Problèmes résolus

Feb 23, 2017

Les problèmes suivants ont été résolus dans XenMobile 10.4. Les problèmes résolus relatifs à l'outil de mise à niveau s'affichent sous l'en-tête « Outil de mise à niveau XenMobile 10.4 » à la fin de cet article.

Remarque : à compter de la version 10.4, les applications mobiles Worx sont renommées applications XenMobile. La plupart des applications XenMobile individuelles ont aussi changé de nom. Pour de plus amples informations, consultez la section À propos des applications XenMobile.

Lorsque vous essayez d'ajouter une application depuis un magasin public pour Windows Phone, lorsque vous entrez une adresse URL depuis le magasin Microsoft, le téléchargement échoue. [CXM-13468]

Avec certaines configurations, après la mise à niveau de XenMobile 9 vers 10.3.6, les appareils qui ont été inscrits dans XenMobile 9 ne peuvent pas ouvrir les applications installées ou télécharger des applications à partir du WorxStore. Les applications disparaissent également de Worx Home et les utilisateurs ne peuvent pas accéder au WorxStore. [CXM-13708]

Lorsque vous créez une stratégie Wi-Fi avec un mot de passe Wi-Fi défini qui contient des caractères spéciaux, tels qu'un symbole inférieurs à (<), un symbole supérieur à (>) ou une esperluette (&), les utilisateurs sont invités à entrer leur mot de passe Wi-Fi. [CXM-13717]

Lorsque vous essayez de charger une application d'entreprise iOS, une erreur « icône introuvable » s'affiche lorsque la taille de l'icône dépasse 1 000 Ko. [CXM-13729]

Si la mise en cluster est activée et qu'un effacement d'appareil est envoyé à une session déconnectée, l'appareil est effacé lorsqu'il se reconnecte, comme prévu. Toutefois, si l'appareil se réinscrit ou se connecte à un autre nœud de cluster, XenMobile efface de nouveau l'appareil. [CXM-13793]

L'autorisation Assistant d'inscription d'appareils partagés est activée par défaut pour le rôle RBAC Admin dans les déploiements XenMobile Service (Cloud). Par conséquent, tous les appareils appartenant aux utilisateurs avec le rôle administrateur s'inscrivent en tant qu'appareils partagés. [CXM-15203]

Lorsque vous configurez l'authentification de certificat client et que l'option Require Server Name Indication est activée sur le serveur de l'autorité de certification, l'inscription échoue. [CXM-15312]

Lors d'une recherche d'application dans Google Play Store à partir de la console XenMobile, la recherche ne renvoie pas les applications basées sur le système d'exploitation Android sur l'appareil inscrit. Par exemple, les applications qui requièrent un système d'exploitation minimum de 4.4 ne s'affichent pas dans les résultats. [CXM-15653]

Lorsque vous créez un utilisateur local affecté à un groupe local et que l'utilisateur local tente de s'inscrire à l'aide d'un appareil Windows 10, l'inscription échoue. [CXM-16895]

Lorsque vous créez une stratégie Citrix Launcher, les utilisateurs peuvent inscrire un appareil Android, mais si vous modifiez un paramètre de stratégie, ils ne peuvent pas fermer Citrix avec le mot de passe que vous avez configuré dans la stratégie. Une solution consiste à réinsérer le mot de passe dans les paramètres de stratégie et à mettre à jour la stratégie. [CXM-17157]

Lorsque vous désactivez l'option Activer ShareFile dans XenMobile, dans Secure Mail pour Android, les utilisateurs ne peuvent accéder à aucune pièce jointe. [CXM-17887]

Lorsque vous mettez à jour XenMobile 10.3.6 avec Rolling Patch 1 vers XenMobile 10.4, les licences permanentes expirent

avec un message d'erreur. [CXM-17900]

Lorsque vous mettez à jour XenMobile 10.3.6 vers XenMobile 10.4, bien que la licence permanente soit toujours valide, un message d'erreur sur l'expiration de la licence s'affiche. [CXM-17987]

Si vous entrez manuellement une adresse URL pour une application de magasin d'applications public Windows et que l'adresse URL ne correspond pas à un magasin basé aux États-Unis, la console XenMobile affiche une erreur. Lorsque vous utilisez l'URL du magasin d'applications basé aux États-Unis, le chargement réussit. [CXM-18013]

Lorsque les utilisateurs reçoivent leur mot de passe à usage unique pour la liaison IMEI (nom d'utilisateur et mot de passe) et les notifications SMS et SMTP, le premier profil s'installe avec succès mais l'installation du second profil échoue avec le message d'erreur « Profile Installation Fails. A connection to the server could not be established. » Les iPhone 6 et iPhone 6 Plus comprennent deux numéros, un numéro IMEI et un numéro MEID, et le mot de passe à usage unique est lié au numéro MEID plutôt qu'au numéro IMEI. Vous pouvez remplacer le numéro IMEI grâce à l'identifiant unique (UDID) de l'iPhone ou utiliser un numéro de téléphone ordinaire. [#606162]

Si vous essayez de télécharger une demande de signature de certificat (CSR) à partir de navigateurs Web Internet Explorer et Firefox, les tentatives échouent avec l'erreur « La page Web ne peut pas être affichée. » Le téléchargement de la demande de signature de certificat fonctionne à partir du navigateur Web Chrome. [#609552]

Si vous ouvrez une session sur la console XenMobile, que vous accédez à **Analyser > Rapports**, puis que vous cliquez sur **Appareils inactifs**, une page blanche s'affiche au lieu de la page de téléchargement du fichier. [#609649]

XenMobile NetScaler Connector ne peut pas obtenir les appareils Samsung 5.x depuis une synchronisation avec ActiveSync. [#613522]

Lorsque vous créez une stratégie Wi-Fi pour Android avec un type d'authentification 802.1x EAP, le champ Mot de passe n'est plus obligatoire. [#614932]

Cette correction résout une faille de sécurité. Pour de plus amples informations, consultez le bulletin de sécurité http://support.citrix.com/article/CTX207824.
Remarque : pour que cette correction de sécurité fonctionne, un redémarrage du serveur XenMobile est requis. [#624347]

Vous ne pouvez pas trouver votre ID Android en entrant *#*#8255#*#*sur votre téléphone, comme indiqué sur la page **Paramètres > Identifiants Google Play** de XenMobile. Utilisez une application d'ID d'appareil à partir du Google Play Store pour rechercher votre ID d'appareil. [#633854]

Il arrive parfois que l'inscription d'appareils Windows Phone ne parvienne pas à démarrer Worx Home. [#633884]

Les applications HDX désactivées ne sont pas énumérées dans le Worx Store. [#634110]

Le serveur XenMobile affiche des données utilisateur incorrectes dans le fichier journal. [#636754]

Après la mise à jour de XenMobile 10.3.1 vers 10.3.6, le type de fichier et le dossier de destination définis dans les propriétés Stratégie de fichiers ne s'affichent pas correctement dans la console XenMobile. [#640334]

La longueur maximale de la zone de texte du jeton VPP est 256 caractères. [#640692]

Les utilisateurs Windows Phone ne peuvent pas inscrire d'appareil avec un sAMAccount. [#640847]

Après la suppression d'utilisateurs inscrits du sous-système de contrôle ShareFile, les utilisateurs inscrits peuvent s'afficher dans le fichier journal d'audit utilisateur de la console XenMobile. [#641342]

Si vous cliquez sur https:///zdm/enrollmdm.html après la mise à niveau de XenMobile Server 10.1 vers 10.3.x, la plate-forme iOS n'est pas répertoriée en tant que plate-forme disponible à la sélection. [#641771]

Lorsque vous inscrivez un appareil iOS auprès de Worx Home, l'inscription MDM peut réussir mais l'enregistrement MAM échoue. [#644892]

La suppression des groupes imbriqués n'est jamais reflétée. [#647557]

Si **Gérer > Inscription** a plus de 2 000 entrées, lorsque vous cliquez sur **Exporter**, la page est vide et le rapport n'est pas généré. [#647855]

Les administrateurs XenMobile qui essayent d'accéder à la console XenMobile peuvent être dirigés vers le portail en libre-service de XenMobile. Cela peut se produire lorsque des groupes d'administrateurs XenMobile sont créés avec un contrôle d'accès basé sur un rôle et qu'un groupe est déplacé d'une unité d'organisation Active Directory à une autre. [#647987]

Le chargement d'applications iOS peut échouer avec l'erreur : L'application mobile chargée n'est pas valide. Icône d'application introuvable. [#649574]

Le serveur XenMobile peut cesser de répondre avec une erreur de mémoire insuffisante. [#650490]

Problèmes d'effacement de l'appareil à cause de messages en cluster. [#650555]

Lors de la configuration d'une stratégie VPN, vous ne pouvez pas spécifier de numéro de port. [#650972]

Après la mise à niveau du serveur XenMobile avec mise en cluster activée, plusieurs blocages peuvent se produire. Le serveur peut cesser de répondre. [#651122]

La console XenMobile n'indique pas le numéro de série de l'appareil lorsque vous êtes invité à confirmer la suppression d'un appareil. [#651185]

La stratégie de compte SSO sur le serveur XenMobile 10.3.6 ne fonctionne pas comme prévu. Les utilisateurs sont invités à entrer un mot de passe. [#651860]

Impossible de désactiver l'association d'applications iPad sur XenMobile 10.3.6 pour les applications VPP.[#652280]

Si vous supprimez un groupe de mise à disposition d'une stratégie d'appareil, XenMobile n'enregistre pas la modification et le groupe de mise à disposition reste attribué à la stratégie. [#652321]

Le compte SSO ne parvient pas à enregistrer le nom de domaine complet court. [#652704]

Lorsqu'un utilisateur supprime les droits Admin. de périphérique de son appareil Android, XenMobile change l'état des appareils MDX et MAM inscrits sur « Orange/non géré » et l'utilisateur n'a pas accès aux applications MDX. L'état MAM doit rester « Vert/géré ». [#655180]

Outil de mise à niveau XenMobile 10.4

Si le paramètre dans XenMobile 9.0 relatif au système d'exploitation minimum ou maximum est défini sur 10 ou plus et relatif aux appareils exclus est défini sur les applications MDX et d'entreprise, la règle n'est pas migrée correctement après la mise à niveau. Les applications qui devraient apparaître ne s'affichent pas et celles qui ne devraient pas apparaître s'affichent. [#603412]

Si Microsoft SQL server est configuré pour respecter la casse, une mise à niveau échoue si le tableau « Id_Generator » est spécifié en tant que « id_generator ». [#623300]

Après la mise à niveau de XenMobile 9 vers XenMobile 10, le type de valeur de la stratégie Personal Hotspot est booléen au lieu de chaîne. [#633337]

Si le nom d'un groupe Active Directory contient le caractère « @ », une mise à niveau échoue. [#633718]

Si votre serveur Device Manager 9.0 est configuré à l'aide d'une base de données PostgreSQL locale et que vous utilisez localhost comme référence pour le serveur de base de données, une mise à niveau échouera. Pour contourner ce problème, modifiez ew-config.properties sur le serveur Device Manager 9.0 et remplacez toutes les références à localhost avec l'adresse IP du serveur de base de données Device Manager, puis continuez avec les conditions requises pour la mise à niveau. [#635023]

Dans XenMobile 9.0, lorsque vous définissez l'**Unité d'organisation des utilisateurs** (OU) dans les paramètres de la connexion LDAP, après la mise à niveau vers XenMobile 10, le contexte racine complet n'est pas ajouté à l'unité d'organisation des utilisateurs. Par exemple, OU=MDMUsers, OU=SALES doit être OU=MDMUsers, OU=SALES, DC=citrite, DC=com. Par conséquent, vous devez effectuer la mise à jour manuellement dans XenMobile 10. [#635981]

Durant une mise à niveau, lorsque vous téléchargez le pack d'assistance, le message d'erreur « MAM set up failed, see the logs for details » s'affiche et l'outil de mise à niveau conserve les données MAM altérées. [#638062]

Si le nom d'un groupe Active Directory contient le caractère « . », un rôle migré en tant que groupe de mise à disposition perd son association au groupe. [#647590]

Si le paramètre de proxy web dans App Controller contient le caractère « \ », le serveur XenMobile 10.1 ne peut pas démarrer et le message « Starting main app... » s'affiche alors que le serveur continue à redémarrer. [#647919]

Après une mise à niveau de XenMobile 9 vers XenMobile 10, les applications VPP payantes ne s'installent pas à partir du magasin XenMobile (Worx) à moins que la configuration de l'application nécessite une installation. [#668102]

Dans une configuration d'authentification inter-domaines, après la mise à niveau vers XenMobile 10.3.6, les appareils qui ont été inscrits précédemment dans XenMobile 9 ne peuvent pas ouvrir les applications installées ou télécharger de nouvelles applications depuis le magasin XenMobile (Worx) ni accéder au magasin. [CXM-13708]

Après une mise à niveau de XenMobile 9 vers XenMobile 10, les applications provenant d'un magasin d'applications public qui sont installées s'affichent comme non inscrites dans le magasin XenMobile (Worx). [CXM-17936]

Si l'URL de connexion à la base de données est localhost, vous n'avez plus besoin de modifier le fichier ew-config.properties.

Si vous avez configuré des rôles RBAC avec un accès limité à LDAP et à Active Directory ou tout enfant, lorsque vous ouvrez une session sur la console XenMobile en tant qu'administrateur après la mise à niveau, les mêmes paramètres ne sont pas sélectionnés.

Problèmes connus

Feb 23, 2017

Vous trouverez ci-dessous les problèmes connus dans XenMobile 10.4.

Lorsque vous configurez Citrix Launcher, l'option **Une seule fois** ne fonctionne pas. Vous devez cliquer sur l'option **Toujours**. [CXM-13413]

Parfois, lorsque les utilisateurs réinscrivent un appareil Android, un effacement des données d'entreprise se produit de façon inattendue. [CXM-13716]

Si vous avez configuré des applications publiques dans la console XenMobile, lorsque vous mettez à jour vers XenMobile 10.4, puis déployez Secure Hub sur une tablette Windows 10, les utilisateurs ne peuvent pas voir les applications publiques. [CXM-16516]

Avec Citrix Launcher, en mode MDM, lorsque les utilisateurs ouvrent XenMobile Store, le magasin s'affiche dans un navigateur par défaut, même si vous avez indiqué un autre navigateur dans une liste blanche. [CXM-17097]

Citrix Launcher ne peut pas télécharger le logo et les images d'arrière-plan à partir d'un serveur disposant d'un certificat auto-signé. [CXM-17159]

Lors de l'utilisation de la console XenMobile avec un navigateur Internet Explorer 11, vous ne pouvez pas ajouter une nouvelle configuration LDAP. [CXM-18324]

Outil de mise à niveau XenMobile 10.4

Problèmes liés aux données et aux stratégies

Après la mise à niveau, les données de configuration du serveur syslog ne sont pas migrées sur le serveur XenMobile. [#558539]

Certaines configurations de stratégie de restriction sont obsolètes depuis la version 10.1. Par conséquent, XenMobile 10.4 ne parvient pas à déployer la stratégie de restriction sur les téléphones Windows 10 après la mise à niveau de XenMobile 9 vers XenMobile 10.4. Toutefois, si vous affichez et enregistrez les paramètres de stratégie dans XenMobile 10.4, la stratégie est déployée avec succès. [#608541]

Si votre déploiement dans XenMobile 9 inclut une application d'entreprise gpsstats.apk, la mise à niveau vers XenMobile 10.4 peut échouer. [CXM-17992]

Après avoir effectué la mise à niveau vers XenMobile 10.4 sur XenMobile 9, les appareils Windows sont en mode MDM plutôt que dans le mode MDM + MAM ; en outre, XenMobile Store ne s'ouvre pas. Pour contourner le problème, les utilisateurs peuvent réinscrire un appareil migré. [CXM-18532]

Applications Google Play

Si vous avez inclus une application Google Play publique pour les appareils Android avec une icône par défaut, après la migration, l'icône par défaut ne s'affiche pas dans la console XenMobile. Vous devez modifier et enregistrer l'application, ou cliquez sur Rechercher les mises à jour pour que l'image s'affiche. [#557996]

SQL Server

Si vous utilisez une base de données PostgreSQL, les appareils MAM ne peuvent pas se réinscrire après une mise à niveau. Pour contourner ce problème, supprimez les entrées de l'appareil dans XenMobile et envoyez des notifications d'inscription aux utilisateurs. [#632831]

RBAC

Problèmes avec les paramètres RBAC après la mise à niveau :

- Si vous avez configuré un rôle de super administrateur, toutes les autorisations sont sélectionnées par défaut. Après la mise à niveau, seules trois autorisations sont sélectionnées : Inscription RBAC et Gestion des versions.
- Si vous avez créé un rôle de super administrateur, toutes les autorisations de support doit être sélectionnées par défaut. Après la mise à niveau, aucun des paramètres d'autorisation de support n'est sélectionné. Pour contourner ce problème, créez l'autorisation de support après la mise à niveau. [#569350, #569395, #569423]

Citrix Secure Hub et Citrix Store

Avant la mise à niveau de XenMobile 9 vers XenMobile 10.4, si votre WorxStore a un nom personnalisé, des problèmes se produisent lors de l'inscription, de l'accès à Worx Home et de l'accès au Worx Store. Pour contourner le problème, utilisez le nom par défaut du magasin, à savoir **Store**, avant la mise à niveau. Pour de plus amples informations sur les solutions aux problèmes avant mise à niveau, consultez la section Pré-requis pour l'outil de mise à niveau. [#619458]

Les utilisateurs avec appareils MAM exclusif ne peuvent pas s'authentifier auprès de Citrix Secure Hub après une mise à niveau de XenMobile 9.0 vers XenMobile 10.4 et la définition de l'option LDAP **Recherche utilisateur par** sur **sAMAccountName**. [#628233]

Android for Work

Après une mise à niveau, l'ouverture de session SAML pour Android for Work échoue car le certificat SAML possède une extension .pem, que le serveur XenMobile ne pourra pas importer. [#631795]

Pour contourner ce problème, assurez-vous que XenMobile dispose du certificat SAML approprié, comme suit :

1. Exportez le certificat SAML de XenMobile 9 App Controller avec une clé privée (AppController.exemple.com). Ce certificat est au format PEM et possède une extension .pem.

2. Utilisez la commande openssl pour générer un fichier PFX à partir du fichier PEM :

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

3. Importez le fichier PFX dans XenMobile 10.3 en tant que keystore SAML.

4. Exportez le certificat SAML sans la clé privée depuis XenMobile 10.4, puis chargez-le sur le domaine Android for Work.

Architecture

Feb 23, 2017

Les composants XenMobile dans l'architecture de référence XenMobile que vous déployez sont basés sur les besoins en matière de gestion des applications ou appareils de votre organisation. Les composants XenMobile sont modulaires et complémentaires. Par exemple, vous souhaitez accorder aux utilisateurs de votre organisation un accès à distance à des applications mobiles et vous devez connaître les types d'appareils avec lesquels les utilisateurs se connectent. Dans ce scénario, vous pouvez déployer XenMobile avec NetScaler Gateway. XenMobile est l'emplacement à partir duquel vous gérez les applications et les appareils, et NetScaler Gateway permet aux utilisateurs de se connecter à votre réseau.

Déploiement des composants XenMobile : vous pouvez déployer XenMobile afin de permettre aux utilisateurs de se connecter à des ressources sur votre réseau interne de l'une des façons suivantes :

- Connexions au réseau interne. Si vos utilisateurs sont distants, ils peuvent se connecter à l'aide d'un VPN ou d'une connexion micro VPN via NetScaler Gateway pour accéder à des applications et des bureaux dans le réseau interne.
- Inscription d'appareils. Les utilisateurs peuvent inscrire des appareils mobiles dans XenMobile de façon à ce que vous puissiez gérer les appareils qui se connectent aux ressources du réseau dans la console XenMobile.
- Applications Web, SaaS et mobiles. Les utilisateurs peuvent accéder à leurs applications Web, SaaS, mobiles à partir de XenMobile via Secure Hub.
- Applications et bureaux virtuels Windows. Les utilisateurs peuvent se connecter par le biais de Citrix Receiver ou un navigateur Web pour accéder à des applications et des bureaux virtuels Windows à partir de StoreFront ou l'Interface Web.

Pour utiliser une partie ou l'ensemble de ces fonctionnalités, Citrix vous recommande de déployer les composants XenMobile dans l'ordre suivant :

- NetScaler Gateway. Vous pouvez configurer les paramètres dans NetScaler Gateway afin de faciliter la communication avec XenMobile, StoreFront ou l'Interface Web à l'aide de l'assistant de configuration rapide. Avant d'utiliser l'assistant de configuration rapide dans NetScaler Gateway, vous devez installer XenMobile, StoreFront ou l'Interface Web de façon à pouvoir communiquer avec ces derniers.
- XenMobile. Après avoir installé XenMobile, vous pouvez configurer les stratégies et les paramètres qui permettent aux utilisateurs d'inscrire leurs appareils mobiles dans la console XenMobile. Vous pouvez également configurer des applications mobiles, Web et SaaS. Les applications mobiles peuvent inclure des applications provenant de l'App Store ou de Google Play. Les utilisateurs peuvent également se connecter à des applications mobiles que vous wrappez avec le MDX Toolkit et que vous chargez sur la console.
- MDX Toolkit. MDX Toolkit peut wrapper de manière sécurisée des applications qui ont été créées au sein de votre organisation ou hors de l'entreprise, telles que les applications XenMobile. Après avoir wrappé une application, vous pouvez utiliser la console XenMobile pour ajouter l'application à XenMobile et modifier la configuration de la stratégie en fonction de vos besoins. Vous pouvez également ajouter des catégories d'applications, appliquer des workflows et déployer des applications sur des groupes de mise à disposition. Consultez la section À propos de MDX Toolkit.
- StoreFront (facultatif) Vous pouvez fournir l'accès à des applications et des bureaux virtuels Windows à partir de StoreFront via des connexions avec Receiver.
- ShareFile Enterprise (facultatif). Si vous déployez ShareFile, vous pouvez activer l'intégration de l'annuaire d'entreprise via XenMobile, qui agit en tant que fournisseur d'identité SAML (Security Assertion Markup Language). Pour de plus amples informations sur la configuration de fournisseurs d'identité pour ShareFile, consultez le site de support de ShareFile.

XenMobile prend en charge une solution intégrée qui fournit une gestion des appareils et des applications via la console

XenMobile. Cette section décrit l'architecture de référence du déploiement XenMobile.

Dans un environnement de production, Citrix vous recommande de déployer la solution XenMobile dans une configuration en cluster à des fins de montée en charge et de redondance. Par ailleurs, l'utilisation de la capacité de déchargement SSL de NetScaler peut réduire la charge sur le serveur XenMobile et augmenter le débit. Pour de plus amples informations sur la configuration de la mise en cluster pour XenMobile 10.x en configurant deux adresses IP virtuelles d'équilibrage de charge sur NetScaler, consultez la section Mise en cluster.

Pour de plus amples informations sur la manière de configurer XenMobile 10 Enterprise Edition pour un déploiement de récupération d'urgence (comprend un diagramme d'architecture), consultez le Guide de récupération d'urgence pour XenMobile.

Les sections suivantes décrivent différentes architectures de référence pour le déploiement XenMobile. Vous trouverez des diagrammes d'architecture de référence dans les articles du manuel de déploiement XenMobile, Reference Architecture for On-Premises Deployments et Reference Architecture for Cloud Deployments. Pour obtenir une liste complète des ports, consultez la section Configuration requise pour les ports.

Mode de gestion de la flotte mobile (MDM)

XenMobile MDM Edition permet de gérer les appareils mobiles pour iOS, Android, Amazon et Windows Phone (voir Plates-formes prises en charge dans XenMobile 10). Vous déployez XenMobile en mode MDM si vous prévoyez d'utiliser uniquement les fonctionnalités MDM de XenMobile. Par exemple, vous devez gérer un appareil fourni par l'entreprise via MDM afin de déployer des stratégies, des applications et récupérer des inventaires logiciels, de même que pour pouvoir réaliser des actions sur les appareils, telles que l'effacement.

Dans le modèle recommandé, le serveur XenMobile est positionné dans la zone démilitarisée (DMZ) avec un NetScaler Gateway au premier plan (facultatif), ce qui offre une protection renforcée pour XenMobile.

Mode de gestion des applications mobiles (MAM)

MAM prend en charge les appareils iOS et Android, mais pas les appareils Windows Phone (voirPlates-formes prises en charge dans XenMobile). Vous déployez XenMobile en mode MAM (aussi appelé mode MAM exclusif) si vous prévoyez d'utiliser uniquement les fonctionnalités MAM de XenMobile sans que les appareils soient inscrits auprès de MDM. Par exemple, vous souhaitez sécuriser les applications et données sur des appareils mobiles BYO ; vous souhaitez mettre à disposition des applications mobiles d'entreprise tout en ayant la possibilité de les verrouiller ou d'effacer les données des appareils. Les appareils ne peuvent pas être inscrits auprès de MDM.

Dans ce modèle de déploiement, le serveur XenMobile est positionné avec un NetScaler Gateway au premier plan, ce qui offre une protection renforcée pour XenMobile.

Mode MDM+MAM

L'utilisation conjointe des modes MAM et MDM permet de gérer les données et les applications mobiles ainsi que les appareils mobiles iOS, Android, et Windows Phone (voir Plates-formes prises en charge dans XenMobile 10). Vous déployez XenMobile en mode ENT (entreprise) si vous prévoyez d'utiliser les fonctionnalités MDM+MAM de XenMobile. Par exemple, vous souhaitez gérer un appareil fourni par l'entreprise via MDM ; vous souhaitez déployer des stratégies et des applications, récupérer l'inventaire des logiciels et être en mesure d'effacer les appareils. Vous souhaitez également mettre à disposition des applications mobiles d'entreprise tout en ayant la possibilité de les verrouiller ou d'effacer les données des appareils.

Dans le modèle de déploiement recommandé, le serveur XenMobile est positionné dans la zone démilitarisée (DMZ) avec un NetScaler Gateway au premier plan, ce qui offre une protection renforcée pour XenMobile.

XenMobile dans le réseau interne : une autre option de déploiement consiste à positionner le serveur XenMobile dans le réseau interne, plutôt que dans la DMZ. Ce type de déploiement est utilisé si votre stratégie de sécurité autorise uniquement le positionnement d'appliances réseau dans la DMZ. Étant donné que le serveur XenMobile n'est pas dans la DMZ, vous n'avez pas besoin d'ouvrir de ports sur le pare-feu interne pour autoriser l'accès à SQL Server et aux serveurs PKI depuis la DMZ.

Configuration système requise et compatibilité

Mar 31, 2017

Pour de plus amples informations sur la configuration requise et la compatibilité, consultez les articles suivants :

- Compatibilité XenMobile
- Plates-formes prises en charge
- Configuration requise pour les ports
- Capacité à monter en charge
- Système de licences
- Conformité FIPS 140-2
- Langues prises en charge

Pour exécuter XenMobile 10.4, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.5.x ou 7.0) ; pour plus de détails, reportez-vous à XenServer
  - VMware (versions prises en charge : ESXi 5.1 ou ESXi 6.0) ; pour de plus amples informations, voir VMware.
  - Hyper-V (versions prises en charge : Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2) ; pour de plus amples informations, voir Hyper-V
- Processeur double cœur
- Quatre processeurs virtuels
- 8 Go de RAM
- 50 Go d'espace disque

XenMobile version 10.4.x requiert le serveur de licences 11.12.1 Citrix ou version ultérieure.

Configuration requise pour NetScaler Gateway

Pour exécuter NetScaler Gateway avec XenMobile 10.4, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.5 ou 7.0)
  - VMWare (versions prises en charge : ESXi 4.1, ESXi 5.1, ESXi 5.5, ESXi 6.0)
  - Hyper-V (versions prises en charge : Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2)
- Deux processeurs virtuels
- 2 Go de RAM
- 20 Go d'espace disque

Vous devez également être en mesure de communiquer avec Active Directory, ce qui nécessite un compte de service. Vous avez uniquement besoin d'un accès de requête/lecture.

Configuration requise pour la base de données XenMobile 10.4

XenMobile nécessite l'une des bases de données suivantes :

- Microsoft SQL Server

  Le référentiel XenMobile nécessite une base de données Microsoft SQL Server exécutant une des versions prises en charge suivantes (pour de plus amples informations sur les bases de données Microsoft SQL Server, voir Microsoft SQL Server) :

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

XenMobile 10.4 prend en charge les groupes de disponibilité AlwaysOn SQL ainsi que la mise en cluster SQL pour assurer une haute disponibilité de la base de données.

Citrix vous recommande d'utiliser Microsoft SQL à distance.

Remarque : vérifiez que le compte de service du serveur SQL à utiliser sur XenMobile dispose de l'autorisation de rôle DBcreator. Pour de plus amples informations sur les comptes de service SQL Server, consultez les pages suivantes sur le site Microsoft Developer Network (ces liens pointent vers des informations concernant SQL Server 2014. Si vous utilisez une version différente, sélectionnez la version de votre serveur dans la liste **Autres versions** :

Configuration du serveur - Comptes de service

Configurer les comptes de service Windows et les autorisations

Rôles de niveau serveur

- PostgreSQL

  PostgreSQL est inclus avec XenMobile. Vous pouvez l'utiliser localement ou à distance.

  Remarque : toutes les éditions de XenMobile prennent en charge Remote PostgreSQL 9.5.2 et 9.3.11 pour Windows avec les limitations suivantes :

  - Jusqu'à 300 appareils pris en charge

    Utilisez SQL Server localement pour plus de 300 appareils.

  - Mise en cluster non prise en charge

Compatibilité StoreFront

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

Configuration requise par XenMobile 10.4 en matière de serveur de messagerie

XenMobile 10.4 prend en charge les serveurs de messagerie suivants :

- Exchange 2016
- Exchange 2013
- Exchange 2010

Configuration requise pour les ports

Feb 23, 2017

Pour autoriser des appareils et des applications à communiquer avec XenMobile, vous devez ouvrir des ports spécifiques dans vos pare-feu. Les tableaux suivants répertorient les ports qui doivent être ouverts.

Ouverture de ports pour NetScaler Gateway et XenMobile afin de gérer des applications

Vous devez ouvrir les ports suivants pour autoriser les connexions utilisateur à partir de Citrix Secure Hub, Citrix Receiver et NetScaler Gateway Plug-in via NetScaler Gateway vers XenMobile, StoreFront, XenDesktop, XenMobile NetScaler Connector, et vers d'autres ressources du réseau interne telles que les sites Web intranet. Pour plus d'informations sur NetScaler Gateway, consultez la section Configuration des paramètres de votre environnement XenMobile dans la documentation NetScaler Gateway. Pour de plus amples informations sur les adresses IP NetScaler, telles que l'adresse IP NetScaler (NSIP), l'adresse IP du serveur virtuel (VIP) et l'adresse IP de sous-réseau (SNIP), consultez la section Comment NetScaler communique avec les clients et les serveurs dans la documentation NetScaler.

Port TCP	**Description**	**Source**	**Destination**
21 ou 22	Utilisé pour envoyer des packs d'assistance à un serveur FTP ou SCP.	XenMobile	Serveur FTP ou SCP
53 (TCP et UDP)	Utilisé pour les connexions DNS.	NetScaler Gateway XenMobile	Serveur DNS
80	NetScaler Gateway transmet la connexion VPN à ressource du réseau interne via le second pare-feu. Cela se produit généralement si les utilisateurs ouvrent une session à l'aide de NetScaler Gateway Plug-in.	NetScaler Gateway	Sites Web intranet
80 ou 8080 443	Port XML et Secure Ticket Authority (STA) utilisé pour l'énumération, la fonctionnalité de ticket et l'authentification. Citrix recommande d'utiliser le port 443.	Trafic réseau XML de StoreFront et l'Interface Web STA NetScaler Gateway	XenDesktop ou XenApp
123 (TCP et UDP)	Utilisé pour les services NTP (Network Time Protocol).	NetScaler Gateway XenMobile	Serveur NTP

389	Utilisé pour les connexions LDAP non sécurisées.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Microsoft Active Directory
443	Utilisé pour les connexions à StoreFront à partir de Citrix Receiver ou Receiver pour Web vers XenApp et XenDesktop.	Internet	NetScaler Gateway
	Utilisé pour les connexions à XenMobile pour la mise à disposition d'applications Web, mobiles et SaaS.	Internet	NetScaler Gateway
	Utilisé pour la communication des appareils avec le serveur XenMobile	XenMobile	XenMobile
	Utilisé pour les connexions à partir d'appareils mobiles à XenMobile pour l'inscription.	Internet	XenMobile
	Utilisé pour les connexions depuis XenMobile vers XenMobile NetScaler Connector.	XenMobile	XenMobile NetScaler Connector
	Utilisé pour les connexions depuis XenMobile NetScaler Connector vers XenMobile.	XenMobile NetScaler Connector	XenMobile
	Utilisé pour les URL de rappel dans les déploiements sans authentification par certificat.	XenMobile	NetScaler Gateway
514	Utilisé pour les connexions entre XenMobile et un serveur syslog.	XenMobile	Serveur Syslog
636	Utilisé pour les connexions LDAP sécurisées.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Active Directory
1494	Utilisé pour les connexions ICA à des applications Windows dans le réseau interne. Citrix recommande de conserver ce port ouvert.	NetScaler Gateway	XenApp ou XenDesktop

1812	Utilisé pour les connexions RADIUS.	NetScaler Gateway	Serveur d'authentification RADIUS
2598	Utilisé pour les connexions aux applications Windows dans le réseau interne à l'aide de la fiabilité de session. Citrix recommande de conserver ce port ouvert.	NetScaler Gateway	XenApp ou XenDesktop
3268	Utilisé pour les connexions LDAP non sécurisées au Microsoft Global Catalog.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Active Directory
3269	Utilisé pour les connexions LDAP sécurisées au Microsoft Global Catalog.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Active Directory
9080	Utilisé pour le trafic HTTP entre NetScaler et XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
9443	Utilisé pour le trafic HTTPS entre NetScaler et XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
45000 80	Utilisé pour la communication entre deux VM XenMobile lors du déploiement dans un cluster.	XenMobile	XenMobile
8443	Utilisé pour l'inscription, XenMobile Store et la gestion des applications mobiles (MAM).	XenMobile NetScaler Gateway Appareils Internet	XenMobile
4443	Utilisé pour l'accès à la console XenMobile par un administrateur via le navigateur.	Point d'accès (navigateur)	XenMobile
	Utilisé pour le téléchargement des journaux et des packs d'assistance pour tous les nœuds de cluster XenMobile à partir d'un seul nœud.	XenMobile	XenMobile
27000	Port par défaut utilisé pour l'accès au serveur de licences Citrix externe	XenMobile	Serveur de licences Citrix

7279	Port par défaut utilisé pour la libération et l'obtention de licences Citrix.	XenMobile	Démon vendeur Citrix

Ouverture des ports XenMobile pour gérer des appareils

Vous devez ouvrir les ports suivants pour autoriser XenMobile à communiquer dans votre réseau.

Port TCP	Description	Source	Destination
25	Port SMTP par défaut du service de notification XenMobile. Si votre serveur SMTP utilise un port différent, assurez-vous que votre pare-feu ne bloque pas ce port.	XenMobile	Serveur SMTP
80 et 443	Connexion de l'App Store d'entreprise à Apple iTunes App Store (ax.itunes.apple.com), Google Play (doit utiliser 80) ou Windows Phone Store. Utilisé pour la publication d'applications à partir des magasins d'application via Citrix Mobile Self-Serve sur iOS, Secure Hub pour Android, ou Secure Hub pour Windows Phone.	XenMobile	Apple iTunes App Store (ax.itunes.apple.com et *.mzstatic.com) Apple Volume Purchase Program (vpp.itunes.apple.com) Pour Windows Phone : login.live.com et *.notify.windows.com Google Play (play.google.com)
80 ou 443	Utilisé pour les connexions sortantes entre XenMobile et Nexmo SMS Notification Relay.	XenMobile	Serveur Nexmo SMS Relay
389	Utilisé pour les connexions LDAP non sécurisées.	XenMobile	Serveur d'authentification LDAP ou Active Directory
443	Utilisé pour l'inscription et l'installation de l'agent pour Android et Windows Mobile.	Internet	XenMobile
	Utilisé pour l'inscription et l'installation de l'agent pour appareils Android et Windows, la console Web XenMobile et le client d'assistance à distance MDM.	Réseau local interne et WiFi	

1433	Utilisé par défaut pour les connexions à un serveur de base de données distant (facultatif).	XenMobile	SQL Server
2195	Utilisé pour les connexions sortantes Apple Push Notification Service (APNS) à gateway.push.apple.com pour les notifications sur les appareils iOS et la transmission de stratégies aux appareils.	XenMobile	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
2196	Utilisé pour les connexions sortantes APNS à feedback.push.apple.com pour les notifications sur les appareils iOS et la transmission de stratégies aux appareils.		
5223	Utilisé pour les connexions sortantes APNS à partir d'appareils iOS sur les réseaux Wi-Fi sur *.push.apple.com.	Appareils iOS sur les réseaux WiFi	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
8081	Utilisé pour les tunnels applicatifs depuis le client d'assistance à distance MDM (facultatif). La valeur par défaut est 8081.	Client d'assistance à distance	Internet, pour les tunnels applicatifs vers les appareils des utilisateurs (Android et Windows uniquement)
8443	Utilisé pour l'inscription d'appareils iOS et Windows Phone.	Internet Réseau local et Wi-Fi	XenMobile

Exigences en matière de port pour la connectivité au service de détection automatique

La configuration de ce port permet de s'assurer que les appareils Android qui se connectent à partir de Secure Hub pour Android, versions 10.2 et 10.3, peuvent accéder au service de détection automatique (ADS) de Citrix depuis le réseau interne. L'accès au service ADS est important lors du téléchargement de mises à jour de sécurité mises à disposition via ADS.

Remarque : les connexions ADS peuvent ne pas fonctionner avec votre serveur proxy. Dans ce scénario, autorisez la connexion ADS à contourner le serveur proxy.

Les clients souhaitant activer le certificate pinning doivent effectuer ce qui suit :

- **Collecter les certificats du serveur XenMobile et de NetScaler.** Les certificats doivent être au format PEM et doivent être des certificats de clé publique et non de clé privée.
- **Contacter l'assistance Citrix et demander l'activation du certificate pinning.** Lors de cette opération, vous êtes invité à fournir vos certificats.

Les nouvelles améliorations apportées au certificat pinning nécessitent que les appareils se connectent à ADS avant l'inscription de l'appareil. Cela garantit que Secure Hub dispose des dernières informations de sécurité pour l'environnement

dans lequel l'appareil s'inscrit. Secure Hub n'inscrira pas un appareil qui ne peut pas contacter le service ADS. Par conséquent, il est primordial d'autoriser l'accès à ADS dans le réseau interne pour permettre aux appareils de s'inscrire.

Pour autoriser l'accès à ADS pour Secure Hub 10.2 pour Android, ouvrez le port 443 pour les adresses IP et les noms de domaine complets suivants :

Nom de domaine complet	Adresse IP
discovery.mdm.zenprise.com	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
	184.72.219.144
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

Capacité à monter en charge et performances

Feb 23, 2017

Comprendre l'échelle de votre infrastructure XenMobile joue un rôle significatif dans la façon dont vous décidez de déployer et de configurer XenMobile. Cet article contient des données provenant de tests de capacité à monter en charge ainsi que des instructions permettant de déterminer les exigences en matière de performance et de capacité à monter en charge des déploiements d'entreprise XenMobile 10.4 sur site à petite ou grande échelle.

La capacité à monter en charge se définit ici comme la capacité des appareils existants (c-à-dire les appareils déjà inscrits dans le déploiement) à se reconnecter au déploiement en même temps.

- La *capacité à monter en charge* se définit comme le nombre maximal d'appareils inscrits dans le déploiement.
- Le *nombre de connexions* se définit comme le nombre maximal d'appareils existants autorisés à se reconnecter au déploiement.

Les données de cet article sont tirées de tests effectués dans des déploiements allant de 10 000 à 60 000 appareils. Pour les besoins des tests, des appareils mobiles avec des charges de travail connues ont été utilisés.

Tous les tests ont été effectués sur XenMobile Enterprise Edition.

Les tests ont été effectués à l'aide de NetScaler Gateway 7500 (pour les déploiements comptant jusqu'à 10 000 appareils) et NetScaler Gateway 5550 (pour les déploiements comptant plus de 10 000 appareils). Un boîtier NetScaler doté d'une capacité identique ou supérieure est censé produire des performances de capacité à monter en charge identiques ou supérieures.

Ce tableau présente les résultats des tests de capacité à monter en charge :

Capacité à monter en charge	**Jusqu'à 60 000 appareils**	
Nombre de connexions	Taux de reconnexion des utilisateurs existants	Jusqu'à 7 500 appareils par heure
Configuration	NetScaler Gateway	MPX 7500, MPX 5550
	XenMobile Enterprise Edition	Cluster à 5 nœuds du serveur XenMobile
	Base de données	Base de données externe Microsoft SQL Server

Résultats des tests en fonction du nombre d'appareils et de la configuration matérielle

Ce tableau contient les résultats des tests de capacité à monter en charge en fonction du nombre d'appareils et de la configuration matérielle testés.

Nombre d'appareils	10 000	30 000	45 000	60 000
Taux de reconnexion d'appareils existants par heure	833	3 750	5 625	7 500
Serveur XenMobile – mode	Autonome	Cluster	Cluster	Cluster
Serveur XenMobile – cluster	S.O.	3	4	5
Serveur XenMobile – boîtier virtuel	Mémoire = 12 Go de RAM Processeurs virtuels = 4	Mémoire = 16 Go de RAM Processeurs virtuels = 6	Mémoire = 24 Go de RAM Processeurs virtuels = 8	Mémoire = 24 Go de RAM Processeurs virtuels = 8
Active Directory	Mémoire = 8 Go de RAM Processeurs virtuels = 4	Mémoire = 16 Go de RAM Processeurs virtuels = 4	Mémoire = 16 Go de RAM Processeurs virtuels = 4	Mémoire = 16 Go de RAM Processeurs virtuels = 4
Base de données externe Microsoft SQL Server	Mémoire = 32 Go de RAM Processeurs virtuels = 16	Mémoire = 32 Go de RAM Processeurs virtuels = 12	Mémoire = 48 Go de RAM Processeurs virtuels = 4, chacun avec 4 cœurs	Mémoire = 48 Go de RAM Processeurs virtuels = 4, chacun avec 4 cœurs

Pour les déploiements de 45 000 appareils, le serveur SQL Server a été réglé pour augmenter le nombre de threads de travail à 2 000. Pour les déploiements de 60 000 appareils, le serveur SQL Server a été réglé pour augmenter le nombre de threads de travail à 3 000. (Pour de plus amples informations sur la configuration du nombre de threads de travail sur le serveur SQL Server, reportez-vous à l'article Microsoft Configure the max worker threads Server Configuration Option).

Profil de capacité à monter en charge

Ces tableaux présentent le profil de test utilisé pour obtenir les données de cet article :

Configuration d'Active Directory	**Profil utilisé**

Utilisateurs	100 000
Groupes	200 000
Niveaux d'imbrication	5

Configuration du serveur XenMobile	Total	Par utilisateur
Stratégies	20	20
Applications	270	50
Publique	200	0
MDX	50	30
Web & SaaS	20	20
Actions	50	
Groupes de mise à disposition	20	
Groupes Active Directory par groupe de mise à disposition	10	

SQL	
Nombre de bases de données	1

Connexions des appareils et activités applicatives

Ces tests de capacité à monter en charge ont collecté des données sur la capacité des appareils inscrits dans un déploiement à se reconnecter au cours d'une période de 8 heures.

Les tests simulaient un intervalle de reconnexion au cours duquel les nœuds du serveur XenMobile étaient soumis à des charges supérieures à la normale, car les appareils se reconnectant obtiennent toutes les stratégies de sécurité autorisées. Durant les reconnexions, seules les nouvelles stratégies ou les stratégies modifiées sont déployées sur les appareils iOS, ce qui réduit la charge sur les nœuds du serveur XenMobile.

Ces tests utilisaient une combinaison de 50 % d'appareils iOS et 50 % d'appareils Android.

Ces tests supposent que les appareils Android qui se reconnectent ont préalablement reçu des notifications GCM.

Durant la durée du test (8 heures), les activités suivantes liées aux applications se sont produites :

- Secure Hub a été ouvert une fois pour énumérer les applications autorisées
- 2 applications Web SAML ont été ouvertes
- 4 applications MAM ont été téléchargées
- 1 STA a été générée pour être utilisée par Secure Mail
- 240 validations de ticket STA, une pour chaque événement de reconnexion à Secure Mail via un micro VPN, ont été effectuées.

Architecture de référence

Pour accéder à l'architecture de référence des déploiements utilisés dans ces tests de capacité à monter en charge, reportez-vous à la section « Core MAM+MDM Reference Architecture » de l'article Reference Architecture for On-Premises Deployments.

Restrictions et limitations

Tenez compte de ce qui suit lorsque vous consultez les résultats des tests de capacité à monter en charge dans cet article :

- La plate-forme Windows n'a pas été testée.
- La transmission de stratégies a été testée sur les appareils iOS et Android.
- Chaque nœud du serveur XenMobile prend en charge un maximum de 10 000 appareils simultanément.

Système de licences

Feb 23, 2017

XenMobile et NetScaler Gateway requièrent des licences. Pour accéder à une feuille technique répertoriant les fonctionnalités XenMobile disponibles dans chaque édition, consultez ce PDF.

Pour plus d'informations sur le système de licences NetScaler Gateway, consultez la section Système de licences dans la documentation NetScaler Gateway. XenMobile utilise le système de licences Citrix pour gérer les licences. Pour plus d'informations sur le système de licences Citrix, veuillez consulter la section Système de licences Citrix.

Lorsque vous achetez XenMobile, vous recevrez un e-mail de confirmation de commande contenant des instructions pour activer vos licences. Les nouveaux clients doivent s'inscrire à un programme de licence avant de passer commande. Pour plus d'informations sur les modèles de licence et programmes XenMobile, consultez la section Système de licences XenMobile.

Vous devez installer le système de licences Citrix avant de télécharger vos licences XenMobile. Le nom du serveur sur lequel vous avez installé le système de licences Citrix est requis pour générer le fichier de licences. Lorsque vous installez XenMobile, le système de licences Citrix est installé sur le serveur par défaut. Éventuellement, vous pouvez utiliser un déploiement de serveur de licences Citrix existant pour gérer vos licences XenMobile. Pour plus d'informations sur l'installation, le déploiement et la gestion du système de licences Citrix, consultez la section Obtenir une licence pour votre produit.

> ## Remarque
>
> La version XenMobile 10.4.x requiert le serveur de licences Citrix 11.12.1 ou une version ultérieure ; les versions antérieures du serveur de licences ne fonctionnent pas avec XenMobile 10.4.x.

> ## Important
>
> si vous envisagez de mettre en cluster des nœuds ou instances de XenMobile, vous devez utiliser le système de licences Citrix sur un serveur distant.

Citrix vous recommande de conserver des copies locales de tous les fichiers de licences que vous recevez. Lorsque vous enregistrez une copie de sauvegarde du fichier de configuration, elle inclut tous les fichiers de licences. Toutefois, si vous réinstallez XenMobile sans sauvegarder le fichier de configuration, vous aurez besoin des fichiers de licences d'origine.

Considérations sur les licences de XenMobile

En l'absence d'une licence, XenMobile reste pleinement fonctionnel en mode d'évaluation pendant une période de grâce de 30 jours. Ce mode d'évaluation ne peut être utilisé qu'une seule fois, et la période de 30 jours commence à l'installation de XenMobile. L'accès à la console Web XenMobile n'est jamais bloqué, qu'une licence XenMobile valide soit disponible ou non. Dans la console XenMobile, vous pouvez voir combien de jours restent pour votre période d'évaluation.

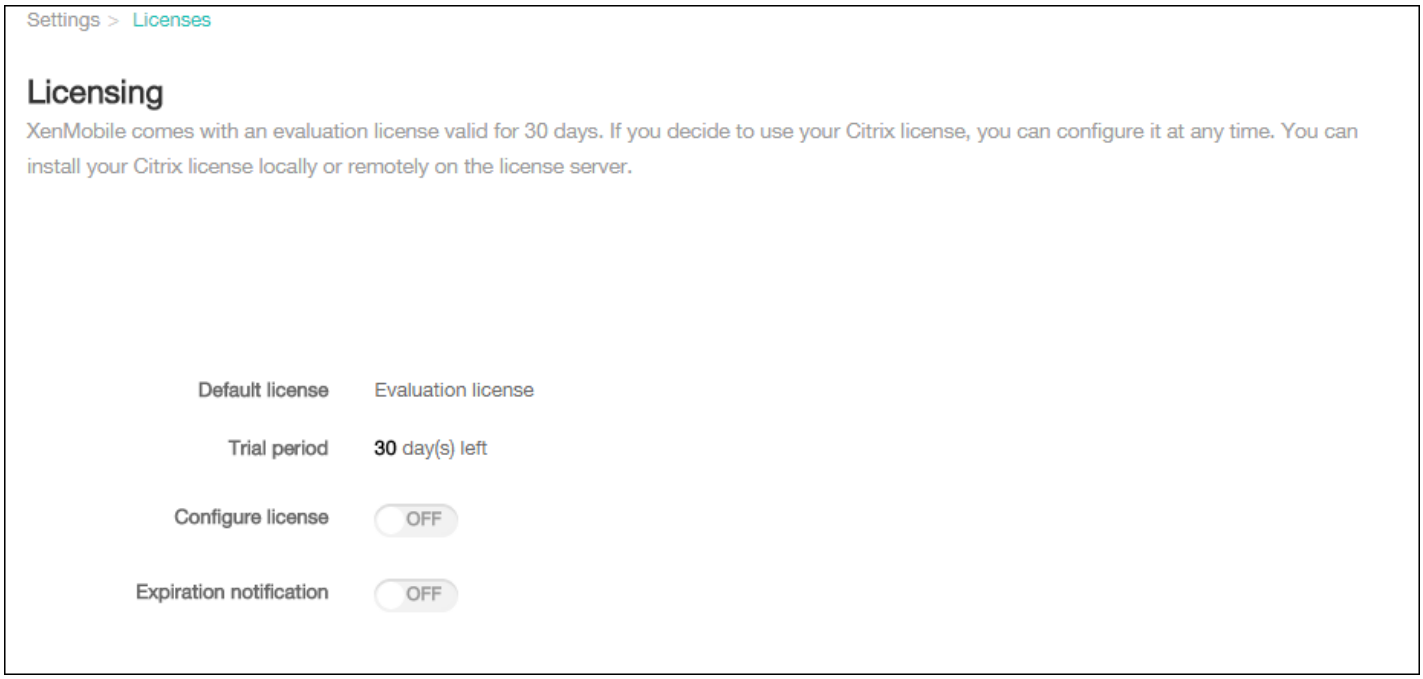
Bien que XenMobile vous permette de charger plusieurs licences, seule une licence peut être activée à la fois.

Lorsqu'une licence XenMobile expire, vous ne pouvez plus exécuter les fonctions de gestion de l'appareil. Par exemple, de nouveaux utilisateurs ou de nouveaux appareils ne peuvent pas être inscrits et les applications et les configurations

déployées sur les appareils inscrits ne peuvent pas être mises à jour. Pour plus d'informations sur les modèles de licence et programmes XenMobile, consultez la section Système de licences XenMobile.

Pour trouver la page Licences sur la console XenMobile

Lorsque la page **Licences** s'affiche pour la première fois après l'installation de XenMobile, la licence est définie par défaut pour le mode d'évaluation de 30 jours et n'est pas encore configurée. Vous pouvez ajouter et configurer des licences sur cette page.



1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Licences**. La page **Licences** s'ouvre.

Pour ajouter une licence locale

Lorsque vous ajoutez de nouvelles licences, elles s'affichent dans le tableau. La première licence ajoutée est automatiquement activée. Si vous ajoutez plusieurs licences de la même catégorie, par exemple, Entreprise et du même type, tel que appareil, ces licences sont affichées dans une seule ligne sur le tableau. Dans ces cas de figure, **Nombre total de licences** et **Nombre utilisé** reflètent le montant cumulé des licences courantes. La date **Expire le** affiche la date d'expiration des licences courantes.

Vous pouvez gérer toutes les licences locales via la console XenMobile.

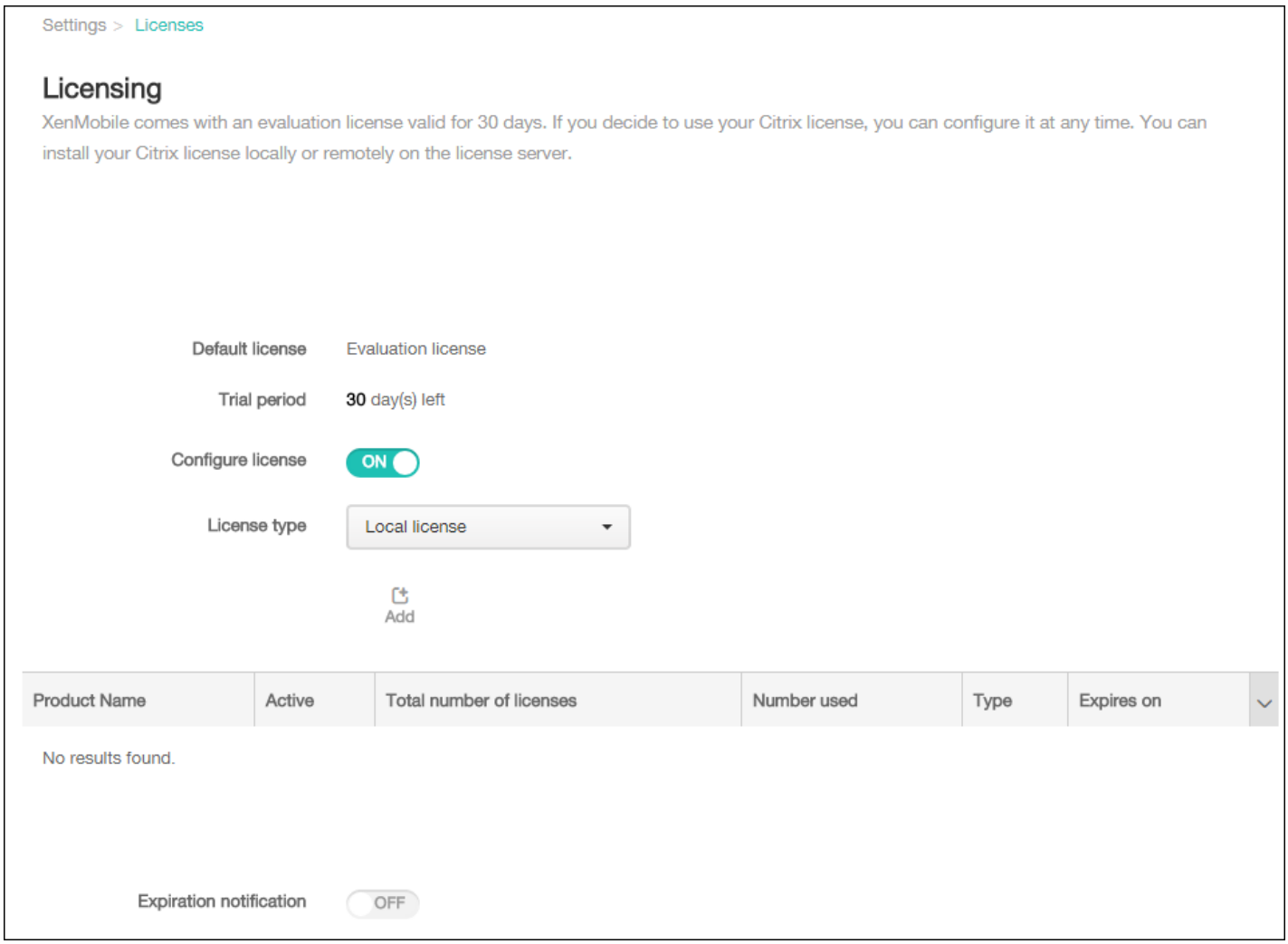
1. Obtenez un fichier de licences à l'aide de Simple License Service, au travers de la console License Administration Console, ou directement à partir de votre compte sur Citrix.com. Pour de plus amples informations, consultez la section Obtention de vos fichiers de licences.

2. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

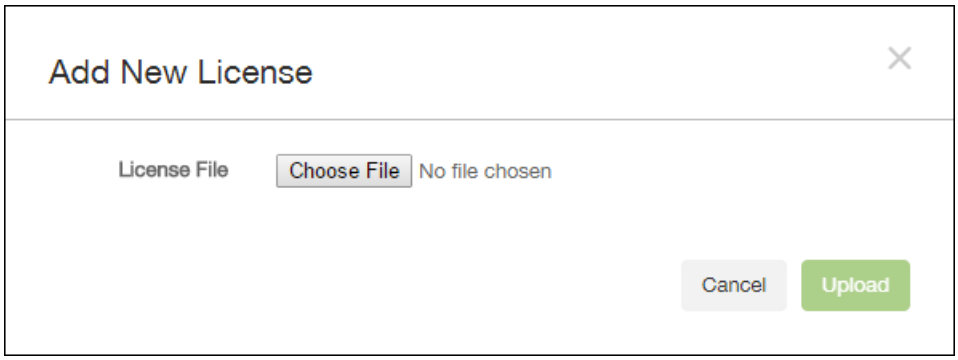
3. Cliquez sur **Licences**. La page **Licences** s'ouvre.

4. Définissez **Configurer licence** sur **On**. La liste **Type de licence**, le bouton **Ajouter**, et le tableau **Licences** apparaissent.

Le tableau **Licences** contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.

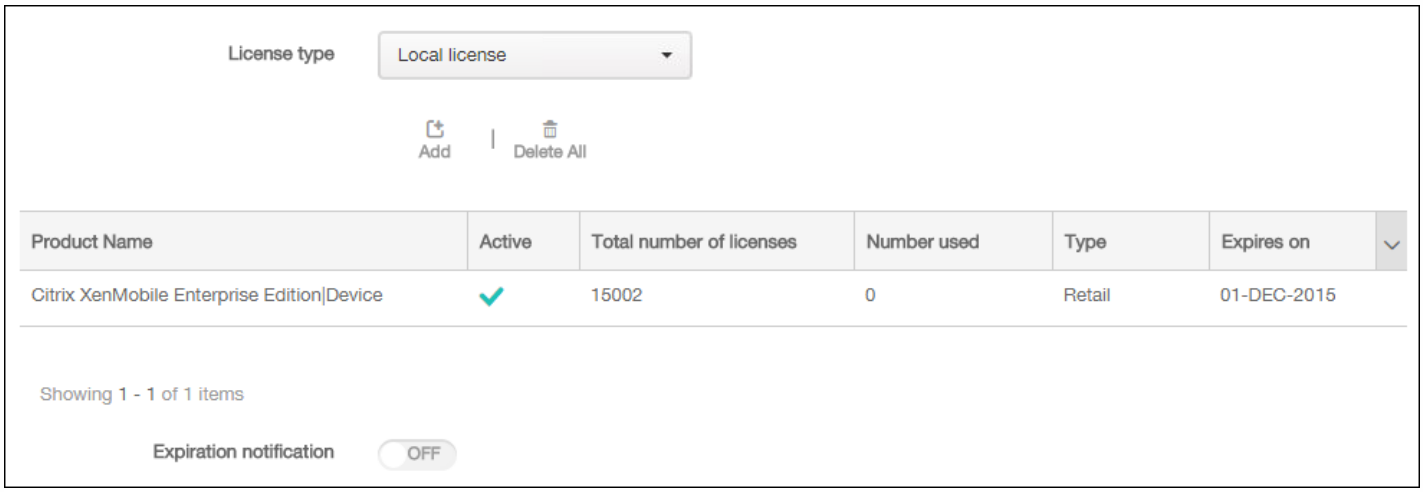


5. Vérifiez que le **type de licence** est défini sur **licence locale**, puis cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle licence** apparaît.



6. Dans la boîte de dialogue **Ajouter une nouvelle licence**, cliquez sur **Choisir un fichier**, puis recherchez l'emplacement de votre fichier de licence.

7. Cliquez sur **Charger**. Les licences sont chargées localement et s'affichent dans le tableau.



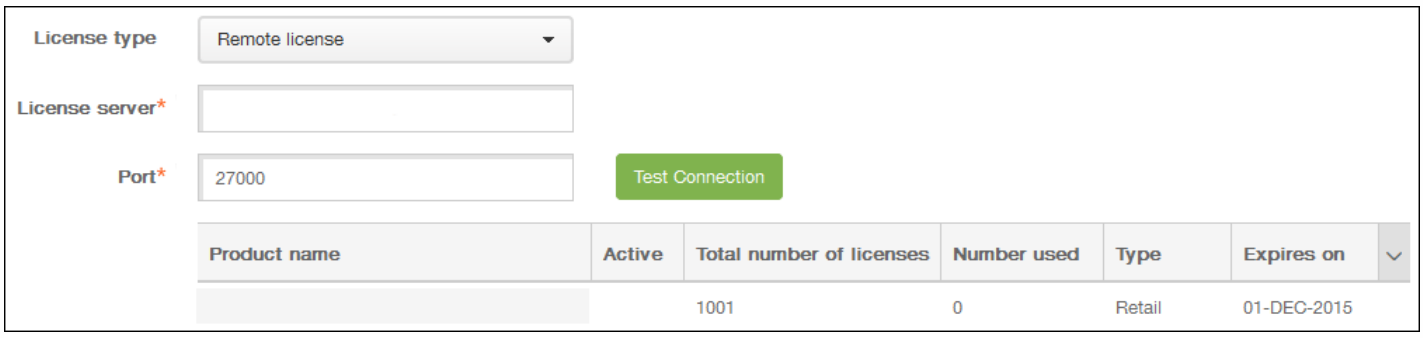
8. Lorsque la licence s'affiche dans le tableau sur la page **Licences**, activez-la. S'il ne s'agit pas de la première licence dans le tableau, la licence est activée automatiquement.

Pour ajouter une licence à distance

Si vous utilisez le serveur de licences Citrix à distance, utilisez le serveur de licences Citrix pour gérer *toutes* les activités liées aux licences. Pour plus de détails, veuillez consulter la rubrique Obtenir une licence pour votre produit.

1. Sur la page **Licences**, définissez **Configurer licence** sur **On**. La liste **Type de licence**, le bouton **Ajouter**, et le tableau **Licences** apparaissent. Le tableau **Licences** contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.

3. Définissez le **type de licence** sur **Licence distante**. Le bouton **Ajouter** est remplacé par les champs **Serveur de licences** et **Port** et le bouton **Tester la connexion**.



4. Configurez les paramètres suivants :

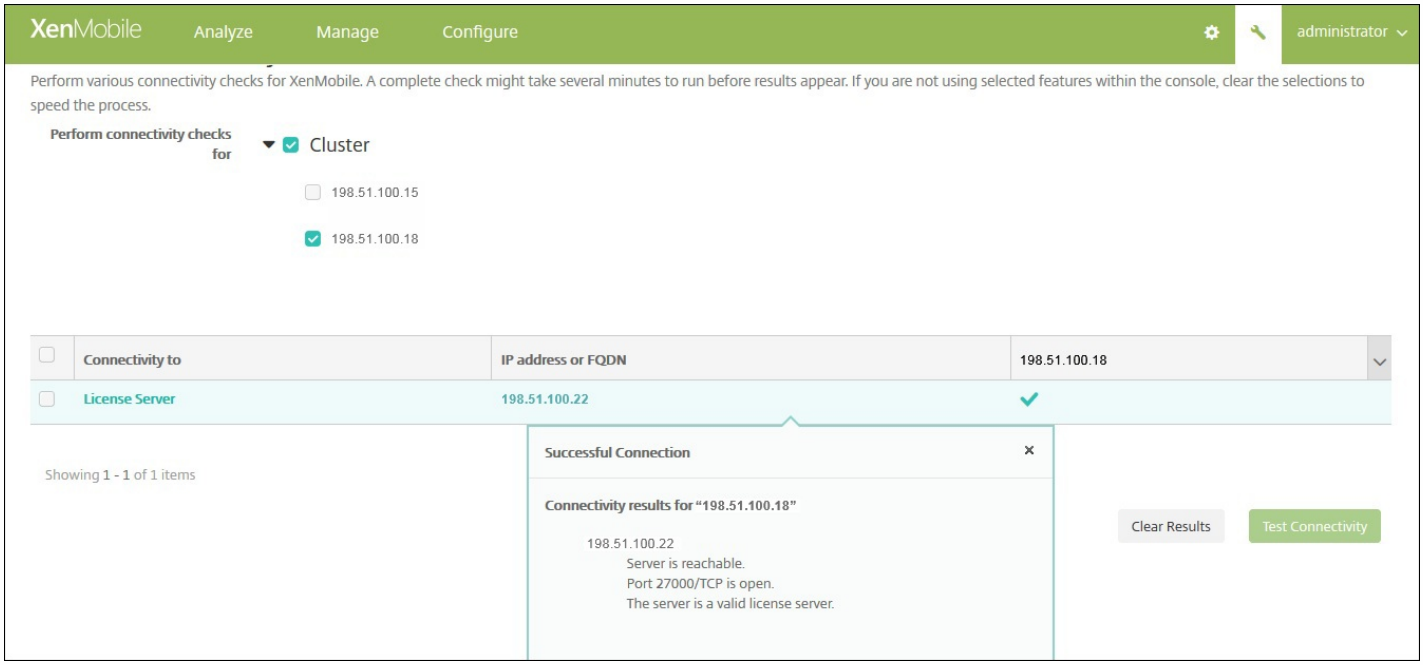
- **Serveur de licences** : entrez l'adresse IP ou le nom de domaine complet (FQDN) de votre serveur de licences distant.
- **Port** : acceptez le port par défaut ou saisissez le numéro de port utilisé pour communiquer avec le serveur de licences.

5. Cliquez sur **Tester la connexion**. Si la connexion est établie, XenMobile se connecte au serveur de licences et le tableau des licences est renseigné avec les licences disponibles. s'il n'existe qu'une seule licence, elle est activée automatiquement.

Lorsque vous cliquez sur **Tester la connexion**, XenMobile vérifie les points suivants :

- XenMobile peut communiquer avec le serveur de licences.
- Les licences sur le serveur de licences sont valides.
- Le serveur de licences est compatible avec XenMobile.

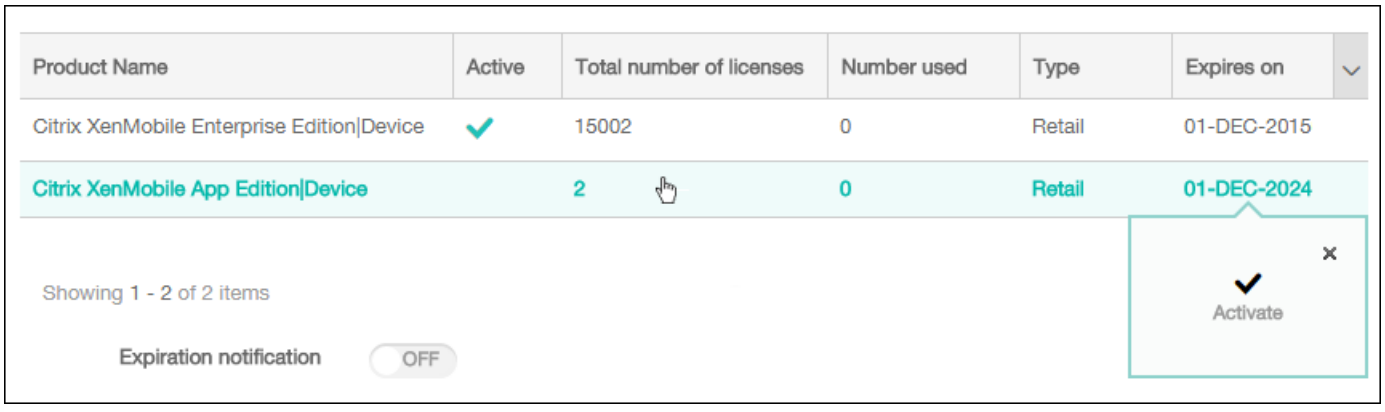
Si la connexion échoue, vérifiez le message d'erreur qui s'affiche, effectuez les corrections nécessaires, puis cliquez sur **Tester la connexion**.



Pour activer une autre licence

Si vous disposez de plusieurs licences, vous pouvez choisir la licence que vous souhaitez activer. Vous ne pouvez disposer que d'une seule licence active à la fois.

1. Sur la page **Licences**, dans le tableau **Licences**, cliquez sur la ligne de la licence que vous souhaitez activer. Une boîte de dialogue de confirmation **Activer** s'affiche à côté de la ligne.



2. Cliquez sur **Activer**. La boîte de dialogue **Activer** s'affiche.

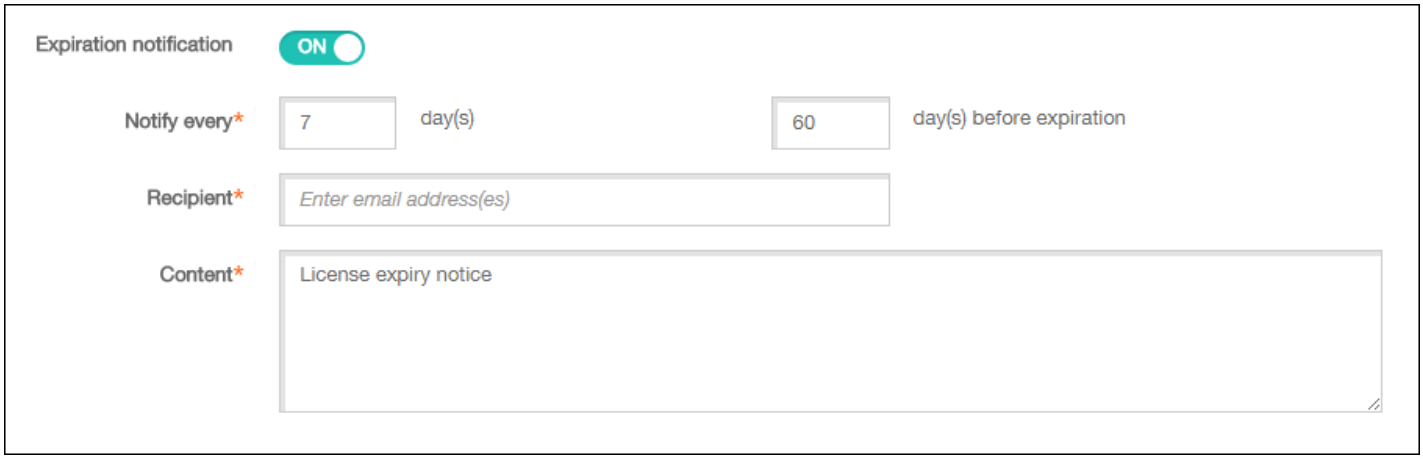
3. Cliquez sur **Activer**. La licence sélectionnée est activée.

> **Important**
>
> si vous activez la licence sélectionnée, la licence actuellement active est désactivée.

Pour automatiser une notification d'expiration

Après avoir activé des licences distantes ou locales, vous pouvez configurer XenMobile pour qu'il vous informe (ou une personne que vous avez désignée) automatiquement lorsque la date d'expiration de la licence approche.

1. Sur la page **Licences**, définissez **Notification d'expiration** sur **On**. Des nouveaux champs liés à la notification apparaissent.



2. Configurez les paramètres suivants :

- **Notifier chaque** : entrez
  - la fréquence à laquelle les notifications sont envoyées, telle que tous les 7 jours.
  - La date à laquelle commencer à envoyer la notification, telle que 60 jours avant l'expiration de la licence.
- **Destinataire** : entrez votre adresse e-mail ou l'adresse e-mail de la personne responsable de la licence.
- **Contenu** : entrez un message de notification d'expiration à l'attention du destinataire.

3. Cliquez sur **Enregistrer**. En se basant sur le nombre de jours avant l'expiration que vous avez défini, XenMobile commence à envoyer des messages contenant le texte que vous avez fourni dans **Contenu** aux destinataires que vous avez spécifiés dans **Destinataire**. Les notifications sont envoyées en fonction de la fréquence que vous avez définie.

Conformité FIPS 140-2

Mar 31, 2017

La norme FIPS (Federal Information Processing Standard), publiée par le US National Institute of Standards and Technologies (NIST), spécifie les exigences de sécurité des modules de chiffrement utilisés dans les systèmes de sécurité. FIPS 140-2 est la seconde version de ce standard. Pour de plus amples informations sur les modules conformes à la norme FIPS 140 validés par le NIST, consultez http://csrc.nist.gov/groupes/STM/cmvp/documents/140-1/140sp/140sp1747.pdf.

Important : la prise en charge de la norme FIPS est uniquement disponible pour les installations sur site du serveur XenMobile. vous pouvez activer le mode XenMobile FIPS uniquement lors de l'installation initiale.
Remarque : la gestion de la flotte mobile XenMobile uniquement, la gestion des applications mobiles XenMobile uniquement et XenMobile Enterprise sont tous conformes à la norme FIPS tant qu'aucune application HDX n'est utilisée.
Toutes les opérations de chiffrement de données au repos et données en transit sur iOS utilisent des modules de chiffrement certifiés FIPS fournis par le OpenSSL et Apple. Sur Android, toutes les opérations de chiffrement de données au repos et données en transit provenant de l'appareil mobile vers NetScaler Gateway utilisent des modules de chiffrement certifiés FIPS fournis par OpenSSL.

Toutes les opérations de chiffrement de données au repos et données en transit pour Mobile Device Management (MDM) sur Windows RT, Microsoft Surface, Windows 8 Pro et Windows Phone 8 utilisent des modules de chiffrement certifiés FIPS fournis par Microsoft.

Toutes les opérations de chiffrement de données au repos et données en transit dans XenMobile Device Manager utilisent des modules de chiffrement certifiés FIPS fournis par OpenSSL. En combinaison avec les opérations cryptographiques décrites ci-dessus pour les appareils mobiles, et entre les appareils mobiles et NetScaler Gateway, toutes les données au repos et données en transit du flux MDM utilisent des modules de chiffrement certifiés FIPS de bout en bout.

Toutes les opérations de chiffrement de données en transit entre appareils mobiles iOS, Android et Windows et NetScaler Gateway utilisent des modules de chiffrement certifiés FIPS. XenMobile utilise un boîtier NetScaler FIPS Edition hébergé dans la DMZ équipé d'un module FIPS certifié pour sécuriser ces données. Pour plus d'informations, veuillez consulter la documentation Netscaler FIPS.

Les applications MDX sont prises en charge sur Windows Phone 8.1 et utilisent des bibliothèques et des API de chiffrement qui sont conformes à la norme FIPS sur Windows Phone 8. Toutes les données au repos pour les applications MDX sur Windows Phone 8.1 et toutes les données en transit entre l'appareil Windows Phone 8.1 et NetScaler Gateway sont cryptées à l'aide de ces bibliothèques et API.

Le MDX Vault chiffre les applications MDX wrappées et les données au repos associées sur les appareils iOS et Android à l'aide des modules cryptographiques certifiés FIPS fournis par OpenSSL.

Pour accéder à la déclaration de conformité FIPS 140-2 complète pour XenMobile, y compris les modules spécifiques utilisés dans chaque cas, contactez votre agent Citrix.

Langues prises en charge

Mar 31, 2017

Les applications XenMobile et la console XenMobile sont conçues pour être utilisées dans des langues autres que l'anglais. Cela inclut la prise en charge les caractères étendus ainsi que les claviers non anglais même lorsque l'application n'est pas traduite dans la langue préférée des utilisateurs. Pour de plus amples informations sur les différents niveaux d'internationalisation de tous les produits Citrix, consultez l'article http://support.citrix.com/article/CTX119253.

Cet article dresse la liste des langues prises en charge dans XenMobile 10.4.

Console XenMobile et le portail en libre-service

- Français
- Allemand
- Coréen
- Portugais
- Chinois simplifié

Applications XenMobile

Un X indique que l'application est disponible dans cette langue. Secure Forms est disponible uniquement en anglais pour le moment.

Remarque : à compter de la version 10.4, les applications mobiles Worx sont renommées applications XenMobile. La plupart des applications XenMobile individuelles ont aussi changé de nom. Pour de plus amples informations, consultez la section À propos des applications XenMobile.

iOS et Android

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japonais	X	X	X	X	X	X
Chinois simplifié	X	X	X	X	X	X
Chinois traditionnel	X	X	X	X	X	X
Français	X	X	X	X	X	X
Allemand	X	X	X	X	X	X
Espagnol	X	X	X	X	X	X

Coréen	X	X	X	X	X	X
Portugais	X	X	X	X	X	X
Néerlandais	X	X	X	X	X	X
Italien	X	X	X	X	X	X
Danois	X	X	X	X	X	X
Suédois	X	X	X	X	X	X
Hébreu	X	X	X	X	X	iOS uniquement
Arabe	X	X	X	X	X	iOS uniquement
Russe	X	X	X	X	X	X

Windows

	Secure Hub	**Secure Mail**	**Secure Web**
Français	X	X	X
Allemand	X	X	X
Espagnol	X	X	X
Italien	X	X	X
Danois	X	X	X
Suédois	X	X	X

Prise en charge des langues de droite à gauche

Le tableau suivant dresse la liste des langues du Moyen-Orient qui sont prises en charge pour chaque application. Un X indique que la fonctionnalité est disponible pour cette plate-forme. La prise en charge des langues de droite à gauche n'est

pas disponible pour les appareils Windows.

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

Installer et configurer

Mar 31, 2017

Avant de commencer :

Vous pouvez utiliser la check-list suivante qui dresse la liste des conditions préalables et des paramètres nécessaires à l'installation de XenMobile. Chaque tâche ou note contient une colonne indiquant la fonction ou le composant pour lesquels la condition s'applique.

De nombreuses considérations sont à prendre en compte lors de la planification d'un déploiement XenMobile. Pour obtenir des conseils, accéder aux questions fréquemment posées et à des cas d'utilisation relatifs à votre environnement XenMobile, consultez le manuel de déploiement de XenMobile.

Vous trouverez la procédure d'installation dans la section Installation de XenMobile plus loin dans cet article.

Checklist de pré-installation

Connectivité réseau de base

Voici les paramètres réseau dont vous avez besoin pour la solution XenMobile.

•	Prérequis ou paramètre	Composant ou fonction	Prendre note du paramètre
	Notez le nom de domaine complet (FQDN) auquel les utilisateurs distants se connectent.	XenMobile NetScaler Gateway	
	Notez les adresses IP locales et publiques. Vous avez besoin de ces adresses IP pour configurer le pare-feu afin de définir la traduction d'adresse réseau (NAT).	XenMobile NetScaler Gateway	
	Notez le masque de sous-réseau.	XenMobile NetScaler Gateway	
	Notez les adresses IP DNS.	XenMobile NetScaler Gateway	
	Notez les adresses IP du serveur WINS (le cas échéant).	NetScaler	

		Gateway	
	Identifiez et prenez note du nom d'hôte de NetScaler Gateway. Remarque : il ne s'agit pas du nom de domaine complet. Le nom de domaine complet est contenu dans le certificat de serveur signé qui est lié au serveur virtuel et auquel les utilisateurs se connectent. Vous pouvez configurer le nom d'hôte à l'aide de l'assistant d'installation dans NetScaler Gateway.	NetScaler Gateway	
	Notez l'adresse IP de XenMobile. Réservez une adresse IP si vous installez une instance de XenMobile. Si vous configurez un cluster, prenez note de toutes les adresses IP dont vous avez besoin.	XenMobile	
	• Une adresse IP publique configurée sur NetScaler Gateway • Une entrée DNS externe pour NetScaler Gateway	NetScaler Gateway	
	Notez l'adresse IP du serveur de proxy Web, le port, la liste d'hôte proxy et le nom d'utilisateur de l'administrateur, ainsi que son mot de passe. Ces paramètres sont facultatifs si vous déployez un serveur proxy dans votre réseau (le cas échéant). Remarque : vous pouvez utiliser le sAMAccountName ou l'UPN lors de la configuration du nom d'utilisateur du proxy Web.	XenMobile NetScaler Gateway	
	Notez l'adresse IP de la passerelle par défaut.	XenMobile NetScaler Gateway	
	Notez l'adresse IP (NSIP) du système et le masque de sous-réseau.	NetScaler Gateway	
	Notez l'adresse IP de sous-réseau (SNIP) et le masque de sous-réseau.	NetScaler Gateway	
	Notez l'adresse IP du serveur virtuel NetScaler Gateway et le nom de domaine complet (FQDN) du certificat. Si vous avez besoin de configurer de multiples serveurs virtuels, notez toutes les adresses IP virtuelles et les noms de domaine complets (FQDN) des certificats.	NetScaler Gateway	
	Notez les réseaux internes auxquels les utilisateurs peuvent accéder via NetScaler	NetScaler	

	Gateway. Exemple : 10.10.0.0/24 Entrez tous les réseaux internes et segments réseau auxquels les utilisateurs doivent accéder lorsqu'ils se connectent avec Secure Hub ou NetScaler Gateway Plug-in lorsque le split tunneling est défini sur Activé.	Gateway	
	Vérifiez que le serveur XenMobile, NetScaler Gateway, le serveur externe Microsoft SQL et le serveur DNS peuvent communiquer entre eux.	XenMobile NetScaler Gateway	

Système de licences

XenMobile nécessite que vous achetiez des options de licences pour NetScaler Gateway et XenMobile. Pour plus d'informations sur le système de licences Citrix, veuillez consulter la section Système de licences Citrix.

•	Configuration requise	Composant	Noter l'emplacement
	Obtenez des licences Universal à partir du site Web de Citrix. Pour plus d'informations, consultez la section Système de licences dans la documentation relative à NetScaler Gateway.	NetScaler Gateway XenMobile Serveur de licences Citrix	

Certificats

XenMobile et NetScaler Gateway nécessitent des certificats pour autoriser les connexions avec d'autres produits et applications Citrix et à partir de machines utilisateur. Pour de plus amples informations, consultez la section Certificats et authentification dans la documentation XenMobile.

✓	Configuration requise	Composant	Remarques
	Obtenez et installez les certificats requis.	XenMobile NetScaler Gateway	

Ports

Vous devez ouvrir les ports pour autoriser la communication avec les composants XenMobile.

✓	Configuration requise	Composant	Remarques

	Ouvrez les ports pour XenMobile	XenMobile NetScaler Gateway	

Base de données

Vous devez configurer une connexion à la base de données. Le référentiel XenMobile nécessite une base de données Microsoft SQL Server exécutant une des versions prises en charge suivantes : Microsoft SQL Server 2014, SQL Server 2012, SQL Server 2008 R2 ou SQL Server 2008. Citrix vous recommande d'utiliser Microsoft SQL à distance. PostgreSQL est inclus avec XenMobile et doit être utilisé localement ou à distance uniquement dans des environnements de test.

•	Configuration requise	Composant	Prendre note du paramètre
	Adresse IP et port du serveur Microsoft SQL. Vérifiez que le compte de service du serveur SQL à utiliser sur XenMobile dispose de l'autorisation de rôle DBcreator.	XenMobile	

Paramètres Active Directory

•	Configuration requise	Composant	Prendre note du paramètre
	Notez l'adresse IP et le port Active Directory pour les serveurs principaux et secondaires. Si vous utilisez le port 636, installez un certificat racine à partir d'une autorité de certification sur XenMobile, puis modifiez l'option Utiliser des connexions sécurisées sur Oui.	XenMobile NetScaler Gateway	
	Notez le nom de domaine Active Directory.	XenMobile NetScaler Gateway	
	Notez le compte de service Active Directory, ce qui requiert un ID utilisateur, un mot de passe et un alias de domaine. Il s'agit du compte utilisé par XenMobile pour interroger Active Directory.	XenMobile NetScaler Gateway	
	Notez le nom unique de l'utilisateur de base. Il s'agit du niveau d'arborescence sous lequel se trouvent les utilisateurs ; par exemple,	XenMobile NetScaler	

	cn=users,dc=ace,dc=com. NetScaler Gateway et XenMobile l'utilisent pour interroger Active Directory.	Gateway	
	Notez le nom unique de base du groupe. Il s'agit du niveau d'arborescence sous lequel se trouvent les groupes. NetScaler Gateway et XenMobile l'utilisent pour interroger Active Directory.	XenMobile NetScaler Gateway	

Connexions entre XenMobile et NetScaler Gateway

	Configuration requise	Composant	Prendre note du paramètre
	Notez le nom d'hôte XenMobile.	XenMobile	
	Notez l'adresse IP ou le nom de domaine complet de XenMobile.	XenMobile	
	Identifiez les applications auxquelles les utilisateurs peuvent accéder.	NetScaler Gateway	
	Notez l'URL de rappel.	XenMobile	

Connexions utilisateur : accès à XenApp, XenDesktop et Citrix Secure Hub

Citrix vous recommande d'utiliser l'assistant de configuration rapide dans NetScaler pour configurer les paramètres de connexion entre XenMobile et NetScaler Gateway et entre XenMobile et Secure Hub. Vous créez un serveur virtuel pour autoriser les connexions utilisateur à partir de Citrix Receiver et de navigateurs Web à se connecter à des applications et des bureaux virtuels Windows dans XenApp et XenDesktop. Citrix vous recommande d'utiliser l'assistant de configuration rapide dans NetScaler pour configurer ces paramètres.

	Configuration requise	Composant	Prendre note du paramètre
	Notez le nom d'hôte de NetScaler Gateway et l'URL externe. L'URL externe est l'adresse Web à laquelle les utilisateurs se connectent.	XenMobile	
	Notez l'URL de rappel de NetScaler Gateway.	XenMobile	
	Notez les adresses IP et les masques de sous-réseau du serveur virtuel.	NetScaler Gateway	

	Notez le chemin d'accès à l'Agent Program Neighborhood ou à un site XenApp Services.	NetScaler Gateway XenMobile	
	Notez le nom de domaine complet ou l'adresse IP du serveur XenApp ou XenDesktop exécutant la Secure Ticket Authority (STA) (pour les connexions ICA uniquement).	NetScaler Gateway	
	Notez le nom de domaine complet public de XenMobile.	NetScaler Gateway	
	Notez le nom de domaine complet public de Secure Hub.	NetScaler Gateway	

Installer XenMobile

La machine virtuelle XenMobile (VM) fonctionne sur Citrix XenServer, VMware ESXi ou Microsoft Hyper-V. Vous pouvez utiliser les consoles de gestion XenCenter ou vSphere pour installer XenMobile.

> ## Remarque
>
> Assurez-vous que l'hyperviseur est configuré avec l'heure correcte, à l'aide d'un serveur NTP ou d'une configuration manuelle, car XenMobile utilise cette heure.

Prérequis XenServer ou VMware ESXi : avant d'installer XenMobile sur XenServer ou VMware ESXi, vous devez effectuer les opérations suivantes. Pour de plus amples informations, reportez-vous à votre documentation XenServer ou VMware.

- Installez XenServer ou VMware ESXi sur un ordinateur doté des ressources matérielles appropriées.
- Installez XenCenter ou vSphere sur un autre ordinateur. L'ordinateur qui héberge XenCenter ou vSphere se connecte à l'hôte XenServer ou VMware ESXi via le réseau.

Prérequis Hyper-V : avant d'installer XenMobile sur Hyper-V, vous devez effectuer les opérations suivantes. Pour plus d'informations, reportez-vous à votre documentation Hyper-V.

- Installez Windows Server 2008 R2, Windows Server 2012 ou Windows Server 2012 R2 avec le rôle Hyper-V activé, sur un ordinateur disposant des ressources système appropriées. Lors de l'installation du rôle Hyper-V, assurez-vous de spécifier les cartes d'interface réseau sur le serveur qui sera utilisé par Hyper-V pour créer les réseaux virtuels. Vous pouvez réserver certaines cartes d'interface réseau pour l'hôte.
- - Supprimez le fichier Virtual Machines/.xml
  - Déplacez le fichier Legacy/.exp dans Virtual Machines

Si vous installez Windows Server 2008 R2 ou Windows Server 2012, effectuez les opérations suivantes :

Ces étapes sont nécessaires, car il y existe deux versions différentes du fichier manifeste Hyper-V représentant la

configuration d'une machine virtuelle (.exp et .xml). Les versions Windows Server 2008 R2 et Windows Server 2012 prennent en charge uniquement les fichiers .exp. Pour ces versions, vous devez uniquement disposer du fichier de manifeste .exp avant l'installation.

Windows Server 2012 R2 ne requiert pas ces étapes supplémentaires.

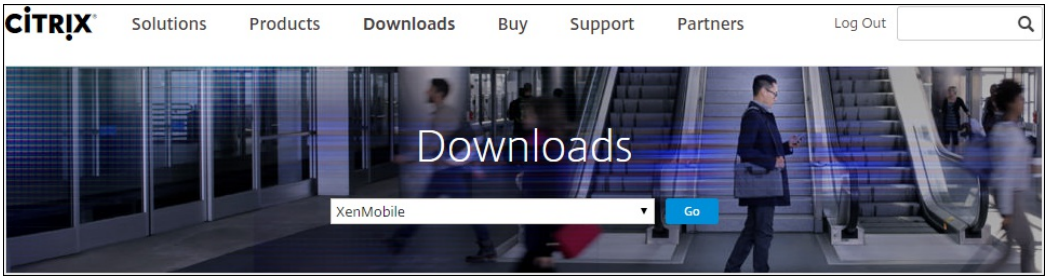
Mode FIPS 140-2 : si vous prévoyez d'installer le serveur XenMobile en mode FIPS, vous devez remplir un certain nombre de conditions préalables, comme abordé dans la section Configuration de FIPS.

Télécharger le logiciel XenMobile

Vous pouvez télécharger le logiciel à partir du site Web de Citrix. Vous devez d'abord ouvrir une session sur le site, puis utiliser le lien Downloads (Téléchargements) sur la page Web de Citrix pour accéder à la page contenant le logiciel que vous voulez télécharger.

Pour télécharger le logiciel pour XenMobile

1. Accédez au site Web Citrix.
2. À côté de la zone de recherche, cliquez sur Log On (Se connecter), puis connectez-vous à votre compte.
3. Cliquez sur l'onglet Downloads(Téléchargements).
4. Sur la page Downloads (Téléchargements), à partir de la liste des produits, cliquez sur XenMobile.



5. Cliquez sur OK (Aller). La page XenMobile s'ouvre.
6. Développez XenMobile 10.
7. Cliquez sur XenMobile 10.0 Server.
8. Sur la page XenMobile 10.0 Server, cliquez sur le bouton Download en regard de l'image virtuelle appropriée pour installer XenMobile sur XenServer, VMware ou Hyper-V.
9. Suivez les instructions affichées à l'écran pour télécharger le logiciel.

Pour télécharger le logiciel pour NetScaler Gateway

Vous pouvez utiliser cette procédure pour télécharger l'appliance virtuelle NetScaler Gateway ou les mises à niveau logicielles de votre appliance NetScaler Gateway existante.

1. Accédez au site Web Citrix.
2. Si vous n'êtes pas déjà connecté au site Web de Citrix, à côté de la zone de recherche, cliquez sur Log On (Se connecter), puis connectez-vous à votre compte.
3. Cliquez sur l'onglet Downloads (Téléchargements).
4. Sur la page Downloads (Téléchargements), à partir de la liste des produits, cliquez sur NetScaler Gateway.
5. Cliquez sur OK (Aller). La page NetScaler Gateway s'affiche.

6. Sur la page NetScaler Gateway, développez la version de NetScaler Gateway que vous exécutez.
7. Sous Firmware, cliquez sur la version du logiciel d'appliance que vous voulez télécharger.
   Remarque : vous pouvez également cliquer sur Virtual Appliances pour télécharger NetScaler VPX. Lorsque vous sélectionnez cette option, vous recevez une liste des logiciels pour la machine virtuelle pour chaque hyperviseur.
8. Cliquez sur la version du logiciel d'appliance que vous voulez télécharger.
9. Sur la page du logiciel d'appliance correspond à la version que vous souhaitez télécharger, cliquez sur le bouton Download de l'appliance virtuelle appropriée.
10. Suivez les instructions affichées à l'écran pour télécharger le logiciel.

Configuration initiale de XenMobile

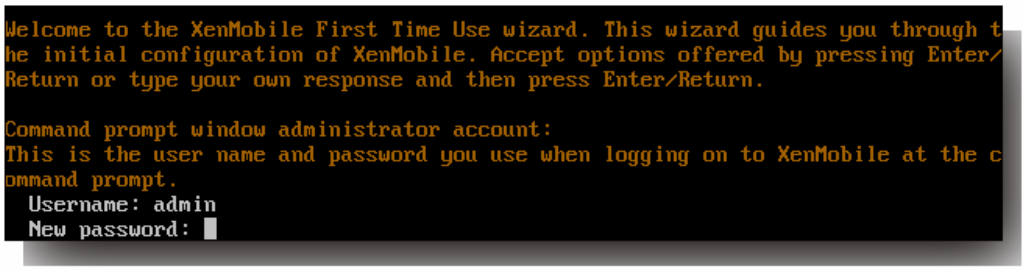
La configuration initiale de XenMobile est un processus en deux parties.

1. Configurez l'adresse IP et le masque de sous-réseau, la passerelle par défaut, les serveurs DNS et plus encore pour XenMobile à l'aide de la console de ligne de commande de XenCenter ou de vSphere.
2. Ouvrez une session sur la console de gestion XenMobile et suivez les étapes des écrans d'ouverture de session.

> **Remarque**
>
> Lorsque vous utilisez un client Web vSphere, il est recommandé de ne pas configurer les propriétés du réseau pendant que vous déployez le modèle OVF sur la page **Customize template**. Dans une configuration à haute disponibilité, cela vous permet d'éviter un problème qui se produit avec l'adresse IP lorsque vous clonez, puis redémarrez la seconde machine virtuelle XenMobile.

Configurer XenMobile dans la fenêtre d'invite de commande

1. Importez la machine virtuelle (VM) XenMobile dans Citrix XenServer, Microsoft Hyper-V ou VMware ESXi. Pour de plus amples informations, consultez la documentation XenServer, Hyper-V ou VMware.
2. Dans votre hyperviseur, sélectionnez la machine virtuelle XenMobile importée et démarrez l'invite de commande. Pour de plus amples informations, consultez la documentation de votre hyperviseur.
3. À partir de la page de la console de l'hyperviseur, créez un compte d'administrateur pour XenMobile dans la fenêtre d'invite de commande en tapant le nom d'utilisateur et le mot de passe d'administrateur.
   Remarque :
   Lorsque vous créez ou modifiez des mots de passe pour le compte d'administrateur dans l'invite de commande, des certificats de serveur PKI et FIPS, XenMobile applique les règles suivantes pour tous les utilisateurs, à l'exception des utilisateurs Active Directory dont les mots de passe sont gérés en dehors de XenMobile :
   - Le mot de passe doit comporter au moins 8 caractères et doit respecter au moins trois des critères de complexité suivants :
     - Majuscules (de A à Z)
     - Minuscules (a à z)
     - Chiffres (de 0 à 9)
     - Caractères spéciaux (par exemple, !, #, $, %)



Remarque : aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe. Rien ne s'affiche.

4. Fournissez les informations de réseau suivantes, puis tapez y pour valider les paramètres :
   1. Adresse IP du serveur XenMobile
   2. Masque réseau
   3. Passerelle par défaut, qui est l'adresse IP de la passerelle par défaut dans la zone démilitarisée (DMZ)
   4. Serveur DNS principal, qui est l'adresse IP du serveur DNS
   5. Serveur DNS secondaire (facultatif)

Remarque : les adresses illustrées dans cette image et les images suivantes ne sont pas réelles et sont fournies uniquement à titre d'exemple.

5. Tapez y pour renforcer la sécurité en générant une phrase secrète de cryptage aléatoire ou n pour fournir votre propre phrase secrète. Citrix vous recommande de taper y pour générer une phrase secrète aléatoire. La phrase secrète est utilisée dans le cadre de la protection des clés de chiffrement utilisées pour sécuriser vos données confidentielles. Un hachage de la phrase secrète, stocké dans le système de fichiers du serveur, est utilisé pour récupérer les clés durant le chiffrement et déchiffrement des données. La phrase secrète ne peut pas être affichée.

   Remarque : si vous souhaitez étendre votre environnement et configurer des serveurs supplémentaires, vous devez fournir votre propre phrase secrète. Il n'est pas possible d'afficher la phrase secrète si vous avez sélectionné une phrase secrète aléatoire.

6. Si vous le souhaitez, vous pouvez activer la norme FIPS (Federal Information Processing Standard). Pour plus de détails sur la norme FIPS, consultez la section FIPS. Vous devez également vous assurer que certaines conditions préalables sont remplies, comme abordé dans la section Configuration de FIPS.

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

7. Fournissez les informations suivantes pour configurer la connexion à la base de données.

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

1. Votre base de données peut être locale ou distante. Tapez l pour locale ou r pour distante.
2. Sélectionnez le type de base de données. Tapez mi pour Microsoft SQL Server ou p pour PostgreSQL.
   Remarque :
   - Citrix vous recommande d'utiliser Microsoft SQL à distance. PostgreSQL est inclus avec XenMobile et doit être utilisé localement ou à distance uniquement dans des environnements de test.
   - La migration de la base de données n'est pas prise en charge. Les bases de données créées dans un environnement de test ne peuvent pas être déplacées dans un environnement de production.
3. Si vous le souhaitez, tapez y pour utiliser l'authentification SSL pour votre base de données.
4. Fournissez le nom de domaine complet (FQDN) du serveur hébergeant XenMobile. Ce serveur hôte fournit à lui seul les services de gestion des appareils et des applications.
5. Entrez le numéro de port de votre base de données s'il est différent du numéro de port par défaut. Le port par défaut de Microsoft SQL Server est 1433 et le port par défaut pour PostgreSQL est 5432.
6. Tapez le nom d'utilisateur d'administrateur de votre base de données.
7. Tapez votre mot de passe d'administrateur de base de données.
8. Tapez le nom de la base de données.
9. Appuyez sur **Entrée** pour valider les paramètres de la base de données.

8. Si vous le souhaitez, tapez y pour activer la mise en cluster des nœuds ou instances XenMobile.

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

Important : si vous activez un cluster XenMobile, une fois la configuration du système terminée, ouvrez le port 80 pour activer les communications en temps réel entre les membres du cluster. Cela doit être effectué sur tous les nœuds du cluster.

9. Tapez le nom de domaine complet (FQDN) du serveur XenMobile.

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

10. Appuyez sur **Entrée** pour valider les paramètres.
11. Identifiez les ports de communication. Pour de plus amples informations sur les ports et leurs utilisations, consultez la section Exigences requises en matière de port.

Remarque : acceptez les ports par défaut en appuyant sur **Entrée** (ou Retour sur un Mac).

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

12. Ignorez la question suivante sur la mise à niveau à partir d'une version précédente de XenMobile, car vous installez XenMobile pour la première fois.
13. Tapez y si vous souhaitez utiliser le même mot de passe pour chaque certificat PKI. Pour plus d'informations sur la fonctionnalité PKI de XenMobile, veuillez consulter la section Chargement de certificats.

```
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:
```

Important : si vous envisagez de mettre en cluster des nœuds ou instances de XenMobile, vous devez fournir les mêmes mots de passe pour chaque nœud.

14. Tapez le nouveau mot de passe, puis retapez-le pour le confirmer.

Remarque : aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe. Rien ne s'affiche.

15. Appuyez sur **Entrée** pour valider les paramètres.
16. Créez un compte d'administrateur pour la connexion à la console XenMobile avec un navigateur Web. Retenez bien ces informations d'identification car vous devrez les réutiliser ultérieurement.

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

Remarque : aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe. Rien ne s'affiche.

17. Appuyez sur **Entrée** pour valider les paramètres. La configuration du système est enregistrée.
18. Lorsque vous êtes invité à indiquer si vous procédez à une mise à niveau, tapez n car il s'agit d'une nouvelle installation.
19. Copiez l'URL complète qui s'affiche sur l'écran et continuez la configuration initiale de XenMobile dans votre navigateur Web.

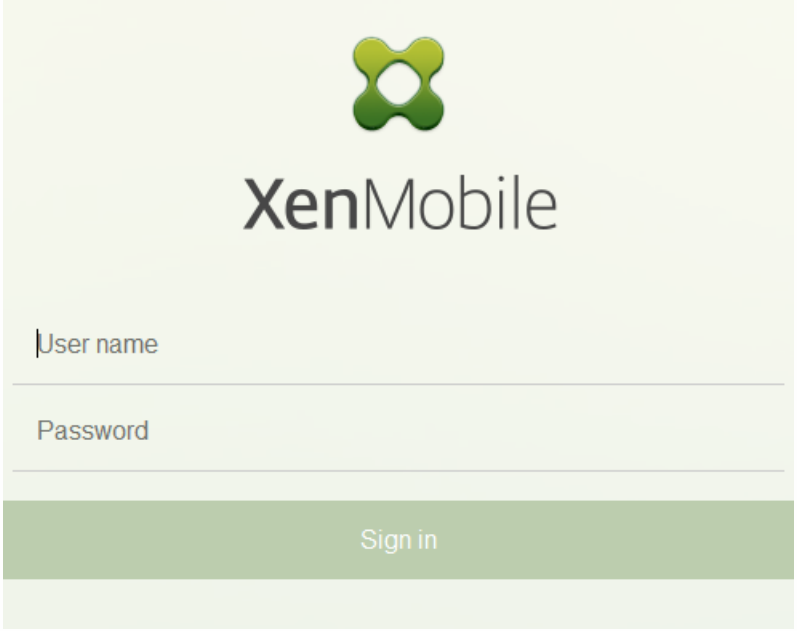
```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

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

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

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

Starting monitoring...                                           [ OK ]
```

Configurer XenMobile dans un navigateur Web

Une fois la première partie de la configuration de XenMobile terminée dans la fenêtre d'invite de commandes de votre hyperviseur, continuez le processus dans votre navigateur Web.

1. Dans votre navigateur Web, accédez à l'emplacement fourni à la fin de la fenêtre d'invite de commandes.

2. Entrez le nom d'utilisateur et le mot de passe du compte administrateur de la console XenMobile console que vous avez créés dans la fenêtre d'invite de commandes.



3. Dans la page Mise en route, cliquez sur Démarrer. La page Licences s'ouvre.
4. Configurez la licence.Si vous ne chargez pas de licence, une licence d'évaluation valide pendant 30 jours sera utilisée. Pour plus d'informations sur l'ajout et la configuration de licences et la configuration de notifications d'expiration, veuillez consulter la section Système de licences.

Important : si vous envisagez d'utiliser la mise en cluster XenMobile en ajoutant des nœuds ou instances de XenMobile, vous devez utiliser le système de licences Citrix sur un serveur distant.
5. Sur la page Certificat, cliquez sur Importer. La boîte de dialogue Importer s'affiche.

6. Importez votre certificat APNS et d'écoute SSL. Si vous gérez des appareils iOS, vous devez disposer d'un certificat APNS. Pour de plus amples informations sur l'utilisation de certificats, consultez la section Certificats.

Remarque : cette étape nécessite le redémarrage du serveur.
7. Si cela est approprié pour l'environnement, configurez NetScaler Gateway. Pour de plus amples informations sur la configuration de NetScaler Gateway, consultez les sections NetScaler Gateway et XenMobile et Configuration des paramètres de votre environnement XenMobile.

Remarque :

- vous pouvez déployer NetScaler Gateway en périphérie du réseau interne de votre organisation (ou intranet) afin d'offrir un point d'accès unique et sécurisé aux serveurs, applications et autres ressources réseau hébergées sur votre réseau interne. Dans ce déploiement, tous les utilisateurs distants doivent se connecter à NetScaler Gateway pour pouvoir accéder aux ressources du réseau interne.

- bien que NetScaler Gateway soit un paramètre facultatif, après la saisie de données sur la page, vous devez effacer ou compléter les champs obligatoires avant de quitter la page.

8. Terminez la configuration LDAP pour accéder aux utilisateurs et groupes à partir d'Active Directory. Pour de plus amples informations sur la configuration de la connexion LDAP, consultez la section Configuration du LDAP.

9. Configurez le serveur de notification de manière à pouvoir envoyer des messages aux utilisateurs. Pour de plus amples informations sur la configuration du serveur de notification, consultez la section Notifications.

Post-requis : redémarrez le serveur XenMobile pour activer vos certificats.

Configurer FIPS avec XenMobile

Feb 23, 2017

Le mode FIPS (Federal Information Processing Standards) dans XenMobile prend en charge les clients du gouvernement fédéral américain en configurant le serveur afin d'utiliser uniquement des annuaires certifiés FIPS 140-2 pour toutes les opérations de cryptage. L'installation de votre serveur XenMobile avec le mode FIPS garantit que toutes les données au repos et en transit, aussi bien pour le client que le serveur XenMobile, sont entièrement conformes à la norme FIPS 140-2.

Avant d'installer un serveur XenMobile en mode FIPS, vous devez remplir les conditions préalables suivantes.

- Vous devez utiliser un SQL Server 2012 ou SQL Server 2014 externe pour la base de données XenMobile. Le SQL Server doit également être configuré pour sécuriser les communications avec SSL. Pour des instructions sur la configuration de communications SSL sécurisées avec SQL Server, consultez la documentation en ligne de SQL Server.
- Les communications SSL sécurisées requièrent l'installation d'un certificat SSL sur votre SQL Server. Le certificat SSL peut être un certificat public provenant d'une autorité de certification commerciale ou un certificat auto-signé provenant d'une autorité de certification interne. Veuillez noter que SQL Server 2014 n'accepte pas les certificats génériques. Citrix vous recommande par conséquent de demander un certificat SSL avec le nom de domaine complet du SQL Server.
- Si vous utilisez un certificat auto-signé pour SQL Server, vous aurez besoin d'une copie du certificat d'autorité de certification racine qui a émis votre certificat auto-signé. Le certificat d'autorité de certification racine doit être importé sur le serveur XenMobile durant l'installation.

Configuration du mode FIPS

Vous pouvez activer le mode FIPS uniquement lors de l'installation initiale du serveur XenMobile. Il n'est pas possible d'activer le mode FIPS une fois l'installation terminée. Par conséquent, si vous envisagez d'utiliser le mode FIPS, vous devez installer le serveur XenMobile avec le mode FIPS dès le début. En outre, si vous disposez d'un cluster XenMobile, le mode FIPS doit être activé sur tous les nœuds du cluster ; un même cluster ne pas contenir un mélange de serveurs XenMobile FIPS et non FIPS.

L'interface de ligne de commande XenMobile contient une option **Toggle FIPS mode** qui n'est pas destinée à être utilisée dans un environnement de production. Cette option est conçue pour les environnements de non production, à des fins de diagnostic et n'est pas prise en charge sur un serveur XenMobile de production.

1. Durant l'installation initiale, activez **FIPS mode**.

2. Chargez le certificat d'autorité de certification racine pour votre SQL Server. Si vous utilisez un certificat SSL auto-signé plutôt qu'un certificat public sur votre SQL Server, choisissez **Yes** pour cette option et effectuez l'une des opérations suivantes :

    a. Copiez et collez le certificat d'autorité de certification.

    b. Importez le certificat d'autorité de certification. Pour importer le certificat d'autorité de certification, vous devez publier le certificat sur un site Web accessible depuis le serveur XenMobile via une URL HTTP. Pour de plus amples informations, consultez la section Importation de certificats plus loin dans cet article.

3. Spécifiez le nom et le port du serveur de votre SQL Server, les informations d'identification permettant de se connecter à SQL Server, et le nom de la base de données à créer pour XenMobile.

Remarque : vous pouvez utiliser au choix une ouverture de session SQL ou un compte Active Directory pour accéder à SQL

Server, mais l'ouverture de session que vous utilisez doit avoir le rôle DBcreator.

4. Pour utiliser un compte Active Directory, entrez les informations d'identification au format domaine\nomutilisateur.

5. Une fois ces étapes terminées, procédez à l'installation initiale de XenMobile.

Pour confirmer que le mode FIPS est opérationnel, ouvrez une session sur l'interface de ligne de commande XenMobile. La phrase **In FIPS Compliant Mode** s'affiche dans la bannière d'ouverture de session.

Importation de certificats

La procédure suivante décrit comment configurer FIPS sur XenMobile en important le certificat, ce qui est requis lorsque vous utilisez un hyperviseur VMware.

Configuration SQL requise

1. La connexion à l'instance SQL à partir de XenMobile doit être sécurisée et doit être SQL Server version 2012 ou SQL Server 2014. Pour sécuriser la connexion, consultez la section Comment faire pour activer le chiffrement SSL pour une instance de SQL Server à l'aide de la console MMC.

2. Si le service ne redémarre pas correctement, vérifiez ce qui suit : ouvrez **Services.msc**.

   a. Copiez les informations du compte d'ouverture de session utilisées pour le service SQL Server.

   b. Ouvrez MMC.exe sur le SQL Server.

   c. Accédez à **Fichier** > **Ajouter/Supprimer un composant logiciel enfichable** et double-cliquez sur les certificats pour ajouter le composant logiciel enfichable Certificats. Sélectionnez le compte d'ordinateur et l'ordinateur local dans les deux pages de l'assistant.

   d. Cliquez sur **OK**.

   e. Développez **Certificats (ordinateur local)** > **Personnel** > **Certificats** et localisez le certificat SSL importé.

   f. Cliquez avec le bouton droit sur le certificat importé (sélectionné dans le Gestionnaire de configuration SQL Server) et cliquez sur **Toutes les tâches** > **Gérer les clés privées**.

   g. Sous **Noms de groupes ou d'utilisateurs**, cliquez sur **Ajouter**.

   h. Entrez le nom de compte du service SQL que vous avez copié dans l'étape précédente.

   i. Décochez l'option **Autoriser Contrôle total**. Par défaut, les autorisations Contrôle totale et Lecture seront accordées au compte de service, toutefois il a seulement besoin de pouvoir lire la clé privée.

   j. Fermez la console **MMC** et démarrez le service SQL.

3. Assurez-vous que le service SQL est démarré correctement.

Conditions requises par les services Internet (IIS)

1. Téléchargez le certificat racine (base 64).

2. Copiez le certificat racine sur le site par défaut sur le serveur IIS, C:\inetpub\wwwroot.

3. Cochez la case **Authentification** du site par défaut.

4. Définissez **Anonyme** sur **Activé**.

5. Sélectionnez la case à cocher des règles **Échec de la demande de suivi**.

6. Assurez-vous que .cer n'est pas bloqué.

7. Accédez à l'emplacement du .cer dans un navigateur Internet Explorer à partir d'un serveur local, http://localhost/certname.cer. Le texte du certificat racine devrait apparaître dans le navigateur.

8. Si le certificat racine ne s'affiche pas dans le navigateur Internet Explorer, assurez-vous que sure ASP est activé sur le serveur IIS comme suit.

   a. Ouvrez le Gestionnaire de serveur**.**

   b. Accédez à l'assistant sous **Gérer** > **Ajouter des rôles et fonctionnalités**.

   c. Dans les rôles de serveur, développez **Serveur Web (IIS)**, développez **Serveur Web**, développez **Développement d'applications** et sélectionnez **ASP**.

   d. Cliquez sur **Suivant** jusqu'à ce que l'installation soit terminée.

9. Ouvrez Internet Explorer et accédez à http://localhost/cert.cer.

Pour de plus amples informations, consultez Internet Information Services (IIS) 8.5.

> **Remarque**
>
> Vous pouvez utiliser l'instance IIS de l'autorité de certification pour cette procédure.

Importation du certificat racine durant la configuration initiale de FIPS

Lorsque vous configurez XenMobile pour la première fois dans la console de ligne de commande, vous devez définir les paramètres suivants pour importer le certificat racine. Pour de plus amples informations sur les étapes d'installation, consultez la section Installation de XenMobile.

- Enable FIPS : Yes
- Upload Root Certificate : Yes
- Copy(c) or Import(i) : i
- Enter HTTP URL to import : http://*nomdomainecomplet du serveur IIS*/cert.cer
- Server : *nomdomainecomplet de SQL Server*
- Port : 1433
- User name : compte de service qui a l'autorisation de créer la base de données (domaine\nomutilisateur).
- Password : mot de passe du compte de service.
- Database Name: nom que vous choisissez librement.

Configurer la mise en cluster

Mar 31, 2017

Dans les versions XenMobile antérieures à la version 10, vous avez configuré Device Manager en tant que cluster et App Controller en tant que paire haute disponibilité. XenMobile 10 intègre XenMobile 9 Device Manager et App Controller. À compter de la version 10, la haute disponibilité n'est plus applicable dans XenMobile. Pour configurer la mise en cluster, par conséquent, vous devez configurer les deux adresses IP virtuelles d'équilibrage de charge suivantes sur NetScaler.

- **Adresse IP virtuelle d'équilibrage de charge MDM** : une adresse IP virtuelle d'équilibrage de charge MDM est requise pour communiquer avec les nœuds XenMobile qui sont configurés dans un cluster. L'équilibrage de charge est effectué en mode pont SSL.
- **Adresse IP virtuelle d'équilibrage de charge MAM** : des adresses IP virtuelles d'équilibrage de charge MAM sont requises pour que NetScaler Gateway communique avec les nœuds XenMobile qui sont configurés dans un cluster. Dans XenMobile 10, par défaut, tout le trafic provenant de NetScaler Gateway est acheminé vers l'adresse IP virtuelle d'équilibrage de charge sur le port 8443.

Le nom de domaine complet (FQDN) de l'adresse IP virtuelle d'équilibrage de charge MDM et des adresses IP virtuelles d'équilibrage de charge MAM est le même que le nom de domaine complet d'inscription, qui est le nom de domaine complet du serveur XenMobile.
Les procédures décrites dans cet article expliquent comment créer une nouvelle machine virtuelle (VM) XenMobile et associer la nouvelle VM à une VM existante, ce qui entraîne la création d'un cluster.

Conditions préalables

- Vous avez entièrement configuré le nœud XenMobile requis.
- Une adresse IP publique pour l'équilibrage de charge MDM.
- Une adresse IP privée, dans une plage définie par la norme RFC 1918, pour l'équilibrage de charge MAM.
- Des certificats de serveur.
- Une adresse IP disponible pour l'adresse IP virtuelle de NetScaler Gateway.

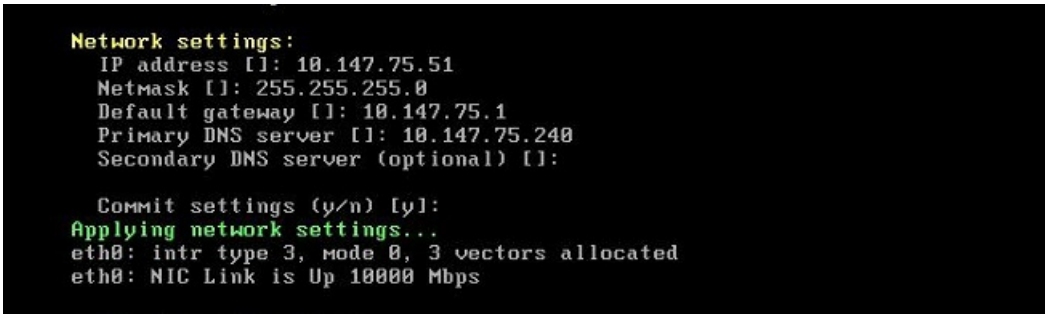
Pour consulter des diagrammes d'architecture de XenMobile 10.x dans des configurations en cluster, reportez-vous à la section Architecture.

Installation des nœuds de cluster XenMobile

En fonction du nombre de nœuds requis, vous pouvez créer de nouvelles VM XenMobile. Pointez la nouvelle VM vers la même base de données et fournissez les mêmes mots de passe de certificat PKI.

1. Ouvrez la console de ligne de commande de la nouvelle VM et entrez le nouveau mot de passe pour le compte d'administrateur.

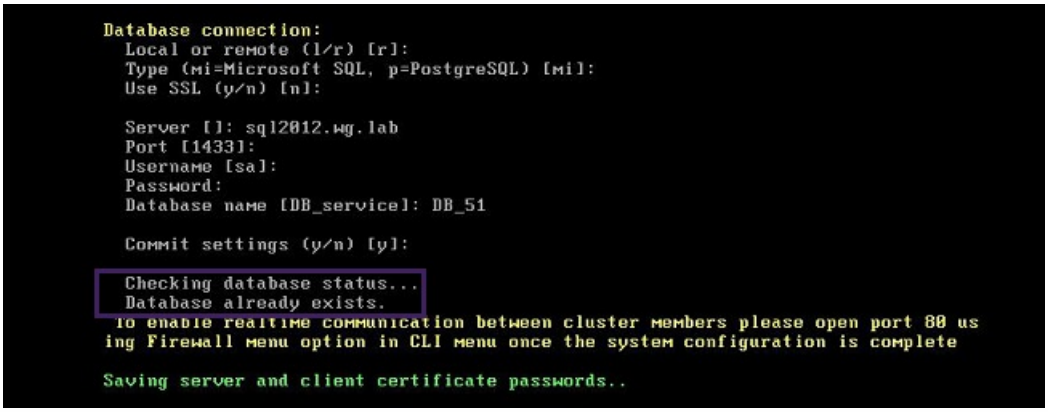
2. Fournissez les informations de configuration du réseau, comme illustré dans la figure suivante.



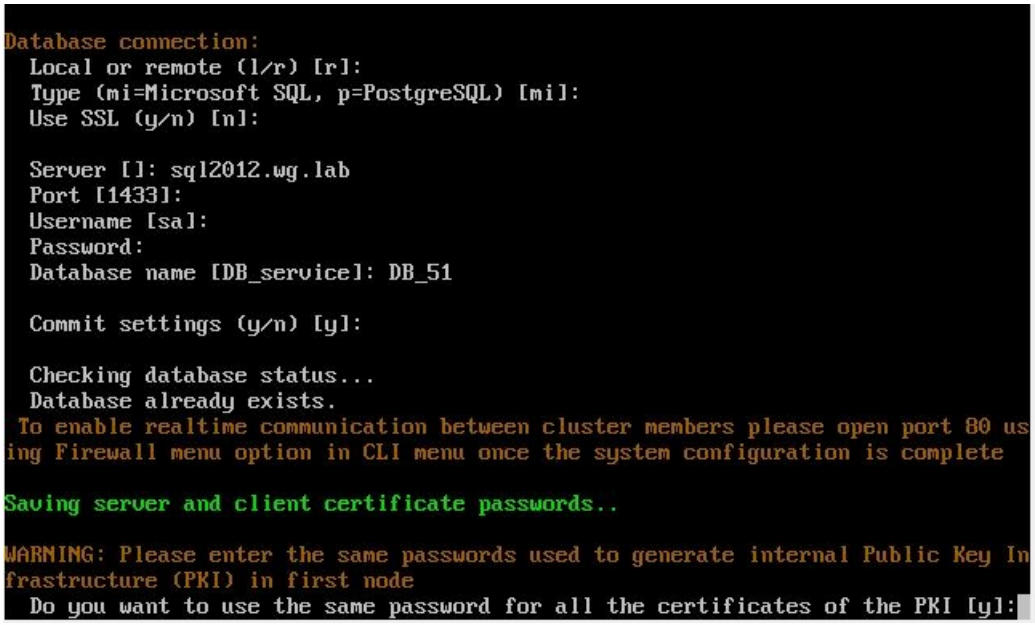
3. Si vous souhaitez utiliser le mot de passe par défaut pour la protection des données, tapez y ; ou tapez n et entrez le nouveau mot de passe.

4. Si vous souhaitez utiliser la norme FIPS, tapez y, sinon tapez n.

5. Configurez la base de données en pointant vers la base de données vers laquelle pointait la VM entièrement configurée auparavant. Le message suivant s'affiche : La base de données existe déjà.

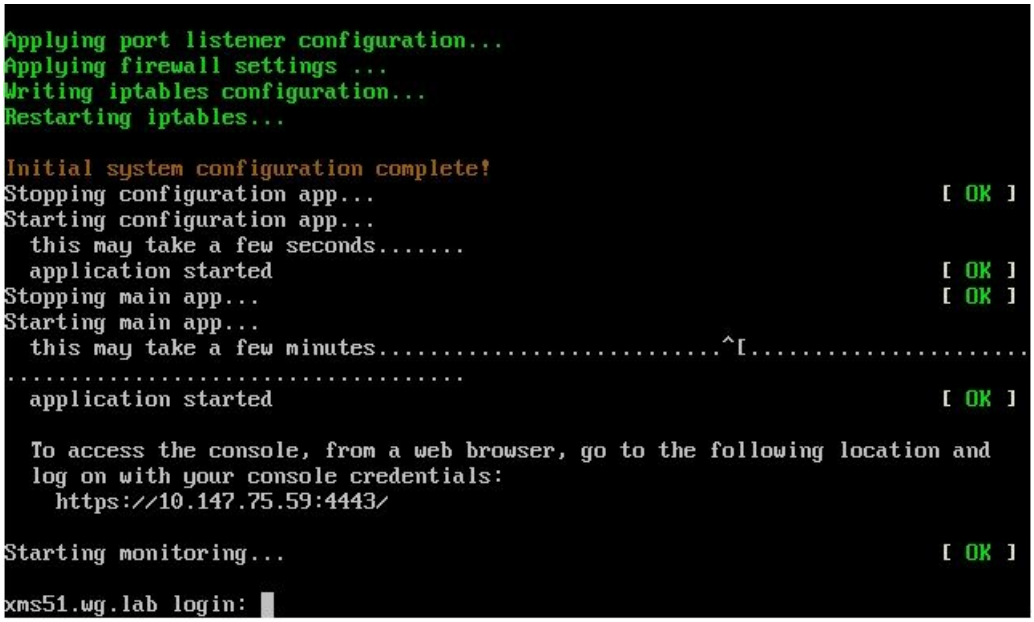


6. Entrez les mots de passe que vous avez spécifiés pour les certificats pour la première VM.



Une fois que vous avez entré le mot de passe, la configuration initiale sur le second nœud se termine.

7. Une fois la configuration terminée, le serveur redémarre et la boîte de dialogue d'ouverture de session s'affiche.



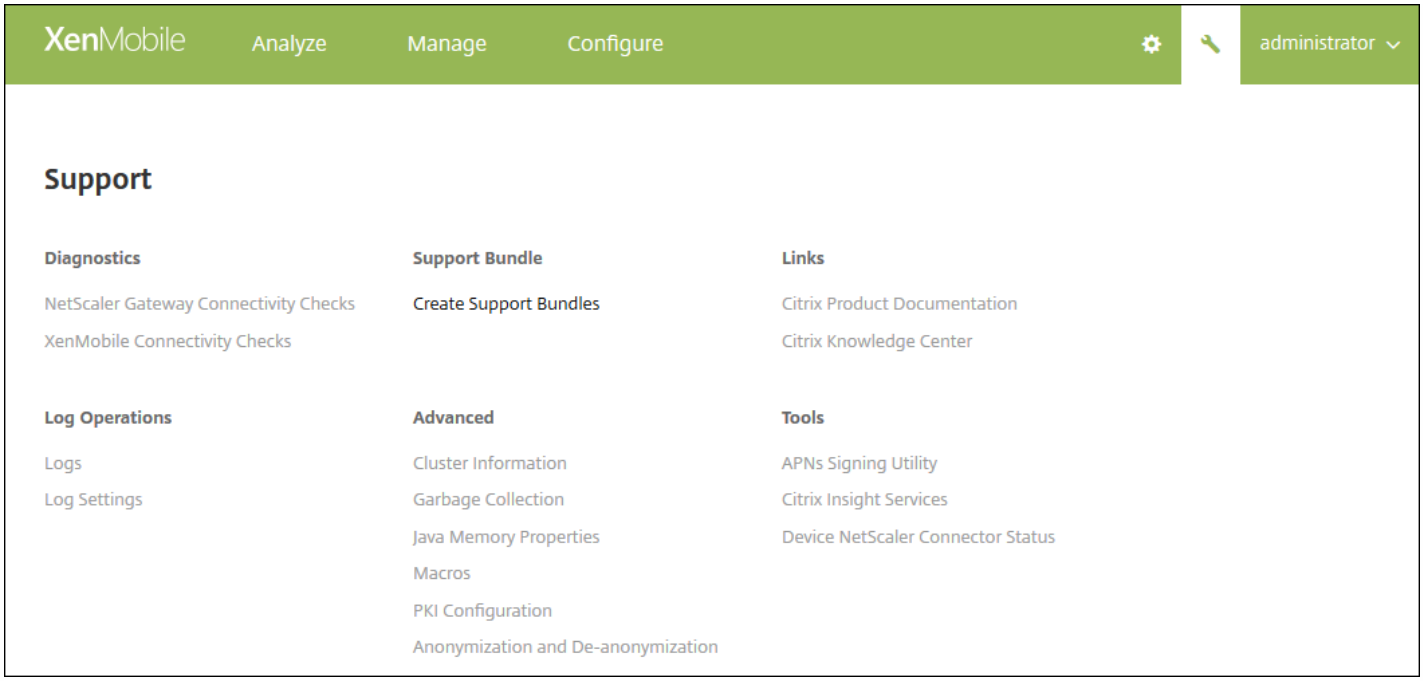
Remarque : la boîte de dialogue d'ouverture de session est identique à la boîte de dialogue d'ouverture de session de la première VM. Cette correspondance vous permet de vérifier que les deux VM utilisent le même serveur de base de données.

8. Utilisez le nom de domaine complet (FQDN) de XenMobile pour ouvrir la console XenMobile dans un navigateur Web.

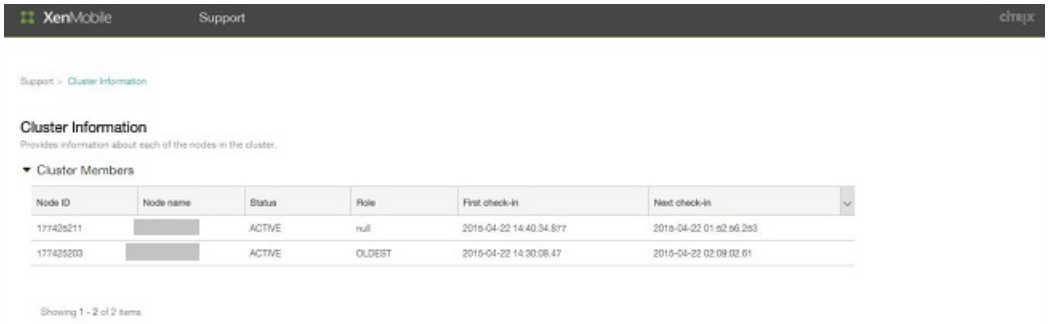
9.Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit.

La page **Support** s'ouvre.

10. Sous **Avancé**, cliquez sur **Informations de cluster**.



Toutes les informations sur le cluster, y compris les membres du cluster, les informations de connexion, les tâches, etc., s'affichent. Le nouveau nœud est maintenant membre du cluster.



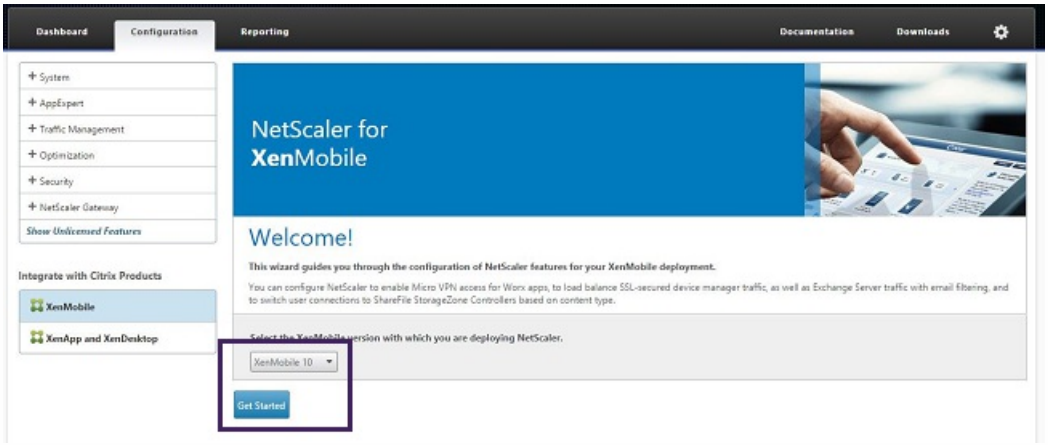
Vous pouvez ajouter d'autres nœuds en suivant les étapes suivantes. Le premier cluster ajouté au nœud a le rôle **PLUS ANCIEN**. Les clusters ajoutés après afficheront un rôle **AUCUN** ou **null**.

Pour configurer l'équilibrage de charge pour le cluster XenMobile dans NetScaler

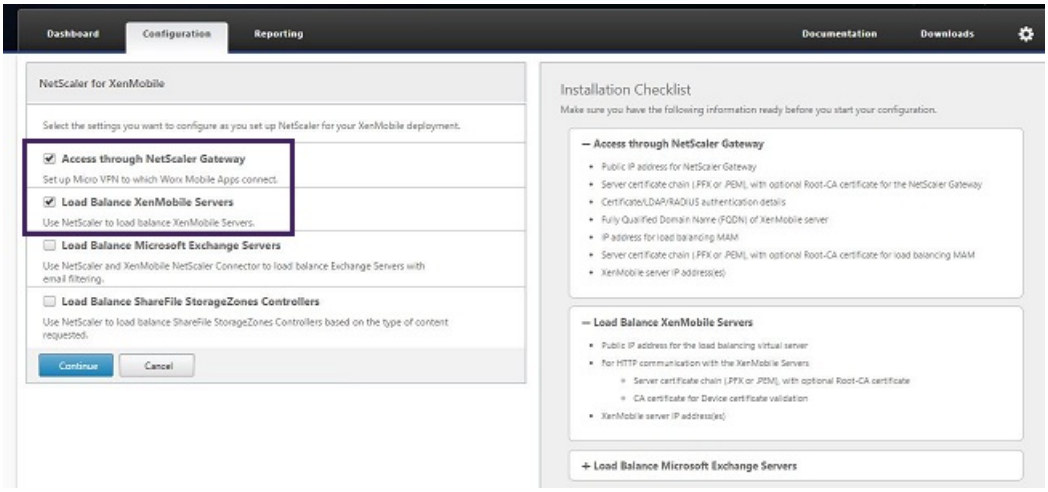
Après avoir ajouté des nœuds en tant que membres du cluster XenMobile, vous avez besoin d'équilibrer la charge des nœuds pour être en mesure d'accéder aux clusters. L'équilibrage de charge est réalisé en exécutant l'assistant XenMobile disponible dans NetScaler 10.5.x. Vous pouvez suivre les étapes de cette procédure pour effectuer l'équilibrage de charge de XenMobile en exécutant l'assistant.

1. Ouvrez une session sur NetScaler.

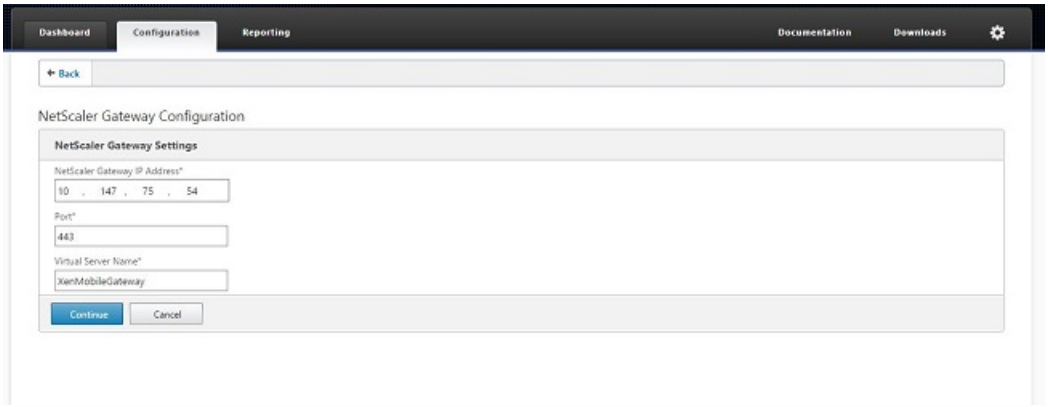
2. Sur l'onglet Configuration, cliquez sur XenMobile, puis sur Get Started.



3. Sélectionnez les cases à cocher Access through NetScaler Gateway et Load Balance XenMobile Servers, puis cliquez sur Continue.

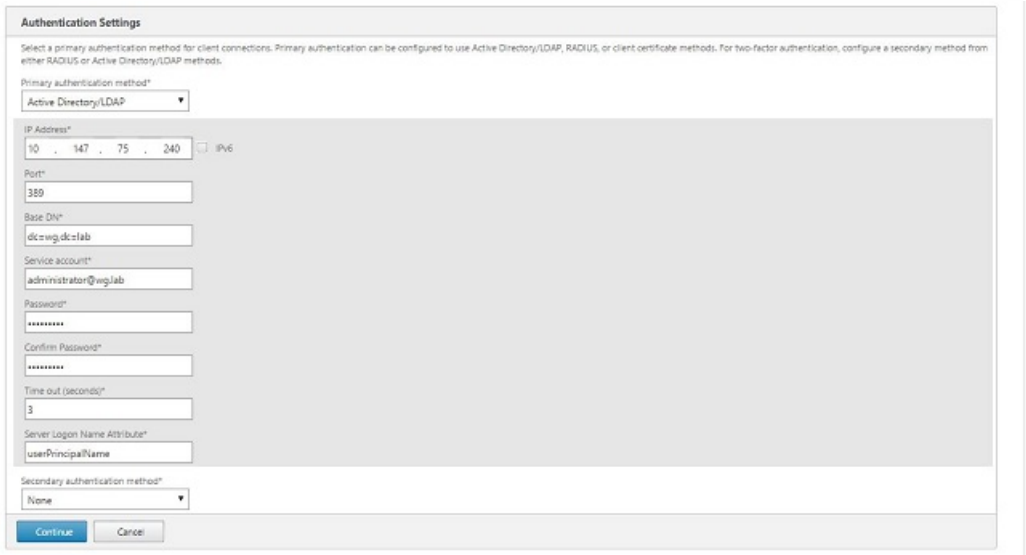


4. Entrez l'adresse IP pour NetScaler Gateway et cliquez sur Continue.

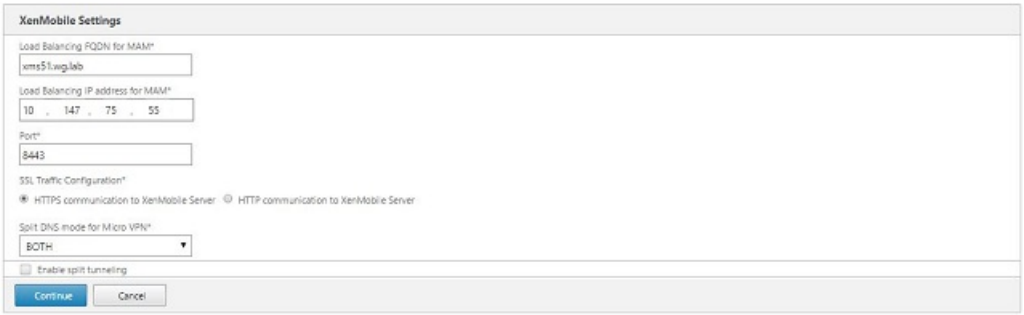


5. Liez le certificat de serveur à l'adresse IP virtuelle de NetScaler Gateway en effectuant l'une des opérations suivantes, puis cliquez sur Continue.
   - Dans Use existing certificate, sélectionnez le certificat de serveur dans la liste.
   - Cliquez sur l'onglet Install Certificate pour charger un nouveau certificat de serveur.

6. Entrez les détails du serveur d'authentification, puis cliquez sur Continue.



   Remarque : assurez-vous que l'attribut Server Logon Name Attribute correspond à celui que vous avez fourni dans la configuration LDAP de XenMobile.
7. Sous XenMobile settings, entrez une valeur pour Load Balancing FQDN for MAM, puis cliquez sur Continue.

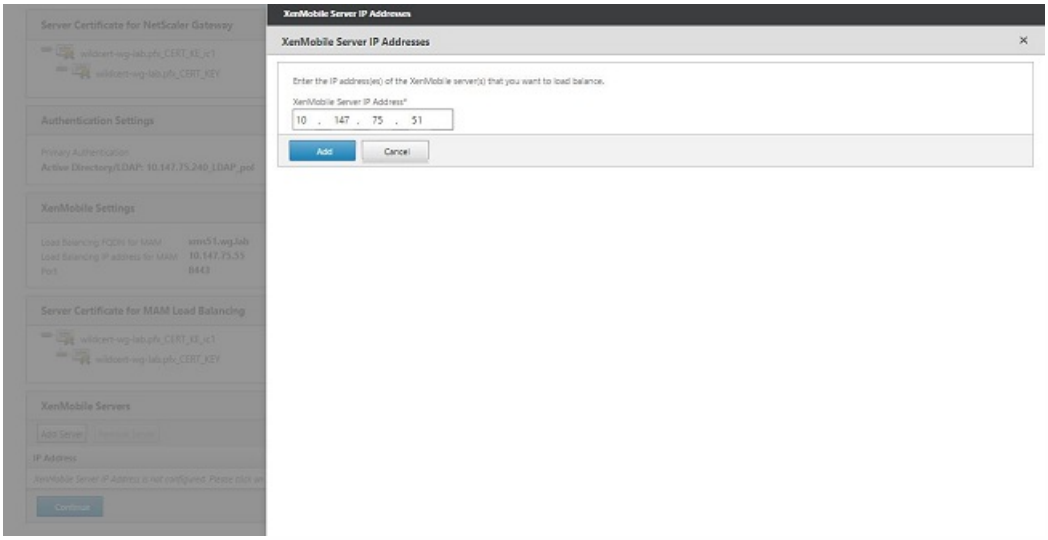


Remarque : assurez-vous que le nom de domaine complet de l'adresse IP virtuelle d'équilibrage de charge MAM et le nom de domaine complet de XenMobile sont les mêmes.

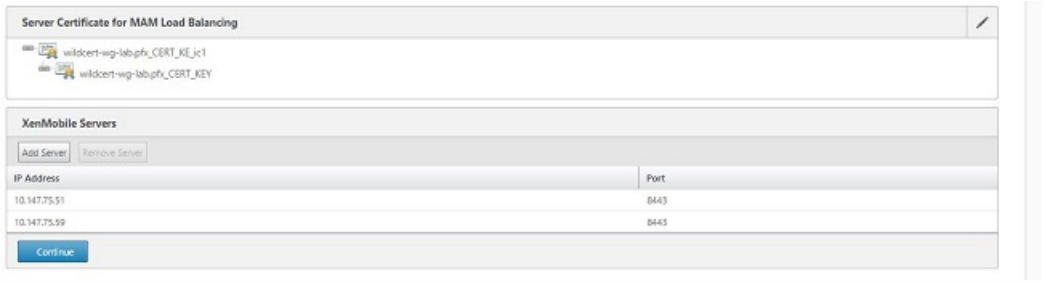
8. Si vous souhaitez utiliser le mode pont SSL (HTTPS), sélectionnez HTTPS communication to XenMobile Server. Toutefois, si vous souhaitez utiliser le déchargement SSL, sélectionnez HTTP communication to XenMobile Server, comme illustré dans la figure précédente. Pour les besoins de cet article, l'option choisie est le mode pont SSL (HTTPS).
9. Liez le certificat de serveur pour l'adresse IP virtuelle d'équilibrage de charge MAM, puis cliquez sur Continue.

10. Sous XenMobile Servers, cliquez sur Add Server pour ajouter les nœuds XenMobile.

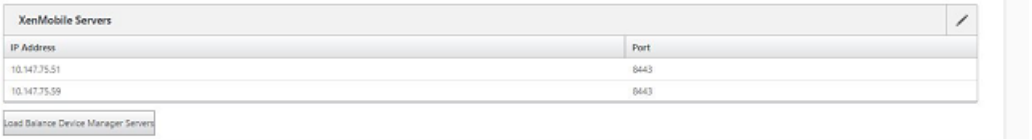
11. Entrez l'adresse IP du nœud XenMobile, puis cliquez sur Add.



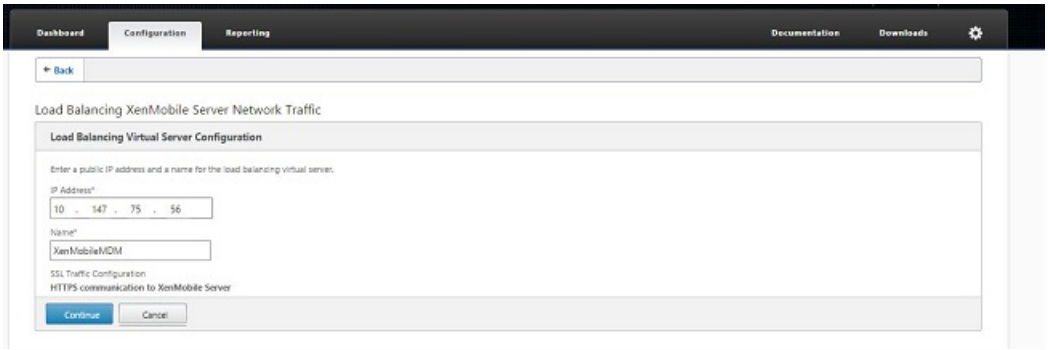
12. Répétez les étapes 10 et 11 pour ajouter d'autres nœuds XenMobile qui font partie du cluster XenMobile. Vous pourrez voir tous les nœuds XenMobile que vous avez ajoutés. Cliquez surContinue.



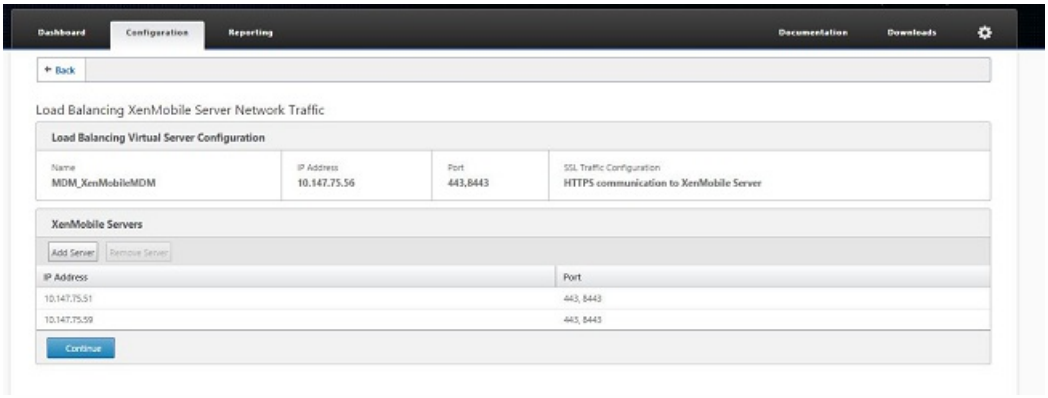
13. Cliquez sur Load Balance Device Manager Servers pour continuer la configuration de l'équilibrage de charge MDM.



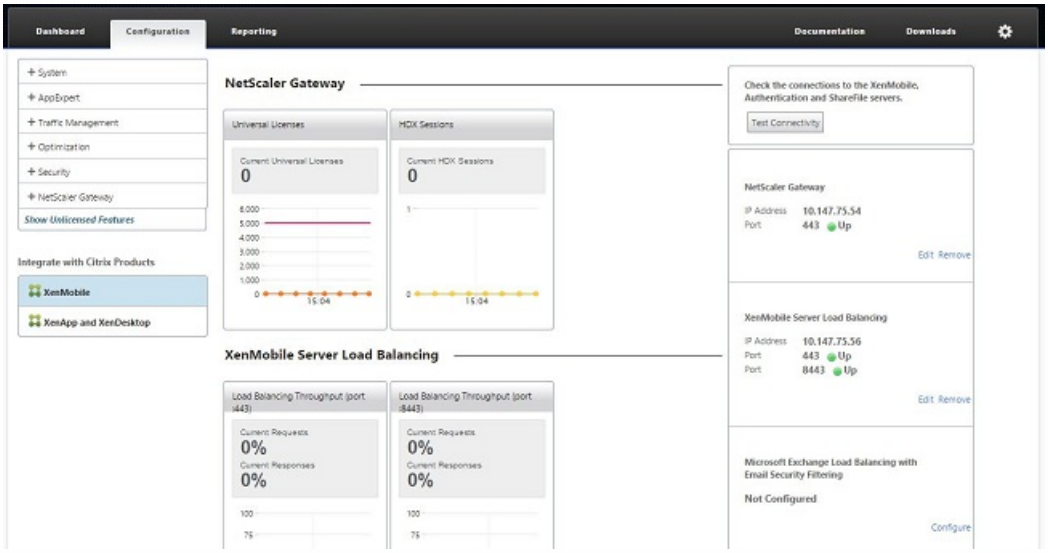
14. Entrez l'adresse IP à utiliser pour l'équilibrage de charge MDM, puis cliquez sur Continue.



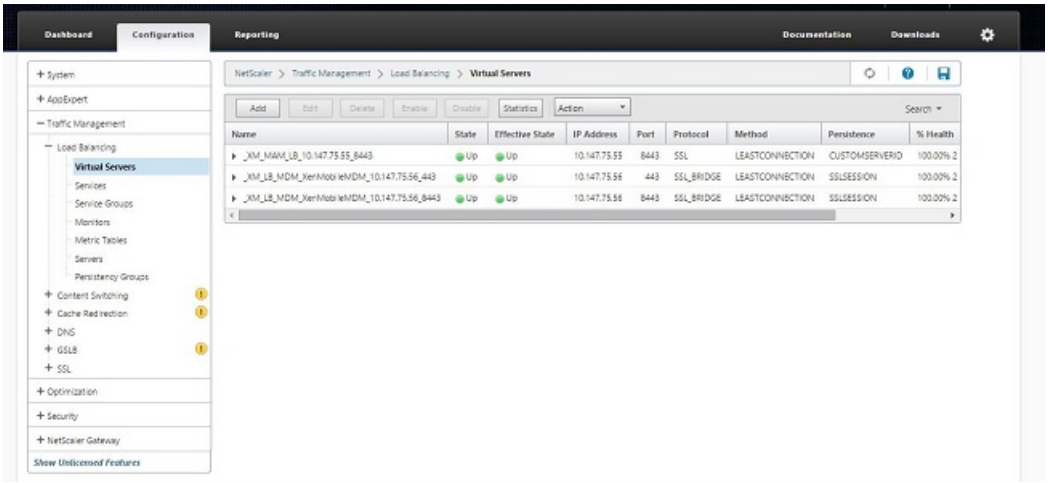
15. Lorsque vous voyez les nœuds XenMobile dans la liste, cliquez sur Continue, puis cliquez sur Done pour terminer le processus.



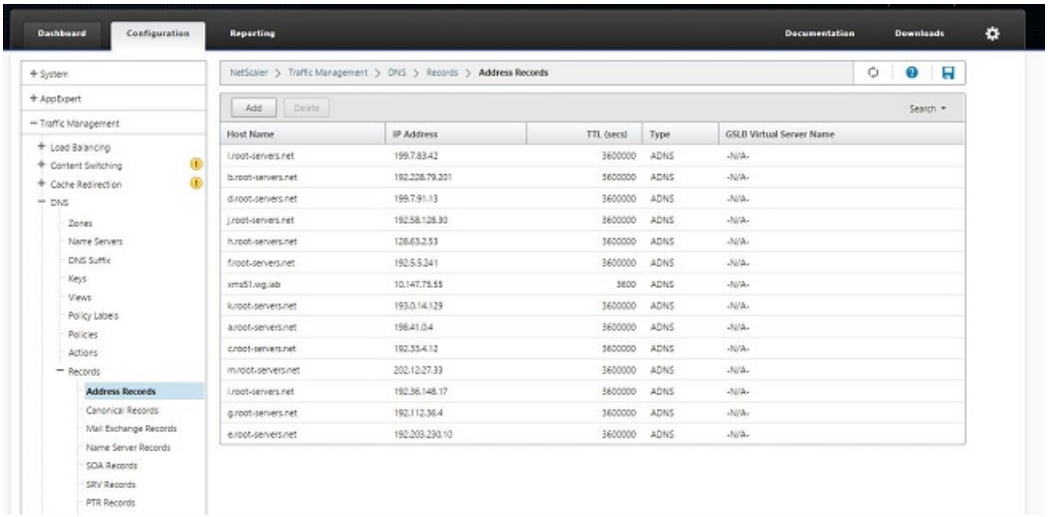
Vous verrez l'état de l'adresse IP virtuelle sur la page XenMobile.



16. Pour vérifier que les adresses IP virtuelles sont opérationnelles, cliquez sur l'onglet Configuration, puis accédez à Traffic Management > Load Balancing > Virtual Servers.



Vous verrez également que l'entrée DNS dans NetScaler pointe vers l'adresse IP virtuelle d'équilibrage de charge MAM.



Guide de récupération d'urgence

Feb 23, 2017

Vous pouvez concevoir et configurer des déploiements XenMobile comprenant plusieurs sites pour la récupération d'urgence à l'aide d'une stratégie de basculement active-passive. Pour plus d'informations, veuillez consulter l'article Disaster Recovery du manuel de déploiement XenMobile.

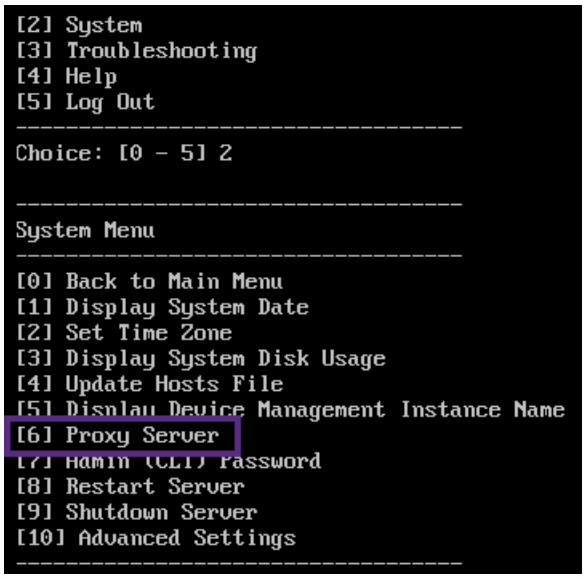
Activer les serveurs proxy

Feb 23, 2017

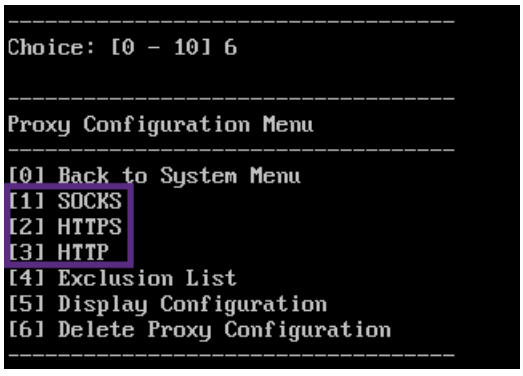
Lorsque vous souhaitez contrôler le trafic Internet sortant, vous pouvez configurer un serveur proxy dans XenMobile pour acheminer ce trafic. Pour ce faire, vous devez configurer le serveur proxy par le biais de l'interface de ligne de commande (CLI). Veuillez noter que la configuration du serveur proxy requiert le redémarrage de votre système.

1. Dans le menu principal de la ligne de commande XenMobile, tapez **2** pour sélectionner le menu système.

2. Dans le menu système, tapez **6** pour sélectionner le menu Serveur proxy.



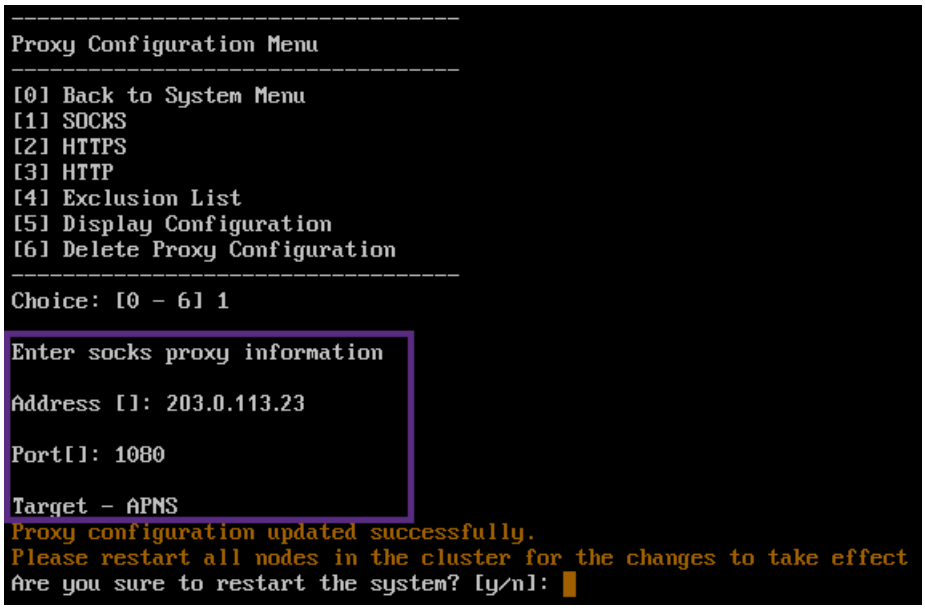
3. Dans le menu Configuration du proxy, tapez **1** pour sélectionnez SOCKS, **2** pour sélectionner HTTPS ou **3** pour sélectionner le protocole HTTP.



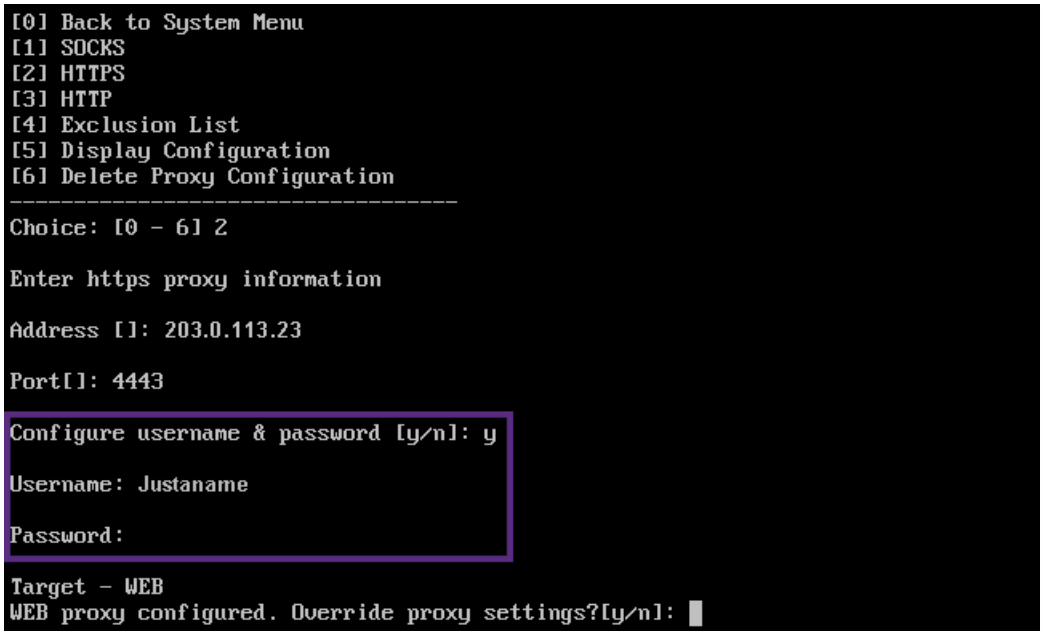
4. Entrez l'adresse IP de votre serveur proxy, le numéro de port et une cible. Reportez-vous au tableau suivant pour consulter la liste des types de cibles prises en charge pour chaque type de serveur proxy.

Type de proxy	Cibles prises en charge

SOCKS	APNS
HTTP	APNS, Web. PKI
HTTPS	Web, PKI
HTTP avec authentification	Web, PKI
HTTPS avec authentification	Web, PKI



5. Si vous choisissez de configurer un nom d'utilisateur et un mot de passe pour l'authentification sur votre serveur proxy HTTP ou HTTPS, tapez **y**, puis entrez le nom d'utilisateur et le mot de passe.



6. Tapez **y** pour terminer la configuration de votre serveur proxy.

Propriétés du serveur

Mar 31, 2017

XenMobile dispose de nombreuses propriétés qui s'appliquent aux opérations du serveur. Cet article décrit un grand nombre des propriétés de serveur et décrit en détail comment ajouter, modifier ou supprimer des propriétés de serveur.

Pour de plus amples informations sur les propriétés généralement configurées, reportez-vous à la section Propriétés du serveur dans le manuel virtuel XenMobile.

Définitions des propriétés du serveur

Add Device Always

Si ce paramètre est défini sur **true**, XenMobile ajoute un appareil à la console XenMobile, même si son inscription échoue, afin que vous puissiez voir les appareils qui ont tenté de s'inscrire. La valeur par défaut est **false**.

Audit Log Cleanup Execution Time

Heure de début du nettoyage du journal d'audit, au format HH:MM AM/PM. Exemple : 04:00 AM. La valeur par défaut est **02:00 AM**.

Audit Log Cleanup Interval (in Days)

Nombre de jours pendant lequel le serveur XenMobile doit conserver le journal d'audit. La valeur par défaut est **1**.

Audit Logger

Si la valeur est **false**, les événements d'interface utilisateur ne sont pas journalisés. La valeur par défaut est **false**.

Audit Log Retention (in Days)

Nombre de jours pendant lequel le serveur XenMobile doit conserver le journal d'audit. La valeur par défaut est **7**.

Certificate Renewal in Seconds

Nombre de secondes avant qu'un certificat expire après lequel XenMobile commence à renouveler les certificats. Par exemple, si un certificat expire le 30 décembre et que cette propriété est définie sur à 30 jours, XenMobile tente de renouveler le certificat si l'appareil se connecte entre le 1er décembre et le 30 décembre. Valeur par défaut : **2592000** secondes (30 jours).

Connection Timeout to Microsoft Certification Server

Nombre de secondes pendant lequel XenMobile attend une réponse du serveur de certificats. Si le serveur de certificats est lent et que le trafic est élevé, vous pouvez augmenter ce nombre à 60 secondes ou plus. Un serveur de certificats qui ne répond pas après 120 secondes doit être contrôlé. Valeur par défaut : **15000** millisecondes (15 secondes).

Deploy Log Cleanup (in Days)

Nombre de jours pendant lequel le serveur XenMobile doit conserver le journal de déploiement. La valeur par défaut

est **7**.

Disable SSL Server Verification

Si la valeur est **True**, elle désactive la validation du certificat de serveur SSL lorsque toutes les conditions suivantes sont remplies : vous avez activé l'authentification par certificats sur votre serveur XenMobile, le serveur d'autorité de certification Microsoft est l'émetteur du certificat et votre certificat a été signé par une autorité de certification racine interne dont la racine n'est pas approuvée par le serveur XenMobile. La valeur par défaut est **true**.

Enable Console

Si la valeur est **true**, les utilisateurs peuvent accéder à la console Portail en libre-service. La valeur par défaut est **true**.

Enable/Disable Hibernate statistics logging for diagnostics

Si la valeur est **True**, permet la journalisation des statistiques de veille prolongée pour faciliter la résolution des problèmes de performances des applications. Veille prolongée est un composant utilisé pour les connexions de XenMobile avec Microsoft SQL Server. Par défaut, la journalisation est désactivée car elle affecte la performance des applications. N'activez la journalisation que pour une courte durée pour éviter la création d'un énorme fichier journal. XenMobile enregistre les journaux sur /opt/sas/logs/hibernate_stats.log. La valeur par défaut est **false**.

Enable Notification Trigger

Active ou désactive les notifications du client Secure Hub. La valeur **true** active les notifications. La valeur par défaut est **true**.

Full Pull of ActiveSync Allowed and Denied Users

Nombre de secondes pendant lequel XenMobile attend une réponse du domaine lors de l'exécution d'une commande PowerShell pour obtenir des données des appareils ActiveSync. Le valeur par défaut est de **28800** secondes.

Identifies if telemetry is enabled or not

Identifie si la télémétrie (Programme d'amélioration de l'expérience utilisateur, ou CEIP) est activée. Vous pouvez choisir de participer au programme CEIP lorsque vous installez ou mettez à niveau XenMobile. La télémétrie est désactivée après 15 tentatives de chargement infructueuses consécutives. La valeur par défaut est **false**.

Inactivity Timeout in Minutes

Si la propriété de serveur **WebServices timeout type** est **INACTIVITY_TIMEOUT**, cette propriété définit le nombre de minutes après lequel XenMobile ferme la session d'un administrateur inactif qui utilisait l'API publique du serveur XenMobile pour accéder à la console XenMobile ou à toute application tierce. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **5**.

iOS Device Management Enrollment Auto-Install Enabled

Si la valeur est définie sur true, cette propriété réduit les interactions des utilisateurs lors de l'inscription d'appareils. Les utilisateurs devront cliquer sur **Root CA install** (si nécessaire) et **MDM Profile install**.

iOS Device Management Enrollment First Step Delayed

Après qu'un utilisateur entre ses informations d'identification lors de l'inscription d'un appareil, cette valeur de propriété spécifie la durée d'attente avant d'afficher un message invitant l'utilisateur à installer l'autorité de certification racine.

Citrix vous recommande de ne pas modifier cette propriété sauf si vous observez des problèmes de latence réseau ou de vitesse. Dans ce cas, ne définissez pas la valeur au-delà de 5 000 millisecondes (5 secondes). Valeur par défaut : **1000** millisecondes (1 seconde).

iOS Device Management Enrollment Last Step Delayed

Lors de l'inscription d'un appareil, cette valeur de propriété spécifie la durée d'attente entre installation du profil MDM et le démarrage de l'agent sur l'appareil. Citrix vous recommande de ne pas modifier cette propriété sauf si vous observez des problèmes de latence réseau ou de vitesse. Dans ce cas, ne définissez pas la valeur au-delà de 5 000 millisecondes (5 secondes). Valeur par défaut : **1000** millisecondes (1 seconde).

iOS Device Management Identity Delivery Mode

Spécifie si XenMobile distribue le certificat MDM aux appareils utilisant **SCEP** (recommandé pour des raisons de sécurité) ou **PKCS12**. En mode PKCS12, la paire de clés est générée sur le serveur et aucune négociation n'est effectuée. Valeur par défaut : **SCEP**.

iOS Device Management Identity Key Size

Définit la taille des clés privées pour les identités MDM, le service de profils iOS et les identités d'agent XenMobile. Valeur par défaut : **1024**.

iOS Device Management Identity Renewal Days

Spécifie le nombre de jours avant qu'un certificat n'expire après lequel XenMobile commence à renouveler les certificats. Par exemple, si un certificat expire dans 10 jours et que cette propriété est **10** jours, lorsqu'un appareil se connecte 9 jours avant l'expiration, XenMobile émet un nouveau certificat. Valeur par défaut : **30** jours.

iOS MDM APNS Private Key Password

Cette propriété contient le mot de passe APNS requis par XenMobile pour les notifications push aux serveurs Apple.

iOS MDM APNS Private Key Password

Cette propriété contient le mot de passe APNS requis par XenMobile pour les notifications push aux serveurs Apple.

MAM_MACRO_SUPPORT

Configure le serveur XenMobile pour les déploiements MAM exclusif de manière à ce que les utilisateurs d'appareils Android ou iOS qui s'inscrivent dans Secure Hub avec des informations d'identification de messagerie soient automatiquement inscrits dans Secure Mail. Cela signifie que les utilisateurs n'ont pas à entrer d'informations supplémentaires ou à effectuer des étapes supplémentaires pour s'inscrire dans Secure Mail. Ajoutez cette clé personnalisée et utilisez la valeur par défaut **True** afin d'activer l'inscription automatique à la messagerie. Les propriétés clientes ENABLE_CREDENTIAL_STORE et SEND_LDAP_ATTRIBUTES sont également requises.

À la première utilisation de Secure Mail, Secure Mail obtient l'adresse e-mail de l'utilisateur, le domaine et l'ID utilisateur depuis Secure Hub. Secure Mail utilise l'adresse e-mail pour la détection automatique. XenMobile identifie le serveur Exchange à l'aide du domaine et ID utilisateur, ce qui permet à Secure Mail d'authentifier l'utilisateur automatiquement. XenMobile invite l'utilisateur à entrer un mot de passe si la stratégie est définie pour ne pas contourner le mot de passe, mais l'utilisateur n'est pas invité à entrer des informations supplémentaires.

NetScaler Single Sign-On

Si la valeur est **False**, elle désactive la fonctionnalité de rappel de XenMobile durant le Single Sign-On depuis NetScaler vers le serveur XenMobile. XenMobile utilise la fonctionnalité de rappel pour vérifier l'ID de session NetScaler Gateway, si la configuration de NetScaler Gateway comprend une adresse URL de rappel. La valeur par défaut est **false**.

Number of consecutive failed uploads

Affiche le nombre d'échecs consécutifs durant les chargements du programme CEIP. XenMobile incrémente la valeur lorsqu'un chargement échoue. Après 15 échecs de chargement, XenMobile désactive le programme CEIP, également appelé télémétrie. Pour plus d'informations, consultez la section de la propriété de serveur **Identifies if telemetry is enabled or not**. XenMobile réinitialise la valeur sur **0** lorsqu'un chargement réussit.

Number of Users Per Device

Nombre maximal d'utilisateurs qui peuvent inscrire le même appareil en mode MDM. La valeur **0** signifie qu'un nombre illimité d'utilisateurs peut inscrire le même appareil. La valeur par défaut est **0**.

Pull of Incremental Change of Allowed and Denied Users

Nombre de secondes pendant lesquelles XenMobile attend une réponse du domaine lors de l'exécution d'une commande PowerShell pour obtenir un delta des appareils ActiveSync. valeur par défaut : **60** secondes.

Read Timeout to Microsoft Certification Server

Nombre de secondes pendant lesquelles XenMobile attend une réponse du serveur de certificats lors d'une opération de lecture. Si le serveur de certificats est lent et que le trafic est élevé, vous pouvez augmenter ce nombre à 60 secondes ou plus. Un serveur de certificats qui ne répond pas après 120 secondes doit être contrôlé. Valeur par défaut : **15000** millisecondes (15 secondes).

REST Web Services

Active ou désactive le service Web REST. La valeur par défaut est **true**.

Session Log Cleanup (in Days)

Nombre de jours pendant lequel le serveur XenMobile doit conserver le journal de session. La valeur par défaut est **7**.

Server Mode

Détermine si XenMobile est exécuté en mode MAM, MDM ou ENT (Enterprise), qui correspond à la gestion des applications, la gestion des appareils ou la gestion des appareils et des applications. Définissez la propriété du mode de serveur en fonction de la façon dont vous voulez que les appareils s'inscrivent, comme indiqué dans le tableau ci-dessous. La valeur par défaut du mode de serveur est **ENT**, quel que soit le type de licence.

Si vous disposez d'une licence XenMobile MDM Edition, le mode de serveur efficace est toujours MDM, quel que soit le mode de serveur que vous avez défini dans les propriétés du serveur. Si vous disposez d'une licence MDM Edition, vous ne pouvez pas activer la gestion des applications en définissant le mode du serveur sur MAM ou ENT.

Vos licences sont cette Édition	Vous voulez que les appareils s'inscrivent dans ce mode	Définissez la propriété du mode de serveur sur
Enterprise / Advanced	Mode MDM	MDM

Enterprise / Advanced	Mode MDM+MAM	ENT
MDM	Mode MDM	MDM

Le mode de serveur efficace est la combinaison du type de licence et du mode de serveur. Pour une licence MDM, le mode de serveur efficace est toujours MDM, quel que soit le paramètre de mode du serveur. Pour les licences Enterprise et Advanced, le mode de serveur efficace correspond au mode du serveur, si le mode du serveur est **ENT** ou **MDM**. Si le mode du serveur est **MAM**, le mode de serveur efficace est ENT.

XenMobile ajoute le mode de serveur au journal du serveur chaque fois qu'une licence est activée ou supprimée et lorsque vous modifiez le mode du serveur dans les propriétés du serveur. Pour de plus amples informations sur la création et l'affichage des fichiers journaux, consultez les sections Journaux et Visualiser et analyser les fichiers journaux dans XenMobile.

Static Timeout in Minutes

Si la propriété de serveur **WebServices timeout type** est **INACTIVITY_TIMEOUT**, cette propriété définit le nombre de minutes après lesquellesl XenMobile ferme la session d'un administrateur qui utilisait l'API publique du serveur XenMobile pour accéder à la console XenMobile ou à toute application tierce. Valeur par défaut : **60**.

Trigger Agent Message Suppression

Active ou désactive la messagerie du client Secure Hub. La valeur **false** active la messagerie. La valeur par défaut est **true**.

Trigger Agent Sound Suppression

Active ou désactive les sons du client Secure Hub. La valeur **false** active les sons. La valeur par défaut est **true**.

Unauthenticated App Download for Android Devices

Si la valeur est **True**, vous pouvez télécharger des applications auto-hébergées sur des appareils Android exécutant Android for Work. XenMobile a besoin de cette propriété si l'option Android for Work permettant de fournir une adresse URL de téléchargement statique dans Google Play Store est activée. Dans ce cas, les adresses URL de téléchargement ne peuvent pas inclure de ticket à usage unique (défini par la propriété du **serveur Ticket à usage unique XAM**) qui possède le jeton d'authentification. La valeur par défaut est **false**.

Unauthenticated App Download for Windows Devices

Utilisé uniquement pour les anciennes versions de Secure Hub qui ne valident pas les tickets à usage unique. Si la valeur est **False**, vous pouvez télécharger des applications non authentifiées depuis XenMobile sur des appareils Windows. La valeur par défaut est **false**.

Use ActiveSync ID to Conduct an ActiveSync Wipe Device

Si la valeur est **true**, XenMobile Mail Manager utilise l'identificateur ActiveSync en tant qu'argument pour la méthode asWipeDevice. La valeur par défaut est **false**.

Users only from Exchange

Si la valeur est **true**, désactive l'authentification utilisateur pour les utilisateurs ActiveSync Exchange. La valeur par défaut est **false**.

WebServices Timeout Type

Indique comment faire expirer un jeton d'authentification récupéré depuis l'API publique. Si **STATIC_TIMEOUT** est sélectionné, XenMobile considère qu'un jeton d'authentification a expiré après expiration de la valeur spécifiée dans la propriété de serveur **Static Timeout in Minutes**.

Si **INACTIVITY_TIMEOUT** est sélectionné, XenMobile considère qu'un jeton d'authentification a expiré si ce dernier reste inactif pendant la valeur spécifiée dans la propriété de serveur **Inactivity Timeout in Minutes**. Valeur par défaut : **STATIC_TIMEOUT**.

XAM One-Time Ticket

Nombre de millisecondes pendant lequel un jeton d'authentification à usage unique (OTT) est valide pour le téléchargement d'une application. Cette propriété fonctionne en conjonction avec les propriétés **Téléchargement d'applications non authentifiées pour Android** et **Téléchargement d'applications non authentifiées pour Windows**, qui spécifient si le téléchargement d'applications non authentifiées est autorisé. Valeur par défaut : **3600000**.

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

Nombre de minutes après lesquelles XenMobile ferme la session d'un utilisateur inactif sur le portail en libre-service de XenMobile. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. Valeur par défaut : **30**.

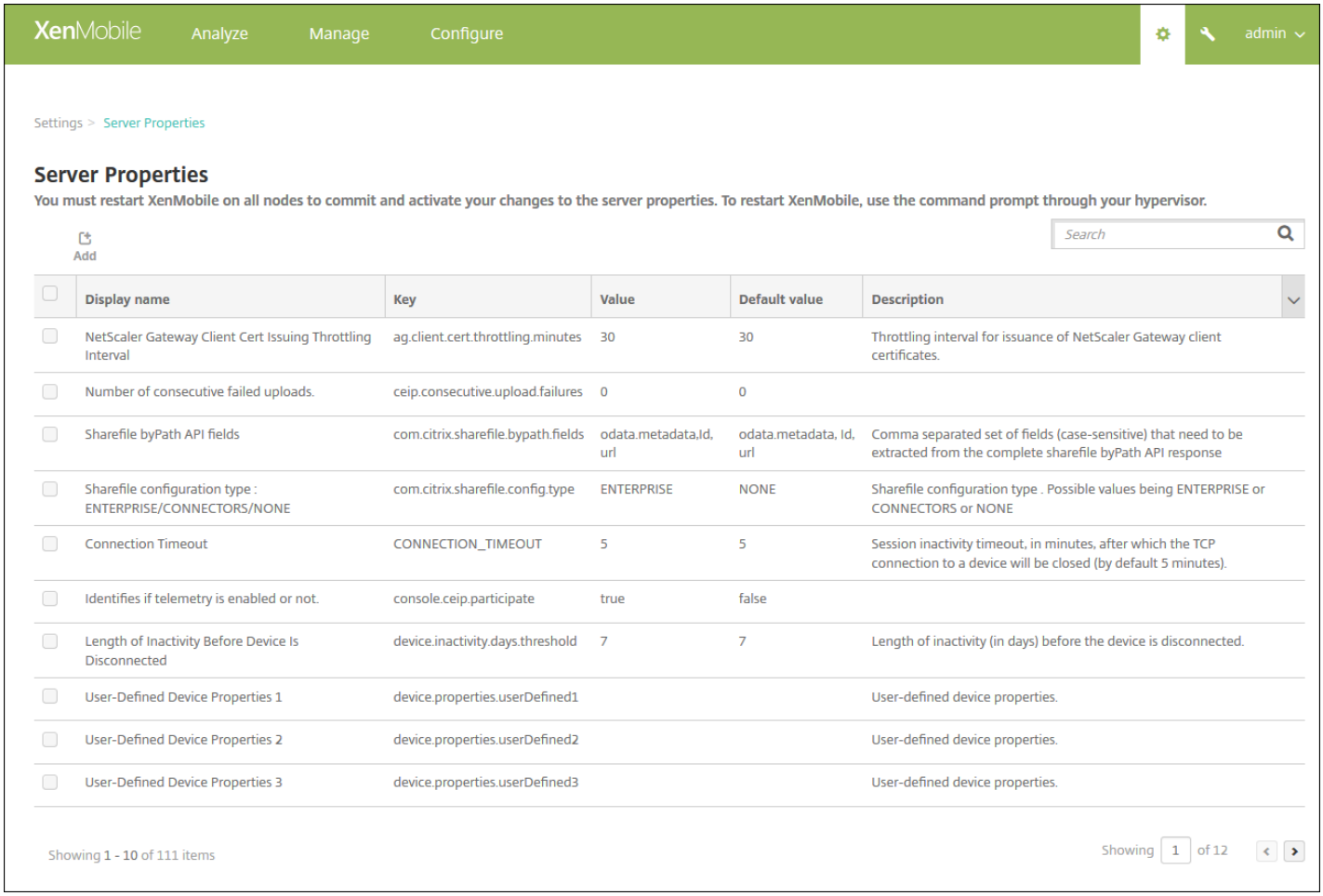
Ajout, modification ou suppression de propriétés de serveur

Dans XenMobile, vous pouvez appliquer des propriétés au serveur. Après avoir effectué des modifications, vous devez redémarrer XenMobile sur tous les nœuds pour valider et activer les modifications.

> ## Remarque
>
> Pour redémarrer XenMobile, utilisez l'invite de commande par le biais de votre hyperviseur.

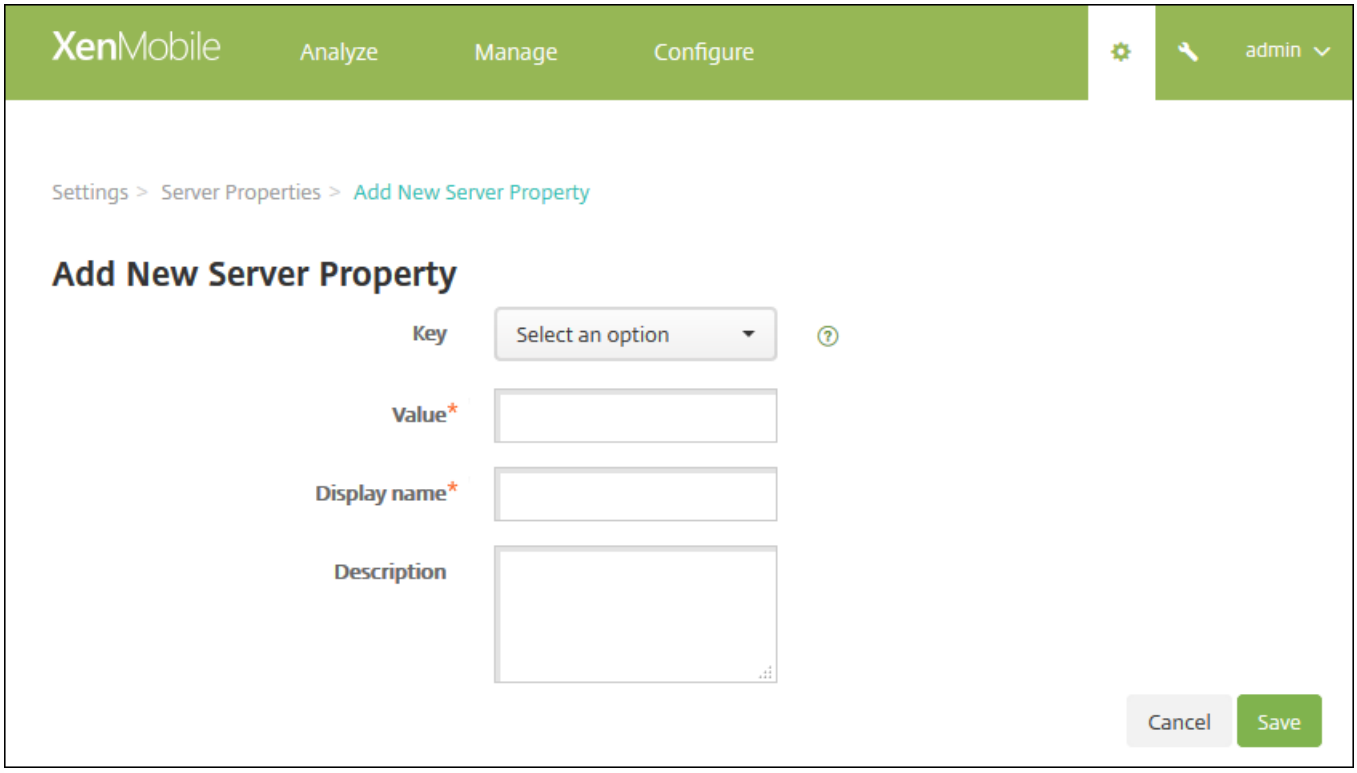
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **Propriétés du serveur**. La page **Propriétés du serveur** s'affiche. Vous pouvez ajouter, modifier ou supprimer des propriétés de serveur à partir de cette page.



Pour ajouter une propriété de serveur

1. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle propriété de serveur** s'affiche.



2. Pour configurer ces paramètres :

- **Clé** : dans la liste, sélectionnez la clé appropriée. les clés sont sensibles à la casse Vous devez contacter le support technique Citrix avant d'apporter des modifications, ou pour demander une clé spéciale.
- **Valeur** : entrez une valeur, en fonction de la clé que vous avez sélectionnée.
- **Nom d'affichage** : entrez un nom pour la nouvelle valeur de propriété qui s'affiche dans le **tableau** Propriétés du serveur**.**
- **Description** : entrez une description pour la nouvelle propriété de serveur (facultatif).

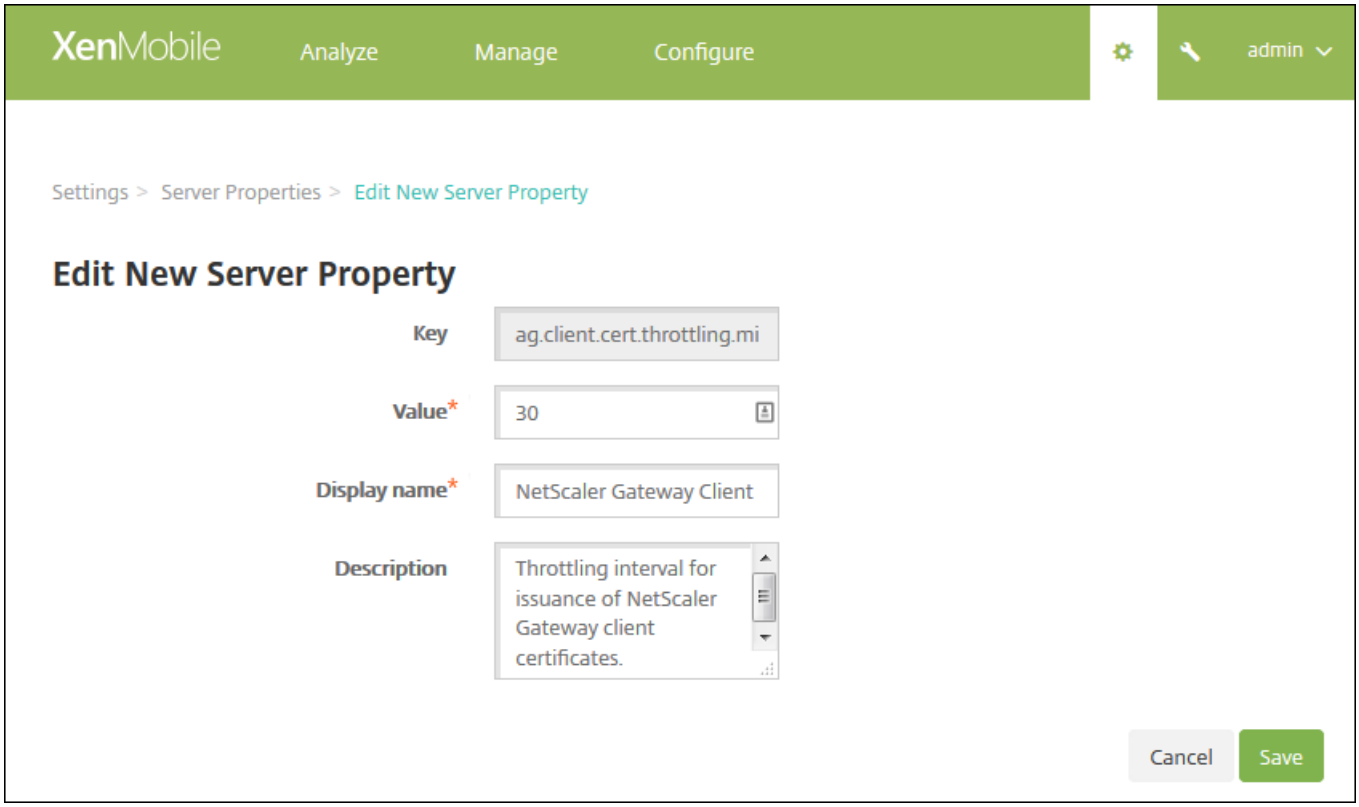
3. Cliquez sur **Enregistrer**.

Pour modifier une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez modifier.

> **Remarque** : lorsque vous sélectionnez la case à cocher en regard d'une propriété de serveur, le menu d'options s'affiche au-dessus de la liste des propriétés de serveur ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

2. Cliquez sur **Modifier**.La page **Modifier une nouvelle propriété de serveur** s'affiche.



3. Modifiez les informations suivantes le cas échéant :

- **Clé** : vous ne pouvez pas modifier ce champ.
- **Valeur** : valeur de la propriété.
- **Nom d'affichage** : nom de la propriété.
- **Description** : description de la propriété.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de serveur

1. Dans le tableau **Propriétés du serveur**, sélectionnez la propriété de serveur que vous voulez supprimer.

   Remarque : vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Supprimer**.Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Options d'interface de ligne de commande

Feb 23, 2017

Vous pouvez accéder à tout moment aux options d'interface de ligne de commande comme suit (CLI) :

- Sur l'hyperviseur sur lequel vous avez installé XenMobile : Citrix XenServer, Microsoft Hyper-V ou VMware ESXi. Dans votre hyperviseur, sélectionnez la machine virtuelle XenMobile importée, démarrez l'invite de commande et connectez-vous à votre compte d'administrateur pour XenMobile. Pour de plus amples informations, consultez la documentation de votre hyperviseur.
- À l'aide de SSH, si SSH est activé dans votre pare-feu. Connectez-vous à votre compte d'administrateur pour XenMobile.

L'interface de ligne de commande vous permet d'effectuer un grand nombre de tâches de configuration et de dépannage. Vous trouverez ci-après le menu de niveau supérieur de la CLI.

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

Options de configuration

Exemples du **menu de configuration** et des paramètres affichés pour chaque option.

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

[1] Réseau

```
 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] Pare-feu

```
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] Base de données

```
  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] Ports d'écoute

```
 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]:
```

Options de mise en cluster

Exemples du **menu de mise en cluster** et des paramètres affichés pour chaque option.

```
-----------------------------------
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] Afficher l'état du cluster

```
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] Activer/désactiver le cluster

Lorsque vous choisissez d'activer la mise en cluster, le message suivant s'affiche :

> Pour activer la communication en temps réel entre membres du cluster, ouvrez le port 80 à l'aide de l'option du menu Pare-feu du menu CLI. Vous pouvez également configurer la liste blanche d'accès dans les paramètres du pare-feu pour limiter l'accès.

Lorsque vous choisissez de désactiver la mise en cluster, le message suivant s'affiche :

> Vous avez choisi de désactiver la mise en cluster. L'accès au port 80 n'est pas nécessaire. Veuillez le désactiver.

[3] Liste blanche des membres du cluster

```
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] Activer ou désactiver le déchargement SSL

Si vous choisissez d'activer ou de désactiver le déchargement SSL, le message suivant s'affiche :

> L'activation du déchargement SSL ouvrira le port 80 pour tout le monde. Veuillez configurer l'accès à la liste blanche dans les paramètres du pare-feu pour un accès limité.

[5] Afficher le cluster Hazelcast

Lorsque vous sélectionnez d'afficher le cluster Hazelcast, les options suivantes s'affichent :

Membres du cluster Hazlecast :

[Adresses IP répertoriées]

REMARQUE : si un nœud configuré ne fait pas partie du cluster, veuillez redémarrer ce nœud.

Options système

À partir du **menu système**, vous pouvez afficher ou définir diverses informations de niveau du système, redémarrer ou arrêter le serveur ou accéder aux **Paramètres avancés**.

```
-----------------------------------
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] Paramètres avancés

```
********************* 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
-----------------------------------
```

Les options de **réglage du serveur** incluent un délai d'expiration de la connexion au serveur, un nombre maximal de connexions (par port), et un nombre maximal de threads (par port).

Options de dépannage

Exemples du **menu de dépannage** et des paramètres affichés pour chaque option.

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

[1] Utilitaires de réseau

```
---------------------------------
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] Journaux

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

[3] Pack d'assistance

```
---------------------------------
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
---------------------------------
```

Présentation des workflows pour la console XenMobile

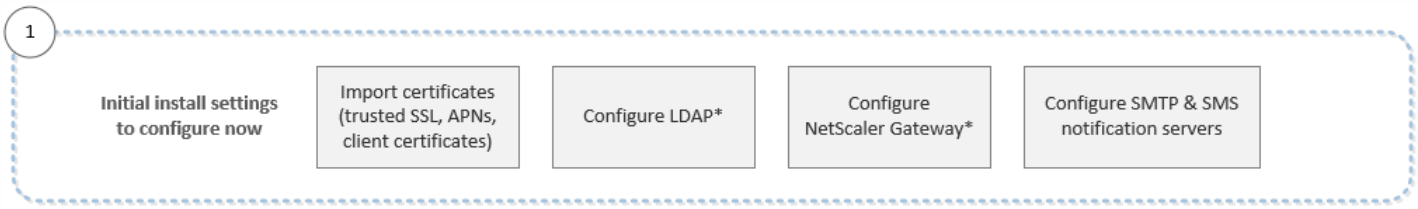
Feb 23, 2017

La console XenMobile est l'outil de gestion unifiée dans XenMobile. Cet article suppose que vous avez installé XenMobile et que vous êtes prêt à travailler dans la console. Si vous devez installer XenMobile, consultez la section Installation de XenMobile. Pour plus de détails sur les navigateurs pris en charge pour la console XenMobile, consultez la section Prise en charge des navigateurs dans l'article Compatibilité XenMobile.

Workflow des paramètres initiaux

Après avoir terminé la configuration de XenMobile dans la console de ligne de commande puis dans la console XenMobile, le tableau de bord s'ouvre. Étant donné que vous ne pouvez pas revenir sur les écrans de configuration initiaux, si vous avez ignoré certaines configurations, vous pouvez configurer les paramètres suivants dans la console. Avant de commencer à ajouter des utilisateurs, des applications et des appareils, il est préférable d'avoir compléter ces paramètres d'installation. Pour commencer, cliquez sur l'icône d'engrenage dans le coin supérieur droit.

Remarque : les éléments marqués d'un astérisque sont facultatifs.



Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles et les sous-articles suivants de la documentation des produits Citrix :

- Authentification
- NetScaler Gateway et XenMobile
- Notifications

Pour prendre en charge les plates-formes Windows, iOS et Android, vous devez configurer votre compte comme suit.

Android

- Créer les informations d'identification Google Play. Pour de plus amples informations, consultez la section Google Play Getting Started with Publishing.
- Créer un compte d'administrateur Android for Work. Pour de plus amples informations, consultez la section Android for Work.
- Vérifier votre nom de domaine avec Google. Pour de plus amples informations, consultez la section Vérifier votre domaine pour Google Apps.
- Activer les API et créer un compte de service pour Android for Work. Pour de plus amples informations, consultez la section Aide de Android for Work.

iOS

- Créer un compte Apple ID et de développeur. Pour de plus amples informations, consultez le site Web Apple Developer Program.
- Créer un certificat APNS (Apple Push Notification Service). Vous avez besoin d'un certificat APNS d'Apple si vous prévoyez de gérer des appareils IOS avec votre déploiement XenMobile Service (cloud) et si vous prévoyez d'utiliser la notification push pour votre déploiement WorxMail. Pour de plus amples informations, consultez le portail Apple Push Certificates Portal. Pour plus d'informations sur XenMobile et APNS, consultez Certificats APNS et Notifications push pour WorxMail pour iOS.
- Créer un jeton d'entreprise VPP (Volume Purchase Program). Pour de plus amples informations, consultez la section Programme d'achat en volume d'Apple.

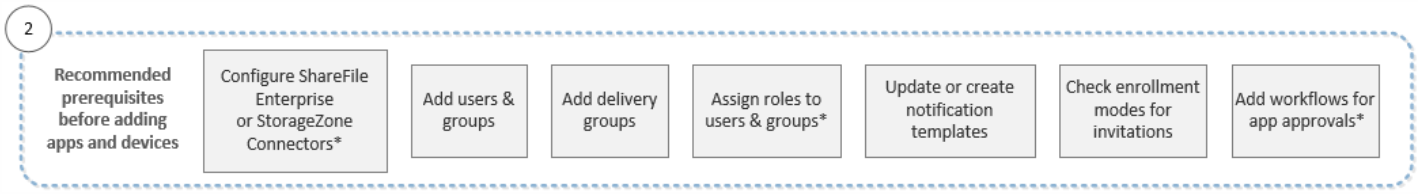
Windows

- Créer un compte de développeur Microsoft Windows Store. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Obtenir un ID Microsoft Windows Store Publisher. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Obtenir un certificat d'entreprise de Symantec. Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.
- Si vous souhaitez utiliser le service de détection automatique de XenMobile pour l'inscription de votre Windows Phone, assurez-vous que vous disposez d'un certificat SSL public. Pour de plus amples informations, consultez la section Détection automatique XenMobile.
- Créer un jeton d'inscription d'application (AET). Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.

Workflow de la configuration requise pour la console

Ce workflow affiche les prérequis recommandés que vous devez configurer avant d'ajouter des applications et des appareils.

Remarque : les éléments marqués d'un astérisque sont facultatifs.



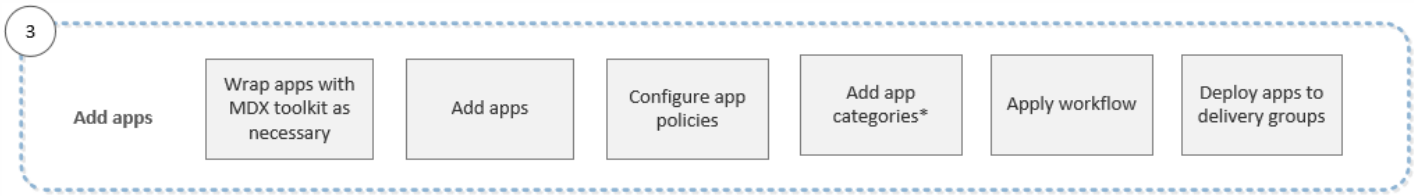
Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles et les sous-articles suivants de la documentation des produits Citrix :

- Comptes utilisateur, rôles et inscription
- Déployer des ressources
- Configurer des rôles avec RBAC
- Notifications
- Créer et gérer des workflows

Workflow d'ajout d'applications

Ce workflow affiche un ordre recommandé à suivre lors de l'ajout d'applications à XenMobile.

Remarque : les éléments marqués d'un astérisque sont facultatifs.



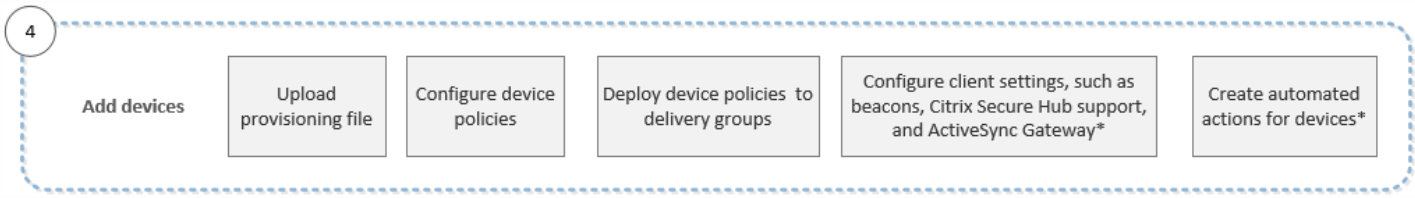
Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles et les sous-articles suivants de la documentation des produits Citrix :

- À propos du MDX Toolkit
- Ajouter des applications.
- Synopsis des stratégies MDX
- Créer et gérer des workflows
- Déployer des ressources

Workflow d'ajout d'appareils

Ce workflow affiche un ordre recommandé à suivre lors de l'ajout et de l'enregistrement d'appareils dans XenMobile.

Remarque : les éléments marqués d'un astérisque sont facultatifs.

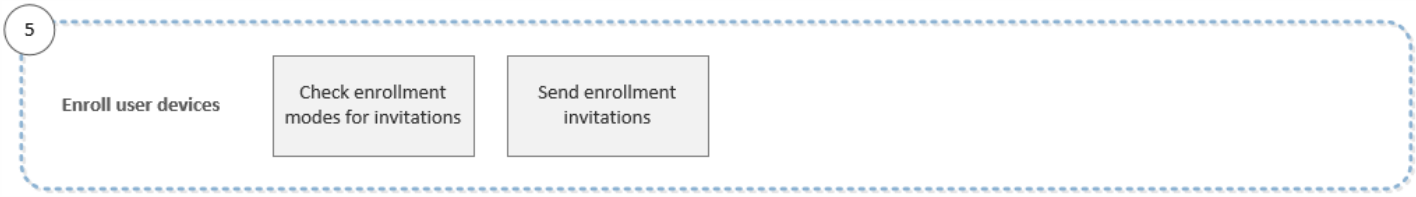


Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles et les sous-articles suivants de la documentation des produits Citrix :

- Appareils
- Plates-formes prises en charge
- Déployer des ressources
- Surveillance et support
- Actions automatisées

Workflow d'inscription d'appareils utilisateur

Ce workflow affiche un ordre recommandé à suivre lors de l'inscription d'appareils utilisateur dans XenMobile.



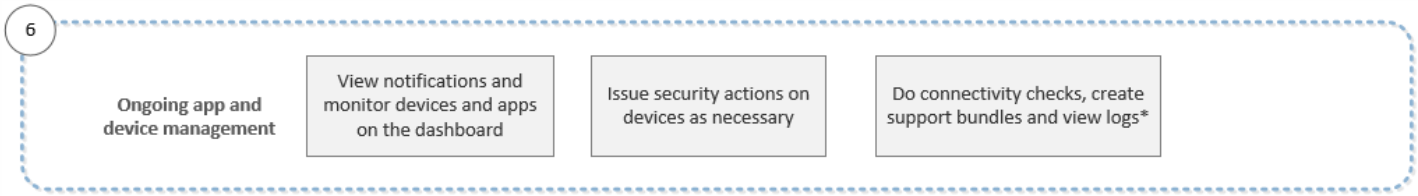
Pour plus d'informations sur chaque paramètre, ainsi que les procédures détaillées, consultez les articles suivants de la documentation des produits Citrix :

- Comptes utilisateur, rôles et inscription
- Notifications

Workflow de gestion des applications et appareils

Ce workflow affiche les activités de gestion des applications et des appareils recommandées que vous pouvez effectuer dans la console.

Remarque : les éléments marqués d'un astérisque sont facultatifs.



Pour de plus amples informations sur les options de support disponibles à partir de l'icône de clé dans le coin supérieur droit de la console, veuillez consulter la section Surveillance et support et ses sous-articles.

Authentification

Mar 31, 2017

Plusieurs composants jouent un rôle dans le processus d'authentification lors des opérations XenMobile :

- **Serveur XenMobile** : le serveur XenMobile vous permet de définir la sécurité liée à l'inscription ainsi que l'expérience d'inscription. Vous pouvez choisir d'ouvrir l'inscription à tous les utilisateurs ou par invitation uniquement et exiger une authentification à deux ou trois facteurs. Dans les propriétés du client XenMobile, vous pouvez activer l'authentification par code PIN Citrix et configurer la complexité et le délai d'expiration du code PIN.
- **NetScaler** : NetScaler fournit un point de terminaison pour les sessions SSL micro VPN, assure la sécurité en transit sur le réseau et vous permet de définir l'expérience d'authentification utilisée chaque fois qu'un utilisateur accède à une application.
- **Secure Hub** : Secure Hub fonctionne avec le serveur XenMobile au cours des opérations d'inscription. Secure Hub est l'entité basée sur un appareil qui communique avec NetScaler : si une session expire, Secure Hub obtient un ticket d'authentification de NetScaler et transmet le ticket aux applications MDX. Citrix vous recommande d'utiliser le certificate pinning, qui empêche les attaques « man-in-the-middle ». Pour de plus amples informations, consultez la section sur le certificate pinning dans l'article Secure Hub.

  Secure Hub gère également le conteneur de sécurité MDX : Secure Hub force les stratégies, crée une nouvelle session avec NetScaler lors de l'expiration d'une application et définit le délai d'expiration MDX et l'authentification. Secure Hub est également responsable de la détection des appareils jailbreakés, des contrôles de géolocalisation et de toute autre stratégie que vous appliquez.

- **Stratégies MDX** : les stratégies MDX créent l'espace de stockage sécurisé sur l'appareil. Les stratégies MDX redirigent les connexions micro VPN vers NetScaler et appliquent les restrictions du mode déconnecté ainsi que les stratégies de client, telles que les délais d'expiration.

Pour de plus amples informations sur les considérations à prendre en compte lors de la configuration de l'authentification, y compris une vue d'ensemble des méthodes d'authentification à un et deux facteurs, veuillez consulter l'article Authentication du manuel de déploiement.

Dans XenMobile, les certificats permettent d'établir des connexions sécurisées et d'authentifier les utilisateurs. Le reste de cet article décrit les certificats. Pour plus d'informations sur la configuration, consultez les articles suivants :

- Authentification domaine ou domaine + jeton de sécurité
- Authentification certificat client ou certificat + domaine
- Entités PKI
- Fournisseurs d'identités
- Certificats APNS
- SAML pour l'authentification unique avec ShareFile
- Paramètres du serveur Microsoft Azure Active Directory

Certificats

Par défaut, XenMobile est équipé d'un certificat SSL auto-signé qui est généré lors de l'installation afin de sécuriser les communications sur le serveur. Citrix vous recommande de remplacer le certificat SSL avec un certificat SSL approuvé

provenant d'une autorité de certification (CA) reconnue.

XenMobile utilise également son propre service d'infrastructure de clé publique (PKI) ou obtient les certificats de l'autorité de certification pour les certificats clients. Tous les produits Citrix prennent en charge les caractères génériques et les certificats SAN. Pour la plupart des déploiements, vous n'aurez besoin que deux caractères génériques ou certificats (SAN).

L'authentification du certificat client offre une couche de sécurité supplémentaire pour les applications mobiles et permet aux utilisateurs d'accéder de manière transparente aux applications HDX. Lorsque l'authentification du certificat client est configurée, les utilisateurs entrent leur code PIN Citrix pour accéder en Single Sign-On aux applications XenMobile. Le code secret Citrix simplifie également l'expérience utilisateur pour l'authentification. Le code PIN Citrix est utilisé pour sécuriser un certificat client ou enregistrement des informations d'identification Active Directory localement sur leur appareil.

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat Apple Push Notification Service (APNS). Ces étapes sont décrites sous Certificats APNS.

Le tableau suivant illustre le format et le type du certificat pour chaque composant de XenMobile :

Composant XenMobile	**Format du certificat**	**Type de certificat requis**
NetScaler Gateway	PEM (BASE64) PFX (PKCS#12)	SSL, racine NetScaler Gateway convertit automatiquement un fichier PFX vers PEM.
Serveur XenMobile	.p12 (.pfx sur les ordinateurs Windows)	SSL, SAML, APNS XenMobile génère également une PKI complète durant le processus d'installation.
StoreFront	PFX (PKCS#12)	SSL, racine

XenMobile prend en charge les certificats d'écoute SSL et les certificats clients de 4096, 2048 et 1024 bits. Veuillez noter que les certificats 1024 bits peuvent être facilement compromis.

Pour NetScaler Gateway et le serveur XenMobile, Citrix recommande d'obtenir les certificats de serveur à partir d'une autorité de certification publique, comme Verisign, Thawte ou DigiCert. Vous pouvez créer une demande de signature de certificat (CSR) à partir de NetScaler Gateway ou de l'utilitaire de configuration XenMobile. Lorsque vous créez la CSR, envoyez-la à l'autorité de certification pour signature. Lorsque l'autorité de certification renvoie le certificat signé, vous pouvez l'installer sur NetScaler Gateway ou XenMobile.

Chargement de certificats dans XenMobile

Chaque certificat que vous chargez est représenté par une entrée dans le tableau Certificats, qui résume son contenu. Lorsque vous configurez des composants d'intégration PKI qui nécessitent un certificat, vous êtes invité à choisir des certificats de serveur répondant à des critères spécifiques au contexte dans une liste. Par exemple, il se peut que vous souhaitiez configurer XenMobile pour s'intégrer à Microsoft CA. La connexion à Microsoft CA doit être authentifiée à l'aide d'un certificat client.

Cette section explique comment charger des certificats. Pour plus d'informations sur la création, le chargement et la configuration de certificats client, consultez la section Authentification certificat client ou certificat + domaine.

Configuration requise pour la clé privée

XenMobile peut posséder ou pas la clé privée d'un certificat donné. De même, XenMobile peut nécessiter ou non une clé privée pour les certificats que vous chargez.

Chargement de certificats sur la console

Vous avez le choix entre deux options principales pour charger des certificats sur la console :

- Vous pouvez cliquer pour importer un keystore et identifier l'entrée dans le référentiel de keystore dans lequel vous souhaitez l'installer, sauf si vous chargez un format PKCS#12.
- Vous pouvez cliquer pour importer un certificat.

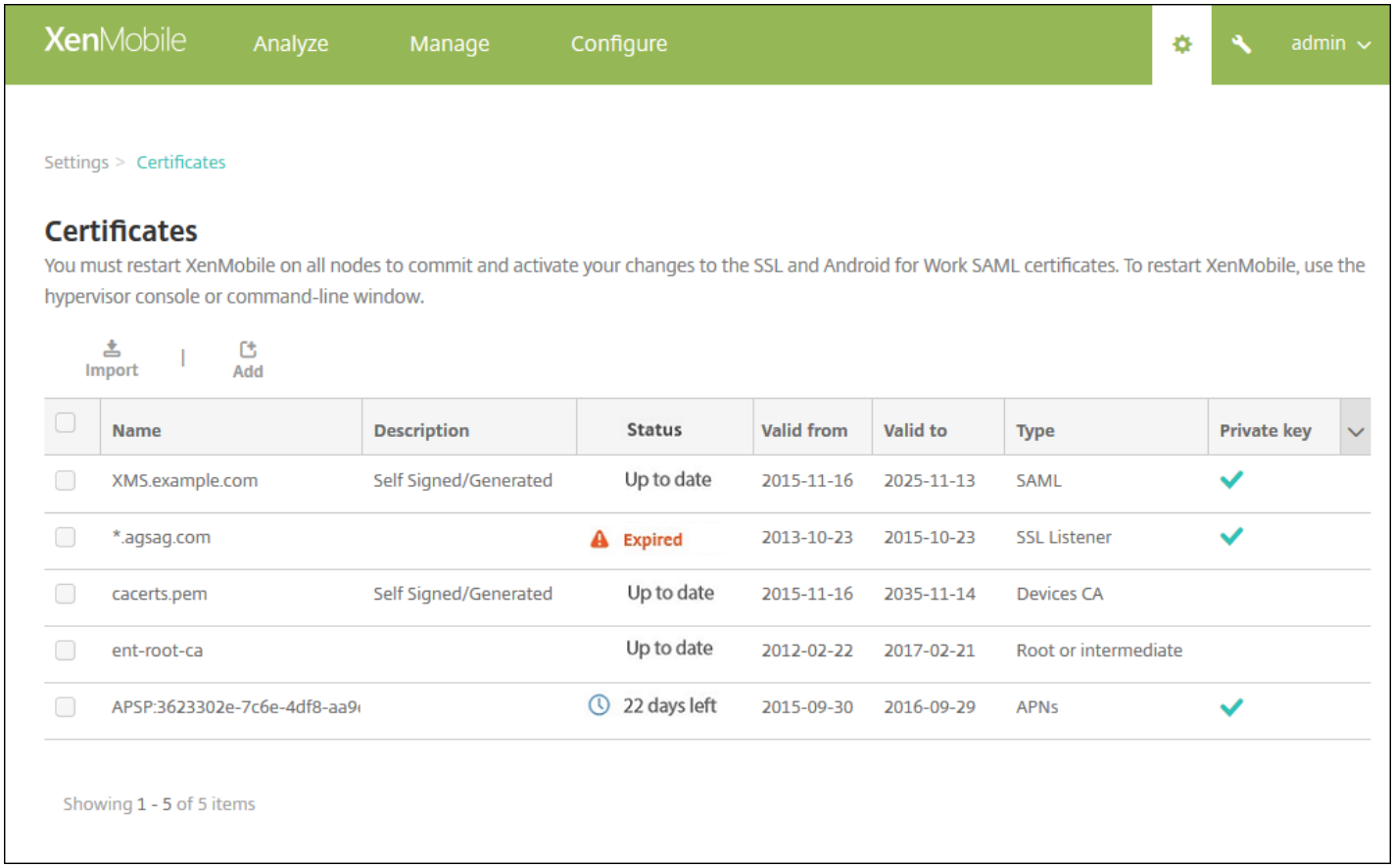
Vous pouvez charger le certificat d'autorité de certification (sans la clé privée) que l'autorité de certification utilise pour signer les demandes, et un certificat client SSL (avec la clé privée) pour l'authentification du client. Lors de la configuration de l'entité Microsoft CA, vous devez spécifier le certificat d'autorité de certification, que vous pouvez sélectionner à partir d'une liste de tous les certificats de serveur qui sont des certificats d'autorité de certification. De même, lorsque vous configurez l'authentification de client, vous pouvez faire votre choix dans une liste de tous les certificats de serveur pour lesquels XenMobile possède la clé privée.

Pour importer un keystore

À dessein, les keystores, qui sont des référentiels de certificats de sécurité, peuvent comporter plusieurs entrées. Par conséquent, lors du chargement à partir d'un keystore, vous êtes invité à indiquer l'alias d'entrée qui identifie l'entrée à charger. Si vous ne spécifiez pas d'alias, la première entrée du magasin est chargée. Étant donné que les fichiers PKCS#12 ne contiennent généralement qu'une seule entrée, le champ d'alias ne s'affiche pas lorsque vous sélectionnez PKCS#12 en tant que type de keystore.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

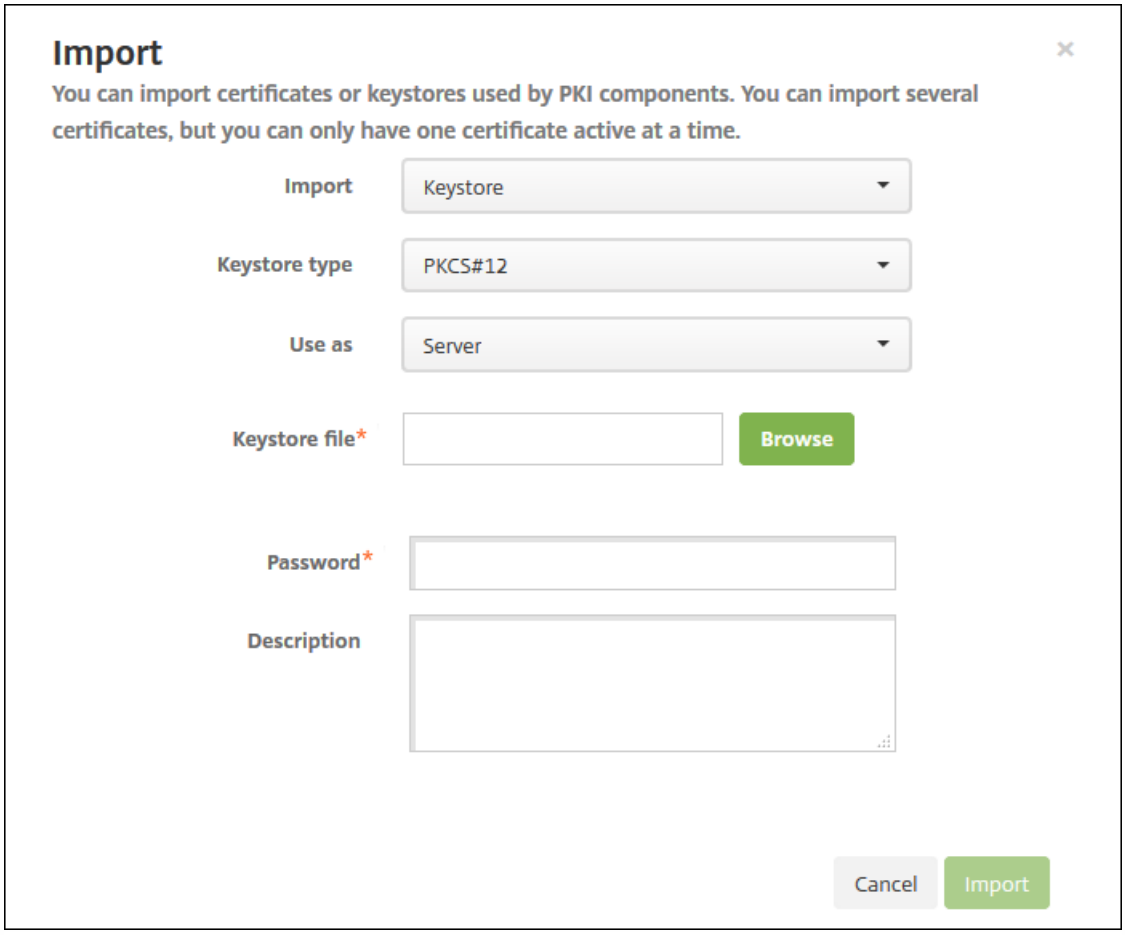
2. Cliquez sur **Certificats**. La page **Certificats** s'affiche.



3. Cliquez sur **Importer**. La boîte de dialogue **Importer** s'affiche.

4. Pour configurer ces paramètres :

- **Importer** : dans la liste, cliquez sur **Keystore**. La boîte de dialogue **Importer** change pour refléter les options de keystore disponibles.



- **Type de keystore** : dans la liste, cliquez sur **PKCS#12**.
- **Utiliser en tant que** : dans la liste, cliquez pour spécifier la manière dont vous utilisez le certificat. Les options disponibles sont :
  - **Serveur**. Les certificats de serveur sont des certificats utilisés par le serveur XenMobile qui sont chargés sur la console Web XenMobile. Ils comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette utilisation s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
  - **SAML**. La certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.
  - **APNS**. Les certificats APNS d'Apple permettent de gérer les appareils mobiles via le réseau Apple Push Network.
  - **Écouteur SSL**. L'écouteur SSL notifie XenMobile de l'activité cryptographique SSL.
- **Fichier de keystore** : recherchez le keystore de type de fichier .p12 que vous souhaitez importer (ou .pfx sur les ordinateurs Windows).
- **Mot de passe** : entrez le mot de passe affecté au certificat.
- **Description** : entrez une description vous permettant de distinguer le keystore de vos autres keystores (facultatif).

5. Cliquez sur **Importer**.Le keystore est ajouté au tableau Certificats.

Pour importer un certificat

Lors de l'importation d'un certificat, soit à partir d'un fichier, soit depuis une entrée de keystore, XenMobile tente de construire une chaîne de certificats à partir de l'entrée et importe tous les certificats dans cette chaîne (créant une entrée de certificat de serveur pour chacun d'eux). Cette opération fonctionne uniquement si les certificats du fichier ou l'entrée keystore forment réellement une chaîne, comme si chaque certificat suivant de la chaîne est l'émetteur du certificat précédent.

Vous pouvez ajouter une description facultative pour le certificat importé à des fins heuristiques. La description est uniquement attachée au premier certificat dans la chaîne. Vous pouvez mettre à jour la description des certificats restants plus tard.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Certificats**.

2. Sur la page **Certificats**, cliquez sur **Importer**.La boîte de dialogue **Importer** apparaît.

3. Dans la boîte de dialogue **Importer**, dans **Importer**, s'il n'est pas déjà sélectionné, cliquez sur **Certificat**.

4. La boîte de dialogue **Importer** change pour refléter les options de certificat disponibles. Dans **Utiliser en tant que**, cliquez pour spécifier la manière dont vous utilisez le keystore. Les options disponibles sont :

- **Serveur**. Les certificats de serveur sont des certificats utilisés par le serveur XenMobile qui sont chargés sur la console Web XenMobile. Ils comprennent des certificats d'autorité de certification, des certificats d'autorité d'inscription et des certificats pour l'authentification des clients avec d'autres composants de votre infrastructure. En outre, vous pouvez utiliser les certificats de serveur en tant que stockage pour les certificats que vous voulez déployer vers des appareils. Cette option s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.
- **SAML**. La certification SAML vous permet de fournir une authentification unique (SSO) aux serveurs, sites Web et applications.
- **Écouteur SSL**. L'écouteur SSL notifie XenMobile de l'activité cryptographique SSL.

5. Recherchez le keystore de type de fichier .p12 que vous souhaitez importer (ou .pfx sur les ordinateurs Windows).

6. Parcourez pour rechercher un fichier de clé privée facultatif pour le certificat. La clé privée est utilisée pour le chiffrement et le déchiffrement en conjonction avec le certificat.

7. Entrez une description pour le certificat (facultatif) pour vous aider à le distinguer de vos autres certificats.

8. Cliquez sur **Importer**. Le certificat est ajouté au tableau Certificats.

Mise à jour d'un certificat

XenMobile n'autorise l'existence que qu'un seul certificat par clé publique dans le système à tout moment donné. Si vous essayez d'importer un certificat pour la même paire de clés qu'un certificat déjà importé, vous avez l'option de remplacer l'entrée existante ou de la supprimer.

Pour une mise à jour efficace de vos certificats, dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**, puis cliquez sur **Certificats**. Dans la boîte de dialogue **Importer**, importez le nouveau certificat.

Lorsque vous mettez un certificat de serveur à jour, les composants qui utilisaient le certificat précédent utilisent automatiquement le nouveau certificat. De même, si vous avez déployé le certificat de serveur sur les appareils, il sera

automatiquement mis à jour lors du prochain déploiement.

Gestion des certificats XenMobile

Nous vous recommandons d'effectuer le suivi des certificats que vous utilisez dans votre déploiement XenMobile, plus particulièrement leurs dates d'expiration et les mots de passe associés. Cette section vise à vous aider à faciliter la gestion des certificats dans XenMobile.

Votre environnement peut inclure certains ou tous les certificats suivants :

Serveur XenMobile
Certificat SSL pour nom de domaine complet MDM
Certificat SAML (pour ShareFile)
Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus et les autres ressources internes (StoreFront/Proxy, etc.)
Certificat APNS pour la gestion des appareils iOS
Certificat APNS interne pour les notifications Secure Hub du serveur XenMobile
Certificat utilisateur PKI pour la connectivité à PKI

MDX Toolkit
Certificat Apple Developer
Profil de provisioning Apple (par application)
Certificat APNS Apple (pour utilisation avec Citrix Secure Mail)
Fichier keystore Android
Windows Phone – Certificat Symantec

NetScaler
Certificat SSL pour nom de domaine complet MDM
Certificat SSL pour nom de domaine complet Gateway
Certificat SSL pour le nom de domaine complet des StorageZone Controller (SZC) ShareFile
Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
Certificat SSL pour l'équilibrage de charge StoreFront
Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

Stratégie d'expiration de certificat XenMobile

Si vous autorisez un certificat à expirer, le certificat n'est plus valide, et vous ne pouvez plus exécuter de transactions sécurisées dans votre environnement et vous ne pouvez pas accéder aux ressources XenMobile.

> ### Remarque
> L'autorité de certification (CA) vous invitera à renouveler votre certificat SSL avant la date d'expiration.

Certificat APNS pour Citrix Secure Mail

Étant donné que les certificats du service de notification push d'Apple (APNS) expirent chaque année, veillez à créer un nouveau certificat SSL pour le service APNS et à le mettre à jour dans le portail Citrix avant expiration.Si le certificat expire,

les utilisateurs rencontrent des problèmes avec les notifications push Secure Mail.De plus, vous ne pouvez plus envoyer de notifications push pour vos applications.

Certificat APNS pour la gestion des appareils iOS

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat APNS Apple.Si le certificat expire, les utilisateurs ne peuvent pas s'inscrire dans XenMobile et vous ne pouvez pas gérer leurs appareils iOS. Pour plus d'informations, consultez la section Certificats APNS.

Vous pouvez afficher l'état et la date d'expiration du certificat APNS en ouvrant une session sur le portail de certificats push Apple. Veillez à ouvrir une session avec les informations de l'utilisateur qui a créé le certificat.

Vous recevrez également une notification par e-mail d'Apple 30 et 10 jours avant la date d'expiration avec des informations similaires à ce qui suit :

« Le certificat du service de notification push d'Apple suivant, créé pour (identifiant AppleID identifiant client) va expirer le (date). La révocation ou l'expiration de ce certificat nécessitera la réinscription des appareils existants avec un nouveau certificat push.

Veuillez contacter votre fournisseur pour générer une nouvelle requête (CSR signée), puis visitez https://identity.apple.com/pushcert pour renouveler votre certificat Apple Push Notification Service.

Merci,

Apple Push Notification Service »

MDX Toolkit (certificat de distribution iOS)

Toute application exécutée sur un appareil iOS physique (autres que des applications dans l'App Store d'Apple) doit être signée avec un profil de provisioning et un certificat correspondant.

Pour vérifier que vous disposez d'un certificat de distribution iOS valide, procédez comme suit :

1. À partir du portail Apple Enterprise Developer, créez un ID d'application explicite pour chaque application que vous voulez wrapper avec le MDX Toolkit. Exemple d'ID d'application acceptable : com.NomEntreprise.NomProduit.
2. À partir du portail Apple Enterprise Developer, accédez à **Provisioning Profiles** > **Distribution** et créez un profil de provisioning interne. Répétez cette étape pour chaque ID d'application créé à l'étape précédente.
3. Téléchargez tous les profils de provisioning. Pour plus d'informations, consultez la section Wrapping des applications mobiles iOS.

Pour vérifier si tous les certificats du serveur XenMobile sont valides, procédez comme suit :

1. Dans la console XenMobile, cliquez sur **Paramètres** et sur **Certificats**.
2. Assurez-vous que tous les certificats y compris les certificats APNS, d'écoute SSL, racine et intermédiaire sont valides.

Keystore Android

Le keystore est un fichier qui contient les certificats utilisés pour signer votre application Android. Lorsque la période de validité de votre clé expire, les utilisateurs ne peuvent plus mettre à niveau vers les nouvelles versions de votre application.

Certificat d'entreprise de Symantec pour Windows Phone

Symantec est le fournisseur exclusif de certificats de signature de code du service Microsoft App Hub. Les développeurs et éditeurs de logiciels rejoignent le hub d'applications pour distribuer des applications Windows Phone et Xbox 360 à télécharger à l'aide de Windows Marketplace. Pour de plus amples informations, consultez la section Symantec Code Signing Certificates for Windows Phone dans la documentation Symantec.

Si le certificat expire, les utilisateurs de Windows Phone ne peuvent pas s'inscrire, installer une application publiée et signée par l'entreprise ou démarrer une application d'entreprise qui a été installée sur le téléphone.

NetScaler

Pour plus d'informations sur la gestion de l'expiration de certificat pour NetScaler, consultez la section How to handle certificate expiry on NetScaler dans le centre de connaissances du support Citrix.

Un certificat NetScaler qui a expiré empêche les utilisateurs de s'inscrire, d'accéder au magasin, de se connecter au serveur Exchange Server lors de l'utilisation de Secure Mail, et d'énumérer et d'ouvrir des applications HDX (en fonction du certificat qui a expiré).

Le Moniteur d'expiration et Command Center peuvent vous aider à effectuer le suivi de vos certificats NetScaler et vous informeront de l'expiration du certificat. Ces deux outils permettent de surveiller les certificats NetScaler suivants :

Certificat SSL pour nom de domaine complet MDM
Certificat SSL pour nom de domaine complet Gateway
Certificat SSL pour nom de domaine complet ShareFile SZC
Certificat SSL pour l'équilibrage de charge Exchange (configuration de déchargement)
SSL CertificateCertificat SSL pour l'équilibrage de charge StoreFront for StoreFront Load Balancing
Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus

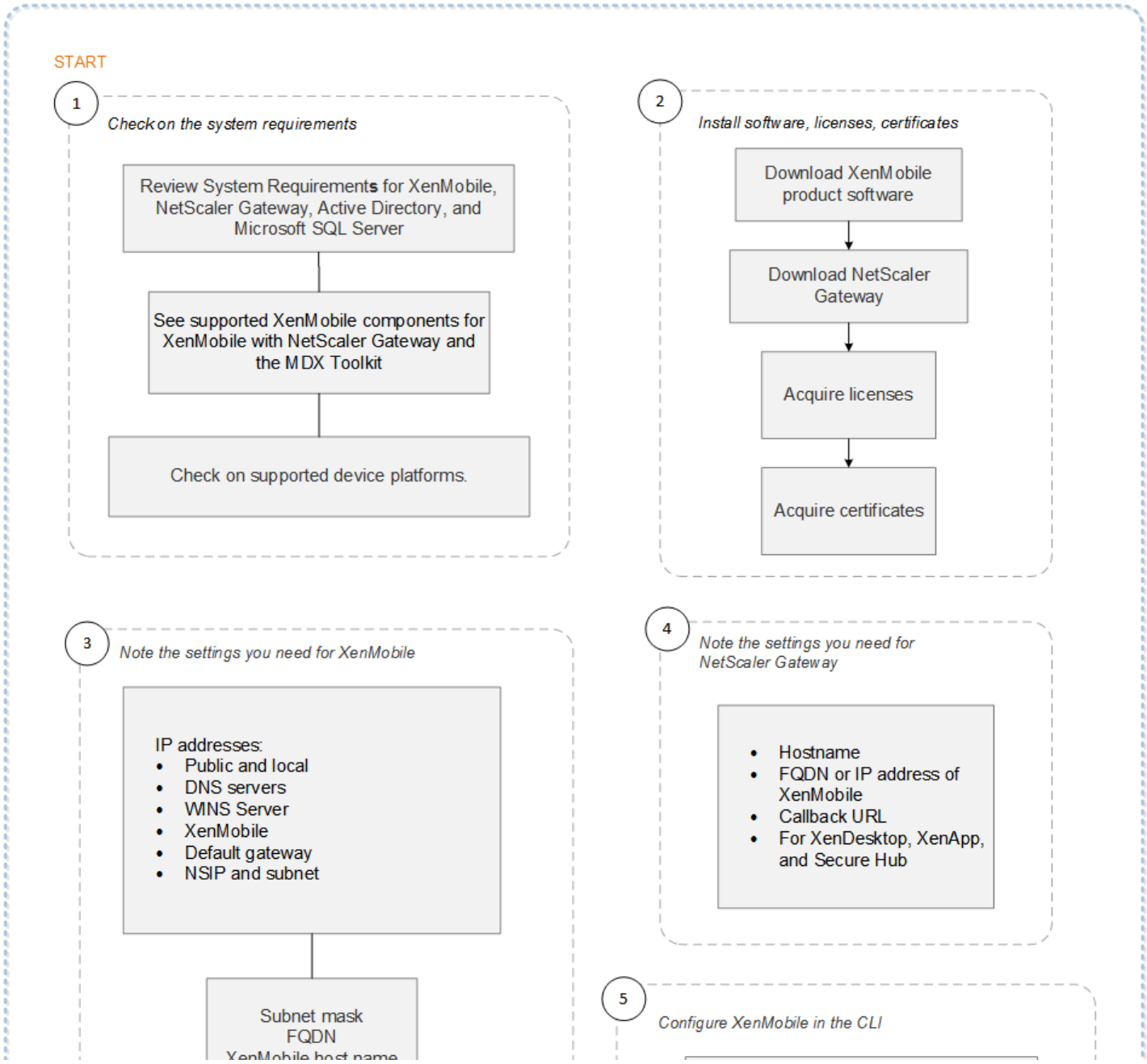
NetScaler Gateway et XenMobile

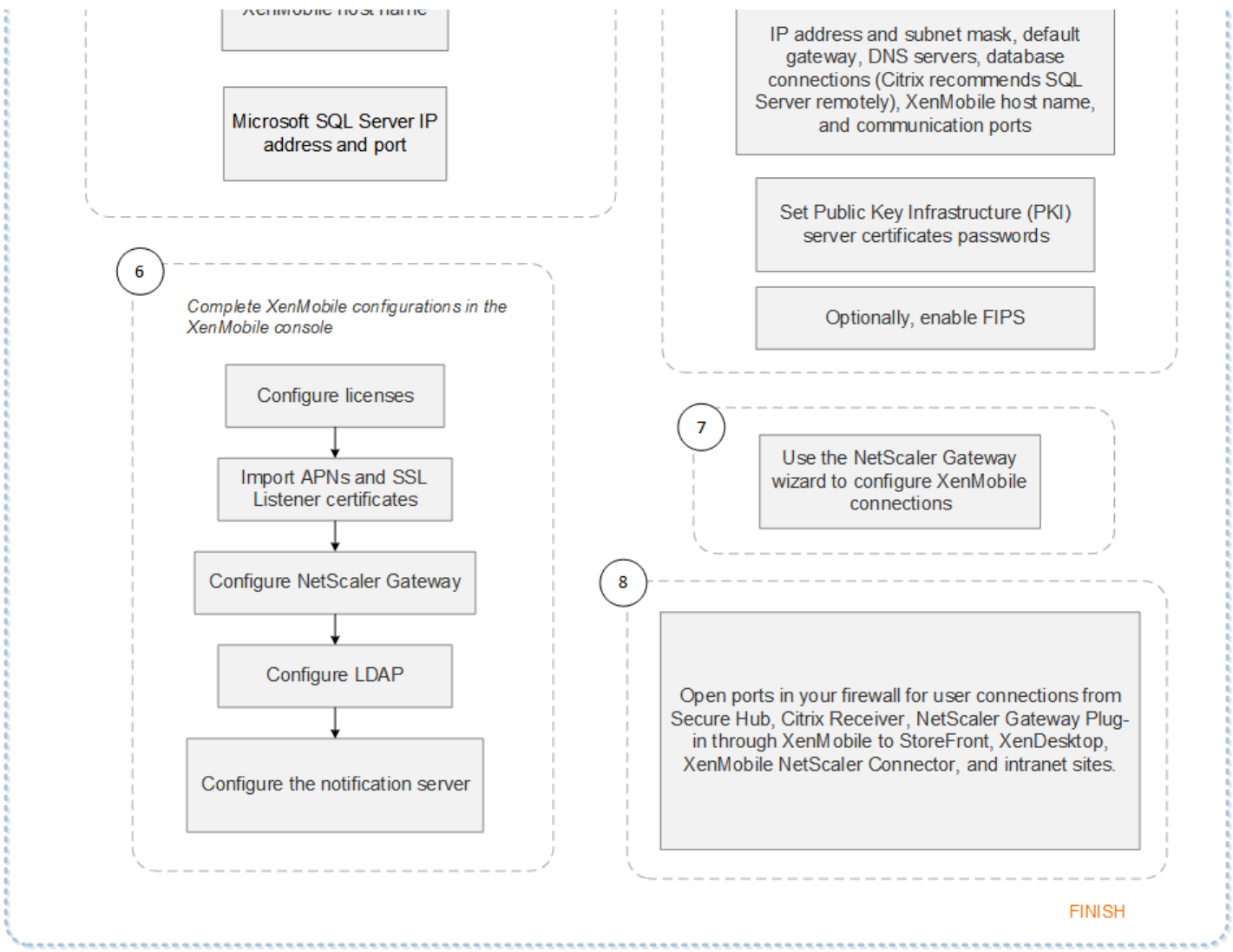
Feb 23, 2017

Lorsque vous configurez NetScaler Gateway à l'aide de XenMobile, vous établissez le mécanisme d'authentification utilisé par les appareils distants pour accéder au réseau interne. Cette fonctionnalité permet aux applications sur un appareil mobile d'accéder à des serveurs d'entreprise situés dans l'intranet en créant un micro VPN depuis les applications vers NetScaler Gateway sur l'appareil. Vous configurez NetScaler Gateway dans la console XenMobile, comme décrit dans cet article.

Organigramme pour le déploiement XenMobile avec NetScaler Gateway

Vous pouvez utiliser cet organigramme pour vous guider dans les étapes principales du déploiement XenMobile avec NetScaler Gateway. Vous trouverez des liens vers des rubriques liées à chaque étape après la figure.





1

- Configuration système requise et compatibilité

2

- Installer et configurer

3

- Checklist de pré-installation

4

- Checklist de pré-installation

5

- Configurer XenMobile dans la fenêtre d'invite de commande

6

- Configurer XenMobile dans un navigateur Web

7

- Configuration des paramètres de votre environnement XenMobile

8

- Ports

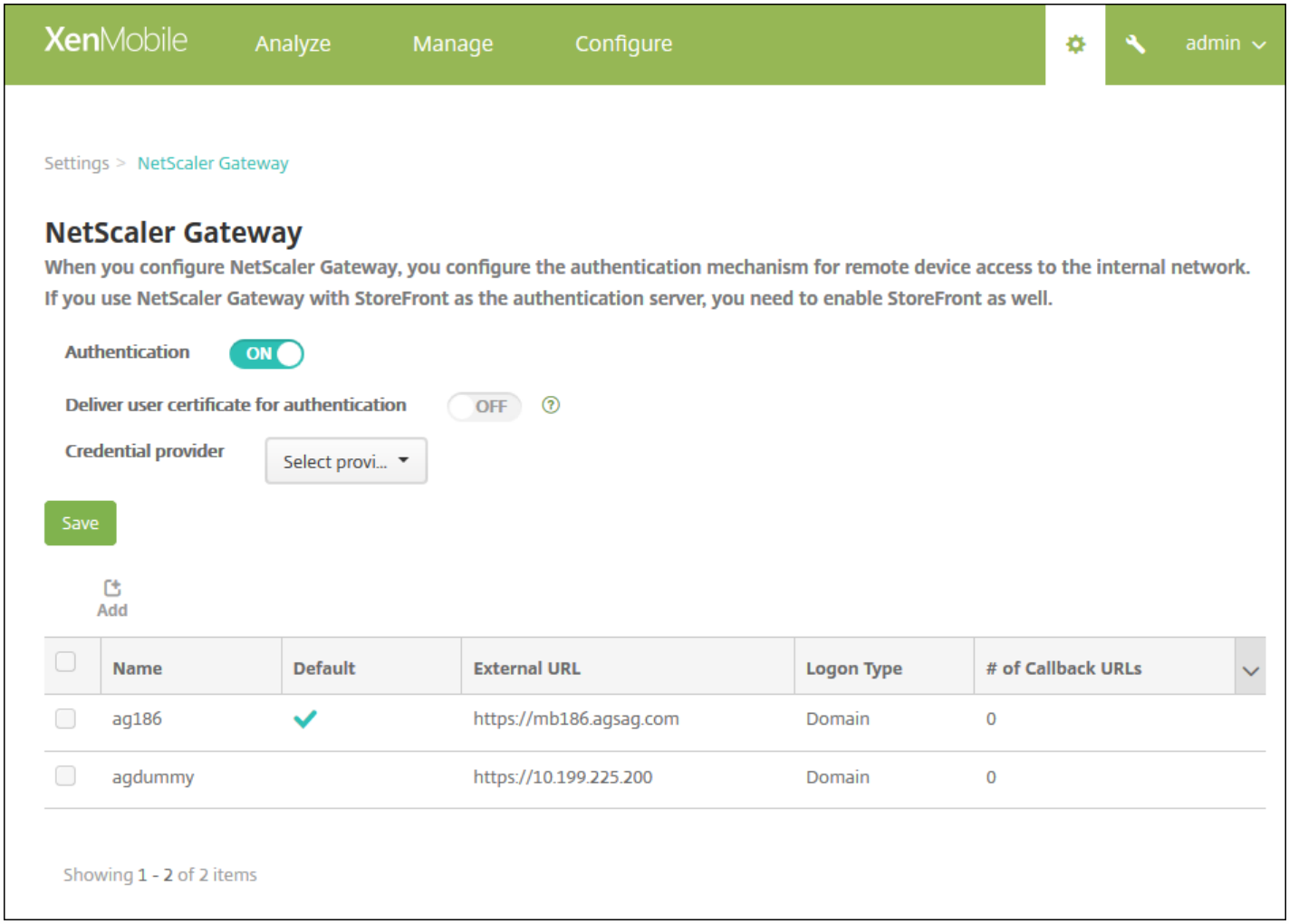
L'organigramme est également disponible au format PDF.

PDF Organigramme pour le déploiement de XenMobile

Pour configurer NetScaler Gateway

1. Dans la console Web XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **NetScaler Gateway**. La page **NetScaler Gateway** s'affiche.



Pour configurer ces paramètres :

- **Authentification** : sélectionnez cette option pour activer l'authentification. La valeur par défaut est **ON**.
- **Délivrer un certificat utilisateur pour l'authentification** : indiquez si vous voulez que XenMobile partage le certificat d'authentification avec Secure Hub afin que NetScaler Gateway gère l'authentification du certificat client. La valeur par défaut est **OFF**.
- **Fournisseur d'identités** : dans la liste, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseur d'identités.

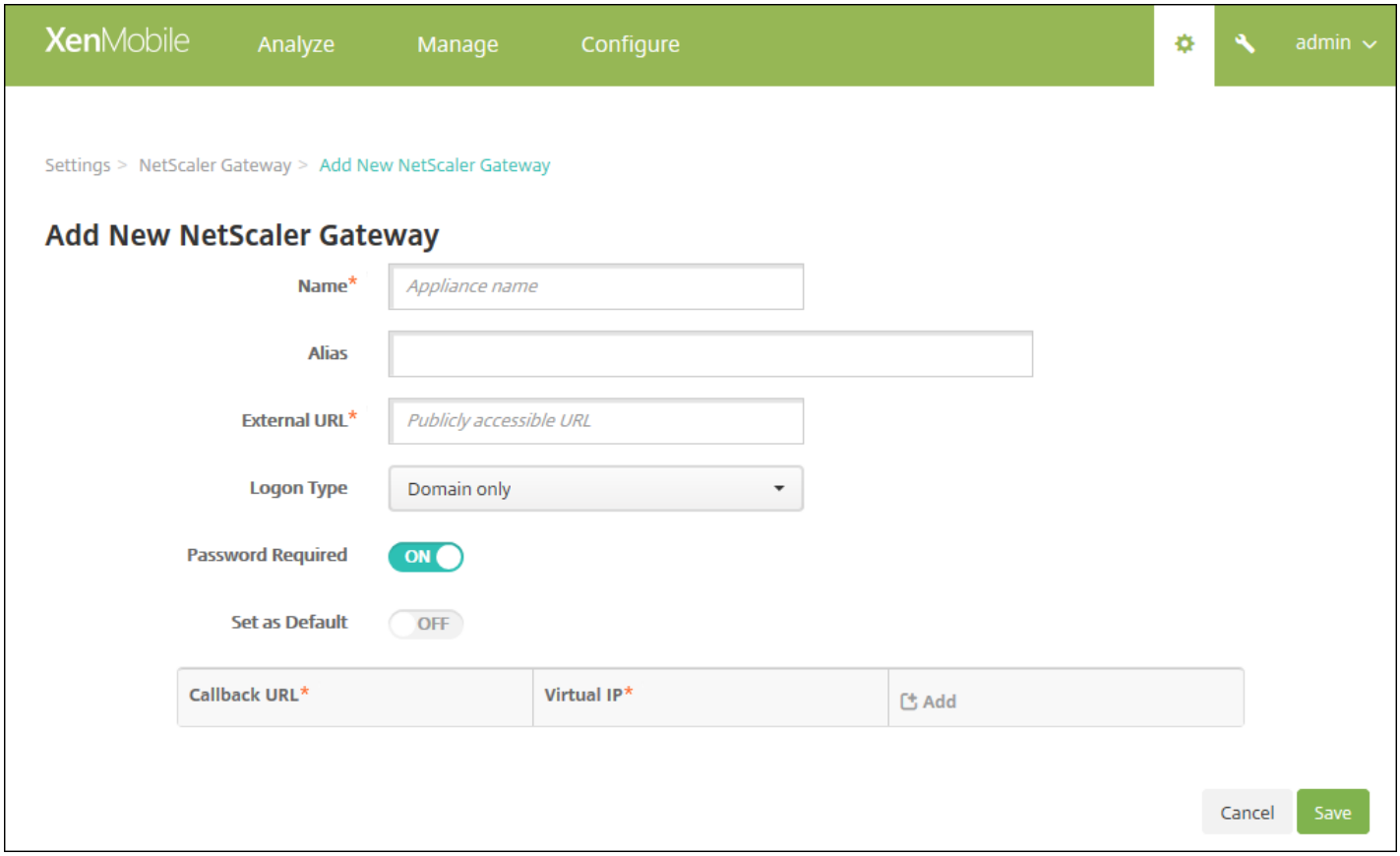
6. Cliquez sur **Enregistrer**.

Pour ajouter une nouvelle instance NetScaler Gateway

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.

2. Sous **Serveur**, cliquez sur **NetScaler Gateway**. La page **NetScaler Gateway** s'affiche.

3. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle passerelle NetScaler Gateway** s'affiche.



4. Configurez les paramètres suivants :

- **Nom** : entrez un nom pour l'instance NetScaler Gateway.
- **Alias** : entrez un alias (facultatif).
- **URL externe** : entrez l'adresse URL publiquement accessible de NetScaler Gateway. Par exemple, https://receiver.com.
- **Type d'ouverture de session**: cliquez sur un type d'ouverture de session dans la liste. Les types disponibles sont les suivants : **Domaine uniquement**, **Jeton de sécurité uniquement**, **Domaine et jeton de sécurité**, **Certificat**, **Certificat et domaine** et **Certificat et jeton de sécurité**. La valeur par défaut est **Domaine uniquement**.

  Si vous disposez de plusieurs domaines, **Domaine uniquement** ne fonctionnera pas, vous devez utiliser **Certificat et domaine**. Pour certaines options, par exemple **Domaine uniquement**, vous ne pouvez pas modifier le champ **Mot de passe**.

  Pour ce type d'ouverture de session, le champ est toujours **ON**. Par ailleurs, les valeurs par défaut pour le champ **Mot de passe requis** changent selon le **Type d'ouverture de session** sélectionné.

  Si vous utilisez **Certificat et jeton de sécurité**, une configuration supplémentaire est requise sur NetScaler Gateway pour la prise en charge de Secure Hub. Pour de plus amples informations, consultez la section Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité.
- **Mot de passe requis** : indiquez si vous souhaitez demander l'authentification par mot de passe. La valeur par défaut est **ON**.
- **Définir par défaut** : indiquez si cette passerelle NetScaler Gateway doit être utilisée par défaut. La valeur par défaut est **OFF**.

5. Cliquez sur **Enregistrer**. La nouvelle passerelle NetScaler Gateway est ajoutée et s'affiche dans le tableau. Vous pouvez modifier ou supprimer une instance en cliquant sur le nom dans la liste.

Après avoir ajouté l'instance NetScaler Gateway, vous pouvez ajouter une adresse URL de rappel et spécifier l'adresse IP virtuelle d'un VPN NetScaler Gateway. **Remarque :** la spécification d'une telle adresse est facultative, mais peut être configurée pour plus de sécurité, plus particulièrement lorsque le serveur XenMobile est dans la DMZ.

1. Dans l'écran NetScaler Gateway, sélectionnez la passerelle NetScaler Gateway dans le tableau et cliquez sur **Ajouter**. La page **Ajouter une nouvelle passerelle NetScaler Gateway** s'affiche.

2. Dans le tableau répertoriant les adresses URL de rappel, cliquez sur **Ajouter**.

3. Spécifiez l'URL de rappel. Ce champ représente le nom de domaine complet (FQDN) et vérifie que la demande émane de NetScaler Gateway. L'adresse URL de rappel doit être résolue en adresse IP accessible depuis le serveur XenMobile, mais elle n'a pas besoin d'être une URL NetScaler Gateway externe.

4. Entrez l'adresse IP virtuelle NetScaler Gateway et cliquez sur **Enregistrer**.

Authentification domaine ou domaine + jeton de sécurité

Feb 23, 2017

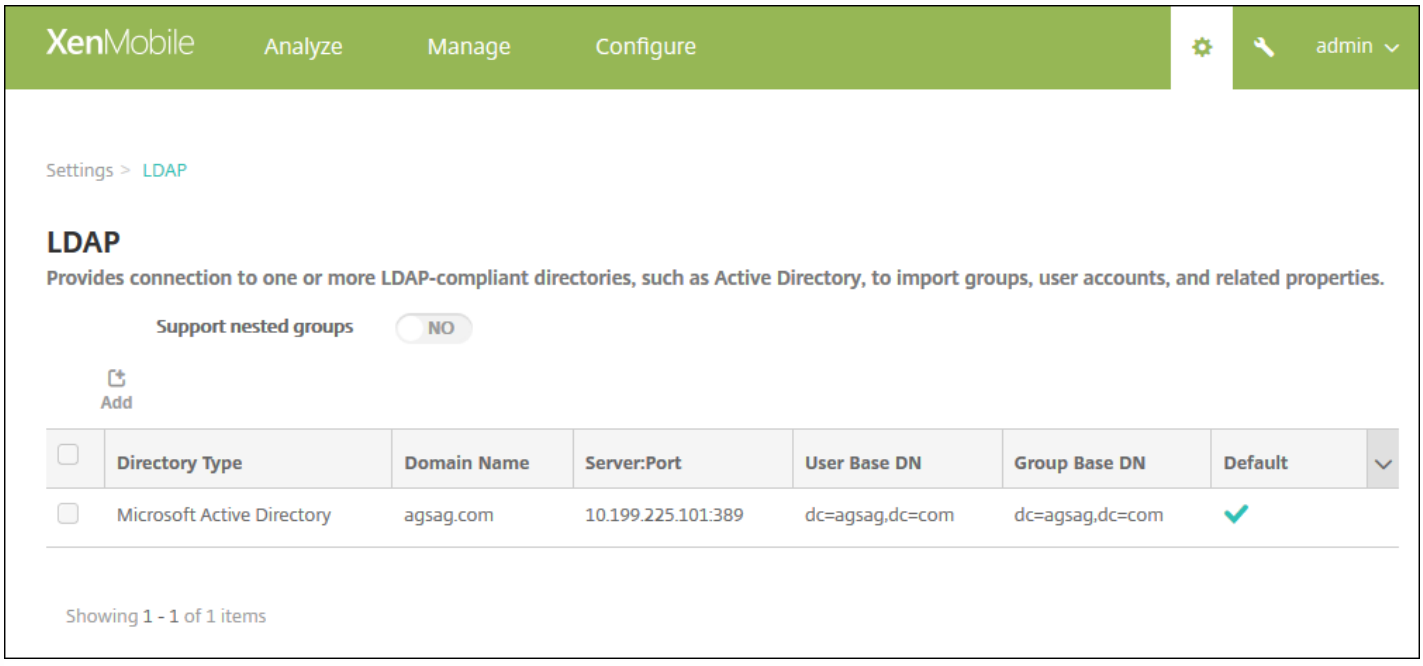
XenMobile prend en charge l'authentification basée sur domaine auprès d'un ou plusieurs annuaires, tels que Active Directory, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). Dans XenMobile, vous pouvez configurer une connexion à un ou plusieurs annuaires, puis utiliser la configuration LDAP pour importer des groupes, des comptes utilisateur et les propriétés correspondantes.

LDAP est un protocole applicatif indépendant open source qui permet d'accéder et de gérer les services d'informations d'annuaire distribués sur un réseau IP (Internet Protocol). Les services d'informations d'annuaire sont utilisés pour partager des informations sur les utilisateurs, les systèmes, les réseaux, les services et les applications disponibles sur le réseau. Une utilisation courante du protocole LDAP consiste à fournir une authentification unique (SSO) pour les utilisateurs, dans le cadre de laquelle un seul mot de passe (par utilisateur) est partagé entre plusieurs services, ce qui permet à un utilisateur d'ouvrir une seule session sur un site Web d'entreprise, et d'être automatiquement connecté à l'intranet d'entreprise.

Un client démarre une session LDAP en se connectant à un serveur LDAP, appelé DSA (Agent système d'annuaire). Le client envoie une demande d'opération au serveur et le serveur répond avec l'authentification appropriée.

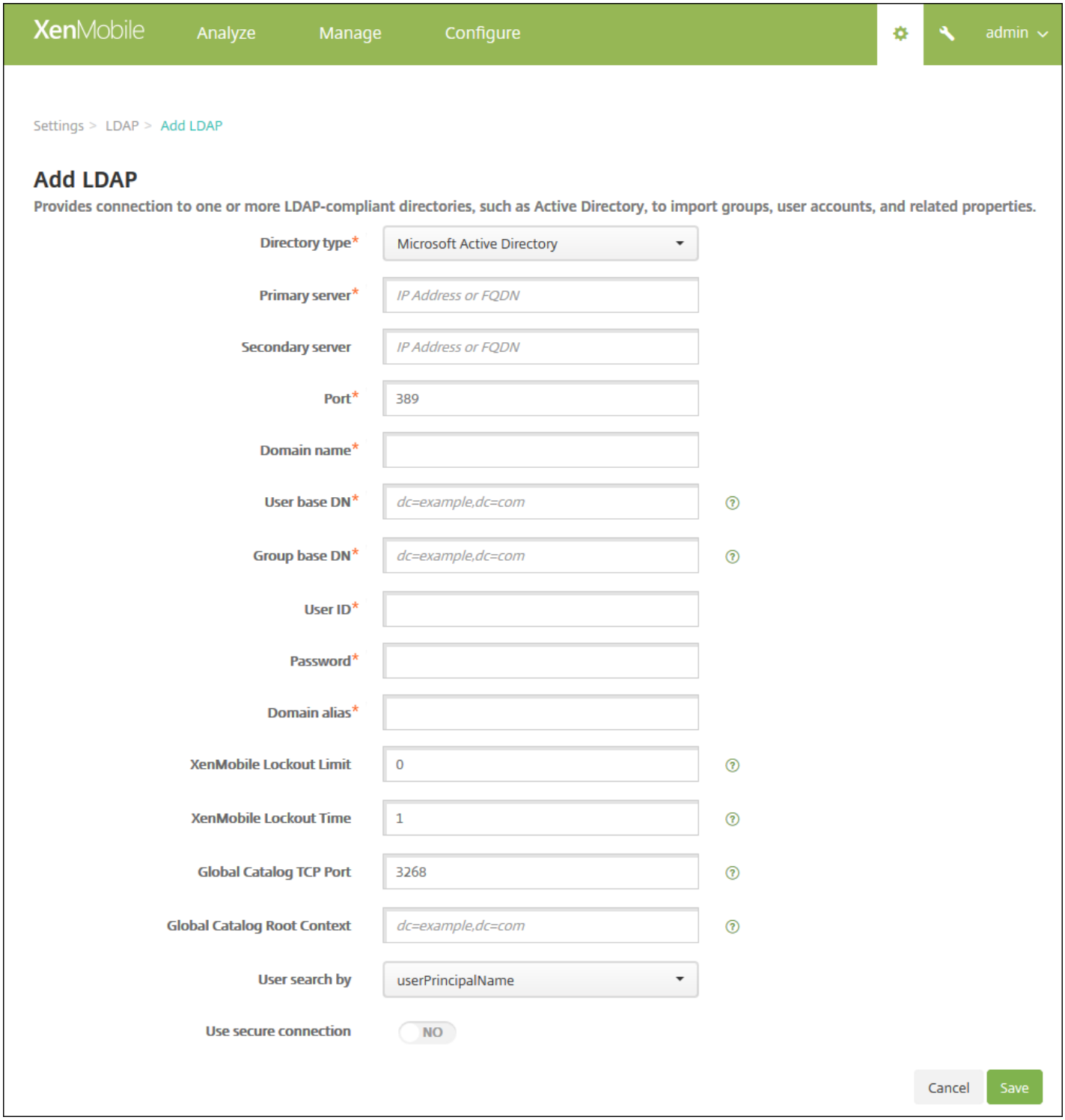
Pour ajouter des connexions LDAP dans XenMobile

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Serveur**, cliquez sur **LDAP**. La page **LDAP** s'affiche. Vous pouvez ajouter, modifier ou supprimer des annuaires compatibles LDAP à partir de cette page.



Pour ajouter un annuaire compatible LDAP

1. Sur la page **LDAP**, cliquez sur **Ajouter**. La page **Ajouter LDAP** s'affiche.



2. Pour configurer ces paramètres :

- **Type d'annuaire** : dans la liste, cliquez sur le type d'annuaire approprié. La valeur par défaut est **Microsoft Active Directory**.
- **Serveur principal** : entrez le serveur principal utilisé pour LDAP ; vous pouvez entrer l'adresse IP ou le nom de domaine complet (FQDN).
- **Serveur secondaire** : éventuellement, si un serveur secondaire a été configuré, entrez l'adresse IP ou le nom de domaine complet du serveur secondaire. Ce serveur est un serveur de basculement utilisé au cas où le serveur principal ne peut pas

être contacté.

- **Port** : entrez le numéro du port utilisé par le serveur LDAP. Par défaut, le numéro de port est défini sur 389 pour les connexions LDAP non sécurisées. Utilisez le numéro de port 636 pour les connexions LDAP sécurisées, 3268 pour les connexions LDAP non sécurisées Microsoft, ou 3269 pour les connexions LDAP sécurisées Microsoft.
- **Nom de domaine** : entrez le nom du domaine.
- **Nom unique de l'utilisateur de base** : entrez l'emplacement des utilisateurs dans Active Directory à l'aide d'un identificateur unique. Exemples de syntaxe : ou=utilisateurs, dc=exemple ou dc=com.
- **Nom unique du groupe de base** : entrez l'emplacement des groupes dans Active Directory. Par exemple, cn=users, dc=domain, dc=net où cn=users représente le nom de conteneur des groupes et dc représente le composant de domaine d'Active Directory.
- **ID utilisateur** : entrez l'ID de l'utilisateur associé au compte Active Directory.
- **Mot de passe** : entrez le mot de passe associé à l'utilisateur.
- **Alias de domaine** : entrez un alias pour le nom de domaine.
- **Limite de verrouillage de XenMobile** : entrez un nombre compris entre 0 et 999 pour le nombre d'échecs de tentatives d'ouverture de session. Si vous définissez ce champ sur 0, XenMobile ne verrouillera jamais l'utilisateur quel que soit le nombre de tentatives d'ouverture de session infructueuses.
- **Durée de verrouillage de XenMobile** : entrez un nombre compris entre 0 et 99 999 représentant le nombre de minutes pendant lesquelles un utilisateur doit patienter après avoir dépassé la limite de verrouillage. Si vous définissez ce champ sur 0, l'utilisateur n'est pas obligé d'attendre après un verrouillage.
- **Port TCP du catalogue global** : entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur 3268 ; pour les connexions SSL, utilisez le numéro de port 3269.
- **Base de recherche du catalogue global** : si vous le souhaitez, entrez la valeur de base de recherche globale utilisée pour activer une recherche du catalogue global dans Active Directory. Cette recherche est en supplément de la recherche LDAP standard, dans tout domaine sans avoir à spécifier le nom de domaine.
- **Recherche utilisateur par** : dans la liste, cliquez sur **userPrincipalName** ou **sAMAccountName**. La valeur par défaut est **userPrincipalName**.
- **Utiliser une connexion sécurisée** : indiquez si des connexions sécurisées doivent être utilisées. La valeur par défaut est **NO**.

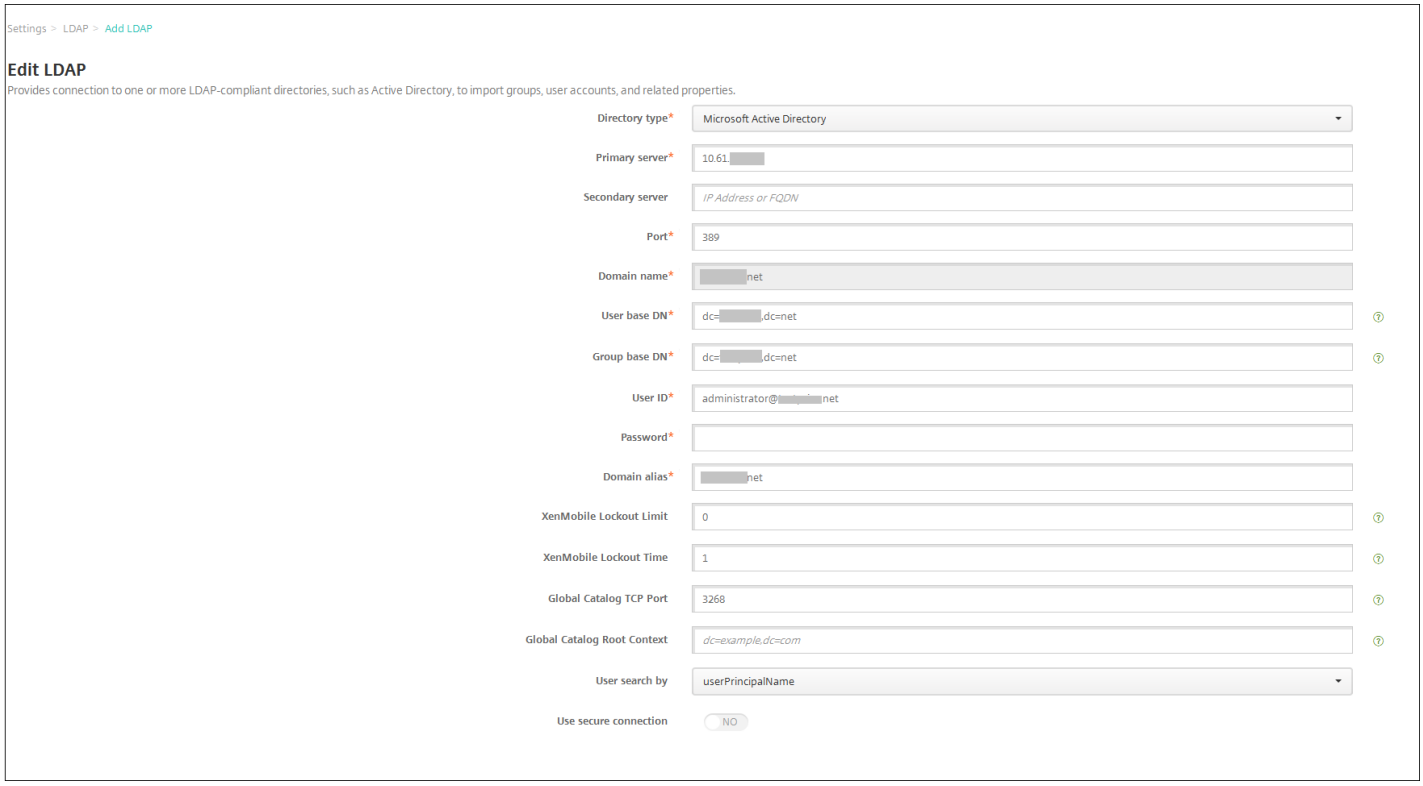
3. Cliquez sur **Enregistrer**.

Pour modifier un annuaire compatible LDAP

1. Dans le tableau **LDAP**, sélectionnez l'annuaire que vous souhaitez modifier.

   Remarque : lorsque vous sélectionnez la case à cocher en regard d'un annuaire, le menu d'options s'affiche au-dessus de la liste LDAP ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

2. Cliquez sur **Modifier**.La page **LDAP** s'affiche.



3. Modifiez les informations suivantes le cas échéant :

- **Type d'annuaire** : dans la liste, cliquez sur le type d'annuaire approprié.
- **Serveur principal** : entrez le serveur principal utilisé pour LDAP ; vous pouvez entrer l'adresse IP ou le nom de domaine complet (FQDN).
- **Serveur secondaire** : entrez l'adresse IP ou le nom de domaine complet du serveur secondaire (facultatif), si un tel serveur a été configuré.
- **Port** : entrez le numéro du port utilisé par le serveur LDAP. Par défaut, le numéro de port est défini sur 389 pour les connexions LDAP non sécurisées. Utilisez le numéro de port 636 pour les connexions LDAP sécurisées, 3268 pour les connexions LDAP non sécurisées Microsoft, ou 3269 pour les connexions LDAP sécurisées Microsoft.
- **Nom de domaine** : vous ne pouvez pas modifier ce champ.
- **Nom unique de l'utilisateur de base** : entrez l'emplacement des utilisateurs dans Active Directory à l'aide d'un identificateur unique. Exemples de syntaxe : ou=utilisateurs, dc=exemple ou dc=com.
- **Nom unique du groupe de base** : entrez le nom unique du groupe de base spécifié comme cn=nomgroupe. Par exemple, cn=utilisateurs, dc=nomserveur, dc=net où cn=utilisateurs est le nom du groupe ; le nom unique et nomserveur représentent le nom du serveur exécutant Active Directory.
- **ID utilisateur** : entrez l'ID de l'utilisateur associé au compte Active Directory.
- **Mot de passe** : entrez le mot de passe associé à l'utilisateur.
- **Alias de domaine** : entrez un alias pour le nom de domaine.
- **Limite de verrouillage de XenMobile** : entrez un nombre compris entre 0 et 999 pour le nombre d'échecs de tentatives d'ouverture de session. Si vous définissez ce champ sur 0, XenMobile ne verrouillera jamais l'utilisateur quel que soit le nombre de tentatives d'ouverture de session infructueuses.
- **Durée de verrouillage de XenMobile** : entrez un nombre compris entre 0 et 99 999 représentant le nombre de minutes pendant lesquelles un utilisateur doit patienter après avoir dépassé la limite de verrouillage. Si vous définissez ce champ sur 0, l'utilisateur n'est pas obligé d'attendre après un verrouillage.

- **Port TCP du catalogue global** : entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur 3268 ; pour les connexions SSL, utilisez le numéro de port 3269.
- **Base de recherche du catalogue global** : si vous le souhaitez, entrez la valeur de base de recherche globale utilisée pour activer une recherche du catalogue global dans Active Directory. Cette recherche est en supplément de la recherche LDAP standard, dans tout domaine sans avoir à spécifier le nom de domaine.
- **Recherche utilisateur par** : dans la liste, cliquez sur **userPrincipalName** ou **sAMAccountName**.
- **Utiliser une connexion sécurisée** : indiquez si des connexions sécurisées doivent être utilisées.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer un annuaire compatible LDAP

1. Dans le tableau **LDAP**, sélectionnez l'annuaire que vous souhaitez supprimer.

   Remarque : vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Configurer l'authentification domaine + jeton de sécurité

Vous pouvez configurer XenMobile de manière à obliger les utilisateurs à s'authentifier avec leurs informations d'identification LDAP plus un mot de passe à usage unique, à l'aide du protocole RADIUS.

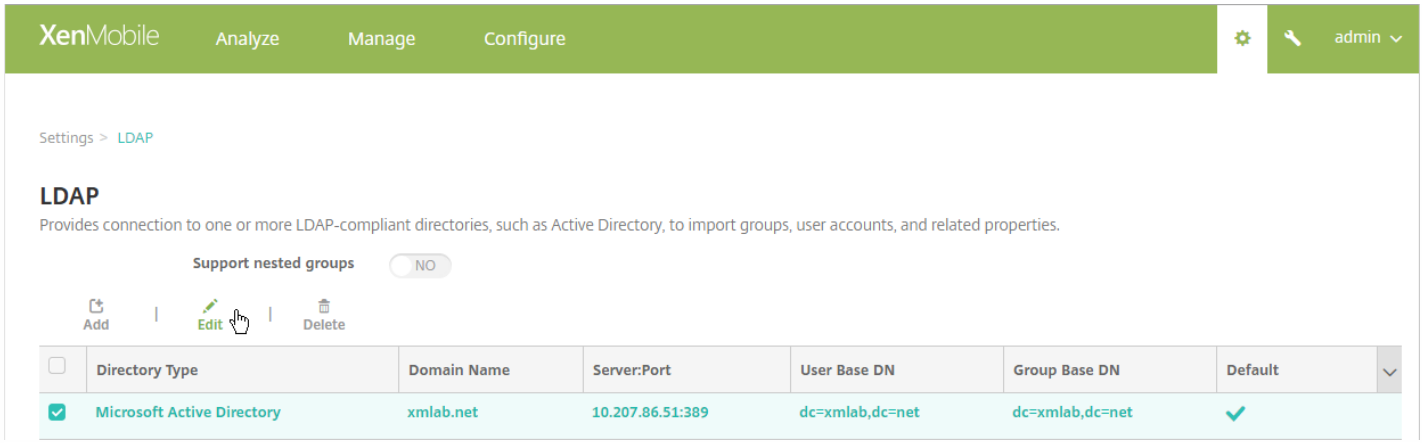
Pour une utilisabilité optimale, vous pouvez combiner cette configuration avec un code PIN Citrix et la mise en cache du mot de passe Active Directory de façon à ce que les utilisateurs n'aient pas à entrer de manière répétée leur nom d'utilisateur et mot de passe Active Directory. Les utilisateurs devront entrer leurs noms et mots de passe lors de l'inscription, de l'expiration du mot de passe et du verrouillage du compte.

Configurer les paramètres LDAP

L'utilisation de LDAP pour l'authentification nécessite que vous installiez un certificat SSL d'une autorité de certification sur XenMobile. Pour de plus amples informations, consultez la section Chargement de certificats dans XenMobile.

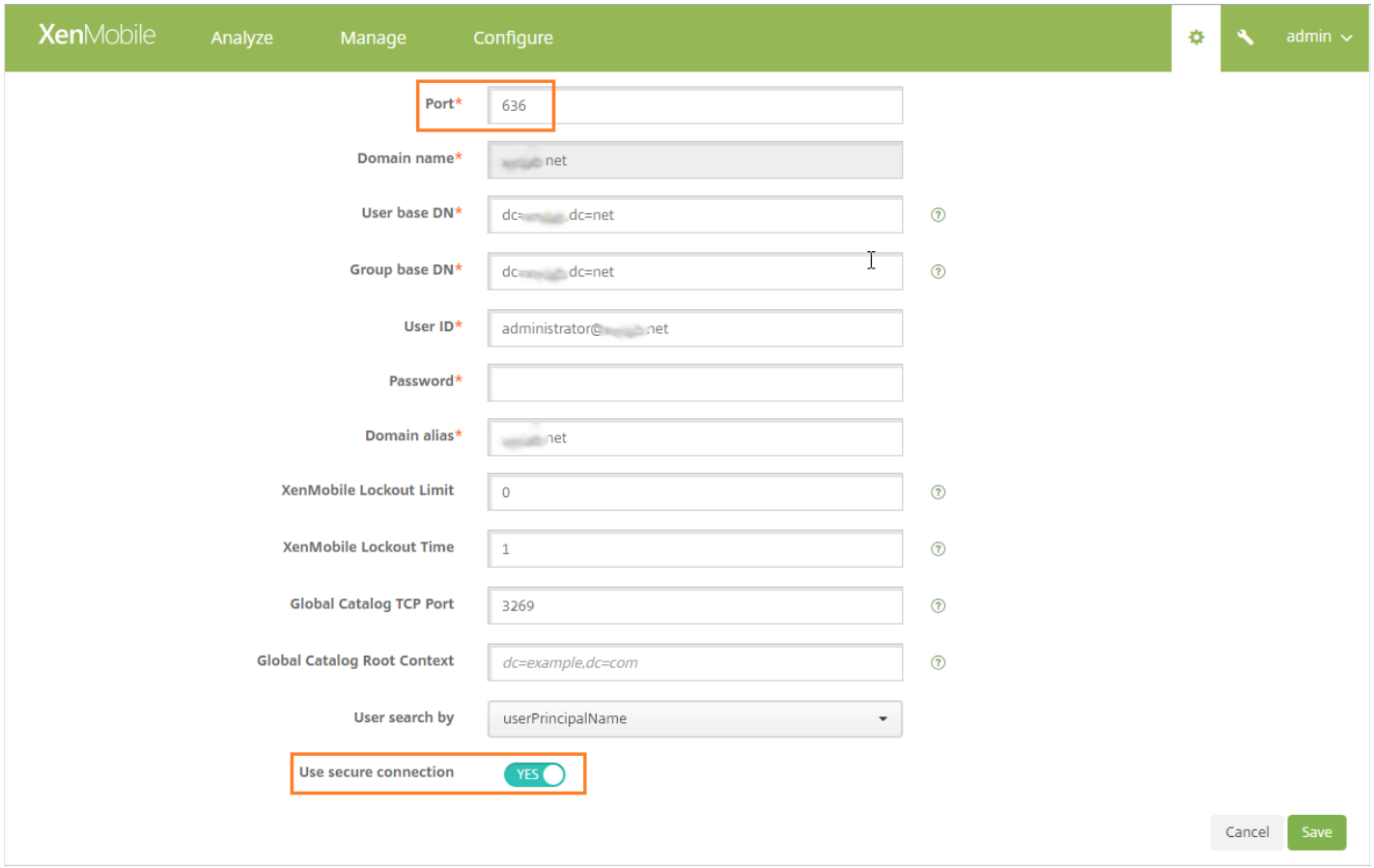
1. Dans **Paramètres**, cliquez sur **LDAP**.

2. Sélectionnez **Microsoft Active Directory** et cliquez sur **Modifier**.



3. Vérifiez que le port Port est 636 pour les connexions LDAP sécurisées ou 3269 pour les connexions LDAP sécurisées Microsoft.

4. Changez **Utiliser une connexion sécurisée** sur **Oui**.



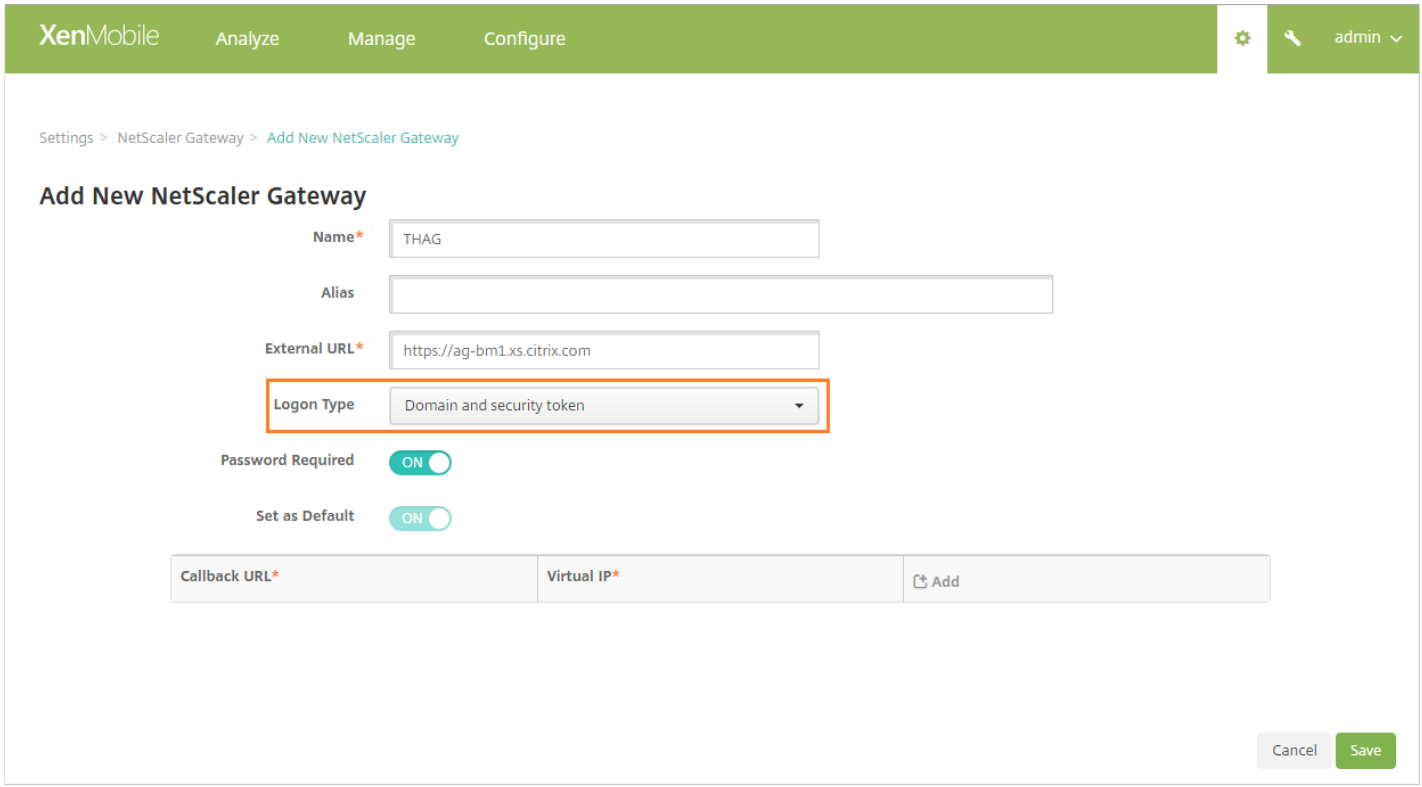
Configurer les paramètres de NetScaler Gateway

Les étapes suivantes supposent que vous avez déjà ajouté une instance NetScaler Gateway à XenMobile. Pour ajouter une instance NetScaler Gateway, consultez la section Pour configurer une nouvelle instance NetScaler Gateway.

1. Dans **Paramètres**, cliquez sur **NetScaler Gateway**.

2. Sélectionnez le **NetScaler Gateway** et cliquez sur **Modifier**.

3. Depuis **Type d'ouverture de session**, sélectionnez **Domaine et jeton de sécurité**.



Activer le code PIN Worx et la mise en cache du mot de passe de l'utilisateur

Pour activer le code PIN Worx et la mise en cache du mot de passe de l'utilisateur, accédez à **Paramètres > Propriétés du client** et sélectionnez les cases **Activer l'authentification par code PIN Worx** et **Activer la mise en cache du mot de passe de l'utilisateur**. Pour de plus amples informations, consultez la section Propriétés du client.

Configurer NetScaler Gateway pour l'authentification par jeton de sécurité et domaine

Configurez des profils de sessions NetScaler Gateway et des stratégies pour les serveurs virtuels que vous utilisez avec XenMobile. Pour de plus amples informations, consultez la section Configuration de l'authentification par jeton de sécurité et domaine pour XenMobile dans la documentation de NetScaler Gateway.

Authentification certificat client ou certificat + domaine

Mar 31, 2017

La configuration par défaut pour XenMobile est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l'environnement XenMobile, vous pouvez utiliser l'authentification basée sur certificats. Dans l'environnement XenMobile, cette configuration est la meilleure combinaison de sécurité et d'expérience utilisateur : vous disposez des meilleures solutions d'authentification unique (SSO) couplées à une sécurité assurée par l'authentification à deux facteurs sur NetScaler.

Si vous n'autorisez pas LDAP et utilisez des cartes à puce ou méthodes similaires, la configuration des certificats vous permet de représenter une carte à puce auprès de XenMobile. Les utilisateurs s'inscrivent alors à l'aide d'un code PIN unique généré par XenMobile. Une fois qu'un utilisateur a accès, XenMobile crée et déploie le certificat utilisé ensuite pour s'authentifier auprès de l'environnement XenMobile.

Vous pouvez utiliser l'assistant NetScaler pour XenMobile pour procéder à la configuration requise pour XenMobile lors de l'utilisation de l'authentification par certificat NetScaler ou certificat + domaine. Vous ne pouvez exécuter l'assistant NetScaler pour XenMobile qu'une seule fois.

Dans les environnements hautement sécurisés où l'utilisation d'informations d'identification LDAP en dehors d'une organisation dans des réseaux publics ou non sécurisés est considérée comme une menace de sécurité majeure pour l'entreprise, il est possible d'opter pour l'authentification à deux facteurs à l'aide d'un certificat client et d'un jeton de sécurité. Pour de plus amples informations, consultez la section Configuration de XenMobile pour l'authentification par certificat et jeton de sécurité.

L'authentification du certificat client est disponible pour le mode XenMobile MAM (MAM exclusif) et le mode ENT (lorsque les utilisateurs s'inscrivent dans MDM). L'authentification du certificat client n'est pas disponible pour le mode XenMobile ENT lorsque les utilisateurs s'inscrivent dans l'ancien mode MAM. Pour utiliser l'authentification du certificat client dans les modes XenMobile ENT et MAM, vous devez configurer le serveur Microsoft, le serveur XenMobile et NetScaler Gateway. Suivez ces étapes générales, décrites dans cet article.

Sur le serveur Microsoft :

1. Ajoutez un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console.
2. Ajoutez le modèle à l'autorité de certification (CA).
3. Créez un certificat PFX depuis le serveur CA.

Sur le serveur XenMobile :

1. Chargez le certificat sur XenMobile.
2. Créez l'entité PKI pour l'authentification par certificat.
3. Configurez les fournisseurs d'informations d'identification.
4. Configurez NetScaler Gateway afin de fournir un certificat utilisateur pour l'authentification.

Sur NetScaler Gateway, effectuez la configuration décrite dans Configuration de l'authentification certificat client ou certificat client + domaine dans la documentation NetScaler Gateway.

Conditions préalables

- Pour les appareils Windows Phone 8.1 utilisant l'authentification du certificat client et le déchargement SSL, vous devez désactiver la réutilisation de session SSL pour le port 443 sur les serveurs virtuels d'équilibrage de charge dans NetScaler. Pour ce faire, exécutez la commande suivante sur les serveurs virtuels pour le port 443 :

  set ssl vserver sessReuse DISABLE

  Remarque : la désactivation de la réutilisation de la session SSL désactive certaines des optimisations fournies par NetScaler, ce qui peut entraîner une diminution des performances sur NetScaler.

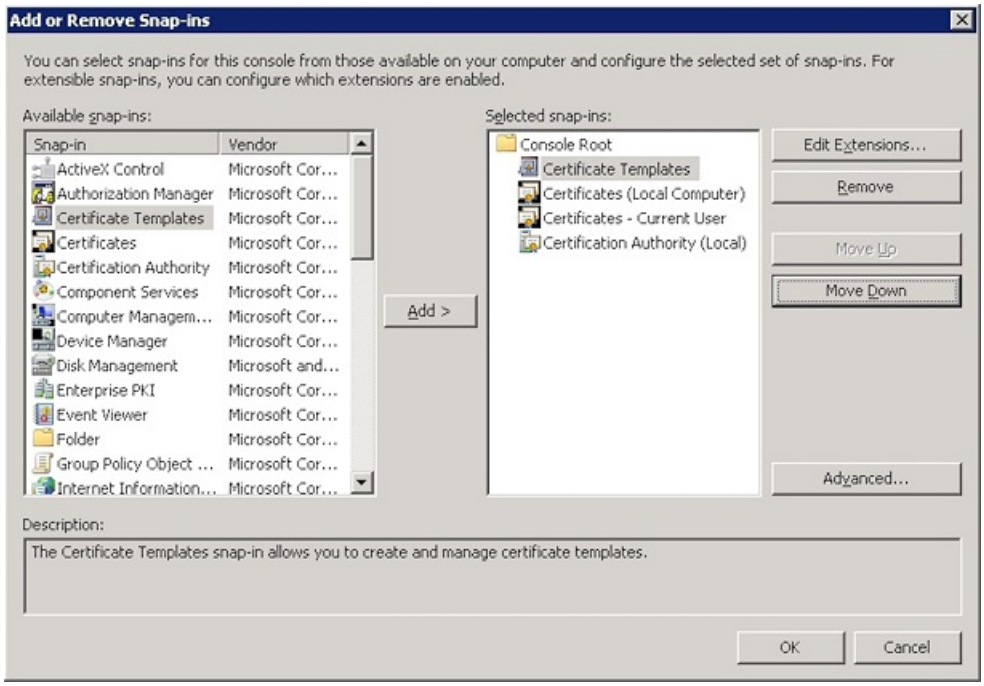
- Pour configurer l'authentification basée sur certificat pour Exchange ActiveSync, consultez le blog de Microsoft.
- Si vous utilisez des certificats de serveur privé pour sécuriser le trafic ActiveSync avec le serveur Exchange, assurez-vous que tous les certificats racine et intermédiaires ont été installés sur les appareils mobiles. Sinon, l'authentification basée sur certificat échouera lors de la configuration de la boîte aux lettres dans Secure Mail. Dans la console Exchange IIS, vous devez :
  - Ajouter un site Web à utiliser par XenMobile avec Exchange et lier le certificat de serveur Web.
  - Utiliser le port 9443.
  - Pour ce site Web, vous devez ajouter deux applications, une pour « Microsoft-Server-ActiveSync » et une pour « EWS ». Pour ces deux applications, sous **Paramètres SSL**, sélectionnez **Exiger SSL**.
- Assurez-vous que Secure Mail pour iOS, Android, et Windows Phone sont wrappés avec la dernière version du MDX Toolkit.

