2017

XenMobileでの通知は以下の目的で利用できます。

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

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

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

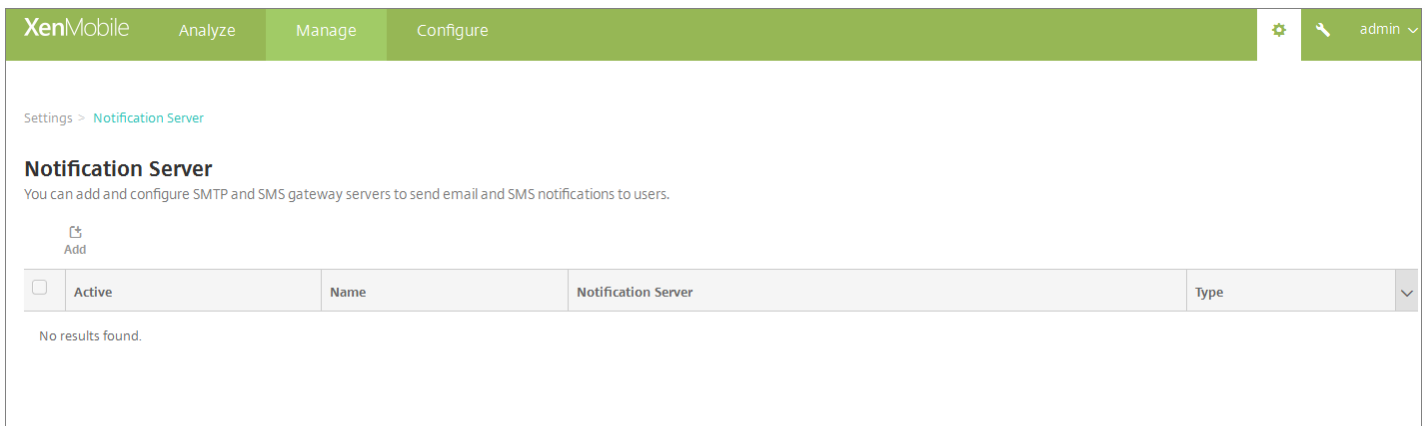
また、XenMobileでキャリアSMSゲートウェイを設定して、電話会社のSMSゲートウェイ経由で送信される通知を構成することもできます。電話会社はSMSゲートウェイを使用して、通信ネットワークと相互にSMSメッセージを送受信します。これらのテキストベースメッセージでは、標準化された通信プロトコルを使用して、固定電話または携帯電話端末でショートテキストメッセージを交換できます。

このアートの手順では、[SMTPサーバー](#)、[SMSゲートウェイ](#)、[キャリアSMSゲートウェイ](#)の構成方法について説明します。

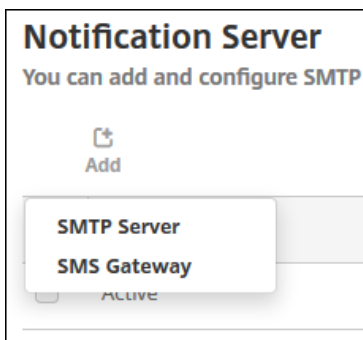
- SMSゲートウェイを構成する前に、システム管理者に問い合わせでサーバー情報を確認してください。SMSサーバーが社内サーバーでホストされているか、ホストされている電子メールサービスに含まれているかを確認することが重要です。前者の場合は、サービスプロバイダーのWebサイトからの情報が必要です。
- メッセージをユーザーに送信するためのSMTP通知サーバーを構成する必要があります。サーバーが社内サーバーでホストされている場合は、システム管理者に構成情報を問い合わせてください。サーバーが、ホストされている電子メールサービスの場合は、サービスプロバイダーのWebサイトで適切な構成情報を確認してください。
- 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コンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。

2. [Notifications] の下の [Notification Server] をクリックします。[Notification Server] ページが開きます。



2. **[Add]** をクリックします。SMTPサーバーおよびSMSゲートウェイを構成するためのオプションが含まれたメニューが開きます。



- SMTPサーバーを追加するには、**[SMTP Server]** を選択します。この設定を構成する手順については、[「SMTPサーバーを追加するには」](#)を参照してください。
- SMSゲートウェイを追加するには、**[SMS Gateway]** を選択します。この設定を構成する手順については、[「SMSゲートウェイを追加するには」](#)を参照してください。

Settings > Notification Server > Add SMTP Server

## Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
SMTP Server*	<input type="text"/>
Secure channel protocol	<input type="text" value="None"/>
SMTP server port*	<input type="text" value="25"/>
Authentication	<input type="checkbox" value="OFF"/>
Microsoft Secure Password Authentication (SPA)	<input type="checkbox" value="OFF"/>
From name*	<input type="text"/>
From email*	<input type="text"/>
<input type="button" value="Test Configuration"/>	
<a href="#">▶ Advanced Settings</a>	

1. 次の設定を構成します。

- **Name** : このSMTPサーバーアカウントに関連付ける名前を入力します。
- **Description** : 任意で、サーバーの説明を入力します。
- **SMTP Server** : サーバーのホスト名を入力します。ホスト名には、完全修飾ドメイン名 (FQDN) またはIPを指定できません。
- **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ンネルプロトコルとして [SSL]、[TLS]、または [None] を選択します。デフォルトは [None] です。
- **SMTP server port** : SMTPサーバーが使用するポートを入力します。デフォルトでは、ポートは25に設定されています。SMTP接続でSSLセキュアチャンネルプロトコルを使用する場合、ポートは465に設定されます。
- **Authentication** : [ON] または [OFF] を選択します。デフォルトは [OFF] です。



- [Authentication] を有効にした場合は、次の設定を構成します。
    - User name : 認証に使用するユーザー名を入力します。
    - Password : 認証に使用するユーザーのパスワードを入力します。
  - Microsoft Secure Password Authentication (SPA) : SMTPサーバーがSPAを使用している場合は、[ON] をクリックします。デフォルトは [OFF] です。
  - From Name : クライアントがこのサーバーから通知メールを受信したとき、メールの送信者として表示される名前を入力します。たとえば、「Corporate IT」です。
  - From email : SMTPサーバーによって送信された通知に、メール受信者が返信する場合に使用されるメールアドレスを入力します。
2. [Test Configuration] をクリックして、テストのメール通知を送信します。
3. [Advanced Settings] を展開して以下の設定を構成します。
- 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。デフォルトは5です。
  - SMTP Timeout : SMTP要求送信時に待機する時間 (秒) を入力します。送信しているメッセージが、タイムアウトに起因して失敗し続ける場合には、この値を大きくします。この値を小さくするとタイムアウト回数が多くなり、配信されないメッセージが増える場合があるため、注意してください。デフォルトは30秒です。
  - Maximum number of SMTP recipients : SMTPサーバーによって送信される各メールメッセージの最大受信者数を入力します。デフォルトは100です。
4. [Add] をクリックします。

Settings > Notification Server > Add SMS Gateway

## Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*	<input type="text"/>
Description	<input type="text"/>
Key*	<input type="text"/>
Secret*	<input type="text"/>
Virtual phone number*	<input type="text"/>
HTTPS	<input type="checkbox"/> OFF
Country code	<input type="text" value="Afghanistan +93"/>
Use Carrier Gateway	<input checked="" type="checkbox"/> ON
	<input type="button" value="Test Configuration"/>

## 注意

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

1. 次の設定を構成します。

- **Name** : SMSゲートウェイ構成の名前を入力します。このフィールドは必須です。
- **Description** : 任意で、構成の説明を入力します。
- **Key** : アカウントをアクティブ化するときシステム管理者から提供された、数値形式の識別子を入力します。このフィールドは必須です。
- **Secret** : パスワードを紛失した場合や盗まれた場合にアカウントへのアクセスに使用する、システム管理者から提供され

たシークレットを入力します。このフィールドは必須です。

- **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。このフィールドで使用できるのは、数字のみです。仮想電話番号はNexmoのWebサイトで購入できます。
- **HTTPS** : NexmoへのSMS要求の伝送にHTTPSを使用するかどうかを選択します。デフォルトは[OFF] です。

**重要** : HTTPSは、 [ON] に設定してください（Citrixサポートから [OFF] に設定するよう指示があった場合を除く）。

- **Country Code** : 一覧から、組織内受信者のデフォルトのSMS国コードプレフィックスを選択します。このフィールドは常に+記号で始まります。デフォルトは [Afghanistan +93] です。



2. [Test Configuration] をクリックし、現在の構成を使用してテストメッセージを送信します。認証エラーや仮想電話番号エラーなど、接続エラーが即時に検出され、表示されます。メッセージは、携帯電話間で送信された場合と同様の所要時間で受信されます。

2. [Add] をクリックします。

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



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

2. [Notifications] の下の [Carrier SMS Gateway] をクリックします。[Carrier SMS Gateway] ページが開きます。



XenMobile Analyze Manage Configure   admin ▾

Settings > Carrier SMS Gateway

## Carrier SMS Gateway

 Add |  Detect

<input type="checkbox"/>	Carrier	SMTP domain	Country code	Sending prefix	▾
<input type="checkbox"/>	Alltel	message.alltel.com	+1		
<input type="checkbox"/>	AT&T	txt.att.net	+1		
<input type="checkbox"/>	Boost Mobile	myboostmobile.com	+1		
<input type="checkbox"/>	Bouygues Telecom	mms.bouyguestelecom.fr	+33		
<input type="checkbox"/>	Cingular	cingularme.com	+1		
<input type="checkbox"/>	Metro PCS	mymetropcs.com	+1		
<input type="checkbox"/>	Nextel	messaging.nextel.com	+1		
<input type="checkbox"/>	Orange	websmsmms.orange.fr	+33		
<input type="checkbox"/>	Powertel	ptel.net	+1		
<input type="checkbox"/>	SFR	sfr.fr	+33		

Showing 1 - 10 of 16 items Showing 1 of 2  

3. 次のいずれかを行います。

- ゲートウェイを自動的に検出するには **[Detect]** をクリックします。新しいキャリアが検出されなかったことを示すダイアログボックス、または登録済みのデバイス間で検出された新しいキャリアを一覧表示したダイアログボックスが開きます。
- **[Add]** をクリックします。 **[Add a Carrier SMS Gateway]** ダイアログボックスが開きます。

## Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

**Carrier\***

**Gateway SMTP domain\***

**Country code\***

**Email sending prefix**

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

4. 次の設定を構成します。

- **Carrier**：電話会社の名前を入力します。
- **Gateway SMTP domain**：SMTPゲートウェイに関連付けられたドメインを入力します。
- **Country code**：一覧から、電話会社の国コードを選択します。
- **Email sending prefix**：任意で、メール送信プレフィックスを指定します。

5. [Add] をクリックして新しいキャリアを追加するか、[Cancel] をクリックして操作を取り消します。

## 通知テンプレートの作成および更新

XenMobileで通知テンプレートを作成または更新し、自動化された操作、登録、およびユーザーに送信される標準通知メッセージで使用できます。Secure Hub、SMTP、SMSの3つの異なるチャネル経由でメッセージを送信するための通知テンプレートを構成します。

XenMobileには、システム内のすべてのデバイスに対してXenMobileが自動的に応答する個別の種類イベントを反映した、定義済みの通知テンプレートが多数用意されています。

注：SMTPまたはSMSチャネルを使用してユーザーに通知を送信する場合は、アクティブ化する前にチャネルを設定する必要があります。通知テンプレートを追加するときにチャネルがまだ設定されていないと、チャネルを設定するよう求めるメッセージが表示されます。

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

Settings > Notification Templates

## Notification Templates

Create notification templates to use in automated actions, enrollment, and standard notification message delivery to users.

Add

<input type="checkbox"/>	Name	Channels	Type	Deletable	Manual sending supported
<input type="checkbox"/>	ActiveSync Gateway Blocked	Worx Home	ActiveSync Gateway blocked device		
<input type="checkbox"/>	Android Download Link	SMTP, SMS	Android Download Link		
<input type="checkbox"/>	APNS cert expiration	SMTP	APNS Cert Expiration		
<input type="checkbox"/>	Certificate renewal	Worx Home	Certificate is renewed		
<input type="checkbox"/>	Enrollment	SMTP, SMS	Enrollment Notification		
<input type="checkbox"/>	Enrollment Confirmation	SMTP, SMS	Enrollment Confirmation		
<input type="checkbox"/>	Enrollment Invitation	SMTP, SMS	Enrollment Invitation		
<input type="checkbox"/>	Enrollment PIN	SMTP, SMS	Enrollment PIN		
<input type="checkbox"/>	Failed Samsung KNOX attestation	Worx Home	Failed Samsung KNOX attestation		<input checked="" type="checkbox"/>
<input type="checkbox"/>	iOS Download Link	SMTP, SMS	iOS Download Link		

Showing 1 - 10 of 25 items Showing  of 3

### 通知テンプレートを追加するには

1. [Add] をクリックします。SMSゲートウェイまたはSMTPサーバーが設定されていない場合、SMSおよびSMTP通知に関するメッセージが表示されます。SMTPサーバーまたはSMSゲートウェイを今すぐ設定するか後で設定するかを選択できます。
- SMSまたはSMTPサーバーを今すぐ設定することを選択した場合は、[Settings] ページの [Notification Server] ページにリダイレクトされます。使用するチャンネルを設定した後、[Notification Template] ページに戻って、通知テンプレートの追加または変更を続けることができます。

## Important

SMSまたはSMTPサーバーの設定を後で行うことを選択した場合、通知テンプレートの追加または編集のときにこれらのチャン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ンネルを使用することができません。

2. 次の設定を構成します。

- **Name** : テンプレートの説明的な名前を入力します。
- **Description** : テンプレートの説明を入力します。
- **Type** : 一覧から、通知の種類を選択します。選択した種類でサポートされるチャネルのみが表示されます。定義済みテンプレートである [APNS Cert Expiration] テンプレートは1つだけ使用できます。つまり、この種類の新しいテンプレートは追加できません。

注 : テンプレートの種類の一部では、種類の下に [Manual sending supported] が表示されます。これは、このテンプレートが [Dashboard] および [Devices] ページの [Notifications] 一覧に表示され、手動でユーザーに通知を送信できることを意味します。いずれのチャネルの場合も、[Subject] フィールドまたは [Message] フィールドに以下のマクロが使われているテンプレートでは、手動送信は使用できません。

- `${outofcompliance.reason(whitelist_blacklist_apps_name)}`
- `${outofcompliance.reason(smug_block)}`

3. [Channels] で、この通知で使用される各チャネルの情報を構成します。一部またはすべてのチャネルを選択できます。選択するチャネルは、通知を送信する方法によって異なります。

- [Secure Hub] を選択した場合、iOSデバイスおよびAndroidデバイスのみが通知を受信し、通知はデバイスの通知トレイに表示されます。
- [SMTP] を選択した場合、ほとんどのユーザーはメールアドレスを使って登録するため、ほとんどのユーザーがメッセージを受信します。
- SMSを選択した場合、SIMカードが搭載されたデバイスのユーザーのみが通知を受信します。

Secure Hub :

- **Activate** : クリックして通知チャネルを有効にします。
- **Message** : ユーザーに送信されるメッセージを入力します。Secure Hubを使用する場合、このフィールドは必須です。
- **Sound File** : 一覧から、ユーザーが通知を受信したときに再生される通知音を選択します。

SMTP :

- **Activate** : クリックして通知チャネルを有効にします。

**重要** : SMTP通知は、SMTPサーバーが既に設定されている場合にのみ有効化できます。

- **Sender** : 任意で、通知の送信者 (名前、メールアドレス、またはその両方) を入力します。
- **Recipient** : このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMTP受信者アドレスに送信されるようにするためのマクロが事前設定されています。テンプレートのマクロは変更しないでください。アドレスをセミコロン (;) で区切って追加することにより、ユーザー以外の受信者 (社内の管理者など) を追加することもできます。アドホック通知を送信するには、このページで個別に受信者を入力するか、[Manage] の [Devices] ページでデバイスを選択して、そこから通知を送信します。詳しくは、「デバイス」を参照してください。
- **Subject** : 通知の説明的な件名を入力します。このフィールドは必須です。
- **Message** : ユーザーに送信されるメッセージを入力します。

SMS :

- **Activate** : クリックして通知チャネルを有効にします。

**重要** : SMS通知は、SMSゲートウェイが既に設定されている場合にのみ有効化できます。

- **Recipient** : このフィールドには、アドホック通知を除くすべての通知で、通知が正しいSMS受信者アドレスに送信されるようにするためのマクロが事前設定されています。テンプレートのマクロは変更しないでください。アドホック通知を送るには、個別に受信者を入力するか、**[Manage]** の **[Devices]** ページでデバイスを選択します。
- **Message** : ユーザーに送信されるメッセージを入力します。このフィールドは必須です。

5. **[Add]** をクリックします。すべてのチャンネルが正しく構成されている場合、**[Notification Templates]** ページに、SMTP、SMS、Secure Hubの順に表示されます。正しく構成されていないチャンネルがあれば、正しく構成されているチャンネルの後に表示されます。

#### 通知テンプレートを編集するには

1. 通知テンプレートを選択します。選択したテンプレートに固有の編集ページが開き、**[種類]** フィールド以外のすべてを変更することができます。チャンネルをアクティブ化または非アクティブ化することもできます。

2. **[Save]** をクリックします。

#### 通知テンプレートを削除するには

注：自分で追加した通知テンプレートのみを削除できます。定義済みの通知テンプレートは削除できません。

1. 既存の通知テンプレートを選択します。

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

2. **[Delete]** をクリックして通知テンプレートを削除するか、**[Cancel]** をクリックして通知テンプレートの削除を取り消します。



# デバイス

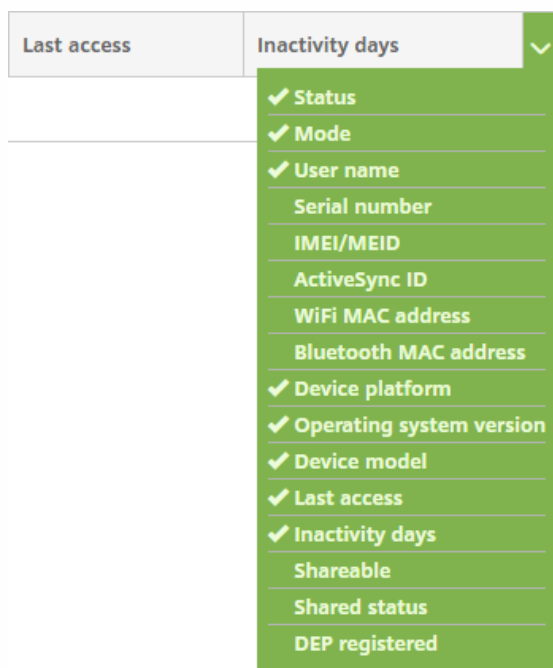
Apr 27, 2017

XenMobileサーバーのデータベースには、モバイルデバイスの一覧が保存されます。各モバイルデバイスは、一意のシリアル番号またはIMEI (International Mobile Station Equipment Identity) /MEID (Mobile Equipment Identifier) 識別番号によって定義されます。XenMobileコンソールにデバイスを追加するには、手動でデバイスを追加するか、ファイルからデバイスの一覧をインポートします。デバイスプロビジョニングファイル形式について詳しくは、「[デバイスプロビジョニングファイル形式](#)」を参照してください。

XenMobileコンソールの [Devices] ページは、各デバイスおよび以下の情報を表示します。

- **Status** (デバイスがジェイルブレイクされているか、管理されているか、Active Sync Gatewayが使用可能か、およびデバイスの展開環境の状態などを示すアイコンです)
- **Mode** (デバイスのモードがMDM、MAM、またはその両方かを示します)
- ほかにも、デバイスの次のような情報を表示できます。**User name**、**Device platform**、**Operating system version**、**Device model**、**Last access**、**Inactivity days**。これらは、デフォルトで表示される見出しです。

末尾の見出しの下向き矢印をクリックし、追加で表示する見出しをオンにしたり表示しない見出しをオフにしたりして、[Devices] ページの表に示される内容をカスタマイズできます。



手動によるデバイスの追加、デバイスプロビジョニングファイルからのデバイスのインポート、デバイスの詳細の編集、デバイスへの通知の送信、デバイスの削除を行うことができます。デバイス表のデータ全体を.csvファイルにエクスポートして、このファイルからカスタムレポートを作成することもできます。すべてのデバイスの属性がエクスポートされますが、フィルターを適用している場合、XenMobileは.csvファイルの作成時にそのフィルターを使用します。

デバイスの管理について詳しくは、以下のセクションを参照してください。

- [手動によるデバイスの追加](#)
- [デバイスプロビジョニングファイルからのデバイスのインポート](#)

- セキュリティの操作を実行する
- デバイスへの通知の送信
- デバイスの削除
- [Devices] の表をエクスポートするには
- ユーザーデバイスの手動タグ付け
- デバイスプロビジョニングファイル形式
- デバイスのプロパティ名と値

1. XenMobileコンソールで、[Manage] > [Devices] の順にクリックします。[Devices] ページが開きます。

Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>	MDM MAM	us1user1@...net "us1 user1"	Android	5.0.2
<input type="checkbox"/>	MDM MAM	us3user3@...net "us3 user3"	iOS	8.4.1

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

3. 次の設定を構成します。

- Select platform : [iOS] または [Android] を選択します。
- Serial Number : デバイスのシリアル番号を入力します。
- IMEI/MEID : Androidデバイスに限り、任意で、デバイスのIMEI/MEID情報を入力します。

4. [Add] をクリックします。[Devices] の表に示される一覧の一番下に、追加したデバイスが表示されます。追加したデバイスを一覧で選択して表示されるメニューで [Edit] をクリックし、デバイスの詳細を表示して確認します。

注：デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Manage' tab is active. Below the tabs, there are sub-tabs for 'Devices', 'Users', and 'Enrollment'. The 'Devices' sub-tab is selected. The main content area is titled 'Device details' and has a close button (X) in the top right corner. On the left side of the 'Device details' panel, there is a table of sections:

1 General
2 Properties
3 Assigned Policies
4 Apps
5 Actions
6 Delivery Groups
7 iOS Profiles
8 iOS Provisioning Profiles
9 Certificates
10 Connections

The main content area is divided into two sections: 'General Identifiers' and 'Security'. The 'General Identifiers' section contains the following information:

Serial Number	A123
IMEI/MEID	NONE
ActiveSync ID	NONE
WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	<input type="radio"/> Corporate <input type="radio"/> BYOD

The 'Security' section contains the following information:

Strong ID	QYD7UUSF
Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device Unlock	No device unlock.

At the bottom right of the 'Device details' panel, there is a green button labeled 'Next >'.

5. [General] ページには、デバイスのID（シリアル番号、ActiveSync ID、プラットフォームの種類に関するその他の情報など）が表示されます。[Device Ownership] で、[Corporate] または [BYOD] を選択します。

[General] ページには、デバイスの [Security] プロパティ（[Strong ID]、[Lock Device]、[Activation Lock Bypass]、プラットフォームの種類に関するその他の情報など）も表示されます。

6. [Properties] ページには、XenMobileがプロビジョニングするデバイスのプロパティが表示されます。この一覧は、デバイスの追加に使用されるプロビジョニングファイルに含まれるデバイスのプロパティを表示します。プロパティを追加するには、[Add] をクリックして一覧からプロパティを選択します。各プロパティの有効な値に関しては、このページの [デバイスのプロパティ名と値](#) を参照してください。

プロパティを追加すると、最初に追加したカテゴリに表示されます。[Next] をクリックして [Properties] ページに戻ると、プロパティは適切な一覧に表示されます。

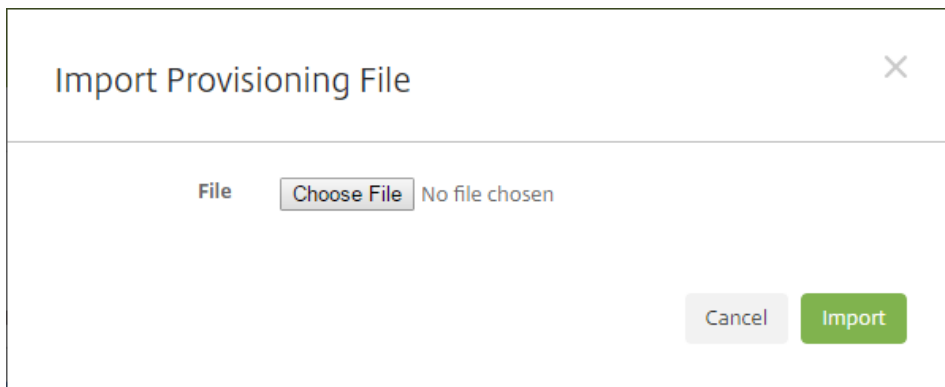
プロパティを削除するには、項目の上にマウスマウスカーソルを置いて、右側の[X] をクリックします。XenMobileデバイスがその項目を検出します。

7. 残りの [Device Details] セクションには、デバイスの概要が含まれます。

- **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、最新展開の情報が表示されます。
- **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。アプリ名、ID、種類、その他の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。最新展開のアクション名と時間が表示されます。
- **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。各展開のデリバリーグループ名と展開時間が表示されます。デリバリーグループを選択すると、状態、アクション、チャンネル、またはユーザーなどの詳細な情報を表示できます。
- **iOS Profiles** : 名前、種類、組織、説明など、最新のiOSプロファイルインベントリが表示されます。
- **iOSプロビジョニングプロファイル** : UUID、有効期限、管理対象かどうかなど、エンタープライズ配布プロビジョニングプロファイルの情報を表示します。
- **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番目の認証時間、最後の認証時間が表示されます。
- **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。

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ったりすることができます。詳しくは、「[デバイスプロビジョニングファイル形式](#)」を参照してください。

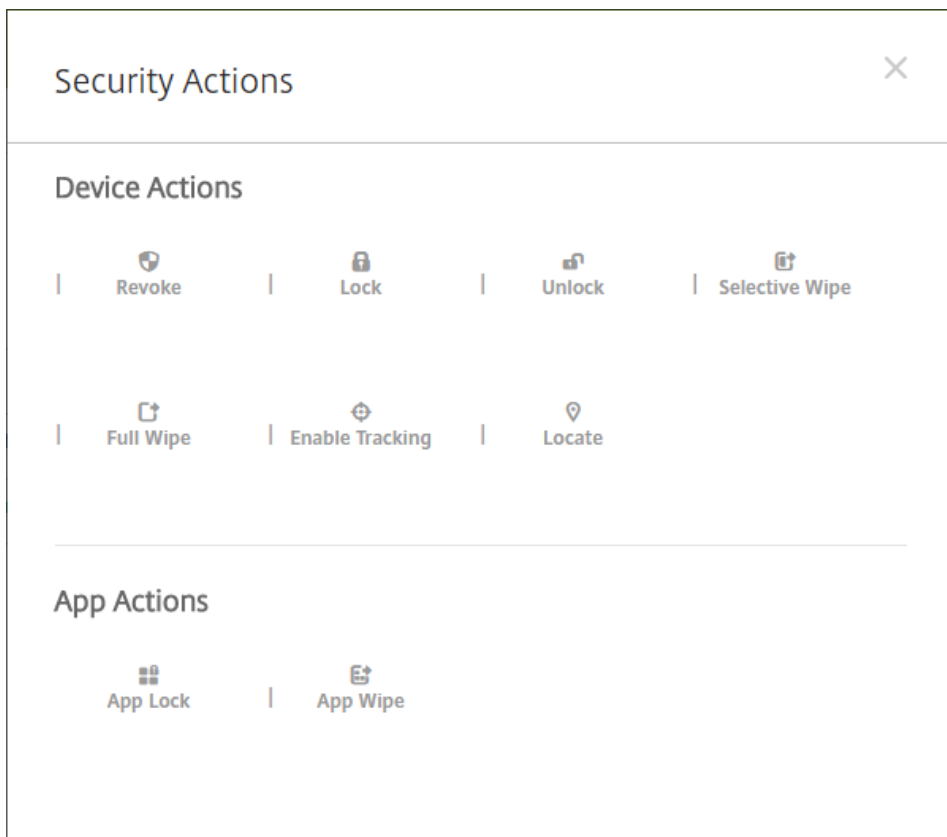
1. [Manage]、[Devices] に移動して、[Import] を選択します。[Import Provisioning File] ダイアログボックスが開きます。



2. [Choose File] を選択して、インポートするファイルまで移動します。
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。
4. デバイスの情報を編集するには、[Device details] を選択して[Edit] をクリックします。[Device details] ページについて詳しくは、「[手動によるデバイスの追加](#)」を参照してください。

[Devices] ページでデバイスやアプリのセキュリティの操作を実行できます。デバイスの操作には、取り消し、ロック、ロック解除、ワイプがあります。アプリのセキュリティの操作には、アプリのロック、アプリのワイプが含まれます。

1. [Manage] > [Devices] に移動し、デバイスを選択して [Secure] をクリックします。
  2. [Security Actions] で、操作をクリックし、表示されるメッセージに対応します。
- 自動化された操作について詳しくは、「[自動化された操作](#)」を参照してください。



アプリのロック、ロック解除、ワイプ、ワイプ解除を実行するには

1. [Manage] > [Devices] に移動し、管理対象デバイスを選択して [Secure] をクリックします。
2. [Security Actions] ダイアログボックスで、アクションをクリックします。

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

3. アクションを確認します。

[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、[通知](#)を参照してください。

1. [Manage] > [Devices] ページで、通知を送信するデバイスを選択します。
2. [Notify] をクリックします。[Notification] ダイアログボックスが開きます。[Recipients] フィールドに、通知を受信するすべてのデバイスの一覧が表示されます。

Notification
✕

---

**Recipients**

**Templates** Ad Hoc ▾

**Channels**  SMTP  SMS

SMTP

SMS

**Sender**

**Subject**

**Message**

Cancel
Notify

3. 次の設定を構成します。

- **Templates** : 一覧から、送信する通知の種類を選択します。[Ad Hoc] を選択した場合を除き、[Subject] フィールドおよび [Message] フィールドには、選択したテンプレートで構成済みのテキストが入力されます。
- **Channels** : メッセージの送信方法を選択します。デフォルトは [SMTP] および [SMS] です。各チャンネルのメッセージの形式を表示するには、タブをクリックします。
- **Sender** : オプションで送信者を入力します。
- **Subject** : アドホックメッセージの場合、件名を入力します。
- **Message** : アドホックメッセージの場合、メッセージを入力します。

4. [Notify] をクリックします。

1. [Devices] の表で、削除するデバイスを選択します。

2. [Delete] をクリックします。確認ダイアログボックスが開きます。もう一度 [Delete] をクリックします。この操作を元に戻すことはできません。

1. エクスポートファイルで表示する内容によって、[Devices] の表にフィルターを適用します。

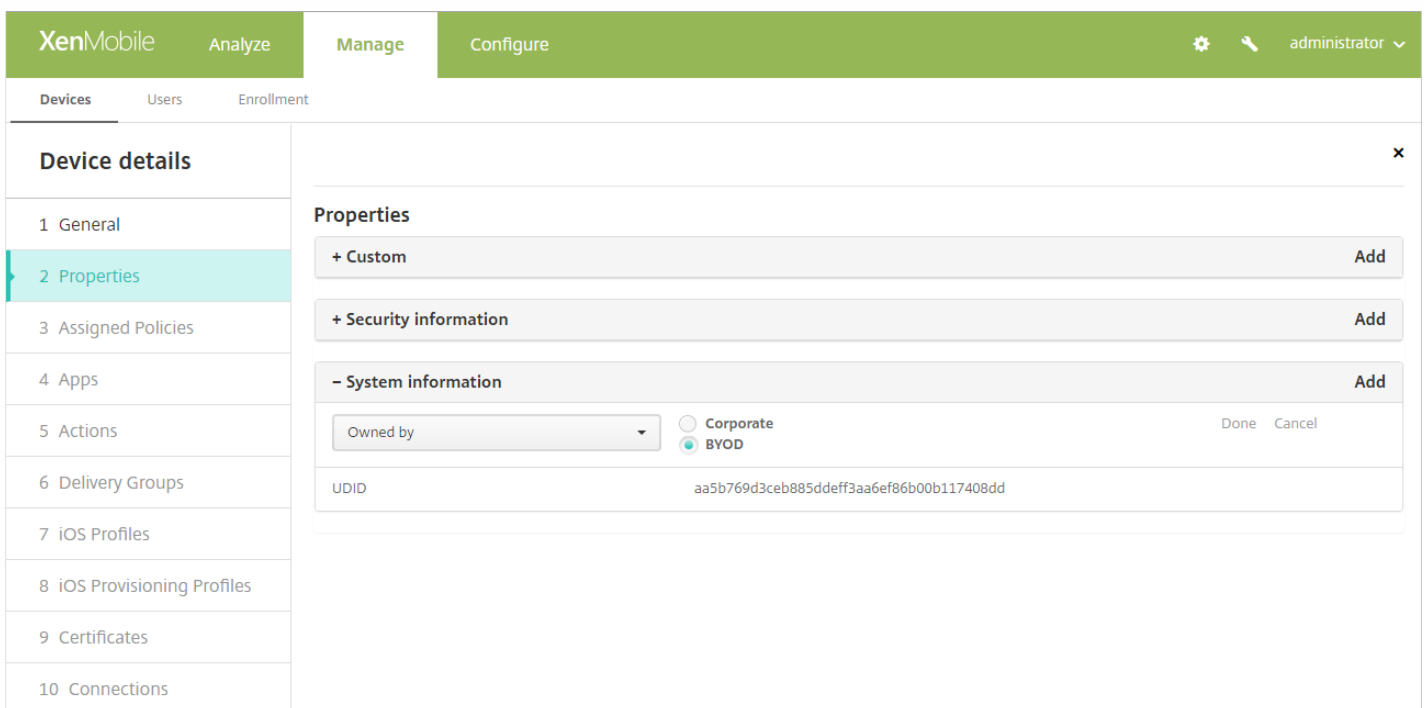
2. [Devices] の表の上にある [Export] をクリックします。XenMobileによって [Delivery] の表の情報が抽出され、.csv ファイルに変換されます。

3. .csvファイルを開くか、保存します。使用するブラウザに応じて、手順が異なります。操作を取り消すこともできます。

次のいずれかの方法で、XenMobileのデバイスに手動でタグ付けすることができます。

- 招待状に基づく登録処理中
- Self Help Portal登録処理中
- デバイスの所有権をデバイスプロパティとして追加する

組織または個人所有のいずれかとして、デバイスにタグ付けするオプションが用意されています。Self Help Portalを使ってデバイスを自動登録するとき、組織または個人所有のいずれかとして、デバイスにタグを付けることもできます。次の図に示すように、手動でデバイスをタグ付けすることもできます。XenMobileコンソールの [Devices] タブからデバイスにプロパティを追加し、[Owned by] という名前のプロパティを追加し、[Corporate] または [BYOD]（従業員所有）を選択します。



## デバイスプロビジョニングファイル形式

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：

- プロパティ名と値について詳しくは、次のセクションの「デバイスのプロパティ名と値」を参照してください。
- UTF-8形式の文字セットを使用します。
- プロビジョニングファイル内では、フィールドをセミコロン (;) で区切ります。フィールドの一部としてセミコロンが含まれる場合は、バックスラッシュ文字 (\) を使ってエスケープする必要があります。

たとえば、次のプロパティの場合：

```
propertyV;test;1;2
```

次のようにエスケープします：

```
propertyV\;test\;1\;2
```

- シリアル番号はiOSデバイスの識別子であるため、iOSデバイスにはシリアル番号が必須です。
- その他のデバイスプラットフォームの場合、シリアル番号またはIMEIが必要です。
- OperatingSystemFamilyの有効な値は、WINDOWS、ANDROID、iOSのいずれかです。

```

1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyN;propertyV$*&&ééétest

3050BF3F517301081610065510590393;35244201625379903;iOS;test;

4050BF3F517301081610065510590393;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

```

ファイルの各行にデバイスの説明が含まれています。上のサンプルの最初のエンタリは以下を意味しています。

- SerialNumber : 1050BF3F517301081610065510590391
- IMEI : 15244201625379901
- OperatingSystemFamily : WINDOWS
- PropertyName : propertyN
- PropertyValue : propertyV\;test\;1\;2;prop 2

## デバイスのプロパティ名と値

[Manage] > [Devices] ページのプロパティ名	デバイスプロビジョニングファイルの名前と値	値の種類
AIKの有無	WINDOWS_HAS_AIK_PRESENT	文字列



アカウントを一時停止しますか?	GOOGLE_AW_DIRECTORY_SUSPENDED	文字列
アクティベーションロックバイパスコード	ACTIVATION_LOCK_BYPASS_CODE	文字列
アクティベーション ロックが有効になっています	ACTIVATION_LOCK_ENABLED 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
アクティブなiTunesアカウント	ACTIVE_ITUNES 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
ActiveSync ID	EXCHANGE_ACTIVESYNC_ID	文字列
MSPにより認知されたActiveSyncデバイス	AS_DEVICE_KNOWN_BY_ZMSP 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
管理者が無効になっています	ADMIN_DISABLED 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
Amazon MDM API実行可能	AMAZON_MDM 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
Android for WorkデバイスID	GOOGLE_AW_DEVICE_ID	文字列
Android for Work対応デバイスですか?	GOOGLE_AW_ENABLED_DEVICE	文字列
Android for Workインストールの種類	GOOGLE_AW_INSTALL_TYPE 値 :	文字列

	DeviceAdministrator (デバイス所有者) AvengerManagedProfile (Work管理対象デバイス) ManagedProfile (Workプロファイル)	
アセットタグ	ASSET_TAG	文字列
自動更新の状態	AUTOUPDATE_STATUS	文字列
使用できるRAM	MEMORY_AVAILABLE	整数
使用できるストレージ領域	TOTAL_DISK_SPACE	整数
BIOS情報	BIOS_INFO	文字列
バックアップバッテリー	BACKUP_BATTERY_PERCENT	整数
ベースバンドファームウェアのバージョン	MODEM_FIRMWARE_VERSION	文字列
バッテリー状態	BATTERY_STATUS	文字列
バッテリー充電	BATTERY_CHARGING 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
MSPによって認知されているBESデバイス	BES_DEVICE_KNOWN_BY_ZMSP 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
BES PIN	BES_PIN	文字列
BESサーバーエージェントID	ENROLLMENT_AGENT_ID	文字列
BESサーバー名	BES_SERVER	文字列
BESサーバーのバージョン	BES_VERSION	文字列

Bit Lockerの状態	WINDOWS_HAS_BIT_LOCKER_STATUS	文字列
Bluetooth MACアドレス	BLUETOOTH_MAC	文字列
ブートデバッグが有効化されているかどうか	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	文字列
ブートマネージャのバージョン	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	文字列
CPUクロック速度	CPU_CLOCK_SPEED	整数
CPUの種類	CPU_TYPE	文字列
キャリア設定バージョン	CARRIER_SETTINGS_VERSION	文字列
携帯ネットワーク緯度	GPS_LATITUDE_FROM_CELLULAR	文字列
携帯ネットワーク経度	GPS_LONGITUDE_FROM_CELLULAR	文字列
携帯ネットワーク テクノロジ	CELLULAR_TECHNOLOGY	整数
携帯ネットワークタイムスタンプ	GPS_TIMESTAMP_FROM_CELLULAR	日付
次のログイン時にパスワードを変更しますか?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	文字列
クライアントデバイスID	CLIENT_DEVICE_ID	文字列
クラウドバックアップが有効になりました	CLOUD_BACKUP_ENABLED 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
コードの整合性チェックが有効化されているかどうか	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	文字列
コード整合性のバージョン	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	文字列
カラー	COLOR	文字列

作成時刻	GOOGLE_AW_DIRECTORY_CREATION_TIME	文字列
現在のキャリアネットワーク	CURRENT_CARRIER_NETWORK	文字列
現在のモバイル国コード	CURRENT_MCC	整数
現在のモバイルネットワークコード	CURRENT_MNC	文字列
DEP ポリシー	WINDOWS_HAS_DEP_POLICY	文字列
データローミングが許可されました	DATA_ROAMING_ENABLED 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
最新の iCloud バックアップ日	LAST_CLOUD_BACKUP_DATE	日付
説明	DESCRIPTION	文字列
デバイス登録プログラムのプロフィール割り当て済み	PROFILE_ASSIGN_TIME	日付
デバイス登録プログラムのプロフィールプッシュ済み	PROFILE_PUSH_TIME	日付
デバイス登録プログラムプロフィールが削除されました	PROFILE_REMOVE_TIME	日付
デバイス登録プログラムの登録者	DEVICE_ASSIGNED_BY	文字列
デバイス登録プログラムの登録日付	DEVICE_ASSIGNED_DATE	日付
デバイスの種類	DEVICE_TYPE	文字列
デバイスのモデル	MODEL_ID	文字列
デバイス名	DEVICE_NAME	文字列

ボイスメールへ自動転送がアクティブになりました	DO_NOT_DISTURB 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
ELAMドライバーが起動されているかどうか	WINDOWS_HAS_ELAM_DRIVER_LOADED	文字列
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	日付
エンタープライズID	ENTERPRISE_ID	文字列
外部ストレージ1: 使用可能領域	EXTERNAL_STORAGE1_FREE_SPACE	整数
外部ストレージ1: 名前	EXTERNAL_STORAGE1_NAME	文字列
外部ストレージ1: 総領域	EXTERNAL_STORAGE1_TOTAL_SPACE	整数
外部ストレージ2: 使用可能領域	EXTERNAL_STORAGE2_FREE_SPACE	整数
外部ストレージ2: 名前	EXTERNAL_STORAGE2_NAME	文字列
外部ストレージ2: 総領域	EXTERNAL_STORAGE2_TOTAL_SPACE	整数
外部ストレージが暗号化されました	EXTERNAL_ENCRYPTION 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
ファイアウォールの状態	FIREWALL_STATUS	文字列
ファームウェアのバージョン	FIRMWARE_VERSION	文字列
最初の同期	ZMSP_FIRST_SYNC	日付
GPS高度	GPS_ALTITUDE_FROM_GPS	文字列
GPS緯度	GPS_LATITUDE_FROM_GPS	文字列

GPS経度	GPS_LONGITUDE_FROM_GPS	文字列
GPSタイムスタンプ	GPS_TIMESTAMP_FROM_GPS	日付
Googleディレクトリのエイリアス	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	文字列
Googleディレクトリのファミリー名	GOOGLE_AW_DIRECTORY_FAMILY_NAME	文字列
Googleディレクトリ名	GOOGLE_AW_DIRECTORY_NAME	文字列
Googleディレクトリのプライマリメール	GOOGLE_AW_DIRECTORY_PRIMARY	文字列
Googleディレクトリユーザー ID	GOOGLE_AW_DIRECTORY_USER_ID	文字列
HAS_CONTAINER	HAS_CONTAINER 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
HTC APIバージョン	HTC_MDM_VERSION	文字列
HTC MDM API実行可能	HTC_MDM 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
ハードウェア暗号化機能	HARDWARE_ENCRYPTION_CAPS	整数
現在ログオンしているiTunesストアアカウントのハッシュ	ITUNES_STORE_ACCOUNT_HASH	文字列
ホームキャリアネットワーク	SIM_CARRIER_NETWORK	文字列
ホームモバイル国コード	SIM_MCC	整数
ホームモバイルネットワークコード	SIM_MNC	文字列
ICCID	ICCID	文字列

IMEI/MEID番号	IMEI	文字列
IMSI	IMSI	文字列
IPの場所	IP_LOCATION	文字列
ID	AS_DEVICE_IDENTITY	文字列
内部ストレージが暗号化されました	LOCAL_ENCRYPTION 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
発行元	WINDOWS_HAS_ISSUED_AT	文字列
ジェイルブレイク済み/ルート指定済み	ROOT_ACCESS 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
カーネルのデバッグが有効化されているかどうか	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	文字列
KIOSKモード	IS_KIOSK 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
前回認知したIPアドレス	LAST_IP_ADDR	文字列
前回のポリシー更新時間	LAST_POLICY_UPDATE_TIME	日付
前回の同期	ZMSP_LAST_SYNC	日付
ロケータサービスが有効になっていません	DEVICE_LOCATOR 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型

MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	文字列
MEID	MEID	文字列
メールボックスセットアップ	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	文字列
メインバッテリー	MAIN_BATTERY_PERCENT	整数
携帯電話番号	TEL_NUMBER	文字列
モデルID	SYSTEM_OEM	文字列
ネットワークアダプターの種類	NETWORK_ADAPTER_TYPE	文字列
NitroDesk TouchDownがインストールされました	TOUCHDOWN_FIND 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
MDMを介してNitroDesk TouchDownがライセンス化されました	TOUCHDOWN_LICENSED_VIA_MDM 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
オペレーティングシステムビルド	SYSTEM_OS_BUILD	文字列
オペレーティングシステム言語 (ロケール)	SYSTEM_LANGUAGE	文字列
オペレーティングシステムのバージョン	SYSTEM_OS_VERSION	文字列
組織のアドレス	ORGANIZATION_ADDRESS	文字列
組織のメール	ORGANIZATION_EMAIL	文字列
組織のマジック	ORGANIZATION_MAGIC	文字列
組織名	ORGANIZATION_NAME	文字列



組織の電話番号	ORGANIZATION_PHONE	文字列
その他	OTHER	文字列
コンプライアンス違反	OUT_OF_COMPLIANCE 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
所有者	CORPORATE_OWNED 値の(意味) : 1 (コーポレート) 0 (BYOD)	ブーリアン型
PCRO	WINDOWS_HAS_PCRO	文字列
ジオフェンスのPINコード	PIN_CODE_FOR_GEO_FENCE	文字列
パスコード準拠	PASSCODE_IS_COMPLIANT 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
構成に準拠したパスコード	PASSCODE_IS_COMPLIANT_WITH_CFG 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
現在のパスコード	PASSCODE_PRESENT 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
境界違反	GPS_PERIMETER_BREACH 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
パーソナルホットスポットがアクティブ	PERSONAL_HOTSPOT_ENABLED	ブーリアン型

になりました	値 (意味) : 1 (はい) 0 (いいえ)	アン型
プラットフォーム	SYSTEM_PLATFORM	文字列
プラットフォームAPIレベル	API_LEVEL	整数
ポリシー名	POLICY_NAME	文字列
プライマリ電話番号	IDENTITY1_PHONENUMBER	文字列
プライマリSIM IMEI	IDENTITY1_IMEI	文字列
プライマリSIM IMSI	IDENTITY1_IMSI	文字列
プライマリSIMローミング	IDENTITY1_ROAMING  値 (意味) : 1 (真) 0 (偽)	ブーリアン型
製品名	PRODUCT_NAME	文字列
発行元デバイスID	PUBLISHER_DEVICE_ID	文字列
リセット回数	WINDOWS_HAS_RESET_COUNT	文字列
再起動の回数	WINDOWS_HAS_RESTART_COUNT	文字列
SBCPハッシュ	WINDOWS_HAS_SBCP_HASH	文字列
SMS可	IS_SMS_CAPABLE  値 (意味) : 1 (真) 0 (偽)	ブーリアン型
セーフモードが有効化されているかどうか	WINDOWS_HAS_SAFE_MODE	文字列

Samsung KNOX API実行可能	SAMSUNG_KNOX 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
Samsung KNOX APIバージョン	SAMSUNG_KNOX_VERSION	文字列
Samsung KNOX構成証明	SAMSUNG_KNOX_ATTESTED 値 (意味) : 1 (成功) 0 (失敗)	ブーリアン型
Samsung KNOX構成証明更新日	SAMSUNG_KNOX_ATT_UPDATED_TIME	日付
Samsung SAFE API実行可能	SAMSUNG_MDM 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
Samsung SAFE APIバージョン	SAMSUNG_MDM_VERSION	文字列
画面 : X軸解像度	SCREEN_XDPI	整数 (PPI)
画面 : Y軸解像度	SCREEN_YDPI	整数 (PPI)
画面 : 高さ	SCREEN_HEIGHT	整数 (ピクセル)
画面 : 色数	SCREEN_NB_COLORS	整数
画面サイズ :	SCREEN_SIZE	10進 (インチ)
画面 : 幅	SCREEN_WIDTH	整数

		(ピクセル)
セカンダリ電話番号	IDENTITY2_PHONENUMBER	文字列
セカンダリSIM IMEI	IDENTITY2_IMEI	文字列
セカンダリSIM IMSI	IDENTITY2_IMSI	文字列
セカンダリSIMローミング	IDENTITY2_ROAMING 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
セキュアブートが有効化されているかどうか	WINDOWS_HAS_SECURE_BOOT_ENABLED	文字列
SecureContainer有効	WINDOWS_HAS_BIT_LOCKER_STATUS	文字列
シリアル番号	SERIAL_NUMBER	文字列
Sony Enterprise API実行可能	SONY_MDM 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
Sony Enterprise APIバージョン	SONY_MDM_VERSION	文字列
監視	監視 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
一時停止理由	GOOGLE_AW_DIRECTORY_SUSPENSION_REASON	文字列
改ざん状態	TAMPERED_STATUS	文字列
契約条件	TERMS_AND_CONDITIONS	文字列

条件および契約を承認しますか?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	文字列
テスト署名が有効化されているかどうか	WINDOWS_HAS_TEST_SIGNING_ENABLED	文字列
RAM合計	MEMORY	整数
総ストレージ領域	FREEDISK	整数
UDID	UDID	文字列
ユーザーエージェント	USER_AGENT	文字列
ユーザー定義#1	USER_DEFINED_1	文字列
ユーザー定義#2	USER_DEFINED_2	文字列
ユーザー定義#3	USER_DEFINED_3	文字列
ユーザー言語 (ロケール)	USER_LANGUAGE	文字列
VSMが有効であること。	WINDOWS_HAS_VSM_ENABLED	文字列
ベンダー	VENDOR	文字列
音声可	IS_VOICE_CAPABLE 値 (意味) : 1 (真) 0 (偽)	ブーリアン型
音声ローミングが許可されました	VOICE_ROAMING_ENABLED 値 (意味) : 1 (はい) 0 (いいえ)	ブーリアン型
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	文字列
WNS通知の状態	WNS_PUSH_STATUS	文字列

WNS通知URL	PROPERTY_WNS_PUSH_URL	文字列
WNS通知URL有効期限	PROPERTY_WNS_PUSH_URL_EXPIRY	文字列
WiFi MACアドレス	WIFI_MAC	文字列
WinPEが有効であること。	WINDOWS_HAS_WINPE	文字列
XenMobileエージェントID	AGENT_ID	文字列
XenMobileエージェントレビジョン	EW_REVISION	文字列
XenMobileエージェントバージョン	EW_VERSION	文字列

# iOSデバイスのロック

Apr 27, 2017

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

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

1. XenMobileコンソールで、**[Manage]** の **[Devices]** をクリックします。**[Devices]** ページが開きます。

XenMobile Analyze Manage Configure

Devices Users Enrollment

Devices Show filter

Add Import Export Refresh

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>		MDM MAM	us1user1@...net "us1 user1"	Android	5.0.2
<input type="checkbox"/>		MDM MAM	us3user3@...net "us3 user3"	iOS	8.4.1

2. ロックするiOSデバイスを選択します。

デバイスの横にあるチェックボックスをオンにすると、デバイス一覧の上にオプションメニューが表示されます。一覧で項目をクリックして、その項目の右側にオプションメニューを表示できます。

XenMobile Analyze Manage Configure administrator

Devices Users Enrollment

Devices Show filter Search

Add Edit Deploy Secure Notify Delete Import Export Refresh

<input type="checkbox"/>	Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
<input checked="" type="checkbox"/>		MDM MAM	ka@...net "ka user1"	SEC14F1C873A5214	Android	4.4.4	GT-19305	08/17/2016 07:40:34 am	0 day
<input type="checkbox"/>		MDM MAM	aa@...net "aa user1"	S7NN8B1R3H38973954LCTS6QLC	iOS	9.3.2	iPhone	08/17/2016 04:48:29 am	0 day

XenMobile Analyze Manage Configure administrator

Devices Users Enrollment

Devices Show filter Search

Add Import Export Refresh

Status	Mode	User name	ActiveSync ID	Device platform	Operating system version	Device model	Last access	Inactivity days
	MDM MAM	ka@...net	SEC14F1C873A5214	Android	4.4.4	GT-I9305	08/17/2016 07:40:34 am	0 day
	MDM MAM	aa@...net	S7NN8B1R3H38973954LCTS6QLC	iOS				

Edit Deploy **Secure** Notify Delete

XME Device Managed

Delivery Groups	2	Policies	5
Actions	2	Apps	15

Show more >

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

Security Actions

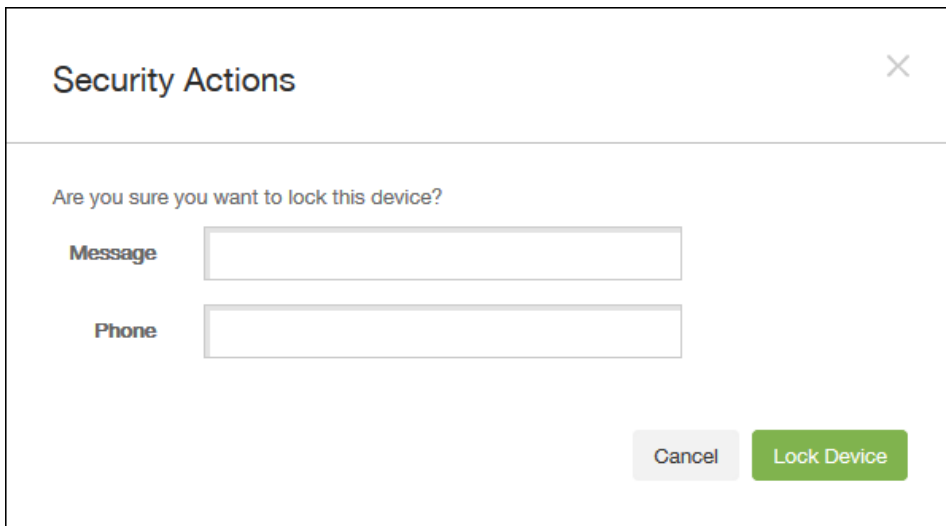
Device Actions

Revoke **Lock** Unlock Selective Wipe

Full Wipe Enable Tracking Locate Request AirPlay Mirroring

4. [Lock] をクリックします。 [Security Actions] 確認ダイアログボックスが開きます。





Security Actions

Are you sure you want to lock this device?

Message

Phone

Cancel Lock Device

5. 必要に応じて、デバイスのロック画面に表示するメッセージと電話番号を入力します。

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

6. [Lock Device] をクリックします。

# XenMobile AutoDiscoveryサービス

Apr 27, 2017

多くのXenMobile展開にとって、自動検出は重要な要素となります。自動検出を使用するとユーザーの登録処理が簡単になります。ユーザーは、ネットワークユーザー名とActive Directoryパスワードを使用してデバイスを登録できます。XenMobileサーバーの詳細を入力する必要はありません。ユーザーは、ユーザー名をユーザープリンシパル名 (User Principal Name : UPN) 形式で入力します (たとえば、user@mycompany.com)。XenMobile AutoDiscoveryサービスを使用すると、Citrixサポートの補助を受けずに自動検出レコードを作成または編集できます。

XenMobile AutoDiscoveryサービスにアクセスするには、<https://xenmobiletools.citrix.com>に移動して [Request Auto Discovery] をクリックします。

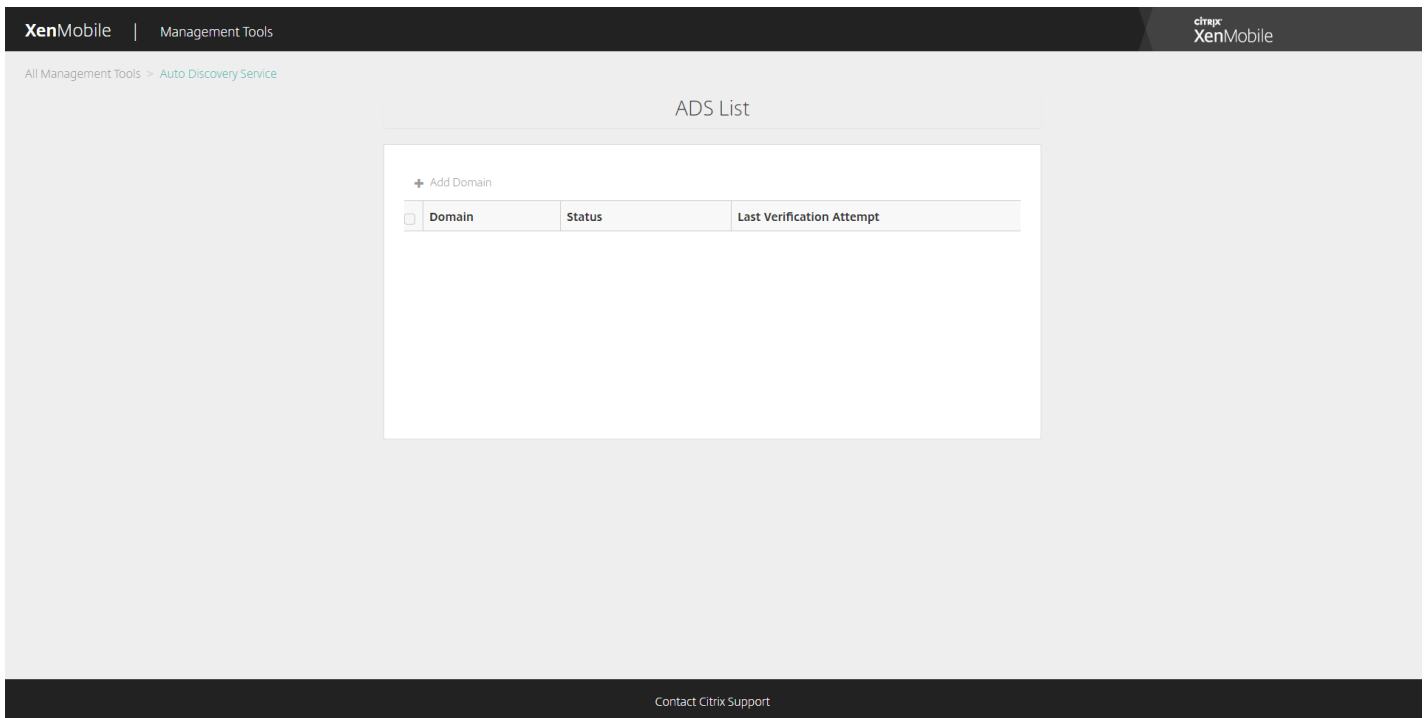
The screenshot shows the XenMobile Management Tools interface. At the top, there is a navigation bar with 'XenMobile | Management Tools' on the left and the Citrix XenMobile logo on the right. Below the navigation bar, the main content area is titled 'All Management Tools' and 'What do you want to do?'. A sub-header reads: 'XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.' Below this, there are four main action cards:

- Analyze and Troubleshoot my XenMobile environment**: XenMobile Analyzer. Follow steps to identify and triage potential issues with your deployment.
- Request Auto Discovery**: Auto Discovery Service. Request and Configure Auto Discovery for your domain's XenMobile Server.
- Request push notification certificate signature**: Create APNs Certificate. Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.
- Enable APNs-based push notifications for WorxMail for iOS**: Upload APNs Certificate. Enable push notifications by uploading APNs certificate from Apple.

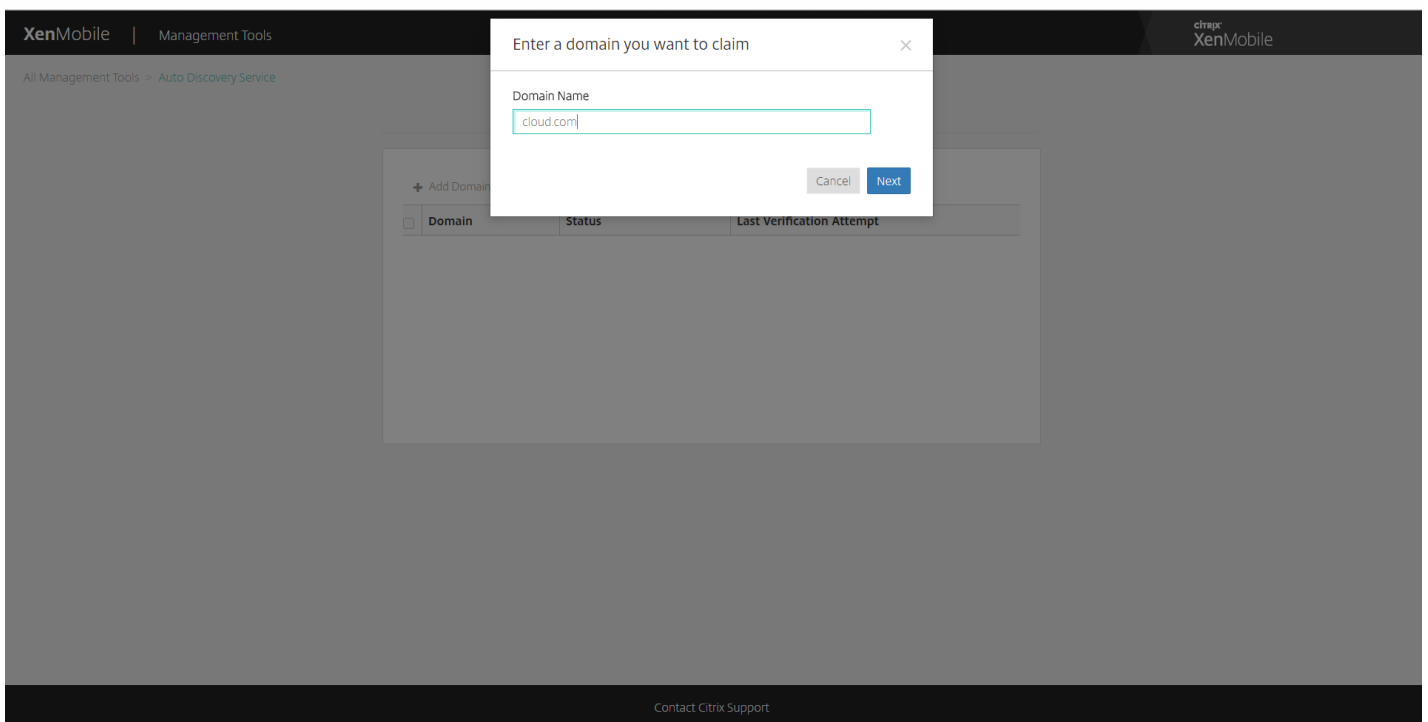
At the bottom of the interface, there is a 'Contact Citrix Support' link.

## AutoDiscoveryのリクエスト

1. AutoDiscoveryサービスのページでは、まずドメインを指定する必要があります。[Add Domain] をクリックします。



2. 開いたダイアログボックスで、お使いのXenMobile環境のドメイン名を入力してから[Next] をクリックします。



3. 次の手順では、ユーザーがドメインの所有者であることを確認するための手順が示されます。

- a. XenMobileツールポータルで提供されたDNSトークンをコピーします。
- b. ドメインホスティングプロバイダーポータルで、ドメインのゾーンファイルにDNS TXTレコードを作成します。

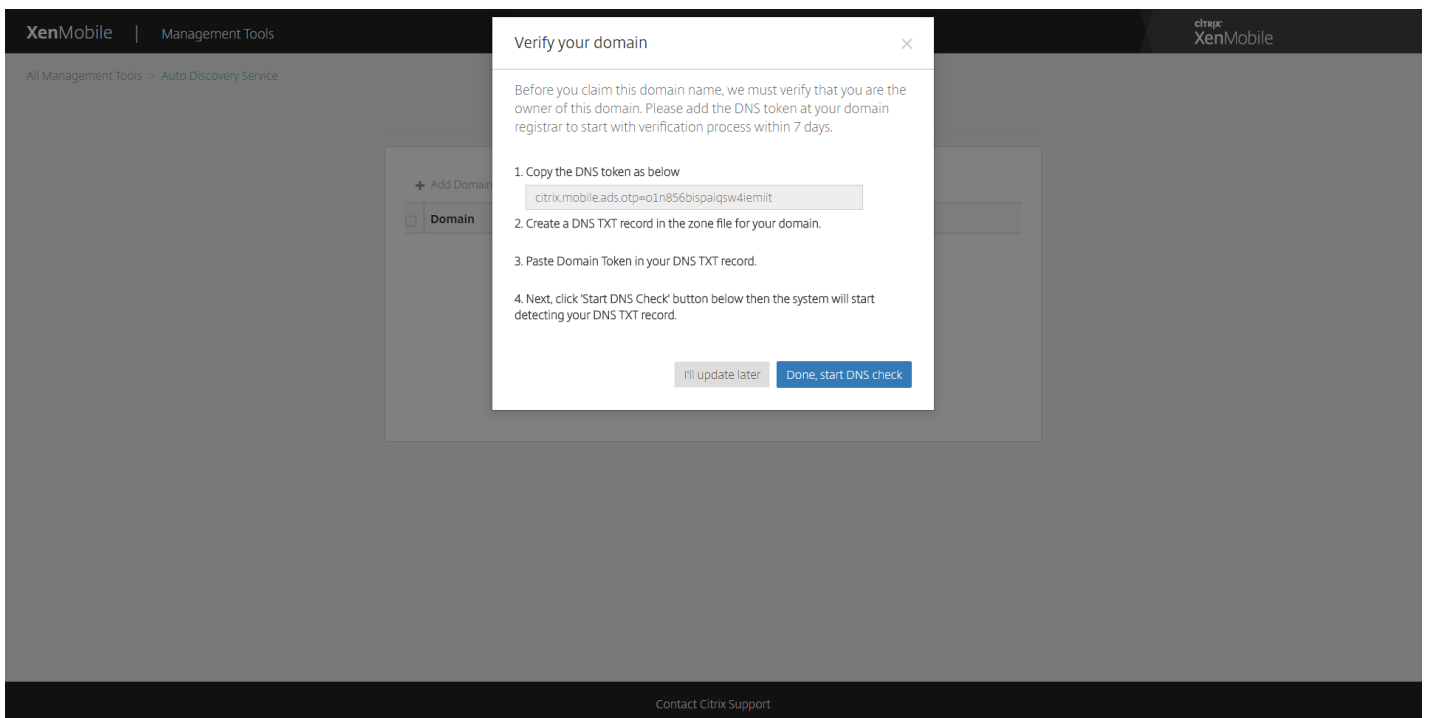
DNS TXTレコードを作成するには、上の手順2で追加したドメインのドメインホスティングプロバイダーポータルにログインする必要があります。ドメインホスティングポータルでは、ドメインネームサーバーレコードを編集したり、カスタムのTXTレコードを追加したりできます。サンプルドメインdomain.comのホスティングポータルでのDNS TXTエントリの追加の例。

c. DNS TXTレコードにドメイントークンを貼り付け、ドメインネームサーバーレコードを保存します。

d. XenMobileツールポータルに戻って [Done] をクリックし、DNSチェックを開始します。

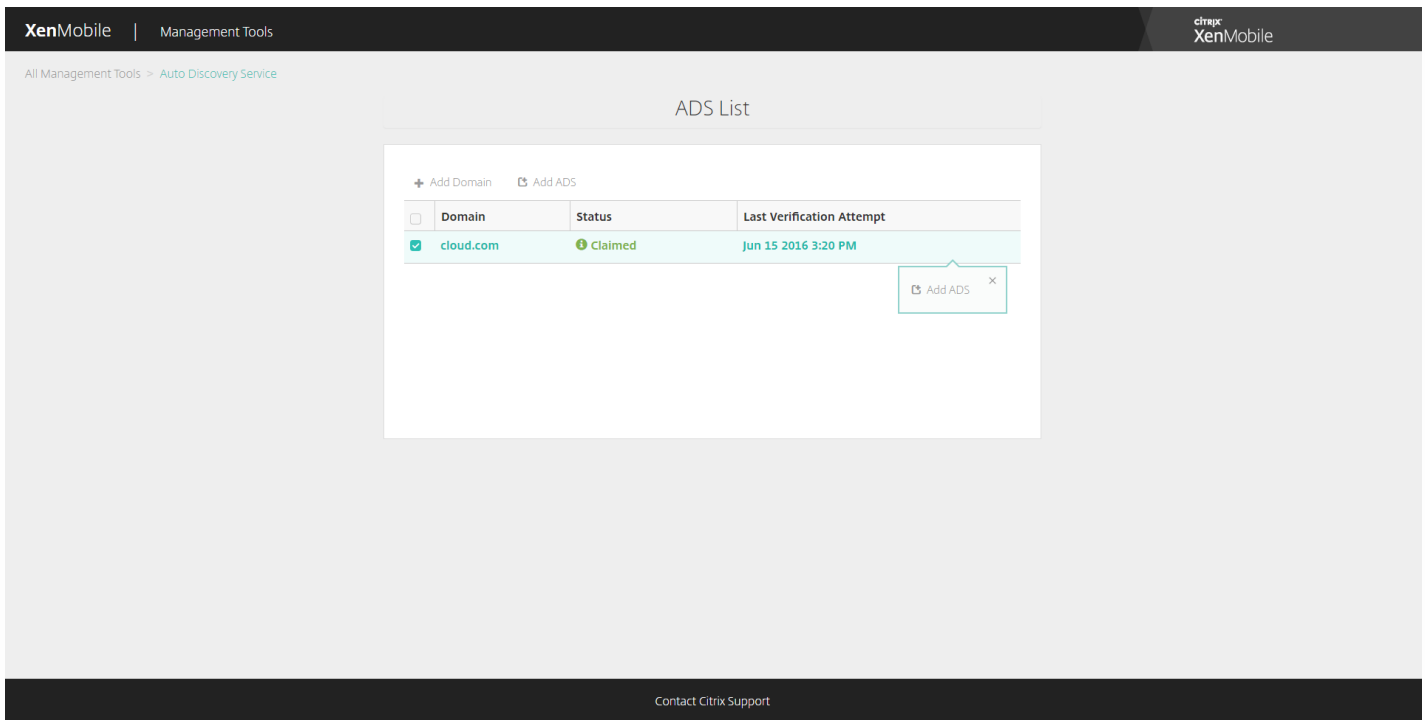
作成したDNS TXTレコードが検出されます。または、 [I'll update later] をクリックして、レコードを保存することもできます。 [Waiting] レコードを選択して [DNS Check] をクリックするまで、DNSチェックは開始されません。

このチェックにかかる時間は最短で約1時間ですが、応答が返されるまでに最大2日かかることがあります。さらに、ステータスの変更を確認するには、ポータルを閉じてから再びアクセスする必要がある場合もあります。

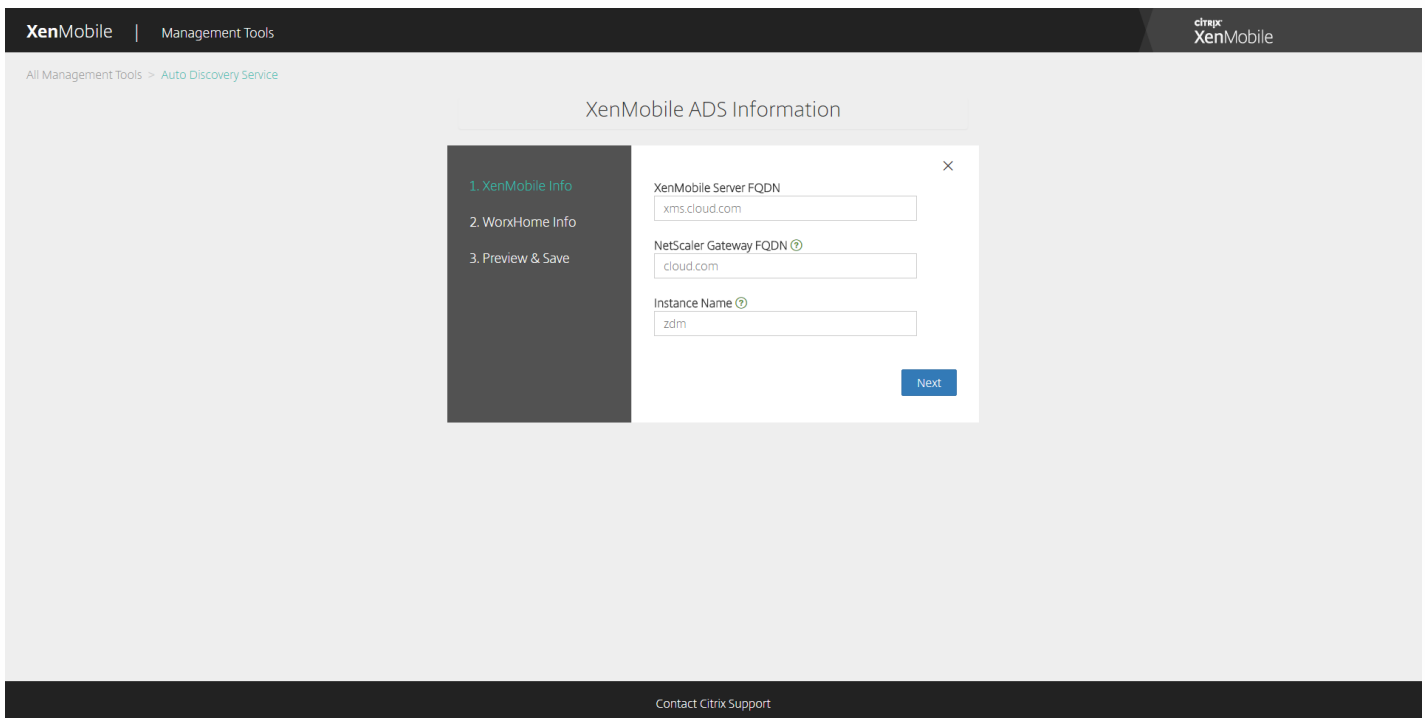


4. ドメインを指定すると、AutoDiscoveryサービス情報を入力できるようになります。自動検出をリクエストするドメインレコードを右クリックしてから、 [Add ADS] をクリックします。

ドメインにすでにAutoDiscoveryレコードがある場合、Citrixテクニカルサポートに事例を記録して、必要に応じて詳細を変更します。



5. XenMobileサーバーの完全修飾ドメイン名、NetScaler Gatewayの完全修飾ドメイン名、およびインスタンス名を入力して、[Next] をクリックします。不明な場合、デフォルトインスタンスの「zdm」を追加します。



上のスクリーンショットのWorx Homeは、現在ではSecure Hubと呼ばれている点に注意してください。

6. Secure Hubに次の情報を入力して、[Next] をクリックします。

a. User ID Type : ユーザーが電子メールアドレスまたはUPNでサインオンするIDのタイプを選択します。

UPNは、ユーザーのUPN（ユーザープリンシパル名）がメールアドレスと同じである場合に使用されます。どちらの方法も、サーバーアドレスを検出するために入力したドメインを使用します。メールアドレスの場合、ユーザーはユーザー名とパスワードを入力するよう求められます。UPNの場合はパスワードを入力するよう求められます。

b. HTTPS Port : HTTPSでSecure Hubサーバーにアクセスするときに使用するポートを入力します。通常、これはポート443です。

c. iOS Enrollment Port : iOS登録時にSecure Hubへのアクセスに使用するポートを入力します。通常、これはポート8443です。

d. Required Trusted CA for XenMobile : XenMobileへのアクセスで信頼された機関からの証明書が必要かどうかを指定します。このオプションは、[OFF] または [ON] にできます。現時点では、この機能のために証明書をアップロードすることはできません。この機能を使用する場合は、Citrixサポートに電話して自動検出のセットアップを依頼する必要があります。証明書ピン留めについて詳しくは、XenMobileアプリのドキュメントの、「[Secure Hub](#)」にある証明書ピン留めについてのセクションを参照してください。証明書ピン留めが機能するために必要なポートについては、「[XenMobile Port Requirements for ADS Connectivity](#)」のサポート記事を参照してください。

XenMobile | Management Tools

All Management Tools > Auto Discovery Service

WorxHome ADS Information

1. XenMobile Info  
2. WorxHome Info  
3. Preview & Save

User ID Type  
E-mail address

HTTPS Port  
443

iOS Enrollment Port  
8443

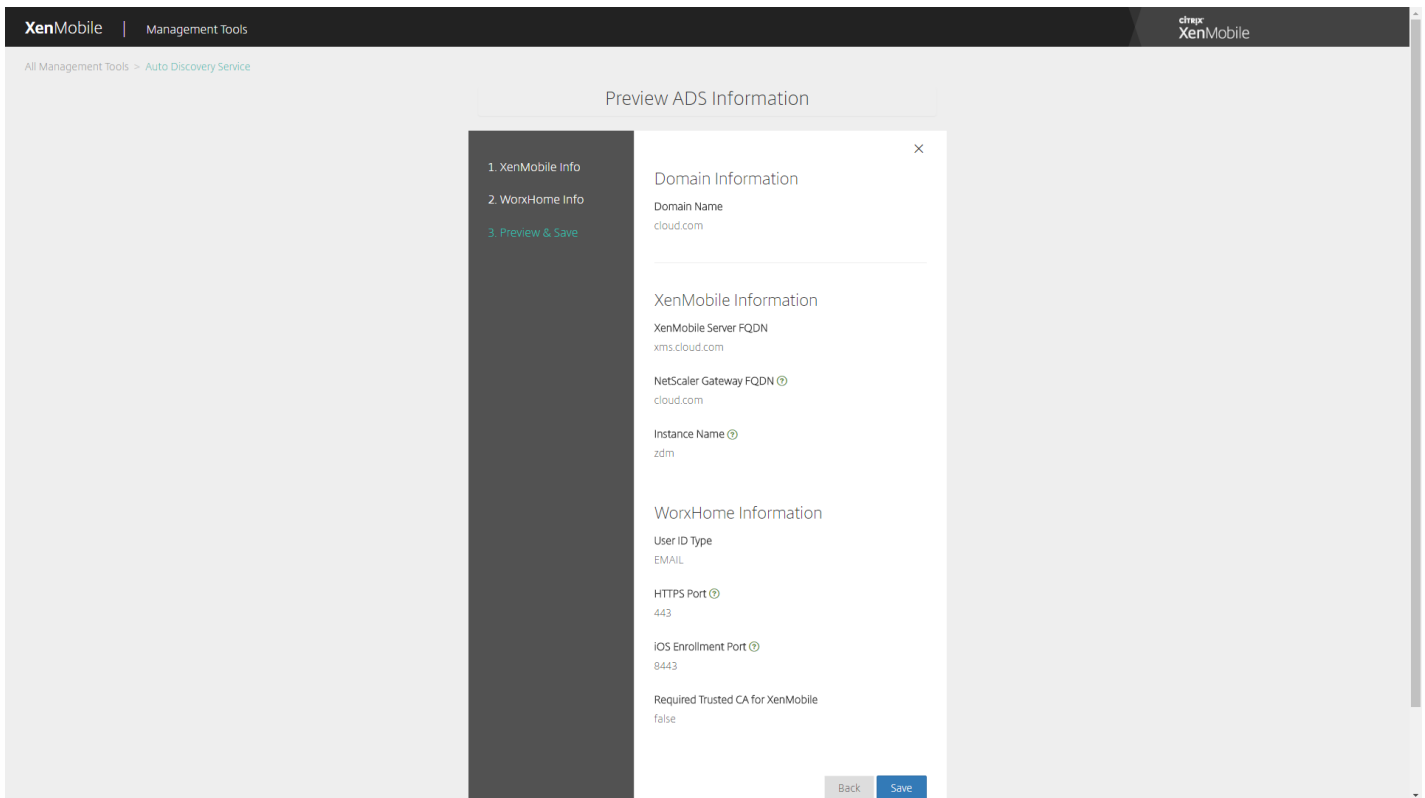
Required Trusted CA for XenMobile  
OFF

Back Next

Contact Citrix Support

上のスクリーンショットのWorx Homeは、現在ではSecure Hubと呼ばれている点に注意してください。

7. 概要ページに、これまでの手順で入力したすべての情報が表示されます。データが正しいことを確認し、[Save] をクリックします。



上のスクリーンショットのWorx Homeは、現在ではSecure Hubと呼ばれている点に注意してください。

## 自己検出の有効化

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)。

自動検出を有効化するには、AutoDiscoveryサービスポータル (<https://xenmobiletools.citrix.com>) にアクセスします。

一部の限られた事例では、自動検出を有効化する場合にCitrixサポートへの連絡が必要な場合があります。そうするために、以下の手順に従って展開の情報をCitrixテクニカルサポートチームに通知できます。また、Windowsデバイスの場合はSSL証明書も送信する必要があります。Citrixでこの情報を受け取った後、ユーザーがデバイスを登録するときに、ドメイン情報が抽出されてサーバーアドレスにマップされます。この情報はXenMobileデータベースで管理され、ユーザーが登録するときに常にアクセスして使用できます。

1. Autodiscoveryサービスポータル (<https://xenmobiletools.citrix.com>) 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zdmであり、大文字と小文字が区別されます。
- ユーザーIDのタイプ。UPNまたはメールのいずれかにできます。デフォルトでは、タイプはUPNです。
- デフォルトポート8443からポート番号を変更した場合は、iOS登録に使用されるポート。
- デフォルトポート443からポート番号を変更した場合は、XenMobileサーバーが接続を受け入れるポート。

- XenMobile管理者のメールアドレス（オプション）。

2. Windowsデバイスを登録する場合は、以下を実行します。

- enterpriseenrollment.mycompany.comの公式に署名された非ワイルドカードSSL証明書を取得します。ここで、mycompany.comはユーザーが登録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。
- 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）。



# デバイスの登録

Apr 27, 2017

ユーザーデバイスをリモートで安全に管理するために、ユーザーデバイスをXenMobileに登録します。XenMobileクライアントソフトウェアがユーザーデバイスにインストールされ、ユーザーのIDが認証されます。次に、XenMobileとユーザーのプロファイルがインストールされます。続いてXenMobileコンソールで、デバイス管理タスクを実行できます。ポリシーの適用、アプリケーションの展開、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、および検索が可能です。

注：iOSデバイスユーザーを登録する前に、APNS証明書を要求する必要があります。詳しくは、[証明書](#)を参照してください。

ユーザーとデバイスの構成オプションを更新するには、[Manage] > [Enrollment] ページを使用します。詳しくは、この記事の「[登録招待状の送信](#)」を参照してください。

## Androidデバイス

1. AndroidデバイスでGoogle Playストアにアクセスして、Citrix Secure Hubアプリをダウンロードしてタップします。
2. インストールを求めるメッセージが表示されたら、[次へ] をクリックし、[インストール] をクリックします。
3. インストールが完了したら、[開く] をタップします。
4. 会社の資格情報（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、Citrix PINの作成を求められる場合があります。Citrix PINは、Secure Hubやその他のほかのXenMobile準拠アプリ（Secure Mail、Secure Web、ShareFileなど）へのサインオンに使用できます。Citrix PINは2回入力する必要があります。[Citrix PINの作成] 画面で、PINを入力します。
8. PINを再入力します。Secure Hubが開きます。その後、XenMobile Storeにアクセスし、Androidデバイスにインストールできるアプリを確認することができます。
9. 登録の後でアプリを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。さらに、XenMobileで構成したポリシーはデバイスに展開されます。[インストール] をタップしてアプリをインストールします。

### Androidデバイスを登録解除および再登録するには

Secure Hub内から登録解除できます。次の手続きを使って登録解除する場合、デバイスはXenMobileコンソールのデバイスインベントリに表示され続けます。ただし、そのデバイス进行操作することはできません。そのデバイスを追跡したり、デバイスのコンプライアンスを監視したりすることはできません。

1. Secure Hubアプリケーションをタップして開きます。
2. スマートフォンかタブレットかに応じて、以下の操作を行います。

スマートフォンの場合：

- a. 画面左側からスワイプして設定ペインを開きます。
- b. [設定]、[アカウント]、[アカウントの削除] の順にタップします。

タブレットの場合：

- a. 右上のメールアドレスの横の矢印をタップします。
- b. [設定]、[アカウント]、[アカウントの削除]の順にタップします。
3. [再登録] をタップします。デバイスの再登録を確認するメッセージが表示されます。
4. [OK] をタップします。

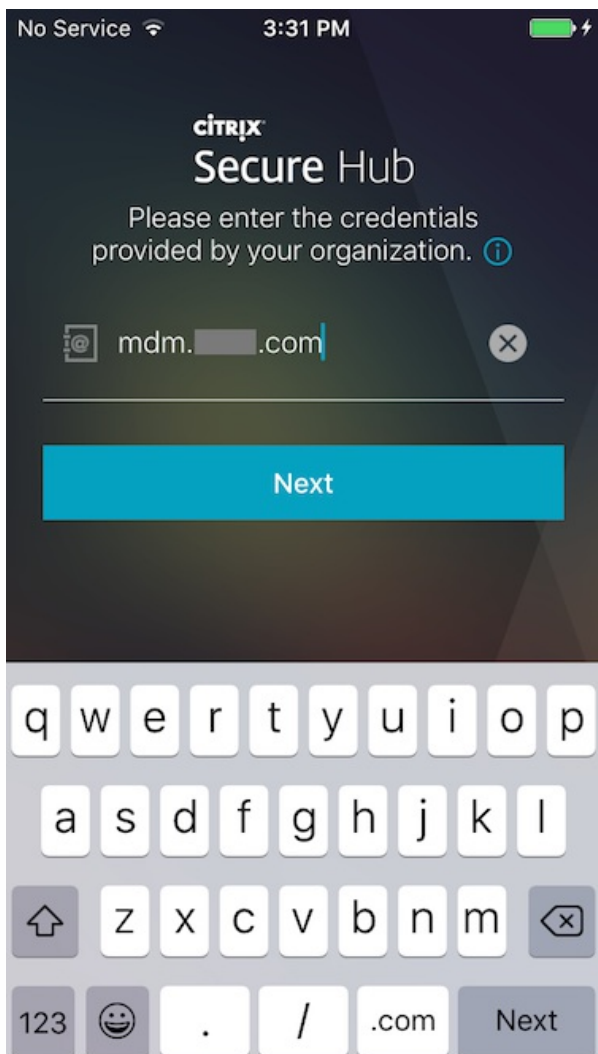
デバイスが登録解除されます。

5. 画面の指示に従って、デバイスを再登録します。

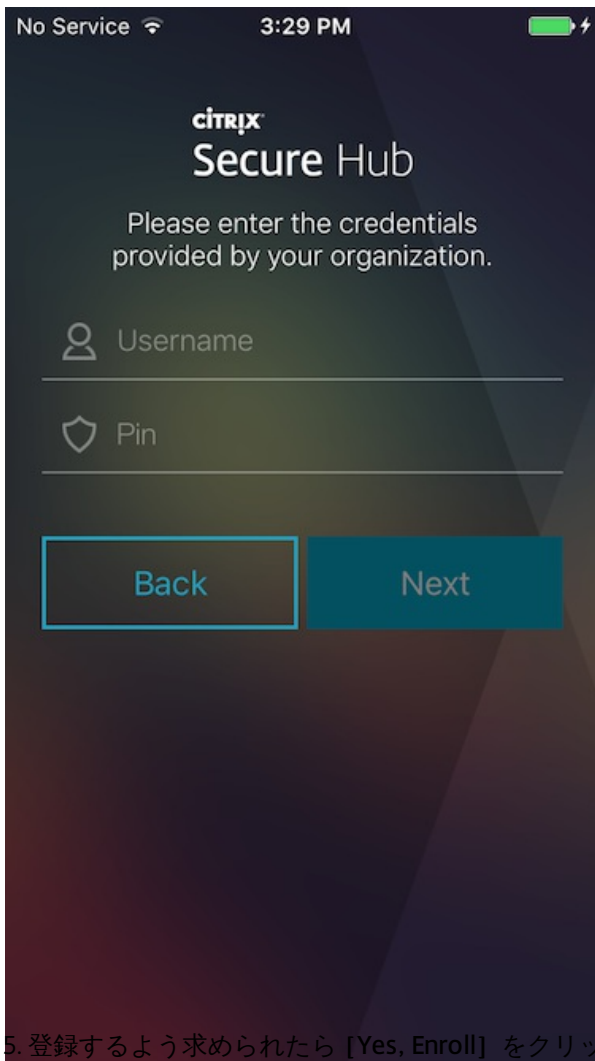
## iOSデバイス

1. Secure HubアプリをデバイスのApple社のiTunes App Storeからダウンロードした後、アプリをデバイスにインストールします。
2. iOSデバイスのホーム画面で、Secure Hubアプリをタップします。
3. Secure Hubの起動後、ヘルプデスクが指定するサーバーアドレスを入力します。

(表示される画面は、XenMobileの構成方法に応じて、次の例と異なる可能性があります。)



4. 画面に指示に従って、ユーザー名とパスワード、またはPINを入力します。[Next] をクリックします。



5. 登録するよう求められたら [Yes, Enroll] をクリックし、続いて画面の指示に従って資格情報を入力します。

**citrix**  
**Secure Hub**

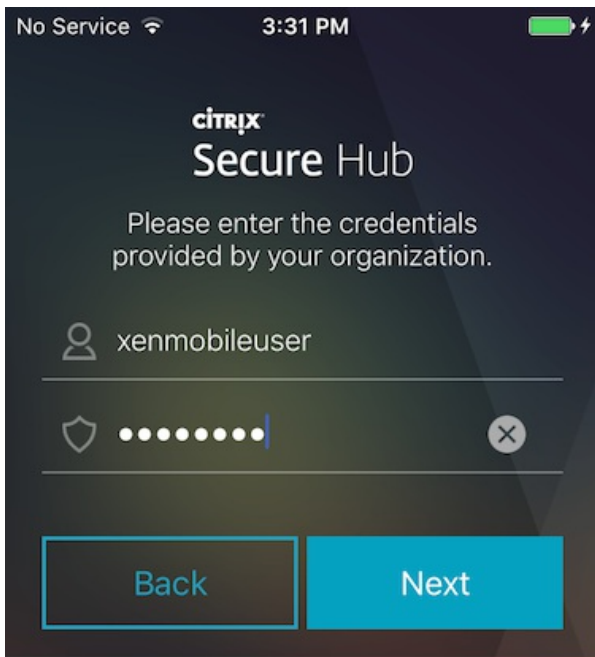
Please enter the credentials provided by your organization. ⓘ

**Enroll Your iPhone**

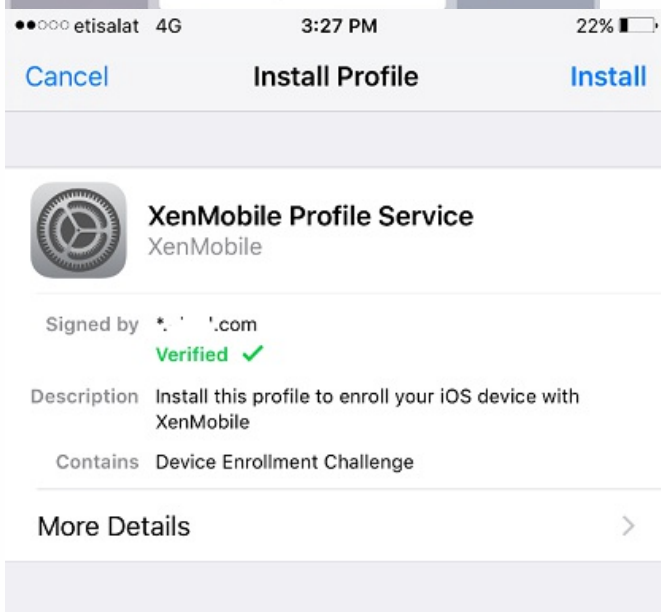
Enrolling secures your iPhone and your work apps. Do you want to enroll your device?

Yes, Enroll

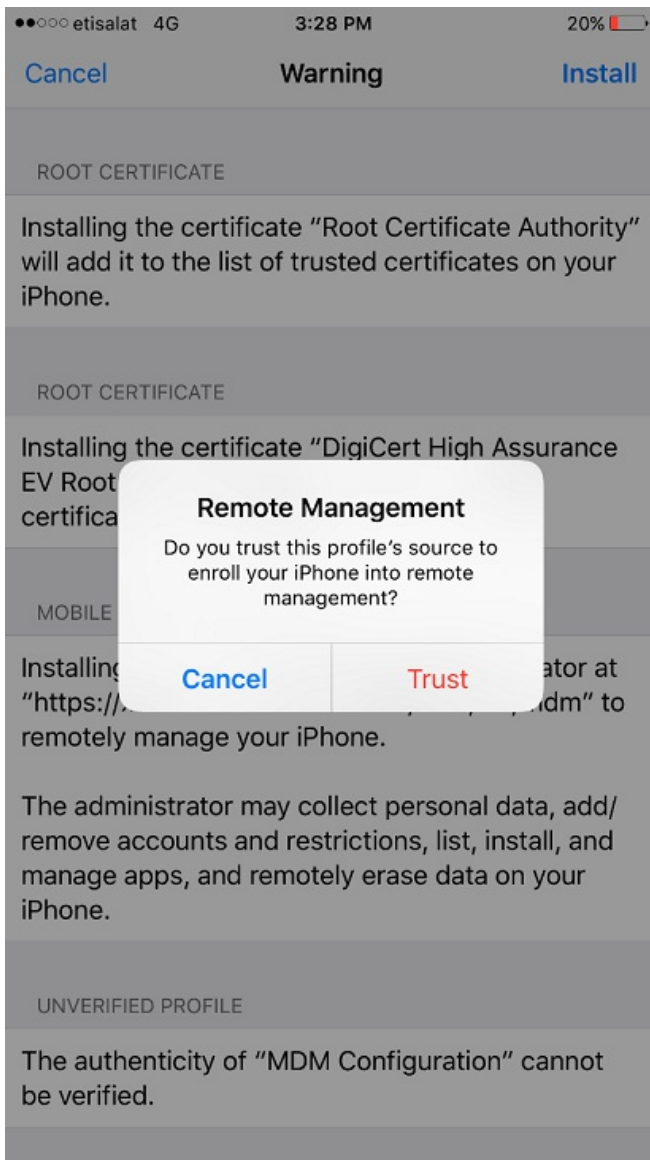
No



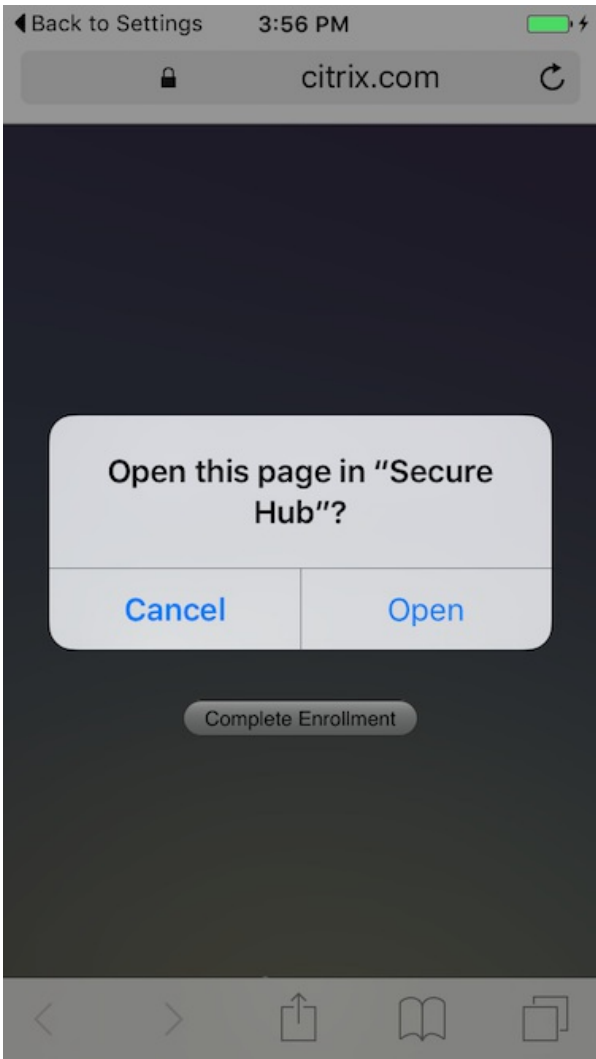
6. [Install] をタップして、Citrix Profileサービスをインストールします。



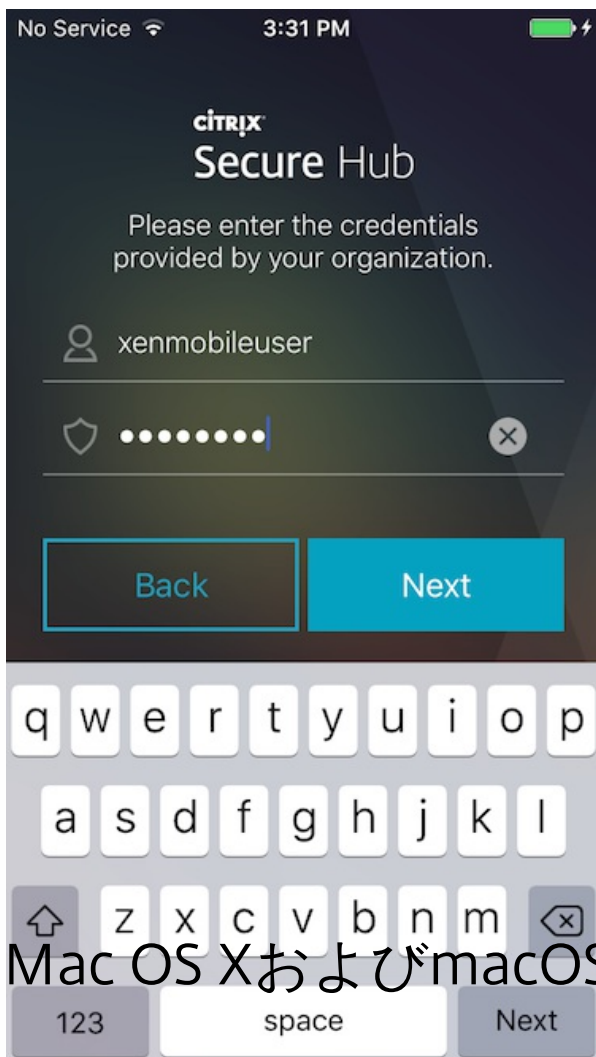
7. [Trust] をタップします。



8. [Open] をタップし、続いて資格情報を入力します。







## Mac OS XおよびmacOSデバイス

MDM-onlyモードのXenMobileで、OS XまたはmacOSが実行されているMacを登録することができます。登録は、Macユーザーが各自のデバイスから無線経由で直接行います。

XenMobile管理者は次の手順に従って、Macデバイスを登録できます。

1. 任意で、XenMobileコンソールでMacのデバイスポリシーを設定します。デバイスポリシーについては、[デバイスポリシー](#)を参照してください。Mac用に構成できるデバイスポリシーを確認するには、[プラットフォーム別のXenMobileデバイスポリシー](#)を参照してください。

2. 登録リンク (<https://:8443/zdm/macOS/otae>) を送信します。

- serverFQDNは、XenMobileが動作するサーバーの完全修飾ドメイン名 (FQDN) です。
- ポート8443は、デフォルトのセキュアポートです。別のポートを構成している場合は、8443ではなく、構成済みのポートを使用します。
- zdmは、サーバーのインストール時に使用されるインスタンス名です。別のインスタンス名を構成している場合は、そのインスタンス名を使用します。

メール招待状でリンクを送信することもできます。詳しくは、[登録招待状の送信](#)を参照してください。

3. 必要に応じて、ユーザーが証明書をインストールします。管理者がiOSおよびMac OS用の公式に信頼されるSSL証明書および公式に信頼されるデジタル署名証明書を構成すると、ユーザーに証明書のインストールを求めるメッセージが表示されます。証明書については、「[証明書](#)」を参照してください。

4. Macデバイスを登録するには、Safariで登録リンクにアクセスします。

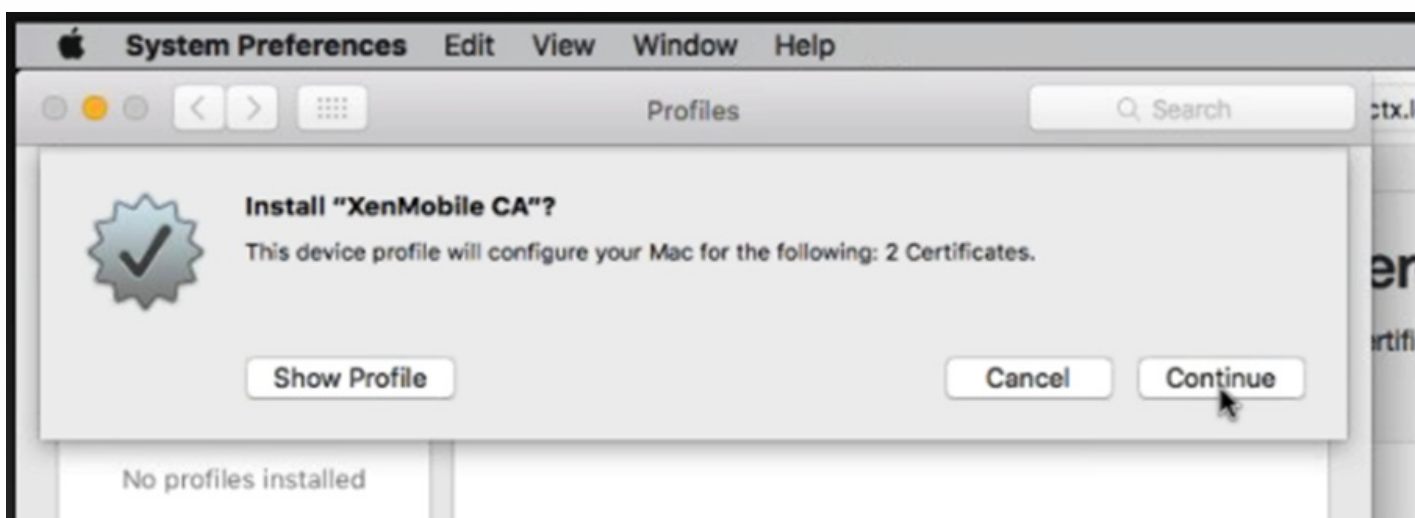
注：このリンクにアクセスできない場合は、ブラウザの履歴とキャッシュを削除するか、別のブラウザを使用します。

5. デフォルトでは、証明書のインストールを求めるメッセージが表示されます。

a. [XenMobile root certificate] をクリックします。

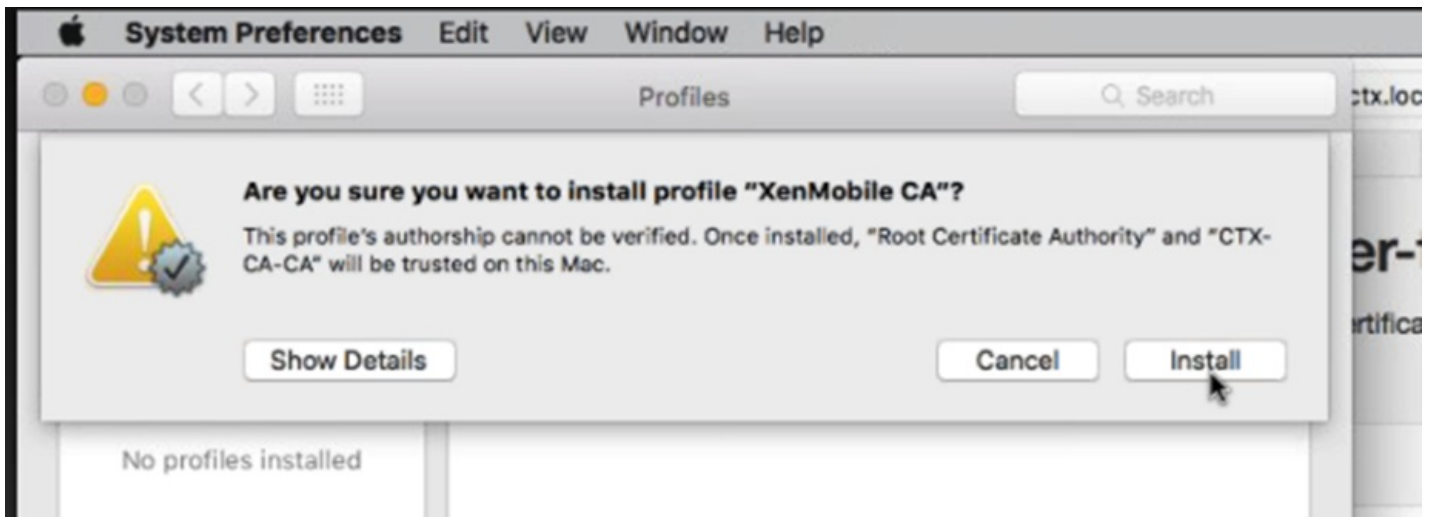


b. [Continue] をクリックして、証明書をインストールします。

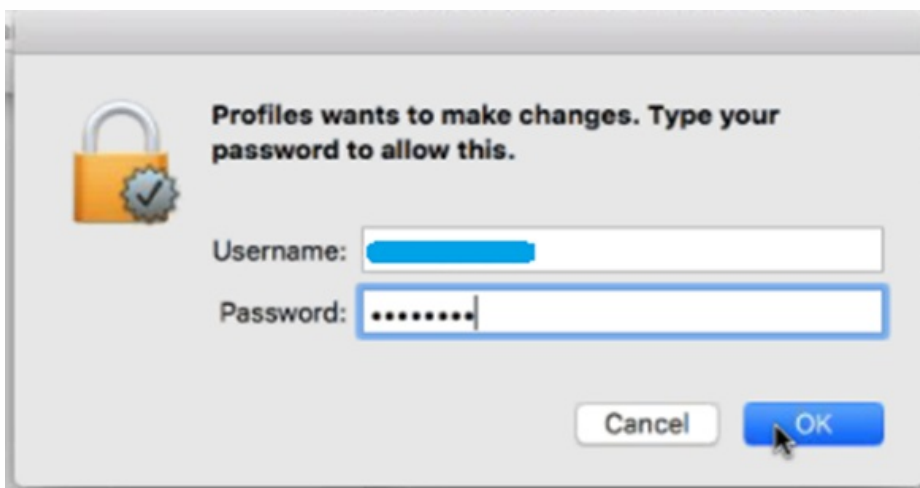


注：XenMobileサーバーのルートCA証明書をインストールすると、デバイスとXenMobileの信頼済みの通信チャネルが有効になります。

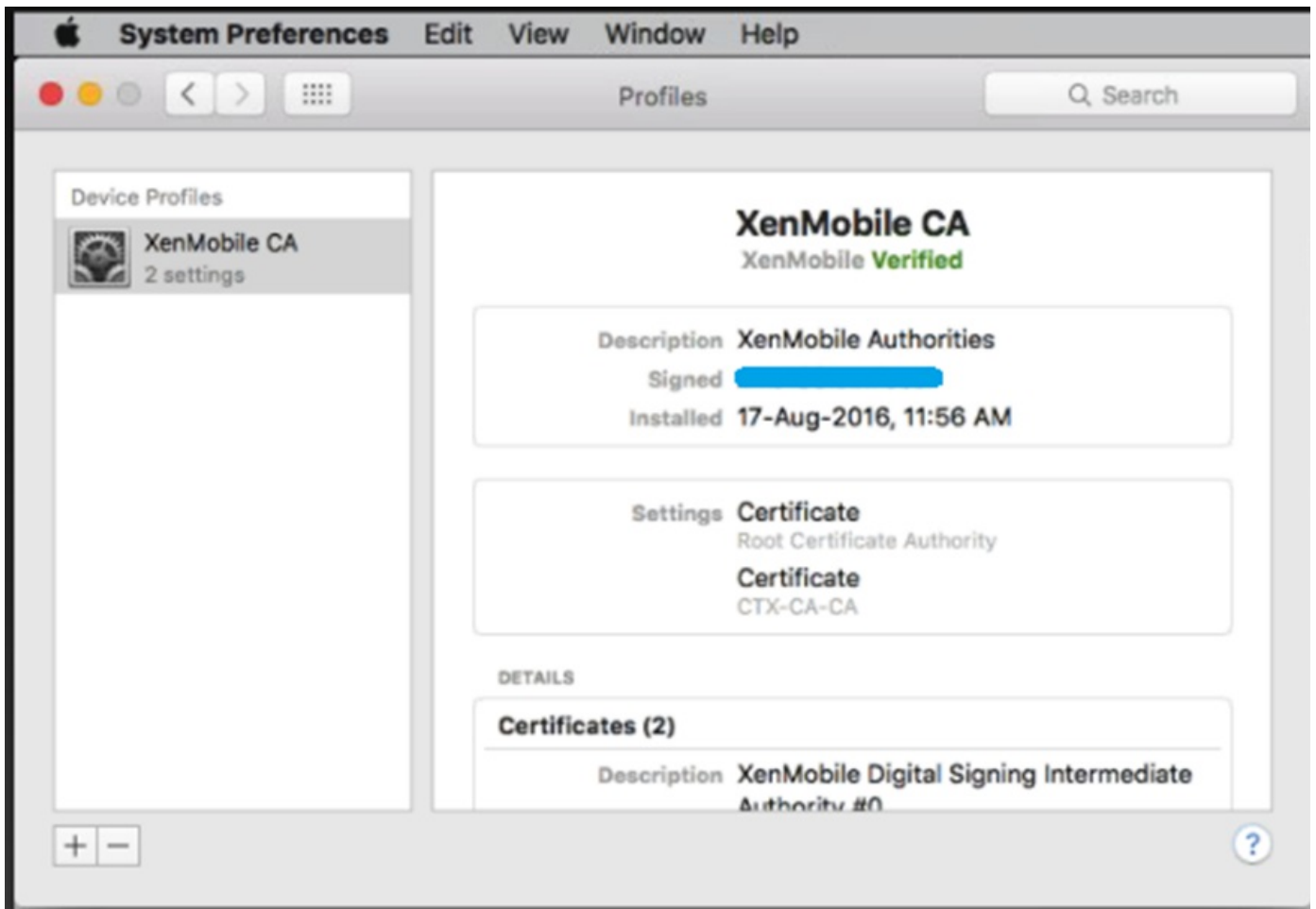
c. [Install] をクリックして、XenMobile Profileをインストールします。



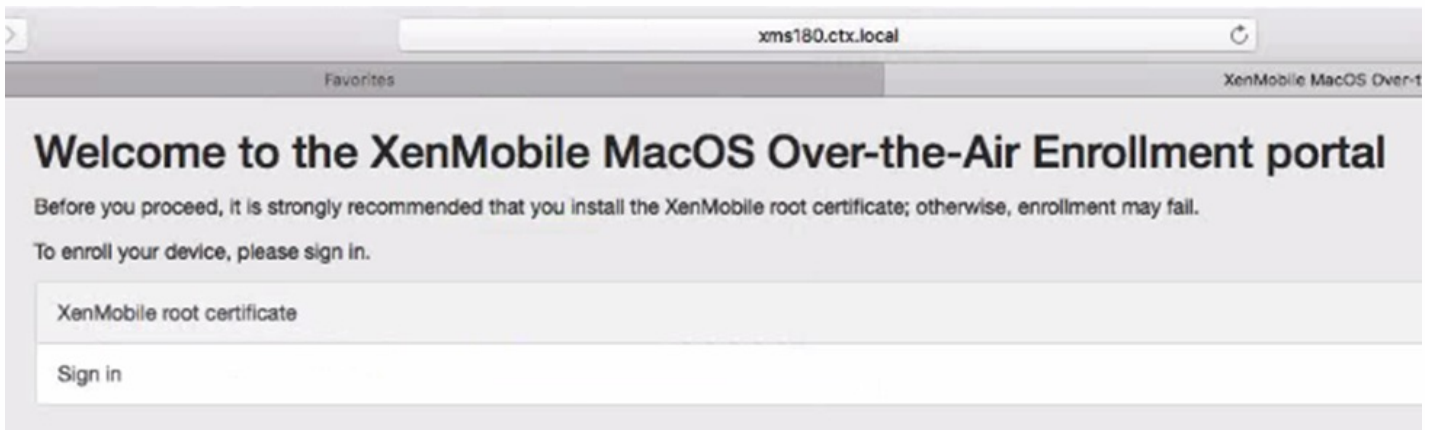
d. 入力画面が表示されたら、デバイスのログオン資格情報を入力します。



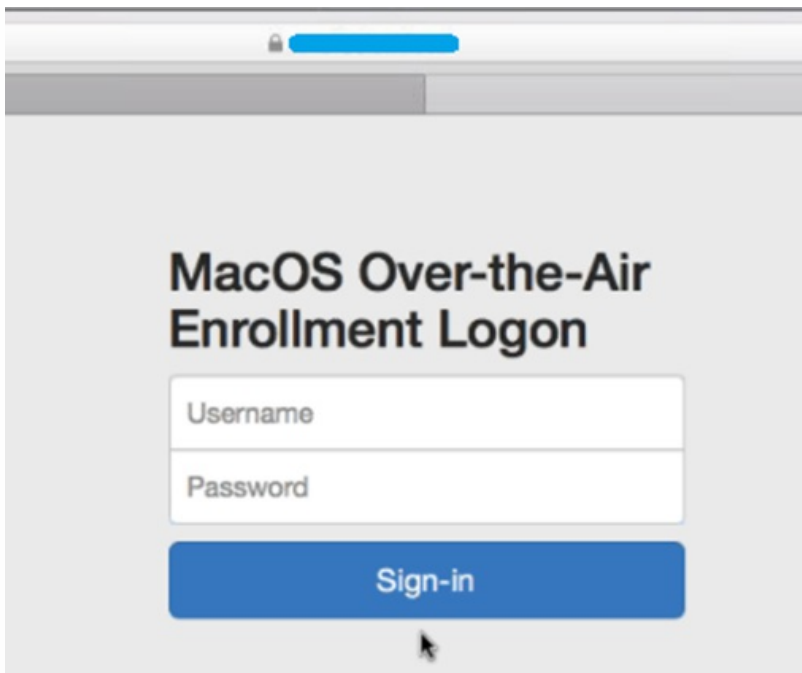
e. この画面は、XenMobile証明書のインストールが成功した場合に [Profiles] の下に表示されます。この画面を閉じて、デバイスの登録に進みます。



6. macOS Over-the-Air Enrollmentポータルで、 [Sign in] をクリックします。

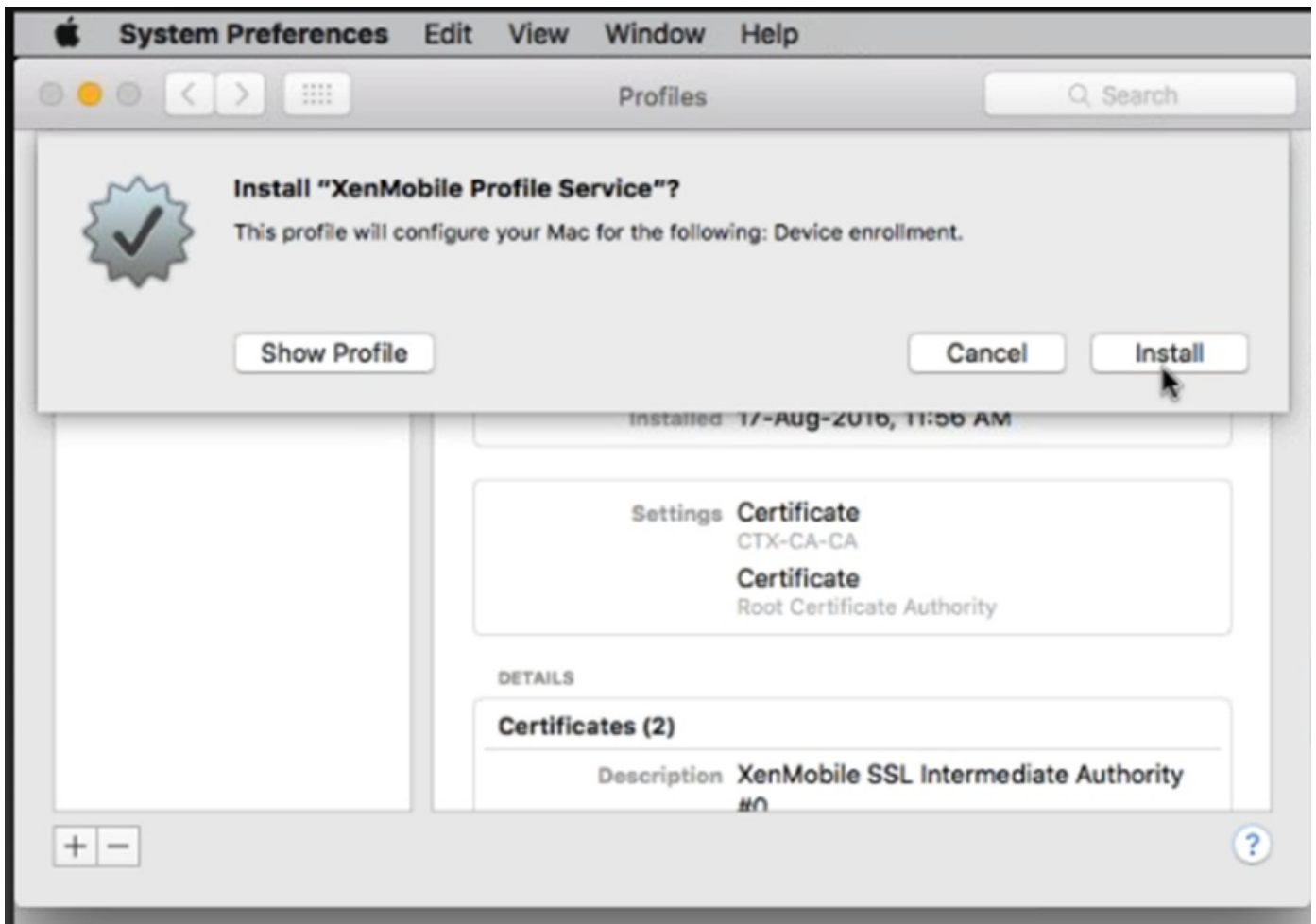


7. XenMobile管理者が構成したユーザーの資格情報をUPNまたはsAMAccountName形式で入力し、 [Sign-in] をクリックします。



注：XenMobileはユーザー要求を検証し、Active Directoryを使用して資格情報を確認します。資格情報は、Active Directoryに対して検証されます。

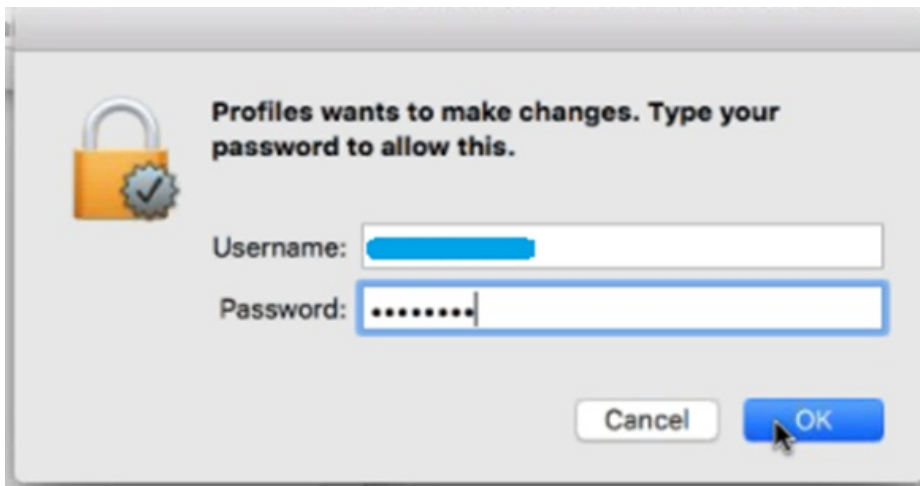
8. ログオンに成功した場合は、XenMobile Profile Service画面が表示されます。[Install] をクリックして、XenMobile Profileをインストールします。XenMobile Profile Serviceをインストールすることによって、XenMobile管理者はリモートでMacデバイスを管理できます。



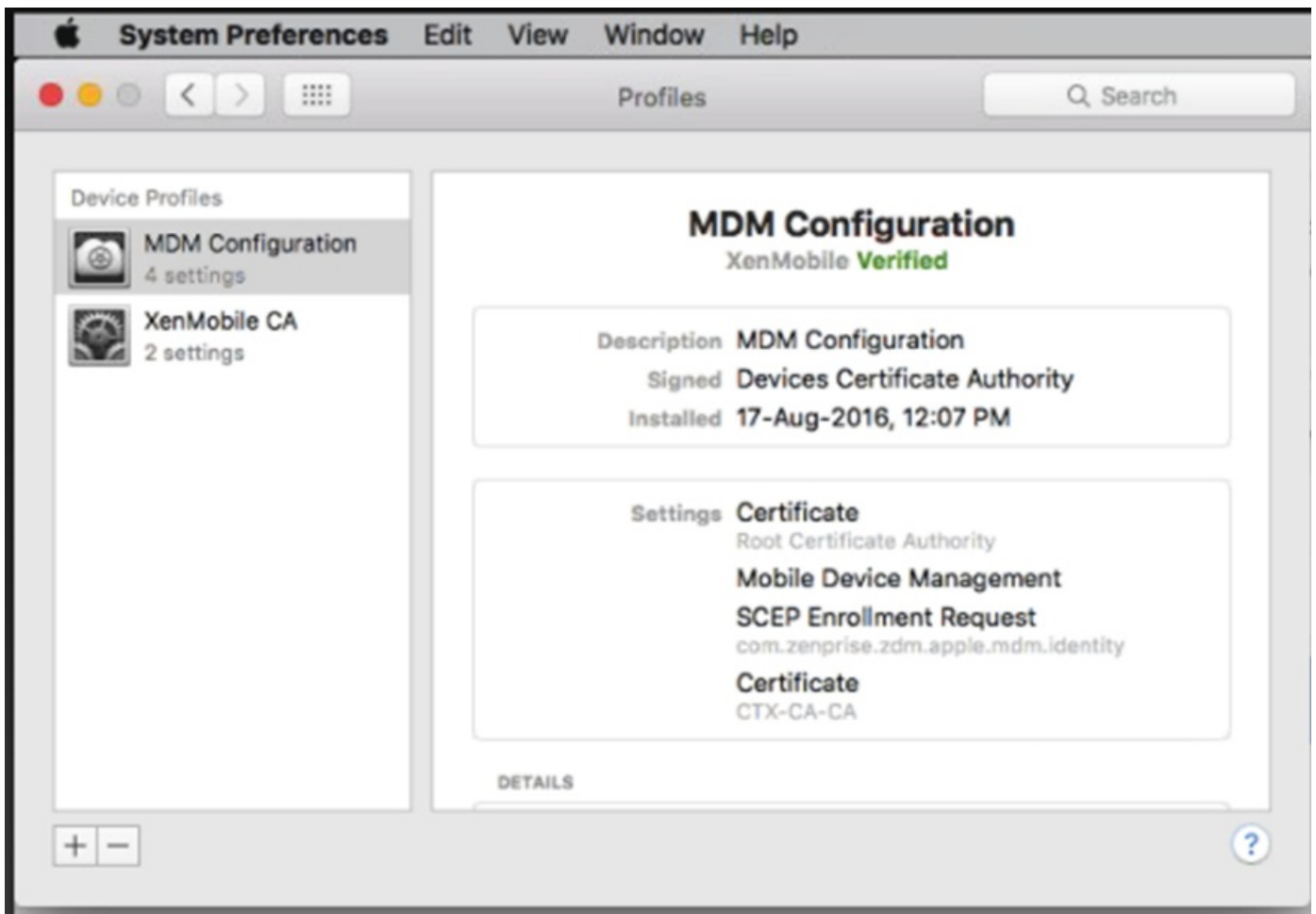
9. MDMプロファイルをインストールするには、[Continue] をクリックしてから、[Install] をクリックします。



10. 入力画面が表示されたら、デバイスのログオン資格情報を入力します。



11. MDM構成プロファイルがインストールされると、MDM構成画面が表示されます。



12. XenMobileコンソールの [Device] タブにMacデバイスが表示されます。これで、モバイルデバイスを管理するのと同じように、XenMobileでMacを管理できるようになります。

<input type="checkbox"/>	Status	Mode	User name	Device platform	Operating system version	Device model
<input type="checkbox"/>		MDM	[REDACTED]	Android	6.0.1	Nexus 6P
<input type="checkbox"/>		MDM MAM	ak@citrix.com	iOS	9.3.2	iPad
<input type="checkbox"/>		MDM MAM	[REDACTED]	Android	6.0.1	SM-G900H
<input type="checkbox"/>		MDM	ak@ctx.local	OS X	10.11.6	MacBook Air

## Windowsデバイス

XenMobileには、以下のWindowsオペレーティングシステムが動作するデバイスを登録できます。

- Windows 8.1およびWindows 10
- Windows Phone 8.1および10

WindowsおよびWindows Phoneのユーザーはデバイスから直接登録します。

ユーザー登録のため自動検出およびWindows検出サービスを構成して、WindowsおよびWindows Phoneデバイスの管理を有効にする必要があります。

### 注意

Windowsデバイスの登録には、SSLリスナー証明書が公開証明書である必要があります。自己署名SSL証明書をアップロード済みの場合、登録は失敗します。

### 自己検出を使用してWindowsデバイスを登録するには

ユーザーは、Windows RT 8.1、Windows 8.1 ProとWindows 8.1 Enterprise（32ビットと64ビット）の両方、およびWindows 10を実行しているデバイスを登録できます。Windowsデバイスの管理を有効にするには、自動検出およびWindows検出サービスを構成することをお勧めします。詳しくは、「[ユーザー登録のためにXenMobileで自動検出を有効にするには](#)」を参照してください。

1. デバイスで使用可能なWindows Updateをすべて確認し、インストールします。この手順は、Windows 8からWindows 8.1にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。
2. チャームメニューで「設定」をタップします。
  - Windows 8.1の場合、[PC設定] > [ネットワーク] > [社内] の順にタップします。
  - Windows 10の場合は、[アカウント] > [職場または学校へのアクセス] > [職場または学校への接続] の順にタップします。
3. コーポレートメールアドレスを入力してから、[デバイス管理を有効にする]（Windows 8.1）または[続行]（Windows



- 10) をタップします。ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します (例: foo@mydomain.com)。これによって、Windowsの埋め込みデバイス管理によって登録が実行される、既知のMicrosoftの制限を回避できます。【サービスに接続しています】ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。デバイスがXenMobileサーバーを自動的に検出し、登録処理が開始されます。
4. パスワードを入力します。XenMobileのユーザーグループのメンバーであるアカウントに関連付けられたパスワードを使用します。
5. Windows 8.1の場合、【IT管理者によるアプリやサービスの管理を許可する】ダイアログボックスで、デバイスの管理に同意して、【オンにする】をタップします。Windows 10の場合：【使用条件】ダイアログボックスで、デバイスの管理に同意して、【同意する】をタップします。

#### 自己検出なしでWindowsデバイスを登録するには

自動検出なしでWindowsデバイスを登録することができます。しかし、自動検出を構成するようお勧めします。自動検出なしで登録すると、希望するURLに接続する前にポート80を呼び出すことになるため、実稼働環境でのベストプラクティスとみなせません。このような処理は、テスト環境や概念実証展開でのみ使用するようにしてください。

1. デバイスで使用可能なWindows Updateをすべて確認し、インストールします。この手順は、Windows 8からWindows 8.1にアップグレードする場合に特に重要です。適用できるすべての更新について自動通知されるとは限らないからです。
2. チャームメニューで【設定】をタップします。
  - Windows 8.1の場合、【PC設定】>【ネットワーク】>【社内】の順にタップします。
  - Windows 10の場合は、【アカウント】>【職場または学校へのアクセス】>【職場または学校への接続】の順にタップします。
3. 会社のメールアドレスを入力します。
4. Windows 10では、自動検出が構成されていない場合、手順5で説明されているようにサーバーの詳細を入力できるオプションが表示されます。Windows 8.1では、【サーバーアドレスを自動検出する】がオンに設定されている場合、タップしてこのオプションをオフにします。
5. 【サーバーアドレスを入力してください】フィールドに以下のアドレスを入力します。
  - Windows 8.1の場合、「https://serverfqdn:8443/serverInstance/Discovery.svc」という形式でサーバーアドレスを入力します。未認証のSSL接続に8443以外のポートが使用される場合、このアドレスの8443の箇所はそのポート番号を指定します。
  - Windows 10の場合、「https://beta.managedm.com:8443/zdm/wpe」というアドレスを入力します。未認証のSSL接続に8443以外のポートが使用される場合、このアドレスの8443の箇所はそのポート番号を指定します。
6. パスワードを入力します。
7. Windows 8.1の場合、【IT管理者によるアプリやサービスの管理を許可する】ダイアログボックスで、デバイスの管理に同意して、【オンにする】をタップします。Windows 10の場合、【使用条件】ダイアログボックスで、デバイスの管理に同意して、【同意する】をタップします。

#### Windows Phoneデバイスを登録するには

XenMobileでWindows Phoneデバイスを登録するには、ユーザーはActive Directoryまたは内部ネットワークのメールアドレスおよびパスワードを入力する必要があります。自動検出がセットアップされていない場合、ユーザーはXenMobile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Secure Hub、サポートする各プラットフォーム向けWindows Phoneアプリを使って）Enterprise Hubポリシーを構成します。

1. Windows Phoneのメイン画面で [設定] アイコンをタップします。

- Windows 10 Phoneの場合は、バージョンに応じて [Accounts] > [Access work or school] > [Connect to work or school] の順にタップするか、 [Accounts] > [Work access] > [Enroll in to device management] の順にタップします。
- Windows Phone 8.1の場合は、 [PC設定] > [ネットワーク] > [社内] の順にタップし、次に [アカウントの追加] をタップします。

2. 次の画面でメールアドレスとパスワードを入力し、 [サインイン] をタップします。

ドメインに自動検出が構成されている場合、以降のいくつかの手順で求められる情報は自動的に抽出されます。手順8に進みます。

ドメインに自動検出が構成されていない場合、次の手順に進みます。ローカルユーザーとして登録するには、ドメイン名は正しいものの、存在しないメールアドレスを入力します (例: foo@mydomain.com) 。これによって既知のMicrosoftの制限を回避できます。 [サービスに接続しています] ダイアログボックスで、ローカルユーザーに関連付けられたユーザー名とパスワードを入力します。

3. 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。

4. ユーザー名とドメインを介して認証が検証される場合、ユーザー名とドメインを入力し、次に [サインイン] をタップします。

5. 証明書に関する問題を通知する画面が表示された場合、そのエラーの原因は自己署名入り証明書の使用です。サーバーが信頼できる場合、 [続行] をタップします。信頼できない場合は、 [キャンセル] をタップします。

6. Windows Phone 8.1で、アカウントを追加すると [業務用アプリをインストール] というオプションが表示されます。管理者が業務用アプリストアを構成済みの場合、このオプションをオンにして、 [完了] をタップします。このオプションをオフにした場合、業務用アプリストアを受信するには再登録が必要になります。

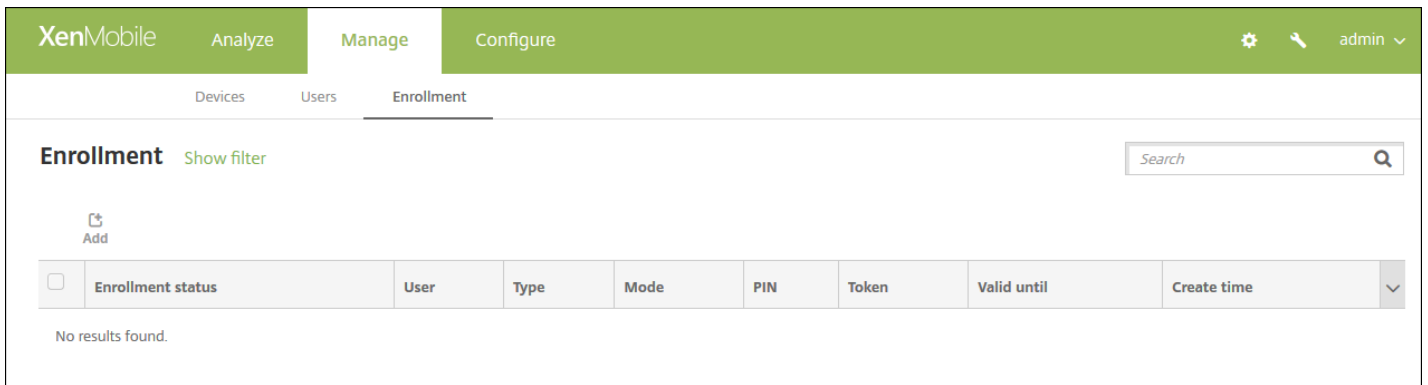
7. Windows Phone 8.1で、 [アカウントが追加されました] 画面で [完了] をタップします。

8. サーバーへの接続を強制的に実行するには、 [最新の情報に更新] アイコンをタップします。デバイスを手動でサーバーに接続できない場合、XenMobileは再接続を試行します。XenMobileは3分ごとに5回連続でデバイスに接続し、その後は2時間ごとに接続します。この接続頻度は、 [サーバーのプロパティ] にある [Windows WNSハートビートの間隔] で変更できます。登録の完了後、Secure Hubがバックグラウンドで登録を実行します。インストールが完了してもそれについては何も通知されません。 [すべてのアプリ] 画面からSecure Hubをタップします。

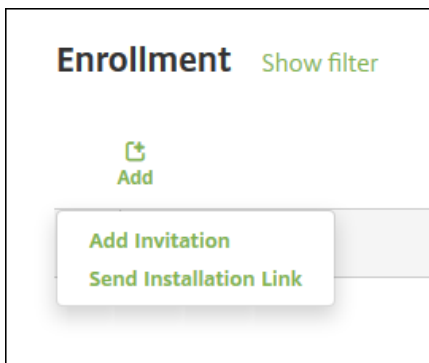
## 登録招待状の送信

XenMobileコンソールで、iOSデバイスまたはAndroidデバイスを使用しているユーザーに登録招待状を送信できます。iOS、Android、Windowsデバイスを使用しているユーザーにインストールリンクを送信することもできます。

1. XenMobileコンソールで、 [Manage] > [Enrollment] の順にクリックします。 [Enrollment] ページが開きます。



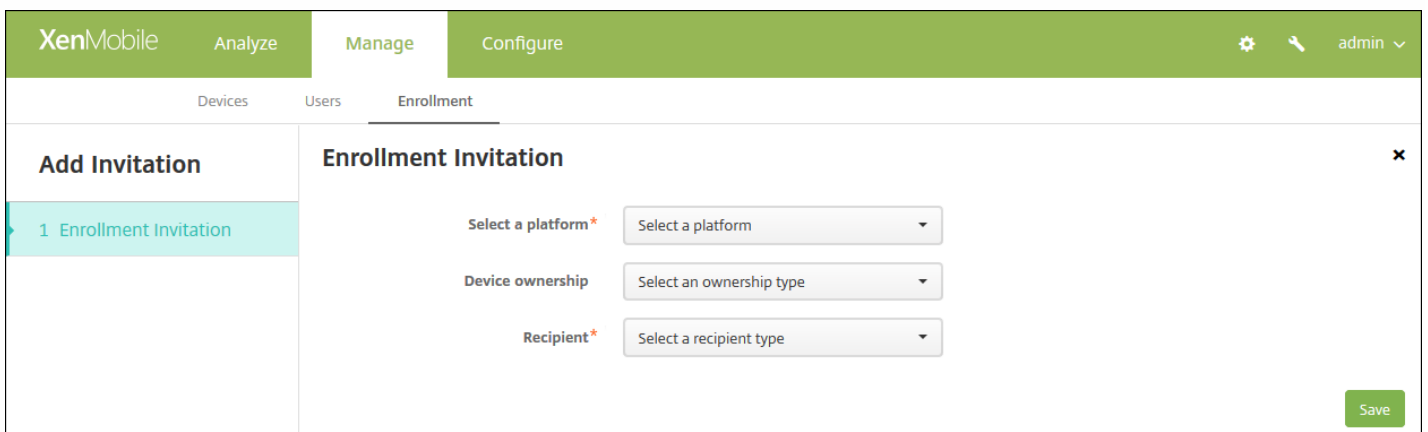
2. [Add] をクリックします。登録オプションが示されたメニューが表示されます。



- 登録招待状をユーザーまたはグループに送信するには、[Add Invitation] を選択します。この設定の構成手順については、「招待状を送信するには」を参照してください。
- SMTPまたはSMS経由で登録インストールリンクを受信者の一覧に送信するには、[Send Installation Link] を選択します。この設定の構成手順については、「インストールリンクを送信するには」を参照してください。

#### 招待状を送信するには

1. [Add Invitation] をクリックします。[Enrollment Invitation] 画面が開きます。



2. 次の設定を構成します。

- Select a platform : 一覧から、[iOS] または [Android] を選択します。

- **Device ownership** : 一覧から、[Corporate] または [Employee] を選択します。
- **Recipient** : 一覧から、[User] または [Group] を選択します。

選択した宛先に応じて、追加の構成設定が表示されます。[User] の設定については「[登録招待状をユーザーに送信するには](#)」を、[Group] の設定については「[登録招待状をグループに送信するには](#)」を参照してください。

### 登録招待状をユーザーに送信するには

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Manage' tab is active, and the 'Enrollment' sub-tab is selected. On the left, there is a sidebar with 'Add Invitation' and a list containing '1 Enrollment Invitation'. The main area is titled 'Enrollment Invitation' and contains the following fields:

- Select a platform\***: iOS
- Device ownership**: Corporate
- Recipient\***: User
- User name\***: (empty text input field)
- Device info**: Serial number (with an empty text input field next to it)
- Phone number**: (empty text input field)
- Carrier**: NONE
- Enrollment mode\***: User name + Password
- Template for agent download**: Select a template
- Template for enrollment URL**: Select a template
- Template for enrollment confirmation**: Select a template
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF (toggle switch)

A 'Save' button is located at the bottom right of the form.

#### 1. [User] について、次の設定を構成します。

- **User name** : ユーザー名を入力します。ユーザーは、XenMobileサーバーのローカルユーザー、またはActive Directoryのユーザーとして存在している必要があります。ローカルユーザーの場合、通知を送信できるようにユーザーの電子メールプロパティが設定されていることを確認します。Active Directoryユーザーの場合、LDAPが構成されていることを確認します。
- **Device info** : 一覧で、[Serial number]、[UDID]、または[IMEI] をクリックします。オプションを選択すると、デバイスに応じて値を入力できるフィールドが表示されます。
- **Phone number** : 任意で、ユーザーの電話番号を入力します。
- **Carrier** : 一覧から、ユーザーの電話番号を関連付ける電話会社を選択します。
- **Enrollment mode** : 一覧から、ユーザーに求める登録の方法を選択します。デフォルトは [User name + Password] です。選択できるオプションは以下のとおりです。
  - 高セキュリティ

- 招待 URL
- 招待 URL および PIN
- 招待 URL およびパスワード
- 2 要素
- ユーザー名および PIN

注：:PINを含む登録モードを選択すると、[Template for enrollment PIN] フィールドが表示されます。このフィールドで、[Enrollment PIN] を選択します。

- **Template for agent download**：一覧から、登録招待に使用するテンプレートを選択します。この一覧では、プラットフォームの種類に基づいてオプションが決まります。たとえば、プラットフォームとして [iOS] を選択した場合、オプションとして [iOS Download Link] が表示されます。
- **Template for enrollment URL**：一覧から、[Enrollment Invitation] を選択します。
- **Template for enrollment confirmation**：一覧から、[Enrollment Confirmation] を選択します。
- **Expire after**：このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Maximum Attempts**：このフィールドは登録処理を行う上限回数を指定するものであり、Enrollment Modeを構成するときに設定します。登録モードの構成について詳しくは、「登録モードを構成するには」を参照してください。
- **Send invitation**：招待状をすぐに送信する場合は [ON] を選択し、[Enrollment] ページの表に招待状を追加するだけの場合は [OFF] を選択します。

2. [Send invitation] を有効にした場合は [Save and Send] をクリックし、それ以外の場合は [Save] をクリックします。[Enrollment] ページの表に招待状が追加されます。

登録招待状をグループに送信するには

The screenshot shows the 'Enrollment Invitation' configuration page in the XenMobile console. The page is titled 'Enrollment Invitation' and has a close button (X) in the top right corner. The configuration is as follows:

- Select a platform\***: iOS
- Device ownership**: Corporate
- Recipient\***: Group
- Domain\***: Select a domain
- Group\***: Select a group
- Enrollment mode\***: User name + Password
- Template for agent download**: Select a template
- Template for enrollment URL**: Select a template
- Template for enrollment confirmation**: Select a template
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF

A 'Save' button is located at the bottom right of the configuration panel.

1. 次の設定を構成します。

- **Domain** : 一覧から、グループを選択するドメインを選択します。
- **Group** : 一覧から、招待状の宛先グループを選択します。
- **Enrollment mode** : 一覧から、グループ内のユーザーに求める登録の方法を選択します。デフォルトは [User name + Password] です。選択できるオプションは以下のとおりです。
  - 高セキュリティ
  - 招待 URL
  - 招待 URL および PIN
  - 招待 URL およびパスワード
  - 2 要素
  - ユーザー名および PIN

注 : PINを含む登録モードを選択すると、 [Template for enrollment PIN] フィールドが表示されます。このフィールドで、 [Enrollment PIN] を選択します。

- **Template for agent download** : 一覧から、登録招待に使用するテンプレートを選択します。この一覧では、プラットフォームの種類に基づいてオプションが決まります。たとえば、プラットフォームとして [iOS] を選択した場合、オプションとして [iOS Download Link] が表示されます。
- **Template for enrollment URL** : 一覧から、 [Enrollment Invitation] を選択します。
- **Template for enrollment confirmation** : 一覧から、 [Enrollment Confirmation] を選択します。
- **Expire after** : このフィールドは登録の期限を示すものであり、登録モードを構成するときに設定します。登録モードの構成について詳しくは、「[登録モードを構成するには](#)」を参照してください。
- **Maximum Attempts** : このフィールドは登録処理を行う上限回数を示すものであり、登録モードを構成するときに設定します。登録モードの構成について詳しくは、「[登録モードを構成するには](#)」を参照してください。
- **Send invitation** : 招待状をすぐに送信する場合は [ON] を選択し、 [Enrollment] ページの表に招待状を追加するだけの場合は [OFF] を選択します。

2. [Send invitation] を有効にした場合は [Save and Send] をクリックし、それ以外の場合は [Save] をクリックします。 [Enrollment] ページの表に招待状が追加されます。

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、[Settings] ページでチャンネル（SMTPまたはSMS）を構成する必要があります。詳しくは、次を参照してください。[通知](#)。

1. 次の設定を構成します。

- **Recipient** : 追加する宛先ごとに、[Add] をクリックして以下の操作を行います。
  - **Email** : 送信先のメールアドレスを入力します。このフィールドは必須です。
  - **Phone number** : 送信先の電話番号を入力します。このフィールドは必須です。
  - **[保存]** をクリックします。

注：既存の送信先を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存の送信先を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

- **Channels** : 登録インストールリンクの送信に使用するチャンネルを選択します。通知はSMTPまたはSMSで送信することが

できます。[Notifications] の [Settings] ページでサーバー設定を構成するまでは、これらのチャネルをアクティブ化できません。詳しくは、次を参照してください。[通知](#)。

- **SMTP** : 次の設定を任意で構成します。これらのフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
  - **Sender** : 任意で送信者を入力します。
  - **Subject** : 任意でメッセージの件名を入力します。たとえば、「Enroll your device」などです。
  - **Message** : 任意で、送信先に送信されるメッセージを入力します。たとえば、「Enroll your device to gain access to organizational apps and email。」などです。
- **SMS** : 以下の設定を構成します。このフィールドに何も入力しない場合は、選択したプラットフォームで構成済みの通知テンプレートに指定されているデフォルト値が使用されます。
  - **Message** : 送信先に送信されるメッセージを入力します。SMSベースの通知の場合、このフィールドは必須です。

注：北米の場合、160文字を超えるSMSメッセージは複数のメッセージとして配信されます。

2. [Send] をクリックします。

## 注意

環境がSAMAccountNameを使用している場合、ユーザーが招待状を受け取ってリンクをクリックした後、認証を完了するには、ユーザー名を編集する必要があります。たとえば、SAMAccountName@domainname.comからドメイン名を削除する必要があります。



# デバイス登録の制限

Apr 27, 2017

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

制限を設定しないと、ユーザーはデバイスをいくつでも登録できます。この機能は、iOSおよびAndroidデバイスでのみサポートされます。

## グローバルデバイス登録制限を構成するには

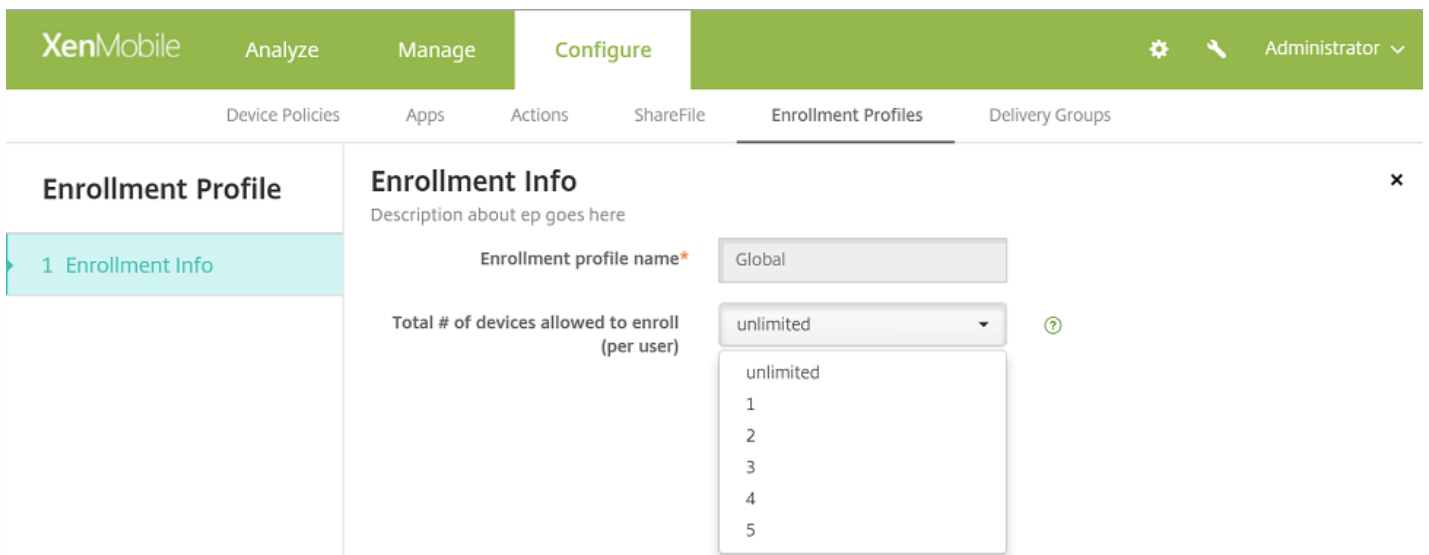
1. [Configure] > [Enrollment Profiles] の順に移動します。
2. [Global] をクリックして、[Edit] を選択します。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Enrollment Profiles' tab is active. A search bar is located in the top right corner. Below the search bar, there is an 'Add' button. The main content area displays a table of enrollment profiles:

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	ep1	2/11/16 1:44 PM	2/11/16 1:44 PM	3
<input type="checkbox"/>	Global	2/8/16 11:21 AM	2/8/16 11:21 AM	unlimited

Below the table, it says 'Showing 1 - 2 of 2 items'. A context menu is open over the 'Global' profile, showing 'Edit' and 'Reset' options.

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

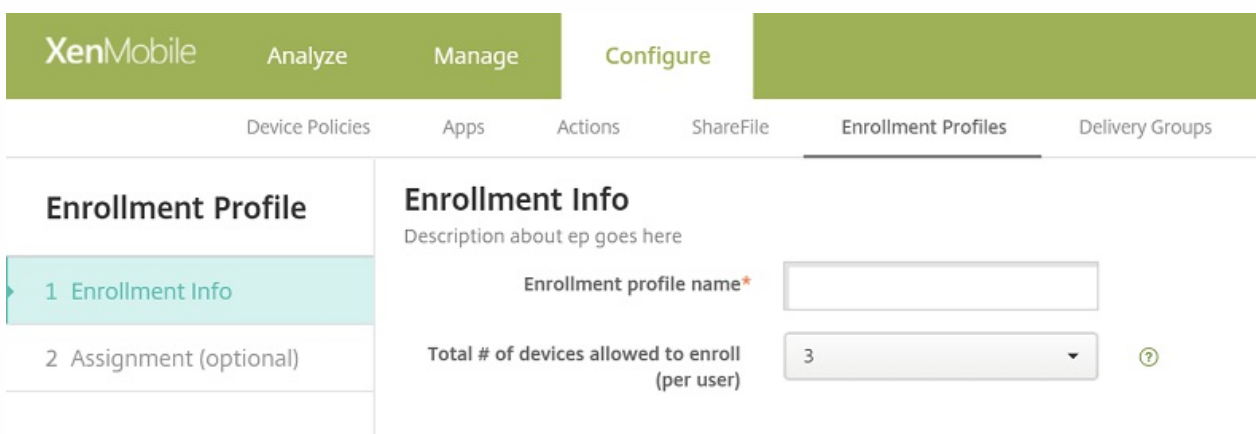


## デリバリーグループのデバイス登録制限を構成するには

1. [Configure] > [Enrollment Profiles] > [Add] の順に移動します。

[Enrollment Info] 画面が開きます。

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



3. [Next] をクリックします。

[Delivery Group Assignment] 画面が開きます。

4. デバイスの登録制限が適用されるデリバリーグループを選択して、[Save] をクリックします。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile **Enrollment Profiles** Delivery Groups

### Enrollment Profile

- 1 Enrollment Info
- 2 Assignment (optional)

## Delivery Group Assignment

Description about the assignment goes here

Choose delivery groups

- AllUsers
- sales
- Engineering

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

XenMobile Analyze Manage **Configure** ⚙️ 🔍 Administrator ▾

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

### Delivery Groups Show filter

| 
  | 
  | 
  |

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input checked="" type="checkbox"/>	<input type="button" value="✕"/>	Engineering	Feb 8 2016 2:39 PM	
<input type="checkbox"/>	<input type="button" value="✕"/>	AllUsers		
<input type="checkbox"/>	<input type="button" value="✕"/>	sales	Feb 8 2016 2:38 PM	

Showing 1 - 3 of 3 items

[Enrollment Profile] 画面が開きます。

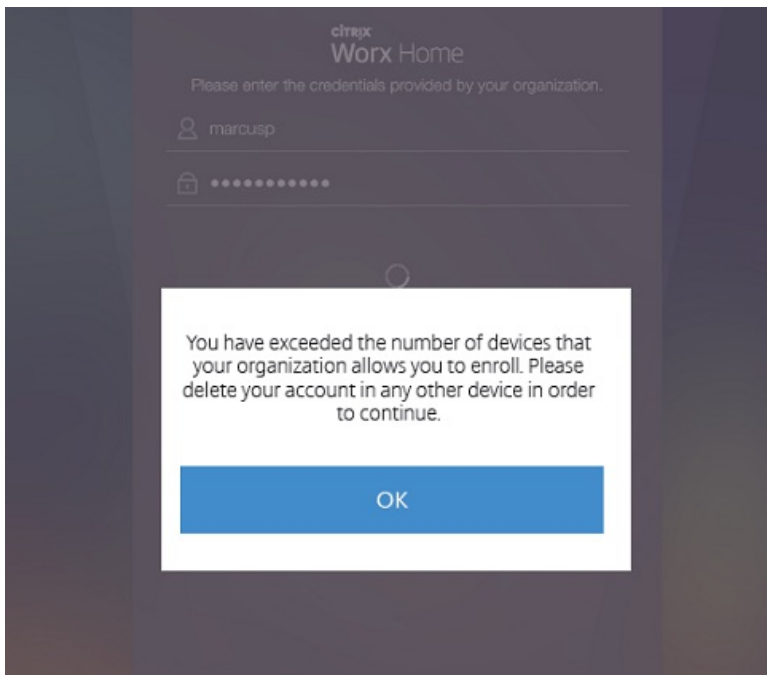
5. この画面から、このデリバリーグループに適用する登録プロファイルを選択してから、[Next] をクリックして変更を表示し、保存します。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, with sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' tab is selected, and the 'Enrollment Profile' sub-tab is active. The main content area displays the 'Enrollment Profile' configuration page. On the left, a sidebar lists the steps: '1 Delivery Group Info', '2 User', '3 Resource (optional)', 'Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profile' (highlighted), and '4 Summary'. The main area shows the title 'Enrollment Profile' and a close button 'x'. Below the title, it says 'Select the enrollment profile that you want the users in this delivery group to see'. There are three radio button options: 'ep1', 'ep2', and 'Global' (which is selected). At the bottom right, there are 'Back' and 'Next >' buttons.

## デバイス登録制限のユーザーエクスペリエンス

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

1. Secure Hubにサインオンします。
2. 登録するサーバーアドレスを入力します。
3. 資格情報を入力します。
4. デバイス制限に達した場合、エラーメッセージが表示され、ユーザーにデバイス登録数を超過したため、管理者に問い合わせるように伝えます。



Secure Hub登録画面が再度表示されます。

# 共有デバイス

Apr 27, 2017

XenMobileでは、複数のユーザーが共有できるデバイスを構成できます。共有デバイス機能を使用すると、たとえば、病院の臨床医は、特定のデバイスを持ち歩くのではなく、近くにある任意のデバイスを使用して、アプリケーションやデータにアクセスできます。場合によっては、法執行機関、リテール、製造などの現場で交代勤務労働者にデバイスを共有させ、機器費用の削減を図る必要があります。

## 共有デバイスに関する注意点

### MDMモード

- iOSおよびAndroid搭載のタブレットおよびスマートフォンで使用できます。XenMobile Enterpriseの共有デバイスでは、基本的なデバイス登録プログラム（DEP）による登録はサポートされません。共有デバイスをこのモードで登録するには、認証済みのDEPを使用する必要があります。
- クライアント証明書認証、Citrix PIN、Touch ID、ユーザーエントロピー、2要素認証はサポートされません。

### MDM+MAMモード

- iOSおよびAndroidタブレットでのみ使用できます。
- XenMobile 10.3以降でサポートされています。
- Active Directoryのユーザー名およびパスワード認証のみがサポートされます。
- クライアント証明書認証、Worx PIN、Touch ID、ユーザーエントロピー、2要素認証はサポートされません。
- MAMのみのモードはサポートされません。デバイスはMDMに登録する必要があります。
- Secure Mail、Secure Web、およびShareFileモバイルアプリのみがサポートされます。HDXアプリはサポートされません。
- Active Directoryユーザーのみがサポートされます。ローカルユーザーおよびグループはサポートされません。
- 既存のMDM-onlyモードの共有デバイスをMDM+MAMモードに更新するには、再登録が必要です。
- ユーザーは、XenMobileアプリケーションおよびMDXラップしたアプリケーションのみを共有できます。デバイスのネイティブのアプリケーションは共有できません。
- 最初の登録時にダウンロードすれば、新しいユーザーがデバイスにログオンするたびにXenMobileアプリケーションがダウンロードされることはありません。新しいユーザーは、デバイスを起動して、サインインし、使用を始めることができます。
- セキュリティのために、Android上で各ユーザーのデータを隔離する場合は、XenMobileコンソールで[Disallow rooted devices] ポリシーを [オン] にする必要があります。

## 共有デバイスの登録の前提条件

共有デバイスを登録する前に、以下の操作を行う必要があります。

- 共有デバイス登録ユーザーの役割を作成します。「[RBACを使用した役割の構成](#)」を参照してください。
- 共有デバイスユーザーを作成します。「[XenMobileでローカルユーザーを追加、編集、または削除するには](#)」を参照してください。
- 共有デバイス登録ユーザーに適用されるベースポリシー、アプリケーション、およびアクションを含むデリバリーグループを作成します。「[デリバリーグループの管理](#)」を参照してください。

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

## 共有デバイスの要件

サイレントインストールやアプリケーションの削除など、最善のユーザーエクスペリエンスが提供されるよう、共有デバイスの構成は以下のプラットフォームで行うことをお勧めします。

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

## 共有デバイスを構成するには

以下の手順に従って、共有デバイスを構成します。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Role-Based Access Control]、[Add] の順にクリックします。[Add Role] 画面が表示されます。
3. [Authorized Access] で [Shared Device Enrollment User] 権限を持つShared Device Enrollment Userという名前の共有デバイス登録ユーザーの役割を作成します。[Console features] の [Devices] を展開し、[Selective Wipe device] をオンにします。この設定によって、共有デバイス登録機能アカウントにプロビジョニングされたアプリとポリシーは、デバイスの登録が解除されるとSecure Hubから削除されます。

[Apply Permissions] で、デフォルト設定の [To all user groups] を保持するか、特定のActive Directoryユーザーグループに [To specific user groups] で権限を割り当てます。

Settings > Role-Based Access Control > Add Role

**Add Role**

- 1 Role Info
- 2 Assignment

**Role Info**

RBAC name\*

RBAC template Select a template Apply

Authorized access

- Admin console access
- Self Help Portal access
- Shared devices enroller
- Remote Support access
- Public api access

Console features

- Dashboard
- Reporting
- Devices
  - Full Wipe device
  - Clear Restriction
  - Selective Wipe device
  - View locations
  - Lock device
  - Unlock device

Apply permissions  To all user groups  To specific user groups

Next >

[Next] をクリックして [Assignment] 画面に進みます。作成したばかりの共有デバイス登録の役割を、前提条件の手順1で共有デバイス登録ユーザーのために作成したActive Directoryグループに割り当てます。下の図でcitrix.labはActive Directoryドメイン、Shared Device EnrollersはActive Directoryグループです。

Settings > Role-Based Access Control > Add Role

**Add Role**

- 1 Role Info
- 2 Assignment

**Assignment**  
Assign the RBAC role to user groups

Select domain citrix.lab

Include user groups shared Search

citrix.lab\Shared Device Enrollers

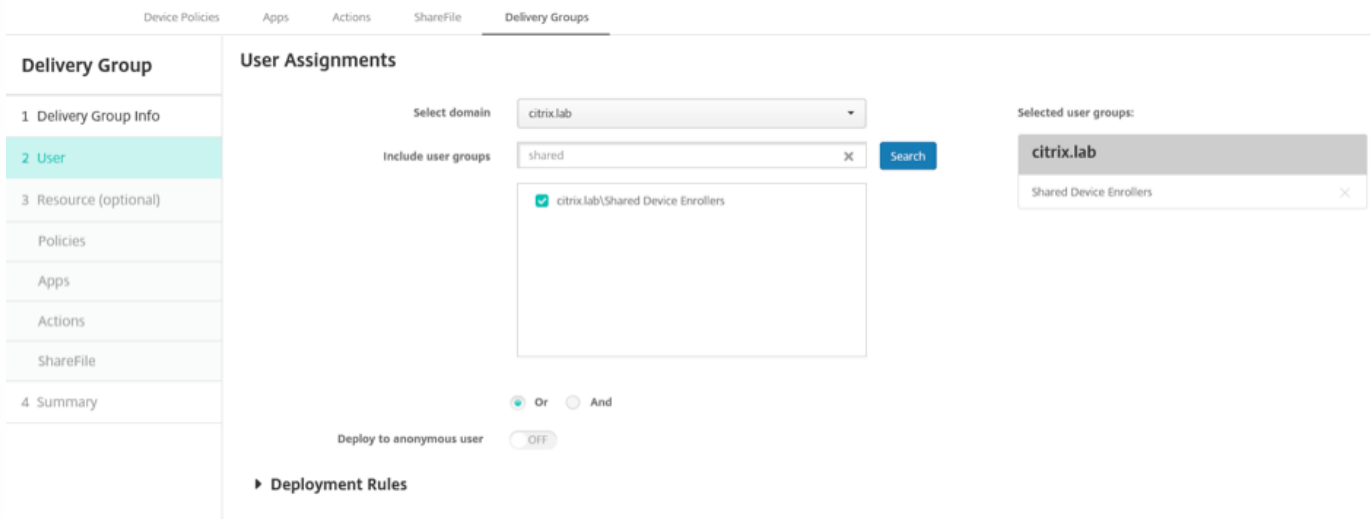
Selected user groups:

**citrix.lab**

Shared Device Enrollers ×

4. ユーザーがサインオンしていないときにデバイスに適用するベースポリシー、アプリケーション、アクションを含むデリバリーグループを作成し、共有デバイス登録ユーザーActive Directoryグループにそのデリバリーグループを関連付けます。





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

6. 認証されたユーザーに異なるポリシーを適用したり、追加のアプリケーションを提供するには、そのユーザーに関連付け、共有デバイスにのみ展開するデリバリーグループを作成する必要があります。グループを作成するときは、展開規則を構成して、パッケージが共有デバイスに展開されるようにします。詳しくは「[展開規則の構成](#)」を参照してください。

7. デバイスの共有を停止するには、選択的ワイプを実行して、共有デバイス登録ユーザーアカウントおよび展開されたアプリケーションとポリシーをデバイスから削除します。

## 共有デバイスのユーザーエクスペリエンス

ユーザーにはそのユーザーが使用できるリソースだけが表示され、すべての共有デバイスに同じエクスペリエンスが提供されます。共有デバイス登録ポリシーとアプリは常にデバイスに残ります。共有デバイス登録ユーザー以外のユーザーがSecure Hubにサインオンすると、そのユーザーのポリシーとアプリケーションがデバイスに展開されます。ユーザーがサインオフすると、共有デバイス登録に必要とされているものを除いて、ポリシーおよびアプリケーションは削除されます。

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

Secure Hubにサインオンできるユーザーは、一度に1人だけです。前のユーザーがサインオフしてからでないと、次のユーザーはサインオンできません。セキュリティ上の理由から、共有デバイスにはユーザーの資格情報が保存されないため、ユーザーはサインオンのたびに資格情報を入力する必要があります。前のユーザーのためのリソースに新しいユーザーがアクセスできないように、前のユーザーに関連付けられているポリシー、アプリケーション、データが削除されている間、新しいユーザーはサインオンできません。

共有デバイス登録によって、アプリケーションのアップグレードプロセスが変更されることはありません。通常通り、共有

デバイスユーザーにアップグレードをプッシュし、共有デバイスユーザーはデバイス上でアプリケーションをアップグレードできます。

## 推奨されるSecure Mailポリシー

- Secure Mailのパフォーマンスを最適化するためには、デバイスを共有するユーザーの数に応じて[Max sync period]を設定します。無制限同期を許可することは推奨されません。

デバイスを共有するユーザーの数	推奨される [Max sync period]
21~25	1週間以内
6~20	2週間以内
5以下	1か月以内

- [Enable contact export] を禁止して、ユーザーの連絡先がデバイスを共有する他のユーザーにさらされないようにします。
- iOSでは、次の設定のみをユーザーごとに設定できます。その他のすべての設定はデバイスを共有しているユーザー間で共通です。

Notifications  
Signature  
Out of Office  
Sync Mail Period  
S/MIME  
Check Spelling

# Android at Work

Apr 27, 2017

Android at Work (Android for Workから改称) は、Android 5.0以降を実行しているAndroidデバイスで使用できるセキュリティ保護されたワークスペースです。このワークスペースはビジネス用のアカウント、アプリ、データを個人のアカウント、アプリ、データから隔離します。XenMobileでは、デバイスに1人の作業プロファイルを作成できるため、BYOD (Bring Your Own Device) と会社が所有するAndroidデバイスの両方を管理できます。ハードウェアの暗号化および展開するポリシーを組み合わせることで、デバイスで業務の領域と個人領域を安全に隔離できます。ユーザーの個人用の領域に影響を与えずに、社用のすべてのポリシー、アプリ、およびデータをリモートで管理できます。サポートされているAndroidデバイスについて詳しくは、[Google Android Enterprise](#)のサイトを参照してください。

Google Playを使用して、アプリを追加、購入、および承認し、デバイスのAndroid at Workワークスペースに展開します。Google Playを使用してプライベートなAndroidアプリ、パブリックアプリ、およびサードパーティアプリを展開できます。Android at Work用のパブリックアプリケーションストアの有料アプリをXenMobileに追加するときに、一括購入ライセンスの状態を確認できます。状態に含まれる情報は、使用できる合計ライセンス数、使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレスです。詳しくは、「[XenMobileへのパブリックアプリケーションストアのアプリケーションの追加](#)」を参照してください。

## Android at Workの要件

- パブリックにアクセスできるドメイン
- Google管理者アカウント
- 管理されたプロファイルサポートがあり、Android 5.0以降のLollipopを実行しているデバイス
- Google PlayがインストールされているGoogleアカウント
- デバイスで設定されたワークプロファイル

Android at Workアプリ制限を設定するには、次の手順を実行する必要があります。

- GoogleのAndroid at Work設定タスクを完了します。
- 一連のGoogle Play資格情報を作成します。
- Android at Workサーバー設定を構成します。
- 少なくとも1つのAndroid at Workデバイスポリシーを作成します。
- Google PlayアプリストアでAndroid at Workアプリを追加、購入、承認します。

Android at Workを管理する場合は、次のリンクを使用できます。

- Google管理コンソール : <https://admin.google.com/AdminHome>
- Google Play管理コンソール : <https://play.google.com/work/apps>
- プライベートチャンネルおよびセルフホストアプリケーション用のGoogle Playの公開 <https://play.google.com/apps/publish>
- サービスアカウント作成のためのGoogle Developer Console : <https://console.developers.google.com>

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

- Android at Workアカウントの作成。
- サービスアカウントのセットアップ。
- Android at Work証明書のダウンロード。
- Google Admin SDKおよびMDM APIの有効化。
- ディレクトリとGoogle Playを使用するためのサービスアカウントの承認。
- バインドトークンを入手します。

次のセクションでは、このそれぞれのタスクの実行方法を説明します。これらのタスクを完了すると、XenMobileで一連のGoogle Play資格情報を作成し、Android設定を構成して、Androidアプリを管理できます。資格情報の作成について詳しくは、「[Google Play資格情報](#)」を参照してください。

## Android at Workアカウントの作成

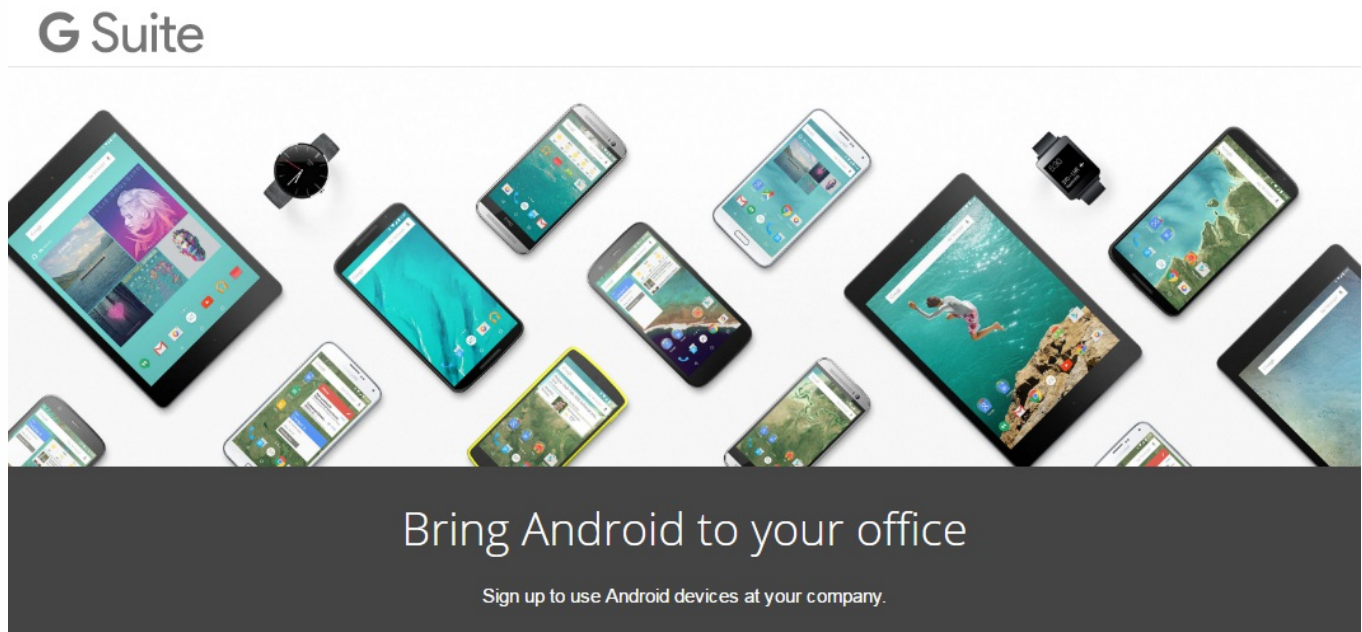
Android at Workアカウントを構成する前に、以下の前提条件を満たす必要があります。

- ドメイン名 (たとえば、example.com) を所有している。
- Googleにドメインの所有権を検証させる。
- EMM (Enterprise Mobility Management : エンタープライズモビリティ管理) プロバイダー (XenMobile 10.1以降など) を介して、Android at Workを有効化し、管理します。

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

1. [https://www.google.com/a/signup/?enterprise\\_product=ANDROID\\_WORK](https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK) に移動します。

管理者情報と会社情報を入力する次のページが開きます。



## ① About you

Name

Current work email

Doesn't have to be an official business email.

Phone

2. 管理者のユーザー情報を入力します。

① About you

Name

Justa ✓ User ✓

Current work email Doesn't have to be an official business email.

justa.user@gmail.com ✓

Phone

+15551234567 ✓

3. 管理者のアカウント情報だけでなく、会社情報も入力してください。

② About your business

Business name

EXAMPLE CORP ✓

Business domain address You'll need to verify that you own this domain.

example.com ✓

Number of employees Country/Region

1 employee United States

③ Your Google admin account Why do I need this?

Username Create an account to manage Android for Work

justa.user ✓ @ example.com

Create a password 8-character minimum; case sensitive

..... ✓

..... ✓

プロセスの最初の手順が完了します。以下のページが開きます。



## Bring Android to your office

With Android, you can manage your company's devices and keep them secure.



Create your domain admin account



Verify domain ownership

Verify you're the owner of your company's domain and protect its security.

START



Connect with your provider

Allow an enterprise mobility management (EMM) provider to keep your organization's devices secure.

### ドメイン所有権の検証


以下のいずれかの方法で、Googleがドメインを検証できるようにします。

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

1. [Start] をクリックして、ドメインの検証を開始します。

[Verify domain ownership] ページが開きます。画面の指示に従ってドメインを検証します。

2. [Verify] をクリック します。



## Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)

After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

**Note:** Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

VERIFY



## Verify domain ownership


### Verification checklist

Follow these steps to help Google verify that you own the domain **example.com**. [Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

VERIFY

3. Googleによってドメイン所有権が検証されます。



## Verify domain ownership

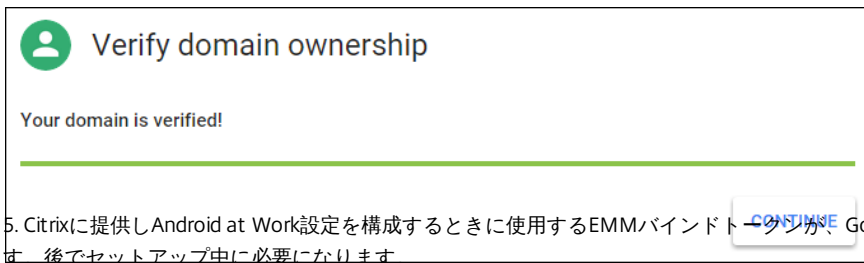
### Verifying your domain ownership

The domain host is updating your information. This might take a bit—you can close this window and come back to [admin.google.com](#) later without interrupting the process. [Learn more](#)

Estimated time remaining: 5 minutes

---

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

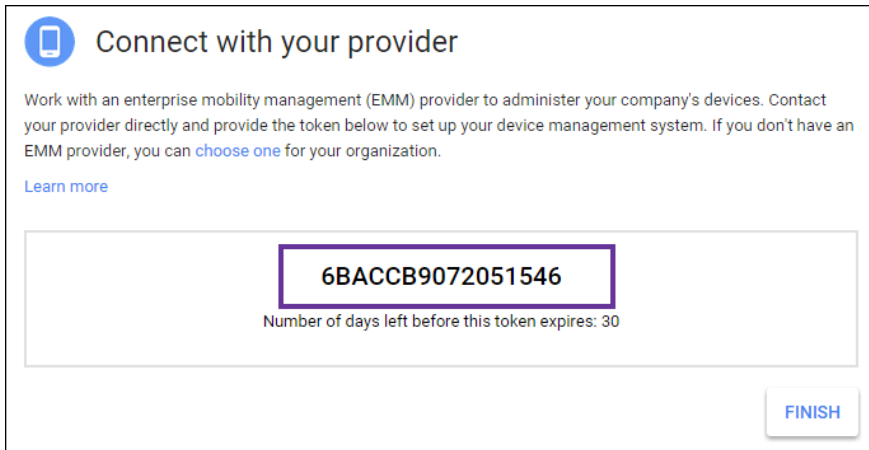


**Verify domain ownership**

Your domain is verified!

5. Citrixに提供しAndroid at Work設定を構成するときに使用するEMMバインドトークンが、Googleによって作成されます。トークンをコピーして保存します。後でセットアップ中に必要になります。

**CONTINUE**



**Connect with your provider**

Work with an enterprise mobility management (EMM) provider to administer your company's devices. Contact your provider directly and provide the token below to set up your device management system. If you don't have an EMM provider, you can [choose one](#) for your organization.

[Learn more](#)

**6BACCB9072051546**

Number of days left before this token expires: 30

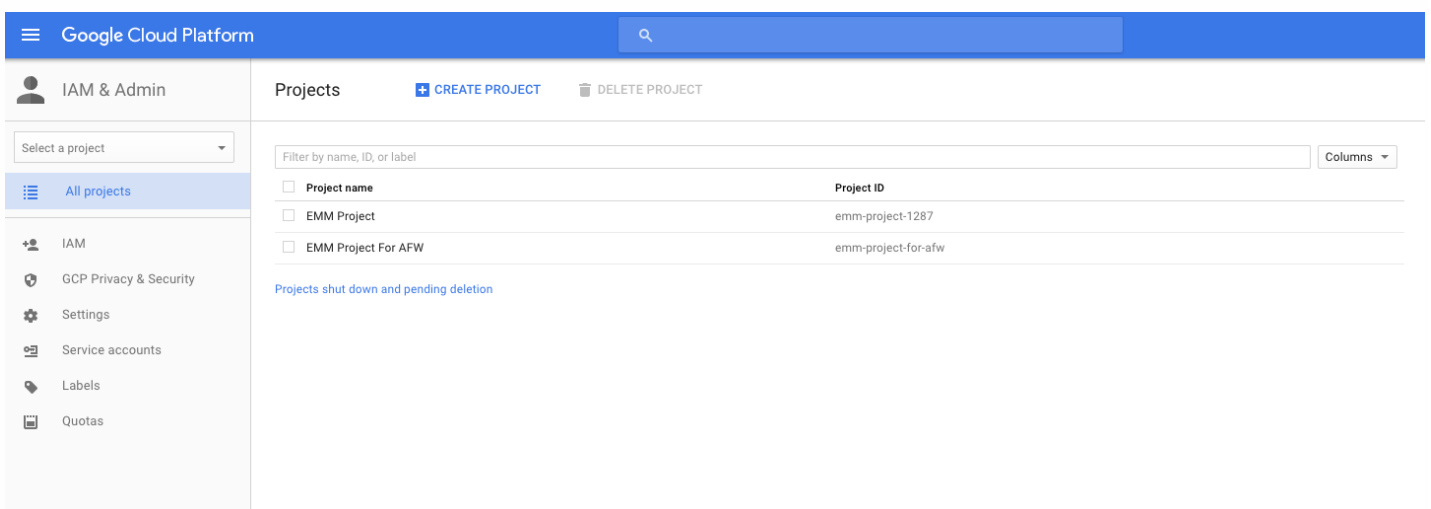
**FINISH**

6. **[Finish]** をクリックしてAndroid at Workの設定を完了します。ドメインの検証に成功したことを示すページが表示されます。Android at Workサービスアカウントを作成すると、Google Adminコンソールにサインインしてモビリティ管理設定を管理できます。

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

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

1. Webブラウザで<https://console.cloud.google.com/project>を開いて、Google管理者の資格情報でサインインします。
2. **[Projects]** の一覧で、**[Create Project]** をクリックします。



Google Cloud Platform

IAM & Admin

Projects **CREATE PROJECT** DELETE PROJECT

Select a project

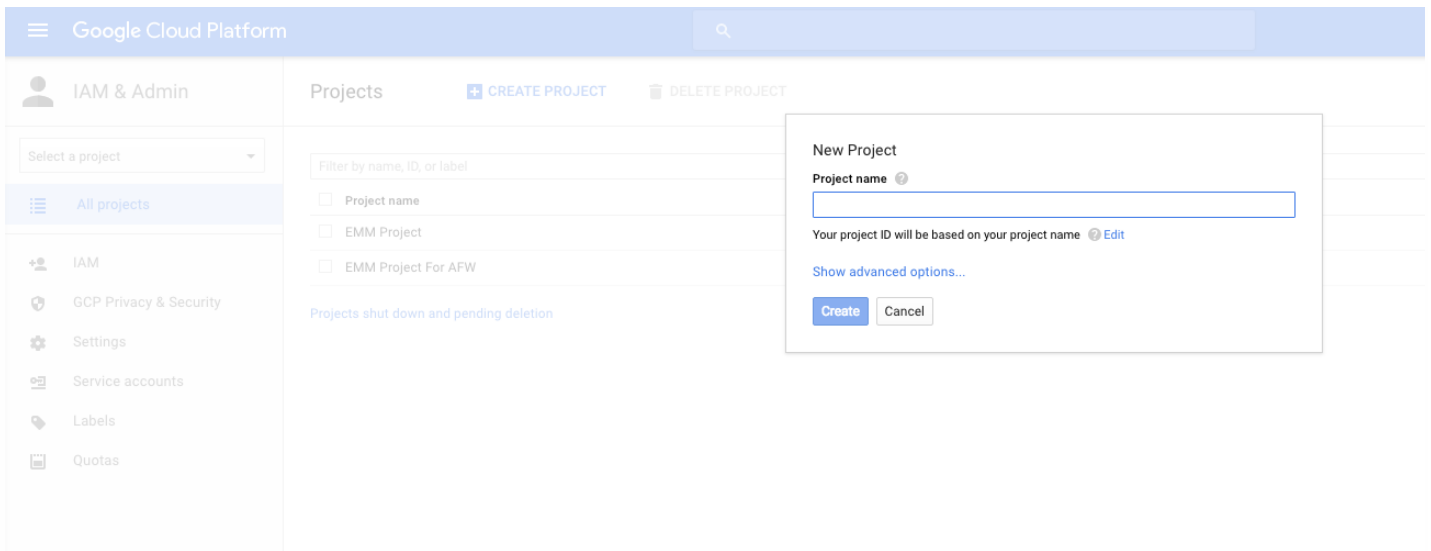
Filter by name, ID, or label

Project name	Project ID
<input type="checkbox"/> EMM Project	emm-project-1287
<input type="checkbox"/> EMM Project For AFW	emm-project-for-afw

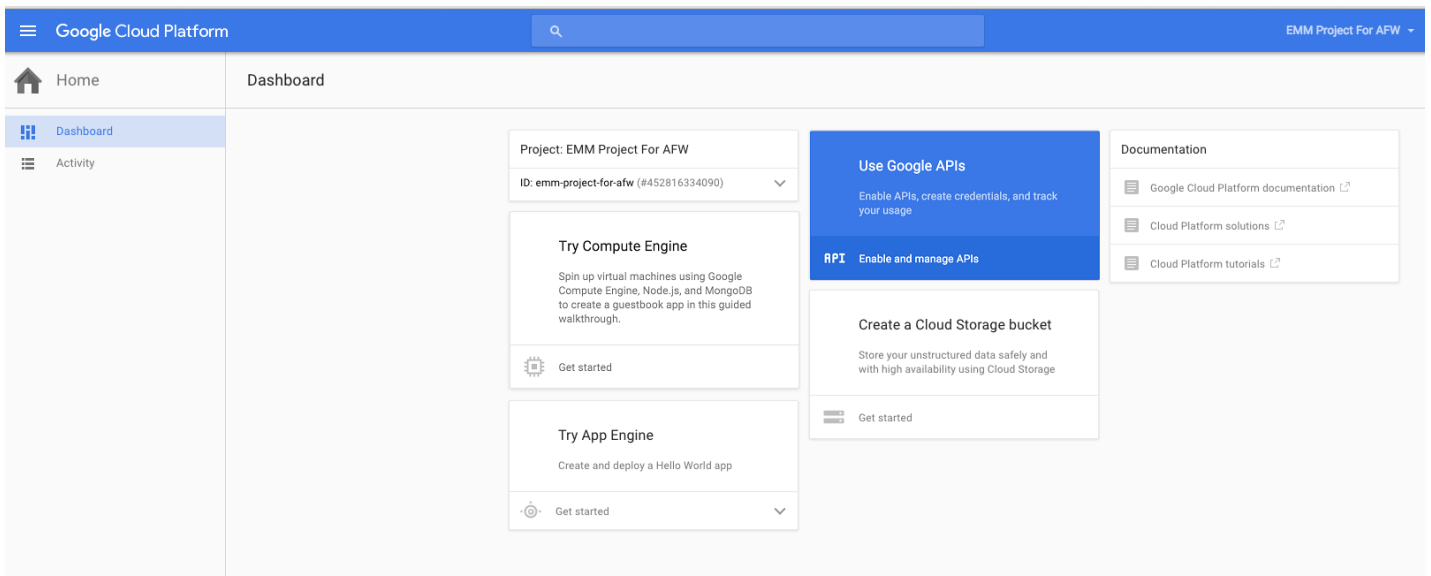
Projects shut down and pending deletion

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

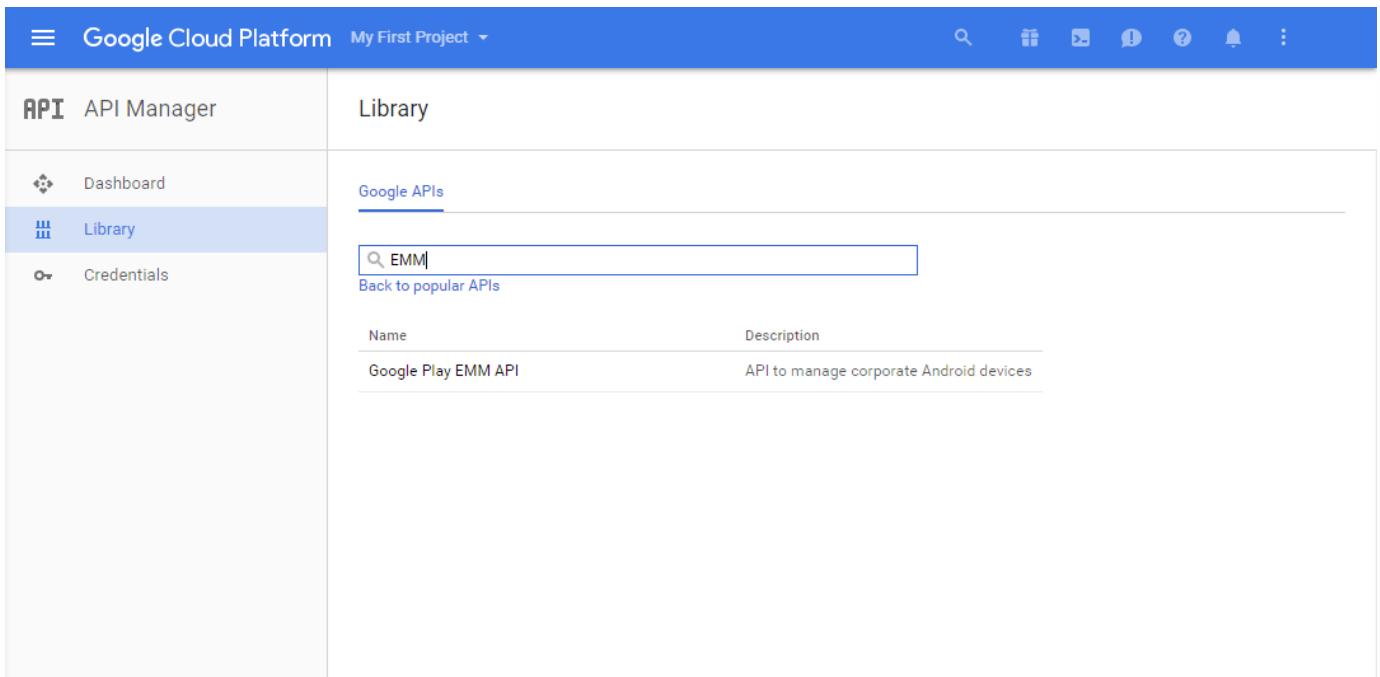




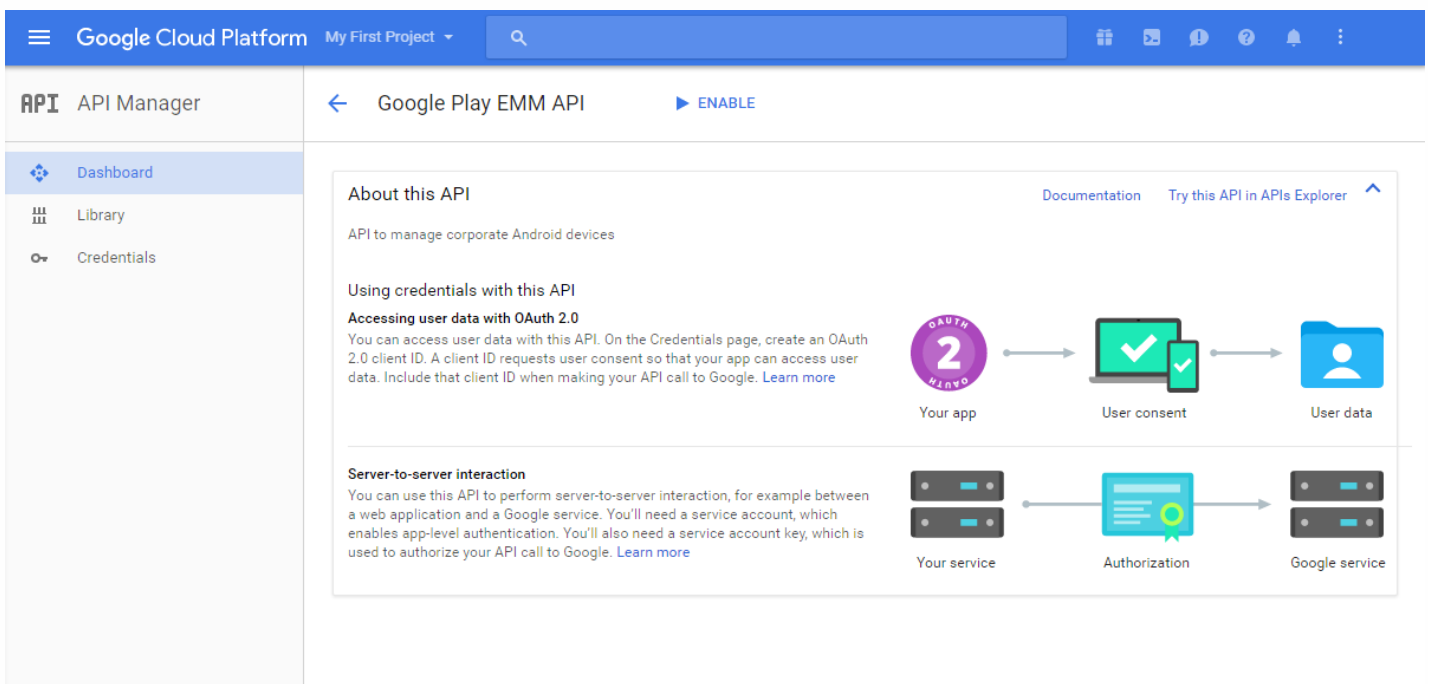
4. [Dashboard] ページで、[Use Google APIs] をクリックします。



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



6. [Overview] ページで、[Enable] をクリックします。



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

Google Cloud Platform

API Manager

Overview

← Disable

Google Play EMM API

⚠ This API is enabled, but you can't use it in your project until you create credentials. Click "Go to Credentials" to do this now (strongly recommended). [Go to Credentials](#)

Overview Usage Quotas

API to manage corporate Android devices  
[Learn more](#)  
[Try this API in APIs Explorer](#)

Using credentials with this API

**Accessing user data with OAuth 2.0**  
 You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. [Learn more](#)

**Server-to-server interaction**  
 You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. [Learn more](#)

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

Google Cloud Platform

API Manager

Credentials

Add credentials to your project

1 Find out what kind of credentials you need

We'll help you set up the correct credentials  
 If you wish you can skip this step and create an [API key](#), [client ID](#), or [service account](#)

**Which API are you using?**  
 Determines what kind of credentials you need.

Google Play EMM API

**Where will you be calling the API from?**  
 Determines which settings you'll need to configure.

Choose...

**What data will you be accessing?**

User data  
 Access data belonging to a Google user, with their permission

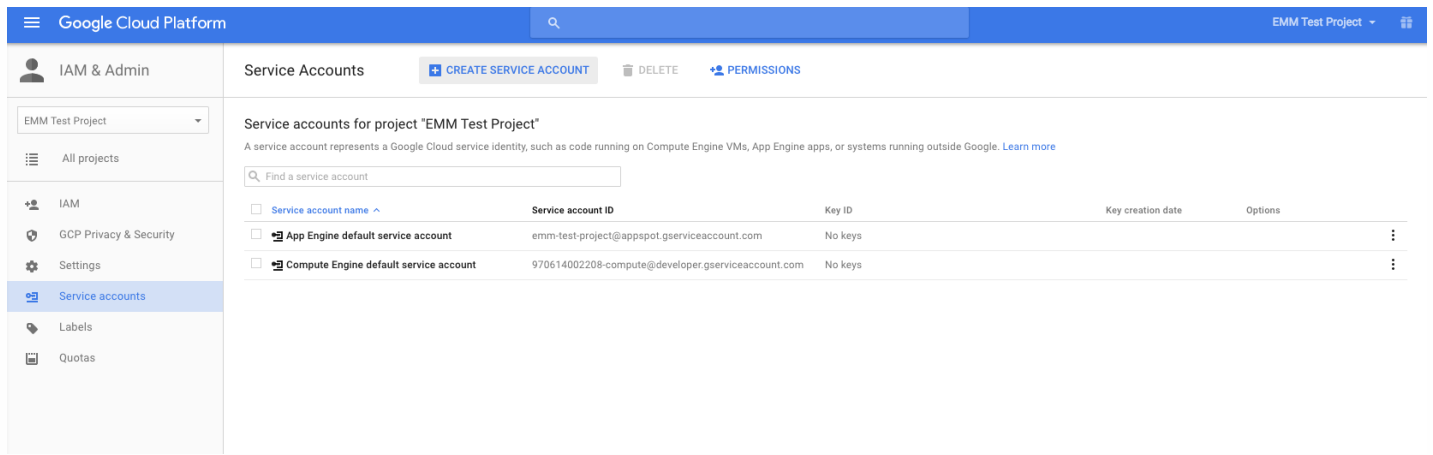
Application data  
 Access data belonging to your own application

[What credentials do I need?](#)

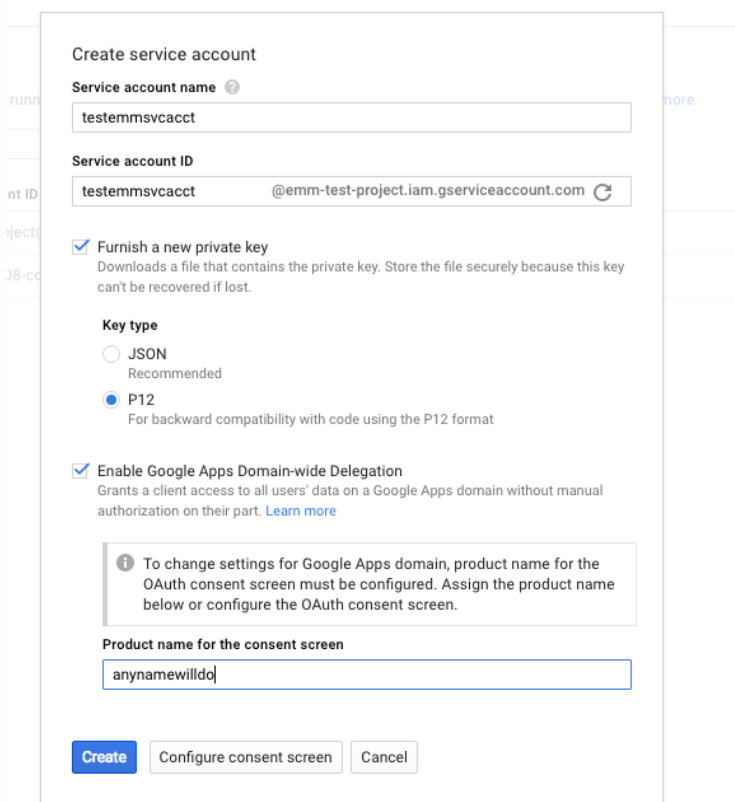
2 Get your credentials

Cancel

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

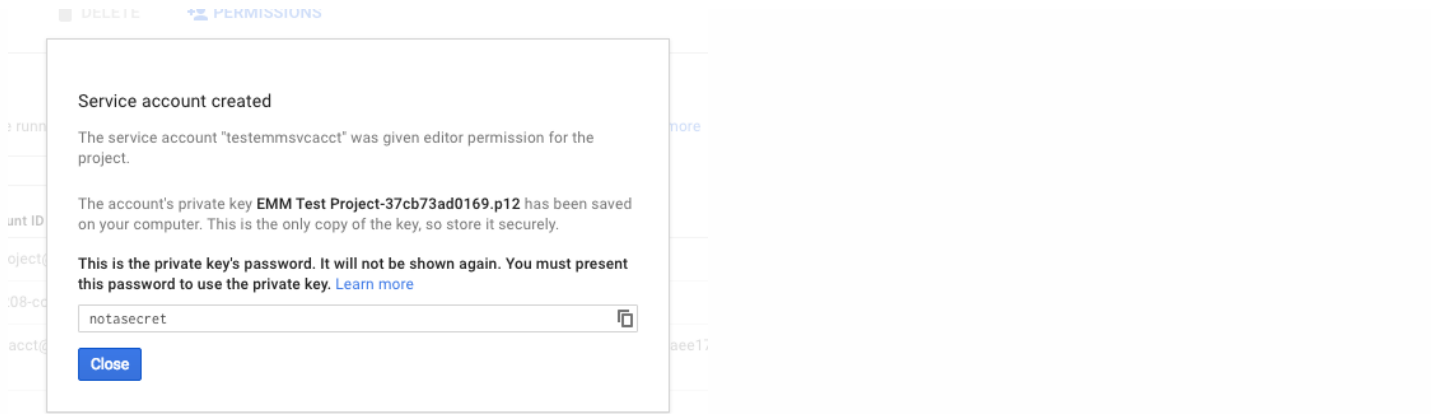


10. [Create service account] で、アカウントに名前を付けて、[Furnish a new private key] をオンにします。[P12] を選択して、[Enable Google Apps Domain-wide Delegation] をオンにし、[Create] をクリックします。

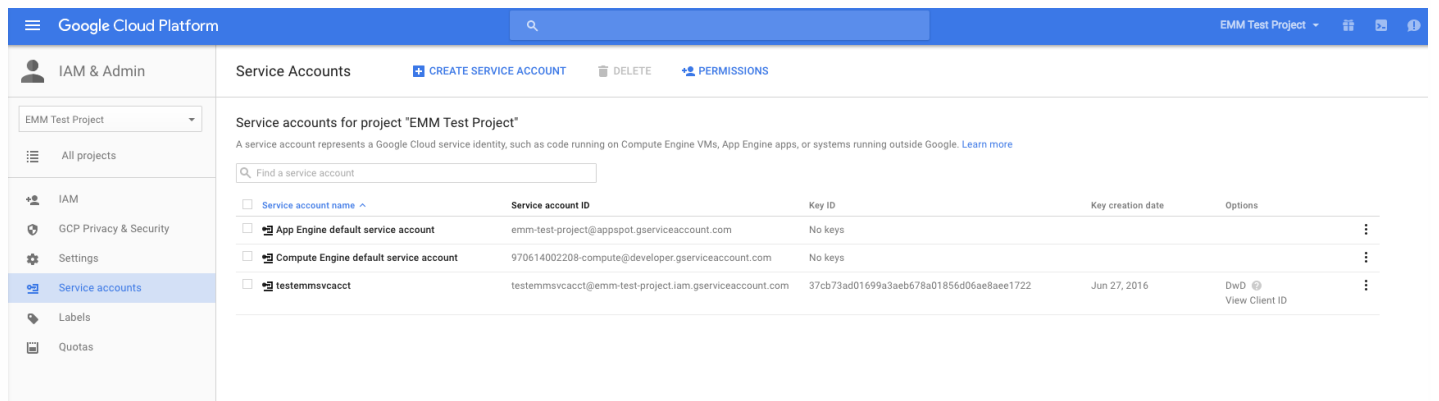


証明書 (P12ファイル) がコンピューターにダウンロードされます。証明書を安全な場所に保存してください。

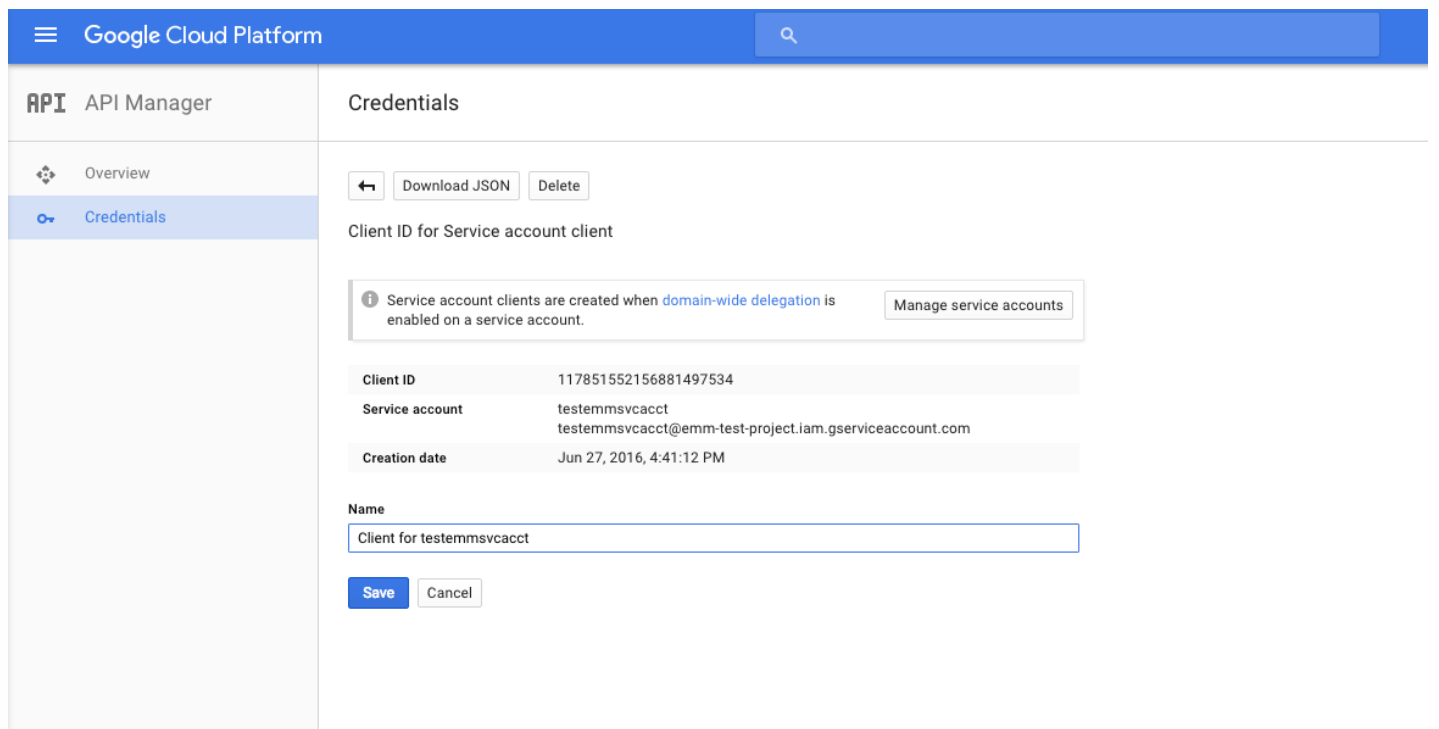
11. [Service account created] 確認画面で、[Close] をクリックします。



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



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



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

Google Cloud Platform My First Project

API Manager

Library

Google APIs

Admin SDK

Back to popular APIs

Name	Description
Admin SDK	Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

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

Google Cloud Platform My First Project

API Manager

Admin SDK ENABLE

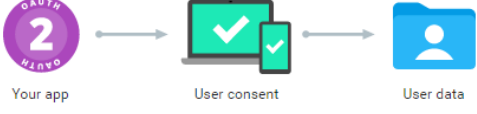
About this API [Documentation](#) [Try this API in APIs Explorer](#)

Admin SDK lets administrators of enterprise domains to view and manage resources like user, groups etc. It also provides audit and usage reports of domain.

Using credentials with this API

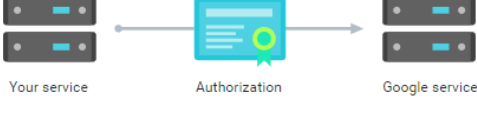
**Accessing user data with OAuth 2.0**

You can access user data with this API. On the Credentials page, create an OAuth 2.0 client ID. A client ID requests user consent so that your app can access user data. Include that client ID when making your API call to Google. [Learn more](#)

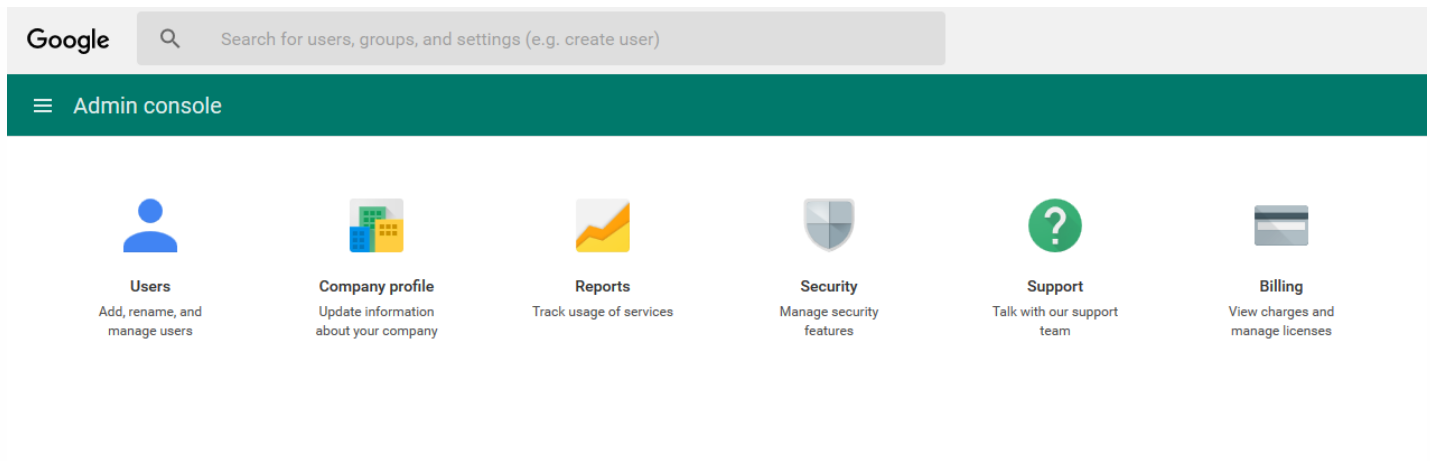


**Server-to-server interaction**

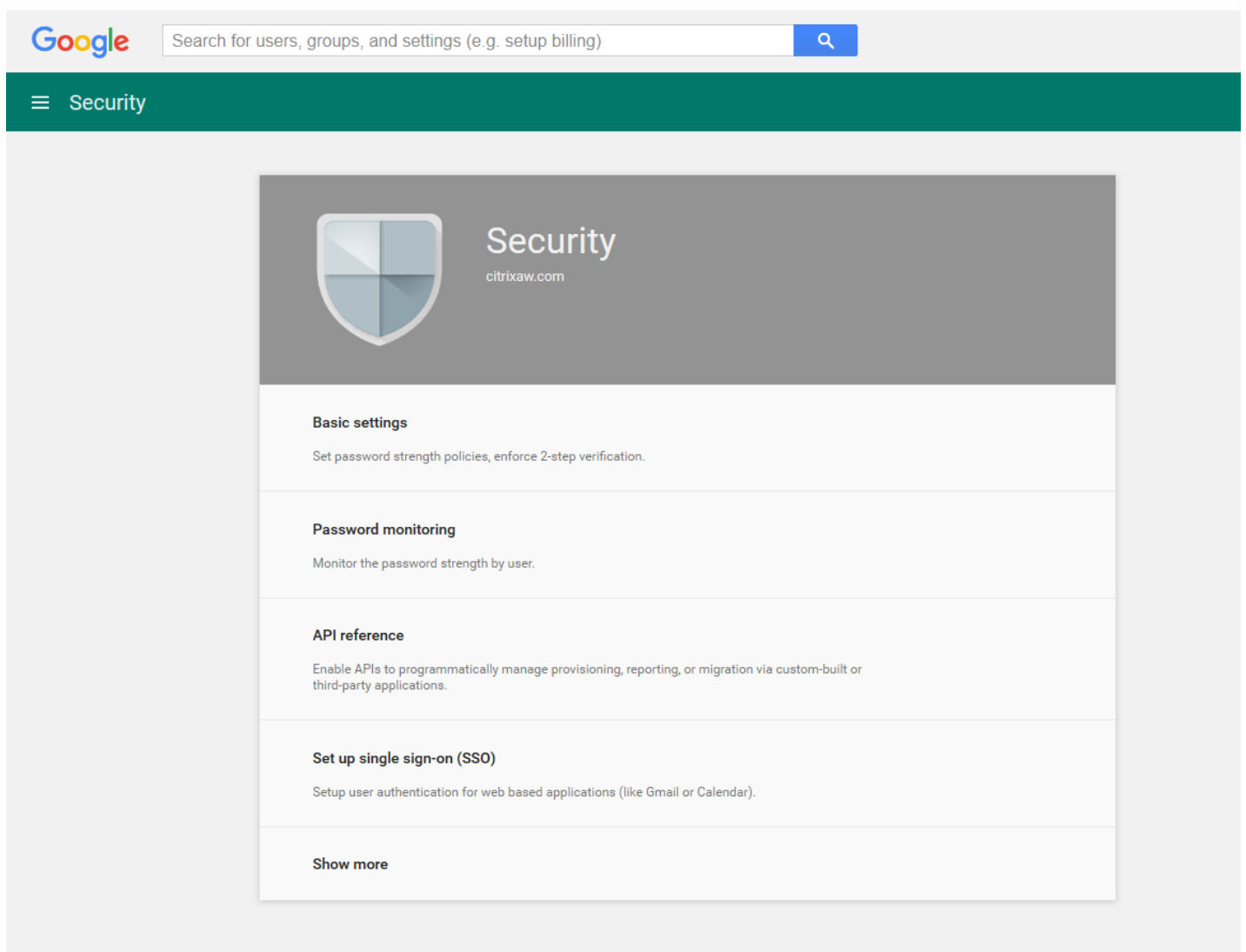
You can use this API to perform server-to-server interaction, for example between a web application and a Google service. You'll need a service account, which enables app-level authentication. You'll also need a service account key, which is used to authorize your API call to Google. [Learn more](#)



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



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





## Security

citrixaw.com

### Basic settings

Set password strength policies, enforce 2-step verification.

### Password monitoring

Monitor the password strength by user.

### API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

### Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

### Manage EMM provider for Android

Keep your company's devices secure with an enterprise mobility management provider.

### Advanced settings

Manage advanced security features such as authentication, and integrating G Suite with internal services.

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



## Security

Monitor the password strength by user.

### API reference

Enable APIs to programmatically manage provisioning, reporting, or migration via custom-built or third-party applications.

### Set up single sign-on (SSO)

Setup user authentication for web based applications (like Gmail or Calendar).

### Manage EMM provider for Android

Keep your company's devices secure with an enterprise mobility management provider.

## Advanced settings

Authentication

[Manage API client access](#)

Allows admins to control access to user data by applications that use OAuth protocol.

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

## Security



### Manage API client access

Developers can register their web applications and other API clients with Google to enable access to data in Google services like Calendar. You can authorize these registered clients to access your user data without your users having to individually give consent or their passwords. [Learn more](#)

#### Authorized API clients

The following API client domains are registered with Google and authorized to access data for your users.

Client Name	One or More API Scopes	Authorize	<a href="#">Learn more about registering new API clients</a>
1234567891011121314 Example: www.example.com	<input type="text" value="https://www.googleapis.com/auth/admin.direc"/> Example: http://www.google.com/calendar/feeds/ (comma-delimited)	<input type="button" value="Authorize"/>	<a href="#">Learn more about registering new API clients</a>

102668191251038864577

[View and manage the provisioning of users on your domain](#) https://www.googleapis.com/auth/admin.directory.user

[Remove](#)

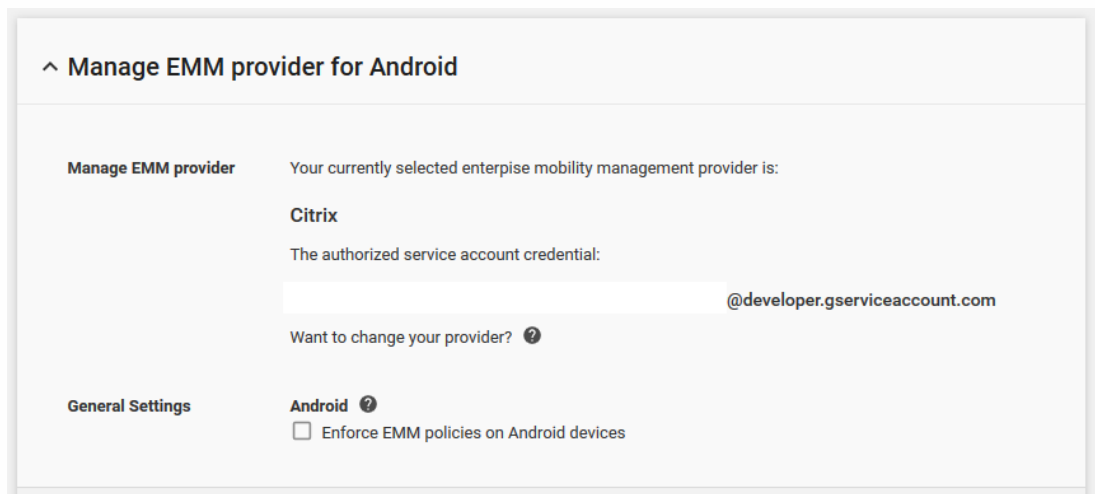
XenMobileを使用してAndroidデバイスを管理するには、Citrixテクニカルサポートにドメイン名、サービスアカウント、およびバインドトークンを提供する必要があります。CitrixはトークンをEMM（エンタープライズモビリティ管理）プロバイダーとしてのXenMobileにバインドします。Citrixテクニカルサポートへのお問い合わせは、[Citrixテクニカルサポートを参照してください](#)。

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

Google Android at WorkアカウントがEMMプロバイダーとしてのCitrixにバインドされていることが表示されます。

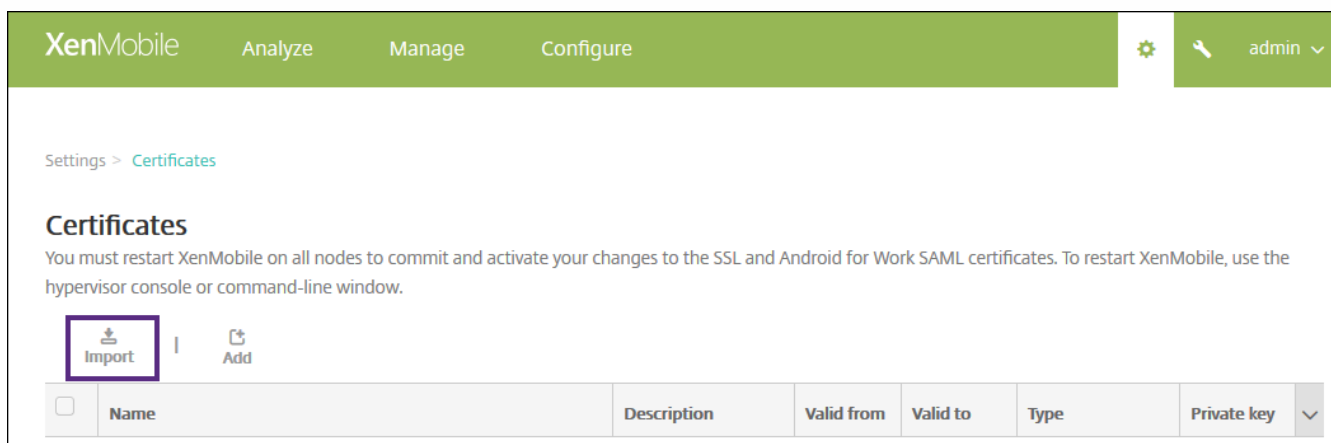
トークンのバインドを確認した後で、XenMobileコンソールを使用してAndroidデバイスの管理を開始できます。手順14で生成したP12証明書をインポートします。Android at Workサーバー設定をセットアップし、SAMLベースのシングルサインオンを有効化し、少なくとも1つAndroid at Workデバイスポリシーを

定義する必要があります。



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

1. XenMobileコンソールにサインインします。
2. コンソールの右上にある歯車アイコンをクリックして [Settings] ページを開き、 [Certificates] をクリックします。 [Certificates] ページが開きます。



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

**Import** ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import: Keystore

Keystore type: PKCS#12

Use as: Server

次の設定を構成します。

- Import : ボックスの一覧から、[Keystore] を選択します。
- Keystore type : ボックスの一覧から、[PKCS#12] を選択します。
- Use as : ボックスの一覧から、[Server] を選択します。
- Keystore file : [Browse] をクリックして、P12証明書を選択します。
- Password : キーストアのパスワードを入力します。
- Description : 任意で、証明書の説明を入力します。

4. [Import] をクリックします。

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

2. [Server] の下の [Android at Work] をクリックします。[Android at Work] ページが開きます。

XenMobile Analyze Manage Configure ⚙️ 🔍 admin ▼

Settings > Android for Work

**Android for Work**  
Provide Android for Work configuration parameters.

Domain Name\*

Domain Admin Account\*

Service Account ID\*

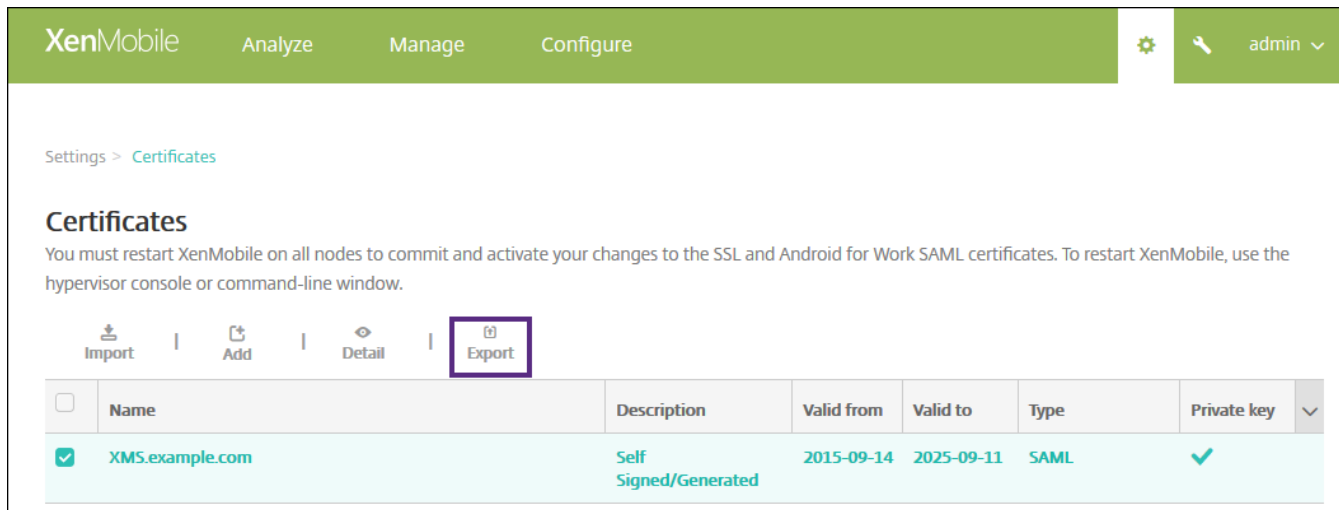
Enable Android for Work  NO

Cancel Save

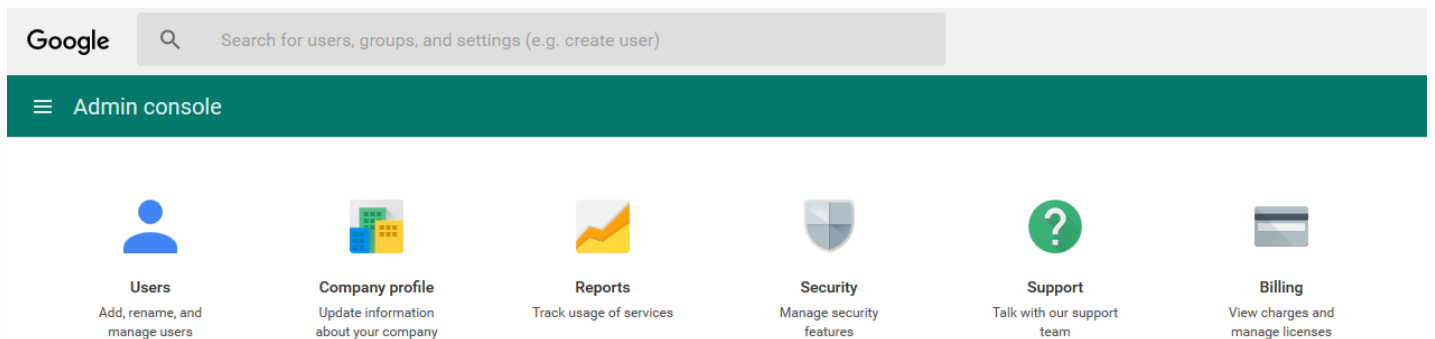
次の設定を構成します。

- **Domain name** : Android at Workのドメイン名を入力します (例 : domain.com) 。
  - **Domain Admin Account** : ドメイン管理者のユーザー名を入力します (例 : Google Developer Portalで使用しているメールアカウント) 。
  - **Service Account ID** : サービスアカウントIDを入力します (例 : Google Service Accountに関連付けられたメールアドレス (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com) ) 。
  - **Enable Android at Work** : クリックして、Android at Workを有効または無効にします。
3. [Save] をクリックします。

1. XenMobileコンソールにサインインします。
2. コンソールの右上にある歯車アイコンをクリックします。 [Settings] ページが開きます。
3. [Certificates] をクリックします。 [Certificates] ページが開きます。



3. 証明書の一覧から、SAML証明書を選択します。
4. [Export] をクリックして証明書をコンピューターに保存します。
5. Android at Workの管理者資格情報でGoogle Adminポータルにサインインします。ポータルへのアクセスについて詳しくは、[Google Admin portal](#)を参照してください。
6. [Security] をクリックします。



7. [Security] の下の [Set up single sign-on (SSO) ] をクリックして以下の設定を構成します。

## ^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

### Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL

URL for signing in to your system and Google Apps

Sign-out page URL

URL for redirecting users to when they sign out

Change password URL

URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled

Verification certificate

The certificate file must contain the public key for Google to verify sign-in requests. ?

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

[DISCARD CHANGES](#) [SAVE CHANGES](#)

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

8. [SAVE CHANGES] をクリックします。

パスワードポリシーをセットアップして、ユーザーが初めて登録するときにデバイスでのパスワード設定を必須にすることをお勧めします。

**Passcode Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung KNOX
- Android for Work**
- Windows Phone
- Windows Tablet

3 Assignment

**Policy Information**

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode Required **ON**

**Passcode requirements**

Minimum length: 6

Biometric recognition: OFF

Advanced rules: OFF A 3.0+

**Passcode security**

Lock device after (minutes of inactivity): None

Passcode expiration in days (1-730): 0

Previous passwords saved (0-50): 0

Maximum failed sign-on attempts: Not defined

► **Deployment Rules**

Back Next >

デバイスポリシーの基本的なセットアップ手順は以下のとおりです。

1. XenMobileコンソールにサインオンします。
2. [Configure] > [Device Policies] をクリックします。
3. [Add] をクリックして、[Add a New Policy] ダイアログボックスから追加するポリシーを選択します。この例では[Passcode] をクリックします。
4. [Policy Information] ページに入力します。
5. [Android at Work] をクリックしてポリシーの設定を構成します。
6. ポリシーをデリバリーグループに割り当てます。

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

## Android at Workアカウント設定の構成

ユーザーのデバイスでAndroidのアプリとポリシーを管理できるようにするには、XenMobileでAndroid at Workのドメインおよびアカウント情報を設定する必要があります。最初にドメイン管理者を設定し、サービスアカウントIDとバインドトークンを取得するために、GoogleでAndroid at Workの設定を完了しておく必要があります。

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

Settings &gt; Android for Work

## Android for Work

Provide Android for Work configuration parameters.

Domain Name*	<input type="text"/>
Domain Admin Account*	<input type="text"/>
Service Account ID*	<input type="text"/>
Enable Android for Work	<input checked="" type="radio"/> YES

3. [Android for Work] ページで以下の設定を構成します。

- **Domain Name** : ドメイン名を入力します。
- **Domain Admin Account** : ドメイン管理者のユーザー名を入力します。
- **Service Account ID** : GoogleのサービスアカウントIDを入力します。
- **Enable Android for Work** : Android for Workを有効にするかどうかを選択します。

4. [Save] をクリックします。

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

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

NFCが使用される理由工場出荷時設定にリセットされたデバイスでは、Bluetooth、Wi-Fi、およびその他の通信モードは無効になっています。この状態のデバイスが使用する通信プロトコルはNFCのみです。

### 前提条件

- Android at Workを有効にしたXenMobile Serverバージョン10.4。
- デバイス所有者モードでAndroid at Work向けにプロビジョニングされた、工場出荷時設定にリセットされたデバイス。この前提条件を完了する手順については、後述します。
- 構成済みのProvisioning Toolを実行している、NFC機能が備わった別のデバイス。Provisioning Toolは、Secure Hub 10.4または[Citrixダウンロードページ](#)から入手できます。

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

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

### デバイス所有者モードでのNFCバンプ

工場出荷時の設定にリセットされたデバイスをプロビジョニングするには、以下のデータをNFCバンプ経由で送信してAndroid at Workを初期化する必要があります。

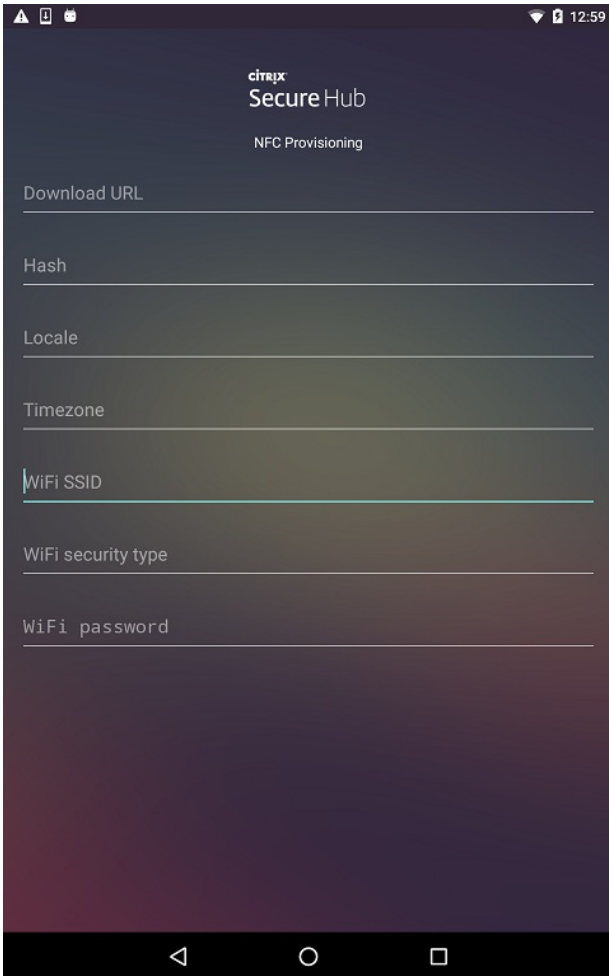
- デバイス所有者として機能するEMMプロバイダーアプリ (この場合は、Secure Hub) のパッケージ名。
- デバイスがEMMプロバイダーアプリをダウンロードできるイントラネット/インターネット上の場所。

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

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

### XenMobile Provisioning Toolの構成

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





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

#### テキストファイルを使用してProvisioning Toolを構成するには

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

テキストファイルには、次のデータを含める必要があります。

#### **android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_PACKAGE\_DOWNLOAD\_LOCATION=**

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

#### **android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_PACKAGE\_CHECKSUM=**

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

#### **android.app.extra.PROVISIONING\_WIFI\_SSID=**

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

#### **android.app.extra.PROVISIONING\_WIFI\_SECURITY\_TYPE=**

サポートされる値は、WEPおよびWPA2です。Wi-Fiが保護されていない場合、このフィールドは空白にする必要があります。

#### **android.app.extra.PROVISIONING\_WIFI\_PASSWORD=**

Wi-Fiが保護されていない場合、このフィールドを空白にする必要があります。

#### **android.app.extra.PROVISIONING\_LOCALE=**

言語コードおよび国コードを入力します。言語コードは、ISO 639-1で定義されている小文字で2文字のISO言語コード（「en」など）です。国コードは、ISO 3166-1で定義されている大文字で2文字のISO国コード（「US」など）です。たとえば、アメリカ合衆国で話されている英語の場合は「en\_US」と入力します。コードを入力しない場合、国と言語は自動的に入力されます。

#### **android.app.extra.PROVISIONING\_TIME\_ZONE=**

これはデバイスが実行されているタイムゾーンです。フォームの地域/場所のOlson名を入力します。たとえば、米国太平洋標準時の場合は「America/Los\_Angeles」です。名前を入力しない場合、タイムゾーンは自動的に入力されます。

#### **android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_PACKAGE\_NAME=**

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

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

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmf dj72LGRFkke4CrbAk\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
android.app.extra.PROVISIONING_LOCALE=en_US
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