Ajout d'un composant logiciel enfichable pour les certificats dans la console Microsoft Management Console

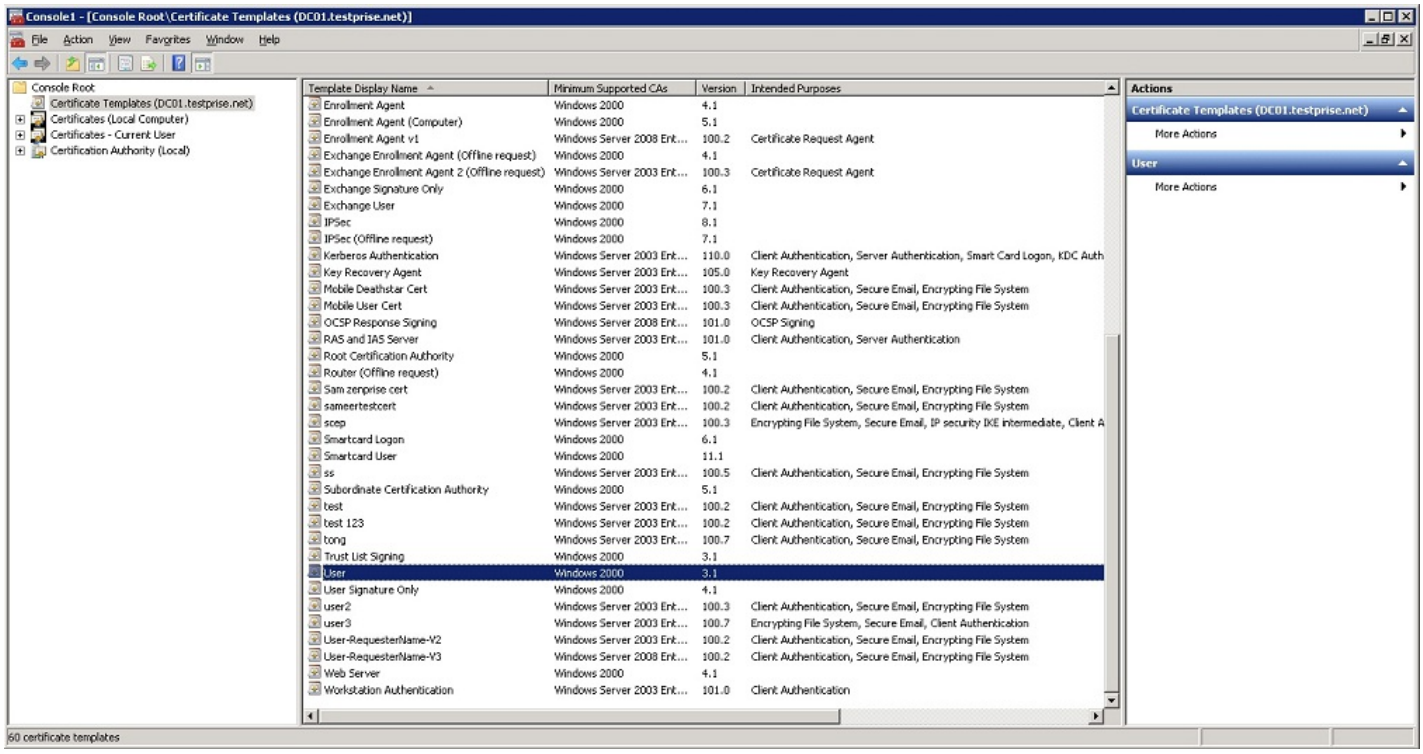
1. Ouvrez la console et cliquez sur **Ajouter/Supprimer un composant logiciel enfichable**.

2. Ajoutez les composants logiciels enfichables suivants :

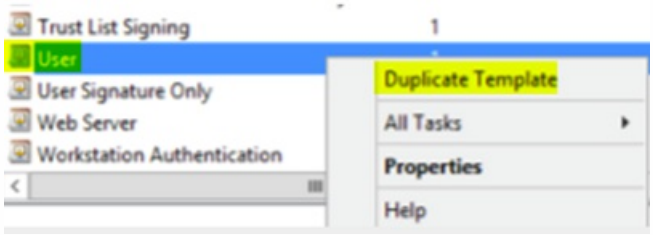
   Modèles de certificats
   Certificats (ordinateur Local)
   Certificats - Utilisateur actuel
   Autorité de certification (locale)



3. Développez **Modèles de certificats**.



4. Sélectionnez le modèle **Utilisateur** et **Dupliquer le modèle**.

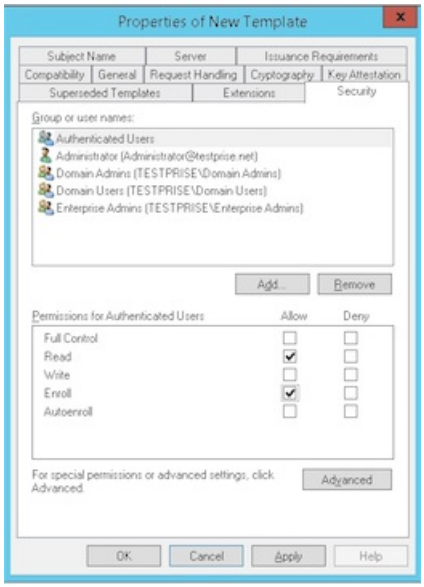


5. Fournissez le nom du modèle.

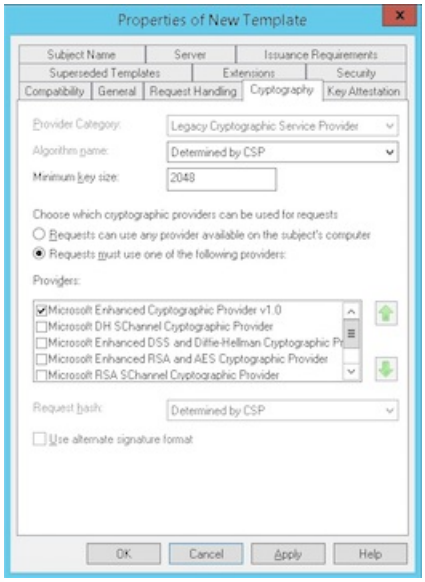
> **Important** : ne sélectionnez pas la case **Publier le certificat dans Active Directory** sauf si cela est nécessaire. Si cette option est sélectionnée, tous les certificats client utilisateur seront émis/créés dans Active Directory, ce qui pourrait encombrer votre base de données Active Directory.

6. Sélectionnez **Windows 2003 Server** comme type de modèle.Dans Windows 2012 R2 Server, sous **Compatibilité**, sélectionnez **Autorité de certification** et définissez le destinataire en tant que **Windows 2003**.

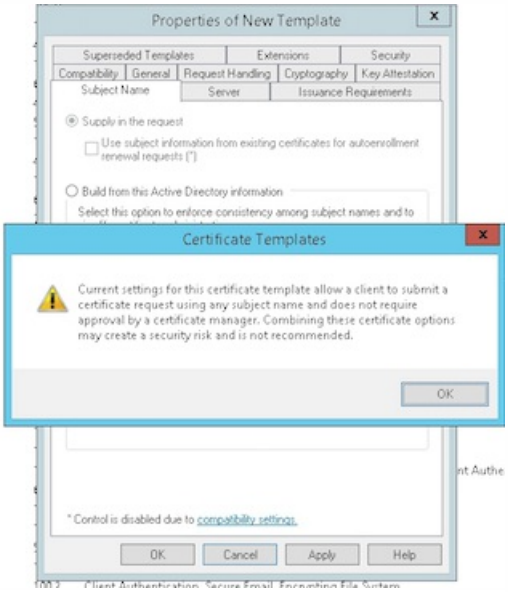
7. Sous **Sécurité**, sélectionnez l'option **Inscrire** dans la colonne **Autoriser** pour les utilisateurs authentifiés.



8. Sous **Cryptographie**, n'oubliez pas de fournir la taille de clé, que vous devrez entrer lors de la configuration de XenMobile.



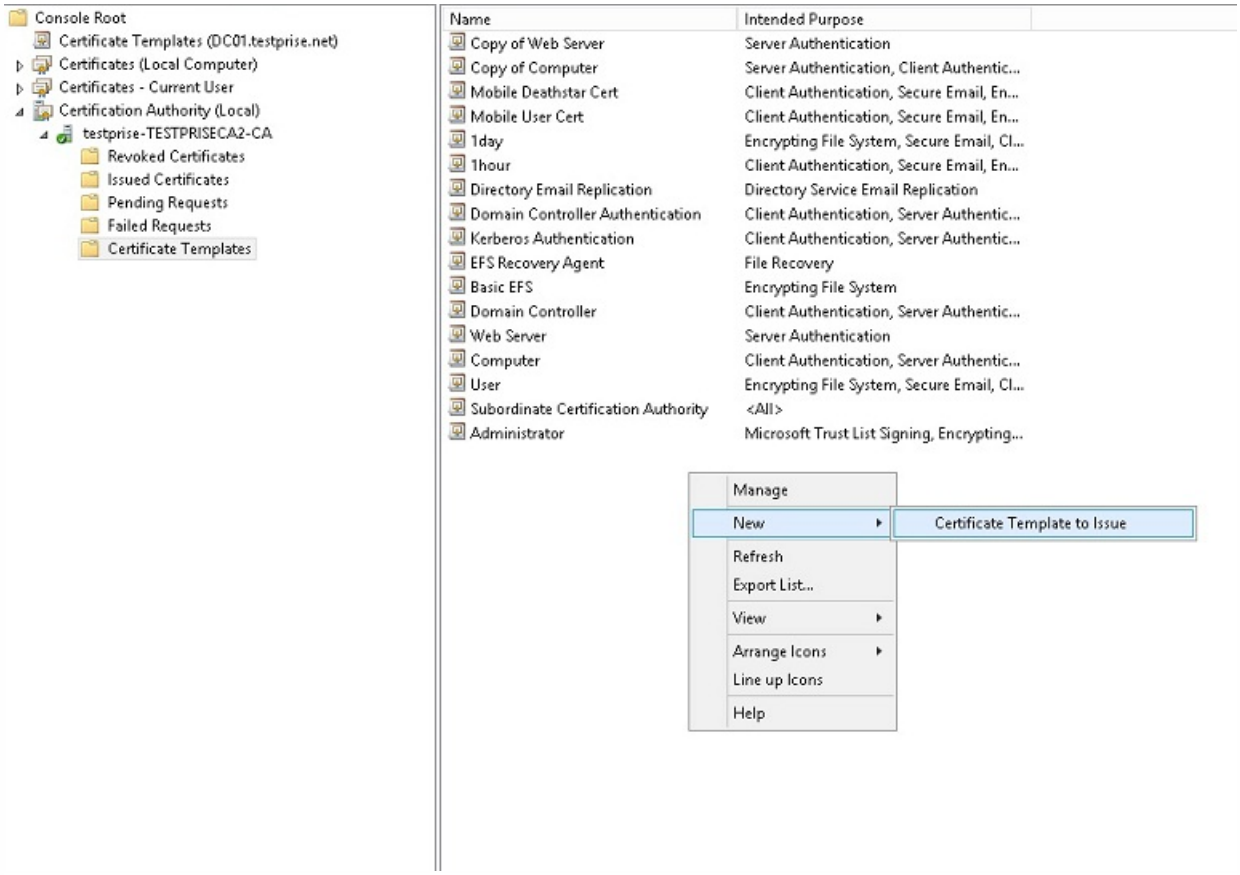
9. Sous **Nom du sujet**, sélectionnez **Fournir dans la demande**. Appliquez les modifications et enregistrez.



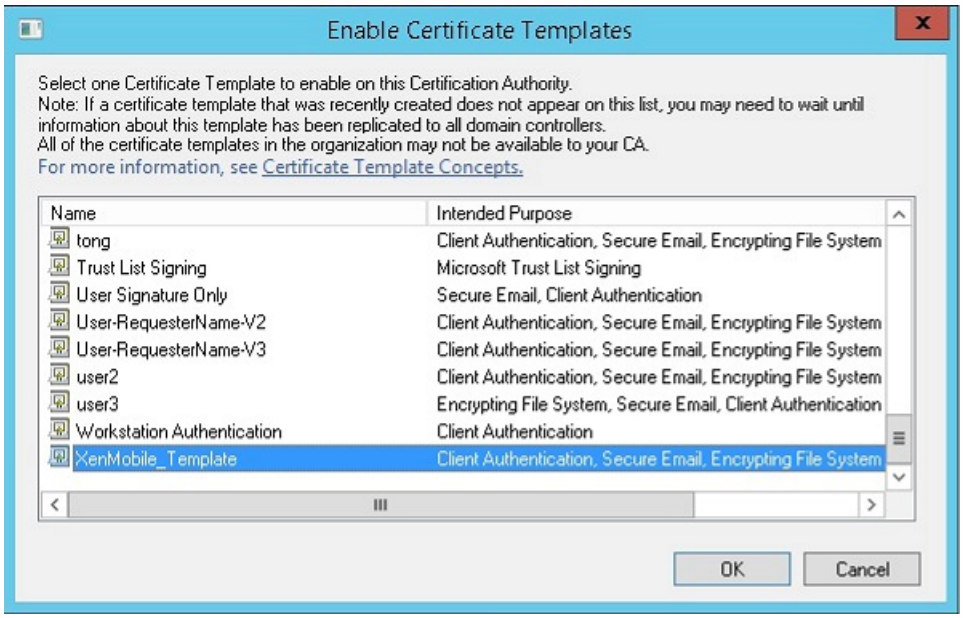
Ajout du modèle à l'autorité de certification (CA)

1. Accédez à **Autorité de certification** et sélectionnez **Modèles de certificats**.

2. Cliquez avec le bouton droit dans le panneau de droite et sélectionnez **Nouveau > Modèle de certificat à délivrer**.



3. Sélectionnez le modèle que vous avez créé à l'étape précédente et cliquez sur **OK** pour l'ajouter à l'**autorité de certification**.

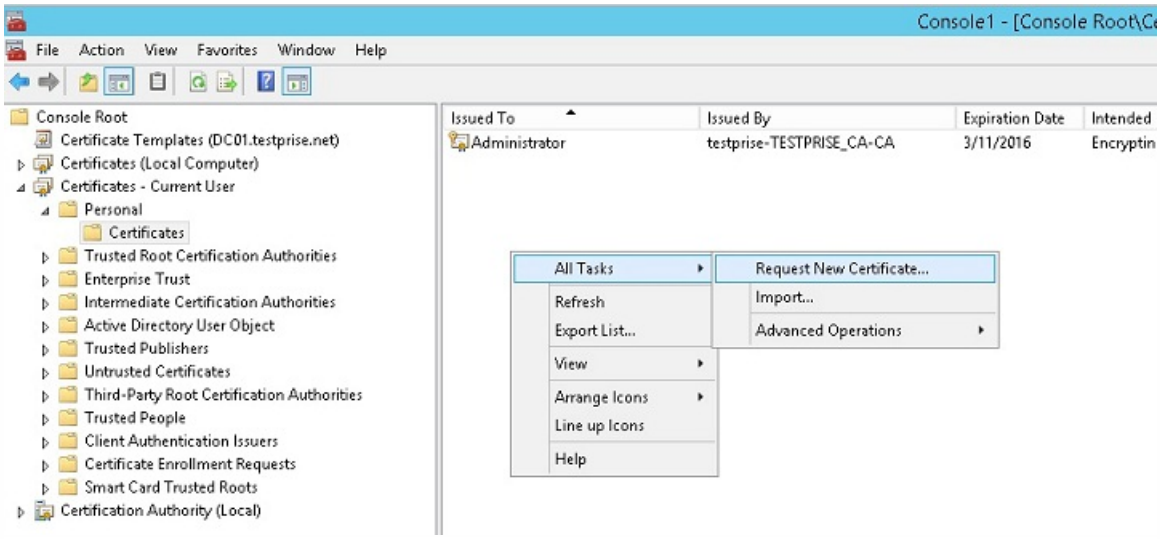


Création d'un certificat PFX depuis le serveur CA

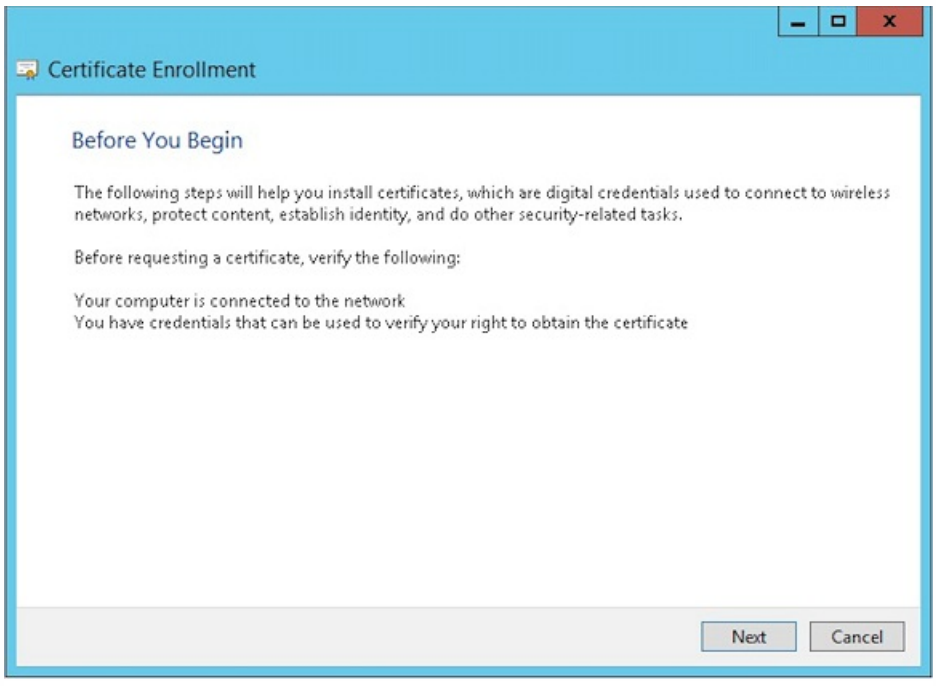
1. Créez un certificat utilisateur .pfx à l'aide du compte de service avec lequel vous vous êtes connecté. Ce fichier .pfx sera chargé dans XenMobile, qui demandera un certificat utilisateur de la part des utilisateurs qui inscrivent leurs appareils.

2. Sous **Utilisateur actuel**, développez **Certificats**.

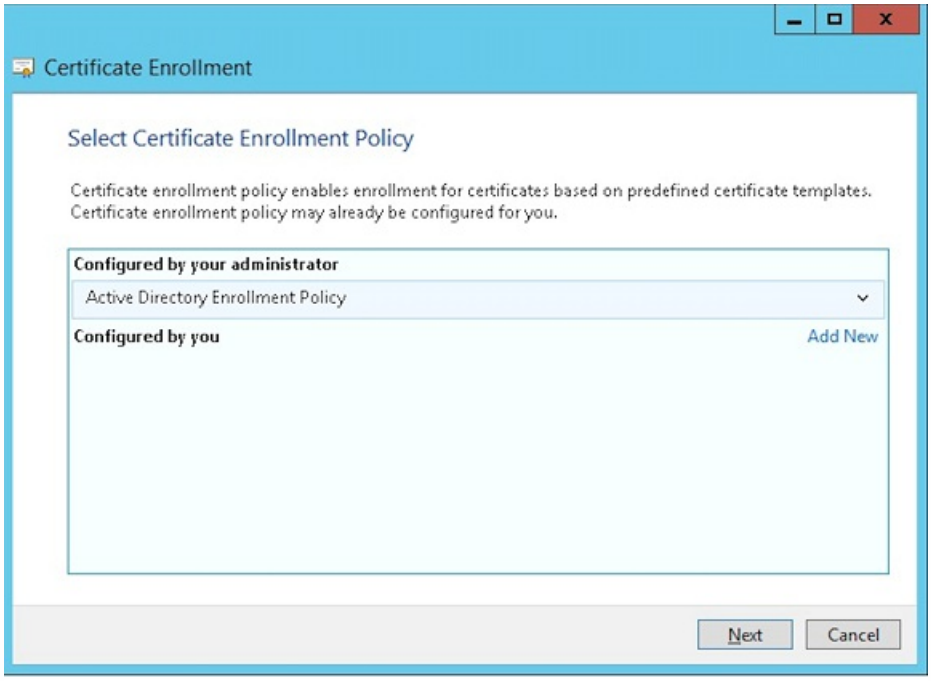
3. Cliquez avec le bouton droit dans le panneau de droite et cliquez sur **Demander un nouveau certificat**.



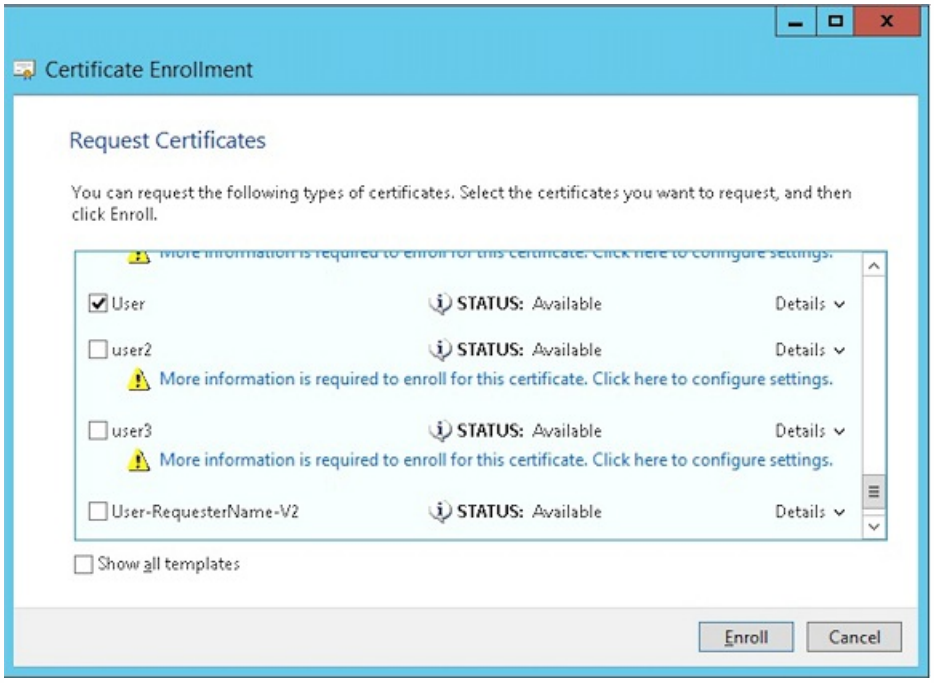
4. L'écran **Inscription de certificats** s'affiche. Cliquez sur **Suivant**.



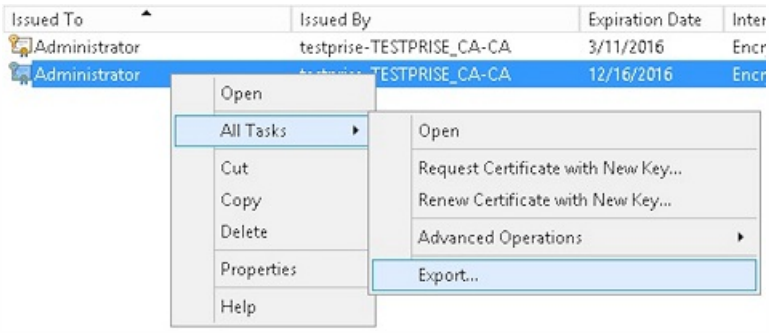
5. Sélectionnez **Stratégie d'inscription à Active Directory** et cliquez sur **Suivant**.



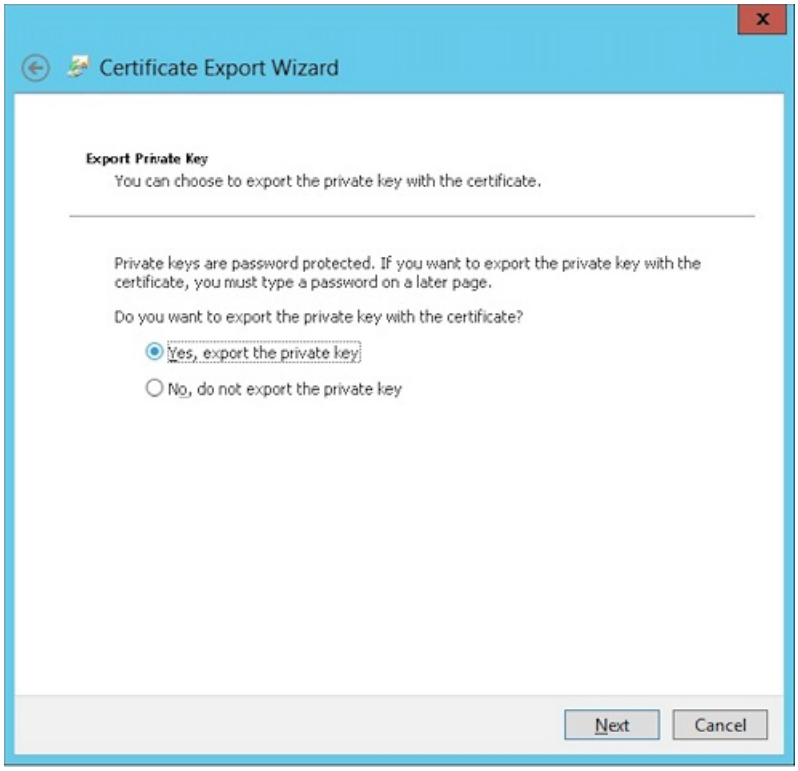
6. Sélectionnez le modèle **Utilisateur** et cliquez sur **Inscrire**.



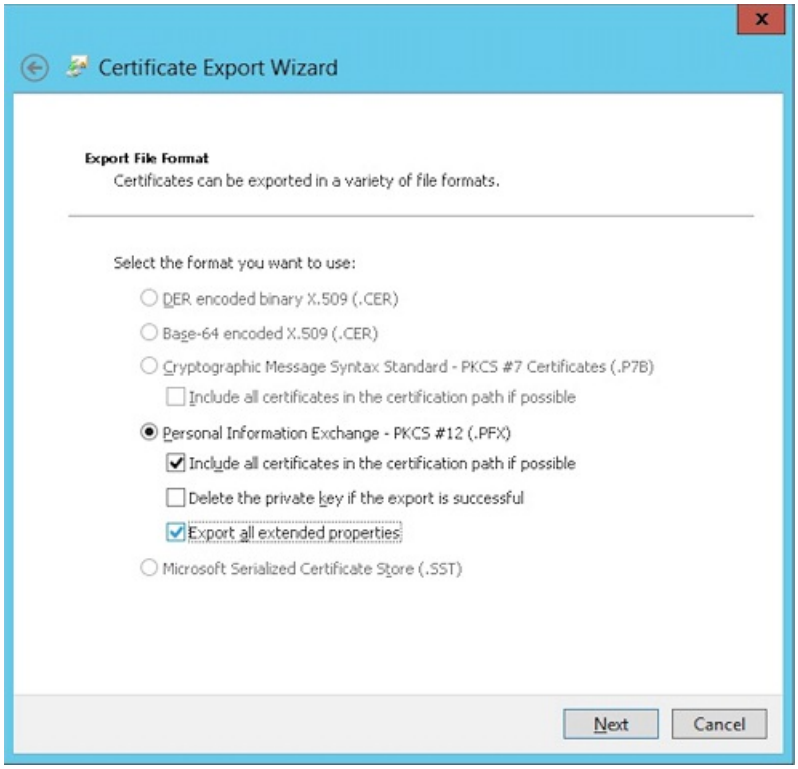
7. Exportez le fichier .pfx que vous avez créé à l'étape précédente.



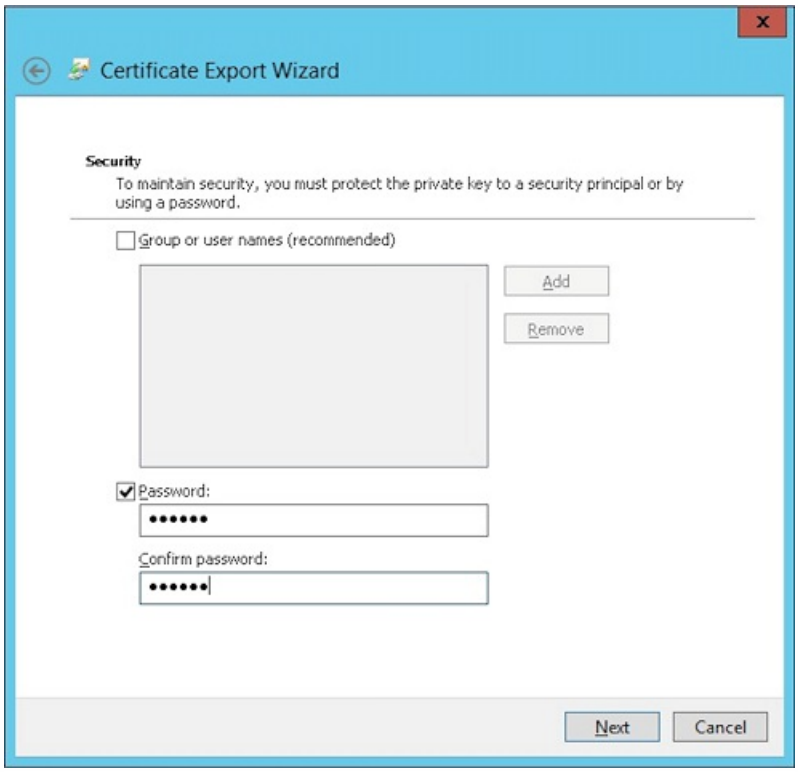
8. Cliquez sur **Oui, exporter la clé privée**.



9. Sélectionnez les cases **Inclure tous les certificats dans le chemin d'accès de certification, si possible** et **Exporter toutes les propriétés étendues**.



10. Définissez un mot de passe que vous utiliserez lors du chargement de ce certificat dans XenMobile.



11. Enregistrez le certificat sur votre disque dur.

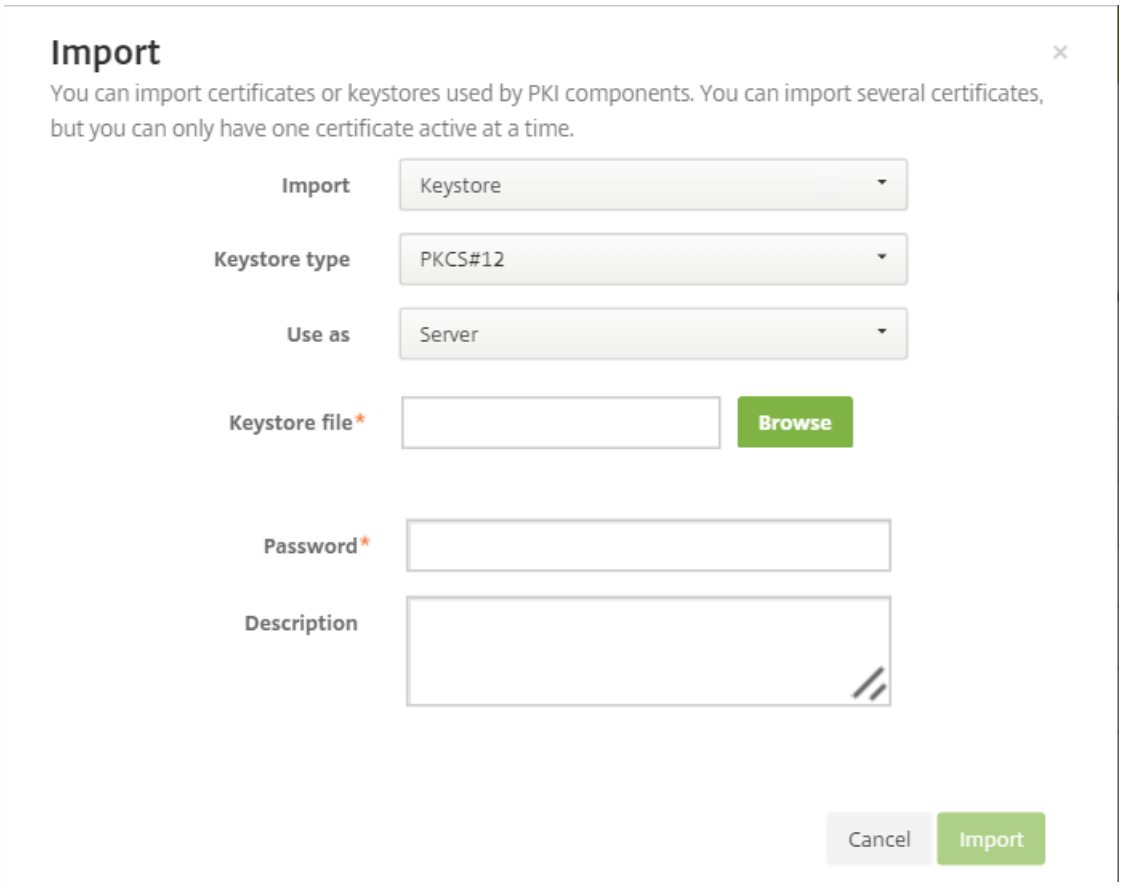
Chargement du certificat sur XenMobile

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.

2. Cliquez sur **Certificats** et sur **Importer**.

3. Entrez les paramètres suivants :

- **Importer** : Keystore
- **Type de keystore** : PKCS#12.
- **Utiliser en tant que** : Serveur
- **Fichier de keystore** : cliquez sur Parcourir pour sélectionner le certificat .pfx que vous venez de créer.
- **Mot de passe** : entrez le mot de passe que vous avez créé pour ce certificat.



4. Cliquez sur **Importer**.

5. Vérifiez que le certificat a été installé correctement. Il doit s'afficher en tant que certificat Utilisateur.

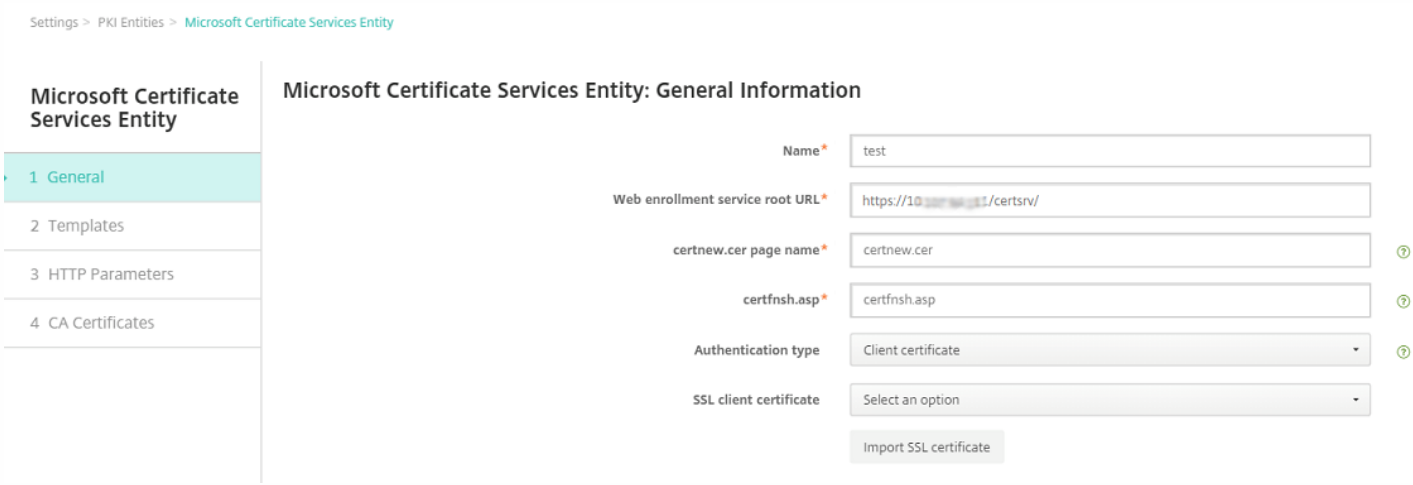
Création de l'entité PKI pour l'authentification par certificat

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Entités PKI**.

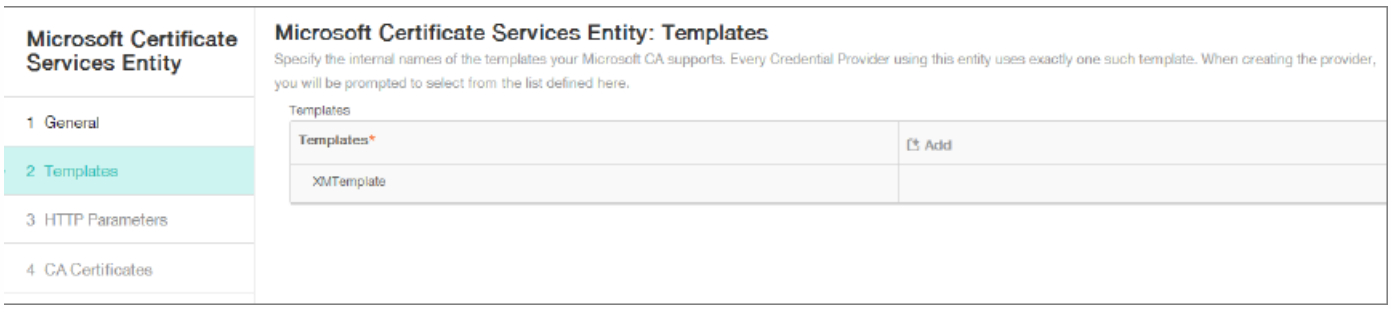
2. Cliquez sur **Ajouter** et sur **Entité Services de certificats Microsoft**. La page **Entité Services de certificats Microsoft : informations générales** s'affiche.

3. Entrez les paramètres suivants :

- **Nom** : entrez un nom quelconque.
- **URL racine du service d'inscription Web** : https://RootCA-URL/certsrv/
  N'oubliez pas d'ajouter la dernière barre oblique (/) dans l'URL.
- **Nom de page certnew.cer** : certnew.cer (valeur par défaut)
- **certfnsh.asp**: certfnsh.asp (valeur par défaut)
- **Type d'authentification** : certificat client
- **Certificat SSL** : sélectionnez le certificat utilisateur à utiliser pour émettre le certificat client XenMobile.

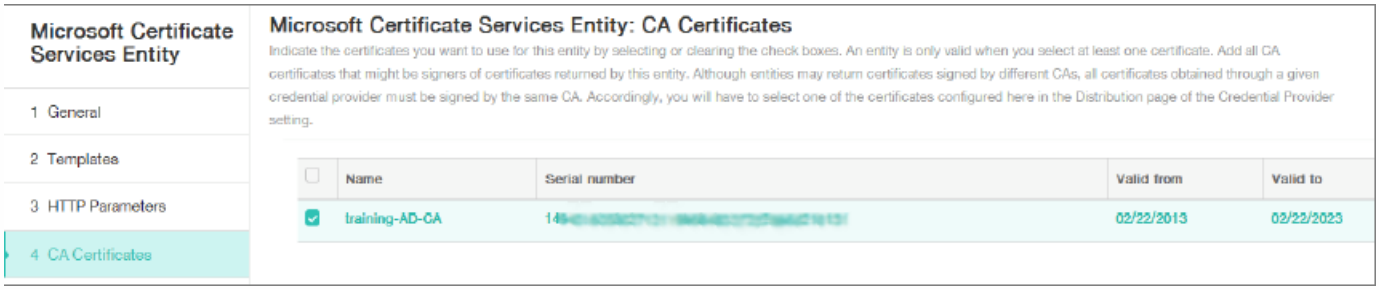


4. Sous **Modèles**, ajoutez le modèle que vous avez créé lors de la configuration du certificat Microsoft. Veillez à ne pas ajouter d'espaces.



5. Ignorez les paramètres HTTP et cliquez sur **Certificats CA**.

6. Sélectionnez le nom de l'autorité de certification racine qui correspond à votre environnement. L'autorité de certification racine fait partie de la chaîne importée depuis le certificat client XenMobile.



7. Cliquez sur **Enregistrer**.

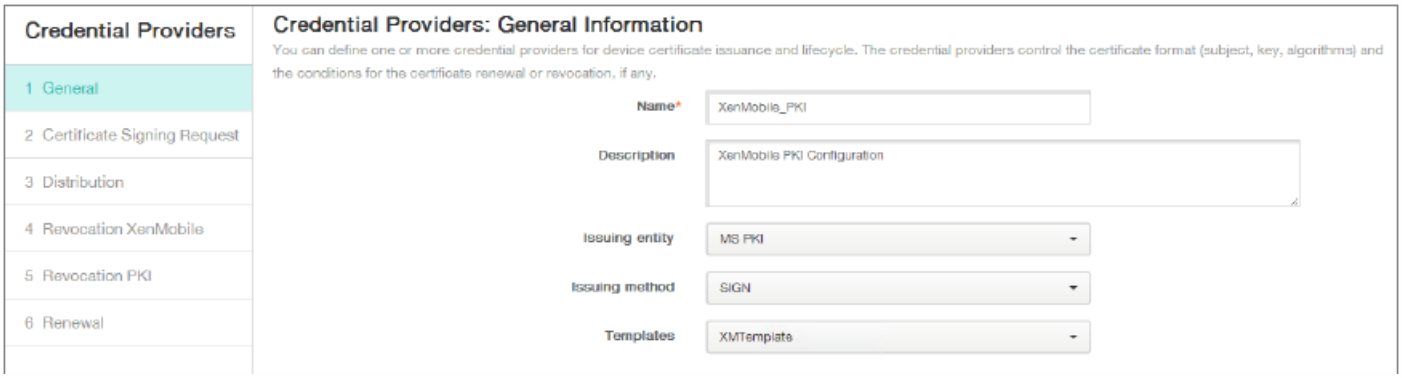
Configuration des fournisseurs d'identités

1. Dans **Paramètres**, accédez à **Plus > Gestion des certificats > Fournisseurs d'identités**.

2. Cliquez sur **Ajouter**.

3. Sous **Général**, entrez les paramètres suivants :

- **Nom** : entrez un nom quelconque.
- **Description** : entrez une description quelconque.
- **Entité émettrice** : sélectionnez l'entité PKI créée précédemment.
- **Méthode d'émission** : SIGNER
- **Modèles** : sélectionnez le modèle ajouté sous l'entité PKI.

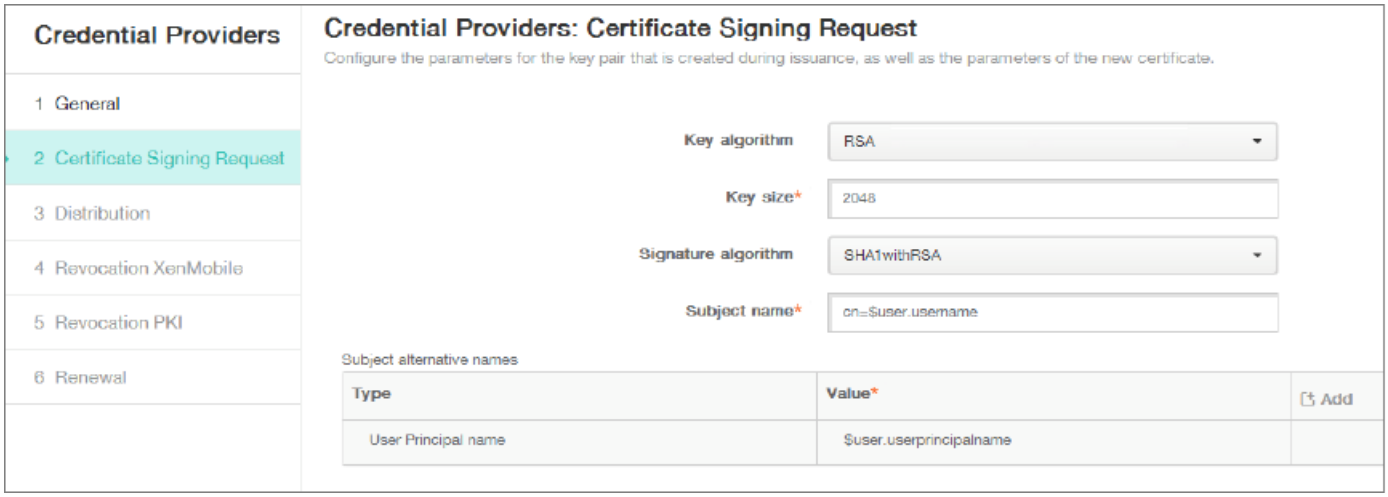


4. Cliquez sur **Demande de signature de certificat** et entrez les paramètres suivants :

- **Algorithme de clé** : RSA
- **Taille de la clé** : 2048
- **Algorithme de signature** : SHA1withRSA
- **Nom du sujet** : cn=$user.username

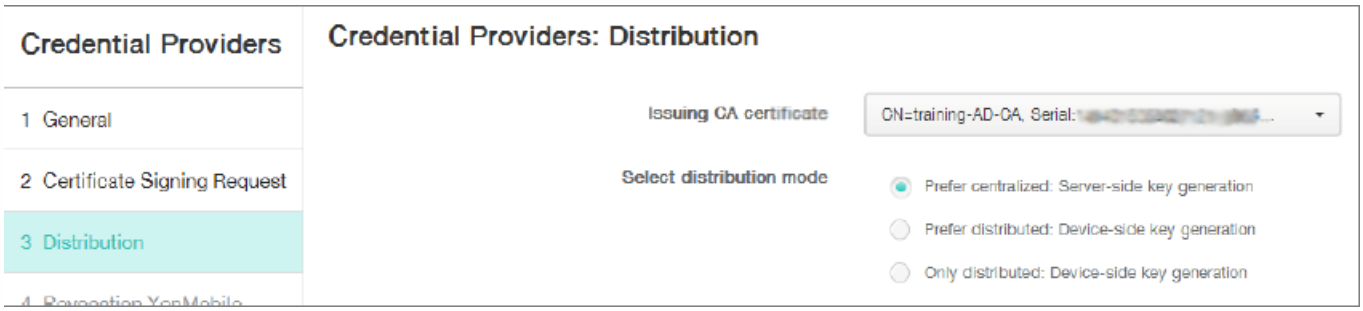
Pour **Noms de sujet alternatifs**, cliquez sur **Ajouter** et entrez les paramètres suivants :

- **Type** : nom principal de l'utilisateur
- **Valeur** : $user.userprincipalname



5. Cliquez sur **Distribution** et entrez les paramètres suivants :

- **Certificat émis par l'autorité de certification** : sélectionnez l'autorité de certification émettrice qui a signé le certificat client XenMobile.
- **Sélectionner le mode de distribution** : sélectionnez **Préférer mode centralisé : génération de la clé sur le serveur**.

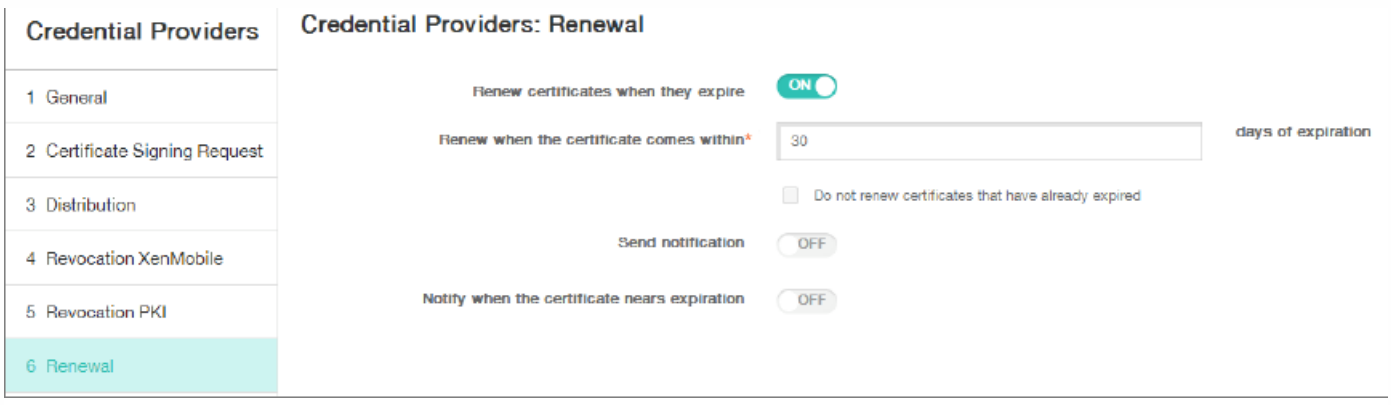


6. Pour les deux prochaines sections -- **Révocation XenMobile** et **Révocation PKI** -- définissez les paramètres comme vous le souhaitez. Pour les besoins de cet article, ces deux options ont été ignorées.

7. Cliquez sur **Renouvellement**.

8. Pour **Renouveler les certificats lorsqu'ils expirent**, sélectionnez **Activé**.

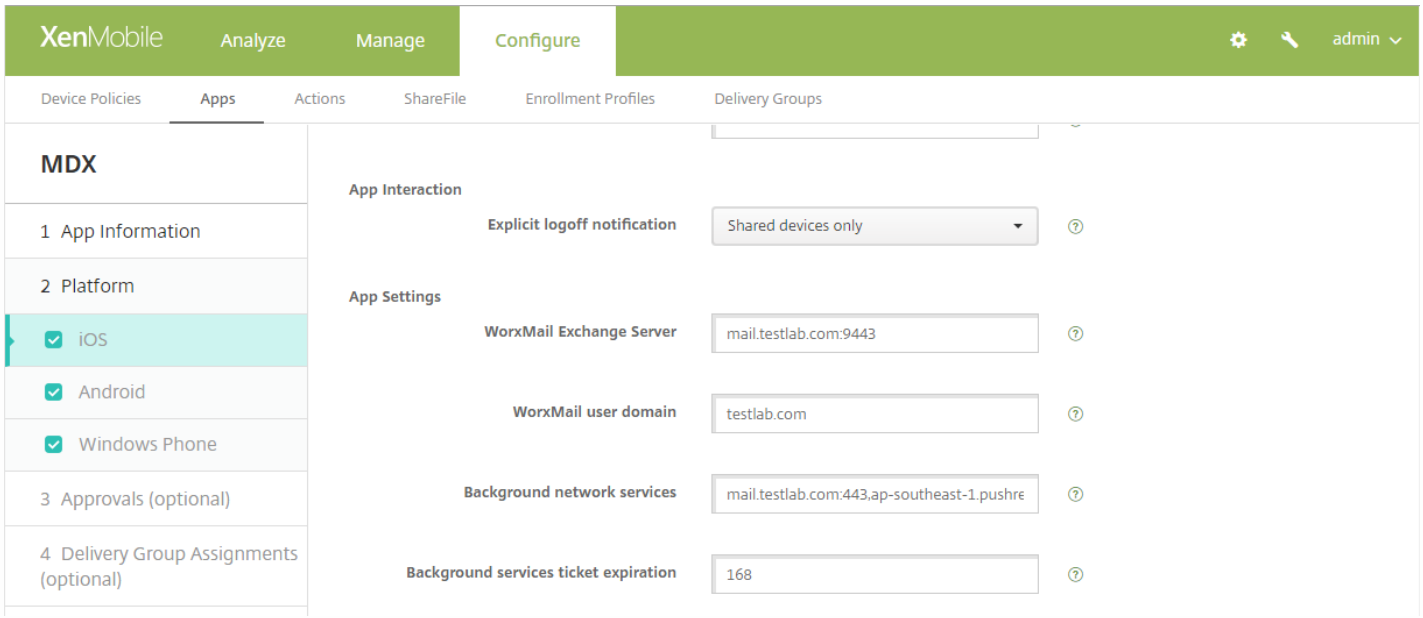
9. Laissez tous les autres paramètres par défaut ou modifiez-les comme vous le souhaitez.



10. Cliquez sur **Enregistrer**.

Configuration de Secure Mail pour utiliser l'authentification basée sur certificat

Lorsque vous ajoutez Secure Mail à XenMobile, n'oubliez pas de configurer les paramètres Exchange sous **Paramètres applicatifs**.



Configuration de la remise de certificats NetScaler dans XenMobile

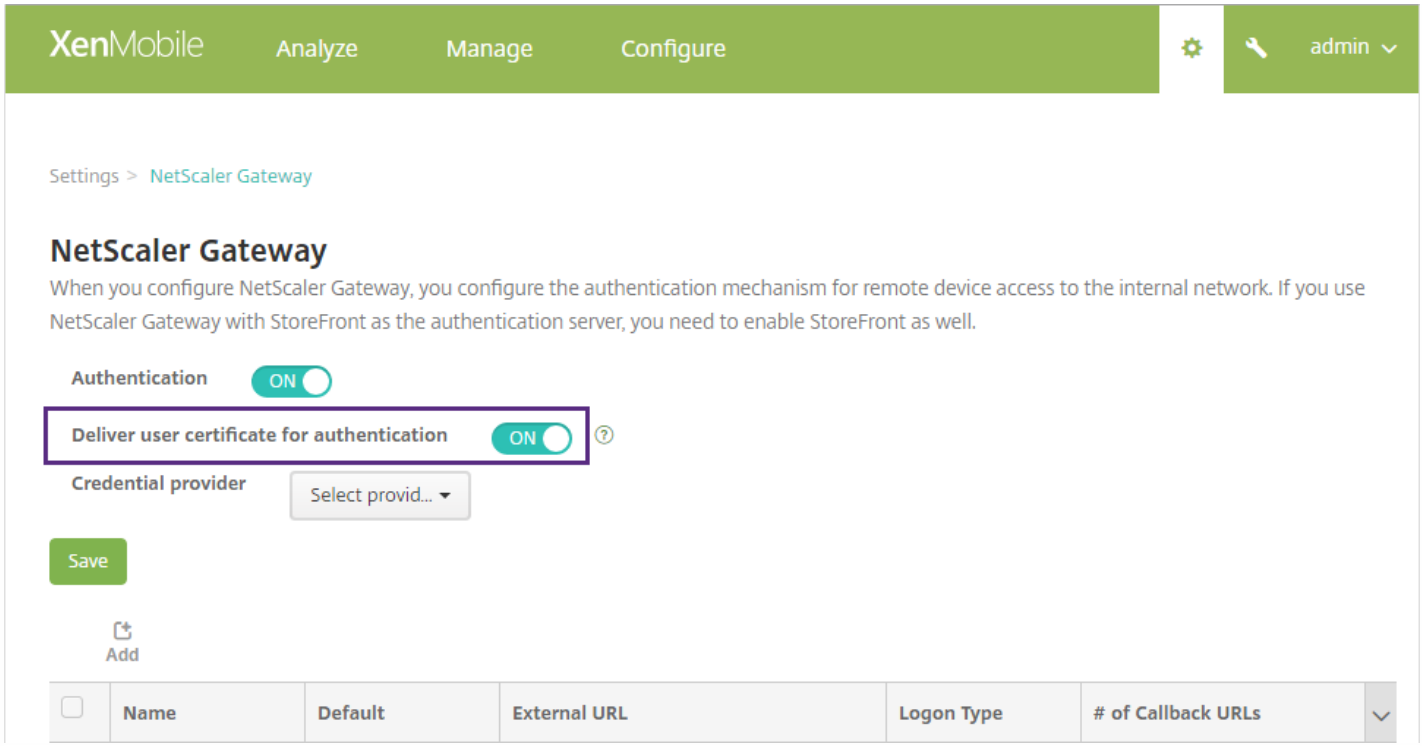
1. Connectez-vous à la console XenMobile et cliquez sur l'icône d'engrenage dans le coin supérieur droit. L'écran **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **NetScaler Gateway**.

3. Si NetScaler Gateway n'est pas déjà ajouté, cliquez sur **Ajouter** et spécifiez les paramètres :

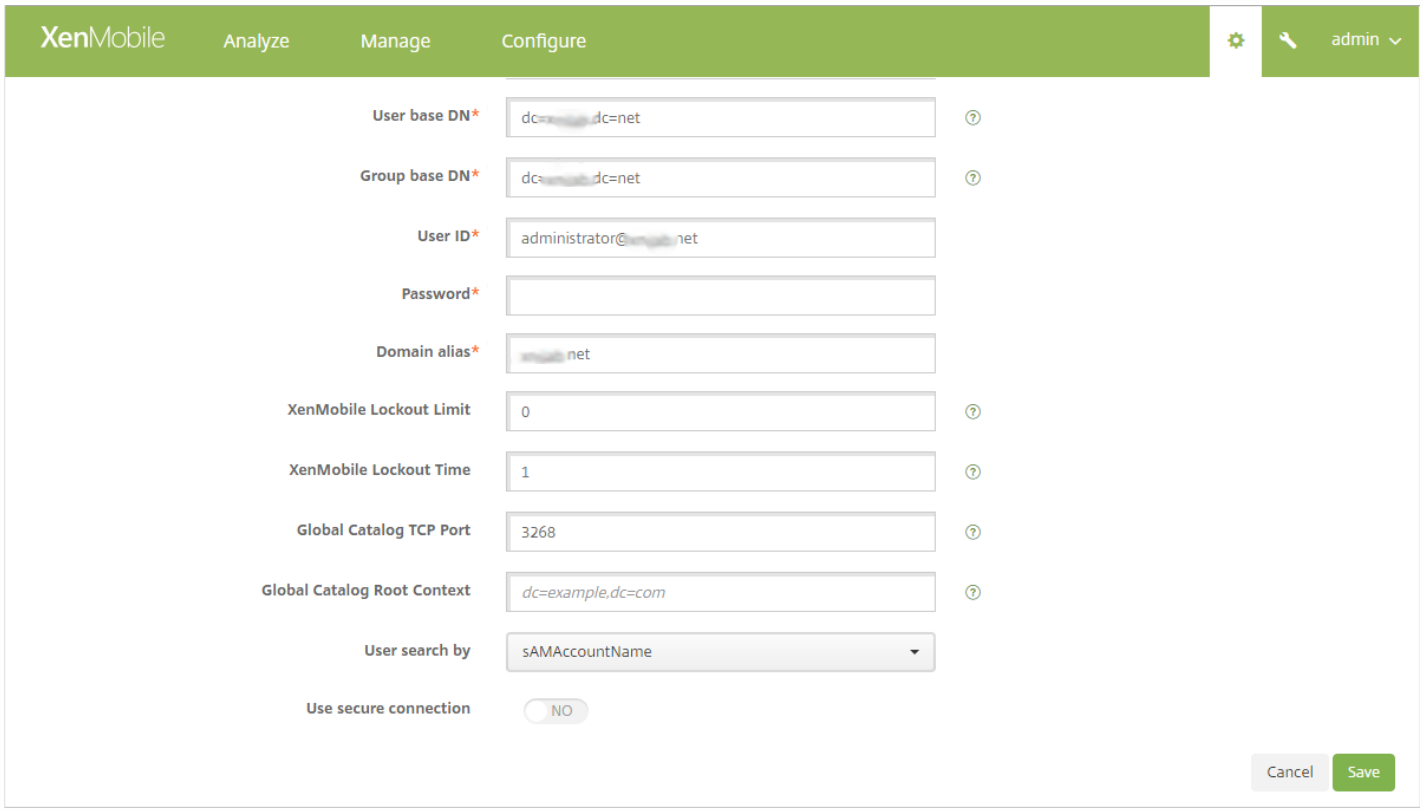
- **URL externe** : https://VotreURLNetScalerGateway
- **Type d'ouverture de session** : Certificat
- **Mot de passe requis** : DÉSACTIVÉ
- **Définir par défaut** : ACTIVÉ

4. Pour **Délivrer un certificat utilisateur pour l'authentification**, sélectionnez **Activé**.



5. Pour **Fournisseur d'identités**, sélectionnez un fournisseur et cliquez sur **Enregistrer**.

6. Si vous utilisez des attributs sAMAccount dans les certificats utilisateur comme une alternative au nom d'utilisateur principal (UPN), configurez le connecteur LDAP dans XenMobile comme suit : accédez à **Paramètres > LDAP**, sélectionnez le répertoire et cliquez sur **Modifier**, puis sélectionnez **sAMAccountName** dans **Recherche utilisateur par**.



Création d'une stratégie d'hub d'entreprise pour Windows Phone 8.1 et 10

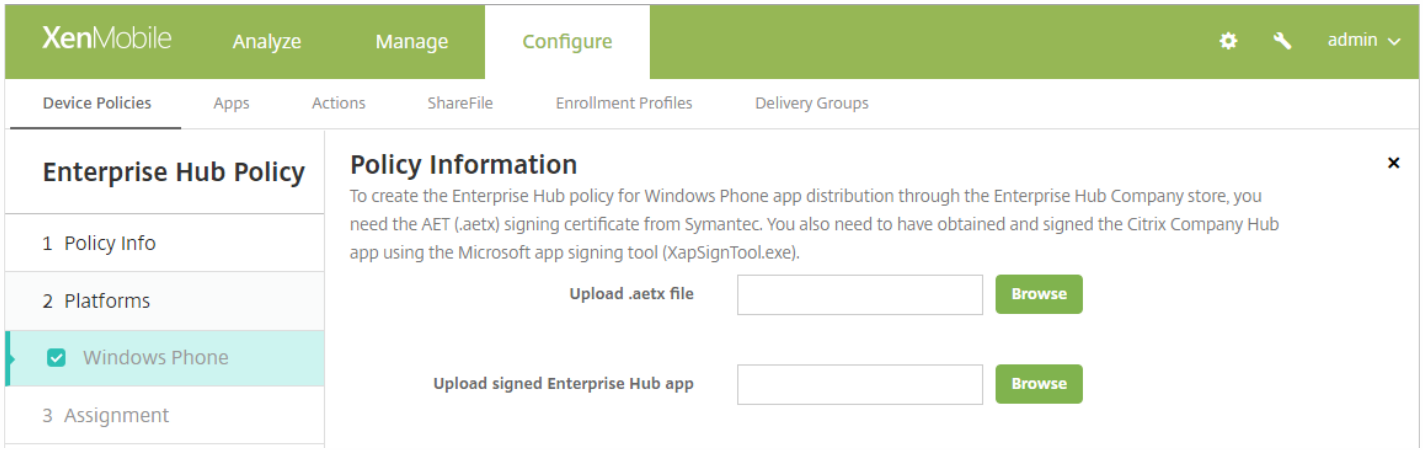
Pour les appareils Windows Phone, vous devez créer une stratégie d'hub d'entreprise pour délivrer le fichier AETX et le client Secure Hub.

> **Remarque**
>
> Assurez-vous que les fichiers AETX et Secure Hub utilisent le même certificat d'entreprise que celui du fournisseur de certificats et le même ID d'éditeur que celui du compte de développeur Windows Store.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**, puis, sous **Plus > Agent XenMobile**, cliquez sur **Hub d'entreprise**.

3. Après avoir attribué un nom à la stratégie, sélectionnez le fichier .AETX correct et l'application Secure Hub signée pour le hub d'entreprise.



4. Attribuez la stratégie à des groupes de mise à disposition et enregistrez-la.

Résolution des problèmes de configuration du certificat client

Une fois la configuration précédente et la configuration NetScaler Gateway effectuées avec succès, le workflow de l'utilisateur est le suivant :

1. Les utilisateurs inscrivent leurs appareils mobiles.

2. XenMobile invite les utilisateurs à créer un code PIN Citrix.

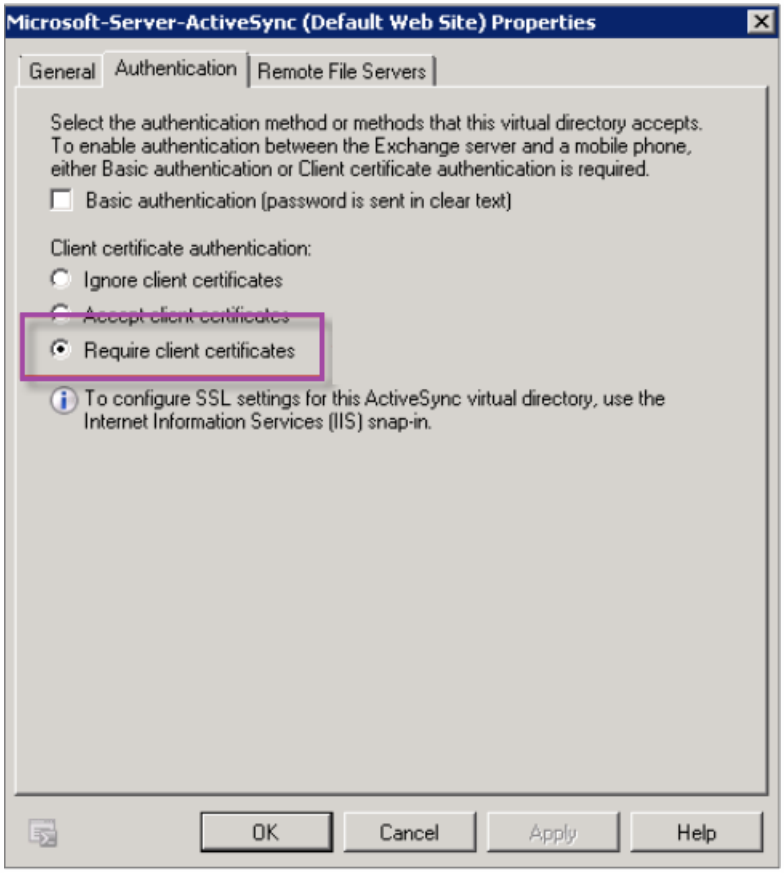
3. Les utilisateurs sont redirigés vers XenMobile Store.

4. Lorsque les utilisateurs démarrent Secure Mail pour iOS, Android ou Windows Phone 8.1, XenMobile ne les invite pas à entrer des informations d'identification afin de configurer leurs boîtes aux lettres. Au lieu de cela, Secure Mail demande le certificat client de Secure Hub et l'envoie à Microsoft Exchange Server pour authentification. Si XenMobile invite les utilisateurs à entrer des informations d'identification lorsqu'ils démarrent Secure Mail, vérifiez votre configuration.

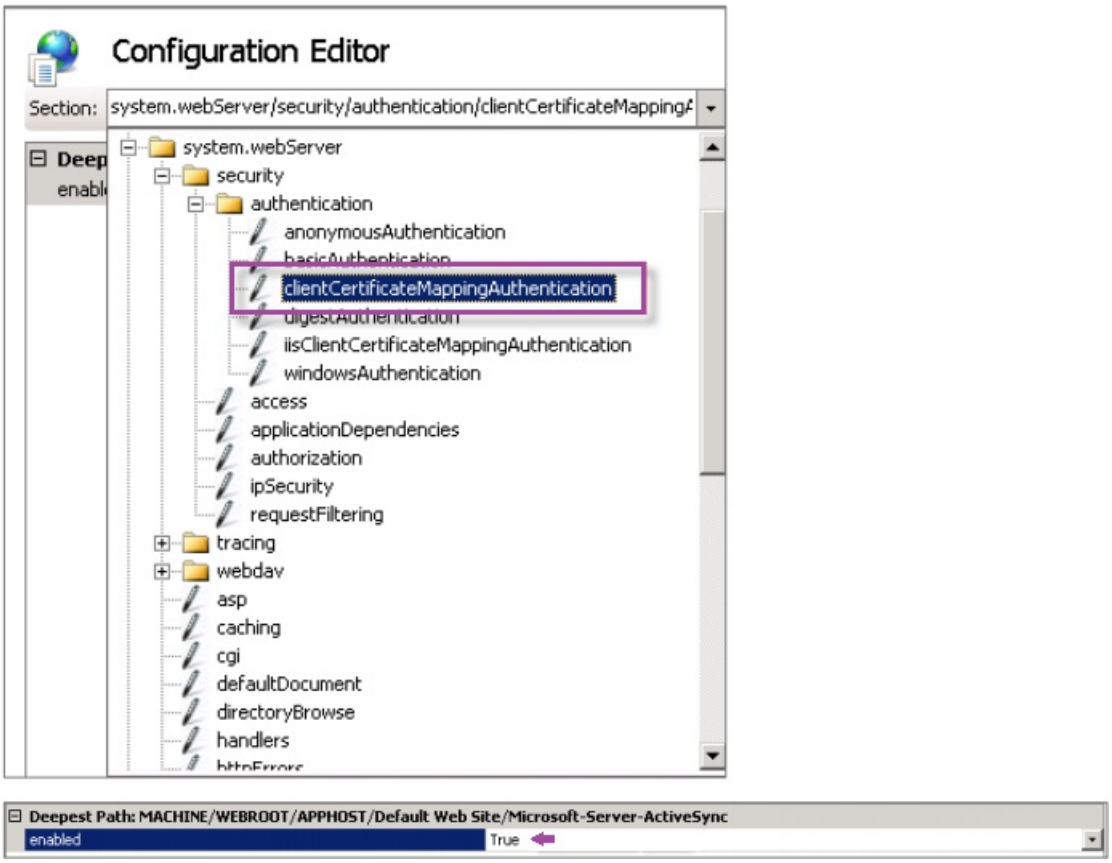
Si les utilisateurs peuvent télécharger et installer Secure Mail, mais que Secure Mail ne termine pas la configuration durant la configuration de la boîte aux lettres :

1. Si Microsoft Exchange Server ActiveSync utilise des certificats de serveur SSL privé pour sécuriser le trafic, vérifiez que les certificats racine/intermédiaire sont installés sur l'appareil mobile.

2. Vérifiez que le type d'authentification sélectionné pour ActiveSync est **Exiger les certificats clients**.



3.Sur Microsoft Exchange Server, sélectionnez le site **Microsoft-Server-ActiveSync** pour activer l'authentification par mappage de certificat client (elle est désactivée par défaut). L'option figure sous **Éditeur de configuration > Sécurité > Authentification**.



Remarque : après avoir sélectionné **Vrai**, cliquez sur **Appliquer** pour que les modifications prennent effet.

4. Vérifiez les paramètres de NetScaler Gateway dans la console XenMobile : assurez-vous que **Délivrer un certificat utilisateur pour l'authentification** est réglé sur **ACTIVÉ**, que le profil correct est sélectionné pour **Fournisseur d'identités**, comme indiqué précédemment dans « Pour configurer la remise de certificats NetScaler dans XenMobile ».

Pour déterminer si le certificat client a été délivré à un appareil mobile :

1. Dans la console XenMobile, accédez à **Gérer > Appareils** et sélectionnez l'appareil.

2. Cliquez sur **Modifier** ou **Afficher plus**.

3. Accédez à la section **Groupes de mise à disposition** et recherchez cette entrée :

    Informations d'identification NetScaler Gateway : Requested credential, CertId=

Pour vérifier si la négociation du certificat client est activée :

1. Exécutez cette commande netsh pour afficher la configuration du certificat SSL qui est liée sur le site Web IIS :

    netsh http show sslcert

2. Si la valeur **Négocier le certificat client** est **désactivée**, exécutez la commande suivante pour l'activer :

    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

Par exemple :

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

Si vous ne pouvez pas délivrer de certificats racine/intermédiaire à un appareil Windows Phone 8.1 via XenMobile :

- Envoyez des fichiers de certificats racine/intermédiaire (.cer) par e-mail à l'appareil Windows Phone 8.1 et installez-les directement.

Si Secure Mail n'est pas installé correctement sur Windows Phone 8.1 :

- Vérifiez que le fichier de jeton d'inscription d'application (.AETX) est délivré via XenMobile à l'aide de la stratégie d'hub d'entreprise.
- Vérifiez que le jeton d'inscription d'application a été créé à l'aide du même certificat d'entreprise que celui du fournisseur de certificats utilisé pour wrapper Secure Mail et signer les applications Secure Hub.
- Vérifiez que le même ID d'éditeur est utilisé pour signer et wrapper Secure Hub, Secure Mail et le jeton d'inscription d'application.

Entités PKI

Feb 23, 2017

Une configuration d'entité d'infrastructure de clé publique (PKI) XenMobile représente un composant réalisant des opérations PKI réelles (émission, révocation et informations d'état). Ces composants peuvent être internes à XenMobile, auquel cas ils sont appelés discrétionnaires, ou externes à XenMobile, s'ils font partie de votre infrastructure d'entreprise.

XenMobile prend en charge les types d'entités PKI suivantes :

- Autorités de certification discrétionnaires (CA)
- PKI génériques (GPKI)
- Services de certificats Microsoft

XenMobile prend en charge les serveurs d'autorité de certification suivants :

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

Concepts de PKI communs

Quel que soit son type, chaque entité PKI possède un sous-ensemble des fonctionnalités suivantes :

- signature : émission d'un nouveau certificat, basé sur une demande de signature de certificat (CSR).
- récupération : récupération d'un certificat existant et d'une paire de clés.
- révocation : révocation d'un certificat client.

À propos des certificats CA

Lorsque vous configurez une entité PKI, vous devez informer XenMobile de la nature du certificat d'autorité de certification qui sera le signataire des certificats émis par (ou récupérés depuis) cette entité. Une seule et même entité PKI peut renvoyer (récupérés ou nouvellement signés) des certificats signés par un certain nombre d'autorités de certification différentes. Vous devez fournir le certificat de chacune de ces autorités de certification dans le cadre de la configuration de l'entité PKI. Pour ce faire, chargez les certificats sur XenMobile puis référencez-les dans l'entité PKI. Pour les autorités de certification discrétionnaire, le certificat est implicitement le certificat de l'autorité de certification de signature, mais pour les entités externes, vous devez le spécifier manuellement.

PKI générique

Le protocole PKI générique (GPKI) est un protocole XenMobile propriétaire exécuté sur une couche du service Web SOAP qui permet un interfaçage avec différentes solutions PKI. Le protocole GPKI définit les trois opérations PKI fondamentales suivantes :

- signature: la carte est capable de prendre des demandes de signature de certificat (CSR), de les transmettre à la PKI et de retourner des certificats nouvellement signés.
- récupération : la carte est capable de récupérer des certificats existants et des paires de clés (selon les paramètres d'entrée) depuis la PKI.
- révocation : la carte peut entraîner la révocation d'un certificat donné par la PKI.

La carte GPKI se trouve en bout du protocole GPKI. La carte convertit les opérations fondamentales pour le type de PKI

spécifique pour lequel elle a été créée. En d'autres termes, il existe une carte GPKI pour RSA, une autre pour EnTrust, etc.

La carte GPKI, en tant que point de terminaison des services Web SOAP, publie une définition WSDL auto-descriptive. La création d'une entité GPKI PKI équivaut à fournir cette définition WSDL à XenMobile, soit par le biais d'une adresse URL soit en chargeant le fichier lui-même.

La prise en charge de chaque opération PKI dans une carte est facultative. Si une carte prend en charge une opération donnée, on considère qu'elle dispose de la capacité correspondante (signature, récupération ou révocation). Chacune de ces fonctionnalités peut être associée à un ensemble de paramètres utilisateur.

Les paramètres utilisateur sont des paramètres qui sont définis par l'adaptateur GPKI pour une opération spécifique et dont vous avez besoin pour fournir des valeurs à XenMobile. XenMobile détermine les opérations prises en charge par la carte (quelles capacités elle possède) et les paramètres requis par la carte pour chacune des opérations en analysant le fichier WSDL. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre XenMobile et la carte GPKI.

Pour ajouter une PKI générique

1. Dans la console Web XenMobile, cliquez sur **Configurer** > **Paramètres** > **Plus** > **Entités PKI**.

2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

Une liste répertoriant les types de PKI que vous pouvez ajouter s'affiche.

3. Cliquez sur **Entité PKI générique**.

La page Entité PKI générique : informations générales s'affiche.

4. Sur la page **Entité PKI générique : informations générales**, procédez comme suit :

- **Nom** : entrez un nom descriptif pour l'entité PKI.
- **URL du WSDL** : entrez l'emplacement du WSDL décrivant la carte.
- **Type d'authentification** : cliquez sur la méthode d'authentification à utiliser.
- **Aucun(e)**
- **HTTP basique** : fournissez le nom d'utilisateur et mot de passe requis pour se connecter à la carte.
- **Certificat client** : sélectionnez le certificat client SSL correct.

5. Cliquez sur **Suivant**.

La page Entité PKI générique : capacité de l'adaptateur s'affiche.

6. Sur la page **Entité PKI générique : capacité de l'adaptateur**, passez en revue les capacités et les paramètres associés à votre carte et cliquez sur **Suivant**.

La page **Entité PKI générique : émission de certificats CA** s'affiche.

7. Sur la page Entité PKI générique : émission de certificats CA, sélectionnez les certificats que vous voulez utiliser pour l'entité.

Remarque : bien que les entités puissent retourner des certificats signés par des autorités de certification différentes, tous les certificats obtenus via un fournisseur de certificats donné doivent être signés par la même autorité de certification. Par conséquent, lorsque vous configurez le paramètre **Fournisseur d'identités**, sur la page **Distribution**, sélectionnez l'un des certificats configuré ici.

8. Cliquez sur **Enregistrer**.

L'entité s'affiche sur le tableau Entités PKI.

Services de certificats Microsoft

XenMobile se connecte avec Microsoft Certificate Services Web par le biais de son interface d'inscription Web. XenMobile prend uniquement en charge l'émission de nouveaux certificats via cette interface (l'équivalent de la fonctionnalité de signature GPKI).

Pour créer une entité PKI Microsoft CA dans XenMobile, vous devez spécifier l'adresse URL de base de l'interface Web des services de certificats. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre XenMobile et l'interface Web des services de certificats.

Pour ajouter une entité Services de certificats Microsoft

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus** > **Entités PKI**.

2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

Une liste répertoriant les types de PKI que vous pouvez ajouter s'affiche.

3. Cliquez sur **Entité Services de certificats Microsoft**.

La page **Entité Services de certificats Microsoft : informations générales** s'affiche.

4. Sur la page Entité Services de certificats Microsoft : informations générales, procédez comme suit :

- Nom : entrez un nom pour votre nouvelle entité, qui sera utilisé plus tard pour faire référence à cette entité. Les noms de l'entité doivent être uniques.
- URL racine du service d'inscription Web : entrez l'adresse URL de votre service d'inscription Web d'autorité de certification Microsoft ; par exemple, https://192.0.2.13/certsrv/. L'adresse URL peut utiliser un format HTTP ou HTTP-over-SSL.
- Nom de page certnew.cer : nom de la page certnew.cer. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
- certfnsh.asp : nom de la page certfnsh.asp. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
- Type d'authentification : cliquez sur la méthode d'authentification à utiliser.
- Aucune
- HTTP basique : fournissez le nom d'utilisateur et mot de passe requis pour se connecter.
- Certificat client : sélectionnez le certificat client SSL correct.

5. Cliquez sur **Suivant**.

La page **Entité Services de certificats Microsoft : modèles** s'affiche. Sur cette page, spécifiez le nom interne des modèles pris en charge par votre autorité de certification Microsoft. Lors de la création de fournisseurs d'identités, vous devez sélectionner un modèle dans la liste définie ici. Chaque fournisseur d'identités utilisant cette entité utilise un seul modèle de ce type.

Pour connaître la configuration requise pour les modèles Services de certificats Microsoft, veuillez consulter la documentation Microsoft relative à votre version de serveur Microsoft. XenMobile ne requiert pas de configuration

particulière pour les certificats qu'il distribue autre que les formats de certificat indiqués dans Certificats.

6. Sur la page **Entité Services de certificats Microsoft : modèles**, cliquez sur **Ajouter**, entrez le nom du modèle et cliquez sur **Enregistrer**. Répétez cette étape pour chaque modèle à ajouter.

7. Cliquez sur **Suivant**.

La page **Entité Services de certificats Microsoft : paramètres HTTP** s'affiche. Sur cette page, spécifiez des paramètres personnalisés que XenMobile doit insérer dans la requête HTTP auprès de l'interface d'inscription Web de Microsoft. Ceci sera utile uniquement si des scripts personnalisés sont exécutés sur l'autorité de certification.

8. Sur la page **Entité Services de certificats Microsoft : paramètres HTTP**, cliquez sur **Ajouter**, entrez le nom et la valeur des paramètres HTTP que vous souhaitez ajouter, puis cliquez sur **Suivant**.

La page **Entité Services de certificats Microsoft : certificats CA** s'affiche. Sur cette page, il vous sera demandé d'informer XenMobile des signataires des certificats que le système va obtenir par le biais de cette entité. Lorsque votre certificat d'autorité de certification est renouvelé, mettez-le à jour dans XenMobile, puis la modification est appliquée de manière transparente à l'entité.

9. Sur la page **Entité Services de certificats Microsoft : certificats CA**, sélectionnez les certificats que vous voulez utiliser pour cette entité.

10. Cliquez sur **Enregistrer**.

L'entité s'affiche sur le tableau Entités PKI.

Liste de révocation de certificats (CRL) NetScaler

XenMobile prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous disposez d'une autorité de certification Microsoft configurée, XenMobile utilise NetScaler pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) NetScaler, **Enable CRL Auto Refresh**. Cette étape permet de s'assurer que l'utilisateur d'un appareil en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. XenMobile émet de nouveau un nouveau certificat, car il n'interdit pas à un utilisateur de générer un certificat utilisateur si un certificat a été révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Autorités de certification discrétionnaires

Une autorité de certification discrétionnaire est créée lorsque vous fournissez un certificat d'autorité de certification et la clé privée qui lui est associée à XenMobile. XenMobile gère l'émission, la révocation et les informations d'état en interne des certificats, selon les paramètres que vous spécifiez.

Lorsque vous configurez une autorité de certification discrétionnaire, vous avez la possibilité d'activer la prise en charge du protocole OCSP pour cette autorité de certification. Si, et uniquement si vous activez la prise en charge du protocole OCSP, l'autorité de certification ajoute une extension id-pe-authorityInfoAccess aux certificats qu'elle émet, pointant vers le répondeur OCSP interne de XenMobile situé à l'adresse suivante.

`https://server/instance/ocsp`

Lors de la configuration du service OCSP, vous devez spécifier un certificat de signature OCSP pour l'entité discrétionnaire en question. Vous pouvez utiliser le certificat d'autorité de certification lui-même en tant que signataire. Si vous voulez éviter la divulgation inutile de la clé privée de votre autorité de certification (recommandé), créez un certificat de signature OCSP

délégué, signé par le certificat d'autorité de certification et incluez une extension id-kp-OCSPSigning extendedKeyUsage.

Le service du répondeur OCSP de XenMobile prend en charge les réponses OCSP de base et les algorithmes de hash suivants utilisés dans les requêtes :

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

Les réponses sont signées avec SHA-256 et l'algorithme de clé du certificat de signature (DSA, RSA ou ECDSA).

Pour ajouter des autorités de certification discrétionnaires

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus** > **Entités PKI**.

2. Sur la page **Entités PKI**, cliquez sur **Ajouter**.

Une liste répertoriant les types de PKI que vous pouvez ajouter s'affiche.

3. Cliquez sur **CA discrétionnaire**.

La page **CA discrétionnaire : informations générales** s'affiche.

4. Sur la page **CA discrétionnaire : informations générales**, procédez comme suit :

- **Nom** : entrez un nom descriptif pour la CA discrétionnaire.
- **Certificat CA utilisé pour signer les demandes de certificat** : cliquez sur un certificat pour la CA discrétionnaire à utiliser pour signer les demandes de certificats. Cette liste de certificats est générée à partir des certificats CA avec des clés privées que vous avez chargées sur XenMobile > **Configure** > **Paramètres** > **Certificats**.

5. Cliquez sur **Suivant**.

La page **CA discrétionnaire : paramètres** s'affiche.

6. Sur la page **CA discrétionnaire : paramètres**, procédez comme suit :
- **Générateur de numéro de série** : la CA discrétionnaire génère des numéros de série pour les certificats qu'elle émet. Dans cette liste, cliquez sur **Séquentiel** ou **Non-séquentiel** pour déterminer comment les numéros sont générés.
- **Numéro de série suivant** : entrez une valeur pour déterminer le numéro suivant émis.
- **Certificat valide pour**: entrez le nombre de jours pendant lesquels le certificat est valide.
- **Utilisation de la clé** : identifiez la fonction des certificats émis par l'autorité de certification discrétionnaire en définissant les clés appropriées sur **On**. Une fois cette option définie, l'autorité de certification peut uniquement émettre des certificats aux fins susmentionnées.
- **Utilisation de clé étendue** : pour ajouter d'autres paramètres, cliquez sur **Ajouter**, entrez le nom de clé, puis cliquez sur **Enregistrer**.

7. Cliquez sur **Suivant**.

La page **CA discrétionnaire : distribution** s'affiche.

Sur la page **CA discrétionnaire : distribution**, sélectionnez un mode de distribution :

- **Centralisé : génération de la clé sur le serveur**. Citrix recommande l'option centralisée. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
- **Distribué : génération de la clé sur l'appareil**. Les clés privées sont générées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec le keyUsage keyEncryption et un certificat de signature RA avec le KeyUsage digitalSignature. Le même certificat peut être utilisé pour le chiffrement et la signature.

9. Cliquez sur **Suivant**.

La page **CA discrétionnaire : protocole OCSP** s'affiche.

Sur la page **CA discrétionnaire : protocole OCSP**, procédez comme suit :

- Si vous souhaitez ajouter une extension AuthorityInfoAccess (RFC2459) pour les certificats signés par cette autorité de certification, définissez **Activer le support d'OCSP pour cette CA** sur **On**. Cette extension pointe vers le répondeur OCSP de l'autorité de certification sur https://serveur/instance/ocsp.
- Si vous avez activé la prise en charge du protocole OCSP, sélectionnez un certificat d'autorité de certification de signature OSCP. Cette liste de certificats est générée à partir des certificats d'autorité de certification que vous avez chargés sur XenMobile.

10. Cliquez sur **Enregistrer**.

L'autorité de certification discrétionnaire s'affiche sur le tableau Entités PKI.

Fournisseurs d'identités

Feb 23, 2017

Les fournisseurs d'identités sont les configurations de certificat réelles que vous utilisez dans différentes parties du système XenMobile. Ils définissent les sources, les paramètres et les cycles de vie de vos certificats, qu'ils fassent partie de configurations d'appareils ou qu'ils soient autonomes, c'est-à-dire transmis tels quels, vers l'appareil.

L'inscription d'appareil limite le cycle de vie du certificat. En effet, XenMobile ne délivre pas de certificats avant l'inscription, bien qu'il puisse en émettre certains dans le cadre de l'inscription. En outre, les certificats émis par la PKI interne dans le cadre d'une inscription sont révoqués lorsque l'inscription est révoquée. Après la fin de la relation de gestion, aucun certificat valide n'est conservé.

Une configuration de fournisseur d'identités peut être utilisée à plusieurs endroits, par conséquent une configuration peut régir un grand nombre de certificats simultanément. L'unité existe alors sur la ressource de déploiement et le déploiement. Par exemple, si le fournisseur d'identités P est déployé sur l'appareil D dans le cadre de la configuration C, alors les paramètres d'émission pour P déterminent le certificat qui est déployé sur D. De même, les paramètres de renouvellement pour D s'appliquent lorsque C est mis à jour, et les paramètres de révocation pour D s'appliquent également lorsque C est supprimé ou que D est révoqué.

Dans ce contexte, la configuration du fournisseur d'identités effectue ce qui suit dans XenMobile :

- Détermine la source des certificats.
- Détermine la méthode grâce à laquelle les certificats sont obtenus : signature d'un nouveau certificat ou récupération d'un certificat existant et d'une paire de clés.
- Détermine les paramètres d'émission ou de récupération. Par exemple, les paramètres de demande de signature de certificat (CSR), tels que la taille de la clé, l'algorithme de clé, le nom unique, les extensions de certificat, etc.
- Détermine la façon dont les certificats sont mis à disposition sur l'appareil.
- Détermine les conditions de révocation. Bien que tous les certificats soient révoqués dans XenMobile lorsque la relation de gestion est rompue, la configuration peut spécifier une révocation antérieure, par exemple lorsque la configuration d'appareil associé est supprimée. En outre, dans certaines conditions, il se peut que la révocation du certificat associé dans XenMobile puisse être envoyée à l'infrastructure interne à clé publique (PKI) principale ; en d'autres termes, sa révocation dans XenMobile peut provoquer sa révocation sur la PKI.
- Détermine les paramètres de renouvellement. Les certificats obtenus via un fournisseur d'identités peuvent être automatiquement renouvelés lors de leur expiration, ou des notifications peuvent être émises lorsque cette expiration approche.

La mesure dans laquelle les différentes options de configuration sont disponibles dépend principalement du type d'entité PKI et de la méthode d'émission que vous sélectionnez pour un fournisseur d'identités.

Méthodes d'émission de certificats

Vous pouvez obtenir un certificat, désigné comme méthodes d'émission de deux manières différentes :

- Signature. Avec cette méthode, l'émission implique la création d'une nouvelle clé privée, la création d'une demande de signature de certificat (CSR) et la soumission de la demande de signature de certificat à une autorité de certification (CA) pour signature. XenMobile prend en charge la méthode de signature des trois entités PKI (Entité Services de certificats Microsoft, PKI générique et CA discrétionnaire).
- Récupération. Dans le cadre de XenMobile, cette méthode implique la récupération d'une paire de clés. XenMobile prend en charge la méthode de récupération uniquement pour l'entité PKI générique.

Un fournisseur d'identités utilise l'une ou l'autre de ces deux méthodes d'émission. La méthode sélectionnée affecte les options de configuration disponibles. Notamment, la configuration CSR et la mise à disposition distribuée sont uniquement disponibles si la méthode d'émission est la signature. Un certificat de récupération est toujours envoyé à l'appareil au format PKCS#12, ce qui correspond à une méthode de mise à disposition centralisée pour la méthode de signature.

Mise à disposition de certificats

Deux modes de mise à disposition de certificats sont disponibles dans XenMobile : centralisée et distribuée. Le mode Distribué utilise le protocole d'inscription du certificat simple (SCEP) et est uniquement disponible dans les situations dans lesquelles le client prend en charge le protocole (iOS uniquement). Le mode distribué est même obligatoire dans certains cas.

Pour qu'un fournisseur d'identités prenne en charge la mise à disposition (assisté par SCEP) distribuée, une étape de configuration spéciale est nécessaire : configuration des certificats de l'autorité d'inscription (RA). Les certificats RA sont requis, car lors de l'utilisation du protocole SCEP, XenMobile agit comme un délégué (registre) pour l'autorité de certification réelle, et doit prouver au client qu'il possède l'autorité d'agir en tant que tel. Cette autorité est établie en offrant à XenMobile les certificats mentionnés plus haut.

Deux rôles de certificat distincts sont requis (bien qu'un seul certificat puisse remplir les deux rôles) : la signature RA et le chiffrement RA. Les contraintes pour ces rôles sont les suivantes :

- Le certificat de signature RA doit posséder une signature numérique d'utilisation de clé X.509.
- Le certificat de chiffrement RA doit posséder un chiffrement de clé d'utilisation de clé X.509.

Pour configurer les certificats RA du fournisseur d'identités, vous devez charger les certificats sur XenMobile, puis les associer au fournisseur d'identités.

Un fournisseur d'identités est considéré comme pouvant uniquement prendre en charge une mise à disposition distribuée s'il possède un certificat configuré pour les rôles de certificat. Chaque fournisseur d'identités peut être configuré pour privilégier au choix le mode centralisé, le mode distribué ou pour requérir le mode distribué. Le résultat réel dépend du contexte : si le contexte ne prend pas en charge le mode distribué, mais que le fournisseur d'identités requiert ce mode, le déploiement échoue. De même, si le contexte requiert le mode distribué, mais que le fournisseur d'identités ne le prend pas en charge, le déploiement échoue. Dans tous les autres cas, le paramètre préféré est appliqué.

Le tableau suivant présente la distribution SCEP au travers de XenMobile :

Contexte	SCEP pris en charge	SCEP requis
Service de profil iOS	Oui	Oui
Inscription à la gestion des appareils mobiles iOS	Oui	Non
Profils de configuration iOS	Oui	Non
Inscription SHTP	Non	Non
Configuration de SHTP	Non	Non
Inscription de Windows Phone et Tablet	Non	Non

Contexte	SCEP pris en charge	SCEP requis
Configuration de Windows Phone et Tablet	Non, à l'exception de la Stratégie Wi-Fi, qui est prise en charge sur Windows Phone 8.1 et la dernière version de Windows 10	Non

Révocation de certificats

Il existe trois types de révocation.

- **Révocation interne**. La révocation interne du certificat affecte le statut du certificat géré par XenMobile. Ce statut est pris en compte lorsque XenMobile évalue un certificat qui lui est présenté, ou lorsque XenMobile doit fournir des informations sur le statut du protocole OCSP pour certains certificats. La configuration du fournisseur d'identités détermine la manière dont le statut est affecté par plusieurs conditions. Par exemple, le fournisseur d'identités peut spécifier que les certificats obtenus auprès du fournisseur de certificats doivent être marqués comme révoqués lorsqu'ils ont été supprimés de l'appareil.
- **Révocation propagée en externe**. Également appelée révocation XenMobile, ce type de révocation s'applique aux certificats obtenus à partir d'une PKI externe. Le certificat est révoqué sur la PKI lorsque le certificat est révoqué en interne par XenMobile, sous les conditions définies par la configuration du fournisseur d'identités. La demande de révocation requiert une entité GPKI disposant d'une capacité de révocation.
- **Révocation induite en interne**. Également appelée PKI de révocation, ce type de la révocation s'applique uniquement aux certificats obtenus à partir d'une PKI externe. Chaque fois que XenMobile évalue le statut d'un certificat donné, XenMobile interroge la PKI afin de déterminer ce statut. Si le certificat est révoqué, XenMobile révoque le certificat en interne. Ce mécanisme utilise le protocole OCSP.

Ces trois types ne sont pas exclusifs, mais s'appliquent conjointement. La révocation interne est provoquée soit par une révocation externe, soit par des observations indépendantes, et à son tour, la révocation interne entraîne potentiellement une révocation externe.

Renouvellement de certificat

Un renouvellement du certificat est la combinaison de révocation d'un certificat existant) et de l'émission d'un autre certificat.

Notez que XenMobile tente tout d'abord d'obtenir le nouveau certificat avant de révoquer le certificat précédent, afin d'éviter une discontinuité du service si l'émission échoue. Si une mise à disposition distribuée (prise en charge par SCEP) est utilisée, la révocation se produit une fois que le certificat a été correctement installé sur l'appareil, sinon la révocation se produit avant que le certificat ne soit envoyé à l'appareil et indépendamment de la réussite ou de l'échec de son installation.

La configuration de la révocation nécessite que vous spécifiiez une certaine durée (en jours). Lorsque l'appareil se connecte, le serveur vérifie que la date du certificat NotAfter est postérieure à la date actuelle, moins la durée spécifiée. Si c'est le cas, un renouvellement est tenté.

Pour créer un fournisseur d'identités

La configuration d'un fournisseur d'identités varie principalement en fonction de l'entité d'émission et de la méthode d'émission sélectionnées pour le fournisseur d'identités. Vous pouvez faire la distinction entre un fournisseur d'identités qui utilise une entité interne, telle que discrétionnaire, et un fournisseur d'identités qui utilise une entité externe, telle que Microsoft CA ou GPKI. La méthode d'émission pour une entité discrétionnaire est toujours signature, ce qui signifie qu'avec chaque opération d'émission, XenMobile signe une nouvelle paire de clés avec le certificat d'autorité de certification sélectionné pour l'entité. L'emplacement où la paire de clés est générée (l'appareil où le serveur) dépend de la méthode de

distribution sélectionnée.

1. Dans la console Web XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console, puis cliquez sur **Plus** > **Fournisseurs d'identités**.

2. Sur la page **Fournisseurs d'identités**, cliquez sur **Ajouter**.

La page **Fournisseurs d'identités : informations générales** s'affiche.

3. Sur la page **Fournisseurs d'identités : informations générales**, procédez comme suit :

- **Nom** : entrez un nom unique pour la nouvelle configuration du fournisseur. Ce nom sera utilisé par la suite pour faire référence à la configuration dans d'autres parties de la console XenMobile.
- **Description** : décrivez le fournisseur d'identités. Bien que ce champ soit facultatif, une description peut être utile dans le futur pour vous aider à vous souvenir des détails sur ce fournisseur d'identités.
- **Entité émettrice** : cliquez sur l'entité qui émet le certificat.
- **Méthode d'émission** : cliquez sur **Signer** ou **Récupérer** pour choisir la méthode que le système utilise pour obtenir des certificats auprès de l'entité configurée. Pour l'authentification de certificat client, utilisez **Signer**.
- Si la liste des modèles est disponible, sélectionnez un modèle pour le fournisseur d'identités.

4. Cliquez sur **Suivant**.

Remarque : ces modèles deviennent disponibles lorsque les entités Services de certificats Microsoft sont ajoutées sur **Paramètres** > **Plus** > **Entités PKI**.

La page **Fournisseur d'identités : demande de signature de certificat** s'affiche.

5. Sur la page **Fournisseur d'identités : demande de signature de certificat**, procédez comme suit :

- **Algorithme de clé** : cliquez sur l'algorithme de clé pour la nouvelle paire de clés. Les valeurs disponibles sont **RSA**, **DSA** et **ECDSA**.
- **Taille de la clé** : entrez la taille en octets de la paire de clés. Il s'agit d'un champ obligatoire.
  Remarque : les valeurs autorisées dépendent du type de clé ; par exemple, la taille maximale des clés DSA est de 1024 bits. Pour éviter de faux résultats négatifs, qui dépendront du matériel ou du logiciel sous-jacent, XenMobile n'exige pas l'utilisation d'une taille de clé particulière. Vous devez toujours tester les configurations de fournisseur d'identités dans un environnement de test avant de les activer dans un environnement de production.

- **Algorithme de signature** : cliquez sur une valeur pour le nouveau certificat. Les valeurs dépendent de l'algorithme de clé.
- **Nom du sujet** : entrez le nom unique (DN) du sujet du nouveau certificat. Par exemple : CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation Il s'agit d'un champ obligatoire.

  Par exemple, pour l'authentification du certificat client, utilisez ces paramètres :

  Algorithme de clé : RSA
  Taille de la clé : 2048
  Algorithme de signature : SHA1withRSA
  Nom du sujet: cn=$user.username

6. Pour ajouter une nouvelle entrée à la table **Noms de sujet alternatifs**, cliquez sur **Ajouter**. Sélectionnez le type de nom alternatif, puis tapez une valeur dans la deuxième colonne.

  Pour l'authentification du certificat client, spécifiez :

Type : nom principal de l'utilisateur
Valeur : $user.userprincipalname

Remarque : comme avec le nom du sujet, vous pouvez utiliser les macros XenMobile dans le champ de valeur.

7. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : distribution** s'affiche.

8. Sur la page **Fournisseurs d'identités : distribution**, procédez comme suit :

- Dans la liste **Certificat émis par l'autorité de certification**, cliquez sur le certificat d'autorité de certification proposé. Étant donné que le fournisseur d'identités utilise une entité d'autorité de certification discrétionnaire, le certificat d'autorité de certification du fournisseur d'identités sera toujours le certificat d'autorité de certification configuré sur l'entité elle-même ; il sera présenté ici à des fins de cohérence avec les configurations qui utilisent des entités externes.
- Dans **Sélectionner le mode de distribution**, sélectionnez l'une des méthodes de génération et de distribution de clés :
  - **Préférer mode centralisé : génération de la clé sur le serveur**. Citrix recommande cette option centralisée. Ce mode prend en charge toutes les plates-formes prises en charge par XenMobile et est requis lors de l'utilisation de l'authentification NetScaler Gateway. Les clés privées sont générées et stockées sur le serveur et distribuées sur les appareils des utilisateurs.
  - **Préférer mode distribué : génération de la clé sur l'appareil**. Les clés privées sont générées et stockées sur les appareils des utilisateurs. Ce mode distribué utilise SCEP et requiert un certificat de chiffrement RA avec le keyUsage keyEncryption et un certificat de signature RA avec le KeyUsage digitalSignature. Le même certificat peut être utilisé pour le chiffrement et la signature.
  - **Distribué uniquement : génération de la clé sur l'appareil**. Cette option fonctionne de la même façon que Préférer mode distribué : génération de la clé sur l'appareil, sauf qu'étant « Uniquement » au lieu de « Préférer », aucune option n'est disponible si la génération de la clé sur l'appareil échoue.

Si vous avez sélectionné **Préférer mode distribué : génération de la clé sur l'appareil** ou **Distribué uniquement : génération de la clé sur l'appareil**, cliquez sur le certificat de signature RA et le certificat de chiffrement RA. Le même certificat peut être utilisé pour les deux modes. De nouveaux champs apparaissent pour ces certificats.

9. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : révocation XenMobile** s'affiche. Sur cette page, vous configurez les conditions dans lesquelles XenMobile marque (en interne) comme révoqué les certificats émis au travers de cette configuration de fournisseur.

12. Sur la page **Fournisseurs d'identités : révocation XenMobile**, procédez comme suit :

- Dans **Révoquer les certificats émis**, sélectionnez l'une des options qui indique quand les certificats doivent être révoqués.
- Si vous voulez que XenMobile envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **On** et choisissez un modèle de notification.

- Si vous souhaitez révoquer le certificat sur la PKI lorsque le certificat est révoqué de XenMobile, définissez **Révoquer le certificat auprès de la PKI** sur **On** et cliquez sur un modèle dans la liste **Entité**. La liste Entité répertorie toutes les entités GPKI disponibles avec des capacités de révocation. Lorsque le certificat est révoqué de XenMobile, une demande de révocation est envoyée à la PKI sélectionnée à partir de la liste Entité.

13. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : révocation PKI** s'affiche. Sur cette page, identifiez les actions à effectuer sur la PKI si le certificat est révoqué. Vous avez aussi la possibilité de créer un message de notification.

14. Sur la page **Fournisseurs d'identités : révocation PKI**, procédez comme suit si vous souhaitez révoquer les certificats de la PKI :

- Modifiez le paramètre **Activer les vérifications de révocation externe** sur **On**. Des champs supplémentaires liés à la PKI de révocation apparaissent.
- Dans la liste **Certificat CA du répondeur OCSP**, cliquez sur le nom unique (DN) du sujet du certificat. **Remarque :** vous pouvez utiliser les macros XenMobile pour les valeurs de champ de nom unique. Par exemple : CN=${user.username}, OU=${user.department}, O=${user.companyname}, C=${user.c}\endquotation
- Dans la liste **Lorsque le certificat est révoqué**, cliquez sur l'une des actions suivantes à entreprendre sur l'entité PKI lorsque le certificat est révoqué :

  Ne rien faire.

  Renouveler le certificat.

  Révoquer et de réinitialiser l'appareil.

- Si vous voulez que XenMobile envoie une notification lorsque le certificat est révoqué, définissez la valeur de **Envoyer une notification** sur **On**.

Vous avez le choix entre deux options de notification :

- Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
- Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

15. Cliquez sur **Suivant**.

La page **Fournisseurs d'identités : renouvellement** s'affiche. Sur cette page, vous pouvez configurer XenMobile pour effectuer les opérations suivantes :

- Renouveler le certificat et envoyer (facultatif) une notification lorsque cette opération est terminée (notification envoyée lors du renouvellement), et exclure (facultatif) les certificats déjà expirés de l'opération.
- Émettre une notification pour les certificats dont l'expiration approche (avant le renouvellement).

16. Sur la page **Fournisseurs d'identités: renouvellement**, procédez comme suit si vous souhaitez renouveler les certificats lorsqu'ils expirent : Réglez **Renouveler les certificats lorsqu'ils expirent** sur **On**.

Des champs supplémentaires s'affichent.

- Dans le champ **Renouveler lorsque le certificat expire dans**, entrez quand le renouvellement doit être effectué, en nombre de jours avant l'expiration.
- Si vous le souhaitez, sélectionnez **Ne pas renouveler les certificats expirés**. **Remarque :** dans ce cas, « expiré » signifie que la date NotAfter (fin de validité) du certificat est dans le passé, et non pas qu'il a été révoqué. XenMobile ne renouvellera pas les certificats une fois qu'ils ont été révoqués en interne.

17. Si vous voulez que XenMobile envoie une notification lorsque le certificat a été renouvelé, définissez **Envoyer une**

notification sur **On**. Vous avez le choix entre deux options de notification :

- Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste Modèle de notification.
- Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

18. Si vous voulez que XenMobile envoie une notification lorsque la certification arrive à échéance, définissez **Notifier quand un certificat va expirer** sur **On**. Vous avez le choix entre deux options de notification :

- Si vous sélectionnez **Sélectionner un modèle de notification**, vous pouvez sélectionner un message de notification pré-rempli que vous pouvez personnaliser. Ces modèles figurent dans la liste **Modèle de notification**.
- Si vous sélectionnez **Entrer les détails de notification**, vous pouvez créer votre propre message de notification. En plus de fournir l'adresse e-mail du destinataire et le message, vous pouvez définir la fréquence à laquelle la notification est envoyée.

19. Dans le champ **Notifier lorsque le certificat expire dans**, entrez le nombre de jours avant expiration du certificat après lequel la notification doit être envoyée.

20. Cliquez sur **Enregistrer**.

Le fournisseur d'identités est ajouté à la table Fournisseur d'identités.

Certificats APNs

Mar 31, 2017

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat Apple Push Notification Service (APNS). Cette section présente les étapes de base à suivre pour demander le certificat APNS :

- Utiliser un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft Internet Information Server (IIS) ou un ordinateur Mac pour générer une demande de signature de certificat (CSR).
- Faire signer la demande de signature de certificat (CSR) par Citrix.
- Demander un certificat APNS à Apple.
- Importer le certificat dans XenMobile.

Remarque :

- Le certificat APNS d'Apple permet de gérer les appareils mobiles via le réseau Apple Push Network. Si vous avez délibérément ou accidentellement révoqué le certificat, vous perdrez la possibilité de gérer vos appareils.
- Si vous avez utilisé iOS Developer Enterprise Program pour créer un certificat push de gestion des appareils mobiles, vous devrez peut-être intervenir en raison de la migration des certificats existants vers le portail Apple Push Certificats Portal.

Les rubriques expliquant les procédures détaillées sont répertoriées par ordre dans cette section comme suit :

Étape 1	Créer une demande de signature de certificat dans IIS Créer une demande de signature de certificat sur un Mac	Générez une demande de signature de certificat avec un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft IIS ou sur un ordinateur Mac. Citrix recommande cette méthode.
Étape 2	Pour signer la CSR	Envoyez la CSR à Citrix sur le site Web XenMobile APNs CSR Signing (un ID MyCitrix est requis). Citrix signe la demande de signature de certificat (CSR) à l'aide de son certificat de signature de gestion d'appareils mobiles et renvoie le fichier signé au format .plist.
Étape 3	Soumettre la demande de signature de certificat (CSR) signée à Apple	Soumettre la demande de signature de certificat (CSR) signée à Apple sur le portail Apple Push certificat Portal (Apple ID obligatoire), puis télécharger le certificat APNS d'Apple.
Étape 4	Pour créer un certificat APNS .pfx avec Microsoft IIS Pour créer un certificat APNS .pfx sur un Mac Créer un certificat	Exporter le certificat APN comme certificat PCKS #12 (.pfx) (sur IIS, Mac ou SSL).

	APNS .pfx en utilisant OpenSSL	
Étape 5	Importer un certificat APNS dans XenMobile	Importez le certificat dans XenMobile.

Informations de migration du certificat Push MDM Apple

Les certificats push MDM (gestion des appareils mobiles) créés dans le iOS Developer Enterprise Program ont été migrés vers le portail Apple Push Certificats Portal. Cette migration affecte la création de nouveaux certificats push MDM, ainsi que le renouvellement, la révocation et le téléchargement de certificats push MDM existants. La migration n'affecte pas les autres certificats APNS (non MDM).

Si votre certificat push MDM a été créé dans le iOS Developer Enterprise Program, les situations suivantes s'appliquent :

- Le certificat a été migré automatiquement pour vous.
- Vous pouvez renouveler le certificat dans le portail Apple Push Certificats Portal sans affecter vos utilisateurs.
- Vous devez utiliser le programme iOS Developer Enterprise Program pour révoquer ou télécharger un certificat préexistant.

Si aucun de vos certificats push MDM n'est proche de l'expiration, vous n'avez rien à faire. Si vous disposez d'un certificat push MDM dont l'expiration est proche, contactez le fournisseur de votre solution MDM. Ensuite, demandez à votre iOS Developer Program Agent de se connecter au portail Apple Push Certificates Portal avec son Apple ID.

Tous les nouveaux certificats push MDM doivent être créés dans le portail Apple Push Certificats Portal. Le programme iOS Developer Enterprise Program n'autorisera plus la création d'un Apple ID avec un identificateur de bundle (section APNS) contenant com.apple.mgmt.

Remarque : vous devez conserver l'Apple ID utilisé pour créer le certificat. En outre, l'Apple ID doit être un ID d'entreprise et non un ID personnel.

Pour créer une demande de signature de certificat à l'aide de Microsoft IIS

La première étape de génération d'une demande de certificat APNS pour les appareils iOS consiste à créer une demande de signature de certificat (CSR). Sur un serveur Windows 2012 R2 où Windows 2008 R2, vous pouvez générer une demande de signature de certificat à l'aide de Microsoft IIS.

1. Ouvrez Microsoft IIS.
2. Double-cliquez sur l'icône Certificats de serveur pour IIS.
3. Dans la fenêtre Certificats de serveur, cliquez sur **Créer une demande de certificat**.
4. Tapez les informations de nom unique (DN) appropriées, puis cliquez sur **Suivant**.
5. Sélectionnez le **Fournisseur de services de chiffrement Microsoft RSA SChannel** pour le fournisseur de services de chiffrement et **2048** pour la longueur en bits, puis cliquez sur **Suivant**.
6. Entrez un nom de fichier et spécifiez un emplacement pour enregistrer la CSR, puis cliquez sur **Terminer**.

Pour créer une demande de signature de certificat sur un Mac

1. Sur un Mac exécutant Mac OS X, sous **Applications** > **Utilitaires**, démarrez l'application Trousseau d'accès.
2. Ouvrez le menu **Trousseau d'accès** et cliquez sur **Préférences**.

3. Cliquez sur l'onglet **Certificats**, définissez les options **OCSP** et **CRL** sur **Désactivé**, puis fermez la fenêtre Préférences.
4. Dans le menu **Trousseau d'accès**, cliquez sur **Assistant de certification** > **Demander un certificat à une autorité de certification**.
5. L'Assistant de certification vous invite à entrer les informations suivantes :
   1. **Adresse e-mail**. Adresse de messagerie de la personne ou du compte de rôle qui est responsable de la gestion du certificat.
   2. **Nom commun**. Nom commun de la personne ou compte de rôle qui est responsable de la gestion du certificat.
   3. **Adresse e-mail de l'AC**. Adresse de messagerie de l'autorité de certification.
6. Sélectionnez **Enregistrée sur le disque** et **Me laisser indiquer les informations sur la bi-clé** et cliquez sur **Continuer**.
7. Entrez un nom pour le fichier CSR, enregistrez le fichier sur votre ordinateur, puis cliquez sur **Enregistrer**.
8. Spécifiez les informations de bi-clé en sélectionnant la **Dimension de clé** de 2048 bits et **Algorithme RSA**, puis cliquez sur **Continuer**. Le fichier CSR est prêt à être chargé dans le cadre du processus de certificat APNS.
9. Cliquez sur **Terminé** lorsque l'Assistant de certification termine le processus de demande de signature de certificat.

Pour créer une demande de signature de certificat avec OpenSSL

Si vous ne pouvez pas utiliser un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft Internet Information Server (IIS) ou un ordinateur Mac pour générer une demande de signature de certificat (CSR) à soumettre à Apple afin d'obtenir le certificat Apple Push Notification Service (APNS), vous pouvez utiliser OpenSSL.

Remarque : pour pouvoir utiliser OpenSSL pour créer une demande de signature de certificat, vous devez télécharger et installer OpenSSL à partir du site Web OpenSSL.

1. Sur l'ordinateur sur lequel vous avez installé OpenSSL, exécutez la commande suivante à partir d'une invite de commandes ou de shell.
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. Le message suivant s'affiche pour les informations de nom du certificat. Entrez les informations demandées.
   Vous êtes sur le point d'être invité à entrer des informations qui seront incorporées
   dans votre requête de certificat.
   Ce que vous allez entrer s'appelle un nom unique ou DN.
   Il existe un grand nombre de champs mais vous pouvez laisser certains champs vides
   . Pour certains champs, il y aura une valeur par défaut.
   Si vous entrez '.', le champ reste vide.

   Country Name (code à 2 lettres) [AU]:US
   State or Province Name (nom complet) [Some-State]:CA
   Locality Name (ville, par exemple) []:RWC
   Organization Name (société, par exemple) [Internet Widgits Pty Ltd]:Customer
   Organizational Unit Name (section, par exemple) []:Marketing
   Common Name (VOTRE nom, par exemple) []:John Doe
   Email Address []:john.doe@customer.com

3. Dans le message suivant, entrez un mot de passe pour la clé privée de la demande de signature de certificat.
   Entrez les deux attributs supplémentaires suivants
   à envoyer avec votre demande de certificat.
   A challenge password []:
   An optional company name []:

4. Envoyez la demande de signature de certificat à Citrix.

Citrix prépare la demande de signature de certificat (CSR) signée et renvoie le fichier par courrier électronique.

Pour signer la CSR

Avant d'envoyer le certificat à Apple, ce dernier doit être signé par Citrix de façon à pouvoir être utilisé avec XenMobile.

1. Dans votre navigateur, accédez au site Web XenMobile APNs CSR Signing.
2. Cliquez sur **Upload the CSR**.
3. Localisez et sélectionnez le certificat.
   Remarque : le certificat doit être au format .pem/txt.
4. Sur la page XenMobile APNs CSR Signing, cliquez sur **Sign**. La CSR est signée et automatiquement enregistrée sur votre dossier de téléchargement configuré.

Pour soumettre la demande de signature de certificat (CSR) à Apple afin d'obtenir le certificat APNS

Après la réception de votre demande de signature de certificat (CSR) signée de Citrix, vous devez la soumettre à Apple pour obtenir le certificat APNS.

Remarque : certains utilisateurs ont signalé des problèmes lors de la connexion au portail Apple Push Portal. Vous pouvez également vous connecter au portail Apple Developer Portal (http://developer.apple.com/devcenter/ios/index.action) avant d'accéder au lien identity.apple.com dans l'étape 1.

1. Dans un navigateur, accédez à https://identity.apple.com/pushcert.
2. Cliquez sur **Create a Certificate**.
3. Si c'est la première fois que vous créez un certificat avec Apple, sélectionnez la case **I have read and agree to these terms and conditions** et cliquez sur **Accept**.
4. Cliquez sur **Choose File** pour charger votre CSR signée, accédez à la demande sur votre ordinateur, puis cliquez sur **Upload**. Un message de confirmation doit s'afficher indiquant que le chargement a réussi.
5. Cliquez sur **Download** pour récupérer le certificat .pem.
   Remarque : si vous utilisez Internet Explorer et que l'extension de fichier est manquante, cliquez sur **Cancel** à deux reprises puis sur Download dans la fenêtre suivante.

Pour créer un certificat APNS .pfx avec Microsoft IIS

Pour utiliser le certificat APNS d'Apple avec XenMobile, vous devez effectuer la demande de certificat dans Microsoft IIS, exporter le certificat comme fichier PCKS #12 (.pfx), puis importer le certificat APNS dans XenMobile.

Important : pour cette tâche, vous devez utiliser le même serveur IIS que le serveur utilisé pour générer la CSR.

1. Ouvrez Microsoft IIS.
2. Cliquez sur l'icône Certificats de serveur.
3. Dans la fenêtre **Certificats de serveur**, cliquez sur **Terminer la demande de certificat**.
4. Accédez au fichier Certificate.pem d'Apple. Tapez ensuite un nom convivial ou le nom du certificat, puis cliquez sur **OK**.
5. Sélectionnez le certificat que vous avez identifié dans l'étape 4, puis cliquez sur **Exporter**.
6. Spécifiez un emplacement et un nom de fichier pour le certificat .pfx ainsi qu'un mot de passe, puis cliquez sur **OK**.
   Remarque : vous devez fournir le mot de passe pour le certificat au cours de l'installation de XenMobile.
7. Copiez le certificat .pfx sur le serveur sur lequel XenMobile sera installé.
8. Ouvrez une session sur la console XenMobile en tant qu'administrateur.

9. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
10. Cliquez sur **Certificats**. La page **Certificats** s'affiche.
11. Cliquez sur **Importer**. La boîte de dialogue **Importer** s'affiche.
12. Depuis le menu **Importer**, sélectionnez **Keystore**.
13. Dans **Utiliser en tant que**, choisissez **APNS**.
14. Dans le fichier **keystore**, sélectionnez le fichier de keystore que vous souhaitez importer, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
15. Dans **Mot de passe**, entrez le mot de passe affecté au certificat.
16. Cliquez sur **Importer**.

Pour créer un certificat APNS .pfx sur un Mac

1. Sur le même ordinateur Mac exécutant Mac OS X que vous avez utilisé pour générer la demande de signature de certificat, localisez le certificat .pem que vous avez reçu d'Apple.
2. Cliquez deux fois sur le fichier de certificat pour importer le fichier dans le trousseau.
3. Si vous êtes invité à ajouter le certificat à un trousseau spécifique, conservez le trousseau de connexion sélectionné par défaut, puis cliquez sur **OK**. Le certificat qui vient d'être ajouté apparaîtra dans votre liste de certificats.
4. Cliquez sur le certificat puis sur le menu **Fichier**, cliquez sur **Exporter** pour commencer l'exportation du certificat dans un certificat PCKS #12 (.pfx).
5. Donnez au fichier de certificat un nom unique à utiliser dans le serveur XenMobile, choisissez un emplacement de dossier pour le certificat enregistré, sélectionnez le format du fichier .pfx, puis cliquez sur **Enregistrer**.
6. Entrez un mot de passe pour l'exportation du certificat. Citrix vous recommande d'utiliser un mot de passe fort et unique. Par ailleurs, conservez le certificat et le mot de passe de manière sécurisée à des fins d'utilisation ultérieure et de référence.
7. L'application Trousseau d'accès vous invitera à saisir le mot de passe ou le trousseau sélectionné. Entrez le mot de passe, puis cliquez sur **OK**. Le certificat enregistré est maintenant prêt à être utilisé avec le serveur XenMobile.
   Remarque : si vous ne souhaitez pas conserver l'ordinateur et le compte d'utilisateur que vous avez utilisés pour générer la demande de signature de certificat et terminer le processus d'exportation du certificat, Citrix vous recommande d'enregistrer ou d'exporter les clés publiques ou personnelles du système local. Sinon, l'accès aux certificats APNS à des fins de réutilisation sera annulé et vous devrez répéter le processus de demande de signature de certificat et APNs depuis le début.

Pour créer un certificat APNS .pfx avec OpenSSL

Lorsque vous utilisez OpenSSL pour créer une demande de signature de certificat (CSR), vous pouvez également utiliser OpenSSL pour créer un certificat APNS .pfx.

1. À l'invite de commandes ou shell, exécutez la commande suivante.
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12

2. Entrez un mot de passe pour le fichier de certificat .pfx. Mémorisez ce mot de passe car vous devez l'utiliser pour charger le certificat sur XenMobile.
3. Notez l'emplacement du fichier de certificat .pfx, puis copiez le fichier sur le serveur XenMobile, de façon à pouvoir utiliser la console XenMobile pour charger le fichier.

Pour importer un certificat APNS dans XenMobile

Une fois que vous avez demandé et reçu un nouveau certificat APNS, vous devez l'importer dans XenMobile pour ajouter le certificat (pour la première fois) ou remplacer un certificat existant.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Cliquez sur **Certificats**. La page **Certificats** s'affiche.
3. Cliquez sur **Importer**. La boîte de dialogue **Importer** s'affiche.
4. Depuis le menu **Importer**, sélectionnez **Keystore**.
5. Dans **Utiliser en tant que**, choisissez **APNS**.
6. Accédez au fichier .p12 sur votre ordinateur.
7. Entrez un mot de passe et cliquez sur **Importer**.

Pour de plus amples informations sur les certificats dans XenMobile, consultez la section Certificats.

Pour renouveler un certificat APNS

Pour renouveler un certificat APNS, vous devez effectuer la même procédure que si vous en créiez un nouveau. Ensuite, visitez le portail Apple Push Certificats Portal et chargez le nouveau certificat. Après avoir ouvert une session, vous pourrez voir votre certificat existant ou un certificat qui a été importé à partir de votre ancien compte Apple Developers. Sur la page Certificats Portal, la seule différence lors du renouvellement du certificat est que vous cliquez sur **Renew**. Vous devez avoir un compte de développeur auprès du Certificates Portal pour accéder au site. Lorsque vous renouvellez votre certificat, assurez-vous d'utiliser le même nom d'organisation et ID Apple.

Remarque : pour déterminer la date à laquelle votre certificat APNS expire, dans la console XenMobile, cliquez sur **Configurer** > **Paramètres** > **Certificats**. Si le certificat a expiré, cependant, ne le révoquez pas.

1. Générez une demande de signature de certificat via Microsoft Internet Information Services (IIS).
2. Sur le site Web XenMobile APNs CSR Signing, chargez la nouvelle CSR et cliquez sur **Sign**.
3. Soumettez la demande de signature de certificat (CSR) signée à Apple sur le portail Apple Push certificat Portal.
4. Cliquez sur **Renew**.
5. Générez un certificat APNS PCKS #12 (.pfx) à l'aide de Microsoft IIS.
6. Mettez à jour le nouveau certificat APNS dans la console XenMobile. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console. La page **Paramètres** s'affiche.
7. Cliquez sur **Certificats**. La page **Certificats** s'affiche.
8. Cliquez sur **Importer**. La boîte de dialogue **Importer** s'affiche.
9. Depuis le menu **Importer**, sélectionnez **Keystore**.
10. Dans **Utiliser en tant que**, choisissez **APNS**.
11. Accédez au fichier .p12 sur votre ordinateur.
12. Entrez un mot de passe et cliquez sur **Importer**.

SAML pour l'authentification unique avec ShareFile

Feb 23, 2017

Vous pouvez configurer XenMobile et ShareFile pour utiliser Security Assertion Markup Language (SAML) afin de fournir un accès SSO (authentification unique) aux applications mobiles ShareFile qui sont wrappées avec le MDX Toolkit, ainsi qu'aux clients ShareFile non wrappés, tel que le site Web, le plug-in Outlook ou les clients de synchronisation.

- **Pour les applications ShareFile wrappées**. Les utilisateurs qui ouvrent une session sur ShareFile via l'application mobile ShareFile sont redirigés vers Secure Hub pour l'authentification utilisateur et pour acquérir un jeton SAML. Une fois l'authentification réussie, l'application mobile ShareFile envoie le jeton SAML à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder à l'application mobile ShareFile via l'authentification unique et peuvent joindre des documents provenant de ShareFile à des e-mails Secure Mail sans ouvrir une session à chaque fois.
- **Pour les clients ShareFile non wrappés**. Les utilisateurs qui ouvrent une session sur ShareFile à l'aide d'un navigateur Web ou d'un autre client ShareFile sont redirigés vers XenMobile pour l'authentification utilisateur et pour acquérir un jeton SAML. Une fois l'authentification réussie, le jeton SAML est envoyé à ShareFile. Après la première ouverture de session, les utilisateurs peuvent accéder aux clients ShareFile via l'authentification unique sans ouvrir une session à chaque fois.

Pour accéder à un diagramme d'architecture de référence détaillé, consultez l'article « Reference Architecture for On-Premises Deployments » du Manuel de déploiement de XenMobile.

Conditions préalables

Vous devez remplir les conditions suivantes pour pouvoir configurer l'authentification unique avec les applications XenMobile et ShareFile :

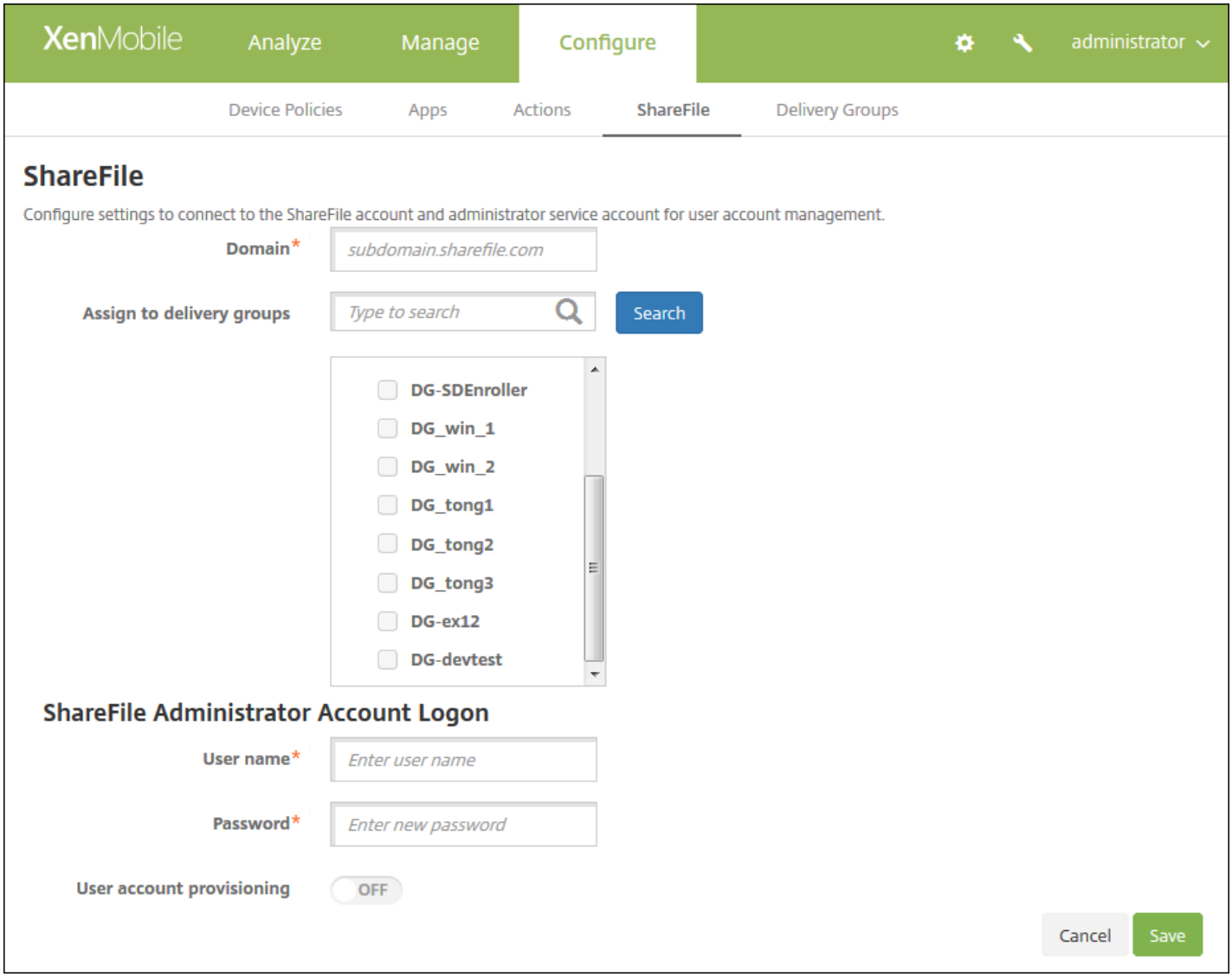
- MDX Toolkit version 9.0.4 ou version ultérieure (pour les applications mobiles ShareFile)
- Applications mobiles ShareFile appropriées :
  - ShareFile pour iPhone version 3.0.x
  - ShareFile pour iPad version 2.2.x
  - ShareFile pour Android version 3.2.x
- Secure Hub 9.0 (pour les applications mobiles ShareFile) : installez la version iOS ou Android.
- Compte d'administrateur ShareFile

Assurez-vous que XenMobile et ShareFile peuvent se connecter.

Configurer l'accès à ShareFile

Avant de configurer SAML pour ShareFile, indiquez les informations d'accès à ShareFile comme suit :

1. Dans la console Web XenMobile, cliquez sur **Configurer > ShareFile**. La page de configuration de **ShareFile** s'affiche.



2. Configurez les paramètres suivants :

- **Domaine** : tapez votre nom de sous-domaine ShareFile, par exemple exemple.sharefile.com.
- **Attribuer aux groupes de mise à disposition** : sélectionnez ou recherchez les groupes de mise à disposition dont vous souhaitez qu'ils puissent utiliser l'authentification unique avec ShareFile.
- **Connexion au compte administrateur ShareFile**
  - **Nom d'utilisateur** : tapez le nom d'utilisateur administrateur ShareFile. Cet utilisateur doit disposer des privilèges d'administrateur.
  - **Mot de passe** : tapez le mot de passe d'administrateur ShareFile.
  - **Provisioning du compte utilisateur** : activez cette option si vous souhaitez activer le provisioning des utilisateurs dans XenMobile ; laissez-la désactivée si vous envisagez d'utiliser ShareFile User Management Tool.

    Remarque : si un utilisateur sans compte ShareFile est inclus dans les rôles sélectionnés, XenMobile provisionne automatiquement un compte ShareFile pour cet utilisateur si vous activez le Provisioning du compte utilisateur. Citrix vous recommande d'utiliser un rôle contenant peu de membres pour tester la configuration. Cela permet d'éviter qu'un grand nombre d'utilisateurs ne disposent pas d'un compte ShareFile.

3. Cliquez sur **Enregistrer**.

Configurer SAML pour les applications ShareFile MDX wrappées

Les étapes suivantes s'appliquent aux applications et appareils iOS et Android.

1. À l'aide du MDX Toolkit, wrappez l'application mobile ShareFile. Pour de plus amples informations sur le wrapping d'applications avec le MDX Toolkit, consultez la section Wrapping d'applications avec le MDX Toolkit.

2. Dans la console XenMobile, chargez l'application mobile ShareFile wrappée. Pour plus d'informations sur le chargement des applications MDX, consultez la section Pour ajouter une application MDX à XenMobile.

3. Vérifiez les paramètres SAML en ouvrant une session sur ShareFile avec le nom d'utilisateur et le mot de passe administrateur que vous avez configurés ci-dessus.

4. Assurez-vous que le même fuseau horaire est configuré pour ShareFile et XenMobile.

Remarque : assurez-vous que XenMobile indique l'heure appropriée par rapport au fuseau horaire configuré. Si ce n'est pas le cas, la fonctionnalité SSO peut échouer.

Valider l'application mobile ShareFile

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Secure Hub.

2. À partir de XenMobile Store, téléchargez et installez l'application mobile ShareFile.

3. Démarrez l'application mobile ShareFile. ShareFile démarre sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Valider avec Secure Mail

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Secure Hub.

2. À partir de XenMobile Store, téléchargez, installez et configurez Secure Mail.

3. Ouvrez un nouveau formulaire électronique et appuyez sur **Joindre à partir de ShareFile**. Les fichiers pouvant être joints à l'e-mail sont affichés sans vous inviter à saisir un nom d'utilisateur ou un mot de passe.

Configurer NetScaler Gateway pour les autres clients ShareFile

Si vous voulez configurer l'accès des clients ShareFile non wrappés, tels que le site Web, le plug-in Outlook ou les clients de synchronisation, vous devez configurer NetScaler Gateway pour prendre en charge l'utilisation de XenMobile en tant que fournisseur d'identité SAML de la manière suivante :

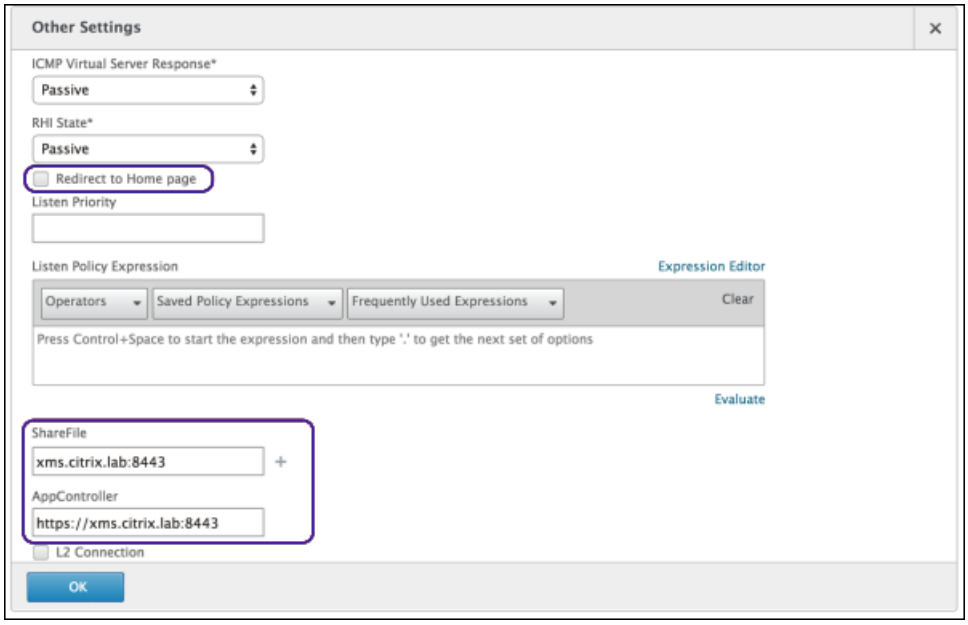
- Désactivez la redirection vers la page d'accueil.
- Créez une stratégie et un profil de session ShareFile.
- Configurez des stratégies sur le serveur virtuel NetScaler Gateway.

Désactiver la redirection vers la page d'accueil

Vous devez désactiver le comportement par défaut pour les demandes qui passent par le chemin d'accès /cginfra de manière à ce que l'utilisateur accède à l'URL interne demandée au lieu de la page d'accueil configurée.

1. Modifiez les paramètres du serveur virtuel NetScaler Gateway qui est utilisé pour les ouvertures de session XenMobile.

Dans NetScaler 10.5, cliquez sur **Other Settings**, puis désactivez la case à cocher intitulée **Redirect to Home Page**.



2. Sous **ShareFile**, tapez le nom de votre serveur interne XenMobile et le numéro de port.

3. Sous **AppController**, tapez l'URL de votre serveur XenMobile.

Cette configuration autorise les demandes pour l'URL indiquée via le chemin d'accès /cginfra.

Créer une stratégie et un profil de demande de session ShareFile

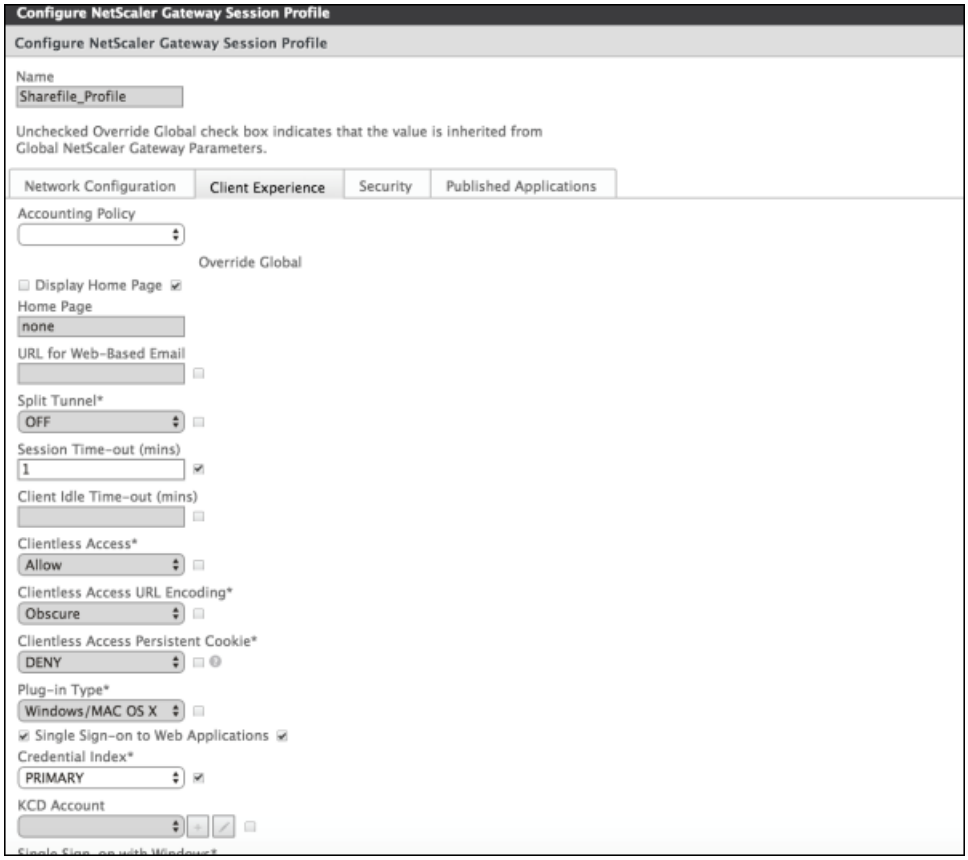
Configurez ces paramètres pour créer une stratégie et un profil de demande de session ShareFile :

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Policies > Session**.

2. Créez une stratégie de session. Dans l'onglet **Policies**, cliquez sur **Add**.

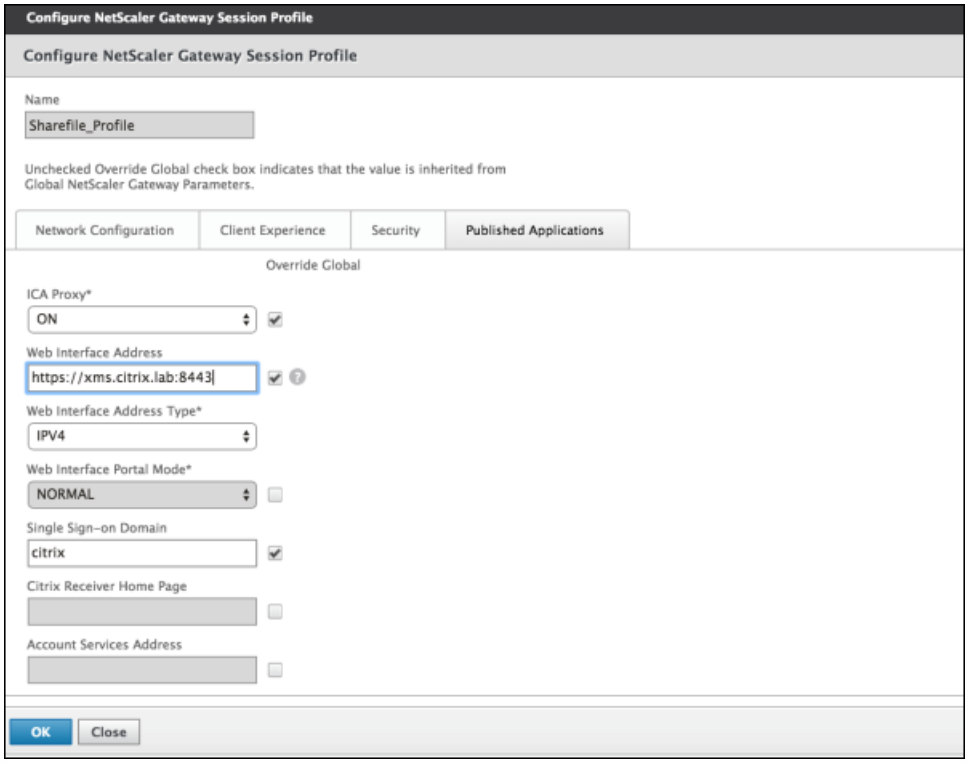
3. Dans le champ **Name**, tapez **ShareFile_Policy**.

4. Créez une action en cliquant sur le bouton **+**. La page **Create NetScaler Gateway Session Profile** s'affiche.



Pour configurer ces paramètres :

- **Name** : tapez ShareFile_Profile.
- Cliquez sur l'onglet **Client Experience**, puis configurez les paramètres suivants :
  - **Home Page** : tapez none.
  - **Session Time-out (mins)** : tapez 1.
  - **Single Sign-on to Web Applications** : sélectionnez ce paramètre.
  - **Credential Index** : dans la liste, cliquez sur PRIMARY.
- Cliquez sur l'onglet **Published Applications**.



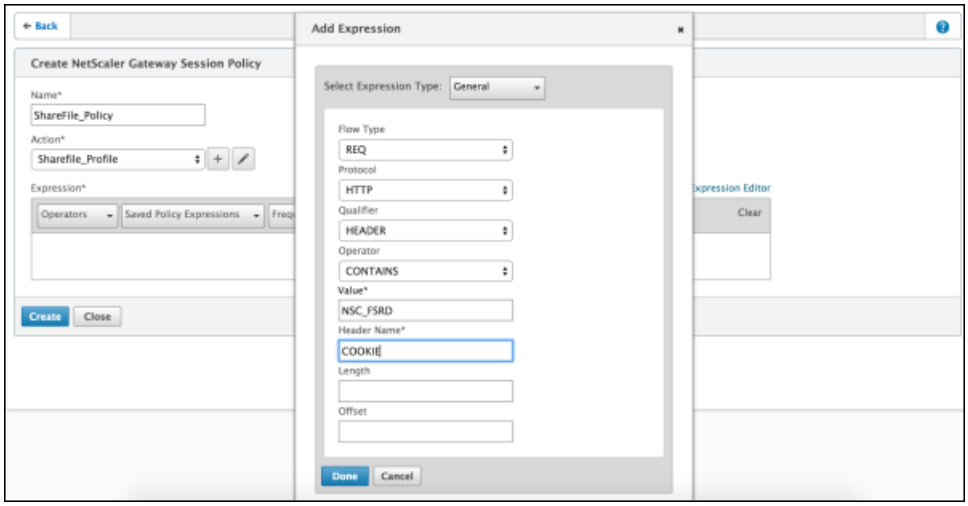
Pour configurer ces paramètres :

- **Proxy ICA** : dans la liste, cliquez sur **ON**.
- **Web Interface Address** : entrez l'URL de votre serveur XenMobile.
- **Single Sign-on Domain** : tapez votre nom de domaine Active Directory.

  Remarque : lors de la configuration du profil de session de NetScaler Gateway, le suffixe de domaine pour **Single Sign-on Domain** doit correspondre à l'alias de domaine XenMobile défini dans LDAP.

5. Cliquez sur **Create** pour définir le profil de session.

6. Cliquez sur **Expression Editor**.



Pour configurer ces paramètres :

- **Value** : tapez NSC_FSRD.
- **Header Name** : tapez COOKIE.
- Cliquez sur **Done**.

7. Cliquez sur **Create**, puis cliquez sur **Close**.

Configurer des stratégies sur le serveur virtuel NetScaler Gateway

Configurez les paramètres suivants sur le serveur virtuel NetScaler Gateway.

1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur **NetScaler Gateway > Virtual Servers**.

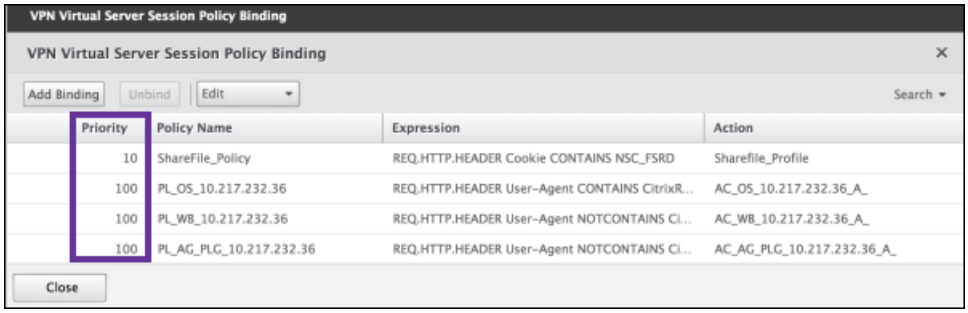
2. Dans le panneau **Details**, cliquez sur votre serveur virtuel NetScaler Gateway.

3. Cliquez sur **Edit**.

4. Cliquez sur **Configured policies > Session policies**, puis sur **Add binding**.

5. Sélectionnez **ShareFile_Policy**.

6. Modifiez le numéro de **priorité (Priority)** généré automatiquement pour la stratégie sélectionnée de manière à lui attribuer la priorité la plus élevée (le plus petit nombre) par rapport aux autres stratégies indiquées, comme illustré sur la figure suivante.



7. Cliquez sur **Terminé**, puis enregistrez la configuration NetScaler actuelle.

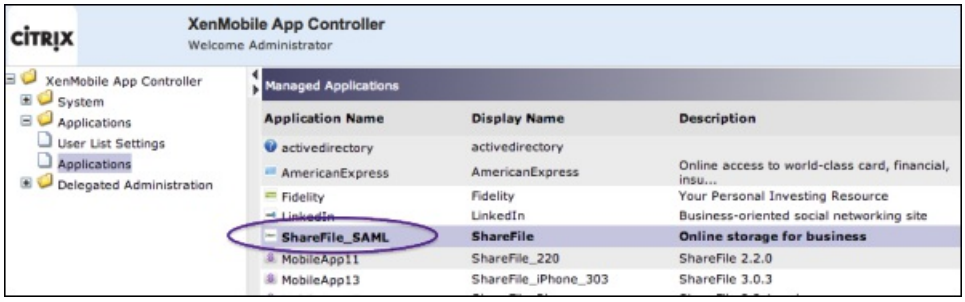
Configurer SAML pour les applications ShareFile non MDX

Procédez comme suit pour trouver le nom d'application interne pour votre configuration de ShareFile.

1. Ouvrez une session sur l'outil d'administration de XenMobile en accédant à la page suivante : **https://:4443/OCA/admin/**. Assurez-vous de saisir « OCA » en majuscules.

2. Dans la liste **View**, cliquez sur **Configuration**.

3. Cliquez sur **Applications** > Applications et notez le **nom de l'application (Application Name)** correspondant à l'application avec le **nom d'affichage (Display Name)** « ShareFile ».



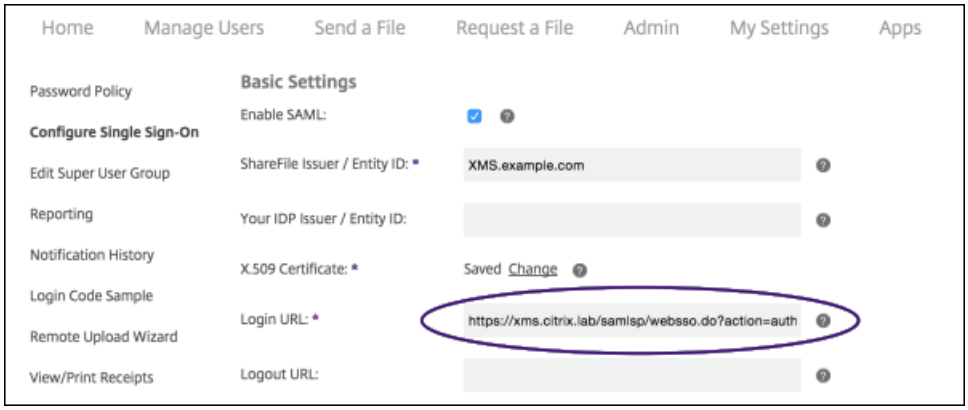
Modifier les paramètres d'authentification unique de ShareFile.com

1. Ouvrez une session sur votre compte ShareFile (https://<sous-domaine>.sharefile.com) en tant qu'administrateur.

2. Dans l'interface Web ShareFile, cliquez sur **Admin**, puis sélectionnez **Configurer le Single Sign-On**.

3. Modifiez **URL de connexion** comme suit :

URL de connexion doit ressembler à ceci : https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- Insérez le nom de domaine complet (FQDN) externe du serveur virtuel de NetScaler Gateway et « /cginfra/https/ » devant le nom de domaine complet du serveur XenMobile, puis ajoutez « 8443 » après le nom de domaine complet de XenMobile.

  L'URL doit maintenant ressembler à ce qui suit :
  https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- Remplacez le paramètre **&app=ShareFile_SAML_SP** par le nom interne de l'application ShareFile indiqué à l'étape 3 dans SAML pour l'authentification unique avec ShareFile. Le nom interne est **ShareFile_SAML** par défaut ; cependant, chaque fois que vous modifiez votre configuration, un nombre est ajouté au nom interne (ShareFile_SAML_2, ShareFile_SAML_3, etc.).

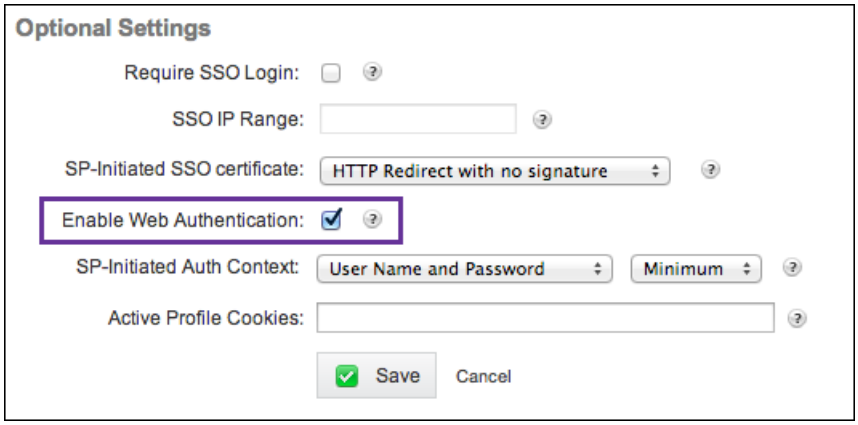
  L'URL doit maintenant ressembler à ce qui suit :
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**&app=ShareFile_SAML**&reqtype=1

- Ajoutez « &nssso=true » à la fin de l'URL.

  L'URL modifiée doit maintenant ressembler à ce qui suit :
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

  Important : chaque fois que vous modifiez ou recréez l'application ShareFile ou que vous modifiez les paramètres ShareFile dans la console XenMobile, un nombre est ajouté au nom d'application interne, ce qui signifie que vous devez également mettre à jour l'URL de connexion sur le site Web de ShareFile pour tenir compte du nouveau nom de l'application.

4. Sous **Paramètres facultatifs**, sélectionnez la case à cocher **Activer l'authentification Web**.



Valider la configuration

Procédez comme suit pour valider la configuration.

1. Dans votre navigateur, accédez à https://<sous-domaine>sharefile.com/saml/login.

Vous êtes redirigé vers l'écran d'ouverture de session de NetScaler Gateway. Si vous n'êtes pas redirigé, vérifiez les paramètres de configuration précédents.

2. Entrez le nom d'utilisateur et le mot de passe pour l'environnement NetScaler Gateway et XenMobile que vous avez configuré.

Vos dossiers ShareFile à l'adresse <sous-domaine>.ShareFile.com s'affichent. Si vos dossiers ShareFile n'apparaissent pas, assurez-vous que les informations d'identification saisies pour l'ouverture de session sont correctes.

Paramètres du serveur Microsoft Azure Active Directory

Mar 31, 2017

Les appareils exécutant Windows 10 s'inscrivent à Azure afin de fédérer l'authentification Active Directory. Vous pouvez associer les appareils Windows 10 à Microsoft Azure AD de l'une des manières suivantes :

- Inscription dans MDM dans le cadre de Azure AD Join la première fois que l'appareil est mis sous tension.
- Inscription dans MDM dans le cadre de Azure AD Join à partir de la page Paramètres de Windows une fois que l'appareil a été configuré. Cette fonctionnalité n'est pas disponible sur Windows Phone 10.
- Inscription dans MDM dans le cadre de Azure AD Join lors de l'ajout d'un compte de travail sur un appareil personnel.

Vous avez besoin d'une licence premium Active Directory Microsoft Azure avant de pouvoir intégrer XenMobile avec Microsoft Azure. La licence est requise pour activer l'intégration MDM avec Azure Active Directory de façon à ce que les utilisateurs avec des appareils Windows 10 puissent s'inscrire à l'aide d'Active Directory. Consultez Microsoft Azure pour de plus amples informations sur l'obtention de la licence premium.Pour plus d'informations sur les tarifs, veuillez consulter la section Tarifs Azure Active Directory.

Avant que les utilisateurs d'appareils Windows puissent s'inscrire à Azure, vous devez configurer les paramètres du serveur Microsoft Azure dans XenMobile, et configurer une stratégie termes et conditions pour les appareils Windows. Cet article explique comment configurer les paramètres Microsoft Azure. Pour de plus amples informations sur la configuration d'une stratégie termes et conditions pour les appareils Windows, consultez la section Stratégies termes et conditions.

Avant de pouvoir configurer les paramètres du serveur Microsoft Azure dans XenMobile, vous devez ouvrir une session sur le portail Azure AD et effectuez les opérations suivantes :

1. Enregistrez votre domaine personnalisé et vérifiez le domaine. Pour de plus amples informations, consultez la section Ajout de votre propre domaine à Azure Active Directory.

2. Étendez votre annuaire local à Azure Active Directory à l'aide des outils d'intégration d'annuaire. Pour de plus amples informations, consultez la section Intégration d'annuaire.

3. Faites du MDM une partie de confiance de Azure Active Directory. Pour ce faire, cliquez sur **Azure Active Directory** > **Applications**, puis sur **Ajouter**. Sélectionnez **Ajouter une application** à partir de la galerie. Accédez à **MOBILE DEVICE MANAGEMENT**, sélectionnez **On-premise MDM application**, puis enregistrez les paramètres.

4. Dans l'application, configurez la détection du serveur XenMobile, les points de terminaison des conditions d'utilisation et l'URI d'ID de l'application comme suit :

- URL de détection MDM : https://:8443/zdm/wpe
- URL des conditions d'utilisation MDM : https://:8443/zdm/wpe/tou
- URI d'ID de l'application : https://:8443/

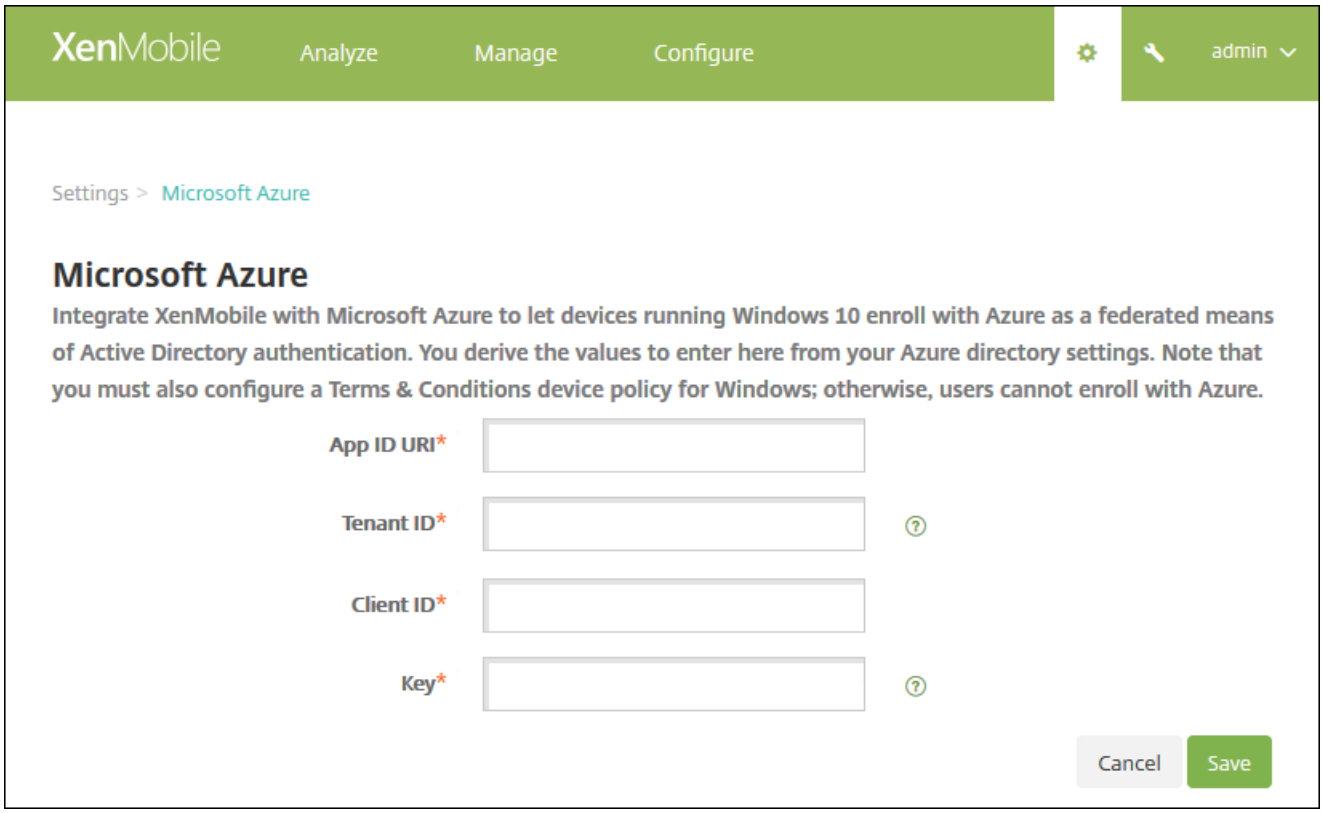
5. Sélectionnez l'application MDM locale que vous avez créée à l'étape 3 et activez l'option **Manage devices for these users** pour activer la gestion MDM pour tous les utilisateurs ou un groupe d'utilisateurs spécifique.

Vous devez également noter les informations suivantes à partir de votre compte Microsoft Azure afin de configurer les paramètres dans la console XenMobile.

- URI ID application : adresse URL du serveur exécutant XenMobile.
- ID du locataire : à partir de la page des paramètres d'application Azure.
- ID du client : identificateur unique pour votre application.
- Clé : dans la page des paramètres d'application Azure.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Plates-formes**, cliquez sur **Microsoft Azure**. La page **Microsoft Azure** s'affiche.



3. Pour configurer ces paramètres :

- **URI ID application** : entrez l'adresse URL du serveur exécutant XenMobile que vous avez entrée lorsque vous avez configuré vos paramètres Azure.
- **ID du locataire** : copiez cette valeur à partir de la page des paramètres d'application Azure. Dans la barre d'adresse du navigateur, copiez la section composée de chiffres et de lettres. Par exemple, dans https://manage.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem ..., l'ID du locataire est : *abc123-abc123-abc123*.
- **ID du client** : copiez et collez cette valeur depuis la page de configuration Azure. Il s'agit de l'identificateur unique pour votre application.
- **Clé** : copiez cette valeur à partir de la page des paramètres d'application Azure. Sous **Clés**, sélectionnez une durée dans la liste puis enregistrez le paramètre. Vous pouvez copier la clé et la coller dans ce champ. Une clé est requise lorsque les applications doivent lire et écrire des données dans Microsoft Azure Active Directory.

4. Cliquez sur **Enregistrer**.

Important

Lorsque les utilisateurs se connectent à Azure AD sur leurs appareils Windows, les stratégies d'appareils XenMobile Store et Weblink que vous avez configurées dans XenMobile sont uniquement disponibles pour les utilisateurs AD Azure, mais pas pour les utilisateurs locaux. Pour que les utilisateurs locaux puissent utiliser ces stratégies, ils doivent effectuer les opérations suivantes :

1. Se connecter à Azure Active Directory pour le compte d'un utilisateur Azure dans **Paramètres** > **À propos** > **Connecter à Azure AD**.
2. Fermer leur session Windows, puis se reconnecter avec un compte Azure AD.

Mettre à niveau

Mar 31, 2017

Lorsque de nouvelles versions ou des mises à jour importantes de XenMobile sont disponibles, elles sont publiées sur Citrix.com, et une notification est envoyée au point de contact de chaque client.

Vous disposez des options suivantes pour procéder à la mise à niveau de XenMobile :

- **Pour mettre à niveau XenMobile 9.0 vers XenMobile 10.4**
  Utilisez l'outil de mise à niveau XenMobile qui est intégré à XenMobile 10.4. Consultez les articles dans cette section pour plus de détails.
  L'outil de mise à niveau prend en charge toutes les éditions de XenMobile 9 : MDM, Applications et Enterprise.
  Pour accéder aux problèmes connus et résolus, veuillez consulter Problèmes résolus et Problèmes connus.
  Veuillez noter que l'ancien outil de mise à niveau n'est plus disponible à partir de Citrix.com.
- **Pour mettre à niveau XenMobile 10.3.x vers XenMobile 10.4**
  Utilisez la page **Gestion des versions** dans la console XenMobile. Consultez les instructions dans cet article pour plus de détails.
  Vous n'utilisez pas l'outil de mise à niveau pour les installations de XenMobile 10.3.x.
- **Pour mettre à niveau XenMobile 10 ou XenMobile 10.1 vers XenMobile 10.4**
  Pour commencer, utilisez la page **Gestion des versions** dans la console XenMobile pour la mise à niveau de XenMobile 10 ou XenMobile 10.1 vers XenMobile 10.3. Utilisez ensuite la page **Gestion des versions** dans la console XenMobile pour mettre à niveau XenMobile 10.3 vers XenMobile 10.4. Consultez les instructions dans cet article pour plus de détails. Vous n'utilisez pas l'outil de mise à niveau pour ces installations.

Récapitulatif des chemins de mise à niveau

Version du serveur XenMobile	Numéro de version	Mise à niveau vers	Numéro de version	Chemin de mise à niveau	Emplacement de mise à jour de la version
XenMobile Server 9 avec le Rolling Patch 9 installé	9.0.0_97106	Serveur XenMobile 10.4	10.4.0.116	Serveur XenMobile 9 vers serveur XenMobile 10.4	Téléchargez les composants requis pour le rolling patch. L'outil de mise à niveau pour XenMobile 10.4 est intégré au serveur XenMobile.
Serveur XenMobile 10 ou serveur XenMobile 10.1	10.1.0.63030	Serveur XenMobile 10.3	10.3.0.824	XenMobile 10 ou XenMobile 10.1 vers XenMobile 10.3	Télécharger
Serveur XenMobile 10.3.x	10.3.x	Serveur XenMobile 10.4	10.4.0.116	XenMobile 10.3.x vers XenMobile 10.4.	Télécharger

10.4.0.?

10.4.0.?

Pour mettre à niveau XenMobile 10 ou XenMobile 10.1 vers XenMobile 10.3 ou XenMobile 10.3 vers XenMobile 10.4

Configuration requise :

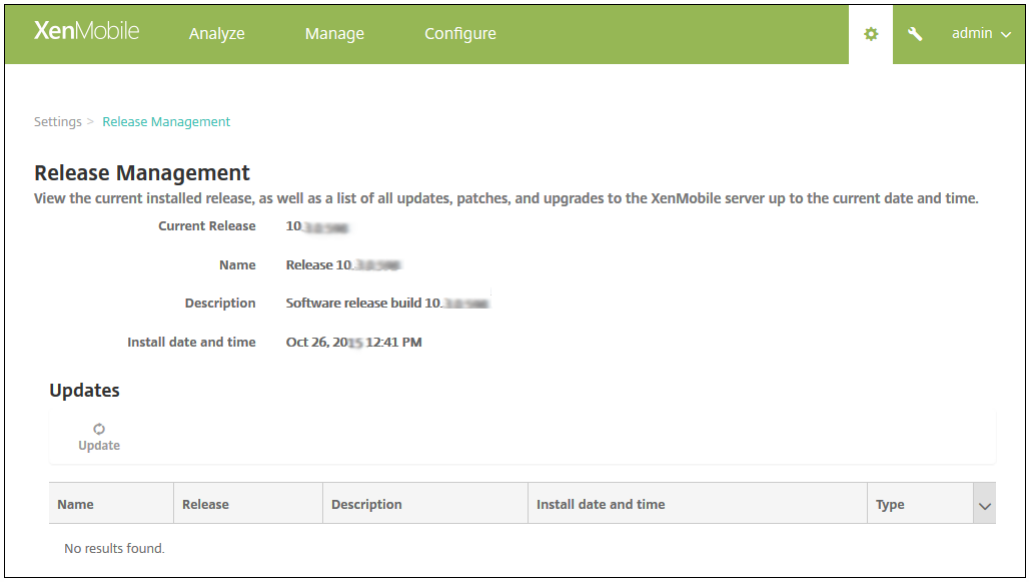
- Avant d'installer une mise à jour XenMobile, utilisez les fonctions de votre machine virtuelle (VM) pour prendre un instantané de votre système.
- Sauvegardez la base de données de configuration de votre système.
- Passez en revue la configuration requise pour la version que vous mettez à jour. Pour XenMobile 10.4, consultez la section Configuration requise.

Si vous disposez d'un déploiement en cluster, reportez-vous aux instructions à la fin de cet article.

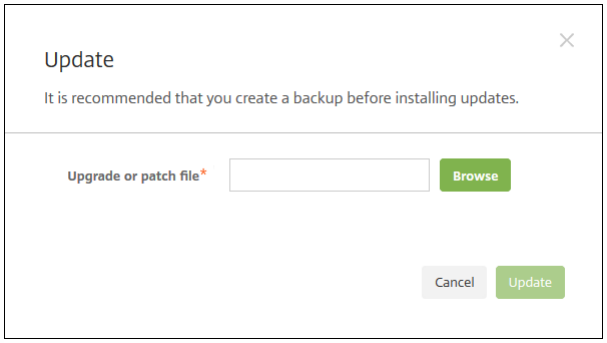
1. Ouvrez une session sur votre compte sur le site Web de Citrix et téléchargez le fichier XenMobile Upgrade (.bin) sur un emplacement approprié.

2. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

3. Cliquez sur **Gestion des versions**. La page **Gestion des versions** s'affiche.



4. Sous **Mises à jour**, cliquez sur **Mettre à jour**.La boîte de dialogue **Mettre à jour** s'affiche.



5. Sélectionnez le fichier de mise à niveau de XenMobile que vous avez téléchargé à partir de Citrix.com en cliquant sur **Parcourir** pour accéder à l'emplacement du fichier.

6. Cliquez sur **Mettre à jour**, et si vous y êtes invité, redémarrez XenMobile.

Si pour une raison quelconque la mise à jour ne peut pas être effectuée avec succès, un message d'erreur s'affiche indiquant le problème. L'état dans lequel votre système était avant la tentative de mise à jour est restauré.

Remarque : il est possible que XenMobile ne nécessite pas un redémarrage après l'installation de la mise à jour. Dans ce cas, un message indiquant que l'installation de la mise à jour a réussi s'affiche. Si, toutefois, XenMobile nécessite un redémarrage, vous devez utiliser la ligne de commande. Il est important d'effacer le cache de votre navigateur après le redémarrage du système.

4. Cliquez sur Parcourir, accédez à l'emplacement sur lequel vous avez enregistré le fichier de mise à niveau de XenMobile que vous avez téléchargé à partir de Citrix.com, puis sélectionnez le fichier.

5. Cliquez sur Mettre à jour, et si vous y êtes invité, redémarrez XenMobile.

Remarque : il est possible que XenMobile ne nécessite pas un redémarrage après l'installation de la mise à jour. Dans ce cas, un message indiquant que l'installation de la mise à jour a réussi s'affiche. Si, t

Important : si votre système est configuré en mode cluster, suivez les étapes suivantes pour mettre à jour chaque nœud :

1. Arrêtez tous les nœuds sauf un.
2. Mettez à jour ce nœud.
3. Vérifiez que le service est en cours d'exécution avant de mettre à jour le nœud suivant.

Si pour une raison quelconque la mise à jour ne peut pas être effectuée avec succès, un message d'erreur s'affiche indiquant le problème. L'état dans lequel votre système était avant la tentative de mi

4. Cliquez sur Parcourir, accédez à l'emplacement sur lequel vous avez enregistré le fichier de mise à niveau de XenMobile que vous avez téléchargé à partir de Citrix.com, puis sélectionnez le fichier.

5. Cliquez sur Mettre à jour, et si vous y êtes invité, redémarrez XenMobile.

Remarque : il est possible que XenMobile ne nécessite pas un redémarrage après l'installation de la mise à jour. Dans ce cas, un message indiquant que l'installation de la mise à jour a réussi s'affiche. Si, t

Important : si votre système est configuré en mode cluster, suivez les étapes suivantes pour mettre à jour chaque nœud :

1. Arrêtez tous les nœuds sauf un.
2. Mettez à jour ce nœud.
3. Vérifiez que le service est en cours d'exécution avant de mettre à jour le nœud suivant.

Si pour une raison quelconque la mise à jour ne peut pas être effectuée avec succès, un message d'erreur s'affiche indiquant le problème. L'état dans lequel votre système était avant la tentative de mi

Pour mettre à niveau des déploiements XenMobile en cluster

Si votre système est configuré en mode cluster, suivez les étapes suivantes pour mettre à jour chaque nœud d'une version de XenMobile 10 :

1. Chargez le fichier .bin sur tous les nœuds depuis **Paramètres > Gestion des versions**.

2. Arrêtez tous les nœuds autres que celui que vous allez mettre à niveau.Pour arrêter un nœud, utilisez **System Menu** dans l'interface de ligne de commande.

3.Mettez à niveau le nœud qui est toujours en cours d'exécution.

3. Vérifiez que le service est en cours d'exécution sur le nœud mis à niveau.

4. Affichez les autres nœuds les uns après les autres.

Si XenMobile ne peut pas effectuer la mise à jour avec succès, un message d'erreur expliquant le problème s'affiche. XenMobile rétablit alors l'état du système à l'état qui était le sien avant la tentative de mise à jour.

Pré-requis pour l'outil de mise à niveau

Feb 23, 2017

Pour mettre à niveau XenMobile 9.0 vers XenMobile 10.4, vous devez utiliser l'outil de mise à niveau intégré à XenMobile 10.4.

L'outil de mise à niveau prend en charge les appareils suivants :

- Appareils iOS et Android inscrits dans tous les modes de serveur XenMobile (ENT, MAM, MDM)
- Téléphones et tablettes Windows inscrits en mode MDM
- Téléphones Windows inscrits dans en mode Enterprise
- Appareils Windows CE en mode MDM

Si la console Multi-Tenant Console (MTC) est activée sur XenMobile 9.0, vous pouvez migrer MTC vers un déploiement XenMobile 10.4 autonome. XenMobile 10 ne prend pas en charge la MTC, c'est la raison pour laquelle vous devez gérer ces instances mises à niveau individuellement. Une fois que vous avez rempli les conditions préalables définies dans cet article, consultez la section Mise à niveau du serveur locataire de la console MTC vers XenMobile 10.1.

XenMobile 10.4 prend en charge les versions de NetScaler Gateway 11.1.x, 11.0.x et 10.5.x.

L'outil de mise à niveau intégré à XenMobile 10.4 prend également en charge la version 10.1.x. de NetScaler Gateway Citrix ne prend pas en charge NetScaler Gateway 10.1 avec XenMobile 10.4. Toutefois, vous pouvez effectuer la mise à niveau d'un déploiement NetScaler Gateway 10.1 à l'aide de l'outil de mise à niveau intégré à XenMobile 10.4. Ensuite, Citrix vous recommande de mettre à niveau NetScaler Gateway vers la dernière version prise en charge.

> ## Important
>
> Le processus de mise à niveau est complexe. Avant de démarrer une mise à niveau, veillez à consulter la liste des problèmes connus, puis planifiez votre mise à niveau et préparez toutes les conditions requises, comme décrit dans cet article. En outre, ce blog comprend des check-lists des conditions préalables qui peuvent vous aider à planifier votre mise à niveau.
>
> Après avoir exécuté l'outil de mise à niveau, vous devez effectuer toutes les configurations requises.
>
> Si les conditions préalables ne sont pas toutes remplies, la mise à niveau peut échouer. Vous devez ensuite configurer une nouvelle instance de XenMobile 10.4 dans la console de ligne de commande et démarrer l'outil de mise à niveau.

Planifier votre mise à niveau

Citrix vous conseille de suivre les étapes suivantes pour procéder à la mise à niveau :

1. Effectuez un test dans un environnement de simulation, en suivant toutes les étapes pré-requises et de l'outil de mise à niveau. Citrix vous recommande de procéder à une mise à niveau test pour vous familiariser avec la manière dont le processus fonctionne et avec les tâches que vous devrez effectuer une fois que la mise à niveau de production est terminée. Une mise à niveau test évalue la mise à niveau de vos données de configuration, et non pas les données utilisateur.

Dans NetScaler 11.1 (ou version minimale NetScaler 10.5), Citrix vous recommande d'utiliser l'assistant NetScaler pour XenMobile pour configurer un nouveau NetScaler avec NetScaler Gateway et des serveurs virtuels d'équilibrage de charge NetScaler.

2. Vérifiez que la mise à niveau test a correctement mis à niveau vos données de configuration, telles que LDAP, stratégies et applications. Vérifiez les machines test.

3. Effectuez une mise à niveau de production dans votre environnement de production et passez en mode opérationnel. Planifiez les temps d'arrêt lors de l'exécution de la mise à niveau.

À propos des tests et des mises à niveau de production

Avec l'outil de mise à niveau XenMobile 10.4, vous testez d'abord la mise à niveau puis vous effectuez la mise à niveau de production.

Lorsque vous choisissez d'effectuer un test :
L'outil de mise à niveau effectue une mise à niveau test à l'aide de données de configuration de production pour comparer XenMobile 9.0 et XenMobile 10.4 sans affecter votre environnement de production. Le test de mise à niveau évalue uniquement les données de configuration ; il ne teste pas les données des appareils (dans le cas de déploiements XenMobile Enterprise Edition) ou les données de l'utilisateur.

Les résultats d'une mise à niveau test sont uniquement à des fins de test. Vous ne pouvez pas mettre à niveau un déploiement test. Vous devez recommencer depuis le début pour la mise à niveau de l'environnement de production. Une mise à niveau test fonctionne avec toute édition de XenMobile 9.0.

Lorsque vous choisissez d'effectuer la mise à niveau :
L'outil de mise à niveau commence par copier toutes les données de configuration, d'appareil et d'utilisateur depuis XenMobile 9.0 vers une nouvelle instance de XenMobile 10.4 avec le même nom de domaine complet (FQDN). XenMobile 9.0 reste inchangé jusqu'à ce que vous déplaciez le serveur XenMobile 10,4 dans l'environnement de production.

Lorsque vous ouvrez une session sur la console XenMobile 10.4 après la mise à niveau, vous pouvez voir toutes les données utilisateur et de l'appareil que la mise à niveau a déplacées depuis XenMobile 9.0.

Ce que l'outil de mise à niveau ne fait pas

Lorsque vous utilisez l'outil de mise à niveau, les informations suivantes ne sont pas mises à niveau vers XenMobile 10.4 :

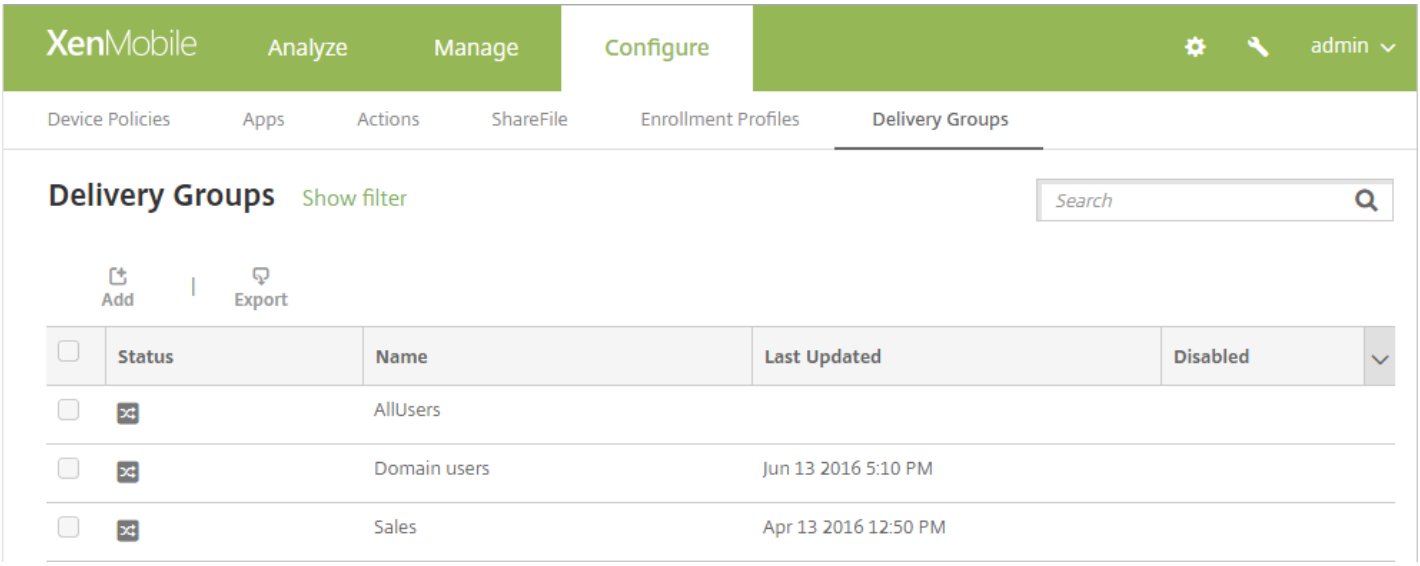
- Les informations de licence.
- Les rapports de données.
- Les stratégies de groupes de serveurs et les déploiements associés (non pris en charge dans XenMobile 10.4).
- Le groupe MSP (Managed Service Provider).
- Les stratégies et les paquetages associés à Windows 8.0.
- Les paquetages de déploiement non utilisés ; par exemple, lorsqu'aucun utilisateur ou groupe n'est assigné à un paquetage de déploiement.
- Toutes les autres données de configuration ou d'utilisateur répertoriées dans le fichier journal de mise à niveau.
- CXM Web (remplacé par Citrix Secure Web).
- Les stratégies DLP (remplacées par Citrix ShareFile).
- Les attributs Active Directory personnalisés.
- Si vous avez configuré plusieurs stratégies de marque, la stratégie de marque n'est pas mise à niveau. XenMobile 10.4 prend en charge une seule stratégie de marque ; vous devez laisser une stratégie de marque dans XenMobile 9.0 pour que votre mise à niveau vers XenMobile 10.4 se réalise avec succès.
- Tous les paramètres du fichier auth.jsp dans XenMobile 9.0 qui sont utilisés pour restreindre l'accès à la console. Les restrictions d'accès à la console dans XenMobile 10.4 sont des paramètres de pare-feu que vous pouvez configurer dans

l'interface de ligne de commande.

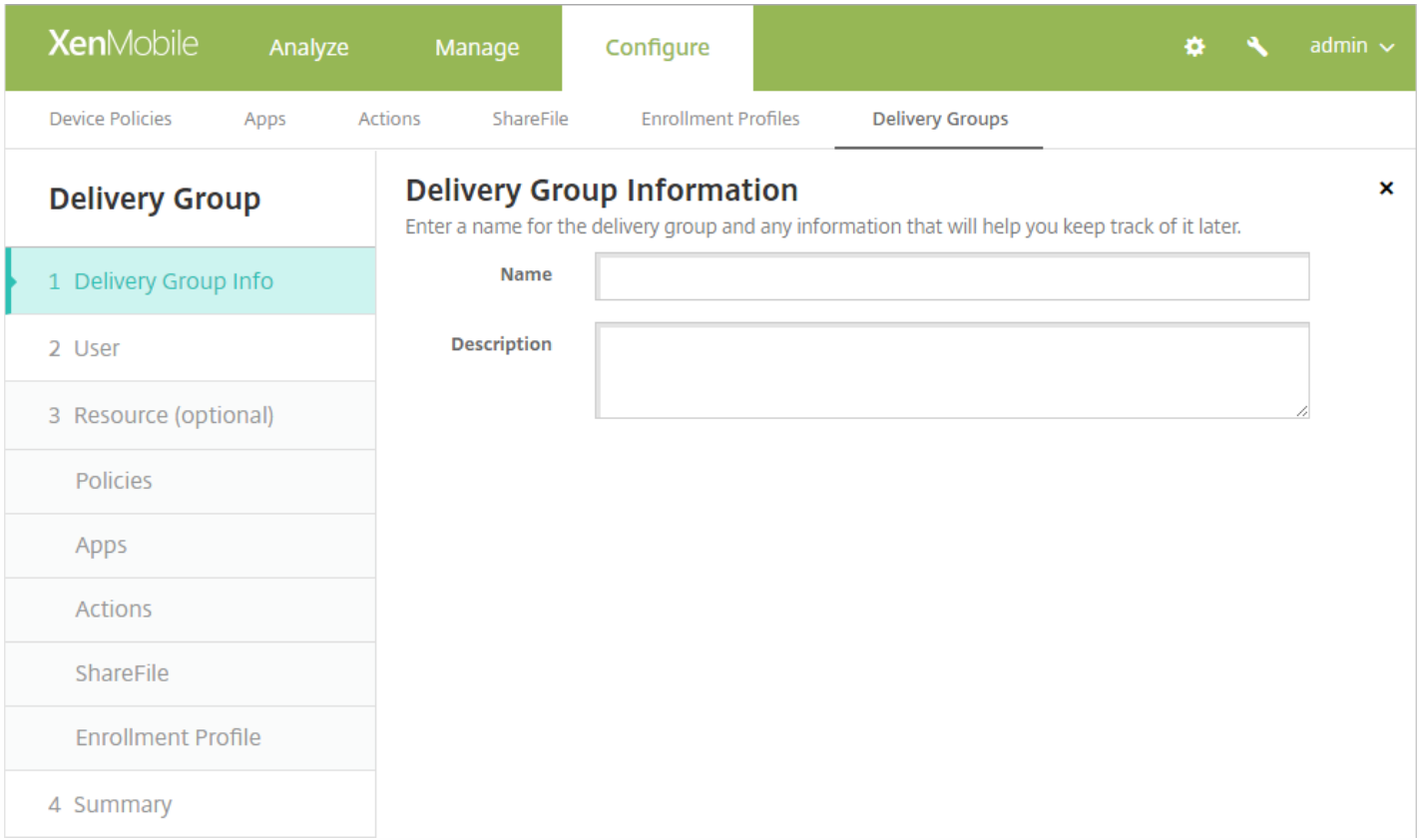
- Les configurations du serveur Syslog.
- Les connecteurs de remplissage de formulaire configurés sur XenMobile 9.0 (non pris en charge dans XenMobile 10.4).

Changements dans XenMobile

- L'outil de mise à niveau ne met pas à niveau les utilisateurs Active Directory qui sont assignés à des groupes locaux. Vous pouvez ensuite attribuer des utilisateurs Active Directory à des groupes locaux.
- XenMobile 10 ne prend pas en charge les groupes imbriqués locaux. Une mise à niveau à partir de XenMobile 9 écrase la hiérarchie de groupes locaux.
- Les paquetages de déploiement dans Device Manager sont appelés groupes de mise à disposition dans XenMobile, comme le montre la figure suivante. Pour de plus amples informations, consultez la section Déployer des ressources.

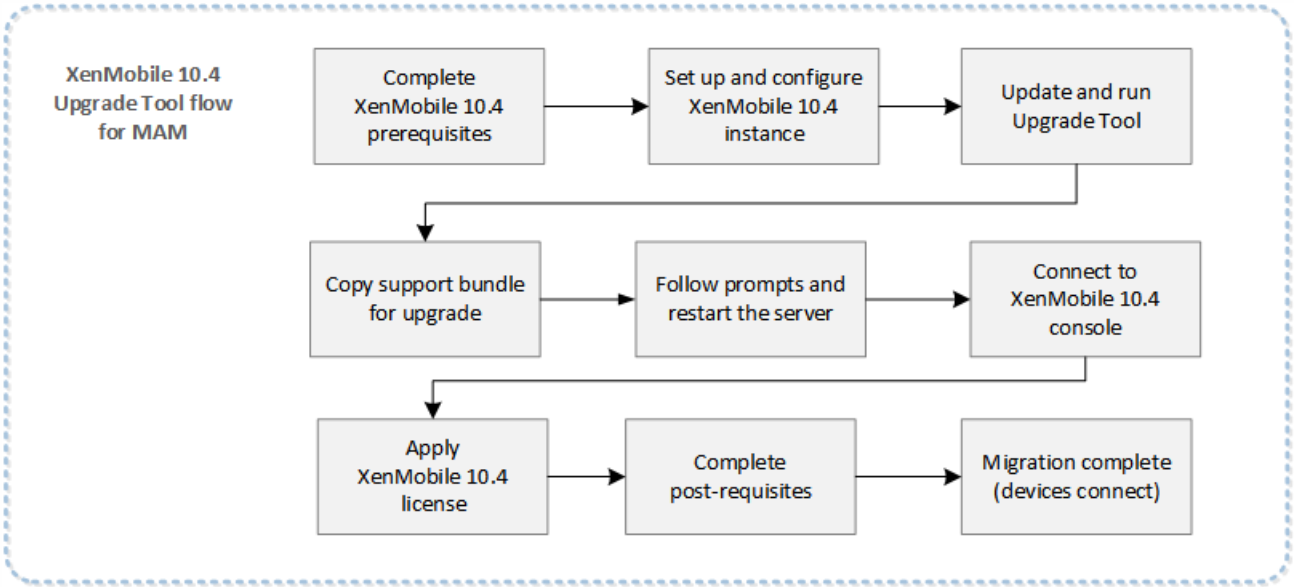


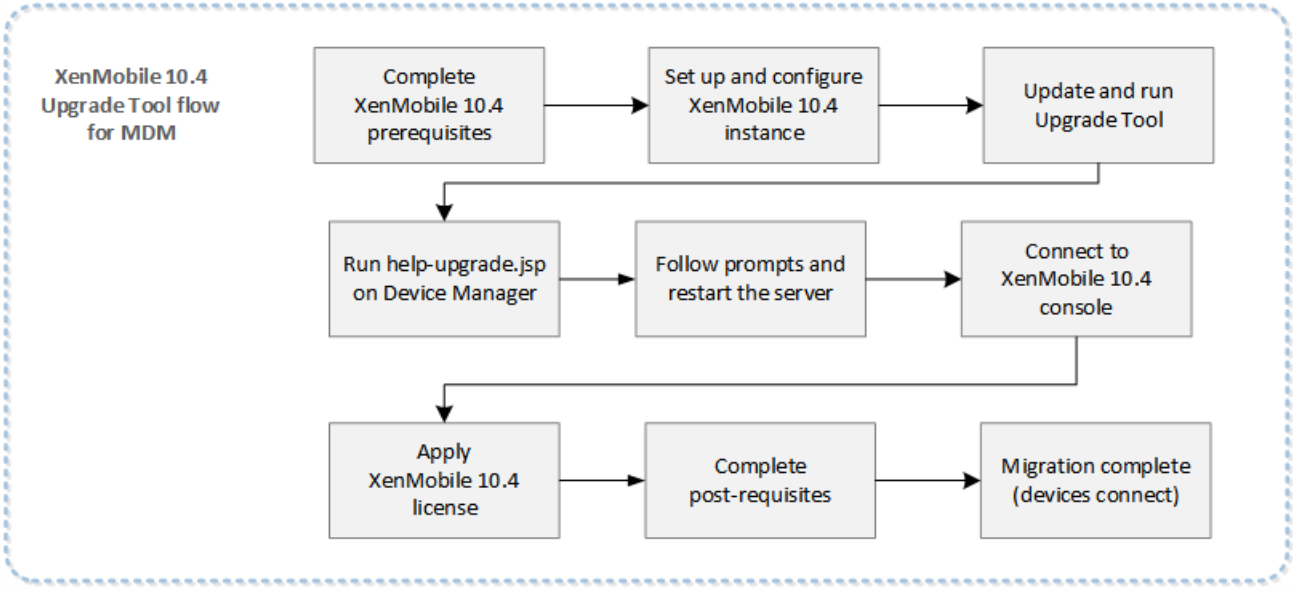
Dans le groupe de mise à disposition, vous pouvez voir les stratégies, les actions et les applications requises par le groupe d'utilisateurs qui requiert des ressources.

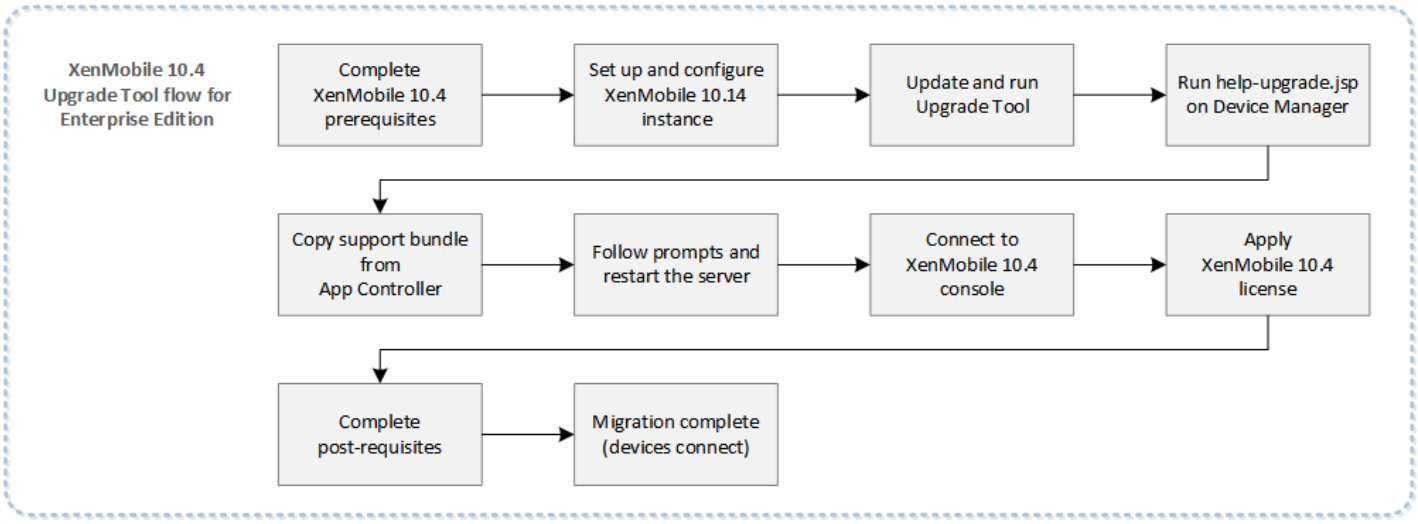


Workflow de mise à niveau de XenMobile 9.0 vers XenMobile 10.4

Les figures suivantes illustrent les étapes de base nécessaires pour effectuer la mise à niveau de XenMobile 9.0 vers XenMobile 10.4.







Conditions préalables pour les téléphones Windows en mode Enterprise

Citrix recommande les étapes suivantes pour mettre à niveau un environnement XenMobile 9.0 Enterprise, avec des téléphones Windows inscrits en mode Enterprise à l'aide de Worx Home 9.x, vers XenMobile 10.4.

1. Mettez à niveau Worx Home sur Device Manager vers la version 10.2, puis déployez Worx Home 10.2.

2. Désinstallez manuellement Worx Home 9.x des appareils des utilisateurs.

3. Demandez aux utilisateurs d'accéder au Download Hub sur leur téléphone pour installer Worx Home 10.2, que vous avez déployé à partir de Device Manager.

4. Une fois que vous avez rempli les conditions préalables décrites dans cet article, effectuez la mise à niveau vers XenMobile 10.4 comme décrit dans la section Activer et exécuter l'outil de mise à niveau de XenMobile.

5. Modifiez NetScaler de manière à autoriser les appareils à se connecter, comme décrit dans la section Post-requis de l'outil de mise à niveau.

Correctif App Controller requis

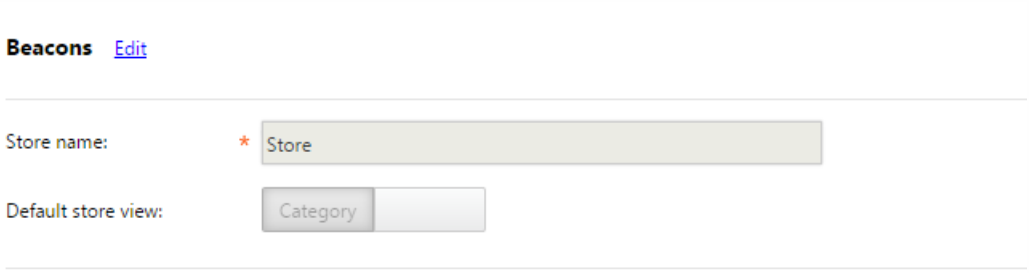
Téléchargez le XenMobile 9.0 App Controller Rolling Patch 9 depuis https://support.citrix.com/article/CTX218552.

Dans la console de gestion App Controller, accédez à **Paramètres > Gestion des versions**. Cliquez sur **Mettre à jour**, puis sélectionnez le fichier correctif que vous avez téléchargé. Cliquez sur **Charger** et redémarrez App Controller.

Noms de magasin personnalisés dans XenMobile 9

Avant d'effectuer la mise à niveau de XenMobile 9 vers XenMobile 10.4, vous devez rétablir le nom par défaut d'un magasin personnalisé de façon à ce que les appareils Windows inscrits puissent continuer à fonctionner après la mise à niveau. Consultez l'article http://support.citrix.com/article/CTX214553 pour de plus amples informations.

Dans une mise à niveau en mode MAM ou Enterprise, si le nom par défaut du magasin Store a été changé sur App Controller, restaurez la valeur par défaut de **Store** avant de générer un pack d'assistance pour la mise à niveau.



Configuration système requise et exigences en matière de port

Pour connaître les versions requises des différents composants tels que le serveur de licences Citrix, consultez la section Configuration système requise et ses sous-articles.

- **NetScaler** : avant de mettre à niveau NetScaler, enregistrez une copie du fichier de configuration Netscaler (ns.conf). Les versions actuelles de Netscaler incluent un utilitaire de déploiement simple et rapide, l'assistant NetScaler pour XenMobile, qui vous guide à travers les étapes requises pour intégrer NetScaler et XenMobile. Pour de plus amples informations, consultez les sections Configuration des paramètres de votre environnement XenMobile et FAQ : Intégration de XenMobile 10 et NetScaler 10.5.
- **Ports de pare-feu** : ouvrez les mêmes ports de pare-feu pour la nouvelle adresse IP du serveur XenMobile 10.4 que ceux ouverts pour l'adresse IP du serveur XenMobile 9.0. Pour les exigences en matière de port pour XenMobile 10.4, consultez la section Configuration requise pour les ports.
- **Serveur LDAP** : assurez-vous que le nouveau serveur XenMobile 10.4 se connecte à un ou plusieurs serveurs LDAP. Vous devez disposer d'une route active vers les serveurs LDAP après la mise à niveau, lorsque vous redémarrez le serveur.

Migration de la base de données

Le tableau suivant dresse la liste des options de migration de base de données possibles. Pour la configuration système requise, consultez la section Configuration requise pour la base de données XenMobile 10.4.

De XenMobile 9.0	à XenMobile 10.4
Édition Enterprise	

App Controller	MDM	
PostgreSQL local	PostgreSQL local	PostgreSQL local
PostgreSQL local	MS SQL	MS SQL
PostgreSQL local	Remote PostgreSQL	Remote PostgreSQL

App Edition	
PostgreSQL local	PostgreSQL local
PostgreSQL local	Remote PostgreSQL
PostgreSQL local	MS SQL

MDM Edition	
PostgreSQL local	PostgreSQL local
MS SQL	MS SQL
Remote PostgreSQL	Remote PostgreSQL

Durant le processus de migration de base de données, XenMobile a besoin d'être autorisé à accéder à la solution base de données implémentée dans XenMobile 9.0 Device Manager. Les ports suivants doivent être ouverts :

- Pour le serveur Microsoft SQL, le port par défaut est 1433.
- Pour PostgreSQL, le port par défaut est 5432.

Pour autoriser les connexions à distance à PostgreSQL, vous devez effectuer les étapes suivantes :

1. Ouvrez le fichier pg_hba.conf et recherchez la ligne suivante :

    host all all 127.0.0.1/32 md5

2. Pour autoriser toutes les adresses IP, modifiez la ligne comme suit :

    host all all 0.0.0.0/0 md5

Vous pouvez également ajouter une autre entrée host afin d'autoriser les connexions à l'adresse IP du serveur

XenMobile :

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

3. Enregistrez le fichier.

4. Arrêtez et démarrez le service.

5. Ouvrez le fichier postgresql.conf et recherchez la ligne suivante :

#listen_addresses = 'localhost'

6. Modifiez la ligne comme suit :

listen_addresses = '*'

7. Arrêtez et redémarrez le service PostgreSQL pour appliquer les modifications.

Si un port personnalisé a été assigné à la solution de base de données, vous devez vous assurer que le port est autorisé et ouvert dans le pare-feu protégeant XenMobile 9.0 Device Manager. Cela permet à XenMobile 10.4 de se connecter à la base de données et de migrer les informations requises.

Noms de paquetages de déploiement avec caractères spéciaux

Les noms de paquetages de déploiement dans XenMobile 9.0 qui contiennent des caractères spéciaux (!, $, (), #, % , +, *, ~, ?, |, {} et []) sont mis à niveau, mais vous ne pouvez pas modifier les groupes de mise à disposition dans XenMobile 10.4 après la mise à niveau. En outre, les utilisateurs locaux et les groupes locaux créés dans XenMobile 9.0 qui contiennent un crochet ouvrant ([) causent des problèmes dans XenMobile 10. 4 lors de la création des invitations d'inscription. Avant une mise à niveau, supprimez tous les caractères spéciaux des noms de paquetages de déploiement et les crochets ouverts des noms d'utilisateurs locaux et de groupes locaux.

Certificat SSL externe

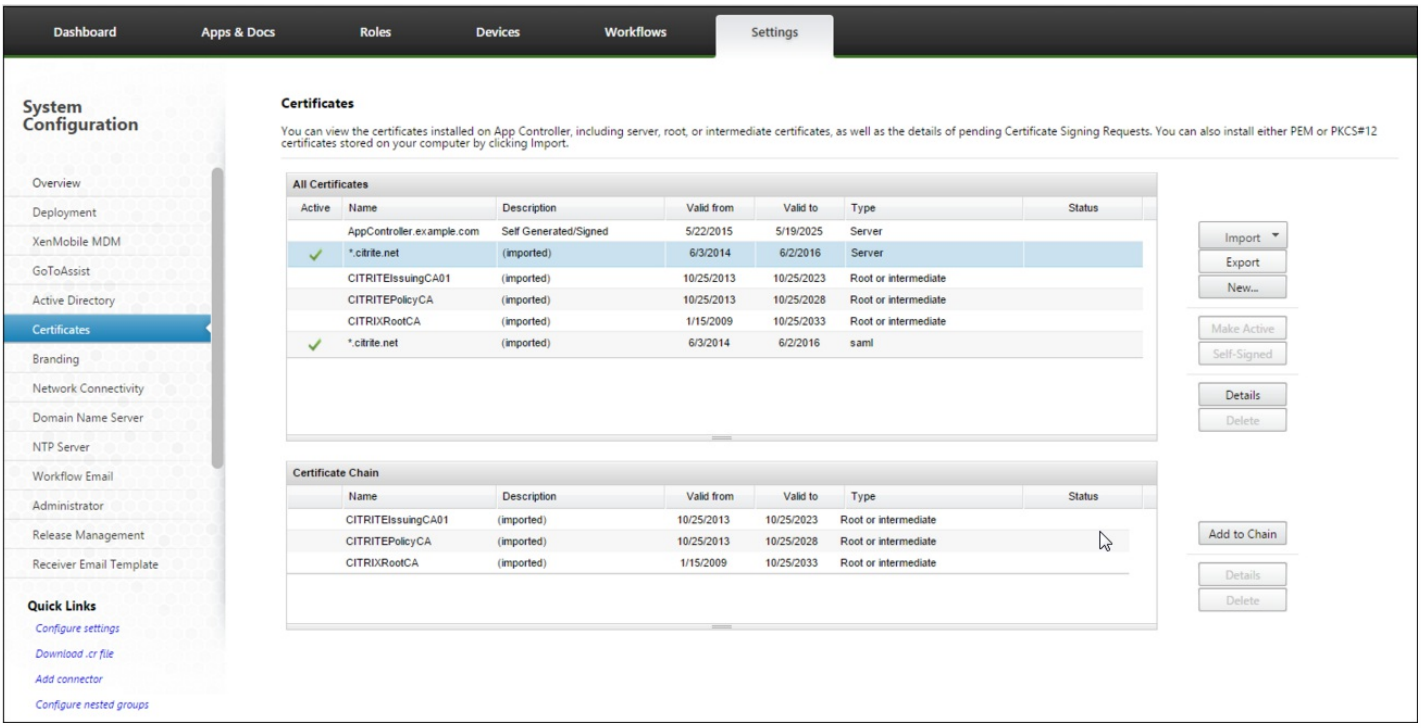
Les certificats SSL externes doivent respecter les critères indiqués dans l'article de support Citrix Comment configurer un certificat SSL externe. Veillez à consulter votre pki.xml avant de démarrer la mise à niveau pour vous assurer que le certificat SSL remplit ces conditions.

Exporter le certificat de serveur XenMobile 9.0

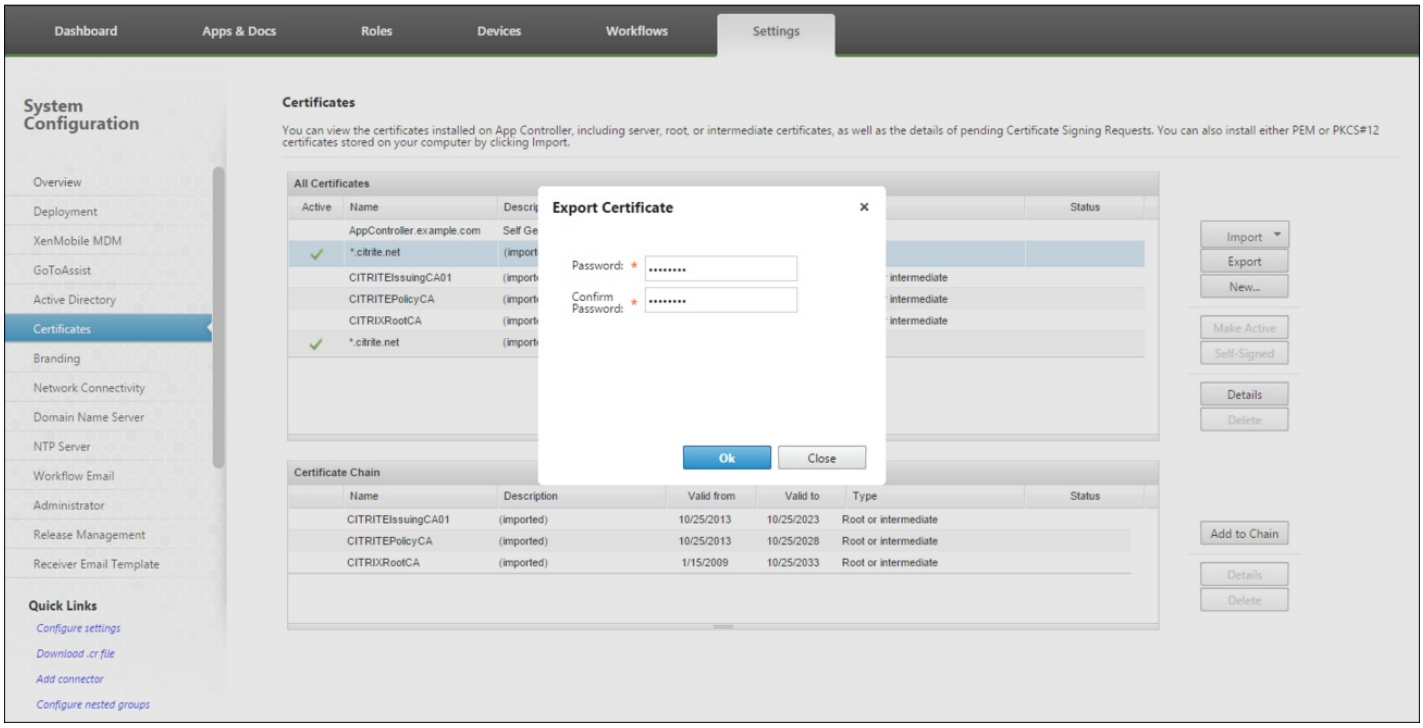
Si vous effectuez la mise à niveau d'un déploiement XenMobile 9.0 Enterprise Edition, vous devez exporter le certificat de serveur App Controller. Plus tard, lors des étapes de configuration requises après la mise à niveau, vous devrez importer le certificat de serveur dans NetScaler Gateway. Suivez ces étapes pour exporter le certificat de serveur :

1. Ouvrez une session sur XenMobile 9.0 App Controller et cliquez sur **Certificats**.

2. Dans la liste des certificats, cliquez sur le certificat de serveur que vous souhaitez exporter, puis cliquez sur **Exporter**.



3. Dans la boîte de dialogue **Exporter certificat**, entrez le mot de passe de votre certificat dans les deux champs et cliquez sur **OK**.



Serveur pour le chargement du pack de support crypté

Préparez un serveur où vous pouvez télécharger le pack de support crypté à partir de l'interface de ligne de commande XenMobile à l'aide du protocole FTP (File Transfer Protocol) ou du protocole SCP (Secure Copy Protocol).

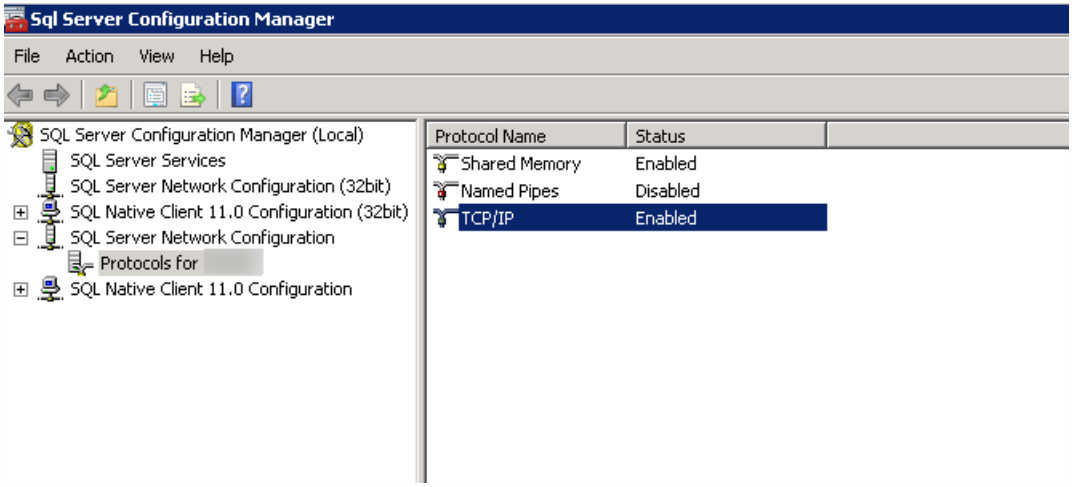
Activer et exécuter l'outil de mise à niveau de XenMobile

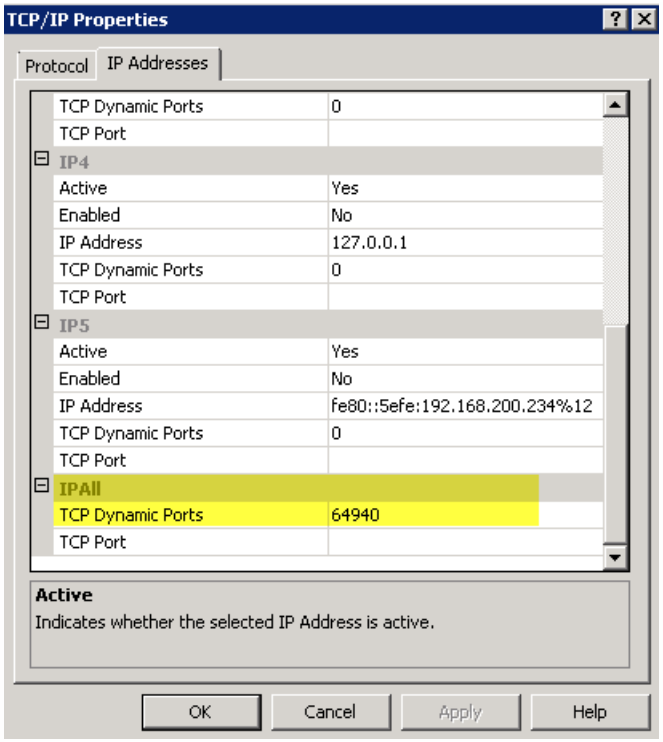
Feb 23, 2017

Si votre environnement XenMobile 9 répond aux conditions préalables suivantes, suivez les étapes de cette section avant de procéder à la mise à niveau.

- XenMobile 9 MDM Edition ou Enterprise Edition doté d'une base de données SQL Server externe.
- La base de données SQL Server s'exécute sur une instance nommée autre que celle par défaut.
- L'instance nommée SQL Server écoute sur un port TCP statique ou dynamique. Vous pouvez confirmer ces conditions préalables en examinant les adresses IP du protocole TCP/IP de l'instance nommée comme illustré dans les figures suivantes.

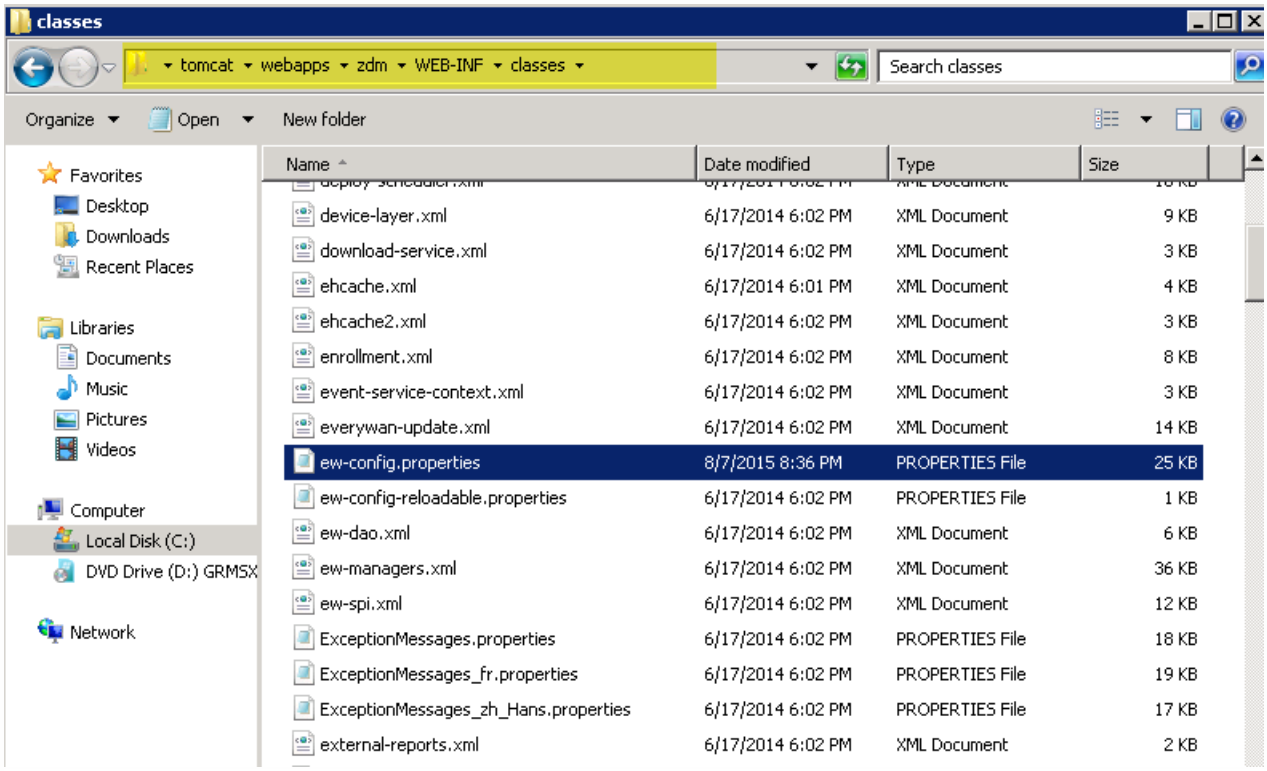
> ## Remarque
>
> Citrix recommande de toujours exécuter l'instance de base de données SQL Server sur un port statique car le serveur XenMobile nécessite un accès continu à la base de données. Cette connexion traverse généralement via un pare-feu. Par conséquent, vous devez ouvrir le port approprié dans le pare-feu ; c'est la raison pour laquelle l'instance de la base de données doit être exécutée sur un port statique.





Étapes préalables à la mise à niveau

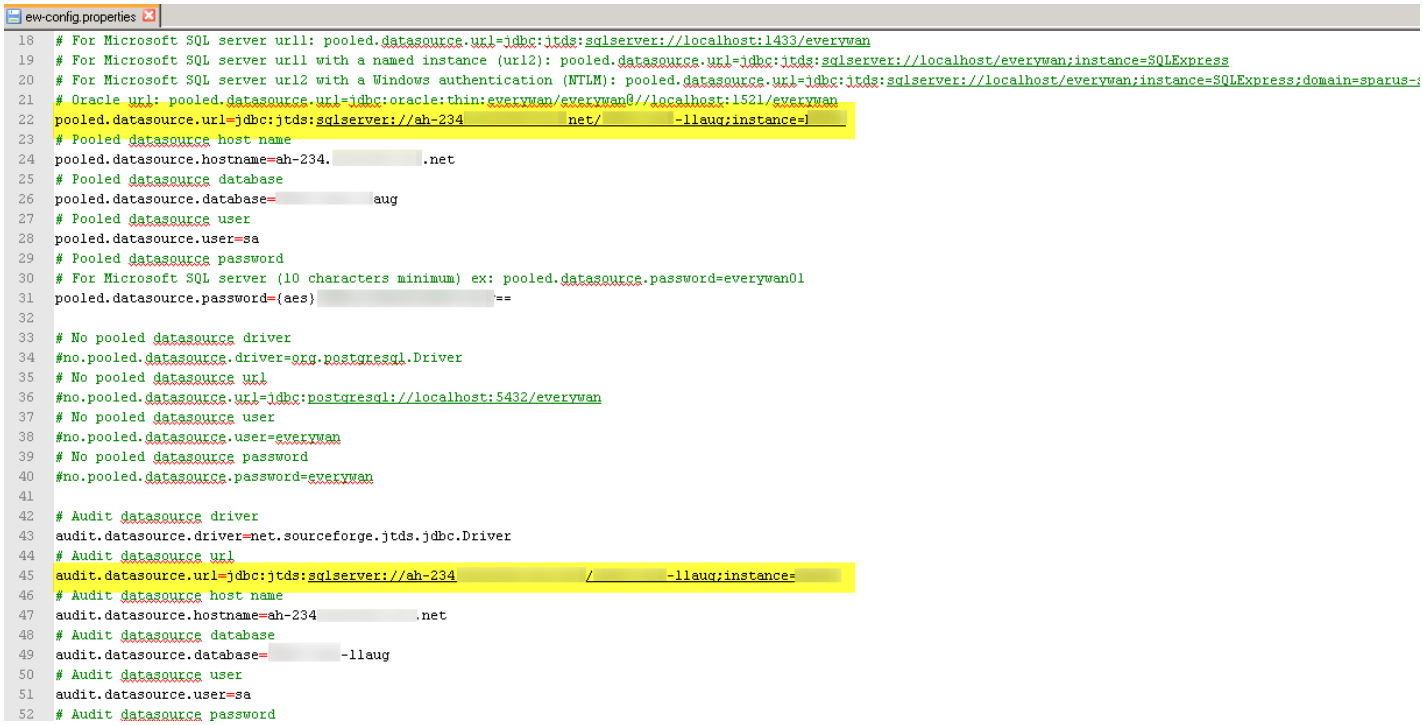
1. Accédez au répertoire d'installation de Device Manager et ouvrez le fichier ew-config.properties. Ce fichier se trouve dans tomcat\webapps\zdm\WEB-INF\classes.



2. Dans le fichier ew-config.properties, recherchez les URL suivantes dans la section DATASOURCE Configuration :

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

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



3. Supprimez le nom d'instance dans les URL précédentes et ajoutez le port et le nom de domaine complet de SQL Server. Dans ce cas, 64940 est le port requis.

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

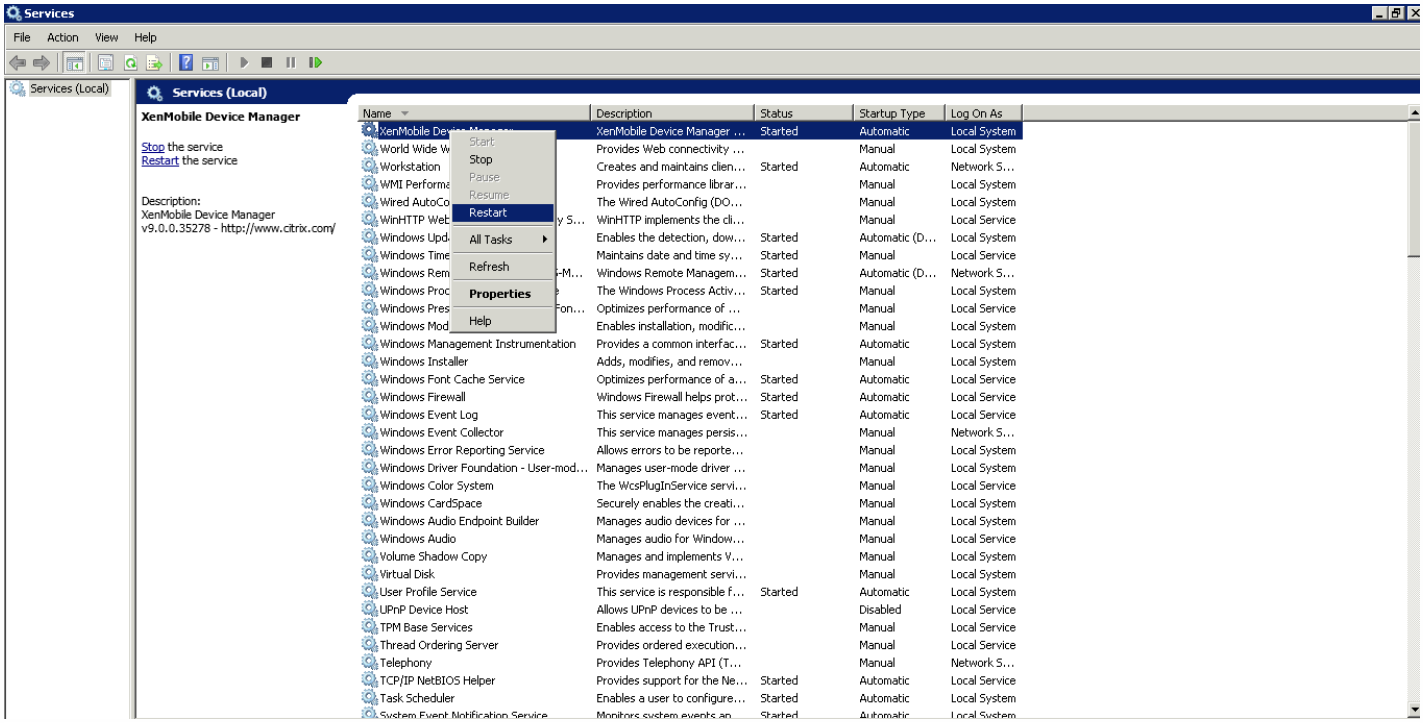
audit.datasource.url=jdbc:jtds:sqlserver:// :64940/

> ## Remarque
>
> Citrix vous recommande d'effectuer une sauvegarde, de copier ou de prendre note des modifications que vous apportez au fichier ew-config.properties. Ces informations s'avèrent utiles en cas d'échec de la mise à niveau.

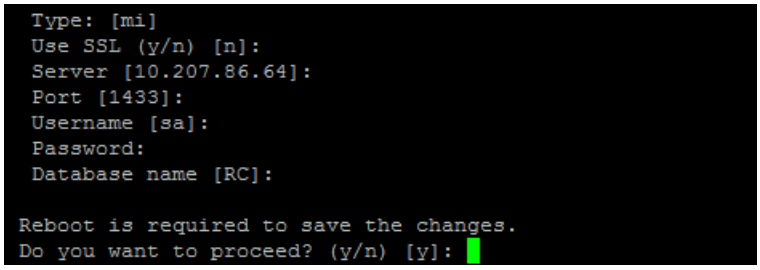
ew-config.properties

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

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

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

4. Redémarrez le service Device Manager. Actualisez les connexions aux appareils après le redémarrage de l'instance de Device Manager.



5. Déterminez si le nouveau serveur XenMobile 10.x a également besoin de fonctionner avec une instance SQL nommée. Si c'est le cas, identifiez le port sur lequel l'instance nommée est exécutée. Si le port est un port dynamique, Citrix vous recommande de convertir le port en port statique. Ultérieurement, lorsque vous atteignez la partie suivante de l'installation de la base de données lors de la mise à niveau, configurez le port statique sur le nouveau serveur XenMobile.



Vous pouvez maintenant procéder à la mise à niveau.

Pour mettre à niveau des déploiements XenMobile en cluster

Si votre système est configuré en mode cluster :

1. Arrêtez tous les nœuds autres que celui que vous allez mettre à niveau. Pour arrêter un nœud, utilisez **Settings** dans l'interface de ligne de commande.

2. Mettez à niveau le nœud qui est toujours en cours d'exécution, comme décrit dans la section suivante, « Pour activer et exécuter l'outil de mise à niveau ».

3. Une fois que vous avez vérifié que la première mise à niveau s'est déroulée comme prévu, rétablissez tous les autres nœuds, un à la fois. Procédez comme suit :

    a. Redémarrez le nœud.

    b. Ne mettez pas le nœud à niveau si vous y êtes invité.

    c. Associez le nœud à la base de données du cluster.

    XenMobile effectuera la mise à niveau automatique d'un nœud une fois que vous l'avez associé au cluster.

4. Effectuez toutes les tâches requises après la mise à niveau sur chaque nœud après leur association au cluster.

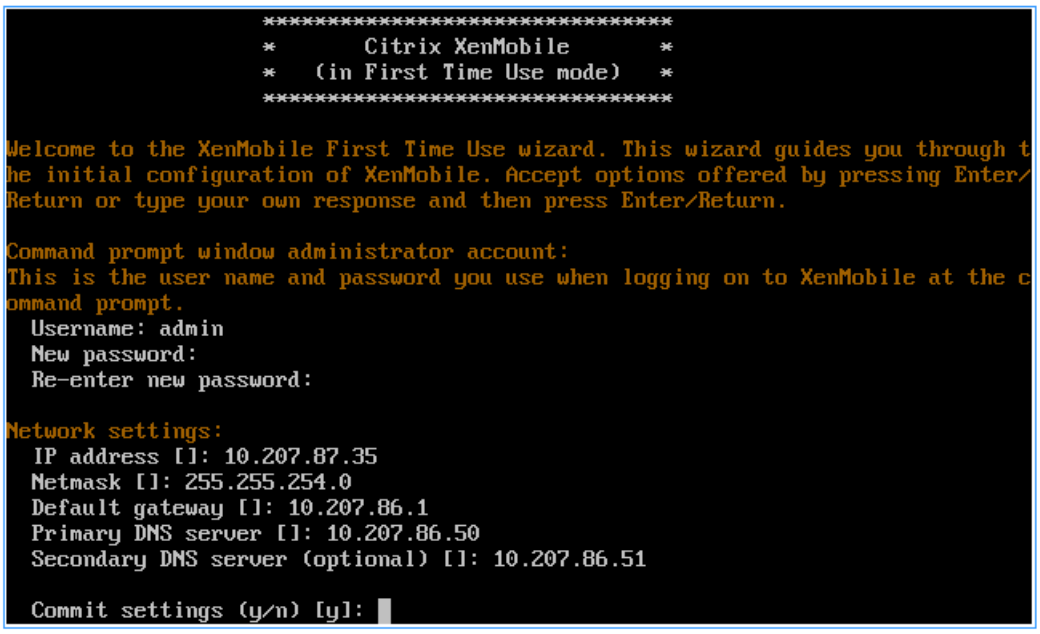
Pour activer et exécuter l'outil de mise à niveau

Activez l'outil de mise à niveau à l'aide de l'interface de ligne de commande lors de l'installation initiale de XenMobile 10.4.

> **Important**
>
> Si vous voulez prendre un instantané de votre système, faites-le après la configuration initiale de XenMobile 10.4 et avant d'accéder à l'outil de mise à niveau.

1. Dans l'interface de ligne de commande, tapez votre nom d'utilisateur et votre mot de passe d'administrateur, puis entrez vos paramètres réseau.

2. Tapez **y** pour valider les paramètres.

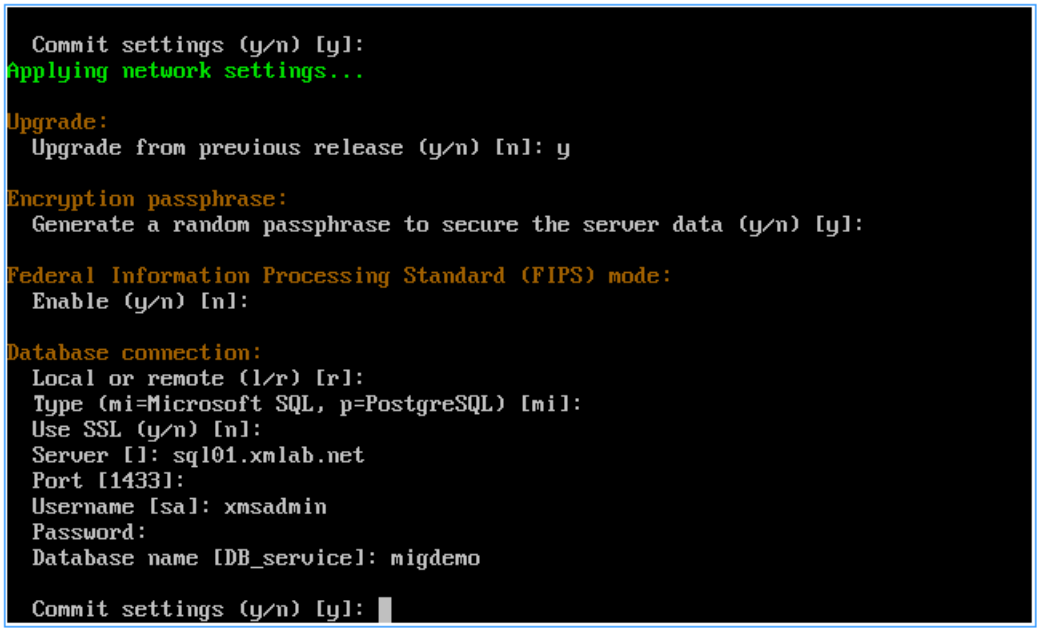


3. Tapez **y** pour mettre à niveau.

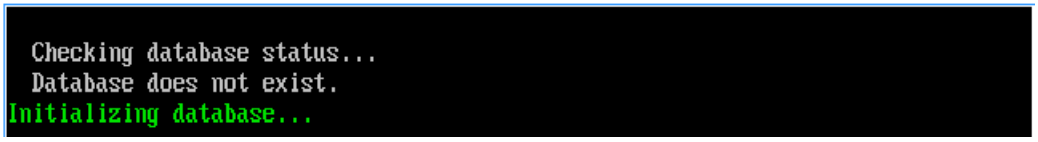
> ## Remarque
>
> Si vous ne tapez pas y ici, vous devez configurer une nouvelle instance de XenMobile 10.4 dans la console de ligne de commande et démarrer l'outil de mise à niveau.

4. Choisissez s'il convient de générer une phrase secrète aléatoire et, éventuellement, d'activer FIPS. Entrez vos informations de connexion à la base de données.

5. Tapez **y** pour valider les paramètres.



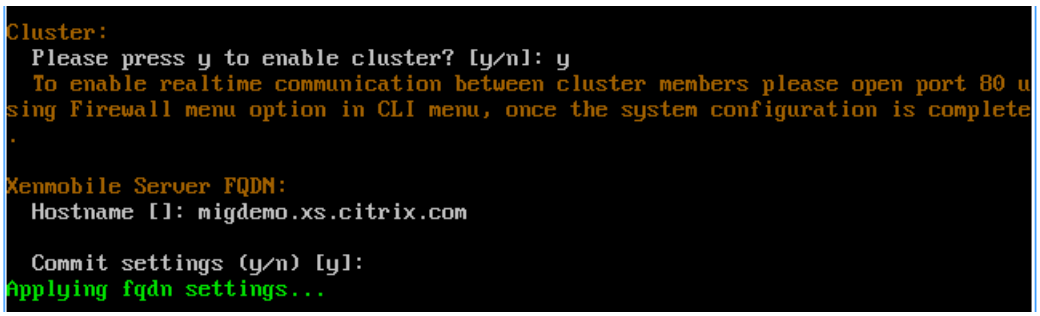
XenMobile initialise la base de données.



6. Sélectionnez s'il convient d'activer les serveurs en cluster. Entrez le nom de domaine complet de XenMobile. Tenez compte de ce qui suit :

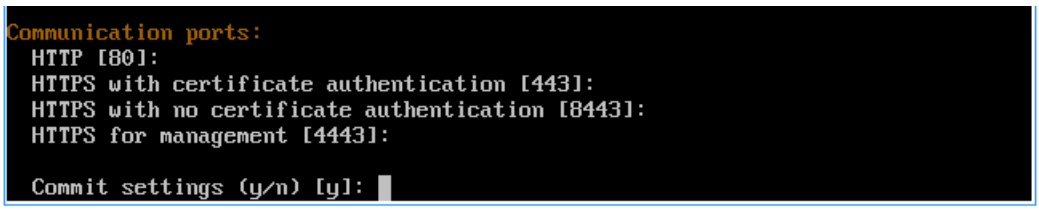
- Pour les déploiements de XenMobile Enterprise Edition, le nom de domaine complet est le même que pour XenMobile 9.0 MDM.
- Pour les déploiements MAM, le nom de domaine complet est le même que pour XenMobile 9.0 App Controller.
- Pour les déploiements MDM, le nom de domaine complet est le même que pour XenMobile 9.0 Device Manager.

> **Important**
>
> Les noms de domaine complets pour les environnements 9.0 et 10.4 doivent correspondre.



7. Tapez **y** pour valider les paramètres.

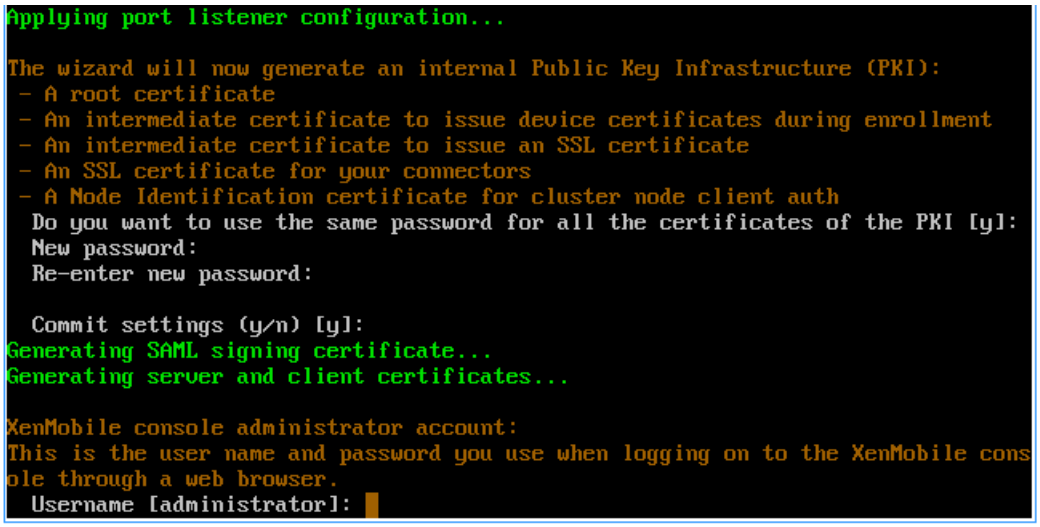
8. Définissez les ports de communication.



9. Tapez **y** pour valider les paramètres.

10. Indiquez si vous souhaitez utiliser le même mot de passe pour tous les certificats et tapez le mot de passe à utiliser pour les certificats.

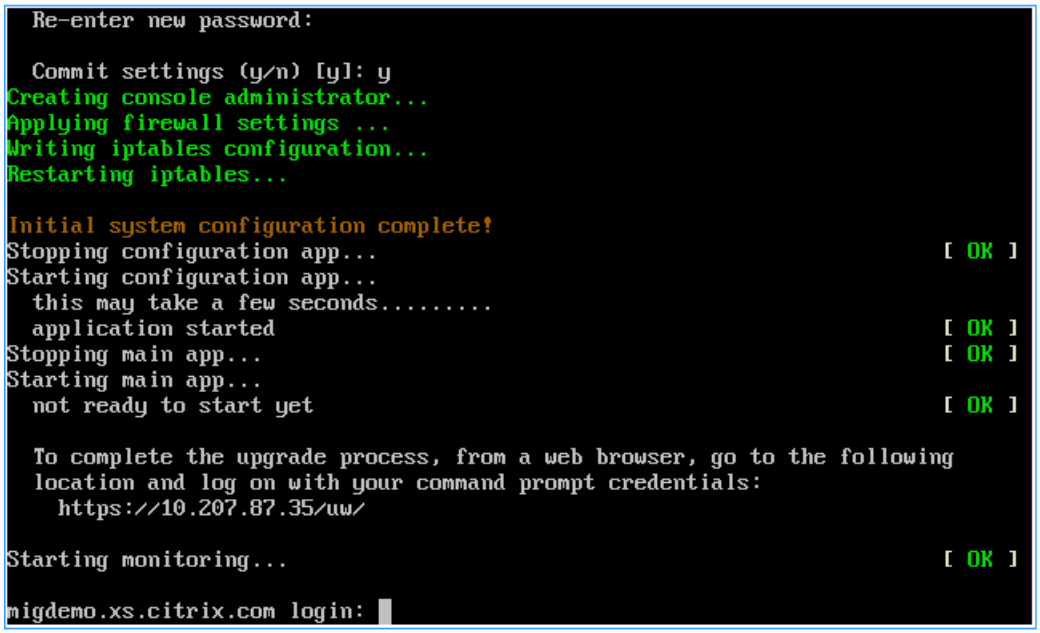
11. Tapez **y** pour valider les paramètres.



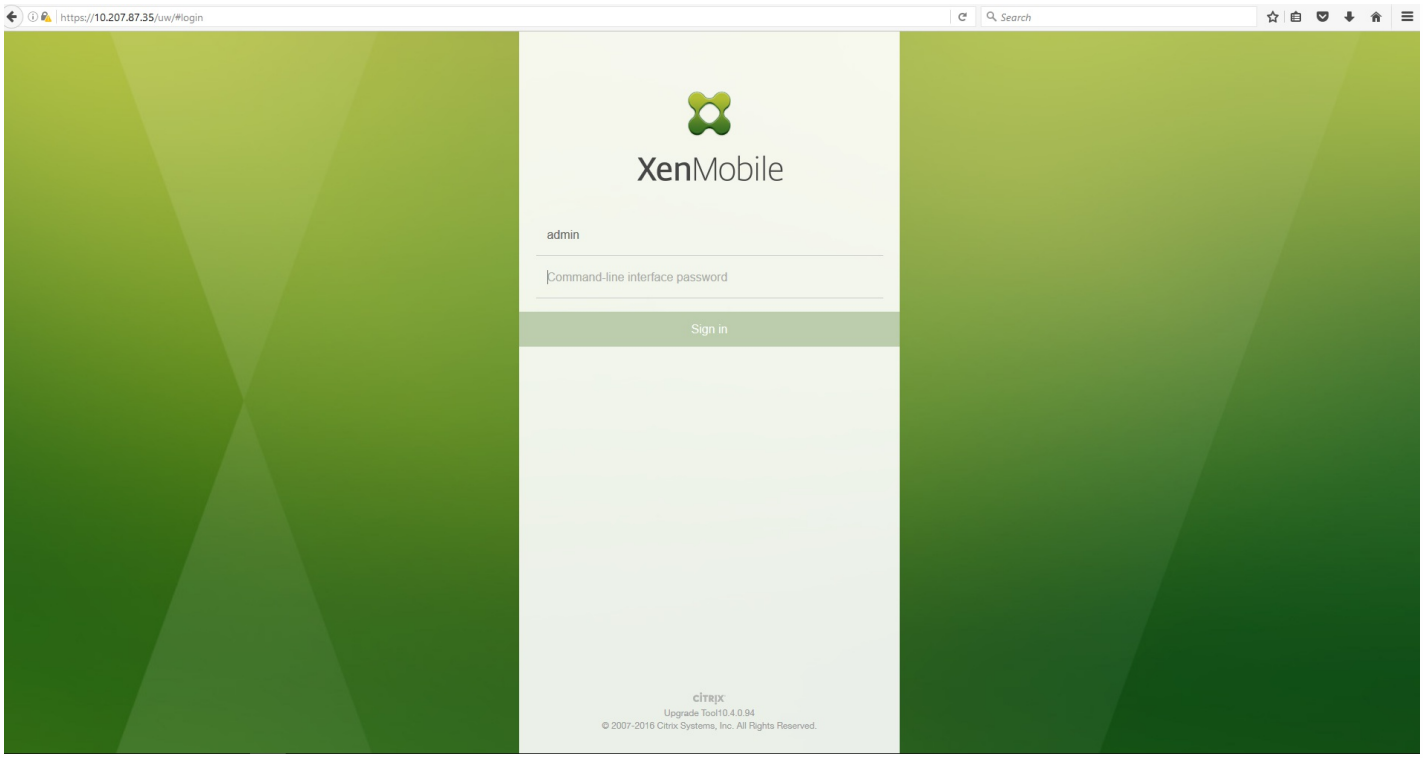
12. Entrez le nom d'utilisateur et le mot de passe de l'administrateur de la console de XenMobile.

13. Tapez **y** pour valider les paramètres.

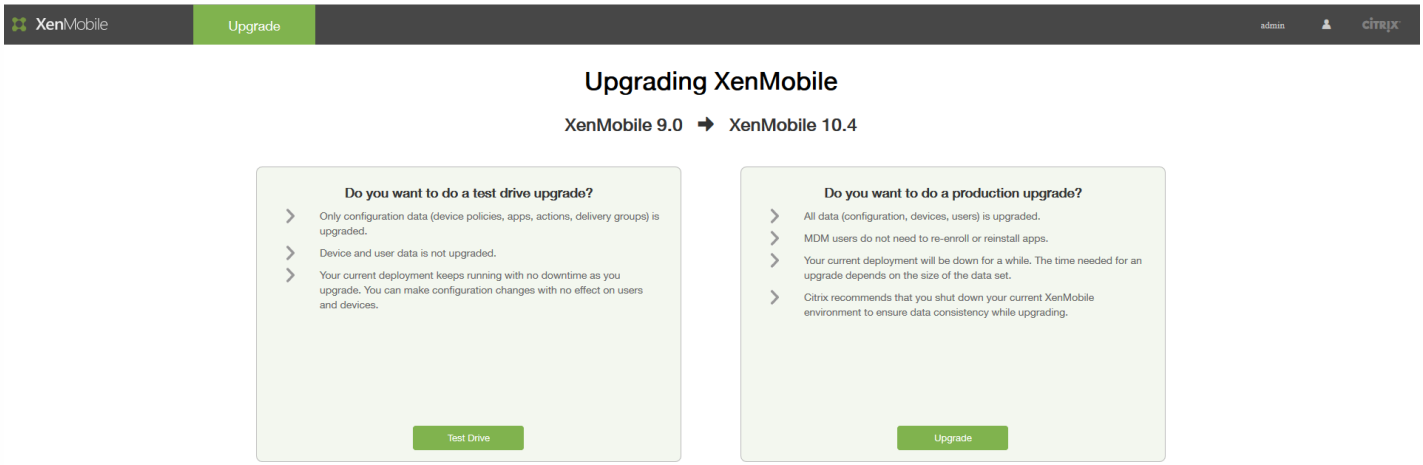
XenMobile 10.4 active l'outil de mise à niveau à usage unique.



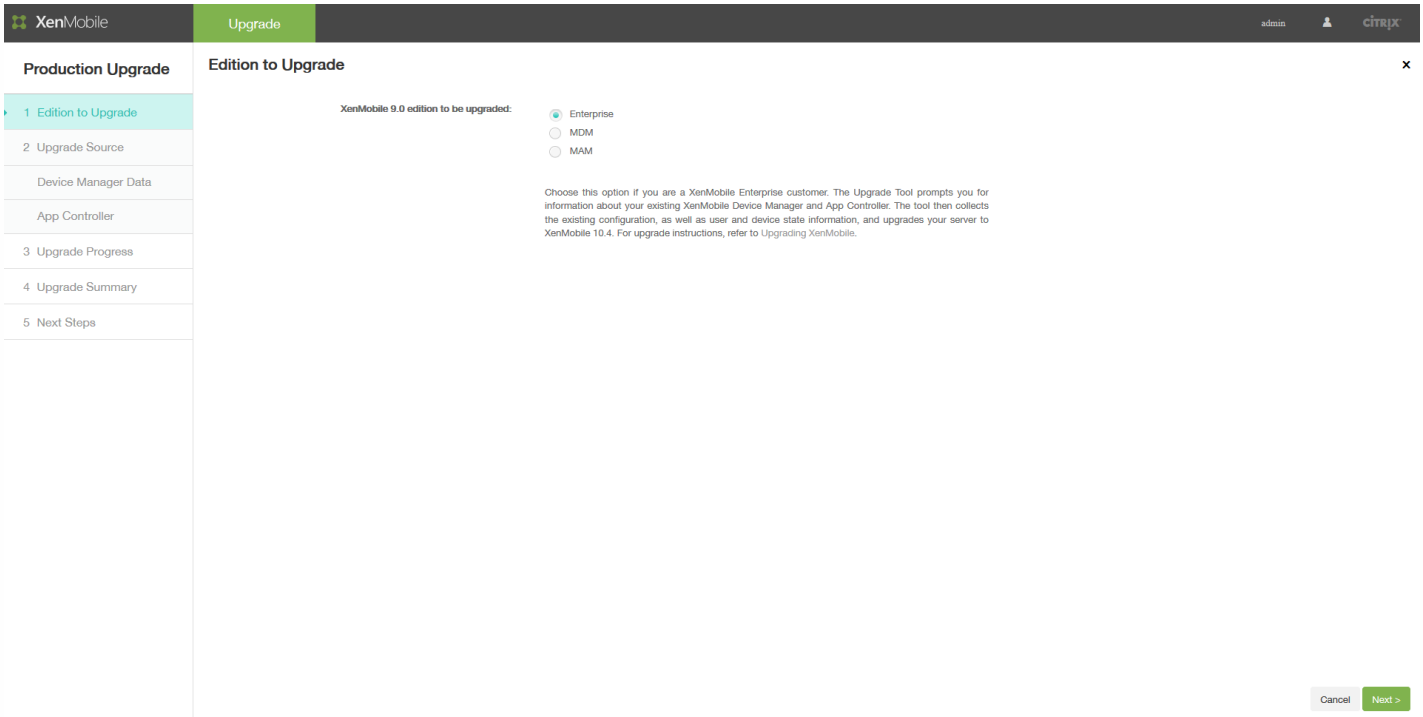
14. Accédez à l'outil de mise à niveau dans un navigateur Web via https://<AdresseIP-serveur-XenMobile>/uw/ et ouvrez une session avec les informations d'identification que vous avez spécifiées à l'aide de l'interface de ligne de commande.



15. Vous pouvez maintenant choisir entre un environnement de test et une mise à niveau de l'environnement de production. Ces instructions font référence à la mise à niveau d'un environnement de production. Dans la page **Upgrading XenMobile**, cliquez sur **Upgrade**.



16. Dans la page **Edition to Upgrade**, sélectionnez votre édition. L'exemple ci-dessous illustre l'écran de l'édition Enterprise.



17. Cliquez sur **Next**.

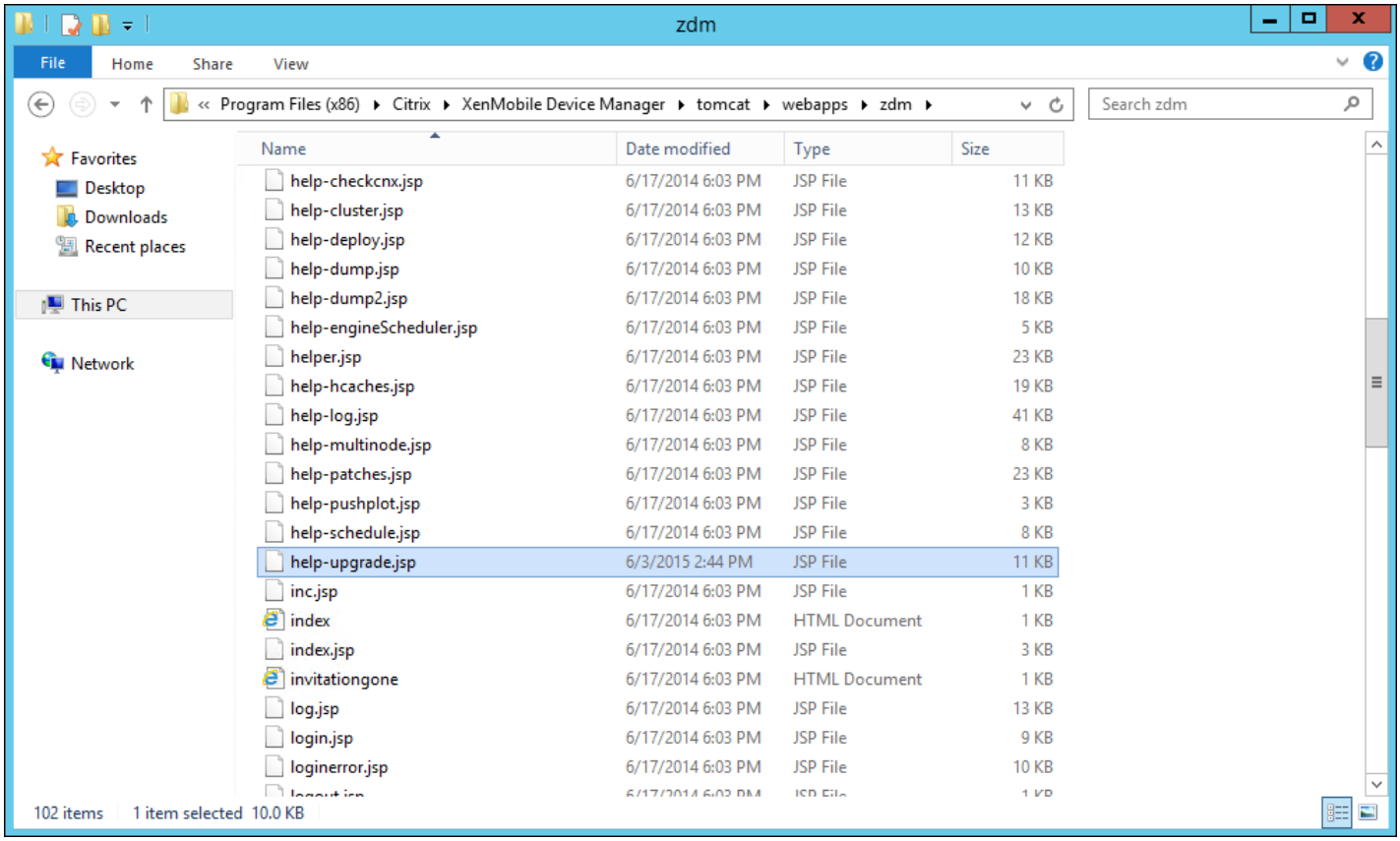
Si vous mettez à niveau une édition Enterprise ou MDM, la page **Device Manager** s'affiche. Suivez les étapes 18 à 22 pour remplir cette page.

Si vous mettez à niveau une édition MAM, passez à l'étape 23 pour remplir la page **App Controller**.

18. Collectez les fichiers requis pour migrer vos données existantes de XenMobile 9.0 Device Manager. Vous devez également avoir accès à l'URL et au nom d'utilisateur de la base de données que vous avez copiés sur la page **Device Manager**.

a. Cliquez sur le lien dans l'étape 1 de la page de **Device Manager**, puis enregistrez le fichier téléchargé help-upgrade.zip.

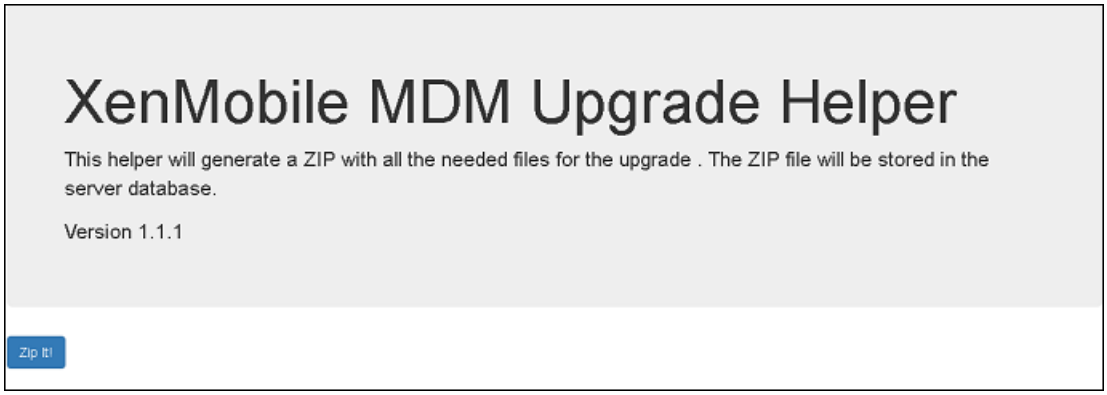
b. Extrayez le fichier help-upgrade.jsp dans <chemin-installation-MDM>\tomcat\webapps\zdm sur votre XenMobile 9.0 Device Manager existant.



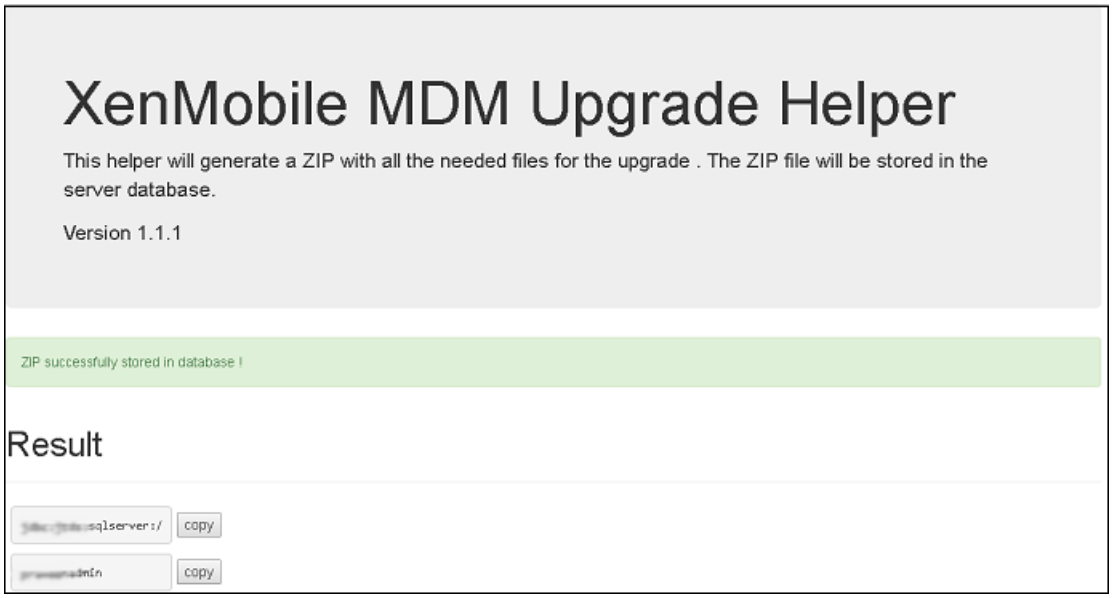
c. Dans une fenêtre de navigateur, connectez-vous au serveur XenMobile 9.0.

d. Dans un onglet de navigateur distinct, entrez cette URL : https://localhost/zdm/help-upgrade.jsp. Cette entrée ouvre la page **XenMobile MDM Upgrade Helper**, qui collecte et compresse tous les fichiers de XenMobile 9.0 qui sont requis pour la mise à niveau vers XenMobile 10.4. Le fichier compressé est stocké dans la base de données du serveur à partir de laquelle il est extrait.

e. Cliquez sur **Zip it** et suivez les instructions à l'écran pour collecter les fichiers requis pour la mise à niveau.



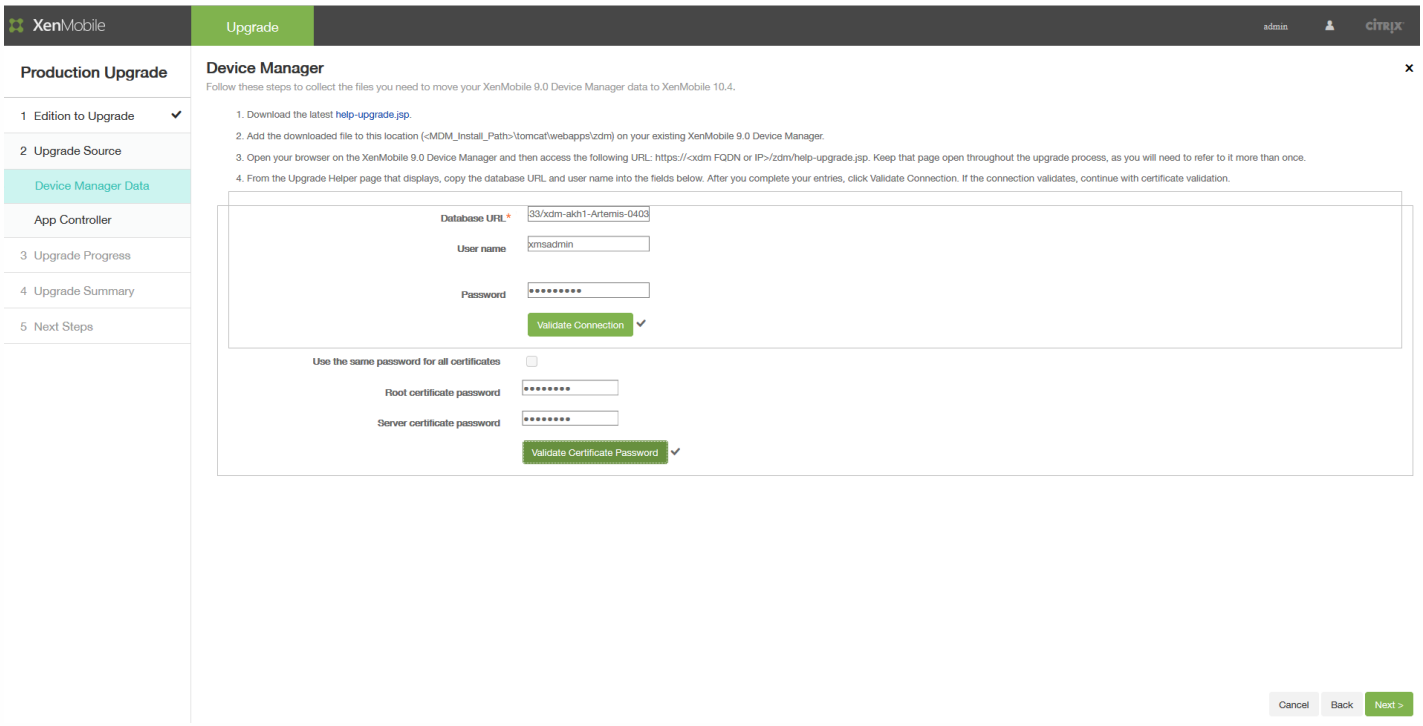
19. Sous **Result**, copiez l'URL et collez-la dans le champ **Database URL** dans la page **Device Manager** de l'outil de mise à niveau. Ensuite, copiez le nom d'utilisateur et collez-le dans la page **Device Manager**.



20. Dans l'outil de mise à niveau :

    a. Entrez le mot de passe et cliquez sur **Validate Connection**.

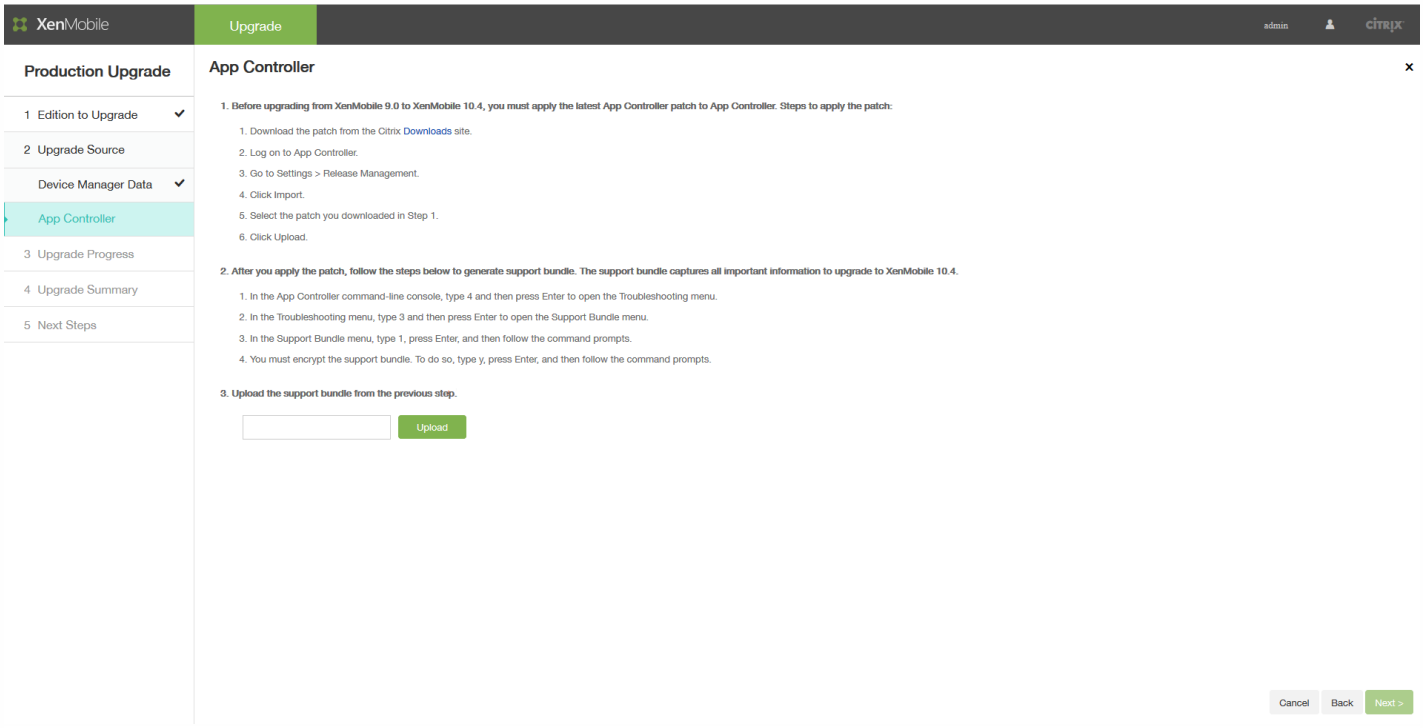
    b. Entrez le mot de passe pour chaque certificat et cliquez sur **Validate Password**.



21. Cliquez sur **Next**.

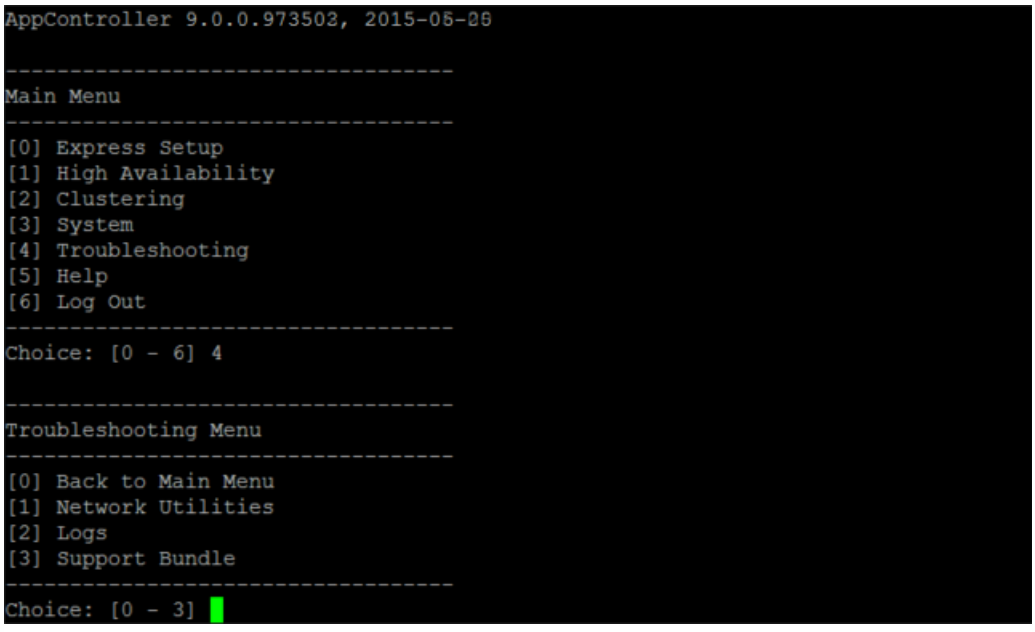
22. Si vous avez modifié le fichier ew-config.properties, redémarrez le service xdm sur XenMobile 9 MDM, puis accédez à https://localhost/zdm/help-upgrade.jsp pour exécuter le fichier zip. De cette façon, le fichier ew-config.properties est lu de nouveau et il est enregistré dans la base de données XenMobile MDM 9 pour préparer la migration.

23. Vous allez ensuite appliquer un correctif de mise à niveau à App Controller, puis générer et charger un pack d'assistance. Commencez par suivre les instructions de la section 1 de la page **App Controller** pour mettre à niveau App Controller.

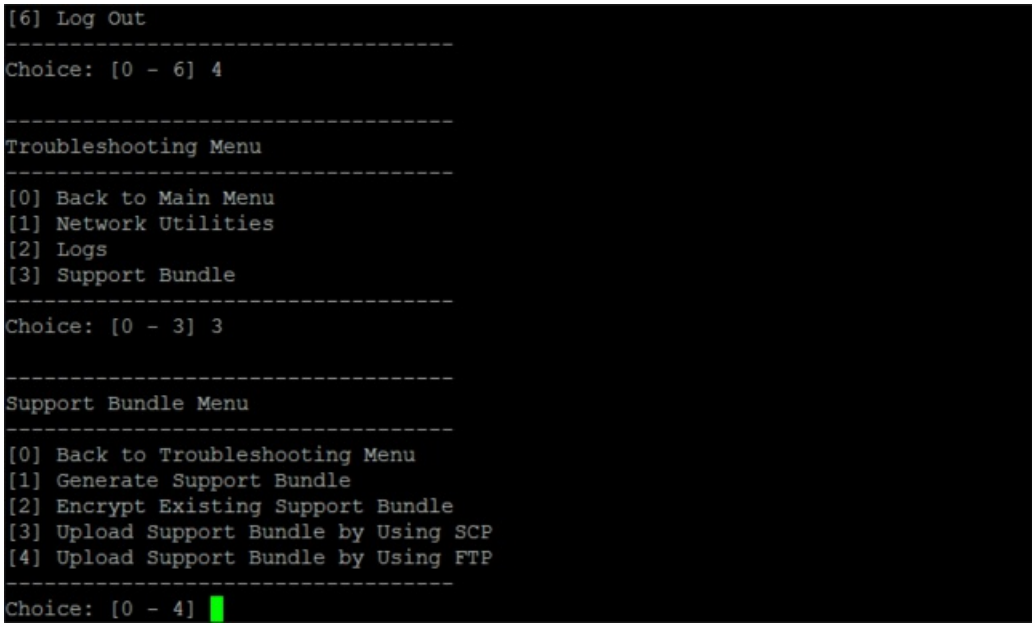


25. Passez aux instructions de la section 2 de la page **App Controller** :

a. Dans la console de ligne de commande d'App Controller, tapez **4**, puis appuyez sur ENTRÉE pour ouvrir le menu Troubleshooting.

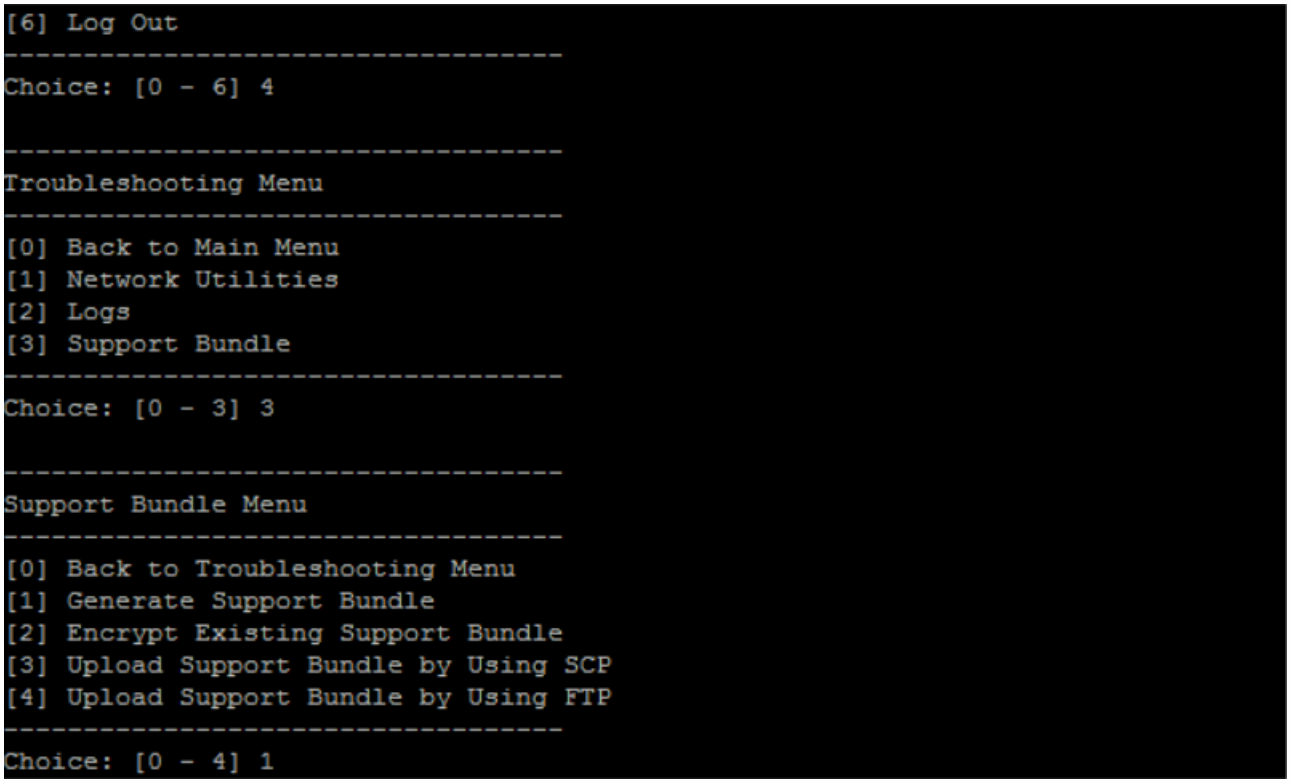


b. Dans le menu Troubleshooting, tapez **3**, puis appuyez sur ENTRÉE pour ouvrir le menu Support Bundle.



c. Dans le menu Support Bundle, tapez **1**, puis appuyez sur ENTRÉE et suivez les invites de commande.

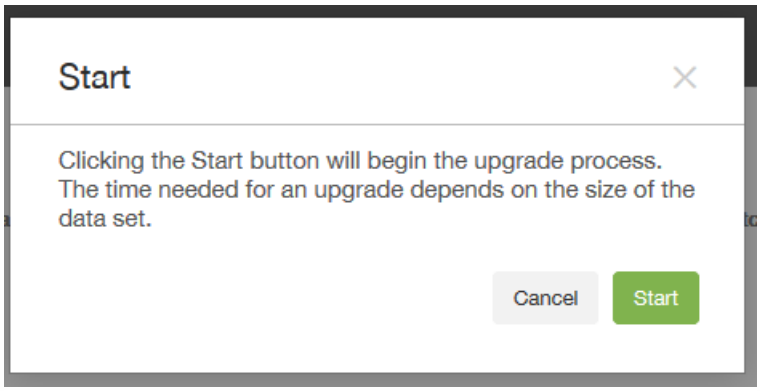
Remarque : vous devez chiffrer le pack d'assistance.



26. Dans la section 3 de la page **App Controller**, spécifiez le pack d'assistance, puis cliquez sur **Upload**.

L'outil de mise à niveau traite les fichiers collectés (pour les éditions XenMobile Enterprise et MAM) et le pack d'assistance. Cette étape peut prendre plus de 15 minutes si vous migrez un grand nombre d'utilisateurs.

27. Cliquez sur **Suivant**. La boîte de dialogue de confirmation **Start** s'affiche.



28. Cliquez sur **Start**. La page **Upgrade Progress** affiche ensuite des indicateurs de progression pour vous permettre de suivre la mise à niveau des données depuis XenMobile 9.0. Une fois la mise à niveau terminée, les indicateurs de progression sont tous à 100 % et le bouton **Next** est activé.

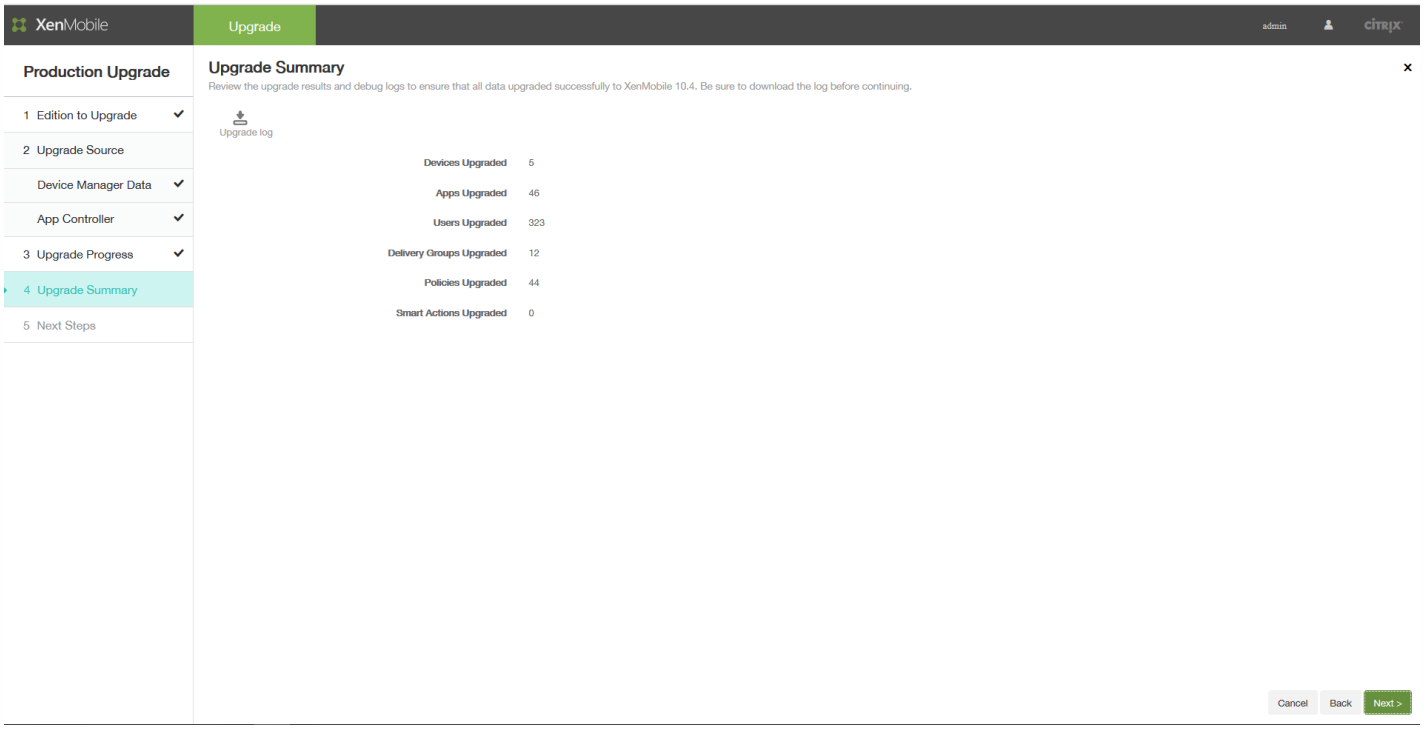
Remarque

Si la mise à niveau échoue, vous pouvez afficher les journaux pour comprendre la raison de l'erreur. Ensuite, vous devez importer une nouvelle instance de XenMobile 10.4 et redémarrer le processus de mise à niveau. Vous ne pouvez pas utiliser le bouton Précédent du navigateur pour revenir sur les pages précédentes et corriger les informations.

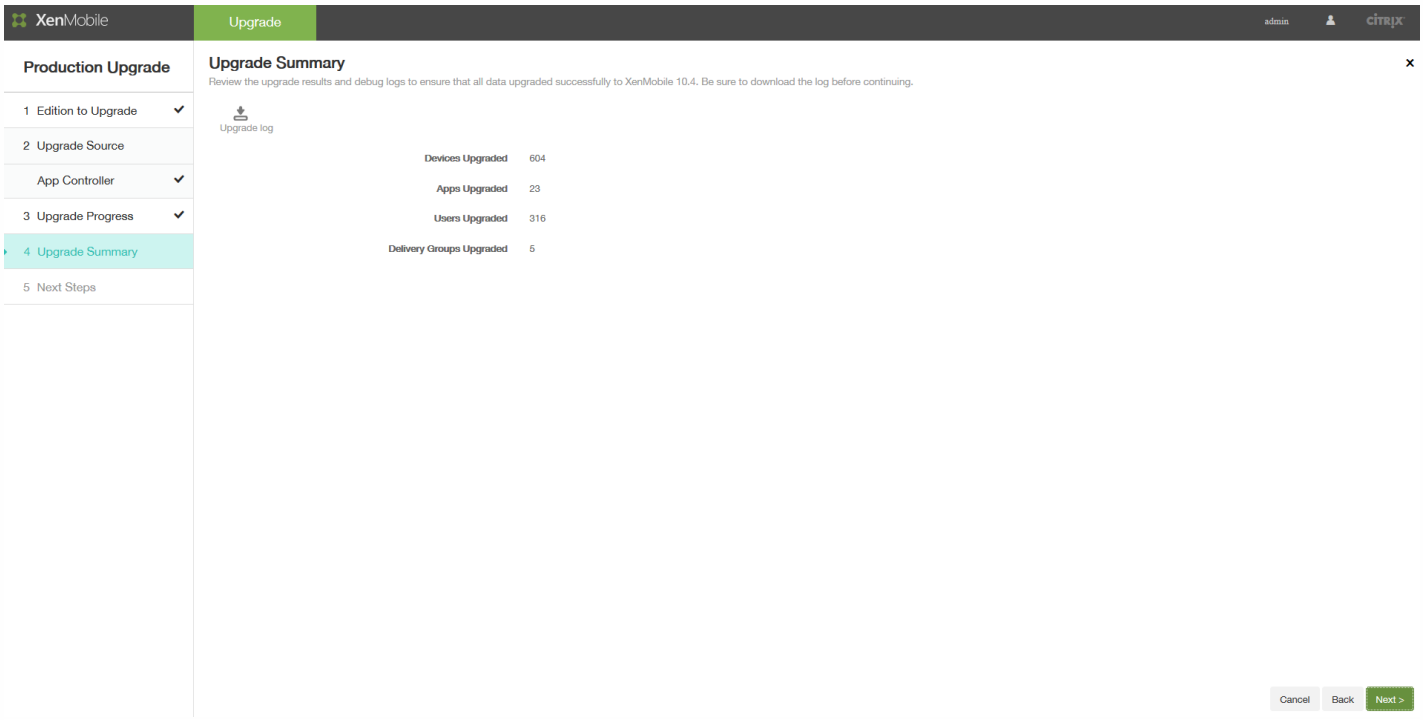
La page Upgrade Progress vous indique quand la mise à niveau est terminée.

29. Cliquez sur **Suivant**. La page **Upgrade Summary** s'affiche.

Si vous mettez à niveau une édition Enterprise ou MAM, la page **Upgrade Summary** peut ressembler à cela :



Si vous mettez à niveau une édition MDM, la page **Upgrade Summary** peut ressembler à cela :

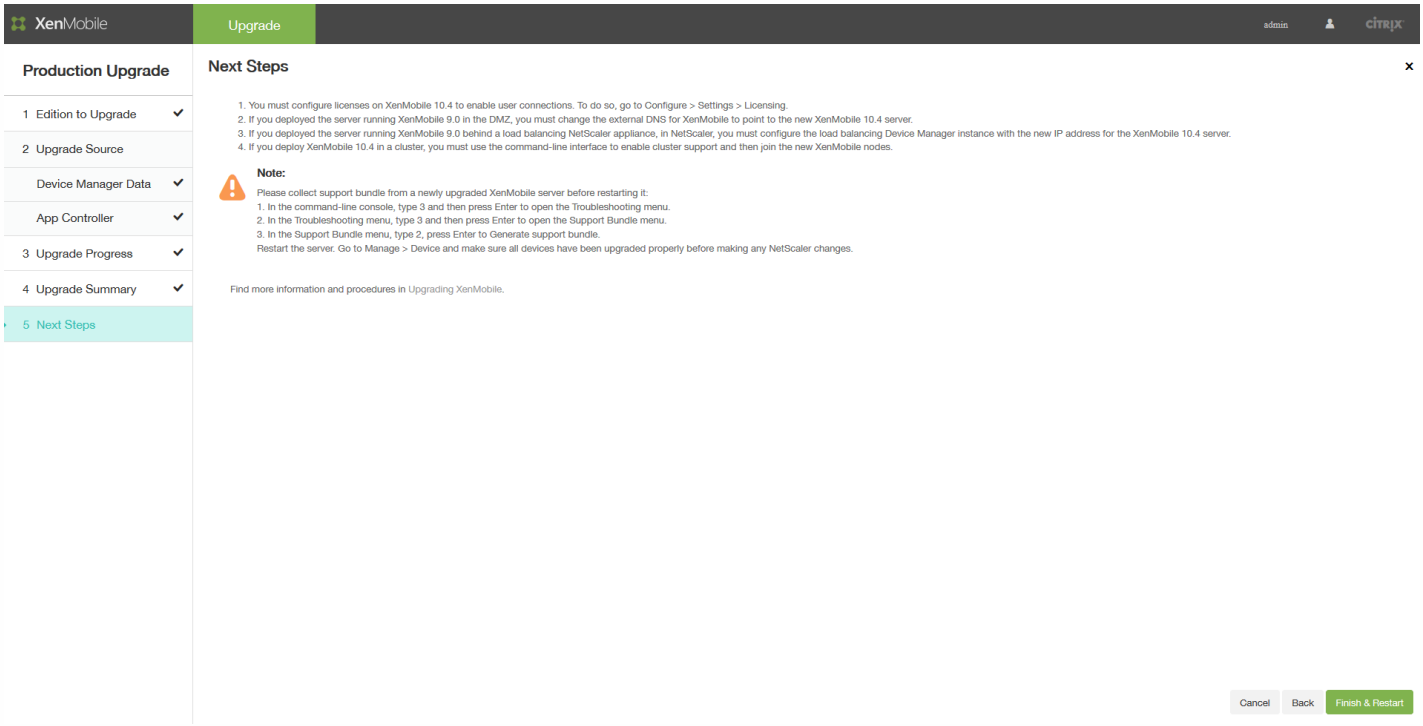


30. Cliquez sur l'icône **Upgrade log** pour télécharger le journal. N'oubliez pas de télécharger le fichier journal avant de quitter cette page.

Citrix vous recommande de consulter le fichier journal pour déterminer les stratégies, paramètres, données utilisateur et ainsi

de suite qui ont été mis à niveau ou non vers XenMobile 10.4.

31. Après avoir téléchargé le journal de mise à niveau, cliquez sur **Next**. La page **Next Steps** s'affiche.



Pour obtenir des instructions liées à ces étapes, veuillez consulter la section Post-requis de l'outil de mise à niveau.

Post-requis de l'outil de mise à niveau

Feb 23, 2017

Une fois que l'outil de mise à niveau a terminé, il fournit une liste générale des étapes suivantes. Les tâches requises pour votre environnement peuvent varier en fonction de votre version installée de NetScaler, selon que vous avez utilisé l'assistant NetScaler pour XenMobile pour configurer NetScaler et selon votre édition de XenMobile.

Veillez à consulter la liste des tâches qui suit et effectuez toutes celles qui s'appliquent à votre environnement.

1. Configurer des licences sur XenMobile pour activer les connexions utilisateur. Pour plus de détails, consultez cette procédure.

2. Si vous avez déployé le serveur exécutant XenMobile 9.0 dans la DMZ, modifiez le DNS externe XenMobile pour le faire pointer vers le nouveau serveur XenMobile 10.4.

3. Si vous avez déployé le serveur exécutant XenMobile 9.0 derrière un boîtier d'équilibrage de charge NetScaler, apportez les modifications suivantes sur NetScaler :

   a. Configurez un nouveau serveur virtuel d'équilibrage de charge pour la mise à niveau. Pour plus de détails, consultez cette procédure.

   b. Configurez un enregistrement d'adresse pour pointer le nom de domaine complet du serveur App Controller vers le nouvel équilibrage de charge pour la mise à niveau. Pour plus de détails, consultez cette procédure.

   c. Changez le serveur virtuel d'équilibrage de charge de Device Manager pour pointer vers la nouvelle adresse IP du serveur XenMobile. Pour plus de détails, consultez cette procédure.

   d. Changez NetScaler Gateway pour pointer vers le nouveau nom de domaine complet du serveur XenMobile. Pour plus de détails, consultez cette procédure.

   e. Les tâches suivantes sont requises uniquement dans ces cas :

      - Si vous avez utilisé l'assistant NetScaler pour XenMobile 9 avec NetScaler 11.1, 11.0 ou 10.5 ; ou

      - Si vous utilisez NetScaler Gateway 10.1 (qui n'est pas recommandé) ; ou

      - Si vous n'avez pas utilisé l'assistant NetScaler pour XenMobile lors de la configuration de NetScaler 10.5 ou version supérieure pour XenMobile.

   Pour les procédures à suivre pour les cas précédents, veuillez consulter les articles suivants dans la documentation de l'outil de mise à niveau XenMobile 10.1 :

      Créez un nouveau serveur virtuel d'équilibrage de charge MAM basé sur une configuration MDM de pont SSL
      Créez un nouveau serveur virtuel d'équilibrage de charge MAM basé sur une configuration MDM de déchargement SSL.

4. Si vous déployez XenMobile 10.4 dans un cluster, vous devez utiliser l'interface de ligne de commande XenMobile 10.4 pour activer la prise en charge de cluster et rejoindre les nouveaux nœuds XenMobile. Pour obtenir de l'aide avec l'interface de ligne de commande XenMobile, consultez la section Options du menu de mise en cluster.

5. Effectuez les étapes requises après la mise à niveau, en fonction des besoins de votre environnement.

Cet article couvre également les étapes requises pour les paramètres liés à Secure Ticket Authority, au protocole NTP, au nom d'hôte du serveur XenMobile, aux informations de mise à jour qui n'ont pas été mises à niveau, au nom du magasin personnalisé et à l'inscription d'appareils XenMobile après la mise à niveau.

Configurer des licences sur XenMobile pour activer les connexions utilisateur

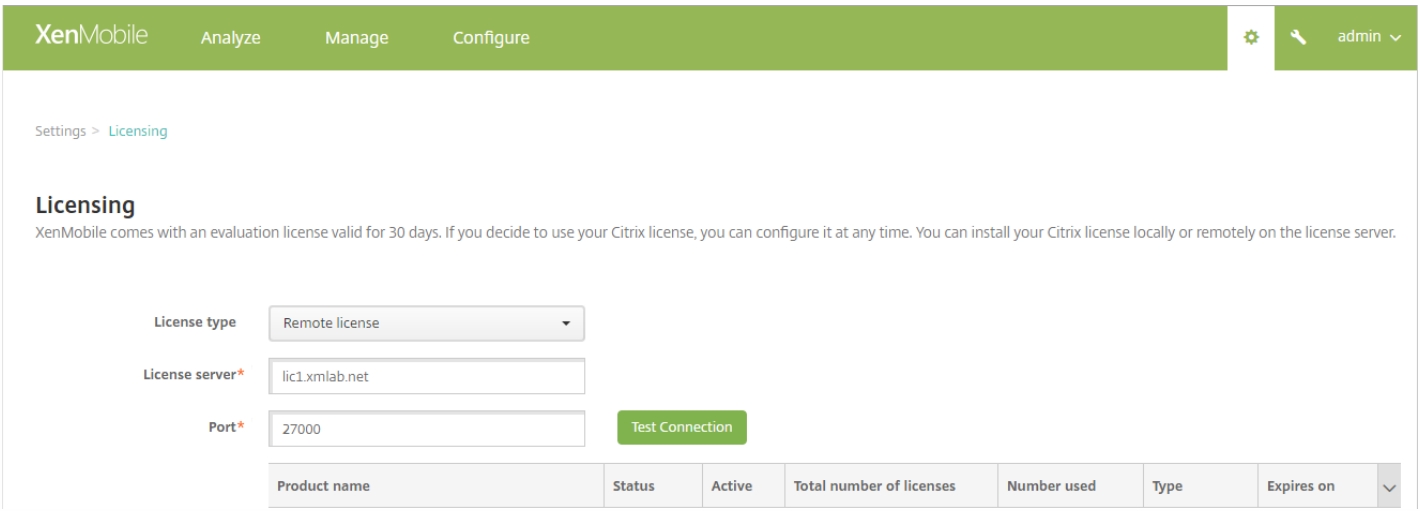
XenMobile 10.4 prend uniquement en charge le système de licences Citrix V6. Vous devez définir la configuration de licence distante ou locale dans la console XenMobile 10.4 pour activer les connexions utilisateur, comme suit.

1. Téléchargez le fichier de licences. Pour ce faire, consultez la section Système de licences Citrix.

2. Ouvrez une session sur la console XenMobile 10.4 mise à niveau : accédez à https://:4443.

- Pour les mises à niveau MDM ou ENT, ouvrez une session à l'aide de vos informations d'identification d'administrateur XenMobile 9.0 Device Manager.
- Pour les mises à niveau MAM, ouvrez une session à l'aide de vos informations d'identification d'administrateur XenMobile 9.0 App Controller.

3. Accédez à **Paramètres > Système de licences**.



Pour de plus amples informations sur l'ajout de licences locales et distantes, consultez la section Système de licences.

Configurez un nouveau serveur virtuel d'équilibrage de charge pour la mise à niveau

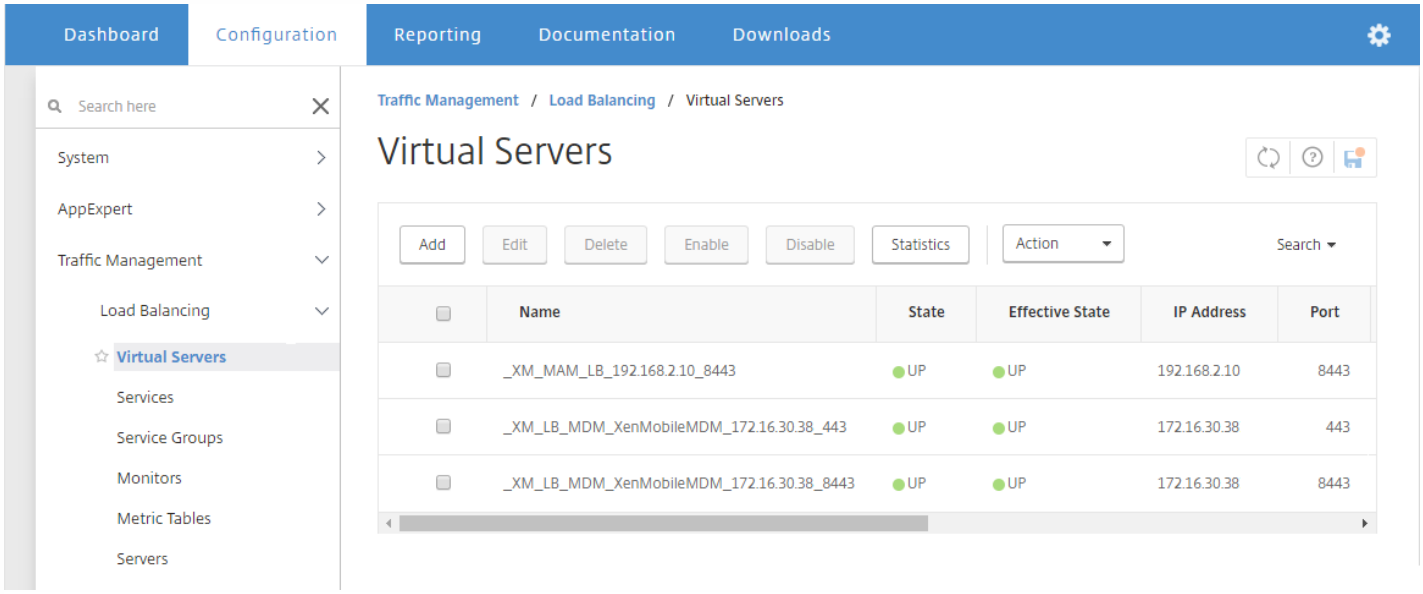
> **Important**
>
> Ce post-requis s'applique *uniquement* lorsque vous mettez à niveau une mise à niveau de production de XenMobile Enterprise Edition ; il ne concerne pas les mises à niveau de MAM ou MDM.

Après une mise à niveau de production de XenMobile Enterprise Edition vers XenMobile 10.4, vous devez configurer un nouveau serveur virtuel d'équilibrage de charge pour le nom de domaine complet de XenMobile 9.0 App Controller. Pour ce faire, vous devez utiliser l'outil de configuration NetScaler Gateway.

Les exemples d'écran dans cette section, pour NetScaler Gateway 11.1, sont similaires à NetScaler Gateway versions 11.0 et

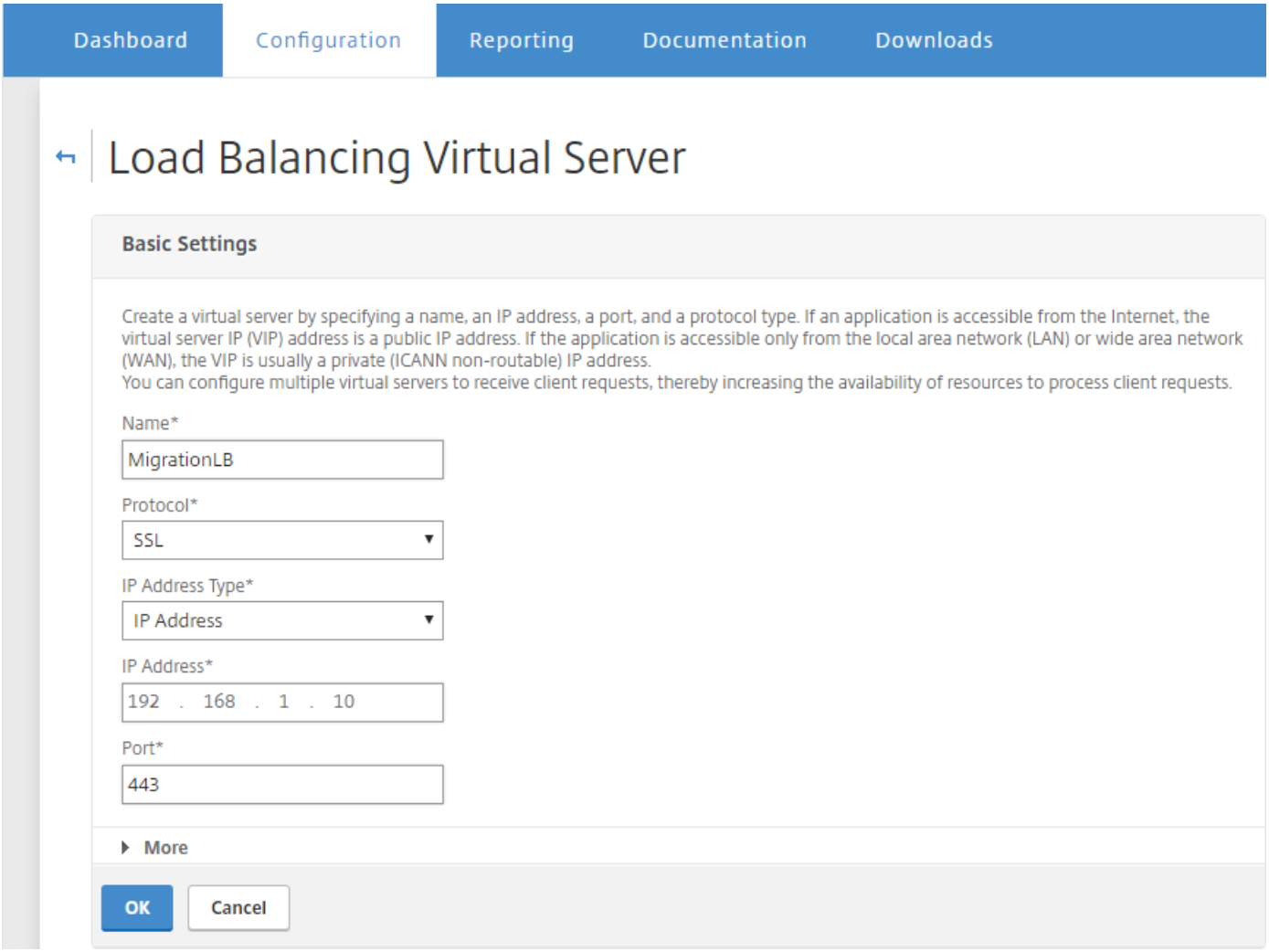
10.5.

1. Cliquez sur **Traffic Management > Load Balancing > Virtual Servers**.



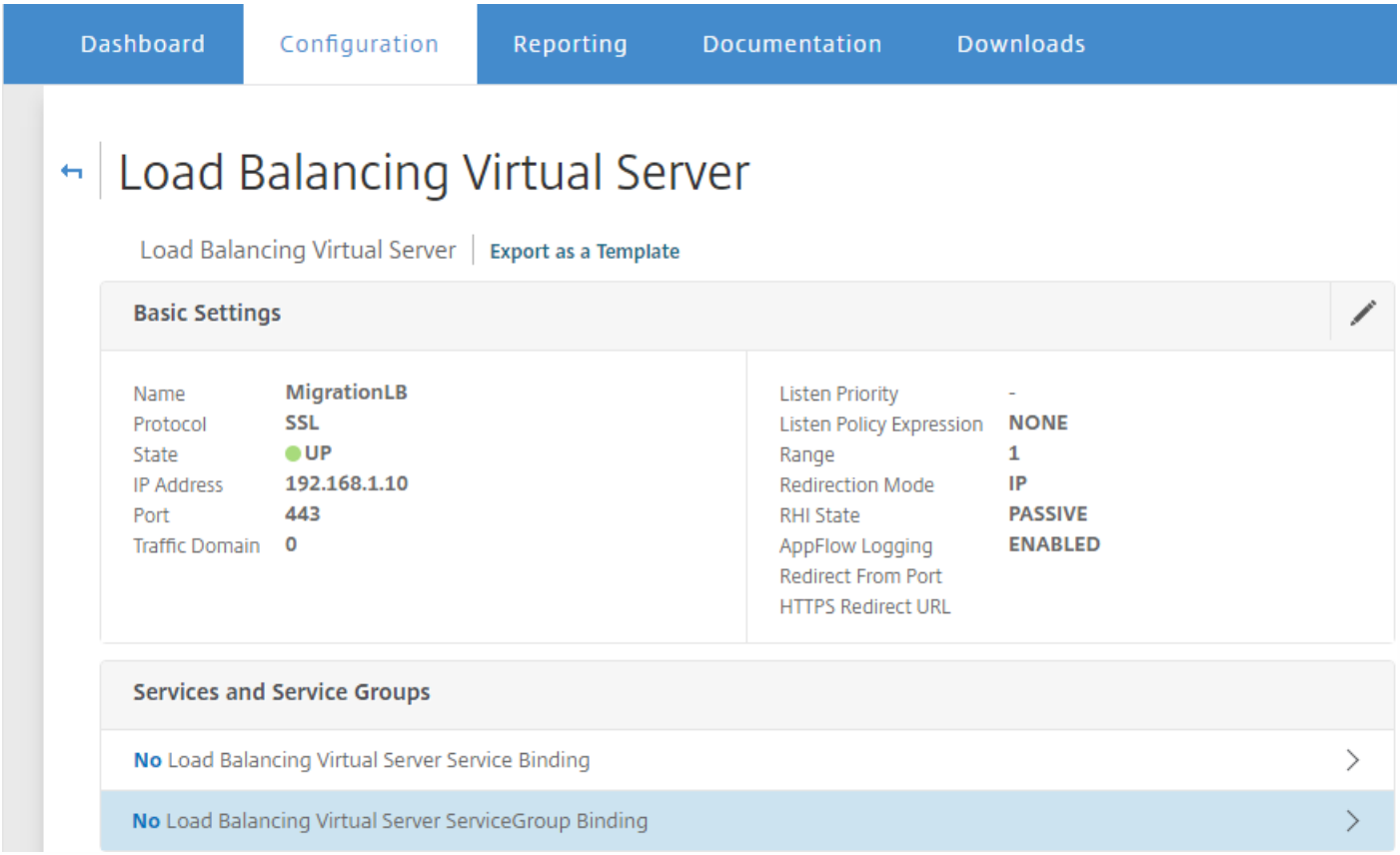
2. Cliquez sur **Ajouter**.

3. Sur la page **Load Balancing Virtual Server**, configurez les paramètres suivants, puis cliquez sur **OK**.

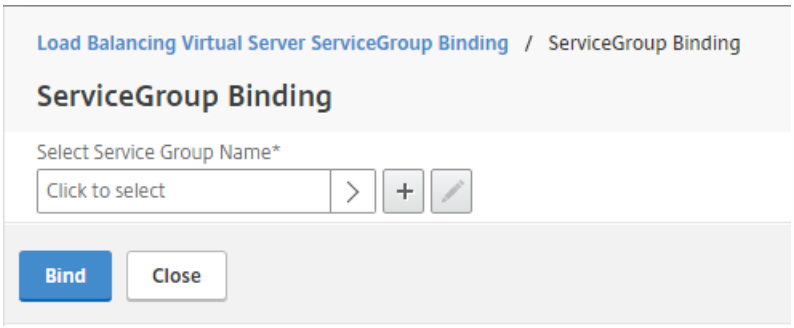


- **Name** : tapez un nom pour le nouvel équilibrage de charge.
- **Protocole** : définissez sur **SSL**. La valeur par défaut est **HTTP**.
- **IP Address** : entrez une adresse IP pour le nouvel équilibrage de charge, en respectant la norme RFC 1918 ; par exemple 192.168.1.10.
- **Port** : définissez sur **443**.

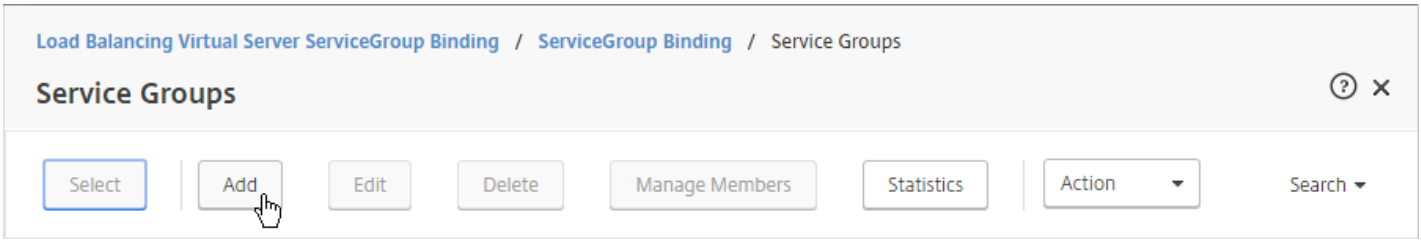
4. Sous **Services and Service Groups**, cliquez sur **No Load Balancing Virtual Server Service Group Binding**.



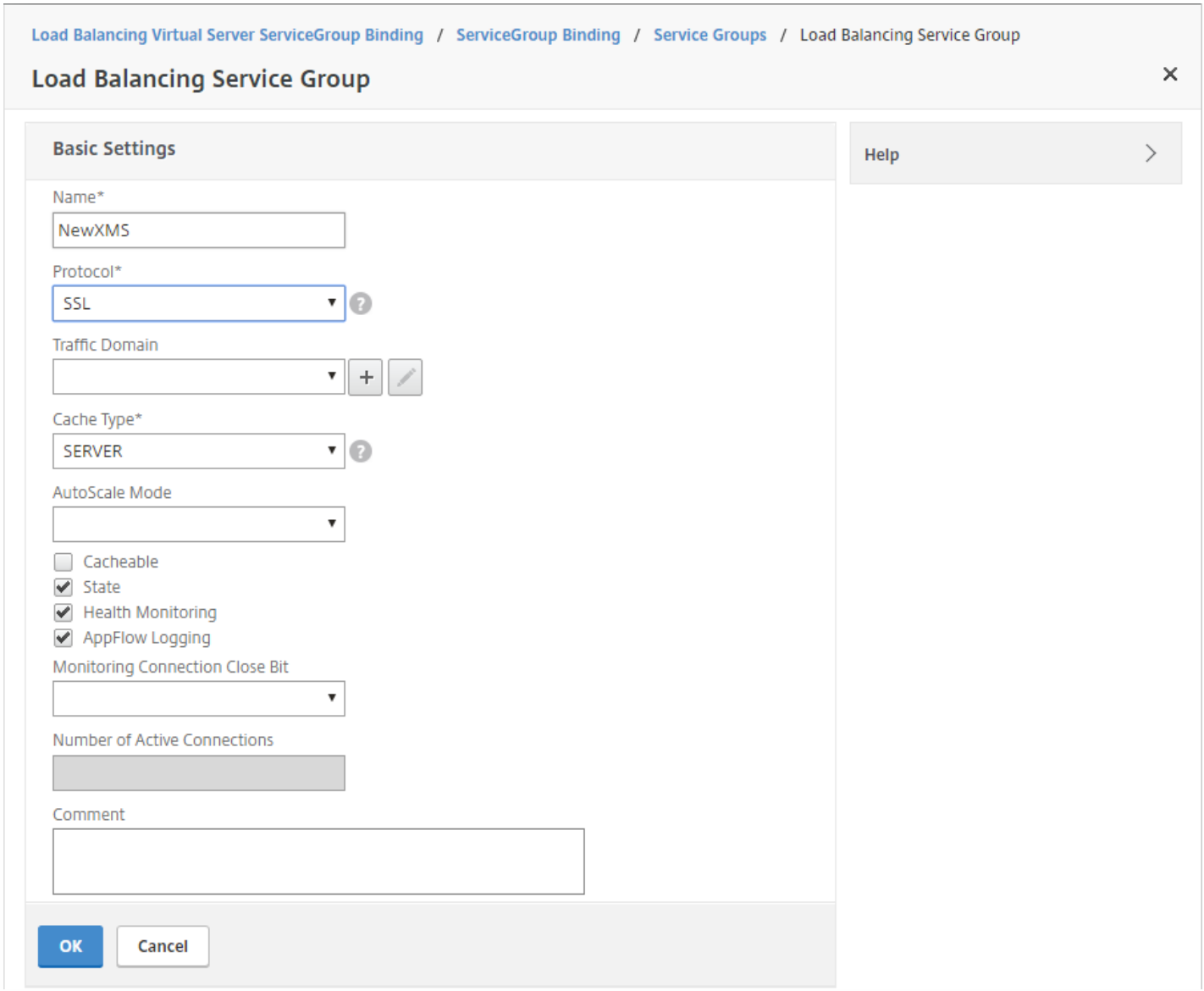
5. Sous **Select Service Group Name**, cliquez sur **Click to Select**.



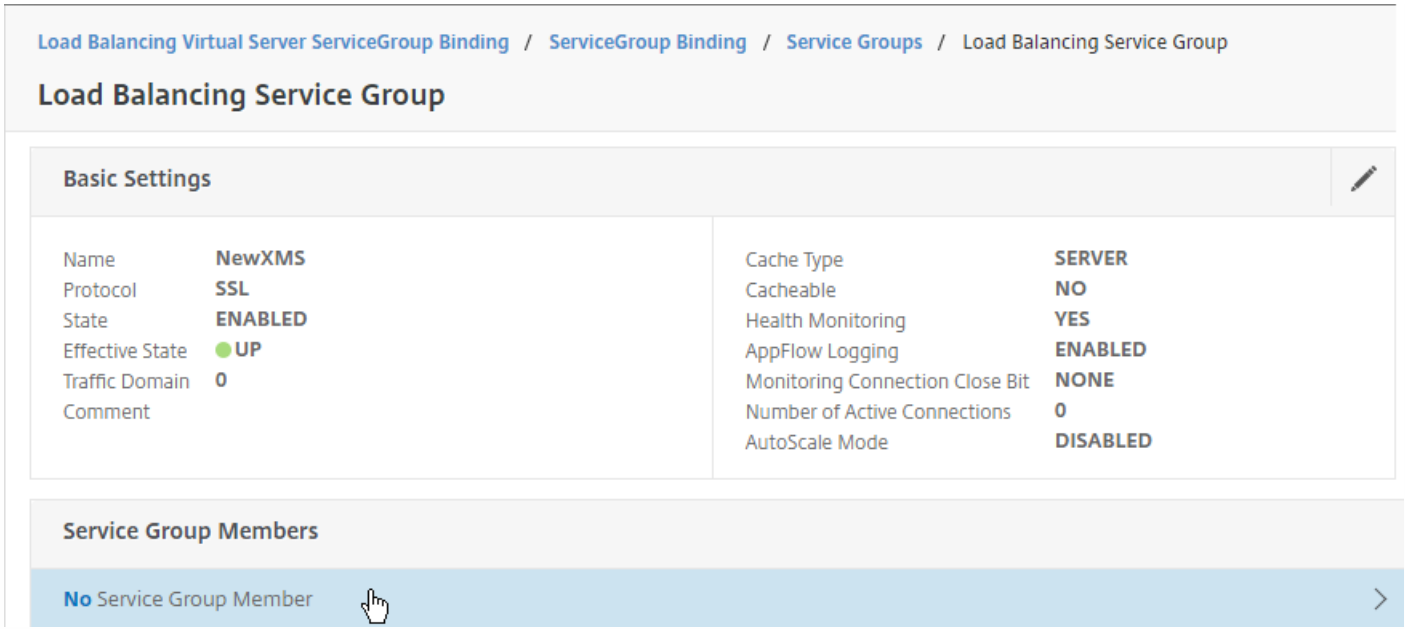
6. Cliquez sur **Add** pour créer un groupe de services.



7. Sur la page **Load Balancing Service Group**, entrez un nom pour le nouveau groupe de services, vérifiez que le protocole est défini sur **SSL**, puis cliquez sur **OK**.

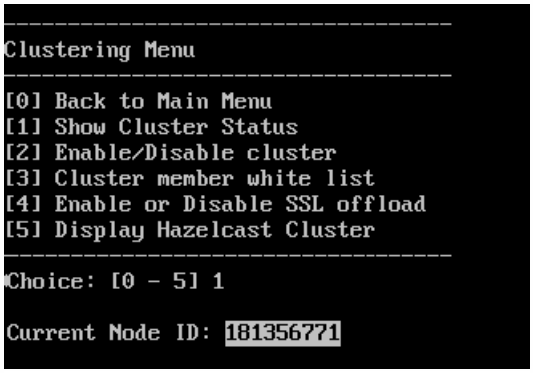


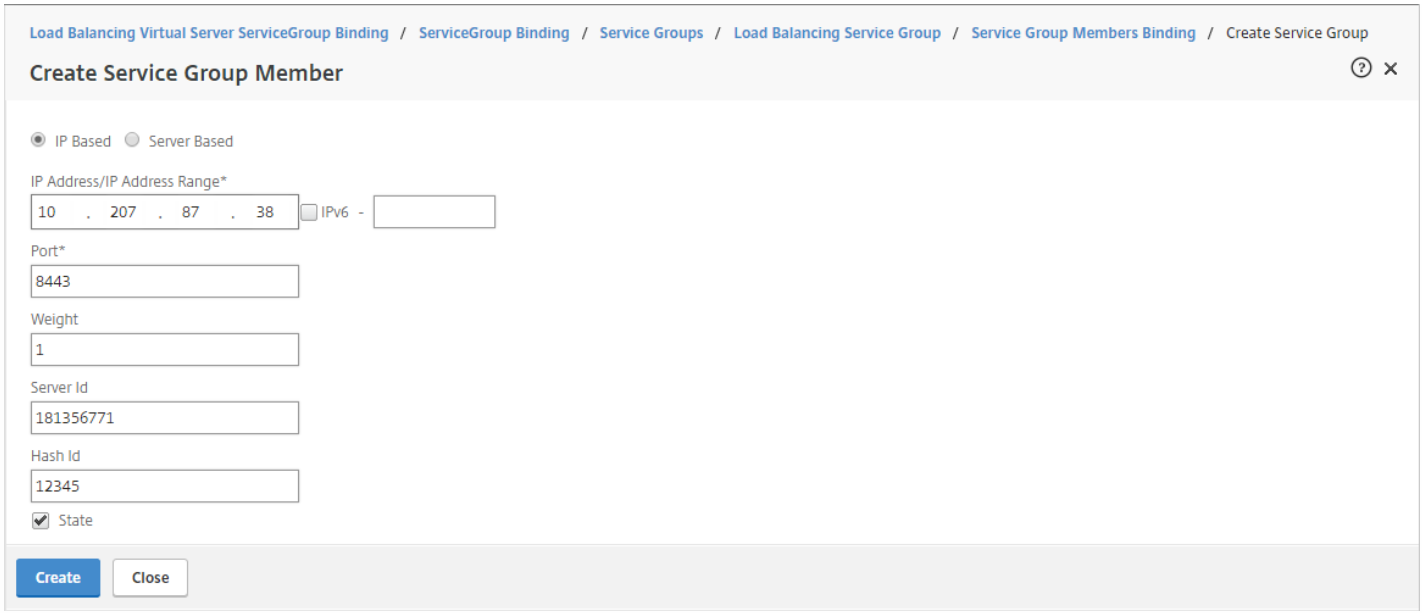
8. Cliquez sur **No Service Group Member**.



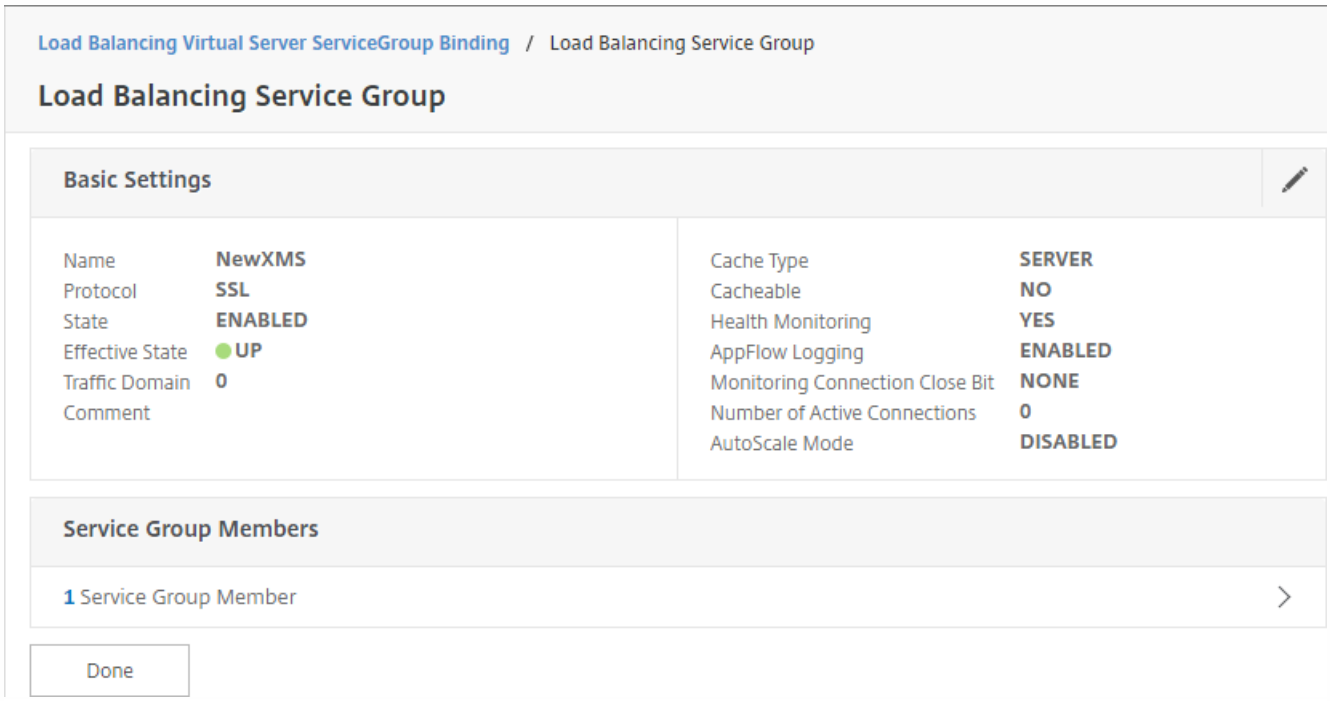
9. Sur la page **Create Service Group Member**, configurez les paramètres suivants :

- **IP Address/IP Address Range*** : entrez l'adresse IP du serveur XenMobile 10.4.
- **Port** : définissez sur **8443**.
- **Server ID** : si vous migrez d'un environnement XenMobile 9.0 en cluster vers un environnement XenMobile 10.4 en cluster, entrez l'ID du nœud de serveur (Server Node ID) du serveur XenMobile actuel. Pour obtenir l'ID du nœud de serveur, connectez-vous à l'interface de ligne de commande du serveur XenMobile 10.4 et tapez **1** pour accéder au menu **Clustering**. L'ID du nœud de serveur dans l'interface de ligne de commande est appelé **ID du nœud actuel** (Current Node ID).



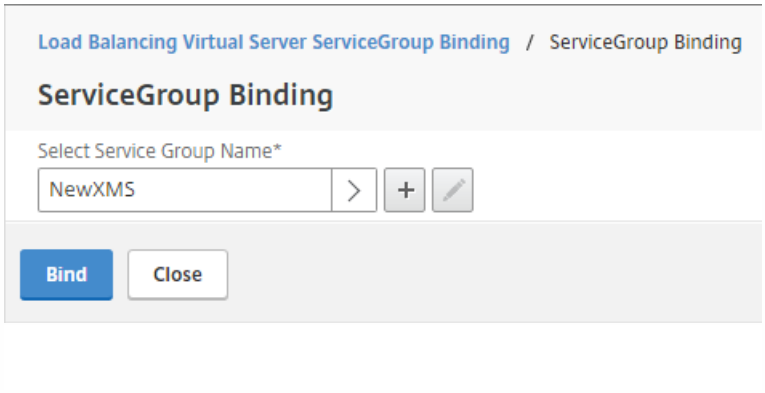


10. Cliquez sur **Create**, puis cliquez sur **Done**.

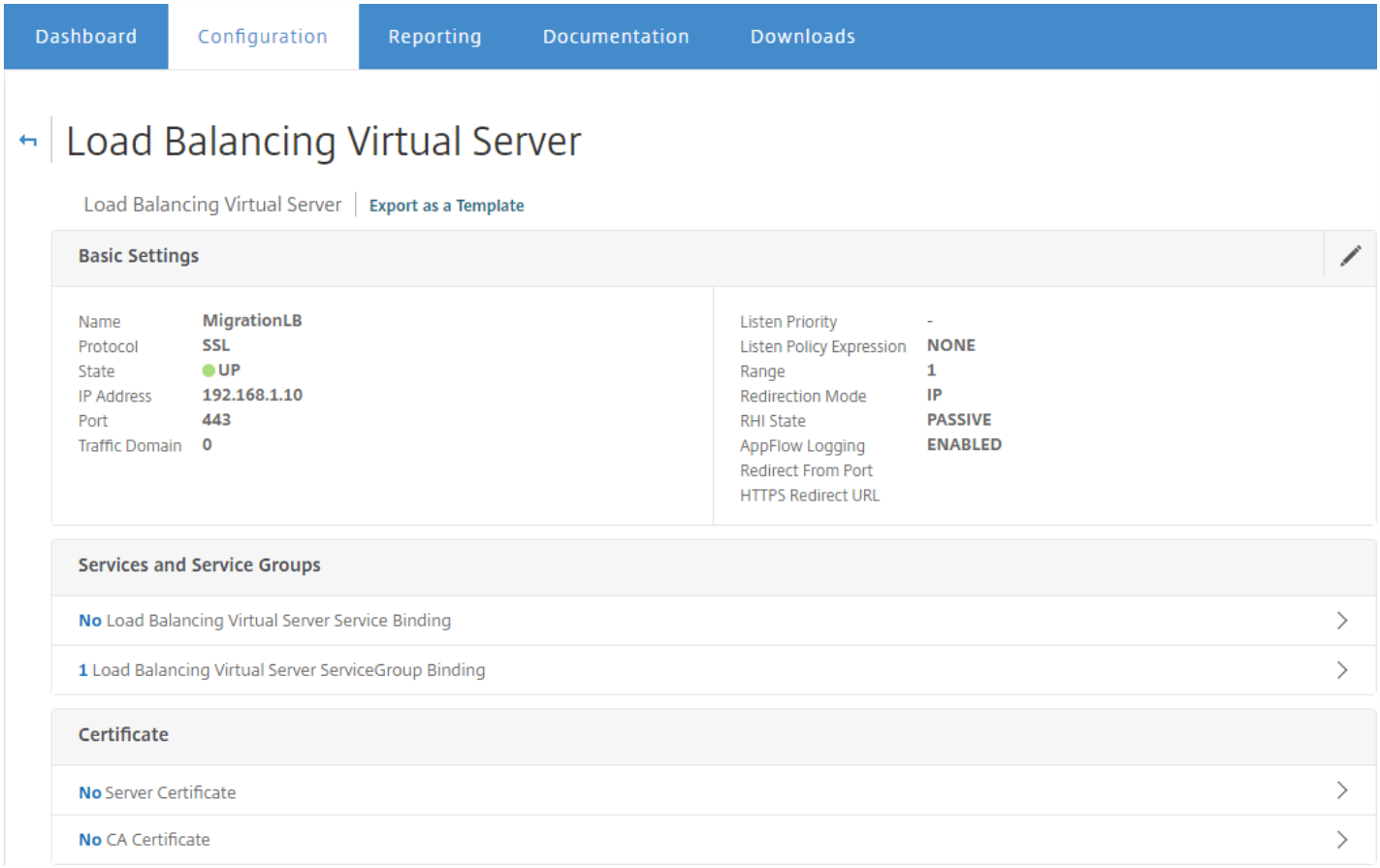


11. Cliquez sur **Done**, puis sur **OK**.

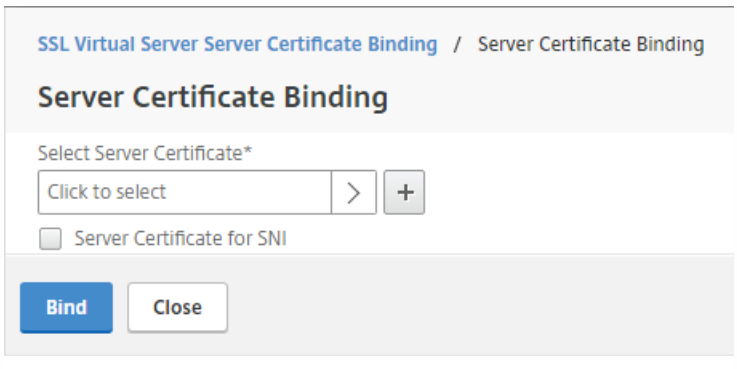
12. Cliquez sur **Bind**, puis sur l'écran suivant, cliquez sur **Done**.



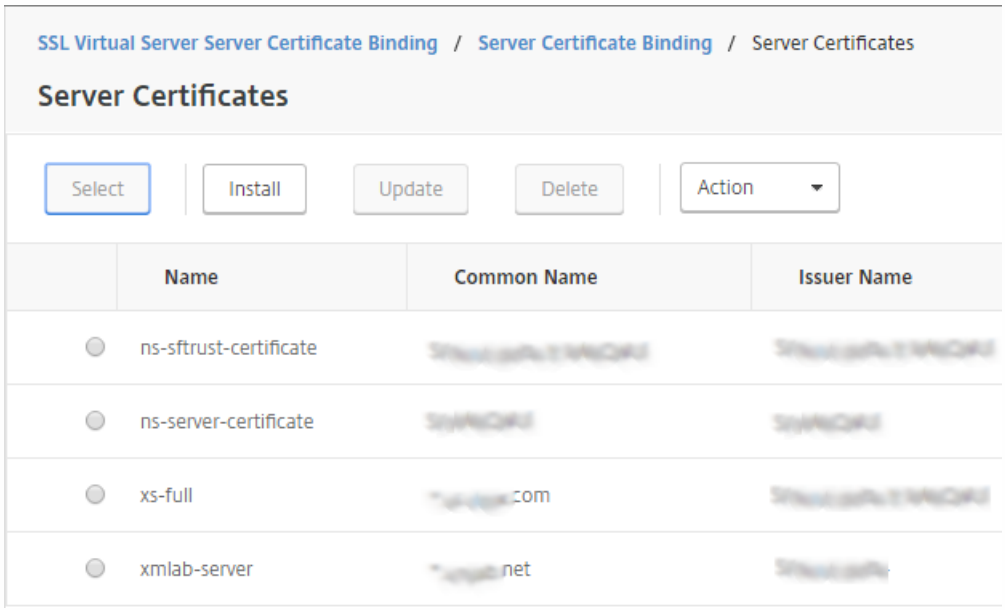
13. Sous **Certificates**, cliquez sur **No Server Certificate**.



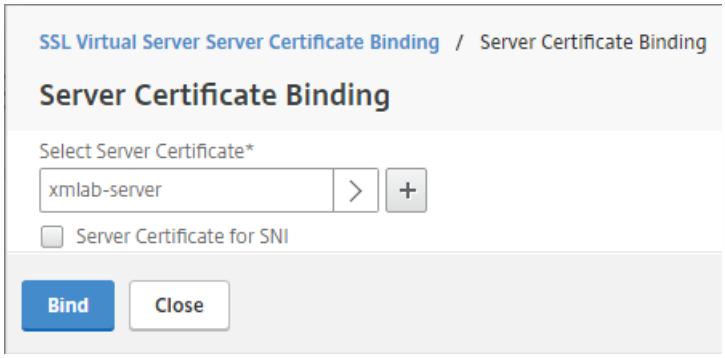
14. Sous **Server Certificate Binding**, cliquez sur **Click to Select**.

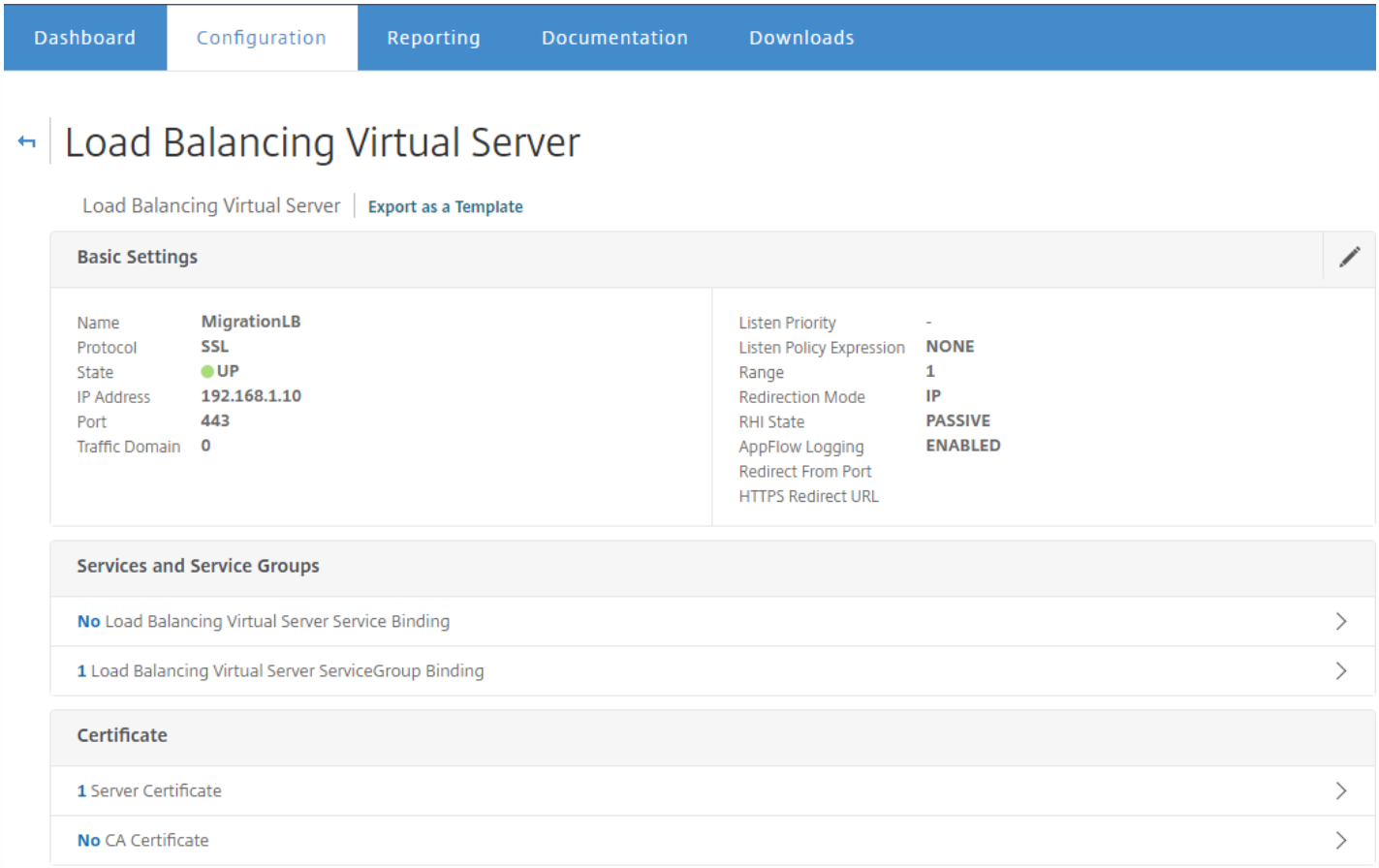


15. Sous **Certificates**, cliquez sur le certificat de serveur XenMobile 9.0 que vous avez exporté dans Prérequis pour l'outil de mise à niveau et cliquez sur **OK**.

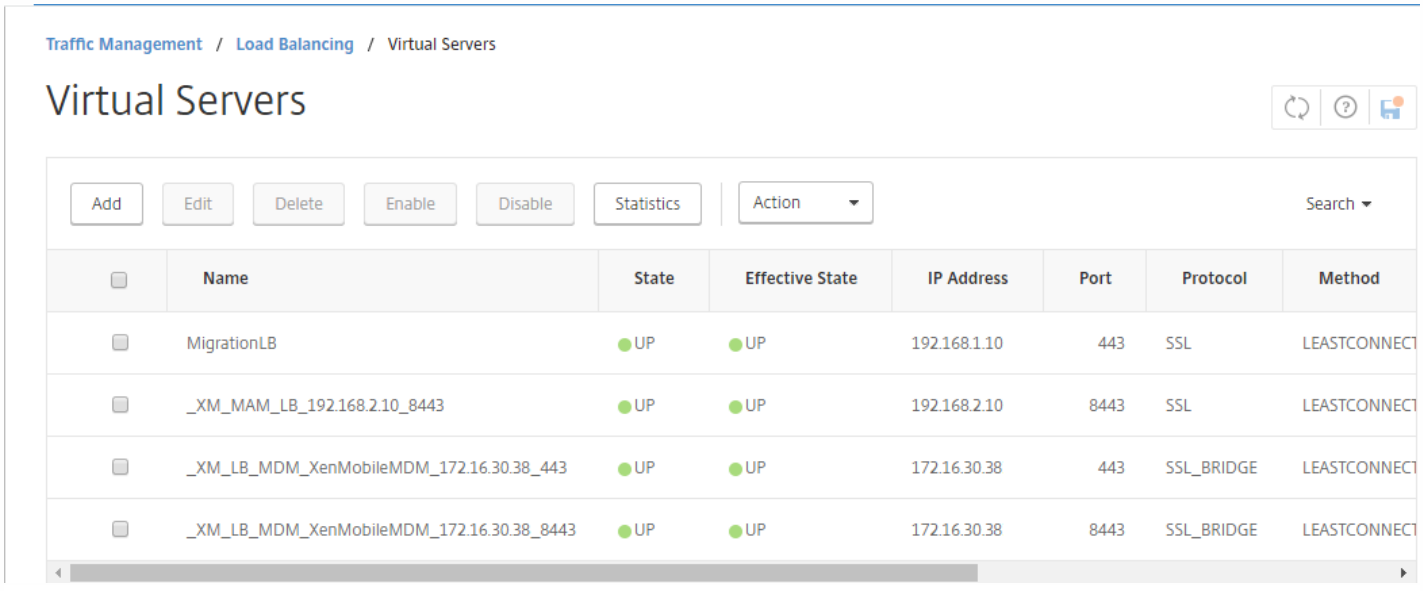


16. Cliquez sur **Bind**, puis sur l'écran suivant, cliquez sur **Done**.





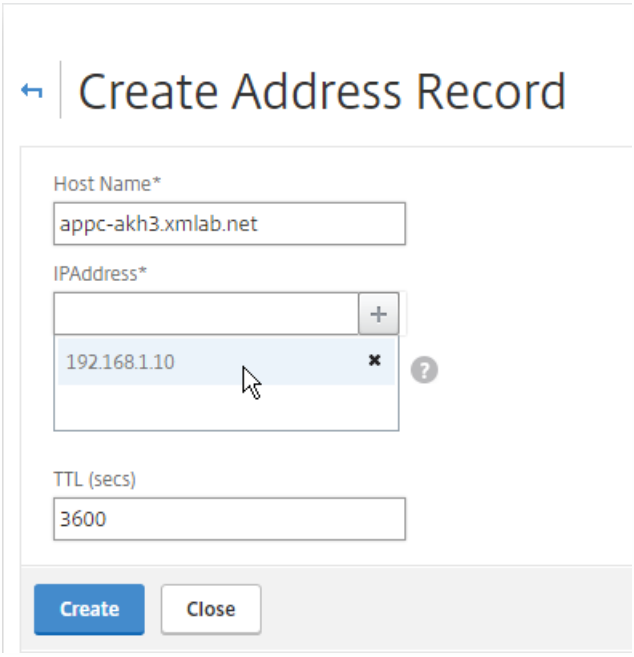
17. Cliquez sur le bouton d'actualisation pour confirmer que le serveur est en fonctionnement.



Configurer un enregistrement d'adresse pour pointer le nom de domaine complet du serveur App Controller vers le nouvel équilibrage de charge pour la mise à niveau

1. Ouvrez une session sur NetScaler, cliquez sur **Traffic Management > DNS > Records > Address Records**, puis cliquez sur **Add**.

> **Remarque**
>
> Si vous disposez d'une configuration d'équilibrage de charge de serveur global, l'ajout d'un enregistrement d'adresse entraîne une réponse faisant autorité du système d'équilibrage de charge du serveur global pour le serveur avec l'adresse IP locale.



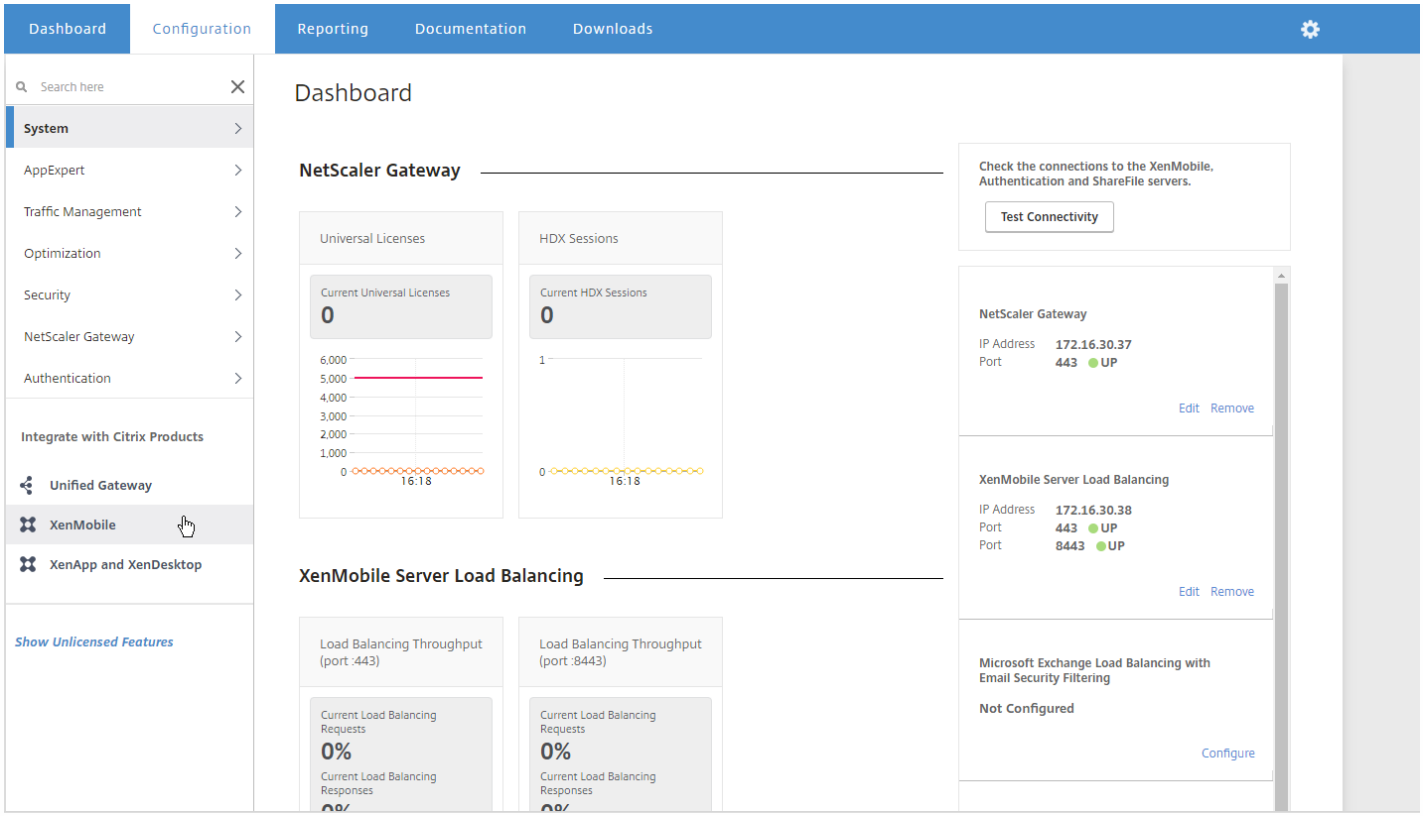
Changez le serveur virtuel d'équilibrage de charge de Device Manager pour pointer vers la nouvelle adresse IP du serveur XenMobile

Si vous avez déployé le serveur exécutant XenMobile 9.0 derrière un boîtier d'équilibrage de charge NetScaler, vous devez configurer l'instance d'équilibrage de charge XenMobile 9.0 Device Manager dans NetScaler avec la nouvelle adresse IP pour le serveur XenMobile 10.4.

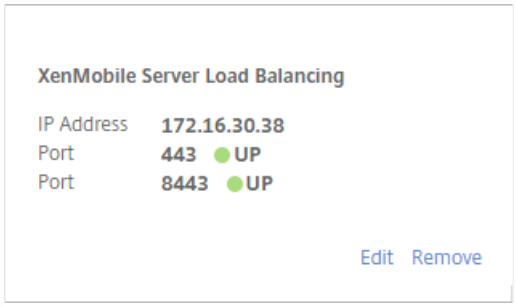
La procédure diffère selon que vous utilisez NetScaler 11.1 ou NetScaler versions 11.0 ou 10.5.

Pour NetScaler 11.1

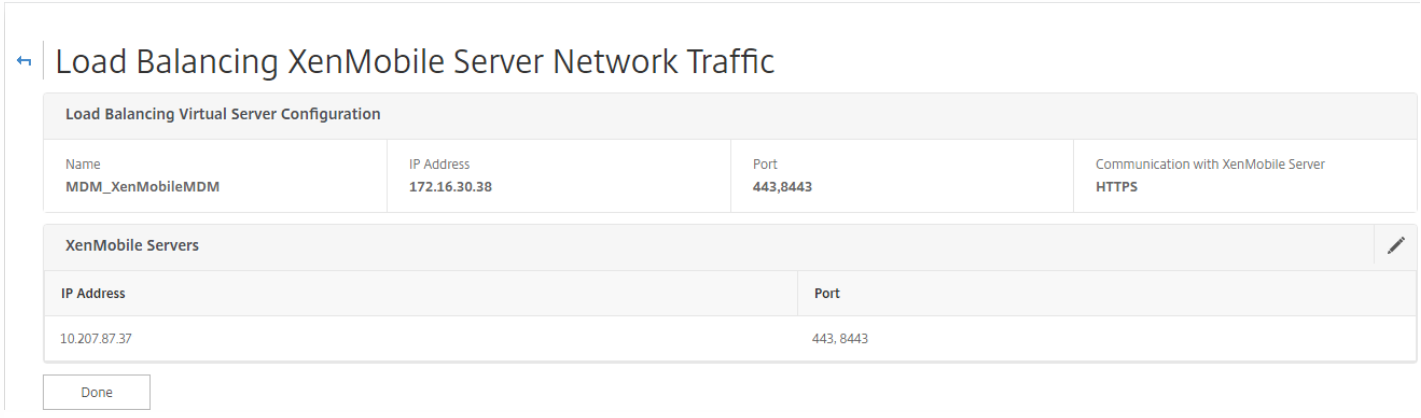
1. Sous **Integrate with Citrix Products**, cliquez sur **XenMobile**.



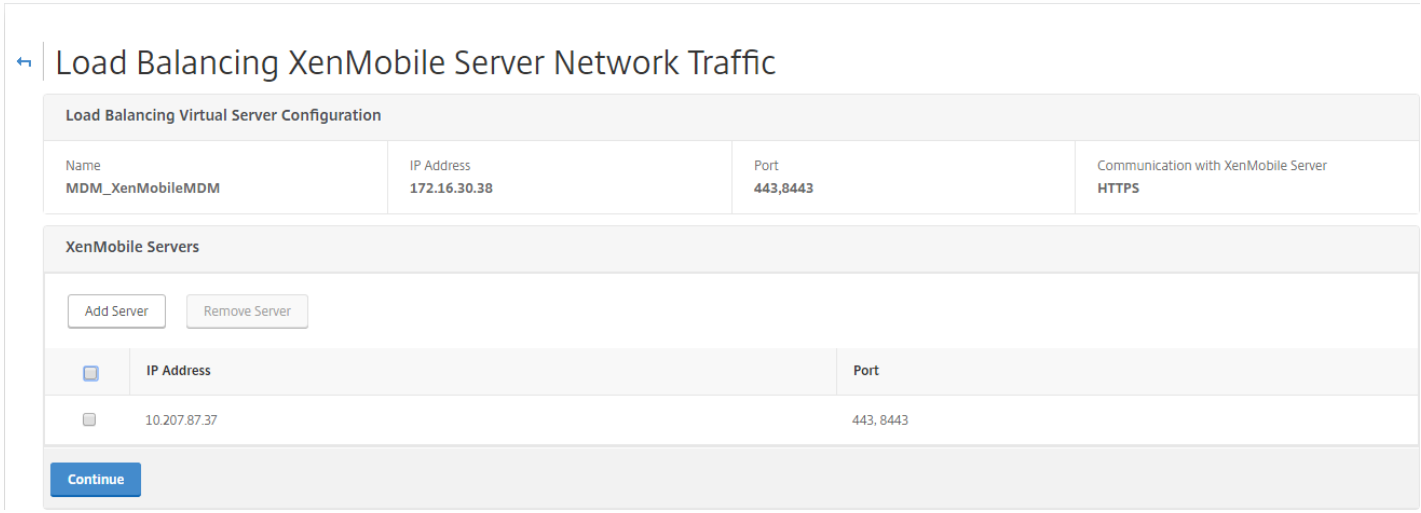
2. Dans la partie droite de l'écran, sous **XenMobile Server Load Balancing**, cliquez sur **Edit**.



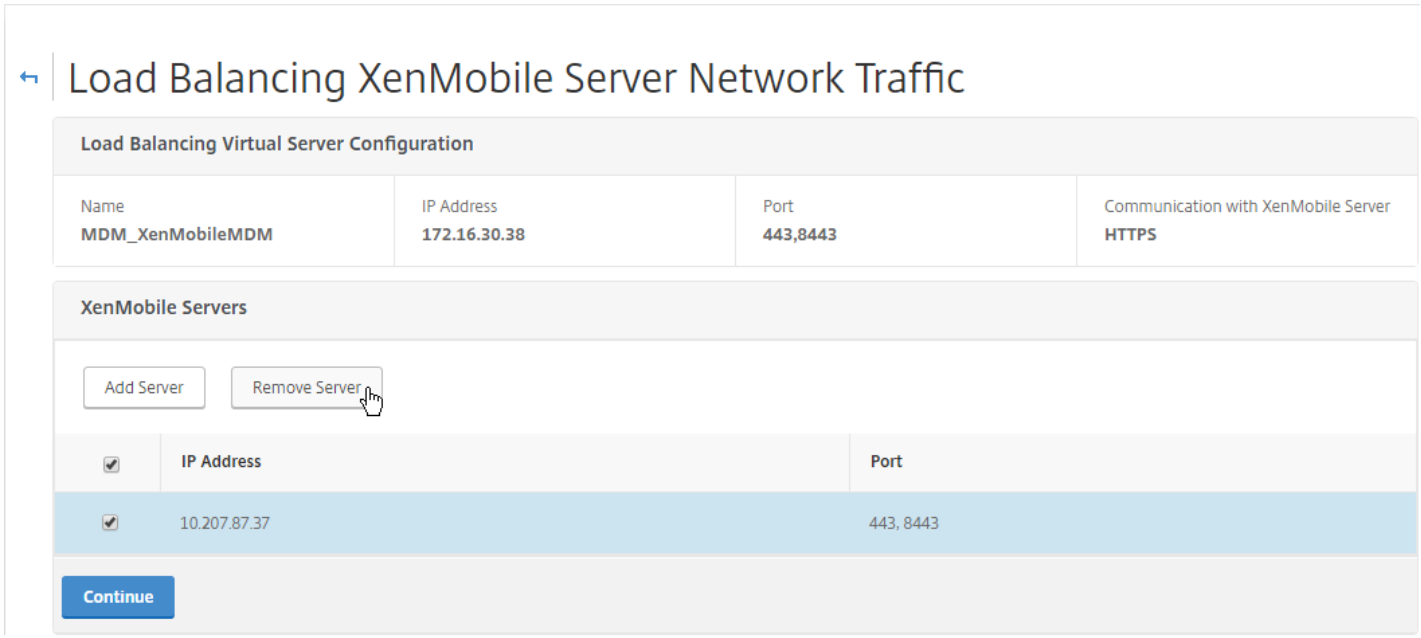
La page **Load Balancing XenMobile Server Network Traffic** apparaît.



3. Cliquez sur l'icône de stylo pour les serveurs XenMobile pour ouvrir ces paramètres.



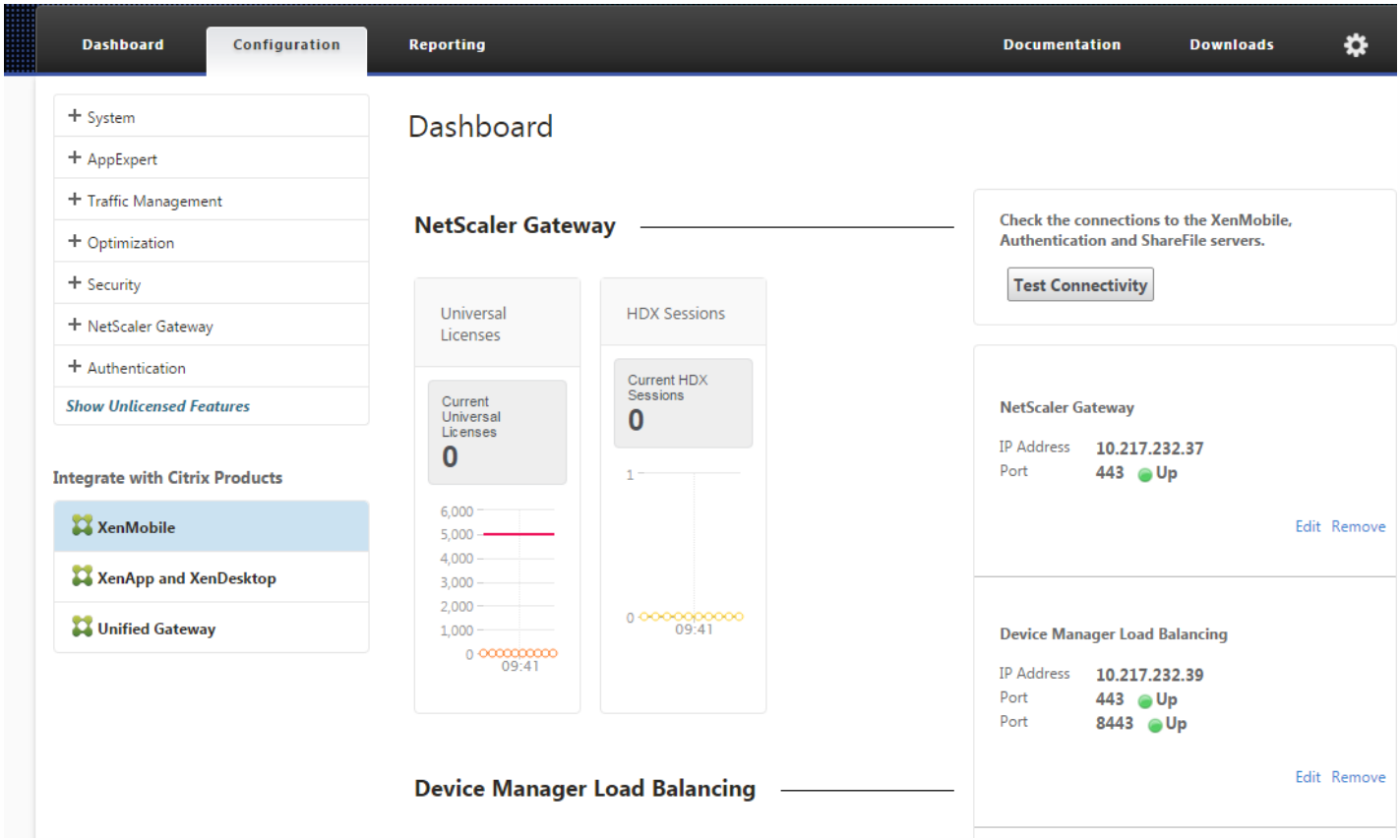
4. Sélectionnez l'adresse IP du serveur Device Manager 9.0 et cliquez sur **Remove Server**.



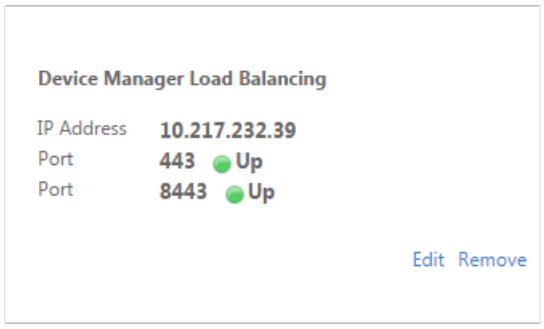
5. Cliquez sur **Add Server** et ajoutez l'adresse IP du nouveau serveur XenMobile 10.4.

Pour les versions de NetScaler 11.0 ou 10.5

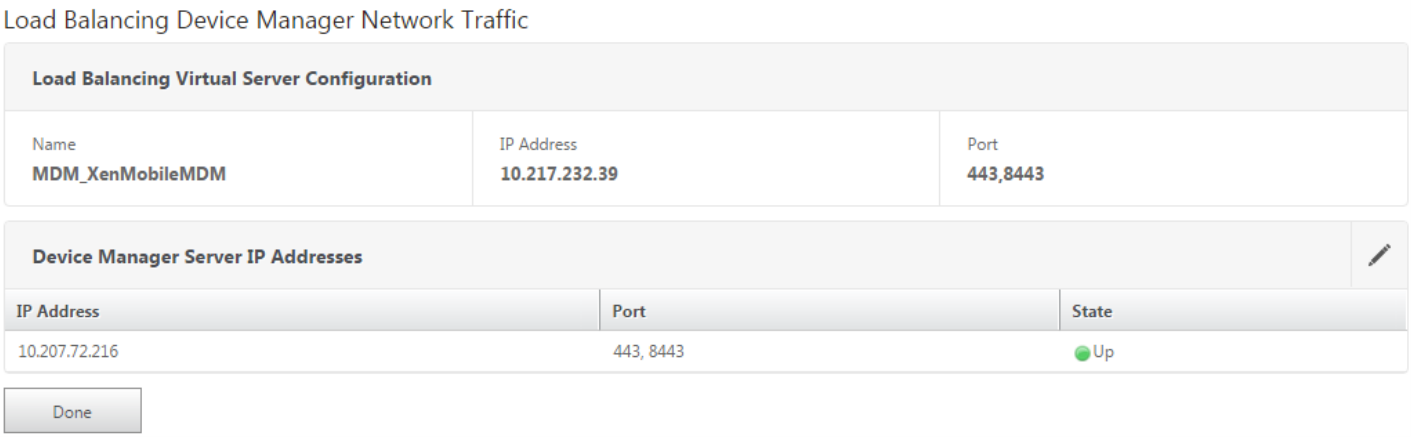
1. Sous **Integrate with Citrix Products**, cliquez sur **XenMobile**.



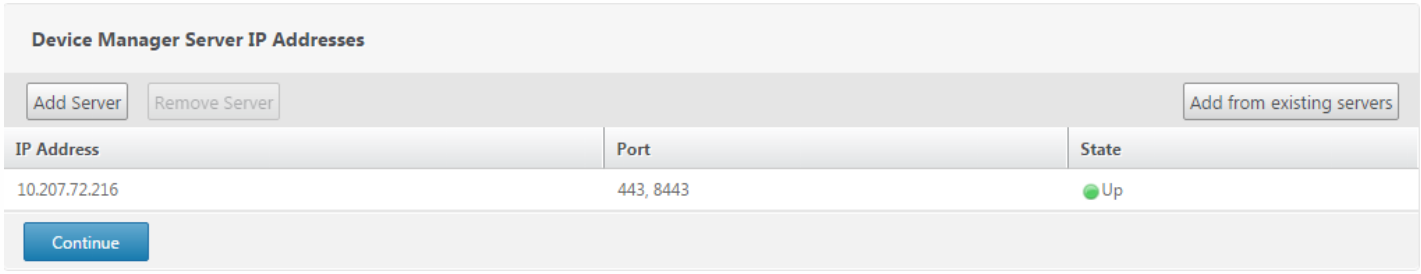
2. Dans la partie droite de l'écran, sous **Device Manager Load Balancing**, cliquez sur **Edit**.



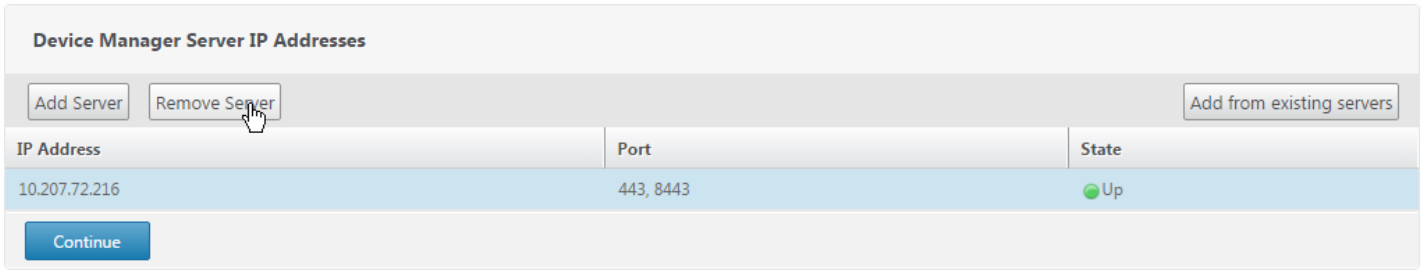
La page **Load Balancing Device Manager Network Traffic** apparaît.



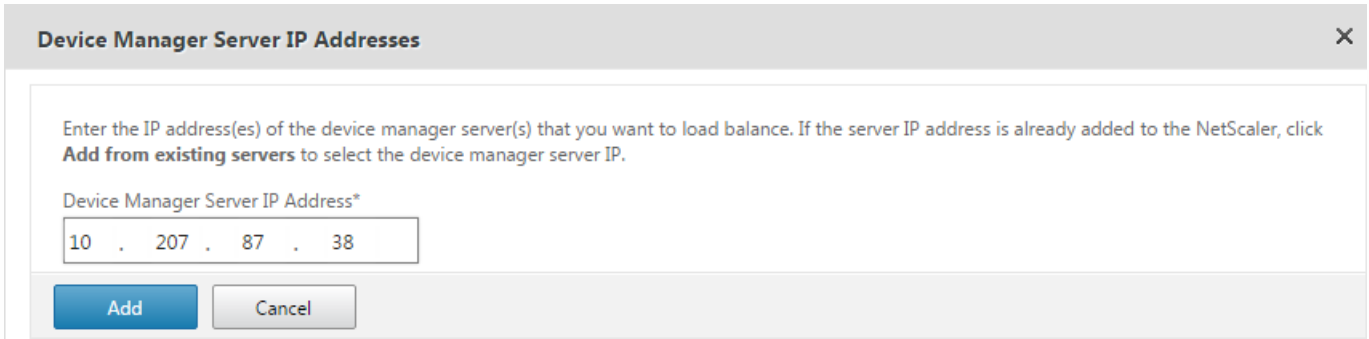
3. Cliquez sur l'icône de stylo pour **Device Manager Server IP Addresses** pour ouvrir ces paramètres.



4. Sélectionnez l'adresse IP du serveur Device Manager 9.0 et cliquez sur **Remove Server**.



5. Cliquez sur **Add Server** et ajoutez l'adresse IP du nouveau serveur XenMobile 10.4.



Changer NetScaler Gateway pour pointer vers le nouveau nom de domaine complet du serveur XenMobile

À ce stade, NetScaler Gateway pointe vers le nom de domaine complet d'App Controller. Vous devez modifier NetScaler pour pointer vers le nouveau nom de domaine complet de XenMobile 10.4. XenMobile 10.4 écoute sur le port 8443 plutôt que sur le port 443. Si vous avez utilisé l'assistant NetScaler pour XenMobile 9 pour configurer votre NetScaler, vous devez inclure le numéro de port avec le nom de domaine complet (FQDN), comme illustré dans les exemples figurant dans les tableaux suivants.

XenMobile Enterprise Edition

Modifiez le nom de domaine complet d'App Controller de manière à pointer vers le nouveau nom de domaine complet de XenMobile 10.4, qui est le nom de domaine complet de XenMobile 9.0 Device Manager suivi du port 8443. Le tableau suivant présente un exemple.

XenMobile 9,0 Composant	**Nom de domaine complet du composant**	**XenMobile 10.4 Enterprise Nom de domaine complet de l'édition**
Device Manager	enroll.example.com	enroll.example.com:8443
App Controller	appc.example.net	S.O.
NetScaler Gateway	access.example.com	S.O.

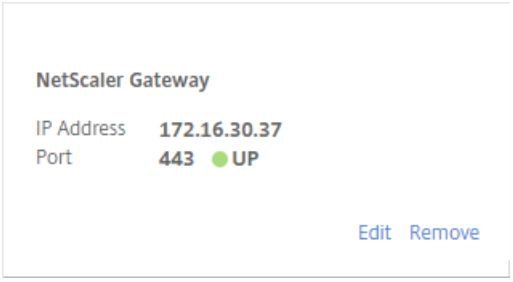
XenMobile App Edition

Modifiez le nom de domaine complet d'App Controller de manière à pointer vers le nouveau nom de domaine complet de XenMobile 10.4, à savoir le nom de domaine complet de XenMobile 9.0 App Controller suivi du port 8443. Le tableau suivant présente un exemple.

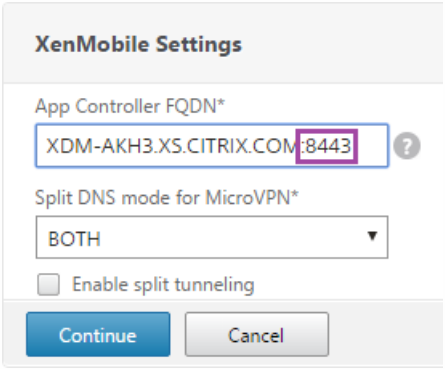
XenMobile 9,0 Composant	**Nom de domaine complet du composant**	**XenMobile 10.4 Enterprise Nom de domaine complet de l'édition**
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	S.O.

1. Sous **Integrate with Citrix Products**, cliquez sur **XenMobile**.

2. Sous **NetScaler Gateway**, cliquez sur **Edit**.



3. Cliquez sur l'icône de crayon à côté de **XenMobile Settings**, puis remplacez le nom de domaine complet d'App Controller par le nom de domaine complet du serveur XenMobile et ajoutez **:8443** au nom de domaine complet. Par exemple, ***EXEMPLE-XENMOBILE.FQDN*.COM:8443**.



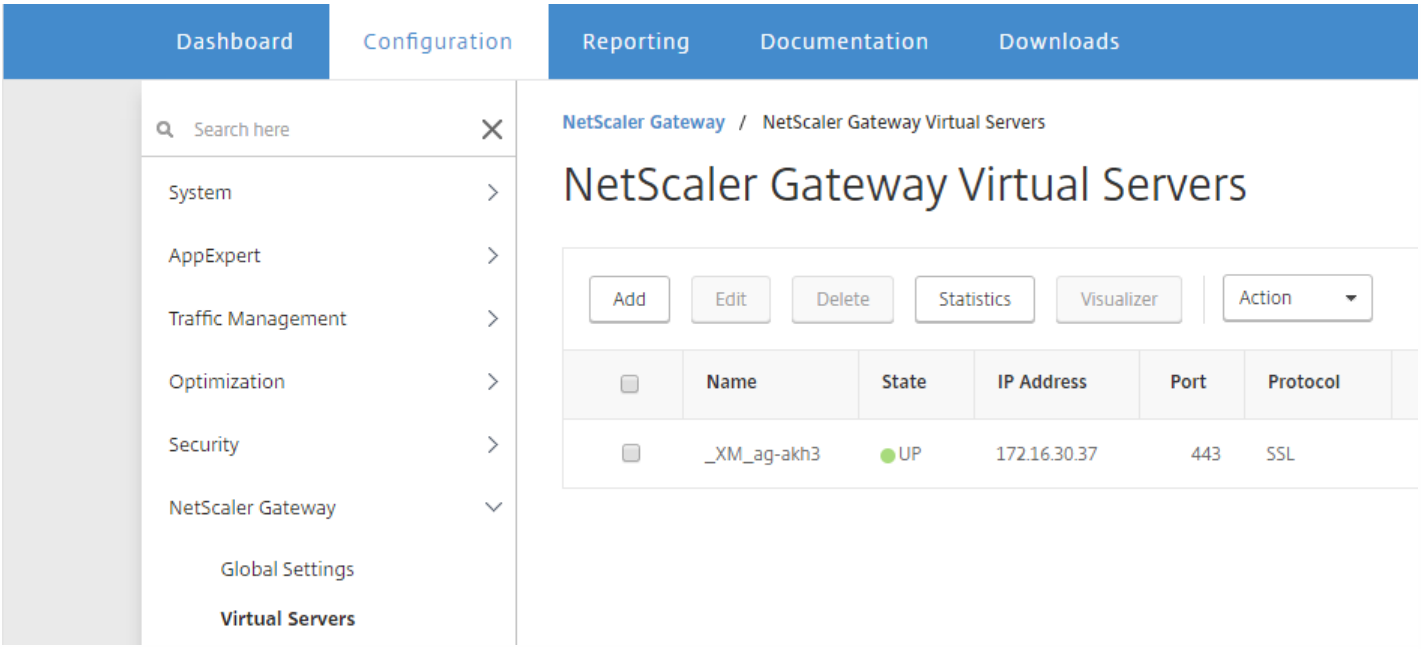
4. Cliquez sur **Continue** et **Finish**.

Ajouter l'adresse IP ou le nom de domaine complet du serveur exécutant la Secure Ticket Authority (STA)

Ensuite, vous devez mettre à jour votre DNS pour résoudre le nom de domaine complet du serveur exécutant la Secure Ticket Authority sur l'adresse IP du serveur XenMobile 10.4. Parfois, une fois que les étapes requises après la mise à niveau ont été effectuées, le serveur Secure Ticket Authority n'est pas lié dans NetScaler, bien qu'il apparaisse dans la liste **VPN Virtual Server STA Server Binding**.

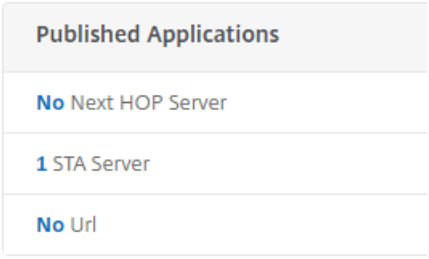
Dans NetScaler Gateway, vous ajoutez l'adresse IP ou le nom de domaine complet du serveur exécutant la Secure Ticket Authority, comme suit :

1. Cliquez sur **Netscaler Gateway > Virtual Servers**.

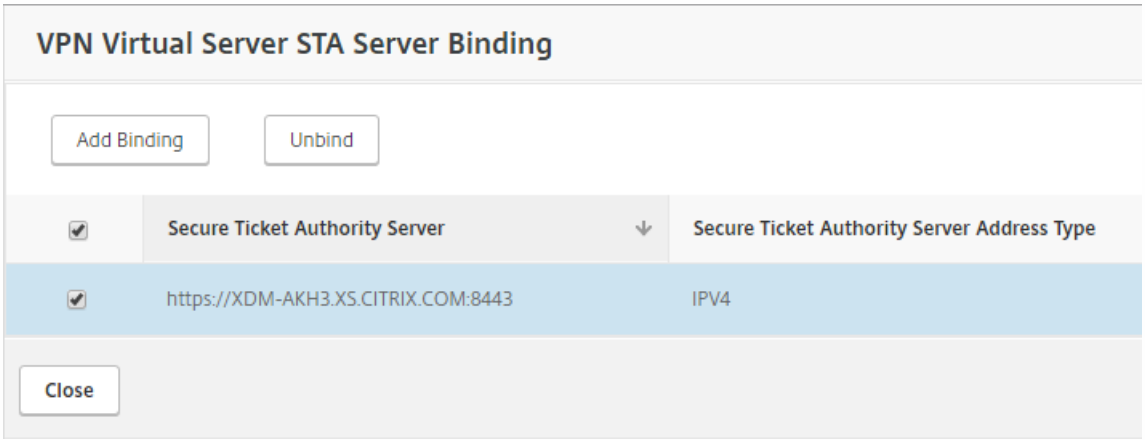


2. Assurez-vous que le serveur virtuel NetScaler Gateway est à l'état **Up**. Sélectionnez la configuration du serveur virtuel NetScaler Gateway, puis cliquez sur **Edit**.

3. Sous **Published Applications**, cliquez sur **STA server**.



4. Notez l'URL de **Secure Ticket Authority Server**, vous l'utiliserez à l'étape 6. Sélectionnez ensuite le serveur Secure Ticket Authority dans la liste.



5. Cliquez sur **Unbind** , puis cliquez sur **Add Binding**.

6. Dans le champ **Secure Ticket Authority Server**, tapez l'URL notée à l'étape 4.

7. Cliquez sur **Bind**, sur **Close**, puis sur **Done**.

Paramètres NTP

Assurez-vous que l'heure de NetScaler est synchronisée avec celle du serveur XenMobile. Si possible, pointez NetScaler et le serveur XenMobile vers le même serveur NTP.

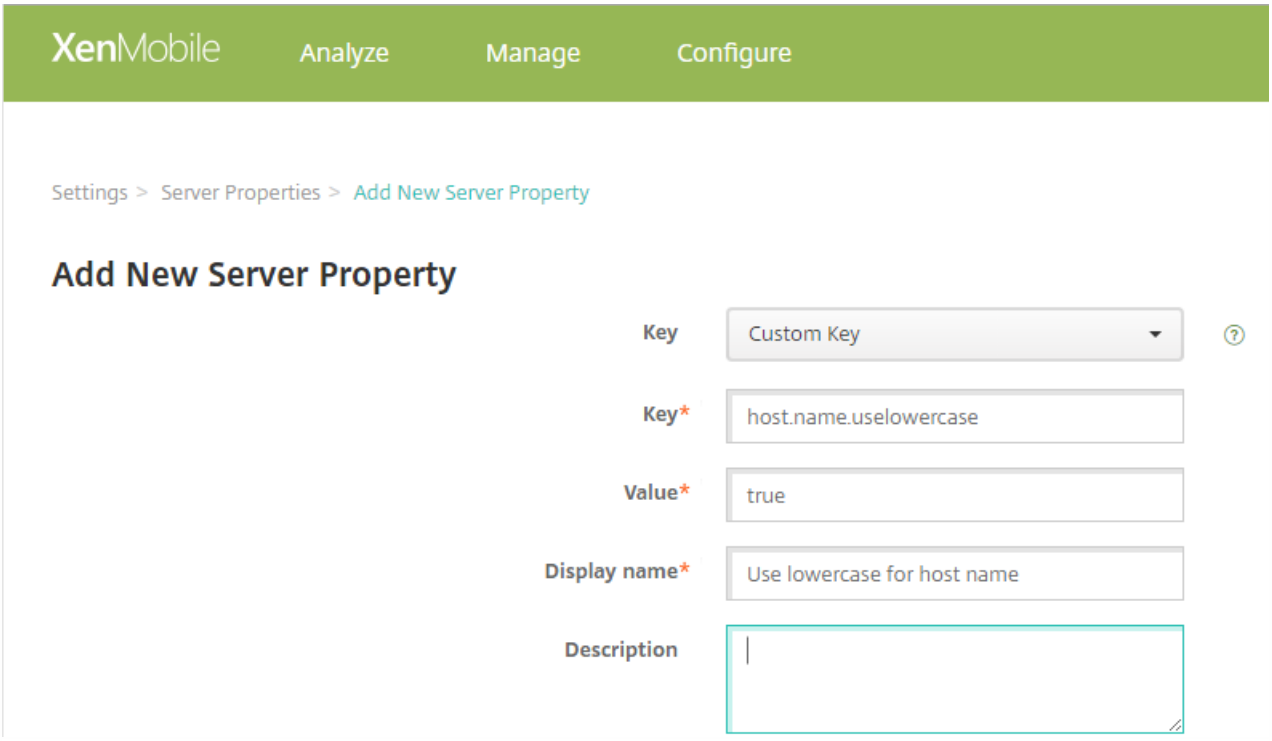
Propriété du serveur si votre nom d'hôte XenMobile 9.0 contient des lettres majuscules

Si votre nom d'hôte XenMobile 9.0 comporte des lettres majuscules, effectuez les étapes suivantes afin que les appareils mobiles puissent accéder à Citrix Store :

1. Dans la console XenMobile 10.4, accédez à **Paramètres > Propriétés du serveur**.

2. Cliquez sur **Ajouter**, puis remplissez les champs comme suit :

- **Clé** : sélectionnez **Clé personnalisée**.
- **Clé** : entrez **host.name.uselowercase**.
- **Valeur** : entrez **true**.
- **Nom d'affichage** : entrez une description pour la clé.



3. Redémarrez le serveur XenMobile.

Mettre à jour les informations qui n'ont pas été mises à niveau

Mettez à jour les informations suivantes, selon les besoins :

- Groupe de fournisseurs de services gérés (MSP)
- Attributs Active Directory personnalisés

- Rôles RBAC
  Avec une mise à niveau locale, des paramètres RBAC rencontrent des problèmes. Pour plus d'informations, veuillez consulter la section Problèmes connus.

- Paramètres de journal
- Toutes les données de configuration ou d'utilisateur répertoriées dans le fichier migration.log
- Toutes les configurations de serveur Syslog

Nom de magasin personnalisé

Avant la mise à niveau, l'une des étapes consistait à rétablir la valeur par défaut du nom de magasin Citrix personnalisé. Si vous n'avez pas suivi cette étape, vous devez suivre l'une des étapes suivantes avant d'utiliser XenMobile Server 10.4 :

- Si vous avez un grand nombre d'appareils Windows, définissez le nom du magasin sur la valeur par défaut. Ensuite, les utilisateurs finaux inscrits avec des appareils iOS et Android doivent se déconnecter de Citrix Secure Hub (précédemment Worx Home), puis se connecter à nouveau.
- Si le nombre d'appareils Windows est inférieur au nombre d'appareils iOS et Android, il est recommandé que les utilisateurs Windows réinscrivent leurs appareils.

Pour de plus amples informations sur ce problème, veuillez consulter l'article http://support.citrix.com/article/CTX214553.

Inscription d'appareils XenMobile après la mise à niveau

Les utilisateurs n'ont pas besoin de réinscrire leurs appareils après une mise à niveau de production vers XenMobile 10.4. Les appareils doivent se connecter automatiquement au serveur XenMobile 10,4 en fonction de l'intervalle de pulsation. Les utilisateurs peuvent toutefois être invités à s'authentifier à nouveau avant que l'appareil puisse se reconnecter.

Une fois les appareils des utilisateurs connectés, vérifiez que les appareils sont affichés dans la console XenMobile, comme l'illustre la figure suivante.

Mettre à niveau le serveur locataire de la console MTC vers XenMobile 10.4

Feb 23, 2017

Si la Multi-Tenant Console (MTC) est activée sur XenMobile 9.0 MDM ou Enterprise Edition, vous pouvez migrer les instances de XenMobile 9 gérées par MTC vers des instances XenMobile 10.4 autonomes. XenMobile 10 ne prend pas en charge la MTC, c'est la raison pour laquelle vous devez gérer ces instances mises à niveau individuellement.

1. Configurez la traduction d'adresses réseau (NAT) devant tous les clients MTC.

2. Installez une instance de XenMobile 10,4.

3. Si aucun mappage de port n'est activé sur le locataire MTC, procédez comme suit :

    a. Assurez-vous que le port du serveur XenMobile 10,4 qui autorise les communications HTTPS avec certificats (généralement le port 443) et sans certificats (8443) correspond au port utilisé pour l'instance de XenMobile.

    b. Configurez un nouveau port pour la gestion.

    c. Une fois le mappage de port activé, utilisez le port mappé et non le port utilisé par le serveur XenMobile pour l'écoute.

4. Durant le démarrage du serveur XenMobile, utilisez le nom de l'instance, **zdm**.

5. Lorsque vous activez l'outil de mise à niveau à l'aide de l'interface de ligne de commande XenMobile, vous devez répondre par **Oui** à l'invite de mise à niveau.

6. Depuis le serveur à partir duquel vous effectuez la mise à niveau, copiez les fichiers suivants depuis C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\webapps\tenant-name\WEB-INF\classes :

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

7. Copiez les fichiers suivants depuis : C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant name

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

8. Effectuez une copie de C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml et effectuez les modifications indiquées dans les étapes suivantes.

9. Supprimez tous les connecteurs de port utilisés par l'autre locataire dans le fichier server.xml, sauf le port 80.

10. Sur le connecteur de port utilisé, supprimez le nom de l'instance de tous les chemins d'accès aux fichiers dans la plage suivante :

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\https.p12"

sur :

keystoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\https.p1"

11. Répétez l'étape 10 pour les chemins d'accès aux fichiers de :

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\tenant-name\cacerts.pem.jks"

sur :

truststoreFile="C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\cacerts.pem.jks"

12. Créez un fichier .zip avec les fichiers que vous avez copiés aux étapes 6 à 8.

13. Ouvrez l'adresse IP du serveur XenMobile 10.4, comme suit : https://*adresseIP:port*/uw/?cloudMode, où *port* est la connexion HTTPS avec un certificat. L'assistant de mise à niveau s'affiche.

14. À l'aide de la procédure décrite dans l'assistant de mise à niveau, sélectionnez **MDM** ou **Enterprise**.

Pour les mises à niveau **MDM**, l'assistant vous invite à charger le fichier .zip. Vous devez également vérifier que la base de données est correcte et entrer le mot de passe pour le certificat d'autorité de certification.

Pour les mises à niveau **Enterprise** , l'assistant vous invite à télécharger le pack de support pour App Controller.

15. Après le redémarrage du serveur XenMobile, connectez-vous à la console XenMobile en utilisant l'adresse IP de votre serveur XenMobile, suivi du numéro de port de gestion.

16. Changez la traduction d'adresses réseau afin de pointer vers un nouveau serveur.

17. Apportez les modifications nécessaires au pare-feu afin d'autoriser les ports utilisés par le serveur XenMobile.

Comptes utilisateur, rôles et inscription

Mar 31, 2017

Dans XenMobile, vous configurez des comptes d'utilisateurs et des groupes et des rôles pour les comptes d'utilisateurs et les groupes. Vous configurez également les invitations et le mode d'inscription. Vous configurez ces paramètres dans la console XenMobile, sur l'onglet **Gérer** et la page **Paramètres**.

À partir de l'onglet **Gérer**, vous pouvez effectuer les opérations suivantes :

- Cliquez sur **Utilisateurs** pour ajouter des comptes utilisateur manuellement ou utilisez un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux. Pour plus de détails, consultez :
  - Pour ajouter, modifier ou supprimer des comptes utilisateur locaux
  - Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv et formats des fichiers de provisioning
  - Pour ajouter ou supprimer des groupes dans XenMobile

  Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes d'utilisateur, comme décrit plus loin dans cet article dans la section Créer et gérer des workflows.

- Cliquez sur **Inscription** pour configurer jusqu'à sept modes. Chaque mode dispose de son propre niveau de sécurité et d'étapes que les utilisateurs doivent suivre pour inscrire leurs appareils, et pour envoyer des invitations d'inscription. Pour plus de détails, consultez :
  - Pour configurer des modes d'inscription et activer le portail en libre-service
  - Activer la détection automatique pour l'inscription utilisateur dans XenMobile

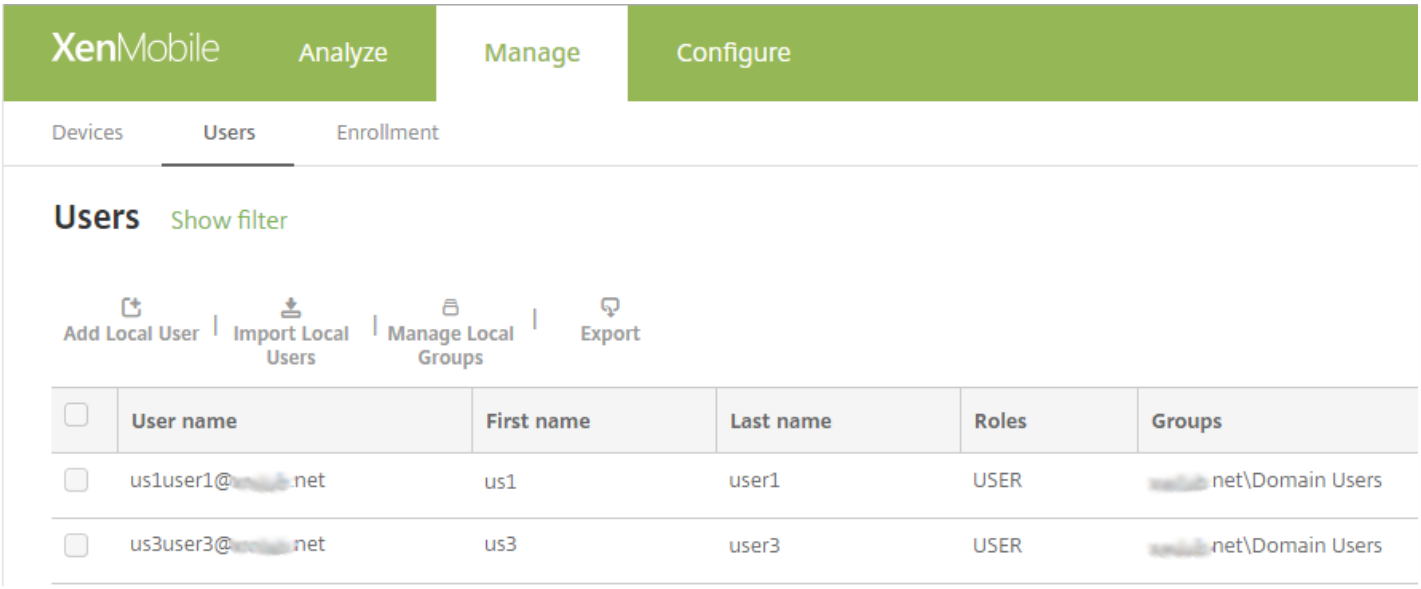
Depuis la page **Paramètres**, vous pouvez effectuer ce qui suit :

- Cliquez sur **Contrôle d'accès basé sur rôle** pour attribuer des rôles prédéfinis ou des ensembles d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système. Pour plus de détails, consultez :
  - Configuration de rôles avec RBAC
- Cliquez sur les **Modèles de notification** à utiliser dans les actions automatisées, l'inscription et les messages de notification standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Secure Hub, SMTP ou SMS. Pour plus de détails, consultez :
  - Création et mise à jour de modèles de notification

Pour ajouter, modifier ou supprimer des comptes utilisateur

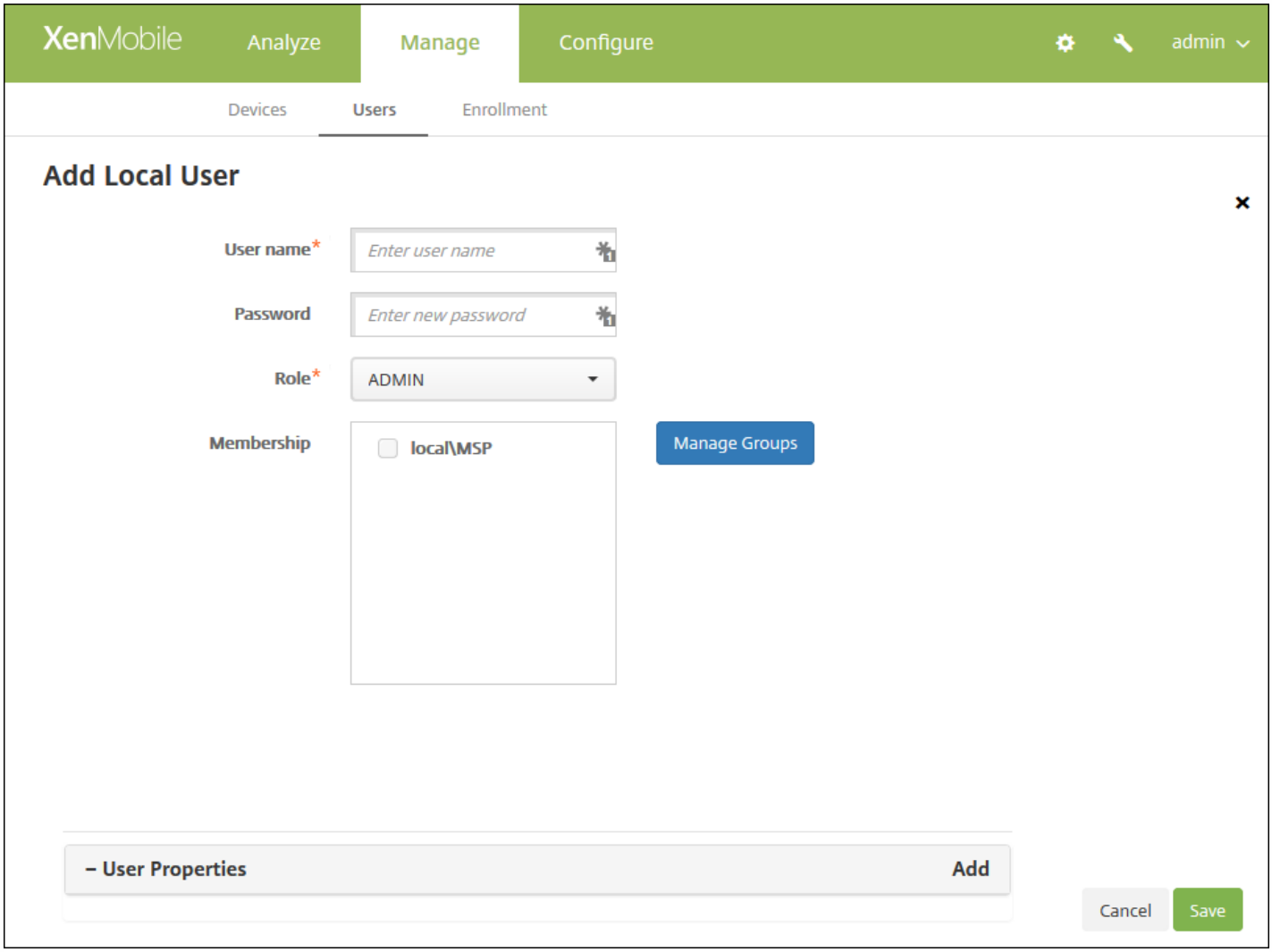
Vous pouvez ajouter des comptes d'utilisateur locaux à XenMobile manuellement ou vous pouvez utiliser un fichier de provisioning pour importer les comptes. Consultez la section Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv pour la procédure d'importation de comptes utilisateur à partir d'un fichier de provisioning.

1. Dans la console XenMobile, cliquez sur **Gérer** > **Utilisateurs**. La page **Utilisateurs** s'affiche.



Pour ajouter un compte d'utilisateur local

1. Sur la page **Utilisateurs**, cliquez sur **Ajouter un utilisateur local**. La page **Ajouter un utilisateur local** s'affiche.

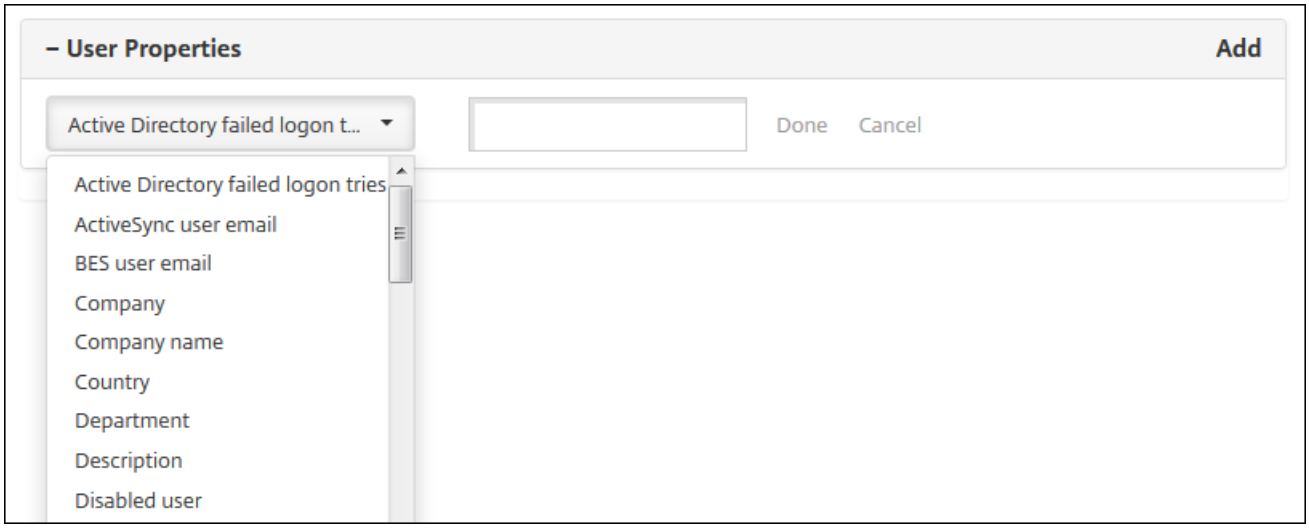


2. Pour configurer ces paramètres :

- **Nom d'utilisateur** : entrez le nom d'utilisateur. Ce champ est obligatoire. Le nom peut contenir des espaces ainsi que des majuscules et des minuscules.
- **Mot de passe** : entrez un mot de passe utilisateur (facultatif).
- **Rôle** : dans la liste, cliquez sur le rôle utilisateur. Pour plus d'informations concernant les rôles, veuillez consulter la section Configuration de rôles avec RBAC. Les options possibles sont les suivantes :
  - ADMIN
  - DEVICE_PROVISIONING
  - SUPPORT
  - USER
- **Adhésion** : dans la liste, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur.
- **Propriétés utilisateur** : ajoutez des propriétés utilisateur (facultatif). Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Propriétés utilisateur** : dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
  - Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler** pour annuler l'opération.

Remarque : pour supprimer une propriété utilisateur existante, placez le curseur sur la ligne contenant la propriété et cliquez sur le X sur le côté droit. La propriété est immédiatement supprimée.

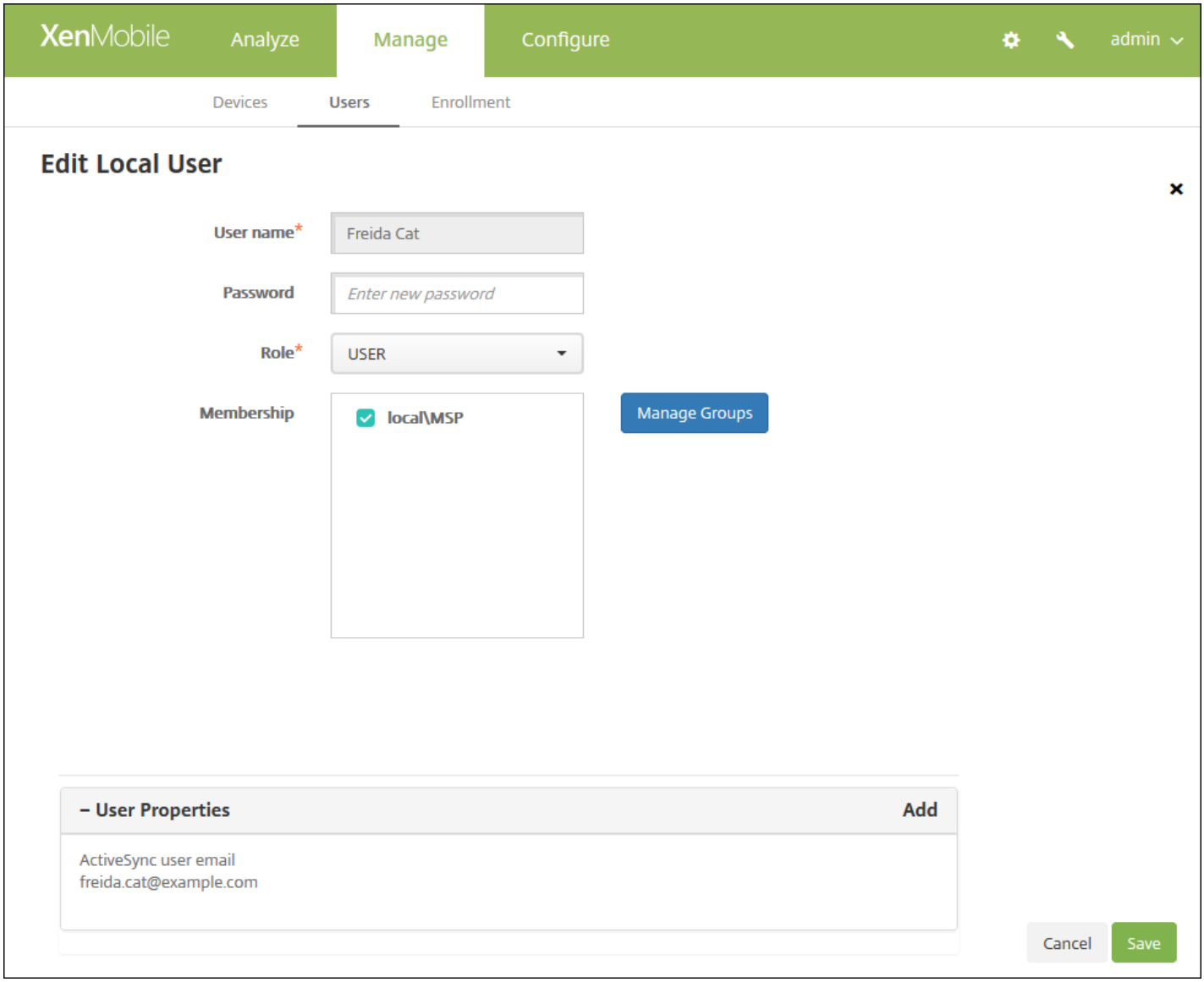
Pour modifier une propriété utilisateur, cliquez sur la propriété et effectuez les modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.



3. Cliquez sur **Enregistrer**.

Pour modifier un compte d'utilisateur local

1. 1. Sur la page **Utilisateurs**, dans la liste des utilisateurs, cliquez pour sélectionner un utilisateur, puis cliquez sur **Modifier**. La page **Modifier un utilisateur local** apparaît.



2. Modifiez les informations suivantes le cas échéant :

- **Nom d'utilisateur** : vous ne pouvez pas modifier le nom d'utilisateur.
- **Mot de passe** : modifiez ou ajoutez un mot de passe utilisateur.
- **Rôle** : dans la liste, cliquez sur le rôle utilisateur.
- **Adhésion** : dans la liste, cliquez sur le groupe ou les groupes pour lesquels ajouter ou modifier le compte utilisateur. Pour supprimer le compte utilisateur d'un groupe, désactivez la case à cocher en regard du nom du groupe.
- **Propriétés utilisateur** : effectuez l'une des opérations suivantes :
  - Pour chaque propriété utilisateur que vous voulez modifier, cliquez sur la propriété et effectuez des modifications. Cliquez sur **Terminé** pour enregistrer les modifications ou sur **Annuler** pour laisser la propriété inchangée.
  - Pour chaque propriété d'utilisateur que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Propriétés utilisateur** : dans la liste, cliquez sur une propriété, puis entrez l'attribut de la propriété utilisateur dans le champ en regard de la propriété.
    - Cliquez sur **Terminé** pour enregistrer la propriété utilisateur ou cliquez sur **Annuler** pour annuler l'opération.
  - Pour chaque propriété utilisateur que vous souhaitez supprimer, placez le curseur sur la ligne contenant la propriété, puis cliquez sur le X sur le côté droit. La propriété est immédiatement supprimée.

3. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser l'utilisateur inchangé.

Pour supprimer un compte d'utilisateur local

1. Sur la page **Utilisateurs**, dans la liste des comptes utilisateur, cliquez pour sélectionner un compte utilisateur.

Remarque : vous pouvez sélectionner plusieurs comptes utilisateur à supprimer en sélectionnant la case à cocher en regard de chaque compte utilisateur.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.

3. Cliquez sur **Supprimer** pour supprimer le compte utilisateur ou cliquez sur **Annuler** pour ne pas supprimer le compte utilisateur.

Importation de comptes utilisateur

Vous pouvez importer des comptes utilisateur locaux et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

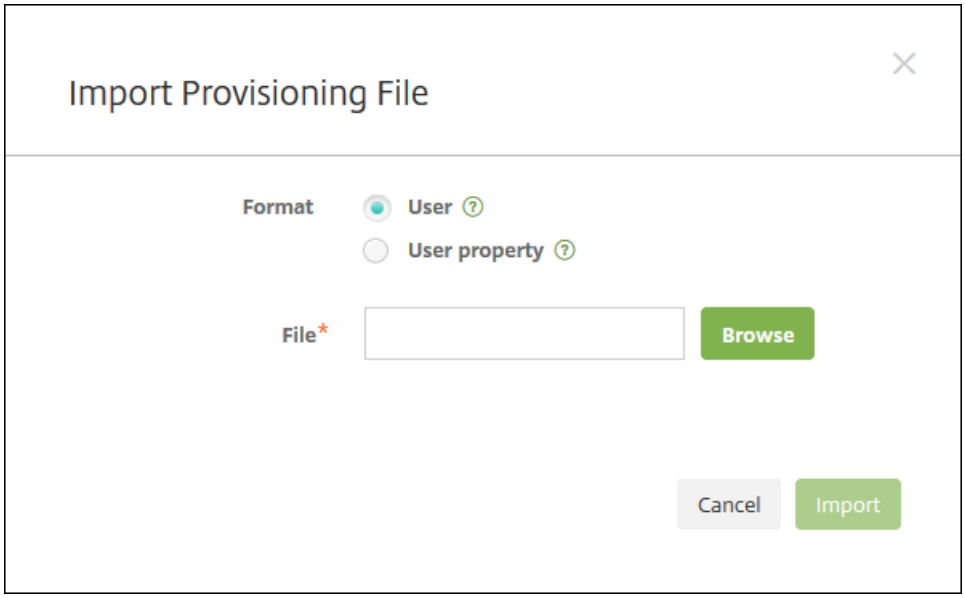
Remarque :

- Pour les utilisateurs locaux, utilisez le nom de domaine ainsi que le nom d'utilisateur du fichier d'importation. Par exemple, spécifiez nomutilisateur@domaine. Lorsque l'utilisateur local que vous créez ou importez dans ce format est destiné à un domaine géré dans XenMobile, tenez compte de ce qui suit. L'utilisateur ne peut pas s'inscrire en utilisant les informations d'identification LDAP correspondantes.
- Lorsque vous importez des comptes utilisateur sur l'annuaire utilisateur interne XenMobile, désactivez le domaine par défaut pour accélérer le processus d'importation. N'oubliez pas que la désactivation du domaine affecte les inscriptions. Par conséquent, vous devez réactiver le domaine par défaut après l'importation des utilisateurs internes.
- Les utilisateurs locaux peuvent être au format « Nom d'utilisateur principal (UPN) », mais nous recommandons de ne pas utiliser le domaine géré. Par exemple, si exemple.com est géré, ne créez pas d'utilisateur local au format UPN : utilisateur@exemple.com.

Lorsque vous préparez un fichier de provisioning, suivez ces étapes pour importer le fichier sur XenMobile.

1. Dans la console XenMobile, cliquez sur **Gérer** > **Utilisateurs**. La page Utilisateurs s'affiche.

2. Cliquez sur **Importer des utilisateurs locaux**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.



3. Sélectionnez **Utilisateur** ou **Propriété** pour le format du fichier de provisioning que vous importez.

4. Sélectionnez le fichier de provisioning à utiliser en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

5. Cliquez sur **Importer**.

Formats des fichiers de provisioning

Un fichier de provisioning que vous créez manuellement et utilisez pour l'importation de comptes utilisateur et de propriétés sur Device Manager doit être dans un des formats suivants :

- **Champs du fichier de provisioning d'utilisateur** : user;password;role;group1;group2
- **Champs du fichier de provisioning d'attribut utilisateur** : user;propertyName1;propertyValue1;propertyName2;propertyValue2

Remarque :

- Les champs dans le fichier de provisioning sont séparés par un point-virgule (;). Si une partie d'un champ contient un point-virgule, elle doit être précédée d'une barre oblique inverse (\). Par exemple, la propriété propertyV;test;1;2 doit être saisie en tant que propertyV\;test\;1\;2 dans le fichier de provisioning.
- Les valeurs valides pour **Role** sont les rôles prédéfinis USER, ADMIN, SUPPORT et DEVICE_PROVISIONING, ainsi que tout autre rôle que vous avez défini.
- Le point (.) est utilisé comme séparateur pour créer la hiérarchie de groupe ; par conséquent, vous ne pouvez pas utiliser de point dans les noms de groupes.
- Les attributs de propriété dans les fichiers de provisioning d'attribut doivent être en minuscules. La base de données est sensible à la casse.

Exemple de contenu de provisioning utilisateur

Cette entrée, user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01, signifie :

- **Utilisateur** : user01
- **Mot de passe** : pwd;01

- **Rôle** : USER
- **Groupes** :
  - myGroup.users01
  - myGroup.users02
  - myGroup.users.users.users01

Dans un autre exemple, AUser0;1.password;USER;ActiveDirectory.test.net, signifie :

- **Utilisateur** : AUser0
- **Mot de passe** : 1.password
- **Rôle** : USER
- **Groupe** : ActiveDirectory.test.net

Exemple de contenu de provisioning d'attribut utilisateur

Cette entrée, user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value, signifie :

- **Utilisateur** : user01
- **Propriété 1**
  - **nom** : propertyN
  - **valeur** : propertyV;test;1;2
- **Propriété 2** :
  - **nom** : prop 2
  - **valeur** : prop2 valeur

Pour configurer des modes d'inscription et activer le portail en libre-service

Vous configurez des modes d'inscription d'appareils pour autoriser les utilisateurs à inscrire leurs appareils dans XenMobile. XenMobile offre sept modes, chacun doté de son propre niveau de sécurité et de ses propres étapes que les utilisateurs doivent suivre pour inscrire leurs appareils. Vous pouvez mettre à disposition certains modes sur le portail en libre-service. Le portail en libre-service est l'emplacement à partir duquel les utilisateurs peuvent ouvrir une session et générer des liens d'inscription. Cela leur permet d'inscrire leurs appareils eux-mêmes ou de s'envoyer une invitation d'inscription. Vous configurez les modes d'inscription dans la console XenMobile sur la page **Paramètres** > **Inscription**.

Vous envoyez des invitations d'inscription depuis la page **Gérer** > **Inscription**. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription.

Remarque : si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.

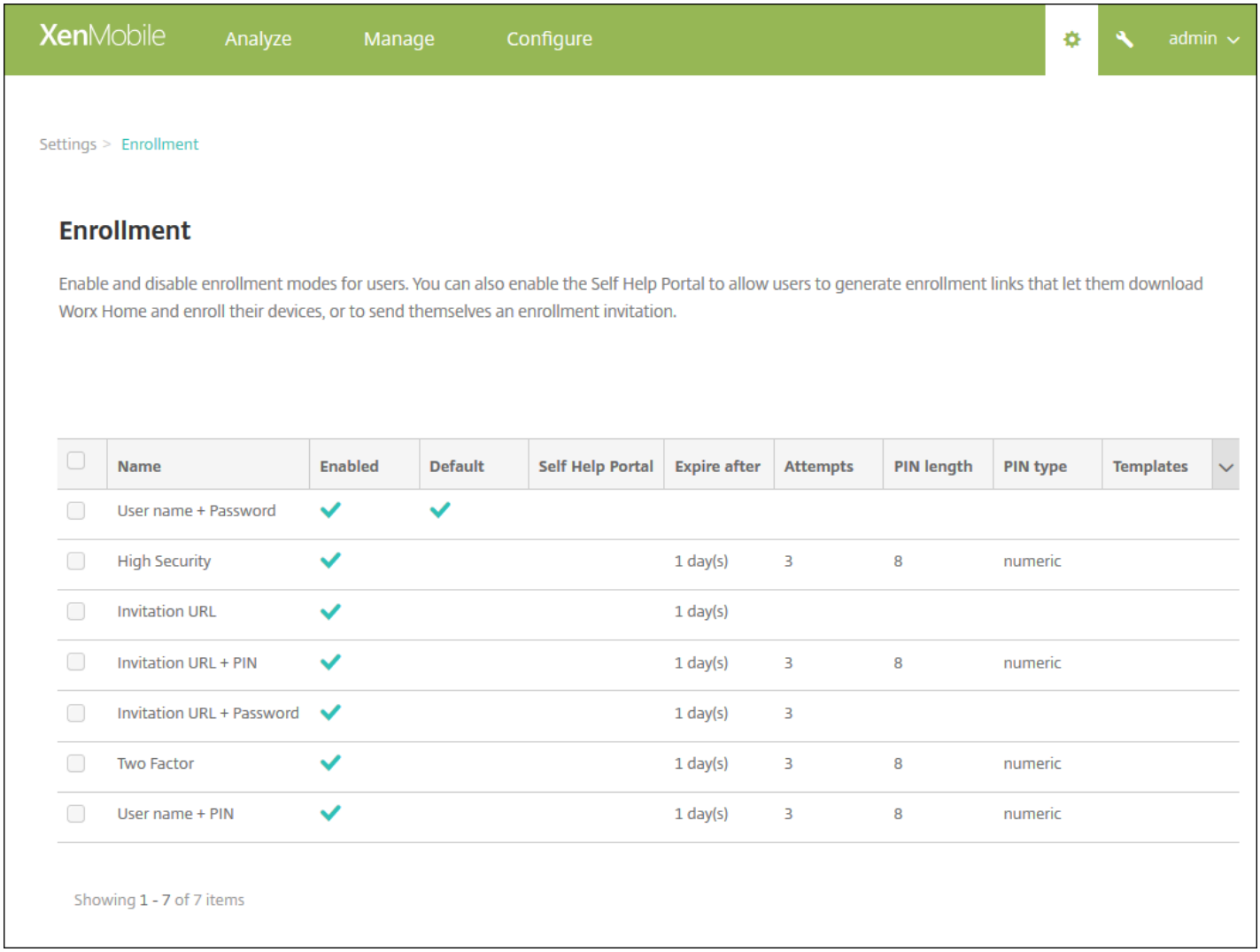
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Inscription**. La page **Inscription** s'affiche. Elle contient un tableau de tous les modes d'inscription disponibles. Par défaut, tous les modes d'inscription sont activés.

3. Sélectionnez un mode d'inscription à modifier dans la liste, puis définissez le mode comme le mode par défaut, désactivez le mode ou autorisez l'accès des utilisateurs via le portail en libre-service.

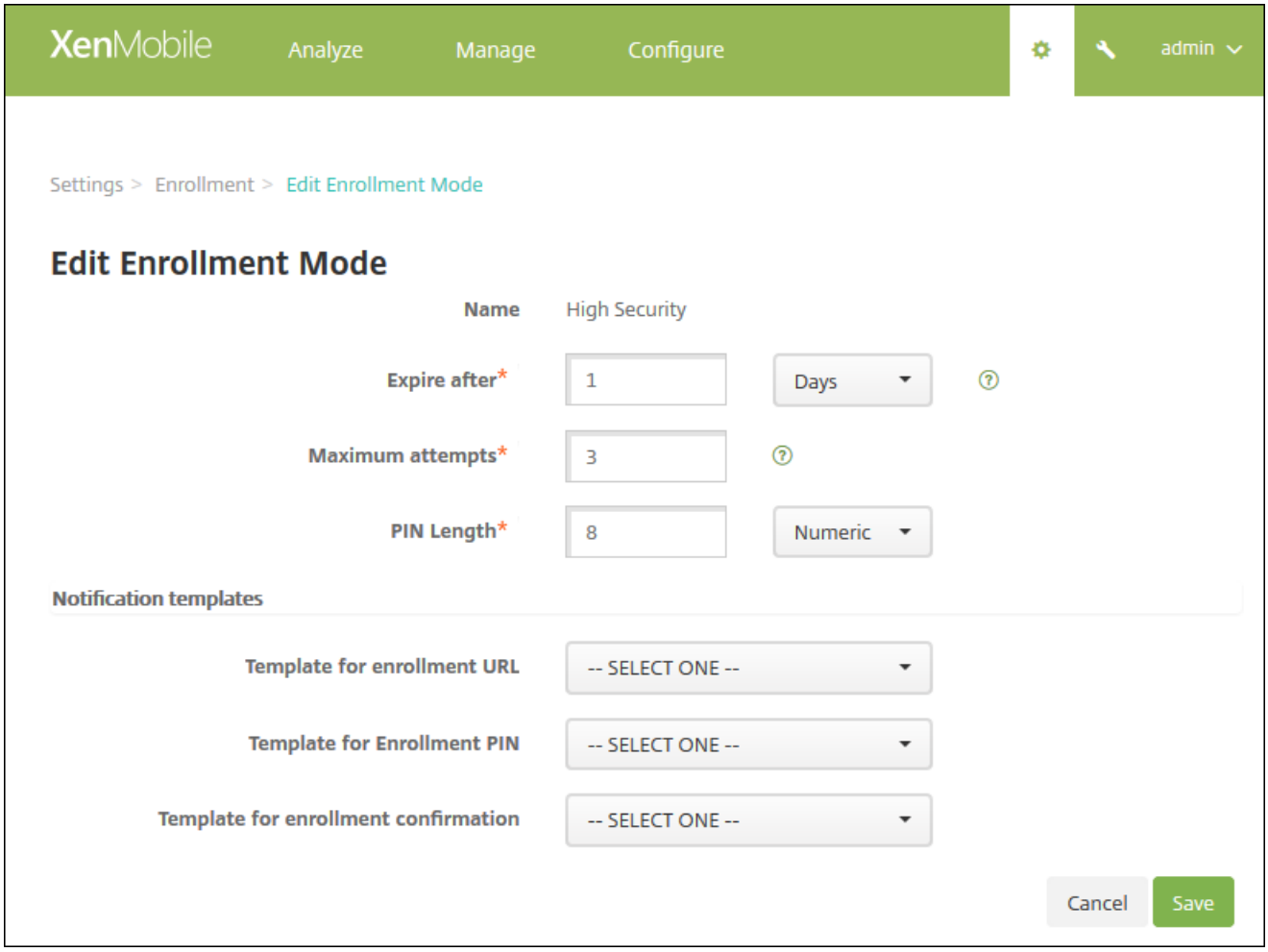
Remarque : lorsque vous sélectionnez la case à cocher en regard d'un mode d'inscription, le menu d'options s'affiche au-dessus de la liste des modes d'inscription. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la

liste.



Pour modifier un mode d'inscription

1. Dans la liste **Inscription**, sélectionnez un mode d'inscription, puis cliquez sur **Modifier**. La page **Modifier le mode d'inscription** apparaît. Selon le mode que vous sélectionnez, vous pouvez voir différentes options.



2. Modifiez les informations suivantes le cas échéant :

- **Expire après** : entrez un délai d'expiration au-delà duquel les utilisateurs ne peuvent pas inscrire leurs appareils. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.
  Remarque : entrez 0 pour empêcher l'invitation d'expirer.

- **Jours** : dans la liste, cliquez sur **Jours** ou **Heures** afin qu'ils correspondent au délai d'expiration que vous avez entré dans **Expire après**.
- **Nbre max de tentatives** : entrez le nombre de tentatives d'inscription qu'un utilisateur peut effectuer avant qu'il ne soit verrouillé du processus d'inscription. Cette valeur s'affiche dans les pages de configuration des invitations d'inscription des utilisateurs et des groupes.
  Remarque : entrez 0 pour autoriser un nombre illimité de tentatives.

- **Longueur du code PIN** : entrez le nombre de chiffres ou de caractères que le code PIN généré doit contenir.
- **Numérique** : dans la liste, cliquez sur **Numérique** ou **Alphanumérique** pour le type de code PIN.
- **Modèles de notification** :
  - **Modèle pour l'URL d'inscription** : sélectionnez un modèle à utiliser pour l'adresse URL d'inscription. Par exemple, le modèle d'invitation d'inscription envoie aux utilisateurs un e-mail ou SMS en fonction de la façon dont vous avez configuré le modèle qui leur permet d'inscrire leurs appareils dans XenMobile. Pour de plus amples informations sur les modèles de notification, consultez la section Création et mise à jour de modèles de notification.
  - **Modèle pour le PIN d'inscription** : dans la liste, sélectionnez un modèle à utiliser pour le PIN d'inscription.

- **Modèle pour la confirmation d'inscription** : dans la liste, sélectionnez un modèle à utiliser pour informer un utilisateur que l'inscription a réussi.

3. Cliquez sur **Enregistrer**.

Pour définir un mode d'inscription comme mode par défaut

Lorsque vous définissez un mode d'inscription en tant que mode par défaut, le mode est utilisé pour toutes les demandes d'inscription d'appareil, sauf si vous sélectionnez un autre mode d'inscription. Si aucun mode d'inscription n'est défini par défaut, vous devez créer une demande d'inscription pour chaque inscription d'appareil.

Remarque : vous pouvez uniquement définir **Nom d'utilisateur + mot de passe**, **Deux facteurs** ou **Nom d'utilisateur + code PIN** en tant que mode d'inscription par défaut.

1. Sélectionnez l'un des trois modes suivants à définir comme mode d'inscription par défaut : **Nom d'utilisateur + mots de passe**, **Deux facteurs** ou **Nom d'utilisateur + PIN**.

Remarque : le mode sélectionné doit être activé pour être défini comme mode par défaut.

2. Cliquez sur **Défaut**. Le mode sélectionné est maintenant le mode par défaut. Si un autre mode d'inscription a été défini comme mode par défaut, le mode n'est plus le mode par défaut.

Pour désactiver un mode d'inscription

La désactivation d'un mode d'inscription rend ce dernier inutilisable, à la fois pour les invitations d'inscription de groupe et sur le portail en libre-service. Vous pouvez modifier la façon dont vous autorisez les utilisateurs à inscrire leurs appareils en désactivant un mode d'inscription et en activant un autre.

1. Sélectionnez un mode d'inscription.

Remarque : vous ne pouvez pas désactiver le mode d'inscription par défaut. Pour désactiver le mode d'inscription par défaut, vous devez d'abord lui retirer son état de mode par défaut.

2. Cliquez sur **Désactiver**. Le mode d'inscription n'est plus activé.

Pour activer un mode d'inscription sur le portail en libre-service

L'activation d'un mode d'inscription sur le portail en libre-service permet aux utilisateurs d'inscrire leurs appareils dans XenMobile individuellement.

Remarque :

- Le mode d'inscription doit être activé et lié à des modèles de notification pour être disponible sur le portail en libre-service.
- Vous ne pouvez activer qu'un seul mode d'inscription à la fois sur le portail en libre-service.

1. Sélectionnez un mode d'inscription.

2. Cliquez sur **Portail en libre-service**. Le mode d'inscription que vous avez sélectionné est maintenant mis à la disposition des utilisateurs sur le portail en libre-service. Tout mode déjà activé sur le portail en libre-service n'est plus disponible.

Ajout ou suppression de groupes

Vous gérez les groupes dans la boîte de dialogue **Gérer les groupes** dans la console XenMobile, que vous pouvez trouver

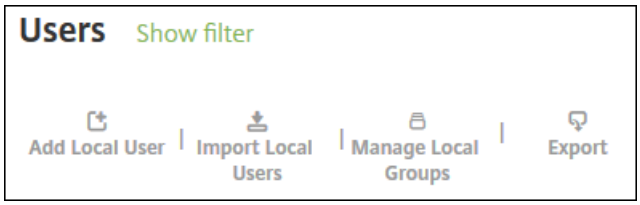
sur la page **Utilisateurs**, la page **Ajouter un utilisateur local** où la page **Modifier un utilisateur local**. Aucune commande ne permet de modifier un groupe.

Si vous supprimez un groupe, n'oubliez pas que la suppression du groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association de l'utilisateur avec ce groupe. Les utilisateurs perdent également l'accès aux applications ou profils fournis par les groupes de mise à disposition qui sont associés à ce groupe. Les autres associations de groupe restent toutefois intactes. Si les utilisateurs ne sont associés à aucun autre groupe local, ils sont associés au niveau supérieur.

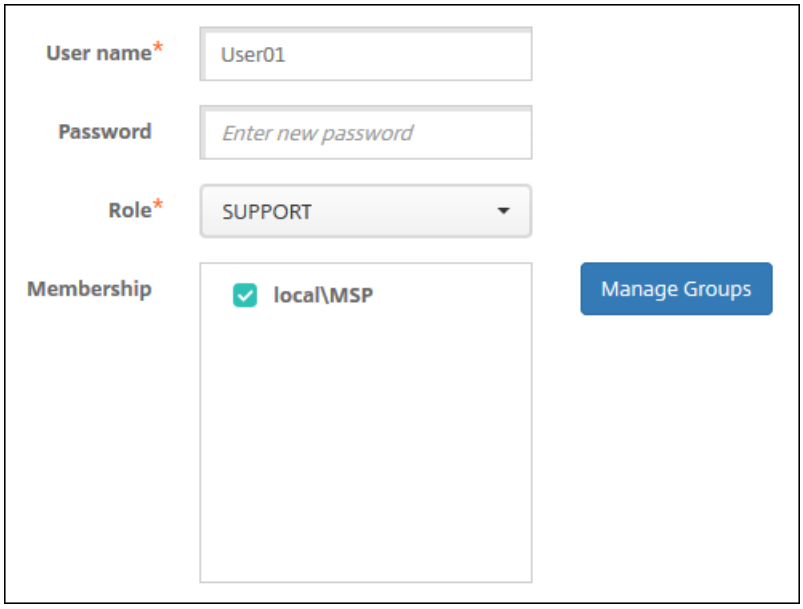
Pour ajouter un groupe local

1. Procédez comme suit :

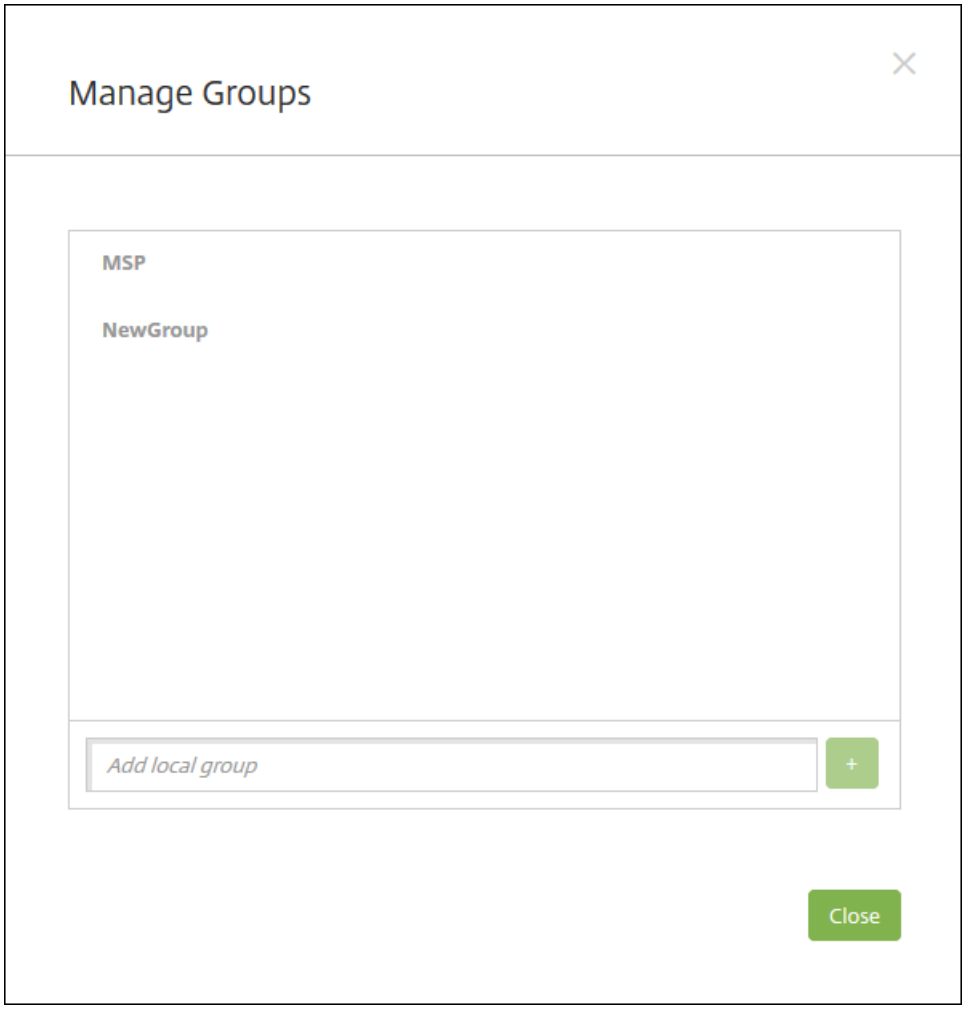
- Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.



- Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.



La boîte de dialogue **Gérer les groupes** s'affiche.



2. Sous les listes de groupes, entrez un nouveau nom de groupe, puis cliquez sur le signe plus (**+**). Le groupe d'utilisateurs est ajouté à la liste.

3. Cliquez sur **Fermer**.

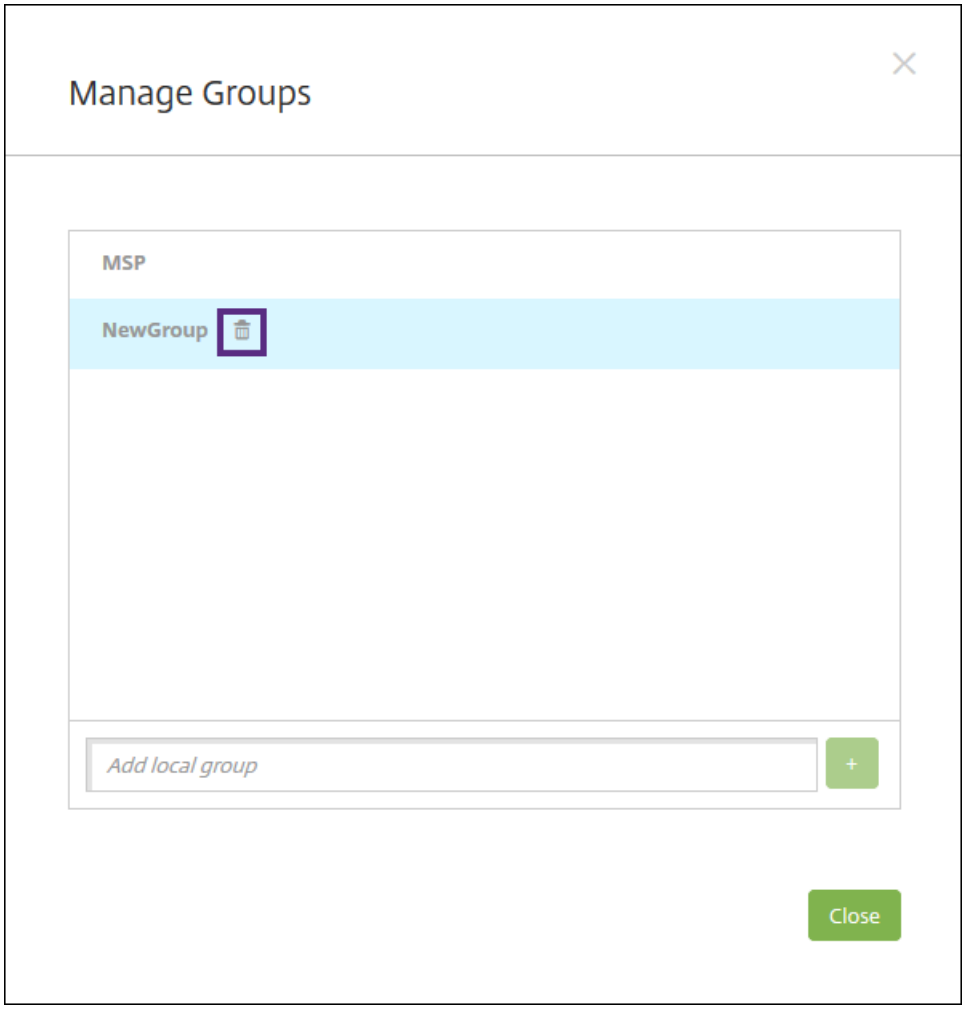
Pour supprimer un groupe

Remarque : la suppression d'un groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association de l'utilisateur avec ce groupe. Les utilisateurs perdent également l'accès aux applications ou profils fournis par les groupes de mise à disposition qui sont associés à ce groupe ; toutes les autres associations de groupe restent toutefois intactes. Si les utilisateurs ne sont associés à aucun autre groupe local, ils sont associés au niveau supérieur.

1. Procédez comme suit :

- Sur la page **Utilisateurs**, cliquez sur **Gérer les groupes locaux**.
- Sur la page **Ajouter un utilisateur local** ou la page **Modifier un utilisateur local**, cliquez sur **Gérer les groupes**.

La boîte de dialogue **Gérer les groupes** s'affiche.



2. Dans la boîte de dialogue **Gérer les groupes**, sélectionnez le groupe que vous souhaitez supprimer.

3. Cliquez sur l'icône de la corbeille à droite du nom de groupe. Une boîte de dialogue de confirmation s'affiche.

4. Cliquez sur **Supprimer** pour confirmer l'opération et supprimer le groupe.

Important : vous ne pouvez pas annuler cette opération.

5. Dans la boîte de dialogue **Gérer les groupes**, cliquez sur **Fermer**.

Créer et gérer des workflows

Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes d'utilisateur. Avant de pouvoir utiliser un workflow, vous devez identifier les personnes de votre organisation chargées d'approuver les demandes d'ouverture de comptes d'utilisateur. Vous pouvez ensuite utiliser le modèle de workflow pour créer et approuver les demandes.

Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres d'e-mail de workflow, qui doivent être définis avant que vous puissiez utiliser des workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert une approbation.

Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

- Dans la page **Workflows** sur la console XenMobile. Sur la page **Workflows**, vous pouvez configurer plusieurs workflows à utiliser pour la configuration d'applications. Lorsque vous configurez des workflows sur la page Workflows, vous pouvez sélectionner le workflow lors de la configuration de l'application.
- Lorsque vous configurez un connecteur d'application, dans l'application, vous devez fournir un nom de workflow, puis configurer les personnes qui peuvent approuver la demande de compte utilisateur. Voir Ajout d'applications à XenMobile.

Vous pouvez désigner jusqu'à trois niveaux pour l'approbation du responsable des comptes d'utilisateur. Si vous voulez faire approuver le compte utilisateur par d'autres personnes, vous pouvez utiliser leur nom ou adresse e-mail pour rechercher et sélectionner des approbateurs. Lorsque XenMobile trouve la personne concernée, vous pouvez l'ajouter au workflow. Toutes les personnes figurant dans le workflow reçoivent un e-mail afin d'approuver ou de refuser l'ouverture du nouveau compte d'utilisateur.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Workflows**. La page **Workflows** s'affiche.

3. Cliquez sur **Ajouter**. La page **Ajouter un workflow** s'affiche.

4. Pour configurer ces paramètres :

- **Nom** : entrez un nom unique pour le workflow.
- **Description** : entrez une description pour le workflow (facultatif).
- **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Vous créez des modèles d'e-mail dans la section **Modèles de notification** sous **Paramètres** dans la console XenMobile. Lorsque vous cliquez sur l'icône d'œil à droite de ce champ, vous voyez un aperçu du modèle que vous êtes en train de configurer.

- **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
  - Pas nécessaire
  - 1 niveau
  - 2 niveaux
  - 3 niveaux
- **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
- **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
- Lorsque le nom s'affiche dans le champ, sélectionnez la case à cocher en regard du nom. Le nom et l'adresse e-mail s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer une personne de la liste Approbateurs supplémentaires requis sélectionnés, procédez comme suit :
    - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    - Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

5. Cliquez sur **Enregistrer**. Le workflow créé s'affiche sur la page **Workflows**.

Après avoir créé le workflow, vous pouvez afficher les détails du workflow, voir les applications associées au workflow ou supprimer le workflow. Vous ne pouvez pas modifier un workflow après sa création. Si vous avez besoin d'un workflow avec différents niveaux d'approbation ou approbateurs, vous devez créer un autre workflow.

Pour afficher les détails d'un workflow et le supprimer

1. Sur la page **Workflows**, dans la liste des workflows, sélectionnez un workflow. Pour ce faire, cliquez sur la ligne dans le tableau ou sélectionnez la case à cocher en regard du workflow.

2. Pour supprimer un workflow, cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**.

Important : vous ne pouvez pas annuler cette opération.

Configurer des rôles avec RBAC

Feb 23, 2017

Chaque rôle RBAC prédéfini dispose de certains accès et de certaines autorisations associés à ce rôle. Cet article explique chacune de ces autorisations. Pour obtenir une liste complète des autorisations par défaut pour chaque rôle intégré, téléchargez le PDF Role-Based Access Control Defaults.

Lorsque vous *appliquez des autorisations*, vous définissez les groupes d'utilisateurs que le rôle RBAC est autorisé à gérer. Veuillez noter que l'administrateur par défaut ne peut pas modifier les paramètres d'autorisation appliqués ; par défaut, les autorisations appliquées s'appliquent à tous les groupes d'utilisateurs.

Lorsque vous procédez à une *attribution*, vous attribuez le rôle RBAC à un groupe, afin que le groupe d'utilisateurs disposent des droits d'administrateur RBAC.

Rôle d'administrateur

Rôle de provisioning d'appareils

Rôle Support

Rôle Utilisateur

Configurer des rôles avec RBAC

La fonctionnalité de contrôle d'accès basé sur rôle (RBAC) de XenMobile vous permet d'attribuer des rôles prédéfinis ou un ensemble d'autorisations aux utilisateurs et aux groupes. Ces autorisations contrôlent le niveau d'accès des utilisateurs aux fonctions du système.

XenMobile implémente quatre rôles utilisateur par défaut de façon à séparer logiquement l'accès aux fonctions système :

- **Administrateur**. Accorde un accès complet au système.
- **Provisioning d'appareils**. Accorde un accès à l'administration de base des appareils pour les appareils Windows CE.
- **Assistance**. Accorde l'accès à l'assistance à distance.
- **Utilisateur**. Utilisé par les utilisateurs autorisés à inscrire des appareils et à accéder au portail en libre-service.

Vous pouvez aussi utiliser les rôles par défaut en tant que modèles que vous personnalisez pour créer de nouveaux rôles utilisateur autorisés à accéder à des fonctions système spécifiques au-delà des fonctions définies par les rôles par défaut.

Les rôles peuvent être attribués à des utilisateurs locaux (au niveau de l'utilisateur) ou à des groupes Active Directory (tous les utilisateurs de ce groupe ont les mêmes autorisations). Si un utilisateur appartient à plusieurs groupes Active Directory, les autorisations sont fusionnées pour définir les autorisations de cet utilisateur. Par exemple, si les utilisateurs ADGroupA peuvent localiser les appareils appartenant à l'entreprise, et que les utilisateurs ADGroupB peuvent réinitialiser les appareils appartenant aux employés, alors un utilisateur qui appartient aux deux groupes peut localiser et réinitialiser les appareils appartenant à l'entreprise et aux employés.

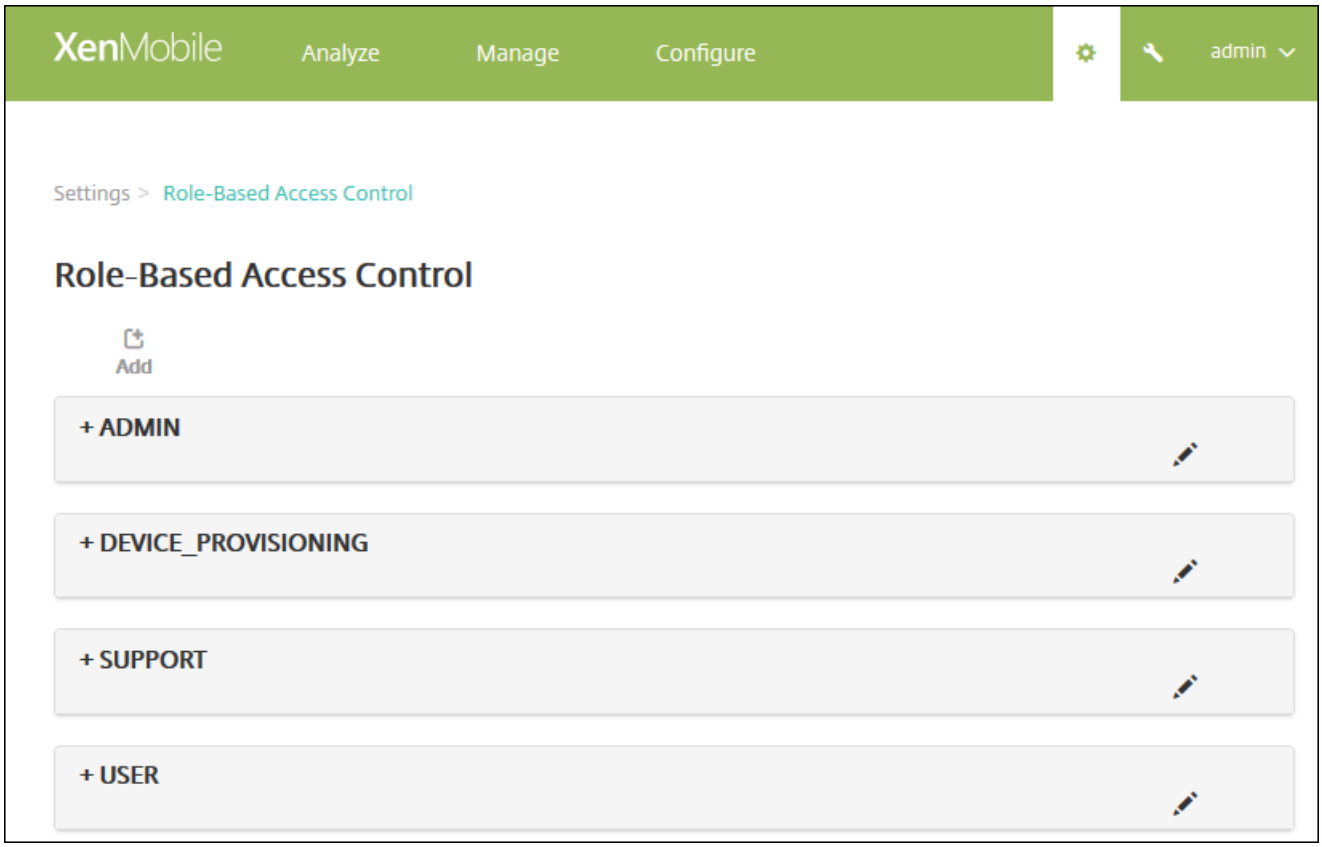
Remarque : un seul rôle peut être attribué aux utilisateurs locaux.

Vous pouvez utiliser la fonctionnalité RBAC dans XenMobile pour effectuer les opérations suivantes :

- Créer un nouveau rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Contrôle d'accès basé sur rôle**. La page **Contrôle d'accès basé sur rôle** qui apparaît affiche les quatre rôles utilisateur par défaut, ainsi que tout rôle que vous avez déjà ajouté.



si vous cliquez sur le signe plus (+) à côté d'un rôle, celui-ci se développe pour afficher toutes les autorisations pour ce rôle, comme illustré dans la figure suivante.

3. Cliquez sur **Ajouter** pour ajouter un nouveau rôle utilisateur, cliquez sur l'icône de crayon à droite d'un rôle existant pour

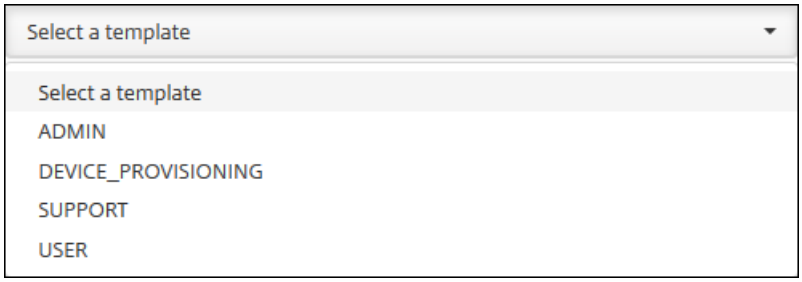
modifier le rôle, ou cliquez sur l'icône de corbeille à droite d'un rôle que vous avez précédemment défini pour supprimer le rôle. Vous ne pouvez pas supprimer les rôles utilisateur par défaut.

- Lorsque vous cliquez sur **Ajouter** ou l'icône de crayon, la page **Ajouter un rôle** ou **Modifier le rôle** s'affiche.
- Lorsque vous cliquez sur l'icône de corbeille, une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer le rôle sélectionné.

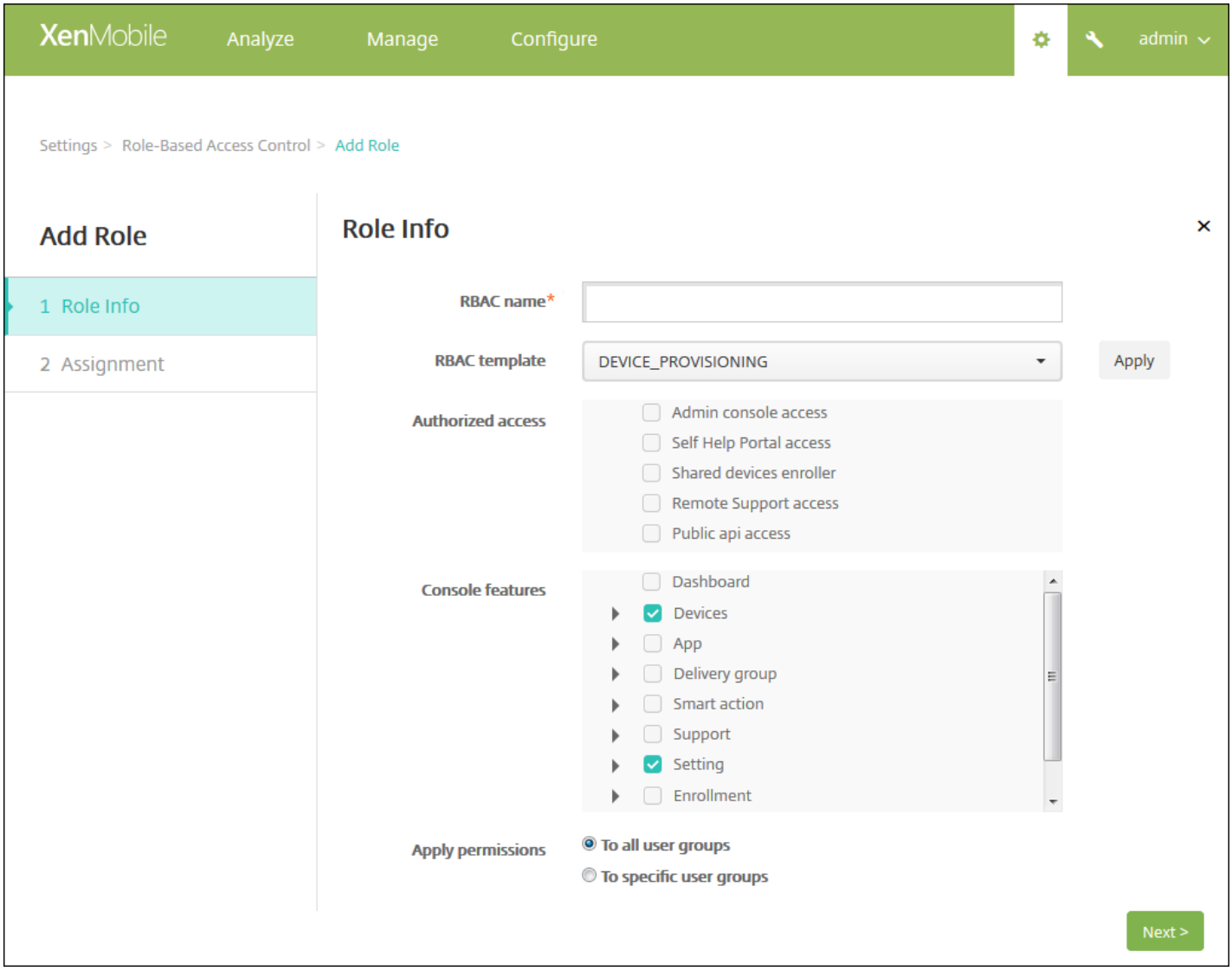
4. Entrez les informations suivantes pour créer un nouveau rôle utilisateur ou pour modifier un rôle utilisateur existant :

- **Nom RBAC** : entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle existant.
- **Modèle RBAC** : si vous le souhaitez, cliquez sur un modèle en tant que point de départ pour le nouveau rôle. Vous ne pouvez pas sélectionner de modèle si vous modifiez un rôle existant.

Les modèles RBAC sont les rôles utilisateur par défaut. Ils définissent l'accès aux fonctions système dont disposent les utilisateurs associés à ce rôle. Lorsque vous sélectionnez un modèle RBAC, vous pouvez voir toutes les autorisations associées à ce rôle dans les champs **Accès autorisé** et **Fonctionnalités de la console**. L'utilisation d'un modèle est facultative ; vous pouvez sélectionner les options que vous voulez attribuer à un rôle directement dans les champs **Accès autorisé** et **Fonctionnalités de la console**.

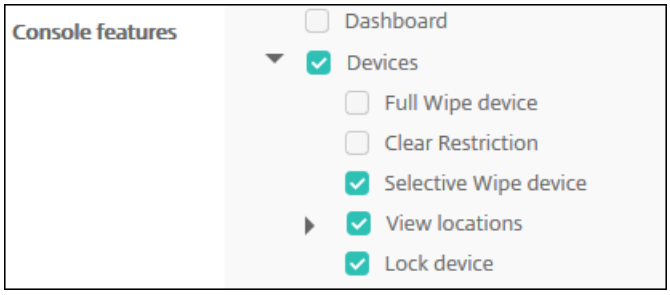


5. Cliquez sur **Appliquer** à droite du champ **Modèle RBAC** pour renseigner les cases **Accès autorisé** et **Fonctionnalités de la console** avec les autorisations d'accès prédéfinies pour le modèle sélectionné.

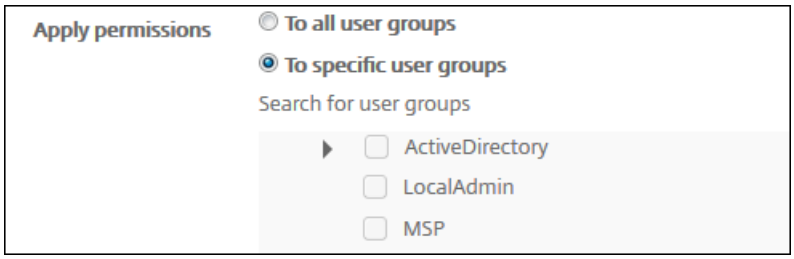


6. Sélectionnez et décochez les cases à cocher appropriées dans **Accès autorisé** et **Fonctionnalités de la console** pour personnaliser le rôle.

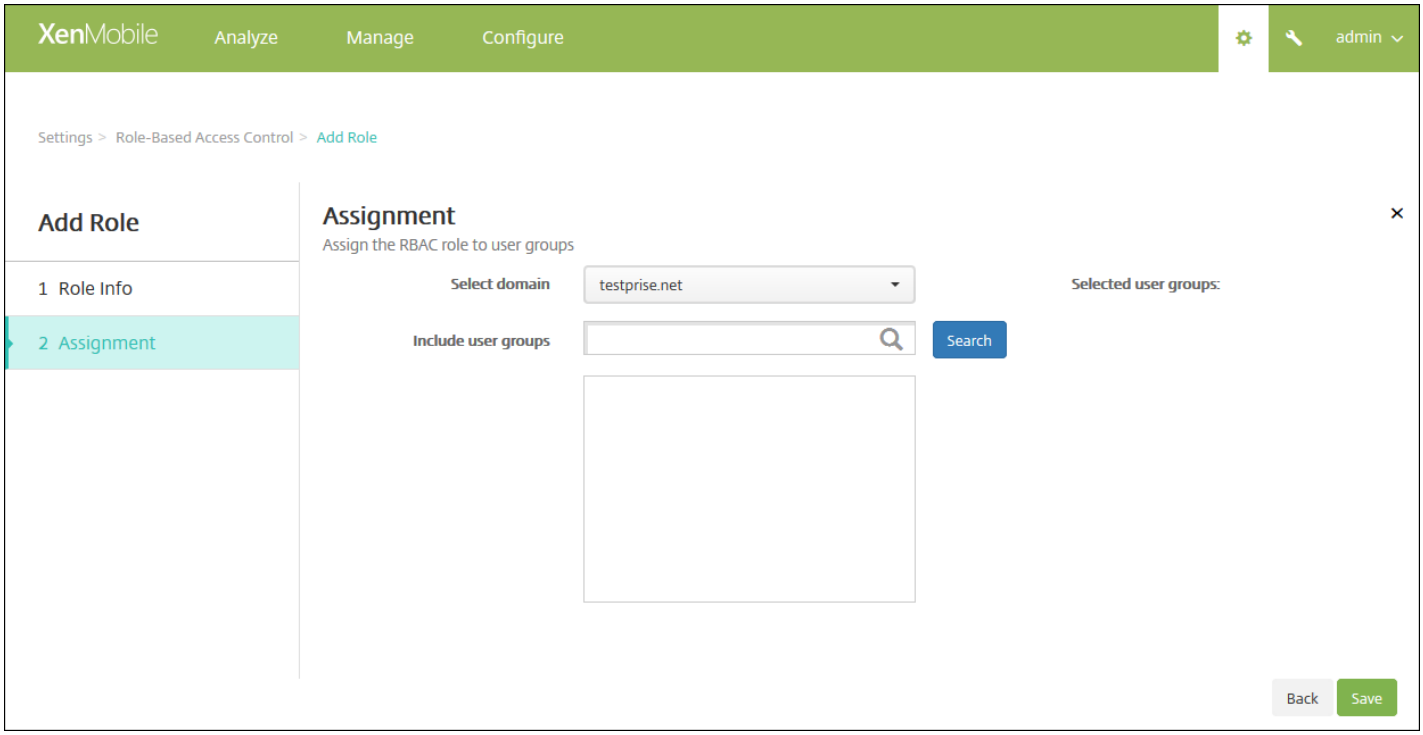
si vous cliquez sur le triangle à côté de Fonctionnalités de la console, les autorisations spécifiques à cette fonctionnalité s'affichent de façon à ce que vous puissiez les sélectionner ou les désélectionner. La case à cocher de niveau supérieur empêche l'accès à cette partie de la console ; vous devez sélectionner des options individuelles en-dessous du niveau supérieur pour activer ces options. Par exemple, dans la figure suivante, les options **Effacer un appareil** et **Effacer les restrictions** ne s'affichent pas sur la console pour les utilisateurs associés au rôle, mais les options sélectionnées s'affichent.



7. **Appliquer les autorisations** : sélectionnez les groupes auxquels vous voulez appliquer les autorisations sélectionnées. Si vous cliquez sur **À des groupes d'utilisateurs spécifiques**, une liste des groupes s'affiche à partir de laquelle vous pouvez sélectionner un ou plusieurs groupes.

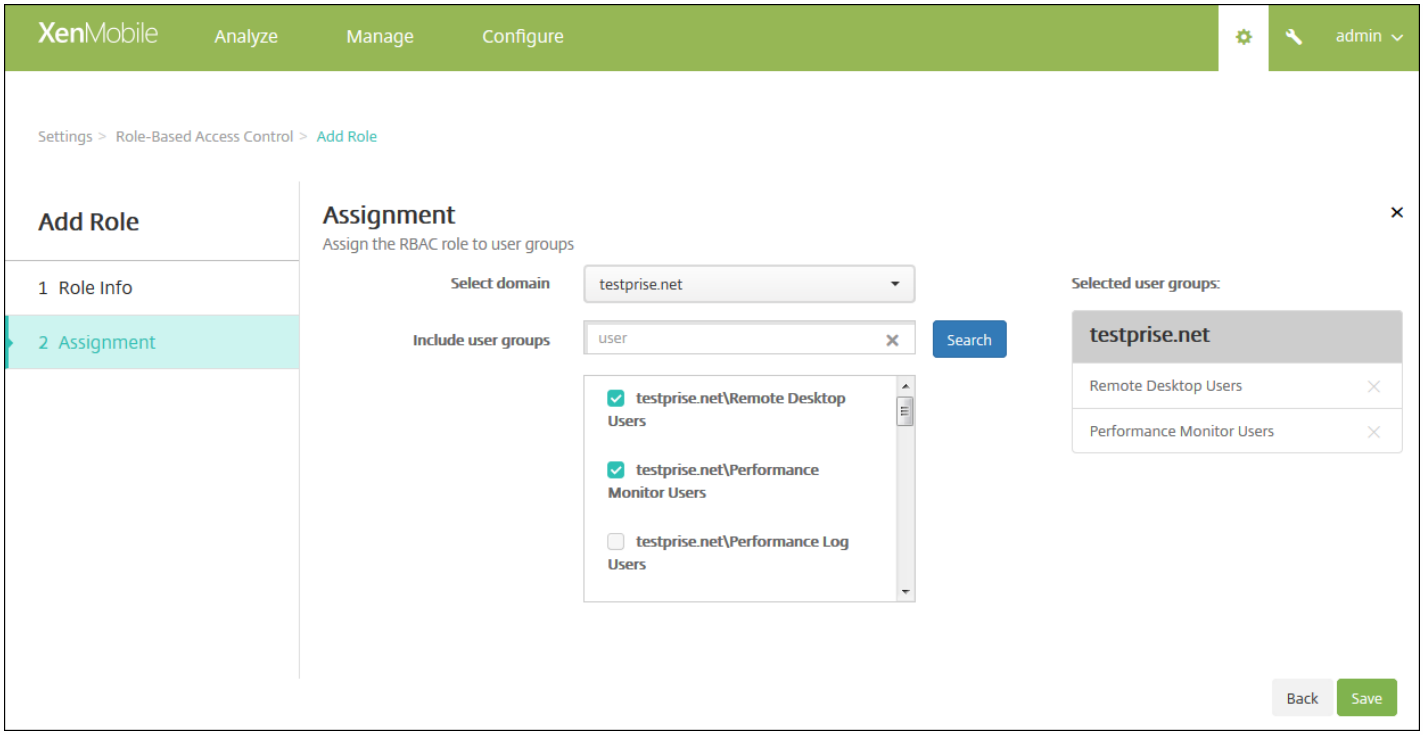


8. Cliquez sur **Next**. La page **Attribution** s'affiche.



9. Entrez les informations suivantes pour attribuer le rôle à des groupes d'utilisateurs.

- **Sélectionner un domaine** : cliquez sur un domaine dans la liste.
- **Inclure des groupes d'utilisateurs** : cliquez sur Rechercher pour afficher une liste de tous les groupes disponibles, ou tapez un nom de groupe complet ou partiel pour limiter la liste aux groupes portant ce nom.
- Dans la liste qui s'affiche, sélectionnez les groupes d'utilisateurs auxquels vous souhaitez attribuer le rôle. Lorsque vous sélectionnez un groupe d'utilisateurs, le groupe apparaît dans la liste **Groupes d'utilisateurs sélectionnés**.



Remarque : pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le X en regard du nom du groupe d'utilisateurs.

10. Cliquez sur **Enregistrer**.

Notifications

Feb 23, 2017

Vous pouvez utiliser les notifications dans XenMobile aux fins suivantes :

- Pour communiquer avec des groupes d'utilisateurs sélectionnés à propos d'un certain nombre de fonctions liées au système. Vous pouvez également cibler ces notifications pour certains utilisateurs ; par exemple, tous les utilisateurs équipés d'appareils iOS, les utilisateurs dont les appareils ne sont pas conformes, les utilisateurs équipés d'appareils leur appartenant, etc.
- Pour inscrire les utilisateurs et leurs appareils.
- Pour notifier automatiquement les utilisateurs (via des actions automatisées) lorsque certaines conditions sont remplies, par exemple lorsque l'accès au domaine d'entreprise est sur le point d'être bloqué en raison d'un problème de conformité, ou lorsqu'un appareil est jailbreaké ou rooté. Pour de plus amples informations sur les actions automatisées, consultez la section Actions automatisées.

Pour envoyer des notifications avec XenMobile, vous devez configurer une passerelle et un serveur de notification. Vous pouvez configurer un serveur de notification dans XenMobile pour configurer des serveurs de passerelle SMTP et SMS de façon à pouvoir envoyer des notifications sous forme d'e-mails et de messages texte (SMS) aux utilisateurs. Vous pouvez utiliser les notifications pour envoyer des messages sur deux canaux : SMTP ou SMS.

- SMTP est un protocole basé sur texte orienté connexion, dans lequel un expéditeur communique avec un récepteur de courrier en émettant des chaînes de commande et en fournissant les données nécessaires, généralement via une connexion TCP. Les sessions SMTP se composent de commandes émanant d'un client SMTP (la personne qui envoie le message) et des réponses correspondantes à partir du serveur SMTP.
- SMS est un composant du service de messagerie texte du téléphone, du Web ou de systèmes de communication mobiles. SMS utilise des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

Vous pouvez également définir une passerelle SMS d'opérateur dans XenMobile pour configurer les notifications envoyées via la passerelle SMS d'un opérateur. Les opérateurs utilisent les passerelles SMS pour envoyer ou recevoir des transmissions SMS vers ou à partir d'un réseau de télécommunications. Ces messages texte utilisent des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

Les procédures décrites dans cet article expliquent comment configurer un serveur SMTP, une passerelle SMS et une passerelle SMS opérateur.

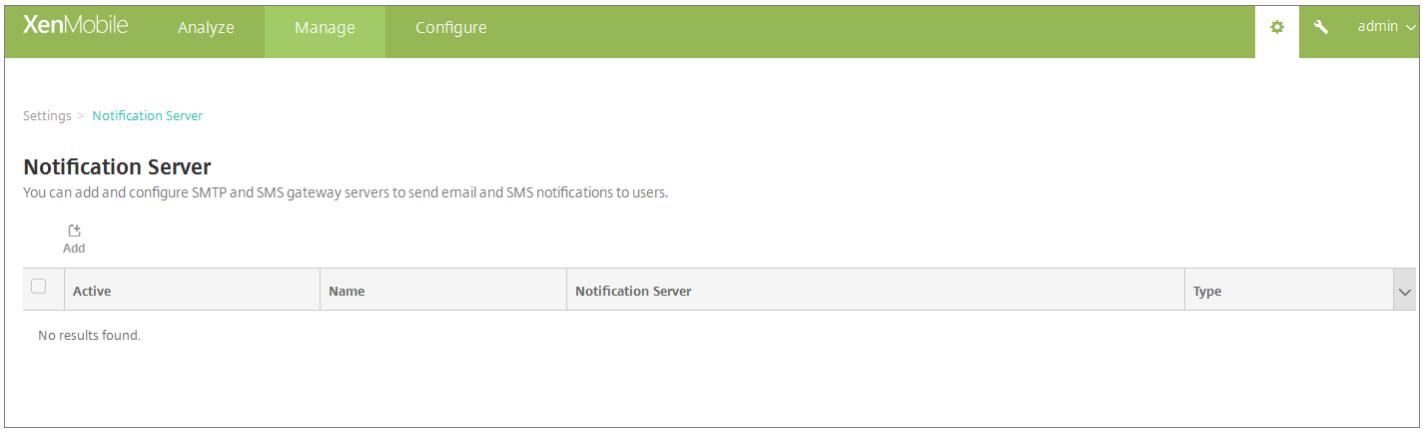
Conditions préalables

- Avant de configurer la passerelle SMS, consultez votre administrateur système pour déterminer les informations de serveur. Il est important de savoir si le serveur SMS est hébergé sur un réseau d'entreprise interne, ou s'il fait partie d'un service de messagerie hébergé, auquel cas vous aurez besoin des informations du site Web du fournisseur de services.
- Vous devez configurer le serveur de notifications SMTP pour envoyer des messages aux utilisateurs. Si le serveur est hébergé sur un serveur interne, contactez votre administrateur système pour obtenir les informations de configuration. Si le serveur est un service de messagerie hébergé, recherchez les informations de configuration appropriées sur le site Web du fournisseur de services.
- Un seul serveur SMTP et un seul serveur SMS sont actifs à la fois.
- Le port 25 doit être ouvert depuis XenMobile dans la zone démilitarisée (DMZ) de votre réseau afin de pointer vers le serveur SMTP sur votre réseau interne pour que les notifications soient envoyées avec succès.

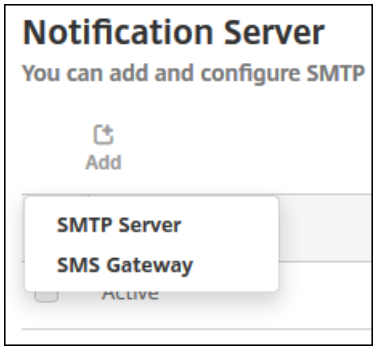
Pour configurer un serveur SMTP et une passerelle SMS

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Notifications**, cliquez sur **Serveur de notification**. La page **Serveur de notification** s'affiche.

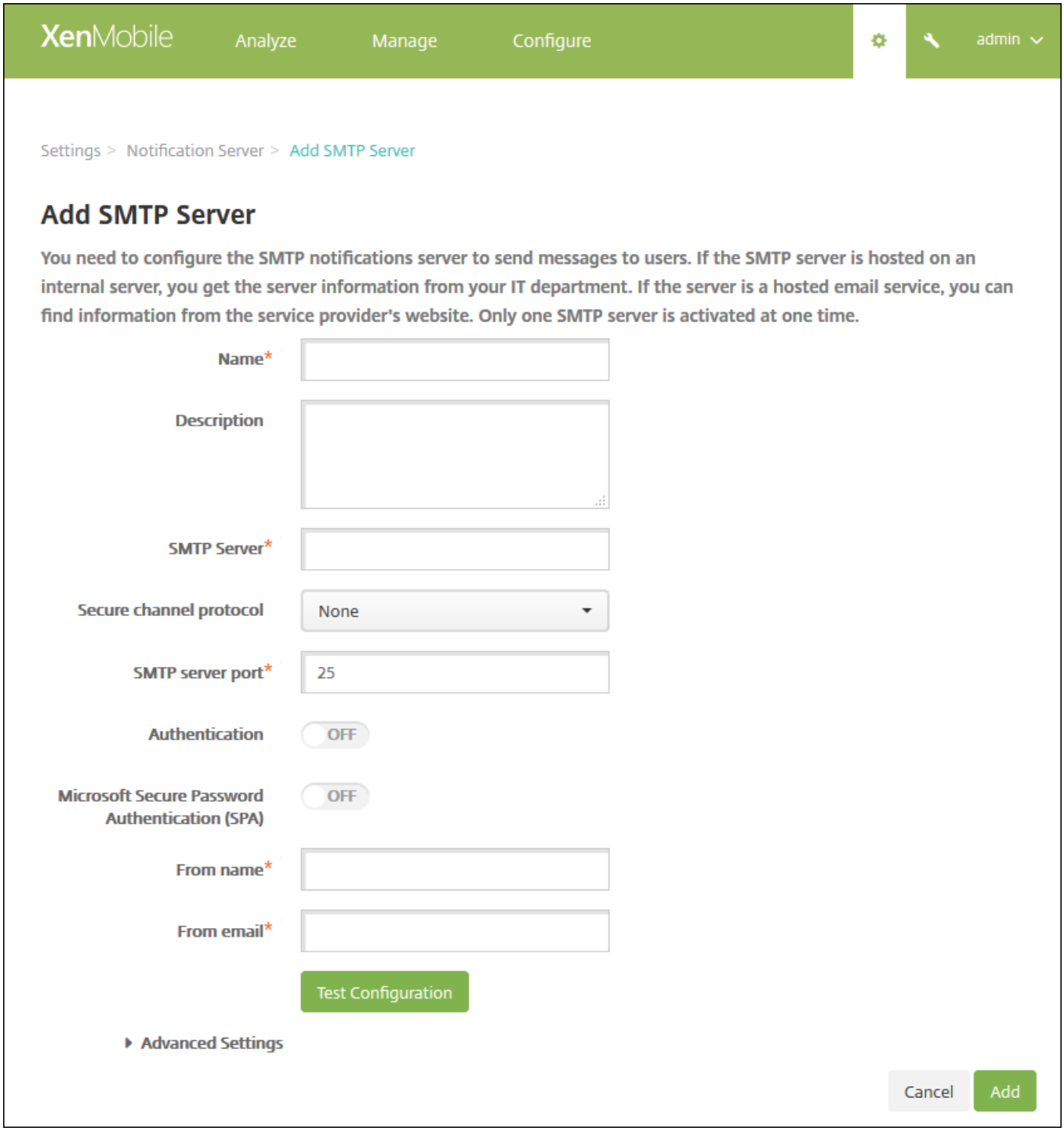


2. Cliquez sur **Add**. Un menu s'affiche avec des options pour configurer un serveur SMTP ou une passerelle SMS.



- Pour ajouter un serveur SMTP, cliquez sur **Serveur SMTP**, puis consultez la section Pour ajouter un serveur SMTP pour connaître les étapes suivantes.
- Pour ajouter une passerelle SMS, cliquez sur **Passerelle SMS**, puis consultez la section Pour ajouter une passerelle SMS pour connaître les étapes suivantes.

Pour ajouter un serveur SMTP



1. Configurez les paramètres suivants :

- **Nom** : entrez le nom associé à ce compte de serveur SMTP.
- **Description** : entrez une description pour le serveur (facultatif).
- **Serveur SMTP** : entrez le nom d'hôte du serveur. Le nom d'hôte peut être un nom de domaine complet (FQDN) ou une adresse IP.
- **Secure Channel Protocol** : dans la liste, cliquez sur le protocole de canal sécurisé approprié utilisé par le serveur (si le serveur est configuré pour utiliser une authentification sécurisée) : **SSL**, **TLS** ou **Aucun**. La valeur par défaut est **Aucun**.
- **Port du serveur SMTP** : entrez le port utilisé par le serveur SMTP. Par défaut, le port est défini sur 25 ; si les connexions

SMTP utilisent le protocole de canal sécurisé SSL, le port est défini sur 465.

- **Authentification** : sélectionnez **ON** ou **OFF**. La valeur par défaut est **OFF**.
- Si vous avez activé **Authentification**, configurez les paramètres suivants :
  - **Nom d'utilisateur** : entrez un nom d'utilisateur à utiliser pour l'authentification.
  - **Mot de passe** : entrez le mot de passe de l'utilisateur.
- **Authentification par mot de passe sécurisé (SPA) Microsoft** : si le serveur SMTP utilise la SPA, cliquez sur **ON**. La valeur par défaut est **OFF**.
- **Nom expéditeur** : entrez le nom affiché dans la case **De** lorsqu'un client reçoit une notification par e-mail à partir de ce serveur. Par exemple, Département Informatique.
- **E-mail expéditeur** : entrez l'adresse e-mail utilisée si le destinataire d'un e-mail répond à la notification envoyée par le serveur SMTP.

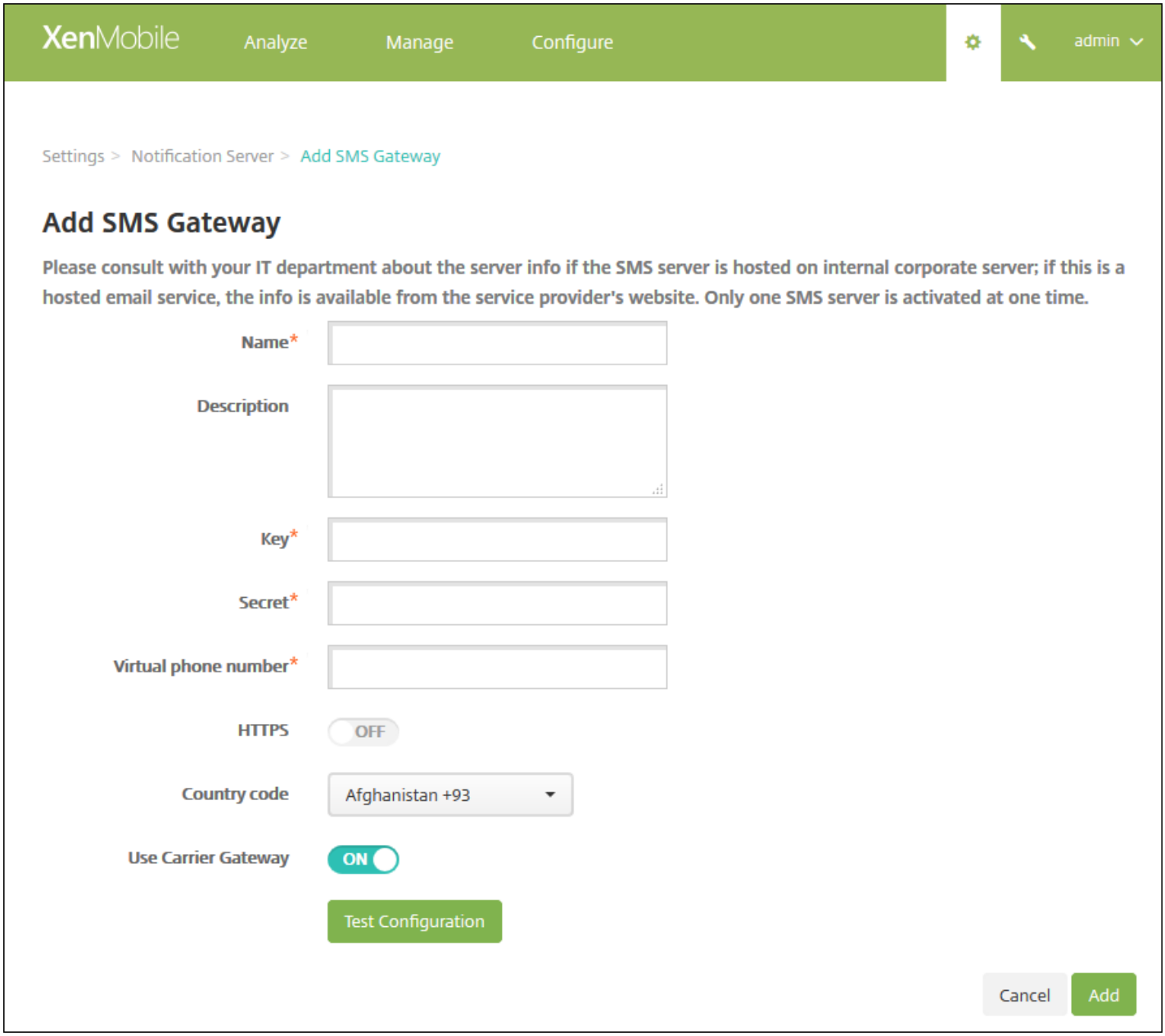
2. Cliquez sur **Tester la configuration** pour envoyer une notification par e-mail test.

3. Développez **Paramètres avancés** et configurez les paramètres suivants :

- **Nombre d'essais SMTP** : entrez le nombre de tentatives d'envoi d'un message dont l'envoi a échoué à partir du serveur SMTP. La valeur par défaut est 5.
- **Délai d'attente SMTP** : entrez la durée d'attente (en secondes) lors de l'envoi d'une demande SMTP. Augmentez cette valeur si l'envoi de messages échoue continuellement en raison de l'expiration des délais. Soyez prudent lorsque vous diminuez cette valeur ; cela pourrait augmenter les échecs dus à l'expiration des délais ainsi que le nombre de messages non remis. La durée par défaut est de 30 secondes.
- **Nombre max de destinataires SMTP** : entrez le nombre maximal de destinataires par message envoyés par le serveur SMTP. La valeur par défaut est 100.

4. Cliquez sur **Add**.

Pour ajouter une passerelle SMS



Remarque

XenMobile prend uniquement en charge la messagerie Nexmo SMS. Si vous ne possédez pas de compte pour utiliser la messagerie Nexmo, visitez leur site Web pour en créer un.

1. Configurez les paramètres suivants :

- **Nom** : entrez un nom pour la configuration de la passerelle SMS. Ce champ est obligatoire.
- **Description** : entrez une description pour la configuration (facultatif).
- **Clé** : entrez l'identificateur numérique fourni par l'administrateur système lors de l'activation du compte. Ce champ est obligatoire.
- **Secret** : entrez un secret fourni par l'administrateur système qui est utilisé pour accéder à votre compte dans le cas où un

mot de passe est perdu ou volé. Ce champ est obligatoire.

- **Numéro de téléphone virtuel** : ce champ est utilisé lors de l'envoi à des numéros de téléphone d'Amérique du Nord (avec le préfixe +1). Vous devez entrer un numéro de téléphone virtuel Nexmo et seuls des chiffres peuvent être utilisés dans ce champ. Vous pouvez acheter des numéros de téléphone virtuels sur le site Web Nexmo.
- **HTTPS** : indiquez si vous souhaitez utiliser le protocole HTTPS pour transmettre des requêtes SMS à Nexmo. La valeur par défaut est **OFF**.

  Important : laissez HTTPS défini sur **ON** sauf si l'assistance Citrix vous demande de désactiver l'option (**OFF**).

- **Indicatif du pays** : dans la liste, cliquez sur le préfixe d'indicatif du pays SMS par défaut pour les destinataires dans votre organisation. Ce champ commence toujours par un symbole +. La valeur par défaut est **Afghanistan +93**.

2. Cliquez sur **Tester la configuration** pour envoyer un message test à l'aide de la configuration actuelle. Les erreurs de connexion, telles que les erreurs de numéro de téléphone d'authentification ou virtuels, sont détectées et apparaissent immédiatement. Les messages sont reçus dans les mêmes délais que ceux envoyés entre téléphones portables.

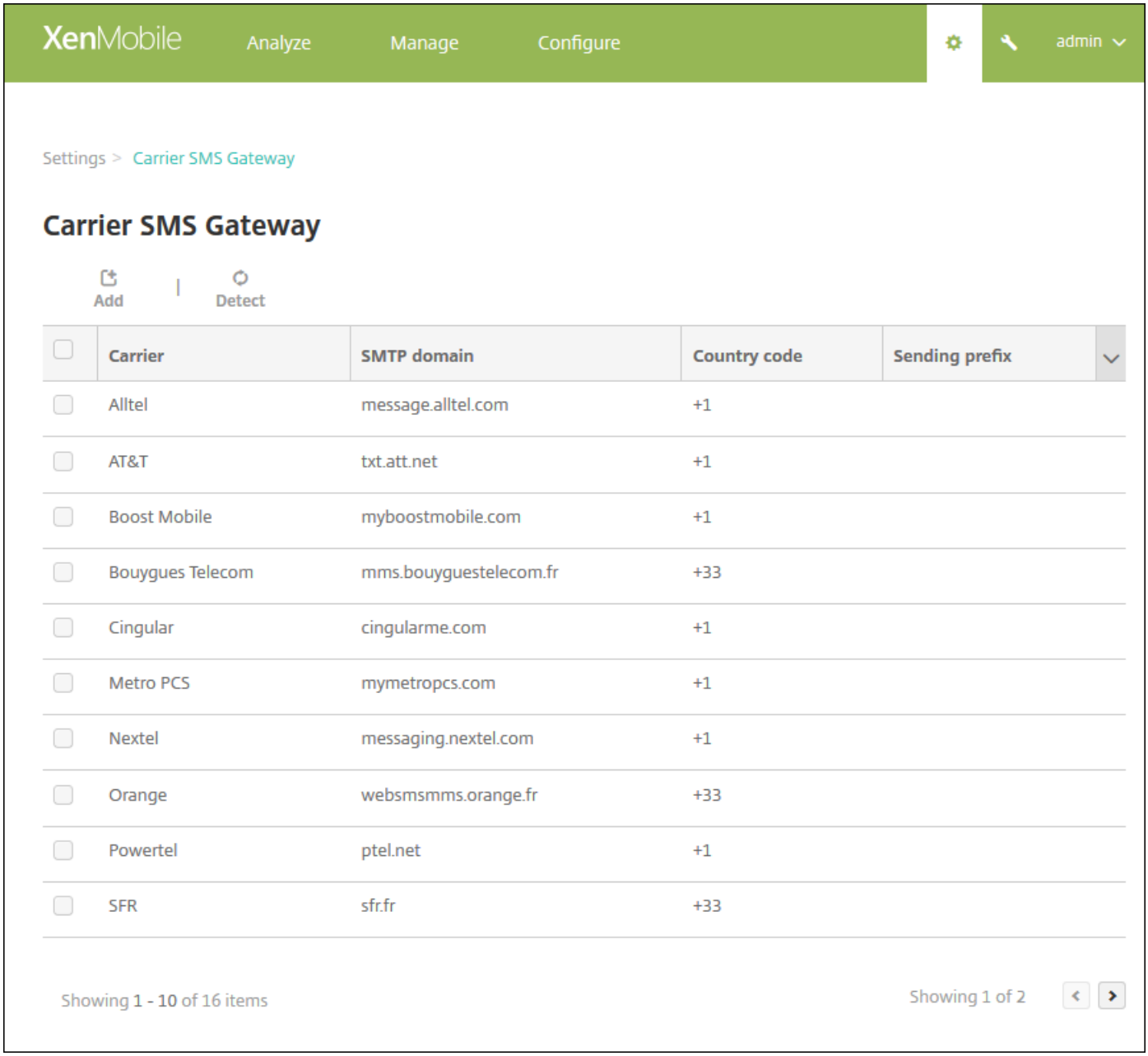
2. Cliquez sur **Add**.

Pour ajouter une passerelle SMS d'opérateur

Vous pouvez configurer une passerelle SMS d'opérateur dans XenMobile pour configurer les notifications qui sont envoyées via la passerelle SMS d'un opérateur. Les opérateurs utilisent les passerelles SMS pour envoyer ou recevoir des transmissions SMS vers ou à partir d'un réseau de télécommunications. Ces messages texte utilisent des protocoles de communication standard pour permettre à des téléphones portables ou fixes d'échanger des messages texte courts.

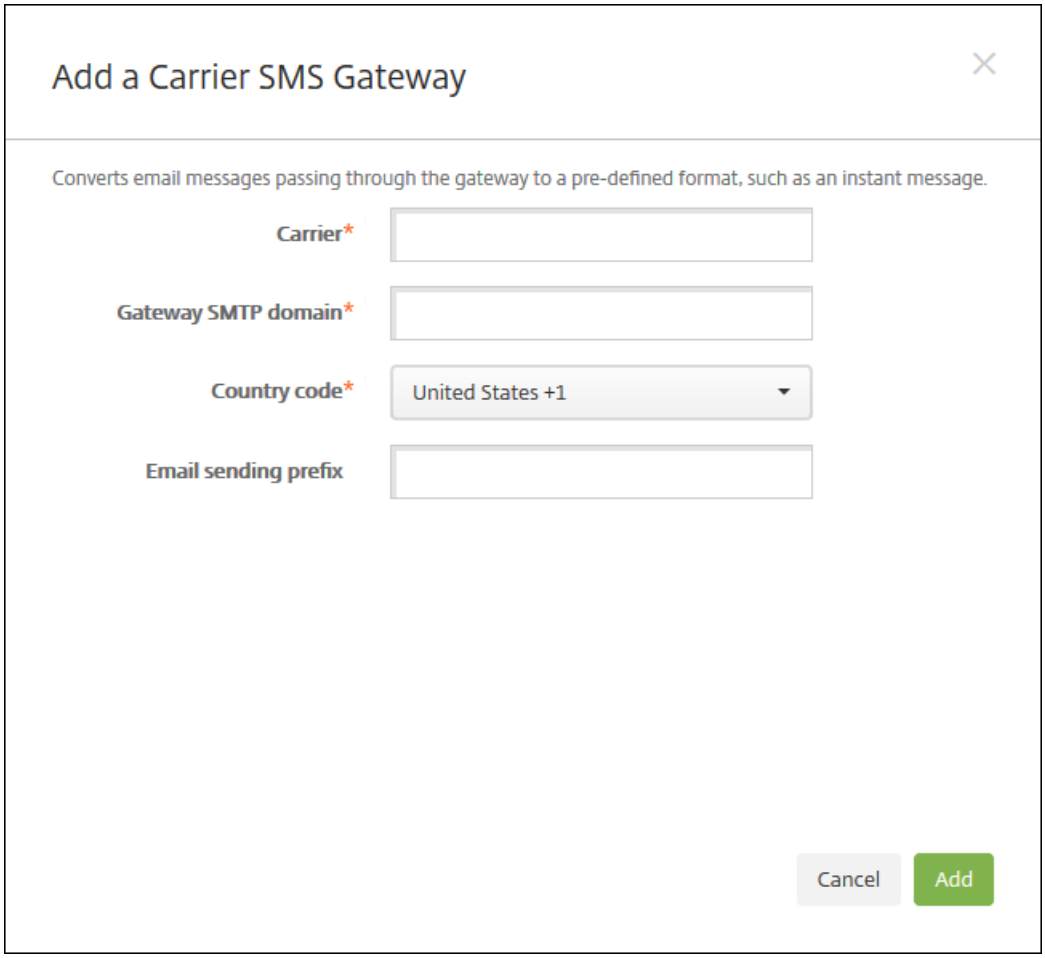
1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Notifications**, cliquez sur **Passerelle SMS de l'opérateur**. La page **Passerelle SMS de l'opérateur** s'ouvre.



3. Procédez comme suit :

- Cliquez sur le bouton **Détecter** pour découvrir automatiquement une passerelle. Une boîte de dialogue s'affiche indiquant qu'aucun nouvel opérateur n'a été détecté ou répertoriant les nouveaux opérateurs détectés parmi les appareils inscrits.
- Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter la passerelle SMS d'un opérateur** apparaît.



Remarque : XenMobile prend uniquement en charge la messagerie Nexmo SMS. Si vous ne possédez pas de compte pour utiliser la messagerie Nexmo, visitez leur site Web pour en créer un.

4. Configurez les paramètres suivants :

- **Opérateur** : entrez le nom de l'opérateur.
- **Domaine SMTP de la passerelle** : entrez le domaine associé à la passerelle SMTP.
- **Indicatif du pays** : dans la liste, cliquez sur l'indicatif de pays pour l'opérateur.
- **Préfixe d'envoi d'e-mail** : si vous le souhaitez, vous pouvez spécifier un préfixe pour l'envoi d'e-mail.

5. Cliquez sur **Ajouter** pour ajouter le nouvel opérateur ou cliquez sur **Annuler** pour ne pas ajouter le nouvel opérateur.

Création et mise à jour de modèles de notification

Vous pouvez créer ou mettre à jour des modèles de notification dans XenMobile à utiliser dans les actions automatisées, l'inscription, et les messages de notifications standard envoyés aux utilisateurs. Vous configurez les modèles de notification pour l'envoi de messages sur trois canaux différents : Secure Hub, SMTP ou SMS.

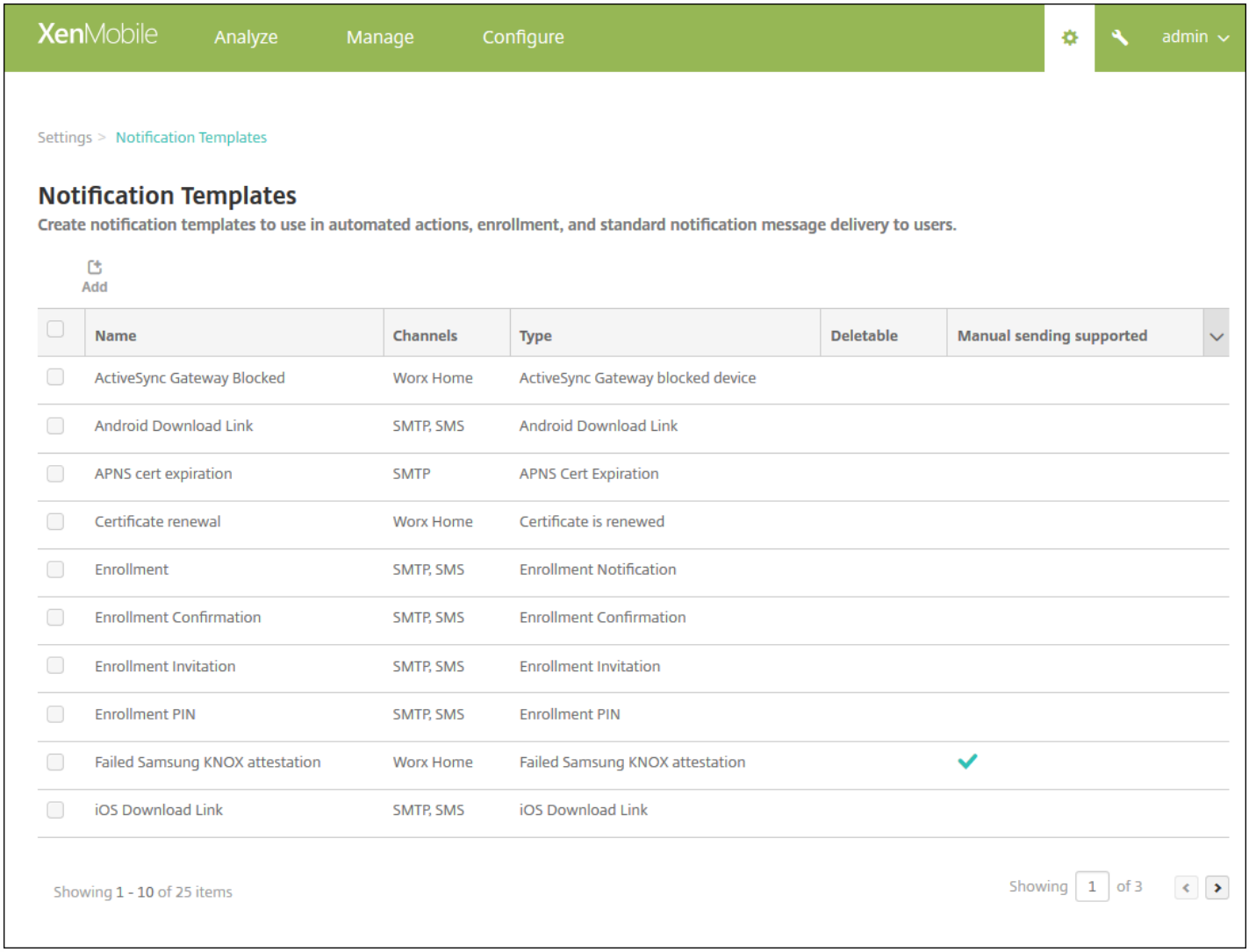
XenMobile comprend plusieurs modèles de notification prédéfinis qui reflètent les différents types d'événements auxquels XenMobile répond automatiquement pour chaque appareil dans le système.

Remarque : si vous prévoyez d'utiliser les canaux SMTP ou SMS pour envoyer des notifications aux utilisateurs, vous devez

définir les canaux avant de pouvoir les activer. XenMobile vous invite à configurer les canaux lorsque vous ajoutez des modèles de notification s'ils ne sont pas déjà configurés.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Modèles de notification**. La page **Modèles de notification** s'affiche.



Pour ajouter un modèle de notification

1. Cliquez sur **Add**. Si aucune passerelle SMS ou aucun serveur SMTP n'a été défini, un message s'affiche relatif à l'utilisation des notifications SMS et SMTP. Vous pouvez choisir de configurer le serveur SMTP ou la passerelle SMS maintenant ou les configurer les plus tard.

Si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP maintenant, vous serez redirigé vers la page **Serveur de notification** sur la page **Paramètres**. Après avoir configuré les canaux que vous souhaitez utiliser, vous pouvez retourner sur la page **Modèle de notification** pour continuer à ajouter ou modifier des modèles de notification.

> Important

si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP ultérieurement, vous ne pourrez pas activer ces canaux lorsque vous ajoutez ou modifiez un modèle de notification, ce qui signifie que ces canaux ne seront pas disponibles pour l'envoi de notifications aux utilisateurs.

2. Pour configurer ces paramètres :

- **Nom** : entrez un nom descriptif pour le modèle.
- **Description** : entrez une description pour le modèle.
- **Type** : dans la liste, cliquez sur le type de notification. Seuls les canaux pris en charge pour le type sélectionné s'affichent. Seul un modèle de type Expiration du certificat APNS est autorisé, qui est un modèle prédéfini. Cela signifie que vous ne pouvez pas ajouter un nouveau modèle de ce type.

Remarque : pour certains types de modèle, la phrase Envoi manuel pris en charge s'affiche en dessous du type. Cela signifie que le modèle est disponible dans la liste **Notifications** sur le **tableau de bord** et sur la page **Appareils** et que vous pouvez envoyer manuellement la notification aux utilisateurs. L'envoi manuel n'est disponible dans aucun des modèles qui utilisent les macros suivantes dans le champ Sujet ou Message d'un canal :

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

3. Sous **Canaux**, entrez ou modifiez les informations pour chaque canal à utiliser avec cette notification. Vous pouvez choisir un ou tous les canaux. Le canal que vous choisissez dépend de la façon dont vous souhaitez envoyer des notifications :

- Si vous choisissez **Secure Hub**, seuls les appareils iOS et Android reçoivent des notifications ; elles apparaissent dans la barre de notification de l'appareil.
- Si vous choisissez **SMTP**, la plupart des utilisateurs recevront le message, car ils se sont inscrits avec leurs adresses e-mail.
- Si vous choisissez **SMS**, seuls les utilisateurs d'appareils équipés d'une carte SIM reçoivent la notification.

Secure Hub :

- **Activer** : cliquez pour activer le canal de notification.
- **Message** : entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez Secure Hub.
- **Fichier son** : dans la liste, cliquez sur le son de notification que l'utilisateur entend lorsque la notification est reçue.

SMTP :

- **Activer** : cliquez pour activer le canal de notification.

  Important : vous ne pouvez activer la notification SMTP que si vous avez déjà configuré le serveur SMTP.

- **Expéditeur** : entrez un expéditeur (facultatif) pour la notification, qui peut être un nom, une adresse e-mail, ou les deux.
- **Destinataire** : ce champ contient une macro préconfigurée pour toutes les notifications sauf les notifications Ad-Hoc pour garantir l'envoi des notifications à l'adresse de destinataire SMTP correcte. Citrix vous recommande de ne pas modifier les macros dans les modèles. Vous pouvez également ajouter des destinataires (par exemple, l'administrateur d'entreprise), en plus de l'utilisateur en ajoutant leurs adresses séparées par un point-virgule (;). Pour envoyer des notifications ad hoc, vous pouvez entrer des destinataires spécifiques sur cette page, ou vous pouvez sélectionner des appareils à partir de la page **Gérer** > **Appareils** et envoyer des notifications à partir de cet emplacement. Pour de plus amples informations, consultez la section Appareils.

- **Sujet** : entrez un sujet pour la notification. Ce champ est obligatoire.
- **Message** : entrez le message à envoyer à l'utilisateur.

SMS :

- **Activer** : cliquez pour activer le canal de notification.

  Important : vous ne pouvez activer la notification SMS que si vous avez déjà configuré la passerelle SMS.

- **Destinataire** : ce champ contient une macro préconfigurée pour toutes les notifications sauf les notifications Ad-Hoc pour garantir l'envoi des notifications à l'adresse de destinataire SMS correcte. Citrix vous recommande de ne pas modifier les macros dans les modèles. Pour envoyer des notifications ad hoc, vous pouvez entrer des destinataires spécifiques, ou vous pouvez sélectionner des appareils à partir de la page **Gérer** > **Appareils**.
- **Message** : entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire.

5. Cliquez sur **Ajouter**. Lorsque tous les canaux sont correctement configurés, ils apparaissent dans cet ordre sur la page **Modèles de notification** : SMTP, SMS et Secure Hub. Tout canal qui n'est pas correctement configuré apparaît après les canaux correctement configurés.

Pour modifier un modèle de notification

1. Sélectionnez un modèle de notification. La page de modification spécifique à ce modèle apparaît dans lequel vous pouvez apporter des modifications à tous les champs sauf **Type**, ainsi qu'activer ou désactiver l'utilisation de canaux.

2. Cliquez sur **Enregistrer**.

Pour supprimer un modèle de notification

Remarque : vous ne pouvez supprimer que les modèles de notification que vous avez ajoutés ; vous ne pouvez pas supprimer des modèles de notification prédéfinis.

1. Sélectionnez un modèle de notification.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche.

3. Cliquez sur **Supprimer** pour supprimer le modèle de notification, ou cliquez sur **Annuler** pour annuler la suppression du modèle de notification.

Appareils

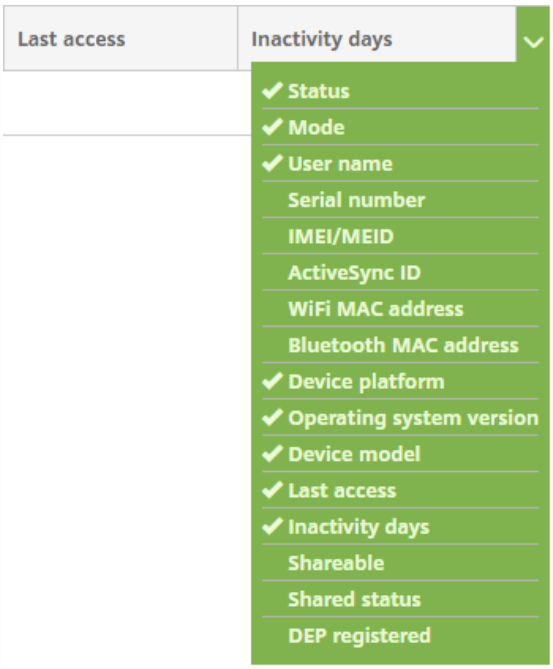
Mar 31, 2017

La base de données du serveur XenMobile stocke une liste des appareils mobiles. Un numéro de série unique ou un numéro IMEI (identité internationale d'équipement mobile)/MEID (identifiant de l'équipement mobile) identifie chaque appareil mobile de manière unique. Pour renseigner la console XenMobile avec vos appareils, vous pouvez ajouter les appareils manuellement ou importer une liste d'appareils à partir d'un fichier. Consultez la section Formats des fichiers de provisioning pour de plus amples informations sur les formats de fichier de provisioning.

La page **Appareils** de la console XenMobile répertorie chaque appareil et les informations suivantes :

- **État** (les icônes indiquent si l'appareil est jailbreaké, géré, si Active Sync Gateway est disponible et l'état du déploiement)
- **Mode** (indique le mode de l'appareil, à savoir MDM, MAM ou les deux)
- D'autres informations sur l'appareil : **Nom d'utilisateur**, **Plate-forme de l'appareil**, **Version du système d'exploitation**, **Modèle d'appareil**, **Dernier accès** et **Jours d'inactivité**. Les en-têtes affichés sont les en-têtes par défaut.

Pour personnaliser le tableau **Appareils**, cliquez sur la flèche vers le bas sur le dernier en-tête, puis sélectionnez les en-têtes supplémentaires que vous voulez voir dans le tableau ou supprimez ceux que vous ne souhaitez pas voir.



Vous pouvez ajouter des appareils manuellement, importer des appareils à partir d'un fichier de provisioning, modifier les détails de l'appareil, exécuter des actions de sécurité, envoyer des notifications aux appareils et supprimer des appareils. Vous pouvez également exporter toutes les données de tableau d'un appareil dans un fichier .csv pour créer un rapport personnalisé. Le serveur exporte tous les attributs de l'appareil et si vous appliquez des filtres, XenMobile les utilise lors de la création du fichier .csv.

Consultez les sections suivantes pour plus d'informations sur la gestion des appareils :

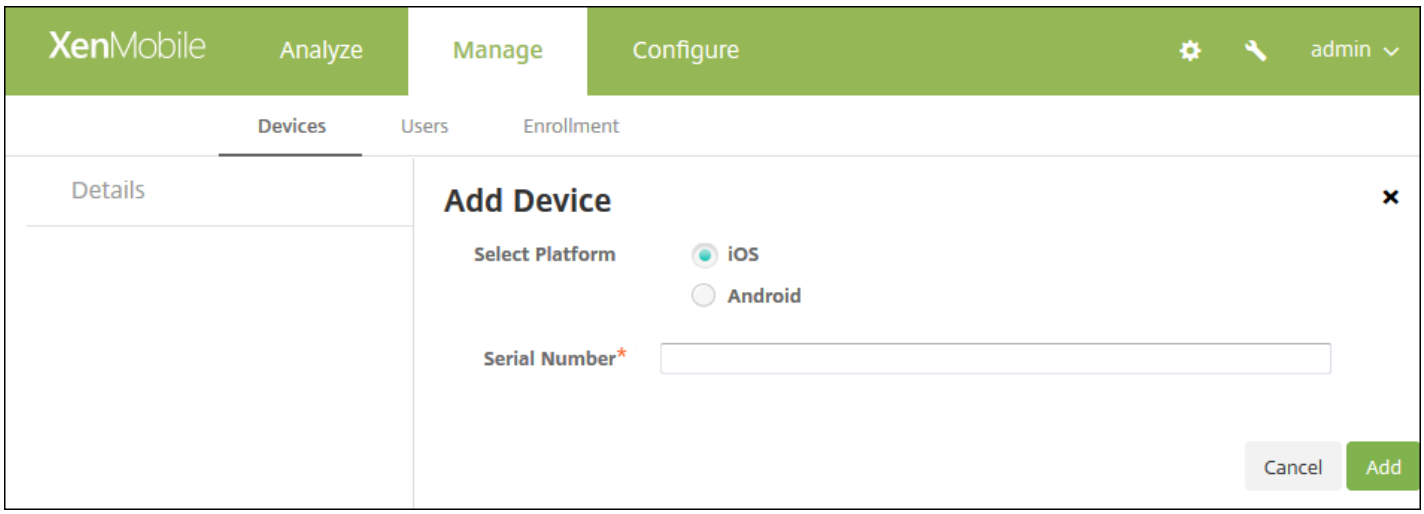
- Ajouter un appareil manuellement
- Importer des appareils à partir d'un fichier de provisioning

- Exécuter des actions de sécurité
- Envoyer une notification aux appareils
- Supprimer des appareils
- Exporter le tableau Appareils
- Identifier les appareils utilisateur manuellement
- Formats des fichiers de provisioning
- Noms et valeurs des propriétés d'appareil

Ajouter un appareil manuellement

1. Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

2. Cliquez sur **Ajouter**.La page **Ajouter un appareil** s'affiche.



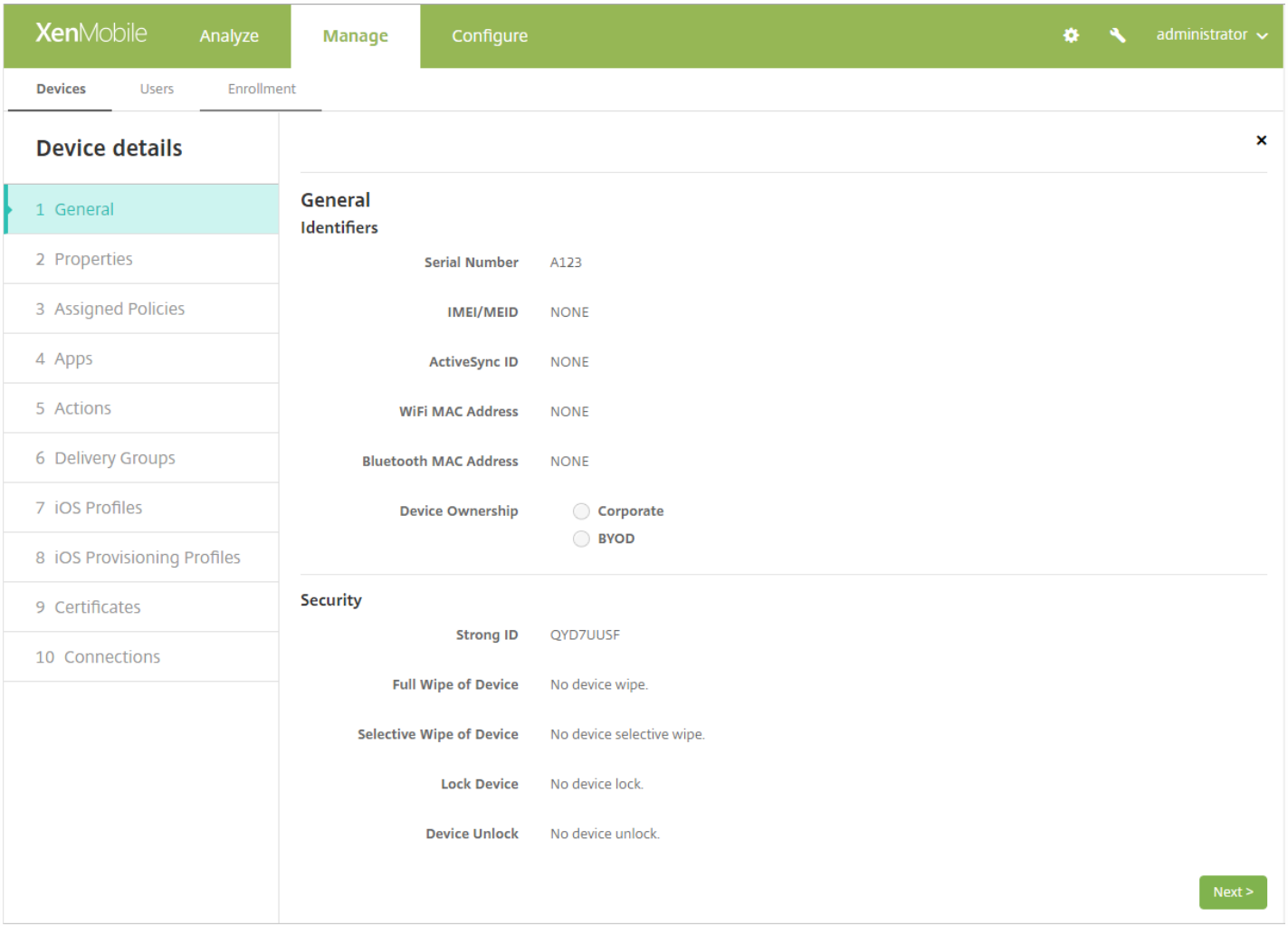
3. Pour configurer ces paramètres :

- **Sélectionner une plate-forme** : cliquez sur **iOS** ou **Android**.
- **Numéro de série** : entrez le numéro de série de l'appareil.
- **IMEI/MEID** : pour les appareils Android uniquement, entrez les informations IMEi/MEID de l'appareil (facultatif).

4. Cliquez sur **Ajouter**.Le tableau **Appareils** s'affiche avec l'appareil ajouté en bas de la liste. Dans la liste, sélectionnez l'appareil que vous avez ajouté, puis dans le menu qui s'affiche, cliquez sur **Modifier** pour afficher et confirmer les détails de

l'appareil.

Remarque : lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



5. La page **Général** dresse la liste des **identificateurs**, tels que le numéro de série, l'ID ActiveSync et d'autres informations relatives au type de plate-forme. Pour **Propriétaire**, sélectionnez **Entreprise** ou **BYOD**.

La page **Général** dresse également la liste des propriétés de **sécurité**, telles que ID fort, Verrouiller l'appareil, Contourner le verrouillage d'activation et d'autres informations relatives au type de plate-forme.

6. La page **Propriétés** dresse la liste des propriétés d'appareil que XenMobile va provisionner. Cette liste affiche toutes les propriétés d'appareil incluses dans le fichier de provisioning utilisé pour ajouter l'appareil. Pour ajouter une propriété, cliquez sur **Ajouter**, puis sélectionnez une propriété dans la liste. Pour connaître les valeurs valides pour chaque propriété, consultez la section Valeurs et noms des propriétés d'appareil dans cet article.

Lorsque vous ajoutez une propriété, elle s'affiche initialement sous la catégorie dans laquelle vous l'avez ajoutée. Après avoir cliqué sur **Suivant** et être revenu sur la page **Propriétés**, la propriété s'affiche dans la liste appropriée.

Pour supprimer une propriété, placez le curseur dessus et cliquez sur le **X** sur le côté droit. XenMobile supprime l'élément immédiatement.

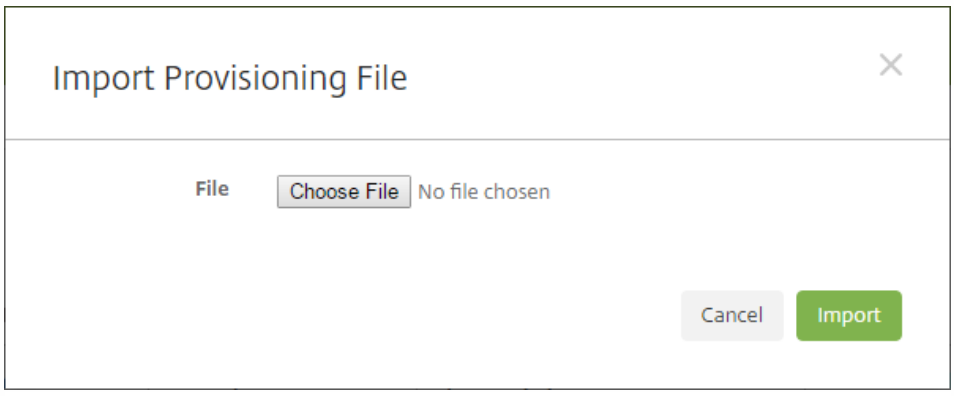
7. Les sections **Détails de l'appareil** restantes contiennent des informations sommaires sur l'appareil.

- **Stratégies attribuées** : affiche le nombre des stratégies attribuées, y compris le nombre de stratégies déployées, en attente ou ayant échoué. Fournit les informations relatives au nom, au type et à la dernière date de déploiement pour chaque stratégie.
- **Applications** : affiche, pour le dernier inventaire, le nombre d'applications installées, en attente et ayant échoué. Fournit le nom de l'application, l'identificateur, le type et d'autres informations.
- **Actions** : affiche le nombre d'actions déployées, en attente et qui ont échoué. Fournit le nom de l'action et l'heure du dernier déploiement.
- **Groupes de mise à disposition** : affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Pour chaque déploiement, fournit le nom du groupe mise à disposition et l'heure déploiement. Sélectionnez un groupe de mise à disposition pour afficher des informations plus détaillées, y compris l'état, l'action, le canal ou l'utilisateur.
- **Profils iOS** : affiche le dernier inventaire de profil iOS, y compris le nom, le type, l'organisation et une description.
- **Profils de provisioning iOS** : affiche les informations du profil de provisioning de distribution d'entreprise, telles que l'UUID, la date d'expiration, et si les profils sont gérés ou non gérés.
- **Certificats** : affiche pour les certificats valides, révoqués ou ayant expiré, des informations telles que le type, le fournisseur, l'émetteur, le numéro de série et le nombre de jours restants avant l'expiration.
- **Connexions** : affiche l'état de la première connexion et de la dernière connexion. Fournit pour chaque connexion, le nom d'utilisateur, l'heure de l'avant-dernière authentification et l'heure de la dernière authentification.
- **TouchDown** (appareils Android uniquement) : affiche des informations sur la dernière authentification de l'appareil et le dernier utilisateur à s'être authentifié. Fournit chaque nom de stratégie et valeur de stratégie applicables.

Importer des appareils à partir d'un fichier de provisioning

Vous pouvez importer un fichier fourni par les opérateurs mobiles ou les fabricants de l'appareil, ou vous pouvez créer votre propre fichier de provisioning. Pour plus d'informations, consultez la section Formats des fichiers de provisioning dans cet article.

1. Accédez à **Gérer > Appareils** et cliquez sur **Importer**. La boîte de dialogue **Importer le fichier de provisioning** apparaît.



2. Cliquez sur **Choisir un fichier** et accédez au fichier que vous souhaitez importer.

3. Cliquez sur **Importer**. Le tableau **Appareils** répertorie le fichier importé.

4. Pour modifier les informations sur l'appareil, sélectionnez-le, puis cliquez sur **Modifier**. Pour plus d'informations sur les pages **Détails de l'appareil**, consultez la section Ajouter un appareil manuellement.

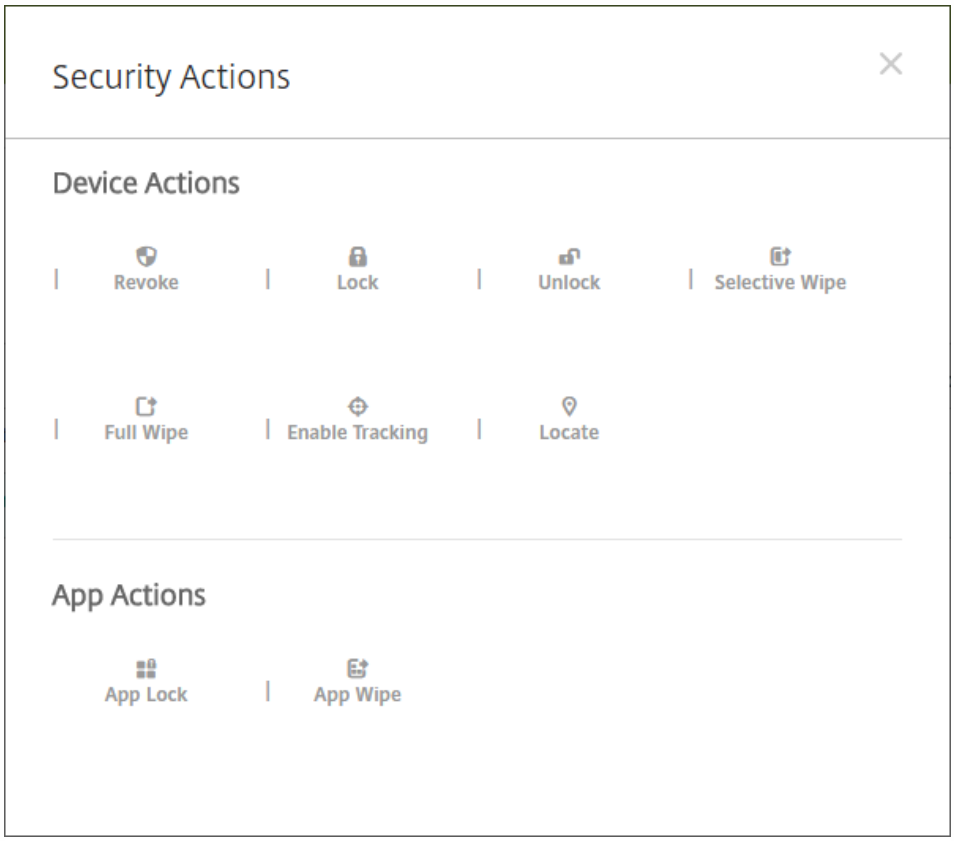
Exécuter des actions de sécurité

Vous pouvez exécuter des actions de sécurité au niveau de l'application et de l'appareil à partir de la page **Appareil**. Vous pouvez exécuter les actions suivantes sur l'appareil : révoquer, verrouiller, déverrouiller et effacer. Vous pouvez exécuter les actions de sécurité suivantes sur les applications : mode kiosque (verrouillage des applications) et effacement des applications.

1. Sur la page **Gérer > Appareils**, sélectionnez un appareil et cliquez sur **Sécurisé**.

2. Dans **Actions de sécurisation**, cliquez sur une action et suivez les invites.

Pour de plus amples informations sur les actions, consultez la section Actions automatisées.



Pour verrouiller, déverrouiller, effacer ou annuler l'effacement d'une application manuellement

1. Accédez à **Gérer** > **Appareils**, sélectionnez un appareil géré et cliquez sur **Sécurisé**.

2. Dans la boîte de dialogue **Actions de sécurisation**, cliquez sur une action.

Remarque : vous pouvez également utiliser cette boîte de dialogue pour vérifier l'état de l'appareil d'un utilisateur dont vous savez qu'il a été désactivé ou supprimé dans Active Directory. La présence des actions Annuler le mode kiosque ou Annuler effacement des applications indique que les applications des utilisateurs sont actuellement verrouillées ou effacées.

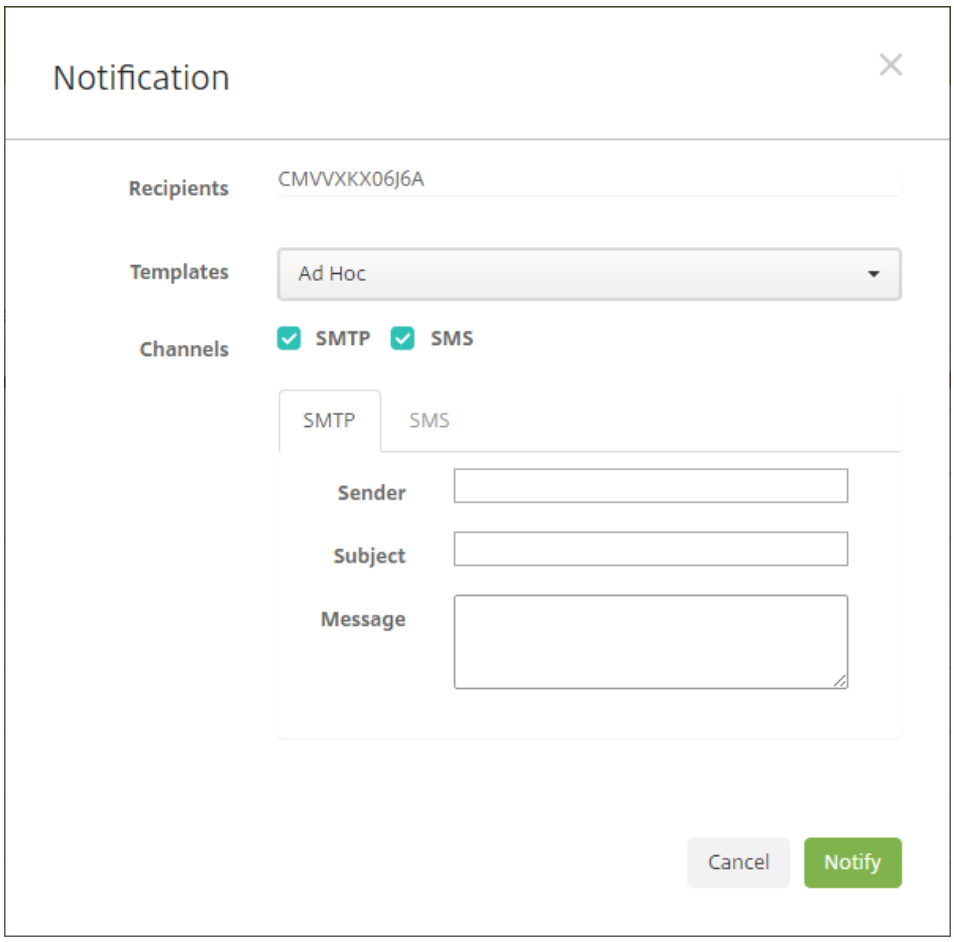
3. Confirmez l'action.

Envoyer une notification aux appareils

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour plus d'informations sur les notifications, veuillez consulter la section Notifications.

1. Sur la page **Gérer > Appareils** sélectionnez l'appareil ou les appareils auxquels vous souhaitez envoyer une notification.

2. Cliquez sur **Notifier**. La boîte de dialogue **Notification** s'affiche. Le champ **Destinataires** répertorie tous les appareils sélectionnés pour recevoir pour la notification.



3. Pour configurer ces paramètres :

- **Modèles** : dans la liste, cliquez sur le type de notification que vous souhaitez envoyer. Pour chaque modèle excepté le modèle **Ad Hoc**, les champs **Sujet** et **Message** sont renseignés avec le texte configuré pour le modèle que vous avez choisi.
- **Canaux** : sélectionnez la méthode à utiliser pour envoyer le message. La valeur par défaut est **SMTP** et **SMS**. Cliquez sur les onglets pour afficher le format du message pour chaque canal.
- **Expéditeur** : entrez un expéditeur (facultatif).
- **Sujet** : entrez un sujet pour un message **ad hoc**.
- **Message** : entrez le message pour un message **ad hoc**.

4. Cliquez sur **Notifier**.

Supprimer des appareils

1. Dans le tableau **Appareils**, sélectionnez l'appareil ou les appareils que vous voulez supprimer.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer**. vous ne pouvez pas annuler cette opération.

Exporter le tableau Appareils

1. Filtrez le tableau **Appareil** en fonction de ce que vous souhaitez voir apparaître dans le fichier d'exportation.

2. Cliquez sur le bouton **Exporter** au-dessus du tableau **Appareils**. XenMobile extrait les informations du tableau **Appareils** filtré et les convertit en fichier .csv.

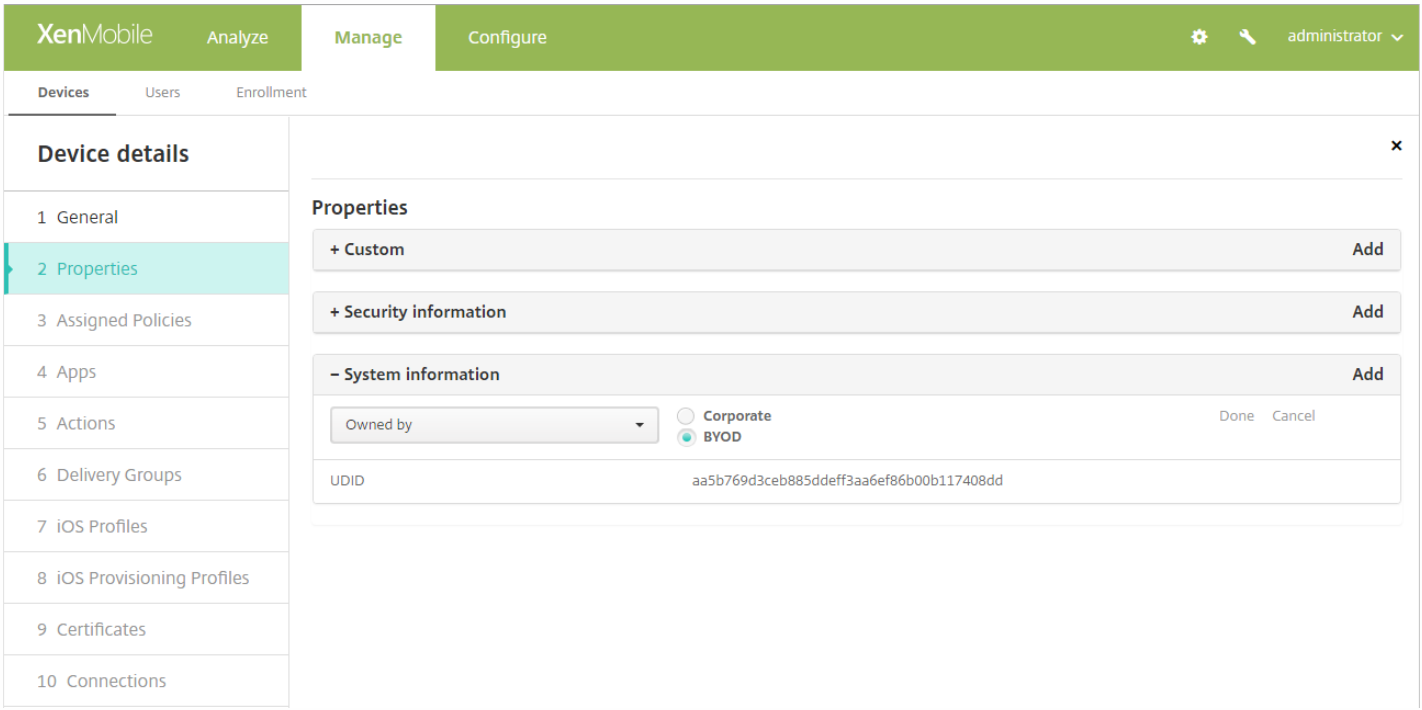
3. Ouvrez ou enregistrez le fichier .csv lorsque vous y êtes invité. Cette opération dépend du navigateur que vous utilisez. Vous pouvez également annuler l'opération.

Identifier les appareils utilisateur manuellement

Vous pouvez manuellement identifier un appareil dans XenMobile de l'une des façons suivantes :

- Durant le processus d'inscription basé sur invitation.
- Durant le processus d'inscription via le portail en libre-service.
- En ajoutant le propriétaire de l'appareil en tant que propriété d'appareil.

Vous avez la possibilité d'identifier l'appareil comme appartenant à la société ou à un employé. Lors de l'utilisation de l'aide du portail d'aide en libre-service pour inscrire un appareil, vous pouvez également identifier l'appareil comme appartenant à la société ou à un employé. Comme indiqué dans la figure suivante, vous pouvez également identifier un appareil manuellement en ajoutant une propriété à l'appareil à partir de l'onglet Appareils dans la console XenMobile, en ajoutant la propriété appelée Appartient à et en choisissant Société ou BYOD (Appartient à l'employé).



Formats des fichiers de provisioning

La plupart des opérateurs mobiles ou des fournisseurs d'appareils fournissent des listes d'appareils mobiles autorisés que vous pouvez utiliser pour éviter d'avoir à entrer manuellement une longue liste d'appareils mobiles. XenMobile prend en charge un format de fichier d'importation commun aux trois types d'appareils pris en charge : Android, iOS et Windows.

Un fichier de provisioning que vous créez manuellement et utilisez pour l'importation d'appareils sur XenMobile doit être au format suivant :

SerialNumber;IMEI;OperatingSystemFamily;propertyName1;propertyValue1;propertyName2;propertyValue2; ... propertyNameN;propertyValueN

Remarques :

- Pour les noms et les valeurs des propriétés, consultez la rubrique « Noms et valeurs des propriétés d'appareil » dans la section suivante.
- Utilisez le jeu de caractères UTF-8.
- Utilisez un point-virgule (;) pour séparer les champs dans le fichier de provisioning. Si une partie d'un champ contient un point-virgule, elle doit être précédée d’une barre oblique inverse (\).

  Par exemple, pour cette propriété :
  propertyV;test;1;2

  Utilisez l'échappement suivant :
  propertyV\;test\;1\;2

- Le numéro de série est requis pour les appareils iOS car le numéro de série est l'identifiant de l'appareil iOS.
- Pour les autres plates-formes, vous devez inclure le numéro de série ou le numéro IMEI.
- Les valeurs valides pour **OperatingSystemFamily** sont : **WINDOWS**, **ANDROID** ou **iOS**.

Exemple de fichier de provisioning d'appareil COPIER

```
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;
```

Chaque ligne du fichier décrit un appareil. La première entrée dans l'exemple ci-dessus signifie :

- SerialNumber : 1050BF3F517301081610065510590391
- IMEI : 15244201625379901
- OperatingSystemFamily : WINDOWS
- PropertyName : propertyN
- PropertyValue : propertyV\;test\;1\;2;prop 2

Noms et valeurs des propriétés d'appareil

Nom de propriété dans la page Gérer > Appareils	Nom et valeurs du fichier de provisioning d'appareil	Type de valeur
AIK présent ?	WINDOWS_HAS_AIK_PRESENT	Chaîne
Compte suspendu ?	GOOGLE_AW_DIRECTORY_SUSPENDED	Chaîne
Code de contournement du verrouillage d'activation	ACTIVATION_LOCK_BYPASS_CODE	Chaîne
Verrouillage d'activation activé	ACTIVATION_LOCK_ENABLED Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Compte iTunes actif	ACTIVE_ITUNES Valeurs (signification) : 1 (oui) 0 (non)	Booléen
ID ActiveSync	EXCHANGE_ACTIVESYNC_ID	Chaîne
Appareil ActiveSync connu par MSP	AS_DEVICE_KNOWN_BY_ZMSP Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Administrateur désactivé	ADMIN_DISABLED Valeurs (signification) : 1 (oui) 0 (non)	Booléen
API Amazon MDM disponible	AMAZON_MDM Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
ID d'appareil Android for Work	GOOGLE_AW_DEVICE_ID	Chaîne

Appareil Android for Work activé ?	GOOGLE_AW_ENABLED_DEVICE	Chaîne
Type d'installation Android for Work	GOOGLE_AW_INSTALL_TYPE Valeurs : DeviceAdministrator (Propriétaire de l'appareil) AvengerManagedProfile (Appareil géré de travail) ManagedProfile (Profil de travail)	Chaîne
Numéro d'identification	ASSET_TAG	Chaîne
État de la mise à jour automatique	AUTOUPDATE_STATUS	Chaîne
RAM disponible	MEMORY_AVAILABLE	Nombre entier
Espace de stockage disponible	TOTAL_DISK_SPACE	Nombre entier
Infos du BIOS	BIOS_INFO	Chaîne
Batterie de secours	BACKUP_BATTERY_PERCENT	Nombre entier
Version du firmware radio	MODEM_FIRMWARE_VERSION	Chaîne
État de la batterie	BATTERY_STATUS	Chaîne
Batterie en charge	BATTERY_CHARGING Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Appareil Bes connu par MSP	BES_DEVICE_KNOWN_BY_ZMSP Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Code PIN BES	BES_PIN	Chaîne

ID de l'agent du serveur BES	ENROLLMENT_AGENT_ID	Chaîne
Nom du serveur BES	BES_SERVER	Chaîne
Version du serveur BES	BES_VERSION	Chaîne
État BitLocker	WINDOWS_HAS_BIT_LOCKER_STATUS	Chaîne
Adresse MAC Bluetooth	BLUETOOTH_MAC	Chaîne
Débogage du démarrage activé ?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED	Chaîne
Version de la liste de révision du Gestionnaire de démarrage	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION	Chaîne
Fréquence du processeur	CPU_CLOCK_SPEED	Nombre entier
Type de processeur	CPU_TYPE	Chaîne
Version des paramètres opérateur	CARRIER_SETTINGS_VERSION	Chaîne
Cellulaire - Latitude	GPS_LATITUDE_FROM_CELLULAR	Chaîne
Cellulaire - Longitude	GPS_LONGITUDE_FROM_CELLULAR	Chaîne
Technologie cellulaire	CELLULAR_TECHNOLOGY	Nombre entier
Cellulaire - Horodatage	GPS_TIMESTAMP_FROM_CELLULAR	Date
Changer le mot de passe lors de la prochaine connexion ?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN	Chaîne
ID de l'appareil client	CLIENT_DEVICE_ID	Chaîne
Sauvegarde sur cloud activée	CLOUD_BACKUP_ENABLED Valeurs (signification) : 1 (oui)	Booléen

	0 (non)	
Intégrité du code activée ?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED	Chaîne
Version de la liste de révision d'intégrité du code	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION	Chaîne
Couleur	COLOR	Chaîne
Date de création	GOOGLE_AW_DIRECTORY_CREATION_TIME	Chaîne
Réseau de l'opérateur actuel	CURRENT_CARRIER_NETWORK	Chaîne
Indicatif de pays du mobile actuel	CURRENT_MCC	Nombre entier
Code réseau du mobile actuel	CURRENT_MNC	Chaîne
Stratégie DEP	WINDOWS_HAS_DEP_POLICY	Chaîne
Itinérance des données autorisée	DATA_ROAMING_ENABLED Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Date de la dernière sauvegarde iCloud	LAST_CLOUD_BACKUP_DATE	Date
Description	DESCRIPTION	Chaîne
Profil du Programme d'inscription des appareils attribué	PROFILE_ASSIGN_TIME	Date
Profil du Programme d'inscription des appareils envoyé	PROFILE_PUSH_TIME	Date
Profil du Programme d'inscription des appareils supprimé	PROFILE_REMOVE_TIME	Date
Enregistrement au Programme d'inscription des appareils au plus tard	DEVICE_ASSIGNED_BY	Chaîne

Date d'enregistrement au Programme d'inscription des appareils	DEVICE_ASSIGNED_DATE	Date
Type d'appareil	DEVICE_TYPE	Chaîne
Modèle d'appareil	MODEL_ID	Chaîne
Nom de l'appareil	DEVICE_NAME	Chaîne
Ne pas déranger activé	DO_NOT_DISTURB Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Pilote ELAM chargé ?	WINDOWS_HAS_ELAM_DRIVER_LOADED	Chaîne
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE	Date
ID d'entreprise	ENTERPRISE_ID	Chaîne
Stockage externe 1 : espace disponible	EXTERNAL_STORAGE1_FREE_SPACE	Nombre entier
Stockage externe 1 : nom	EXTERNAL_STORAGE1_NAME	Chaîne
Stockage externe 1 : espace total	EXTERNAL_STORAGE1_TOTAL_SPACE	Nombre entier
Stockage externe 2 : espace disponible	EXTERNAL_STORAGE2_FREE_SPACE	Nombre entier
Stockage externe 2 : nom	EXTERNAL_STORAGE2_NAME	Chaîne
Stockage externe 2 : espace total	EXTERNAL_STORAGE2_TOTAL_SPACE	Nombre entier
Stockage externe chiffré	EXTERNAL_ENCRYPTION Valeurs (signification) :	Booléen

	1 (oui) 0 (non)	
État du pare-feu	FIREWALL_STATUS	Chaîne
Version du firmware	FIRMWARE_VERSION	Chaîne
Première synchronisation	ZMSP_FIRST_SYNC	Date
GPS - Altitude	GPS_ALTITUDE_FROM_GPS	Chaîne
GPS - Latitude	GPS_LATITUDE_FROM_GPS	Chaîne
GPS - Longitude	GPS_LONGITUDE_FROM_GPS	Chaîne
GPS - Horodatage	GPS_TIMESTAMP_FROM_GPS	Date
Alias Google Directory	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS	Chaîne
Nom de famille Google Directory	GOOGLE_AW_DIRECTORY_FAMILY_NAME	Chaîne
Nom Google Directory	GOOGLE_AW_DIRECTORY_NAME	Chaîne
E-mail principal Google Directory	GOOGLE_AW_DIRECTORY_PRIMARY	Chaîne
ID utilisateur Google Directory	GOOGLE_AW_DIRECTORY_USER_ID	Chaîne
HAS_CONTAINER	HAS_CONTAINER Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Version API HTC	HTC_MDM_VERSION	Chaîne
API MDM HTC disponible	HTC_MDM Valeurs (signification) : 1 (oui) 0 (non)	Booléen

Capacités de chiffrement du matériel	HARDWARE_ENCRYPTION_CAPS	Nombre entier
Hash du compte iTunes Store actuellement connecté	ITUNES_STORE_ACCOUNT_HASH	Chaîne
Opérateur de la carte SIM	SIM_CARRIER_NETWORK	Chaîne
Indicatif de pays du mobile domestique	SIM_MCC	Nombre entier
Code réseau de la carte SIM	SIM_MNC	Chaîne
ICCID	ICCID	Chaîne
Numéro IMEI/MEID	IMEI	Chaîne
IMSI	IMSI	Chaîne
Adresse IP	IP_LOCATION	Chaîne
Identité	AS_DEVICE_IDENTITY	Chaîne
Stockage interne chiffré	LOCAL_ENCRYPTION Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Date d'émission	WINDOWS_HAS_ISSUED_AT	Chaîne
Jailbreaké/rooté	ROOT_ACCESS Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Débogage du noyau activé ?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED	Chaîne
Mode Kiosque	IS_KIOSK	Booléen

	Valeurs (signification) : 1 (Vrai) 0 (Faux)	
Dernière adresse IP connue	LAST_IP_ADDR	Chaîne
Dernière date de mise à jour de la stratégie	LAST_POLICY_UPDATE_TIME	Date
Dernière synchronisation	ZMSP_LAST_SYNC	Date
Service de localisation activé	DEVICE_LOCATOR Valeurs (signification) : 1 (oui) 0 (non)	Booléen
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY	Chaîne
MEID	MEID	Chaîne
Configuration de la boîte aux lettres	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP	Chaîne
Batterie principale	MAIN_BATTERY_PERCENT	Nombre entier
Numéro de téléphone	TEL_NUMBER	Chaîne
ID du modèle	SYSTEM_OEM	Chaîne
Type de carte réseau	NETWORK_ADAPTER_TYPE	Chaîne
NitroDesk TouchDown installé	TOUCHDOWN_FIND Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Licence NitroDesk TouchDown activée via MDM	TOUCHDOWN_LICENSED_VIA_MDM Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen

Build du système d'exploitation	SYSTEM_OS_BUILD	Chaîne
Langue du système d'exploitation (paramètres régionaux)	SYSTEM_LANGUAGE	Chaîne
Version du système d'exploitation	SYSTEM_OS_VERSION	Chaîne
Adresse de l'organisation	ORGANIZATION_ADDRESS	Chaîne
E-mail de l'organisation	ORGANIZATION_EMAIL	Chaîne
Organisation Magic	ORGANIZATION_MAGIC	Chaîne
Nom de l'organisation	ORGANIZATION_NAME	Chaîne
N° de tél. de l'organisation	ORGANIZATION_PHONE	Chaîne
Autre	OTHER	Chaîne
Non conforme	OUT_OF_COMPLIANCE Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Appartient à	CORPORATE_OWNED Valeurs (signification) : 1 (Entreprise) 0 (BYOD)	Booléen
PCR0	WINDOWS_HAS_PCR0	Chaîne
Code PIN du géofencing	PIN_CODE_FOR_GEO_FENCE	Chaîne
Code secret conforme	PASSCODE_IS_COMPLIANT Valeurs (signification) : 1 (oui) 0 (non)	Booléen

Code secret conforme à la configuration	PASSCODE_IS_COMPLIANT_WITH_CFG Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Code secret présent	PASSCODE_PRESENT Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Violation du périmètre	GPS_PERIMETER_BREACH Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Personal Hotspot activé	PERSONAL_HOTSPOT_ENABLED Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Plate-forme	SYSTEM_PLATFORM	Chaîne
Niveau d'API de la plate-forme	API_LEVEL	Nombre entier
Nom de la stratégie	POLICY_NAME	Chaîne
Numéro de téléphone principal	IDENTITY1_PHONENUMBER	Chaîne
N° IMEI de la carte SIM principale	IDENTITY1_IMEI	Chaîne
N° IMSI de la carte SIM principale	IDENTITY1_IMSI	Chaîne
Itinérance de la carte SIM principale	IDENTITY1_ROAMING Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Nom du produit	PRODUCT_NAME	Chaîne

ID d'éditeur de l'appareil	PUBLISHER_DEVICE_ID	Chaîne
Nombre de réinitialisations	WINDOWS_HAS_RESET_COUNT	Chaîne
Nombre de redémarrages	WINDOWS_HAS_RESTART_COUNT	Chaîne
Hachage SBCP	WINDOWS_HAS_SBCP_HASH	Chaîne
Prise en charge des SMS	IS_SMS_CAPABLE Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Mode sans échec activé ?	WINDOWS_HAS_SAFE_MODE	Chaîne
API Samsung KNOX disponible	SAMSUNG_KNOX Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Version API Samsung KNOX	SAMSUNG_KNOX_VERSION	Chaîne
Attestation Samsung KNOX	SAMSUNG_KNOX_ATTESTED Valeurs (signification) : 1 (Succès) 0 (Échec)	Booléen
Date de mise à jour de l'attestation Samsung KNOX	SAMSUNG_KNOX_ATT_UPDATED_TIME	Date
API Samsung SAFE disponible	SAMSUNG_MDM Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Version API Samsung SAFE	SAMSUNG_MDM_VERSION	Chaîne

Écran : résolution axe X	SCREEN_XDPI	Entier (PPI)
Écran : résolution axe Y	SCREEN_YDPI	Entier (PPI)
Écran : hauteur	SCREEN_HEIGHT	Entier (pixels)
Écran : nombre de couleurs	SCREEN_NB_COLORS	Nombre entier
Écran : taille	SCREEN_SIZE	Nombre décimal (pouces)
Écran : largeur	SCREEN_WIDTH	Entier (pixels)
Numéro de téléphone secondaire	IDENTITY2_PHONENUMBER	Chaîne
N° IMEI de la carte SIM secondaire	IDENTITY2_IMEI	Chaîne
N° IMSI de la carte SIM secondaire	IDENTITY2_IMSI	Chaîne
Itinérance de la carte SIM secondaire	IDENTITY2_ROAMING Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Démarrage sécurisé activé ?	WINDOWS_HAS_SECURE_BOOT_ENABLED	Chaîne
Conteneur sécurisé activé	WINDOWS_HAS_BIT_LOCKER_STATUS	Chaîne
Numéro de série	SERIAL_NUMBER	Chaîne
API Sony Enterprise disponible	SONY_MDM Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen

Version de l'API Sony Enterprise	SONY_MDM_VERSION	Chaîne
Supervisé	Supervised Valeurs (signification) : 1 (oui) 0 (non)	Booléen
Motif de la suspension	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON	Chaîne
État altéré	TAMPERED_STATUS	Chaîne
Termes et conditions	TERMS_AND_CONDITIONS	Chaîne
Termes et conditions acceptés ?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS	Chaîne
Signature du test activée ?	WINDOWS_HAS_TEST_SIGNING_ENABLED	Chaîne
RAM totale	MEMORY	Nombre entier
Espace de stockage total	FREEDISK	Nombre entier
UDID	UDID	Chaîne
Agent utilisateur	USER_AGENT	Chaîne
Défini par l'utilisateur #1	USER_DEFINED_1	Chaîne
Défini par l'utilisateur #2	USER_DEFINED_2	Chaîne
Défini par l'utilisateur #3	USER_DEFINED_3	Chaîne
Langue de l'utilisateur (paramètres régionaux)	USER_LANGUAGE	Chaîne
VSM activé ?	WINDOWS_HAS_VSM_ENABLED	Chaîne
Fournisseur	VENDOR	Chaîne

Prise en charge de la voix	IS_VOICE_CAPABLE Valeurs (signification) : 1 (Vrai) 0 (Faux)	Booléen
Itinérance voix autorisée	VOICE_ROAMING_ENABLED Valeurs (signification) : 1 (oui) 0 (non)	Booléen
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY	Chaîne
État de la notification WNS	WNS_PUSH_STATUS	Chaîne
URL de notification WNS	PROPERTY_WNS_PUSH_URL	Chaîne
Date d'expiration de l'URL de notification WNS	PROPERTY_WNS_PUSH_URL_EXPIRY	Chaîne
Adresse MAC Wi-Fi	WIFI_MAC	Chaîne
WinPE activé ?	WINDOWS_HAS_WINPE	Chaîne
ID d'agent XenMobile	AGENT_ID	Chaîne
Révision de l'agent XenMobile	EW_REVISION	Chaîne
Version de l'agent XenMobile	EW_VERSION	Chaîne

Verrouiller les appareils iOS

Mar 31, 2017

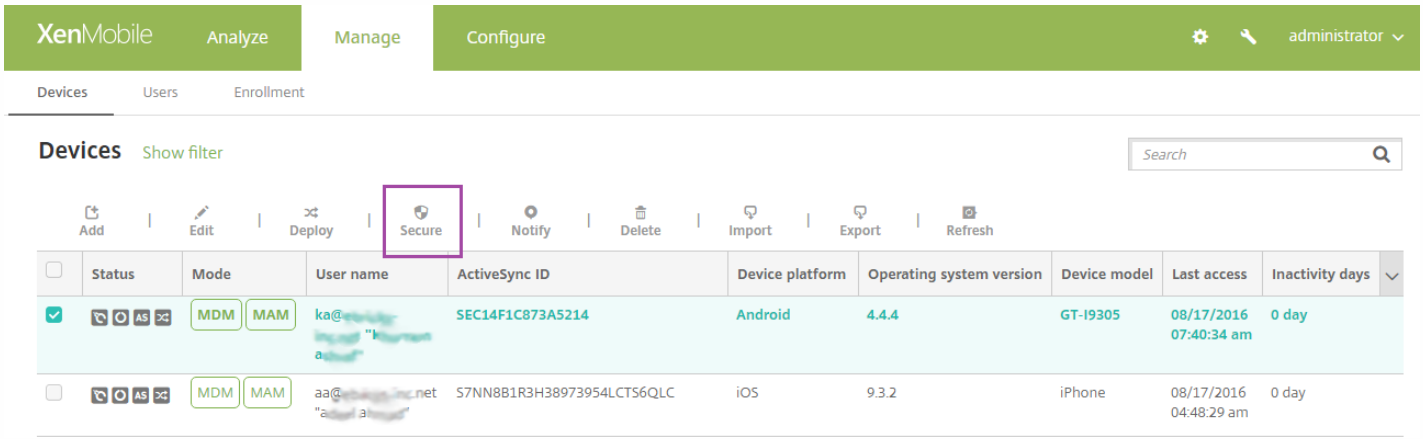
Vous pouvez verrouiller un appareil iOS avec l'affichage d'un message et d'un numéro de téléphone sur l'écran de verrouillage. Cette fonctionnalité est prise en charge sur les appareils exécutant iOS 7 et versions plus récentes.

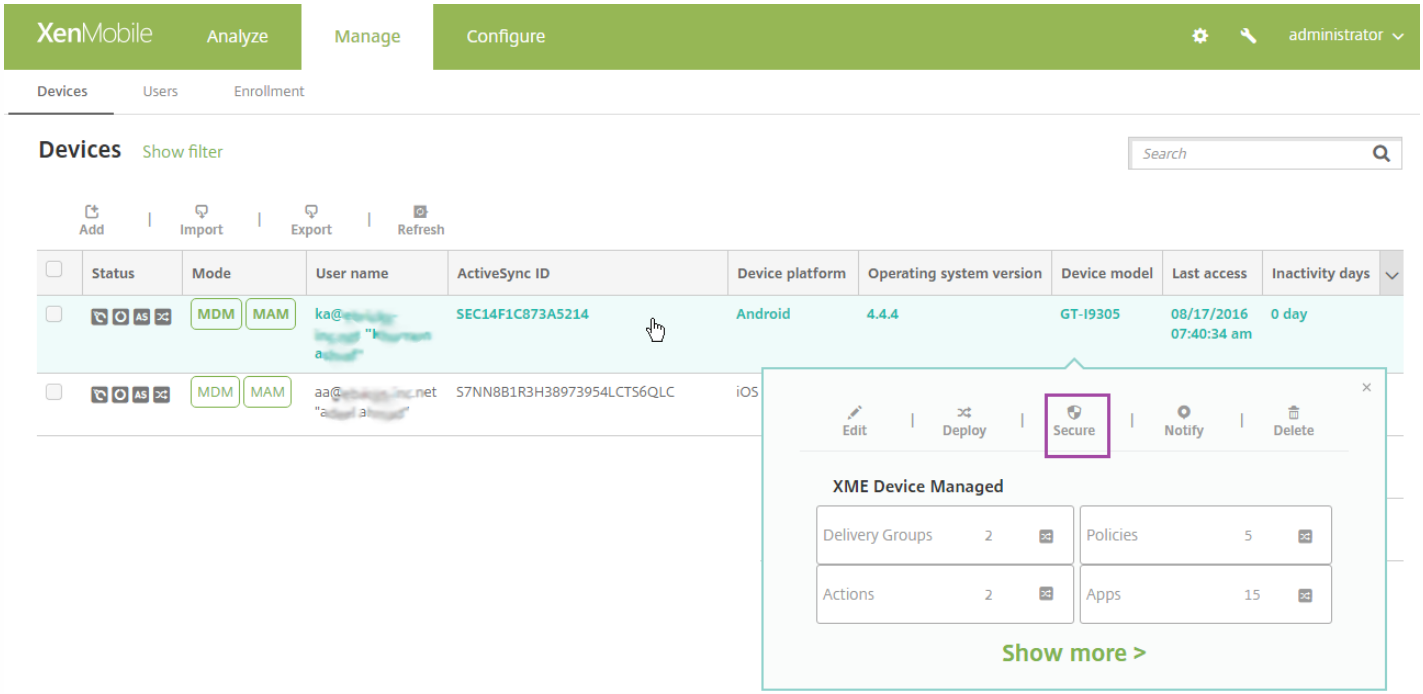
Pour qu'un message et un numéro de téléphone s'affichent sur un appareil verrouillé, la stratégie Code secret doit être définie sur true dans la console XenMobile. Les utilisateurs peuvent également activer la saisie d'un code secret sur l'appareil manuellement.

1. Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'affiche.

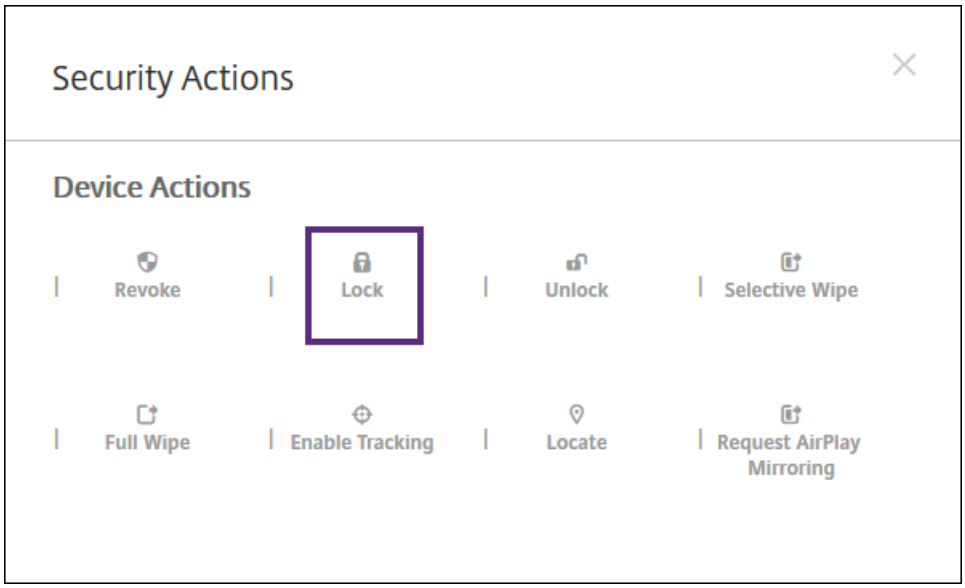
2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

Lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils. Lorsque vous cliquez dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

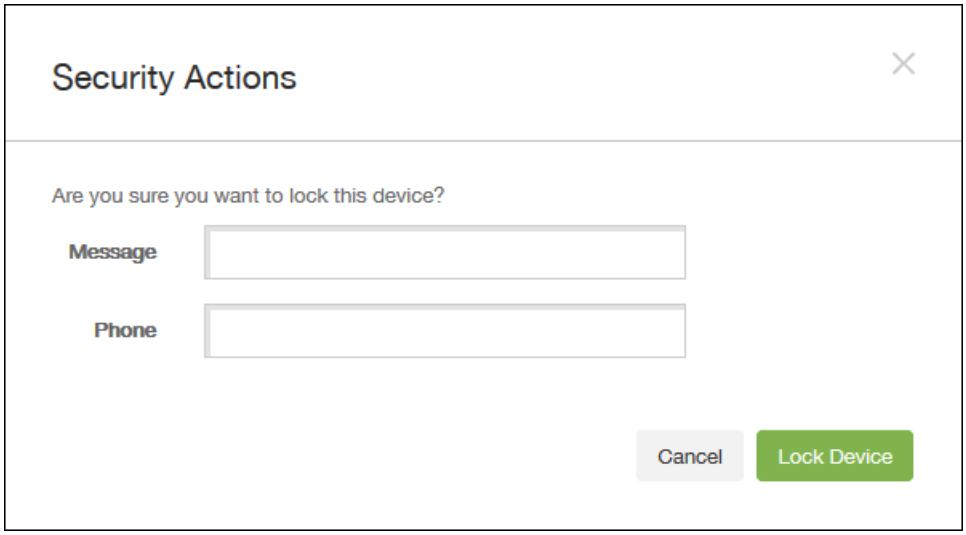




3. Dans le menu d'options, sélectionnez **Sécurisé**. La boîte de dialogue **Actions de sécurisation** s'affiche.



4. Cliquez sur **Verrouiller**. La boîte de dialogue de confirmation **Actions de sécurisation** s'affiche.



5. Si vous le souhaitez, entrez un message et un numéro de téléphone qui s'afficheront sur l'écran de verrouillage de l'appareil.

Pour les iPads exécutant iOS 7 et versions ultérieures : iOS ajoute les mots « iPad perdu » à ce que vous entrez dans le champ **Message**. Pour les iPhones exécutant iOS 7 et versions ultérieures : si vous laissez le champ **Message** vide et que vous entrez un numéro de téléphone, Apple affiche le message « Appeler propriétaire » sur l'écran de verrouillage de l'appareil.

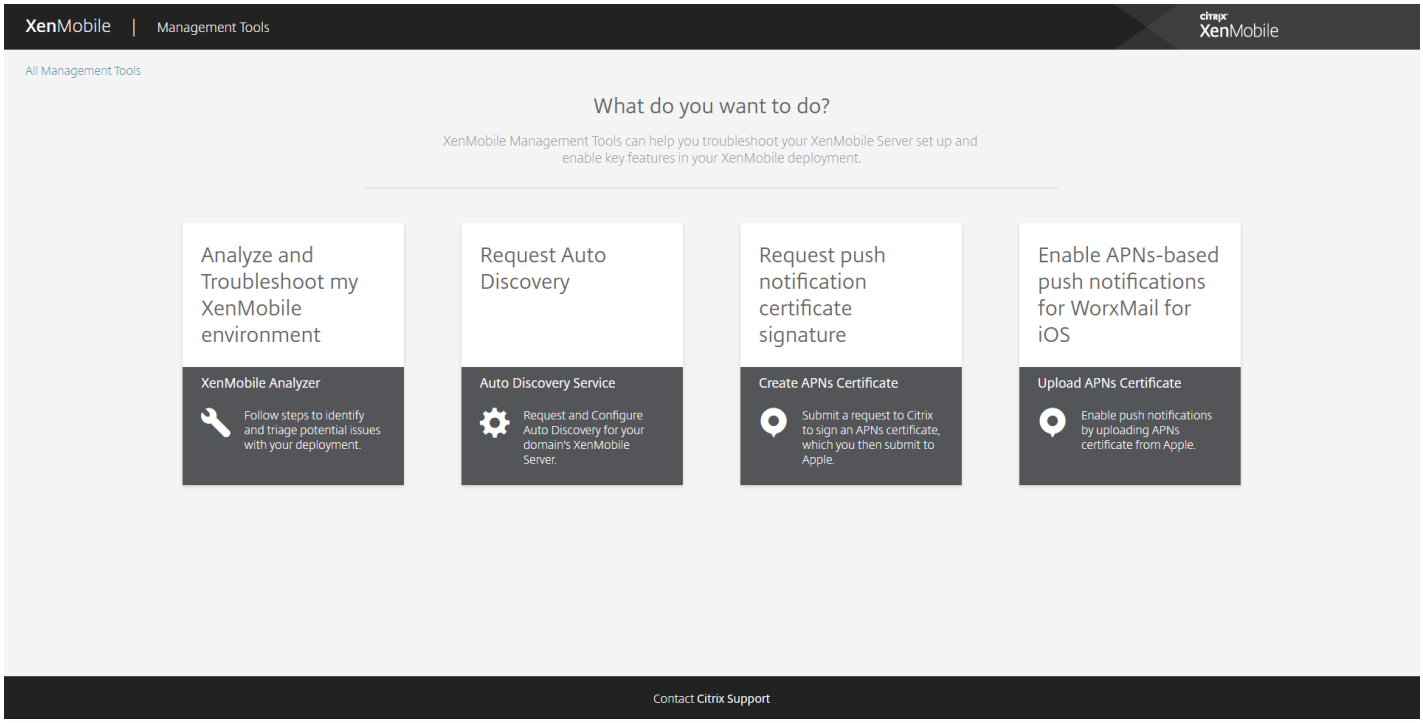
6. Cliquez sur **Verrouiller l'appareil**.

Détection automatique XenMobile

Feb 23, 2017

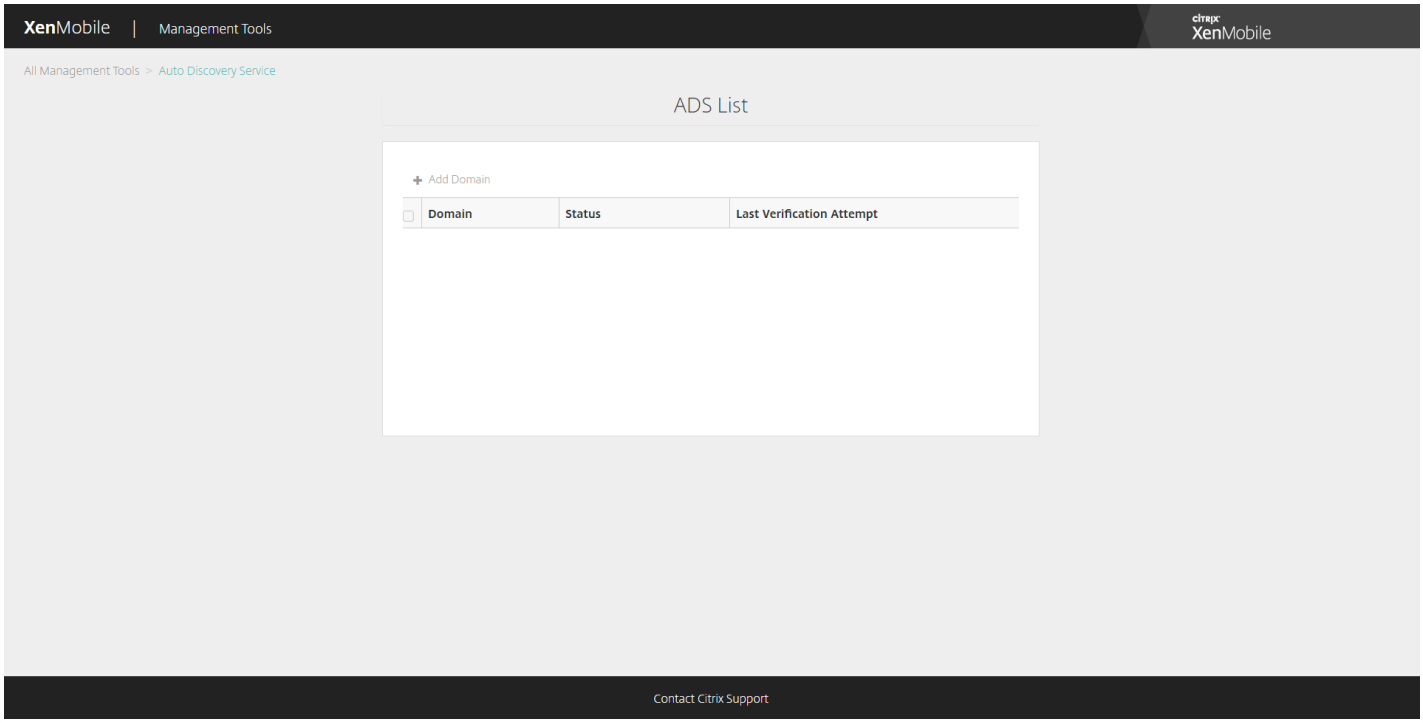
La détection automatique jour un rôle important dans la plupart des déploiements XenMobile. La détection automatique simplifie le processus d'inscription pour les utilisateurs. Ils peuvent utiliser leurs noms d'utilisateur réseau et leurs mots de passe Active Directory pour inscrire leurs appareils, et n'ont pas besoin d'entrer ces détails sur le serveur XenMobile. Le nom d'utilisateur doit être entré au format UPN (nom d'utilisateur principal) ; par exemple, utilisateur@monentreprise.com. XenMobile AutoDiscovery Service vous permet de créer ou de modifier un enregistrement de détection automatique sans l'aide de l'assistance Citrix.

Pour accéder à XenMobile AutoDiscovery Service, accédez à https://xenmobiletools.citrix.com et cliquez sur **Request Auto Discovery**.

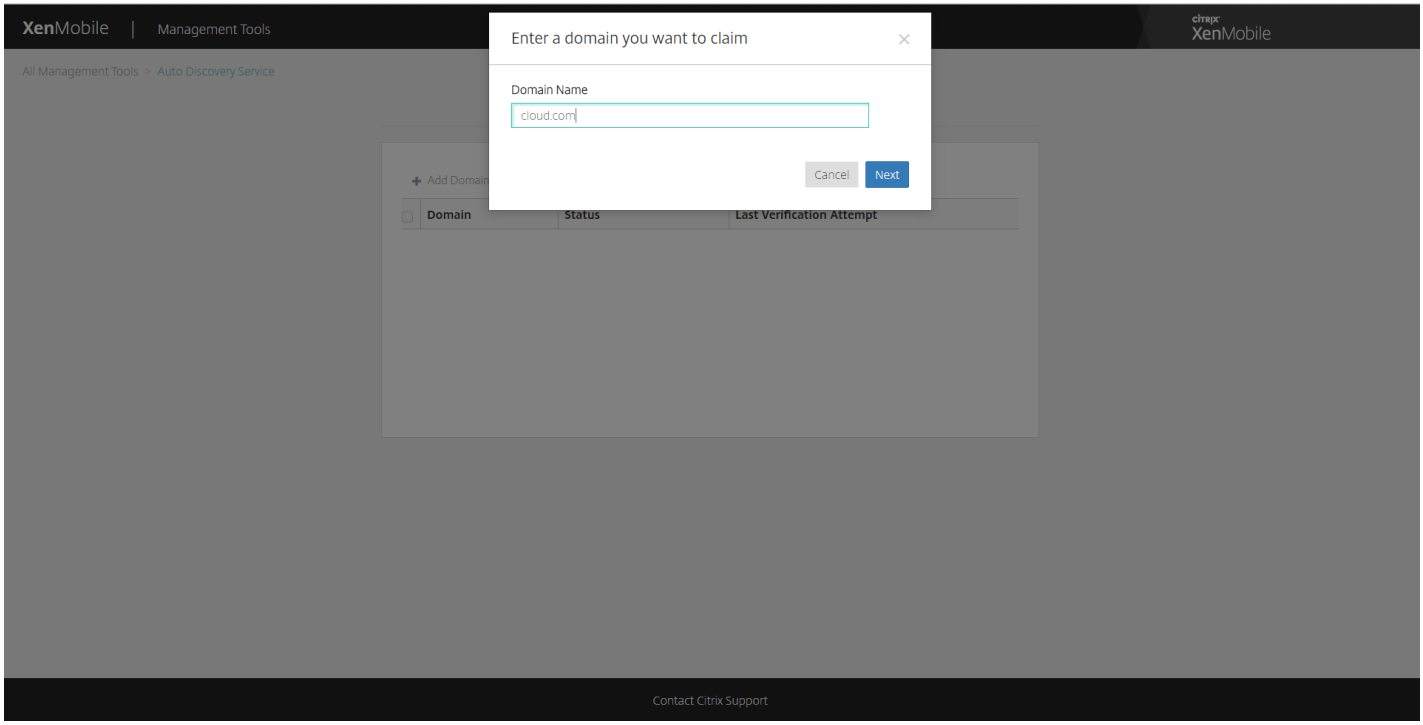


Faire une demande de détection automatique

1. Sur la page AutoDiscovery Service, vous devez d'abord revendiquer un domaine. Cliquez sur **Add Domain**.



2. Dans la boîte de dialogue qui s'affiche, entrez le nom de domaine de votre environnement XenMobile et cliquez sur **Next**.



3. L'étape suivante vous explique comment vérifier que vous êtes le propriétaire du domaine.

a. Copiez le jeton DNS fourni dans le XenMobile Tools Portal.

b. Créez un enregistrement TXT DNS dans le fichier de zone de votre domaine dans le portail Domain Hosting Provider.

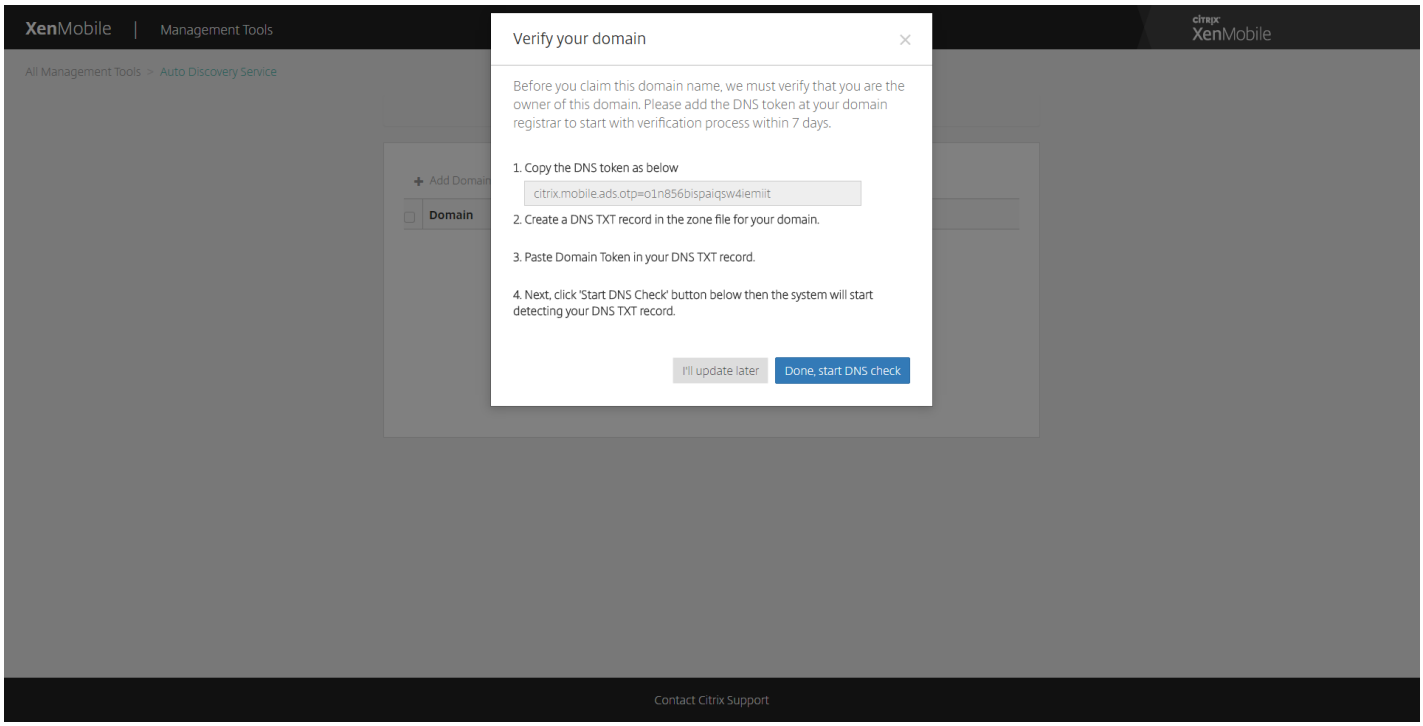
Pour créer un enregistrement TXT DNS, vous devez vous connecter au portail Domain Hosting Provider pour le domaine que vous avez ajouté à l'étape 2 ci-dessus. Dans le portail Domain Hosting, vous pouvez modifier vos enregistrements DNS et ajouter un enregistrement TXT personnalisé. Vous trouverez ci-dessous un exemple d'ajout d'une entrée TXT DNS dans un portail d'hébergement pour le domaine domaine.com.

c. Collez le jeton de domaine dans votre enregistrement TXT DNS et enregistrez votre enregistrement DNS.

d. De retour dans XenMobile Tools Portal, cliquez sur Done et démarrez la vérification du DNS.

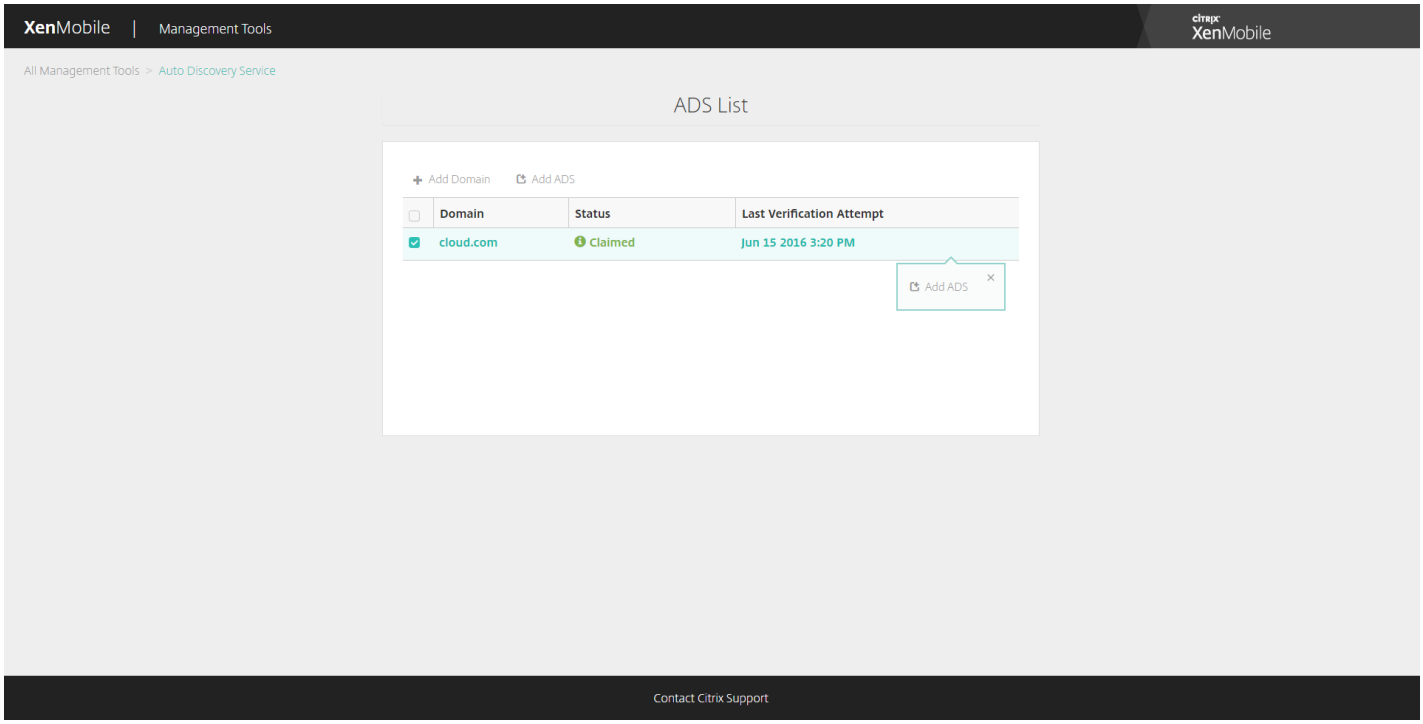
Le système détecte votre enregistrement TXT DNS. Vous pouvez éventuellement cliquer sur I'll update later et l'enregistrement est enregistré. La vérification du DNS ne démarrera pas tant que vous n'avez pas sélectionné l'enregistrement Waiting et cliqué sur DNS Check.