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

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmf dj72LGRFkke4CrbAk\u003d
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
android.app.extra.PROVISIONING_LOCALE=en_US
```

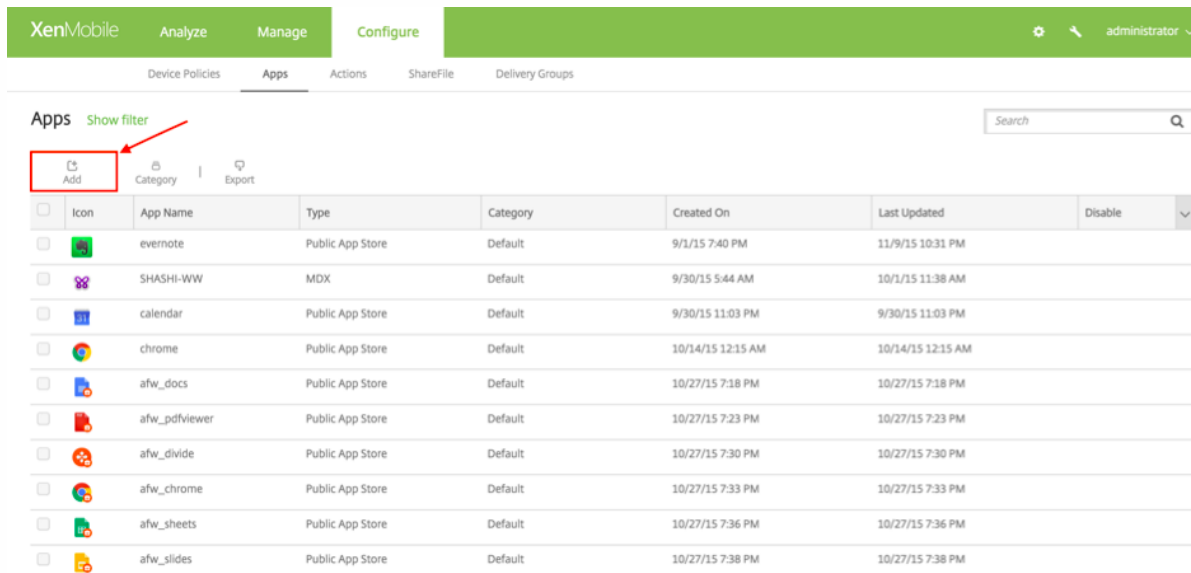
android.app.extra.PROVISIONING\_TIME\_ZONE=America/Los\_Angeles

Secure Hubチェックサムを取得するには

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

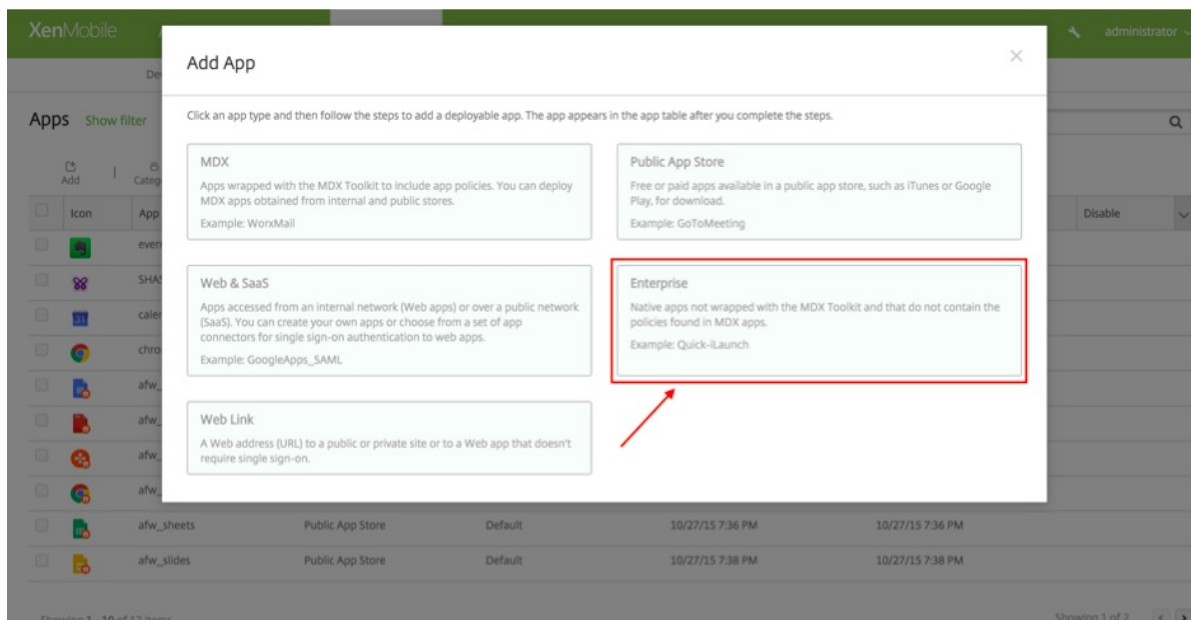
1. XenMobileコンソールで、[Configure] > [Apps] > [Add] の順にクリックします。

[Add App] ウィンドウが開きます。



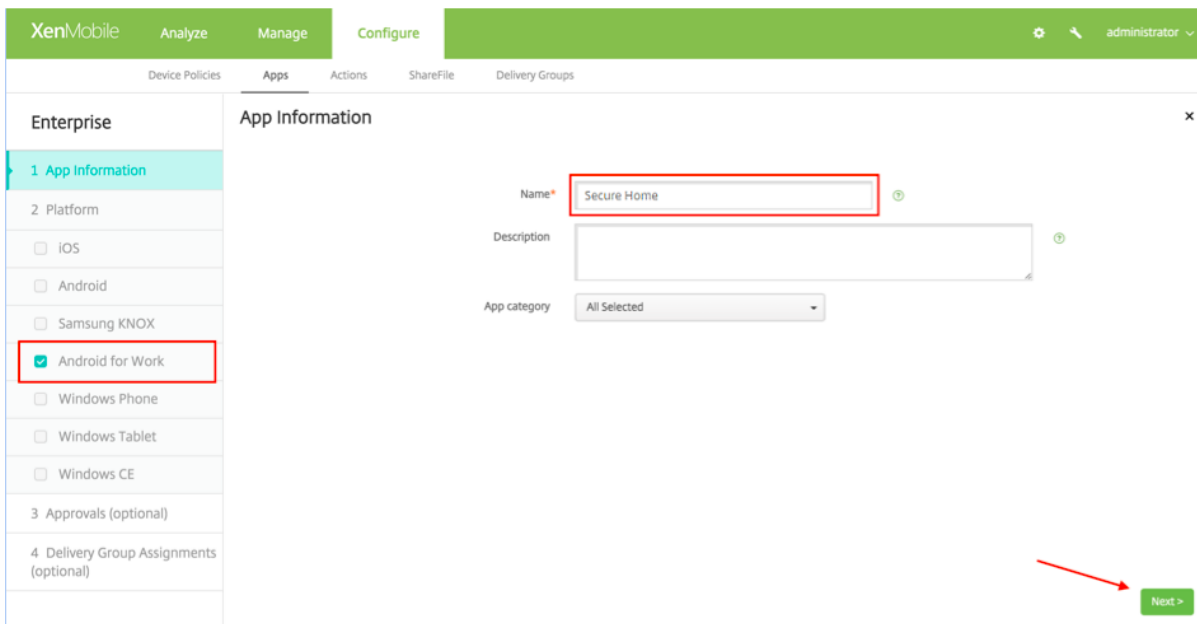
2. [Enterprise] をクリックします。

[App Information] ページが開きます。

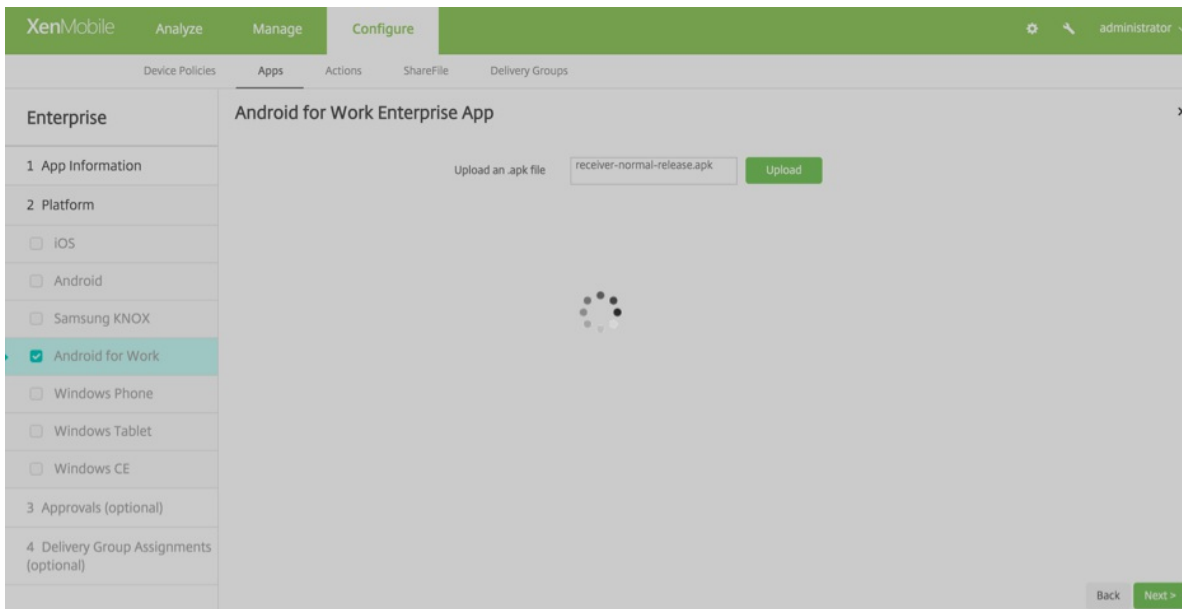


3. 次の構成を選択して [次へ] をクリックします。

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



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



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



- /記号はすべて\_に変換します。
- 末尾の\u003dは=に置き換えます。

ハッシュをデバイスのSDカードのnfcprovisioning.txtファイルに格納すると、安全のための変換が行われます。ただし、ハッシュを手動で入力すると、URIの安全性は入力者の責任になります。

#### 使用するライブラリ

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

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

# iOSデバイスバルク登録

Apr 27, 2017

次の2つの方法で多数のiOSデバイスをXenMobileに追加できます。

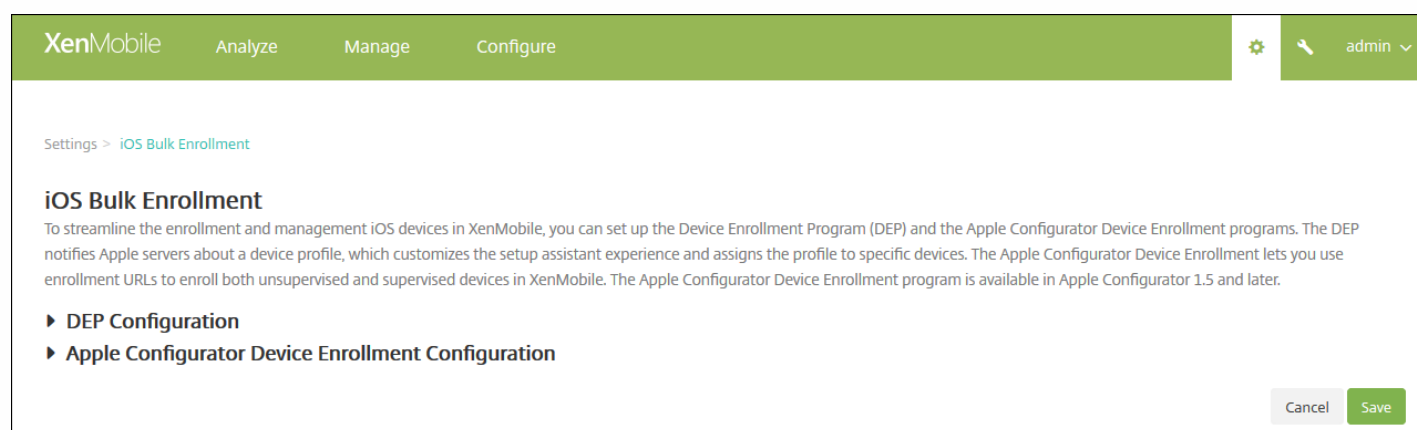
- AppleのDevice Enrollment Program (DEP) を使用して、Appleまたはプログラムに参加しているApple正規販売店または通信事業者から直接購入したデバイスを登録することができます。
- Appleから直接購入したかどうかにかかわらず、Apple Configuratorを使用してデバイスを登録できます。

XenMobile 10.xは、Apple Configurator v2をサポートします。

DEPでは、実物のデバイスを直に設定つまり準備する必要はありません。DEP経由でデバイスのシリアル番号を送信するか、発注番号を購入します。次に、XenMobileでデバイスを構成するか登録します。デバイスの登録後、構成内容をユーザーに提供するためユーザー側の構成は必要ありません。また、DEPでデバイスをセットアップすると、セットアップアシスタントの手順を省略できます。これによって、最初にデバイスを起動したときにユーザーが完了する必要があるタスクを省略します。DEPのセットアップについて詳しくは、Appleの[Device Enrollment Program](#)ページを参照してください。

Apple Configuratorの場合は、OS X 10.7.2以降およびApple Configuratorアプリが動作するAppleコンピューターにデバイスを接続します。Apple Configuratorでデバイスを準備してポリシーを構成します。必要なポリシーでデバイスをプロビジョニングした後で、デバイスをXenMobileに接続すると、ポリシーが適用されデバイスの管理を開始できます。Apple Configuratorの使用について詳しくは、[Apple Configurator](#)ページを参照してください。

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



DEP設定を構成するには、以下を参照してください。DEP設定を構成する場合は以下を参照してください。Apple Configurator設定を構成する場合は、「[Apple Configurator設定の構成](#)」を参照してください。

**前提条件：** 続行する前に、[deploy.apple.com](https://deploy.apple.com)でApple DEPアカウントを作成しておく必要があります。DEPアカウントの作成後、仮想MDMサーバーをセットアップしてXenMobileとAppleの通信を許可します。これを実行するには、XenMobile公開キーをAppleにアップロードする必要があります。Appleが公開キーを受信したら、XenMobileにインポートするサーバートークンが返されます。

次の手順に従って、XenMobileとApple間での通信を確立します。

1. 公開キーを取得してAppleにアップロードするには、[iOS Bulk Enrollment] ページで、[DEP Configuration] を展開し、[Export Public Key] をクリックしてファイルをコンピューターに保存します。
2. [deploy.apple.com](https://deploy.apple.com)にアクセスして、DEPアカウントにログインし、MDMサーバーのセットアップ手順に従います。この処理の一部として、Appleによりサーバートークンが提供されます。
3. [iOS Bulk Enrollment] ページで [Import Token File] をクリックして、AppleサーバートークンをXenMobileに追加します。
4. トークンファイルがXenMobileにアップロードされると、[Server tokens] フィールドに値が自動的に入ります。
5. [Test Connectivity] をクリックして、XenMobileと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は、「[ポート要件](#)」を参照してください。

XenMobile Analyze Manage Configure admin

Settings > iOS Bulk Enrollment

### iOS Bulk Enrollment

To streamline the enrollment and management iOS devices in XenMobile, you can set up the Device Enrollment Program (DEP) and the Apple Configurator Device Enrollment programs. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. The Apple Configurator Device Enrollment lets you use enrollment URLs to enroll both unsupervised and supervised devices in XenMobile. The Apple Configurator Device Enrollment program is available in Apple Configurator 1.5 and later.

#### DEP Configuration

Export Public Key | Import Token File

Allow Device Enrollment Program (DEP)  NO

#### Server Tokens

Consumer key\*

Consumer secret\*

Access token\*

Access secret\*

Access token expiration

#### Organization Info

Business unit\*

Unique service ID

Support phone number\*

Support email address

Enrollment Settings

Require device enrollment  ⓘ

Supervised mode  YES ⓘ

Enrollment profile removal  Allow ⓘ  
 Deny

Pairing  Allow ⓘ  
 Deny

Require credentials for device enrollment  ⓘ

Wait for configuration to complete setup  ⓘ

Setup Assistant Options

Do not set up  Location Services  
 Touch ID (iOS 8.0+)  
 Passcode Lock  
 Set Up as New or Restore  
 Move from Android (iOS 9.0+)  
 Apple ID  
 Terms and Conditions  
 Apple Pay (iOS 8.0+)  
 Siri  
 App Analytics  
 Display Zoom (iOS 8.0+)

▶ Apple Configurator Device Enrollment Configuration

Cancel Save

6. 次の設定を構成してDEP構成を完了します。

### 組織情報

- **Business unit** : デバイスを割り当てる事業単位または部門を入力します。このフィールドは必須です。
- **Unique service ID** : 任意で、一意のIDを入力します。
- **Support phone number** : ユーザーがセットアップ時にサポートが必要となった場合に連絡するサポートの電話番号を入力します。このフィールドは必須です。
- **Support email address** : 任意で、サポートのメールアドレスを入力します。

### 登録設定

- **Require device enrollment** : ユーザーにデバイス登録を要求するかどうかを選択します。デフォルトでは登録が必要です。
- **Supervised mode** : DEPで登録したデバイスをApple Configuratorで管理する場合、または [Wait for configuration to complete setup] が有効な場合は、 [Yes] に設定する必要があります。デフォルトは [Yes] です。iOSデバイスをSupervisedモードにする方法については、このトピックで後述されている「[Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには](#)」を参照してください。
- **Enrollment profile removal** : リモートから削除できるプロファイルをデバイスで使用することを許可するかどうかを選択します。デフォルトは [Deny] です。
- **Pairing** : DEPで登録したデバイスをiTunesおよびApple Configuratorで管理することを許可するかどうかを選択します。デフォルトは [Deny] です。
- **Require credentials for device enrollment** : DEPのセットアップ時にユーザーに資格情報の入力を要求するかどうかを選択します。これはiOS 7.1以降で使用できます。注：初回のセットアップでDEPを有効にしており、このオプションをオンにしない場合、DEPユーザー、Secure Hub、ソフトウェアインベントリ、DEP展開グループなどのDEPコンポーネント



が最初から作成されます。このオプションをオンにした場合は、ユーザーが資格情報を入力するまでコンポーネントは作成されません。そのため、後でこのオプションをオフにしても、これらのDEPコンポーネントは存在しないため、資格情報を入力していないユーザーはDEP登録を実行できません。その場合、DEPコンポーネントを追加するには、DEPアカウントを無効化してもう一度有効化する必要があります。

- **Wait for configuration to complete setup** : すべてのMDMリソースがユーザーのデバイスに展開されるまで、デバイスをSetup Assistantモードのままにしておく必要があるかどうかを選択します。これはiOS 9.0以降のSupervisedモードのデバイスでのみ使用できます。
  - 注 : Appleのドキュメントには、デバイスがSetup Assistantモードの間は以下のコマンドが機能しない場合があると述べられています。
    - InviteToProgram
    - InstallApplication
    - ApplyRedemptionCode
    - InstallMedia
    - RequestMirroring
    - DeviceLock

## セットアップ

ユーザーが初めてデバイスを起動して使用するときに実行する必要がないiOS設定アシスタントの手順（すなわち、スキップできる手順）を選択します。

- **Location Services** : デバイスに位置情報サービスを設定します。
- **Touch ID** : iOS 8.0以降のデバイスにTouch IDを設定します。
- **Passcode Lock** : デバイスのパスコードを作成します。
- **Set up as New or Restore** : 新規に、またはiCloudかiTunesのバックアップからデバイスを設定します。
- **Move from Android** : AndroidデバイスからiOS 9以降のデバイスへのデータ転送を有効にします。このオプションは、[Set up as New] または [Restore] がオンの場合（すなわち、手順をスキップする場合）にのみ使用できます。
- **Apple ID** : デバイスのApple IDアカウントを設定します。
- **Terms and Conditions** : デバイスの使用契約条件に対する同意をユーザーに要求します。
- **Apple Pay** : iOS 8.0以降のデバイスにApple Payを設定します。
- **Siri** : デバイスでSiriを使用するかどうかを選択します。
- **App Analytics** : クラッシュデータおよび使用状況の統計情報をAppleと共有するかどうかを設定します。
- **Display Zoom** : iOS 8.0以降のデバイスにディスプレイ解像度（標準またはズーム）を設定します。

XenMobile Analyze Manage Configure admin

Settings > iOS Bulk Enrollment

### iOS Bulk Enrollment

To streamline the enrollment and management iOS devices in XenMobile, you can set up the Device Enrollment Program (DEP) and the Apple Configurator Device Enrollment programs. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. The Apple Configurator Device Enrollment lets you use enrollment URLs to enroll both unsupervised and supervised devices in XenMobile. The Apple Configurator Device Enrollment program is available in Apple Configurator 1.5 and later.

▶ DEP Configuration

▼ Apple Configurator Device Enrollment Configuration

Export Anchor Certificates

Allow Apple Configurator Device Enrollment  NO

XenMobile URL to copy in Apple Configurator `https://mb187.agsag.com:8443/zdm/ios/otae/dobulkenrollment`

Require device registration  ⓘ

Require credentials for device enrollment  ⓘ

Cancel Save

1. [Apple Configurator Device Enrollment Configuration] を展開します。

2. [Enable Apple Configurator Device Enrollment] を [Yes] に設定します。

3. 以下の設定を確認して構成します。

- **MDM server URL to copy in Apple Configurator** : この読み取り専用のフィールドはAppleと通信するXenMobileサーバーのURLです。このURLをコピーして、後の手順でApple Configuratorに貼り付けます。Apple Configurator 2の場合、登録URLは、XenMobileサーバーの完全修飾ドメイン名 (FQDN) またはIPアドレスです (例 : mdm.server.url.com) 。
- **Require device registration** : この設定を選択する場合は、デバイスを登録する前に、構成済みのデバイスをXenMobileの [Devices] タブに手動でまたはCSVファイルを介して追加する必要があります。これにより、未知のデバイスの登録を防ぎます。デフォルトでは、デバイスの追加が必要です。
- **Require credentials for device enrollment** : iOS 7.1以降のデバイスに対して、登録時に資格情報の入力を要求します。デフォルトでは資格情報は不要です。

## 注意

XenMobileサーバーで信頼済みのSSL証明書を使用する場合は、次の手順をスキップします。

4. [Export Anchor Certs] をクリックしてcertchain.pemファイルをOS Xキーチェーン (ログインまたはシステム) に保存します。

5. Apple Configuratorを開始して [Prepare] > [Setup] > [Configure Settings] の順に選択します。

6. Configuratorの [Device Enrollment] 設定の [MDM server URL] フィールドに、手順4のMDMサーバーURLを貼り付けます。

7. XenMobileで信頼済みのSSL証明書を使用しない場合は、[Device Enrollment] 設定の [Anchor] 証明書にルート証明

書およびSSLサーバー証明書をコピーします。

8. DockコネクタUSBケーブルを使用して、最大で30台のデバイスを同時にApple Configuratorが動作するMacに接続して構成します。Dockコネクタがない場合は、1台または複数のPowered USB 2.0高速ハブを使用してデバイスを接続します。
9. **[Prepare]** をクリックします。Apple Configuratorを使用したデバイスの準備について詳しくは、Apple Configuratorのヘルプページ「[デバイスを準備する](#)」を参照してください。
10. Apple Configuratorで必要なデバイスポリシーを構成します。
11. 準備ができたデバイスから電源を入れてiOS設定アシスタントを開始し、初回使用のためにデバイスを準備します。

XenMobile Secure Sockets Layer (SSL) 証明書が更新されたら、XenMobileコンソールで **[Settings] > [Certificates]** の順に選択し、新しい証明書をアップロードします。 **[Import]** ダイアログボックスの **[Use as]** で、 **[SSL Listener]** をクリックして証明書がSSLに使用されるようにします。サーバーを再起動すると、新しいSSL証明書が使用されるようになります。XenMobileの証明書について詳しくは、「[XenMobileでの証明書のアップロード](#)」を参照してください。

SSL証明書を更新するときに、Apple DEPとXenMobileの間の信頼関係を再構築する必要はありません。ただし、この記事の」記の手順に従って、いつでもDEP設定を再構成できます。

Apple DEPについて詳しくは、[Appleのドキュメント](#)を参照してください。

この設定に関する既知の問題および解決方法について詳しくは、「[XenMobile Server 10.4の既知の問題](#)」を参照してください。

## Important

デバイスをSupervisedモードにすると、特定のバージョンのiOSがデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリケーションがデバイスから完全に消去されます。

1. iTunesから[Apple Configurator](#)をインストールします。
2. iOSデバイスをAppleコンピューターに接続します。
3. Apple Configuratorを起動します。監視の準備が整っているデバイスがあることがConfiguratorに表示されます。
4. デバイスの監視の準備を行うには：
  - a. **[監視]** コントロールを **[オン]** に切り替えます。構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。
  - b. 必要に応じてデバイスの名前を指定します。
  - c. 最新バージョンのiOSをインストールする場合、 **[iOS]** ボックスの一覧で **[最新]** を選択します。
5. デバイスの監視の準備が整ったら、 **[Prepare]** をクリックします。

# Apple DEPを介したiOSデバイスの展開

Apr 27, 2017

XenMobileでApple DEP for iOSデバイス登録および管理を利用できるようにするには、Apple Developer Enterprise Program (DEP) アカウントが必要です。Apple DEPへサインアップするために組織で必要となるのは主に次のものです。

- 会社または機関の電話番号とメールアドレス
- 検証の連絡先
- 会社または機関の情報 (D-U-N-S/税金ID)
- Appleカスタマー番号




Apple DEPについて詳しくは、Apple社のこのPDFファイルを参照してください。Apple DEPは個人ではなく法人向けのものであることに留意する必要があります。またApple DEPアカウントを作成するため、相当量の会社の詳細および情報について提供の必要があることを認識しておく必要もあります。これはつまり、カスタマーがアカウントを要求してその承認を受信するまでに、時間がかかることがあるということです。

DEPアカウントを申し込む場合、ベストプラクティスはdep@company.comなど組織に紐づけされたメールアドレスを使うことです。

Apple Deployment Programs ?

## Welcome

Enroll your organization in one of the following:

	<b>Device Enrollment Program</b> Streamline the on boarding of institutionally owned devices. Enroll devices in MDM during activation and skip basic setup steps to get users up and running quickly.	<a href="#">Enroll</a>
	<b>Volume Purchase Program</b> Easily find, buy, and distribute content to users. Users enroll without sharing their Apple ID, then apps are assigned to them using an MDM solution.	<a href="#">Enroll</a>
	<b>Apple ID for Students</b> Manage student accounts and parental consent.	<a href="#">Enroll</a>

1. 組織に関する情報を入力した後、メール経由で新しいApple IDの一時パスワードを受け取ります。

- 1 Your Details
- 2 Verification Contact
- 3 Institution Details
- 4 Review

## Check Your E-mail

An e-mail has been sent to [redacted] with your Apple ID and temporary password, and the next steps to continue your enrollment.

### 1. Complete your Apple ID setup.

[Visit My Apple ID >](#)

Using the Apple ID and temporary password included in the e-mail, sign in and complete your account setup at My Apple ID.

### 2. Enable two-step verification for this account as it is required by some programs.

### 3. Continue your Deployment Programs enrollment.

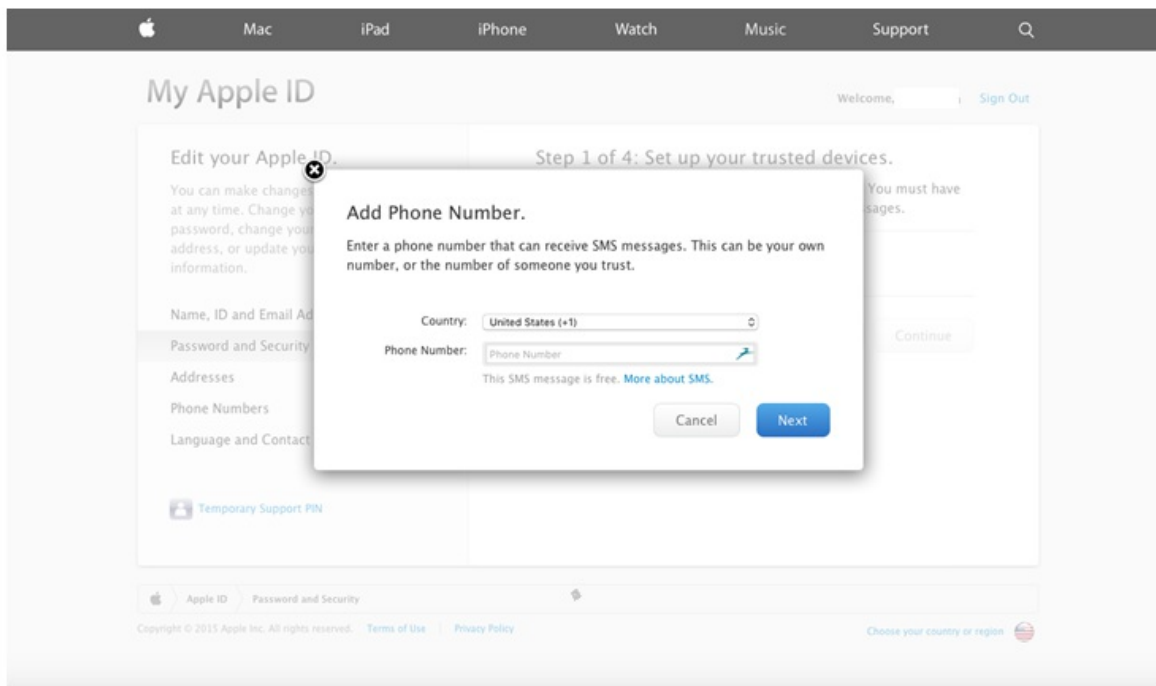
After completing the steps above, please return and continue this enrollment here at [deploy.apple.com](https://deploy.apple.com).

Resend E-mail

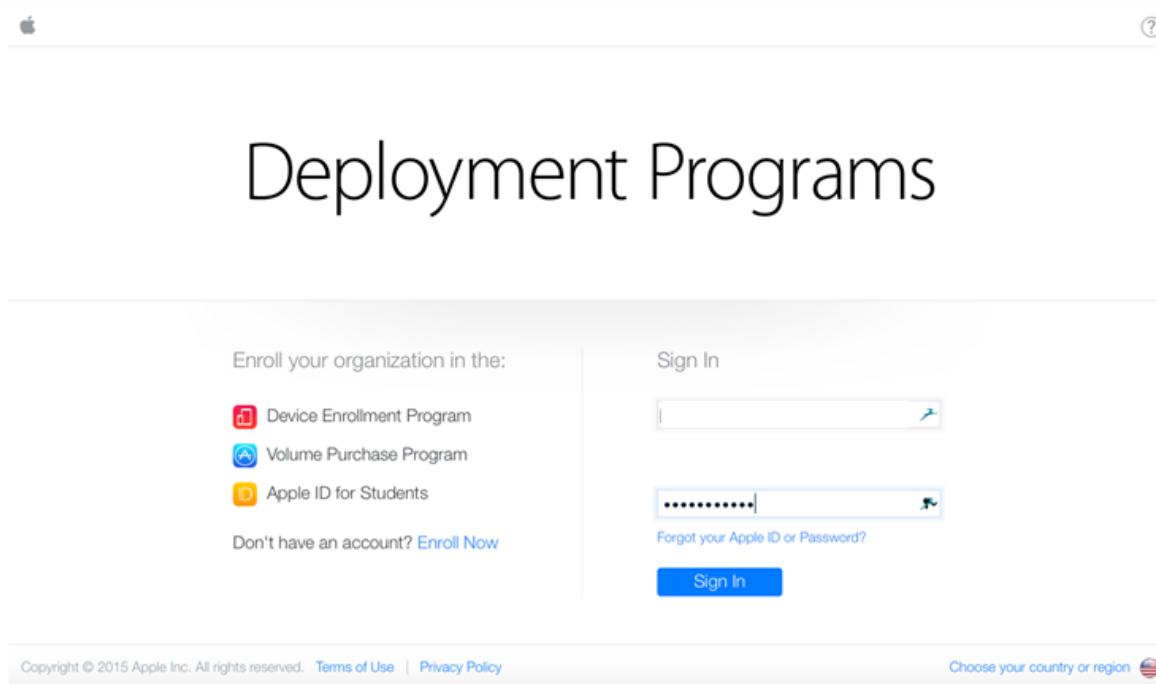
2. 次に、Apple IDでサインインしてアカウントのセキュリティ設定を完了させます。

The screenshot shows the 'My Apple ID' page with a navigation bar at the top containing 'Mac', 'iPad', 'iPhone', 'Watch', 'Music', and 'Support'. The main content is divided into two columns. The left column is titled 'Edit your Apple ID.' and contains a list of settings: 'Name, ID and Email Addresses', 'Password and Security' (which is selected), 'Addresses', 'Phone Numbers', and 'Language and Contact Preferences'. The right column is titled 'Manage your security settings.' and contains three sections: 'Two-Step Verification' with a 'Get started...' link, 'Choose a new password.' with a 'Change Password' link, and 'Security Questions.' with a dropdown menu for 'Name of your best friend?' and a text input for the answer. Below this is the 'Select your birth date.' section with dropdown menus for the month (September), day (7), and year (1973).

3. 2段階認証を構成して有効にします。これは、DEP Portalで使用するために必要です。この手順では、2段階認証用の4ケタのPINを受信する電話番号を追加します。



4. DEP Portalにログインし、セットアップしたばかりの2段階認証を使用するアカウント構成を完了させます。



5. 会社の詳細を追加して、デバイスを購入する場所を選択します。購入オプションについては、「DEP対応デバイスの注文」を参照してください。

7 ADD INSTITUTION DETAILS Need Help?

Company Name <input type="text"/>	Company D-U-N-S <span>?</span> <input type="text"/>
Address Line 1 <input type="text"/>	Address Line 2 <input type="text"/>
City <input type="text"/>	State <input type="text"/>
ZIP Code <input type="text"/>	Country <input type="text" value="USA"/>
<input type="text" value="Choose..."/> Reseller Apple Inc. (Direct) <input type="text" value="Choose..."/>	

[Add another...](#)

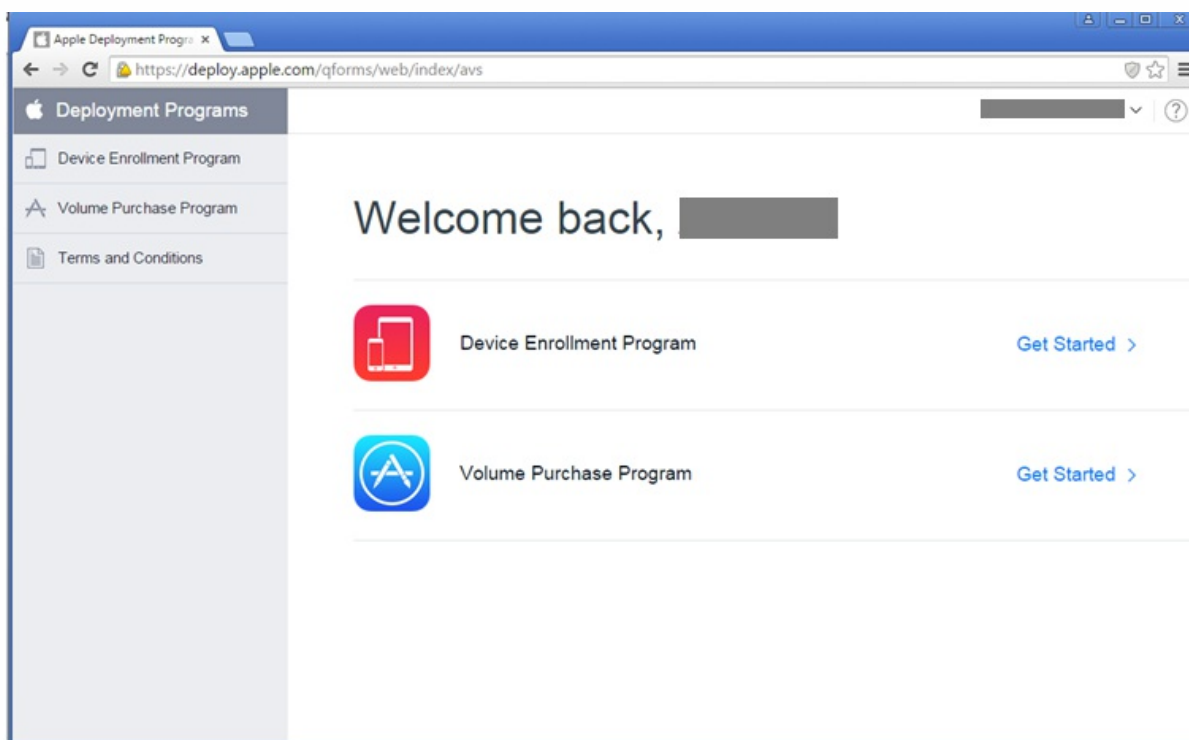
6. Apple Customer NumberまたはDEP Reseller IDを追加して、登録の詳細を認証し、Appleがアカウントを承認するのを待ちます。

7 ADD INSTITUTION DETAILS Need Help?

Company Name <input type="text"/>	Company D-U-N-S <span>?</span> <input type="text"/>
Address Line 1 <input type="text"/>	Address Line 2 <input type="text"/>
City <input type="text"/>	State <input type="text"/>
ZIP Code <input type="text"/>	Country <input type="text" value="USA"/>
Web Site <input type="text"/>	
Devices Purchased From <input type="text" value="Reseller"/>	DEP Reseller ID <span>?</span> <input type="text"/>

[Add another...](#)

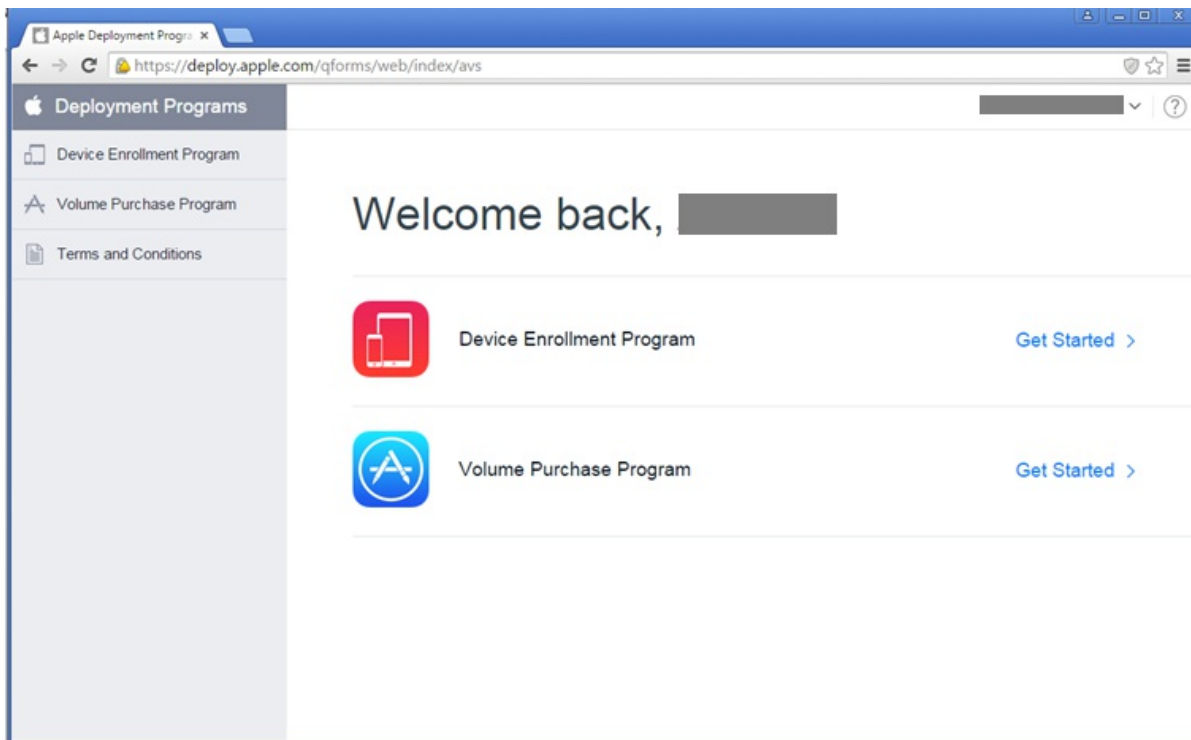
7. Appleからログオン資格情報を受け取ったら、Apple DEP Portalにログインします。その後で、次のセクションに示す手順に従ってXenMobileでアカウントに接続します。



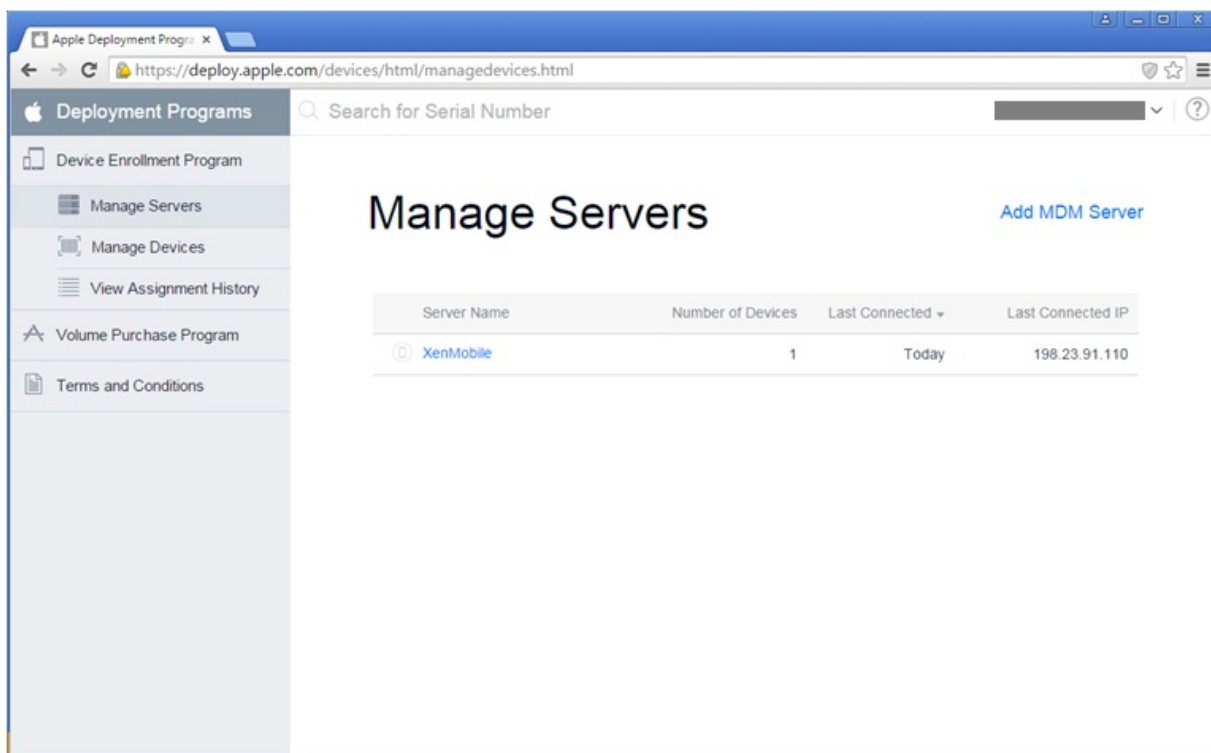
このセクションで示す手順に従い、XenMobileサーバー展開でApple DEPアカウントに接続します。

1. Apple DEP Portalの左側にある [Device Enrollment Program] をクリックします。

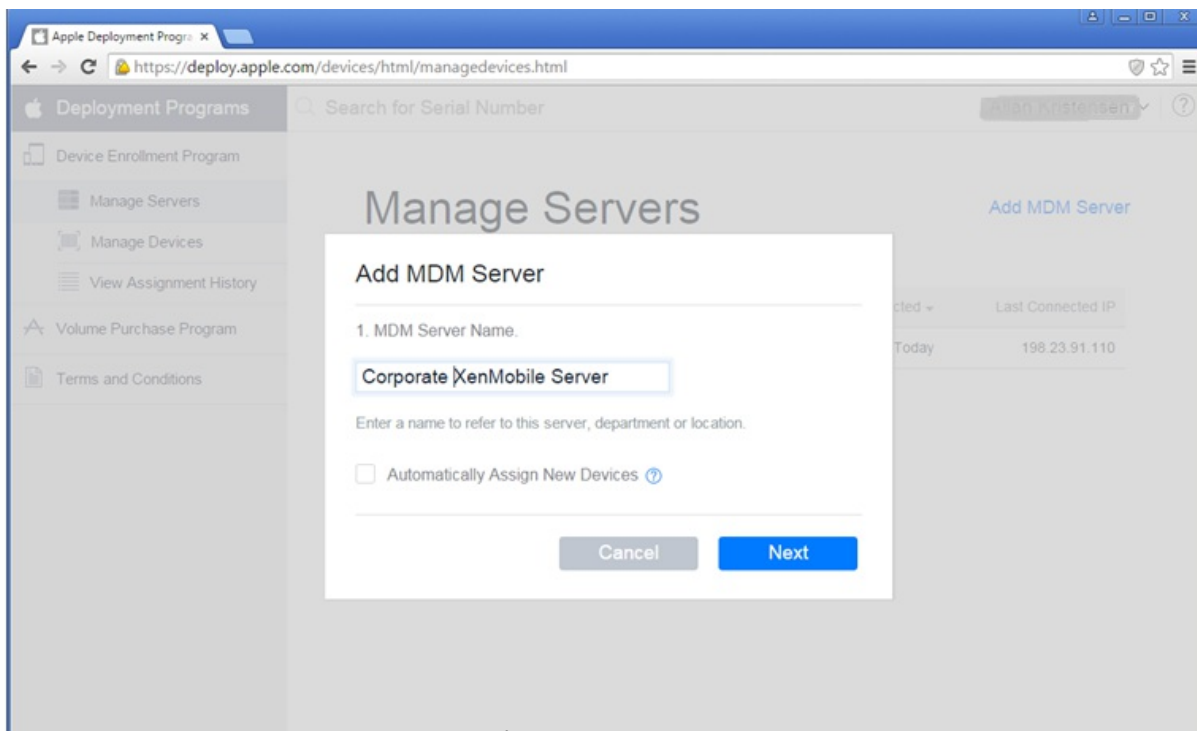




2. [Manage Servers] をクリックし、右側にある [Add MDM Server] をクリックします。



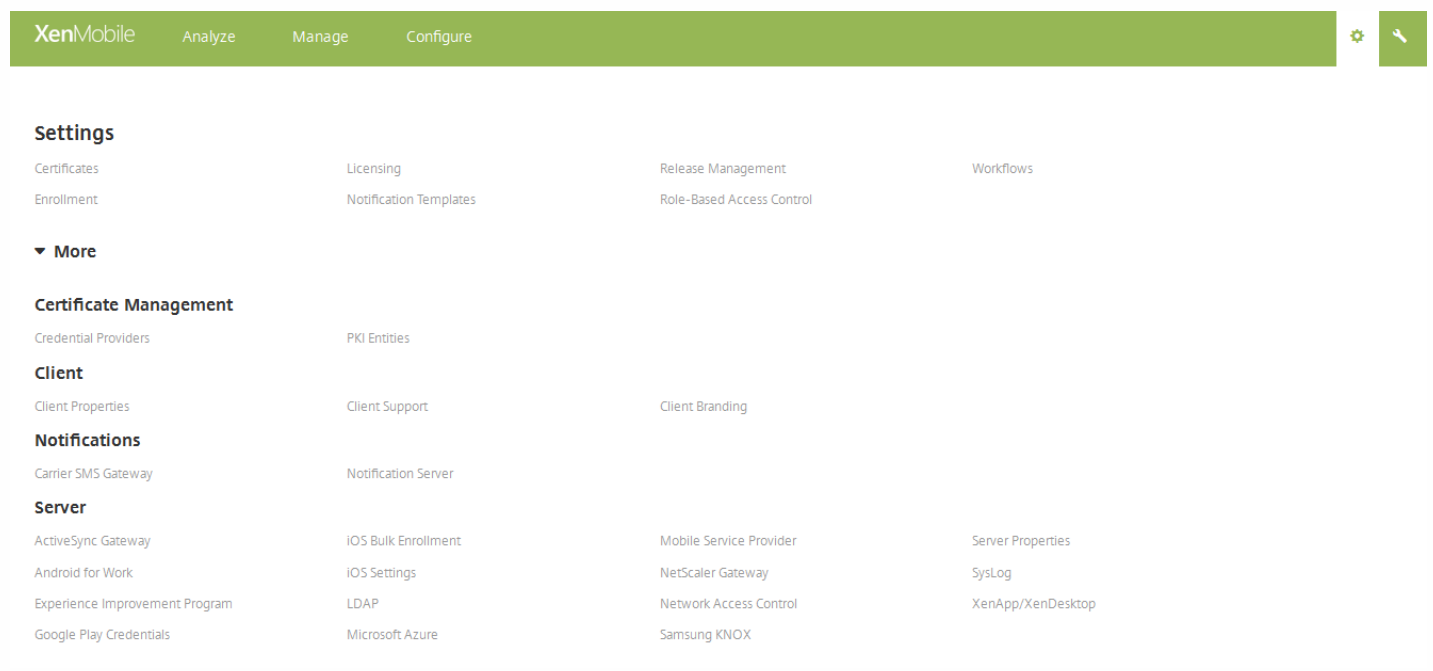
3. [Add MDM Server] にXenMobileサーバーの名前を入力し、[Next] をクリックします。



4. XenMobileサーバーから公開キーをアップロードします。XenMobileからキーを生成するには、次のようにします。

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

[More] で [iOS Bulk Enrollment] をクリックします。



[iOS Bulk Enrollment] ページで [DEP Configuration] を展開してから、 [Export Public Key] をクリックします。公開キーがダウンロードされます。

Settings > iOS Bulk Enrollment

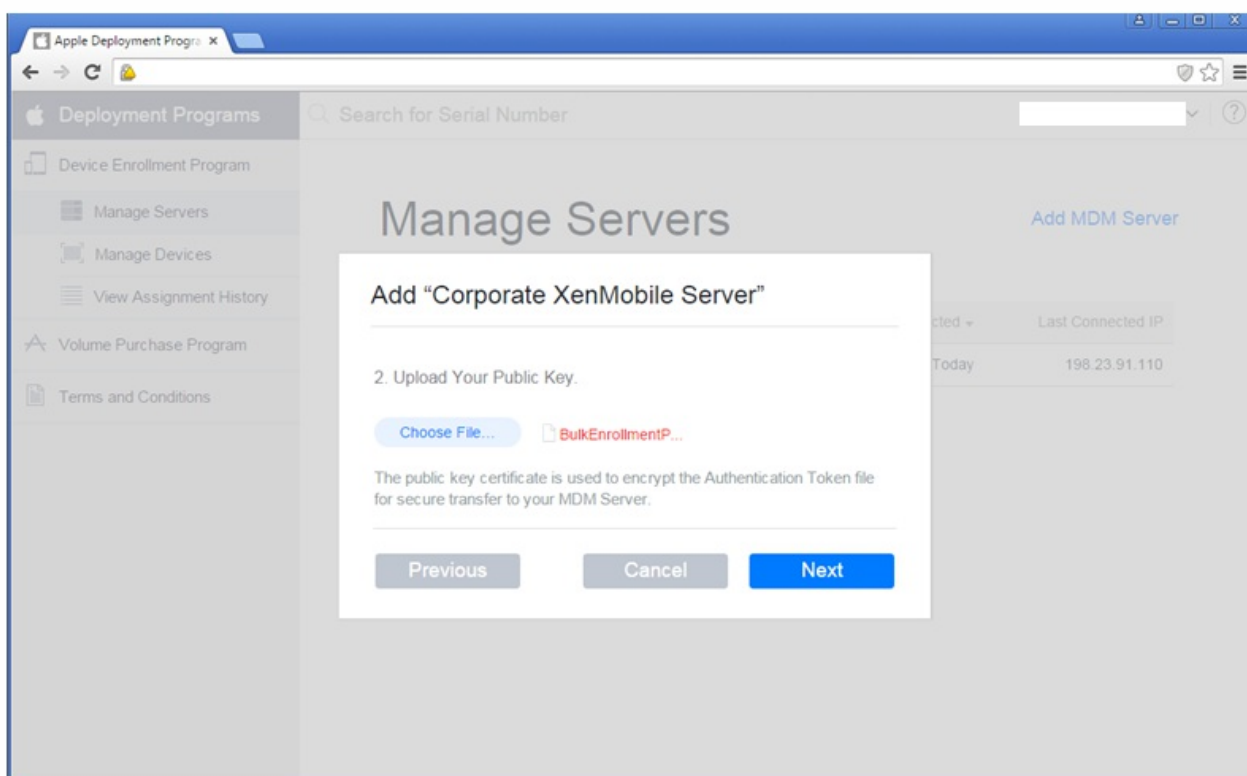
## iOS Bulk Enrollment

To streamline the enrollment and management of iOS devices in XenMobile, you can set up the Device Enrollment Program (DEP) and the Apple Configurator Device Enrollment programs. The DEP notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. The Apple Configurator Device Enrollment lets you use enrollment URLs to enroll both unsupervised and supervised devices in XenMobile. The Apple Configurator Device Enrollment program is available in Apple Configurator 1.5 and later.

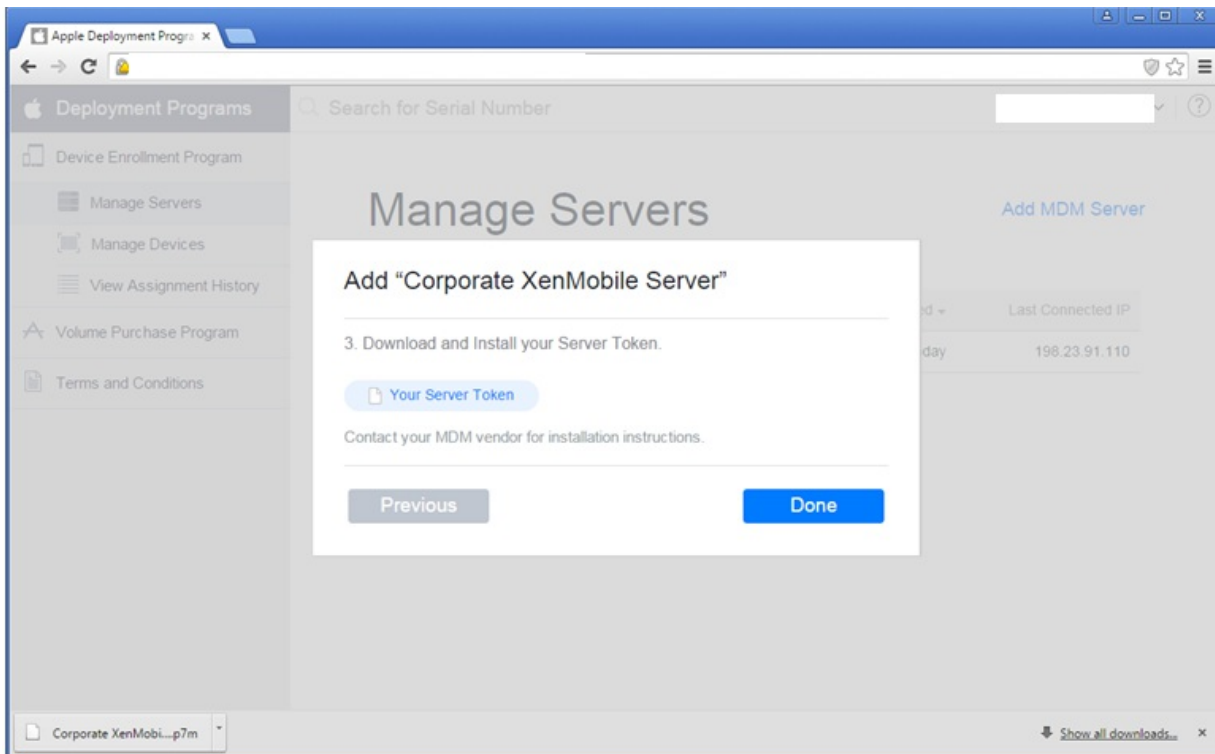
### ▼ DEP Configuration

Export Public Key | Import Token File

5. Apple DEP Portalで、**[Choose file]** をクリックしてダウンロードしたばかりの公開キーを選択し、次に**[Next]** をクリックします。



6. **[Your Server Token]** をクリックして、ブラウザからダウンロードされるサーバートークンを生成し、**[Done]** をクリックします。



7. XenMobileコンソールの [Allow Device Enrollment Program (DEP)] の隣の [iOS Bulk Enrollment] ページで、[YES] をクリックし、[Import Token File] をクリックして前の手順でダウンロードしたトークンファイルをアップロードします。

#### ▼ DEP Configuration

Export Public Key | Import Token File

Allow Device Enrollment Program (DEP)  YES

#### Import Token File ×

Choose the token file downloaded from the Device Enrollment Program web portal and click Import.

Token File\*

トークンファイルをインポートした後、Apple DEPトークン情報がXenMobileコンソールに表示されます。

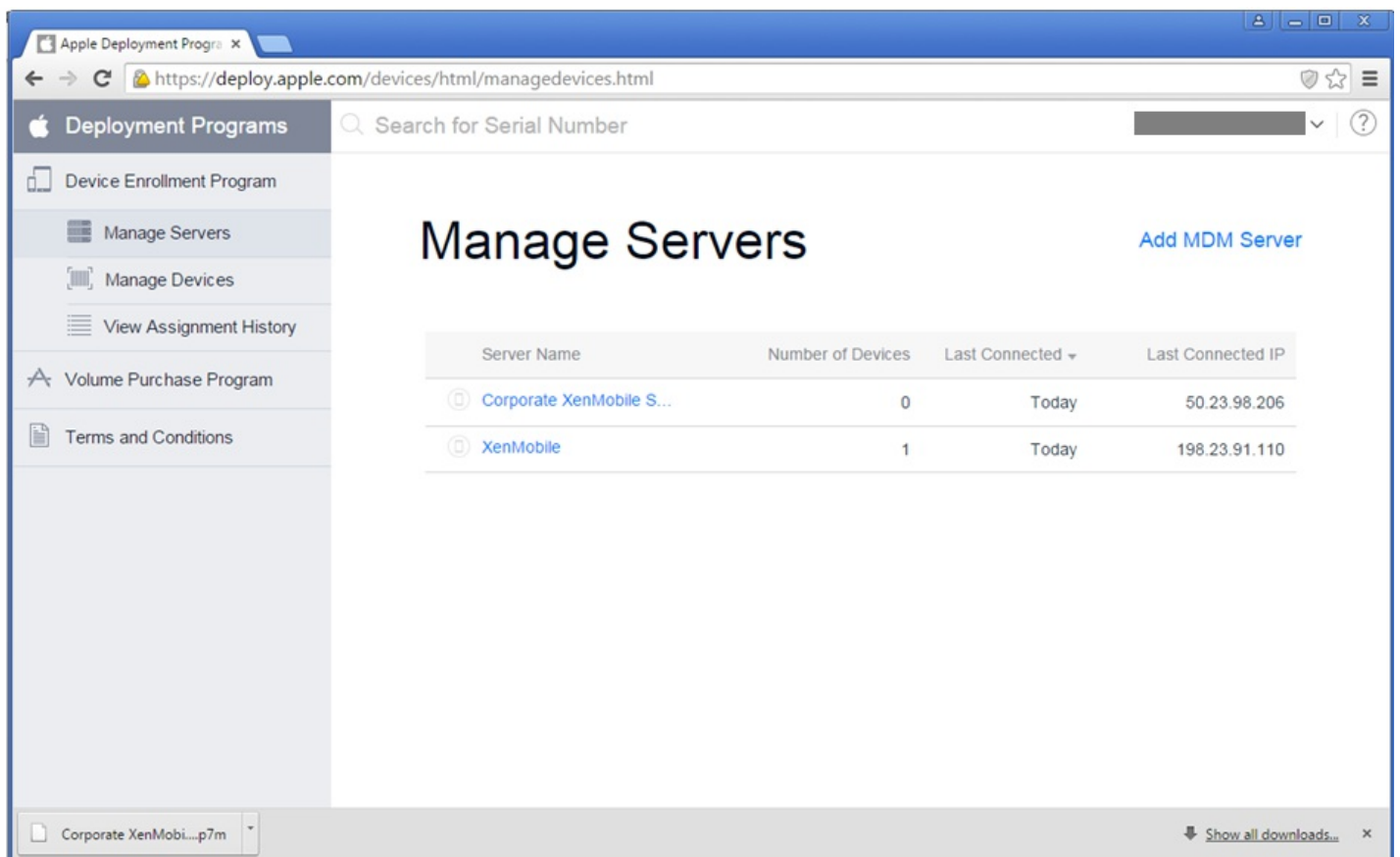
8. [Test Connection] をクリックしてApple DEP接続をXenMobileで認証します。

#### Server Tokens

Consumer key*	<input type="text"/>
Consumer secret*	<input type="text"/>
Access token*	<input type="text"/>
Access secret*	<input type="text"/>
Access token expiration	<input type="text"/>
<input type="button" value="Test Connection"/>	

9. [iOS Bulk Enrollment] ページで追加の設定を完了させて、Apple DEPデバイスに実装するApple DEPコントロールとポリシーを選択し、[Save] をクリックします。

XenMobileサーバーがApple DEP Portalに表示されます。

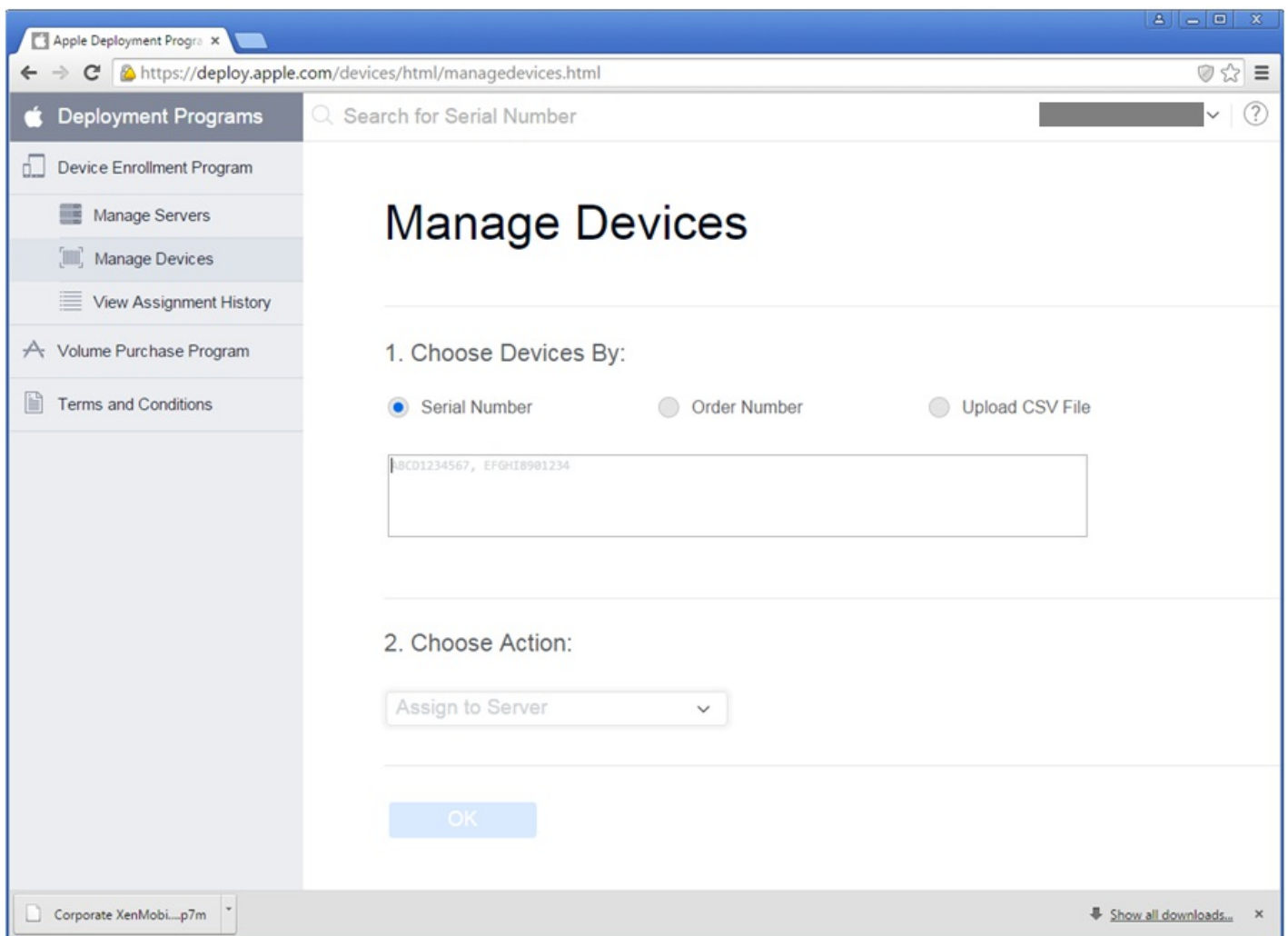


DEP対応デバイスをAppleから直接、またはDEP対応認証リセラーまたはキャリアから注文できます。Appleから注文するには、Apple DEP Portal内でApple Customer IDを提供して、AppleがApple DEPアカウントにデバイス購入を割り当てられるようにする必要があります。

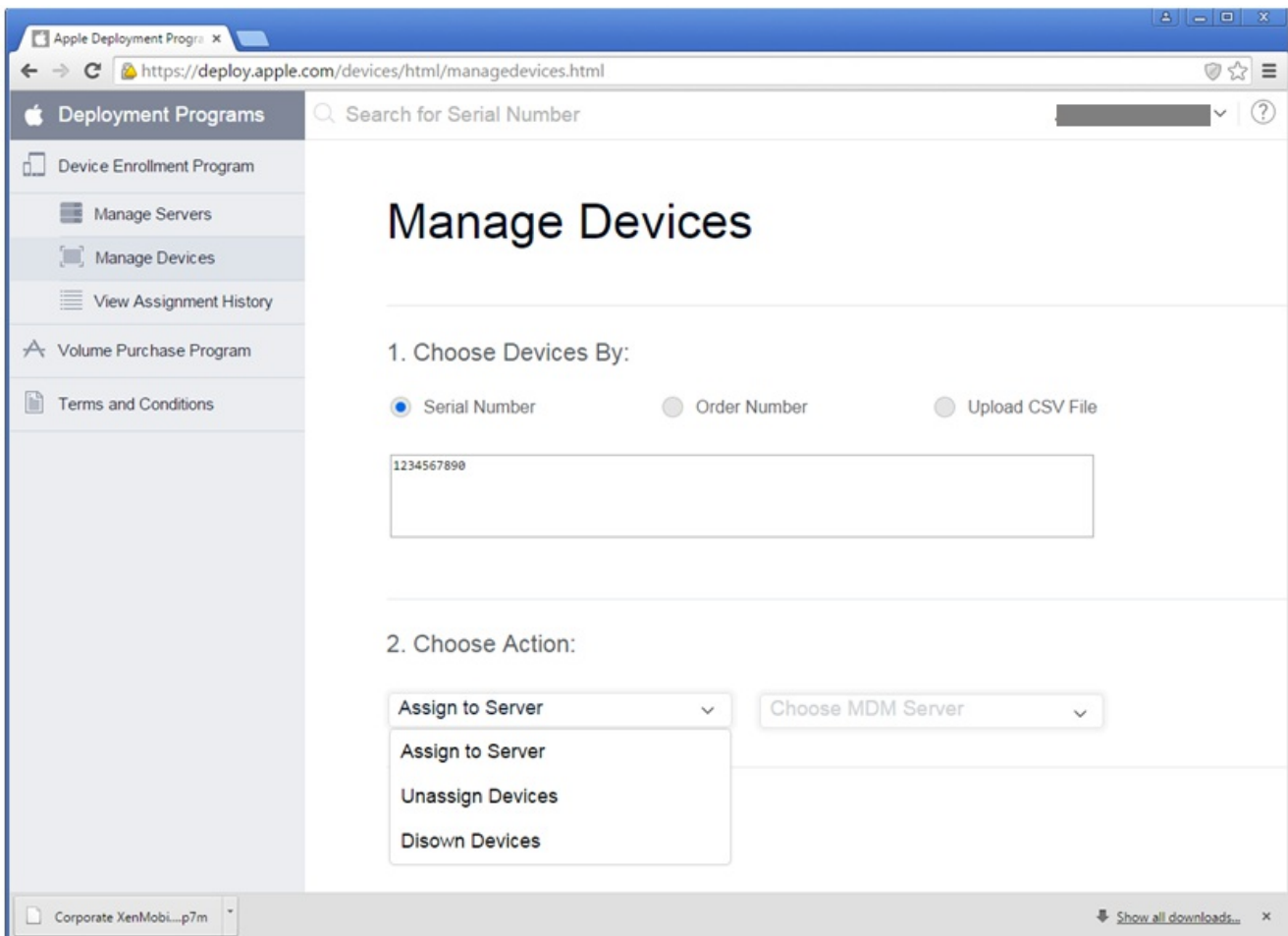
リセラーやキャリアから注文するには、AppleリセラーまたはキャリアにApple DEPに参加しているかどうかを問い合わせます。デバイスを購入する場合、リセラーのApple DEP IDが必要です。Apple DEPリセラーをApple DEPアカウントに追加するにはこの情報が必要となります。承認されたら、リセラーのApple DEP IDを追加した後にDEPカスタマーIDを受け取ります。DEPカスタマーIDをリセラーに提供します。リセラーはこのIDを使ってデバイス購入に関する情報をAppleに送信します。詳しくは、[AppleのWebサイト](#)を参照してください。

これらの手順に従って、DEP Portalを介してApple DEPアカウント内でデバイスをXenMobileサーバーに割り当てます。

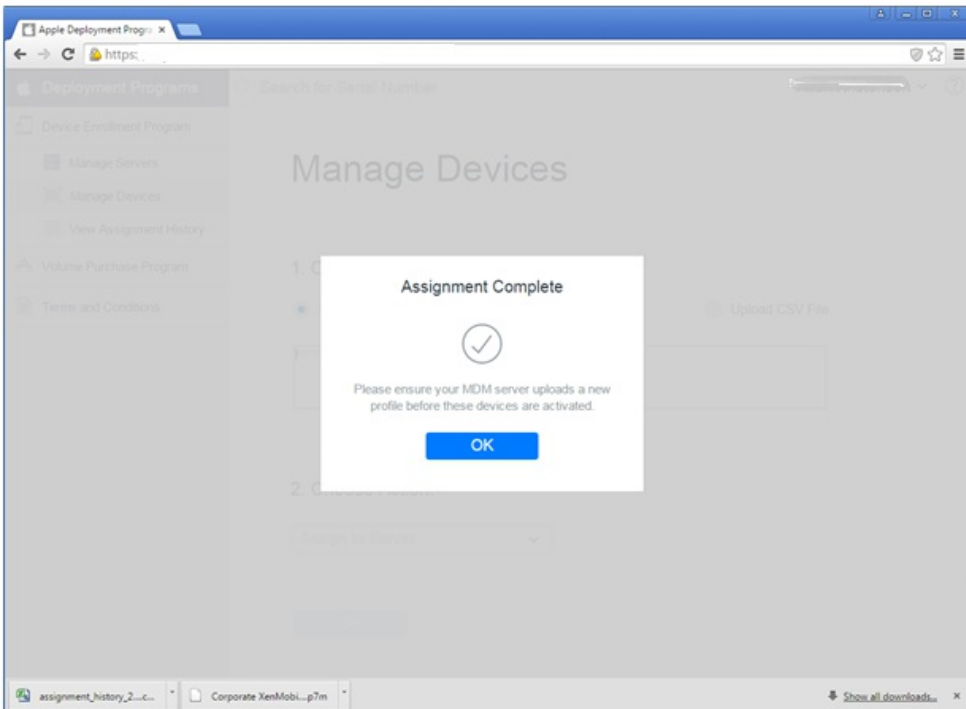
1. Apple DEP Portalにログオンします。
2. [Device Enrollment Program] をクリックして [Manage Devices] をクリックし、次に [Choose Devices By] で Apple DEP対応デバイスをアップロードして定義するためのオプションである [Serial Number]、[Order Number]、または [Upload CSV File] を選択します。



3. デバイスをXenMobileサーバーに割り当てるため、[Choose Action] で [Assign to Server] をクリックしてから一覧内でXenMobileサーバーの名前をクリックし、[OK] をクリックします。



Apple DEPデバイスが選択したXenMobileサーバーに割り当てられました。





ユーザーがApple DEP対応デバイスを登録する場合の手順は次の通りです。

1. Apple DEP対応デバイスを開始します。
2. 構成ウィザードを使ってiOSデバイスで初期設定を構成します。
3. デバイスが自動的にXenMobileデバイス登録処理を開始します。ウィザードの指示に従って、Apple DEP対応デバイスに割り当てられたXenMobileサーバー内にデバイスを登録します。

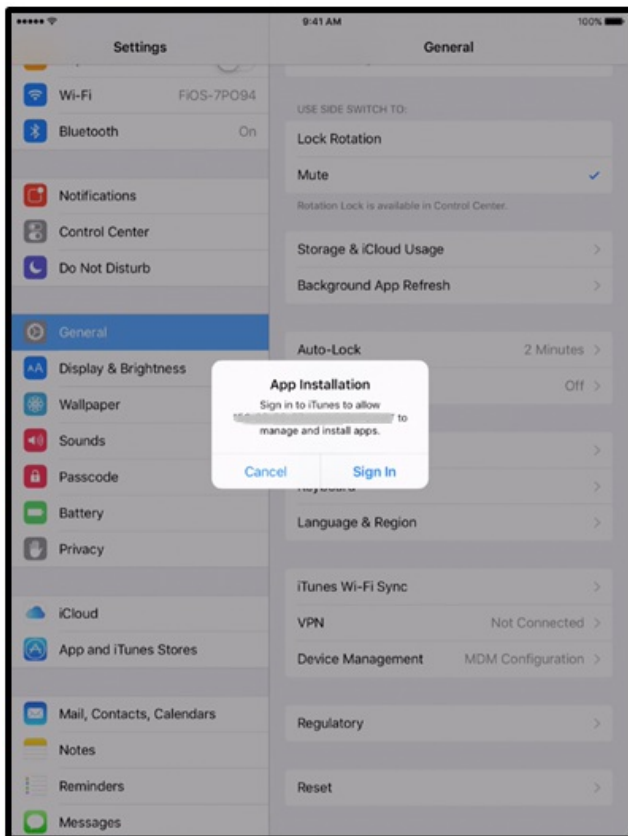
Apple DEP登録処理が、Apple DEP対応デバイスの初期iOS構成フローの一部として自動的に開始されます。



4. XenMobileコンソールで構成したApple DEP構成がApple DEP対応デバイスに配信されます。ユーザーはウィザードの指示に従って、デバイスを構成します。



5. Secure Hubをダウンロードできるように、iTunesへのサインインを求めるプロンプトが表示されることがあります。



6. Secure Hubを開いて資格情報を入力します。ポリシーにより求められる場合、Citrix PINを作成して検証するようプロンプトが表示されることがあります。

必須アプリについてのリマインダーがデバイスに表示されます。

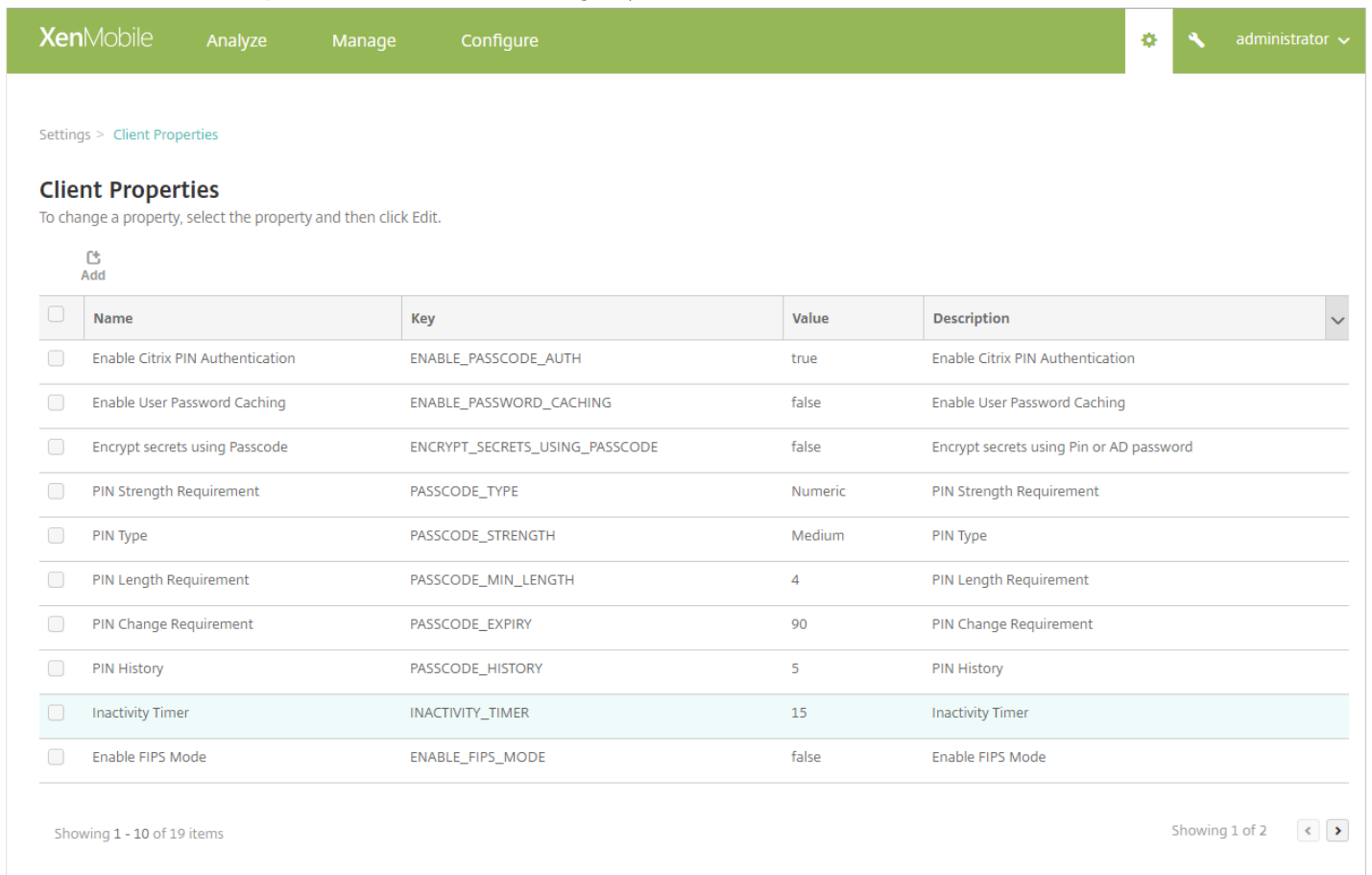
# クライアントプロパティ

Apr 27, 2017

クライアントプロパティには、ユーザーのデバイスのSecure Hubに直接提供される情報が含まれています。これらのプロパティを使用して、Citrix PINなどの詳細設定を構成することができます。クライアントプロパティはCitrixサポートから取得します。

クライアントプロパティは、クライアントアプリケーション（特にSecure Hub）のリリースごとに変更されます。一般的に構成されたクライアントプロパティについて詳しくは、「[クライアントプロパティリファレンス](#)」を参照してください。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Client] の下の [Client Properties] をクリックします [Client Properties] ページが開きます。このページでは、クライアントプロパティを追加、編集、または削除できます。



XenMobile Analyze Manage Configure administrator

Settings > Client Properties

### Client Properties

To change a property, select the property and then click Edit.

Add

<input type="checkbox"/>	Name	Key	Value	Description
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	true	Enable Citrix PIN Authentication
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	4	PIN Length Requirement
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

Showing 1 - 10 of 19 items Showing 1 of 2

1. [Add] をクリックします。[Add New Client Property] ページが開きます。

XenMobile Analyze Manage Configure admin

Settings > Client Properties > Add New Client Property

### Add New Client Property

Key  ?

Value\*

Name\*

Description\*

Cancel Save

2. 次の設定を構成します。

- **Key** : 一覧から、追加するプロパティキーを選択します。**重要** : 変更を行う前にCitrixのサポート担当者にお問い合わせるか、変更を行うための特殊キーを要求してください。
- **Value** : 選択したプロパティの値を入力します。
- **Name** : プロパティの名前を入力します。
- **Description** : プロパティの説明を入力します。

3. [Save] をクリックします。

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。

XenMobile Analyze Manage Configure administrator

Settings > Client Properties > Edit Client Property

### Edit Client Property

Key	ENABLE_PASSCODE_AUTH
Value*	true
Name*	Enable Citrix PIN Authentication
Description*	Enable Citrix PIN Authentication

3. 必要に応じて以下の情報を変更します。

- **Key** : このフィールドは変更できません。
- **Value** : プロパティの値です。
- **Name** : プロパティの名前です。
- **Description** : プロパティの説明です。

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

1. [クライアントプロパティ] 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

次に、XenMobileの定義済みクライアントプロパティとそのデフォルトの設定を示します。

### CONTAINER\_SELF\_DESTRUCT\_PERIOD

表示名 : MDX Container Self Destruct Period

非アクティブな状態で一定の日数を経過すると、自動削除機能により、Secure Hubおよび管理対象アプリケーションにアクセスできなくなります。有効期限を過ぎると、アプリケーションは使用できなくなり、XenMobileサーバーへのユーザーデバイスの登録が解除されます。データのワイプでは、各インストール済みアプリケーションのアプリケーションデータ（アプリケーションキャッシュ、ユーザーデータなど）が消去されます。非アクティブ状態とは、サーバーが一定期間、ユーザーの検証をするための認証要求を受け取っていない状態です。たとえば、このポリシーに30日を設定した場合、ユーザーがSecure Hubまたはほかのアプリケーションを30日を超えて使用しない状況が続くと、このポリシーが適用されます。

このグローバルセキュリティポリシーは、既存のアプリケーションロックポリシーおよびワイプポリシーの機能拡張であり、iOSおよびAndroidのプラットフォームに適用されます。

このグローバルポリシーを構成するには、[Settings] > [Client Properties] の順に選択し、カスタムキーCONTAINER\_SELF\_DESTRUCT\_PERIODを追加します。

値：日数

#### DEVICE\_LOGS\_TO\_IT\_HELP\_DESK

表示名：Send device logs to IT help desk

このプロパティで、ITヘルプデスクへのログ送信機能を有効または無効にします。

設定可能な値：trueまたはfalse

デフォルト値：false

#### DISABLE\_LOGGING

表示名：Disable Logging

このプロパティでは、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。Secure Hubおよびすべてのインストール済みMDXアプリのログ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。ログ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。この効果はユーザーのデバイスに対してだけでなく、Secure Hub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もできなくなります。

このプロパティをtrueに設定すると、Secure Hub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アプリのログギングが停止します。

設定可能な値：trueまたはfalse

デフォルト値：false (ログギングは有効です)

#### ENABLE\_CRASH\_REPORTING

表示名：Enable Crash Reporting

このプロパティでは、XenMobileアプリケーションのCrashlyticsを使用した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

#### ENABLE\_FIPS\_MODE

表示名：Enable FIPS Mode

このプロパティでは、モバイルデバイスでFIPSモードを有効または無効にします。値を変更すると、Secure Hubは、次のオンライン認証のときに新しい値をデバイスに送信します。

設定可能な値：trueまたはfalse

デフォルト値：false

#### ENABLE\_NETWORK\_EXTENSION

表示名 : ENABLE\_NETWORK\_EXTENSION

Secure Hubがインストールされると、XenMobileはデフォルトでApple Network Extensionフレームワークを有効にします。Network Extensionを無効にするには、[Settings] > [Client Properties] でカスタムキーENABLE\_NETWORK\_EXTENSIONを追加し、[Value] をfalseに設定します。

デフォルト値 : true

## ENABLE\_PASSCODE\_AUTH

表示名 : Enable Citrix PIN Authentication

このプロパティを使用すると、Citrix PIN機能を有効にできます。ユーザーは、Citrix PINまたはパスコードにより、Active Directoryパスワードの代わりに使用するPINを定義するように求められます。ENABLE\_PASSWORD\_CACHINGが有効になっているとき、またはXenMobileで証明書認証を使用しているときは、この設定が自動的に有効になります。

ユーザーがオフライン認証を実行している場合、Citrix PINがローカルで検証されて、要求したアプリやコンテンツへのアクセスがユーザーに許可されます。ユーザーがオンライン認証を実行している場合、Citrix 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せん。

設定可能な値 : trueまたはfalse

デフォルト値 : false

## ENABLE\_PASSWORD\_CACHING

表示名 : Enable User Password Caching

このプロパティによって、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。このプロパティをtrueに設定する場合、ENABLE\_PASSCODE\_AUTHプロパティもtrueに設定する必要があります。ユーザーパスワードのキャッシュを有効にすると、ユーザーはCitrix PINまたはパスコードを設定するよう求められます。

設定可能な値 : trueまたはfalse

デフォルト値 : false

## ENABLE\_TOUCH\_ID\_AUTH

表示名 : Enable Touch ID Authentication

Touch ID認証対応デバイスの場合、このプロパティでデバイスのTouch ID認証の有効化、無効化を設定します。要件 :

ユーザーデバイスでCitrix PINまたはLDAPを有効にする必要があります。LDAP認証がオフの場合（証明書による認証が使用されている場合など）、ユーザーはCitrix PINを設定する必要があります。この場合、ENABLE\_PASSCODE\_AUTHがfalseであっても、XenMobileにCitrix PINが必要になります。

ENABLE\_PASSCODE\_AUTHをfalseに設定します。これによって、ユーザーがアプリを起動したとき、Touch IDの使用を促すメッセージが表示されます。

設定可能な値 : trueまたはfalse

デフォルト値 : false



## ENABLE\_WORXHOME\_CEIP

表示名 : Enable Worx Home CEIP

このプロパティにより、カスタマーエクスペリエンス向上プログラムがオンになります。このプログラムにより、構成および使用データが定期的に、匿名でCitrixに送信されます。このデータは、XenMobileの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。

値 : trueまたはfalse

デフォルト値 : false

## ENABLE\_WORXHOME\_GA

表示名 : Enable Google Analytics in Worx Home

このプロパティでは、Worx HomeのGoogle Analyticsを使用したデータ収集機能を有効または無効にします。この設定を変更した場合、ユーザーが次回Secure Hub (Worx Home) にログオンすると初めて新しい値が設定されます。

設定可能な値 : trueまたはfalse

デフォルト値 : true

## ENCRYPT\_SECRETS\_USING\_PASSCODE

表示名 : Encrypt secrets using Passcode

このプロパティでは、機密データをプラットフォームベースのネイティブな格納場所 (iOSキーチェーンなど) ではなく、モバイルデバイスのSecret Vaultに格納できます。このプロパティにより、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、このプロパティを有効にすることをお勧めします。これによって、Citrix PINの認証メッセージが増えます。

設定可能な値 : trueまたはfalse

デフォルト値 : false

## INACTIVITY\_TIMER

表示名 : Inactivity Timer

このプロパティで、ユーザーがデバイスを非アクティブにした後で、Citrix PINまたはパスコードの入力を求められずにアプリにアクセスできる時間 (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Secure Hubにリダイレクトされます。この設定を変更すると、ユーザーが次回認証を求められたときに値が有効になります。

注 : iOSでは、Inactivity TimerはMDXアプリとMDX以外のアプリのSecure Hubへのアクセスにも対応します。

設定可能な値 : 正の整数

デフォルト値 : 15

## ON\_FAILURE\_USE\_EMAIL

表示名 : On failure Use Email to Send device logs to IT help desk

このプロパティで、メールを使用してITにデバイスログを送信する機能を有効または無効にします。

設定可能な値 : trueまたはfalse

デフォルト値 : true

## PASSCODE\_EXPIRY

表示名 : PIN Change Requirement

このプロパティで、Citrix PINまたはパスコードが有効な期間（日単位）を定義します。この期間を過ぎると、ユーザーはCitrix PINまたはパスコードを変更する必要があります。この設定を変更すると、ユーザーの現在のCitrix PINまたはパスコードの有効期限が切れた場合のみ、新しい値が設定されます。

設定可能な値 : 1から99までの間を推奨。ユーザーがPINをリセットする必要があるようにするためには、大きな値に設定してください（例 : 100,000,000,000）。有効期限を1から99日の間で設定し、その期間中に大きな値に変更した場合、PINは最初に設定した期間の最終日に満期になり、満期がその後に設定されることはありません。

デフォルト値 : 90

## PASSCODE\_HISTORY

表示名 : PIN History

このプロパティでは、使用済みであり、Citrix PINまたはパスコードの変更時にユーザーが再使用できないCitrix PINまたはパスコードの個数を定義します。この設定を変更すると、ユーザーがCitrix PINまたはパスコードを次回再設定したときに新しい値が設定されます。

設定可能な値 : 1から99までの間

デフォルト値 : 5

## PASSCODE\_MAX\_ATTEMPTS

表示名 : PIN Attempts

このプロパティで、完全認証が必要になる前に、ユーザーが誤ったCitrix PINまたはパスコードを入力できる回数を定義します。完全認証に成功した後で、ユーザーは新しいCitrix PINまたはパスコードを作成するように求められます。

設定可能な値 : 正の整数

デフォルト値 : 15

## PASSCODE\_MIN\_LENGTH

表示名 : PIN Length Requirement

このプロパティは、Citrix PINの最小文字数を定義します。

設定可能な値 : 1から99までの間

デフォルト値 : 6

## PASSCODE\_STRENGTH

表示名 : PIN Strength Requirement

このプロパティで、Citrix PINまたはパスコードの強度を定義します。この設定を変更すると、ユーザーは、次回認証を求められたときに、新しいCitrix PINまたはパスコードを設定するように求められます。

設定可能な値 : Low、Medium、またはStrong

デフォルト値 : Medium

次の表は、PASSCODE\_TYPE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せん。	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
Medium (デフォルト設定)	1. すべての番号を同じにはできません。たとえば、444444は使用できません。  2. すべての番号を連番にはできません。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~
高	Citrix PINのパスコード強度「Medium」と同じです。	パスコードには、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、DFGH2  使用可 : Abcd12、jkrtA2、23Bc#、AbCd
強	Citrix PINのパスコード強度「Medium」と同じです。	パスコードに1つ以上の数字、1つ以上の特殊記号、1つ以上の大文字、および1つ以上の小文字が含まれている必要があります。

使用不可 : abcd12、Abcd12、dfgh12、jkrtA2

使用可 : Abcd1#、Ab123~、xY12#3、Car12#、AAbc1#

## PASSCODE\_TYPE

表示名 : PIN Type

このプロパティで、数字のCitrix PINまたは英数字パスコードのいずれをユーザーが定義できるようにするのかを定義します。[Numeric] を選択した場合、ユーザーは数字のみを使用できます (Citrix PIN)。[Alphanumeric] を選択した場合、ユーザーは文字と数字の組み合わせを使用できます (パスコード)。

注 : この設定を変更すると、ユーザーは、次回認証を求められたときに、新しいCitrix PINまたはパスコードを設定する必要があります。

設定可能な値 : Numeric または Alphanumeric

デフォルト値 : Numeric

## REFRESHINTERVAL

表示名 : REFRESHINTERVAL

デフォルトで、XenMobileはAuto Discovery Server (ADS) のピンニングされた証明書に対して3日ごとにpingを実行します。更新間隔を変更するには、[Settings] > [Client Properties] でカスタムキーREFRESHINTERVALを追加して、[Value] を時間数に設定します。

デフォルト値 : 72時間 (3日)

## SEND\_LDAP\_ATTRIBUTES

MAM-only展開の場合、XenMobileを、AndroidまたはiOSデバイスを持ち、電子メール資格情報でSecure Hubに登録するユーザーがSecure Mailに自動的に登録されるように構成します。これは、ユーザーが追加情報を入力する必要がないか、Secure Mailに登録する追加手順を実行する必要がないことを意味します。サーバープロパティMAM\_MACRO\_SUPPORTを設定する必要があります。

このグローバルクライアントポリシーを構成するには、[Settings] > [Client Properties] の順に選択し、カスタムキーSEND\_LDAP\_ATTRIBUTESを追加して、[Value] を以下のように設定します。

値 : userPrincipalName=\${user.userprincipalname},sAMAccountName=\${user.samaccountname},  
displayName=\${user.displayName},mail=\${user.mail}

MDMポリシーと同様、属性値はマクロとして指定されます。

このプロパティのアカウントサービスレスポンスのサンプルを以下に示します。

注 : このプロパティでは、XenMobileはコンマ文字を文字列の終わりとして扱います。そのため、属性値がコンマを含む場合、含まれているコンマをクライアントが属性値の末尾と解釈しないようにするには、その前にバックスラッシュを置く必要があります。バックスラッシュ文字は「\」と表します。



# ActiveSyncゲートウェイ

Apr 27, 2017

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、[Missing Required Apps] の規則をアクティブ化した場合、XenMobileは必須アプリのアプリアクセスポリシーをチェックし、必須アプリが不足している場合はActiveSyncデータへのアクセスを拒否します。規則ごとに、[Allow] または [Deny] を選択できます。デフォルト設定は、[Allow] です。

アプリケーションアクセスデバイスポリシーについて詳しくは、[「アプリケーションアクセスデバイスポリシー」](#) を参照してください。

XenMobileでは、次の規則がサポートされます。

**匿名デバイス** : デバイスが匿名モードではないかを確認します。このチェックは、デバイスが再接続を試行したときにXenMobileがユーザーを再認証できない場合に使用できます。

**Samsung KNOX 構成証明に失敗しました** : デバイスが、Samsung KNOX構成証明サーバーのクエリに失敗していないかを確認します。

**Forbidden Apps** : アプリアクセスポリシーの定義に基づいて、デバイスに禁止アプリがあるかチェックします。

**Implicit Allow and Deny** : このアクションはActiveSync Gatewayのデフォルトで、そのほかのフィルター規則条件に合致しないすべてのデバイスの一覧が作成され、この一覧に基づいてデバイスが許可または拒否されます。いずれの規則にも合致しない場合、デフォルトは黙示的な許可です。

**Inactive Devices** : [サーバー プロパティ] でデバイスの [非アクティブな日数のしきい値] に定義された期間、非アクティブであったかを確認します。

**Missing Required Apps** : 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。

**Non-suggested Apps** : 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。

**Noncompliant Password** : ユーザーパスワードが正しいかを確認します。iOSデバイスおよびAndroidデバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかをXenMobileが確認できます。たとえば、iOSでは、XenMobileがデバイスにパスコードポリシーを送信する場合、ユーザーは60分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

**Out of Compliance Devices** : [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。通常、このプロパティは自動化された操作により変更されるか、XenMobile APIを利用するサードパーティにより変更されます。

**Revoked Status** : デバイスの証明書が失効していないかを確認します。取り消されたデバイスは再認証されるまで再登録できません。

**Rooted Android and Jailbroken iOS Devices** : AndroidまたはiOSデバイスがジェイルブレイクされていないかを確認します。

**Unmanaged Devices** : 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

るデバイスや未登録のデバイスは管理されていません。

**Send Android domain users to ActiveSync Gateway** : XenMobileによってAndroidデバイスの情報がActiveSync Gatewayに送信されるようにするには、**[YES]** をクリックします。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 Gatewayに送信されます。

ActiveSyncゲートウェイ設定を構成するには

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

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. On the right, there is a gear icon and a user profile 'admin'. Below the navigation bar, the breadcrumb 'Settings > ActiveSync Gateway' is visible. The main heading is 'ActiveSync Gateway' with a sub-heading 'Allows or denies access to devices and users based on rules and properties.' Underneath, there is a section 'All devices' and a sub-section 'Activate the following rule(s)'. This section contains a list of 13 rules, each with an unchecked checkbox: 'Anonymous Devices', 'Failed Samsung KNOX attestation', 'Forbidden Apps', 'Implicit Allow and Deny', 'Inactive Devices', 'Missing Required Apps', 'Non-Suggested Apps', 'Noncompliant Password', 'Out of Compliance Devices', 'Revoked Status', 'Rooted Android and Jailbroken iOS Devices', and 'Unmanaged Devices'. Below this list, there is a section 'Android only' with a toggle switch for 'Send Android domain users to ActiveSync Gateway' which is currently set to 'YES'. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. **[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。

4. **[Android-only]** の **[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。
5. **[Save]** をクリックします。



# ネットワークアクセス制御

Apr 27, 2017

XenMobileで、Cisco ISEなどのNAC（Network Access Control：ネットワークアクセス制御）アプライアンスをネットワークで設定する場合は、フィルターで規則またはプロパティに基づいてデバイスをNACに準拠または非準拠として設定することができます。XenMobileの管理対象デバイスが指定された条件を満たしておらず、その結果 [非準拠] としてマークされている場合、そのデバイスはNACアプライアンスによりネットワーク上でブロックされます。

XenMobileコンソールの一覧で、デバイスを非準拠として設定する条件を1つまたは複数選択します。

XenMobileでは、次のNAC準拠フィルターがサポートされます。

**Anonymous Devices**：デバイスが匿名モードであるかチェックします。このチェックは、デバイスが再接続を試行したときにXenMobileがユーザーを再認証できない場合に使用できます。

**Failed Samsung KNOX attestation**：デバイスがSamsung KNOX認証サーバーのクエリに失敗したかチェックします。

**Forbidden Apps**：アプリアクセスポリシーの定義に基づいて、デバイスに禁止アプリがあるかチェックします。アプリケーションアクセスデバイスポリシーについて詳しくは、「[アプリケーションアクセスデバイスポリシー](#)」を参照してください。

**Inactive Devices**：サーバープロパティのデバイス無効日数しきい値設定の定義に基づいて、デバイスが無効であるかチェックします。詳しくは、「[サーバープロパティ](#)」を参照してください。

**Missing Required Apps**：アプリアクセスポリシーの定義に基づいて、デバイスに不足している必須アプリがあるかチェックします。

**Non-suggested Apps**：アプリアクセスポリシーの定義に基づいて、デバイスに非推奨アプリがあるかチェックします。

**Noncompliant Password**：ユーザーパスワードが準拠しているかチェックします。iOSデバイスおよびAndroidデバイスで、デバイス上の現在のパスワードが、デバイスに送信されるパスコードポリシーに準拠しているかをXenMobileが確認できます。たとえば、iOSでは、XenMobileがデバイスにパスコードポリシーを送信する場合、ユーザーは60分間でパスワードを設定する必要があります。ユーザーがパスワードを設定するまでの間、パスコードは非準拠になる可能性があります。

**Out of Compliance Devices**：非準拠デバイスプロパティに基づいて、デバイスが非準拠であるかチェックします。通常、このプロパティは自動化された操作により変更されるか、XenMobile APIを利用するサードパーティにより変更されます。

**Revoked Status**：デバイス証明書が取り消されたかチェックします。取り消されたデバイスは再認証されるまで再登録できません。

**Rooted Android and Jailbroken iOS Devices**：Androidデバイスがroot化されているか、またはiOSデバイスがジェイルブレイクされているかチェックします。

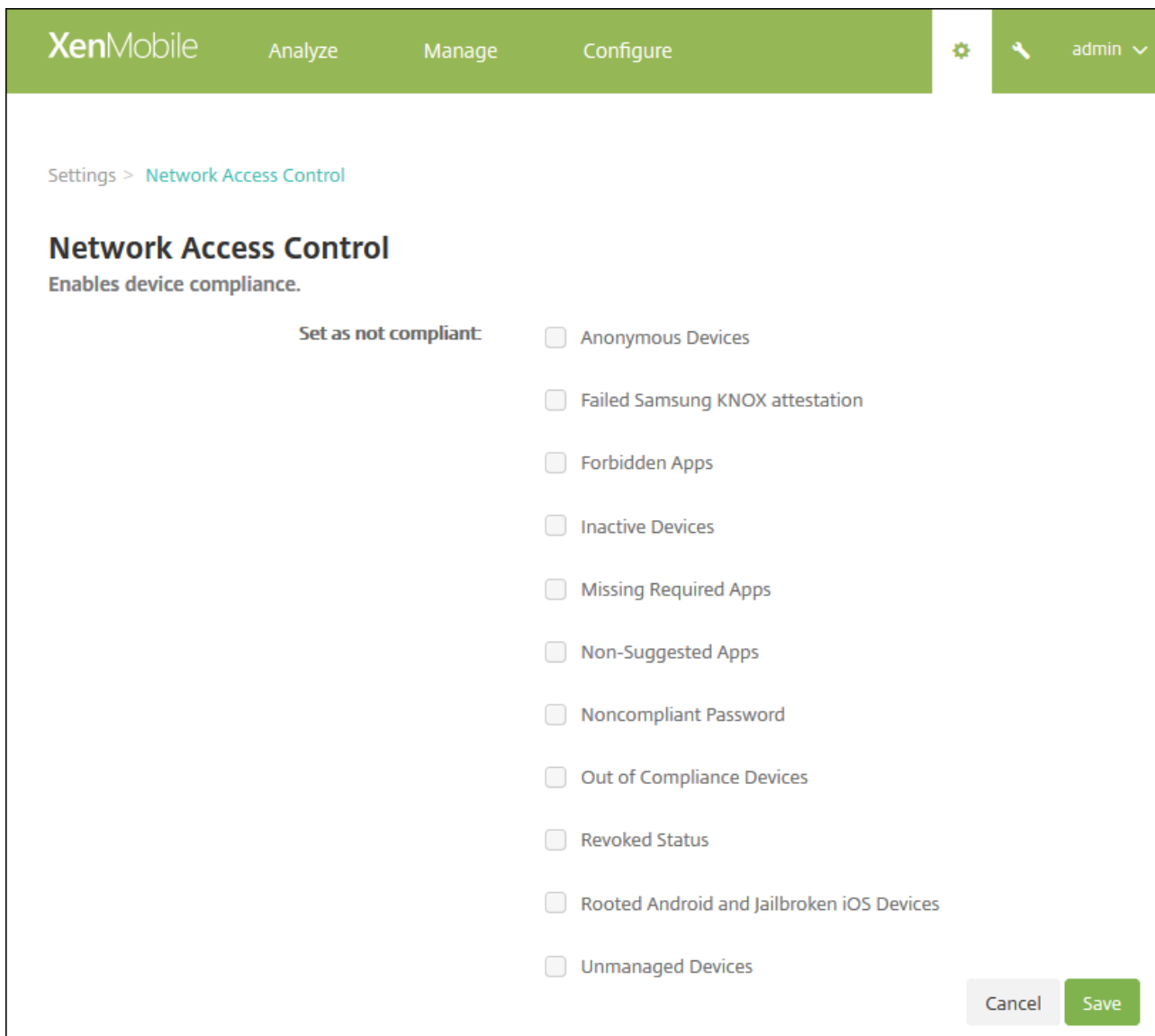
**Unmanaged Devices**：デバイスがXenMobileで現在も管理されている状態であるかチェックします。たとえば、MAMモードで実行されているデバイスや未登録のデバイスは管理されていません。

## 注意

[Implicit Compliant] または [Not Compliant] フィルターは、XenMobileによる管理対象デバイスでのみデフォルト値を設定します。たとえば、ブラックリストに入っているアプリケーションがインストールされているデバイスや、登録されていないデバイスは [Not-Compliant] としてマークされ、NACアプライアンスによりネットワークからブロックされます。

# ネットワークアクセス制御の構成

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



3. 有効にする [Set as not compliant] フィルターのチェックボックスを選択します。
4. [Save] をクリックします。

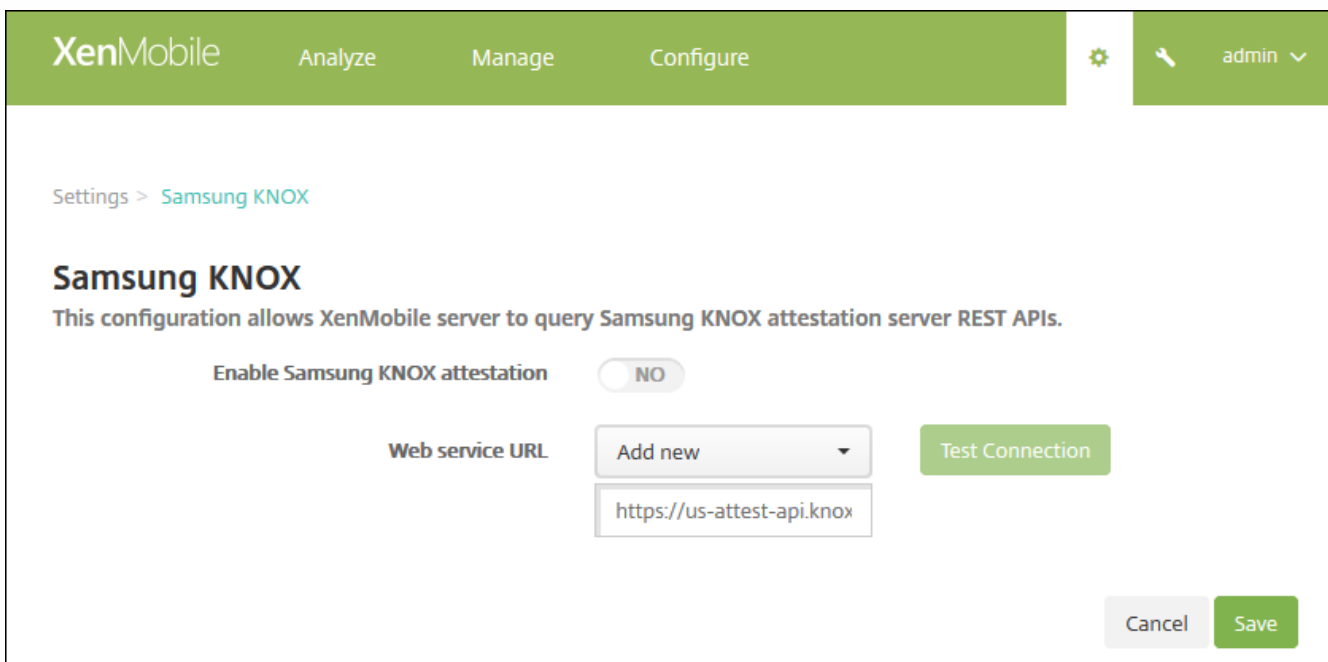
# Samsung KNOX

Apr 27, 2017

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

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

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



The screenshot shows the XenMobile web console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs, along with a gear icon and a user profile 'admin'. Below the navigation bar, the breadcrumb 'Settings > Samsung KNOX' is visible. The main heading is 'Samsung KNOX' with a sub-heading: 'This configuration allows XenMobile server to query Samsung KNOX attestation server REST APIs.' There are two main sections: 'Enable Samsung KNOX attestation' with a toggle switch currently set to 'NO', and 'Web service URL' with a dropdown menu showing 'Add new' and a text input field containing 'https://us-attest-api.knox'. To the right of the URL field is a green 'Test Connection' button. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. [Enable Samsung KNOX attestation] で、Samsung KNOX認証を有効にするかどうかを選択します。デフォルトは [NO] です。
4. [Enable Samsung KNOX attestation] を [YES] に設定すると、[Web service URL] オプションが有効になります。一覧から、次のいずれかを選択します。
  - a. 適切な認証サーバーを選択します。  
[Add new] を選択して、WebサービスURLを入力します。
5. [Test Connection] をクリックして、接続を検証します。成功、または失敗のメッセージが表示されます。
6. [Save] をクリックします。

## 注意

Samsung KNOX Mobile Enrollmentを使用すると、複数のSamsung KNOXデバイスをXenMobile（または、その他のモバイルデバイス

マネージャー)に登録する場合に、各デバイスを手動で構成する必要がありません。詳しくは、「[Samsung KNOX Bulk Enrollment](#)」を参照してください。

# Google Cloud Messaging

Apr 27, 2017

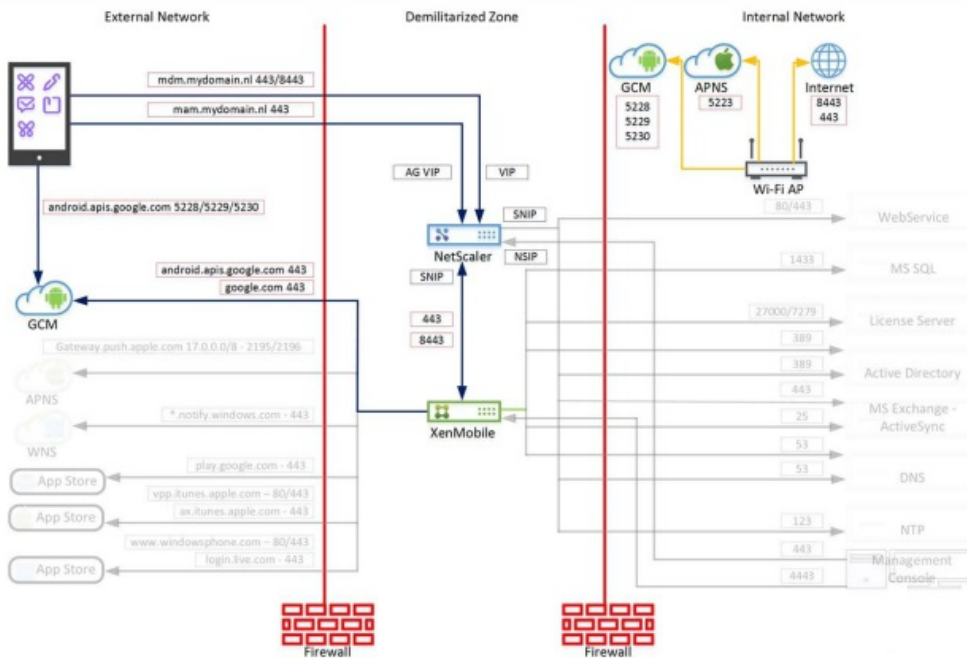
[Active poll period] ポリシーの代わりにFirebase Cloud Messaging (FCM) を使用して、AndroidデバイスがXenMobileに接続するタイミングと方法を制御することができます。次の構成を使用することで、セキュリティアクションや展開コマンドによって、ユーザーにXenMobileサーバーへの再接続を求めるプッシュ通知が送信されます。

## 前提条件

- XenMobile 10.3.x
- 最新のSecure Hubクライアント
- Googleデベロッパーアカウントの資格情報
- Android.apis.google.comおよびGoogle.comに向けたXenMobileのポート443の開放

## アーキテクチャ

次の図は、外部および内部ネットワークにおけるFCMの通信フローを示しています。



## GoogleアカウントをFCM向けに構成するには

1. Googleデベロッパーアカウントの資格情報を使用して次のURLにサインインします。

<https://console.firebase.google.com/?pli=1>

2. [Create a project] をクリックします。

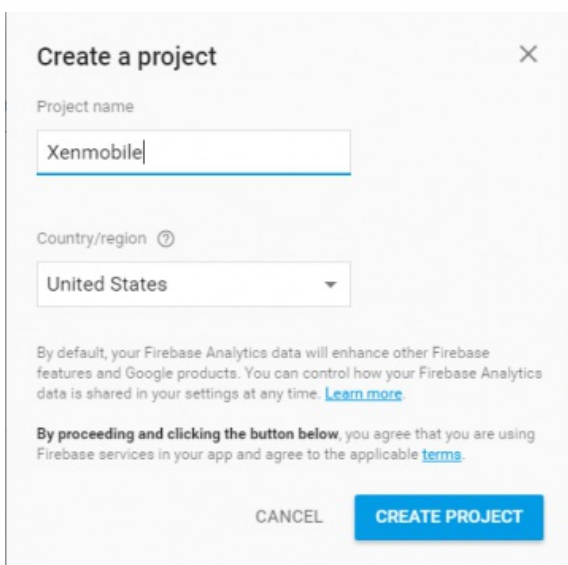
## Welcome to Firebase

Tools from Google for developing great apps,  
engaging with your users and earning more through  
mobile ads. [Learn more](#)

**CREATE NEW PROJECT**

[or import a Google project](#)

3.プロジェクト名を入力し、[Create Project] をクリックします。



**Create a project** [X]

Project name  
Xenmobile

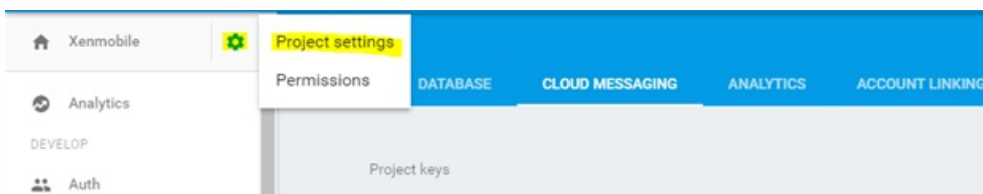
Country/region ⓘ  
United States

By default, your Firebase Analytics data will enhance other Firebase features and Google products. You can control how your Firebase Analytics data is shared in your settings at any time. [Learn more](#)

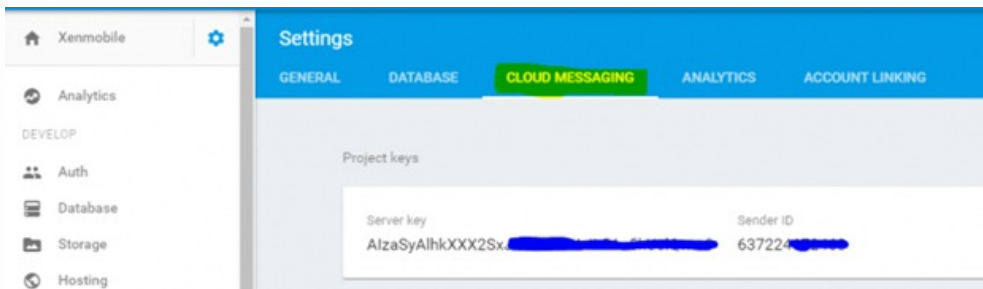
By proceeding and clicking the button below, you agree that you are using Firebase services in your app and agree to the applicable [terms](#).

CANCEL **CREATE PROJECT**

4. 左上のプロジェクト名の隣の歯車アイコンをクリックして、[プロジェクトの設定] を選択します。



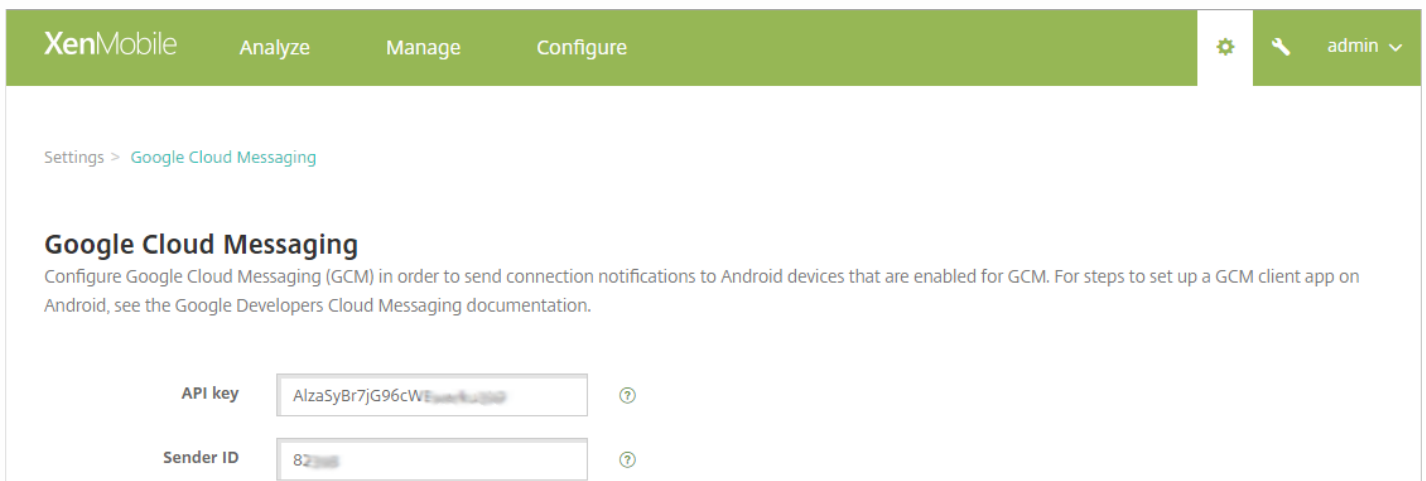
5. [Cloud Messaging] タブを選択します。そのページに送信者IDとサーバーキーが表示されます。これらの値をコピーします。XenMobileサーバーにそれらを設定する必要があります。2016年9月以降に作成するサーバーキーは、必ずFirebaseコンソールで作成する必要があることに注意が必要です。



## XenMobileをGCM向けに構成するには

1. XenMobile管理コンソールにサインインし、[Settings] > [Server Properties] の順に選択します。検索バーで、「GCM」と入力し、検索をクリックします。

- a. [GCM API key] を編集して、Firebase Cloud Messaging構成の最後の手順でコピーしたFirebase Cloud Messaging APIキーを入力します。
- b. [GCMSender ID] を編集して、前の手続きでコピーした送信者ID値を入力します。



## 構成をテストするには

FCM構成をテストする前提条件として、[Scheduling] ポリシーを構成してはなりません。また、ポリシーを[Always Connect] に設定しないでください。[Scheduling] ポリシーの構成について詳しくは、「[Scheduling device policy](#)」を参照してください。

1. Androidデバイスを登録します。
2. このデバイスを少しの時間アイドル状態にして、XenMobileサーバーから切断します。
3. XenMobile管理コンソールにログオンして [Manage] をクリックし、Androidデバイスを選択して [Secure] をクリックします。

XenMobile Analyze **Manage** Configure

Devices Users Enrollment

Devices Show filter

Add Edit **Secure** Notify Delete Import Export Refresh

Status	Mode	User name	Device platform	Operating system version	Device model
<input checked="" type="checkbox"/>	MDM MAM	hemanth@kronos.lab	Android	4.3	GT-19300

4. [Device Actions] で、[Selective Wipe] をクリックします。

Security Actions

Device Actions

Revoke Lock **Selective Wipe** Full Wipe

Locate

正常に構成されている場合、XenMobileに再接続せずにデバイスで選択的なワイプが行われます。



# Google Play資格情報

Apr 27, 2017

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。

Android IDを確認するには、お使いの電話機で「\*##8255##」を入力します。お使いのデバイスタイプ上でコードによりデバイスIDを検出できない場合、デバイスIDを導出するデバイスIDサードパーティ製アプリを使用できる場合があります。取得する必要があるIDは、Google Services Framework IDとラベルGSF IDです。

## 注意

XenMobileコンソールからGoogle Play Storeアプリを検索する場合、検索はデバイス上のAndroidオペレーティングシステムに対応したアプリを表示します。たとえば、Samsung S6 Edgeがオペレーションシステムバージョン6.0.1を実行しているとします。アプリを検索すると、検索結果にはAndroidバージョン6.0.1と互換性のあるアプリのみが表示されます。

## Important

XenMobileでアプリケーション情報の抽出を有効にするには、安全でない接続を許可するようにGmailアカウントを構成する必要があります。手順については、[Googleサポートサイト](#)を参照してください。

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

XenMobile Analyze Manage Configure

Settings > Google Play Credentials

### Google Play Credentials

XenMobile cannot extract app information without logon information. To find your Android ID, you can type \*##8255## on your phone.

User name\*

Password\*

Device ID\*

Cancel Save

3. 次の設定を構成します。

- [User name] : Google Playアカウントに関連付けられた名前を入力します。

- **Password** : ユーザーパスワードを入力します。
  - **Device ID** : Android IDを入力します。  
Android IDを取得する手順については、上記の「注」を参照してください。
3. **[Save]** をクリックします。

# デバイスポリシー

Apr 27, 2017

ポリシーを作成して、XenMobileとデバイスの連携方法を構成できます。多くのポリシーはすべてのデバイスに共通ですが、各デバイスのオペレーティングシステムに固有のポリシーもあります。そのため、プラットフォーム間で異なる場合や、Androidを実行するデバイスの製造元によっても違いがある場合があります。プラットフォーム別ポリシーのマトリックスについては、「[Device Policies by Platform Matrix PDF](#)」を参照してください。

新しいポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定のデリバリーグループを作成します。
- 必要なCA証明書をインストールします。

デバイスポリシーの基本的な作成手順は次のとおりです。

1. ポリシーの名前と説明を指定します。
2. 1つまたは複数のプラットフォームを構成します。
3. 展開規則を作成します（任意）。
4. ポリシーをデリバリーグループに割り当てます。
5. 展開スケジュールを構成します（任意）。

XenMobileで次のデバイスポリシーを構成できます。

デバイスポリシー名	デバイスポリシーの説明
AirPlayミラー化	XenMobileでデバイスポリシーを追加して、特定のAirPlayデバイス（Apple TVやほかのMacコンピュータなど）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デバイスのみ限定するオプションもあります。
AirPrint	AirPrintデバイスポリシーで、AirPrintプリンターをユーザーのiOSデバイスのAirPrintプリンター一覧に追加できます。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。  注： <ul style="list-style-type: none"><li>● このポリシーはiOS 7.0以降に適用されます。</li><li>● 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。</li></ul>
Android for Workアプリケーション制限	このポリシーによって、Android for Workアプリに関連する制限を変更できますが、そのためには、次の前提条件を満たす必要があります。 <ul style="list-style-type: none"><li>● GoogleのAndroid for Work設定タスクを完了します。詳しくは、「<a href="#">XenMobileでのAndroid for Workによるデバイスの管理</a>」を参照してください。</li><li>● Android for Workアカウントの作成詳しくは、「<a href="#">Android for Workアカウントの作成</a>」を参照してください。</li><li>● Android for WorkアプリをXenMobileに追加します。詳しくは、「<a href="#">XenMobileへのアプリケー</a></li></ul>

	<p>「<a href="#">シヨンの追加</a>」を参照してください。</p>
APN	<p>このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマーAPNを使用しない組織で使われます。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。</p>
アプリケーションアクセス	<p>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。</p>
アプリケーション属性	<p>アプリケーション属性デバイスポリシーで、iOSデバイスのための属性 (管理対象アプリのバンドルIDやアプリごとのVPN識別子など) を指定できます。</p>
アプリケーション構成	<p>このポリシーでは、管理された構成をサポートするアプリケーションのさまざまな設定および動作をリモートで構成できます。XML構成ファイル (プロパティ一覧またはplistと呼ばれるファイル) をユーザーのiOSデバイスに展開するか、キー/値ペアをユーザーのWindows 10 Phoneまたはタブレット/デスクトップデバイスに展開できます。</p>
アプリケーションインベントリ	<p>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。</p>
アプリケーションロック	<p>XenMobileでは、ポリシーを作成して、デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行を禁止するアプリの一覧を定義できます。</p> <p>このポリシーは、iOSデバイスとAndroidデバイスの両方に対して構成できますが、ポリシーが実際にどのように機能するかは各プラットフォームで異なります。たとえば、iOSデバイスで複数のアプリを禁止することはできません。</p> <p>注：デバイスポリシーは大部分のAndroid LおよびMデバイスで機能しますが、アプリのロックは、必要なAPIがGoogleによって廃止されたため、Android N以降のデバイスでは機能しません。</p> <p>また、iOSデバイスで選択できるiOSアプリは、ポリシーあたり1つのみです。これによって、デバイスで実行できるのは1つのアプリのみになります。アプリのロックポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。</p>
アプリケーションネットワーク使用状況	<p>ネットワーク使用状況規則を設定して、iOSデバイスで管理対象のアプリケーションが携帯データネットワークなどのネットワークをどのように使用するかを指定できます。規則は管理対象のアプリケーションにのみ適用されます。管理対象のアプリケーションとは、XenMobileを使用して</p>

	<p>ユーザーのデバイスに展開されるアプリケーションです。これには、ユーザーがXenMobileを使用して展開することなく直接デバイスにダウンロードしたアプリケーションや、デバイスのXenMobileへの登録時に既にデバイスにインストールされていたアプリケーションは含まれません。</p>
アプリケーション制限	<p>このポリシーによって、ユーザーによるSamsung KNOXデバイスへのインストールを禁止するアプリケーションのブラックリストを作成したり、ユーザーによるインストールを許可するアプリケーションのホワイトリストを作成したりできます。</p>
アプリトンネル	<p>アプリトンネルポリシーは、モバイルアプリケーションのサービスの継続性およびデータ転送の信頼性を向上させるように構成できます。アプリトンネルは、モバイルデバイスアプリケーションのクライアントコンポーネントとアプリケーションサーバーコンポーネント間のプロキシパラメーターを定義します。また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。</p> <p>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。</p>
アプリケーションのアンインストール	<p>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。</p>
アプリケーションのアンインストール制限	<p>このポリシーによって、ユーザーがインストールできる、またはインストールできないアプリを指定できます。</p>
Webブラウザー	<p>ブラウザーデバイスポリシーを作成して、ユーザーのデバイスでブラウザーを使用できるかどうかを定義したり、ユーザーのデバイスで使用できるブラウザー機能を制限したりすることができます。Samsungデバイスでは、ブラウザーを完全に無効にすることや、ポップアップ、JavaScript、Cookie、オートフィル、不正Webサイト警告の適用の有無を有効または無効にすることができます。</p>
カレンダー (CalDav)	<p>XenMobileでデバイスポリシーを追加して、カレンダー (CalDAV) アカウントをユーザーのiOSデバイスまたはMax OS Xデバイスに追加し、CalDAVをサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。</p>
移動体通信	<p>このポリシーを使用すると、モバイルネットワーク設定を構成できます。</p>
接続マネージャー	<p>XenMobileでは、インターネットおよびプライベートネットワークに自動的に接続するアプリケーションの接続設定を指定できます。このポリシーはWindows Pocket PCでのみ使用できます。</p>

連絡先 (CardDAV)	XenMobileでデバイスポリシーを追加して、iOS連絡先 (CardDAV) アカウントをユーザーのiOSデバイスまたはMac OS Xデバイスに追加し、CardDAVをサポートするサーバーとそのデバイスの連絡先データを同期することができます。
Samsungコンテナへのアプリケーションのコピー	デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナまたはKNOXコンテナにコピーされるように指定できます。SEAMSコンテナにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナにコピーされたアプリケーションは、ユーザーがKNOXコンテナにサインインした場合のみ使用できます。
資格情報	<p>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、「<a href="#">XenMobileでの証明書</a>」を参照してください。</p> <p>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、「<a href="#">資格情報デバイスポリシー</a>」の記事で説明しています。</p> <p>注：このポリシーを作成するには、各プラットフォームで使用する予定の資格情報と、証明書およびパスワードが必要です。</p>
Samsungコンテナへのアプリケーションのコピー	デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナまたはKNOXコンテナにコピーされるように指定できます。サポートされるデバイスの詳細については、Samsungの <a href="#">Samsung KNOX Supported Devices</a> を参照してください。SEAMSコンテナにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナにコピーされたアプリケーションは、ユーザーがKNOXコンテナにサインインした場合のみ使用できます。
資格情報	WiFiポリシーと連携して使用されることの多いこのポリシーによって、組織が認証証明書を必要とする内部のリソースに認証証明書を展開することができます。
カスタムXML	<p>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。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul> <p>WindowsでOpen Mobile Alliance Device Management (OMA DM) APIを使用して、カスタムXML構成を作成します。OMA DM APIを使用したカスタムXMLの作成については、このトピックでは扱いません。OMA DM APIの使用について詳しくは、Microsoft Developer Networkサイトの「<a href="#">OMA Device Management</a>」を参照してください。</p>
ファイルおよび	XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のファイルまたはフォル

フォルダーの削除	データを削除できます。
レジストリ キーと値の削除	XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のレジストリキーおよび値を削除することができます。
デバイス正常性構成証明	<p>XenMobileでは、分析目的で特定のデータおよびランタイム情報をHealth Attestation Service (HAS) に送信させ、Windows 10デバイスに正常性状態を報告させるポリシーを作成することができます。HASは、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスからXenMobileに送信されます。XenMobileは正常性構成証明書を受信すると、その内容に基づいて、管理者が以前に設定した自動アクションを展開します。</p> <p>HASによって検証されるデータは以下のとおりです。</p> <ul style="list-style-type: none"> <li>● AIKの有無</li> <li>● Bit Lockerの状態</li> <li>● ブートデバッグが有効化されているかどうか</li> <li>● ブートマネージャーのバージョン</li> <li>● コードの整合性チェックが有効化されているかどうか</li> <li>● コード整合性のバージョン</li> <li>● DEP ポリシー</li> <li>● ELAMドライバーが起動されているかどうか</li> <li>● 発行元</li> <li>● カーネルのデバッグが有効化されているかどうか</li> <li>● PCR</li> <li>● リセット回数</li> <li>● 再起動の回数</li> <li>● セーフモードが有効化されているかどうか</li> <li>● SBCPハッシュ</li> <li>● セキュアブートが有効化されているかどうか</li> <li>● テスト署名が有効化されているかどうか</li> <li>● VSMが有効であること。</li> <li>● WinPEが有効であること。</li> </ul> <p>詳しくは、Microsoftの「<a href="#">HealthAttestation CSP</a>」ページを参照してください。</p>
名前	デバイス名ポリシーでは、デバイスを特定しやすくするために、iOSデバイスおよびMac OS Xデバイスに名前を設定できます。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。マクロについて詳しくは、「 <a href="#">XenMobileのマクロ</a> 」を参照してください。
エンタープライズハブ	<p>Windows PhoneのEnterprise Hubデバイスポリシーでは、Enterprise Hub Companyストアを通じてアプリケーションを配布できます。</p> <p>このポリシーを作成するには以下が必要です。</p> <ul style="list-style-type: none"> <li>● SymantecからのAET (.aetx) 署名証明書</li> <li>● 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</li> </ul>

	<p>注：XenMobileでは、Windows Phone Secure Hubの1つのモードについて、1つのEnterprise Hubポリシーがサポートされています。たとえば、Windows Phone Secure Hub for XenMobile Enterprise Editionをアップロードするために、複数のEnterprise HubポリシーをさまざまなバージョンのWork Home for XenMobile Enterprise Edition用に作成する必要はありません。デバイスの登録中に最初のEnterprise Hubポリシーを展開するだけです。</p>
Exchange	<p>XenMobileでは、電子メールを送信する2つのオプションがあります。コンテナ化されたSecure Mailアプリを使用してActiveSyncメールを送信するか、MDM Exchangeポリシーを使用してデバイス上のネイティブの電子メールクライアントでActiveSyncメールを有効にできます。</p>
ファイル	<p>このポリシーで、ユーザーに対して特定の機能を実行するスクリプトファイル、またはAndroidデバイスユーザーがデバイスでアクセスできるドキュメントファイルを、XenMobileに追加できます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。たとえば、Androidユーザーが会社のドキュメントまたは.pdfファイルを受け取るようにする場合は、ファイルをデバイスに展開し、ユーザーにファイルがある場所を知らせます。</p> <p>このポリシーで追加できるファイルの種類は次のとおりです。</p> <ul style="list-style-type: none"> <li>● テキストベースのファイル (.xml、.html、.pyなど)</li> <li>● ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル</li> <li>● Windows MobileおよびWindows CEのみ：MortScriptで作成されたスクリプトファイル</li> </ul>
フォント	<p>XenMobileでこのデバイスポリシーを追加して、追加フォントをユーザーのiOSデバイスおよびMac OS Xデバイスに追加することができます。フォントはTrueType (.ttf) またはOpenType (.oft) である必要があります。フォントコレクション (.ttcまたは.otc) はサポートされません。</p> <p>注：iOSの場合、このポリシーはiOS 7.0以降にのみ適用されます。</p>
iOSおよびMac OS Xプロファイルのインポート	<p>iOSおよびOS Xデバイス用のデバイス構成MXLファイルをXenMobileにインポートできます。XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。Apple Configuratorの使用による構成ファイルの作成については、Appleの<a href="#">Configuratorヘルプページ</a>を参照してください。</p>
キオスク	<p>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。</p> <p>注：</p> <ul style="list-style-type: none"> <li>● 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。</li> <li>● 一部のオプションは、Samsungモバイルデバイス管理 (MDM) API 4.0以降にのみ適用されます。</li> </ul>



ランチャー構成	このAndroidデバイス用ポリシーを使用すると、Citrix Launcher、Citrix Launcherアイコンのカスタムロゴ画像、Citrix Launcherのカスタム背景画像、およびランチャーを終了するためのパスワード要件を指定できます。
LDAP	<p>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。</p> <p>このポリシーを構成するには、LDAPホスト名が必要です。</p>
場所	位置情報ポリシーは地図上で位置を検出できるデバイスのGPSがSecure Hubに対応している場合に使用できます。このポリシーがデバイスでプッシュされると、管理者はXenMobileサーバーから位置を確認するコマンドを送信し、デバイスは位置情報を返信します。ジオフェンシングおよび追跡ポリシーもサポートされます。
メール	XenMobileでメールデバイスポリシーを追加して、ユーザーのiOSデバイスまたはMac OS Xデバイスのメールアカウントを構成することができます。
管理対象ドメイン	<p>このポリシーによって、メールおよびSafariブラウザーに適用する管理対象ドメインを定義できます。管理対象ドメインを使用すると、Safariを使用してドメインからダウンロードしたドキュメントを開くことができるアプリケーションを制御して、会社のデータを保護することができます。URLまたはサブドメインを使用して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御します。このポリシーは、iOS 8以降の監視対象デバイスでのみサポートされます。iOSデバイスをSupervisedモードに設定する手順については、「<a href="#">Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには</a>」を参照してください。</p> <p>ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上で該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。</p> <p>ユーザーがSafariを使用して、管理対象Webドメイン一覧に含まれているWebドメインから取得したアイテム（ドキュメントや添付ファイルなど、ダウンロードしたもの）を開こうとすると、適切な社内アプリケーションによってアイテムが開かれます。アイテムが管理対象Webドメイン一覧にあるWebドメインから取得されたものでない場合、ユーザーは社内アプリケーションでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリケーションを使用する必要があります。</p>
MDMオプション	<p>XenMobileでデバイスポリシーを作成して、監視対象のiOS 7.0以降のモバイルデバイスで [iPhone/iPadを探す] の [アクティベーションロック] を管理することができます。iOSデバイスをSupervisedモードに設定する手順については、「<a href="#">Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには</a>」または「<a href="#">iOSバルク登録</a>」を参照してください。</p> <p>アクティベーションロックは、紛失したり、盗まれたりしたデバイスが再アクティベーションされないようにすることを目的とした [iPhone/iPadを探す] の機能であり、ユーザーのApple IDおよびパスワードを必須にすることで、誰かが [iPhoneを探す] をオフにしたり、デバイスを消去した</p>

	<p>り、デバイスを再アクティベーションして使用したりするのを防ぎます。XenMobileでは、MDM オプションデバイスポリシーでアクティベーションロックを有効にすることにより、必須とされているApple IDおよびパスワードの入力をバイパスできます。ユーザーから返却されたデバイスで [iPhoneを探す] が有効になっていた場合、Appleの資格情報なしでXenMobileコンソールからデバイスを管理することができます。</p>
組織情報	<p>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せん。</p>
パスコード	<p>パスコードポリシーによって、管理対象デバイスにPINコードまたはパスワードを適用できます。このパスコードポリシーは、デバイス上でパスコードの複雑さやタイムアウトを設定します。</p>
個人用ホットスポット	<p>このポリシーによって、iOSデバイスの個人用ホットスポット機能を介して携帯データネットワーク接続を使用することにより、ユーザーがWiFiネットワーク圏外にいてもインターネットに接続できるようにすることができます。iOS 7.0以降で利用できます。</p>
プロファイル削除	<p>XenMobileで、アプリケーションプロファイル削除デバイスポリシーを作成することができます。ポリシーを展開すると、ユーザーのiOSデバイスまたはMac OS Xデバイスからアプリケーションプロファイルが削除されます。</p>
プロビジョニングプロファイル	<p>iOSエンタープライズアプリを開発しコード署名するときは、通常は、iOSデバイスで実行するアプリにAppleが求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。</p> <p>プロビジョニングプロファイルの主な問題は、Apple Developer Portalで生成されてから1年で期限が切れるので、ユーザーによって登録されたすべてのiOSデバイス上のすべてのプロビジョニングプロファイルの期限を追跡する必要があります。期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信する、プロビジョニングプロファイルをWebポータルに置いてダウンロードとインストールを可能にする、という2つの方法があります。これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Webポータルにアクセスして適切なプロファイルをダウンロードしインストールすることを求めたりするので、エラーが発生する傾向があります。</p> <p>このプロセスをユーザーが意識しないで済むように、XenMobileではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。</p>
プロビジョニングプロファイルの削除	<p>デバイスポリシーを使用してiOSプロビジョニングプロファイルを削除できます。プロビジョニングプロファイルについて詳しくは、「<a href="#">プロビジョニングプロファイルの追加</a>」を参照してください。</p>

プロキシDHCP	<p>XenMobileでデバイスポリシーを追加して、Windows Mobile/CEおよびiOS 6.0以降を実行しているデバイスのグローバルHTTPプロキシ設定を指定できます。グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。</p> <p>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、「<a href="#">Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには</a>」を参照してください。</p>
レジストリ	<p>Windows Mobile/CEのレジストリには、アプリケーション、ドライバー、ユーザー設定、および構成設定に関するデータが格納されています。XenMobileでは、Windows Mobile/CEデバイスを管理するためのレジストリキーおよび値を定義できます。</p>
リモートサポート	<p>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。</p> <ul style="list-style-type: none"> <li>• [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。</li> <li>• [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。</li> </ul>
制限事項	<p>制限ポリシーによって、管理者は管理対象デバイスの機能をロックダウンおよび制御するさまざまなオプションを使用できます。文字通り数百の制限オプションがあり、デバイスのカメラやマイクを無効にしたり、ローミング規則の適用やアプリケーションストアのようなサードパーティサービスへのアクセスなどに対応します。</p> <p>XenMobileでデバイスポリシーを追加して、ユーザーのデバイス、電話、タブレットなどの特定の機能を制限できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。</p> <p>このデバイスポリシーでは、デバイスの特定の機能（カメラなど）をユーザーが使用することを許可または制限します。また、セキュリティ制限、メディアコンテンツの制限、ユーザーがインストールできる（できない）アプリケーションの種類の制限を設定できます。ほとんどの制限設定は、デフォルトでは [ON]（許可）に設定されています。例外は、iOSセキュリティの強制機能とすべてのWindowsタブレット機能です。デフォルトで [OFF]（制限）に設定されています。</p> <p>ヒント：オプションでONを選択した場合、ユーザーは該当する操作を実行、または該当する機能を使用できます。次に例を示します。</p> <ul style="list-style-type: none"> <li>• 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。</li> <li>• [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。</li> </ul>
移動	<p>XenMobileでデバイスポリシーを追加して、ユーザーのiOSデバイスおよびWindows Mobile/CEデバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。音声通</p>

	<p>話ローミングを無効にした場合、データローミングは自動的に無効になります。iOSの場合、このポリシーはiOS 5.0以降のデバイスでのみ使用できます。</p>
Samsung SAFEファイアウォール	<p>このポリシーにより、Samsungデバイスのファイアウォール設定を構成できます。デバイスにアクセスを許可するIPアドレス、ポート、ホスト名、またはデバイスのアクセスをブロックするIPアドレス、ポート、ホスト名を入力します。プロキシおよびプロキシ再ルーティングの設定を構成することもできます。</p>
Samsung MDMライセンスキー	<p>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。</p> <p>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があります。Samsung KLMSはモバイルデバイス管理 (MDM : Mobile Device Management) ソリューションに有効なライセンスをプロビジョニングし、モバイルデバイスでSamsung KNOX APIをアクティブ化できるようにします。これらのライセンスはSamsungから取得する必要があり、Citrixからは提供されません。</p> <p>Secure HubをSamsung ELMキーと共に展開し、SAFEおよびSamsung KNOX APIを有効にする必要があります。SAFE APIが有効になっていることは、デバイスプロパティをチェックすることで確認できます。Samsung ELMキーが展開されると、[Samsung MDM API available] 設定が [True] に設定されます。</p>
スケジュール設定	<p>このポリシーは、AndroidおよびWindows MobileデバイスがMDM管理、アプリのプッシュ、ポリシーの展開のためにXenMobileサーバーに接続する際に必要です。このポリシーを送信せず、Google FCMを有効にしていない場合、デバイスはサーバーに接続することができません。このため、デバイスの登録では、ベースパッケージでこのポリシーをプッシュする必要があります。</p>
SCEP	<p>このポリシーでiOSデバイスとMax OS Xデバイスを構成し、SCEP (Simple Certificate Enrollment Protocol) を使用して外部SCEPサーバーから証明書を取得することができます。XenMobileに接続されているPKIからSCEPを使用してデバイスに証明書を配布する場合は、PKIエンティティとPKIプロバイダーを分散モードで作成する必要があります。詳しくは、「<a href="#">PKIエンティティ</a>」を参照してください。</p>
サイドローディングキー	<p>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。</p> <p>このポリシーを作成する前に以下の情報が必要です。</p> <ul style="list-style-type: none"> <li>● サイドローディングプロダクトキー。Microsoftポリュームライセンスサービスセンターにサイ</li> </ul>

	<p>ンインして取得します。</p> <ul style="list-style-type: none"> <li>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。</li> </ul>
証明書署名	<p>XenMobileでデバイスポリシーを追加して、APPXファイルへの署名に使用される署名証明書を構成することができます。署名証明書は、ユーザーにAPPXファイルを配布して、ユーザーがWindowsタブレットにアプリケーションをインストールできるようにする場合に必要です。</p>
Single Sign On (SSO) アカウント	<p>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ますようにします。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。</p> <p>注：このポリシーはiOS 7.0以降にのみ適用されます。</p>
ストレージ暗号化	<p>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。</p> <p>Samsung SAFE、Windows Phone、Android Sonyデバイスに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値については詳しくは、ストレージ暗号化ポリシーのトピックで説明しています。</p>
ストア	<p>XenMobileでポリシーを作成して、iOS、Android、またはWindowsタブレットデバイスのホーム画面でXenMobile StoreのWebクリップを表示するかどうかを指定できます。</p>
サブスクライブされたカレンダー	<p>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、<a href="http://www.apple.com/downloads/macosx/calendars">www.apple.com/downloads/macosx/calendars</a>にあります。</p> <p>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。</p>
契約条件	<p>社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、XenMobileで契約条件デバイスポリシーを作成します。ユーザーがXenMobileにデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。</p> <p>社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。AndroidデバイスおよびiOSデバイスの場合は、PDFファイルを提供する必要があります。Windowsデバイスの場合は、テキスト (TXT) ファイルと付属のイメージファイルを提供する必要があります。</p>

VPN	<p>従来のVPN Gatewayテクノロジーでバックエンドシステムにアクセスを提供したい場合、このVPNポリシーを使用してVPNゲートウェイ接続の詳細をデバイスにプッシュできます。このポリシーでは、さまざまなVPNプロバイダー（Citrix VPNに加えてCisco AnyConnect、Juniperなど）がサポートされています。また、このポリシーをCAにリンクして、オンデマンドでVPNオンデマンドを有効にできます（VPNゲートウェイがこのオプションをサポートしている場合）。</p> <p>XenMobileでデバイスポリシーを追加して、VPN（Virtual Private Network：仮想プライベートネットワーク）の設定を構成し、ユーザーのデバイスが社内リソースに安全に接続できるようにすることができます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、VPNのトピックで説明しています。</p>
壁紙	<p>.pngファイルまたはjpgファイルを追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。iOS 7.1.2以降で使用できます。iPadおよびiPhoneで異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。</p>
Webコンテンツフィルター	<p>XenMobileでデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトとAppleのオートフィルター機能を組み合わせて使用して、iOSデバイスでWebコンテンツをフィルタリングできます。このポリシーはiOS 7.0以降のSupervisedモードのデバイスでのみ使用できます。iOSデバイスをSupervisedモードにする方法について詳しくは、「<a href="#">Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには</a>」を参照してください。</p>
[Webclip	<p>このポリシーでは、ショートカットやWebクリップをWebサイトに配置してユーザーデバイスのアプリと一緒に表示できます。iOS、Mac OS X、AndroidデバイスのWebクリップを表す独自のアイコンを指定できます。Windowsタブレットのみ、ラベルおよびURLが必要になります。</p>
WiFi	<p>WiFiポリシーによって、管理者はSSID、認証データ、構成データなどWiFiルーターの詳細を簡単に管理対象デバイスにプッシュできます。</p> <p>WiFiポリシーでは、ネットワークの名前と種類、認証およびセキュリティポリシー、プロキシサーバーの使用の有無や、そのほかのWiFi関連事項を、特定のプラットフォームのすべてのユーザーに対して一貫的に定義し、ユーザーデバイスのWiFiネットワークへの接続方法を管理できます。</p>
Windows CE証明書	<p>このデバイスポリシーを追加して、外部のPKIを基にWindows Mobile/CE PKI証明書を作成し、ユーザーのデバイスに配布できます。証明書およびPKIエンティティについて詳しくは、「<a href="#">証明書</a>」を参照してください。</p>
XenMobileオプション	<p>XenMobileオプションポリシーを追加して、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのSecure Hubの動作を構成します。</p>
XenMobileのアンインストール	<p>XenMobileでこのデバイスポリシーを追加して、XenMobileをAndroidデバイスおよびWindows Mobile/CEデバイスからアンインストールすることができます。このポリシーを展開すると、展開グループ内のすべてのデバイスからXenMobileが削除されます。</p>

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。

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status
<input type="checkbox"/>	MBWifi	Wifi	10/26/15 1:03 PM	10/26/15 1:03 PM	
<input type="checkbox"/>	Passcode	Password	10/29/15 8:33 AM	10/29/15 8:33 AM	
<input type="checkbox"/>	Restrictions	Restrictions	10/29/15 8:34 AM	10/29/15 8:34 AM	
<input type="checkbox"/>	Personal Hotspot	Personal Hotspot	10/29/15 8:35 AM	10/29/15 8:35 AM	

[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。

The screenshot shows the XenMobile 'Configure' interface. The 'Device Policies' section is active, displaying a table of policies. The 'Passcode' policy is selected. A deployment summary dialog is open over the table, showing the following data:

Policy name	Type	Created on	Last updated on	Status
MBWifi	Wifi	10/26/15 1:03 PM	10/26/15 1:03 PM	
<b>Passcode</b>	<b>Password</b>	<b>10/29/15 8:33 AM</b>	<b>10/29/15 8:33 AM</b>	
Restrictions	Restrictions			
Personal Hotspot	Personal Hotspot			

The deployment summary dialog shows:

- 0 Installed
- 0 Pending
- 0 Failed

Below the summary is a link: [Show more >](#)

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。

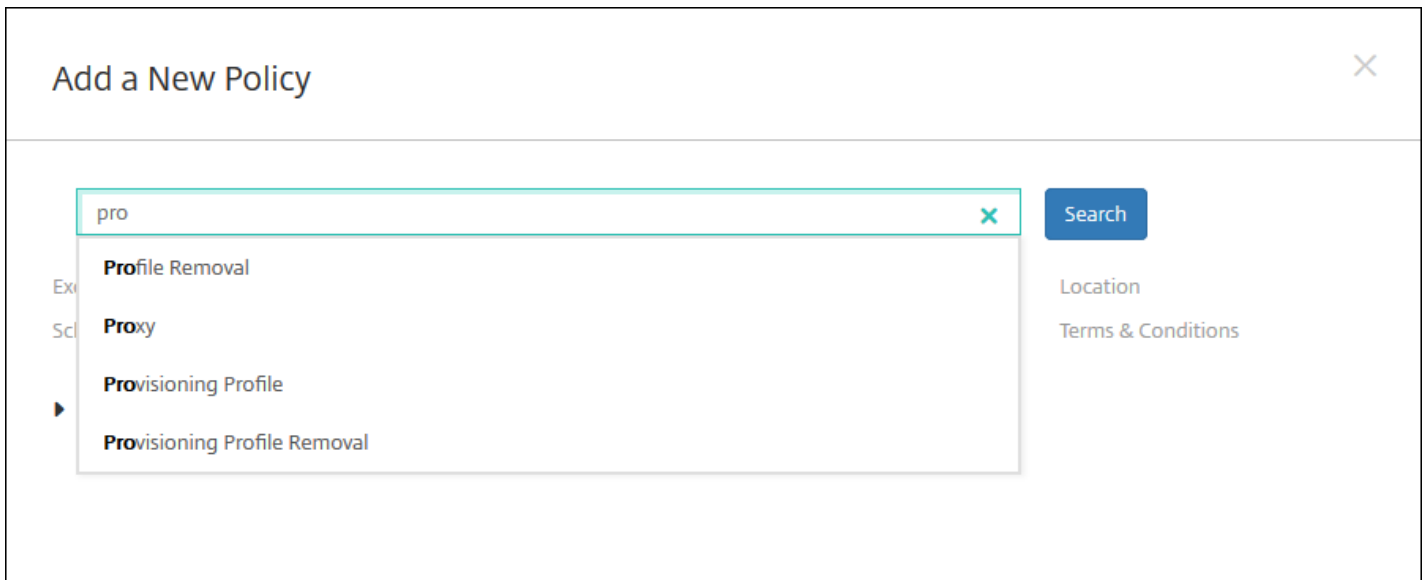
The 'Add a New Policy' dialog box contains the following elements:

- Search bar: *Type or select a policy from the list*
- Search button: Search
- Policy categories: Exchange, Scheduling, Passcode, Restrictions, VPN, WiFi, Location, Terms & Conditions
- More link: [More](#)



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。

## Passcode Policy

### 1 Policy Info

### 2 Platforms

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

5. プラットフォームページの入力を完了します。手順3.で選択した各プラットフォームのページが開きます。これらのページはポリシーごとに異なります。各ポリシーはプラットフォームによって異なる場合があります。すべてのポリシーがすべてのプラットフォームでサポートされるわけではありません。[Next] をクリックすると、次のプラットフォームページに移動します。すべてのプラットフォームページの入力が完了した場合は、[Assignment] ページに移動します。

6. [Assignments] ページで、ポリシーを適用するデリバリーグループを選択します。デリバリーグループをクリックすると、[Delivery groups to receive app assignment] ボックスにそのグループが表示されます。

注： [Delivery groups to receive app assignment] ボックスは、デリバリーグループを選択するまで表示されません。

7. [Save] をクリックします。

ポリシーが [Device Policies] の表に追加されます。

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

Apr 27, 2017

プラットフォーム別のポリシーを確認するには、「[Device Policies by Platform Matrix PDF](#)」を参照してください。

デバイスポリシーの追加と構成は、XenMobileコンソールの[Configure]の[Device Policies]をクリックすると開くページで実行できます。

XenMobile 10.4は、以下のプラットフォームのデバイスポリシーをサポートしています。

- Amazon
- iOS
- Mac OS X
- Android HTC
- Android TouchDown
- Android at Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Mobile/CE (.cabファイル)
- Windows Phone 8/Windows 10 Mobile
- Windows 8およびWindows 10 Desktop/Tablet (.86)

XenMobile 10.xでサポートされるデバイスについて詳しくは、「[サポート対象のデバイスプラットフォーム](#)」を参照してください。

## 注意

- XenMobile 10.3では、Symbianデバイスのサポートは廃止されました。
- 環境がグループポリシーオブジェクト (GPO) 構成されていて、Windows 10でXenMobileデバイスポリシーを構成する場合、登録済みのWindows 10デバイス間でポリシーの競合が発生した場合、GPOに合っているポリシーが優先されます。

# AirPlayミラーリングデバイスポリシー

Apr 27, 2017

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デバイスのみで限定するオプションもあります。デバイスをSupervisedモードにする方法については、「[Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには](#)」を参照してください。

注： 続行する前に、追加するすべてのデバイスのデバイスIDとパスワードがあることを確認してください。

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

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

3. [More] を展開した後、[End user] の下の [AirPlay Mirroring] をクリックします。[AirPlay Mirroring] ページが開きます。

The screenshot shows the XenMobile console interface for configuring an AirPlay Mirroring Policy. The main content area is titled "AirPlay Mirroring Policy" and includes a "Policy Information" section. This section contains a "Policy Name\*" field and a "Description" field, both of which are currently empty. Below the "Policy Information" section is a "Next >" button. On the left side, there is a sidebar with three sections: "1 Policy Info", "2 Platforms", and "3 Assignment". The "2 Platforms" section is expanded, showing two options: "iOS" and "Mac OS X", both of which are checked with a green checkmark. The top navigation bar includes "XenMobile", "Analyze", "Manage", "Configure", and "admin".

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

次の設定を構成します。

- **AirPlay Password**：追加するデバイスごとに、**[Add]** をクリックして以下の操作を行います。
  - **Device ID**：ハードウェアのアドレス (MACアドレス) を「xx:xx:xx:xx:xx:xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - **Password**：任意で、デバイスのパスワードを入力します。
  - **[Add]** をクリックしてデバイスを追加するか、**[Cancel]** をクリックしてデバイスの追加を取り消します。
- **Whitelist ID**：この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーのデバイスで使用できるAirPlayデバイスのデバイスIDのみを追加できます。一覧に追加するAirPlayデバイスごとに、**[追加]** をクリックして以下の操作を行います。
  - **Device ID**：デバイスIDを「xx:xx:xx:xx:xx:xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - **[Add]** をクリックしてデバイスを追加するか、**[Cancel]** をクリックしてデバイスの追加を取り消します。

注：既存のデバイスを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存のデバイスを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[ユーザーにポリシーの削除を許可]** の一覧で、**[常に]**、**[パスワードが必要]**、**[しない]** のいずれかを選択しま

す。

- [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。

The screenshot shows the XenMobile configuration interface for an AirPlay Mirroring Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is divided into a sidebar and a main panel. The sidebar shows 'AirPlay Mirroring Policy' with sub-sections: 1 Policy Info, 2 Platforms (with 'Mac OS X' selected), and 3 Assignment. The main panel is titled 'Policy Information' and contains the following sections:

- AirPlay Password:** A table with columns 'Device Name\*' and 'Password\*', and an 'Add' button.
- Whitelist ID:** A table with a 'Device ID\*' column and an 'Add' button.
- Policy Settings:** Includes 'Remove policy' (radio buttons for 'Select date' and 'Duration until removal (in days)'), 'Allow user to remove policy' (dropdown menu set to 'Always'), and 'Profile scope' (dropdown menu set to 'User').
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right of the main panel, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **AirPlay Password** : 追加するデバイスごとに、 [Add] をクリックして以下の操作を行います。
  - **Device ID** : ハードウェアのアドレス (MACアドレス) を「xx:xx:xx:xx:xx:xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - **パスワード** : 任意で、デバイスのパスワードを入力します。
  - [追加] をクリックしてデバイスを追加するか、 [キャンセル] をクリックしてデバイスの追加を取り消します。
- **ホワイトリストID** : この一覧は、監視対象ではないデバイスでは無視されます。この一覧には、ユーザーのデバイスで使用できるAirPlayデバイスのデバイスIDのみを追加できます。一覧に追加するAirPlayデバイスごとに、 [追加] をクリックして以下の操作を行います。
  - **デバイスID** : デバイスIDを「xx:xx:xx:xx:xx:xx」の形式で入力します。このフィールドでは大文字と小文字が区別されません。
  - [Add] をクリックしてデバイスを追加するか、 [Cancel] をクリックしてデバイスの追加を取り消します。

注：既存のデバイスを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

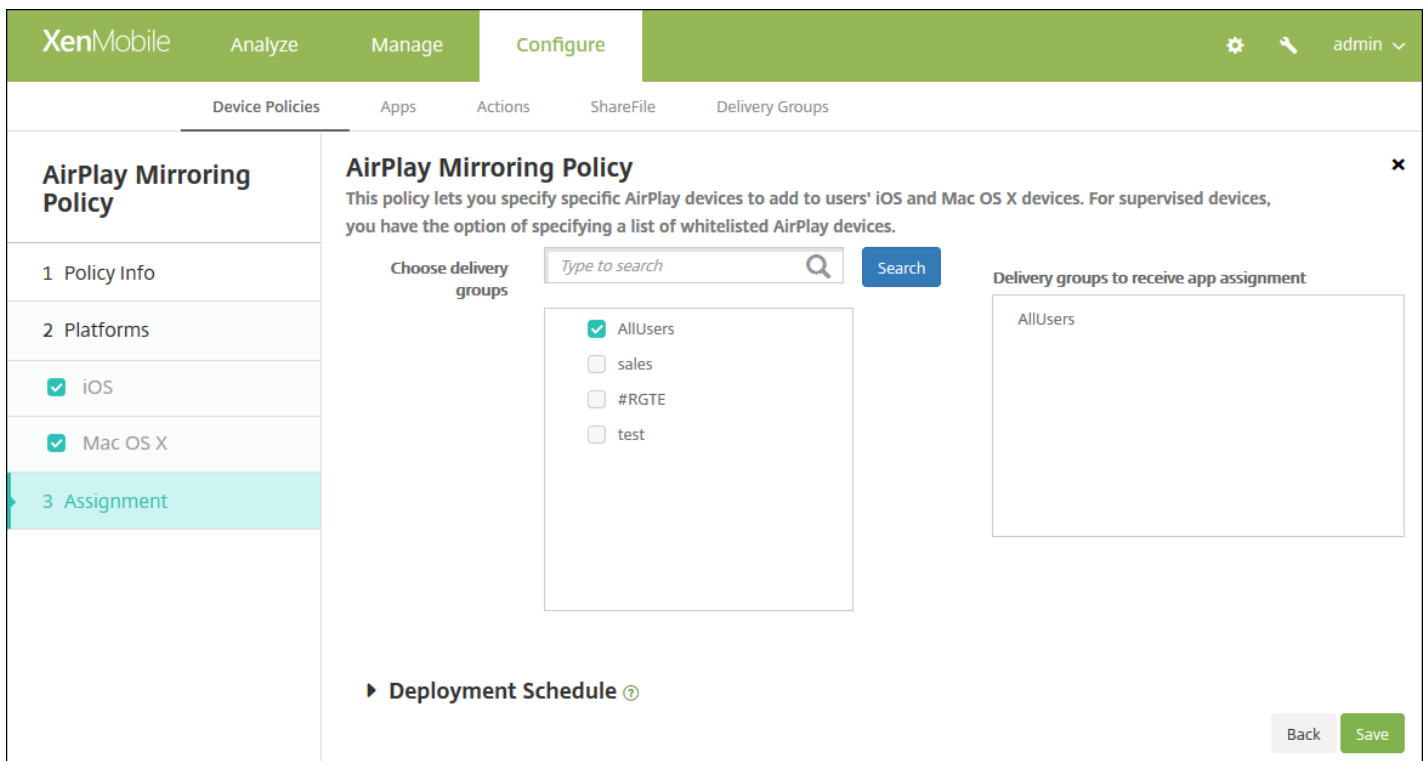
既存のデバイスを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックし

ます。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

- ポリシー設定

- [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
- [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。
- [Profile scope] の横にある、[User] または [System] を選択します。デフォルトは [User] です。

8. [Next] をクリックします。[AirPlay Mirroring Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。

- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# AirPrintデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、AirPrintプリンターをユーザーのiOSデバイスのAirPrintプリンター一覧に追加できます。このポリシーにより、プリンターとデバイスが異なるサブネットに存在している環境のサポートが容易になります。

注：

- このポリシーはiOS 7.0以降に適用されます。
- 各プリンターのIPアドレスとリソースパスがあることを確認してください。

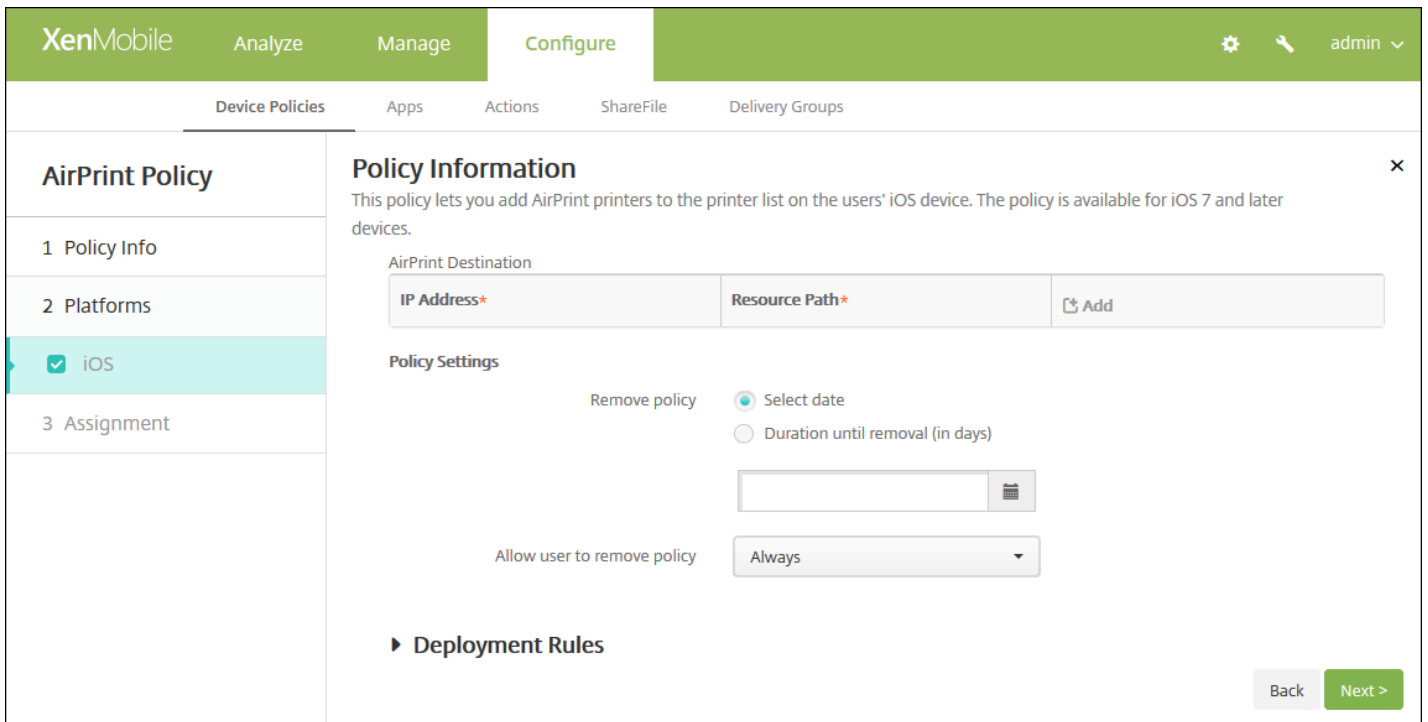
1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** をクリックした後、**[End user]** の下の **[AirPrint]** をクリックします。**[AirPrint Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'AirPrint Policy' and has a sidebar on the left with three sections: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. Under '1 Policy Info', there is a checkbox for 'iOS' which is checked. The main area is titled 'Policy Information' and contains a description: 'This policy lets you add AirPrint printers to the printer list on the users' iOS device. The policy is available for iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

5. **[Next]** をクリックします。**[iOS Platform Information]** ページが開きます。



6. 次の設定を構成します。

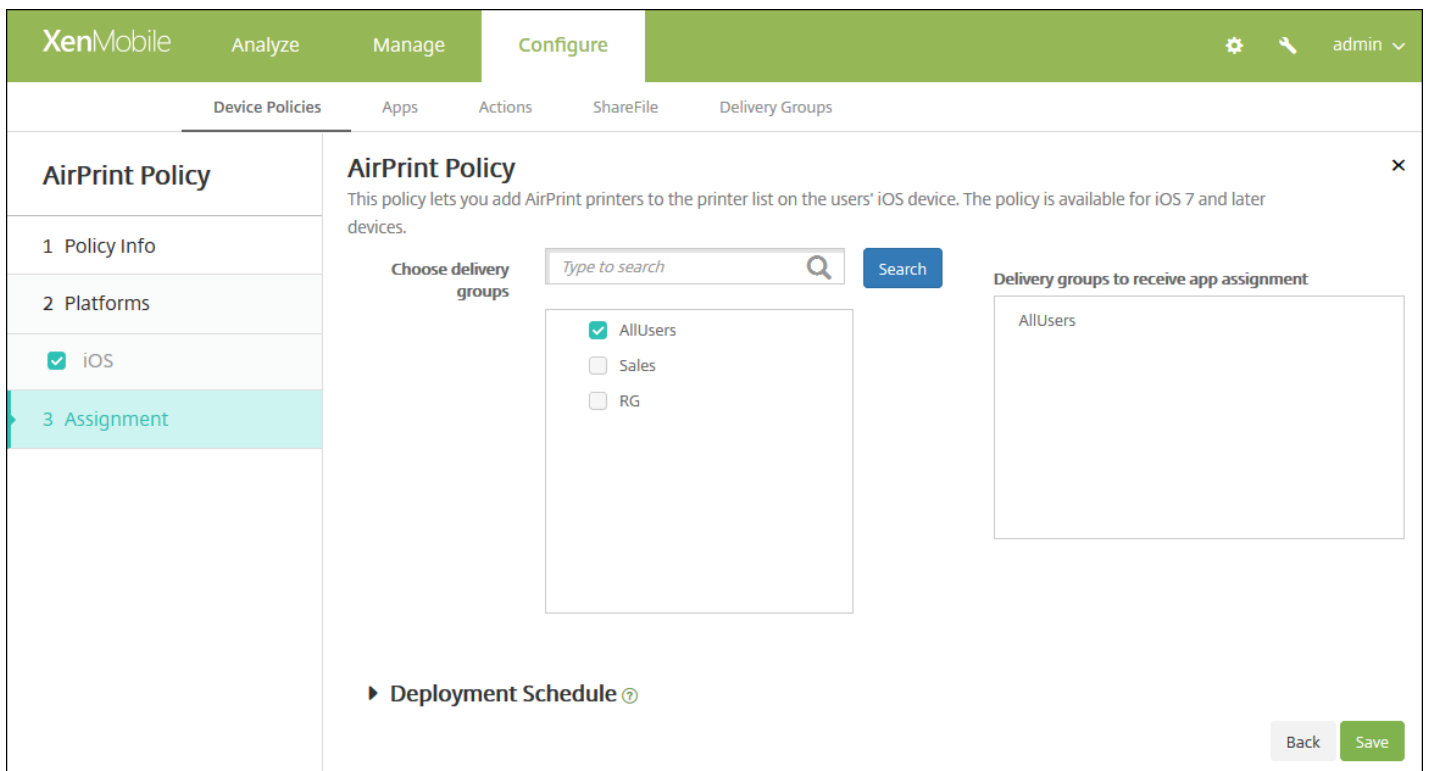
- **AirPrint Destination** : 追加するAirPrintの出力先ごとに、**[Add]** をクリックして以下の操作を行います。
  - **IP Address** : AirPrintプリンターのIPアドレスを入力します。
  - **Resource Path** : プリンターに関連付けられているリソースパスを入力します。この値は、\_ipps.tcpというBonjourレコードのパラメーターに対応します。たとえば、printers/Canon\_MG5300\_series or printers/Xerox\_Phaser\_7600。
  - **[Save]** をクリックしてプリンターを追加するか、**[Cancel]** をクリックしてプリンターの追加を取り消します。

注：既存のプリンターを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存のプリンターを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

- **ポリシー設定**
  - **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。

8. **[Next]** をクリックします。**[AirPrint Policy]** 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択されたグループは、[Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# Android for Workアプリ制限ポリシー

Apr 27, 2017

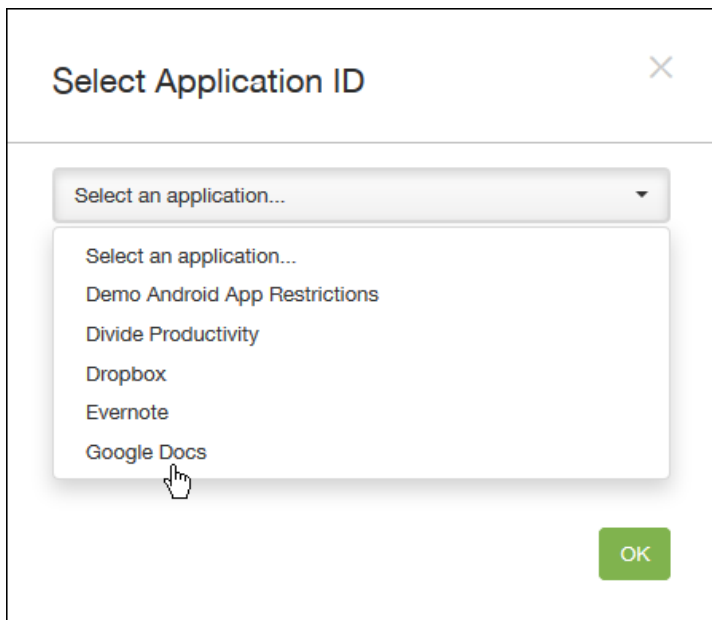
Android for Workアプリに関連する制限を変更できますが、そのためには、次の前提条件を満たす必要があります。

- GoogleのAndroid for Work設定タスクを完了します。詳しくは、「[Android for Workでのデバイスの管理](#)」を参照してください。
- Android for Workアカウントの作成詳しくは、「[Android for Workアカウントの作成](#)」を参照してください。
- Android for WorkアプリをXenMobileに追加します。詳しくは、「[XenMobileへのアプリケーションの追加](#)」を参照してください。

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。

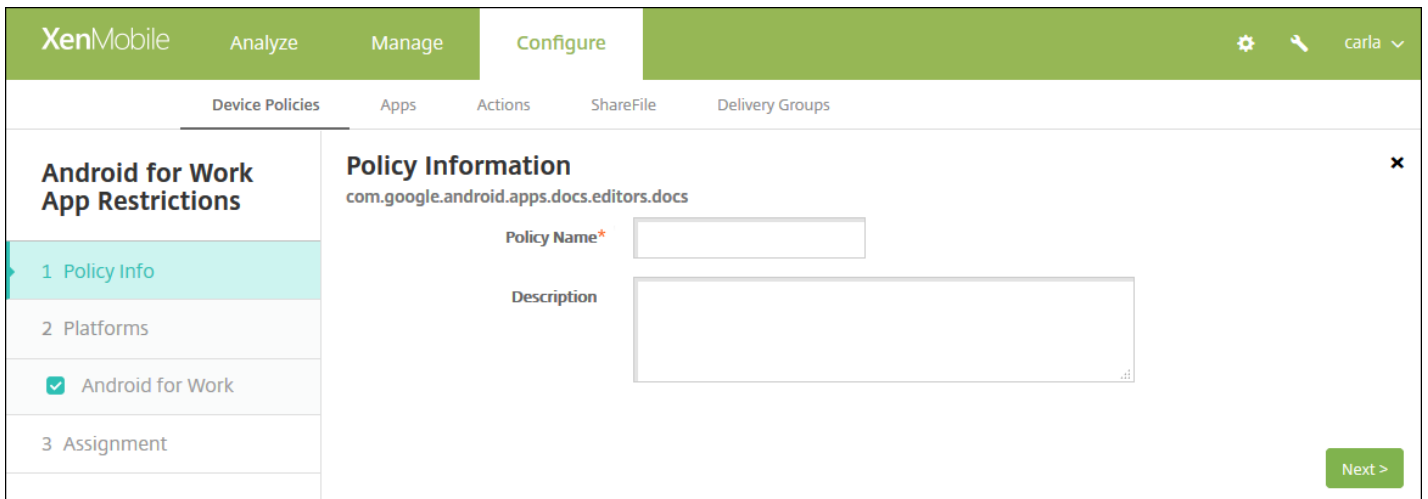
2. 新しいポリシーを追加するには **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。

3. **[More]** を展開し、**[Security]** で **[Android for Work App Restrictions]** をクリックします。アプリの選択を求めるダイアログボックスが開きます。



4. 一覧から、制限の適用先のアプリを選択して、**[OK]** をクリックします。

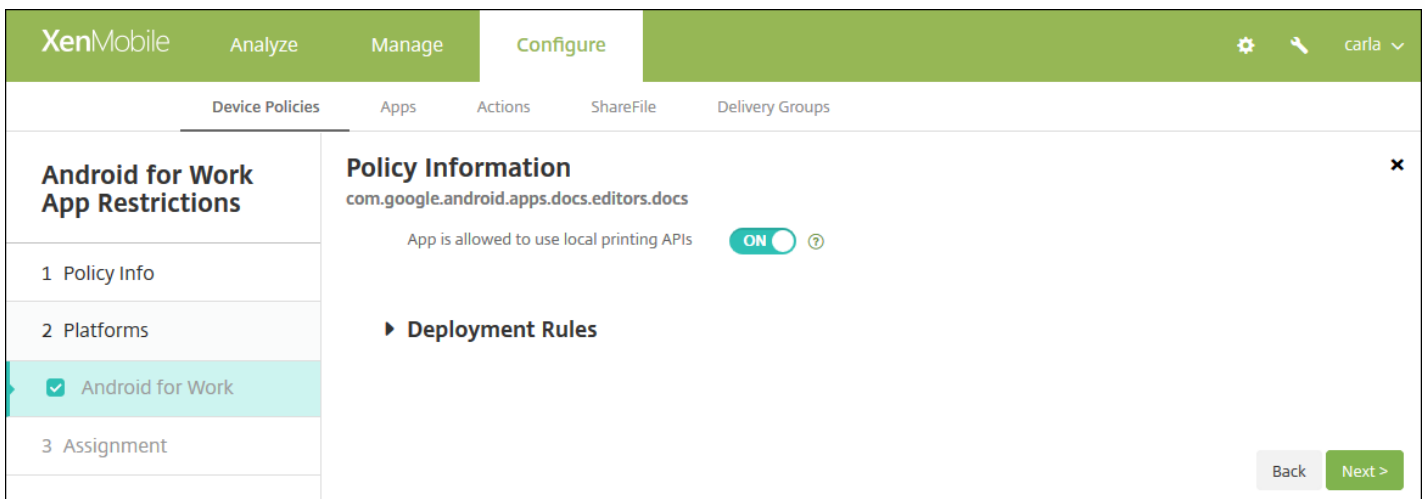
- XenMobileに追加されたAndroid for Workアプリがない場合は、続行できません。XenMobileへのアプリの追加について詳しくは、「[XenMobileへのアプリケーションの追加](#)」を参照してください。
- アプリに制限が関連付けられていない場合は、その効果についての通知が表示されます。**[OK]** をクリックして、このダイアログボックスを閉じます。
- アプリに制限が関連付けられている場合は、**[Android for WorkApp Restrictions Policy]** 情報ページが開きます。



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

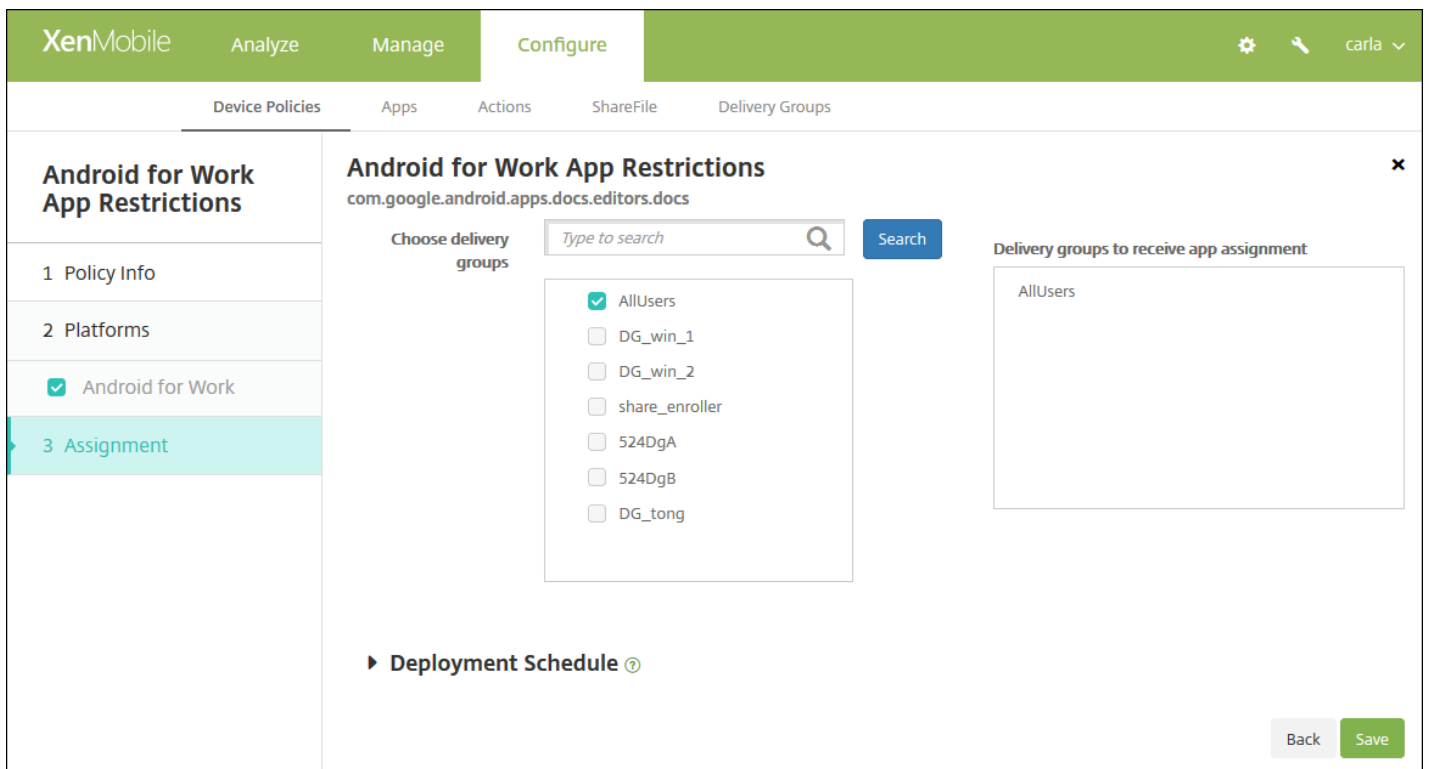
- **Policy Name** : ポリシーの説明的な名前を入力します。
- **説明** : 任意で、ポリシーの説明を入力します。

6. [Next] をクリックします。[Android for Work Platform] ページが開きます。



7. 選択したアプリケーションの設定を構成します。表示される設定は、選択したアプリに関連付けられている制限によって異なります。

9. [Next] をクリックします。[Android for Work App Restrictions Policy] 割り当てページが開きます。



10. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

12. [Save] をクリックします。

# APNデバイスポリシー

Apr 27, 2017

iOS、Android、Windows Mobile/CEデバイスのカスタムアクセスポイント名（APN）デバイスポリシーを追加できます。このポリシーは、モバイルデバイスからインターネットへの接続にコンシューマーAPNを使用しない組織で使用します。APNポリシーによって、特定の電話会社の汎用パケット無線サービス（General Packet Radio Service : GPRS）にデバイスを接続するときに使用される設定が決まります。ほとんどの新しい電話機において、この設定は既に定義されています。

## iOSの設定

## Androidの設定

## Windows Mobile/CEの設定

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** をクリックした後、**[Network access]** の下の **[APN]** をクリックします。**[APN Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure. The 'Configure' tab is active. Below the navigation, there are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The 'Device Policies' sub-tab is selected. The main content area is titled 'APN Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is expanded, showing a 'Policy Information' dialog box. The dialog box has a close button (X) in the top right corner. The text inside the dialog box reads: 'This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.' Below the text, there are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty, and the 'Description' field is also empty. At the bottom right of the dialog box, there is a green button labeled 'Next >'. The '2 Platforms' section in the sidebar shows three checkboxes: 'iOS', 'Android', and 'Windows Mobile/CE', all of which are checked. The '3 Assignment' section is partially visible below it.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。

注 : **[Policy Platforms]** ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォームが表示されます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'APN Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS', 'Android', and 'Windows Mobile/CE' are all checked. The 'Policy Information' section contains the following fields: 'APN\*' (with a lock icon), 'User name', 'Password' (with a key icon), 'Server proxy address', and 'Server proxy port'. The 'Policy Settings' section includes 'Remove policy' with radio buttons for 'Select date' (selected) and 'Duration until removal (in days)', a date picker, and 'Allow user to remove policy' with a dropdown menu set to 'Always'. A 'Deployment Rules' section is partially visible at the bottom. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **APN** : アクセスポイントの名前を入力します。これは承認されているiOSのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **User name** : このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password** : このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **Server proxy address** : APNプロキシのIPアドレスまたはURLです。
- **Server proxy port** : APNプロキシのポート番号です。サーバーのプロキシアドレスを入力した場合は必須です。
- [Policy Settings] の下の [Remove policy] の横にある、 [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。



XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### APN Policy

**Policy Information** ×

This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.

1 Policy Info

2 Platforms

iOS

**Android**

Windows Mobile/CE

3 Assignment

APN \*

User name

Password

Server

APN type

Authentication type: None

Server proxy address

Server proxy port

MMSC

Multimedia Messaging Server (MMS) proxy address

MMS port

► Deployment Rules

Back Next >

次の設定を構成します。

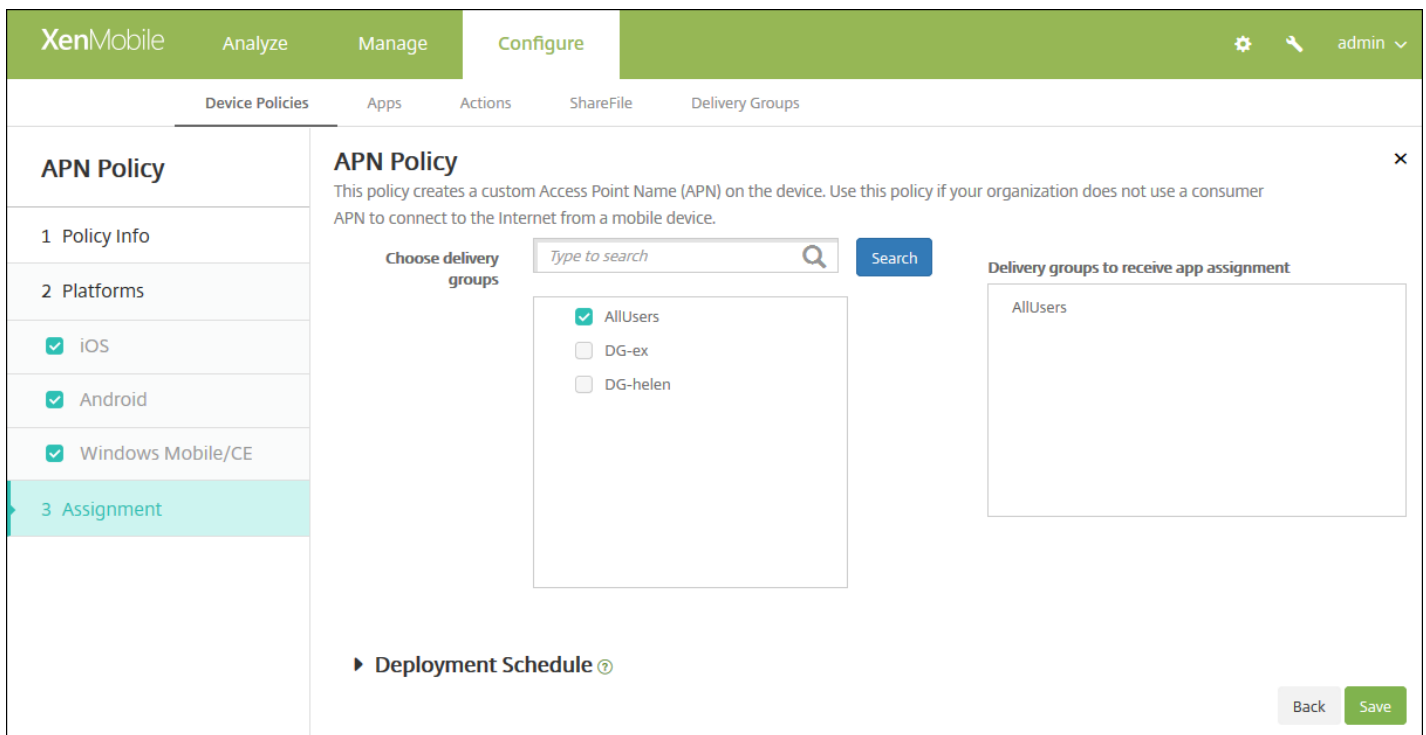
- **APN** : アクセスポイントの名前を入力します。これは承認されているAndroidのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **User name** : このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password** : このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。
- **Server** : この設定はスマートフォンに先行するもので、通常は空白です。標準のWebサイトにアクセスできない、または標準のWebサイトを表示できない電話機用のワイヤレスアプリケーションプロトコル (WAP) ゲートウェイサーバーを参照します。
- **APN type** : この設定は、電話会社が想定しているアクセスポイントの使用方法に一致している必要があります。内容はAPNサービス指定子のコンマ区切り文字列であり、携帯電話会社が公開している定義と一致している必要があります。以下に例を示します。
  - \*。すべてのトラフィックがこのアクセスポイントを経由します。
  - mms。マルチメディアトラフィックがこのアクセスポイントを経由します。
  - default。マルチメディアトラフィックを含め、すべてのトラフィックがこのアクセスポイントを経由します。
  - supl。SUPL (Secure User Plane Location) は補助GPSに関連付けられています。
  - dun。ダイヤルアップネットワークは古いため、ほとんど使用されません。
  - hipri。高優先度ネットワークです。

- fota。FOTA (Firmware over the air) は、ファームウェア更新の受信に使用されます。
- **Authentication type** : ボックスの一覧で、使用する認証の種類を選択します。デフォルトは [None] です。
- **Server proxy address** : 電話会社のAPN HTTPプロキシのIPアドレスまたはURLです。
- **Server proxy port** : APNプロキシのポート番号です。サーバーのプロキシアドレスを入力した場合は必須です。
- **MMSC** : 電話会社が提供するMMSゲートウェイサーバーのアドレスです。
- **Multimedia Messaging Server (MMS) proxy address** : これは、MMSトラフィック用のマルチメディアメッセージングサービスサーバーです。MMSはSMSの後継で、画像やビデオなどのマルチメディアコンテンツを含む大きいサイズのメッセージを送信できます。これらのサーバーは特定のプロトコルを必要とします (MM1、... MM11など) 。
- **MMS port** : MMSプロキシに使用されるポートです。

次の設定を構成します。

- **APN** : アクセスポイントの名前を入力します。これは承認されているAndroidのAPNと一致する必要があります。一致しない場合、ポリシーは機能しません。
- **Network** : 一覧から、使用するネットワークの種類を選択します。デフォルトは [Built-in office] です。
- **User name** : このAPNのユーザー名を指定する文字列です。ユーザー名がない場合、デバイスでは、プロファイルのインストール中に文字列の入力が求められます。
- **Password** : このAPNのユーザーのパスワードです。難読化のために、パスワードはエンコードされます。ペイロードにパスワードがない場合、デバイスでは、プロファイルのインストール中にパスワードの入力が求められます。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択されたグループは、[Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# アプリケーション属性デバイスポリシー

Apr 27, 2017

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

The screenshot shows the XenMobile 'Configure' page for 'App Attributes Policy'. The left sidebar has '1 Policy Info' selected. The main area is titled 'Policy Information' and contains a text input for 'Policy Name\*' and a larger text area for 'Description'. A 'Next >' button is at the bottom right.

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

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

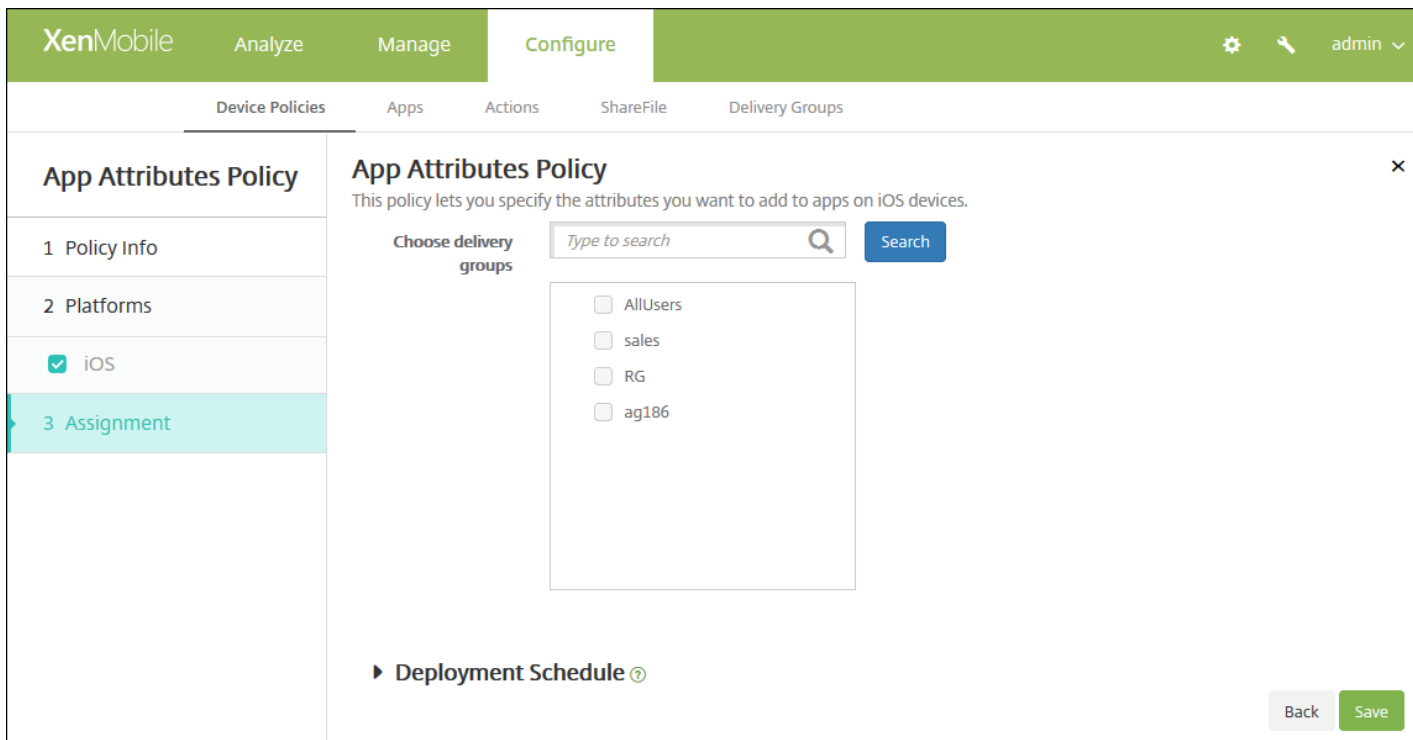
5. [Next] をクリックします。[App Attributes] プラットフォーム情報ページが開きます。

The screenshot shows the XenMobile 'Configure' page for 'App Attributes Policy'. The left sidebar has '2 Platforms' selected, and 'iOS' is checked. The main area shows 'Managed app bundle ID\*' with a dropdown menu set to 'Make a selection', and 'Per-app VPN identifier' with a dropdown menu set to 'None'. A 'Deployment Rules' section is partially visible. 'Back' and 'Next >' buttons are at the bottom right.

6. 次の設定を構成します。

- **Managed app bundle ID** : 一覧からアプリケーションバンドルIDを選択するか、[Add new] をクリックします。
  - [Add new] をクリックした場合は、表示されるフィールドにアプリケーションバンドルIDを入力します。
- **Per-app VPN identifier** : 一覧から、アプリケーションごとのVPN IDを選択します。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# アプリケーションアクセスデバイスポリシー

Apr 27, 2017

XenMobileのアプリケーションアクセスデバイスポリシーでは、デバイスへのインストールが必須のアプリケーション、デバイスにインストール可能なアプリケーション、デバイスへのインストールが禁止されるアプリケーションの一覧を定義できます。次に、そのアプリケーション一覧に準拠しているデバイスに対して行う自動化された操作を作成できます。アプリケーションアクセスポリシーは、iOS、Android、Windows Mobile/CEデバイスに対して作成できます。

アクセスポリシーは一度に1種類のみ構成できます。必須アプリケーション、推奨アプリケーション、禁止アプリケーションのいずれかの一覧のポリシーを追加できますが、同じアプリケーションアクセスポリシー内に混在させることはできません。一覧の種類ごとにポリシーを作成する場合、XenMobileでどのポリシーがどのアプリケーション一覧に適用されるかがわかるようにするため、各ポリシーの名前付けに注意することをお勧めします。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開し、**[Apps]** の下の **[App Access]** をクリックします。**[App Access Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Access Policy' and contains a 'Policy Information' section. This section has a sub-header 'Policy Information' and a description: 'This policy lets you create lists of apps that you designate as required, suggested, or forbidden by users to run on their devices.' Below the description, there are two input fields: 'Policy Name' (with a red asterisk) and 'Description'. The 'Policy Name' field is empty, and the 'Description' field is also empty. At the bottom right of the page, there is a green 'Next >' button.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

6. 選択したプラットフォームごとに、次の設定を構成します。

- **Access policy** : [Required]、[Suggested]、[Forbidden] のいずれかをクリックします。デフォルトは [Required] です。
- 1つまたは複数のアプリケーションを一覧に追加するには、[Add] をクリックして以下の操作を行います。
  - **App name** : アプリケーション名を入力します。
  - **App Identifier** : 任意で、アプリケーション識別子を入力します。
  - [Save] または [Cancel] をクリックします。
  - 追加するアプリケーションごとに上記の手順を繰り返します。

注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

8. [Next] をクリックします。次のプラットフォームのページまたは [App Access Policy] 割り当てページが開きます。

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# アプリケーション構成デバイスポリシー

Apr 27, 2017

管理された構成をサポートするアプリケーションをリモートで構成できます。XML構成ファイル（プロパティ一覧またはplisと呼ばれるファイル）をユーザーのiOSデバイスに展開するか、キー/値ペアをWindows 10 Phone、タブレット、またはデスクトップデバイスに展開できます。構成では、アプリのさまざまな設定や動作を指定します。XenMobileは、ユーザーがアプリをインストールしたデバイスに構成をプッシュします。実際に構成できる設定および動作はアプリケーションによって異なるため、このアールティクルでは扱いません。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ページが開きます。
3. [More] を展開し、[Apps] で [App Configuration] をクリックします。[App Configuration Policy] 情報ページが開きます。

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

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

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

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

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



XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Configuration Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

#### Policy Information

This policy lets you define a configuration of a managed app to be applied on the iOS device. After you enter the dictionary content, you can check the syntax.

Identifier\*

Dictionary content\*

► **Deployment Rules**

XenMobile Analyze Manage **Configure** administrator

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### App Configuration Policy

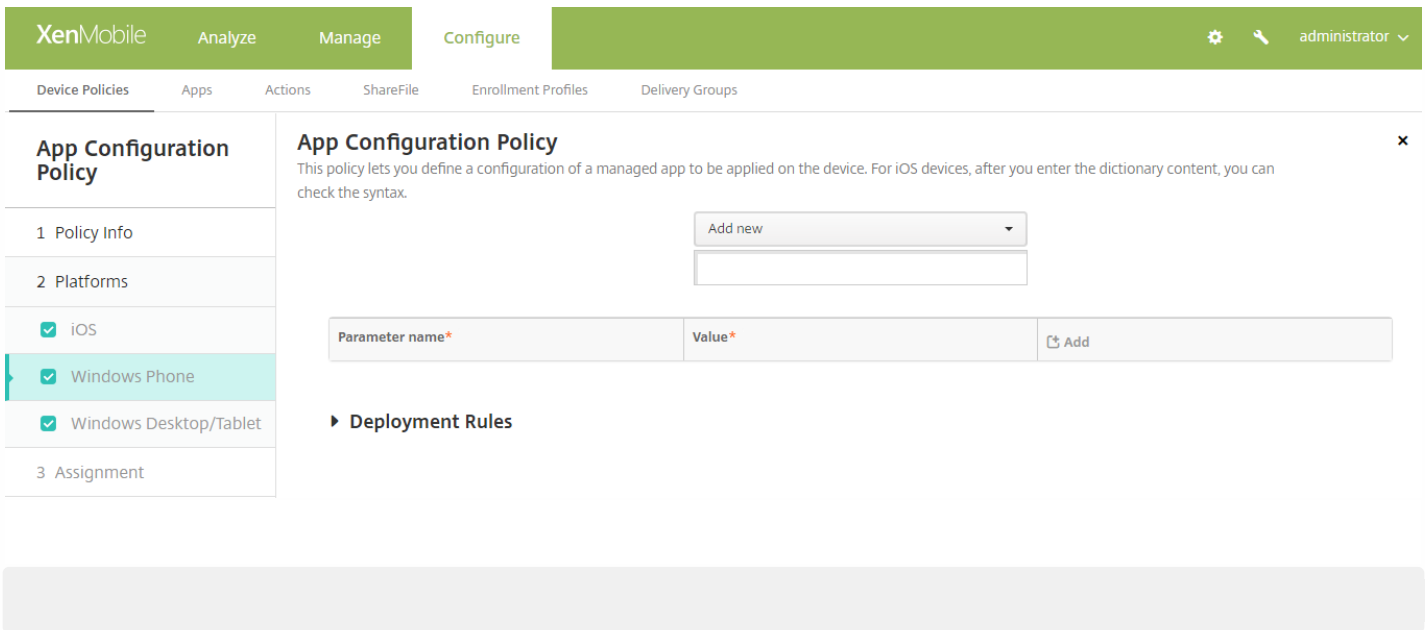
- 1 Policy Info
- 2 Platforms
  - iOS
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

#### App Configuration Policy

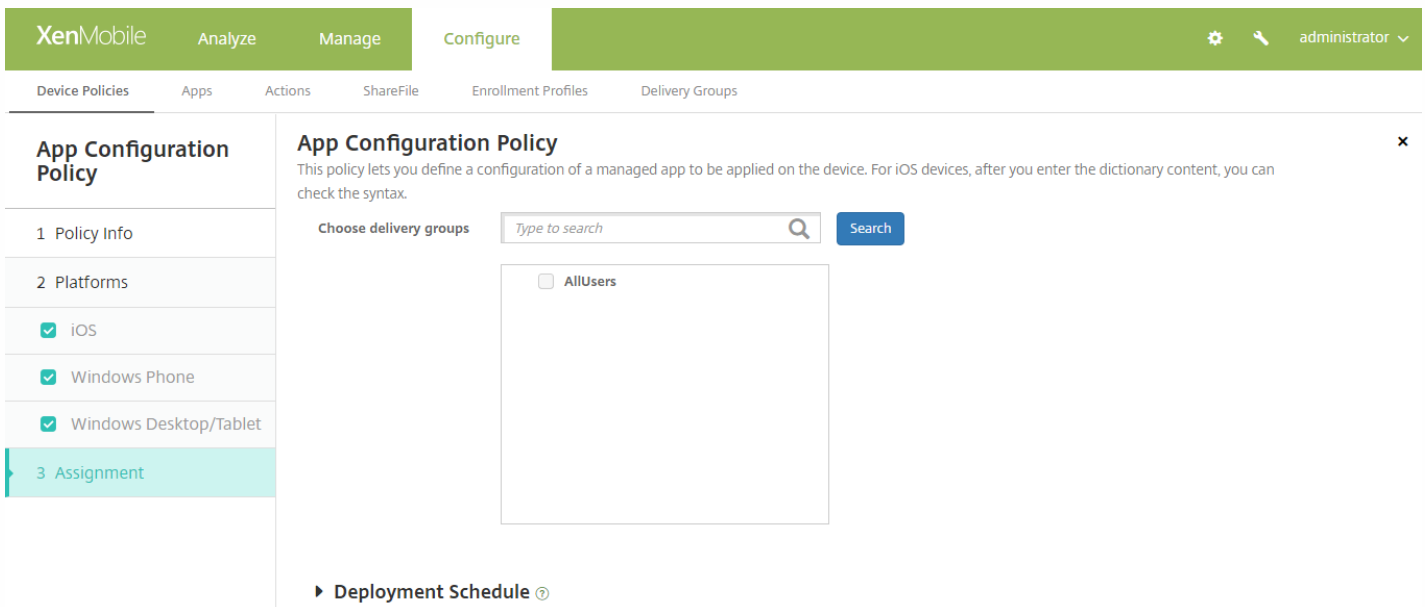
This policy lets you define a configuration of a managed app to be applied on the device. For iOS devices, after you enter the dictionary content, you can check the syntax.

Parameter name*	Value*	<input type="button" value="Add"/>

► **Deployment Rules**



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



8. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。

- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

10. [Save] をクリックします。

# アプリケーションインベントリデバイスポリシー

Apr 27, 2017

XenMobileのアプリケーションインベントリポリシーにより、管理されているデバイスのアプリケーションのインベントリ収集できます。その後、インベントリは、それらのデバイスに展開されたアプリケーションアクセスポリシーと比較されます。この方法で、アプリケーションのブラックリスト（アプリケーションアクセスポリシーで禁止）またはホワイトリスト（アプリケーションアクセスポリシーで必須）に表示されるアプリケーションを検出し、それに応じた操作を実行することができます。アプリケーションアクセスポリシーは、iOS、Mac OS X、Android（Android for Work対応デバイスを含む）、Windowsデスクトップ/タブレット、Windows Phone、Windows Mobile/CEデバイスに対して作成できます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。
3. **[More]** を展開し、**[Apps]** の下の **[App Inventory]** をクリックします。**[App Inventory Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Inventory Policy' and 'Policy Information'. On the left, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing a list of operating systems with checkboxes: iOS, Mac OS X, Android, Windows Desktop/Tablet, Windows Phone, and Windows Mobile/CE. All checkboxes are checked. The 'Policy Information' section on the right contains a 'Policy Name\*' text input field and a 'Description' text area. At the bottom right, there is a green 'Next >' button.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。

The screenshot shows the XenMobile configuration interface. At the top, there's a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there's a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Inventory Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Windows Desktop/Tablet, Windows Phone, and Windows Mobile/CE. All are checked. To the right, the 'Policy Information' section has a description and a toggle for 'ios' which is currently 'ON'. Below that is a 'Deployment Rules' section. At the bottom right, there are 'Back' and 'Next >' buttons.

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

6. 選択したプラットフォームごとに、デフォルト設定のままにしておくか、設定を[OFF] に変更します。デフォルトは [ON] です。

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

The screenshot shows the XenMobile configuration page for an App Inventory Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is titled 'App Inventory Policy' and includes a description: 'This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.' Below this, there are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked) and 'Sales' (unchecked). The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. Below this is a 'Deployment Schedule' section with a plus icon. At the bottom right are 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# アプリケーションロックデバイスポリシー

Apr 27, 2017

XenMobileでは、ポリシーを作成して、デバイスでの実行を許可するアプリの一覧、またはデバイスでの実行を禁止するアプリの一覧を定義できます。このポリシーは、iOSデバイスとAndroidデバイスの両方に対して構成できますが、ポリシーが実際にどのように機能するかは各プラットフォームで異なります。たとえば、iOSデバイスで複数のアプリを禁止することはできません。

また、iOSデバイスで選択できるiOSアプリは、ポリシーあたり1つのみです。これによって、デバイスで実行できるのは1つのアプリのみになります。アプリのロックポリシーが適用された場合に管理者が個別に許可したオプションを除いて、ユーザーはそのデバイスで他のアクティビティを実行できません。

また、iOSデバイスは、アプリのロックポリシーをプッシュするように監視される必要があります。

デバイスポリシーは大部分のAndroid LおよびMデバイスで機能しますが、アプリのロックは、必要なAPIがGoogleによって廃止されたため、Android N以降のデバイスでは機能しません。

## iOSの設定

## Androidの設定

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Security] の下の [App Lock] をクリックします。[App Lock Policy] ページが開きます。

4. [Policy Information] ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 必要に応じて、ポリシーの説明を入力します。
5. [Next] をクリックします。[Platforms] ページが開きます。

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。



XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

## App Lock Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Android
- 3 Assignment

### Policy Information

This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.

App bundle ID\*

#### Options

- Disable touch screen  ON iOS 7.0+
- Disable device rotation sensing  OFF iOS 7.0+
- Disable volume buttons  OFF iOS 7.0+
- Disable ringer switch  OFF iOS 7.0+
- Disable sleep/wake button  OFF iOS 7.0+
- Disable auto lock  OFF iOS 7.0+
- Enable VoiceOver  OFF iOS 7.0+
- Enable zoom  OFF iOS 7.0+
- Enable invert colors  OFF iOS 7.0+
- Enable AssistiveTouch  OFF iOS 7.0+
- Enable speak selection  OFF iOS 7.0+
- Enable mono audio  OFF iOS 7.0+

#### User Enabled Options

- Allow VoiceOver adjustment  OFF iOS 7.0+
- Allow zoom adjustment  OFF iOS 7.0+
- Allow invert colors adjustment  OFF iOS 7.0+
- Allow AssistiveTouch adjustment  OFF iOS 7.0+

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

#### Deployment Rules

次の設定を構成します。

- **App bundle ID** : 一覧からこのポリシーを適用するアプリケーションを選択するか、[Add new] をクリックして、新しいアプリケーションを一覧に追加します。[Add new] をクリックした場合は、表示されるフィールドにアプリケーション名を入力します。
- **Options** : 以下の各オプションは、iOS 7.0以降にのみ適用されます。[Disable touch screen] を除き、各オプションのデフォルトは [OFF] です ( [Disable touch screen] はデフォルトで [ON] に設定されています) 。
  - Disable touch screen
  - Disable device rotation sensing
  - Disable volume buttons
  - Disable ringer switch - 注 : このオプションが無効の場合、着信動作は、スイッチが最初に無効化されたときの場所に依存します。
  - Disable sleep/wake button
  - Disable auto lock
  - Disable VoiceOver
  - Enable zoom
  - Enable invert colors
  - Enable AssistiveTouch
  - Enable speak selection
  - Enable mono audio
- **User Enabled Options** : 以下の各オプションは、iOS 7.0以降にのみ適用されます。どのオプションも、デフォルトは [OFF] です。
  - Allow VoiceOver adjustment
  - Allow zoom adjustment
  - Allow invert colors adjustment
  - Allow AssitiveTouch adjustment
- **Policy Settings**
  - ○ [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - ○ [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - ○ [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - ○ [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

The screenshot shows the XenMobile configuration interface for an App Lock Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation tabs are 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'App Lock Policy' configuration steps: 1 Policy Info, 2 Platforms (with 'iOS' and 'Android' checked), and 3 Assignment. The main content area is titled 'Policy Information' and contains the following settings:

- App Lock parameters:**
  - Lock message: [Text input field]
  - Unlock password: [Text input field]
  - Prevent uninstall: [OFF] (toggle)
  - Lock screen: [Text input field] [Browse]
- Enforce:**
  - Blacklist (selected)
  - Whitelist
- Apps:**
  - App name\*: [Text input field] [Add]

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

次の設定を構成します。

- **App Lock parameters**
  - **Lock message** : ユーザーがロックされているアプリケーションを開こうとしたときに表示されるメッセージを入力します。
  - **Unlock password** : アプリケーションのロックを解除するパスワードを入力します。
  - **Prevent uninstall** : ユーザーにアプリケーションのアンインストールを許可するかどうかを選択します。デフォルトは [OFF] です。
  - **Lock screen** : [Browse] をクリックして、デバイスのロック画面に表示するイメージファイルの場所へ移動し、ファイルを選択します。
  - **Enforce** : [Blacklist] をクリックしてデバイスでの実行を禁止するアプリケーションの一覧を作成するか、[Whitelist] をクリックしてデバイスでの実行を許可するアプリケーションの一覧を作成します。
- **Apps** : [Add] をクリックして、以下の操作を行います。
  - **App name** : 一覧からホワイトリストまたはブラックリストに追加するアプリケーションの名前を選択するか、[Add new] をクリックして、選択可能なアプリケーションの一覧に新しいアプリケーションを追加します。
  - [Add new] をクリックした場合は、表示されるフィールドにアプリケーション名を入力します。
  - [Save] または [Cancel] をクリックします。
  - ホワイトリストまたはブラックリストに追加するアプリケーションごとに、上記の手順を繰り返します。

注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをク

リックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

8. [Next] をクリックします。[App Lock Policy] 割り当てページが表示されます。

The screenshot shows the XenMobile configuration interface for an App Lock Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Lock Policy' and includes a description: 'This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.' The 'Choose delivery groups' section has a search bar and a list of groups: AllUsers (checked), sales, RG, and ag186. The 'Delivery groups to receive app assignment' section shows 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

ます。ただしiOSには、 [Deploy for always on connection] は適用されません。

11. [Save] をクリックします。

# アプリケーションネットワーク使用状況デバイスポリシー

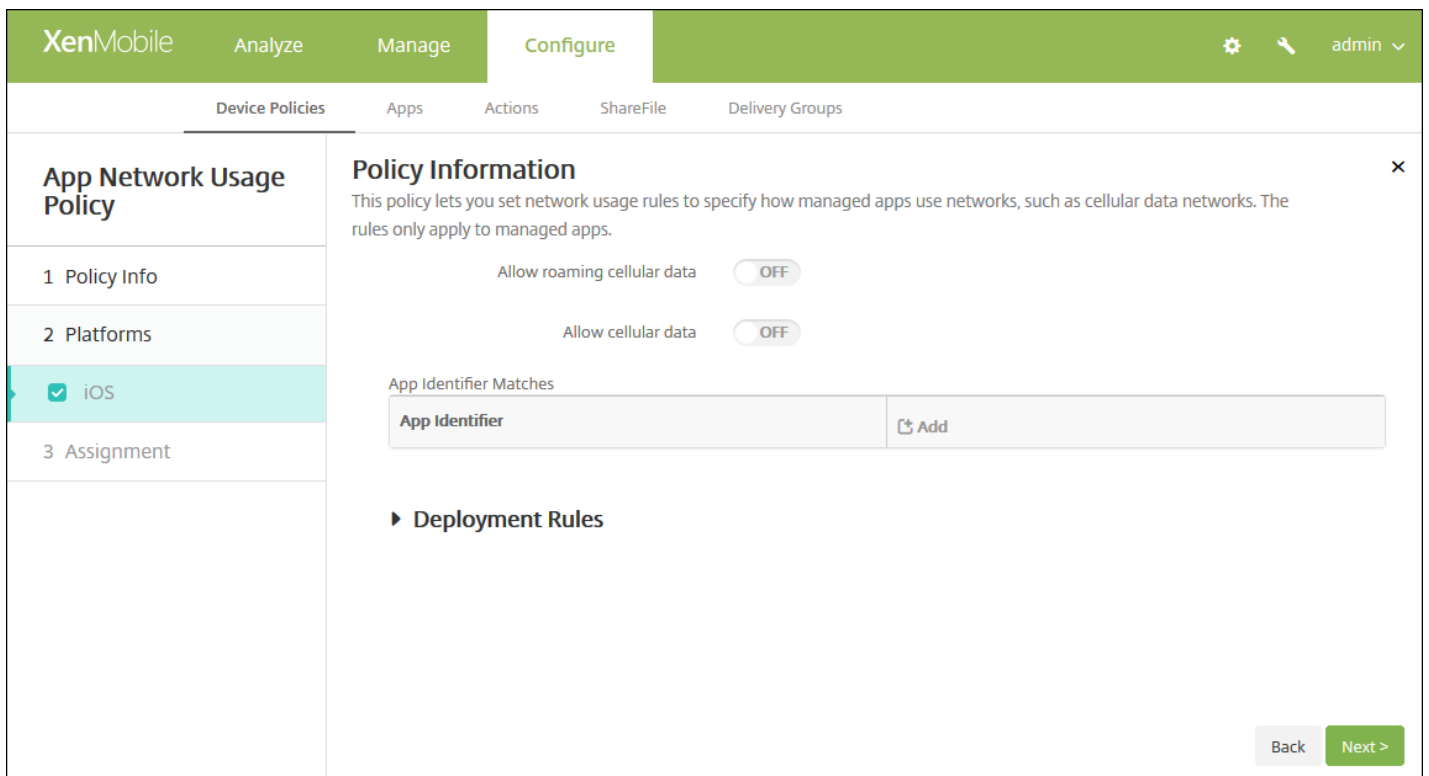
Apr 27, 2017

ネットワーク使用状況規則を設定して、iOSデバイスで管理対象のアプリケーションが携帯データネットワークなどのネットワークをどのように使用するかを指定できます。規則は管理対象のアプリケーションにのみ適用されます。管理対象のアプリケーションとは、XenMobileを使用してユーザーのデバイスに展開されるアプリケーションです。これには、ユーザーがXenMobileを使用して展開することなく直接デバイスにダウンロードしたアプリケーションや、デバイスのXenMobileへの登録時に既にデバイスにインストールされていたアプリケーションは含まれません。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。
2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開し、 **[Apps]** で **[App Network Usage]** をクリックします。 **[App Network Usage Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Network Usage Policy' and contains a 'Policy Information' section. This section includes a description and two input fields: 'Policy Name\*' and 'Description'. A sidebar on the left shows a progress indicator with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' step is active. Under '2 Platforms', 'iOS' is selected. A 'Next >' button is located at the bottom right.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



6. 次の設定を構成します。

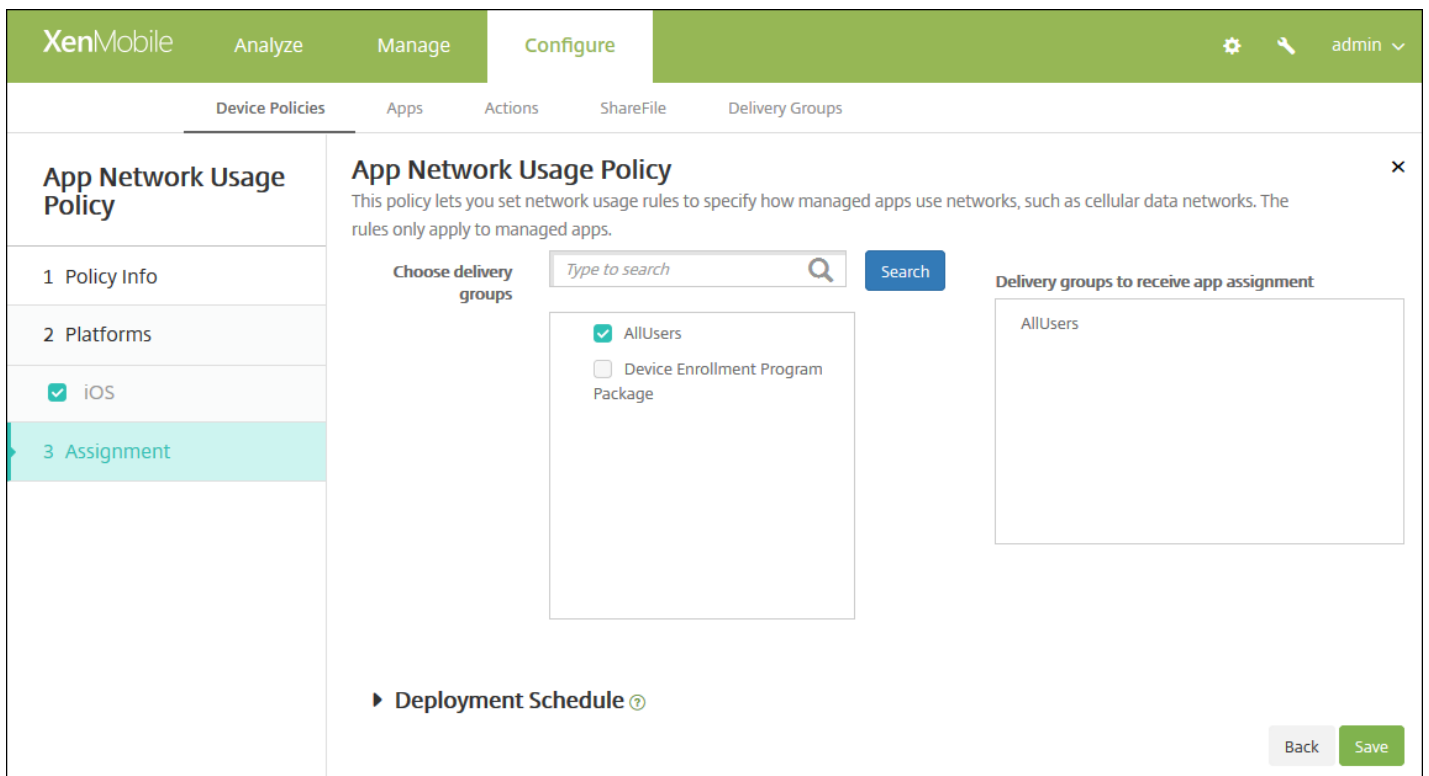
- **Allow roaming cellular data** : 指定したアプリケーションに、ローミング中に携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは **[OFF]** です。
- **Allow cellular data** : 指定したアプリケーションに、携帯データネットワーク接続を使用することを許可するかどうかを選択します。デフォルトは **[OFF]** です。
- **App Identifier Matches** : 一覧に追加するアプリケーションごとに、**[Add]** をクリックして以下の操作を行います。
  - **App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

注 : 既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

## 7. 展開規則を構成します

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。



# アプリケーション制限デバイスポリシー

Apr 27, 2017

ユーザーによるSamsung KNOXデバイスへのインストールを禁止するアプリケーションのブラックリストを作成したり、ユーザーによるインストールを許可するアプリケーションのホワイトリストを作成したりできます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Security] の下の [App Restrictions] をクリックします。[App Restrictions Policy] 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

#### Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Policy Name\*

Description

Next >

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

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

5. [Next] をクリックします。[Samsung KNOXプラットフォーム] ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Restrictions Policy

- 1 Policy Info
- 2 Platforms
- Samsung KNOX
- 3 Assignment

#### Policy Information

This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.

Allow/Deny	New app restriction*	Add
		<input type="button" value="Add"/>

► Deployment Rules

Back Next >

6. [Allow/Deny] の一覧に追加するアプリケーションごとに、[Add] をクリックして以下の操作を行います。

- **Allow/Deny** : ユーザーにアプリケーションのインストールを許可するかどうかを選択します。
- **New app restriction** : アプリケーションパッケージID (例: com.kmdmaf.crackle) を入力します。
- [Allow/Deny] の一覧にアプリケーションを保存する場合は [保存] をクリックし、保存しない場合は [キャンセル] をクリックします。

注: 既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

## 7. 展開規則を構成します。

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

The screenshot displays the XenMobile configuration interface for an App Restrictions Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Restrictions Policy' and includes a description: 'This policy lets you create blacklists for apps you want to prevent users from installing on Samsung KNOX devices, as well as whitelists for apps you want to allow users to install.' Under 'Choose delivery groups', there is a search bar and a list of groups: 'AllUsers' (checked) and 'sales' (unchecked). To the right, 'Delivery groups to receive app assignment' shows 'AllUsers' in a list. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。

- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# アプリケーショントンネリングデバイスポリシー

Apr 27, 2017

アプリトンネルは、モバイルアプリケーションのサービスの継続性およびデータ転送の信頼性を向上させるように設計されています。アプリトンネルは、モバイルデバイスアプリケーションのクライアントコンポーネントとアプリケーションサーバコンポーネント間のプロキシパラメーターを定義します。また、アプリトンネルを使用して、デバイスへのリモートサポートトンネル（管理のサポートに使用）も作成できます。アプリケーショントンネリングポリシーは、AndroidデバイスおよびWindows Mobile/CEデバイスに対して構成できます。

注：このポリシーで定義したトンネルを使用して送信されるアプリケーショントラフィックは、XenMobileを経由してから、アプリケーションを実行するサーバーにリダイレクトされます。

## Androidの設定

## Windows Mobile/CEの設定

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Network access] の下の [Tunnel] をクリックします。[Tunnel Policy] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below the tabs, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is active, and the 'Tunnel Policy' page is displayed. The page has a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing 'Android' and 'Windows Mobile/CE' with checkboxes that are checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. [Policy Information] ペインで、以下の情報を入力します。
    - Policy Name : ポリシーの説明的な名前を入力します。
    - Description : 任意で、ポリシーの説明を入力します。
  5. [Next] をクリックします。[Policy Platforms] ページが開きます。
  6. [Platforms] で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。
- 1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile administration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Configure' tab is active, and the 'Tunnel Policy' section is selected in the sidebar. The main content area is titled 'Policy Information' and contains the following configuration options:

- Use this tunnel for remote support:** A toggle switch set to 'OFF'.
- Connection configuration:**
  - Connection initiated by:** A dropdown menu set to 'Device'.
  - Maximum connections per device\*:** A text input field containing the number '1'.
  - Define connection time out:** A toggle switch set to 'OFF'.
  - Block cellular connections passing by this tunnel:** A toggle switch set to 'OFF'.
- App device parameters:**
  - Client port\*:** An empty text input field.
- App server parameters:**
  - IP address or server name\*:** An empty text input field.
  - Server port\*:** An empty text input field.

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- [Use this tunnel for remote support] : トンネルをリモートサポートで使用するかどうかを選択します。  
注 : リモートサポートを選択するかどうかによって、構成手順が異なります。
- リモートサポートを選択しない場合、以下の手順を実行します。
  - Connection initiated by : 一覧から [Device] または [Server] を選択して、接続の開始元を指定します。
  - Maximum connections per device : 数値を入力して、アプリケーションが確立できる同時TCP接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - Define connection time out : アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - Connection time out : [Define connection time out] を [On] に設定した場合に、アプリケーションのアイドル状態を継続できる時間 (秒) を入力します。この時間を超えると、トンネルは閉じられます。
  - Block cellular connections passing by this tunnel : ローミング中、このトンネルをブロックするかどうかを選択します。  
注 : WiFiおよびUSB接続はブロックされません。
  - Client port : クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
  - IP address or server name : アプリケーションサーバーのIPアドレスまたは名前を入力します。このフィールドはデバ

イスで開始する接続にのみ適用されます。

- **Server port** : サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - **Use this tunnel for remote support** : [On] に設定します。
  - **Define connection time out** : アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out** : [Define connection time out] を [On] に設定した場合に、アプリケーションのアイドル状態を継続できる時間 (秒) を入力します。この時間を超えると、トンネルは閉じられます。
  - **Use SSL connection** : このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **Block cellular connections passing by this tunnel** : ローミング中、このトンネルをブロックするかどうかを選択します。

注 : WiFiおよびUSB接続はブロックされません。

The screenshot shows the XenMobile web interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Tunnel Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are checked. The 'Policy Information' section is expanded, showing the following settings:

- Use this tunnel for remote support**: OFF
- Connection configuration**
  - Connection initiated by**: Device
  - Protocol**: Generic TCP
  - Maximum connections per device\***: 1
  - Define connection time out**: OFF
  - Block cellular connections passing by this tunnel**: OFF
- App device parameters**
  - Redirect to XenMobile**: Through app settings
  - Client port\***: (empty field)
- App server parameters**
  - IP address or server name\***: (empty field)
  - Server port\***: (empty field)

At the bottom of the configuration area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

次の設定を構成します。

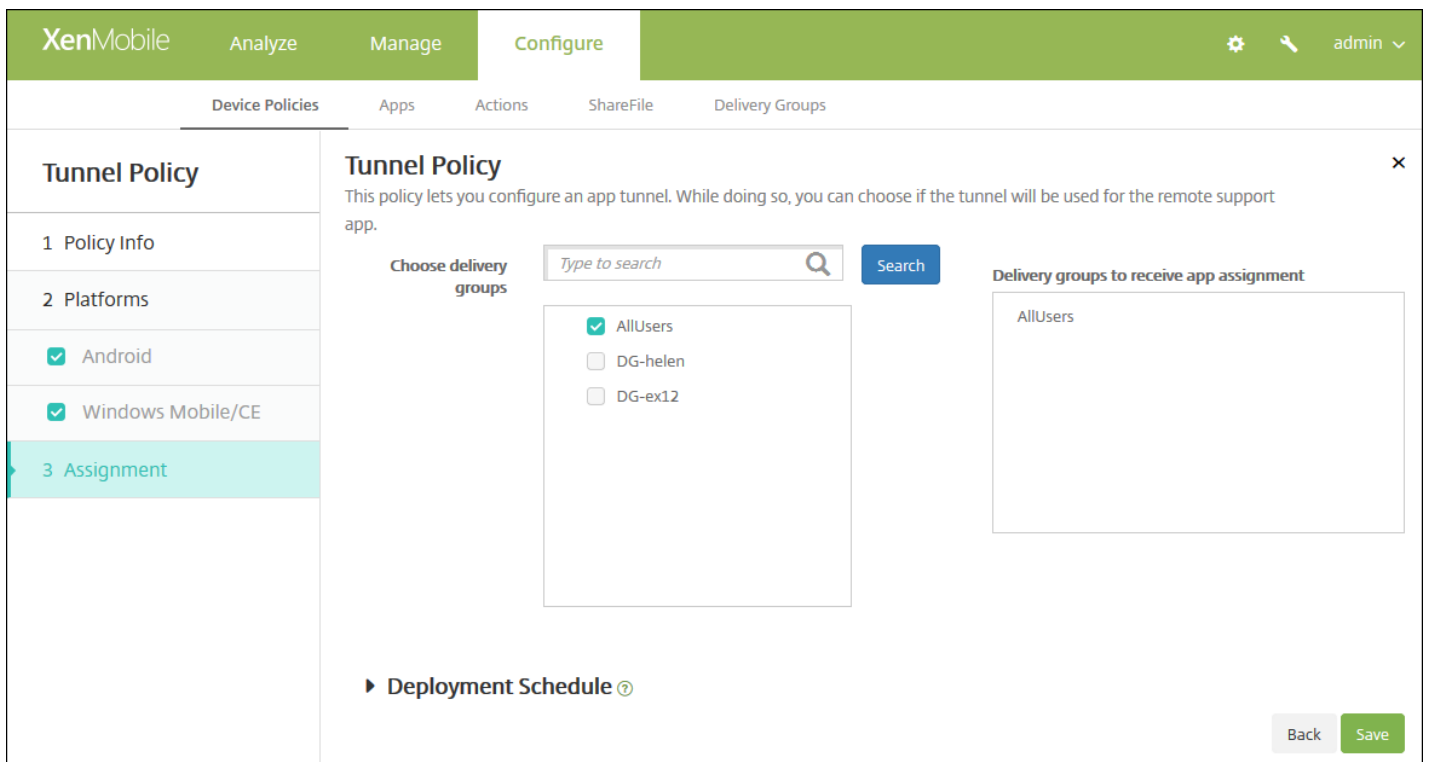
- [Use this tunnel for remote support] : トンネルをリモートサポートで使用するかどうかを選択します。

注：リモートサポートを選択するかどうかによって、構成手順が異なります。

- リモートサポートを選択しない場合、以下の手順を実行します。
  - **Connection initiated by**：一覧から [Device] または [Server] を選択して、接続の開始元を指定します。
  - **Protocol**：一覧で使用するプロトコルを選択します。デフォルトは [Generic TCP] です。
  - **Maximum connections per device**：数値を入力して、アプリケーションが確立できる同時TCP接続数を指定します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**：[Define connection time out] を [On] に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。  
注：WiFiおよびUSB接続はブロックされません。
- **Redirect to XenMobile**：一覧から、XenMobileへのデバイスの接続方法を選択します。デフォルトは [Through app settings] です。
  - [Using a local alias] を選択した場合は、[Local alias] にエイリアスを入力します。デフォルト値は [localhost] です。
  - [An IP address range] を選択した場合は、[IP address range from] に開始IPアドレスを入力し、[IP address range to] に終了IPアドレスを入力します。
  - **Client port**：クライアントのポート番号を入力します。ほとんどの場合、この値はサーバーポートと同じです。
  - **IP address or server name**：アプリケーションサーバーのIPアドレスまたは名前を入力します。このフィールドはデバイスで開始する接続にのみ適用されます。
  - **Server port**：サーバーのポート番号を入力します。
- リモートサポートを選択する場合、以下の手順を実行します。
  - **Use this tunnel for remote support**：[On] に設定します。
  - **Define connection time out**：アプリケーションのアイドル状態を継続できる時間を設定するかどうかを選択します。この時間を超えると、トンネルは閉じられます。
    - **Connection time out**：[Define connection time out] を [On] に設定した場合に、アプリケーションのアイドル状態を継続できる時間（秒）を入力します。この時間を超えると、トンネルは閉じられます。
  - **Use SSL connection**：このトンネルで、安全なSSL接続を使用するかどうかを選択します。
  - **Block cellular connections passing by this tunnel**：ローミング中、このトンネルをブロックするかどうかを選択します。  
注：WiFiおよびUSB接続はブロックされません。

## 7. 展開規則を構成します。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# アプリケーションアンインストールデバイスポリシー

Apr 27, 2017

iOS、Android、Samsung KNOX、Android for Work、Windowsデスクトップ/タブレット、およびWindows Mobile/CEのプラットフォームに対するアプリケーションアンインストールポリシーを作成できます。アプリケーションアンインストールポリシーにより、さまざまな理由でユーザーのデバイスからアプリケーションを削除できます。この理由には、特定のアプリケーションをサポートしなくなったことや、会社が既存アプリケーションから異なるベンダーが提供する類似アプリケーションへの置き換えを希望していることなどがあります。このポリシーがユーザーのデバイスに展開されると、アプリケーションが削除されます。Samsung KNOX以外のデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージが表示されます。Samsung KNOXデバイスでは、ユーザーにアプリケーションのアンインストールを求めるメッセージは表示されません。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Apps] の下の [App Uninstall] をクリックします。[App Uninstall Policy] ページが開きます。

The screenshot shows the 'App Uninstall Policy' configuration page in the XenMobile console. The page is divided into a sidebar and a main content area. The sidebar on the left is titled 'App Uninstall Policy' and contains three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are six checkboxes, all of which are checked: 'iOS', 'Android', 'Samsung KNOX', 'Android for Work', 'Windows Desktop/Tablet', and 'Windows Mobile/CE'. The main content area is titled 'Policy Information' and contains a sub-header 'Policy Information' followed by a description: 'This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.' Below this description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is a text input box, and the 'Description' field is a larger text area with a small icon in the bottom right corner. At the bottom right of the page, there is a green button labeled 'Next >'.

4. [ポリシー情報] ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Policy Platforms] ページが開きます。
6. [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing a list of platforms with checkboxes: iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet, and Windows Mobile/CE. The 'Policy Information' section contains a description and a 'Managed app bundle ID' field with a dropdown menu. The 'Deployment Rules' section is currently collapsed. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Managed app bundle ID** : 一覧で、既存のアプリケーションを選択するか、[Add new] をクリックします。このプラットフォームに対してアプリケーションが構成されていない場合は一覧が空になるため、新しいアプリケーションを追加する必要があります。
- [Add] をクリックすると、アプリケーション名を入力できるフィールドが表示されます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Uninstall Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Android
  - Samsung KNOX
  - Android for Work
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.

Apps to uninstall

App Name *	Add
------------	-----

► Deployment Rules

Back Next >

次の設定を構成します。

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

注：アンインストールポリシーから既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

#### 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration page for an 'App Uninstall Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a navigation menu with '1 Policy Info', '2 Platforms', and '3 Assignment' (highlighted). The main content area is titled 'App Uninstall Policy' and contains a description: 'This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.' Below the description is a 'Choose delivery groups' section with a search input field and a 'Search' button. A list of delivery groups is shown with checkboxes: 'AllUsers' and 'Sales'. Below this is a 'Deployment Schedule' section with a help icon. At the bottom right, there are 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# アプリケーションアンインストール制限デバイスポリシー

Apr 27, 2017

ユーザーにSamsung SAFEデバイスまたはAmazonデバイスでのアンインストールを許可するアプリケーションを指定することができます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Apps] で [AppUninstall Restrictions] をクリックします。[App Uninstall Restrictions Policy] 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Uninstall Restrictions Policy

1 Policy Info

2 Platforms

Samsung SAFE

Amazon

3 Assignment

#### Policy Information

This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

Policy Name\*

Description

Next >

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[ポリシープラットフォーム] ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### App Uninstall Restrictions Policy

1 Policy Info

2 Platforms

Samsung SAFE

Amazon

3 Assignment

#### Policy Information

This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.

App Uninstall Restriction Settings

App Name*	Rule	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Deployment Rules

Back Next >

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、次の設定を構成します。

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

注：既存のアプリを削除するには、その項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

## 8. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'App Uninstall Restrictions Policy' and includes a description: 'This policy lets you specify the apps users can or cannot uninstall on a Samsung SAFE or Amazon device.' There is a 'Choose delivery groups' section with a search input field and a 'Search' button. Below this, there are two radio button options: 'AllUsers' and 'Device Enrollment Program Package'. At the bottom right, there are 'Back' and 'Save' buttons. On the left side, there is a sidebar with a list of steps: '1 Policy Info', '2 Platforms', '3 Assignment', and 'Deployment Schedule'.

10. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

12. [Save] をクリックします。





以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

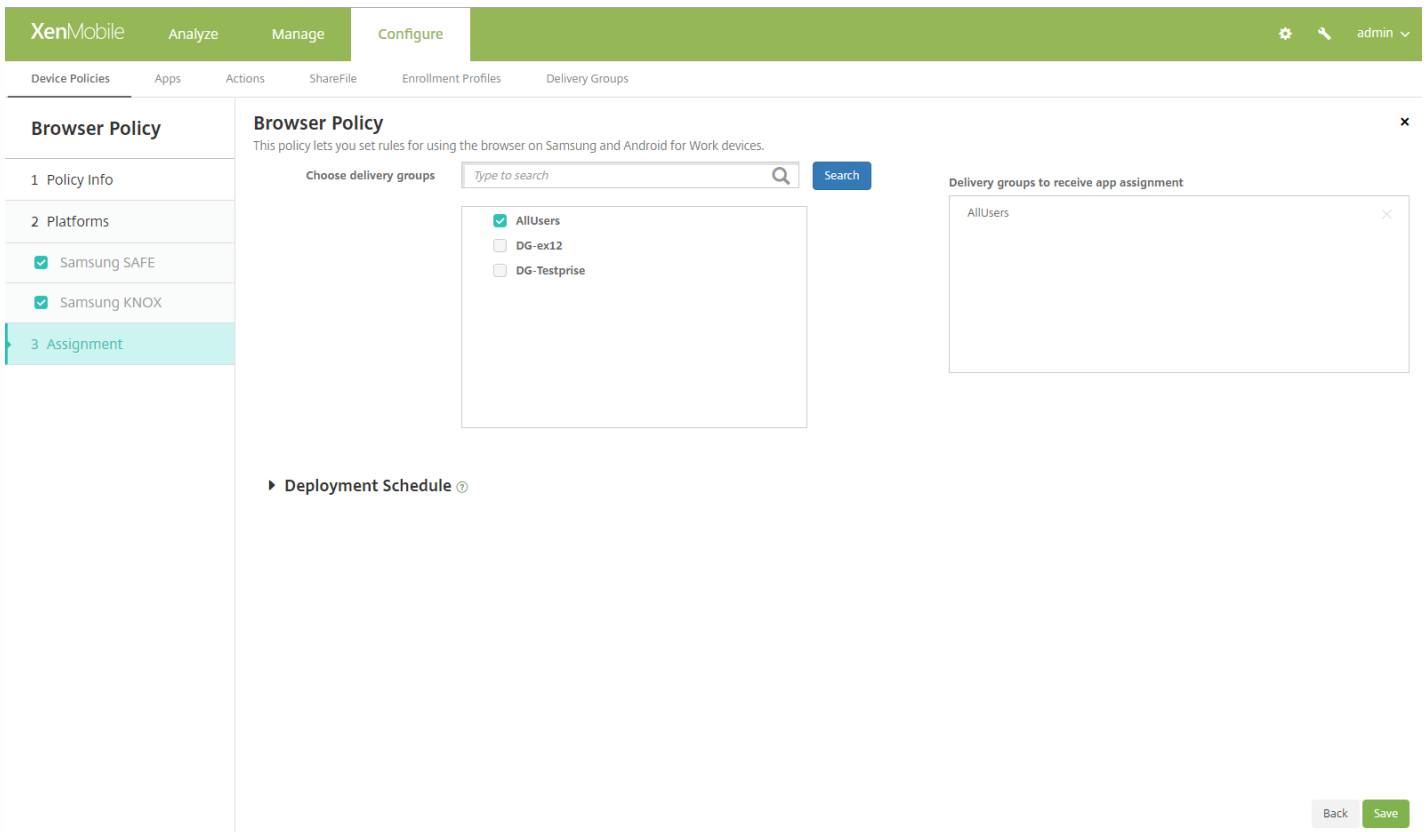
The screenshot shows the XenMobile Configure interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Browser Policy' and includes a description: 'This policy lets you set rules for using the browser on Samsung and Android for Work devices.' There are six toggle switches, all currently set to 'OFF': 'Disable browser', 'Disable pop-up', 'Disable Javascript', 'Disable cookies', 'Disable autofill', and 'Force fraud warning'. Below these is a section for 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Disable browser** : ユーザーのデバイスでSamsungブラウザ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を使用できます。ブラウザを無効にした場合、以下のオプションは表示されなくなります。
- **Disable pop-up** : ブラウザーでポップアップメッセージを許可するかどうかを選択します。
- **Disable Javascript** : ブラウザーでJavaScriptの実行を許可するかどうかを選択します。
- **Disable cookies** : Cookieを許可するかどうかを選択します。
- **Disable autofill** : ユーザーがブラウザのオートフィル機能をオンにできるかどうかを選択します。
- **Force fraud warning** : ユーザーが不正な、または信頼できないWebサイトを参照したときに、警告メッセージを表示するかどうかを選択します。

#### 7. 展開規則を構成します。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# カレンダー (CalDav) デバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、カレンダー (CalDAV) アカウントをユーザーのiOSデバイスまたはMac OS Xデバイスに追加し、CalDAVをサポートするサーバーとそのデバイスのスケジュールデータを同期することができます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[End user] の下の [Calendar (CalDAV)] をクリックします。[Calendar (CalDAV) Policy] ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Calendar (CalDAV) Policy' page is displayed, with a sidebar on the left containing '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a description and two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. [Policy Information] ペインで、以下の情報を入力します。
    - Policy Name : ポリシーの説明的な名前を入力します。
    - Description : 任意で、ポリシーの説明を入力します。
  5. [Next] をクリックします。[Platforms] ページが開きます。
  6. [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。
- 1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Calendar (CalDAV) Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
- 3 Assignment

#### Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

► Deployment Rules

Back Next >

次の設定を構成します。

- **Account description** : アカウントの説明を入力します。このフィールドは必須です。
- **Host name** : CalDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **Port** : CalDAVサーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **Principal URL** : ユーザーのカレンダーに対するベースURLを入力します。
- **User name** : ユーザーのログオン名を入力します。このフィールドは必須です。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Use SSL** : CalDAVサーバーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは[ON]です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Calendar (CalDAV) Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
- 3 Assignment

#### Policy Information

This policy lets you add a calendar (CalDAV) account to an iOS and Mac OS X device to enable synchronization of scheduling data with any server that supports CalDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL  ON

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

Profile scope  OS X 10.7+

► Deployment Rules

Back Next >

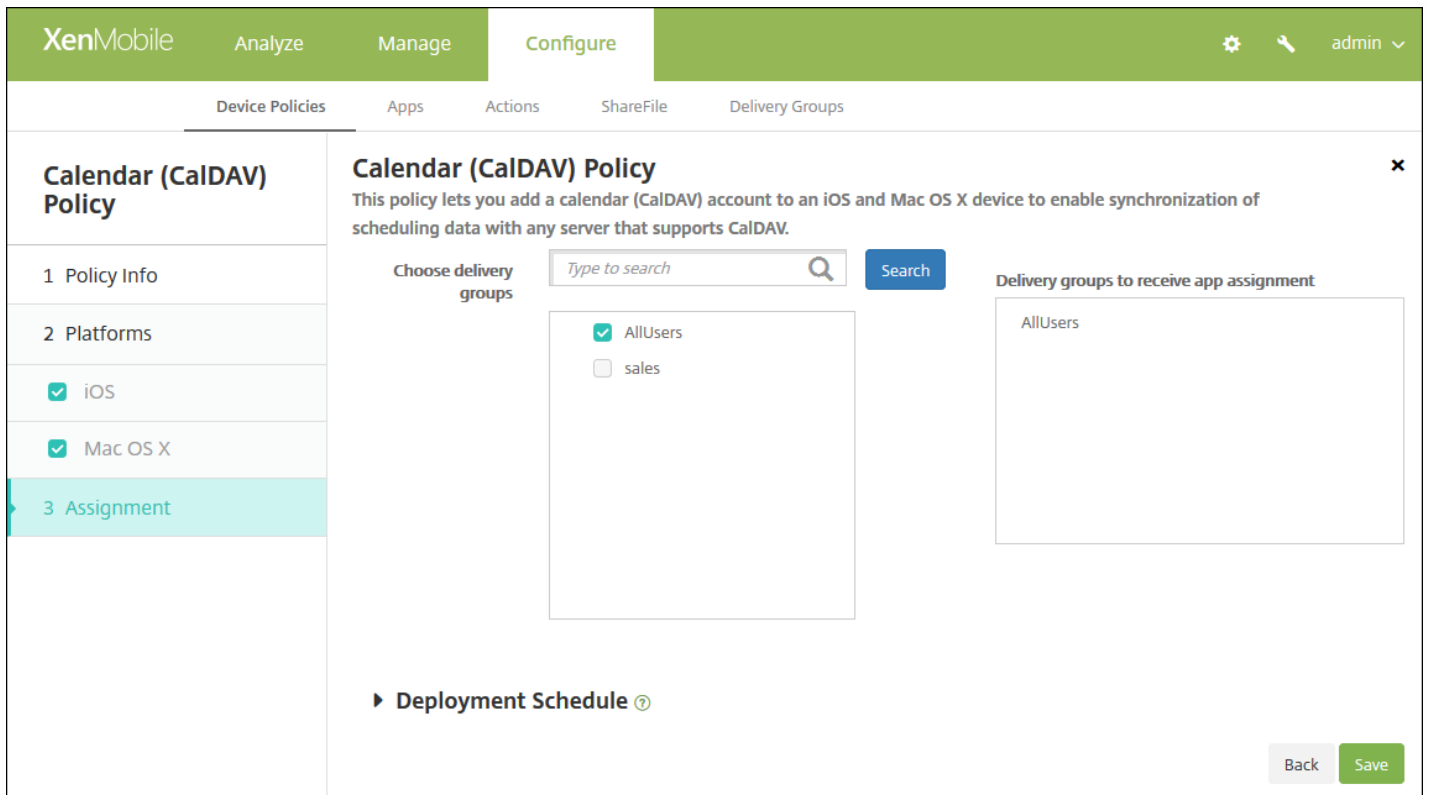
次の設定を構成します。

- **Account description** : アカウントの説明を入力します。このフィールドは必須です。
- **Host name** : CalDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **Port** : CalDAVサーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **Principal URL** : ユーザーのカレンダーに対するベースURLを入力します。
- **User name** : ユーザーのログオン名を入力します。このフィールドは必須です。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Use SSL** : CalDAVサーバーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは[ON]です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。
  - [Profile scope] の横にある、 [User] または [System] を選択します。デフォルトは [User] です。このオプション

ンはOS X 10.7以降でのみ使用できます。

## 7. 展開規則を構成します。

8. [Next] をクリックします。[Calendar (CalDAV) Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# モバイルデバイスポリシー

Apr 27, 2017

このポリシーを使用すると、iOSデバイスのモバイルネットワーク設定を構成できます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ページが開きます。
3. [More] を展開した後、[Network Access] の下の [Celluar] をクリックします。[Cellular Network Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Cellular Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is active. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you configure cellular network settings on an iOS device.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[iOS Platform] 情報ページが開きます。



XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Cellular Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

### Policy Information

This policy lets you configure cellular network settings on an iOS device.

**Attach APN**

Name

Authentication type **PAP**

User name

Password

**APN**

Name

Authentication type **PAP**

User name

Password

Proxy server

Proxy server port

**Policy Settings**

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy **Always**

► **Deployment Rules**

Back Next >

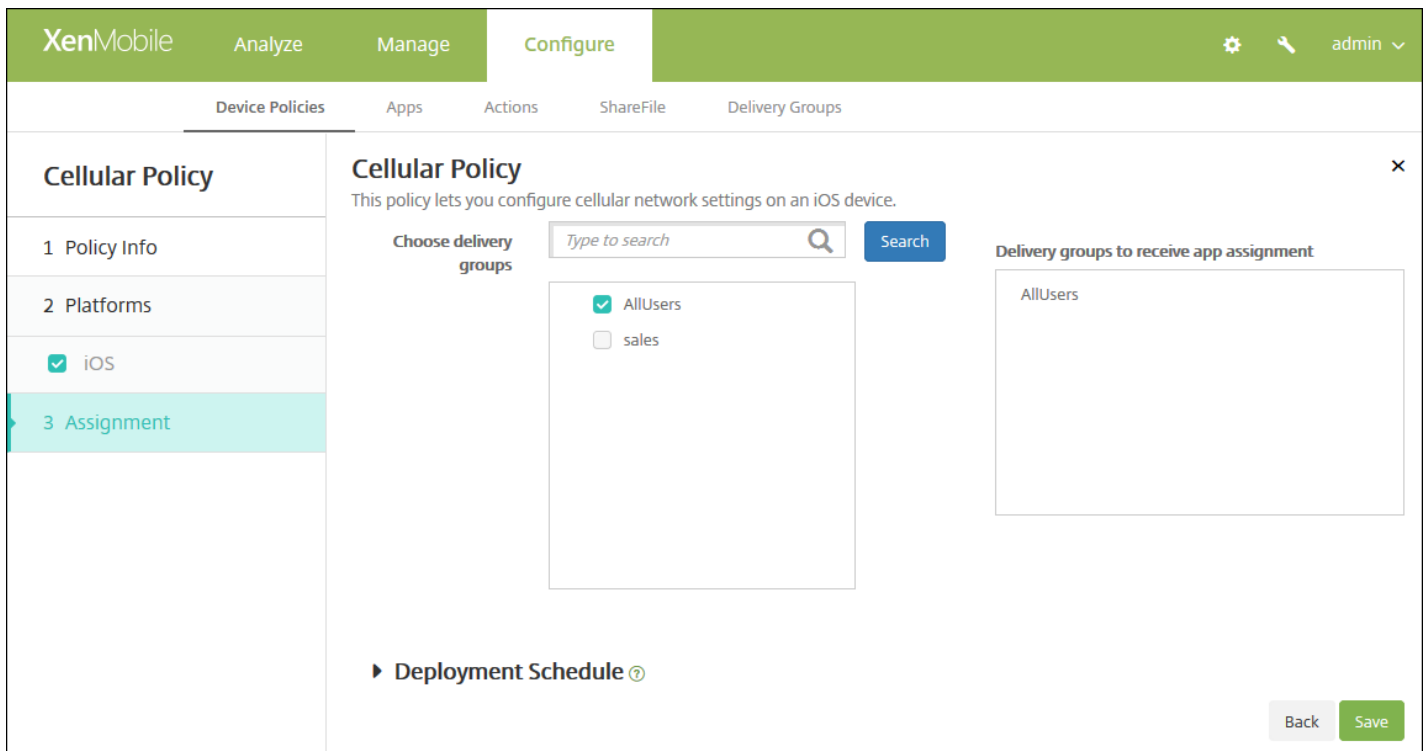
6. 次の設定を構成します。

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

- Proxy server : プロキシサーバーのネットワークアドレスを入力します。
- ポリシー設定
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

## 7. 展開規則を構成します。

8. [Next] をクリックします。[Cellular Network Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# 接続マネージャーデバイスポリシー

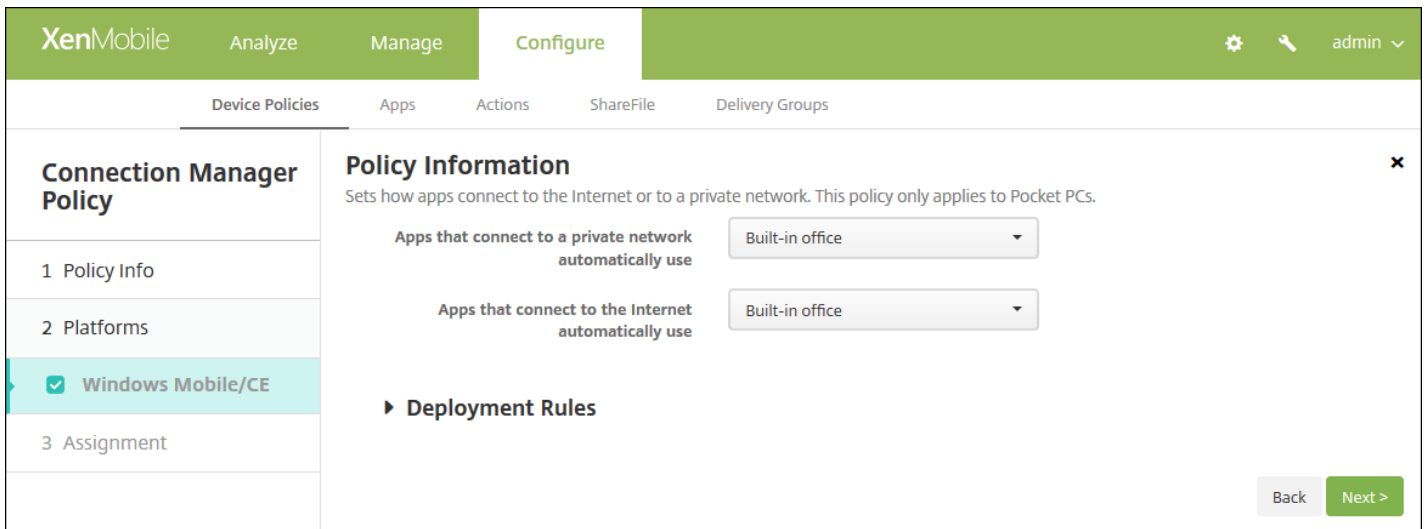
Apr 27, 2017

XenMobileでは、インターネットおよびプライベートネットワークに自動的に接続するアプリケーションの接続設定を指定できます。このポリシーはWindows Pocket PCでのみ使用できます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** をクリックした後、**[Network access]** の下の **[Connection Manager]** をクリックします。**[Connection Manager Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Manager Policy' and contains a 'Policy Information' section. This section includes a description: 'Sets how apps connect to the Internet or to a private network. This policy only applies to Pocket PCs.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Windows Mobile/CE Platform]** ページが開きます。



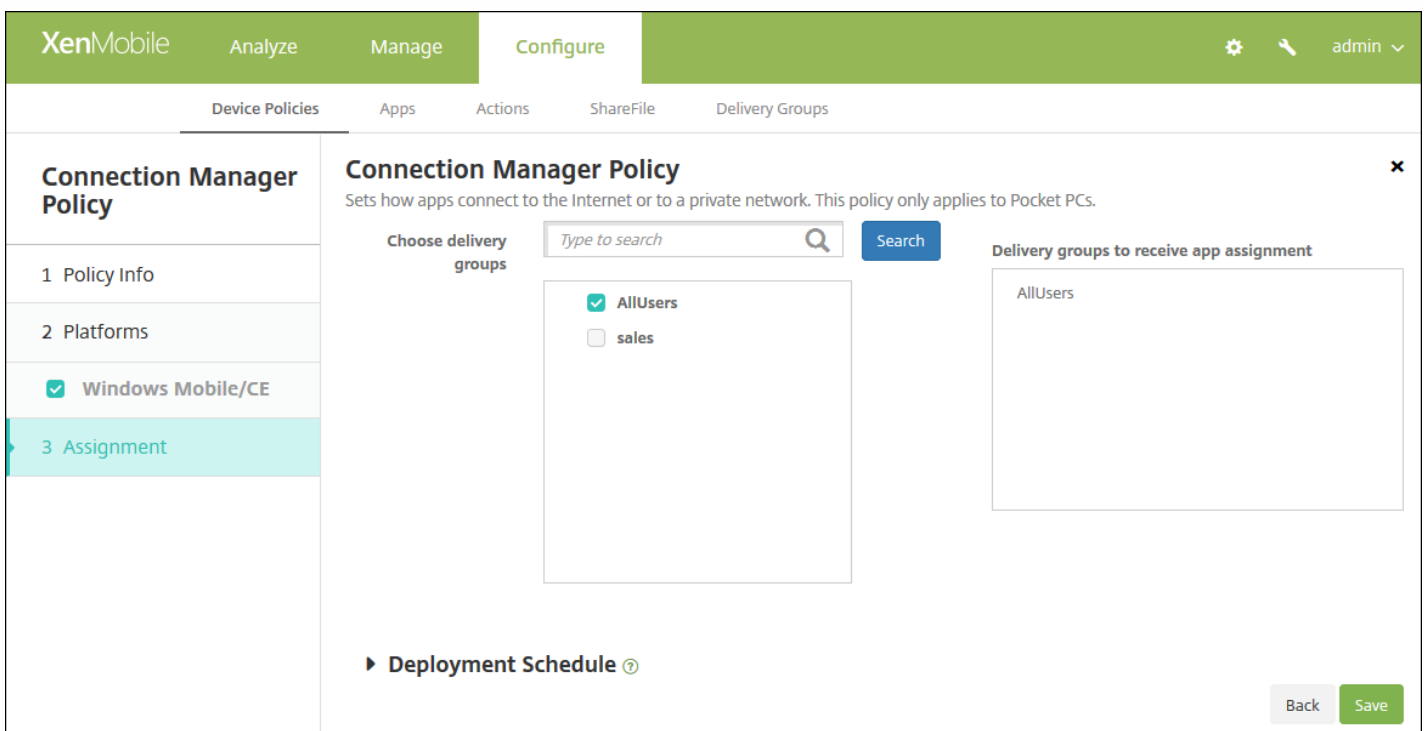
6. 次の設定を構成します。

注： [Built-in office] は、すべての接続先が社内イントラネットであることを意味します。 [Built-in Internet] は、すべての接続先がインターネットであることを意味します。

- Apps that connect to a private network automatically use : 一覧から、 [Built-in office] または [Built-in Internet] を選択します。デフォルトは [Built-in office] です。
- Apps that connect to the Internet automatically use 一覧から、 [Built-in office] または [Built-in Internet] を選択します。デフォルトは [Built-in office] です。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Connection Manager] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# 接続スケジュールデバイスポリシー

Apr 27, 2017

接続スケジュールポリシーを作成して、ユーザーのデバイスをXenMobileに接続する方法と時間を管理します。このポリシーは、Android for Work対応デバイスに対しても構成できます。

ユーザーが手動でデバイスを接続するか、デバイスが永続的に接続されたままにするか、定義した期間内にデバイスが接続されるようにするかを指定できます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [Scheduling] をクリックします。[Connection Scheduling Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the tabs, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. The main content area is titled 'Connection Scheduling Policy' and contains a 'Policy Information' section. The description reads: 'This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set.' There are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is a large text area, also empty. On the left side, there is a sidebar with '1 Policy Info' selected, and other options like '2 Platforms', '3 Assignment', and a 'Next >' button at the bottom right.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、次の設定を構成します。

- **Require devices to connect** : このスケジュールに対して設定するオプションをクリックします。
  - **Always** : 接続のオンライン状態を永続的に維持します。ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後、XenMobileサーバーへの再接続を試行し、一定の間隔でコントロールパケットを送信することによって接続を監視します。最適化されたセキュリティについては、このオプションをお勧めします。【Always】を選択する場合は、デバイスでトンネルポリシーの【Define connection time-out】設定も使用して、接続によりバッテリーが切れないようにします。接続のオンライン状態を維持することにより、ワイプやロックなどのセキュリティコマンドを必要に応じてデバイスにプッシュできます。デバイスに展開された各ポリシーで、【Deployment Schedule】の【Deploy for always-on connections】オプションを選択する必要もあります。
  - **Never** : 手動で接続します。ユーザーがデバイス上のXenMobileから接続を開始する必要があります。デバイスにセキュリティポリシーを展開できず、新しいアプリやポリシーを受信しなくなるため、実稼働環境ではこのオプションはお勧めしません。
  - **Every** : 指定された間隔で接続されます。このオプションが有効な状態でロックやワイプなどのセキュリティポリシーを送信すると、この操作は次回デバイスが接続されたときに処理されます。このオプションを選択すると、【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** : 有効にすると、ユーザーのデバイス上のXenMobileは、ネットワーク接続が失われた後にXenMobileサーバーへの再接続を試行し、定義した期間中、一定の間隔でコントロールパケットを送信することによって接続を監視します。接続期間の定義方法については、「[接続期間の定義](#)」を参照してください。
    - **Maintain permanent connection during these hours** : 定義した期間中、ユーザーのデバイスが接続されている必要があります。
    - **Require a connection within each of these ranges** : 定義した期間内に1回以上、ユーザーのデバイスが接続される必要があります。
    - **Use local device time rather than UTC** : 定義した期間を、UTC (Coordinated Universal Time : 協定世界時) ではなくローカルデバイスの時間に同期させます。





The screenshot shows the XenMobile Configuration console. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Connection Scheduling Policy' and includes a description: 'This policy defines parameters for how and when devices connect to the XenMobile server. You can require users to manual connect, or for the device to connect automatically, or for connections to occur according to a time range you set.' The 'Choose delivery groups' section has a search bar and a list with 'AllUsers' (checked) and 'sales'. The 'Delivery groups to receive app assignment' section shows 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

10. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

12. [Save] をクリックします。

# 連絡先 (CardDAV) デバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、iOS連絡先 (CardDAV) アカウントをユーザーのiOSデバイスまたはMac OS Xデバイスに追加し、CardDAVをサポートするサーバーとそのデバイスの連絡先データを同期することができます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Security] の下の [Contacts (CardDAV)] をクリックします。[CardDAV Policy] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is selected. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is active. The main content area is titled 'CardDAV Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section is active, showing a description: 'This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.' Below the description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty, and the 'Description' field is a large text area. A 'Next >' button is located at the bottom right of the form.

4. [Policy Information] ペインで、以下の情報を入力します。
    - Policy Name : ポリシーの説明的な名前を入力します。
    - Description : 任意で、ポリシーの説明を入力します。
  5. [Next] をクリックします。[Platforms] ページが開きます。
  6. [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。
- 1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### CardDAV Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
- 3 Assignment

### Policy Information

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL

### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy

► Deployment Rules

次の設定を構成します。

- **Account description** : アカウントの説明を入力します。このフィールドは必須です。
- **Host name** : CardDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **Port** : CardDAVサーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **Principal URL** : ユーザーのカレンダーに対するベースURLを入力します。
- **User name** : ユーザーのログオン名を入力します。このフィールドは必須です。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Use SSL** : CardDAVサーバーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは[ON]です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### CardDAV Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
- 3 Assignment

#### Policy Information

This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.

Account description\*

Host name\*

Port\*

Principal URL\*

User name\*

Password

Use SSL

#### Policy Settings

Remove policy  Select date  Duration until removal (in days)

Allow user to remove policy  ▾

Profile scope  ▾ OS X 10.7+

▶ Deployment Rules

次の設定を構成します。

- **Account description** : アカウントの説明を入力します。このフィールドは必須です。
- **Host name** : CardDAVサーバーのアドレスを入力します。このフィールドは必須です。
- **Port** : CardDAVサーバーへの接続用ポートを入力します。このフィールドは必須です。デフォルトは**8443**です。
- **Principal URL** : ユーザーのカレンダーに対するベースURLを入力します。
- **User name** : ユーザーのログオン名を入力します。このフィールドは必須です。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Use SSL** : CardDAVサーバーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは[ON]です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。
  - [Profile scope] の横にある、 [User] または [System] を選択します。デフォルトは [User] です。このオプション

ンはOS X 10.7以降でのみ使用できます。

## 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration page for a CardDAV Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'CardDAV Policy' and includes a description: 'This policy lets you add contacts (CardDAV) accounts for iOS and Mac OS X to an iOS or Mac OS X device to enable synchronization of contact data with any server that supports CardDAV.' The 'Assignment' section is active, showing 'Choose delivery groups' with a search bar and a list of groups (AllUsers, Sales, RG). The 'Delivery groups to receive app assignment' section shows 'AllUsers' selected. There are 'Back' and 'Save' buttons at the bottom right.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# Samsungコンテナへのアプリケーションのコピーデバイスポリシー

Apr 27, 2017

デバイスに既にインストールされているアプリケーションが、サポートされているSamsungデバイス上のSEAMSコンテナまたはKNOXコンテナにコピーされるように指定できます（サポートされるデバイスについては、[SamsungのSamsung KNOX Supported Devices](#)ページを参照してください）。SEAMSコンテナにコピーされたアプリケーションは、ユーザーのホーム画面で使用できます。KNOXコンテナにコピーされたアプリケーションは、ユーザーがKNOXコンテナにサインインした場合のみ使用できます。

## 前提条件：

- デバイスをXenMobileに登録する必要があります。
- Samsung MDMキー（ELMおよびKLM）を展開する必要があります（展開方法については、「Samsung MDMライセンスキーデバイスポリシー」を参照してください）。
- アプリケーションがデバイスにインストール済みである必要があります。
- デバイスでKNOXを初期化して、アプリケーションをKNOXコンテナにコピーします。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。

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

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

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Copy Apps to Samsung Container Policy

1 Policy Info

2 Platforms

- Samsung SEAMS
- Samsung KNOX

3 Assignment

#### Policy Information

This policy lets you create a SEAMS or KNOX container for apps on Samsung devices.

Policy Name\*

Description

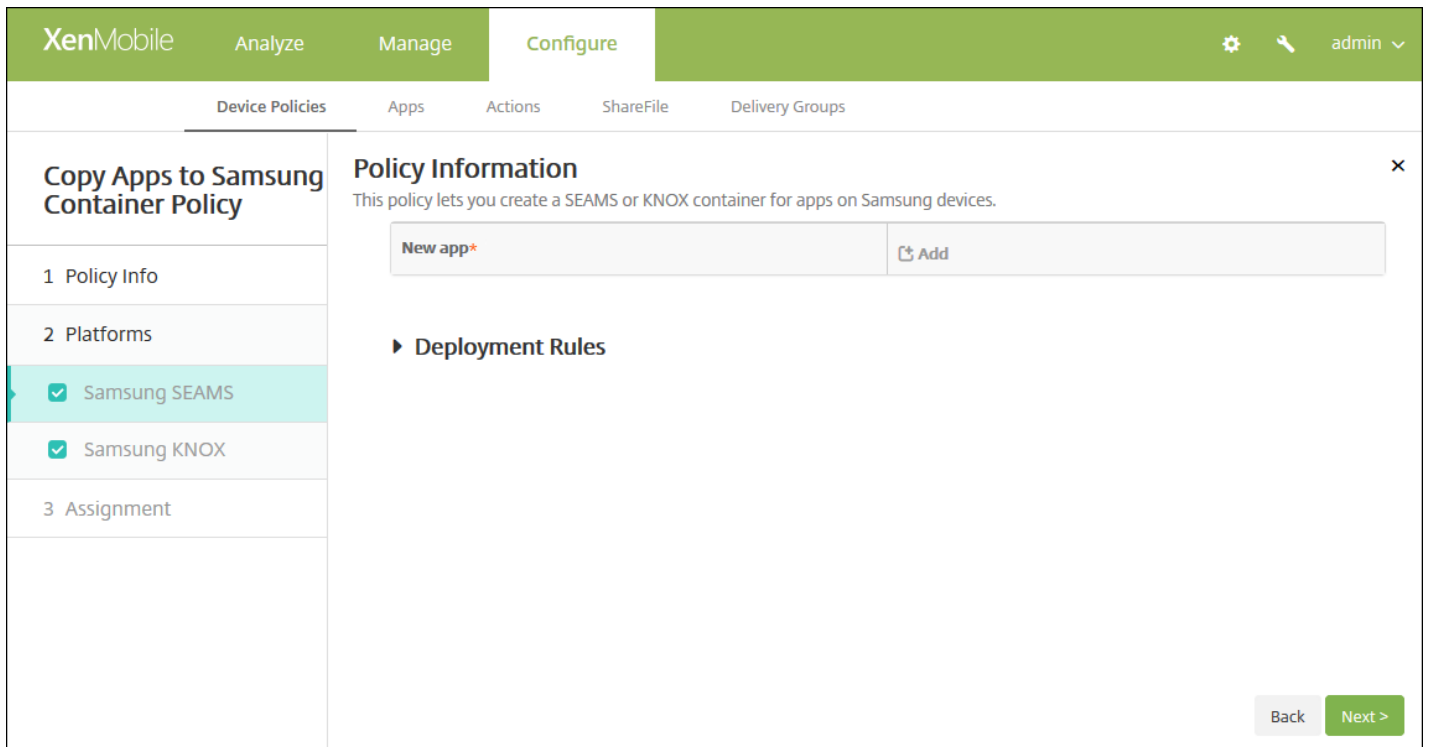
Next >

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



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

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



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

1つのプラットフォームの設定の構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

7.7. 選択したプラットフォームごとに、次の設定を構成します。

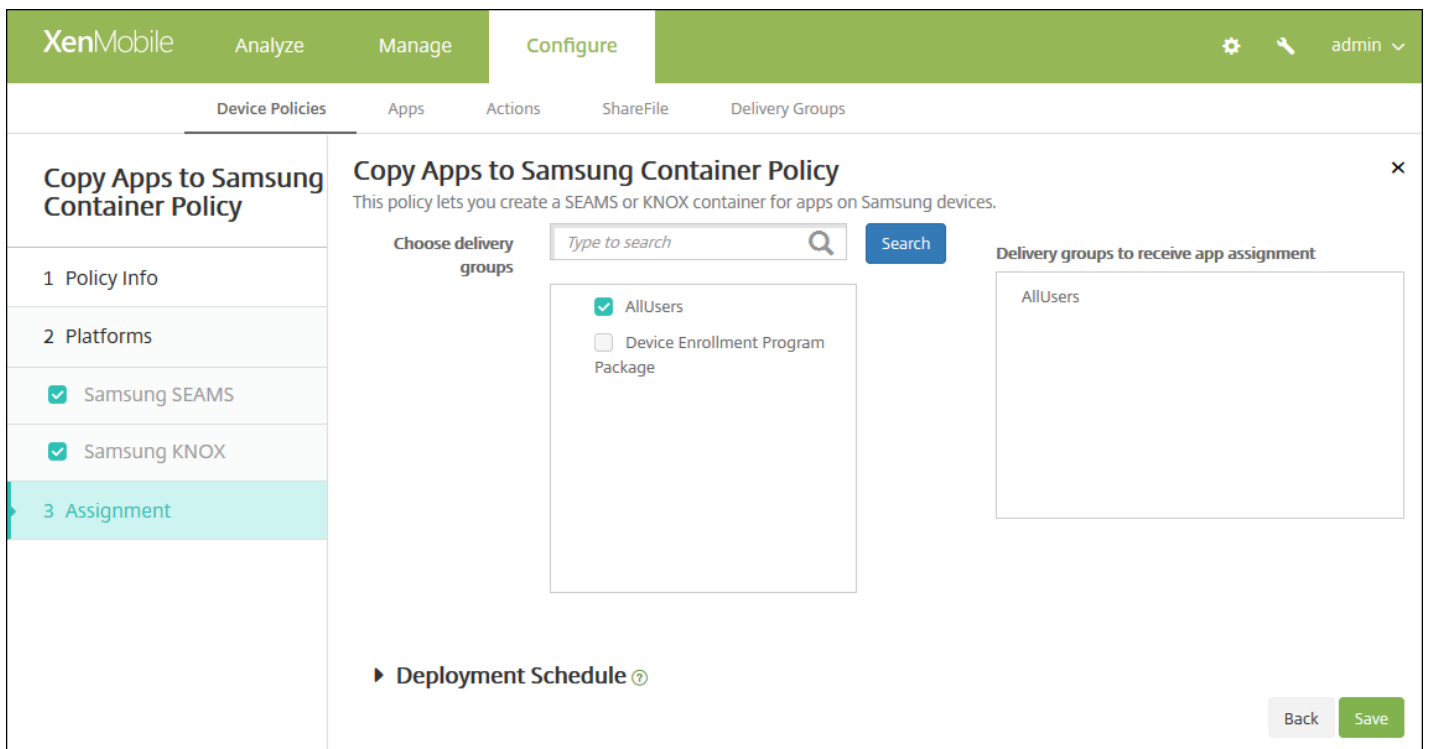
- **New app** : 一覧に追加するアプリケーションごとに、[Add] をクリックして以下の操作を行います。
  - パッケージIDを入力します。たとえば、LacingArtアプリの場合、「lacingart」と入力します。
  - [Save] または [Cancel] をクリックします。

注：既存のアプリを削除するには、その項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

#### 8. 展開規則を構成します。

9. [Next] をクリックします。次のプラットフォームのページまたはポリシーの [Copy Apps to Samsung Container Policy] 割り当てページが開きます。



10. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [アプリ割り当てを受信するためのデリバリーグループ] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

12. [Save] をクリックしてポリシーを保存します。

ポリシーが正常に展開されると、SEAMSアプリケーションは [Device details] ページの見出し [Location: Enterprise SEAMS Location] の下に、KNOXアプリケーションは見出し [Location: Enterprise Location] の下に表示されます。

# 資格情報デバイスポリシー

Apr 27, 2017

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。資格情報については、「[証明書](#)」を参照してください。

資格情報ポリシーは、iOS、Mac OS X、Android、Android for Work、Windowsデスクトップ/タブレット、Windows Mobile/CE、Windows Phoneデバイスに対して作成できます。プラットフォームごとに必要な値が異なります。これらの値については、[ここで説明しています](#)。

[iOSの設定](#)

[Mac OS Xの設定](#)

[AndroidおよびAndroid for Workの設定](#)

[Windowsデスクトップ/タブレットの設定](#)

[Windows Mobile/CEの設定](#)

[Windows Phoneの設定](#)

このポリシーを作成するには、各プラットフォームで使用する予定の資格情報と、証明書およびパスワードが必要です。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[Security]** の下の **[Credentials]** をクリックします。**[Credentials Policy]** 情報ページが開きます。

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

The screenshot shows the 'Configure' page for a 'Credentials Policy' in XenMobile. The interface includes a top navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is divided into a left sidebar and a main panel. The sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main panel is titled 'Policy Information' and contains the following sections:
 

- Credential type:** A dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)'.
- Credential name:** A text input field with a red asterisk indicating it is required.
- The credential file path:** A text input field with a 'Browse' button.
- Policy Settings:**
  - Remove policy:** Two radio buttons: 'Select date' (selected) and 'Duration until removal (in days)'.
  - Allow user to remove policy:** A dropdown menu set to 'Always'.
- Deployment Rules:** A section header with a right-pointing arrow.

 At the bottom right of the main panel, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Credential type** : 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name** : 資格情報の固有の名前を入力します。
    - **The credential file path** : [Browse] をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - **キーストア**
    - **Credential name** : 資格情報の固有の名前を入力します。
    - **The credential file path** : [Browse] をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
    - **Password** : 資格情報のキーストアパスワードを入力します。
  - **サーバー証明書**
    - **Server certificate** : ボックスの一覧で、使用する証明書を選択します。
  - **資格情報プロバイダー**
    - **Credential provider** : ボックスの一覧で、資格情報プロバイダーの名前を選択します。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。

The screenshot shows the 'Configure' page for a 'Credentials Policy' in XenMobile. The interface includes a top navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is divided into a left sidebar and a main configuration panel. The sidebar has three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X (highlighted), Android, Android for Work, Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main configuration panel is titled 'Credentials Policy' and includes a descriptive text: 'This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' The configuration options include:
 

- Credential type:** A dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)'.
- Credential name:** An empty text input field.
- The credential file path:** An empty text input field with a 'Browse' button.
- Policy Settings:**
  - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'.
  - Allow user to remove policy:** A dropdown menu set to 'Always'.
  - Profile scope:** A dropdown menu set to 'User', with a note 'OS X 10.7+'.
- Deployment Rules:** A section header with a right-pointing arrow.

 At the bottom right of the configuration panel, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Credential type** : 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name** : 資格情報の固有の名前を入力します。
    - **The credential file path** : **[Browse]** をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
  - **キーストア**
    - **Credential name** : 資格情報の固有の名前を入力します。
    - **The credential file path** : **[Browse]** をクリックしてファイルの場所に移動し、資格情報ファイルを選択します。
    - **Password** : 資格情報のキーストアパスワードを入力します。
  - **サーバー証明書**
    - **Server certificate** : ボックスの一覧で、使用する証明書を選択します。
  - **資格情報プロバイダー**
    - **Credential provider** : ボックスの一覧で、資格情報プロバイダーの名前を選択します。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
  - **[Policy scope]** の横にある、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。

次の設定を構成します。

- **Credential type** : 一覧からこのポリシーで使用する資格情報の種類を選択し、選択した資格情報について以下の情報を入力します。
  - **証明書**
    - **Credential name** : 資格情報の固有の名前を入力します。
    - **The credential file path** : [Browse] をクリックして資格情報ファイルの場所に移動し、そのファイルを選択します。
  - **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。
- **Credential provider**
  - **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。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Credentials Policy

This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Android for Work
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**OS version\*** 10

**Certificate Type** ROOT

**Store device** root

**Location** System

**Credential type** Certificate (.cer, .crt, .der and .pem)

**Credential file path\***  **Browse**

► **Deployment Rules**

[Back](#) [Next >](#)

次の設定を構成します。

- **OS version** : 一覧から、Windows 8.1の場合は **[8.1]** を、Windows 10の場合は **[10]** を選択します。デフォルトは**10**です。

[Windows 10の設定](#)

[Windows 8.1設定](#)



次の設定を構成します。

- **Store device** : ボックスの一覧から、資格情報の証明書ストアの場所を選択します。デフォルトは [root] です。次のオプションがあります。
  - **Privileged execution trust authorities** - このストアに属する証明書で署名されたアプリケーションが、特権信頼レベルで実行されます。
  - **Unprivileged execution trust authorities**- このストアに属する証明書で署名されたアプリケーションが、標準信頼レベルで実行されます。
  - **SPC (Software Publisher Certificate)** - .cabファイルの署名にソフトウェア発行元証明書 (SPC) が使用されます。
  - **root**- ルート証明書または自己署名証明書を含む証明書ストア。
  - **CA** - 暗号化情報を含む証明書ストア (中間証明機関を含む)。
  - **MY** - エンドユーザーの個人証明書を含む証明書ストア。
- **Credential type** : Windows Mobile/CEデバイスの場合、資格情報の種類は証明書のみです。
- **The credential file path** : [ブラウザー] をクリックして資格情報ファイルの場所へ移動し、そのファイルを選択します。

次の設定を構成します。

- **Certificate Type** : 一覧から、 [ROOT] または [CLIENT] を選択します。
- [ROOT] を選択した場合は、次の設定を構成します。
  - **Store device** : 資格情報の証明書ストアの場所に応じて、ボックスの一覧で [root] 、 [My] 、 [CA] のいずれかを選択します。 [My] を選択すると、証明書はユーザーの証明書ストアに保存されます。
  - **Location** : Windows Phoneの場合、場所は [System] のみです。
  - **Credential type** : Windows Phoneの場合、資格情報の種類は証明書のみです。
  - **Credential file path** : [Browse] をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
- [CLIENT] を選択した場合は、次の設定を構成します。
  - **Location** : Windows Phoneの場合、場所は [System] のみです。
  - **Credential type** : Windows Phoneの場合、資格情報の種類はキーストアのみです。
  - **Credential name** : 資格情報の名前を入力します。このフィールドは必須です。
  - **Credential file path** : [Browse] をクリックして証明書ファイルの場所に移動し、そのファイルを選択します。
  - **Password** : 資格情報に関連付けられたパスワードを入力します。このフィールドは必須です。

## 7. 展開規則を構成します。

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] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# カスタムXMLデバイスポリシー

Apr 27, 2017

Windows Phone、Windowsデスクトップ/タブレット、Windows Mobile/CEデバイスの以下の機能をカスタマイズする場合、XenMobileでカスタムXMLポリシーを作成できます。

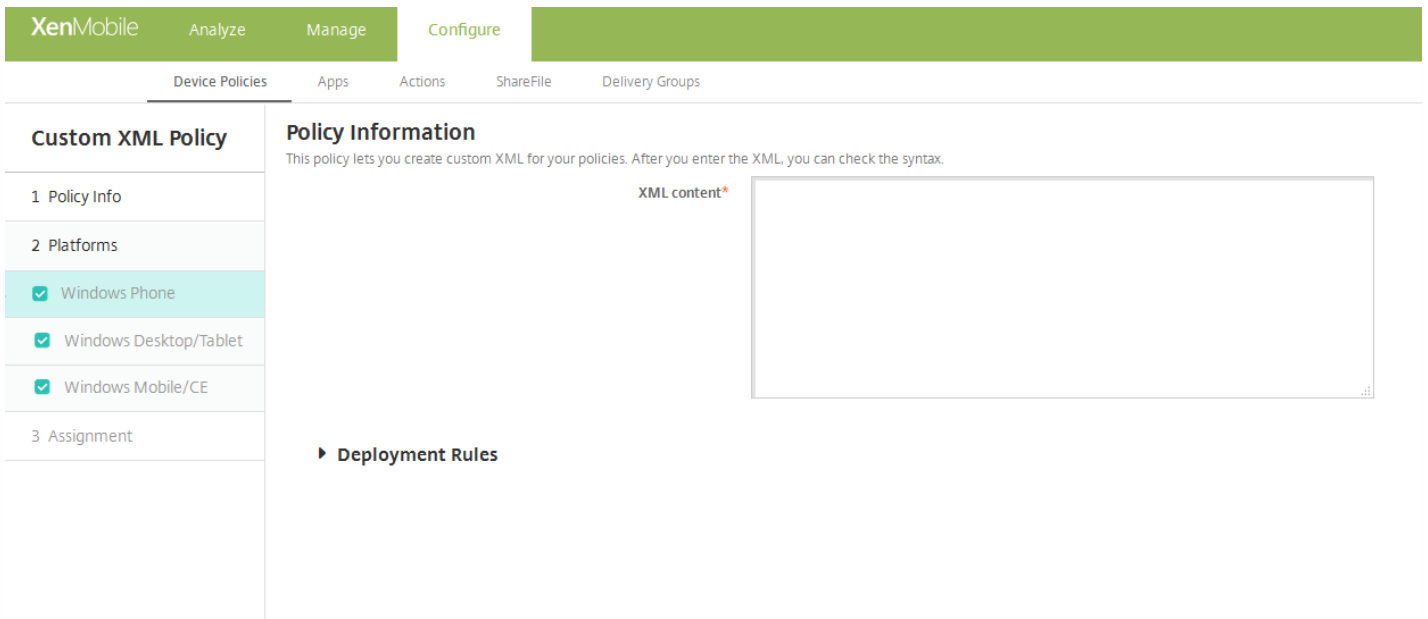
- プロビジョニング。デバイスの構成や、機能の有効化/無効化などです。
- デバイス構成。ユーザーによる、設定やデバイスパラメーターの変更の許可などです。
- ソフトウェアのアップグレード。アプリケーションやシステムソフトウェアなど、デバイスにロードされる新しいソフトウェアやバグ修正の提供などです。
- 障害管理。デバイスからのエラーおよび状態レポートの受信などです。

WindowsでOpen Mobile Alliance Device Management (OMA DM) APIを使用して、カスタムXML構成を作成します。OMA DM APIを使用したカスタムXMLの作成については、このトピックでは扱いません。OMA DM APIの使用については、Microsoft Developer Networkサイトの「[OMA Device Management](#)」を参照してください。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[Custom] の下の [Custom XML] をクリックします。[Custom XML Policy] 情報ページが開きます。

The screenshot shows the 'Custom XML Policy' configuration page in the XenMobile console. The page is divided into several sections. At the top, there is a green navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Custom XML Policy' and has a left sidebar with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a text box for 'Policy Name\*' and a larger text area for 'Description'. Below the 'Policy Info' step, there are three platform selection options, all of which are checked: 'Windows Phone', 'Windows Desktop/Tablet', and 'Windows Mobile/CE'.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Policy Platforms] ページが開きます。



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

7. 選択したプラットフォームごとに、次の設定を構成します。

- **XML content** : ポリシーに追加するカスタムXMLコードを入力するか、コピーして貼り付けます。

#### 8. 展開規則を構成します。

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

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注 :

- このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用され

ます。

12. [Save] をクリックします。

# ファイルおよびフォルダーの削除デバイスポリシー

Apr 27, 2017

XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のファイルまたはフォルダーを削除できます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add New Policy] ダイアログボックスが開きます。
3. [More] を展開し、[Apps] で [Delete Files and Folders] をクリックします。[Delete Files and Folders Policy] 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which files and folders need to be deleted.

Policy Name\*

Description

Next >

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

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

5. [Next] をクリックします。[Windows Mobile/CE Platform] ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Files and Folders Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which files and folders need to be deleted.

Files and folders to delete

Path*	Type	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

► Deployment Rules

Back Next >

6. 次の設定を構成します。

- **Files and folders to delete** : 削除するファイルまたはフォルダーごとに、 [Add] をクリックして以下の操作を行います。
  - **Path** : ファイルまたはフォルダーまでのパスを入力します。
  - **Type** : 一覧から、 [File] または [Folder] を選択します。デフォルトは [File] です。
  - **[Save]** をクリックしてファイルまたはフォルダーを保存するか、 **[Cancel]** をクリックして操作を取り消します。

注：既存の一覧を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、 **[Save]** をクリックして変更した項目を保存するか、 **[Cancel]** をクリックして項目を変更せずそのままにします。

### 7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Delete Files and Folders Policy]** 割り当てページが開きます。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Delete Files and Folders Policy' and contains a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment' (highlighted). The 'Assignment' section shows 'Choose delivery groups' with a search box and a list of 'AllUsers' (checked) and 'sales' (unchecked). To the right, 'Delivery groups to receive app assignment' shows 'AllUsers'. At the bottom, there is a 'Deployment Schedule' link and 'Back' and 'Save' buttons.

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。



- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# レジストリキーおよび値デバイスポリシーの削除

Apr 27, 2017

XenMobileでポリシーを作成して、Windows Mobile/CEデバイスから特定のレジストリキーおよび値を削除することができます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[Apps] の下の [Delete Registry Keys and Values] をクリックします。[Delete Registry Keys and Values Policy] 情報ページが開きます。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Policy Name\*

Description

Next >

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

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

5. [Next] をクリックします。[Windows Mobile/CE Platform] ページが開きます。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### Delete Registry Keys and Values Policy

1 Policy Info

2 Platforms

Windows Mobile/CE

3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.

Registry keys and values to delete

Key*	Value	Add
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

► Deployment Rules

Back Next >

6. 次の設定を構成します。

- **Registry keys and values to delete** : 削除するレジストリキーおよび値ごとに、**[Add]** をクリックして以下の操作を行います。
  - **Key** : レジストリキーのパスを入力します。これは必須フィールドです。レジストリキーのパスは、HKEY\_CLASSES\_ROOT\、HKEY\_CURRENT\_USER\、HKEY\_LOCAL\_MACHINE\、またはHKEY\_USERS\で始まる必要があります。
  - **Value** : 削除する値の名前を入力します。または、レジストリキー全体を削除する場合は、このフィールドを空白のままにします。
  - **[Save]** をクリックしてキーおよび値を保存するか、**[Cancel]** をクリックして操作を取り消します。

注：既存の項目を削除するには、その項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

## 7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Delete Registry Keys and Values Policy]** 割り当てページが開きます。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Delete Registry Keys and Values Policy' and includes a description: 'This policy allows you to specify which registry keys and values need to be deleted. An empty value means that the entry is a registry key.' There are two main sections: 'Choose delivery groups' with a search box and a list of groups (AllUsers, sales) where 'AllUsers' is selected, and 'Delivery groups to receive app assignment' which also shows 'AllUsers'. A 'Deployment Schedule' section is partially visible at the bottom. 'Back' and 'Save' buttons are at the bottom right.

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。

- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# デバイス正常性構成証明デバイスポリシー

Apr 27, 2017

XenMobileでは、分析目的で特定のデータおよびランタイム情報をHealth Attestation Service (HAS) に送信させ、Windows 10デバイスに正常性状態を報告させることができます。HASは、正常性構成証明書を作成してデバイスに返します。その後、この証明書はデバイスからXenMobileに送信されます。XenMobileは正常性構成証明書を受信すると、その内容に基づいて、管理者が以前に設定した自動アクションを展開します。

HASによって検証されるデータは以下のとおりです。

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

詳しくは、Microsoftの「[HealthAttestation CSP](#)」ページを参照してください。

1. XenMobileコンソールで、[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、[Custom] の下の [Device Health Attestation policy] をクリックします。[Device Health Attestation Policy] 情報ページが開きます。

**Device Health Attestation Policy**

**Policy Information**  
This policy enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine the health of a Windows 10 device and take compliance actions when necessary.

Policy Name\*

Description

1 Policy Info

2 Platforms

Windows Phone

Windows Desktop/Tablet

3 Assignment

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

**Device Health Attestation Policy**

This policy enables Device Health Attestation, a security and data loss prevention (DLP) feature in Windows 10 that lets you determine the health of a Windows 10 device and take compliance actions when necessary.

Enable Device Health Attestation

► Deployment Rules

1 Policy Info

2 Platforms

Windows Phone

Windows Desktop/Tablet

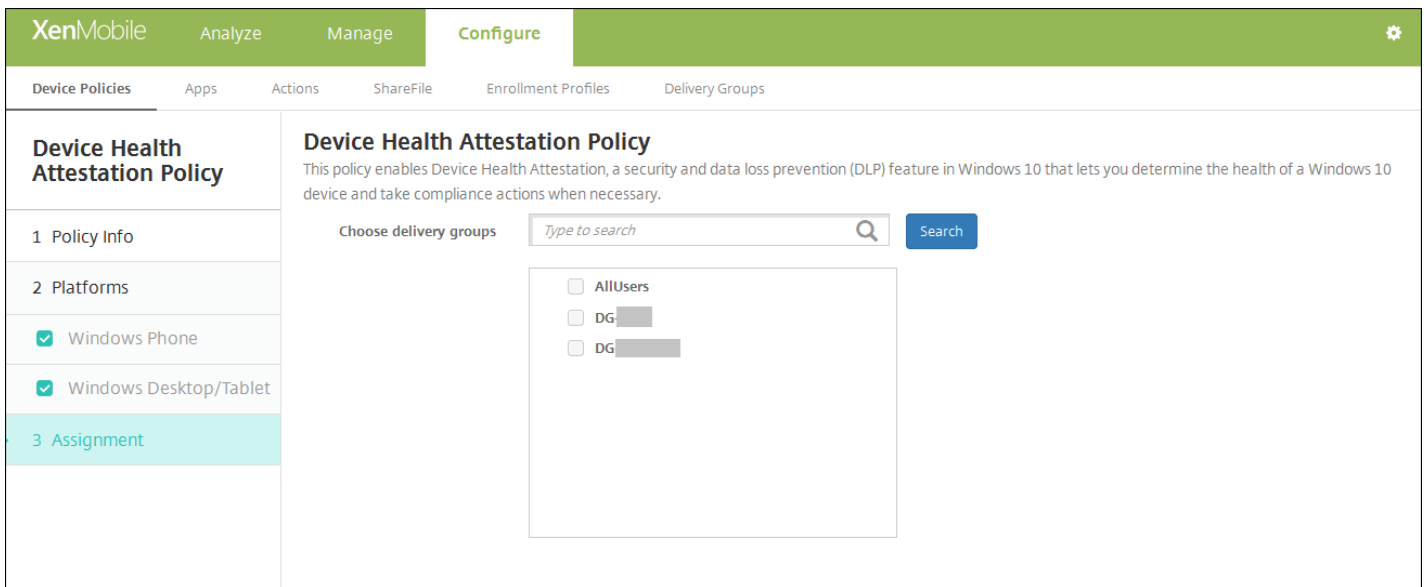
3 Assignment

選択したプラットフォームごとに、次の設定を構成します。

- Enable Device Health Attestation : デバイス正常性構成証明を必須とするかどうかを選択します。デフォルトは [OFF] です。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Device Health Attestation Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# デバイス名デバイスポリシー

Apr 27, 2017

デバイスを特定しやすくするために、iOSデバイスおよびMac OS Xデバイスに名前を設定できます。デバイス名は、マクロ、テキスト、または両方の組み合わせを使用して定義することができます。たとえば、デバイス名をデバイスのシリアル番号として設定するには、`${device.serialNumber}`を使用します。デバイス名をユーザー名とドメインの組み合わせとして設定するには、`${user.username}@example.com`を使用します。マクロについて詳しくは、「[XenMobileのマクロ](#)」を参照してください。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。
3. **[More]** を展開した後、**[End user]** の下の **[Device Name]** をクリックします。**[Device Name Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Device Name Policy' and 'Policy Information'. It includes a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The main content area has a 'Policy Name\*' field and a 'Description' text area. A 'Next >' button is visible at the bottom right.

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

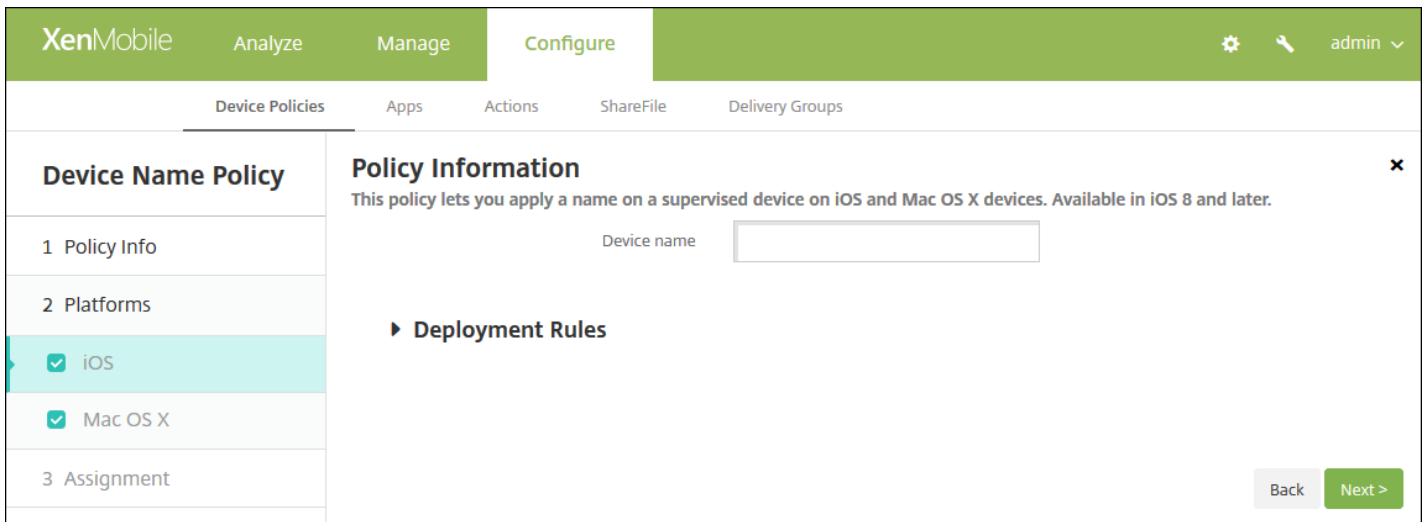
- **Policy Name** : ポリシーの説明的な名前を入力します。
- **Description** : 任意で、ポリシーの説明を入力します。

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。



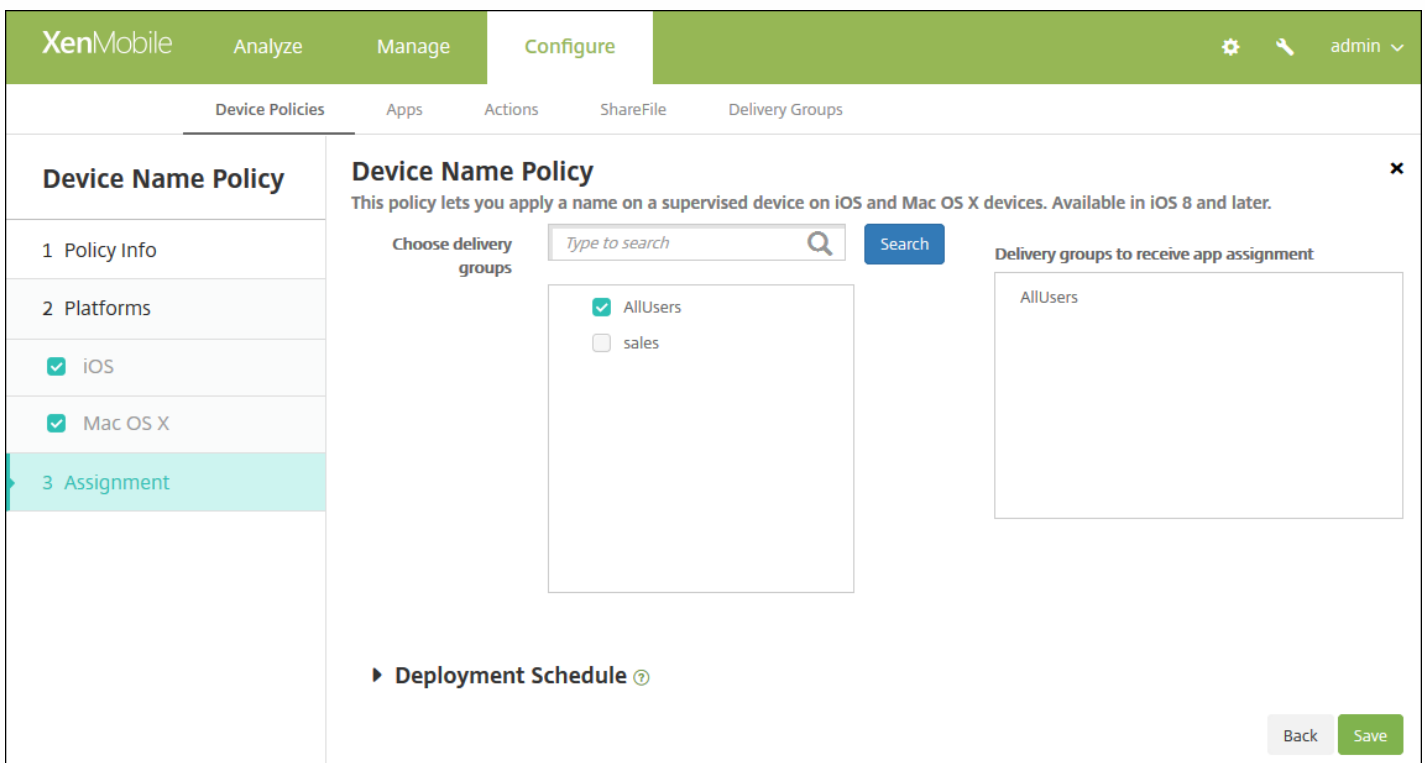


選択したプラットフォームごとに、次の設定を構成します。

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

#### 7. 展開規則を構成します。

8. [Next] をクリックします。[Device Name Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# Enterprise Hubデバイスポリシー

Apr 27, 2017

Windows PhoneのEnterprise Hubデバイスポリシーでは、Enterprise Hub Companyストアを通じてアプリケーションを配布できます。

このポリシーを作成するには以下が必要です。

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

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

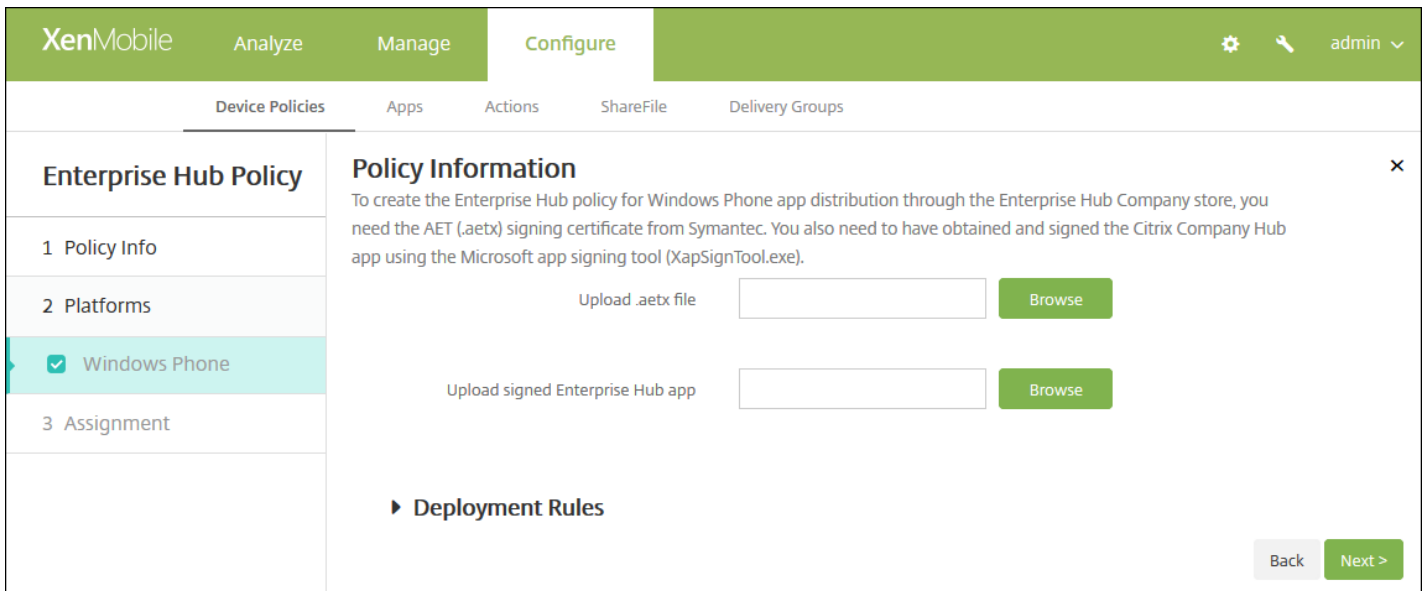
1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[XenMobile agent] の下の [Enterprise Hub] をクリックします。[Enterprise Hub Policy] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Enterprise Hub Policy' and contains a 'Policy Information' section. This section includes a text box for 'Policy Name\*' and a larger text box for 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

5. [Next] をクリックします。[Windows Phone] プラットフォームページが開きます。

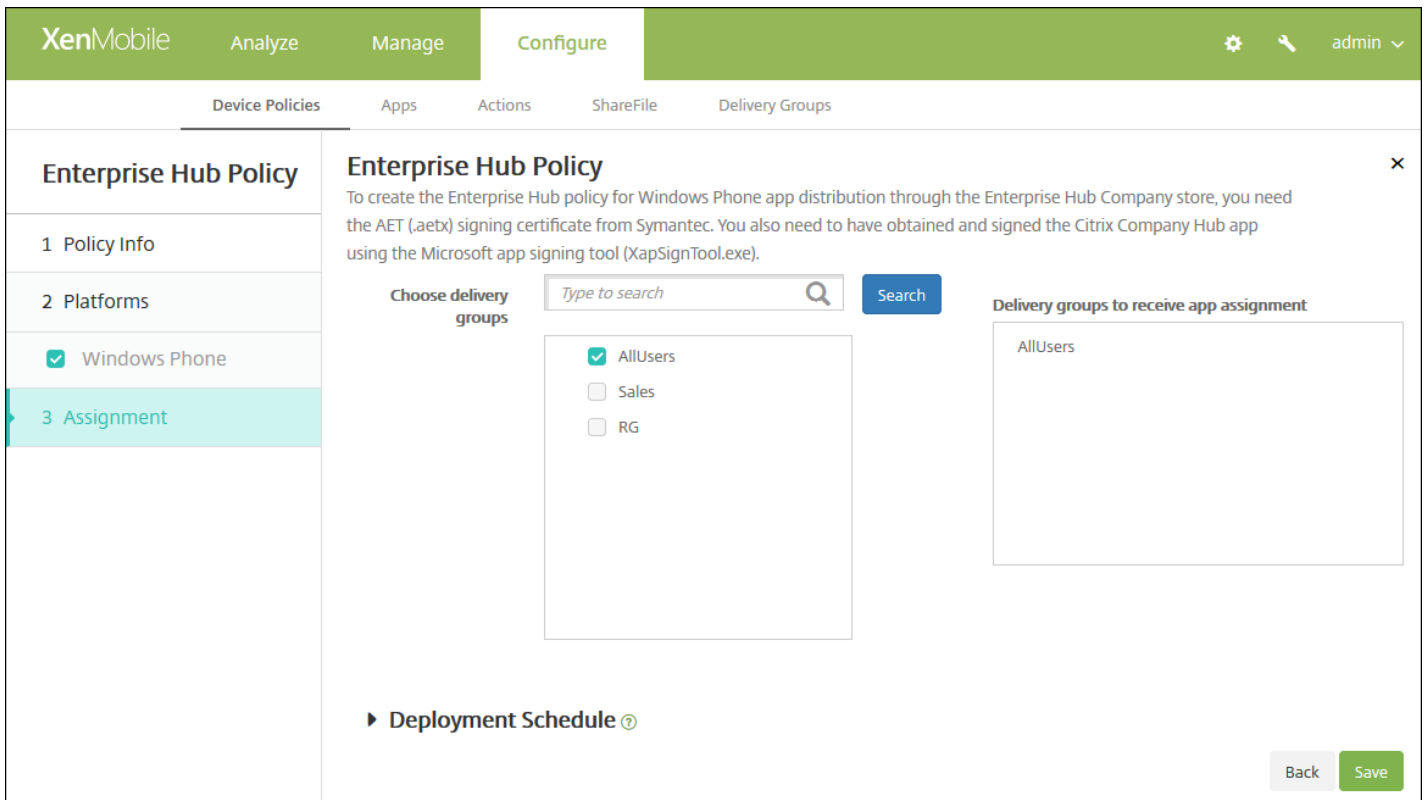


6. 次の設定を構成します。

- Upload .aetx file : [Browse] をクリックして .aetx ファイルの場所へ移動し、そのファイルを選択します。
- Upload signed Enterprise Hub app : [Browse] をクリックして Enterprise Hub アプリケーションの場所へ移動し、アプリケーションを選択します。

7. 展開規則を構成します。

8. [Next] をクリックします。[Enterprise Hub Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# ファイルデバイスポリシー

Apr 27, 2017

ユーザーに対して特定の機能を実行するスクリプトファイル、またはAndroidデバイスユーザーがデバイスでアクセスできるドキュメントファイルを、XenMobileに追加できます。ファイルを追加するときは、デバイス上のファイルを格納するフォルダーも指定できます。たとえば、Androidユーザーが会社のドキュメントまたは.pdfファイルを受け取るようにする場合は、ファイルをデバイスに展開し、ユーザーにファイルがある場所を知らせます。

このポリシーで追加できるファイルの種類は次のとおりです。

- テキストベースのファイル (.xml、.html、.pyなど)
- ドキュメント、写真、スプレッドシート、プレゼンテーションなどのほかのファイル
- Windows MobileおよびWindows CEのみ：MortScriptで作成されたスクリプトファイル

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[Apps] の下の [Files] をクリックします。[Files Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. The 'Configure' tab is active. Below the navigation bar, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. The main content area is titled 'Files Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked items: 'Android' and 'Windows Mobile/CE'. The main area is titled 'Policy Information' and contains a description: 'This policy lets you upload files and executable scripts to devices.' Below this are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

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

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected.

On the left, a sidebar titled 'Files Policy' contains three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' and 'Windows Mobile/CE' are both checked with green checkmarks.

The main content area is titled 'Policy Information' and includes the following fields and controls:

- 'File to be imported\*': A text input field with a green 'Browse' button to its right.
- 'File type': Radio buttons for 'File' (selected) and 'Script'.
- 'Replace macro expressions': A toggle switch set to 'OFF' with a help icon.
- 'Destination folder': A dropdown menu showing '%XenMobile Folder%' with a help icon.
- 'Destination file name': A text input field with a help icon.
- 'Copy file only if different': A dropdown menu.

At the bottom of the main area, there is a '► Deployment Rules' link. In the bottom right corner, there are 'Back' and 'Next >' buttons.

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile configuration interface for a Files Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Files Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with 'Android' and 'Windows Mobile/CE' checked), and '3 Assignment'. The main area is titled 'Policy Information' and contains the following fields:

- File to be imported\***: A text input field with a 'Browse' button.
- File type**: Radio buttons for 'File' (selected) and 'Script'.
- Replace macro expressions**: A toggle switch set to 'OFF' with a help icon.
- Destination folder**: A dropdown menu showing '%XenMobile Folder%' with a help icon.
- Destination file name**: A text input field with a help icon.
- Copy file only if different**: A dropdown menu showing 'Copy file only if different'.

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

次の設定を構成します。

- **File to be imported** : [Browse] をクリックしてインポートするファイルの場所へ移動し、そのファイルを選択します。
- **File type** : [File] または [Script] を選択します。[Script] を選択すると、[Execute immediately] が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは [OFF] です。
- **Replace macro expressions** : スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは [OFF] です。
- **Destination folder** : 一覧からアップロードしたファイルを格納する場所を選択するか、[Add new] をクリックして、一覧にない場所を選択します。また、パス識別子の先頭に%XenMobile Folder%または%Flash Storage%というマクロを使用することもできます。
- **Destination file name** : オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- **Copy file only if different** : 一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。



The screenshot shows the 'Configure' page for a 'Files Policy' in XenMobile. The left sidebar has 'Files Policy' selected, with sub-sections for '1 Policy Info', '2 Platforms' (including 'Android' and 'Windows Mobile/CE'), and '3 Assignment'. The main area is titled 'Policy Information' and contains the following settings:

- File to be imported\***: A text input field with a 'Browse' button.
- File type**: Radio buttons for 'File' (selected) and 'Script'.
- Replace macro expressions**: A toggle switch set to 'OFF'.
- Destination folder**: A dropdown menu showing '%My Documents%'.
- Destination file name**: A text input field with a help icon.
- Copy file only if different**: A dropdown menu showing 'Copy file only if different'.
- Read only file**: A toggle switch set to 'OFF'.
- Hidden file**: A toggle switch set to 'OFF'.

At the bottom of the main area, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

次の設定を構成します。

- **File to be imported** : [Browse] をクリックしてインポートするファイルの場所へ移動し、そのファイルを選択します。
- **File type** : [File] または [Script] を選択します。[Script] を選択すると、[Execute immediately] が表示されます。ファイルがアップロードされたらすぐにスクリプトを実行するかどうかを選択します。デフォルトは [OFF] です。
- **Replace macro expressions** : スクリプトに含まれるマクロのトークン名をデバイスまたはユーザーのプロパティで置き換えるかどうかを選択します。デフォルトは [OFF] です。
- **Destination folder** : 一覧からアップロードしたファイルを格納する場所を選択するか、[Add new] をクリックして、一覧にない場所を選択します。また、パス識別の先頭に以下のマクロを使用することもできます。
  - %Flash Storage%
  - %XenMobile Folder%
  - %Program Files%
  - %My Documents%
  - %Windows%
- **Destination file name** : オプションです。デバイスにファイルを展開する前に名前を変更する必要がある場合は、ファイルの別名を入力します。
- **Copy file only if different** : 一覧から、アップロードするファイルが既存のファイルと異なる場合にコピーするかどうかを選択します。デフォルトの設定では、既存のファイルと異なる場合にのみファイルがコピーされます。
- **Read only file** : ファイルを読み取り専用にするかどうかを選択します。デフォルトは [OFF] です。
- **非表示のファイル** : ファイルをファイル一覧で非表示にするかどうかを選択します。デフォルトは [OFF] です。

7. 展開規則を構成します。

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

The screenshot shows the XenMobile Configure interface for the 'Files Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Files Policy' page is active, showing a sidebar with 'Files Policy' selected. The main content area has a title 'Files Policy' and a description: 'This policy lets you upload files and executable scripts to devices.' Below this is a 'Choose delivery groups' section with a search bar and a 'Search' button. A list of delivery groups is shown, with 'AllUsers' selected. To the right, there is a 'Delivery groups to receive app assignment' section with a list containing 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# フォントデバイスポリシー

Apr 27, 2017

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

注：iOSの場合、このポリシーはiOS 7.0以降にのみ適用されます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** をクリックした後、**[End user]** の下の **[Font]** をクリックします。**[Font Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' section is expanded to show 'Font Policy'. The 'Font Policy' page has a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is selected. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is a large text area, also empty. At the bottom right of the main content area is a green button labeled 'Next >'.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Font Policy' configuration steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS' and 'Mac OS X' are both checked. The main content area is titled 'Policy Information' and contains the following fields and options:

- User-visible name:** A text input field with a help icon.
- Font file:** A text input field with a 'Browse' button.
- Policy Settings:**
  - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'.
  - Duration until removal (in days):** A date picker field.
  - Allow user to remove policy:** A dropdown menu currently set to 'Always'.
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **User-visible name** : ユーザーのフォント一覧に表示される名前を入力します。
- **Font file** : [参照] をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、そのファイルを選択します。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。

Mac OS Xの設定の構成

The screenshot shows the XenMobile configuration interface for a Font Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows 'Font Policy' with sub-items: '1 Policy Info', '2 Platforms' (with 'iOS' and 'Mac OS X' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you add additional fonts to an iOS and Mac OS X device. The policy is available on iOS 7 and later devices.' Below this are input fields for 'User-visible name' and 'Font file\*' (with a 'Browse' button). The 'Policy Settings' section includes: 'Remove policy' with radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'; a date picker; 'Allow user to remove policy' with a dropdown set to 'Always'; and 'Profile scope' with a dropdown set to 'User'. A 'OS X 10.7+' label is positioned to the right of the 'Profile scope' dropdown. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **User-visible name** : ユーザーのフォント一覧に表示される名前を入力します。
- **Font file** : **[Browse]** をクリックしてユーザーのデバイスに追加するフォントファイルの場所に移動し、そのファイルを選択します。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
  - **[Profile scope]** の横にある、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。

#### 7. 展開規則を構成します。

8. **[Next]** をクリックします。**[Font Policy]** 割り当てページが開きます。

The screenshot shows the XenMobile Configure interface for a 'Font Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Font Policy' section is active, showing a sidebar with 'Policy Info', 'Platforms', and 'Assignment' (highlighted). The 'Assignment' section is expanded to show 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list with 'AllUsers' checked and 'sales' unchecked. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. There are 'Back' and 'Save' buttons at the bottom right.

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の **[Delivery groups to receive app assignment]** の一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# iOSおよびMac OS Xプロファイルのインポートデバイスポリシー

Apr 27, 2017

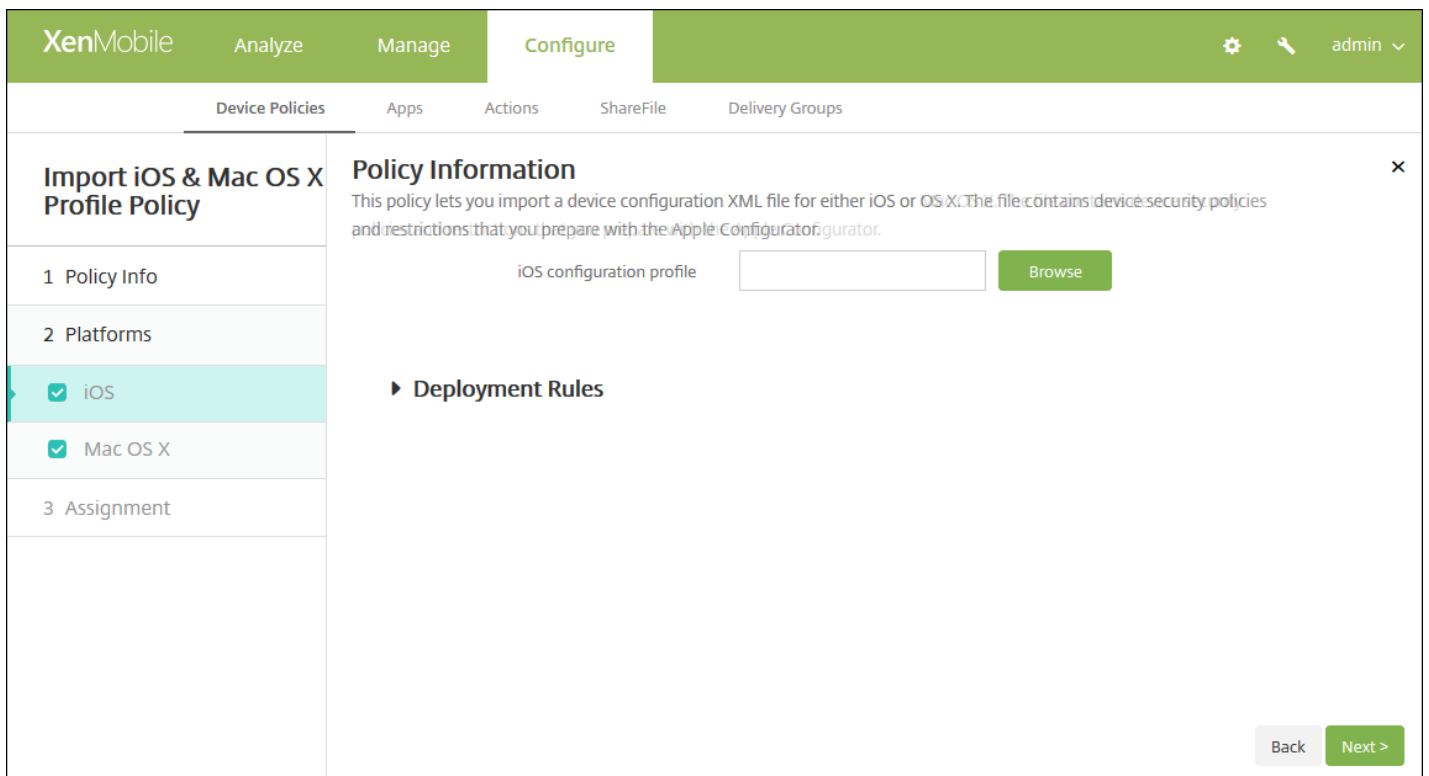
iOSおよびOS Xデバイス用のデバイス構成XMLファイルをXenMobileにインポートできます。XMLファイルには、Apple Configuratorを使用して作成するデバイスセキュリティポリシーおよび制限が含まれます。

この記事で説明するように、Apple Configuratorを使用してiOSデバイスをSupervisedモードにできます。Apple Configuratorの使用による構成ファイルの作成について詳しくは、Appleの[Configuratorヘルプページ](#)を参照してください。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。
2. **[Add]** をクリックします。 **[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[Custom]** の下の **[Import iOS & Mac OS X Profile]** をクリックします。 **[Import iOS & Mac OS X Profile Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure (which is highlighted). Below these are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. A dialog box titled 'Import iOS & Mac OS X Profile Policy' is open. The dialog has a sidebar on the left with three sections: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. Under '1 Policy Info', there are two input fields: 'Policy Name\*' and 'Description'. Under '2 Platforms', there are two checked checkboxes: 'iOS' and 'Mac OS X'. At the bottom right of the dialog, there is a green button labeled 'Next >'. The background of the console shows the 'Configure' tab and the 'Device Policies' sub-tab.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。 **[Policy Platforms]** ページが開きます。



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

1つのプラットフォームの設定の構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

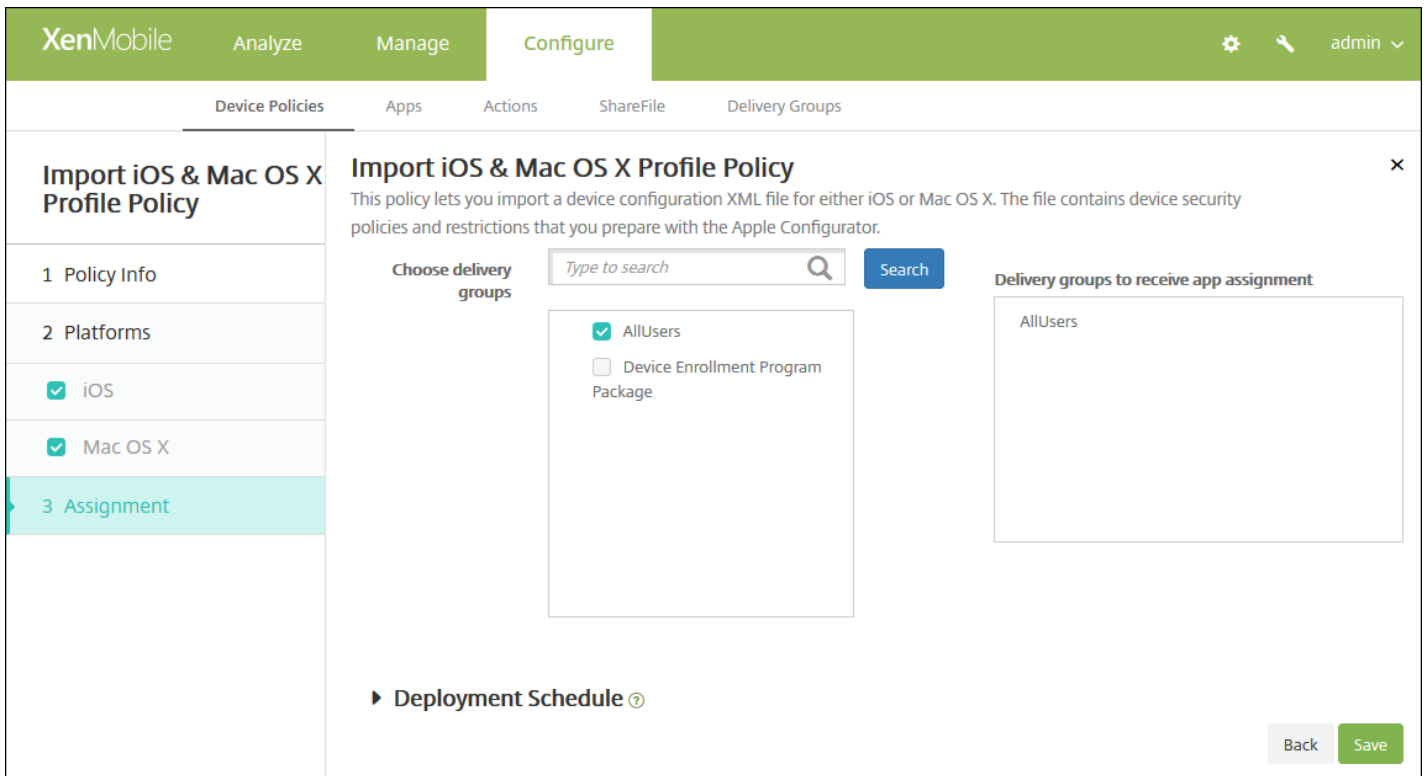
7. 選択したプラットフォームごとに、次の設定を構成します。

- **iOS configuration profile** または **Mac OS X configuration profile** : **[Browse]** をクリックしてインポートする構成ファイルの場所に移動し、そのファイルを選択します。

8. 展開規則を構成します。

9. **[Next]** をクリックします。 **[Import iOS & Mac OS X Profile Policy]** 割り当てページが開きます。





10. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

12. **[Save]** をクリックしてポリシーを保存します。

Apple Configuratorを使用してiOSデバイスをSupervisedモードにする

Apple Configuratorを使用するには、AppleコンピューターでOS X 10.7.2以降を実行している必要があります。

## Important

デバイスをSupervisedモードにすると、特定のバージョンのiOSがデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリケーションがデバイスから完全に消去されます。

1. iTunesからApple Configuratorをインストールします。
2. iOSデバイスをAppleコンピューターに接続します。
3. Apple Configuratorを起動します。監視の準備が整っているデバイスがあることがConfiguratorに表示されます。
4. デバイスの監視の準備を行うには：
  - a. **[Supervision]** コントロールを **[On]** に切り替えます。構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。
  - b. 必要に応じてデバイスの名前を指定します。
  - c. 最新バージョンのiOSをインストールする場合、**[iOS]** ボックスの一覧で **[Latest]** を選択します。
5. デバイスの監視の準備が整ったら、**[Prepare]** をクリックします。

# Samsung SAFEのキオスクデバイスポリシー

Apr 27, 2017

XenMobileでキオスクポリシーを作成して、特定のアプリケーションのみをSamsung SAFEデバイスで使用できるように指定することができます。このポリシーは、特定の種類またはクラスのアプリケーションのみを実行するように設計されているコーポレートデバイスで役立ちます。また、このポリシーを使用して、デバイスがキオスクモードのときのホーム画面およびロック画面の壁紙用のカスタムイメージを選択することができます。

## Samsung SAFEデバイスをキオスクモードにするには

1. 「[Samsung MDMライセンスキーデバイスポリシー](#)」の説明に従って、モバイルデバイス上でSamsung SAFE APIキーを有効にします。この手順で、Samsung SAFEデバイス上でポリシーを有効にします。
2. 「[接続スケジュールデバイスポリシー](#)」の説明に従って、Androidデバイスの接続スケジュールポリシーを有効にします。この手順で、Androidデバイスの接続をXenMobileに戻すことができます。
3. 次のセクションの説明に従って、キオスクデバイスポリシーを追加します。
4. 適切なデリバリーグループに、それら3つのデバイスポリシーを割り当てます。他のポリシー（たとえばアプリケーションインベントリ）をデリバリーグループに含めるかどうかを検討します。

後でキオスクモードからデバイスを削除するには、[キオスクモード]を[無効化]に設定した新しいキオスクデバイスポリシーを作成します。デリバリーグループを更新して、キオスクモードを有効にしたキオスクポリシーを削除し、キオスクモードを無効にするキオスクポリシーを追加します。

## キオスクデバイスポリシーを追加するには

注：

- キオスクモード用に指定したすべてのアプリケーションが、ユーザーのデバイスに既にインストールされている必要があります。
- 一部のオプションは、Samsungモバイルデバイス管理 (MDM) API 4.0以降にのみ適用されます。

1. XenMobileコンソールで、[Configure]の[Device Policies]をクリックします。[Device Policies]ページが開きます。
2. [Add]をクリックします。[Add a New Policy]ダイアログボックスが開きます。
3. [More]を展開した後、[Security]の下の[Kiosk]をクリックします。[Kiosk Policy]ページが開きます。

The screenshot shows the XenMobile interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Kiosk Policy' section is active, with a sidebar containing '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' form includes a 'Policy Name\*' field and a 'Description' field. A 'Next >' button is located at the bottom right of the form area.

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

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

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

The screenshot shows the XenMobile configuration interface for a Kiosk Policy. The left sidebar lists 'Kiosk Policy' with sub-items: '1 Policy Info', '2 Platforms', '3 Assignment', and 'Samsung SAFE'. The main area is titled 'Policy Information' and contains the following settings:

- General**
  - Kiosk mode:  Enable,  Disable
  - Launcher package: [Text input field]
  - Emergency phone number: [Text input field] (MDM 4.0+)
  - Allow navigation bar:  ON (MDM 4.0+)
  - Allow multi-window mode:  ON (MDM 4.0+)
  - Allow status bar:  ON (MDM 4.0+)
  - Allow system bar:  ON
  - Allow task manager:  ON
  - Common SAFE passcode: [Text input field]
- Wallpapers**
  - Define a home wallpaper:  OFF
  - Define a lock wallpaper:  OFF (MDM 4.0+)
- Apps**
  - New app to add\*: [Text input field] [Add]
- Deployment Rules**

At the bottom right, there are 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- **Kiosk mode** : [Enable] または [Disable] を選択します。デフォルトは [Enable] です。 [Disable] をクリックすると、以下のオプションはすべて表示されなくなります。
- **Launcher package** : ユーザーがキオスクアプリケーションを起動できる社内用ランチャーを開発した場合を除き、このフィールドは空白のままにしておくことをお勧めします。社内用ランチャーを使用している場合、ランチャーアプリケーションパッケージの完全な名前を入力します。
- **Emergency phone number** : オプションで電話番号を入力します。紛失したデバイスの発見者が会社に連絡するとき、この番号を使用できます。MDM 4.0以降にのみ適用されます。
- **Allow navigation bar** : キオスクモードのときに、ユーザーにナビゲーションバーを表示して使用できるようにするかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは [ON] です。
- **Allow multi-window mode** : キオスクモードのときに、ユーザーが複数のウィンドウを使用できるようにするかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは [ON] です。
- **Allow status bar** : キオスクモードのときに、ユーザーにステータスバーを表示するかどうかを選択します。MDM 4.0以降にのみ適用されます。デフォルトは [ON] です。

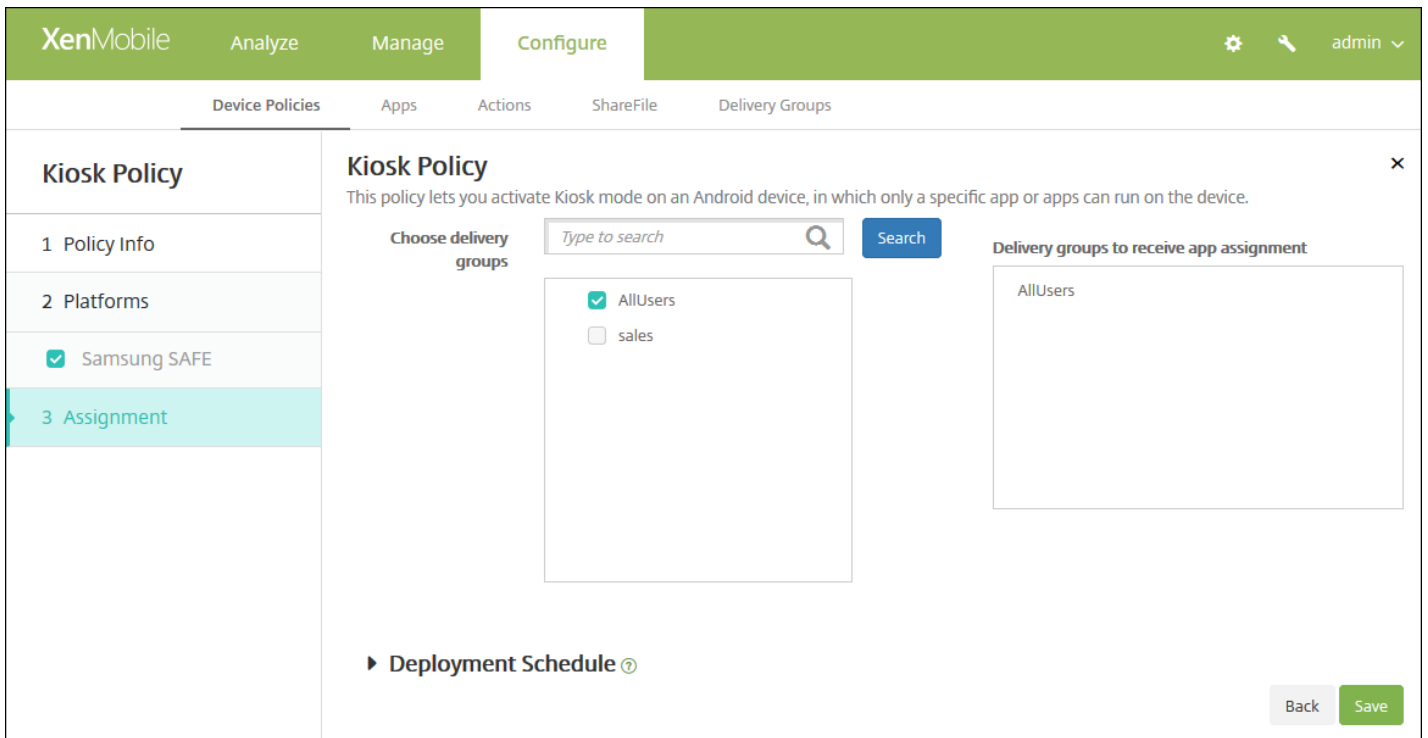
- **Allow system bar** : キオスクモードのときに、ユーザーにシステムバーを表示するかどうかを選択します。デフォルトは [ON] です。
- **Allow task manager** : キオスクモードのときに、ユーザーにタスクマネージャーを表示して使用できるようにするかどうかを選択します。デフォルトは [ON] です。
- **Common SAFE passcode** : すべてのSamsung SAFEデバイスを対象とする汎用パスコードポリシーを設定した場合、オプションとして、このフィールドにパスコードを入力します。
- **壁紙**
  - **Define a home wallpaper** : キオスクモードのときに、ホーム画面でカスタムイメージを使用するかどうかを選択します。デフォルトは [OFF] です。
    - **Home image** : [Define a home wallpaper] を有効にした場合、[Browse] をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
  - **Define a lock wallpaper** : キオスクモードのときに、ロック画面でカスタムイメージを使用するかどうかを選択します。デフォルトは [OFF] です。MDM 4.0以降にのみ適用されます。
    - **Lock image** : [Define a lock wallpaper] を有効にした場合、[Browse] をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。
- **Apps** : キオスクモードに追加するアプリケーションごとに、[Add] をクリックして以下の操作を行います。
  - **New app to add** : 追加するアプリケーションの完全な名前を入力します。たとえば、「com.android.calendar」を入力すると、ユーザーがAndroidのカレンダーアプリケーションを使用できます。
  - [Save] をクリックしてアプリを追加するか、[Cancel] をクリックしてアプリの追加を取り消します。

注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のアプリケーションを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

## 7. 展開規則を構成します。

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



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# Androidのランチャー構成デバイスポリシー

Apr 27, 2017

Citrix Launcherを使用すると、XenMobileによって展開されたAndroidデバイスのユーザーエクスペリエンスをカスタマイズできます。Launcher Configurationポリシーを追加すると、次のCitrix Launcher機能を制御できます。

- ユーザーは管理者が指定したアプリにのみアクセスできるようにAndroidデバイスを管理する。
- Citrix Launcherアイコンのカスタムロゴ画像と、Citrix Launcherのカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

Citrix Launcherを使用するとそれらのデバイスレベルの制約を適用できますが、ランチャーは、デバイス設定（たとえば、Wi-Fi設定、Bluetooth設定、およびデバイスパスコード設定）への組み込みのアクセスを介して、必要な操作上の柔軟性をユーザーに付与します。Citrix Launcherは、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Citrix Launcherを展開すると、XenMobileがそれをインストールし、デフォルトのAndroidランチャーを置換します。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. まず「**Launcher**」と入力し、一覧から **[Launcher Configuration]** を選択します。**[Launcher Configuration Policy]** ページが開きます。
4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Androidプラットフォーム]** 情報ページが開きます。



The screenshot shows the XenMobile configuration interface for a Launcher Configuration Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Launcher Configuration Policy' and contains a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section includes a description, a 'Launcher app configuration' section with 'Define a logo image' and 'Define a background image' (both set to 'ON'), and an 'Allowed apps' table. The table has columns for 'App name', 'Package Name\*', and 'Add'. A 'Password' field is also present. At the bottom right, there are 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- **Define a logo image** : Citrix Launcherアイコンにカスタムロゴ画像を使用するかどうかを選択します。デフォルトは [OFF] です。
- **Logo image** : [Define a logo image] を有効にした場合、[Browse] をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、およびGIFです。
- **Define a background image** : Citrix Launcherの背景にカスタム画像を使用するかどうかを選択します。デフォルトは [OFF] です。
- **Background image** : [Define a background image] を有効にした場合、[Browse] をクリックしてイメージファイルの場所に移動し、そのファイルを選択します。サポートされているファイルの種類は、PNG、JPG、JPEG、およびGIFです。
- **Allowed apps** : Citrix Launcherで許可するアプリケーションごとに、[Add] をクリックして以下の操作を行います。
  - **New app to add** : 追加するアプリケーションの完全な名前を入力します。たとえば、Androidのカレンダーアプリケーションの場合は「com.android.calendar」です。
  - [Save] をクリックしてアプリを追加するか、[Cancel] をクリックしてアプリの追加を取り消します。

注：既存のアプリケーションを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [削除] をクリックし、項目をそのままにするには [キャンセル] をクリックします。

既存の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。

- **パスワード** : Citrix Launcherを終了するために入力する必要があるパスワード。

7. 展開規則を構成します。

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

#### 9. 展開規則を構成します。

10. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

12. **[Save]** をクリックします。

# LDAPデバイスポリシー

Apr 27, 2017

XenMobileでiOSデバイスのLDAPポリシーを作成して、必要なアカウント情報など、使用するLDAPサーバーに関する情報を指定できます。また、LDAPサーバーの照会に使用するLDAP検索ポリシーのセットが提供されます。

このポリシーを構成するには、LDAPホスト名が必要です。

## iOSの設定

## Mac OS Xの設定

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. 新しいポリシーを追加するには **[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]** を展開した後、**[End user]** の下の **[LDAP]** をクリックします。**[LDAP Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'LDAP Policy' and contains a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section is expanded, showing a description: 'This policy lets you configure an LDAP server and search policies for querying the server.' Below this are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). In the 'Platforms' section, 'iOS' and 'Mac OS X' are both checked with green checkmarks. At the bottom right of the main content area, there is a green button labeled 'Next >'.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

## iOSの設定の構成

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### LDAP Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
- 3 Assignment

### Policy Information

This policy lets you configure an LDAP server and search policies for querying the server.

Account description

Account user name

Account password

LDAP host name\*

Use SSL

#### Search Settings

Description*	Scope	Search base*	Add
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

#### Policy Settings

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy

► Deployment Rules

次の設定を構成します。

- **Account description** : オプションで、アカウントの説明を入力します。
- **Account user name** : オプションで、ユーザー名を入力します。
- **Account password** : オプションで、パスワードを入力します。これは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP host name** : LDAPサーバーのホスト名を入力します。このフィールドは必須です。
- **Use SSL** : LDAPサーバーに対してSSL (Secure Socket Layer) 接続を使用するかどうかを選択します。デフォルトは **[ON]** です。
- **Search Settings** : LDAPサーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも1つ入力してください。 **[Add]** をクリックして、以下の操作を行います。
  - **[Description]** : 検索設定の説明を入力します。このフィールドは必須です。
  - **Scope** : ボックスの一覧で **[Base]**、**[One level]**、**[Subtree]** のいずれかを選択して、LDAPツリーをどの深さまで検索するかを定義します。デフォルトは **[Base]** です。
    - **[Base]** を選択すると、**[Search base]** で参照されているノードを検索します。
    - **[One level]** を選択すると、**[Base]** を選択した場合の検索対象ノードとその1つ下のレベルを検索します。
    - **[Subtree]** を選択すると、**[Base]** を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - **Search base** : 検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」

です。このフィールドは必須です。

- [Save] をクリックして検索設定を追加するか、[Cancel] をクリックして検索設定の追加を取り消します。
- 追加する検索設定ごとに上記の手順を繰り返します。

注：既存の検索設定を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存の検索設定を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

- [Policy Settings] の下の [Remove policy] の横にある、[Select date] または [Duration until removal (in days)] をクリックします。
- [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

## Mac OS Xの設定の構成

The screenshot shows the XenMobile configuration interface for an LDAP Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active, and the 'Device Policies' section is selected. The left sidebar shows the policy configuration steps: 1 Policy Info, 2 Platforms (with 'Mac OS X' selected), and 3 Assignment. The main content area is titled 'Policy Information' and contains the following settings:

- Account description:** Text input field.
- Account user name:** Text input field.
- Account password:** Text input field.
- LDAP host name\*:** Text input field.
- Use SSL:** Toggle switch set to 'ON'.
- Search Settings:** A table with columns for 'Description\*', 'Scope', and 'Search base\*', and an 'Add' button.
- Policy Settings:**
  - Remove policy:** Radio buttons for 'Select date' (selected) and 'Duration until removal (in days)'.
  - Allow user to remove policy:** Dropdown menu set to 'Always'.
  - Profile scope:** Dropdown menu set to 'User', with a note 'OS X 10.7+'.
- Deployment Rules:** Section header with a right-pointing arrow.

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Account description** : オプションで、アカウントの説明を入力します。
- **Account user name** : オプションで、ユーザー名を入力します。
- **Account password** : オプションで、パスワードを入力します。これは、暗号化されたプロファイルに対してのみ使用します。
- **LDAP host name** : LDAPサーバーのホスト名を入力します。このフィールドは必須です。
- **Use SSL** : LDAPサーバーに対してSSL (Secure Socket Layer) 接続を使用するかどうかを選択します。デフォルトは **[ON]** です。
- **Search Settings** : LDAPサーバーの照会に使用する検索設定を追加します。必要な数の検索設定を入力できますが、アカウントを便利にするために、検索設定を少なくとも1つ入力してください。 **[Add]** をクリックして、以下の操作を行います。
  - **[Description]** : 検索設定の説明を入力します。このフィールドは必須です。
  - **Scope** : ボックスの一覧で **[Base]**、**[One level]**、**[Subtree]** のいずれかを選択して、LDAPツリーをどの深さまで検索するかを定義します。デフォルトは **[Base]** です。
    - **[Base]** を選択すると、**[Search base]** で参照されているノードを検索します。
    - **[One level]** を選択すると、**[Base]** を選択した場合の検索対象ノードとその1つ下のレベルを検索します。
    - **[Subtree]** を選択すると、**[Base]** を選択した場合の検索対象ノードに加え、その子ノードを深さにかかわらずすべて検索します。
  - **Search base** : 検索の開始位置とするノードへのパスを入力します。たとえば、「ou=people」や「0=example corp」です。このフィールドは必須です。
  - **[Save]** をクリックして検索設定を追加するか、**[Cancel]** をクリックして検索設定の追加を取り消します。
  - 追加する検索設定ごとに上記の手順を繰り返します。

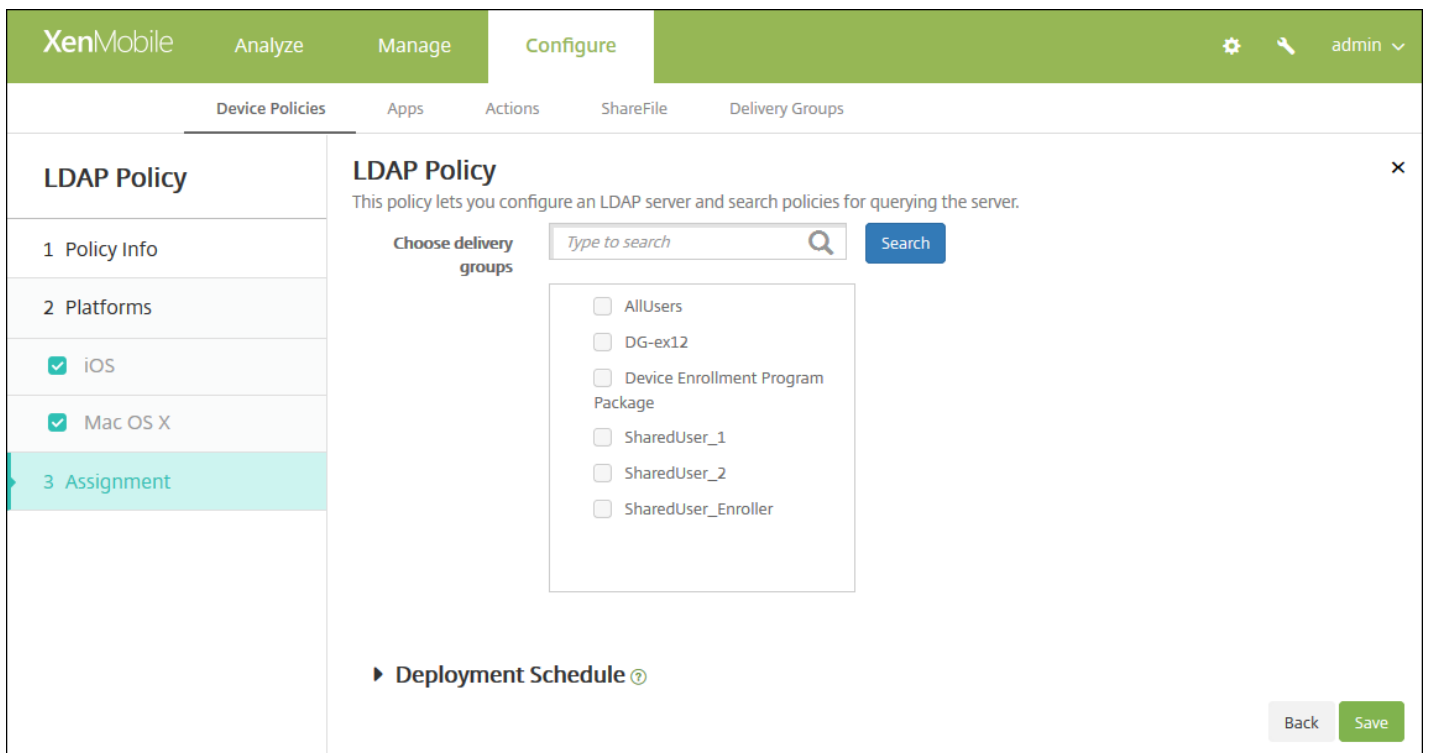
注：既存の検索設定を削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存の検索設定を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

- **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
- **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
- **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
- **[Profile scope]** で、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。

## 7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[LDAP Policy]** 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# 位置情報デバイスポリシー

Apr 27, 2017

XenMobileで位置情報デバイスポリシーを作成して、地理的な境界を適用したり、ユーザーのデバイスの位置や移動を追跡したりすることができます。定義された境界（ジオフェンス）の外にユーザーが出た場合、XenMobileで選択的ワイプまたは完全なワイプを直ちに実行することができます。また、許可された場所にユーザーが戻ることができるように、一定の時間が経過してから実行することもできます。

位置情報デバイスポリシーは、iOSおよびAndroidに対して作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[Location]** をクリックします。**[Location Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile' and tabs for 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Location Policy' and has a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section has two checkboxes, 'iOS' and 'Android', both of which are checked. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



**XenMobile** Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Location Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Android
- 3 Assignment

### Policy Information

This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.

**Device agent configuration**

Location Timeout: 1 Minutes

Tracking duration: 6 Hours

Accuracy: 328 Feet

Report if Location Services are disabled: OFF

Geofencing: OFF

► Deployment Rules

Back Next >

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。
- ジオフェンシング

**Geofencing**

Radius: 16400 Feet

Center point latitude\*: 0.000000

Center point longitude\*: 0.000000

Warn user on perimeter breach: OFF

Wipe corporate data on perimeter breach: OFF

[Geofencing] を選択した場合は、次の設定を構成します。

- **Radius** : 数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。有効な半径の値は次のとおりです。
  - 164 ~ 164000フィート
  - 50 ~ 50000m
  - 54 ~ 54680ヤード
  - 1 ~ 31マイル
- **Center point latitude** : 緯度 (37.787454など) を入力して、ジオフェンスの中心点の緯度を定義します。
- **Center point longitude** : 経度 (122.402952など) を入力して、ジオフェンスの中心点の経度を定義します。
- **Warn user on perimeter breach** : 定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは **[OFF]** です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- **Wipe corporate data on perimeter breach** : ユーザーのデバイスが境界の外に出た場合にワイプするかどうかを選択します。デフォルトは **[OFF]** です。このオプションを有効にすると、 **[Delay on local wipe]** フィールドが表示されます。
  - 数値を入力し、一覧から **[Seconds]** または **[Minutes]** を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

Androidの設定の構成

The screenshot shows the XenMobile configuration interface for a Location Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Location Policy' section is active, showing a sidebar with '1 Policy Info', '2 Platforms' (with 'iOS' and 'Android' checked), and '3 Assignment'. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.' Below this is the 'Device agent configuration' section with the following settings: 'Poll interval' is set to '10' with a unit dropdown set to 'Minutes'; 'Report if Location Services is disabled' is set to 'OFF'; and 'Geofencing' is set to 'OFF'. At the bottom right, there are 'Back' and 'Next >' buttons.

- **Poll interval** : 数値を入力して、ボックスの一覧で **[Minutes]**、**[Hours]**、**[Days]** のいずれかを選択し、XenMobile がデバイスの位置情報の特定を試行する頻度を設定します。有効な値は、1~1440分、1~24時間、または任意の日数です。デフォルトは10分です。この値を10分未満に設定すると、デバイスのバッテリー寿命に悪影響を及ぼす可能性があります。
- **Report if Location Services are disabled** : GPSが無効になっている場合に、デバイスからXenMobileにレポートを送信するかどうかを選択します。デフォルトは **[OFF]** です。
- ジオフェンシング

The screenshot shows the detailed configuration for Geofencing. The 'Geofencing' toggle is turned ON. The 'Radius' is set to 16400 with a unit dropdown set to 'Feet'. The 'Center point latitude' and 'Center point longitude' are both set to 0.000000. The 'Warn user on perimeter breach' toggle is OFF. Under 'Device connects to XenMobile for policy refresh', the option 'Perform no action on perimeter breach' is selected.

[Geofencing] を選択した場合は、次の設定を構成します。

- **Radius** : 数値を入力して、ボックスの一覧で半径の測定に使用する単位を選択します。デフォルトは16,400フィートです。有効な半径の値は次のとおりです。

- 164 ~ 164000フィート
- 1 ~ 50km
- 50 ~ 50000m
- 54 ~ 54680ヤード
- 1 ~ 31マイル
- **Center point latitude** : 緯度 (37.787454など) を入力して、ジオフェンスの中心点の緯度を定義します。
- **Center point longitude** : 経度 (122.402952など) を入力して、ジオフェンスの中心点の経度を定義します。
- **Warn user on perimeter breach** : 定義された境界の外にユーザーが出た場合に、警告メッセージを表示するかどうかを選択します。デフォルトは **[OFF]** です。警告メッセージの表示にXenMobileへの接続は必要ありません。
- **Device connects to XenMobile for policy refresh** : ユーザーが境界の外に出た場合のオプションを以下から1つ選択します。
  - **Perform no action on perimeter breach** : 何もしません。これがデフォルトの設定です。
  - **Wipe corporate data on perimeter breach** : 指定した時間が経過すると、企業データがワイプされます。このオプションを有効にすると、 **[Delay on local wipe]** フィールドが表示されます。
    - 数値を入力し、一覧から **[Seconds]** または **[Minutes]** を選択して、ユーザーのデバイスの企業データがワイプされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによって選択的にワイプされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。
  - **Delay on lock** : 指定した時間が経過すると、ユーザーのデバイスがロックされます。このオプションを有効にすると、 **[Delay on lock]** フィールドが表示されます。
    - 数値を入力し、一覧から **[Seconds]** または **[Minutes]** を選択して、ユーザーのデバイスがロックされるまでの猶予時間を設定します。これにより、デバイスがXenMobileによってロックされる前に、許可された場所にユーザーが戻る機会を設けることができます。デフォルトは0秒です。

## 7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Location Policy]** 割り当てページが開きます。

The screenshot shows the XenMobile configuration interface for a Location Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main content area is titled 'Location Policy' and contains the following sections:

- Policy Info**
- Platforms**: iOS and Android are both checked.
- Assignment**: This section is highlighted. It includes a search bar for delivery groups, a list of delivery groups with 'AllUsers' checked and 'sales' unselected, and a 'Delivery groups to receive app assignment' box containing 'AllUsers'.
- Deployment Schedule**: A section with a question mark icon.

At the bottom right, there are 'Back' and 'Save' buttons.

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。選択されたグループは、**[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# メールデバイスポリシー

Apr 27, 2017

XenMobileでメールデバイスポリシーを追加して、ユーザーのiOSデバイスまたはMac OS Xデバイスのメールアカウントを構成することができます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. 新しいポリシーを追加するには [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 [Mail] をクリックします。[Mail Policy] ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Mail Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is currently selected. The main area displays 'Policy Information' with a note: 'This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the configuration area.

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

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

5. [Next] をクリックします。メールポリシーの [Platforms] ページが開きます。

The screenshot shows the XenMobile console interface, similar to the previous one. The '2 Platforms' section in the sidebar is now selected. The main area displays 'Policy Information' with the same note. There are five input fields: 'Account description\*', 'Account type' (a dropdown menu with 'IMAP' selected), 'Path prefix', 'User display name\*', and 'Email address\*'. A 'Next >' button is located at the bottom right of the configuration area.

**Incoming email**

Email server host name\*

Email server port\*

User name\*

Authentication type

Password

Use SSL

**Outgoing email**

Email server host name\*

Email server port\*

User name\*

Authentication type

Password

Outgoing password same as incoming

Use SSL

**Policy**

Authorize email move between accounts  iOS 5.0+

Sending email only from mail app  iOS 5.0+

Disable mail recents syncing  iOS 6.0+

Enable S/MIME  iOS 5.0+

**Policy Settings**

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy

**► Deployment Rules**

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

1つのプラットフォームの設定の構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームで次の設定を構成します。

- **Account description** : メールおよび設定アプリケーションに表示される、アカウントの説明を入力します。このフィールドは必須です。
- **Account type** : ボックスの一覧で **[IMAP]** または **[POP]** をクリックし、ユーザーアカウントで使用するプロトコルを選択します。デフォルトは **[IMAP]** です。 **[POP]** を選択した場合、以下の **[パスのプレフィックス]** オプションは表示されなくなります。
- **Path prefix** : 「**INBOX**」と入力します。プレフィックスが**INBOX**ではない場合は、IMAPメールアカウントのパスプレフィックスを入力します。このフィールドは必須です。
- **User display name** : メッセージなどで使用する完全なユーザー名を入力します。このフィールドは必須です。
- **Email address** : アカウントの完全なメールアドレスを入力します。このフィールドは必須です。
- 受信メール設定
  - **Email server host name** : 受信メールサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
  - **Email server port** : 受信メールサーバーのポート番号を入力します。デフォルトは**143**です。このフィールドは必須です。
  - **User name** : メールアカウントのユーザー名を入力します。この名前は一般的に、ユーザーのメールアドレスの@記号より前の部分と同じです。このフィールドは必須です。
  - **Authentication type** : ボックスの一覧から、使用する認証の種類をクリックします。デフォルトは **[Password]** です。 **[なし]** を選択した場合、以下の **[パスワード]** フィールドは表示されなくなります。
  - **Password** : 任意で、受信メールサーバーのパスワードを入力します。
  - **Use SSL** : 受信メールサーバーでSSL (Secure Socket Layer) 認証を使用するかどうかを選択します。デフォルトは **[OFF]** です。
- 送信メール設定
  - **Email server host name** : 送信メールサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
  - **Email server port** : 送信メールサーバーのポート番号を入力します。ポート番号を入力しなかった場合、指定されたプロトコルのデフォルトポートが使用されます。
  - **User name** : メールアカウントのユーザー名を入力します。これは一般的に、ユーザーのメールアドレスの@記号より前の部分と同じです。このフィールドは必須です。
  - **Authentication type** : ボックスの一覧から、使用する認証の種類をクリックします。デフォルトは **[Password]** です。 **[None]** を選択した場合、以下の **[Password]** フィールドは表示されなくなります。
  - **Password** : 任意で、送信メールサーバーのパスワードを入力します。
  - **Outgoing password same as incoming** : 受信パスワードと送信パスワードが同じであるかどうかを選択します。デフォルトは **[OFF]** で、パスワードが異なることを意味します。 **[ON]** に設定した場合、直前の **[Password]** フィールドは表示されなくなります。
  - **Use SSL** : 送信メールサーバーでSSL (Secure Socket Layer) 認証を使用するかどうかを選択します。デフォルトは **[OFF]** です。
- ポリシー
  - 注 : iOSの設定を構成する場合、これらのオプションはiOS 5.0以降にのみ適用されます。Mac OS Xを構成する場合、制限はありません。
  - **Authorize email move between accounts** : ユーザーが電子メールをこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。デフォルトは **[OFF]** です。
  - **Sending email only from mail app** : ユーザーの電子メールの送信をiOSメールアプリケーションからのみに制限するかどうかを選択します。
  - **Disable mail recents syncing** : ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは **[OFF]** です。このオプションはiOS 6.0以降にのみ適用されます。
  - **Enable S/MIME** : このアカウントでS/MIME認証および暗号化をサポートするかどうかを選択します。デフォルト



は [OFF] です。 [ON] に設定した場合、以下の2つのフィールドが表示されます。

- **Signing identity credential** : ボックスの一覧で、使用する署名資格情報を選択します。
- **Encryption identity credential** : ボックスの一覧で、使用する暗号化資格情報を選択します。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。
  - [Profile scope] ボックスの隣りにある [User] または [System] をクリックします。デフォルトは [User] です。このオプションはMax OS X 10.7以降でのみ使用できます。

## 8. 展開規則を構成します。

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

The screenshot shows the XenMobile Configure interface for a Mail Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Mail Policy' and includes a sub-header 'Mail Policy' with a close button. Below the sub-header is a description: 'This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search box and a list of groups: 'AllUsers' (checked), 'DG-ex12', 'Device Enrollment Program Package', 'SharedUser\_1', 'SharedUser\_2', and 'SharedUser\_Enroller'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. At the bottom, there is a 'Deployment Schedule' section with a plus icon, and 'Back' and 'Save' buttons.

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] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、 [OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。 [OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment

**has failed**] をクリックします。デフォルトのオプションは、**[On every connection]** です。

- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

12. **[Save]** をクリックしてポリシーを保存します。

# 管理対象ドメインデバイスポリシー

Apr 27, 2017

メールおよびSafariブラウザーに適用する管理対象ドメインを定義できます。管理対象ドメインを使用すると、Safariを使用してドメインからダウンロードしたドキュメントを開くことができるアプリケーションを制御して、会社のデータを保護することができます。URLまたはサブドメインを使用して、ユーザーがドキュメント、添付ファイルなど、ブラウザーからダウンロードしたものを開く方法を制御します。このポリシーは、iOS 8以降の監視対象デバイスでのみサポートされます。iOSデバイスをSupervisedモードに設定する手順については、「[Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには](#)」を参照してください。

ユーザーが管理対象メールドメインの一覧に含まれていないドメインの宛先にメールを送信すると、ユーザーのデバイス上該当するメッセージにフラグが付き、メッセージの送信先が社内ドメイン外の人物であることが警告されます。

ユーザーがSafariを使用して、管理対象Webドメイン一覧に含まれているWebドメインから取得したアイテム（ドキュメントや添付ファイルなど、ダウンロードしたもの）を開こうとすると、適切な社内アプリケーションによってアイテムが開かれます。アイテムが管理対象Webドメイン一覧にあるWebドメインから取得されたものでない場合、ユーザーは社内アプリケーションでアイテムを開くことができません。この場合、ユーザーは各自の非管理対象アプリケーションを使用する必要があります。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[Security]** の下の **[Managed domains]** をクリックします。**[Managed Domains Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Under 'Configure', there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is active, showing a list of 'Managed Domains Policy' on the left. The selected policy is '1 Policy Info'. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you define managed domains that apply to the Safari browser. The payloads are supported only on iOS 8 and later supervised devices.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[iOS Platform]** ページが開きます。

The screenshot shows the XenMobile configuration interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure. Below these are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The main content area is titled 'Managed Domains Policy' and includes a sidebar with sections: 1 Policy Info, 2 Platforms (with 'iOS' selected), and 3 Assignment. The main content area has a 'Policy Information' section with a close button, followed by 'Managed Domains' (Unmarked Email Domains) and 'Managed Safari Web Domains' (Managed Web Domain), each with an 'Add' button. Below these are 'Policy Settings' with radio buttons for 'Remove policy' (Select date or Duration until removal) and a dropdown for 'Allow user to remove policy' (Always). At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

## ドメインを指定する方法

6. 次の設定を構成します。

### ● 管理対象ドメイン

- **Unmarked Email Domains** : 一覧に含めるメールアドレスごとに、**[Add]** をクリックして以下の操作を行います。
  - **Managed Email Domain** : メールアドレスを入力します。
  - **[Save]** をクリックしてメールアドレスを保存するか、**[Cancel]** をクリックして操作を取り消します。
- **管理対象のSafari Webドメイン** : 一覧に含めるWebドメインごとに、**[Add]** をクリックして以下の操作を行います。
  - **Managed Web Domain** : Webドメインを入力します。
  - **[Save]** をクリックしてWebドメインを保存するか、**[Cancel]** をクリックして操作を取り消します。

注 : 既存のドメインを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには **[Delete]** をクリックし、項目をそのままにするには **[Cancel]** をクリックします。

既存のドメインを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、**[Save]** をクリックして変更した項目を保存するか、**[Cancel]** をクリックして項目を変更せずそのままにします。

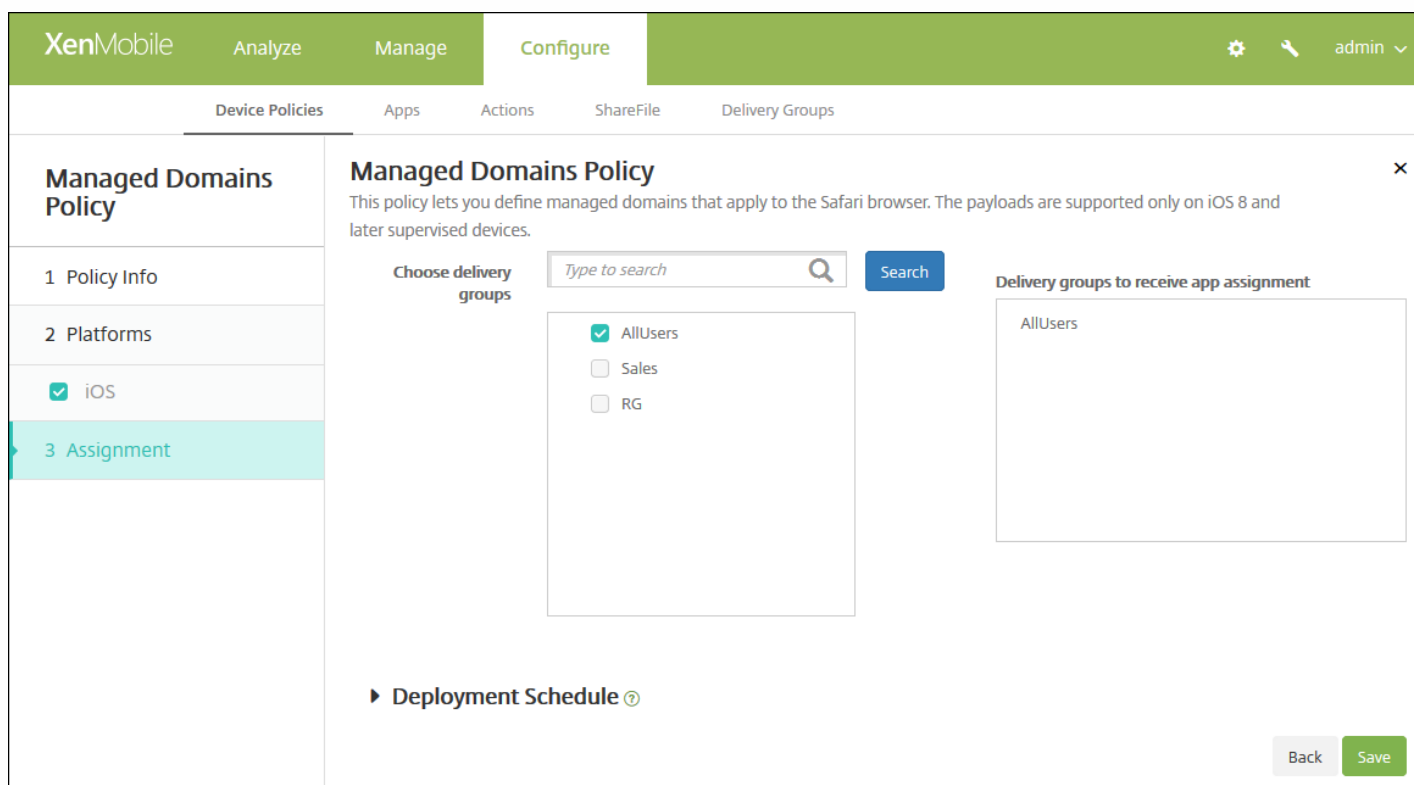
### ● ポリシー設定

- **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
- **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。

- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

### 7. 展開規則を構成します。

8. [Next] をクリックします。[Managed Domains Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

ます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

# MDMオプションデバイスポリシー

Apr 27, 2017

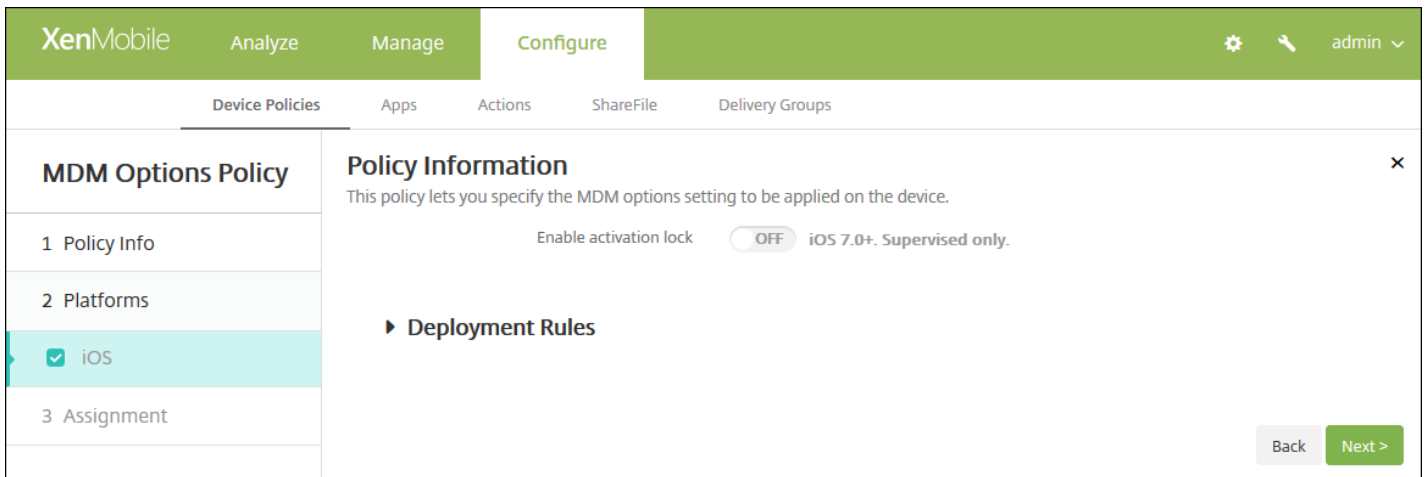
XenMobileでデバイスポリシーを作成して、監視対象のiOS 7.0以降のモバイルデバイスで [iPhone/iPadを探す] の [アクティベーションロック] を管理することができます。iOSデバイスをSupervisedモードに設定する手順については、「[Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには](#)」または「[iOSバルク登録](#)」を参照してください。

アクティベーションロックは、紛失したり、盗まれたりしたデバイスが再アクティベーションされないようにすることを目的とした [iPhone/iPadを探す] の機能であり、ユーザーのApple IDおよびパスワードを必須にすることで、誰かが [iPhoneを探す] をオフにしたり、デバイスを消去したり、デバイスを再アクティベーションして使用したりするのを防ぎます。XenMobileでは、MDMオプションデバイスポリシーでアクティベーションロックを有効にすることにより、必須とされているApple IDおよびパスワードの入力をバイパスできます。ユーザーから返却されたデバイスで [iPhoneを探す] が有効になっていた場合、Appleの資格情報なしでXenMobileコンソールからデバイスを管理することができます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[End user]** の下の **[MDM Options]** をクリックします。**[MDM Options Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. Below this, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'MDM Options Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you specify the MDM options setting to be applied on the device.' There are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area). A 'Next >' button is located at the bottom right of the form. The left sidebar shows a navigation menu with '1 Policy Info' selected, '2 Platforms', and '3 Assignment'.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[iOS MDM ポリシー プラットフォーム]** ページが開きます。

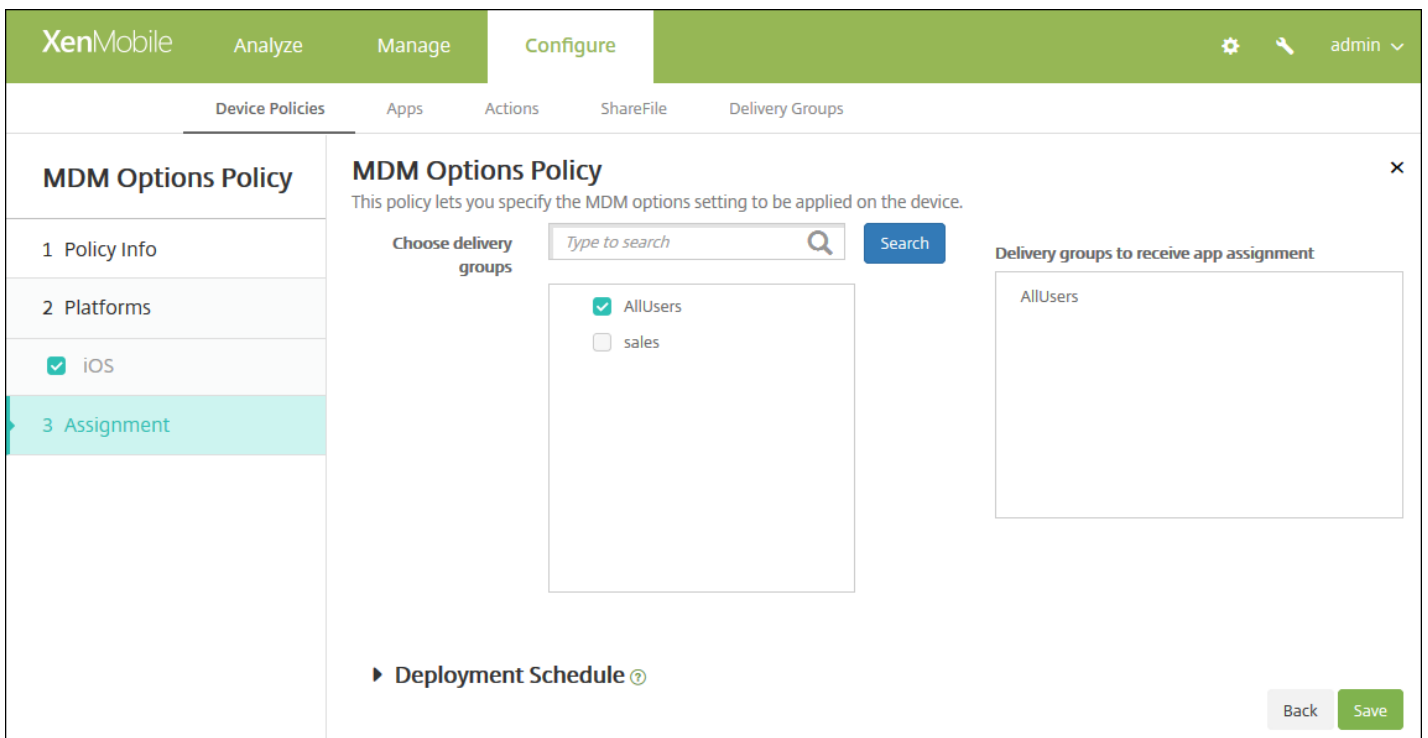


6. 次の設定を構成します。

- アクティベーション ロックを有効化：このポリシーを展開するデバイスでアクティベーションロックを有効にするかどうかを選択します。デフォルトは **[OFF]** です。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[MDM Options Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。テ



フォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。

- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# Microsoft Exchange ActiveSyncデバイスポリシー

Apr 27, 2017

Exchange ActiveSyncデバイスポリシーを使用してユーザーのデバイスのメールクライアントを構成し、Exchangeでホストされている会社のメールにアクセスできるようにすることができます。iOS、MAC OS X、Android HTC、Android TouchDown、Android for Work、Samsung SAFE、Samsung KNOX、Windows Phoneに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、以下のセクションで説明しています。

[iOSの設定](#)

[Mac OS Xの設定](#)

[Android HTCの設定](#)

[Android TouchDownの設定](#)

[Android for Workの設定](#)

[Samsung SAFEおよびSamsung KNOXの設定](#)

[Windows Phoneの設定](#)

このポリシーを作成するには、事前にExchange Serverのホスト名またはIPアドレスを把握しておく必要があります。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[Exchange]** をクリックします。**[Exchange Policy]** 情報ページが開きます。

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' section is active, showing a list of platforms on the left and a 'Policy Information' form on the right. The form includes a 'Policy Name\*' field and a 'Description' text area. A 'Next >' button is located at the bottom right of the form area.

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成

次の設定を構成します。

- **Exchange ActiveSyncアカウント名**：ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **Exchange ActiveSyncホスト名**：メールサーバーのアドレスを入力します。
- **Use SSL**：ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは **[ON]** です。
- **Domain**：Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ\${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User**：Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ\${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address**：ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ\${user.mail}を使用して、ユーザーのメールアドレス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。
- **メールの同期間隔**：一覧から、メールをExchange Serverと同期する頻度を選択します。デフォルトは、**[3 days]** です。
- **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。デフォルトは、**None**です。
- **Authorize email move between accounts**：ユーザーが電子メールをこのアカウントから別のアカウントに移動したり、ほかのアカウントから転送および返信したりできるようにするかどうかを選択します。デフォルトは **[OFF]** です。
- **Send email only from email app**：ユーザーの電子メールの送信をiOSメールアプリケーションからのみに制限するかどうかを選択します。デフォルトは、**[OFF]** です。
- **Disable email recent syncing**：ユーザーが最近のアドレスを同期できないようにするかどうかを選択します。デフォルトは **[OFF]** です。このオプションはiOS 6.0以降にのみ適用されます。
- **Enable S/MIME**：このアカウントでS/MIME認証および暗号化をサポートするかどうかを選択します。デフォルト

は [OFF] です。 [ON] に設定した場合、以下の2つのフィールドが表示されます。

- **Signing identity credential** : デフォルトは [None] です。
- **Encryption identity credential** : デフォルトは [None] です。
- **Enable per message S/MIME switch** : ユーザーがメッセージごとに送信メールを暗号化できるようにするかどうかを選択します。デフォルトは、 [OFF] です。

## Mac OS Xの設定の構成

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Mac OS X' is selected. The 'Policy Information' section contains the following fields and options:

- Exchange ActiveSync account name\*
- User\*
- Email address\*
- Password
- Internal Exchange host
- Internal server port
- Internal server path
- Use SSL for internal Exchange host:  ON
- External Exchange host

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Exchange ActiveSync account name** : ユーザーのデバイスに表示されるメールアカウントの説明を入力します。
- **User** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ\${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ\${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Password** : 任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Internal Exchange host** : Exchangeのホスト名を内部と外部で別のものにする場合、任意で内部のExchangeホスト名を入力します。
- **Internal server port** : Exchangeのサーバーポートを内部と外部で別のものにする場合、任意で内部のExchangeサーバーのポート番号を入力します。
- **Internal server path** : Exchangeのサーバーパスを内部と外部で別のものにする場合、任意で内部のExchangeサーバーパスを入力します。
- **Use SSL for internal Exchange host** : ユーザーのデバイスと内部のExchangeホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは [ON] です。
- **External Exchange host** : Exchangeのホスト名を内部と外部で別のものにする場合、任意で外部のExchangeホスト名を

入力します。

- **External server port** : Exchangeのサーバーポートを内部と外部で別のものにする場合、任意で外部のExchangeサーバーのポート番号を入力します。
- **External server path** : Exchangeのサーバーパスを内部と外部で別のものにする場合、任意で外部のExchangeサーバーパスを入力します。
- **Use SSL for external Exchange host** : ユーザーのデバイスと外部のExchangeホスト間の接続をセキュリティで保護するかどうかを選択します。デフォルトは **[ON]** です。
- **Allow Mail Drop** : ユーザーが2台のMac間で、既存のネットワークに接続することなくワイヤレスでファイルを共有できるようにするかどうかを選択します。デフォルトは **[OFF]** です。

## Android HTCの設定の構成

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and is divided into three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several options are listed with checkboxes, including 'Android HTC' which is selected. The 'Policy Information' section contains the following fields: 'Configuration display name\*', 'Server address\*', 'User ID\*', 'Password', 'Domain', and 'Email address\*'. The 'Use SSL' option is a toggle switch currently set to 'ON'. Below these fields is a section for 'Deployment Rules'. At the bottom right of the configuration area are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Configuration display name** : ユーザーのデバイスで表示される、このポリシーの名前を入力します。
- **Server address** : Exchange Serverのホスト名またはIPアドレスを入力します。
- **User ID** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ `{user.username}` を使用して、ユーザーの名前を自動的に検索することができます。
- **Password** : 任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Domain** : Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ `{user.domainname}` を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ `{user.mail}` を使用して、ユーザーのメールアドレスを自動的に検索することができます。
- **Use SSL** : ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは **[ON]** です。

## Android TouchDownの設定の構成

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The interface is divided into a sidebar and a main content area. The sidebar on the left lists various policy categories, with 'Exchange Policy' selected. The main content area is titled 'Policy Information' and contains the following sections:

- Policy Information:** This section provides instructions and fields for configuring Microsoft Exchange ActiveSync. It includes a text box for 'Server name or IP address\*', a 'Domain' field, a 'User ID\*' field, a 'Password' field, an 'Email address' field, and a dropdown menu for 'Identity credential (keystore or PKI)' set to 'None'.
- Policies and Apps:** This section contains two tables for configuring app settings and policies. The 'App Setting' table has columns for 'Name', 'Value', and an 'Add' button. The 'Policy' table also has columns for 'Name', 'Value', and an 'Add' button.

At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Server name or IP address** : Exchange Serverのホスト名またはIPアドレスを入力します。
- **Domain** : Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ\${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ\${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password** : 任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ\${user.mail}を使用して、ユーザーのメールアドレス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。デフォルトは **[None]** です。
- **App Setting** : オプションで、このポリシーのTouchDownアプリケーション設定を追加します。
- **Policy** : オプションで、このポリシーのTouchDownポリシーを追加します。

## Android for Workの構成

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar lists policy sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work (highlighted), Samsung SAFE, Samsung KNOX, and Windows Phone. The main content area is titled 'Policy Information' and contains a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' Below the description are several input fields: 'Server name or IP address\*', 'Domain', 'User ID\*', 'Password', 'Email address', and 'Identity credential (keystore or PKI)' with a dropdown menu set to 'None'. At the bottom right of the main area are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Server name or IP address** : Exchange Serverのホスト名またはIPアドレスを入力します。
- **Domain** : Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ\${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ\${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password** : 任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ\${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Identity credential (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。デフォルトは **[None]** です。

Samsung SAFEおよびSamsung KNOXの設定の構成



The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows the 'Exchange Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE (highlighted), Samsung KNOX, and Windows Phone. The main area, titled 'Policy Information', contains the following fields and controls:

- Server name or IP address\***: Text input field.
- Domain**: Text input field.
- User ID\***: Text input field.
- Password**: Text input field.
- Email address\***: Text input field.
- Identity credential (keystore or PKI)**: Dropdown menu with 'None' selected.
- Use SSL connection**: Toggle switch set to 'ON'.
- Sync contacts**: Toggle switch set to 'ON'.
- Sync calendar**: Toggle switch set to 'ON'.

At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Server name or IP address** : Exchange Serverのホスト名またはIPアドレスを入力します。
- **Domain** : Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ\${user.domainname}を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ\${user.username}を使用して、ユーザーの名前を自動的に検索することができます。
- **Password** : 任意で、Exchangeユーザーアカウントのパスワードを入力します。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ\${user.mail}を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Identity credential (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の設定の構成

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Exchange Policy' is selected in the left sidebar. The main area is titled 'Policy Information' and contains the following fields:

- Account name or display name\* (text input)
- Server name or IP address\* (text input)
- Domain (text input)
- User ID or user name\* (text input)
- Email address\* (text input)
- Use SSL connection (toggle switch, currently OFF)
- Sync items: Past days to sync (dropdown menu, currently All content)
- Sync scheduling: Frequency (dropdown menu, currently When item arrives)

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

注：このポリシーを使ってユーザーパスワードを設定することはできません。ユーザーはポリシーがプッシュされた後に、デバイスでパラメーターを設定する必要があります。

- **Account name or display name** : Exchange ActiveSyncアカウント名を入力します。
- **Server name or IP address** : Exchange Serverのホスト名またはIPアドレスを入力します。
- **Domain** : Exchange Serverがあるドメインを入力します。このフィールドでシステムマクロ `$(user.domainname)` を使用して、ユーザーのドメイン名を自動的に検索することができます。
- **User ID or user name** : Exchangeユーザーアカウントのユーザー名を指定します。このフィールドでシステムマクロ `$(user.username)` を使用して、ユーザーの名前を自動的に検索することができます。
- **Email address** : ユーザーの完全なメールアドレスを指定します。このフィールドでシステムマクロ `$(user.mail)` を使用して、ユーザーのメールアカウントを自動的に検索することができます。
- **Use SSL connection** : ユーザーのデバイスとExchange Server間の接続をセキュリティで保護するかどうかを選択します。デフォルトは **[OFF]** です。
- **Past days to sync** : ボックスの一覧で、デバイス上のすべてのコンテンツをExchange Serverと過去にさかのぼって同期する日数を選択します。デフォルトは **[All content]** です。
- **None** : ボックスの一覧で、Exchange Serverからデバイスへ送信されるデータの同期に使用するスケジュールを選択します。デフォルトは **[When it arrives]** です。
- **Logging level** : ボックスの一覧で、 **[Disabled]** 、 **[Basic]** 、または **[Advanced]** を選択して、Exchangeのアクティビティをログ記録する詳細レベルを指定します。デフォルトは **[Disabled]** です。

#### 7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Exchange Policy]** 割り当てページが表示されます。

The screenshot shows the XenMobile configuration interface for an Exchange Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Exchange Policy' and includes a description: 'This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.' There are two main sections: 'Choose delivery groups' with a search bar and a list of groups (AllUsers, DG-helen, DG-ex12), and 'Delivery groups to receive app assignment' with a list containing 'AllUsers'. A 'Deployment Schedule' section is partially visible below. At the bottom right, there are 'Back' and 'Save' buttons.

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# 組織情報デバイスポリシー

Apr 27, 2017

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. **[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。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is selected. Below the navigation, there are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is active. On the left, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is highlighted. The main content area is titled 'Organization Info Policy' and contains a description: 'This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.' Below the description are two input fields: 'Policy Name\*' (a text box) and 'Description' (a text area). A 'Next >' button is located at the bottom right of the form.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 必要に応じて、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[iOSプラットフォーム情報]** ページが開きます。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Organization Info Policy

- 1 Policy Info
- 2 Platforms
  - iOS
- 3 Assignment

### Policy Information ✕

This policy lets you specify your organization's information for alert messages that are pushed from XenMobile to the device. The policy is available for iOS 7 and later devices.

Name	<input type="text"/>	?	
			iOS 7.0+
Address	<input type="text"/>	?	
			iOS 7.0+
Phone	<input type="text"/>	?	
			iOS 7.0+
Email	<input type="text"/>	?	
			iOS 7.0+
Magic	<input type="text"/>	?	
			iOS 7.0+

▶ **Deployment Rules**

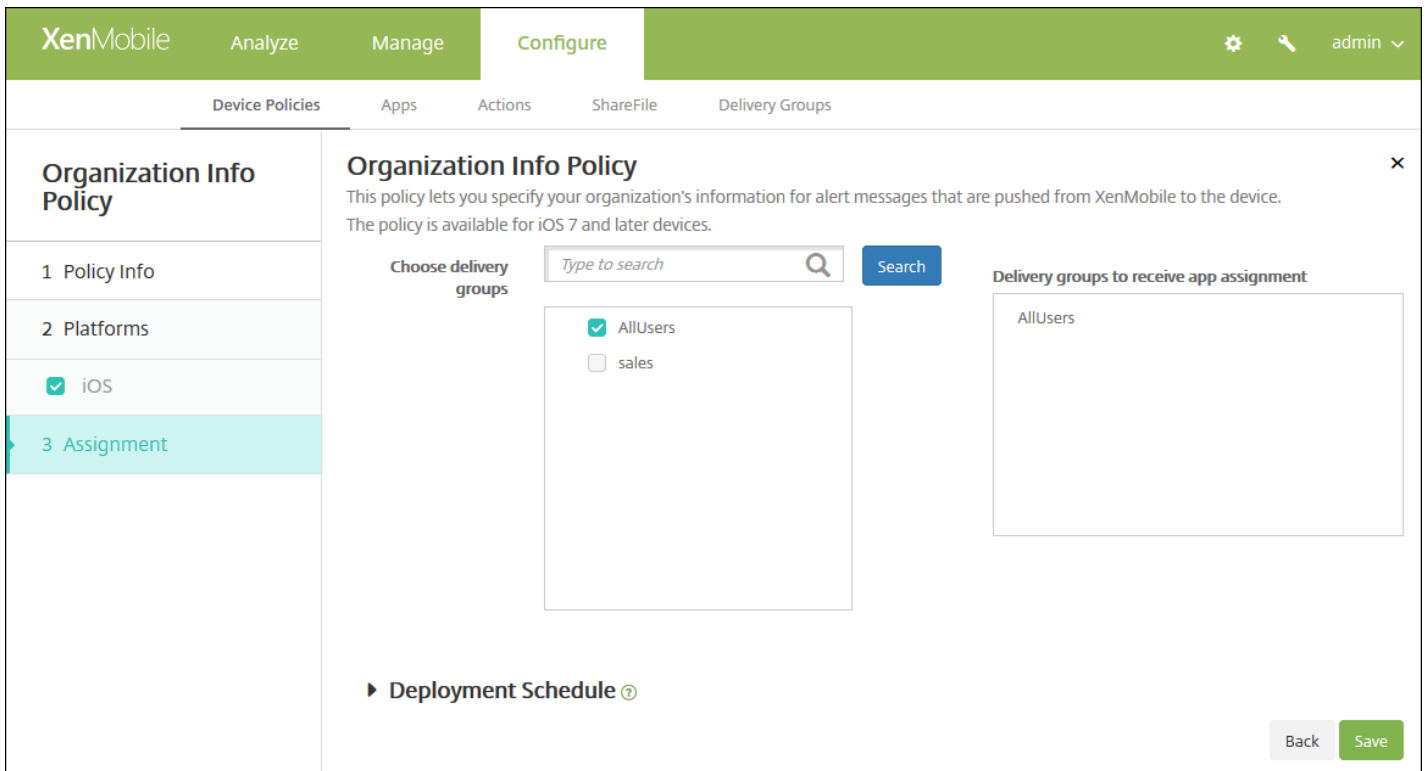
Back Next >

次の設定を構成します。

- **Name** : XenMobileを実行している組織の名前を入力します。
- **Address** : 組織の住所を入力します。
- **Phone** : 組織のサポート電話番号を入力します。
- **Email** : サポートメールアドレスを入力します。
- **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. 展開規則を構成します。

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 **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# パスコードデバイスポリシー

Apr 27, 2017

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、Mac OS X、Android、Samsung KNOX、Android for Work、Windows Phone、およびWindowsデスクトップ/タブレットに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値については、ここで説明しています。

[iOSの設定](#)

[Mac OS Xの設定](#)

[Androidの設定](#)

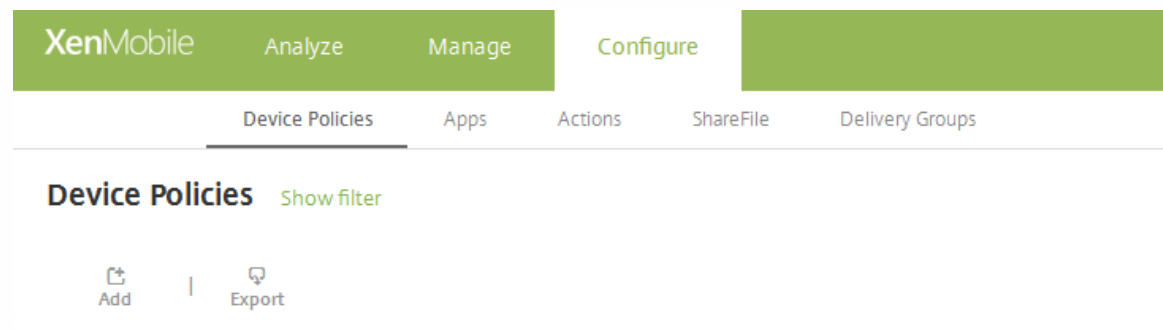
[Samsung KNOXの設定](#)

[Android for Workの設定](#)

[Windows Phoneの設定](#)

[Windowsデスクトップ/タブレットの設定](#)

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



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

3. **[パスコード]** をクリックします。**[Passcode Policy]** 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Passcode Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung KNOX
  - Android for Work
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

#### Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Policy Name\*

Description

Next >

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成



XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Delivery Groups

### Passcode Policy

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung KNOX
- Android for Work
- Windows Phone
- Windows Desktop/Tablet

3 Assignment

### Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

Passcode required

Passcode requirements

Minimum length

Allow simple passcodes

Required characters

Minimum number of symbols

Passcode security

Device lock grace period (minutes of inactivity)

Lock device after (minutes of inactivity)

Passcode expiration in days (1-730)

Previous passcodes saved (0-50)

Maximum failed sign-on attempts

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。デフォルト値は**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。デフォルトは **0** です。
- **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。
  - **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、デバイスはワイプされます。デフォルトは **[Not defined]** です。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。

- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

## Mac OS Xの設定の構成

The screenshot shows the XenMobile configuration page for a Passcode Policy. The left sidebar lists platforms, with 'Mac OS X' selected. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The configuration options are as follows:

- Passcode required:** ON (toggle)
- Passcode requirements:**
  - Minimum length:** 6
  - Allow simple passcodes:** ON
  - Required characters:** OFF
  - Minimum number of symbols:** 0
- Passcode security:**
  - Device lock grace period (minutes of inactivity):** None
  - Lock device after (minutes of inactivity):** None
  - Passcode expiration in days (1-730):** 0
  - Previous passwords saved (0-50):** 0
  - Maximum failed sign-on attempts:** Not defined

次の設定を構成します。

- **パスコードを要求:** このオプションをオンにするとパスコードが必須になり、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。
- [Passcode required] を有効にしない場合は、[Delay after failed sign-on attempts, in minutes] の横で、ユーザーがパスコードを再入力できるようになるまでの待機時間を分単位で入力します。
- [Passcode required] 有効にした場合は、次の設定を構成します。
- **パスコード要件**
  - **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。デフォルトは0です。
- **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。
- **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。
- **Delay after failed sign-on attempts, in minutes** : ユーザーがパスワードを再入力できるようになるまでの待機時間を分単位で入力します。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
  - **[Profile scope]** の横にある、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。

## Androidの設定の構成

The screenshot shows the 'Configure' page for a 'Passcode Policy' in XenMobile. The left sidebar lists 'Policy Info', 'Platforms', and 'Assignment'. Under 'Platforms', 'Android' is selected. The main configuration area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The settings are as follows:

- Passcode Required:** ON (toggle)
- Passcode requirements:**
  - Minimum length: 6
  - Biometric recognition: OFF
  - Required characters: No restriction
  - Advanced rules: OFF (A 3.0+)
- Passcode security:**
  - Lock device after (minutes of inactivity): None
  - Passcode expiration in days (1-730): 0
  - Previous passwords saved (0-50): 0
  - Maximum failed sign-on attempts: Not defined
- Encryption:** (empty field)

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

注：Androidのデフォルト設定は【オフ】です。

- **パスコードを要求** : このオプションをオンにするとパスコードが必須になり、Androidのパスコードデバイスポリシーの構成オプションが表示されます。ページが展開され、パスコード要件、パスコードセキュリティ、暗号化、Samsung SAFEの設定を構成できます。
- **パスコード要件**

- **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、[Require 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]、[numbers and letters]、[Numbers only]、[Letters only] のいずれかを選択して、パスコードの作成方法を構成します。デフォルトは [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]** を有効にした場合、以下のボックスの一覧のそれぞれで、パスコードに含める必要がある文字、記号、または数字の数を、種類ごとに選択します。
  - **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。
  - **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、デバイスはワイプされます。デフォルトは **[Not defined]** です。
- **暗号化**
  - **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。

注：デバイスを暗号化するには、ユーザーはまず充電済みのバッテリーを用意し、暗号化にかかる時間またはそれ以上の時間にわたってデバイスをコンセントに接続したままにする必要があります。暗号化処理を中断すると、デバイス上のデータの一部またはすべてが失われる可能性があります。デバイスを暗号化した後は、出荷時の設定へのリセットを実行してデバイス上のすべてのデータを消去しない限り、元に戻すことはできません。

- **Samsung SAFE**
  - **すべてのユーザーに同じパスコードを使用** : すべてのユーザーに対して同じパスコードを使用するかどうかを選択します。デフォルトは **[OFF]** です。この設定は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。
  - **[Use same passcode across all users]** を有効にした場合は、**[Passcode]** フィールドにすべてのユーザーが使用するパスコードを入力します。
  - **[Passcode required]** を有効にした場合は、次のSamsung SAFEの設定を構成します。
    - **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。デフォルト値は0です。
    - **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。デフォルト値は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。デフォルト値は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。デフォルト値は0です。

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。デフォルトは [ON] です。
- **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。拒否する文字列ごとに [Add] をクリックして、以下の操作を行います。
  - **Forbidden strings** : ユーザーに使用できないようにする文字列を入力します。
  - [Save] をクリックして文字列を追加するか、[Cancel] をクリックして文字列の追加を取り消します。

注：既存の文字列を削除するには、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。

既存の文字列を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

## Samsung KNOXの設定の構成

The screenshot shows the XenMobile Configure interface for the Passcode Policy. The sidebar on the left has sections for '1 Policy Info', '2 Platforms' (with checkboxes for iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, Windows Desktop/Tablet), and '3 Assignment'. The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The settings are organized into sections: 'Passcode requirements' (Minimum length: 6, Allow users to make password visible: OFF), 'Forbidden Strings' (with an 'Add' button), 'Minimum number of' (Changed characters\*, Symbols\*), and 'Maximum number of' (Number of times a character can occur\*, Alphabetic sequence length\*, Numeric sequence length\*). A 'Passcode security' field is at the bottom. Navigation buttons 'Back' and 'Next >' are in the bottom right corner.

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。デフォルト値は6です。
  - **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。拒否する文字列ごとに [Add] をクリックして、以下の操作を行います。
    - **Forbidden strings** : ユーザーに使用できないようにする文字列を入力します。

- **[Save]** をクリックして文字列を追加するか、**[Cancel]** をクリックして文字列の追加を取り消します。

注：既存の文字列を削除するには、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。

既存の文字列を編集するには、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。

- **最小数**

- **Changed characters** : ユーザーが前のパスワードから変更する必要がある文字数を入力します。デフォルト値は**0**です。
- **Symbols** : パスワードに含める必要がある記号の最小数を入力します。デフォルト値は**0**です。

- **最大数**

- **Number of times a character can occur** : パスワード内に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。デフォルト値は**0**です。
- **Alphabetic sequence length** : パスワードに含まれる、連続するアルファベットの最大文字数を入力します。デフォルト値は**0**です。
- **Numeric sequence length** : パスワードに含まれる、連続する数字の最大文字数を入力します。デフォルト値は**0**です。

- **パスワードセキュリティ**

- **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秒数を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは **[None]** です。
- **Passcode expiration in days (1-730)** : パスワ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、パスワ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。
- **サインオンの失敗回数が上限を超えると、デバイスはロックされます**。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。
- **サインオンの失敗回数が上限を超えると、デバイスはワイプされます**。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、KNOXコンテナ（とKNOXデータ）がデバイスからワイプされます。ユーザーは、ワイプが発生した後、KNOXコンテナを再度初期化する必要があります。デフォルトは、 **[Not defined]** です。

## Android for Workの設定の構成

XenMobile Analyze Manage **Configure** ⚙️

Device Policies Apps Actions ShareFile Delivery Groups

### Passcode Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung KNOX
  - Android for Work**
  - Windows Phone
  - Windows Desktop/Tablet
- 3 Assignment

### Policy Information

This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.

**Passcode Required**  ON

**Passcode requirements**

- Minimum length**
- Biometric recognition**  OFF
- Required characters**
- Advanced rules**  OFF A 3.0+

**Passcode security**

- Lock device after (minutes of inactivity)**
- Passcode expiration in days (1-730)**
- Previous passwords saved (0-50)**  ⓘ
- Maximum failed sign-on attempts**  ⓘ

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、Android for Work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、パスコード要件およびパスコードセキュリティ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。デフォルト値は**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。この機能は現在サポートされていません。
  - **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、パスコ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 5.0より前のAndroidデバイスでは使用できません。デフォルトは**[OFF]** です。
  - **[Advanced rules]** を有効にした場合、以下のボックスの一覧のそれぞれで、パスコードに含める必要がある文字、記号、または数字の最小数を、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分数を選択します。この時間が過ぎると、デバイスはロックされます。デフォルトは**[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。
- **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、KNOXコンテナ（とKNOXデータ）がデバイスからワイプされます。ユーザーは、ワイプが発生した後、KNOXコンテナを再度初期化する必要があります。デフォルトは、 **[Not defined]** です。

## Windows Phoneの設定の構成

The screenshot shows the XenMobile configuration interface for a Passcode Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Passcode Policy' and contains a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' The settings are organized into sections: 'Passcode required' (ON), 'Allow simple passcodes' (OFF), 'Passcode requirements' (Minimum length: 6, Characters required: Letters only, Minimum number of symbols: 1), and 'Passcode security' (Lock device after (minutes of inactivity): 0, Passcode expiration in 0-730 days: 0, Previous passwords saved (0-50): 0, Maximum failed sign-on attempts before wipe (0-999): 0). A 'Back' button and a 'Next >' button are located at the bottom right of the configuration area.

次の設定を構成します。

- **パスコードを要求** : Windows Phoneデバイスでパスコードを要求しない場合、このオプションを選択します。デフォルト設定は **[ON]** で、パスコードを要求します。この設定を無効にすると、ページが折りたたまれ、以下のオプションは表示されなくなります。
- **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。デフォルト値は**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。デフォルト値は**1**です。