Cette vérification prend généralement une heure, mais le renvoi d'une réponse peut prendre jusqu'à deux jours. En outre, vous devrez peut-être quitter le portail et y retourner pour actualiser l'état.

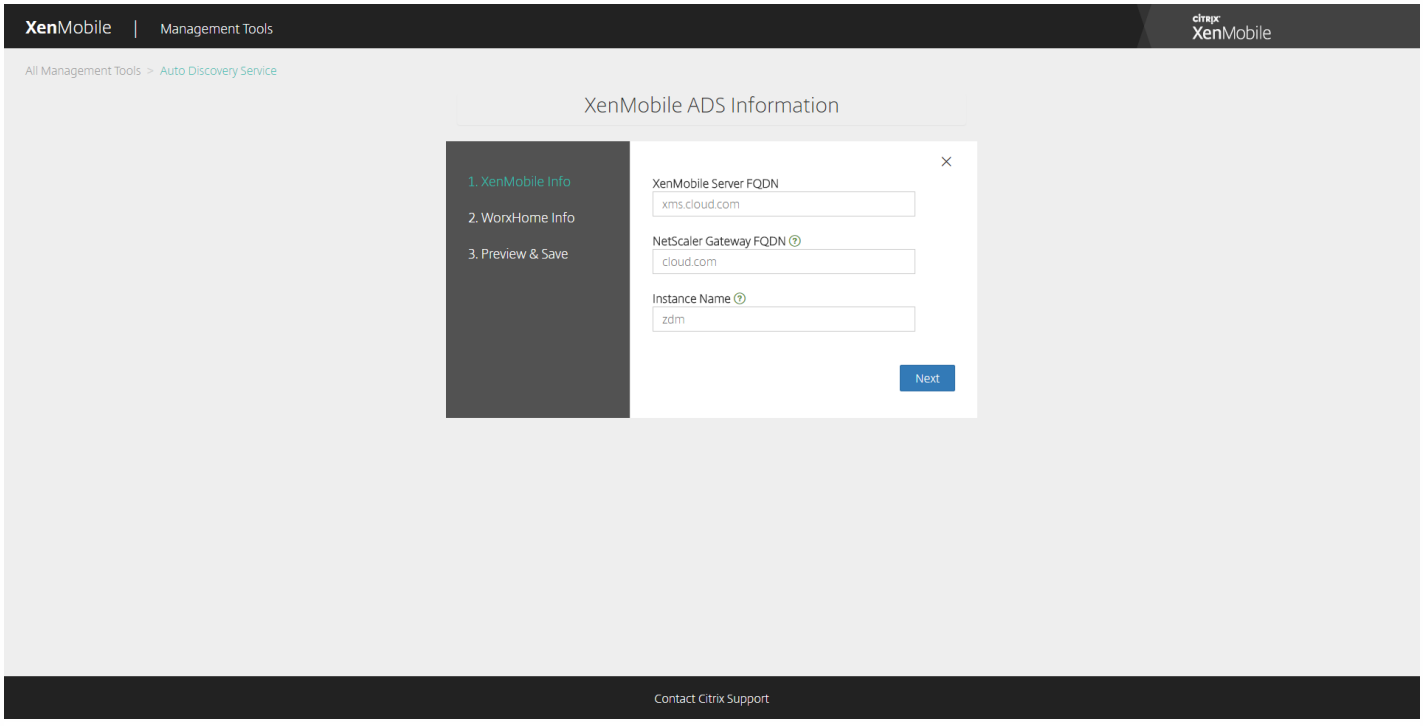


4. Après avoir revendiqué votre domaine, vous pouvez entrer les informations relatives au AutoDiscovery Service. Cliquez avec le bouton droit sur l'enregistrement de domaine pour lequel vous souhaitez faire une demande de détection automatique, puis cliquez sur **Add ADS**.

Si votre domaine dispose déjà d'un enregistrement AutoDiscovery, ouvrez un ticket auprès de l'assistance technique Citrix pour modifier les détails en fonction de vos besoins.



5. Entrez votre **XenMobile Server FQDN**, **NetScaler Gateway FQDN** et **Instance Name**, et cliquez sur **Next**. Si vous le souhaitez, ajoutez une instance par défaut de « zdm ».



Dans l'écran ci-dessus, veuillez noter que Worx Home est maintenant appelé Secure Hub.

6. Entrez les informations suivantes pour Secure Hub et cliquez sur **Next**.

a. **User ID Type** : sélectionnez le type d'ID avec lequel les utilisateurs se connectent, soit **l'adresse e-mail** soit le

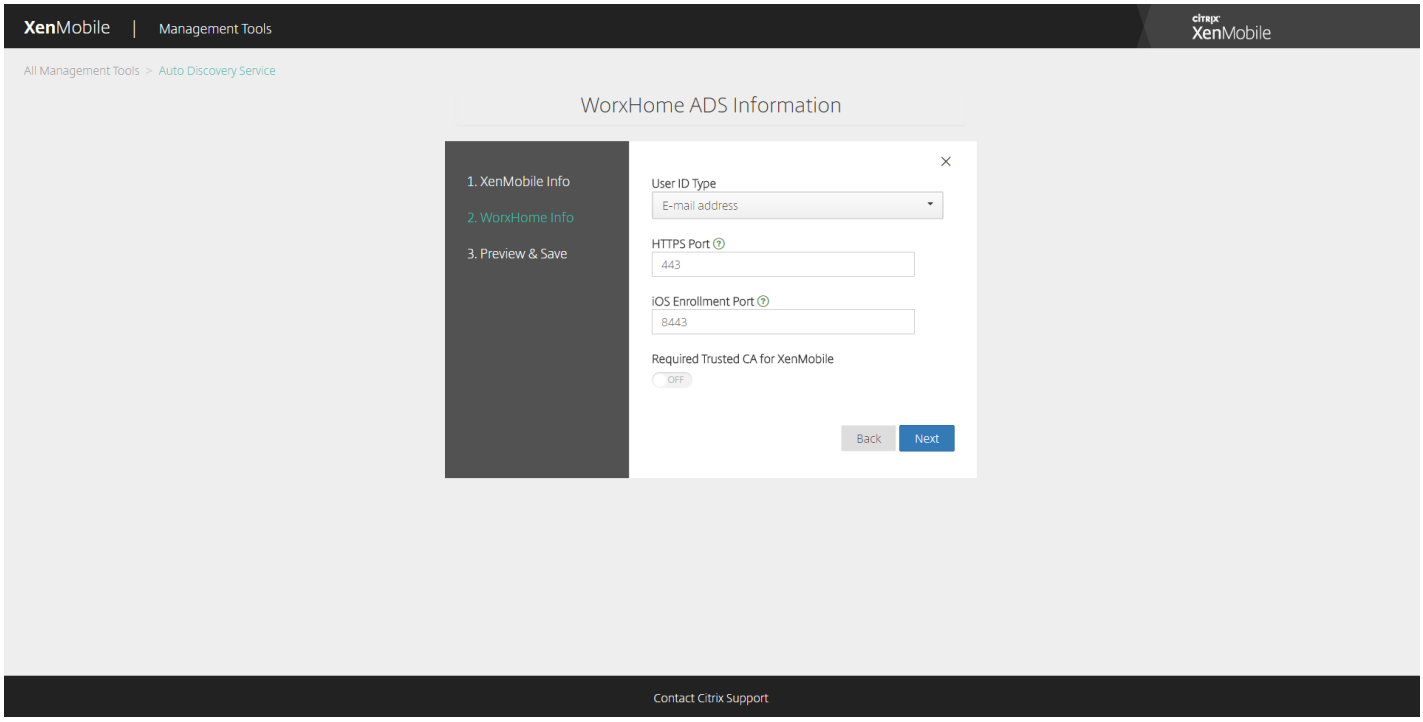
nom **UPN**.

UPN est utilisé lorsque l'UPN (nom d'utilisateur principal) de l'utilisateur est le même que son adresse e-mail. Les deux méthodes utilisent le domaine entré pour trouver l'adresse du serveur. Avec **E-mail address**, les utilisateurs seront invités à entrer leur nom d'utilisateur et mot de passe, et avec **UPN**, ils seront invités à entrer leur mot de passe.

b. **HTTPS Port** : entrez le numéro de port utilisé pour accéder à Secure Hub sur HTTPS. En règle générale, il s'agit du port 443.

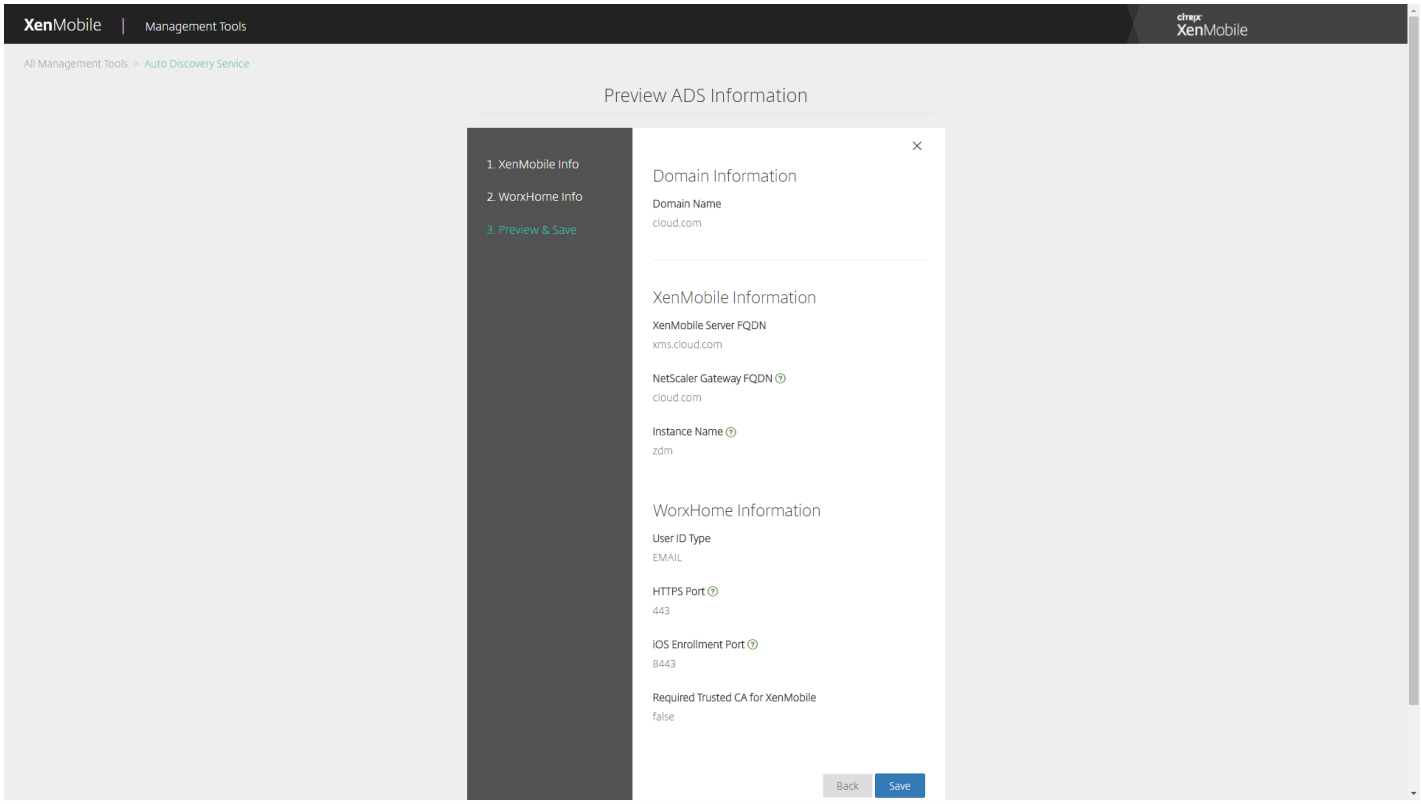
c. **iOS Enrollment Port** : entrez le numéro de port utilisé pour accéder à Secure Hub pour l'inscription iOS. En règle générale, il s'agit du port 8443.

d. **Required Trusted CA for XenMobile** : indiquez si un certificat approuvé est nécessaire pour accéder à XenMobile. Cette option peut être **OFF** ou **ON**. La possibilité de charger un certificat pour cette fonctionnalité n'est pas actuellement disponible. Si vous souhaitez utiliser cette fonctionnalité, vous devez appeler le support Citrix pour qu'ils configurent la détection automatique pour vous. Pour en savoir plus sur le certificate pinning, consultez la section correspondante dans Secure Hub dans la documentation des applications XenMobile. Pour en savoir plus sur les ports requis pour assurer le fonctionnement du certificate pinning, consultez l'article Exigences requises par XenMobile en matière de port pour la connectivité ADS.



Dans l'écran ci-dessus, veuillez noter que Worx Home est maintenant appelé Secure Hub.

7. Une page de résumé affiche les informations que vous avez entrées dans les étapes précédentes. Vérifiez que les données sont correctes et cliquez sur **Save**.



Dans l'écran ci-dessus, veuillez noter que Worx Home est maintenant appelé Secure Hub.

Activer la détection automatique

La détection automatique simplifie le processus d'inscription pour les utilisateurs. Ils peuvent utiliser leurs noms d'utilisateur réseau et leurs mots de passe Active Directory pour inscrire leurs appareils, et n'ont pas besoin d'entrer ces détails sur le serveur XenMobile. Le nom d'utilisateur doit être entré au format UPN (nom d'utilisateur principal) ; par exemple, utilisateur@monentreprise.com.

Pour activer la détection automatique, vous pouvez accéder au portail Autodiscovery Service à l'adresse https://xenmobiletools.citrix.com.

Il se peut, dans certains cas limités, que vous deviez contacter le support technique Citrix pour activer la détection automatique. Pour ce faire, vous pouvez suivre les procédures ci-dessous pour transmettre vos informations de déploiement à l'équipe d'assistance technique, et dans le cas d'appareils Windows, un certificat SSL. Après que Citrix a reçu ces informations, lorsque les utilisateurs inscrivent leurs appareils, les informations de domaine sont extraites et mappées à une adresse de serveur. Ces informations sont conservées dans la base de données XenMobile afin qu'elles soient toujours accessibles et disponibles lorsque les utilisateurs s'inscrivent.

1. Si vous ne parvenez pas à activer la détection automatique à l'aide du portail Autodiscovery Service sur https://xenmobiletools.citrix.com, ouvrez un ticket de support technique Citrix à l'aide du portail d'assistance Citrix et fournissez les informations suivantes :

- Le domaine contenant les comptes avec les utilisateurs vont s'inscrire.
- Le nom de domaine complet (FQDN) du serveur XenMobile.

- Le nom de l'instance XenMobile. Par défaut, le nom de l'instance est zdm et est sensible à la casse.
- Le type d'ID utilisateur, qui peut être UPN ou E-mail. Le paramètre par défaut est UPN.
- Le port utilisé pour l'inscription iOS si vous avez modifié le numéro de port par défaut 8443.
- Le port sur lequel le serveur XenMobile accepte les connexions si vous avez modifié le numéro de port par défaut 443.
- Si vous le souhaitez, une adresse e-mail pour votre administrateur XenMobile.

2. Si vous prévoyez d'inscrire des appareils Windows, procédez comme suit :

- Obtenez un certificat SSL non générique signé publiquement pour enterpriseenrollment.masociété.com, où masociété.com est le domaine contenant les comptes avec lesquels les utilisateurs vont s'inscrire. Joignez le certificat SSL au format .pfx et son mot de passe à votre demande.
- Créez un nom canonique (CNAME) dans votre DNS et mappez l'adresse de votre certificat SSL (enterpriseenrollment.masociété.com) vers autodisc.zc.zenprise.com. Lorsque l'utilisateur d'un appareil Windows s'inscrit à l'aide d'un nom UPN, en plus de fournir les détails de votre serveur XenMobile, le serveur d'inscription Citrix invite l'appareil à demander un certificat valide depuis le serveur XenMobile.

Votre ticket de support technique sera mis à jour lorsque vos informations et votre certificat, si nécessaire, sont ajoutés aux serveurs Citrix. À ce stade, les utilisateurs peuvent démarrer l'inscription à l'aide de la détection automatique.

Remarque : vous pouvez également utiliser un certificat multi-domaines si vous voulez vous inscrire à l'aide de plus d'un domaine. Le certificat multi-domaines doit avoir la structure suivante :

- Un SubjectDN avec un CN (nom commun) qui spécifie le domaine principal qu'il sert (par exemple, enterpriseenrollment.masociété1.com).
- Les SAN appropriés pour les domaines restants (par exemple, enterpriseenrollment.masociété2.com, enterpriseenrollment.masociété3.com, etc).

Inscrire des appareils

Mar 31, 2017

Pour gérer les appareils utilisateur à distance et de manière sécurisée, ces derniers sont inscrits dans XenMobile. Le logiciel client XenMobile est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée. Ensuite, XenMobile et le profil utilisateur sont installés. Vous pouvez ensuite effectuer les tâches de gestion dans la console XenMobile. Vous pouvez appliquer des stratégies, déployer des applications, envoyer des données sur l'appareil et verrouiller, effacer et localiser des appareils perdus ou volés.

Remarque : avant de pouvoir inscrire des utilisateurs d'appareils iOS, vous devez demander un certificat APNS. Pour plus d'informations, consultez la section Certificats.

Pour mettre à jour les options de configuration pour les utilisateurs et les appareils, accédez à la page **Gérer > Inscription**. Pour de plus amples informations, consultez la section Envoyer une invitation d'inscription dans cet article.

Appareils Android

1. Accédez au magasin Google Play sur votre Android et téléchargez l'application Citrix Secure Hub, puis touchez l'application.
2. Lorsque vous êtes invité à installer l'application, cliquez sur **Suivant**, puis cliquez sur **Installer**.
3. Après l'installation de Secure Hub, touchez **Ouvrir**.
4. Entrez vos informations d'identification d'entreprise, telles que le nom du serveur XenMobile de votre organisation, le nom d'utilisateur principal (UPN), ou votre adresse e-mail et cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Activer l'administrateur de l'appareil**, touchez **Activer**.
6. Entrez votre mot de passe d'entreprise, puis touchez **Se connecter**.
7. En fonction de la manière dont XenMobile est configuré, vous pouvez être invité à créer un code PIN Citrix, que vous pouvez utiliser pour vous connecter à Secure Hub et à d'autres applications XenMobile, telles que Secure Mail, Secure Web, ShareFile, et bien plus encore. Vous devez entrer votre code PIN Citrix deux fois. Sur l'écran **Créer un code PIN Citrix**, entrez un code PIN.
8. Entrez de nouveau le code PIN. Secure Hub s'affiche. Vous pouvez ensuite accéder à XenMobile Store pour afficher les applications que vous pouvez installer sur votre appareil Android.
9. Si vous avez configuré XenMobile pour distribuer automatiquement des applications sur les appareils des utilisateurs après l'inscription, des messages les inviteront à installer les applications. En outre, les stratégies que vous configurez dans XenMobile sont déployées sur l'appareil. Cliquez sur **Installer** pour installer les applications.

Pour désinscrire et réinscrire un appareil Android

Les utilisateurs peuvent se désinscrire depuis Secure Hub. Lorsque les utilisateurs se désinscrivent à l'aide de la procédure suivante, l'appareil s'affiche toujours dans l'inventaire d'appareils dans la console XenMobile. Toutefois, vous ne pouvez pas intervenir sur l'appareil. Vous ne pouvez pas suivre l'appareil ni contrôler sa conformité.

1. Touchez pour ouvrir l'application Secure Hub.

2. Selon que vous possédez une tablette ou un téléphone, procédez comme suit :

Sur un téléphone :

a. Balayez l'écran à partir de la gauche pour ouvrir un panneau de paramètres.

b. Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.

Sur une tablette :

a. Touchez la flèche en regard de votre adresse e-mail sur le coin supérieur droit.

b. Touchez **Préférences**, **Comptes**, puis touchez **Supprimer le compte**.

3. Touchez **Réinscription**. Un message s'affiche afin de confirmer que vous souhaitez réinscrire votre appareil.

4. Touchez **OK**.

Votre appareil est désinscrit.

5. Suivez les instructions à l'écran pour réinscrire votre appareil.

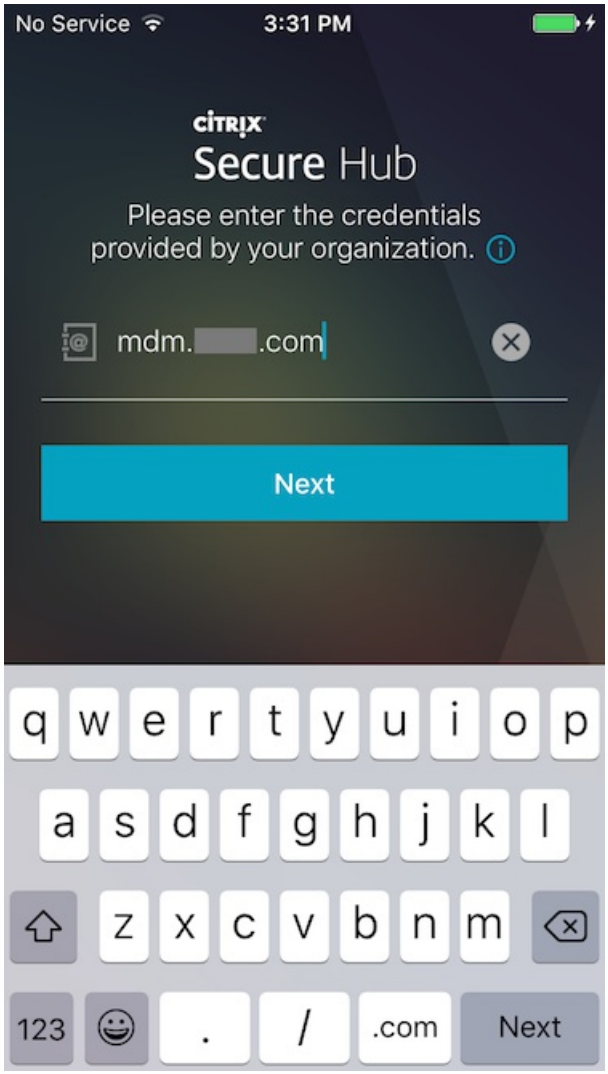
Appareils iOS

1. Téléchargez l'application Secure Hub à partir de l'App Store Apple iTunes sur l'appareil, puis installez l'application sur l'appareil.

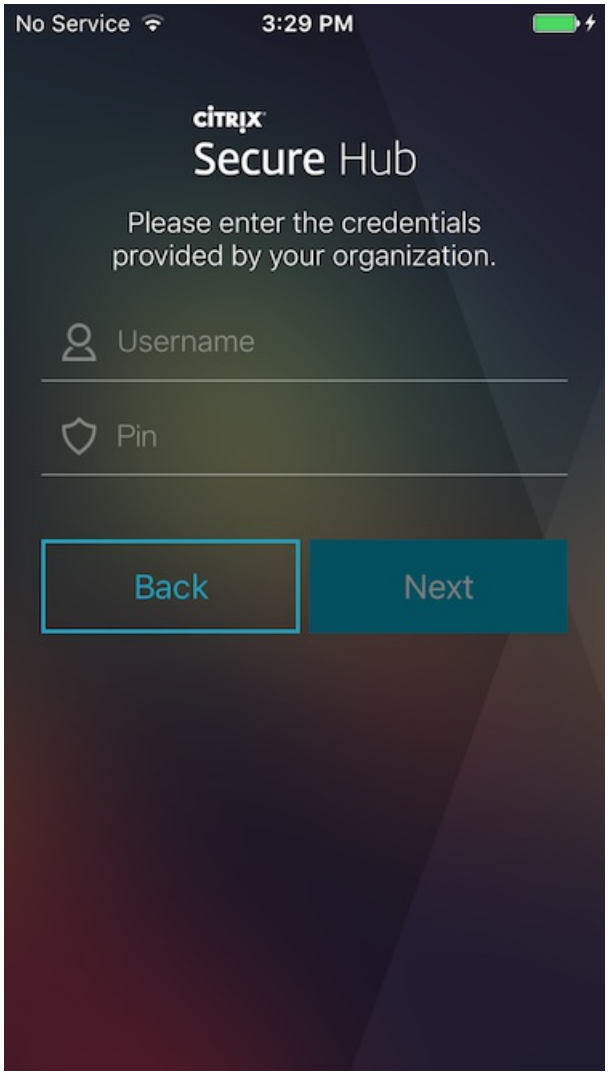
2. Sur l'écran d'accueil de l'appareil iOS, tapotez l'application Secure Hub.

3. Lorsque l'application Secure Hub s'affiche, entrez l'adresse du serveur fournie par votre service d'assistance.

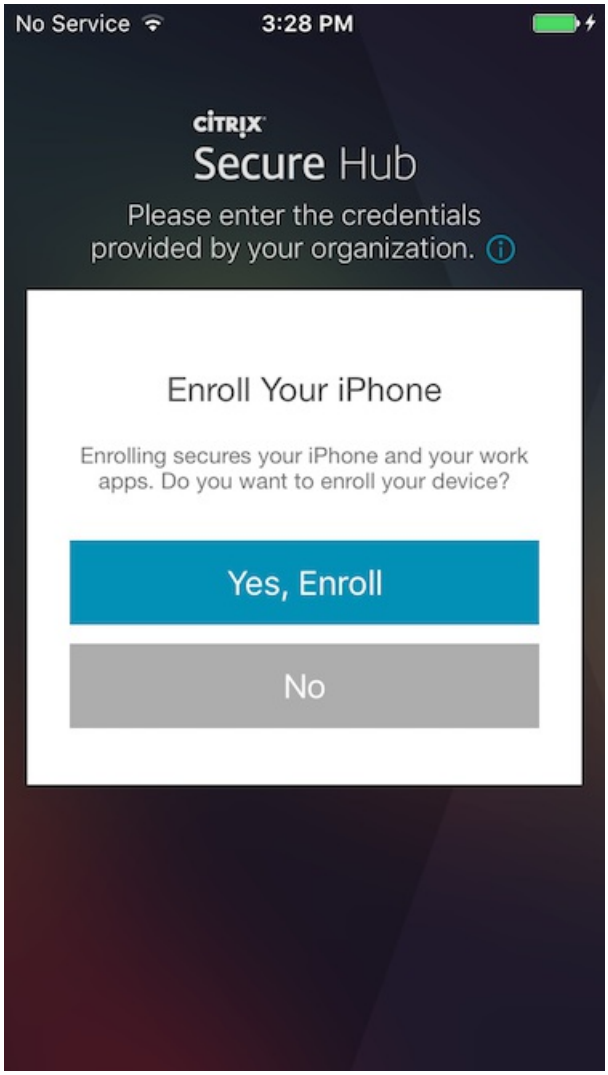
(Les écrans présentés peuvent différer de ces exemples en fonction de la façon dont XenMobile est configuré.)

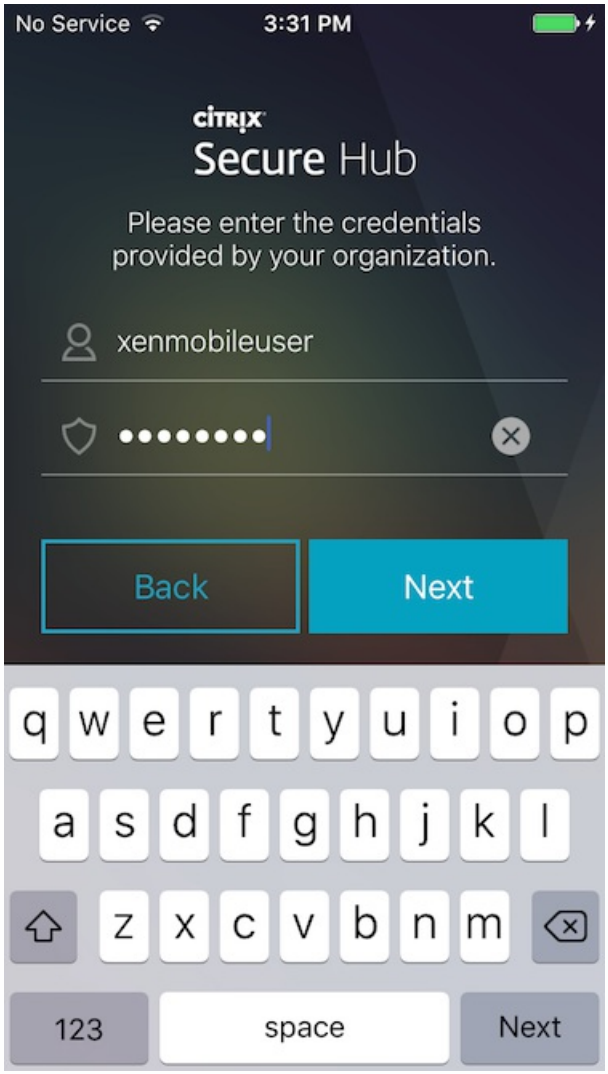


4. Lorsque vous y êtes invité, entrez vos nom d'utilisateur et mot de passe ou code PIN. Cliquez sur **Suivant**.



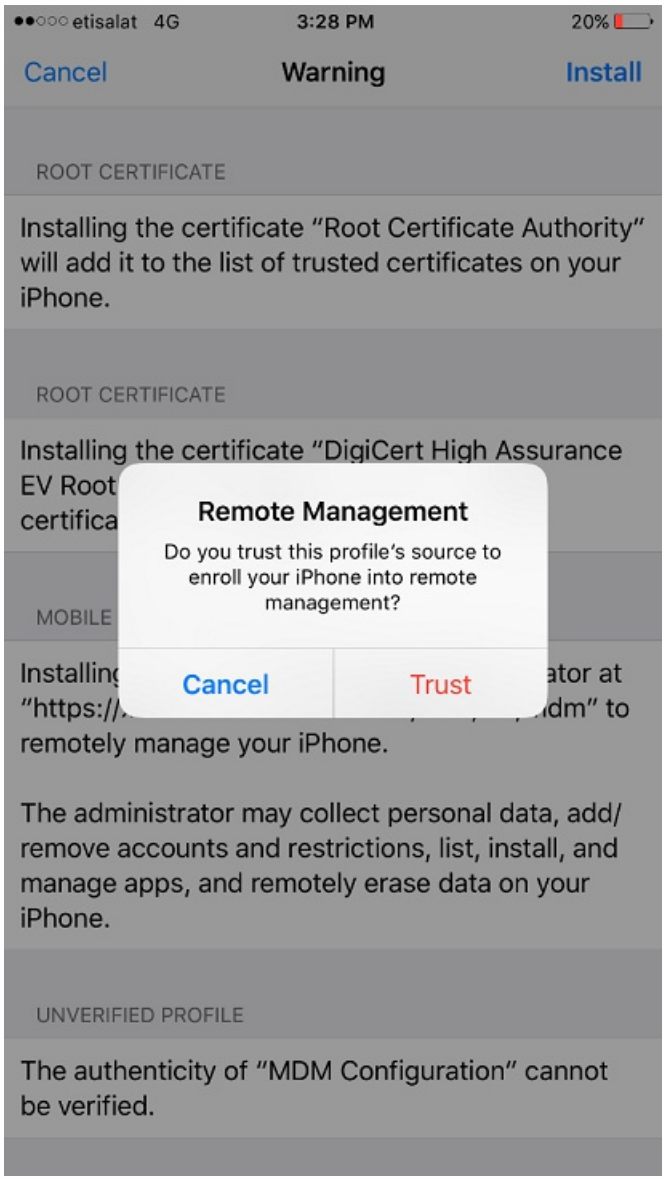
5. Lorsque vous êtes invité à vous inscrire, cliquez sur **Oui, inscrire** et entrez vos informations d'identification lorsque vous y êtes invité.



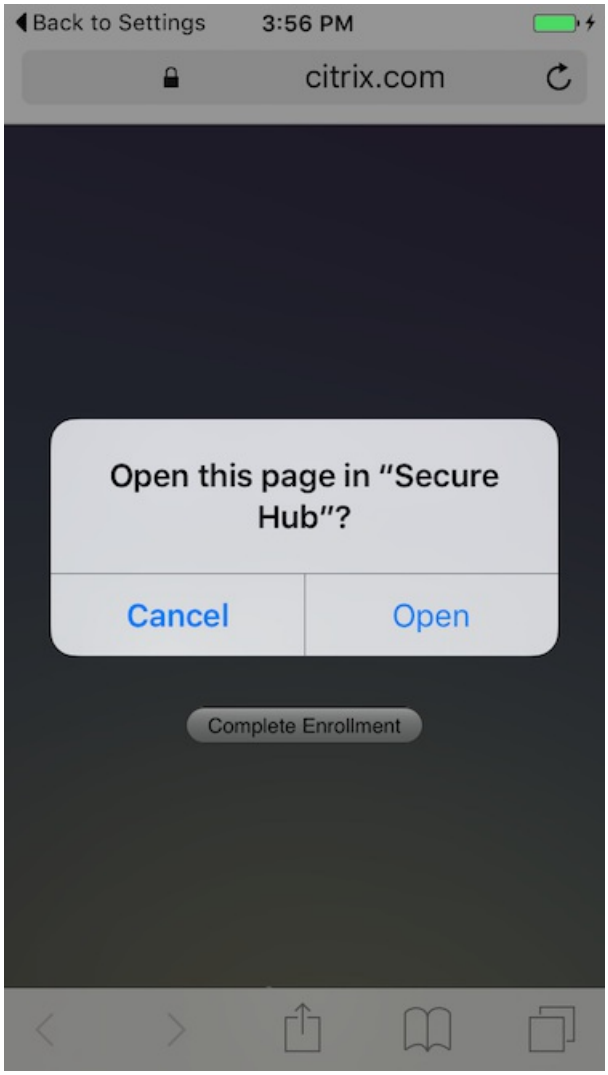


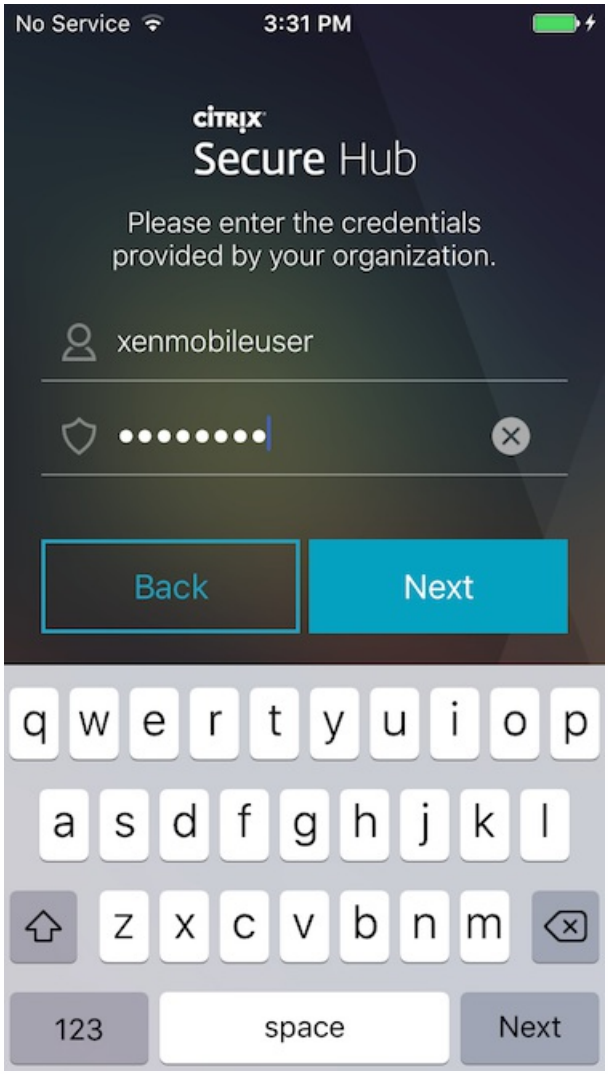
6. Cliquez sur **Installer** pour installer Citrix Profile Services.

7. Appuyez sur **Faire confiance**.



8. Appuyez sur **Ouvrir** puis entrez vos informations d'identification.





Appareils Mac OS X et macOS

Vous pouvez inscrire des appareils Mac qui exécutent Mac OS X ou macOS dans XenMobile en mode MDM exclusif. Les utilisateurs Mac s'inscrivent sans fil (OTA) directement depuis leurs appareils.

Pour inscrire des appareils Mac, les administrateurs XenMobile procèdent comme suit :

1. Si vous le souhaitez, vous pouvez définir des stratégies Mac dans la console XenMobile. Consultez la section Stratégies d'appareil pour de plus amples informations sur les stratégies d'appareil. Pour savoir quelles stratégies d'appareils vous pouvez configurer pour des Mac, consultez la section Stratégies XenMobile par plate-forme.

2. Envoyez le lien d'inscription à l'utilisateur : https://:8443/zdm/macos/otae

- FQDNserveur est le nom de domaine complet du serveur exécutant XenMobile.
- Le port 8443 est le port sécurisé par défaut. Si vous avez configuré un port différent, utilisez-le à la place de 8443.
- zdm est le nom de l'instance par défaut utilisé lors de l'installation du serveur. Si vous avez configuré un nom d'instance différent, utilisez plutôt le nom de cette instance.

Vous pouvez également envoyer le lien dans une invitation électronique. Pour de plus amples informations, consultez la section Envoyer des invitations d'inscription.

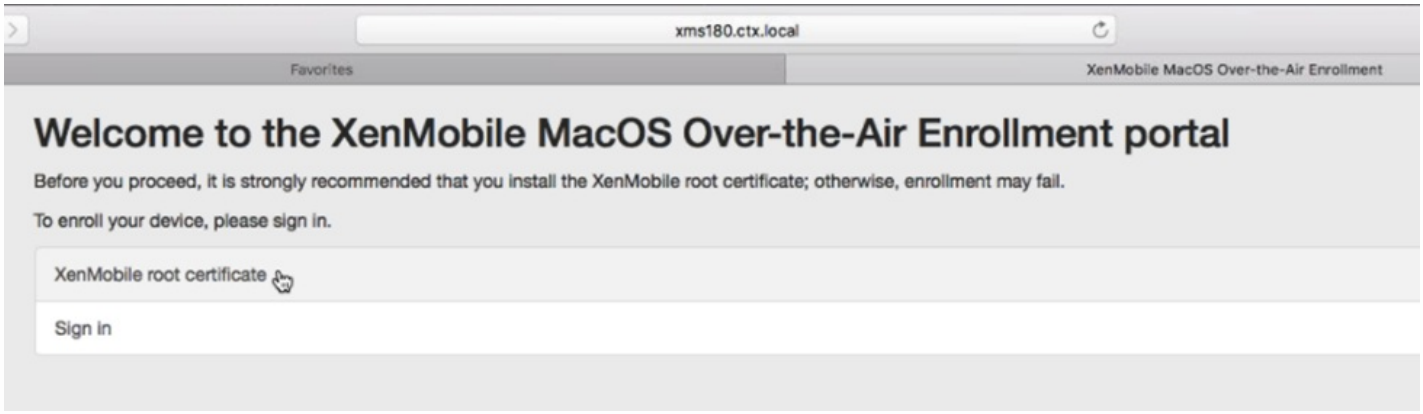
3. Les utilisateurs installent les certificats, selon les besoins. Si vous avez configuré un certificat SSL approuvé publiquement et un certificat numérique signé approuvé publiquement pour iOS et macOS, les utilisateurs sont invités à installer les certificats. Pour de plus amples informations sur les certificats, consultez Certificats.

4. Sur le Mac à inscrire, les utilisateurs accèdent au lien d'inscription à l'aide de Safari.

> **Remarque** : si les utilisateurs ne peuvent pas accéder au lien, ils peuvent effacer l'historique de navigation et le cache ou utiliser un autre navigateur.

5. Par défaut, ces instructions d'installation de certificats s'affichent.

a. Les utilisateurs cliquent sur **Certificat racine XenMobile**.

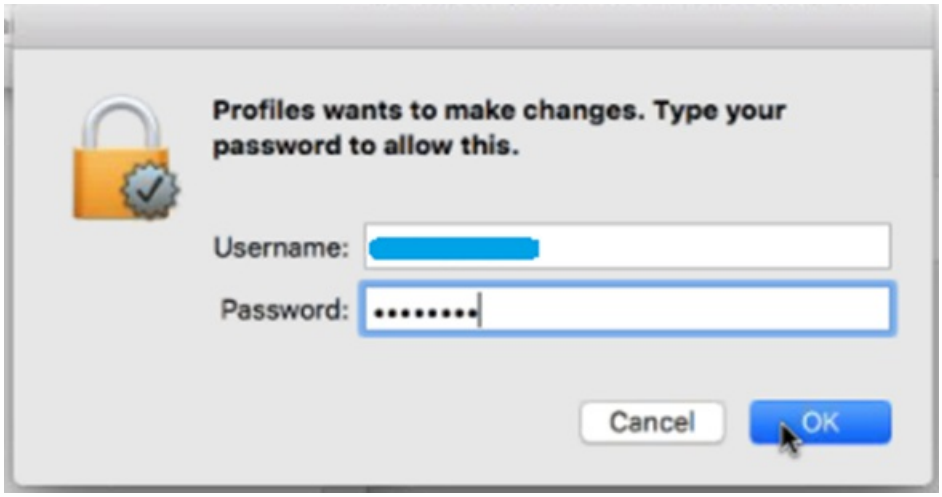


b. les utilisateurs cliquent sur **Continuer** pour installer les certificats.

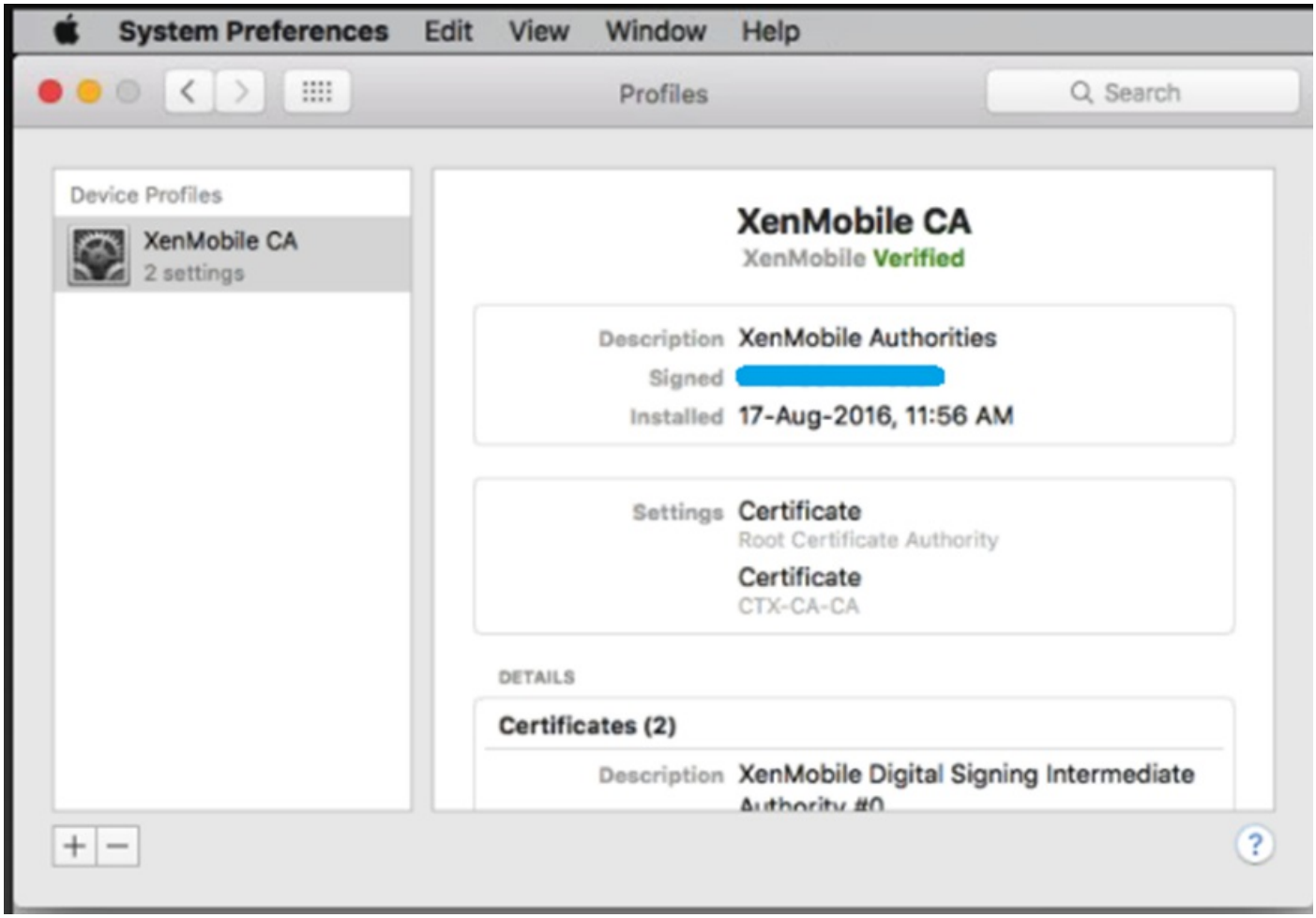
> **Remarque** : l'installation du certificat d'autorité de certification racine du serveur XenMobile active un canal de communication de confiance entre l'appareil et XenMobile.

c. Les utilisateurs cliquent sur **Installer** pour installer le profil XenMobile.

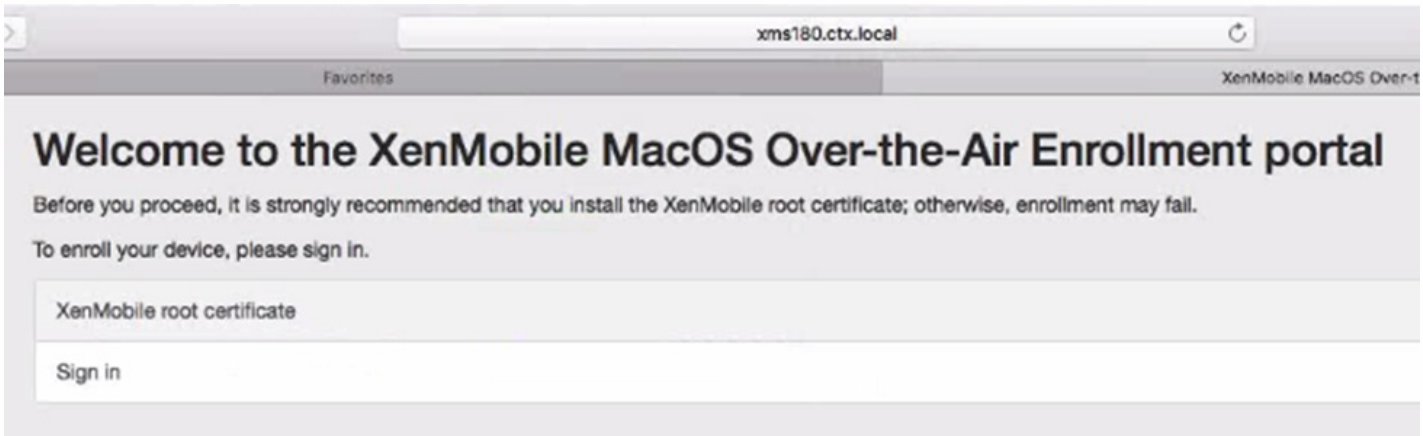
d. Les utilisateurs entrent les informations d'identification d'ouverture de session lorsqu'ils y sont invités.



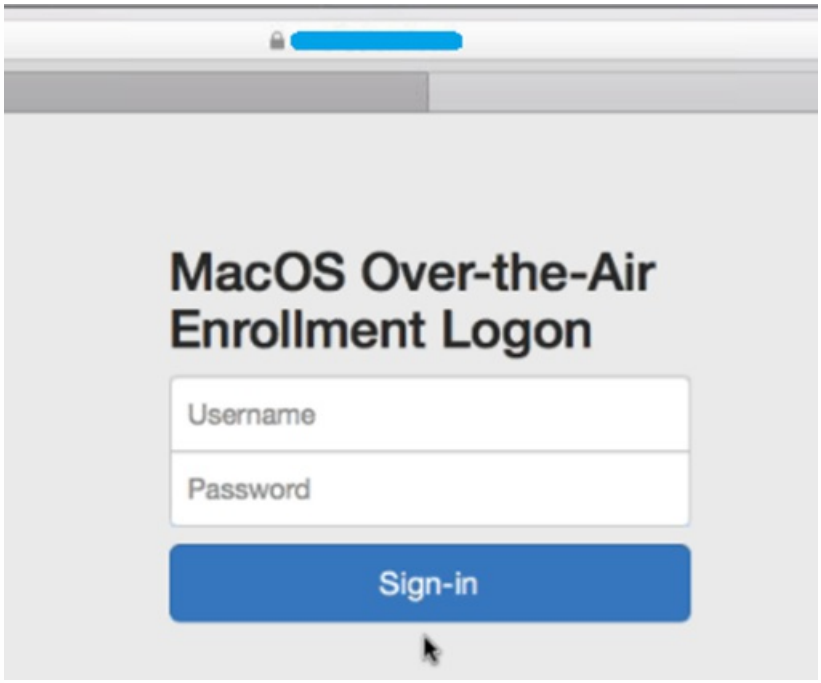
e. Cet écran s'affiche suite à l'installation des certificats XenMobile sous **Profils**. Les utilisateurs ferment cet écran pour procéder à l'inscription de l'appareil.



6. Sur le portail d'inscription OTA pour macOS, les utilisateurs cliquent sur **Sign in**.

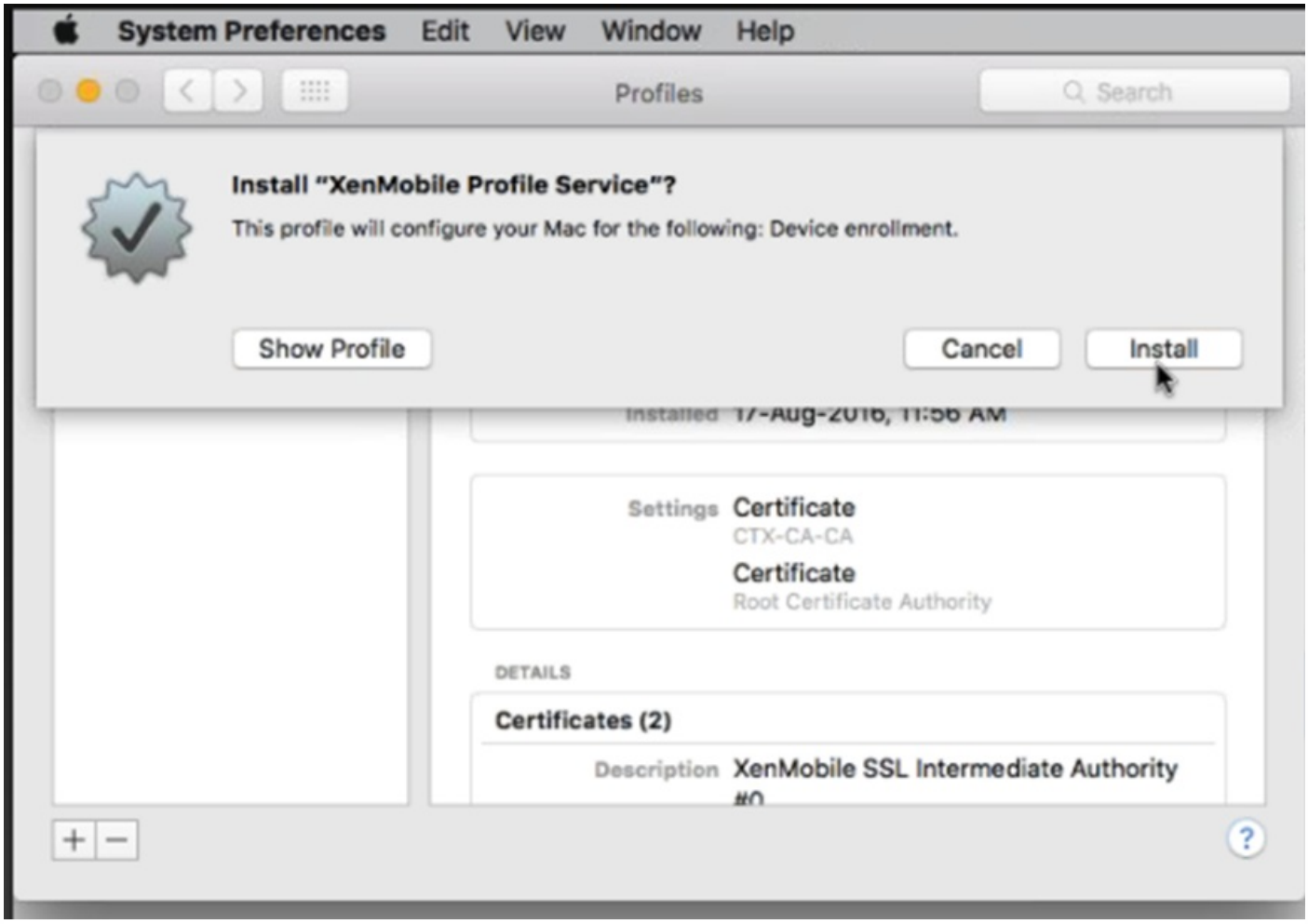


7. Les utilisateurs saisissent leurs informations d'identification au format UPN ou sAMAccountName, en fonction de la méthode configurée par l'administrateur de XenMobile, puis ils cliquent sur **Sign-in**.



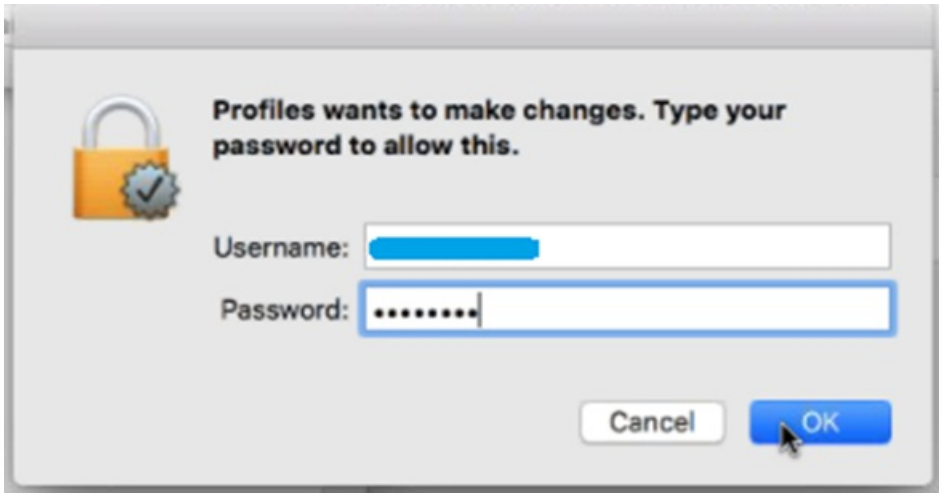
Remarque : XenMobile valide la demande de l'utilisateur et vérifie les informations d'identification à l'aide d'Active Directory. Les informations d'identification sont validées par rapport à Active Directory.

8. Si l'ouverture de session réussit, la fenêtre XenMobile Profile Service s'affiche. Les utilisateurs cliquent sur **Install** pour installer le XenMobile Profile Service. L'installation du XenMobile Profile Service permet à l'administrateur de XenMobile de gérer le Mac à distance.

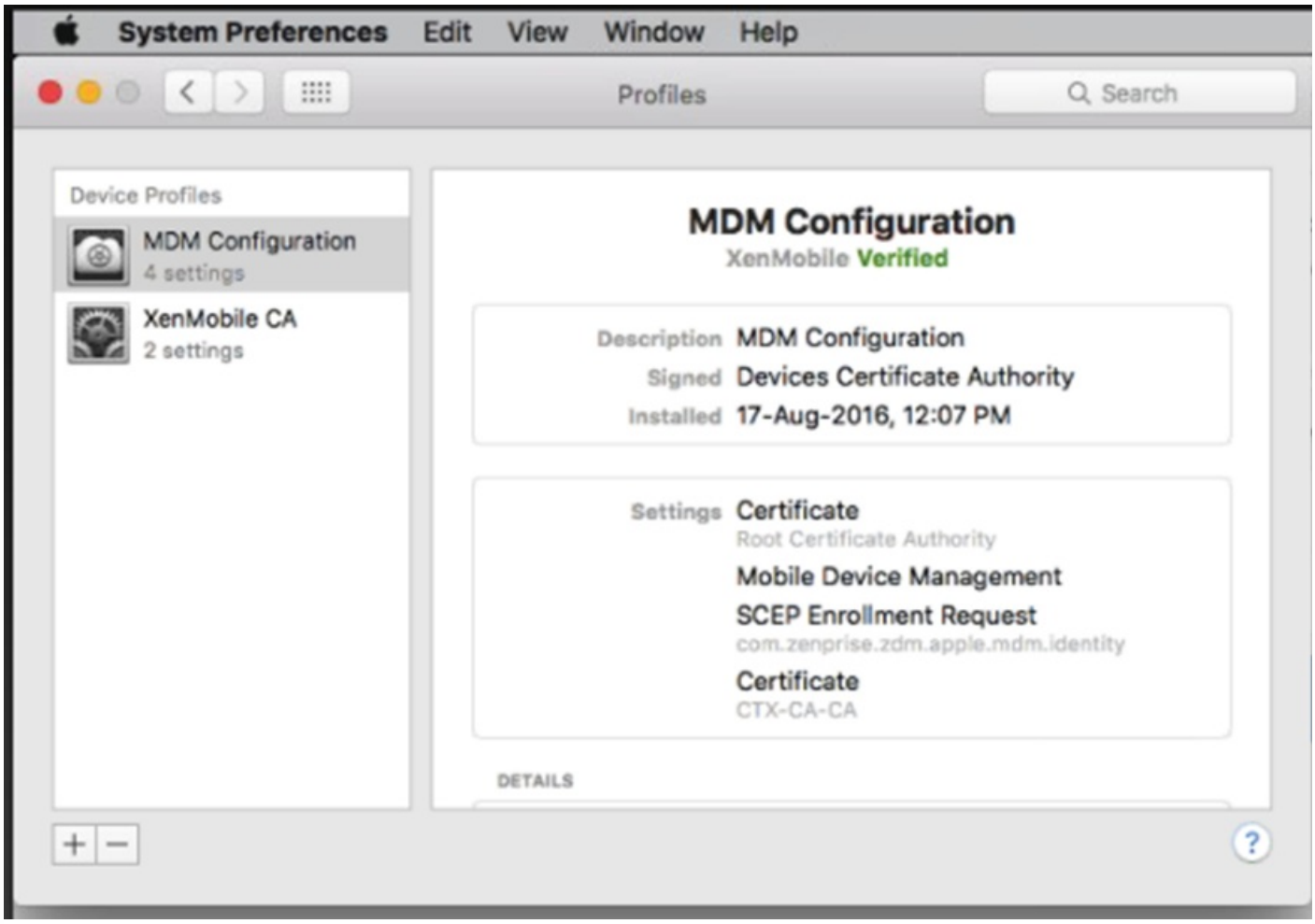


9. Pour installer le profil MDM, les utilisateurs cliquent sur **Continue**, puis sur **Install**.

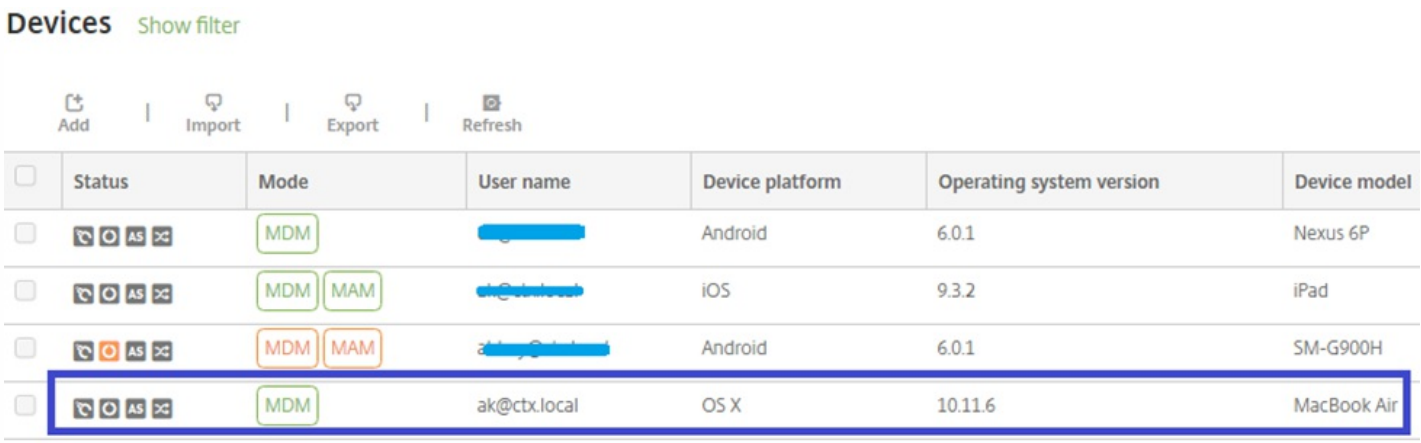
10. Les utilisateurs entrent les informations d'identification d'ouverture de session lorsqu'ils y sont invités.



11. Une fois le profil de configuration MDM installé avec succès, l'écran MDM Configuration s'affiche.



12. Votre Mac apparaît à présent dans l'onglet Appareil de la console XenMobile. Vous pouvez maintenant démarrer la gestion des Mac avec XenMobile de la même façon que vous gérez les appareils mobiles.



Machines Windows

Vous pouvez inscrire des appareils dans XenMobile qui exécutent les systèmes d'exploitation Windows suivants :

- Windows 8.1 et Windows 10
- Windows Phone 8.1 et 10

Les utilisateurs Windows et Windows Phone s'inscrivent directement au travers de leurs appareils.

Vous devez configurer la détection automatique et le service de découverte Windows pour l'inscription de l'utilisateur afin d'autoriser la gestion des appareils Windows et Windows Phone.

> ## Remarque
>
> Pour pouvoir inscrire des appareils Windows, le certificat d'écoute SSL doit être un certificat SSL. L'inscription échoue si vous avez chargé un certificat SSL auto-signé.

Pour inscrire des appareils Windows à l'aide de la détection automatique

Les utilisateurs peuvent inscrire des appareils exécutant Windows RT 8.1, les versions 32 bits et 64 bits de Windows 8.1 Professionnel et Windows 8.1 Entreprise et Windows 10. Pour activer la gestion des appareils Windows, Citrix vous recommande de configurer la détection automatique ainsi que le service de découverte Windows. Pour de plus amples informations, consultez la section Pour activer la détection automatique pour l'inscription utilisateur dans XenMobile.

1. Sur l'appareil, recherchez et installez toutes les mises à jour Windows disponibles. Cette étape est particulièrement importante lors de la mise à niveau de Windows 8 vers Windows 8.1 car les utilisateurs risquent de ne pas être automatiquement avertis de toutes les mises à jour disponibles.

2. Dans le menu Icônes, touchez Paramètres et :

- Pour Windows 8.1, touchez Paramètres du PC > Réseau > Espace de travail.
- Pour Windows 10, touchez Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école.

3. Entrez votre adresse de messagerie d'entreprise, puis touchez **Activer la gestion des appareils** sur Windows 8.1 ou

Continuer sur Windows 10. Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, foo@mondomaine.com). Cela vous permet de contourner une limitation Microsoft connue dans laquelle l'inscription est réalisée par la gestion des appareils intégrée sur Windows ; dans la boîte de dialogue **Connexion à un service**, entrez le nom d'utilisateur et le mot de passe associés à l'utilisateur local. L'appareil découvre automatiquement un serveur XenMobile et démarre le processus d'inscription.
4. Entrez votre mot de passe. Utilisez le mot de passe associé à un compte qui est membre d'un groupe d'utilisateurs dans XenMobile.
5. Pour Windows 8.1, dans la boîte de dialogue **Autorisez les applications et services de l'administrateur**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Activer**. Pour Windows 10, dans la boîte de dialogue **Termes d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**.

Pour inscrire des appareils Windows sans détection automatique

Il est possible d'inscrire des appareils Windows sans détection automatique. Cependant, Citrix vous recommande de configurer la détection automatique. L'inscription sans détection automatique provoque un appel vers le port 80 avant de se connecter à l'adresse URL de votre choix ; cette méthode de déploiement n'est donc pas recommandée dans un environnement de production. Citrix vous recommande d'utiliser ce processus uniquement dans des environnements de test et des déploiements de preuve de concept.

1. Sur l'appareil, recherchez et installez toutes les mises à jour Windows disponibles. Cette étape est particulièrement importante lors de la mise à niveau de Windows 8 vers Windows 8.1 car les utilisateurs risquent de ne pas être automatiquement avertis de toutes les mises à jour disponibles.

2. Dans le menu Icônes, touchez **Paramètres** et :

- Pour Windows 8.1, touchez **Paramètres du PC > Réseau > Espace de travail**.
- Pour Windows 10, touchez **Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école**.

3. Entrez votre adresse de messagerie d'entreprise.

4. Sur Windows 10, si la détection automatique n'est pas configurée, une option vous permettant d'entrer les détails du serveur apparaît, comme décrit dans l'étape 5. Sur Windows 8.1, si l'option **Détecter automatiquement l'adresse du serveur** est activée, touchez pour la désactiver.

5. Dans le champ **Entrer l'adresse du serveur** :

- Pour Windows 8.1, tapez l'adresse du serveur au format suivant : https://fqdnserveur:8443/Instanceserveur/Discovery.svc. Si un port autre que 8443 est utilisé pour les connexions SSL non authentifiées, utilisez ce numéro de port à la place de 8443 dans cette adresse.
- Pour Windows 10, utilisez cette adresse : https://beta.managedm.com:8443/zdm/wpe. Si un port autre que 8443 est utilisé pour les connexions SSL non authentifiées, utilisez ce numéro de port à la place de 8443 dans cette adresse.

6. Entrez votre mot de passe.
7. Pour Windows 8.1, dans la boîte de dialogue **Autorisez les applications et services de l'administrateur**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Activer**. Pour Windows 10, dans la boîte de dialogue **Termes d'utilisation**, indiquez que vous acceptez que votre appareil soit géré, puis touchez **Accepter**.

Pour inscrire des appareils Windows Phone

Pour inscrire des appareils Windows Phone dans XenMobile, les utilisateurs ont besoin de leur adresse e-mail de réseau interne ou Active Directory et d'un mot de passe. Si la détection automatique n'est pas configurée, les utilisateurs ont également besoin de l'adresse Web du serveur XenMobile. Ensuite, ils suivent cette procédure sur leurs appareils pour

s'inscrire.

Remarque : si vous prévoyez de déployer des applications via le magasin d'entreprise Windows Phone, avant que vos utilisateurs ne s'inscrivent, assurez-vous d'avoir configuré une stratégie d'hub d'entreprise (avec une application Secure Hub Windows Phone signée pour chaque plate-forme que vous prenez en charge).

1. Sur l'écran principal de Windows Phone, touchez l'icône **Paramètres**.

- Pour Windows Phone 10, en fonction de votre version, touchez **Comptes > Accès professionnel ou d'école > Connecter à l'entreprise ou l'école** ou touchez **Comptes > Accès professionnel > S'inscrire à la gestion des appareils**.
- Pour Windows Phone 8.1, touchez **Paramètres du PC > Réseau > Espace de travail**, puis touchez **Ajouter un compte**.

2. Dans l'écran suivant, entrez une adresse de messagerie et un mot de passe et touchez **Connexion**.

Si la détection automatique est configurée pour votre domaine, les informations requises dans les étapes suivantes sont automatiquement renseignées. Passez à l'étape 8.

Si la détection automatique n'est pas configurée pour votre domaine, passez à l'étape suivante. Pour vous inscrire en tant qu'utilisateur local, entrez une nouvelle adresse de messagerie avec le nom de domaine correct (par exemple, foo@mondomaine.com). Cela vous permet de contourner une limitation Microsoft connue ; dans la boîte de dialogue **Connexion à un service**, entrez le nom d'utilisateur et le mot de passe associés à l'utilisateur local.

3. Sur l'écran suivant, entrez l'adresse Web du serveur XenMobile, telle que : https://://wpe. Par exemple : https://monentreprise.mdm.com:8443/zdm/wpe. **Remarque** : le numéro de port doit être adapté à votre implémentation, mais doit être le même port que vous avez utilisé pour une inscription iOS.

4. Entrez le nom d'utilisateur et le domaine si l'authentification est validée à l'aide d'un nom d'utilisateur et un domaine, puis tapotez **Connexion**.

5. Si un écran apparaît indiquant un problème avec le certificat, l'erreur est due à l'utilisation d'un certificat auto-signé. Si le serveur est approuvé, touchez **Continuer**. Sinon, cliquez sur **Annuler**.

6. Sur Windows Phone 8.1, lorsque le compte est ajouté, vous avez la possibilité de sélectionner **Installer l'application de l'entreprise**. Si votre administrateur a configuré un magasin d'applications d'entreprise, sélectionnez cette option et touchez **Terminé**. Si vous désactivez cette option, vous devrez réinscrire votre appareil pour recevoir le magasin d'applications d'entreprise.

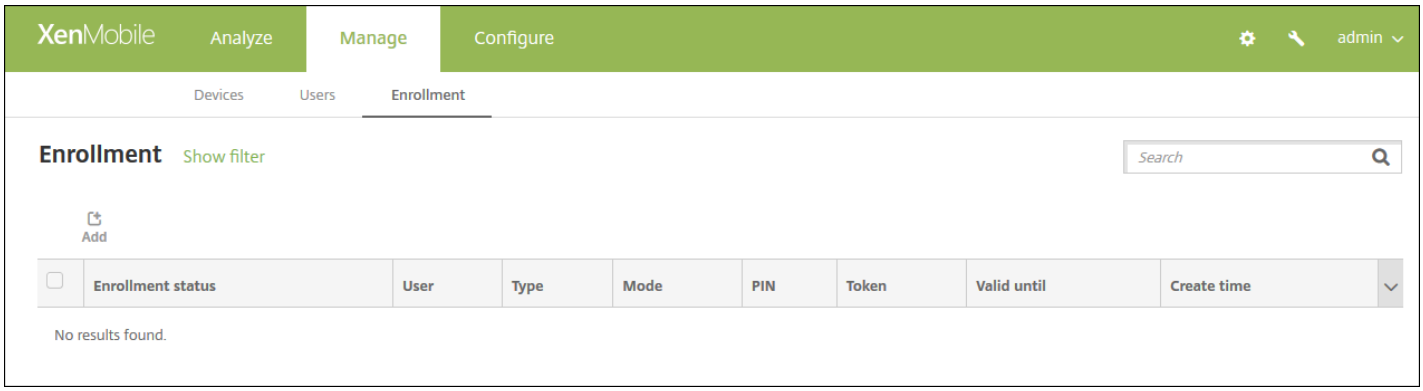
7. Sur Windows Phone 8.1, sur l'écran **Compte ajouté**, touchez **terminé**.

8. Pour forcer une connexion au serveur, cliquez sur l'icône d'actualisation. Si l'appareil ne se connecte pas manuellement au serveur, XenMobile essaye de se reconnecter. XenMobile se connecte à l'appareil toutes les 3 minutes à 5 reprises, puis toutes les 2 heures par la suite. Vous pouvez modifier cet intervalle de connexion dans **Intervalle de pulsation WNS Windows** situé dans **Propriétés du serveur**. Une fois l'inscription terminée, Secure Hub s'inscrit en arrière-plan. Aucun indicateur n'apparaît lorsque l'installation est terminée. Appuyez sur Secure Hub sur l'écran **Toutes les applications**.

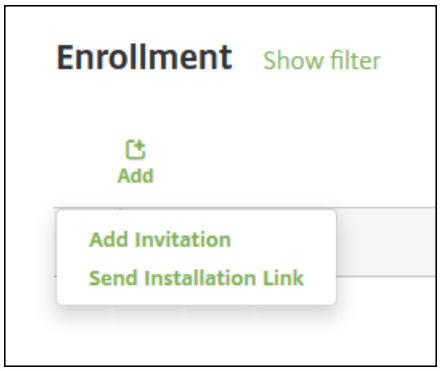
Envoyer une invitation d'inscription

Dans la console XenMobile, vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS ou Android. Vous pouvez également envoyer un lien d'installation aux utilisateurs d'appareils iOS, Android ou Windows.

1. Dans la console XenMobile, cliquez sur **Gérer** > **Inscription**. La page **Inscription** s'affiche.



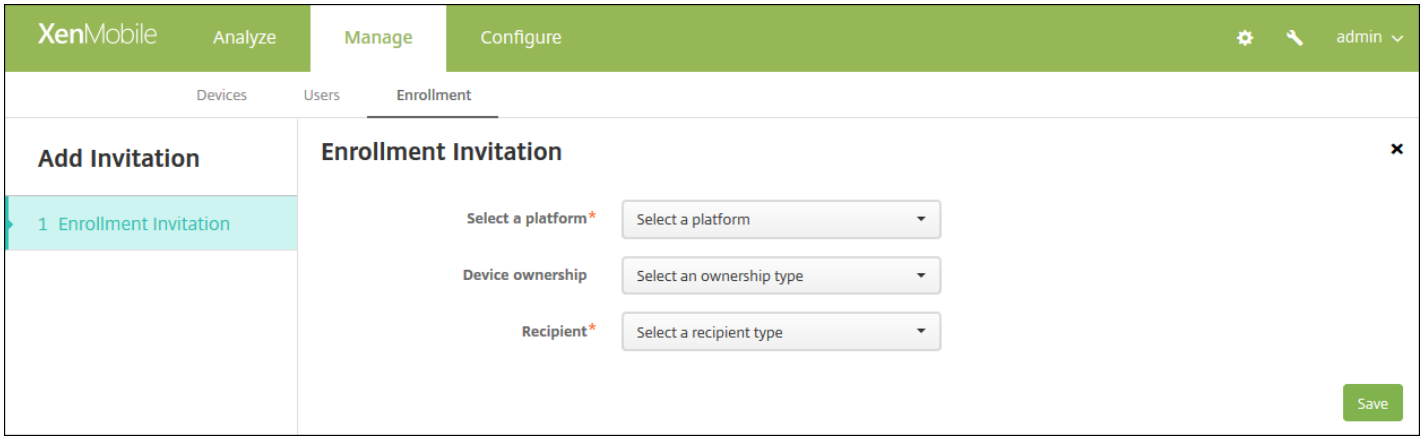
2. Cliquez sur **Ajouter**. Un menu répertoriant les options d'inscription s'affiche.



- Pour envoyer une invitation d'inscription à un utilisateur ou groupe, cliquez sur **Ajouter une invitation**, puis consultez la section Pour envoyer une invitation pour connaître les étapes suivantes.
- Pour envoyer un lien d'installation d'inscription à une liste de destinataires via SMTP ou SMS, cliquez sur **Envoyer lien d'installation**, puis consultez la section Pour envoyer un lien d'installation pour connaître les étapes suivantes.

Pour envoyer une invitation

1. Cliquez sur **Ajouter une invitation**. L'écran **Invitation d'inscription** s'affiche.

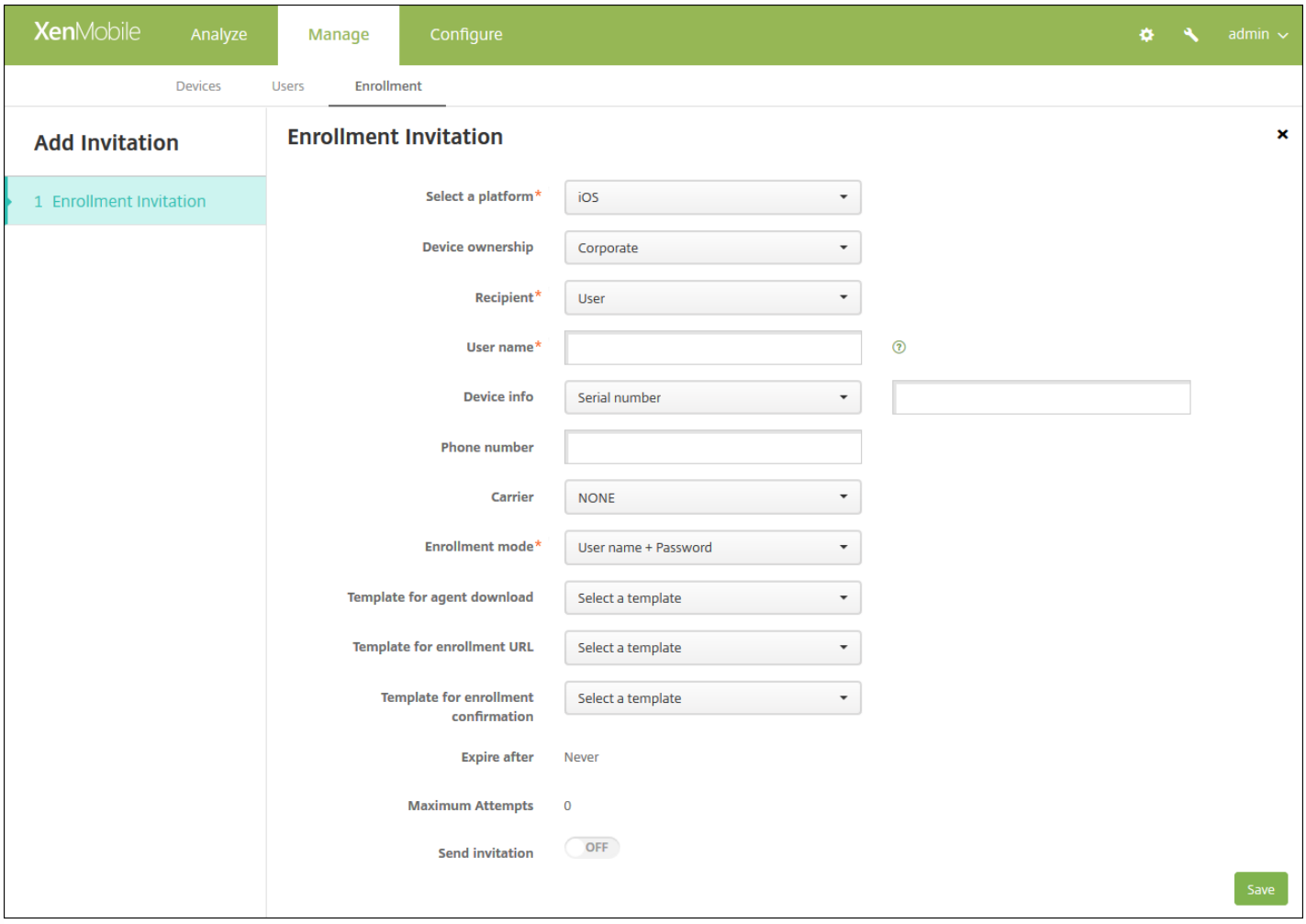


2. Pour configurer ces paramètres :

- **Sélectionner une plate-forme** : dans la liste, cliquez sur **iOS** ou **Android**.
- **Propriétaire** : dans la liste, cliquez sur **Entreprise** ou **Employé**.
- **Destinataire** : dans la liste, cliquez sur **Utilisateur** ou **Groupe**.

En fonction du destinataire que vous sélectionnez, vous pouvez voir des paramètres de configuration supplémentaires. Pour les paramètres **Utilisateur**, consultez la section Pour envoyer une invitation d'inscription à un utilisateur ; pour les paramètres **Groupe**, consultez la section Pour envoyer une invitation d'inscription à un groupe.

Pour envoyer une invitation d'inscription à un utilisateur



1. Configurez ces paramètres **Utilisateur** :

- **Nom d'utilisateur** : entrez un nom d'utilisateur. L'utilisateur doit exister dans le serveur XenMobile en tant qu'utilisateur local ou en tant qu'utilisateur dans Active Directory. Si l'utilisateur est local, assurez-vous que la propriété Email de l'utilisateur est configurée pour vous permettre de lui envoyer des notifications. S'il s'agit d'un utilisateur Active Directory, assurez-vous que LDAP est configuré.
- **Infos appareil** : dans la liste, cliquez sur **Numéro de série**, **UDID** ou **IMEI**. Après avoir choisi une option, un champ s'affiche dans lequel vous pouvez entrer la valeur correspondante à l'appareil.
- **Numéro de téléphone** : si vous le souhaitez, entrez le numéro de téléphone de l'utilisateur.

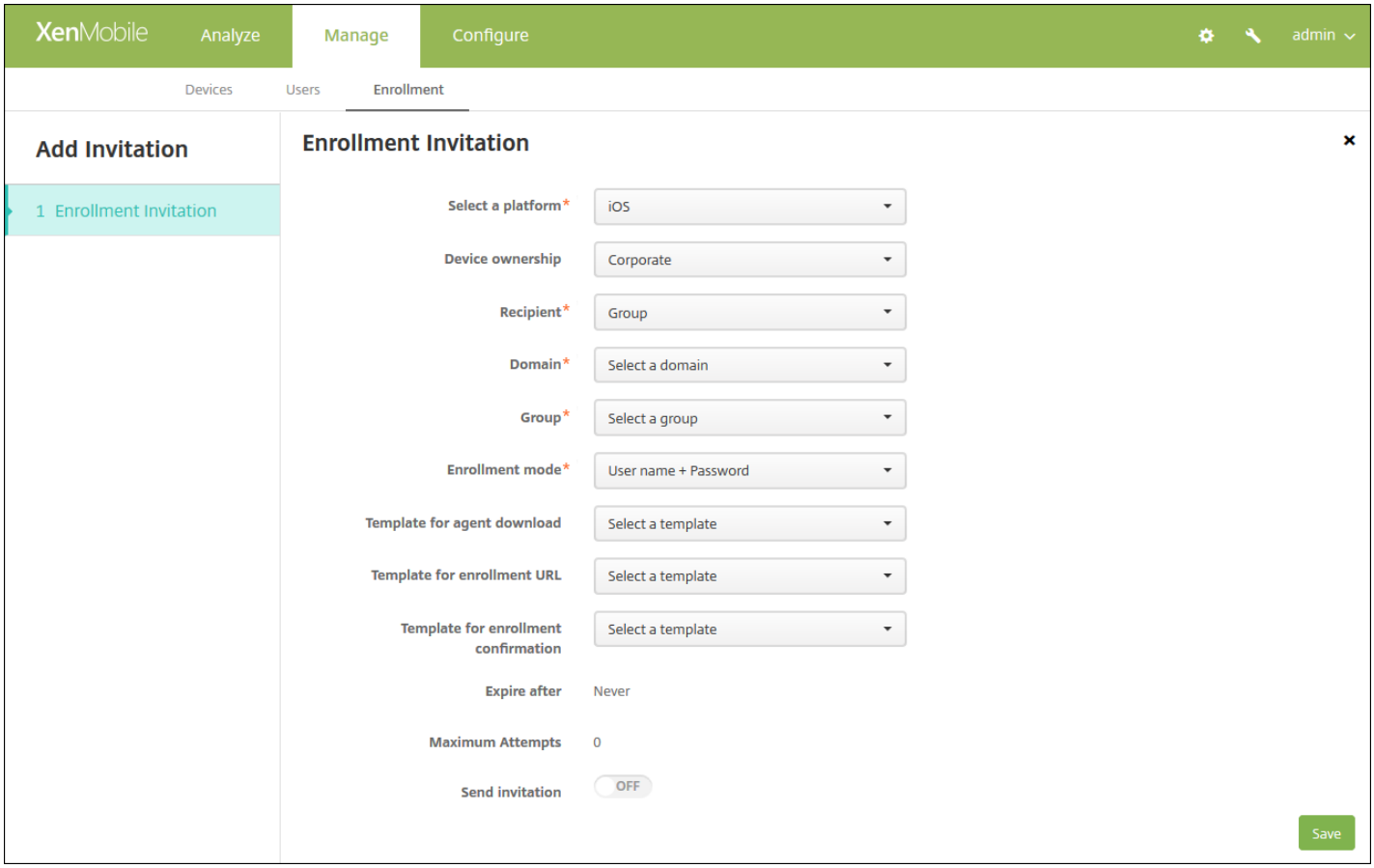
- **Opérateur** : dans la liste, sélectionnez un opérateur auquel associer le numéro de téléphone de l'utilisateur.
- **Mode d'inscription** : dans la liste, cliquez sur la manière dont vous souhaitez que les utilisateurs s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Les options possibles sont les suivantes :
  - Haute sécurité
  - URL d'invitation
  - URL d'invitation + PIN
  - URL d'invitation + mot de passe
  - Deux facteurs
  - Nom d'utilisateur + PIN

  Remarque : lorsque vous sélectionnez un mode d'inscription qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche, dans lequel vous cliquez sur **Code PIN d'inscription**.

- **Modèle pour téléchargement de l'agent** : dans la liste, cliquez sur le modèle à utiliser pour l'invitation d'inscription. Les choix pour cette option sont basés sur le type de plate-forme. Par exemple, le **lien de téléchargement iOS** s'affiche si vous avez sélectionné **iOS** en tant que plate-forme.
- **Modèle pour l'URL d'inscription** : dans la liste, cliquez sur **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription** : dans la liste, cliquez sur **Confirmation d'inscription**.
- **Expire après** : ce champ est défini lorsque vous configurez le mode d'inscription et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes d'inscription.
- **Nbre max de tentatives** : ce champ est défini lorsque vous configurez le **Mode d'inscription** et indique le nombre maximal de fois que le processus d'inscription peut être tenté. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes d'inscription.
- **Envoyer invitation** : sélectionnez **ON** pour envoyer l'invitation immédiatement ou cliquez sur **OFF** pour uniquement ajouter l'invitation au tableau de la page **Inscription**.

2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation** ; sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Inscription**.

Pour envoyer une invitation d'inscription à un groupe



1. Pour configurer ces paramètres :

- **Domaine** : dans la liste, cliquez sur le domaine à partir duquel choisir le groupe.
- **Groupe** : dans la liste, cliquez sur le groupe qui recevra l'invitation.
- **Mode d'inscription** : dans la liste, cliquez sur la manière dont vous souhaitez que les utilisateurs du groupe s'inscrivent. La valeur par défaut est **Nom d'utilisateur + mot de passe**. Les options possibles sont les suivantes :
  - Haute sécurité
  - URL d'invitation
  - URL d'invitation + PIN
  - URL d'invitation + mot de passe
  - Deux facteurs
  - Nom d'utilisateur + PIN

  Remarque : lorsque vous sélectionnez un mode d'inscription qui comprend un code PIN, le champ **Modèle pour le code PIN d'inscription** s'affiche, dans lequel vous cliquez sur **Code PIN d'inscription**.

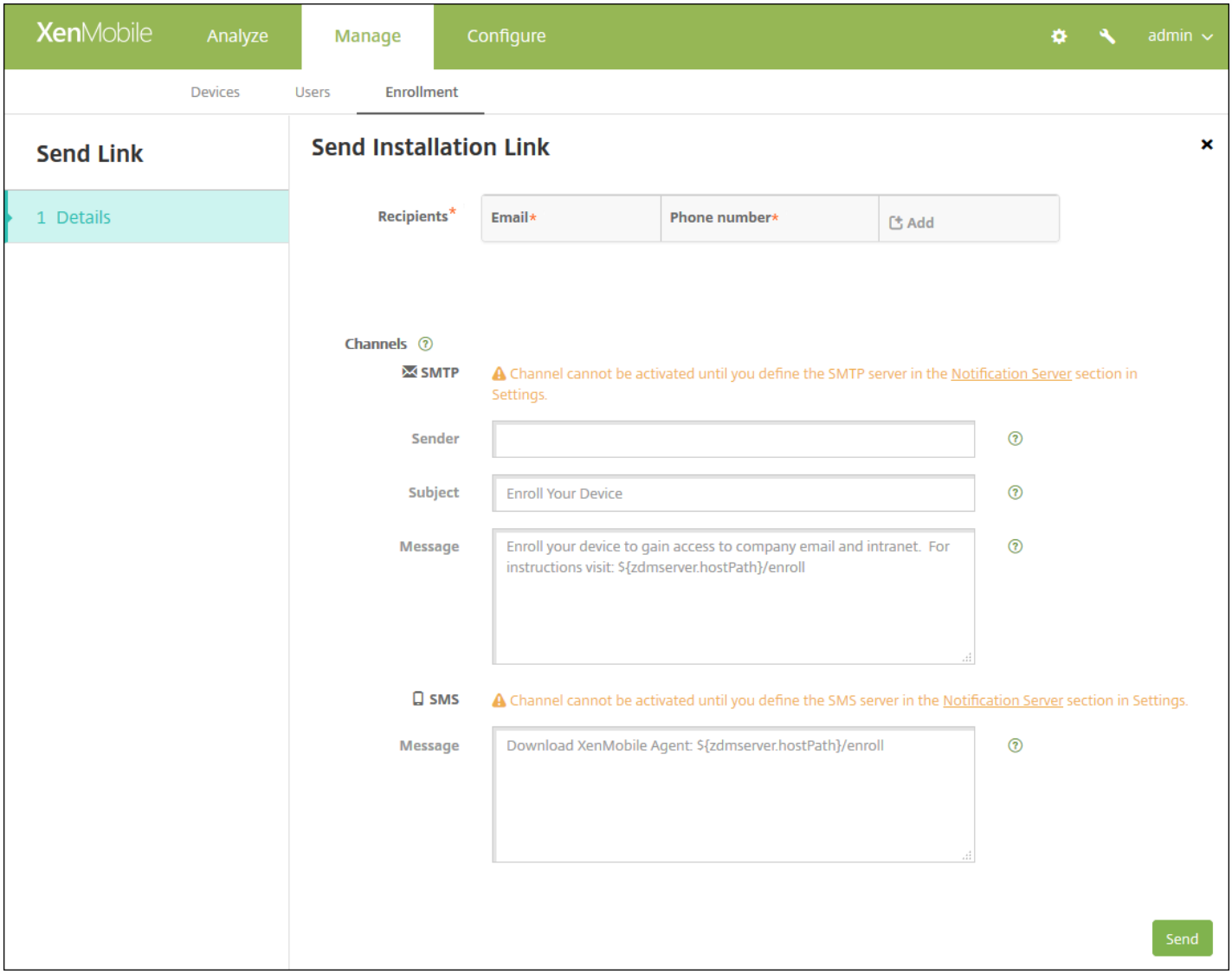
- **Modèle pour téléchargement de l'agent** : dans la liste, cliquez sur le modèle à utiliser pour l'invitation d'inscription. Les choix pour cette option sont basés sur le type de plate-forme. Par exemple, le **lien de téléchargement iOS** s'affiche si vous avez sélectionné **iOS** en tant que plate-forme.
- **Modèle pour l'URL d'inscription** : dans la liste, cliquez sur **Invitation d'inscription**.
- **Modèle pour la confirmation d'inscription** : dans la liste, cliquez sur **Confirmation d'inscription**.
- **Expire après** : ce champ est défini lorsque vous configurez le mode d'inscription et indique quand l'inscription expire. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes

d'inscription.

- **Nbre max de tentatives** : ce champ est défini lorsque vous configurez le Mode d'inscription et indique le nombre maximal de fois que le processus d'inscription peut être tenté. Pour plus d'informations sur la configuration des modes d'inscription, veuillez consulter la section Pour configurer les modes d'inscription.
- **Envoyer invitation** : sélectionnez **ON** pour envoyer l'invitation immédiatement ou cliquez sur **OFF** pour uniquement ajouter l'invitation au tableau de la page **Inscription**.

2. Cliquez sur **Enregistrer et Envoyer** si vous avez activé **Envoyer invitation** ; sinon, cliquez sur **Enregistrer**. L'invitation apparaît dans le tableau sur la page **Inscription**.

Pour envoyer un lien d'installation



Avant de pouvoir envoyer un lien d'installation de l'inscription, vous devez configurer les canaux (SMTP ou SMS) sur le serveur de notification à partir de la page **Paramètres**. Pour plus de détails, consultez Notifications.

1. Pour configurer ces paramètres :

- **Destinataire** : pour chaque destinataire que vous souhaitez ajouter, cliquez sur Ajouter et procédez comme suit :

- **Adresse électronique** : entrez l'adresse e-mail du destinataire. Ce champ est obligatoire.
- **Numéro de téléphone** : entrez le numéro de téléphone de l'utilisateur. Ce champ est obligatoire.
- Cliquez sur **Enregistrer**.

  Remarque : pour supprimer un destinataire existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

  Pour modifier un destinataire, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

- **Canaux** : sélectionnez un canal à utiliser pour envoyer le lien d'installation de l'inscription. Vous pouvez envoyer des notifications via **SMTP** ou **SMS**. Ces canaux (SMTP ou SMS) ne peuvent pas être activés tant que vous n'avez pas configuré les paramètres du serveur sur la page **Paramètres** dans **Serveur de notification**. Pour plus de détails, consultez Notifications.
  - **SMTP** : configurez ces paramètres facultatifs. Si vous ne renseignez pas ces champs, les valeurs par défaut spécifiées dans le modèle de notification configuré pour la plate-forme que vous avez sélectionnée sont utilisées :
    - **Expéditeur**. Entrez un expéditeur (facultatif).
    - **Sujet** : entrez un sujet pour le message (facultatif). Par exemple, « inscription de votre appareil ».
    - **Message** : entrez le message à envoyer au destinataire (facultatif). Par exemple, « Inscrivez votre appareil pour accéder à la messagerie et aux applications de l'entreprise ».
  - **SMS** : configurez ce paramètre. Si vous ne renseignez pas ce champ, la valeur par défaut spécifiée dans le modèle de notification configuré pour la plate-forme que vous avez sélectionnée est utilisée :
    - **Message** : entrez le message à envoyer aux destinataires. Ce champ est obligatoire pour les notifications SMS.

      Remarque : en Amérique du Nord, les messages SMS qui dépassent 160 caractères sont remis dans plusieurs messages.

2. Cliquez sur **Envoyer**.

> ## Remarque
>
> Si votre environnement tire parti de l'attribut SAMAccountName, après que les utilisateurs aient reçu l'invitation et cliqué sur le lien, ils doivent modifier le nom d'utilisateur pour compléter l'authentification. Par exemple, ils doivent supprimer nomdomaine dans SAMAccountName@nomdomaine.com.

Limite d'inscription d’appareils

Feb 23, 2017

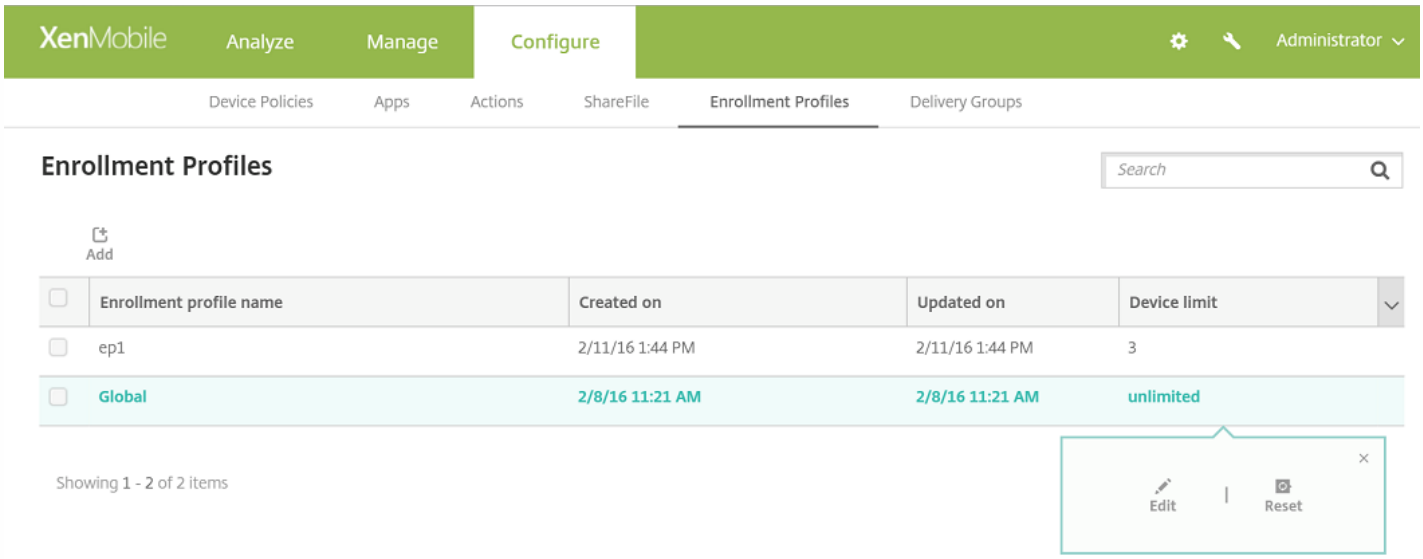
Vous pouvez limiter le nombre d'appareils qu'un utilisateur peut inscrire sous **Configurer > Profils d'inscription** dans la console XenMobile, en modes de serveur ENT, MDM et MAM. Ces limitations peuvent s'appliquer de manière globale ou par groupe de mise à disposition. Vous pouvez créer plusieurs profils d'inscription et les associer à différents groupes de mise à disposition.

Si vous ne définissez aucune limite, les utilisateurs peuvent inscrire un nombre illimité d'appareils. Cette fonctionnalité est uniquement prise en charge sur les appareils iOS et Android.

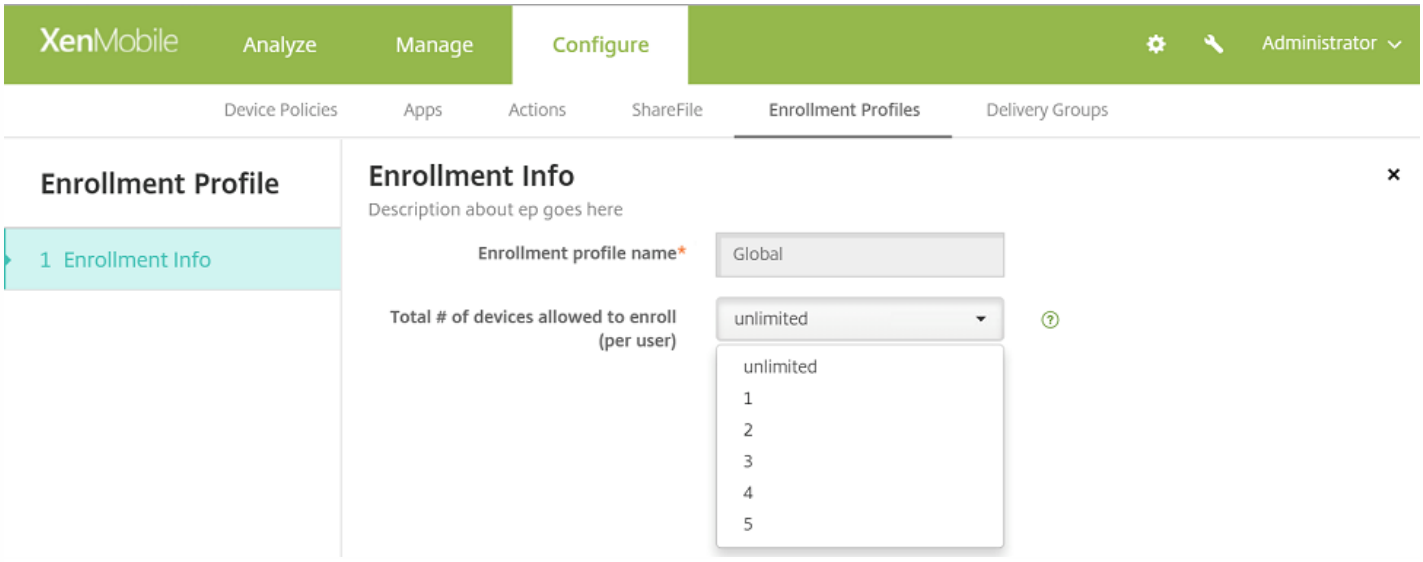
Pour configurer une limite d'inscription d'appareils globale

1. Accédez à **Configurer > Profils d'inscription**.

2. Cliquez sur **Global** et sélectionnez **Modifier**.



L'écran **Infos d'inscription** s'affiche et **Global** est renseigné automatiquement en tant que nom de profil. À ce stade, vous pouvez sélectionner le nombre total d'appareils que les utilisateurs sont autorisés à inscrire. Cette limitation s'appliquera à tous les utilisateurs inscrits auprès de XenMobile.

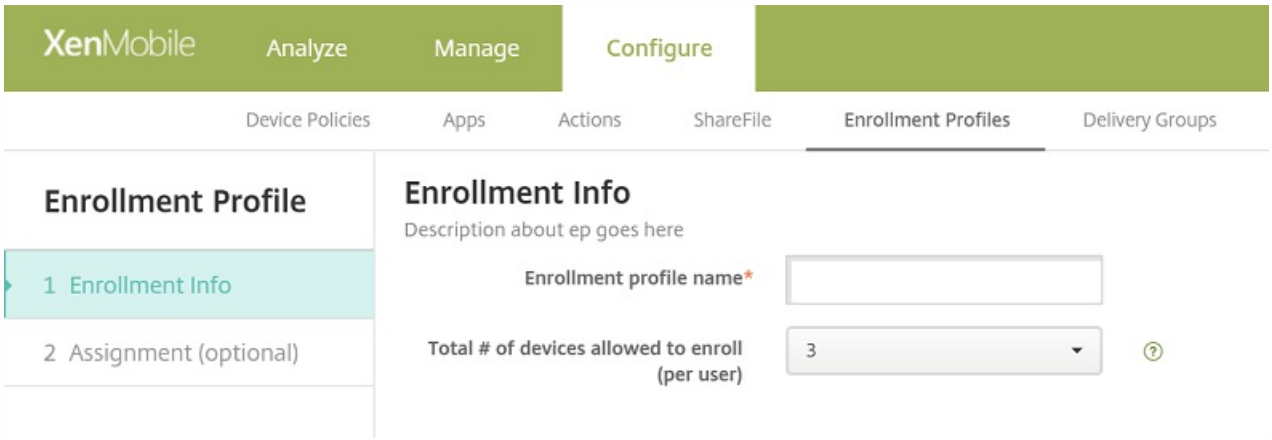


Pour configurer une limite d'inscription d'appareils pour un groupe de mise à disposition

1. Accédez à **Configurer > Profils d'inscription > Ajouter**.

   L'écran **Infos d'inscription** s'affiche.

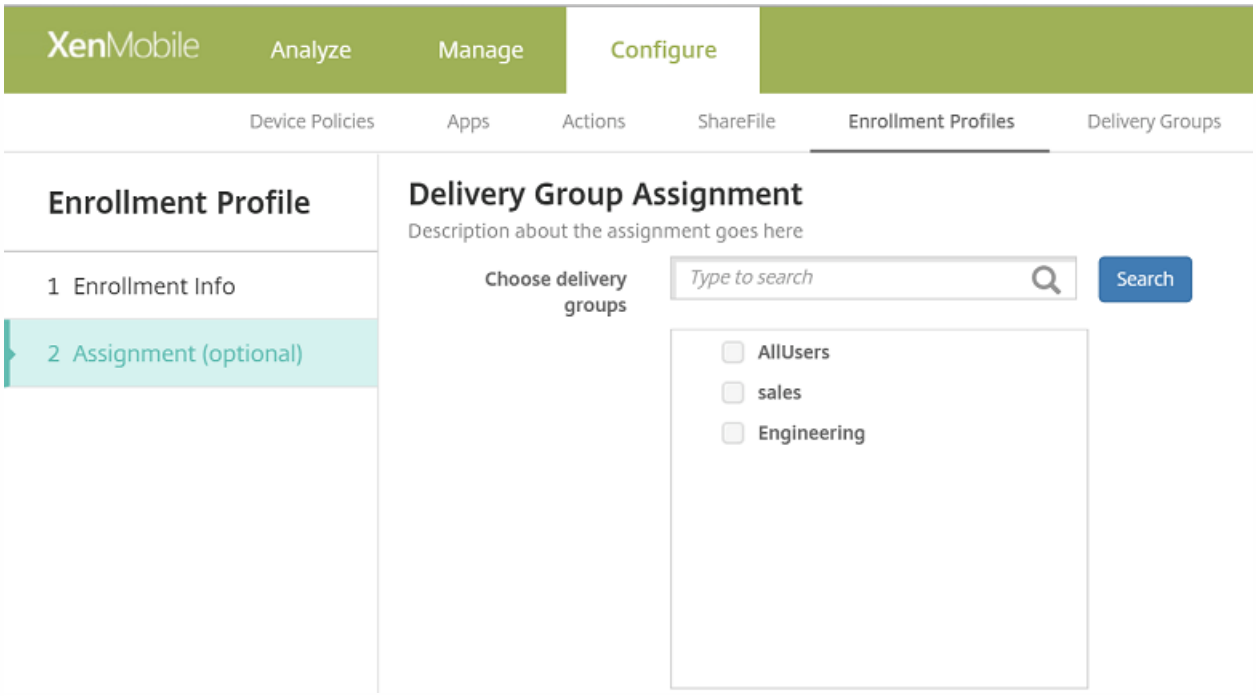
2. Entrez un nom pour le nouveau profil d'inscription, puis sélectionnez le nombre d'appareils que les membres de ce profil sont autorisés à inscrire.



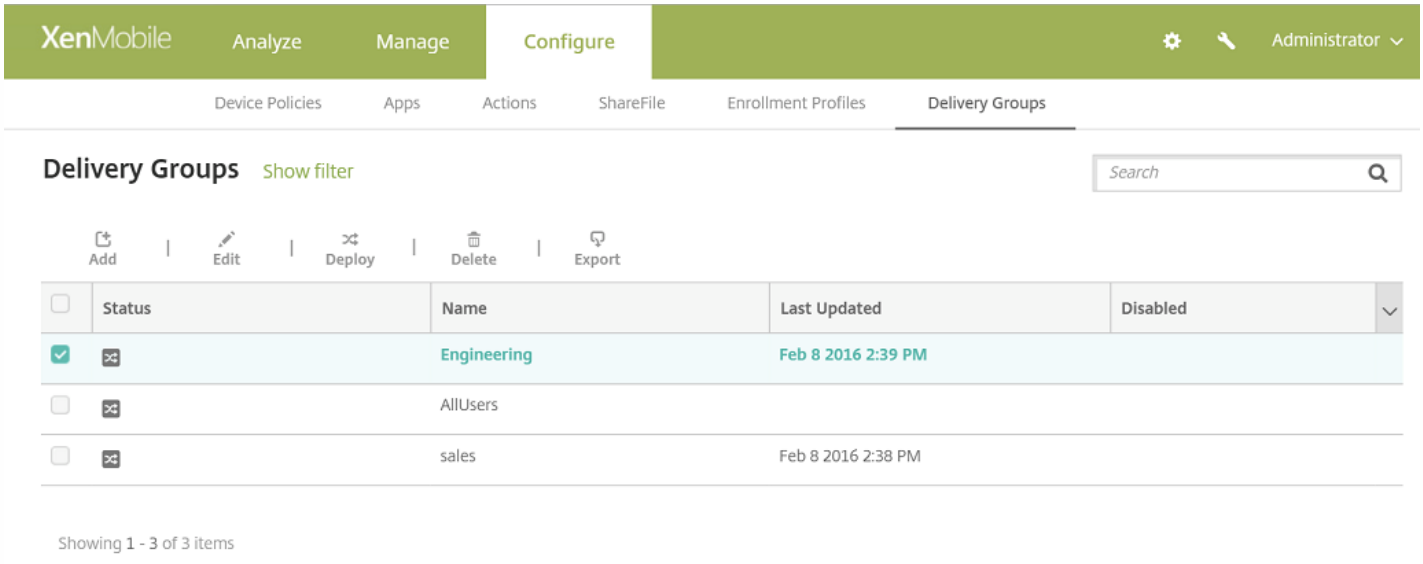
3. Cliquez sur **Next**.

   L'écran **Attribution de groupes de mise à disposition** s'affiche.

4. Sélectionnez les groupes de mise à disposition auxquels la limite d'inscription d'appareils doit s'appliquer, puis cliquez sur **Enregistrer**.

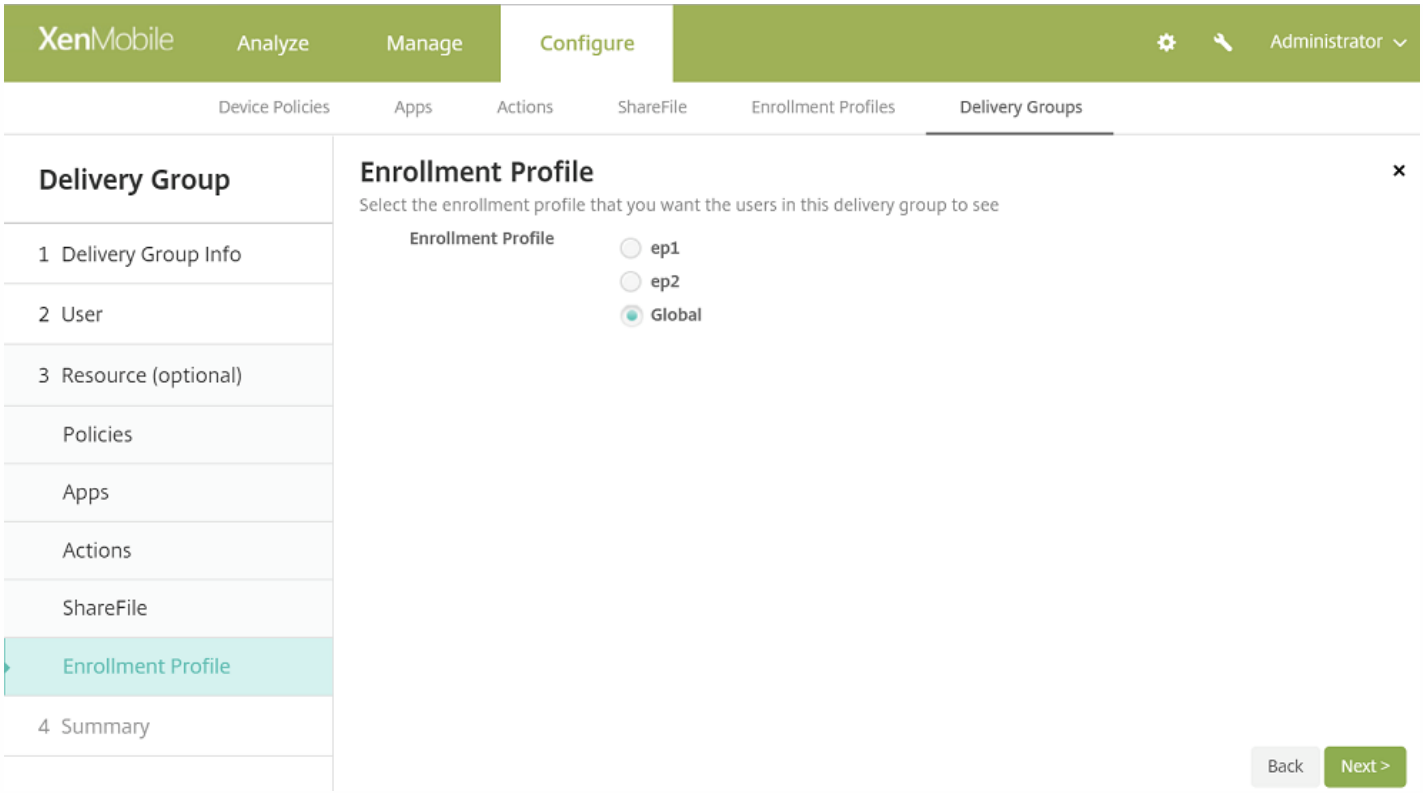


Si vous souhaitez modifier le profil d'inscription d'un groupe de mise à disposition ultérieurement, accédez à **Configurer > Groupes de mise à disposition**. Sélectionnez le groupe en question, puis cliquez sur **Modifier**.



L'écran **Profil d'inscription** s'affiche.

5. Sur cet écran, sélectionnez le profil d'inscription que vous souhaitez appliquer à ce groupe de mise à disposition, puis cliquez sur **Suivant** pour afficher et enregistrer vos modifications.



Expérience utilisateur avec une limite d'inscription d'appareils

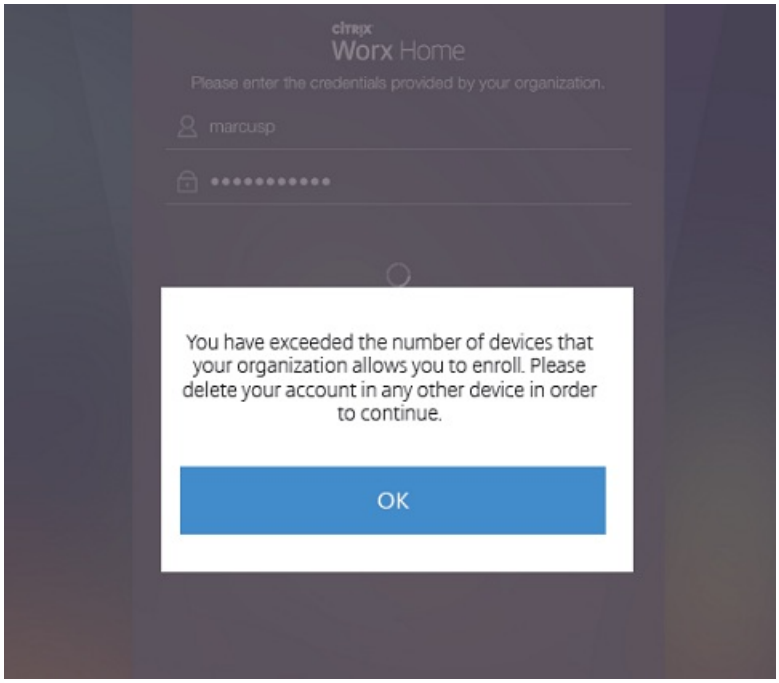
Lorsque vous définissez la limite d'inscription d'appareils et que les utilisateurs tentent d'inscrire un appareil, ils procèdent comme suit :

1. Ils se connectent à Secure Hub.

2. Ils entrent une adresse de serveur pour s'inscrire.

3. Ils entrent leurs informations d'identification.

4. Si la limite d'appareils est atteinte, un message d'erreur s'affiche, indiquant à l'utilisateur que le nombre maximal d'enregistrements d'appareils est dépassé et qu'il doit contacter un administrateur.



L'écran d'inscription Secure Hub s'affiche de nouveau.

Appareils partagés

Feb 23, 2017

XenMobile vous permet de configurer des appareils qui peuvent être partagés par de multiples utilisateurs. Cette fonctionnalité permet, par exemple, aux médecins hospitaliers d'utiliser tout appareil à portée pour accéder à des applications et des données plutôt que d'avoir à transporter un appareil spécifique. Il peut aussi être utile pour les employés travaillant en équipe dans des domaines tels que la force publique, le commerce et le secteur industriel de partager des appareils pour réduire le coût du matériel.

Points clés à propos des appareils partagés

Mode MDM

- Disponible sur tablettes et smartphones iOS et Android. L'inscription au programme Device Enrollment Program (DEP) de base n'est pas prise en charge pour un appareil partagé XenMobile Enterprise. Vous devez utiliser une DEP autorisée pour inscrire un appareil partagé dans ce mode.
- L'authentification de certificat client, le code PIN Citrix, Touch ID, l'entropie utilisateur et l'authentification à deux facteurs ne sont pas pris en charge.

Mode MDM+MAM

- Disponible uniquement sur tablettes iOS et Android.
- Pris en charge sur XenMobile 10.3.x et versions ultérieures.
- Seule l'authentification par nom d'utilisateur et mot de passe Active Directory est prise en charge.
- L'authentification de certificat client, le code PIN Worx, Touch ID, l'entropie utilisateur et l'authentification à deux facteurs ne sont pas pris en charge.
- Le mode MAM exclusif n'est pas pris en charge. Les appareils doivent s'inscrire en mode MDM.
- Seuls Secure Mail, Secure Web et l'application mobile ShareFile sont pris en charge. Les applications HDX ne sont pas prises en charge.
- Seuls les utilisateurs Active Directory sont pris en charge, contrairement aux utilisateurs et aux groupes locaux.
- Une réinscription est requise pour les appareils partagés en mode MDM exclusif afin de mettre à jour vers le mode MDM+MAM.
- Les utilisateurs peuvent uniquement partager des applications XenMobile et des applications wrappées MDX, mais ils ne peuvent pas partager d'applications natives sur les appareils.
- Une fois les applications XenMobile téléchargées lors de la première inscription, il est inutile de les télécharger à nouveau à chaque fois qu'un utilisateur se connecte sur l'appareil. Le nouvel utilisateur peut récupérer l'appareil, ouvrir une session, et se lancer.
- Sur Android, afin d'isoler les données de chaque utilisateur pour des raisons de sécurité, la stratégie **Disallow rooted devices** de la console XenMobile doit être définie sur **Activé**.

Configuration requise pour l'inscription d'appareils partagés

Avant d'inscrire les appareils partagés, vous devez effectuer les opérations suivantes :

- Créer un rôle utilisateur d'inscription d'appareil partagé. Voir Configuration de rôles avec RBAC.
- Créer un utilisateur d'appareil partagé. Voir Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile.
- Créer un groupe de mise à disposition qui contient les stratégies de base, les applications et les actions que vous souhaitez appliquer à l'utilisateur d'inscription d'appareil partagé. Voir Gestion des groupes de mise à disposition.

Conditions préalables pour le mode MDM+MAM

1. Créez un groupe Active Directory nommé, par exemple, **Shared Device Enrollers**.
2. Ajoutez à ce groupe les utilisateurs Active Directory qui vont inscrire des appareils partagés. Si vous souhaitez utiliser un nouveau compte à cette fin, créez un utilisateur Active Directory (par exemple **sdenroll**) et ajoutez cet utilisateur au groupe Active Directory.

Configuration requise pour les appareils partagés

Pour garantir une expérience utilisateur optimale, y compris l'installation et la suppression silencieuse des applications, Citrix recommande de configurer les appareils partagés sur les plates-formes suivantes :

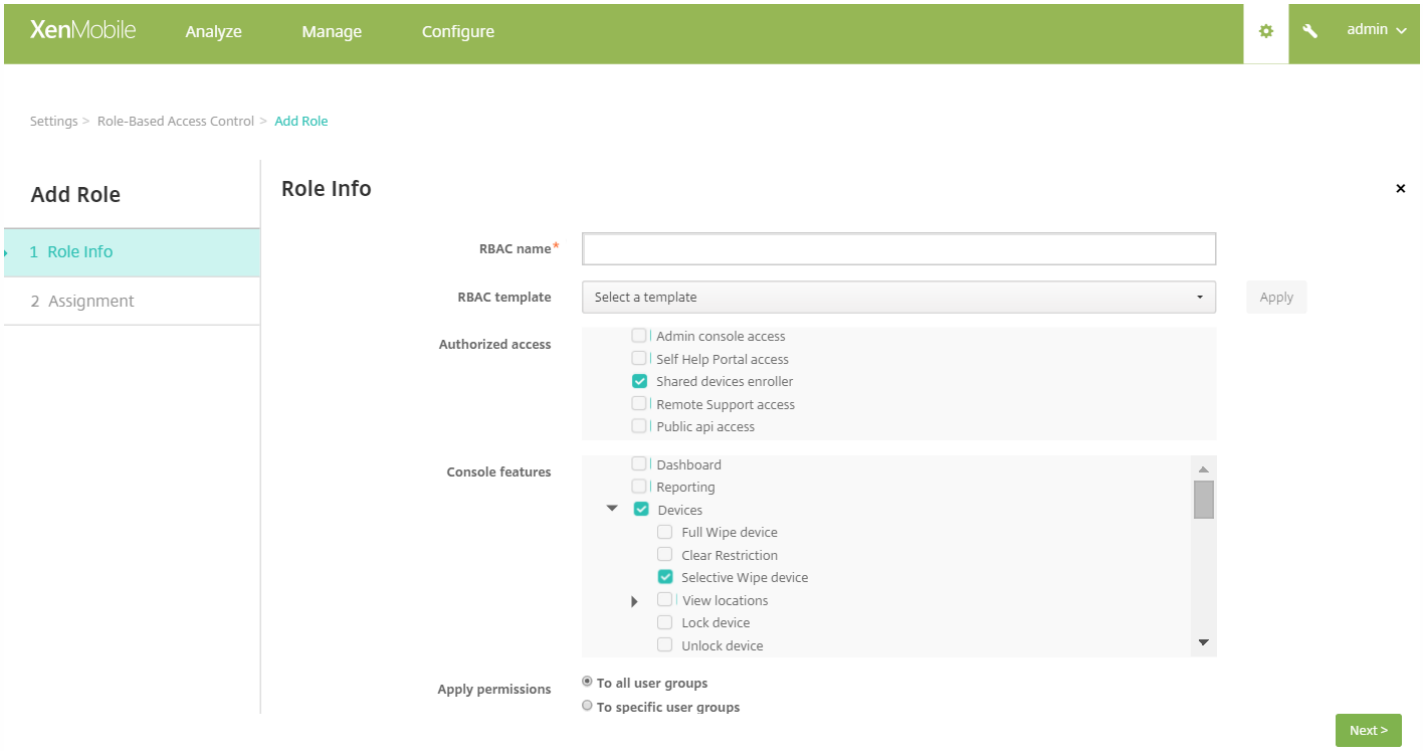
- iOS 9 et 10
- Android M
- Android 5.x
- Android 4.4.x
- Android 4.0.x (mode MDM exclusif)

Configuration d'un appareil partagé

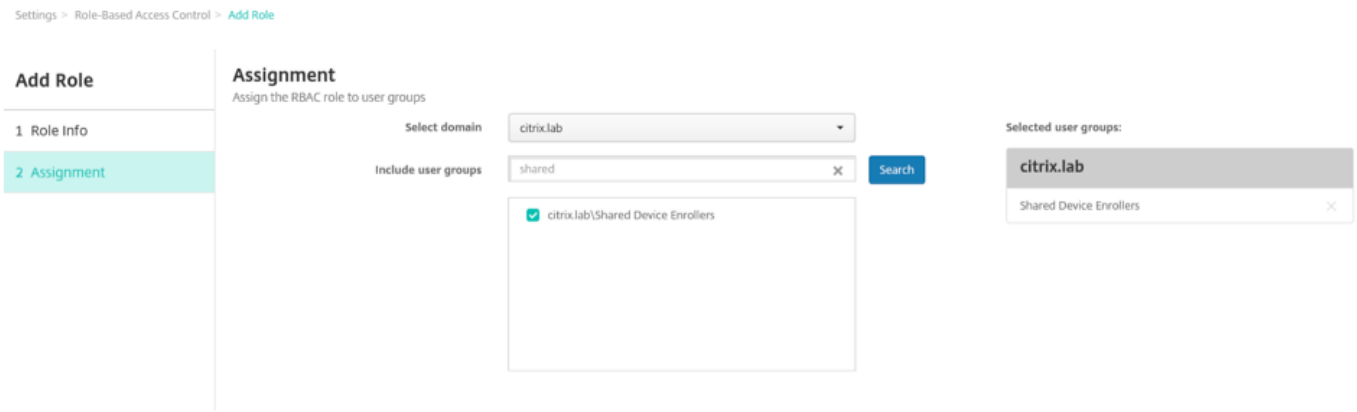
Suivez les étapes ci-dessous pour configurer un appareil partagé.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page Paramètres s'affiche.
2. Cliquez sur **Contrôle d'accès basé sur rôle**, puis cliquez sur **Ajouter**. L'écran **Ajouter un rôle** s'affiche.
3. Créez un rôle utilisateur destiné à l'inscription d'appareils partagés, nommé **Utilisateur pour inscription d'appareils partagés**, disposant des autorisations **Assistant d'inscription d'appareils partagés** sous **Accès autorisé**. Veillez à développer **Appareils** dans **Fonctionnalités de la console**, puis sélectionnez **Effacer les données d'entreprise d'un appareil**. Ce paramètre garantit que les applications et les stratégies configurées à l'aide du compte de l'assistant d'inscription d'appareils partagés sont supprimées via Secure Hub lors de la désinscription de l'appareil.

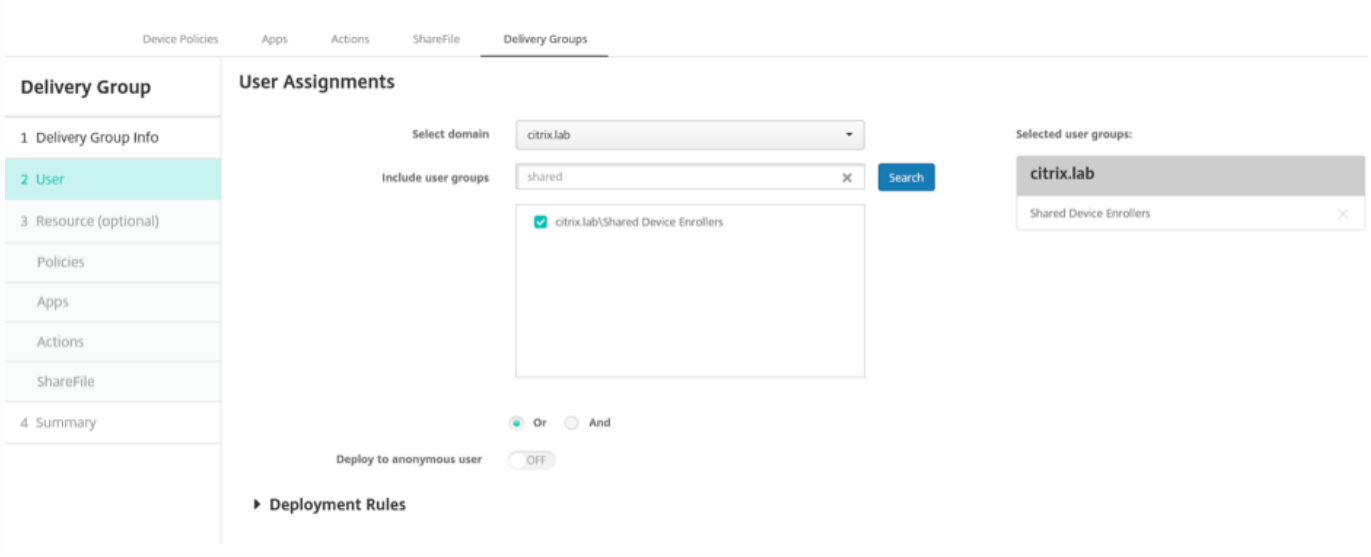
   Pour **Appliquer les autorisations**, conservez le paramètre par défaut, qui est **À tous les groupes d'utilisateurs**, ou attribuez des autorisations à des groupes d'utilisateurs Active Directory spécifiques avec le paramètre **À des groupes d'utilisateurs spécifiques**.



Cliquez sur **Suivant** pour passer à l'écran **Attribution**. Attribuez le rôle d'inscription d'appareil partagé que vous venez de créer au groupe Active Directory que vous avez créé pour les utilisateurs destinés à l'inscription d'appareils partagés à l'étape 1 sous Conditions préalables. Dans l'image ci-dessous, **citrix.lab** est le domaine Active Directory et **Shared Device Enrollers** est le groupe Active Directory.



4. Créez un groupe de mise à disposition contenant les stratégies de base, les applications et les actions que vous voulez appliquer à l'appareil lorsqu'un utilisateur n'est pas connecté. Associez ensuite ce groupe de mise à disposition au groupe Active Directory de l'utilisateur d'inscription d'appareil partagé.



5. Installez Secure Hub sur l'appareil partagé et inscrivez-le sur XenMobile à l'aide du compte utilisateur d'inscription sur appareil partagé. Vous pouvez maintenant voir et gérer l'appareil dans la console XenMobile. Pour de plus amples informations, consultez la section Inscription d'appareils.

6. Pour appliquer différentes stratégies ou pour fournir des applications supplémentaires aux utilisateurs authentifiés, vous devez créer un groupe de mise à disposition associé à ces utilisateurs et déployé uniquement sur des appareils partagés. Lors de la création de groupes, configurez des règles de déploiement pour vous assurer que les packages sont déployés sur des appareils partagés. Pour plus d'informations, consultez la section Configuration des règles de déploiement.

7. Pour arrêter le partage de l'appareil, effacez les données d'entreprise afin de supprimer le compte utilisateur d'inscription sur appareil partagé de l'appareil, ainsi que toute application ou stratégie ayant été déployée sur cet appareil.

Expérience utilisateur relative à l'utilisation d'un appareil partagé

Mode MDM

Les utilisateurs voient uniquement les ressources qui leur sont disponibles, et leur expérience est la même sur chaque appareil partagé. Les stratégies et applications de l'inscription d'appareil partagé restent toujours sur l'appareil. Lorsqu'un utilisateur non inscrit sur les appareils partagés ouvre une session sur Secure Hub, les stratégies et applications de cette personne sont déployées sur l'appareil. Lorsque cet utilisateur se déconnecte, les stratégies et les applications qui diffèrent de celles de l'inscription d'appareil partagé sont supprimées, tandis que les ressources de l'inscription d'appareil partagé restent intactes.

Mode MDM+MAM

Secure Mail et Secure Web sont déployés sur l'appareil lorsqu'ils sont inscrits par l'utilisateur d'inscription d'appareil partagé. Les données utilisateur sont conservées de manière sécurisée sur l'appareil. Les données ne sont pas affichées pour d'autres utilisateurs lorsqu'ils se connectent à Secure Mail ou Secure Web.

Un seul utilisateur à la fois peut se connecter à Secure Hub. L'utilisateur précédent doit se déconnecter pour que le prochain

utilisateur puisse se connecter. Pour des raisons de sécurité, Secure Hub ne stocke pas les informations d'identification de l'utilisateur sur les appareils partagés, si bien que les utilisateurs doivent entrer leurs informations d'identification chaque fois qu'ils se connectent. Pour vous assurer qu'un nouvel utilisateur ne puisse pas accéder aux ressources destinées à l'utilisateur précédent, Secure Hub n'autorise pas les nouveaux utilisateurs à se connecter alors que des stratégies, applications et données associées à l'utilisateur précédent sont en cours de suppression.

L'inscription d'appareil partagé ne modifie pas le processus de mise à niveau des applications. Vous pouvez distribuer des mises à niveau aux utilisateurs d'appareils partagés comme vous le faites habituellement. Ces derniers peuvent alors mettre à niveau les applications directement sur leurs appareils.

Stratégies Secure Mail recommandées

- Pour obtenir des performances Secure Mail optimales, définissez la **Période de synchronisation maximale** en fonction du nombre d'utilisateurs qui partagent l'appareil. Il n'est pas recommandé d'autoriser un nombre illimité de synchronisation.

Nombre d'utilisateurs partageant l'appareil	Période de synchronisation maximale recommandée
21 à 25	1 semaine ou moins
6 à 20	2 semaines ou moins
5 ou moins	1 mois ou moins

- Bloquez **Activer l'exportation des contacts** afin de ne pas divulguer les contacts d'un utilisateur aux autres utilisateurs qui partagent l'appareil.

- Sur iOS, seuls les paramètres suivants peuvent être définis par utilisateur. Tous les autres paramètres seront communs à tous les utilisateurs qui partagent l'appareil :

  Notifications
  Signature
  Absent(e) du bureau
  Période de synchronisation des messages
  S/MIME
  Orthographe

Android for Work

Mar 31, 2017

Android at Work (anciennement appelé Android for Work) est un espace de travail sécurisé disponible sur les appareils Android exécutant Android 5.0 et versions ultérieures. L'espace de travail isole les comptes, applications et données d'entreprise des comptes, applications et données personnels. Dans XenMobile, vous pouvez gérer les appareils BYOD et les appareils Android appartenant à l'entreprise en permettant aux utilisateurs de créer un profil professionnel séparé sur leurs appareils. En combinant le cryptage du matériel et les stratégies que vous déployez, vous séparez de manière sécurisée les zones professionnelles et personnelles d'un appareil. Vous pouvez gérer ou effacer à distance toutes les stratégies, applications et données d'entreprise sans affecter la zone personnelle de l'utilisateur. Pour de plus amples informations sur les appareils Android pris en charge, consultez le site Web Google Android Enterprise.

Vous utilisez Google Play pour ajouter, acheter et approuver des applications en vue de les déployer sur l'espace Android at Work d'un appareil. Vous pouvez utiliser Google Play pour déployer vos applications Android privées, en plus d'applications tierces et publiques. Lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour Android for Work à XenMobile, vous pouvez vérifier l'état de la licence d'achat groupé. Ce état représente le nombre total de licences disponibles, le nombre en cours d'utilisation et l'adresse e-mail de chaque utilisateur qui consomme des licences. Pour de plus amples informations sur l'ajout d'une application à XenMobile, consultez la section Pour ajouter un magasin d'applications public à XenMobile.

Configuration requise pour Android at Work :

- Un domaine publiquement accessible
- Un compte d'administrateur Google
- Les appareils qui prennent en charge les profils gérés et qui exécutent Android 5.0+ Lollipop
- Un compte Google sur lequel Google Play est installé
- Un profil de travail configuré sur l'appareil.

Avant de pouvoir définir des restrictions applicatives Android at Work, vous devez effectuer les opérations suivantes :

- Effectuer les tâches de configuration d'Android at Work sur Google.
- Créer des informations d'identification Google Play.
- Configurer les paramètres de serveur Android at Work.
- Créer au moins une stratégie Android at Work.
- Ajouter, acheter et approuver des applications Android at Work dans le magasin d'applications Google Play.

Vous pouvez utiliser les liens suivants lorsque vous gérez Android at Work :

- Console d'administration Google : https://admin.google.com/AdminHome
- Console d'administration Google Play : https://play.google.com/work/apps
- Publication sur Google Play pour les applications de chaînes privées et auto-hébergées : https://play.google.com/apps/publish
- Console Google Developer pour la création d'un compte de service : https://console.developers.google.com

Conditions requises par Android at Work

Avant de pouvoir administrer Android at Work dans XenMobile, vous devez effectuer les opérations suivantes :

- Créer un compte Android at Work.
- Configurer un compte de service.
- Télécharger un certificat Android at Work.
- Activer et autoriser les API SDK et MDM d'administrateur Google.
- Autoriser votre compte de service à utiliser Directory et Google Play.
- Obtenir un jeton de liaison.

Les sections suivantes expliquent comment effectuer chacune de ces tâches. Après avoir effectué ces tâches, vous pouvez créer des informations d'identification Google Play, configurer les paramètres Android et gérer les applications Android dans XenMobile. Pour plus d'informations sur la création d'un jeu d'informations d'identification, veuillez consulter la section Identifiants Google Play.

Créer un compte Android at Work

Vous devez remplir les conditions préalables suivantes avant de pouvoir configurer un compte Android at Work :

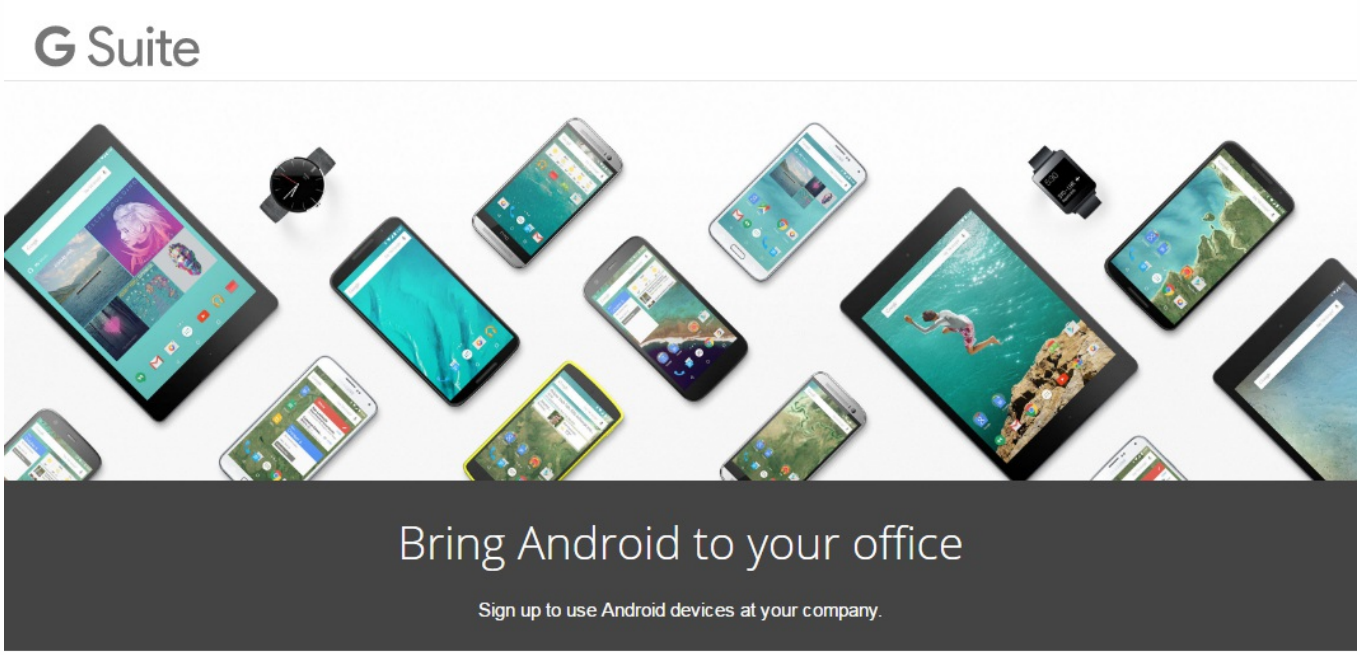
- Vous devez disposer d'un nom de domaine ; par exemple, exemple.com.
- Vous devez autoriser Google à vérifier que le domaine vous appartient.
- Vous devez activer et administrer Android at Work par le biais d'un fournisseur de gestion de la mobilité d'entreprise (EMM), tel que XenMobile 10.0 ou

version ultérieure.

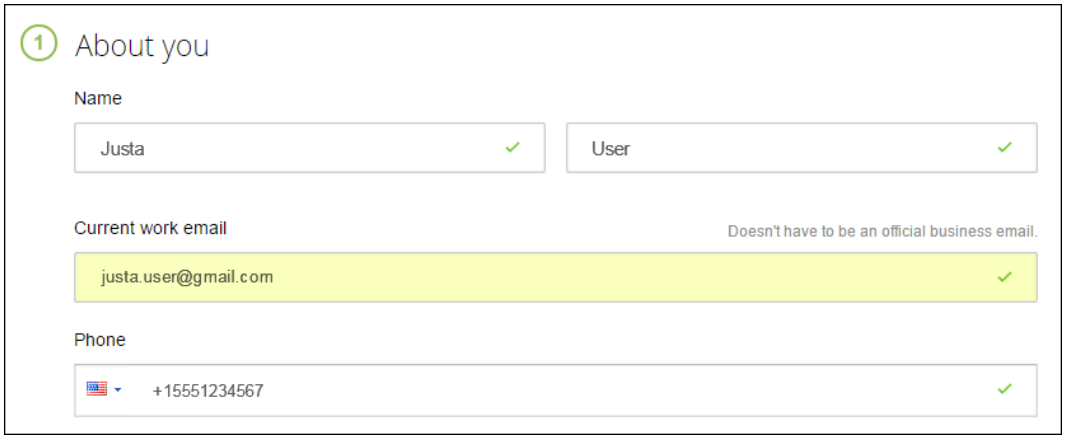
Si vous avez déjà vérifié votre nom de domaine auprès de Google, vous pouvez passer à cette étape : Configurer un compte de service Android at Work et télécharger un certificat Android at Work.

1. Accédez à https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

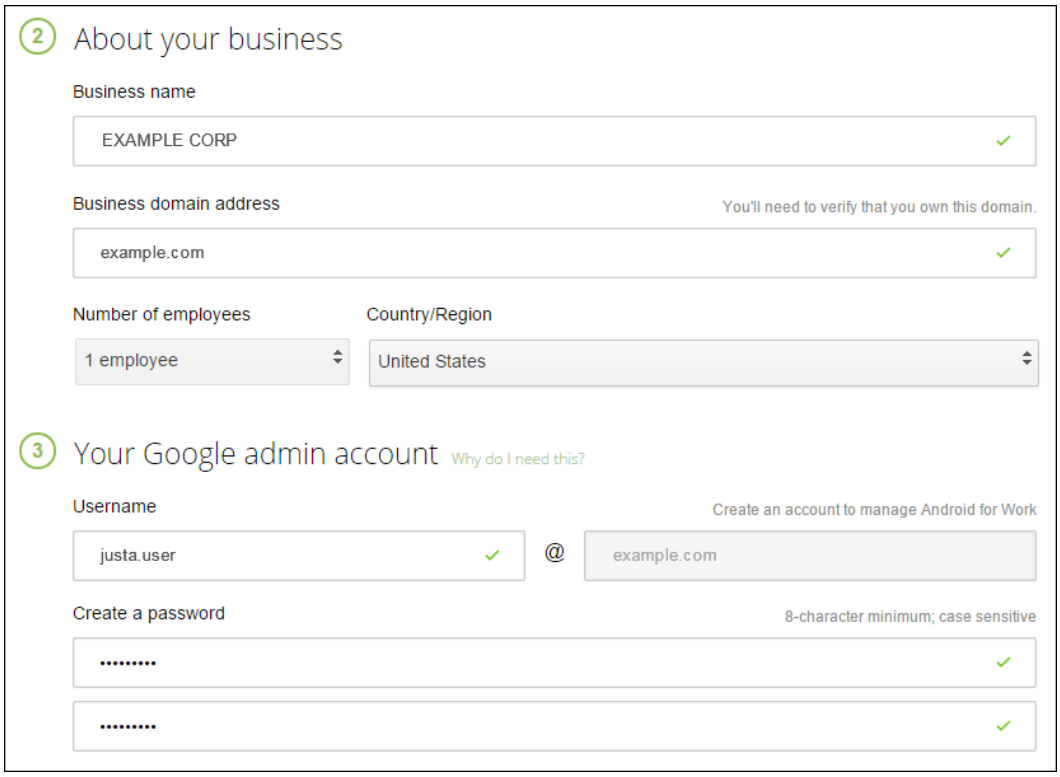
La page suivante s'affiche où vous entrez vos informations d'administrateur et les informations sur l'entreprise.



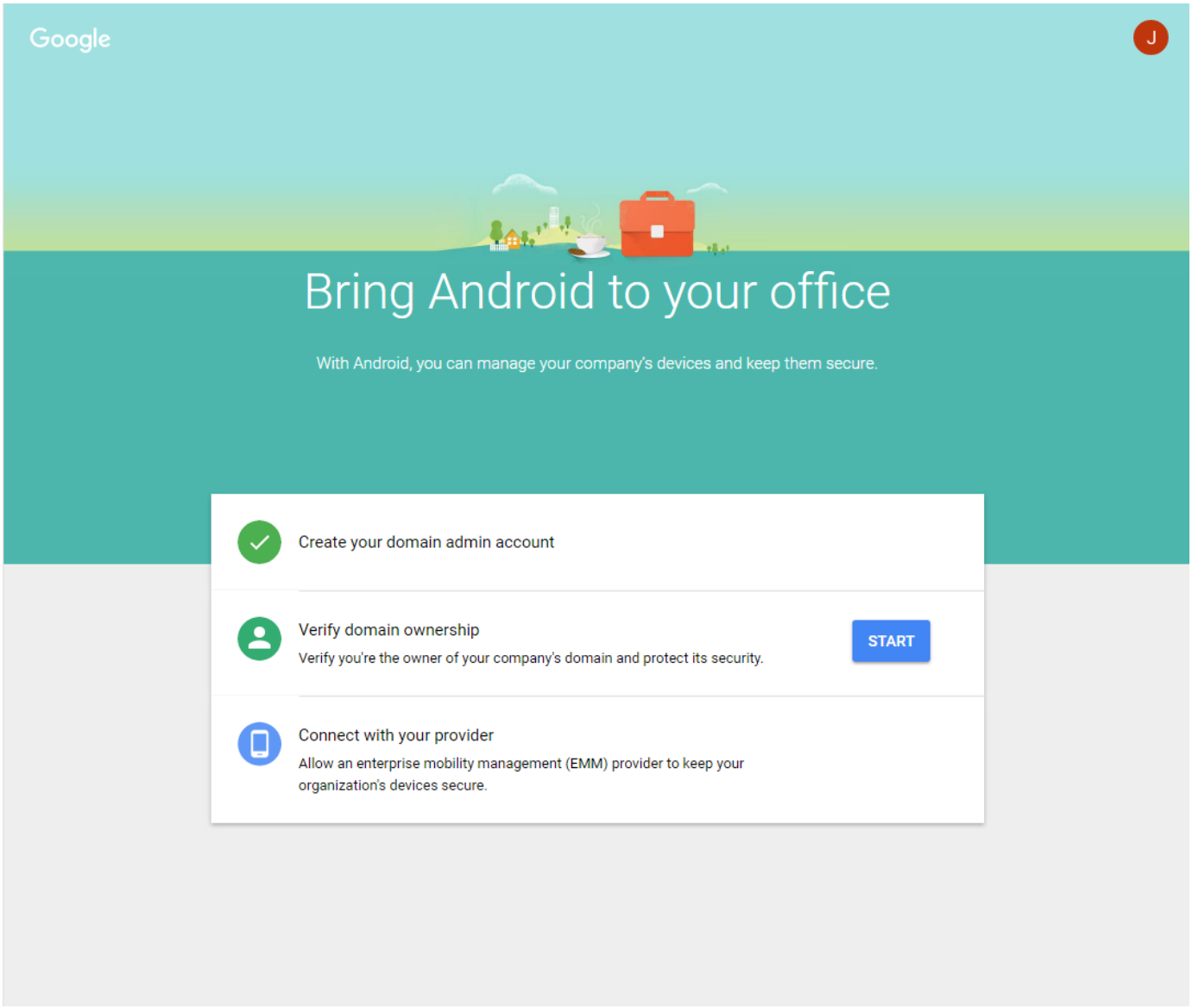
2. Entrez vos informations d'utilisateur administrateur.



2. Entrez vos informations d'entreprise, en plus de vos informations de compte d'administrateur.



La première étape de ce processus est terminée et la page suivante s'affiche.



Vérifier le propriétaire du domaine

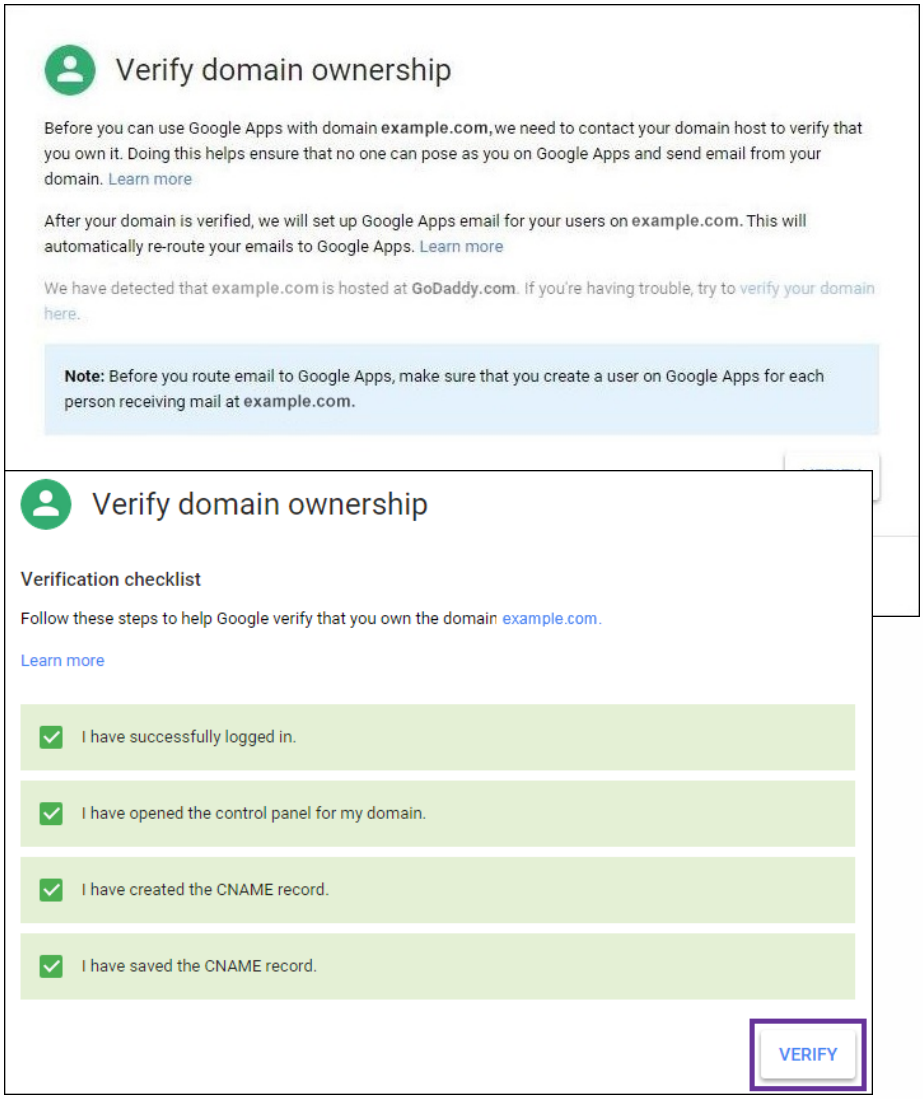
Autorisez Google à vérifier votre domaine de l'une des manières suivantes :

- Ajoutez un enregistrement TXT ou CNAME au site Web de votre hôte de domaine.
- Chargez un fichier HTML sur le serveur Web de votre domaine.
- Ajoutez une balise à votre page d'accueil. Google recommande la première méthode. Cet article ne couvre pas les étapes permettant de vérifier que votre domaine vous appartient, mais vous pouvez trouver les informations dont vous avez besoin sur : https://support.google.com/a/answer/6095407/.

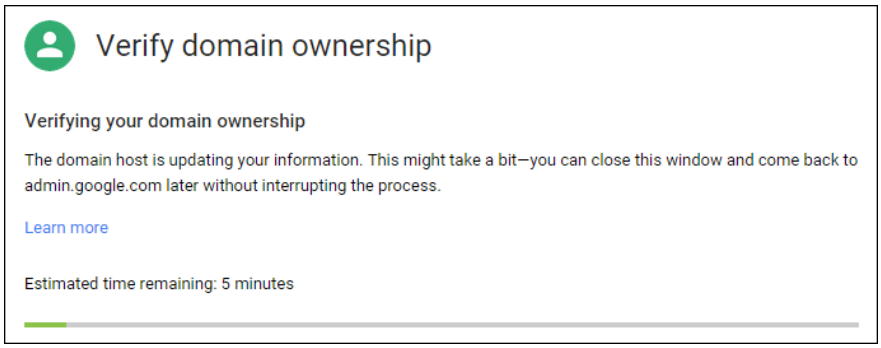
1. Cliquez sur **Démarrer** pour commencer la vérification de votre domaine.

La page **Valider la propriété du domaine** s'affiche. Suivez les instructions sur la page pour vérifier votre domaine.

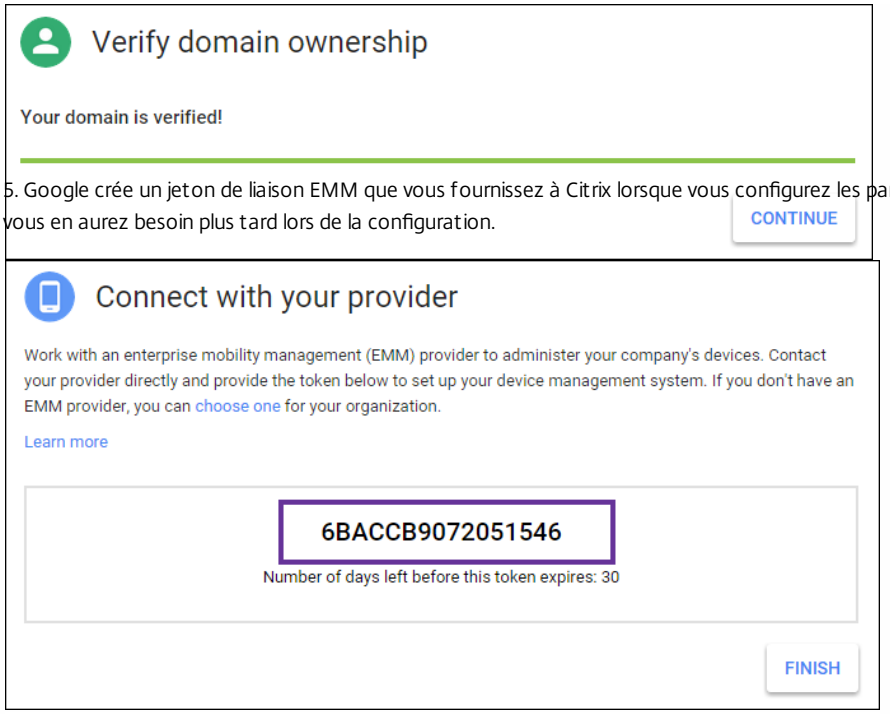
2. Cliquez sur **Vérifier**.



3. Google vérifie que vous êtes le propriétaire du domaine.



4. La page suivante s'affiche si la vérification réussit. Cliquez sur **Continuer**.



5. Google crée un jeton de liaison EMM que vous fournissez à Citrix lorsque vous configurez les paramètres d'Android at Work. Copiez et enregistrez le jeton ; vous en aurez besoin plus tard lors de la configuration.

6. Cliquez sur **Terminer** pour terminer la configuration Android at Work. Une page s'affiche indiquant que vous avez vérifié avec succès votre domaine.

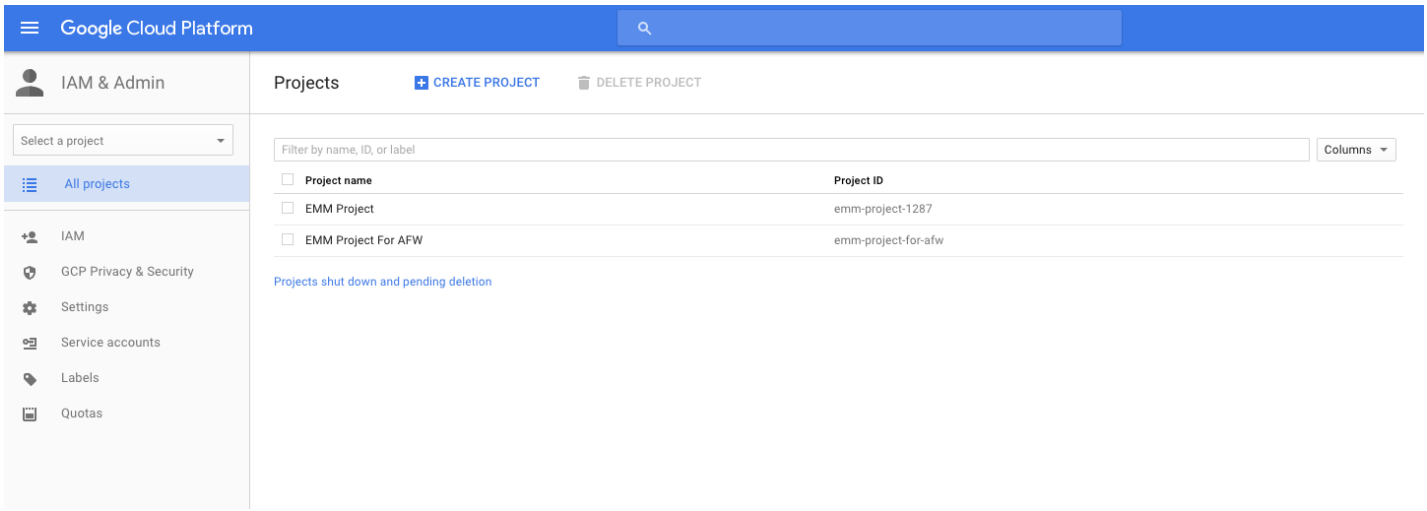
Une fois que vous avez créé un compte de service Android at Work, vous pouvez ouvrir une session sur la console d'administration Google pour gérer vos paramètres de gestion de la mobilité.

Définir un compte de service Android at Work et télécharger un certificat Android at Work

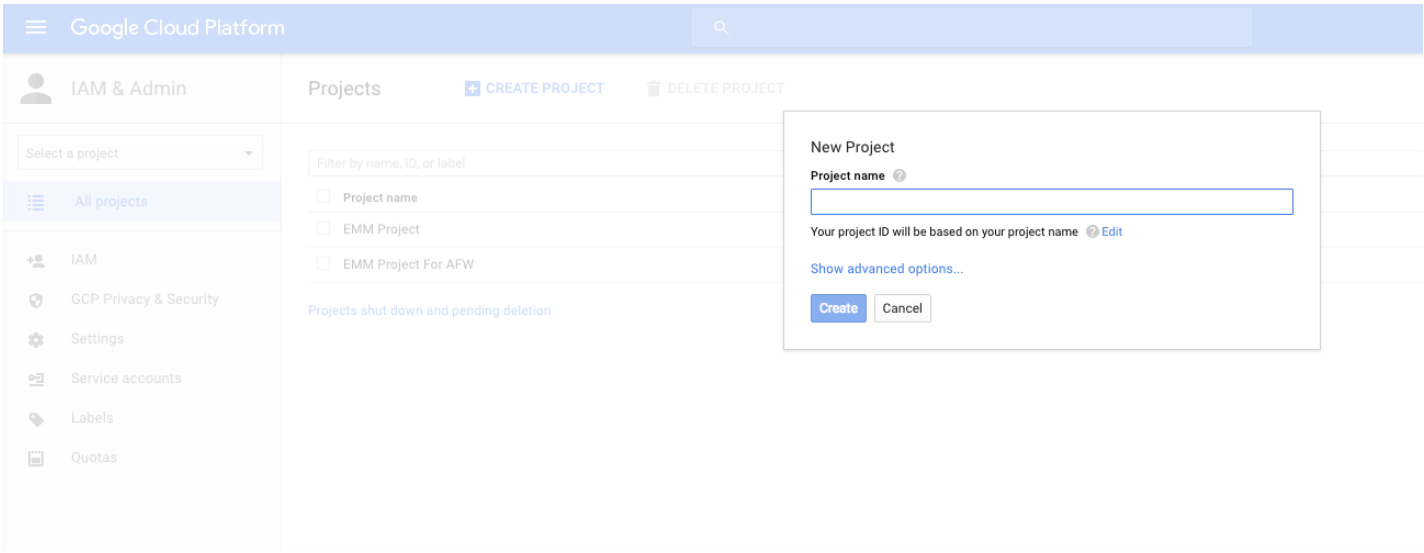
Pour autoriser XenMobile à contacter les services Google Play et Directory, vous devez créer un compte de service à l'aide du portail Project de Google destiné aux développeurs. Ce compte de service est utilisé pour permettre les communications entre serveurs entre XenMobile et les services Google pour Android. Pour de plus amples informations sur le protocole d'authentification utilisé, accédez à https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

1. Dans un navigateur Web, accédez à https://console.cloud.google.com/project et ouvrez une session à l'aide de vos informations d'identification d'administrateur Google.

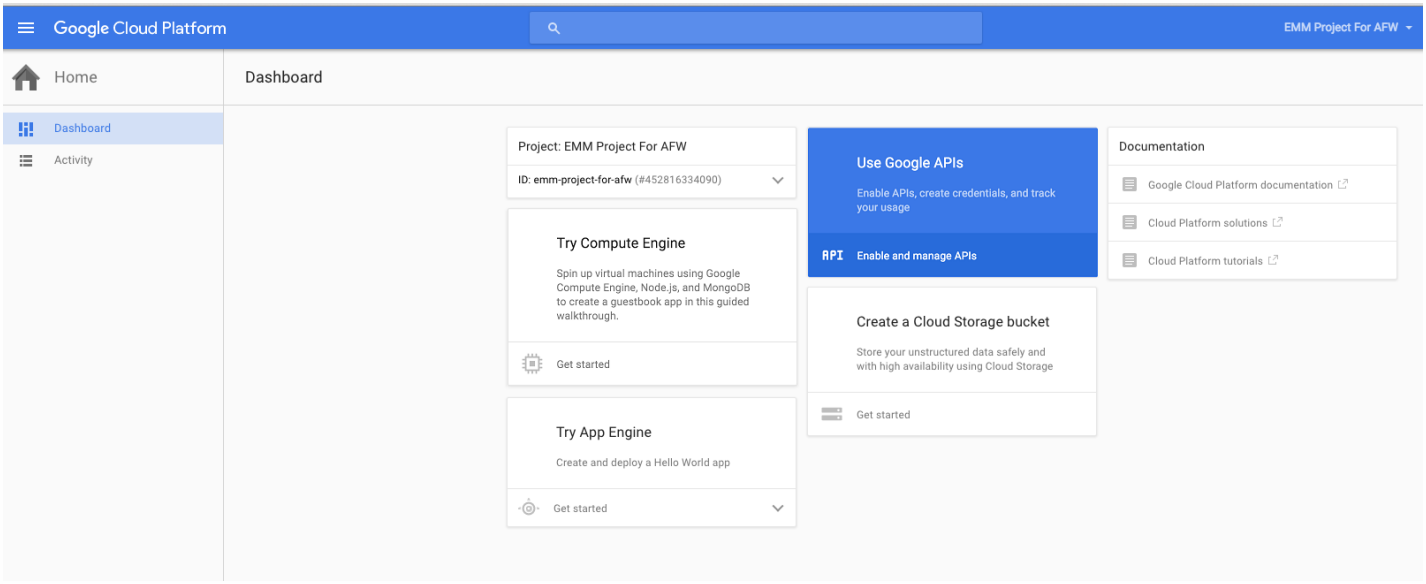
2. Dans la liste **Projets**, cliquez sur **Créer un projet.**



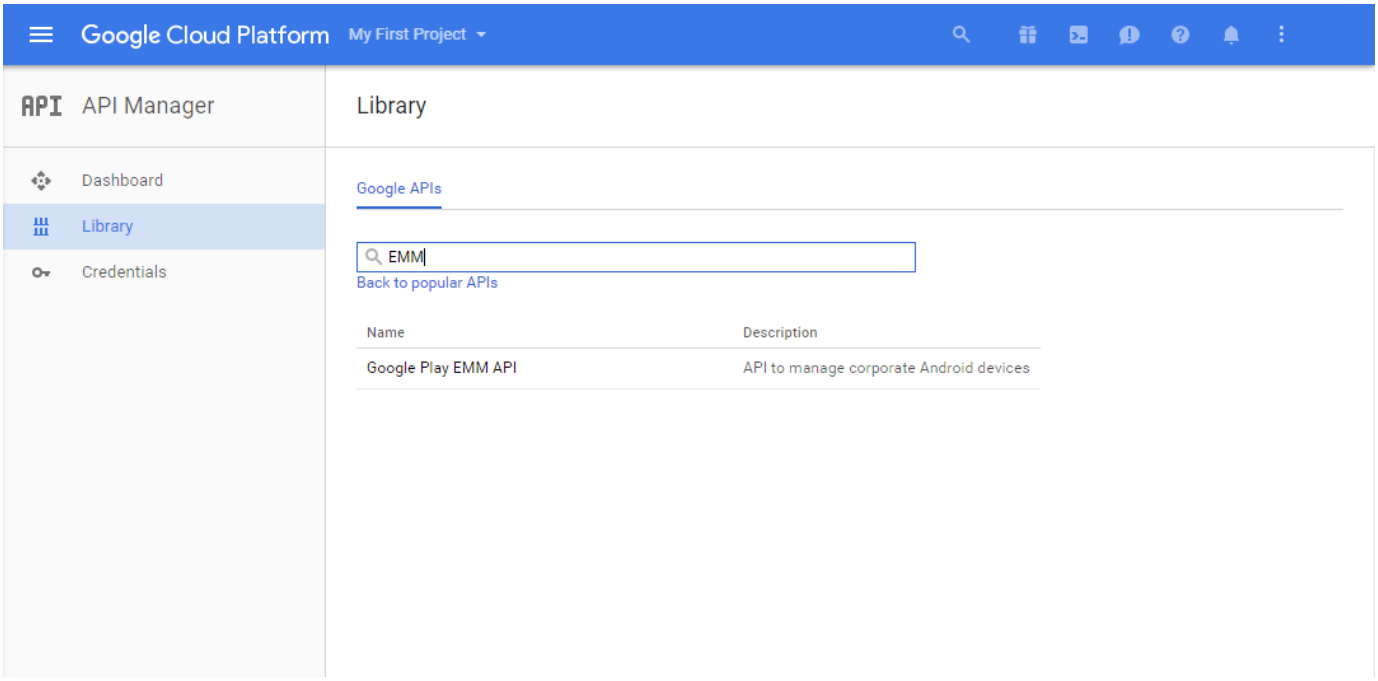
3. Dans **Nom du projet**, entrez un nom pour le projet.



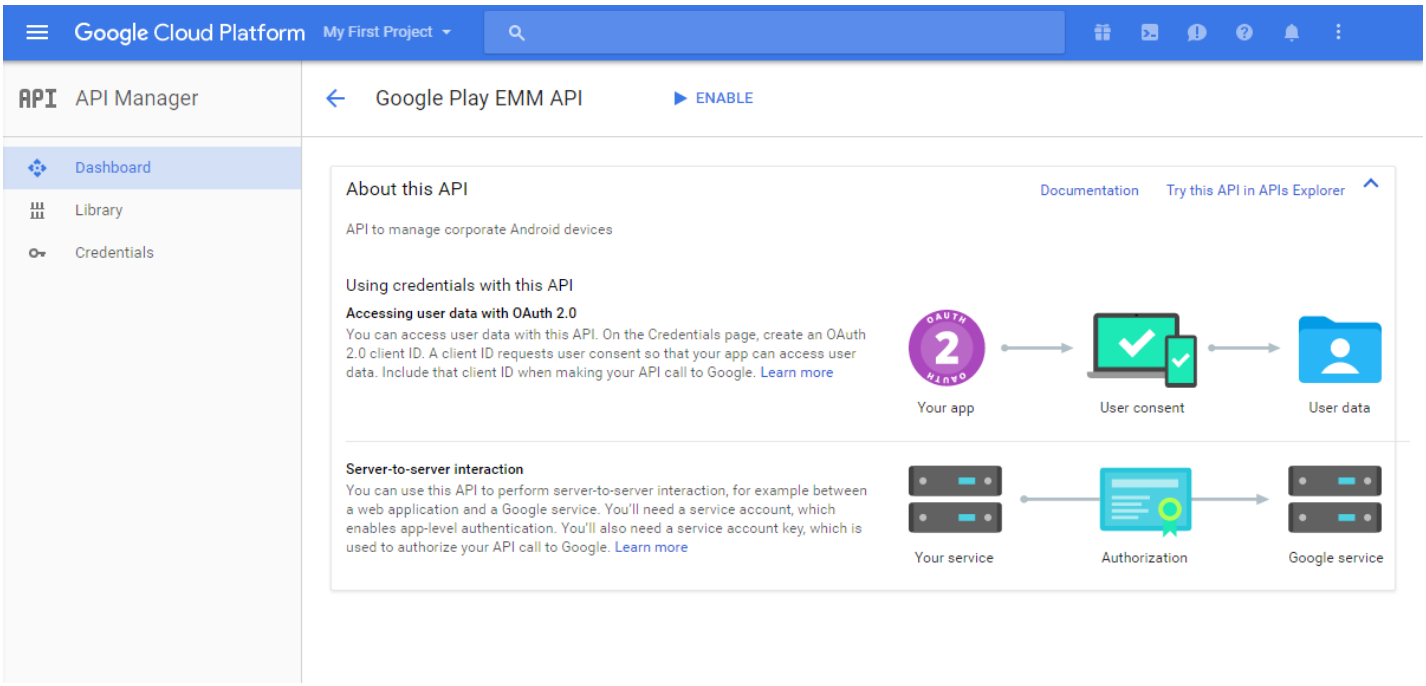
4. Sur le tableau de bord, cliquez sur **Utiliser les API de Google**.



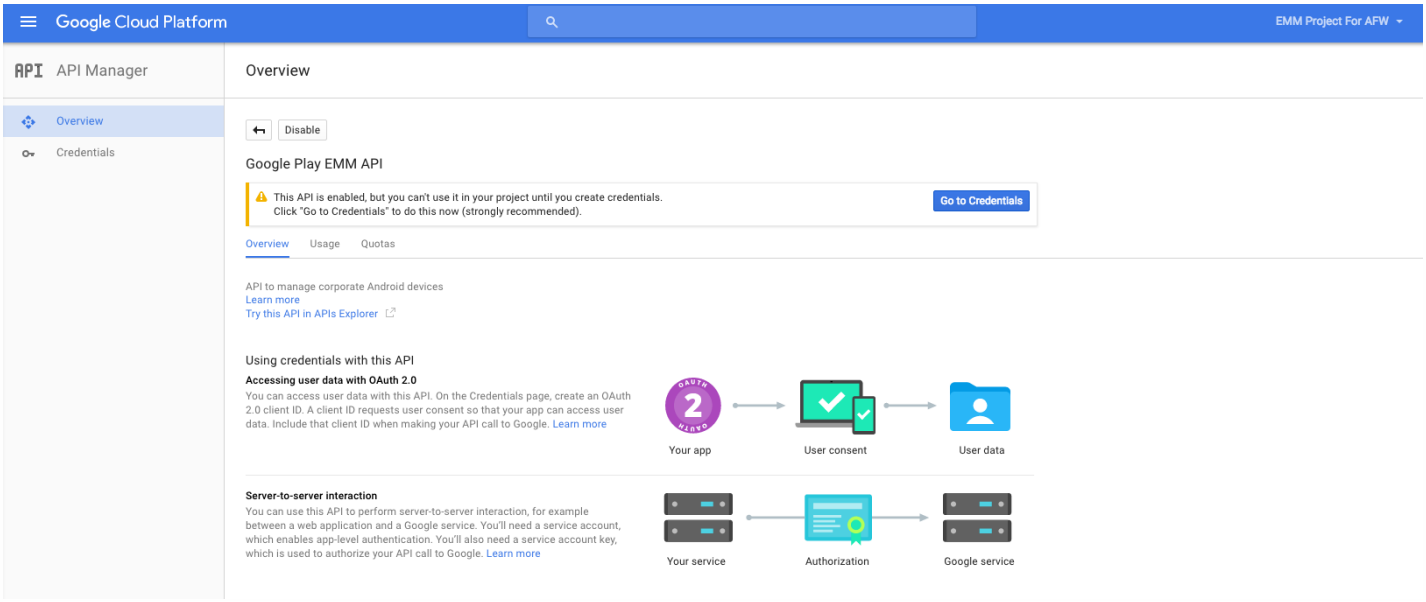
5. Cliquez sur **Bibliothèque** et dans **Rechercher**, entrez **EMM** , puis cliquez sur le résultat de la recherche.



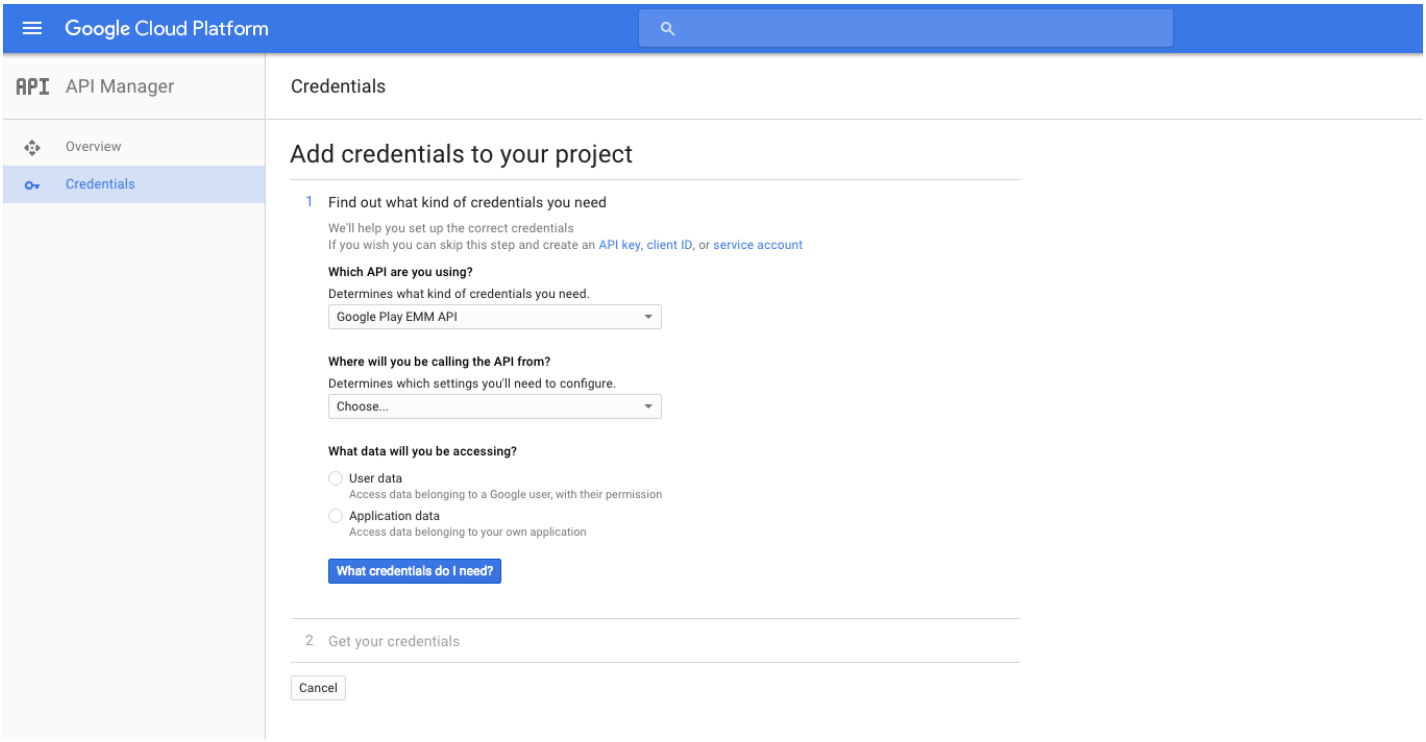
6. Sur la page de **présentation**, cliquez sur **Activer**.



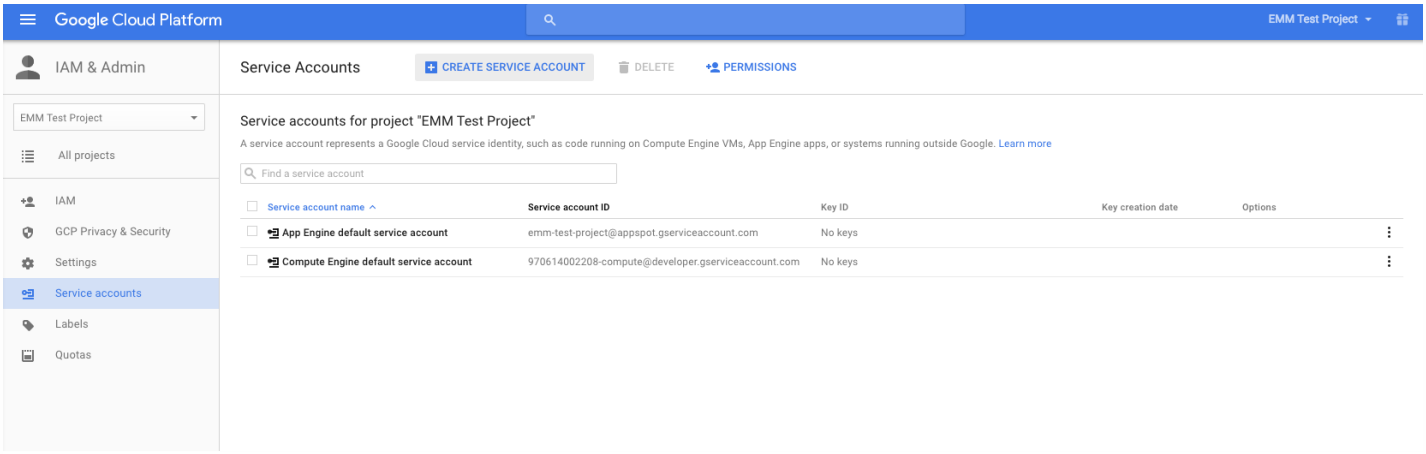
7. En regard de **Google Play EMM API**, cliquez sur **Accéder aux identifiants**.



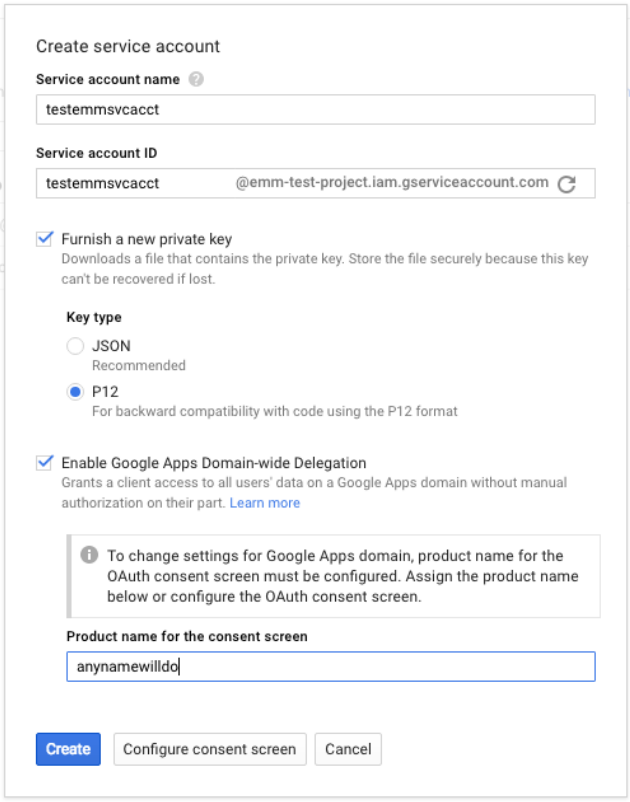
8. Dans la liste **Add credentials to our project**, dans l'étape 1, cliquez sur **service account**.



9. Sur la page **Comptes de service**, cliquez sur **Créer un compte de service**.

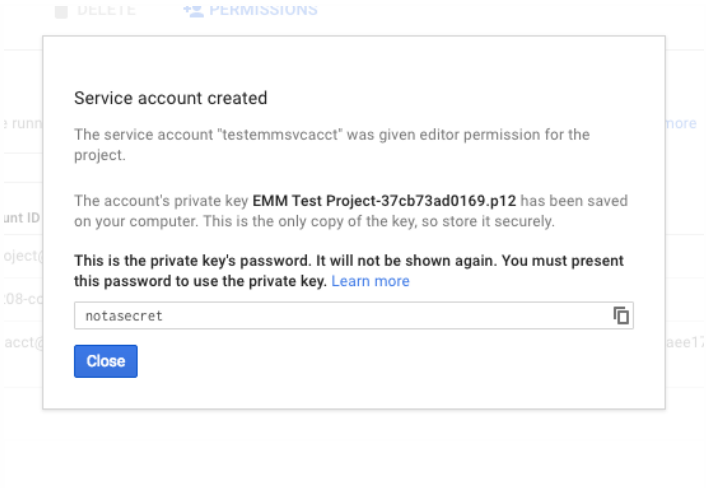


10. Dans **Créer un compte de service**, nommez le compte et sélectionnez la case **Indiquer une nouvelle clé privée**. Cliquez sur **P12**, sélectionnez la case à cocher **Activer la délégation G Suite au niveau du domaine**, puis cliquez sur **Créer.**

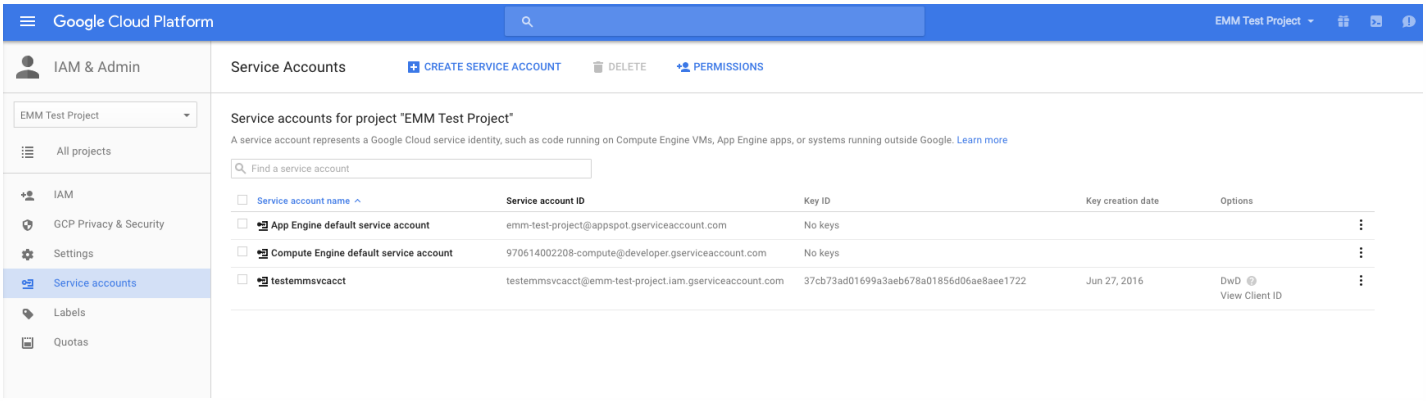


Le certificat (fichier P12) est téléchargé sur votre ordinateur. Veillez à enregistrer le certificat dans un emplacement sécurisé.

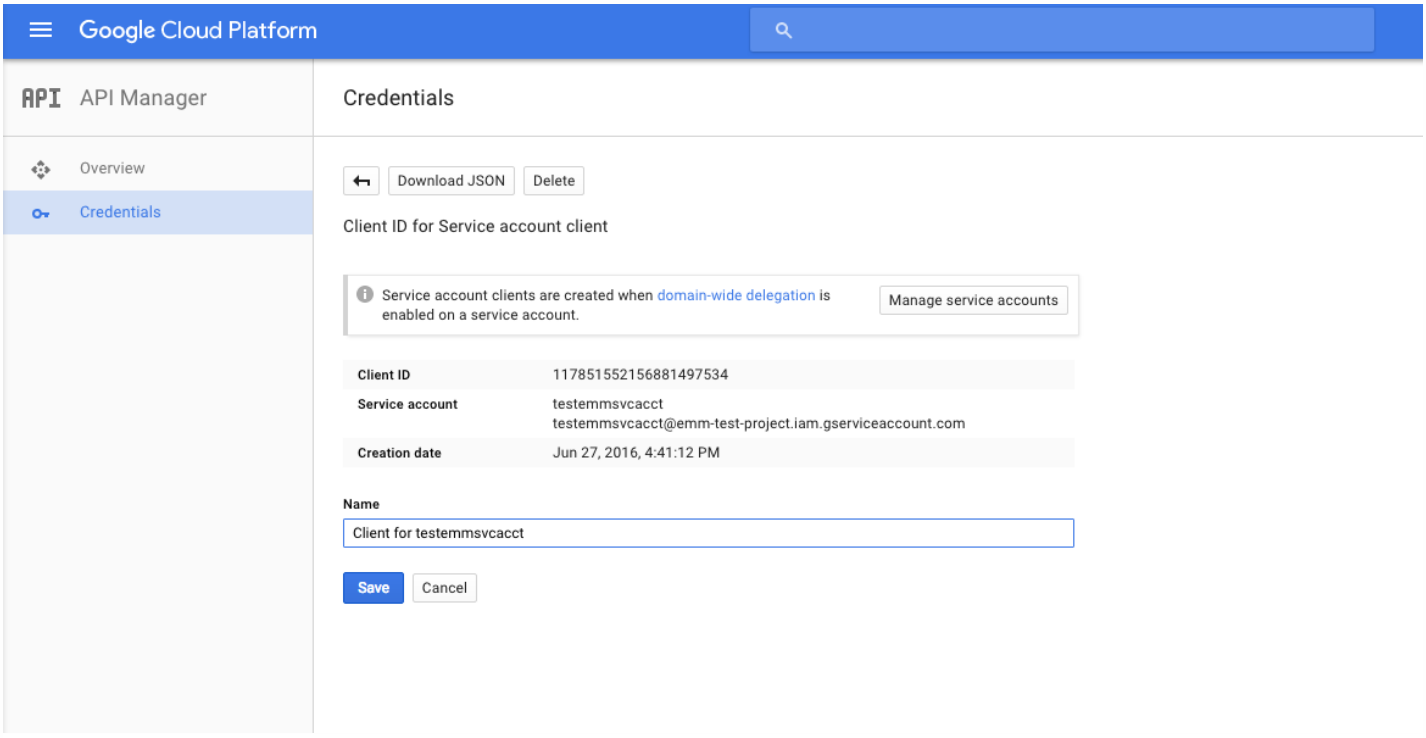
11. Sur l'écran **Compte de service créé**, cliquez sur **Fermer**.



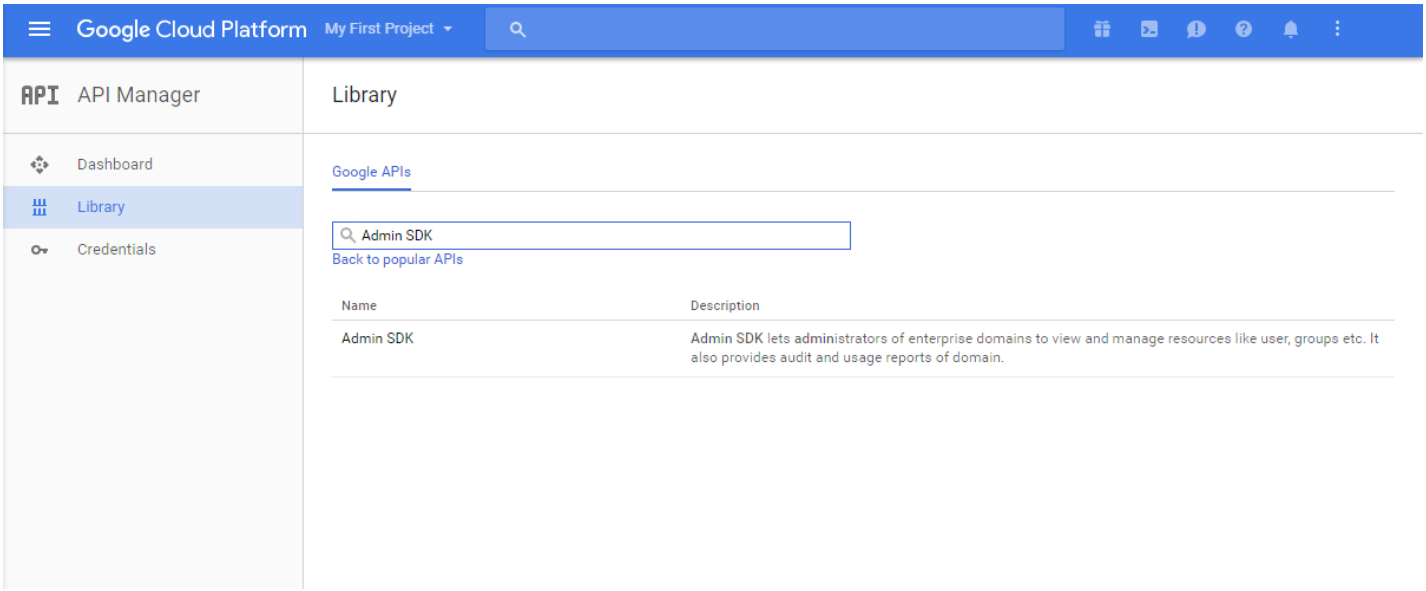
12. Dans **Autorisations**, cliquez sur **Comptes de service**, puis sous **Options** pour votre compte de service, cliquez sur **Afficher l'ID client**.



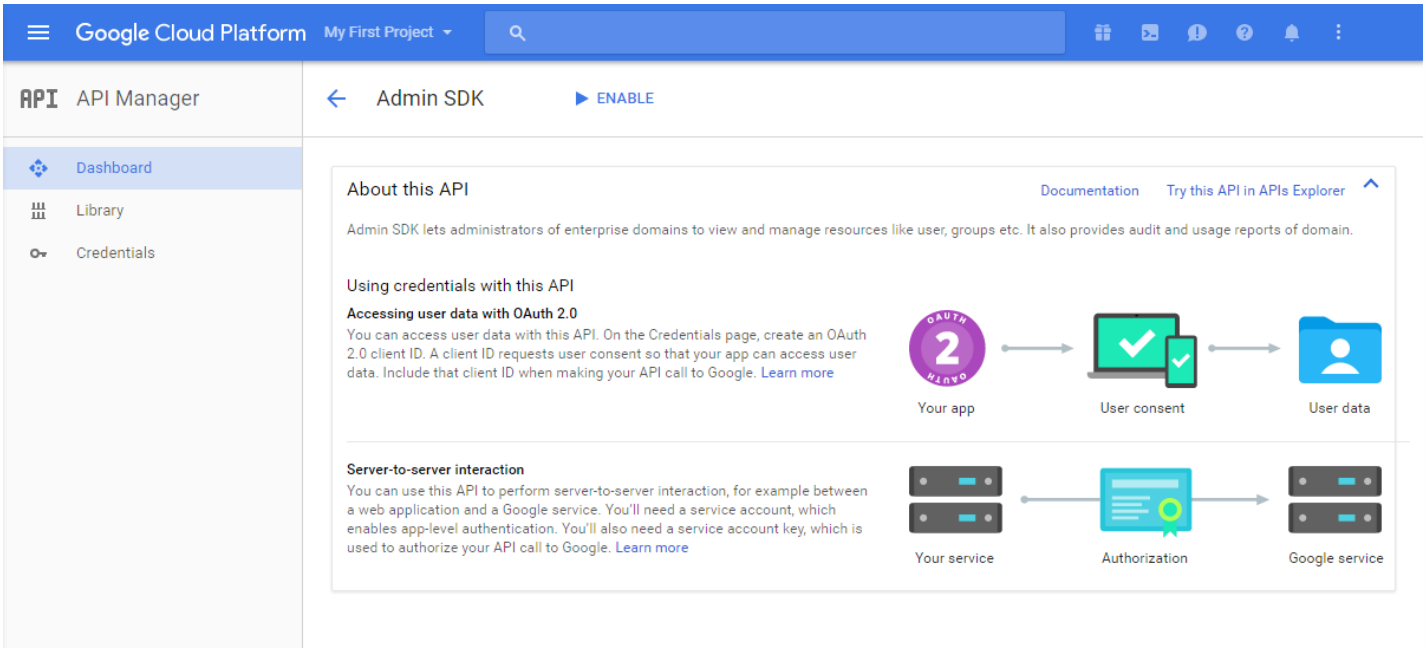
13. Les détails requis pour l'autorisation du compte sur la console d'administration Google s'affichent. Copiez les valeurs des champs **ID client** et **ID compte de service** sur un emplacement où vous pourrez les récupérer ultérieurement. Vous avez besoin de ces informations, ainsi que du nom de domaine afin de les envoyer à l'assistance Citrix afin qu'ils puissent les placer en liste blanche.



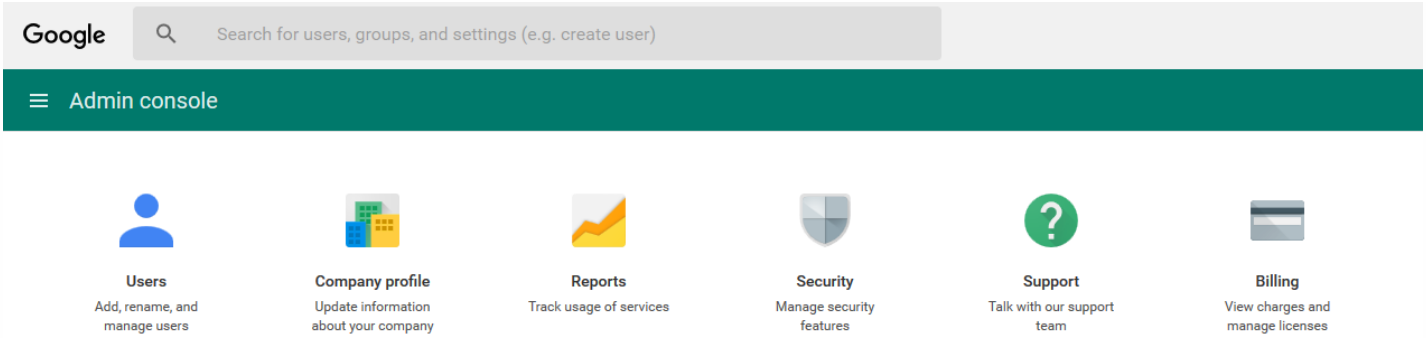
14. Sur la page **Bibliothèque**, recherchez **Admin SDK** et cliquez sur le résultat de la recherche.



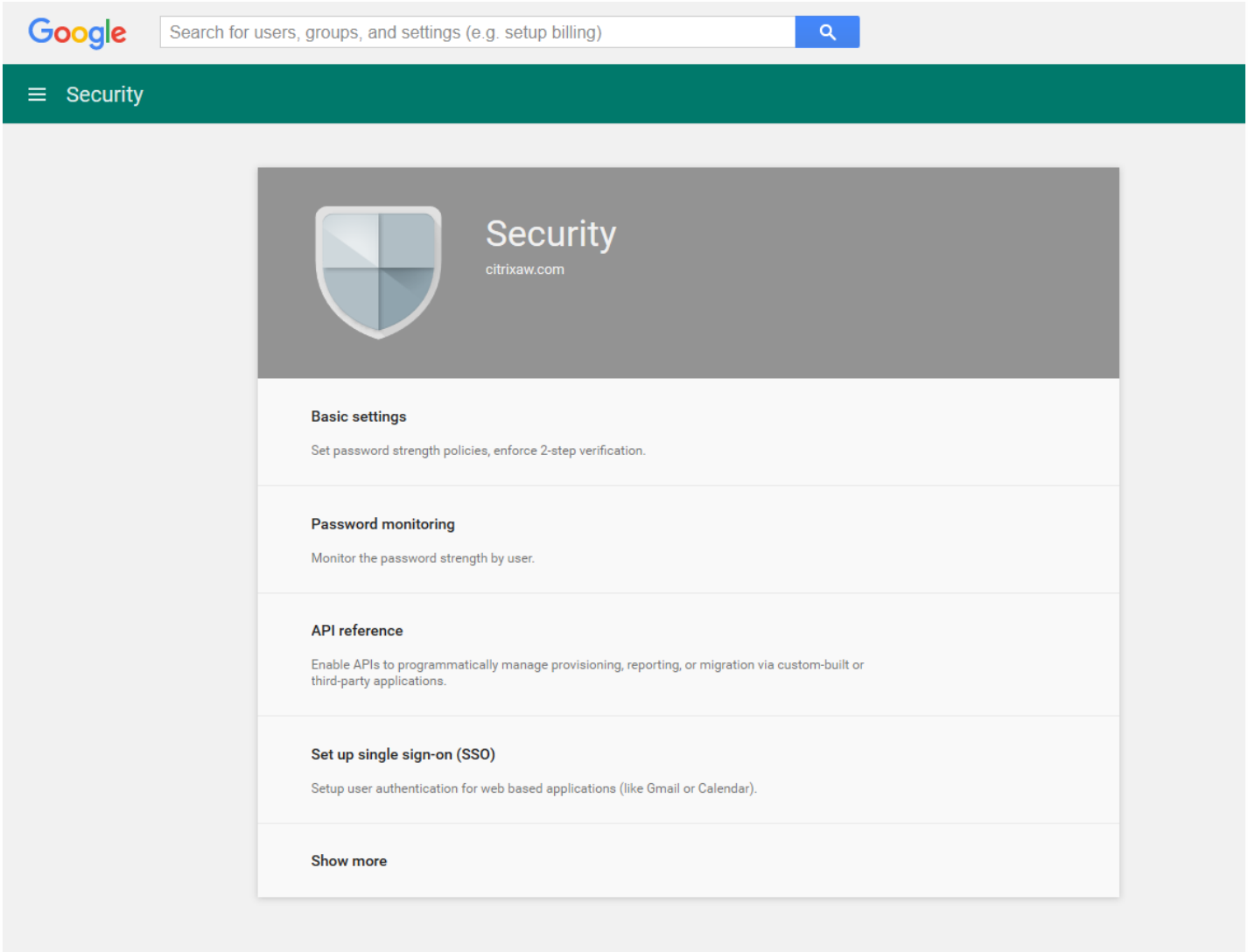
15. Sur la page de **présentation**, cliquez sur **Activer**.

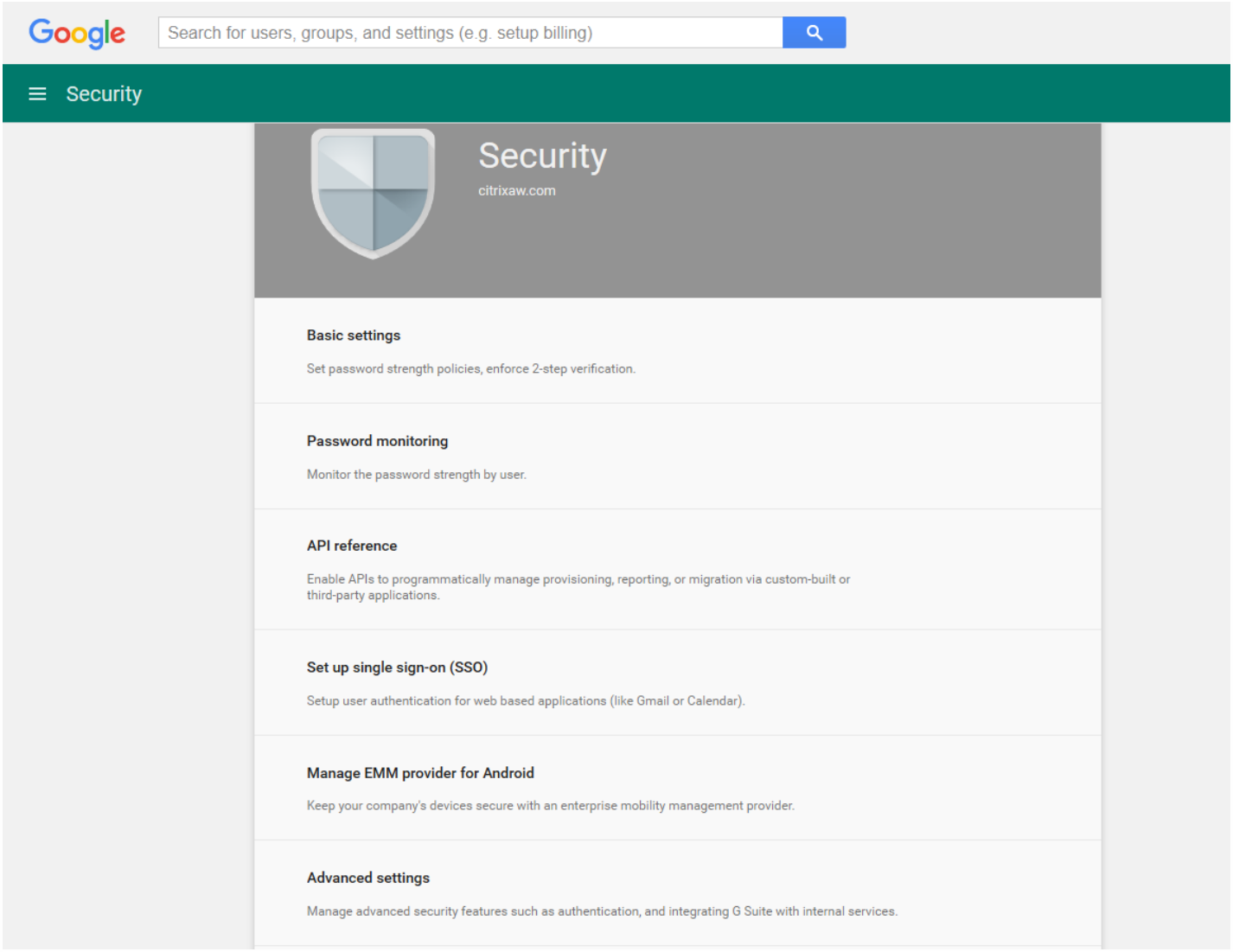


16. Ouvrez la console d'administration Google pour votre domaine et cliquez sur **Sécurité**.

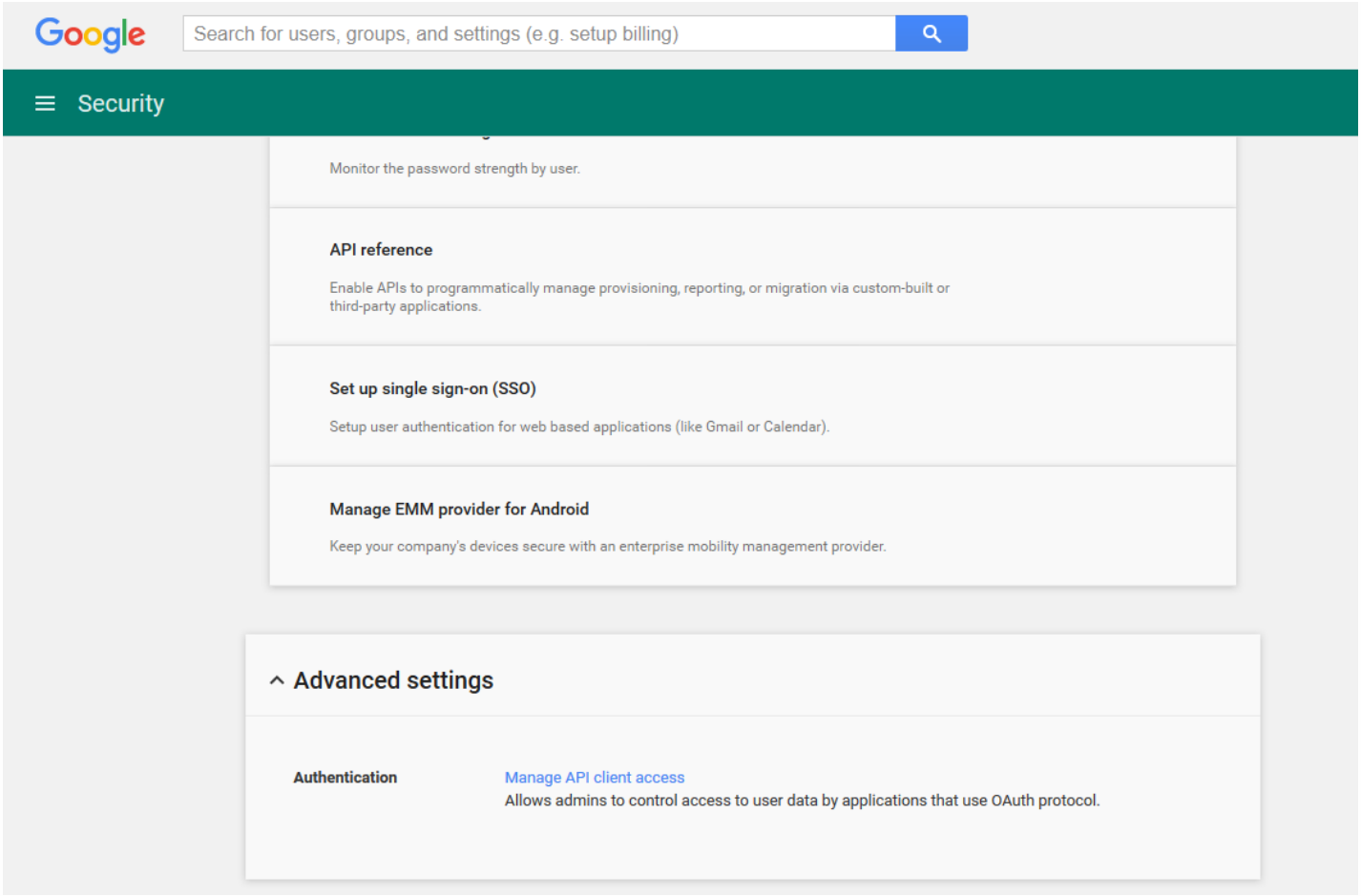


17. Sur la page **Paramètres**, cliquez sur **Afficher plus**, puis cliquez sur **Paramètres avancés**.

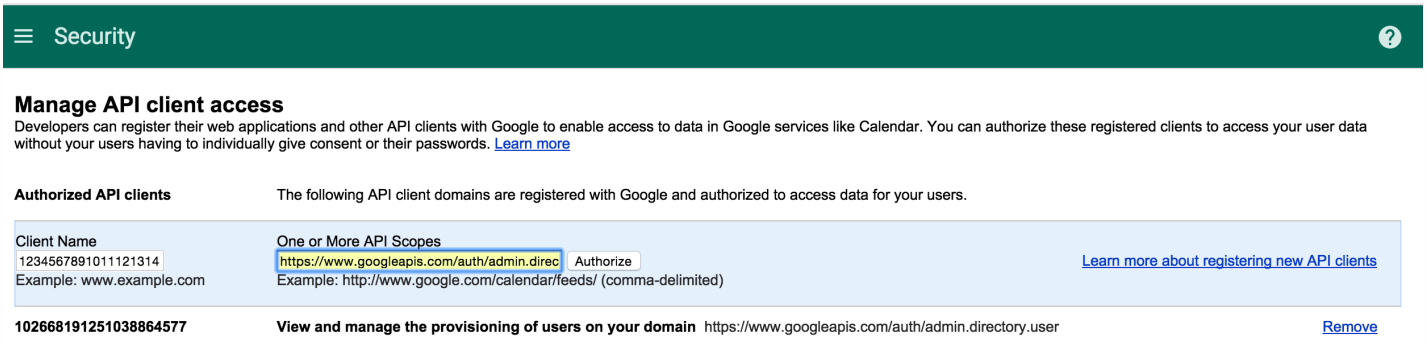




18. Cliquez sur **Gérer l'accès au client d'API**.



19. Dans **Nom du client**, entrez l'ID de client que vous avez enregistré précédemment, dans **Une ou plusieurs étendues d'API**, entrez https://www.googleapis.com/auth/admin.directory.user puis cliquez sur **Autoriser**.



Liaison à EMM

Avant de pouvoir utiliser XenMobile pour gérer vos appareils Android, vous devez contacter l'assistance technique de Citrix et fournir votre nom de domaine, compte de service et jeton de liaison. Citrix lie le jeton à XenMobile en tant que fournisseur de gestion de la mobilité d'entreprise (EMM). Pour consulter les informations de contact de l'assistance technique Citrix, consultez la section Assistance technique Citrix.

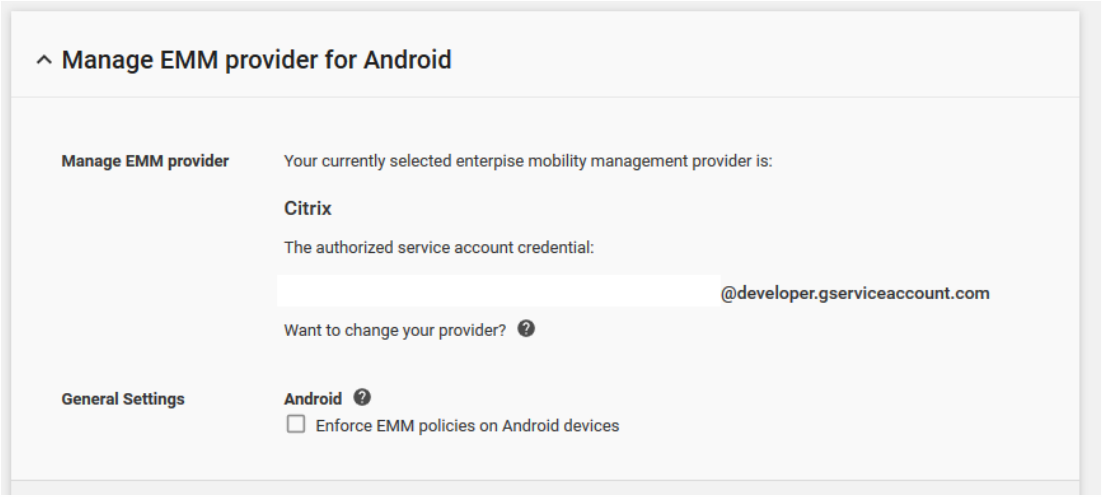
1. Pour confirmer la liaison, ouvrez une session sur le portail de la console d'administration Google et cliquez sur **Sécurité**.

2. Cliquez sur **Gérer le fournisseur EMM pour Android**.

Votre compte Google Android for Work est maintenant lié à Citrix en tant que fournisseur EMM.

Après avoir confirmé la liaison du jeton, vous pouvez commencer à utiliser la console XenMobile pour gérer vos appareils Android. Importez le certificat P12 que vous avez généré à l'étape 14. Configurez les paramètres du serveur Android at Work, activez l'authentification unique SAML et définissez au moins une

stratégie d'appareil Android at Work.

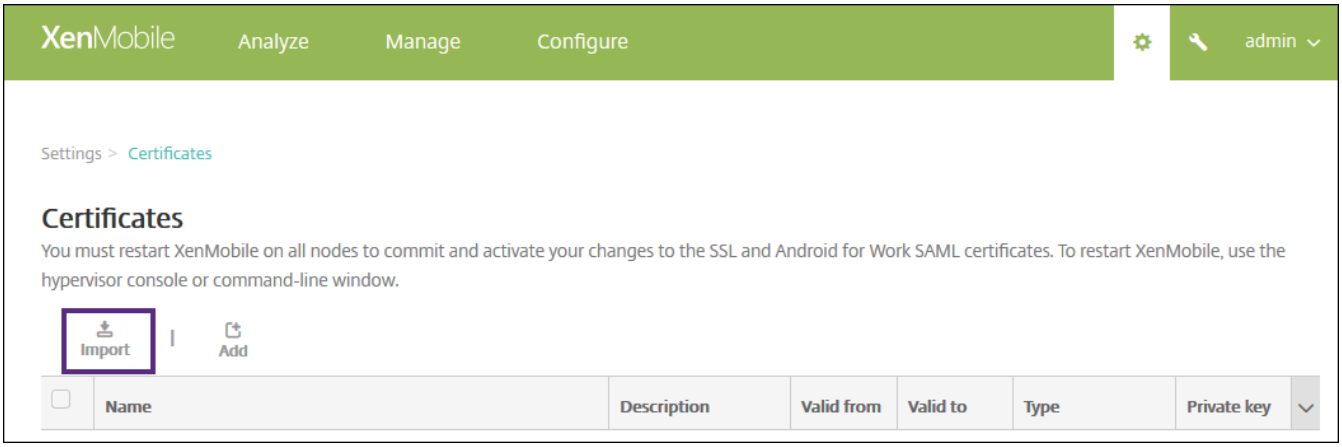


Importer le certificat P12

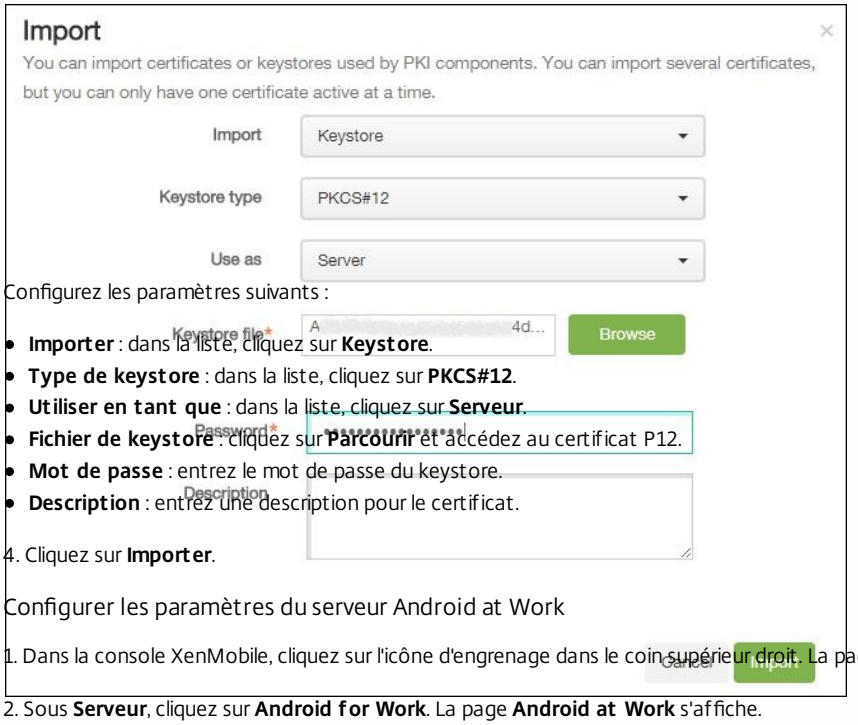
Suivez ces étapes pour importer votre certificat P12 Android at Work :

1. Connectez-vous à la console XenMobile.

2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**, puis cliquez sur **Certificats**. La page **Certificats** s'affiche.



3. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît.



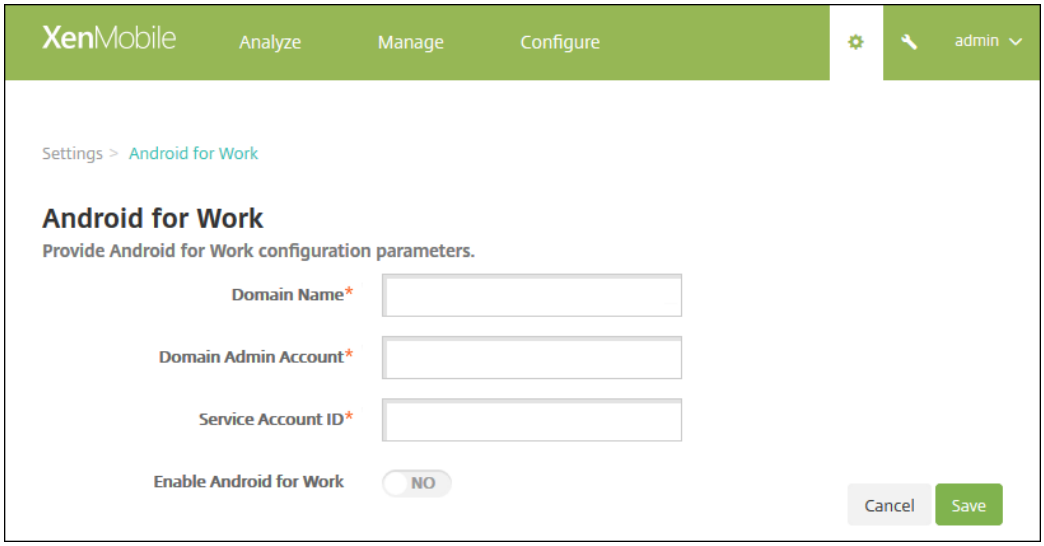
Configurez les paramètres suivants :

- **Importer** : dans la liste, cliquez sur **Keystore**.
- **Type de keystore** : dans la liste, cliquez sur **PKCS#12**.
- **Utiliser en tant que** : dans la liste, cliquez sur **Serveur**.
- **Fichier de keystore** : cliquez sur **Parcourir** et accédez au certificat P12.
- **Mot de passe** : entrez le mot de passe du keystore.
- **Description** : entrez une description pour le certificat.

4. Cliquez sur **Importer**.

Configurer les paramètres du serveur Android at Work

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.
2. Sous **Serveur**, cliquez sur **Android for Work**. La page **Android at Work** s'affiche.



Configurez les paramètres suivants :

- **Nom de domaine** : entrez votre nom de domaine Android at Work ; par exemple, domaine.com.
- **Compte d'administrateur de domaine** : entrez le nom d'utilisateur de l'administrateur de domaine ; par exemple, le compte de messagerie utilisé pour le portail Google Developer.
- **ID du compte de service** : entrez votre ID de compte de service, par exemple, l'adresse e-mail associée au compte de service Google (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com).
- **Activer Android at Work** : cliquez pour activer ou désactiver Android at Work.

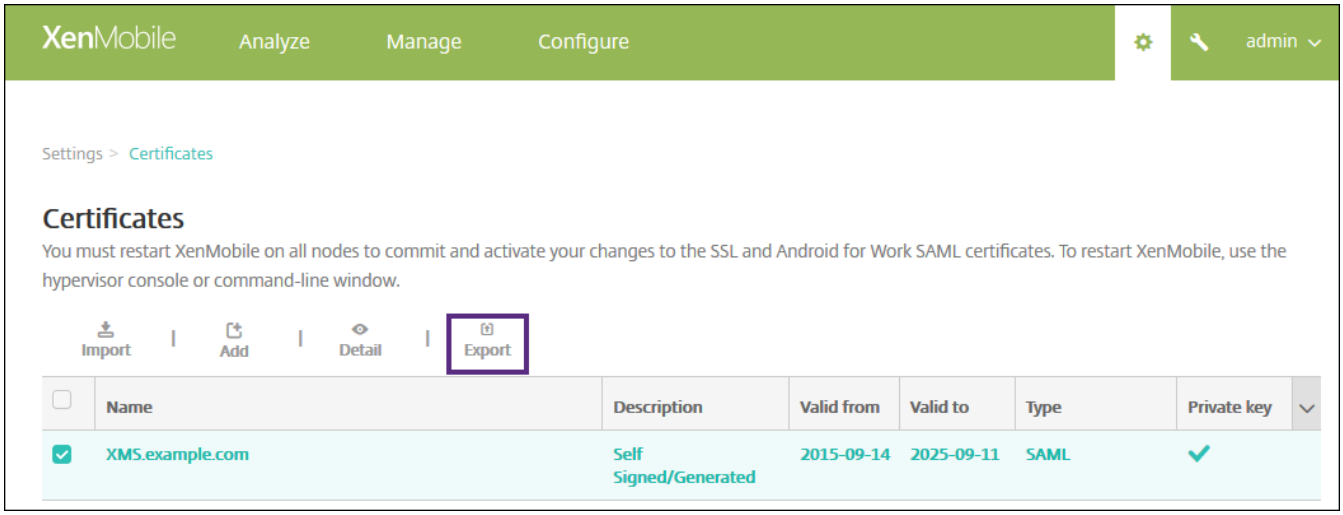
3. Cliquez sur **Enregistrer**.

Activer l'authentification unique SAML

1. Connectez-vous à la console XenMobile.

2. Cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console. La page **Paramètres** s'ouvre.

3. Cliquez sur **Certificats**. La page **Certificats** s'affiche.

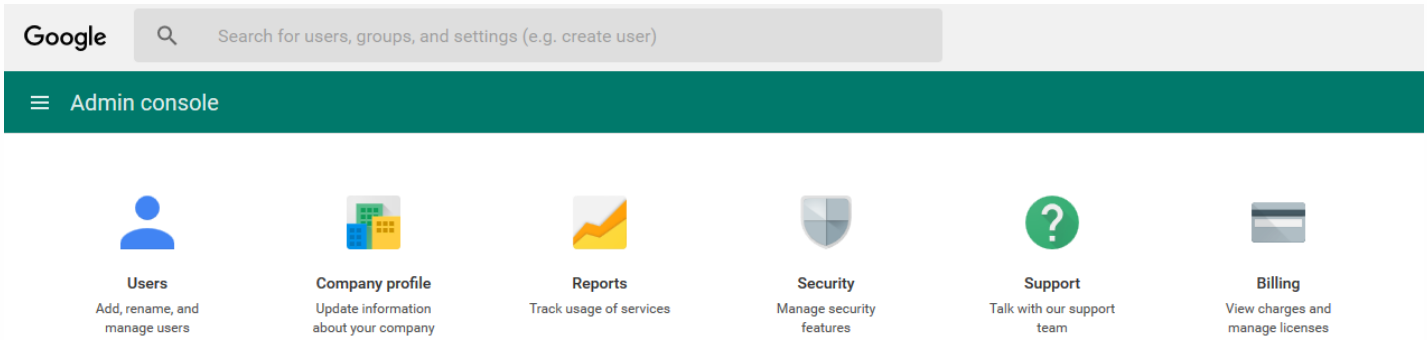


3. Dans la liste des certificats, cliquez sur le certificat SAML.

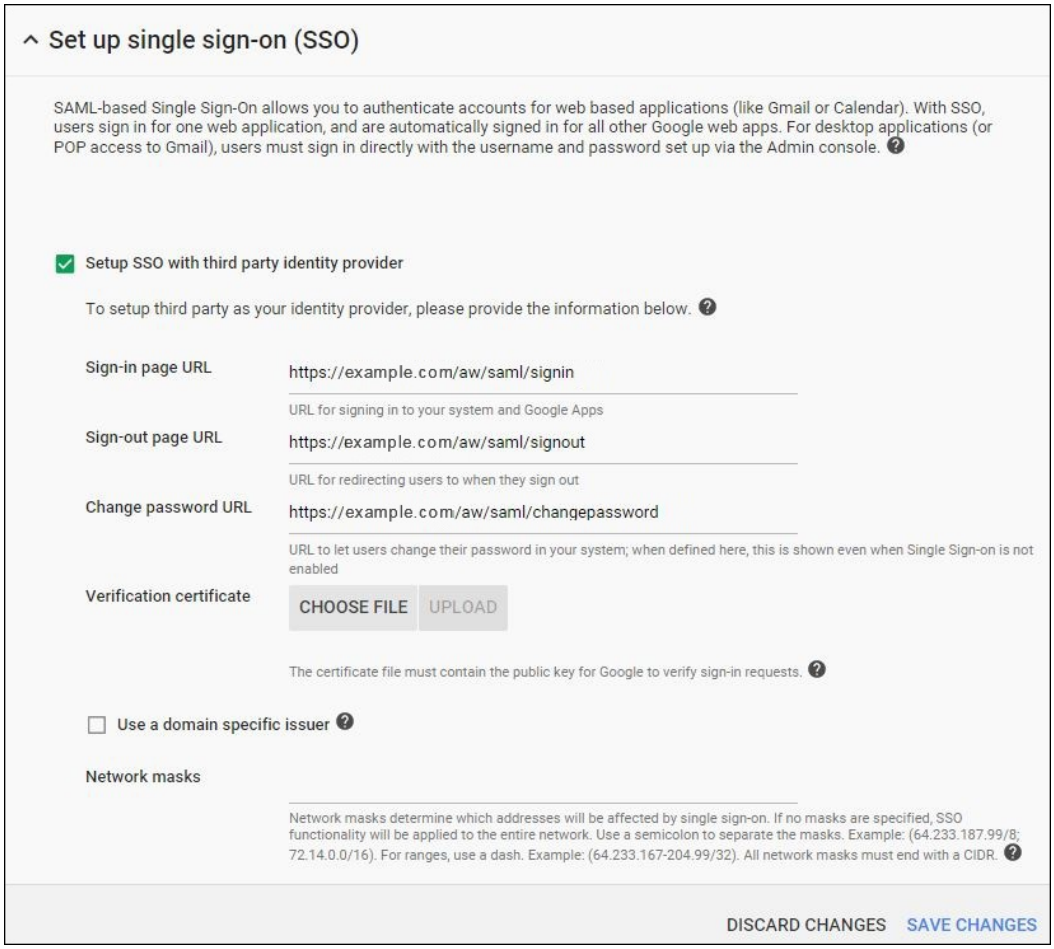
4. Cliquez sur **Exporter** et enregistrez le certificat sur votre ordinateur.

5. Connectez-vous au portail de la console d'administration Google à l'aide de vos informations d'identification d'administrateur Android at Work. Pour accéder au portail, veuillez consulter la section Console d'administration Google.

6. Cliquez sur **Sécurité**.



7. Dans **Sécurité**, cliquez sur **Configurer l'authentification unique (SSO)** et configurez les paramètres suivants :

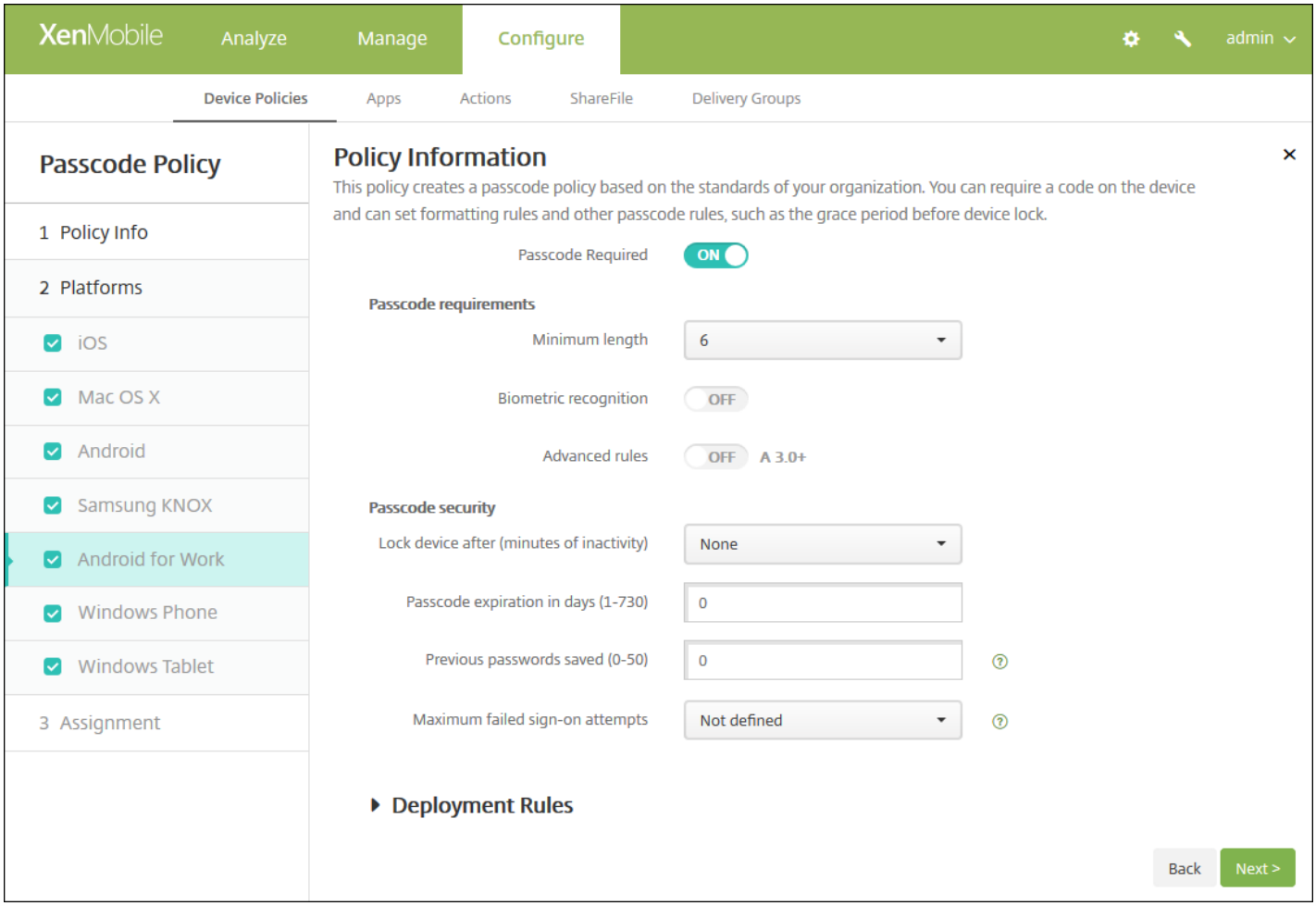


- **URL de la page de connexion** : entrez l'adresse URL pour les utilisateurs qui se connectent à votre système et Google Apps. Par exemple : https:///aw/saml/signin.
- **URL de la page de déconnexion** : entrez l'adresse URL vers laquelle les utilisateurs sont redirigés lorsqu'ils se déconnectent. Par exemple : https:///aw/saml/signout.
- **URL de la page de modification du mot de passe** : entrez l'adresse URL pour permettre aux utilisateurs de modifier leur mot de passe dans votre système. Par exemple : https:///aw/saml/changepassword. Si ce champ est défini, cette invite s'affiche même lorsque l'authentification unique (SSO) n'est pas disponible.
- **Certificat de vérification** : cliquez sur **CHOISIR FICHIER** et accédez à l'emplacement du certificat SAML exporté depuis XenMobile.

8. Cliquez sur **ENREGISTRER LES MODIFICATIONS**.

Configurer une stratégie d'appareil Android at Work

Il est recommandé de configurer une stratégie de code secret afin d'obliger les utilisateurs à créer un code secret sur leurs appareils la première fois qu'ils s'inscrivent.



Les étapes de base pour configurer une stratégie sont les suivantes.

1. Connectez-vous à la console XenMobile.

2. Cliquez sur **Configurer** et sur **Stratégies d'appareil**.

3. Cliquez sur **Ajouter**, puis sélectionnez la stratégie que vous souhaitez ajouter à partir de la boîte de dialogue **Ajouter une nouvelle stratégie**. Dans cet exemple, vous cliquez sur **Code secret**.

4. Remplissez la page **Informations sur la stratégie**.

5. Cliquez sur **Android for Work** et configurez les paramètres pour la stratégie.

6. Attribuez la stratégie à un groupe de mise à disposition.

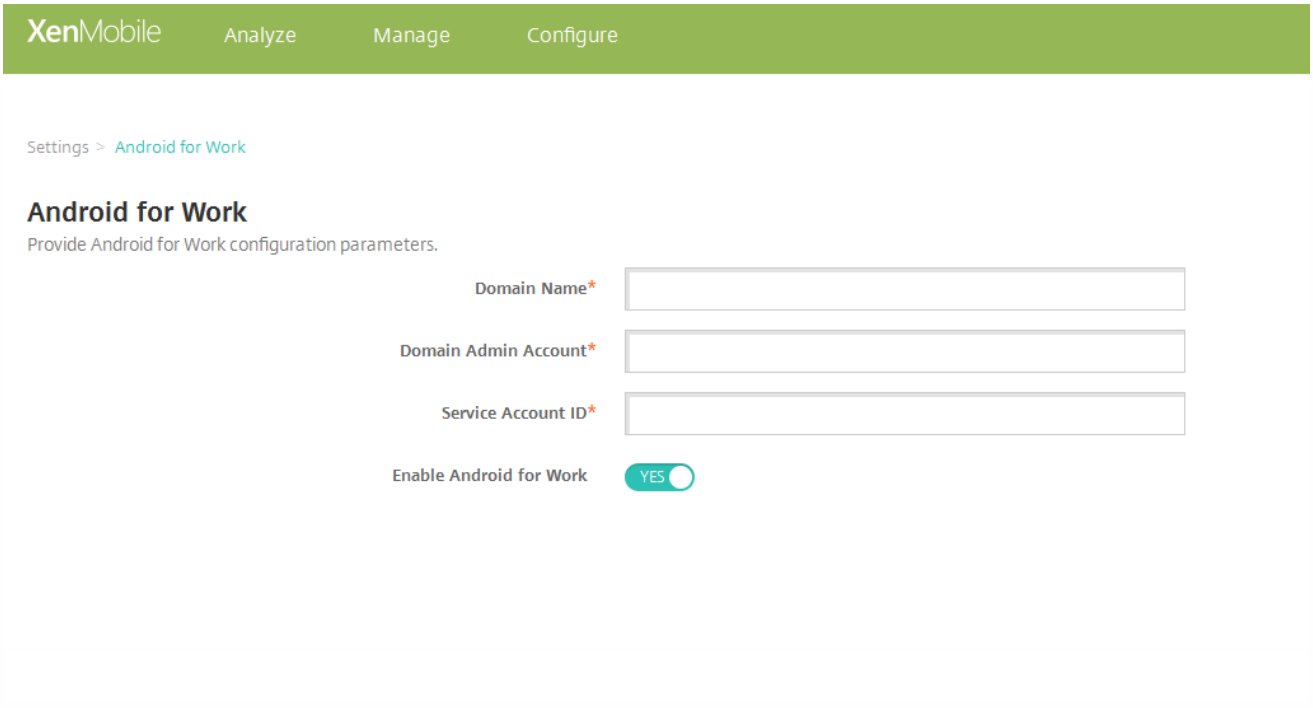
Pour de plus amples informations sur la configuration d'autres stratégies disponibles pour Android for Work, consultez la section Stratégies XenMobile par plate-forme.

Configurer les paramètres de compte Android at Work

Avant de démarrer la gestion des applications et des stratégies Android sur les appareils, vous devez définir les informations de domaine et de compte Android at Work dans XenMobile. Commencez par effectuer les tâches de configuration Android at Work sur Google pour configurer un administrateur de domaine et obtenir un ID de compte de service et un jeton de liaison.

1. Dans la console Web de XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'ouvre.

2. Sous **Serveur**, cliquez sur **Android for Work**. La page de configuration **Android for Work** s'affiche.



3. Sur la page **Android for Work**, configurez les paramètres suivants :

- **Nom de domaine** : entrez le nom du domaine.
- **Compte d'administrateur de domaine** : entrez le nom d'utilisateur de l'administrateur de domaine.
- **ID du compte de service** : entrez votre ID du compte de service Google.
- **Activer Android for Work** : sélectionnez cette option pour activer Android for Work.

4. Cliquez sur **Enregistrer**.

Provisioning du mode Device Owner dans Android at Work

Si vous souhaitez provisionner Android at Work en mode Device Owner, vous devez transférer les données via NFC en cognant deux appareils. L'un doit exécuter l'application XenMobile Provisioning Tool et les paramètres d'usine doivent avoir été réinitialisés sur l'autre. Le mode Device Owner est uniquement disponible pour les appareils appartenant à l'entreprise.

Pourquoi utiliser le NFC ? Bluetooth, Wi-Fi et les autres modes de communication sont désactivés sur un appareil dont les paramètres d'usine ont été réinitialisés. NFC est le seul protocole de communication que l'appareil peut utiliser dans cet état.

Conditions préalables

- Version 10.4 du serveur XenMobile activée pour Android at Work.
- Un appareil dont les paramètres d'usine ont été réinitialisés, provisionné pour Android at Work en mode Device Owner. Les étapes à suivre pour satisfaire ces conditions préalables sont disponibles plus loin dans cet article.
- Un autre appareil avec capacité NFC, exécutant l'application Provisioning Tool configurée. Provisioning Tool est disponible dans Secure Hub 10.4 où sur la page des téléchargements de Citrix.

Chaque appareil ne peut disposer que d'un profil Android at Work, géré par une application de gestion de la mobilité d'entreprise (EMM). Un seul profil est autorisé sur chaque appareil. Si vous essayez d'ajouter une deuxième application EMM, la première application EMM sera supprimée.

Vous pouvez démarrer le mode Device Owner sur des nouveaux appareils ou sur des appareils dont les paramètres d'usine ont été réinitialisés. La gestion de l'appareil est effectuée entièrement sur XenMobile.

Partage de données à l'aide du NFC en mode Device Owner mode

Le provisioning d'un appareil dont les paramètres d'usine ont été réinitialisés requiert que vous envoyiez les données suivantes via NFC pour initialiser Android at Work :

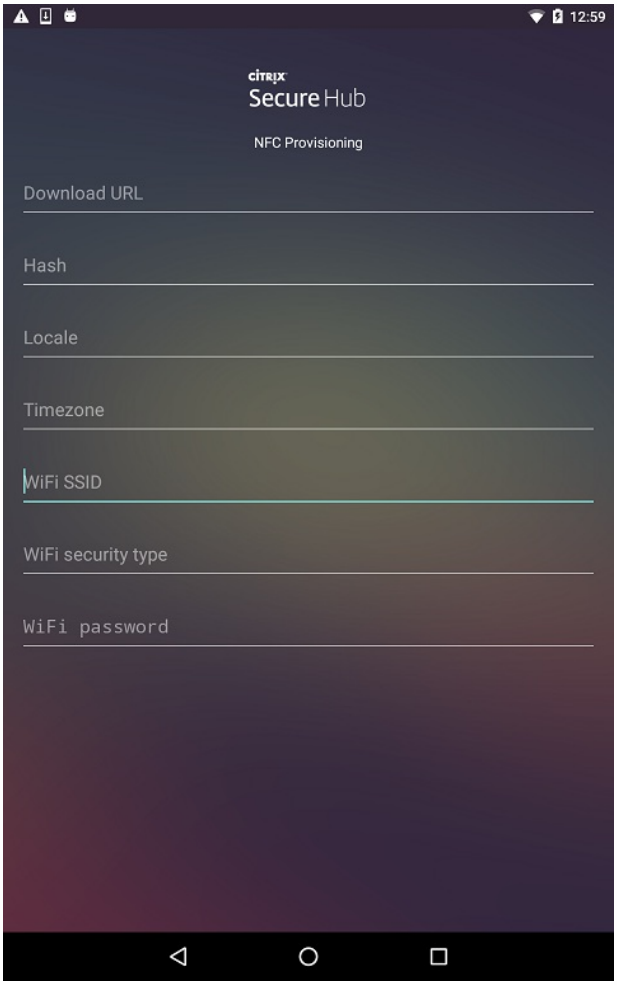
- Nom du package de l'application EMM du fournisseur qui fait office de propriétaire de l'appareil (dans ce cas, Secure Hub).
- Emplacement intranet/Internet à partir duquel l'appareil peut télécharger l'application EMM du fournisseur.

- Hachage SHA1 de l'application EMM du fournisseur pour vérifier que le téléchargement a réussi.
- Détails de la connexion Wi-Fi de façon à ce qu'un appareil dont les paramètres d'usine ont été réinitialisés puisse se connecter et télécharger l'application EMM du fournisseur. Remarque : Android ne prend pas charge 802.1x Wi-Fi pour cette étape.
- Fuseau horaire de l'appareil (facultatif).
- Emplacement géographique de l'appareil (facultatif).

Lorsque les deux appareils sont « cognés », les données de Provisioning Tool sont envoyées à l'appareil dont les paramètres d'usine ont été réinitialisés. Ces données sont ensuite utilisées pour télécharger Secure Hub avec des paramètres d'administrateur. Si vous ne précisez pas le fuseau horaire ni l'emplacement, Android les configure automatiquement sur le nouvel appareil.

Configuration de XenMobile Provisioning Tool

Avant de partager des données avec NFC, vous devez configurer Provisioning Tool. Cette configuration est ensuite transférée à l'appareil dont les paramètres d'usine ont été réinitialisés durant le partage des données avec NFC.



Vous pouvez entrer des données dans les champs requis ou les renseigner via un fichier texte. Les étapes de la procédure suivante décrivent comment configurer le fichier texte et contiennent des descriptions pour chaque champ. L'application n'enregistre pas les informations après qu'elles soient entrées, il

peut donc s'avérer utile de créer un fichier texte afin de conserver les informations pour une utilisation ultérieure.

Pour configurer le Provisioning Tool à l'aide d'un fichier texte

Appelez le fichier nfcprovisioning.txt et placez-le dans le dossier /sdcard/ sur la carte SD de l'appareil. Cela permet à l'application de lire le fichier texte et renseigner les valeurs.

Le fichier texte doit contenir les données suivantes :

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=
Il s'agit de l'emplacement intranet/Internet de l'application EMM du fournisseurr. Après que l'appareil dont les paramètres d'usine ont été réinitialisés se soit connecté au Wi-Fi suite au partage NFC, il doit avoir accès à cet emplacement pour le téléchargement. L'adresse URL est une adresse URL standard qui ne requiert aucun formatage spécial.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=
Il s'agit de la somme de contrôle de l'application EMM du fournisseur. Elle est utilisée pour vérifier que le téléchargement a réussi. Les étapes à suivre pour obtenir la somme de contrôle sont abordées plus loin dans cet article.

android.app.extra.PROVISIONING_WIFI_SSID=
Il s'agit du SSID Wi-Fi connecté de l'appareil sur lequel Provisioning Tool est exécuté.

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=
Les valeurs prises en charge sont WEP et WPA2. Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

android.app.extra.PROVISIONING_WIFI_PASSWORD=
Si le Wi-Fi n'est pas protégé, ce champ doit être vide.

android.app.extra.PROVISIONING_LOCALE=
Entrez un code de langue et de pays. Les codes de langue sont des codes ISO de deux lettres minuscules (tels que fr) comme défini dans l'ISO 639-1. Les codes de pays sont des codes ISO de deux lettres majuscules (tels que FR) comme défini dans l'ISO 3166-1. À titre d'exemple, entrez fr_FR pour la langue française parlée en France. Si vous n'entrez aucun code, la langue et le pays sont automatiquement renseignés.

android.app.extra.PROVISIONING_TIME_ZONE=
Fuseau horaire dans lequel l'appareil est exécuté. Entrez un nom basé sur la base de données Olson au format zone/emplacement. Par exemple, Europe/Paris pour l'heure de l'Europe occidentale. Si vous n'entrez rien, le fuseau horaire est automatiquement renseigné.

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=
Ce nom n'est pas requis car la valeur est codée en dur dans l'application Secure Hub. Il n'est mentionné ici que par souci de complétude.