- **パスコードセキュリティ**
  - **Lock device after (minutes of inactivity)** : デバイスを非アクティブにしておくことができる分数を入力します。この時間が過ぎると、デバイスはロックされます。デフォルト値は**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0~730



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)** : ユーザーが正常なサインオンの前に失敗できる回数を入力します。この回数を超えると、企業データがデバイスからワイプされます。デフォルト値は0です。

## Windowsデスクトップ/タブレットの設定の構成

The screenshot shows the 'Configure' page for a 'Passcode Policy' in XenMobile. The left sidebar lists navigation steps: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, and Windows Desktop/Tablet (which is selected). The main content area is titled 'Passcode Policy' and includes a description: 'This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.' Below this are several settings: 'Disallow convenience logon' (toggle OFF), 'Minimum passcode length' (dropdown 6), 'Maximum passcode attempts before wipe' (dropdown 4), 'Passcode expiration in days (0-730)\*' (input 0), 'Passcode history (1-24)\*' (input 0), and 'Maximum inactivity before device lock in minutes (1-999)' (input 0). A 'Deployment Rules' section is partially visible. At the bottom right, there are 'Back' and 'Next >' buttons.

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。
- **Minimum passcode length** : 一覧から、パスコードの最小文字数を選択します。デフォルト値は6です。
- **Maximum passcode attempts before wipe** : ユーザーが正常なサインオンの前に失敗できる回数を入力します。この回数を超えると、企業データがデバイスからワイプされます。デフォルト値は4です。
- **Passcode expiration in days (0-730)** : 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0~730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。
- **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。デフォルトは0です。
- **Maximum inactivity before device lock in minutes (1-999)** : デバイスを非アクティブにしておくことができる分数を入力します。この時間が過ぎると、デバイスはロックされます。有効な値は1~999です。このフィールドには1~999の数値を入力する必要があります。デフォルト値は0です。

### 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface. At the top, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Configure' tab is active. On the left, a sidebar lists sections: '1 Policy Info', '2 Platforms' (with sub-items for iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone, and Windows Desktop/Tablet), and '3 Assignment'. The main content area is titled 'Passcode Policy' and contains a search bar for 'Choose delivery groups' with a search button. Below the search bar, there are two checkboxes: 'AllUsers' and 'Sales'. At the bottom right, there are 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# 個人用ホットスポットデバイスポリシー

Apr 27, 2017

iOSデバイスの個人用ホットスポット機能を介して携帯データネットワーク接続を使用することにより、ユーザーがWiFiネットワーク圏外にいてもインターネットに接続できるようにすることができます。iOS 7.0以降で利用できます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。
3. **[More]** をクリックした後、**[Network Access]** の下の **[Personal Hotspot]** をクリックします。**[Personal Hotspot Policy]** 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

#### Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Policy Name\*

Description

Next >

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

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

5. **[Next]** をクリックします。**[iOS Platform]** 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Personal Hotspot Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

#### Policy Information

This policy lets you enable or disable a personal hotspot on a device. This policy is available for iOS 7 and later devices.

Disable personal hotspot  OFF  iOS 7.0+

#### Deployment Rules

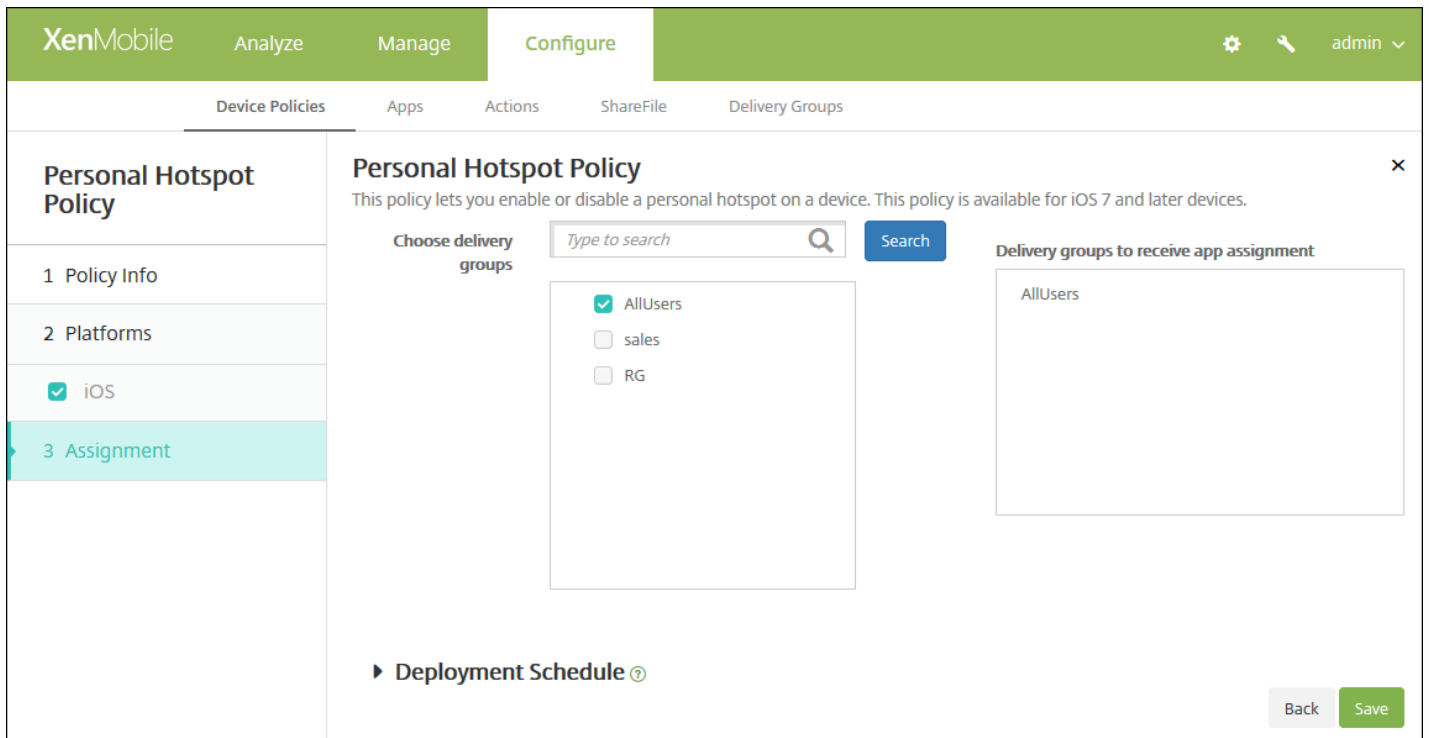
Back Next >

6. 次の設定を構成します。

- **Disable personal hotspot** : ユーザーのデバイスで個人用ホットスポット機能を無効にするかどうかを選択します。デフォルトは **[OFF]** で、ユーザーのデバイスで個人用ホットスポットは無効になっています。このポリシーでは機能は無効になりません。ユーザーは、引き続きデバイスで個人用ホットスポットを使用できますが、ポリシーが展開されると、デフォルトでオンのままにならないように、個人用ホットスポットがオフになります。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Personal Hotspot Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# プロファイル削除デバイスポリシー

Apr 27, 2017

XenMobileで、アプリケーションプロファイル削除デバイスポリシーを作成することができます。ポリシーを展開すると、ユーザーのiOSデバイスまたはMac OS Xデバイスからアプリケーションプロファイルが削除されます。

1. XenMobileコンソールで、 **[Configure]** の **[Device Policies]** をクリックします。 **[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。 **[Add New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開し、 **[Removal]** で **[Profile Removal]** をクリックします。 **[Profile Removal Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Profile Removal Policy' and contains a 'Policy Information' section. This section includes a description and two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is a large text area, also empty. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'iOS' and 'Mac OS X', both of which are checked. At the bottom right of the main content area, there is a green button labeled 'Next >'.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。 **[Platforms]** ページが開きます。
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成

次の設定を構成します。

- **Profile ID** : 一覧から、アプリケーションプロファイルIDを選択します。このフィールドは必須です。
- **Comment** : 任意でコメントを入力します。

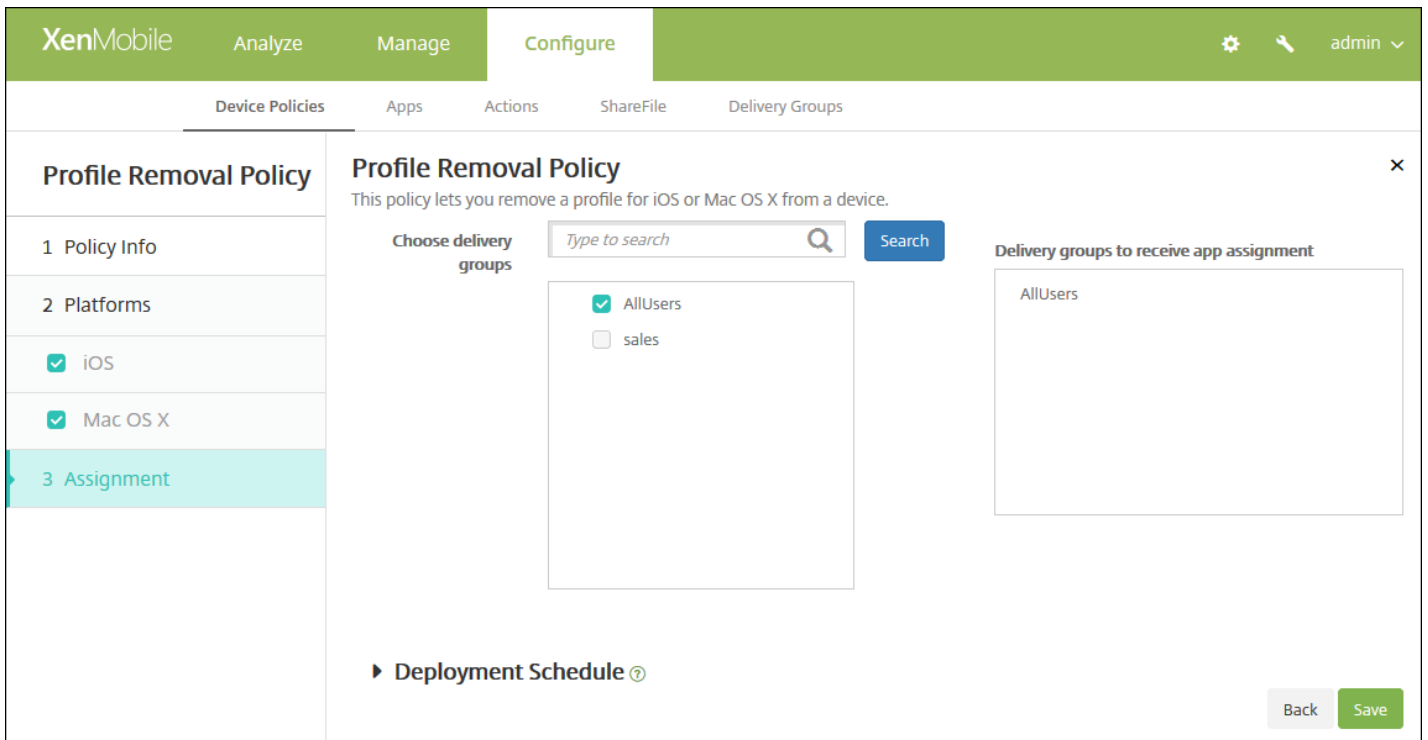
Mac OS Xの設定の構成

次の設定を構成します。

- **Profile ID** : 一覧から、アプリケーションプロファイルIDを選択します。このフィールドは必須です。
- **Deployment scope** : 一覧から、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。
- **Comment** : 任意でコメントを入力します。

#### 7. 展開規則を構成します。

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



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。



# プロビジョニングプロファイルデバイスポリシー

Apr 27, 2017

iOSエンタープライズアプリを開発しコード署名するときは、通常は、iOSデバイスで実行するアプリにAppleが求めるエンタープライズ配布プロビジョニングプロファイルを含めます。プロビジョニングプロファイルが見つからない場合、または期限が切れている場合は、ユーザーがそのアプリをタップして開こうとするとクラッシュします。

プロビジョニングプロファイルの主な問題は、Apple Developer Portalで生成されてから1年で期限が切れるので、ユーザーによって登録されたすべてのiOSデバイス上のすべてのプロビジョニングファイルの期限を追跡する必要があります。期限の追跡では、実際の期限だけでなく、どのユーザーがどのバージョンのアプリを使用しているかも追跡する必要があります。解決策としては、ユーザーにプロビジョニングプロファイルを電子メールで送信する、プロビジョニングプロファイルをWebポータルに置いてダウンロードとインストールを可能にする、という2つの方法があります。これらの解決策は有効ですが、ユーザーに電子メールの指示に従って処理をすることを求めたり、Webポータルにアクセスして適切なプロファイルをダウンロードインストールすることを求めたりするので、エラーが発生する傾向があります。

このプロセスをユーザーが意識しないで済むように、XenMobileではデバイスポリシー付きのプロビジョニングプロファイルをインストールおよび削除できます。紛失した、または期限が切れたプロファイルは必要に応じて削除され、最新のプロファイルがユーザーのデバイスにインストールされるので、タップして開くだけでアプリを使用できます。

プロビジョニングプロファイルポリシーを作成するには、プロビジョニングプロファイルのファイルを作成する必要があります。詳しくは、Apple Developerサイトの[プロビジョニングプロファイルの作成](#)に関するページを参照してください。

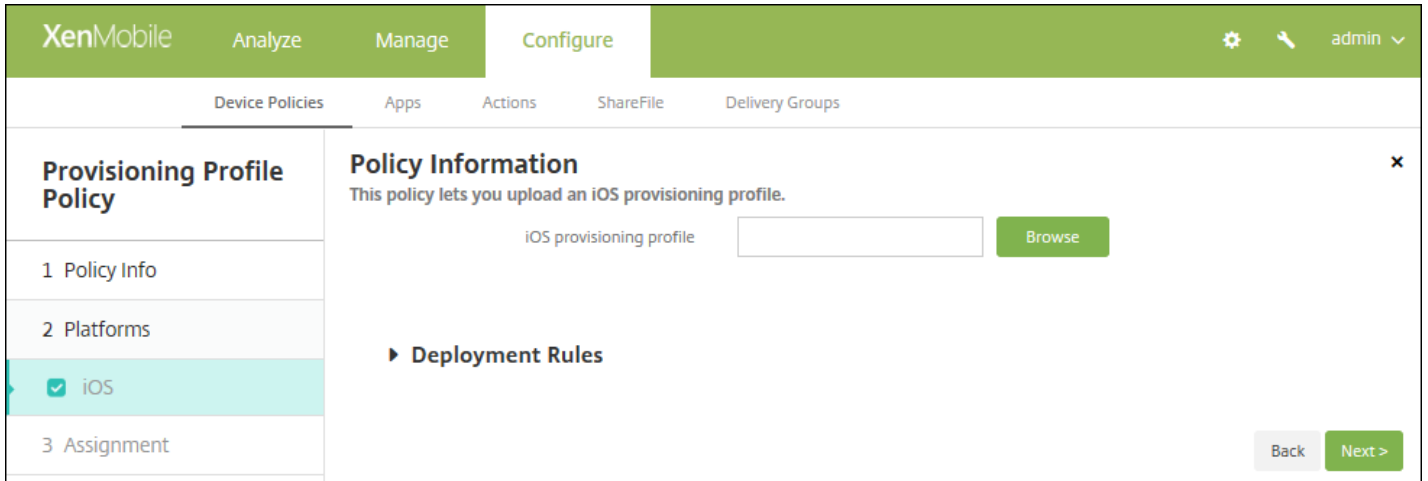
1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。
3. **[More]** を展開し、**[Apps]** の下の **[Provisioning Profile]** をクリックします。**[Provisioning Profile Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs: 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you upload an iOS provisioning profile.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

5. [Next] をクリックします。[iOS Platform] 情報ページが開きます。

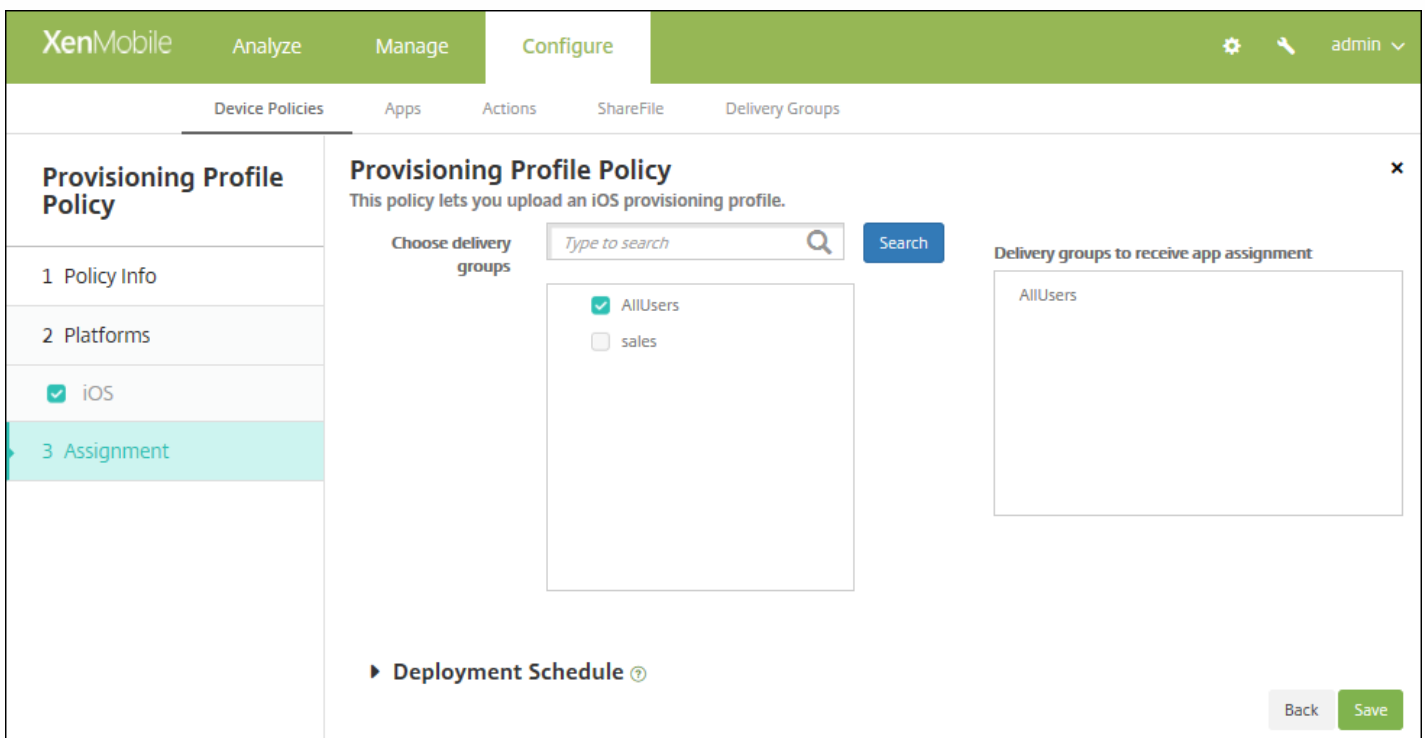


6. 次の設定を構成します。

- **iOS Platform Information** : [Browse] をクリックしてプロビジョニングプロファイルファイルの場所に移動し、そのファイルを選択します。

7. 展開規則を構成します。

8. [Next] をクリックします。[Provisioning Profile Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# プロファイル削除デバイスポリシー

Apr 27, 2017

デバイスポリシーを使用してiOSプロビジョニングプロファイルを削除できます。プロビジョニングプロファイルについては、「[プロビジョニングプロファイルの追加](#)」を参照してください。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ページが開きます。
3. **[More]** を展開し、**[Removal]** で **[Provisioning Profile Removal]** をクリックします。**[Provisioning Profile Removal Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Provisioning Profile Removal Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets remove a provisioning profile from an iOS device.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[iOS Platform]** ページが開きます。

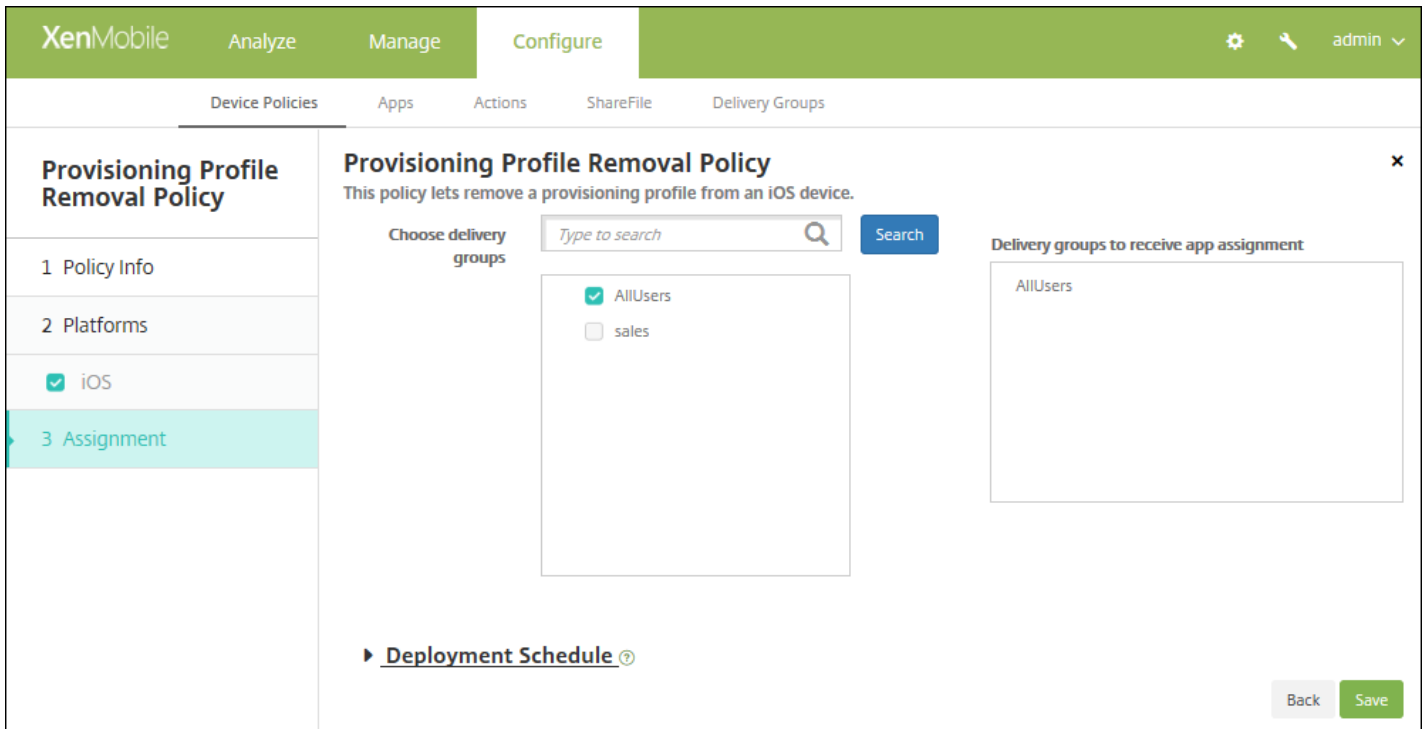
The screenshot shows the XenMobile console interface, continuing from the previous step. The main content area is titled 'Provisioning Profile Removal Policy' and contains a section for 'iOS provisioning profile\*'. This section includes a dropdown menu with the text 'Select an option' and a 'Comment' input field. Below this, there is a section for 'Deployment Rules'. A 'Back' button and a 'Next >' button are located at the bottom right of the form.

6. 次の設定を構成します。

- **iOS プロビジョニング プロファイル**：一覧から削除するプロビジョニングプロファイルを選択します。
- **コメント**：必要に応じてコメントを追加します。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[Provisioning Profile Removal Policy]** 割り当てページが開きます。



9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[オン]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

- このオプションは、 **[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュール

を構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

# プロキシデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、Windows Mobile/CEおよびiOS 6.0以降を実行しているデバイスのグローバルHTTPプロキシ設定を指定できます。グローバルHTTPプロキシポリシーはデバイスごとに1つのみ展開できます。

注：このポリシーを展開する前に、グローバルHTTPプロキシを設定するすべてのiOSデバイスを必ず監視モードに設定してください。詳しくは、「[Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには](#)」を参照してください。

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

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' tab is active, showing a 'Proxy Policy' configuration page. The page has a sidebar on the left with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is selected. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. For iOS, the policy is available for iOS 6. You must also set the iOS device into supervised mode.' Below the description are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name**：ポリシーの説明的な名前を入力します。
  - **Description**：任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

iOSの設定の構成

**Proxy Policy**

1 Policy Info

2 Platforms

iOS

Windows Mobile/CE

3 Assignment

**Policy Information**

This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. For iOS, the policy is available for iOS 6. You must also set the iOS device into supervised mode.

Proxy configuration: Manual

Host name or IP address for the proxy server \*

Port for the proxy server \*

User name

Password

Allow bypassing proxy to access captive networks: OFF

Policy Settings

Remove policy:  Select date,  Duration until removal (in days)

Allow user to remove policy: Always

► Deployment Rules

Back Next >

次の設定を構成します。

- **Proxy configuration** : ユーザーのデバイスでのプロキシの構成方法に関して、一覧から **[Manual]** または **[Automatic]** を選択します。
  - **[手動]** を選択した場合は、次の設定を構成します。
    - **プロキシサーバーのホスト名または IP アドレス**: プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
    - **Port for the proxy server** : プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - **User name** : 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - **Password** : 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - **[Automatic]** を選択した場合は、次の設定を構成します。
    - **Proxy PAC URL** : プロキシ構成を定義するPACファイルのURLを入力します。
    - **PACに到達不能である場合は直接接続を許可**: PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは **[ON]** です。このオプションはiOS 7.0以降でのみ使用できます。
- **キャプティブネットワークへのアクセスのためにプロキシのバイパスを許可**: キャプティブネットワークにアクセスするためにプロキシをバイパスすることを許可するかどうかを選択します。デフォルトは **[OFF]** です。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択しま



す。

- [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。

## Windows Mobile/CEの設定の構成

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Proxy Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. For iOS, the policy is available for iOS 6. You must also set the iOS device into supervised mode.' Below the description are several configuration fields: 'Network' (set to 'Built-in office'), 'Network' (set to 'HTTP'), 'Host name or IP address for the proxy server', 'Port for the proxy server' (set to '80'), 'User name', 'Password', and 'Domain name'. There is also an 'Enable' toggle switch which is currently turned 'ON'. At the bottom right of the main area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Network** : 一覧から、使用するネットワークの種類を選択します。デフォルトは [Built-in office] です。選択できるオプションは以下のとおりです。
  - User-defined office
  - User-defined Internet
  - Built-in office
  - Built-in Internet
- **Network** : 一覧から、使用するネットワーク接続プロトコルを選択します。デフォルトは [HTTP] です。選択できるオプションは以下のとおりです。
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **Hostname or IP address for the proxy server** : プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
- **Port for the proxy server** : プロキシサーバーのポート番号を入力します。このフィールドは必須です。デフォルトは80です。
- **User name** : 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。

- **Password** : 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
- **Domain name** : 任意で、ユーザー名を入力します。
- **Enable** : プロキシを有効にするかどうかを選択します。デフォルトは[オン] です。

### 7. 展開規則を構成します。

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

The screenshot shows the XenMobile Configure interface for a Proxy Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Proxy Policy' and includes a description: 'This policy lets you configure a single, or global, HTTP proxy to be used by all apps that send traffic through HTTP. For iOS, the policy is available for iOS 6. You must also set the iOS device into supervised mode.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search box and a 'Search' button, with 'AllUsers' selected and 'sales' unselected. The 'Delivery groups to receive app assignment' section shows 'AllUsers' in a list. At the bottom, there is a 'Deployment Schedule' section with a dropdown arrow, and 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。 [OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注 :

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

ます。ただしiOSには、**[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

# レジストリデバイスポリシー

Apr 27, 2017

Windows Mobile/CEのレジストリには、アプリケーション、ドライバー、ユーザー設定、および構成設定に関するデータが納められています。XenMobileでは、Windows Mobile/CEデバイスを管理するためのレジストリキーおよび値を定義できます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[Custom]** の下の **[Registry]** をクリックします。**[Registry Policy]** 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Registry Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.

Policy Name\*

Description

Next >

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

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

5. **[Next]** をクリックします。**[Windows Mobile/CE Platform]** ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Registry Policy

- 1 Policy Info
- 2 Platforms
- Windows Mobile/CE
- 3 Assignment

#### Policy Information

This policy allows you to specify which registry keys and values need to be defined on the device. An empty value means that the entry is a registry key.

Registry key path*	Registry value name	Type	Value	Add
--------------------	---------------------	------	-------	-----

Deployment Rules

Back Next >

6. 次の設定を構成します。

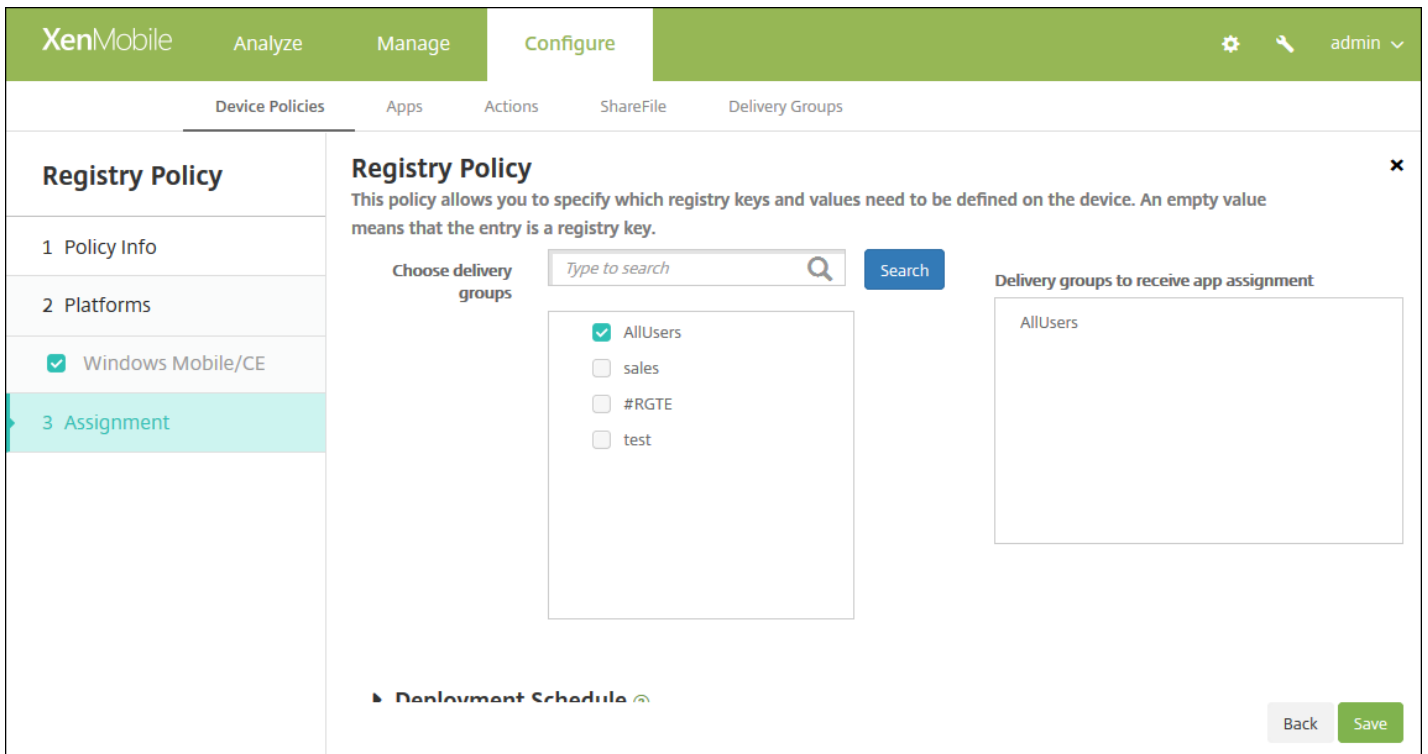
- 追加するレジストリキーまたはレジストリキーと値のペアごとに、[Add] をクリックして以下の操作を行います。
- **Registry key path** : レジストリキーのフルパスを入力します。たとえば、「*HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows*」と入力して、HKEY\_LOCAL\_MACHINEルートキーからWindowsキーまでのルートを指定します。
- **Registry value name** : レジストリキー値の名前を入力します。たとえば、「*ProgramFilesDir*」と入力して、レジストリキーのパスHKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersionに値の名前を追加します。このフィールドを空白のままにすると、レジストリキーと値のペアではなく、レジストリキーを追加することになります。
- **Type** : 一覧から、値のデータの種類を選択します。デフォルトは [DWORD] です。選択できるオプションは以下のとおりです。
  - **DWORD** : 32ビットの未署名の整数
  - **String** : あらゆる文字列
  - **Extended string** : %TEMP%や%USERPROFILE%のような環境変数を含めることができる文字列値
  - **Binary** : あらゆる任意のバイナリデータ
- **Value** : [Registry value name] に関連付ける値を入力します。たとえば、ProgramFilesDirの値を指定するには、「*C:\Program Files*」と入力します。
- レジストリキー情報を保存する場合は [Save] をクリックし、保存しない場合は [Cancel] をクリックします。

注：既存のレジストリキーを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のキーをレジストリ編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

## 7. 展開規則を構成します。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# リモートサポートデバイスポリシー

Apr 27, 2017

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、「[アプリケーショントンネリングデバイスポリシー](#)」を参照してください。
- このトピックの説明に従ってSamsung KNOXのリモートサポートデバイスポリシーを構成します。
- アプリトンネルリモートサポートポリシーと、Samsung KNOXのリモートサポートポリシーの両方をユーザーのデバイスに展開します。

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

2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。

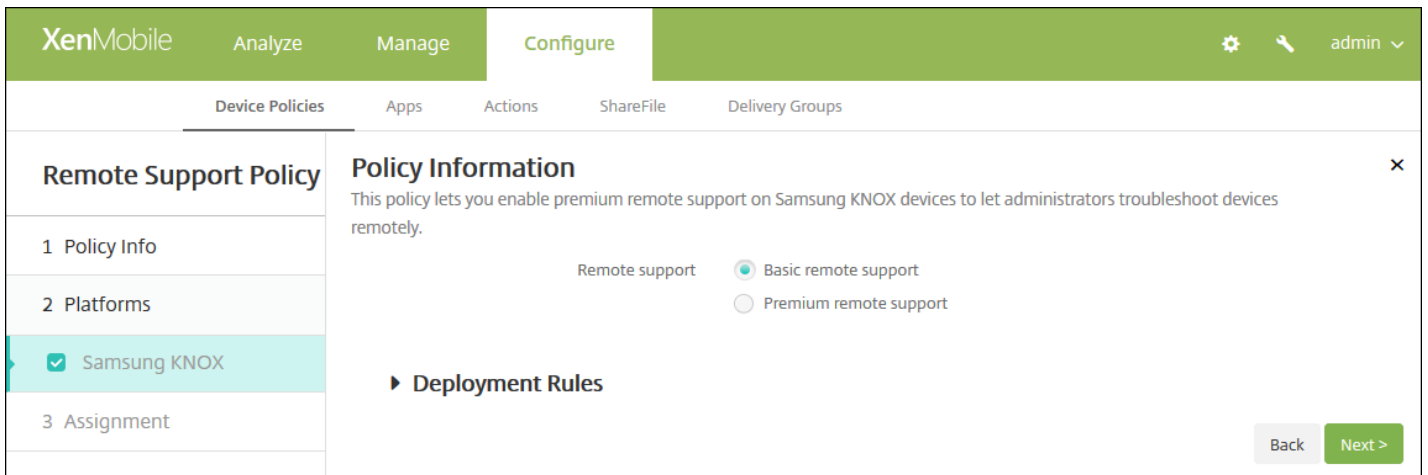
3. **[More]** を展開した後、**[Network access]** の下の **[Remote Support]** をクリックします。**[リモートサポートポリシー]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Remote Support Policy' and contains a 'Policy Information' section. The description reads: 'This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

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

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

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

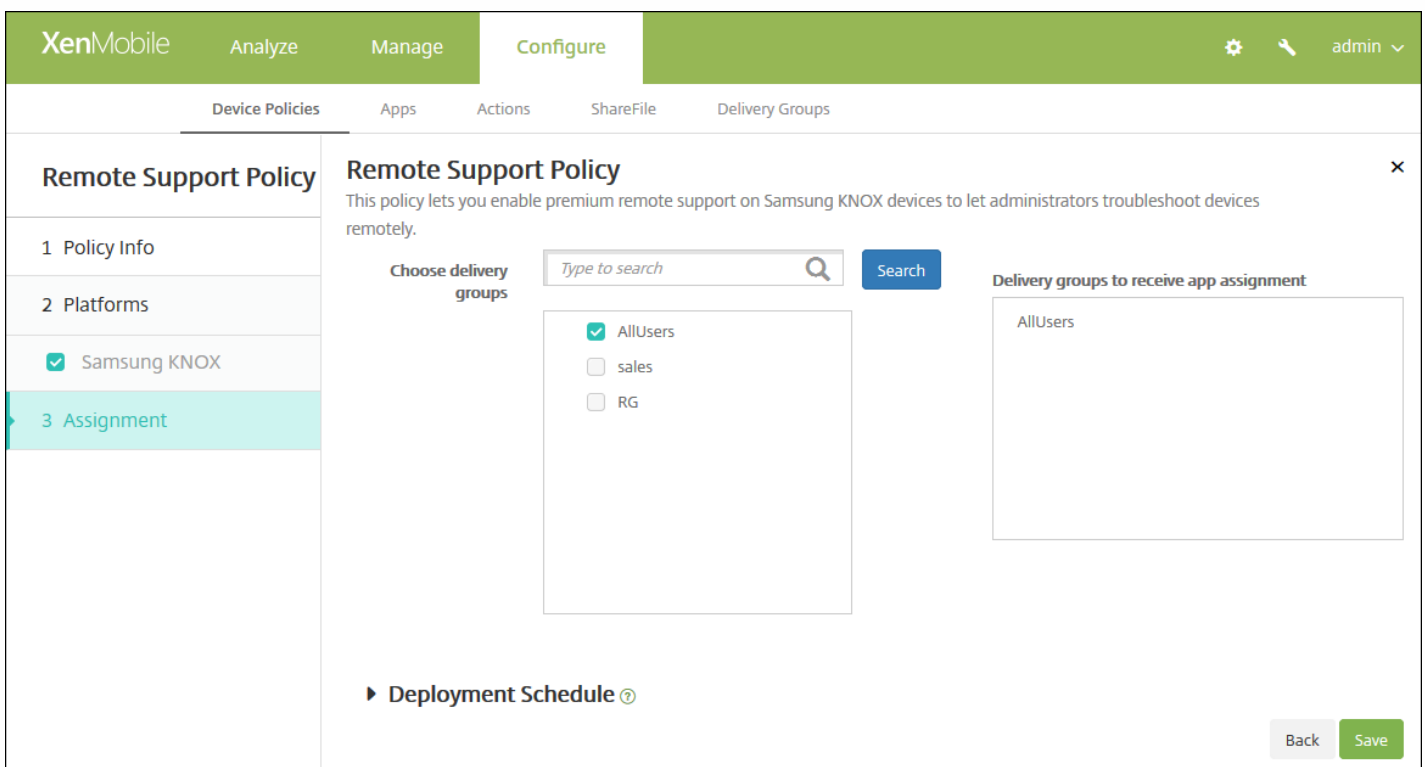


6. 次の設定を構成します。

- **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. 展開規則を構成します。

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 [Delivery groups to receive app assignment] 一覧に表示されます。

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



- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[常時接続に対する展開]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

11. **[Save]** をクリックします。

# 制限デバイスポリシー

Apr 27, 2017

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、MAC OS X、Samsung SAFE、Samsung KNOX、Windowsタブレット、Windows Phone、Amazon、Windows Mobile/CE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。例外は、iOSセキュリティの強制機能とすべてのWindowsタブレット機能です。デフォルトで【OFF】（制限）に設定されています。

ヒント：オプションで【ON】を選択した場合、ユーザーは  
—該当する操作を実行、または該当する機能を使用できます。

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。

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。制限の【Policy information】ページが開きます。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Desktop/Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

Policy Name\*

Description

Next >

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

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

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

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。

**選択するプラットフォーム :**

iOSの場合はこちらを設定を構成します。

Mac OS Xの場合はこちらを設定を構成します。

Samsung SAFEの場合はこちらを設定を構成します。

Samsung KNOXの場合はこちらを設定を構成します。

Windows Phoneの場合はこちらを設定を構成します。

Windows Tabletの場合はこちらを設定を構成します。

Amazonの場合はこちらを設定を構成します。

Windows Mobile/CEの場合はこちらを設定を構成します。

プラットフォームに対する制限の設定が完了した後の、プラットフォームの展開規則の設定方法については、このトピックの後半にある手順7を参照してください。

**[iOS]** を選択した場合は、次の設定を構成します。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Camera
- FaceTime
- Screen shots
- Photo streams  iOS 5.0+
- Shared photo streams  iOS 6.0+
- Voice dialing
- Siri 
  - Allow while device is locked
  - Siri profanity filter
- Installing apps

Back Next >

## iOSの設定

### Mac OS Xの設定の構成

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X**
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Preferences**

- Restrict items in System Preferences  OFF

**Apps**

- Allow use of Game Center  ON OS X 10.11+
- Allow adding Game Center friends  ON
- Allow multiplayer gaming  ON
- Allow Game Center account modification  ON
- Allow App Store adoption  ON
- Allow Safari AutoFill  ON
- Require admin password to install or update apps  OFF

Back Next >

## Mac OS Xの設定

### Samsung SAFEの設定の構成

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Enable ODE Trusted Boot Verification
- Allow Development Mode
- Allow Emergency Calls Only
- Allow Firmware Recovery
- Allow Fast Encryption
- Common Criteria Mode
- Factory reset
- Date Time Change
- DOD boot banner
- Settings changes
- Backup
- Over The Air Upgrade  ⓘ
- Background data
- Camera

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Desktop/Tablet
- Amazon
- Windows Mobile/CE

3 Assignment

Back Next >

## Samsung SAFEの設定

### Samsung KNOXの設定の構成

### Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX**
  - Windows Phone
  - Windows Desktop/Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

**Restrictions Policy**

- Allow use of camera
- Enable Revocation Check
- Move Apps To Container
- Enforce Multifactor Authentication
- Enable TIMA Key store
- Enforce Auth For Container
- Share List
- Enable Audit Log
- Use Secure Keypad
- Enable Google Apps
- Authentication Smart Card Browser

► Deployment Rules

[Back](#) [Next >](#)

## Samsung KNOXの設定

### Windows Phoneの設定の構成

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**WiFi Settings**

- Allow WiFi
- Allow Internet sharing
- Allow auto-connect to WiFi Sense hotspots
- Allow hotspot reporting
- Allow manual configuration

**Connectivity**

- Allow NFC
- Allow bluetooth
- Allow VPN over cellular
- Allow VPN over cellular while roaming

Back Next >

## Windows Phoneの設定

Windowsデスクトップ/タブレットの設定の構成



XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet**
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Network**

Roaming data  OFF

**Security**

User account control  ▾

Enable Windows error reporting  OFF

Enable smart screen  OFF

**Other**

Enterprise client sync product's URL enable  OFF

Enterprise client sync product's URL

▶ **Deployment Rules**

## Windowsデスクトップ/タブレットの設定

### Amazonの設定の構成

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Factory reset
- Profiles

**Allow apps**

- Non-Amazon Appstore apps
- Social networks

**Network**

- Bluetooth
- WiFi switch
- WiFi settings
- Cellular data

Back Next >

## Amazonの設定

### Windows Mobile/CEの設定の構成

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### Restrictions Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

- Bluetooth/infrared beaming (Obex)
- Camera
- WiFi switch
- Bluetooth

### Deployment Rules

Back Next >

## Windows Mobile/CEの設定

### 7. 展開規則を構成します。

8. **[Next]** をクリックすると **[App Uninstall Restrictions Policy]** 割り当てページが開きます。

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

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

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

10. **[Save]** をクリックしてポリシーを保存します。

# ローミングデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、ユーザーのiOSデバイスおよびWindows Mobile/CEデバイスの音声通話ローミングおよびデータローミングを許可するかどうかを構成できます。音声通話ローミングを無効にした場合、データローミングは自動的に無効になります。iOSの場合、このポリシーはiOS 5.0以降のデバイスでのみ使用できます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Network access] の下の [Roaming] をクリックします。[Roaming Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below these are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Roaming Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is active, showing 'Policy Information' with a description: 'This policy lets you limit the device from using voice and data roaming. For iOS, the policy applies to iOS 5 and later devices.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

次の設定を構成します。

- **Disable voice roaming** : 音声通話ローミングを無効にするかどうかを選択します。このオプションを有効にした場合、データローミングは自動的に無効になります。デフォルトは [OFF] で、音声通話ローミングを許可します。
- **Disable data roaming** : データローミングを無効にするかどうかを選択します。このオプションは、音声通話ローミングが有効になっている場合にのみ使用できます。デフォルトは [OFF] で、データローミングを許可します。

次の設定を構成します。

- ローミング中

- **Use on-demand connection only** : ユーザーがデバイスで接続を手動でトリガーする場合、またはモバイルアプリケーションが強制接続を要求する場合のみ (Exchange Serverに相応の設定があらかじめされている場合のプッシュ型のメール要求など)、デバイスはXenMobileに接続します。このオプションにより、デフォルトデバイス接続スケジュールポリシーは一時的に無効化される点に注意してください。
- **Block all cellular connections except the ones managed by XenMobile** : XenMobileアプリケーショントンネルまたはその他のほかのXenMobileデバイス管理タスクで公式に宣言されているデータトラフィックを除き、ほかのデータはデバイスによって送受信されません。たとえば、このオプションではデバイスのWebブラウザを使用したインターネットへの接続がすべて無効化されます。
- **Block all cellular connections managed by XenMobile** : XenMobileトンネルを使用して転送されるすべてのアプリケーションデータ (XenMobile Remote Supportを含む) がブロックされます。ただし、純粋なデバイス管理に関連するデータトラフィックはブロックされません。
- **Block all cellular connections to XenMobile** : この場合、USB、Wi-Fi、またはデフォルトのモバイル事業者のモバイルネットワークを通じてデバイスが再接続されるまで、デバイスとXenMobile間のトラフィックの転送は発生しません。
- **国内ローミング中**
  - **Ignore domestic roaming** : ユーザーが国内でローミングしている間はデータがブロックされません。

## 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface for a Roaming Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Roaming Policy' and includes a description: 'This policy lets you limit the device from using voice and data roaming. For iOS, the policy applies to iOS 5 and later devices.' There are two main sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked) and 'sales' (unchecked). The 'Delivery groups to receive app assignment' section shows a list with 'AllUsers'. At the bottom right, there are 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、その他のオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。

- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# Samsung MDMライセンスキーデバイスポリシー

Apr 27, 2017

XenMobileはSamsung for Enterprise (SAFE) およびSamsung KNOXポリシーの両方をサポートし、拡張しています。SAFEは、モバイルデバイス管理 (MDM : Mobile Device Management) ソリューションとの統合を通じてビジネス向けのセキュリティおよび機能拡張を提供するソリューションファミリーです。Samsung KNOXは、企業向けにより高いセキュリティで保護されたAndroidプラットフォームを提供する、SAFEプログラム内のソリューションです。

SAFEのポリシーおよび制限を展開する前に、組み込みのSamsung Enterprise License Management (ELM) キーをデバイスに展開することによってSAFE APIを有効にする必要があります。また、Samsung KNOX APIを有効にするには、Samsung ELMキーの展開に加え、Samsung KNOX License Management System (KLMS) を使用してSamsung KNOXワークスペースライセンスを購入する必要があります。Samsung KLMSはモバイルデバイス管理 (MDM : Mobile Device Management) ソリューションに有効なライセンスをプロビジョニングし、モバイルデバイスでSamsung KNOX APIをアクティブ化できるようにします。これらのライセンスはSamsungから取得する必要があり、Citrixからは提供されません。

Secure HubをSamsung ELMキーと共に展開し、SAFEおよびSamsung KNOX APIを有効にする必要があります。SAFE APIが有効になっていることは、デバイスプロパティをチェックすることで確認できます。Samsung ELMキーが展開されると、[Samsung MDM API available] 設定がTrueに設定されます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Security] の下の [Samsung MDM License Key] をクリックします。[Samsung MDM License Key Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area displays the 'Samsung MDM License Key Policy' configuration page. The page title is 'Policy Information' and it includes a description: 'This policy lets you generate a Samsung ELM license key.' There are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is a large text area, also empty. On the left side, there is a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checked checkboxes: 'Samsung SAFE' and 'Samsung KNOX'. At the bottom right, there is a green 'Next >' button.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Platforms] ページが開きます。

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile Configure interface for the 'Samsung MDM License Key Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung SAFE' and 'Samsung KNOX' are both checked. The main area is titled 'Policy Information' and contains a text description: 'This policy lets you generate a Samsung ELM license key.' Below this is a text input field labeled 'ELM license key\*' with the value '\$\${elm.license.key}'. There is also a 'Deployment Rules' section with a right-pointing arrow. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- ELM License key : このフィールドには、既にELMライセンスキーを生成するマクロが入力されています。このフィールドが空白の場合は、「`$$${elm.license.key}`」というマクロを入力します。

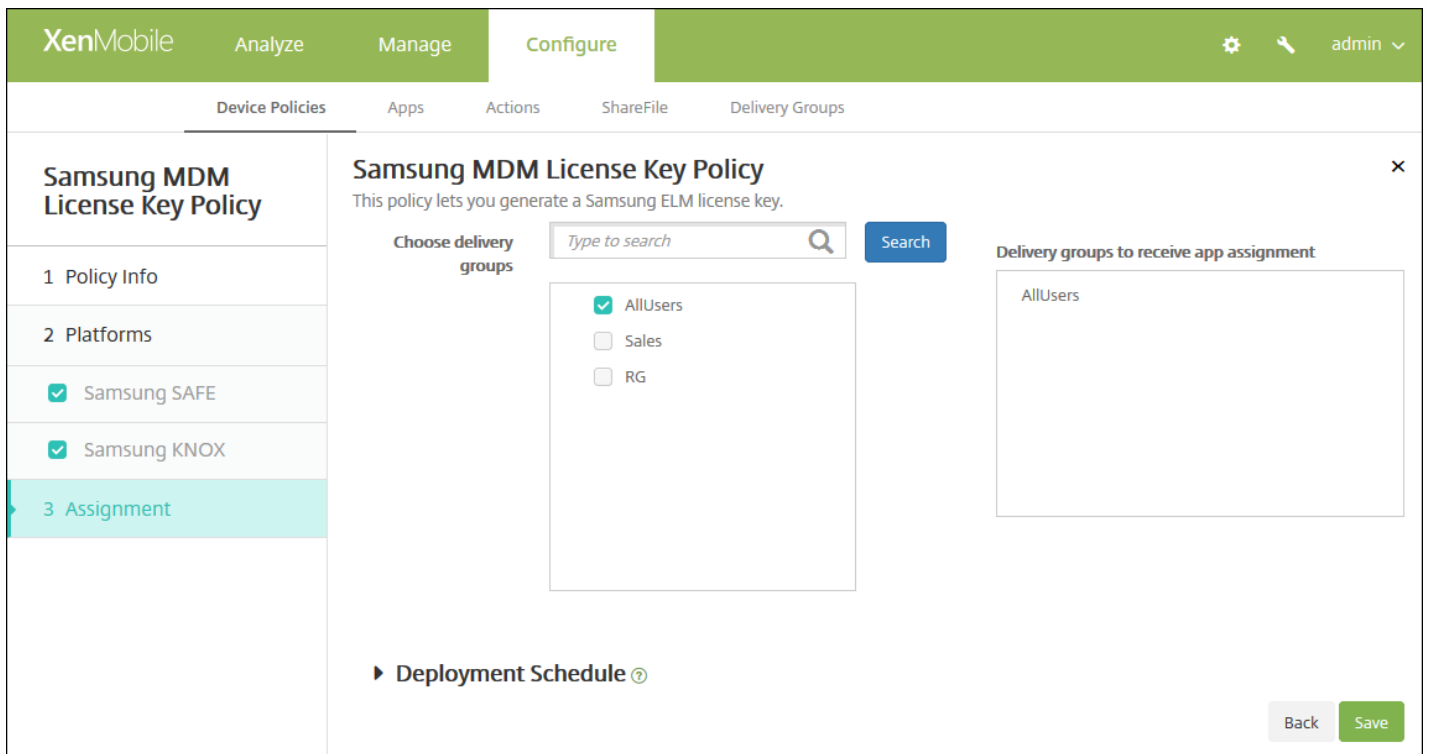
The screenshot shows the XenMobile Configure interface for the 'Samsung MDM License Key Policy'. The left sidebar has sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Samsung KNOX' is checked. The main area is titled 'Policy Information' and contains a text description: 'This policy lets you generate a Samsung ELM license key.' Below this is a text input field labeled 'KNOX license key\*' which is currently empty. To the right of the field is a help icon (question mark in a circle). There is also a 'Deployment Rules' section with a right-pointing arrow. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- KNOX License key : Samsungから取得したKNOXライセンスキーを入力します。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Samsung MDM License 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] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

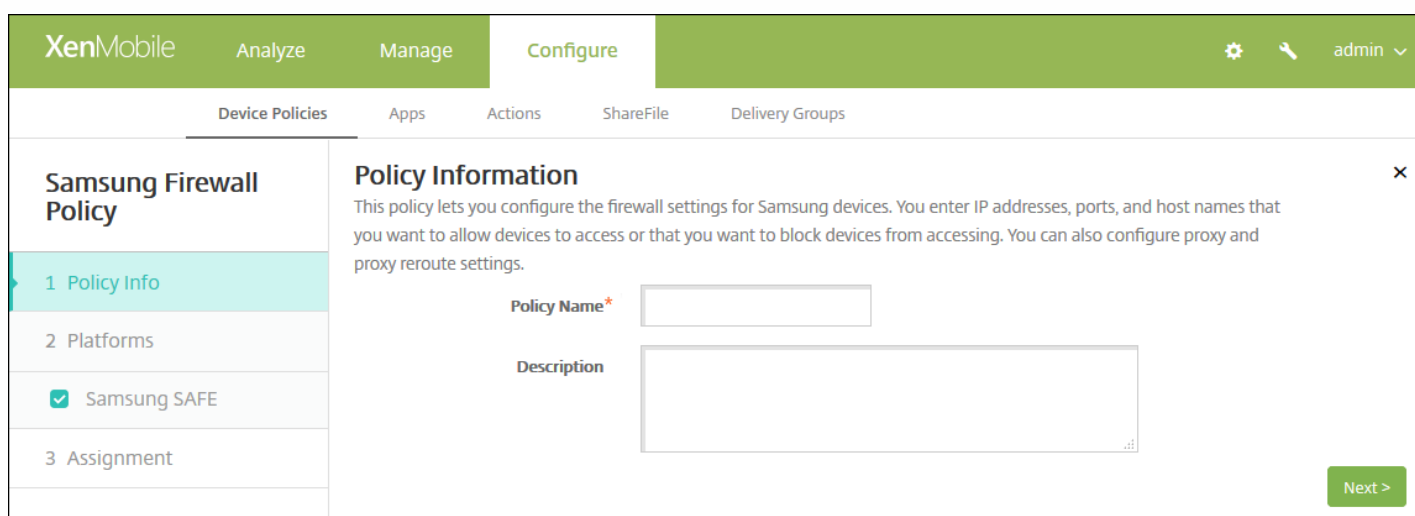
11. [Save] をクリックします。

# Samsung SAFEのファイアウォールデバイスポリシー

Apr 27, 2017

このポリシーにより、Samsungデバイスのファイアウォール設定を構成できます。デバイスにアクセスを許可するIPアドレス、ポート、ホスト名、またはデバイスのアクセスをブロックするIPアドレス、ポート、ホスト名を入力します。プロキシおよびプロキシ再ルーティングの設定を構成することもできます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Network access] の下の [Samsung Firewall] をクリックします。[Samsung ファイアウォールポリシー] ページが開きます。



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Samsung Firewall Policy' and is divided into a left sidebar and a main 'Policy Information' section. The sidebar has three items: '1 Policy Info' (selected), '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a description: 'This policy lets you configure the firewall settings for Samsung devices. You enter IP addresses, ports, and host names that you want to allow devices to access or that you want to block devices from accessing. You can also configure proxy and proxy reroute settings.' Below the description are two input fields: 'Policy Name\*' (with an asterisk indicating it is required) and 'Description'. A green 'Next >' button is located at the bottom right of the form.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Samsung SAFE] プラットフォーム情報ページが開きます。

The screenshot shows the XenMobile configuration interface for a Samsung Firewall Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', 'Configure', and 'admin'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view with 'Samsung Firewall Policy' expanded, and 'Samsung SAFE' selected under 'Device Policies'. The main content area is titled 'Policy Information' and contains the following sections:

- Allow/Deny hosts:** A table with columns 'Host name/IP range\*', 'Port/port range\*', and 'Allow/deny rule filter', followed by an 'Add' button.
- Reroute configuration:** A table with columns 'Host name/IP address/IP range\*', 'Port/port range\*', 'Proxy IP\*', and 'Proxy Port\*', followed by an 'Add' button.
- Proxy Configuration:** Two input fields labeled 'Proxy IP' and 'Port'.
- Deployment Rules:** A section header with a right-pointing arrow.

At the bottom right of the main content area, there are 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- ホストを許可/禁止

- アクセスを許可または拒否するホストごとに、[Add] をクリックして以下の操作を行います。
  - Host name/IP range : ポリシーを適用するサイトのホスト名またはIPアドレスの範囲を入力します。
  - Port/port range : ポートまたはポートの範囲を入力します。
  - Allow/deny rule filter : サイトへのアクセスを許可する場合は [ホワイトリスト] を選択し、サイトへのアクセスを拒否する場合は [ブラックリスト] を選択します。
  - [Save] または [Cancel] をクリックします。

- 経路変更構成

- 構成するプロキシごとに、[Add] をクリックして以下の操作を行います。
  - Host name/IP range : プロキシ再ルーティングのホスト名またはIPアドレスの範囲を入力します。
  - Port/port range : ポートまたはポートの範囲を入力します。
  - Proxy IP : プロキシIPアドレスを入力します。
  - Proxy port : プロキシのポート番号を入力します。
  - [Save] または [Cancel] をクリックします。

注：既存のアイテムを削除するには、その項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存の項目を編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

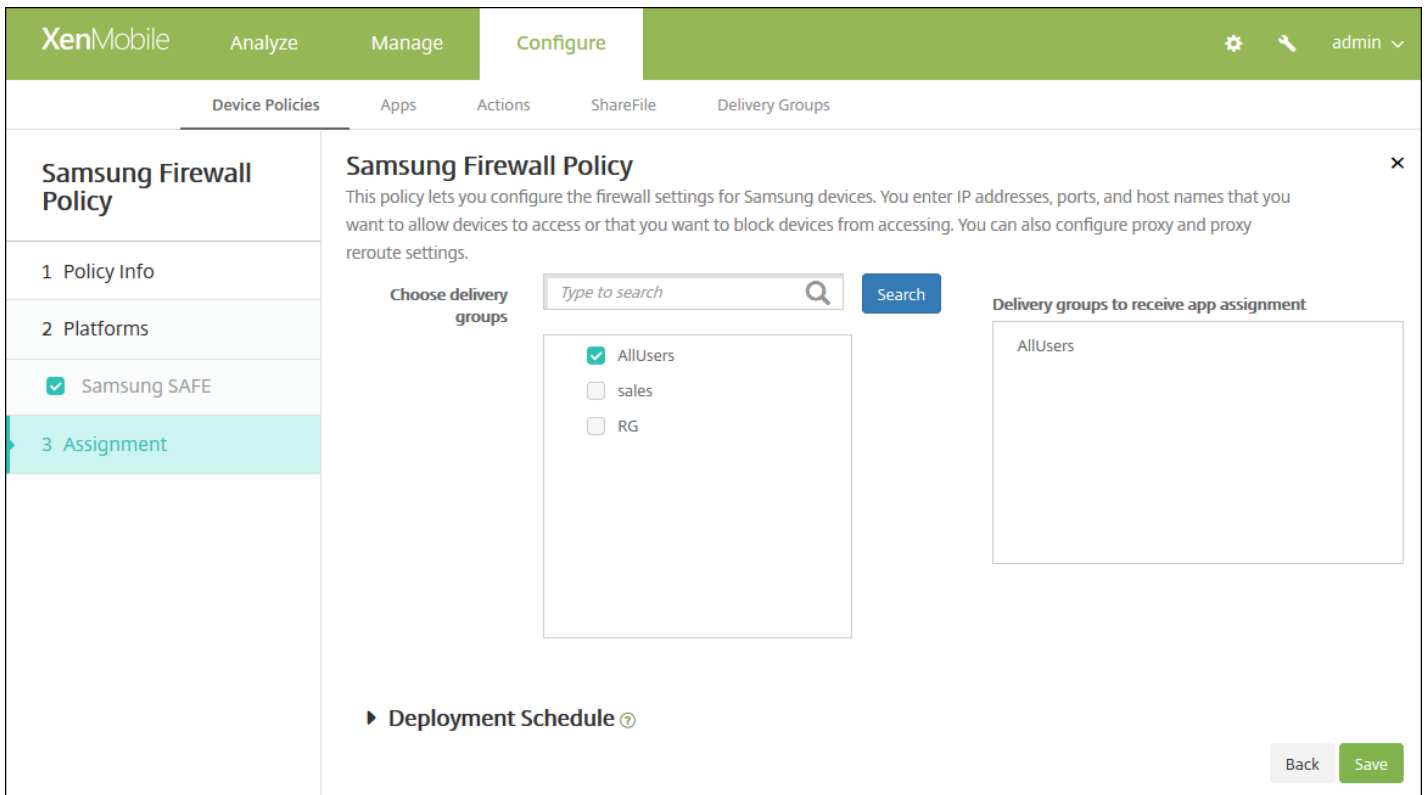
- ポート構成

- Proxy IP : プロキシサーバーのIPアドレスを入力します。

- Port : プロキシサーバーのポート番号を入力します。

## 7. 展開規則を構成します。

8. [Next] をクリックします。 [Samsung Firewall Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

### 注 :

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

11. [Save] をクリックします。

# SCEPデバイスポリシー

Apr 27, 2017

このポリシーでiOSデバイスとMac OS Xデバイスを構成し、SCEP (Simple Certificate Enrollment Protocol) を使用して外部SCEPサーバーから証明書を取得することができます。XenMobileに接続されているPKIからSCEPを使用してデバイスに証明書を配布する場合は、PKIエンティティとPKIプロバイダーを分散モードで作成する必要があります。詳しくは、「[PKIエンティティ](#)」を参照してください。

## iOSの設定

## Mac OS Xの設定

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[Security]** の下の **[SCEP]** をクリックします。**[SCEP Policy]** 情報ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this is a sub-navigation bar with 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SCEP Policy' and has a left-hand navigation menu with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Info' section is active. The main content area is titled 'Policy Information' and contains the following text: 'This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.' Below this text are two form fields: 'Policy Name\*' (a text input field) and 'Description' (a large text area). The 'Policy Name\*' field is empty. The 'Description' field is also empty. Below the form fields, there is a section for 'Platforms' with two options: 'iOS' and 'Mac OS X', both of which are checked with a green checkmark.

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。



XenMobile
Analyze
Manage
Configure
⚙️ 🔍 admin ▾

Device Policies
Apps
Actions
ShareFile
Delivery Groups

### SCEP Policy

1 Policy Info

2 Platforms

iOS

Mac OS X

Windows Phone

Windows Tablet

3 Assignment

### Policy Information ✕

This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

URL base\*

Instance name\*

Subject X.500 name (RFC 2253)

Subject alternative names type None ▾

Maximum retries

Retry delay

Challenge password

Key size (bits) 1024 ▾

Use as digital signature OFF

Use for key encipherment OFF

SHA1/MD5 fingerprint (hexadecimal string)

**Policy Settings**

Remove policy  Select date  Duration until removal (in days)

📅

Allow user to remove policy Always ▾

▶ **Deployment Rules**

Back
Next >

次の設定を構成します。

- **URL base** : HTTPまたはHTTPSを介したSCEP要求の送信先を定義するSCEPサーバーのアドレスを入力します。秘密キーに証明書署名要求 (Certificate Signing Request : CSR) と一緒に送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するためにHTTPSを使用してください。これは必須の手順です。
- **Instance name** : SCEPサーバーで認識される文字列を入力します。たとえば、example.orgのようなドメイン名です。CAに複数のCA証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。
- **Subject X.500 name (RFC 2253)** : オブジェクト識別子 (OID) と値の配列として示されるX.500の名前の表現を入力しま

す。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[["C","US"],["O","Apple Inc."],...,[["1.2.5.3","bar"]]]」のように解釈されます。OIDはドット付き数値として表すことができ、略語は国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) を表しています。

- **[Subject alternative names type]** : 一覧から、代替名の種類を選択します。SCEPポリシーは、CAが証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。[None]、[RFC 822 name]、[DNS name]、[URI] のいずれかを指定できます。
- **Maximum retries** : SCEPサーバーがPENDING応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは、3です。
- **Retry delay** : 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは10です。
- **Challenge password** : 事前共有シークレットを入力します。
- **[Key size (bits)]** : 一覧から、1024または2048のいずれかのキーサイズ (ビット) を選択します。デフォルトは1024です。
- **Use as digital signature** : デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合 (証明書がCAによって発行されたかどうかを確認する場合など)、公開キーを使ってハッシュを復号化する前に、SCEPサーバーではデジタル署名に証明書を使用できるかどうかを確認されます。
- **Use for key encipherment** : キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかを最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5 fingerprint (hexadecimal string)** : CAでHTTPが使われている場合、このフィールドを使って、CA証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CAの応答の信頼性を確認するためにデバイスで使われます。SHA1またはMD5のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。
- **ポリシー設定**
  - **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。

XenMobile
Analyze
Manage
Configure
⚙️ 🔍 admin ▾

Device Policies
Apps
Actions
ShareFile
Delivery Groups

### SCEP Policy

1 Policy Info

2 Platforms

iOS

Mac OS X

Windows Phone

Windows Tablet

3 Assignment

### Policy Information ✕

This policy lets you create a Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

URL base\*

Instance name\*

Subject X.500 name (RFC 2253)

Subject alternative names type None ▾

Maximum retries

Retry delay

Challenge password

Key size (bits) 1024 ▾

Use as digital signature OFF

Use for key encipherment OFF

SHA1/MD5 fingerprint (hexadecimal string)

Certificate expiration notification threshold

**Policy Settings**

Remove policy 
 Select date  
 Duration until removal (in days)

📅

Allow user to remove policy Always ▾

Profile scope User ▾ OS X 10.7+

**▶ Deployment Rules**

Back
Next >

次の設定を構成します。

- **URL base** : HTTPまたはHTTPSを介したSCEP要求の送信先を定義するSCEPサーバーのアドレスを入力します。秘密キーに証明書署名要求 (Certificate Signing Request : CSR) と一緒に送信されないため、暗号化されていない状態で要求を送信しても安全な場合があります。ただし、ワンタイムパスワードの再利用が許可されている場合は、パスワードを保護するためにHTTPSを使用してください。これは必須の手順です。
- **Instance name** : SCEPサーバーで認識される文字列を入力します。たとえば、example.orgのようなドメイン名です。CAに複数のCA証明書がある場合、このフィールドを使用して必要なドメインを区別できます。これは必須の手順です。

- **Subject X.500 name (RFC 2253)** : オブジェクト識別子 (OID) と値の配列として示されるX.500の名前の表現を入力します。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」の場合は、「[[["C", "US"], [{"O", "Apple Inc."}], ..., [{"1.2.5.3", "bar"}]]」のように解釈されます。OIDはドット付き数値として表すことができ、略語は国 (C)、地域 (L)、州 (ST)、組織 (O)、組織単位 (OU)、共通名 (CN) を表しています。
- **[Subject alternative names type]** : 一覧から、代替名の種類を選択します。SCEPポリシーは、CAが証明書を発行するために必要な値を提供する、オプションの代替名の種類を指定できます。[None]、[RFC 822 name]、[DNS name]、[URI] のいずれかを指定できます。
- **Maximum retries** : SCEPサーバーがPENDING応答を送信した場合にデバイスが再試行する回数を入力します。デフォルトは、3です。
- **Retry delay** : 次の再試行までの待機時間を秒数で入力します。最初の再試行は直ちに試行されます。デフォルトは10です。
- **Challenge password** : 事前共有シークレットを入力します。
- **[Key size (bits)]** : 一覧から、1024または2048のいずれかのキーサイズ (ビット) を選択します。デフォルトは1024です。
- **Use as digital signature** : デジタル署名に証明書を使用するかどうかを指定できます。別のユーザーがデジタル署名を確認するために証明書を使用している場合 (証明書がCAによって発行されたかどうかを確認する場合など)、公開キーを使ってハッシュを復号化する前に、SCEPサーバーではデジタル署名に証明書を使用できるかどうかを確認されます。
- **Use for key encipherment** : キーの暗号化に証明書を使用するかどうかを指定します。サーバーで、クライアントが提供する証明書の公開キーを使用して、データが秘密キーを使って暗号化されているかを確認している場合、キーの暗号化に証明書を使用できるかどうかを最初に確認されます。できない場合は、操作に失敗します。
- **SHA1/MD5 fingerprint (hexadecimal string)** : CAでHTTPが使われている場合、このフィールドを使って、CA証明書のフィンガープリントを提供します。このフィンガープリントは、登録時、CAの応答の信頼性を確認するためにデバイスで使われます。SHA1またはMD5のフィンガープリントを入力することも、署名をインポートする証明書を選択することもできます。
- **ポリシー設定**
  - **[Policy Settings]** の下の **[Remove policy]** の横にある、**[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。
  - **[Profile scope]** の横にある、**[User]** または **[System]** を選択します。デフォルトは **[User]** です。このオプションはOS X 10.7以降でのみ使用できます。

## 7. 展開規則を構成します。

8. **[Next]** をクリックします。[SCEP Policy] 割り当てページが開きます。
9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の **[Delivery groups to receive app assignment]** の一覧に表示されます。
10. **[Deployment Schedule]** を展開して以下の設定を構成します。
  - **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
  - **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
  - **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。

- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックしてポリシーを保存します。

# サイドローディングキーデバイスポリシー

Apr 27, 2017

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] を展開した後、[Apps] の下の [Sideload Key] をクリックします。[Sideload Key Policy] ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Sideload Key Policy' configuration page is displayed, featuring a sidebar with '1 Policy Info', '2 Platforms', and '3 Assignment'. The 'Policy Information' section contains a 'Policy Name\*' text input field and a 'Description' text area. A 'Next >' button is located at the bottom right of the form.

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

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

5. [Next] をクリックします。[Windows Tablet Platform] 情報ページが開きます。

**Sideload Key Policy**

1 Policy Info

2 Platforms

Windows Tablet

3 Assignment

**Policy Information**

This policy lets you configure the product key for sideloading apps on Windows 8.1 devices.

Sideload key\*

Key activations\*

License usage

► Deployment Rules

Back Next >

6. 次の設定を構成します。

- **Sideload 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。
- **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。
- **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. 展開規則を構成します。

8. [Next] をクリックします。[Sideload Key Policy] 割り当てページが開きます。

**Sideload Key Policy**

1 Policy Info

2 Platforms

Windows Tablet

**3 Assignment**

**Sideload Key Policy**

This policy lets you configure the product key for sideloading apps on Windows 8.1 devices.

Choose delivery groups

AllUsers

sales

RG

ag186

Delivery groups to receive app assignment

AllUsers

► Deployment Schedule ⓘ

Back Save

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを

選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [オン] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[接続するたび] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# 署名証明書デバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、APPXファイルへの署名に使用される署名証明書を構成することができます。署名証明書は、ユーザーにAPPXファイルを配布して、ユーザーがWindowsタブレットにアプリケーションをインストールできるようにする場合に必要です。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Apps] の下の [Signing Certificate] をクリックします。[Signing Certificate Policy] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: Analyze, Manage, and Configure. The 'Configure' tab is active. Below the navigation, there are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar for the 'Signing Certificate Policy' with three sections: '1 Policy Info' (highlighted), '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Windows Tablet' is selected with a checkmark. The main content area is titled 'Policy Information' and contains a description: 'This policy lets you add the signing certificate that was used to sign an APPX file compatible with Windows 8.1 and later.' There are two input fields: 'Policy Name\*' (required) and 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 必要に応じて、ポリシーの説明を入力します。
5. [Next] をクリックします。[Windows Tablet Platform] ページが開きます。

6. 次の設定を構成します。

- **Signing certificate** : [Browse] をクリックしてAPPXファイルへの署名に使用する証明書ファイルの場所へ移動し、ファイルを選択します。
- **Password** : 署名証明書へのアクセスに必要なパスワードを入力します。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Signing Certificate Policy] 割り当てページが開きます。

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

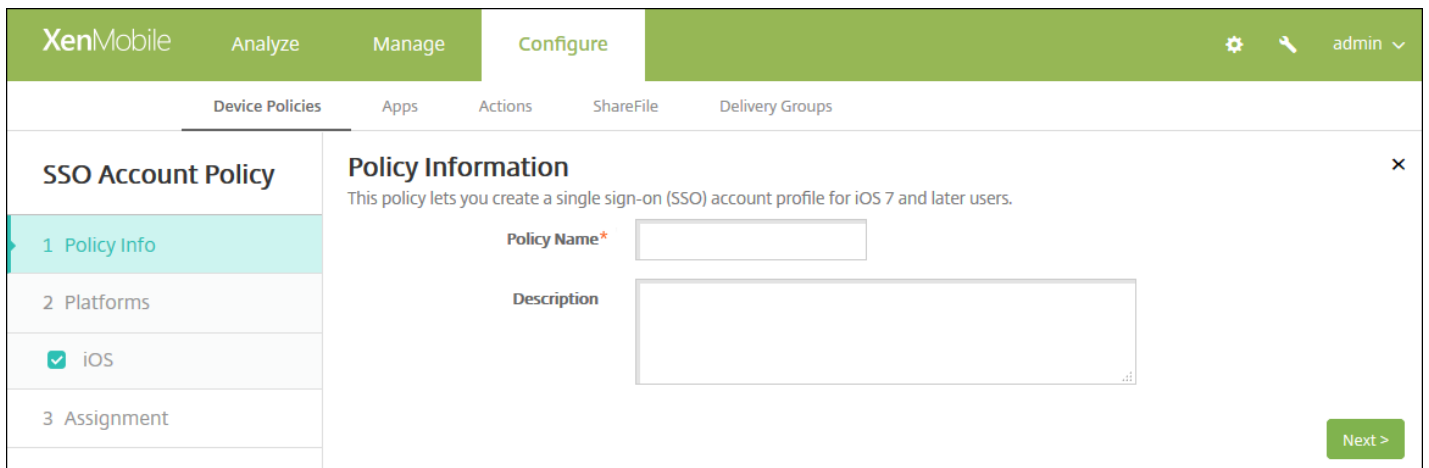
# シングルサインオンアカウントデバイスポリシー

Apr 27, 2017

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. [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。



The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SSO Account Policy' and contains a 'Policy Information' section. This section includes a description: 'This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located at the bottom right of the form.

4. [SSO Account Policy] 情報ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[iOS Platform] 情報ページが開きます。

**XenMobile** Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

**SSO Account Policy**

1 Policy Info

2 Platforms

iOS

3 Assignment

**Policy Information** ×

This policy lets you create a single sign-on (SSO) account profile for iOS 7 and later users.

Account name\*

Kerberos principal name\*

Identity credential (Keystore or PKI credential) None

Kerberos realm\*

Permitted URLs

Permitted URL  Add

App Identifiers

App Identifier  Add

Policy Settings

Remove policy  Select date  Duration until removal (in days)

📅

Allow user to remove policy Always

► **Deployment Rules**

Back Next >

## 6. 次の設定を構成します。

- **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。
- **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。
- **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。
- **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。
- **Permitted URLs** : シングルサインオンを要求するURLごとに、**[Add]** をクリックして以下の操作を行います。
  - **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デバイスでは、前のKerberosログオンでデバイスにキャッシュされた可能性があるKerberosトークンを提供したSSOは試行されません。URL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。
    - **[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。
- **App Identifiers** : このログインを許可するアプリケーションごとに、**[Add]** をクリックして以下の操作を行います。

- **App Identifier** : 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。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。
- **[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。

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。

- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、**[Always]**、**[Password required]**、**[Never]** のいずれかを選択します。
  - **[Password required]** を選択した場合、**[Removal password]** の横に必要なパスワードを入力します。

## 7. 展開規則を構成します。

8. **[Next]** をクリックします。**[SSO Account Policy]** 割り当てページが開きます。

The screenshot shows the XenMobile configuration interface for an SSO Account Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'SSO Account Policy' and includes a sidebar with '3 Assignment' selected. The main content area is titled 'SSO Account Policy' and includes a 'Choose delivery groups' section with a search box and a list of groups: 'AllUsers' (checked) and 'sales' (unchecked). There is also a 'Delivery groups to receive app assignment' section showing 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section and 'Back' and 'Save' buttons.

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

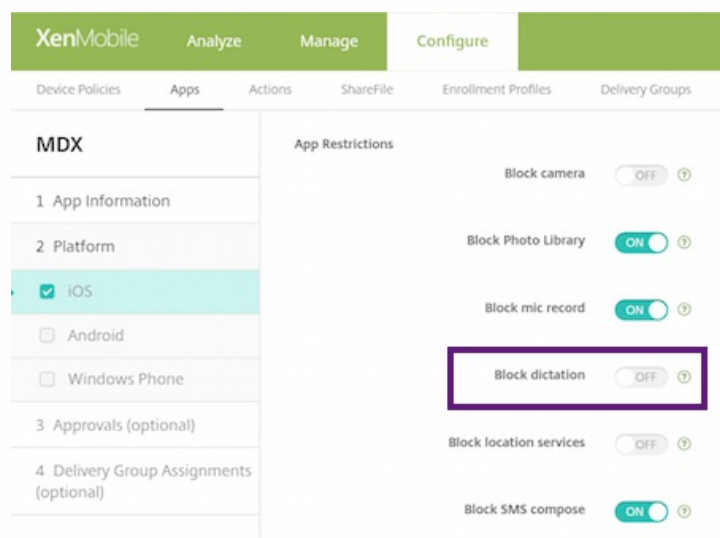
# Siriとディクテーションのポリシー

Apr 27, 2017

管理されたiOSデバイス上でユーザーがSiriに何かを求めると、テキストを口述する場合、AppleはSiriの改善のために音声データを収集します。音声データはAppleのクラウドベースのサービスを通じて、したがって、セキュアなXenMobileコンテナの外側に存在します。ただし、ディクテーションの結果として生じたテキストは、コンテナ内に残ります。

XenMobileでは、セキュリティのニーズの要件に応じて、Siriおよびディクテーションサービスをブロックできます。

MAM展開では、各アプリのディクテーションブロックポリシーはデフォルトで **[On]** であり、デバイスのマイクは無効になります。ディクテーションを許可する場合、**[Off]** に設定します。XenMobileコンソールの **[Configure]** > **[Apps]** で、ポリシーを検出できます。アプリを選択し、**[Edit]** をクリックしてから **[iOS]** をクリックします。



MDM展開では、**[Configure]** > **[Device Policies]** > **[Restrictions Policy]** > **[iOS]** で、SiriポリシーとともにSiriを無効にすることもできます。Siriの使用は、デフォルトで許可されています。



XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

## Restrictions Policy

This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.

**Allow hardware controls**

- Camera  ON
- FaceTime
- Screen shots  ON
- Photo streams  ON iOS 5.0+
- Shared photo streams  ON iOS 6.0+
- Voice dialing  ON
- Siri  ON
- Allow while device is locked
- Siri profanity filter

Back Next >

Siriおよびディクテーションを許可するかどうか決定するときの留意事項：

- Appleが公開した情報によると、AppleはSiriおよびディクテーション音声クリップデータを最大で2年間保持します。データにはユーザーを表す乱数が割り当てられ、音声ファイルはこの乱数に関連付けられます。詳しくは、Wiredの記事「[Apple reveals how long Siri keeps your data](#)」を参照してください。
- iOSデバイスで [設定] > [一般] > [キーボード] と移動して、[音声入力] の下のリンクをタップすると、Appleのプライバシーポリシーを確認できます。

# ストレージ暗号化デバイスポリシー

Apr 27, 2017

XenMobileでストレージ暗号化デバイスポリシーを作成して、内部ストレージと外部ストレージを暗号化したり、デバイスによっては、ユーザーがデバイスでストレージカードを使用できないようにしたりします。

Samsung SAFE、Windows Phone、Android Sonyデバイスに対してポリシーを作成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

[Samsung SAFEの設定](#)

[Windows Phoneの設定](#)

[Android Sonyの設定](#)

注：Samsung SAFEデバイスの場合は、このポリシーを構成する前に、次の要件が満たされていることを確認します。

- ユーザーのデバイスで画面のロックオプションを設定する必要があります。
- ユーザーのデバイスがコンセントに接続され、80%充電されている必要があります。
- 数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Security] の下の [Storage Encryption] をクリックします。[Storage Encryption Policy] 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

## Storage Encryption Policy

### Policy Information

This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.

Policy Name\*

Description

1 Policy Info

2 Platforms

- Samsung SAFE
- Windows Phone
- Android Sony

3 Assignment

Next >

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

The screenshot shows the XenMobile Configure interface for a Storage Encryption Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Storage Encryption Policy' page is displayed, featuring a left sidebar with sections: '1 Policy Info', '2 Platforms' (containing 'Samsung SAFE', 'Windows Phone', and 'Android Sony'), and '3 Assignment'. The main content area is titled 'Policy Information' and contains the following text: 'This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.' Below this text are two toggle switches: 'Encrypt internal storage' (ON) and 'Encrypt external storage' (ON). A 'Deployment Rules' section is visible but collapsed. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Encrypt internal storage** : ユーザーのデバイスの内部ストレージを暗号化するかどうかを選択します。内部ストレージには、デバイスのメモリと内部ストレージが含まれます。デフォルトは [ON] です。
- **Encrypt external storage** : ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。デフォルトは [ON] です。

The screenshot shows the XenMobile configuration interface for a Storage Encryption Policy. The left sidebar contains a navigation menu with sections: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', three options are listed: Samsung SAFE, Windows Phone, and Android Sony, all with checked checkboxes. The main content area is titled 'Policy Information' and includes a descriptive paragraph. Below this, there are two toggle switches: 'Require device encryption' and 'Disable storage card', both currently set to 'OFF'. A 'Deployment Rules' section is partially visible below. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Require device encryption** : ユーザーのデバイスを暗号化するかどうかを選択します。デフォルトは[OFF] です。
- **Disable storage card** : ユーザーがデバイスでストレージカードを使用できないようにするかどうかを選択します。デフォルトは [OFF] です。

This screenshot shows the same XenMobile configuration interface, but with the 'Encrypt external storage' toggle switch set to 'ON'. The 'Require device encryption' and 'Disable storage card' options remain 'OFF'. The 'Platforms' section is identical to the previous screenshot, with Samsung SAFE, Windows Phone, and Android Sony selected. The 'Deployment Rules' section is still partially visible. The 'Back' and 'Next >' buttons are present at the bottom right.

次の設定を構成します。

- **Encrypt external storage** : ユーザーのデバイスの外部ストレージを暗号化するかどうかを選択します。数字と文字（または記号）が両方含まれているデバイスパスワードが必要です。デフォルトは [ON] です。

## 7. 展開規則を構成します。

8. [Next] をクリックします。[Storage Encryption Policy] 割り当てページが開きます。

The screenshot shows the XenMobile configuration interface for a Storage Encryption Policy. The interface is divided into several sections:

- Storage Encryption Policy**: This policy lets you encrypt stored data and prevent storage card usage depending on the device platform. For Samsung SAFE devices, the Screen Lock option must also be set on the device in order for this policy to work.
- Choose delivery groups**: A search bar with the placeholder text "Type to search" and a "Search" button. Below the search bar is a list of delivery groups: "AllUsers" (checked) and "sales" (unchecked).
- Delivery groups to receive app assignment**: A list showing "AllUsers".
- Deployment Schedule**: A section with a right-pointing arrow and a circled question mark icon.
- Buttons**: "Back" and "Save" buttons are located at the bottom right of the interface.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# サブスクライブされたカレンダーデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、サブスクライブされたカレンダーをユーザーのiOSデバイスのカレンダー一覧に追加することができます。サブスクライブできる公開カレンダーの一覧は、[www.apple.com/downloads/macosx/calendars](http://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. [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。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. Under 'Configure', there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Subscribed Calendars Policy' and 'Policy Information'. Below the title, there is a description: 'This policy adds the parameters for a subscribed calendar to a users' calendars list.' There are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is a text input, and the 'Description' field is a larger text area. A 'Next >' button is located at the bottom right of the form. The left sidebar shows a navigation menu with '1 Policy Info' selected, '2 Platforms', and '3 Assignment'.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[iOS Platform Information] ページが開きます。

The screenshot shows the 'Configure' page for a 'Subscribed Calendars Policy'. The left sidebar has 'Subscribed Calendars Policy' selected, with sub-items '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (checked). The main area is titled 'Policy Information' and contains the following fields:

- Description\* (text input)
- URL\* (text input)
- User name\* (text input)
- Password (password input)
- Use SSL (toggle set to OFF)
- Policy Settings:
  - Remove policy:  Select date,  Duration until removal (in days)
  - Allow user to remove policy: dropdown menu set to 'Always'

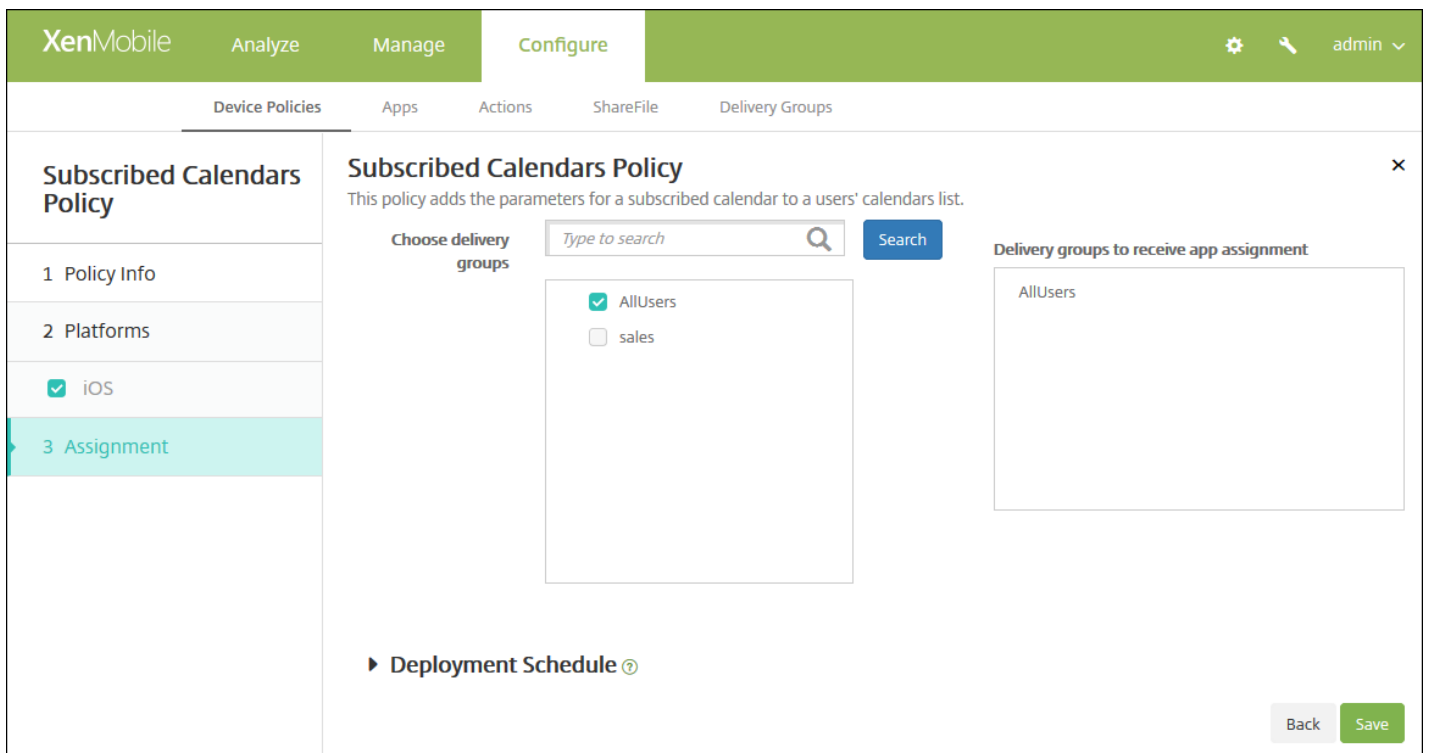
At the bottom right, there are 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- **Description** : カレンダーの説明を入力します。このフィールドは必須です。
- **URL** : カレンダーのURLを入力します。iCalendarファイル (.ics) へのwebcal:// URLまたはhttp://リンクを入力してください。このフィールドは必須です。
- **User name** : ユーザーのログオン名を入力します。このフィールドは必須です。
- **Password** : 任意で、ユーザーのパスワードを入力します。
- **Use SSL** : カレンダーに対してSecure Socket Layer接続を使用するかどうかを選択します。デフォルトは、 [Off] です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Subscribed Calendars Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# 契約条件デバイスポリシー

Apr 27, 2017

社内ネットワークに接続するときに適用される、会社の特定のポリシーの承諾をユーザーに求める場合、XenMobileで契約条件デバイスポリシーを作成します。ユーザーがXenMobileにデバイスを登録するときに、この契約条件が示され、ユーザーは自分のデバイスを登録するためにこれに同意する必要があります。契約条件を拒否すると、登録処理が取り消されます。

社内に複数の国のユーザーがおり、それぞれの母国語で契約条件の承諾を求める場合は、異なる言語での契約条件のポリシーをそれぞれ作成できます。展開する予定のプラットフォームと言語の組み合わせごとに、個別のファイルを提供する必要があります。AndroidデバイスおよびiOSデバイスの場合は、PDFファイルを提供する必要があります。Windowsデバイスの場合は、テキスト（TXT）ファイルと付属のイメージファイルを提供する必要があります。

[iOSおよびAndroidの設定](#)

[Windows PhoneおよびWindowsタブレットの設定](#)

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [Terms & Conditions] をクリックします。[Terms & Conditions Policy] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are navigation tabs: XenMobile, Analyze, Manage, and Configure. The 'Configure' tab is active. Below the navigation, there are sub-tabs: Device Policies, Apps, Actions, ShareFile, and Delivery Groups. The 'Device Policies' sub-tab is selected. On the left, there is a sidebar for the 'Terms & Conditions Policy' with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', four options are listed with checkboxes: iOS, Android, Windows Phone, and Windows Tablet. All four are checked. The main content area is titled 'Policy Information' and contains a text input field for 'Policy Name\*' and a larger text area for 'Description'. A 'Next >' button is located at the bottom right of the main content area.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Terms & Conditions Platforms] 情報ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Terms & Conditions Policy

This policy lets you upload your own Terms & Conditions file in a preferred language for users to view and accept on their devices. You can upload files in additional languages as well. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

File to be imported\*

Default Terms & Conditions  OFF

Back

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Terms & Conditions Policy

This policy lets you upload your own Terms & Conditions file in a preferred language for users to view and accept on their devices. You can upload files in additional languages as well. For Windows Phone/Tablet, the payloads are supported only on Windows 10 and later supervised devices.

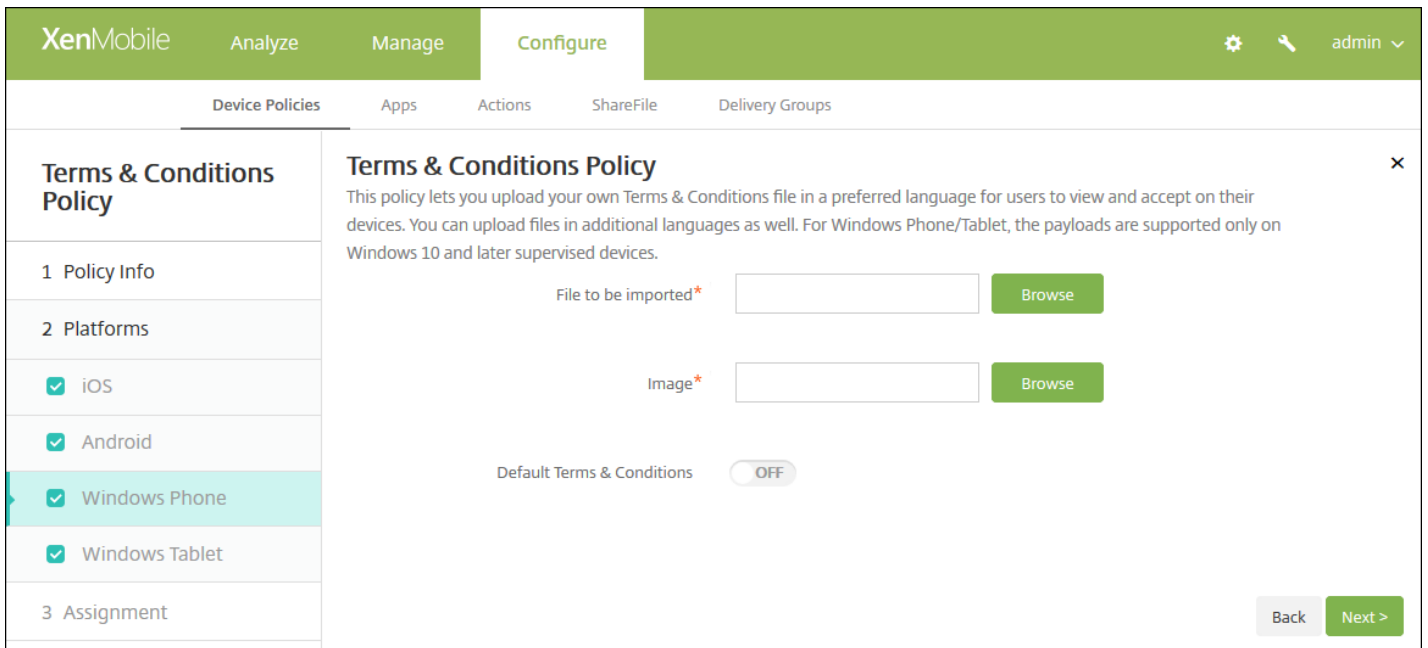
File to be imported\*

Default Terms & Conditions  OFF

Back

次の設定を構成します。

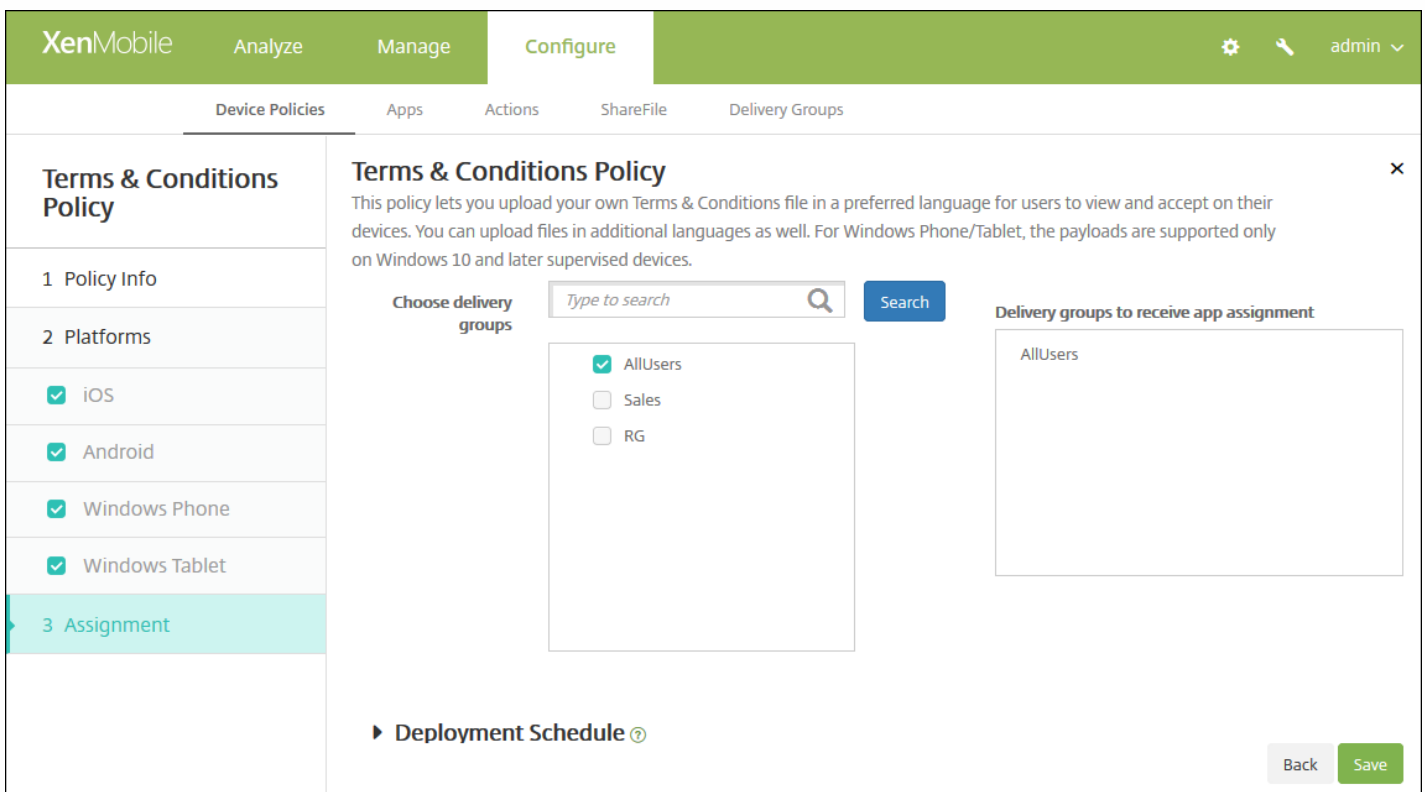
- **File to be imported** : **[Browse]** をクリックしてインポートする契約条件ファイルの場所へ移動し、そのファイルを選択します。
- **Default Terms & Conditions** : このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは **[OFF]** です。



次の設定を構成します。

- **File to be imported** : **[Browse]** をクリックしてインポートする契約条件ファイルの場所へ移動し、そのファイルを選択します。
- **Image**: **[Browse]** をクリックしてインポートするイメージファイルの場所へ移動し、そのファイルを選択します。
- **Default Terms & Conditions** : このファイルを、契約条件の異なる複数のグループのメンバーであるユーザーのデフォルトのドキュメントにするかどうかを選択します。デフォルトは **[OFF]** です。

6. **[Next]** をクリックします。 **[Terms & Conditions Policy]** 割り当てページが開きます。



7. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

8. [Save] をクリックします。

# Apple Configuratorを使用してiOSデバイスをSupervisedモードにするには

Apr 27, 2017

Apple Configuratorの場合は、Apple Configuratorアプリが動作するAppleコンピューターにデバイスを接続します。Apple Configuratorでデバイスを準備してポリシーを構成します。必要なポリシーでデバイスをプロビジョニングした後で、初めてデバイスをXenMobileに接続すると、ポリシーが適用されデバイスの管理を開始できます。システム要件などApple Configuratorについて詳しくは、[Apple Support](#)を参照してください。

## Important

デバイスをSupervisedモードにすると、特定のバージョンのiOSがデバイスにインストールされ、以前に保存されたユーザーデータまたはアプリケーションがデバイスから完全に消去されます。

1. iTunesからApple Configuratorをインストールします。
2. iOSデバイスをAppleコンピューターに接続します。
3. Apple Configuratorを起動します。監視の準備が整っているデバイスがあることがConfiguratorに表示されます。
4. デバイスの監視の準備を行うには：
  1. [Supervision] コントロールを [On] に切り替えます。構成を定期的に再適用することによって継続的にデバイスを管理する場合は、この設定を選択することをお勧めします。
  2. 必要に応じてデバイスの名前を指定します。
  3. 最新バージョンのiOSをインストールする場合、[iOS] ボックスの一覧で [Latest] を選択します。
5. デバイスの監視の準備が整ったら、[Prepare] をクリックします。

# VPNデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、VPN (Virtual Private Network : 仮想プライベートネットワーク) の設定を構成し、ユーザーのデバイスが社内リソースに安全に接続できるようにすることができます。VPNポリシーは、iOS、Android (Android for Work対応デバイスを含む)、Samsung SAFE、Samsung KNOX、Windowsタブレット、Windows Phone、Amazonの各プラットフォームに対して構成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

[iOSの設定](#)

[Mac OS Xの設定](#)

[Androidの設定](#)

[Samsung SAFEの設定](#)

[Samsung KNOXの設定](#)

[Windows Phoneの設定](#)

[Windowsタブレットの設定](#)

[Amazonの設定](#)

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[VPN]** をクリックします。**[VPN Policy]** ページが開きます。

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

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

5. [Next] をクリックします。[Policy Platforms] ページが開きます。[Policy Platforms] ページが開いたときはすべてのプラットフォームがオンになっており、最初はiOSプラットフォームが表示されます。

6. [Platforms] の下で、追加するプラットフォームをオンにします。構成しないプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
- 3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name

Connection type **L2TP**

Server name or IP address\*

User account

Password authentication  
 RSA SecureID authentication

Shared secret

Send all traffic **OFF**

**Proxy**

Proxy configuration **None**

**Policy Settings**

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy **Always**

► **Deployment Rules**

Back Next >

次の設定を構成します。

- **Connection name** : 接続の名前を入力します。
- **Connection type** : 一覧から、この接続において使用するプロトコルを選択します。デフォルトは[L2TP] です。
  - L2TP : レイヤー2トンネリングプロトコルと事前共有キー認証。
  - PPTP : Point-to-Pointトンネリング。
  - IPsec : 社内VPN接続
  - Cisco AnyConnect : Cisco AnyConnect VPNクライアント
  - Juniper SSL : Juniper Networks SSL VPNクライアント
  - F5 SSL : F5 Networks SSL VPNクライアント
  - SonicWALL Mobile Connect : iOS用Del統合VPNクライアント
  - Ariba VIA : Aruba Networks仮想インターネットアクセスクライアント
  - IKEv2 (iOS only) : iOS専用インターネットキー交換バージョン2
  - Citrix VPN : iOS用Citrix VPNクライアント
  - Custom SSL : カスタムSSL (Secure Socket Layer)



次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

L2TPプロトコルの構成

PPTPプロトコルの構成

IPSecプロトコルの構成

Cisco AnyConnectプロトコルの構成

Juniper SSLプロトコルの構成

F5 SSLプロトコルの構成

SonicWALLプロトコルの構成

Ariba VIAプロトコルの構成

[IKEv2] プロトコルの構成

Citrix VPNプロトコルの構成

カスタムSSLプロトコルの構成

[Enable VPN on demand] オプションの構成

- プロキシDHCP

- Proxy configuration : 一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。デフォルトは [None] です。
  - [Manual] を有効にした場合は、次の設定を構成します。
    - Host name or IP address for the proxy server : プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
    - Port for the proxy server : プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - User name : 任意で、プロキシサーバーのユーザー名を入力します。
    - Password : 任意で、プロキシサーバーのパスワードを入力します。
  - [Automatic] を選択した場合は、次の設定を構成します。
    - Proxy server URL : プロキシサーバーのURLを入力します。このフィールドは必須です。

- ポリシー設定

- [Policy Settings] の下の [Remove policy] の横にある、[Select date] または [Duration until removal (in days)] をクリックします。
- [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet
  - Amazon
- 3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name

Connection type **L2TP**

Server name or IP address\*

User account

Password authentication  
 RSA SecureID authentication  
 Kerberos authentication  
 CryptoCard authentication

Shared secret

Send all traffic **OFF**

#### Proxy

Proxy configuration **None**

#### Policy Settings

Remove policy  Select date  
 Duration until removal (in days)

Allow user to remove policy **Always**

Profile scope **User** OS X 10.7+

#### Deployment Rules

Back Next >

次の設定を構成します。

- **Connection name** : 接続の名前を入力します。
- **Connection type** : 一覧から、この接続において使用するプロトコルを選択します。デフォルトは [L2TP] です。
  - L2TP : レイヤー2トンネリングプロトコルと事前共有キー認証。
  - PPTP : Point-to-Pointトンネリング。
  - IPsec : 社内VPN接続
  - Cisco AnyConnect : Cisco AnyConnect VPNクライアント
  - Juniper SSL : Juniper Networks SSL VPNクライアント
  - F5 SSL : F5 Networks SSL VPNクライアント
  - SonicWALL Mobile Connect : iOS用Dell統合VPNクライアント

- **Ariba VIA** : Aruba Networks仮想インターネットアクセスクライアント
- **Citrix VPN** : Citrix VPNクライアント
- **Custom SSL** : カスタムSSL (Secure Socket Layer)

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

[L2TPプロトコルの構成](#)

[PPTPプロトコルの構成](#)

[IPSecプロトコルの構成](#)

[Cisco AnyConnectプロトコルの構成](#)

[Juniper SSLプロトコルの構成](#)

[F5 SSLプロトコルの構成](#)

[SonicWALLプロトコルの構成](#)

[Ariba VIAプロトコルの構成](#)

[Citrix VPNプロトコルの構成](#)

[カスタムSSLプロトコルの構成](#)

[\[Enable VPN on demand\] オプションの構成](#)

#### ● プロキシDHCP

- **Proxy configuration** : 一覧から、VPN接続のプロキシサーバーのルーティング方法を選択します。デフォルトは [None] です。
  - [Manual] を有効にした場合は、次の設定を構成します。
    - **Host name or IP address for the proxy server** : プロキシサーバーのホスト名またはIPアドレスを入力します。このフィールドは必須です。
    - **Port for the proxy server** : プロキシサーバーのポート番号を入力します。このフィールドは必須です。
    - **User name** : 任意で、プロキシサーバーのユーザー名を入力します。
    - **Password** : 任意で、プロキシサーバーのパスワードを入力します。
  - [Automatic] を選択した場合は、次の設定を構成します。
    - **Proxy server URL** : プロキシサーバーのURLを入力します。このフィールドは必須です。

#### ● ポリシー設定

- [Policy Settings] の下の [Remove policy] の横にある、[Select date] または [Duration until removal (in days)] をクリックします。
- [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
- [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。
- [Profile scope] の横にある、[User] または [System] を選択します。デフォルトは [User] です。このオプションはOS X 10.7以降でのみ使用できます。

The screenshot shows the XenMobile configuration interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar lists 'VPN Policy' with sub-sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android (highlighted), Samsung SAFE, Samsung KNOX, Windows Phone, Windows Tablet, and Amazon. The main content area is titled 'Policy Information' and contains the following configuration options:

- Cisco AnyConnect VPN**
  - Connection name\* (text input)
  - Server name or IP address\* (text input)
  - Backup VPN server (text input)
  - User group (text input)
  - Identity credential (dropdown menu, currently set to 'None')
- Trusted Networks**
  - Automatic VPN policy (toggle switch, currently set to 'OFF')
- Deployment Rules** (expandable section)

At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- Cisco AnyConnect VPN
  - Connection name : Cisco AnyConnect VPN接続の名前を入力します。このフィールドは必須です。
  - Server name or IP address : VPNサーバーの名前またはIPアドレスを入力します。このフィールドは必須です。
  - Backup VPN server : バックアップVPNサーバー情報を入力します。
  - User group : ユーザーグループ情報を入力します。
  - Identity credential : 一覧から、ID資格情報を選択します。
- 信頼されたネットワーク
  - Automatic VPN policy : このオプションをオンまたはオフにして、信頼できるネットワークおよび信頼できないネットワークに対するVPNの動作方法を設定します。有効にした場合は、次の設定を構成します。
    - Trusted network policy : 一覧から、目的のポリシーを選択します。デフォルトは [Disconnect] です。選択できるオプションは以下のとおりです。
      - Disconnect : クライアントにより、信頼できるネットワーク圏内のVPN接続が終了されます。これがデフォルトの設定です。
      - Connect : クライアントにより、信頼できるネットワーク圏内のVPN接続が開始されます。
      - Do Nothing : クライアントによるアクションはありません。
      - Pause : 信頼できるネットワーク圏外でVPNセッションが確立された後、信頼済みとして構成されたネットワークにユーザーがアクセスすると、VPNセッションが (切断ではなく) 一時停止されます。ユーザーが信頼できるネットワークから離れると、セッションが再開されます。これにより、信頼できるネットワークを離れた後に新しいVPNセッションを確立する手間が省かれます。
    - Untrusted network policy : 一覧から、目的のポリシーを選択します。デフォルトは [Connect] です。選択できる

オプションは以下のとおりです。

- **Connect** : クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。
- **Do Nothing** : クライアントにより、信頼できないネットワーク圏内でVPN接続が開始されます。このオプションにより、[Always-on VPN] が無効化されます。
- **Trusted domains** : クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるドメインサフィックスごとに、[Add] をクリックして以下の操作を行います。
  - **Domain** : 追加するドメインを入力します。
  - [Save] をクリックしてドメインを保存するか、[Cancel] をクリックして操作を取り消します。
- **Trusted servers** : クライアントが信頼できるネットワーク圏内にある場合にネットワークインターフェイスに設定することができるサーバーアドレスごとに、[Add] をクリックして以下の操作を行います。
  - **Servers** : 追加するサーバーを入力します。
  - [Save] をクリックしてサーバーを保存するか、[Cancel] をクリックして操作を取り消します。

注 : 既存のサーバーを削除するには、項目が含まれる行の上にマウスポインターを置き、右側のごみ箱アイコンをクリックします。確認ダイアログボックスが開きます。項目を削除するには [Delete] をクリックし、項目をそのままにするには [Cancel] をクリックします。

既存のサーバーを編集するには、項目が含まれる行の上にマウスポインターを置き、右側のペンアイコンをクリックします。項目を変更し、[Save] をクリックして変更した項目を保存するか、[Cancel] をクリックして項目を変更せずそのままにします。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The 'Configure' section is active, showing a sidebar with 'VPN Policy' selected. The main content area is titled 'Policy Information' and contains a form for configuring a VPN connection. The form includes fields for 'Connection name\*', 'Vpn Type' (set to 'L2TP with pre-shared key'), 'Host name\*', 'User name', 'Password', and 'Pre-shared key\*'. Below the form is a section for 'Deployment Rules'. At the bottom right, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Connection name** : 接続の名前を入力します。
- **Vpn type** : 一覧から、この接続において使用するプロトコルを選択します。デフォルトは**L2TP with pre-shared key**です。選択できるオプションは以下のとおりです。
  - **L2TP with pre-shared key** : レイヤー2トンネリングプロトコルと事前共有キー認証。これがデフォルトの設定です。
  - **L2TP with certificate** : レイヤー2トンネリングプロトコルと証明書。
  - **PPTP** : Point-to-Pointトンネリング。
  - **Enterprise** : 社内VPN接続。Version 2.0よりも前のSAFEバージョンに適用されます。
  - **Generic** : 一般的なVPN接続。Version 2.0以降のSAFEバージョンに適用されます。

以下のセクションでは、上記のVPNの種類ごとに構成オプションを示します。

[L2TP with pre-shared key] プロトコルの構成

[L2TP with certificate] プロトコルの構成

[PPTP] プロトコルの構成

[Enterprise] プロトコルの構成

[Generic] プロトコルの構成

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX**
  - Windows Phone
  - Windows Tablet
  - Amazon
- 3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Vpn Type: Enterprise

Connection name\*:

Host name\*:

Enable backup server: OFF

Enable user authentication: OFF

Group name:

Authentication method: Certificate

Identity credential: None

CA certificate: Select certificate

Enable default route: OFF

Enable smartcard authentication: OFF

Enable mobile option: OFF

Diffie-Hellman group value (key strength): 0

Split tunnel type: Auto

SuiteB Type: GCM-128

**Forward routes**

Forward route

Forward route	Add
<input type="text"/>	<input type="button" value="Add"/>

► **Deployment Rules**

Back Next >

注：Samsung KNOXのポリシーを構成した場合、ポリシーはSamsung KNOXコンテナにのみ適用されます。

次の設定を構成します。

- **Vpn Type**：一覧で、構成するVPN接続の種類として、[Enterprise]（Version 2.0より前のKNOXバージョンに適用）または [Generic]（Version 2.0以降のKNOXバージョンに適用）をクリックします。デフォルトは [Enterprise] です。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

**VPN Policy**

1 Policy Info

2 Platforms

- iOS
- Mac OS X
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Tablet
- Amazon

3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

Connection name\*

Profile type

VPN server name\*

Tunneling protocol\*

Authentication method\*

EAP method\*

DNS suffix

Trusted networks

Require smart card certificate

Automatically select client certificate

Remember credential

Always-on VPN

Bypass For Local

► Deployment Rules

Back Next >

注：これらの設定は、Windows 10以降の監視対象Windows Phoneでのみサポートされます。

次の設定を構成します。

- **Connection name** : 接続の名前を入力します。このフィールドは必須です。
- **Profile type** : 一覧から、[Native] または [Plugin] を選択します。デフォルトは [Native] です。次のセクションでは、各オプションの設定について説明します。
- **Configure Native profile type settings** : 以下の設定は、ユーザーのWindows Phoneに組み込まれているVPNに適用されます。
  - **VPN server name** : VPNサーバーのFQDNまたはIPアドレスを入力します。このフィールドは必須です。



- **Tunneling protocol** : 一覧から、使用するVPNトンネルの種類を選択します。デフォルトは [L2TP] です。選択できるオプションは以下のとおりです。
  - L2TP : レイヤー2トンネリングプロトコルと事前共有キー認証。
  - PPTP : Point-to-Pointトンネリング。
  - IKEv2 : インターネットキー交換バージョン2
- **Authentication method** : 一覧から、使用する認証方法を選択します。デフォルトは [EAP] です。選択できるオプションは以下のとおりです。
  - EAP : 拡張認証プロトコル。
  - MSChapV2 : 相互認証にMicrosoftのチャレンジハンドシェイク認証を使用します。トンネルの種類に [IKEv2] を選択した場合、このオプションは使用できません。 [MSChapV2] を選択すると、 [Automatically use Windows credentials] オプションが表示されます。デフォルトは [OFF] です。
- **EAP method** : 一覧から、使用するEAP方法を選択します。デフォルトは [TLS] です。 [MSChapV2] 認証が有効になっている場合、このフィールドは使用できません。選択できるオプションは以下のとおりです。
  - TLS : Transport Layer Security
  - PEAP : 保護された拡張認証プロトコル
- **DNS Suffix** : DNSサフィックスを入力します。
- **Trusted networks** : アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
- **Require smart card certificate** : スマートカード証明書を必須とするかどうかを選択します。デフォルトは [OFF] です。
- **Automatically select client certificate** : 認証に使用するクライアント証明書が自動的に選択されるようにするかどうかを選択します。デフォルトは [OFF] です。 [Require smart card certificate] が有効になっている場合、このオプションは使用できません。
- **Remember credential** : 資格情報をキャッシュするかどうかを選択します。デフォルトは [OFF] です。有効にすると、可能な場合に資格情報がキャッシュされます。
- **Always on VPN** : VPNを常にオンにするかどうかを選択します。デフォルトは [OFF] です。有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
- **Bypass For Local** : ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。
- **Configure Plugin protocol type** : 以下の設定は、Windows Storeから取得し、ユーザーのデバイスにインストールしたVPNプラグインに適用されます。
  - **Server address** : VPNサーバーのURLホスト名またはIPアドレスを入力します。
  - **Client app ID** : VPNプラグインのパッケージファミリー名を入力します。
  - **Plugin Profile XML** : 使用するカスタムVPNプラグインプロファイルの場所に [Browse] をクリックして移動し、ファイルを選択します。形式などの詳細については、プラグインプロバイダーにお問い合わせください。
  - **DNS Suffix** : DNSサフィックスを入力します。
  - **Trusted networks** : アクセスにVPN接続を必要としないネットワークの一覧をコンマ区切りで入力します。たとえば、ユーザーが社内ワイヤレスネットワークのメンバーであれば、保護されているリソースに直接アクセスすることができます。
  - **Remember credential** : 資格情報をキャッシュするかどうかを選択します。デフォルトは [OFF] です。有効にすると、可能な場合に資格情報がキャッシュされます。
  - **Always on VPN** : VPNを常にオンにするかどうかを選択します。デフォルトは [OFF] です。有効にすると、ユーザーが手動で切断するまで、VPN接続はオンのままです。
  - **Bypass For Local** : ローカルリソースによるプロキシサーバーのバイパスを許可するアドレスおよびポート番号を入力します。

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- Policy Info
- Platforms
  - iOS
  - Mac OS X
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Phone
  - Windows Tablet**
  - Amazon
- Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.

OS version\*

Connection name\*

Profile type

Server address\*

Remember credential

DNS suffix

Tunnel type\*

Authentication method\*

EAP method\*

Trusted networks

Require smart card certificate

Automatically select client certificate

Always-on VPN

Bypass For Local

► **Deployment Rules**

[Back](#) [Next >](#)

https://web.mail.comcast.net/zimbra/mail?app=mail#1

次の設定を構成します。

- **OS version** : 一覧から、Windows 8.1の場合は [8.1] を、Windows 10の場合は [10] を選択します。デフォルトは10です。

[Windows 10の設定の構成](#)

[Windows 8.1設定の構成](#)

XenMobile Analyze Manage **Configure** ⚙️ 🔍 admin ▾

Device Policies Apps Actions ShareFile Delivery Groups

### VPN Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Android
  - Samsung SAFE
  - Samsung KNOX
  - Windows Tablet
  - Windows Phone
  - Amazon
- 3 Assignment

### Policy Information

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet.

Connection name\*

Vpn Type

Server address\*

User name

Password

L2TP Secret

IPSec Identifier

IPSec pre-shared key

DNS search domains

DNS servers

Forwarding routes

▶ Deployment Rules

次の設定を構成します。

- **Connection name** : 接続の名前を入力します。
- **Vpn type** : 一覧から、接続の種類を選択します。選択できるオプションは以下のとおりです。
  - **L2TP PSK** : レイヤー2トンネリングプロトコルと事前共有キー認証。これがデフォルトの設定です。
  - **L2TP RSA** : レイヤー2トンネリングプロトコルとRSA認証。
  - **IPSEC XAUTH PSK** : インターネットプロトコルセキュリティと事前共有キーおよび拡張認証。
  - **IPSEC HYBRID RSA** : インターネットプロトコルセキュリティとハイブリッドRSA認証。
  - **PPTP** : Point-to-Pointトンネリング。

次のセクションは、上記の接続の種類ごとに、構成オプションを示しています。

[L2TP PSKの設定の構成](#)

[L2TP RSAの設定の構成](#)

[IPSEC XAUTH PSKの設定の構成](#)

IPSEC AUTH RSAの設定の構成

IPSEC HYBRID RSAの設定の構成

PPTP設定の構成

7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface for a VPN Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'VPN Policy' and contains a description: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the payloads are supported only on Windows 10 and later supervised devices.' The 'Choose delivery groups' section has a search box and a 'Search' button. Below the search box is a list of delivery groups: 'AllUsers' (checked) and 'sales' (unchecked). To the right, the 'Delivery groups to receive app assignment' section shows a list with 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a right-pointing arrow and a help icon. The page also features a 'Back' button and a 'Save' button.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：

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

11. [Save] をクリックします。

# 壁紙デバイスポリシー

Apr 27, 2017

.pngファイルまたは.jpgファイル追加して、iOSデバイスのロック画面かホーム画面、または両方の画面の壁紙に設定することができます。iOS 7.1.2以降で使用できます。iPadおよびiPhoneで異なる壁紙を使用するには、別の壁紙ポリシーを作成して、それを適切なユーザーに展開する必要があります。

次の表に、Apple社がiOSデバイス用に推奨しているイメージサイズを示します。

デバイス		イメージサイズ (ピクセル)
iPhone - なし。	iPad	
4、4s		640 x 960
5、5c、5s		640 x 1136
6、6s		750 x 1334
6 Plus		1080 x 1920
	Air、 2	1536 x 2048
	4、 3	1536 x 2048
	Mini 2、 3	1536 x 2048
	Mini	768 x 1024

1. XenMobileコンソールで、 [Configure] の [Device Policies] をクリックします。 [Device Policies] ページが開きます。
2. [Add] をクリックします。 [Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、 [End User] の下の [Wallpaper] をクリックします。 [Wallpaper Policy] ページが開きます。

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Wallpaper Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

#### Policy Information

This policy lets you add a .png or .jpg file to set wallpaper on a supervised device lock screen, home screen or both. Available in iOS 7.1.2 and later.

Policy Name\*

Description

Next >

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

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

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

XenMobile Analyze Manage **Configure** admin

Device Policies Apps Actions ShareFile Delivery Groups

### Wallpaper Policy

- 1 Policy Info
- 2 Platforms
- iOS
- 3 Assignment

#### Policy Information

This policy lets you add a .png or .jpg file to set wallpaper on a supervised device lock screen, home screen or both. Available in iOS 7.1.2 and later.

Apply to

Wallpaper file

► Deployment Rules

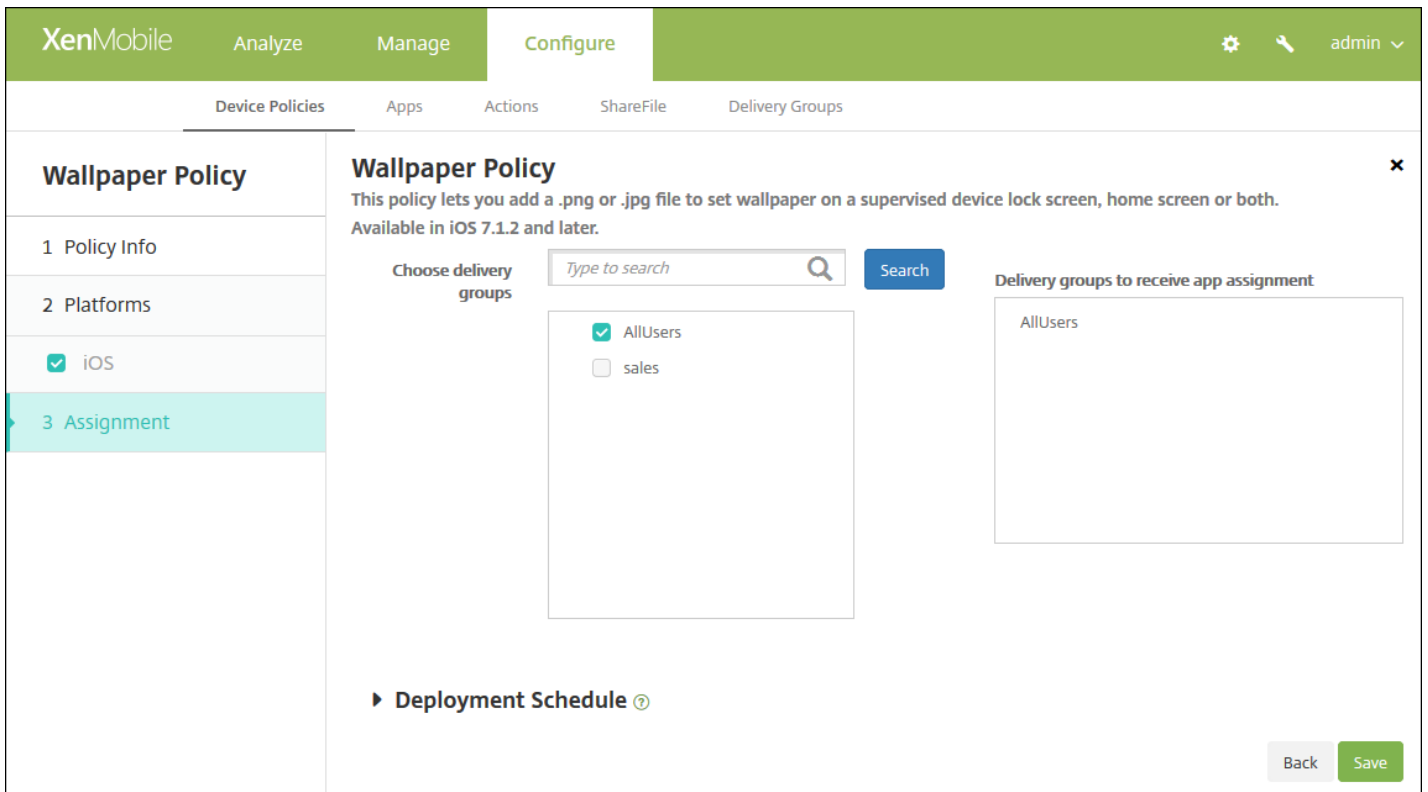
Back Next >

次の設定を構成します。

- Apply to : 一覧から、[Lock screen]、[Home (icon list) screen]、[Lock and home screens] のいずれかを選択して、壁紙を表示する場所を設定します。
- Wallpaper file : [Browse] をクリックして壁紙ファイルの場所に移動し、ファイルを選択します。

#### 7. 展開規則を構成します。

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



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。



# Webコンテンツデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加し、ホワイトリストおよびブラックリストに追加した特定のサイトとAppleのオートフィルター機能を組み合わせて使用して、iOSデバイスでWebコンテンツをフィルタリングできます。このポリシーはiOS 7.0以降のSupervisedモードのデバイスでのみ使用できます。iOSデバイスを監視モードにする方法については、「[Apple Configuratorを使用してiOSデバイスを監視モードにするには](#)」を参照してください。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] をクリックした後、[Security] の下の [Web Content Filter] をクリックします。[Web Content Filter Policy] ページが開きます。

The screenshot shows the XenMobile console interface for configuring a Web Content Filter Policy. The main content area is titled 'Web Content Filter Policy' and contains a 'Policy Information' section. This section includes a note: 'This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.' Below the note are two input fields: 'Policy Name\*' (with an asterisk indicating it is required) and 'Description'. The 'Policy Name' field is currently empty, and the 'Description' field is also empty. The 'Policy Name' field has a small icon in the bottom right corner. The 'Description' field has a small icon in the bottom right corner. The page has a green header with 'XenMobile' and 'Configure' tabs. The left sidebar shows 'Web Content Filter Policy' with three steps: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' step is selected. The 'Platforms' section shows 'iOS' selected with a checkmark. A 'Next >' button is visible in the bottom right corner.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[iOS Platform] 情報ページが開きます。

The screenshot shows the 'Configure' page for a 'Web Content Filter Policy'. The left sidebar has a navigation menu with 'Web Content Filter Policy' at the top, followed by '1 Policy Info', '2 Platforms', '3 Assignment', and 'iOS' (which is selected). The main content area is titled 'Policy Information' and includes a description: 'This policy lets you whitelist and blacklist specific URLs. The policy is supported only on iOS 7 and later supervised devices.' Below this, there are several sections: 'Filter type' (Built-in), 'Web Content Filter' (Auto filter enabled: OFF), 'Permitted URLs' (with an 'Add' button), 'Blacklisted URLs' (with an 'Add' button), 'Bookmark Whitelist' (with columns for URL\*, Bookmark Folder, Title\*, and an 'Add' button), and 'Policy Settings' (Remove policy: Select date, Duration until removal (in days) with a calendar icon, Allow user to remove policy: Always). At the bottom, there is a 'Deployment Rules' section and 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- **Filter type** : 一覧から [Built-in] または [Plug-in] を選択し、選択したオプションに応じた手順を実行します。デフォルトは [Built-in] です。

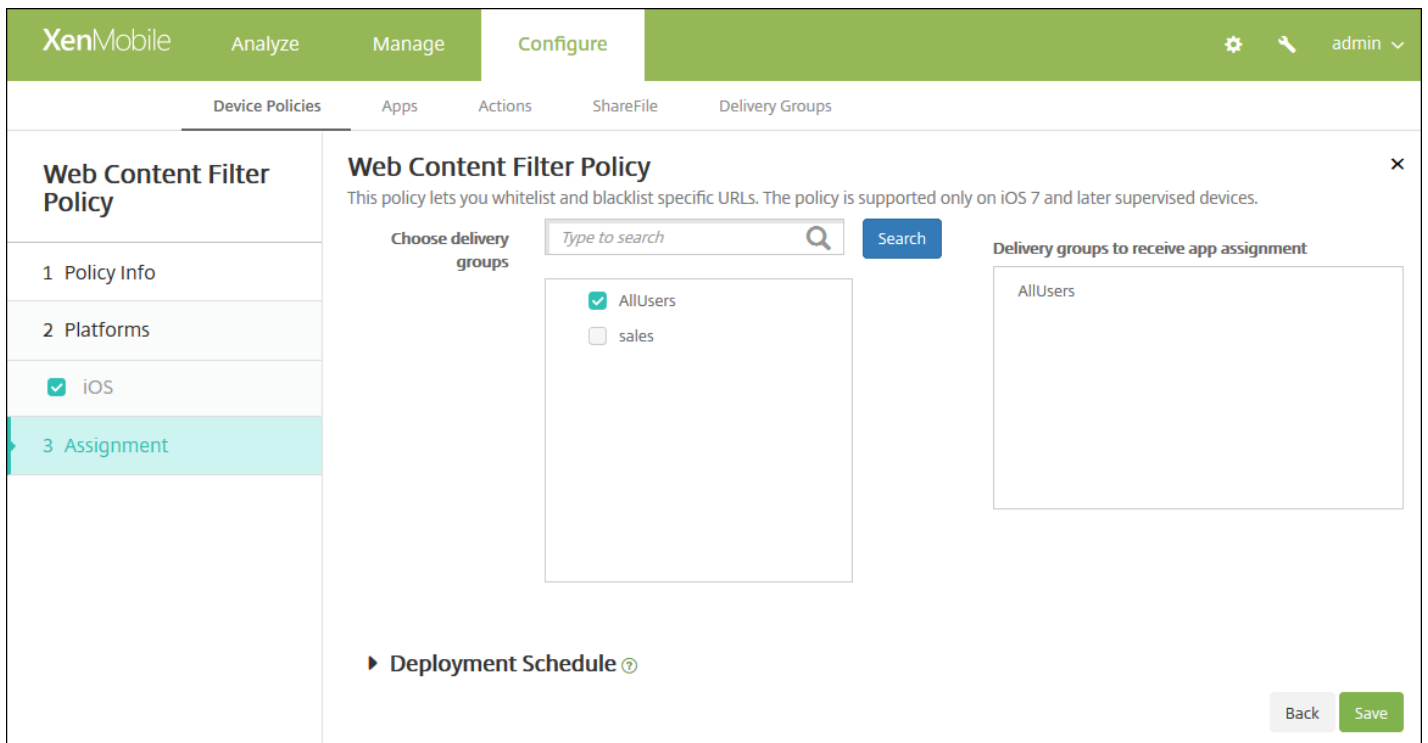
[組み込みフィルターの種類の設定](#)

[プラグインフィルターの種類の設定](#)

- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、 [Always] 、 [Password required] 、 [Never] のいずれかを選択します。
  - [Password required] を選択した場合、 [Removal password] の横に必要なパスワードを入力します。

[7. 展開規則を構成します。](#)

8. [Next] をクリックします。 [Web Content Filter Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# Webクリップデバイスポリシー

Apr 27, 2017

ショートカットやWebクリップをWebサイトに配置してユーザーデバイスのアプリと一緒に表示できます。iOS、Mac OS X、AndroidデバイスのWebクリップを表す独自のアイコンを指定できます。Windowsタブレットのみ、ラベルおよびURLが必要になります。

[iOSの設定](#)

[Mac OS Xの設定](#)

[Androidの設定](#)

[Windowsデスクトップ/タブレットの設定](#)

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開し、**[Apps]** の下の **[Webclip]** をクリックします。**[Webclip Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Configure' tab is active. Below this, the 'Webclip Policy' page is displayed. On the left, a sidebar contains three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' section is expanded, showing a list of operating systems with checkboxes: 'iOS', 'Mac OS X', 'Android', and 'Windows Desktop/Tablet'. All checkboxes are checked. The main content area is titled 'Policy Information' and includes a description: 'This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.' Below the description are two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area).

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7.を参照してプラットフォームの展開規則を設定します。

次の設定を構成します。

- **Label** : Webクリップと共に表示するラベルを入力します。
- **URL** : Webクリップに関連付けるURLを入力します。URLはプロトコル (例 : http://server) で始まる必要があります。
- **Removable** : ユーザーがWebクリップを削除できるかどうかを選択します。デフォルトは[OFF] です。
- **Icon to be updated** : [Browse] をクリックしてファイルの場所に移動し、Webクリップに使用するアイコンを選択します。
- **Precomposed icon** : アイコンにエフェクト (角丸、影付き、反射光) を適用するかどうかを選択します。デフォルトは [OFF] で、エフェクトが追加されます。
- **全画面** : リンクされているWebページを全画面モードで開くかどうかを選択します。デフォルトは[OFF] です。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Webclip Policy

This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.

1 Policy Info

2 Platforms

iOS

Mac OS X

Android

Windows Desktop/Tablet

3 Assignment

**Webclip Policy**

Label\*

URL\*  ⓘ

Icon to be updated

Policy Settings

Remove policy  Select date  
 Duration until removal (in days)

ⓘ

Allow user to remove policy  ⓘ

► Deployment Rules

次の設定を構成します。

- **Label** : Webクリップと共に表示するラベルを入力します。
- **URL** : Webクリップに関連付けるURLを入力します。URLはプロトコル (例 : http://server) で始まる必要があります。
- **Icon to be updated** : [Browse] をクリックしてファイルの場所に移動し、Webクリップに使用するアイコンを選択します。
- **ポリシー設定**
  - [Remove policy] の横にある [Select date] または [Duration until removal (in days)] をクリックします。
  - [Select date] をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - [Allow user to remove policy] の一覧で、[Always]、[Password required]、[Never] のいずれかを選択します。
  - [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。
  - [Profile scope] の一覧から、[User] または [System] を選択します。このオプションはOS X 10.7以降で使用できます。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Webclip Policy

This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.

1 Policy Info

2 Platforms

iOS

Mac OS X

Android

Windows Desktop/Tablet

3 Assignment

Rule  Add  Remove

Label\*

URL\*

Define an icon  OFF

► Deployment Rules

次の設定を構成します。

- **Rule** : このポリシーでWebクリップを追加または削除するかどうかを選択します。デフォルトは[追加]です。
- **Label** : Webクリップと共に表示するラベルを入力します。
- **URL** : Webクリップに関連付けるURLを入力します。
- **Define an icon** : アイコンファイルを使用するかどうかを選択します。デフォルトは[OFF]です。
- **Icon file** : [Define an icon] が [ON] の場合は、[Browse] をクリックしてアイコンファイルの場所へ移動し、ファイルを選択します。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### Webclip Policy

This policy lets you place shortcuts, or webclips, to websites to appear alongside apps on devices.

1 Policy Info

2 Platforms

iOS

Mac OS X

Android

Windows Desktop/Tablet

3 Assignment

Name\*

URL\*

► Deployment Rules

次の設定を構成します。

- **Name** : Webクリップと共に表示するラベルを入力します。
- **URL** : Webクリップに関連付けるURLを入力します。

#### 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface for a Webclip Policy. The left sidebar contains a navigation menu with sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Windows Desktop/Tablet' is selected. The main area is titled 'Webclip Policy' and contains a search box for 'Choose delivery groups' and a list of delivery groups including 'AllUsers' and two 'DG-' entries. Below this is a section for 'Deployment Schedule'.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。



注：

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

11. [Save] をクリックしてポリシーを保存します。

# WiFiデバイスポリシー

Apr 27, 2017

XenMobileコンソールの **[Configure]** > **[Device Policies]** ページを使用して、XenMobileで新しいWiFiデバイスポリシーを作成するか、既存のWiFiデバイスポリシーを編集します。WiFiポリシーでは、ネットワークの名前と種類、認証およびセキュリティポリシー、プロキシサーバーの使用や、そのほかのWiFi関連事項を、特定のデバイスプラットフォームのすべてのユーザーに対して一貫して定義し、ユーザーデバイスのWiFiネットワークへの接続方法を管理できます。

ユーザーのWiFi設定は、iOS、Mac OS X、Android (Android for Work対応デバイスを含む)、Windows Phone、Windowsデスクトップ/タブレットの各プラットフォームについて構成できます。プラットフォームごとに必要な値が異なります。これらの値について詳しくは、ここで説明しています。

[iOSの設定](#)

[Mac OS Xの設定](#)

[Androidの設定](#)

[Windows Phoneの設定](#)

[Windowsデスクトップ/タブレットの設定](#)

## Important

新しいポリシーを作成する前に、以下の手順を完了してください。

- 使用する予定の展開グループを作成します。
- ネットワークの名前と種類を確認します。
- 使用する予定の認証またはセキュリティの種類を確認します。
- 必要な場合、プロキシサーバーの情報を確認します。
- 必要なCA証明書をインストールします。
- 必要な共有キーを取得します。
- 証明書に基づいた認証のためにPKIエンティティを作成します。
- 資格情報プロバイダーを構成します。

詳しくは、「[Authentication](#)」とそのサブ記事を参照してください。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[WiFi]** をクリックします。**[WiFi Policy]** ページが開きます。

XenMobile Analyze Manage Configure

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

- 1 Policy Info
- 2 Platforms
  - iOS
  - Mac OS X
  - Android
  - Windows Phone
  - Windows Desktop/Tablet
  - Windows Mobile/CE
- 3 Assignment

### Policy Information

This policy lets you configure a WiFi profile for devices.

Policy Name\*

Description

Next >

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

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

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

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

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**Network type**: Standard

**Network name\***:

**Hidden network (enable if network is open or off)**: OFF

**Auto join (automatically join this wireless network)**: ON

**Security type**: None

**Proxy server settings**

**Proxy configuration**: None

**Policy Settings**

**Remove policy**:  Select date  Duration until removal (in days)

**Allow user to remove policy**: Always

**Deployment Rules**

Back Next >

次の設定を構成します。

- **Network type** : 一覧から、[Standard]、[Legacy Hotspot]、または[Hotspot 2.0]を選択して、使用する予定のネットワークの種類を設定します。
- **Network Name** : デバイスの使用可能なネットワークの一覧に表示されるSSIDを入力します。Hotspot 2.0には適用されません。
- **Hidden network (enable if network is open or off)** : ネットワークを隠しネットワークにするかどうかを選択します。
- **Auto Join (automatically join this wireless network)** : ネットワークに自動的に参加するかどうかを選択します。デフォルトは[ON]です。
- **Security type** : 一覧から、使用する予定のセキュリティの種類を選択します。Hotspot 2.0には適用されません。
  - None - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2パーソナル
  - 任意 (パーソナル)
  - WEPエンタープライズ
  - WPA/WPA2エンタープライズ
  - Any (Enterprise)

以下では、上記の接続の種類ごとに、構成するオプションを示します。

WPA、WPA Personal、Any (Personal)

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、Any (Enterprise)

- **プロキシサーバーの設定**
  - **Proxy configuration** : 一覧から、[None]、[Manual]、または[Automatic]を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は[None]で、そのほかの構成は不要です。
  - **[Manual]**を選択した場合は、次の設定を構成します。
    - **Hostname/IP address** : プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **Port** : プロキシサーバーのポート番号を入力します。
    - **Username** : 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - **Password** : 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - **[Automatic]**を選択した場合は、次の設定を構成します。
    - **Server URL** : プロキシ構成を定義するPACファイルのURLを入力します。
    - **Allow direct connection if PAC is unreachable** : PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは[ON]です。このオプションはiOS 7.0以降でのみ使用できます。
- **ポリシー設定**
  - **[Remove policy]**の横にある**[Select date]**または**[Duration until removal (in days)]**をクリックします。
  - **[Select date]**をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]**の一覧で、**[Always]**、**[Password required]**、**[Never]**のいずれかを選択します。
  - **[Password required]**を選択した場合、**[Removal password]**の横に必要なパスワードを入力します。

XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**Network type**: Standard

**Network name\***:

**Hidden network (enable if network is open or off)**:  OFF

**Auto join (automatically join this wireless network)**:  ON

**Security type**: None

**Proxy server settings**

**Proxy configuration**: None

**Policy Settings**

**Remove policy**:  Select date  Duration until removal (in days)

**Allow user to remove policy**: Always

**Profile scope**: User OS X 10.7+

**Deployment Rules**

[Back](#) [Next >](#)

次の設定を構成します。

- **Network type** : 一覧から、 [Standard]、 [Legacy Hotspot]、または [Hotspot 2.0] を選択して、使用する予定のネットワークの種類を設定します。
- **Network Name** : デバイスの使用可能なネットワークの一覧に表示されるSSIDを入力します。Hotspot 2.0には適用されません。
- **Hidden network (enable if network is open or off)** : ネットワークを隠しネットワークにするかどうかを選択します。
- **Auto join (automatically join this wireless network)** : ネットワークに自動的に参加するかどうかを選択します。デフォルトは [ON] です。
- **Security type** : 一覧から、使用する予定のセキュリティの種類を選択します。Hotspot 2.0には適用されません。
  - None - そのほかの構成は不要です。
  - WEP
  - WPA/WPA2パーソナル
  - 任意 (パーソナル)
  - WEPエンタープライズ
  - WPA/WPA2エンタープライズ
  - Any (Enterprise)

以下では、上記の接続の種類ごとに、構成するオプションを示します。

WPA、WPA Personal、WPA 2 Personal、Any (Personal)

WEP Enterprise、WPA Enterprise、WPA2 Enterprise、Any (Enterprise)

- **Use as a Login Window configuration** : ユーザーの認証に、ログインウィンドウで入力したものと同一資格情報を使用するかどうかを選択します。
- **プロキシサーバーの設定**
  - **Proxy configuration** : 一覧から、 [None]、 [Manual]、または [Automatic] を選択してVPN接続のプロキシサーバーのルーティング方法を設定し、そのほかのオプションを構成します。デフォルト設定は [None] で、そのほかの構成は不要です。
  - **[Manual]** を選択した場合は、次の設定を構成します。
    - **Hostname/IP address** : プロキシサーバーのホスト名またはIPアドレスを入力します。
    - **Port** : プロキシサーバーのポート番号を入力します。
    - **Username** : 任意で、プロキシサーバーへの認証に使用するユーザー名を入力します。
    - **Password** : 任意で、プロキシサーバーへの認証に使用するパスワードを入力します。
  - **[Automatic]** を選択した場合は、次の設定を構成します。
    - **Server URL** : プロキシ構成を定義するPACファイルのURLを入力します。
    - **Allow direct connection if PAC is unreachable** : PACファイルに到達できない場合、ユーザーが直接宛先に接続できるようにするかどうかを選択します。デフォルトは [ON] です。このオプションはiOS 7.0以降でのみ使用できます。
- **ポリシー設定**
  - **[Remove policy]** の横にある **[Select date]** または **[Duration until removal (in days)]** をクリックします。
  - **[Select date]** をクリックした場合、カレンダーをクリックして削除を実行する特定の日付を選択します。
  - **[Allow user to remove policy]** の一覧で、 **[Always]**、 **[Password required]**、 **[Never]** のいずれかを選択します。

- [Password required] を選択した場合、[Removal password] の横に必要なパスワードを入力します。
- [Profile scope] の横にある、[User] または [System] を選択します。デフォルトは [User] です。このオプションはOS X 10.7以降でのみ使用できます。

The screenshot shows the XenMobile 'Configure' interface for a 'WiFi Policy'. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows a tree view with 'WiFi Policy' selected, containing sections for '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, Mac OS X, Android (highlighted), Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE. The main configuration area is titled 'WiFi Policy' and includes a description: 'This policy lets you configure a WiFi profile for devices.' It contains the following fields:
 

- Network name\***: A text input field with a help icon.
- Authentication**: A dropdown menu set to 'Open'.
- Encryption**: A dropdown menu set to 'WEP'.
- Password\***: A text input field.
- Hidden network (enable if network is open or off)**: A toggle switch set to 'OFF'.

 Below these fields is a section for 'Deployment Rules'. At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

- **Network name** : ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Authentication** : 一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - オープン
  - 共有
  - WPA
  - WPA-PSK
  - WPA2
  - WPA2-PSK
  - 802.1x EAP

以下では、上記の接続の種類ごとに、構成するオプションを示します。

Open, Shared

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

- **Hidden network (Enable if network is open or off)** : ネットワークを隠しネットワークにするかどうかを選択します。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

1 Policy Info	
2 Platforms	
<input type="checkbox"/> iOS	
<input type="checkbox"/> Mac OS X	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input type="checkbox"/> Windows Mobile/CE	
3 Assignment	

**Network name\***  ⓘ

**Authentication**

**Encryption**

**EAP Type**

**Connect if hidden**  OFF

**Connect automatically**  ON

**Push certificate via SCEP**  ON

**Credential provider for SCEP\***

**Proxy server settings**

**Host name or IP address**

**Port**

次の設定を構成します。

- **Network name** : ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Authentication** : 一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPA-2 Enterprise : Windows 10の最新リリースでWPA-2 Enterpriseを使用するには、SCEPを構成する必要があります。これによって、XenMobileは証明書をデバイスに送信し、WiFiサーバーに認証できます。SCEPを構成するには、[Settings] > [Credential Providers] の [Distribution] ページに移動します。詳しくは、「[資格情報プロバイダー](#)」を参照してください。

以下では、上記の接続の種類ごとに、構成するオプションを示します。

オープン

WPA Personal、WPA-2 Personal

WPA-2エンタープライズ

- **プロキシサーバーの設定**
  - **Host name or IP address** : プロキシサーバーの名前またはIPアドレスを入力します。
  - **Port** : プロキシサーバーのポート番号を入力します。

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

1 Policy Info	OS version* 10
2 Platforms	Network name* WiFi_24G
<input type="checkbox"/> iOS	Authentication WPA-2 Enterprise
<input type="checkbox"/> Mac OS X	Encryption AES
<input type="checkbox"/> Android	EAP Type PEAP-MSCHAPv2
<input checked="" type="checkbox"/> Windows Phone	Hidden network (enable if network is open or off) OFF
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Connect automatically ON
<input type="checkbox"/> Windows Mobile/CE	Enable SCEP? ON
3 Assignment	Credential provider for SCEP* certsrv-cpwifi
	Proxy server settings
	Host name or IP address
	Port

次の設定を構成します。

- OS version : 一覧から、Windows 8.1の場合は [8.1] を、Windows 10の場合は [10] を選択します。デフォルトは10です。

## Windows 10の設定

- Authentication : 一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPAエンタープライズ
  - WPA-2 Enterprise : Windows 10の最新リリースでWPA-2 Enterpriseを使用するには、SCEPを構成する必要があります。これによって、XenMobileは証明書をデバイスに送信し、WiFiサーバーに認証できます。SCEPを構成するには、[Settings] > [Credential Providers] の [Distribution] ページに移動します。詳しくは、「資格情報プロバイダー」を参照してください。

以下では、上記の接続の種類ごとに、構成するオプションを示します。

オープン

WPA Personal, WPA-2 Personal

WPA-2エンタープライズ

## Windows 8.1設定

- Network name : ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- Authentication : 一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPAパーソナル
  - WPA-2パーソナル
  - WPAエンタープライズ
  - WPA-2エンタープライズ
- Hidden network (Enable if network is open or off) : ネットワークを隠しネットワークにするかどうかを選択します。
- Connect automatically : ネットワークに自動的に接続するかどうかを選択します。



XenMobile Analyze Manage Configure admin

Device Policies Apps Actions ShareFile Enrollment Profiles Delivery Groups

### WiFi Policy

This policy lets you configure a WiFi profile for devices.

**1 Policy Info**

**2 Platforms**

- iOS
- Mac OS X
- Android
- Windows Phone
- Windows Desktop/Tablet
- Windows Mobile/CE

**3 Assignment**

**WiFi Policy**

Network name\*

Device-to-device connection (ad-hoc)  OFF

Network

Authentication

Encryption

Key provided (automatic)  OFF

Password

Key index

► Deployment Rules

Back Next >

次の設定を構成します。

- **Network name** : ユーザーのデバイスで使用可能なネットワークの一覧に表示されるSSIDを入力します。
- **Device-to-device connection (ad-hoc)** : 2つのデバイスを直接接続できます。デフォルトは [Off] です。
- **Network** : デバイスを外部インターネットソースに接続するか、オフィスのイントラネットに接続するかを選択します。
- **Authentication** : 一覧から、このWiFi接続で使用するセキュリティの種類を選択します。
  - オープン
  - WPA/パーソナル
  - WPA-2/パーソナル
  - WPA-2エンタープライズ

以下では、上記の接続の種類ごとに、構成するオプションを示します。

#### オープン

WPA Personal、WPA-2 Personal

#### WPA-2エンタープライズ

- **Key provided (automatic)** : キーが自動的に指定されるかどうかを選択します。デフォルトは [Off] です。
- **Password** : このフィールドにパスワードを入力します。
- **Key index** : キーインデックスを表示します。使用可能なオプションは、1、2、3、4です。

#### 7. 展開規則を構成します。

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

The screenshot shows the XenMobile configuration interface for a WiFi Policy. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation menu has 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The left sidebar shows the 'WiFi Policy' configuration steps: 1 Policy Info, 2 Platforms, and 3 Assignment (highlighted). The main content area is titled 'WiFi Policy' and includes a description: 'This policy lets you configure a WiFi profile for devices.' Below this, there are two sections: 'Choose delivery groups' and 'Delivery groups to receive app assignment'. The 'Choose delivery groups' section has a search bar and a list of groups: 'AllUsers' (checked), 'DG-ex12', and 'DG-Testprise'. The 'Delivery groups to receive app assignment' section shows 'AllUsers' selected. Below these sections is the 'Deployment Schedule' section, which is currently collapsed. At the bottom right, there are 'Back' and 'Save' buttons.

9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが[Delivery groups to receive app assignment] 一覧に表示されます。

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

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

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

11. [Save] をクリックします。

# Windows CE証明書デバイスポリシー

Apr 27, 2017

XenMobileでは、外部のPKIを基にWindows Mobile/CE証明書を作成し、ユーザーのデバイスに配布するデバイスポリシーを作成できます。証明書およびPKIエンティティについては、「[証明書](#)」を参照してください。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[Security] の下の [Windows CE Certificate] をクリックします。[Windows CE Certificate Policy] 情報ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Windows CE Certificate Policy' and 'Policy Information'. It contains a description: 'This configuration allows you to create and deliver a certificate from an External PKI to your device.' There are two input fields: 'Policy Name\*' and 'Description'. A 'Next >' button is located in the bottom right corner.

4. [Policy Information] ペインで、以下の情報を入力します。
  - Policy Name : ポリシーの説明的な名前を入力します。
  - Description : 任意で、ポリシーの説明を入力します。
5. [Next] をクリックします。[Windows CE Certificate Policy Platform] 情報ページが開きます。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The left sidebar shows a tree view with 'Windows CE Certificate Policy' selected. The main content area is titled 'Policy Information' and contains the following fields:

- Credential Provider\***: A dropdown menu with 'None' selected.
- Password of generated PKCS#12\***: A text input field.
- Destination folder**: A dropdown menu with '%My Documents%' selected.
- Destination file name\***: A text input field with a help icon (?) to its right.

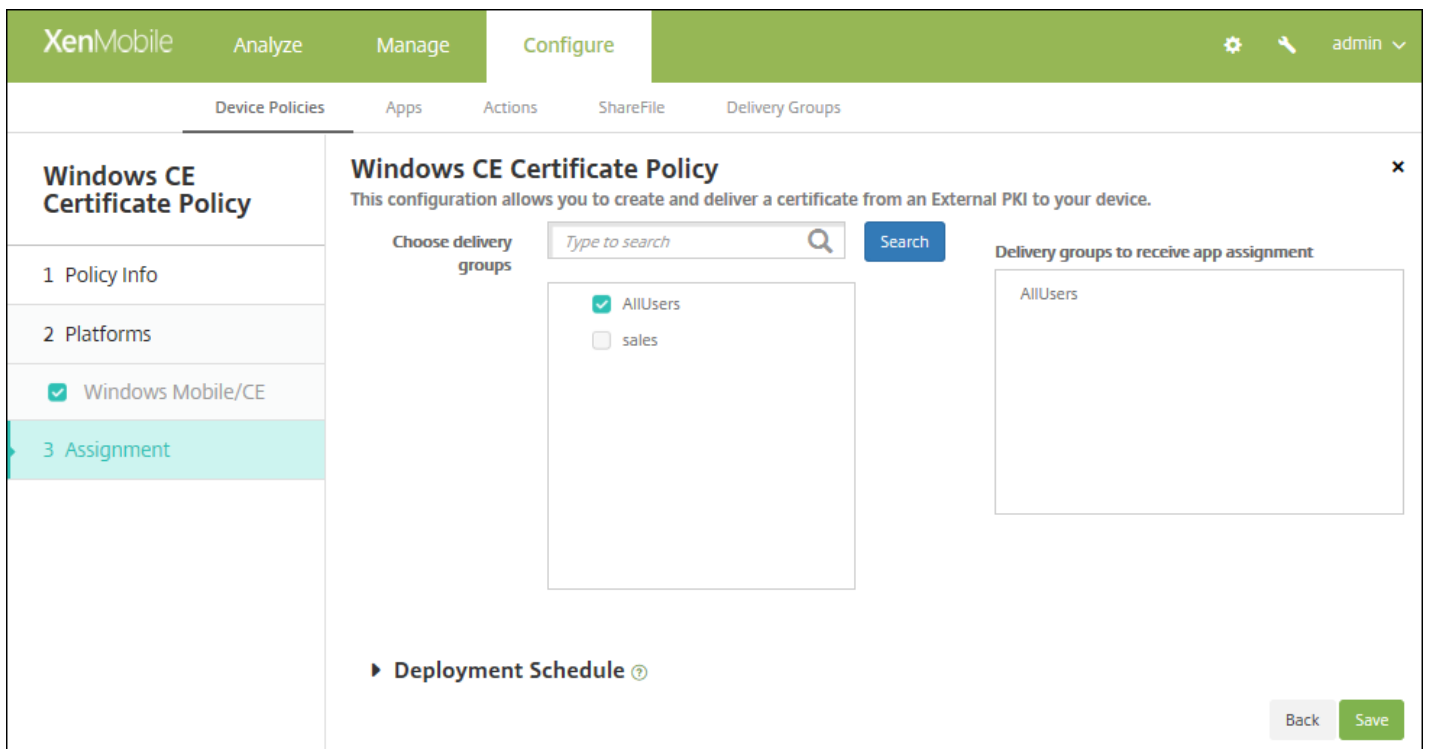
Below these fields is a section for 'Deployment Rules'. At the bottom right of the main area are 'Back' and 'Next >' buttons.

6. 次の設定を構成します。

- **Credential provider** : ボックスの一覧で、資格情報プロバイダーを選択します。デフォルトは [None] です。
- **Password of generated PKCS#12** : 資格情報の暗号化に使用するパスワードを入力します。
- **Destination folder** : 一覧から資格情報の宛先フォルダーを選択するか、 [Add new] をクリックして、一覧に表示されていないフォルダーを追加します。事前定義済みのオプションは以下のとおりです。
  - %Flash Storage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %My Documents%\
  - %Windows%\
- **Destination file name** : 資格情報ファイルの名前を入力します。

7. 展開規則を構成します。

8. [Next] をクリックします。 [Windows CE Certificate Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

10. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[常時接続に対する展開] は適用されません。

11. [保存] をクリックします。

# XenMobile Storeデバイスポリシー

Apr 27, 2017

XenMobileでポリシーを作成して、iOS、Android、またはWindowsタブレットデバイスのホーム画面でXenMobile StoreのWebクリップを表示するかどうかを指定できます。

1. XenMobileコンソールで、[Configure] の [Device Policies] をクリックします。[Device Policies] ページが開きます。
2. [Add] をクリックします。[Add a New Policy] ダイアログボックスが開きます。
3. [More] を展開した後、[Apps] の下の [Store] をクリックします。[Store Policy] ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The main content area is titled 'Store Policy' and contains a sidebar with three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '1 Policy Info' section is active, showing a 'Policy Information' dialog box. This dialog box has a title bar with a close button (X) and a subtitle: 'This policy specifies when devices display a Store webclip on the devices.' It contains two input fields: 'Policy Name\*' (a text box) and 'Description' (a larger text area).

4. [Policy Information] ペインで、以下の情報を入力します。

- Policy Name : ポリシーの説明的な名前を入力します。
- Description : 必要に応じて、ポリシーの説明を入力します。

5. [Next] をクリックします。[Platforms] ページが開きます。

The screenshot shows the XenMobile console interface, similar to the previous one. The 'Store Policy' sidebar is still visible. The '2 Platforms' section is now active, showing a 'Store Policy' dialog box. This dialog box has a title bar with a close button (X) and a subtitle: 'This policy specifies when devices display a Store webclip on the devices.' It contains a toggle switch for 'iOS' which is currently turned 'ON'. Below this, there is a section titled 'Deployment Rules' with a right-pointing arrow.

6. [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

7. 構成するプラットフォームごとに、ユーザーデバイスにXenMobile Store Webクリップを表示するかどうかを選択します。デフォルトは [ON] です。

各プラットフォームの構成が完了したら、手順8を参照してプラットフォームの展開規則を設定します。

#### 8. 展開規則を構成します。

9. [Next] をクリックします。[XenMobile Store Policy] 割り当てページが表示されます。

10. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の [Delivery groups to receive app assignment] の一覧に表示されます。

11. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、[Settings] > [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[Deploy for always on connection] は適用されません。

12. [Save] をクリックします。

# XenMobileオプションデバイスポリシー

Apr 27, 2017

XenMobileオプションポリシーを追加して、AndroidデバイスおよびWindows Mobile/CEデバイスからXenMobileに接続するときのSecure Hubの動作を構成します。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** をクリックした後、**[XenMobile agent]** の下の **[XenMobile Options]** をクリックします。**[XenMobileオプションポリシー]** ページが開きます。

The screenshot shows the XenMobile console interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'XenMobile Options Policy' and contains a 'Policy Information' section. This section has a description: 'This policy lets you configure parameters for connections to XenMobile.' There are two input fields: 'Policy Name\*' and 'Description'. The 'Policy Name\*' field is empty. The 'Description' field is also empty. On the left side, there is a sidebar with 'XenMobile Options Policy' and three sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', there are two checkboxes: 'Android' and 'Windows Mobile/CE', both of which are checked. At the bottom right, there is a green 'Next >' button.

4. **[Policy Information]** ペインで、以下の情報を入力します。
  - **Policy Name** : ポリシーの説明的な名前を入力します。
  - **Description** : 任意で、ポリシーの説明を入力します。
5. **[Next]** をクリックします。**[Policy Platforms]** ページが開きます。
6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。



XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

**Device agent configuration**

Traybar notification - hide traybar icon  OFF

Connection time-out(s)\*

Keep-alive interval(s)\*

**Remote support**

Prompt the user before allowing remote control  OFF

Before a file transfer

► Deployment Rules

Back Next >

次の設定を構成します。

- **Traybar notification - hide traybar icon** : トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは [OFF] です。
- **Connection: time-out(s)** : 接続のアイドル状態を継続できる時間 (秒) を入力します。この時間を超えると、接続はタイムアウトになります。デフォルトは20秒です。
- **Keep-alive interval(s)** : 接続を開いたままにする時間 (秒) を入力します。デフォルトは120秒です。
- **Prompt the user before allowing remote control** : Remote Supportの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは [OFF] です。
- **Before a file transfer** : 一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。使用可能な値は、**使用可能な値は**、 [Do not warn the user] 、 [Warn the user] 、および [Ask for user permission] です。デフォルトは [Do not warn the user] です。

The screenshot displays the 'XenMobile Options Policy' configuration interface. The left-hand navigation pane is titled 'XenMobile Options Policy' and contains three main sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', both 'Android' and 'Windows Mobile/CE' are selected with checkmarks. The main content area is titled 'XenMobile Options Policy' and includes a sub-header: 'This policy lets you configure parameters for connections to XenMobile.' Below this, there are three sections of settings:

- Device agent configuration:**
  - XenMobile backup configuration: Disabled (dropdown menu)
  - Connect to the office network: ON (toggle)
  - Connect to the Internet network: ON (toggle)
  - Connect to the built-in office network: ON (toggle)
  - Connect to the built-in Internet network: ON (toggle)
  - Traybar notification - hide traybar icon: OFF (toggle)
  - Connection time-out(s)\*: 20 (input field)
  - Keep-alive interval(s)\*: 120 (input field)
- Remote support:**
  - Prompt the user before allowing remote control: OFF (toggle)
  - Before a file transfer: Do not warn the user (dropdown menu)
- Deployment Rules:** (indicated by a right-pointing arrow)

At the bottom right of the configuration area, there are 'Back' and 'Next >' buttons.

次の設定を構成します。

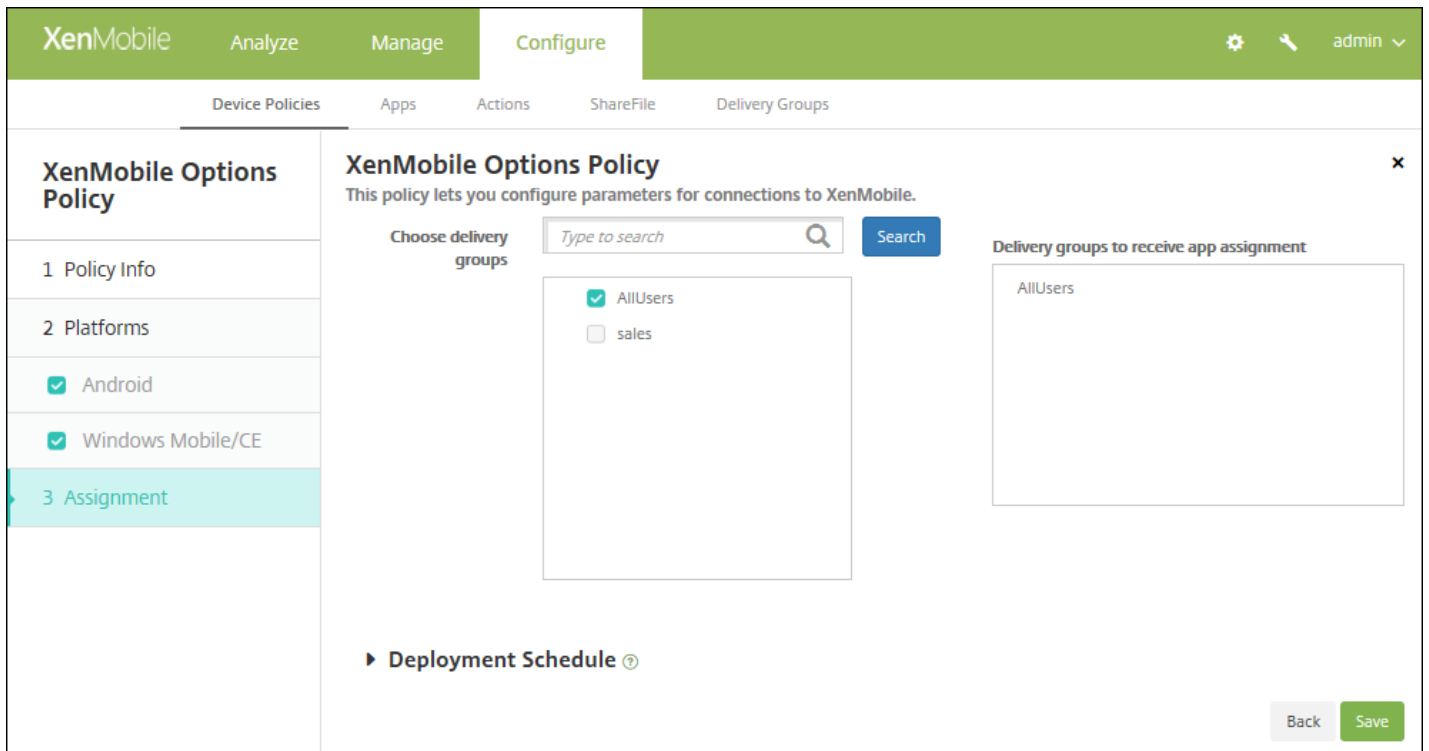
- **デバイス エージェント構成**

- **XenMobile backup configuration** : 一覧から、ユーザーのデバイスにXenMobileの構成をバックアップするためのオプションを選択します。デフォルトは **[Disabled]** です。選択できるオプションは以下のとおりです。
  - 無効
  - XenMobileインストール後の初回接続時
  - 各デバイスの再起動後の初回接続時
- **オフィス ネットワークに接続**
- **インターネット ネットワークに接続**
- **Connect to the built-in office network** : **[ON]** に設定した場合、XenMobileによりネットワークが自動的に検出されます。
- **Connect to the built-in Internet network** : **[ON]** に設定した場合、XenMobileによりネットワークが自動的に検出されます。
- **Traybar notification - hide traybar icon** : トレイバーアイコンを非表示にするか表示するかを選択します。デフォルトは **[OFF]** です。
- **Connection time-out(s)** : 接続のアイドル状態を継続できる時間 (秒) を入力します。この時間を超えると、接続はタイムアウトになります。デフォルトは20秒です。
- **Keep-alive interval(s)** : 接続を開いたままにする時間 (秒) を入力します。デフォルトは120秒です。

- リモート サポート
  - **Prompt the user before allowing remote control** : Remote Supportの制御を許可する前にユーザーに確認メッセージを表示するかどうかを選択します。デフォルトは [OFF] です。
  - **Before a file transfer** : 一覧から、ファイル転送についてユーザーに対して警告を表示するか、ユーザーの許可を求めるかを選択します。使用可能な値は、**使用可能な値は**、 [Do not warn the user] 、 [Warn the user] 、および [Ask for user permission] です。デフォルトは [Do not warn the user] です。

## 7. 展開規則を構成します。

8. [Next] をクリックします。 [XenMobile Options Policy] 割り当てページが開きます。



9. [Choose delivery groups] の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが [Delivery groups to receive app assignment] 一覧に表示されます。

10. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、 [OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。 [OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[Deploy for always on connection] は適用されません。

11. [Save] をクリックします。

# XenMobileアンインストールデバイスポリシー

Apr 27, 2017

XenMobileでデバイスポリシーを追加して、XenMobileをAndroidデバイスおよびWindows Mobile/CEデバイスからアンインストールすることができます。このポリシーを展開すると、展開グループ内のすべてのデバイスからXenMobileが削除されます。

1. XenMobileコンソールで、**[Configure]** の **[Device Policies]** をクリックします。**[Device Policies]** ページが開きます。
2. **[Add]** をクリックします。**[Add a New Policy]** ダイアログボックスが開きます。
3. **[More]** を展開した後、**[XenMobile agent]** の下の **[XenMobile Uninstall]** をクリックします。**[XenMobile Uninstall Policy]** ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there are tabs for 'Analyze', 'Manage', and 'Configure'. The 'Configure' tab is active. Below the tabs, there are sub-tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The 'Device Policies' sub-tab is selected. The main content area is titled 'XenMobile Uninstall Policy' and contains a 'Policy Information' section. The description reads: 'This policy lets you choose to uninstall XenMobile on Android, Windows Mobile, and Windows CE devices upon deployment of the policy.' There are two input fields: 'Policy Name\*' and 'Description'. The 'Platforms' section shows 'Android' and 'Windows Mobile/CE' checked. The 'Assignment' section is partially visible. A 'Next >' button is located at the bottom right of the main content area.

4. **[Policy Information]** ペインで、以下の情報を入力します。

- **Policy Name** : ポリシーの説明的な名前を入力します。
- **Description** : 任意で、ポリシーの説明を入力します。

5. **[Next]** をクリックします。**[Policy Platforms]** 情報ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順7を参照してプラットフォームの展開規則を設定します。

AndroidおよびWindows Mobile/CEの設定の構成

選択したプラットフォームごとに、次の設定を構成します。

- **Uninstall XenMobile from devices** : このポリシーを展開するすべてのデバイスからXenMobileをアンインストールするかどうかを選択します。デフォルトは **[OFF]** です。

7. 展開規則を構成します。

8. **[Next]** をクリックします。 **[XenMobile Uninstall Policy]** 割り当てページが開きます。

9. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが **[Delivery groups to receive app assignment]** 一覧に表示されます。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

- このオプションは、**[Settings] > [Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]** は適用されません。

11. **[Save]** をクリックします。

# アプリケーションの追加

Apr 27, 2017

アプリケーションをXenMobileに追加して管理します。アプリケーションはXenMobileコンソールに追加します。このコンソールでは、アプリケーションをカテゴリ別に分類し、ユーザーに展開することができます。

以下の種類のアプリケーションをXenMobileに追加できます。

- **MDX**。MDX Toolkitでラップされたアプリケーション（および関連付けられたポリシー）です。内部ストアおよび公開ストアから取得したMDXアプリケーションを展開します。
- **パブリックアプリケーションストア**。これらのアプリケーションには、iTunesやGoogle Playなどのパブリックアプリケーションストアで無料または有料で提供されているアプリケーションが含まれます。たとえば、GoToMeetingです。
- **WebおよびSaaS**。これらのアプリケーションには、内部ネットワークからアクセスされるアプリケーション（Webアプリケーション）やパブリックネットワーク経由でアクセスされるアプリケーション（SaaS）が含まれます。独自のアプリケーションを作成するか、一連のアプリケーションコネクタの中から選択して、既存のWebアプリケーションのシングルサインオン認証に使用することができます。たとえば、GoogleApps\_SAMLです。
- **エンタープライズ**。これらのアプリケーションは、MDX Toolkitでラップされておらず、MDXアプリケーションに関連付けられたポリシーを含んでいない、ネイティブアプリケーションです。
- **Webリンク**。パブリックサイトやプライベートサイト、またはシングルサインオンを必要としないWebアプリケーションのWebアドレス (URL) です。

## 注意

iOSおよびSamsung Androidアプリのサイレントインストールがサポートされます。サイレントインストールとは、ユーザーはデバイスに展開するアプリのインストールを求められず、アプリがバックグラウンドで自動的にインストールされることを意味します。サイレントインストールを実装するには、以下の前提条件を満たす必要があります。

- iOSアプリの場合、管理されているiOSデバイスがSupervisedモードである必要があります。詳しくは、[iOSおよびMac OS Xプロファイルのインポートデバイスポリシー](#)を参照してください。
- Androidアプリの場合、Samsung for Enterprise (SAFE) またはKNOXポリシーがデバイスで有効になっている必要があります。このためには、Samsung MDMライセンスキーデバイスポリシーを設定して、Samsung ELMおよびKNOXライセンスキーを生成します。詳しくは、「[Samsung MDMライセンスキーデバイスポリシー](#)」を参照してください。

## モバイルおよびMDXアプリケーションのしくみ

XenMobileでは、Secure Hub、Secure Mail、Secure WebなどのXenMobile Appsを含むiOS、Mac OS X、Android、およびWindowsアプリケーションと、MDXポリシーの使用がサポートされます。XenMobileコンソールを使用し、アプリケーションをアップロードしてユーザーデバイスに配信できます。XenMobileアプリケーションに加えて、次の種類のアプリケーションを追加できます。

- 自社開発のカスタムアプリケーション。
- MDXポリシーを使ってデバイスの機能を許可または制限するアプリケーション。

XenMobile Apps for iOSおよびAndroidを配布するには、CitrixからパブリックストアMDXファイルをダウンロードし、これらのファイルをXenMobileコンソールにアップロードし（**[Configure] > [Apps]**）、必要に応じてMDXポリシーを更新してから、MDXファイルをパブリックアプリケーションストアにアップロードします。詳しくは、このトピックの「[MDXアプリケーションの追加](#)」を参照してください。



XenMobile Apps for Windowsを配布するには、Citrixからアプリファイルをダウンロードし、MDX Toolkitでラッピングしてから、XenMobileコンソールにアップロードします。必要に応じてMDXポリシーを変更して、デリバリーグループ経由でユーザーデバイスにアプリを配信します。詳しくは、XenMobileアプリドキュメントの「[Public App Store Delivery of XenMobile Apps](#)」を参照してください。

Citrixは、CitrixのロジックおよびポリシーでiOS、Mac OS X、Android、およびWindowsデバイス用のアプリケーションをラップするためのMDX Toolkitを提供しています。このツールは、組織内で作成されたアプリケーションまたは社外で作成されたアプリケーションに安全に対処できます。

### WebおよびSaaSアプリケーションのしくみ

XenMobileには、一連のアプリケーションコネクタが用意されています。これらは、WebアプリケーションおよびSaaS（Software as a Service：サービスとしてのソフトウェア）アプリケーションのSSO（Single Sign-On：シングルサインオン）を構成するためのテンプレートで、ユーザーアカウントを作成したり管理したりすることもできます。XenMobileには、Security Assertion Markup Language（SAML）コネクタが含まれています。SAMLコネクタは、SSOおよびユーザーアカウント管理用のSAMLプロトコルをサポートするWebアプリケーションで使用されます。XenMobileは、SAML 1.1およびSAML 2.0をサポートします。

また、独自のエンタープライズSAMLコネクタを構築することもできます。

詳しくは、「[WebおよびSaaSアプリケーションの追加](#)」を参照してください。

### エンタープライズアプリケーションのしくみ

エンタープライズアプリケーションは、通常は内部ネットワークに存在します。ユーザーはSecure Hubを使ってそのアプリケーションに接続できます。エンタープライズアプリケーションを追加すると、XenMobileはそのアプリケーションコネクタを作成します。詳しくは、この記事の「[エンタープライズアプリケーションの追加](#)」を参照してください。

### パブリックアプリケーションストアのしくみ

Apple App Store、Google Play、およびWindows Storeからアプリケーションの名前と説明を取得するための設定を構成できます。ストアからアプリケーション情報を取得すると、XenMobileにより既存の名前と説明が上書きされます。詳しくは、この記事の「[パブリックアプリケーションストアのアプリケーションの追加](#)」を参照してください。

### Webリンクのしくみ

WebリンクはインターネットサイトまたはイントラネットサイトのWebアドレスです。Webリンクは、SSOを必要としないWebアプリケーションも参照できます。Webリンクの構成が完了すると、リンクはXenMobile Storeにアイコンとして表示されます。ユーザーがSecure Hubを使ってログオンすると、リンクは使用可能なアプリケーションおよびデスクトップの一覧と共に表示されます。詳しくは、この記事の「[Webリンクアプリケーションの追加](#)」を参照してください。

## MDXアプリケーションの追加

iOS、Android、またはWindows Phoneデバイス用のラップされたMDXモバイルアプリケーションを取得したら、そのアプリケーションをXenMobileにアップロードできます。アプリケーションをアップロードした後、アプリケーションの詳細とポリシー設定を構成できます。各デバイスプラットフォームの種類で利用できるアプリケーションポリシーについて詳しくは、「[MDX Policies at a Glance](#)」を参照してください。このトピックでは、ポリシーの詳細についても説明しています。

1. XenMobileコンソールで、**[Configure]** の **[Apps]** をクリックします。**[Apps]** ページが開きます。

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

**Apps** Show filter

Add | Category | Export

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM		
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM		
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM		
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM		
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM		
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM		
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM		
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM		
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM		

2. [Add] をクリックします。[Add App] ダイアログボックスが開きます。

### Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

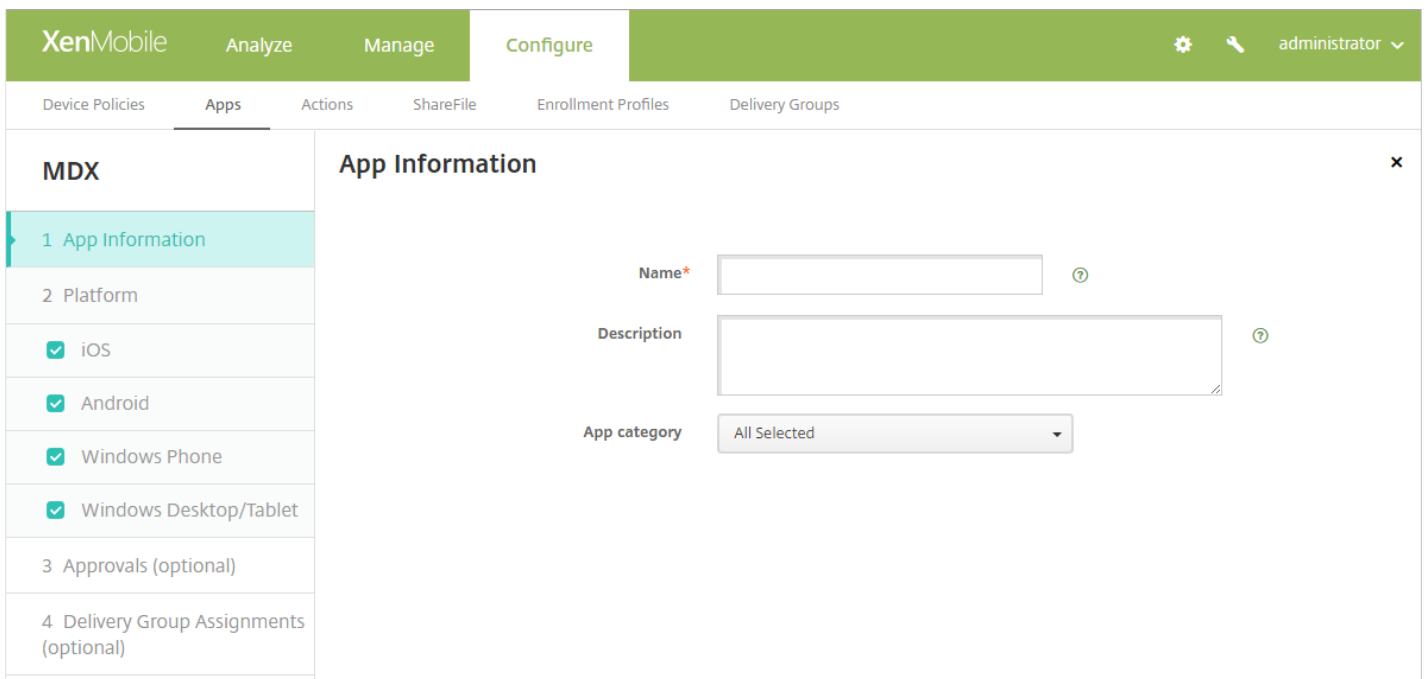
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. [MDX] をクリックします。[MDX App Information] ページが開きます。



4. **[App Information]** ペインで、以下の情報を入力します。

- **Name** : アプリケーションの説明的な名前を入力します。この情報は、[アプリ] の表の [アプリ名] の下に表示されます。
- **Description** : 任意で、アプリケーションの説明を入力します。
- **App category** : 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリケーションカテゴリについては、「[アプリケーションカテゴリの作成](#)」を参照してください。

5. **[Next]** をクリックします。 **[App Platforms]** ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順11を参照してプラットフォームの展開規則を設定します。

7. **[Upload]** をクリックしてアップロードする.mdxファイルの場所へ移動し、そのファイルを選択します。

- iOS VPP B2Bアプリケーションを追加する場合は、 **[Your application is a VPP B2B application?]** をクリックして、

8. **[Next]** をクリックします。アプリケーション詳細ページが開きます。

9. 次の設定を構成します。

- **File name** : アプリケーションに関連付けられているファイル名を入力します。
- **App Description** : アプリケーションの説明を入力します。
- **App version** : 任意で、アプリケーションのバージョン番号を入力します。
- **Minimum OS version** : 任意で、アプリケーションを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。
- **Maximum OS version** : 任意で、アプリケーションを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
- **Excluded devices** : 任意で、アプリケーションを実行できないデバイスの製造元またはモデルを入力します。

- **Remove app if MDM profile is removed** : MDMプロファイルが削除された場合にデバイスからアプリケーションを削除するかどうかを選択します。デフォルトは **[ON]** です。
- **Prevent app data backup** : ユーザーがアプリケーションデータをバックアップできないようにするかどうかを選択します。デフォルトは **[ON]** です。
- **Force app to be managed** : アプリケーションが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリケーションの管理を許可するように求めるかどうかを選択します。デフォルトは **[ON]** です。iOS 9.0以降で利用できます。

10. **MDX Policies** を構成します。MDXポリシーはプラットフォームによって異なり、認証、デバイスセキュリティ、ネットワーク要件、その他アクセス、暗号化、アプリケーション相互作用、アプリケーション制限、アプリケーションネットワークアクセス、アプリケーションログ、アプリケーションジオフェンスなどのポリシー領域で適用するオプションが含まれます。XenMobileコンソールでは、ポリシーごとに、ポリシーを説明するヒントが提供されます。ポリシーが適用されるプラットフォームの種類を示す表など、MDXアプリケーションのアプリケーションポリシーについて詳しくは、「[MDX Policies at a Glance](#)」を参照してください。

11. 展開規則を構成します。

12. **[XenMobile Store Configuration]** を展開します。

**▼ Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File	Choose File	Choose File	Choose File
Choose File			

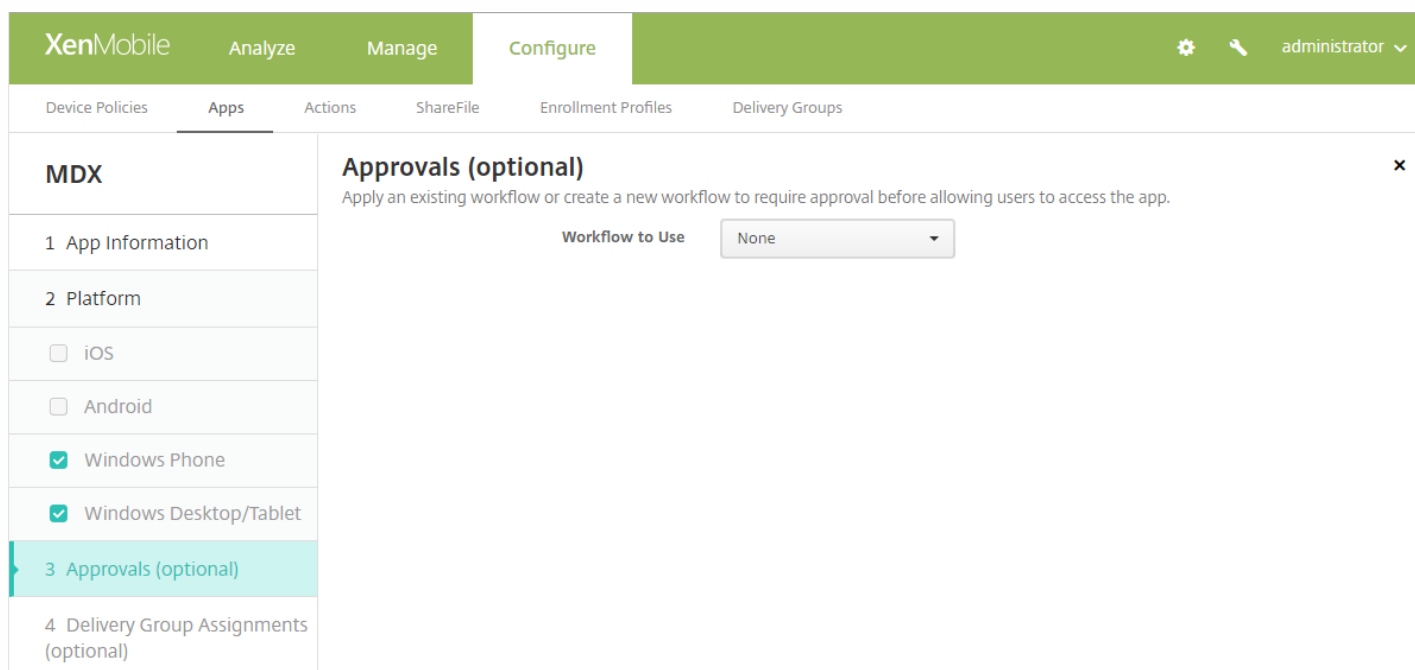
Allow app ratings

Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかを設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは[ON]です。
  - **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [ON] です。

13. [Next] をクリックします。[Approvals] ページが開きます。



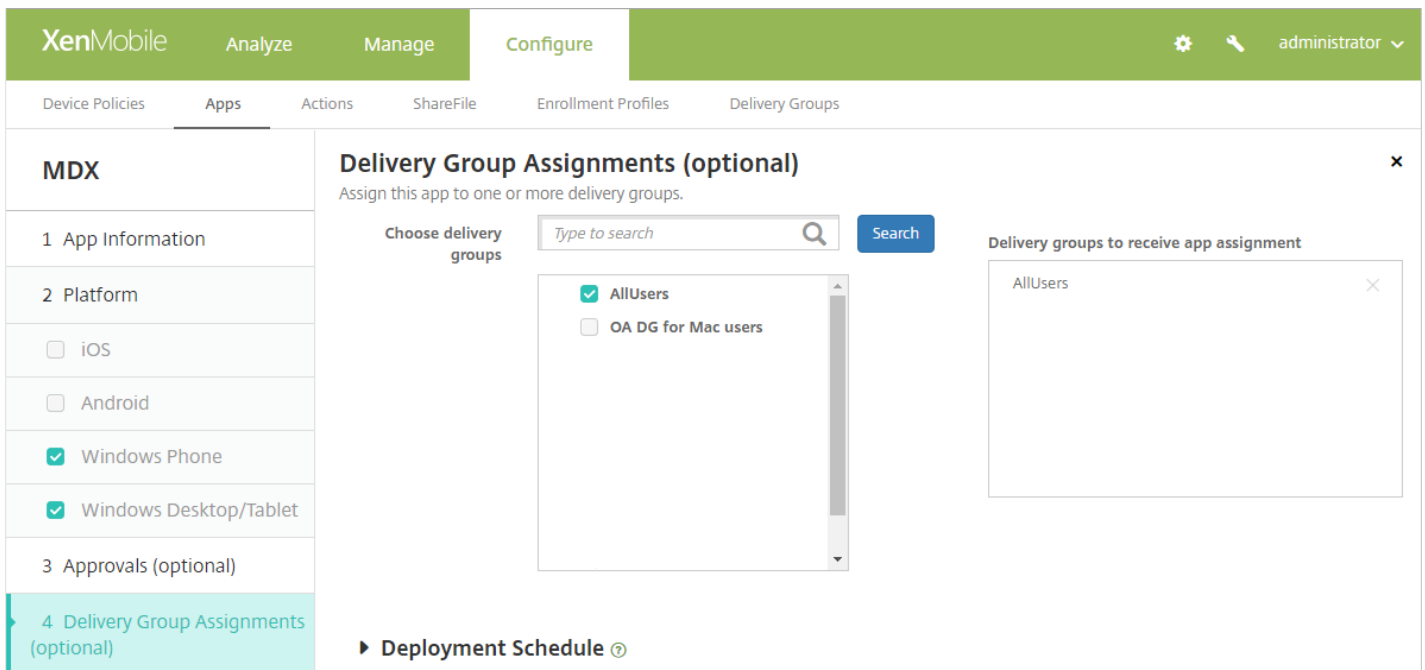
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順15に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use** : 一覧から既存のワークフローを選択するか、[Create a new workflow] をクリックします。デフォルトは [None] です。
- [Create a new workflow] を選択した場合は、次の設定を構成します。
  - **Name** : ワークフローの固有の名前を入力します。
  - **Description** : 任意で、ワークフローの説明を入力します。
  - **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval** : 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは [1 level] です。選択できるオプションは以下のとおりです。
    - Not Needed

- 1 level
- 2 levels
- 3 levels
- **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
- **Find additional required approvers** : 検索フィールドに、追加で必要なユーザーの名前を入力して、[Search] をクリックします。名前はActive Directoryで取得されます。
- ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが [Selected additional required approvers] の一覧に表示されます。
  - [Selected additional required approvers] の一覧からユーザーを削除するには、次のいずれかを行います。
    - [Search] をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して [Search] をクリックし、検索結果を絞り込みます。
    - [Selected additional required approvers] の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

14. [Next] をクリックします。[Delivery Group Assignment] ページが開きます。



15. オプションとして、[Delivery Groups Assignment] ページの [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。

16. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[Deploy for **always on connection**] は適用されません。

17. [Save] をクリックします。

## アプリケーションカテゴリの作成

ユーザーがSecure Hubにログオンすると、XenMobileで追加および設定したアプリケーション、Webリンク、ストアの一覧が表示されます。管理者がアプリケーションカテゴリを使用することにより、ユーザーは指定されたアプリケーション、ストア、またはWebリンクだけにアクセスできます。たとえば、「Finance」カテゴリを作成して財務関連のアプリケーションを追加したり、「Sales」カテゴリを構成して営業関連のアプリケーションを追加したりすることができます。

XenMobileコンソールの [Apps] ページで、カテゴリを構成します。次に、アプリケーション、Webリンク、ストアを追加または編集するとき、構成した1つまたは複数のカテゴリにアプリケーションを追加できます。

1. XenMobileコンソールで、[Configure] の [Apps] をクリックします。[Apps] ページが開きます。
2. [Category] をクリックします。[Categories] ダイアログボックスが開きます。

Categories

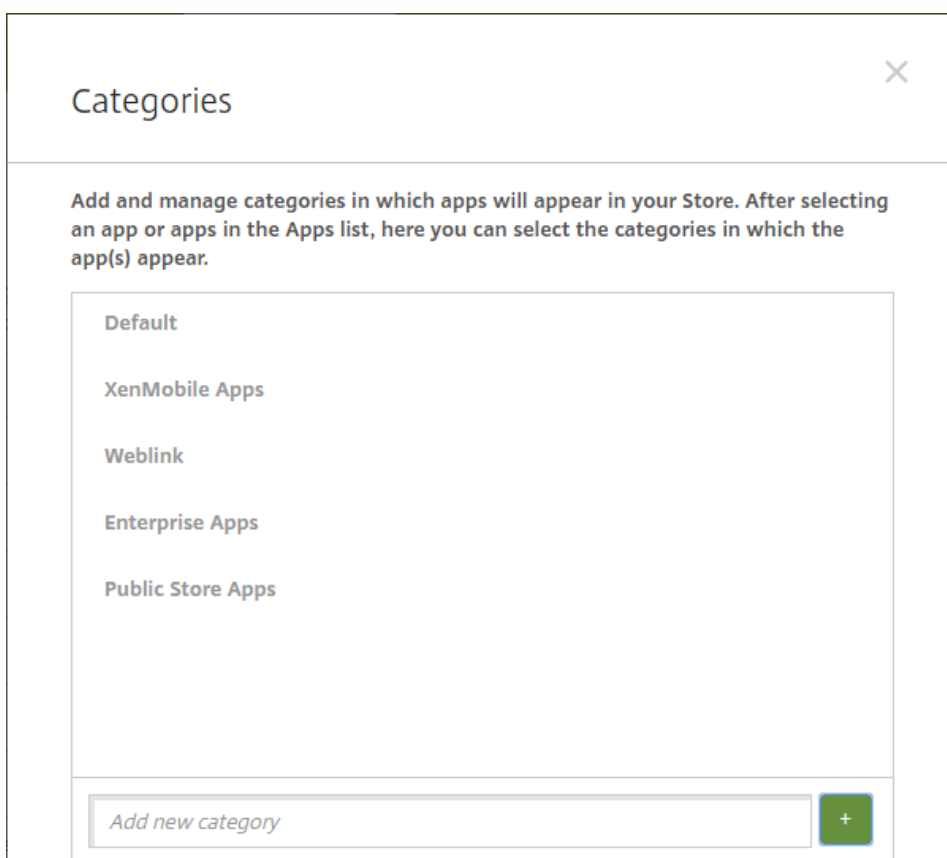
Add and manage categories in which apps will appear in your Store. After selecting an app or apps in the Apps list, here you can select the categories in which the app(s) appear.

Default

Add new category

3. 追加するカテゴリごとに、以下の操作を行います。

- ダイアログボックス下部にある **[Add a new category]** フィールドに、追加するカテゴリの名前を入力します。たとえば、「Enterprise Apps」と入力して、エンタープライズアプリケーションのカテゴリを作成することができます。
- プラス記号 (+) をクリックしてカテゴリを追加します。新しく作成したカテゴリが追加され、**[Categories]** ダイアログボックスに表示されます。





4. カテゴリの追加が終了したら、**[Categories]** ダイアログボックスを閉じます。

5. **[Apps]** ページで、既存のアプリケーションを新しいカテゴリに分類できます。

- 分類するアプリケーションを選択します。
- **[Edit]** をクリックします。**[App Information]** ページが開きます。
- **[App category]** の一覧で、新しいカテゴリのチェックボックスをオンにしてカテゴリを適用します。既存のカテゴリでアプリケーションに適用しないものについては、チェックボックスをオフにします。
- **[Delivery Groups Assignments]** タブをクリックするか、後続の各ページで**[Next]** をクリックして、残りのアプリケーションセットアップページに示される手順に従います。
- **[Delivery Groups Assignments]** のページの**[Save]** をクリックして新しいカテゴリを適用します。新しいカテゴリがアプリケーションに適用され、**[Apps]** の表に表示されます。

## パブリックアプリケーションストアのアプリケーションの追加

iTunesやGoogle Playなどのパブリックアプリケーションストアで入手できる無料または有料のアプリケーションをXenMobileに追加できます。たとえば、GoToMeetingです。Android for Work用にパブリックアプリケーションストアの有料アプリを追加するときに、一括購入ライセンスの状態（使用できるライセンス数の合計、現在使用中のライセンス数、ライセンスを使用している各ユーザーのメールアドレス）を確認できます。Android for Workの一括購入プランを利用すると、組織のアプリやその他のデータの検索、購入、配布の処理が簡単になります。

1. XenMobileコンソールで、**[Configure]** の**[Apps]** をクリックします。**[Apps]** ページが開きます。

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

**Apps** Show filter

Add | Category | Export

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	▼
<input type="checkbox"/>		hh viber	Public App Store	Default	10/18/16 7:55 AM	10/18/16 7:55 AM		
<input type="checkbox"/>		hh ebay	Public App Store	Default	10/18/16 8:04 AM	10/18/16 8:04 AM		
<input type="checkbox"/>		hh green	Enterprise	Default	10/18/16 8:07 AM	10/18/16 8:07 AM		
<input type="checkbox"/>		hh pink	Enterprise	Default	10/18/16 8:08 AM	10/18/16 8:08 AM		
<input type="checkbox"/>		hh web & saas	Web & SaaS	Default	10/18/16 8:09 AM	10/18/16 8:09 AM		
<input type="checkbox"/>		hh weblink	Web Link	Default	10/18/16 8:10 AM	10/18/16 8:10 AM		
<input type="checkbox"/>		MRF Android Enterprise TD	Enterprise	Default	10/18/16 8:12 AM	10/18/16 8:12 AM		
<input type="checkbox"/>		hh UWH	Enterprise	Default	10/18/16 8:17 AM	10/18/16 8:17 AM		
<input type="checkbox"/>		hh WW	MDX	Default	10/18/16 8:18 AM	10/18/16 8:18 AM		

2. **[Add]** をクリックします。**[Add App]** ダイアログボックスが開きます。

## Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. **[Public App Store]** をクリックします。**[App Information]** ページが開きます。

4. **[App Information]** ペインで、以下の情報を入力します。

- **Name** : アプリケーションの説明的な名前を入力します。この情報は、[Apps] の表の [App Name] の下に表示されま
- **Description** : 任意で、アプリケーションの説明を入力します。
- **App category** : 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリケーションカテゴリについて詳しくは、「[アプリケーションカテゴリの作成](#)」を参照してください。

5. [Next] をクリックします。[App Platforms] ページが開きます。

6. [Platforms] の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10を参照してプラットフォームの展開規則を設定します。

7. 追加するアプリケーションの名前を検索ボックスに入力し、[Search] をクリックして、アプリケーションを選択します。検索条件に一致するアプリケーションが表示されます。次の図は、「podio」の検索結果を示しています。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, and the 'Public App Store' section is expanded to show '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. The 'Platform' section is expanded to show 'iPhone', 'iPad', 'Google Play', 'Android for Work', 'Windows Desktop/Tablet', and 'Windows Phone', all of which are checked. The 'iPhone App Settings' section is also expanded, showing a search box with 'podio' entered and a 'Search' button. Below the search box, the search results for 'podio' in iPhone apps are displayed, showing two results: 'Podio Podio' and 'Podio Chat Podio'. Below the search results, there is a message: 'Didn't find the app you were looking for?'.

8. 追加するアプリケーションをクリックします。[App Details] フィールドには、選択したアプリケーションに関連する情報（名前、説明、バージョン番号、関連付けられたイメージなど）が事前に設定されています。

## App Details

The screenshot shows the 'App Details' configuration interface. It includes the following fields and settings:

- Name\***: Podio
- Description\***: The ultimate companion app for Podio – enabling you to run your projects and collaborate with your team from anywhere.  
Take your content and conversations with you, no matter where your workday takes you.
- Version**: 5.0.1
- Image**: [App icon]
- Paid app**: OFF
- Remove app if MDM profile is removed**: ON
- Prevent app data backup**: ON
- Force app to be managed**: OFF
- Force license association to device**: ON

Navigation buttons: Back, Next >

### 9. 次の設定を構成します。

- 必要に応じて、アプリケーションの名前と説明を変更します。
- **Paid app** : このフィールドは事前に構成されており、変更できません。
- **Remove app if MDM profile is removed** : MDMプロファイルが削除された場合にアプリケーションを削除するかどうかを選択します。デフォルトは **[ON]** です。
- **Prevent app data backup** : アプリケーションのデータをバックアップできないようにするかどうかを選択します。デフォルトは **[ON]** です。
- **Force app to be managed** : アプリケーションが非管理対象としてインストールされたときに、ユーザーに監視対象ではないデバイスでのアプリケーションの管理を許可するように求めるかどうかを選択します。デフォルトは **[OFF]** です。iOS 9.0以降で利用できます。
- **Force license to association to device** : デバイスの関連付けを有効にして開発されたアプリケーションを、ユーザーではなくデバイスに関連付けるかどうかを選択します。iOS 9以降で利用できます。選択したアプリケーションがデバイスへの割り当てをサポートしていない場合、このフィールドは変更できません。

### 10. 展開規則を構成します。

### 11. [XenMobile Store Configuration] を展開します。

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

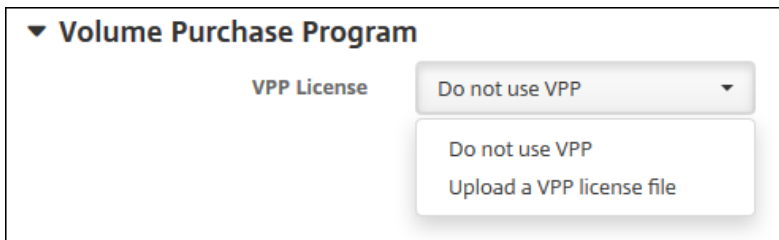
Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかを設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは [ON] です。
  - **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。

12. [Volume Purchase Program] を展開するか、Android for Workの場合は [Bulk Purchase] を展開します。

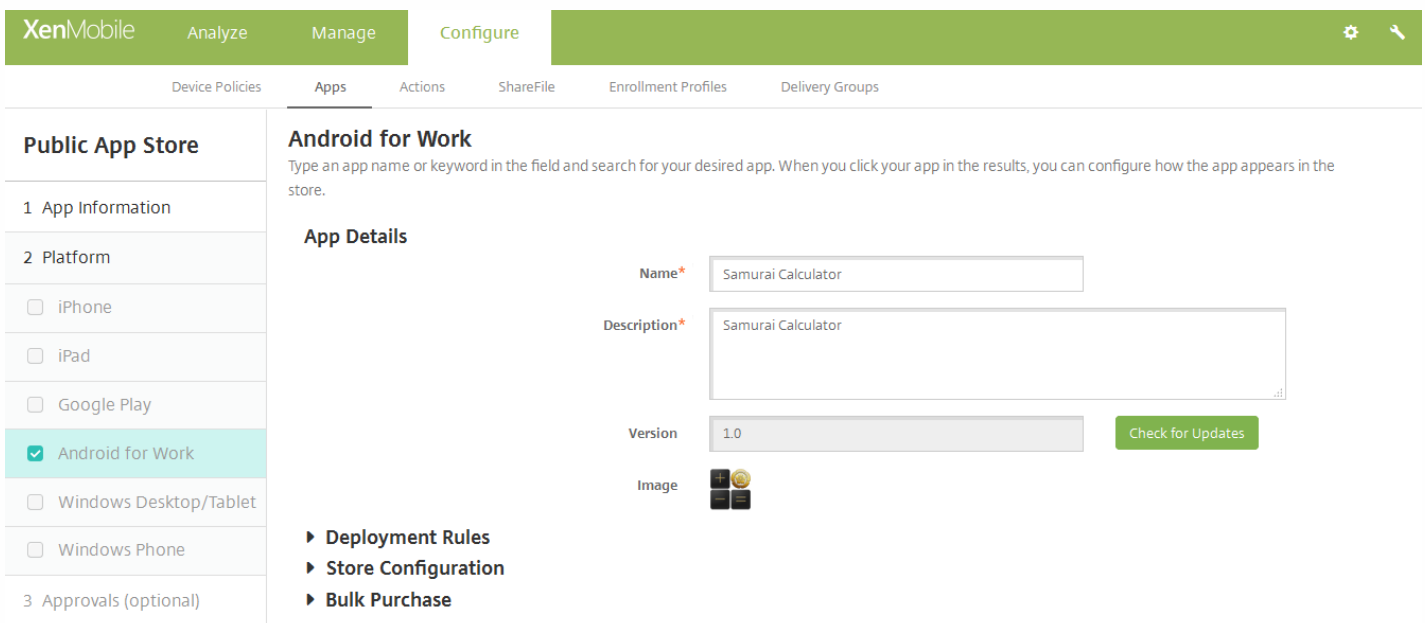
このVolume Purchase Programについて、次の手順に従います。



a. XenMobileでアプリケーションのVPPライセンスを適用できるようにする場合は、**[VPP license]** の一覧から、**[Upload a VPP license file]** を選択します。

ダイアログボックスが開いたら、ライセンスをインポートします。

Android for Workの一括購入の場合は、**[Bulk Purchase]** セクションを展開します。



[License Assignment] の表に、そのアプリケーションについての使用できる合計数と、現在使用されているライセンス数が表示されます。ユーザーを選択して **[Disassociate]** をクリックすると、そのユーザーへのライセンスの割り当てが終了し、別のユーザー向けにライセンスを空けることができます。ただし、ライセンスの割り当て解除は、そのユーザーが特定のアプリを含むデリバリーグループに属していない場合に限り実行できます。

### ▼ Bulk Purchase

#### License Assignment

Disassociate		License Usage: 2 of 3
<input type="checkbox"/>	Associated User	
<input checked="" type="checkbox"/>	@.net	
<input type="checkbox"/>		

Showing 1 - 2 of 2 items

13. **[Next]** をクリックします。 **[Approvals]** ページが開きます。

ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、次の手順に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use** : 一覧から既存のワークフローを選択するか、 **[Create a new workflow]** をクリックします。デフォルトは **[None]** です。
- **[Create a new workflow]** を選択した場合は、次の設定を構成します。
  - **Name** : ワークフローの固有の名前を入力します。
  - **Description** : 任意で、ワークフローの説明を入力します。
  - **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval** : 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは **[1 level]** です。選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers** : 検索フィールドに、追加に必要なユーザーの名前を入力して、 **[Search]** をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[Selected additional required approvers]** の一覧に表示されます。
    - **[Selected additional required approvers]** の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[Search]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
    - **[Selected additional required approvers]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。

14. **[Next]** をクリックします。 **[Delivery Group Assignment]** ページが開きます。

15. オプションとして、 **[Delivery Groups Assignment]** ページの **[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。

16. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注 :

- このオプションは、**[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、**[Deploy for always on connection]** は適用されません。

17. **[Save]** をクリックします。

## WebまたはSaaSアプリケーションの追加

XenMobileコンソールを使用して、モバイル、エンタープライズ、Web、SaaS (Software as a Service) アプリケーションへのSSO (Single Sign-On : シングルサインオン) 認証をユーザーに提供できます。アプリケーションのSSOは、アプリケーションコネクタのテンプレートを使用して有効にできます。XenMobileで使用できるコネクタの種類の一覧については、「[アプリケーションコネクタの種類](#)」を参照してください。WebアプリまたはSaaSアプリを追加すると、XenMobileで独自のコネクタを構築することもできます。

アプリケーションがSSOのみに対応している場合に、前記の設定の構成を完了してその設定を保存すると、アプリケーションがXenMobileコンソールの **[Apps]** タブに表示されます。

1. XenMobileコンソールで、**[Configure]** の **[Apps]** をクリックします。**[Apps]** ページが開きます。
2. **[Add]** をクリックします。**[Add App]** ダイアログボックスが開きます。

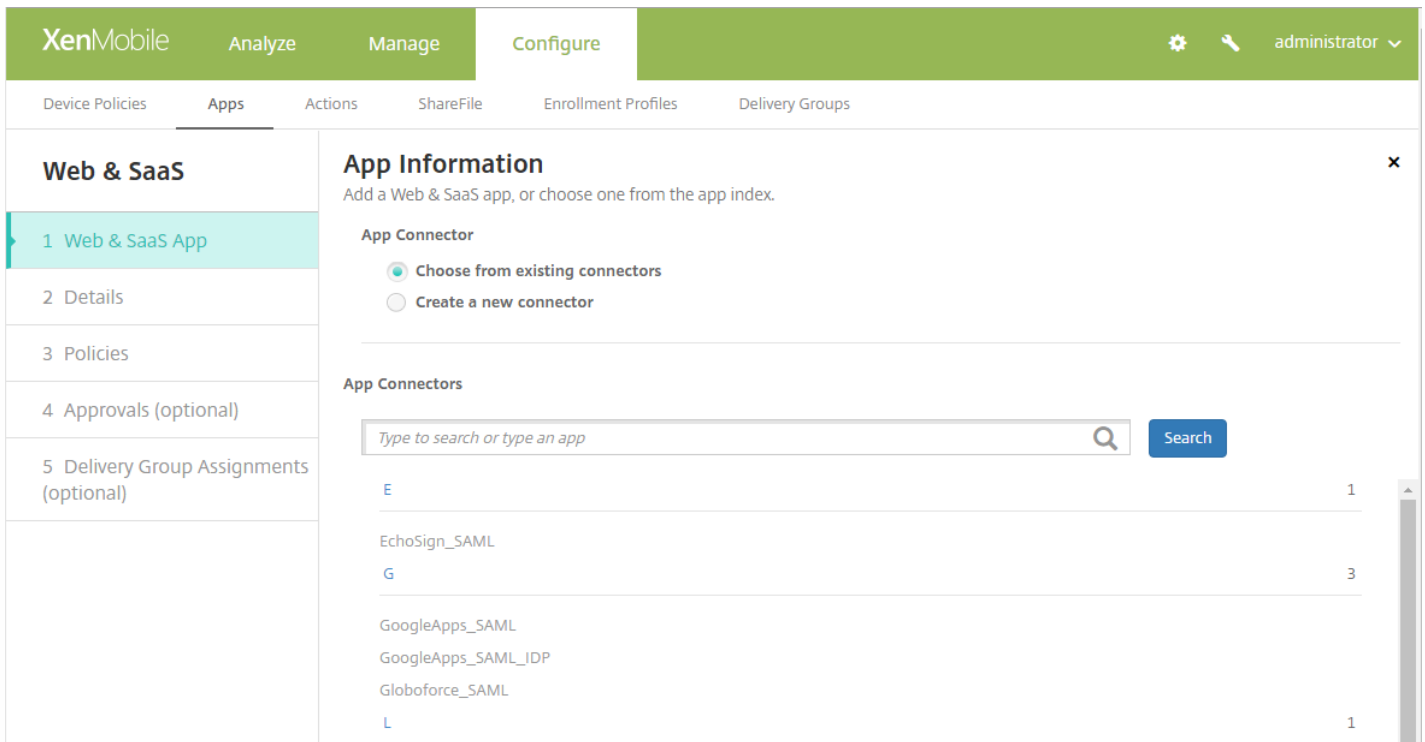
Add App
×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

<p><b>MDX</b></p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p><b>Public App Store</b></p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p><b>Web &amp; SaaS</b></p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p><b>Enterprise</b></p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p><b>Web Link</b></p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

3. **[Web & SaaS]** を選択します。**[App Information]** ページが開きます。





4. 既存のまたは新しいアプリケーションコネクタは、以下のように構成します。

既存のアプリケーションコネクタを構成するには

[App Information] ページで、上のように [Choose from existing connectors] が既に選択されています。[App Connectors] 一覧で、使用するコネクタを選択します。アプリケーションコネクタの情報が表示されます。

次の設定を構成します。

- **App name** : 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- **App description** : 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL** : 事前に入力されているURLをそのまま使用するか、アプリケーションのWebアドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
- **Domain name** : 該当する場合、アプリケーションのドメイン名を入力します。
- **App is hosted in internal network** : 内部ネットワークのサーバーでアプリケーションを実行するかどうかを選択します。ユーザーがリモートから内部アプリケーションに接続する場合は、NetScaler Gatewayを介して接続する必要があります。このオプションを [ON] に設定すると、VPNキーワードがアプリケーションに追加され、NetScaler Gatewayを介して接続できるようになります。デフォルトは [OFF] です。
- **App category** : 一覧から、アプリケーションに適用する任意のカテゴリを選択します。
- **User account provisioning** : アプリケーションのユーザーアカウントを作成するかどうかを選択します。Globoforce\_SAMLコネクタを使用している場合は、このオプションを有効にして、シームレスなSSO統合が行われるようにする必要があります。
- [User account provisioning] を有効にした場合は、次の設定を構成します。
  - サービス アカウント
    - **User name** : アプリケーション管理者の名前を入力します。このフィールドは必須です。
    - **Password** : アプリケーション管理者のパスワードを入力します。このフィールドは必須です。
  - ユーザーアカウント

- **When user entitlement ends** : 一覧から、ユーザーがアプリケーションへのアクセスを許可されなくなった場合に実行するアクションを選択します。選択できるオプションは以下のとおりです。
  - アカウントの無効化
  - アカウントの維持
  - アカウントを削除
- **ユーザー名規則**
  - 追加するユーザー名の規則ごとに、以下の操作を行います。
    - **User attributes** : 一覧から、規則に追加するユーザー属性を選択します。
    - **Length (characters)** : 一覧から、ユーザー名の規則で使用するユーザー属性の文字数を選択します。デフォルトは **[All]** です。
    - **Rule** : 追加した各ユーザー属性が、ユーザー名の規則に自動的に追加されます。
- **パスワード要件**
  - **Length** : ユーザーパスワードの最小文字数を入力します。デフォルトは **8** です。
- **パスワードの有効期限**
  - **Validity (days)** : パスワードの有効期間 (日数) を入力します。有効な値は **0 ~ 90** です。デフォルトは **90** です。
  - **Automatically reset password after it expires** : 有効期限が切れたときにパスワードを自動的にリセットするかどうかを選択します。デフォルトは **[OFF]** です。このフィールドを有効にしないと、ユーザーパスワードの有効期限が切れたときにアプリケーションを開くことができなくなります。

新しいアプリケーションコネクタを構成するには

**[App Information]** ページで、**[Create a new connector]** を選択します。アプリケーションコネクタのフィールドが表示されます。

XenMobile Analyze Manage **Configure** admin

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

### Web & SaaS

- 1 Web & SaaS App
- 2 Details
- 3 Policies
- 4 Approvals (optional)
- 5 Delivery Group Assignments (optional)

### App Information

Add a Web & SaaS app, or choose one from the app index.

App Connector  Choose from existing connectors  Create a new connector

Name\*

Description\*

Logon URL\*

SAML version  1.1  2.0

Entity ID\*

Relay state URL

Name ID format  Email Address  Unspecified

ACS URL\*

Image  Use default  Upload your own app image

**Add**

次の設定を構成します。

- **Name** : コネクタの名前を入力します。このフィールドは必須です。
- **Description** : コネクタの説明を入力します。このフィールドは必須です。
- **Logon URL** : ユーザーがサイトにログオンするときに使用するURLを入力するか、コピーして貼り付けます。たとえば、追加するアプリにログオンページがある場合、Webブラウザを開いてアプリのログオンページに移動します。「http://www.example.com/logon」などです。このフィールドは必須です。
- **SAML version** : **[1.1]** または **[2.0]** を選択します。デフォルトは**1.1**です。
- **Entity ID** : SAMLアプリケーションのIDを入力します。
- **Relay State URL** : SAMLアプリケーションのWebアドレスを入力します。リレーステートURLはアプリケーションからの応答URLです。
- **Name ID format** : **[Email Address]** または **[Unspecified]** を選択します。デフォルトは **[Email Address]** です。
- **ACS URL** : IDプロバイダーまたはサービスプロバイダーのアサーションコンシューマーサービスURL (ACS URL) を入力します。ACS URLでは、ユーザーがシングルサインオン機能を使用できます。
- **Image** : デフォルトのCitrixイメージを使用するのか、独自のアプリケーションイメージをアップロードするのを選択します。デフォルトは **[Use default]** です。
  - 独自のイメージをアップロードする場合は、**[Browse]** をクリックしてアップロードするファイルの場所に移動し、ファイルを選択します。このファイルはPNGファイルである必要があります。JPEGファイルやGIFファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。
  - 完了したら、**[Add]** をクリックします。**[Details]** ページが開きます。

5. [Next] をクリックします。[App Policy] ページが開きます。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Apps' tab is active, showing a list of app policies on the left and the configuration details for a selected policy on the right. The configuration details include sections for 'Device Security' and 'Network Requirements'. The 'Block jailbroken or rooted' toggle is turned on, while 'WiFi required' and 'Internal network required' are turned off. There is an input field for 'Internal WiFi networks'. At the bottom right, there are 'Back' and 'Next >' buttons.

- 次の設定を構成します。
  - デバイスセキュリティ
    - **Block jailbroken or rooted** : ジェイルブレイク済みまたはルート化済みのデバイスによるアプリケーションへのアクセスをブロックするかどうかを選択します。デフォルトは [ON] です。
  - ネットワーク要件
    - **WiFi required** : アプリケーションの実行にWiFi接続が必要であるかどうかを選択します。デフォルトは [OFF] です。
    - **Internal network required** : アプリケーションの実行に内部ネットワークが必要であるかどうかを選択します。デフォルトは [OFF] です。
    - **Internal WiFi networks** : [WiFi required] を有効にした場合は、使用する内部WiFiネットワークを入力します。

6. [XenMobile Store Configuration] を展開します。

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

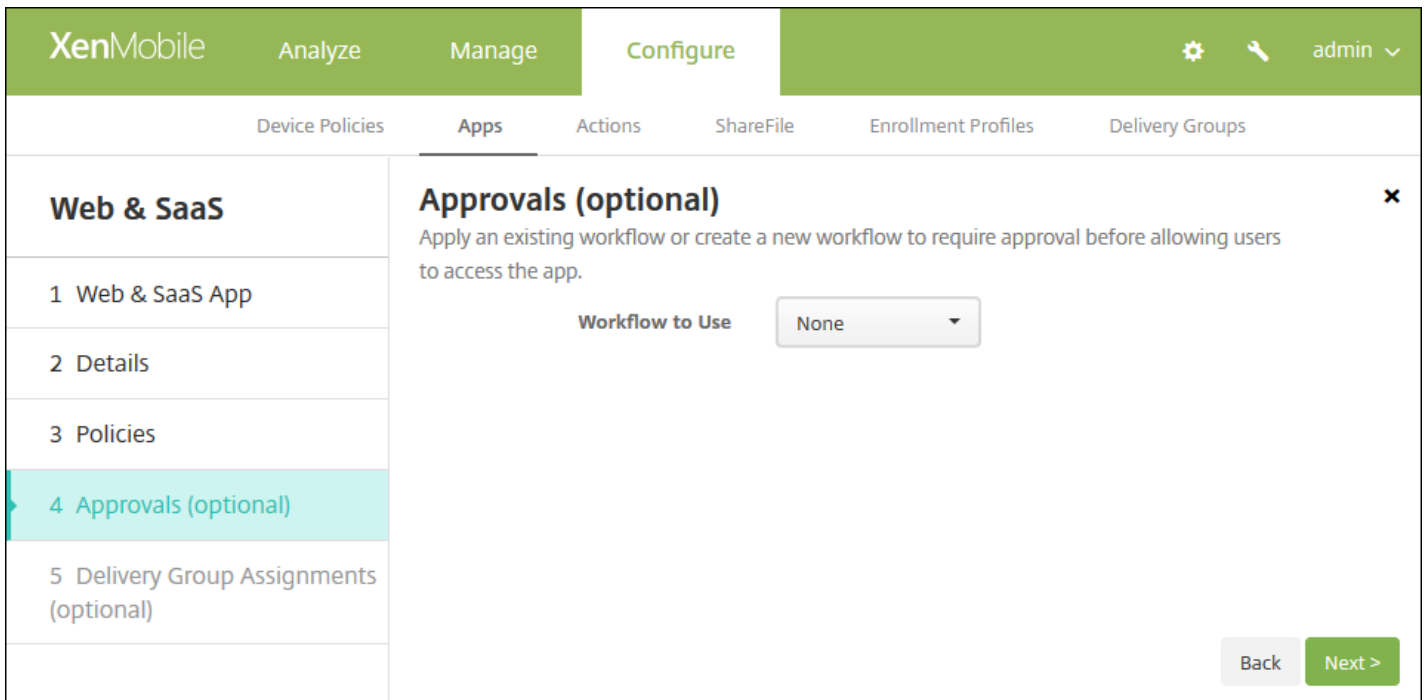
Allow app ratings

Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかを設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは[ON]です。
  - **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [ON] です。

7. [Next] をクリックします。[Approvals] ページが開きます。



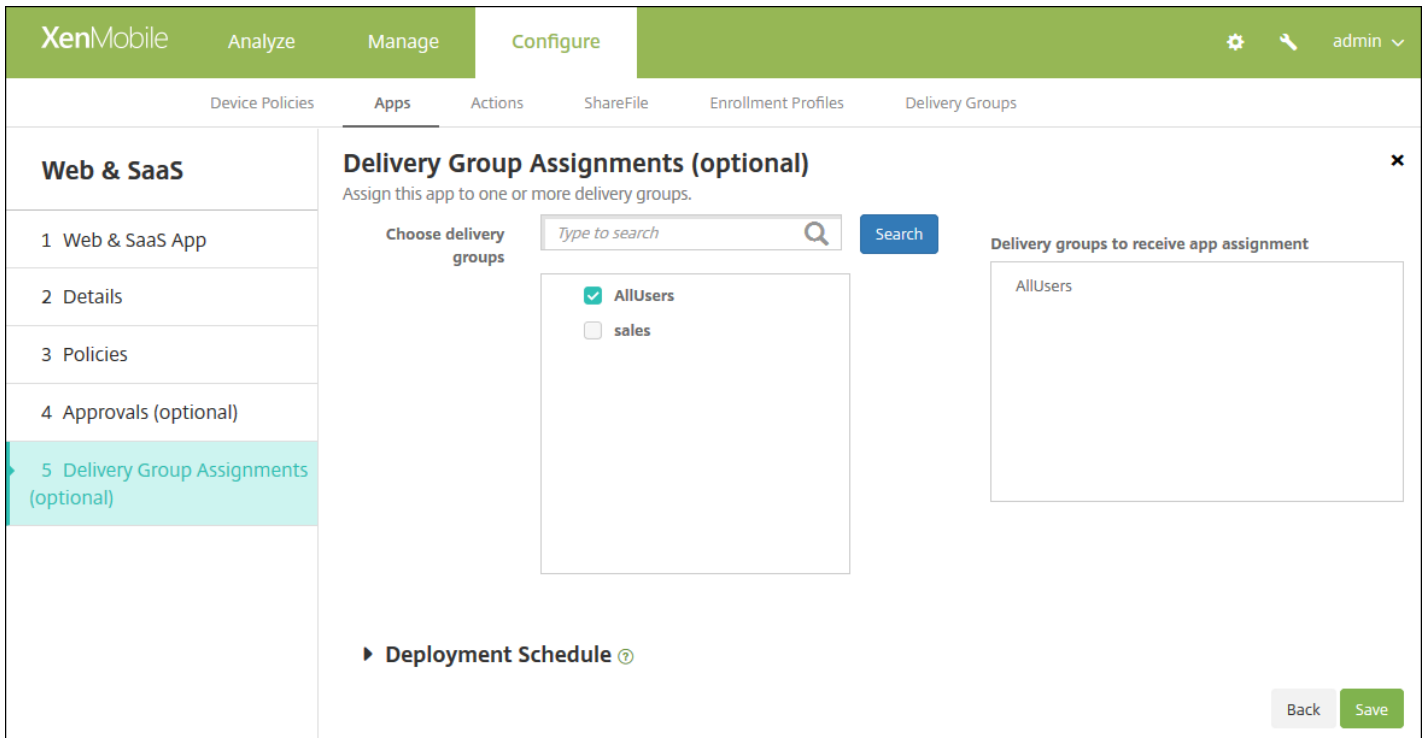
ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順8に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use** : 一覧から既存のワークフローを選択するか、 **[Create a new workflow]** をクリックします。デフォルトは **[None]** です。
- **[Create a new workflow]** を選択した場合は、次の設定を構成します。
  - **Name** : ワークフローの固有の名前を入力します。
  - **Description** : 任意で、ワークフローの説明を入力します。
  - **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval** : 一覧から、このワークフローで必要なマネージャー承認のレベル数を選択します。デフォルトは **[1 level]** です。選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers** : 検索フィールドに、追加で必要なユーザーの名前を入力して、 **[Search]** をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[Selected additional required approvers]** の一覧に表示されます。
    - **[Selected additional required approvers]** の一覧からユーザーを削除するには、次のいずれかを行います。
      - **[Search]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
      - **[Selected additional required approvers]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにし

す。

8. **[Next]** をクリックします。 **[Delivery Group Assignment]** ページが開きます。



9. オプションとして、 **[Delivery Groups Assignment]** ページの **[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。

10. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、 **[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。 **[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、 **[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、 **[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプションは **[OFF]** です。

注：

- このオプションは、 **[Settings]** の **[Server Properties]** において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 **[Deploy for always on connection]** は適用されません。

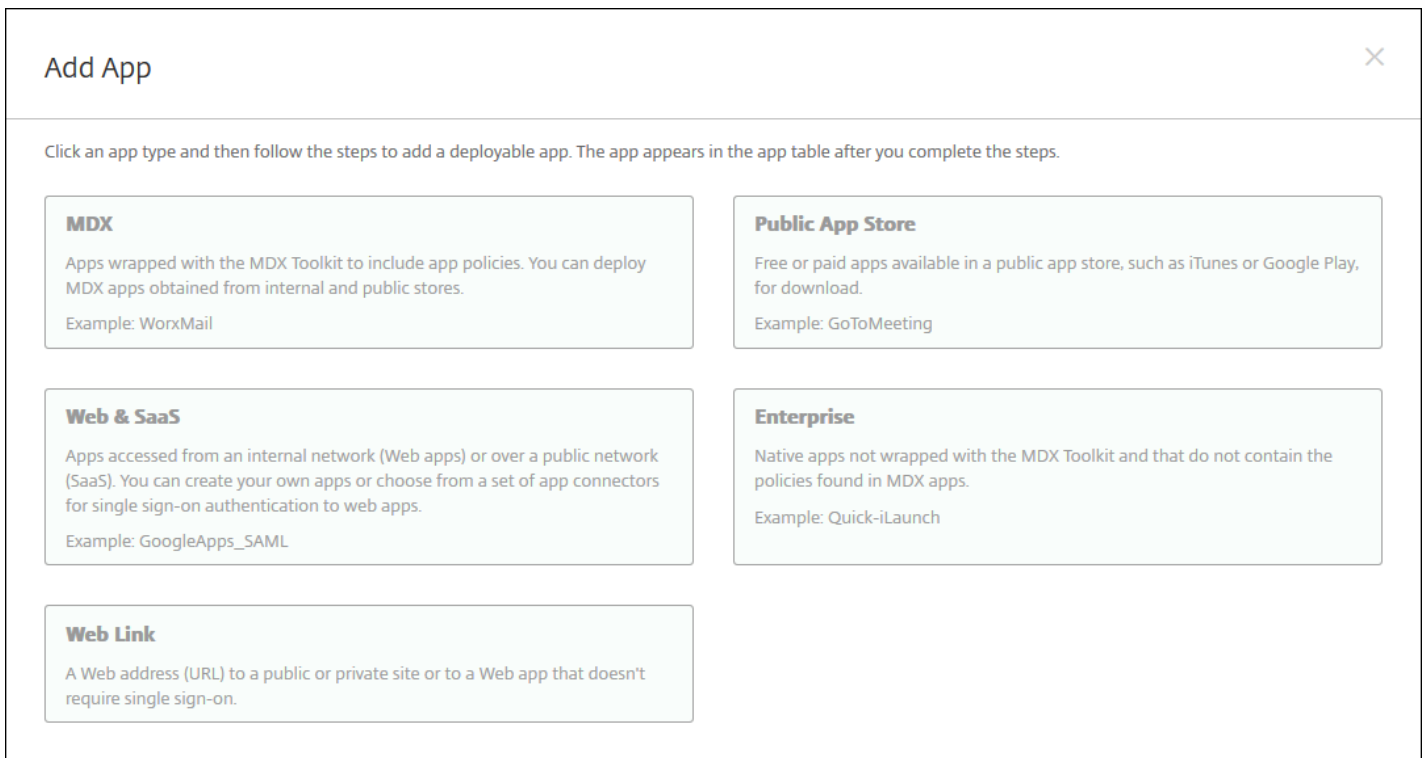
11. **[Save]** をクリックします。

# エンタープライズアプリケーションの追加

XenMobileのエンタープライズアプリケーションとは、MDX Toolkitでラップされておらず、MDXアプリケーションに関連付けられたポリシーを含んでいない、ネイティブアプリケーションを意味します。エンタープライズアプリケーションのアップロードは、XenMobileコンソールの **[Apps]** タブで行うことができます。エンタープライズアプリケーションは、以下のプラットフォーム（および対応するファイルの種類）をサポートします。

- iOS (.ipaファイル)
- Android (.apkファイル)
- Samsung KNOX (.apkファイル)
- Android for Work (.apkファイル)
- Windows Phone (.xapまたは.appxファイル)
- Windowsタブレット (.appxファイル)
- Windows Mobile/CE (.cabファイル)

1. XenMobileコンソールで、 **[Configure]** の **[Apps]** をクリックします。 **[Apps]** ページが開きます。
2. **[Add]** をクリックします。 **[Add App]** ダイアログボックスが開きます。



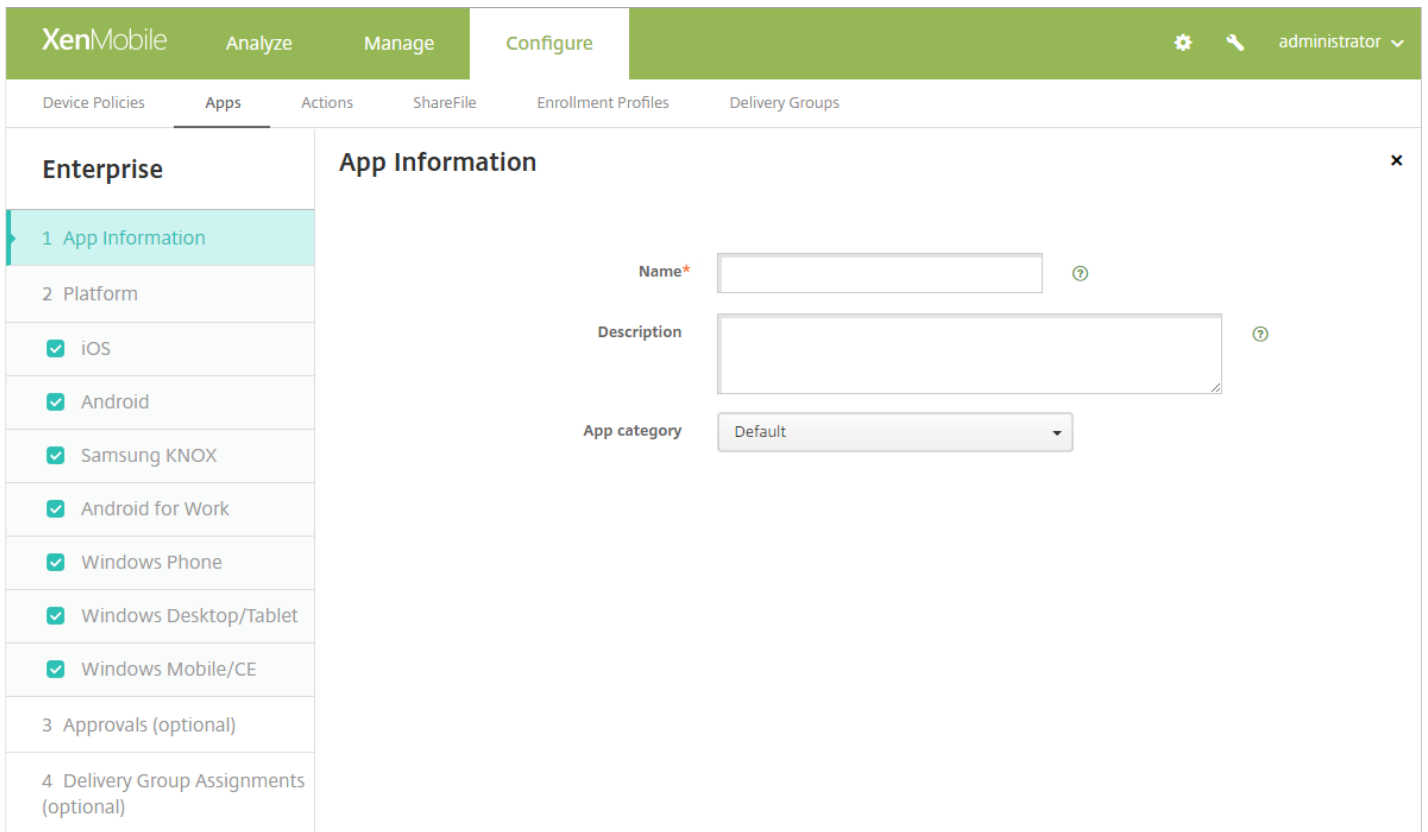
**Add App** ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

<p><b>MDX</b></p> <p>Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.</p> <p>Example: WorxMail</p>	<p><b>Public App Store</b></p> <p>Free or paid apps available in a public app store, such as iTunes or Google Play, for download.</p> <p>Example: GoToMeeting</p>
<p><b>Web &amp; SaaS</b></p> <p>Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.</p> <p>Example: GoogleApps_SAML</p>	<p><b>Enterprise</b></p> <p>Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.</p> <p>Example: Quick-iLaunch</p>
<p><b>Web Link</b></p> <p>A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.</p>	

3. **[Enterprise]** をクリックします。 **[App Information]** ページが開きます。





4. **[App Information]** ペインで、以下の情報を入力します。

- **Name** : アプリケーションの説明的な名前を入力します。この情報は、[Apps] の表の [App Name] の下に表示されません。
- **Description** : 任意で、アプリケーションの説明を入力します。
- **アプリケーションカテゴリ** : 任意で、一覧から、アプリを追加するカテゴリを選択します。アプリケーションカテゴリについて詳しくは、「[XenMobileでのアプリケーションカテゴリの作成](#)」を参照してください。

5. **[Next]** をクリックします。**[App Platforms]** ページが開きます。

6. **[Platforms]** の下で、追加するプラットフォームをオンにします。1つのプラットフォームのみを構成する場合は、それ以外のプラットフォームをオフにします。

1つのプラットフォームの設定の構成が完了したら、手順10を参照してプラットフォームの展開規則を設定します。

7. 選択したプラットフォームごとに、**[Browse]** をクリックしてアップロードするファイルの場所に移動し、そのファイルを選択します。

8. **[Next]** をクリックします。プラットフォームのアプリケーション情報ページが開きます。

9. プラットフォームの種類について、以下の設定を構成します。

- **File name** : 任意で、アプリケーションの名前を新たに入力します。
- **App Description** : 任意で、アプリケーションの説明を新たに入力します。
- **App version** : このフィールドは変更できません。
- **Minimum OS version** : 任意で、アプリケーションを使用するためにデバイスで実行できるオペレーティングシステムの最も古いバージョンを入力します。

- **Maximum OS version** : 任意で、アプリケーションを使用するためにデバイスで実行されている必要があるオペレーティングシステムの最も新しいバージョンを入力します。
- **Excluded devices** : 任意で、アプリケーションを実行できないデバイスの製造元またはモデルを入力します。
- **Remove app if MDM profile is removed** : MDMプロファイルが削除された場合にデバイスからアプリケーションを削除するかどうかを選択します。デフォルトは **[ON]** です。
- **Prevent app data backup** : アプリケーションのデータをバックアップできないようにするかどうかを選択します。デフォルトは **[ON]** です。
- **Force app to be managed** : 非管理対象のアプリケーションをインストールして、監視対象デバイスのユーザーにアプリケーションの管理を許可するよう求める場合は、 **[ON]** を選択します。この設定は、iOS 9.xデバイスに適用されます。

## 10. 展開規則を構成します。

11. **[XenMobile Store Configuration]** を展開します。

**▼ Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

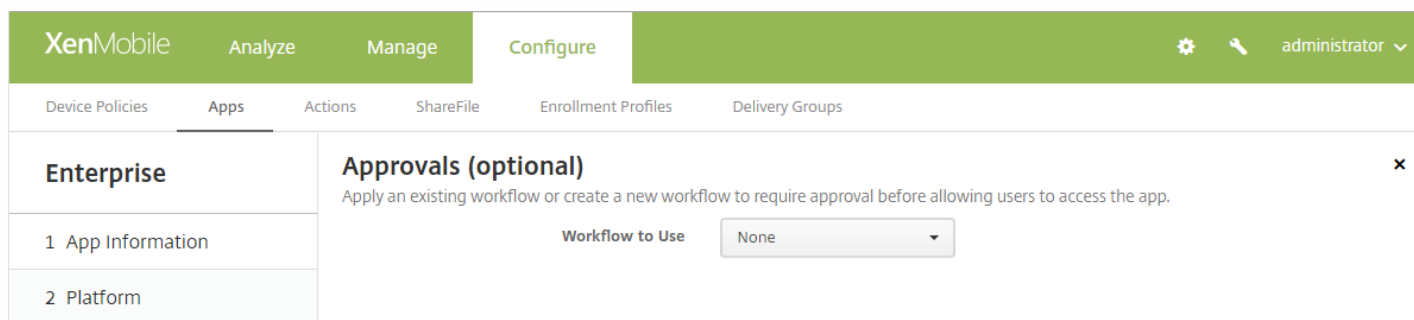
Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかを設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。

- **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
- **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは[ON]です。
- **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [ON] です。

12. [Next] をクリックします。 [Approvals] ページが開きます。



ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順13に進みます。

ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use** : 一覧から既存のワークフローを選択するか、 [Create a new workflow] をクリックします。デフォルトは [None] です。
- [Create a new workflow] を選択した場合は、次の設定を構成します。
  - **Name** : ワークフローの固有の名前を入力します。
  - **Description** : 任意で、ワークフローの説明を入力します。
  - **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval** : 一覧から、このワークフローに必要なマネージャー承認のレベル数を選択します。デフォルトは [1 level] です。選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers** : 検索フィールドに、追加が必要なユーザーの名前を入力して、 [Search] をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが [Selected additional required approvers] の一覧に表示されます。
    - [Selected additional required approvers] の一覧からユーザーを削除するには、次のいずれかを行います。
      - [Search] をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して [Search] をクリックし、検索結果を絞り込みます。
      - [Selected additional required approvers] の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにし

す。

13. [Next] をクリックします。 [Delivery Group Assignment] ページが開きます。

The screenshot shows the XenMobile configuration interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', and 'Delivery Groups'. The main content area is titled 'Enterprise' and 'Delivery Group Assignments (optional)'. It includes a search bar for 'Choose delivery groups' with a search button. Below the search bar, there are two columns of delivery groups: 'AllUsers' (checked) and 'sales' (unchecked). To the right, there is a section for 'Delivery groups to receive app assignment' which currently contains 'AllUsers'. At the bottom, there is a 'Deployment Schedule' section with a dropdown arrow. The interface also features a 'Back' button and a 'Save' button.

14. オプションとして、 [Delivery Groups Assignment] ページの [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。

15. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、 [OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。 [OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、 [Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 [Deploy for always on connection] は適用されません。

16. [Save] をクリックします。

## Webリンクの追加

XenMobileで、パブリックサイトやプライベートサイト、またはシングルサインオン (SSO) を必要としないWebアプリケーションのWebアドレス (URL) を設置できます。

Webリンクの構成は、XenMobileコンソールの [Apps] タブで行うことができます。Webリンクの構成が完了すると、リンクは [Apps] の表にある一覧にリンクアイコンとして表示されます。ユーザーがSecure Hubを使ってログオンすると、リンクは使用可能なアプリケーションおよびデスクトップの一覧と共に表示されます。

リンクを追加するには、次の情報を指定します。

- リンクの名前
- リンクの説明
- Webアドレス (URL)
- カテゴリ
- 役割
- .png形式の画像 (オプション)

1. XenMobileコンソールで、 [Configure] の [Apps] をクリックします。 [Apps] ページが開きます。

2. [Add] をクリックします。 [Add App] ダイアログボックスが開きます。

The screenshot shows a dialog box titled "Add App" with a close button (X) in the top right corner. Below the title bar, there is a line of instructional text: "Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps." Below this text are five rectangular boxes, each representing an app type with a title, description, and an example:

- MDX**: Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores. Example: WorxMail
- Public App Store**: Free or paid apps available in a public app store, such as iTunes or Google Play, for download. Example: GoToMeeting
- Web & SaaS**: Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps. Example: GoogleApps\_SAML
- Enterprise**: Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps. Example: Quick-iLaunch
- Web Link**: A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. [Web Link] をクリックします。 [App Information] ページが開きます。

4. 次の設定を構成します。

- **App name** : 事前に入力されている名前をそのまま使用するか、新しい名前を入力します。
- **App description** : 事前に入力されている説明をそのまま使用するか、独自の説明を入力します。
- **URL** : 事前に入力されているURLをそのまま使用するか、アプリケーションのWebアドレスを入力します。選択したコネクタによっては、このフィールドにプレースホルダーが含まれる場合があります。このプレースホルダーは、次のページに移動する前に置き換える必要があります。
- **App is hosted in internal network** : 内部ネットワークのサーバーでアプリケーションを実行するかどうかを選択します。ユーザーがリモートから内部アプリケーションに接続する場合は、NetScaler Gatewayを介して接続する必要があります。このオプションを **[ON]** に設定すると、VPNキーワードがアプリケーションに追加され、NetScaler Gatewayを介して接続できるようになります。デフォルトは **[OFF]** です。
- **App category** : 一覧から、アプリケーションに適用する任意のカテゴリを選択します。
- **Image** : デフォルトのCitrixイメージを使用するのか、独自のアプリケーションイメージをアップロードするのを選択します。デフォルトは [Use default] です。
  - 独自のイメージをアップロードする場合は、**[Browse]** をクリックしてアップロードするファイルの場所に移動し、ファイルを選択します。このファイルはPNGファイルである必要があります。JPEGファイルやGIFファイルはアップロードできません。カスタムグラフィックを追加した場合、後でそのグラフィックを変更することはできません。

5. **[XenMobile Store Configuration]** を展開します。

**▼ Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかを設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは[ON] です。
  - **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [ON] です。

6. [Next] をクリックします。[Delivery Group Assignment] ページが開きます。

7. オプションとして、[Delivery Groups Assignment] ページの [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。

8. [Deployment Schedule] を展開して以下の設定を構成します。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。

- [Deployment condition] の横の [On every connection] をクリックするか、 [Only when previous deployment has failed] をクリックします。デフォルトのオプションは、 [On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、 [Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、 [Deploy for always on connection] は適用されません。

9. [Save] をクリックします。

## Microsoft 365アプリの有効化

MDXコンテナを開いて、Secure Mail、Secure Web、およびShareFileがMicrosoft Office 365アプリにドキュメントやデータを転送するようにできます。詳しくは、「[Allowing Secure Interaction with Office 365 Apps](#)」を参照してください。

## ワークフローの作成および管理

ワークフローを使用して、ユーザーアカウントの作成および削除を管理できます。ワークフローを使用する前に、ユーザーアカウント要求を承認する権限を持つ組織内のユーザーを特定する必要があります。その後で、ワークフローテンプレートを使用して、ユーザーアカウント要求を作成および承認できます。

XenMobileを初めて設定するときに、ワークフローのメール設定を構成します。これは、ワークフローを使用する前に設定する必要があります。ワークフローの電子メール設定はいつでも変更できます。これらの設定には、メールサーバー、ポート、メールアドレス、およびユーザーアカウントの作成要求に承認が必要かどうかなどが含まれます。



XenMobileの次の2つの方法でワークフローを構成できます。

- XenMobileコンソールの [Workflows] ページ。 [Workflows] ページでは、アプリケーションの構成で使用する複数のワークフローを構成できます。 [Workflows] ページでワークフローを構成するとき、アプリケーションを構成するときのワークフローを選択できます。
- アプリケーションコネクタを構成するとき、アプリケーションで、ワークフロー名を入力し、ユーザーアカウント要求を承認できるユーザーを構成します。

ユーザーアカウントの管理者承認を最大3レベルまで割り当てることができます。ほかのユーザーにユーザーアカウントを承認してもらう必要がある場合は、ユーザーの名前またはメールアドレスを使用して追加のユーザーを検索し選択することができます。ユーザーが見つかったら、そのユーザーをワークフローに追加します。ワークフローのすべてのユーザーが、新しいユーザーアカウントを承認または却下するための電子メールを受け取ります。


1. XenMobileコンソールで、右上の歯車アイコンをクリックします。 [Settings] ページが開きます。
2. [Workflows] をクリックします。 [Workflows] ページが開きます。



XenMobile Analyze Manage Configure   admin ▾

Settings > Workflows



## Workflows

 Add

<input type="checkbox"/>	Name	Description	Workflow email template	▾
<input type="checkbox"/>	WF 1		Workflow Approval Request	

Showing 1 - 1 of 1 items

3. **[Add]** をクリックします。 **[Add Workflow]** ページが開きます。


XenMobile Analyze Manage Configure   admin ▾

Settings > Workflows > Add Workflow

## Add Workflow


**Name\***

**Description**

**Email Approval Templates** Workflow Approval Request 

**Levels of manager approval** 1 level ▾

**Select Active Directory domain** agsag.com ▾

**Find additional required approvers**  

**Selected additional required approvers**

4. 次の設定を構成します。

- **Name** : ワークフローの固有の名前を入力します。
- **Description** : 任意で、ワークフローの説明を入力します。
- **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。電子メールテンプレートの作成は、XenMobileコンソールの [Settings] の [Notification Templates] セクションで行います。このフィールドの右にある、目のアイコンをクリックすると、以下のダイアログボックスが表示されます。

## Workflow Approval Request

To modify the workflow template, please go to the notification template section in Settings.

Email Title	Workflow Approval Request for an Application
Email Content	Please approve the application \${applicationName} for your staff by clicking the following link. Thank you for spending the time to approve the application.

Close

- **Levels of manager approval** : 一覧から、このワークフローに必要なマネージャー承認のレベル数を選択します。デフォルトは [1 level] です。選択できるオプションは以下のとおりです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers** : 検索フィールドに、追加で必要なユーザーの名前を入力して、[Search] をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[Selected additional required approvers]** の一覧に表示されます。
    - **[Selected additional required approvers]** の一覧からユーザーを削除するには、次のいずれかを行います。
      - [Search] をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
      - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
      - **[Selected additional required approvers]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにします。
5. **[Save]** をクリックします。作成したワークフローが **[Workflows]** ページに表示されます。

ワークフローを作成すると、ワークフローの詳細を表示したり、ワークフローに関連付けられたアプリケーションを表示したり、ワークフローを削除したりできます。ワークフローを作成した後でワークフローを編集することはできません。承認レベルまたは承認者が異なるワークフローが必要な場合は、新しいワークフローを作成する必要があります。

ワークフローの詳細の表示および削除を行うには

1. **[Workflows]** ページの既存のワークフローの一覧で、表の行をクリックするかワークフローの横にあるチェックボックスをオンにして、特定のワークフローを選択します。
2. ワークフローを削除するには、**[Delete]** をクリックします。確認ダイアログボックスが開きます。もう一度 **[Delete]** をクリックします。

**重要** : この操作を元に戻すことはできません。

# アプリコネクタの種類

Apr 27, 2017

次の表に、WebアプリまたはSaaSアプリを追加する場合にXenMobile内で使用できるコネクタとコネクタの種類を示します。WebまたはSaaSアプリを追加すると、新しいコネクタを追加することもできます。

この表は、各コネクタがユーザーアカウント管理をサポートするかどうかについて示します。ユーザーアカウント管理がサポートされる場合、管理者は新しいアカウントを自動的に作成したり、ワークフローを使って作成したりできます。

コネクタ名	SSO SAML	ユーザーアカウント管理のサポート
EchoSign_SAML	はい	はい
Globoforce_SAML		注：このコネクタを使用する場合は、[User Management for Provisioning] を有効にして、シームレスなSSO統合が行われるようにする必要があります。
GoogleApps_SAML	はい	はい
GoogleApps_SAML_IDP	はい	はい
Lynda_SAML	はい	はい
Office365_SAML	はい	はい
Salesforce_SAML	はい	はい
Salesforce_SAML_SP	はい	はい
SandBox_SAML	はい	
SuccessFactors_SAML	はい	
ShareFile_SAML	はい	
ShareFile_SAML_SP	はい	
WebEx_SAML_SP	はい	はい

# MDXまたはエンタープライズアプリケーションのアップグレード

Apr 27, 2017

XenMobileでMDXまたはエンタープライズアプリケーションをアップグレードするには、XenMobileコンソールでアプリケーションを無効にしてから、アプリケーションの新しいバージョンをアップロードします。

1. XenMobileコンソールで、**[Configure]** の **[Apps]** をクリックします。**[Apps]** ページが開きます。



2. 管理対象デバイス（モバイルデバイス管理でXenMobileに登録されたデバイス）の場合は、スキップして手順3に進みます。非管理対象デバイス（エンタープライズアプリケーション管理の目的のみでXenMobileに登録されたデバイス）の場合は、次の手順に従います。

- **[Apps]** の表で、アプリケーションの横のチェックボックスをオンにするか、更新するアプリケーションを含む行をクリックします。
- 表示されるメニューで、**[Disable]** をクリックします。

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable	
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM		
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/10/15 3:13 PM		
<input type="checkbox"/>		worxweb	MDX	Worxapps				
<input type="checkbox"/>		Angrybird	Public App Store	Public				
<input type="checkbox"/>		WorxTasks	MDX	Default				
<input type="checkbox"/>		WorxMail2	MDX	MDX				
<input type="checkbox"/>		WorxNotes-iOS	MDX	MDX				
<input type="checkbox"/>		worxweb2	MDX	MDX				
<input type="checkbox"/>		ShareFile1	MDX	MDX				

Showing 1 - 9 of 9 items

- 確認のダイアログボックスで **[Disable]** をクリックします。アプリケーションの **[Disable]** 列に「**Disabled**」と表示されます。

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Onebug	Web Link	Weblink	10/26/15 1:04 PM	11/6/15 9:14 AM	
<input type="checkbox"/>		Worxmail	MDX	Worxapps	10/26/15 1:06 PM	11/11/15 8:55 AM	Disabled

注：アプリケーションを無効にすると、アプリケーションが保守モードになります。アプリケーションが無効になっている場合、ユーザーはログオフ後にそのアプリケーションに再接続することはできません。アプリケーションの無効化は任意の設定ですが、アプリケーションの機能の問題を避けるために、アプリケーションを無効にすることをお勧めします。ポリシーを更新する場合や、XenMobileにアプリケーションをアップロードすると同時にユーザーがダウンロードを要求する場合などに問題が発生することがあります。

3. [アプリ] の表で、アプリケーションの横のチェックボックスをオンにするか、更新するアプリケーションを含む行をクリックします。
  4. 5. 表示されるメニューで、[Edit] をクリックします。アプリケーションに対して最初に選択したプラットフォームが選択された状態で、[App Information] ページが開きます。
  5. 次の設定を構成します。
    - **Name**：任意で、アプリケーション名を変更します。
    - **Description**：任意で、アプリケーションの説明を変更します。
    - **App category**：任意で、アプリケーションのカテゴリを変更します。
  6. [Next] をクリックします。最初に選択したプラットフォームのページが開きます。選択したプラットフォームごとに、以下の操作を行います。
    - [Upload] をクリックしてアップロードするファイルの場所に移動し、置き換えるファイルを選択します。アプリケーションがXenMobileにアップロードされます。
    - 任意で、プラットフォームのアプリケーションの詳細とポリシー設定を変更します。
    - 任意で、展開規則の構成（手順7を参照）およびXenMobile Storeの構成（手順8を参照）を行います。
7. 展開規則を構成します。
8. [Store Configuration] を展開します。

▼ **Store Configuration**

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

任意で、アプリケーションに関するFAQや、XenMobile Storeに表示される画面キャプチャを追加できます。また、ユーザーにアプリケーションの評価やアプリケーションについてのコメントを許可するかどうかも設定できます。

- 次の設定を構成します。
  - **App FAQ** : アプリケーションに関するFAQの質問および回答を追加します。
  - **App screenshots** : アプリケーションをXenMobile Storeで分類しやすくするための画面キャプチャを追加します。アップロードするグラフィックはPNGである必要があります。GIFイメージやJPEGイメージはアップロードできません。
  - **Allow app ratings** : ユーザーにアプリケーションの評価を許可するかどうかを選択します。デフォルトは[ON]です。
  - **Allow app comments** : 選択したアプリケーションについてユーザーがコメントできるようにするかどうかを選択します。デフォルトは [ON] です。

9. [Next] をクリックします。 [Approvals] ページが開きます。

10. ユーザーアカウントの作成時に承認が必要な場合は、ワークフローを使用します。承認ワークフローを設定する必要がない場合は、手順11に進みます。

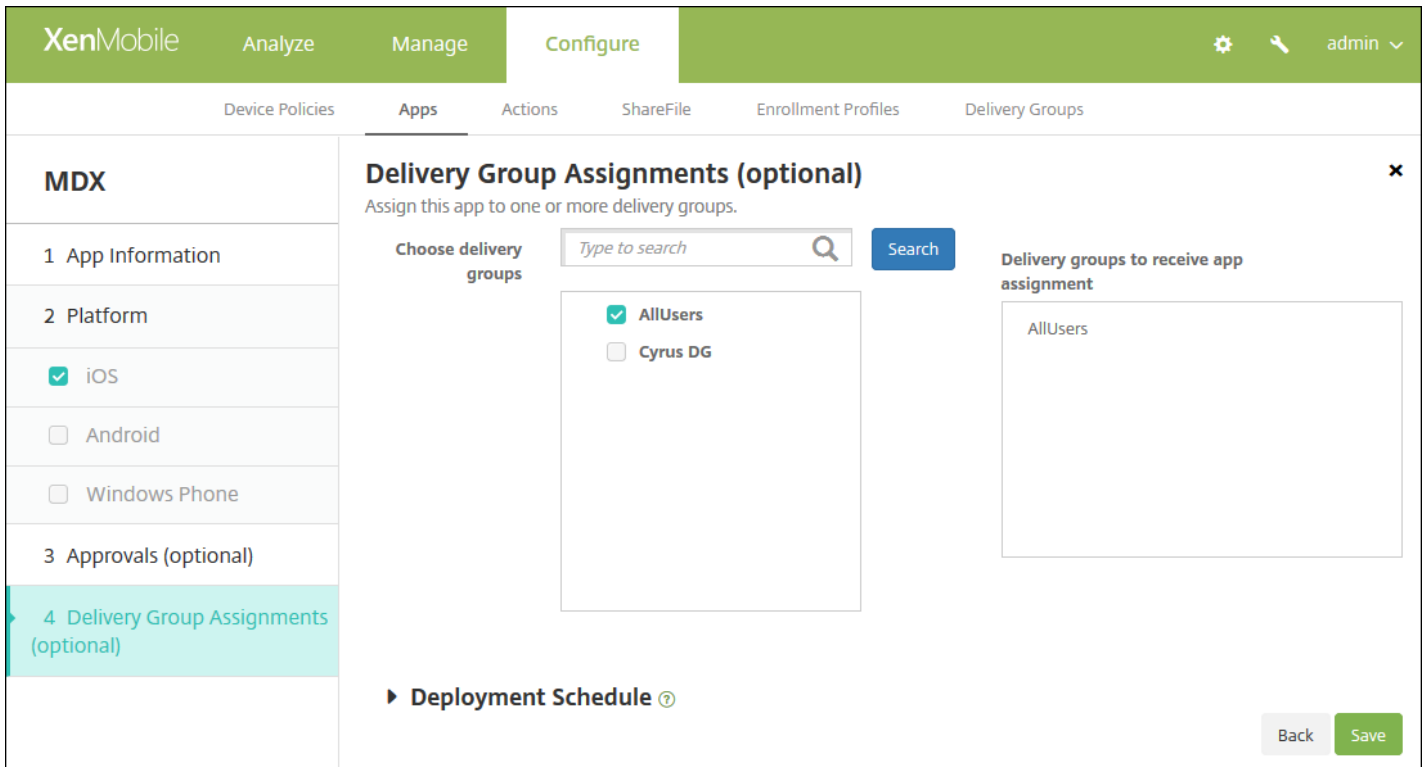
ワークフローを割り当てるか作成する必要がある場合は、次の設定を構成します。

- **Workflow to Use** : 一覧から既存のワークフローを選択するか、 **[Create a new workflow]** をクリックします。デフォルトは **[None]** です。
- **[Create a new workflow]** を選択した場合は、次の設定を構成します。
  - **Name** : ワークフローの固有の名前を入力します。
  - **Description** : 任意で、ワークフローの説明を入力します。
  - **Email Approval Templates** : 一覧から、割り当てる電子メール承認テンプレートを選択します。このフィールドの右にある目のアイコンをクリックすると、ダイアログボックスが開き、テンプレートをプレビューできます。
  - **Levels of manager approval** : 一覧から、このワークフローに必要なマネージャー承認のレベル数を選択します。デフォルトは **1 level** です。以下は使用できるオプションです。
    - Not Needed
    - 1 level
    - 2 levels
    - 3 levels
  - **Select Active Directory domain** : 一覧から、ワークフローで使用する適切なActive Directoryドメインを選択します。
  - **Find additional required approvers** : 検索フィールドに、追加が必要なユーザーの名前を入力して、 **[Search]** をクリックします。名前はActive Directoryで取得されます。
  - ユーザーの名前がフィールドに表示されたら、名前の横にあるチェックボックスをオンにします。ユーザーの名前とメールアドレスが **[Selected additional required approvers]** の一覧に表示されます。
  - **[Selected additional required approvers]** の一覧からユーザーを削除するには、次のいずれかを行います。
    - **[Search]** をクリックして、選択したドメイン内のすべてのユーザーの一覧を表示します。
    - 名前の全体または一部を検索ボックスに入力して **[Search]** をクリックし、検索結果を絞り込みます。
    - **[Selected additional required approvers]** の一覧に含まれるユーザーは、結果一覧に表示される名前の横にチェックマークがあります。一覧をスクロールし、削除するそれぞれの名前の横のチェックボックスをオフにしま



す。

11. [Next] をクリックします。[Deliver Group Assignment] ページが開きます。



12. オプションとして、[Delivery Groups Assignment] ページの [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。選択したグループは [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。

- [Deploy] の横の [ON] をクリックすると展開がスケジュールされ、[OFF] をクリックすると展開が行われません。デフォルトのオプションは [ON] です。[OFF] を選択した場合、そのほかのオプションを構成する必要はありません。
- [Deployment schedule] の横の [Now] または [Later] をクリックします。デフォルトのオプションは [Now] です。
- [Later] をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- [Deployment condition] の横の [On every connection] をクリックするか、[Only when previous deployment has failed] をクリックします。デフォルトのオプションは、[On every connection] です。
- [Deploy for always-on connection] の横の [ON] または [OFF] をクリックします。デフォルトのオプションは [OFF] です。

注：

- このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。
- 構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[Deploy for always on connection] は適用されません。

14. [Save] をクリックします。[Apps] ページが開きます。

15. 手順2でアプリケーションを無効にした場合は、次の手順に従います。

- [Apps] の表で更新したアプリケーションをクリックして選択し、表示されるメニューで[Enable] をクリックします。
- 確認ダイアログボックスが表示されたら、[Enable] をクリックします。これで、ユーザーがアプリケーションにアクセスでき、アプリケーションのアップグレードを求める通知を受信できるようになりました。

# MDXアプリケーションポリシーの概要

Apr 27, 2017

制限事項とCitrixの推奨事項が注に記載されたiOS、Android、およびWindows PhoneのMDXアプリケーションポリシーの一覧については、MDX Toolkitのドキュメントの「[MDXアプリケーションポリシーの概要](#)」を参照してください。

# XenMobile StoreおよびCitrix Secure Hubのブランド設定

Apr 27, 2017

ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、iOSおよびAndroidのモバイルデバイス上でSecure HubおよびXenMobile Store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。

カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および340px×50px（2x）を超過しないようにする必要があります。
- ファイルの名前はHeader.pngおよびHeader@2x.pngにします。
- ファイルを含むフォルダーではなく、ファイルから.zipファイルを作成します。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Dashboard', 'Manage', and 'Configure' tabs. On the right side of the navigation bar, there is a gear icon for settings and an 'Admin' dropdown menu. The main content area is titled 'Settings' and is organized into three columns of settings categories. The first column includes 'Certificate Management' (Certificates, Credential Providers, PKI Entities) and 'Client' (Client Branding, Client Properties, Client Support). The second column includes 'Notifications' (Carrier SMS Gateway, Notification Server, Notification Templates) and 'Platforms' (Android for Work, Google Play Credentials, iOS Bulk Enrollment, iOS Settings, Samsung KNOX). The third column includes 'Server' (ActiveSync Gateway, Enrollment, LDAP, Licensing, Local Users and Groups, Mobile Service Provider, NetScaler Gateway, Network Access Control, Release Management, Role-Based Access Control, Server Properties, SysLog, Workflows, XenApp/XenDesktop). On the right side of the main content area, there is a 'Frequently Accessed' sidebar with links to Certificates, Enrollment, Licensing, Local Users and Groups, Role-Based Access Control, and Release Management.

2. [Client] で [Create Branding] をクリックします。[Client Branding] ページが開きます。

Settings &gt; Client Branding

## Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

**Store name\***  ⓘ

**Default store view**

Category

A-Z

**Device**

Phone

Tablet

**Branding file**

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
  - The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
  - Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

次の設定を構成します。

- **Store name** : ユーザーのアカウント情報に含まれるストア名が表示されます。この名前を変更すると、ストアサービスのアクセスに使用されるURLも変更されます。通常、デフォルトの名前をそのまま使用します。
- **Default store view** : **[Category]** または **[A-Z]** を選択します。デフォルトは **[A-Z]** です。
- **Device option** : **[Phone]** または **[Tablet]** を選択します。デフォルトは **[Phone]** です。
- **Branding file** : **[Browse]** をクリックしてブランド設定に使用するイメージまたはイメージの.zipファイルの場所に移動し、ファイルを選択します。

3. **[Save]** をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、パッケージをユーザーのデバイスに展開する必要があります。

# Citrix Launcher

Apr 27, 2017

Citrix Launcherを使用すると、XenMobileによって展開されたAndroidデバイスのユーザーエクスペリエンスをカスタマイズできます。Citrix LauncherのSecure Hub管理でサポートされるAndroidの最小バージョンは、Android 4.0.3です。**Launcher Configuration Policy**を追加すると、次のCitrix Launcher機能を制御できます。

- ユーザーは管理者が指定したアプリにのみアクセスできるようにAndroidデバイスを管理する。
- Citrix Launcherアイコンのカスタムロゴ画像と、Citrix Launcherのカスタム背景画像をオプションで指定する。
- ユーザーがランチャーを終了するために入力する必要があるパスワードを指定する。

デバイスのランチャーは、WiFi、Bluetooth、デバイスコード、その他の設定のデバイス設定への組み込みアクセスを提供します。Citrix Launcherは、デバイスプラットフォームで既に提供されているセキュリティを強化するものではありません。

Citrix LauncherをAndroidデバイスに提供するには、次の一般的な手順に従います。

1. Citrix LauncherアプリをXenMobileエディションの[Citrix XenMobileダウンロード](#)ページからダウンロードします。ファイル名はCitrixLauncher.apkです。ファイルはすぐにXenMobileにアップロードできる状態で、ラッピングを必要としません。
2. デバイスポリシー**Launcher Configuration Policy**を追加します。[**Configure**] > [**Device Policies**] の順にクリックして、[**Add**] をクリックし、[**Add a New Policy**] ダイアログボックスに「**Launcher**」と入力を開始します。詳しくは、「[Launcher Configurationポリシー](#)」を参照してください。

The screenshot shows the XenMobile web interface in the 'Configure' section. The left sidebar has a 'Launcher Configuration Policy' section with three sub-items: '1 Policy Info', '2 Platforms', and '3 Assignment'. The '2 Platforms' item is expanded to show 'Android' selected. The main content area is titled 'Policy Information' and contains the following configuration options:

- Launcher app configuration**
  - Define a logo image**:  ON. Logo image: ribbon.png.
  - Define a background image**:  ON. Background image: .
- Allowed apps**

App name	Package Name*	<input type="button" value="Add"/>
test	test.com	
- Password**:
- Deployment Rules**:

3. Citrix LauncherアプリをエンタープライズアプリとしてXenMobileに追加します。[**Configure**] > [**Apps**] で、[**Add**] をクリックします。続いて、[**Enterprise**] をクリックします。詳しくは、「[エンタープライズアプリケーションの追加](#)」を参照してください。

## Add App ×

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

**MDX**

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

**Public App Store**

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

**Web & SaaS**

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps\_SAML

**Enterprise**

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

Example: Quick-iLaunch

**Web Link**

A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

4. **[Configure] > [Delivery groups]** で次のように構成して、Citrix Launcherのデリバリーグループを作成します。

- **[Policies]** ページで、**[Launcher Configuration Policy]** を追加します。
- **[Apps]** ページで、**Citrix Launcher**を **[Required Apps]** にドラッグします。
- **[Summary]** ページで **[Deployment Order]** をクリックして、**Citrix Launcher**アプリが**Launcher Configuration**ポリシーよりも先であることを確認します。

## Deployment Order ×

Change the deployment order by dragging the policies, apps and actions into position.

Citrix Launcher

Launcher Configuration

詳しくは、「[リソースの展開](#)」を参照してください。

# iOS Volume Purchase Planの設定

Apr 27, 2017

Apple iOSのVolume Purchase Program (VPP) を使用してiOSアプリのライセンスを管理できます。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です。VPPを利用すると、組織のアプリケーションやデータ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によって、XenMobileがアプリ（XenMobileアプリおよびその他のMDXアプリなど）をデバイスに直接配布したり、引き換え可能なコードでユーザーにコンテンツを割り当てたりできます。iOS Volume Purchase Plan (VPP) に固有の設定を構成します。

このトピックは、管理されたライセンスでVPPを使用して、XenMobileでアプリを配布できるようにする方法について説明します。現在引き換えコードを使用中で、管理された配布に変更する場合は、Apple社のサポートドキュメントの[Migrate from redemption codes to managed distribution with the Volume Purchase Program](#)を参照してください。

iOS Volume Purchase Programについて詳しくは、<http://www.apple.com/business/vpp/>を参照してください。VPPに登録するには、<https://deploy.apple.com/qforms/open/register/index/avs/>にアクセスしてください。iTunesのVPPストアにアクセスするには、<https://vpp.itunes.apple.com/?l=en>に移動してください。

XenMobileでiOS VPP設定を保存して検証すると、購入したアプリケーションがXenMobileコンソールの **[Configure] > [Apps]** ページの表に追加されます。

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックします。 **[Settings]** ページが開きます。
2. **[Platform]** で **[iOS Settings]** をクリックします。 **[iOS Settings]** 構成ページが開きます。

Settings > iOS Settings

### iOS Settings

Configure these iOS-specific settings. When saved and validated, the Volume Purchase Program (VPP) apps are added to the table on the Apps tab.

Store user password in Secure Hub  ?

User property for VPP country mapping  ?

#### VPP Accounts

<input type="checkbox"/>	Name	Suffix	Organization	Country	Expiration Date	User Login
<input type="checkbox"/>	VPP	VPP	CITRIX SYSTEMS, INC.	United States	04/12/2017 02:57:32 pm	TestAccount@outlook.com

3. 次の設定を構成します。

- **Store user password in Secure Hub** : XenMobile認証用のユーザー名とパスワードをSecure Hubに保存するかどうかを選択します。デフォルトでは、この安全な方法で情報を保存します。
- **User property for VPP country mapping** : ユーザーが国固有のアプリケーションストアからアプリケーションをダウンロードできるようにするコードを入力します。

このマッピングはVPPのプロパティプールの選択に使用されます。たとえば、ユーザープロパティが米国で、アプリ





この構成を完了すると、ユーザーはデバイスを登録できるようになります。以下は、この手順で検討する事項です。

- VPPアプリ設定（ [Configure] > [Apps] ）を構成すると、 [Force license association to device] が有効になります。監視対象デバイスでApple VPPおよびDEPを使用する利点は、XenMobileがアプリをデバイスレベル（ユーザーレベルではなく）で割り当てることができるようになることです。これによって、Apple IDデバイスを使用する必要がなくなり、ユーザーはVPP Programに参加するための招待が必要なく、iTunesアカウントにサインインせずにアプリをダウンロードできるようになります。

The screenshot shows the XenMobile configuration interface for an app. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Configure' tab is active, and the 'Apps' sub-tab is selected. On the left, a sidebar lists 'Public App Store' with a list of platforms: '1 App Information', '2 Platform', '3 Approvals (optional)', and '4 Delivery Group Assignments (optional)'. Under '2 Platform', 'iPhone', 'iPad', and 'Google Play' are checked. The main area is titled 'iPhone App Settings' and contains a search field for the app name 'GoToMeeting'. Below this is the 'App Details' section with fields for 'Name\*', 'Description\*', 'Version' (6.6.5.1134), and 'Image'. There are also toggle switches for 'Paid app' (OFF), 'Remove app if MDM profile is removed' (ON), 'Prevent app data backup' (ON), 'Force app to be managed' (ON), and 'Force license association to device' (ON). The 'Force license association to device' toggle is highlighted with a red box. At the bottom right, there are 'Back' and 'Next >' buttons.

アプリのVPP情報を表示するには、 [Volume Purchase Program] を展開します。 [VPP ID Assignment] の表で、ライセンスがデバイスに関連付けられていることにご注意ください。デバイスのシリアル番号は [Associated Device] 列に表示されます。ユーザーがトークンを削除して再度インポートすると、シリアル番号ではなく「非表示」と表示されます。これはApple社のプライバシー制限によるものです。

XenMobile Analyze Manage **Configure** administrator

Device Policies **Apps** Actions ShareFile Enrollment Profiles Delivery Groups

### Public App Store

- 1 App Information
- 2 Platform
  - iPhone
  - iPad
  - Google Play
  - Android for Work
  - Windows Desktop/Tablet
  - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

Remove app if MDM profile is removed  ON

Prevent app data backup  ON

Force app to be managed  ON ?

Force license association to device  ON

► Deployment Rules

► Store Configuration

▼ Volume Purchase Program

VPP ID Assignment License Usage: 2 of 2

Disassociate

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input type="checkbox"/>	82684302	Used		
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

VPP License Keys

Import

ライセンスの関連付けを解除するには、該当ライセンスの行を選択して[Disassociate] をクリックします。

**Disassociate VPP license**

Are you sure you want to disassociate the selected users with this VPP license ID?

Cancel Disassociate

**VPP ID Assignment**

Disassociate

License Usage: 2 of 2

<input type="checkbox"/>	License ID	Usage Status	Associated User	Associated Device
<input checked="" type="checkbox"/>	82684302	Used	[Redacted]	
<input type="checkbox"/>	82684301	Used		F9FMW440FCM5

Showing 1 - 2 of 2 items

**VPP License Keys**

Import

VPPライセンスをユーザーに関連付けると、XenMobileはユーザーをVPPアカウントに統合し、ユーザーのiTunes IDをVPPアカウントに関連付けます。ユーザーのiTunes IDがユーザーの会社やXenMobileサーバーに表示されることはありません。Apple社はユーザーのプライバシーを確保するために、透過的に関連付けを作成します。ユーザーアカウントからすべてのライセンスの関連付けを解除することで、VPPプログラムからユーザーを削除できます。ユーザーを削除するには、**[Manage] > [Devices]** にアクセスします。

XenMobile Analyze **Manage** Configure admin

Devices Users Enrollment

### Device details

- 1 General
- 2 Properties
- 3 User Properties**
- 4 Assigned Policies
- 5 Apps
- 6 Actions
- 7 Delivery Groups
- 8 iOS Profiles
- 9 iOS Provisioning Profiles
- 10 Certificates
- 11 Connections
- 12 MDM Status

### User Properties

User name: user123

Password: Enter new password

Role\*: USER

Membership:  local\MSP [Manage Groups](#)

VPP Accounts:  VPP [Retire](#)

[Back](#) [Next >](#)

- アプリをデリバリーグループに割り当てると、XenMobileはデフォルトでアプリを任意アプリとして認識します。XenMobileで確実にアプリがデバイスに展開されるようにするには、**[Configure] > [Delivery Groups]** に移動し、**[Apps]** ページでアプリを **[Required Apps]** 一覧に移動します。
- パブリックアプリケーションストアのアプリの更新が使用可能で、アプリがVPP経由でプッシュされる場合、ユーザーが更新をチェックして適用するまで、このアプリは自動的にデバイスで更新されません。たとえば、Secure Hub（ユーザーではなくデバイスに割り当てられている場合）の更新をプッシュするには、プラットフォームページの **[Configure] > [Apps]** で **[Check for Updates]** を選択して更新を適用します。

### Public App Store

- 1 App Information
- 2 Platform
  - iPhone
  - iPad
  - Google Play
  - Android for Work
  - Windows Desktop/Tablet
  - Windows Phone
- 3 Approvals (optional)
- 4 Delivery Group Assignments (optional)

### iPhone App Settings


Type an app name or keyword in the field and search for your desired app. When you click your app in the results, you can configure how the app appears in the store.

#### App Details

**Name\***

**Description\***

**Version**  Check for Updates

**Image** 

**Paid app**  OFF

**Remove app if MDM profile is removed**  ON

**Prevent app data backup**  ON

**Force app to be managed**  ON ⓘ

**Force license association to device**  ON

▶ **Deployment Rules**  
▶ **Store Configuration**  
▶ **Volume Purchase Program**

Back Next >

# Citrix Secure Hubを介したXenAppおよびXenDesktop

Apr 27, 2017

XenMobileでは、XenAppおよびXenDesktopからアプリケーションを収集して、XenMobile Storeでモバイルデバイスユーザーがそのアプリケーションを使用できるようにすることができます。ユーザーは、XenMobile Store内から直接アプリケーションをサブスクライブして、Secure Hubから起動します。アプリケーションを起動するために、Citrix Receiverをユーザーのデバイスにインストールする必要があります。ただし、構成する必要はありません。

この設定を構成するには、Web InterfaceサイトまたはStoreFrontの完全修飾ドメイン名（Fully Qualified Domain Name : FQDN）またはIPアドレスと、ポート番号が必要です。

1. XenMobile Webコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [XenApp/XenDesktop] をクリックします。[XenApp/XenDesktop] ページが開きます。

The screenshot shows the XenMobile Web Console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. On the right, there is a gear icon for settings and a user profile 'admin'. Below the navigation bar, the breadcrumb 'Settings > XenApp/XenDesktop' is visible. The main heading is 'XenApp/XenDesktop' with a sub-heading 'Allows users to add XenApp and XenDesktop through Secure Hub.' The form contains the following fields:

- Host\***: A text input field with the placeholder text 'FQDN or IP address'.
- Port\***: A text input field with the value '80'.
- Relative Path\***: A text input field with the placeholder text 'Example: /Citrix/PNAgent/config.xml'.
- Use HTTPS**: A toggle switch currently set to 'OFF'.

At the bottom right of the form, there are two buttons: 'Cancel' and 'Save'.

3. 次の設定を構成します。

- **Host** : Web InterfaceサイトまたはStoreFrontの完全修飾ドメイン名（FQDN）またはIPアドレスを入力します。
- **Port** : Web InterfaceサイトまたはStoreFrontのポート番号を入力します。デフォルトは80です。
- **Relative Path** : パスを入力します。たとえば、「/Citrix/PNAgent/config.xml」と入力します。
- **Use HTTPS** : Web InterfaceサイトまたはStoreFrontとクライアントデバイスの間で安全な認証を有効にするかどうかを選択します。デフォルトは [OFF] です。

4. [Save] をクリックします。

# リソースの展開

Apr 27, 2017

デバイスの構成および管理は、通常XenMobileでリソース（ポリシーおよびアプリケーション）および操作を作成し、デリバリーグループを使用してそれらをパッケージ化します。XenMobileがリソースおよび操作をデリバリーグループでプッシュする順番は、展開順と呼ばれます。このトピックでは、デリバリーグループを追加、管理、展開する方法、デリバリーグループのリソースや操作の展開順を変更する方法、ユーザーが複数のデリバリーグループに存在し、重複および競合するポリシーがある場合、XenMobileが展開順を決定する方法について説明します。

デリバリーグループによって、ポリシー、アプリケーション、アクションを組み合わせることで展開する対象となるデバイスのユーザーのカテゴリを指定します。通常、デリバリーグループへの追加は、ユーザーの会社、国、部門、オフィスの住所、役職などの特性に基づいて行われます。デリバリーグループを使用することにより、どのユーザーがどのリソースをいつ取得するかを詳細に管理できます。デリバリーグループは、全員に展開することや、より絞り込んで定義したユーザーグループに展開することができます。

デリバリーグループへの展開とは、デリバリーグループに属するiOS、Windows Phone、Windowsタブレットデバイスを持つすべてのユーザーがXenMobileに再接続するようにプッシュ通知を送信することを意味します。これによってデバイスを再評価し、アプリケーション、ポリシー、アクションを展開できるようにします。そのほかのプラットフォームデバイスを持つユーザーは、接続済みの場合は直ちにリソースを受信します。接続済みでない場合は、スケジュール設定ポリシーに基づいて次に接続したときにリソースを受信します。

デフォルトのAllUsersデリバリーグループは、XenMobileをインストールして構成するときに作成されます。このグループには、すべてのローカルユーザーとActive Directoryユーザーが含まれます。AllUsersグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

## 展開順の作成

展開順はXenMobileがリソースをデバイスにプッシュする順番です。展開順はXenMobileのMDMモードでのみサポートされます。

展開順を判断する際、XenMobileはポリシー、アプリ、操作、デリバリーグループにフィルターを適用して条件（展開規則、展開スケジュール）を制御します。デリバリーグループを追加する前に、展開の目的に合わせてこのセクションの情報を参照してください。

以下は、展開順に関する主な概念の要約です。

- **展開順**：XenMobileがリソース（ポリシーやアプリ）および操作をデバイスにプッシュする順序です。契約条件やソフトウェアインベントリのような一部のポリシーの展開順は、ほかのリソースに影響を与えません。アクションが展開される順序はほかのリソースに影響を与えません。したがって、XenMobileでリソースが展開されるとき、リソースの位置は無視されます。
- **展開規則**：XenMobileは、展開規則によってデバイスプロパティを指定して、ポリシー、アプリ、操作、デリバリーグループをフィルター処理できます。たとえば、ドメイン名が特定の値に一致した場合、展開規則が展開パッケージをプッシュするよう指定できます。
- **展開スケジュール**：XenMobileは、展開スケジュールを使用して、操作、アプリ、デバイスポリシーを指定し、これらのアイテムの展開を制御できます。展開が即座に実行されるか、特定の日時に実行されるか、展開条件に従って実行されるかを指定できます。



以下の表は、特定のオブジェクトまたはリソースに関連付けてこれらをフィルター処理したり、これらの展開を制御するさまざまな条件です

オブジェクト/リソース	フィルター/制御条件
デバイスポリシー	デバイスのプラットフォーム デバイスプロパティに基づく展開規則 展開スケジュール
アプリ	デバイスのプラットフォーム デバイスプロパティに基づく展開規則 展開スケジュール
アクション	デバイスプロパティに基づく展開規則 展開スケジュール
デリバリーグループ	ユーザー/グループ デバイスプロパティに基づく展開規則

通常的环境下、複数のデリバリーグループが単一ユーザーに割り当てられ、次のような状況が発生する可能性があります。

- デリバリーグループ内に重複したオブジェクトが存在する。
- 1つ以上のデリバリーグループが単一ユーザーに割り当てられることによって、特定のポリシーに異なる構成が存在する。

このような状況が発生した場合、XenMobileは、デバイスに配布し実行するすべてのオブジェクトの展開順を計算します。計算の手順はデバイスプラットフォームに共通です。

計算の手順：

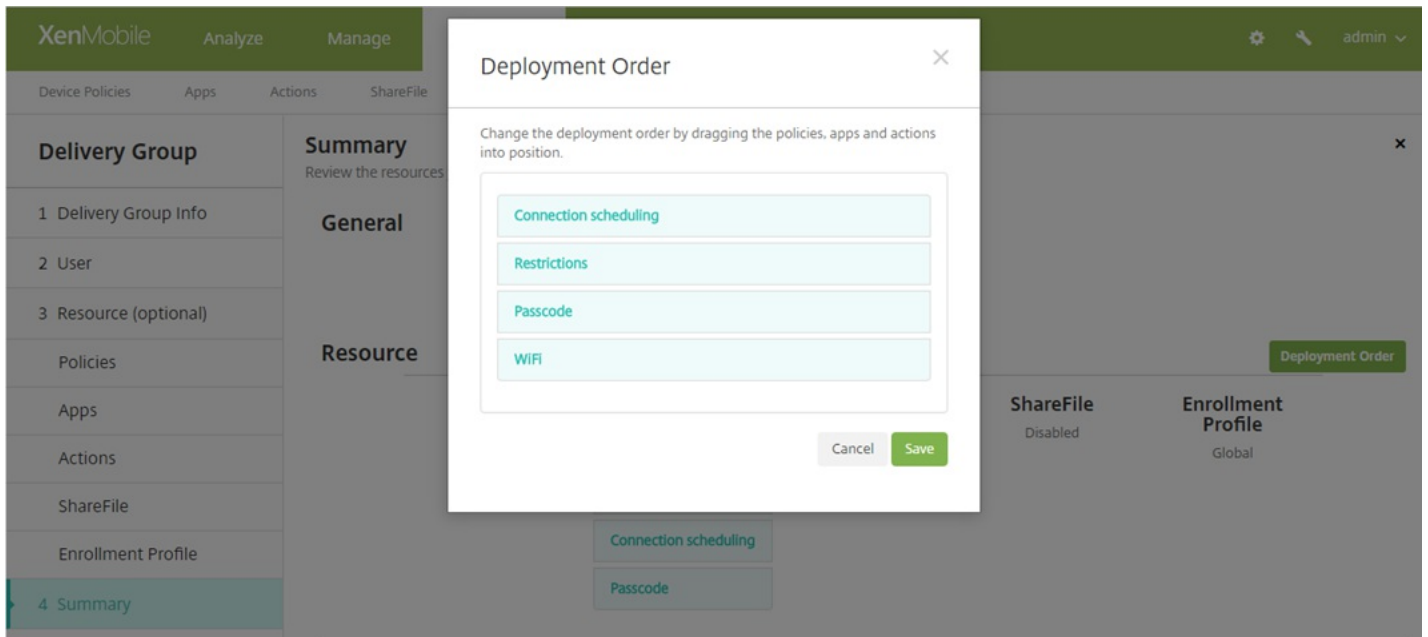
1. ユーザーやグループのフィルターおよび展開規則に基づいて、特定のユーザーが存在するすべてのデリバリーグループを判断します。
2. 選択されたデリバリーグループ内で、デバイスプラットフォーム、展開規則、展開スケジュールのフィルターが適用されるすべてのリソース（ポリシー、操作、アプリ）の順序一覧を作成します。順序のアルゴリズムは、次のとおりです。
  - a. ユーザー定義の展開順があるデリバリーグループのリソースを、展開順がないデリバリーグループの前に配置します。こうする理由は、これらの手順の後に説明します。
  - b. 同じ条件のデリバリーグループの中から、デリバリーグループ名に従ってリソースを順序付けします。たとえば、デリバリーグループAのリソースをデリバリーグループBの前に配置します。
  - c. 並べ替え中、デリバリーグループのリソースにユーザー定義の展開順が指定されている場合、その順序を保持します。そうでない場合は、デリバリーグループ内でリソースをリソース名で並べ替えることができます。

d. 同じリソースが複数回表示される場合、重複するリソースを削除します。

リソースに関連したユーザー定義の順序を持つリソースを、ユーザー定義の順序のないリソースの前に展開します。リソースは、ユーザーに割り当てられた複数のデリバリーグループに存在する可能性があります。上記の手順で示されたように、計算のアルゴリズムは余分なリソースを削除し、この一覧の最初のリソースのみを配布します。この方法で重複するリソースを削除することによって、XenMobile管理者が定義する順序をXenMobileに適用します。

たとえば、次のような2つのデリバリーグループがあるとします。

- デリバリーグループ、Account Manager1：リソースの順序が**未指定**で、**WiFi**ポリシーおよび**Passcode**ポリシーを含みません。
- デリバリーグループ、Account Manager2：リソースの順序が**指定**されていて、**Connection scheduling**ポリシー、**Restrictions**ポリシー、**Passcode**ポリシー、**WiFi**ポリシーを含みます。この事例では、**WiFi**ポリシーの前に**Passcode**ポリシーを配信するように指定されます。



計算アルゴリズムが名前のみを基準に展開グループを順序づけた場合、XenMobileはデリバリーグループAccount Manager 1から開始して、次の順序で展開を実行します：**WiFi**、**Passcode**、**Connection scheduling**および**Restrictions**。XenMobileは、Account Manager 2デリバリーグループの重複する**Passcode**および**WiFi**を無視します。

ただし、Account Manager 2グループには管理者が指定した展開順序があるため、計算アルゴリズムは、Account Manager 2デリバリーグループからのリソースを、Account Manager 1デリバリーグループからのものより一覧で上位に配置します。結果的に、XenMobileはポリシーを次の順序で展開します。**Connection scheduling**、**Restrictions**、**Passcode**、**WiFi**。XenMobileは、Account Manager 1デリバリーグループからのポリシー**WiFi**および**パスコード**を無視します。重複しているためです。このアルゴリズムは、XenMobile管理者によって指定された順序を優先します。

デリバリーグループを追加するには

1. XenMobileコンソールで、**[Configure]** の **[Delivery Groups]** をクリックします。**[Delivery Groups]** ページが開きます。

**Delivery Groups** [Show filter](#)

[Add](#) | [Export](#)

<input type="checkbox"/>	Status	Name	Last Updated	Disabled
<input type="checkbox"/>		AllUsers		
<input type="checkbox"/>		Domain users	Jun 13 2016 5:10 PM	
<input type="checkbox"/>		Sales	Apr 13 2016 12:50 PM	

2. [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。

**Delivery Group Information** ×

Enter a name for the delivery group and any information that will help you keep track of it later.

**Name**

**Description**

3. [Delivery Group Information] ページで、以下の情報を入力します。

- **Name** : デリバリーグループの説明的な名前を入力します。
- **Description** : 任意で、デリバリーグループの説明を入力します。

4. [Next] をクリックします。[User Assignments] ページが開きます。

5. 次の設定を構成します。

- **Select domain** : 一覧から、ユーザーを選択するドメインを選択します。
- **Include user groups** : 次のいずれかを行います。
  - ユーザーグループの一覧で、追加するグループを選択します。選択したグループが[**Selected user groups**] 一覧に表示されます。
  - - [**Search**] をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - - グループ名の全体または一部を検索ボックスに入力して [**Search**] をクリックし、ユーザーグループの一覧を絞り込みます。
    - [**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。
      - [**Selected user groups**] の一覧で、削除する各グループの横にある [**X**] をクリックします。
      - - [**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。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
      - - グループ名の全体または一部を検索ボックスに入力して [**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。一覧をスクロールし、削除する各グループのチェックボックスをオフにします。
- **Or/And** : リソースが展開されるユーザーがいずれかのグループに属していればよいか ( [**Or**] ) 、すべてのグループに属している必要があるか ( [**And**] ) を選択します。
- **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。

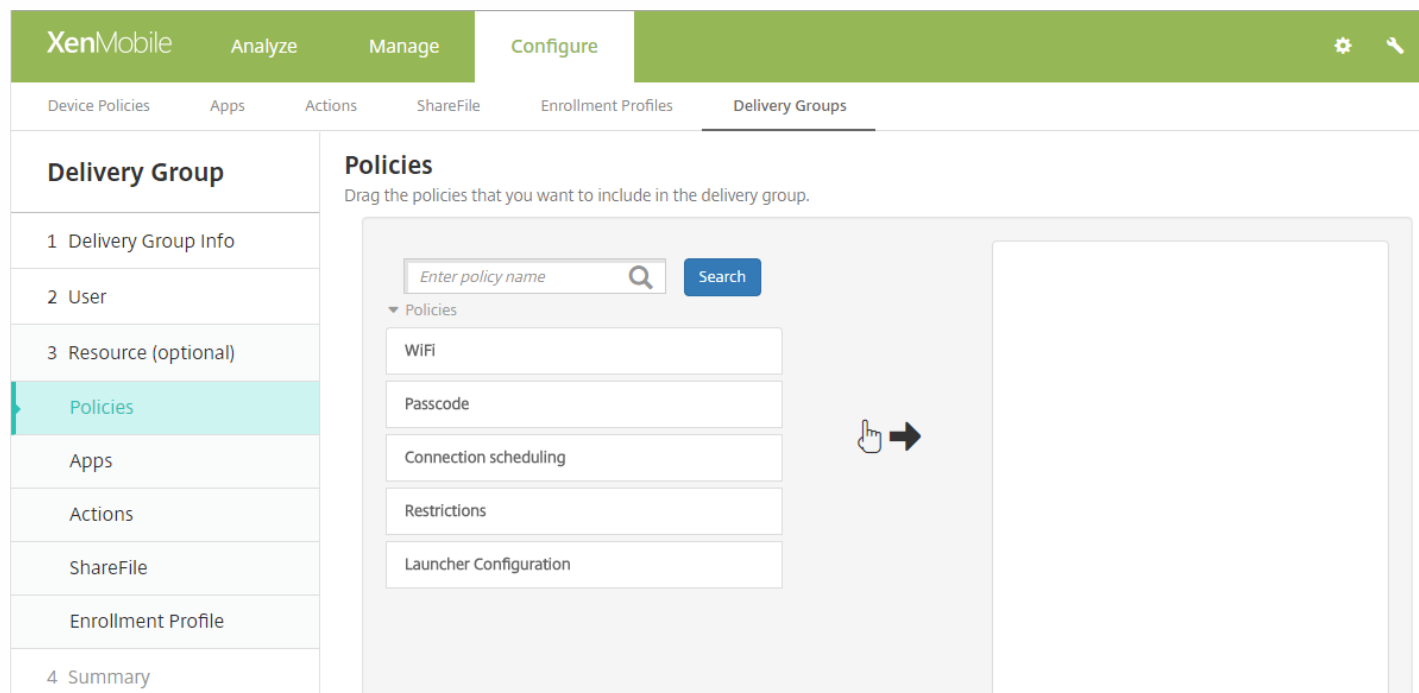
注 : 認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

## 6. 展開規則を構成します。

デリバリーグループに任意のリソースを追加するには

任意のリソースをデリバリーグループに追加して、特定のポリシーを追加したり、必須および任意のアプリケーションを提供したり、自動アクションを追加したり、コンテンツおよびデータへのシングルサインオンに対してShareFileを有効にしたりすることができます。次のセクションでは、ポリシー、アプリケーション、アクションを追加する方法と、ShareFileを有効にする方法について説明します。デリバリーグループには、これらのリソースの一部またはすべてを追加できます。また、何も追加しないでおくこともできます。リソースの追加をスキップするには、**[Summary]** をクリックします。

## ポリシーの追加



The screenshot shows the XenMobile interface. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. Below this, there are tabs for 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Delivery Groups' tab is active, and a sidebar on the left lists 'Delivery Group' with sub-items: '1 Delivery Group Info', '2 User', '3 Resource (optional)', 'Policies' (highlighted), 'Apps', 'Actions', 'ShareFile', 'Enrollment Profile', and '4 Summary'. The main content area is titled 'Policies' and contains the instruction 'Drag the policies that you want to include in the delivery group.' Below this is a search box labeled 'Enter policy name' with a 'Search' button. A list of policies is shown: 'WiFi', 'Passcode', 'Connection scheduling', 'Restrictions', and 'Launcher Configuration'. A hand icon with an arrow points from the 'WiFi' policy towards the right, indicating it can be dragged.

1. 追加するポリシーごとに、以下の操作を行います。

- 使用可能なポリシーの一覧をスクロールして、追加するポリシーを見つけます。
- または、ポリシーの一覧を絞り込むため、検索ボックスにポリシー名の全体または一部を入力して**[Search]** をクリックします。
- 追加するポリシーをクリックして、右側のボックス内へドラッグします。

注：ポリシーを削除するには、右側のボックス内のポリシー名の横にある**[X]** をクリックします。

2. **[Next]** をクリックします。 **[Apps]** ページが開きます。

## アプリケーションの追加

1. 追加するアプリケーションごとに、以下の操作を行います。

- 使用可能なアプリケーションの一覧をスクロールして、追加するアプリケーションを見つけます。
- または、アプリケーションの一覧を絞り込むため、検索ボックスにアプリケーション名の全体または一部を入力して **[Search]** をクリックします。
- 追加するアプリケーションをクリックして、**[Required Apps]** ボックス内または **[Optional Apps]** ボックス内へドラッグします。

注：アプリケーションを削除するには、右側のボックス内のアプリケーション名の横にある **[X]** をクリックします。

2. **[Next]** をクリックします。 **[Actions]** ページが開きます。

## アクションの追加

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

### Delivery Group

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
  - Policies
  - Apps
  - Actions**
  - ShareFile
  - Enrollment Profile
- 4 Summary


### Actions

Drag the actions that you want to include in the delivery group.

Enter action name

▼ Actions

- Action - Out of compliance
- Action - Send notification



1. 追加するアクションごとに、以下の操作を行います。

- 使用可能なポリシーの一覧をスクロールして、追加するアクションを見つけます。
- または、アクションの一覧を絞り込むため、検索ボックスにアクション名の全体または一部を入力して[Search] をクリックします。
- 追加するアクションをクリックして、右側のボックス内へドラッグします。

注：操作を削除するには、右側のボックス内の操作名の横にある [X] をクリックします。

2. [Next] をクリックします。[ShareFile] ページが開きます。

## ShareFile の有効化

XenMobile Analyze Manage **Configure**

Device Policies Apps Actions ShareFile Enrollment Profiles **Delivery Groups**

**Delivery Group**

- 1 Delivery Group Info
- 2 User
- 3 Resource (optional)
- Policies
- Apps
- Actions
- ShareFile**
- Enrollment Profile
- 4 Summary

**ShareFile**  
Enable ShareFile to provide users in the delivery group with single sign-on (SSO) access to content and data.

Enable ShareFile  OFF

1. 次の設定を構成します。

- **Enable ShareFile** : [ON] を選択して、コンテンツおよびデータへのShareFileシングルサインオンアクセスを有効にします。

2. [Next] をクリックします。[Summary] ページが開きます。

登録プロファイル



The screenshot shows the XenMobile interface with the 'Configure' tab selected. The 'Delivery Groups' sub-tab is active. On the left, a 'Delivery Group' sidebar lists steps: 1 Delivery Group Info, 2 Resource (optional), Policies, Apps, Actions, ShareFile, Enrollment Profile (highlighted), and 3 Summary. The main content area is titled 'Enrollment Profile' and contains the instruction: 'Select the enrollment profile that you want the users in this delivery group to see'. Below this, there are two radio buttons: 'Enrollment Profile' (disabled) and 'Global' (selected).

1. 次の設定を構成します。

- **登録プロファイル**：登録プロファイルを選択します。登録プロファイルを作成するには、「[デバイス登録の制限](#)」を参照してください。

2. **[Next]** をクリックします。 **[Summary]** ページが開きます。

構成したオプションの確認および展開順序の変更

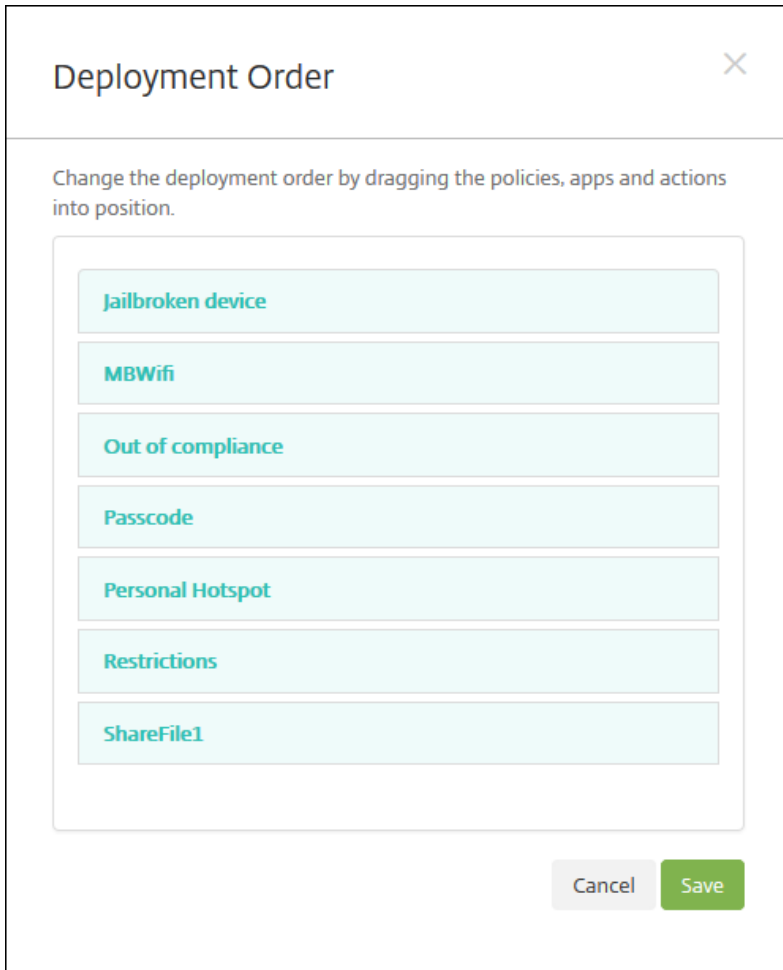
The screenshot shows the XenMobile interface with the 'Configure' tab selected. The 'Delivery Groups' sub-tab is active. On the left, a 'Delivery Group' sidebar lists steps: 1 Delivery Group Info, 2 User, 3 Resource (optional), Policies, Apps, Actions, ShareFile, Enrollment Profile, and 4 Summary (highlighted). The main content area is titled 'Summary' and contains the instruction: 'Review the resources you are about to assign to the delivery group.' Below this, there are sections for 'General' and 'Resource'. The 'General' section has a 'Name' field with 'Local' entered and a 'Description' field. The 'Resource' section shows a list of resources with their counts and status: Apps (0), Policies (0), Actions (0), ShareFile (Disabled), and Enrollment Profile (Global). A 'Deployment Order' button is visible in the top right corner of the resource list.

[Summary] ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。  
[Summary] ページには、リソースがカテゴリ別に表示されます。展開順序を反映してはいません。

1. 構成の調整が必要な場合は、[Back] をクリックして前のページに戻ります。
2. 展開順序を表示するか、展開順序を並べ替えるには、[Deployment Order] をクリックします。
3. [Save] をクリックして、デリバリーグループを保存します。

展開順を変更するには

1. [Deployment Order] をクリックします。[Deployment Order] ダイアログボックスが開きます。



2. リソースをクリックして展開する場所にドラッグします。展開順序を変更すると、一覧の上から下への順にリソースが展開されます。

3. **[Save]** をクリックして、展開順序を保存します。

デリバリーグループを編集するには

1. **[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、編集するデリバリーグループを選択し、**[Edit]** をクリックします。**[Delivery Group Information]** 編集ページが開きます。

## 注意

デリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に**[Edit]** コマンドが表示されます。

2. **[Description]** ボックスに説明を追加するか、または既存の説明を変更します。

注：既存のグループの名前は変更できません。

**[Next]** をクリックします。**[User Assignments]** ページが開きます。

4. **[Select User Groups]** ページで、以下の情報を入力または変更します。

- **Select domain** : 一覧から、ユーザーを選択するドメインを選択します。
- **ユーザーグループを含める** : 次のいずれかを行います。
  - ユーザーグループの一覧で、追加するグループを選択します。選択したグループが**[Selected user groups]** 一覧に表示されます。
  - - **[Search]** をクリックして、選択したドメイン内のすべてのユーザーグループの一覧を表示します。
  - - グループ名の全体または一部を検索ボックスに入力して**[検索]** をクリックし、ユーザーグループの一覧を絞り込みます。

注 : ユーザーグループを削除するには、**[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。

- **Or/And** : 展開対象のユーザーがいずれかのグループに属していればよいか ( **[Or]** )、すべてのグループに属している必要があるか ( **[And]** ) を選択します。
- **Deploy to anonymous user** : デリバリーグループ内の認証が不要なユーザーに展開するかどうかを選択します。

注 : 認証が不要なユーザーとは、ユーザーを認証できなかったものの、デバイスをXenMobileに接続することを許可したユーザーを指します。

5. **[Deployment Rules]** を展開し、前に述べた手順の手順5で実行したように、設定を構成します。

6. **[Next]** をクリックします。 **[Delivery Group Resources]** ページが開きます。このページでポリシー、アプリケーション、アクションを追加または削除します。この手順をスキップするには、 **[Delivery Group]** の **[Summary]** をクリックしてデリバリーグループ構成の概要情報を表示します。
7. リソースの変更が完了したら、 **[Next]** をクリックするか、 **[Delivery Group]** の **[Summary]** をクリックします。
8. **[Summary]** ページで、デリバリーグループに対して構成したオプションを確認し、リソースの展開順を変更できます。
9. 構成の調整が必要な場合は、 **[Back]** をクリックして前のページに戻ります。
10. リソースの展開順序を並べ替えるには **[Deployment Order]** をクリックします。展開順序の変更については、「[展開順序を変更するには](#)」を参照してください。
11. **[Save]** をクリックして、デリバリーグループを保存します。

AllUsersデリバリーグループを有効化および無効化するには

## 注意

AllUsersは、有効化または無効化することができる唯一のデリバリーグループです。

1. **[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、Windowsタブレットデバイスを持つすべてのユーザーがXenMobileに再接続できるようにプッシュ通知を送信することを意味します。これによってデバイスを再評価し、アプリケーション、ポリシー、アクションを展開できるようにします。そのほかのプラットフォームデバイスを持つユーザーは、接続済みの場合は直ちにリソースを受信します。接続済みでない場合は、スケジュール設定ポリシーに基づいて次に接続したときにリソースを受信します。

注：ユーザーのAndroidデバイスで、XenMobile 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。

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。

The screenshot displays the 'Delivery Groups' management page. At the top, there are 'Add' and 'Export' buttons, a search bar, and a 'Show filter' link. Below is a table with columns for 'Status', 'Name', 'Last Updated', and 'Disabled'. Three groups are listed: 'AllUsers', 'sales', and 'DG for CAT'. The 'sales' group is highlighted in green and shows a deployment status of 'Oct 26 2015 12:48 PM'. An overlay window is open over the 'sales' group, showing deployment statistics: 1 Installed, 0 Pending, and 0 Failed. The 'Status' column header and the 'Deployment' overlay are highlighted with a purple box.

デリバリーグループを削除するには

## 注意

AllUsersデリバリーグループは削除できませんが、リソースをユーザーすべてにはプッシュしない場合、このグループを無効にできます。

1. **[Delivery Groups]** ページで、次のいずれかを行います。

- 複数のデリバリーグループを同時に削除するには、削除するグループの横にあるチェックボックスをオンにします。
- 1つのデリバリーグループを削除するには、グループ名の横にあるチェックボックスをオンにするか、グループ名を含む行

をクリックします。

2. **[Delete]** をクリックします。 **[Delete]** ダイアログボックスが開きます。

注：1つのデリバリーグループを選択した方法に応じて、デリバリーグループの上または右側に**[Delete]** コマンドが表示されます。

3. **[Delete]** をクリックします。

## Important

このアクションを元に戻すことはできません。

[Delivery Groups] の表をエクスポートするには

1. **[Delivery Groups]** の表の上にある **[Export]** をクリックします。XenMobileによって **[Delivery Groups]** の表の情報が抽出され、.csvファイルに変換されます。

2. .csvファイルを開くか、保存します。使用するブラウザーに応じて、手順が異なります。操作を取り消すこともできます。

# マクロ

Apr 27, 2017

XenMobileでは、強力なマクロが提供されています。マクロにはいろいろな用途がありますが、たとえば、プロフィール、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プロフィールにユーザーのメールアドレスの値を事前に設定できます。

この機能は現在、iOSおよびAndroidデバイスの構成とテンプレートの場合にのみ使用できます。

## ユーザーマクロの定義

以下のユーザーマクロは常に使用できます。

- loginname (ユーザー名とドメイン名)
- username (loginnameからドメイン名を除去したもの、ある場合)
- domainname (ドメイン名またはデフォルトドメイン)

以下の管理者が定義するプロパティも使用できる場合があります。

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename
- postalcode
- postofficebox



- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (前述のプロパティを上書きします)

さらに、ユーザーがLDAPなどの認証サーバーを使用して認証されている場合、そのストアでユーザーに関連付けられているすべてのプロパティを使用できます。

## マクロの構文

マクロの形式は次のとおりです。

- `${type.PROPERTYNAME}`
- `${type.PROPERTYNAME ['DEFAULT VALUE'] [ | FUNCTION [(ARGUMENT1, ARGUMENT2)]]}`

原則として、ドル記号 (\$) に続くすべての構文は中かっこ ({} ) で囲む必要があります。

- 修飾されたプロパティ名は、ユーザープロパティ、デバイスプロパティ、またはカスタムプロパティを示します。
- 修飾されたプロパティ名は、プレフィックスと実際のプロパティ名で構成されます。
- ユーザープロパティの形式は、`${user.[PROPERTYNAME] (prefix="user.")}` です。
- デバイスプロパティの形式は、`${device.[PROPERTYNAME] (prefix="device.")}` です。

たとえば、`${user.username}` はポリシーのテキストフィールドにユーザー名の値を設定します。これは、複数のユーザーが使用する Exchange ActiveSync プロファイルおよびそのほかのプロファイルを構成するのに便利です。

カスタムマクロ (ユーザーが定義するプロパティ) の場合、プレフィックスは `${custom}` です。プレフィックスは省略できます。

注: プロパティ名の大文字と小文字は区別されます。

# 自動化された操作

Apr 27, 2017

XenMobileで自動化された操作を作成して、イベント、ユーザー、デバイスプロパティ、またはユーザーデバイスでのアプリケーションの存在に対する対応をプログラミングします。自動化された操作を作成する場合は、操作のトリガーに基づいてユーザーのデバイスがXenMobileに接続されたときに、そのデバイスに及ぼす効果を設定します。イベントがトリガーされたときに、より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信できます。

たとえば、事前にブラックリストに追加したアプリケーション（例：Words with Friends）を検出する場合は、ユーザーのデバイスでWords with Friendsが検出されたときに、そのデバイスをコンプライアンス違反に設定するトリガーを指定できます。この操作では次に、そのアプリケーションを削除して、デバイスが再度コンプライアンス遵守状態に戻す必要があることが通知されます。デバイスを選択的にワイプするなどのより深刻な操作を実行するまでに、ユーザーがコンプライアンス遵守状態に戻すのを待機する時間制限を設定できます。

ユーザーのデバイスがコンプライアンス不遵守状態になった後で、デバイスがコンプライアンス遵守状態になるようユーザーがデバイスを修正した場合、デバイスをコンプライアンス遵守状態にリセットするパッケージを展開するようポリシーを構成する必要があります。

自動的に発生する効果は、次の範囲から設定します。

- デバイスに選択的ワイプまたは完全なワイプを実行する。
- デバイスをコンプライアンス不遵守に設定する。
- デバイスを取り消す。
- より深刻な操作が実行される前に問題を修正するよう、ユーザーに通知を送信する。

この記事では、XenMobileでの自動化された操作の追加、編集、フィルターの手法、およびアプリロックおよびアプリワイプ操作をMAM-onlyモード用に構成する方法について説明します。

## 注意

ユーザーに通知するには、XenMobileがメッセージを送信できるように、[Settings] で通知サーバー（SMTPおよびSMS）を構成している必要があります。次を参照してください。[XenMobileでの通知](#)。また、続行する前に使用予定の通知テンプレートを設定します。通知テンプレートの設定について詳しくは、「[XenMobileで通知テンプレートを作成または更新するには](#)」を参照してください。

1. XenMobileコンソールで、**[Configure]** の **[Actions]** をクリックします。**[Actions]** ページが開きます。

2. **[Actions]** ページで、次のいずれかを行います。

- 新しい操作を追加するには **[Add]** をクリックします。
- 編集または削除する既存の操作を選択します。使用するオプションをクリックします。

注：操作の横にあるチェックボックスをオンにすると、操作一覧の上にオプションメニューが表示されます。一覧のそのほかの場所をクリックすると、一覧の右側にオプションメニューが表示されます。

3. **[Action Information]** ページが開きます。

4. **[Action Information]** ページで、次の情報を入力または変更します。

- **Name** : 操作を一意に識別する名前を入力します。このフィールドは必須です。
- **Description** : 操作の意図する内容を説明します。

5. **[Next]** をクリックします。 **[Action details]** ページが開きます。

注 : 次の例では**Event**トリガーの設定方法を示します。別のトリガーを選択した場合、この図で示されているものとは異なるオプションになります。

The screenshot shows the XenMobile interface for configuring an action. The top navigation bar includes 'XenMobile', 'Analyze', 'Manage', and 'Configure'. The main navigation menu has 'Device Policies', 'Apps', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Actions' section is active, showing a sidebar with '1 Action Info', '2 Details', '3 Assignment (optional)', and '4 Summary'. The 'Action details' form is open, with the following fields:

- Trigger\***: A dropdown menu with the text 'Select a trigger'.
- Action\***: A dropdown menu with the text 'Select an action'.
- Summary**: A text area containing the prompt 'If **CONDITION IS FULFILLED**, then **DO ACTION**'.

Below the form, there is a list of deployment rules:

- ▶ Deployment Rules (iOS)
- ▶ Deployment Rules (Mac OS X)
- ▶ Deployment Rules (Android)
- ▶ Deployment Rules (Windows Mobile/CE)
- ▶ Deployment Rules (Windows Desktop/Tablet)
- ▶ Deployment Rules (Windows Phone)

At the bottom right, there are 'Back' and 'Next >' buttons.

6. **[Action details]** ページで、次の情報を入力または変更します。

- **[Trigger]** の一覧で、この操作に対するイベントトリガーの種類をクリックします。各トリガーの意味は次のとおりです。
  - **Event** : 定義済みのイベントに対応します。
  - **Device property** : MDMモードで収集されたデバイスのデバイス属性を確認して、それに対応します。
  - **User property** : ユーザー属性 (通常、Active Directoryからの属性) に対応します。
  - **Installed app name** : インストール中のアプリケーションに対応します。MAM-onlyモードには適用されません。デバイスでアプリケーションインベントリポリシーを有効にする必要があります。デフォルトでは、アプリケーションインベントリポリシーはすべてのプラットフォームで有効です。詳しくは、「[アプリケーションインベントリデバイスポリシーを追加するには](#)」を参照してください。

7. 次の一覧で、トリガーに対する応答をクリックします。

8. **[Action]** の一覧で、トリガーの条件が満たされたときに実行される操作をクリックします。 **[Send notification]** 以外では、トリガーの原因となった問題をユーザーが解決できる期間を選択します。その期間内に問題が解決されない場合は、選択した操作が実行されます。実行できるアクションは次のとおりです。

- **Selectively wipe the device** : 個人のデータとアプリケーションは残して、企業のすべてのデータとアプリケーションをデバイスから消去します。

- **Completely wipe the device** : デバイスからすべてのデータやアプリケーションを消去します。デバイスに装備されている場合、メモリカードもその対象となります。
- **Revoke the device** : デバイスからXenMobileへの接続を禁止します。
- **App lock** : デバイスのすべてのアプリケーションへのアクセスを拒否します。Androidでは、ユーザーはまったくXenMobileにログインできなくなります。iOSでは、ユーザーはまだログインできますが、アプリケーションにアクセスできません。詳しくは、この記事で後述する「MAM-onlyモードでのアプリロックとアプリワイプ操作」を参照してください。
- **App wipe** : Androidでは、これによりユーザーのXenMobileアカウントが削除されます。iOSでは、これにより、ユーザーがXenMobile機能にアクセスするために必要な暗号キーが削除されます。詳しくは、この記事で後述する「MAM-onlyモードでのアプリロックとアプリワイプ操作」を参照してください。
- **Mark the device as out of compliance** : デバイスを規則違反として設定します。
- **Send notification** : ユーザーへのメッセージの送信します。

[Send notification] を選択すると、以降の手順で通知の送信方法について説明します。

9. 次の一覧で、通知に使用するテンプレートを選択します。選択したイベントに関連した通知テンプレートが表示されます（通知の種類に既にテンプレートが存在する場合）。テンプレートがない場合、テンプレートの構成を促す次のメッセージが表示されます：このイベントの種類にテンプレートがありません（No template for this event type.） [\[Settings\]](#) の通知テンプレートでテンプレートを作成します。

注：ユーザーに通知するには、XenMobileがメッセージを送信できるように、[Settings] で通知サーバー（SMTPおよびSMS）を構成している必要があります。次を参照してください。 [XenMobileでの通知](#)。また、続行する前に使用予定の通知テンプレートを設定します。通知テンプレートの設定について詳しくは、「[XenMobileで通知テンプレートを作成または更新するには](#)」を参照してください。

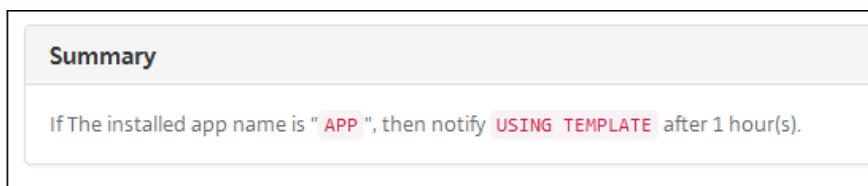
注：テンプレートを選択した後、[Preview notification message] をクリックして通知をプレビュー表示できます。

10. 以下のフィールドで、操作が実行されるまでの遅延（日単位、時間単位、または分単位）と、トリガーの原因となった問題をユーザーが解決するまでに操作を繰り返す間隔を設定します。



The screenshot shows a configuration form with four input fields. The first field contains the number '1'. The second field is a dropdown menu currently set to 'Hours'. The third field contains the number '0'. The fourth field is a dropdown menu currently set to 'Minutes'.

11. **[Summary]** で、意図したとおりに、自動化された操作を作成したことを確認します。



The screenshot shows the 'Summary' section of a configuration form. It contains the text: 'If The installed app name is " APP ", then notify USING TEMPLATE after 1 hour(s).'

12. アクション詳細を構成したら、プラットフォームごとに個別に展開規則を構成できます。これを行うには、選択した各プラットフォームに対して、手順13を実行します。

### 13. 展開規則を構成します

14. 操作のプラットフォームの展開規則の構成が完了したら、**[Next]** をクリックします。**[Actions]** 割り当てページが開きます。ここで操作をデリバリーグループに割り当てます。この手順はオプションです。

15. **[Choose delivery groups]** の横に、ポリシーを割り当てるデリバリーグループを入力して検索するか、一覧でグループを選択します。選択したグループが右側の **[Delivery groups to receive app assignment]** の一覧に表示されます。

16. **[Deployment Schedule]** を展開して以下の設定を構成します。

- **[Deploy]** の横の **[ON]** をクリックすると展開がスケジュールされ、**[OFF]** をクリックすると展開が行われません。デフォルトのオプションは **[ON]** です。**[OFF]** を選択した場合、そのほかのオプションを構成する必要はありません。
- **[Deployment schedule]** の横の **[Now]** または **[Later]** をクリックします。デフォルトのオプションは **[Now]** です。
- **[Later]** をクリックした場合は、カレンダーアイコンをクリックして展開日時を選択します。
- **[Deployment condition]** の横の **[On every connection]** をクリックするか、**[Only when previous deployment has failed]** をクリックします。デフォルトのオプションは、**[On every connection]** です。
- **[Deploy for always-on connection]** の横の **[ON]** または **[OFF]** をクリックします。デフォルトのオプション

は [OFF] です。

注：このオプションは、[Settings] の [Server Properties] において、バックグラウンドで展開するキーのスケジュールを構成した場合に適用されます。常時接続オプションは、iOSデバイスでは使用できません。

注：構成した展開スケジュールはすべてのプラットフォームについて同一です。すべてのプラットフォームに変更が適用されます。ただしiOSには、[Deploy for always on connection] は適用されません。

17. [Next] をクリックします。[Summary] ページが開きます。ここで操作の構成を確認できます。

18. [Save] をクリックして変更を保存します。

### MAM-onlyモードでのアプリロックとアプリワイプ操作

XenMobileにリストされたトリガーの4つのカテゴリすべてに応じて、デバイスでアプリケーションをワイプまたはロックできます。4つのカテゴリは、Event、Device property、User property、Installed app nameです。

自動でアプリのワイプまたはロックを構成するには

1. XenMobileコンソールで、[Configure] の [Actions] をクリックします。
2. [Actions] ページで、[Add] をクリックします。
3. [Action Information] ページで、アクションの名前および必要に応じて説明を入力します。
4. [Action Details] ページで、目的のトリガーを選択します。
5. [Action] でアクションを選択します。

この段階で、以下の条件に注意してください。

トリガーの種類がEvent で、値がActive Directory disabled userではない場合、[App wipe] および [App lock] アクションは表示されません。

トリガーの種類がDevice propertyで値がMDM lost mode enabledである場合、次のアクションが表示されます。

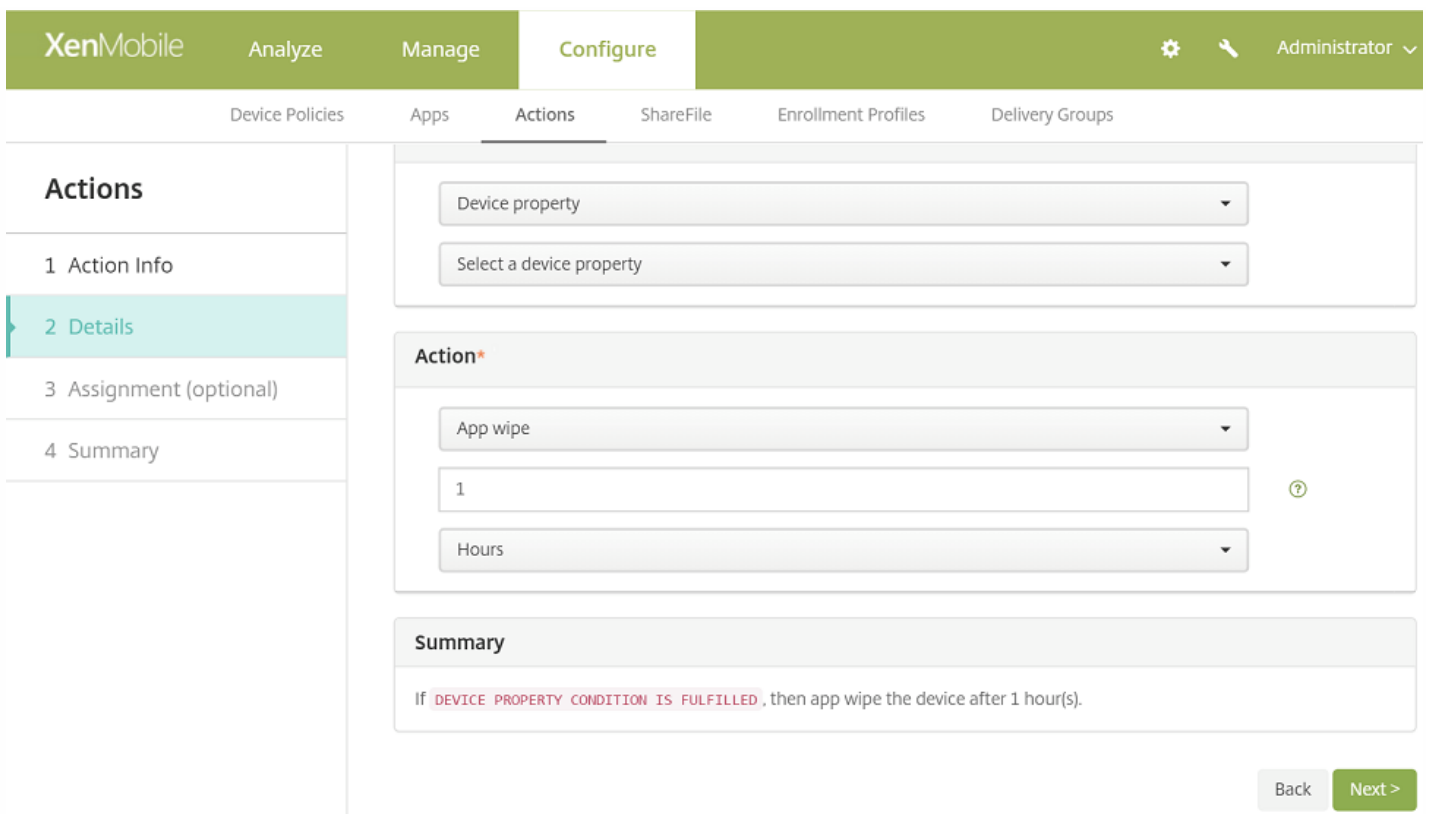
- デバイスを選択的にワイプ
- デバイスを完全にワイプ
- デバイスを取り消す

各オプションでは、自動で1時間の遅延が設定されていますが、遅延の期間は分単位、時間単位、日数単位を選択できます。遅延によって、ユーザーはアクションを実行する前に、修正のための時間を確保できます（修正が可能な場合）。アプリのワイプとアプリのロックについて詳しくは、「RBACを使用した役割の構成」を参照してください。

## 注意

トリガーをeventに設定すると、繰り返し間隔は自動的に最小1時間となります。通知を生成するには、デバイスはポリシーの更新を実行して、サーバーと同期する必要があります。通常、ユーザーのサインオン時、またはSecure Hubでポリシーを手動で更新すると、デバイスはサーバーと同期します。

Active DirectoryデータベースとXenMobileとの同期を許可するアクションが実行される前に、さらに約1時間、遅延を追加できます。



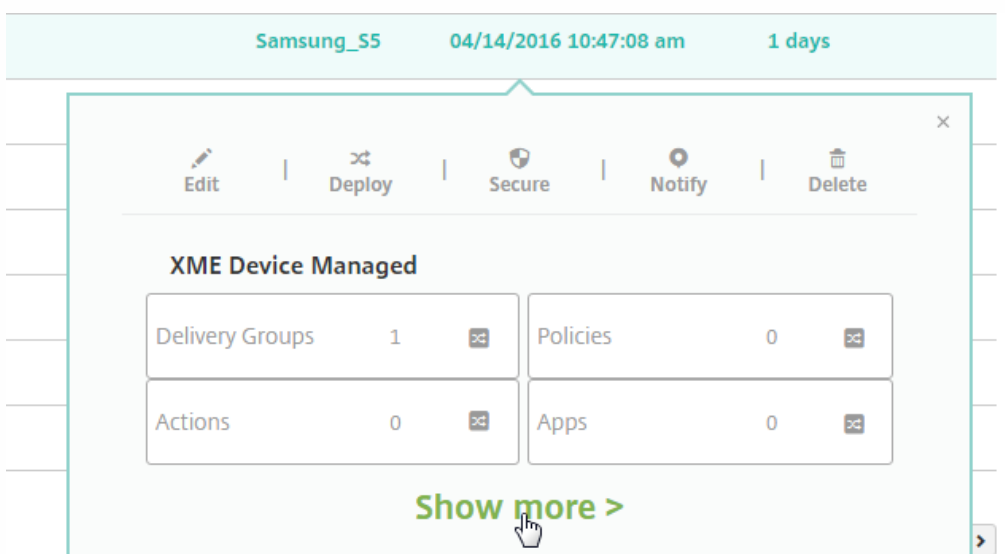
6. 展開規則を構成して、[Next] をクリックします。

7. デリバリーグループの割り当てと展開スケジュールを構成して、[Next] をクリックします。

8. [Save] をクリックします。

アプリロックとアプリワイプの状態を確認するには

1. [Manage] > [Devices] に移動し、デバイスをクリックしてから [Show more] をクリックします。



2. [Device App Wipe] および [Device App Lock] までスクロールします。

**Device details**

- 1 General
- 2 Properties
- 3 User Properties
- 4 Assigned Policies
- 5 Apps
- 6 Actions
- 7 Delivery Groups
- 8 Certificates
- 9 Connections
- 10 TouchDown

WiFi MAC Address	NONE
Bluetooth MAC Address	NONE
Device Ownership	<input type="radio"/> Corporate <input type="radio"/> BYOD
<b>Security</b>	
Strong ID	YEMXRMSG
Full Wipe of Device	No device wipe.
Selective Wipe of Device	No device selective wipe.
Lock Device	No device lock.
Device locate	No device locate.
Device App Wipe	No device App Wipe.
Device App Lock	App Lock was requested at 04/15/2016 01:59:47 pm.

[Next >](#)



# モニターとサポート

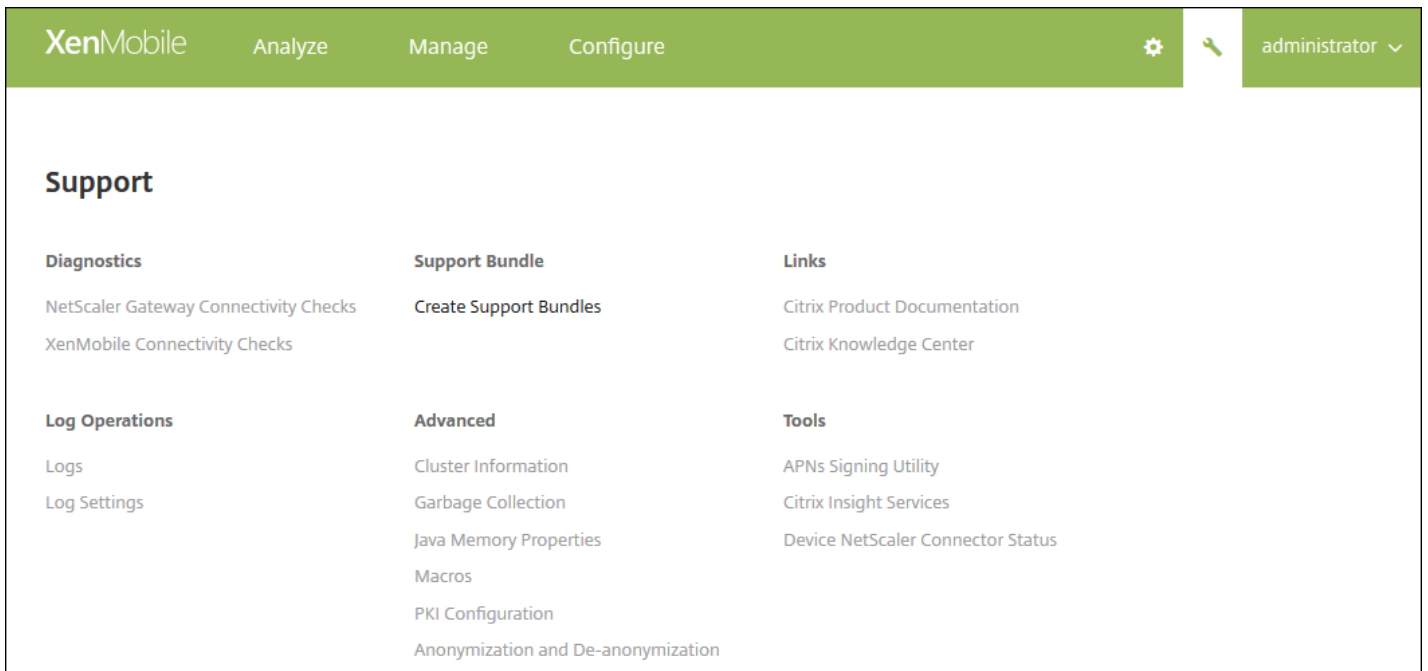
Apr 27, 2017

[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、「[コマンドラインインターフェイスオプション](#)」を参照してください。

XenMobileコンソールで、右上のレンチアイコンをクリックします。



[Support] ページが開きます。



[XenMobile サポート] ページを使用して以下を行います。

- 診断へのアクセス
- サポートバンドルの作成
- Citrixの製品ドキュメントおよびKnowledge Centerへのリンクへのアクセス
- ログ操作へのアクセス
- 一連の詳細情報および構成オプションからの選択
- 一連のツールおよびユーティリティへのアクセス

# レポート

Apr 27, 2017

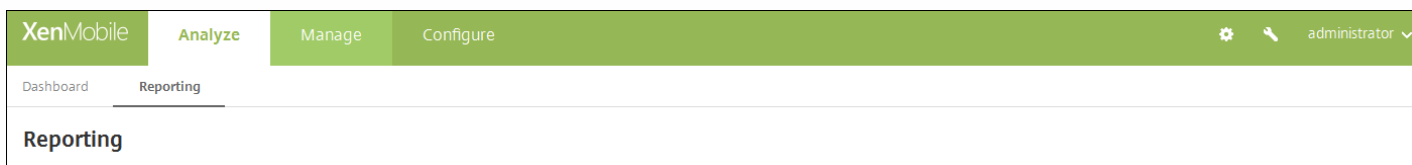
XenMobileには、以下の事前定義されたレポートが用意されており、アプリケーションおよびデバイスの展開を分析できます。

- **Apps by Devices & User** : ユーザーのデバイスに存在している管理対象アプリケーションを一覧表示します。このレポートには、デバイスにインストールされている個人用アプリは含まれません。
- **Terms & Conditions** - 使用条件契約に同意したユーザーおよび同意しなかったユーザーを一覧表示します。
- **Top 25 Apps** - ほとんどのユーザーのデバイスに存在している上位25のアプリケーションを一覧表示します。
- **Jailbroken/Rooted Devices** - ルート化済みiOSデバイスおよびジェイルブレイクされたAndroidデバイスを一覧表示します。
- **Top 10 Apps** - Failed Deployment - 展開に失敗したアプリケーションを一覧表示します。
- **Inactive Devices** - 指定期間に非アクティブになったデバイスを一覧表示します。
- **Apps by Type & Category** - アプリケーションをバージョン別、種類別、およびカテゴリ別に一覧表示します。
- **Device Enrollment** - 登録されたすべてのデバイスを一覧表示します。
- **Apps by Platform** - アプリケーションとアプリケーションバージョンを、デバイスプラットフォーム別およびバージョン別に一覧表示します。
- **Blacklisted Apps by Devices & User** - ユーザーのデバイスに存在し、ブラックリストに登録されているアプリケーションを一覧表示します。
- **デバイスおよびアプリ** - 管理対象アプリケーションを実行しているデバイスを一覧表示します。

レポートは.csv形式なので、Microsoft Excelのようなプログラムで開くことができます。

レポートを作成するには以下の手順を実行します。

1. XenMobileコンソールで **[Analyze]** タブをクリックして、**[Reporting]** をクリックします。**[Reporting]** ページが開きます。



各レポートの種類には、以下のように、レポートが収集する情報の説明および具体的なレポートデータが含まれます。

### Terms & Conditions

List of accepted and declined Terms and Conditions agreements by device users.

**Report Data:** document name, created on, platform, user name, delivery group, acceptance status.

2. 作成するレポートを選択します。使用するブラウザーに応じて、ファイルが自動的にダウンロードされるか、ファイルを保存するように求められます。

3. 作成するレポートごとに、手順2を繰り返します。

次の図は、Top 25 AppsをMicrosoft Excelで表示した例です。

	A	B	C	D	E	F	G	H	I	J
1	APP_NAME	APP_VERSION	APP_CATEGORIES	AVAILABLE_DATE	APP_OWNER	DEPLOYMENT_TOTAL	DEPLOYMENT_SUCCESS	DEPLOYMENT_FAILED	DEPLOYMENT_PENDING	APP_TYPE
2	GoToMeeting	6.6.4.1127	Default	10/17/2016 14:21		7	7	0	0	Public App Store
3	Secure Web - Inception	10.4.0-11	Default	10/17/2016 14:37	citrix.com	7	6	0	1	MDX
4	Secure Mail	10.4.1-221	Default	10/17/2016 16:06	citrix.com	6	5	0	1	MDX
5	Twitter	6.64	appstore	10/17/2016 17:04		3	3	0	0	Public App Store
6	Salesforce1	11.0.3	Default	12/14/2016 17:52		2	2	0	0	Public App Store

## Important

カスタムレポートの作成にSQL Serverを使用することは可能ですが、お勧めしません。この方法でSQL Serverデータベースを使用すると、XenMobile展開環境で予期しない結果になることがあります。このレポート作成方法を実行する場合は、SQLクエリが読み取り専用アカウントで実行されるようにしてください。

# Mobile Service Provider

Apr 27, 2017

XenMobileでMobile Service Providerインターフェイスの使用を有効にして、BlackBerryやExchange ActiveSyncデバイスに対してクエリを実行したり、操作を発行したりできます。

たとえば、組織に1,000ユーザーが存在し、各ユーザーが1つまたは複数のデバイスを使用するとします。すべてのユーザーに対して、管理のためにデバイスをXenMobileに登録する必要があることを通知した後、XenMobileコンソールはユーザーが登録したデバイスの数を表示します。この設定を構成することで、Exchange Serverに接続しているデバイスの数を判断できます。これによって、次の操作を実行できます。

- ほかにデバイスを登録する必要のあるユーザーがいるかどうかを確認する。
- Exchange Serverに接続するユーザーデバイスにコマンド（データワイプなど）を発行する。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。

2. [Server] の下の [Mobile Service Provider] をクリックします。[Mobile Service Provider] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a navigation bar with 'XenMobile', 'Analyze', 'Manage', and 'Configure' tabs. On the right, there is a gear icon and a user profile 'admin'. Below the navigation bar, the breadcrumb 'Settings > Mobile Service Provider' is visible. The main heading is 'Mobile Service Provider' with a sub-heading: 'Allows XenMobile to use the Mobile Service Provider interface to query BlackBerry and other Exchange ActiveSync devices and issue operations.' The configuration form includes three input fields: 'Web service URL\*' with the value 'http://XmmServer/services/zdm', 'User name\*' with the value 'domain\admin', and 'Password\*'. Below these is a toggle switch for 'Automatically update BlackBerry and ActiveSync device connections' set to 'OFF'. A green 'Test Connection' button is located below the toggle. At the bottom right, there are 'Cancel' and 'Save' buttons.

3. 次の設定を構成します。

- **Web service URL** : WebサービスのURL (http://XmmServer/services/xdmserviceなど) を入力します。
- **User name** : domain\adminの形式でユーザー名を入力します。
- **Password** : パスワードを入力します。
- **Automatically update BlackBerry and ActiveSync device connections** : デバイス接続を自動的に更新するかどうかを選択します。デフォルトは [OFF] です。
- [Test Connection] をクリックして、接続を検証します。

4. [Save] をクリックします。

# Syslog

Apr 27, 2017

XenMobileを構成して、ログファイルをシステムログ (syslog) サーバーに送信できます。サーバーのホスト名またはIPアドレスが必要です。

Syslogは、監査モジュール (アプライアンス上で実行) とサーバー (リモートシステムで実行可能) の2つのコンポーネントを使用する、標準ロギングプロトコルです。Syslogプロトコルでは、データ転送でユーザーデータプロトコル (UDP) を使用します。管理者イベントとユーザーイベントが記録されます。

サーバーを構成して、以下の種類の情報を収集できます。

- XenMobileで実行されたアクションの記録が含まれるシステムログ
- XenMobileのシステムアクティビティの時系列の記録が含まれる監査ログ

syslogサーバーがアプライアンスから収集したログ情報は、メッセージ形式でログファイルに保存されます。通常、これらのメッセージには次の情報が含まれています。



- ログメッセージを生成したアプライアンスのIPアドレス
- タイムスタンプ
- メッセージの種類
- イベントに関連付けられたログレベル (重要、エラー、通知、警告、情報、デバッグ、アラート、または緊急)
- メッセージの情報

この情報を使用してアラートの原因を分析したり、必要に応じて修正作業を行ったりすることができます。

## 注意

XenMobileサービス (クラウド) 環境では、オンプレミスのsyslogサーバーとのsyslog統合はサポートされません。代わりに、XenMobileコンソールの [Support] ページからログをダウンロードできます。これを行う場合は、**[Download All]** をクリックしてシステムログを取得する必要があります。詳しくは、「[XenMobileでのログファイルの表示および分析](#)」を参照してください。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。
2. [Syslog] をクリックします。[Syslog] ページが開きます。

XenMobile Analyze Manage Configure   admin ▾


Settings > SysLog


## SysLog

You can configure XenMobile to send log files to a systems log (syslog) server using the server host name or IP address.

Server\*

Port\*

Information to log  System Logs 

Audit 

3. 次の設定を構成します。

- **Server** : syslogサーバーのIPアドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
- **Port** : ポート番号を入力します。デフォルトのポートは、514です。
- **Information to log** : **[System Logs]** チェックボックスおよび **[Audit]** チェックボックスをオンまたはオフにします。
  - システムログには、XenMobileで実行されたアクションが含まれます。
  - 監査ログには、XenMobileのシステムアクティビティの時系列の記録が含まれます。

4. **[Save]** をクリックします。

# カスタマーエクスペリエンス向上プログラム

Apr 27, 2017

Citrixカスタマーエクスペリエンス向上プログラム（CEIP）では、XenMobileの構成および使用に関するデータが匿名で収集され、そのデータがCitrixに自動的に送信されます。このデータは、XenMobileの品質、信頼性、およびパフォーマンスを向上させる目的で使用させていただきます。CEIPへのご参加は任意です。XenMobileの初回インストール時、または更新のインストール時に、CEIPへの参加が可能です。選択した場合、データは通常週単位で、パフォーマンスおよび使用に関するデータは時間単位で収集されます。これらのデータはディスク上に格納され、1週間ごとにHTTPSにより安全にCitrixに送信されます。CEIPに参加するかどうかは、XenMobileコンソールで変更できます。CEIPについて詳しくは、『[Citrixカスタマーエクスペリエンス向上プログラム（CEIP）について](#)』を参照してください。

## CEIPで参加を選択する

XenMobileの初回インストール時、または更新時に、参加を促す以下のダイアログボックスが開きます。


### Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

**How does it work?**

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)



**Would you like to help make Citrix products better by joining the program?**  
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

**Yes, send anonymous usage and statistics information.**

**No**

## CEIP参加設定の変更

1. CEIP参加設定を変更するには、XenMobileコンソールで右上の歯車アイコンをクリックして[**Settings**] ページを開きます。
2. [**Server**] の下で [**Experience Improvement Program**] をクリックします。[**Customer Experience Improvement Program**] ページが開きます。表示される実際のページは、現在CEIPに参加しているかどうかによって異なります。



Settings > [Experience Improvement Program](#)

## Customer Experience Improvement Program

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

### How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer



[Learn more](#)

You are currently participating in the Customer Experience Improvement Program.

- Continue participating
- Stop participating

Cancel

Save

3. 現在CEIPに参加していて、中止を希望する場合、 [**Stop participating**] をクリックします。
4. 現在CEIPに参加していないで、開始を希望する場合、 [**Start participating**] をクリックします。
5. [**Save**] をクリックします。



# GotoAssistおよびRemote Support

Apr 27, 2017

メールアドレスと電話番号を指定することにより、サポートスタッフへのさまざまな連絡方法をユーザーに提供できます。ユーザーがデバイスからサポートを要求すると、管理者が設定したオプションが表示されます。

ユーザーがデバイスからヘルプデスクにログを送信する方法も構成できます。ログを直接送信するか、メールで送信するよう構成できます。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。

The screenshot shows the XenMobile Settings page. The header is green with 'XenMobile' on the left and 'Admin' on the right. The main content area is titled 'Settings' and is divided into three columns. The first column contains 'Certificate Management' (Certificates, Credential Providers, PKI Entities) and 'Client' (Client Branding, Client Properties, Client Support). The second column contains 'Notifications' (Carrier SMS Gateway, Notification Server, Notification Templates) and 'Platforms' (Android for Work, Google Play Credentials, iOS Bulk Enrollment, iOS Settings, Samsung KNOX). The third column contains 'Server' (ActiveSync Gateway, Enrollment, LDAP, Licensing, Local Users and Groups, Mobile Service Provider, NetScaler Gateway, Network Access Control, Release Management, Role-Based Access Control, Server Properties, SysLog, Workflows, XenApp/XenDesktop). On the right side of the settings area, there is a 'Frequently Accessed' sidebar with links to Certificates, Enrollment, Licensing, Local Users and Groups, Role-Based Access Control, and Release Management.

2. [Client] の下の [Client Support] をクリックします。[Client Support] ページが開きます。

3. 以下の設定を構成して電話番号およびメールアドレスを設定し、デバイスがヘルプデスクにログを送信する方法を指定します。

- **Support phone (IT help desk)** : ITヘルプデスクの電話番号を入力します。
- **Support email (IT help desk)** : ITヘルプデスク担当者のメールアドレスを入力します。
- **Send device logs to IT help desk** : デバイスログの送信方法として [directly] または [by email] を選択します。デフォルトは [by email] です。
- [directly] を有効にすると、[Store logs on ShareFile] の設定が表示されます。[Store logs on ShareFile] を有効にすると、ログはShareFileに直接送信されます。このオプションを有効にしない場合、ログはXenMobileに送信されてからヘルプデスクにメール送信されますさらに、[If sending directly fails, use email] オプションが表示されます。こ

のオプションはデフォルトで有効化されています。サーバーに問題が生じたときにログの送信にクライアントのメールを使用しない場合は、このオプションを無効にすることができます。ただし、このオプションを無効にすると、サーバーに問題があってもログが送信されません。

- [by email] を有効にすると、ログの送信では常にクライアントのメールが使用されます。

#### 4. [Save] をクリックします。

### リモートサポート

Remote Supportを使用すると、ヘルプデスクの担当者は管理対象のWindowsおよびAndroidモバイルデバイスをリモートで制御できます。

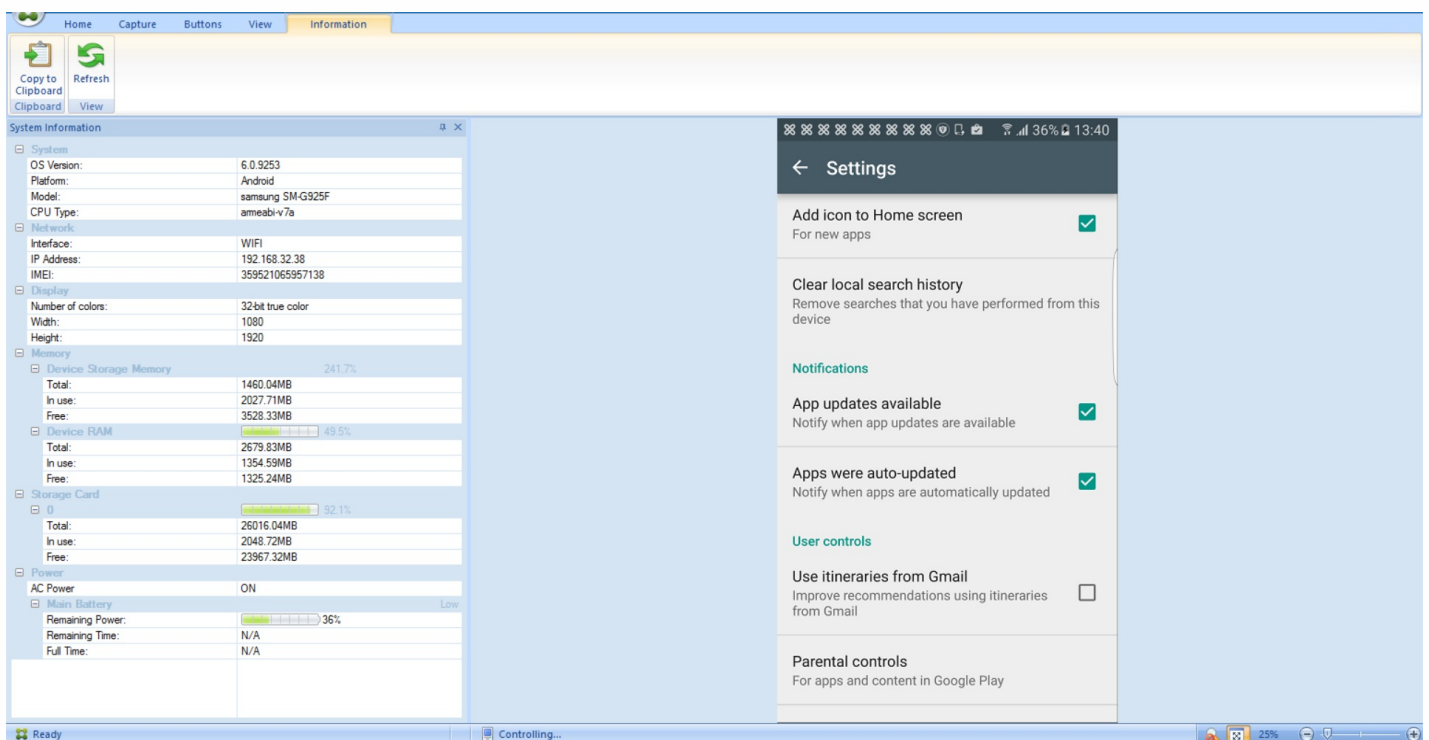
Remote Supportは、すべてのWindows MobileデバイスおよびAndroidのSamsung SAFEデバイスおよびSamsung以外のデバイスで使用できます。

画面のキャストはSamsung KNOXでのみサポートされています。

iOSデバイスのリモート制御はサポートされていません。

リモート制御セッション時の動作は次のようになります。

- ユーザーのモバイルデバイスには、リモート制御セッションがアクティブであることを示すアイコンが表示されます。
- Remote Supportアプリケーションウィンドウが開いて、[Remote Control] ウィンドウに制御対象デバイスが表示されます。



Remote Supportで、次のことを実行できます。

- ユーザーのモバイルデバイスにリモートでサインオンし、デバイスの画面を制御する。ユーザーはヘルプデスク担当者になる画面の移動を確認できるため、ユーザーのトレーニングとしても役に立つことがあります。
- リアルタイムでリモートデバイス内を移動して修復する。構成の変更、オペレーティングシステムの問題のトラブル

シューティング、問題があるアプリケーションやプロセスの無効化または終了を行うことができます。

- ネットワークアクセスの無効化、不正プロセスの停止、アプリまたはマルウェアの削除をリモートに実行することで、ほかのモバイルデバイスに脅威が広がる前に、その脅威を隔離して封じこめる。
- ユーザーがデバイスを見つけられるように、デバイスの着信音や電話の発信をリモートで有効にする。デバイスを見つけられなかった場合は、重要なデータが侵害されないように、デバイスにワイプを実行できます。

Remote Supportでは、サポート担当者に次の機能も提供されます。

- 1つまたは複数のXenMobileインスタンスについて、接続しているすべてのデバイスの一覧を表示する。
- デバイスのモデル、オペレーティングシステムのレベル、IMEI (International Mobile Station Equipment Identity) およびシリアル番号、メモリおよびバッテリーの状態、接続状態などのシステム情報を表示する。
- XenMobileのユーザーおよびグループを表示する。
- アクティブなプロセスの表示や停止、およびモバイルデバイスの再起動を行うためのデバイスタスクマネージャーを実行する。
- モバイルデバイスと中央ファイルサーバー間の双方向のリモートファイル転送を実行する。
- 1つまたは複数のモバイルデバイスに対するソフトウェアプログラムの一括ダウンロードおよびインストール。
- デバイスのレジストリキーのリモートからの構成。
- 携帯電話ネットワークによる狭帯域幅接続でのレスポンスを最適化するリアルタイムのデバイス画面リモート制御。
- さまざまなモバイルデバイスブランドおよびモデルのデバイススキンを表示する。スキンエディターを表示して、新規デバイスモデルの追加および物理キーのマッピングを行うことができます。
- デバイス画面の取り込み、記録、再生により、デバイスでの一連のビデオAVIファイル作成操作を記録できるようにする。
- 共有ホワイトボード、VoIPベースの音声通信、およびチャットによるモバイルユーザーとサポート担当者間のLive Meeting。

## Remote Supportのシステム要件

Remote Supportソフトウェアは、以下の要件を満たすWindowsベースのコンピューターにインストールします。ポートの要件については、「[ポート要件](#)」を参照してください。

サポートされるプラットフォームは、以下のとおりです。

- Intel Xeon/Pentium 4-1GHz以上のワークステーションクラス
- 512MB以上のRAM
- 100MB以上の空きディスク領域

以下のオペレーティングシステムがサポートされています。

- Microsoft Windows 2003 Server Standard EditionまたはEnterprise Edition SP1以降
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2以降
- Microsoft Windows Vista SP1以降
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

## Remote Supportソフトウェアをインストールするには

1. Remote Supportのインストーラーをダウンロードするには、[XenMobile 10ダウンロードページ](#)にアクセスしてアカウントにログオンします。
2. **[Tools]** を展開して、XenMobile Remote Support v9をダウンロードします。

Remote Supportのファイル名はXenMobileRemoteSupport-9.0.0.35265.exeです。

3. Remote Supportインストーラーをダブルクリックし、表示されるインストールウィザードの指示に従います。

コマンドラインから**Remote Support**をインストールするには：

次のコマンドを実行します。