Si un accès protégé Wi-Fi WPA2 est utilisé, un fichier **nfcprovisioning.txt** peut ressembler à ce qui suit :

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

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name

android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2

android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere

android.app.extra.PROVISIONING_LOCALE=en_US

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

Si un accès non protégé Wi-Fi est utilisé, un fichier nfcprovisioning.txt peut ressembler à ce qui suit :

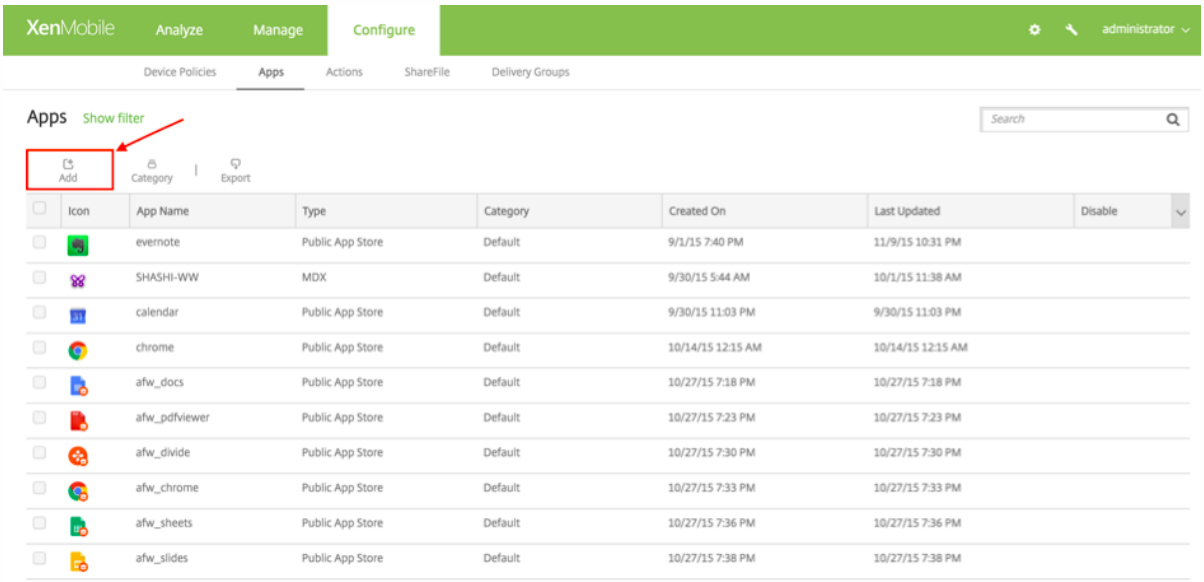
```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=http://www.somepublicurlhere.com/path/to/securehub.apk

android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4CrbAk\u003d

android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name

android.app.extra.PROVISIONING_LOCALE=en_US

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

Pour obtenir la somme de contrôle de Secure Hub

Pour obtenir la somme de contrôle d'une application, ajoutez l'application en tant qu'application d'entreprise.

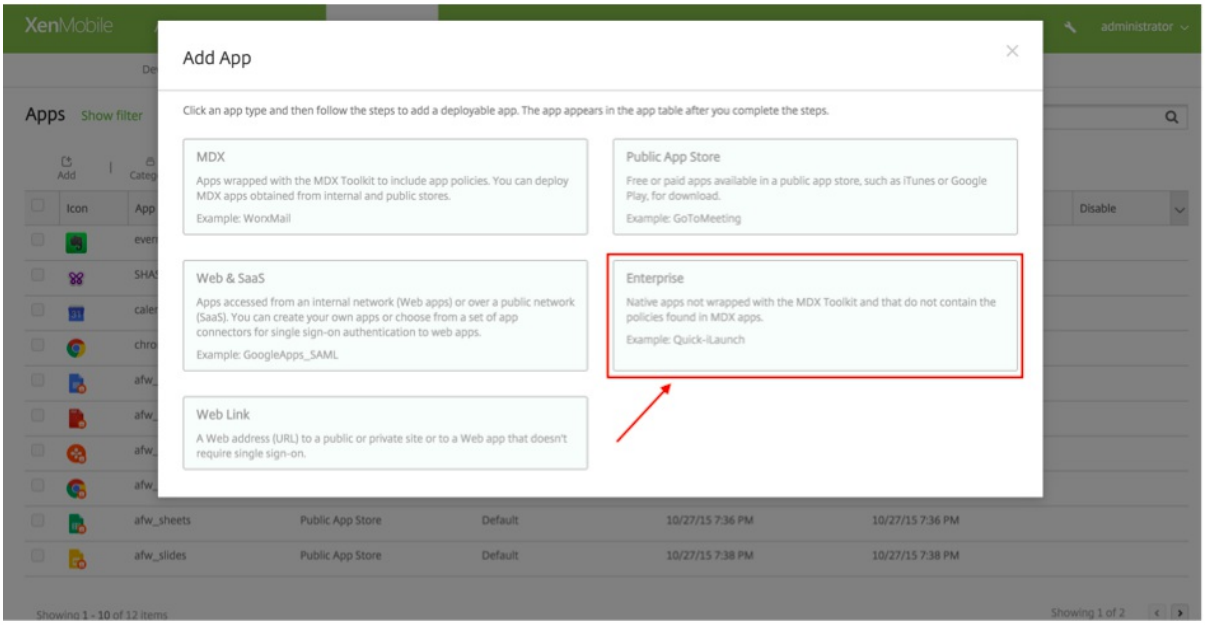
1. Dans la console XenMobile, Accédez à **Configurer > Applications > Ajouter**.

La fenêtre **Ajouter une application** s'affiche.



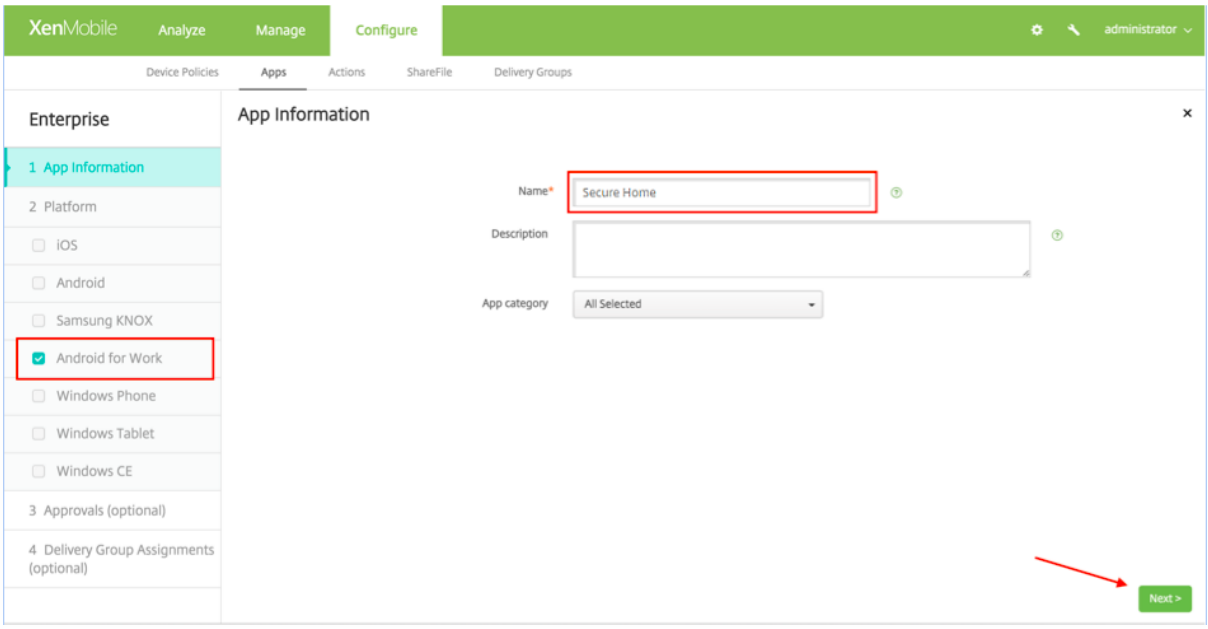
2. Cliquez sur **Entreprise**.

La page **Informations sur l'application** s'affiche.

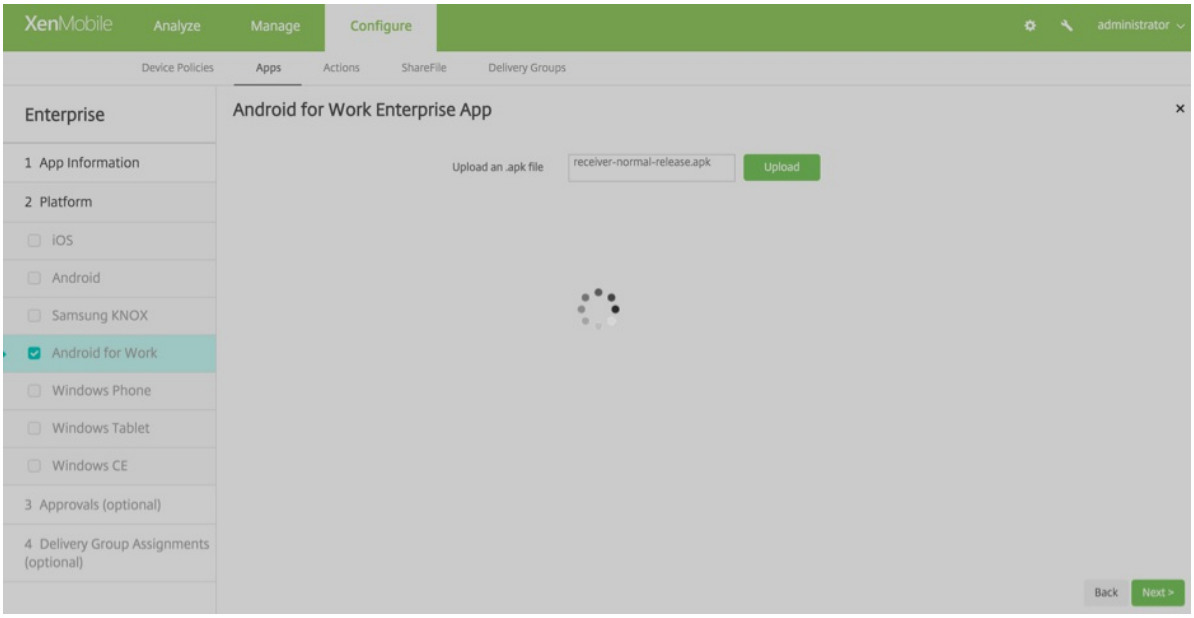


3. Sélectionnez la configuration suivante et cliquez sur **Suivant**.

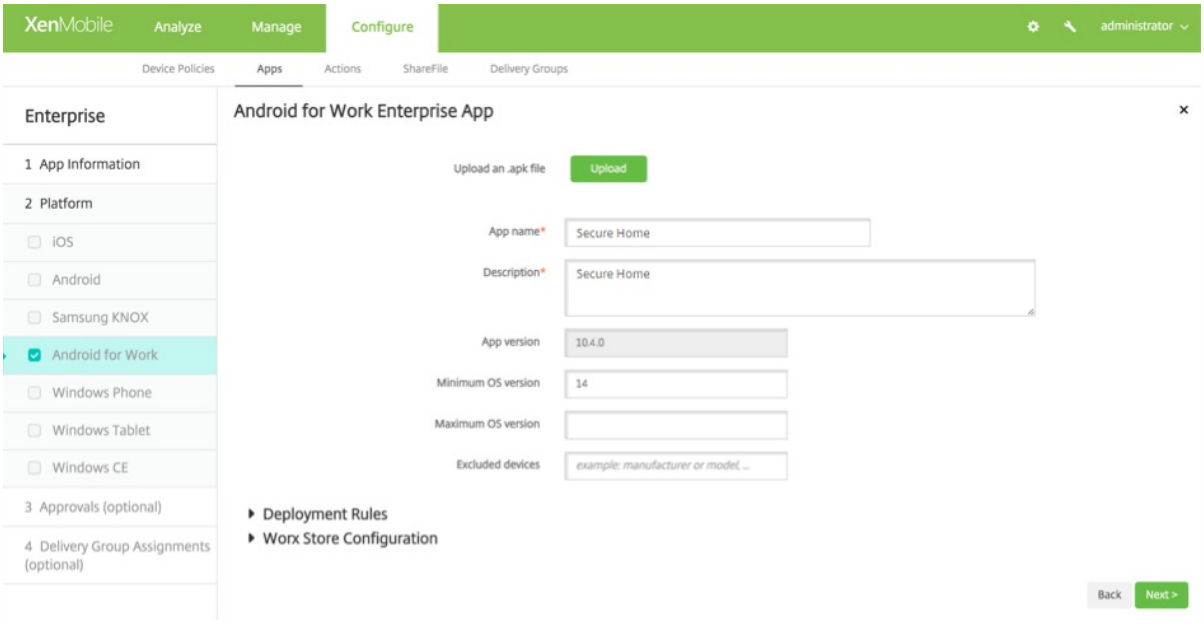
L'écran **Application Android for Work d'entreprise** s'affiche.



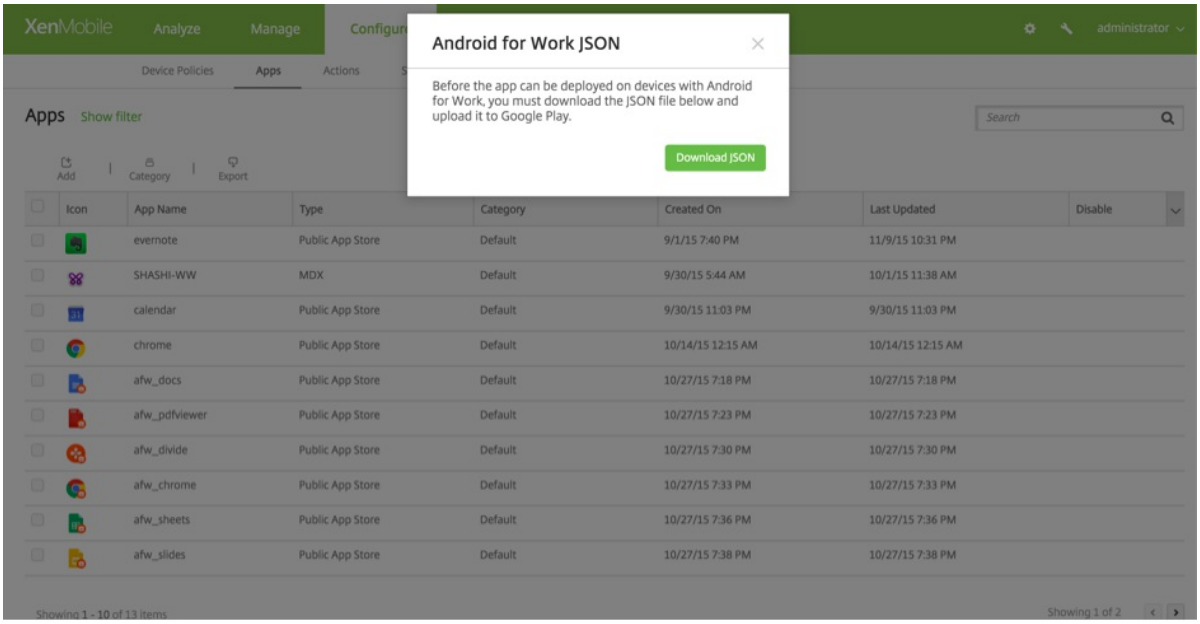
4. Fournissez le chemin d'accès au fichier .apk et cliquez sur **Suivant** pour charger le fichier.



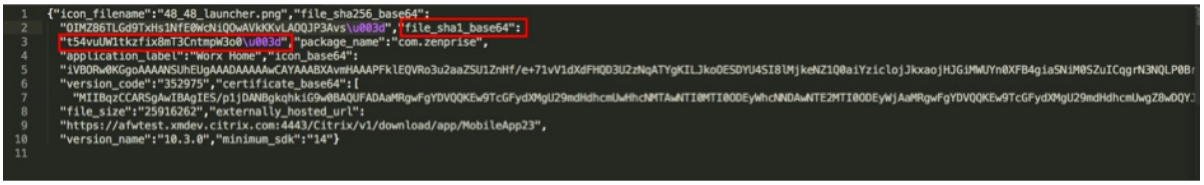
Une fois le chargement terminé, vous verrez les détails du package chargé.



5. Cliquez sur **Suivant** pour afficher une page permettant de télécharger le fichier JSON, que vous pouvez ensuite utiliser pour le chargement sur Google Play. Pour Secure Hub, le chargement sur Google Play n'est pas requis, mais vous avez besoin du fichier JSON pour lire la valeur SHA1.



Un fichier JSON typique ressemble à ce qui suit :



6. Copiez la valeur de **file_sha1_base64** et utilisez-la dans le champ **Hash** de Provisioning Tool. **Remarque** : l'URL du hachage doit être sécurisée.

- Convertissez tous les symboles **+** en **-**
- Convertissez tous les symboles **/** en **_**

- Remplacez **\u003d** à la fin de la valeur par **=**

Si vous stockez le hachage dans le fichier nfcprovisioning.txt de la carte SD de l'appareil, l'application procède à la conversion de sécurité. Toutefois, si vous décidez d'entrer le hachage manuellement, il est de votre responsabilité de vous assurer que l'URL est sécurisée.

Bibliothèques utilisées

Provisioning Tool utilise les bibliothèques suivantes dans son code source :

- Bibliothèque v7 appcompat par Google sous licence Apache 2.0
- Bibliothèque Design Support par Google sous licence Apache 2.0
- Bibliothèque v7 Palette par Google sous licence Apache 2.0
- Butter Knife par Jake Wharton sous licence Apache 2.0

Inscription en bloc d'appareils iOS

Mar 31, 2017

Vous pouvez inscrire un grand nombre d'appareils iOS dans XenMobile de deux façons.

- Vous pouvez utiliser le programme d'inscription des appareils (DEP) d'Apple pour inscrire les appareils que vous achetez directement auprès d'Apple ou d'un revendeur ou opérateur Apple agréé.
- Vous pouvez utiliser Apple Configurator pour inscrire des appareils, que vous les ayez achetés ou non directement auprès d'Apple.

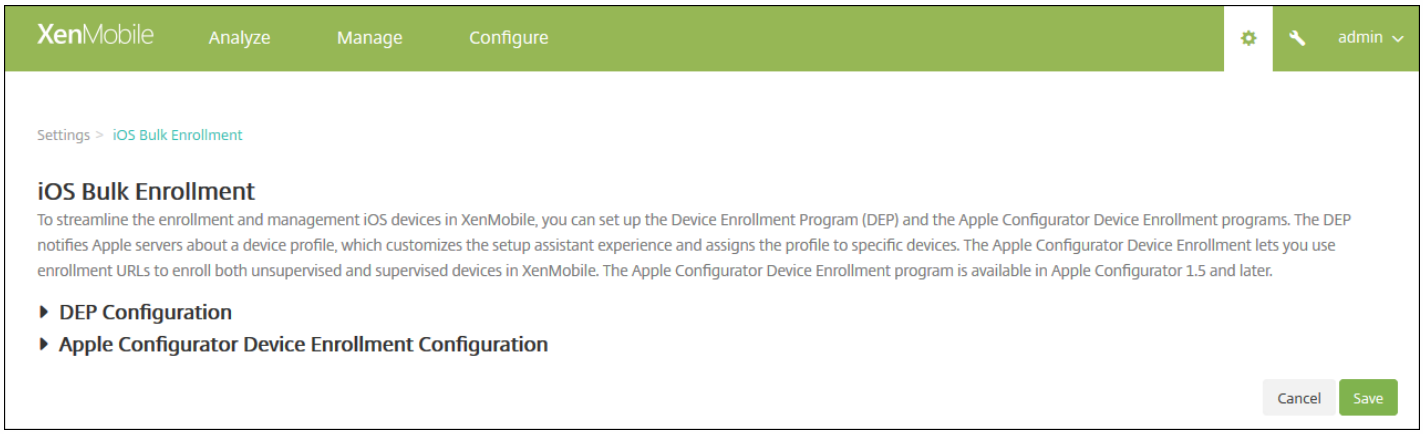
XenMobile 10.x prend en charge Apple Configurator v2.

Avec le programme DEP, vous n'avez aucune tâche de préparation à effectuer sur les appareils. Vous envoyez les numéros de série d'appareil ou numéros de commande via DEP. Vous configurez et inscrivez ensuite les appareils dans XenMobile. Après l'inscription des appareils, ils peuvent être distribués aux utilisateurs qui peuvent les utiliser sans aucune configuration supplémentaire. De plus, lorsque vous configurez des appareils avec le programme DEP, vous pouvez supprimer certaines des étapes de l'assistant d'installation. Cela élimine les tâches que les utilisateurs auraient dû effectuer lors du démarrage de leurs appareils pour la première fois. Pour de plus amples informations sur la configuration du programme DEP, reportez-vous à la page Programme d'inscription des appareils d'Apple.

Avec Apple Configurator, vous associez des appareils à un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure et l'application Apple Configurator. Vous préparez les appareils et configurez des stratégies à l'aide de Apple Configurator. Après avoir provisionné les appareils avec les stratégies requises et que les appareils se connectent à XenMobile, les stratégies sont appliquées et vous pouvez commencer à gérer les appareils. Pour de plus amples informations sur l'utilisation de Apple Configurator, consultez Apple Configurator.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **Inscription en bloc iOS**. La page **Inscription en bloc iOS** s'affiche.



Si vous configurez des paramètres DEP, voir ci-dessous. Si vous configurez les paramètres d'Apple Configurator, veuillez consulter la section Configuration des paramètres d'Apple Configurator.

Configuration des paramètres DEP

Conditions préalables : avant de continuer, vous devez avoir créé un compte Apple DEP sur deploy.apple.com. Après avoir

créé un compte DEP, configurez un serveur MDM virtuel pour autoriser les communications entre XenMobile et Apple. Pour ce faire, vous devez charger une clé publique XenMobile sur le site d'Apple. Une fois la clé publique reçue, Apple renvoie un jeton de serveur que vous importez dans XenMobile.

Suivez ces étapes pour établir la connexion entre XenMobile et Apple.

1. Pour obtenir la clé publique à charger sur Apple, sur la page **Inscription en bloc iOS**, développez **Configuration DEP**, cliquez sur **Exporter la clé publique** et enregistrez le fichier sur votre ordinateur.

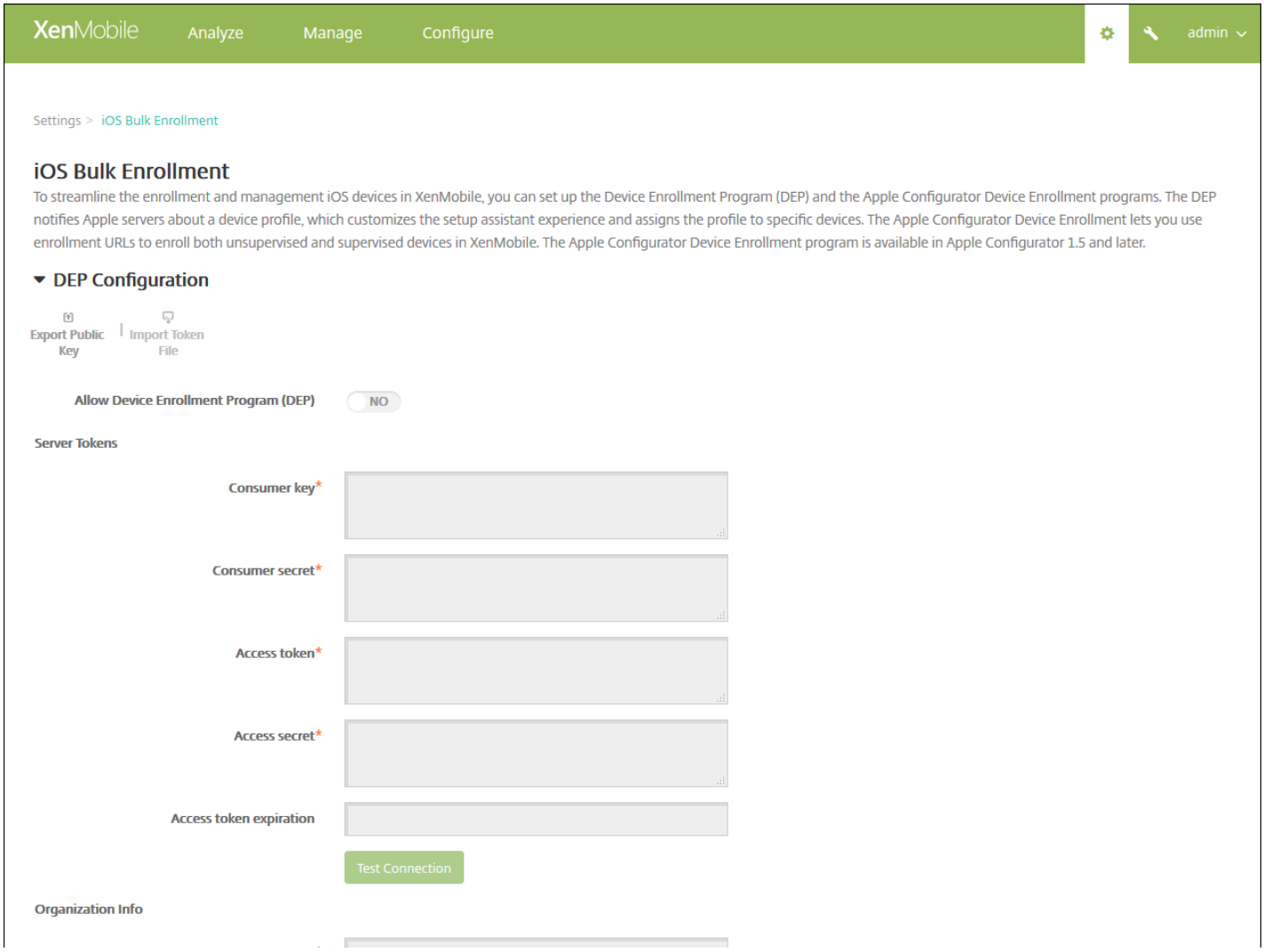
2. Accédez à deploy.apple.com, connectez-vous à votre compte DEP et suivez les instructions pour configurer un serveur MDM. Dans le cadre de ce processus, Apple fournit un jeton de serveur.

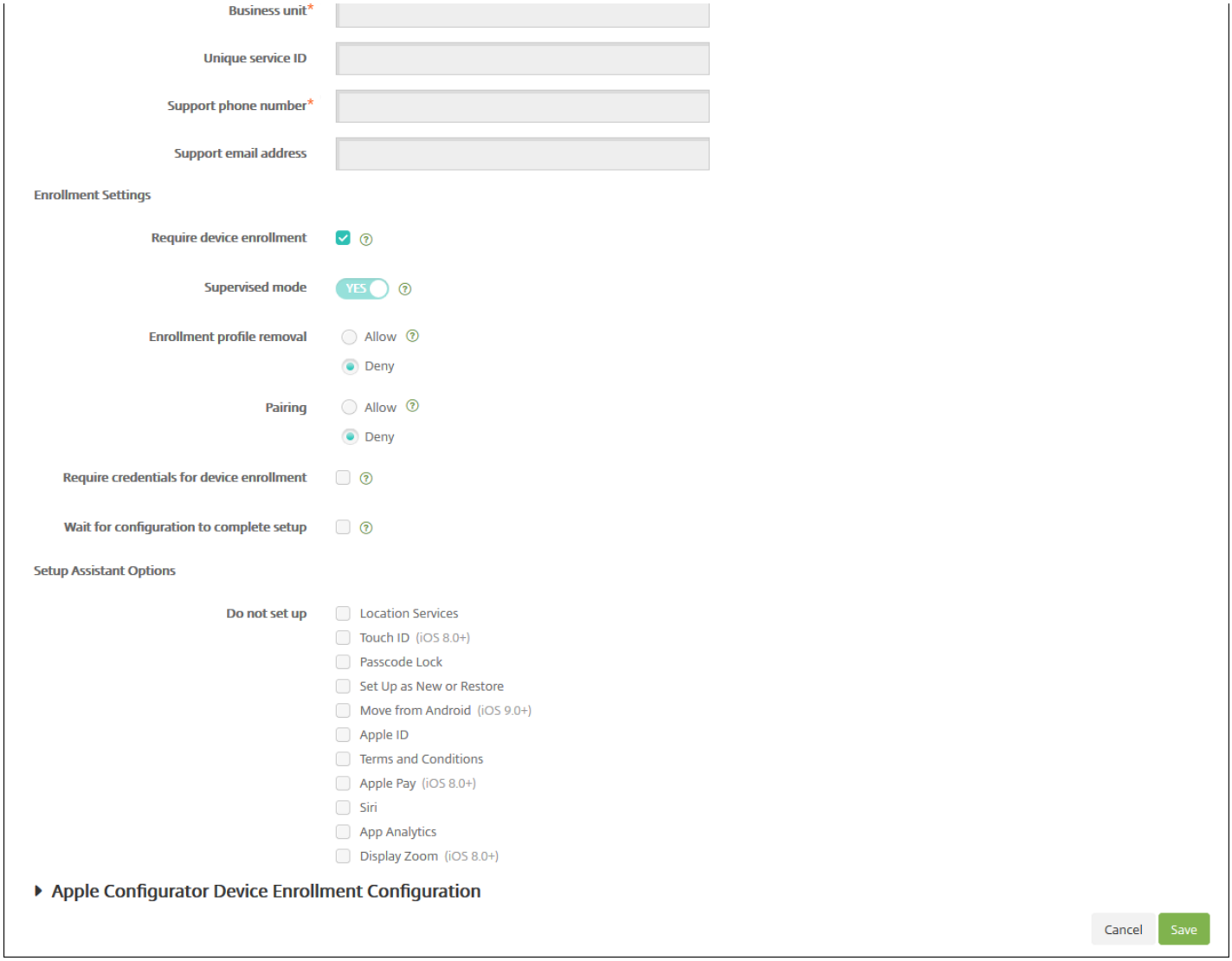
3. Sur la page **Inscription en bloc iOS**, cliquez sur **Importer un fichier jeton** pour ajouter le jeton de serveur Apple à XenMobile.

4. Le champ **Jetons de serveur** est renseigné automatiquement dès que le fichier de jeton est chargé sur XenMobile.

5. Cliquez sur **Tester la connectivité** pour confirmer que XenMobile et Apple peuvent communiquer.

Si le test de la connexion échoue, vérifiez que vous avez bien ouvert tous les ports requis car ce type de problème est à l'origine de la plupart des échecs. Pour de plus amples informations sur les ports qui doivent être ouverts dans XenMobile, consultez la section Configuration requise pour les ports.





6. Configurez les paramètres suivants pour terminer la configuration DEP :

Informations sur l'organisation

- **Division** : entrez la division ou le département à laquelle ou auquel l'appareil est attribué. Ce champ est obligatoire.
- **ID de service unique** : entrez un ID unique (facultatif).
- **Numéro de téléphone de l'assistance** : entrez un numéro de téléphone d'assistance que les utilisateurs peuvent appeler pour obtenir de l'aide au cours de la configuration. Ce champ est obligatoire.
- **Adresse e-mail de l'assistance** : entrez une adresse e-mail d'assistance (facultatif).

Paramètres d'inscription

- **Exiger l'inscription des appareils** : sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. Par défaut, l'inscription est exigée.
- **Mode supervisé** : doit être défini sur **Oui** si vous utilisez Apple Configurator pour gérer les appareils inscrits auprès de DEP ou lorsque **Attendre la fin de l'installation** est activé. La valeur par défaut est **Oui**. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator plus loin dans cet article.

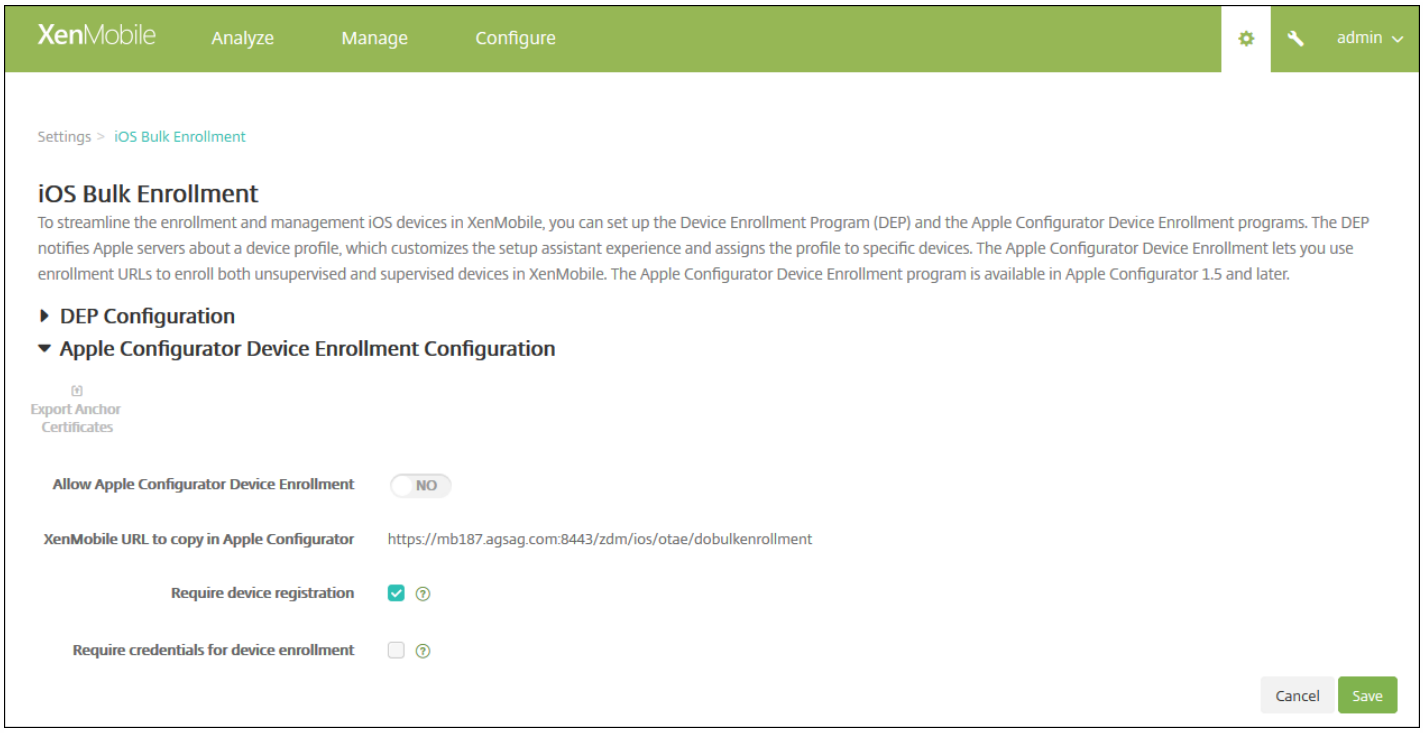
- **Suppression du profil d'inscription** : indiquez si vous souhaitez autoriser les appareils à utiliser un profil qui peut être supprimé à distance. La valeur par défaut est **Refuser**.
- **Couplage** : sélectionnez cette option pour autoriser les appareils inscrits par le biais du programme DEP à être gérés via iTunes et Apple Configurator. La valeur par défaut est **Refuser**.
- **Exiger des informations d'identification pour l'inscription de l'appareil** : indiquez si vous souhaitez demander aux utilisateurs d'entrer leurs informations d'identification lors de la configuration de DEP. Cette option est disponible pour iOS 7.1 et version supérieure.**Remarque** : lorsque DEP est activé lors de la première configuration et que vous ne sélectionnez pas cette option, les composants DEP, tels que l'utilisateur DEP, Secure Hub, l'inventaire logiciel et le groupe de déploiement DEP sont créés dès le début. Si vous sélectionnez cette option, les composants ne sont pas créés tant que l'utilisateur n'a pas entré ses informations d'identification. Par conséquent, si vous désactivez cette option ultérieurement, les utilisateurs qui n'ont pas entré leurs informations d'identification ne peuvent pas s'inscrire au programme DEP, car ces composants DEP n'existent pas. Pour ajouter les composants DEP, dans ce cas, il est conseillé de désactiver et d'activer le compte DEP.
- **Attendre la fin de l'installation** : indiquez si les appareils des utilisateurs doivent rester dans le mode Assistant d'installation jusqu'à ce que toutes les ressources MDM soient déployées sur l'appareil. Cette option est disponible sur les appareils iOS 9.0 et versions ultérieures en mode supervisé.
  - **Remarque** : la documentation Apple indique que les commandes suivantes peuvent ne pas fonctionner lorsqu'un appareil est en mode Assistant d'installation :
    - InviteToProgram
    - InstallApplication
    - ApplyRedemptionCode
    - InstallMedia
    - RequestMirroring
    - DeviceLock

Installation

Sélectionnez les étapes de l'Assistant d'installation iOS que vos utilisateurs ne devront pas utiliser (étapes à ignorer) lorsqu'ils démarreront leurs appareils pour la première fois.

- **Services de localisation** : configurez le service de localisation sur l'appareil.
- **Touch ID** : configurez Touch ID dans iOS 8.0 et versions ultérieures.
- **Verrouillage par code secret** : créez un code secret pour l'appareil.
- **Définir comme nouveau ou restaurer** : configurez l'appareil comme nouveau ou restaurez-le à partir d'une copie de sauvegarde d'iCloud ou d'iTunes.
- **Déplacer depuis Android** : activez le transfert des données à partir d'un appareil Android vers un appareil iOS 9 ou version ultérieure. Cette option est disponible uniquement lorsque **Définir comme nouveau** ou **Restaurer** est sélectionné (sinon, cette étape est ignorée).
- **Apple ID** : configurez un compte Apple ID pour l'appareil.
- **Termes et conditions** : exigez que l'utilisateur accepte les termes et conditions pour utiliser l'appareil.
- **Apple Pay** : configurez Apple Pay dans iOS 8.0 et versions ultérieures.
- **Siri** : utilisez ou non Siri sur l'appareil.
- **Analyse de l'application** : configurez cette option si vous souhaitez partager les données d'incidents et les statistiques d'utilisation avec Apple.
- **Zoom d'affichage** : définissez la résolution d'affichage (standard ou zoom) sur les appareils iOS 8.0 et versions ultérieures.

Configuration des paramètres d'Apple Configurator



1.Développez **Configuration du DEP Apple Configurator**.

2. Définissez **Activer l'inscription d'appareils dans Apple Configurator** sur **Oui**.

3. Notez et configurez les paramètres suivants :

- **URL XenMobile à copier dans Apple Configurator** : ce champ en lecture seule est l'adresse URL du serveur XenMobile qui communique avec Apple, et que vous copiez et collez dans Apple Configurator ultérieurement. Dans Apple Configurator 2, l'adresse URL d'inscription est le nom de domaine complet (FQDN) ou l'adresse IP du serveur XenMobile, comme mdm.server.url.com.
- **Exiger l'inscription de l'appareil** : la sélection de ce paramètre nécessite que vous ajoutiez les appareils configurés sur l'onglet **Appareils** dans XenMobile manuellement ou via un fichier CSV avant de pouvoir les inscrire. Cela permet de garantir qu'aucun appareil inconnu ne peut s'inscrire. La valeur par défaut est de demander l'ajout d'appareils.
- **Exiger des informations d'identification pour l'inscription de l'appareil** : exigez que les utilisateurs d'appareils iOS 7.1 et versions ultérieures entrent leurs informations d'identification lors de l'inscription. Par défaut, les informations d'identification ne sont pas exigées.

> ## Remarque
>
> Si le serveur XenMobile utilise un certificat SSL approuvé, passez à l'étape suivante.

4. Cliquez sur **Exporter les certificats d'ancrage** et enregistrez le fichier certchain.pem sur le trousseau OS X (de connexion ou système).

5. Démarrez Apple Configurator et accédez à **Prepare** -> **Setup** -> **Configure Settings**.

6. Dans le paramètre Device Enrollment, collez l'URL du serveur MDM de l'étape 4 dans le champ **MDM server URL** du

Configurator.

7. Dans le paramètre **Device Enrollment**, copiez l'autorité de certification racine et l'autorité de certification des serveurs SSL sur les certificats d'**ancrage**, si XenMobile n'utilise pas un certificat SSL approuvé.

8. Utilisez un câble Dock Connector vers USB pour connecter des appareils au Mac exécutant Apple Configurator pour configurer simultanément jusqu'à 30 appareils connectés. Si vous ne disposez pas d'un Dock Connector, utilisez un ou plusieurs hubs (alimentés) USB 2.0 haute vitesse pour connecter les appareils.

9. Cliquez sur **Prepare**. Pour plus d'informations sur la préparation d'appareils avec Apple Configurator, consultez la page d'aide d'Apple Configurator Prepare devices.

10. Dans Apple Configurator, configurez les stratégies dont vous avez besoin.

11. À mesure que chaque appareil est préparé, activez-le pour démarrer l'Assistant d'installation iOS, qui prépare l'appareil pour la première utilisation.

Pour renouveler ou mettre à jour des certificats lors de l'utilisation du programme DEP d'Apple

Lorsque le certificat SSL de XenMobile est renouvelé, vous chargez un nouveau certificat dans la console XenMobile dans **Paramètres** > **Certificats**. Dans la boîte de dialogue **Importer**, dans **Utiliser en tant que**, cliquez sur **Écouteur SSL** afin que le certificat soit utilisé pour SSL. Lorsque vous redémarrez le serveur, XenMobile utilise le nouveau certificat SSL. Pour de plus amples informations sur les certificats dans XenMobile, consultez la section Chargement de certificats dans XenMobile.

Il n'est pas nécessaire de rétablir la relation d'approbation entre le programme DEP d'Apple et XenMobile lorsque vous renouvelez ou mettez à jour le certificat SSL. Vous pouvez, cependant, reconfigurer vos paramètres DEP à tout moment en suivant les étapes précédentes dans cet article.

Pour plus d'informations sur le programme DEP d'Apple, consultez la documentation Apple.

Pour plus d'informations sur un problème connu et la solution de contournement associée à cette configuration, consultez la section Problèmes connus de XenMobile Server 10.4.

Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator

> **Important**
>
> le fait de placer un appareil en mode supervisé installera la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

1. Installez Apple Configurator depuis iTunes.

2. Connectez l'appareil iOS à votre ordinateur Apple.

3. Démarrez Apple Configurator. Configurator indique que vous possédez un appareil à préparer pour la supervision.

4. Pour préparer l'appareil à des fins de supervision :

    a. Basculer le contrôle de supervision sur **Activé**. Citrix vous recommande de sélectionner ce paramètre si vous prévoyez de gérer le contrôle de l'appareil en appliquant à nouveau une configuration régulièrement.

b. Si vous le souhaitez, entrez un nom pour l'appareil.

c. Dans **iOS**, cliquez sur l'option **appropriée** afin d'obtenir la version la plus récente d'iOS que vous souhaitez installer.

5. Lorsque vous êtes prêt à préparer l'appareil pour la supervision, cliquez sur **Préparer**.

Déploiement d'appareils iOS via le programme DEP d'Apple

Feb 23, 2017

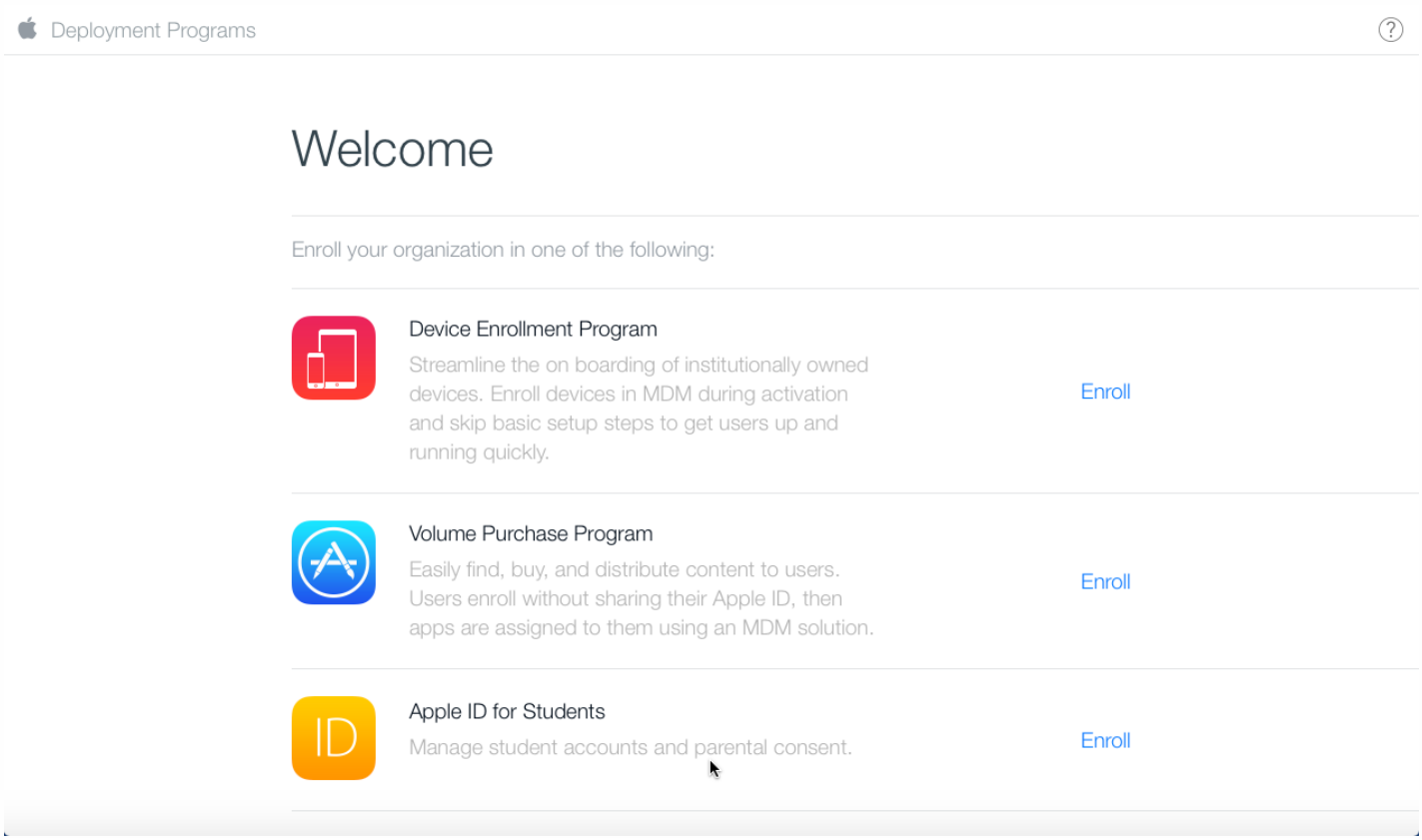
Vous avez besoin d'un compte Apple Developer Enterprise Program (DEP) pour bénéficier du programme DEP d'Apple pour inscrire et gérer des appareils iOS dans XenMobile. Les conditions principales que les organisations doivent respecter pour s'inscrire au programme DEP d'Apple sont les suivantes.

- Coordonnées professionnelles (adresse e-mail et numéro de téléphone)
- Contact pour validation
- Informations sur l'établissement (numéro DUNS / d'immatriculation fiscale)
- Numéro de client Apple

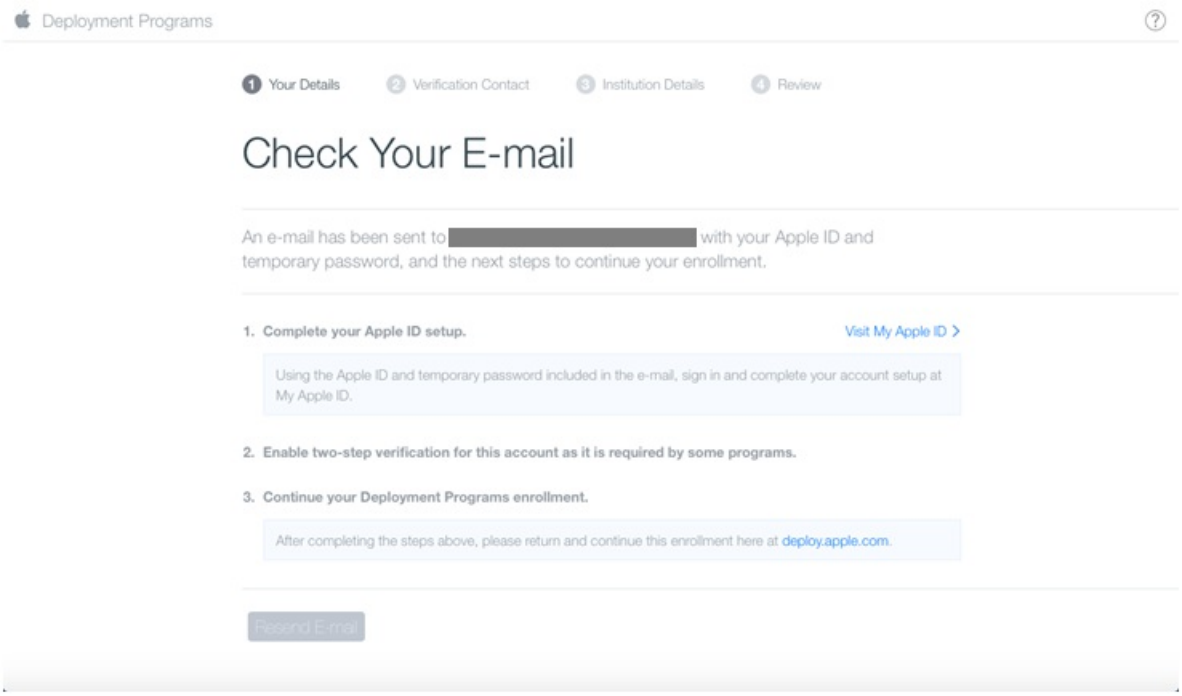
Pour de plus amples informations sur les détails du programme DEP d'Apple, consultez ce PDF d'Apple. Il est important de souligner que le programme DEP d'Apple est uniquement destiné aux organisations et non aux individus. Il est tout aussi important de savoir qu'un certain nombre de détails sur l'entreprise sont nécessaires pour créer un compte Apple DEP, par conséquent il peut s'écouler un certain temps entre la demande d'ouverture d'un compte et son approbation.

Demander l'ouverture d'un compte Apple DEP

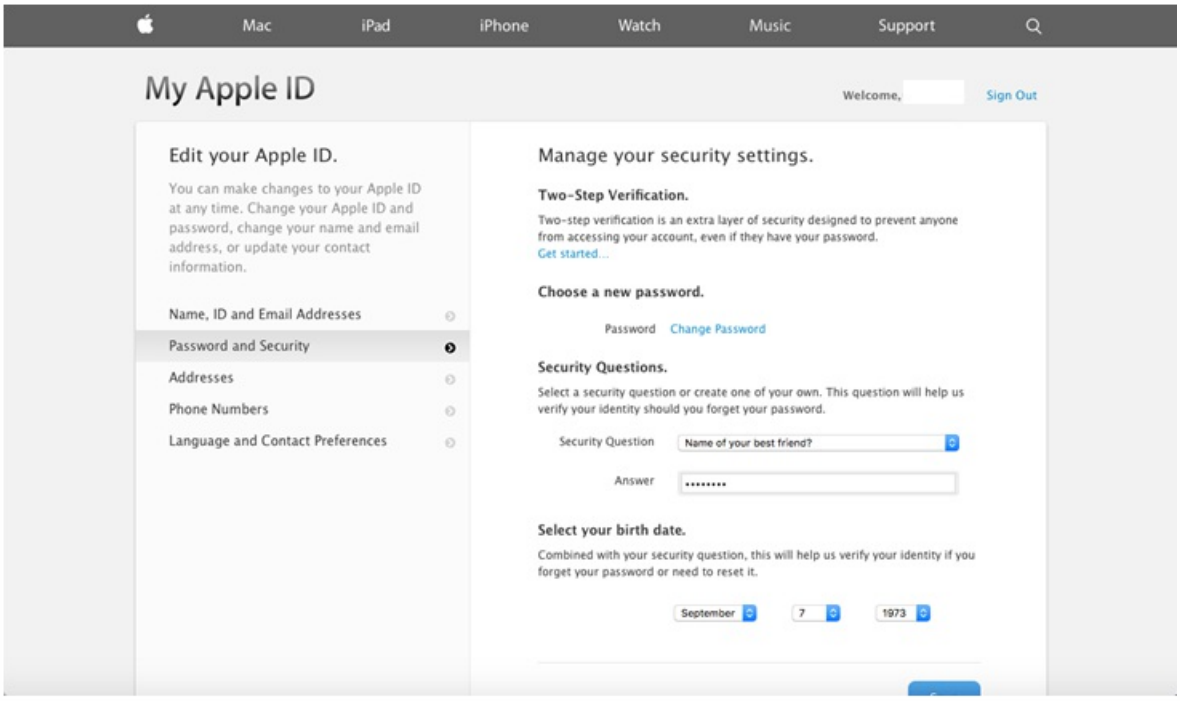
Lors de la demande d'ouverture d'un compte DEP, il est préconisé d'utiliser une adresse e-mail liée à l'organisation, telle que dep@société.com.



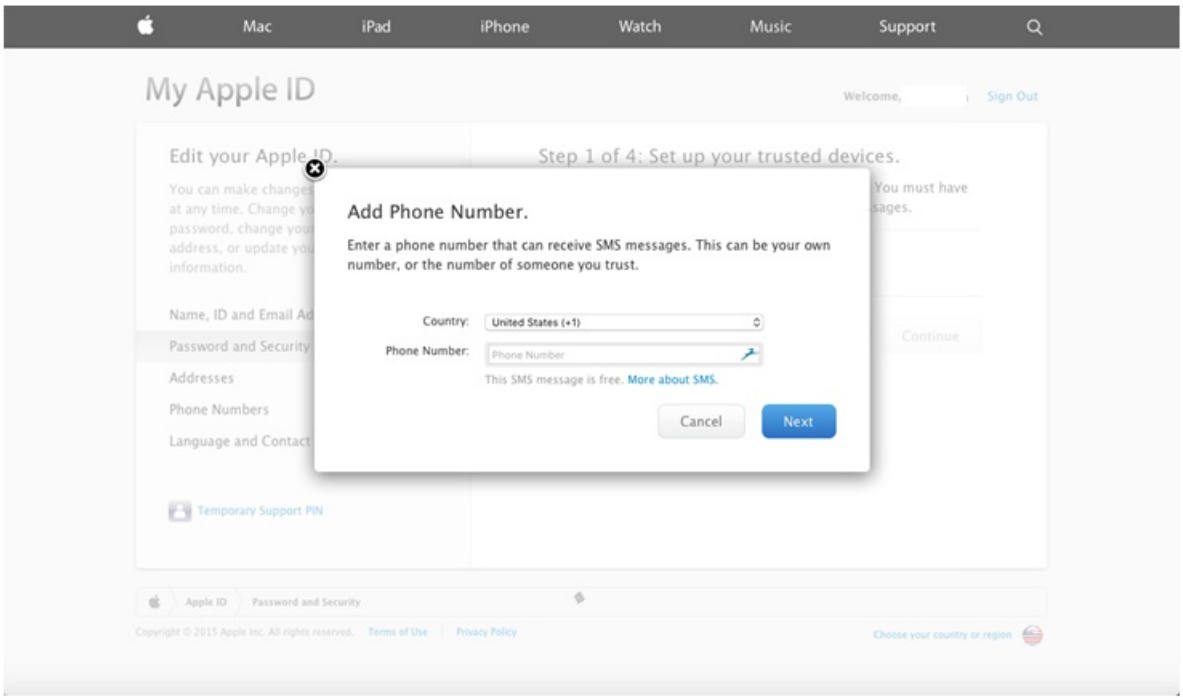
1. Après avoir entré les informations sur votre entreprise, vous allez recevoir par e-mail votre mot de passe temporaire ainsi qu'un nouvel identifiant Apple.



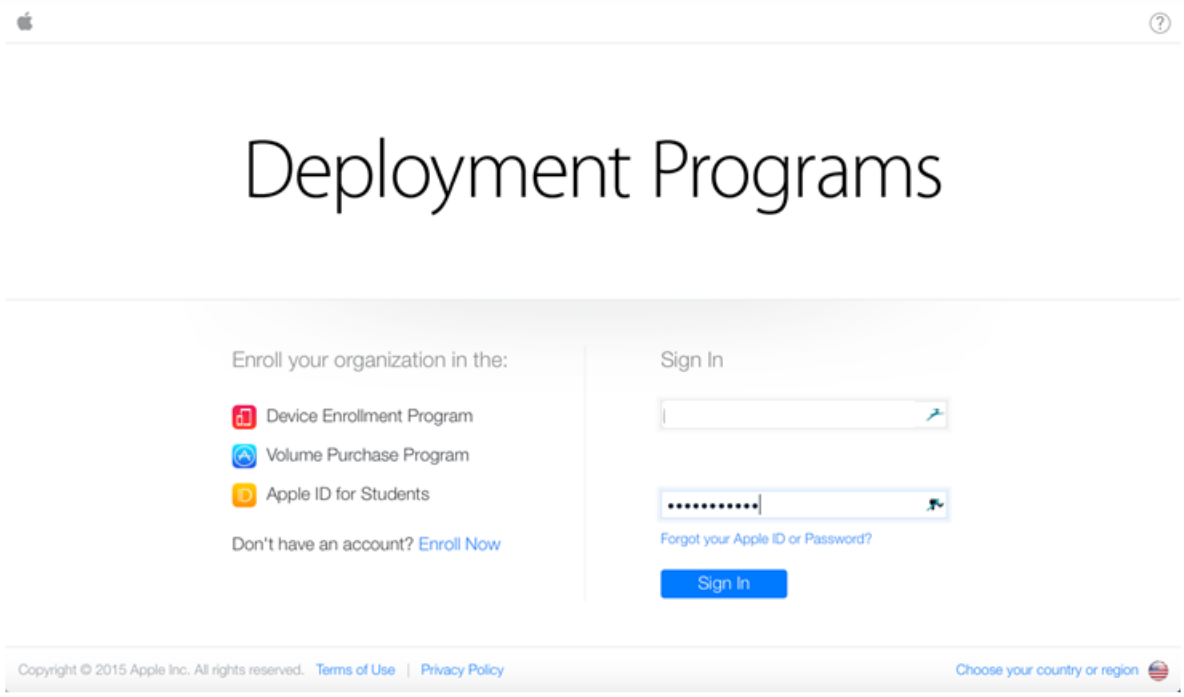
2. Connectez-vous à l'aide de cet identifiant Apple et configurez les paramètres de sécurité du compte.



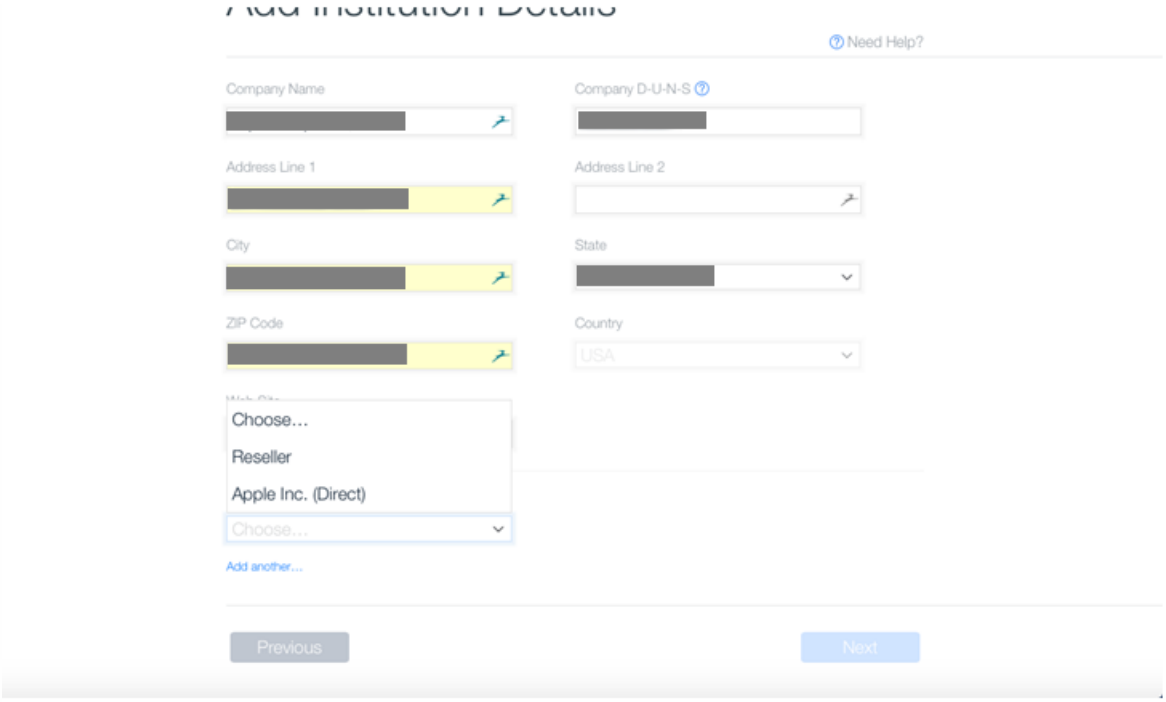
3. Configurez et activez la validation en deux étapes, ce qui est nécessaire pour utiliser le portail DEP. Durant ces étapes, vous ajoutez un numéro de téléphone par le biais duquel vous recevrez le code PIN à 4 chiffres requis pour la validation en deux étapes.



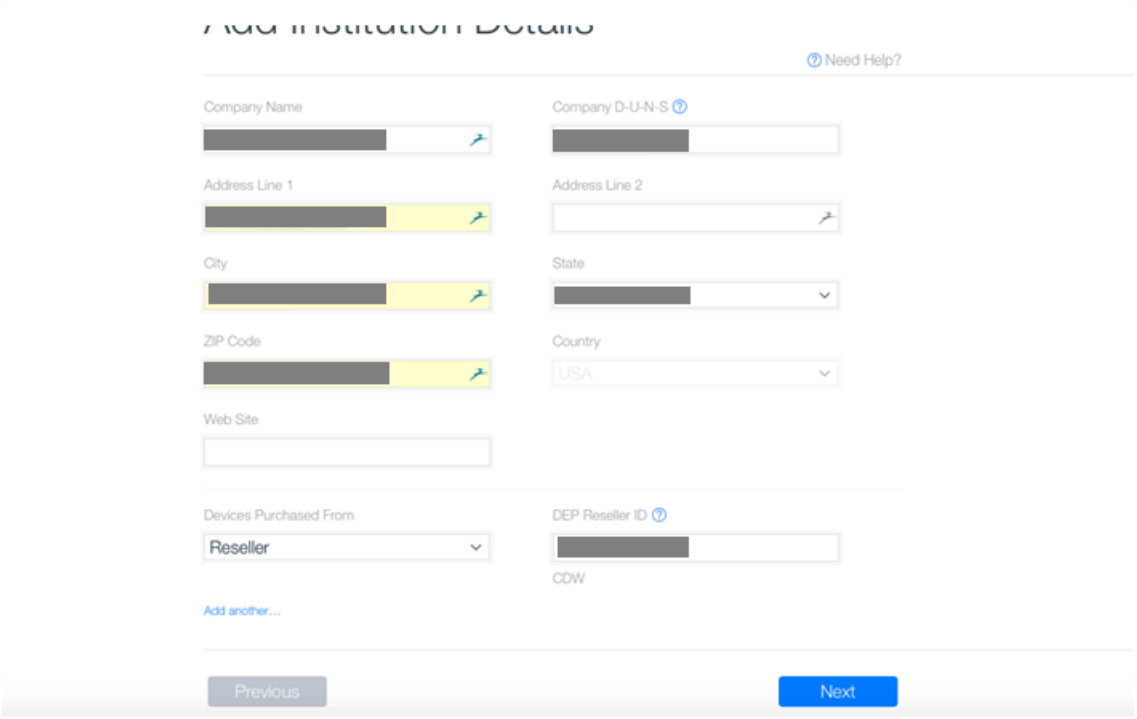
4. Connectez-vous au portail DEP pour terminer la configuration du compte à l'aide de la validation en deux étapes que vous venez de configurer.

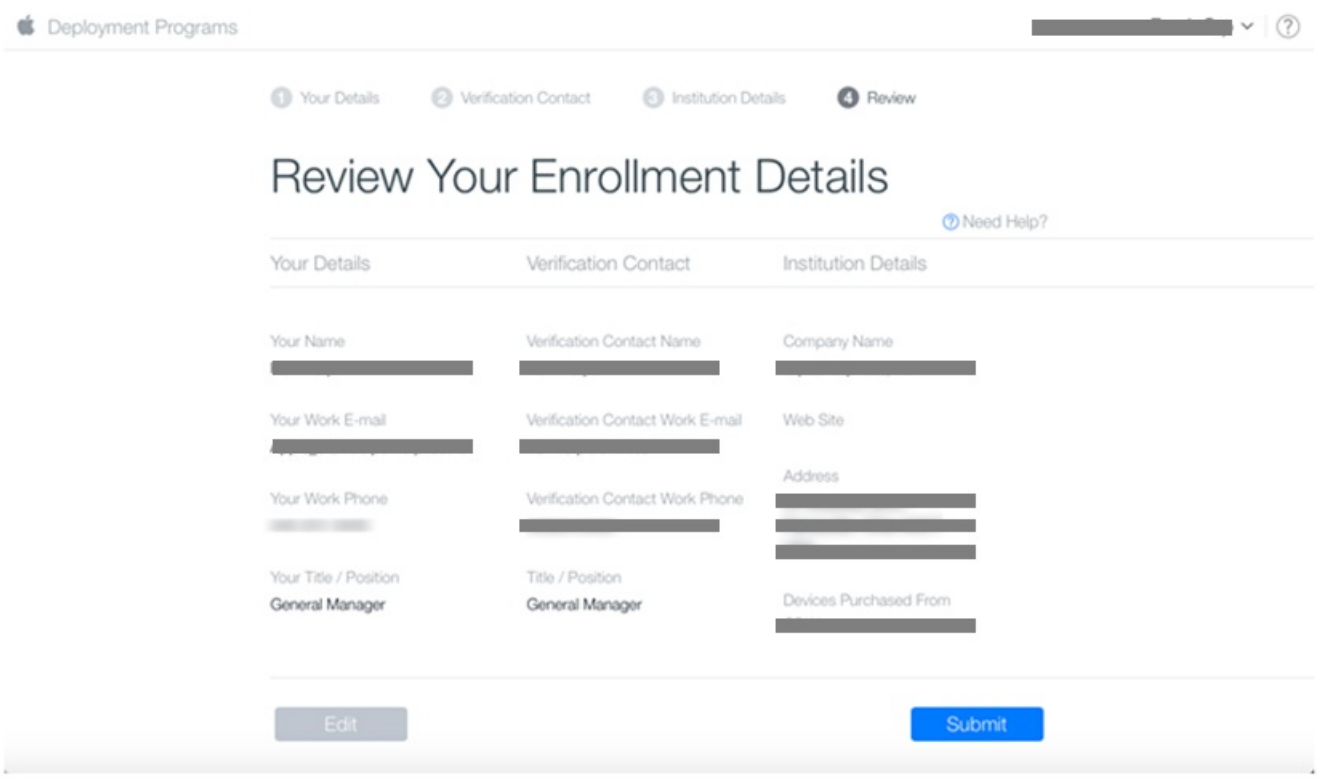


5. Ajoutez les détails de votre entreprise et sélectionnez là où vous avez acheté vos appareils. Pour de plus amples informations sur les options, consultez la section suivante, Commander des appareils compatibles avec le programme DEP.

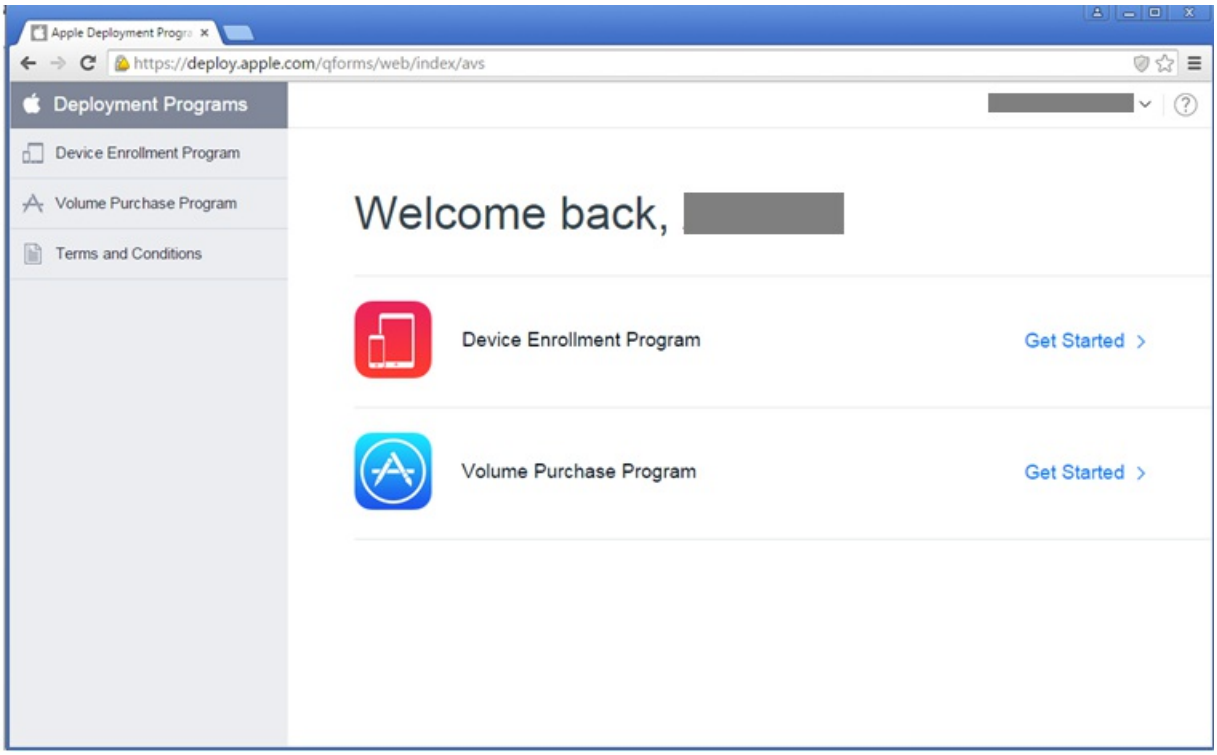


6. Ajoutez le numéro de client Apple ou l'ID du revendeur DEP, vérifiez vos détails d'inscription et attendez que Apple approuve votre compte.





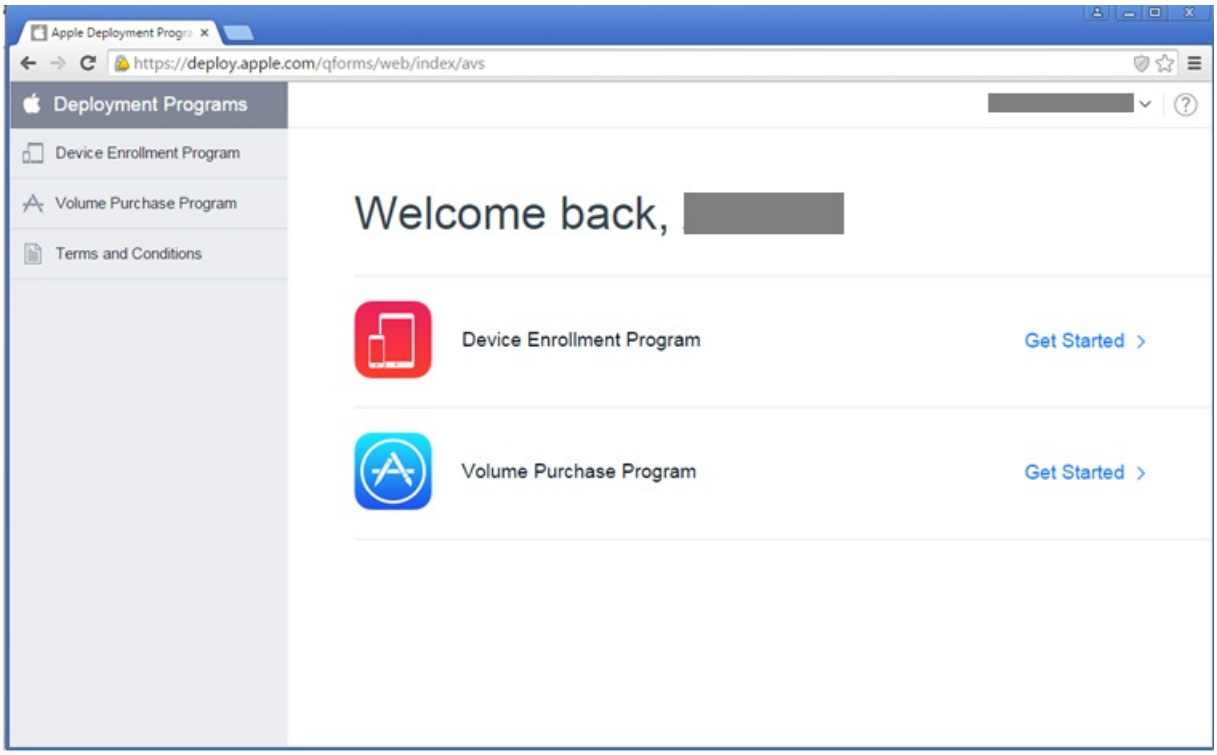
7. Après avoir reçu vos identifiants de connexion d'Apple, connectez-vous au portail DEP d'Apple. Suivez ensuite les étapes de la section suivante pour connecter votre compte avec XenMobile.



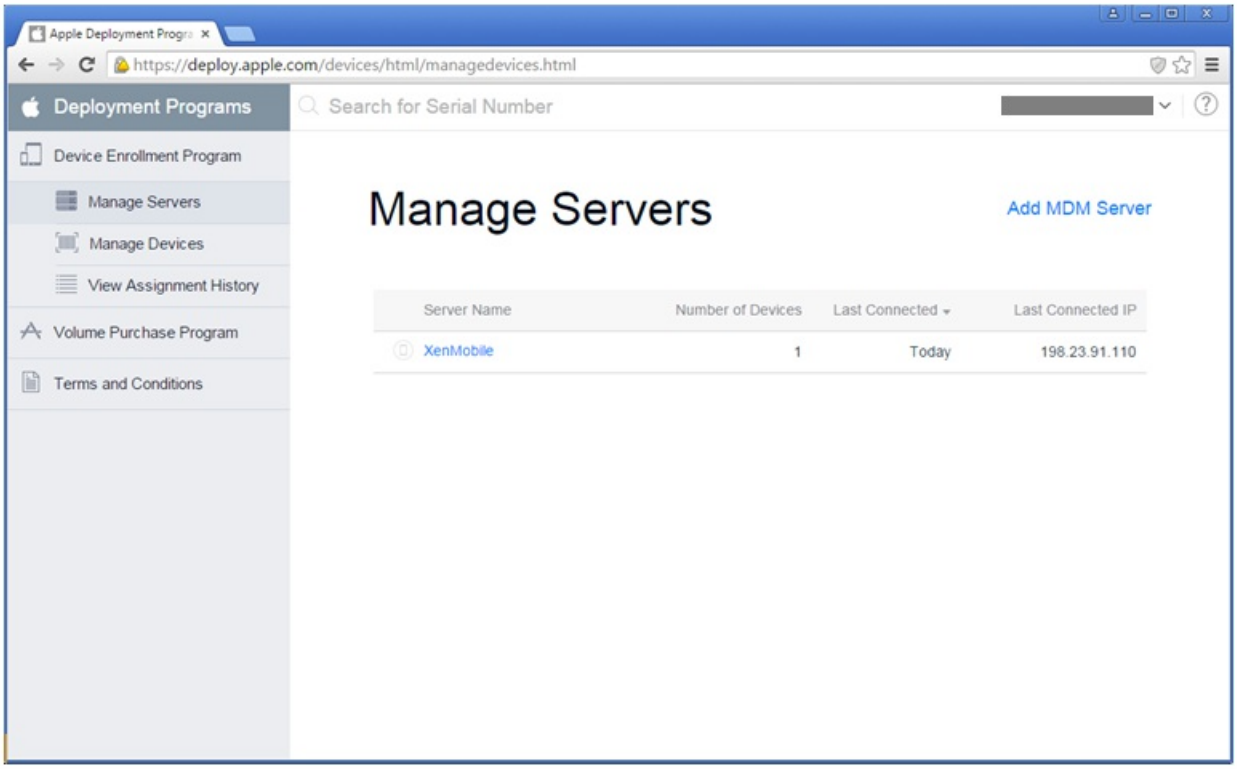
Intégration de votre compte DEP avec XenMobile

Suivez les étapes dans cette section pour connecter votre compte Apple DEP avec votre déploiement du serveur XenMobile.

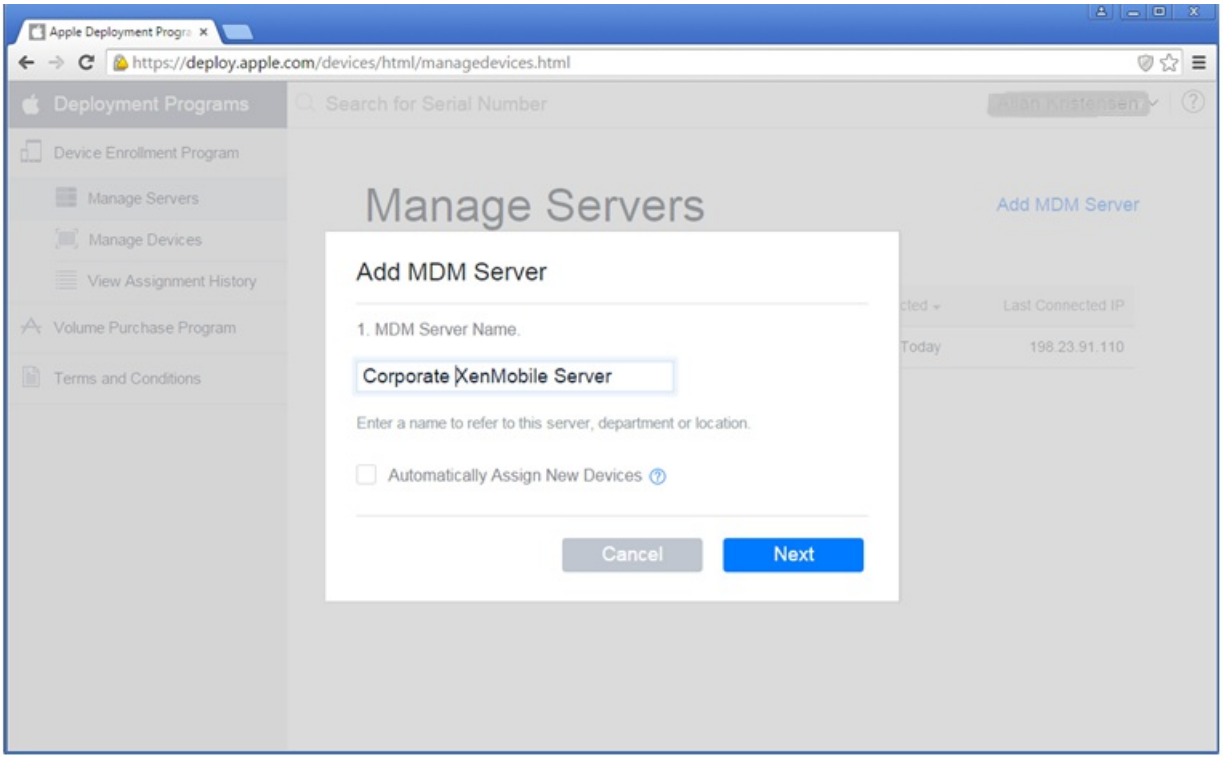
1. Sur le côté gauche du portail Apple DEP, cliquez sur **Programme d'inscription d'appareils**.



2. Cliquez sur **Gérer les serveurs** et sur le côté droit, cliquez sur **Ajouter un serveur MDM**.



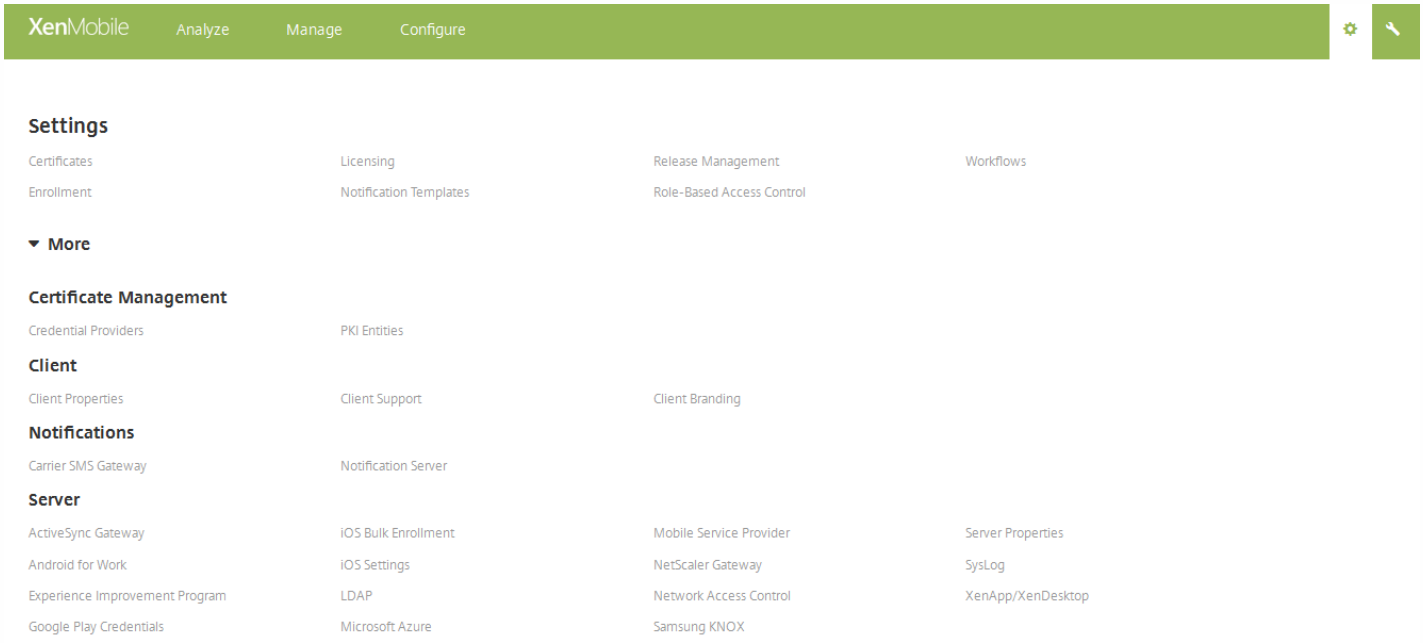
3. Dans **Ajouter un serveur MDM**, entrez un nom pour votre serveur XenMobile et cliquez sur **Suivant**.



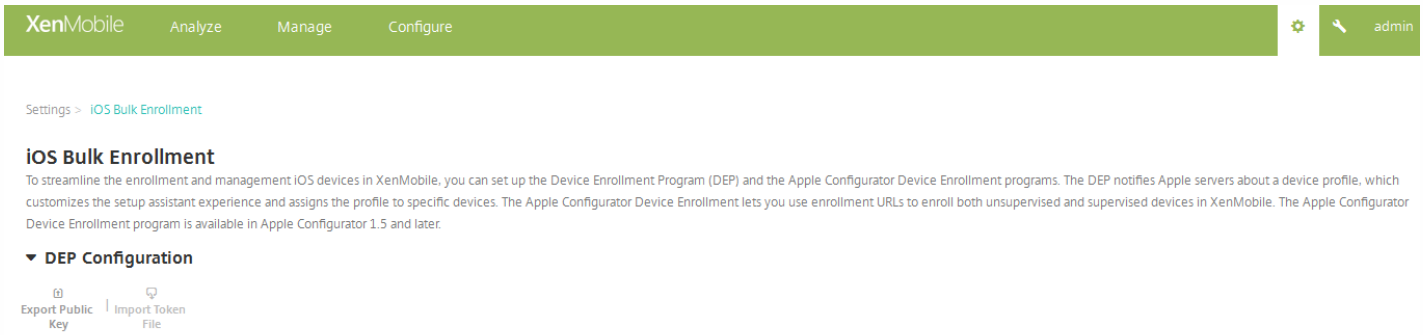
4. Chargez une clé publique depuis votre serveur XenMobile. Pour générer la clé depuis XenMobile, procédez comme suit :

    a. Connectez-vous à la console XenMobile et cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

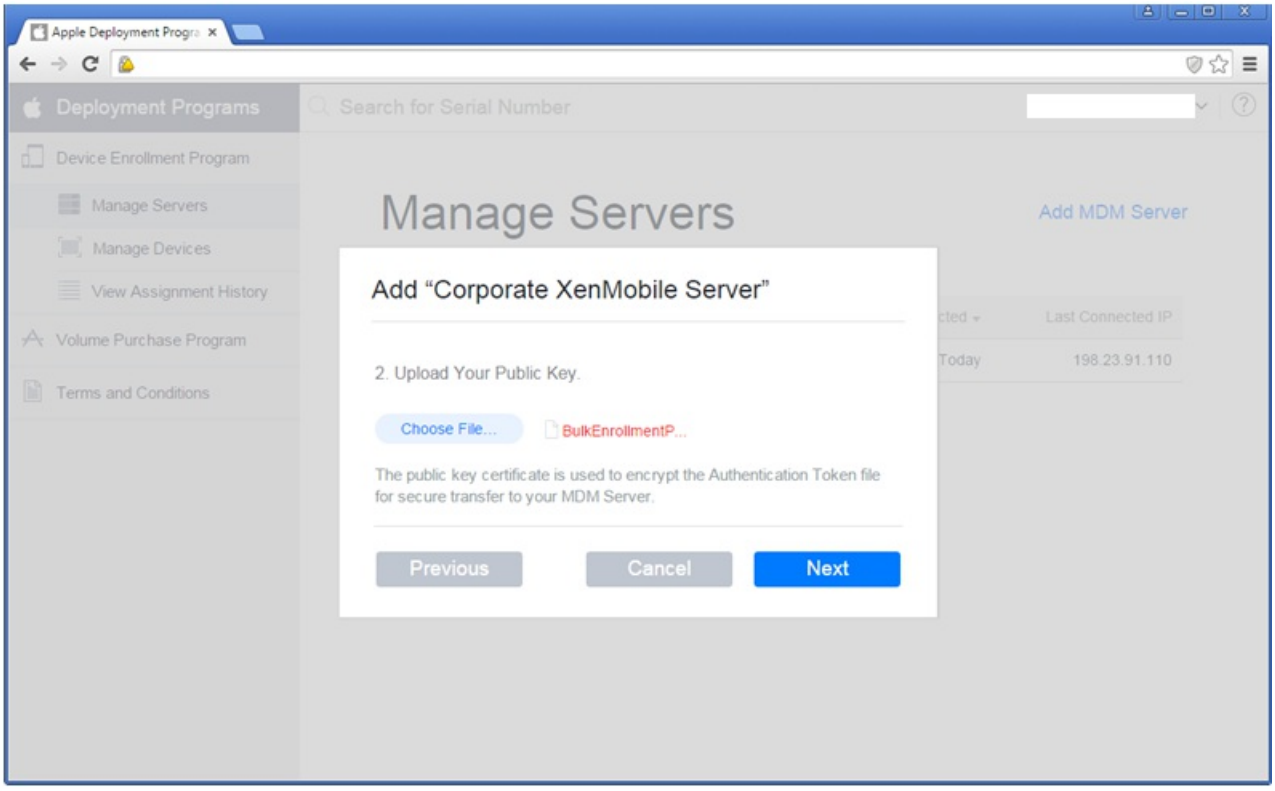
    b. Sous **Plus**, cliquez sur **Inscription en bloc iOS**.



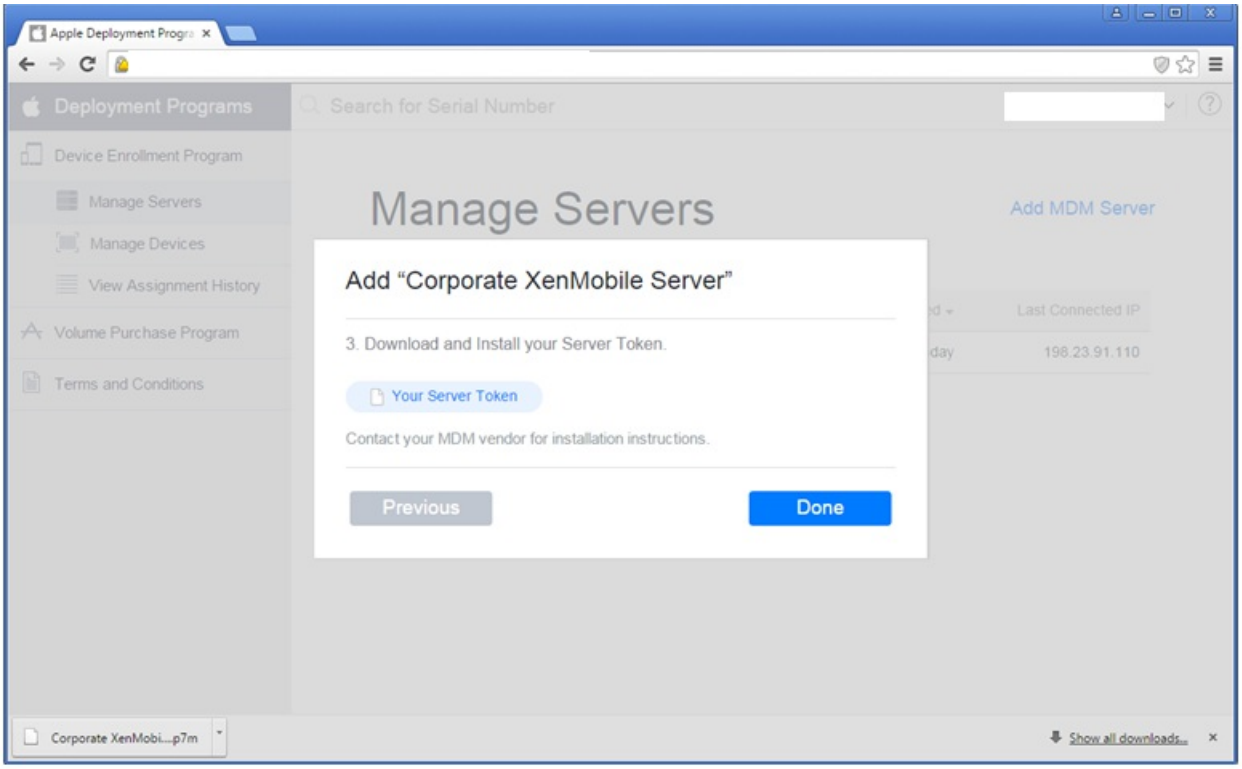
b. Sur la page **Inscription en bloc iOS**, développez **Configuration DEP** et cliquez sur **Exporter la clé publique**. La clé publique est téléchargée.



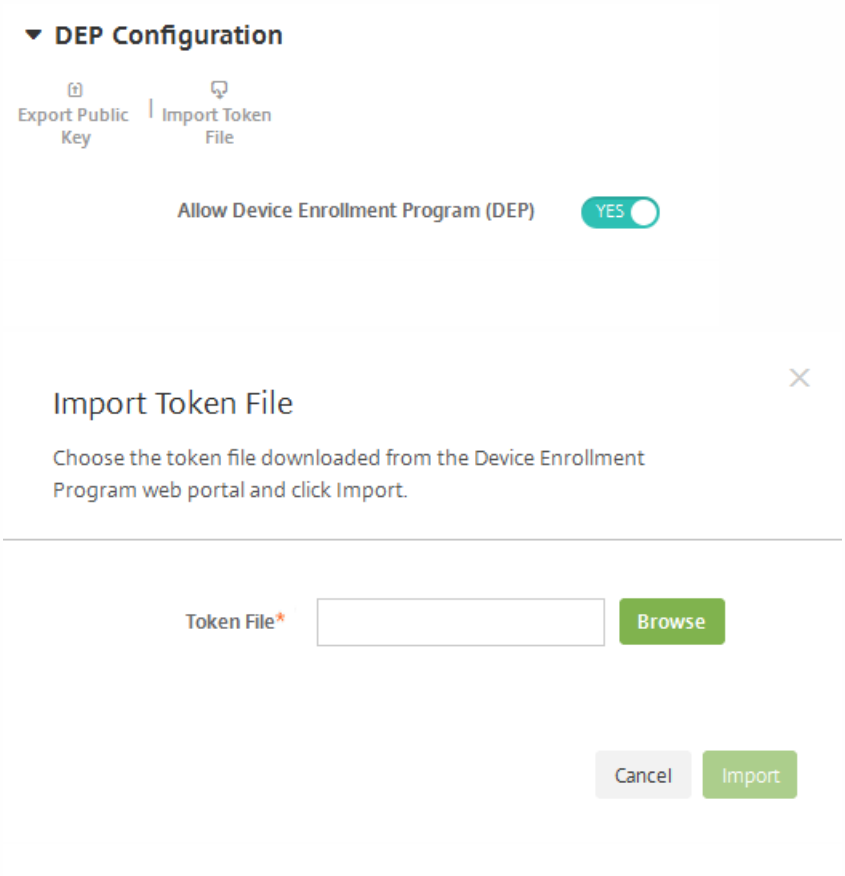
5. Sur le portail Apple DEP, cliquez **Choisir un fichier**, sélectionnez la clé publique que vous venez de télécharger et cliquez sur **Suivant**.



6. Cliquez sur **Votre jeton de serveur** pour générer un jeton de serveur, lequel est téléchargé depuis le navigateur, et cliquez sur **Terminé**.

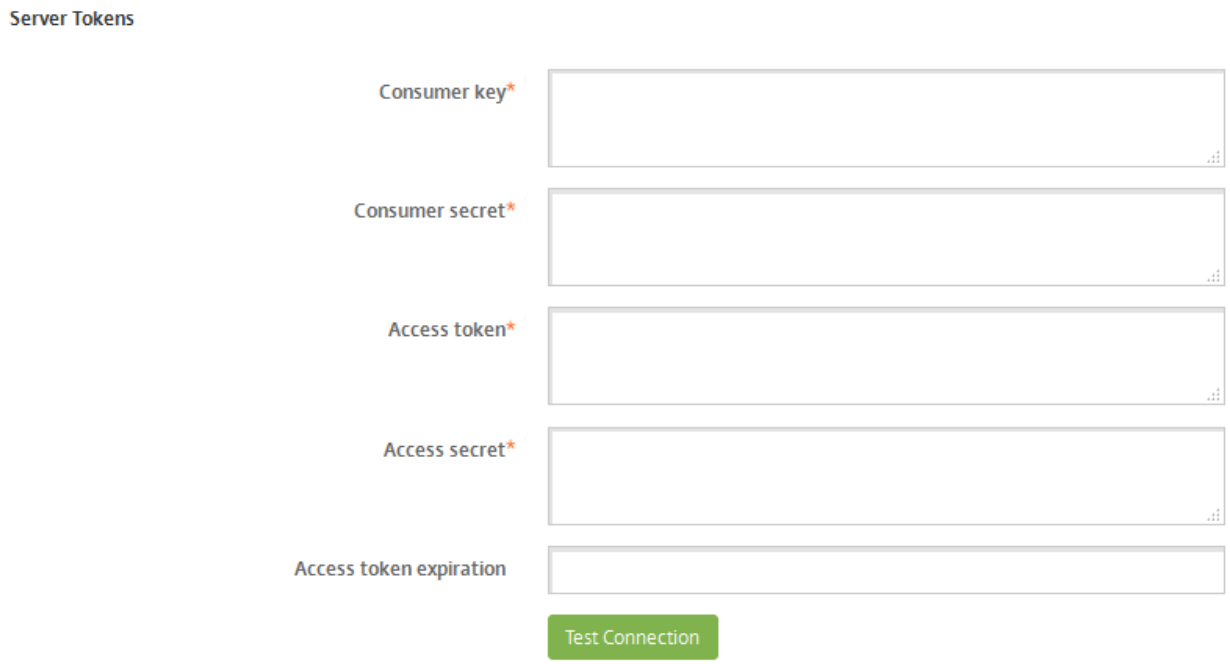


7. Sur la page **Inscription en bloc iOS** de la console XenMobile, en regard de **Autoriser Device Enrollment Program (DEP)**, cliquez sur OUI, cliquez sur **Importer un fichier jeton** et chargez le fichier jeton que vous avez téléchargé dans l'étape précédente.



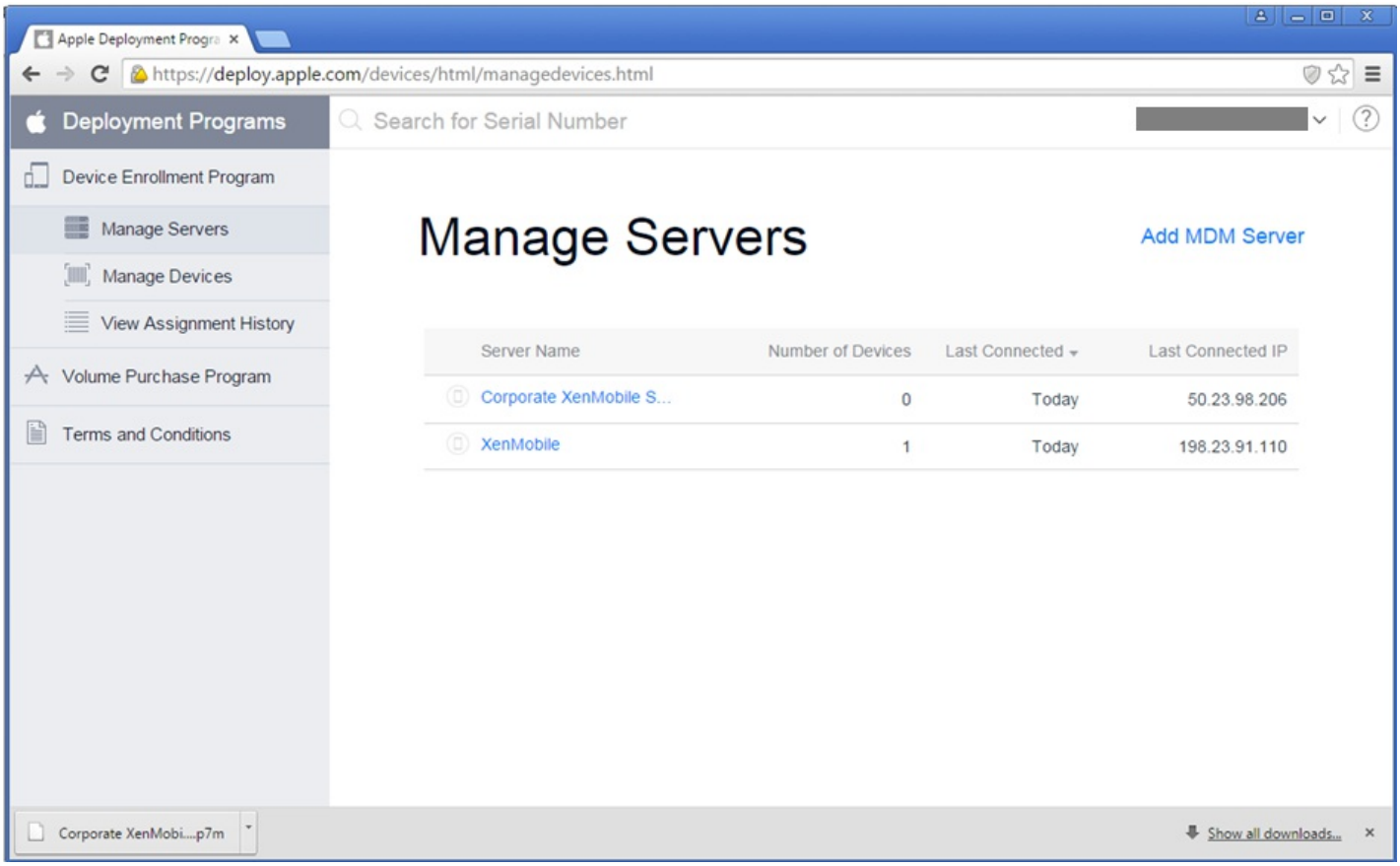
Les informations de votre jeton Apple DEP s'affichent dans la console XenMobile après l'importation du fichier de jeton.

8. Cliquez sur **Tester la connexion** pour vérifier la connexion du programme DEP d'Apple avec XenMobile.



9. Sur la page **Inscription en bloc iOS**, finalisez les paramètres supplémentaires, sélectionnez les contrôles et stratégies du programme DEP d'Apple que vous voulez implémenter sur les appareils inscrits auprès du programme DEP et cliquez sur **Enregistrer**.

Le serveur XenMobile s'affiche dans le portail DEP d'Apple.



Commander des appareils compatibles avec le programme DEP

Vous pouvez commander des appareils compatibles avec le programme DEP directement auprès d'Apple ou de revendeurs ou opérateurs agrées. Pour commander directement auprès d'Apple, vous devez fournir votre numéro de client Apple dans le portail DEP pour permettre à Apple d'associer l'appareil acheté avec votre compte DEP Apple.

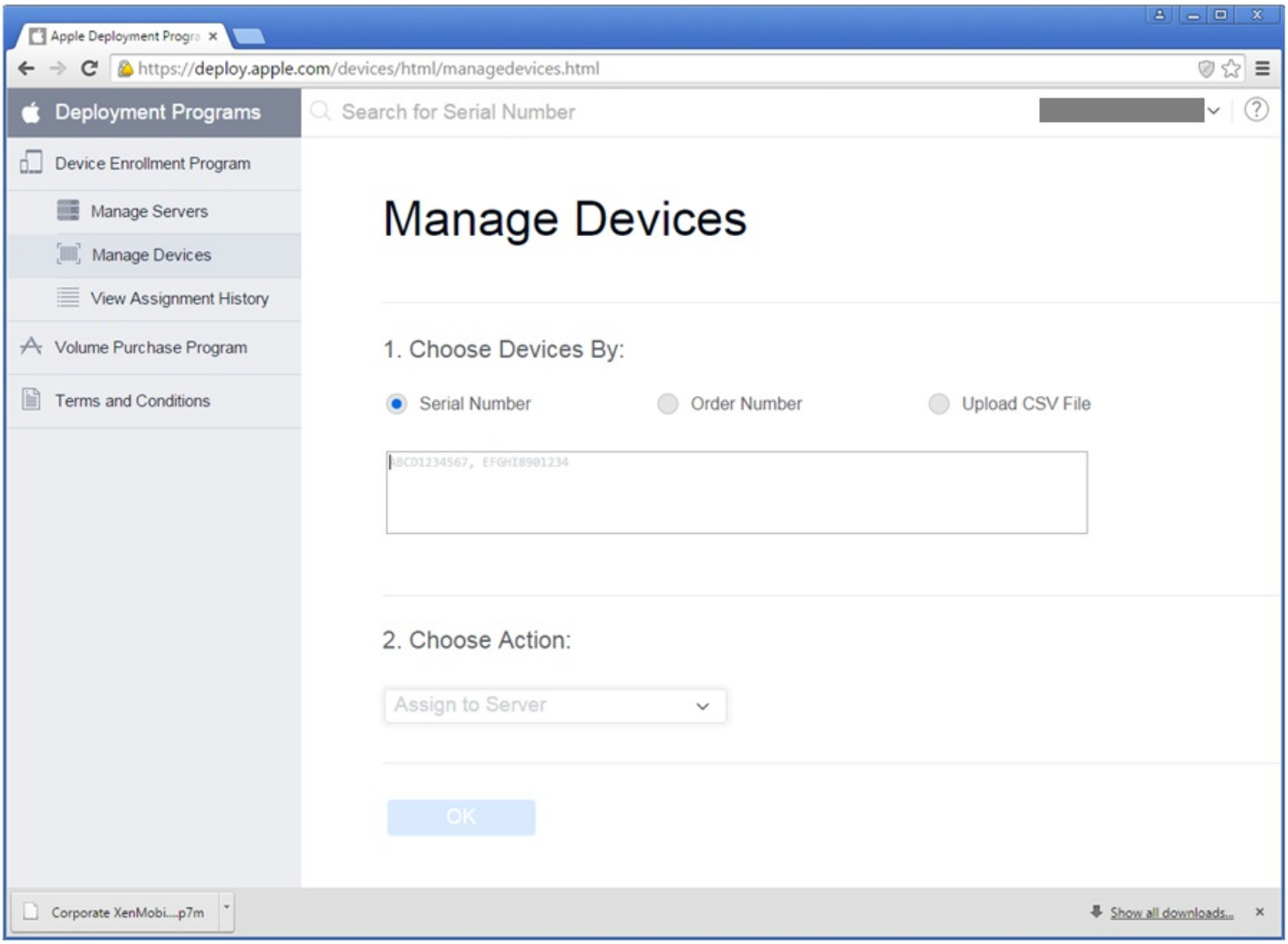
Pour commander auprès de votre revendeur ou d'un opérateur, contactez votre revendeur Apple ou opérateur pour savoir s'ils participent au programme DEP d'Apple. Lorsque vous achetez des appareils, demandez l'ID du programme DEP des revendeurs. Vous aurez besoin de ces informations pour ajouter votre revendeur DEP à votre compte Apple DEP. Une fois l'approbation obtenue, vous recevrez un ID de client DEP après avoir ajouté l'ID DEP Apple des revendeurs. Fournissez l'ID de client DEP au revendeur, qui utilisera l'ID pour soumettre les informations à propos des appareils que vous avez achetés à Apple. Pour plus d'informations, veuillez consulter ce site Web Apple.

Gestion des appareils compatibles avec le programme DEP

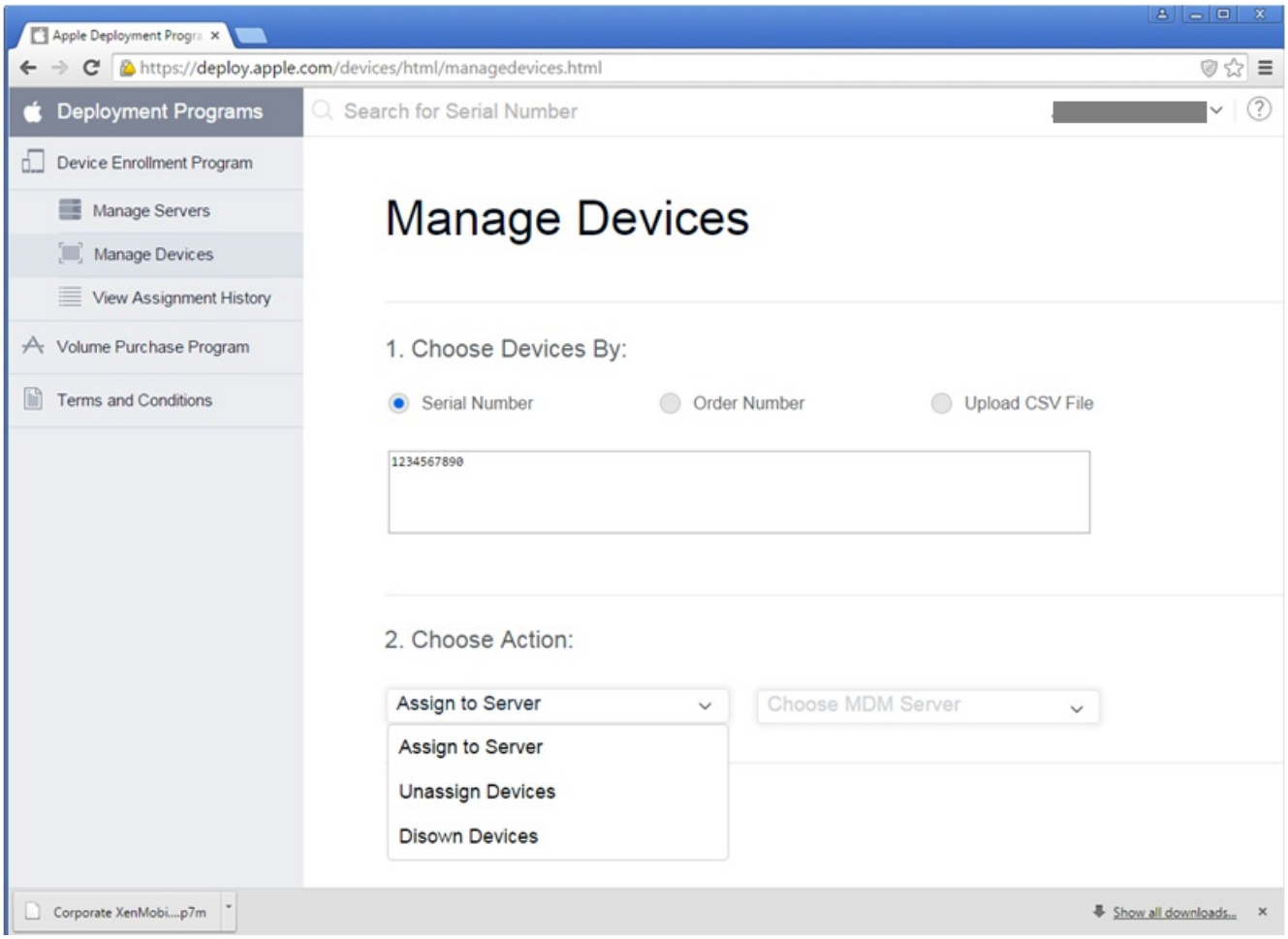
Suivez ces étapes pour associer des appareils avec votre serveur XenMobile dans votre compte Apple DEP via le portail DEP.

1. Connectez-vous au portail Apple DEP.

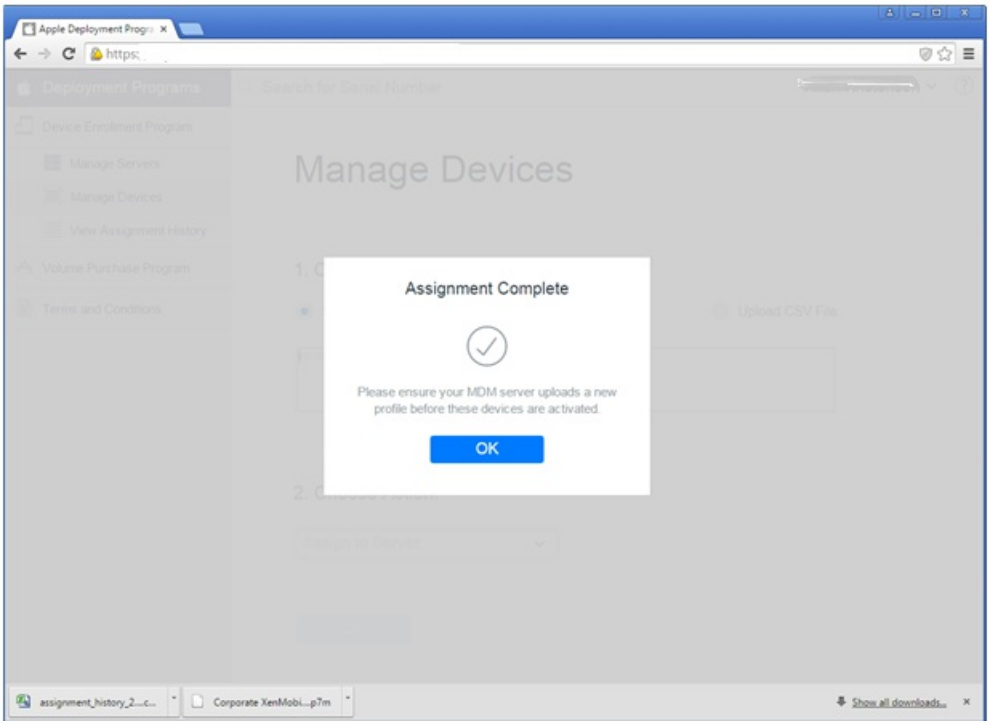
2. Cliquez sur **Programme d'inscription d'appareils**, sur **Gérer les appareils** et dans **Choisir des appareils**, sélectionnez l'option à utiliser pour charger et définir les appareils compatibles avec le programme DEP : **Numéro de série**, **Numéro de commande** ou **Télécharger un fichier CSV**.



3. Sous **Choisir une action**, pour attribuer vos appareils à un serveur XenMobile, cliquez sur **Attribuer au serveur**, et dans la liste, cliquez sur le nom de votre serveur XenMobile et cliquez sur **OK**.



Vos appareils DEP sont maintenant associés au serveur XenMobile sélectionné.



Expérience d'inscription d'appareils au programme DEP d'Apple

Lorsque les utilisateurs inscrivent un appareil au programme DEP d'Apple, ils suivent la procédure suivante.

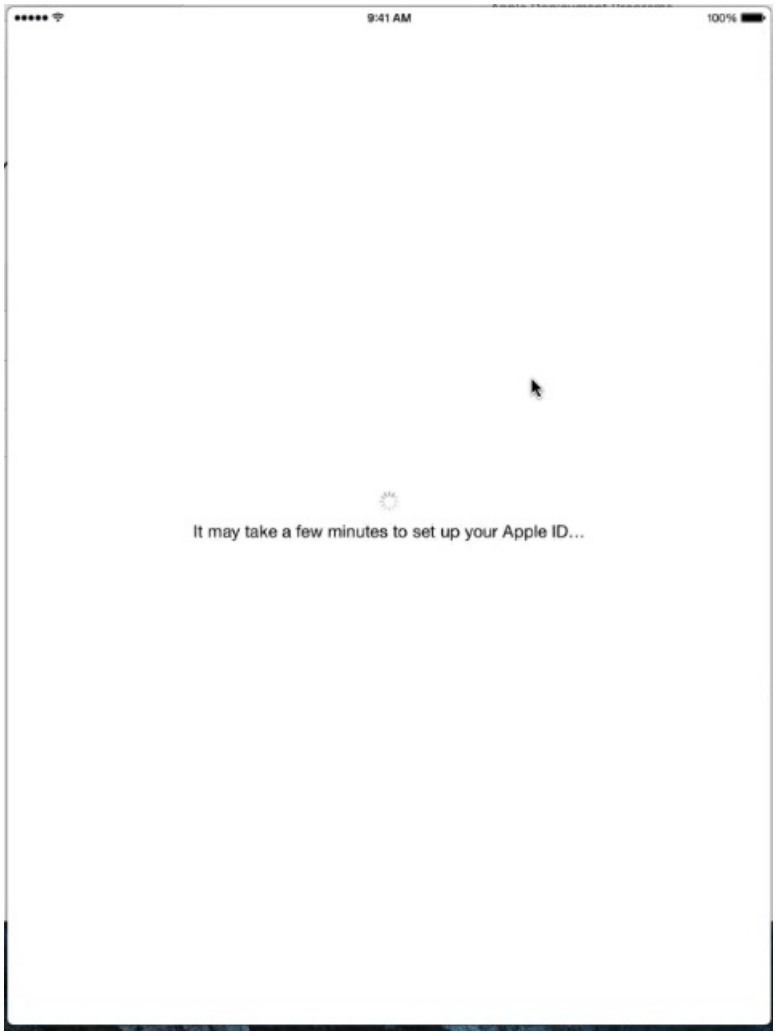
1. Ils démarrent leur appareil.

2. Ils utilisent l'assistant de configuration pour configurer les paramètres initiaux sur leur appareil iOS.

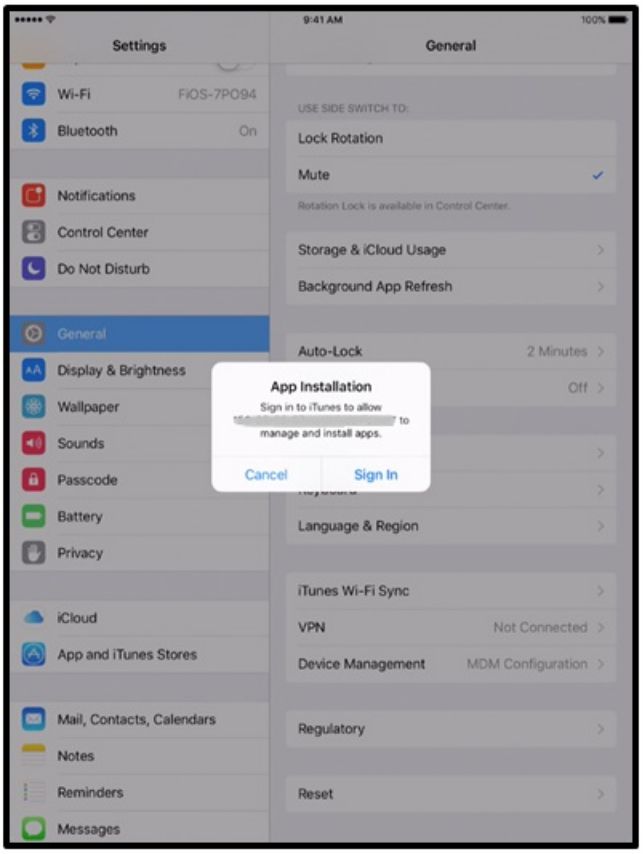
3. L'appareil démarre automatiquement le processus d'inscription d'appareils de XenMobile. Ils suivent l'assistant pour inscrire l'appareil auprès du serveur XenMobile associé à l'appareil compatible avec le programme DEP.

Le processus d'inscription auprès du programme DEP d'Apple démarre automatiquement dans le cadre du processus de configuration iOS initial des appareils compatibles avec le programme DEP.

4. La configuration DEP que vous avez configurée dans la console XenMobile est transmise à l'appareil. Les utilisateurs suivent l'assistant pour configurer l'appareil.



5. Il est possible qu'ils soient invités à se connecter à iTunes de façon à ce que Secure Hub puisse être téléchargé.



6. Les utilisateurs ouvrent Secure Hub et entrent leurs informations d'identification. Si cela est requis par la stratégie, les utilisateurs peuvent être invités à créer et vérifier un code PIN.

Le reste des applications requises est transmis à l'appareil.

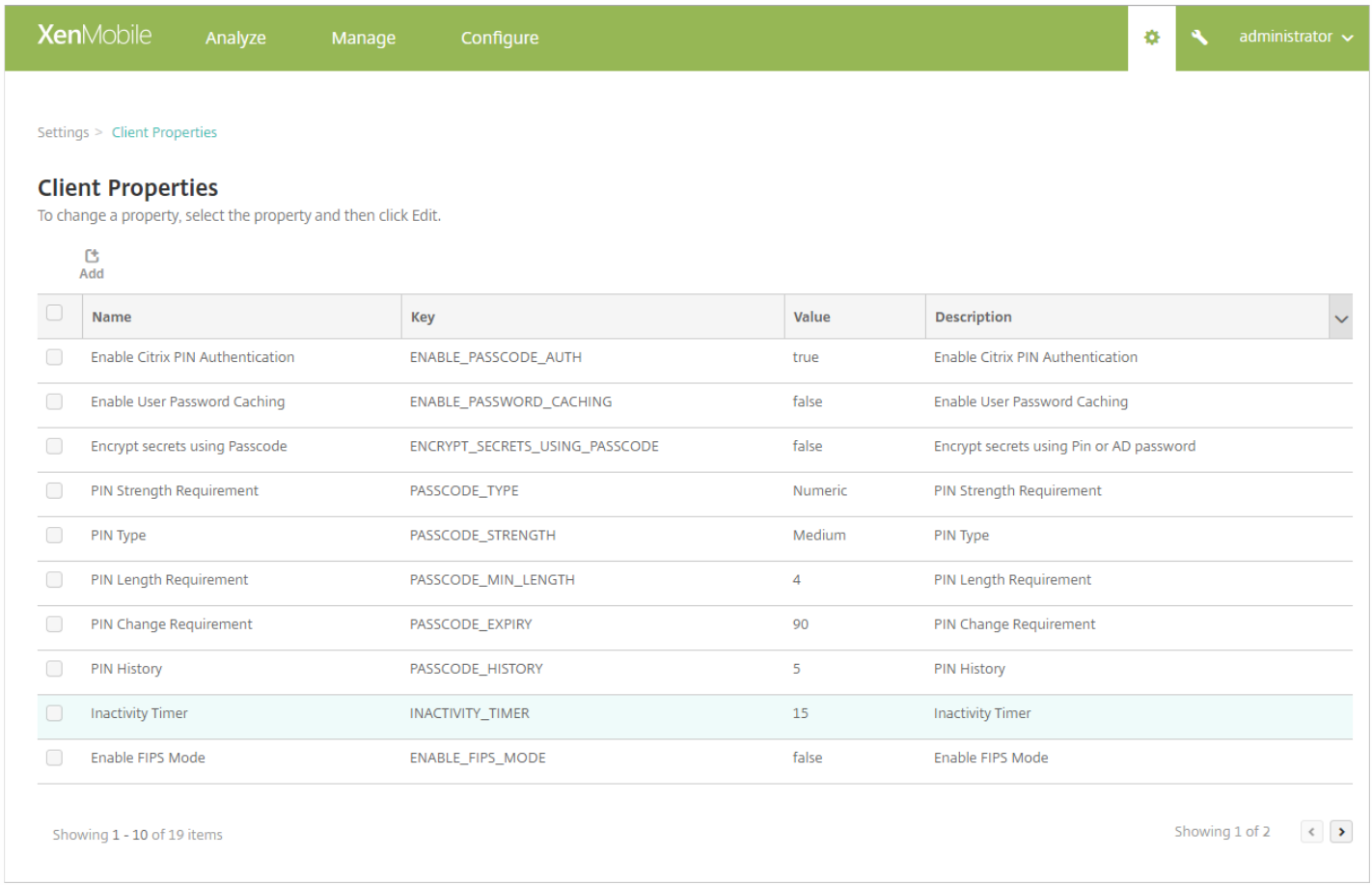
Propriétés du client

Mar 31, 2017

Les propriétés du client contiennent des informations qui sont fournies directement à Secure Hub sur les appareils des utilisateurs.Vous pouvez utiliser ces propriétés pour configurer des paramètres avancés tels que le code PIN Citrix. Vous obtenez les propriétés du client à partir du support de Citrix.

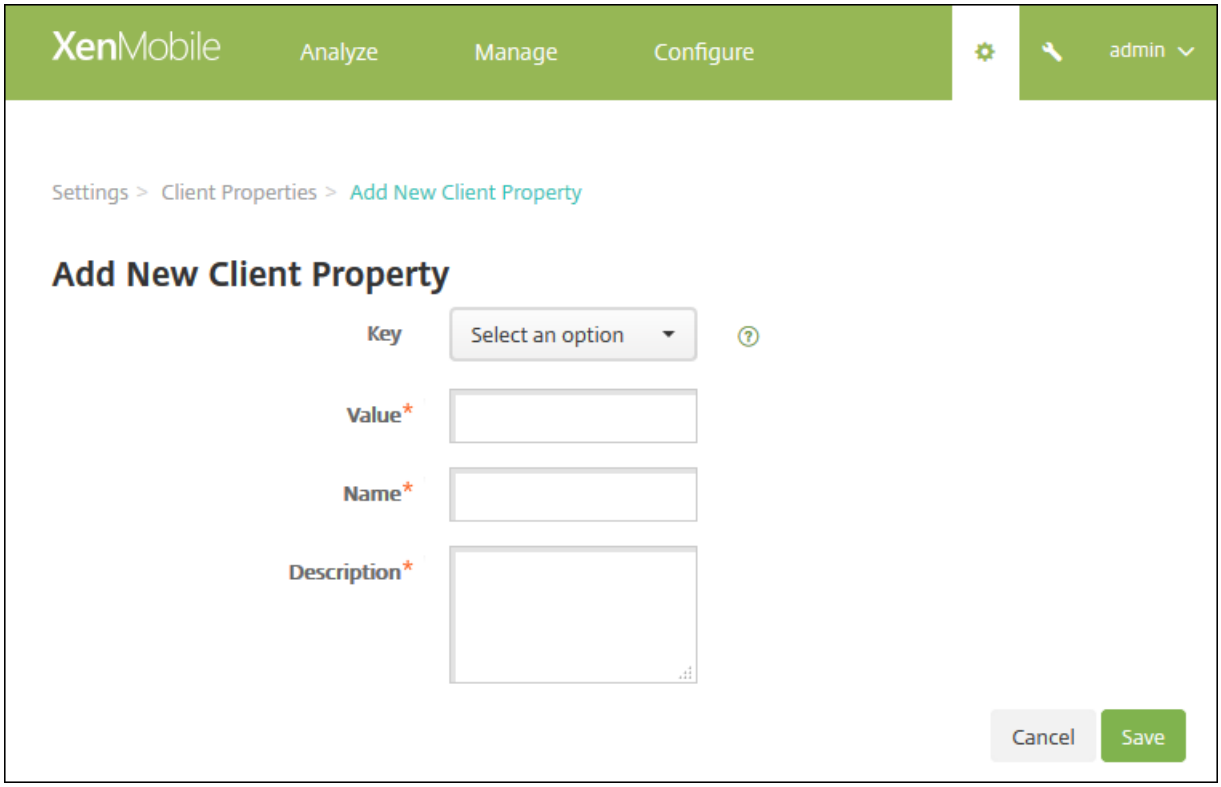
les propriétés du client sont susceptibles d'être modifiées avec chaque nouvelle version des applications clientes, et plus particulièrement Secure Hub. Pour de plus amples informations sur les propriétés du client les plus couramment configurées, consultez la section Propriété client, plus loin dans cet article.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.
2. Sous **Client**, cliquez sur **Propriétés du client**. La boîte de dialogue **Propriétés du client** s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.



Pour ajouter une propriété de client

1. Cliquez sur **Ajouter**.La page **Ajouter une nouvelle propriété de client** s'affiche.



2. Pour configurer ces paramètres :

- **Clé** : dans la liste, cliquez sur la clé de propriété que vous souhaitez ajouter.**Important** : contactez le support Citrix avant d'apporter des modifications ou pour demander une clé spéciale pour effectuer une modification.
- **Valeur** : entrez la valeur de la propriété sélectionnée.
- **Nom** : entrez un nom pour la propriété.
- **Description** : entrez une description pour la propriété.

3. Cliquez sur **Enregistrer**.

Pour modifier une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez modifier.

Remarque : lorsque vous sélectionnez la case à cocher en regard d'une propriété de client, le menu d'options s'affiche au-dessus de la liste des propriétés de client ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

2. Cliquez sur **Modifier**.La page **Modifier la propriété client** s'affiche.

3. Modifiez les informations suivantes le cas échéant :

- **Clé** : vous ne pouvez pas modifier ce champ.
- **Valeur** : valeur de la propriété.
- **Nom** : nom de la propriété.
- **Description** : description de la propriété.

4. Cliquez sur **Enregistrer** pour enregistrer vos modifications ou sur **Annuler** pour laisser la propriété inchangée.

Pour supprimer une propriété de client

1. Dans le tableau **Propriétés du client**, sélectionnez la propriété de client que vous voulez supprimer.

   Remarque : vous pouvez sélectionner plusieurs propriétés à supprimer en sélectionnant la case à cocher en regard de chaque propriété.

2. Cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Supprimer** .

Propriété client

Les propriétés client prédéfinies de XenMobile et leurs paramètres par défaut sont comme suit.

CONTAINER_SELF_DESTRUCT_PERIOD

Nom d'affichage : MDX Container Self Destruct Period (Période d'auto-destruction du conteneur MDX)

La fonction d'auto-destruction empêche l'accès à Secure Hub et aux applications gérées, après un certain nombre de jours d'inactivité. Après ce délai, les applications ne sont plus utilisables et l'utilisateur de l'appareil est désinscrit du serveur XenMobile. L'effacement des données inclut la suppression des données d'application pour chaque application installée, y compris le cache et les données d'utilisateur de l'application. Le délai d'inactivité correspond à une période de temps spécifique pendant laquelle le serveur ne reçoit pas de demande d'authentification pour valider l'utilisateur. Par exemple, si vous définissez un délai de 30 jours pour la stratégie et que l'utilisateur n'utilise pas Secure Hub ou d'autres applications pendant plus de 30 jours, la stratégie s'applique.

Cette stratégie de sécurité globale s'applique aux plates-formes iOS et Android et représente une amélioration des stratégies d'effacement et de verrouillage d'application existantes.

Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, puis ajoutez la clé personnalisée **CONTAINER_SELF_DESTRUCT_PERIOD**.

Valeur : nombre de jours.

DEVICE_LOGS_TO_IT_HELP_DESK

Nom d'affichage : Send device logs to IT help desk (Envoyer les journaux de l'appareil au service d'assistance

Cette propriété active ou désactive la possibilité d'envoyer des journaux au service d'assistance informatique.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

DISABLE_LOGGING

Nom d'affichage : Disable Logging (Désactiver la journalisation)

Cette propriété vous permet de désactiver la possibilité pour les utilisateurs de collecter et de télécharger des journaux à partir de leurs appareils. La journalisation est désactivée pour Secure Hub et pour toutes les applications MDX installées. Les utilisateurs ne peuvent pas envoyer de journaux d'application à partir de la page Support ; bien que la boîte de dialogue de composition d'un message s'affiche, les journaux ne sont pas joints et un message indique que la journalisation est désactivée. Outre l'incidence de cette clé sur les appareils des utilisateurs, vous ne pouvez pas modifier les paramètres de journal dans la console XenMobile pour les applications Secure Hub et MDX.

Lorsque cette clé est définie sur **true**, Secure Hub définit la stratégie **Bloquer les journaux d'application** sur **true** afin que les applications MDX arrêtent la journalisation lorsque la nouvelle stratégie est appliquée.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false** (la journalisation n'est pas désactivée)

ENABLE_CRASH_REPORTING

Nom d'affichage : Enable Crash Reporting (Activer les rapports de plantage)

Cette propriété active ou désactive les rapports de plantage à l'aide de Crashlytics pour les applications XenMobile.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **true**

ENABLE_FIPS_MODE

Nom d'affichage : Enable FIPS Mode (Activer le mode FIPS)

Cette propriété active ou désactive le mode FIPS sur les appareils mobiles. Lorsque vous modifiez la valeur, Secure Hub transmet la nouvelle valeur à l'appareil lors de la prochaine authentification en ligne.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

ENABLE_NETWORK_EXTENSION

Nom d'affichage : ENABLE_NETWORK_EXTENSION

Par défaut, XenMobile active l'infrastructure d'extension de réseau d'Apple durant l'installation de Secure Hub. Pour désactiver l'extension de réseau, accédez à **Paramètres > Propriétés du Client** , ajoutez la clé personnalisée **ENABLE_NETWORK_EXTENSION** et définissez la **valeur** sur **false**.

Valeur par défaut : **true**

ENABLE_PASSCODE_AUTH

Nom d'affichage : Enable Citrix PIN Authentication (Activer l'authentification du code PIN Citrix)

Cette propriété permet d'activer la fonctionnalité de code PIN Citrix. Avec le code PIN ou code secret Citrix, les utilisateurs sont invités à définir un code PIN à utiliser à la place de leur mot de passe Active Directory. Ce paramètre est automatiquement activé si ENABLE_PASSWORD_CACHING est activé ou si XenMobile utilise l'authentification par certificat.

Si les utilisateurs s'authentifient en mode hors connexion, le code PIN Citrix est validé localement et les utilisateurs sont autorisés à accéder à l'application ou au contenu demandé. Si les utilisateurs s'authentifient en ligne, le code PIN ou code secret Citrix est utilisé pour déverrouiller le mot de passe Active Directory ou le certificat qui est ensuite envoyé à des fins d'authentification auprès de XenMobile.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

ENABLE_PASSWORD_CACHING

Nom d'affichage : Enable User Password Caching (Activer la mise en cache du mot de passe de l'utilisateur)

Cette propriété vous permet d'autoriser la mise en cache locale du mot de passe Active Directory de l'utilisateur sur l'appareil mobile. Lorsque vous définissez cette propriété sur **true**, vous devez également définir la propriété ENABLE_PASSCODE_AUTH sur **true**. Lorsque la mise en cache du mot de passe de l'utilisateur est activée, les utilisateurs sont invités à créer un code PIN ou code secret Citrix.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

ENABLE_TOUCH_ID_AUTH

Nom d'affichage : Enable Touch ID Authentication (Activer l'authentification TouchID)

Pour les appareils qui prennent en charge l'authentification Touch ID, cette propriété active ou désactive l'authentification Touch ID sur l'appareil. Configuration requise :

Le code PIN Citrix ou l'authentification LDAP doivent être activés sur les appareils utilisateur. Si l'authentification LDAP est désactivée (par exemple, car seule l'authentification basée sur certificat est utilisée), les utilisateurs doivent définir un code PIN Citrix. Dans ce cas, XenMobile nécessite le code PIN Citrix même si **ENABLE_PASSCODE_AUTH** est défini sur **false**.

Définissez **ENABLE_PASSCODE_AUTH** sur **false** de façon à ce que lorsque les utilisateurs lancent une application, ils soient invités à utiliser Touch ID.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

ENABLE_WORXHOME_CEIP

Nom d'affichage : Enable Worx Home CEIP (Activer le programme CEIP de Worx Home)

Cette propriété active le Programme d'amélioration de l'expérience utilisateur. Ce dernier va envoyer périodiquement des données de configuration et d'utilisation anonymes à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de XenMobile.

Valeur : **true** ou **false**

Valeur par défaut : **false**

ENABLE_WORXHOME_GA

Nom d'affichage : Enable Google Analytics in Worx Home (Activer Google Analytics dans Worx Home)

Cette propriété active ou désactive la possibilité de collecter des données à l'aide de Google Analytics dans Worx Home. Lorsque vous modifiez ce paramètre, la nouvelle valeur est appliquée la prochaine fois que l'utilisateur se connecte à Secure Hub (Worx Home).

Valeurs possibles : **true** ou **false**

Valeur par défaut : **true**

ENCRYPT_SECRETS_USING_PASSCODE

Nom d'affichage : Encrypt secrets using Passcode (Chiffrer les secrets à l'aide d'un code secret)

Cette propriété permet de stocker les données sensibles sur l'appareil mobile dans un coffre sécurisé plutôt que dans un magasin natif basé sur la plate-forme, tel que le trousseau iOS. Cette propriété de configuration permet un cryptage renforcé des artefacts clés, mais ajoute également une entropie utilisateur (un code PIN généré de manière aléatoire connu uniquement de l'utilisateur).

Citrix vous recommande d'activer cette propriété de manière à fournir une sécurité plus élevée sur les appareils des utilisateurs. Par conséquent, les utilisateurs seront invités plus fréquemment à entrer le code PIN Citrix.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **false**

INACTIVITY_TIMER

Nom d'affichage : Inactivity Timer (Délai d'inactivité)

Cette propriété définit la durée en minutes pendant laquelle les utilisateurs peuvent laisser leurs appareils inactifs et accéder à une application sans être invité à entrer un code PIN ou code secret Citrix. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre Code secret d'application sur Activé. Si le paramètre Code secret

d'application est défini sur Désactivé, les utilisateurs sont redirigés vers Secure Hub pour effectuer une authentification complète. Lorsque vous modifiez ce paramètre, la valeur prend effet la prochaine fois que les utilisateurs sont invités à s'authentifier.

Remarque : sur iOS, le délai d'inactivité gère également l'accès des applications MDX et non MDX à Secure Hub.

Valeurs possibles : tout entier positif

Valeur par défaut : **15**

ON_FAILURE_USE_EMAIL

Nom d'affichage : On failure Use Email to Send device logs to IT help desk (En cas d'échec, utiliser la messagerie pour envoyer les journaux de l'appareil au service d'assistance)

Cette propriété active ou désactive la possibilité d'utiliser la messagerie pour envoyer les journaux de l'appareil au service informatique.

Valeurs possibles : **true** ou **false**

Valeur par défaut : **true**

PASSCODE_EXPIRY

Nom d'affichage : PIN Change Requirement (Exigences en matière de modification du code PIN)

Cette propriété définit la durée (en jours) pendant laquelle le code PIN ou code secret Citrix est valide, et après laquelle l'utilisateur est obligé de modifier son code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie uniquement lorsque le code PIN ou code secret Citrix de l'utilisateur expire.

Valeurs possibles : **1**-**99** recommandé. Si vous voulez que les utilisateurs n'aient jamais à réinitialiser leur code PIN, définissez la valeur sur un nombre très élevé (par exemple, 100 000 000 000). Si vous avez initialement défini une période d'expiration comprise entre 1 et 99 jours et que vous la modifiez au profit d'une valeur beaucoup plus élevée, les codes PIN expireront toujours à la fin de la période initiale mais plus jamais après.

Valeur par défaut : **90**

PASSCODE_HISTORY

Nom d'affichage : PIN History (Historique du code PIN)

Cette propriété définit le nombre de codes PIN ou codes secrets Citrix précédemment utilisés que les utilisateurs ne sont pas autorisés à réutiliser lorsqu'ils changent leur code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie la prochaine fois que les utilisateurs réinitialisent leur code PIN ou code secret Citrix.

Valeurs possibles : **1**-**99**

Valeur par défaut : **5**

PASSCODE_MAX_ATTEMPTS

Nom d'affichage : PIN Attempts (Nombre de tentatives de saisie du code PIN)

Cette propriété définit le nombre de tentatives de saisie infructueuses du code PIN ou code secret Citrix que les utilisateurs peuvent effectuer avant d'être invités à fournir une authentification complète. Une fois que les utilisateurs ont effectué une authentification complète, ils sont invités à créer un nouveau code PIN ou code secret Citrix.

Valeurs possibles : tout entier positif

Valeur par défaut : **15**

PASSCODE_MIN_LENGTH

Nom d'affichage : PIN Length Requirement (Exigences en matière de longueur du code PIN)

Cette propriété définit la longueur minimale des codes PIN Citrix.

Valeurs possibles : **1**-**99**

Valeur par défaut : **6**

PASSCODE_STRENGTH

Nom d'affichage : PIN Strength Requirement (Exigences en matière de sûreté du code PIN)

Cette propriété définit le niveau de sécurité du code PIN ou code secret Citrix. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : **Low**, **Medium** ou **Strong**

Valeur par défaut : **Medium**

Le tableau suivant décrit les règles de mot de passe pour chaque paramètre de sécurité en fonction du paramètre PASSCODE_TYPE :

Niveau de sécurité du code secret	**Règles pour code secret numérique**	**Règles pour code secret alphanumérique**
Faible	Sont autorisés tous les nombres et toute séquence	Doit contenir au moins un nombre et une lettre. Non autorisé : AAAaaa, aaaaaa, abcdef Autorisé : aa11b1, Abcd1 Ab123 ~#„, aa11aa aaaa11
Moyen (paramètre par défaut)	1. Ne doit contenir aucun chiffre identique. Par exemple, 444444 n'est pas autorisé. 2. Ne doit contenir aucun chiffre consécutif. Par exemple, 123456 ou 654321 n'est pas autorisé. Autorisé : 444333, 124567, 136790, 555556,	En plus des règles de sécurité pour un code secret de niveau moyen : 1. Les lettres et tous les nombres ne peuvent pas être identiques. Par exemple, aaaa11, aa11aa ou aaa111 ne sont pas autorisés. 2. Les lettres et les nombres ne peuvent pas être

	788888	consécutifs. Par exemple, abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123 ne sont pas autorisés. Autorisé : aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Élevé	Identique au niveau de sécurité moyen du code secret Citrix.	Le code secret doit contenir au moins une lettre majuscule et une lettre minuscule. Non autorisé : abcd12, DFGH2 Autorisé : Abcd12, jkrtA2, 23Bc#AbCd
Fort	Identique au niveau de sécurité moyen du code secret Citrix.	Le code secret doit contenir au moins un nombre, un symbole spécial, une lettre majuscule et une lettre minuscule. Non autorisé : abcd12, Abcd12, dfgh12, jkrtA2 Autorisé : Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#

PASSCODE_TYPE

Nom d'affichage : PIN Type (Type de code PIN)

Cette propriété définit si les utilisateurs peuvent définir un code PIN Citrix numérique ou un code secret alphanumérique. Lorsque vous sélectionnez la valeur **Numeric**, les utilisateurs peuvent uniquement utiliser des chiffres (code PIN Citrix). Lorsque vous sélectionnez la valeur **Alphanumeric**, l'utilisateur peut utiliser une combinaison de lettres et de chiffres (code secret).

Remarque : si vous modifiez ce paramètre, les utilisateurs doivent définir un nouveau code PIN ou code secret Citrix la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : **Numeric** ou **Alphanumeric**

Valeur par défaut : **Numeric**

REFRESHINTERVAL

Nom d'affichage : REFRESHINTERVAL

Par défaut, XenMobile envoie un ping au serveur de détection automatique (ADS) afin « d'épingler » les certificats tous les 3 jours. Pour modifier l'intervalle d'actualisation, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **REFRESHINTERVAL** et définissez la **valeur** sur le nombre d'heures.

Valeur par défaut : **72** heures (3 jours)

SEND_LDAP_ATTRIBUTES

Pour les déploiements MAM exclusif, vous pouvez configurer XenMobile de manière à ce que les utilisateurs d'appareils Android ou iOS qui s'inscrivent dans Secure Hub avec des informations d'identification de messagerie soient automatiquement inscrits dans Secure Mail. Cela signifie que les utilisateurs n'ont pas à entrer d'informations supplémentaires ou à effectuer des étapes supplémentaires pour s'inscrire dans Secure Mail. Vous devez également définir la propriété de serveur MAM_MACRO_SUPPORT.

Pour configurer cette stratégie globale, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **SEND_LDAP_ATTRIBUTES** et définissez la **valeur** comme suit.

Valeur : userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName=${user.displayName},mail=${user.mail}

Les valeurs d'attribut sont spécifiées en tant que macros, similaires à des stratégies MDM.

Voici un exemple de réponse de service de compte pour cette propriété :

Remarque : pour cette propriété, XenMobile traite les les virgules en tant que terminaison de chaîne. Par conséquent, si une valeur d'attribut comprend une virgule, elle doit être précédée d'une barre oblique inverse pour empêcher le client d'interpréter la virgule comme la fin de la valeur d'attribut. Représentez les barres obliques inverses par « \\ ».

ActiveSync Gateway

Feb 23, 2017

ActiveSync est un protocole de synchronisation des données mobiles développé par Microsoft. ActiveSync synchronise les données avec les périphériques portables et ordinateurs de bureau (ou portables).

Vous pouvez configurer des règles ActiveSync Gateway dans XenMobile. Basé sur ces règles, les appareils peuvent être autorisés ou non à accéder aux données ActiveSync. Par exemple, si vous activez la règle Applications requises manquantes, XenMobile vérifie la stratégie d'accès aux applications requises et refuse l'accès aux données ActiveSync si les applications requises sont manquantes. Pour chaque règle, vous avez le choix entre **Autoriser** ou **Refuser**. Le paramètre par défaut est **Autoriser**.

Pour plus d'informations sur la stratégie d'accès aux applications, consultez la section Stratégies d'accès aux applications.

XenMobile prend en charge les règles suivantes :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si XenMobile ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Échec de l'attestation Samsung KNOX : vérifie si un appareil n'est pas parvenu à répondre à une requête du serveur d'attestation Samsung KNOX.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications.

Autorisation et refus implicites : il s'agit de l'action par défaut pour ActiveSync Gateway. Elle crée une liste de tous les appareils qui ne répondent à aucun des autres critères de règle de filtre et autorise ou refuse les connexions en se basant sur cette liste. Si aucune règle ne correspond, la valeur par défaut est Autorisation implicite.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre Nombre de jours maximum d'inactivité dans la boîte de dialogue Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, XenMobile peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si XenMobile envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou un tiers tirant parti des API XenMobile.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

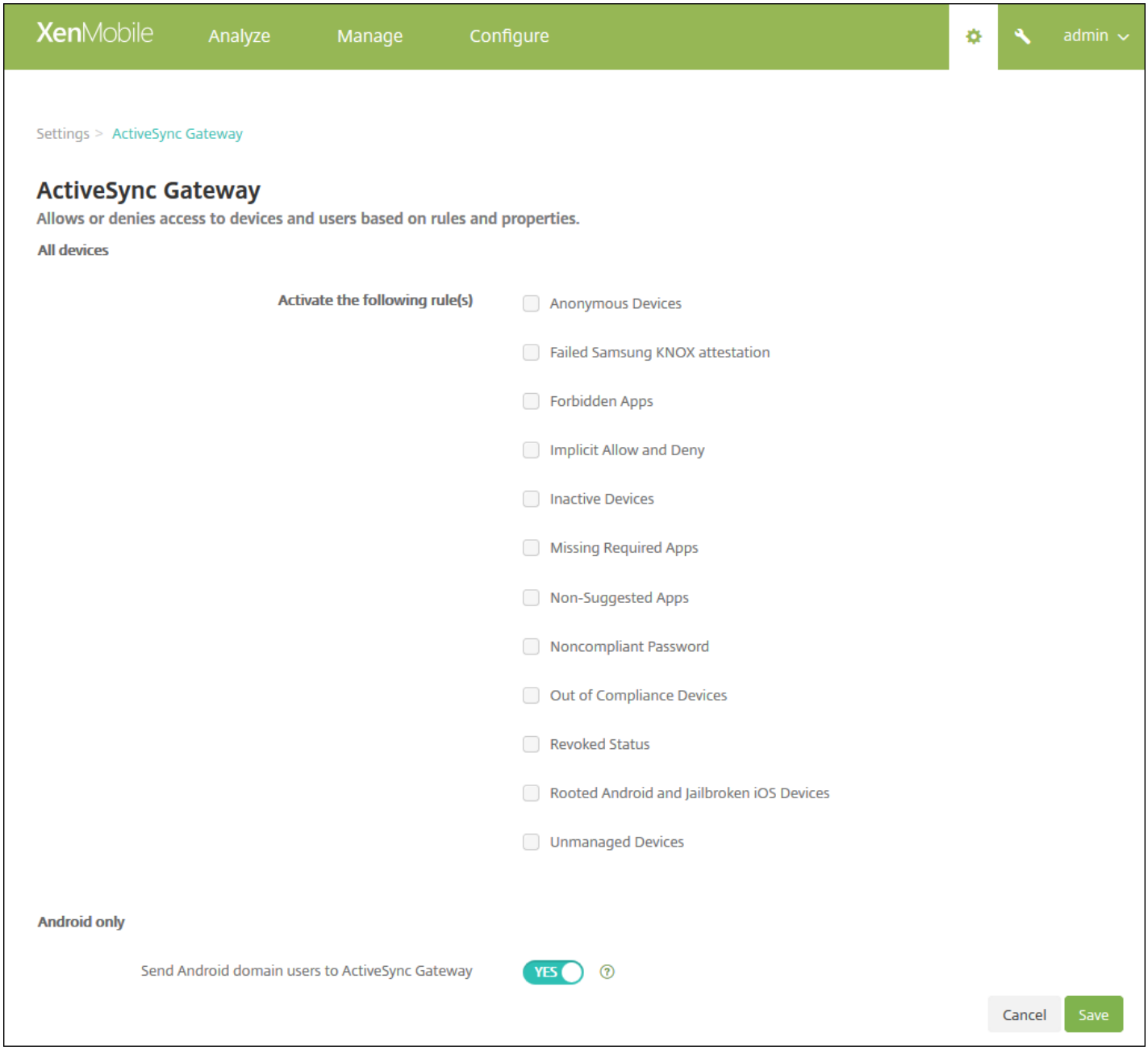
Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

Envoyer les utilisateurs Android à ActiveSync Gateway : cliquez sur **OUI** pour vous assurer que XenMobile envoie des informations de l'appareil Android à ActiveSync Gateway. Lorsque cette option est activée, elle garantit que XenMobile envoie les informations de l'appareil Android à ActiveSync Gateway au cas où XenMobile ne disposerait pas de l'identificateur ActiveSync de l'utilisateur de cet appareil Android.

Pour configurer les paramètres ActiveSync Gateway

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Serveur**, cliquez sur **ActiveSync Gateway**. La page **ActiveSync Gateway** s'affiche.



3. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.

4. Dans **Android uniquement**, sous **Envoyer les utilisateurs Android à ActiveSync Gateway**, cliquez sur **OUI** pour vous assurer que XenMobile envoie les informations de l'appareil Android à ActiveSync Gateway.

5. Cliquez sur **Enregistrer**.

Contrôle d'accès réseau

Feb 23, 2017

Si vous disposez d'un boîtier de contrôle d'accès réseau (NAC) sur votre réseau (tel qu'un réseau Cisco ISE), dans XenMobile, vous pouvez activer des filtres pour définir les appareils comme conformes ou non conformes au NAC, en vous basant sur des règles ou des propriétés. Si un appareil géré dans XenMobile ne répond pas aux critères spécifiés, et qu'il est marqué comme non conforme, le boîtier NAC bloque l'appareil sur votre réseau.

Dans la console XenMobile, sélectionnez les critères dans la liste en fonction desquels un appareil est jugé comme non conforme.

XenMobile prend en charge les filtres de conformité au contrôle d'accès réseau (NAC) suivants :

Appareils anonymes : vérifie si un appareil est en mode anonyme. Cette vérification est disponible si XenMobile ne parvient pas à authentifier à nouveau l'utilisateur lorsqu'un appareil tente de se reconnecter.

Échec de l'attestation Samsung KNOX : vérifie si un appareil n'est pas parvenu à répondre à une requête du serveur d'attestation Samsung KNOX.

Applications sur liste noire : vérifie si un appareil dispose d'applications interdites, telles que définies dans une stratégie d'accès aux applications. Pour plus d'informations sur la stratégie d'accès aux applications, consultez la section Stratégies d'accès aux applications.

Appareils inactifs : vérifie si un appareil est inactif, tel que cela est défini par le paramètre Nombre de jours maximum d'inactivité dans la boîte de dialogue Propriétés du serveur. Pour de plus amples informations, consultez la section Propriétés du serveur.

Applications requises manquantes : vérifie si des applications nécessaires sont manquantes sur un appareil, tel que cela est défini dans une stratégie d'accès aux applications.

Applications non suggérées : vérifie si un appareil dispose d'applications non suggérées, telles que définies dans une stratégie d'accès aux applications.

Mot de passe non conforme : vérifie si le mot de passe utilisateur est conforme. Sur les appareils iOS et Android, XenMobile peut déterminer si le mot de passe actuel de l'appareil est conforme à la stratégie de code secret envoyée à l'appareil. Par exemple, sur iOS, l'utilisateur dispose de 60 minutes pour définir un mot de passe si XenMobile envoie une stratégie de code secret à l'appareil. Avant qu'un mot de passe ne soit défini par l'utilisateur, le code secret peut ne pas être conforme.

Appareils non conformes : vérifie si un appareil n'est pas conforme, en fonction de la propriété de l'appareil Non conforme. Cette propriété est généralement modifiée par les actions automatisées ou parce qu'un tiers utilise les API XenMobile.

État révoqué : vérifie si le certificat de l'appareil a été révoqué. Un appareil révoqué ne peut pas se réinscrire tant qu'il n'a pas été à nouveau autorisé.

Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

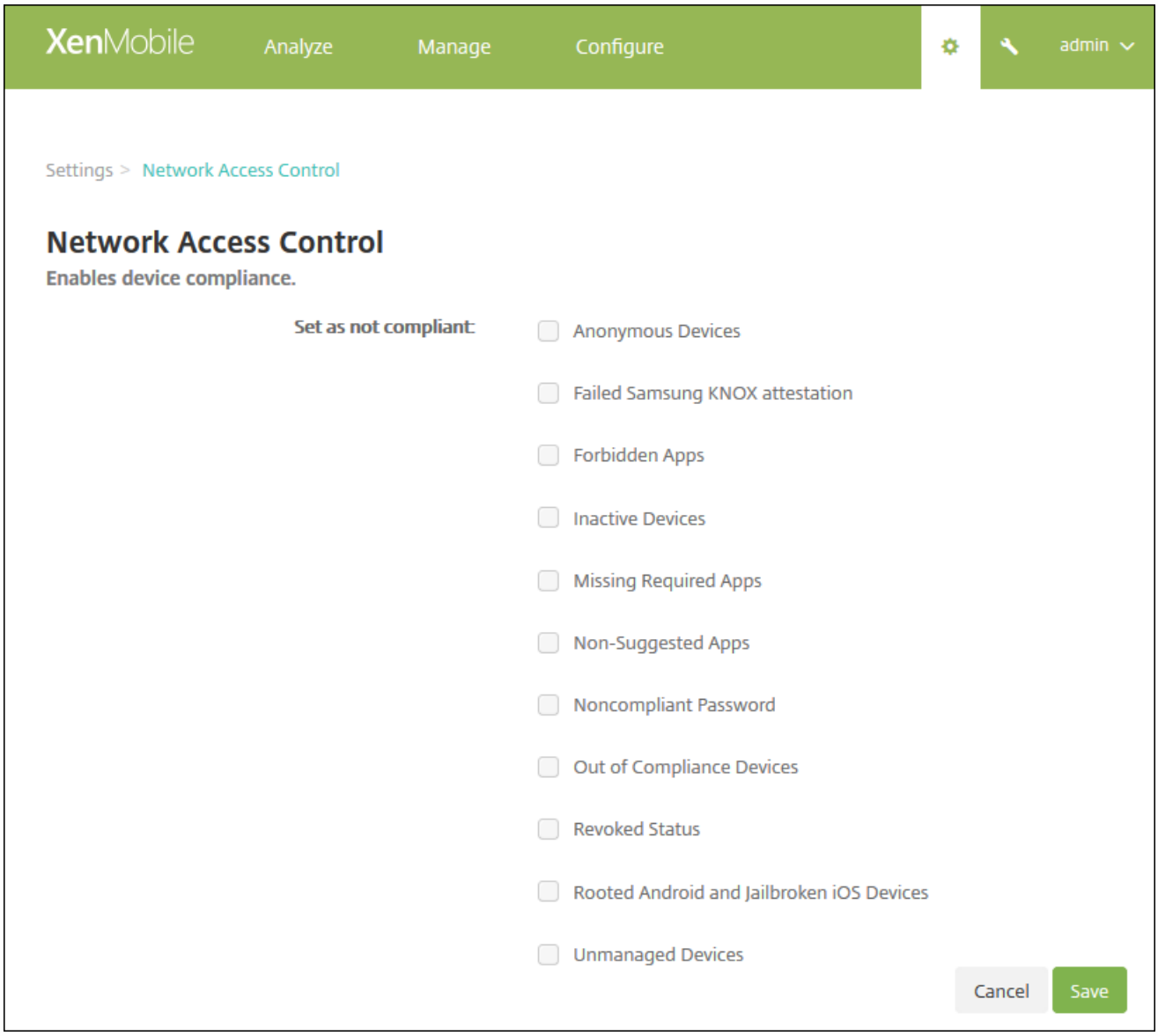
Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

> **Remarque**
>
> le filtre Conformité/non conformité implicite définit la valeur par défaut uniquement sur les appareils qui sont gérés par XenMobile. Par exemple, les appareils sur lesquels une application en liste noire est installée ou qui ne sont pas inscrits sont marqués comme Non conformes et seront bloqués sur votre réseau par le boîtier NAC.

Configurer le contrôle d'accès réseau

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Dans **Serveur**, cliquez sur **Contrôle d'accès réseau**. La page **Contrôle d'accès réseau** s'affiche.



3. Cochez les cases correspondant aux filtres **Définir comme non conforme** que vous souhaitez activer.

4. Cliquez sur **Enregistrer**.

Samsung KNOX

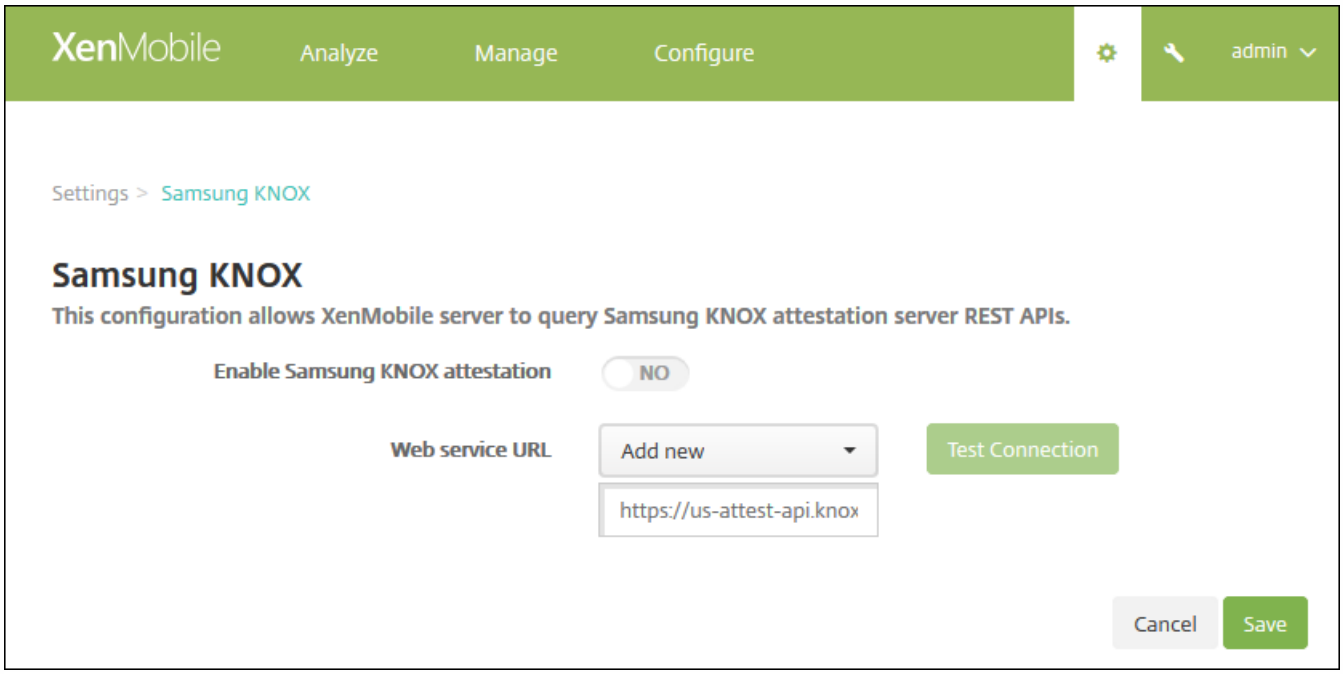
Feb 23, 2017

Vous pouvez configurer XenMobile pour interroger les API REST du serveur d'attestation Samsung KNOX.

Samsung KNOX tire profit des capacités de sécurité du matériel qui fournissent différents niveaux de protection pour le système d'exploitation et les applications. L'un des niveaux de cette sécurité réside sur la plate-forme via l'attestation. Un serveur d'attestation permet de vérifier les logiciels du système de base de l'appareil mobile (par exemple, les chargeurs de démarrage et le noyau) au moment de l'exécution en fonction des données collectées au cours du démarrage sécurisé.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Plates-formes**, cliquez sur **Samsung KNOX**. La page **Samsung KNOX** s'affiche.



3. Dans **Activer la certification Samsung KNOX**, sélectionnez si vous souhaitez activer la certification Samsung KNOX. La valeur par défaut est **NON**.

4. Lorsque vous définissez **Activer la certification Samsung KNOX** sur **OUI**, l'option **URL du service Web** est activée. Ensuite, dans la liste, procédez comme suit :

   a. Cliquez sur le serveur d'attestation approprié.

   b. Cliquez sur **Ajouter** et entrez l'URL du service Web.

5. Cliquez sur **Tester la connexion** pour vérifier la connexion. Un message de réussite ou d'échec s'affiche.

6. Cliquez sur **Enregistrer**.

Remarque

Vous pouvez utiliser Samsung KNOX Mobile Enrollment pour inscrire plusieurs appareils Samsung KNOX dans XenMobile (ou toute solution de gestion de la flotte mobile) sans avoir à configurer manuellement chaque appareil. Pour de plus amples informations, consultez la section Inscription en bloc Samsung KNOX.

Google Cloud Messaging

Mar 31, 2017

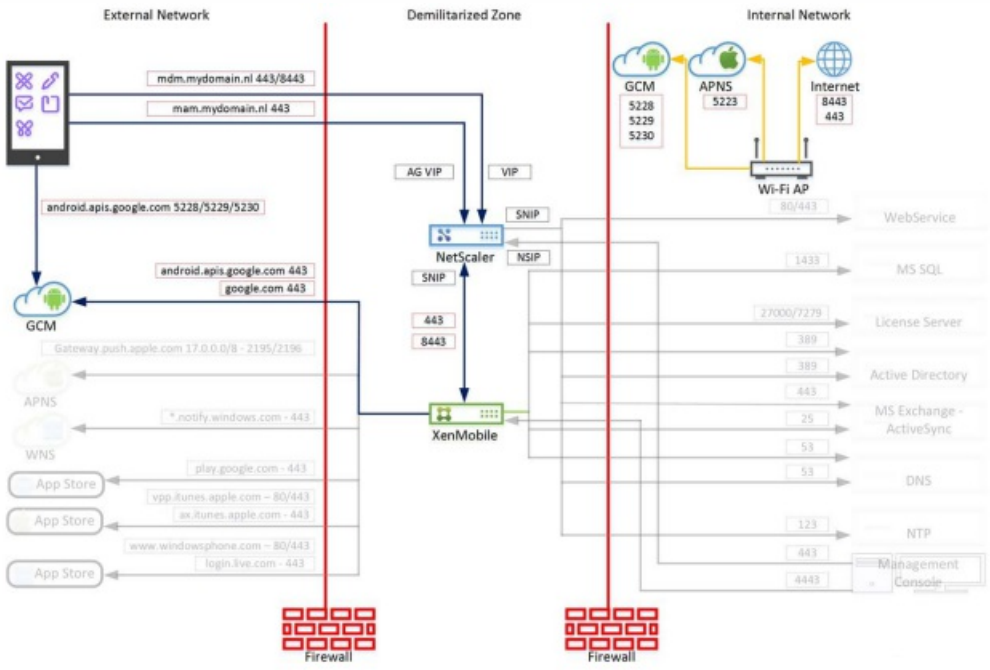
En tant qu'alternative à la stratégie **Période d'interrogation active**, vous pouvez utiliser Firebase Cloud Messaging (FCM) pour contrôler quand et comment les appareils Android se connectent à XenMobile. En utilisant la configuration suivante, toute action de sécurité ou commande de déploiement déclenche une notification push à Secure Hub afin d'inviter l'utilisateur à se reconnecter au serveur XenMobile.

Conditions préalables

- XenMobile 10.3.x
- Dernier client Secure Hub
- Informations d'identification du compte Google Developer
- Ouvrez le port 443 sur XenMobile pour Android.apis.google.com et Google.com

Architecture

Ce diagramme illustre le flux de communication pour FCM dans le réseau interne et externe.

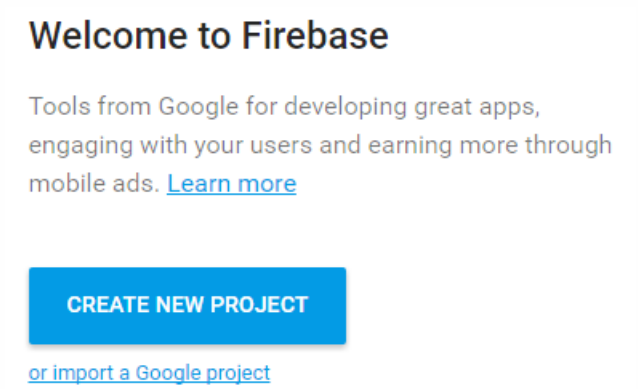


Pour configurer votre compte Google pour FCM

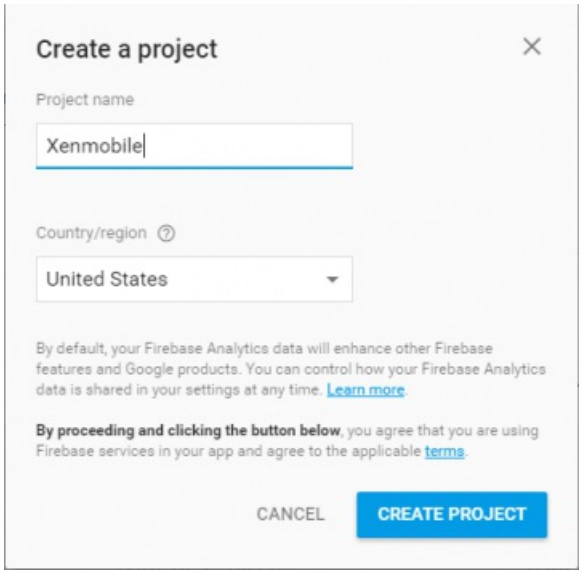
1. Connectez-vous à l'adresse URL suivante à l'aide des informations d'identification de votre compte Google Developer :

   https://console.firebase.google.com/?pli=1

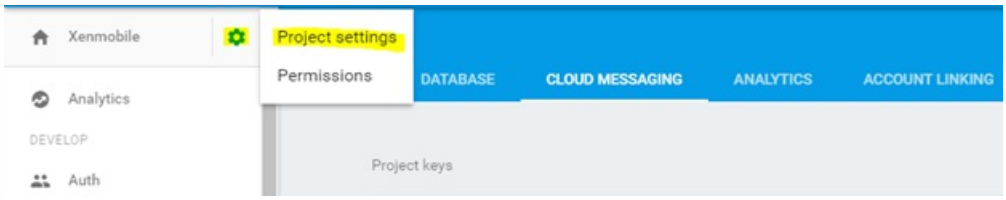
2. Cliquez sur **Créer un projet**.



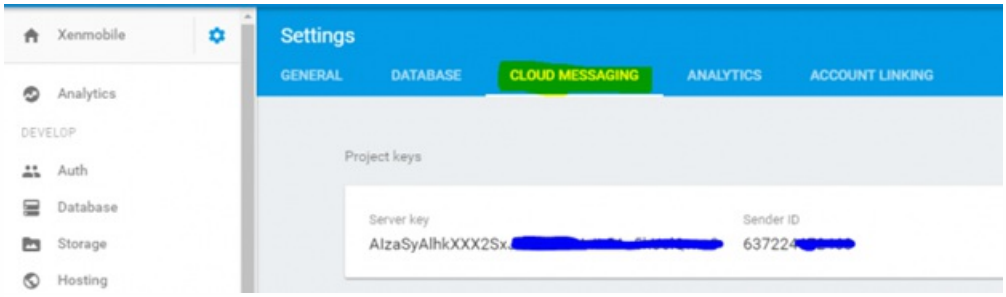
3. Entrez un **nom de projet** et cliquez sur **Créer un projet**.



4. Cliquez sur l'icône d'engrenage en regard du nom de votre projet dans le coin supérieur gauche et cliquez sur **Paramètres du projet**.



5. Sélectionnez l'onglet **Cloud Messaging**. Vous trouverez votre ID de l'expéditeur et la clé de serveur sur cette page. Copiez ces valeurs car vous devez les entrer dans le serveur XenMobile. Il est important de noter que les clés de serveur créées après septembre 2016 doivent être créées dans la console Firebase.

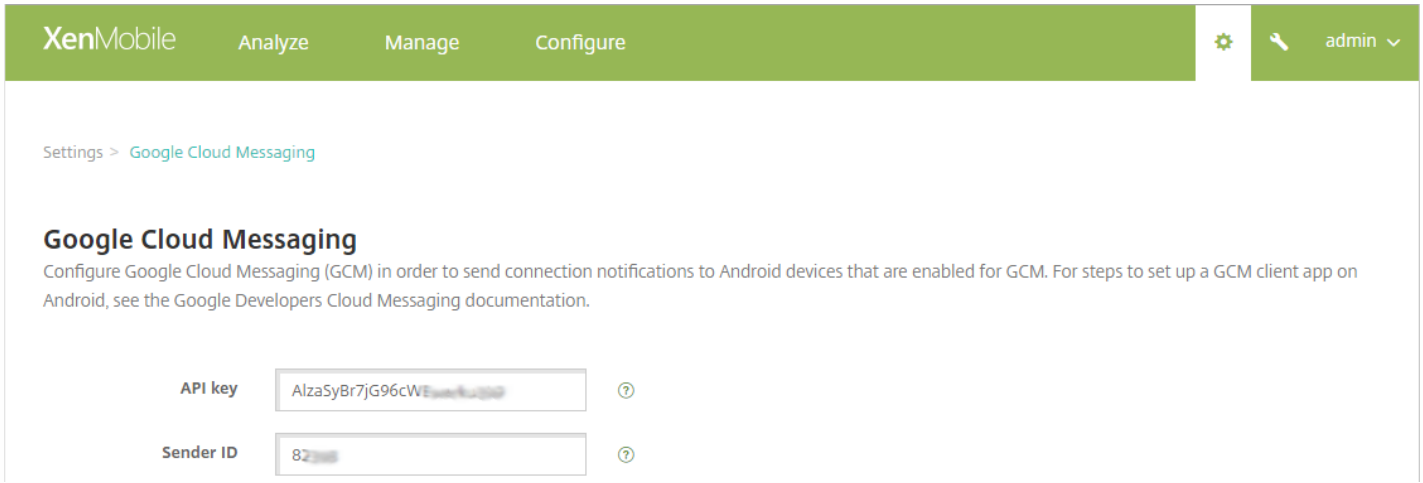


Pour configurer XenMobile pour GCM

1. Connectez-vous à la console XenMobile et cliquez sur **Paramètres > Propriétés du serveur**. Dans la barre de recherche, tapez **GCM** et cliquez sur Rechercher.

    a. Modifiez la **clé API GCM** et entrez la clé API de Firebase Cloud Messaging que vous avez copiée dans la dernière étape de configuration de Firebase Cloud Messaging.

    b. Modifiez l'**ID de l'expéditeur GCM** et copiez la valeur de l'ID de l'expéditeur dont vous avez pris note dans la procédure précédente.



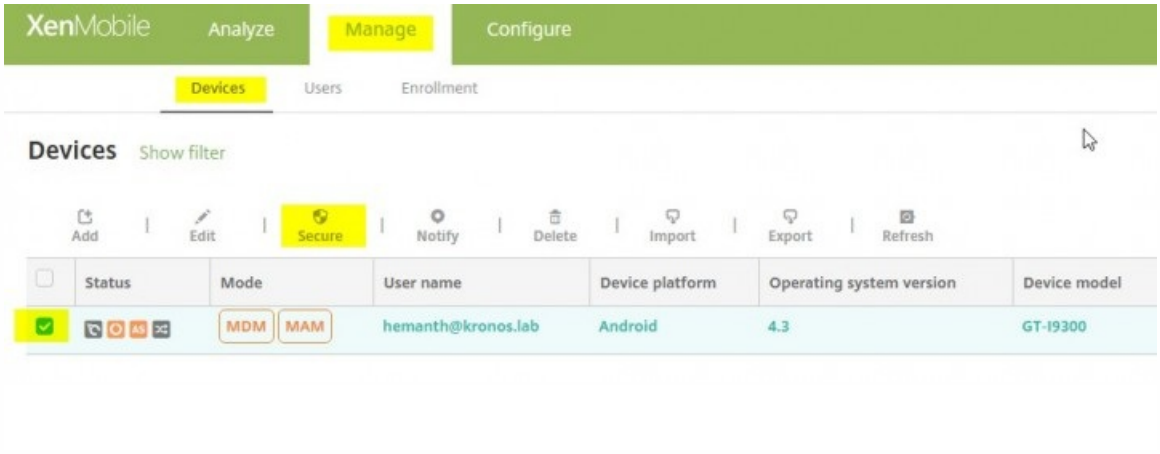
Pour tester votre configuration

Avant de commencer à tester votre configuration FCM, assurez-vous qu'aucune stratégie de **planification** n'est configurée. Alternativement, ne définissez pas la stratégie sur **Toujours connecter**. Pour plus d'informations sur la configuration de **planification**, consultez la section Stratégie de planification.

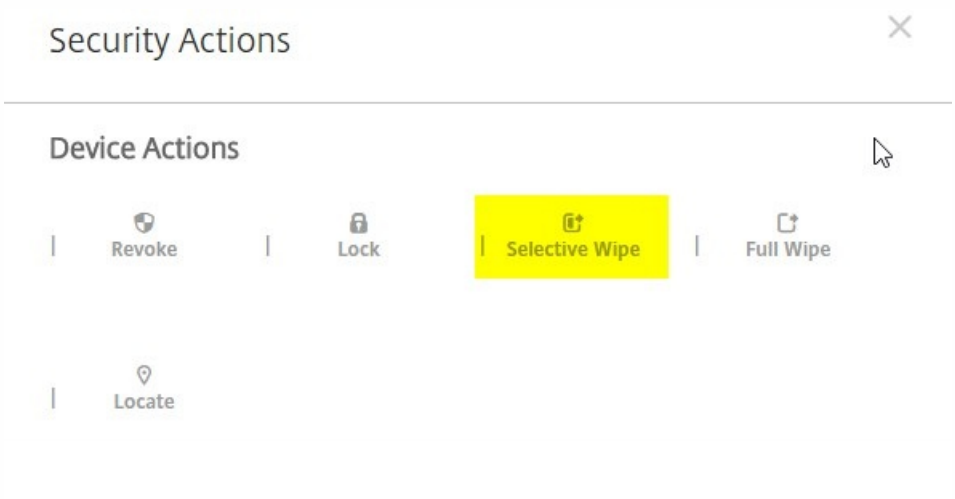
1. Inscrivez un appareil Android.

2. Laissez l'appareil inactif pendant un certain temps, de façon à ce qu'il se déconnecte du serveur XenMobile.

3. Connectez-vous à la console XenMobile, cliquez sur **Gérer**, sélectionnez l'appareil Android, puis cliquez sur **Sécurisé**.



4. Sous **Actions de l'appareil**, cliquez sur **Effacer les données d'entreprise**.



Dans une configuration effectuée avec succès, l'effacement des données d'entreprise a lieu sur l'appareil.

Identifiants Google Play

Feb 23, 2017

XenMobile utilise les informations d'identification Google Play pour extraire les informations applicatives pour l'appareil.

Pour trouver votre ID Android, entrez *#*#8255#*#*sur votre téléphone. Si le code ne révèle pas l'ID de l'appareil sur votre type d'appareil, il est possible d'utiliser une application tierce d'ID d'appareil pour obtenir l'ID d'appareil. L'ID que vous devez obtenir est l'ID Google Services Framework portant le label GSF ID.

Remarque

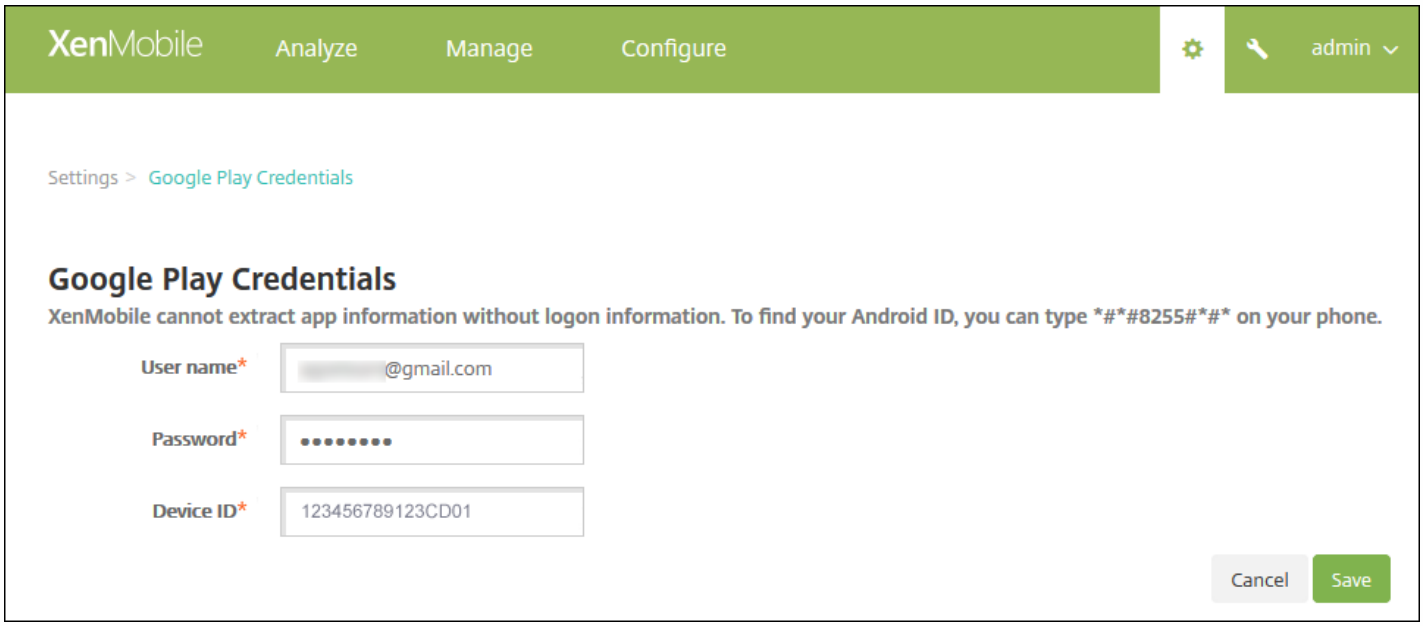
Lors d'une recherche d'application dans Google Play Store à partir de la console XenMobile, la recherche renvoie les applications basées sur le système d'exploitation Android de l'appareil. Prenons le cas d'un Samsung S6 Edge exécutant un système d'exploitation 6.0.1. Lorsque vous recherchez des applications, les seules applications qui s'affichent dans les résultats de la recherche sont des applications qui sont compatibles avec Android version 6.0.1.

Important

Pour permettre à XenMobile d'extraire les informations de l'application, vous devrez peut-être configurer votre compte Gmail pour autoriser les connexions non sécurisées. Pour obtenir des instructions détaillées, consultez le site de support de Google.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Plates-formes**, cliquez sur **Identifiants Google Play**. La page Identifiants Google Play s'affiche.



3. Configurez les paramètres suivants :

- Dans **Nom d'utilisateur**, entrez le nom associé au compte Google Play.
- **Mot de passe** : entrez le mot de passe de l'utilisateur.
- **ID de l'appareil** : entrez votre ID Android.
  Reportez-vous à la remarque plus haut dans l'article pour obtenir des instructions détaillées sur l'obtention de votre ID Android.

3. Cliquez sur **Enregistrer**.

Stratégies d'appareil

Mar 31, 2017

Vous pouvez configurer la façon dont XenMobile fonctionne avec vos appareils en créant des stratégies. Bien que la plupart des stratégies soient communes à tous les appareils, chaque appareil dispose de stratégies spécifiques à son système d'exploitation. Par conséquent, vous pouvez constater des différences entre les plates-formes et même entre différents fournisseurs d'appareils exécutant Android. Pour accéder aux stratégies par plate-forme, téléchargez le PDF de Matrice des stratégies applicatives par plate-forme.

Avant de créer une nouvelle stratégie, vous devez effectuer les étapes suivantes :

- Créer les groupes de mise à disposition que vous voulez utiliser.
- Installer les certificats d'autorité de certification nécessaires.

Les étapes de base pour créer une stratégie sont les suivantes :

1. Fournissez un nom et une description pour la stratégie.
2. Configurez une ou plusieurs plates-formes.
3. Créez des règles de déploiement (facultatif).
4. Attribuez la stratégie à des groupes de mise à disposition.
5. Configurez le calendrier de déploiement (facultatif).

Vous pouvez configurer les stratégies d'appareil suivantes dans XenMobile.

Nom de la stratégie d'appareil	**Description de la stratégie d'appareil**
Mise en miroir AirPlay	Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des appareils AirPlay spécifiques (tels que Apple TV ou un autre ordinateur Mac) aux appareils iOS des utilisateurs. Vous avez aussi la possibilité d'ajouter des appareils à une liste blanche d'appareils supervisés, ce qui limite l'accès des utilisateurs uniquement aux appareils AirPlay figurant sur la liste blanche.
AirPrint	Une stratégie AirPrint vous permet d'ajouter des imprimantes AirPrint à la liste des imprimantes AirPrint sur les appareils iOS des utilisateurs. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents. Remarque : • Cette stratégie s'applique à iOS 7.0 et versions supérieures. • Vérifiez que vous disposez de l'adresse IP et du chemin d'accès à la ressource pour chaque imprimante.
Restrictions applicatives Android	Cette stratégie vous permet de modifier les restrictions associées aux applications Android for Work, mais vous devez avant cela effectuer les actions suivantes :

for Work	• Effectuer les tâches de configuration d'Android for Work sur Google. Pour de plus amples informations, consultez la section Gestion des appareils avec Android for Work. • Créer un compte Android for Work. Pour de plus amples informations, consultez la section Créer un compte Android for Work. • Ajouter des applications Android for Work à XenMobile. Pour obtenir plus de détails, consultez la section Ajout d'applications à XenMobile.
APN	Vous pouvez utiliser cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile. Une stratégie APN détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones les plus récents.
Accès applicatif	Une stratégie d'accès aux applications dans XenMobile vous permet de définir une liste d'applications dont l'installation sur les appareils est obligatoire, facultative ou interdite. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport à cette liste d'applications.
Attributs d'application	La stratégie Attributs d'application vous permet de spécifier des attributs, tels qu'un Bundle ID d'application gérée, ou un identifiant VPN par application pour les appareils iOS.
Configuration de l'application	Avec cette stratégie, vous pouvez configurer à distance différents paramètres et comportements des applications qui prennent en charge la configuration gérée par le déploiement d'un fichier de configuration XML (appelé liste de propriétés, ou plist) sur les appareils iOS des utilisateurs ou par le déploiement des paires clé/valeur vers les téléphones, tablettes ou ordinateurs Windows 10 des utilisateurs.
Inventaire des applications	Une stratégie d'inventaire des applications vous permet d'établir un inventaire des applications sur les appareils gérés, puis l'inventaire est comparé aux stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste noire (interdites dans une stratégie d'accès aux applications) ou blanche (requis dans une stratégie d'accès aux applications) et prendre les mesures qui s'imposent.
Mode kiosque	Vous pouvez créer une stratégie dans XenMobile afin de définir une liste d'applications dont l'exécution est autorisée ou interdite sur un appareil. Vous pouvez configurer cette stratégie pour les appareils iOS et Android, mais la manière dont la stratégie fonctionne diffère pour chaque plate-forme. Par exemple, vous pouvez bloquer plusieurs applications sur un appareil iOS. Remarque : bien que la stratégie d'appareil fonctionne sur la plupart des appareils Android L et M, le verrouillage d'applications ne fonctionne pas sur les appareils Android N ou plus récents en raison de l'abandon par Google de l'API requise. Pour les appareils iOS, vous pouvez sélectionner une seule application iOS par stratégie. Cela signifie que les utilisateurs peuvent uniquement utiliser leurs appareils pour exécuter une seule

	application. Ils ne peuvent effectuer aucune autre activité sur l'appareil, à l'exception des options que vous avez spécifiquement autorisées lorsque la stratégie de mode kiosque est appliquée.
Utilisation des réseaux	Vous pouvez définir des règles d'utilisation du réseau pour spécifier la manière dont les applications gérées utilisent les réseaux, tels que les réseaux de données cellulaires, sur les appareils iOS. Les règles s'appliquent uniquement aux applications gérées. Les applications gérées sont des applications que vous déployez sur les appareils des utilisateurs via XenMobile. Elles n'incluent pas les applications que les utilisateurs ont téléchargées directement sur leurs appareils sans qu'elles soient déployées via XenMobile ou les applications déjà installées sur les appareils lorsqu'ils ont été inscrits dans XenMobile.
Restrictions applicatives	Grâce à cette stratégie, vous pouvez créer des listes noires d'applications dont vous souhaitez interdire l'installation sur les appareils Samsung KNOX, ainsi que des listes blanches d'applications que vous souhaitez autoriser les utilisateurs à installer.
Tunnel applicatif	Vous pouvez configurer la stratégie de tunnel applicatif pour augmenter la continuité du service et la fiabilité du transfert des données de vos applications mobiles. Les tunnels applicatifs définissent les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications. Vous pouvez également utiliser des tunnels applicatifs pour créer des tunnels d'assistance à distance pour la gestion du support. Remarque : tout trafic applicatif envoyé via un tunnel que vous définissez dans cette stratégie transite via XenMobile avant d'être redirigé vers le serveur exécutant l'application.
Désinstallation d'applications	Une stratégie de désinstallation d'application vous permet de supprimer des applications des appareils utilisateur pour un certain nombre de raisons. Il se peut que vous ne souhaitiez plus prendre en charge certaines applications et que votre entreprise désire remplacer des applications par d'autres similaires mais provenant d'autres fournisseurs, etc. Les applications sont supprimées lorsque cette stratégie est déployée sur les appareils de vos utilisateurs. À l'exception des appareils Samsung KNOX, les utilisateurs reçoivent une invitation à désinstaller l'application ; les utilisateurs d'appareils Samsung KNOX ne reçoivent pas d'invitation à désinstaller l'application.
Restriction de désinstallation d'applications	Grâce à cette stratégie, vous pouvez spécifier les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller.
Navigateur	Vous pouvez créer des stratégies de navigateur afin de définir si les appareils peuvent utiliser le navigateur ou pour limiter les fonctions du navigateur auxquelles les appareils ont accès. Sur les appareils Samsung, vous pouvez désactiver complètement le navigateur, ou vous pouvez activer ou désactiver les fenêtres publicitaires intempestives JavaScript, les cookies, le remplissage automatique, et l'affichage d'avertissements en cas de visite d'un site frauduleux.
Calendrier (CalDav)	Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de calendrier

	(CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.
Cellulaire	Cette stratégie vous permet de configurer des paramètres réseau cellulaire.
Gestionnaire de connexions	Dans XenMobile, vous pouvez spécifier les paramètres de connexion pour les applications qui se connectent automatiquement à Internet et à des réseaux privés. Cette stratégie est uniquement disponible pour Windows Pocket PC.
Contacts (CardDAV)	Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CalDAV.