```
RemoteSupport.exe /S
```

ここで、*RemoteSupport*はインストールプログラムの名前です。次に例を示します。

```
XenMobileRemoteSupport-9.0.0.35265.exe /S
```

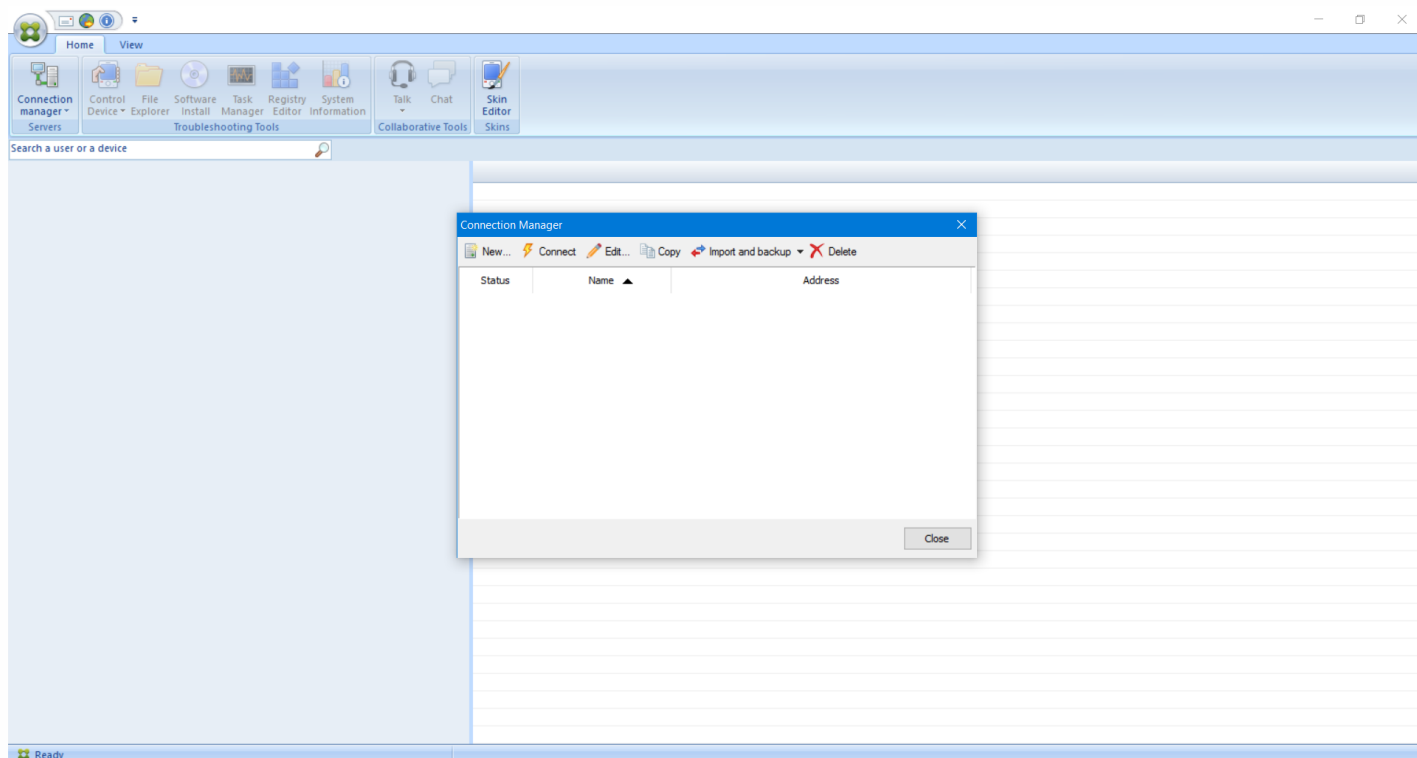
Remote Supportソフトウェアのインストール時には、次の変数を使用できます。

- /S : デフォルトのパラメーターを使用してRemote Supportソフトウェアをインストールします。
- /D=dir. カスタムのインストールディレクトリを指定します。

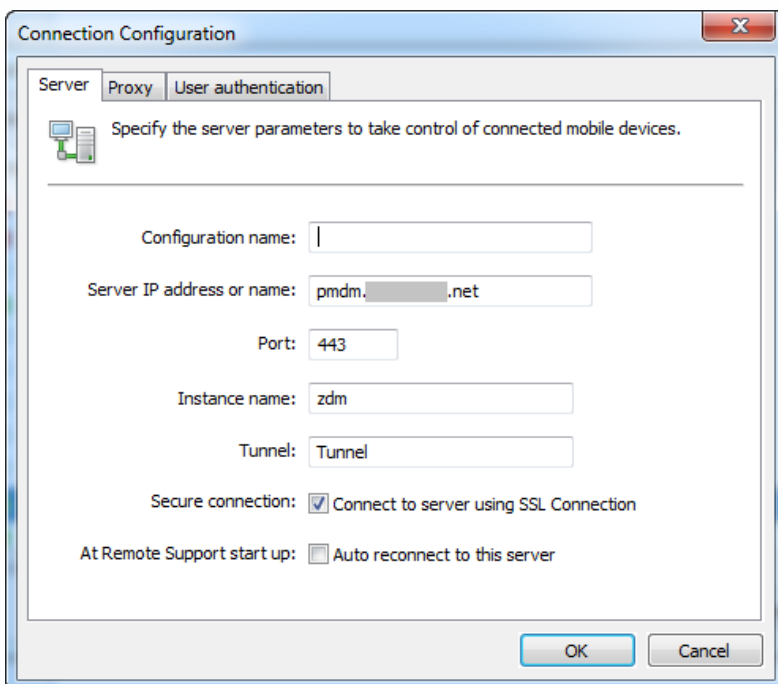
## Remote SupportをXenMobileに接続するには

管理対象デバイスへのリモートサポート接続を確立するには、Remote Supportからの接続を、該当のデバイスを管理する1つまたは複数のXenMobileサーバーに追加する必要があります。この接続は、AndroidおよびWindows Mobile/CEデバイス向けのデバイスポリシーであるトンネルMDMポリシーで定義したアプリトンネル上で実行されます。Remote SupportをXenMobileに接続するには、アプリトンネルを定義します。詳しくは、「[アプリケーショントンネリングデバイスポリシー](#)」を参照してください。

1. Remote Supportソフトウェアを起動し、XenMobileの資格情報を使用してサインオンします。
2. **[Connection Manager]** で、**[New]** をクリックします。



3. **[Connection Configuration]** ダイアログボックスの **[Server]** タブで、次の値を入力します。
  - a. **[Configuration name]** に構成エントリの名前を入力します。
  - b. **[Server IP address or name]** にXenMobileサーバーのIPアドレスまたはDNS名を入力します。
  - c. **[Port]** に、XenMobileサーバー構成で定義されているTCPポート番号を入力します。
  - d. XenMobileがマルチテナント環境に含まれている場合は、**[Instance name]** にインスタンス名を入力します。
  - e. **[Tunnel]** にトンネルポリシーの名前を入力します。
  - f. **[Connect to server using SSL Connection]** チェックボックスをオンにします。
  - g. Remote Supportアプリケーションが起動するたびに、構成したXenMobileサーバーに接続するには、**[Auto reconnect to this server]** チェックボックスをオンにします。



The screenshot shows the 'Connection Configuration' dialog box with the 'Server' tab selected. The dialog contains the following fields and options:

- Configuration name:** An empty text input field.
- Server IP address or name:** A text input field containing 'pmdm. .net'.
- Port:** A text input field containing '443'.
- Instance name:** A text input field containing 'zdm'.
- Tunnel:** A text input field containing 'Tunnel'.
- Secure connection:** A checked checkbox labeled 'Connect to server using SSL Connection'.
- At Remote Support start up:** An unchecked checkbox labeled 'Auto reconnect to this server'.

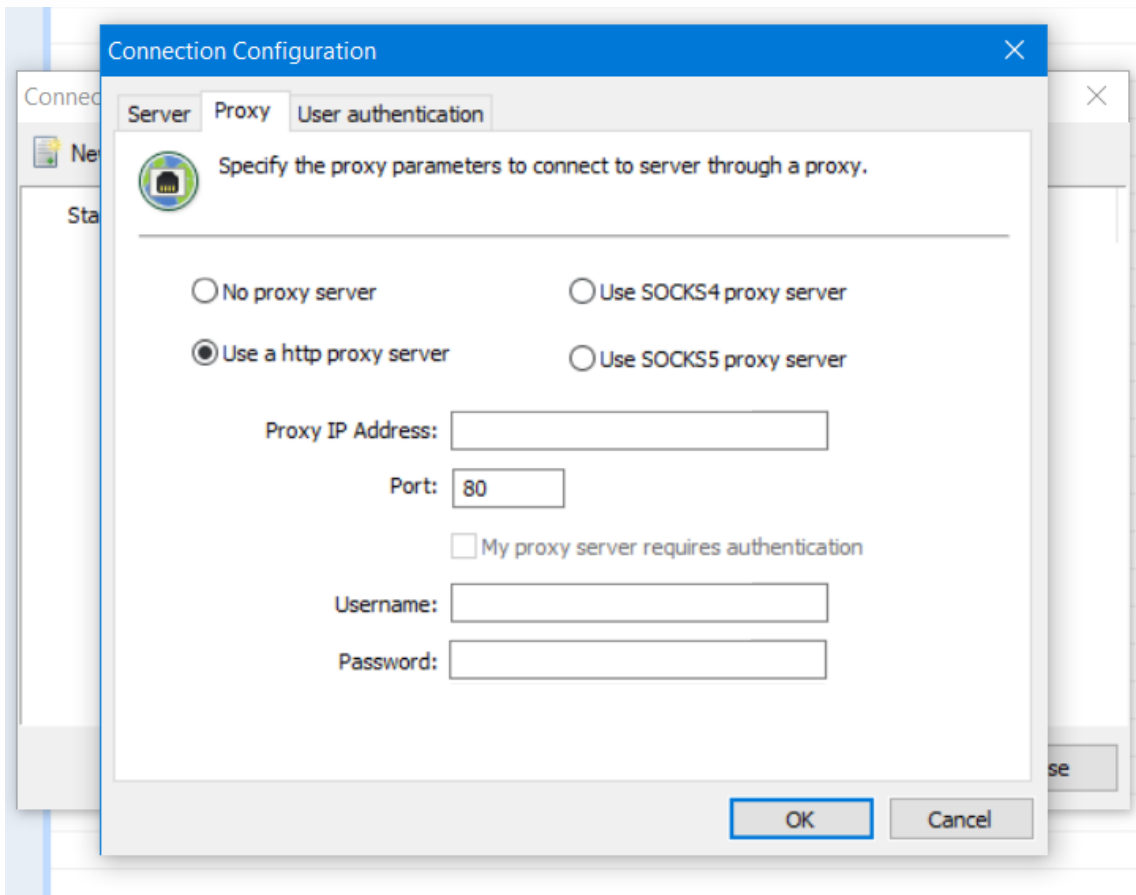
At the bottom of the dialog are 'OK' and 'Cancel' buttons.

4. **[Proxy]** タブで、**[Use a http proxy server]** を選択して次の情報を入力します。

- a. [Proxy IP Address] に、プロキシサーバーのIPアドレスを入力します。
- b. [Port] に、プロキシで使用するTCPポート番号を入力します。
- c. プロキシサーバーでトラフィックの許可に認証が必要な場合は、[My proxy requires authentication] チェックボックスをオンにします。

[Username] に、プロキシサーバーで認証するユーザー名を入力します。

- e. [Password] に、プロキシサーバーで認証するパスワードを入力します。



5. **[User Authentication]** タブで、**[Remember my login and password]** チェックボックスをオンにして資格情報を入力します。

6. **[OK]** をクリックします。

XenMobileに接続するには、作成した接続をダブルクリックし、この接続用に構成したユーザー名とパスワードを入力します。

## Samsung KNOXデバイスでリモートサポートを有効にするには

XenMobileでRemote Supportポリシーを作成して、Samsung KNOXデバイスへのリモートアクセスを行うことができます。次の2種類のサポートを構成できます。

- **[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。

プレミアムサポートでは、XenMobileコンソールでSamsung MDMライセンスキーのデバイスポリシーを構成する必要があります。このポリシーを構成する場合、**Samsung KNOX**プラットフォームのみを選択します。XenMobileでSamsungデバイスを登録すると、ELMキーが自動的に展開されるため、Samsung SAFEプラットフォームを構成する必要はありません。詳しくは、「[Samsung MDMライセンスキー](#)」を参照してください。

リモートサポートポリシーの構成について詳しくは、「[リモートサポートデバイスポリシー](#)」を参照してください。

## リモートサポートセッションを使用するには

Remote Supportを起動すると、Remote Supportアプリケーションウィンドウの左側に、XenMobileコンソールで定義したXenMobileユーザーグループが表示されます。デフォルトでは、現在接続されているユーザーが含まれているグループのみが表示されます。ユーザーエントリの横に、各ユーザーのデバイスが表示されます。

1. すべてのユーザーを表示するには、左側の列の各グループを展開します。  
XenMobileサーバーに現在接続されているユーザーは、緑のアイコンで表示されます。
2. すべてのユーザー（現在接続されていないユーザーを含む）を表示するには、**[View]** をクリックし、**[Non-connected devices]** を選択します。  
接続されていないユーザーは、緑のアイコンなしで表示されます。

XenMobileサーバーに接続されているもののユーザーに割り当てられていないデバイスは、匿名モードで表示されます（一覧に「**Anonymous**」と表示されます）。これらのデバイスは、ログインユーザーのデバイスと同じように制御できます。

デバイスを制御するには、デバイスの行をクリックしてデバイスを選択してから、**[Control Device]** をクリックします。デバイスが**[Remote Control]** ウィンドウに表示されます。制御対象デバイスは次の方式で操作できます。

- デバイス画面のメインウィンドウまたは別の浮動ウィンドウを制御する（色の制御を含む）。
- ヘルプデスクとユーザー間のボイスオーバーIP（VoIP）セッションを確立する。VoIP設定を構成します。
- ユーザーとのチャットセッションを確立する。

- デバイスのタスクマネージャーにアクセスして、メモリの使用率、CPUの使用率、実行中のアプリケーションなどのアイミムを管理する。
- モバイルデバイスのローカルディレクトリを探索する。ファイルを転送する。
- Windows Mobileデバイス上のデバイスレジストリを編集する。
- デバイスシステム情報およびインストールされているすべてのソフトウェアを表示する。
- XenMobileサーバーとモバイルデバイスの接続状態を更新する。



# Secure HubおよびGoToAssistサポートオプションの作成

Apr 27, 2017

ストアでのアプリの表示方法を設定したり、ロゴを追加したりすることで、iOSおよびAndroidのモバイルデバイス上でSecure HubおよびXenMobile Store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。

カスタムイメージは、以下の要件を満たす必要があります。

- ファイルは.png形式にする必要があります。
- 透明な背景に純粋な白で描かれたロゴまたはテキスト（72dpi）を使用してください。
- 会社ロゴの高さおよび幅は、170px×25px（1x）および340px×50px（2x）を超過しないようにする必要があります。
- ファイルの名前はHeader.pngおよびHeader@2x.pngにします。
- ファイルを含むフォルダーではなく、ファイルから.zipファイルを作成します。

1. XenMobileコンソールで、右上の歯車アイコンをクリックします。[Settings] ページが開きます。

The screenshot shows the XenMobile console interface. At the top, there is a green navigation bar with the following elements: 'XenMobile' logo, 'Dashboard', 'Manage', 'Configure' tabs, a gear icon for settings, and 'Admin' with a dropdown arrow. Below the navigation bar, the main content area is titled 'Settings'. This area is organized into three columns of settings categories. The first column, 'Certificate Management', includes 'Certificates', 'Credential Providers', and 'PKI Entities'. The second column, 'Notifications', includes 'Carrier SMS Gateway', 'Notification Server', and 'Notification Templates'. The third column, 'Server', includes 'ActiveSync Gateway', 'Enrollment', 'LDAP', 'Licensing', 'Local Users and Groups', 'Mobile Service Provider', 'NetScaler Gateway', 'Network Access Control', 'Release Management', 'Role-Based Access Control', 'Server Properties', 'SysLog', 'Workflows', and 'XenApp/XenDesktop'. To the right of these columns is a 'Frequently Accessed' sidebar containing links to 'Certificates', 'Enrollment', 'Licensing', 'Local Users and Groups', 'Role-Based Access Control', and 'Release Management'. The 'Client' section is also visible, containing 'Client Branding', 'Client Properties', and 'Client Support'.

2. [Client] で [Create Branding] をクリックします。[Client Branding] ページが開きます。

Settings &gt; Client Branding

## Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

**Store name\***  ⓘ

**Default store view**

Category

A-Z

**Device**

Phone

Tablet

**Branding file**

**Note:**

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
  - The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
  - Files should be named as Header.png and Header@2x.png.
- A .zip file should be created from the files, not a folder with the files inside of it.

### 3. 次の設定を構成します。

- **Store name** : ユーザーのアカウント情報に含まれるストア名が表示されます。この名前を変更すると、ストアサービスへのアクセスに使用されるURLも変更されます。通常、デフォルトの名前をそのまま使用します。
- **Default store view** : **[Category]** または **[A-Z]** を選択します。デフォルトは **[A-Z]** です。
- **Device option** : **[Phone]** または **[Tablet]** を選択します。デフォルトは **[Phone]** です。
- **Branding file** : **[Browse]** をクリックしてブランド設定に使用するイメージまたはイメージの.zipファイルの場所に移動し、ファイルを選択します。

### 4. [保存] をクリックします。

このパッケージをユーザーのデバイスに展開するには、展開パッケージを作成し、展開する必要があります。

# 接続確認

Apr 27, 2017

XenMobileの **[Support]** ページで、NetScaler Gatewayおよびそのほかのサーバーや場所へのXenMobileの接続を確認できます。

XenMobileの接続確認の実行

1. XenMobileコンソールで、右上のレンチアイコン ( ) をクリックします。 **[Support]** ページが開きます。
2. **[Diagnostics]** の下の **[XenMobile Connectivity Checks]** をクリックします。 **[XenMobile Connectivity Checks]** ページが開きます。XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。

<input type="checkbox"/>	Connectivity to	IP address or FQDN
<input type="checkbox"/>	Windows Phone Store	windowsphone.com
<input type="checkbox"/>	Database	.....net
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com
<input type="checkbox"/>	LDAP	.....net
<input type="checkbox"/>	Domain Name System (DNS)	.....
<input type="checkbox"/>	Nexmo Gateway	-
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com
<input type="checkbox"/>	Google Play	play.google.com
<input type="checkbox"/>	Windows Security Token Service	login.live.com

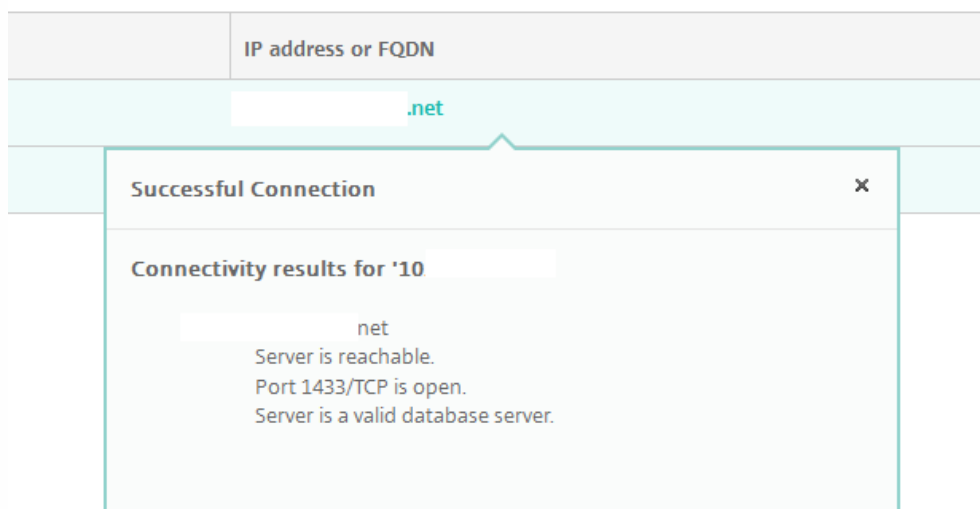
2. 接続テストに含めるサーバーをオンにして、 **[Test Connectivity]** をクリックします。 **[Test Results]** ページが開きます。

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	.....net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

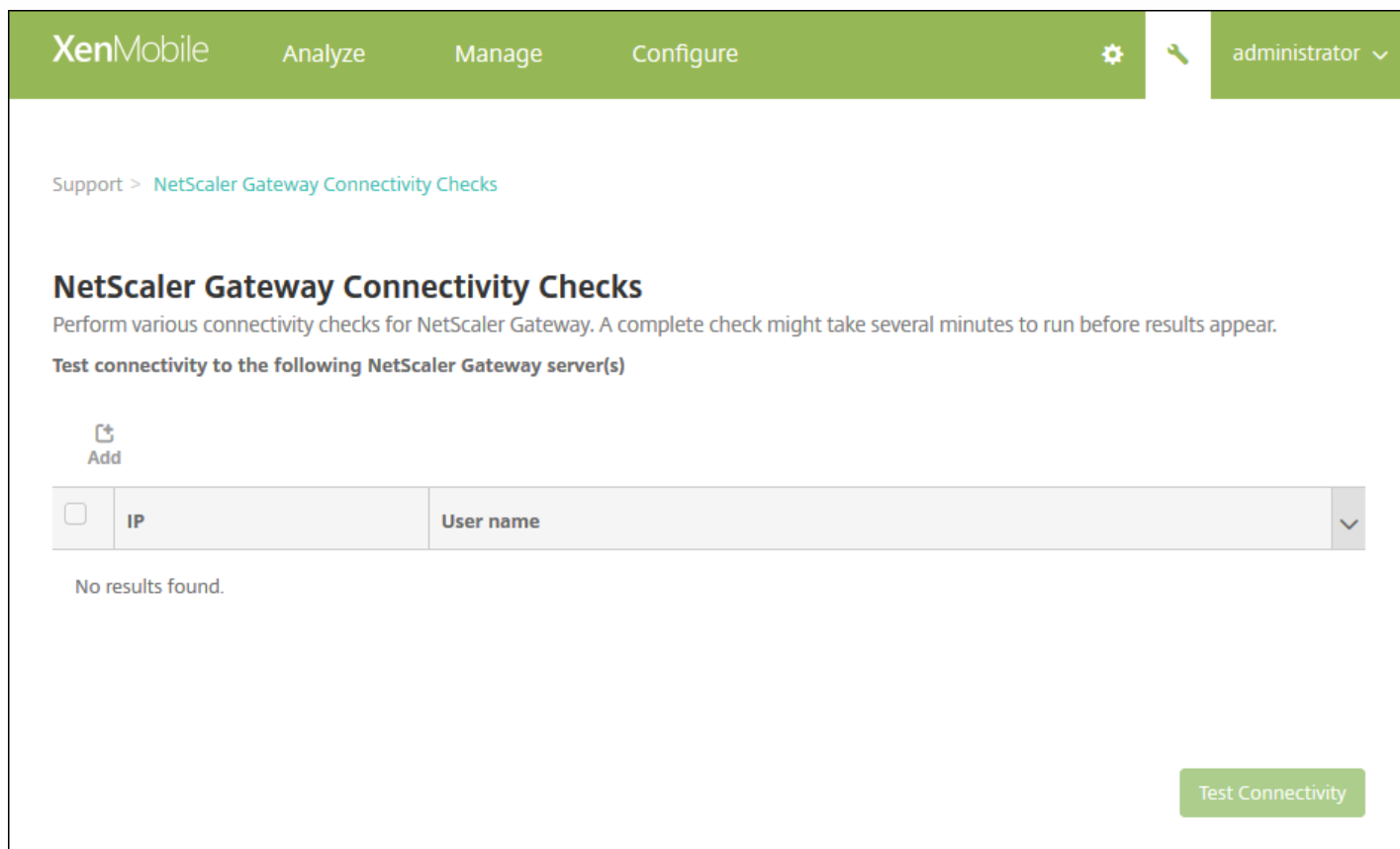
Clear Results Test Connectivity

3. [Test Results] の表でサーバーを選択して、そのサーバーの結果の詳細を参照します。

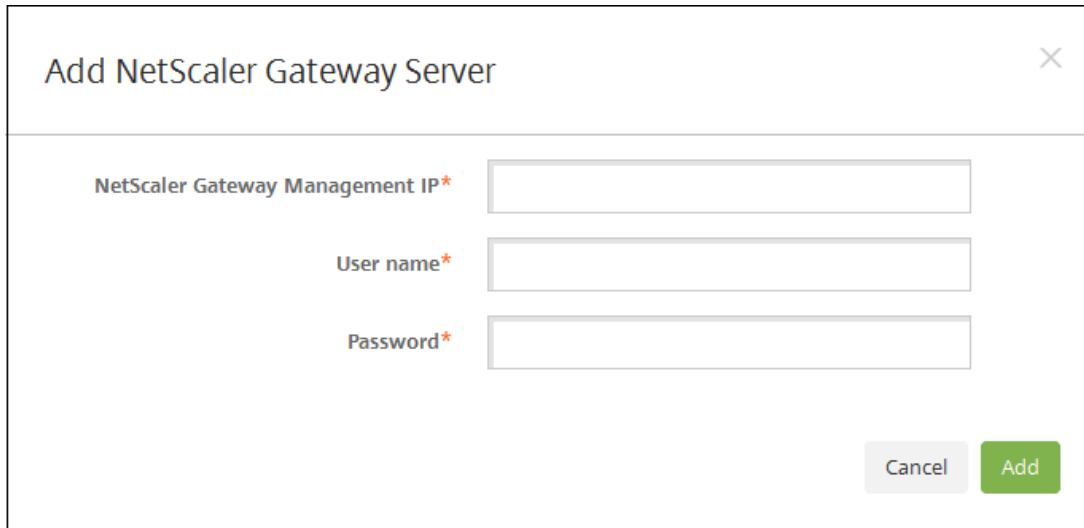


## NetScaler Gatewayの接続確認の実行

1. [Support] ページで、[Diagnostics] の下の [NetScaler Gateway Connectivity Checks] をクリックします。[NetScaler Gateway Connectivity Checks] ページが開きます。NetScaler Gatewayサーバーが追加されていない場合、表は空白です。



2. **[Add]** をクリックします。 **[Add NetScaler Gateway Server]** ダイアログボックスが開きます。



The screenshot shows a dialog box titled "Add NetScaler Gateway Server". It features three input fields: "NetScaler Gateway Management IP\*", "User name\*", and "Password\*", each followed by a text input box. At the bottom right, there are two buttons: "Cancel" and "Add".

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. NetScaler Gatewayサーバーを選択して、 **[接続性をテスト]** をクリックします。

[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。

# サポートバンドル

Apr 27, 2017

Citrixに問題を報告する場合や問題をトラブルシューティングする場合、サポートバンドルを作成してCitrix Insight Services (CIS) にアップロードできます。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。[Support] ページが開きます。
2. [Support] ページで、[Create Support Bundles] をクリックします。[Create Support Bundles] ページが開きます。XenMobile環境内にクラスターノードがある場合は、すべてのノードが表示されます。

The image displays two screenshots of the XenMobile console's 'Create Support Bundles' page. The top screenshot shows the initial state where the 'Support Bundle for XenMobile' checkbox is checked, and the 'Support Bundle for\*' dropdown is set to 'Cluster'. The bottom screenshot shows the expanded options for 'Support Bundle for\*' set to '198.51.100.3'. Under 'Include from database\*', the 'No data' radio button is selected. Other options include 'Custom data', 'Configuration data', 'Delivery group data', 'Devices and user info', and 'All data'. A note indicates that support data anonymization is turned on. A 'Create' button is visible at the bottom right of the second screenshot.

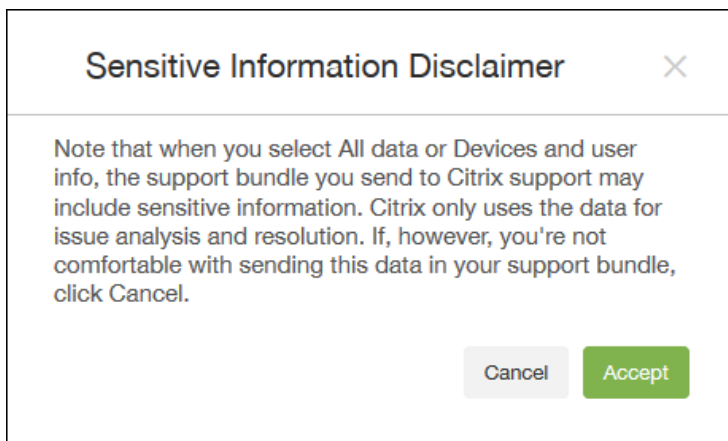
3. [Support Bundle for XenMobile] チェックボックスがオンになっていることを確認します。

4. XenMobile環境内にクラスターノードがある場合は、[Support Bundle for] ですべてのノードを選択するか、データの取得先にするノードの組み合わせを選択できます。

5. [Include from Database] で、次のいずれかを実行します。

- [No data] をクリックします。
- [Custom data] をクリックして、次のいずれかまたはすべてをオンにします（デフォルトでは、すべてのオプションが選択されています）。
  - Configuration data : 証明書構成とデバイスマネージャーポリシーを含めます。
  - Delivery group data : アプリケーションの種類やアプリケーションデリバリーポリシー詳細など、アプリケーションのデリバリーグループの情報を含めます。
  - Devices and user info : デバイスポリシー、アプリケーション、アクション、デリバリーグループを含めます。
- [All data] をクリックします。

注: [Devices and user info] または [All data] を選択し、かつこれが初めて作成するサポートバンドルである場合は、[Sensitive Information Disclaimer] ダイアログボックスが開きます。免責事項を読み、[Accept] または [Cancel] をクリックします。[Cancel] をクリックした場合は、サポートバンドルをCitrixにアップロードできません。[Accept] をクリックした場合は、サポートバンドルをCitrixにアップロードでき、次回デバイスやユーザーデータを含むサポートバンドルを作成するときに免責事項が表示されなくなります。



6. [Support data anonymization is turned on] オプションのデフォルト設定はデータの匿名化で、機密性の高いユーザー、サーバー、ネットワークのデータをサポートバンドルで匿名化します。

この設定を変更するには、[Anonymization and de-anonymization] を選択します。詳しくは、「[サポートバンドルのデータの匿名化](#)」を参照してください。

7. NetScaler Gatewayからのサポートバンドルを含める場合は、[Support Bundle for NetScaler Gateway] チェックボックスをオンにして以下を行います。

- a. [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。

Add NetScaler Gateway Server

NetScaler Gateway Management IP \*

User name \*

Password \*

Cancel Add

b. [NetScaler Gateway Management IP] ボックスに、サポートバンドルの取得先にするNetScaler GatewayのNetScaler管理IPアドレスを入力します。

注：既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、IPアドレスは入力されています。

c. [User name] ボックスと [Password] ボックスに、NetScaler Gatewayを実行しているサーバーへのアクセスに必要なユーザー資格情報を入力します。

注：既に追加されているNetScaler Gatewayサーバーからバンドルを作成する場合、ユーザー名は入力されています。

7. [Add] をクリックします。新しいNetScaler Gatewayサポートバンドルが表に追加されます。

8. 手順7を繰り返し、ほかのNetScaler Gatewayサポートバンドルを追加します。

9. [Create] をクリックします。サポートバンドルが作成され、[Upload to CIS] と [Download to Client] の2つの新しいボタンが表示されます。

サポートバンドルを作成した後、Citrix Insight Services (CIS) にバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。以下の手順は、CISにバンドルをアップロードする方法を示しています。CISにアップロードするには、MyCitrixのIDおよびパスワードが必要です。

1. [Create Support Bundles] ページで、[Upload to CIS] をクリックします。[Upload to Citrix Insight Services (CIS)] ダイアログボックスが開きます。



### Upload to Citrix Insight Services (CIS) ×

**CIS Website** cis.citrix.com

**User name\***

**Password\***

**Associate with SR#**

2. [User Name] ボックスにMyCitrix IDを入力します。

3. [Password] ボックスにMyCitrixパスワードを入力します。

4. このバンドルを既存のサービスリクエスト番号に関連付ける場合は、[Associate with SR#] チェックボックスをオンにし、新たに表示される2つのフィールドで以下を実行します。

- [SR#] ボックスに、このバンドルを関連付けるサービスリクエスト番号 (8桁) を入力します。
- [SR Description] ボックスに、SRの説明を入力します。

5. [Upload] をクリックします。

CISにサポートバンドルをアップロードするのはこれが初めてであり、ほかの製品を介してCISのアカウントを作成したことがなく、かつデータの収集とプライバシーについての契約に同意していない場合は、以下のダイアログボックスが表示されます。アップロードを開始する前にこの契約に同意する必要があります。CISのアカウントを作成済みで、以前に契約に同意している場合は、サポートバンドルが直ちにアップロードされます。

### Data Collection and Privacy ×

By uploading your data to Citrix pursuant to the instructions on this website, you are agreeing that Citrix may store, transmit and use technical and related information about your use of your Citrix products, including configuration information, number and types of users, error reports, features enabled, performance, version and patch management information, and non-personally identifiable usage statistics ("Collected Data") to facilitate the provisioning of product updates, support, education, self-help tools, market assessment and analysis, product development, invoicing and online services. Collected Data is subject to Citrix's Privacy Policy.

6. 契約を読み、 **[Agree and upload]** をクリックします。サポートバンドルがアップロードされます。

サポートバンドルを作成した後、CISにバンドルをアップロードしたり、コンピューターにバンドルをダウンロードしたりすることができます。問題のトラブルシューティングを自分で行う場合は、サポートバンドルをコンピューターにダウンロードします。

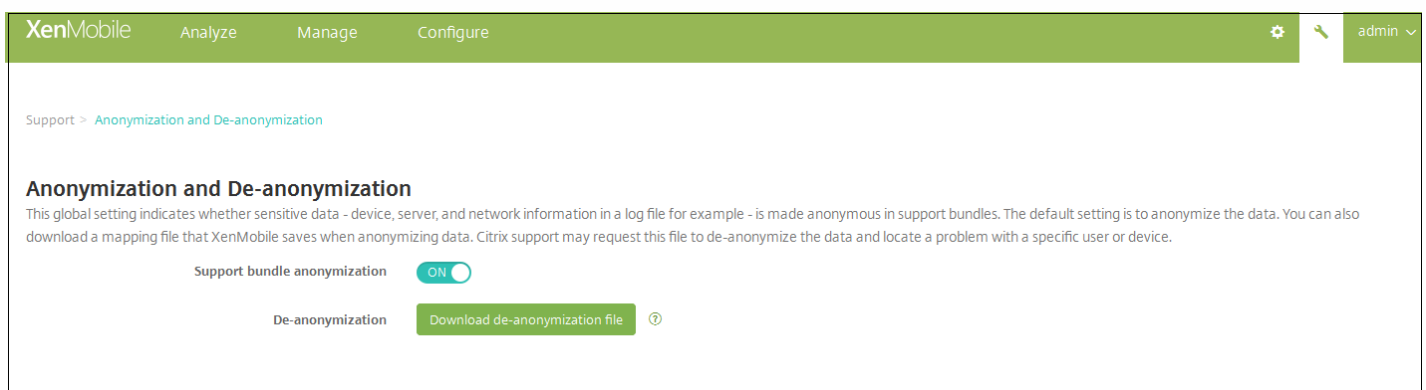
[Create Support Bundles] ページで、 [Download to Client] をクリックします。バンドルがコンピューターにダウンロードされます。

# サポートバンドルのデータの匿名化

Apr 27, 2017

XenMobileでサポートバンドルを作成する場合、デフォルトでは、機密性の高いユーザー、サーバー、ネットワークのデータは匿名化されます。この動作は、[Anonymization and De-anonymization] ページで変更することができます。また、XenMobileがデータの匿名化時に保存したマッピングファイルをダウンロードすることもできます。データの匿名化を解除したり、ユーザーまたはデバイスで発生した問題を特定したりする目的で、Citrixのサポートからこのファイルを要求される場合があります。

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。[Support] ページが開きます。
2. [Support] ページで、[Advanced] の下の [Anonymization and De-anonymization] をクリックします。[Anonymization and De-anonymization] ページが開きます。



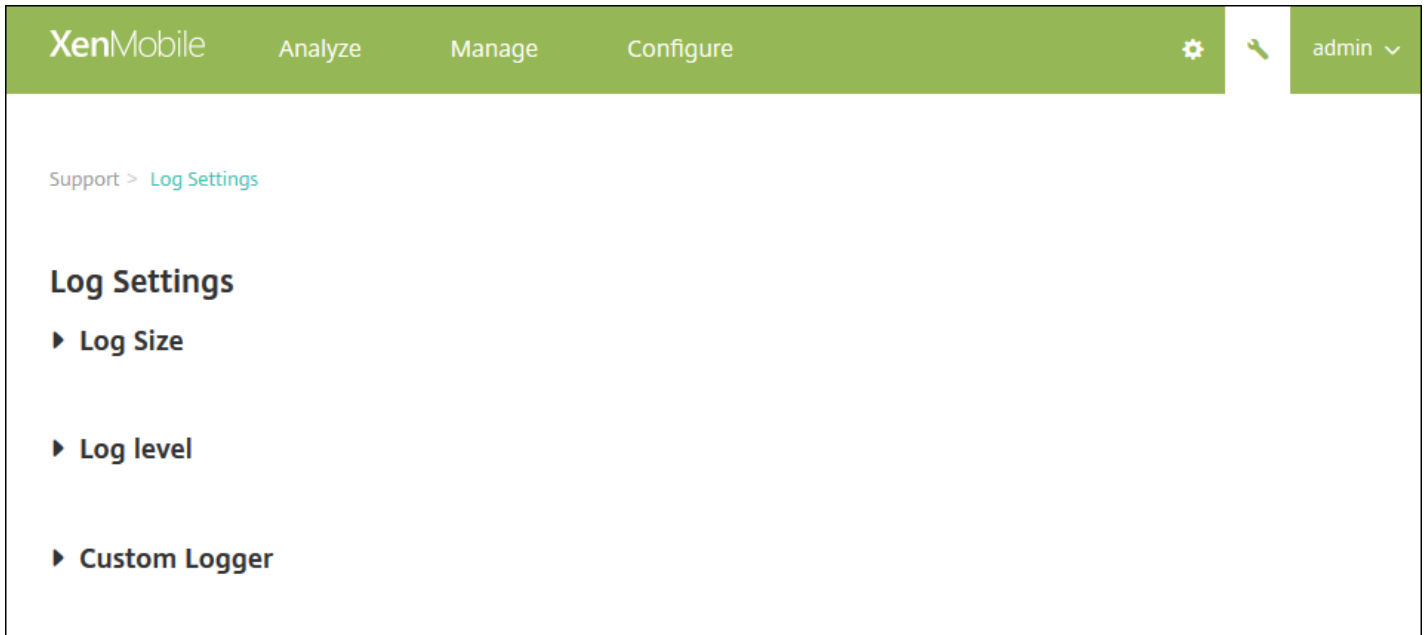
3. [Support bundle anonymization] で、データを匿名化するかどうかを選択します。デフォルトは[ON] です。
4. Citrixのサポートで問題の診断に特定のデバイスまたはユーザーの情報が必要な場合にサポートに送信するマッピングファイルを、[De-anonymization] の横の [Download de-anonymization file] をクリックしてダウンロードします。

# ログ

Apr 27, 2017

ログ設定を構成して、XenMobileで生成されるログの出力をカスタマイズすることができます。XenMobileサーバーをクラスタ化している場合は、XenMobileコンソールでログ設定を構成すると、その設定はクラスター内のほかのすべてのサーバーと共有されます。

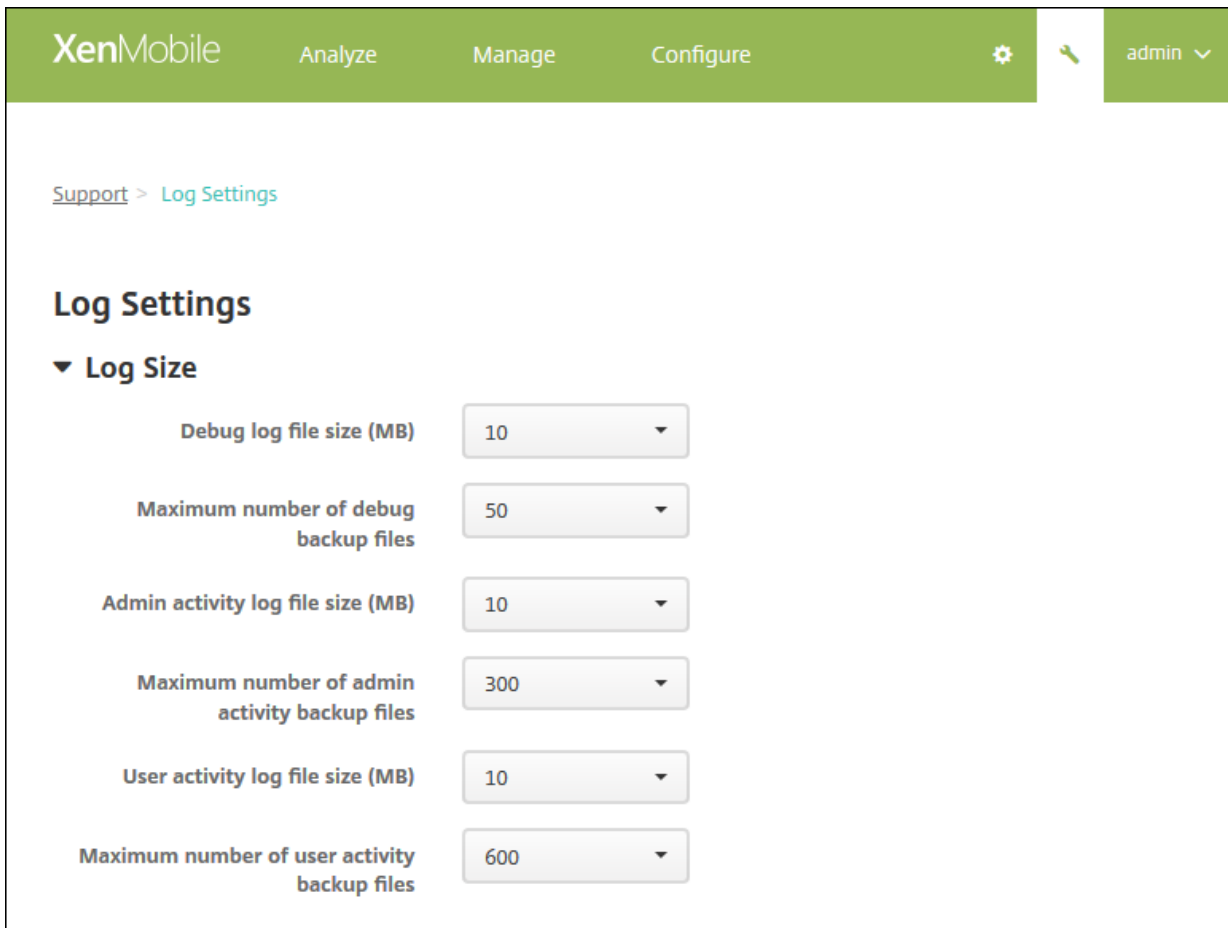
1. XenMobileコンソールで、右上のレンチアイコン ( ) をクリックします。[Support] ページが開きます。
2. [Log Operations] の下の [Log Settings] をクリックします。[Log Settings] ページが開きます。



[Log Settings] ページでは、以下のオプションにアクセスできます。

- **Log Size**。このオプションを使用して、ログファイルのサイズと、データベースで保持されるログのバックアップファイルの最大数を制御します。ログのサイズは、XenMobileでサポートされる各ログ（デバッグログ、管理者アクティビティログ、およびユーザーアクティビティログ）に適用されます。
- **Log level**。このオプションを使用して、ログレベルを変更したり、設定を永続的にしたりします。
- **Customer Logger**。このオプションを使用して、カスタムロガーを作成します。カスタムログには、クラス名とログレベルが必要です。

1. [Log Settings] ページで [Log Size] を展開します。





2. 次の設定を構成します。

- **Debug log file size (MB)** : 一覧からサイズ (5~20MB) を選択して、デバッグファイルの最大サイズを変更します。デフォルトのファイルサイズは10 MBです。
- **Maximum number of debug backup files** : サーバーにより保持されるデバッグファイルの最大数をクリックします。デフォルトでは、サーバーに50件のバックアップファイルが保持されます。
- **Admin activity log file size (MB)** : 一覧からサイズ (5~20MB) を選択して、管理者アクティビティファイルの最大サイズを変更します。デフォルトのファイルサイズは10 MBです。
- **Maximum number of admin activity backup files** : サーバーにより保持される管理者アクティビティファイルの最大数をクリックします。デフォルトでは、サーバーに300件のバックアップファイルが保持されます。
- **User activity log file size (MB)** : 一覧からサイズ (5~20MB) を選択して、ユーザーアクティビティファイルの最大サイズを変更します。デフォルトのファイルサイズは10 MBです。
- **Maximum number of user activity backup files** : サーバーにより保持されるユーザーアクティビティファイルの最大数をクリックします。デフォルトでは、サーバーに300件のバックアップファイルが保持されます。

ログレベルを設定することにより、XenMobileでログに収集される情報の種類を指定できます。すべてのクラスに同じレベルを設定することも、個別のクラスに特定のレベルを設定することもできます。

1. [Log Settings] ページで [Log level] を展開します。すべてのログクラスの表が表示されます。



XenMobile Analyze Manage Configure   admin ▾

Support > [Log Settings](#)

## Log Settings

▶ Log Size

▼ Log level

 Edit all |  Reset

<input type="checkbox"/>	Class	Sub-class	Log level	▼
<input type="checkbox"/>	Data Access	All	Info	
<input type="checkbox"/>	Data Access	XDM	Info	
<input type="checkbox"/>	Data Access	XAM	Info	
<input type="checkbox"/>	Data Access	Console	Info	
<input type="checkbox"/>	Data Access	OCA	Info	
<input type="checkbox"/>	IMI Services	All	Info	
<input type="checkbox"/>	IMI Services	Category Service	Info	
<input type="checkbox"/>	IMI Services	OPN Service	Info	

2. 次のいずれかを行います。

- 1つのクラスの横のチェックボックスをクリックして **[Set Level]** をクリックし、そのクラスのログレベルのみを変更します。
- **[Edit all]** をクリックしてログレベルの変更を表内のすべてのクラスに適用します。

**[Set Log Level]** ダイアログボックスが開き、ログレベルを設定したり、XenMobileサーバーを再起動したときにログレベルの設定を保持するかどうかを選択したりできます。

- **Class Name** : すべてのクラスのログレベルを変更する場合はこのフィールドに [All] と表示されます。そうでない場合は個別のクラス名が表示されます。編集できません。
- **Sub-class name** : すべてのクラスのログレベルを変更する場合はこのフィールドに [All] と表示されます。そうでない場合は個別のクラスのサブクラス名が表示されます。編集できません。
- **Log level** : 一覧でログレベルをクリックします。サポートされるログレベルは以下のとおりです。
  - 重大
  - エラー
  - 警告
  - 詳細
  - デバッグ
  - トレース
  - 電源 - オフ
- **Included Loggers** : すべてのクラスのログレベルを変更する場合はこのフィールドは空白です。そうでない場合は個別のクラスに対して現在構成されているロガーが表示されます。編集できません。
- **Persist settings** : サーバーを再起動してもログレベルの設定を維持する場合はこのチェックボックスをオンにします。このチェックボックスがオフの場合は、サーバーを再起動するとログレベル設定がデフォルト設定に戻ります。

3. [Set] をクリックして変更を確定します。

1. [Log Settings] ページで [Custom Logger] を展開します。[Custom Logger] の表が表示されます。カスタムロガーがまだ追加されていない場合、最初はこの表が空白の状態が表示されます。

Support &gt; Log Settings

## Log Settings

### ▶ Log Size

### ▶ Log level

### ▼ Custom Logger



Add



Set Level



Delete

<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Showing 1 - 2 of 2 items

2. [Add] をクリックします。[Add custom logger] ダイアログボックスが開きます。

### Add custom logger ×

**Class name**

**Log level**

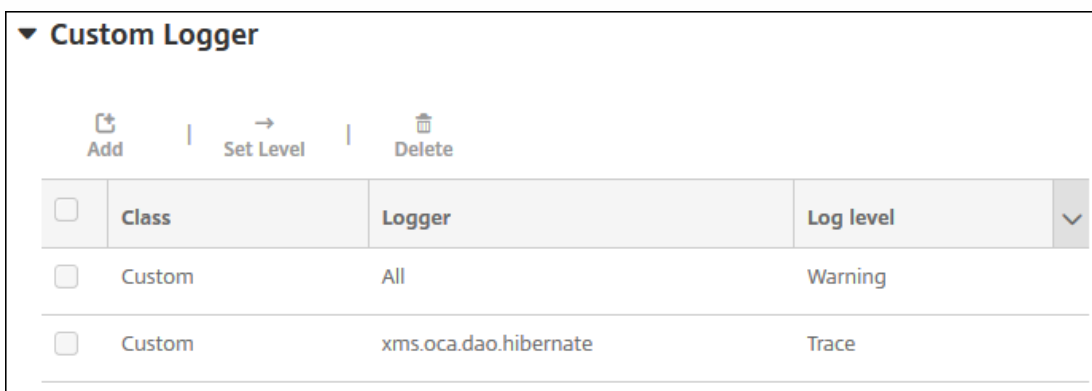
**Included loggers**



3. 次の設定を構成します。

- **Class Name** : このフィールドには [Custom] と表示されます。編集できません。
- **Log level** : 一覧でログレベルをクリックします。サポートされるログレベルは以下のとおりです。
  - 重大
  - エラー
  - 警告
  - 詳細
  - デバッグ
  - トレース
  - 電源 - オフ
- **Included Loggers** : カスタムロガーに含める特定のロガーを入力するか、このフィールドを空白にしてすべてのロガーが含まれるようにします。

4. [Add] をクリックします。カスタムロガーが [Custom Logger] の表に追加されます。



<input type="checkbox"/>	Class	Logger	Log level	
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

1. [Log Settings] ページで [Custom Logger] を展開します。

2. 削除するカスタムロガーを選択します。

3. [Delete] をクリックします。カスタムロガーを削除するかどうかを確認するダイアログボックスが開きます。[OK] をクリックします。

**重要** : この操作を元に戻すことはできません。

# XenMobile Analyzer ツール

Apr 27, 2017

XenMobile Analyzerは、インストールやその他の機能についてのXenMobileに関連する問題の診断とトラブルシューティングを行うことができる、クラウドベースのツールです。このツールにより、XenMobile環境内でのデバイスまたはユーザーの登録と認証の問題がチェックされます。

このチェックを有効にするには、お使いのXenMobileサーバーをポイントするようにツールを構成して、サーバーの展開の種類、モバイルプラットフォーム、認証の種類、テスト用のユーザー資格情報などの情報を入力する必要があります。設定が完了するとツールはサーバーに接続し、構成の問題をチェックするために環境をスキャンします。XenMobile Analyzerで問題が検出されると、ツールにより問題を修正するための推奨事項が示されます。

## XenMobile Analyzerの主な機能

- 安全な、クラウドベースのマイクロサービスを提供して、すべてのXenMobile関連の問題点をトラブルシューティングします。
- XenMobileの構成関連の問題点がある場合、正確な推奨事項を提供します。
- サポートへの問い合わせ件数を低減し、より短時間でXenMobile環境のトラブルシューティングを可能にします。
- XenMobileサーバーリリースに対してゼロデイサポートを提供します。
- iOSカスタム登録を有効化します。XenMobile (8443番ポート以外) のカスタムポートのサポート。
- 信頼できないか不完全なサーバー証明書に対して証明書受け入れダイアログボックスを表示します。
- 2要素認証シナリオを自動的に検出します。
- イン트라ネットサイトへのSecure Webの到達可能性をテストします。
- Secure Mail Auto Discoveryサービスのチェックを行います。
- ShareFileへのシングルサインオンをチェックします。
- NetScalerのカスタムポートサポートを有効化します。
- 英語版以外のブラウザをサポートします。

## 前提条件

製品	サポートされるバージョン
XenMobileサーバー	10.3.0以降
NetScaler Gateway	10.5以降
クライアント登録シミュレーション	iOSまたはAndroid

MyCitrix資格情報を使用して、<https://xenmobiletools.citrix.com>からツールにアクセスします。表示された [XenMobile Management Tools] ページで、XenMobile Analyzerを起動し、[Analyze and Troubleshoot my XenMobile Environment] をクリックします。

All Management Tools

## What do you want to do?

XenMobile Management Tools can help you troubleshoot your XenMobile Server set up and enable key features in your XenMobile deployment.

Analyze and  
Troubleshoot my  
XenMobile  
environment

XenMobile Analyzer



Follow steps to identify and triage potential issues with your deployment.

Request Auto  
Discovery

Auto Discovery Service



Request and Configure Auto Discovery for your domain's XenMobile Server.

Request push  
notification  
certificate  
signature

Create APNs Certificate



Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

Enable APNs-based

XenMobile Analyzerには、トリアージプロセスを実行しサポートチケットを削減するための5つの主要な手順があります。この手順により、かかる費用を抑えることができます。

手順は次のとおりです。

**1.Environment Check** - この手順では、設定に問題がないかどうかをチェックするテストを設定します。また、デバイス、ユーザー登録、および認証に関する問題についての推奨事項も示されます。

## All Steps

## XenMobile Analyzer

Identify potential issues with your deployment

## Step 1: Environment Check

Is your environment authentication and enrollment set up correctly?

## How it works:

Point XenMobile Analyzer to your XenMobile Server

xm.test.citrix.com

Provide a few details of your XenMobile Server setup to create a test environment.

Track Real Time Test Progress



- Follow the progress of your test as it is running or come back to it later.
- In case of failure, identify the exact step of your setup where issues occur.

Follow Step By Step Recommendations



View reports with support content for specific fixes to issues. Come back to rerun tests any time.

[Get Started](#)

## Step 2: Advanced Diagnostics

Is your environment optimized to prevent problems?

## Step 3: Secure Mail Readiness

Is your mail server prepared to deploy to your XenMobile environment?

## Feedback

2.Advanced Diagnostics - この手順では、環境チェックで見逃された可能性のある問題を見つけるための、Citrix Insight Servicesの使用に関する情報が提供されます。

## All Steps

## XenMobile Analyzer

Identify potential issues with your deployment

**Step 1: Environment Check**

Is your environment authentication and enrollment set up correctly? ▾

**Step 2: Advanced Diagnostics**

Is your environment optimized to prevent problems? ▲

**How it works:**

Citrix Insight Service (CIS) is Citrix's flagship Big Data platform for instrumentation &amp; telemetry and business insight generation.

Collect information on your environment

Go to your XenMobile Console &gt; Support &gt; Create Support Bundle

Upload to Citrix Insight Services

After you have created a Support Bundle, upload it to Citrix Insights Services from XenMobile Console. You will receive an email confirmation.

Analyze and fix issues

The uploaded data will be auto-analyzed against a list of known issues and best practices. A personalized report, including next step resolution recommendations will be provided - a link will be sent to your email. You can also go to CIS to view a report.

[Go To CIS](#)**Step 3: Secure Mail Readiness**

Is your mail server prepared to deploy to your XenMobile environment? ▾

## Feedback

**3. Secure Mail Readiness** - この手順では、XenMobile Exchange ActiveSync Testアプリケーションをダウンロードします。このアプリケーションを使用すると、XenMobile環境へのActiveSyncサーバーの展開に関するトラブルシューティングを行うことができます。

**Step 1: Environment Check**

Is your environment authentication and enrollment set up correctly? ▾

**Step 2: Advanced Diagnostics**

Is your environment optimized to prevent problems? ▾

**Step 3: Secure Mail Readiness**

Is your mail server prepared to deploy to your XenMobile environment? ▲

**How it works:**

Mail Test application is designed to help troubleshoot the ActiveSync servers for their readiness to be deployed with XenMobile environment. For a complete walk through the steps of this test, visit [Mail Test Application](#)

**Download app**

- Launch the Mail Test Application on your iOS device. You can choose to wrap the app.
- Add Server in Server list > Provide the credentials > Accept all certificates > Select device type and device OS

**Diagnose and fix issues**

After the test is complete, a list of servers with reports for each will be available. You can view reports and share them with Send Report.

[Download](#)**Step 4: Server Connectivity Checks**

Is your connection with NetScaler, XenMobile, Authentication and ShareFile servers working properly? ▲

**How it works:**

Check the connections to the XenMobile, Authentication and ShareFile servers

- Go to your XenMobile Console > Support > NetScaler Gateway Connectivity Checks
- Add your NetScaler Gateway Server information
- Run Test Connectivity

[Feedback](#)

4.サーバー接続チェック - この手順では、サーバーの接続性をテストする方法が示されます。

5.Citrixサポートへの問い合わせ - この手順では、依然として問題が発生する場合にCitrixサポートケースを登録するためのサイトのリンクが表示されます。

**Step 4: Server Connectivity Checks**

Is your connection with NetScaler, XenMobile, Authentication and ShareFile servers working properly? ▾

**How it works:**

Check the connections to the XenMobile, Authentication and ShareFile servers

- Go to your XenMobile Console > Support > NetScaler Gateway Connectivity Checks
- Add your NetScaler Gateway Server information
- Run Test Connectivity
  
- Go to your XenMobile Console > Support > XenMobile Connectivity Checks
- Select the server from the list
- Run Test Connectivity

**Step 5: Contact Citrix Support**

Need help in troubleshooting or to create a support case? ▾

Still having issues? Citrix Support can help!

[Create Case](#)

## Feedback

以下のセクションで、これらの手順についてより詳しく説明します。

## 環境チェックの実行

1. XenMobile Analyzerにログオンし、 [Step 1: Environment Checks] をクリックします。
2. [Get Started] をクリックします。

XenMobile | Analyzer @citrix.com

All Steps

### XenMobile Analyzer

Identify potential issues with your deployment

---

**Step 1: Environment Check**  
Is your environment authentication and enrollment set up correctly? ^

**How it works:**

Point XenMobile Analyzer to your XenMobile Server xm.test.citrix.com Provide a few details of your XenMobile Server setup to create a test environment.

Track Real Time Test Progress  • Follow the progress of your test as it is running or come back to it later.  
• In case of failure, identify the exact step of your setup where issues occur.

Follow Step By Step Recommendations   View reports with support content for specific fixes to issues. Come back to rerun tests any time.

[Get Started](#)

---

**Step 2: Advanced Diagnostics**  
Is your environment optimized to prevent problems? v

---

**Step 3: Secure Mail Readiness**  
Is your mail server prepared to deploy to your XenMobile environment? v

Feedback

3. [Add Test Environment] をクリックします。

XenMobile | Analyzer @citrix.com

All Steps > Test Environments

### Test Environment List

Test your server setup before deploying

+ Add Test Environment
🔄 Refresh

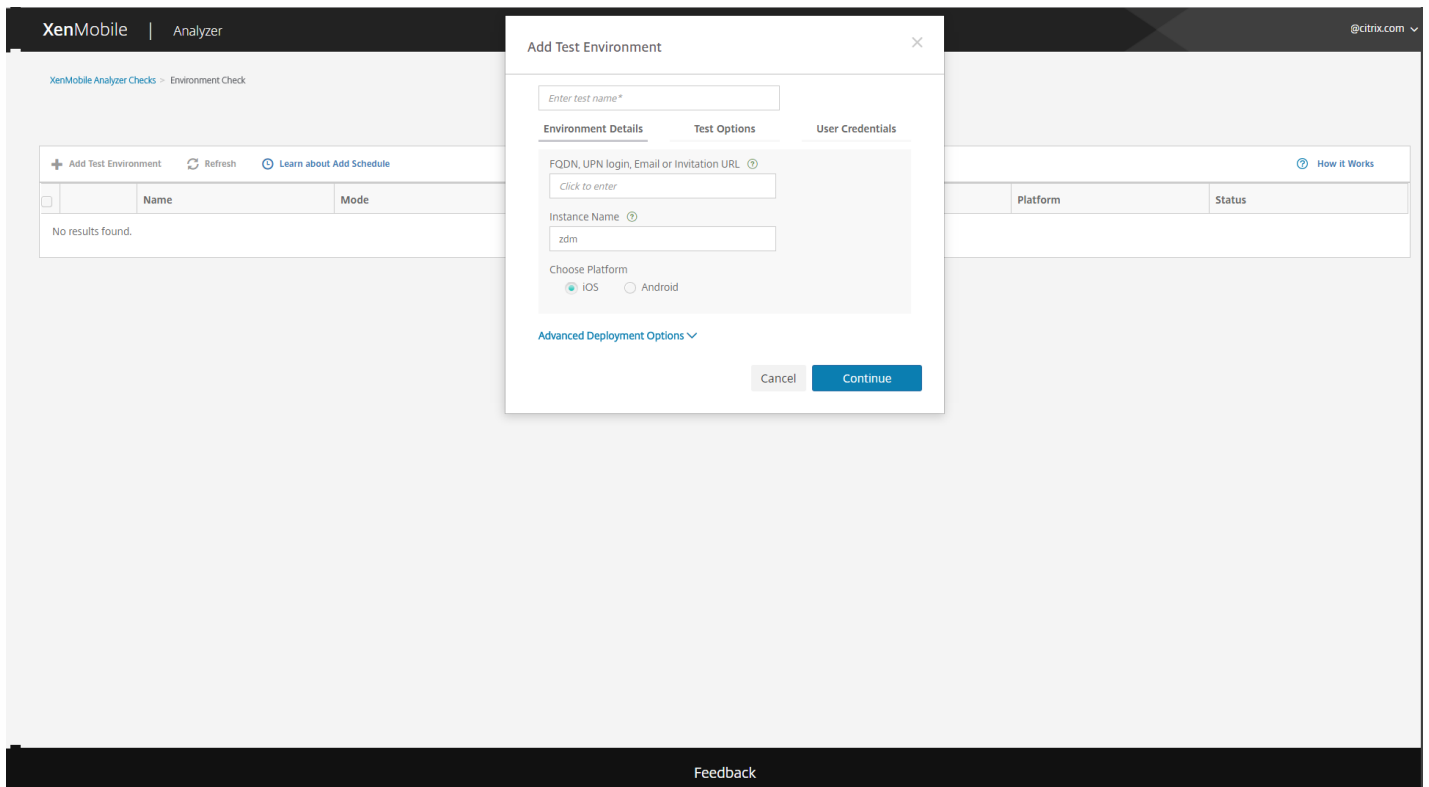
<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
No results found.						

Feedback

4. 新しい [Add Test Environment] ダイアログボックスで、以下の操作を行います。

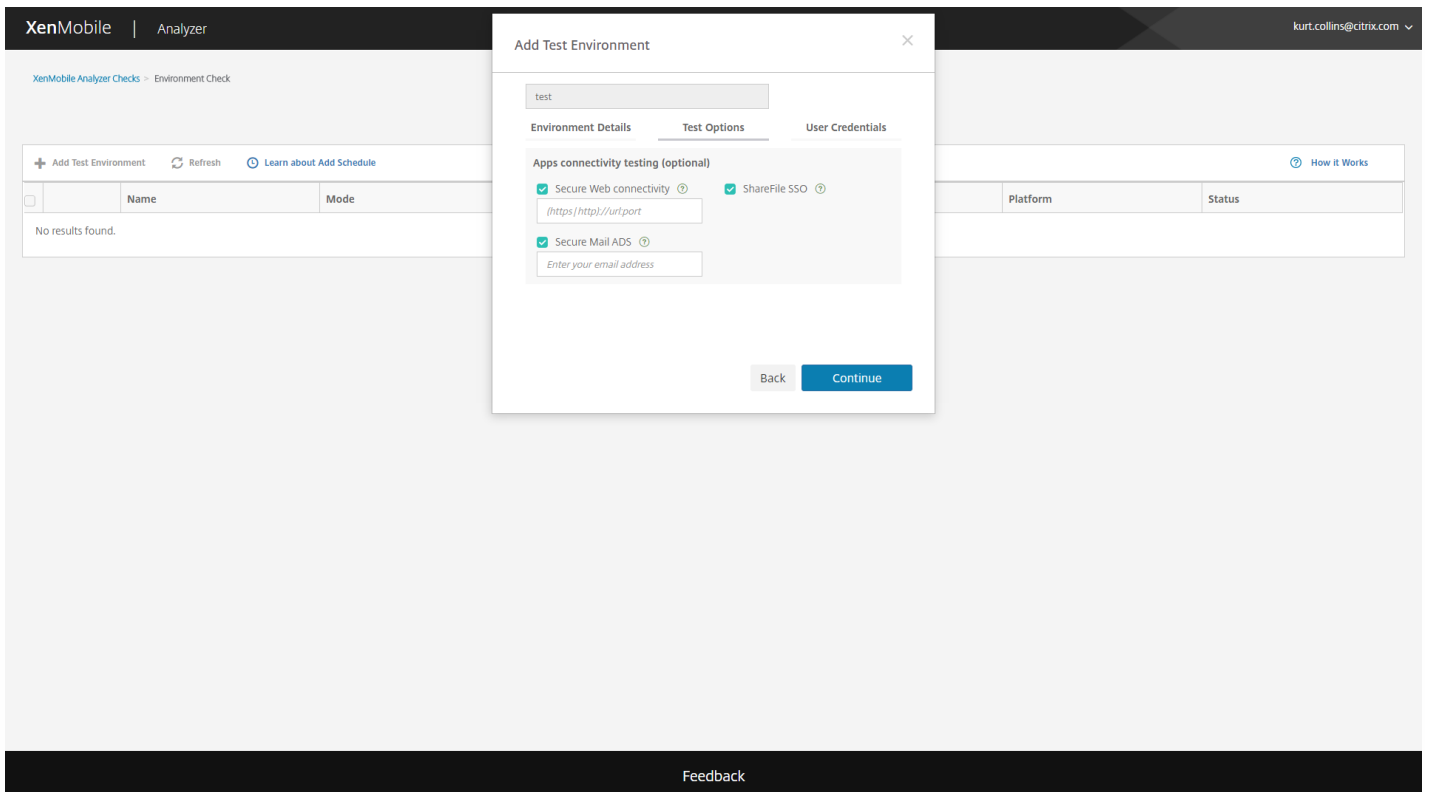


上のスクリーンショットのWorx Homeは、現在ではSecure Hubと呼ばれている点に注意してください。

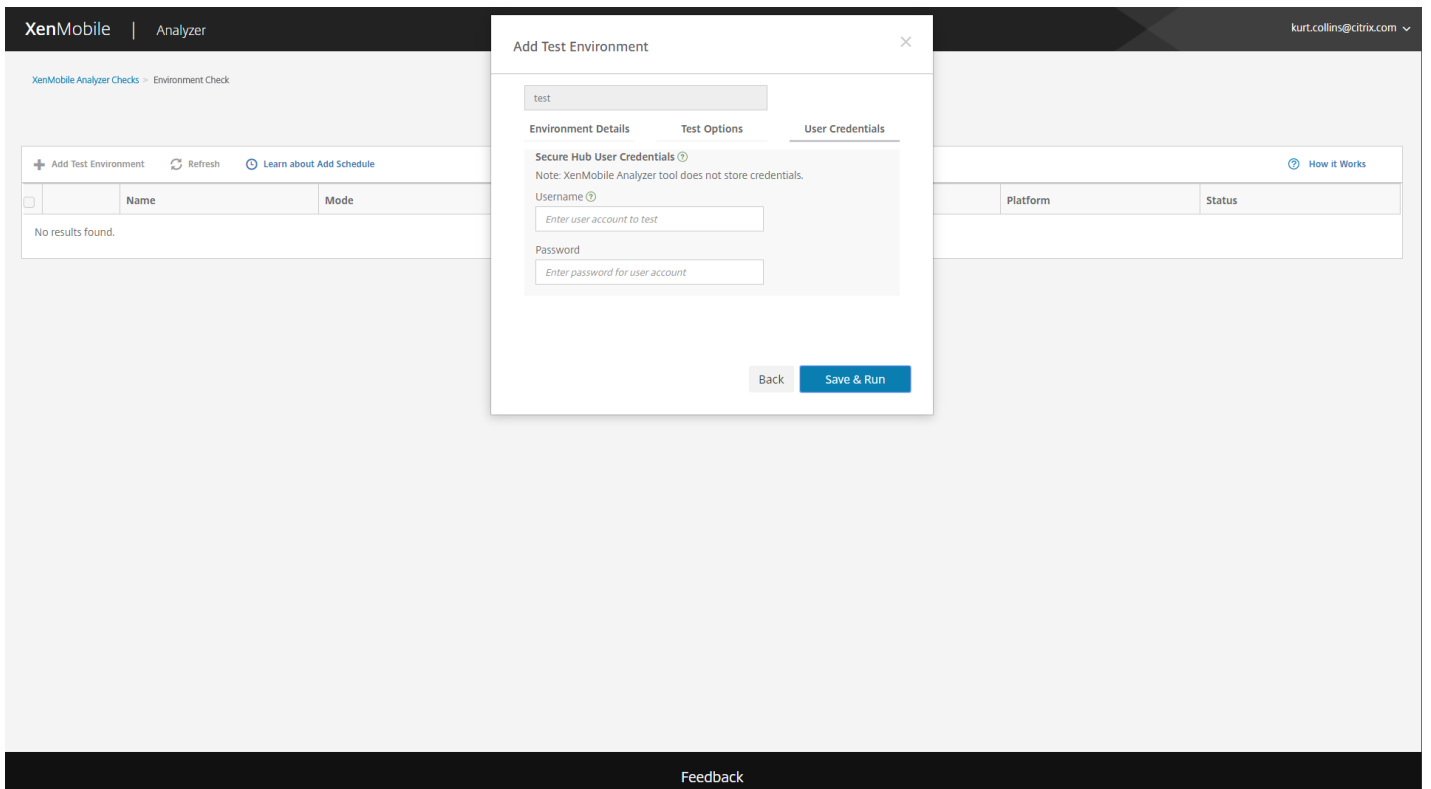


- a. 今後テストを特定できるように、テストの一意の名前を入力します。
- b. [FQDN, UPN login, Email or URL Invitation] フィールドで、サーバーへのアクセスに使用する情報を入力します。
- c. カスタムインスタンスを使用している場合は、[Instance Name] にその値を入力します。
- d. [Choose Platform] で、テスト用のプラットフォームとしてOSまたはAndroidを選択します。
- e. [Advanced Deployment Options] を展開すると、[Deployment Mode] 一覧で、使用するXenMobile展開モードを選択できます。使用できるオプションは [Enterprise (MDM + MAM)]、[App Management (MAM)] または [Device Management (MDM)] です。

上のスクリーンショットのWorx Homeは、現在ではSecure Hubと呼ばれている点に注意してください。



5. [Continue] をクリックします。



上のスクリーンショットのWorxWebは現在ではSecure Web、WorxMailはSecure Mailと呼ばれている点に注意してください。

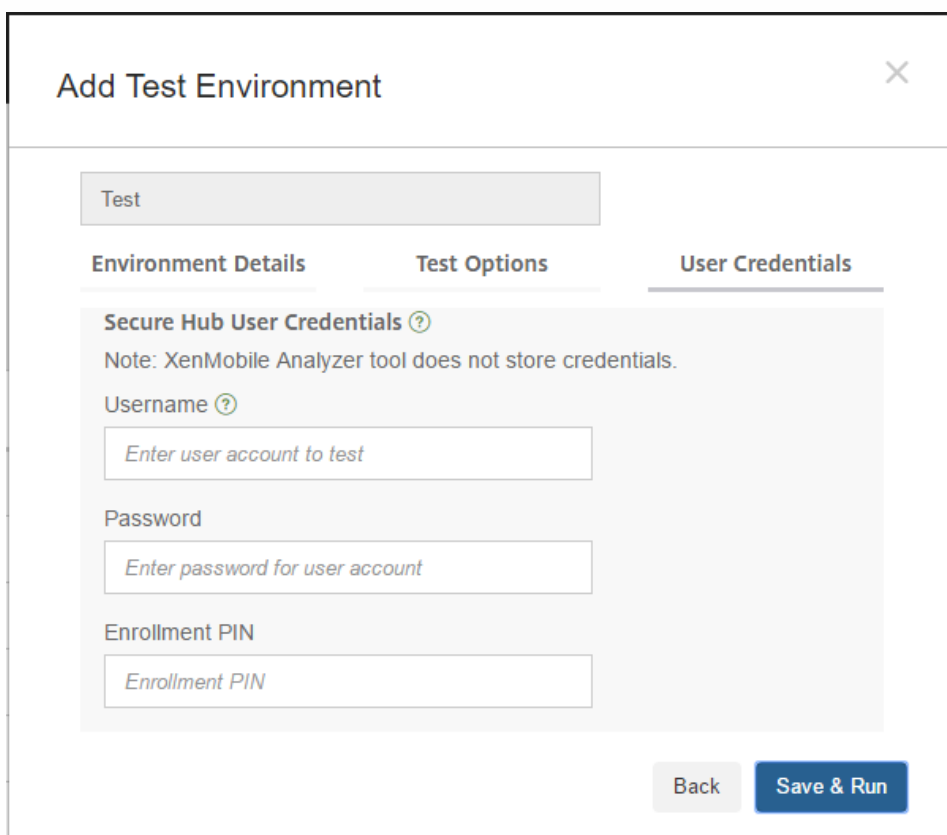
6. 実行するアプリケーションレベルのテストを選択します。次のテストの1つ以上を選択できます。

a. **Secure Web micro VPN Connectivity with intranet sites**。イントラネットのURLを指定します。ツールにより、入力したURLの到達可能性がテストされます。このテストでは、イントラネットのURLへの接続時にSecure Webアプリで生じる可能性のある、接続に関する問題が検出されます。

b. **Secure Mail ADS**。ユーザーの電子メールIDを指定します。このIDを使用して、XenMobile環境にあるMicrosoft Exchange Serverの自動検出機能がテストされます。Secure Mail Auto Discovery関連の問題があるかどうかを検出されます。

c. **ShareFile SSO**。このテストを選択した場合、ShareFileのDNS解決が正常に行われるかどうか、および指定したユーザー資格情報でShareFileシングルサインオン (SSO) を行うことができるかどうかをテストされます。

7. [Continue] をクリックします。

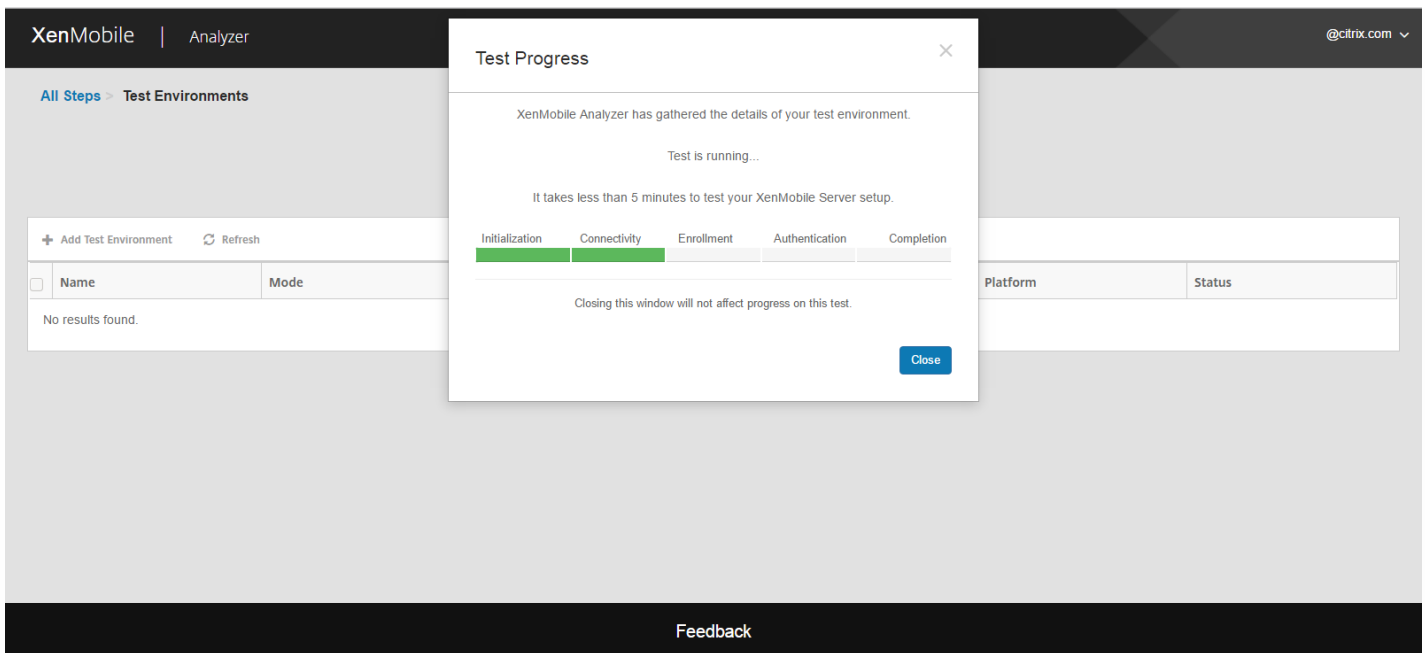


8. サーバーのセットアップによっては [User Credentials] の入力フィールドが異なる表示になることがあります。このフィールドには、[Username] のみ、[Username] と [Password]、または [Username]、[Password]、および [Enrollment PIN] があります。

9. この情報を入力後、[Save & Run] をクリックしてテストを開始します。

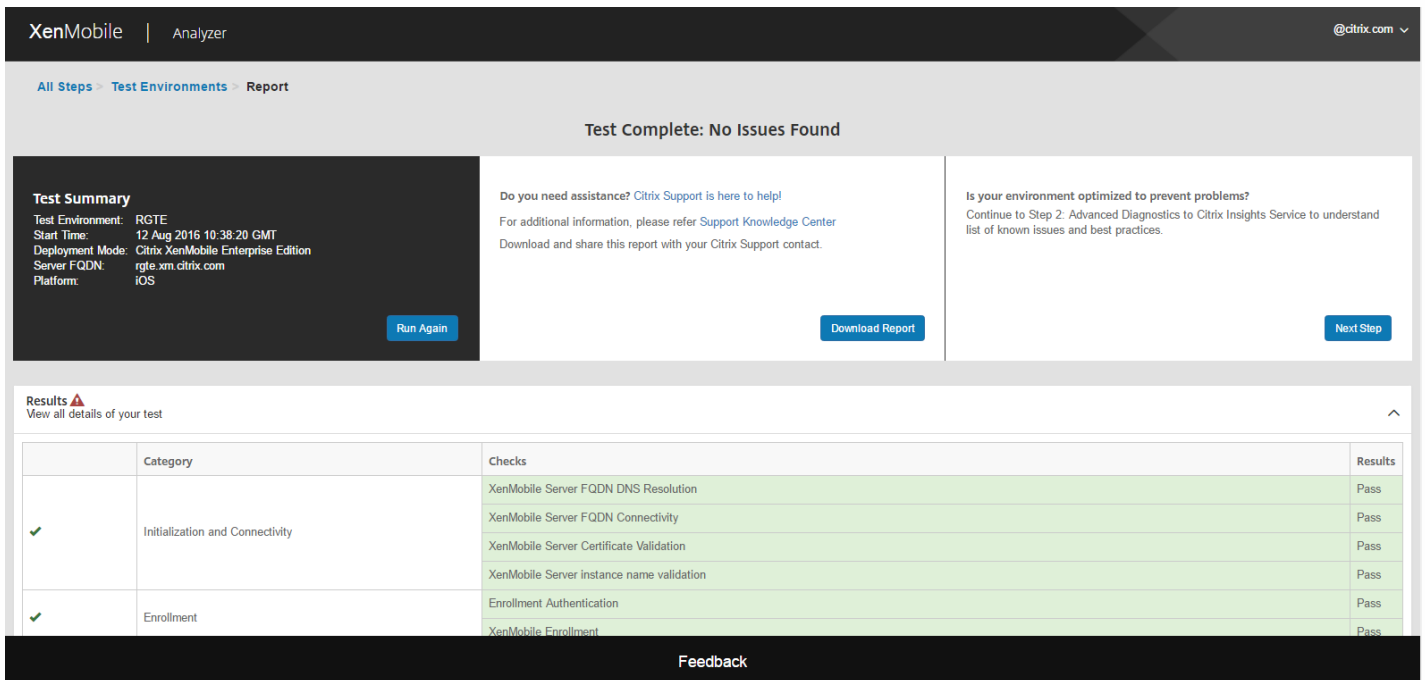
進行状況が表示されます。この進行状況を示すダイアログボックスは開いたままにしても、閉じて構いません。どちらの場合でもテストは続行されます。

問題なく完了したテストは緑色で表示されます。失敗したテストは赤色で表示されます。



8. 進行状況を示すダイアログボックスを閉じた後、[Test Environments List] ページに戻って [View Report] アイコンをクリックすると、テスト結果を確認することができます。

[Results] ページには、テストの詳細、推奨項目、結果が表示されます。



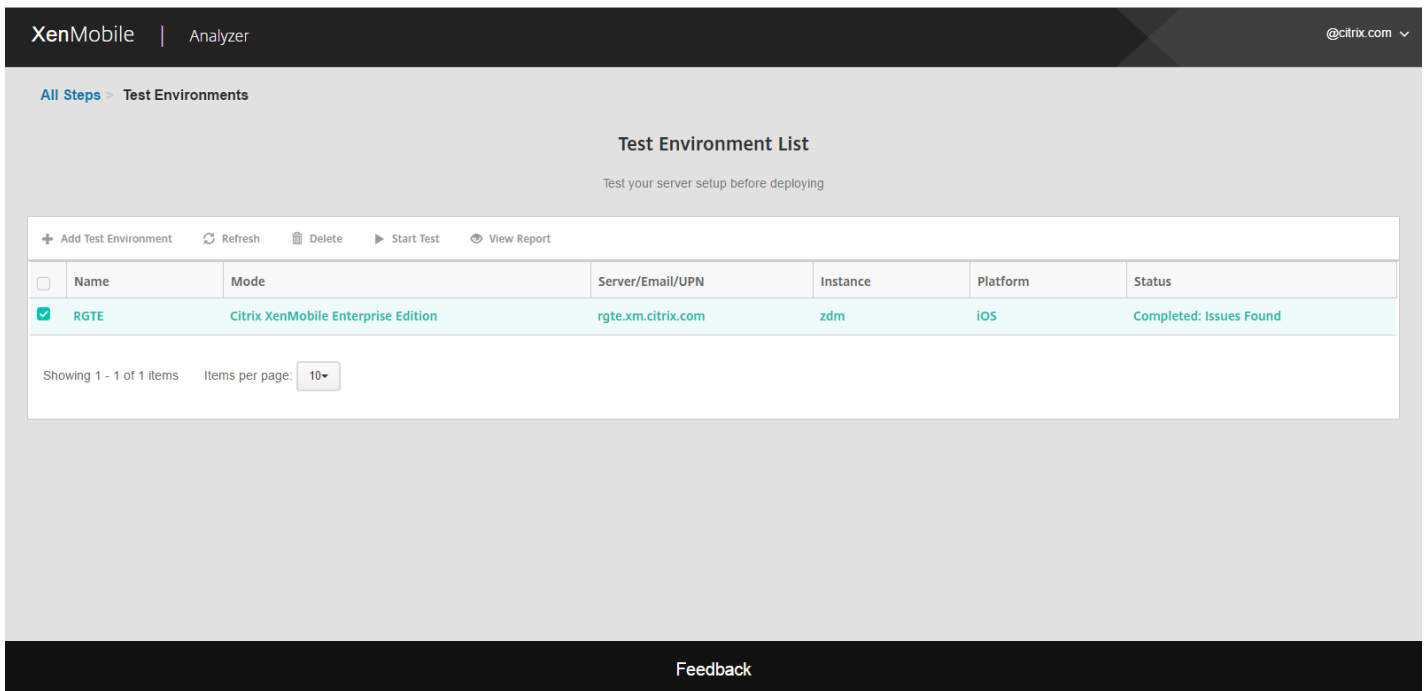
✓	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✓	App Enumeration	Device Registration	Pass
		WorxStore Connectivity	Pass
		WorxStore App Listing (13)	Pass
✓	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

## Feedback

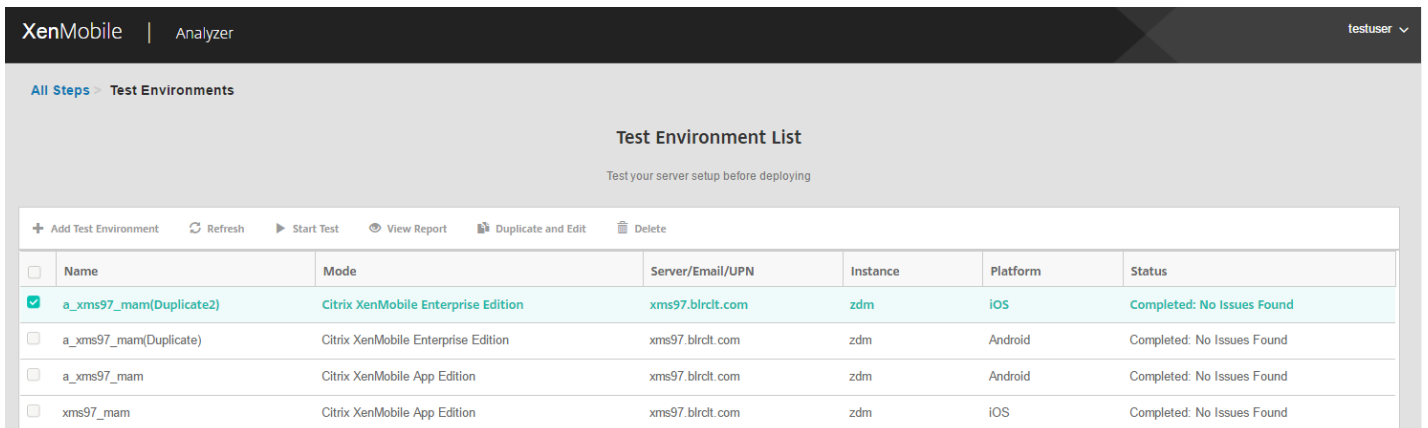
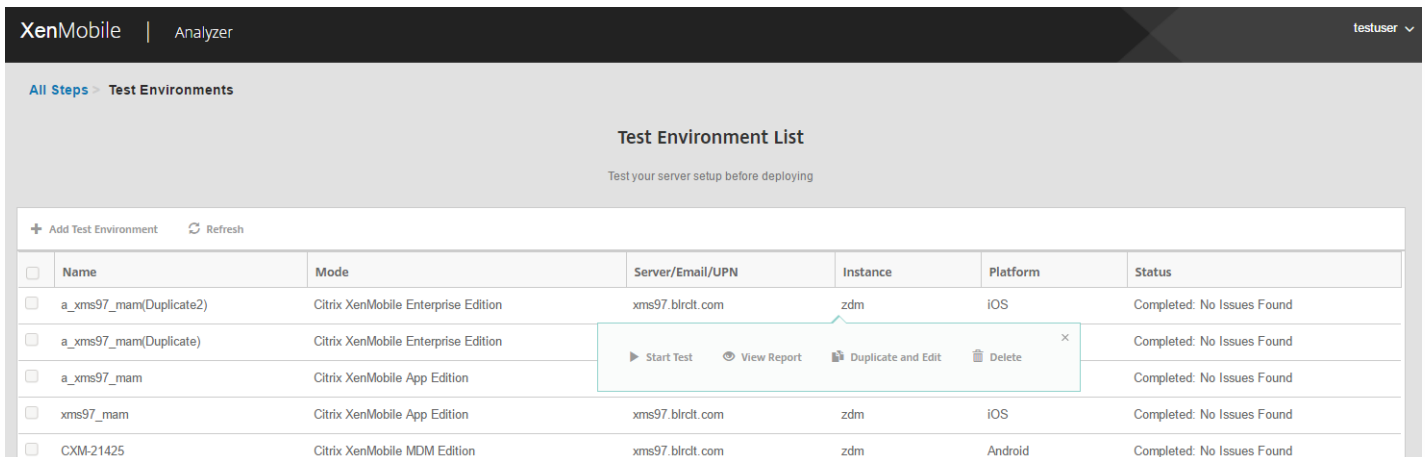
上のスクリーンショットのWorxWebは現在ではSecure Web、WorxNotesはSecure Notes、WorxTasksはSecure Tasks、WorxStoreはXenMobile Storeと呼ばれている点に注意してください。

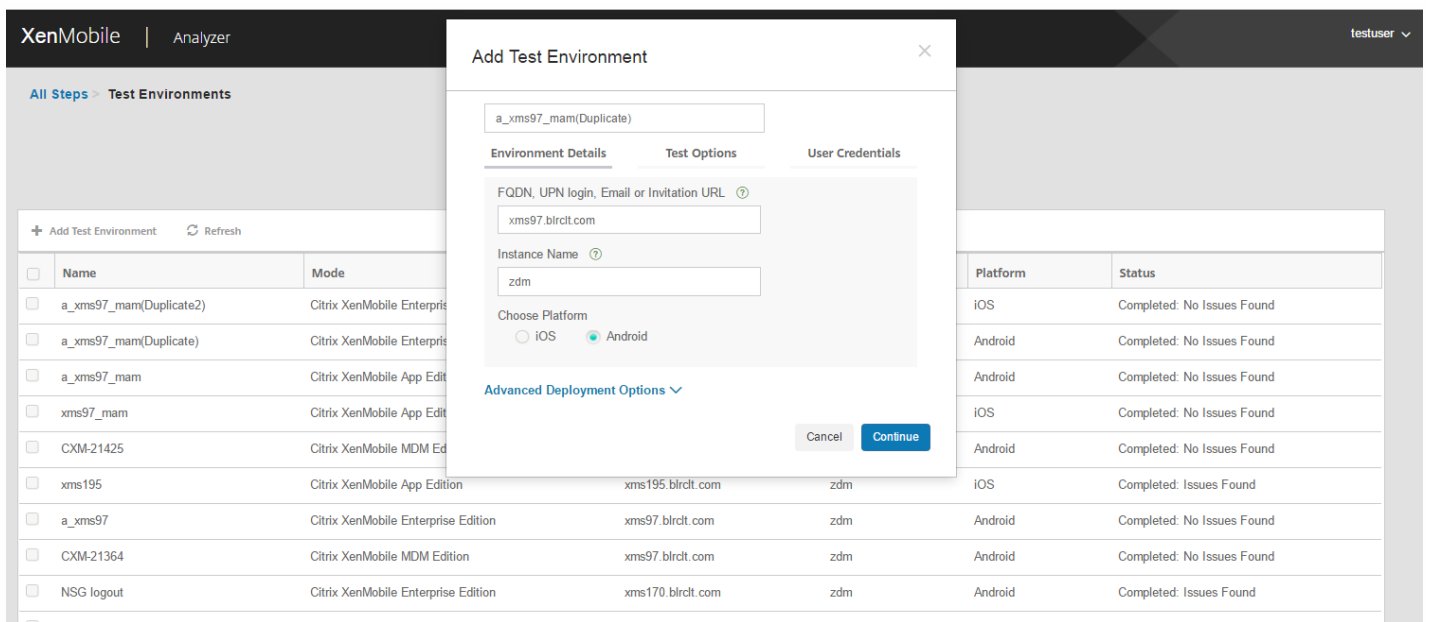
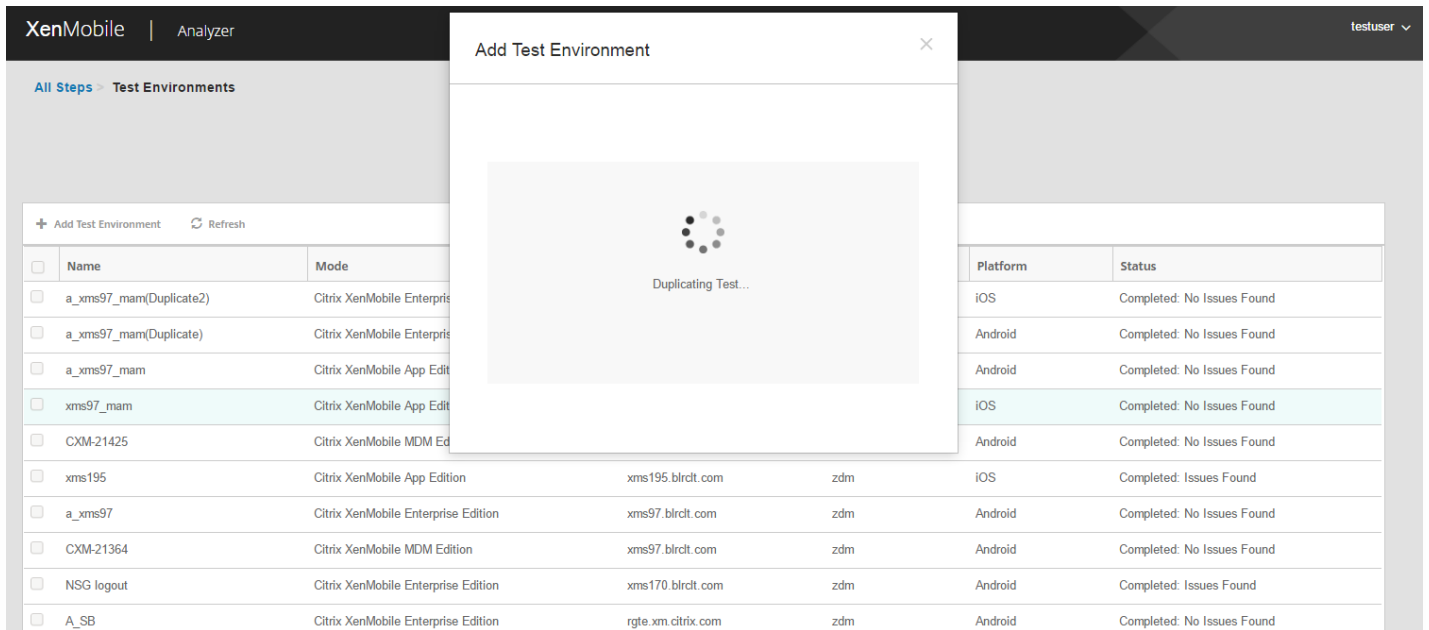
Citrix Knowledge Baseの記事に関連する推奨事項がある場合は、該当の記事がこのページに一覧表示されます。

9. **[Results]** タブをクリックすると、個別のカテゴリーとツールが実行したテストが、結果とともに表示されます。
  - a. レポートをダウンロードするには、**[Download Report]** をクリックします。
  - b. テスト環境の一覧に戻るには、**[Test Environments]** をクリックします。
  - c. 同じテストをもう一度実行するには、**[Run Again]** をクリックします。
  - d. 別のテストをもう一度実行するには、**[Test Environments]** に戻って再実行するテストを選択し、**[Start Test]** をクリックします。
  - e. XenMobile Analyzerの次の手順に進むには、**[Next Step]** をクリックします。



10. [Test Environments] ページで、テストをコピーし、編集できます。このためには、テストを選択し、[Duplicate and Edit] をクリックします。選択したテストのコピーが作成され、[Add Test Environment] ダイアログが開いて新しいテストを変更できるようになります。





## XenMobile Analyzerの手順2～5の実行

XenMobile Analyzerの環境チェック手順では直接操作してテストを実行しますが、手順2～5では役立つ情報が提供されます。これらの各手順では、XenMobile環境を正しく設定するために使用できる他のツールに関する情報が提供されます。

- **手順2 - 詳細診断**：この手順では、環境に関する情報を収集して、Citrix Insight Servicesにアップロードします。このツールによってデータが分析され、環境に合ったレポートが推奨される解決方法とともに提供されます。
- **手順3 - Secure Mailの用意**：この手順では、XenMobile Exchange ActiveSync Testアプリケーションをダウンロードして実行します。このアプリケーションでは、XenMobile環境への展開についてのActiveSyncサーバーのトラブルシューティング

グを行います。アプリケーションを実行した後に、レポートを確認したり他のユーザーと共有したりできます。

- 手順4 - サーバー接続チェック：この手順では、XenMobileサーバー、認証サーバー、およびShareFileサーバーへの接続を確認するための手順が示されます。
- 手順5 - Citrixサポートへの問い合わせ：他のすべての手順が失敗した場合は、Citrixサポートでサポートチケットを作成できます。

## 既知の問題

XenMobile Analyzerに関する既知の問題は次のとおりです。

- XenMobile Serverにプラットフォーム制限ポリシーが設定されている場合、一覧に記載されるアプリの数は、クライアントに応じて異なることがあります。
- Secure Webのイントラネット接続に関するチェックを実行する場合、テキストボックスに複数のURLを入力することはできません。
- Secure Hubの共有デバイス認証機能は使用できません。
- Secure Webテストは入力されたURLへの接続をチェックするだけで、関連サイトへの認証はチェックしません。
- PINベースの認証モードで、Secure Mail ADSテストを選択する場合、テストを実行するためのパスワードの入力が必要です。このパスワードは、登録や認証のためのものではありません。

## 解決された問題

以下のXenMobile Analyzerの問題は解決されました。

- 登録招待を使用してチェックを実行すると、テストは成功しますが登録招待は受理されません。



# XenMobileでのログファイルの表示および分析

Apr 27, 2017

1. XenMobileコンソールで、右上のレンチアイコンをクリックします。[Support] ページが開きます。
2. [Log Operations] の下の [Logs] をクリックします。[Logs] ページが開きます。表に個別のログが表示されます。

XenMobile Analyze Manage Configure administrator

Support > Logs

## Logs

Analyze the details of various types of logs.

Download All

<input type="checkbox"/>	Log Name	Log Type
<input type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

3. 表示するログをオンにします。

- デバッグログファイルには、エラーメッセージやサーバー関連のアクションなど、Citrixのサポート担当者向けの有用な情報が含まれています。
- 管理監査ログファイルには、XenMobileコンソール上の活動についての監査情報が含まれています。
- ユーザー監査ログファイルには構成済みユーザーに関連する情報が含まれています。

4. 表の上にあるアクションを使用して、すべてダウンロード、表示、回転、単一ログのダウンロード、選択したログの削除を行います。

## Logs

Analyze the details of various types of logs.

 Download All | 
  View | 
  Rotate | 
  Download | 
  Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug

注：






- 複数のログファイルを選択した場合は、[Download All] と [Rotate] のみを使用できます。
- XenMobileサーバーをクラスター化している場合は、接続しているサーバーのログのみを表示できます。ほかのサーバーのログを表示するには、ダウンロードオプションのいずれかを使用します。

5. 次のいずれかを行います。

- **Download All** : システム上に存在するすべてのログ（デバッグ、管理監査、ユーザー監査、サーバーのログなど）をダウンロードします。
- **View** : 表の下に選択したログの内容を表示します。
- **Rotate** : 現在のログファイルをアーカイブし、ログエントリを取得するための新しいファイルを作成します。ログファイルをアーカイブするときに、ダイアログボックスが開きます。[Rotate] をクリックして続行します。
- **Download** : 選択されている単一の種類のログファイルのみをダウンロードします。アーカイブ済みの同じ種類のログもダウンロードされます。
- **Delete** : 選択したログファイルを完全に削除します。

### Logs

Analyze the details of various types of logs.

 Download All | 
  View | 
  Rotate | 
  Download | 
  Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2016-11-06T06:28:38.908-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTaskJob: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2.
2016-11-06T06:30:38.945-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.985-0800 | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.593-0800 | INFO | pool-7-thread-1 | com.zenoss.plugins.cdm.plugins.OscoReconnectorService | Reloading OCSB Service data

```



# REST API

Apr 27, 2017

XenMobile REST APIにより、XenMobileコンソールで公開されるサービスを呼び出すことができます。RESTクライアントを使用して、RESTサービスを呼び出すことができます。APIについて、サービスを呼び出すためにXenMobileコンソールにサインオンする必要はありません。

現在使用できるAPIの完全な一覧については、[XenMobile REST APIリファレンスのPDFファイル](#)をダウンロードしてください。この記事には、APIの完全なセットは含まれません。

## REST APIへのアクセスに必要な権限

REST APIにアクセスするには、次の権限のうち1つが必要です。

- 役割ベースのアクセス構成の一部として設定されたパブリックAPIアクセス権限（役割ベースのアクセスの設定については、「[RBACを使用した役割の構成](#)」を参照してください）
- スーパーユーザー権限

## REST APIサービスを呼び出すには

RESTクライアントまたはCURLコマンドを使用して、REST APIサービスを呼び出すことができます。以下の例では、Advanced REST client for Chromeを使用します。

### 注意

以下の例のホスト名とポート番号は、自分の環境に合わせて変更してください。

URL : `https://<ホスト名>:<ポート番号>/xenmobile/api/v1/authentication/login`

Request: { "login":"administrator", "password":"password" }

Method type : POST

Content type : application/json

https://localhost:4443/xenmobile/api/v1/publicapi/login

GET
  POST
  PUT
  PATCH
  DELETE
  HEAD
  OPTIONS
  Other

Raw Form Headers

Raw Form Files (0) Payload

Encode payload Decode payload

```

{
  "login": "administrator",
  "password": "password"
}

```

application/json Set "Content-Type" header to overwrite this value.