Copier les applications sur le conteneur Samsung	Vous pouvez spécifier des applications déjà installées sur un appareil à copier vers un conteneur SEAMS ou un conteneur KNOX sur les appareils Samsung pris en charge. Les applications copiées sur le conteneur SEAMS sont disponibles sur les écrans d'accueil des utilisateurs ; les applications copiées sur le conteneur KNOX sont uniquement disponibles lorsque les utilisateurs se connectent au conteneur KNOX.
Informations d'identification	Vous pouvez créer des stratégies d'informations d'identification dans XenMobile afin d'intégrer l'authentification à votre configuration PKI dans XenMobile, comme une entité PKI, un keystore, un fournisseur d'informations d'identification ou un certificat de serveur. Pour plus d'informations sur les informations d'identification, veuillez consulter la section Certificats dans XenMobile. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Stratégie d'informations d'identification. Remarque : avant de pouvoir créer cette stratégie, vous devez connaître les informations d'identification que vous projetez d'utiliser pour chaque plate-forme, ainsi que les certificats et les mots de passe.
Copier les applications sur le conteneur Samsung	Vous pouvez spécifier des applications déjà installées sur un appareil à copier vers un conteneur SEAMS ou un conteneur KNOX sur les appareils Samsung pris en charge. Pour de plus amples informations sur les appareils pris en charge, reportez-vous à la section Appareils Samsung KNOX pris en charge de Samsung. Les applications copiées sur le conteneur SEAMS sont disponibles sur les écrans d'accueil des utilisateurs ; les applications copiées sur le conteneur KNOX sont uniquement disponibles lorsque les utilisateurs se connectent au conteneur KNOX.
Informations d'identification	Souvent utilisée en conjonction avec une stratégie Wi-Fi, cette stratégie permet aux entreprises de déployer des certificats pour l'authentification auprès de ressources internes qui nécessitent une authentification par certificat.
XML personnalisé	Vous pouvez créer des stratégies XML personnalisées dans XenMobile pour personnaliser les fonctionnalités suivantes :

	• Provisioning, qui comprend la configuration de l'appareil, et l'activation ou la désactivation de fonctionnalités. • Configuration de l'appareil, ce qui permet aux utilisateurs de modifier les paramètres sur l'appareil. • Mises à niveau logicielles, ce qui comprend la mise à disposition de nouveaux logiciels ou de correctifs de bogues à charger sur l'appareil, y compris des applications et logiciels système. • Gestion des pannes, ce qui comprend la réception de rapports d'erreur et d'état à partir de l'appareil. Vous créez votre propre configuration XML personnalisée à l'aide de l'API Open Mobile Alliance Device Management (OMA DM) dans Windows. La création de code XML personnalisé avec l'API OMA DM n'est pas couverte dans cette rubrique. Pour de plus amples informations sur l'utilisation de l'API OMA DM, veuillez consulter la section OMA Device Management sur le site de Microsoft Developer Network.
Supprimer des fichiers et dossiers	Vous pouvez créer une stratégie dans XenMobile pour supprimer des fichiers ou dossiers spécifiques d'appareils Windows Mobile/CE.
Supprimer des clés et valeurs de registre	Vous pouvez créer une stratégie dans XenMobile pour supprimer des clés et valeurs de Registre spécifiques d'appareils Windows Mobile/CE.
Attestation de l'intégrité des appareils	Dans XenMobile, vous pouvez une stratégie qui nécessite que les appareils Windows 10 communiquent leur état d'intégrité : pour cela, ces appareils envoient des informations d'exécution et des données spécifiques au service HAS pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie ensuite à XenMobile. Lorsque XenMobile reçoit le certificat d'attestation d'intégrité, en fonction du contenu de l'attestation, des actions automatiques que vous avez configurées précédemment peuvent être déployées. Les données vérifiées par le service HAS sont les suivantes : • AIK présent ? • État BitLocker • Débogage du démarrage activé ? • Version de la liste de révision du Gestionnaire de démarrage • Intégrité du code activée ? • Version de la liste de révision d'intégrité du code • Stratégie DEP • Pilote ELAM chargé ? • Date d'émission • Débogage du noyau activé ? • PCR • Nombre de réinitialisations • Nombre de redémarrages • Mode sans échec activé ? • Hachage SBCP

	• Démarrage sécurisé activé ? • Signature du test activée ? • VSM activé ? • WinPE activé ? Pour de plus amples informations, reportez-vous à la page HealthAttestation CSP de Microsoft.
Nom de l'appareil	Une stratégie de nom d'appareil vous permet de définir les noms sur des appareils iOS et Mac OS X, de façon à identifier facilement les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil. Pour de plus amples informations sur les macros, consultez la section Macros dans XenMobile.
Hub d'entreprise	Une stratégie d'hub d'entreprise pour Windows Phone vous permet de distribuer des applications d'entreprise via le magasin hub d'entreprise. Avant de pouvoir créer la stratégie, vous avez besoin des éléments suivants : • Un certificat de signature AET (.aetx) de Symantec • L'application d'hub d'entreprise Citrix signée à l'aide de l'outil de signature d'applications Microsoft (XapSignTool.exe) Remarque : XenMobile prend en charge une seule stratégie d'hub d'entreprise pour un mode Windows Phone Secure Hub. Par exemple, pour télécharger Windows Phone Secure Hub pour XenMobile Enterprise Edition, vous ne devez pas créer de multiples stratégies d'hub d'entreprise avec différentes versions de Worx Home pour XenMobile Enterprise Edition. Vous pouvez uniquement déployer la stratégie d'hub d'entreprise initiale lors de l'inscription de l'appareil.
Exchange	XenMobile vous offre deux options pour distribuer des e-mails. Vous pouvez mettre à disposition la messagerie ActiveSync à l'aide de l'application Secure Mail en conteneur, ou vous pouvez utiliser cette stratégie MDM Exchange pour activer la messagerie ActiveSync pour le client de messagerie natif sur l'appareil.
Fichiers	Grâce à cette stratégie, vous pouvez ajouter des fichiers de script à XenMobile qui exécutent certaines fonctions pour les utilisateurs, ou vous pouvez ajouter des fichiers de documents auxquels vous voulez que les utilisateurs Android aient accès sur leurs appareils. Lorsque vous ajoutez le fichier, vous pouvez également spécifier le répertoire dans lequel vous souhaitez que le fichier soit stocké sur l'appareil. Par exemple, si vous souhaitez que les utilisateurs Android reçoivent un document d'entreprise ou fichier .pdf, vous pouvez déployer le fichier sur l'appareil et informer les utilisateurs de son emplacement. Vous pouvez ajouter les types de fichiers suivants avec cette stratégie : • Fichiers texte (.xml, .html, .py, etc.) • Autres fichiers tels que des documents, images, feuilles de calcul ou présentations • Pour Windows Mobile and Windows CE uniquement : fichiers de script créés avec MortScript

Police	Vous pouvez ajouter cette stratégie dans XenMobile pour ajouter des polices supplémentaires sur les appareils iOS et Mac OS X des utilisateurs. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge. Remarque : pour iOS, cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.
Importer le profil iOS et Mac OS X	Vous pouvez importer les fichiers XML de configuration d'appareil pour iOS et OS X dans XenMobile. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator. Pour de plus amples informations sur l'utilisation d'Apple Configurator pour créer un fichier de configuration, consultez la page d'aide sur Configurator d'Apple.
Kiosque	Lorsque vous créez une stratégie kiosque dans XenMobile, seules une ou des applications spécifiques peuvent être exécutées sur les appareils Samsung SAFE. Cette stratégie est utile pour les appareils d'entreprise conçus pour n'exécuter qu'un type spécifique ou une classe d'applications. Cette stratégie vous permet également de choisir des images personnalisées à utiliser comme fond d'écran de l'écran d'accueil et de l'écran de verrouillage lorsque l'appareil est en mode Kiosque. Remarque : • Toutes les applications que vous spécifiez pour le mode kiosque doivent déjà être installées sur les appareils des utilisateurs. • Certaines options ne s'appliquent qu'à l'API Samsung Mobile Device Management (MDM) 4.0 et versions ultérieures.
Configuration du Launcher	Avec cette stratégie pour les appareils Android, vous pouvez spécifier les applications autorisées par le Citrix Launcher, une image de logo personnalisé pour l'icône Citrix Launcher, une image d'arrière-plan personnalisée pour le Citrix Launcher et des exigences de mot de passe pour quitter le Launcher.
LDAP	Vous créez une stratégie LDAP pour appareils iOS dans XenMobile pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information sur le compte nécessaires. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP. Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.
Emplacement	La stratégie d'emplacement peut être utilisée pour géo-localiser les appareils sur une carte, en supposant que le GPS est activé pour Secure Hub sur l'appareil. Une fois cette stratégie transmise à l'appareil, les administrateurs peuvent envoyer une commande de localisation à partir du serveur XenMobile et l'appareil répondra avec ses coordonnées d'emplacement. Les stratégies de géofencing et de suivi sont également prises en charge.
Messagerie	Vous pouvez ajouter une stratégie de messagerie dans XenMobile pour configurer un compte de

	messagerie sur les appareils iOS ou Mac OS X des utilisateurs.
Domaines gérés	Vous pouvez définir des domaines gérés via cette stratégie qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari. Vous pouvez spécifier des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur. Cette stratégie est uniquement prise en charge sur les appareils supervisés iOS 8 et versions ultérieures. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator. Lorsqu'un utilisateur envoie un e-mail à un destinataire dont le domaine n'est pas sur la liste des domaines de messagerie gérés, un message s'affiche sur l'appareil de l'utilisateur pour l'avertir qu'il envoie un message à un utilisateur en dehors de votre domaine d'entreprise. Lorsqu'un utilisateur tente d'ouvrir un élément (document, pièce jointe ou téléchargement) à l'aide de Safari depuis un domaine Web se trouvant sur la liste de domaines gérés, l'application d'entreprise appropriée ouvre l'élément. Si l'élément ne provient pas d'un domaine Web se trouvant sur la liste des domaines Web gérés, l'utilisateur ne peut pas ouvrir l'élément avec une application d'entreprise ; il doit utiliser une application non gérée, personnelle.
Options MDM	Vous pouvez créer une stratégie d'appareil dans XenMobile pour gérer les fonctions Localiser mon iPhone/Verrouillage d'activation iPad sur les appareils supervisés iOS 7.0 et versions ultérieures. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator ou Inscription en bloc iOS. Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui est conçue pour empêcher la réactivation des appareils perdus ou volés ; l'ID et le mot de passe Apple de l'utilisateur sont exigés pour désactiver la fonction Localiser mon iPhone, effacer l'appareil ou réactiver et utiliser l'appareil. Dans XenMobile, vous pouvez contourner l'obligation d'entrer ID et mot de passe en activant l'option Verrouillage d'activation dans la stratégie d'options MDM. Lorsqu'un utilisateur renvoie un appareil sur lequel la fonction Localiser mon iPhone est activée, vous pouvez gérer l'appareil à partir de la console XenMobile sans ses informations d'identification Apple.
Info organisation	Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin de spécifier les coordonnées de votre organisation à utiliser pour envoyer les messages d'alerte qui sont transmis depuis XenMobile vers les appareils iOS. La stratégie est disponible pour iOS 7 et versions ultérieures.
Code secret	Une stratégie de code secret vous permet de définir un code PIN ou un mot de passe sur un appareil géré. Cette stratégie de code secret vous permet de définir la complexité et les délais d'expiration du code secret sur l'appareil.

Personal Hotspot	Grâce à cette stratégie, vous pouvez autoriser les utilisateurs à se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi en utilisant la connexion des données cellulaires au travers de la fonctionnalité Partage de connexion (Personal Hotspot) de leurs appareils iOS. Disponible sur iOS 7.0 et version ultérieure.
Suppression de profil	Vous pouvez créer une stratégie de suppression de profil dans XenMobile. La stratégie, lorsqu'elle est déployée, supprime le profil d'application des appareils iOS ou Mac OS X des utilisateurs.
Profil de provisioning	Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning de distribution d'entreprise, dont Apple a besoin pour que l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir. Le principal problème avec les profils de provisioning est qu'ils expirent un an après qu'ils sont générés sur le portail Apple Developer et vous devez conserver les dates d'expiration pour tous les profils de provisioning sur tous les appareils iOS inscrits par vos utilisateurs. Le suivi des dates d'expiration non seulement implique de surveiller les dates d'expiration, mais aussi quels utilisateurs utilisent quelle version de l'application. Les deux solutions consistent à envoyer par e-mail les profils de provisioning aux utilisateurs ou à les placer dans un portail Web pour le téléchargement et l'installation. Ces solutions fonctionnent, mais elles peuvent entraîner des erreurs car elles requièrent que les utilisateurs réagissent à des instructions dans un e-mail ou accèdent au portail Web pour télécharger le profil approprié et l'installer. Pour effectuer cette opération de façon transparente pour les utilisateurs, dans XenMobile, vous pouvez installer et supprimer les profils de provisioning avec les stratégies d'appareil. Les profils manquants ou arrivés à expiration sont supprimés si nécessaire et des profils à jour sont installés sur les appareils des utilisateurs, de façon à ce qu'il leur suffise de taper sur une application pour l'ouvrir.
Suppression du profil de provisioning	Vous pouvez supprimer des profils de provisioning iOS avec des stratégies d'appareil. Pour de plus amples informations sur les profils de provisioning, consultez la section Ajout d'un profil de provisioning.
Proxy	Vous pouvez ajouter une stratégie dans XenMobile pour spécifier les paramètres de proxy HTTP globaux pour les appareils exécutant Windows Mobile/CE et iOS 6.0 ou version ultérieure. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil. Remarque : avant de déployer cette stratégie, assurez-vous de définir tous les appareils iOS pour lesquels vous souhaitez définir un proxy HTTP global en mode supervisé. Pour de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.
Registre	Le registre Windows Mobile/CE stocke des données sur les applications, pilotes, préférences utilisateur et paramètres de configuration. Dans XenMobile, vous pouvez définir les clés et valeurs de registre qui vous permettent de gérer les appareils Windows Mobile/CE.

Assistance à distance	Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX des utilisateurs. Vous pouvez configurer deux types d'assistance : • Assistance à distance de base : cette option vous permet d'afficher des informations de diagnostic sur l'appareil, telles que les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés, etc. • Assistance à distance premium : cette option vous permet de contrôler à distance l'écran de l'appareil, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.
Restrictions	La stratégie de restriction offre aux administrateurs plusieurs façons de verrouiller et contrôler les fonctionnalités sur l'appareil géré. Il existe des centaines d'options de restriction, en passant par la désactivation de l'appareil photo ou du micro d'un appareil jusqu'à l'application de règles d'itinérance et d'accès aux services de tiers tels que des magasins d'applications. Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour limiter l'accès des utilisateurs à certaines fonctionnalités sur leurs appareils, téléphones, tablettes, etc. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article. Cette stratégie permet ou empêche les utilisateurs d'utiliser certaines fonctionnalités sur leurs appareils, telles que l'appareil photo. Vous pouvez également définir des restrictions de sécurité, des restrictions d'accès au contenu multimédia ainsi que des restrictions sur les types d'applications que les utilisateurs peuvent ou ne peuvent pas installer. La plupart des paramètres de restriction sont réglés par défaut sur ON ou autorise. Les principales exceptions sont la fonctionnalité Sécuriser - Forcer dans iOS et toutes les fonctionnalités de Windows Tablet, lesquelles prennent par défaut la valeur OFF ou appliquent des restrictions. Conseil : toute option définie sur ON signifie que l'utilisateur peut effectuer l'opération ou utiliser la fonctionnalité. Par exemple : • Appareil photo. Si l'option est réglée sur ON, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil. • Captures d'écrans. Si l'option est réglée sur ON, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.
Itinérance	Vous pouvez ajouter une stratégie d'itinérance dans XenMobile afin d'activer les services de voix et de données en itinérance sur des appareils iOS et Windows Mobile/CE. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée. Pour iOS, cette stratégie est uniquement disponible sur les appareils iOS 5.0 et versions ultérieures.

Pare-feu Samsung SAFE	Cette stratégie vous permet de configurer les paramètres de pare-feu pour les appareils Samsung. Vous pouvez entrer les adresses IP, les ports et les noms d'hôte auxquels vous souhaitez autoriser les appareils à accéder ou auxquels vous souhaitez empêcher les appareils d'accéder. Vous pouvez également configurer les paramètres de redirection de proxy et de proxy.
Clé de licence MDM Samsung	XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX. SAFE fait partie d'une famille de solutions qui fournit des améliorations de sécurité pour les entreprises via l'intégration à des solutions MDM. Samsung KNOX est une solution du programme SAFE destinée à une utilisation professionnelle conçue pour renforcer la sécurité sur la plate-forme Android. Vous devez activer les API SAFE en déployant la clé Samsung ELM (Enterprise License Management) intégrée sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. Pour activer les API Samsung KNOX, vous devez acheter une licence Samsung KNOX à l'aide du Samsung KNOX License Management System (KLMS) en plus de déployer la clé Samsung ELM. Le KMLS Samsung provisionne des licences valides sur des solutions MDM afin d'activer les API Samsung KNOX sur les appareils mobiles. Vous devez vous procurer ces licences auprès de Samsung car elles ne sont pas fournies par Citrix. Vous devez déployer Secure Hub en conjonction avec la clé Samsung ELM pour activer les API SAFE et Samsung KNOX. Vous pouvez vérifier que les API SAFE sont activés en consultant les propriétés de l'appareil. Lorsque la clé Samsung ELM est déployée, le paramètre API Samsung MDM disponible est défini sur True.
Planification	Cette stratégie est requise pour que les appareils Android et Windows Mobile puissent se connecter au serveur XenMobile pour pouvoir utiliser la gestion MDM, distribuer des applications et déployer des stratégies. Si vous n'envoyez pas cette stratégie et que vous n'avez pas activé Google FCM, un appareil ne se reconnectera pas au serveur. Par conséquent, il est important de distribuer cette stratégie au paquetage de base pour l'inscription d'appareils.
SCEP	Cette stratégie vous permet de configurer des appareils iOS et Mac OS X afin de récupérer un certificat à l'aide du protocole d'inscription du certificat simple (SCEP) à partir d'un serveur SCEP externe. Si vous souhaitez délivrer un certificat sur l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à XenMobile, vous devez créer une entité PKI et un fournisseur PKI en mode distribué. Pour plus d'informations, veuillez consulter la section Entités PKI.
Clé de sideloading	Le sideloading dans XenMobile vous permet de déployer des applications sur des appareils Windows 8.1 qui n'ont pas été achetées à partir du Windows Store. Dans la plupart des cas, vous sideloadez les applications que vous développez pour une utilisation en entreprise que vous ne souhaitez pas rendre publiques dans le Windows Store. Pour sideloader des applications, vous devez configurer la clé de sideloading et l'activation de clés et déployer les applications sur les appareils des utilisateurs. Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie : • La clé de sideloading du produit, que vous pouvez obtenir en vous connectant au Centre de

	gestion des licences en volume Microsoft. • L'activation de clé, que vous créez via la ligne de commande après avoir obtenu la clé de sideloading du produit.
Certificat de signature	Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour configurer les certificats de signature à utiliser pour signer les fichiers APPX. Vous avez besoin des certificats de signature si vous voulez distribuer des fichiers APPX aux utilisateurs pour les autoriser à installer des applications sur leurs tablettes Windows.
Compte SSO	Vous créez des comptes SSO dans XenMobile pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à XenMobile et à vos ressources d'entreprise internes à partir de différentes applications. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Les informations d'identification utilisateur d'entreprise du compte SSO sont utilisées pour toutes les applications, y compris les applications provenant de l'App Store. Cette stratégie est conçue pour fonctionner avec l'authentification Kerberos. Remarque : cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.
Chiffrement du stockage	Vous pouvez créer des stratégies de chiffrement du stockage dans XenMobile pour chiffrer le stockage interne et externe, et, en fonction de l'appareil, pour empêcher les utilisateurs d'utiliser une carte de stockage sur leurs appareils. Vous pouvez créer des stratégies pour Samsung SAFE, Windows Phone et Android Sony. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article Stratégie de chiffrement du stockage de cette section.
Magasin	Vous pouvez créer une stratégie dans XenMobile afin de spécifier si les appareils iOS, Android ou Windows Tablet affichent un clip Web XenMobile Store sur l'écran d'accueil des appareils.
Abonnements calendriers	Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS des utilisateurs. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur www.apple.com/downloads/macosx/calendars. Remarque : vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.
Termes et conditions	Vous créez des stratégies de termes et conditions dans XenMobile lorsque vous souhaitez que les utilisateurs acceptent les stratégies spécifiques à votre entreprise qui régissent les connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de XenMobile, ils voient s'afficher les termes et conditions et doivent les accepter pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription. Vous pouvez créer différentes stratégies pour les termes et conditions dans différentes langues

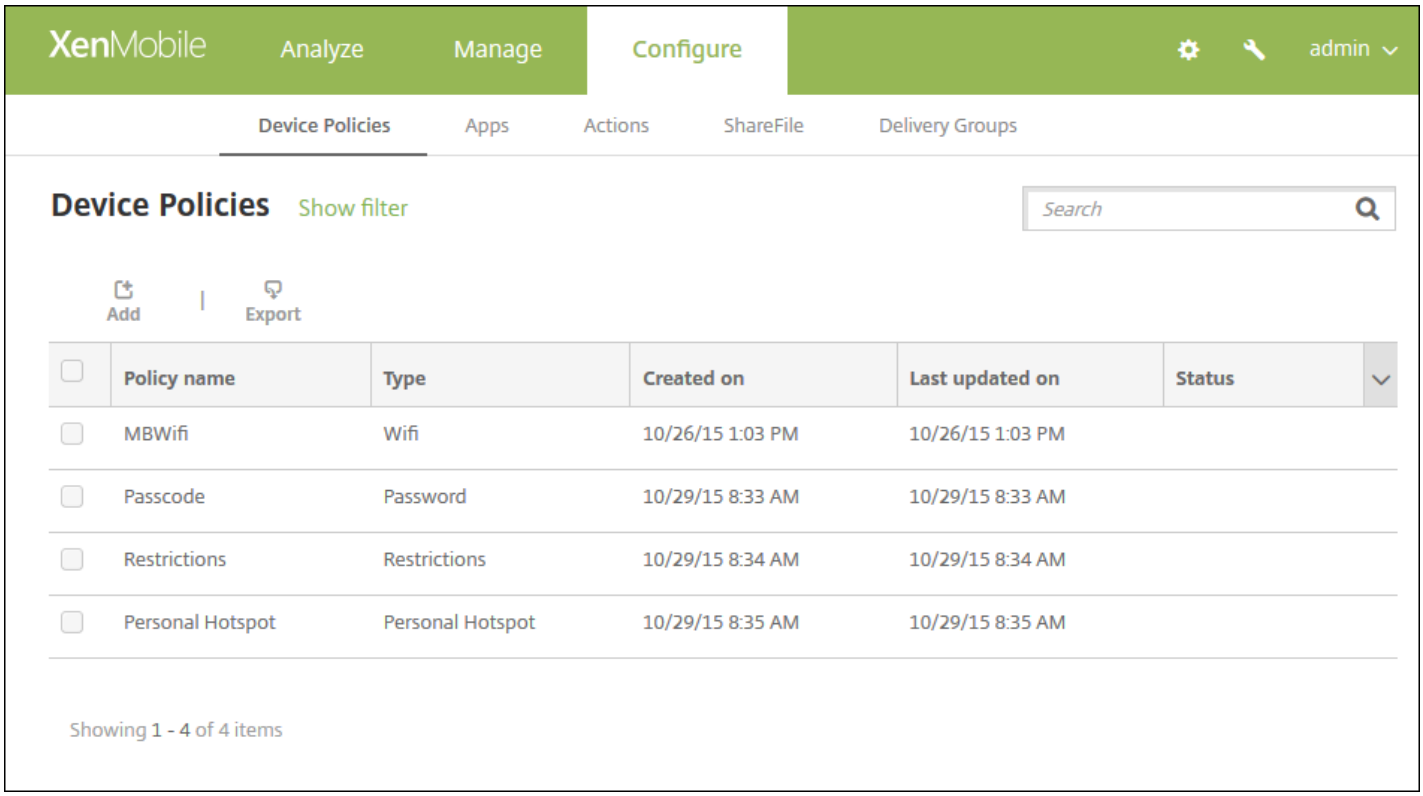
	si votre société dispose d'utilisateurs internationaux pour leur permettre d'accepter les termes et conditions dans leur langue maternelle. Vous devez fournir un fichier pour chaque combinaison de plate-forme et de langue que vous souhaitez déployer. Pour les appareils Android et iOS, vous devez fournir des fichiers PDF. Pour les appareils Windows, vous devez fournir des fichiers texte (.txt) et les fichiers image connexes.
VPN	Pour les clients désirant fournir l'accès aux systèmes principaux à l'aide de l'ancienne technologie de passerelle VPN, cette stratégie VPN peut être utilisée pour distribuer les détails de connexion de la passerelle VPN à l'appareil. Un certain nombre de fournisseurs VPN sont pris en charge via la stratégie y compris Cisco AnyConnect, Juniper ainsi que Citrix VPN. Il est également possible d'associer cette stratégie à une autorité de certification et d'activer le VPN à la demande (en supposant que la passerelle VPN prenne en charge cette option). Vous pouvez ajouter une stratégie dans XenMobile pour configurer des paramètres de réseau privé virtuel (VPN) permettant aux appareils de se connecter de manière sécurisée aux ressources d'entreprise. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans l'article VPN de cette section.
Fond d'écran	Vous pouvez ajouter un fichier .png ou .jpg en tant que fond d'écran sur l'écran d'accueil, l'écran de verrouillage ou les deux. Disponible dans iOS 7.1.2 et version ultérieure. Pour utiliser un fond d'écran différent sur iPad et iPhone, vous devez créer différentes stratégies de fond d'écran et les déployer vers les utilisateurs appropriés.
Filtre de contenu Web	Vous pouvez ajouter une stratégie dans XenMobile destinée à filtrer le contenu Web sur les appareils iOS à l'aide de la fonction de filtrage automatique d'Apple en conjonction avec les sites spécifiques que vous ajoutez aux listes blanches et listes noires. Cette stratégie est uniquement disponible sur les appareils iOS 7.0 et versions ultérieures en mode Supervisé. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.
Clip Web	Grâce à cette stratégie, vous pouvez placer des raccourcis ou clips Web sur des sites Web de manière à ce qu'ils apparaissent à côté des applications sur les appareils des utilisateurs. Vous pouvez spécifier vos propres icônes pour représenter les clips Web sur des appareils iOS, Mac OS X et Android ; Windows Tablet requiert uniquement un nom et une adresse URL.
Wi-Fi	La stratégie Wi-Fi permet aux administrateurs de facilement distribuer les détails du routeur Wi-Fi (SSID, données de configuration et d'authentification) sur un appareil géré. Les stratégies Wi-Fi vous permettent de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux sans fil en définissant ce qui suit : noms et types de réseau, stratégies d'authentification et de sécurité, serveurs proxy et d'autres détails liés à l'utilisation du Wi-Fi pour tous les utilisateurs sur les plates-formes que vous avez choisies.
Certificat Windows CE	Ajoutez cette stratégie d'appareil afin de créer et de mettre à disposition des certificats Windows Mobile/CE à partir d'une PKI externe vers les appareils des utilisateurs. Pour de plus

	amples informations sur les certificats et les entités PKI, consultez la section Certificats.
Options XenMobile	Vous ajoutez une stratégie d'options XenMobile pour configurer le comportement de Secure Hub lors de la connexion à XenMobile à partir d'appareils Android et Windows Mobile/CE.
Désinstallation de XenMobile	Vous pouvez ajouter cette stratégie dans XenMobile afin de désinstaller XenMobile des appareils Android et Windows Mobile/CE. Lorsqu'elle est déployée, cette stratégie supprime XenMobile sur tous les appareils du déploiement.

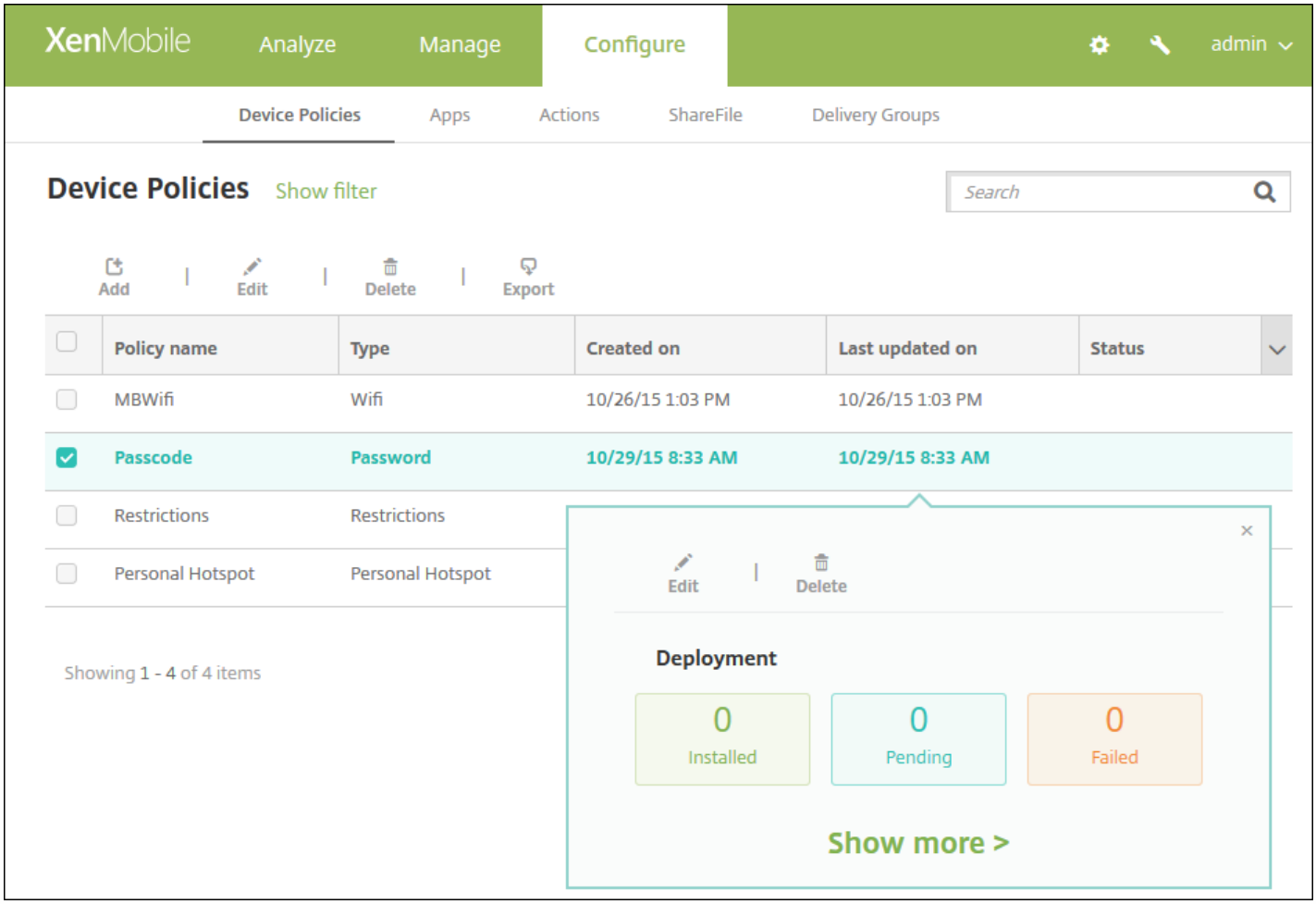
Page Stratégies d'appareil dans la console

Les stratégies sont accessibles à partir de la page **Stratégies d'appareil** dans la console XenMobile. Pour accéder à la page **Stratégies d'appareil**, cliquez sur **Configurer > Stratégies d'appareil**. À partir de cette fenêtre, vous pouvez ajouter de nouvelles stratégies, consulter l'état de stratégies existantes, et modifier ou supprimer des stratégies.

La page **Stratégies d'appareil** contient une table répertoriant toutes les stratégies actuelles.



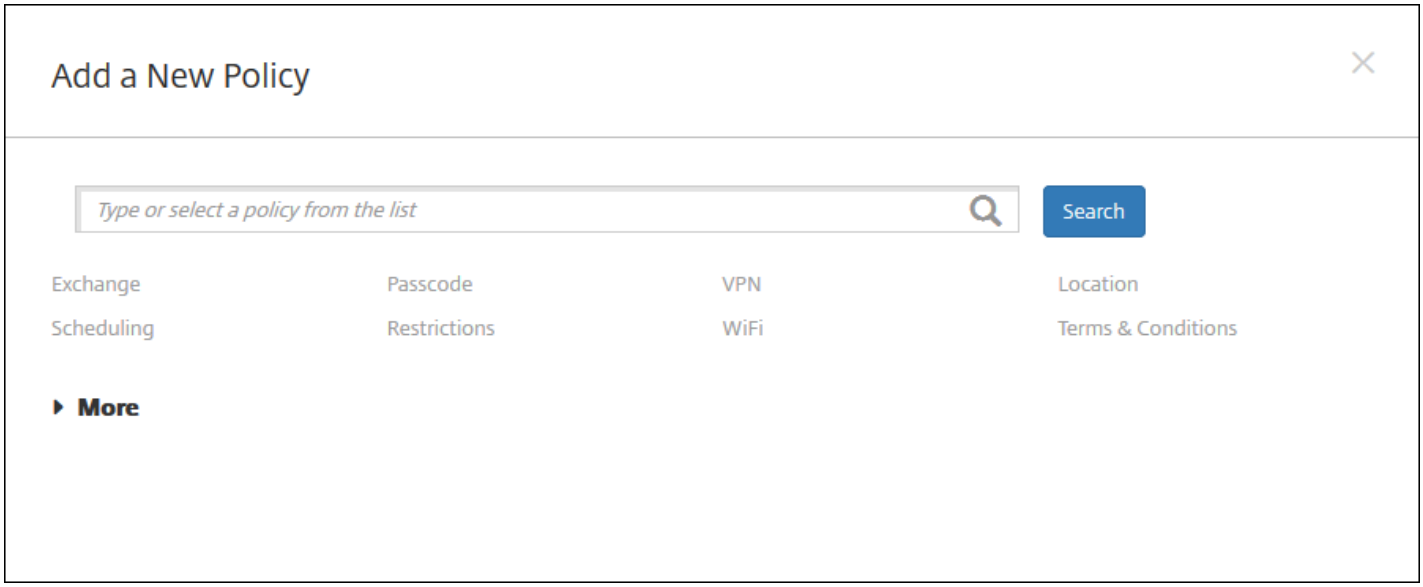
Pour modifier ou supprimer une stratégie sur la page **Stratégies d'appareil**, vous pouvez sélectionner la case à cocher en regard d'une stratégie pour afficher les options de menu au-dessus de la liste de stratégie, ou vous pouvez cliquer sur une stratégie dans la liste pour afficher le menu d'options sur le côté droit de la liste. Si vous cliquez sur **Afficher plus**, les détails de stratégie s'affichent.



Pour ajouter une stratégie d'appareil

1.Sur la page **Stratégies d'appareil**, cliquez sur **Ajouter**.

La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît. Vous pouvez développer **Plus** pour afficher d'autres stratégies.

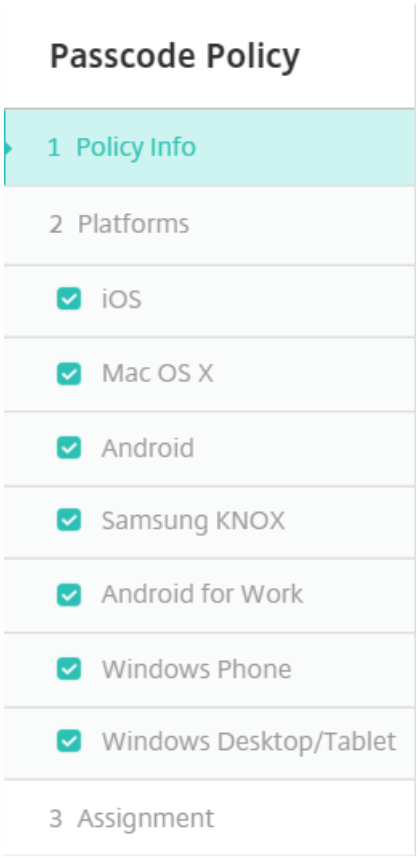


2. Pour trouver la stratégie que vous souhaitez ajouter, effectuez l'une des opérations suivantes :

- Cliquez sur la stratégie.
  La page **Informations sur la stratégie** pour la stratégie sélectionnée s'affiche.
- Entrez le nom de la stratégie dans le champ de recherche. À mesure que vous tapez, des correspondances potentielles s'affichent. Si votre stratégie figure dans la liste, cliquez dessus. Seule la stratégie sélectionnée reste dans la boîte de dialogue. Cliquez dessus pour ouvrir la page **Informations de stratégie** pour cette stratégie.
  Important : si votre stratégie sélectionnée figure dans la zone **Plus**, elle est uniquement visible si vous développez **Plus**.

3.Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour les plates-formes sélectionnées s'affichent dans l'étape 5.

Remarque : seules les plates-formes prises en charge par la stratégie sont répertoriées.

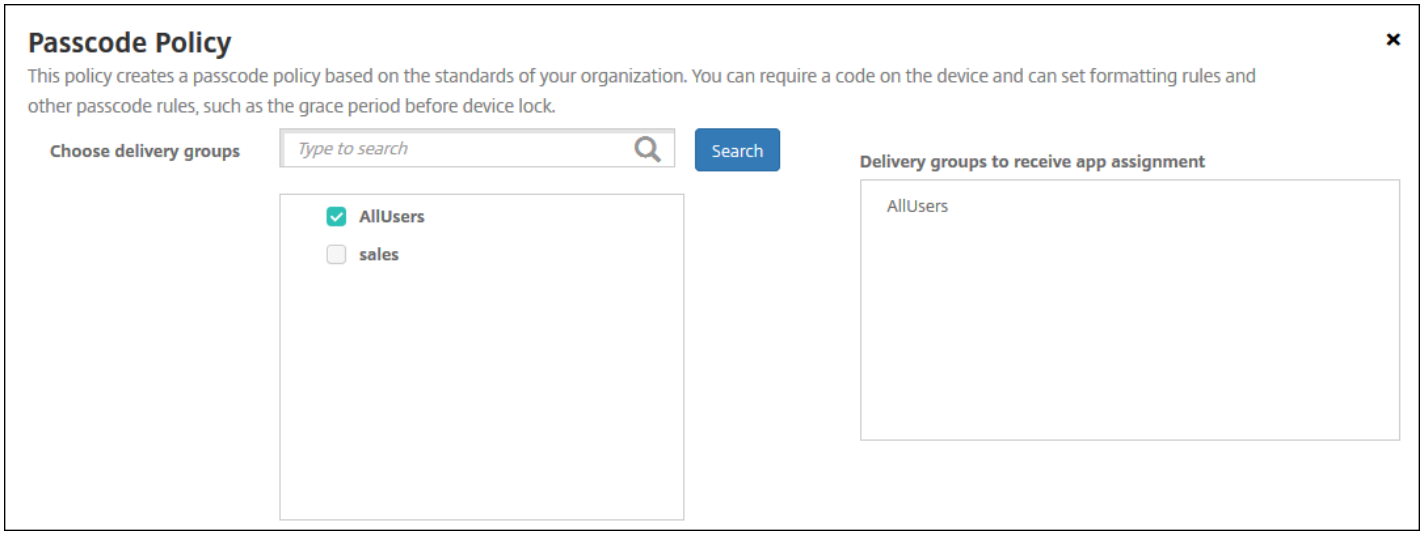


4. Remplissez la page **Informations de stratégie** puis cliquez sur **Suivant**. La page **Informations de stratégie** collecte des informations, comme le nom de la stratégie, pour vous aider à identifier et à suivre vos stratégies. Cette page est identique pour toutes les stratégies.

5. Renseignez les pages de plates-formes. Les pages de plates-formes s'affichent pour chaque plate-forme que vous avez sélectionnée dans l'étape 3. Ces pages sont différentes pour chaque stratégie. Chaque stratégie peut être différente entre les plates-formes. Les stratégies ne sont pas toutes prises en charge par toutes les plates-formes. Cliquez sur **Suivant** pour passer à la page de plate-forme suivante, ou lorsque toutes les pages de plate-forme sont remplies, à la page **Attribution**.

6. Sur la page **Attribution**, sélectionnez les groupes de mise à disposition auxquels vous voulez appliquer la stratégie. Lorsque vous cliquez sur un groupe de mise à disposition, le groupe apparaît dans la zone **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

Remarque : la zone Groupes de mise à disposition qui vont recevoir l'attribution d'applications n'apparaît pas tant que vous n'avez pas sélectionné un groupe de mise à disposition.



7. Cliquez sur **Enregistrer**.

La stratégie est ajoutée au tableau **Stratégies d'appareil**.

Pour modifier ou supprimer une stratégie d'appareil

1. Dans le tableau **Stratégies d'appareil**, sélectionnez la case à cocher en regard de la stratégie que vous souhaitez modifier ou supprimer.

2. Cliquez sur **Modifier** ou **Supprimer**.

- Si vous cliquez sur **Modifier**, vous pouvez modifier tous les paramètres.
- Si vous cliquez sur le bouton **Supprimer**, dans la boîte de dialogue de confirmation, cliquez de nouveau sur **Supprimer**.

Stratégies XenMobile par plate-forme

Mar 31, 2017

Pour afficher les stratégies par plate-forme, téléchargez le PDF de la Matrice des stratégies applicatives par plate-forme.

Vous ajoutez et configurez les stratégies dans la console XenMobile depuis **Configurer > Stratégies d'appareil**. XenMobile 10.4 prend en charge les stratégies d'appareil pour les plates-formes suivantes :

- Amazon
- iOS
- Mac OS X
- HTC Android
- Android TouchDown
- Android for Work
- Android
- Samsung SAFE
- Samsung SEAMS
- Windows Mobile/CE
- Windows Phone 8/Windows 10 Mobile
- Windows 8 et Windows 10 Desktop/Tablet (.86)

Pour de plus amples informations sur les appareils pris en charge dans XenMobile 10.x, consultez la section Plates-formes prises en charge.

> ## Remarque
>
> - La prise en charge des appareils Symbian est obsolète dans XenMobile 10.3.
> - Si votre environnement est configuré avec des objets de stratégie de groupe (GPO), lorsque vous configurez des stratégies d'appareil XenMobile pour Windows 10, tenez compte de la règle suivante. Si une stratégie entre en conflit avec un ou plusieurs appareils Windows 10 inscrits, la stratégie alignée avec le GPO est prioritaire.

Stratégies de mise en miroir AirPlay

Feb 23, 2017

La fonctionnalité AirPlay d'Apple permet aux utilisateurs de streamer sans fil du contenu à partir d'un appareil iOS sur un écran de télé grâce à Apple TV, ou d'afficher tout ce qui figure sur l'écran d'un appareil sur un écran de télévision ou un autre ordinateur Mac.

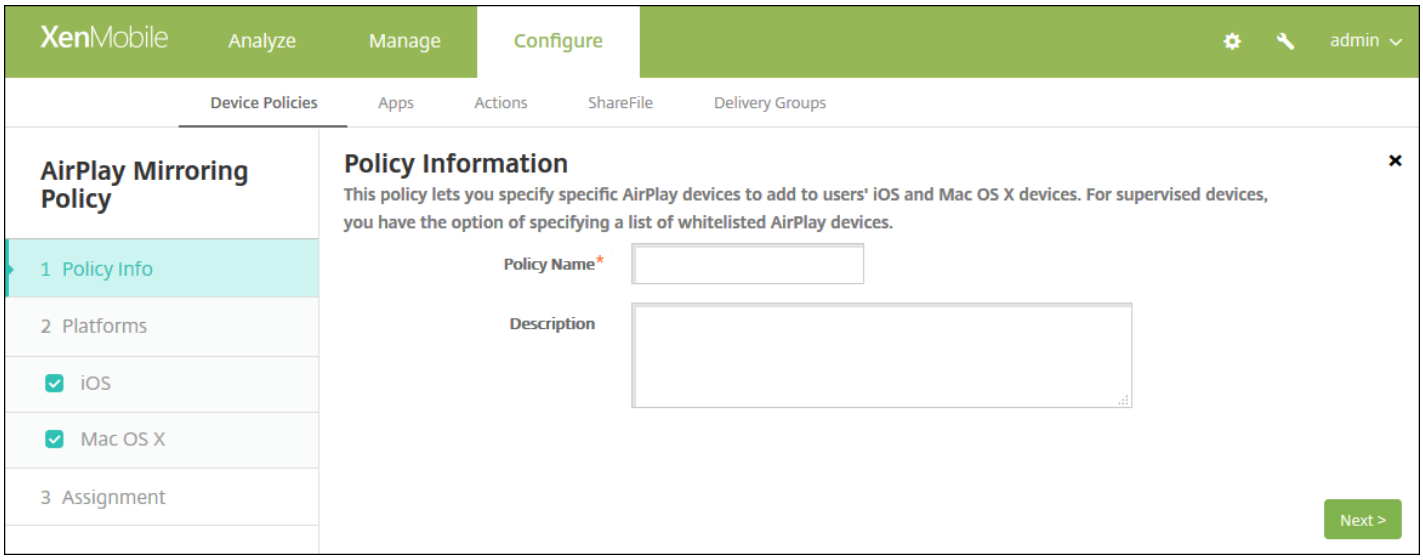
Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des appareils AirPlay spécifiques (tels que Apple TV ou un autre ordinateur Mac) aux appareils iOS des utilisateurs. Vous avez aussi la possibilité d'ajouter des appareils à une liste blanche d'appareils supervisés, ce qui limite l'accès des utilisateurs uniquement aux appareils AirPlay figurant sur la liste blanche. Pour de plus amples informations sur le placement d'un appareil en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

Remarque : avant de continuer, vérifiez que vous disposez des ID et des mots de passe de tous les appareils que vous voulez ajouter.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis sous **Utilisateur final**, cliquez sur **Mise en miroir AirPlay**. La page **Stratégie de mise en miroir AirPlay** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

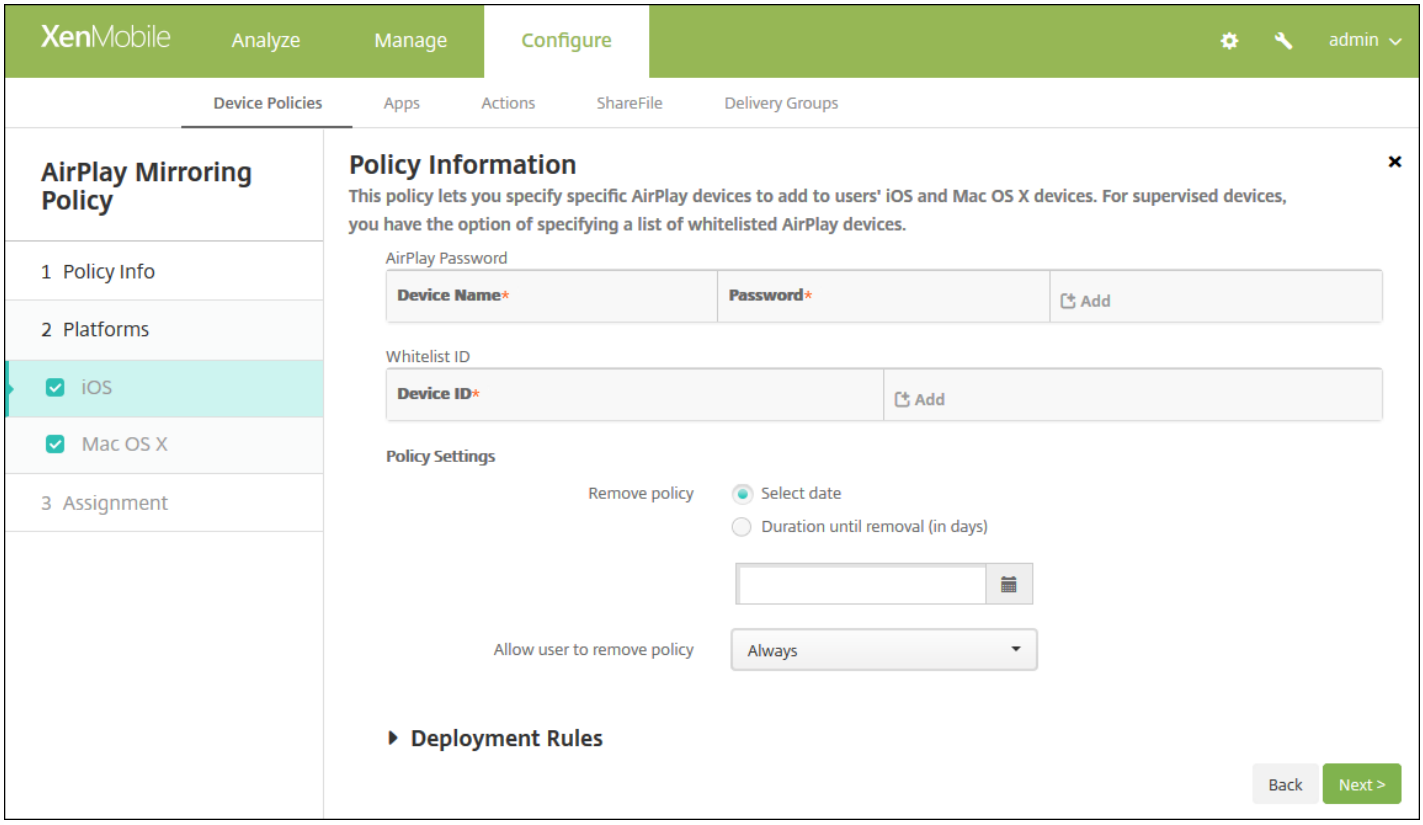
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **Mot de passe AirPlay** : pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil** : entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe** : entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.
- **ID de liste blanche :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil** : entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

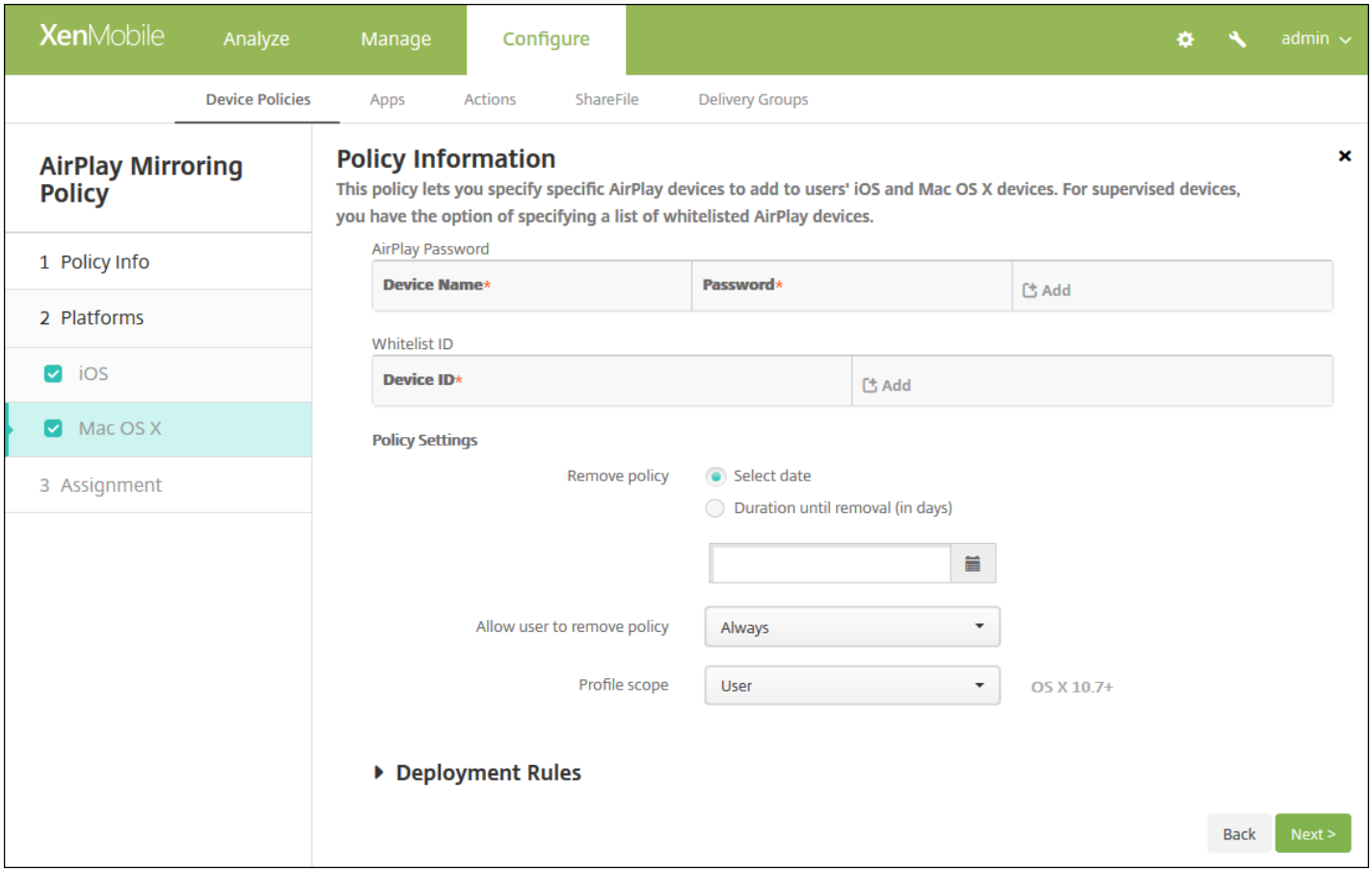
    Remarque : pour supprimer un appareil existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier un appareil existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la

suppression.

- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X



Pour configurer ces paramètres :

- **Mot de passe AirPlay** : pour chaque appareil que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil** : entrez l'adresse du matériel (adresse MAC) au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - **Mot de passe** : entrez un mot de passe pour l'appareil (facultatif).
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.
- **ID de liste blanche :** cette liste est ignorée pour les appareils non supervisés. Les ID d'appareil de cette liste sont les seuls appareils AirPlay disponibles pour les utilisateurs. Pour chaque appareil AirPlay que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **ID de l'appareil** : entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
  - Cliquez sur **Ajouter** pour ajouter l'appareil ou cliquez sur **Annuler** pour annuler l'ajout de l'appareil.

  Remarque : pour supprimer un appareil existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

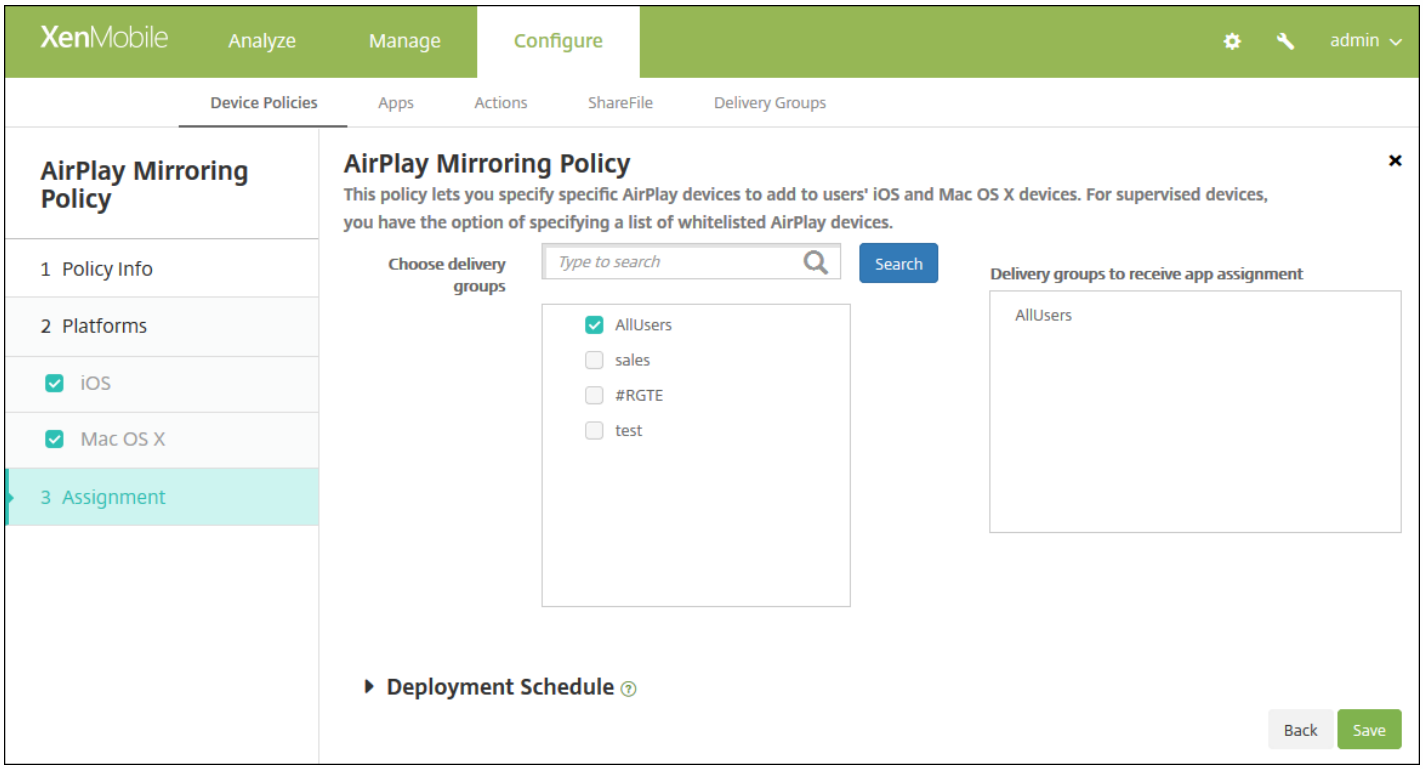
  Pour modifier un appareil existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le

côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de mise en miroir AirPlay** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.

- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie AirPrint

Feb 23, 2017

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des imprimantes AirPrint à la liste des imprimantes AirPrint sur les appareils iOS des utilisateurs. Cette stratégie facilite la prise en charge d'environnements dans lesquels les imprimantes et les appareils figurent sur des sous-réseaux différents.

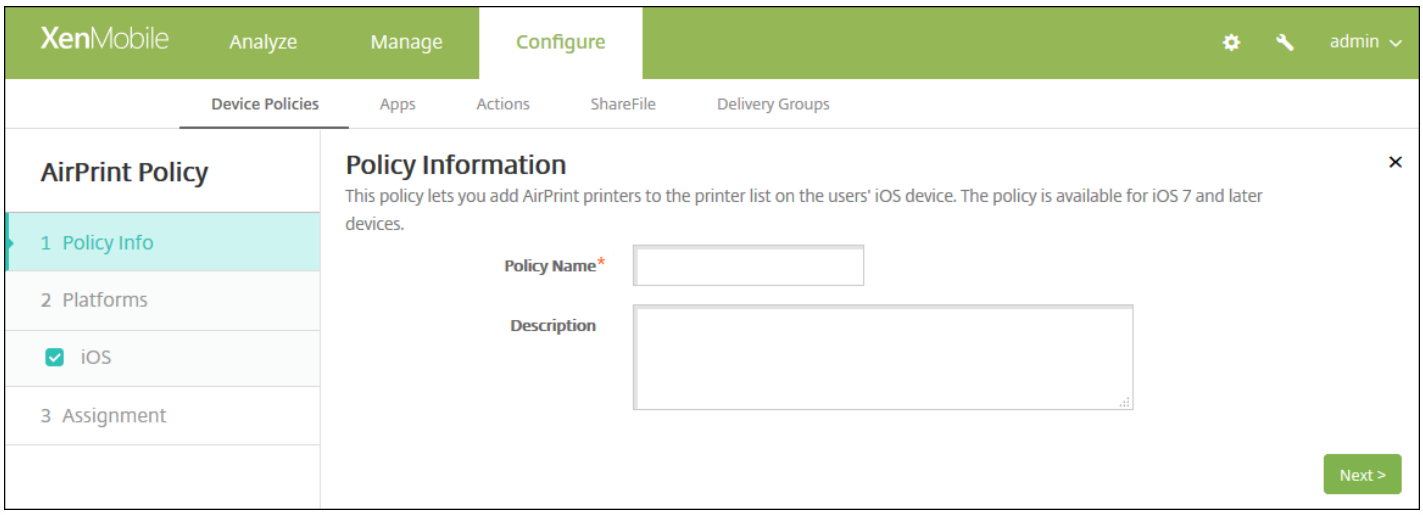
Remarque :

- Cette stratégie s'applique à iOS 7.0 et versions supérieures.
- Vérifiez que vous disposez de l'adresse IP et du chemin d'accès à la ressource pour chaque imprimante.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

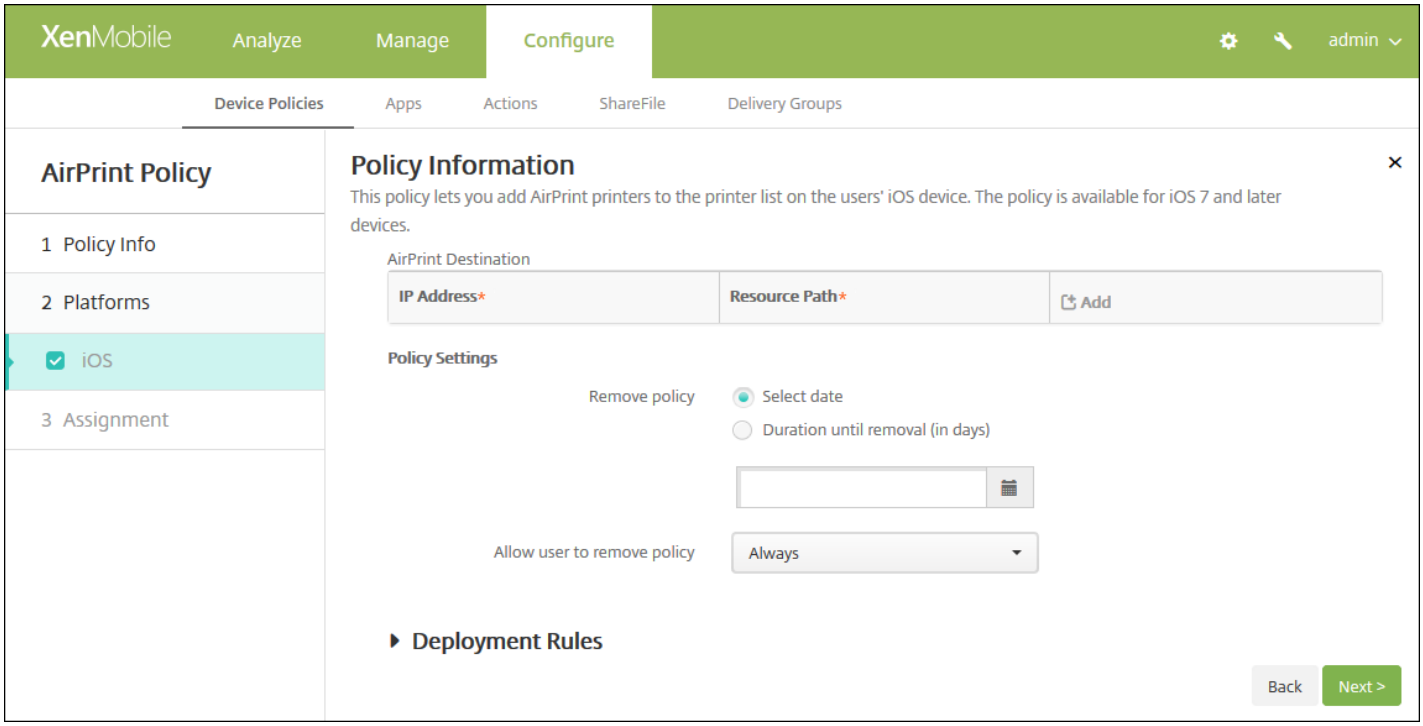
3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **AirPrint**. La page **Stratégie AirPrint** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Informations sur la plate-forme iOS** s'affiche.



6. Configurez les paramètres suivants :

- **Destination AirPrint** : pour chaque destination AirPrint que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Adresse IP** : entrez l'adresse IP de l'imprimante AirPrint.
  - **Chemin d'accès à la ressource** : entrez le chemin d'accès à la ressource associé à l'imprimante. Cette valeur correspond au paramètre de l'enregistrement Bonjour _ipps.tcp. Par exemple, imprimantes/Canon_MG5300_series ou imprimantes/Xerox_Phaser_7600.
  - Cliquez sur **Enregistrer** pour ajouter l'imprimante ou sur **Annuler** pour annuler l'ajout de l'imprimante.

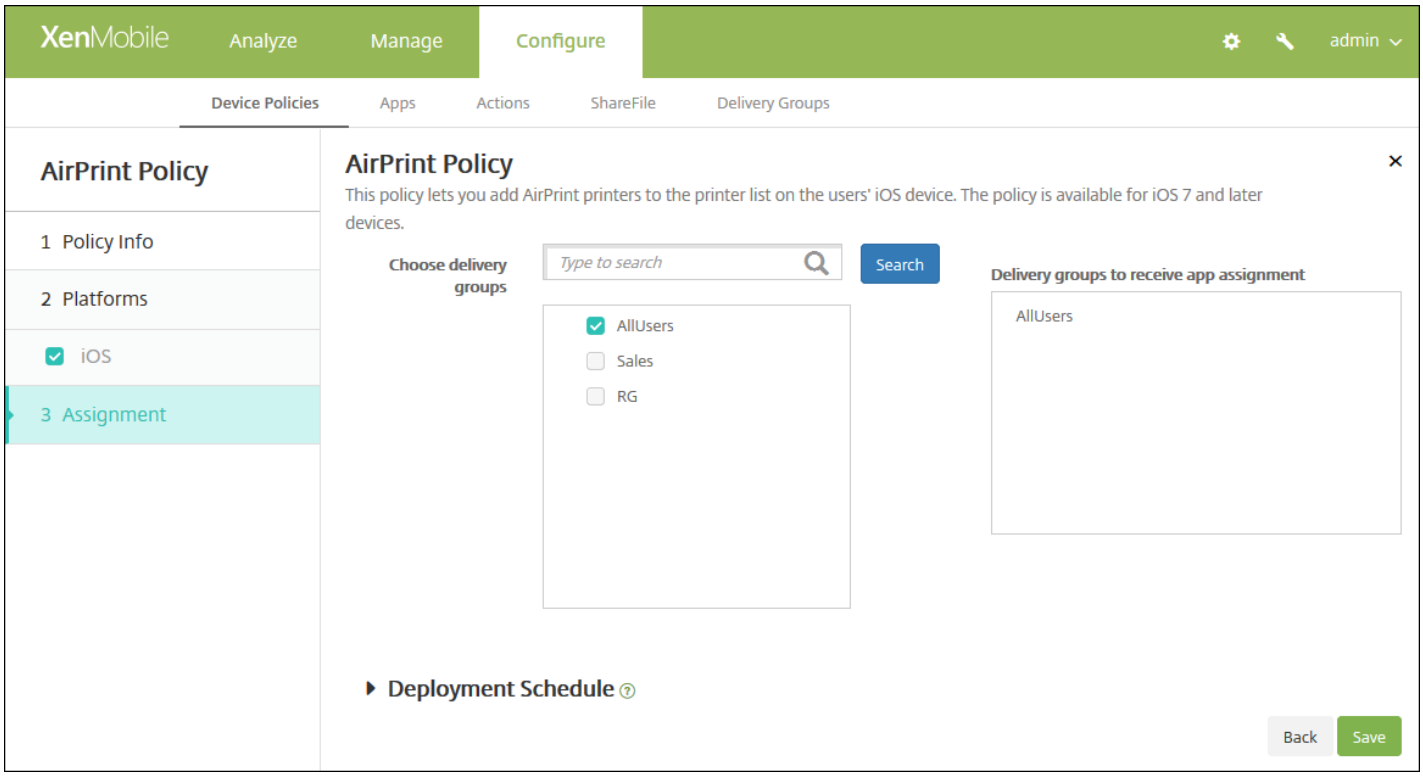
    Remarque : pour supprimer une imprimante existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

    Pour modifier une imprimante existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

- **Paramètres de stratégie**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie AirPrint** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de restrictions applicatives Android for Work

Feb 23, 2017

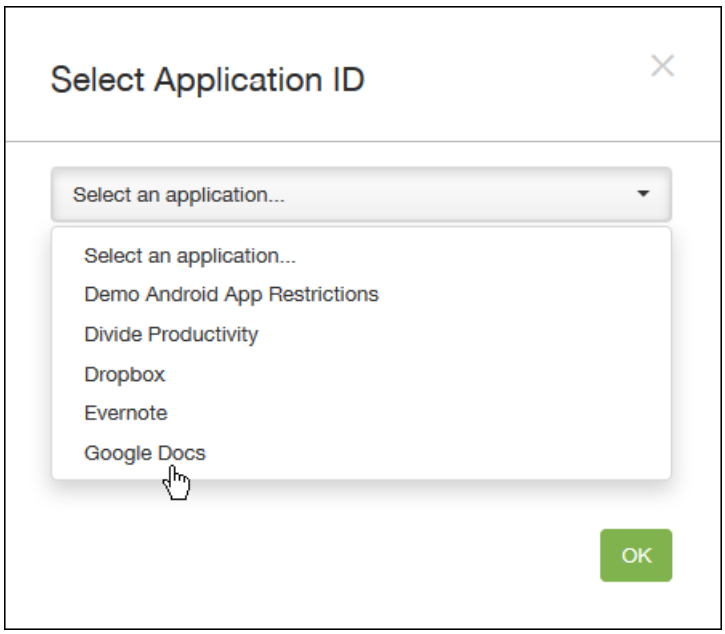
Vous pouvez modifier les restrictions associées avec les applications Android for Work, mais vous devez avant cela effectuer les actions suivantes :

- Effectuer les tâches de configuration d'Android for Work sur Google. Pour de plus amples informations, consultez la section Gestion d'appareils avec Android for Work.
- Créer un compte Android for Work. Pour de plus amples informations, consultez la section Créer un compte Android for Work.
- Ajouter des applications Android for Work à XenMobile. Pour de plus amples informations, consultez la section Ajout d'applications à XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

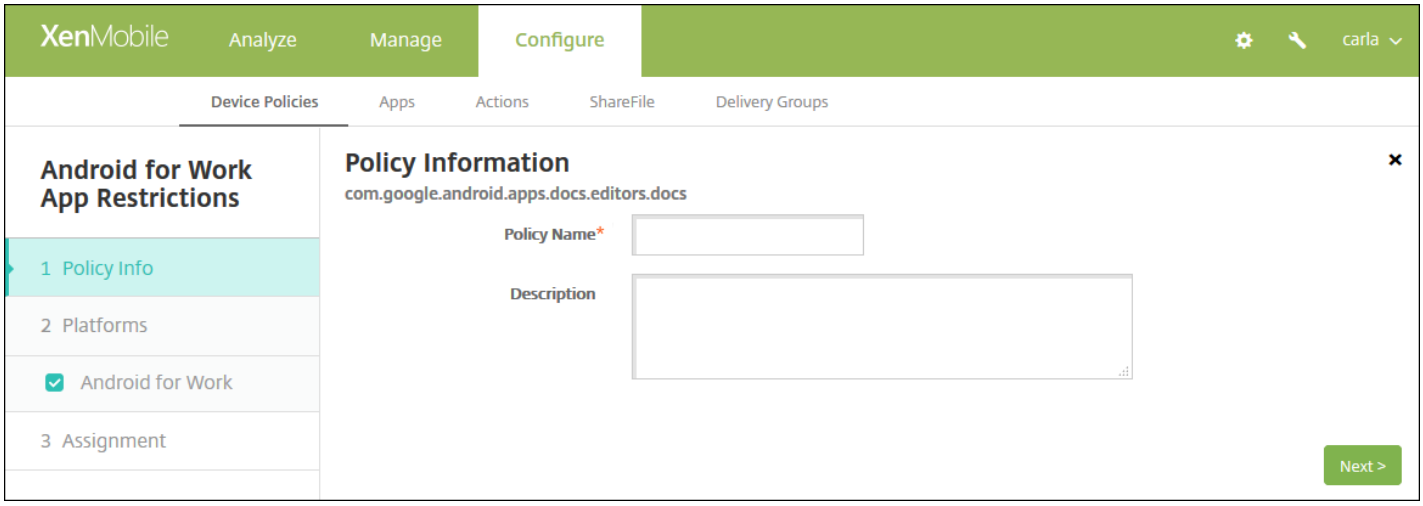
2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La page **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis sous **Sécurité**, cliquez sur **Restrictions applicatives Android for Work**. Une boîte de dialogue s'affiche, vous invitant à sélectionner une application.



4. Dans la liste, sélectionnez l'application pour laquelle vous souhaitez appliquer des restrictions, puis cliquez sur **OK**.

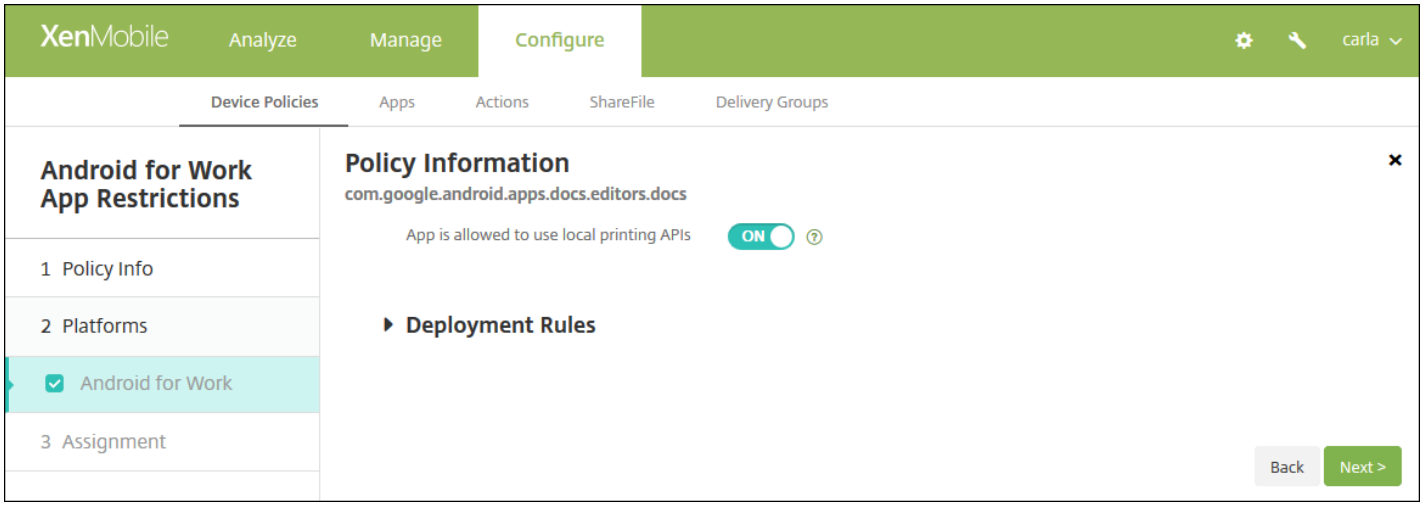
- Si aucune application Android for Work n'a été ajoutée à XenMobile, vous ne pouvez pas continuer. Pour de plus amples informations sur l'ajout d'applications à XenMobile, consultez la section Ajout d'applications à XenMobile.
- Si l'application n'est associée à aucune restriction, une notification à cet effet s'affiche. Cliquez sur **OK** pour fermer la boîte de dialogue.
- Si l'application est associée à des restrictions, la page d'informations **Stratégie de restrictions applicatives Android for Work** s'affiche.



5. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

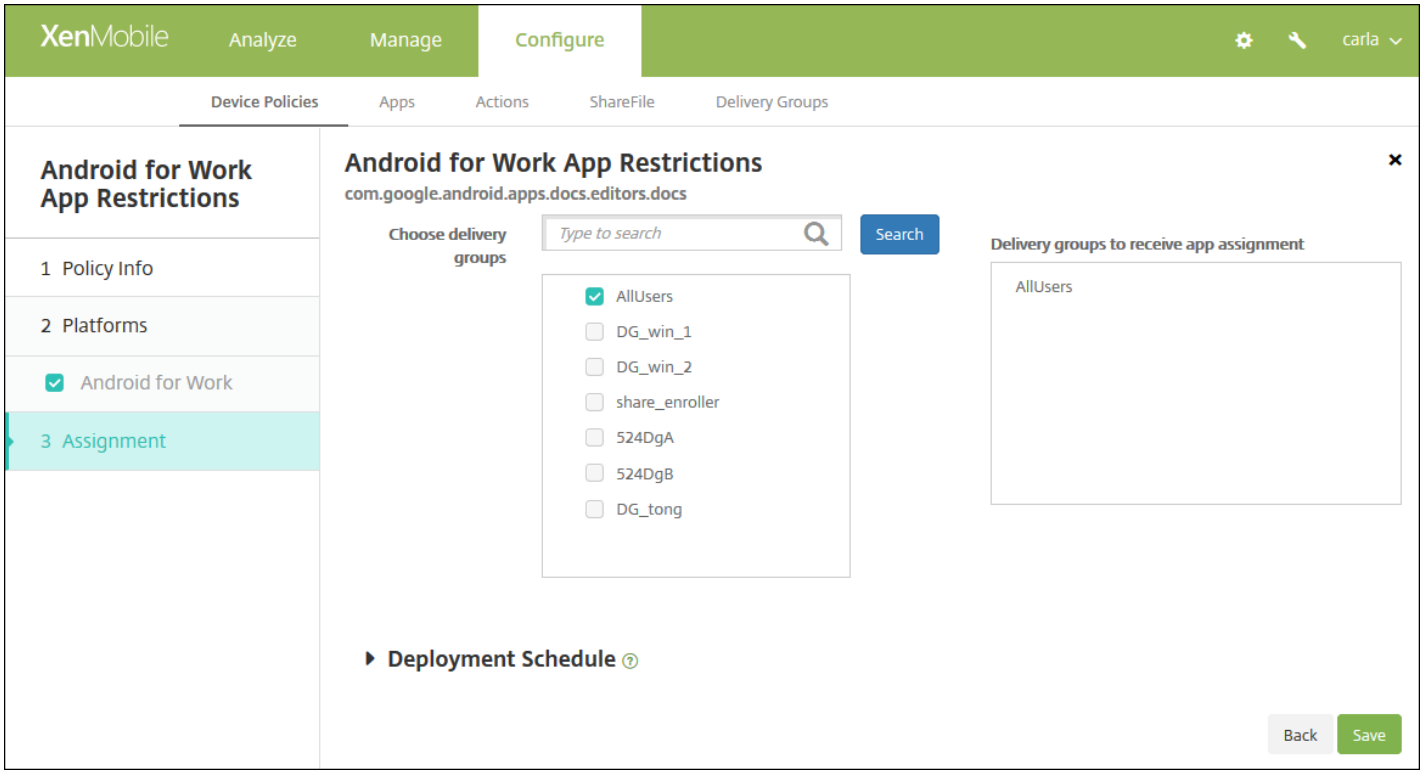
6. Cliquez sur **Next**. La page **Plate-forme Android for Work** s'affiche.



7. Configurez les paramètres pour l'application que vous avez sélectionnée. Les paramètres que vous voyez dépendent des restrictions associées à l'application sélectionnée.

8. Configurez les règles de déploiement.

9. Cliquez sur **Next**. La page d'attribution **Stratégie de restrictions applicatives Android for Work** s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas.

12. Cliquez sur **Enregistrer**.

Stratégies APN

Feb 23, 2017

Vous pouvez ajouter une stratégie de nom de point d'accès (APN) personnalisée pour iOS, Android et Windows Mobile/CE. Vous pouvez utiliser cette stratégie si votre entreprise n'utilise pas d'APN consommateur pour se connecter à Internet à partir d'un appareil mobile. Une stratégie APN détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones les plus récents.

Paramètres iOS

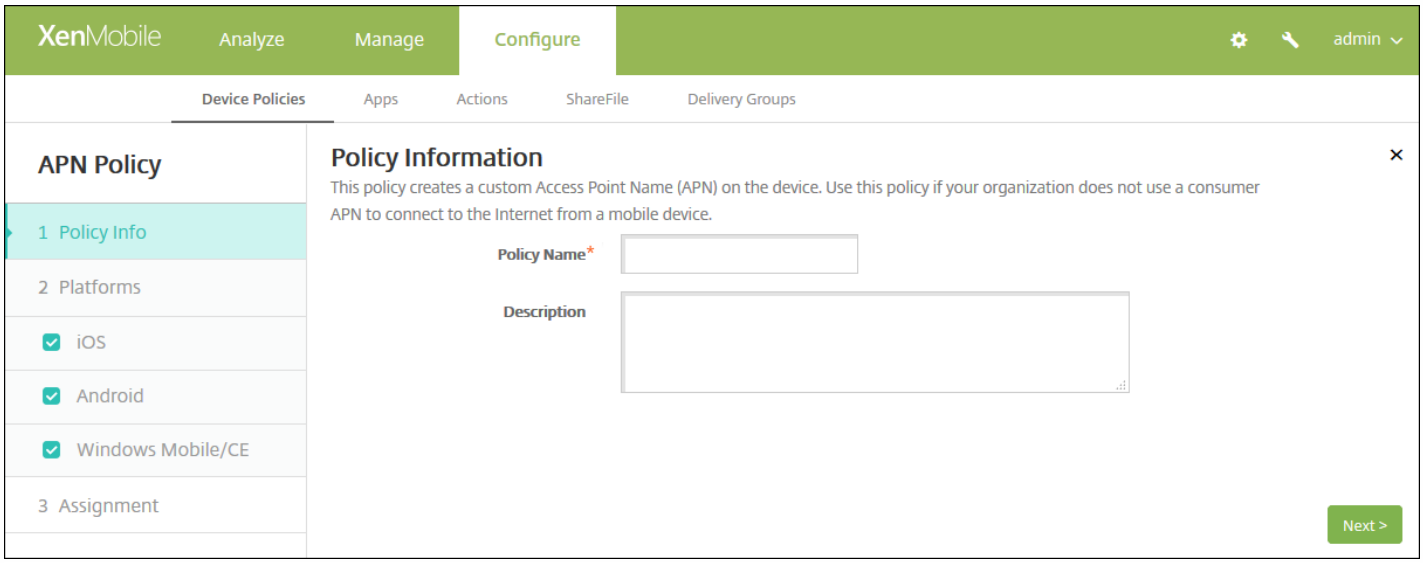
Paramètres Android

Paramètres Windows Mobile/CE

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **APN**. La page d'informations **Stratégie APN** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

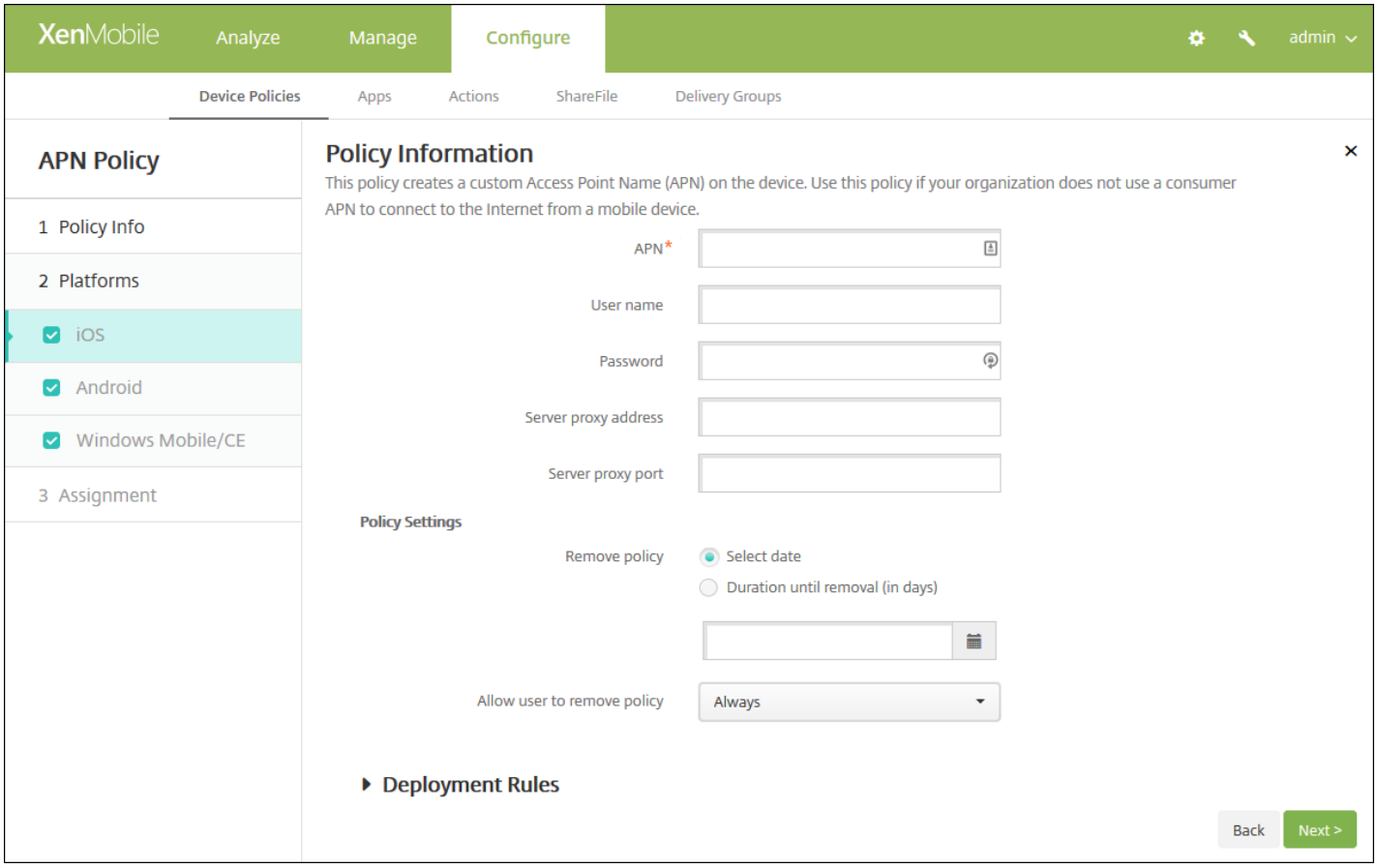
5. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.

Remarque : lorsque la page **Stratégie par plate-forme** s'affiche, toutes les plates-formes sont sélectionnées et la plate-forme iOS s'affiche en premier.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

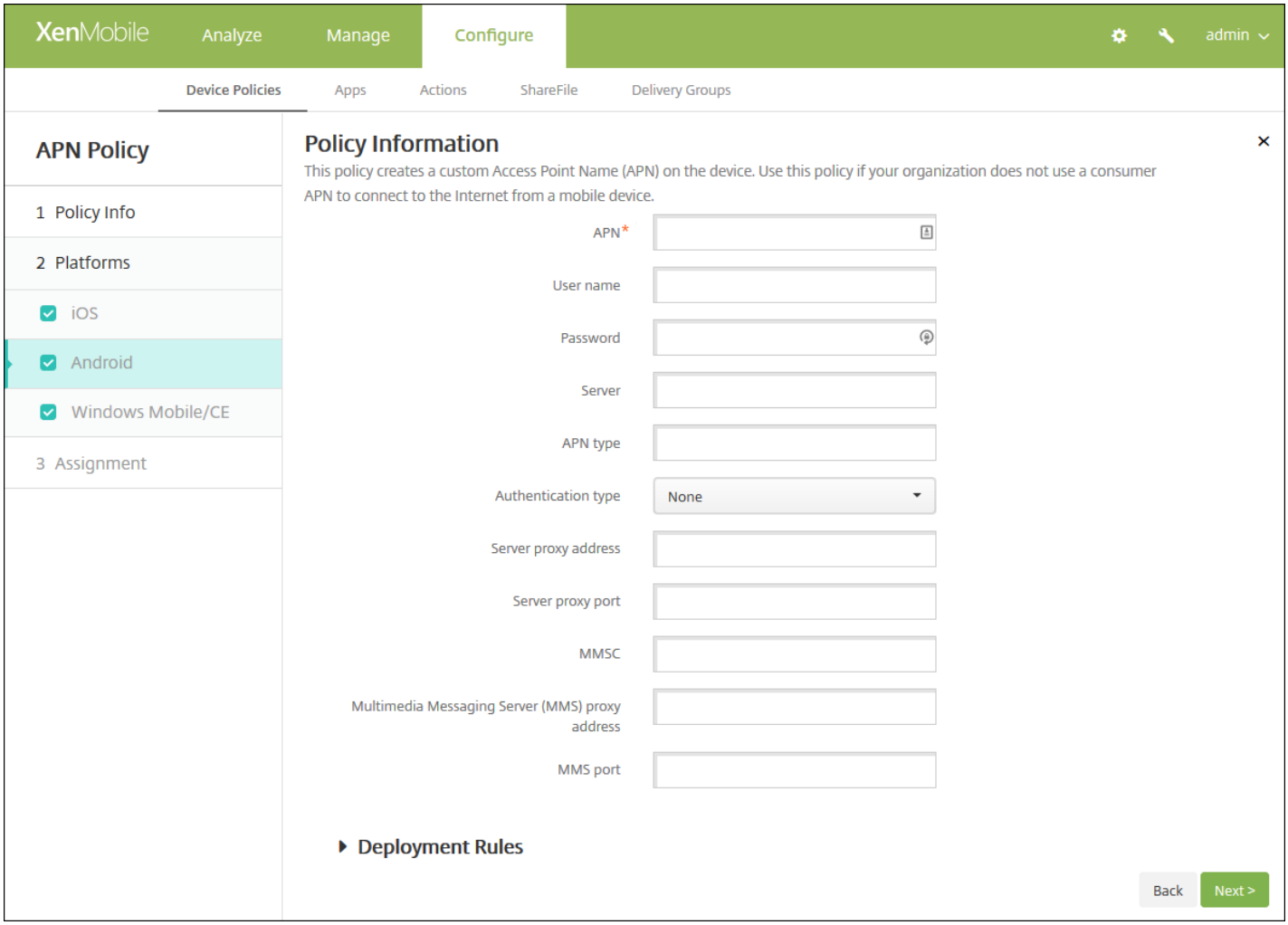
Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **APN** : entrez le nom du point d'accès. Ce dernier doit correspondre à un APN iOS accepté ou la stratégie échouera.
- **Nom d'utilisateur** : cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe** : mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Adresse du serveur proxy** : adresse IP ou adresse URL du proxy APN.
- **Port du serveur proxy** : numéro de port du proxy APN. Nécessaire que si vous avez entré une adresse de serveur proxy.
- Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Android

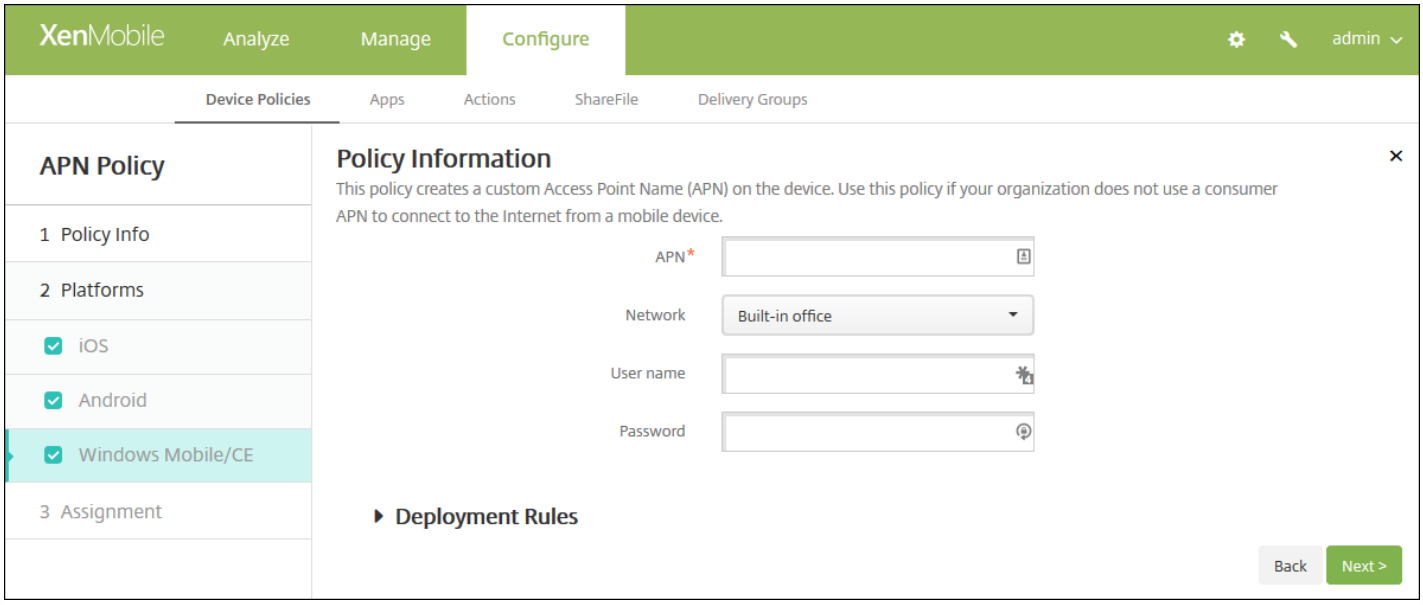


Pour configurer ces paramètres :

- **APN** : entrez le nom du point d'accès. Ce dernier doit correspondre à un APN Android accepté ou la stratégie échouera.
- **Nom d'utilisateur** : cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe** : mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.
- **Serveur** : ce paramètre, antérieur à l'arrivée des smartphones, est généralement vide. Il fait référence à un serveur de passerelle WAP (Wireless Application Protocol) pour les téléphones qui ne pouvaient pas accéder ou restituer des sites Web standard.
- **Type d'APN** : ce paramètre doit s'aligner avec l'utilisation prévue par l'opérateur du point d'accès. Il s'agit d'une chaîne délimitée par des virgules des spécificateurs de service APN et doit correspondre aux définitions publiées de l'opérateur sans fil. Exemples :
  - *. Tout le trafic transite via ce point d'accès.
  - mms. Le trafic multimédia transite via ce point d'accès.
  - default. Tout le trafic, y compris le multimédia, transite via ce point d'accès.
  - supl. Le protocole SUPL est associé au GPS assisté.
  - dun. L'accès réseau à distance est obsolète et rarement utilisé.
  - hipri. Réseau haute priorité.
  - fota. FOTA (Firmware over the air) est utilisé pour recevoir les mises à jour du firmware.

- **Type d'authentification** : dans la liste, cliquez sur le type d'authentification à utiliser. Valeur par défaut Aucun.
- **Adresse du serveur proxy** : adresse IP ou adresse URL du proxy HTTP APN de l'opérateur.
- **Port du serveur proxy** : numéro de port du proxy APN. Nécessaire que si vous avez entré une adresse de serveur proxy.
- **MMSC** : adresse du serveur MMS fournie par l'opérateur.
- **Adresse du proxy MMS** : serveur du service de messagerie pour le trafic MMS. MMS a succédé à SMS pour l'envoi de messages plus volumineux avec du contenu multimédia, tels que des images ou des vidéos. Ces serveurs nécessitent des protocoles spécifiques (tels que MM1, ... MM11).
- **Port MMS** : port utilisé par le proxy MMS.

Configurer les paramètres pour Windows Mobile/CE

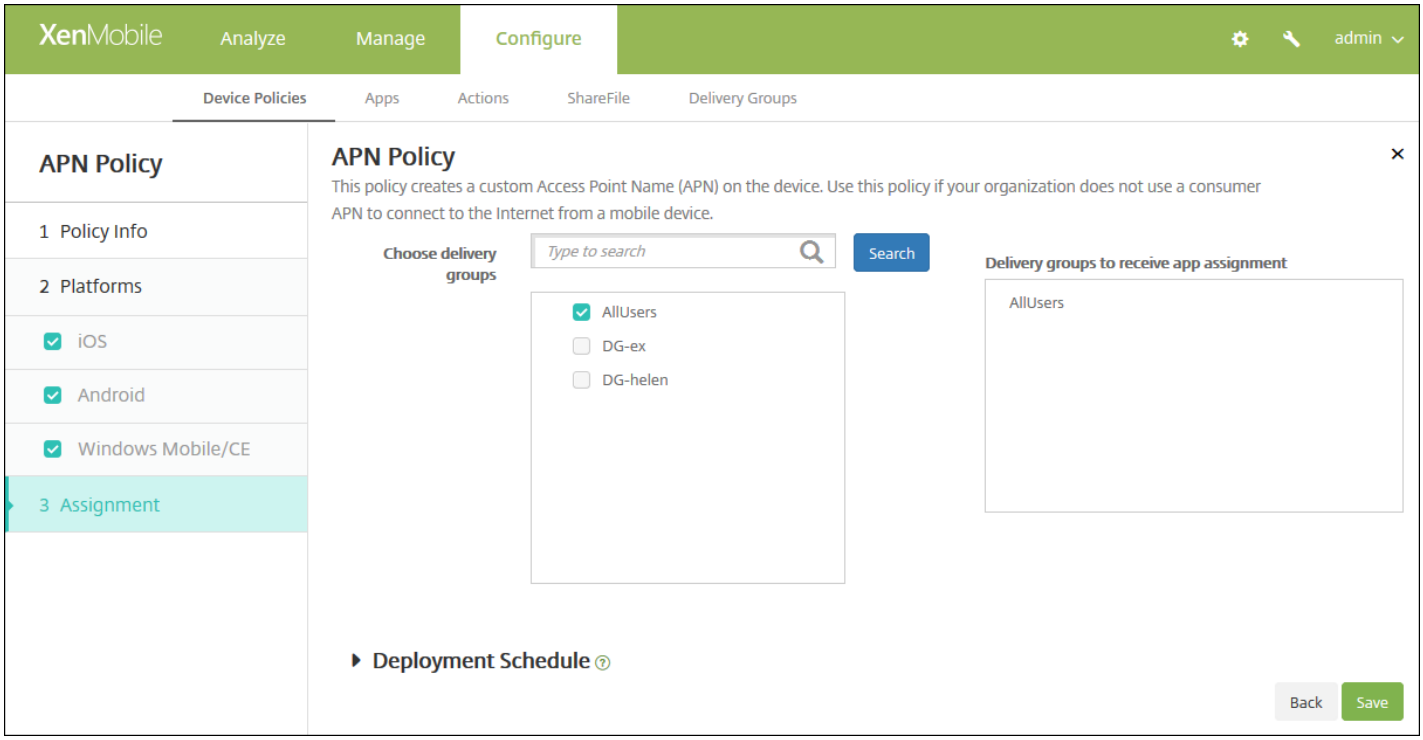


Configurez les paramètres suivants :

- **APN** : entrez le nom du point d'accès. Ce dernier doit correspondre à un APN Android accepté ou la stratégie échouera.
- **Réseau** : dans la liste, cliquez sur le type de réseau à utiliser. La valeur par défaut est **Bureau intégré**.
- **Nom d'utilisateur** : cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
- **Mot de passe** : mot de passe utilisateur pour ce point d'accès. Afin de masquer le mot de passe, ce dernier est codé. S'il est manquant dans la charge utile, l'appareil vous invite à le saisir lors de l'installation du profil.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie APN** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

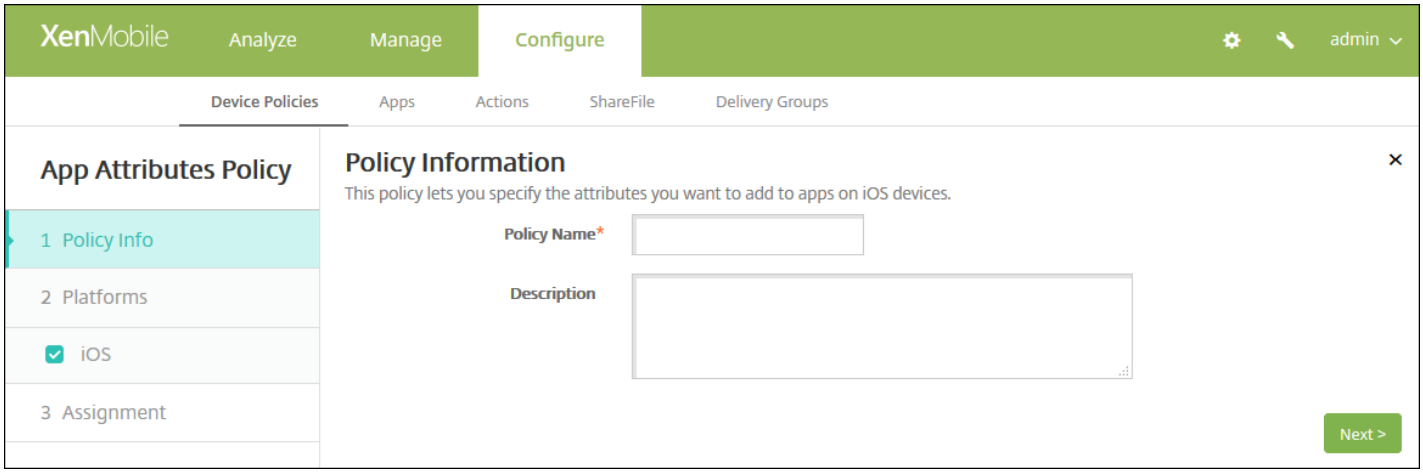
- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégie d'attributs d'application

Feb 23, 2017

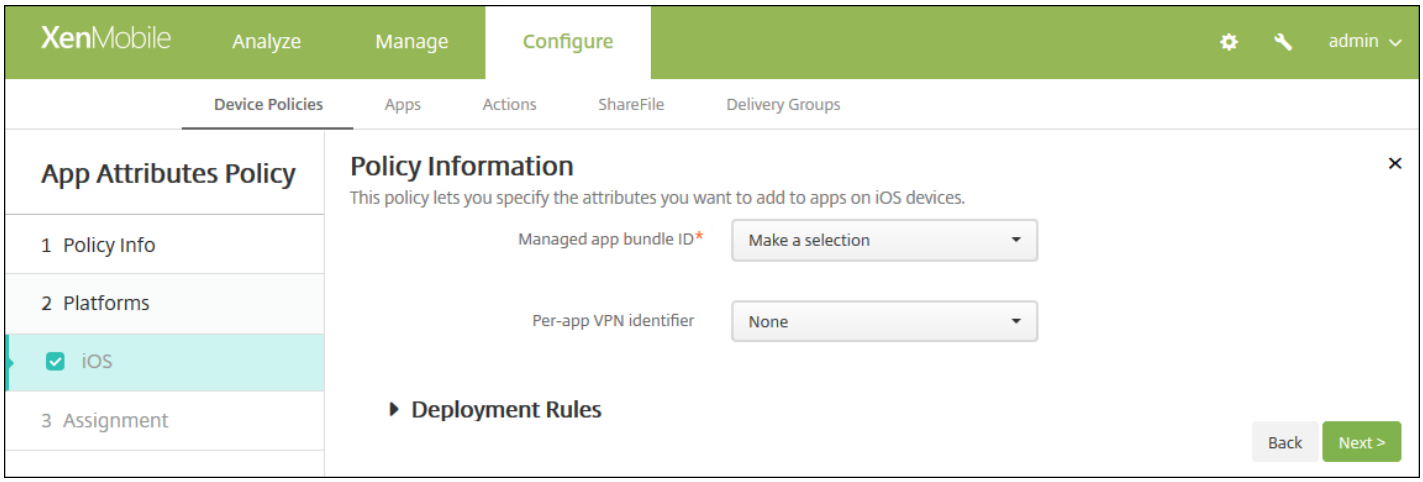
La stratégie Attributs d'application vous permet de spécifier des attributs, tels qu'un Bundle ID d'application gérée, ou un identifiant VPN par application pour les appareils iOS.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Attributs d'application** s'affiche.

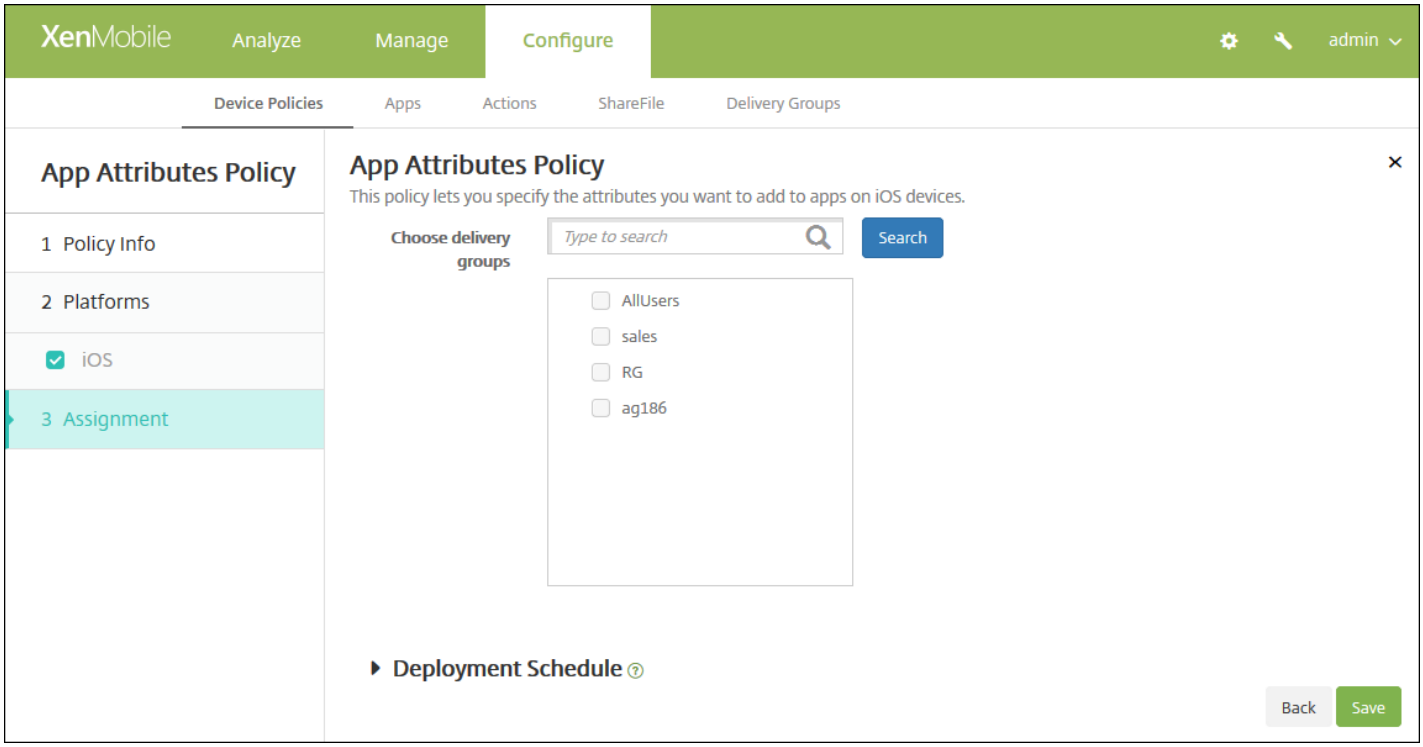


6. Configurez les paramètres suivants :

- **Bundle ID d'application gérée :** dans la liste, cliquez sur un bundle ID d'application ou cliquez sur **Ajouter**.
  - Si vous cliquez sur **Ajouter**, entrez le bundle ID d'application dans le champ qui s'affiche.
- **Identifiant Per App VPN** : dans la liste, cliquez sur l'identifiant Per App VPN.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la Stratégie d'attributs d'application s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans Paramètres > Propriétés du serveur. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de Déployer pour les connexions permanentes, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies d'accès aux applications

Feb 23, 2017

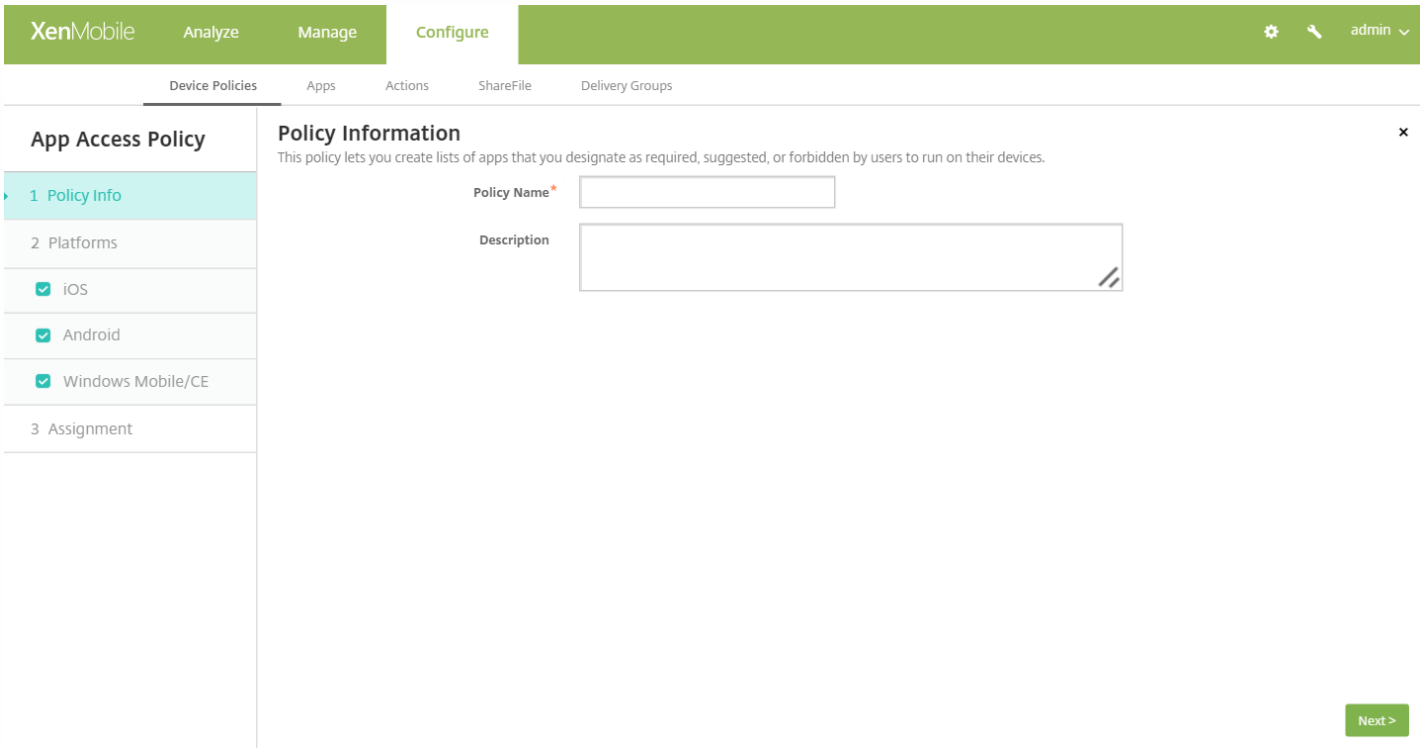
La stratégie d'accès aux applications dans XenMobile vous permet de définir une liste d'applications dont l'installation sur les appareils est obligatoire, facultative ou interdite. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport à cette liste d'applications. Vous pouvez créer des stratégies d'accès aux applications pour iOS, Android et Windows Mobile/CE.

Vous ne pouvez configurer qu'un type de stratégie d'accès à la fois. Vous pouvez ajouter une stratégie pour une liste d'applications obligatoires, d'applications suggérées ou d'applications interdites, mais vous ne pouvez pas combiner ces trois types de liste au sein de la même stratégie d'accès. Si vous créez une stratégie pour chaque type de liste, il est conseillé de nommer chaque stratégie avec soin, afin de pouvoir déterminer à quelle stratégie la liste des applications s'applique dans XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Applications**, cliquez sur **Accès aux applications**. La page d'informations sur la **Stratégie d'accès aux applications** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.

Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme,

désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

6. Configurez les paramètres suivants pour chaque plate-forme que vous avez sélectionnée.

- **Stratégie d'accès** : cliquez sur Requise, Suggérée ou Interdite. La valeur par défaut est Requise.
- Pour ajouter une ou plusieurs applications à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom app** : entrez un nom pour l'application.
  - **Identifiant app** : entrez un identifiant pour l'application (facultatif).
  - Cliquez sur **Enregistrer** ou sur **Annuler**.
  - Répétez ces étapes pour chaque application à ajouter.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur Next. La page de plate-forme suivante ou la page d'attribution **Stratégie d'accès aux applications** s'affiche.

9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de configuration d'application

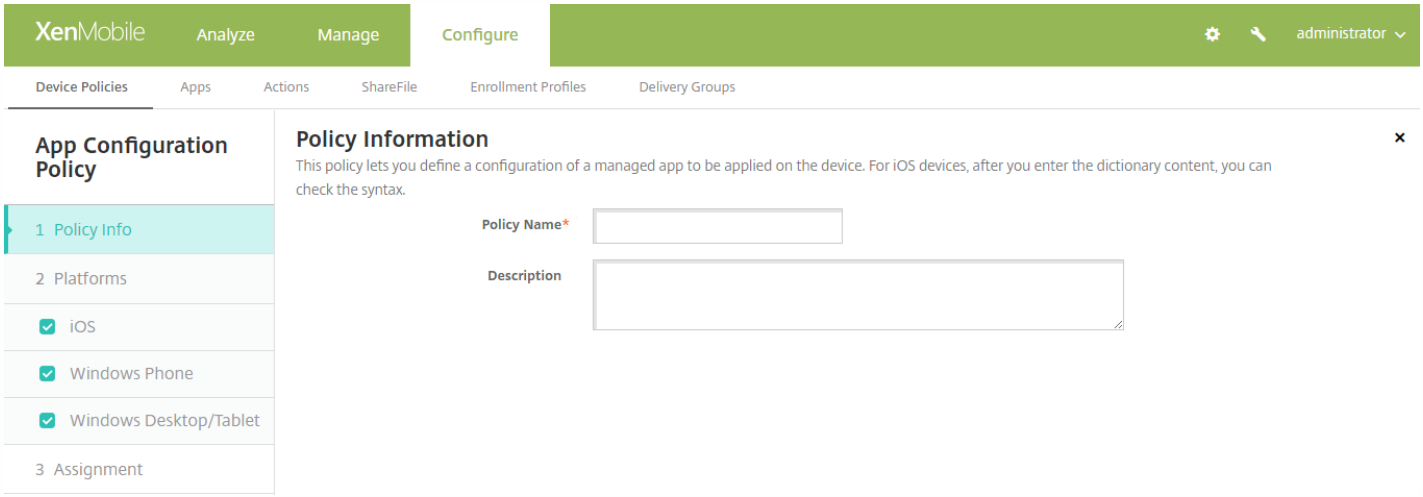
Feb 23, 2017

Vous pouvez configurer à distance des applications qui prennent en charge la configuration gérée par le déploiement d'un fichier de configuration XML (appelé liste de propriétés, ou plist) sur les appareils iOS des utilisateurs ou des paires clé/valeur pour les téléphones, tablettes ou ordinateurs Windows 10. La configuration spécifie différents paramètres et comportements dans l'application. XenMobile force la configuration sur les appareils lorsque l'utilisateur installe l'application. Les paramètres et les comportements que vous pouvez configurer dépendent de l'application et ne sont pas couverts dans cet article.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Applications**, cliquez sur **Configuration appli**. La page d'informations sur la **Stratégie de configuration d'application** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

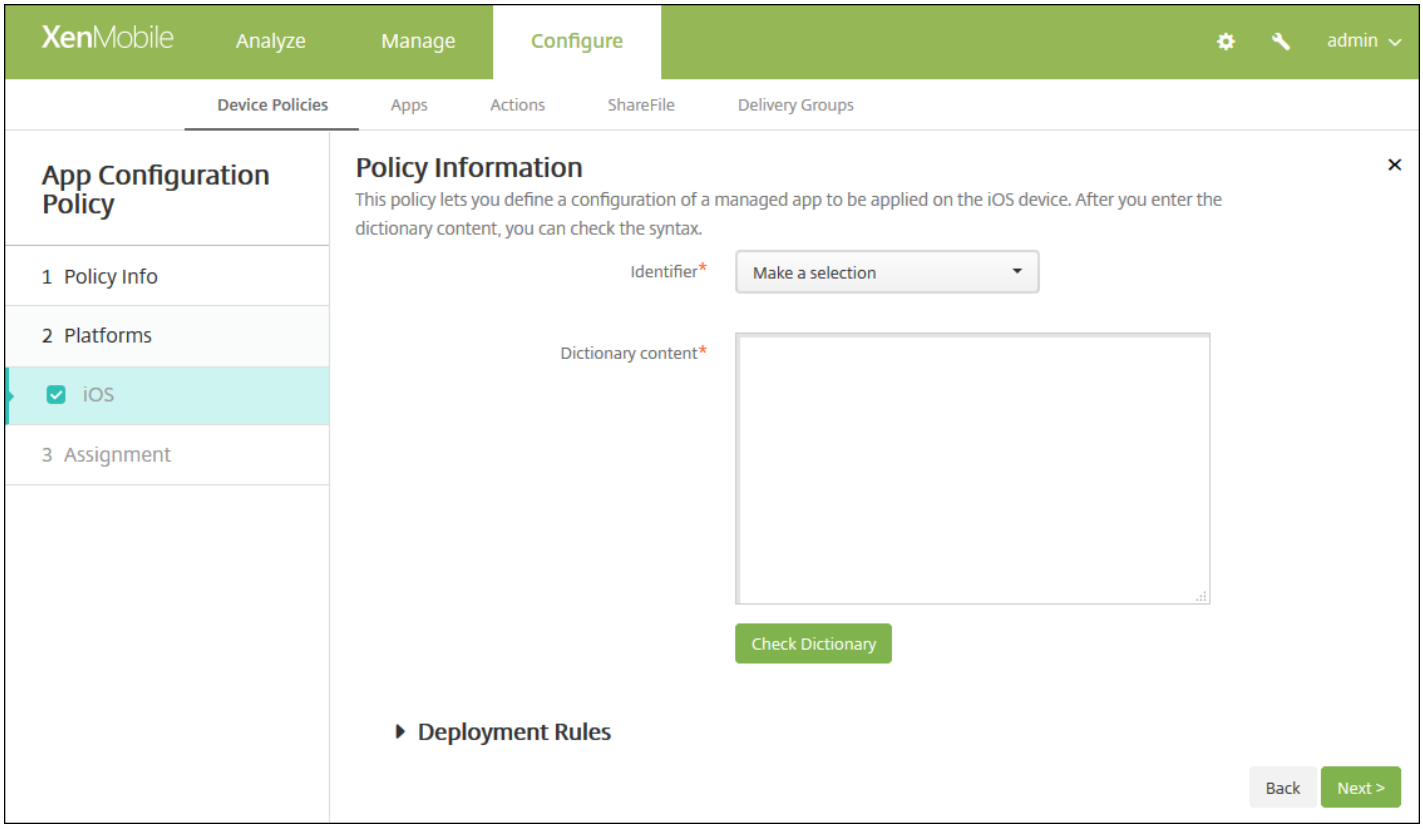
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

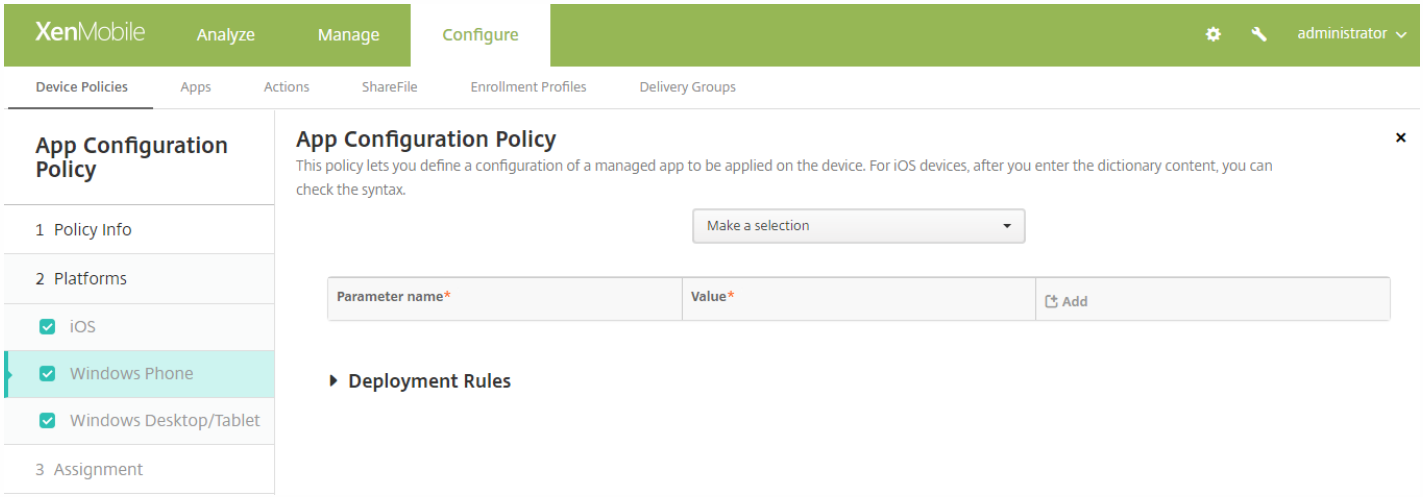
Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

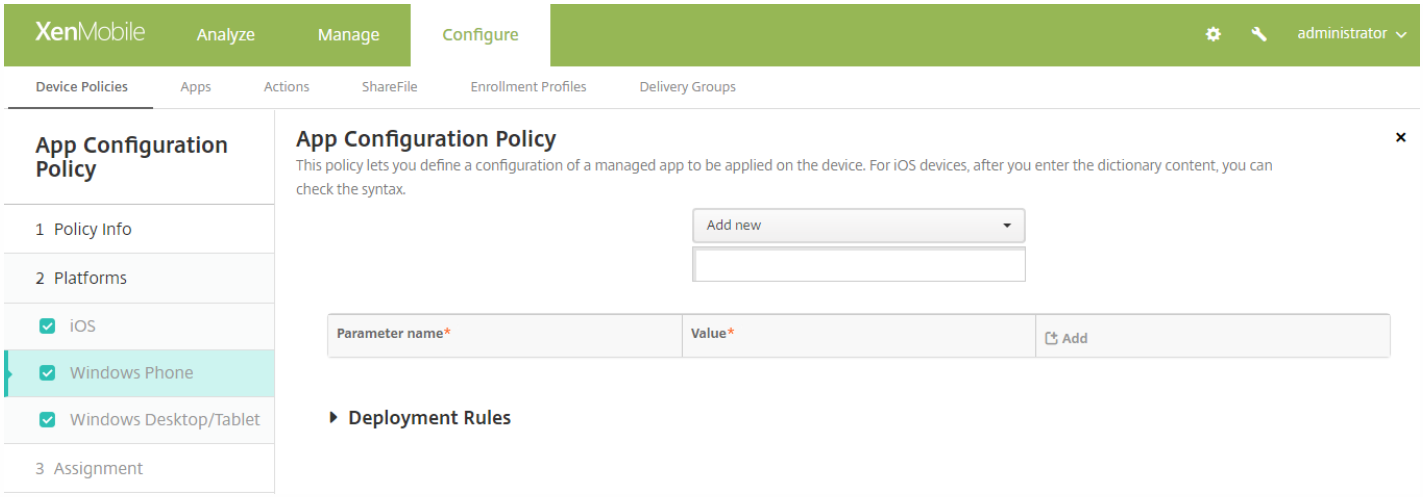
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 6 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



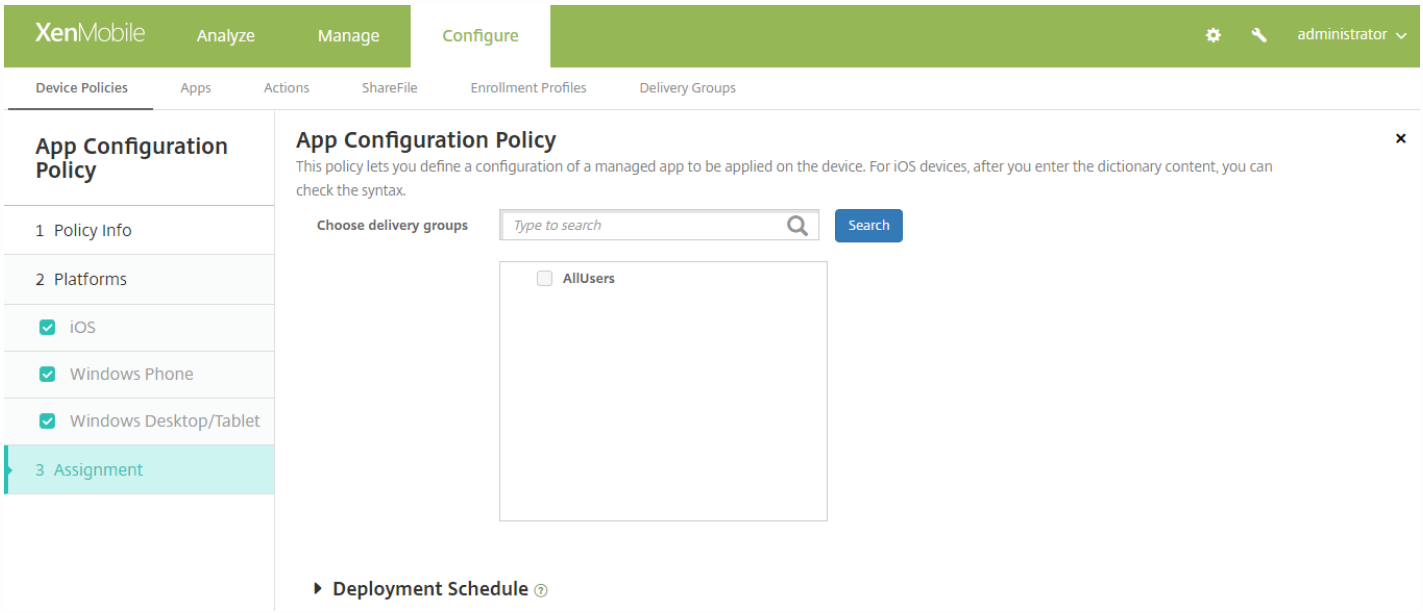
Configurer les paramètres pour Windows Phone ou Desktop/Tablet





6. Configurez les règles de déploiement.

7. Cliquez sur **Next**. La page d'attribution **Stratégie de configuration d'application** s'affiche.



8. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

9. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

10. Cliquez sur **Enregistrer**.

Stratégies d'inventaire des applications

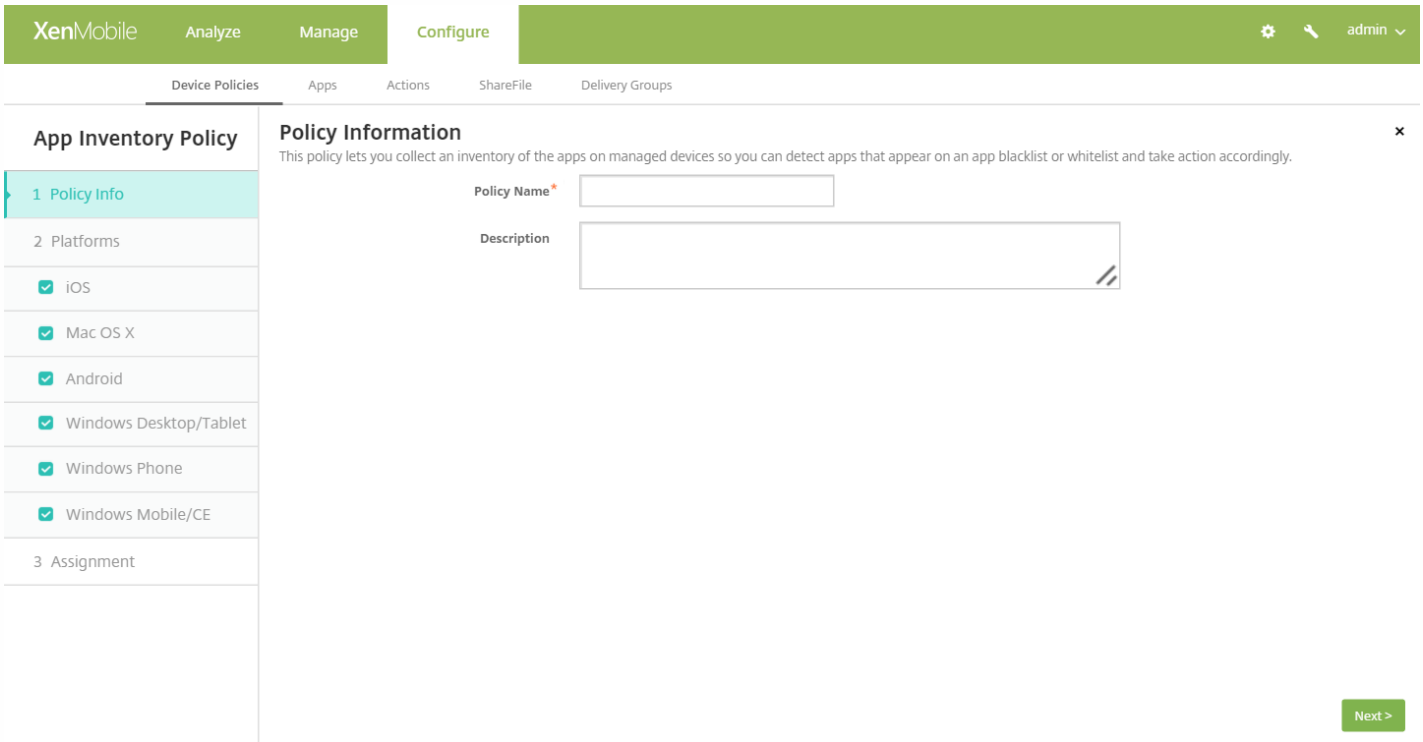
Feb 23, 2017

Une stratégie d'inventaire des applications dans XenMobile vous permet d'établir un inventaire des applications sur les appareils gérés, puis l'inventaire est comparé aux stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste noire (interdites dans une stratégie d'accès aux applications) ou blanche (requis dans une stratégie d'accès aux applications) et prendre les mesures qui s'imposent. Vous pouvez créer des stratégies d'accès aux applications pour les appareils iOS, Mac OS X, Android (y compris pour les appareils activés pour Android for Work), Windows Desktop/Tablet, Windows Phone ou Windows Mobile/CE.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

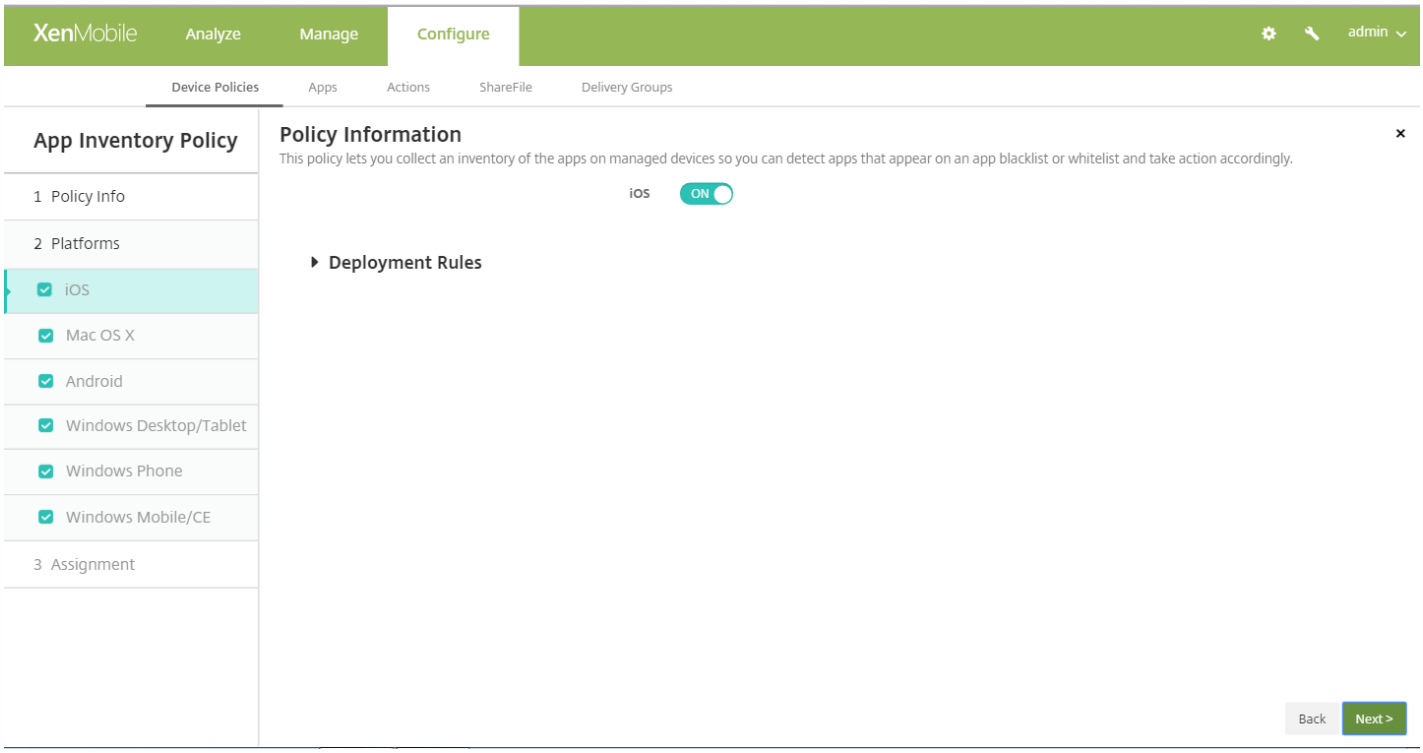
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Stratégie d'inventaire**. La page **Stratégie d'inventaire des applications** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



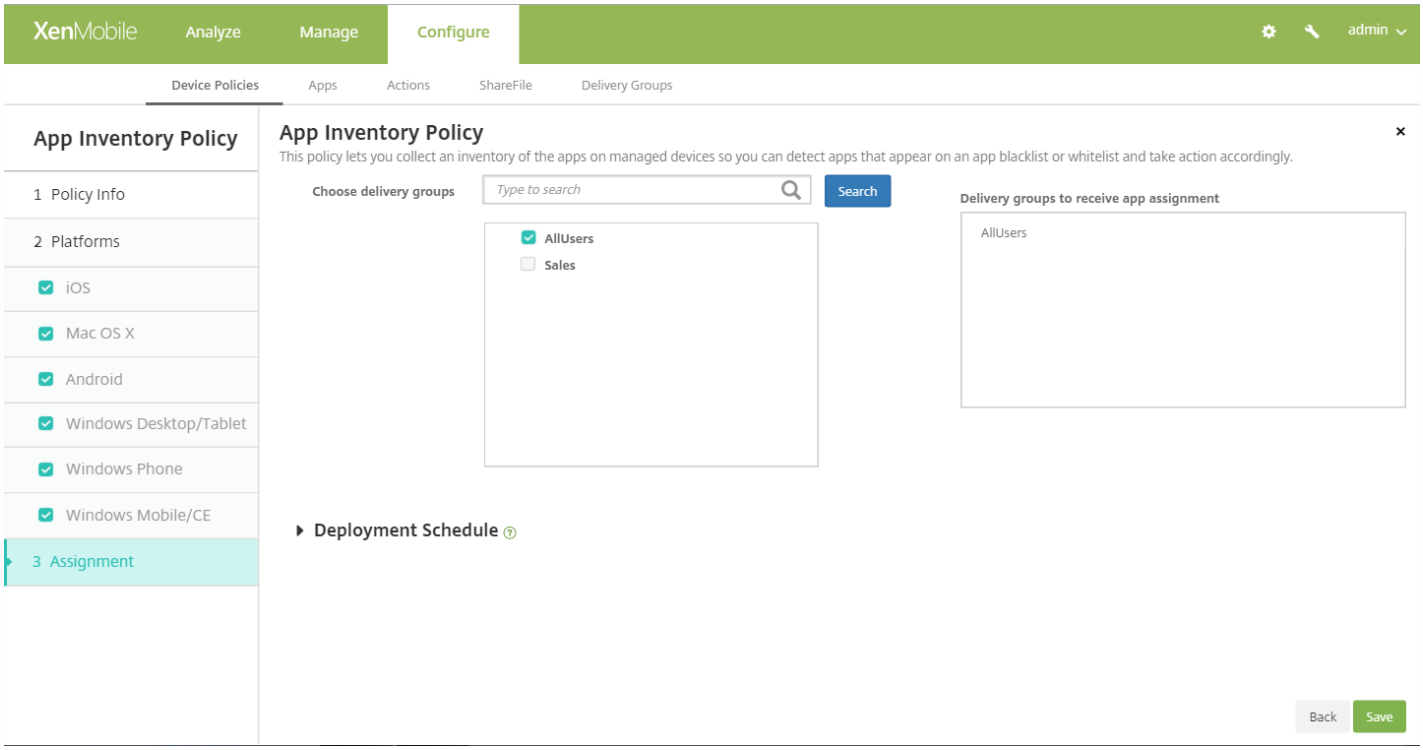
Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

6. Pour chaque plate-forme que vous sélectionnez, conservez le paramètre par défaut ou modifiez le paramètre (**OFF**). La valeur par défaut est **ON**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'inventaire des applications** s'affiche.



9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

10. Développez Calendrier de déploiement et configurez les paramètres suivants :

- En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
- En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
- Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement précédent a échoué. L'option par défaut est À chaque connexion.
- En regard de Déployer pour les connexions permanentes, cliquez sur ON ou OFF. L'option par défaut est OFF.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de mode kiosque

Feb 23, 2017

Vous pouvez créer une stratégie dans XenMobile afin de définir une liste d'applications dont l'exécution est autorisée ou interdite sur un appareil. Vous pouvez configurer cette stratégie pour les appareils iOS et Android, mais la manière dont la stratégie fonctionne diffère pour chaque plate-forme. Par exemple, vous pouvez bloquer plusieurs applications sur un appareil iOS.

De même, pour les appareils iOS, vous pouvez sélectionner une seule application iOS par stratégie. Cela signifie que les utilisateurs peuvent uniquement utiliser leurs appareils pour exécuter une seule application. Ils ne peuvent effectuer aucune autre activité sur l'appareil, à l'exception des options que vous avez spécifiquement autorisées lorsque la stratégie de mode kiosque est appliquée.

En outre, les appareils iOS doivent être supervisés pour pouvoir transmettre des stratégies de verrouillage d'applications.

Bien que la stratégie d'appareil fonctionne sur la plupart des appareils Android L et M, le verrouillage d'applications ne fonctionne pas sur les appareils Android N ou plus récents en raison de l'abandon par Google de l'API requise.

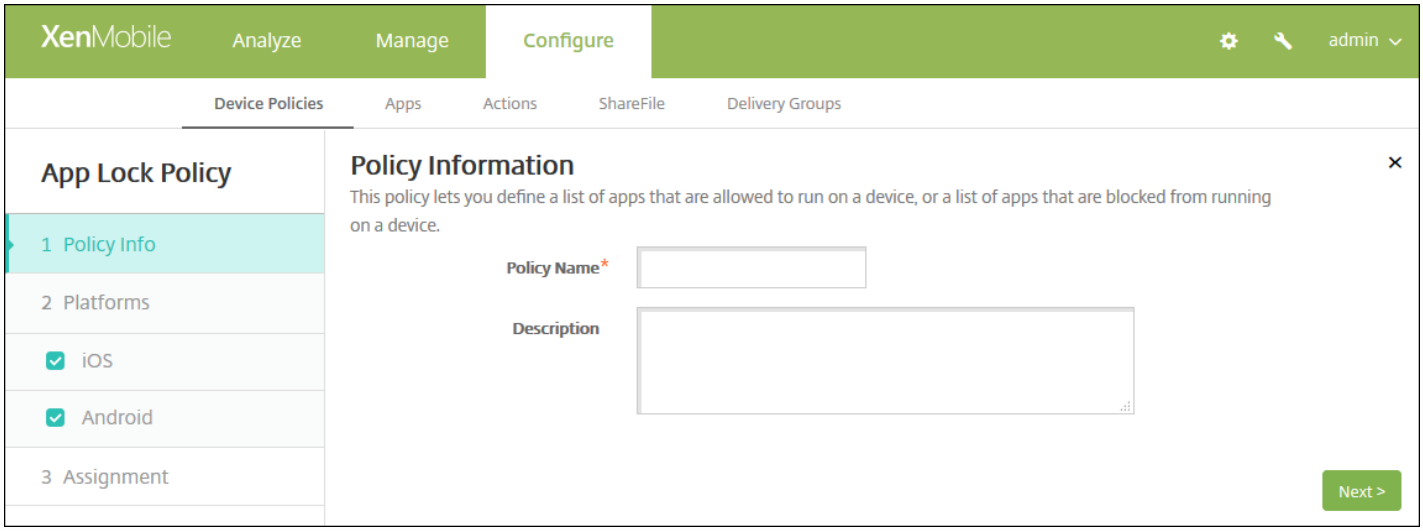
Paramètres iOS

Paramètres Android

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Mode kiosque**. La page **Stratégie de mode kiosque** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

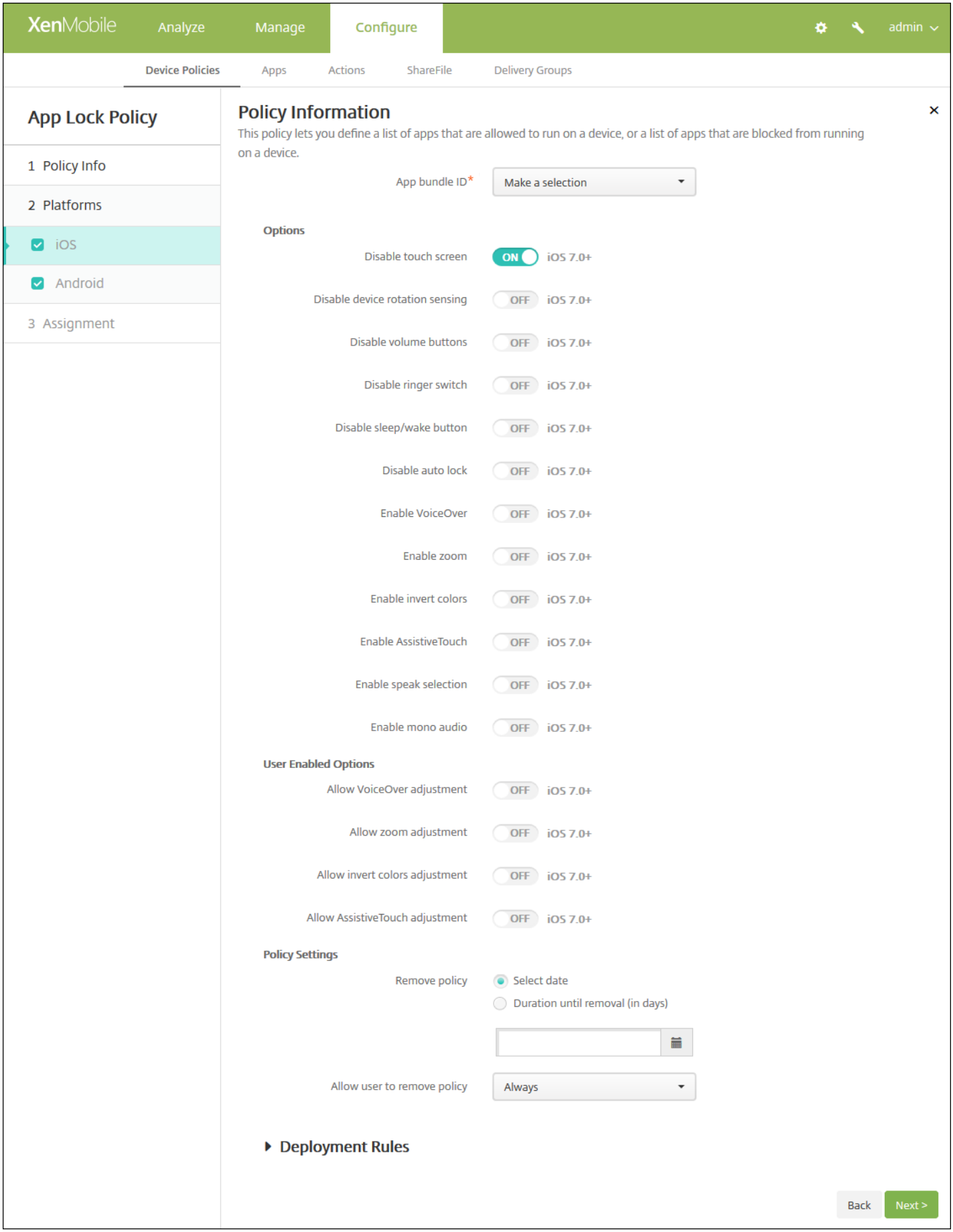
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

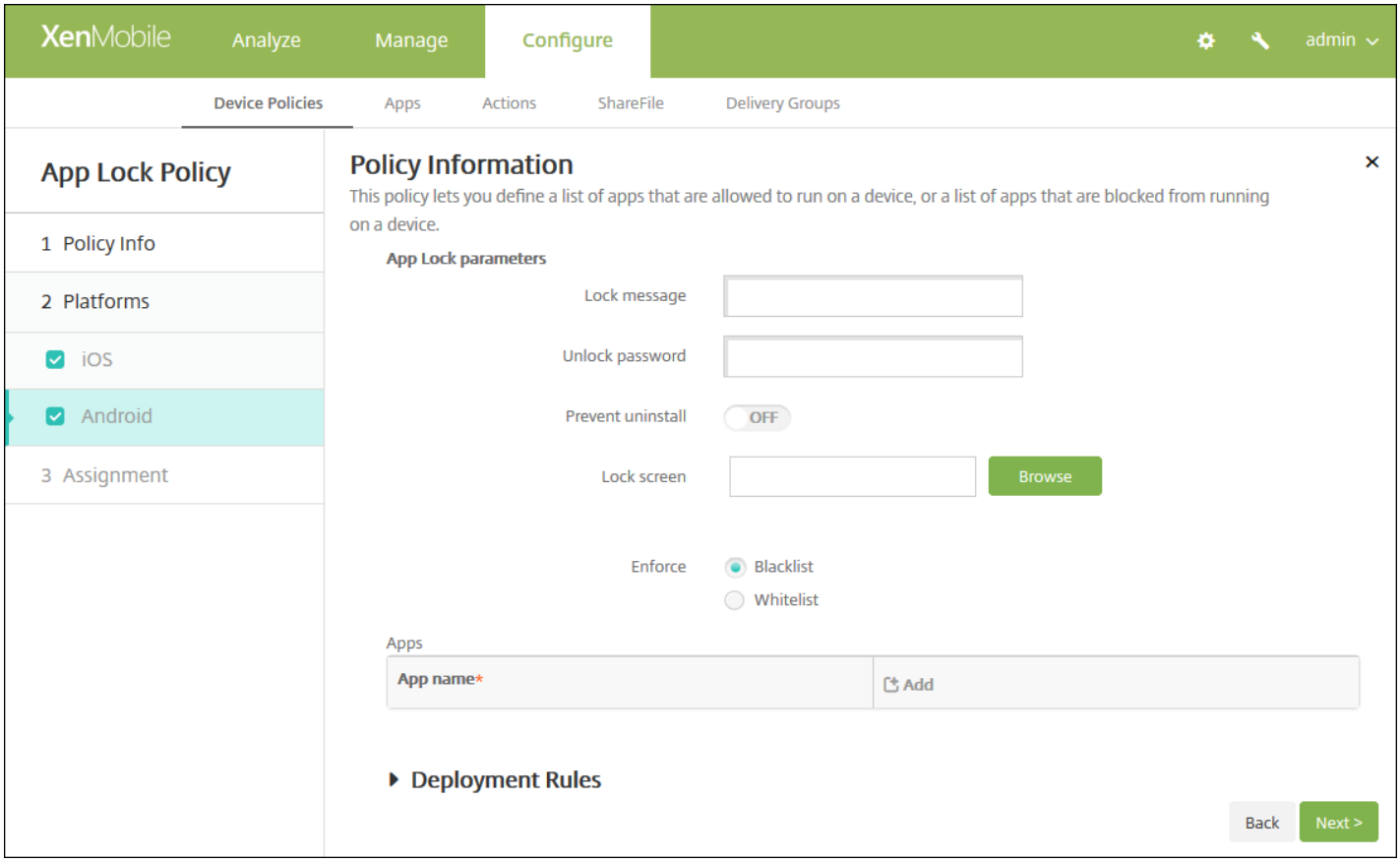
Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **Bundle ID d'application** : dans la liste, cliquez sur l'application à laquelle cette stratégie s'applique, ou cliquez sur **Ajouter** pour ajouter une application à la liste. Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
- **Options** : chacune des options suivantes s'applique uniquement à iOS 7.0 ou version ultérieure. Pour chaque option, la valeur par défaut est **OFF**, sauf pour Désactiver l'écran tactile, qui est réglée par défaut sur **ON**.
  - Désactiver l'écran tactile
  - Désactiver détection de rotation
  - Désactiver boutons volume
  - Désactiver bouton sonnerie - **Remarque** : lorsque cette option est désactivée, le comportement de la sonnerie dépend de la position dans laquelle se trouvait le bouton lorsqu'il a été désactivé.
  - Désactiver le bouton veille
  - Désactiver verrouillage auto
  - Désactiver VoiceOver
  - Activer zoom
  - Activer l'inversion de couleurs
  - Activer AssistiveTouch
  - Activer Énoncer la sélection
  - Activer l'audio mono
- **Options utilisateur** : chacune des options suivantes s'applique uniquement à iOS 7.0 ou version ultérieure. Pour chaque option, la valeur par défaut est **OFF**.
  - Autoriser le réglage de VoiceOver
  - Autoriser le réglage du zoom
  - Autoriser le réglage d'inversion des couleurs
  - Autoriser le réglage Assistive Touch
- **Paramètres de stratégie**
  - o En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - o Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - o Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - o Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Android



Pour configurer ces paramètres :

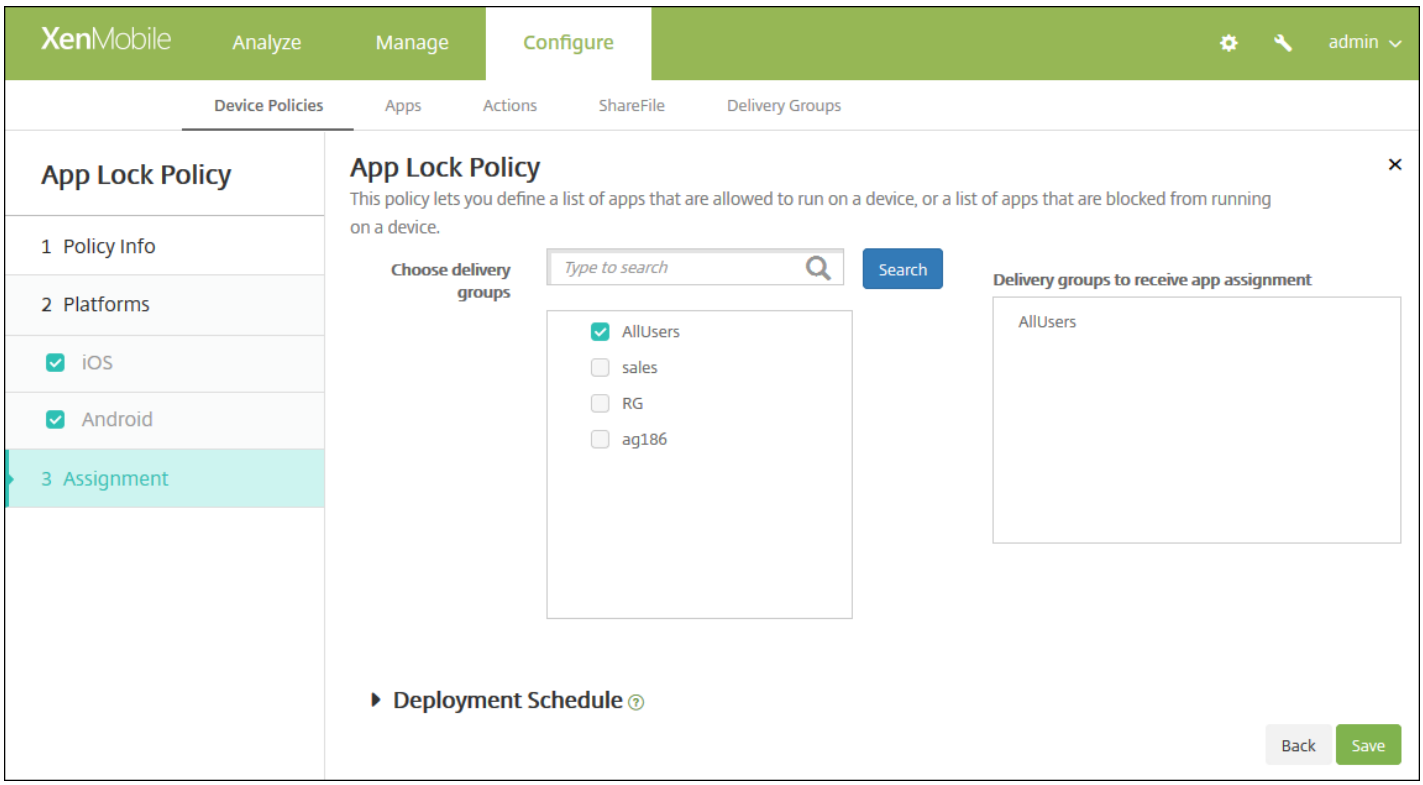
- **Paramètres du mode kiosque**
  - **Message de verrouillage** : entrez un message que les utilisateurs voient lorsqu'ils tentent d'ouvrir une application en mode kiosque.
  - **Mot de passe de déblocage** : entrez le mot de passe pour déverrouiller l'application.
  - **Empêcher la désinstallation** : indiquez si les utilisateurs sont autorisés à désinstaller les applications. La valeur par défaut est **OFF**.
  - **Écran de verrouillage** : sélectionnez l'image qui s'affiche sur l'écran de verrouillage de l'appareil en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
  - **Appliquer** : cliquez sur **Liste noire** pour créer une liste d'applications qui ne sont pas autorisées à s'exécuter sur les appareils ou cliquez sur **Liste blanche** pour créer une liste d'applications qui sont autorisées à s'exécuter sur les appareils.
- **Applications** : cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application** : dans la liste, cliquez sur le nom de l'application à ajouter à la liste blanche ou liste noire ou cliquez sur **Ajouter** pour ajouter une application à la liste des applications disponibles.
  - Si vous sélectionnez **Ajouter**, entrez le nom de l'application dans le champ qui s'affiche.
  - Cliquez sur **Enregistrer** ou sur **Annuler**.
  - Répétez ces étapes pour chaque application que vous souhaitez ajouter à la liste blanche ou liste noire.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**, la page d'attribution de **Stratégie de mode kiosque** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que

vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie d'utilisation des réseaux

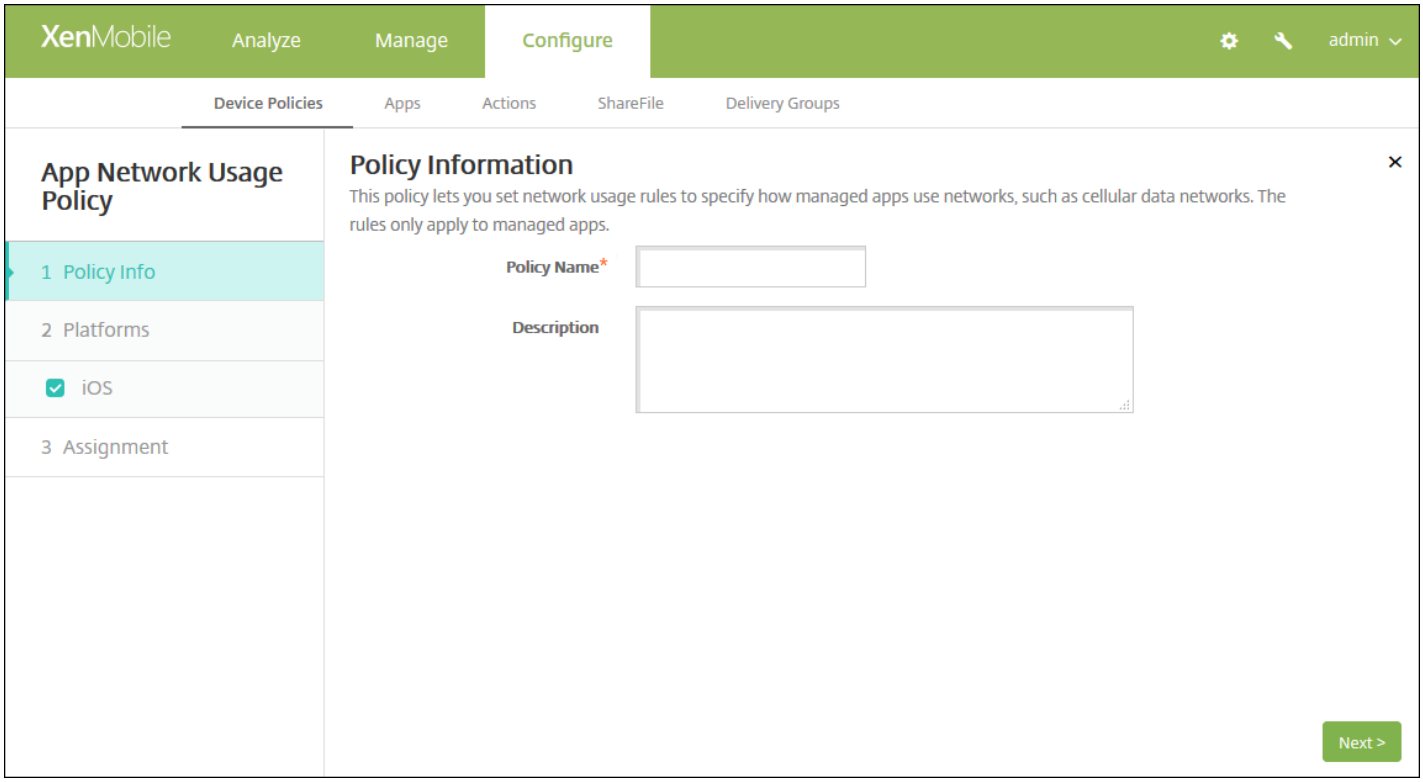
Feb 23, 2017

Vous pouvez définir des règles d'utilisation du réseau pour spécifier la manière dont les applications gérées utilisent les réseaux, tels que les réseaux de données cellulaires, sur les appareils iOS. Les règles s'appliquent uniquement aux applications gérées. Les applications gérées sont celles que vous déployez sur les appareils des utilisateurs via XenMobile. Elles n'incluent pas les applications que les utilisateurs ont téléchargées directement sur leurs appareils sans qu'elles soient déployées via XenMobile ou celles déjà installées sur les appareils lorsqu'ils ont été inscrits dans XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

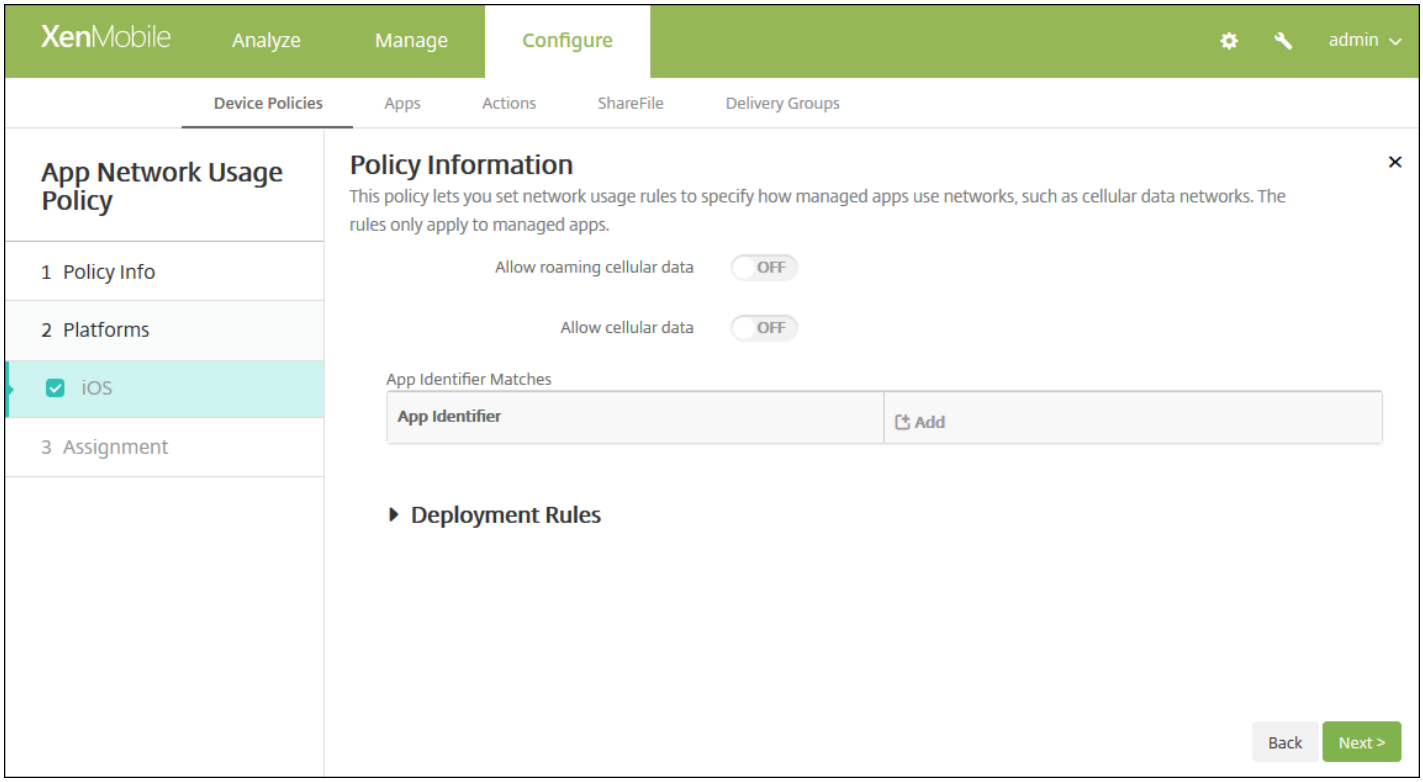
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Utilisation des réseaux**. La page d'informations sur la **Stratégie d'utilisation des réseaux** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Configurez ces paramètres.

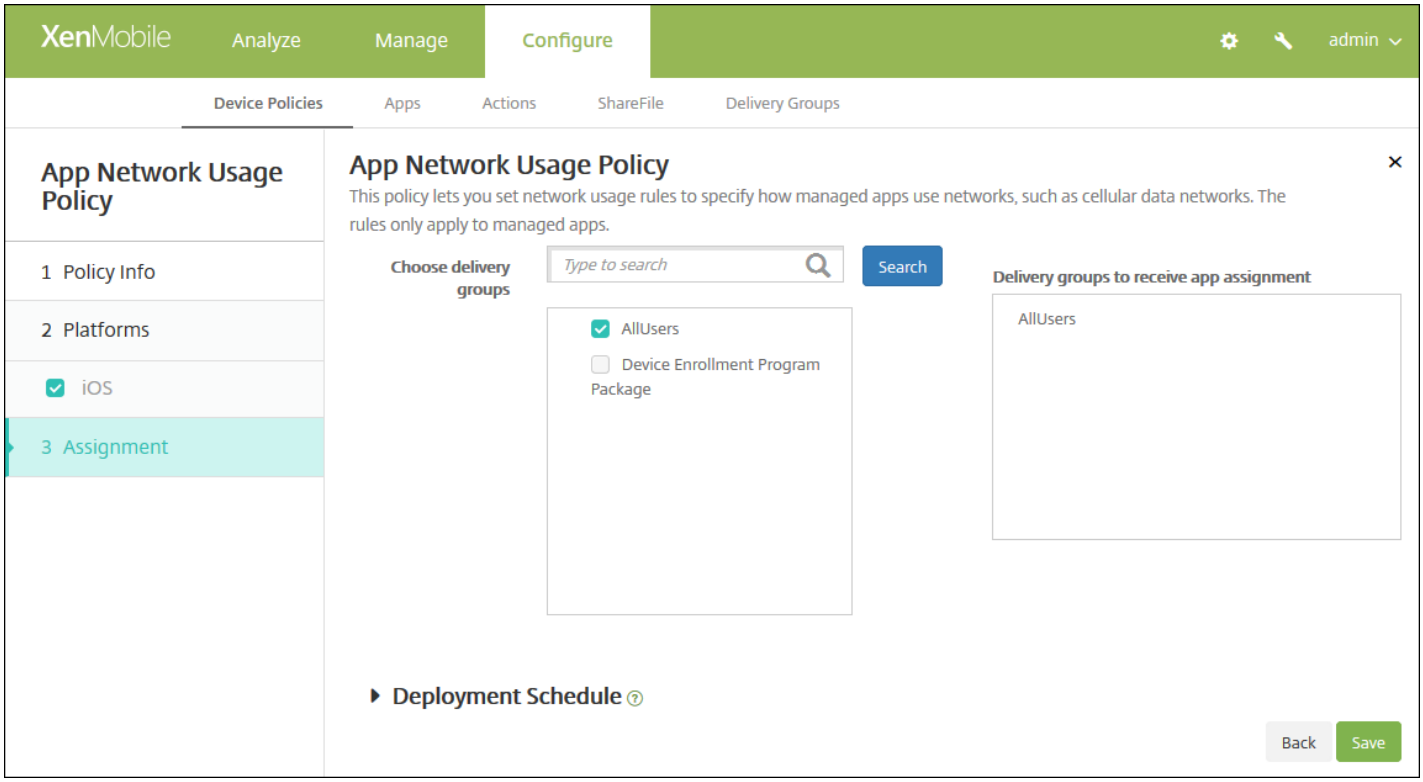
- **Autoriser les données cellulaires en itinérance** : indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires en itinérance. La valeur par défaut est **OFF**.
- **Autoriser les données cellulaires** : indiquez si les applications spécifiées peuvent utiliser une connexion de données cellulaires. La valeur par défaut est **OFF**.
- **Correspondances de l'identifiant d'application** : pour chaque application que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Identifiant app** : entrez un identifiant pour l'application.
  - Cliquez sur **Enregistrer** pour enregistrer l'application dans la liste ou sur **Annuler** pour ne pas l'enregistrer dans la liste.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie d'utilisation des réseaux** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégie de restriction d'application

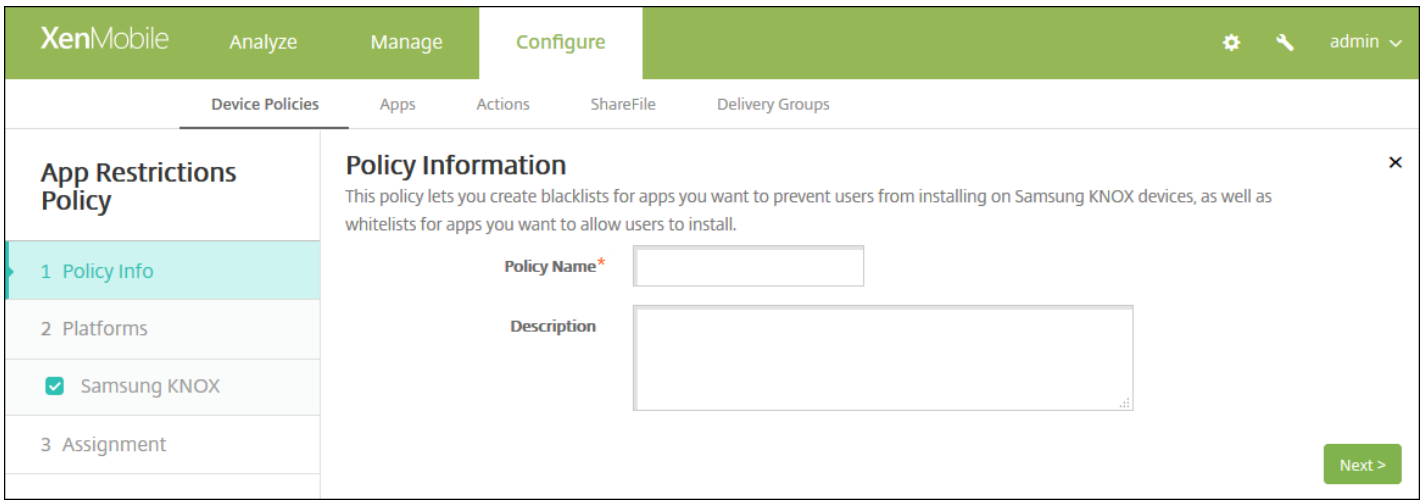
Feb 23, 2017

Vous pouvez créer des listes noires d'applications dont vous souhaitez interdire l'installation sur les appareils Samsung KNOX, ainsi que des listes blanches d'applications que vous souhaitez autoriser les utilisateurs à installer.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

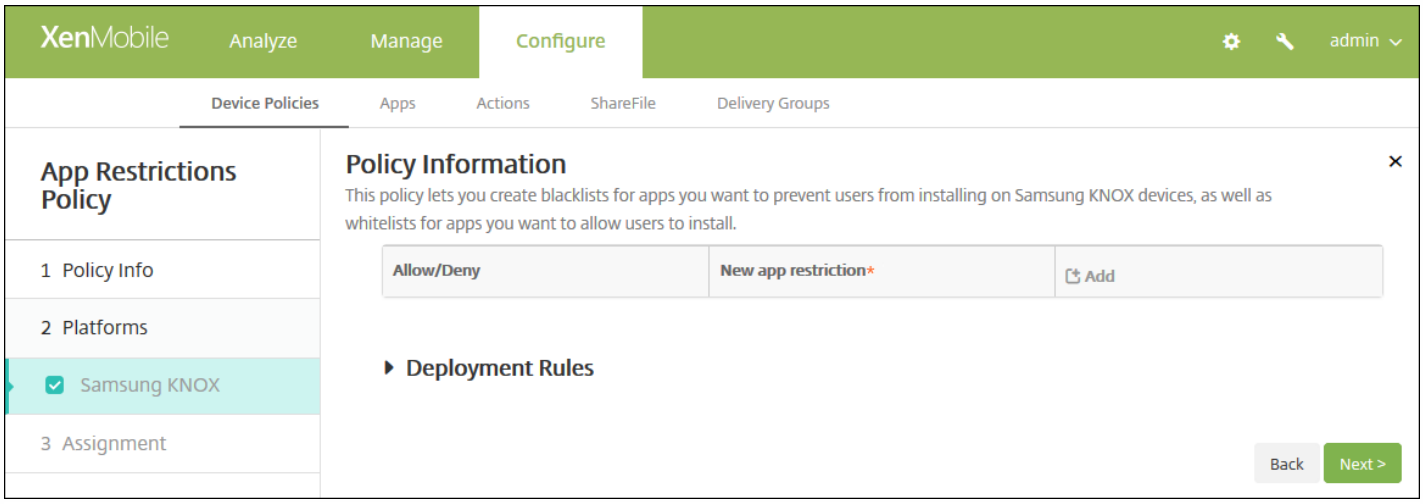
3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Restrictions applicatives**. La page d'informations sur la **Stratégie de restriction d'application** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Samsung KNOX** s'affiche.



6. Pour chaque application que vous souhaitez ajouter à la liste Autoriser/refuser, cliquez sur **Ajouter**, puis procédez comme suit :

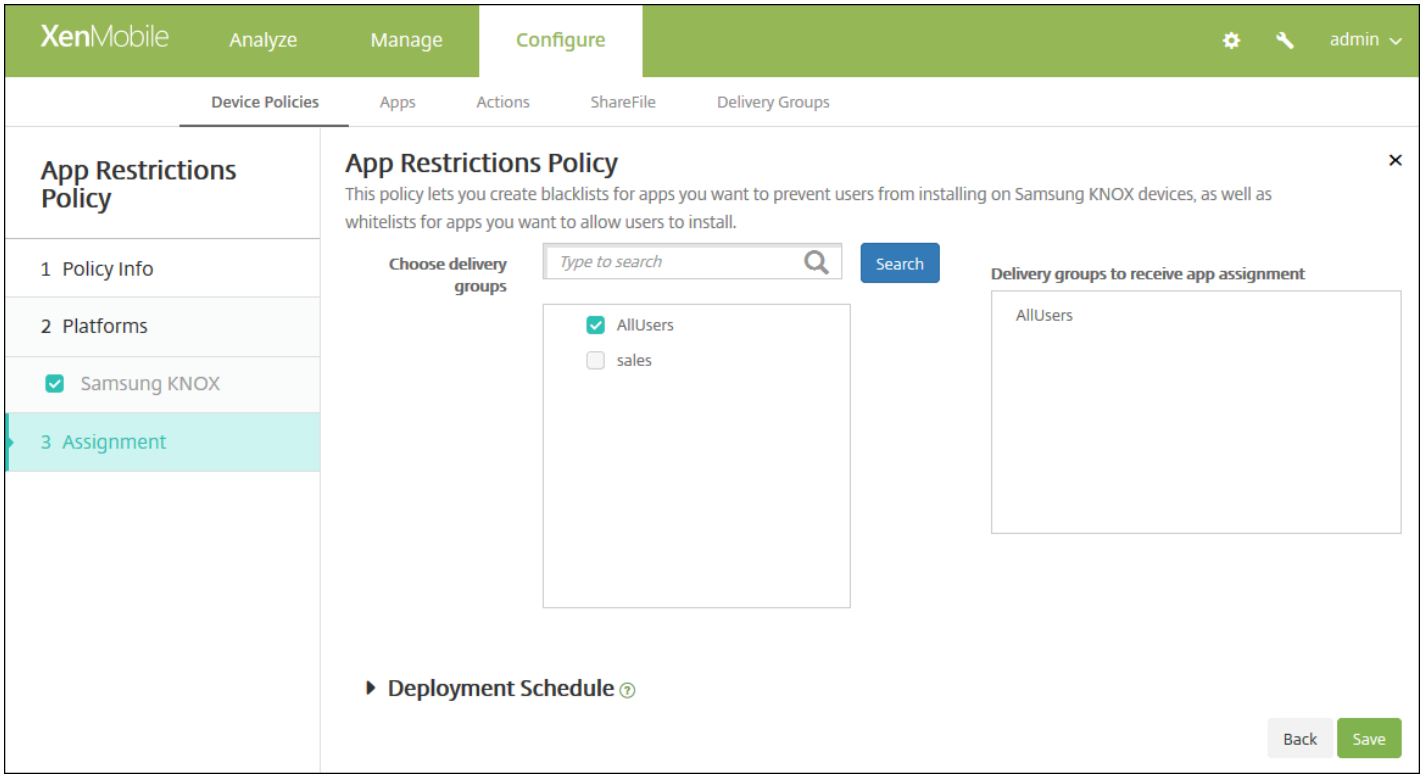
- **Autoriser/refuser** : indiquez si les utilisateurs sont autorisés à installer l'application.
- **Nouvelle restriction applicative** : entrez l'ID du paquetage de l'application ; par exemple, com.kmdm.af.crackle.
- Cliquez sur **Enregistrer** pour enregistrer l'application dans la liste Autoriser/refuser ou sur **Annuler** pour ne pas l'enregistrer dans la liste.

  Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

  Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'informations sur la **Stratégie de désinstallation des applications** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de tunnel applicatif

Mar 31, 2017

Les tunnels applicatifs sont conçus pour accroître la continuité du service et la fiabilité du transfert de données pour vos applications mobiles. Les tunnels applicatifs définissent les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications. Vous pouvez également utiliser des tunnels applicatifs pour créer des tunnels d'assistance à distance pour la gestion du support. Vous pouvez configurer la stratégie de tunnel applicatif pour les appareils Android et Windows Mobile/CE.

Remarque : tout trafic applicatif envoyé via un tunnel que vous définissez dans cette stratégie transite via XenMobile avant d'être redirigé vers le serveur exécutant l'application.

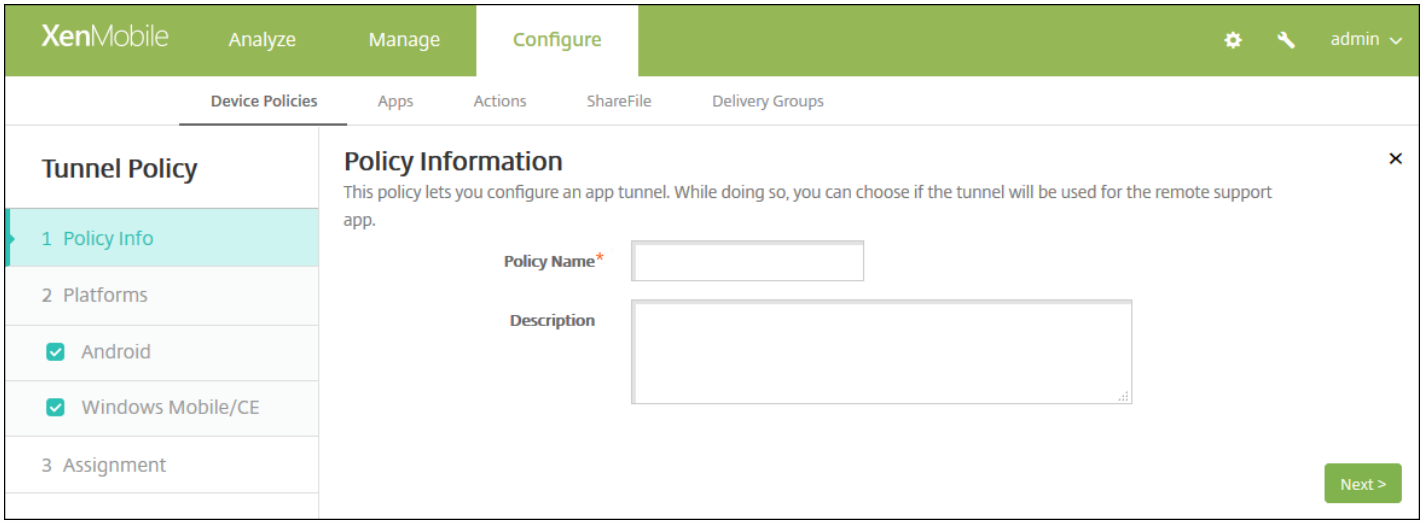
Paramètres Android

Paramètres Windows Mobile/CE

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**.La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **Tunnel**.La page **Stratégie de tunnel** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

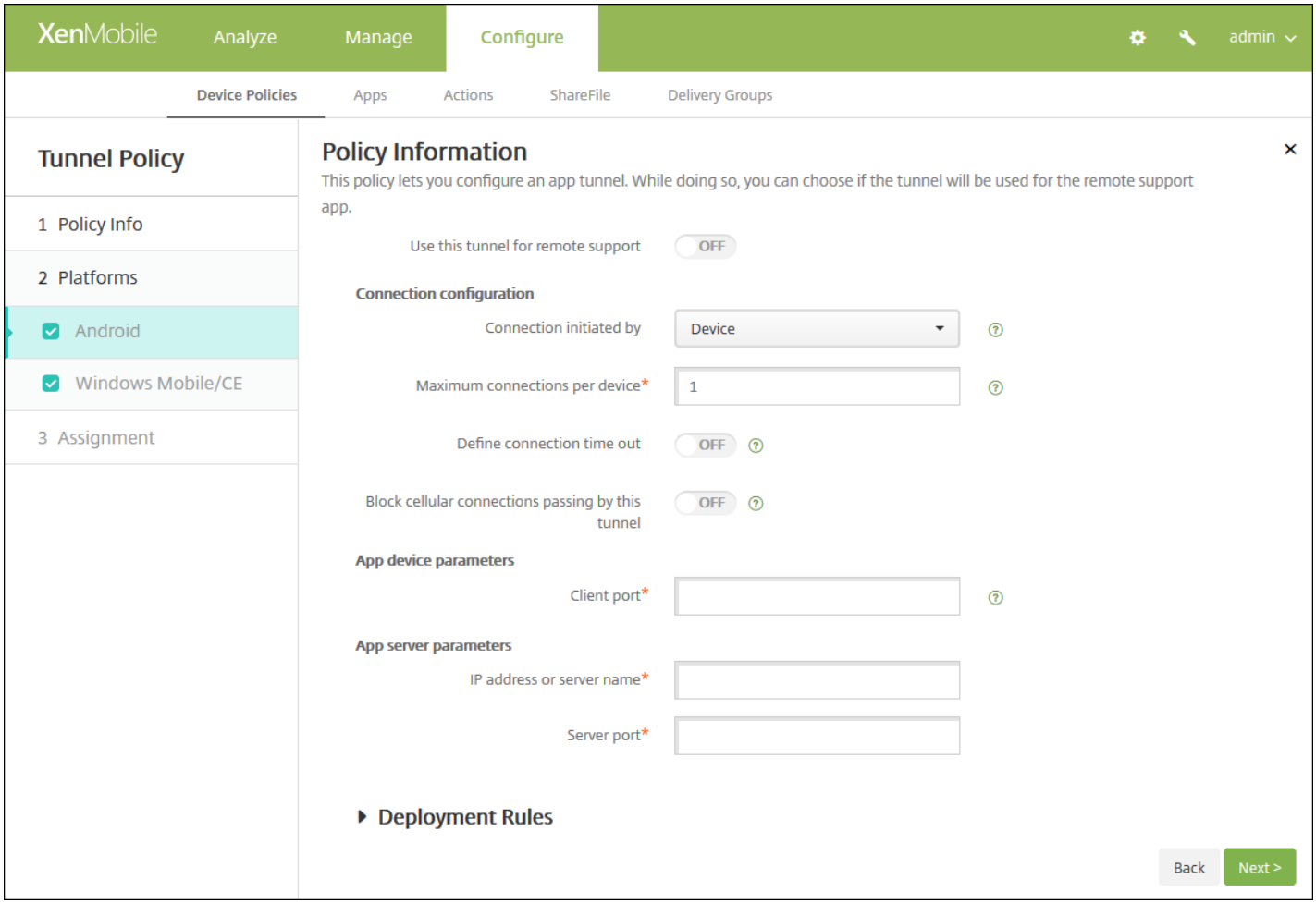
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour Android



Pour configurer ces paramètres :

- **Utiliser ce tunnel pour l'assistance à distance** : spécifiez si le tunnel est utilisé pour l'assistance à distance.

  Remarque : les étapes de configuration diffèrent selon que l'assistance à distance est sélectionnée ou non.

- Si vous ne sélectionnez pas l'assistance à distance, procédez comme suit :
  - **Connexion initiée par** : cliquez sur **Appareil** ou **Serveur** pour spécifier la source lançant la connexion.
  - **Connexions max. par appareil** : tapez un nombre pour définir le nombre de connexions TCP simultanées que l'application peut établir. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
  - **Définir le délai d'expiration de la connexion** : sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
    - **Délai d'expiration de la connexion**
    : si vous définissez **Définir le délai d'expiration de la connexion** sur **On**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Bloquer les connexions cellulaires transitant par ce tunnel** : sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.
  Remarque : les connexions Wi-Fi et USB ne sont pas bloquées.

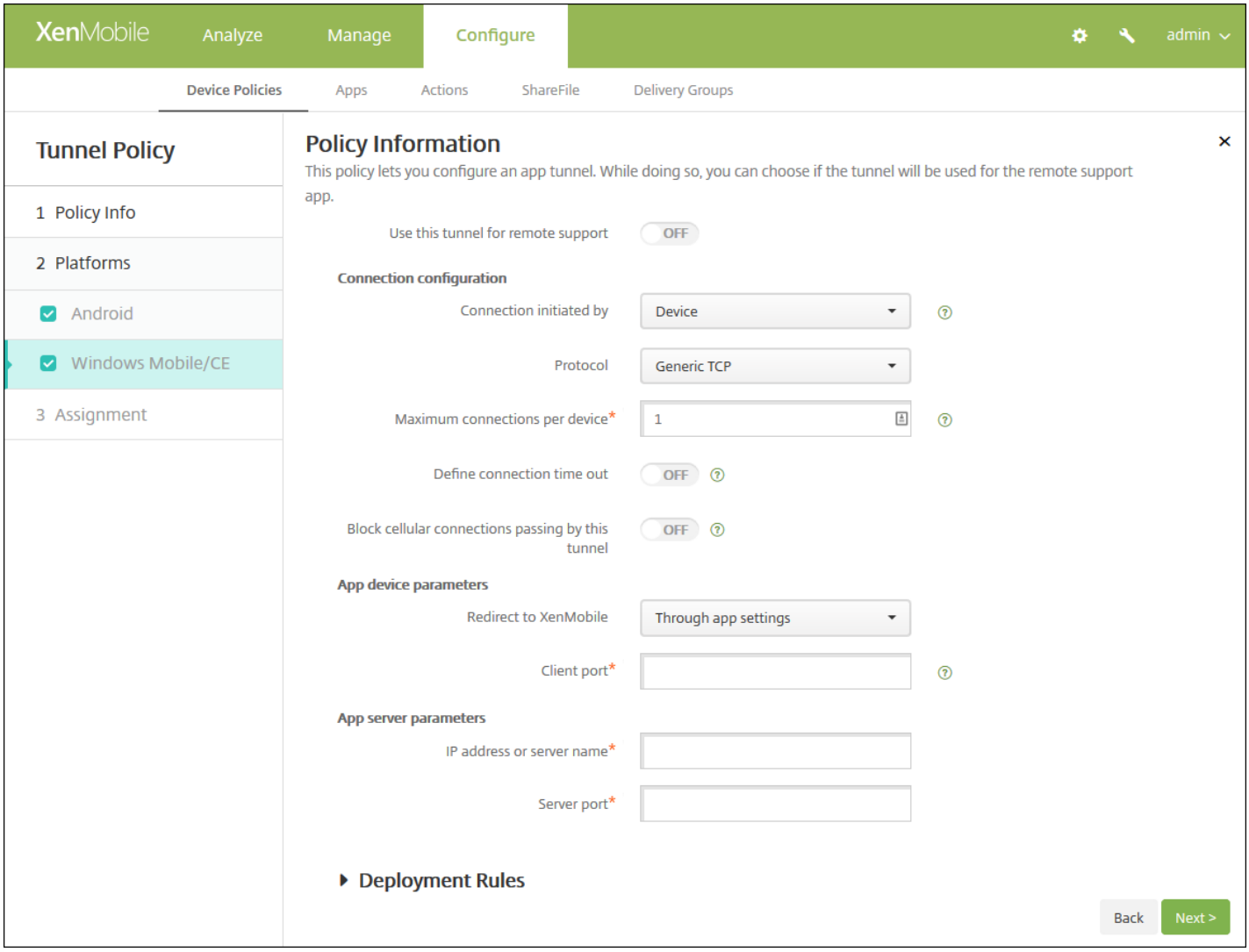
- **Port client** : entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port

serveur.

- **Adresse IP ou nom du serveur** : entrez l'adresse IP ou le nom du serveur applicatif. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
- **Port serveur** : entrez le numéro de port du serveur.

- Si vous sélectionnez l'assistance à distance, procédez comme suit :
- **Utiliser ce tunnel pour l'assistance à distance** : définissez cette option sur **On**.
- **Définir le délai d'expiration de la connexion** : sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Délai d'expiration de la connexion** : si vous définissez **Définir le délai d'expiration de la connexion sur On**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Utiliser une connexion SSL** : indiquez si vous souhaitez utiliser une connexion SSL sécurisée pour ce tunnel.
- **Bloquer les connexions cellulaires transitant par ce tunnel** : sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.
  Remarque : les connexions Wi-Fi et USB ne sont pas bloquées.

Configurer les paramètres pour Windows Mobile/CE



Pour configurer ces paramètres :

- **Utiliser ce tunnel pour l'assistance à distance** : spécifiez si le tunnel est utilisé pour l'assistance à distance.

  Remarque : les étapes de configuration diffèrent selon que l'assistance à distance est sélectionnée ou non.

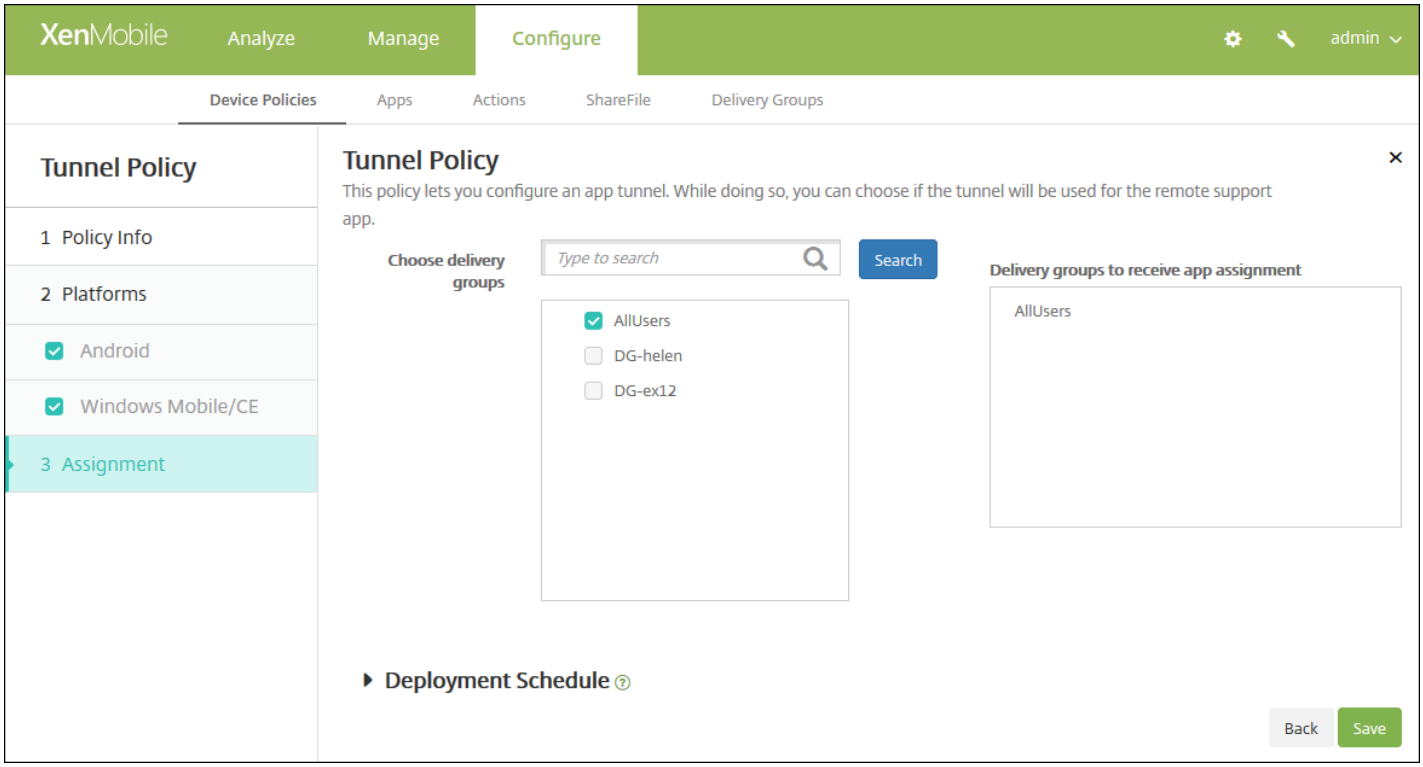
- Si vous ne sélectionnez pas l'assistance à distance, procédez comme suit :
  - C**onnexion initiée par** : cliquez sur **Appareil** ou **Serveur** pour spécifier la source lançant la connexion.
  - **Protocole** : dans la liste, cliquez sur le protocole à utiliser. La valeur par défaut est **TCP générique**.
  - **Connexions max. par appareil** : tapez un nombre pour définir le nombre de connexions TCP simultanées que l'application peut établir. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
  - **Définir le délai d'expiration de la connexion** : sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
    - **Délai d'expiration de la connexion**
    : si vous définissez **Définir le délai d'expiration de la connexion** sur **On**, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Bloquer les connexions cellulaires transitant par ce tunnel** : sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.
  Remarque : les connexions Wi-Fi et USB ne sont pas bloquées.

- **Rediriger vers XenMobile** : dans la liste, cliquez sur la manière dont l'appareil se connecte à XenMobile. La valeur par défaut est **Via les paramètres de l'application**.
  - Si vous sélectionnez **Via un alias local**, tapez l'alias dans **Alias local**. La valeur par défaut est **localhost**.
  - Si vous sélectionnez **Via une plage d'adresses IP**, entrez le début de la plage d'adresses IP dans **Plage d'adresses IP : de** et entrez **l'adresse IP de fin dans** Plage d'adresses IP :
- **Port client** : entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port serveur.
- **Adresse IP ou nom du serveur** : entrez l'adresse IP ou le nom du serveur applicatif. Ce champ ne s'applique qu'aux connexions initiées par l'appareil.
- **Port serveur** : entrez le numéro de port du serveur.

- Si vous sélectionnez l'assistance à distance, procédez comme suit :
- **Utiliser ce tunnel pour l'assistance à distance** : définissez cette option sur **On**.
- **Définir le délai d'expiration de la connexion** : sélectionnez cette option pour définir une durée pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
  - **Délai d'expiration de la connexion** : si vous définissez Définir le délai d'expiration de la connexion sur On, saisissez la durée en secondes pendant laquelle une application peut rester inactive avant que le tunnel ne soit fermé.
- **Utiliser une connexion SSL** : indiquez si vous souhaitez utiliser une connexion SSL sécurisée pour ce tunnel.
- **Bloquer les connexions cellulaires transitant par ce tunnel** : sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.
  Remarque : les connexions Wi-Fi et USB ne sont pas bloquées.

7. Configurer les règles de déploiement

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de tunnel** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie.Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**.Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de désinstallation d'application