Clear Send

Status **200 OK** Loading time: 265 ms

Request headers

- User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36
- Origin: chrome-extension://hgmlfoofddfdnphfgcellkdfbfjeloo
- Content-Type: application/json
- Accept: \*/\*
- Accept-Encoding: gzip, deflate
- Accept-Language: en-US,en;q=0.8
- Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163

Response headers

- Server: Apache-Coyote/1.1
- Content-Type: text/plain
- Content-Length: 53
- Date: Sun, 22 Mar 2015 22:43:48 GMT

Raw Parsed Response

Open output in new window Copy to clipboard Save as file Open in JSON tab

```

{"auth_token": "d4fdecf6-2e5a-4aed-8d60-f9a513b5c358"}

```

Code highlighting thanks to [Code Mirror](#)

# SOAP API

Apr 27, 2017

Citrixは、SOAP WebサービスAPIのサポートを停止しました。代わりに、REST APIを使用してください。詳しくは、[REST API](#)を参照してください。

# XenMobile Mail Manager 10.x

Apr 27, 2017

XenMobile Mail Managerには、XenMobileの機能を拡張する以下の機能が備わっています。

- Exchange ActiveSync (EAS) デバイスに対するダイナミックアクセス制御。EASデバイスのExchangeサービスに対するアクセスを自動的に許可または禁止できます。
- Exchangeが提供するEASデバイスパートナーシップ情報にアクセスする機能のXenMobileへの提供。
- モバイルデバイスでEASワイプを実行する機能のXenMobileへの提供。
- Blackberryデバイスに関する情報にアクセスしたり、ワイプやパスワードリセットなどの制御操作を実行したりする機能のXenMobileへの提供。

XenMobile Mail Managerをダウンロードするには、[Citrix.com](http://Citrix.com)のXenMobile 10サーバーのサーバーコンポーネントのセクションに移動します。

## XenMobile Mail Manager 10.1の新機能

### アクセス規則

[Rule Analysis] ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。

デフォルトのアクセス権 (Allow、Block、またはUnchanged) とActiveSyncコマンドモード (PowerShellまたはSimulation) は、XenMobile展開に構成されている各Microsoft Exchange環境ごとに別々に設定されます。

### スナップショット

スナップショット履歴に表示されるスナップショットの最大数を構成できます。

メジャースナップショット時にどのエラーを無視するかを構成できます。無視可能と構成されていないエラーがメジャースナップショットにより戻された場合、スナップショットの結果は放棄されます。

エラーを無視可能と構成するには、XMLエディターを使用してconfig.xmlファイルを次のように編集します。

- Exchange ServerがOffice 365の場合は、  
/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。正規表現がサポートされます。
- Exchange Serverがオンプレミスの場合は、  
/ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrorsノードに移動し、子要素として照合する、既存のError子要素と同じ形式のテキストを追加します。正規表現がサポートされます。
- 複数のExchange環境が構成されている場合は、/ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='目的のExchange環境に対応するID']/ExchangeServer/Specialists/PowerShellノードに移動します。無視するエラーそれぞれに対して、IgnorableErrors子ノードをPowerShellノードに追加します。照合するテキストをCDATAセクションに含むError子ノードをIgnorableErrorsノードに追加します。正規表現がサポートされます。

config.xmlを保存して、XenMobile Mail Managerサービスを再起動します。

### PowerShellおよびExchange

XenMobile Mail Managerは、使用するコマンドレットを、接続先のExchangeのバージョンに基づいて動的に決定するようになりました。たとえば、Exchange 2010の場合はGet-ActiveSyncDeviceを使用しますが、Exchange 2013およびExchange 2016の場合はGet-MobileDeviceを使用します。

### Exchangeの構成

Exchange Server構成は、XenMobile Mail Managerサービスを再起動せずに編集および更新できます。

Exchange環境の [概要] タブに追加された2つの新しい列には、各環境のコマンドモード (PowerShellまたはSimulation) とアクセスモード (Allow、Block、またはUnchanged) が表示されます。

## トラブルシューティングおよび診断

Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

コンソールの [Configuration] ウィンドウの [Test Connectivity] ボタンを使用してExchangeサービスの接続性をテストすると、サービスが使用するすべての読み取り専用コマンドレットが実行され、構成されたユーザーのRBAC権限テストがExchange Serverに対して実行され、エラーや警告が色分けされて表示されます (警告は青と黄、エラーは赤とオレンジ)。

新しいトラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。

サポートシナリオでは、コンソールで診断ダイアログボックスを選択することで、XenMobile Mail Managerによって管理されるすべてのデバイス上のすべてのメールボックスのすべてのプロパティを保存できます。

サポートシナリオで、トレースレベルのログがサポートされるようになりました。

## 認証

XenMobile Mail Managerは、オンプレミス展開でBasic認証をサポートします。これにより、XenMobile Mail ManagerサーバーがExchange Serverが存在するドメインのメンバーでなくても、XenMobile Mail Managerを使用できるようになります。

# 解決された問題

## アクセス規則

XenMobile Mail Managerは、Active Directory (AD) グループに1000人以上のユーザーが含まれる場合でも、ADグループのすべてのユーザーにローカルアクセス制御ルールを適用します。以前、XenMobile Mail Managerは、ADグループの最初の1000人のユーザーだけにローカルアクセス制御ルールを適用していました。[#548705]

1000人以上のユーザーが含まれるActive Directoryグループに対してクエリを行った場合、XenMobile Mail Managerコンソールが応答しなくなる場合があります。[CXM-11729]

[LDAP Configuration] ウィンドウに不正確な認証モードが表示されないようになりました。[CXM-5556]

## スナップショット

ユーザー名にアポストロフィが含まれていても、マイナースナップショットが失敗しなくなりました。[#617549]

パイプライン化が無効化されたサポートシナリオで (XenMobile Mail Managerコンソールの [構成] ウィンドウで [パイプライン化の無効化] オプションを選択)、オンプレミスExchange環境でもメジャースナップショットが失敗しなくなりました。[#586083]

パイプライン化が無効化されたサポートシナリオで (XenMobile Mail Managerコンソールの [Configuration] ウィンドウで [Disable Pipelining] オプションを選択)、詳細スナップショットと簡易スナップショットのどちらのために環境が構成されているかに関係なく、詳細スナップショット用のデータが収集されなくなりました。詳細スナップショット用のデータが収集されるのは、環境が詳細スナップショット用に構成されているときだけになりました。[#586092]

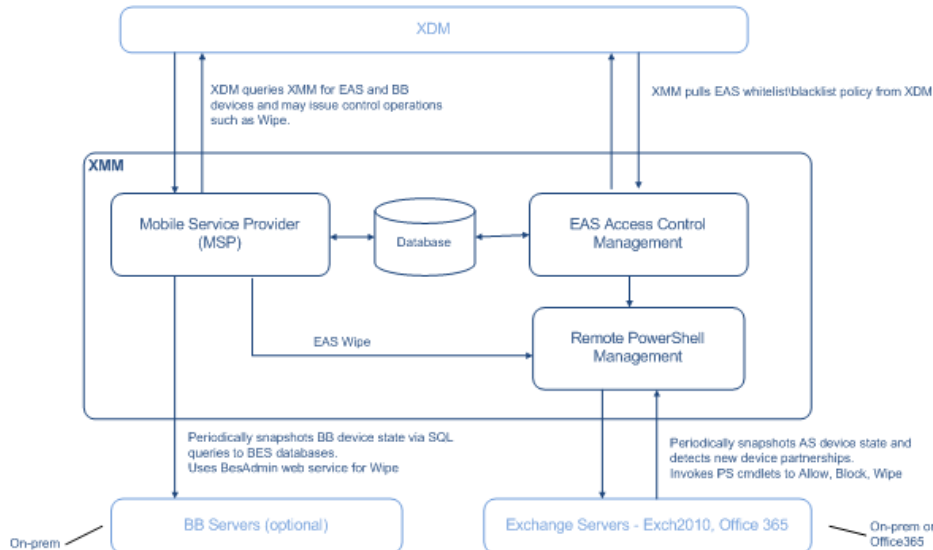
初期インストール後の最初のメジャースナップショットがエラーになることがあり、その場合、XenMobile Mail Managerサービスが再起動されるまで、XenMobile Mail Managerがあらためてメジャースナップショットを実行することはできませんでした。そのようなことにもう発生しません。[CXM-5536]



# アーキテクチャ

Apr 27, 2017

次の図に、XenMobile Mail Managerの主要コンポーネントを示します。リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の、[オンプレミス展開のリファレンスアーキテクチャ](#)についての記事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

Apr 27, 2017

XenMobile Mail Managerを使用するには、以下のシステム環境が必要です。

- Windows Server 2012 R2、Windows Server 2008 R2（英語ベースのサーバーであることが必須）
- Microsoft SQL Server 2016、SQL Server 2012、SQL Server 2012 Express LocalDB、またはSQL Server Express 2008
- Microsoft .NET Framework 4.5
- Blackberry Enterprise Service, version 5（オプション）

## Microsoft Exchange Serverのサポートされる最小バージョン

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 SP2

## デバイスのメールクライアント

すべてのメールクライアントが、デバイスに関して一貫して同じActiveSync IDを返すわけではありません。XenMobile Mail Managerは、各デバイスに対して一意のActiveSync IDを前提とするため、デバイスごとに一意の同じActiveSync IDを一貫して生成するメールクライアントのみをサポートします。以下のメールクライアントはテスト済みで、エラーなく実行できます。

- HTCのネイティブメールクライアント
- Samsungのネイティブメールクライアント
- iOSのネイティブメールクライアント
- Touchdown for Smartphones

- Windows Management Frameworkがインストールされていること。
  - PowerShell V5、V4、V3
- PowerShell実行ポリシーがSet-ExecutionPolicy RemoteSignedによってRemoteSignedに設定されていること。
- XenMobile Mail Managerを実行しているコンピューターとリモートのExchange Serverの間で、TCPポート80が開いていること。

## Exchangeを実行しているオンプレミスコンピューターの要件

**権限。**Exchangeの構成UIで指定される資格情報を使用してExchange Serverに接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセスが付与される必要があります。

- **Exchange Server 2010 SP2の場合：**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

● **Exchange Server 2013およびExchange Server 2016の場合 :**

- Get-CASMailbox
- Set-CASMailbox
- Get-Mailbox
- Get-MobileDevice
- Get-MobileDeviceStatistics
- Clear-MobileDevice
- Get-ExchangeServer
- Get-ManagementRole
- Get-ManagementRoleAssignment

- フォレスト全体を表示するようにXenMobile Mail Managerが構成されている場合は、Set-AdServerSettings -ViewEntireForest \$trueを実行するための権限が付与されている必要があります。
- 指定された資格情報には、リモートシェルを介して、Exchange Serverに接続する権限が与えられている必要があります。デフォルトでは、Exchangeをインストールしたユーザーがこの権限を持ちます。
- Microsoft TechNetサポート技術情報「[about\\_Remote\\_Requirements](#)」によれば、リモート接続を確立してリモートコマンドを実行するには、資格情報がリモートマシンの管理者であるユーザーに対応している必要があります。ブログ記事[You Don't Have to Be An Administrator to Run Remote PowerShell Commands](#)に記載されているように、Set-PSSessionConfigurationを使用して管理要件を無視できます。ただし、このコマンドの詳細のサポートと説明については、このドキュメントでは扱いません。
- Exchange Serverは、HTTPを介してリモートPowerShell要求をサポートするように構成されている必要があります。通常、Exchange Serverで次のPowerShellコマンドを実行する管理者にとって必要なのは、WinRM QuickConfigだけです。
- Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。Exchange 2010の場合、1人のユーザーに許可されている同時接続数のデフォルトは18です。接続数の上限に達すると、XenMobile Mail ManagerはExchange Serverに接続できなくなります。PowerShellの同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShellによるリモート管理に関連する、Exchangeの調整ポリシーについて調べてください。

- **権限。**Exchangeの構成UIで指定される資格情報を使用してOffice 365に接続でき、次のExchange固有のPowerShellコマンドレットを実行するためのフルアクセスが付与される必要があります。

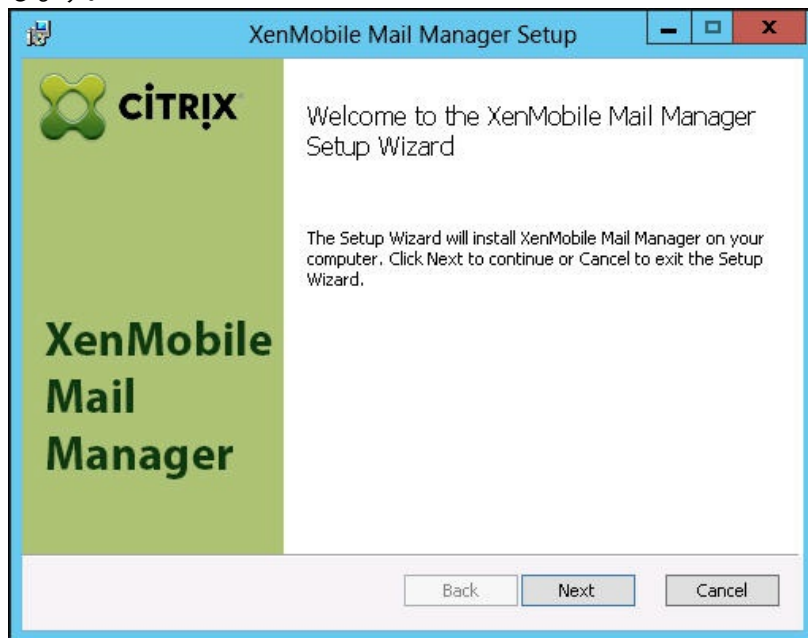
- Get-CASMailbox
- Set-CASMailbox
- Get-Mailbox
- Get-MobileDevice
- Get-MobileDeviceStatistics
- Clear-MobileDevice
- Get-ExchangeServer
- Get-ManagementRole
- Get-ManagementRoleAssignment

- **特権。**指定された資格情報には、リモートシェルを介して、Office 365サーバーに接続する権限が与えられている必要があります。デフォルトでは、Office 365のオンライン管理者には、必要な権限が備えられています。
- **調整ポリシー。**Exchangeには多くの調整ポリシーがあります。調整ポリシーのいずれかによって、各ユーザーに対して許可されるPowerShellの同時接続数が制御されます。Office 365の場合、1人のユーザーに許可されている同時接続数のデフォルトは3です。接続数の上限に達すると、XenMobile Mail ManagerはExchange Serverに接続できなくなります。PowerShellの同時接続数の上限を変更する方法はいくつかありますが、このドキュメントでは扱いません。関心がある場合は、PowerShellによるリモート管理に関連する、Exchangeの調整ポリシーについて調べてください。

# インストールと構成

Apr 27, 2017

1. XmmSetup.msiファイルをクリックして、インストーラーのプロンプトに従い、XenMobile Mail Managerをインストールします。



2. セットアップウィザードの最後の画面で、**[Launch the Configure utility]** をオンのままにしておきます。または、[スタート]メニューの[XenMobile Mail Manager]を選択します。

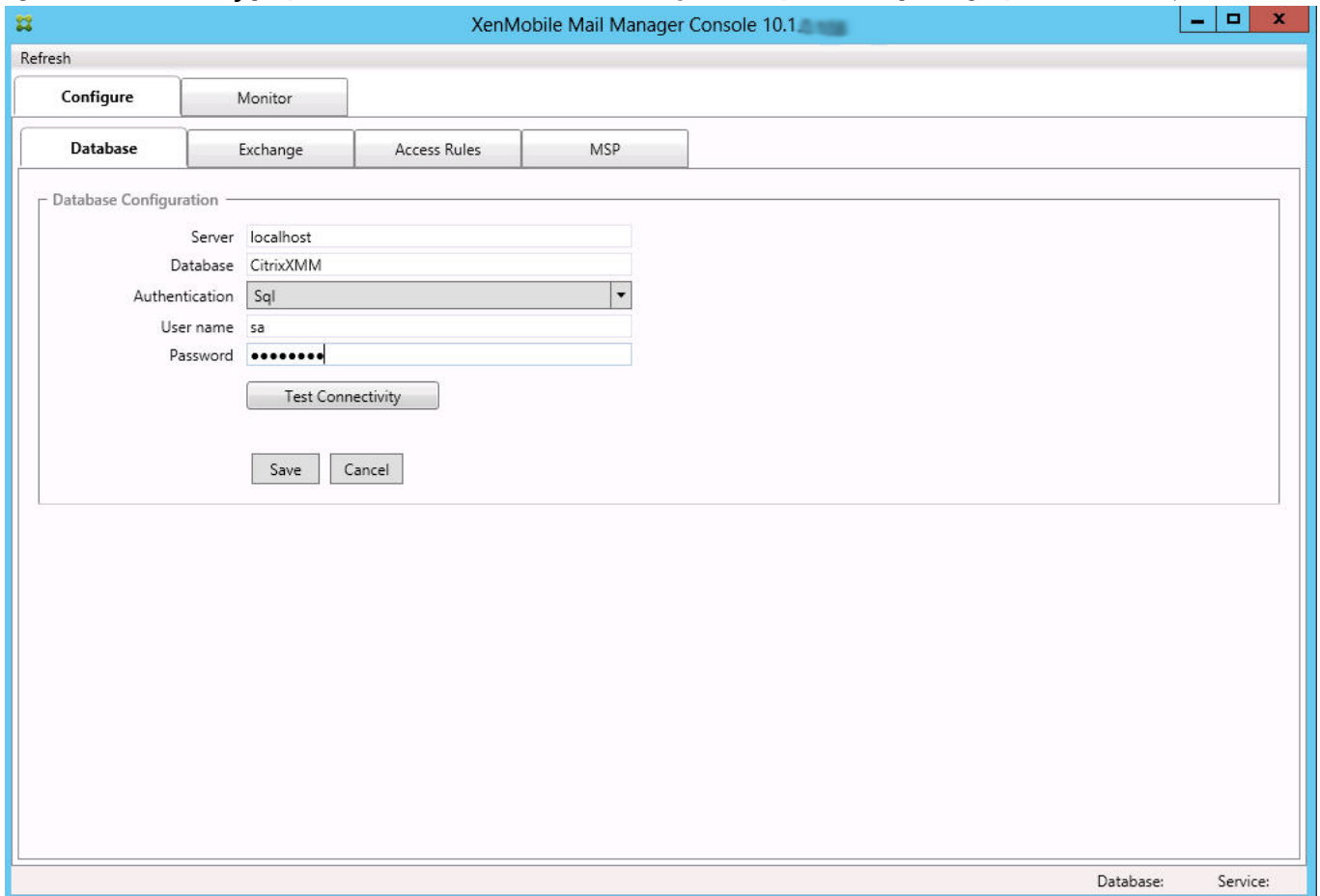


3. 次のデータベースプロパティを構成します。
  1. [Configure] の [Access Rules] タブを選択します。
  2. SQL Serverの名前（デフォルトはlocalhost）を入力します。
  3. データベースはデフォルトのCitrixXmmのままにします。
  4. SQLに使用される次のいずれかの認証モードを選択します。

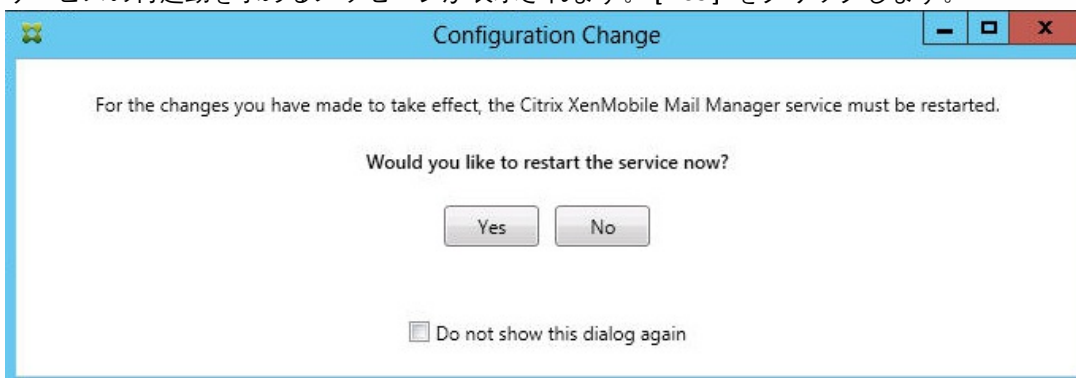
- **Sql**。有効なSQLユーザーのユーザー名とパスワードを入力します。
- **Windows Integrated**。このオプションを選択した場合、XenMobile Mail Managerサービスのログオン資格情報を、SQL Serverにアクセスするための権限を持つWindowsアカウントに変更する必要があります。これを行うには、[コントロールパネル]、[管理ツール]、[サービス]の順に選択し、XenMobile Mail Managerサービスエントリを右クリックし、[ログオン] タブをクリックします。

注：BlackBerryデータベース接続に対しても [Windows Integrated] を選択している場合は、ここで指定されているWindowsアカウントにBlackBerryデータベースへのアクセスも付与する必要があります。

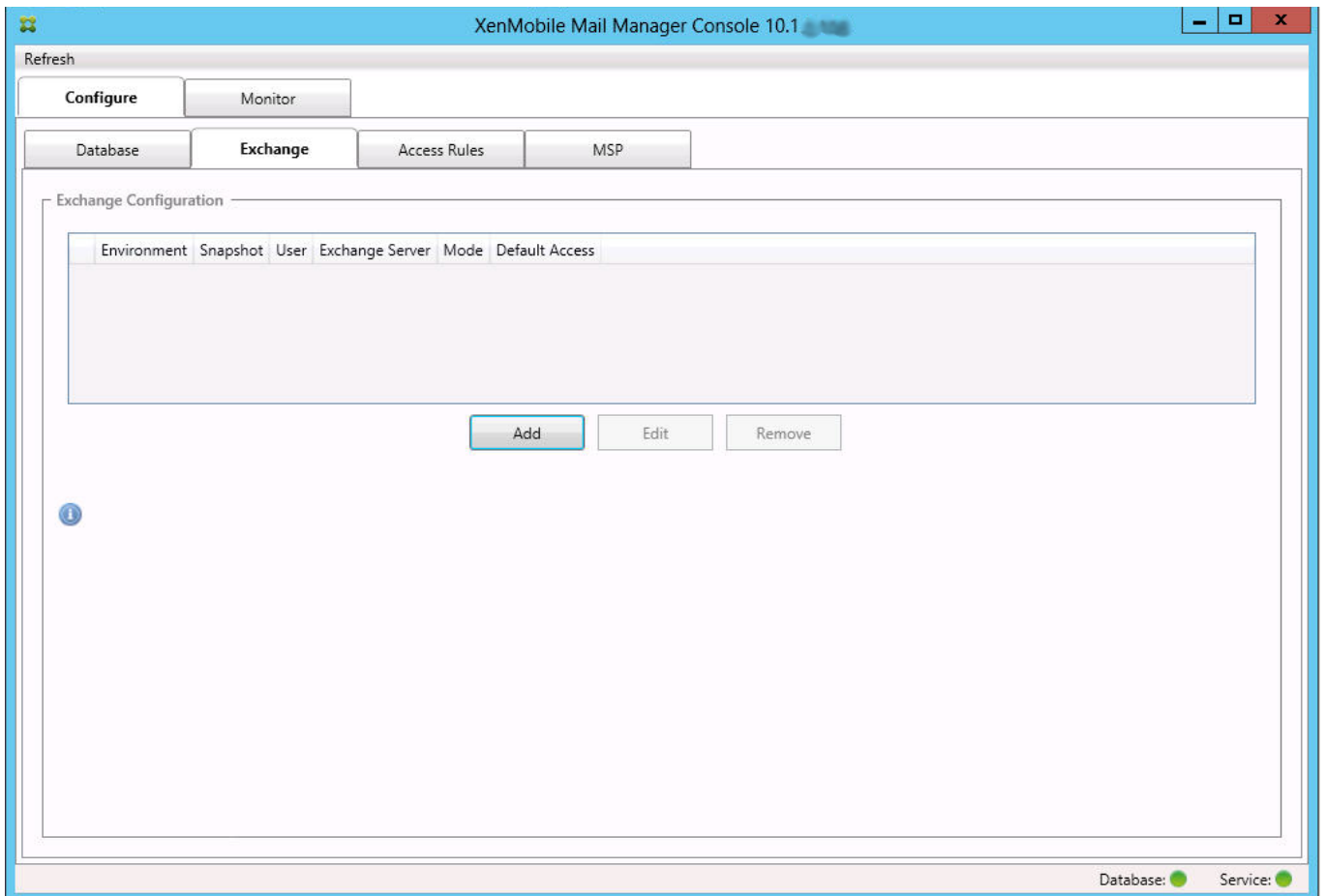
5. [Test Connectivity] をクリックしてSQL Serverに接続できることを確認し、[Save] をクリックします。



4. サービスの再起動を求めるメッセージが表示されます。[Yes] をクリックします。



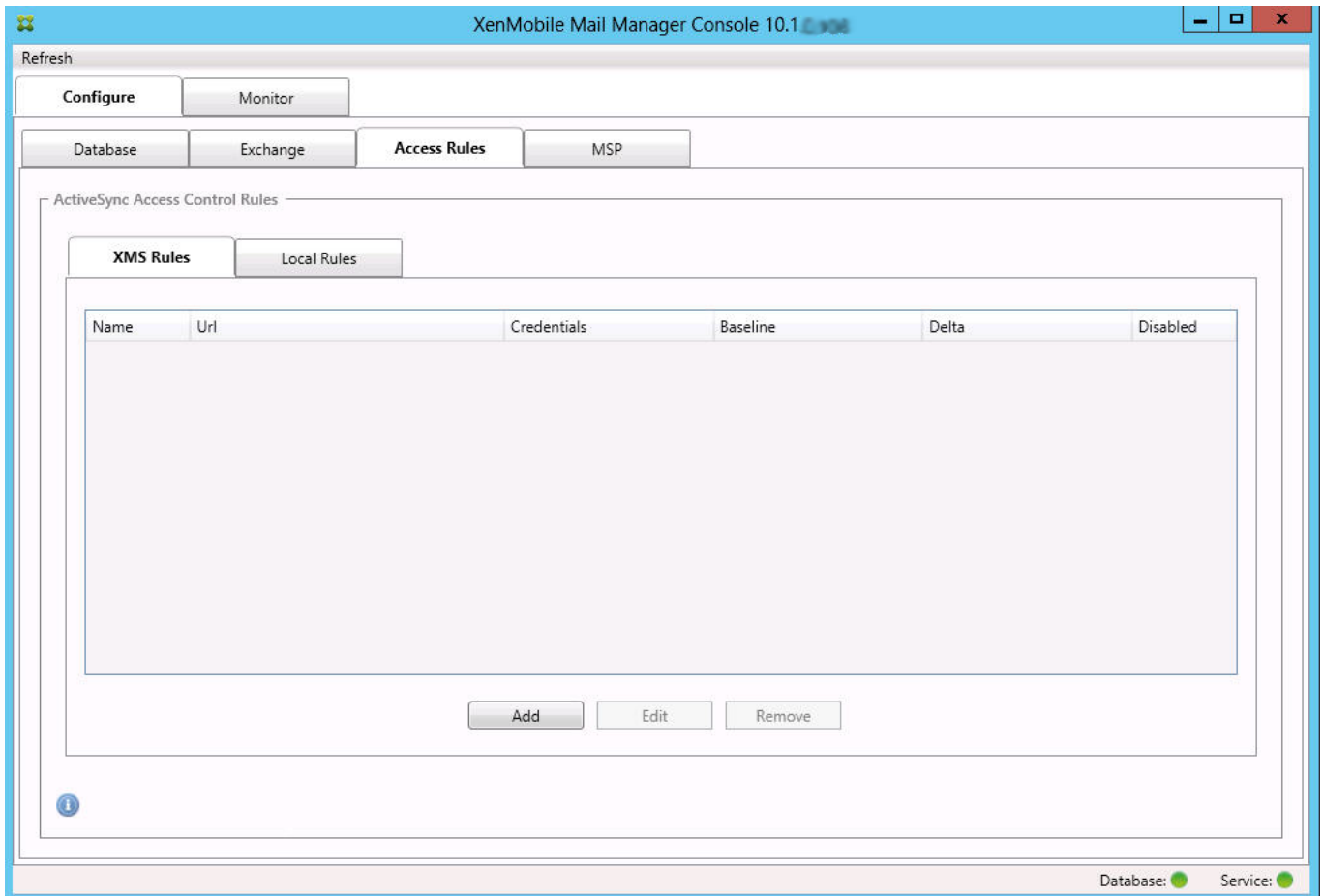
5. 1つまたは複数のExchange Serverを構成します。
  1. 単一のExchange環境を管理している場合は、単一のサーバーを指定する必要があるのみです。複数のExchange環境を管理している場合は、Exchange環境ごとに単一のExchange Serverを指定する必要があります。
  2. [Configure] の [Exchange] タブをクリックします。



3. [追加] をクリックします。
4. Exchange Server環境の種類として、 [On Premise] または [Office 365] を選択します。

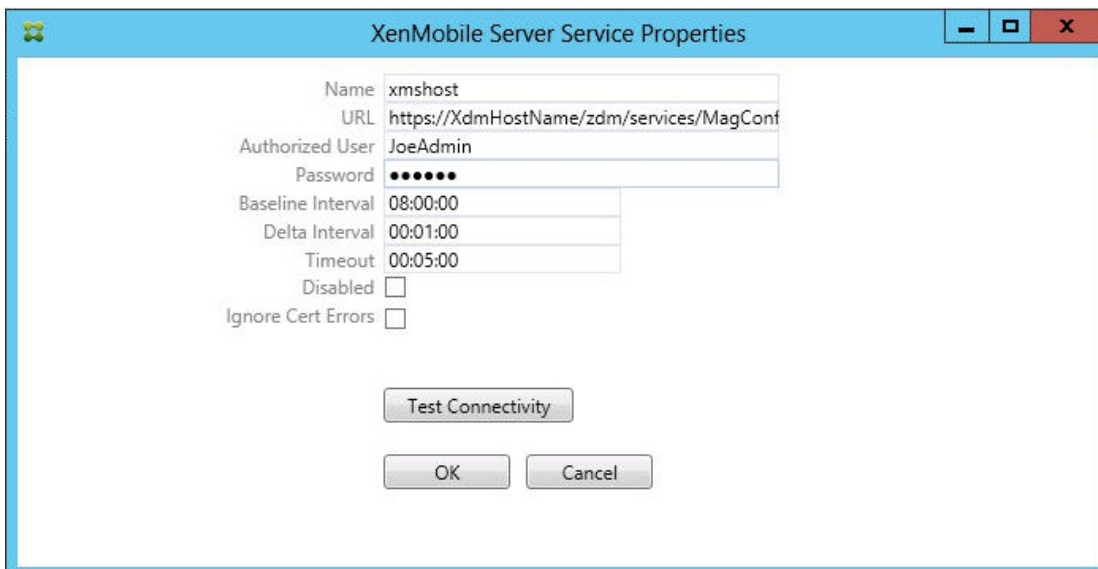
5. **[On Premise]** を選択した場合は、リモート PowerShell コマンド用に使用する Exchange Server の名前を入力します。
6. 要件セクション内で指定されているとおりの、Exchange Server に対する適切な権限を持つ Windows ID のユーザー名を入力します。
7. ユーザーのパスワードを **[Password]** ボックスに入力します。
8. メジャースナップショットを実行するスケジュールを選択します。メジャースナップショットにより、すべての Exchange ActiveSync パートナーシップが検出されます。
9. マイナースナップショットを実行するスケジュールを選択します。マイナースナップショットにより、新しく作成された Exchange ActiveSync パートナーシップが検出されます。
10. スナップショットの種類を選択：**[Deep]** または **[Shallow]** を選択します。通常、簡易スナップショットははるかに高速で、XenMobile Mail Manager の Exchange ActiveSync アクセス制御機能をすべて実行するには十分です。詳細スナップショット (XenMobile で、非管理対象デバイスを照会できます) は、処理にかかる時間が著しく長くなることもあり、Mobile Service Provider が ActiveSync に対して有効にされている場合にのみ必要です。
11. **[Default Access]** で、**[Allow]**、**[Block]**、または **[Unchanged]** を選択します。これにより、明示的な XenMobile またはローカル規則で特定されたものを除くすべてのデバイスの処理方法が制御されます。**[Allow]** を選択した場合は該当するすべてのデバイスに対する ActiveSync アクセスが許可され、**[Block]** を選択した場合はアクセスが拒否され、**[Unchanged]** を選択した場合は変更されません。
12. **[ActiveSync Command Mode]** で、**[PowerShell]** または **[Simulation]** を選択します。
  - **[PowerShell]** モードでは、XenMobile Mail Manager は PowerShell コマンドを発行し、目的のアクセス制御を有効にします。
  - **[Simulation]** モードでは、XenMobile Mail Manager は PowerShell コマンドを発行しませんが、想定しているコマンドと結果をデータベースに記録します。**[Simulation]** モードでは、PowerShell モードを有効にした場合の結果を **[Monitor]** タブを使って確認できます。
13. Exchange 環境で Active Directory フォレスト全体を表示するように XenMobile Mail Manager を構成するには、**[View Entire Forest]** を選択します。

14. 認証プロトコルとして [Kerberos] または [Basic] を選択します。XenMobile Mail Managerは、オンプレミス展開で Basic認証をサポートします。これにより、XenMobile Mail ManagerサーバーがExchange Serverが存在するドメインのメンバーでなくても、XenMobile Mail Managerを使用できるようになります。
  15. [Test Connectivity] をクリックしてExchange Serverに接続できることを確認し、[Save] をクリックします。
  16. サービスの再起動を求めるメッセージが表示されます。[Yes] をクリックします。
6. アクセス規則を構成します。
    1. [Configure] の [Access Rules] タブをクリックします。
    2. [XDM Rules] タブをクリックします。

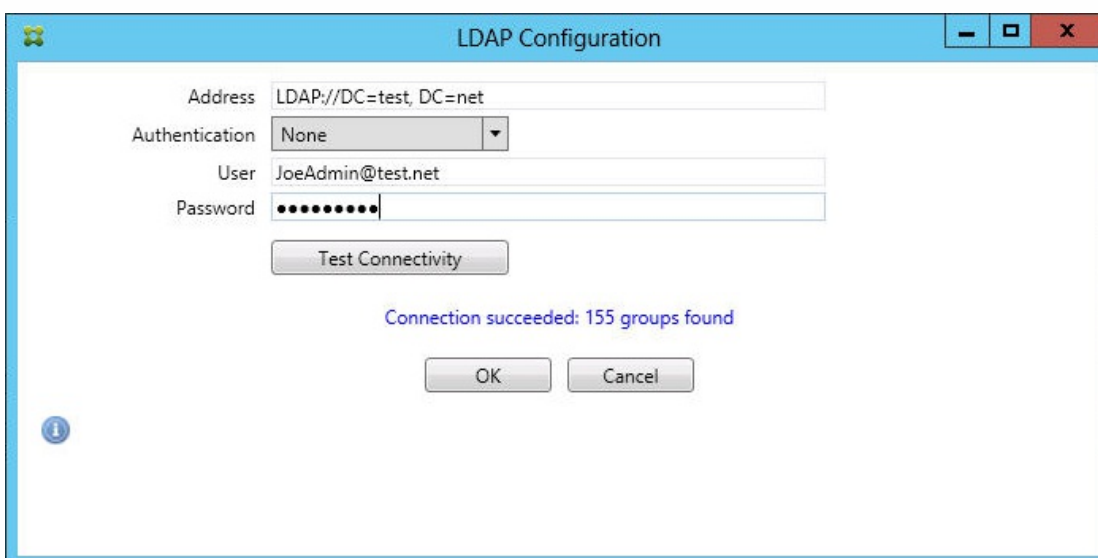


3. [Add] をクリックします。





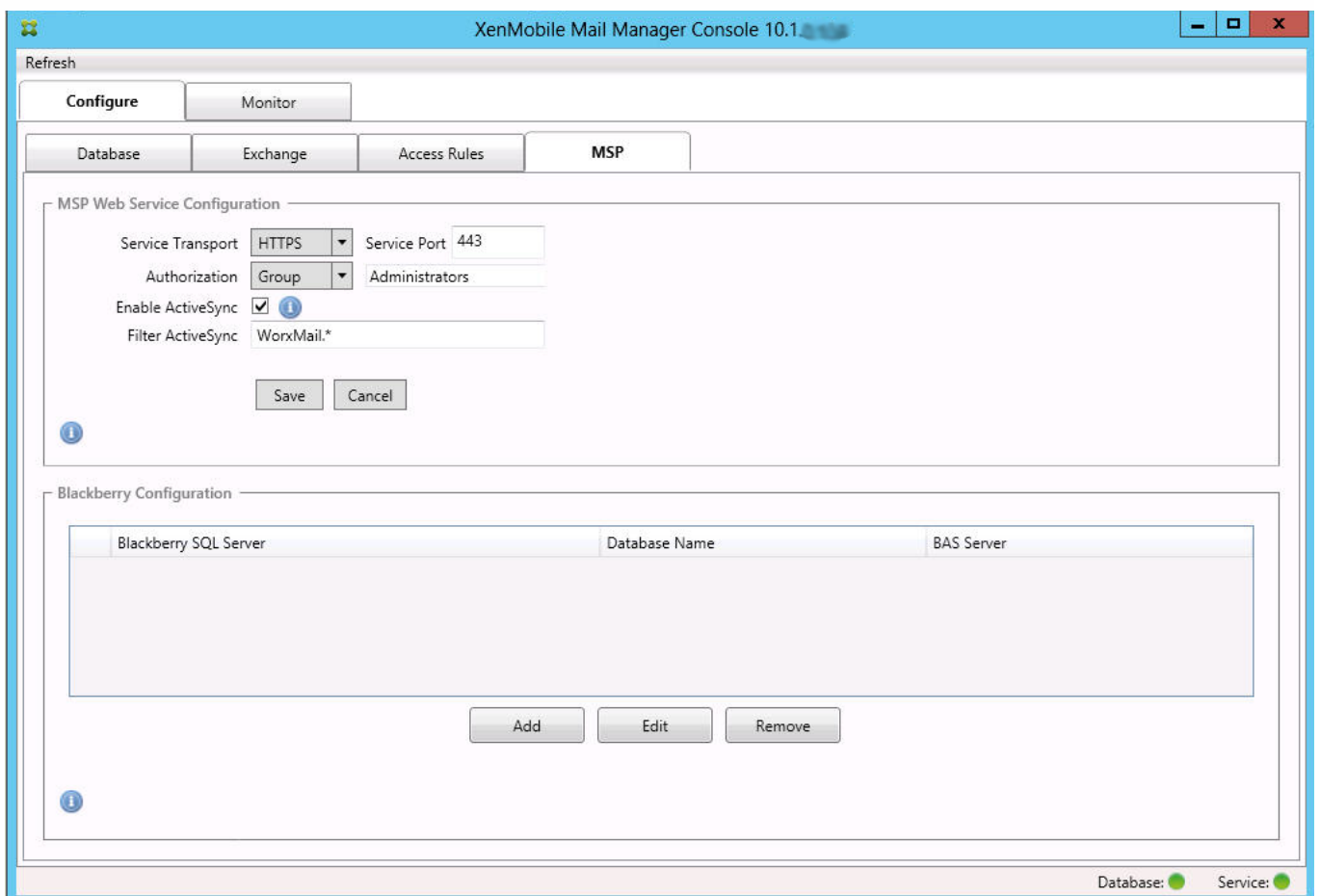
4. XenMobileサーバー規則の名前 (XdmHostなど) を入力します。
5. XenMobileサーバーを参照するようにURL文字列を変更します。たとえば、サーバー名がXdmHostである場合は、「http://XdmHostName/zdm/services/MagConfigService」と入力します。
6. サーバーで認証されているユーザーを入力します。
7. そのユーザーのパスワードを入力します。
8. [Baseline Interval]、[Delta Interval]、および [Timeout] はデフォルト値のままにします。
9. [Test Connectivity] をクリックして、サーバーへの接続を確認します。  
注： [Disabled] チェックボックスがオンの場合は、XenMobile MailサービスでXenMobileサーバーからポリシーが収集されません。
10. [OK] をクリックします。
7. [Local Rules] タブをクリックします。
  1. Active Directoryのグループに対して使用するローカル規則を作成する場合は、[Configure LDAP] をクリックし、LDAP接続プロパティを構成します。



2. [ActiveSync Device ID]、[Device Type]、[AD Group;]、[User]、またはデバイスの [UserAgent] に基づいてローカル規則を追加できます。一覧で、適切な種類を選択します。詳しくは「[XenMobile Mail Managerのアクセ](#)

ス制御規則」を参照してください。

3. テキストボックスにテキストまたはテキストフラグメントを入力します。必要に応じて、クエリボタンをクリックしてフラグメントに一致するエンティティを表示します。  
注：グループ以外のすべての種類の場合、システムはスナップショットで見つかったデバイスを使用します。したがって、操作を開始したばかりでスナップショットが完了していない場合は、エンティティが使用できません。
  4. テキスト値を選択し、[Allow] または [Deny] をクリックして右側の [Rule List] ペインに追加します。[Rule List] ペインの右側にあるボタンを使用して、規則の順序を変更したり、規則を削除したりすることができます。指定したユーザーおよびデバイスに対して、規則は表示順に評価され、上位の規則（より上部に近い規則）に一致すると以降の規則が無効になるので、順序は重要です。たとえば、すべてのiPadデバイスを許可する規則とユーザー「Matt」をブロックする下位の規則がある場合、MattのiPadは許可されます。この理由は、「iPad」規則の効果の優先度が「Matt」規則よりも高いからです。
  5. 規則一覧内の規則の分析を実行して、上書き、競合、または補足構造の可能性を検出する場合は、[Analyze] をクリックします。
  6. [Save] をクリックします。
  8. Mobile Service Providerを構成します。  
注：Mobile Service Providerはオプションであり、Mobile Service Providerインターフェイスを使用して非管理対象デバイスを照会するようにXenMobileがさらに構成されている場合にのみ必要です。
1. [Configure] > [MSP] タブをクリックします。



2. Mobile Service Providerサービスのサービストランスポートの種類（[HTTP] または [HTTPS] ）を設定します。
3. Mobile Service Providerサービスのサービスポート（通常、80または443）を設定します。  
注：ポート443を使用する場合は、IISのこのポートにバインドされたSSL証明書が必要です。
4. 承認グループまたはユーザーを設定します。これにより、XenMobileからMobile Service Providerサービスに接続できる

ユーザーまたは一連のユーザーが設定されます。

5. ActiveSyncクエリを有効または無効に設定します。  
XenMobileサーバーでActiveSyncクエリが有効の場合は、Exchange Server (1つまたは複数) のスナップショットの種類を **[Deep]** に設定する必要があります。これにより、スナップショットの取得に重大なパフォーマンスコストがかかる場合があります。
6. デフォルトでは、正規表現「Secure Mail.\*」に一致するActiveSyncデバイスは、XenMobileに送信されません。必要に応じてこの動作を変更するには、 **[Filter ActiveSync]** フィールドを変更します。  
注：空白は、すべてのデバイスがXenMobileに転送されることを意味します。
7. **[Save]** をクリックします。
9. 任意で、1つまたは複数のBlackBerry Enterprise Server (BES) を構成します。
  1. **[Add]** をクリックします。
  2. BES SQL Serverのサーバー名を入力します。

The screenshot shows the 'BES Properties' dialog box. It is divided into two main sections. The top section, 'BES Sql Server', contains the following fields: 'Server' (text box with 'BesServer'), 'Database' (text box with 'BesMgmt'), 'Authentication' (dropdown menu with 'Sql' selected), 'User name' (text box with 'JoeAdmin'), 'Password' (text box with masked characters), a 'Test Connectivity' button, and 'Sync Schedule' (dropdown menu with 'Every 30 Minutes'). The bottom section, 'Blackberry Device Administration from XMS', contains: an 'Enabled' checkbox (checked), 'BAS Server' (text box with 'BAServer'), 'BAS Port' (text box with '443'), 'Domain\User' (text box with 'ServerName\JoeAdmin'), 'Password' (text box with masked characters), and a 'Test Connectivity' button. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

3. BES管理データベースのデータベース名を入力します。
4. 認証モードを選択します。 **[Windows Integrated authentication]** を選択する場合、XenMobile Mail Managerサービスのユーザーアカウントが、BES SQL Serverへの接続に使用するアカウントになります。  
注：XenMobile Mail Managerデータベース接続に対しても **[Windows Integrated]** を選択している場合は、ここで指定したWindowsアカウントにXenMobile Mail Managerデータベースへのアクセスも付与する必要があります。
5. **[SQL authentication]** を選択する場合は、ユーザー名とパスワードを入力します。

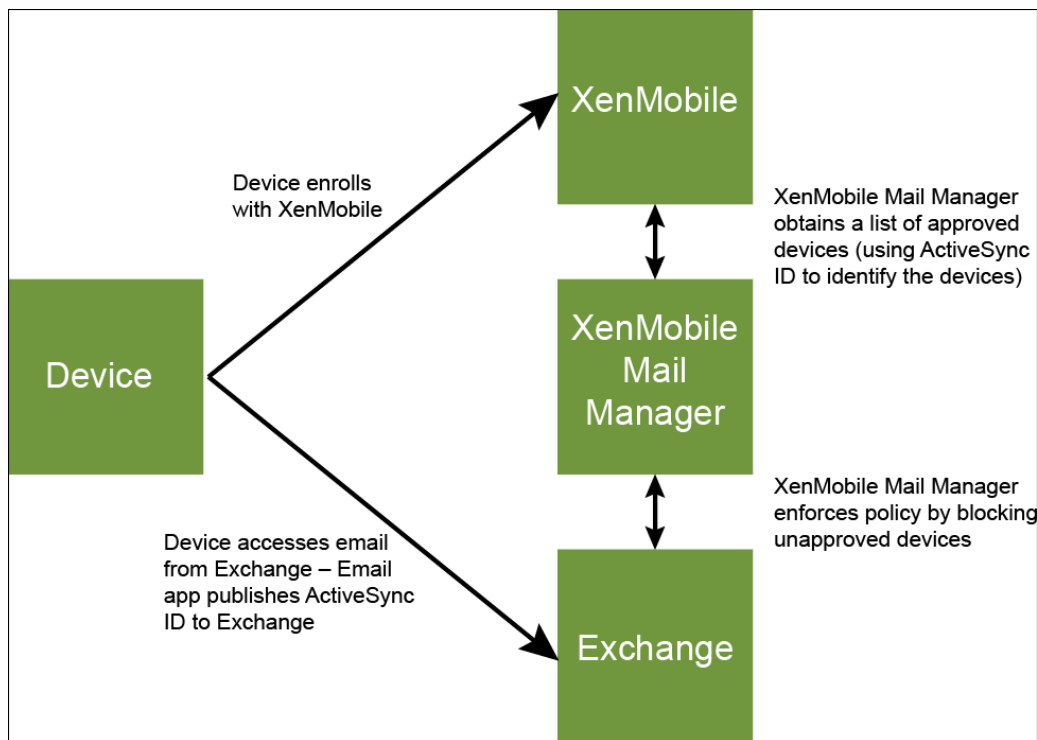
6. **[Sync Schedule]** を設定します。これは、BES SQL Serverへの接続とデバイス更新のチェックに使用するスケジュールです。
7. **[Test Connectivity]** をクリックして、SQL Serverへの接続を確認します。  
注： **[Windows Integrated]** を選択している場合、このテストでは、XenMobile Mail Managerサービスのユーザーではなく、現在ログオンしているユーザーが使用されるため、SQL認証が正確にテストされません。
8. XenMobileからのBlackBerryデバイスのリモートでのワイプやResetPasswordをサポートする場合は、**[Enabled]** チェックボックスをオンにします。
  1. BESの完全修飾ドメイン名 (Fully Qualified Domain Name : FQDN) を入力します。
  2. 管理者Webサービスで使用するBESポートを入力します。
  3. BESサービスに必要な完全修飾ユーザー名とパスワードを入力します。
  4. **[Test Connectivity]** をクリックして、BESへの接続をテストします。
  5. **[Save]** をクリックします。

# ActiveSync IDによるメールポリシーの適用

Apr 27, 2017

企業のメールポリシーによっては、特定のデバイスで企業メールを使用することが認められない場合があります。このポリシーに従うには、そのようなデバイスから従業員が企業メールにアクセスできないようにする必要があります。XenMobile Mail ManagerおよびXenMobileを連携させ、そのようなメールポリシーを適用することができます。XenMobileで企業メールアクセスのポリシーを設定し、未承認のデバイスがXenMobileに登録されたときにXenMobile Mail Managerでポリシーを適用します。

デバイス上のメールクライアントはデバイスIDを使用してExchange Server（またはOffice 365）にクライアントの存在を通知します。このIDはActiveSync IDとも呼ばれ、デバイスを一意に識別するために使用されます。Secure Hubでは同様の識別子を取得し、デバイスが登録されるとXenMobileにこの識別子を送信します。XenMobile Mail Managerで2つのデバイスIDを比較することによって、特定のデバイスに企業メールへのアクセスを許可するかどうかが判定されます。次の図は、この概略を示しています。



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 [デフォルトで禁止] に設定することでXenMobile Mail Managerでメールを禁止するように構成することができます。これは、従業員がAndroidデバイスにTouchdown以外のメールクライアントを構成し、ActiveSync IDの検出が適切に動作しない場合は、従業員は企業メールへのアクセスを拒否されるということを意味します。

# アクセス制御規則

Apr 27, 2017

XenMobile Mail Managerでは、Exchange ActiveSyncデバイスのアクセス制御を動的に構成するための、規則に基づく手法が提供されます。XenMobile Mail Managerのアクセス制御規則は、一致式と目的のアクセス状態（許可またはブロック）の2つで構成されます。特定のExchange ActiveSyncデバイスに対して規則を評価して、その規則がデバイスに適用されるかどうか、またはデバイスと一致するかどうかを判別できます。一致式にはいくつかの種類があります。たとえば、規則は、特定のデバイスの種類のすべてのデバイス、特定のExchange ActiveSyncデバイスID、特定のユーザーのすべてのデバイスと一致するなどの条件を指定できます。

規則一覧の規則を追加、削除、および並べ替えているときに [Cancel] をクリックすると、規則一覧が最初に開いたときの状態に戻ります。 [Save] をクリックしない限り、構成ツールを閉じるとこのウィンドウに対して加えた変更が失われます。

XenMobile Mail Managerには、ローカル規則、XenMobileサーバー規則（XDM規則とも呼ばれます）、およびデフォルトのアクセス規則の3種類の規則があります。

**ローカル規則：**ローカル規則は最も優先されます。デバイスがローカル規則と一致すると、規則の評価は停止します。XenMobileサーバー規則とデフォルトのアクセス規則は参照されません。ローカル規則は、 [Configure] > [Access Rules] > [Local Rules] タブから、XenMobile Mail Managerに対してローカルに構成します。サポート一致は、特定のActive Directoryグループ内のユーザーのメンバーシップに基づきます。サポート一致は、次のフィールドの正規表現に基づきます。

- Active SyncデバイスID
- ActiveSyncデバイスの種類
- ユーザープリンシパル名（User Principal Name : UPN）
- ActiveSyncユーザーエージェント（通常、デバイスプラットフォームまたはメールクライアント）

メジャースナップショットが完了し、デバイスが検出されている限り、通常の規則または正規表現の規則のいずれかを追加できます。メジャースナップショットが完了していない場合、正規表現の規則のみを追加できます。

**XenMobileサーバー規則。**XenMobileサーバー規則は、管理対象デバイスに関する規則を提供する外部のXenMobileサーバーへの参照です。XenMobileサーバーは、デバイスがジェイルブレイク済みかどうかや、デバイスに禁止アプリケーションが含まれているかどうかなど、XenMobileが認識しているプロパティに基づいてデバイスが許可されるか、ブロックされるかを識別する独自の高レベルの規則を使用して構成できます。XenMobileでは、高レベルの規則が評価され、許可またはブロックする一連のActiveSyncデバイスIDが生成されて、これらがXenMobile Mail Managerに配信されます。

**デフォルトのアクセス規則。**デフォルトのアクセス規則は、すべてのデバイスと一致する可能性があり、常に最後に評価されるという点で独特です。この規則は、あらゆる状況に対応できる規則です。つまり、特定のデバイスがローカル規則とXenMobileサーバー規則のいずれにも一致しない場合は、デフォルトのアクセス規則での目的のアクセス状態によってデバイスにおける目的のアクセス状態が決まります。

- **Default Access – Allow。**ローカル規則とXenMobileサーバー規則のいずれにも一致しないすべてのデバイスが許可されます。
- **Default Access – Block。**ローカル規則とXenMobileサーバー規則のいずれにも一致しないすべてのデバイスがブロックされます。
- **Default Access - Unchanged。**ローカル規則とXenMobileサーバー規則のいずれにも一致しないすべてのデバイスのアクセス状態は、XenMobile Mail Managerによって変更されません。ExchangeによってデバイスがQuarantineモードになっている場合、アクションは実行されません。たとえば、Quarantineモードからデバイスを削除する方法は、ローカル規則またはXDM規則で隔離を明示的に上書きすることのみです。

## 規則の評価について

ExchangeからXenMobile Mail Managerに報告されるデバイスごとに、次のように優先度の高い順に規則が評価されます。

- ローカル規則
- XenMobileサーバー規則
- デフォルトのアクセス規則

一致が検出されると、評価は停止します。たとえば、ローカル規則が特定のデバイスと一致すると、そのデバイスはXenMobileサーバー規則またはデフォルトのアクセス規則に対して評価されません。このことは、特定の種類の規則内でも当てはまります。たとえば、ローカル規則一覧で、特定のデバイスに対して複数の一致がある場合、最初の一致が見つかる時点で評価は停止します。

デバイスプロパティが変更されたとき、デバイスが追加または削除されたとき、または規則自体が変更されたときは、現在定義されている一連の規則がXenMobile Mail Managerによって再評価されます。メジャースナップショットにより、構成可能な間隔でデバイスのプロパティ変更または削除が確認されます。マイナースナップショットにより、構成可能な間隔で新しいデバイスが確認されます。

Exchange ActiveSyncにも、アクセスを管理する規則があります。XenMobile Mail Managerのコンテキストでこれらの規則がどのように機能するかを理解することが重要です。Exchangeは、個人の適用除外、デバイスの規則、組織の設定という3つのレベルの規則で構成できます。XenMobile Mail Managerでは、リモートPowerShell要求をプログラムで発行して個人の適用除外一覧に反映させることで、アクセス制御を自動化します。これらは、特定のメールボックスに関連する、許可またはブロックするExchange ActiveSyncデバイスIDの一覧です。展開すると、XenMobile Mail ManagerはExchange内の適用除外一覧の管理機能を効果的に引き継ぎます。詳細については、この[Microsoftの技術文書](#)を参照してください。

分析は、同じフィールドに対して複数の規則が定義されている場合に特に便利です。規則間の関係をトラブルシューティングできます。規則フィールドの観点から分析を実行します。たとえば、ActiveSyncデバイスID、ActiveSyncデバイスの種類、ユーザー、ユーザーエージェントなどの照合されるフィールドに基づくグループで規則が分析されます。

### 規則の用語：

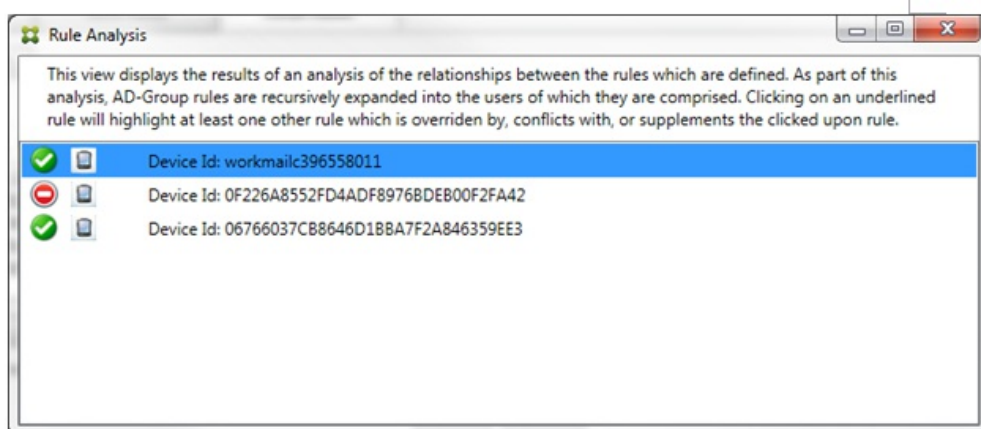
- **上書き規則**。同じデバイスに複数の規則が適用される可能性がある場合に上書きが発生します。一覧の優先度の順序で規則が評価されるので、優先度の低い、適用される可能性がある規則のインスタンスが評価されない場合があります。
- **競合規則**。同じデバイスに複数の規則が適用される可能性があり、アクセス（許可/ブロック）が一致しない場合に競合が発生します。競合規則が正規表現の規則でない場合、競合には常に暗黙的に上書きの意味も含まれます。
- **補足規則**。正規表現の規則が複数あるので、2つ（またはそれ以上）の正規表現を1つの正規表現の規則に結合できるか、またはそれらの機能が重複していないようにする必要がある場合に補足が発生します。補足規則もアクセス（許可/ブロック）で競合する場合があります。
- **プライマリ規則**。プライマリ規則は、ダイアログボックス内でクリックされた規則です。この規則は、実線の罫線で囲まれて示されます。この規則には、上方向または下方向を指す1つまたは2つの緑色の矢印も示されます。矢印が上方向を指している場合は、プライマリ規則よりも優先される補助規則があることを示しています。矢印が下方向を指している場合は、プライマリ規則よりも優先度の低い補助規則があることを示しています。アクティブにできるプライマリ規則は、常に1つのみです。
- **補助規則**。補助規則は、上書き、競合、または補足の関係のいずれかで、プライマリ規則と何らかの関係を持ちます。この規則は、破線の罫線で囲まれて示されます。各プライマリ規則に対して、1対多の補助規則を指定できます。下線付きのエントリをクリックしたときに強調表示される補助規則は、常にプライマリ規則の観点から示されます。たとえば、補助規則がプライマリ規則によって上書きされたり、プライマリ規則とアクセスで競合したり、プライマリ規則を補足したりします。

### [Rule Analysis] ダイアログボックスのルールの種類の外観

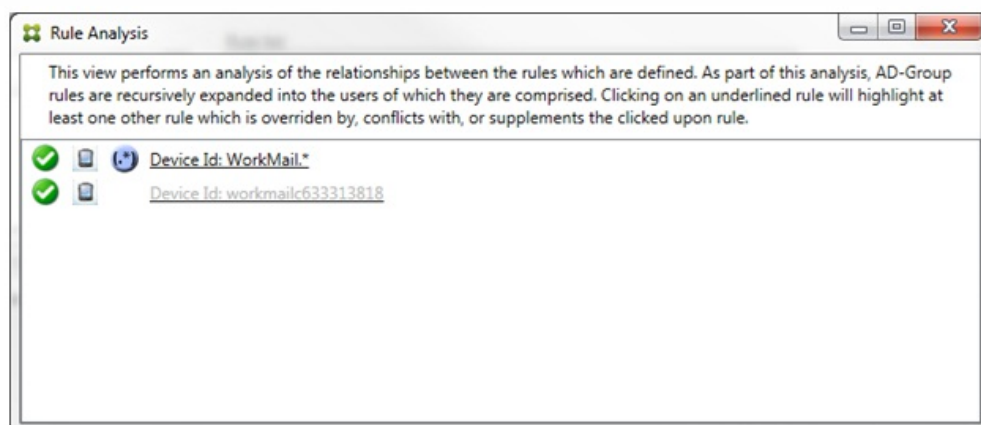


競合、上書き、または補足がない場合、[Rule Analysis] ダイアログボックスに下線付きのエントリは表示されません。どのアイテムをクリックしても影響はありません。通常の選択済みアイテムの表示になります。

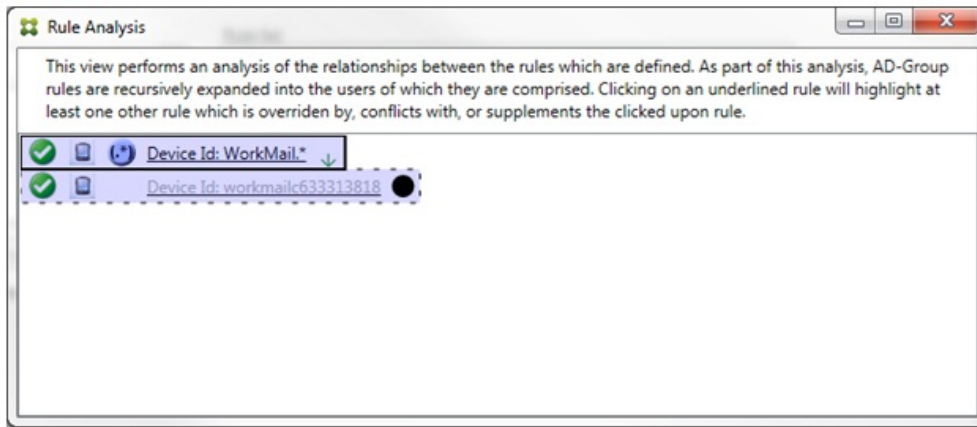
[Rule Analysis] ウィンドウにあるチェックボックスを選択すると、競合、上書き、重複、または補足構造であるルールのみが表示されます。



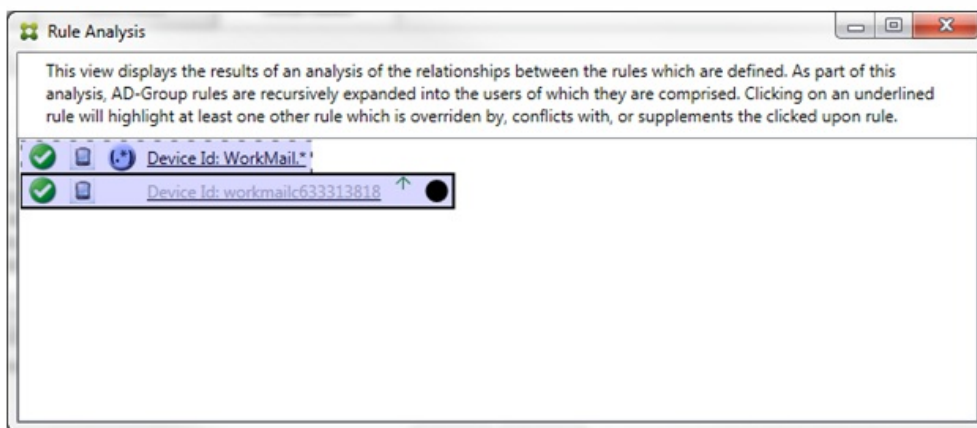
上書きが発生した場合、2つ以上の規則（プライマリ規則と、1つまたは複数の補助規則）に下線が付けられます。1つまたは複数の補助規則が淡色のフォントで表示され、より優先度の高い規則によって上書きされたことが示されます。上書きされた規則をクリックして、その規則を上書きした規則を確認できます。規則がプライマリ規則または補助規則であることの結果として上書きされた規則が強調表示されている場合は常に、その規則が非アクティブであることを示す追加表示として、その規則の横に黒の円が表示されます。たとえば、規則をクリックする前は、次のようにダイアログボックスが表示されます。



最も優先度の高い規則をクリックすると、ダイアログボックスの表示は次のようになります。

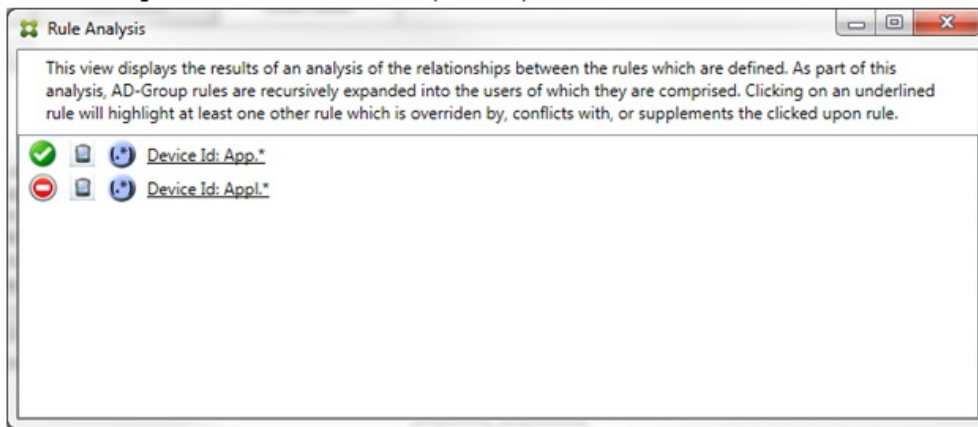


この例では、正規表現の規則WorkMail.\*がプライマリ規則（実線の罫線で表示）で、通常の規則workmailc633313818が補助規則（破線の罫線で表示）です。補助規則の横の黒点は、より優先度の高い正規表現の規則が優先されるので、その規則が非アクティブである（評価されない）ことを示す追加表示です。上書きされる規則をクリックすると、ダイアログボックスの表示は次のようになります。

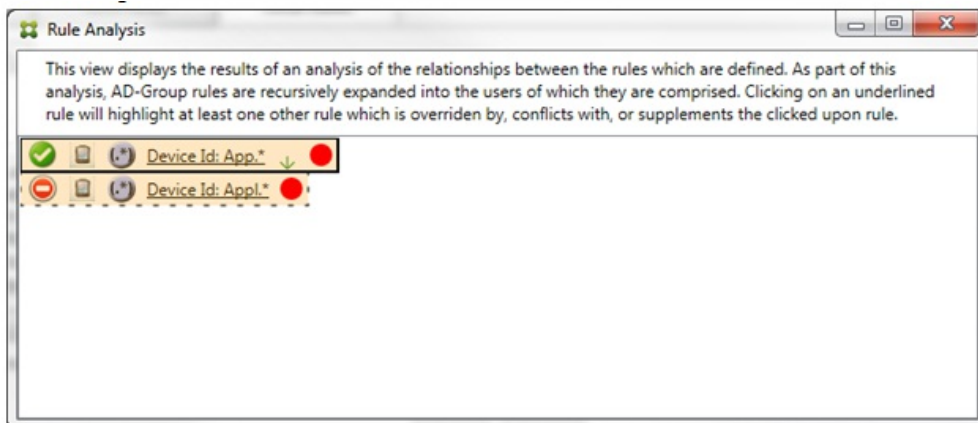


上記の例では、正規表現の規則WorkMail.\*が補助規則（破線の罫線で表示）で、通常の規則workmailc633313818がプライマリ規則（実線の罫線で表示）です。このシンプルな例では、大きな違いはありません。より複雑な例については、このトピックで後述する複雑な式の例を参照してください。多くの規則が定義されたシナリオでは、上書きされる規則をクリックすると、その規則を上書きした規則がすばやく識別されます。

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。

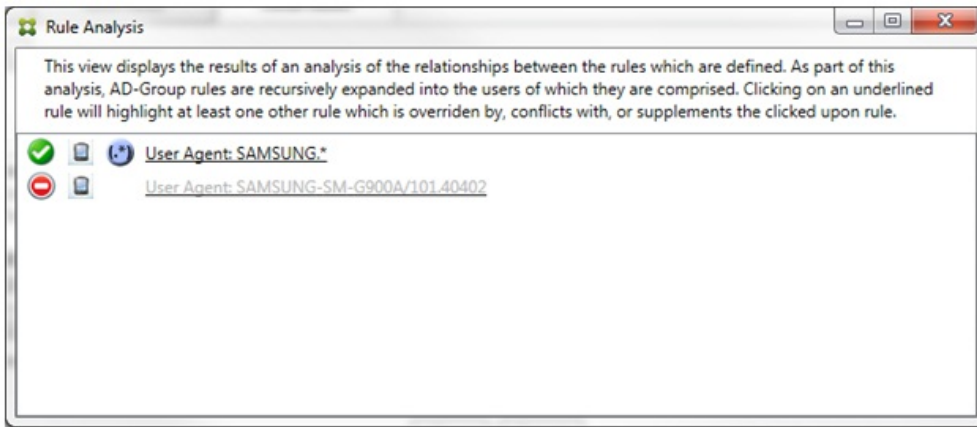


2つの正規表現の規則を確認すると、最初の規則で「App」がデバイスIDに含まれるすべてのデバイスを許可し、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスを拒否することがわかります。さらに、2つ目の規則で「Appl」がデバイスIDに含まれるすべてのデバイスが拒否されますが、許可する規則の優先度の方が高いので、その一致条件のデバイスは拒否されません。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



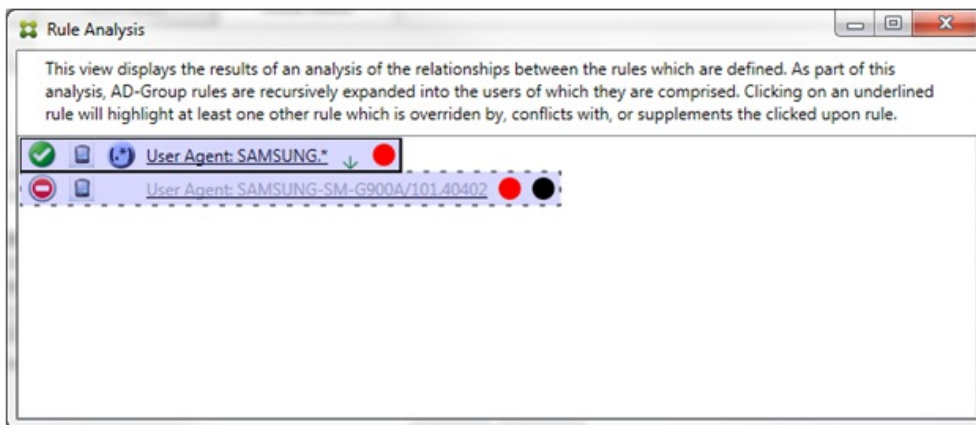
前述のシナリオでは、プライマリ規則（正規表現の規則App.\*）と補助規則（正規表現の規則Appl.\*）の両方が黄色で強調表示されます。これは、複数の正規表現の規則を単一の一致可能なフィールドに適用したことについての単純な警告の表示です。この警告は、冗長性の問題や、より深刻な問題を示す場合があります。

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。



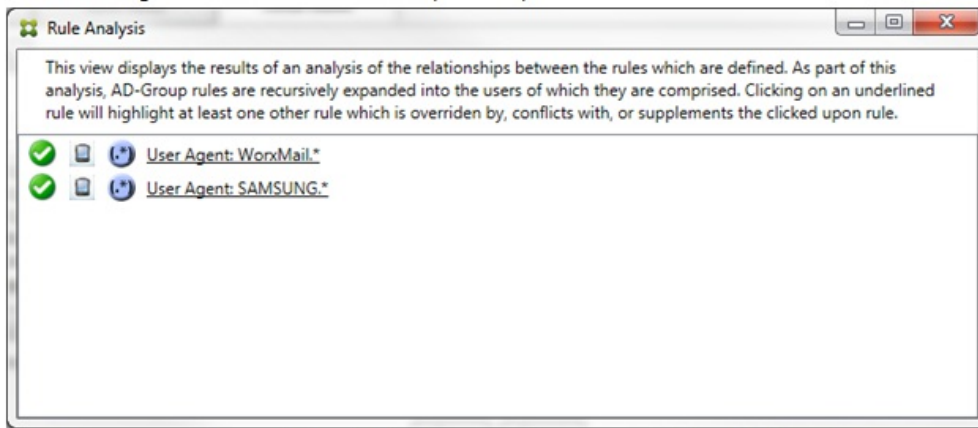
上記の例では、最初の規則（正規表現の規則SAMSUNG.\*）が次の規則（通常の規則SAMSUNG-SM-G900A/101.40402）を上書きするだけでなく、2つの規則のアクセスが異なる（プライマリ規則では許可を指定し、補助規則ではブロックを指定）ことも容易に確認できます。2つ目の規則（通常の規則SAMSUNG-SM-G900A/101.40402）は淡色のテキストで表示され、上書きされて非アクティブであることが示されます。

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。

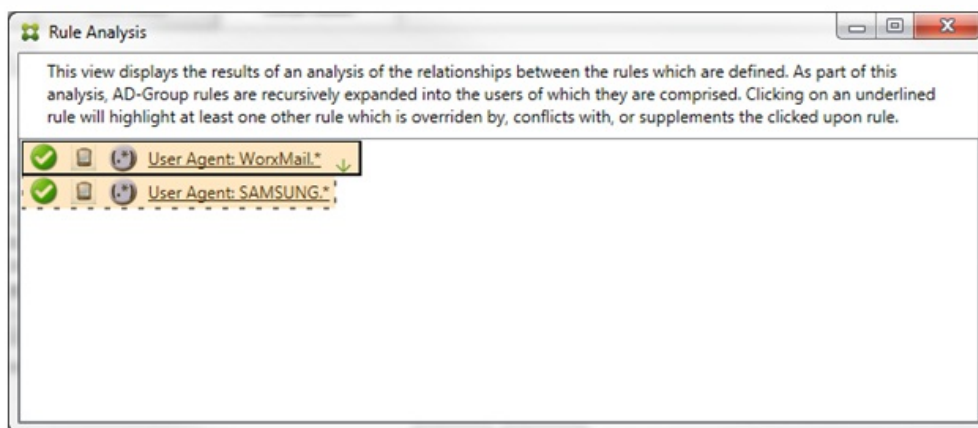


プライマリ規則（正規表現の規則SAMSUNG.\*）の末尾には赤色の点が付けられて、アクセス状態が1つまたは複数の補助規則と競合していることが示されます。補助規則（通常の規則SAMSUNG-SM-G900A/101.40402）の末尾には、アクセス状態がプライマリ規則と競合していることを示す赤色の点に加えて、その規則が上書きされて非アクティブであることを示す黒点が付けられます。

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。




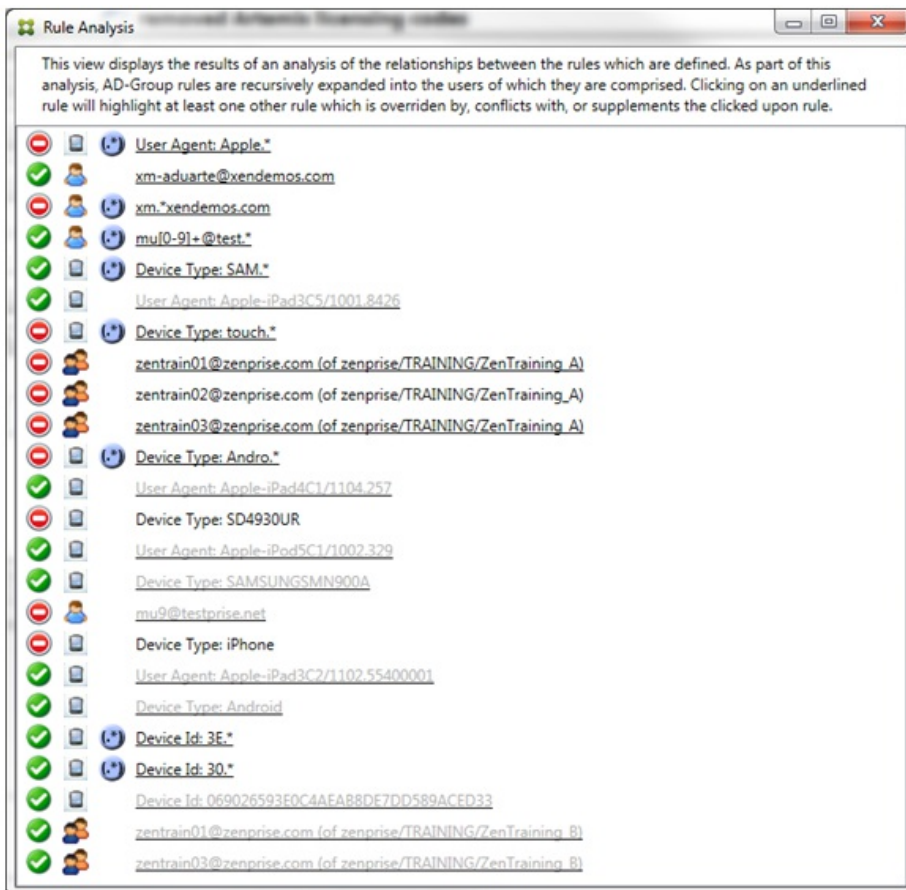
目視で確認すると、両方の規則が正規表現の規則で、両方ともXenMobile Mail Managerの [ActiveSync device ID] フィールドに適用されていることが容易にわかります。最初の規則をクリックすると、ダイアログボックスの表示は次のようになります。



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

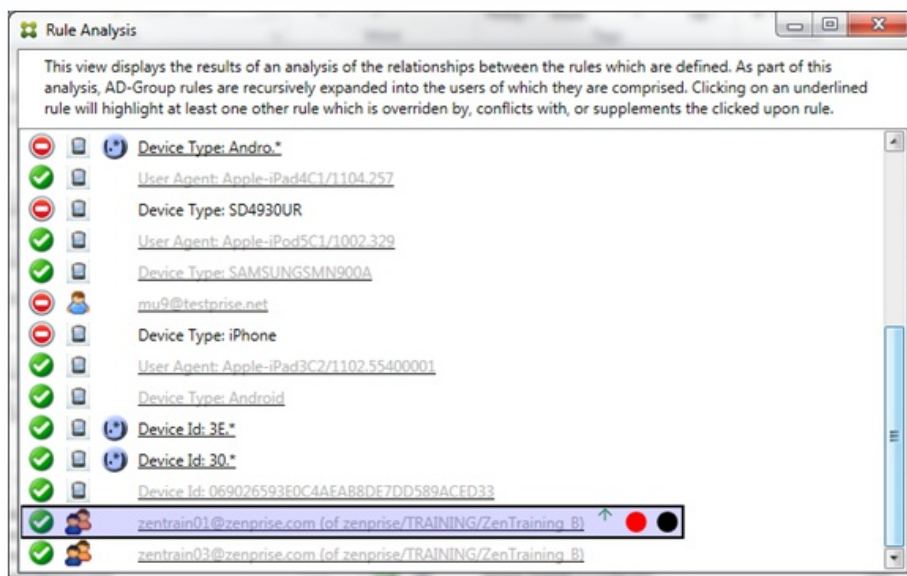
発生する可能性のある上書き、競合、または補足は多くあるので、発生する可能性のあるシナリオの例をすべて示すことはできません。次の例では、すべきでないことについて説明し、ルール分析の完全な視覚的構造を示します。次の図では、ほとんどのアイテムに下線が付けられています。多くのアイテムが淡色のフォントで表示され、問題となる規則が、何らかの方法でより優先度の高い規則によって上書きされていることが示されています。同様に、 アイコンで示される多数の正規表現の規則も一覧に含まれています。



## 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。

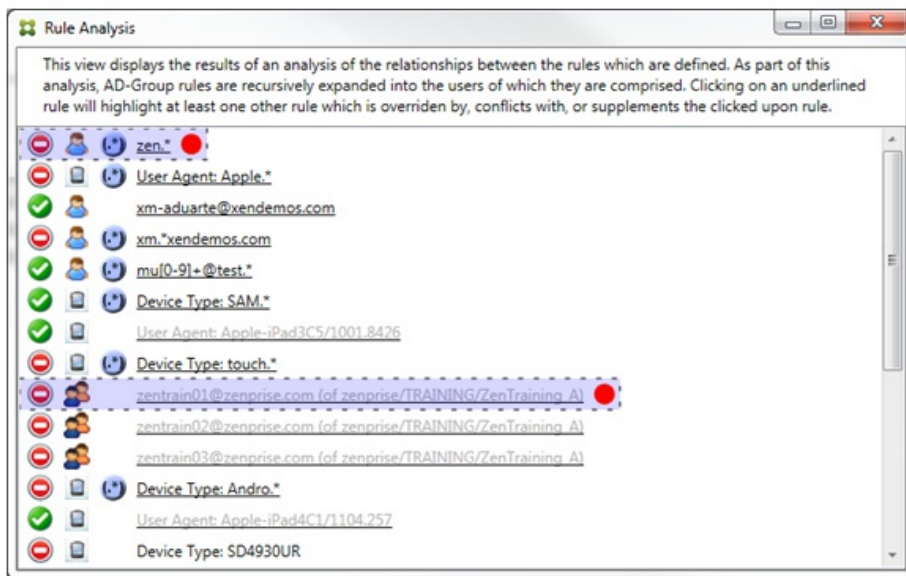
例1：この例では、zenrain01@zenprise.comが上書きされた理由を調べます。



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。

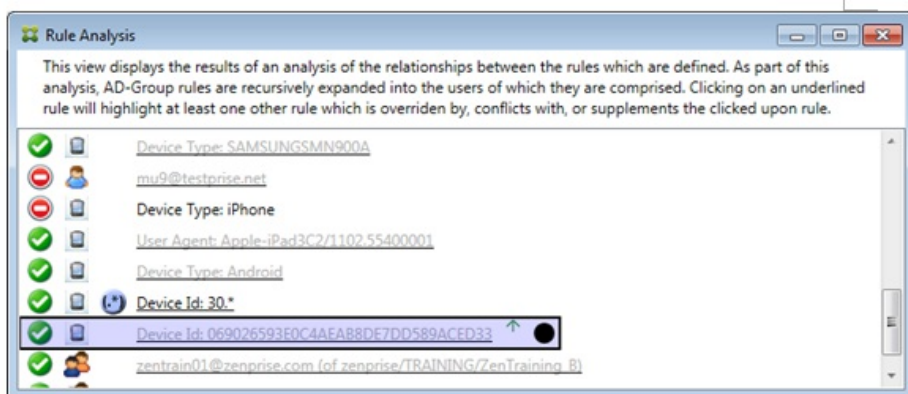
- 青色で強調表示され、実線の罫線で囲まれている。
- 上方向を指す緑色の矢印が付けられている (すべての補助規則がこの規則より上に表示されていることを示します)。
- 末尾に、1つまたは複数の補助規則とアクセスが競合していることを示す赤色の点と、プライマリ規則が上書きされて非アクティブであることを示す黒点が付けられている。

上方向にスクロールすると、次が表示されます。



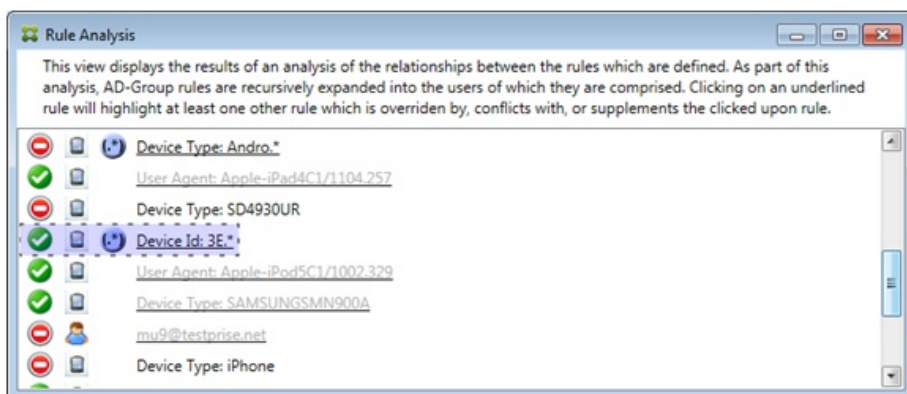
この場合、プライマリ規則を上書きする2つの補助規則 (正規表現の規則zen.\*と通常の規則zentrain01@zenprise.com (of zenprise/TRAINING/ZenTraining A)) があります。後者の補助規則の場合、Active Directoryグループ規則ZenTraining Aにユーザーzentrain01@zenprise.comが含まれる一方で、Active Directoryグループ規則ZenTraining Bにもユーザーzentrain01@zenprise.comが含まれることとなります。ただし、補助規則の優先度がプライマリ規則の優先度よりも高いので、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。

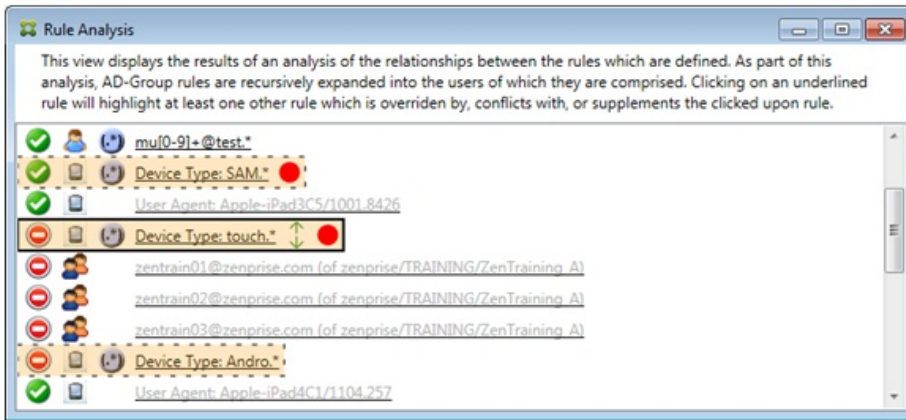
## 補足および競合の分析方法

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。

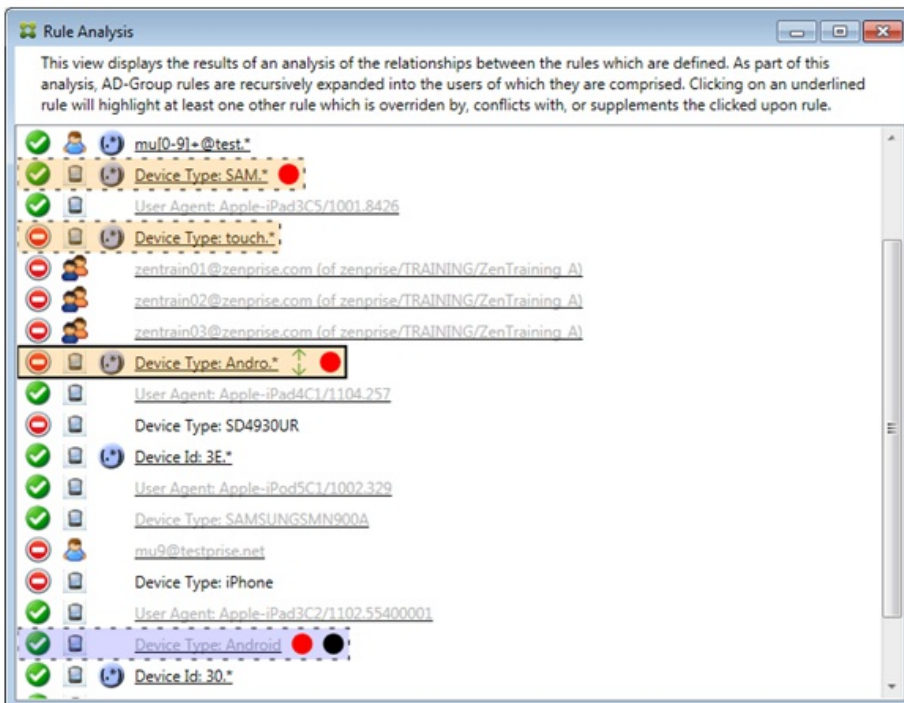


- 両方の補助規則に黄色のオーバーレイが適用され、ActiveSyncデバイスの種類の規則フィールドにこれらが補足として適用されていることが示されている。
- このようなシナリオでは、正規表現の規則が冗長でないようにする必要がある。



### 規則の高度な分析方法

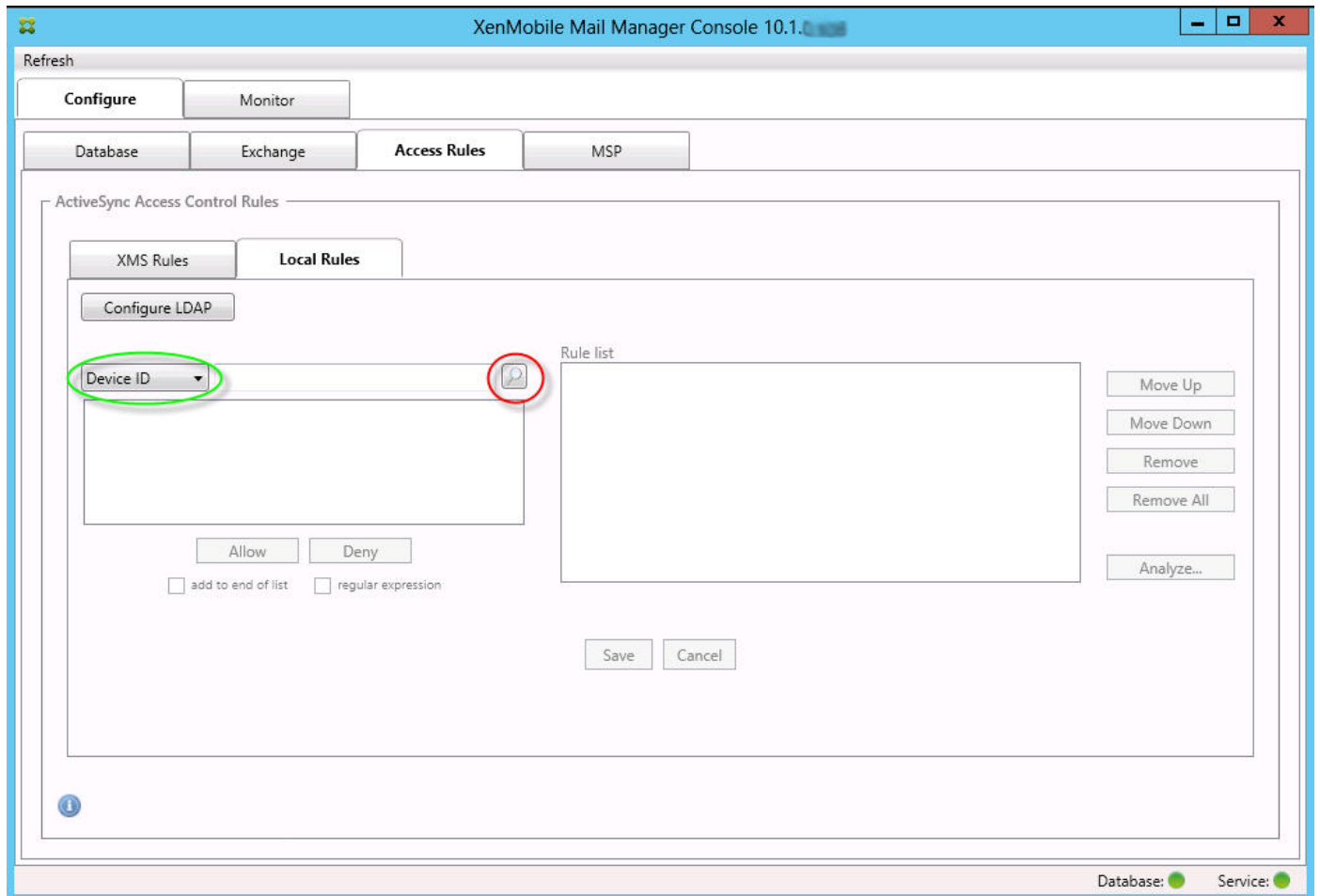
次の例では、規則の関係が常にプライマリ規則の観点から示されるしくみを確認します。前述の例では、デバイスの種類の規則フィールドに適用され、値がtouch.\*である正規表現の規則をクリックした場合を示しました。補助規則Andro.\*をクリックすると、別の一連の補助規則が強調表示されます。



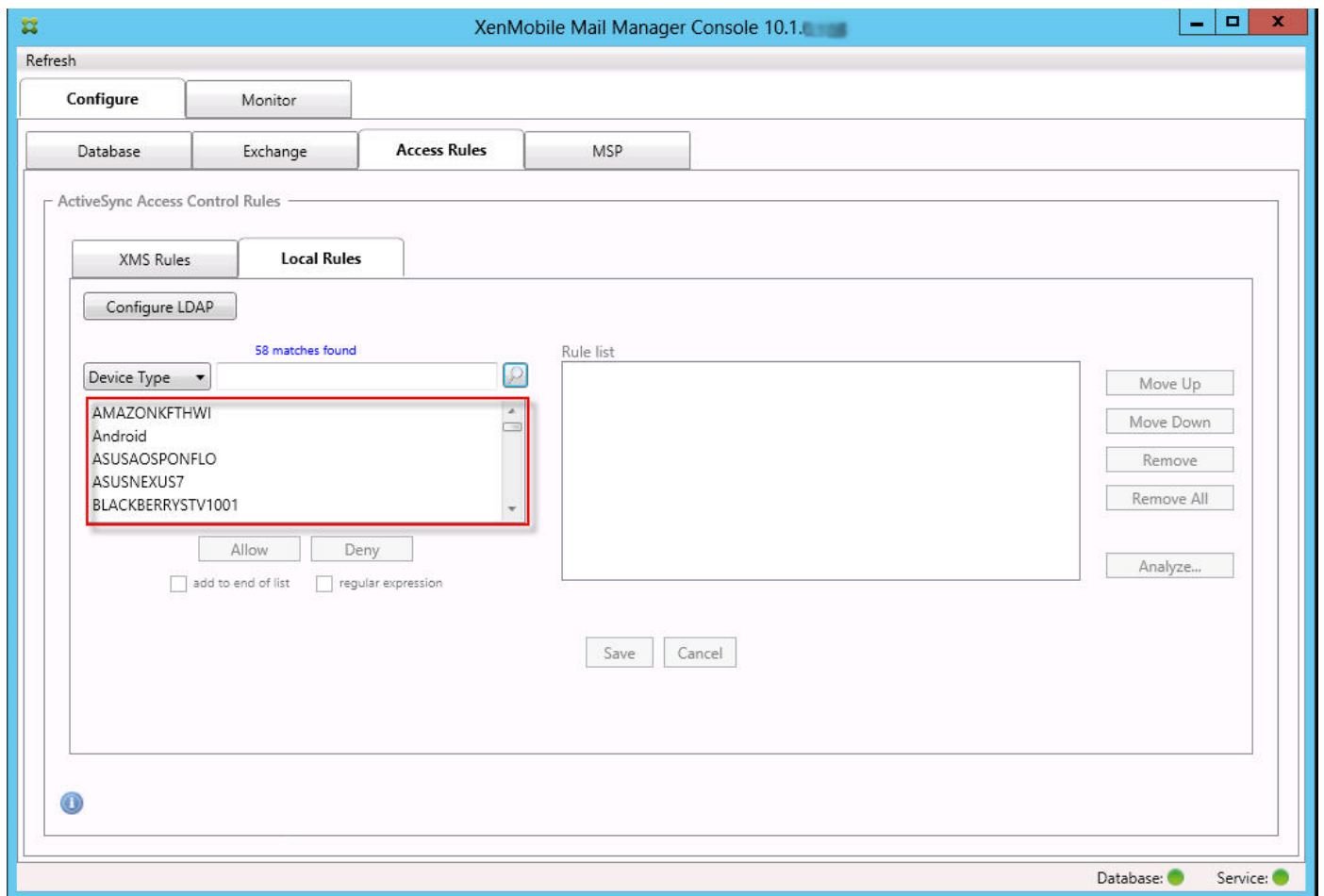
この例では、規則の関係に含まれる上書きされた規則が示されています。この規則は、通常のActiveSyncデバイスの種類の規

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ため、通常のActiveSyncデバイスの種類の規則Androidは補助規則として表示されていませんでした。

1. [Access Rules] タブをクリックします。

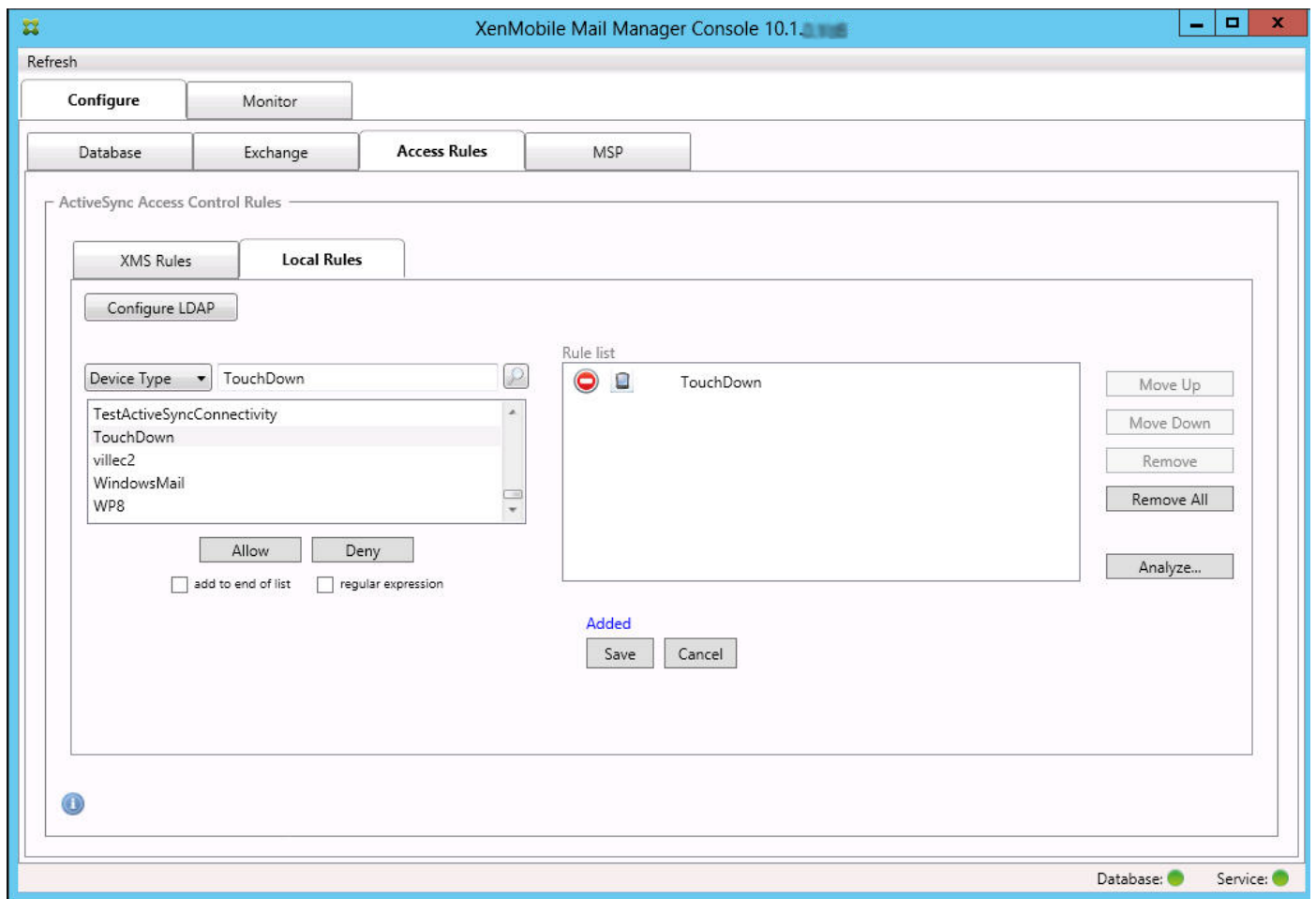


2. [Device ID] 一覧で、ローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[Device Type] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 表示されたリストボックスでいずれかのアイテムをクリックして、次のいずれかのオプションをクリックします。
- 許可を選ぶと、すべての一致するデバイスに対して、ActiveSyncトラフィックを許可するようにExchangeが構成されます。
  - 禁止を選ぶとすべての一致するデバイスに対して、ActiveSyncトラフィックを拒否するようにExchangeが構成されます。

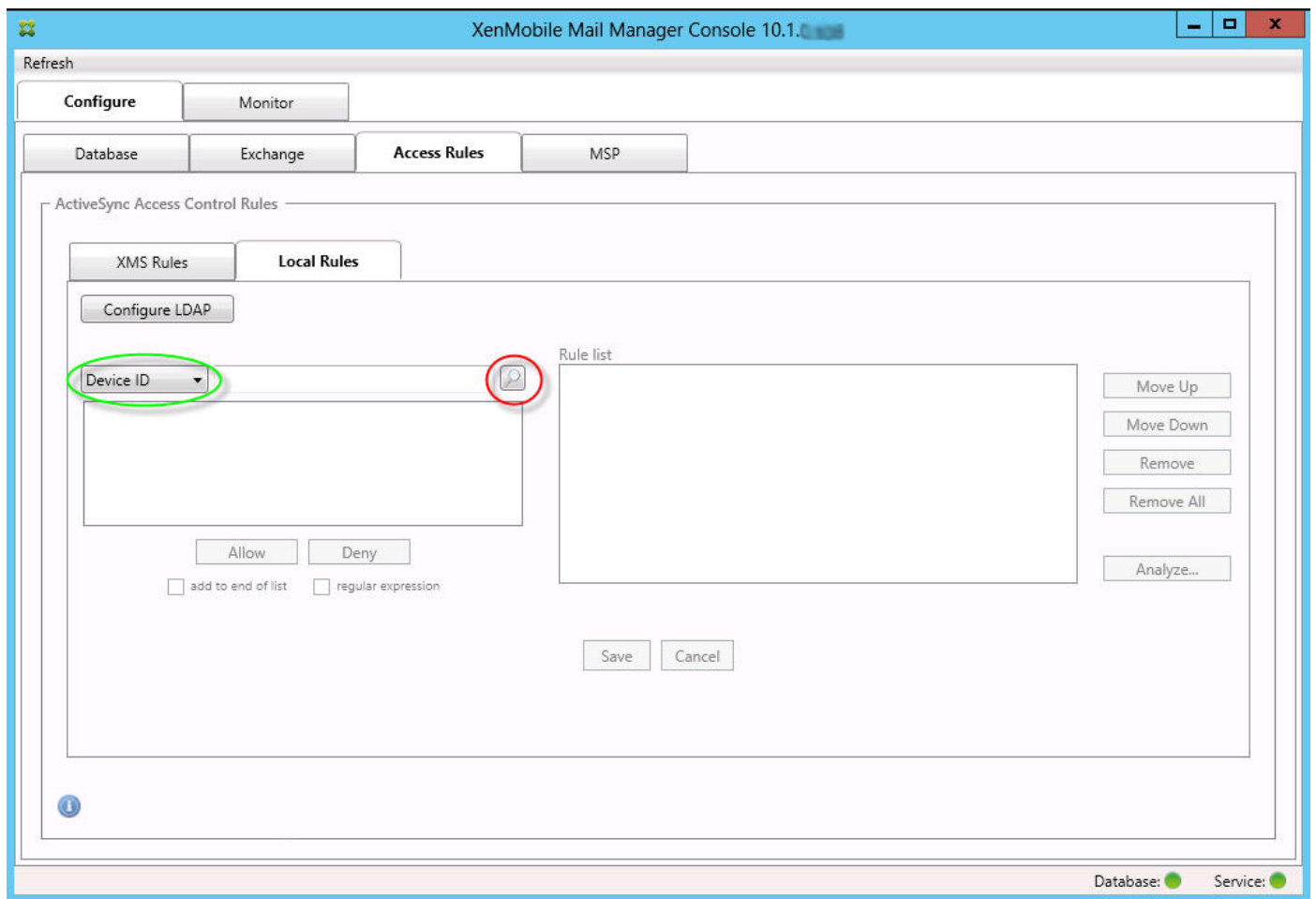
この例では、デバイスの種類がTouchDownであるすべてのデバイスのアクセスが拒否されます。



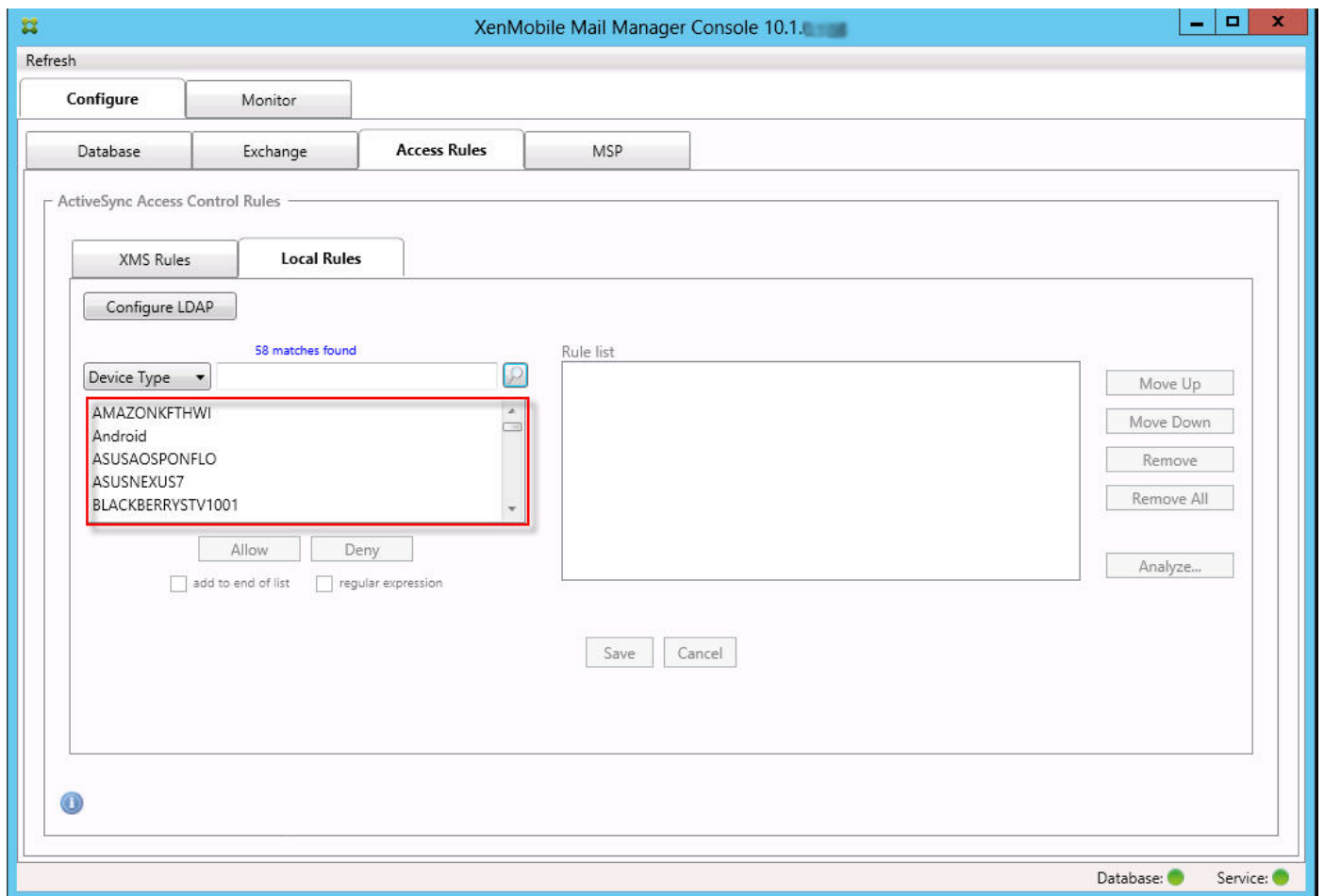
正規表現のローカル規則は、横に表示されるアイコン (.\* ) で識別できます。正規表現の規則を追加するには、特定のフィールドの結果一覧にある既存の値から正規表現の規則を作成（メジャースナップショットが完了している場合）するか、または必要な正規表現をそのまま入力します。

既存のフィールド値から正規表現を作成するには

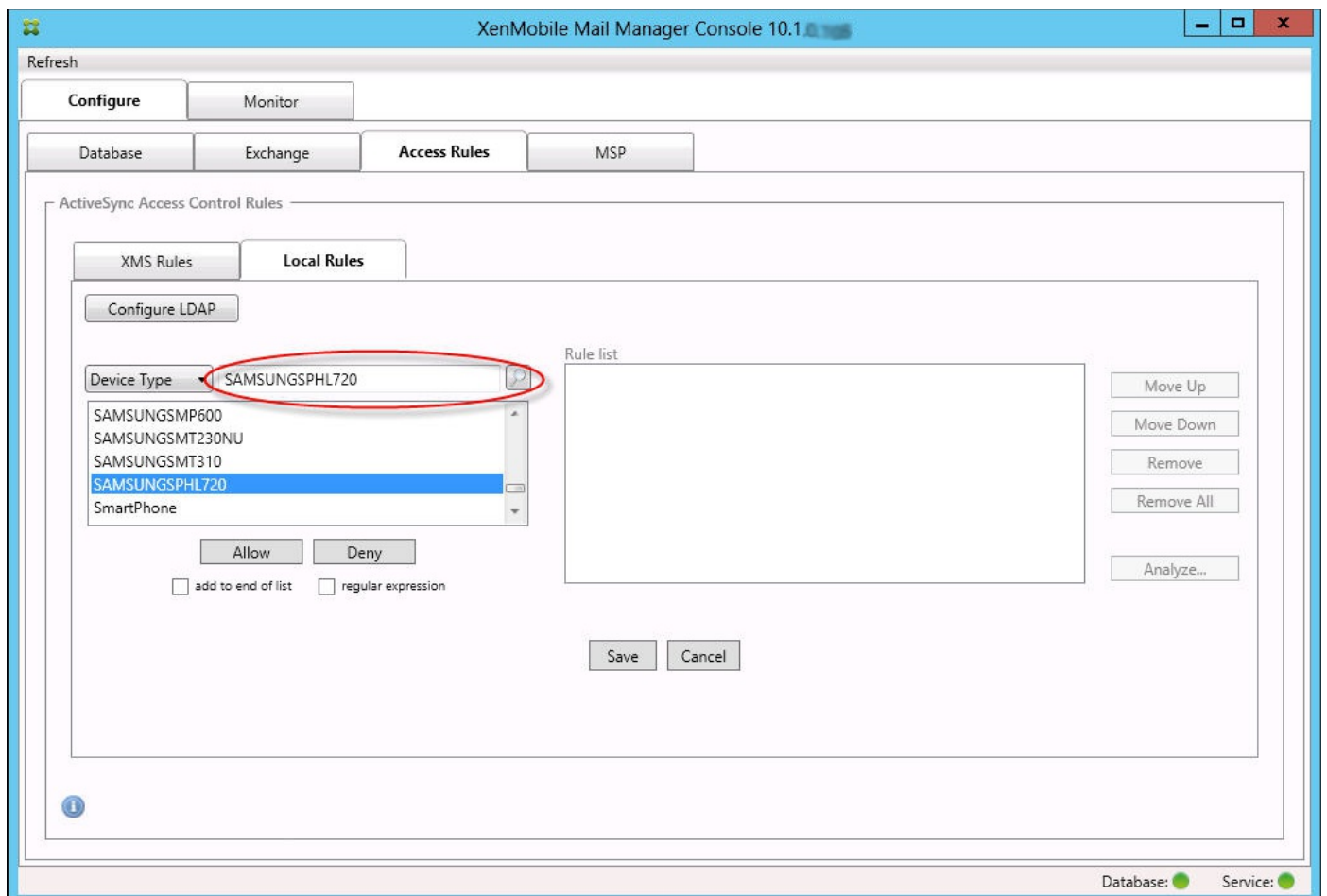
1. [Access Rules] タブをクリックします。



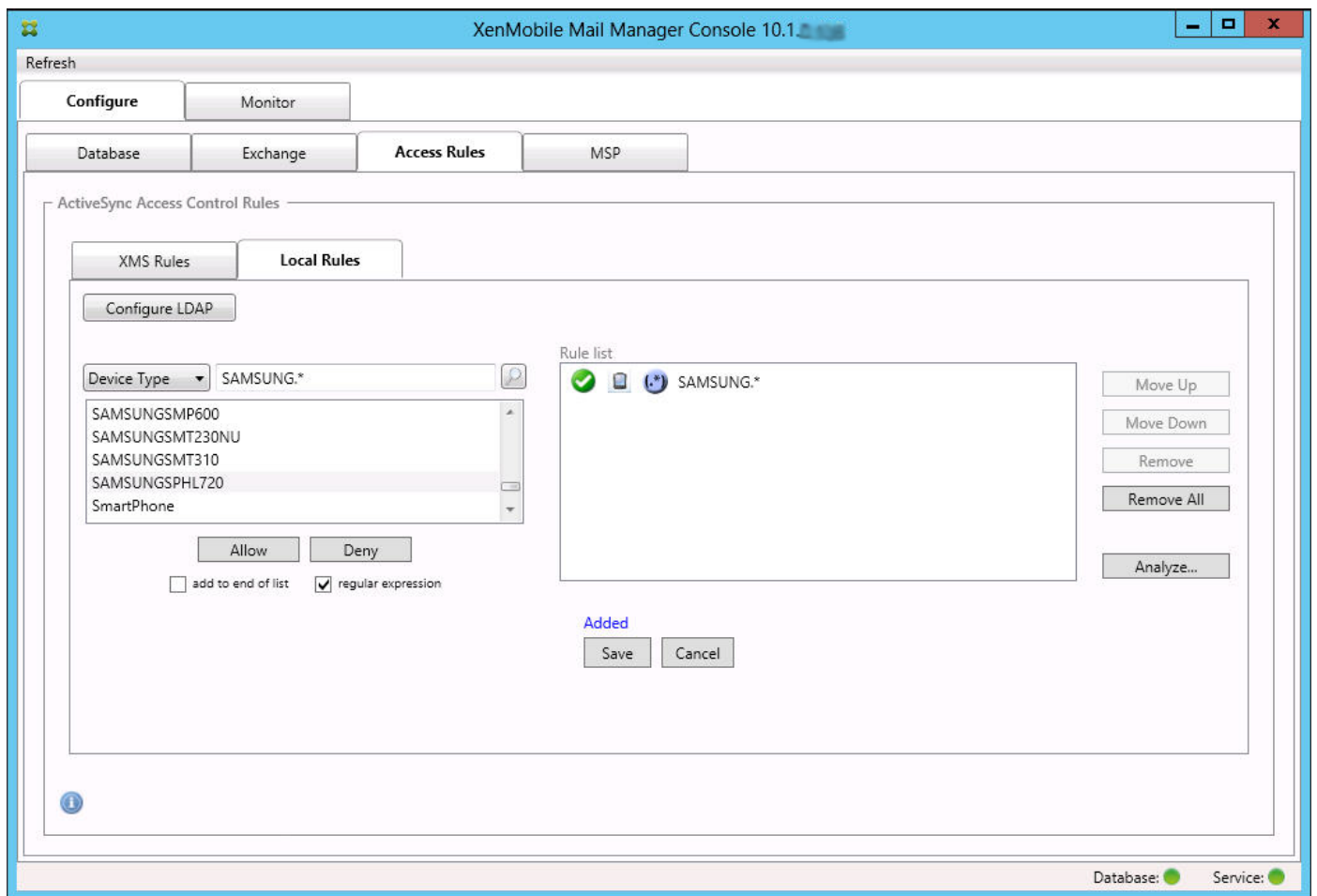
2. [Device ID] 一覧で、正規表現のローカル規則を作成するフィールドを選択します。
3. 虫眼鏡アイコンをクリックして、選択したフィールドに固有の一致をすべて表示します。この例では、[Device Type] フィールドが選択され、下のリストボックスに選択肢が表示されています。



4. 結果一覧でいずれかのアイテムをクリックします。この例では、SAMSUNGSPHL720が選択され、[Device Type] に隣接するテキストボックスに表示されています。

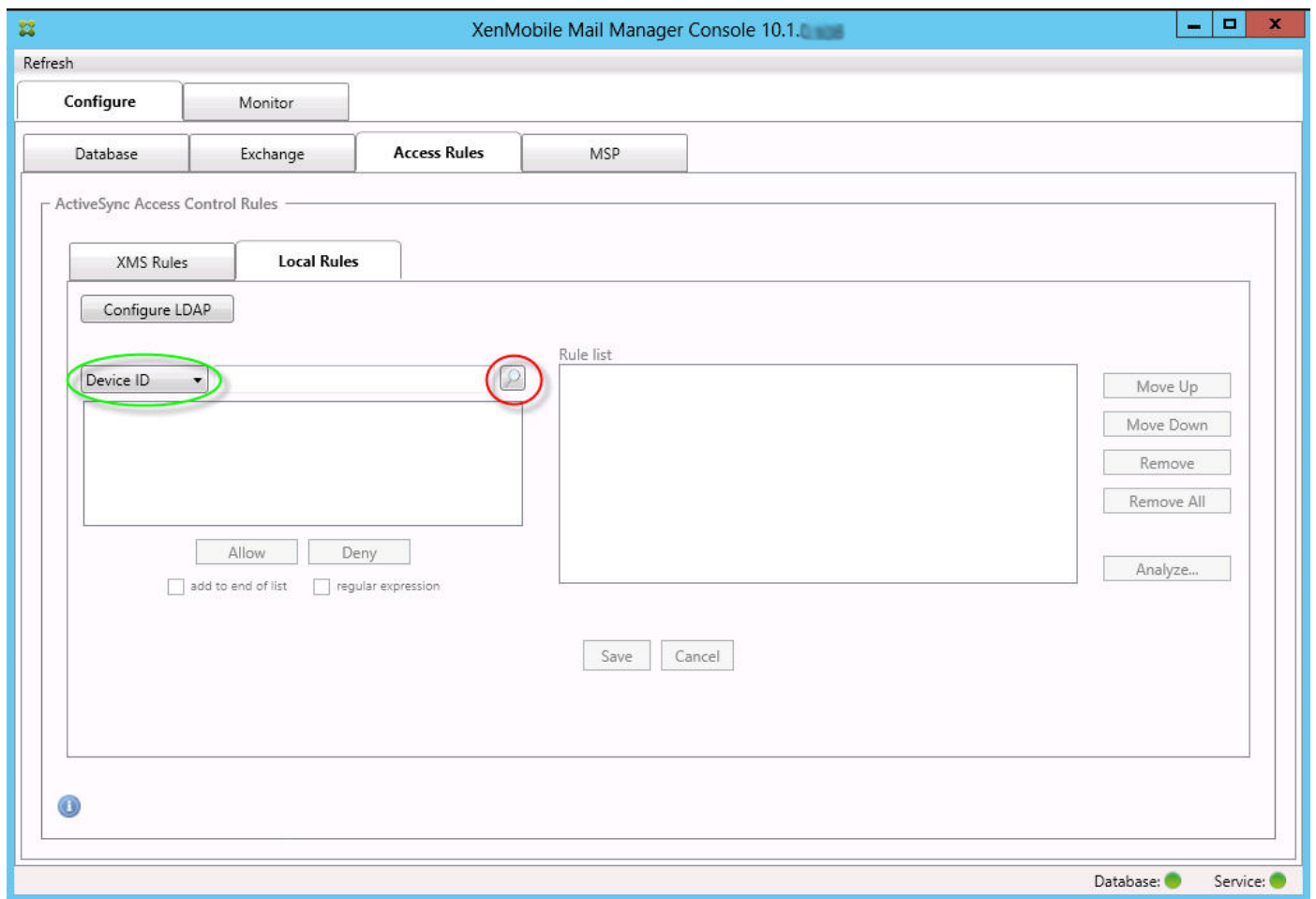


5. デバイスの種類の値に「Samsung」が含まれるすべてのデバイスの種類を許可するには、次の手順に従って正規表現の規則を追加します。
1. 選択済みアイテムのテキストボックス内をクリックします。
  2. SAMSUNGSPHL720からSAMSUNG.\*にテキストを変更します。
  3. [regular expression] チェックボックスをオンにします。
  4. [Allow] をクリックします。

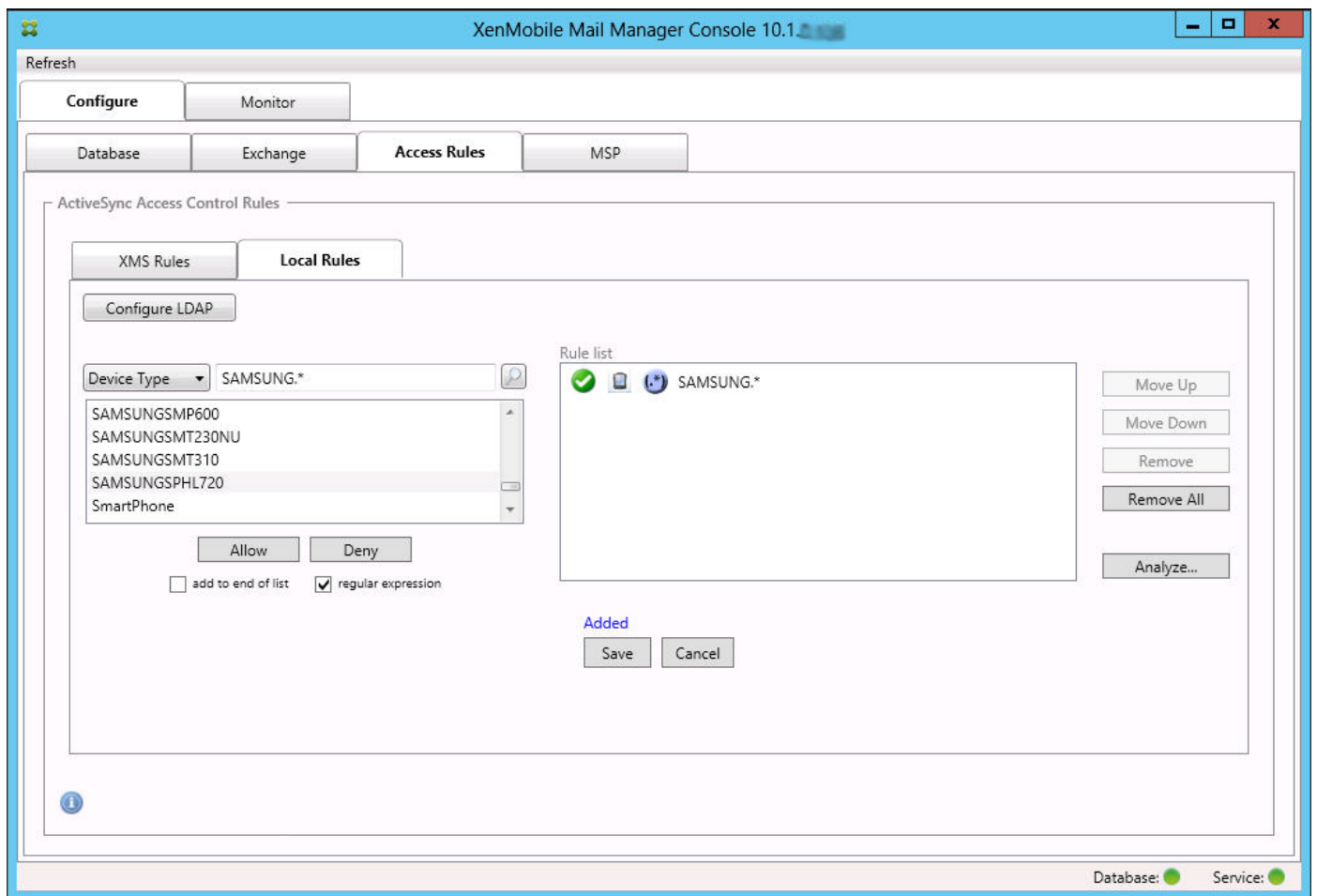


1. [Local Rules] タブをクリックします。
2. 正規表現を入力するには、[Device ID] 一覧と選択済みアイテムのテキストボックスの両方を使用する必要があります。



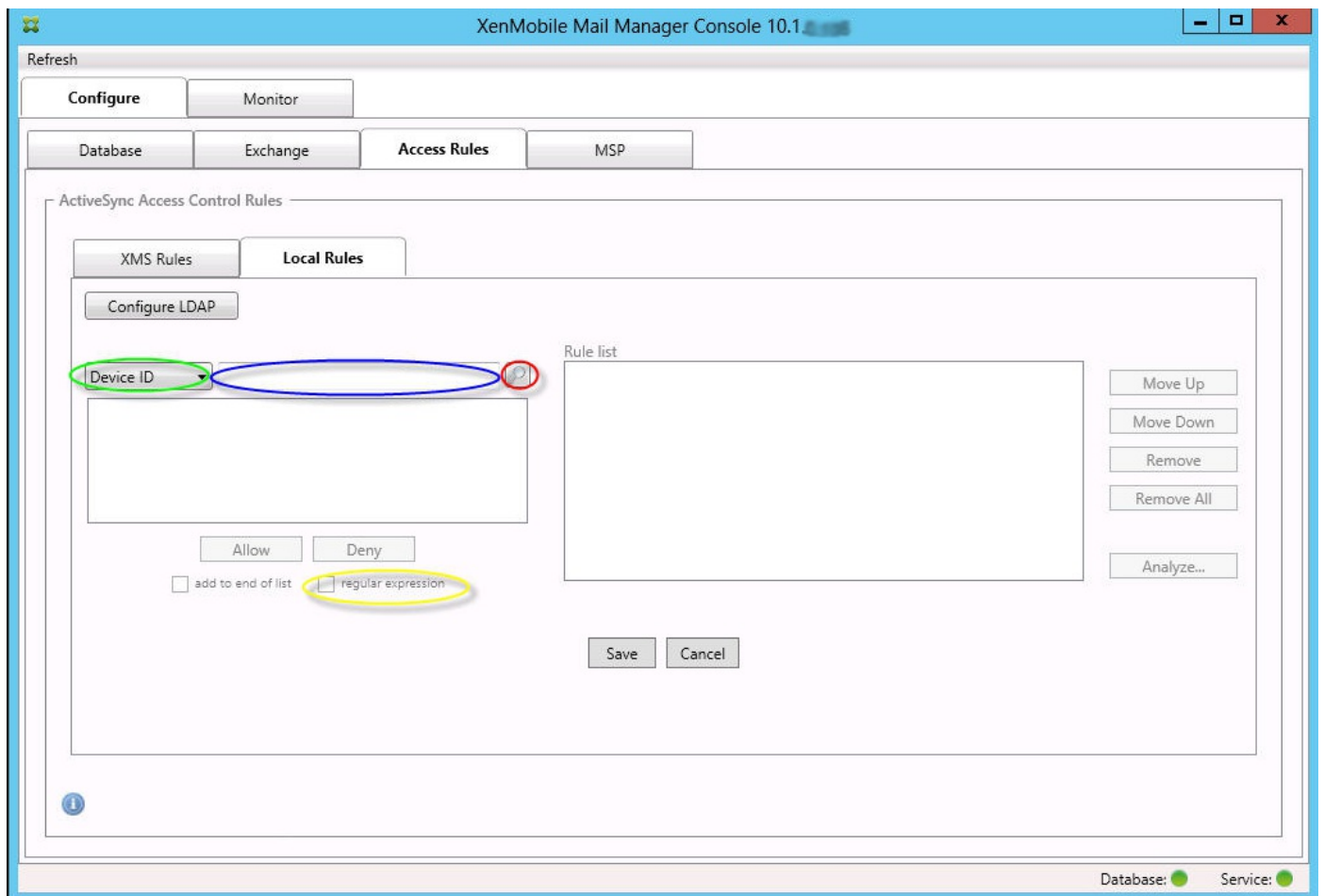


3. 照合するフィールドを選択します。この例では [Device Type] を使用します。
4. 正規表現を入力します。この例では `samsung.*` を使用します。
5. [regular expression] チェックボックスをオンにして、[Allow] または [Deny] をクリックします。この例では、[Allow] を選択し、最終結果は次のようになります。

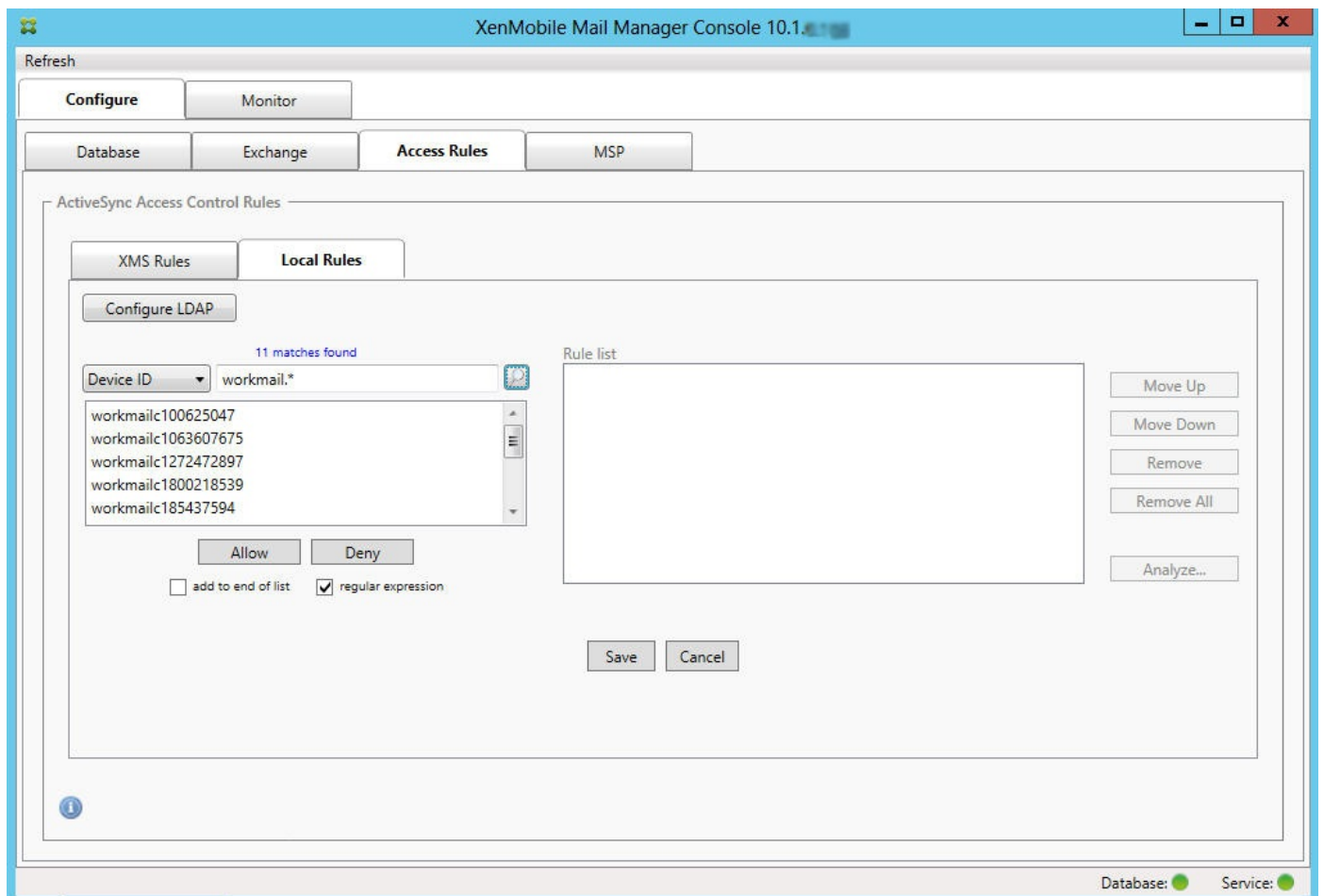


[regular expression] チェックボックスをオンにして、特定の式に一致する特定のデバイスの検索を実行できます。この機能は、メジャースナップショットが正常に完了している場合にのみ利用できます。正規表現の規則を使用しない場合でも、この機能を使用できます。たとえば、ActiveSyncデバイスIDにテキスト「workmail」が含まれるすべてのデバイスを検出するとします。これを行うには、以下の手順に従います。

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。



[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。

XenMobile Mail Manager Console 10.1

Refresh

Configure    **Monitor**

ActiveSync Devices    Blackberry Devices    Automation History

Selection

All Devices    Anytime    User: user    Device:    Go    Export...

Reported State	Requested State	User	Device ID	Type	Model
✓	?	auser1@xmlab.net	workmailc1800218539	MOTOROLAXT1528	XT1528
User Agent: WorkMail/10.3.0.225 (MOT Identity: xmlab.net/XM1/Lorna J Chan Last snapshot: 8/10/2016 1:49:52 PM First Sync: 4/12/2016 2:28:49 PM					
✓	?	auser1@xmlab.net	A182EB4483E64A99B4CED204444A63C7	iPad	iPad
✓	?	auser101@xmlab.net	96D3D564B5EA4EF28E891EE1D987817A	iPad	iPad
✓	?	auser101@xmlab.net	E4562615700543C58C68E5125D67DFBD	iPad	iPad
✓	?	auser101@xmlab.net	38939C2CE9254CE5A0A2ED18E906F9C1	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc680977375	MOTOROLAXT1068	XT1068
✓	?	auser101@xmlab.net	workmailc1929821768	MOTOROLANEXUS6	Nexus 6
✓	?	auser101@xmlab.net	0BD6E5254A6348FC9E3BF3EAF8FD8901	iPhone	iPhone
✓	?	auser101@xmlab.net	580D5785F02F48669457BD7E680DB38B	iPhone	iPhone
✓	?	auser101@xmlab.net	7DA7ED686ACE43C3928C6C357F6D7B97	iPhone	iPhone
✓	?	auser101@xmlab.net	workmailc185437594	HTCNEXUS9	Nexus 9
✓	?	auser101@xmlab.net	workmailc100625047	SAMSUNGSMT230NU	SM-T230NU
✓	?	auser101@xmlab.net	2FAFE4CF00794BA18A84647F581C0148	iPhone	iPhone

70 records read, 39 records displayed

Database: ● Service: ●

# デバイス監視

Apr 27, 2017

XenMobile Mail Managerの [Monitor] タブでは、検出されたExchange ActiveSyncデバイスおよびBlackBerryデバイスと、これまで自動で発行されたPowerShellコマンドの履歴を参照できます。 [Monitor] タブには、次の3つのタブがあります。

- ActiveSync デバイス :
  - [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サーバー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

Apr 27, 2017

XenMobile Mail Managerでは、エラーなどの動作情報がログファイル（\log\XmmWindowsService.log）に記録されます。また、Windowsイベントログに、重要なイベントが記録されます。

一般的なエラーを以下に示します。

## 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。

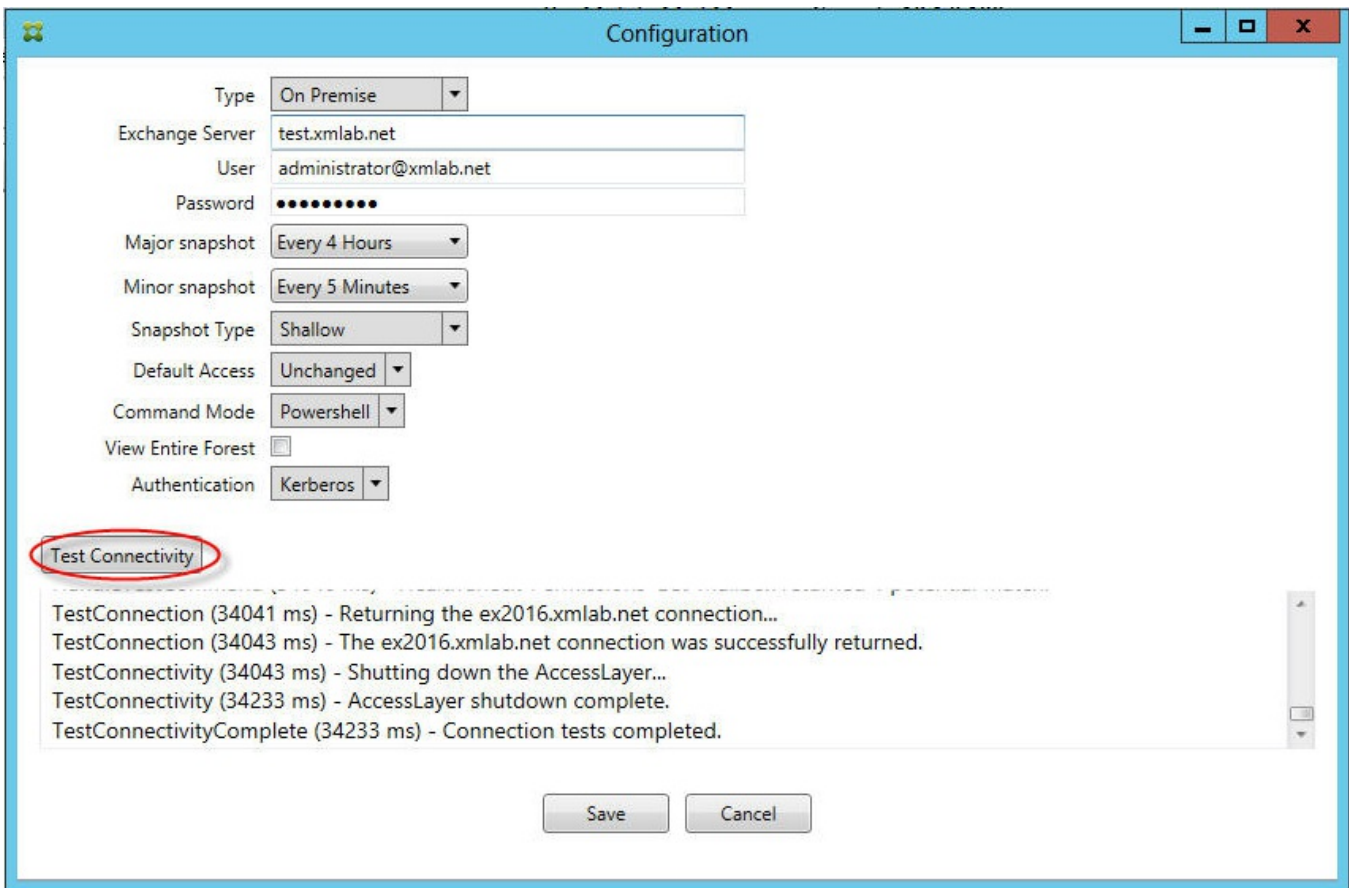
## XenMobileがMSPに接続できない

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。



Support\PowerShellフォルダーに、トラブルシューティング用のPowerShellユーティリティー式が用意されています。

トラブルシューティングツールは、ユーザーのメールボックスやデバイスを詳細に分析してエラー条件や障害が発生しやすい領域を検出し、また、ユーザーの詳細RBAC分析を行います。すべてのコマンドレットの未加工の出力をテキストファイルに保存することができます。



# XenMobile NetScaler Connector

Apr 27, 2017

XenMobile NetScaler Connectorでは、Exchange ActiveSyncプロトコルのリバースプロキシとして動作するNetScalerに、ActiveSyncクライアントのデバイスレベルの認証サービスを提供します。認証は、XenMobile内で定義されたポリシーの組み合わせと、XenMobile NetScaler Connectorによりローカルで定義されたルールによって制御されます。

詳しくは、次の記事を参照してください。

- [XenMobile NetScaler Connector](#)
- [XenMobileでのActiveSyncゲートウェイ](#)

リファレンスアーキテクチャ図について詳しくは、『XenMobile展開ハンドブック』の、[オンプレミス展開のリファレンスアーキテクチャ](#)についての記事を参照してください。