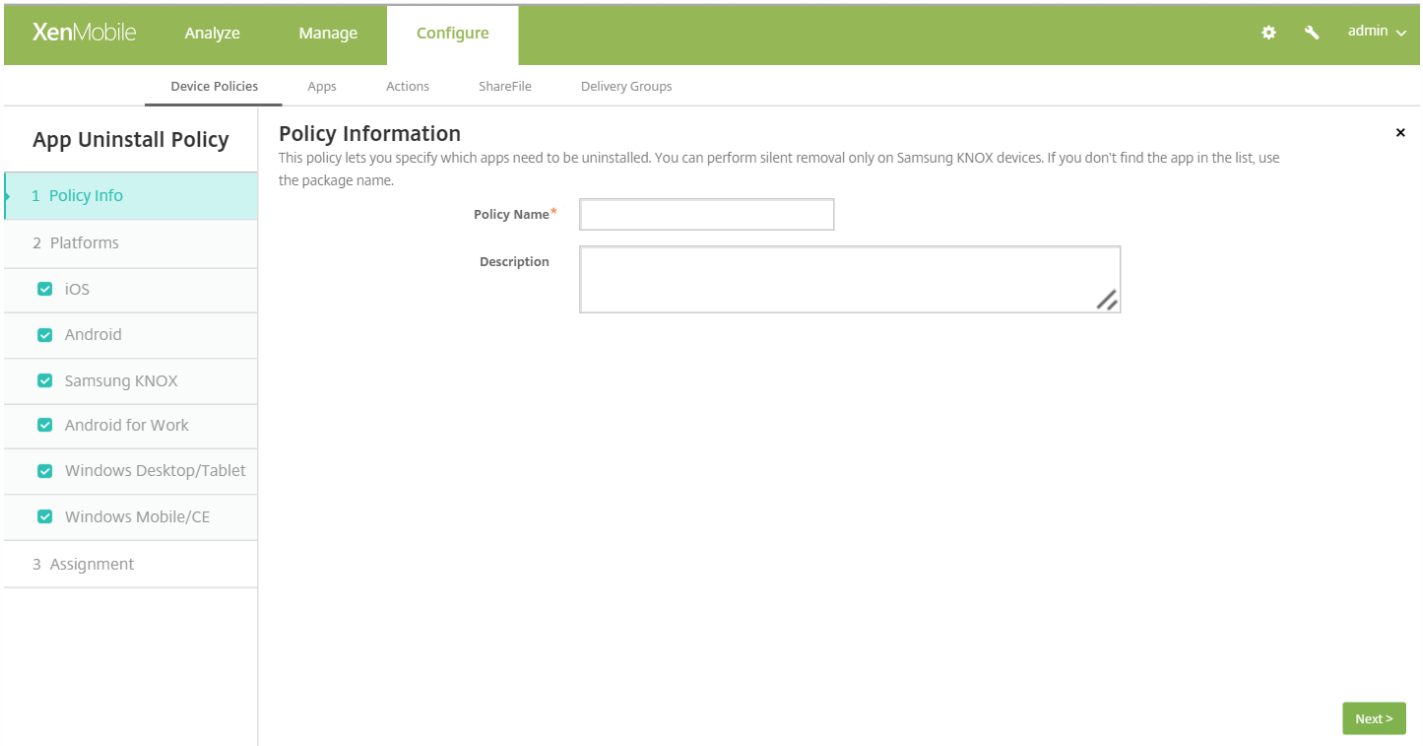
Feb 23, 2017

Vous pouvez créer une stratégie de désinstallation d'application pour les plates-formes iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet et Windows Mobile/CE. Une stratégie de désinstallation d'application vous permet de supprimer des applications des appareils utilisateur pour un certain nombre de raisons. Il se peut que vous ne souhaitiez plus prendre en charge certaines applications et que votre entreprise désire remplacer des applications par d'autres similaires mais provenant d'autres fournisseurs, etc. Les applications sont supprimées lorsque cette stratégie est déployée sur les appareils de vos utilisateurs. À l'exception des appareils Samsung KNOX, les utilisateurs reçoivent une invitation à désinstaller l'application ; les utilisateurs d'appareils Samsung KNOX ne reçoivent pas d'invitation à désinstaller l'application.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Applications**, cliquez sur **Désinstallation de l'application**. La page **Stratégie de désinstallation des applications** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

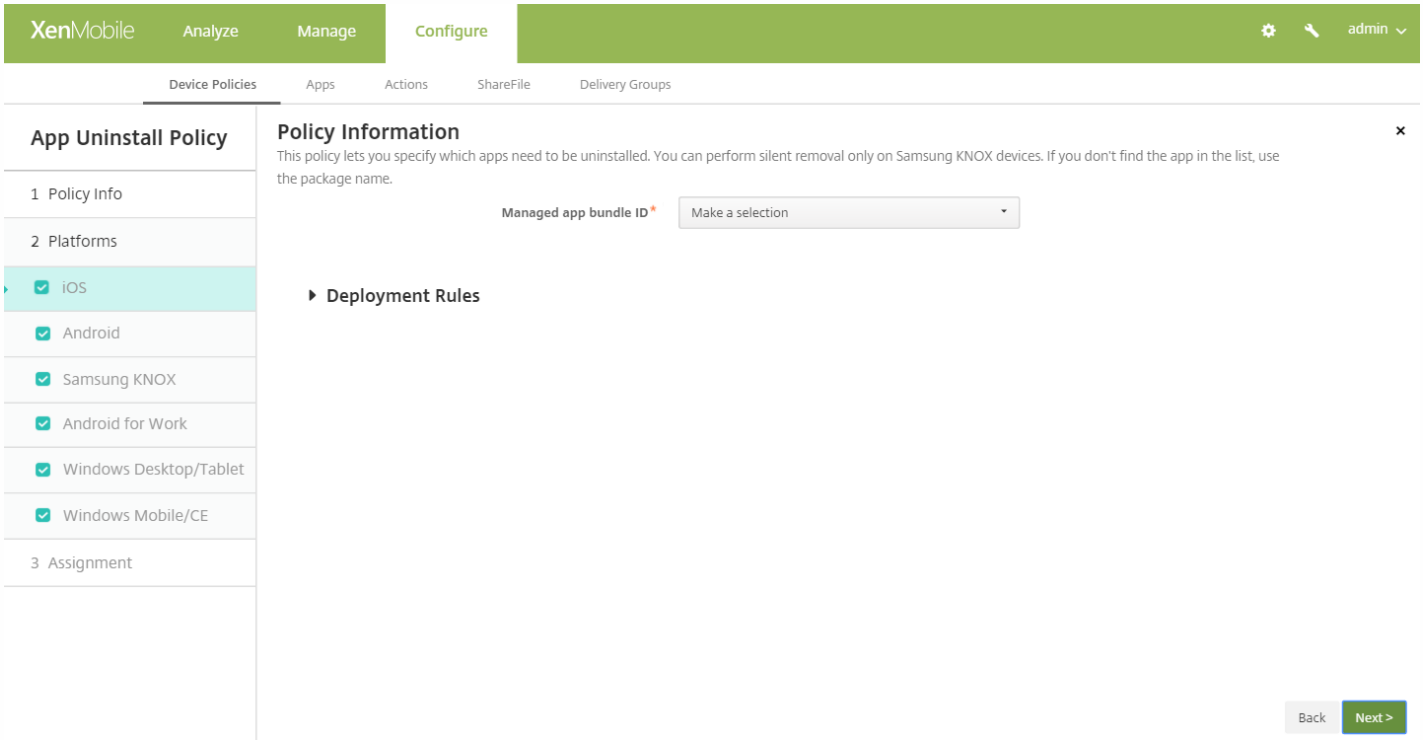
5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-

forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

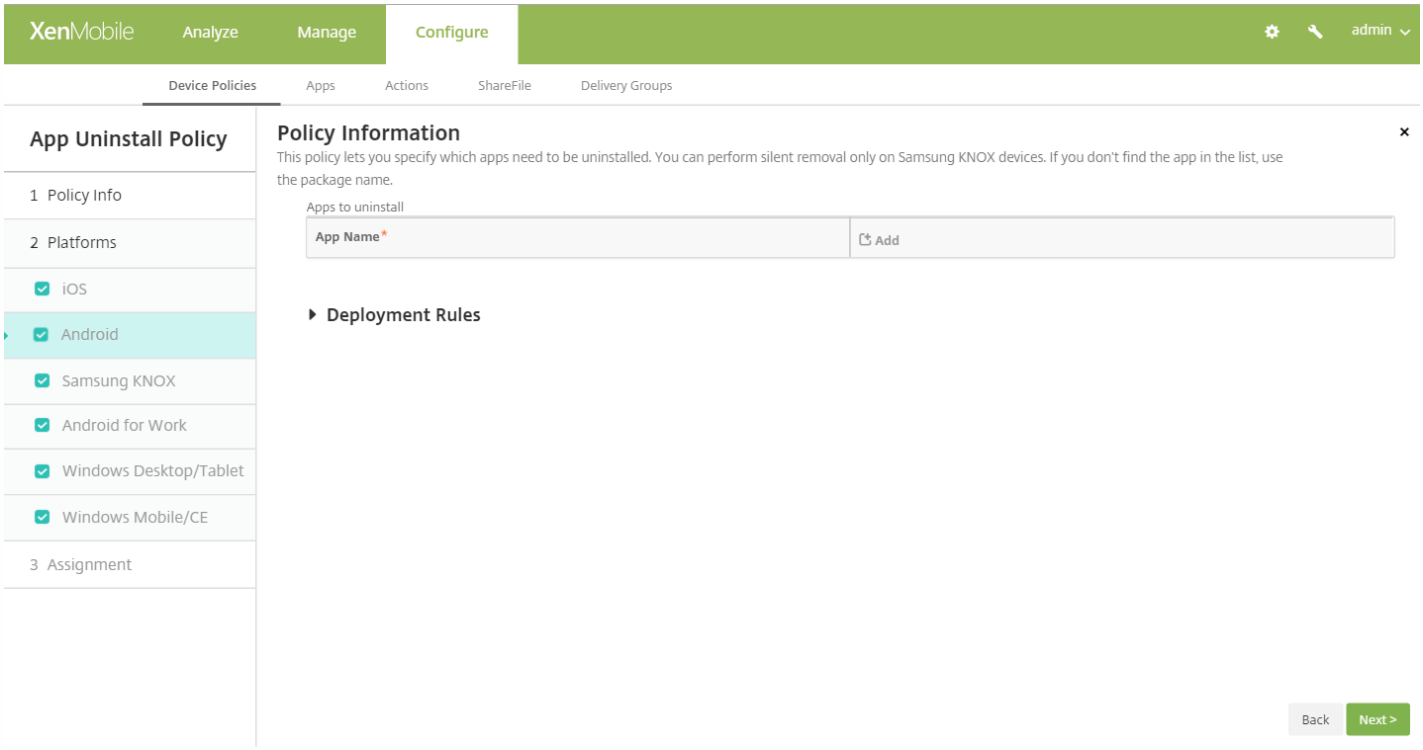
Configurer les paramètres pour iOS



Configurez ce paramètre :

- **Bundle ID d'application gérée :** dans la liste, cliquez sur une application existante ou cliquez sur **Ajouter**. s'il n'existe aucune application configurée pour cette plate-forme, la liste est vide et vous devez ajouter une nouvelle application.
  - Lorsque vous cliquez sur **Ajouter** un champ apparaît dans lequel vous pouvez entrer un nom pour l'application.

Configurer tous les autres paramètres de plate-forme



Configurez ce paramètre :

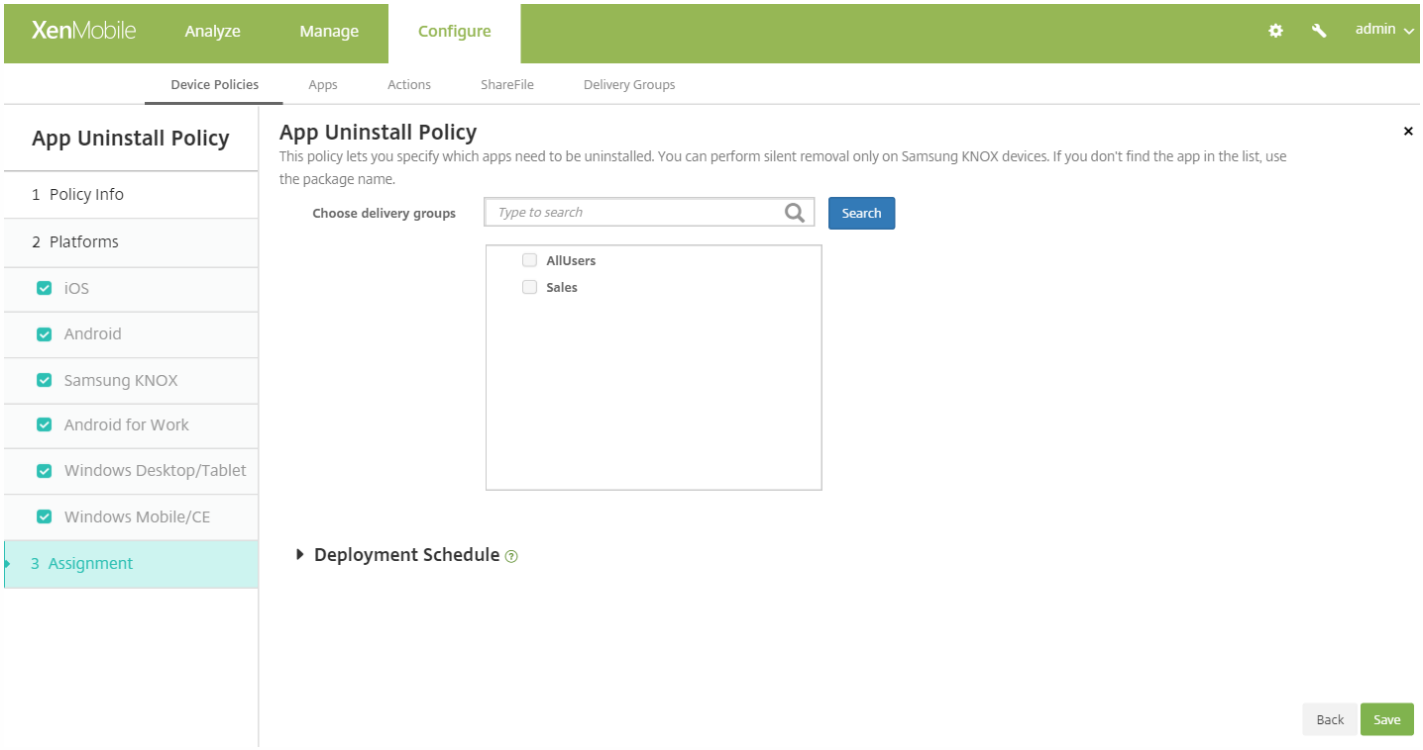
- **Applications à désinstaller** : pour chaque application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom app** : dans la liste, cliquez sur une application existante ou sur **Ajouter** pour entrer un nouveau nom d'application. s'il n'existe pas d'applications configurées pour cette plate-forme, la liste est vide et vous devez ajouter de nouvelles applications.
  - Cliquez sur **Ajouter** pour ajouter l'application ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

    Remarque : pour supprimer une application existante de la stratégie de désinstallation, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de désinstallation des applications** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de restriction de désinstallation d'applications

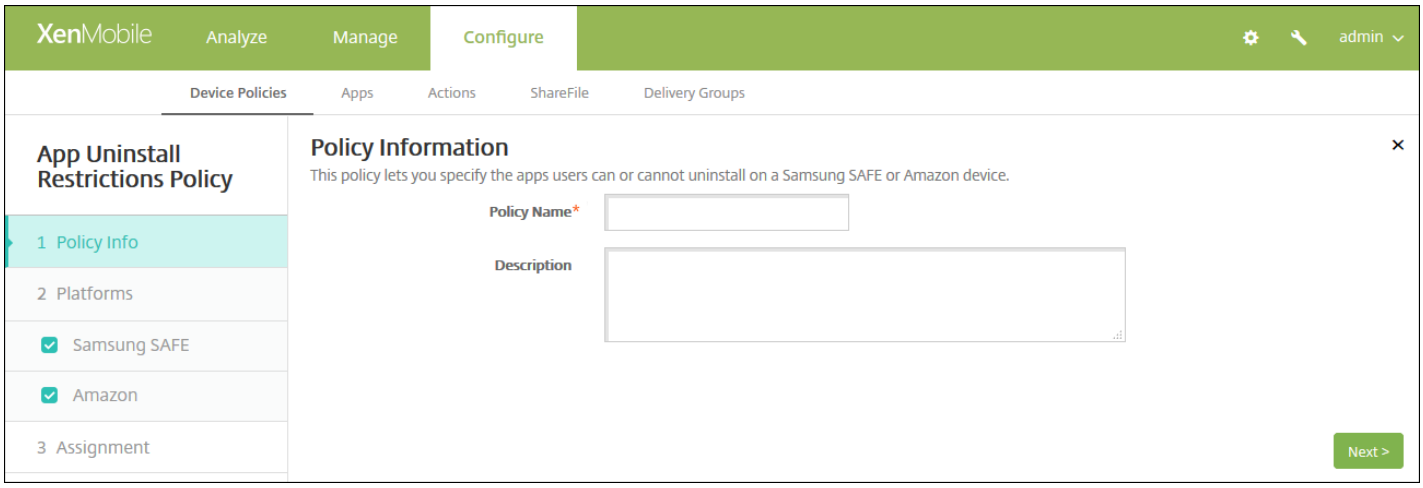
Feb 23, 2017

Vous pouvez spécifier les applications que les utilisateurs peuvent ou ne peuvent pas désinstaller sur un appareil Samsung SAFE ou Amazon.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

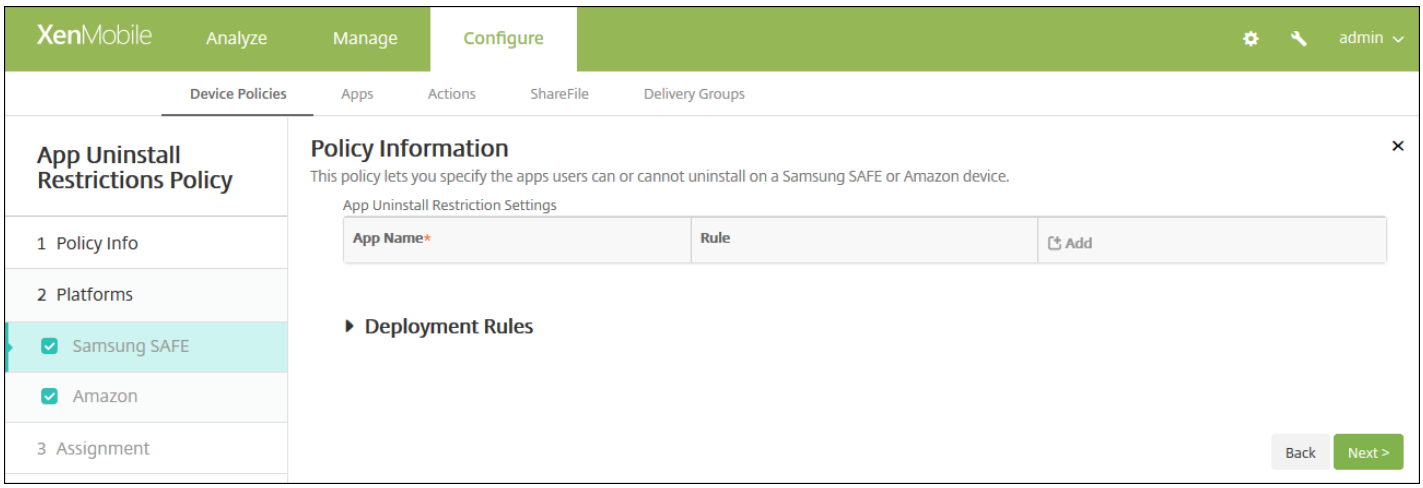
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Restriction de désinstallation d'applications**. La page d'informations de la **Stratégie de restriction de désinstallation d'applications** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Configurez ces paramètres pour chaque plate-forme que vous avez sélectionnée :

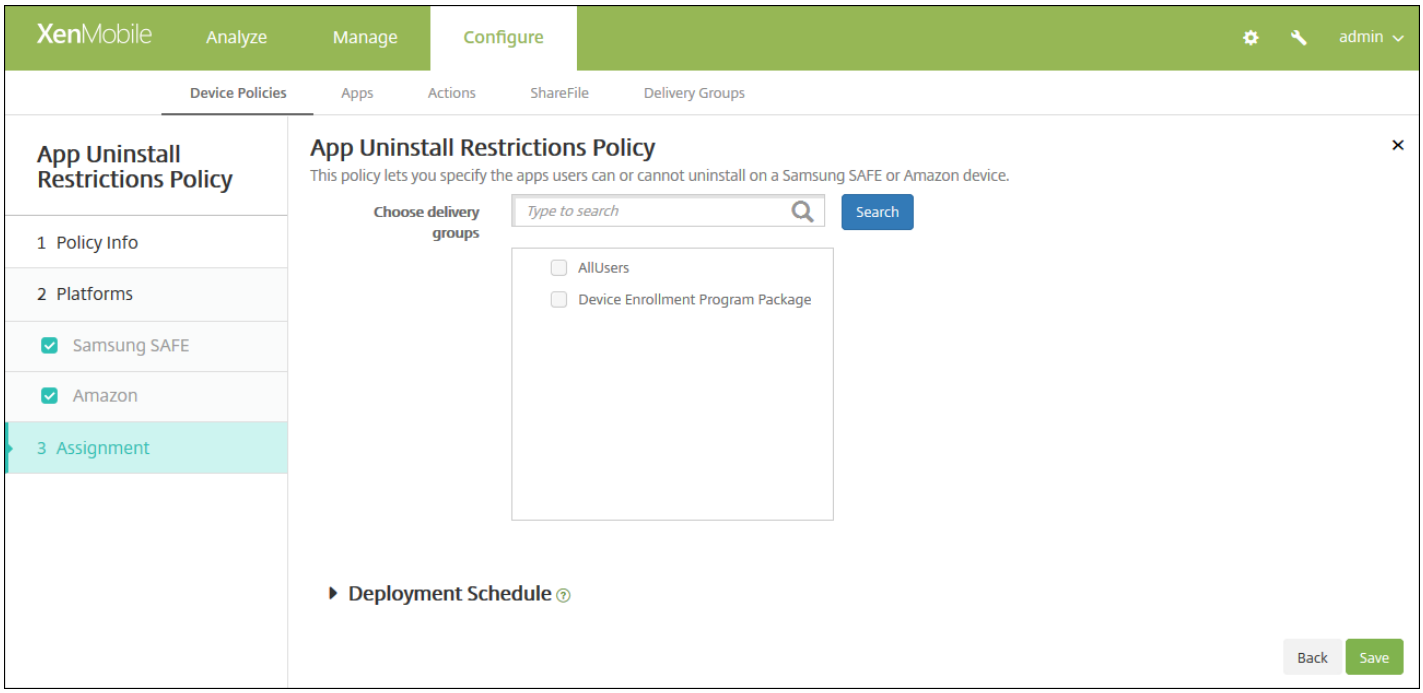
- **Paramètres de restriction de désinstallation d'application** : pour chaque règle d'application que vous souhaitez ajouter, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nom de l'application** : dans la liste, cliquez sur une application ou sur sur **Ajouter** pour ajouter une nouvelle application.
  - **Règle** : indiquez si les utilisateurs peuvent désinstaller l'application. Par défaut, la désinstallation est autorisée.
  - Cliquez sur **Enregistrer** ou sur **Annuler**.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

8. Configurez les règles de déploiement.

9. Cliquez sur **Next**. La page d'attribution de la **Stratégie de restriction de désinstallation d'applications** s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous

sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

12. Cliquez sur **Enregistrer**.

Stratégies de navigateur

Feb 23, 2017

Vous pouvez créer des stratégies de navigateur pour Samsung SAFE ou Samsung KNOX afin de définir si les appareils peuvent utiliser le navigateur ou pour limiter les fonctions du navigateur que les appareils peuvent utiliser.

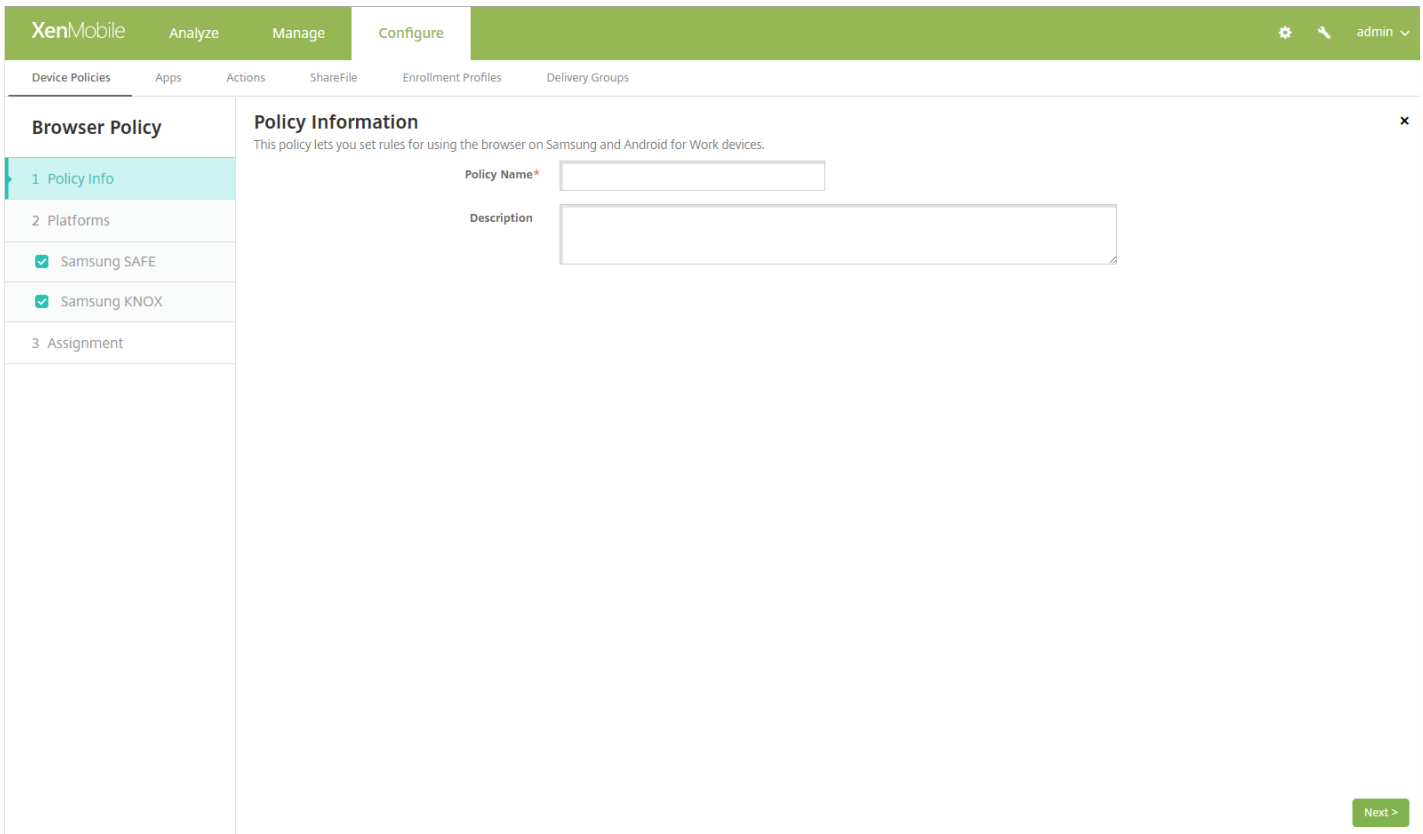
Sur les appareils Samsung, vous pouvez désactiver complètement le navigateur, ou vous pouvez activer ou désactiver les fenêtres publicitaires intempestives JavaScript, les cookies, le remplissage automatique, et l'affichage d'avertissements en cas de visite d'un site frauduleux.

Paramètres Samsung SAFE et Samsung KNOX

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus** puis, sous **Applications**, cliquez sur **Navigateur**. La page d'informations **Stratégie de navigateur** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

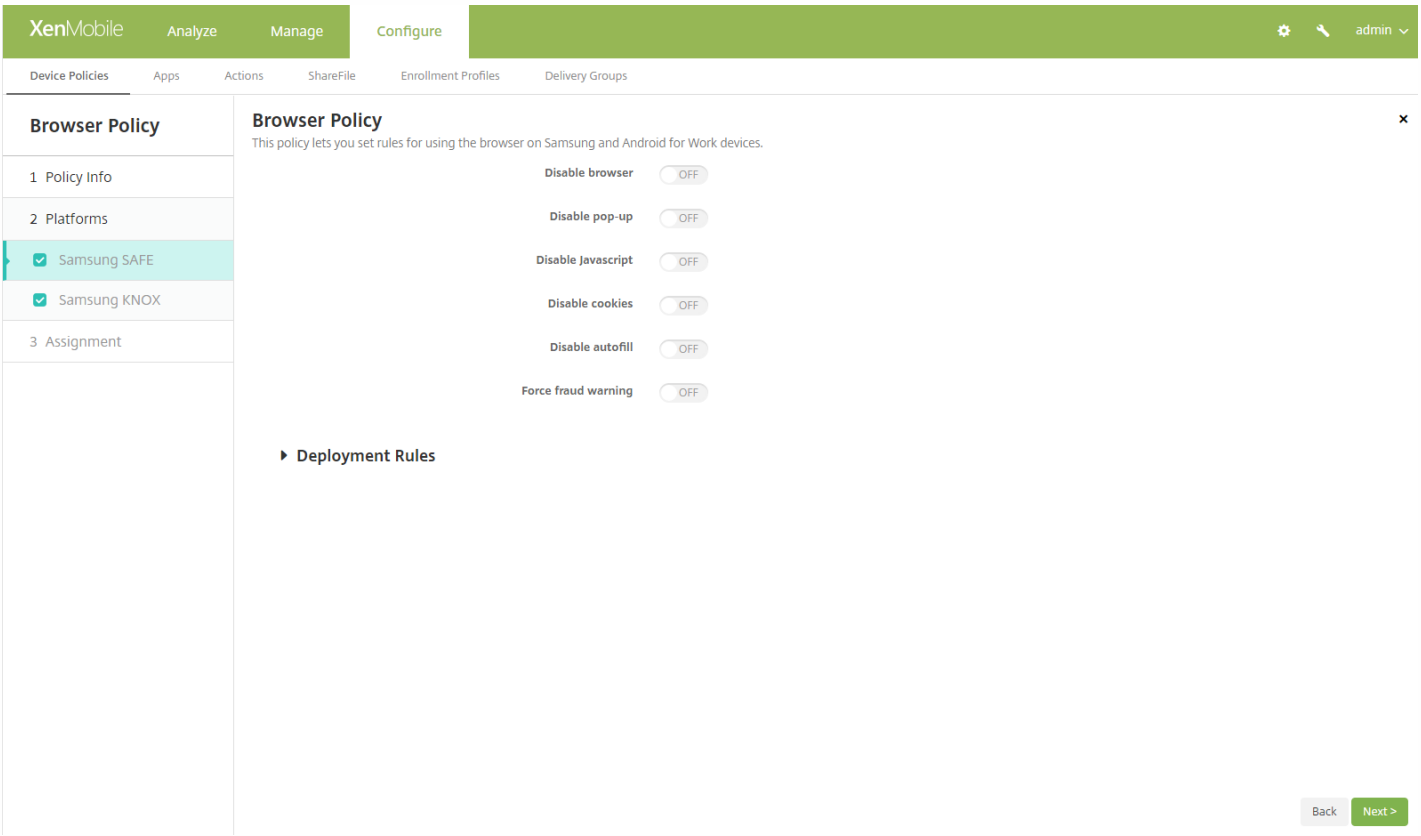
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres Samsung SAFE et Samsung KNOX

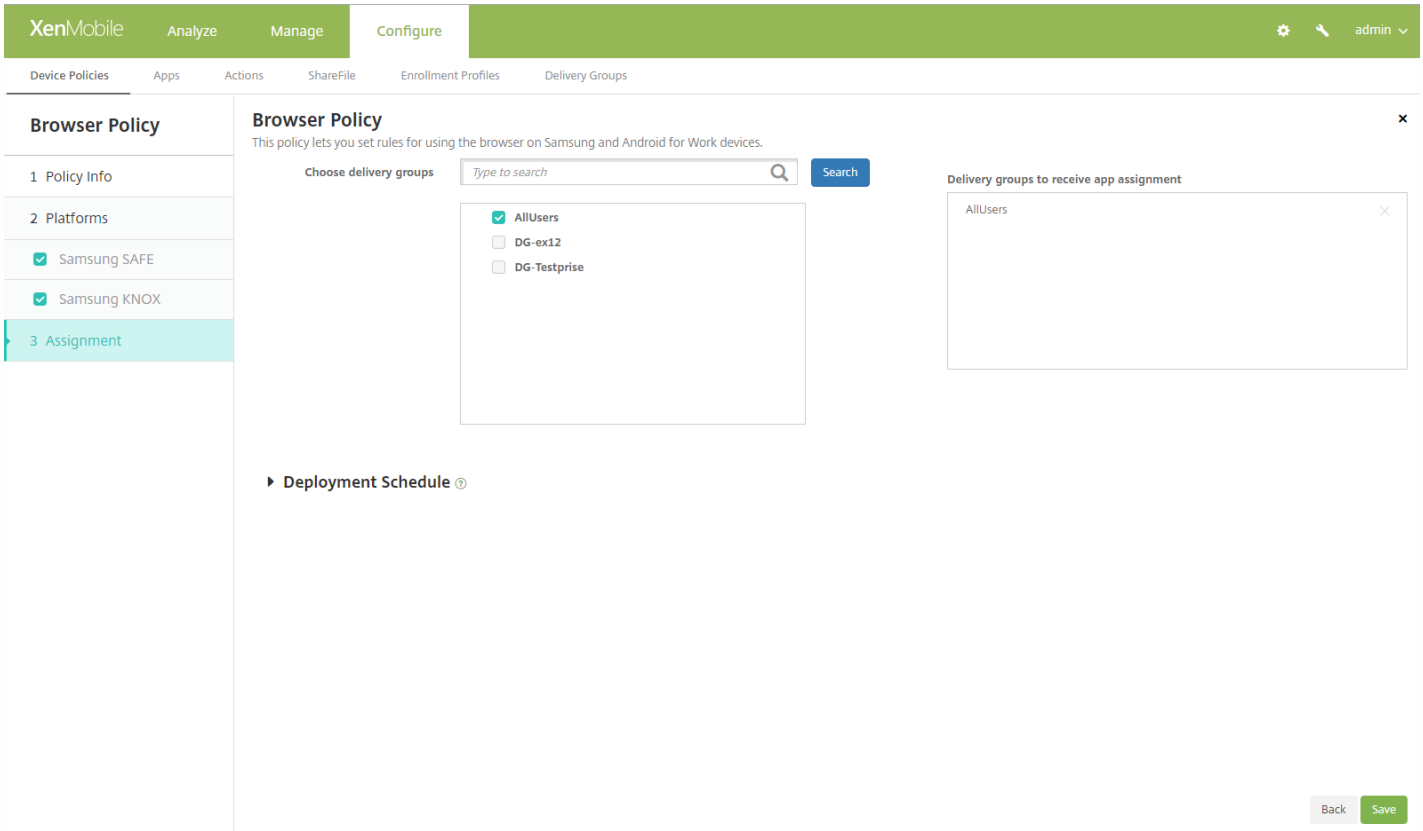


Pour configurer ces paramètres :

- **Désactiver le navigateur** : sélectionnez cette option pour désactiver complètement le navigateur Samsung sur les appareils des utilisateurs. La valeur par défaut est **OFF**, ce qui permet aux utilisateurs d'utiliser le navigateur. Lorsque vous désactivez le navigateur, les options suivantes disparaissent.
- **Désactiver les fenêtres pop-up** : sélectionnez cette option pour autoriser les messages dans le navigateur.
- **Désactiver le Javascript** : sélectionnez cette option pour autoriser l'exécution de JavaScript sur le navigateur.
- **Désactiver les cookies** : sélectionnez cette option pour autoriser les cookies.
- **Désactiver le remplissage automatique** : sélectionnez cette option pour autoriser les utilisateurs à activer la fonction de remplissage automatique du navigateur.
- **Forcer l'avertissement de fraude** : sélectionnez cette option pour afficher un avertissement lorsqu'un utilisateur visite un site Web frauduleux.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution **Stratégie de navigateur** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégies de calendrier (CalDav)

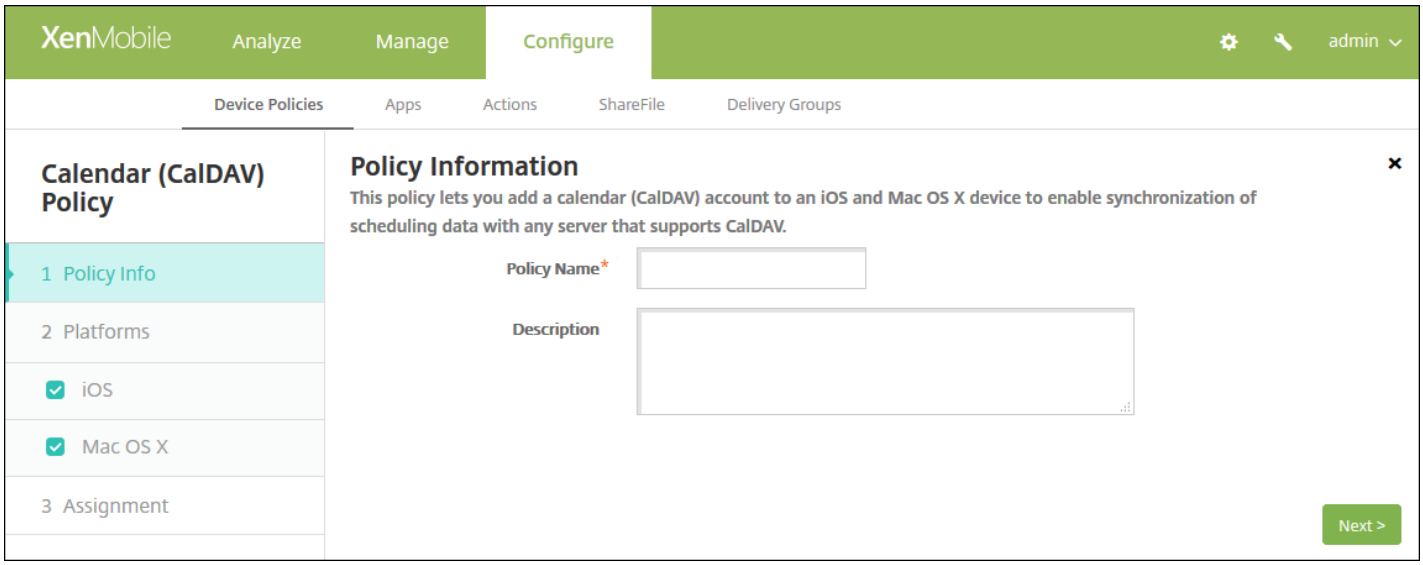
Feb 23, 2017

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de calendrier (CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de planification avec tout serveur qui prend en charge CalDAV.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **Calendrier (CalDav)**. La page **Stratégie de calendrier (CalDAV)** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

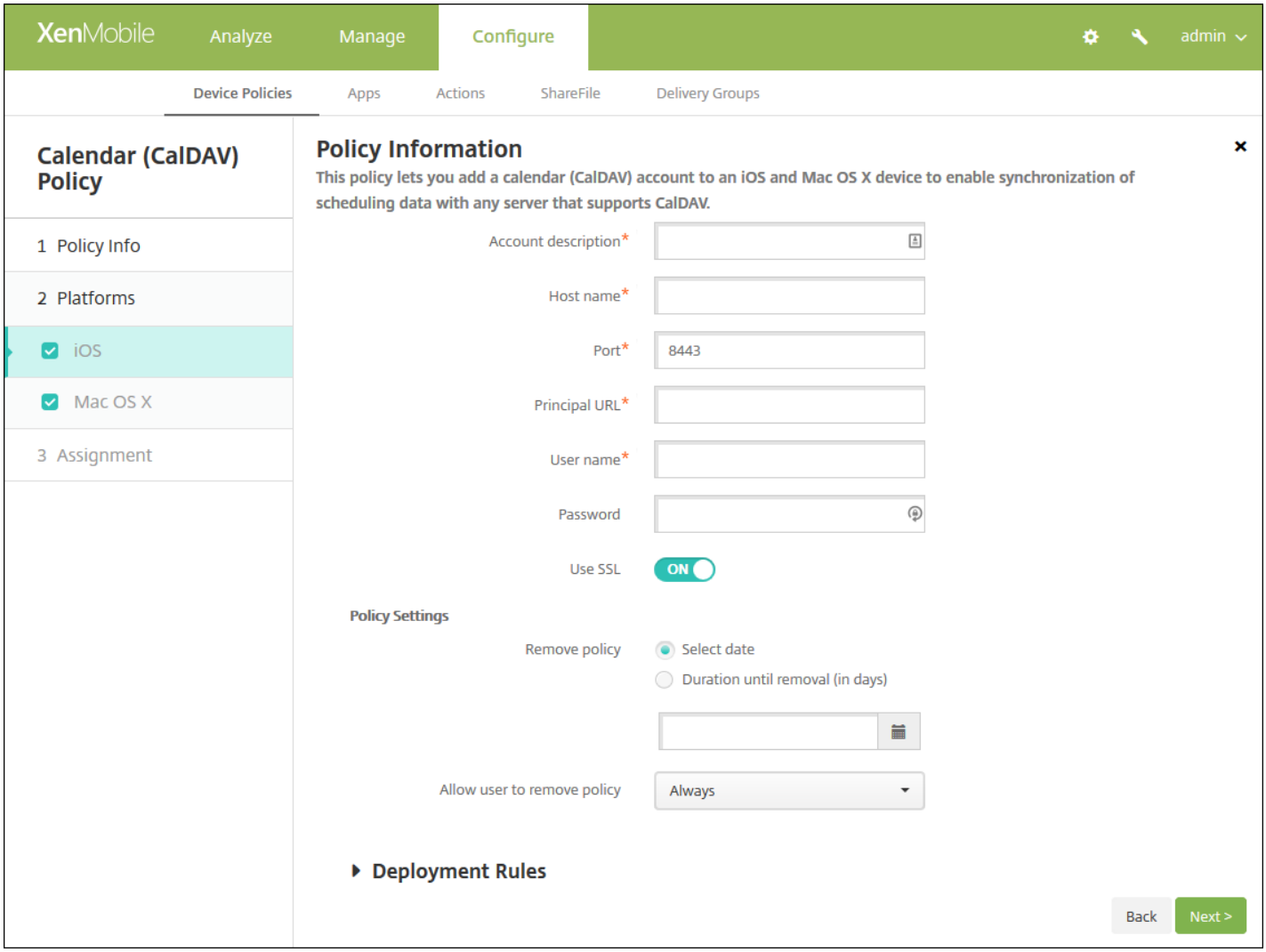
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

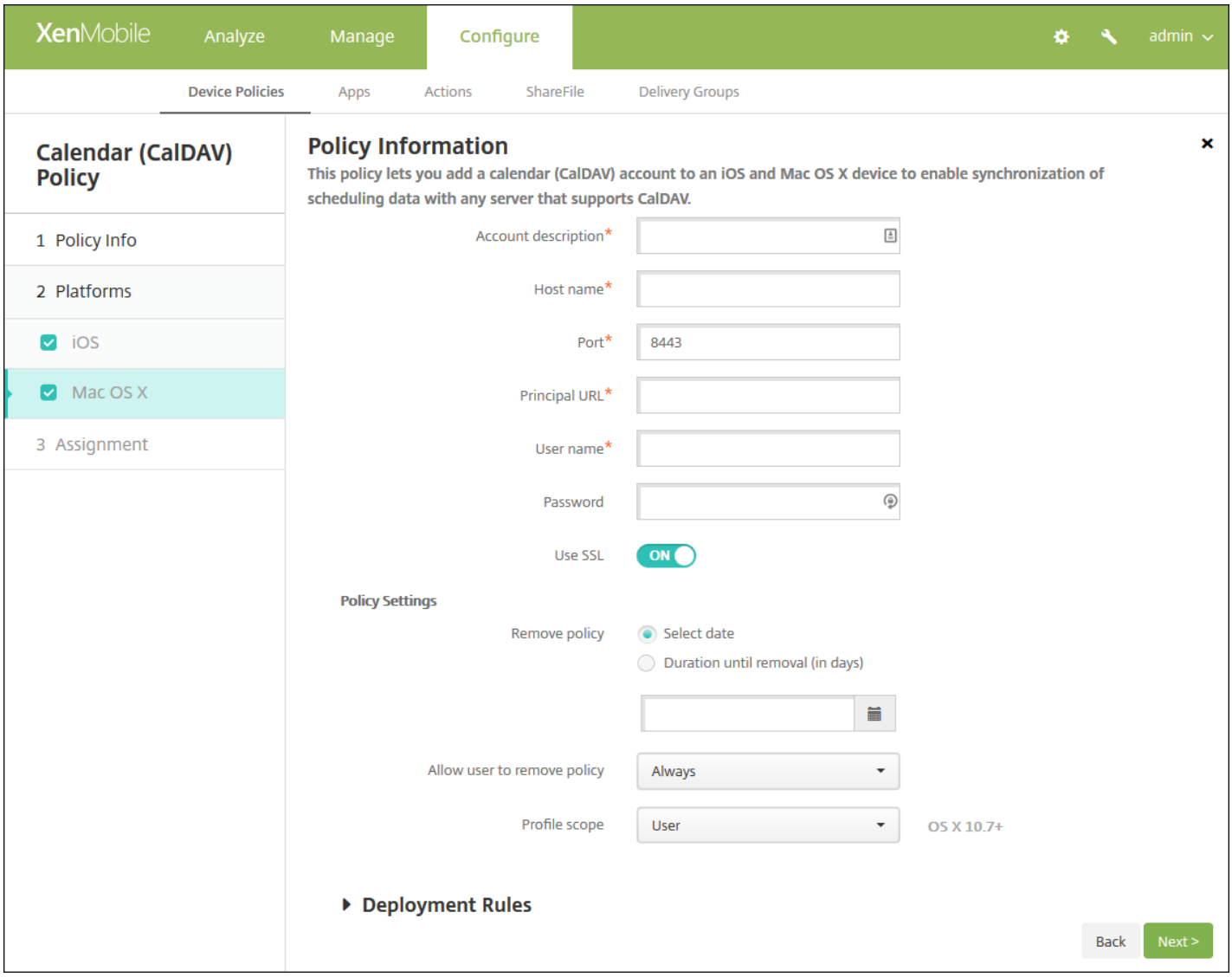
Configurer les paramètres pour iOS



Configurez les paramètres suivants :

- **Description du compte** : entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte** : entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port** : entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est de **8443**.
- **URL principale** : entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur** : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe** : entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **ON**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X



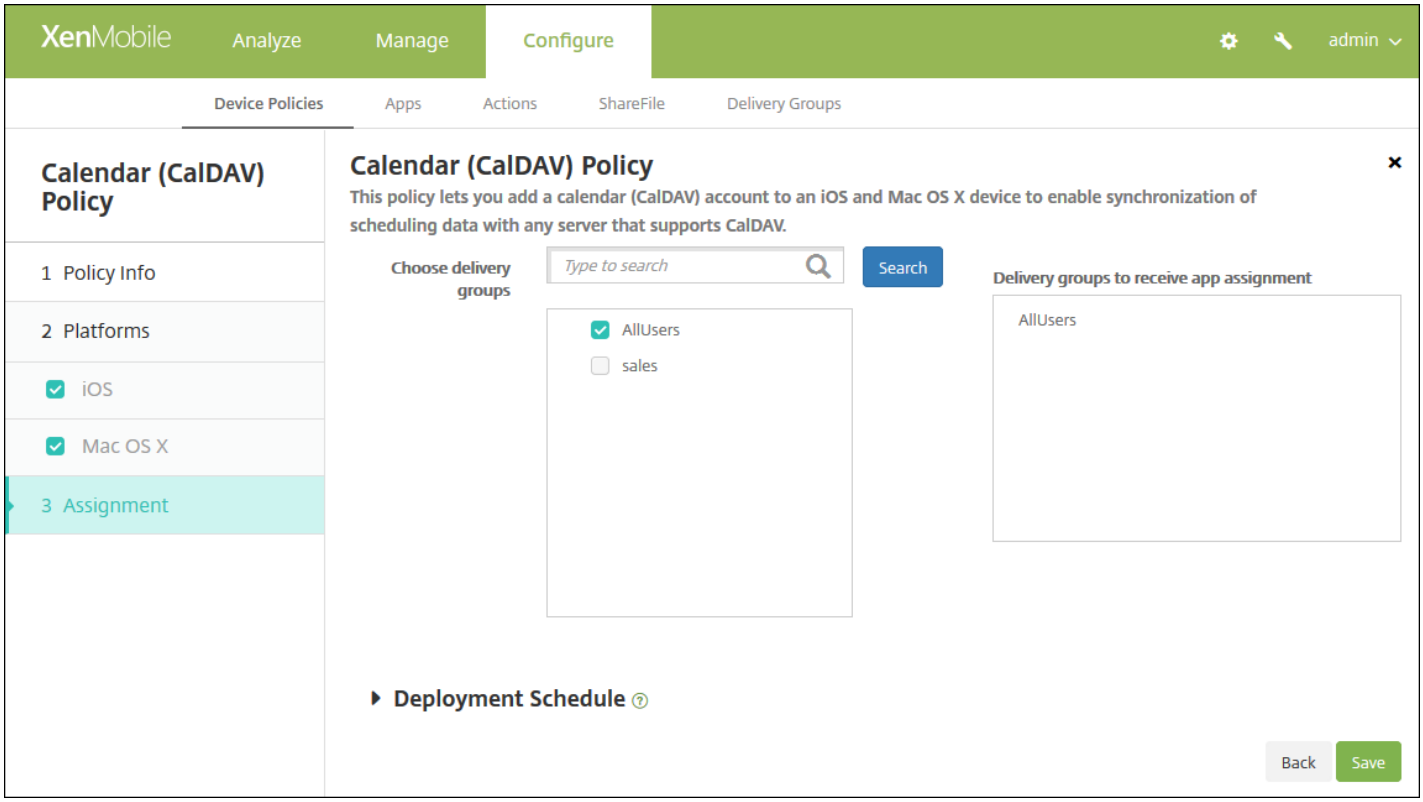
Configurez les paramètres suivants :

- **Description du compte** : entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte** : entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
- **Port** : entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est de **8443**.
- **URL principale** : entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur** : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe** : entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est **ON**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

- En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de calendrier (CalDAV)** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que

vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie cellulaire

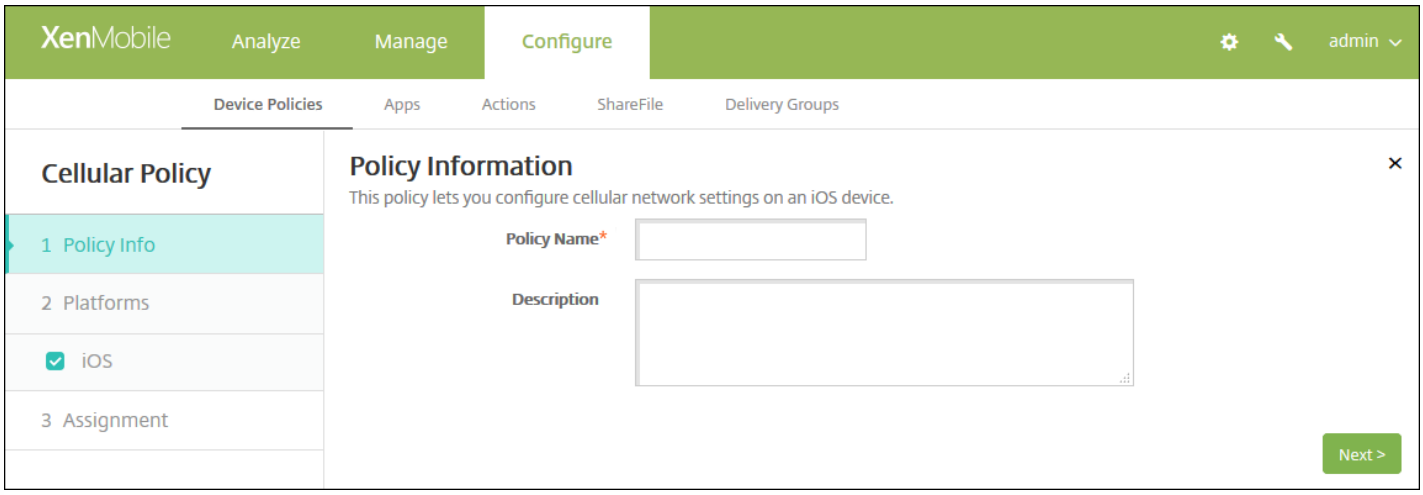
Feb 23, 2017

Cette stratégie vous permet de configurer des paramètres réseau cellulaire sur un appareil iOS.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

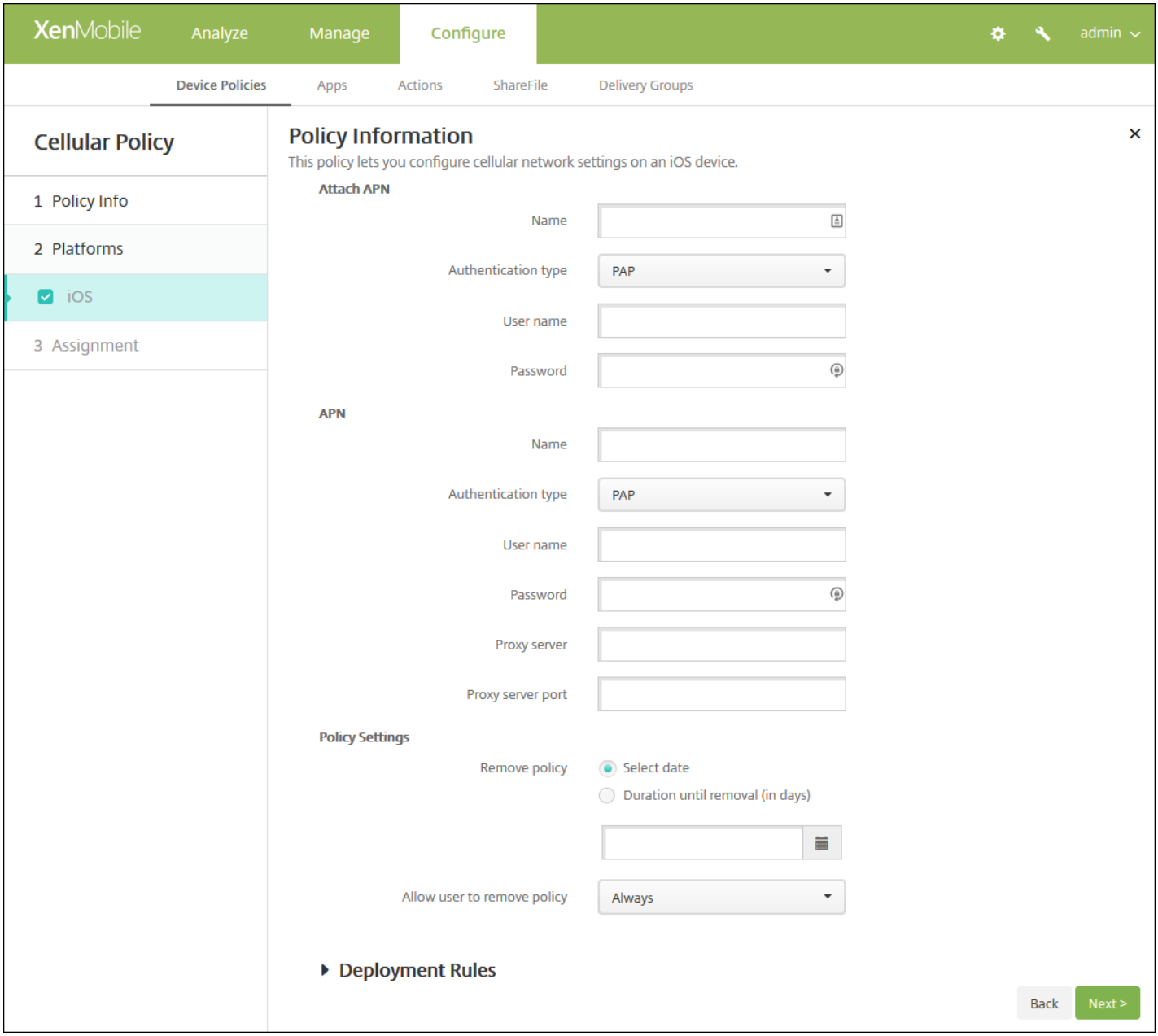
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Cellulaire**. La page d'informations sur la **Stratégie de réseau cellulaire** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Plate-forme iOS** s'affiche.



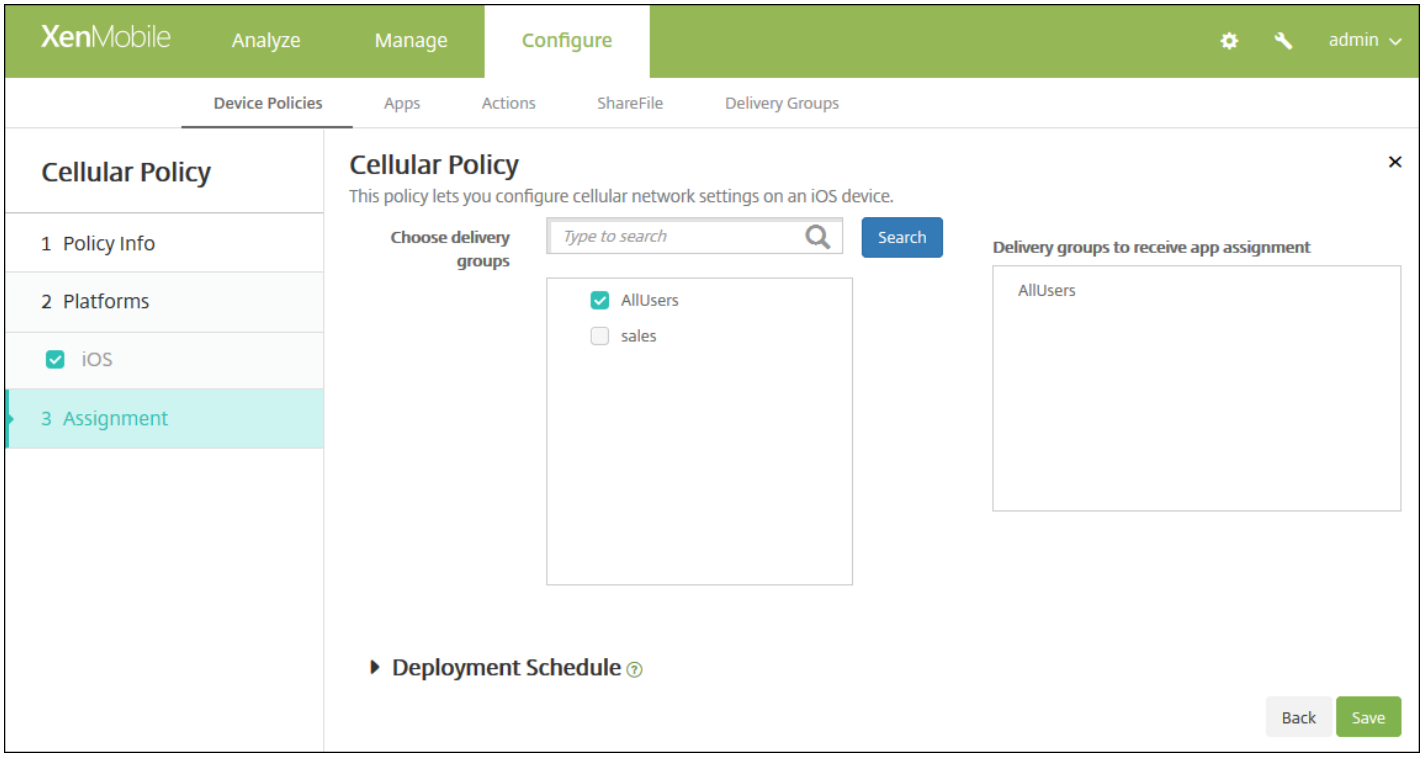
6. Configurez les paramètres suivants :

- **Attacher APN**
  - **Nom** : entrez un nom pour cette configuration.
  - **Type d'authentification** : dans la liste, cliquez sur **CHAP** (Challenge Handshake Authentication Protocol) ou **PAP** (Password Authentication Protocol). La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** : entrez un nom d'utilisateur à utiliser pour l'authentification.
- **APN**
  - **Nom** : entrez un nom pour la configuration du nom du point d'accès (APN).
  - **Type d'authentification** : dans la liste, cliquez sur **CHAP** ou **PAP**. La valeur par défaut est **PAP**.
  - **Nom d'utilisateur** : entrez un nom d'utilisateur à utiliser pour l'authentification.
  - **Mot de passe** : entrez un mot de passe à utiliser pour l'authentification.
  - **Serveur proxy** : entrez l'adresse réseau du serveur proxy.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de réseau cellulaire** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans

Paramètres > Propriétés du serveur. L'option de calendrier permanent n'est pas disponible pour iOS.

- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie du gestionnaire de connexions

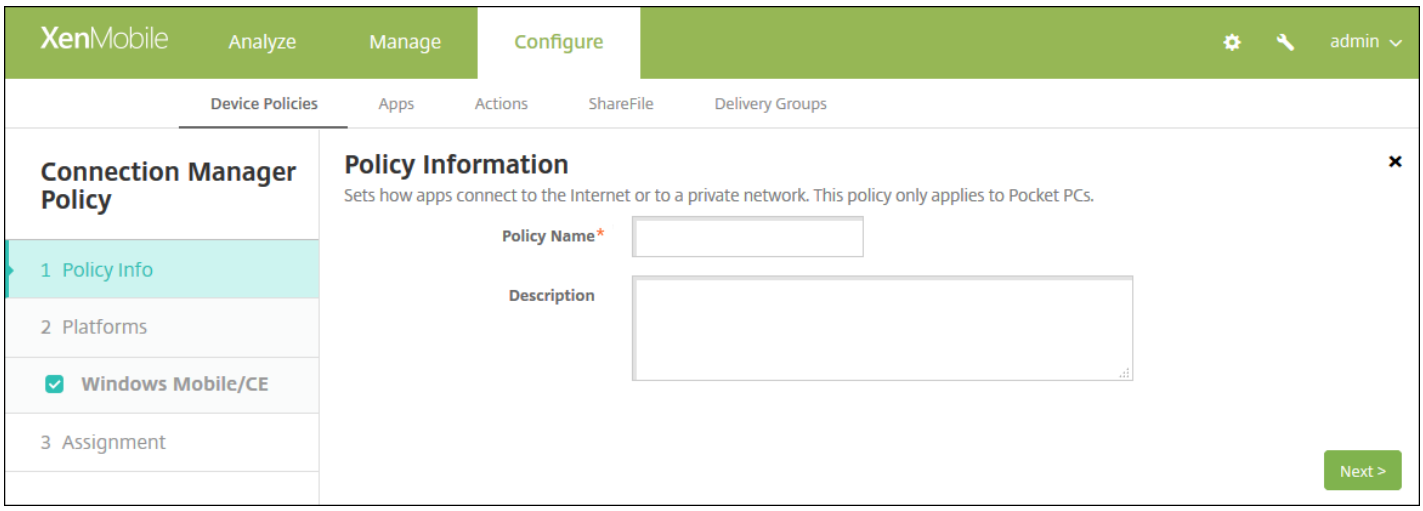
Feb 23, 2017

Dans XenMobile, vous pouvez spécifier les paramètres de connexion pour les applications qui se connectent automatiquement à Internet et à des réseaux privés. Cette stratégie est uniquement disponible pour Windows Pocket PC.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

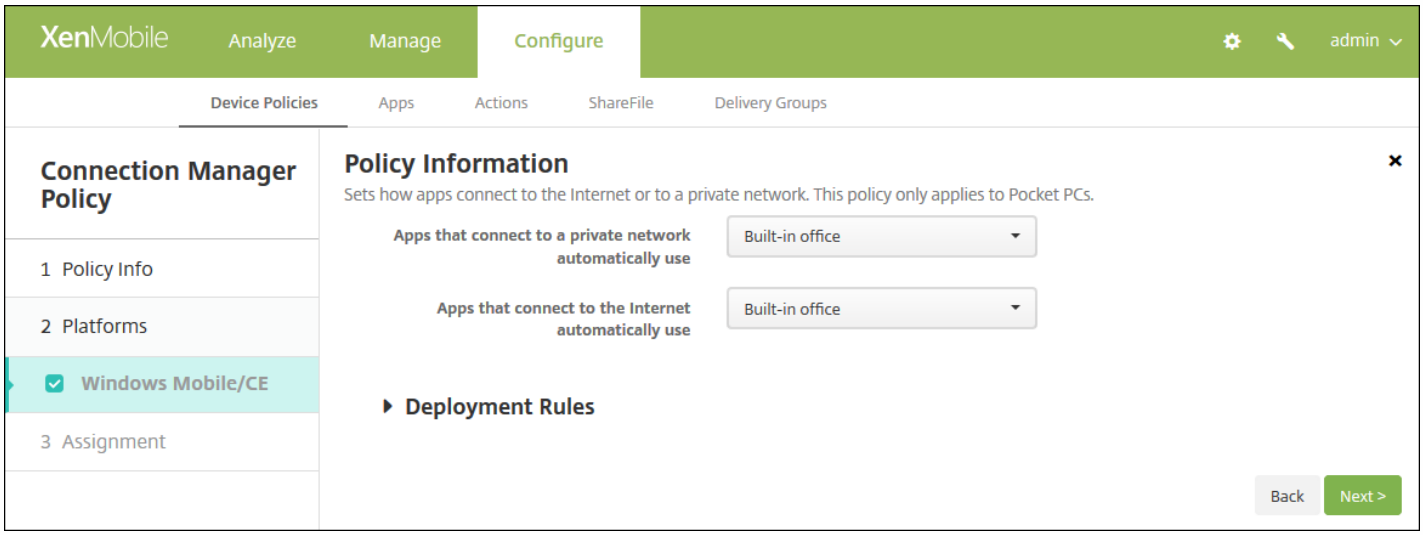
3. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **Gestionnaire de connexions**. La page d'informations **Gestionnaire de connexions** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Plate-forme : Windows Mobile/CE** s'affiche.



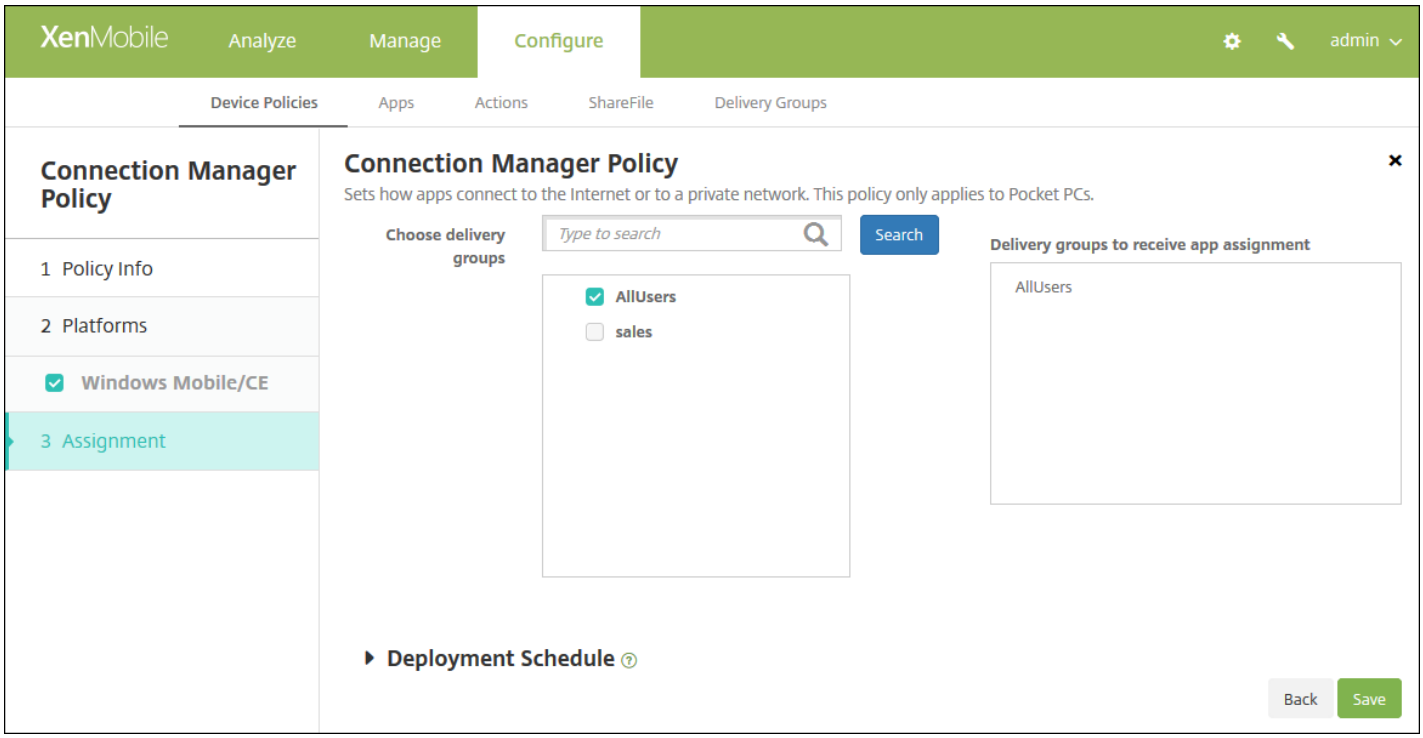
6. Configurez ces paramètres.

Remarque : **Bureau intégré** signifie que toutes les connexions sont effectuées vers l'intranet de votre entreprise et **Internet intégré** signifie que toutes les connexions sont effectuées vers Internet.

- **Les applications qui se connectent à un réseau privé utilisent automatiquement** : dans la liste, cliquez sur **Bureau intégré** ou **Internet intégré**. La valeur par défaut est **Bureau intégré**.
- **Les applications qui se connectent à Internet utilisent automatiquement** : dans la liste, cliquez sur **Bureau intégré** ou **Internet intégré**. La valeur par défaut est **Bureau intégré**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Gestionnaire de connexions** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de planification de connexion

Feb 23, 2017

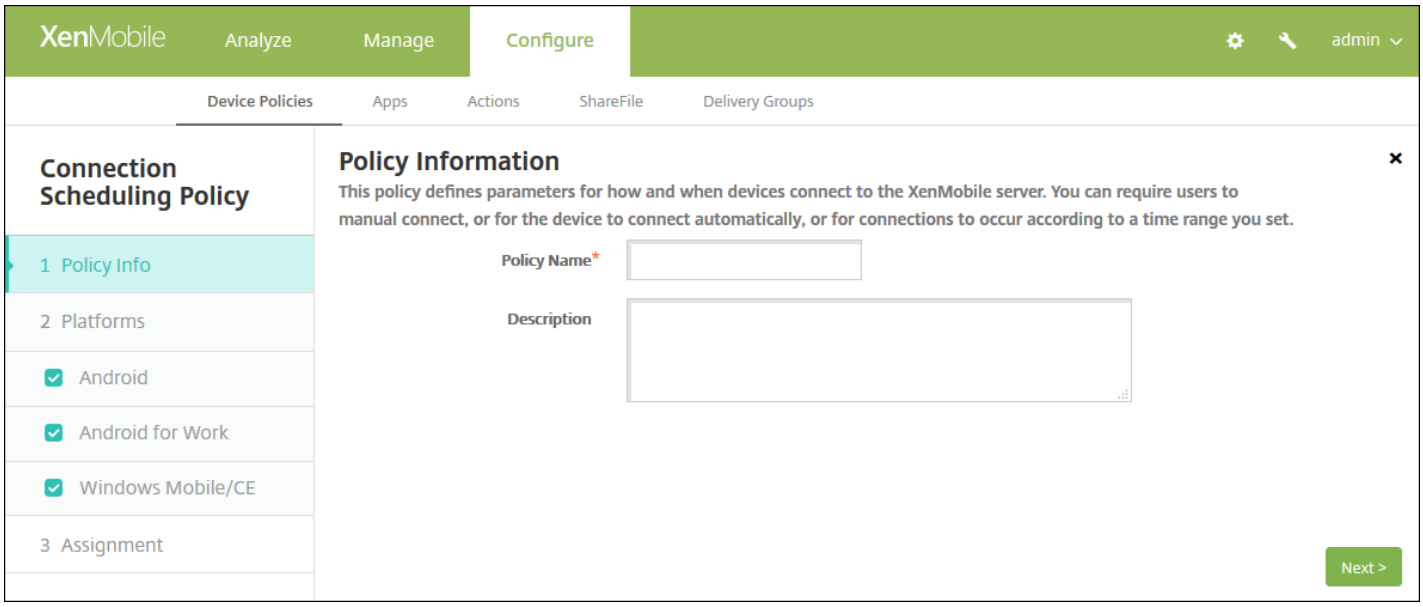
Vous pouvez créer des stratégies de planification de connexion afin de contrôler comment et quand les appareils se connectent à XenMobile. Notez que vous pouvez également configurer cette stratégie pour les appareils activés pour Android for Work.

Vous pouvez spécifier que les utilisateurs connectent leurs appareils manuellement, que les appareils restent connectés de manière permanente, ou que les appareils se connectent dans un intervalle de temps défini.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

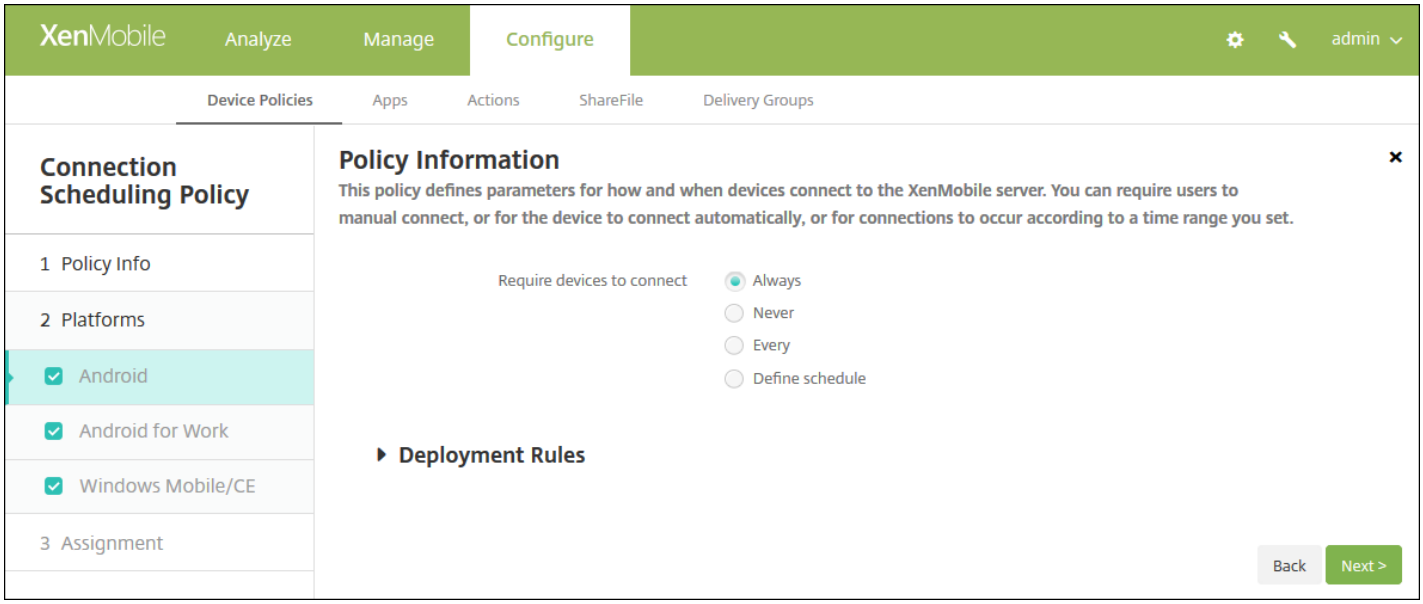
3. Cliquez sur **Planification**. La page d'informations **Stratégie de planification de connexion** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 8 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Configurez les paramètres suivants pour chacune des plates-formes sélectionnées :

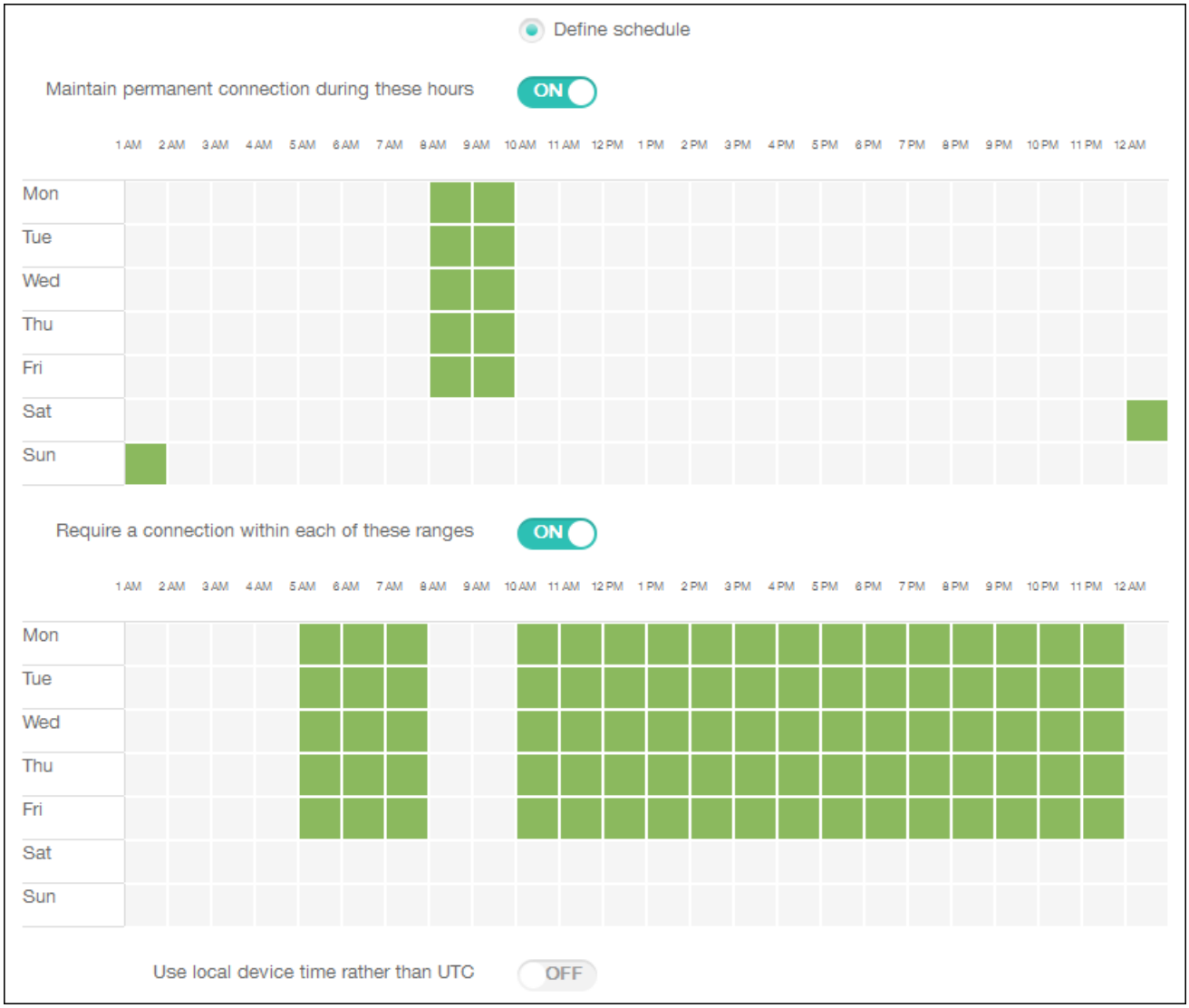
- **Exiger que les appareils se connectent** : cliquez sur l'option que vous souhaitez définir pour cette planification.
  - **Toujours** : conserve la connexion active de façon permanente. Sur l'appareil de l'utilisateur, XenMobile tente de se reconnecter au serveur XenMobile après une perte de connexion réseau et surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers. Citrix recommande cette option pour optimiser la sécurité. Lorsque vous sélectionnez **Toujours**, utilisez également le paramètre **Définir le délai d'expiration de la connexion** pour la **Stratégie de tunnel** pour vous assurer que la connexion ne décharge pas la batterie. En conservant la connexion active, vous pouvez distribuer des commandes de sécurité telles que l'effacement ou le verrouillage de l'appareil à la demande. Vous devez également sélectionner l'option **Calendrier de déploiement Déployer pour les connexions permanentes** dans chaque stratégie déployée sur l'appareil.
  - **Jamais** : connexion manuelle. Les utilisateurs doivent lancer la connexion depuis XenMobile sur leurs appareils. Citrix ne recommande pas cette option pour les déploiements de production, car elle empêche le déploiement des stratégies de sécurité sur les appareils, ce qui signifie que les utilisateurs ne recevront jamais les nouvelles applications ou stratégies.
  - **Toutes les** : se connecte à l'intervalle défini. Lorsque cette option est activée et que vous envoyez une stratégie de sécurité telle qu'un effacement ou verrouillage, XenMobile traite l'action sur l'appareil la prochaine fois que l'appareil se connecte. Lorsque vous sélectionnez cette option, le champ **Se connecter toutes les N minutes** apparaît. Vous devez y entrer le nombre de minutes après lesquelles l'appareil doit se reconnecter. La valeur par défaut est de **20**.
  - **Définir un calendrier** : lorsque cette option est activée, sur l'appareil de l'utilisateur, XenMobile tente de se reconnecter au serveur XenMobile après une perte de connexion réseau et surveille la connexion en transmettant des paquets de contrôle à intervalles réguliers dans le délai imparti. Pour savoir comment définir un délai de connexion, consultez la section Définition d'un délai de connexion.
    - **Maintenir une connexion permanente durant ces heures** : les appareils des utilisateurs doivent être connectés pendant l'intervalle de temps défini.

- **Exiger une connexion dans chacun de ces intervalles** : les appareils des utilisateurs doivent être connectés au moins une fois dans les intervalles de temps définis.
- **Utiliser l'heure locale de l'appareil comme référence et non l'heure UTC** : synchronise les intervalles définis avec l'appareil local plutôt que le temps universel coordonné (UTC).

Définition d'un délai de connexion

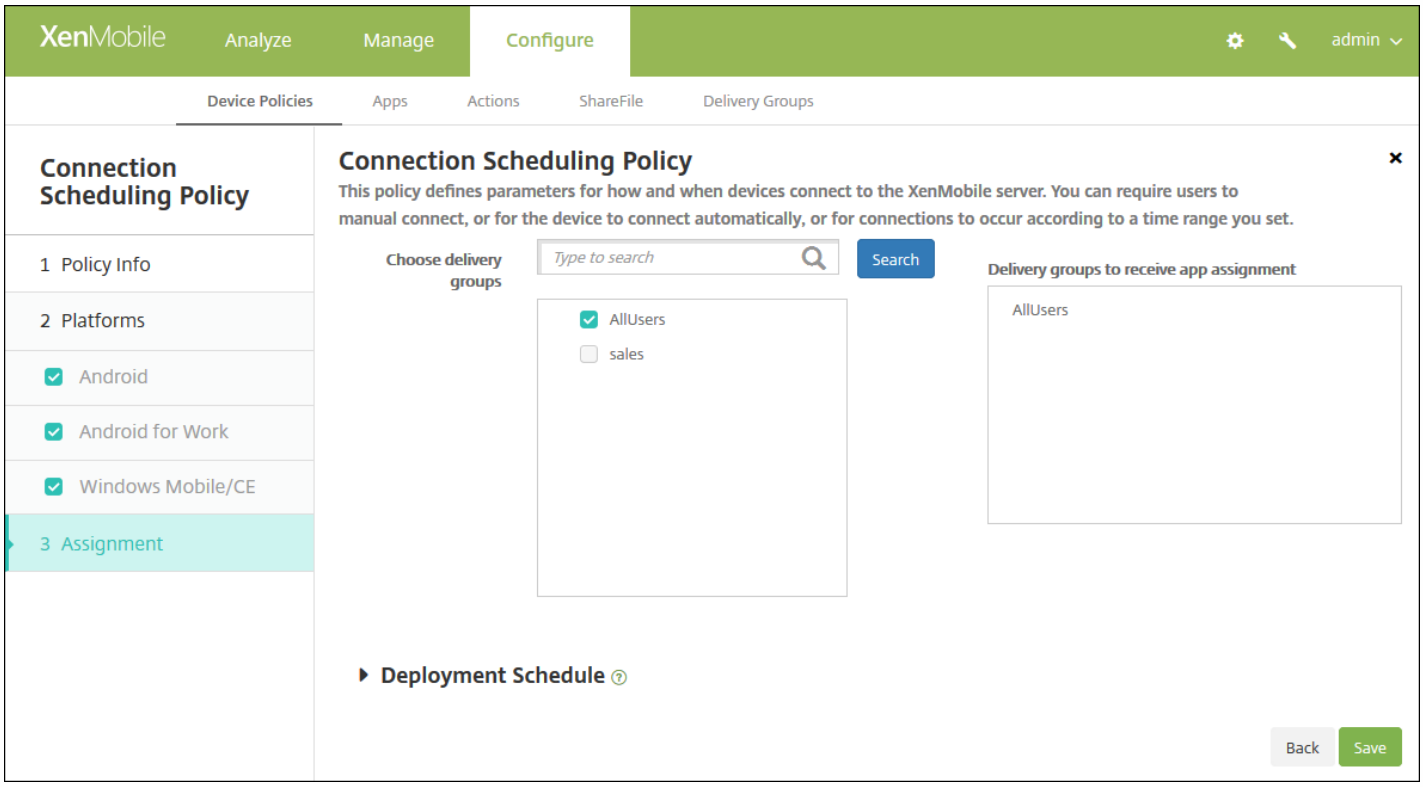
Lorsque vous activez les options suivantes, un calendrier s'affiche dans lequel vous pouvez définir les délais souhaités. Vous pouvez activer l'une ou l'autre de ces options ou les deux options pour exiger une connexion permanente durant des heures spécifiques ou exiger une connexion dans des délais impartis. Chaque carré dans le calendrier correspond à 30 minutes, par conséquent si vous souhaitez établir une connexion entre 8:00 AM et 9:00 AM chaque jour de la semaine, cliquez sur les deux carrés sur le calendrier entre 8 AM et 9 AM chaque jour de la semaine.

Par exemple, les deux calendriers dans la figure suivante requièrent une connexion permanente entre 8:00 et 9:00 chaque jour de la semaine, une connexion permanente entre 12:00 AM samedi et 1:00 AM dimanche, et au moins une connexion chaque jour de la semaine entre 5:00 AM et 8:00 AM ou entre 10:00 et 11:00 PM.



8. Configurez les règles de déploiement.

9. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de planification de connexion** s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

12. Cliquez sur **Enregistrer**.

Stratégie de contacts (CardDAV)

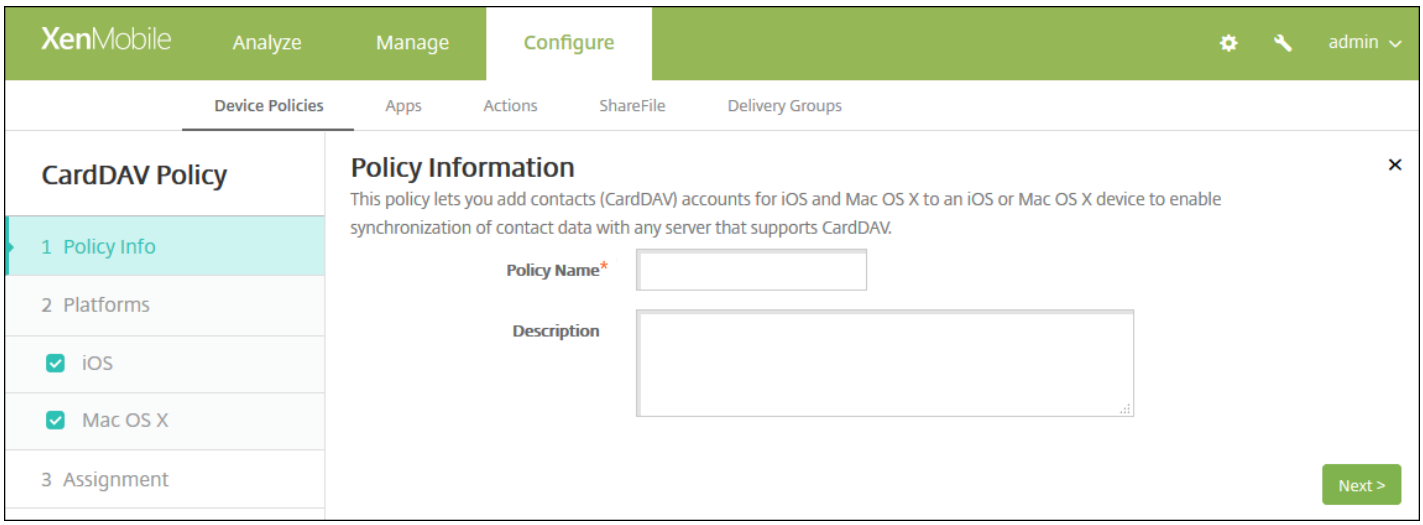
Feb 23, 2017

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS ou Mac OS X pour permettre à leurs utilisateurs de synchroniser les données de contact avec tout serveur qui prend en charge CalDAV.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Contacts (CardDAV)**. La page **Stratégie CardDAV** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

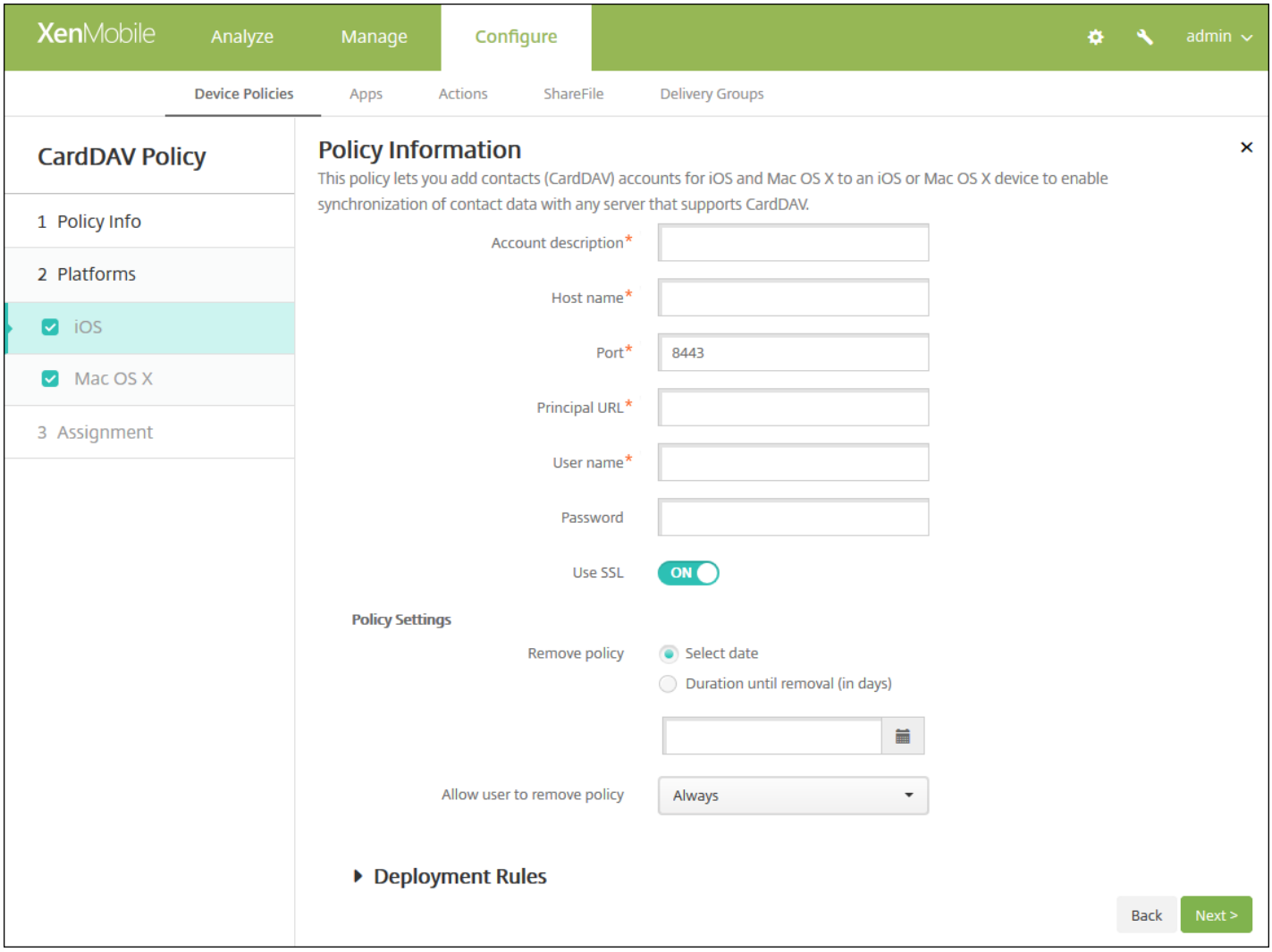
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

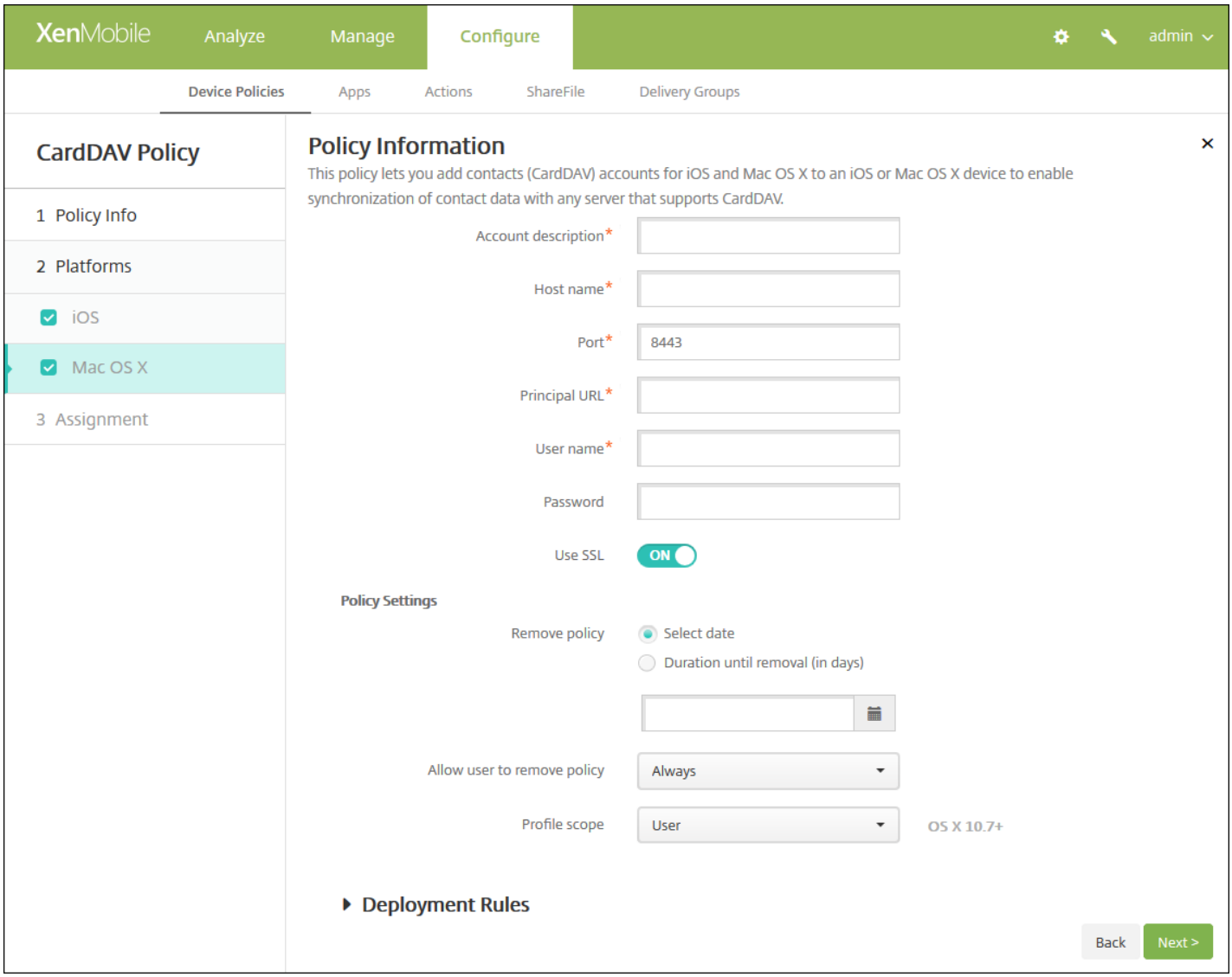
Configurer les paramètres pour iOS



Pour configurer ces paramètres :

- **Description du compte** : entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte** : entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port** : entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est de **8443**.
- **URL principale** : entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur** : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe** : entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **ON**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de Code secret de suppression, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X



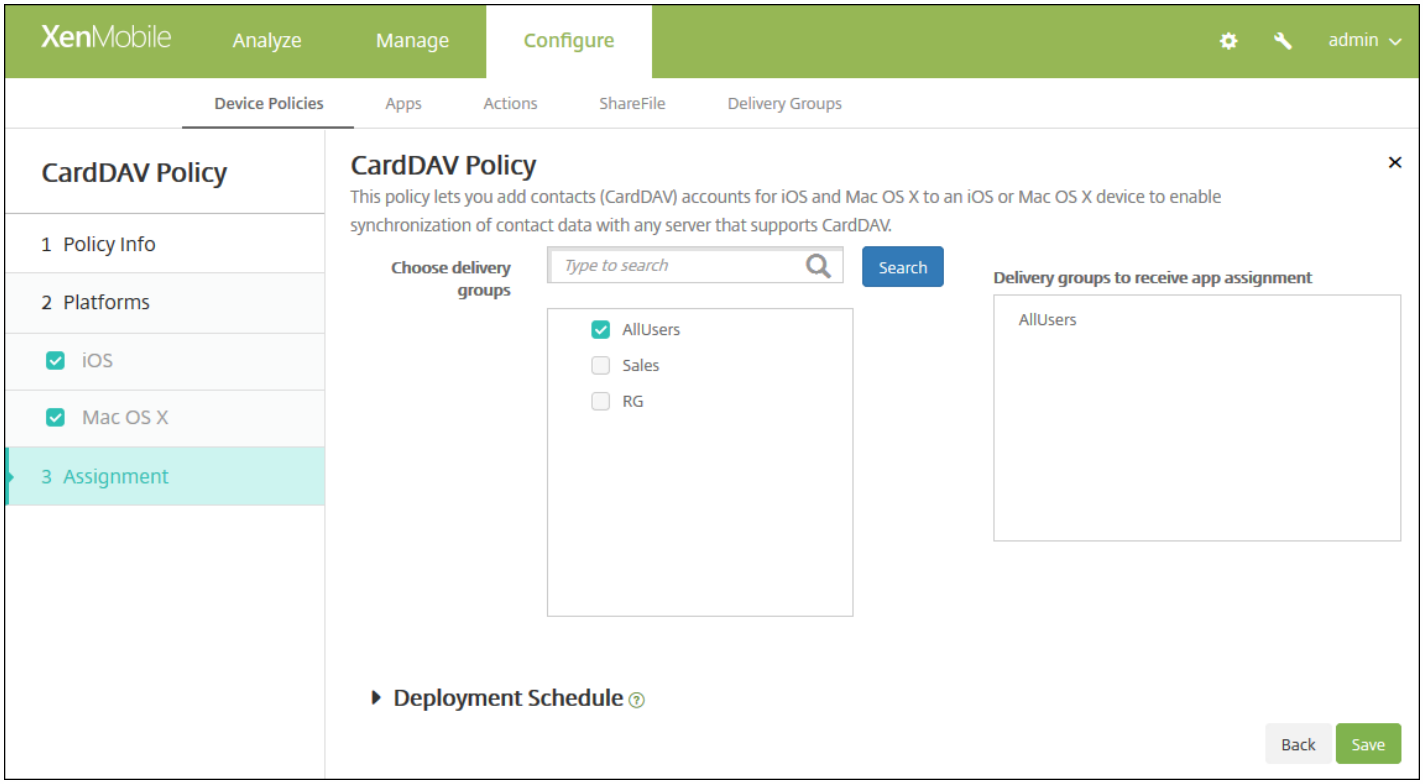
Pour configurer ces paramètres :

- **Description du compte** : entrez une description du compte. Ce champ est obligatoire.
- **Nom d'hôte** : entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
- **Port** : entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est de **8443**.
- **URL principale** : entrez l'adresse URL du calendrier de l'utilisateur.
- **Nom d'utilisateur** : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
- **Mot de passe** : entrez un mot de passe utilisateur (facultatif).
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est **ON**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de Code secret de suppression, entrez le mot de passe requis.

- En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie CardDAV** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**,

qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies Copier les applications sur le conteneur Samsung

Feb 23, 2017

Vous pouvez spécifier des applications déjà installées sur un appareil à copier vers un conteneur SEAMS ou un conteneur KNOX sur les appareils Samsung pris en charge (pour plus d'informations sur les appareils pris en charge, consultez la section Appareils Samsung KNOX pris en charge de Samsung). Les applications copiées sur le conteneur SEAMS sont disponibles sur les écrans d'accueil des utilisateurs ; les applications copiées sur le conteneur KNOX sont uniquement disponibles lorsque les utilisateurs se connectent au conteneur KNOX.

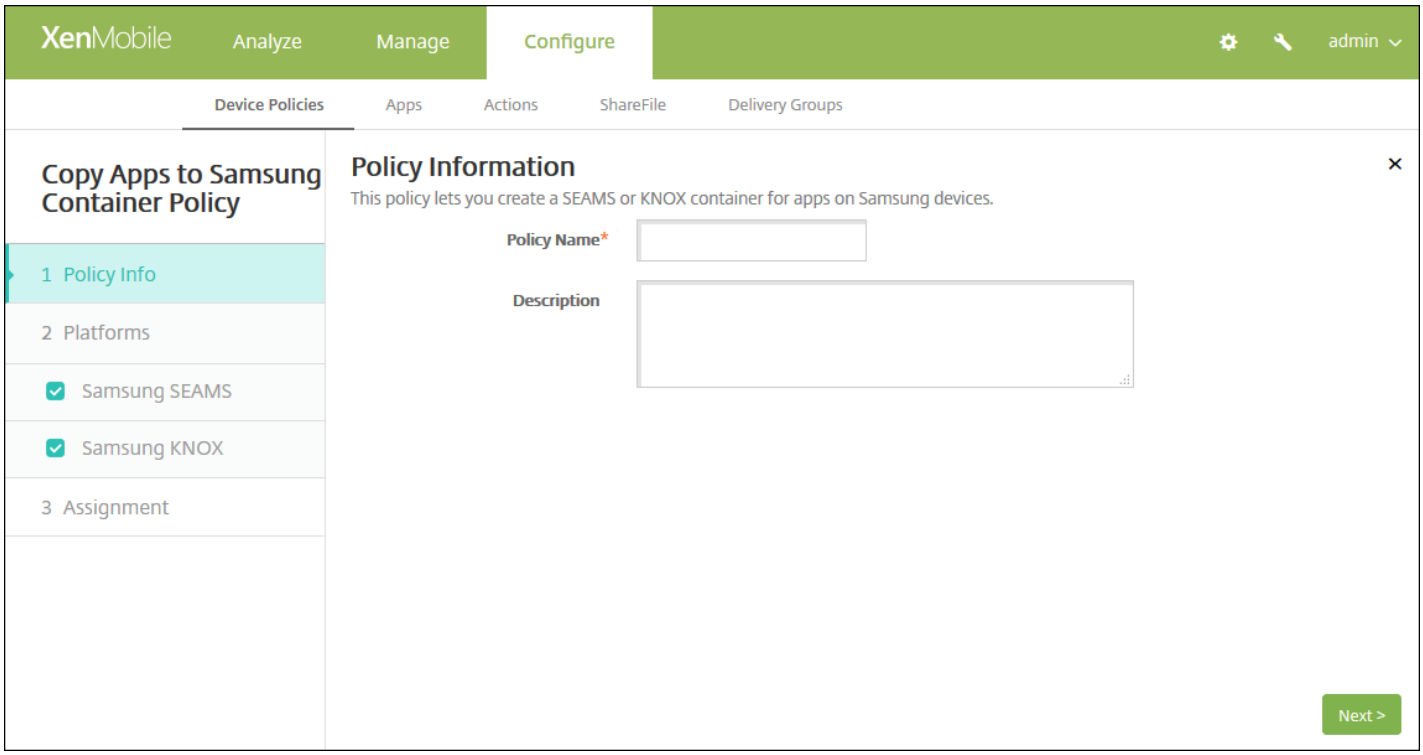
Configuration requise :

- L'appareil doit être inscrit dans XenMobile.
- Les clés MDM Samsung (ELM et KLM) doivent être déployées (pour la marche à suivre, consultez la section Stratégies de clé de licence MDM Samsung).
- Les applications sont déjà installées sur l'appareil
- Initialisez KNOX sur l'appareil pour copier les applications dans le conteneur KNOX.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

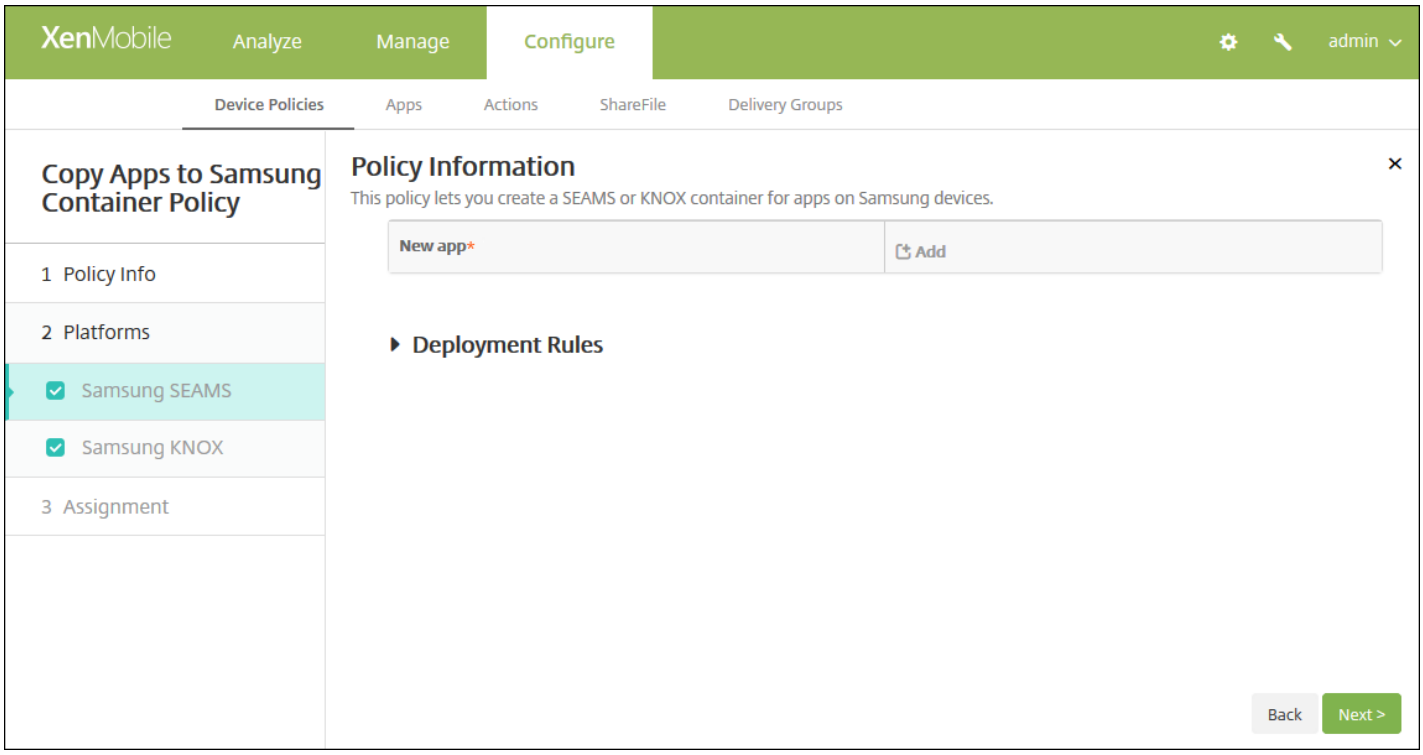
3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Copier les applications sur le conteneur Samsung**. La page d'informations **Copier les applications sur la stratégie de conteneur Samsung** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous Plates-formes, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 8 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Configurez le paramètre suivant pour chaque plate-forme que vous avez sélectionnée.

- **Nouvelle application** : pour chaque application que vous souhaitez ajouter à la liste, cliquez sur **Ajouter**, puis procédez comme suit :
  - Entrez un ID de package ; par exemple, com.mobiwolf.lacingart pour l'application LacingArt.
  - Cliquez sur **Enregistrer** ou sur **Annuler**.

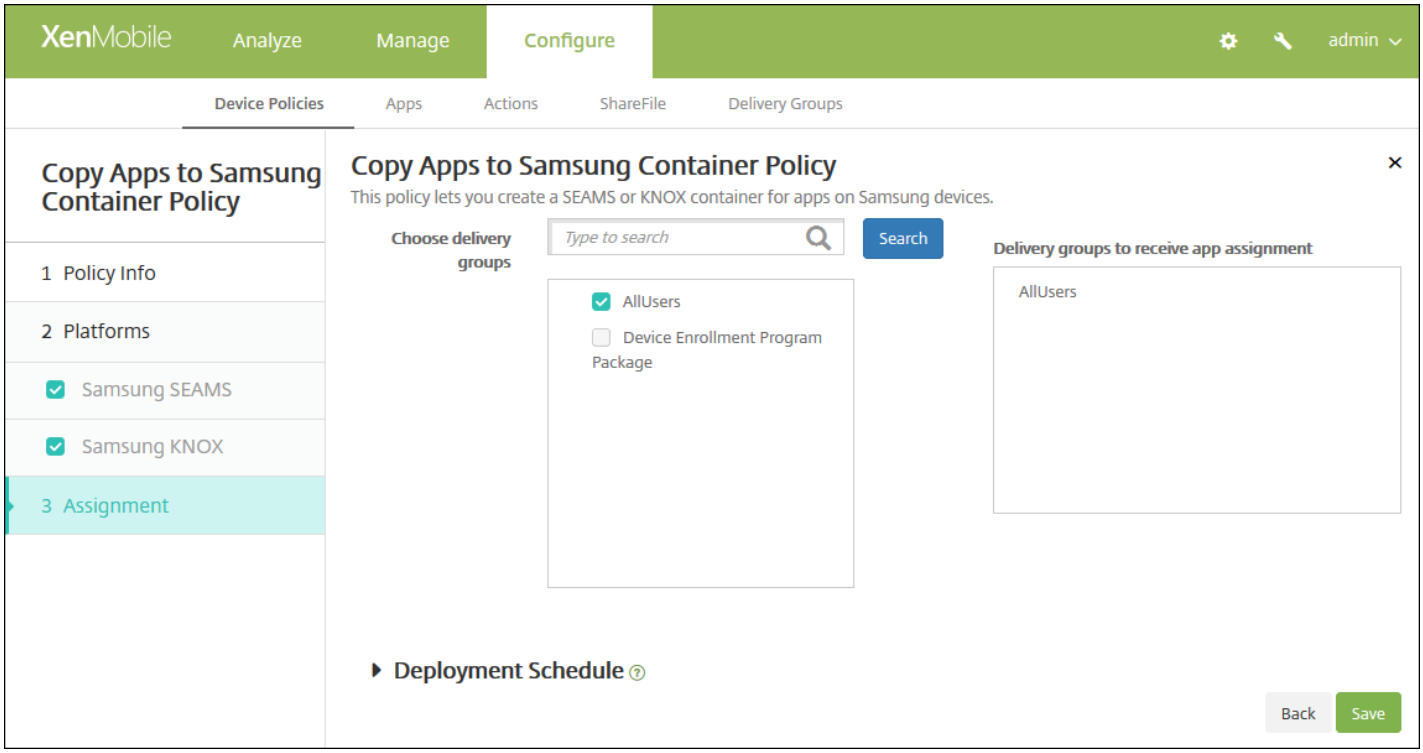
    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

8. Configurez les règles de déploiement.

9. Cliquez sur **Next**. La page de plate-forme suivante ou la page d'attribution **Copier les applications sur la stratégie de**

conteneur Samsung s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans Paramètres > Propriétés du serveur. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de Déployer pour les connexions permanentes, qui ne s'applique pas à iOS.

12. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Une fois que la stratégie est correctement déployée, les applications SEAMS s'affichent sur la page **Détails de l'appareil** sous l'en-tête **Emplacement: emplacement du SEAMS d'entreprise** et les applications KNOX s'affichent sous l'en-tête

Emplacement: Entreprise.

Stratégies d'informations d’identification

Feb 23, 2017

Vous pouvez créer des stratégies d'informations d'identification dans XenMobile afin d'intégrer l'authentification à votre configuration PKI dans XenMobile, comme une entité PKI, un keystore, un fournisseur d'informations d'identification ou un certificat de serveur. Pour de plus amples informations sur les informations d’identification, consultez Certificats.

Vous pouvez créer des stratégies d'informations d'identification pour les appareils iOS, Mac OS X, Android, Android for Work, Windows /DesktopTablet, Windows Mobile/CE et Windows Phone. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Paramètres iOS

Paramètres Mac OS X

Paramètres Android et Android for Work

Paramètres Windows Desktop/Tablet

Paramètres Windows Mobile/CE

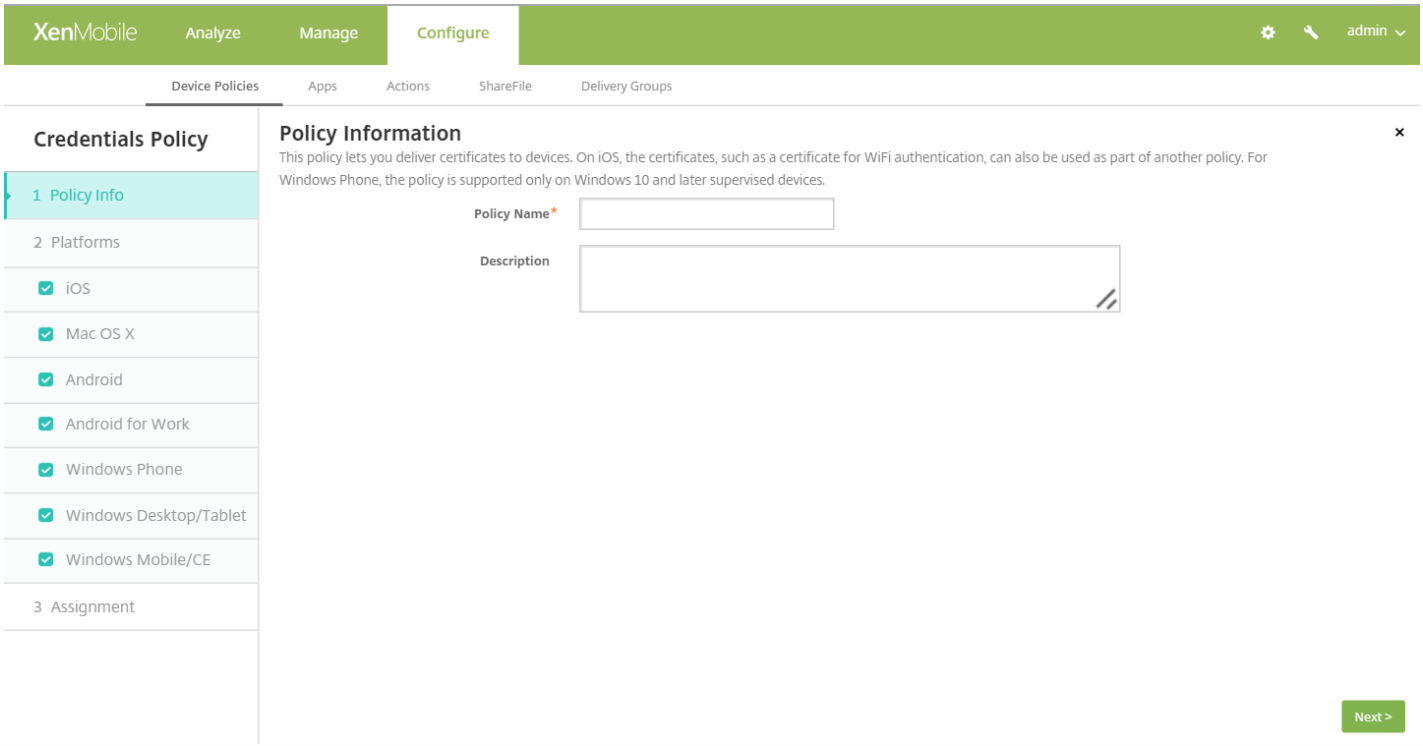
Paramètres Windows Phone

Avant de pouvoir créer cette stratégie, vous devez connaître les informations d'identification que vous projetez d'utiliser pour chaque plate-forme, ainsi que les certificats et les mots de passe.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Informations d'identification**. La page **Stratégie d'informations d'identification** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

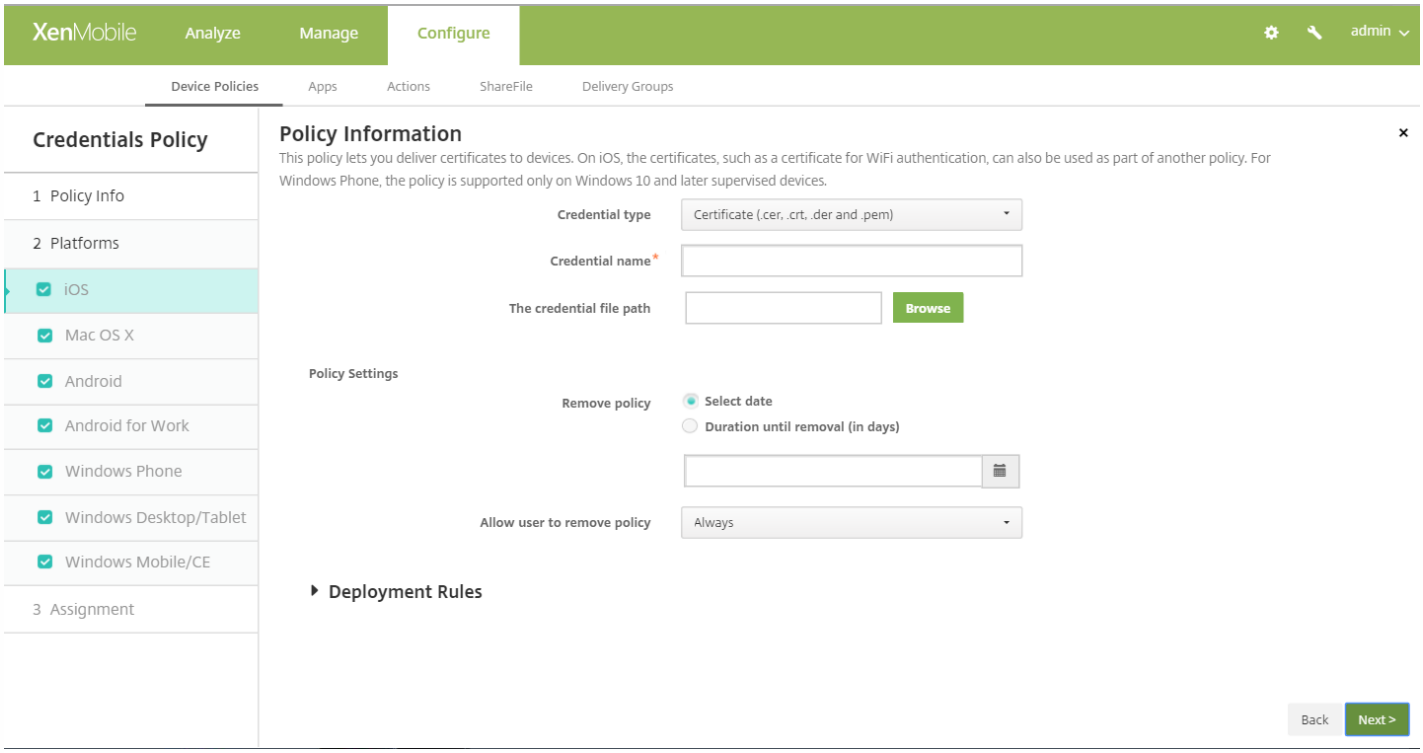
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

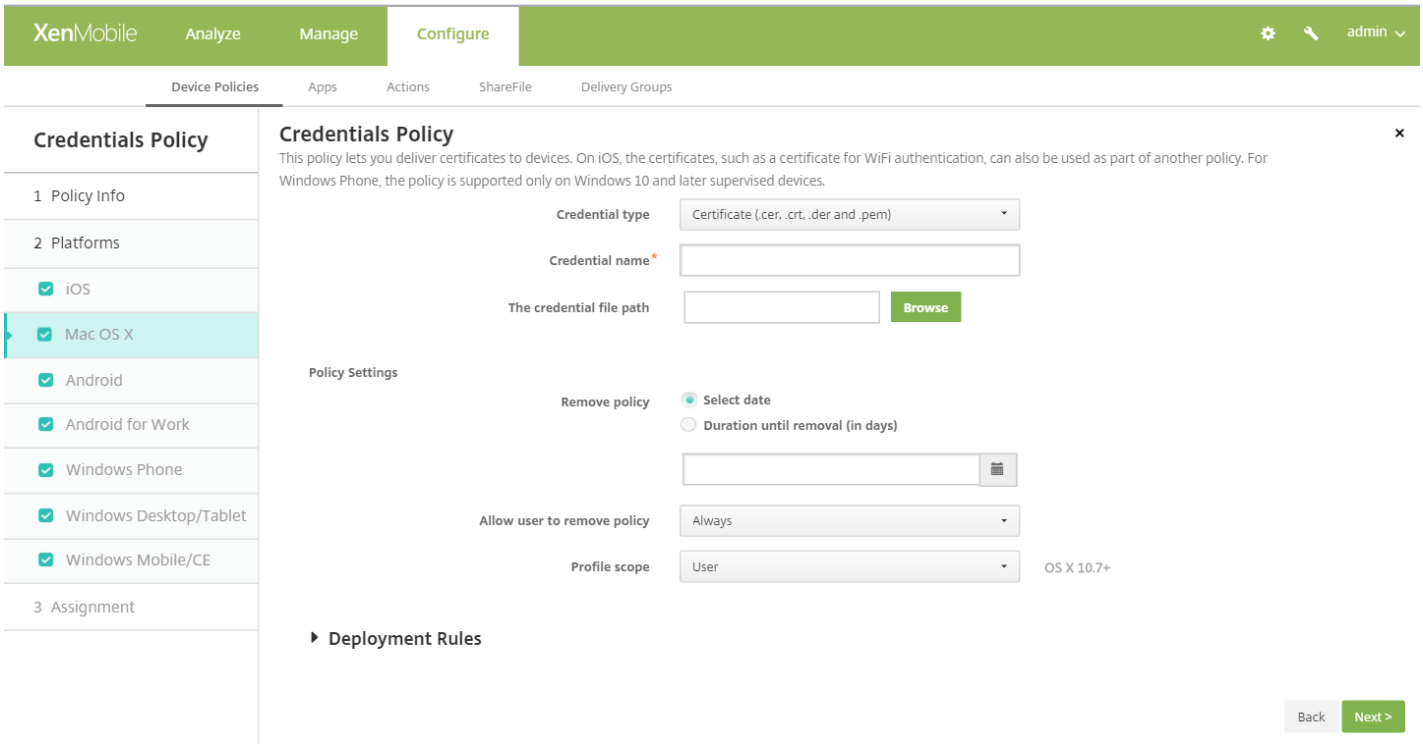
Configurer les paramètres pour iOS



Configurez les paramètres suivants :

- **Type de certificat** : dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat, en cliquant sur Parcourir et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat, en cliquant sur Parcourir et accédez à l'emplacement du fichier.
    - **Mot de passe** : entrez le mot de passe du magasin de clés pour le certificat.
  - **Certificat de serveur**
    - **Certificat serveur** : dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités** : dans la liste, cliquez sur le nom du fournisseur d'identités.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la **liste Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

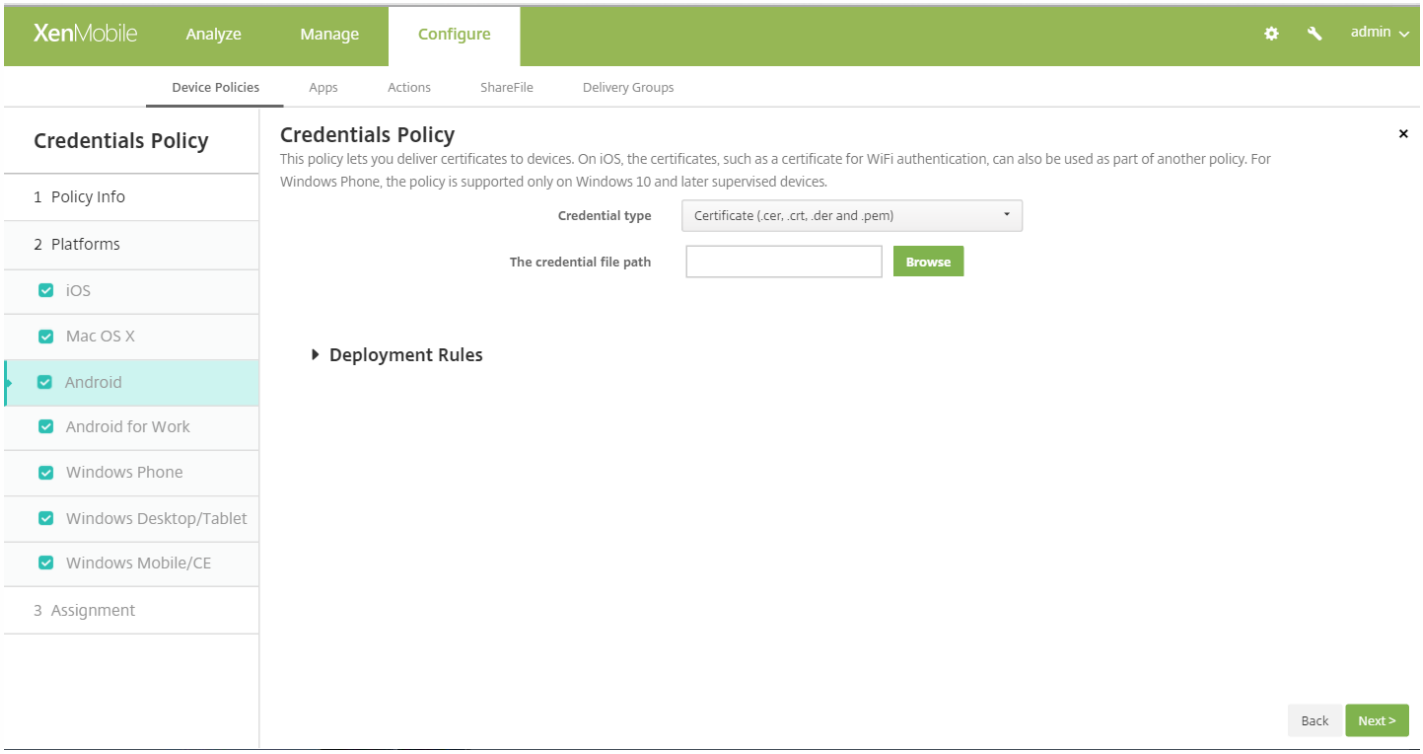
Configurer les paramètres pour Mac OS X



Configurez les paramètres suivants :

- **Type de certificat** : dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
    - **Mot de passe** : entrez le mot de passe du magasin de clés pour le certificat.
  - **Certificat de serveur**
    - **Certificat serveur** : dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités** : dans la liste, cliquez sur le nom du fournisseur d'identités.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la **liste Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
  - En regard de **Étendue de la stratégie**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

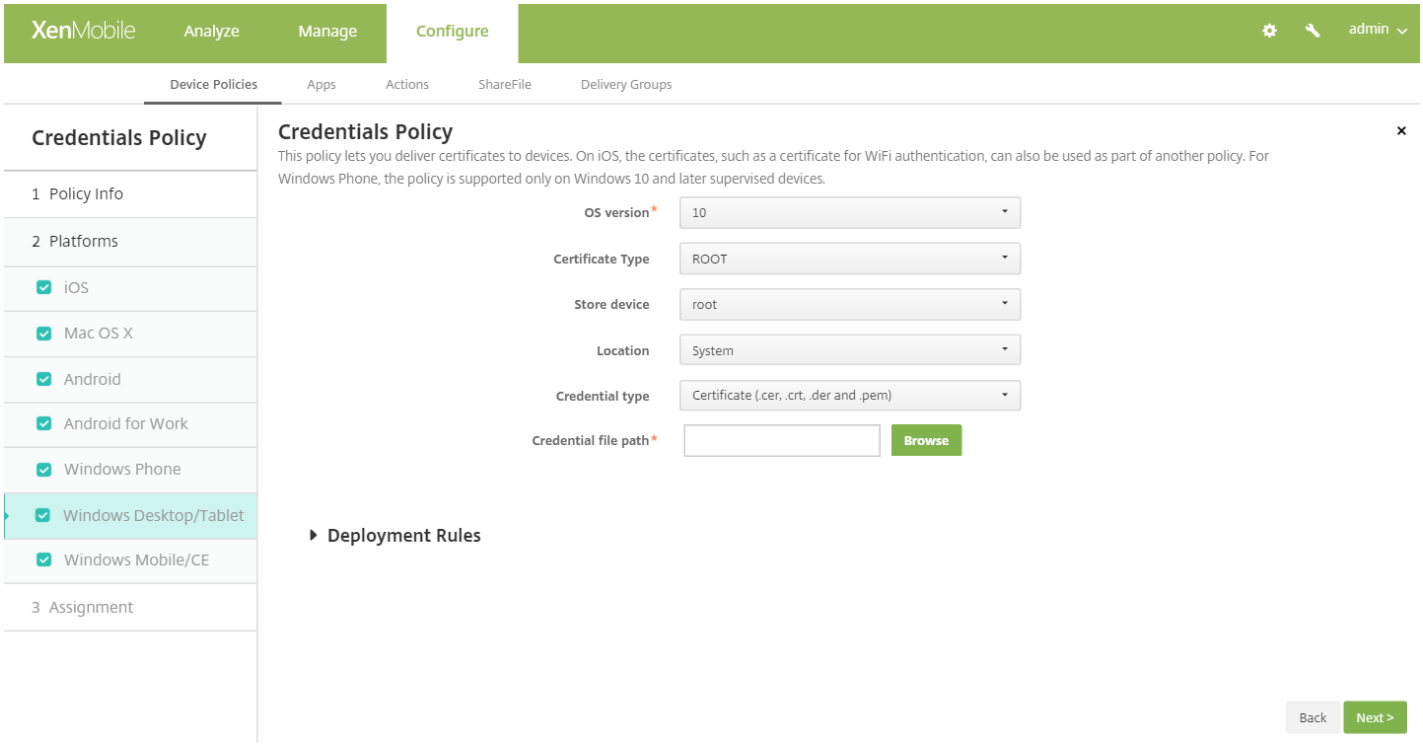
Configurer les paramètres pour Android et Android for Work



Configurez les paramètres suivants :

- **Type de certificat** : dans la liste, cliquez sur le type de certificat à utiliser avec cette stratégie et entrez les informations suivantes pour le certificat que vous sélectionnez :
  - **Certificat**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat en cliquant sur Parcourir et accédez à l'emplacement du fichier.
  - **Keystore**
    - **Nom du certificat** : entrez un nom unique pour le certificat.
    - **Emplacement du certificat** : sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
    - **Mot de passe** : entrez le mot de passe du magasin de clés pour le certificat.
  - **Certificat de serveur**
    - **Certificat serveur** : dans la liste, cliquez sur le certificat à utiliser.
  - **Fournisseur d'identités**
    - **Fournisseur d'identités** : dans la liste, cliquez sur le nom du fournisseur d'identités.

Configurer les paramètres pour Windows Desktop/Tablet



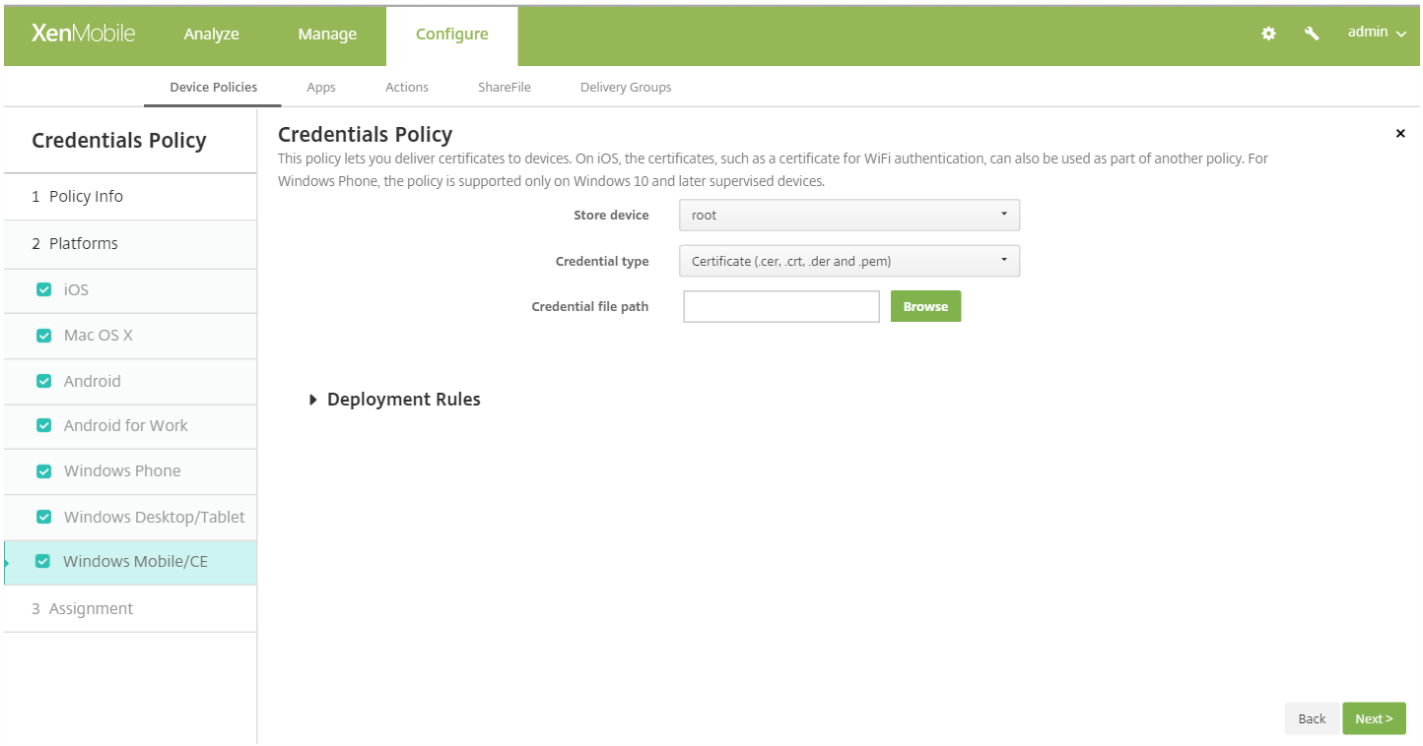
Configurez les paramètres suivants :

- **Version de l'OS** : dans la liste, cliquez sur **8.1** pour Windows 8.1 ou **10** pour Windows 10. La valeur par défaut est **10**.

Paramètres pour Windows 10

Paramètres Windows 8.1

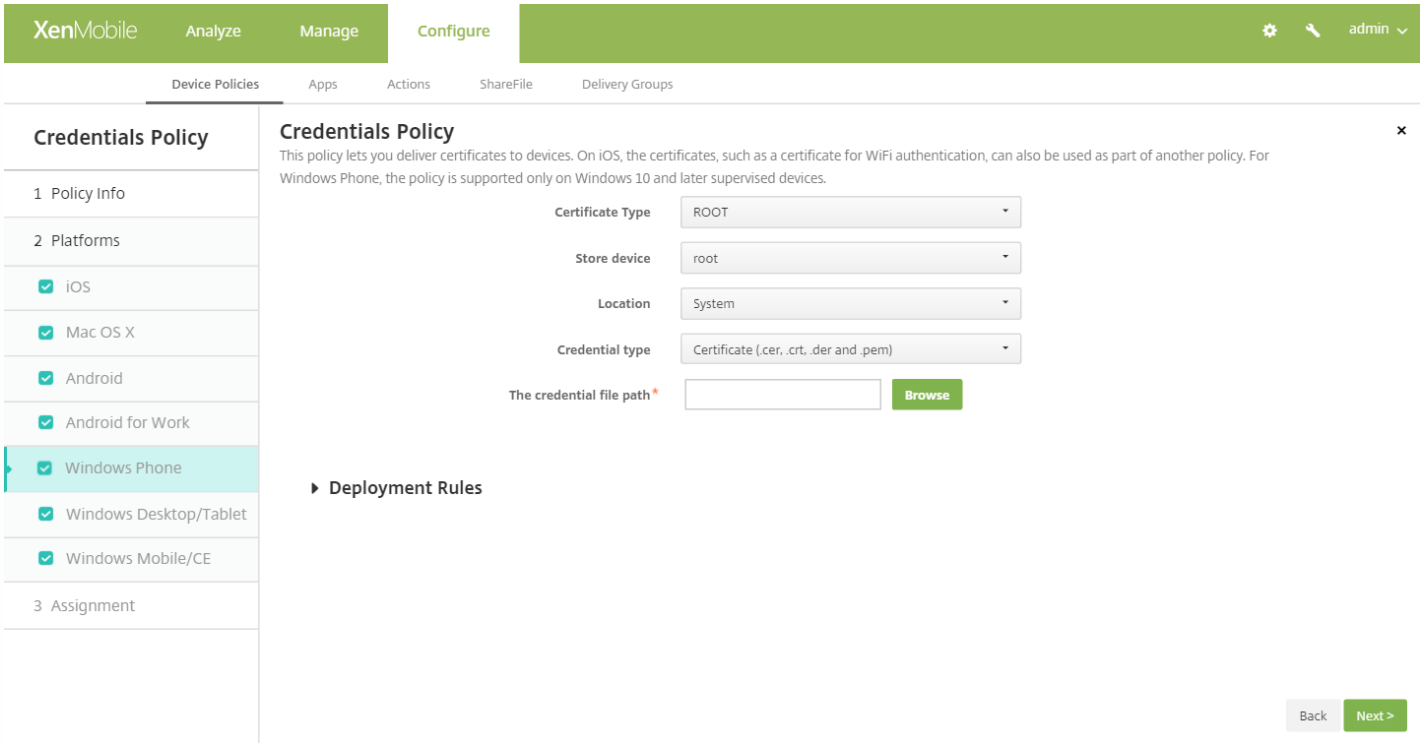
Configurer les paramètres pour Windows Mobile/CE



Configurez les paramètres suivants :

- **Périphérique de stockage** : dans la liste, cliquez sur l'emplacement du magasin de certificats pour le certificat. La valeur par défaut est **racine**. Les options sont les suivantes :
  - **Autorités de certification privilégiées** : les applications signées avec un certificat appartenant à ce magasin s'exécutent avec un niveau de confiance privilégié.
  - **Autorités de certification non privilégiées** : les applications signées avec un certificat appartenant à ce magasin s'exécutent avec un niveau de confiance normal.
  - **Editeurs de logiciels approuvés** : des éditeurs de logiciels approuvés sont utilisés pour signer les fichiers .cab..
  - **root** : un magasin de certificats qui contient des certificats racines ou auto-signés.
  - **Autorité de certification** : magasin de certificats qui contient des informations cryptographiques, y compris des autorités de certificat intermédiaire.
  - **Mon magasin** : magasin de certificats qui contient des certificats personnels.
- **Type de certificat** : le certificat est le seul type de certificat pour appareils Windows Mobile/CE.
- **Emplacement du certificat** : sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

Configurer les paramètres pour Windows Phone

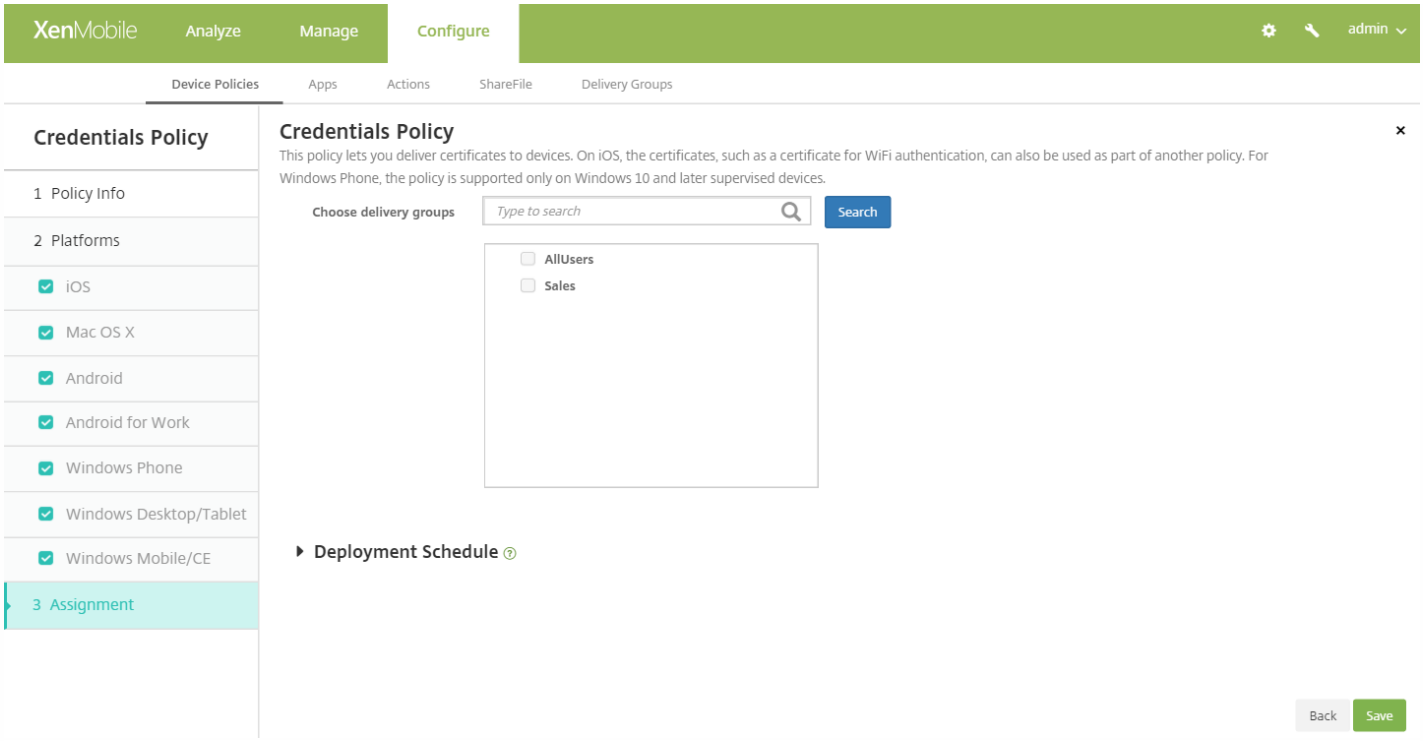


Configurez les paramètres suivants :

- **Type de certificat** : dans la liste, cliquez sur **ROOT** ou **CLIENT**.
- Si vous avez sélectionné **ROOT**, configurez les paramètres suivants :
  - **Périphérique de stockage** : dans la liste, cliquez sur **racine**, **Mon magasin**, ou **Autorité de certification** pour l'emplacement du magasin de certificats pour le certificat. **Mon magasin** stocke les certificats dans les magasins de certificats des utilisateurs.
  - **Emplacement** : Système est le seul emplacement pour les téléphones Windows.
  - **Type de certificat** : le certificat est le seul type de certificat pour téléphones Windows.
  - **Emplacement du certificat** : sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- Si vous avez sélectionné **CLIENT**, configurez les paramètres suivants :
  - **Emplacement** : **Système** est le seul emplacement pour les téléphones Windows.
  - **Type de certificat** : **Keystore** est le seul type de certificat pour téléphones Windows.
  - **Nom du certificat** : entrez un nom pour le certificat. Ce champ est obligatoire.
  - **Emplacement du certificat** : sélectionnez le fichier de certificat en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
  - **Mot de passe** : entrez le mot de passe associé au certificat. Ce champ est obligatoire.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie d'informations d'identification** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies XML personnalisées

Feb 23, 2017

Vous pouvez créer des stratégies XML personnalisées dans XenMobile pour personnaliser les fonctionnalités suivantes sur Windows Phone, Windows Desktop/Tablet, and Windows Mobile/CE :

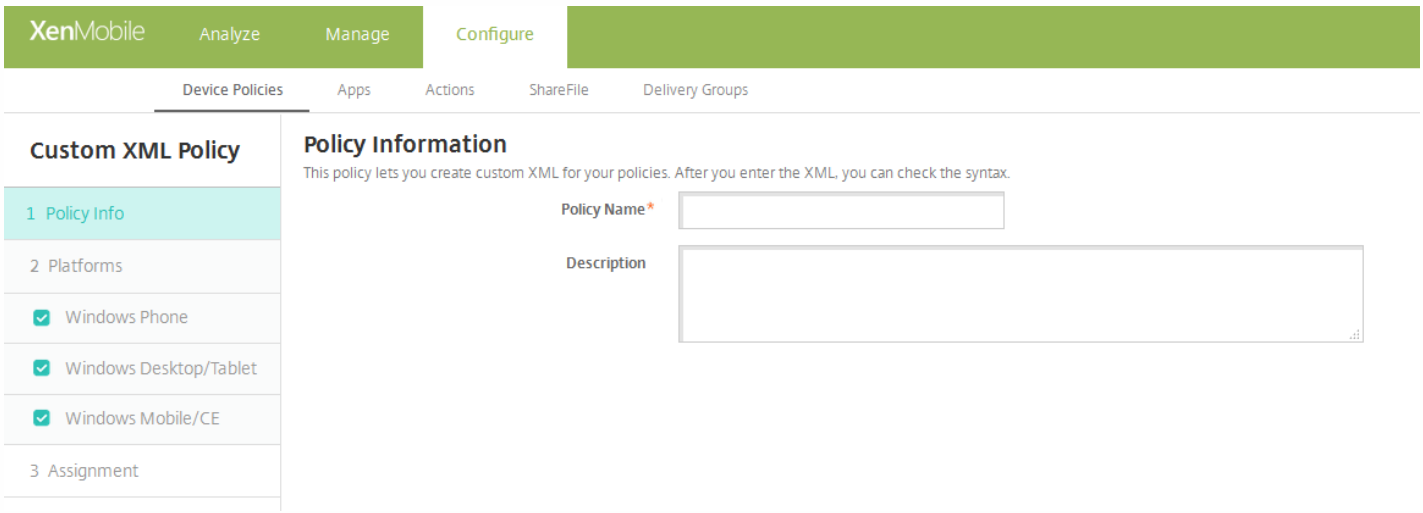
- Provisioning, qui comprend la configuration de l'appareil, et l'activation ou la désactivation de fonctionnalités.
- Configuration de l'appareil, ce qui permet aux utilisateurs de modifier les paramètres sur l'appareil.
- Mises à niveau logicielles, ce qui comprend la mise à disposition de nouveaux logiciels ou de correctifs de bogues à charger sur l'appareil, y compris des applications et logiciels système.
- Gestion des pannes, ce qui comprend la réception de rapports d'erreur et d'état à partir de l'appareil.

Vous créez votre propre configuration XML personnalisée à l'aide de l'API Open Mobile Alliance Device Management (OMA DM) dans Windows. La création de code XML personnalisé avec l'API OMA DM n'est pas couverte dans cette rubrique. Pour de plus amples informations sur l'utilisation de l'API OMA DM, veuillez consulter la section OMA Device Management sur le site de Microsoft Developer Network.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

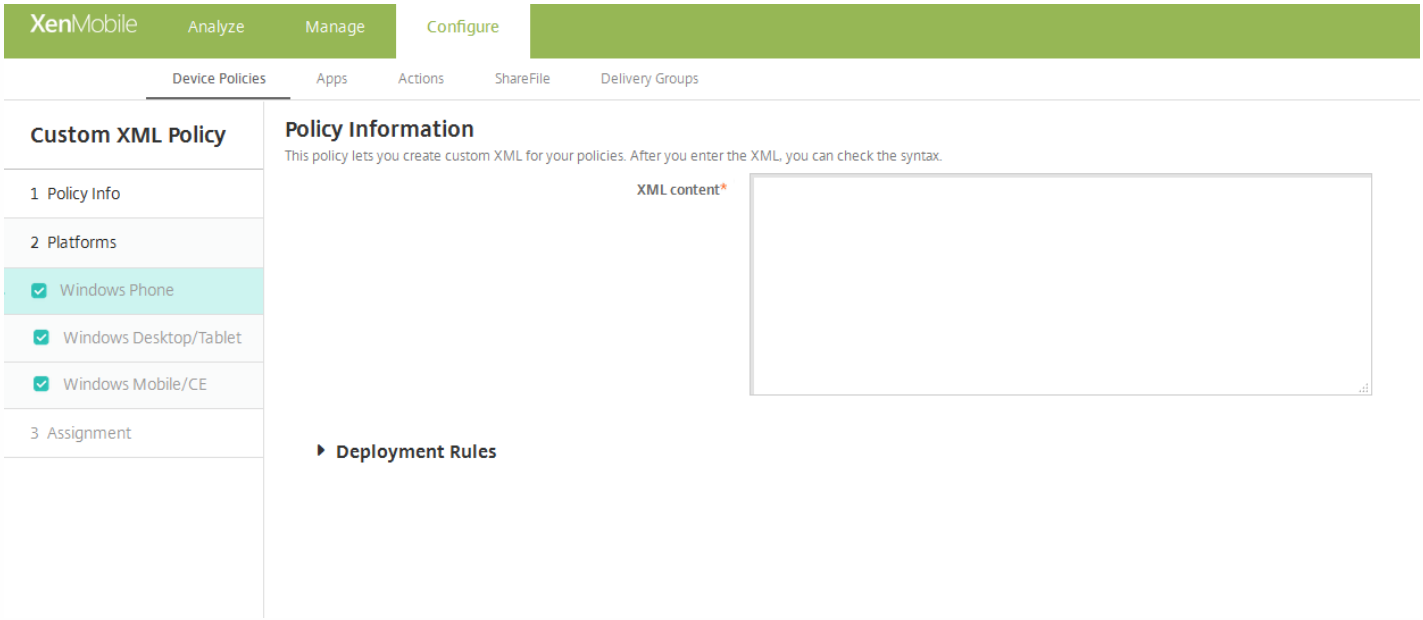
Cliquez sur **Plus** puis, sous **Personnalisé**, cliquez sur **XML personnalisé**. La page d'informations **Stratégie XML personnalisée** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

7. Configurez le paramètre suivant pour chaque plate-forme que vous avez sélectionnée.

- **Contenu XML** : entrez, ou copiez et collez, le code XML personnalisé que vous souhaitez ajouter à la stratégie.

8. Configurez les règles de déploiement.

9. Cliquez sur **Suivant**. XenMobile vérifie la syntaxe du contenu XML. Les erreurs de syntaxe s'affichent en dessous de la zone de contenu. Vous devez résoudre les erreurs avant de continuer.

S'il n'existe pas d'erreurs de syntaxe, la page d'attribution de la **Stratégie XML personnalisée** s'affiche.

10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Toutes les modifications

que vous apportez s'appliquent à toutes les plates-formes.

12. Cliquez sur **Enregistrer**.

Stratégie de suppression des fichiers et dossiers

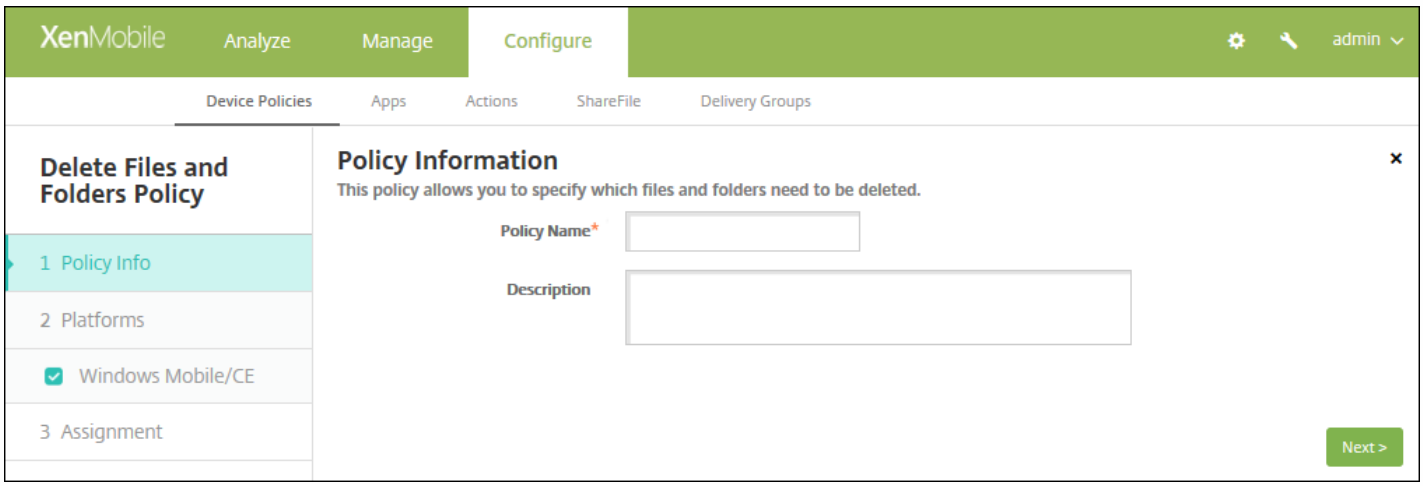
Feb 23, 2017

Vous pouvez créer une stratégie dans XenMobile pour supprimer des fichiers ou dossiers spécifiques d'appareils Windows Mobile/CE.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

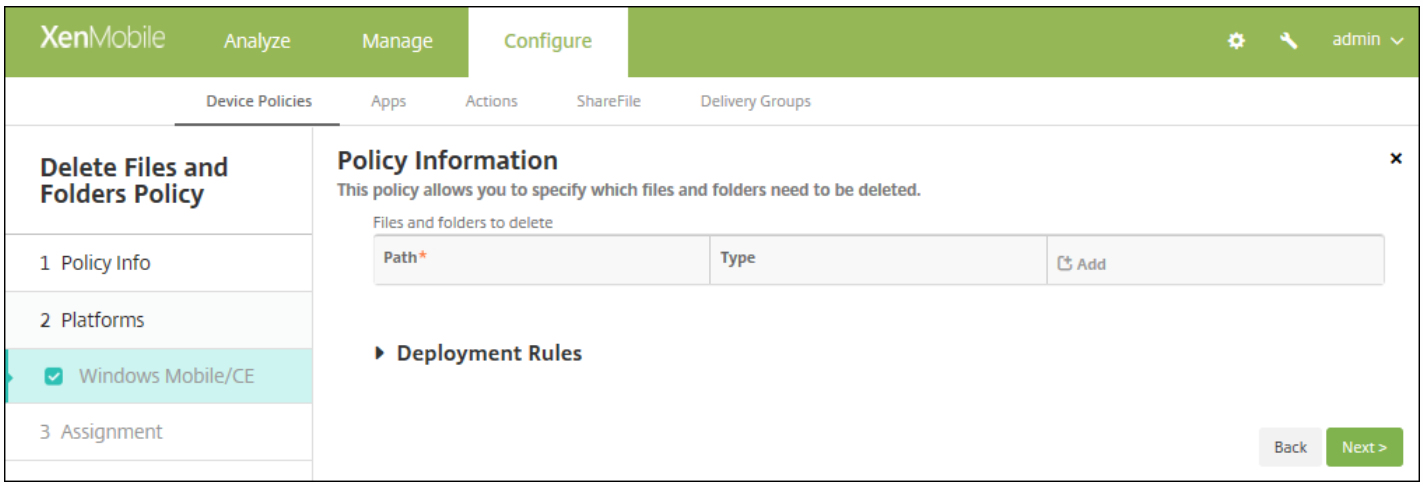
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Supprimer les fichiers et dossiers**. La page d'informations **Stratégie de suppression des fichiers et dossiers** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Plate-forme : Windows Mobile/CE** s'affiche.



6. Configurez les paramètres suivants :

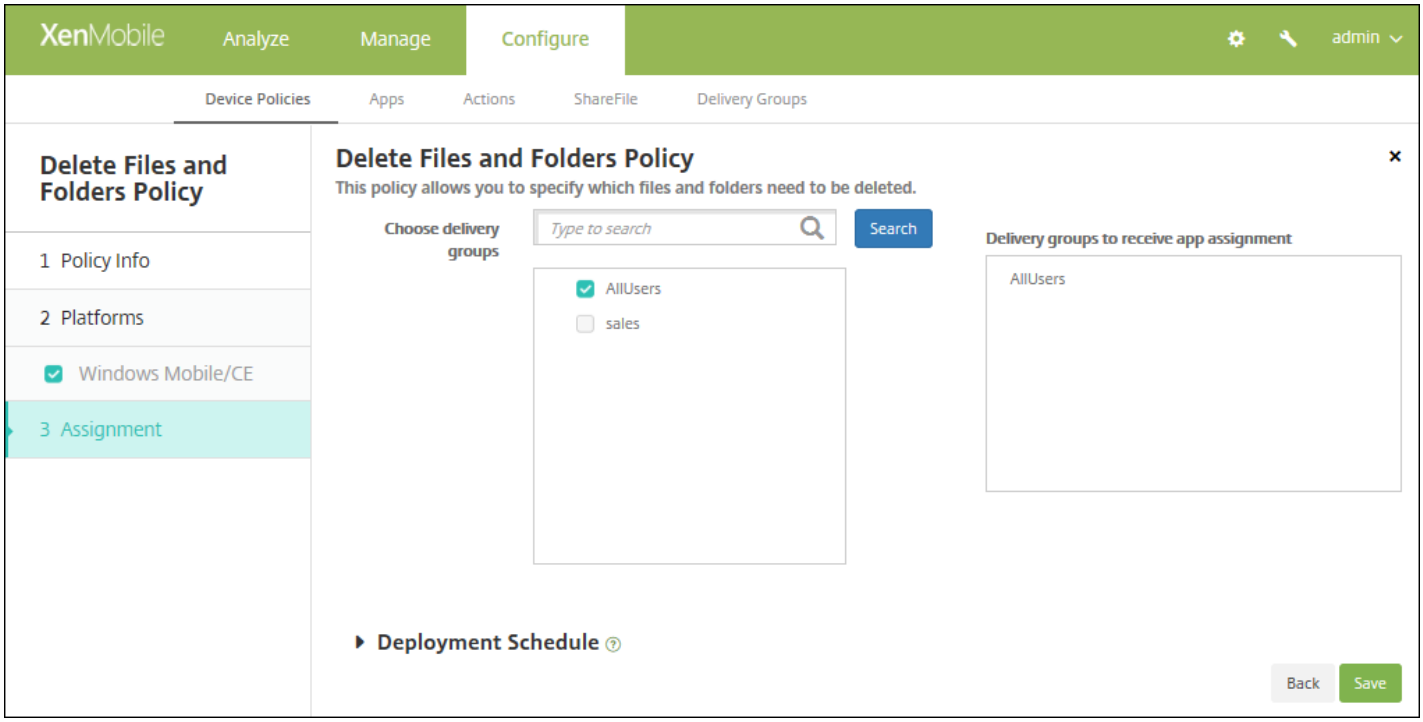
- **Fichiers et dossiers à supprimer** : pour chaque fichier ou dossier que vous souhaitez supprimer, cliquez sur Ajouter, puis procédez comme suit :
  - **Chemin d'accès** : entrez le chemin d'accès au fichier ou dossier.
  - **Type** : dans la liste, cliquez sur Fichier ou Dossier. La valeur par défaut est Fichier.
  - Cliquez sur **Enregistrer** pour enregistrer le fichier ou dossier, ou cliquez sur **Annuler** pour ne pas enregistrer le fichier ou dossier.

    Remarque : pour supprimer une liste, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une liste, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression des fichiers et dossiers** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de suppression de clés et valeurs de Registre

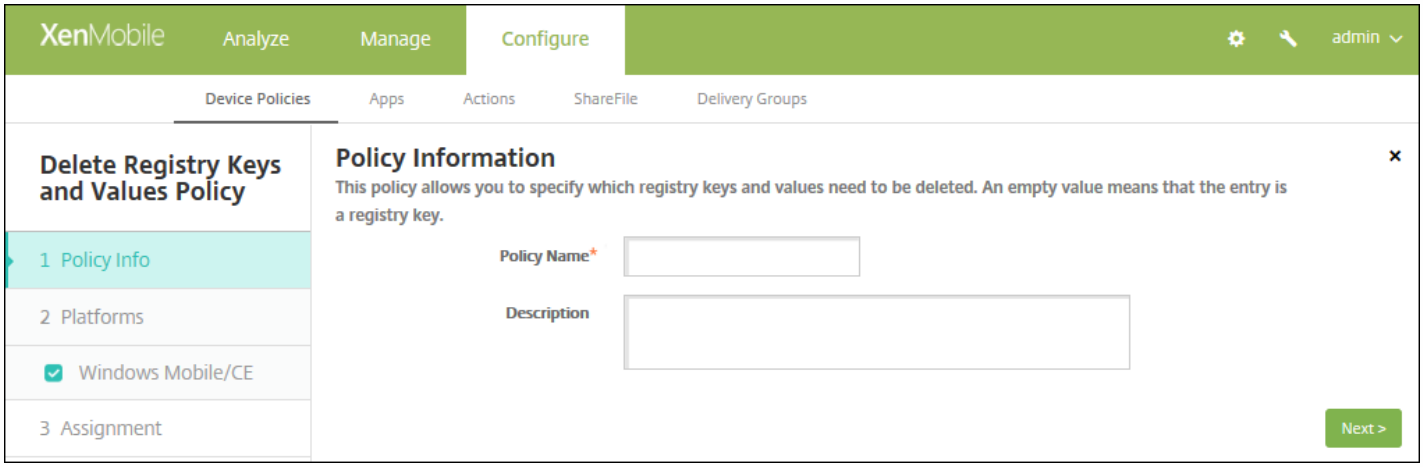
Feb 23, 2017

Vous pouvez créer une stratégie dans XenMobile pour supprimer des clés et valeurs de Registre spécifiques d'appareils Windows Mobile/CE.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

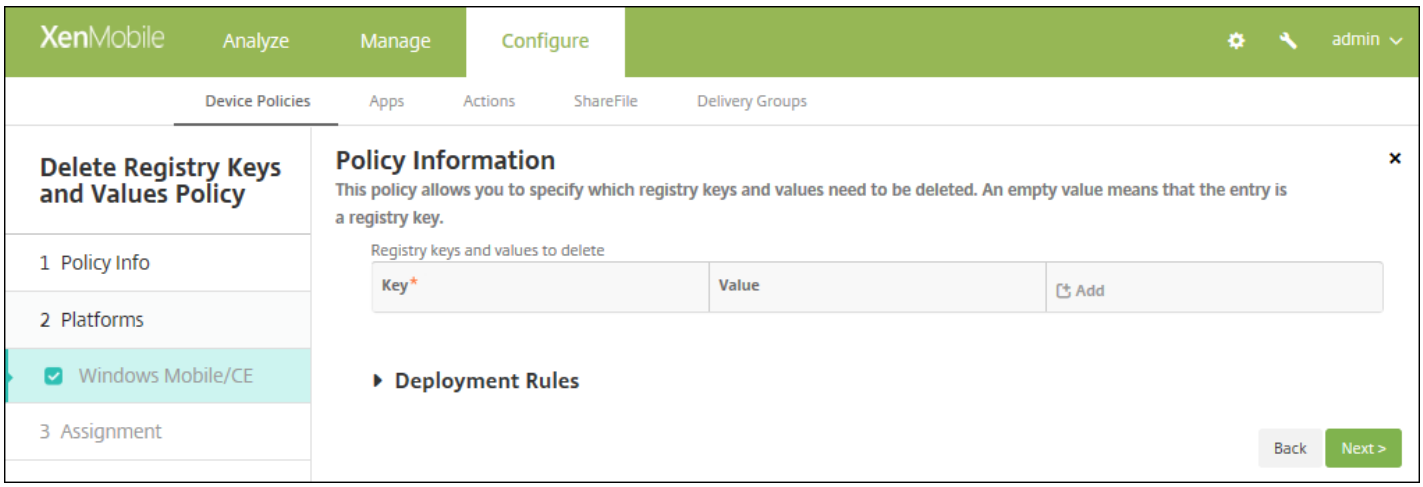
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Supprimer des clés et valeurs de Registre**. La page d'informations **Stratégie de suppression de clés et valeurs de Registre** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Plate-forme : Windows Mobile/CE** s'affiche.



6. Configurez les paramètres suivants :

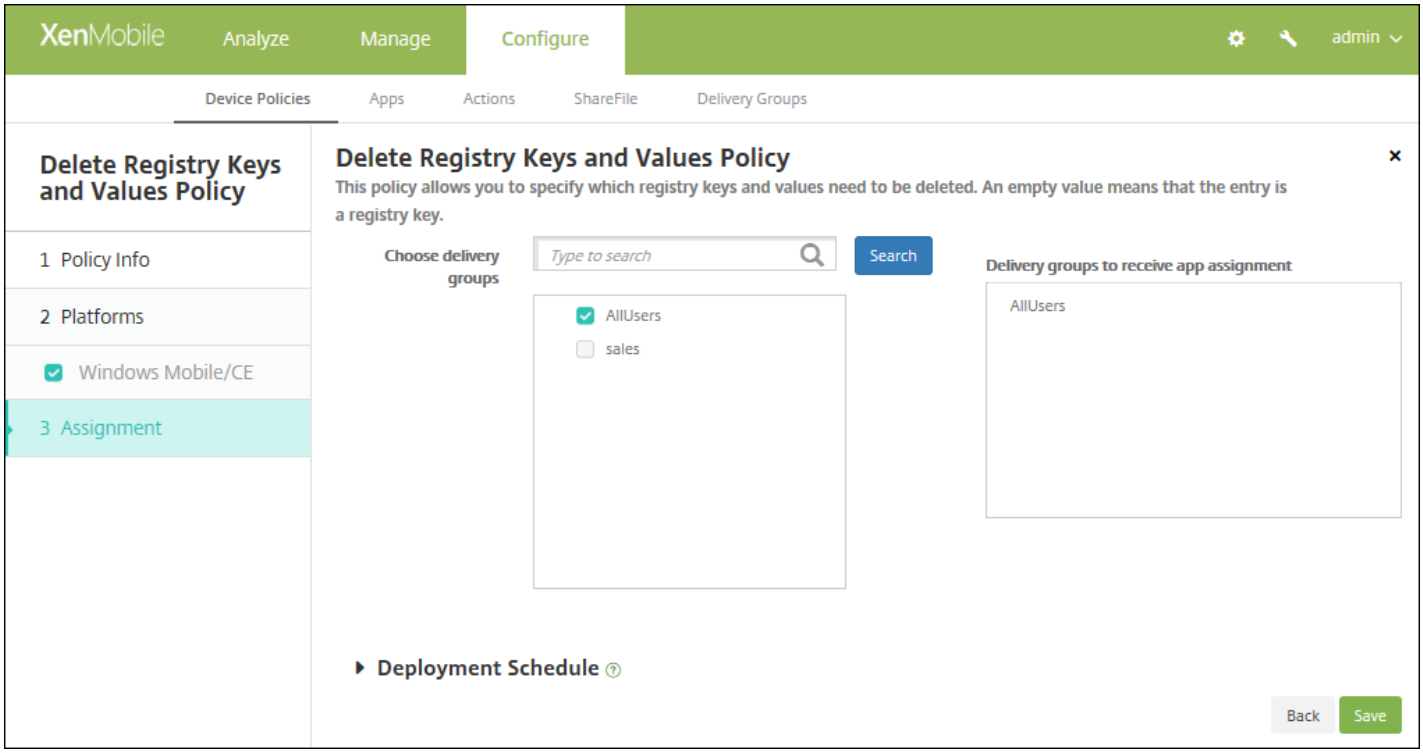
- **Clés et valeurs de Registre à supprimer** : pour chaque clé de Registre et valeur que vous souhaitez supprimer, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Clé** : entrez le chemin de la clé de Registre. Ce champ est obligatoire. Le chemin d'accès doit commencer par HKEY_CLASSES_ROOT\ ou HKEY_CURRENT_USER\ ou HKEY_LOCAL_MACHINE\ ou HKEY_USERS\.
  - **Valeur** : entrez le nom de la valeur à supprimer ou laissez ce champ vide pour supprimer la clé de Registre en entier.
  - Cliquez sur **Enregistrer** pour enregistrer la clé et la valeur, ou cliquez sur **Annuler** pour ne pas enregistrer la clé et la valeur.

    Remarque : pour supprimer une liste, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une liste, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression de clés et valeurs de Registre** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.

- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie d'attestation de l'intégrité des appareils

Feb 23, 2017

Dans XenMobile, vous pouvez exiger que les appareils Windows 10 communiquent leur état d'intégrité : pour cela, ces appareils envoient des informations d'exécution et des données spécifiques au service HAS pour analyse. Le service HAS crée et renvoie un certificat d'attestation d'intégrité que l'appareil envoie ensuite à XenMobile. Lorsque XenMobile reçoit le certificat d'attestation d'intégrité, en fonction du contenu de l'attestation, des actions automatiques que vous avez configurées précédemment peuvent être déployées.

Les données vérifiées par le service HAS sont les suivantes :

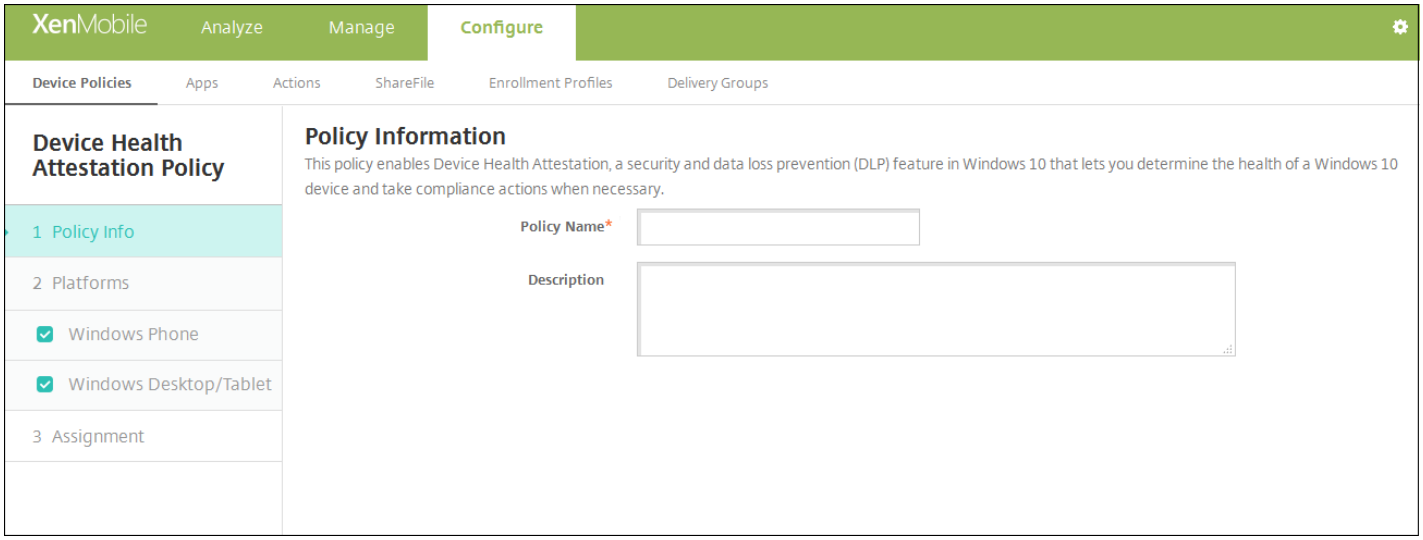
- AIK présent ?
- État BitLocker
- Débogage du démarrage activé ?
- Version de la liste de révision du Gestionnaire de démarrage
- Intégrité du code activée ?
- Version de la liste de révision d'intégrité du code
- Stratégie DEP
- Pilote ELAM chargé ?
- Date d'émission
- Débogage du noyau activé ?
- PCR
- Nombre de réinitialisations
- Nombre de redémarrages
- Mode sans échec activé ?
- Hachage SBCP
- Démarrage sécurisé activé ?
- Signature du test activée ?
- VSM activé ?
- WinPE activé ?

Pour de plus amples informations, reportez-vous à la page HealthAttestation CSP de Microsoft.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus** puis, sous **Personnalisé**, cliquez sur **Stratégie d'attestation de l'intégrité des appareils**. La page d'informations sur la **Stratégie d'attestation de l'intégrité des appareils** s'affiche.



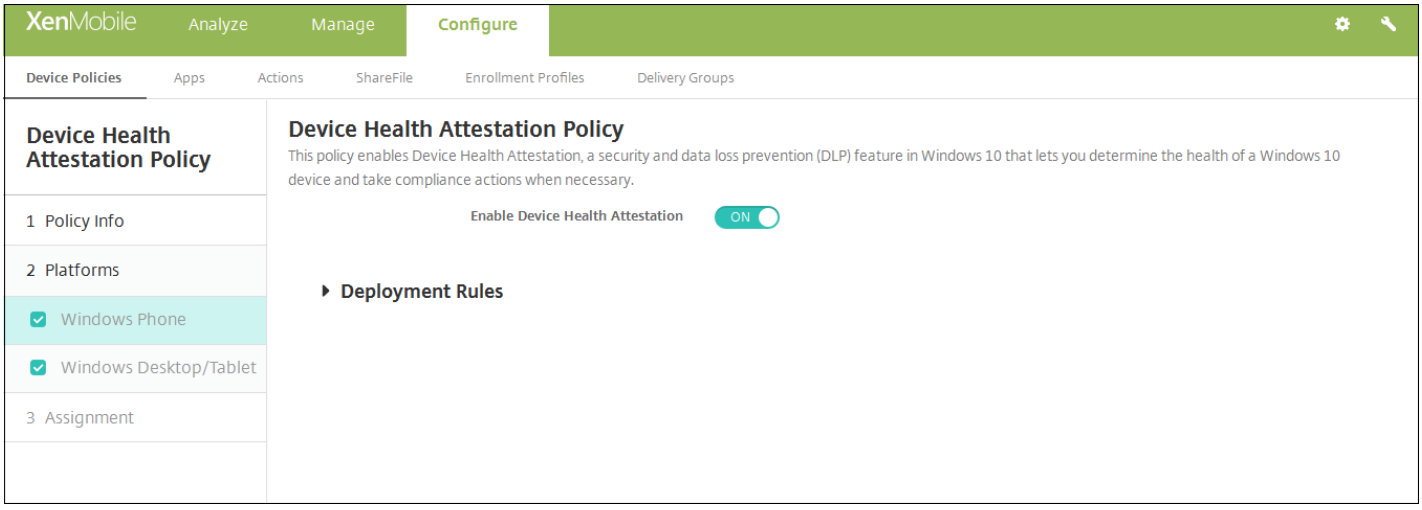
4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

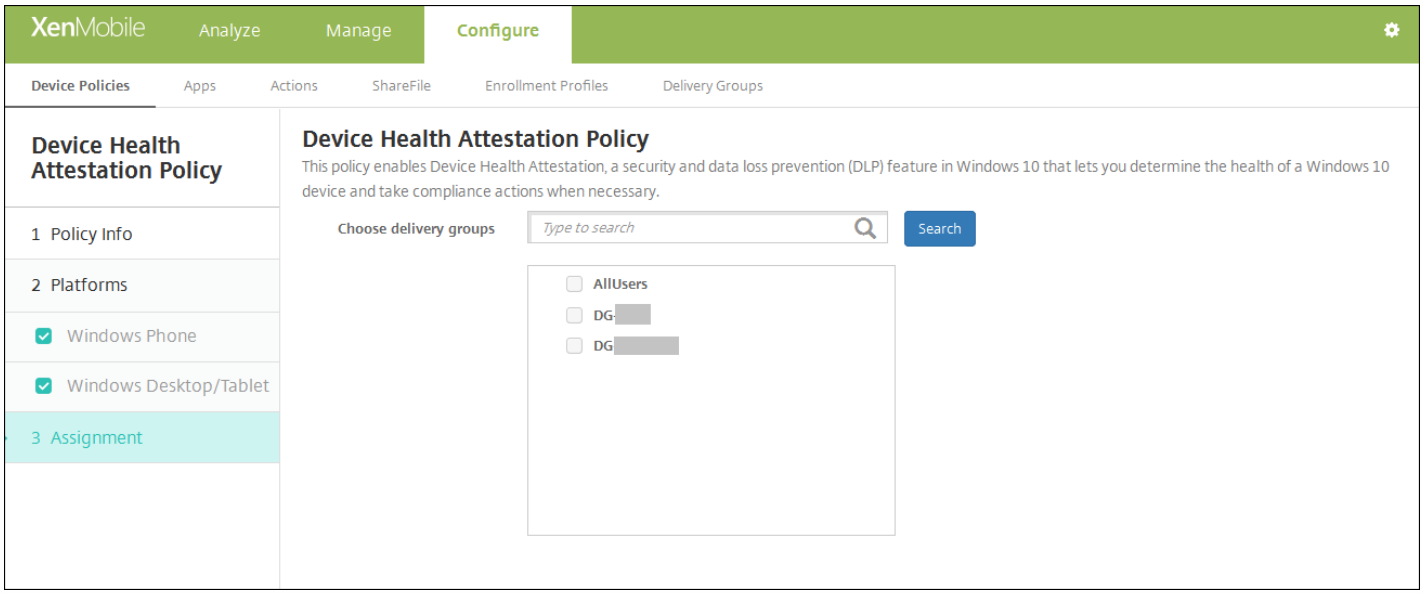


Configurez ce paramètre pour chaque plate-forme que vous sélectionnez :

- **Activer l'attestation de l'intégrité des appareils** : sélectionnez cette option pour exiger l'attestation de l'intégrité des appareils. La valeur par défaut est **OFF**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie d'attestation de l'intégrité des appareils** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de nom d'appareil

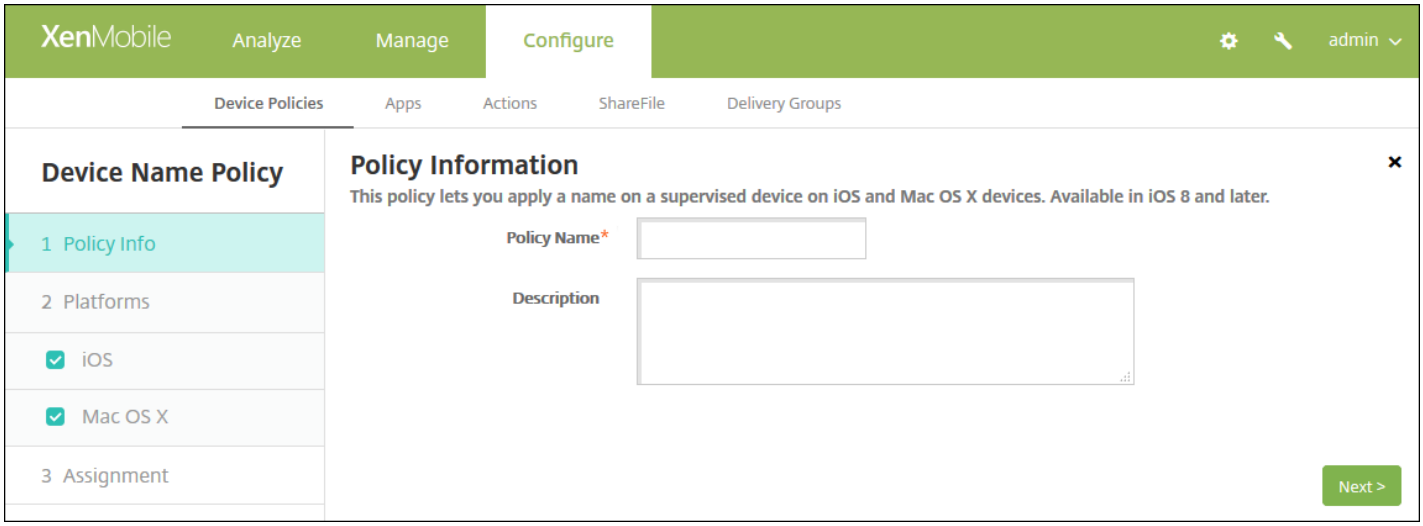
Feb 23, 2017

Vous pouvez définir les noms sur des appareils iOS et Mac OS X, ce qui vous permet d'identifier facilement les appareils. Vous pouvez utiliser des macros et du texte, ou une combinaison des deux pour définir le nom de l'appareil. Par exemple, pour définir le nom de l'appareil à partir du numéro de série de l'appareil, vous devez utiliser ${device.serialnumber}. Pour définir le nom de l'appareil comme la combinaison du nom d'utilisateur et de votre domaine, vous devez utiliser ${user.username}@exemple.com. Consultez la section Macros dans XenMobile pour plus d'informations sur les macros.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Utilisateur final**, cliquez sur **Nom de l'appareil**. La page d'informations sur la **Stratégie de nom d'appareil** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

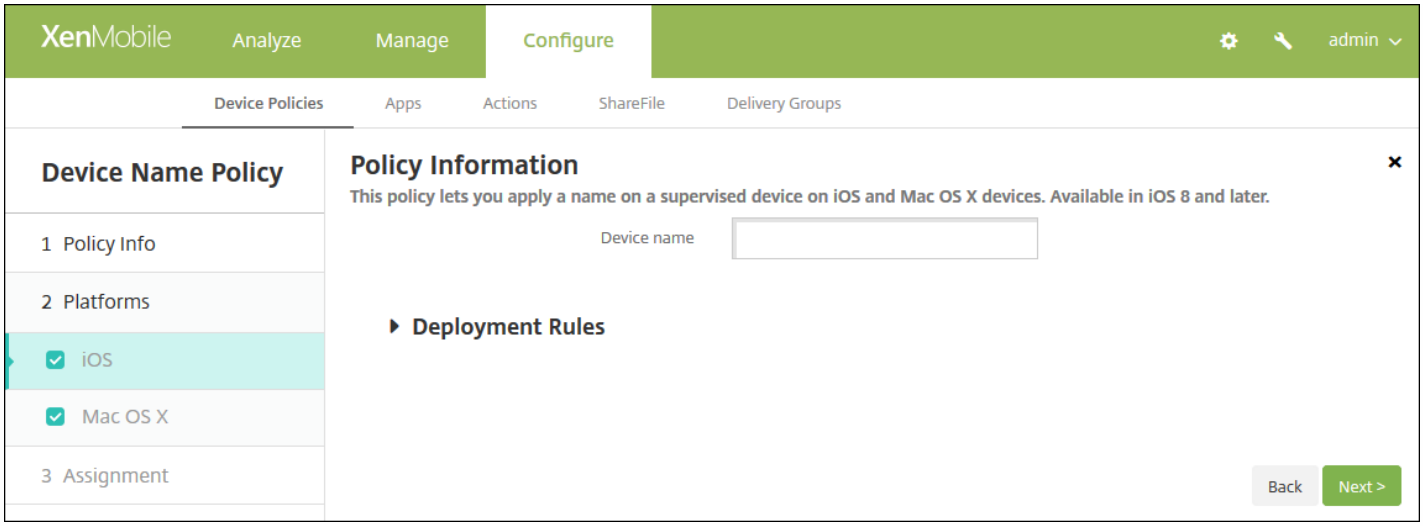
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS et Mac OS X

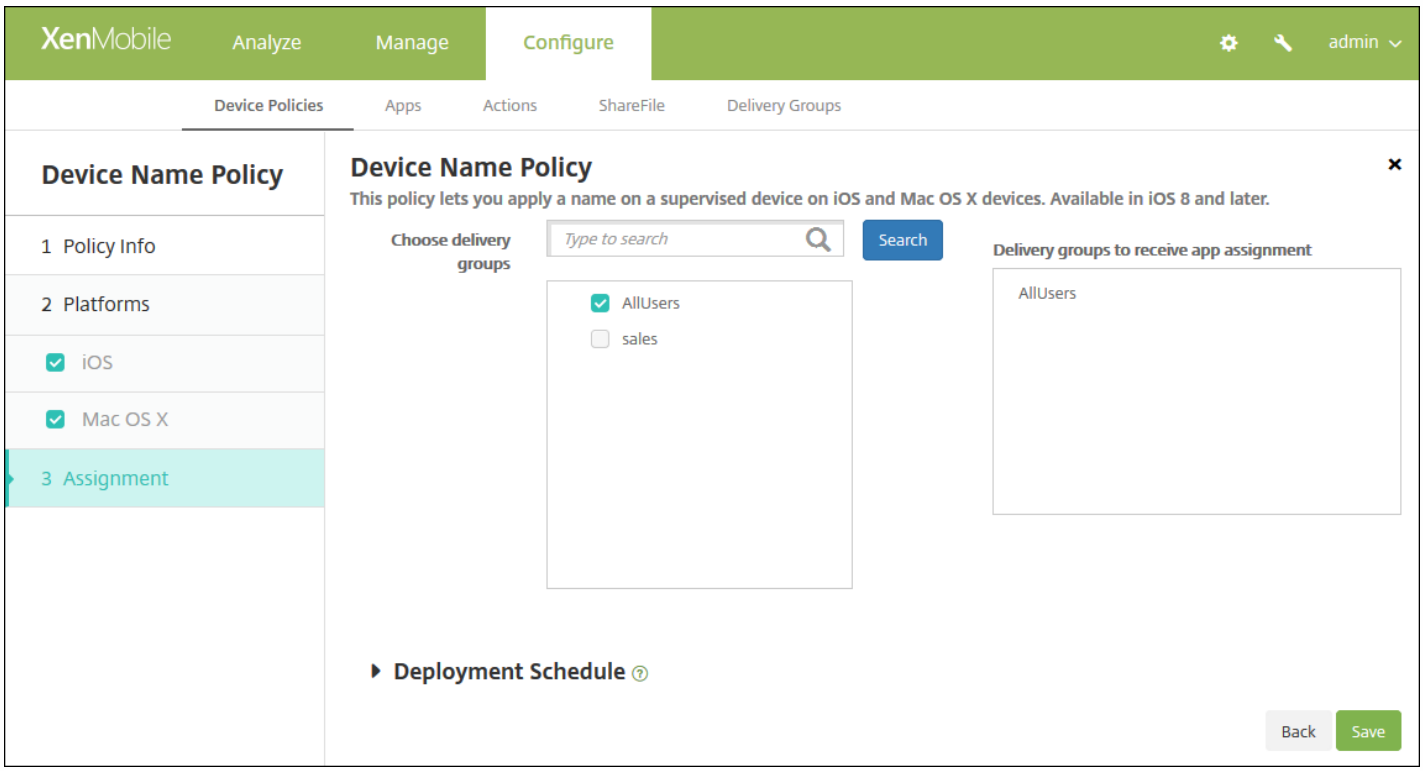


Configurez ce paramètre pour les plates-formes que vous sélectionnez :

- **Nom de l'appareil** : entrez la macro, une combinaison de macros, ou une combinaison de macros et de texte pour donner un nom unique à chaque appareil. Par exemple, utilisez ${device.serialnumber} pour définir les noms d'appareil selon leur numéro de série ou utilisez ${device.serialnumber} ${user.username} pour inclure le nom de l'utilisateur dans le nom de l'appareil.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de nom d'appareil** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou

sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégie d'hub d'entreprise

Feb 23, 2017

Une stratégie d'hub d'entreprise pour Windows Phone vous permet de distribuer des applications d'entreprise via le magasin hub d'entreprise.

Avant de pouvoir créer la stratégie, vous avez besoin des éléments suivants :

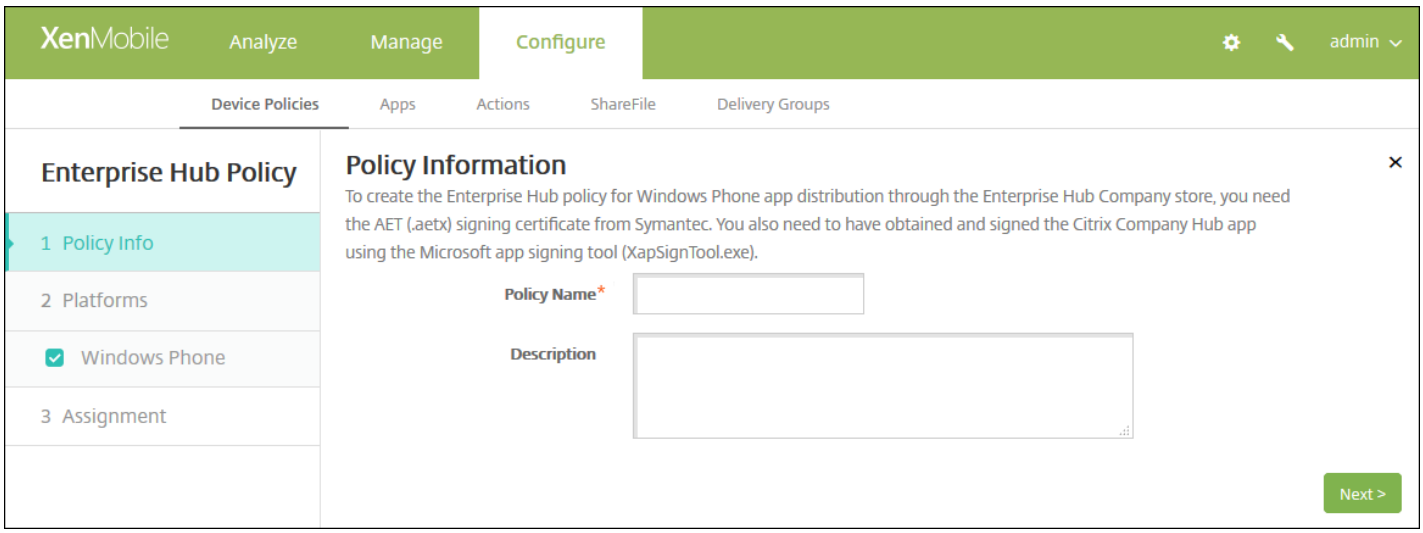
- Un certificat de signature AET (.aetx) de Symantec
- L'application d'hub d'entreprise Citrix signée à l'aide de l'outil de signature d'applications Microsoft (XapSignTool.exe)

Remarque : XenMobile prend en charge une seule stratégie d'hub d'entreprise pour un mode Windows Phone Secure Hub. Par exemple, pour télécharger Windows Phone Secure Hub pour XenMobile Enterprise Edition, vous ne devez pas créer de multiples stratégies d'hub d'entreprise avec différentes versions de Worx Home pour XenMobile Enterprise Edition. Vous pouvez uniquement déployer la stratégie d'hub d'entreprise initiale lors de l'inscription de l'appareil.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

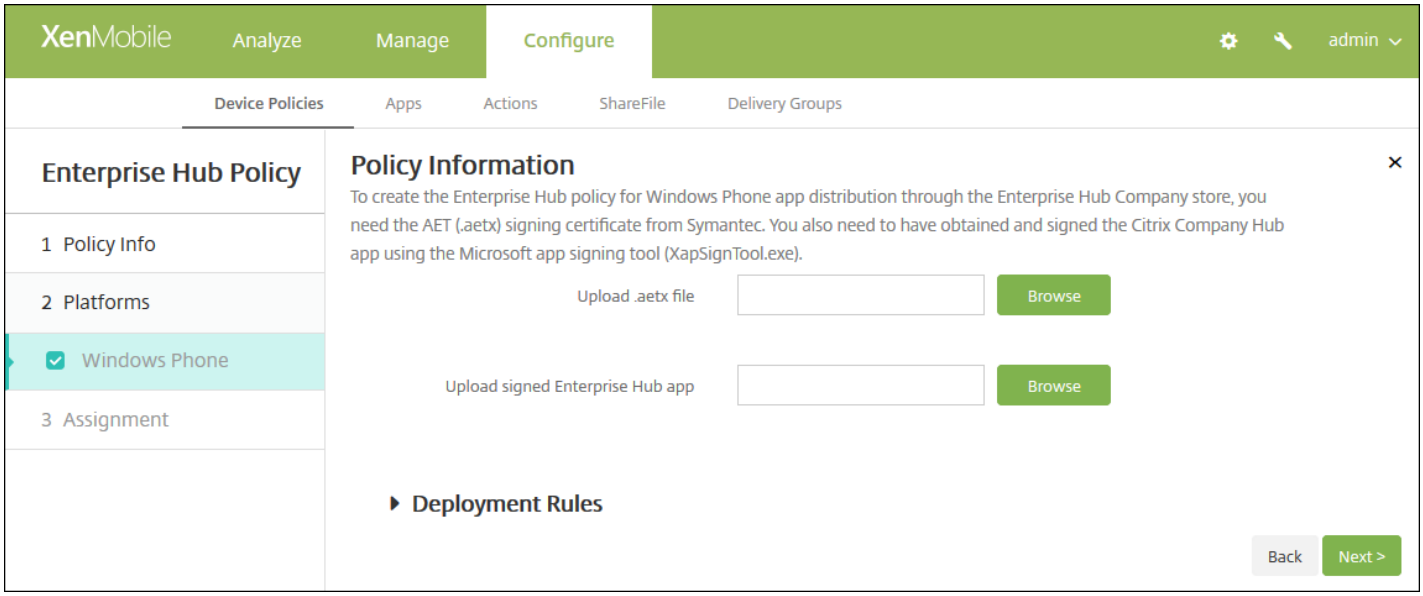
3. Cliquez sur **Plus**, puis, sous **Agent XenMobile**, cliquez sur **Hub d'entreprise**. La page **Stratégie d'hub d'entreprise** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page de plate-forme **Windows Phone** s'affiche.

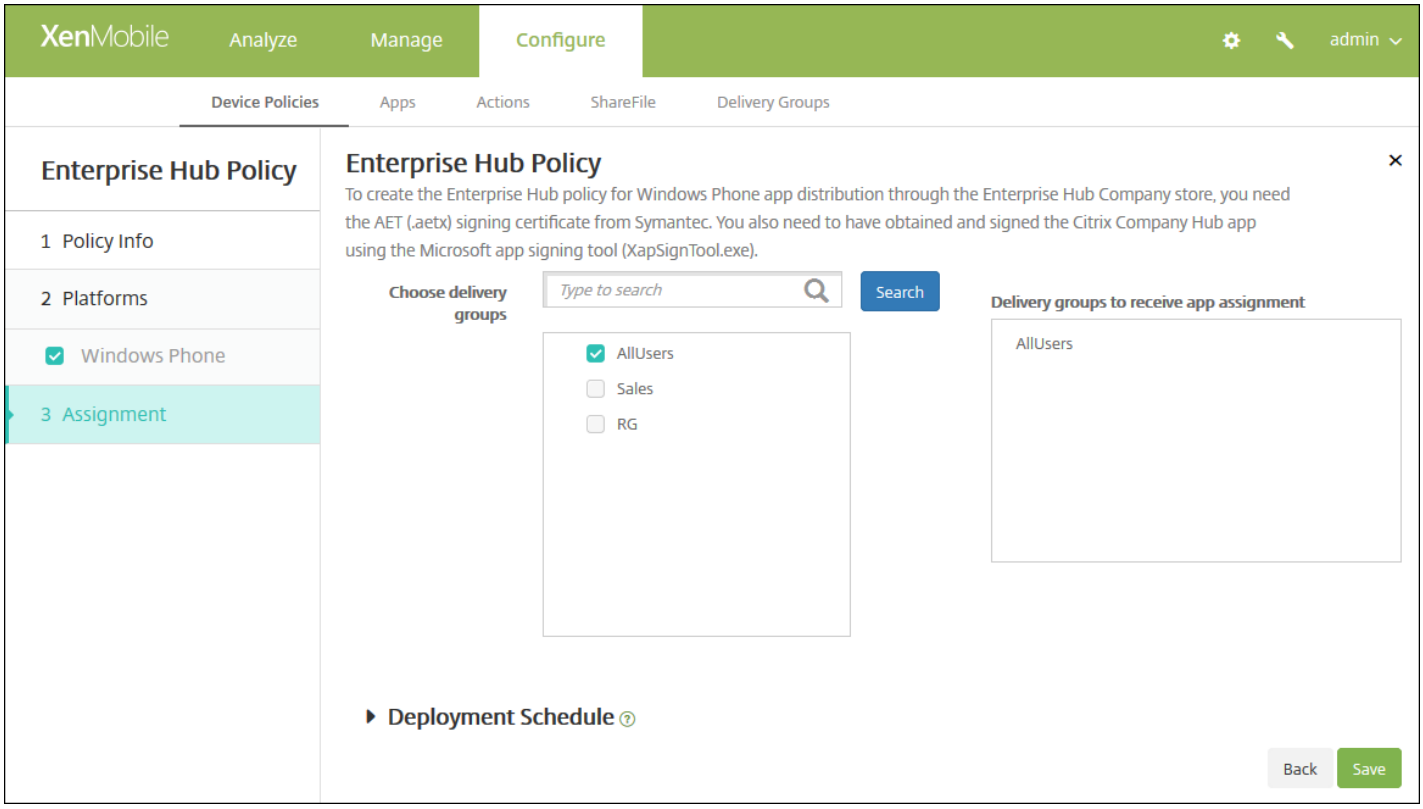


6. Configurez les paramètres suivants :

- **Charger fichier .aetx** : sélectionnez le fichier .aetx, en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.
- **Charger application d'hub d'entreprise signée** : sélectionnez l'application Hub d'entreprise, en cliquant sur **Parcourir** et accédez à l'emplacement de l'application.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie d'hub d'entreprise** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de fichiers

Feb 23, 2017

Vous pouvez ajouter des fichiers de script à XenMobile qui exécutent certaines fonctions pour les utilisateurs, ou vous pouvez ajouter des fichiers de documents auxquels vous voulez que les utilisateurs Android aient accès sur leurs appareils. Lorsque vous ajoutez le fichier, vous pouvez également spécifier le répertoire dans lequel vous souhaitez que le fichier soit stocké sur l'appareil. Par exemple, si vous souhaitez que les utilisateurs Android reçoivent un document d'entreprise ou fichier .pdf, vous pouvez déployer le fichier sur l'appareil et informer les utilisateurs de son emplacement.

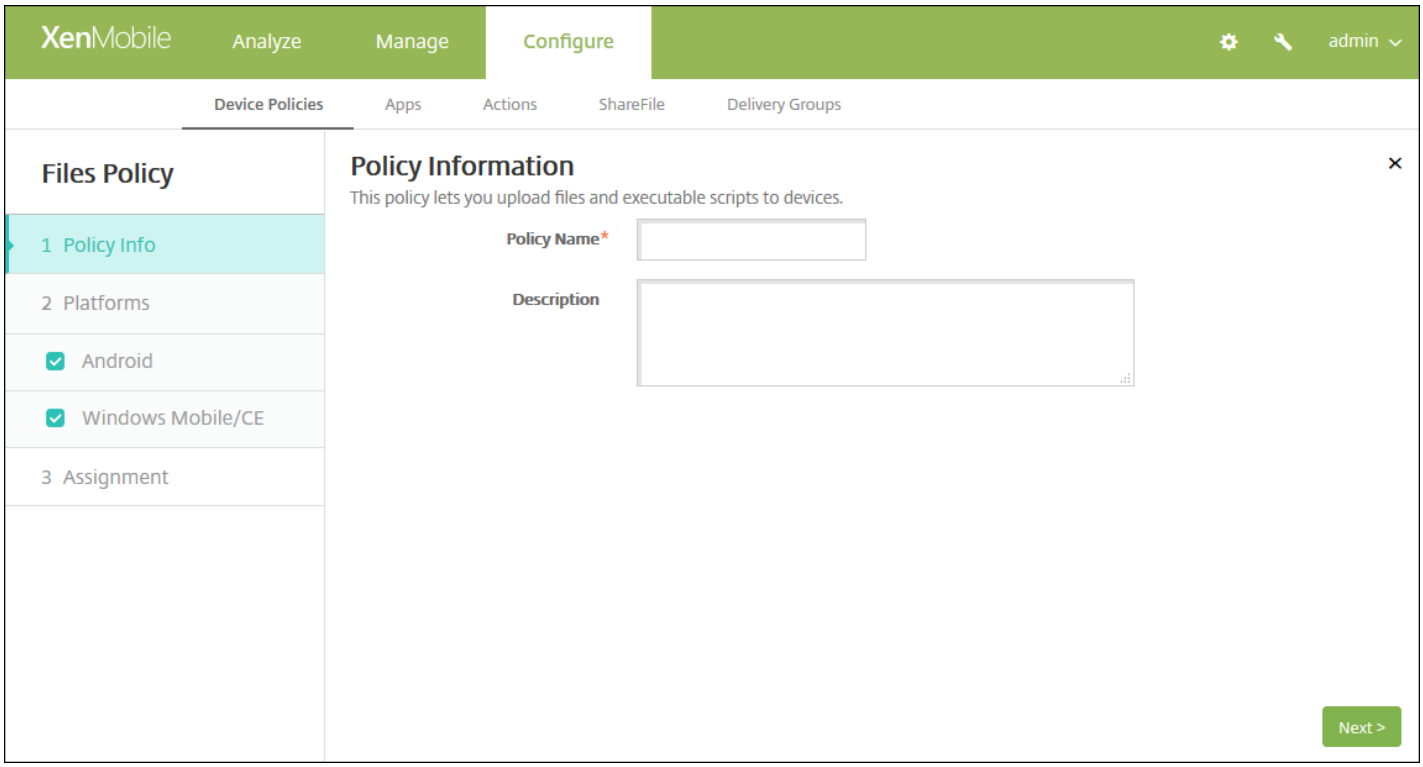
Vous pouvez ajouter les types de fichiers suivants avec cette stratégie :

- Fichiers texte (.xml, .html, .py, etc.)
- Autres fichiers tels que des documents, images, feuilles de calcul ou présentations
- Pour Windows Mobile and Windows CE uniquement : fichiers de script créés avec MortScript

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

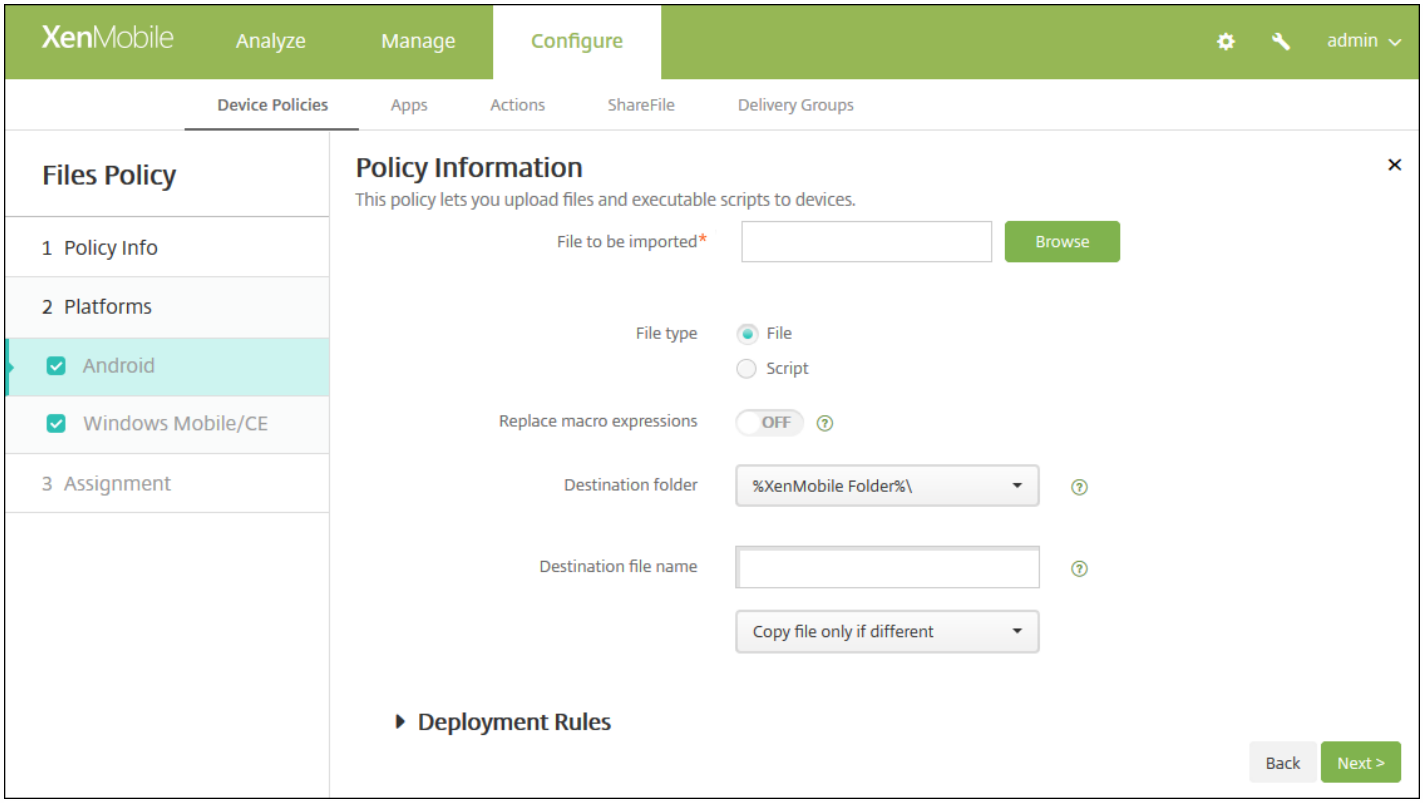
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Fichiers**. La page d'informations **Stratégie de fichiers** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

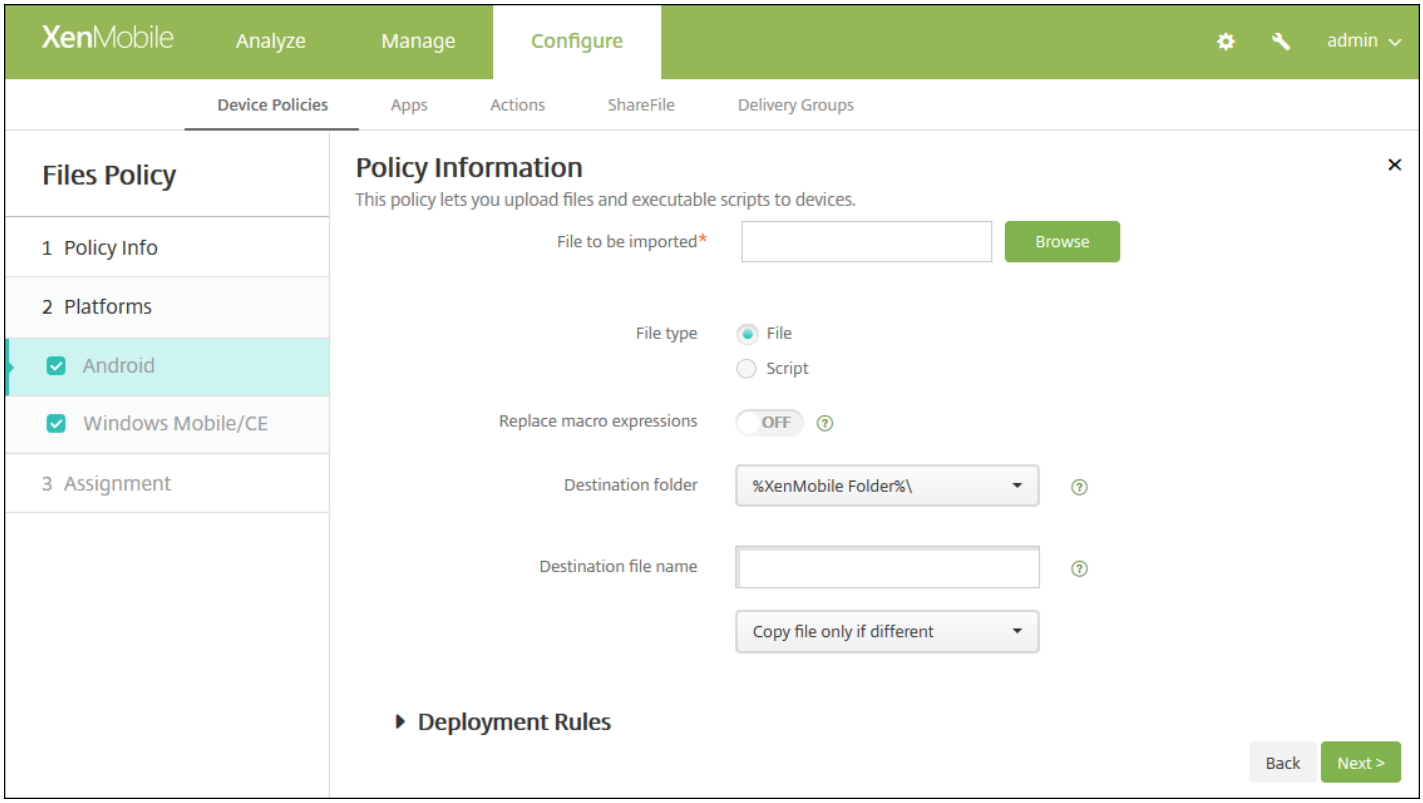
5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

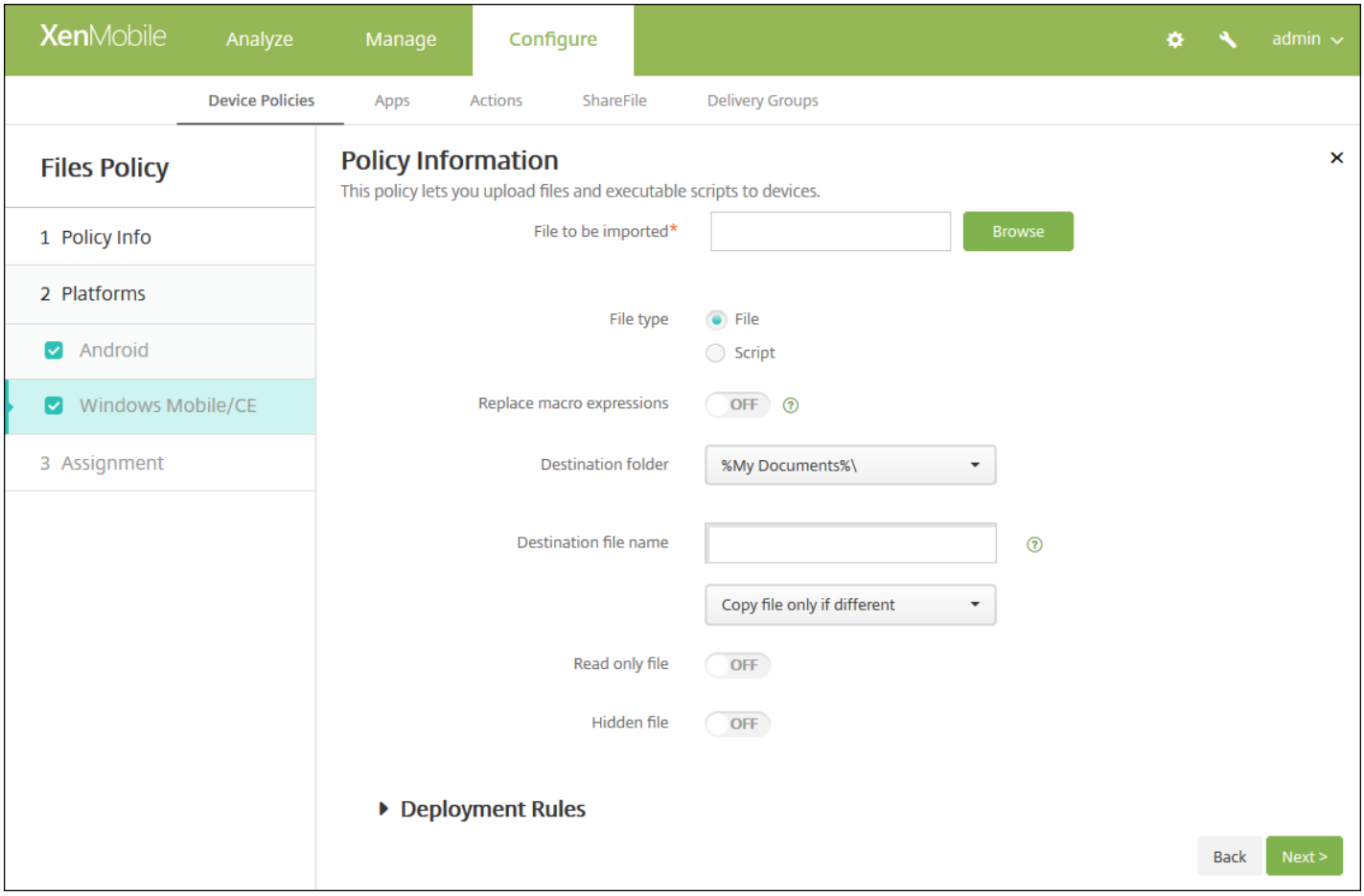
Configurer les paramètres pour Android



Configurez les paramètres suivants :

- **Fichier à importer** : sélectionnez le fichier à importer en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
- **Type de fichier** : sélectionnez **Fichier** ou **Script**. Lorsque vous sélectionnez **Script**, **Exécuter immédiatement** s'affiche. Sélectionnez si le script est exécuté dès que le fichier est chargé. La valeur par défaut est **OFF**.
- **Substituer les macros** : sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. La valeur par défaut est **OFF**.
- **Dossier de destination** : dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé ou cliquez sur **Ajouter** pour choisir un emplacement de fichier non répertorié. En outre, vous pouvez utiliser les macros %XenMobile Folder%\ ou %Carte de stockage%\ comme début de chemin d'accès.
- **Nom du fichier de destination** : si vous le souhaitez, entrez un autre nom pour le fichier s'il doit être modifié avant d'être déployé sur un appareil.
- **Copier le fichier s'ils sont différents** : dans la liste, sélectionnez si vous souhaitez copier le fichier s'il est différent du fichier existant. Par défaut, le fichier est copié uniquement s'il est différent.

Configurer les paramètres pour Windows Mobile/CE

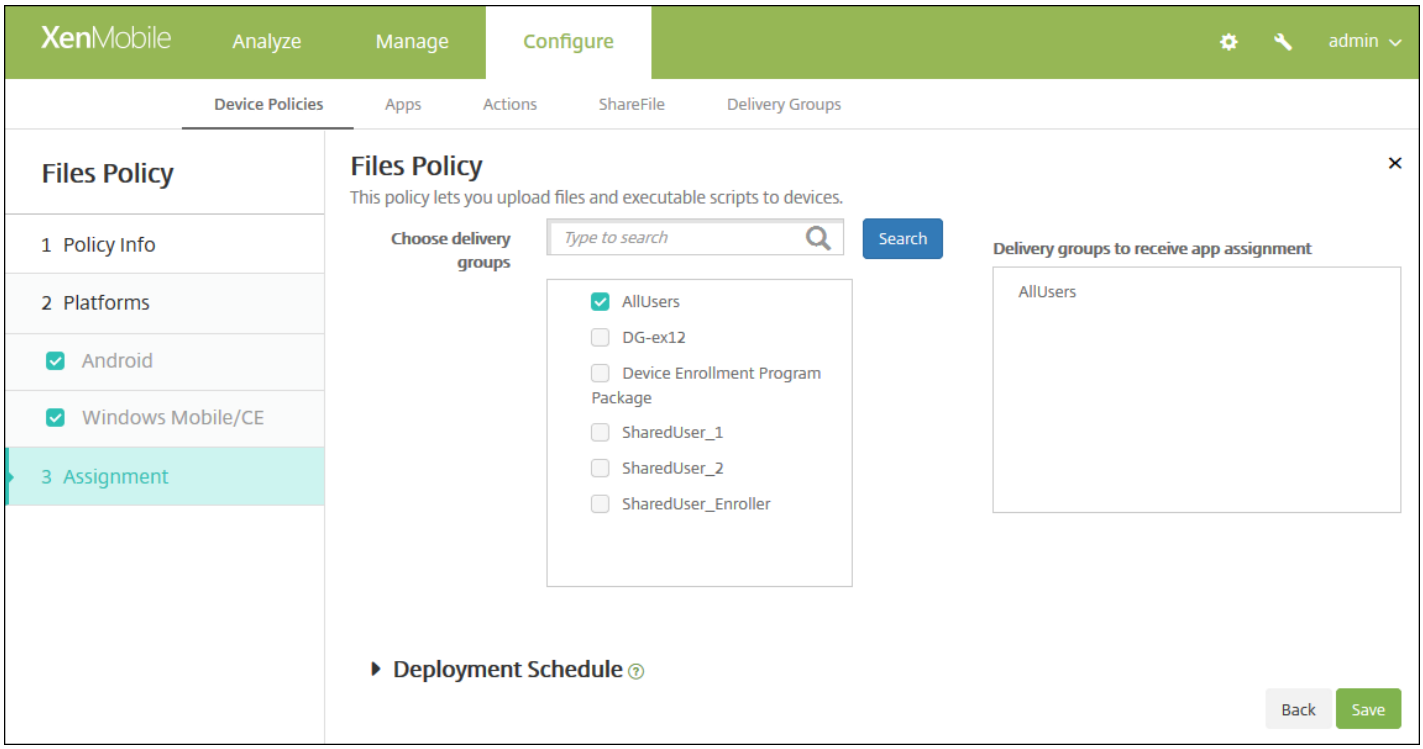


Configurez les paramètres suivants :

- **Fichier à importer** : sélectionnez le fichier à importer en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
- **Type de fichier** : sélectionnez **Fichier** ou **Script**. Lorsque vous sélectionnez **Script**, **Exécuter immédiatement** s'affiche. Sélectionnez si le script est exécuté dès que le fichier est chargé. La valeur par défaut est **OFF**.
- **Substituer les macros** : sélectionnez cette option si vous voulez remplacer les noms des jetons de macro dans un script avec une propriété d'appareil ou d'utilisateur. La valeur par défaut est **OFF**.
- **Dossier de destination** : dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé ou cliquez sur **Ajouter** pour choisir un emplacement de fichier non répertorié. En outre, vous pouvez utiliser les macros suivantes comme début de chemin d'accès :
  - %Carte de stockage%\
  - %XenMobile Folder%\
  - %Program Files%\
  - %Mes Documents%\
  - %Windows%\
- **Nom du fichier de destination** : si vous le souhaitez, entrez un autre nom pour le fichier s'il doit être modifié avant d'être déployé sur un appareil.
- **Copier le fichier s'ils sont différents** : dans la liste, sélectionnez si vous souhaitez copier le fichier s'il est différent du fichier existant. Par défaut, le fichier est copié uniquement s'il est différent.
- **Fichier en lecture seule** : indiquez si le fichier est en lecture seule. La valeur par défaut est **OFF**.
- **Fichier masqué** : indiquez si le fichier ne doit pas être affiché dans la liste de fichiers. La valeur par défaut est **OFF**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution **Stratégie de fichiers** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégies de police

Feb 23, 2017

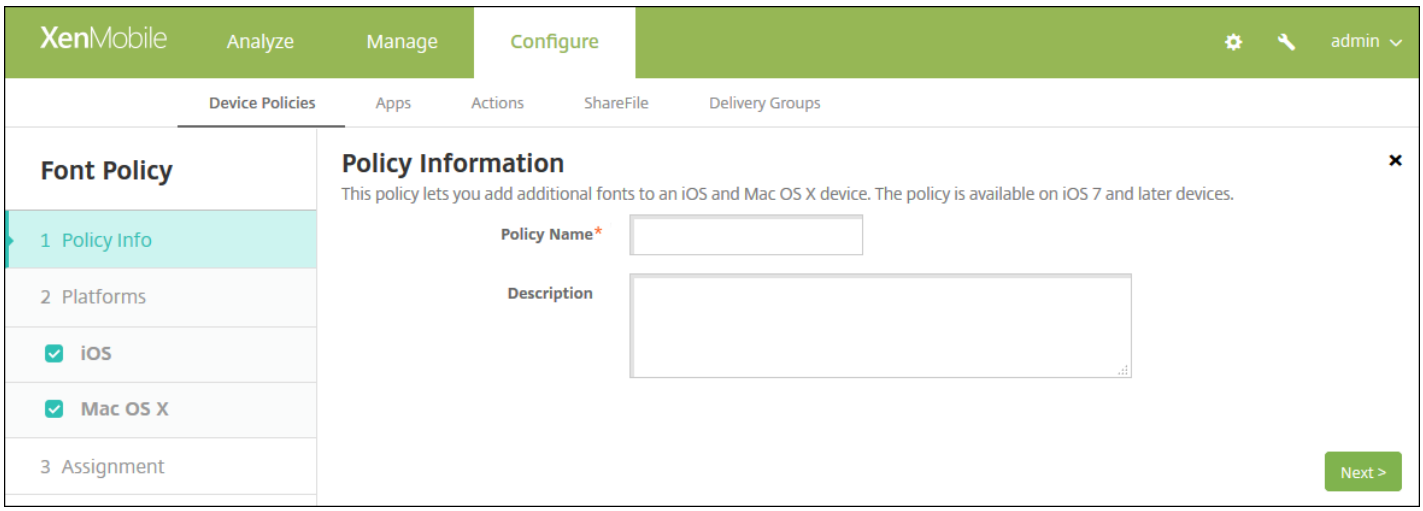
Vous pouvez ajouter une stratégie de police dans XenMobile pour ajouter des polices supplémentaires sur les appareils iOS et Mac OS X des utilisateurs. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge.

Remarque : pour iOS, cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis, sous **Utilisateur final**, cliquez sur **Police**. La page **Stratégie de police** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

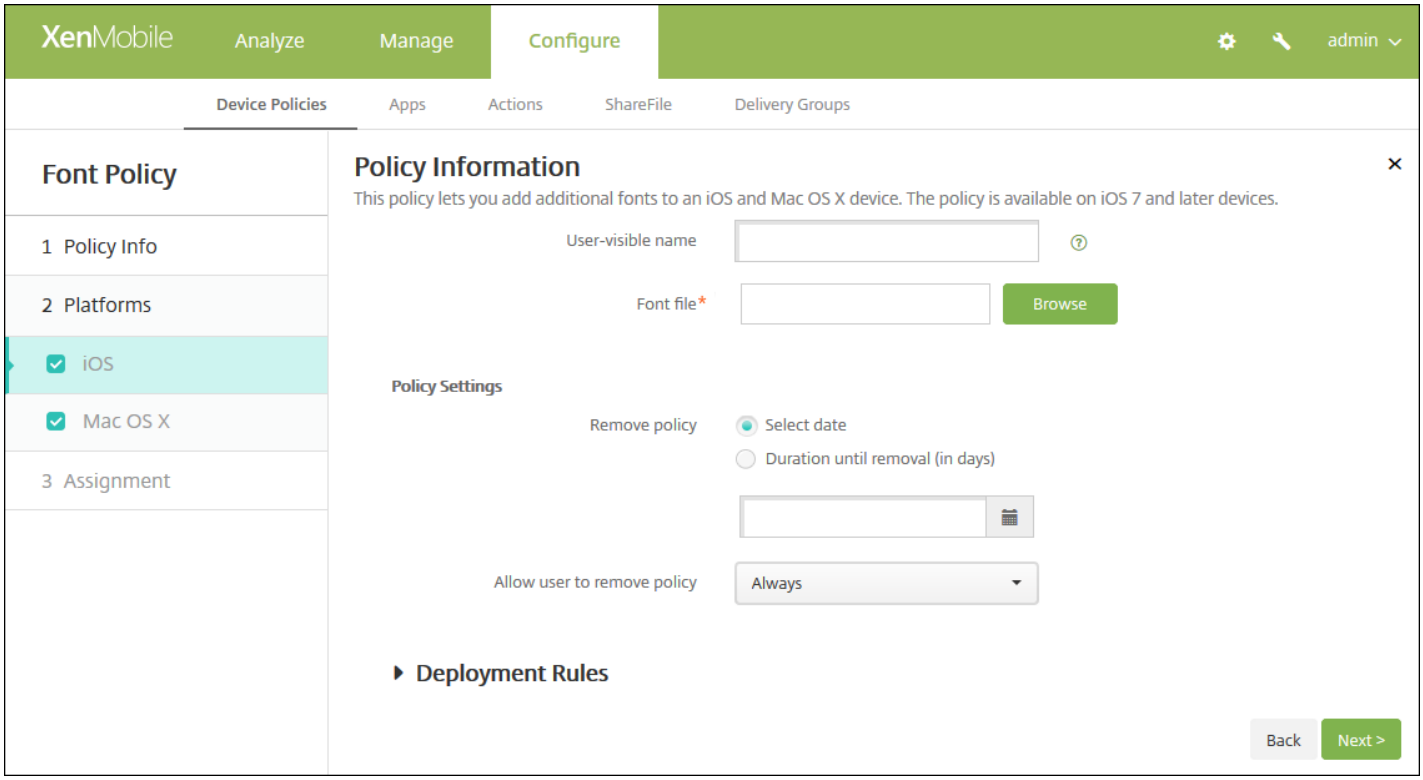
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

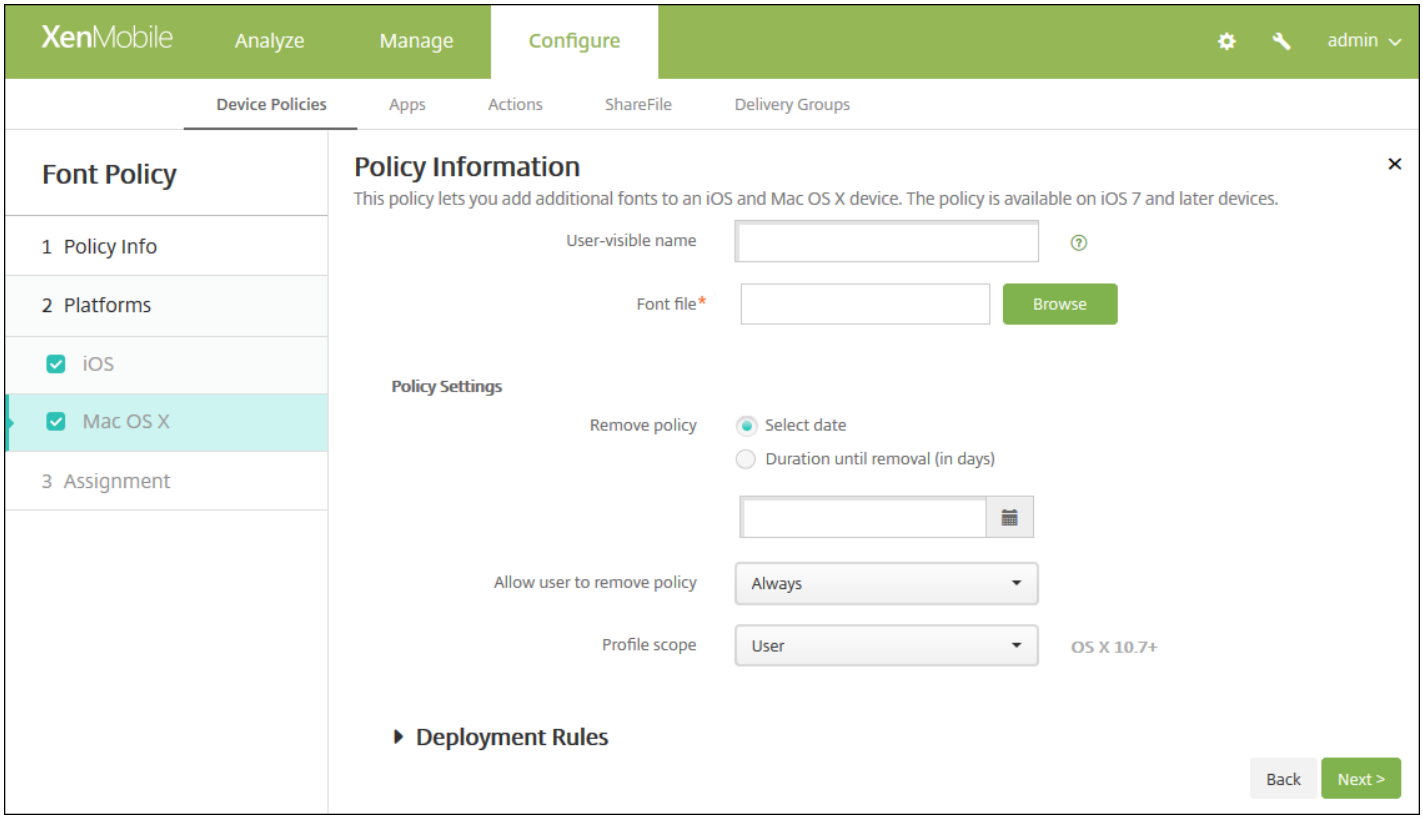
Configurer le paramètre pour iOS



Configurez les paramètres suivants :

- **Nom visible par l'utilisateur** : entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police** : sélectionnez le fichier de police à ajouter aux périphériques utilisateur en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X

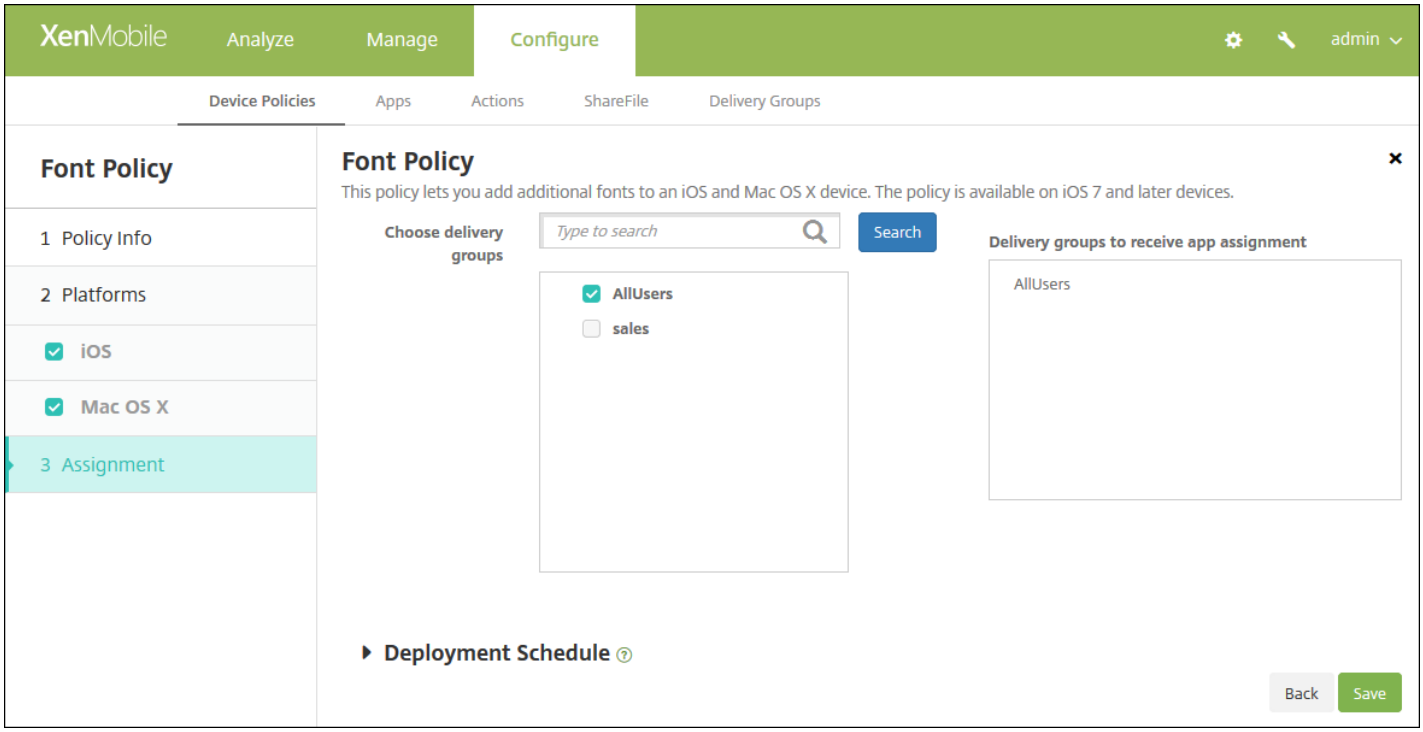


Configurez les paramètres suivants :

- **Nom visible par l'utilisateur** : entrez le nom que les utilisateurs voient dans leurs listes de polices.
- **Fichier de police** : sélectionnez le fichier de police à ajouter aux périphériques utilisateur en cliquant sur **Parcourir**, puis accédez à l'emplacement du fichier.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de police** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Importer des stratégies de profil iOS et Mac OS X

Feb 23, 2017

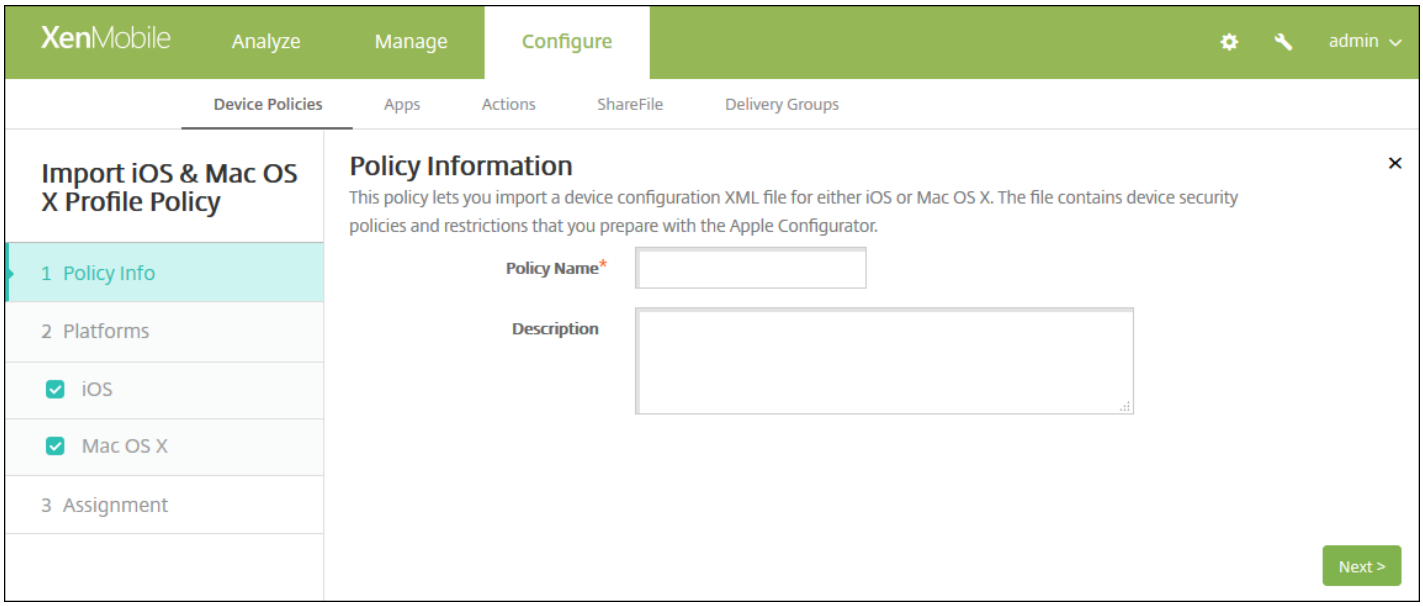
Vous pouvez importer les fichiers XML de configuration d'appareil pour iOS et OS X dans XenMobile. Le fichier contient des stratégies de sécurité et des restrictions que vous préparez avec Apple Configurator.

Vous pouvez placer un appareil iOS en mode supervisé à l'aide de Apple Configurator, comme décrit plus loin dans cet article. Pour de plus amples informations sur l'utilisation d'Apple Configurator pour créer un fichier de configuration, consultez la page d'aide sur Configuratord'Apple.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

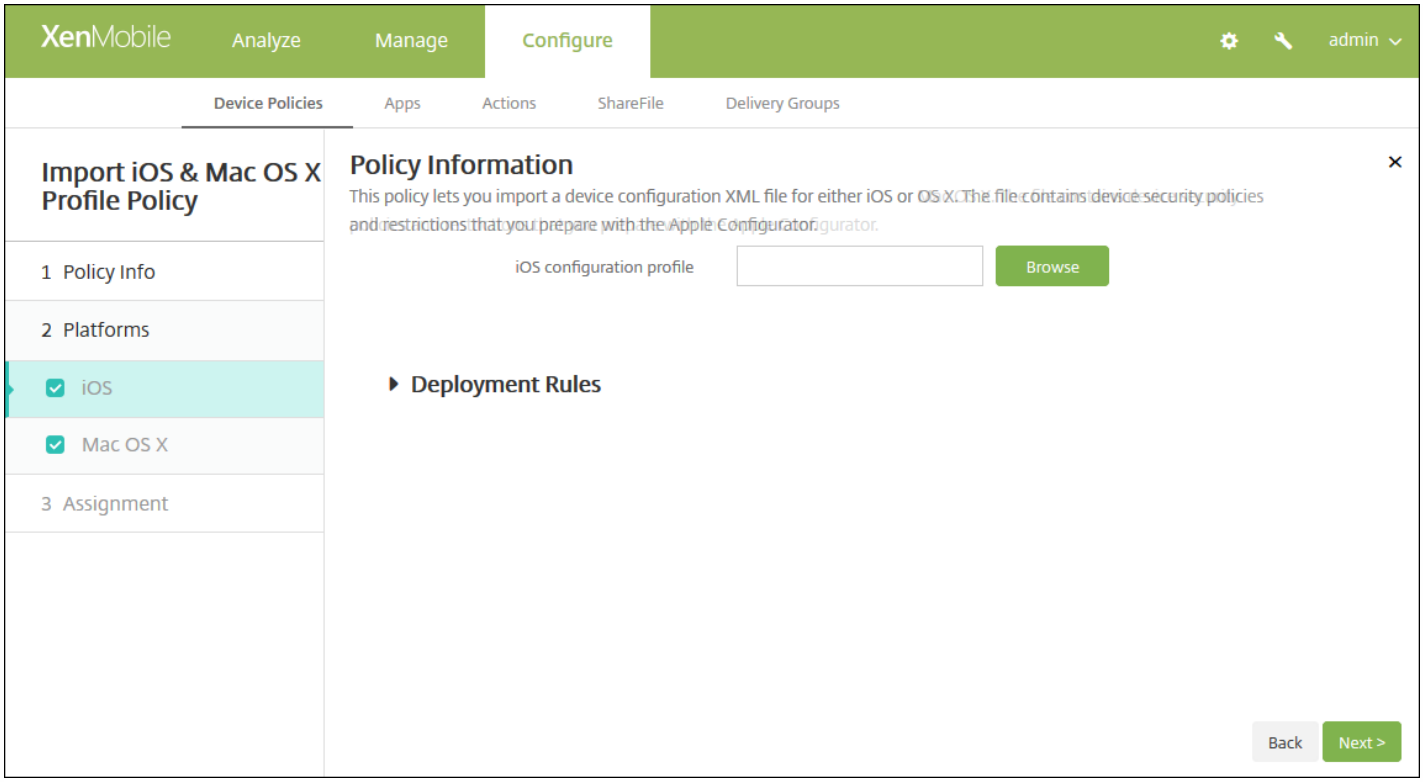
3. Développez **Plus** puis, sous **Personnaliser**, cliquez sur **Importer le profil iOS et Mac OS X**. La page d'informations **Importer le profil iOS et Mac OS X** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.



6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

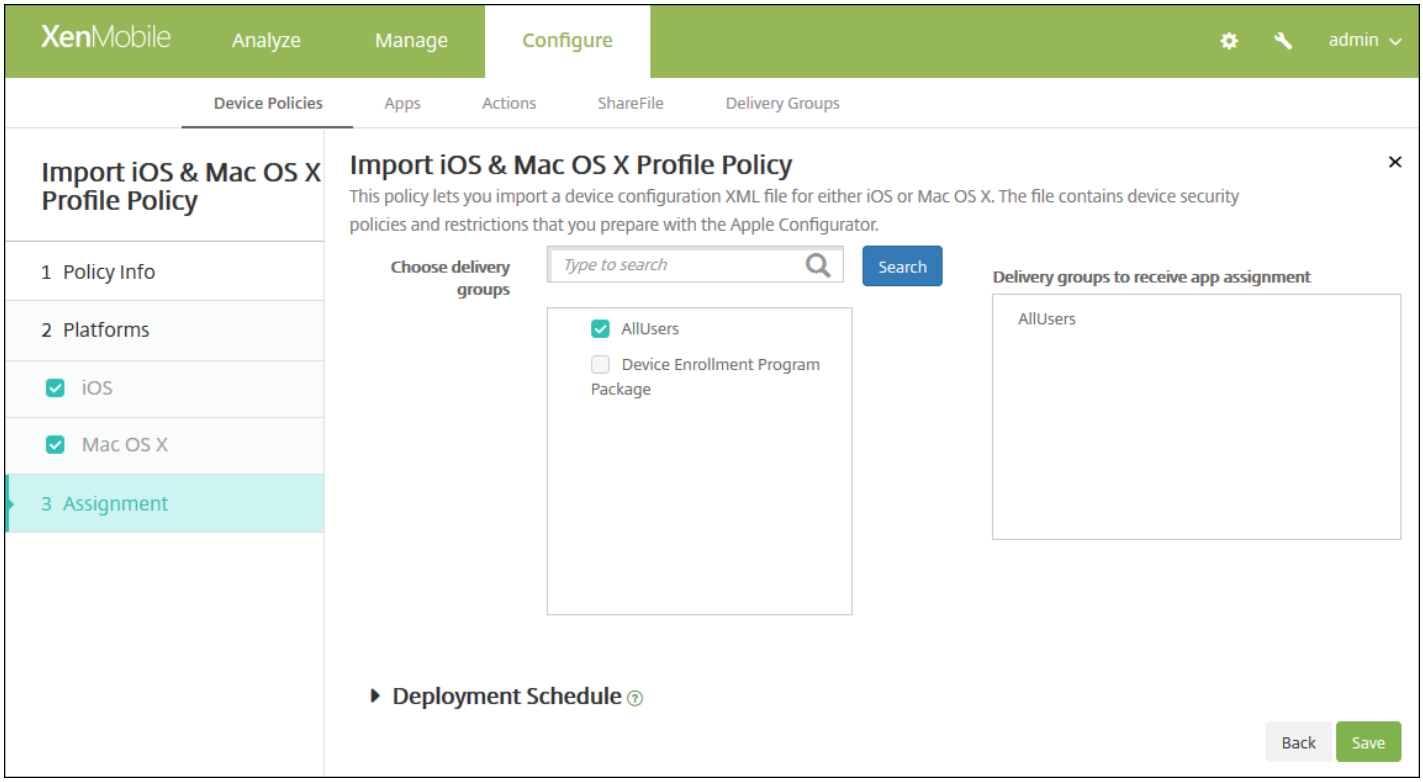
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 8 pour savoir comment définir les règles de déploiement de cette plate-forme. .

7. Configurez ce paramètre pour chaque plate-forme que vous avez sélectionnée :

- **Profil de configuration iOS** ou **Profil de configuration OS X** : sélectionnez le fichier de configuration à importer en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

8. Configurez les règles de déploiement.

9. Cliquez sur **Next**. La page d'attribution **Importer le profil iOS et Mac OS X** s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

12. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Placer un appareil iOS en mode supervisé avec Apple Configurator

Pour utiliser Apple Configurator, vous avez besoin d'un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure.

> **Important**
>
> le fait de placer un appareil en mode supervisé installera la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

1. Installez Apple Configurator depuis iTunes.

2. Connectez l'appareil iOS à votre ordinateur Apple.

3. Démarrez Apple Configurator. Le Configurateur indique que vous possédez un appareil à préparer pour la supervision.

4. Pour préparer l'appareil à des fins de supervision :

a. Basculez le contrôle de **supervision** sur **Activé**. Citrix vous recommande de sélectionner ce paramètre si vous prévoyez de gérer le contrôle de l'appareil en appliquant à nouveau une configuration régulièrement.

c. Si vous le souhaitez, entrez un nom pour l'appareil.

c. Dans iOS, cliquez sur l'option appropriée afin d'obtenir la version **la plus récente** d'iOS que vous souhaitez installer.

5. Lorsque vous êtes prêt à préparer l'appareil pour la supervision, cliquez sur **Préparer**.

Stratégie kiosque pour Samsung SAFE

Feb 23, 2017

Lorsque vous créez une stratégie kiosque dans XenMobile, cela vous permet de spécifier les applications spécifiques autorisées à être exécutées sur des appareils Samsung SAFE. Cette stratégie est utile pour les appareils d'entreprise conçus pour n'exécuter qu'un type spécifique ou une classe d'applications. Cette stratégie vous permet également de choisir des images personnalisées à utiliser comme fond d'écran de l'écran d'accueil et de l'écran de verrouillage lorsque l'appareil est en mode Kiosque.

Pour placer un appareil Samsung SAFE en mode kiosque

1. Activez la clé d'API Samsung SAFE sur l'appareil mobile, comme décrit dans la section Stratégies de clé de licence MDM Samsung. Cette étape vous permet d'activer des stratégies sur des appareils Samsung SAFE.

2. Activez la Stratégie de planification de connexion pour appareils Android, comme décrit dans la section Stratégies de planification de connexion. Cette étape permet aux appareils Android de se connecter à XenMobile.

3. Ajoutez une stratégie kiosque, comme décrit dans la section suivante.

4. Attribuez ces trois stratégies aux groupes de mise à disposition appropriés. Déterminez si vous souhaitez inclure d'autres stratégies, telles que Inventaire des applications, à ces groupes de mise à disposition.

Si vous souhaitez supprimer les appareils du mode kiosque ultérieurement, créez une nouvelle stratégie kiosque pour laquelle le **mode kiosque** est défini sur **Désactiver**. Mettez à jour le ou les groupes de mise à disposition pour supprimer la stratégie kiosque qui activait le mode kiosque et pour ajouter la stratégie kiosque qui désactive le mode kiosque.

Pour ajouter une stratégie kiosque

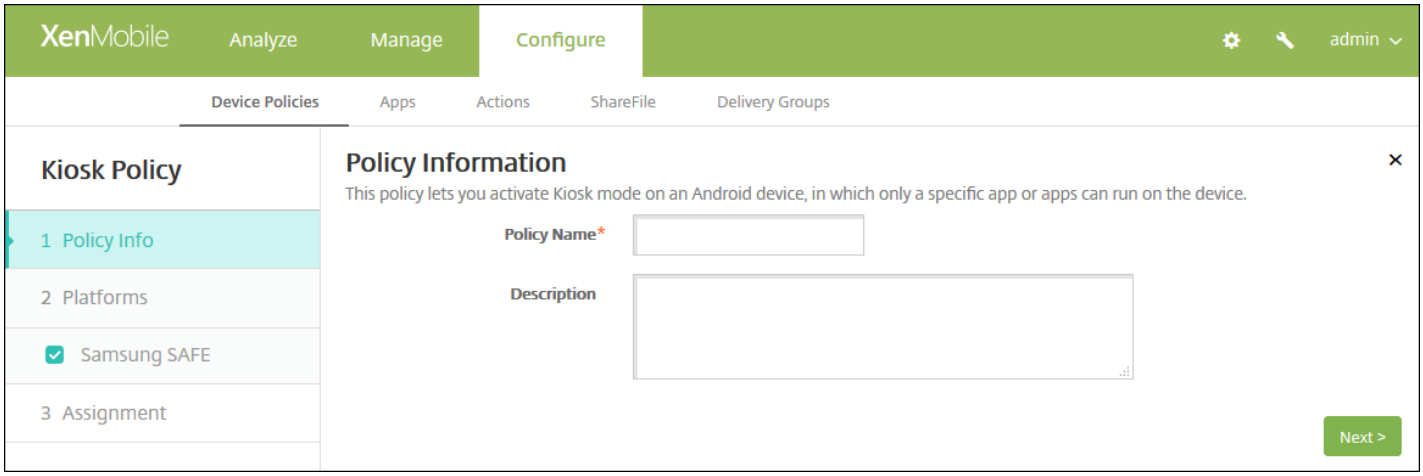
Remarque :

- Toutes les applications que vous spécifiez pour le mode kiosque doivent déjà être installées sur les appareils des utilisateurs.
- Certaines options ne s'appliquent qu'à l'API Samsung Mobile Device Management (MDM) 4.0 et versions ultérieures.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

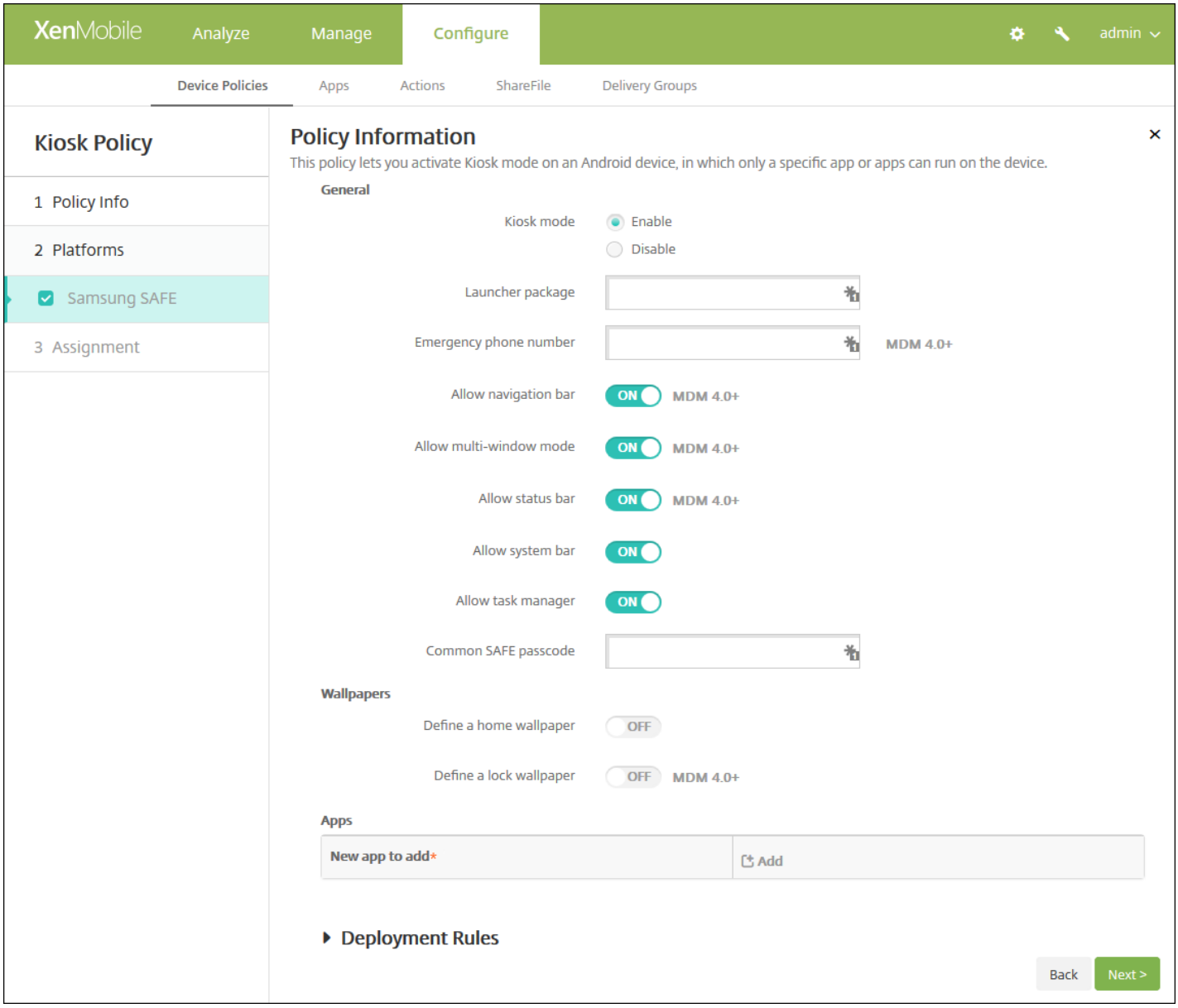
3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Kiosque**. La page **Stratégie kiosque** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Samsung SAFE** s'affiche.



6. Configurez les paramètres suivants :

- **Mode kiosque** : cliquez sur **Activer** ou **Désactiver**. La valeur par défaut est **Activer**. Lorsque vous cliquez sur **Désactiver**, toutes les options suivantes disparaissent.
- **Paquetage du lanceur** : Citrix vous recommande de laisser ce champ vide si vous avez développé un lanceur interne pour permettre aux utilisateurs d'ouvrir l'application ou les applications kiosque. Si vous utilisez un lanceur interne, entrez le nom complet du paquetage de l'application du lanceur.
- **Téléphone d'urgence** : entrez un numéro de téléphone (facultatif). Ce numéro peut être utilisé par toute personne qui trouve un appareil perdu pour contacter votre société. S'applique uniquement à MDM 4.0 et versions ultérieures.
- **Autoriser la barre de navigation** : sélectionnez cette option pour permettre aux utilisateurs de voir et utiliser la barre de navigation en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **ON**.
- **Autoriser le mode multi-fenêtre** : sélectionnez cette option pour permettre aux utilisateurs d'utiliser plusieurs fenêtres en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **ON**.
- **Autoriser la barre d'état** : sélectionnez cette option pour permettre aux utilisateurs de voir la barre d'état en mode Kiosque. S'applique uniquement à MDM 4.0 et versions ultérieures. La valeur par défaut est **ON**.

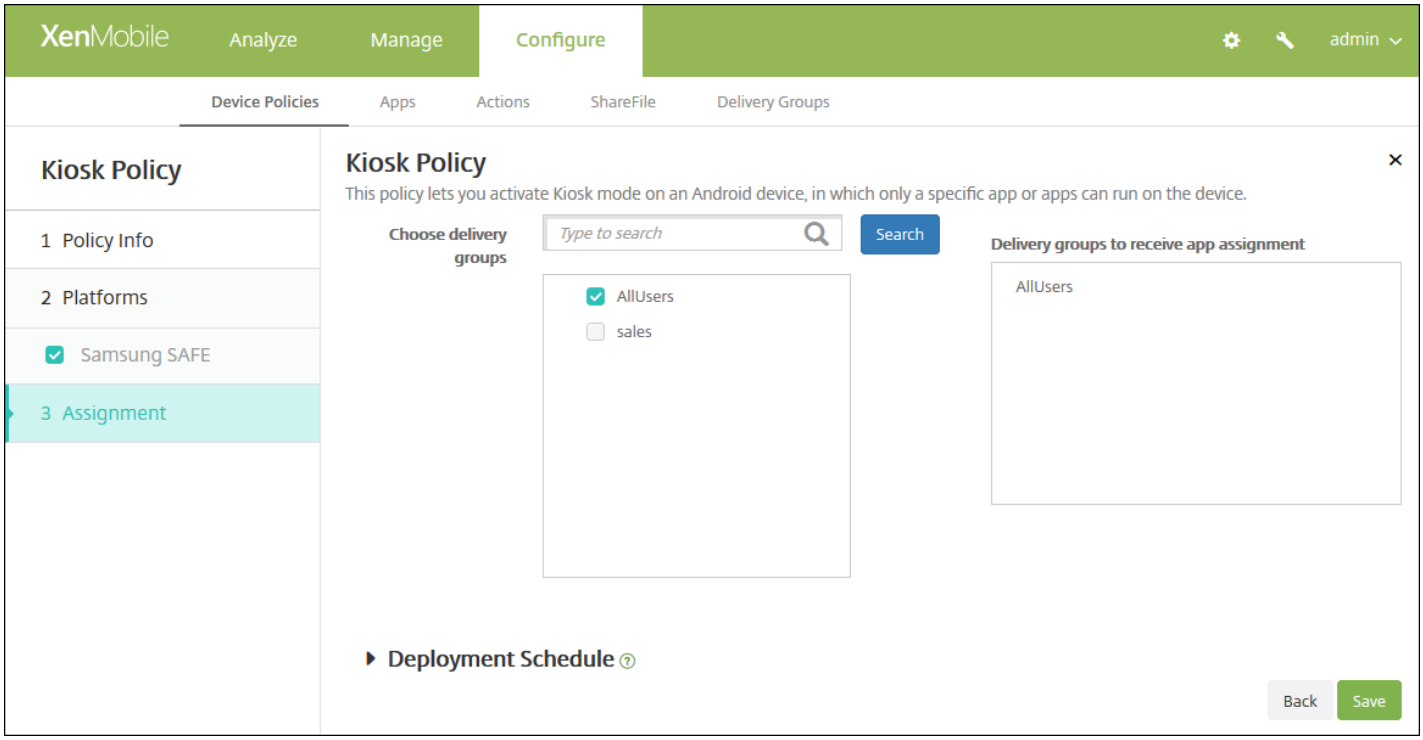
- **Autoriser la barre système** : sélectionnez cette option pour permettre aux utilisateurs de voir la barre système en mode Kiosque. La valeur par défaut est **ON**.
- **Autoriser le gestionnaire de tâches** : sélectionnez cette option pour permettre aux utilisateurs de voir et utiliser le gestionnaire de tâches en mode Kiosque. La valeur par défaut est **ON**.
- **Code secret SAFE** : si vous avez défini une stratégie de code secret générale pour tous les appareils Samsung SAFE, entrez ce code facultatif dans ce champ.
- **Fonds d'écran**
  - **Définir un fond d'écran accueil** : sélectionnez cette option pour utiliser une autre image personnalisée pour l'écran d'accueil en mode Kiosque. La valeur par défaut est **OFF**.
    - **Image accueil** : lorsque vous activez **Définir un fond d'écran accueil**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
  - **Définir un fond d'écran verrou** : sélectionnez cette option pour utiliser une autre image personnalisée pour l'écran de verrouillage en mode Kiosque. La valeur par défaut est **OFF**. S'applique uniquement à MDM 4.0 et versions ultérieures.
    - **Image verrou** : lorsque vous activez **Définir un fond d'écran verrou**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.
- **Applications** : pour chaque application que vous souhaitez ajouter au mode kiosque, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nouvelle application à ajouter** : entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar permet aux utilisateurs d'utiliser l'application calendrier d'Android.
  - Cliquez sur **Enregistrer** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie kiosque** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de configuration du Launcher pour Android

Feb 23, 2017

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android déployés par XenMobile. Vous pouvez ajouter une stratégie de configuration du Launcher pour contrôler ces fonctionnalités de Citrix Launcher :

- Gérez les appareils Android, de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

Si Citrix Launcher vous permet d'appliquer ces restrictions sur l'appareil, il donne aux utilisateurs la flexibilité opérationnelle dont ils ont besoin via un accès intégré à des paramètres de l'appareil tels que les paramètres Wi-Fi, les réglages Bluetooth et les paramètres de code secret de l'appareil. Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

Lorsque vous déployez Citrix Launcher, XenMobile l'installe et il remplace le Launcher Android par défaut.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

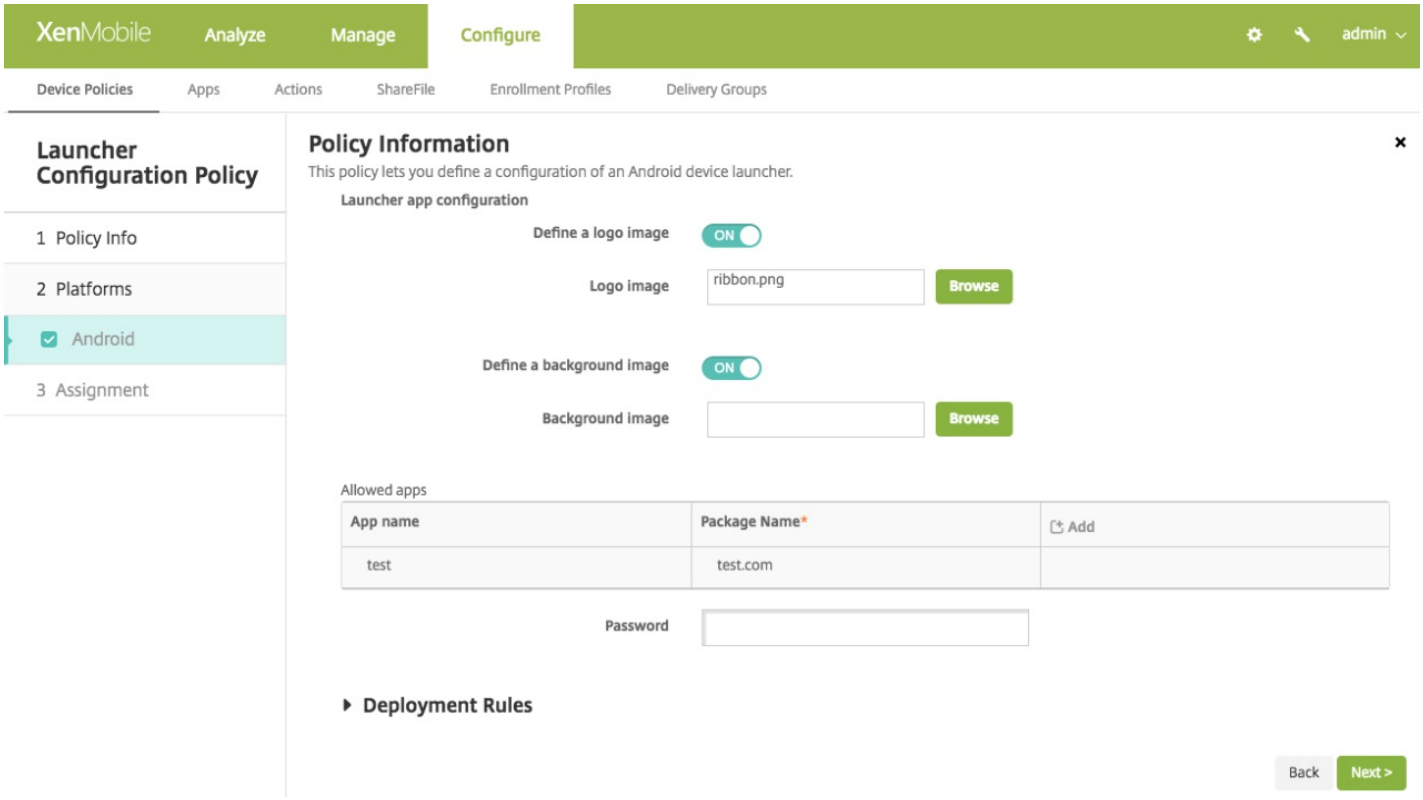
2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Commencez à taper **Launcher**, puis sélectionnez **Launcher Configuration** dans la liste. L'écran **Stratégie de configuration du Launcher** s'affiche.

4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Plate-forme Android** s'affiche.



6. Configurez les paramètres suivants :

- **Définir une image de logo** : indiquez si vous souhaitez utiliser une image de logo personnalisé pour l'icône Citrix Launcher. La valeur par défaut est **OFF**.
- **Image du logo** : lorsque vous activez **Définir une image de logo**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Définir une image d'arrière-plan** : indiquez si vous souhaitez utiliser une image personnalisée pour l'arrière-plan de Citrix Launcher. La valeur par défaut est **OFF**.
- **Image d'arrière-plan** : lorsque vous activez **Définir une image d'arrière-plan**, sélectionnez le fichier d'image en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Les types de fichier pris en charge sont PNG, JPG, JPEG et GIF.
- **Applications autorisée** : pour chaque application que vous souhaitez autoriser dans Citrix Launcher, cliquez sur **Ajouter**, puis procédez comme suit :
  - **Nouvelle application à ajouter** : entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar pour l'application calendrier d'Android.
  - Cliquez sur **Enregistrer** pour ajouter l'application, ou cliquez sur **Annuler** pour annuler l'ajout de l'application.

    Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.
- **Mot de passe** : le mot de passe qu'un utilisateur doit entrer pour quitter Citrix Launcher.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de configuration du Launcher** s'affiche.

9. Configurez les règles de déploiement.

10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

12. Cliquez sur **Enregistrer**.

Stratégies LDAP

Feb 23, 2017

Vous créez une stratégie LDAP pour appareils iOS dans XenMobile pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information sur le compte nécessaires. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.

Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.

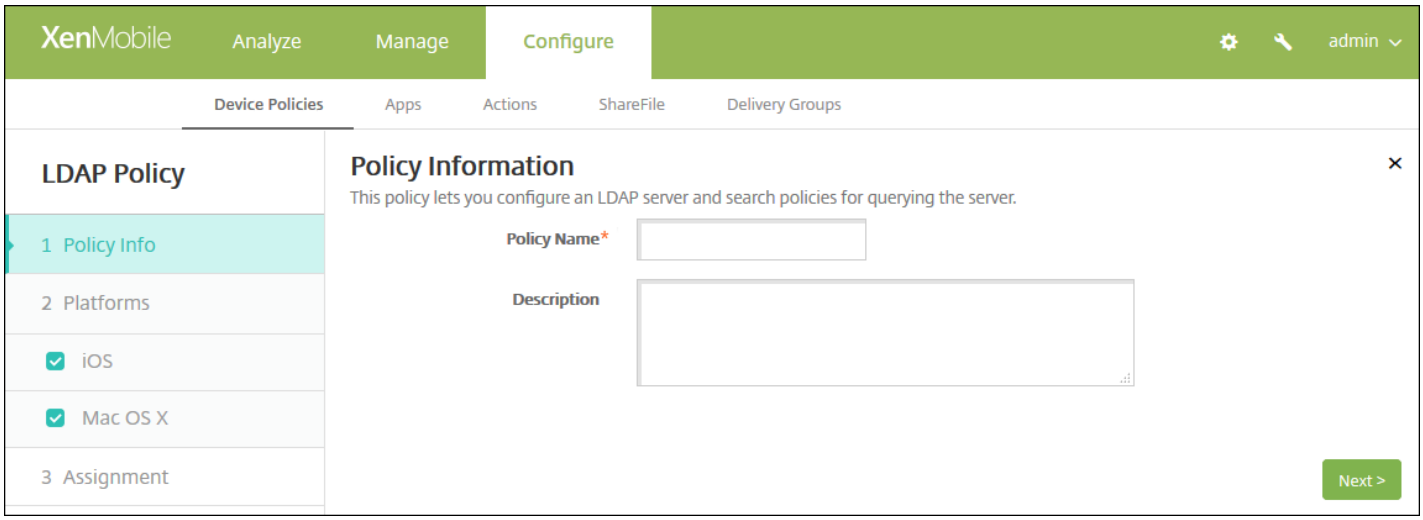
Paramètres iOS

Paramètres Mac OS X

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis, sous **Utilisateur final**, cliquez sur **LDAP**. La page **Stratégie LDAP** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

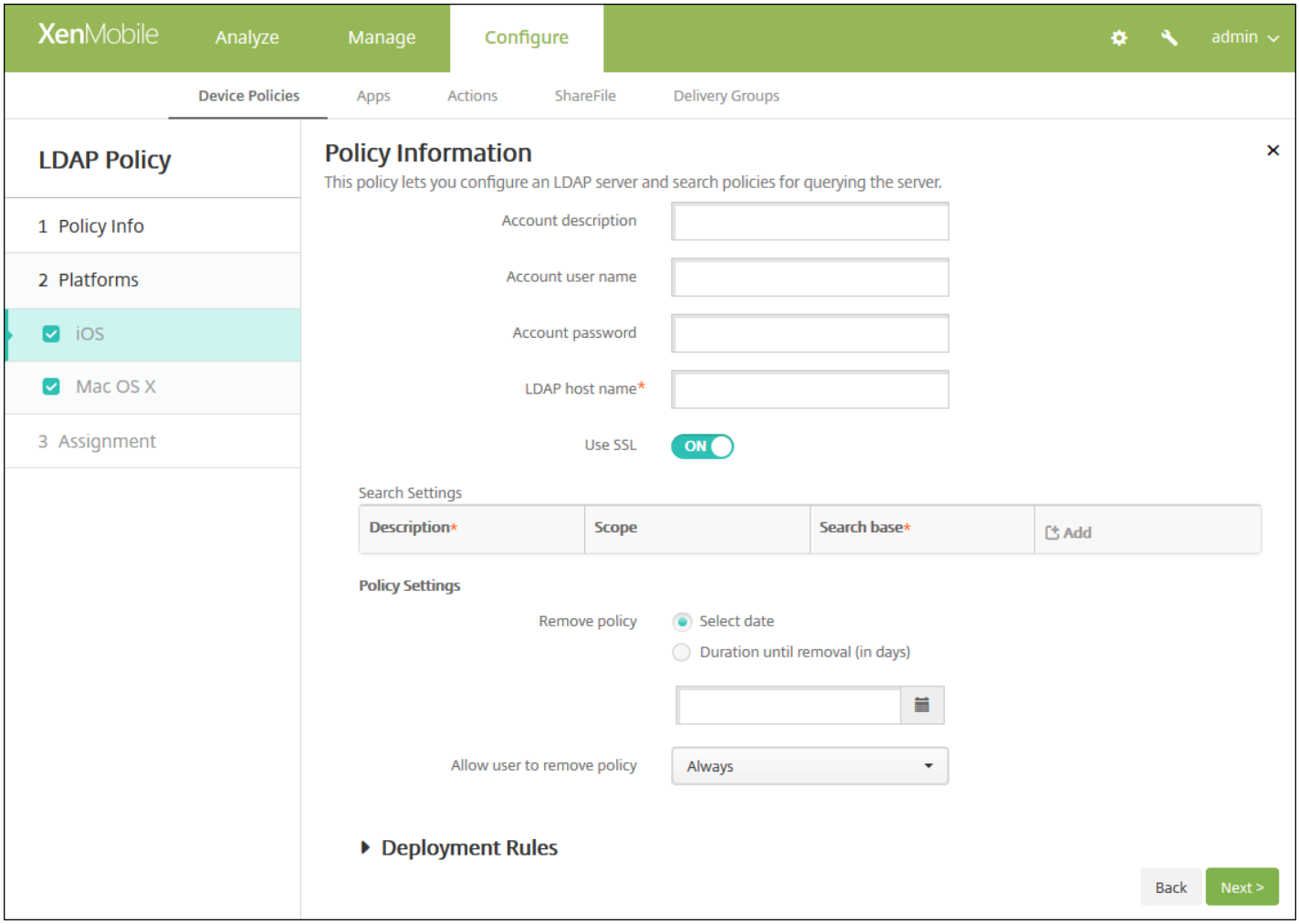
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



Configurez les paramètres suivants :

- **Description du compte** : entrez une description du compte (facultatif).
- **Nom d'utilisateur du compte** : entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte** : entrez un mot de passe (facultatif). À utiliser uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP** : entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **ON**.
- **Paramètres de recherche** : ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :
  - **Description** : entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
  - **Portée** : dans la liste, cliquez sur **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est Base.
    - Base recherche le nœud indiqué par la Base de recherche.
    - Un niveau recherche le nœud Base et un niveau en dessous.
    - Sous-arborescence recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche** : entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur Annuler pour annuler l'ajout du paramètre de

recherche.

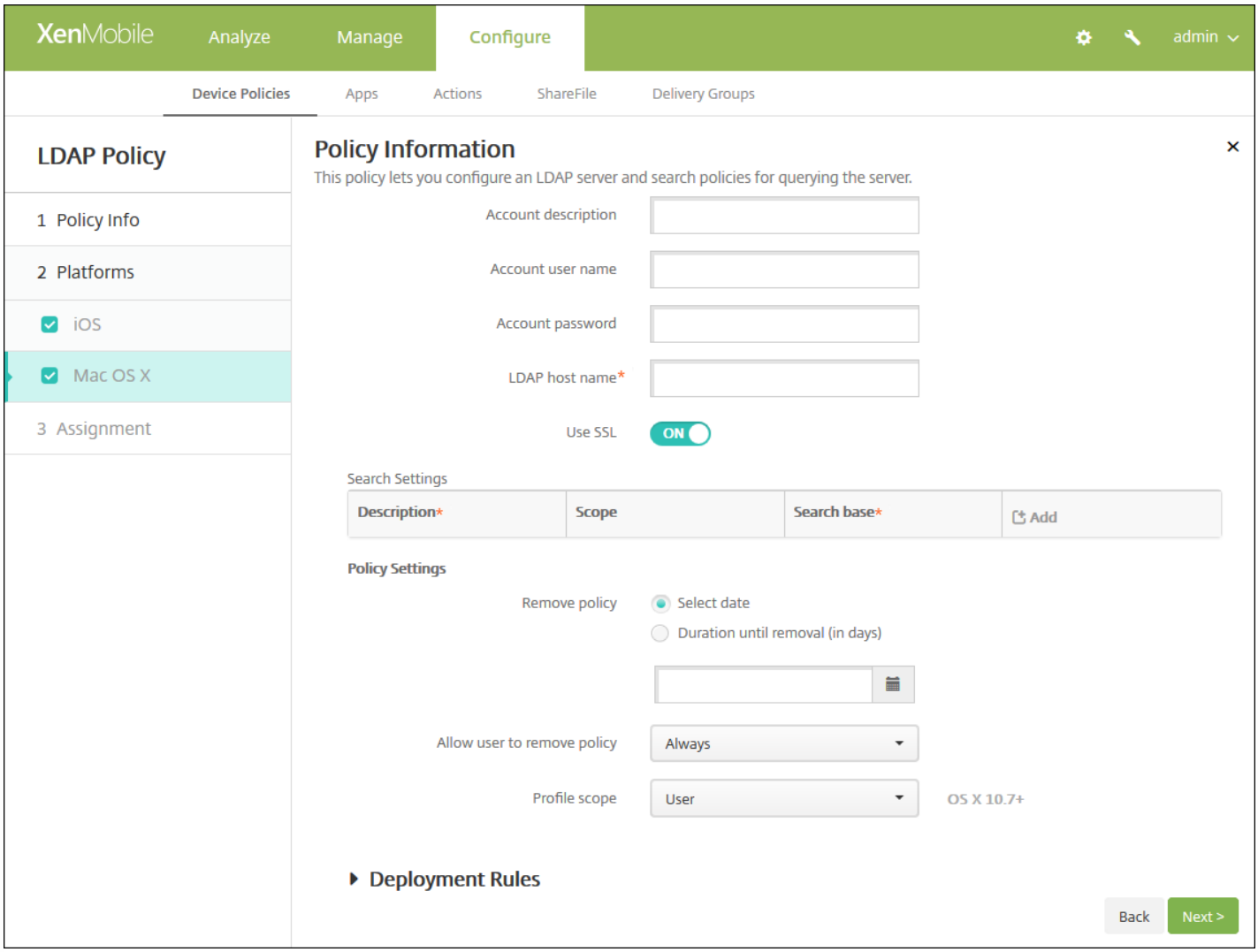
- Répétez ces étapes pour chaque paramètre de recherche à ajouter.

  Remarque : pour supprimer un paramètre de recherche, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

  Pour modifier un paramètre de recherche, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

- Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
- Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X



Configurez les paramètres suivants :

- **Description du compte** : entrez une description du compte (facultatif).
- **Nom d'utilisateur du compte** : entrez un nom d'utilisateur (facultatif).
- **Mot de passe du compte** : entrez un mot de passe (facultatif). À utiliser uniquement avec des profils chiffrés.
- **Nom d'hôte LDAP** : entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.
- **Utiliser SSL** : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est **ON**.
- **Paramètres de recherche** : ajoutez les paramètres de recherche à utiliser lors de l'interrogation du serveur LDAP. vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous devez ajouter au moins un paramètre de recherche pour faire du compte une ressource utile. Cliquez sur **Ajouter**, puis procédez comme suit :
  - **Description** : entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
  - **Portée** : dans la liste, cliquez sur **Base**, **Un niveau** ou **Sous-arborescence** pour définir la profondeur de la recherche dans l'arborescence LDAP. La valeur par défaut est Base.
    - Base recherche le nœud indiqué par la Base de recherche.
    - Un niveau recherche le nœud Base et un niveau en dessous.
    - Sous-arborescence recherche le nœud Base, ainsi que tous ses enfants, quelle que soit la profondeur.
  - **Base de recherche** : entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Par exemple, ou=people ou 0=example corp. Ce champ est obligatoire.
  - Cliquez sur **Ajouter** pour ajouter le paramètre de recherche ou cliquez sur Annuler pour annuler l'ajout du paramètre de recherche.
  - Répétez ces étapes pour chaque paramètre de recherche à ajouter.

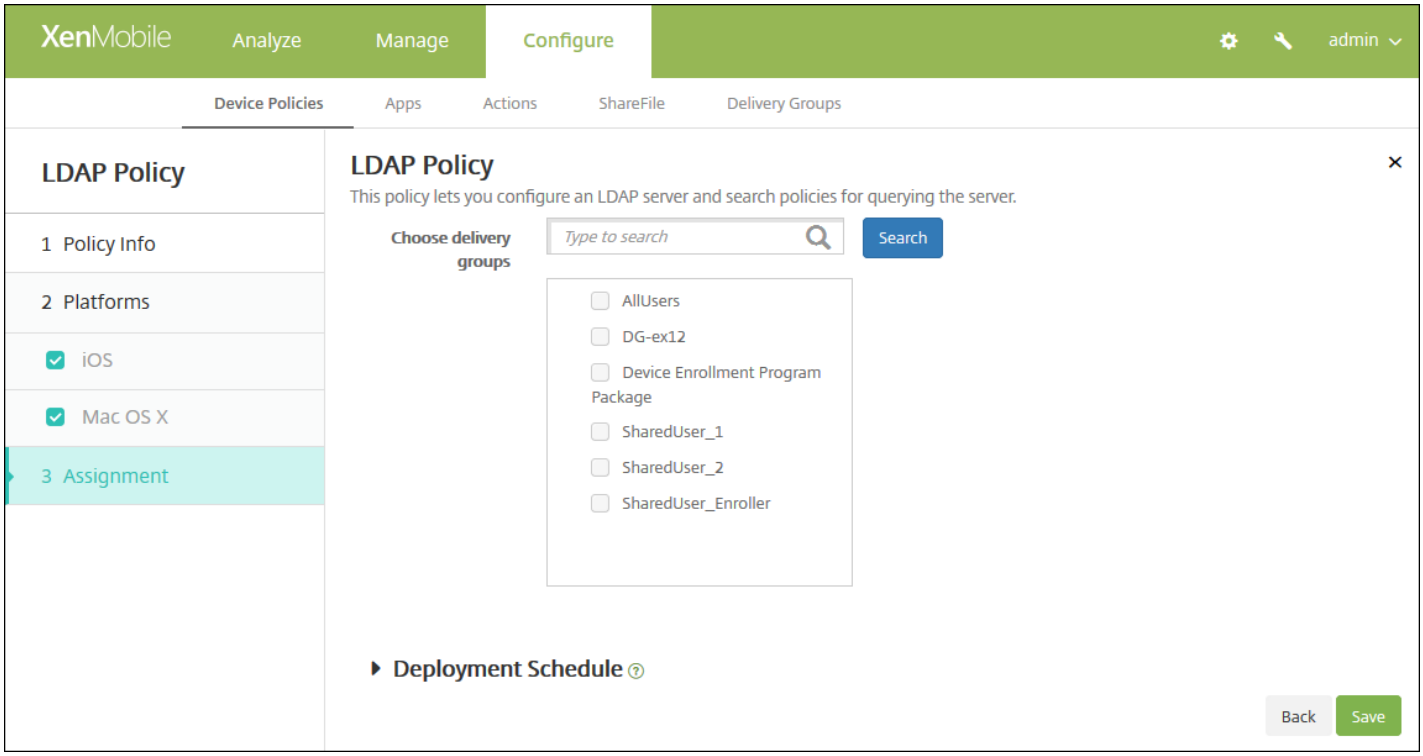
    Remarque : pour supprimer un paramètre de recherche, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

    Pour modifier un paramètre de recherche, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

- Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.
- Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
- Dans **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie LDAP** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégies d'emplacement

Feb 23, 2017

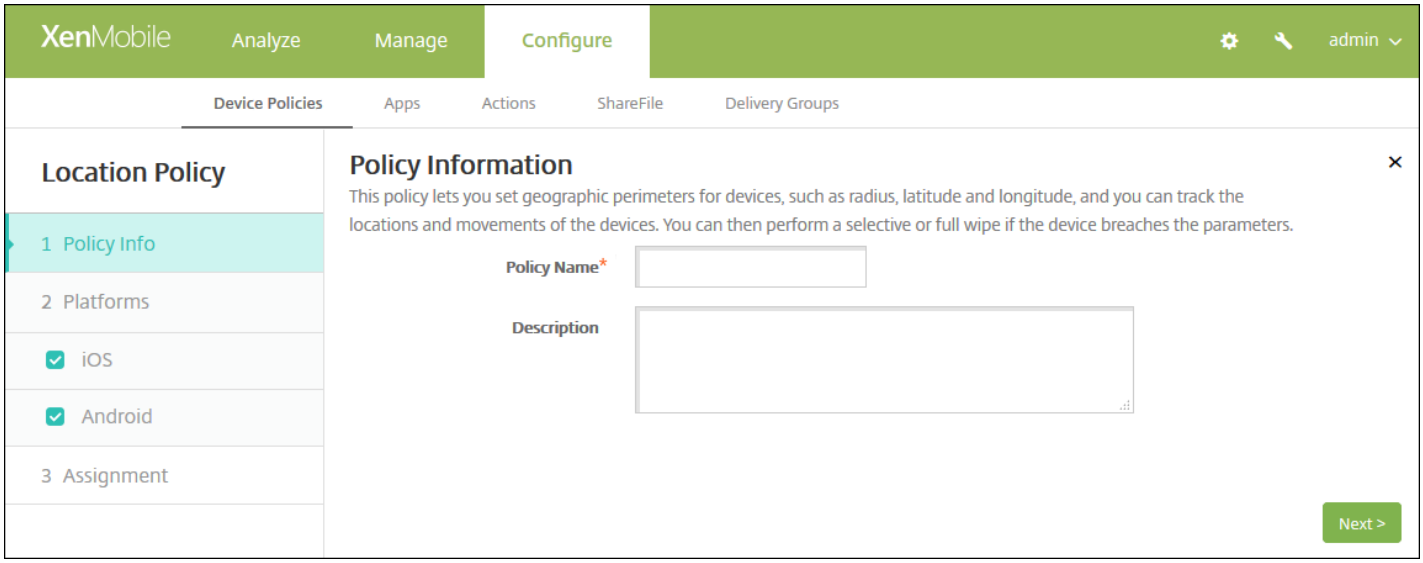
Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques, et suivre l'emplacement et les déplacements des appareils des utilisateurs. Lorsque les utilisateurs violent le périmètre défini, également appelé *géofencing*, XenMobile peut effacer immédiatement toutes les données sur l'appareil ou uniquement les données d'entreprise, ou les effacer après une période de temps donnée pour laisser le temps aux utilisateurs de revenir dans le périmètre autorisé.

Vous pouvez créer des stratégies d'emplacement pour iOS et Android. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Emplacement**. La page d'informations **Stratégie d'emplacement** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

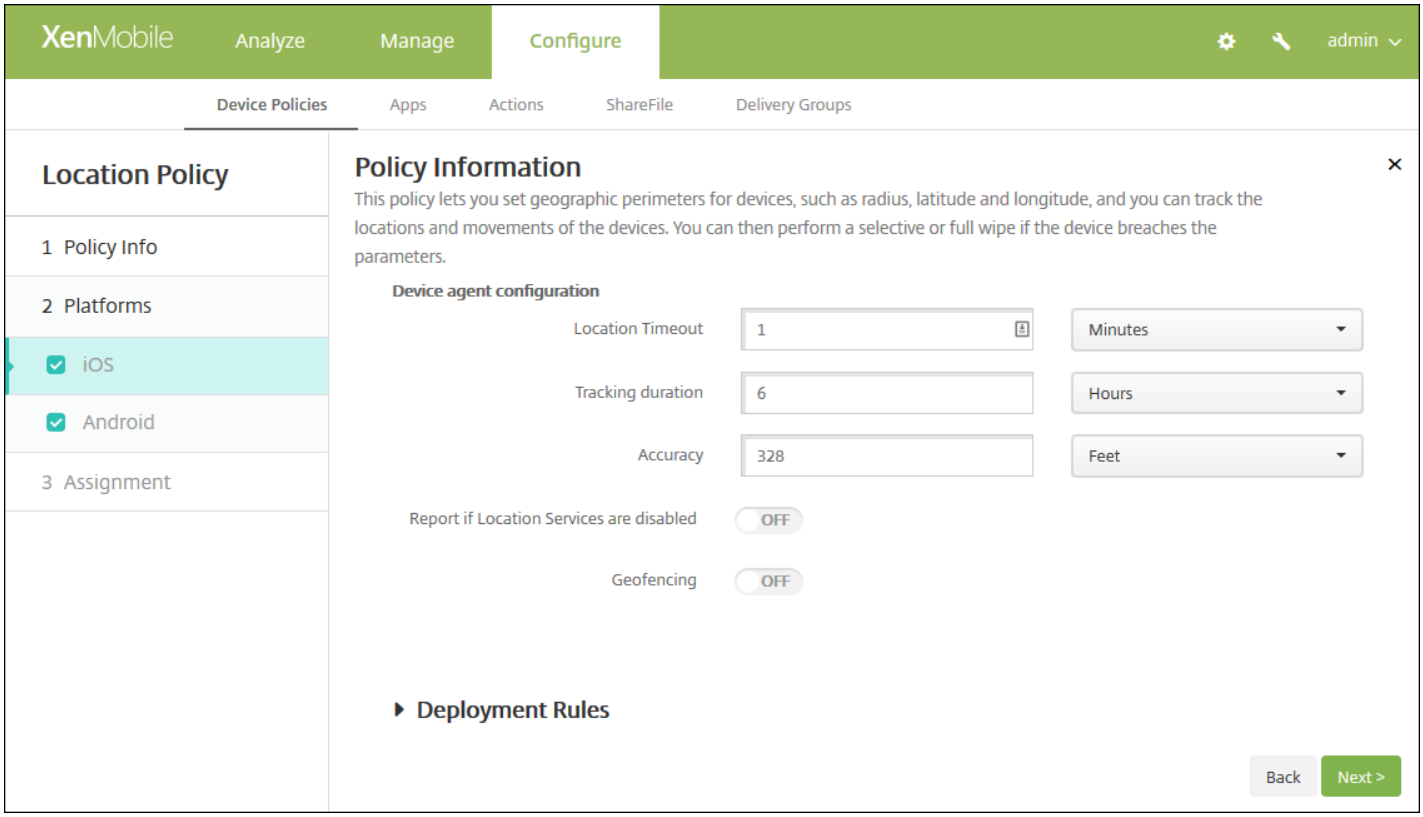
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

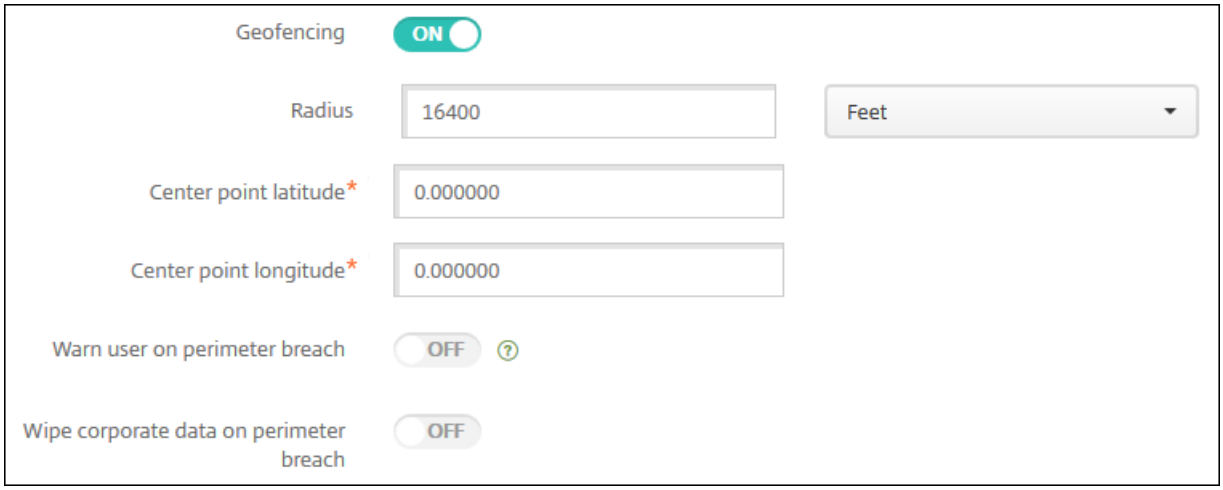
Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



Pour configurer ces paramètres :

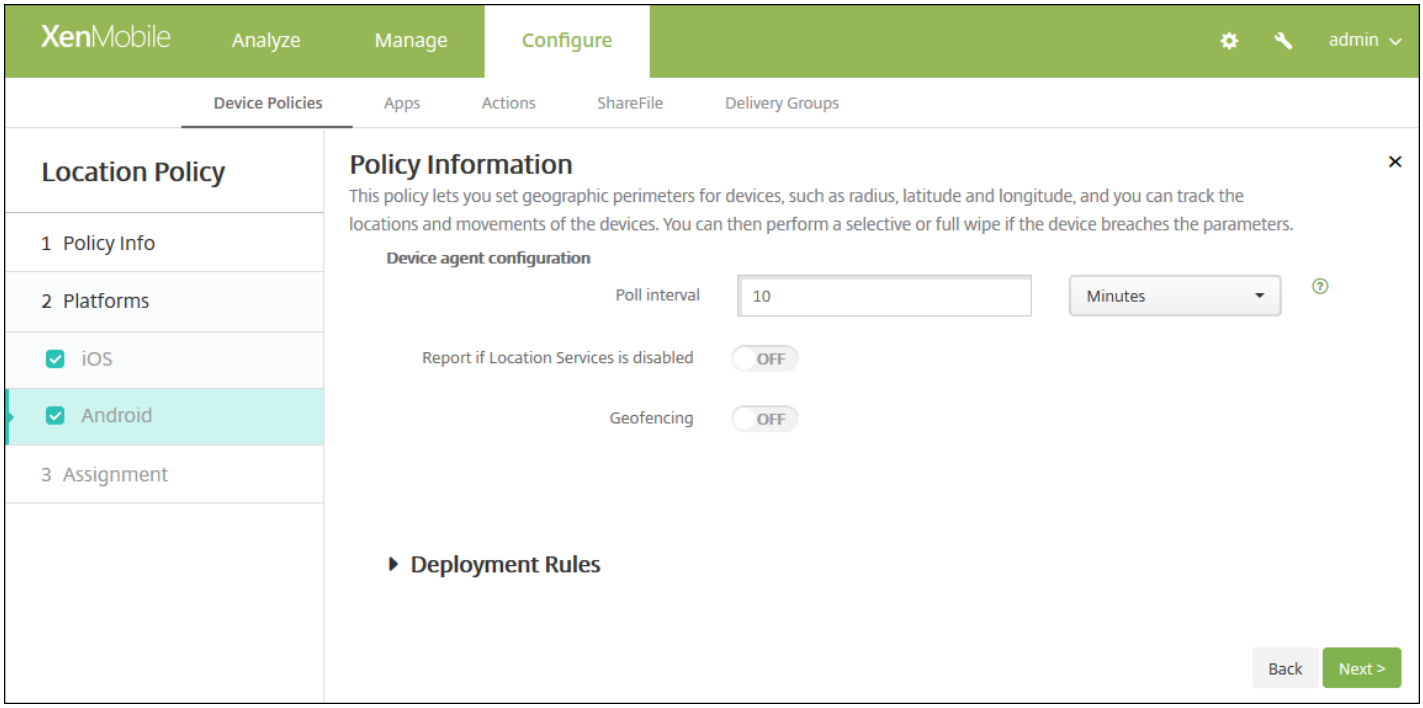
- **Délai max. de localisation** : entrez un chiffre, puis, dans la liste, cliquez sur **Secondes** ou **Minutes** pour définir la fréquence à laquelle XenMobile tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 60–900 secondes ou 1–15 minutes. La valeur par défaut est 1 minute.
- **Durée du suivi** : entrez un chiffre, puis, dans la liste, cliquez sur **Secondes** ou **Minutes** pour définir la durée pendant laquelle XenMobile suit l'appareil. Les valeurs valides sont 1 à 6 heures ou 10 à 360 minutes. La valeur par défaut est 6 heures.
- **Précision** : entrez un chiffre, puis cliquez sur **Mètres**, **Feet** ou **Yards** dans la liste pour définir la précision du suivi effectué par XenMobile. Les valeurs valides sont 10–5000 yards ou mètres ou 30–15000 feet. La valeur par défaut est 328 feet.
- **M'avertir si les services de localisation sont désactivés** : sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile lorsque le GPS est désactivé. La valeur par défaut est **OFF**.
- **Géofencing**



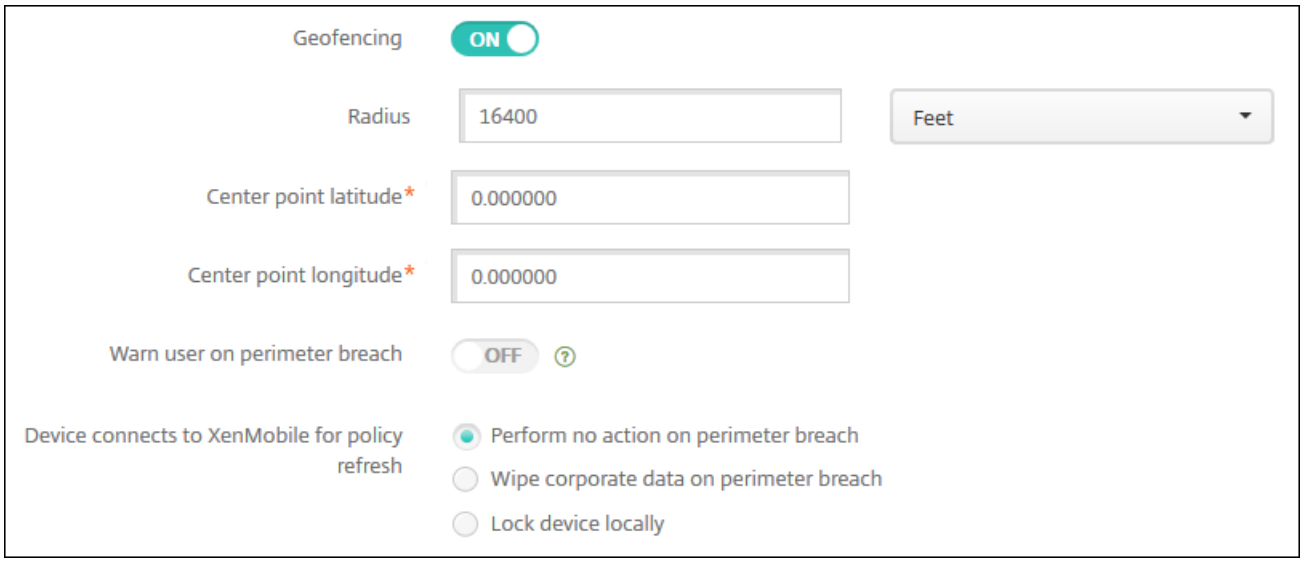
Lorsque vous activez Géofencing, configurez les paramètres suivants :

- **Rayon** : entrez un chiffre, puis, dans la liste, cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est 16 400 feet. Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 50–50000 mètres
  - 54–54680 yards
  - 1–31 miles
- **Latitude du point central** : entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central** : entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre** : choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **OFF**. Aucune connexion à XenMobile n'est nécessaire pour afficher le message d'avertissement.
- **Effacer les données d'entreprise en cas de violation du périmètre** : indiquez si vous souhaitez effacer les appareils des utilisateurs lorsqu'ils violent le périmètre. La valeur par défaut est **OFF**. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
  - Entrez un chiffre, puis, dans la liste, cliquez sur **Secondes** ou **Minutes** pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Cela offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile n'efface leurs appareils. La durée par défaut est de 0 secondes.

Configurer les paramètres pour Android



- **Echantillonnage** : entrez un chiffre, puis, dans la liste, cliquez sur **Minutes**, **Heures** ou **Jours** pour définir la fréquence à laquelle XenMobile tente de déterminer l'emplacement de l'appareil. Les valeurs valides sont 1–1440 minutes, 1–24 heures ou un nombre quelconque de jours. La valeur par défaut est 10 minutes. si la valeur définie est inférieure à 10 minutes, cela peut avoir un impact négatif sur l'autonomie de la batterie.
- **M'avertir si les services de localisation sont désactivés** : sélectionnez cette option si vous voulez que l'appareil envoie un rapport à XenMobile lorsque le GPS est désactivé. La valeur par défaut est **OFF**.
- **Géofencing**



Lorsque vous activez Géofencing, configurez les paramètres suivants :

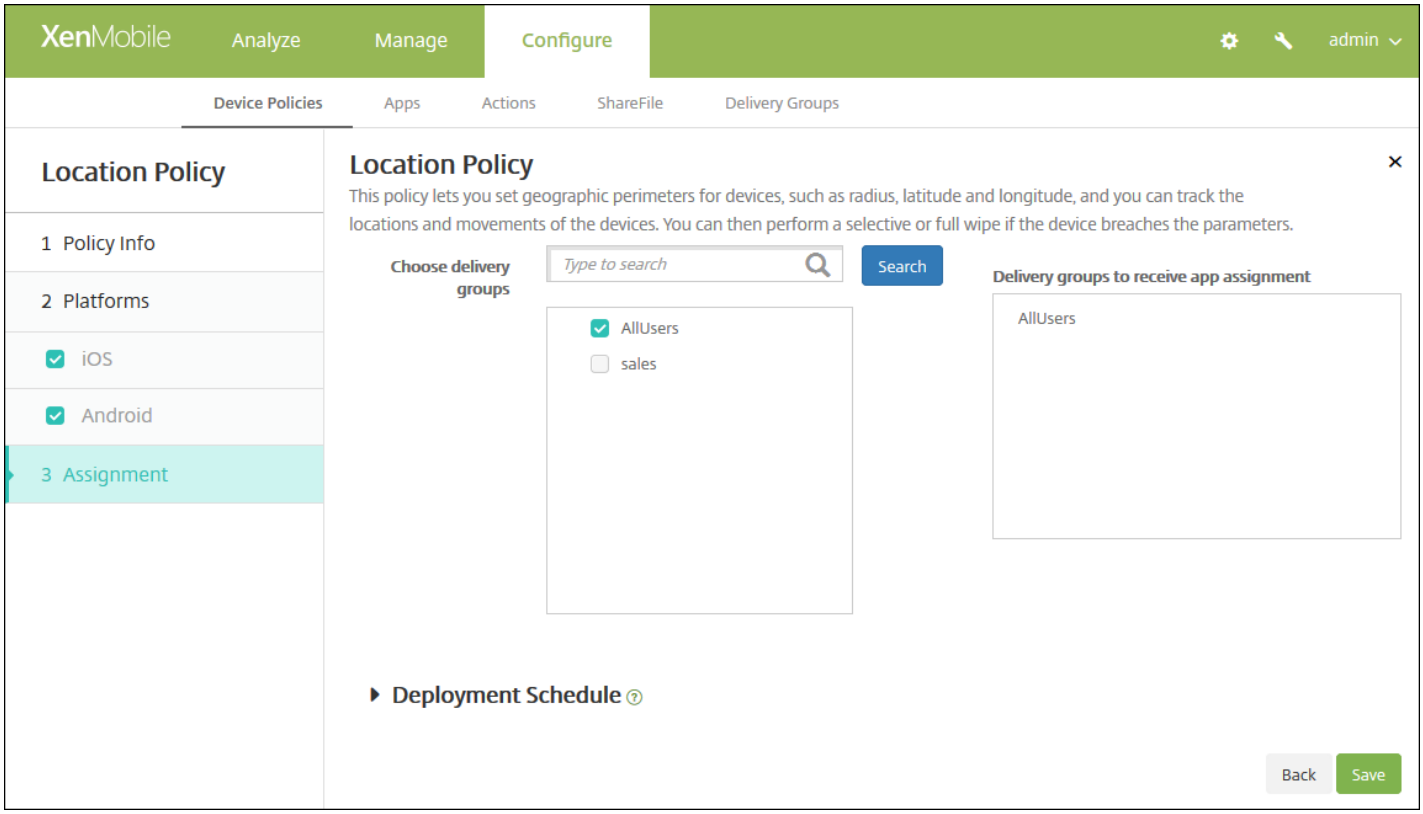
- **Rayon** : entrez un chiffre, puis, dans la liste, cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est 16 400 feet. Les valeurs valides pour le rayon sont :

- 164–164000 feet
- 1–50 kilomètres
- 50–50000 mètres
- 54–54680 yards
- 1–31 miles

- **Latitude du point central** : entrez une latitude, par exemple 37.787454, pour définir la latitude du point central du géofencing.
- **Longitude du point central** : entrez une longitude, par exemple 122.402952, pour définir la longitude du point central du géofencing.
- **Avertir l'utilisateur en cas de violation du périmètre** : choisissez d'afficher un message d'avertissement lorsque les utilisateurs violent le périmètre établi. La valeur par défaut est **OFF**. Aucune connexion à XenMobile n'est nécessaire pour afficher le message d'avertissement.
- **L'appareil se connecte à XenMobile pour actualiser la stratégie** : sélectionnez l'une des options suivantes à exécuter lorsque les utilisateurs violent le périmètre :
  - **N'effectuer aucune action en cas de violation du périmètre** : aucune action n'est prise. Il s'agit de l'option par défaut.
  - **Effacer les données d'entreprise en cas de violation du périmètre** : les données d'entreprise sont effacées après une durée spécifiée. Lorsque vous activez cette option, le champ **Délai avant l'effacement local** s'affiche.
    - Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Cela offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile n'efface leurs appareils. La durée par défaut est de 0 secondes.
  - **Délai du verrouillage** : verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ **Délai du verrouillage** s'affiche.
    - Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Cela offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile ne verrouille leurs appareils. La durée par défaut est de 0 secondes.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie d'emplacement** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de messagerie

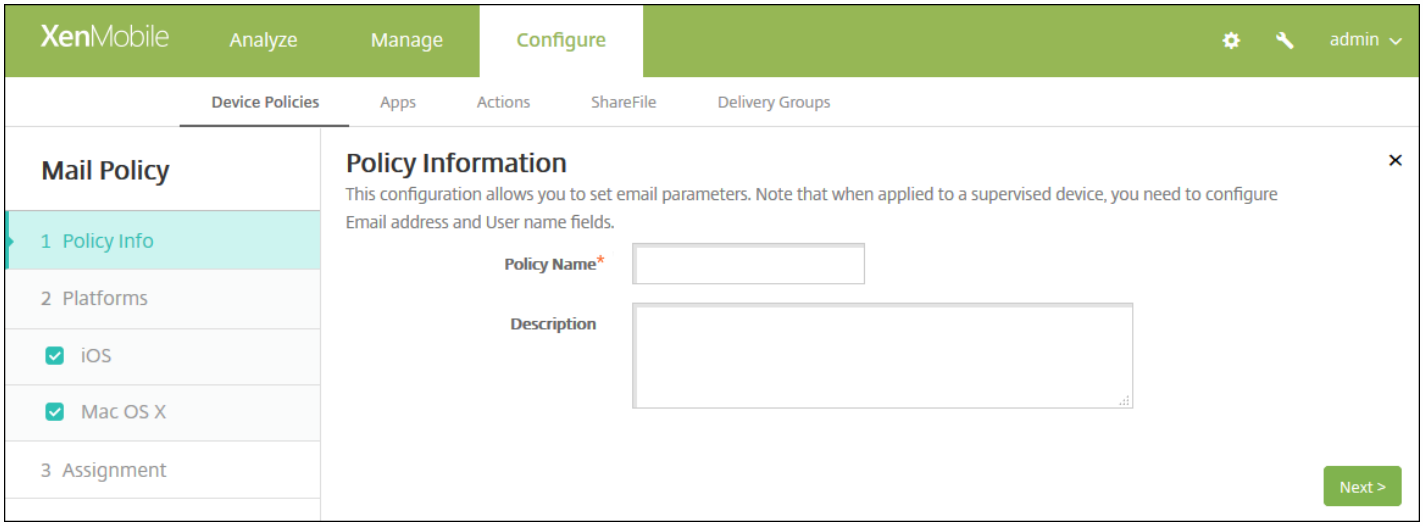
Feb 23, 2017

Vous pouvez ajouter une stratégie de messagerie dans XenMobile pour configurer un compte de messagerie sur les appareils iOS ou Mac OS X des utilisateurs.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

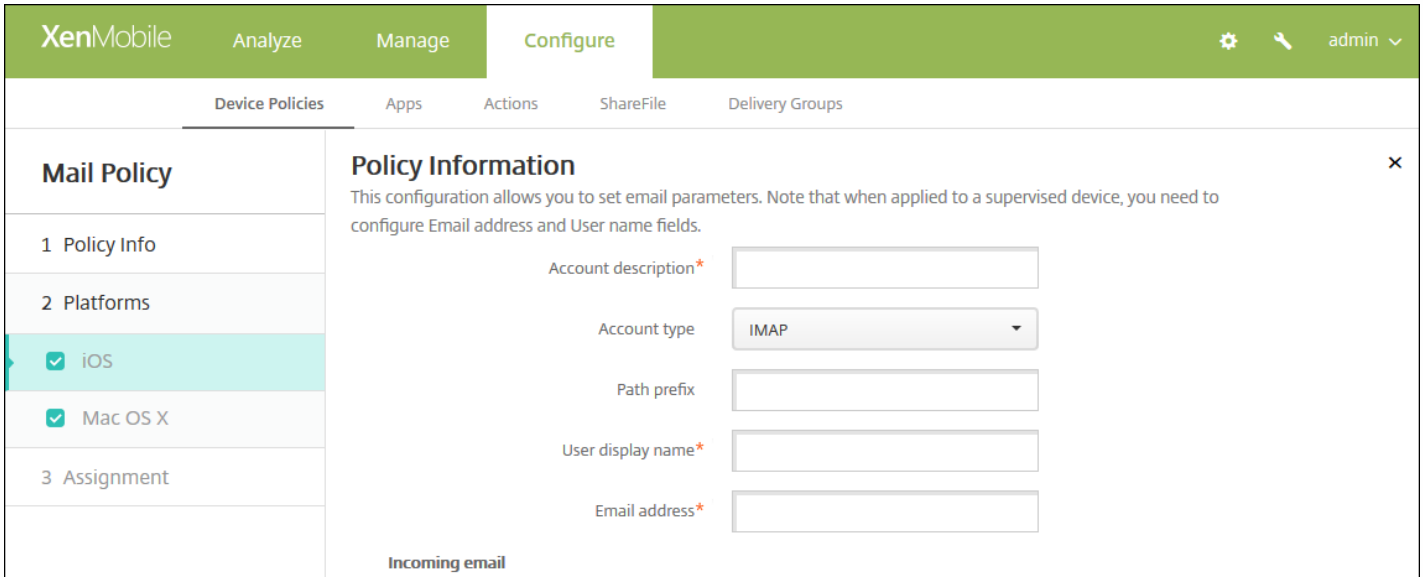
3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **Messagerie**. La page **Stratégie de messagerie** s'affiche.

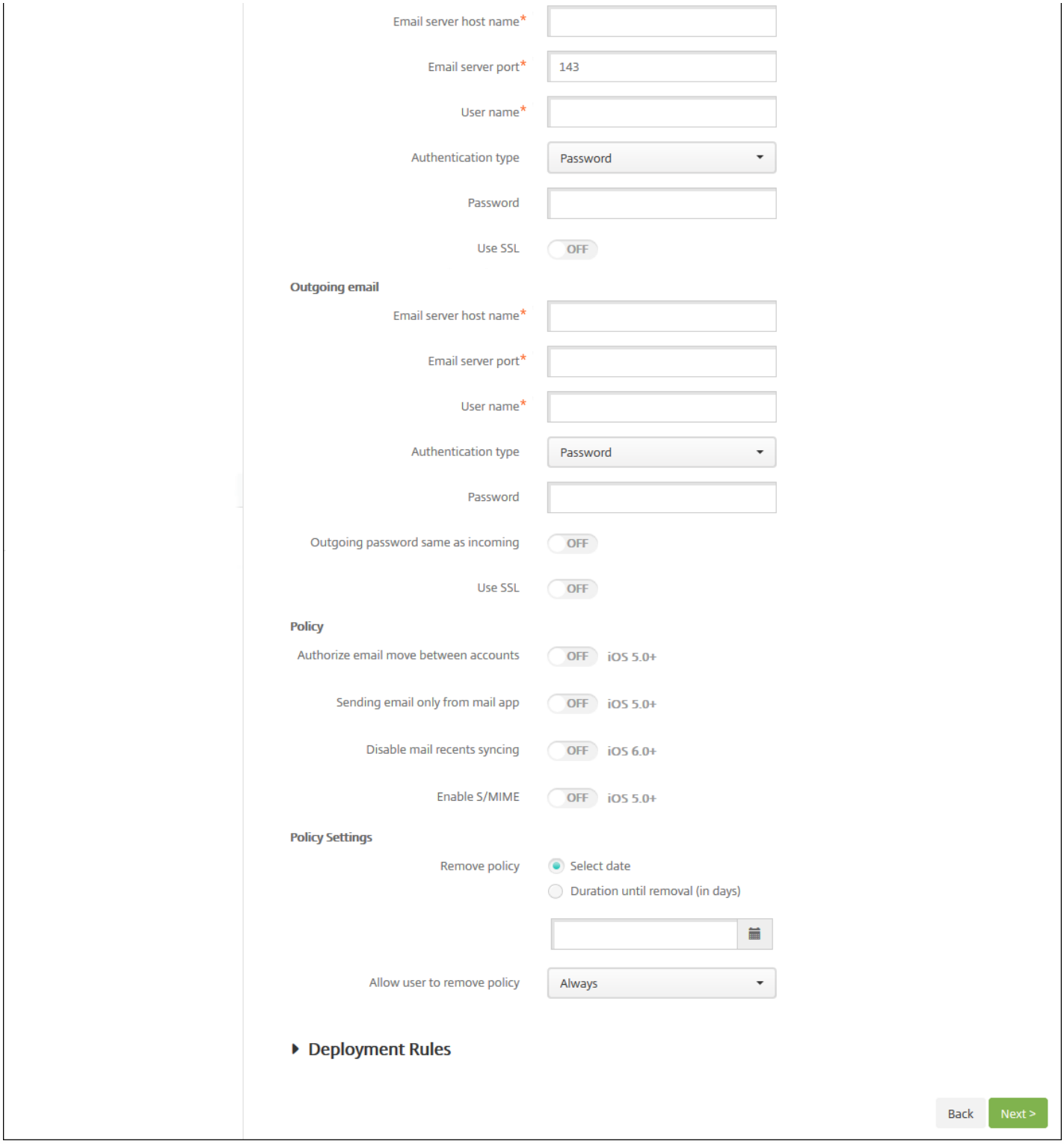


4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page de la **Stratégie par plate-forme de messagerie** s'affiche.





6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 8 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Configurez les paramètres suivants pour chaque plate-forme que vous avez sélectionnée.

- **Description du compte** : entrez une description pour le compte ; elle apparaît dans les applications de messagerie et de paramètres. Ce champ est obligatoire.
- **Type de compte** : dans la liste, cliquez sur **IMAP** ou **POP** pour sélectionner le protocole à utiliser pour les comptes d'utilisateur. La valeur par défaut est **IMAP**. Lorsque vous sélectionnez le protocole **POP**, l'option **Préfixe chemin** disparaît.
- **Préfixe chemin** : entrez **INBOX** ou le chemin d'accès à votre compte de messagerie IMAP s'il ne s'agit pas de **INBOX**. Ce champ est obligatoire.
- **Nom d'affichage de l'utilisateur** : entrez le nom d'utilisateur à utiliser dans les messages, etc. Ce champ est obligatoire.
- **Adresse électronique** : entrez l'adresse e-mail du compte. Ce champ est obligatoire.
- **Paramètres du courrier entrant**
  - **Nom d'hôte du serveur de messagerie** : entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier entrant. Ce champ est obligatoire.
  - **Port du serveur de messagerie** : entrez le numéro de port du serveur de courrier entrant. La valeur par défaut est de **143**. Ce champ est obligatoire.
  - **Nom d'utilisateur** : entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail de l'utilisateur à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification** : dans la liste, cliquez pour sélectionner le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**. Lorsque **Aucun** est sélectionné, le champ **Mot de passe** suivant disparaît.
  - **Mot de passe** : entrez un mot de passe pour le serveur de messagerie de courrier entrant (facultatif).
  - **Utiliser SSL** : sélectionnez cette option pour que le serveur de messagerie du courrier entrant utilise l'authentification SSL. La valeur par défaut est **OFF**.
- **Paramètres de messagerie du courrier sortant**
  - **Nom d'hôte du serveur de messagerie** : entrez le nom d'hôte ou l'adresse IP du serveur de messagerie du courrier sortant. Ce champ est obligatoire.
  - **Port du serveur de messagerie** : entrez le numéro de port du serveur de messagerie de courrier sortant. Si vous n'entrez pas de numéro de port, le port par défaut du protocole donné est utilisé.
  - **Nom d'utilisateur** : entrez le nom d'utilisateur du compte de messagerie. Ce nom est généralement le même que l'adresse e-mail de l'utilisateur à hauteur du caractère @. Ce champ est obligatoire.
  - **Type d'authentification** : dans la liste, cliquez pour sélectionner le type d'authentification à utiliser. La valeur par défaut est **Mot de passe**. Lorsque **Aucun** est sélectionné, le champ **Mot de passe** suivant disparaît.
  - **Mot de passe** : entrez un mot de passe pour le serveur de messagerie de courrier sortant (facultatif).
  - **Mot de passe sortant identique au mot de passe entrant** : sélectionnez cette option pour spécifier si les mots de passe entrants et sortants sont les mêmes. La valeur par défaut est OFF, ce qui signifie que les mots de passe sont différents. Lorsque cette option est définie sur **ON**, le champ **Mot de passe** précédent disparaît.
  - **Utiliser SSL** : sélectionnez cette option pour que le serveur de messagerie du courrier sortant utilise l'authentification SSL. La valeur par défaut est **OFF**.
- **Stratégie**
  - **Remarque** : lorsque vous configurez les paramètres iOS, ces options s'appliquent uniquement à iOS 5.0 et versions ultérieures ; il n'existe aucune restriction lorsque vous configurez Mac OS X.
  - **Autoriser le déplacement des e-mails entre les comptes** : sélectionnez cette option pour autoriser les utilisateurs à déplacer les messages de ce compte vers un autre compte et à transférer des messages et y répondre à partir d'un autre compte. La valeur par défaut est **OFF**.
  - **N'envoyer des e-mails que depuis l'application de messagerie** : sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS.
  - **Désactiver la synchronisation des e-mails récents** : sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **OFF**. Cette option s'applique uniquement à iOS 6.0 et

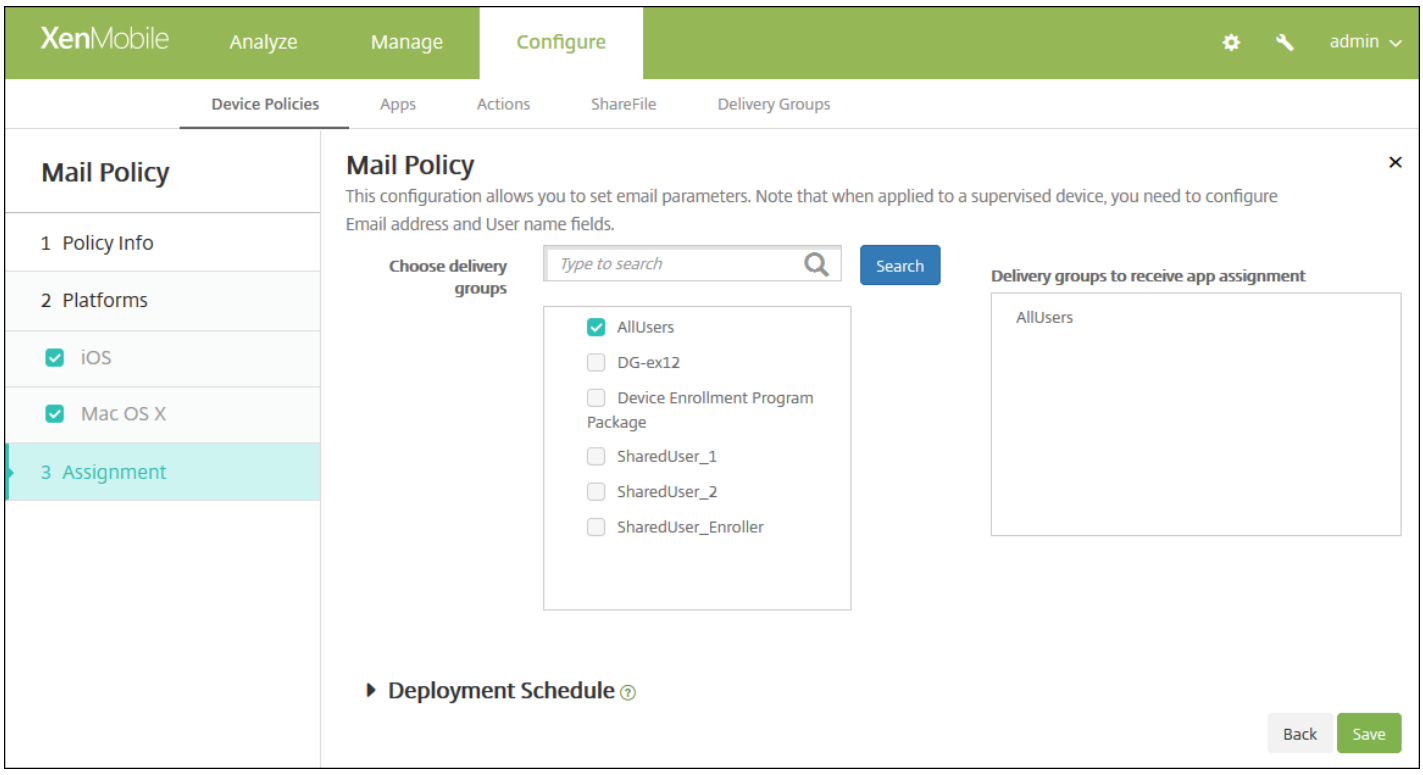
versions ultérieures.

- **Activer S/MIME** : sélectionnez cette option si vous souhaitez que ce compte prenne en charge l'authentification et le chiffrement S/MIME. La valeur par défaut est **OFF**. Lorsque la valeur est définie sur ON, les deux champs suivants apparaissent.
- **Informations d'identification de l'identité de signature** : dans la liste, sélectionnez les informations d'identification de signature à utiliser.
- **Informations d'identification de l'identité de chiffrement** : dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
  - En regard de **Étendue du profil**, dans la liste, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur Mac OS X 10.7 et versions ultérieures.

8. Configurez les règles de déploiement.

9. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de messagerie** s'affiche.



10. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

11. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

12. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

Stratégies de domaines gérés

Feb 23, 2017

Vous pouvez définir des domaines gérés qui s'appliquent à la messagerie et au navigateur Safari. Les domaines gérés vous aident à protéger les données d'entreprise en contrôlant les applications qui peuvent ouvrir des documents téléchargés depuis des domaines à l'aide de Safari. Vous pouvez spécifier des adresses URL ou des sous-domaines pour contrôler la manière dont les utilisateurs peuvent ouvrir des documents, des pièces jointes et des téléchargements à partir du navigateur. Cette stratégie est uniquement prise en charge sur les appareils supervisés iOS 8 et versions ultérieures. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

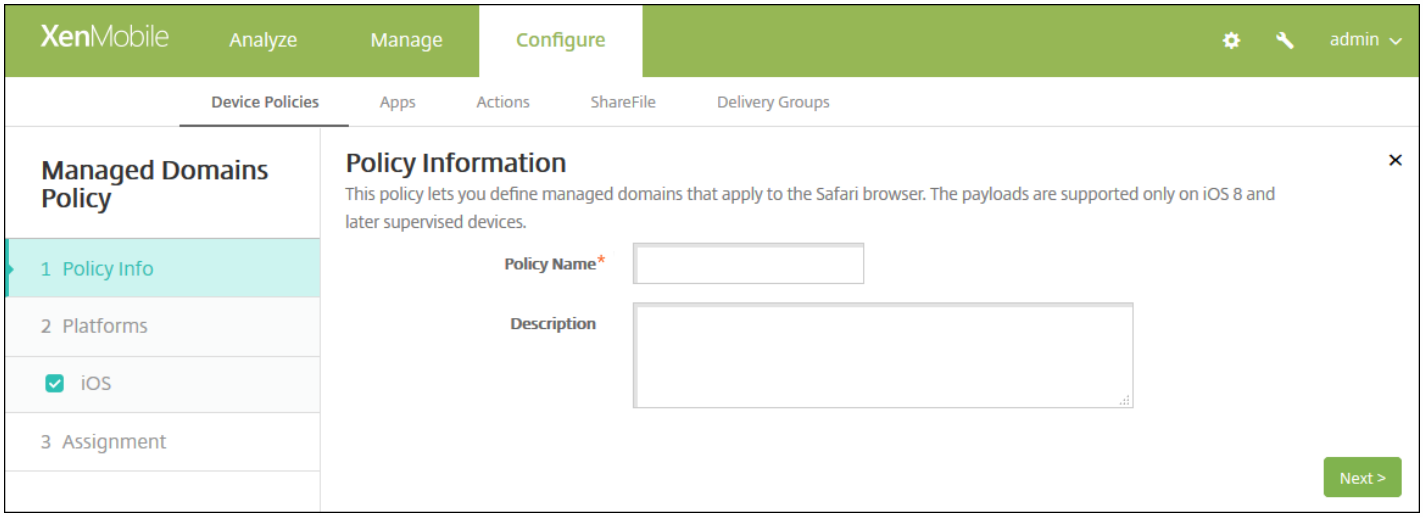
Lorsqu'un utilisateur envoie un e-mail à un destinataire dont le domaine n'est pas sur la liste des domaines de messagerie gérés, un message s'affiche sur l'appareil de l'utilisateur pour l'avertir qu'il envoie un message à un utilisateur en dehors de votre domaine d'entreprise.

Lorsqu'un utilisateur tente d'ouvrir un élément (document, pièce jointe ou téléchargement) à l'aide de Safari depuis un domaine Web se trouvant sur la liste de domaines gérés, l'application d'entreprise appropriée ouvre l'élément. Si l'élément ne provient pas d'un domaine Web se trouvant sur la liste des domaines Web gérés, l'utilisateur ne peut pas ouvrir l'élément avec une application d'entreprise ; il doit utiliser une application non gérée, personnelle.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

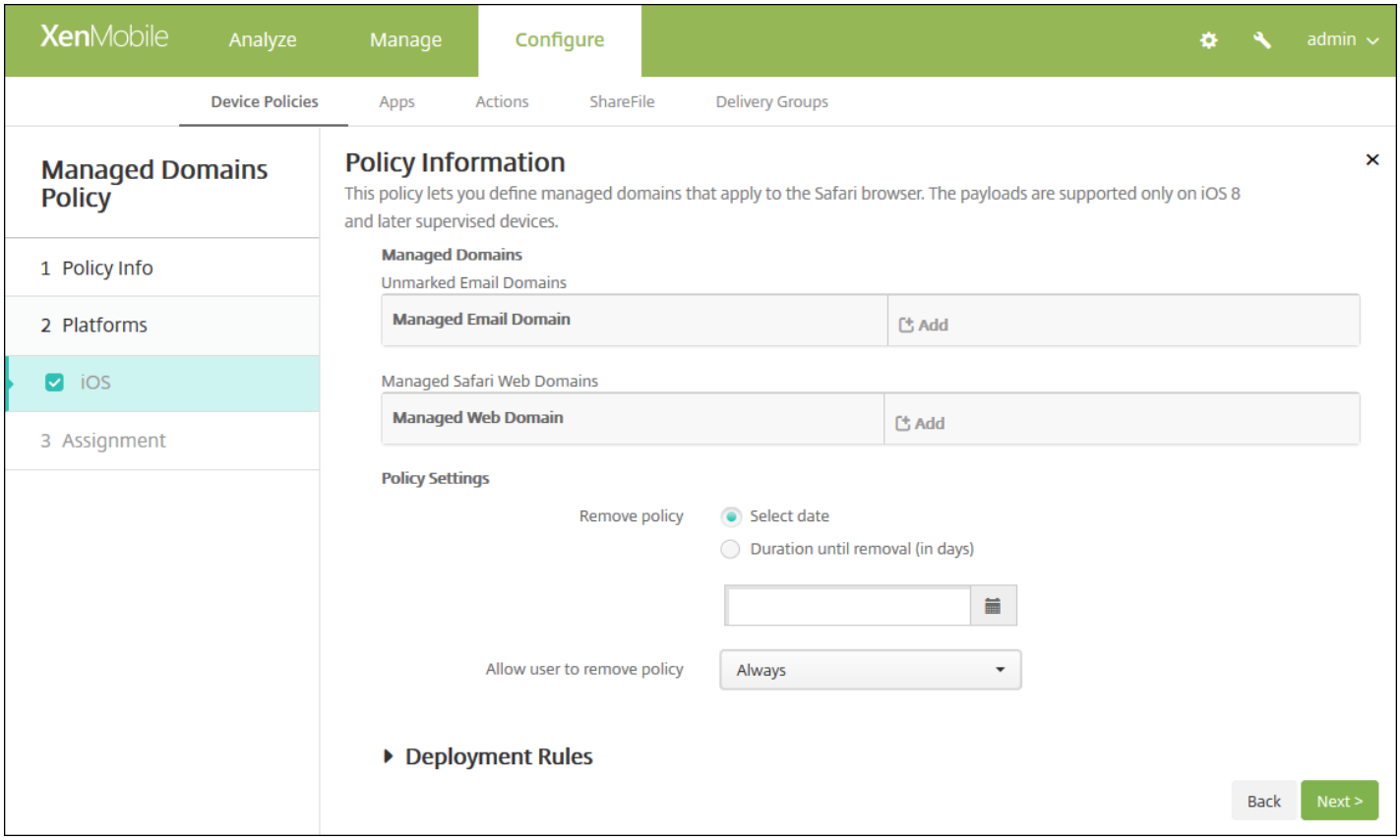
3. Développez **Plus** puis, sous **Sécurité**, cliquez sur **Domaines gérés**. La page d'informations **Stratégies de domaines gérés** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plate-forme iOS** s'affiche.



Comment spécifier les domaines

6. Configurez les paramètres suivants :

- **Domaines gérés**
  - **Domaines de messagerie non marqués** : pour chaque domaine de messagerie à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine de messagerie géré** : entrez le domaine de messagerie.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine de messagerie ou cliquez sur **Annuler** pour ne pas l'enregistrer.
  - **Domaines Web Safari gérés** : pour chaque domaine Web à inclure dans la liste, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Domaine Web géré** : entrez le domaine Web.
    - Cliquez sur **Enregistrer** pour enregistrer le domaine Web ou cliquez sur **Annuler** pour ne pas l'enregistrer.

      Remarque : pour supprimer un domaine existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

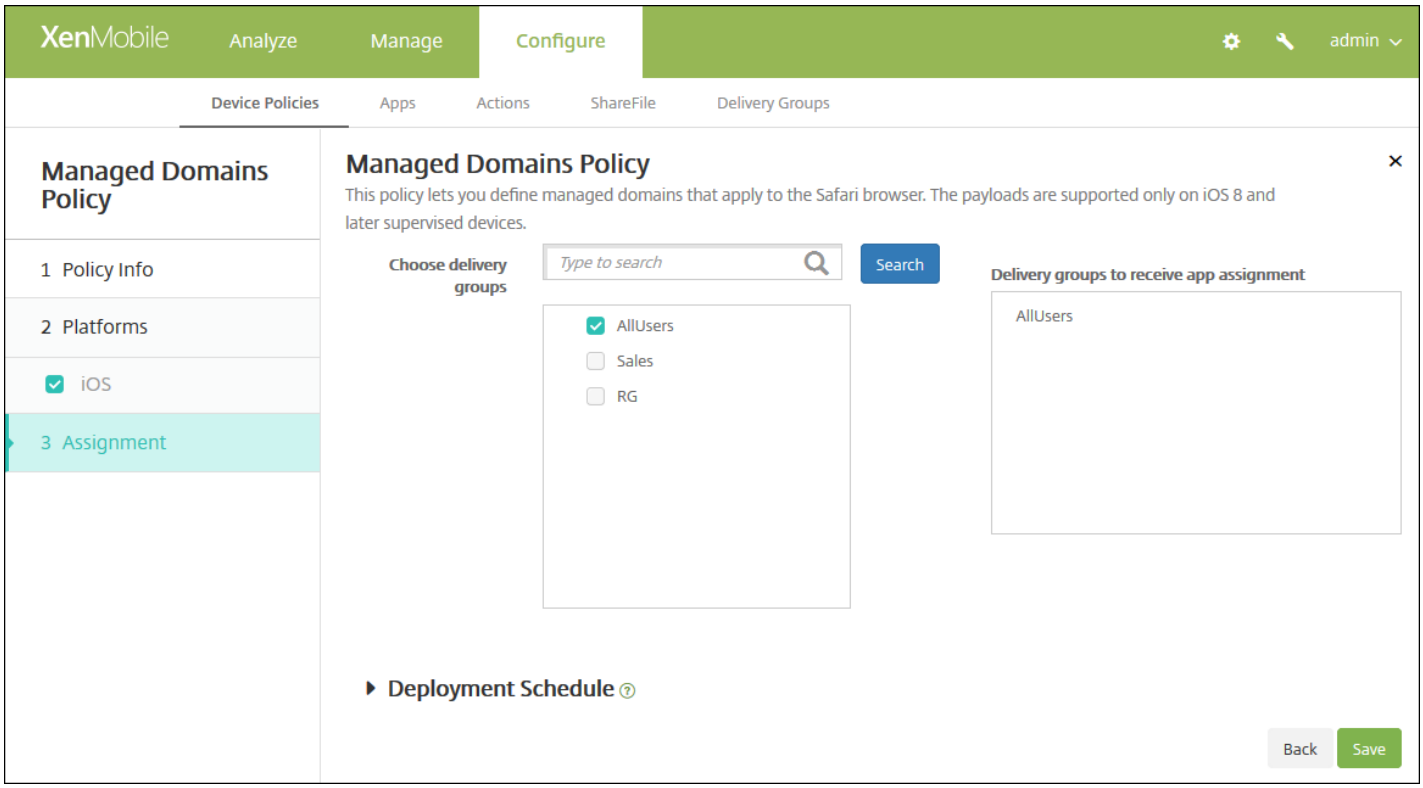
      Pour modifier un domaine, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

- **Paramètres de stratégie**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.

- Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégies de domaines gérés** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez OFF, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est OFF.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.

- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie d'options MDM

Feb 23, 2017

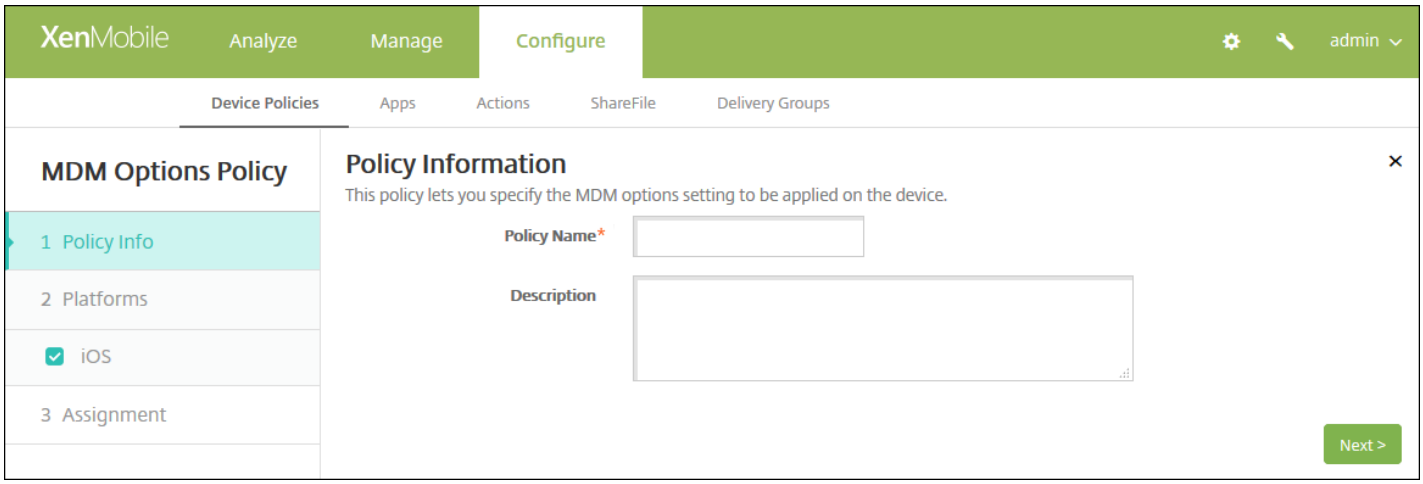
Vous pouvez créer une stratégie d'appareil dans XenMobile pour gérer les fonctions Localiser mon iPhone/Verrouillage d'activation iPad sur les appareils supervisés iOS 7.0 et versions ultérieures. Pour obtenir les instructions sur la définition d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator ou Inscription en bloc iOS.

Le verrouillage d'activation est une fonctionnalité de Localiser mon iPhone/iPad qui est conçue pour empêcher la réactivation des appareils perdus ou volés ; l'ID et le mot de passe Apple de l'utilisateur sont exigés pour désactiver la fonction Localiser mon iPhone, effacer l'appareil ou réactiver et utiliser l'appareil. Dans XenMobile, vous pouvez contourner l'obligation d'entrer ID et mot de passe en activant l'option Verrouillage d'activation dans la stratégie d'options MDM. Lorsqu'un utilisateur renvoie un appareil sur lequel la fonction Localiser mon iPhone est activée, vous pouvez gérer l'appareil à partir de la console XenMobile sans ses informations d'identification Apple.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

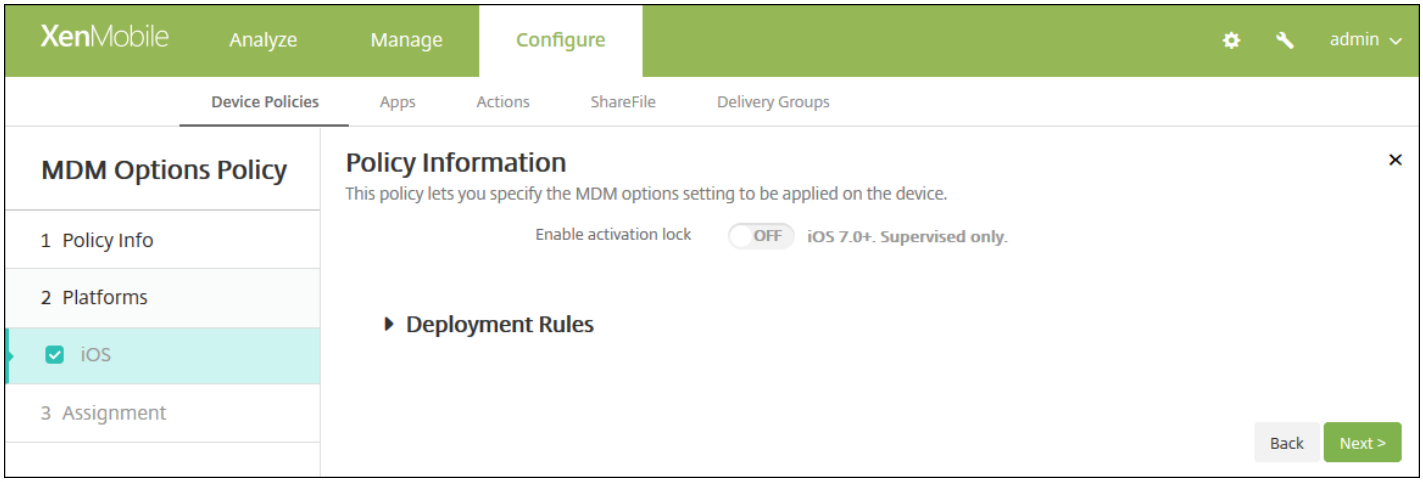
3. Développez **Plus**, puis, sous **Utilisateur final**, cliquez sur **Options MDM**. La page d'informations **Stratégie d'options MDM** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie MDM iOS** s'affiche.

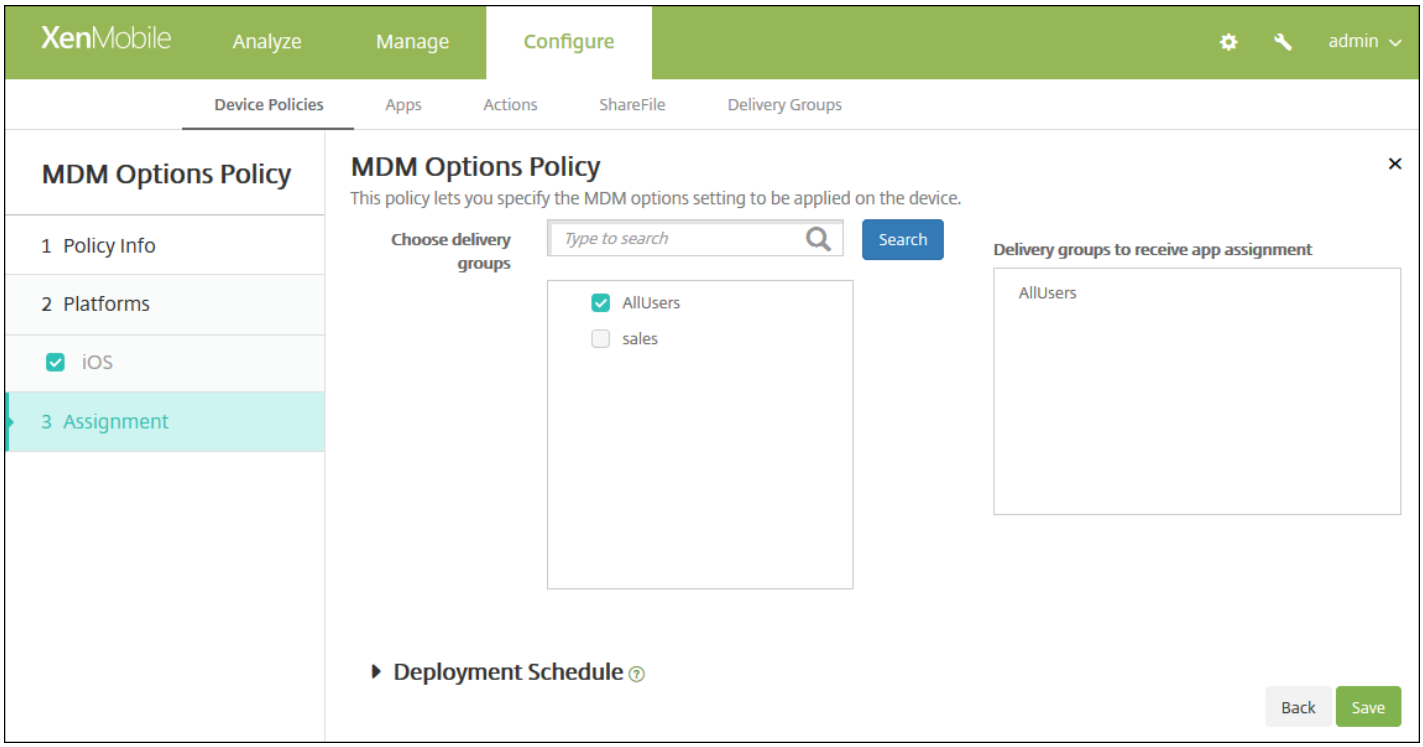


6. Configurez ce paramètre :

- **Activer le verrouillage d'activation** : indiquez si vous souhaitez activer l'option Verrouillage d'activation sur les appareils sur lesquels vous déployez cette stratégie. La valeur par défaut est **OFF**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'options MDM** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies Microsoft Exchange ActiveSync

Feb 23, 2017

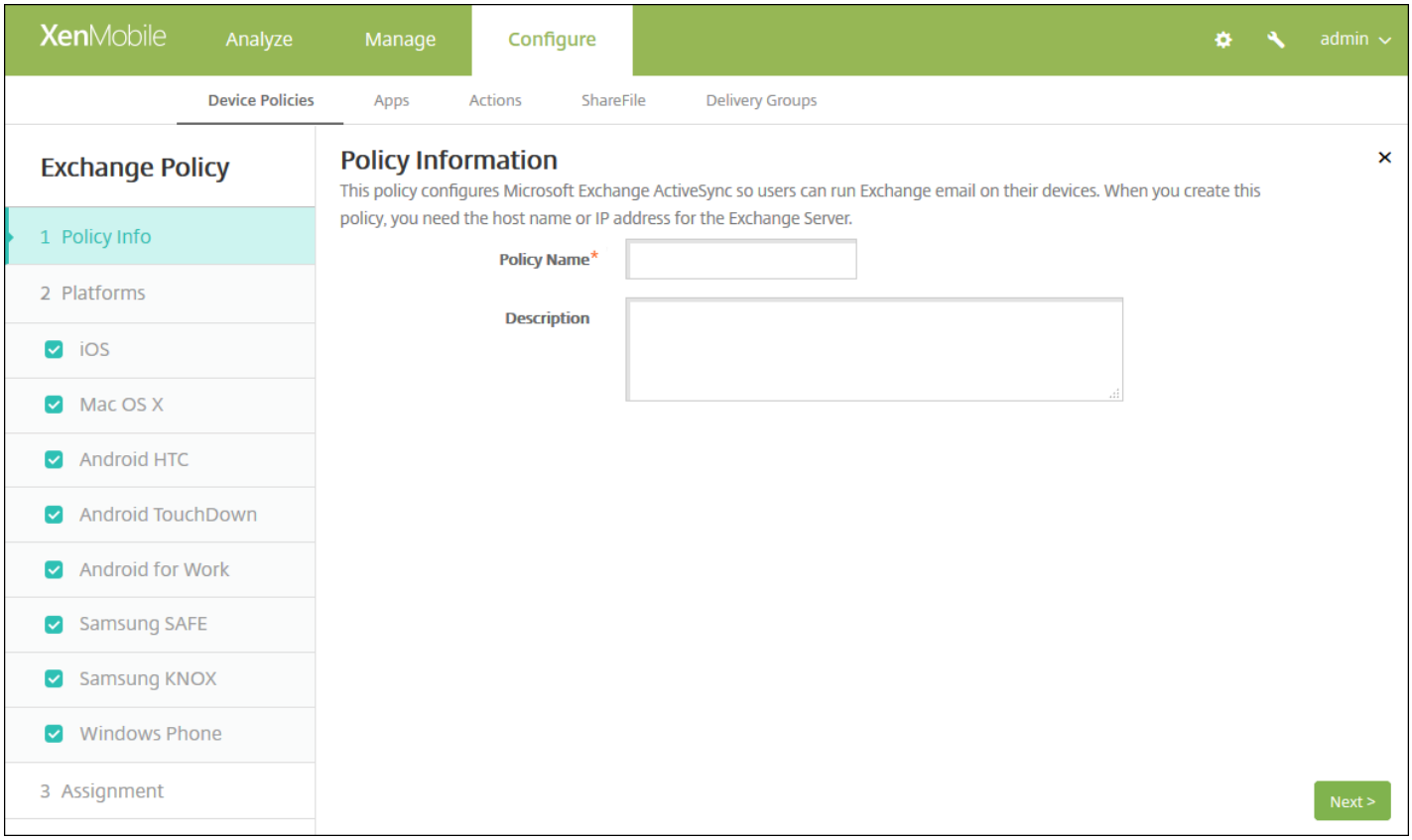
Vous pouvez utiliser la stratégie Exchange ActiveSync pour configurer un client de messagerie sur les appareils des utilisateurs pour leur permettre d'accéder à leur messagerie d'entreprise hébergée sur Exchange. Vous pouvez créer des stratégies pour iOS, Mac OS X, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX et Windows Phone. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans les sections suivantes.

Avant de pouvoir créer cette stratégie, vous devez connaître le nom d'hôte ou l'adresse IP du serveur Exchange.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Exchange**. La page d'informations **Stratégie Exchange** s'affiche.



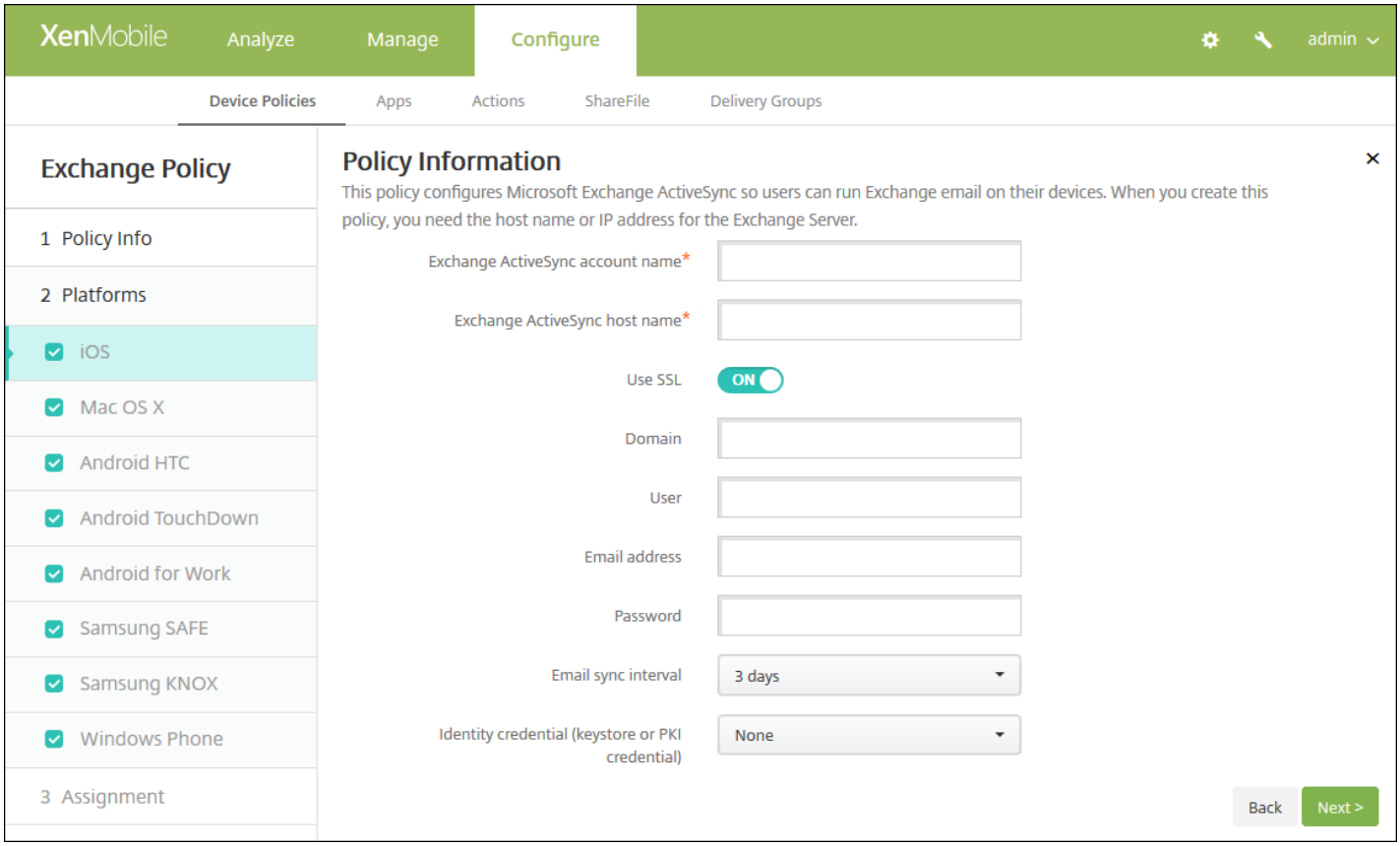
4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS



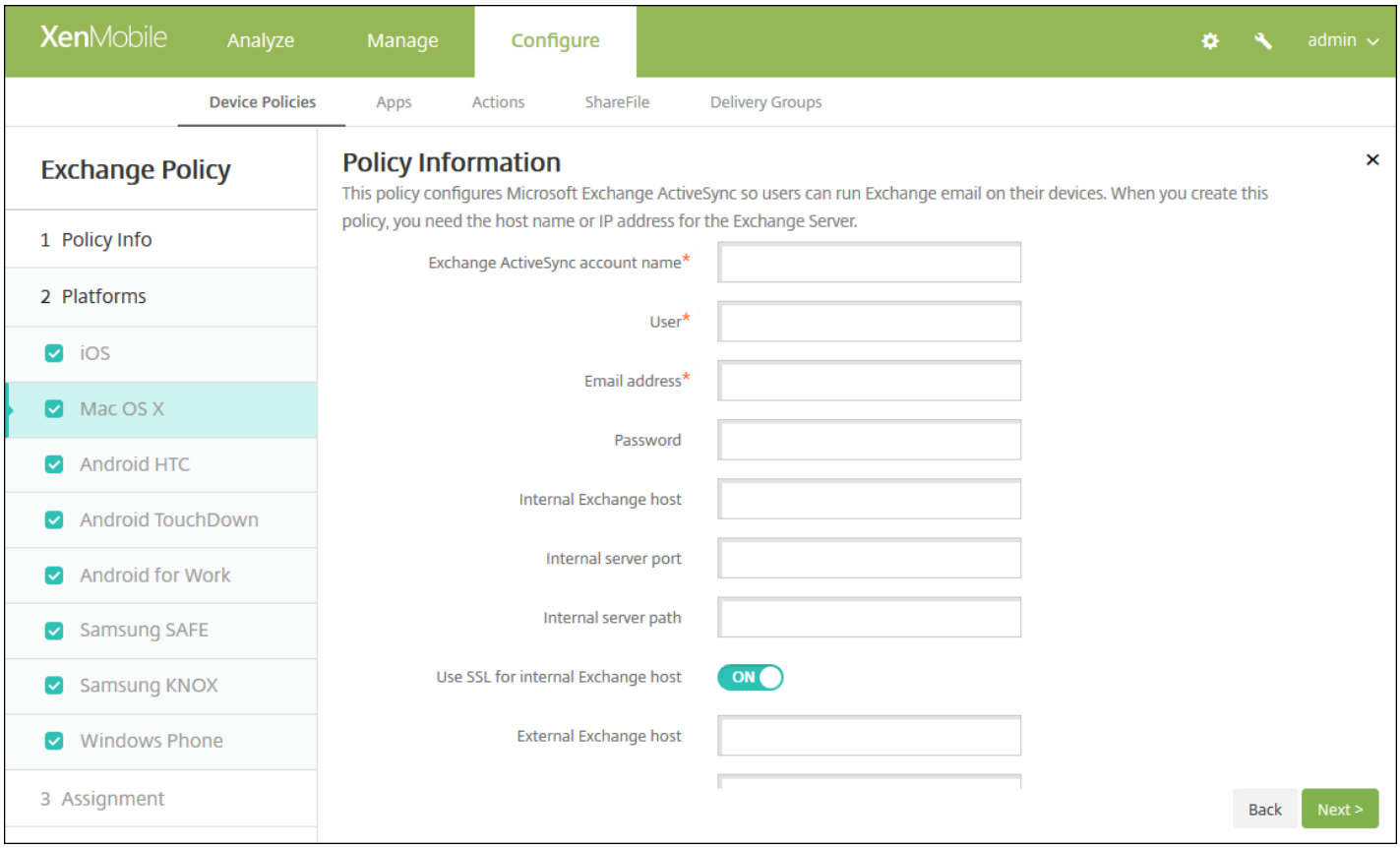
Pour configurer ces paramètres :

- **Nom du compte Exchange ActiveSync** : entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Nom d'hôte Exchange ActiveSync** : entrez l'adresse du serveur de messagerie.
- **Utiliser SSL** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **ON**.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **Utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Intervalle de synchronisation des e-mails** : dans la liste, choisissez la fréquence de synchronisation des e-mails avec Exchange Server. La valeur par défaut est **3 jours**.
- **Infos d'identification de l'identité (PKI ou keystore)** : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucune**.
- **Autoriser le déplacement des e-mails entre les comptes** : sélectionnez cette option pour autoriser les utilisateurs à déplacer les messages de ce compte vers un autre compte et à transférer des messages et y répondre à partir d'un autre compte. La valeur par défaut est **OFF**.
- **N'envoyer le courrier que depuis l'application de messagerie** : sélectionnez cette option si vous voulez que les utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS. La valeur par défaut

est **OFF**.

- **Désactiver la synchronisation des courriers récents** : sélectionnez cette option pour empêcher les utilisateurs de synchroniser les adresses récentes. La valeur par défaut est **OFF**. Cette option s'applique uniquement à iOS 6.0 et versions ultérieures.
- **Activer S/MIME** : sélectionnez cette option si vous souhaitez que ce compte prenne en charge l'authentification et le chiffrement S/MIME. La valeur par défaut est **OFF**. Lorsque la valeur est définie sur **ON**, les deux champs suivants apparaissent :
  - **Informations d'identification de l'identité de signature**. La valeur par défaut est **Aucune**.
  - **Informations d'identification de l'identité de chiffrement**. La valeur par défaut est **Aucune**.
- **Activer commutateur de chiffrement S/MIME par message** : sélectionnez cette option pour autoriser les utilisateurs à crypter les e-mails sortants message par message. La valeur par défaut est **OFF**.

Configurer les paramètres pour Mac OS X



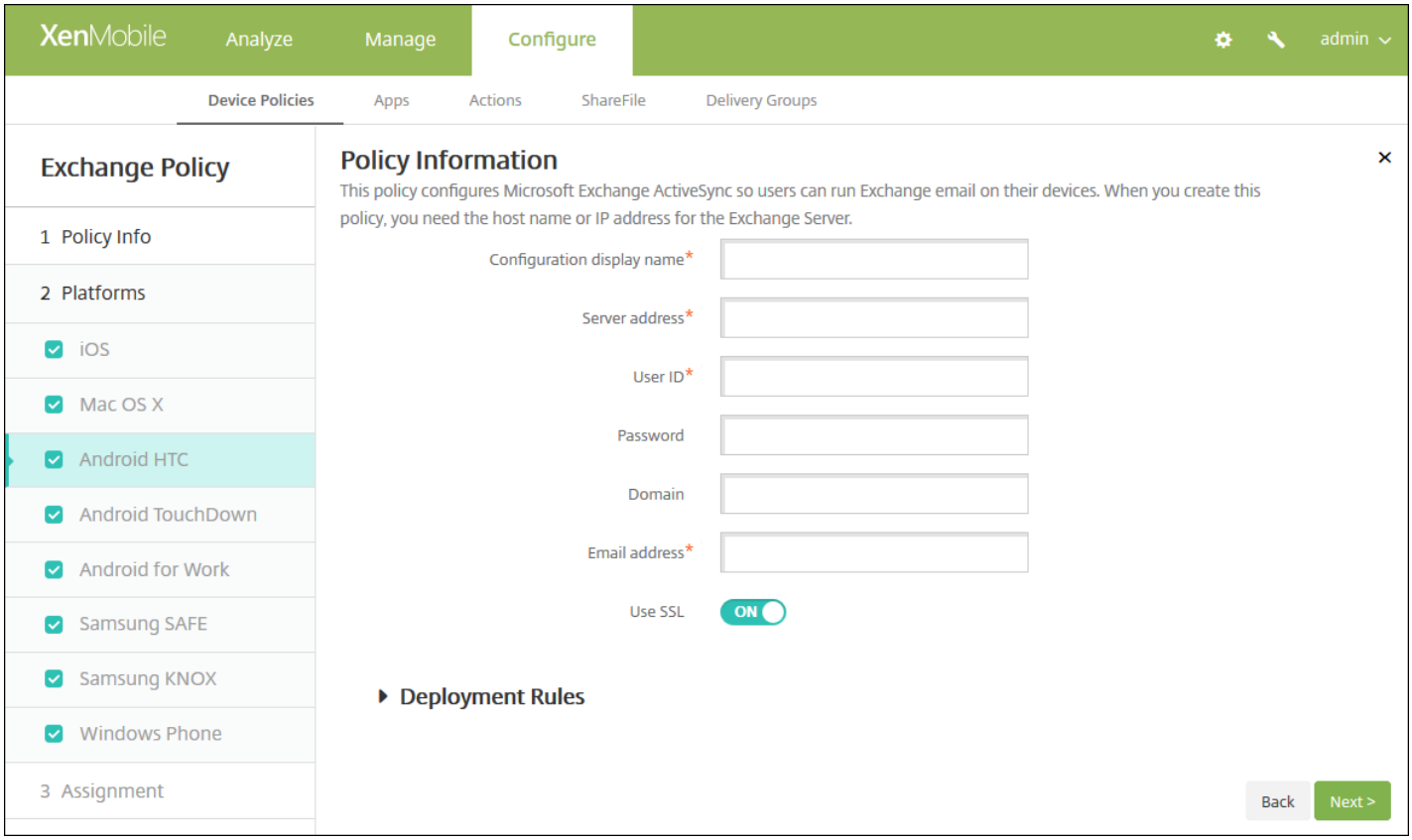
Pour configurer ces paramètres :

- **Nom du compte Exchange ActiveSync** : entrez la description du compte de messagerie qui est affichée sur les appareils des utilisateurs.
- **Utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Hôte Exchange interne** : si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un

nom d'hôte Exchange interne (facultatif).

- **Port du serveur interne** : si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange interne (facultatif).
- **Chemin d'accès au serveur interne** : si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange interne (facultatif).
- **Utiliser SSL pour l'hôte Exchange interne** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **ON**.
- **Hôte Exchange externe** : si vous voulez que vos noms d'hôte Exchange interne et externe soient différents, tapez un nom d'hôte Exchange externe (facultatif).
- **Port du serveur externe** : si vous voulez que vos ports de serveur Exchange interne et externe soient différents, tapez un numéro de port Exchange externe (facultatif).
- **Chemin d'accès au serveur externe** : si vous voulez que vos chemins d'accès au serveur Exchange interne et externe soient différents, tapez un chemin d'accès au serveur Exchange externe (facultatif).
- **Utiliser SSL pour l'hôte Exchange externe** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et l'hôte Exchange interne. La valeur par défaut est **ON**.
- **Autoriser Mail Drop** : sélectionnez cette option pour permettre aux utilisateurs de partager sans fil des fichiers entre deux Mac, sans avoir à se connecter à un réseau existant. La valeur par défaut est **OFF**.

Configurer les paramètres pour Android HTC



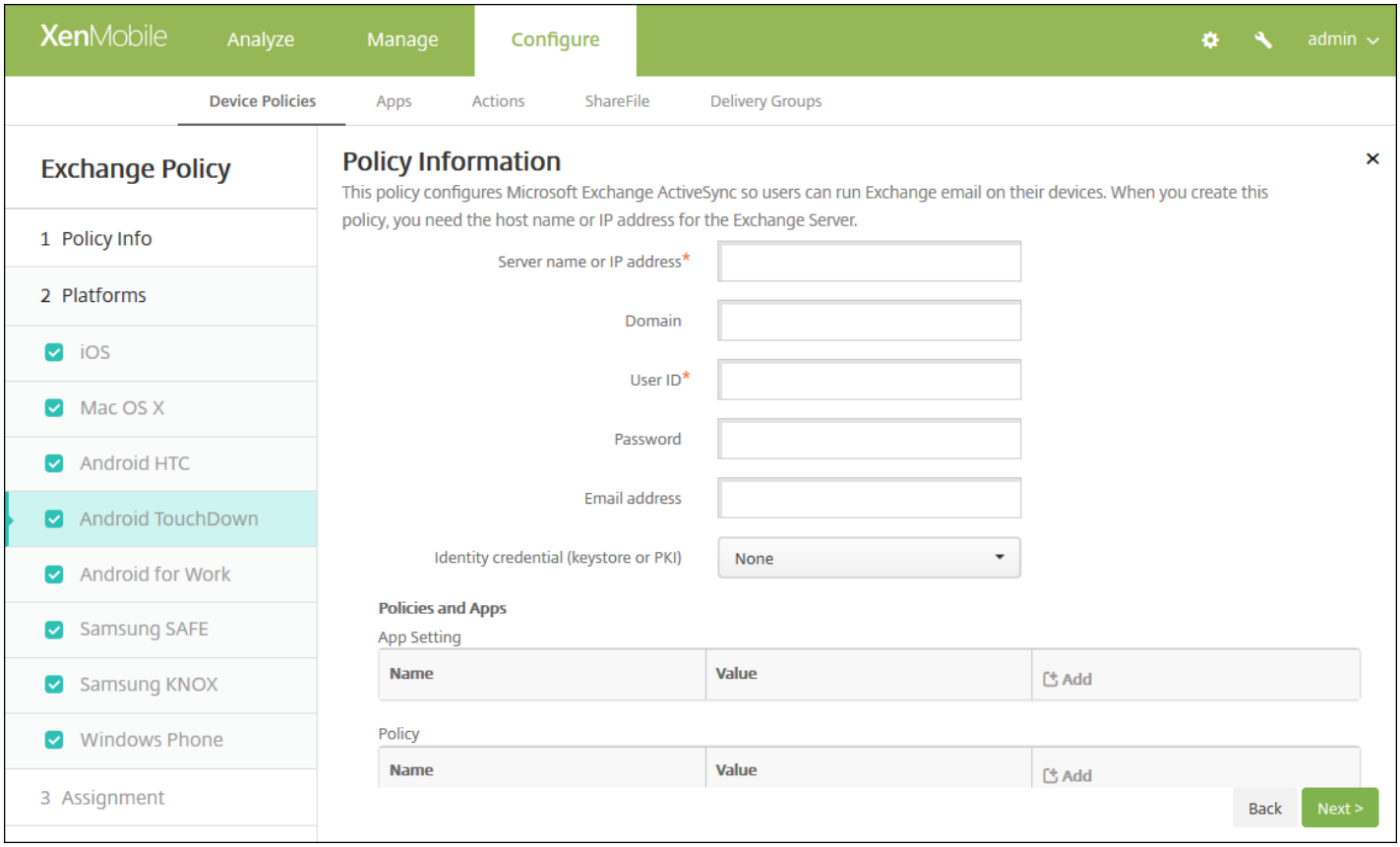
Pour configurer ces paramètres :

- **Nom d'affichage de la configuration** : entrez le nom de cette stratégie qui s'affiche sur les appareils des utilisateurs.
- **Adresse du serveur** : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **ID utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username}

dans ce champ pour rechercher automatiquement les noms d'utilisateurs.

- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser SSL** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **ON**.

Configurer les paramètres pour Android TouchDown

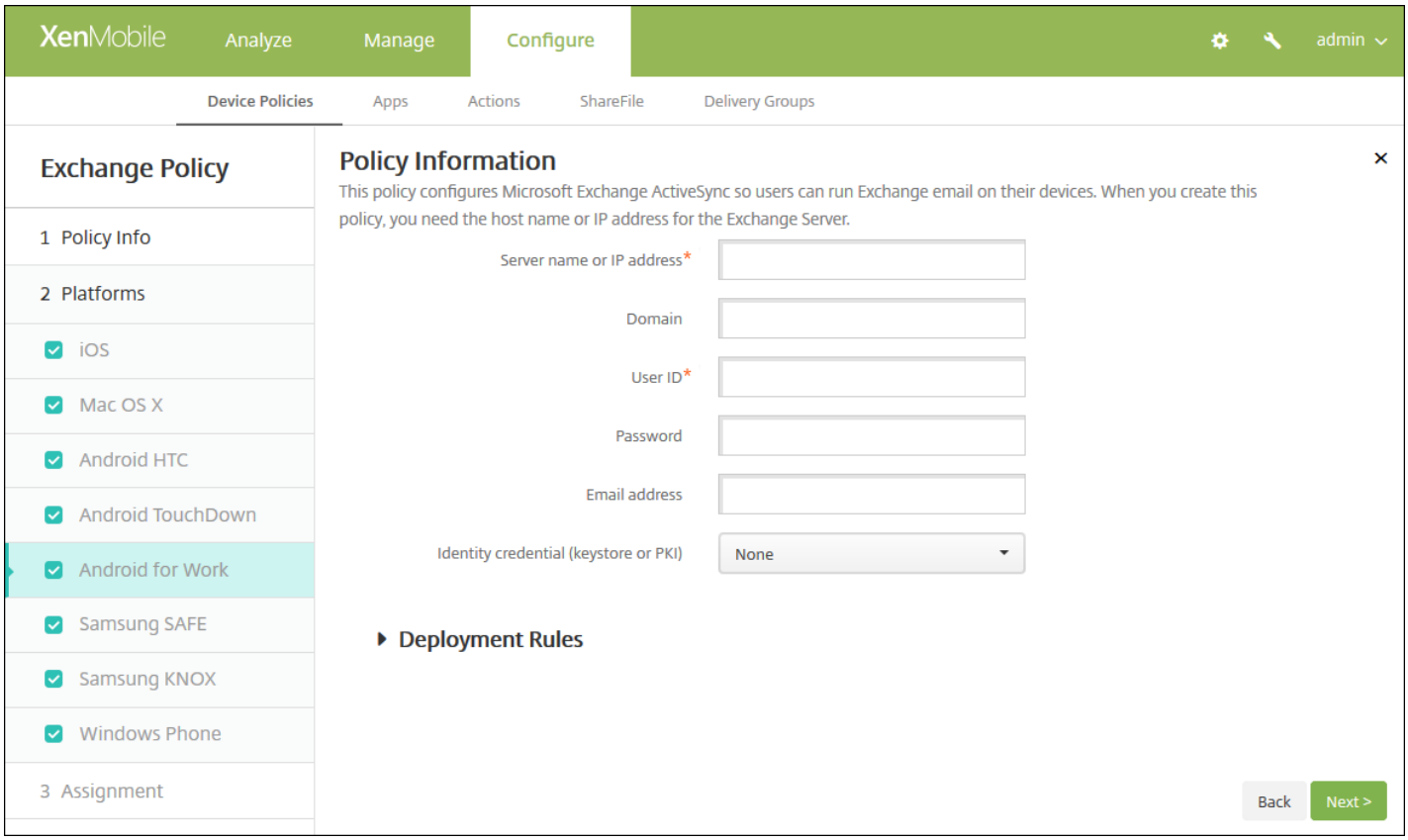


Pour configurer ces paramètres :

- **Nom du serveur ou adresse IP** : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Infos d'identification de l'identité (PKI ou keystore)** : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucune**.

- **Paramètre applicatif** : si vous le souhaitez, ajoutez des paramètres applicatifs TouchDown pour cette stratégie.
- **Stratégie** : si vous le souhaitez, ajoutez des stratégies TouchDown pour cette stratégie.

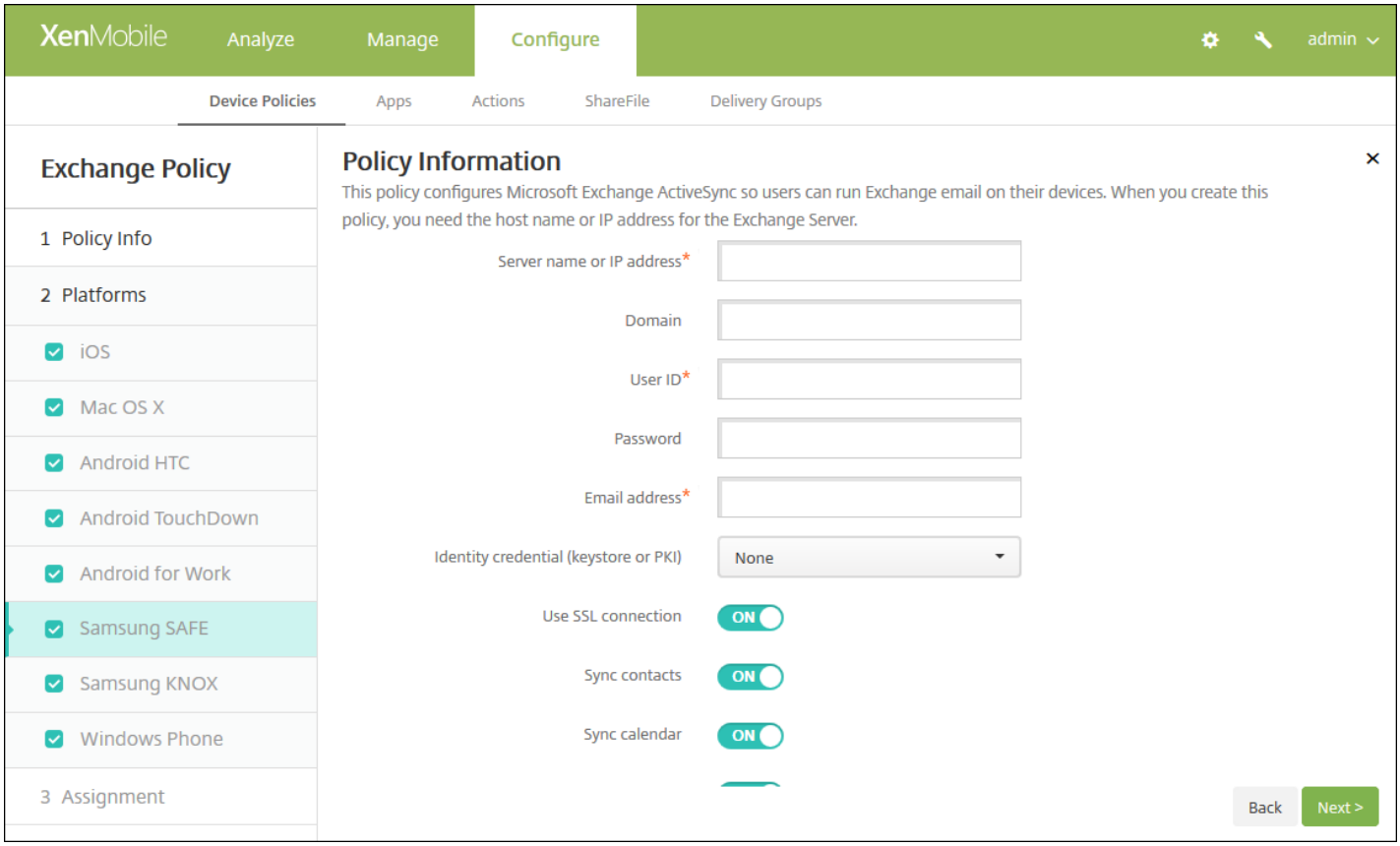
Configurer Android for Work



Pour configurer ces paramètres :

- **Nom du serveur ou adresse IP** : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Infos d'identification de l'identité (PKI ou keystore)** : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client. La valeur par défaut est **Aucune**.

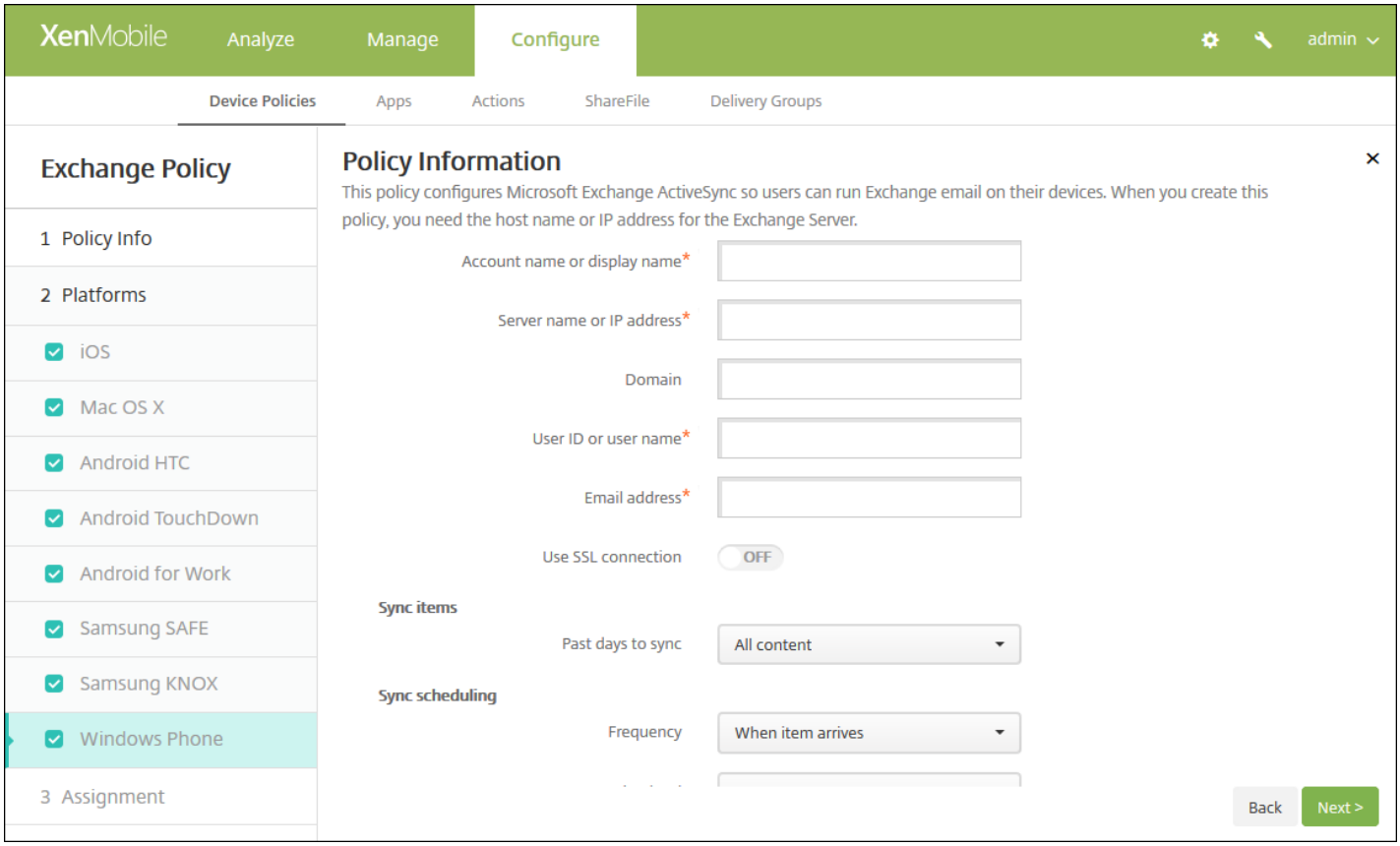
Configurer les paramètres Samsung SAFE et Samsung KNOX



Pour configurer ces paramètres :

- **Nom du serveur ou adresse IP** : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Mot de passe** : entrez un mot de passe pour le compte utilisateur Exchange.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Infos d'identification de l'identité (PKI ou keystore)** : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client.
- **Utiliser une connexion SSL** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **ON**.
- **Synchroniser les contacts** : sélectionnez cette option pour activer la synchronisation des contacts des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est **ON**.
- **Synchroniser le calendrier** : sélectionnez cette option pour activer la synchronisation des calendriers des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est **ON**.
- **Compte par défaut** : sélectionnez cette option pour faire du compte Exchange des utilisateurs le compte par défaut pour l'envoi de courrier électronique à partir de leurs appareils. La valeur par défaut est **ON**.

Configurer les paramètres pour Windows Phone



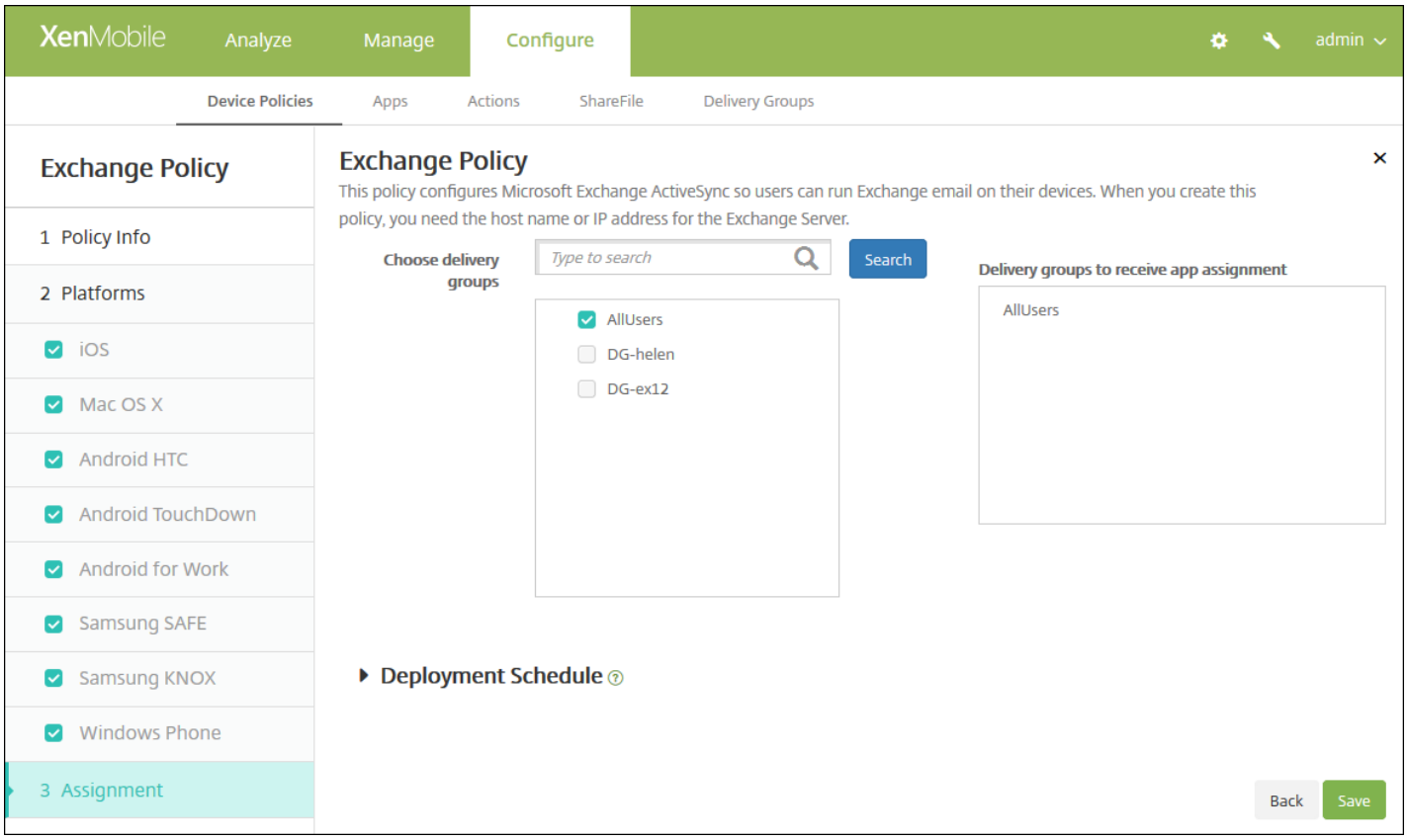
Pour configurer ces paramètres :

Remarque : cette stratégie ne vous permet pas de définir le mot de passe utilisateur. Les utilisateurs doivent définir ce paramètre à partir de leurs appareils après transmission de la stratégie.

- **Nom du compte ou nom d'affichage** : entrez le nom du compte Exchange ActiveSync.
- **Nom du serveur ou adresse IP** : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.
- **Domaine** : entrez le domaine dans lequel réside le serveur Exchange. Vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
- **ID utilisateur ou nom d'utilisateur** : spécifiez le nom d'utilisateur du compte utilisateur Exchange. Vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateurs.
- **Adresse e-mail** : spécifiez l'adresse e-mail complète de l'utilisateur. Vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.
- **Utiliser une connexion SSL** : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est **OFF**.
- **Contenu à synchroniser** : dans la liste, cliquez sur le nombre de jours à prendre en compte pour synchroniser tout le contenu de l'appareil avec le serveur Exchange. Le paramètre par défaut est **Tout le contenu**.
- **Périodicité** : dans la liste, cliquez sur le calendrier à utiliser lors de la synchronisation des données envoyées à partir du serveur Exchange. La valeur par défaut est **À la réception d'un e-mail**.
- **Niveau d'enregistrement** : dans la liste, cliquez sur **Désactivé**, **De base** ou **Avancé** pour spécifier le niveau de détail lors de la journalisation des activités Exchange. La valeur par défaut est **Désactivé**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie Exchange** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie d'informations sur l'organisation

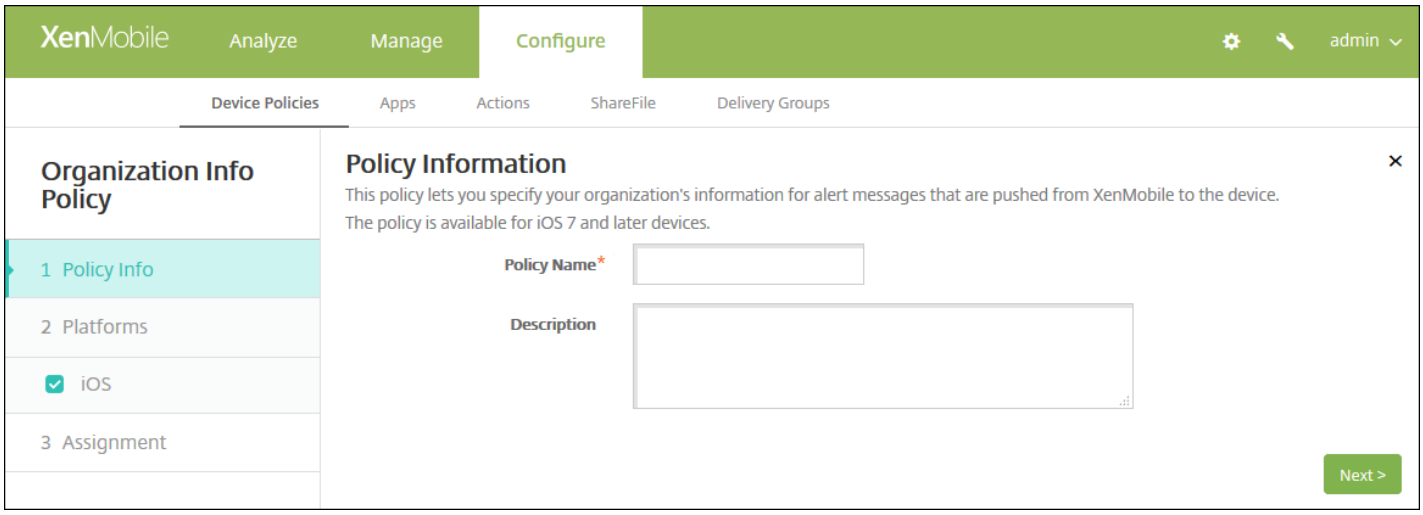
Feb 23, 2017

Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin de spécifier les coordonnées de votre organisation à utiliser pour envoyer les messages d'alerte qui sont transmis depuis XenMobile vers les appareils iOS. La stratégie est disponible pour iOS 7 et versions ultérieures.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

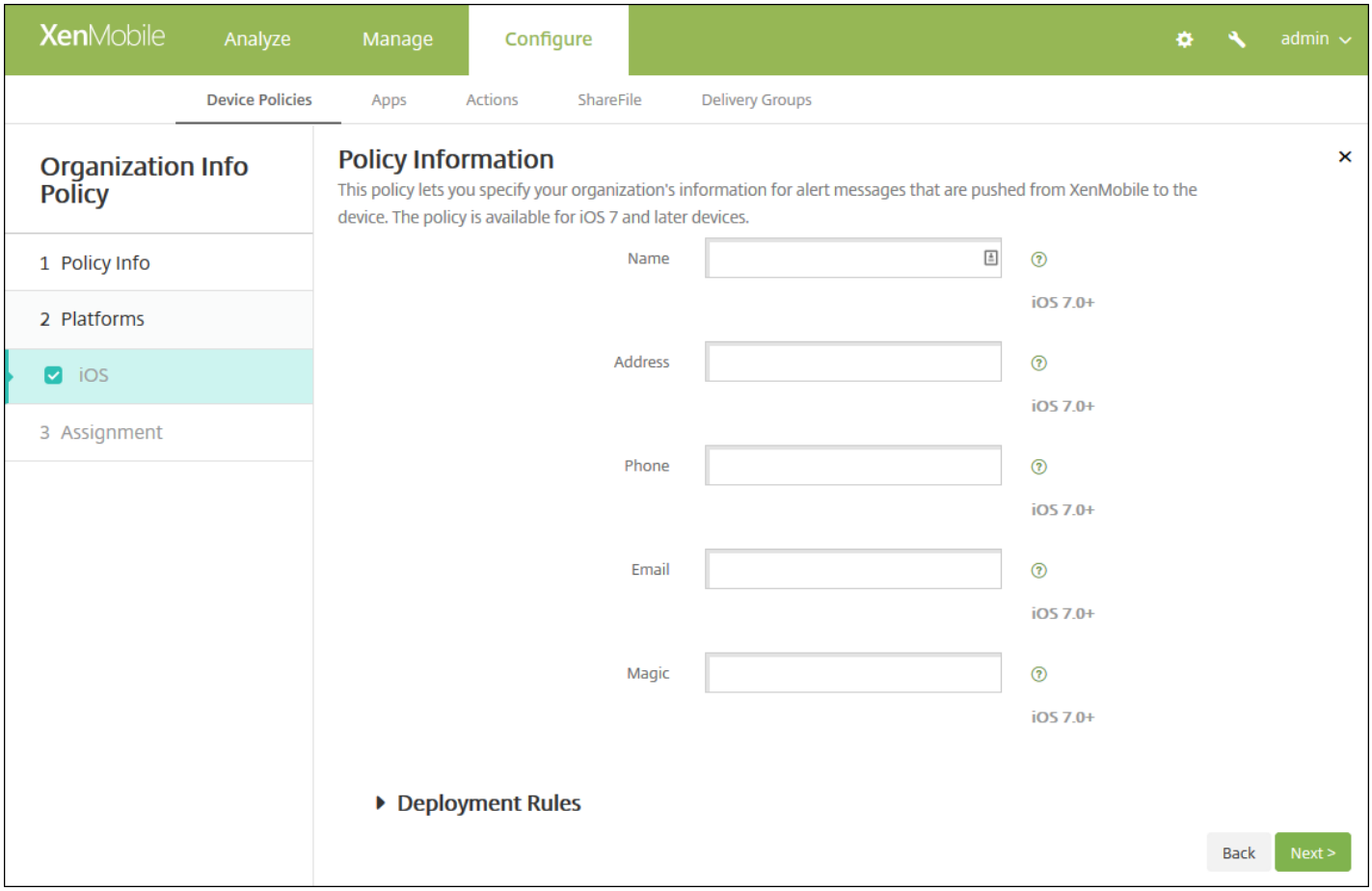
3. Cliquez sur **Plus**, puis, sous **Utilisateur final**, cliquez sur **Info organisation**. La page **Stratégie d'informations sur l'organisation** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Informations sur la plate-forme iOS** s'affiche.

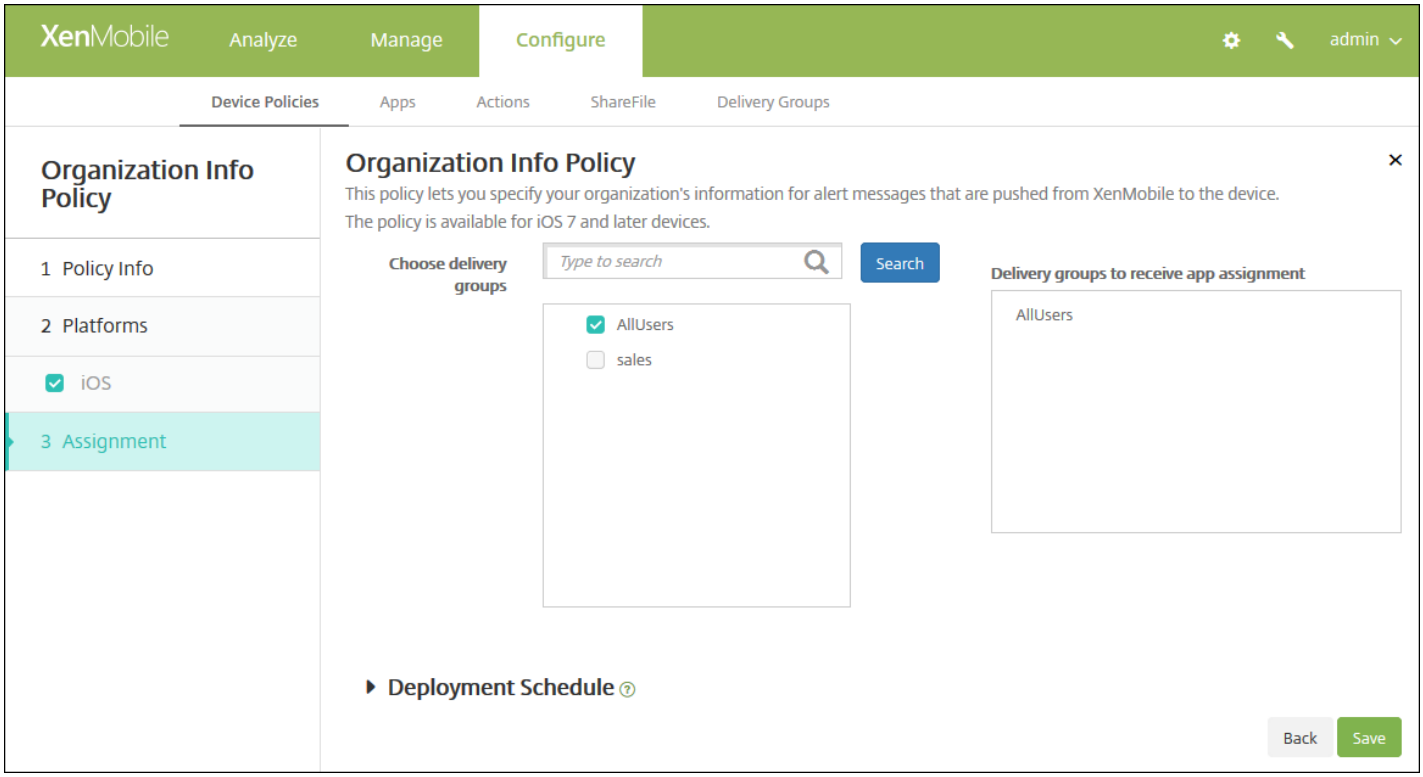


Pour configurer ces paramètres :

- **Nom** : entrez le nom de l'organisation exécutant XenMobile.
- **Adresse** : entrez l'adresse de l'organisation.
- **Téléphone** : entrez le numéro de téléphone d'assistance de l'organisation.
- **Adresse électronique** : entrez l'adresse e-mail d'assistance.
- **Magic** : entrez un mot ou une phrase décrivant les services gérés par l'organisation.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie d'informations sur l'organisation** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de code secret

Feb 23, 2017

Vous créez une stratégie de code secret dans XenMobile en fonction des normes de votre organisation. Vous pouvez exiger la saisie de codes secrets sur les appareils des utilisateurs et définir diverses règles de code secret et de formatage. Vous pouvez créer des stratégies pour iOS, Mac OS X, Android, Samsung KNOX, Android for Work, Windows Phone et Windows Desktop/Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Paramètres iOS

Paramètres Mac OS X

Paramètres Android

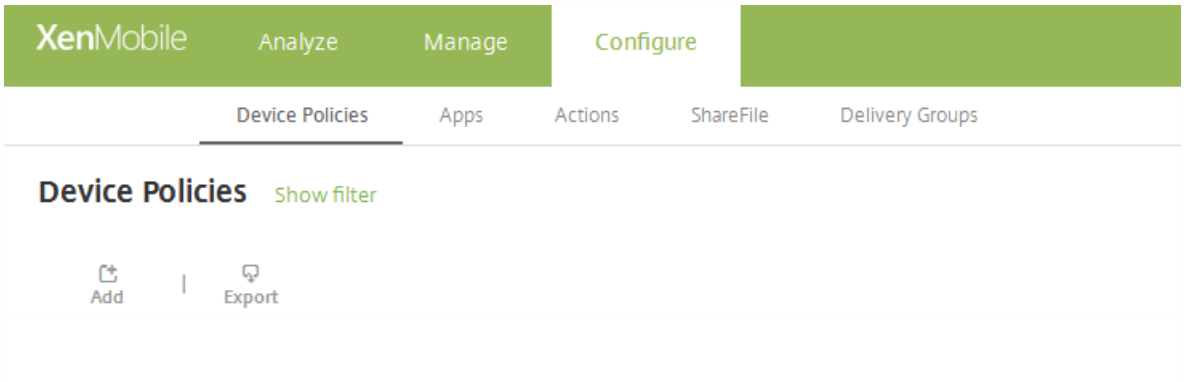
Paramètres Samsung KNOX

Paramètres Android for Work

Paramètres Windows Phone

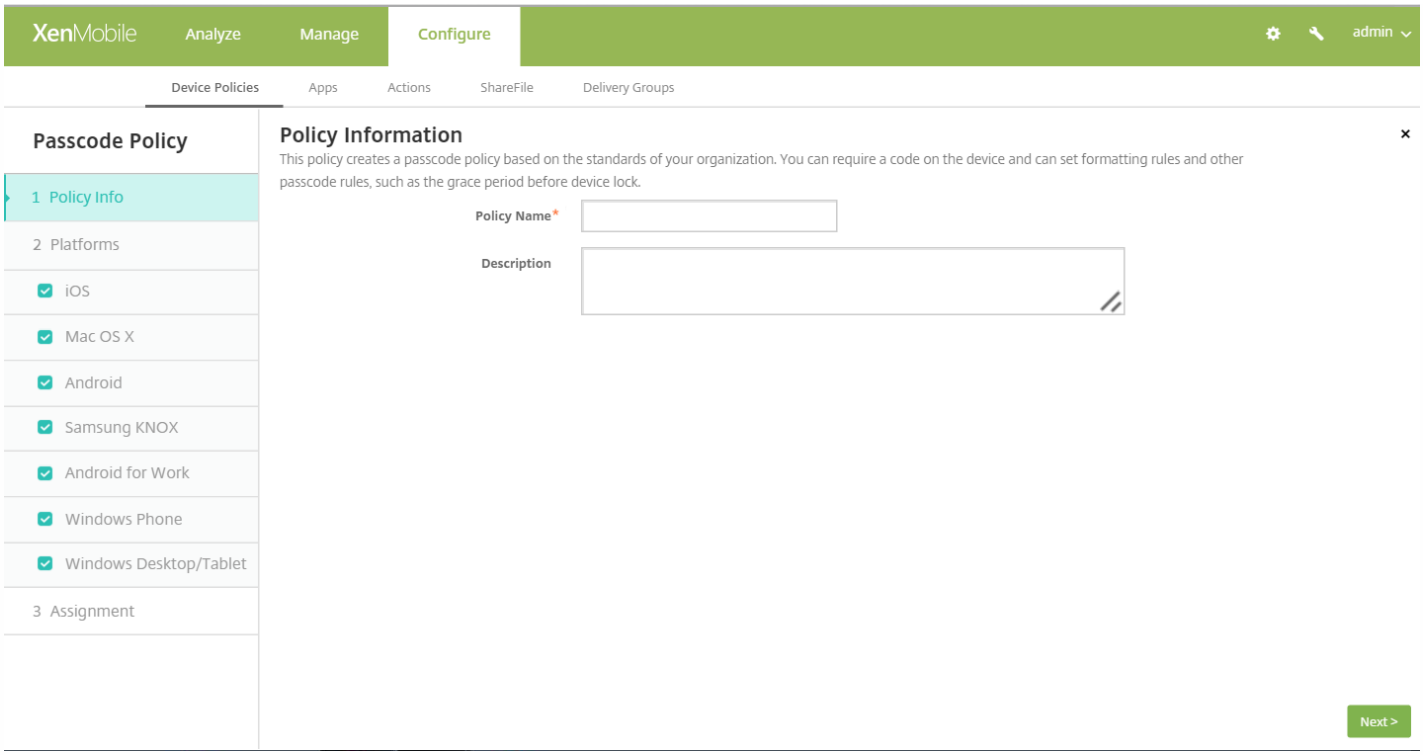
Paramètres Windows Desktop/Tablet

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.



2. Cliquez sur **Ajouter**. La page Ajouter une nouvelle stratégie apparaît.

3. Cliquez sur **Code secret**. La page d'informations Stratégie de code secret s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

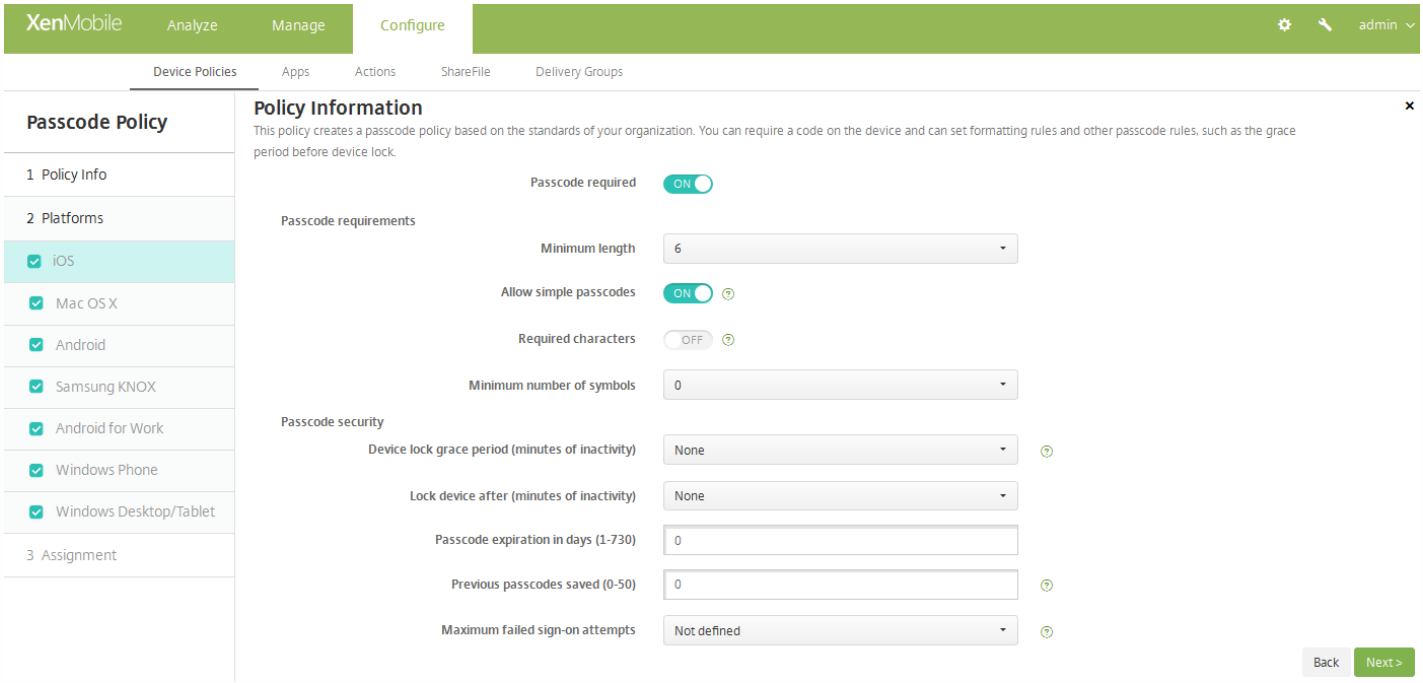
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS

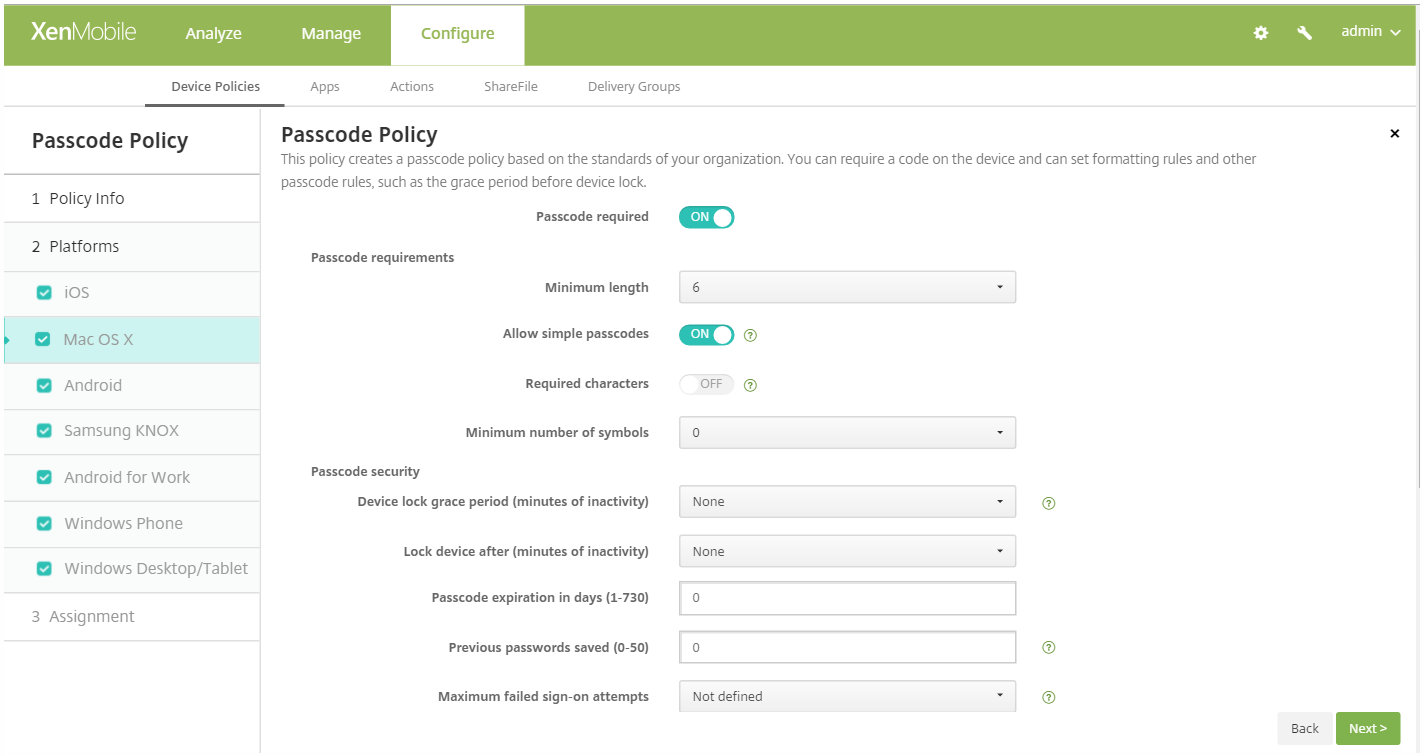


Configurez les paramètres suivants :

- **Code secret requis** : sélectionnez cette option pour exiger la saisie d'un code secret et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est **6**.
  - **Autoriser les codes secrets simples** : sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **ON**.
  - **Caractères requis** : sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **OFF**.
  - **Nombre minimum de symboles** : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **Période de grâce avant verrouillage de l'appareil (minutes d'inactivité)** : dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est **Aucune**.
  - **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est Aucune.
  - **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil subit un effacement complet. La valeur par défaut est **Aucun nombre défini**.
- **Paramètres de stratégie**

- En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
- Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Mac OS X



Pour configurer ces paramètres :

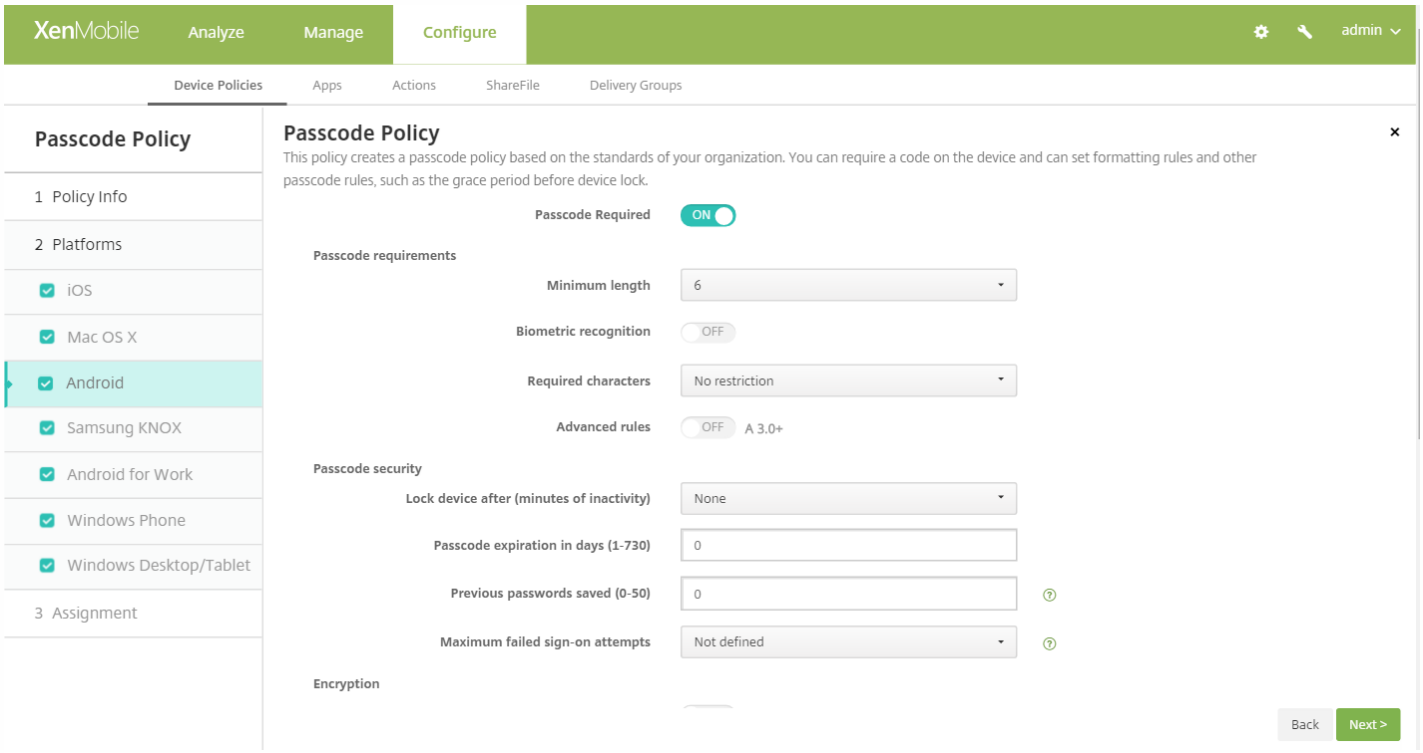
- **Code secret requis** : sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.
- Si vous n'activez pas **Code secret requis**, en regard de **Délai après les échecs de tentatives de connexion, en minutes**, entrez le nombre de minutes après lesquelles les utilisateurs peuvent retenter de saisir leur code secret.
- Si vous activez **Code secret requis**, configurez les paramètres suivants :
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
  - **Autoriser les codes secrets simples** : sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est **ON**.
  - **Caractères requis** : sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est **OFF**.
  - **Nombre minimum de symboles** : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **Période de grâce avant verrouillage de l'appareil (minutes d'inactivité)** : dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est

Aucune.

- **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.
- **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Nombre maximum de tentatives de connexion infructueuses** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est verrouillé. La valeur par défaut est **Aucun nombre défini**.
- **Délai après les échecs de tentatives de connexion, en minutes** : entrez le nombre de minutes après lesquelles les utilisateurs peuvent retenter de saisir leur code secret.

- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.
  - Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
  - Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
  - Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.
  - En regard de **Étendue du profil**, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.

Configurer les paramètres pour Android



Pour configurer ces paramètres :

Remarque : le paramètre par défaut pour Android est **OFF**.

- **Code secret requis** : sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour Android. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité du code secret, chiffrement et Samsung SAFE.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est 6.
  - **Reconnaissance biométrique** : sélectionnez cette option pour activer la reconnaissance biométrique. Si vous activez cette option, le champ Caractères requis est masqué. La valeur par défaut est **OFF**.
  - **Caractères requis** : dans la liste, cliquez sur Aucune restriction, Chiffres et lettres, Chiffres uniquement ou Lettres uniquement pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est Aucune restriction.
  - **Règles avancées** : sélectionnez cette option si vous souhaitez appliquer des règles de code secret avancées. Cette option est disponible pour Android 3.0 et versions ultérieures. La valeur par défaut est **OFF**.
  - Lorsque le paramètre **Règles avancées** est activé, à partir de chacune des listes suivantes et pour chaque type de caractère, cliquez sur le nombre minimal de caractère qu'un code secret doit contenir :
    - **Symboles** : nombre minimal de symboles.
    - **Lettres** : nombre minimal de lettres.
    - **Minuscules** : nombre minimum de minuscules.
    - **Majuscules** : nombre minimum de majuscules.
    - **Chiffres ou symboles** : nombre minimal de chiffres ou de symboles.
    - **Chiffres** : nombre minimal de chiffres.
- **Sécurité des codes secrets**
  - **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.
  - **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Nombre maximum de tentatives de connexion infructueuses** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est effacé. La valeur par défaut est **Aucun nombre défini**.
- **Chiffrement**
  - **Activer le chiffrement** : sélectionnez cette option si vous souhaitez activer le cryptage. Cette option est disponible pour Android 3.0 et versions ultérieures. L'option est disponible, que le paramètre **Code secret requis** soit sélectionné ou non.

    Remarque : pour crypter leurs appareils, les utilisateurs doivent commencer avec une batterie chargée et laisser l'appareil branché pendant le délai nécessaire au cryptage, une heure au minimum. Si le processus de cryptage est interrompu, les utilisateurs risquent de perdre certaines ou toutes les données de leurs appareils. Une fois qu'un appareil est crypté, le processus ne peut pas être annulé sauf en effectuant une réinitialisation d'usine, ce qui entraîne la suppression de toutes les données de l'appareil.

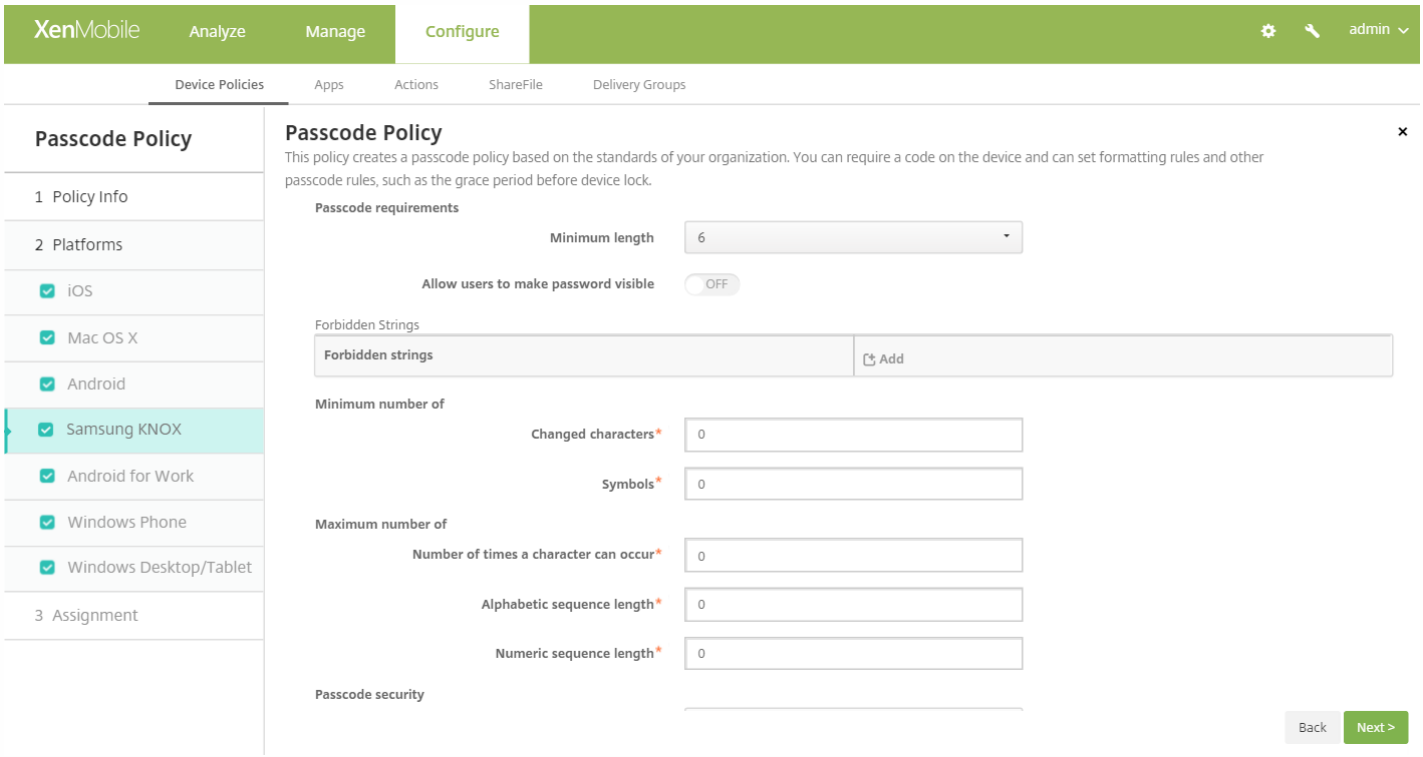
- **Samsung SAFE**
  - **Utiliser le même code secret pour tous les utilisateurs** : sélectionnez cette option si vous souhaitez utiliser le même code secret pour tous les utilisateurs. La valeur par défaut est **OFF**. Ce paramètre s'applique uniquement aux appareils Samsung SAFE et il est disponible, que le paramètre **Code secret requis** soit sélectionné ou non.
  - Lorsque vous activez l'option **Utiliser le même code secret pour tous les utilisateurs**, saisissez le code secret à utiliser par les utilisateurs dans le champ **Code secret**.

- Lorsque vous activez l'option **Code secret requis**, configurez les paramètres suivants pour Samsung SAFE :
  - **Caractères modifiés** : entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est de **0**.
  - **Nombre d'occurrences d'un caractère** : entrez le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences alphabétiques** : entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences numériques** : entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est de **0**.
  - **Autoriser les utilisateurs à afficher le mot de passe** : indiquez si les utilisateurs peuvent afficher leurs codes secrets. La valeur par défaut est **ON**.
  - **Chaînes interdites** : créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez refuser, cliquez sur **Ajouter**, puis procédez comme suit :
    - **Chaînes interdites** : entrez la chaîne que les utilisateurs ne peuvent pas utiliser.
    - Cliquez sur **Enregistrer** pour ajouter la chaîne ou sur **Annuler** pour annuler l'ajout de la chaîne.

      Remarque : pour supprimer une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

      Pour modifier une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

Configurer les paramètres pour Samsung KNOX



Pour configurer ces paramètres :

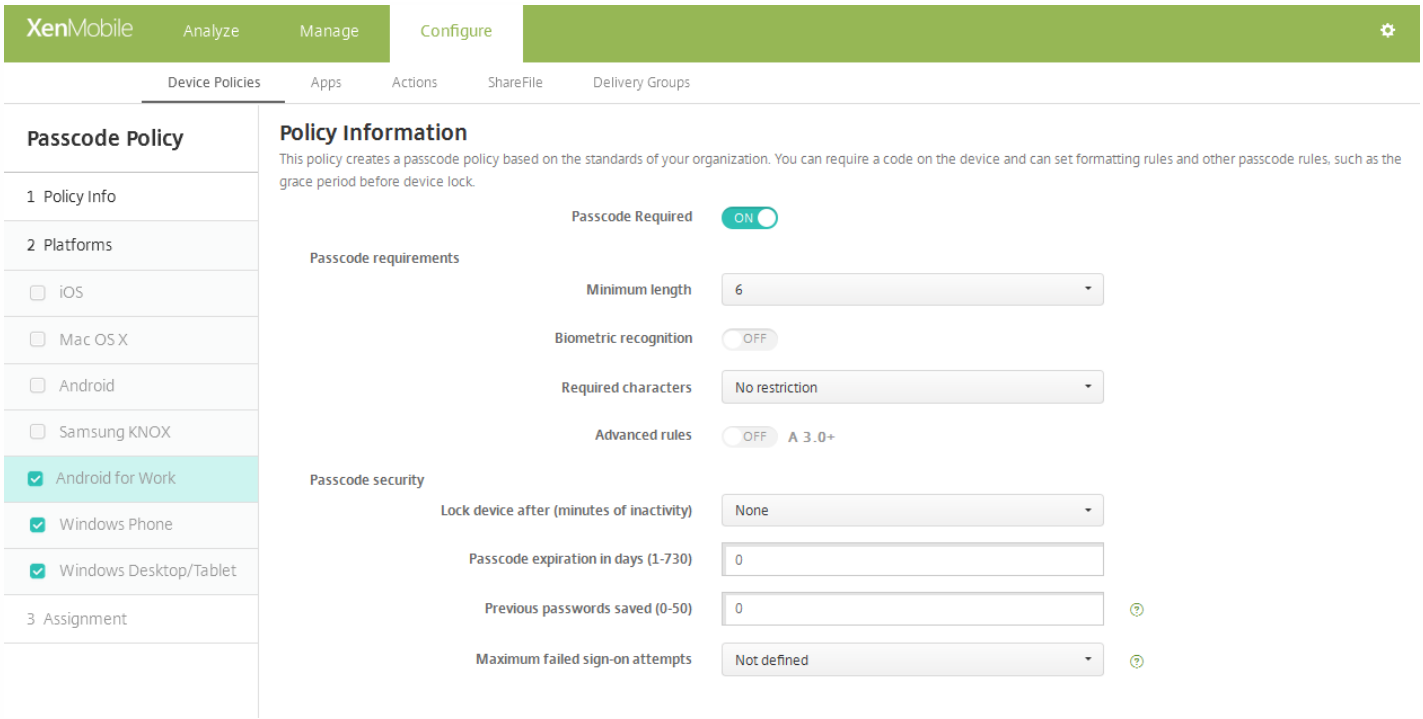
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
  - **Autoriser les utilisateurs à afficher les mots de passe** : sélectionnez cette option pour autoriser les utilisateurs à afficher le mot de passe.
  - **Chaînes interdites** : créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Pour chaque chaîne que vous souhaitez refuser, cliquez sur Ajouter, puis procédez comme suit :
    - **Chaînes interdites** : entrez la chaîne que les utilisateurs ne peuvent pas utiliser.
    - Cliquez sur **Enregistrer** pour ajouter la chaîne ou sur **Annuler** pour annuler l'ajout de la chaîne.

      Remarque : pour supprimer une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

      Pour modifier une chaîne existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

- **Nombre minimum de**
  - **Caractères modifiés** : entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est de **0**.
  - **Symboles** : entrez le nombre minimum de symboles requis dans un code secret. La valeur par défaut est de **0**.
- **Nombre maximum de**
  - **Nombre d'occurrences d'un caractère** : entrez le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences alphabétiques** : entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est de **0**.
  - **Longueur des séquences numériques** : entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est de **0**.
- **Sécurité des codes secrets**
  - **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur le nombre de secondes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.
  - **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
  - **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
  - **Si le nombre de tentatives de connexion infructueuses est dépassé, l'appareil est bloqué** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est verrouillé. La valeur par défaut est **Aucun nombre défini**.
  - **Si le nombre de tentatives de connexion infructueuses est dépassé, l'appareil est effacé** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que le conteneur KNOX (ainsi que les données KNOX) ne soient effacés de l'appareil. Les utilisateurs doivent réinitialiser le conteneur KNOX après l'effacement. La valeur par défaut est **Aucun nombre défini**.

Configurer les paramètres pour Android for Work

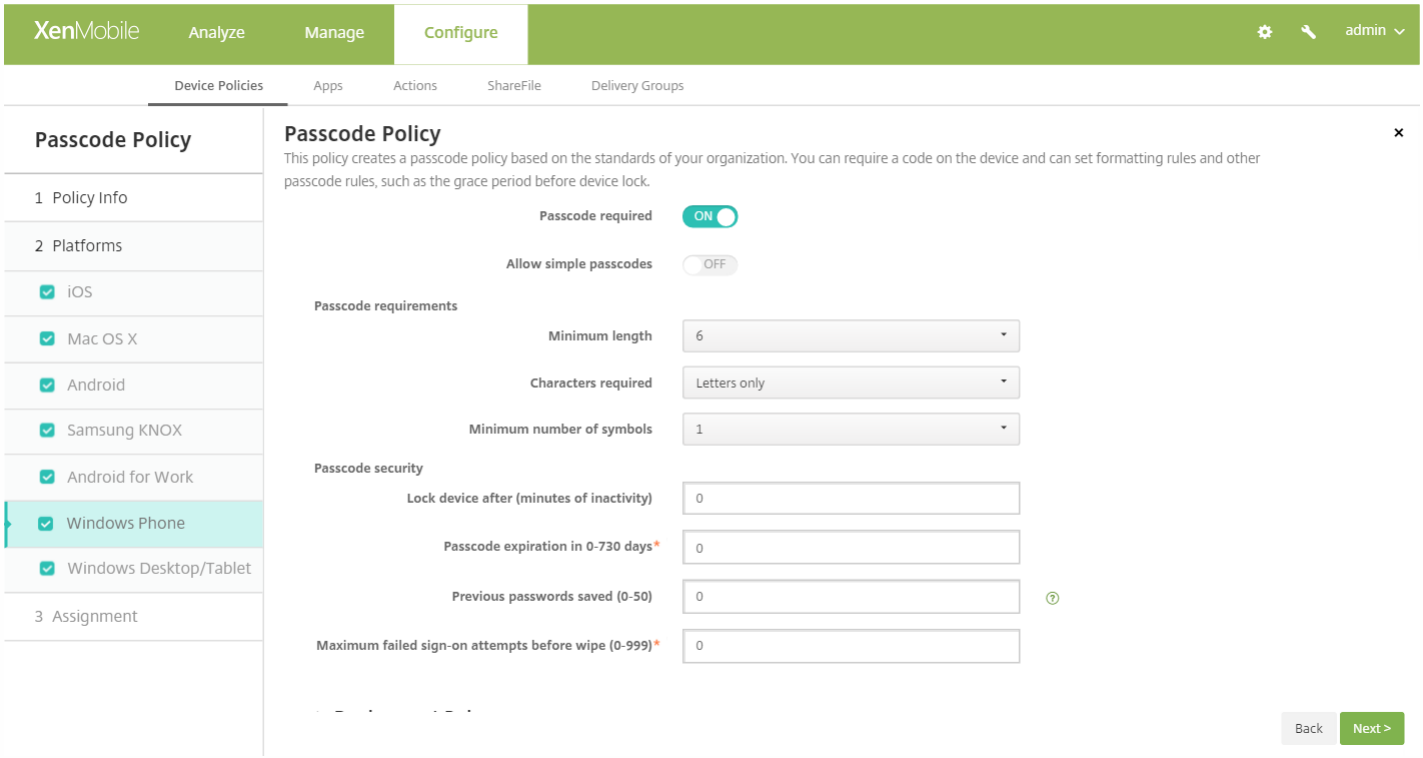


Pour configurer ces paramètres :

- **Code secret requis** : sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour Android for Work. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret et à la sécurité du code secret.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
  - **Reconnaissance biométrique** : sélectionnez cette option pour activer la reconnaissance biométrique. Si vous activez cette option, le champ **Caractères requis** est masqué. La valeur par défaut est **OFF**. Notez que cette fonctionnalité n'est pas prise en charge.
  - **Caractères requis** : dans la liste, cliquez sur **Aucune restriction**, **Chiffres et lettres**, **Chiffres uniquement** ou **Lettres uniquement** pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est **Aucune restriction**.
  - **Règles avancées** : sélectionnez cette option si vous souhaitez appliquer des règles de code secret avancées. Cette option n'est pas disponible pour les appareils Android de versions antérieures à Android 5.0. La valeur par défaut est **OFF**.
  - Lorsque le paramètre **Règles avancées** est activé, à partir de chacune des listes suivantes et pour chaque type de caractère, cliquez sur le nombre minimal de caractère qu'un code secret doit contenir :
    - **Symboles** : nombre minimal de symboles.
    - **Lettres** : nombre minimal de lettres.
    - **Minuscules** : nombre minimum de minuscules.
    - **Majuscules** : nombre minimum de majuscules.
    - **Chiffres ou symboles** : nombre minimal de chiffres ou de symboles.
    - **Chiffres** : nombre minimal de chiffres.
- **Sécurité des codes secrets**
  - **Verrouiller l'appareil après (minutes d'inactivité)** : dans la liste, cliquez sur le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est **Aucune**.

- **Expiration du code secret en jours (1 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Nombre maximum de tentatives de connexion infructueuses** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que le conteneur KNOX (ainsi que les données KNOX) ne soient effacés de l'appareil. Les utilisateurs doivent réinitialiser le conteneur KNOX après l'effacement. La valeur par défaut est **Aucun nombre défini**.

Configurer les paramètres pour Windows Phone

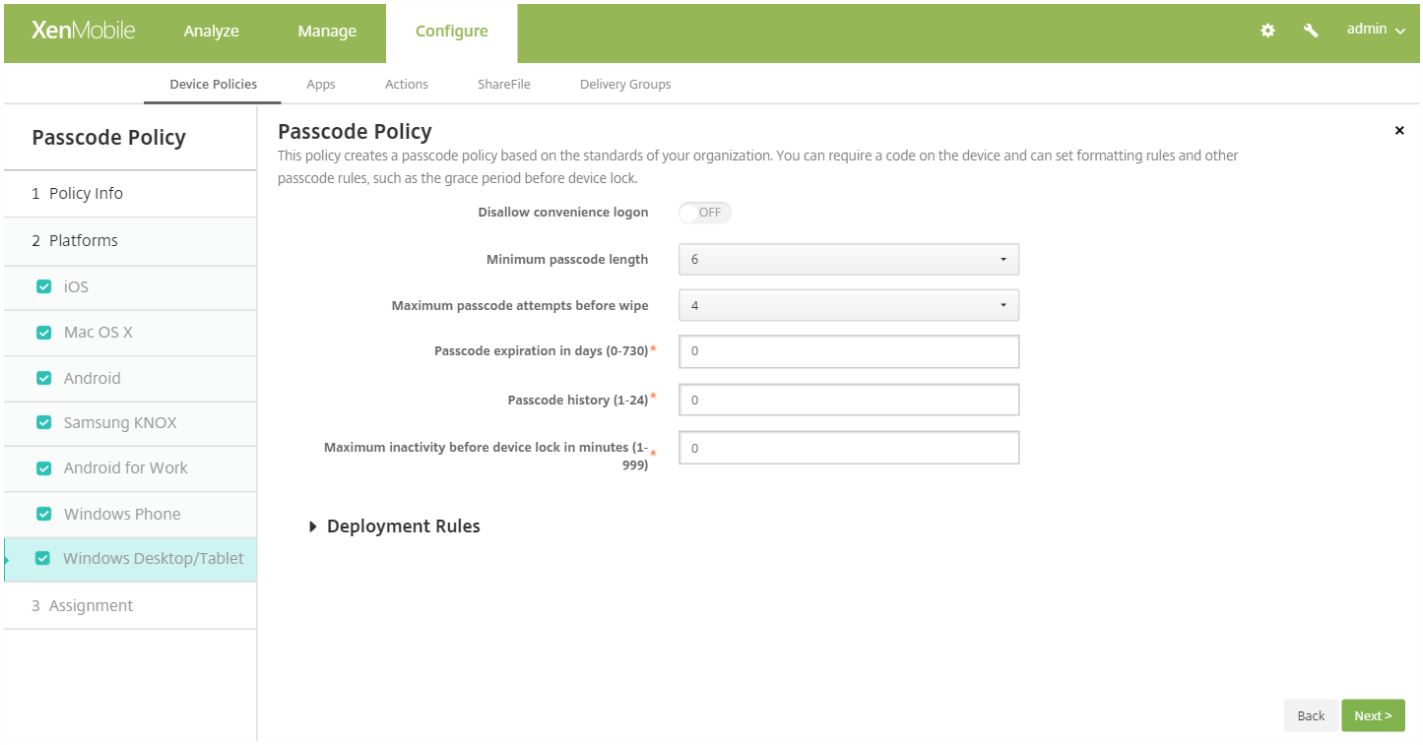


Pour configurer ces paramètres :

- **Code secret requis** : sélectionnez cette option pour ne pas exiger de code secret sur les appareils Windows Phone. Le paramètre par défaut est **ON**, ce qui nécessite un mot de passe. La page se réduit et les options suivantes disparaissent lorsque vous désactivez ce paramètre.
- **Autoriser les codes secrets simples** : sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est OFF.
- **Conditions requises pour les codes secrets**
  - **Longueur minimale** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
  - **Caractères requis** : dans la liste, cliquez sur **Numérique ou alphanumérique**, **Lettres uniquement** ou **Chiffres uniquement** pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est **Lettres uniquement**.
  - **Nombre minimum de symboles** : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de **1**.
- **Sécurité des codes secrets**

- **Verrouiller l'appareil après (minutes d'inactivité)** : entrez le nombre de minutes pendant lesquelles un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est de **0**.
- **Expiration du mot de passe dans 0 - 730 jours** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 0-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Mots de passe précédents enregistrés (0-50)** : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est **0**, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
- **Nombre maximum de tentatives de connexion infructueuses avant effacement (0 - 999)** : entrez le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que les données d'entreprise ne soient effacées de l'appareil. La valeur par défaut est de **0**.

Configurer les paramètres pour Windows Desktop/Tablet



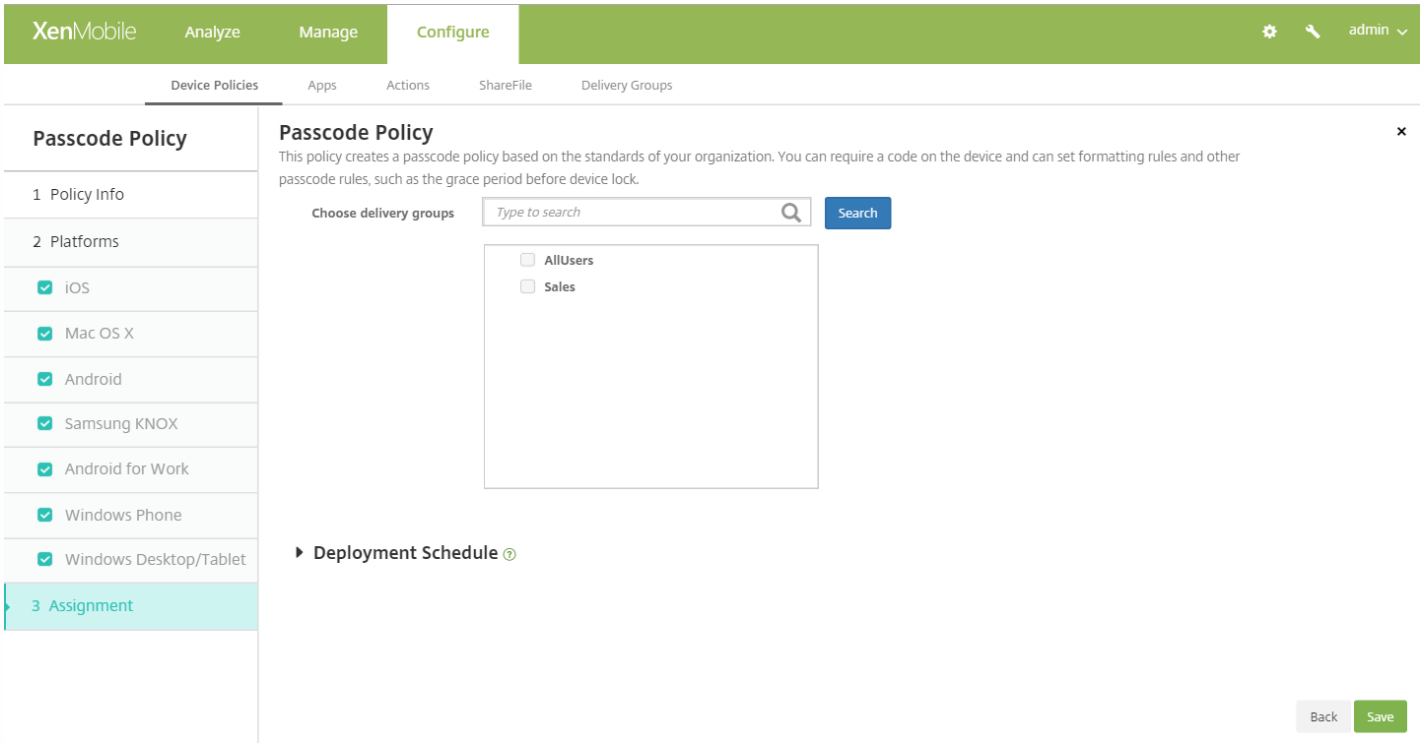
Pour configurer ces paramètres :

- **Interdire les dispositifs de connexion pratiques** : sélectionnez cette option pour autoriser les utilisateurs à accéder à leurs appareils à l'aide de mots de passe image ou d'ouvertures de session biométriques. La valeur par défaut est **OFF**.
- **Longueur minimum du code secret** : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de **6**.
- **Nombre maximum de tentatives de saisie du code secret avant effacement (0 - 999)** : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que les données d'entreprise ne soient effacées de l'appareil. La valeur par défaut est de **4**.
- **Expiration du code secret en jours (0 - 730)** : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 0-730. La valeur par défaut est **0**, ce qui signifie que le code secret n'expire jamais.
- **Historique du code secret (1 - 24)** : entrez le nombre de codes secrets utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des codes secrets figurant dans cette liste. Les valeurs valides sont 1-24. Vous devez entrer un nombre compris entre 1 et 24. La valeur par défaut est de **0**.

- **Période d'inactivité maximale avant verrouillage de l'appareil en minutes (0 - 999)** : entrez la durée en minutes pendant laquelle un appareil peut rester inactif avant d'être verrouillé. Les valeurs valides sont 1-999. Vous devez entrer un nombre compris entre 1 et 999. La valeur par défaut est de **0**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de code secret** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**,

qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie Personal Hotspot

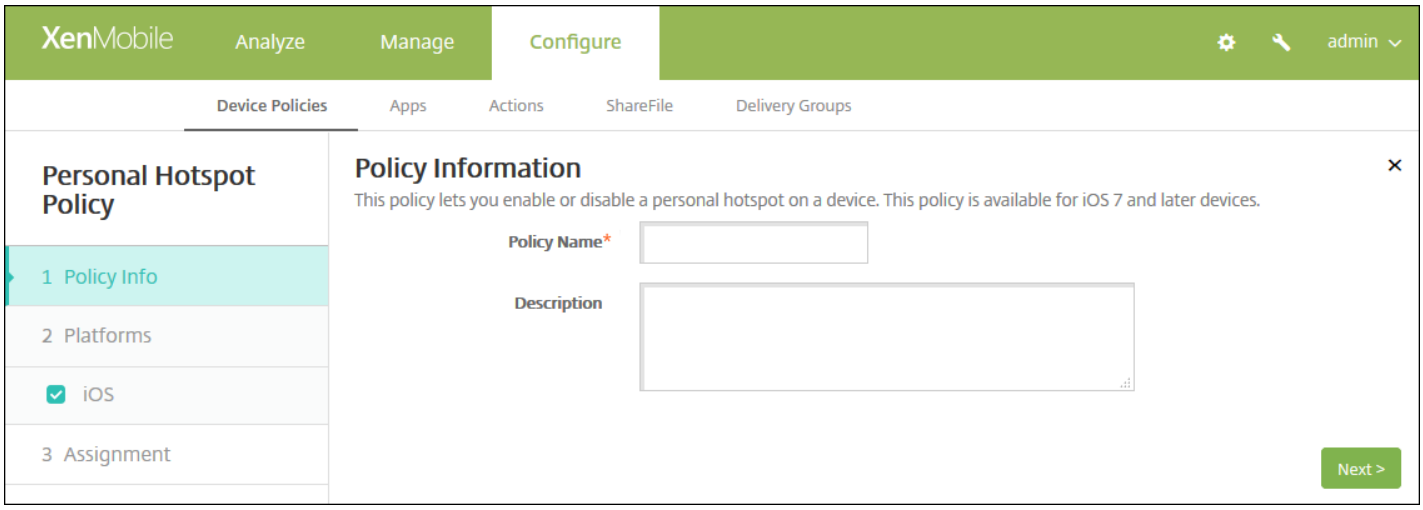
Feb 23, 2017

Vous pouvez autoriser les utilisateurs à se connecter à Internet lorsqu'ils ne sont pas à portée d'un réseau Wi-Fi en utilisant la connexion des données cellulaires au travers de la fonctionnalité Partage de connexion (Personal Hotspot) de leurs appareils iOS. Disponible sur iOS 7.0 et version ultérieure.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

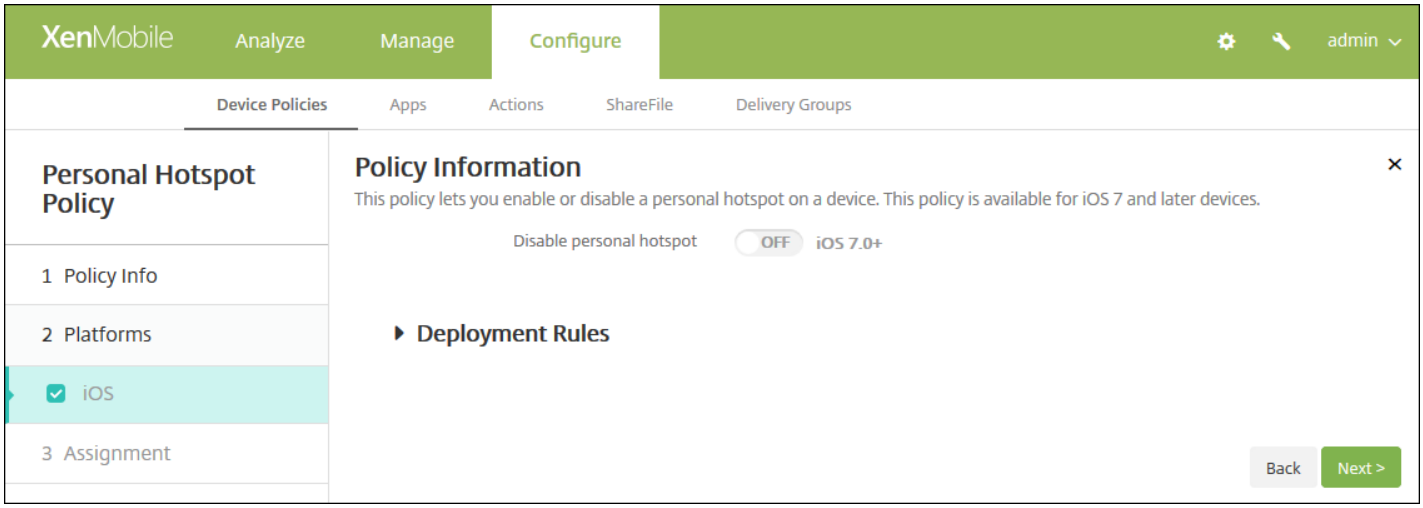
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Personal Hotspot**. La page d'informations sur la **Stratégie Personal Hotspot** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Plate-forme iOS** s'affiche.

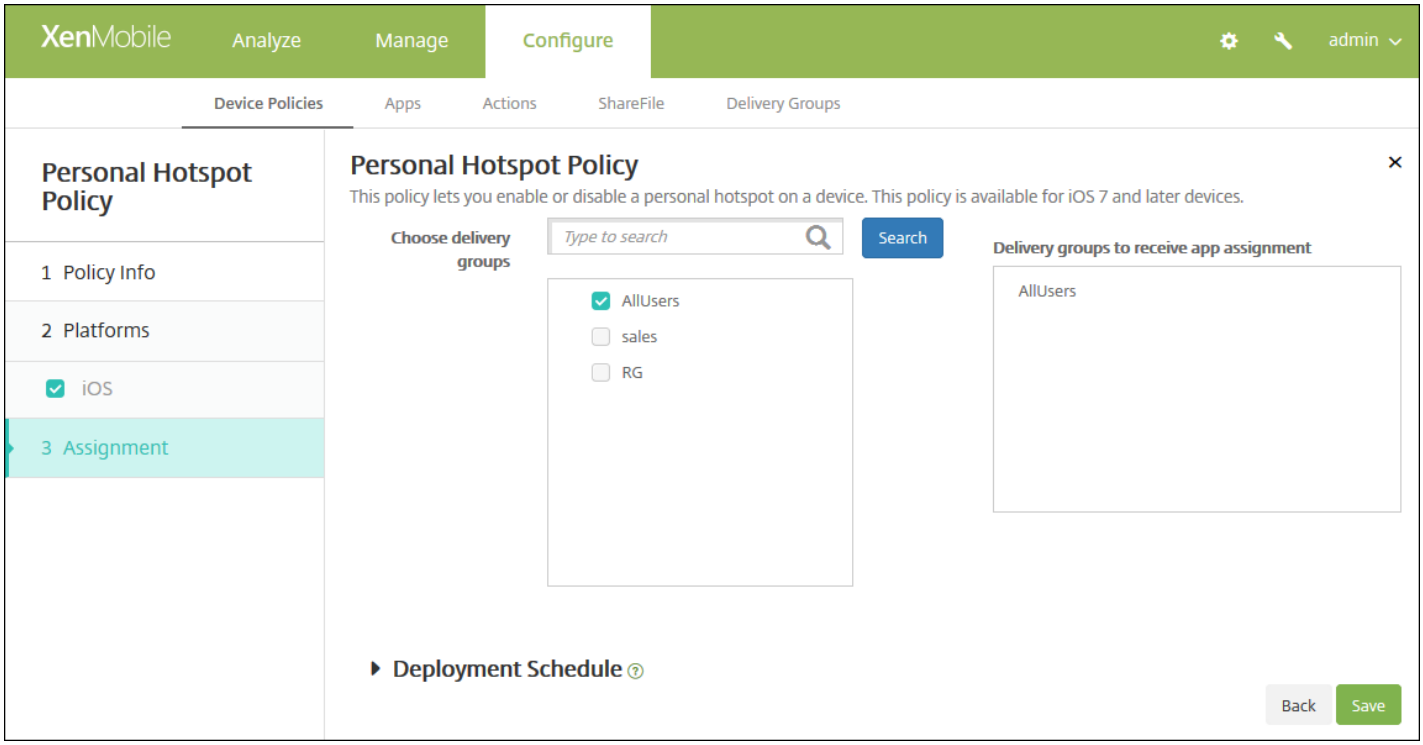


6. Configurez ce paramètre :

- **Désactiver Personal Hotspot** : sélectionnez cette option pour désactiver la fonctionnalité Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. La valeur par défaut est **OFF**, ce qui désactive Partage de connexion (Personal Hotspot) sur les appareils des utilisateurs. Cette stratégie ne désactive pas la fonctionnalité ; les utilisateurs peuvent toujours utiliser Partage de connexion (Personal Hotspot) sur leurs appareils, mais lorsque la stratégie est déployée, Personal Hotspot est désactivé de manière à ne pas rester activé par défaut.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie Personal Hotspot** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de suppression de profil

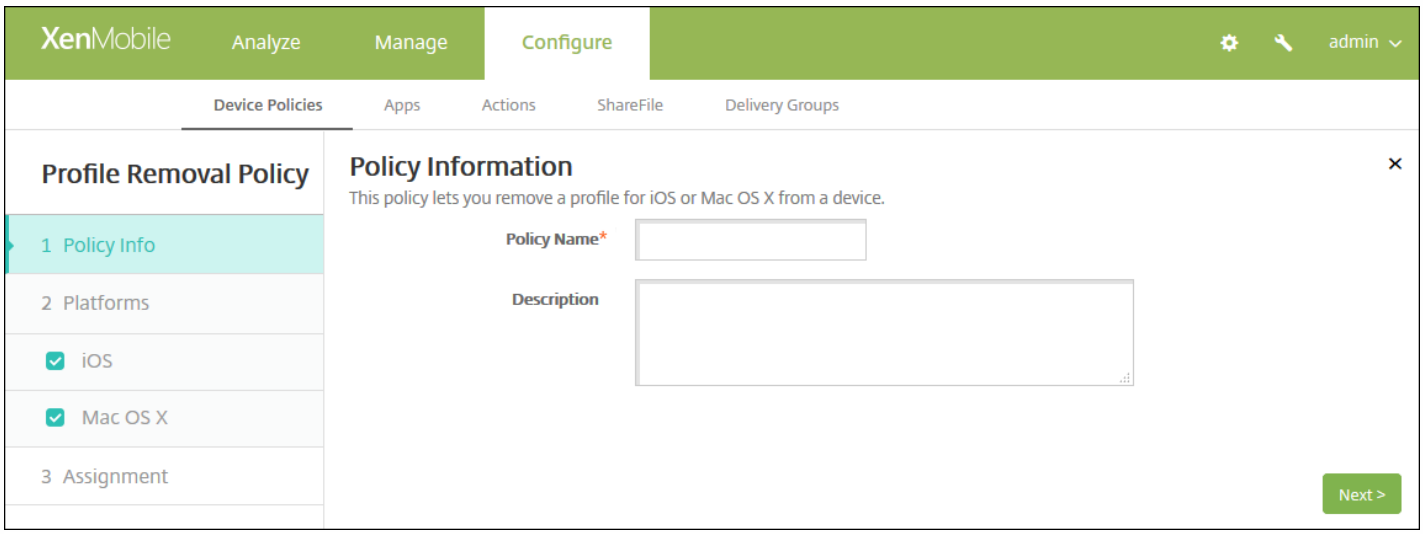
Feb 23, 2017

Vous pouvez créer une stratégie de suppression de profil dans XenMobile. La stratégie, lorsqu'elle est déployée, supprime le profil d'application des appareils iOS ou Mac OS X des utilisateurs.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page Stratégies d'appareil s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus** puis, sous **Suppression**, cliquez sur **Suppression du profil**. La page d'informations **Stratégie de suppression du profil** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

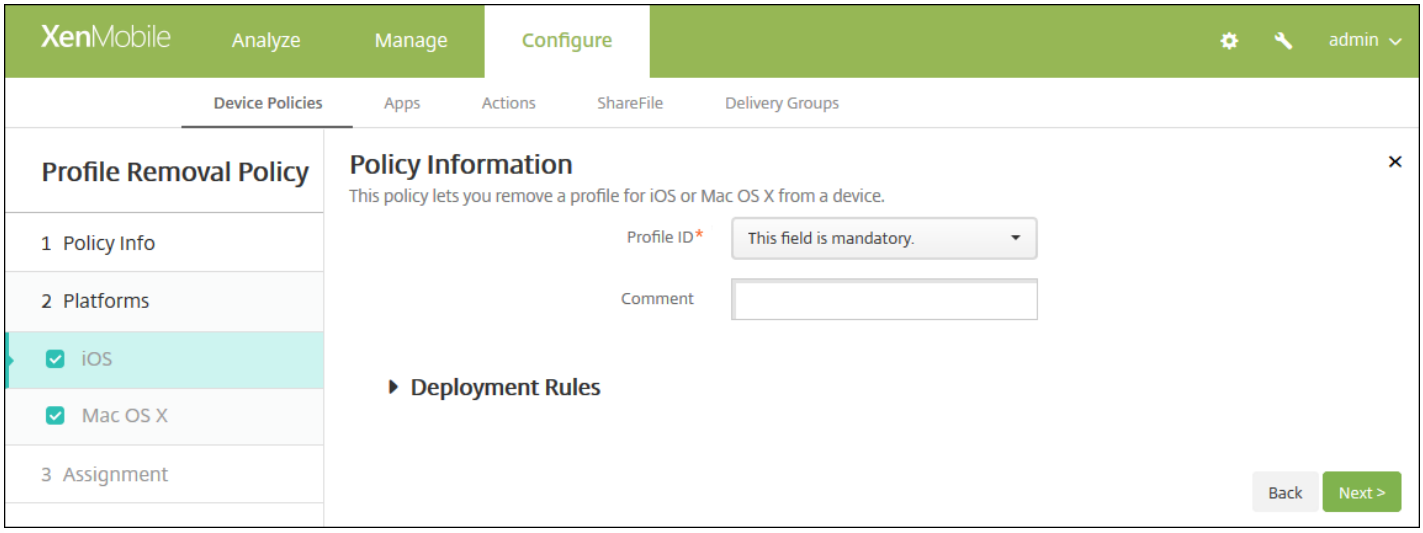
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plates-formes** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

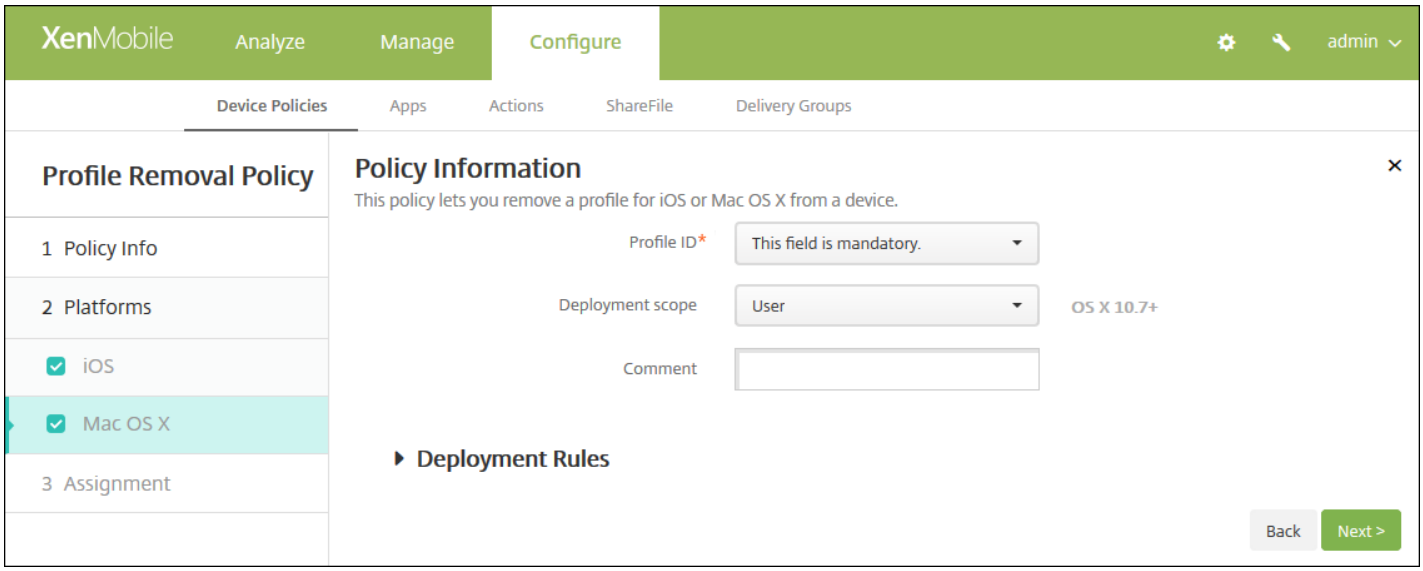
Configurer le paramètre pour iOS



Pour configurer ces paramètres :

- **ID du profil** : dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.
- **Commentaires** : entrez un commentaire (facultatif).

Configurer les paramètres pour Mac OS X

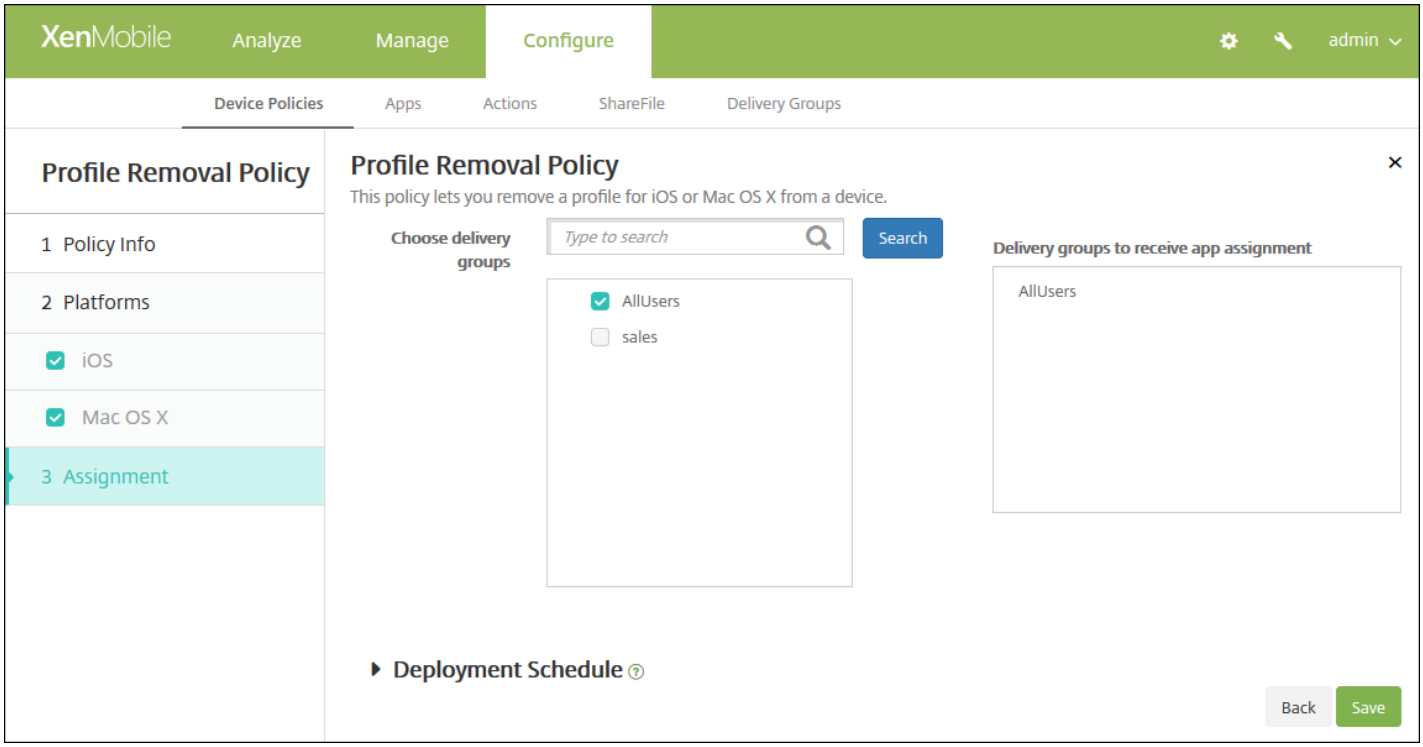


Pour configurer ces paramètres :

- **ID du profil** : dans la liste, cliquez sur l'ID du profil d'application. Ce champ est obligatoire.
- **Étendue du déploiement** : dans la liste, cliquez sur **Utilisateur** ou **Système**. La valeur par défaut est **Utilisateur**. Cette option est disponible uniquement sur OS X 10.7 et versions ultérieures.
- **Commentaires** : entrez un commentaire (facultatif).

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression du profil** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de profil de provisioning

Feb 23, 2017

Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning de distribution d'entreprise, dont Apple a besoin pour que l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se bloque lorsque l'utilisateur tape pour l'ouvrir.

Le principal problème avec les profils de provisioning est qu'ils expirent un an après qu'ils sont générés sur le portail Apple Developer et vous devez conserver les dates d'expiration pour tous les profils de provisioning sur tous les appareils iOS inscrits par vos utilisateurs. Le suivi des dates d'expiration non seulement implique de surveiller les dates d'expiration, mais aussi quels utilisateurs utilisent quelle version de l'application. Les deux solutions consistent à envoyer par e-mail les profils de provisioning aux utilisateurs ou à les placer dans un portail Web pour le téléchargement et l'installation. Ces solutions fonctionnent, mais elles peuvent entraîner des erreurs car elles requièrent que les utilisateurs réagissent à des instructions dans un e-mail ou accèdent au portail Web pour télécharger le profil approprié et l'installer.

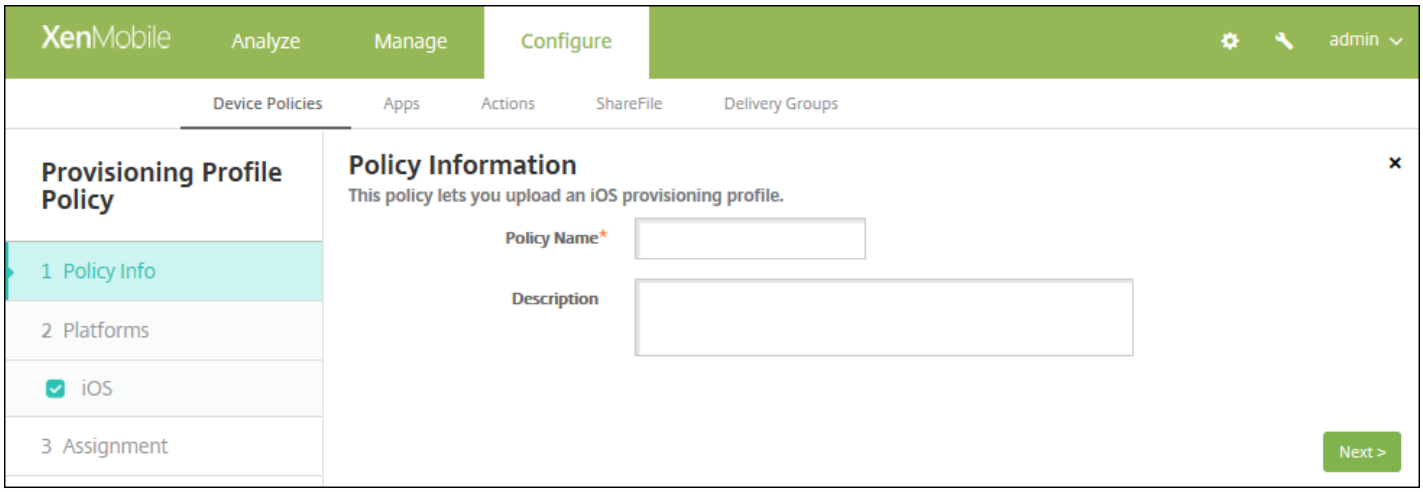
Pour effectuer cette opération de façon transparente pour les utilisateurs, dans XenMobile, vous pouvez installer et supprimer les profils de provisioning avec les stratégies d'appareil. Les profils manquants ou arrivés à expiration sont supprimés si nécessaire et des profils à jour sont installés sur les appareils des utilisateurs, de façon à ce qu'il leur suffise de taper sur une application pour l'ouvrir.

Avant de pouvoir créer une stratégie de profil de provisioning, vous devez créer un fichier de profil de provisioning. Pour plus d'informations, veuillez consulter la section Création de profils de provisioning sur le site Apple Developer.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

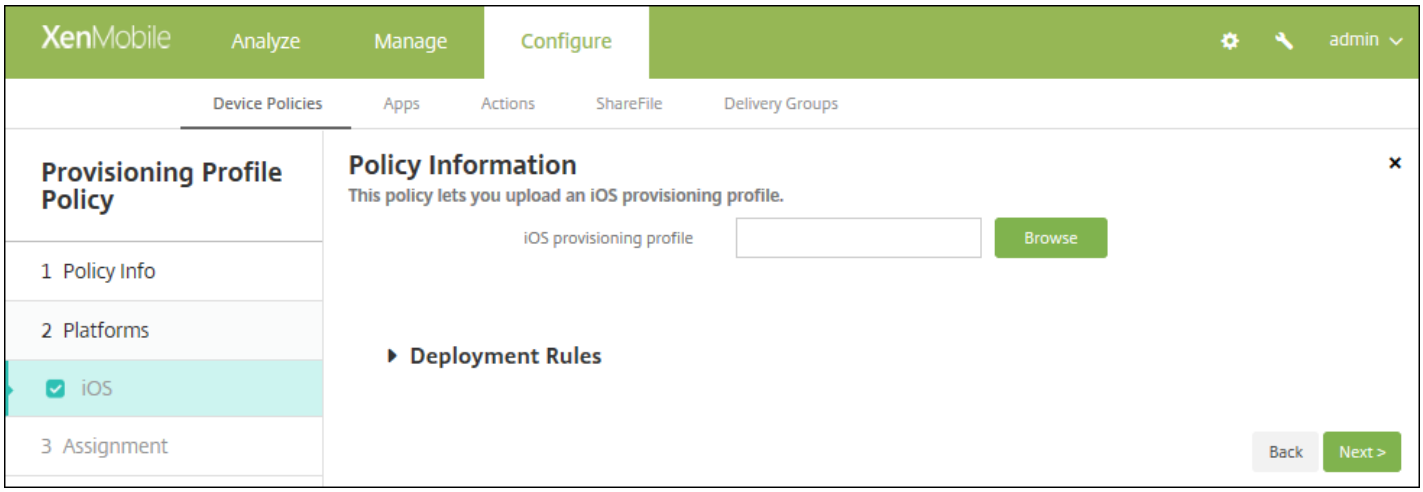
3. Développez **Plus** puis, sous **Applications**, cliquez sur **Profil de provisioning**. La page d'informations **Stratégie de profil de provisioning** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Suivant**. La page d'informations **Plate-forme iOS** s'affiche.

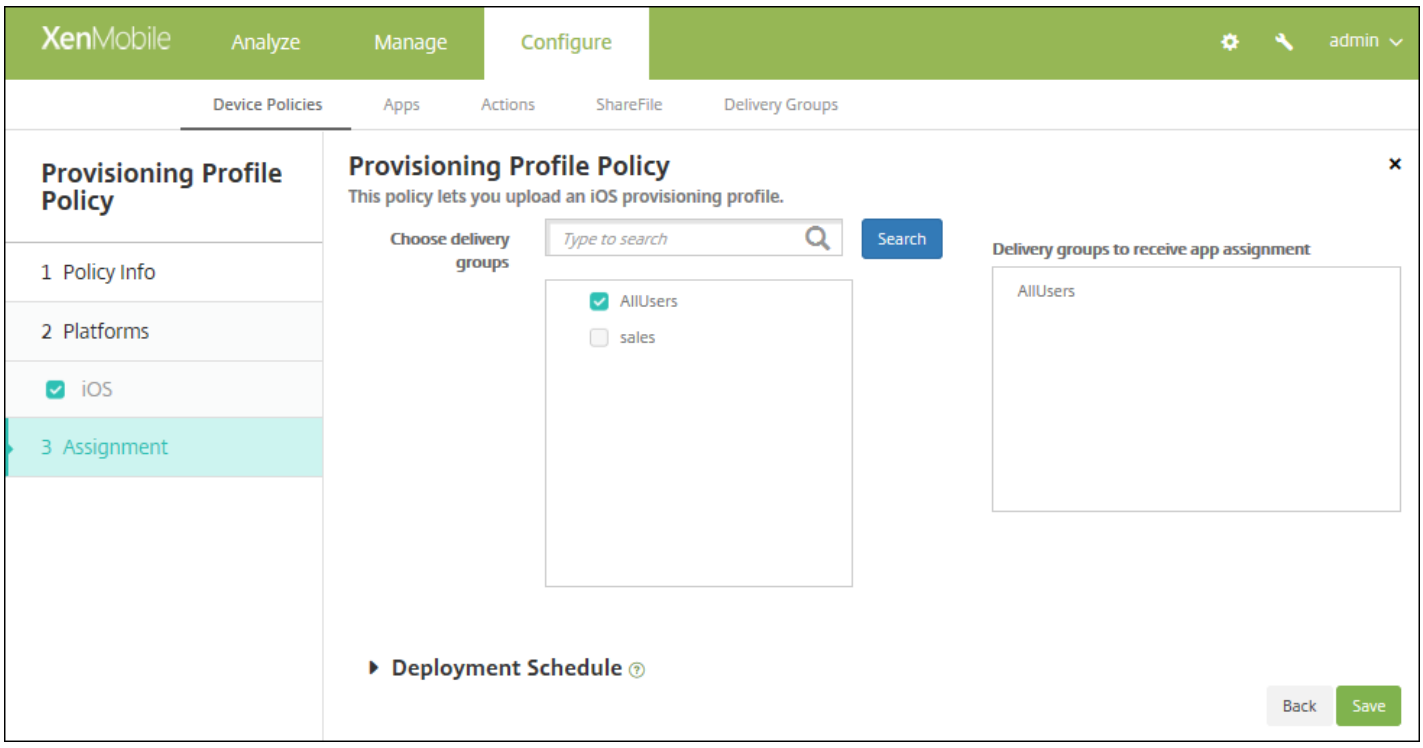


6. Effectuez la configuration suivante :

- **Profil de provisioning iOS** : sélectionnez le fichier de profil de provisioning à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution **Stratégie de profil de provisioning** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de suppression de profil de provisioning

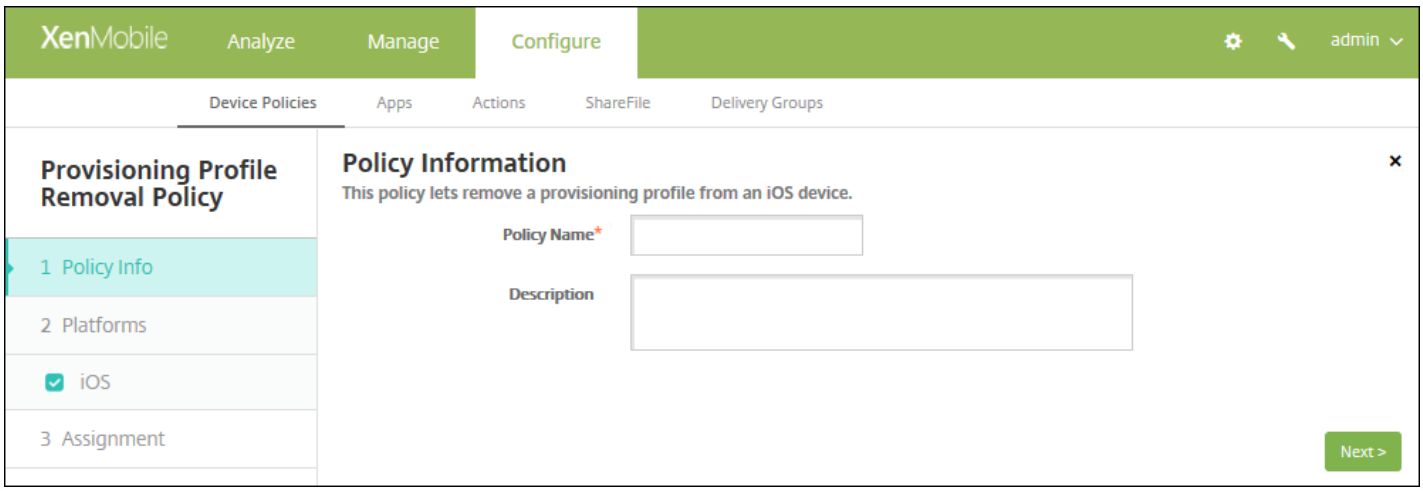
Feb 23, 2017

Vous pouvez supprimer des profils de provisioning iOS avec des stratégies d'appareil. Pour de plus amples informations sur les profils de provisioning, consultez la section Ajout d'un profil de provisioning.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

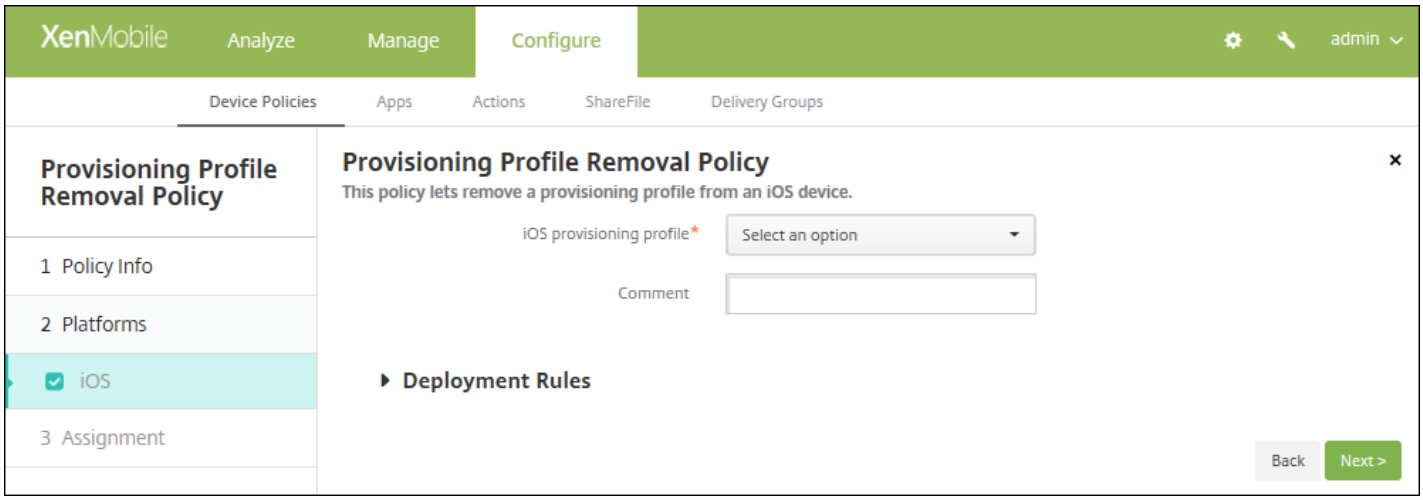
3. Développez **Plus** puis, sous **Suppression**, cliquez sur **Suppression du profil de provisioning**. La page d'informations **Stratégie de suppression du profil de provisioning** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Plate-forme iOS** s'affiche.

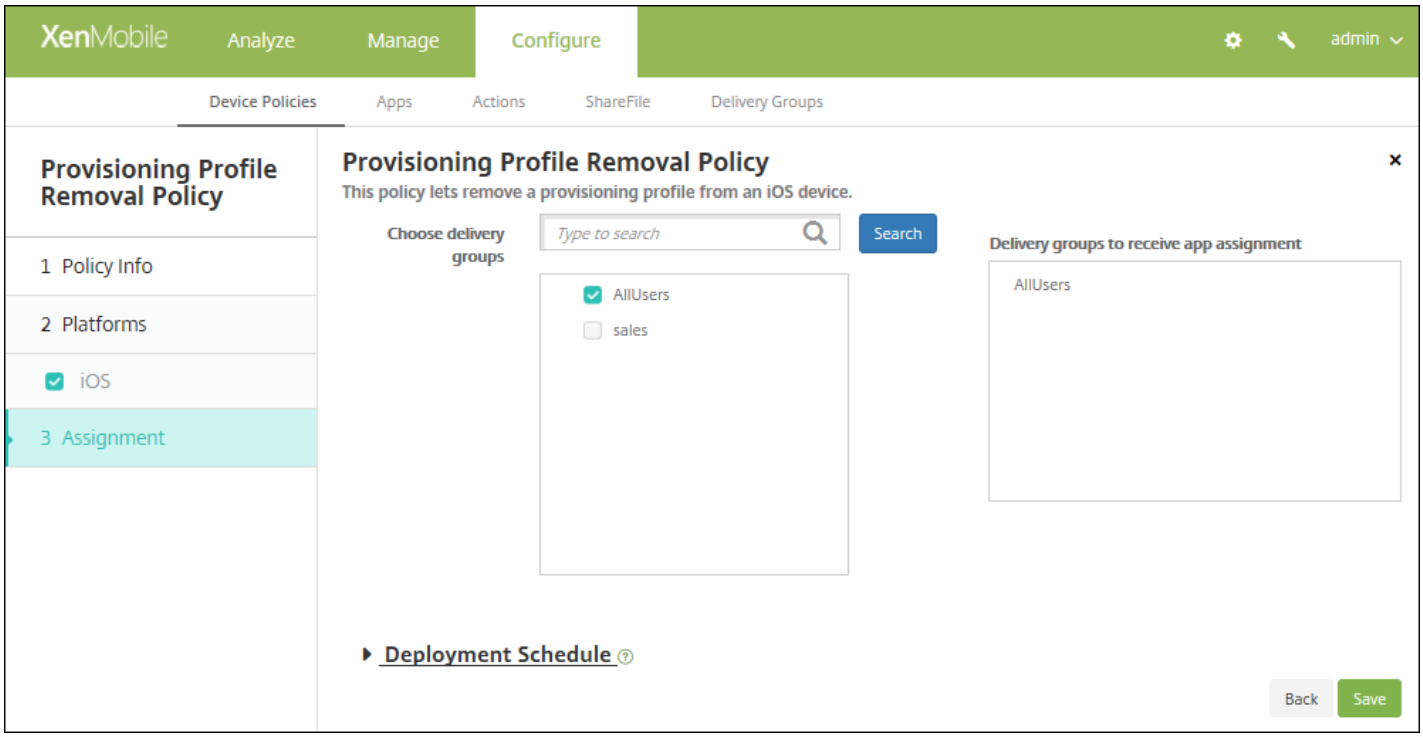


6. Configurez les paramètres suivants :

- **Profil de provisioning iOS** : dans la liste, cliquez sur le profil de provisioning que vous souhaitez supprimer.
- **Commentaire** : si vous le souhaitez, ajoutez un commentaire.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution **Stratégie de suppression du profil de provisioning** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**,

qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de proxy

Feb 23, 2017

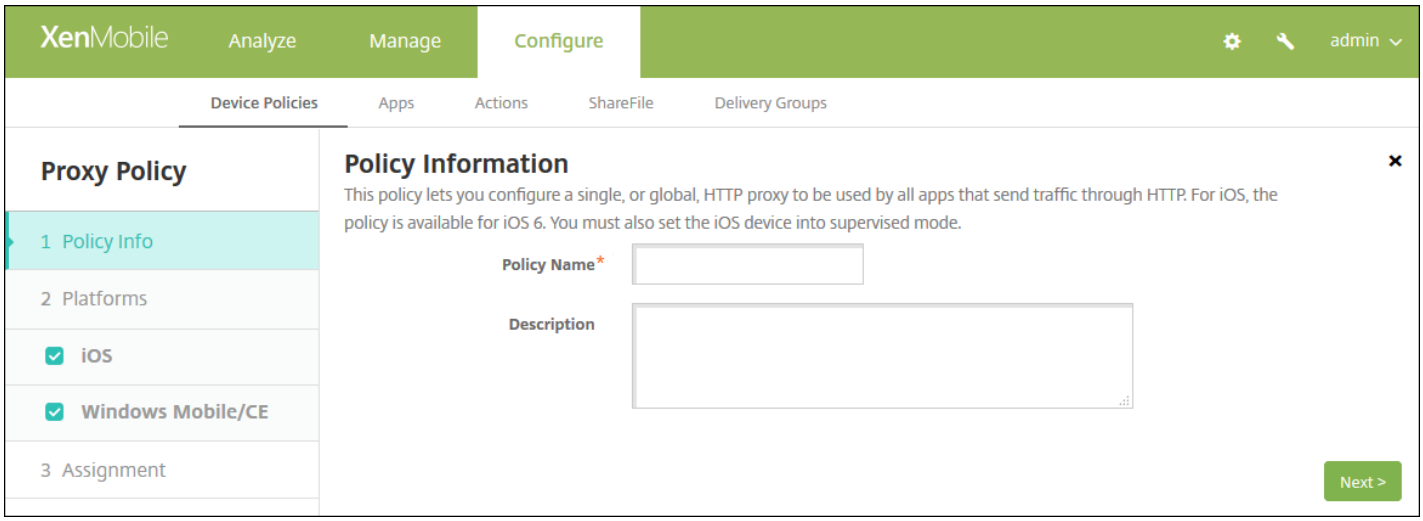
Vous pouvez ajouter une stratégie dans XenMobile pour spécifier les paramètres de proxy HTTP globaux pour les appareils exécutant Windows Mobile/CE et iOS 6.0 ou version ultérieure. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.

Remarque : avant de déployer cette stratégie, assurez-vous de définir tous les appareils iOS pour lesquels vous souhaitez définir un proxy HTTP global en mode supervisé. Pour de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Plus**, puis, sous **Accès réseau**, cliquez sur **Proxy**. La page **Stratégie de proxy** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

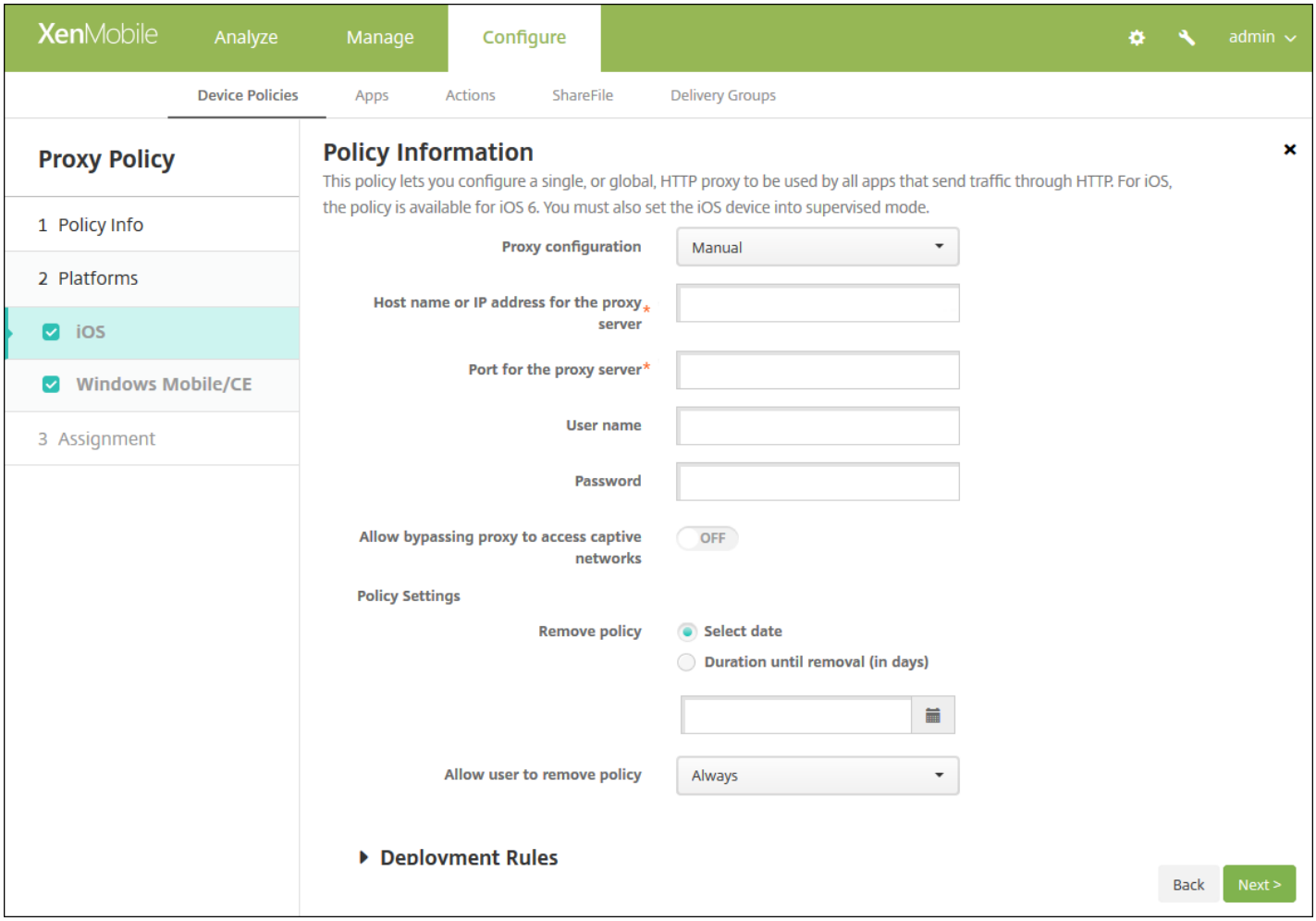
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour iOS

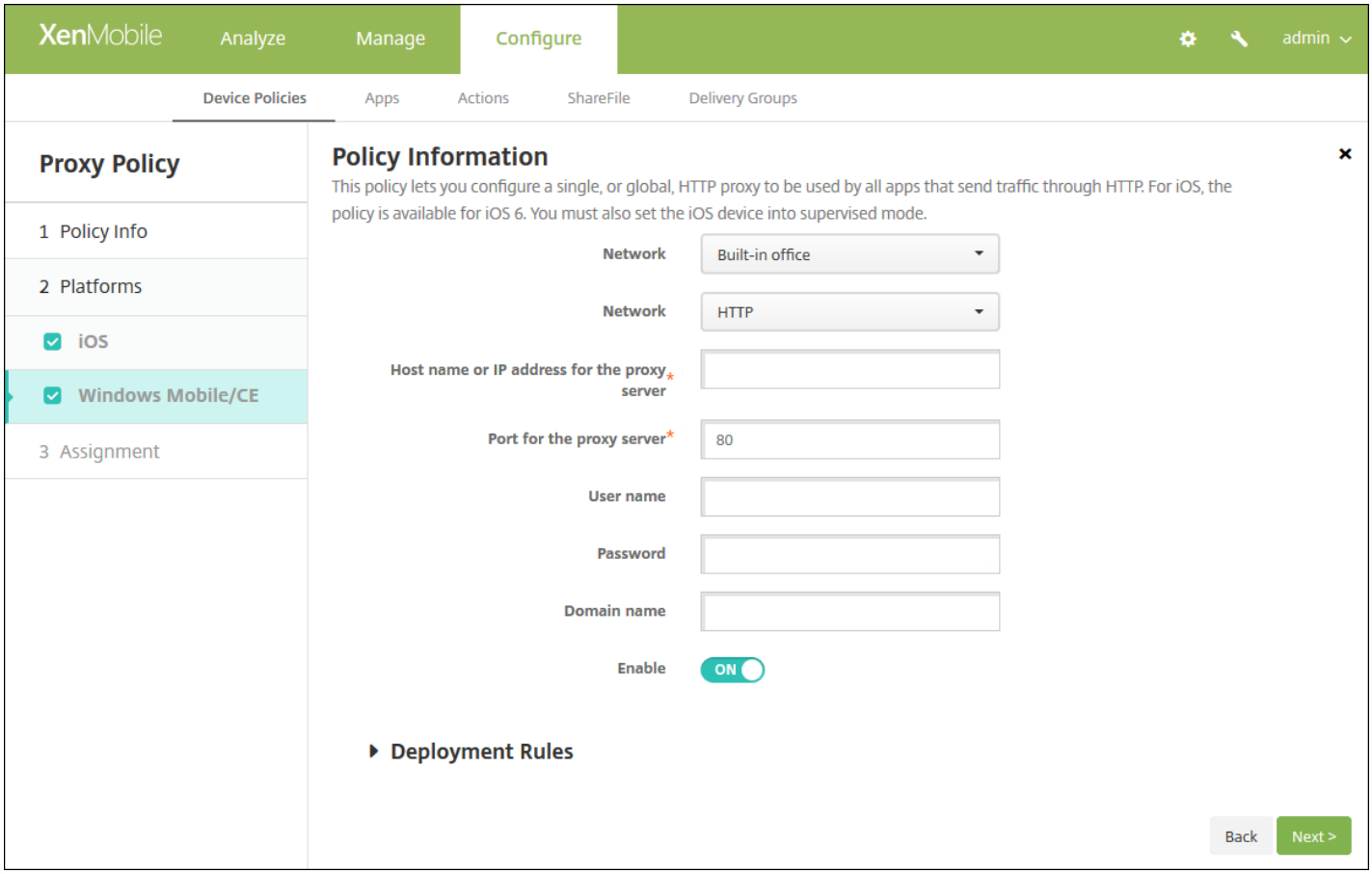


Pour configurer ces paramètres :

- **Configuration du proxy** : cliquez sur **Manuel** ou **Automatique** pour choisir la méthode à utiliser pour configurer le proxy sur les appareils des utilisateurs.
  - Si vous avez sélectionné **Manuel**, configurez les paramètres suivants :
    - **Nom d'hôte ou adresse IP du serveur proxy** : entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.
    - **Port du serveur proxy** : entrez le numéro de port du serveur proxy. Ce champ est obligatoire.
    - **Nom d'utilisateur** : entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
    - **Mot de passe** : entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
  - Si vous avez sélectionné **Automatique**, configurez les paramètres suivants :
    - **URL du fichier de configuration automatique de proxy** : entrez l'adresse URL du fichier PAC qui définit la configuration proxy.
    - **Autoriser la connexion directe si le PAC est injoignable** : indiquez si les utilisateurs sont autorisés à se connecter directement à la destination si le fichier PAC est inaccessible. La valeur par défaut est **ON**. Cette option est disponible uniquement sur iOS 7.0 et versions ultérieures.
- **Autoriser le contournement du proxy pour accéder aux réseaux captifs** : sélectionnez cette option pour autoriser le contournement du proxy afin d'accéder aux réseaux captifs. La valeur par défaut est **OFF**.
- **Paramètres de stratégie**
  - En regard de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou sur **Délai avant suppression (en jours)**.

- Si vous cliquez sur **Sélectionner une date**, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
- Dans la liste **Autoriser l'utilisateur à supprimer la stratégie**, cliquez sur **Toujours**, **Mot de passe requis** ou **Jamais**.
- Si vous cliquez sur **Mot de passe requis**, à côté de **Code secret de suppression**, entrez le mot de passe requis.

Configurer les paramètres pour Windows Mobile/CE



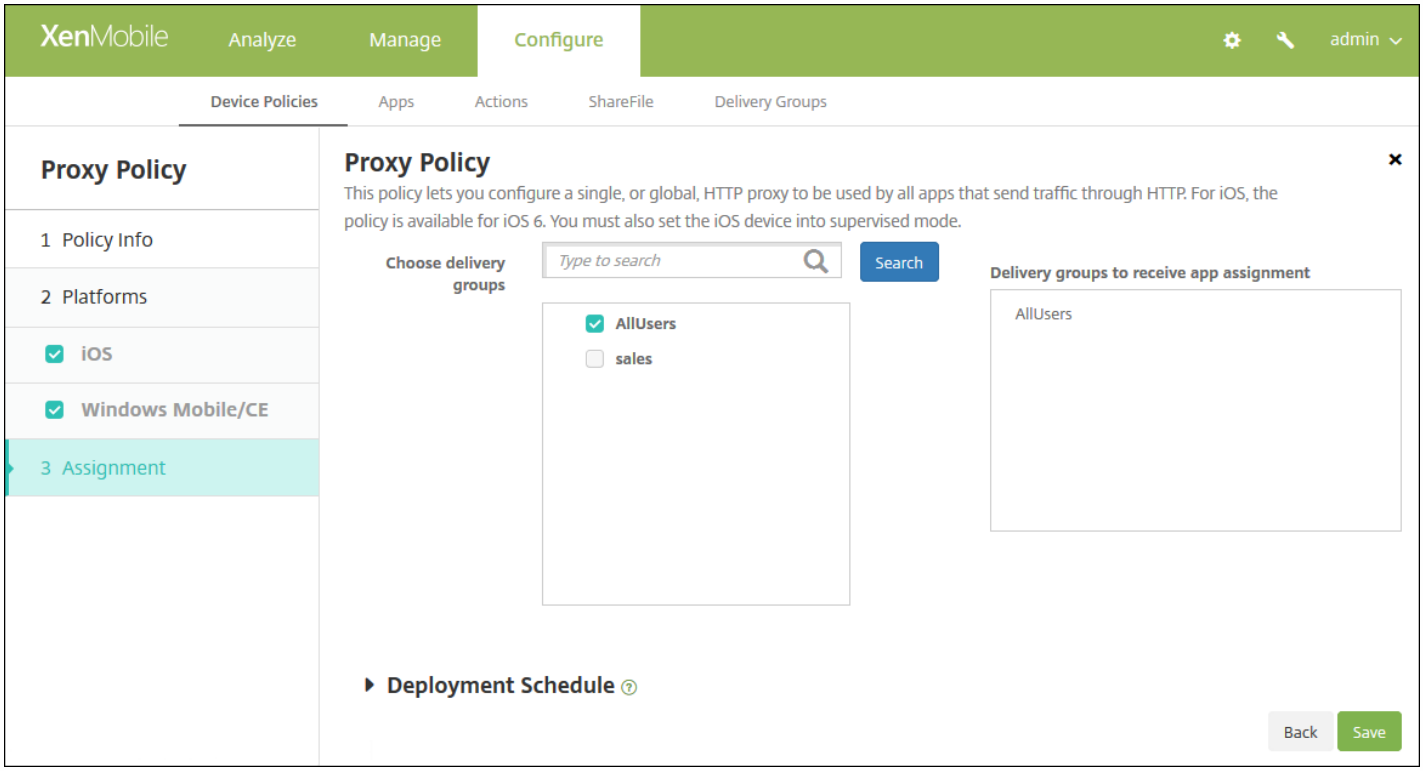
Pour configurer ces paramètres :

- **Réseau** : dans la liste, cliquez sur le type de réseau à utiliser. La valeur par défaut est **Bureau intégré**. Les options possibles sont les suivantes :
  - Bureau
  - Internet
  - Bureau intégré
  - Internet intégré
- **Réseau** : dans la liste, cliquez sur le protocole de connexion réseau à utiliser. La valeur par défaut est **HTTP**. Les options possibles sont les suivantes :
  - HTTP
  - WAP
  - Socks 4
  - Socks 5
- **Nom d'hôte ou adresse IP du serveur proxy** : entrez le nom d'hôte ou l'adresse IP du serveur proxy. Ce champ est obligatoire.

- **Port du serveur proxy** : entrez le numéro de port du serveur proxy. Ce champ est obligatoire. La valeur par défaut est de **80**.
- **Nom d'utilisateur** : entrez un nom d'utilisateur pour l'authentification auprès du serveur proxy (facultatif).
- **Mot de passe** : entrez un mot de passe pour l'authentification auprès du serveur proxy (facultatif).
- **Nom de domaine** : entrez le nom du domaine (facultatif).
- **Activer** : sélectionnez cette option pour activer le proxy. La valeur par défaut est **ON**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de proxy** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie de Registre

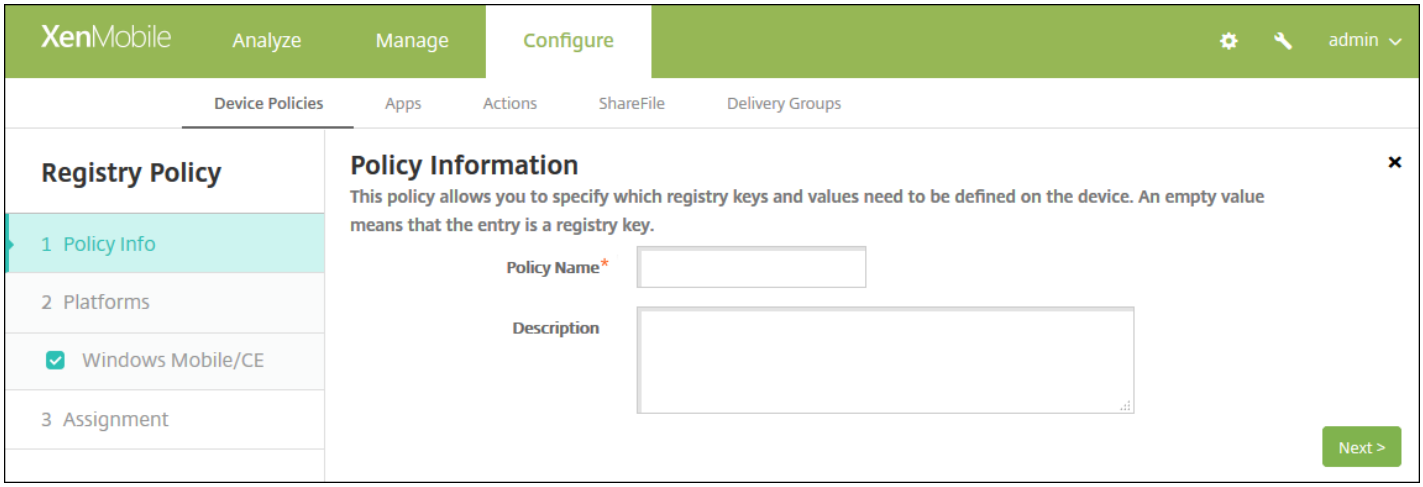
Feb 23, 2017

Le registre Windows Mobile/CE stocke des données sur les applications, pilotes, préférences utilisateur et paramètres de configuration. Dans XenMobile, vous pouvez définir les clés et valeurs de registre qui vous permettent de gérer les appareils Windows Mobile/CE.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

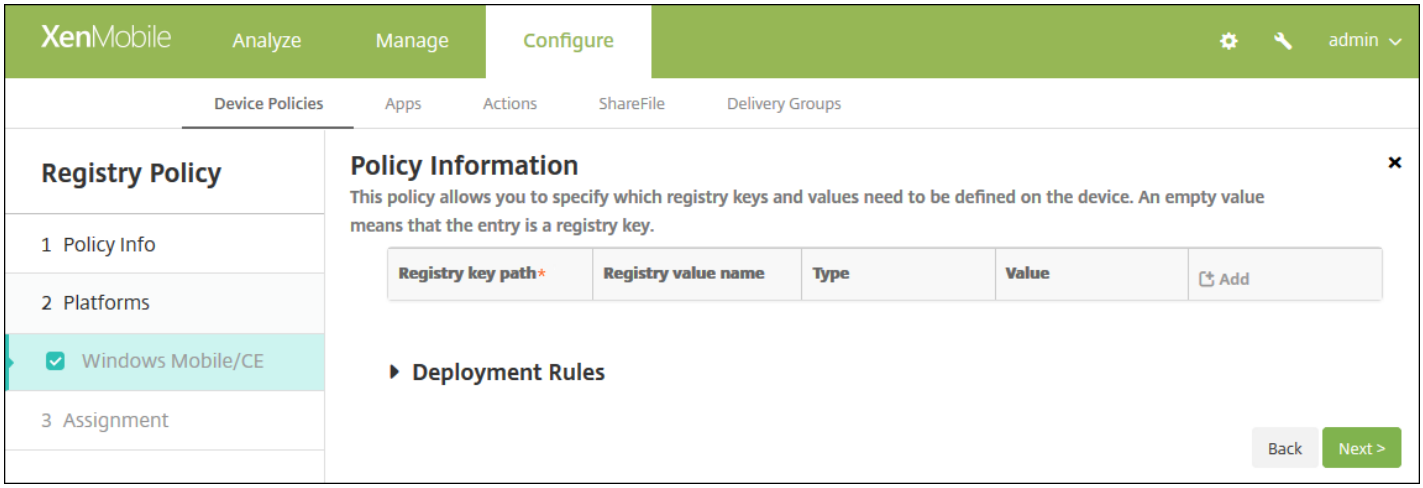
3. Développez **Plus** puis, sous **Personnalisé**, cliquez sur **Registre**. La page d'informations **Stratégie de Registre** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Plate-forme : Windows Mobile/CE** s'affiche.



6. Configurez les paramètres suivants :

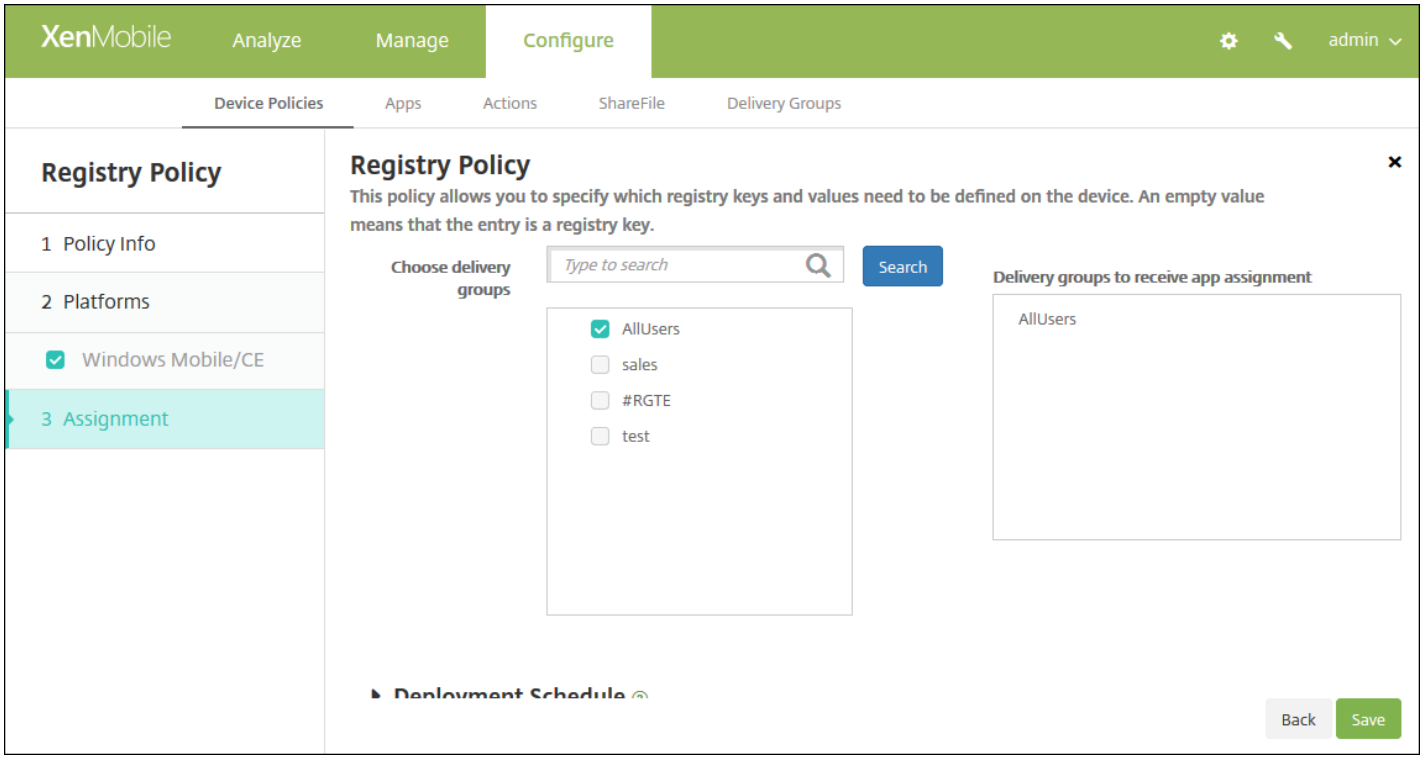
- Pour chaque clé de registre ou paire de clé/valeur de registre que vous souhaitez ajouter, cliquez sur **Ajouter** et procédez comme suit :
- **Chemin d'accès à la clé de Registre** : entrez le chemin d'accès complet pour la clé de registre. Par exemple, tapez *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows* pour spécifier le chemin vers la clé Windows à partir de la clé racine HKEY_LOCAL_MACHINE.
- **Nom de valeur de Registre** : entrez le nom de la valeur de la clé de registre. Par exemple, tapez *ProgramFilesDir* pour ajouter ce nom de valeur au chemin de la clé de registre HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion. Si vous laissez ce champ vide, cela signifie que vous ajoutez une clé de registre et non une paire clé/valeur de registre.
- **Type** : dans la liste, cliquez sur le type de données pour la valeur. La valeur par défaut est **DWORD**. Les options possibles sont les suivantes :
  - **DWORD** : entier non signé 32 bits.
  - **Chaîne** : toute chaîne.
  - **Chaîne étendue** : valeur de chaîne qui peut contenir des variables d'environnement comme %TEMP% ou %USERPROFILE%.
  - **Binaire** : toutes données binaires arbitraires.
- **Valeur** : entrez la valeur associée au nom de la valeur de registre. Par exemple, pour spécifier la valeur de ProgramFilesDir, tapez *C:\Program Files*.
- Cliquez sur **Enregistrer** pour enregistrer les informations de clé de registre ou cliquez sur **Annuler** pour ne pas enregistrer ces informations de clé de registre.

  Remarque : pour supprimer une clé de registre existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur **Supprimer** pour supprimer la liste ou sur **Annuler** pour conserver la liste.

  Pour modifier une clé de registre, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur **Enregistrer** pour enregistrer la nouvelle liste ou sur **Annuler** pour laisser la liste inchangée.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie de Registre** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégie d'assistance à distance

Feb 23, 2017

Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX des utilisateurs. Vous pouvez configurer deux types d'assistance :

- **Assistance à distance de base** : cette option vous permet d'afficher des informations de diagnostic sur l'appareil, telles que les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés, etc.
- **Assistance à distance premium** : cette option vous permet de contrôler à distance l'écran de l'appareil, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.

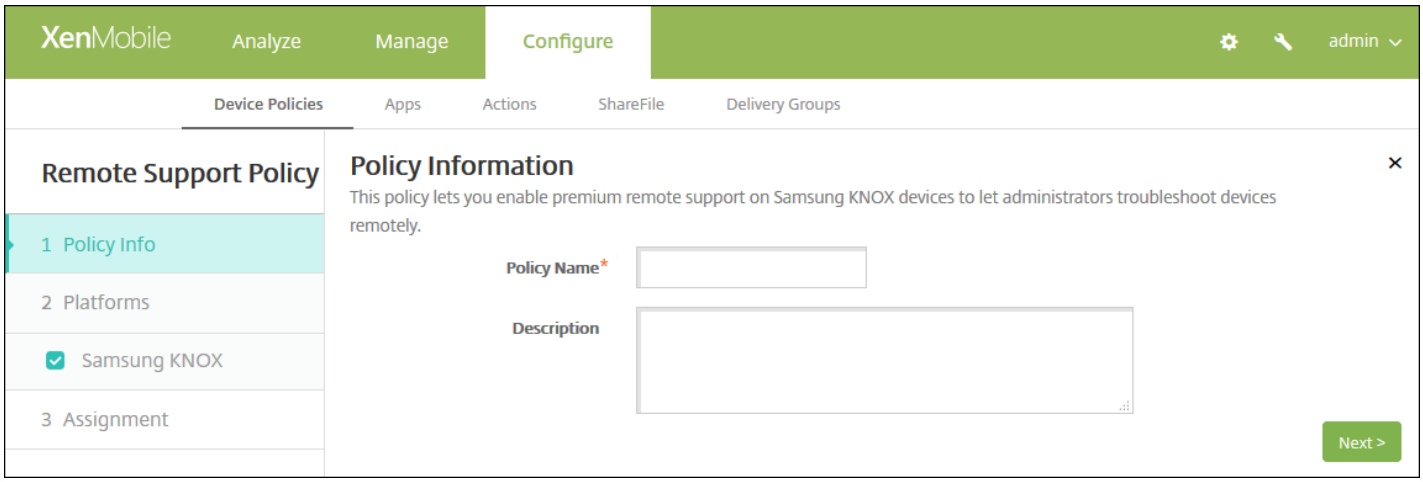
Remarque : pour implémenter cette stratégie, vous devez effectuer les tâches suivantes :

- Installez l'application d'assistance à distance XenMobile dans votre environnement.
- Configurez un tunnel applicatif d'assistance à distance. Pour plus de détails, consultez la section Stratégies de tunnel applicatif.
- Configurez une stratégie d'assistance à distance Samsung KNOX comme décrit dans cette rubrique.
- Déployez la stratégie de tunnel applicatif à utiliser pour l'assistance à distance et la stratégie d'assistance à distance Samsung KNOX sur les appareils des utilisateurs.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

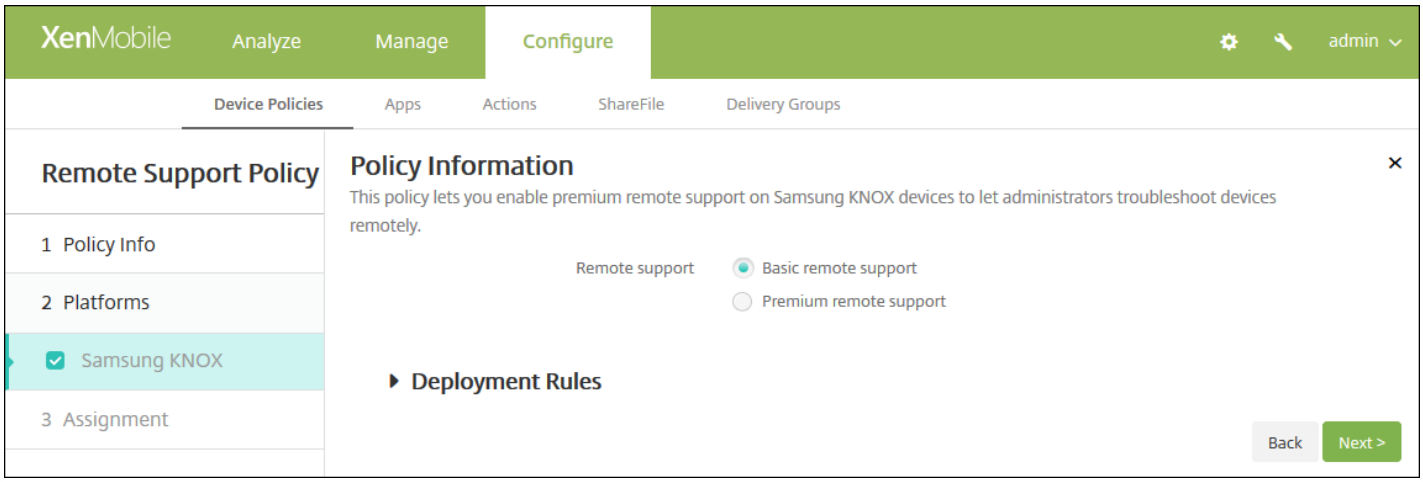
3. Développez **Plus**, puis, sous **Accès réseau**, cliquez sur **Assistance à distance**. La page **Stratégie d'assistance à distance** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations sur la plate-forme **Samsung KNOX** s'affiche.

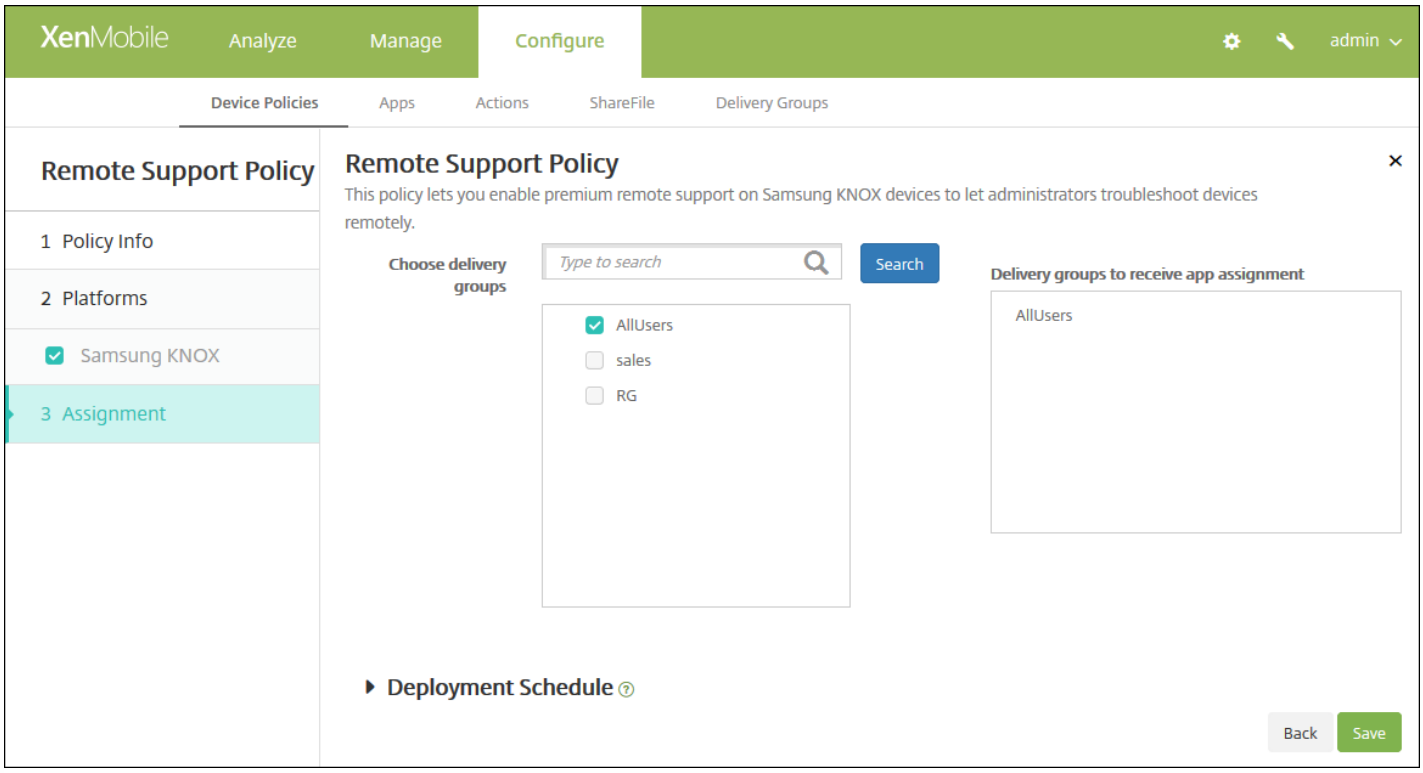


6. Configurez ce paramètre :

- **Assistance à distance** : sélectionnez **Assistance à distance de base** ou **Assistance à distance premium**. La valeur par défaut est **Assistance à distance de base**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Next**. La page d'attribution de la **Stratégie d'assistance à distance** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Stratégies de restrictions

Feb 23, 2017

Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour limiter l'accès des utilisateurs à certaines fonctionnalités sur leurs appareils, téléphones, tablettes, etc. Vous pouvez configurer la stratégie de restrictions pour les plates-formes suivantes : iOS, Mac OS X, Samsung SAFE, Samsung KNOX, tablettes Windows, Windows Phone, Amazon et Windows Mobile/CE. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Cette stratégie permet ou empêche les utilisateurs d'utiliser certaines fonctionnalités sur leurs appareils, telles que l'appareil photo. Vous pouvez également définir des restrictions de sécurité, des restrictions d'accès au contenu multimédia ainsi que des restrictions sur les types d'applications que les utilisateurs peuvent ou ne peuvent pas installer. La plupart des paramètres de restriction sont réglés par défaut sur **ON** ou *autorise*. Les principales exceptions sont la fonctionnalité Sécuriser - Forcer dans iOS et toutes les fonctionnalités de Windows Tablet, lesquelles prennent par défaut la valeur **OFF** ou appliquent des *restrictions*.

Conseil : toute option définie sur **ON** signifie que l'utilisateur

— peut

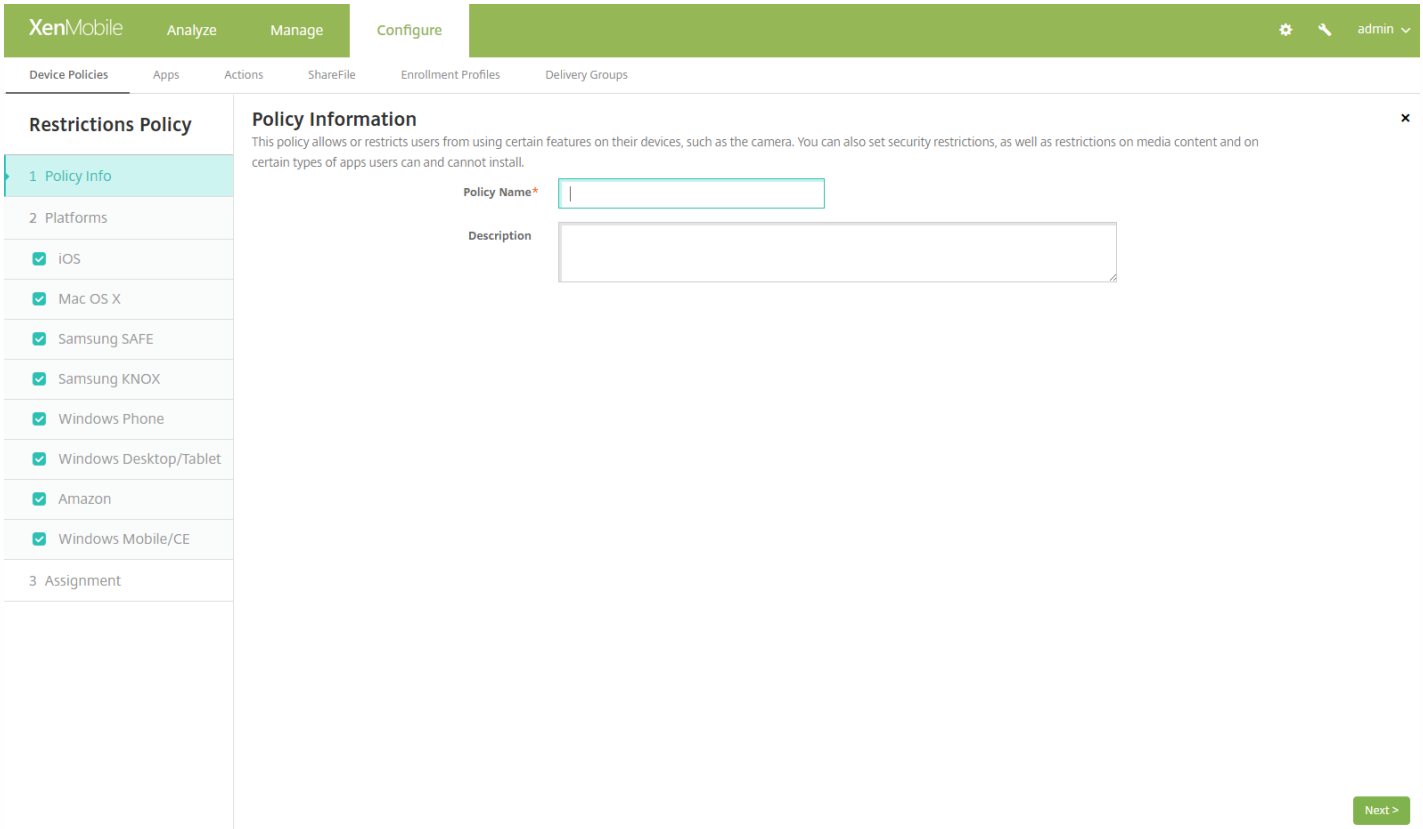
effectuer l'opération ou utiliser la fonctionnalité. Par exemple :

- **Appareil photo**. Si l'option est réglée sur **ON**, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur **OFF**, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil.
- **Captures d'écrans**. Si l'option est réglée sur **ON**, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur **OFF**, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**.La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La page **Ajouter une nouvelle stratégie** apparaît.

3. Cliquez sur **Restrictions**. La page d'informations **Stratégie de restrictions** s'affiche.



4. Dans le panneau **Informations sur la stratégie**, entrez les informations suivantes :

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

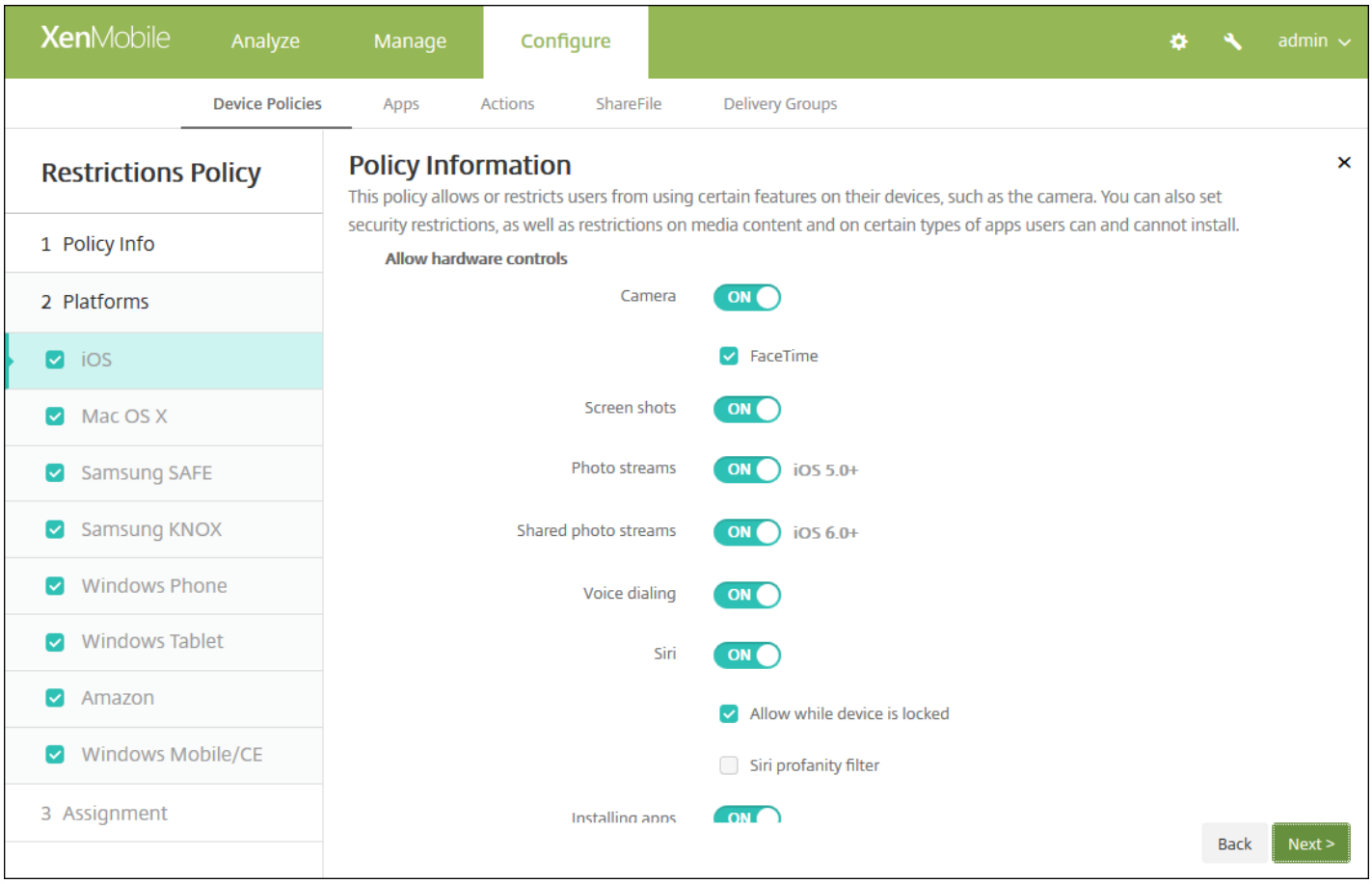
4. Cliquez sur **Next**. La page **Stratégie par plate-forme** s'affiche.

5. Sous **Plates-formes**, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter. Vous pouvez ensuite modifier les informations de stratégie pour chaque plate-forme que vous avez sélectionnée. Cliquez pour limiter les fonctionnalités dans les sections suivantes, ce qui désactive le paramètre (**OFF**). Sauf spécification contraire, la fonctionnalité est activée par défaut.

Si vous avez sélectionné :
iOS, configurez ces paramètres
Mac OS X, configurez ces paramètres
Samsung SAFE, configurez ces paramètres
Samsung KNOX, configurez ces paramètres
Windows Phone, configurez ces paramètres
Windows Tablet, configurez ces paramètres
Amazon, configurez ces paramètres
Windows Mobile/CE, configurez ces paramètres

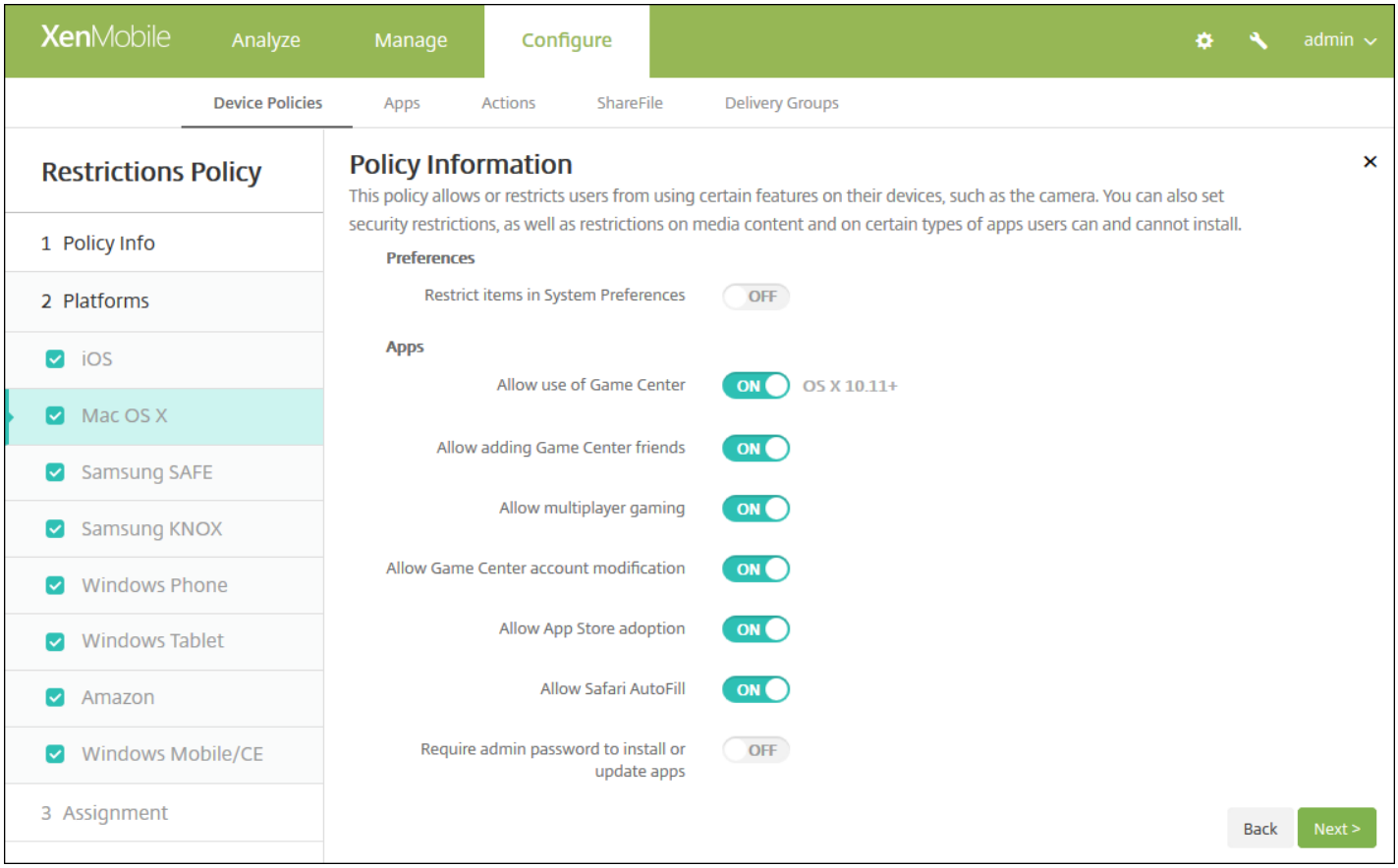
Une fois que vous avez fini de définir des restrictions pour une plate-forme, reportez-vous à l'étape 7 plus loin dans cet article pour savoir comment configurer les règles de déploiement de cette plate-forme.

Si vous avez sélectionné iOS, configurez les paramètres suivants.



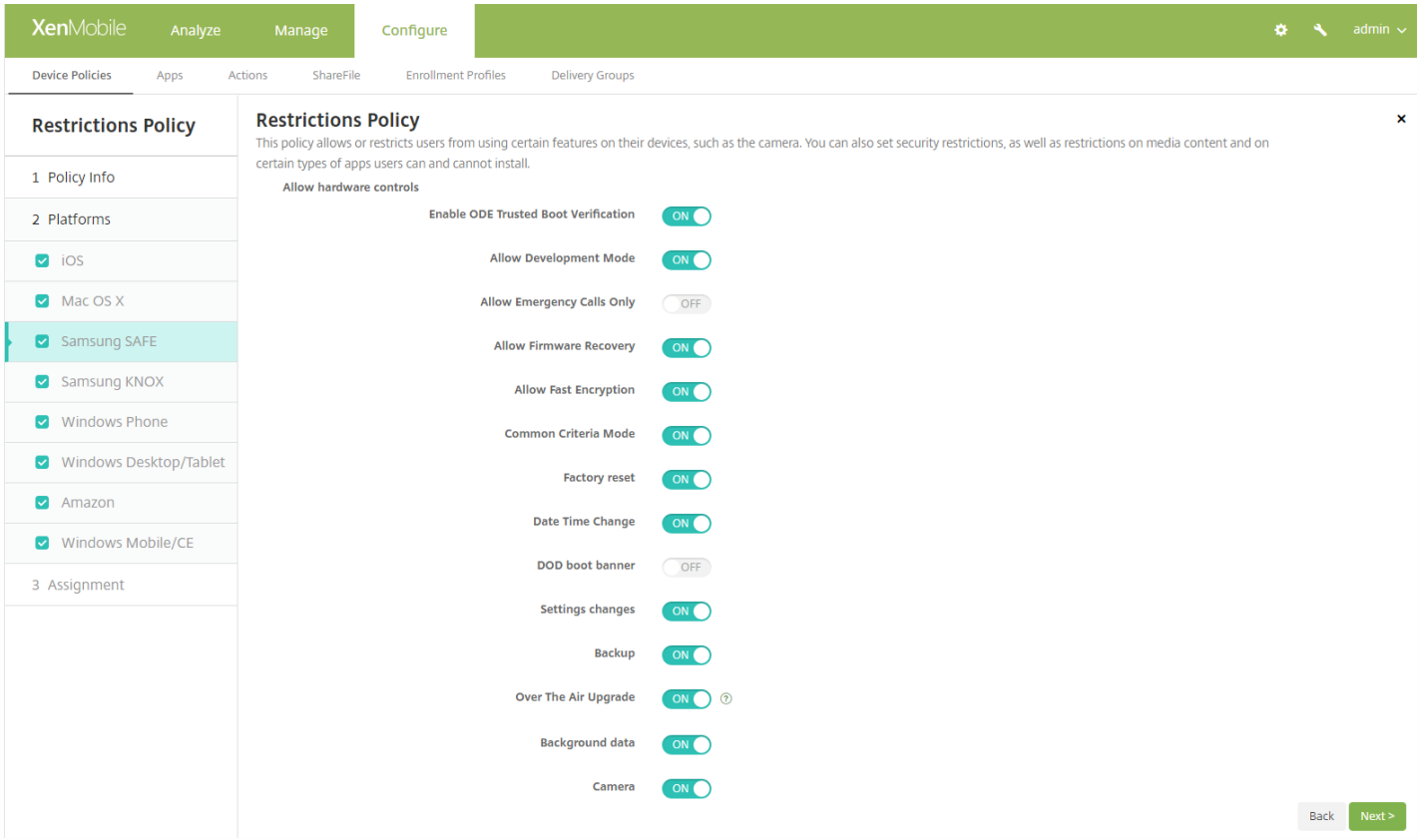
Paramètres iOS

Configurer les paramètres pour Mac OS X



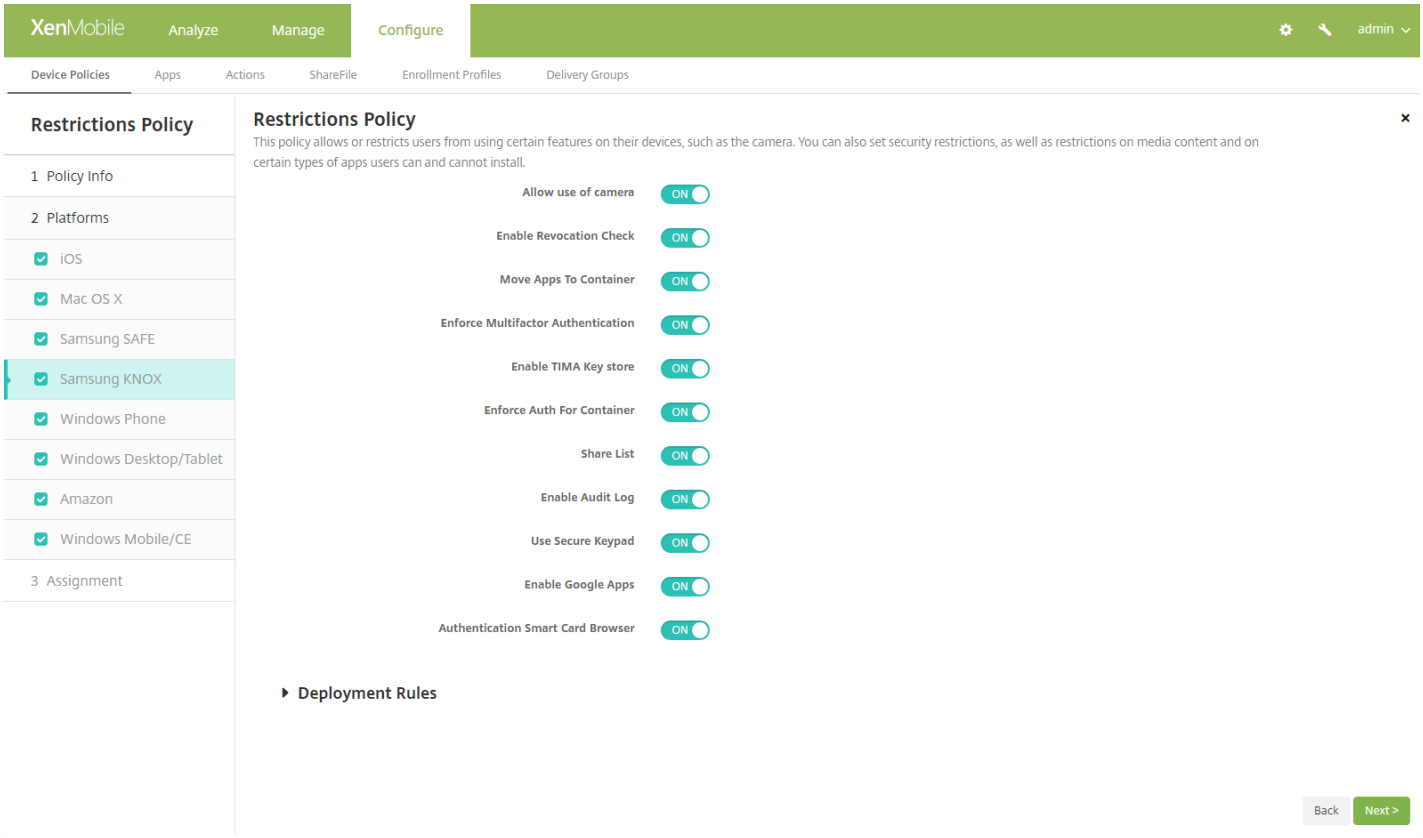
Paramètres Mac OS X

Configurer les paramètres pour Samsung SAFE



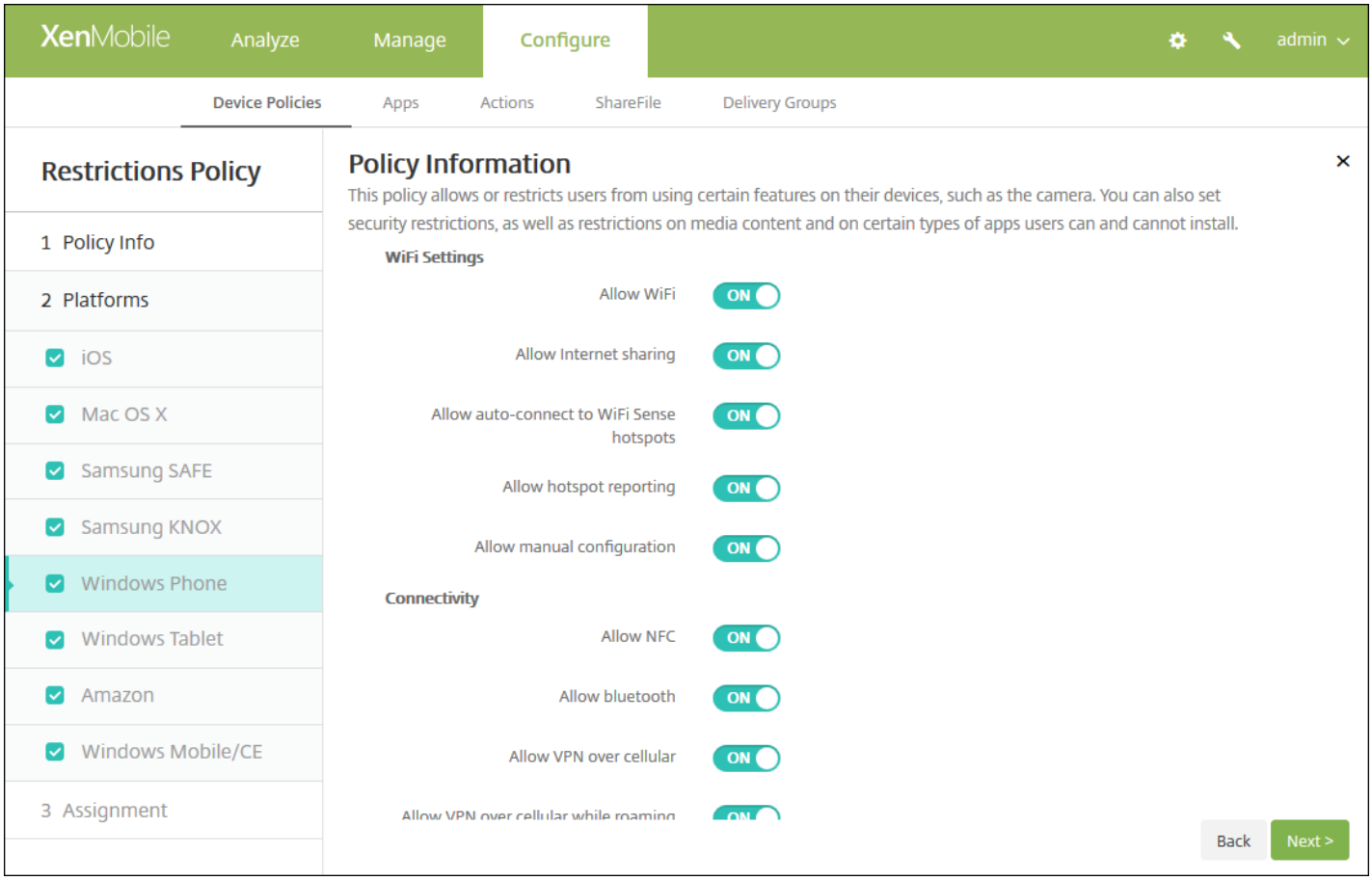
Paramètres Samsung SAFE

Configurer les paramètres pour Samsung KNOX



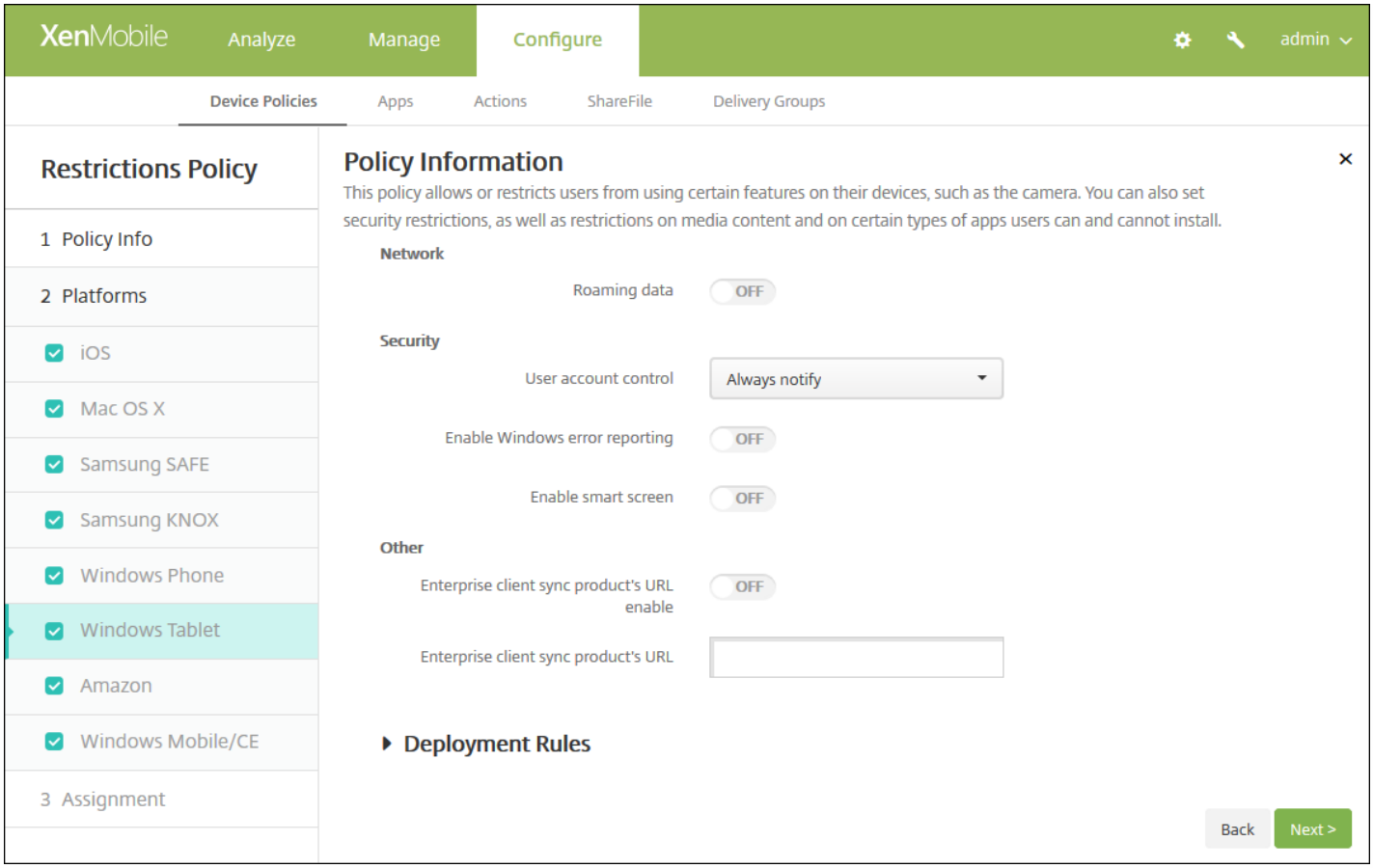
Paramètres Samsung KNOX

Configurer les paramètres pour Windows Phone



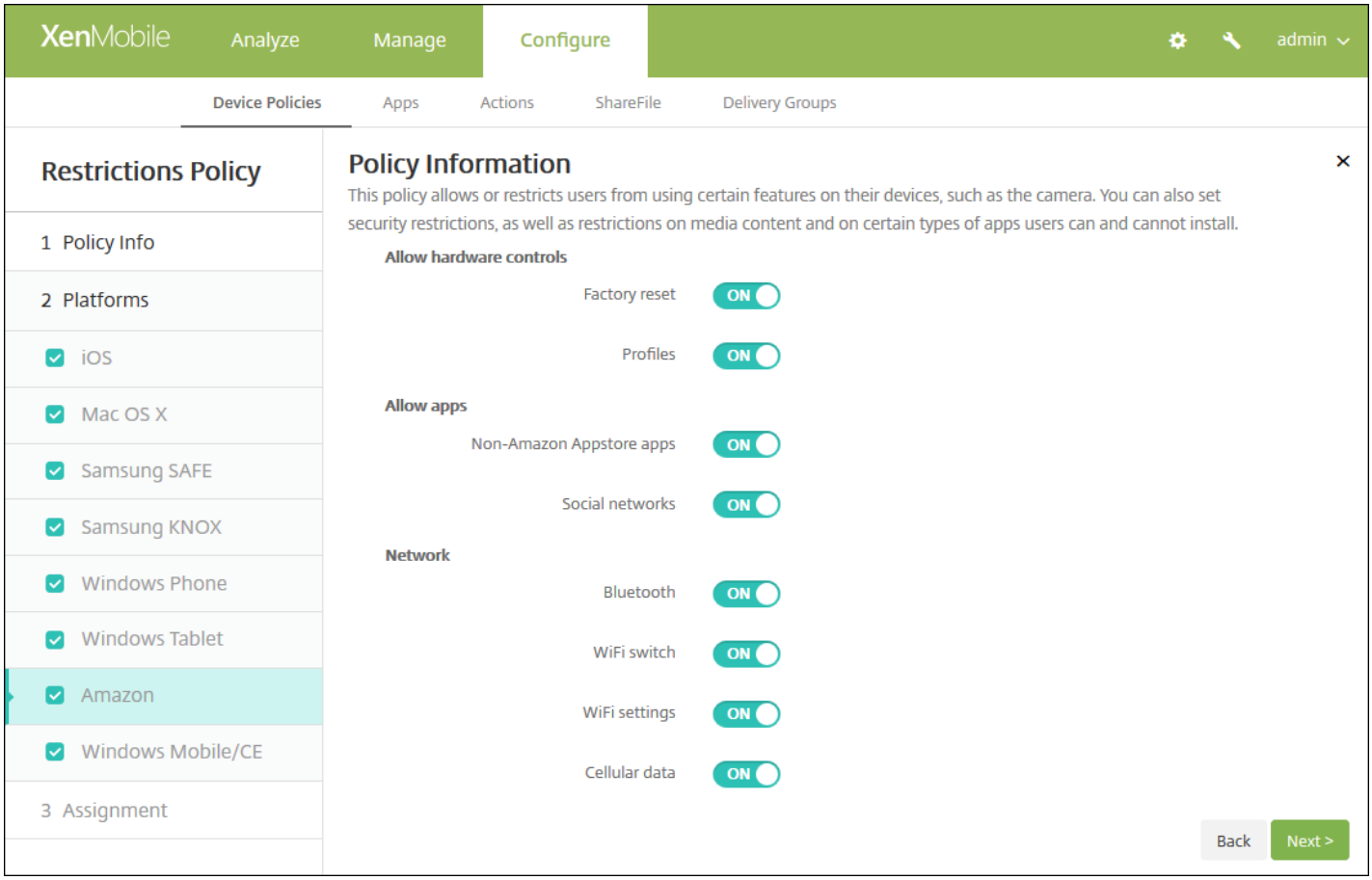
Paramètres Windows Phone

Configurer les paramètres pour Windows Desktop/Tablet



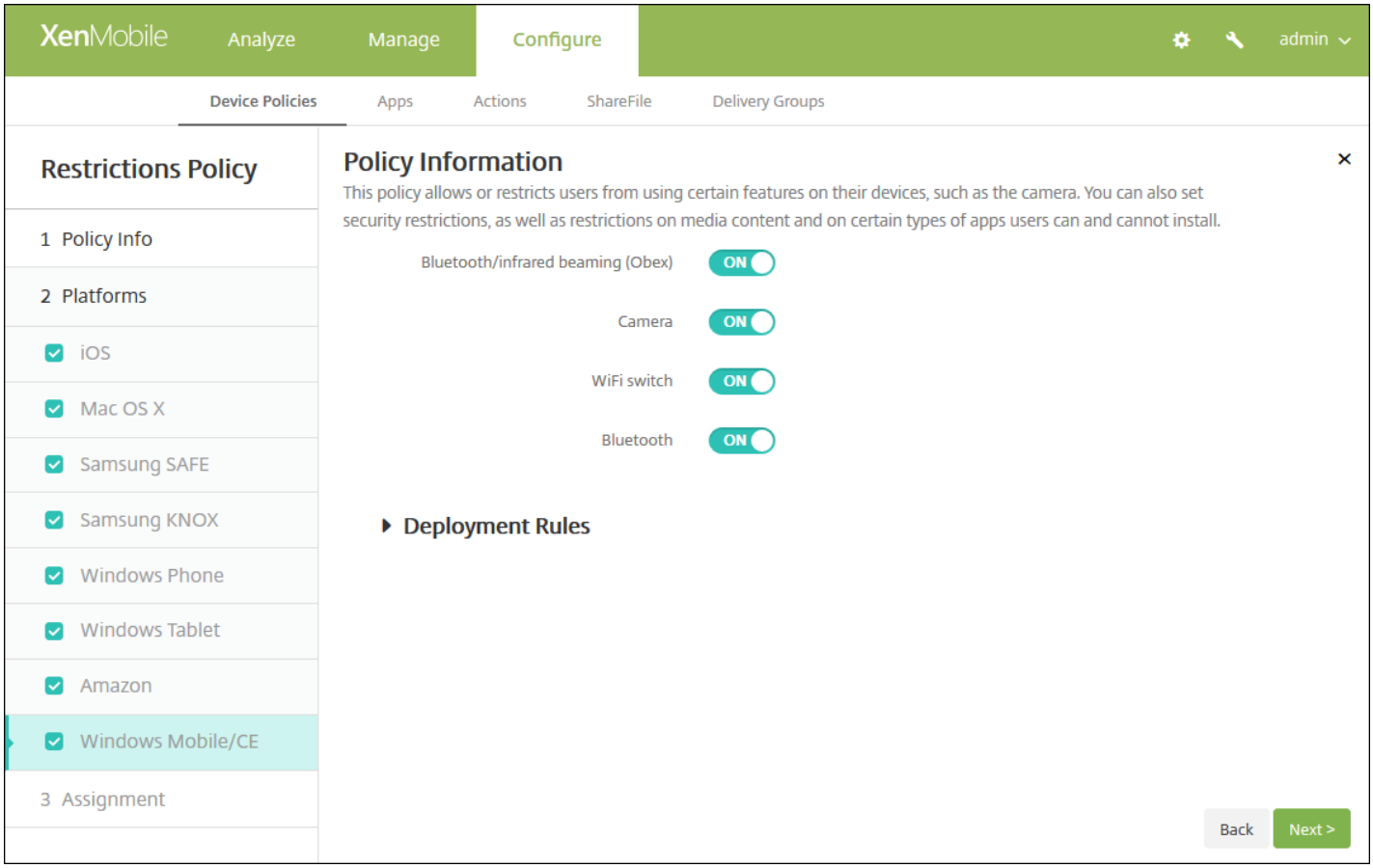
Paramètres Windows Desktop/Tablet

Configurer les paramètres pour Amazon



Paramètres Amazon

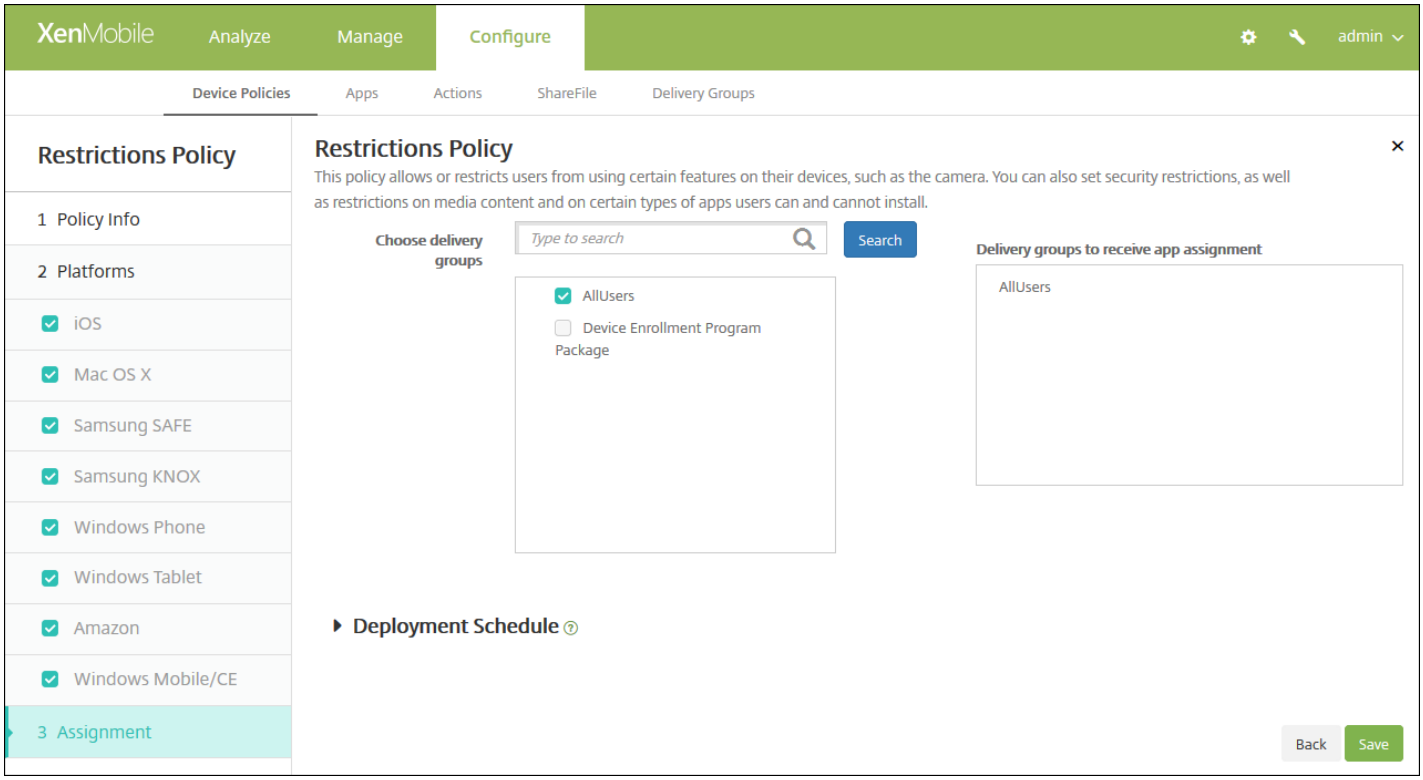
Configurer les paramètres pour Windows Mobile/CE



Paramètres Windows Mobile/CE

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**, la page d'attribution de **Stratégie de restrictions** s'affiche.



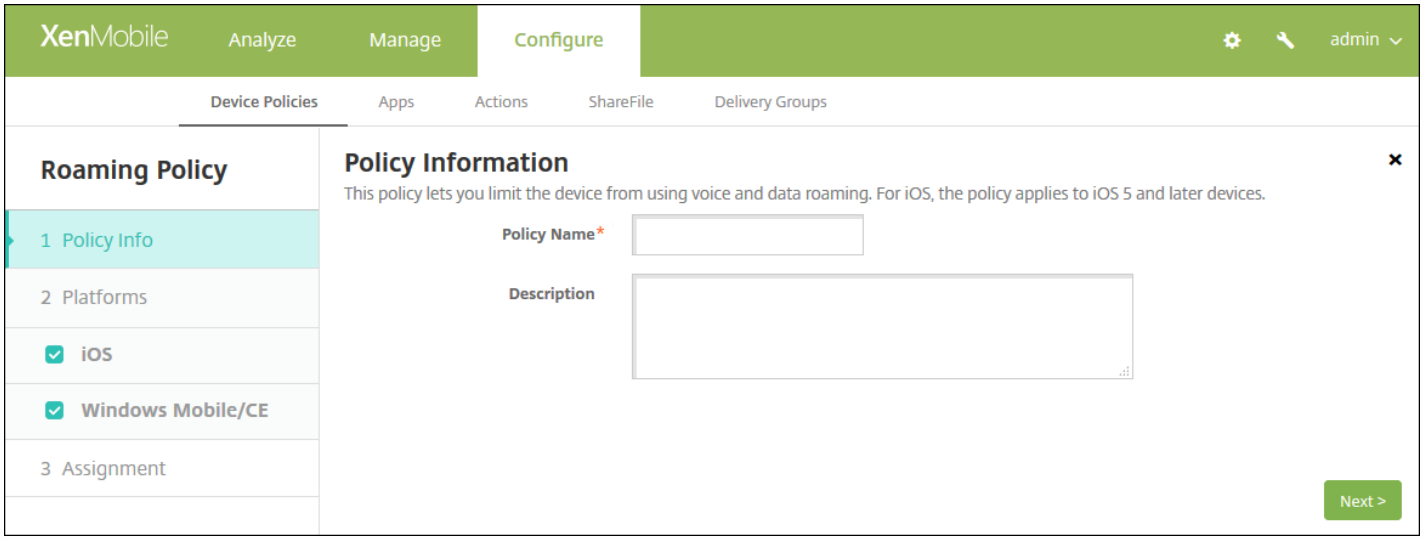
9. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

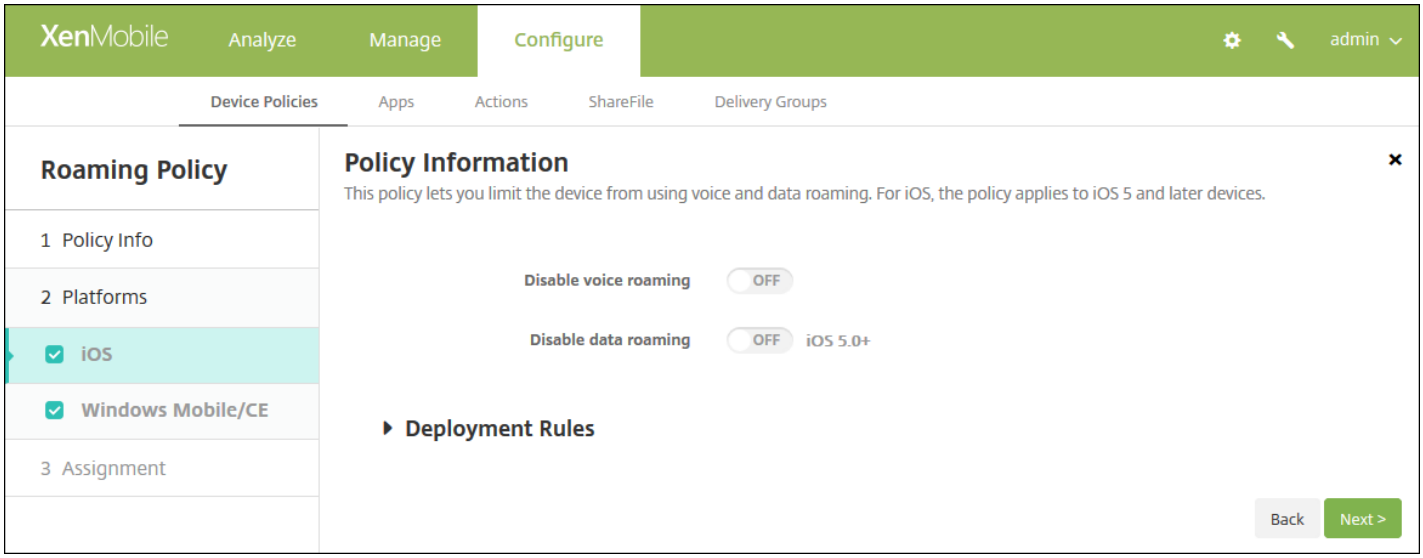
- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

10. Cliquez sur **Enregistrer** pour enregistrer la stratégie.



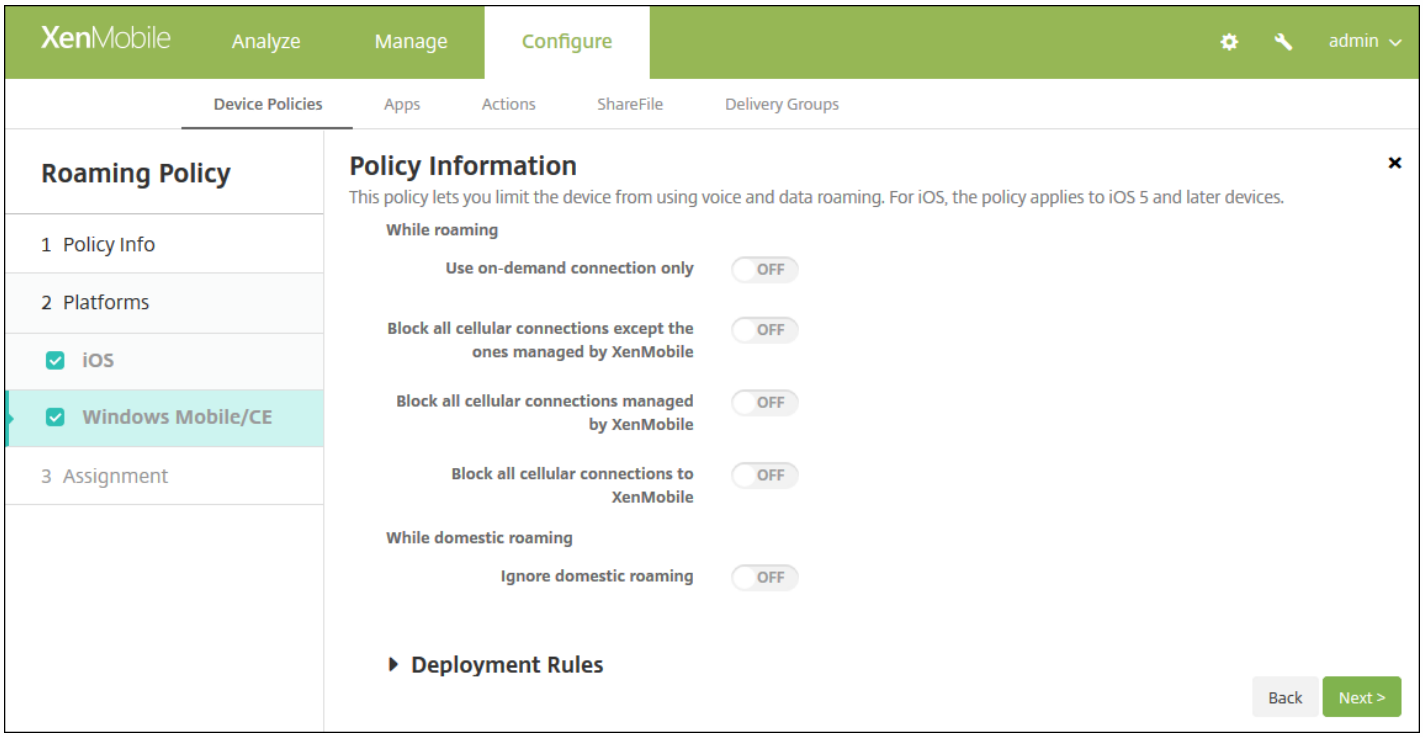
-
-

Configurer les paramètres pour iOS



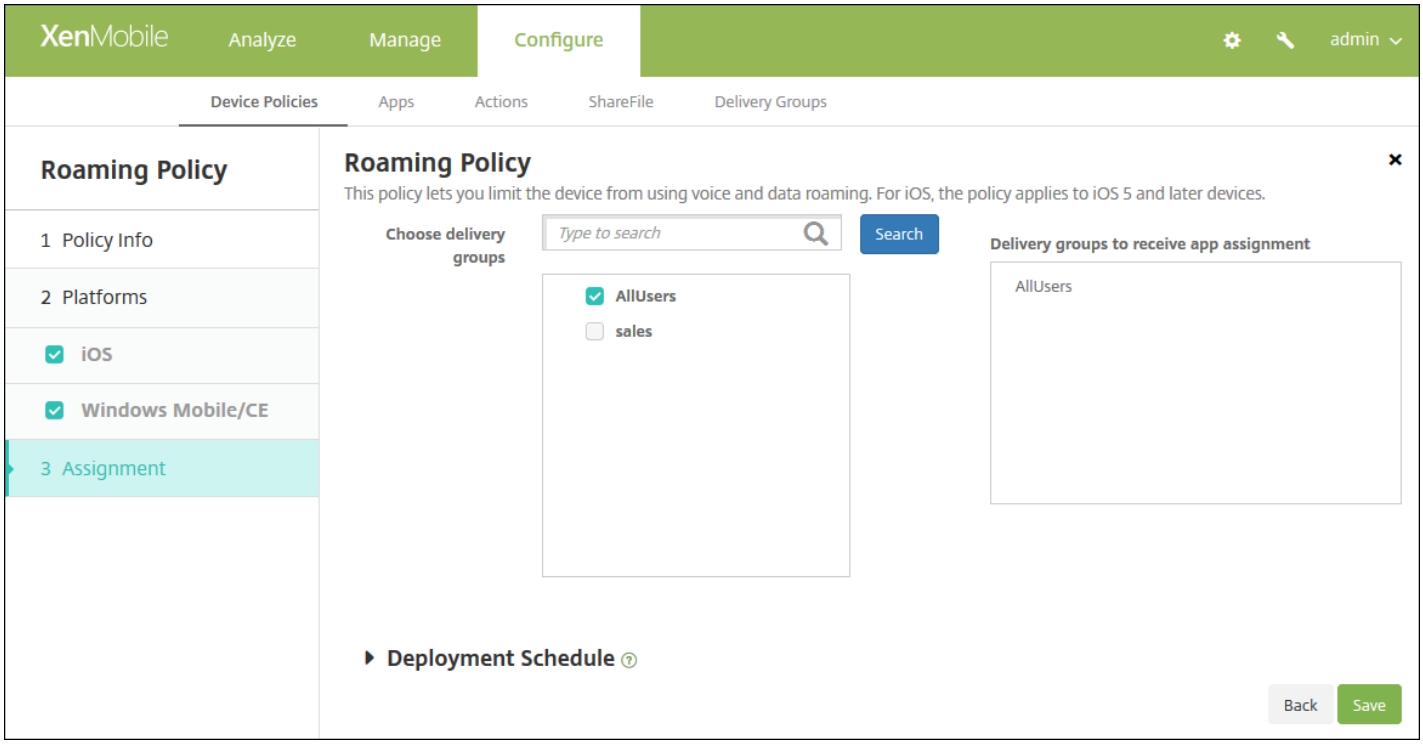
-
-

Configurer les paramètres pour Windows Mobile/CE

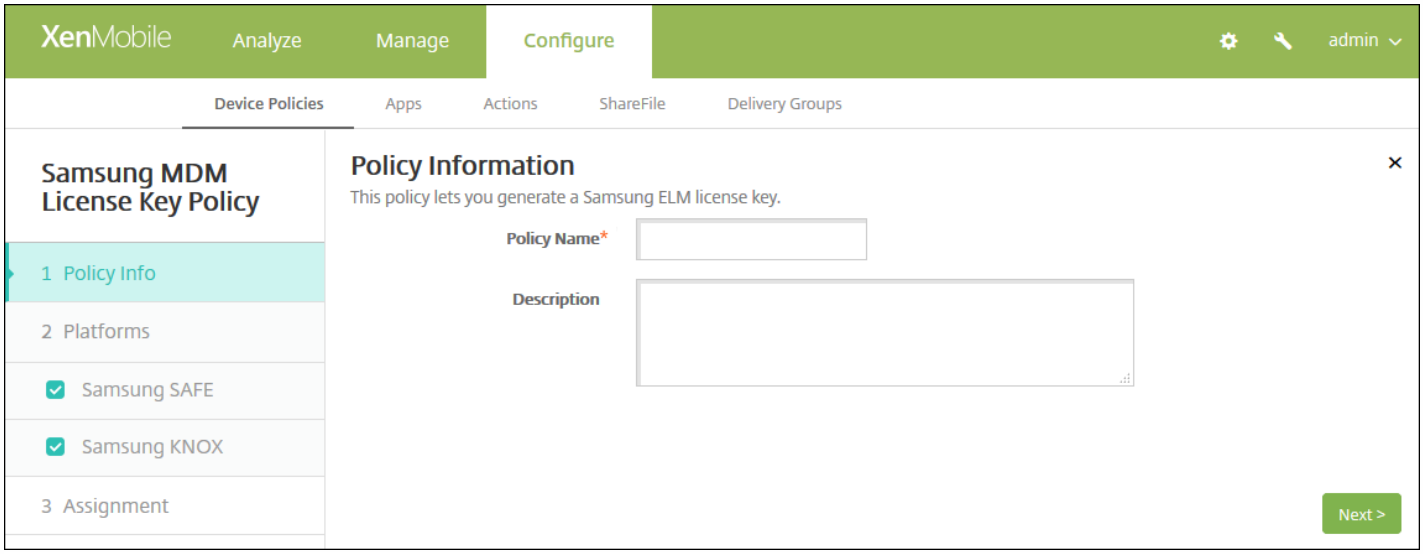


-
  -
  -
  -
  -
-
  -

7. Configurez les règles de déploiement.

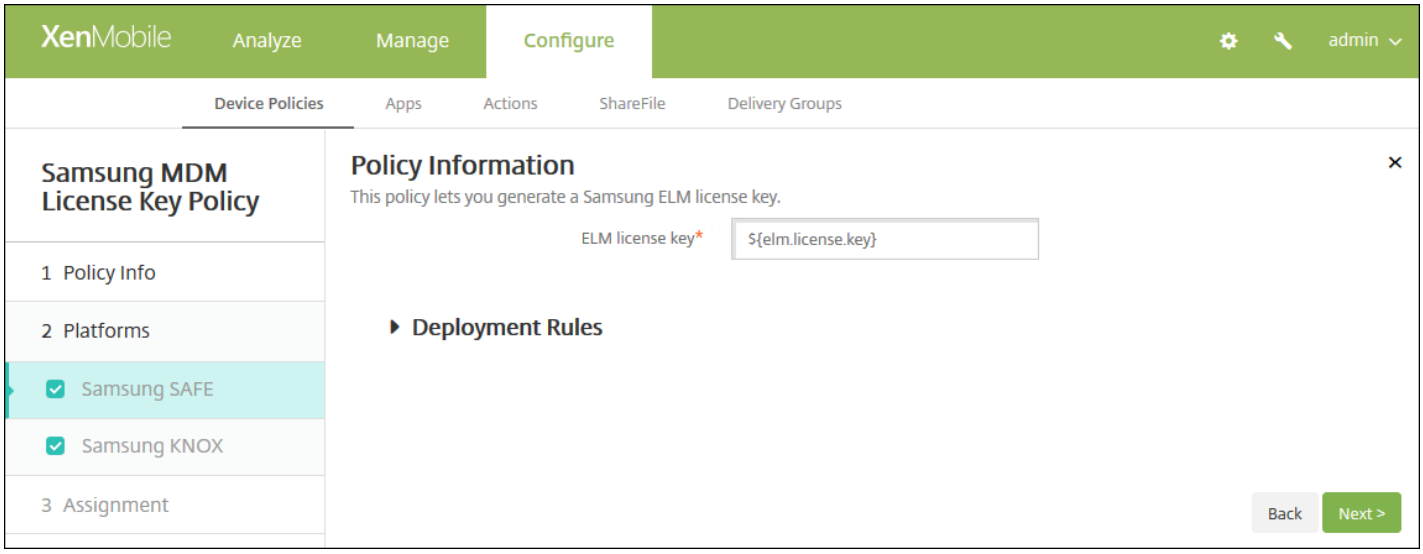


-
-
-
-
-
-
-



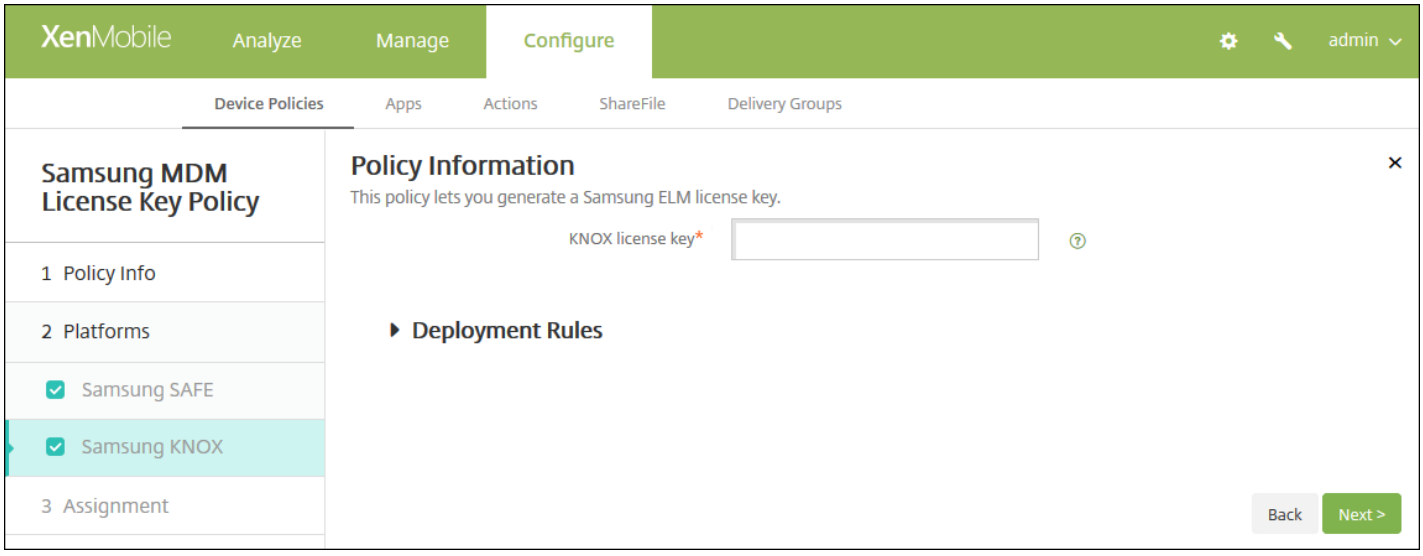
-

Configurer les paramètres pour Samsung SAFE



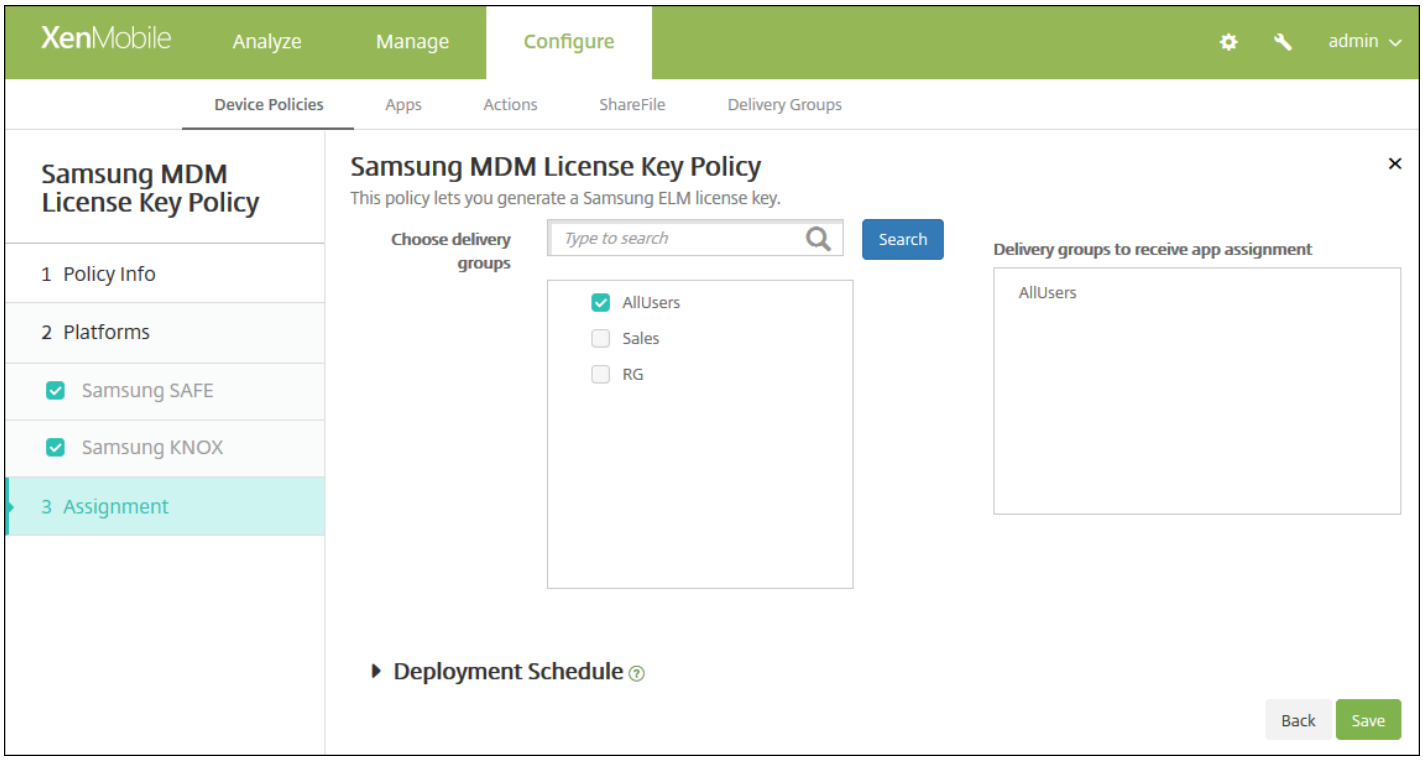
-

Configurer les paramètres pour Samsung KNOX



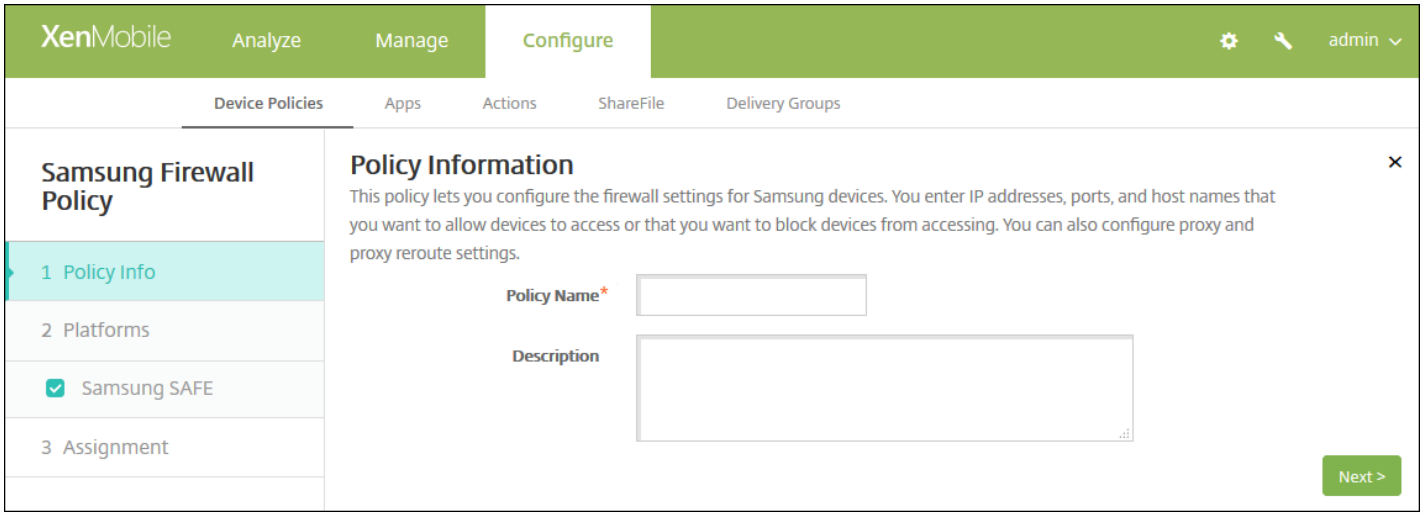
-

7. Configurez les règles de déploiement.

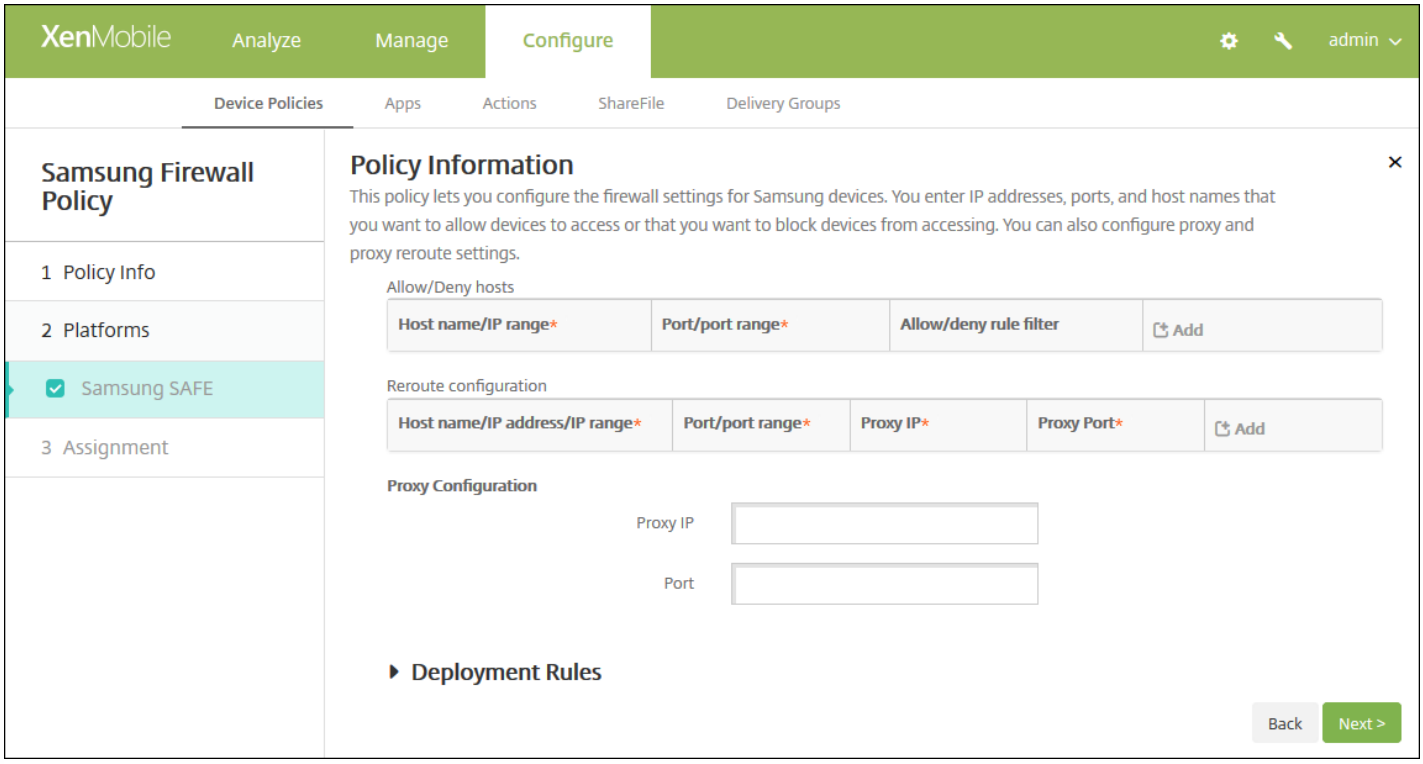


-
-
-
-
-

-
-



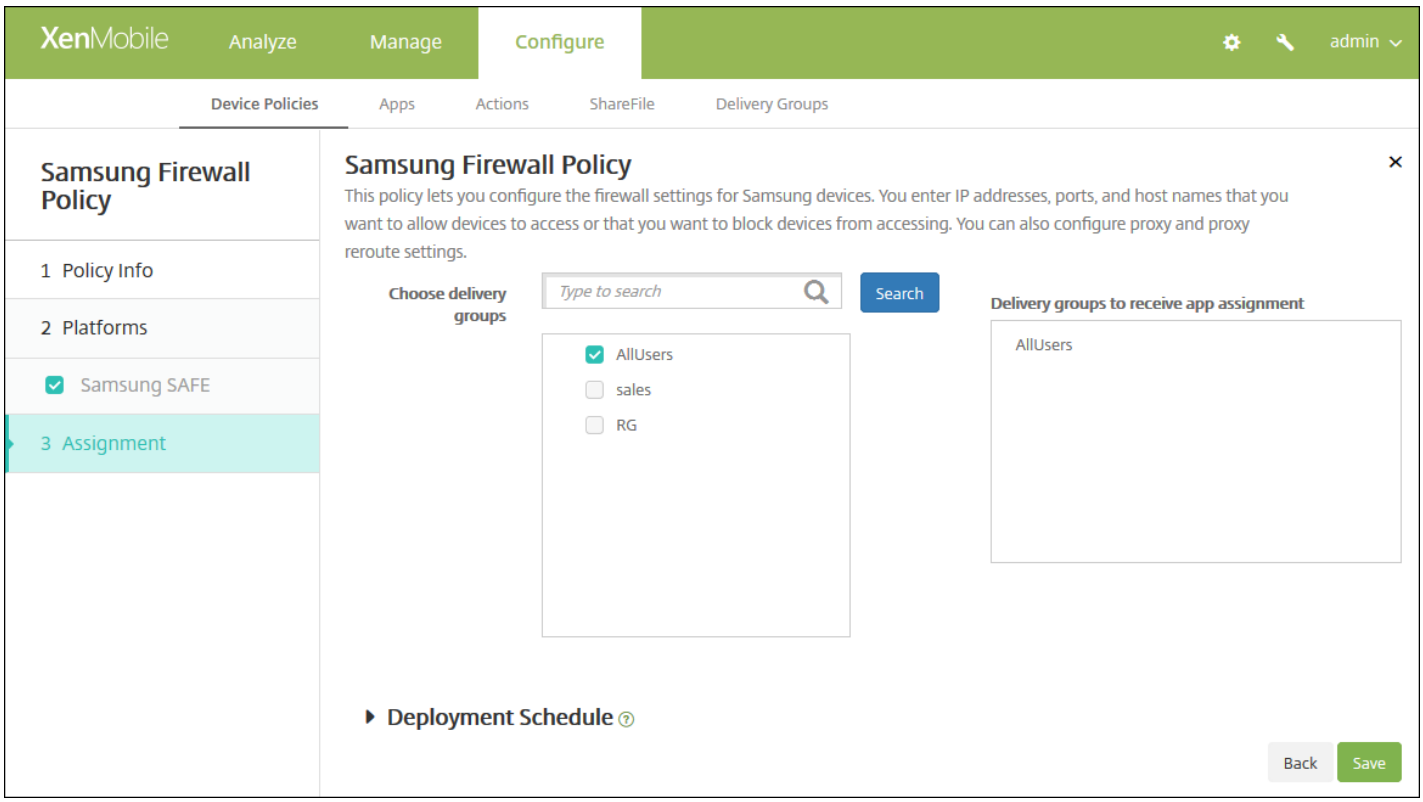
-
-



-
  -
    -
    -
    -
    -
-
  -
    -
    -
    -
    -
    -

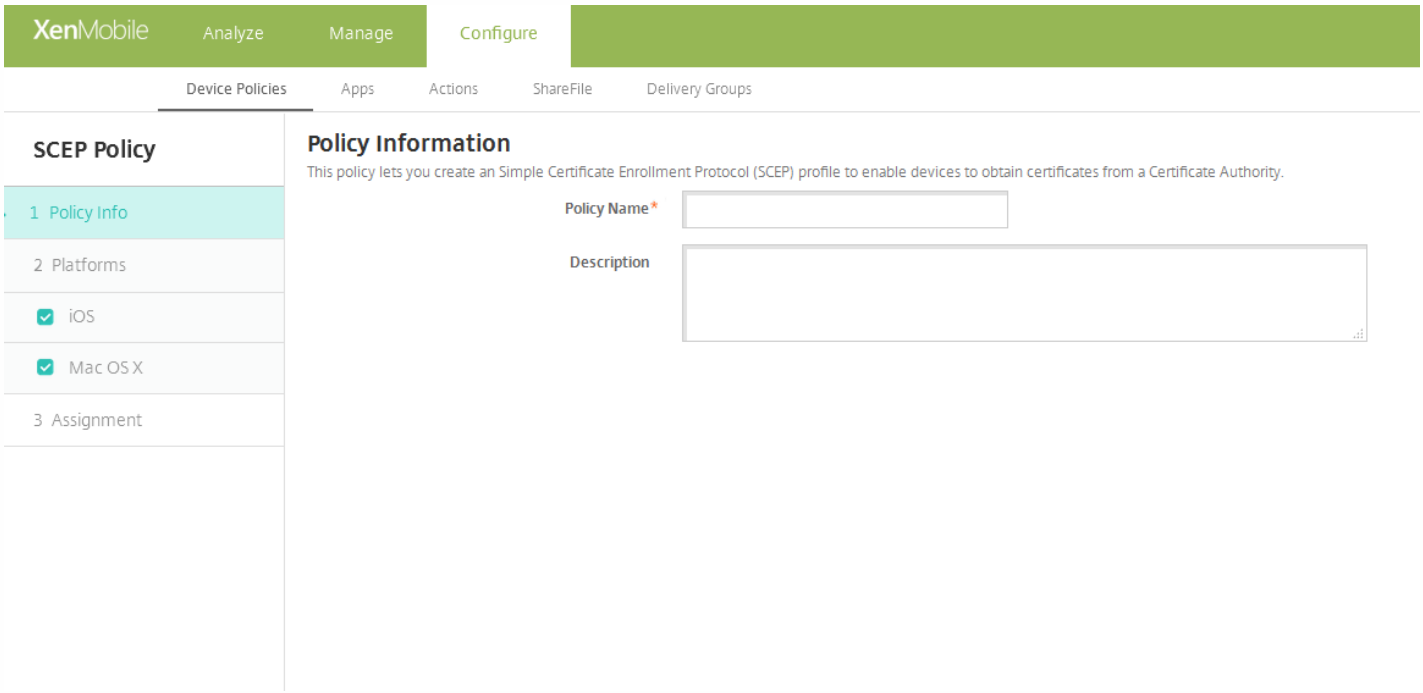
-
  -
  -

7. Configurez les règles de déploiement.



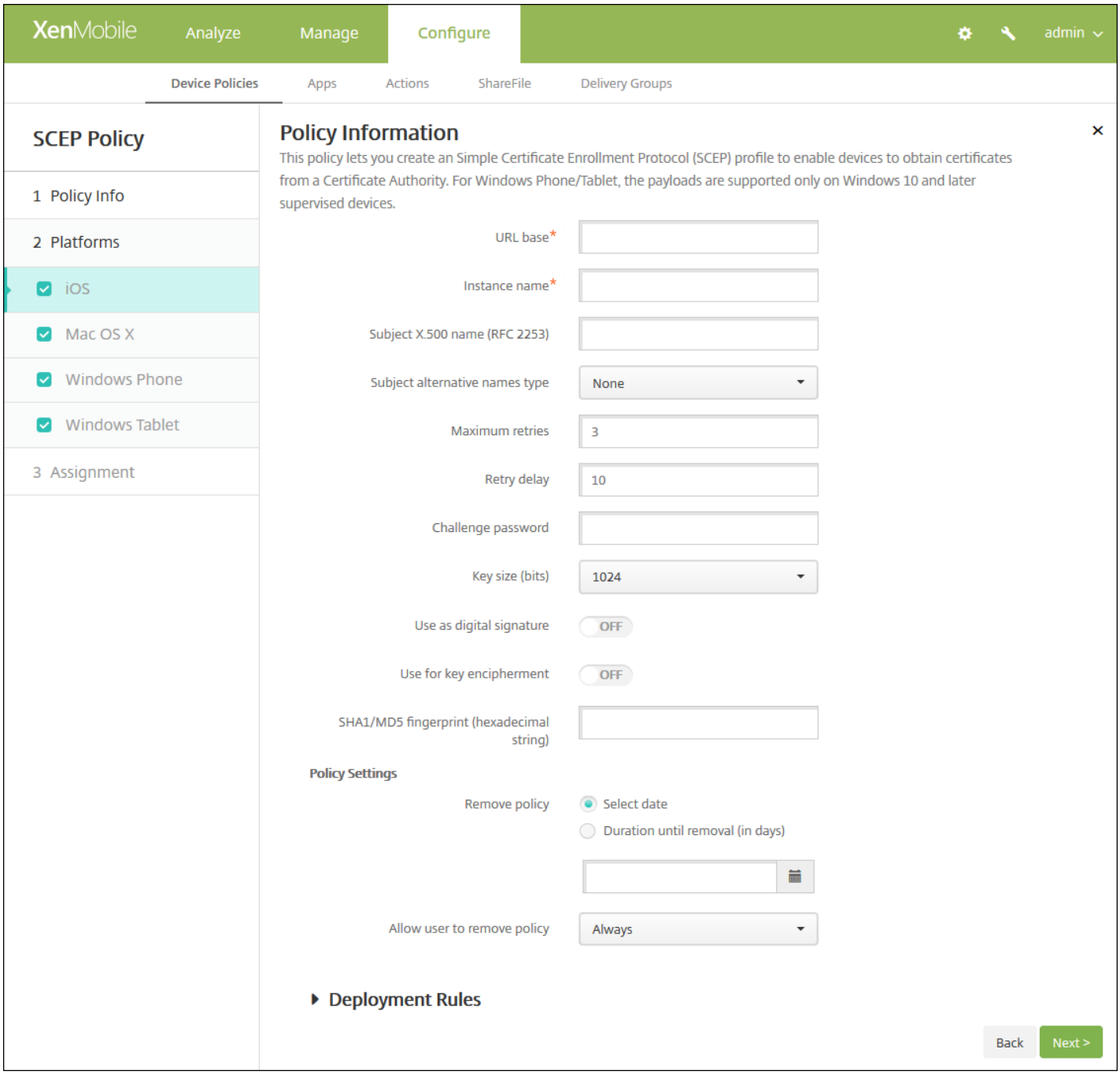
-
-
-
-
-

-
-



-
-

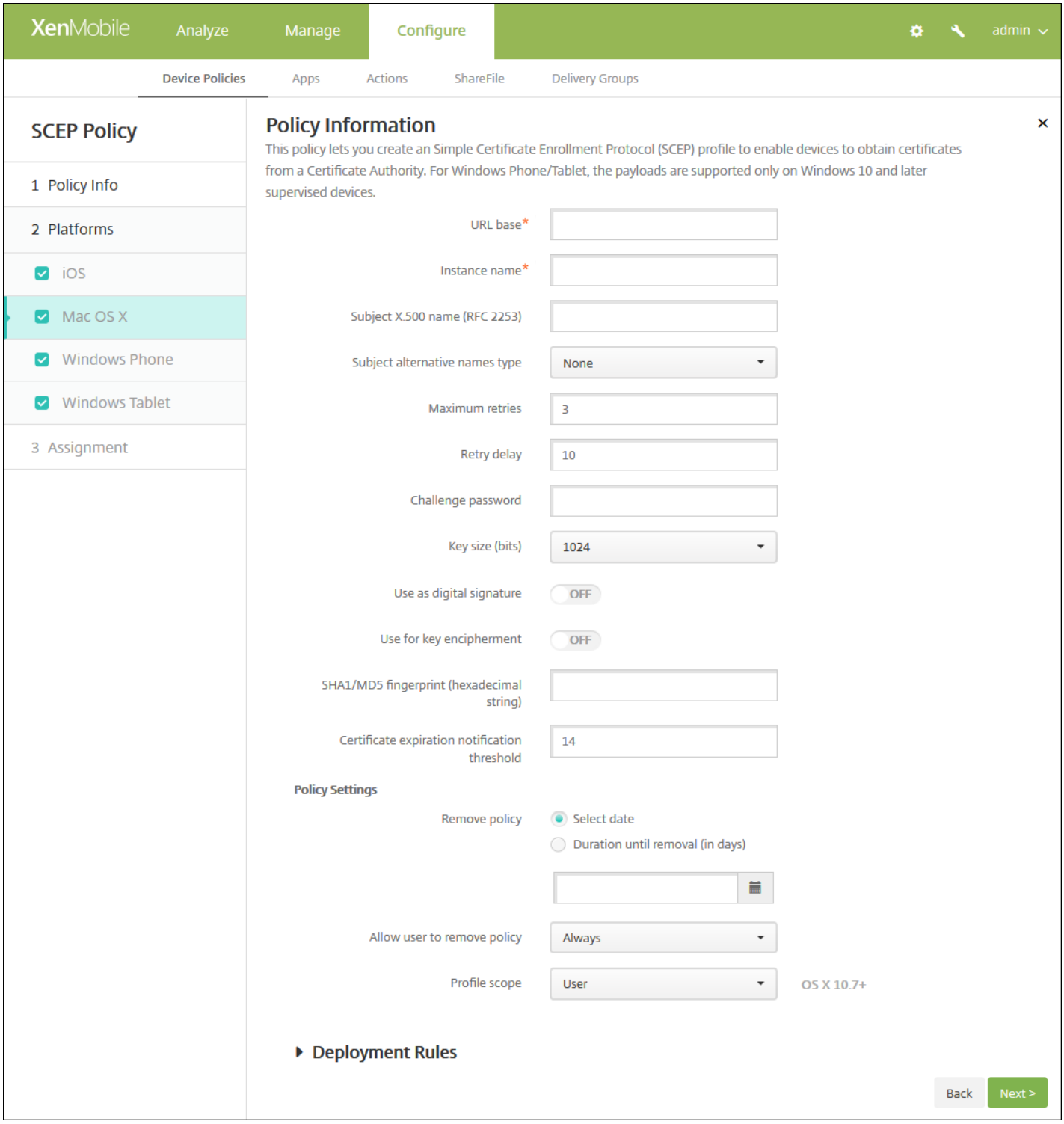
Configurer les paramètres pour iOS



•

-
-
-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -

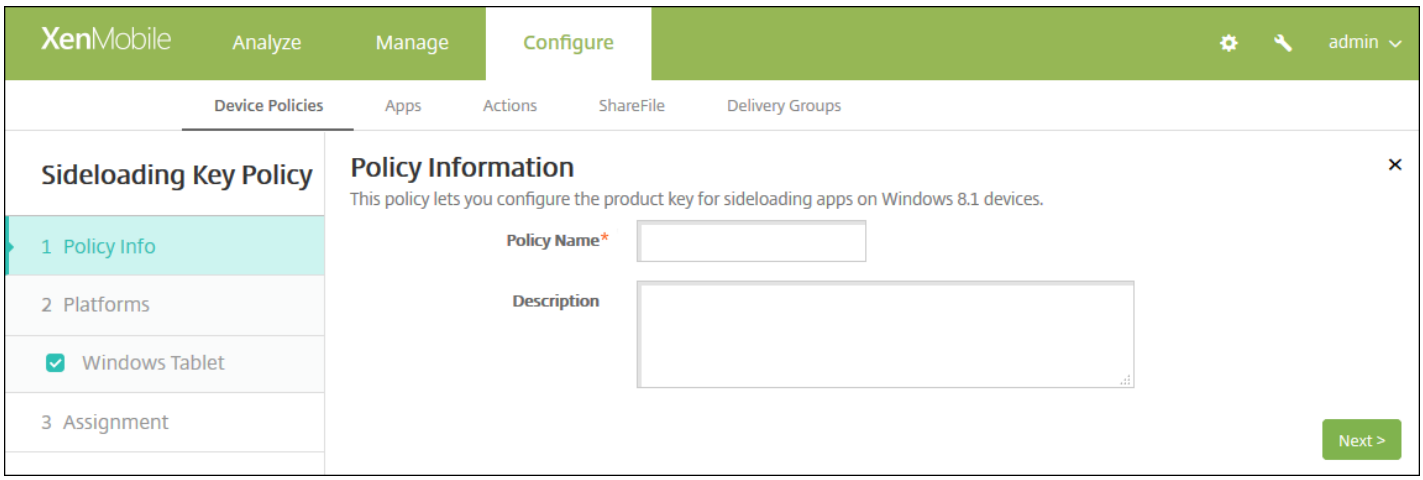
Configurer les paramètres pour Mac OS X



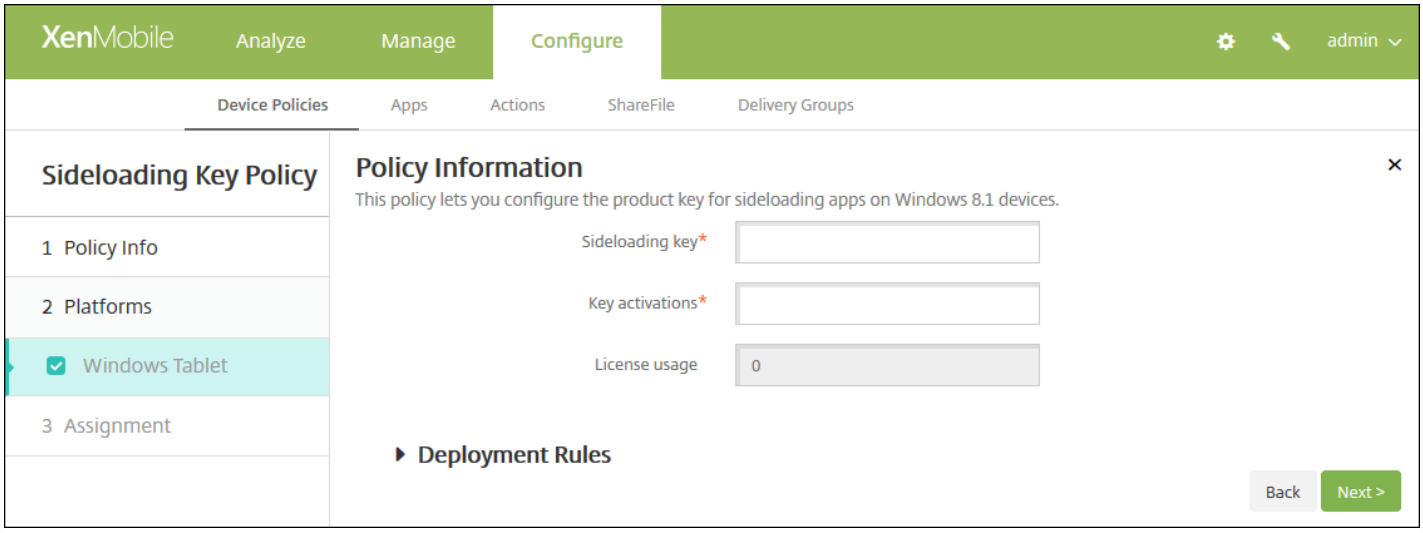
7. Configurez les règles de déploiement.

-
-
-
-
-
-
-

-
-

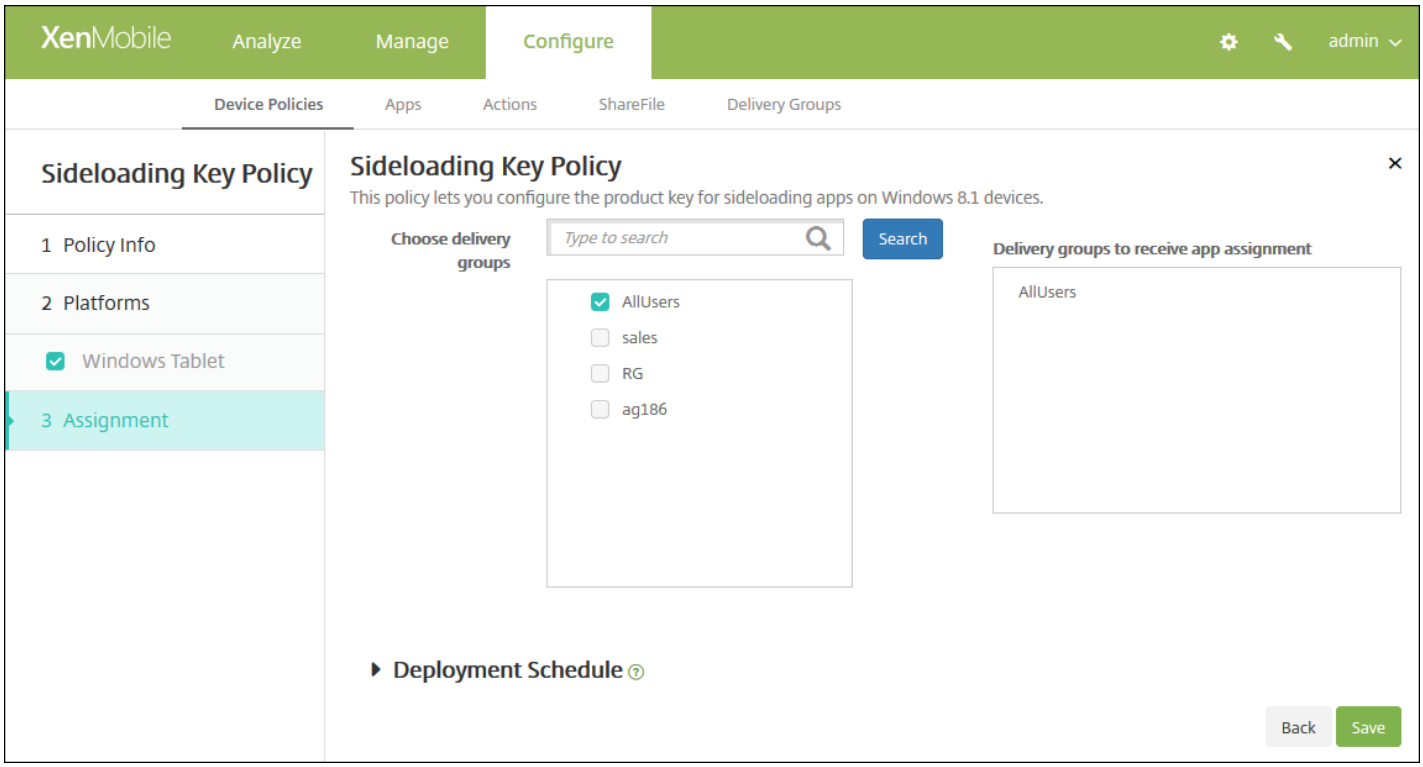


-
-

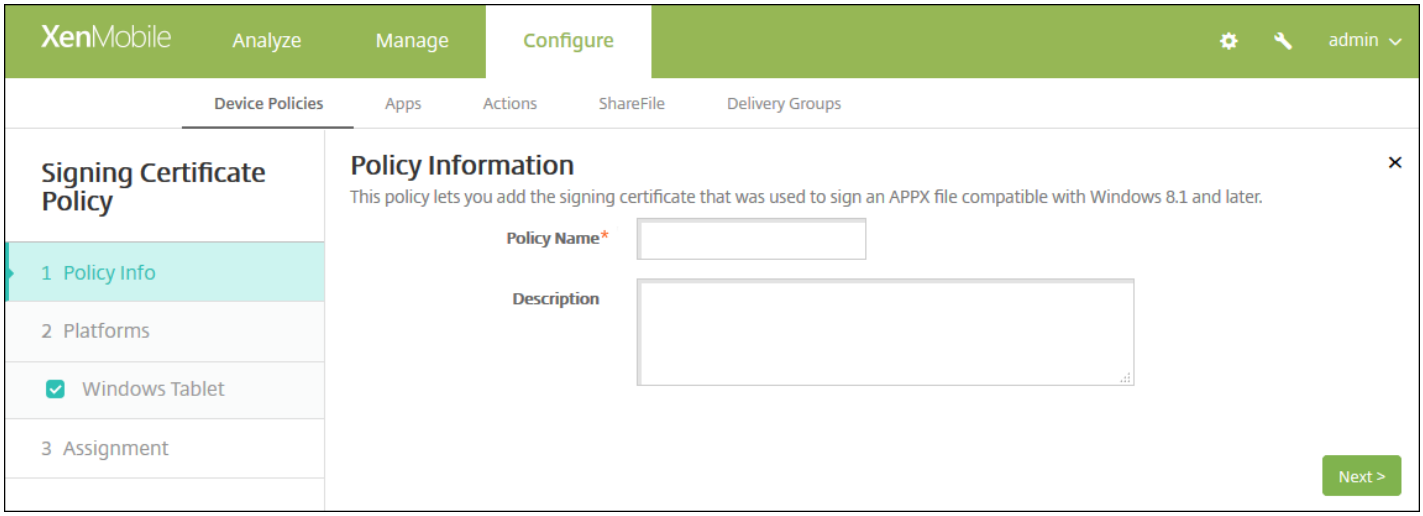


-
-
-

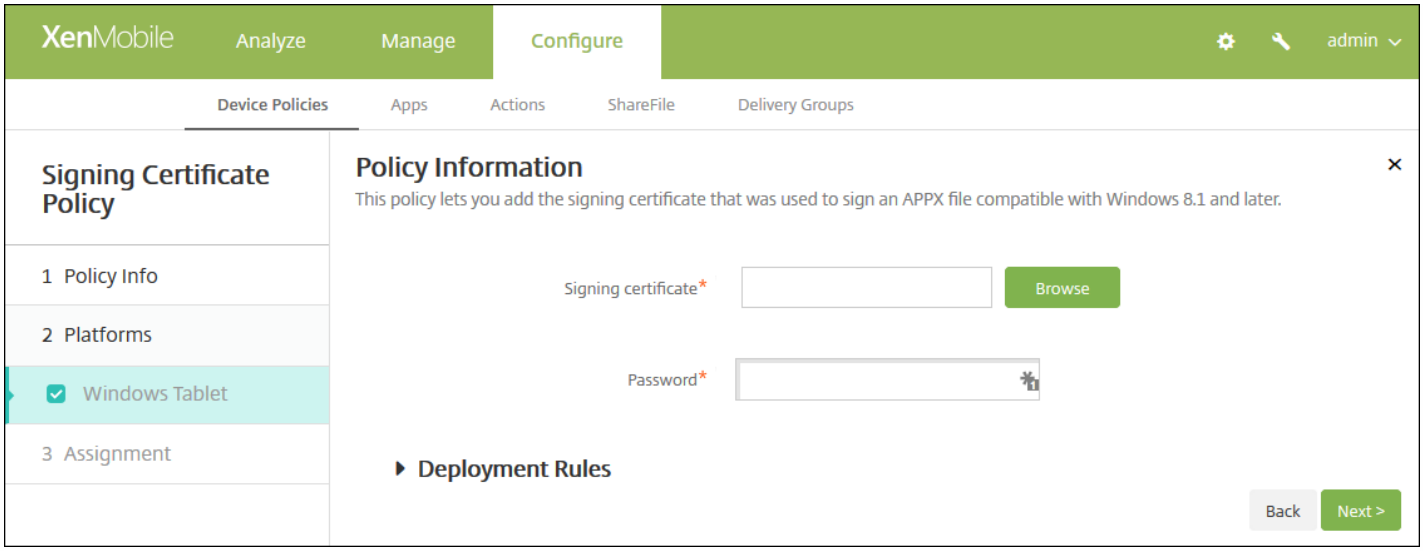
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-

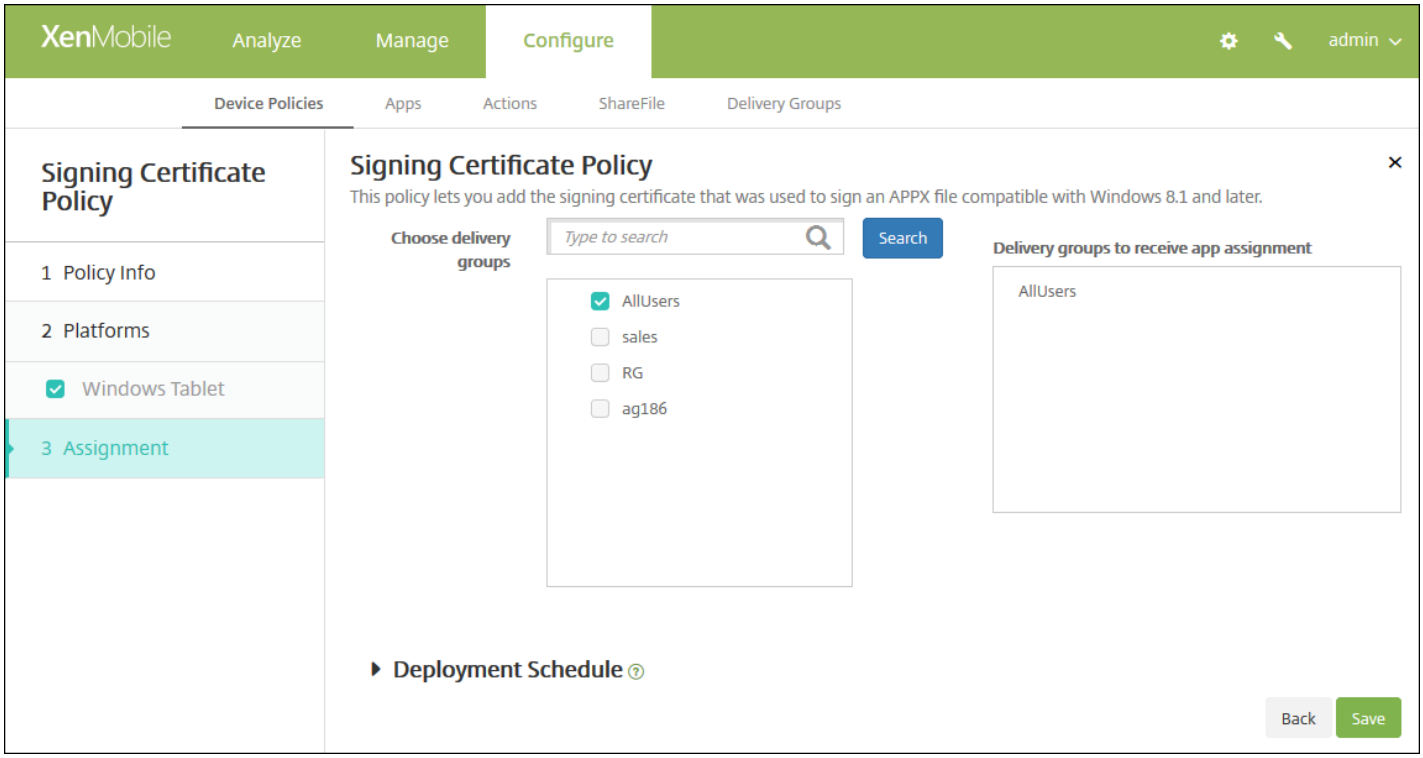


-
-

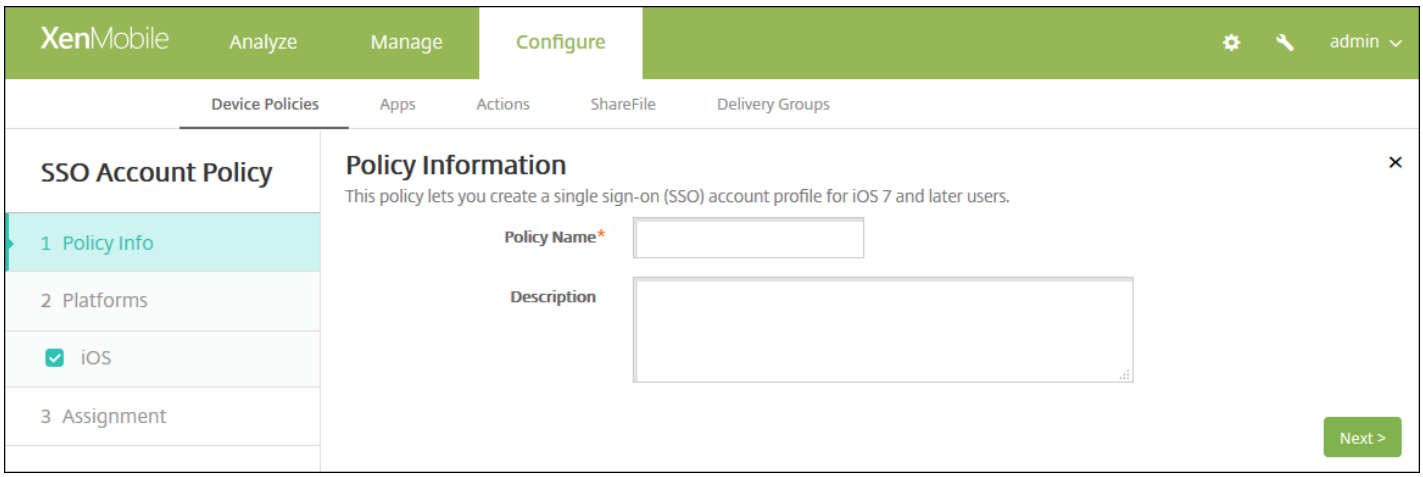


-
-

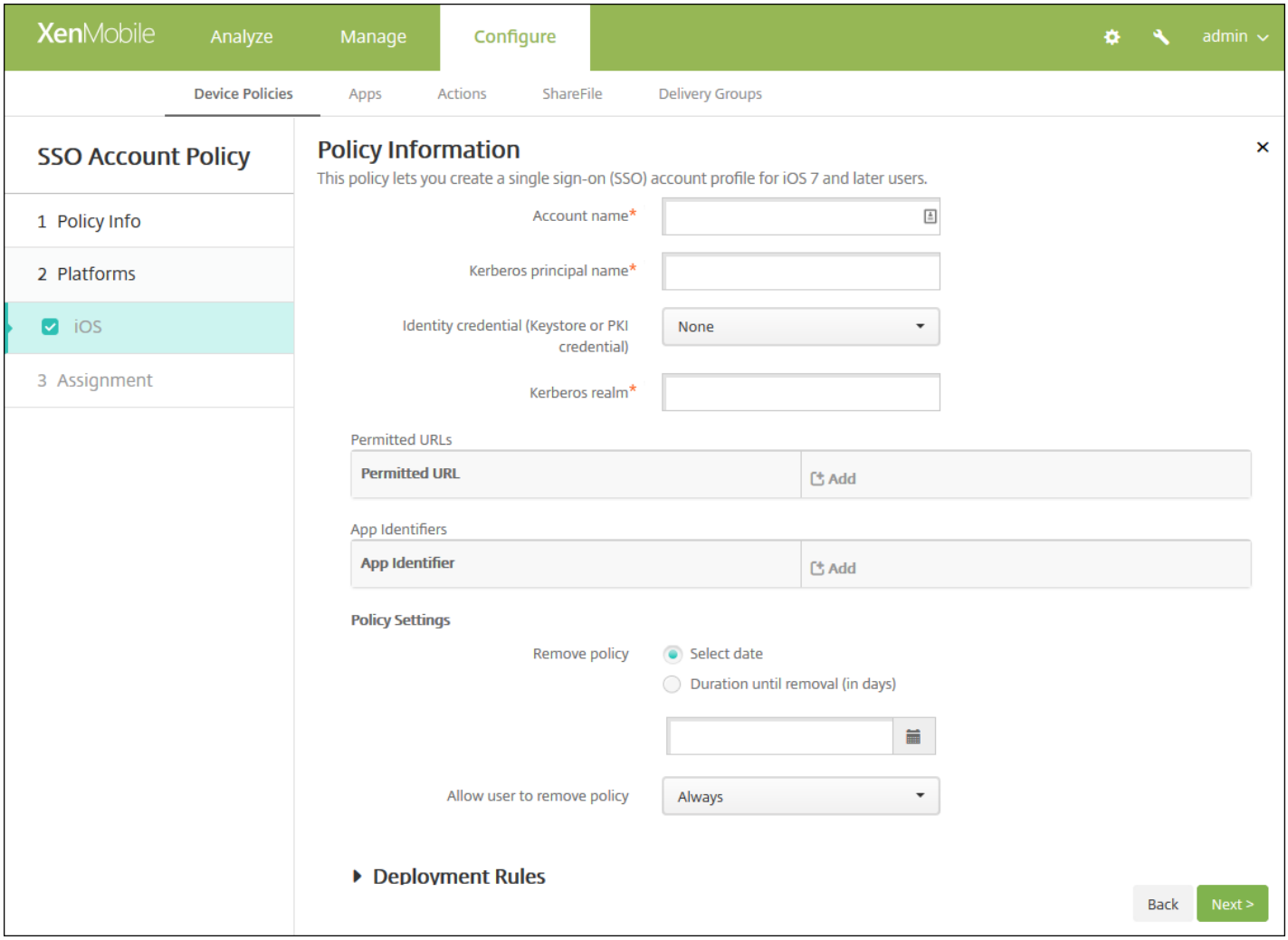
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-

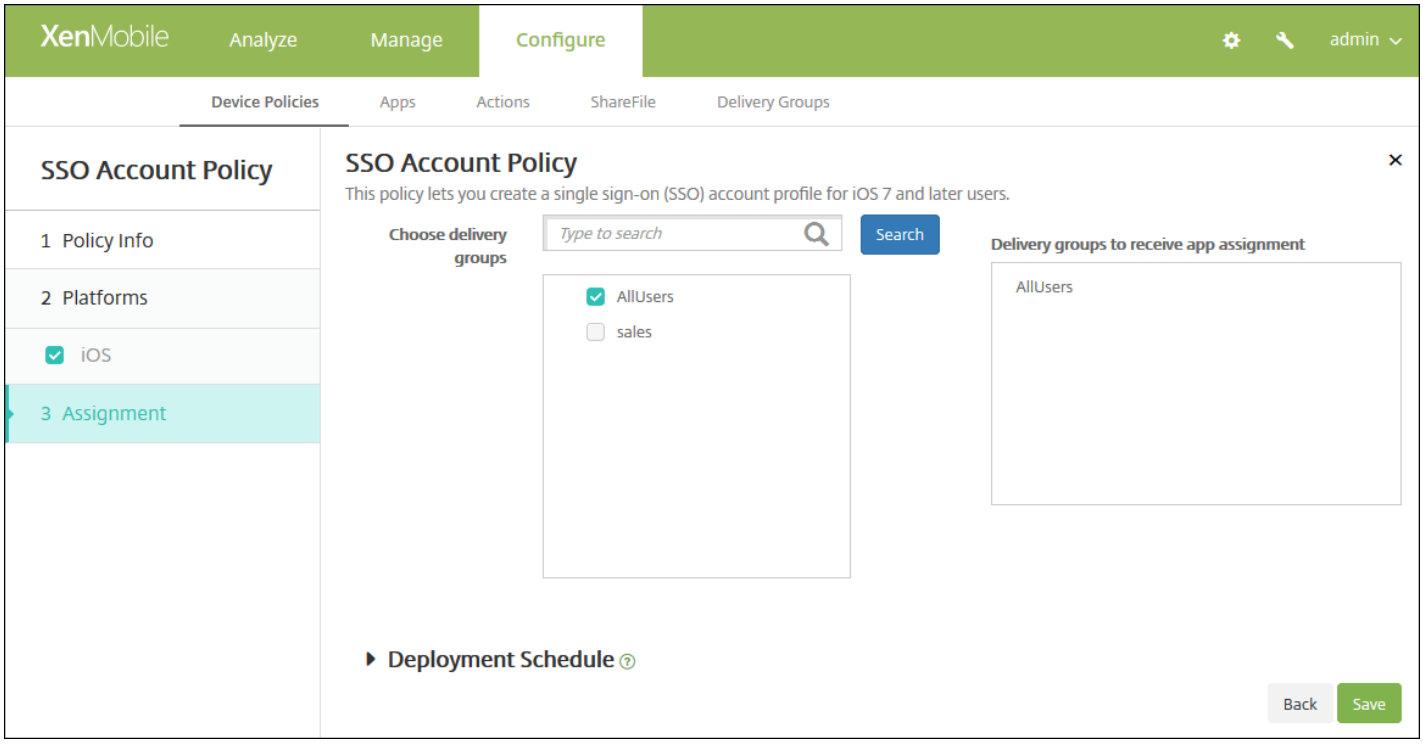


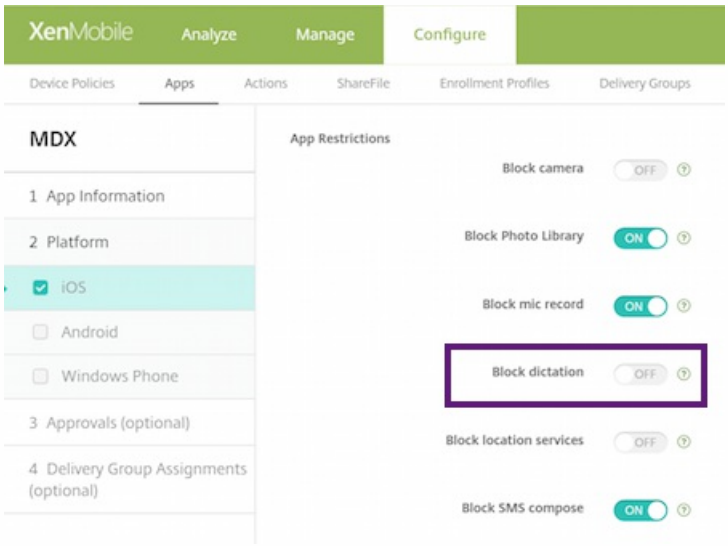
-
-

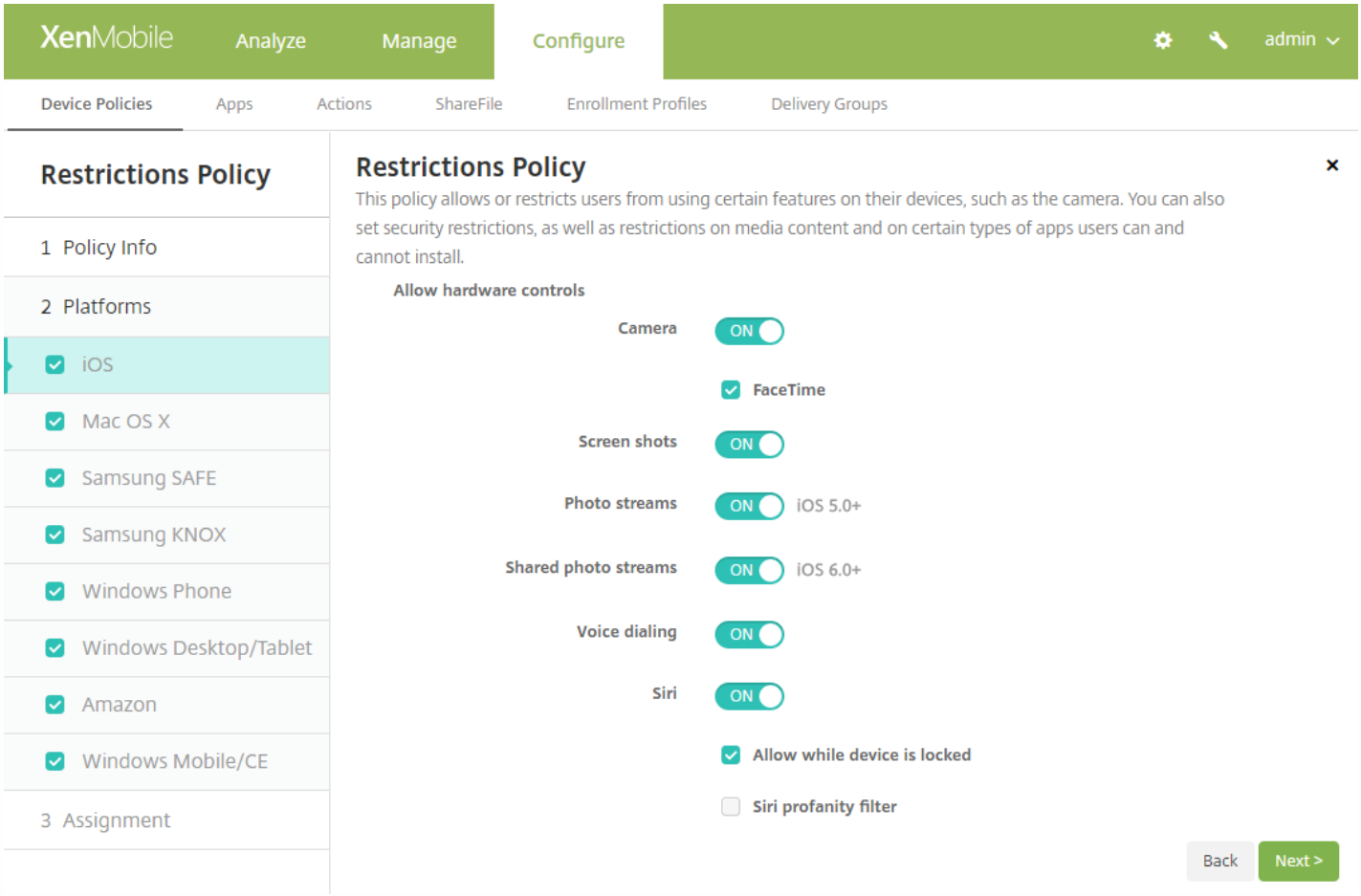


-
-
-
-
-
-

7. Configurez les règles de déploiement.

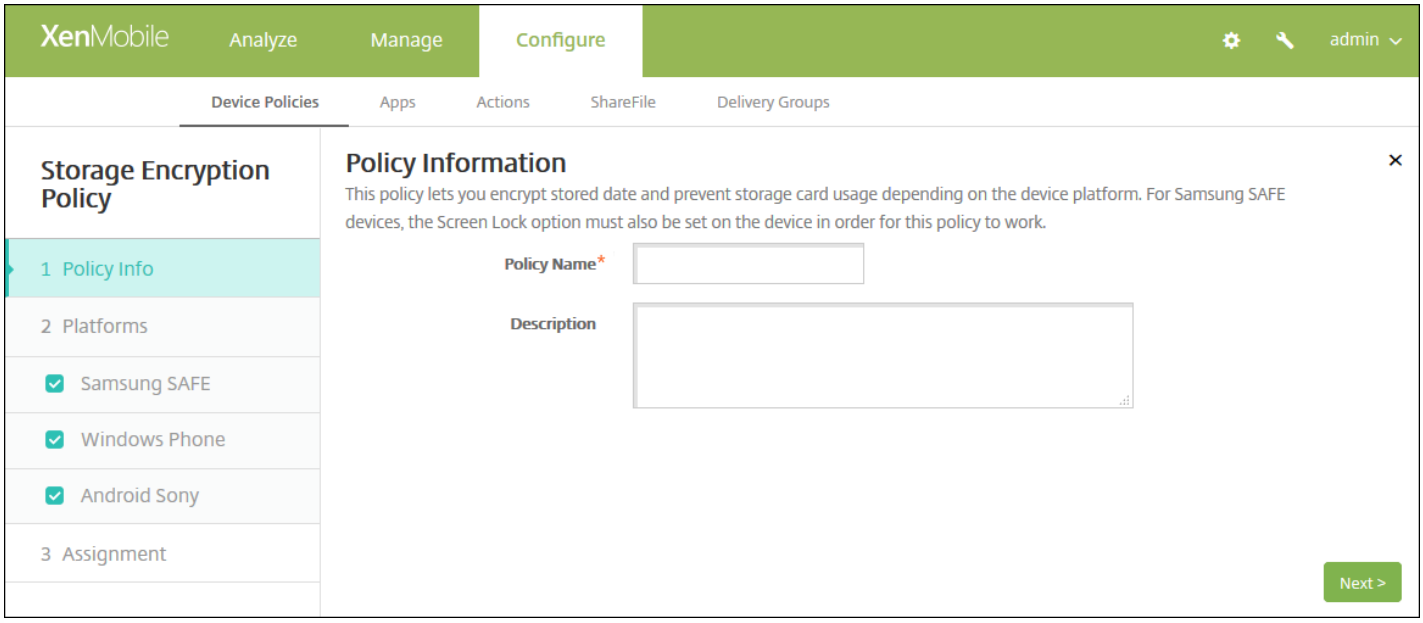






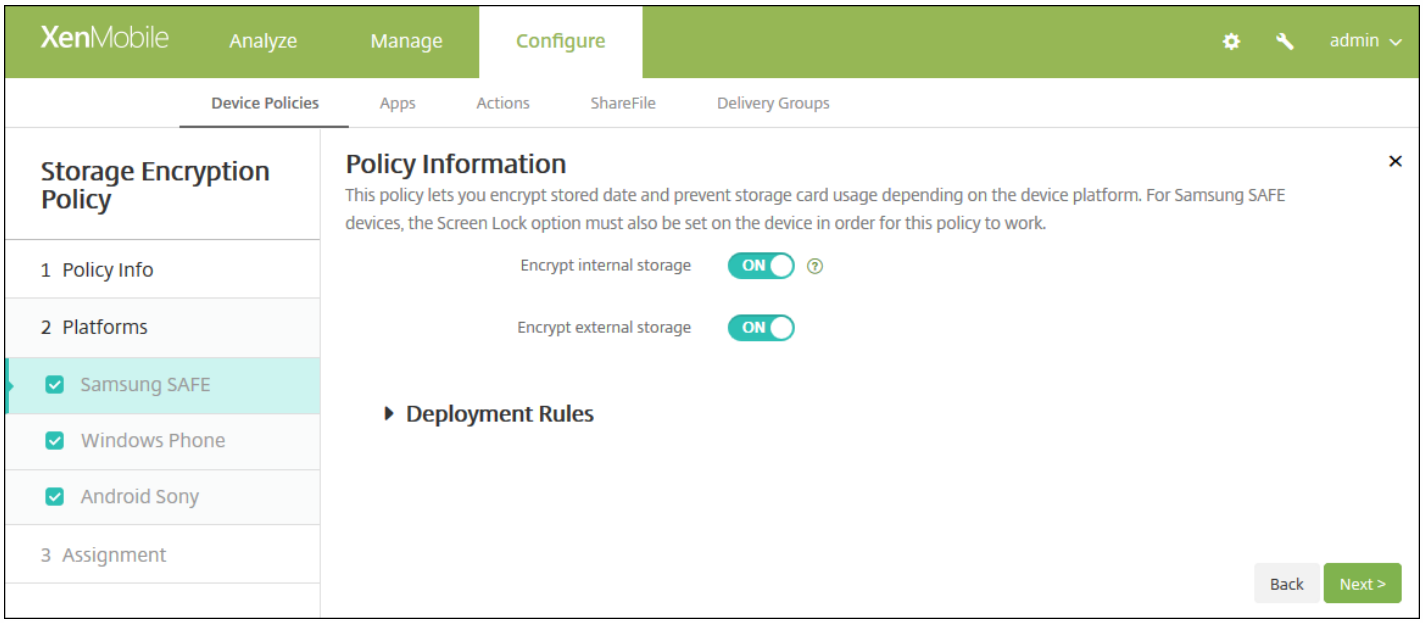
-
-

-
-
-



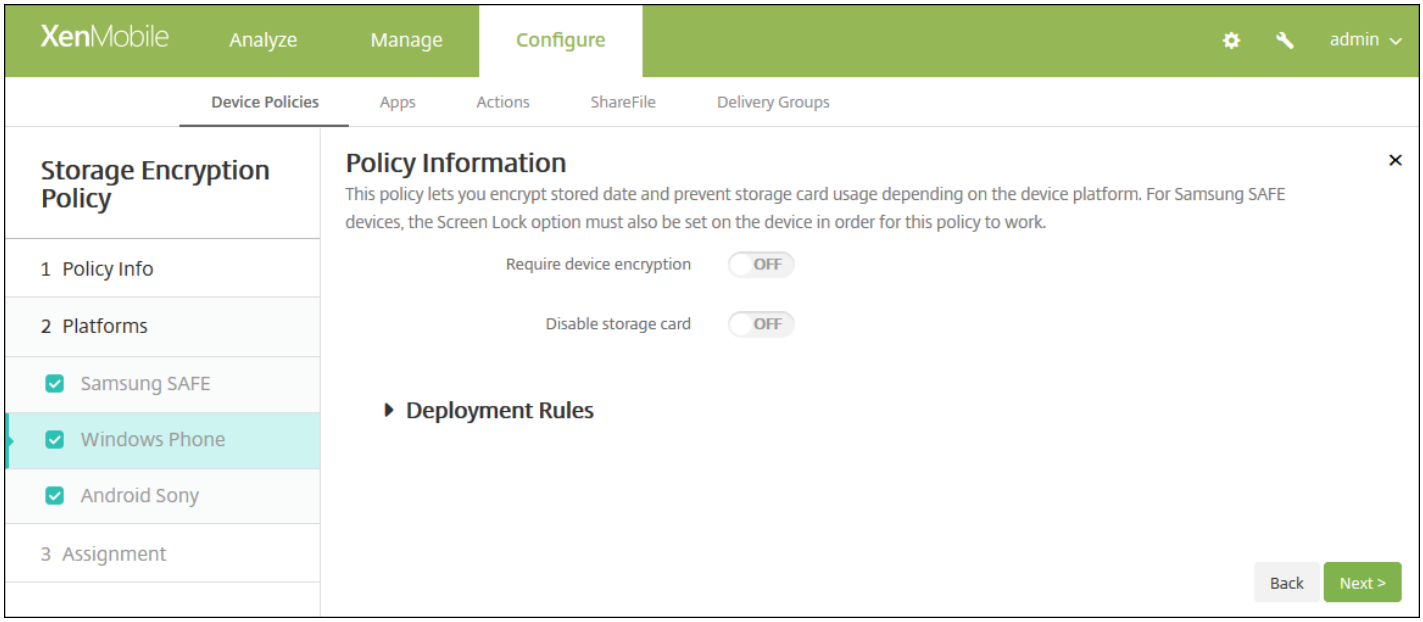
-
-

Configurer les paramètres pour Samsung SAFE



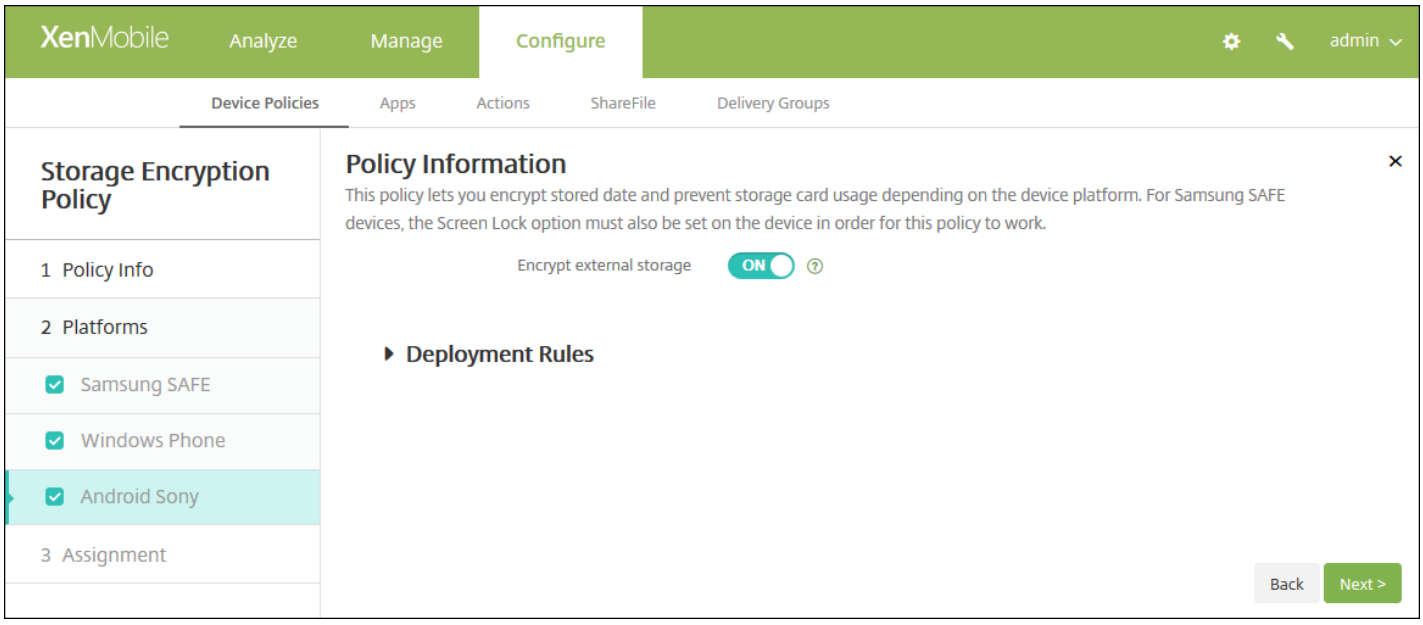
-
-

Configurer les paramètres pour Windows Phone



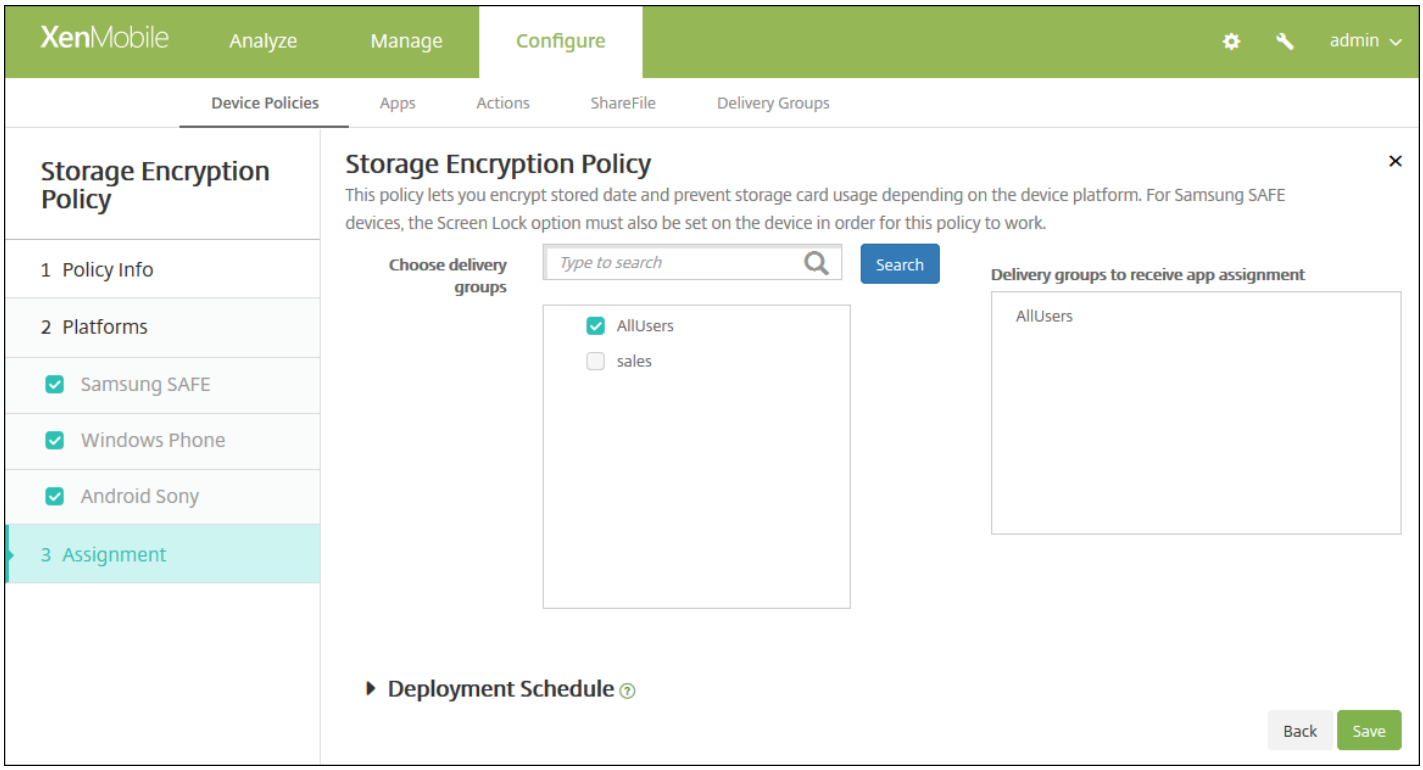
-
-

Configurer les paramètres pour Android Sony

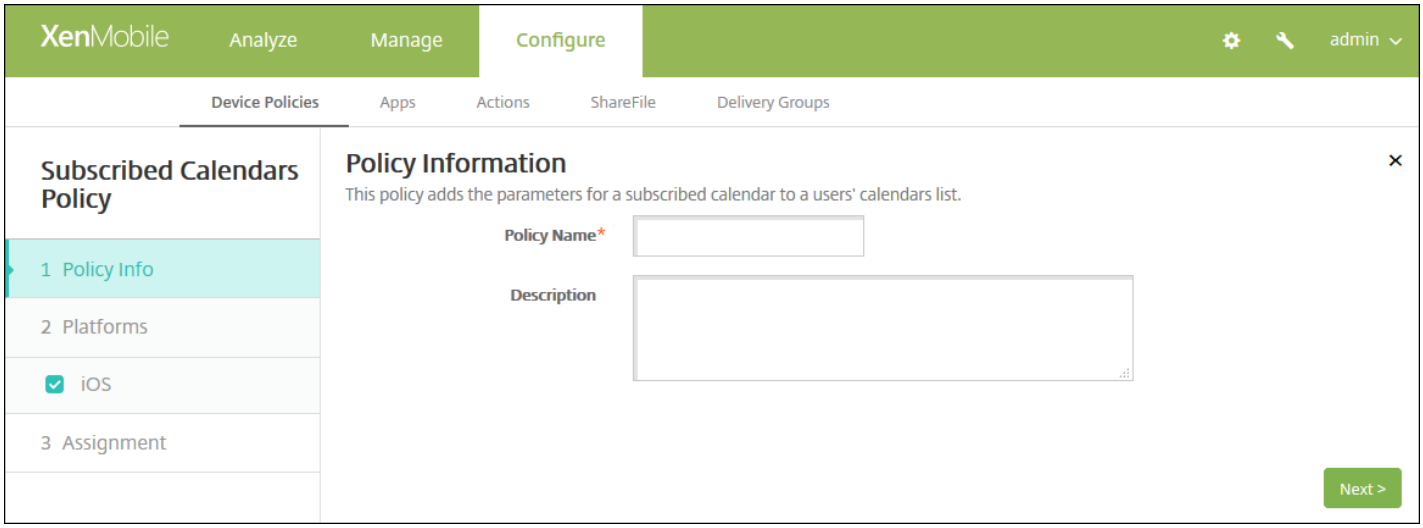


-

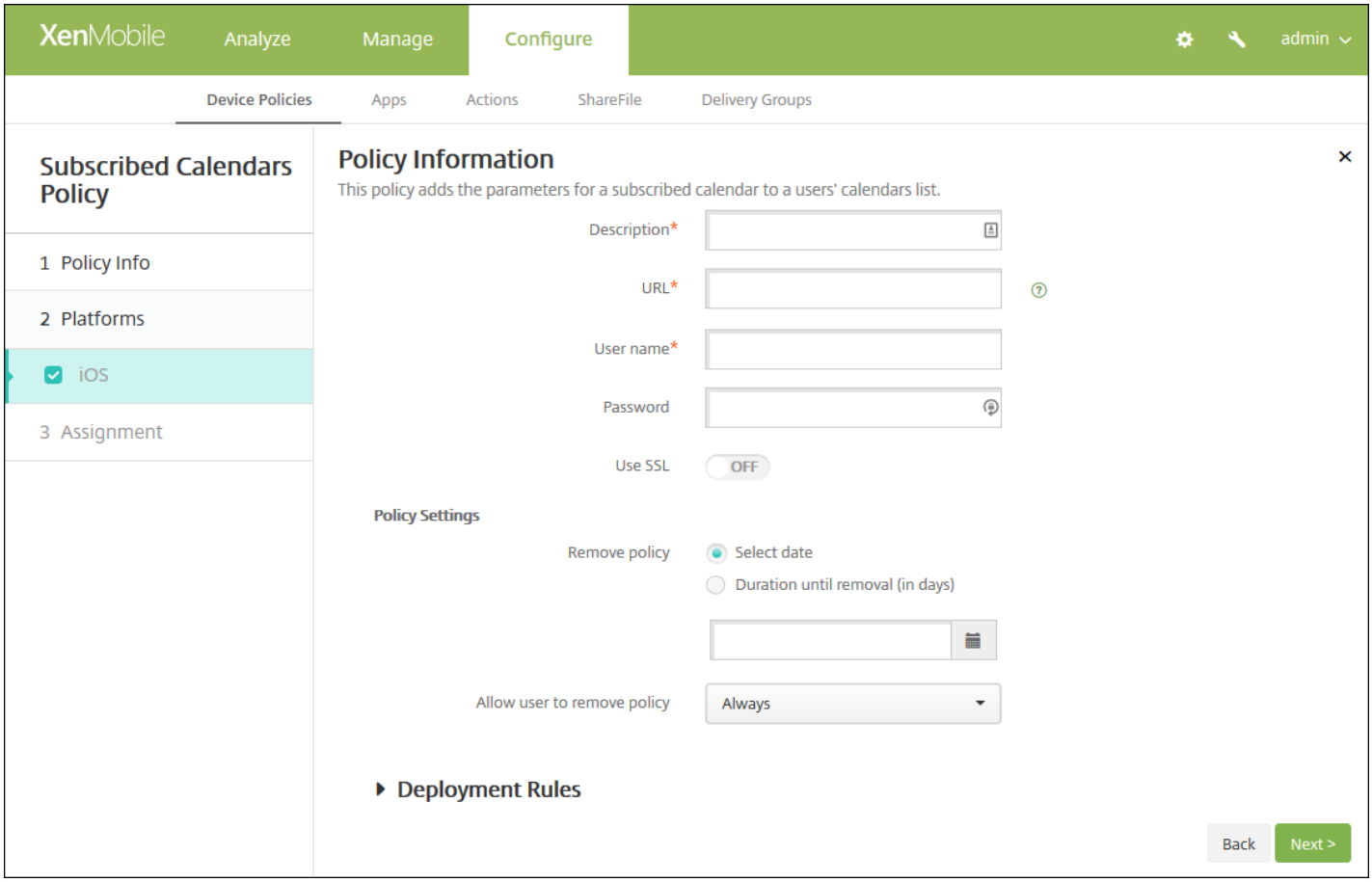
7. Configurez les règles de déploiement.



-

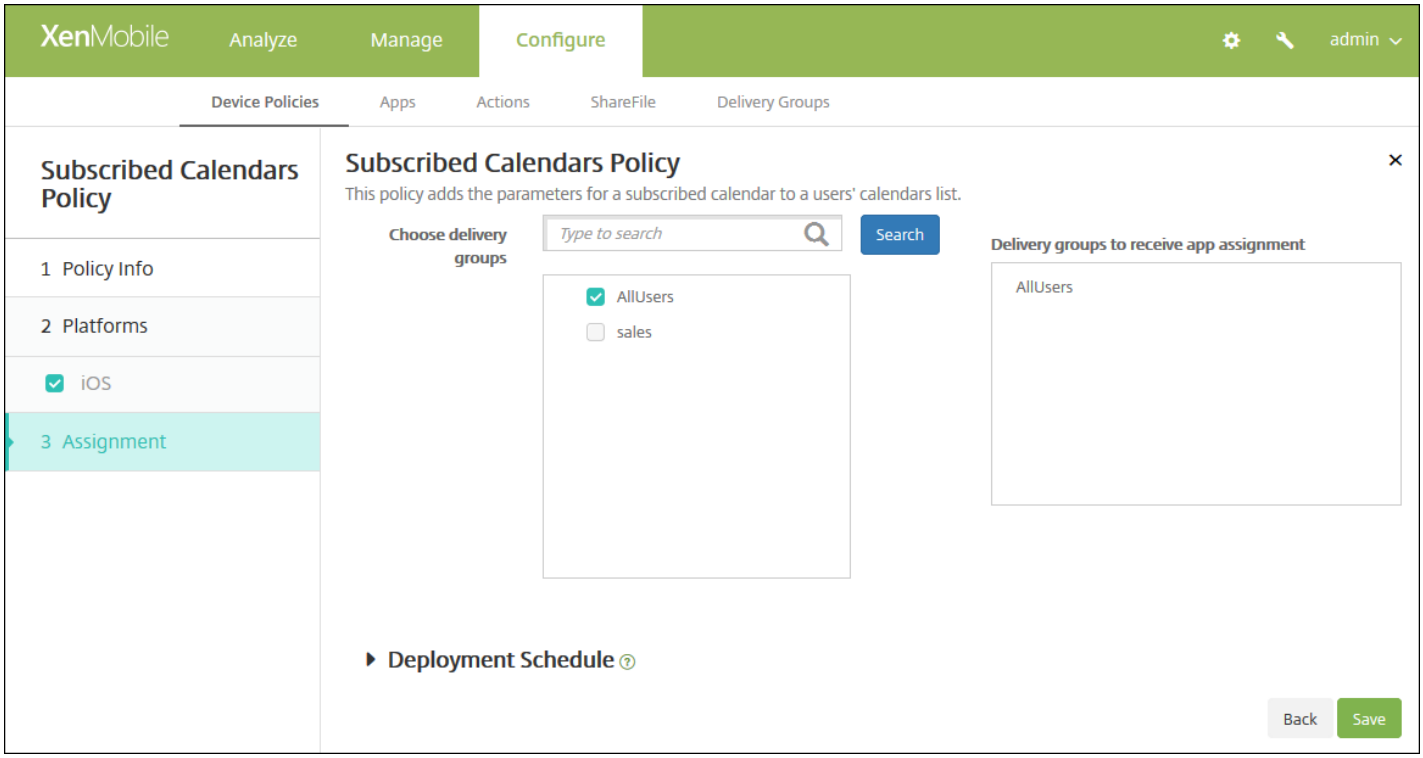


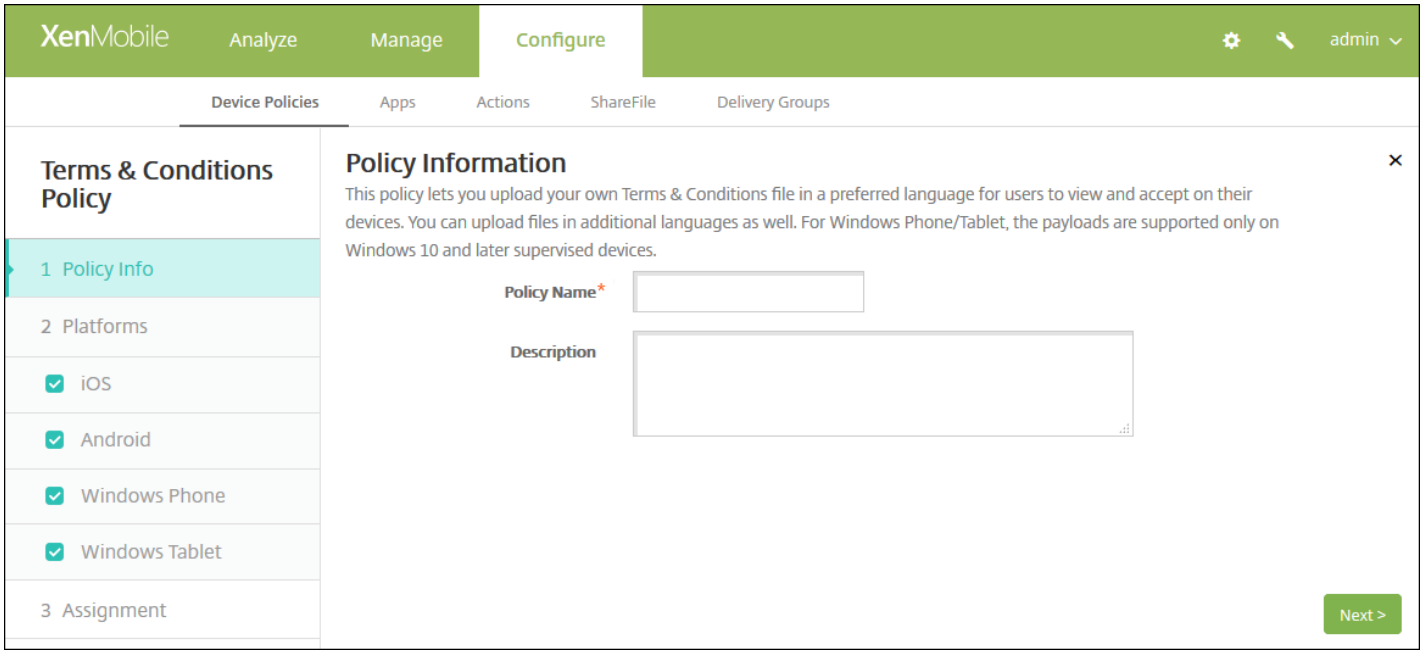
-
-



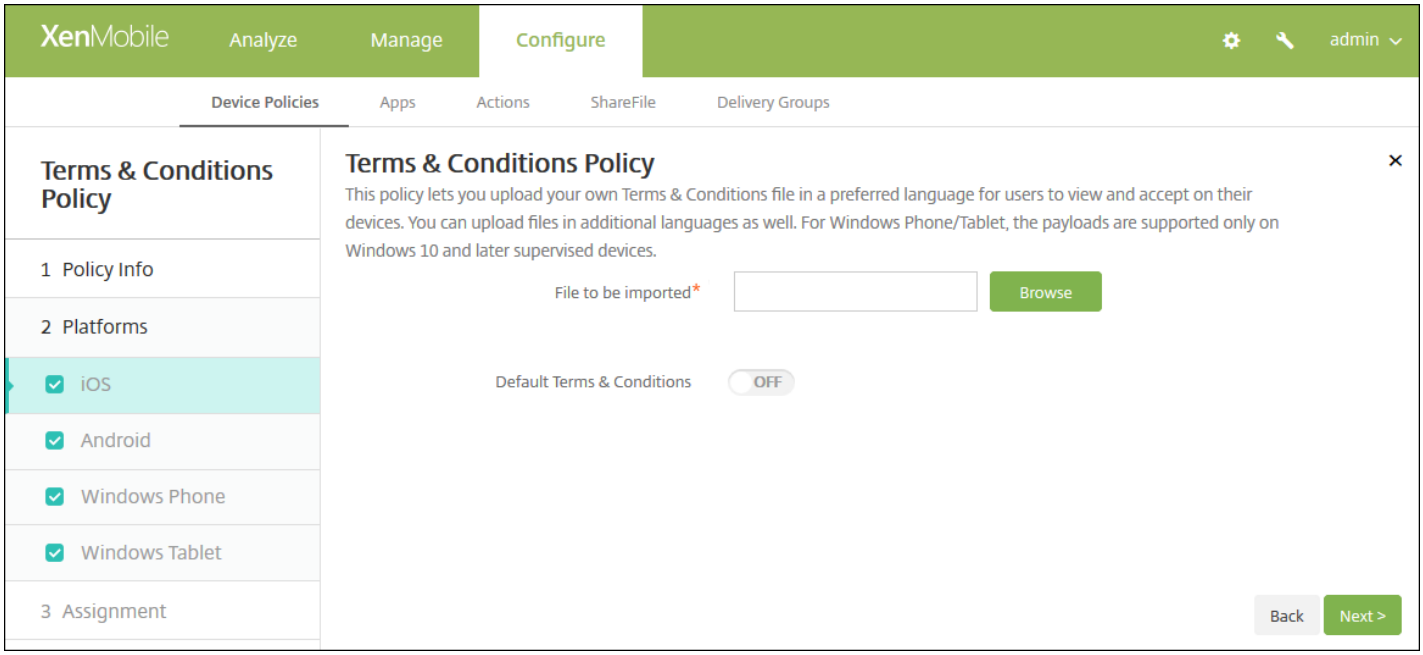
-
-
-
-
-
-
  -
  -
  -
  -

7. Configurez les règles de déploiement.

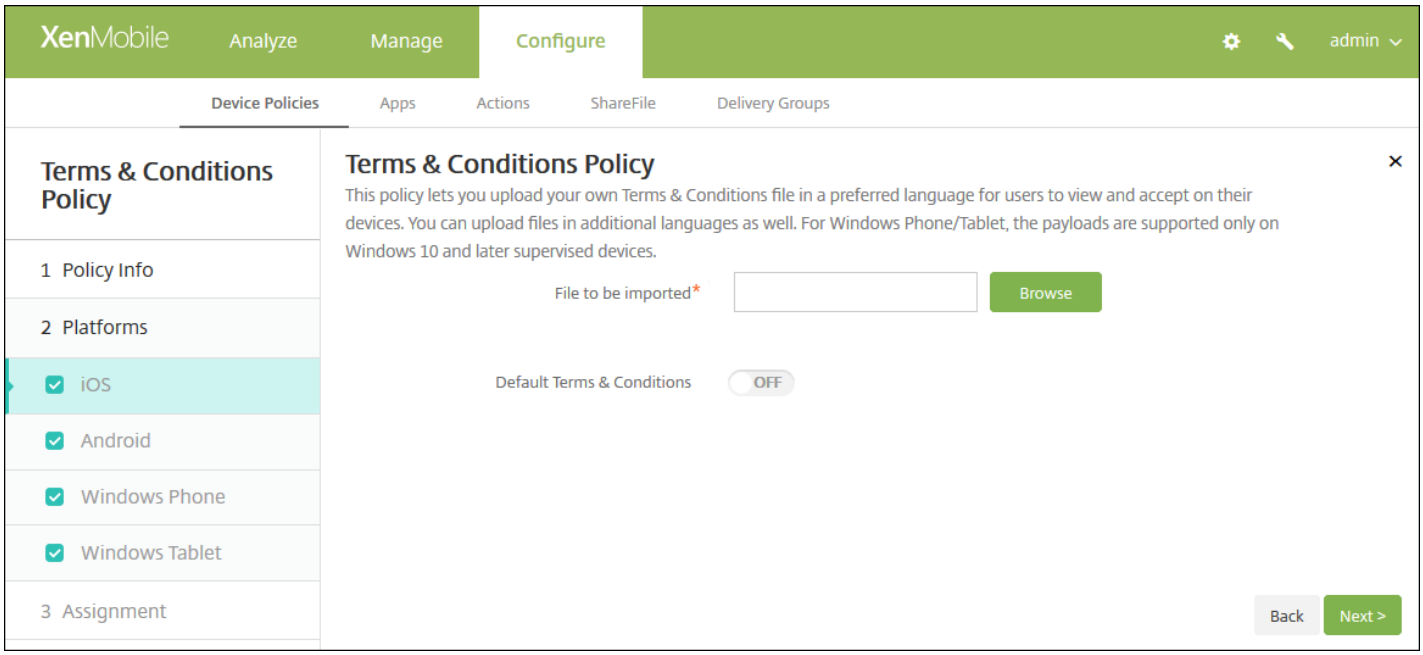




-
-

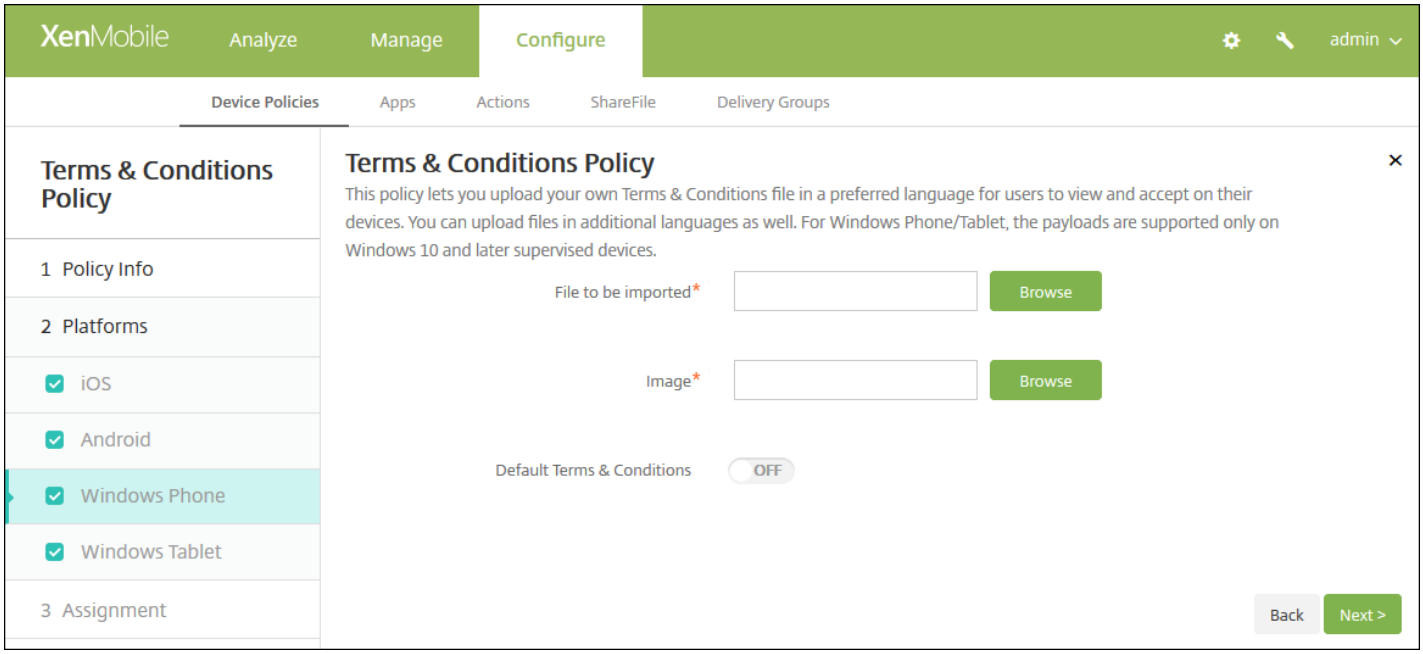


Paramètres iOS et Android.

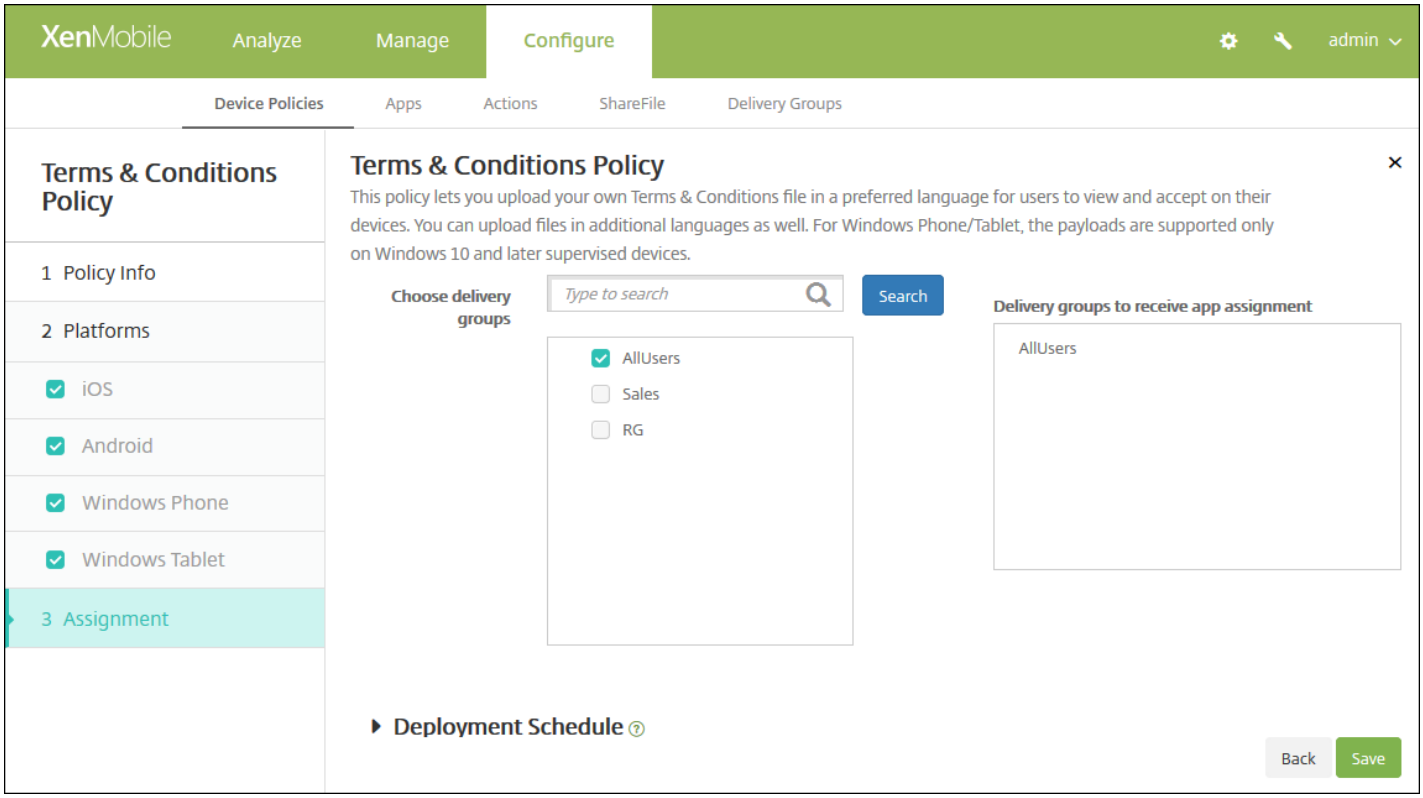


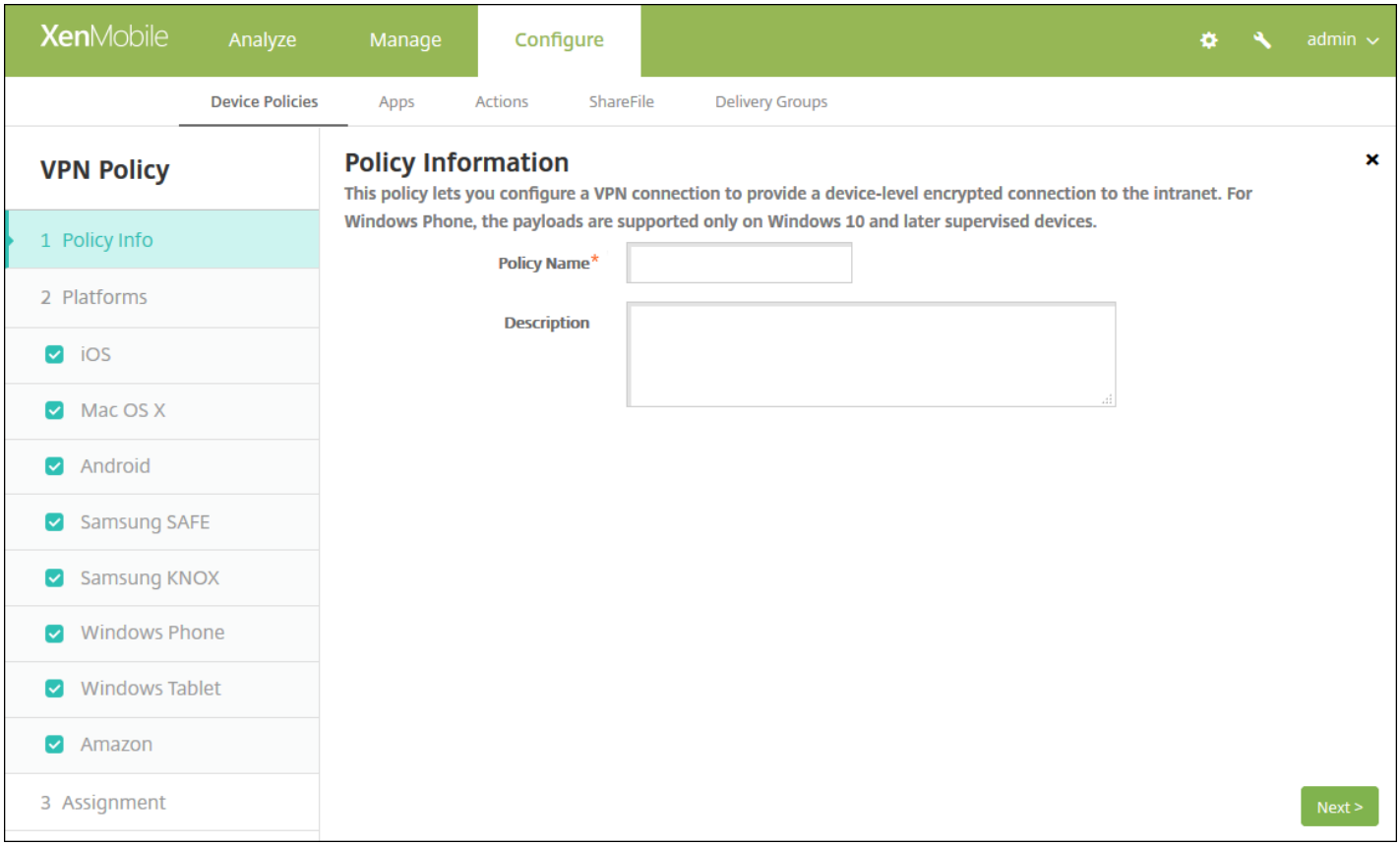
-
-

Paramètres Windows Phone et Windows Tablet



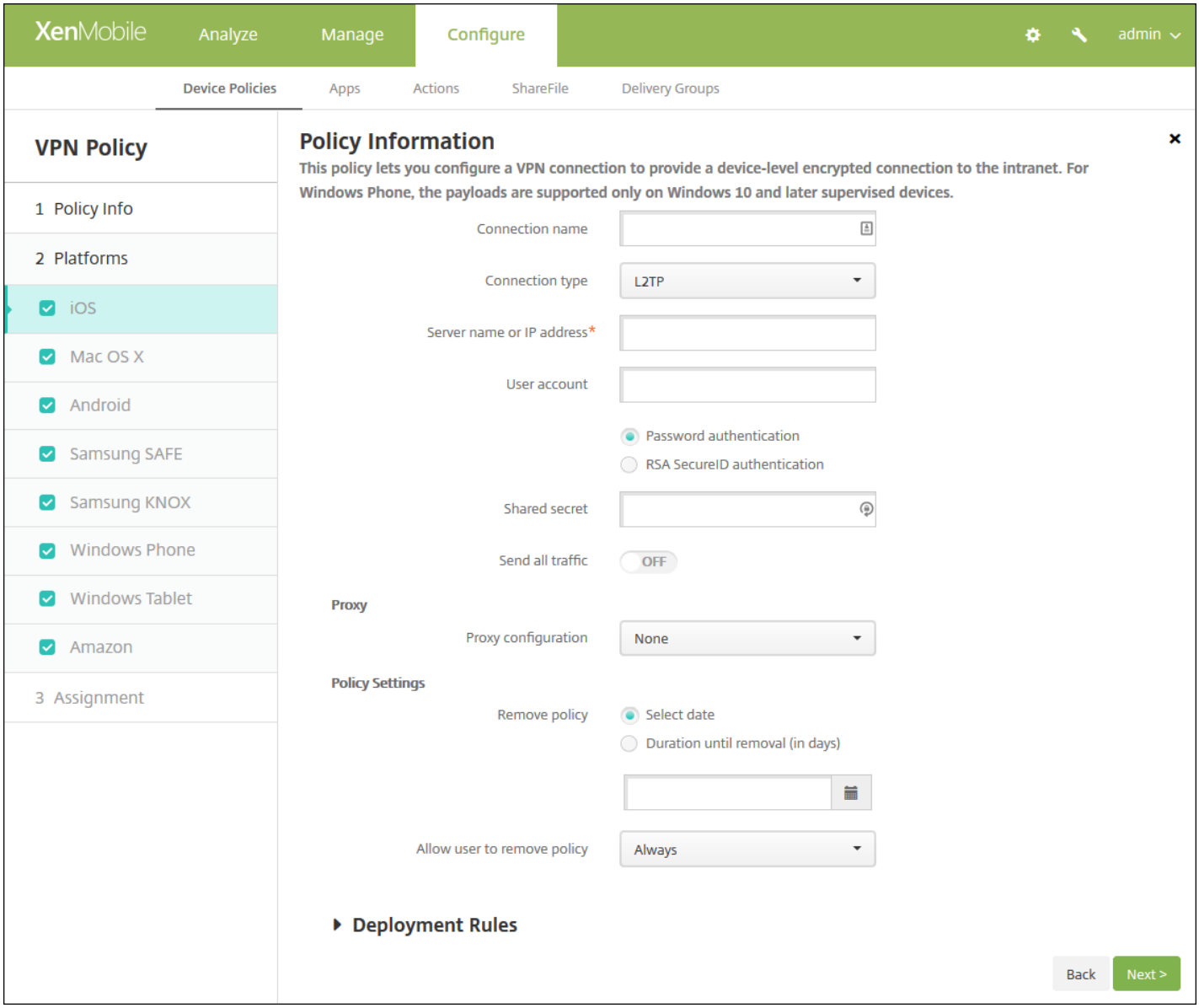
-
-
-





-
-

Configurer les paramètres pour iOS



-
-

-
-
-
-
-
-
-
-
-
-

-

Configurer le protocole L2TP

Configurer le protocole PPTP

Configurer le protocole IPSec

Configurer le protocole Cisco AnyConnect

Configurer le protocole SSL Juniper

Configurer le protocole F5 SSL

Configurer le protocole SonicWALL

Configurer le protocole Ariba VIA

Configurer le protocole IKEv2

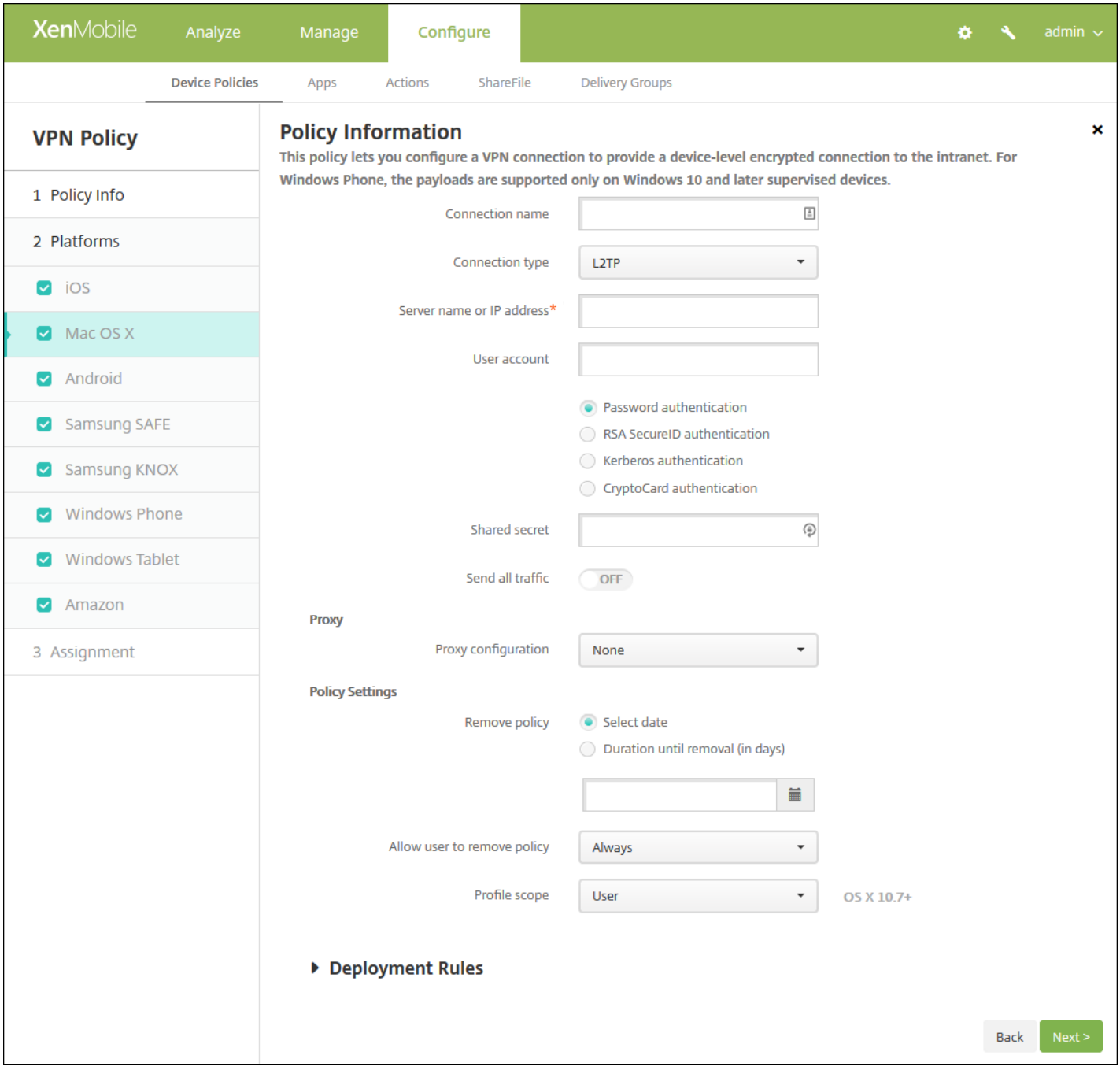
Configurer le protocole Citrix VPN

Configurer le protocole SSL personnalisé

Configurer les options de l'activation VPN sur demande

-
  -
    -
      -
      -
      -
      -
    -
      -
-
  -
  -
  -
  -

Configurer les paramètres pour Mac OS X



-
-

  -
  -
  -

-
-
-
-
-
-
-

Configurer le protocole L2TP

Configurer le protocole PPTP

Configurer le protocole IPSec

Configurer le protocole Cisco AnyConnect

Configurer le protocole SSL Juniper

Configurer le protocole F5 SSL

Configurer le protocole SonicWALL

Configurer le protocole Ariba VIA

Configurer le protocole Citrix VPN

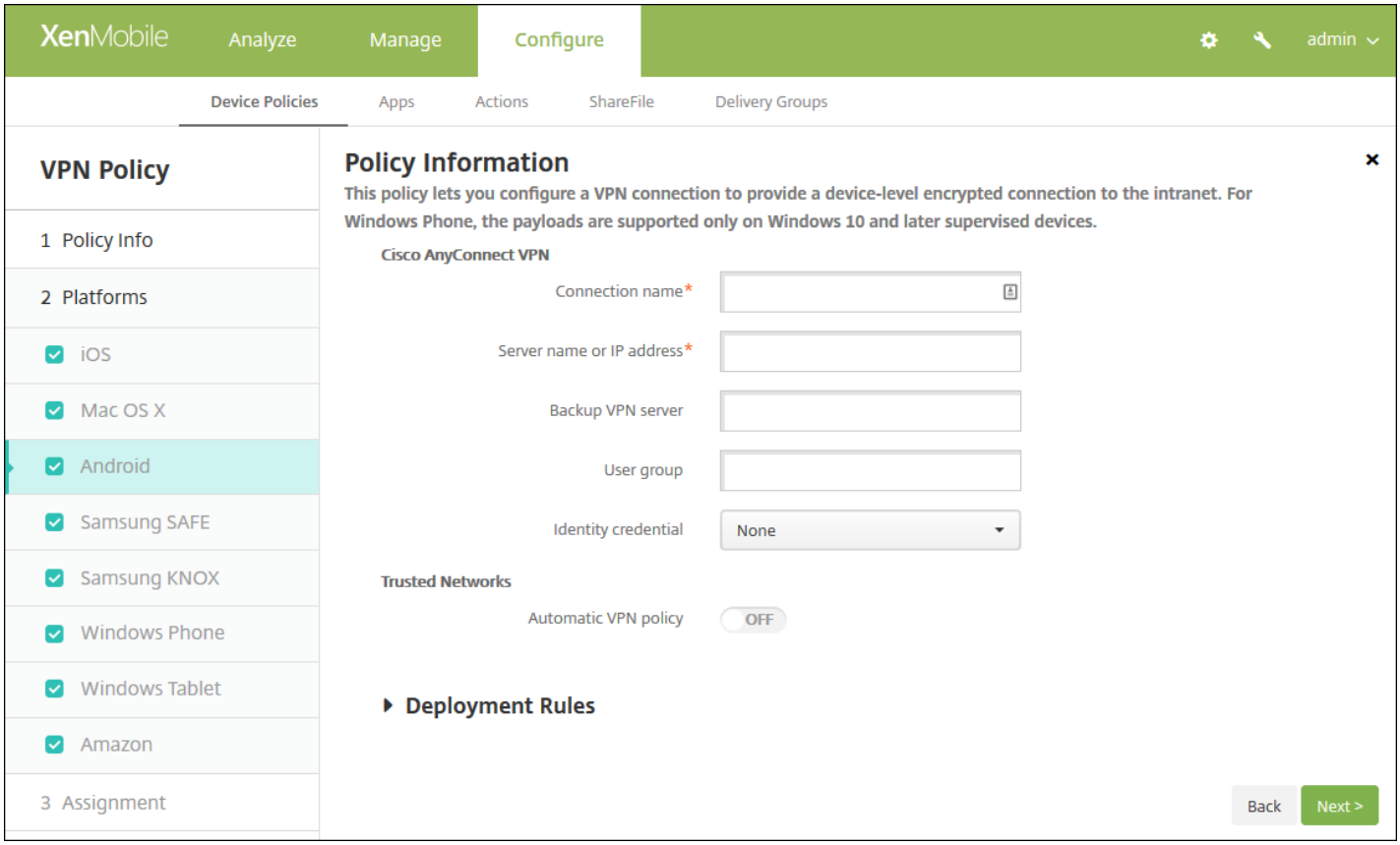
Configurer le protocole SSL personnalisé

Configurer les options de l'activation VPN sur demande

-
  -
    -
      -
      -
      -
      -
    -
      -
-
  -
  -

-
-
-

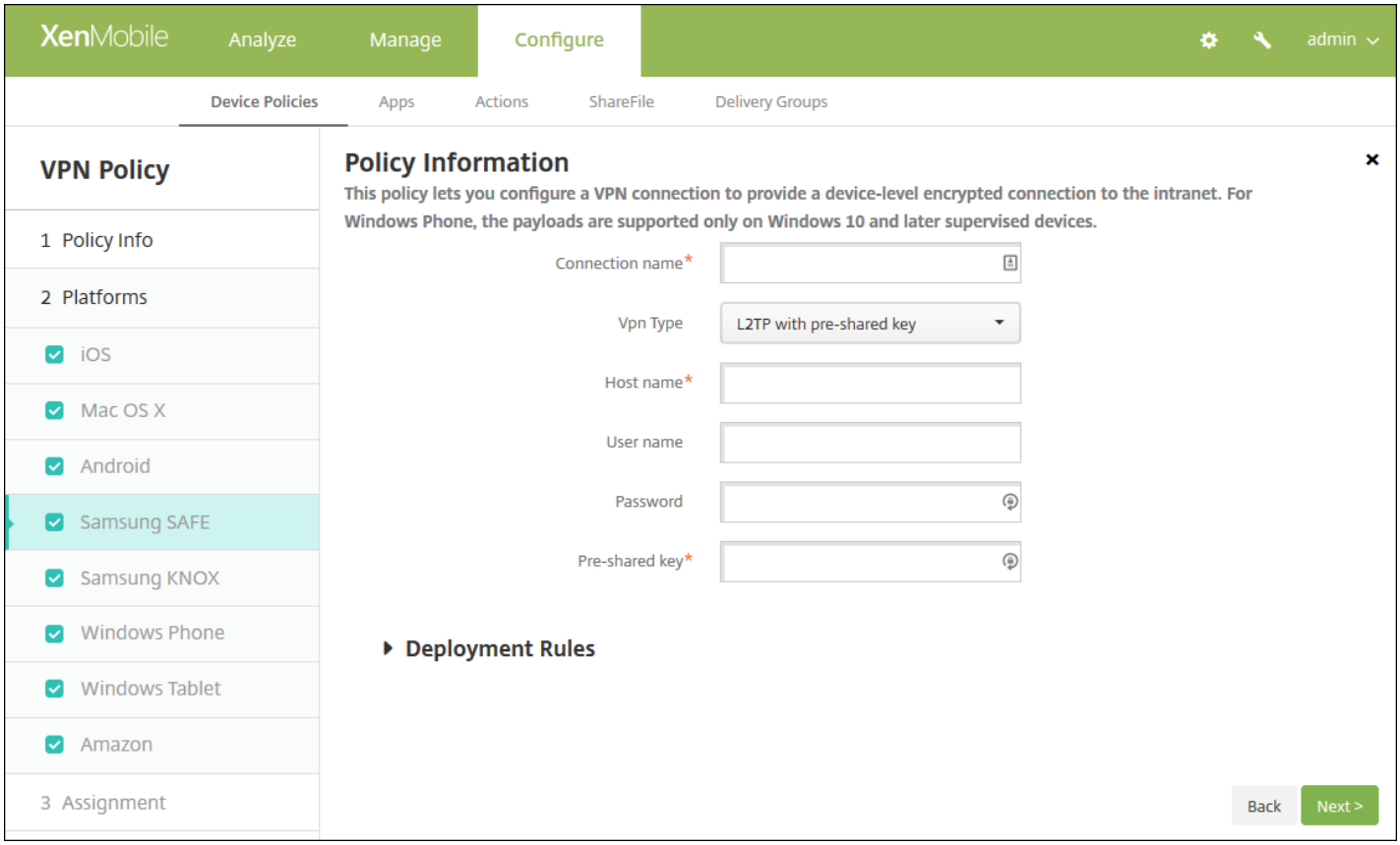
Configurer les paramètres pour Android



-
  -
  -
  -
  -
  -
-
  -

-
  -
    -
    -
    -
    -
  -
    -
    -
-
  -
  -
-
  -
  -
-

Configurer les paramètres pour Samsung SAFE



-
-
  -
  -
  -
  -
  -

Configurer le protocole L2TP avec clé prépartagée

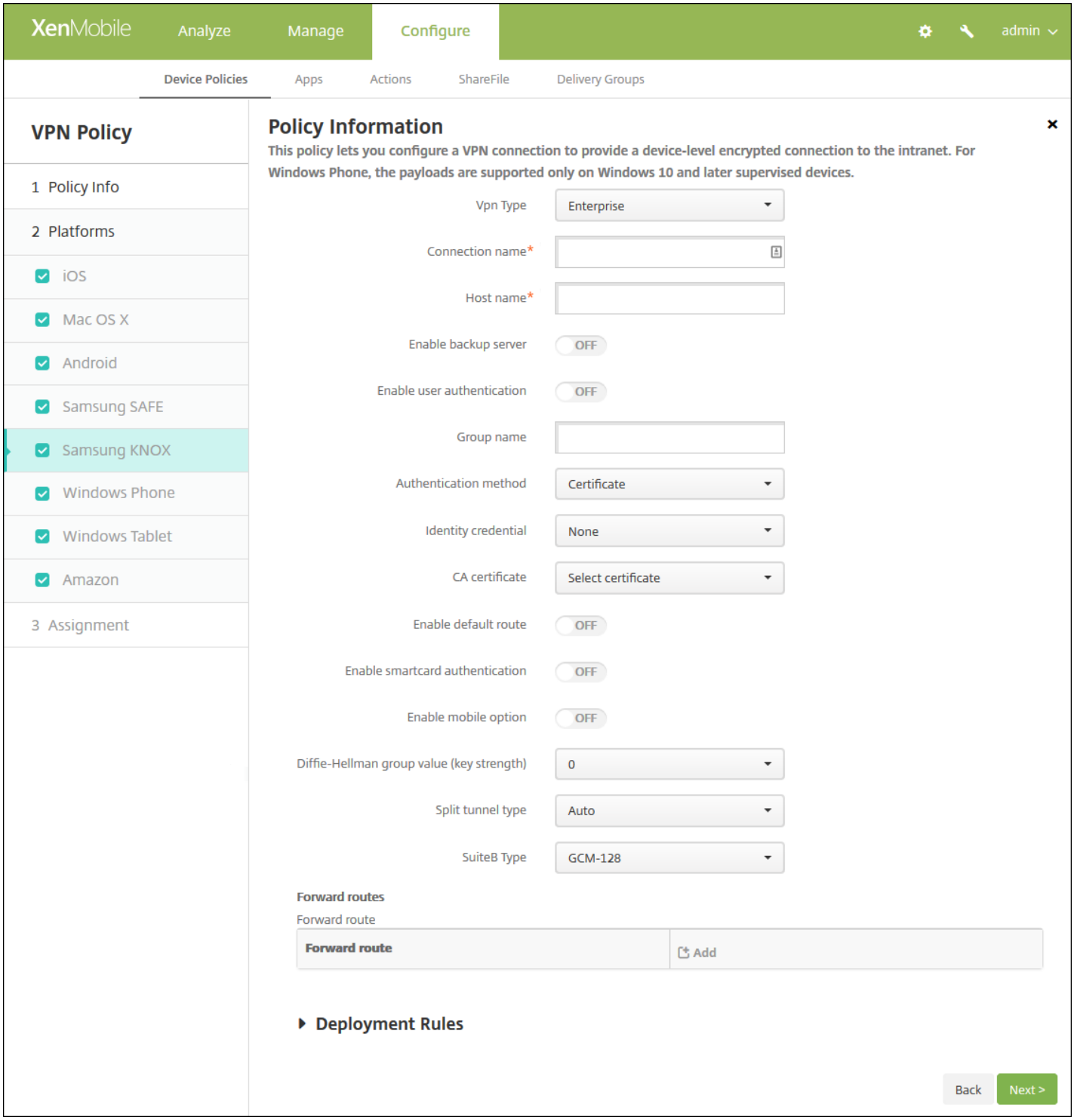
Configurer le protocole L2TP avec certificat

Configurer le protocole PPTP

Configurer le protocole Enterprise

Configurer le protocole générique

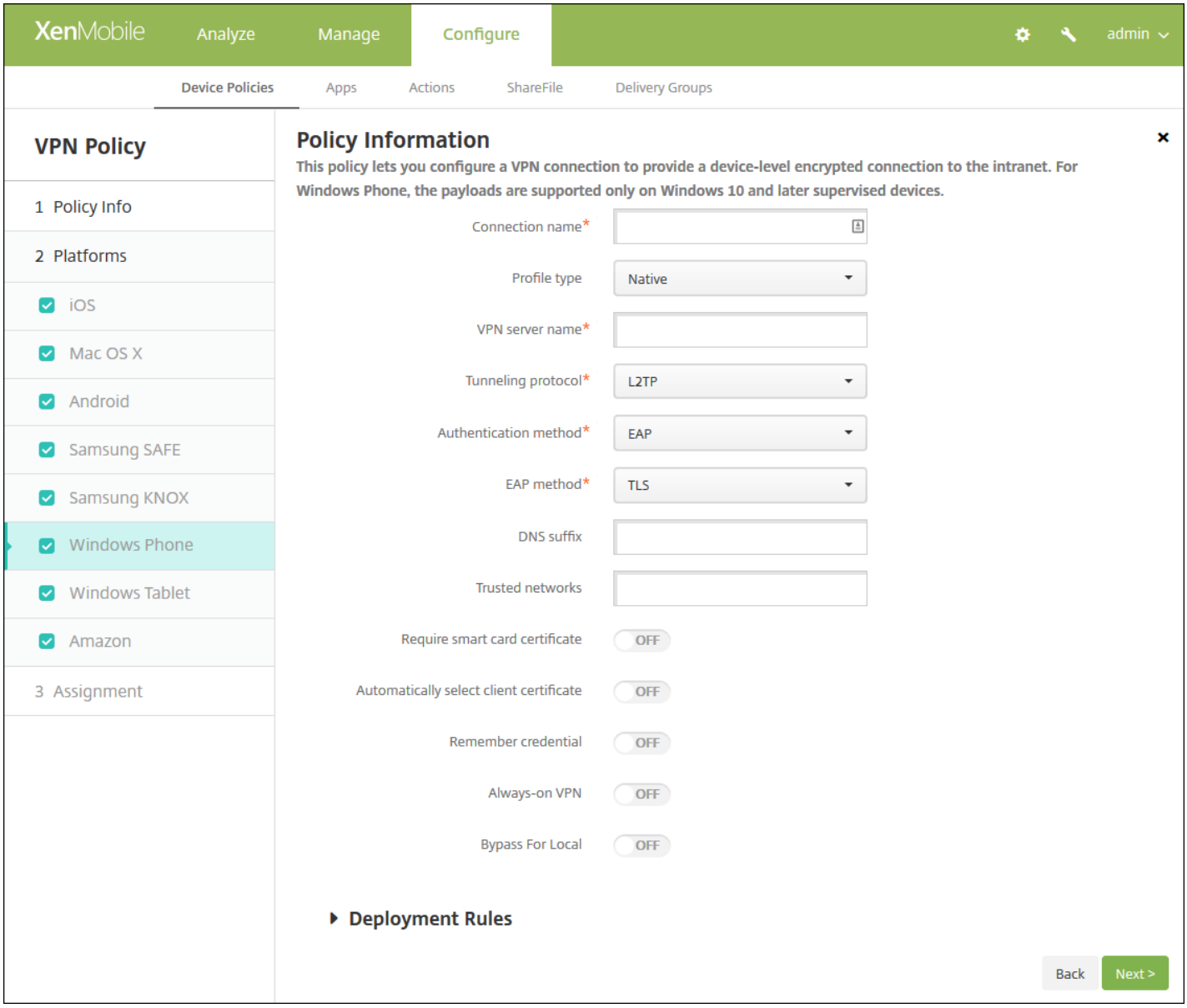
Configurer les paramètres pour Samsung KNOX



Configurer le protocole Enterprise

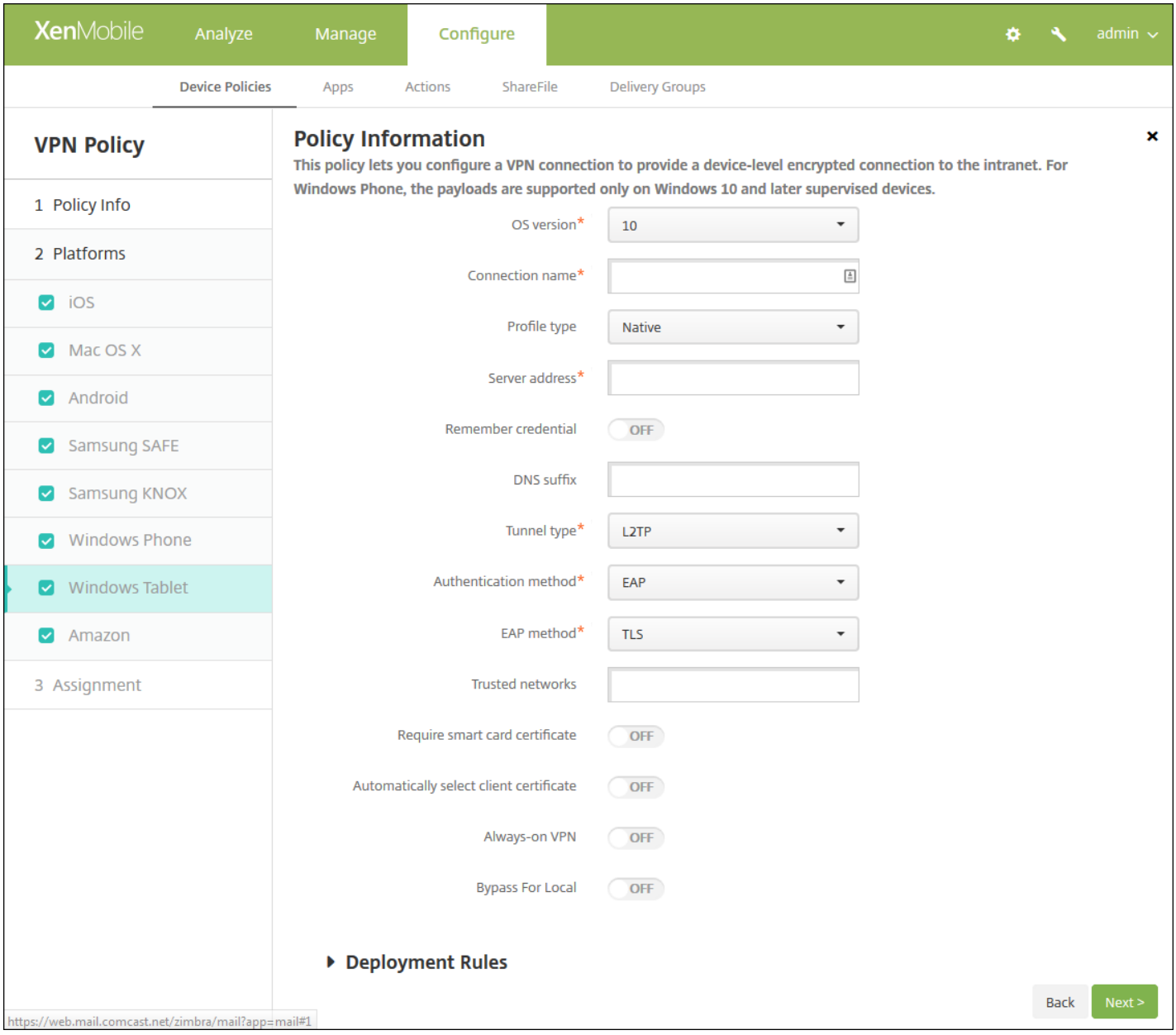
Configurer le protocole générique

Configurer les paramètres pour Windows Phone



-
-
-
-
-

Configurer les paramètres pour Windows Tablet

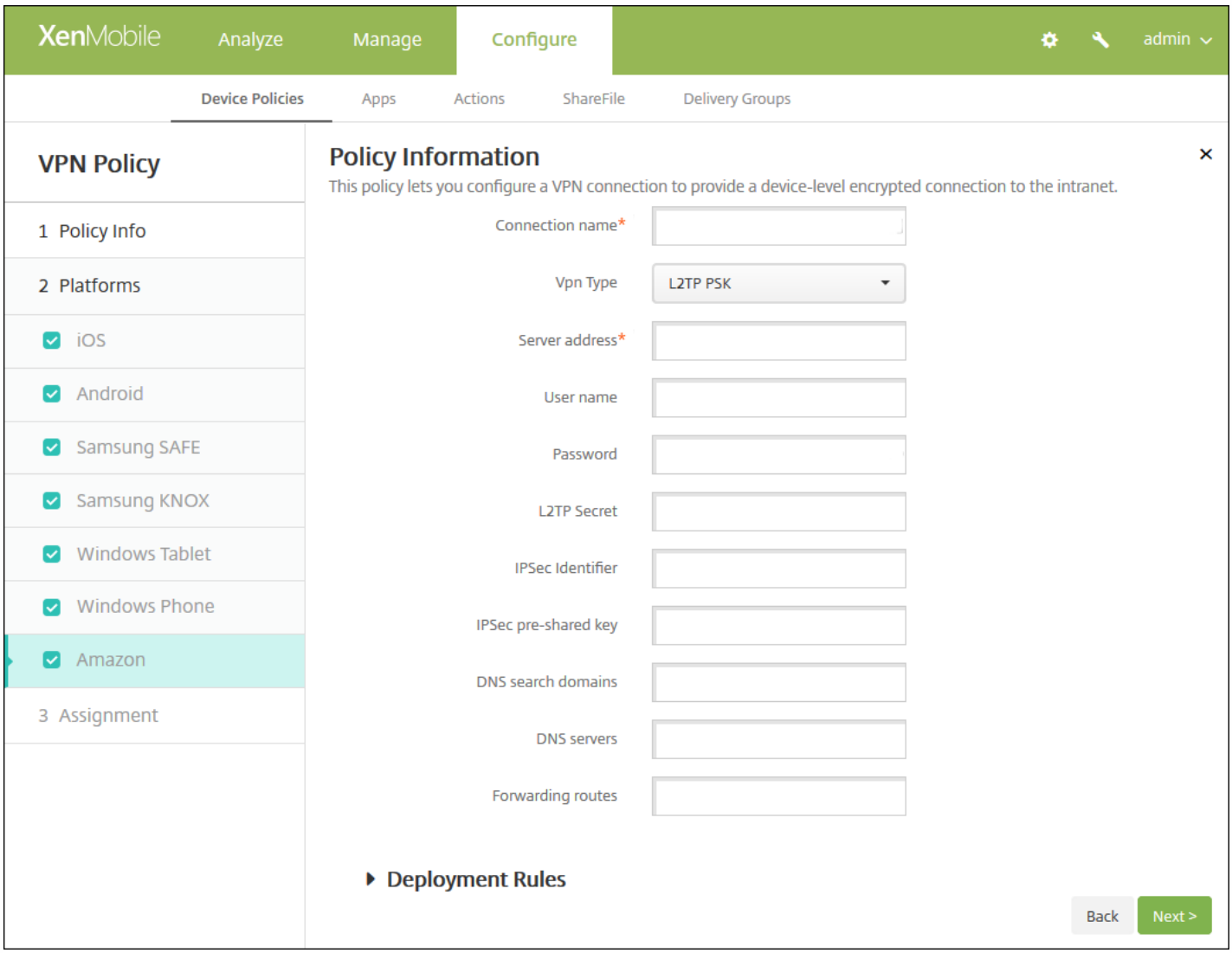


-

Configurer les paramètres pour Windows 10

Configurer les paramètres Windows 8.1

Configurer les paramètres pour Amazon



-
-
  -
  -

-
-
-

Configurer les paramètres L2TP PSK

Configurer les paramètres L2TP RSA

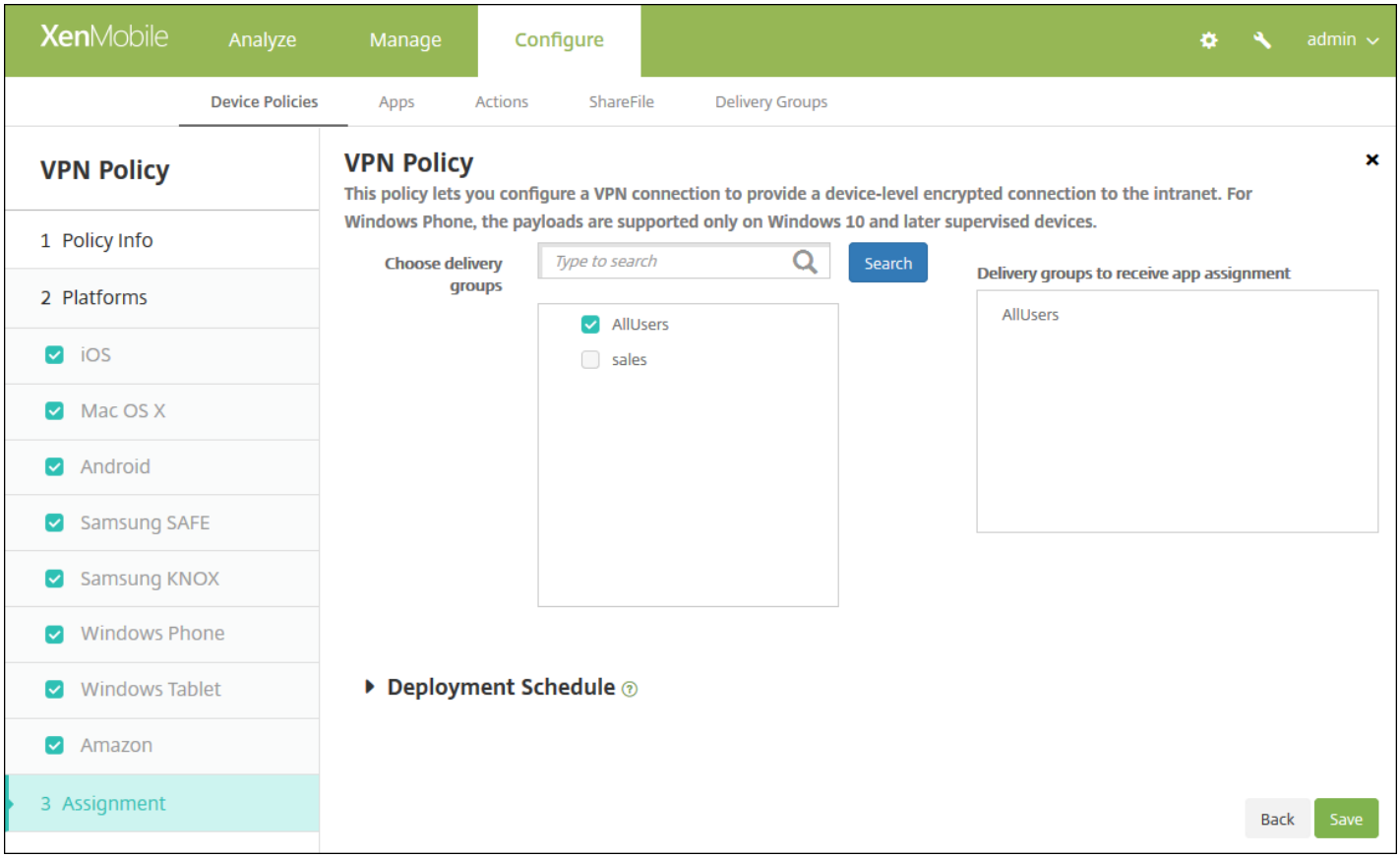
Configurer les paramètres IPSEC XAUTH PSK

Configurer les paramètres IPSEC AUTH RSA

Configurer les paramètres IPSEC HYBRID RSA

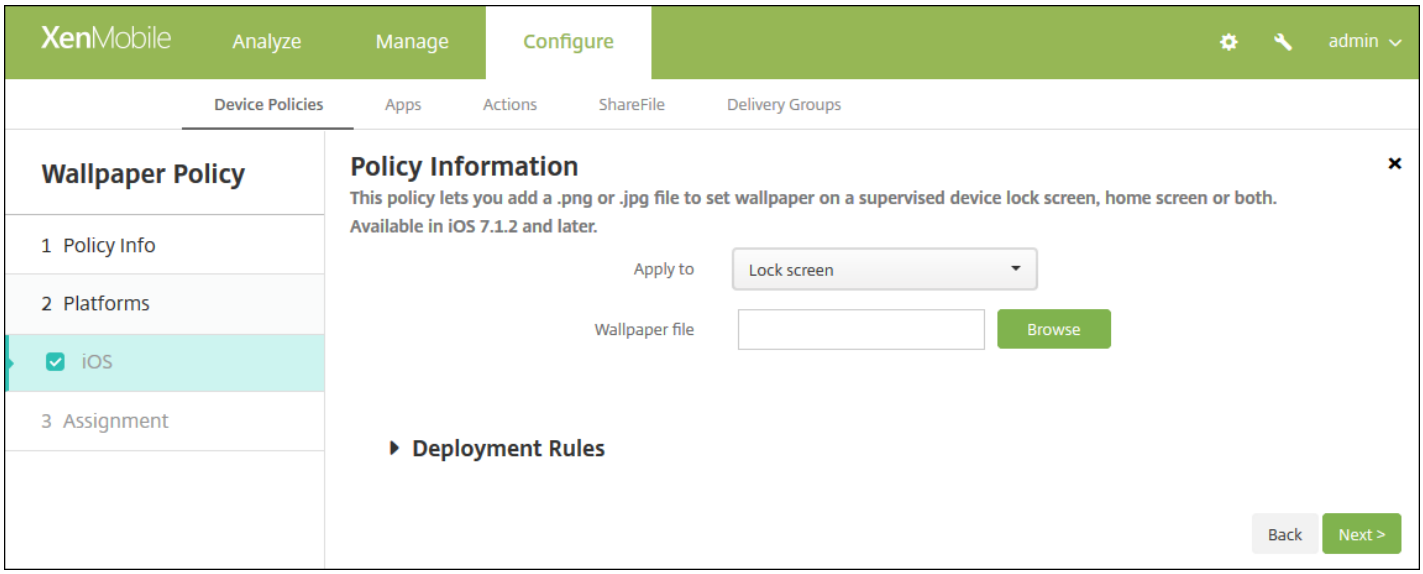
Configurer les paramètres PPTP

7. Configurez les règles de déploiement.



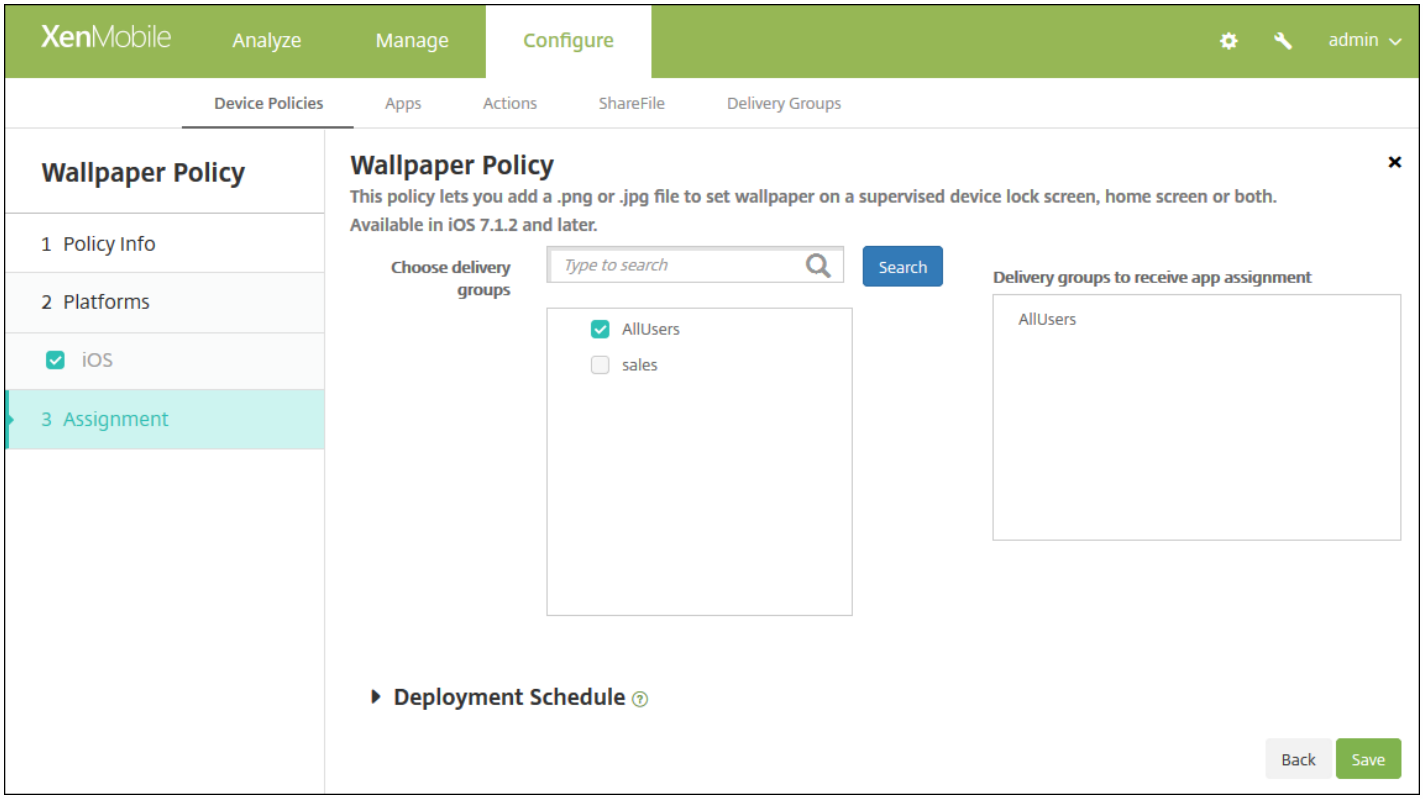
-
-
-
-
-
-
-

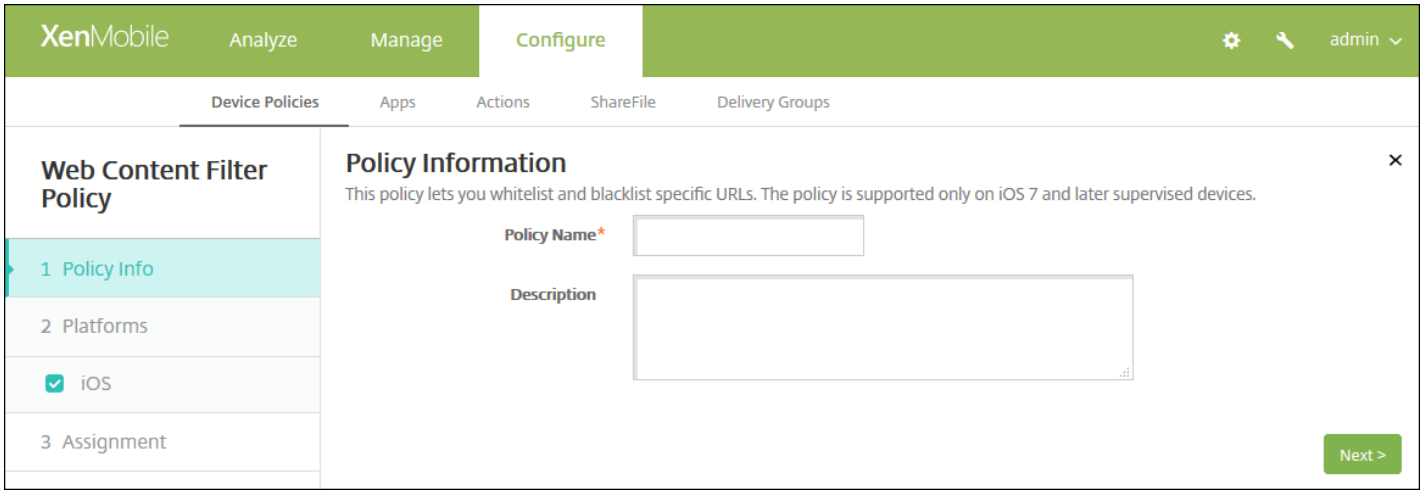
-
-



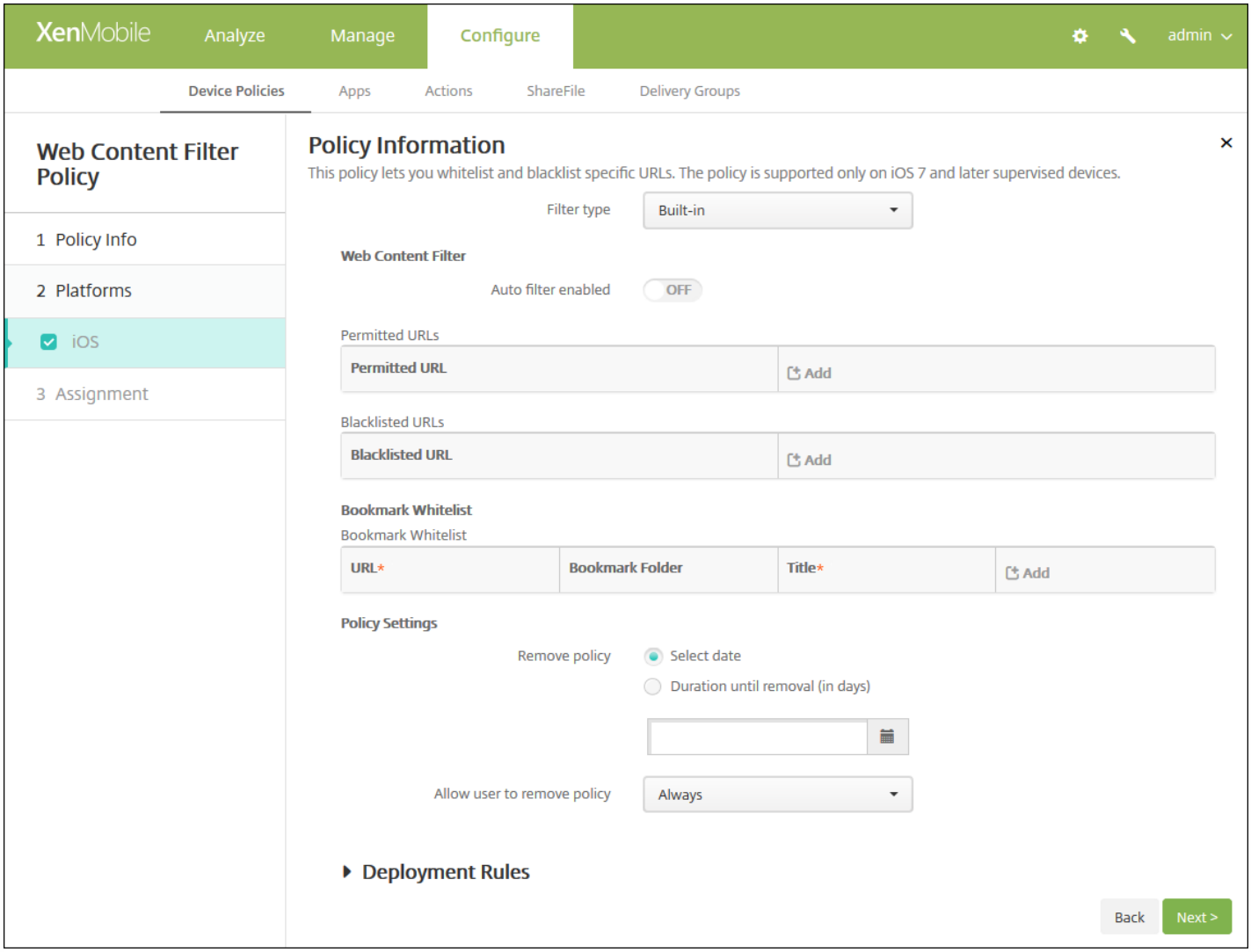
-
-

7. Configurez les règles de déploiement.





-
-



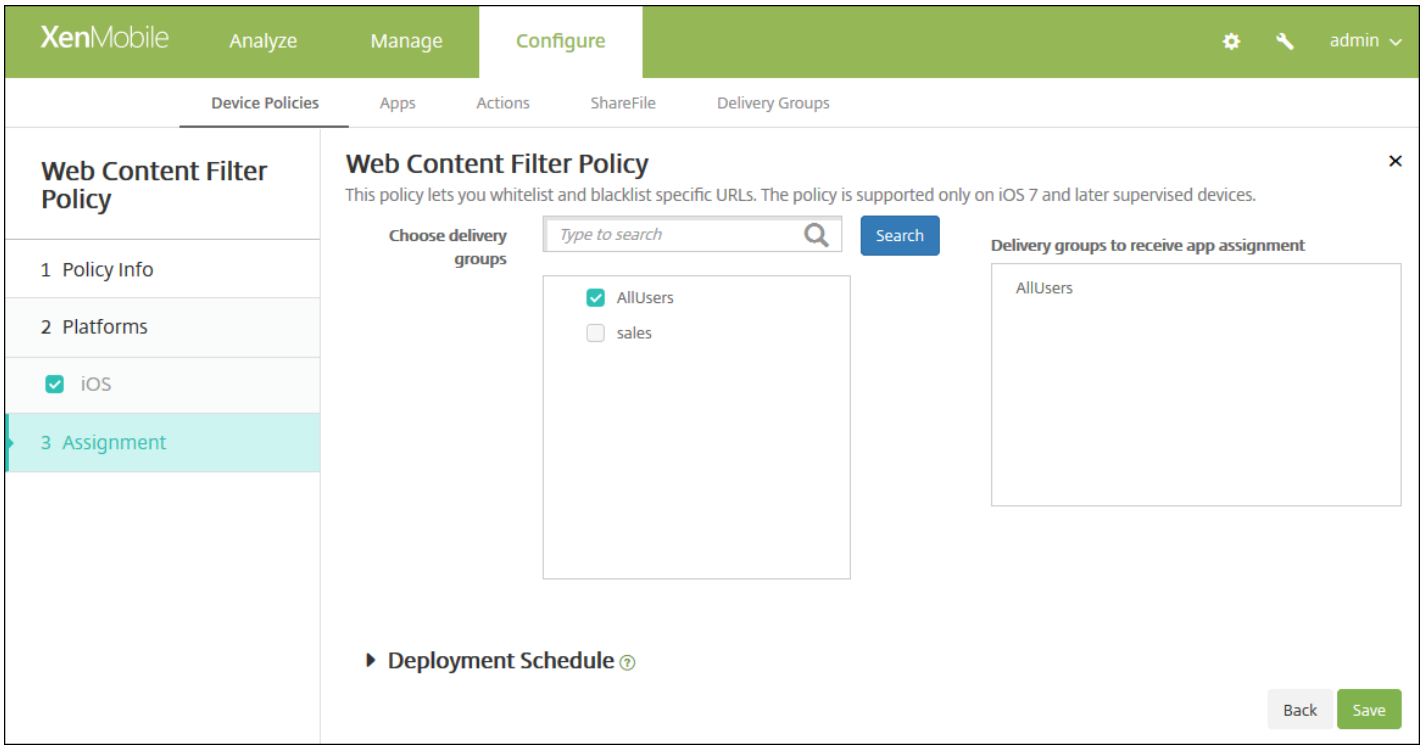
-

Paramètres du type de filtre Intégré

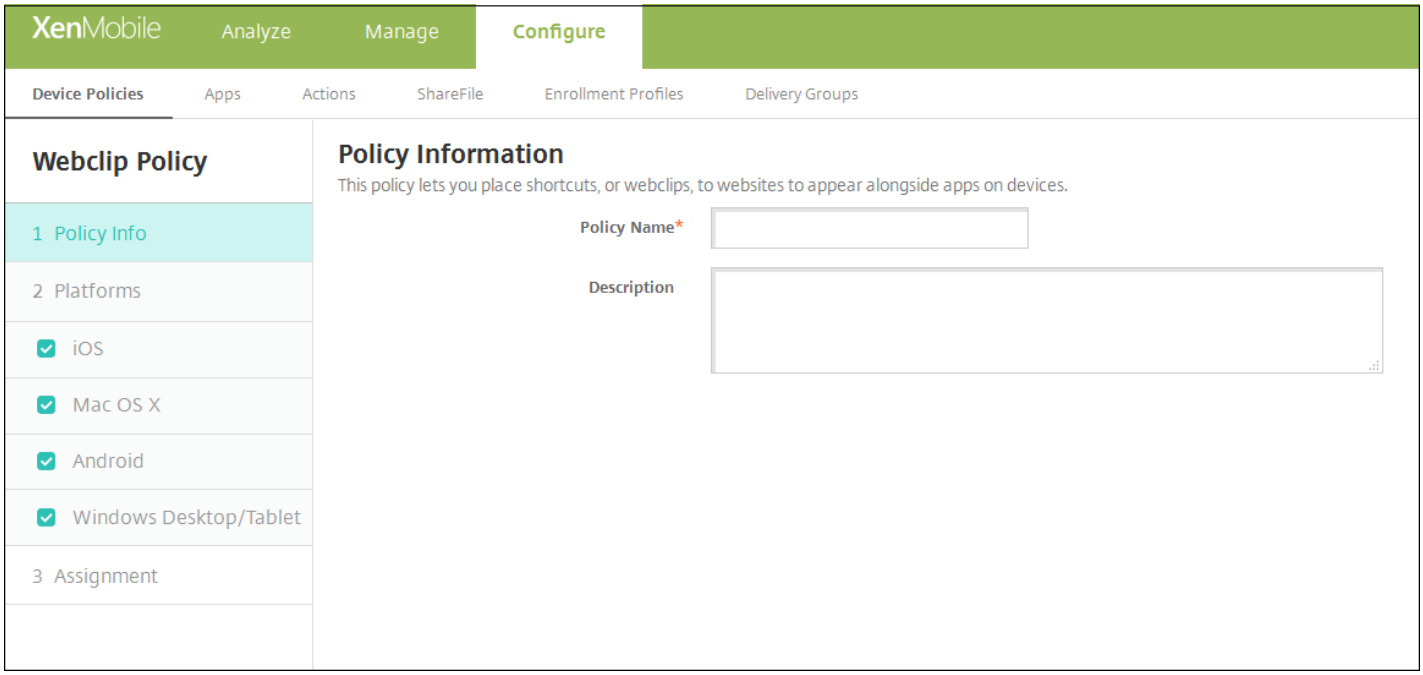
Paramètres du type de filtre Plug-in

-
  -
  -
  -
  -

7. Configurez les règles de déploiement.

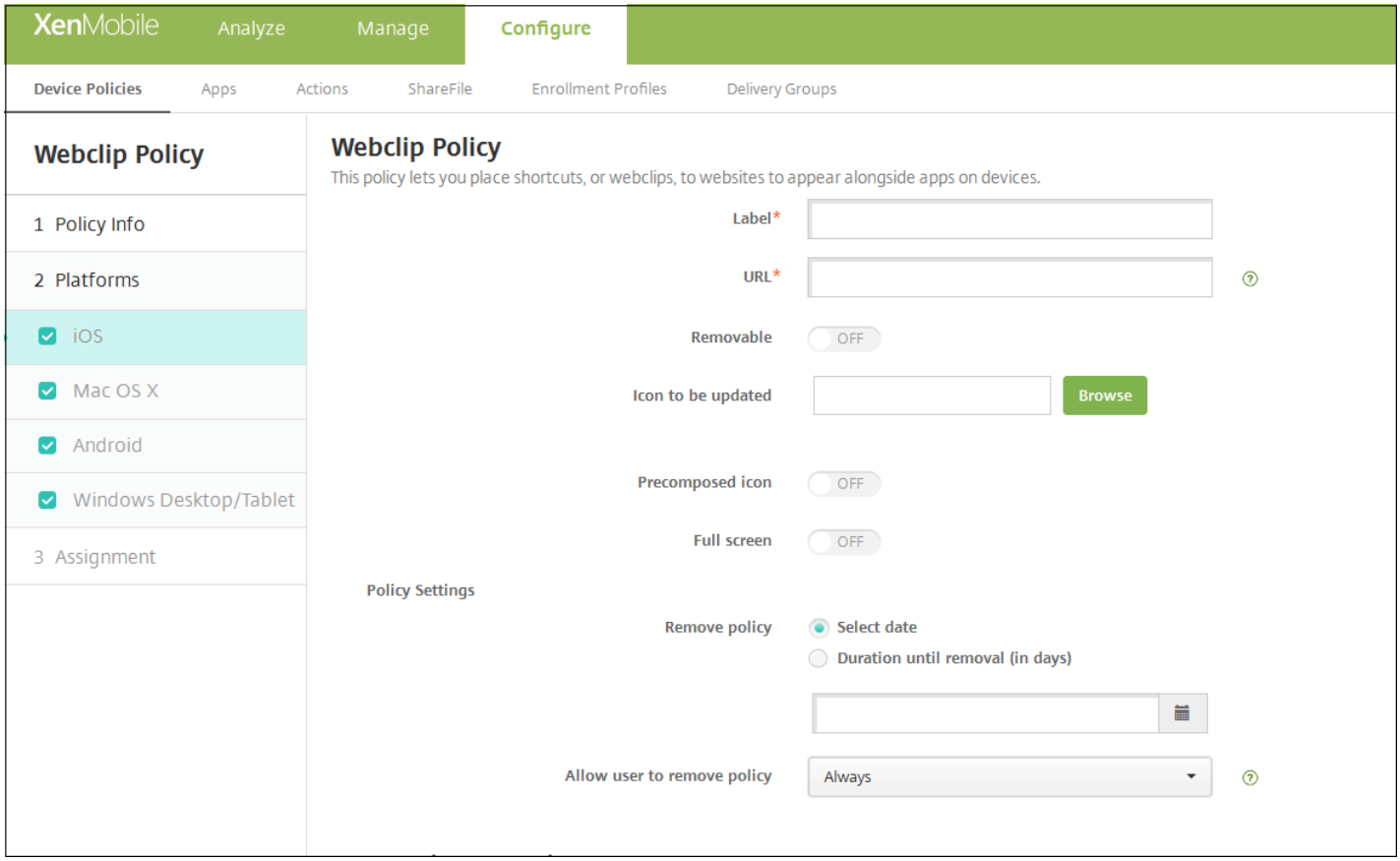


-



-
-

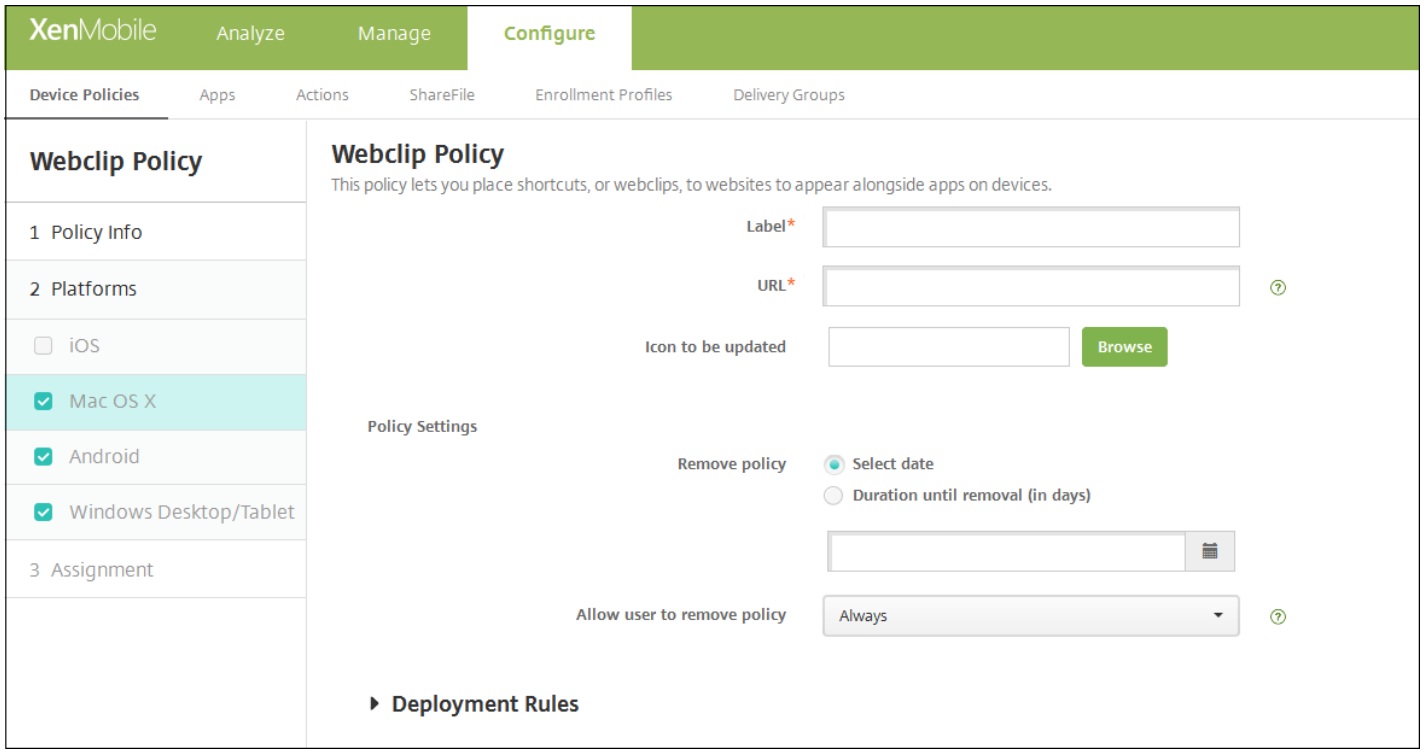
Configurer les paramètres pour iOS



-
-
-
-
-
-
-
  -
  -

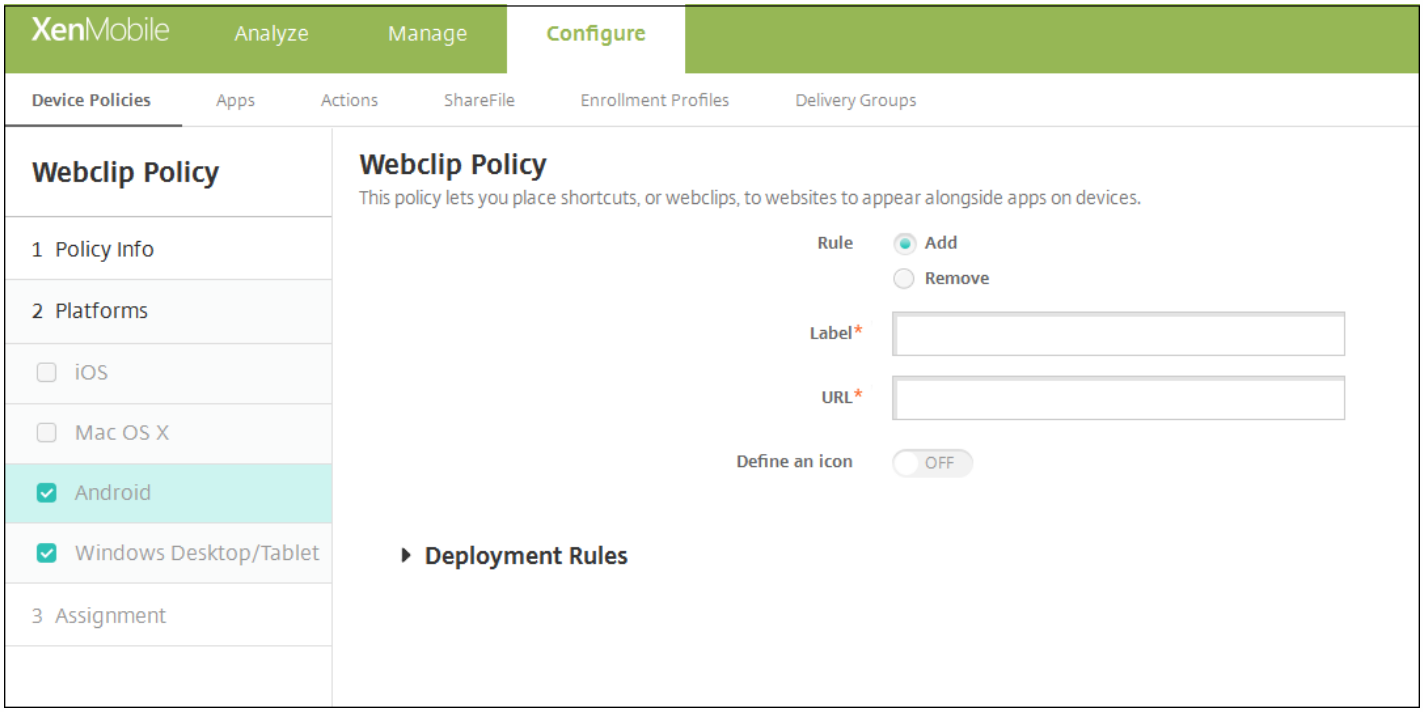
-
-

Configurer les paramètres pour Mac OS X



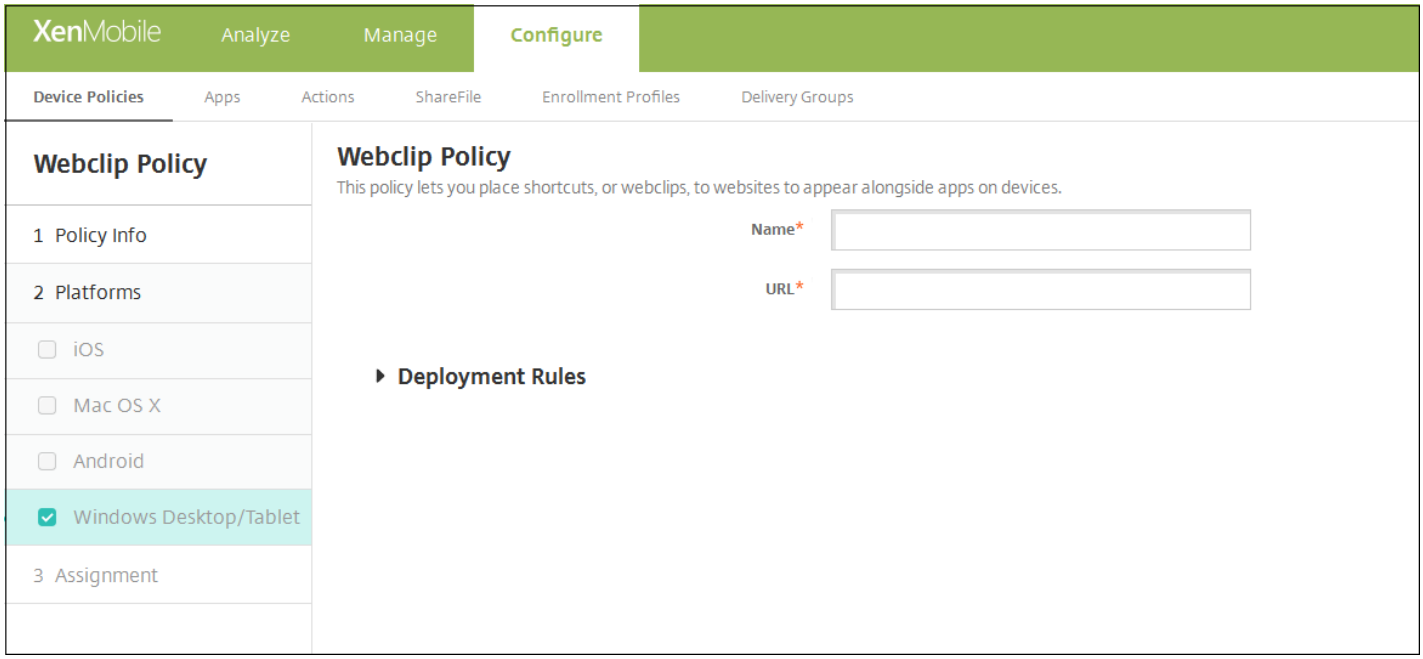
-
-
-
-
  -
  -
  -
  -
  -

Configurer les paramètres pour Android



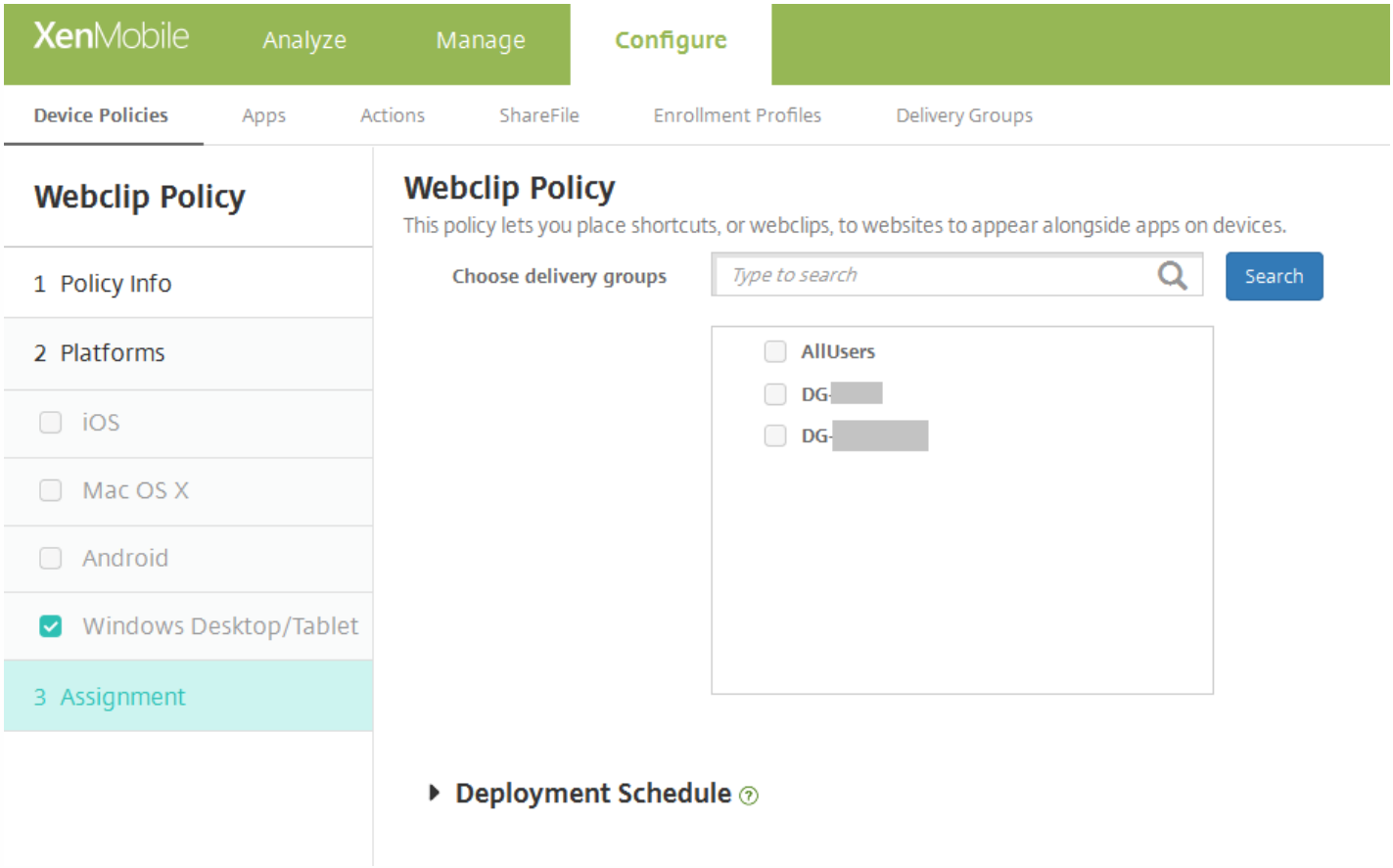
-
-
-
-
-

Configurer les paramètres pour Windows Desktop/Tablet



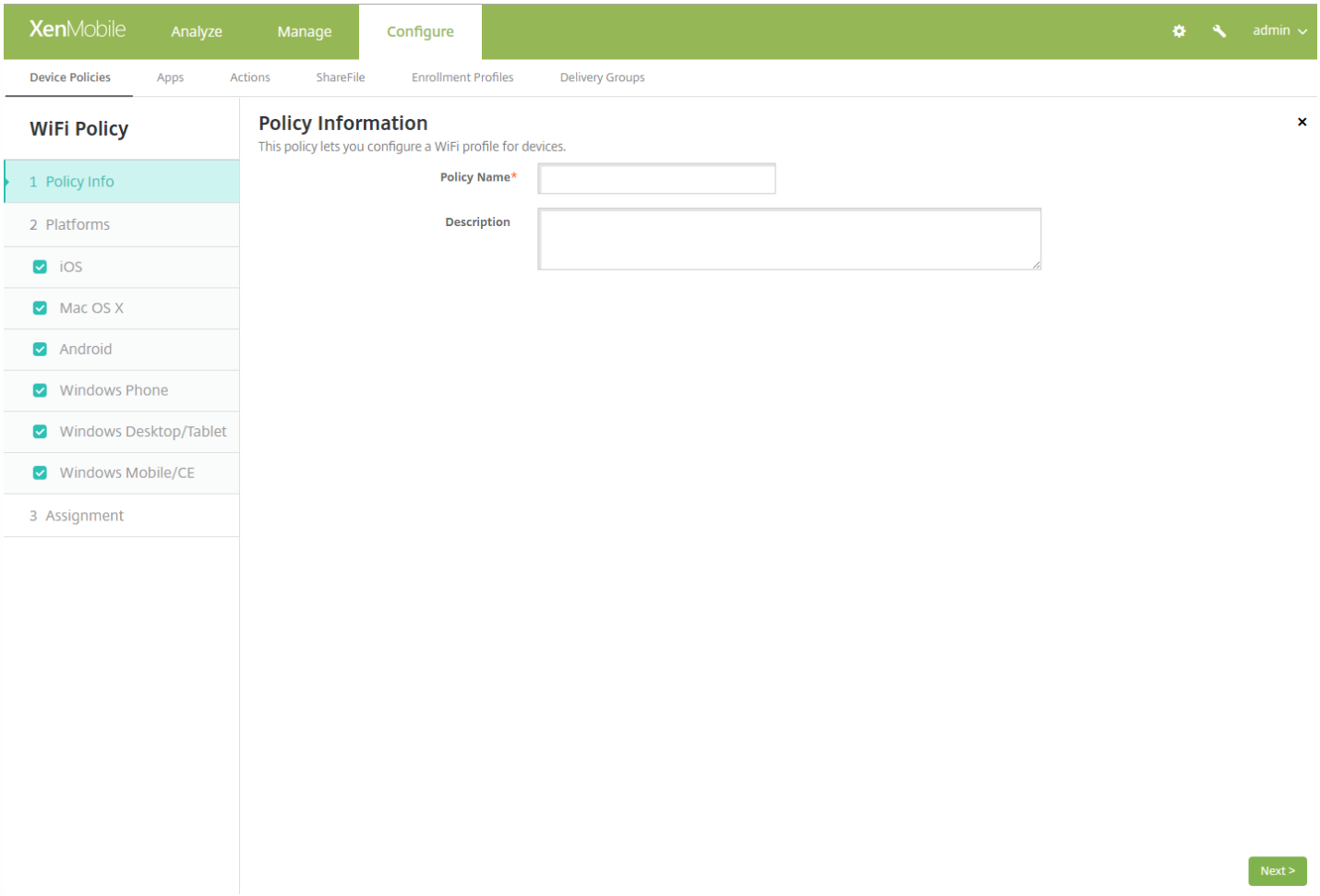
-
-

7. Configurez les règles de déploiement.



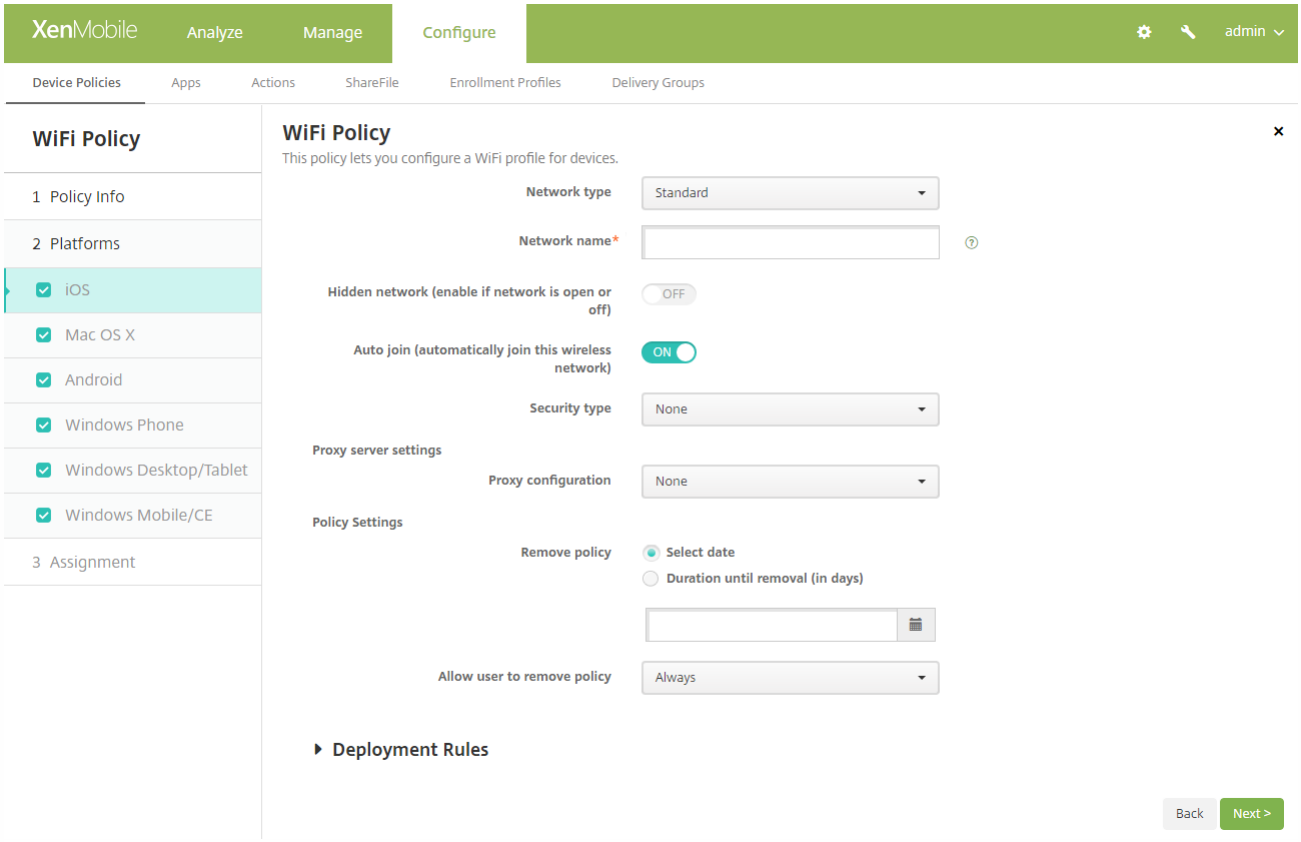
-
-
-
-
-
-

-



-
-

Configurer les paramètres pour iOS



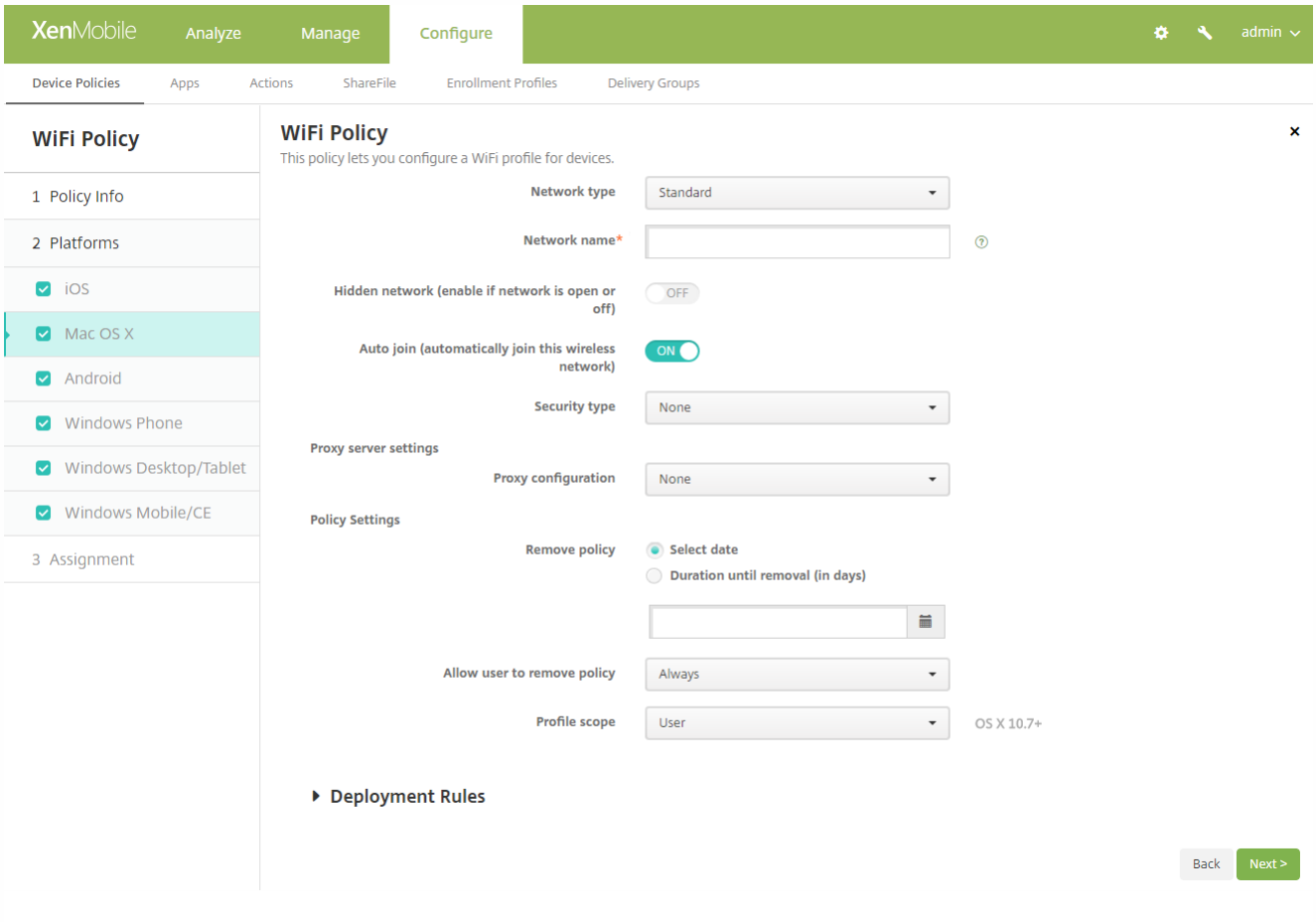
-
-
-
-
-
  -
  -
  -
  -
  -
  -
  -
  -

WPA, WPA Personnel, Tous (Personnel)

WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise)

-
  -
    -
      -
      -
      -
      -
    -
      -
      -
-
  -
  -
  -
  -

Configurer les paramètres pour Mac OS X



-
-
-
-
-
  -
  -
  -
  -
  -
  -
  -
  -

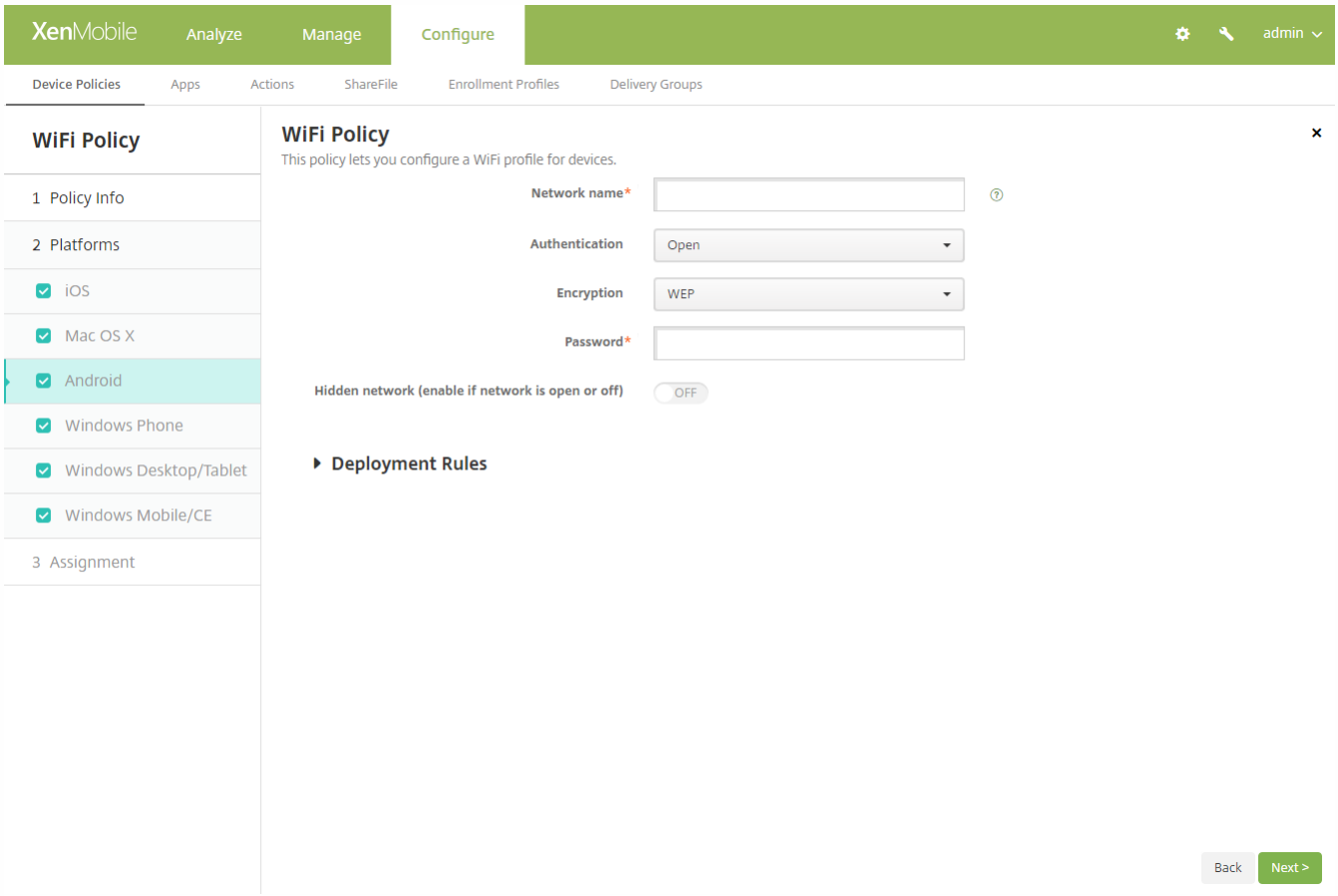
WPA, WPA Personnel, WPA 2 Personnel, Tous (Personnel)

WEP Entreprise, WPA Entreprise, WPA2 Entreprise, Tous (Entreprise)

-
-
  -
  -
    -
      -
      -
      -
      -
    -
      -
      -

-
  -
  -
  -
  -
  -

Configurer les paramètres pour Android



-
-
  -
  -
  -
  -
  -
  -
  -

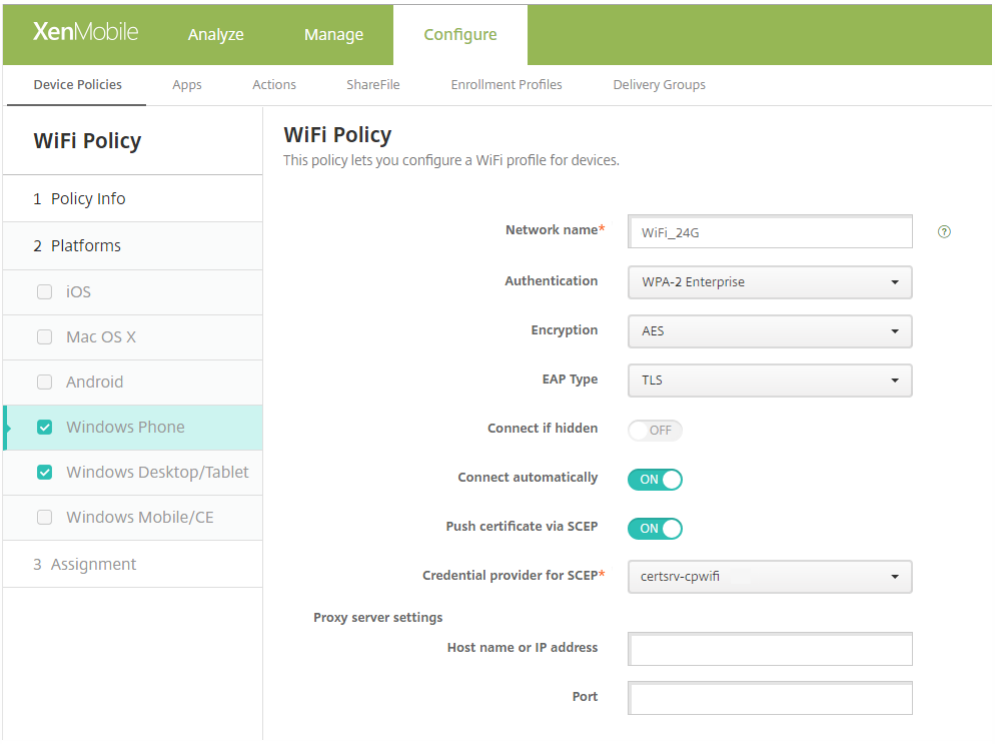
Ouvert, partagé

WPA, WPA-PSK, WPA2, WPA2-PSK

802.1x

-

Configurer les paramètres pour Windows Phone



-
-
  -
  -
  -
  -

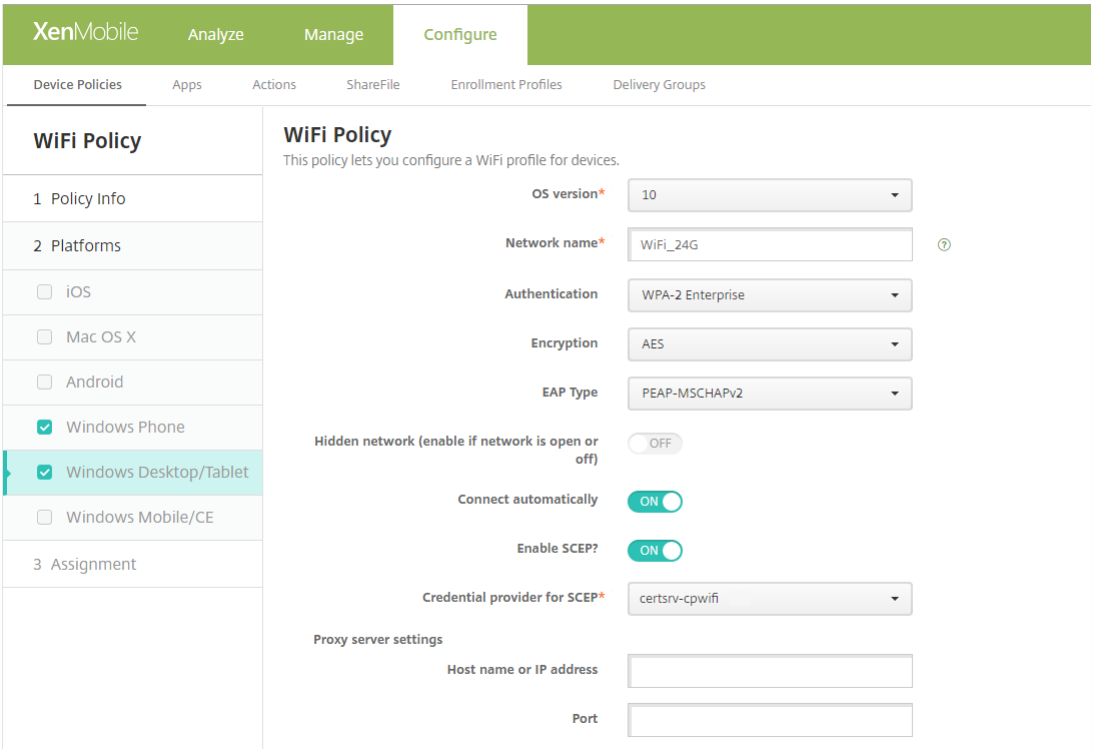
Ouverte

WPA Personnel, WPA-2 Personnel

WPA-2 Enterprise

-
  -
  -

Configurer les paramètres pour Windows Desktop/Tablet



-
-
  -
  -
  -
  -
  -

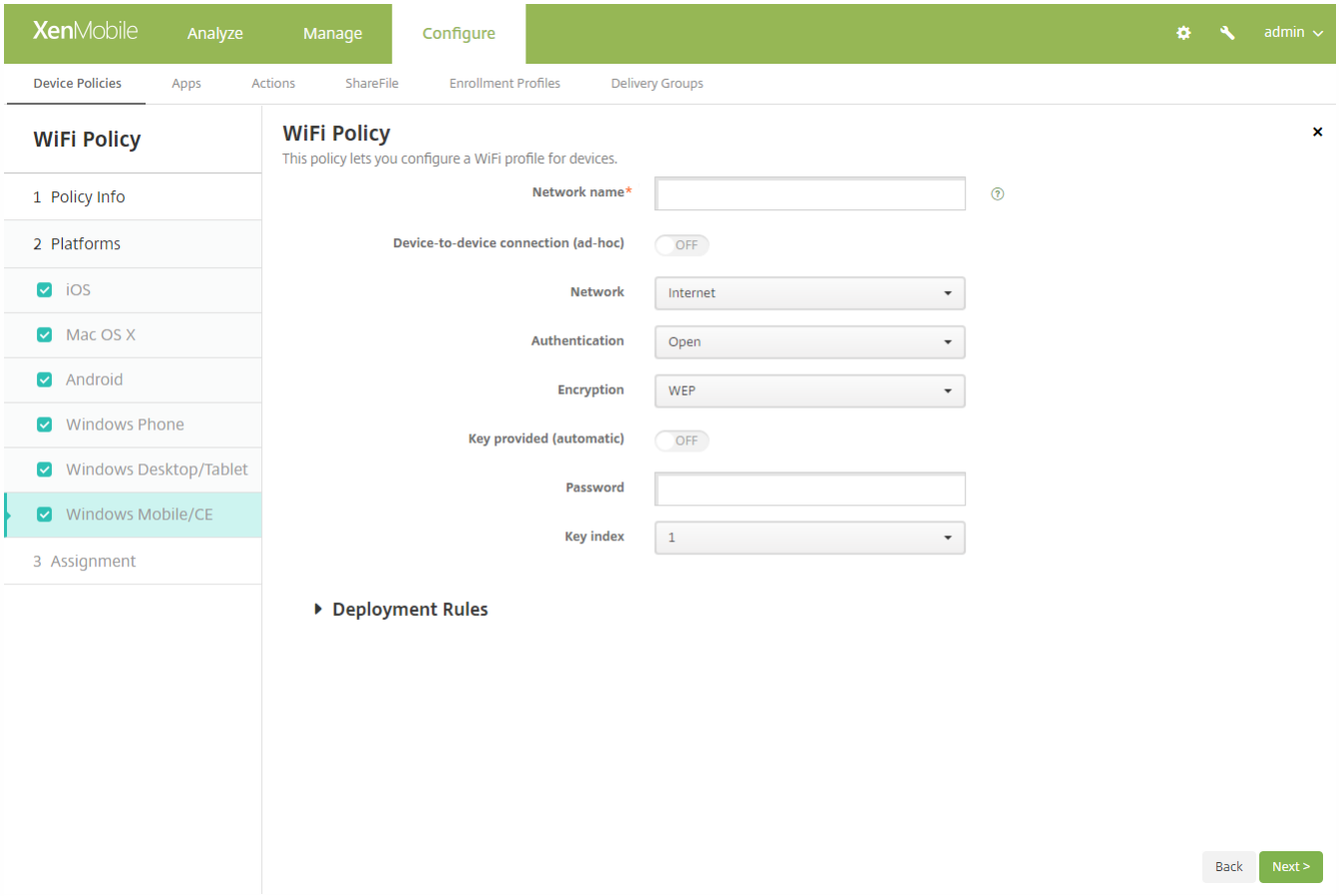
Ouverte

WPA Personnel, WPA-2 Personnel

WPA-2 Enterprise

-
-
  -
  -
  -
  -
  -
-
-

Configurer Windows Mobile/CE



-
-
-
-
  -
  -
  -
  -

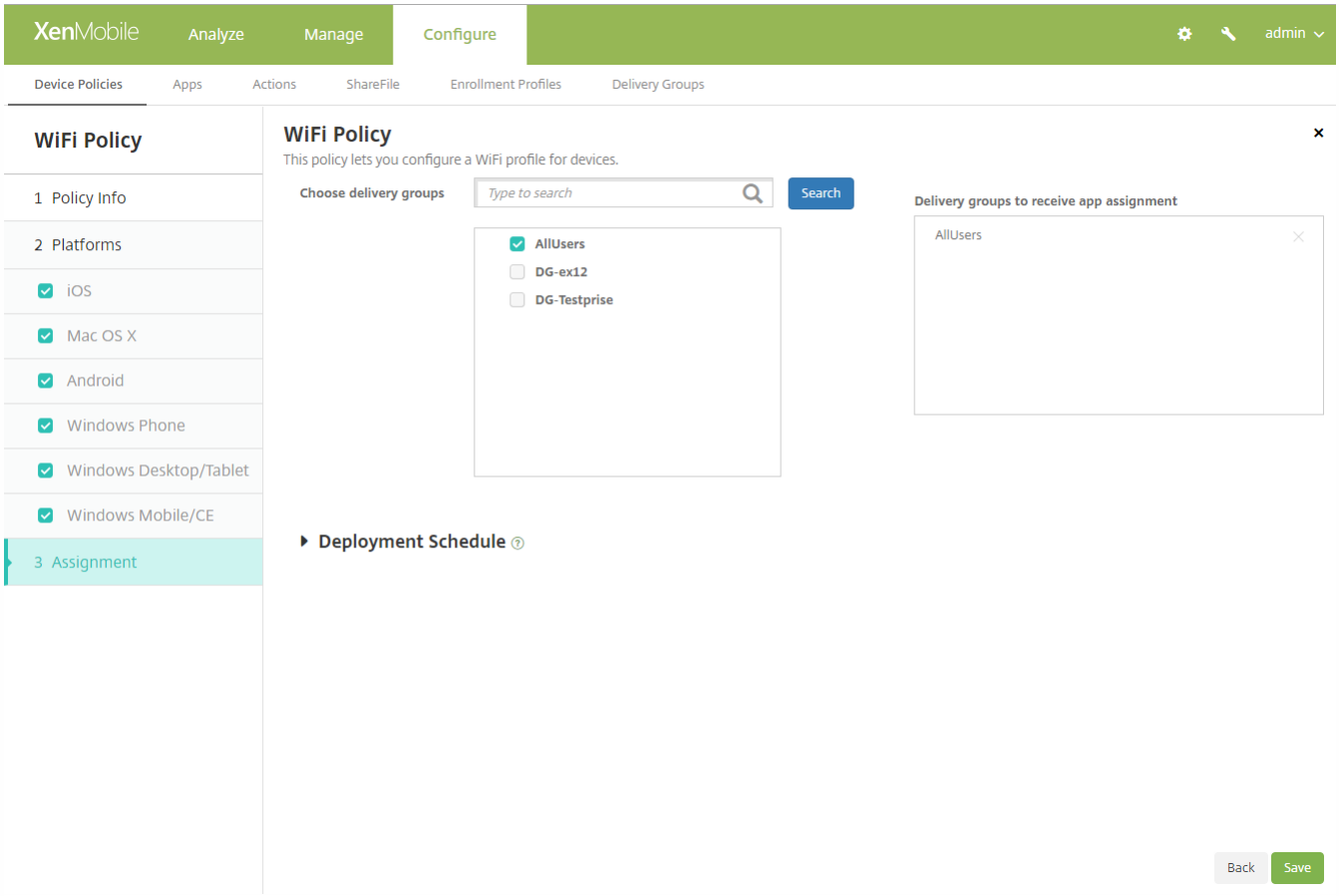
Ouverte

WPA Personnel, WPA-2 Personnel

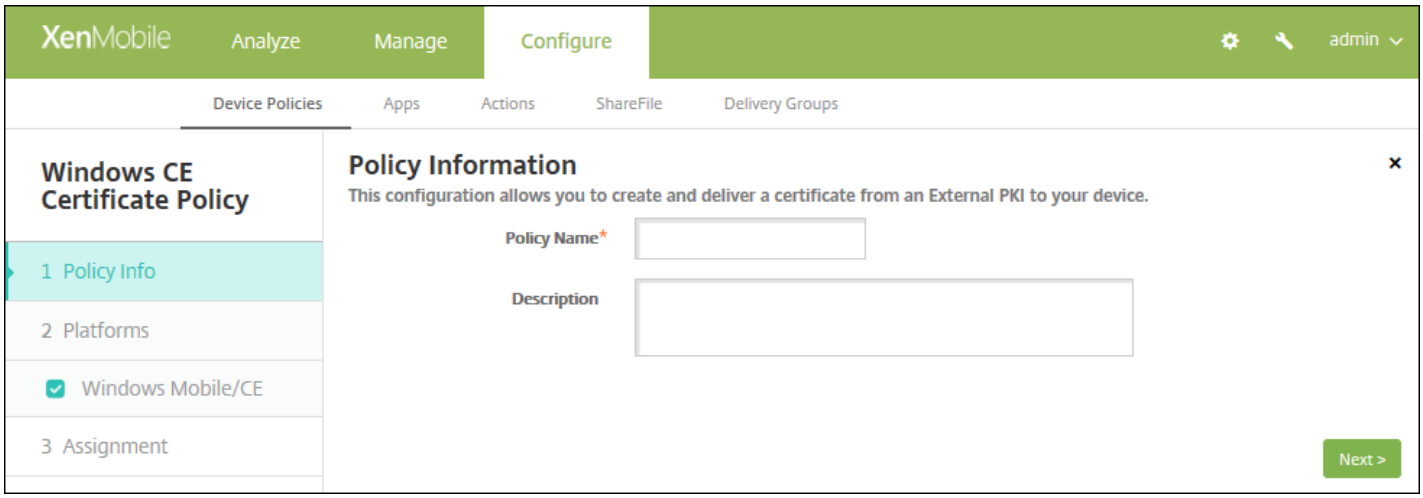
WPA-2 Enterprise

-
-
-

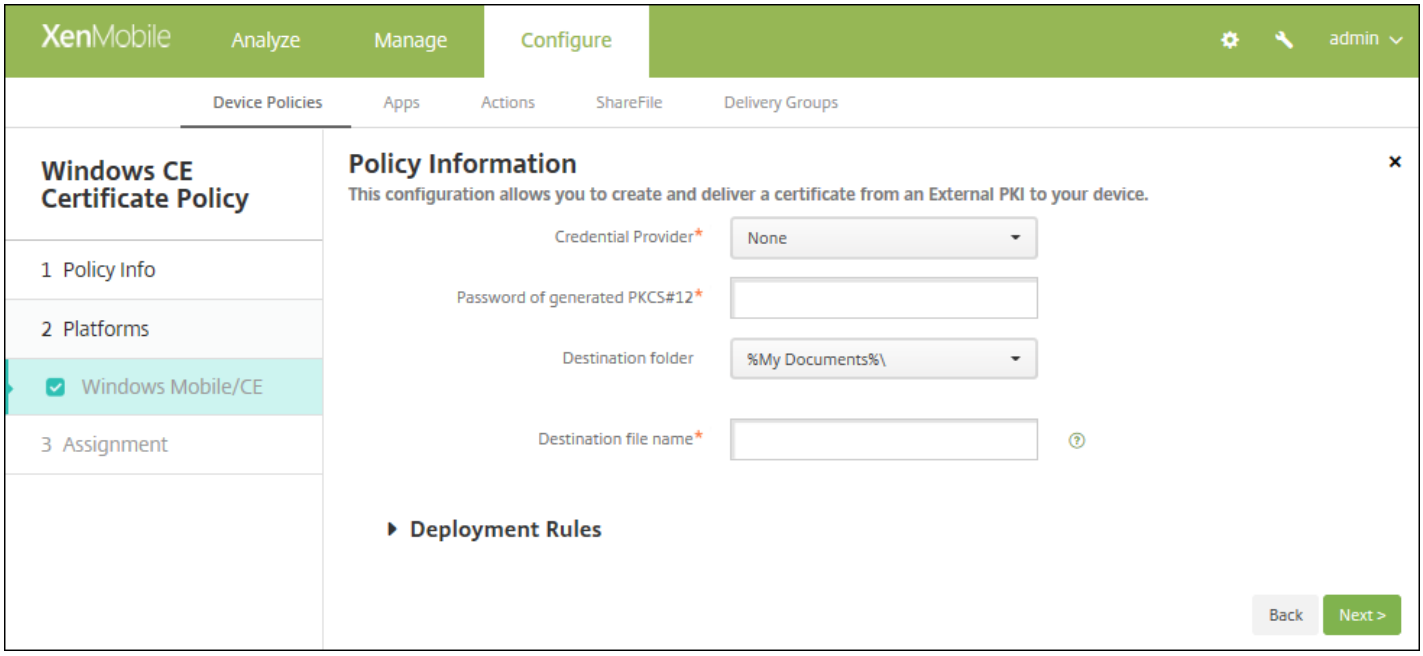
7. Configurez les règles de déploiement.



-
-
-
-
-
-
-

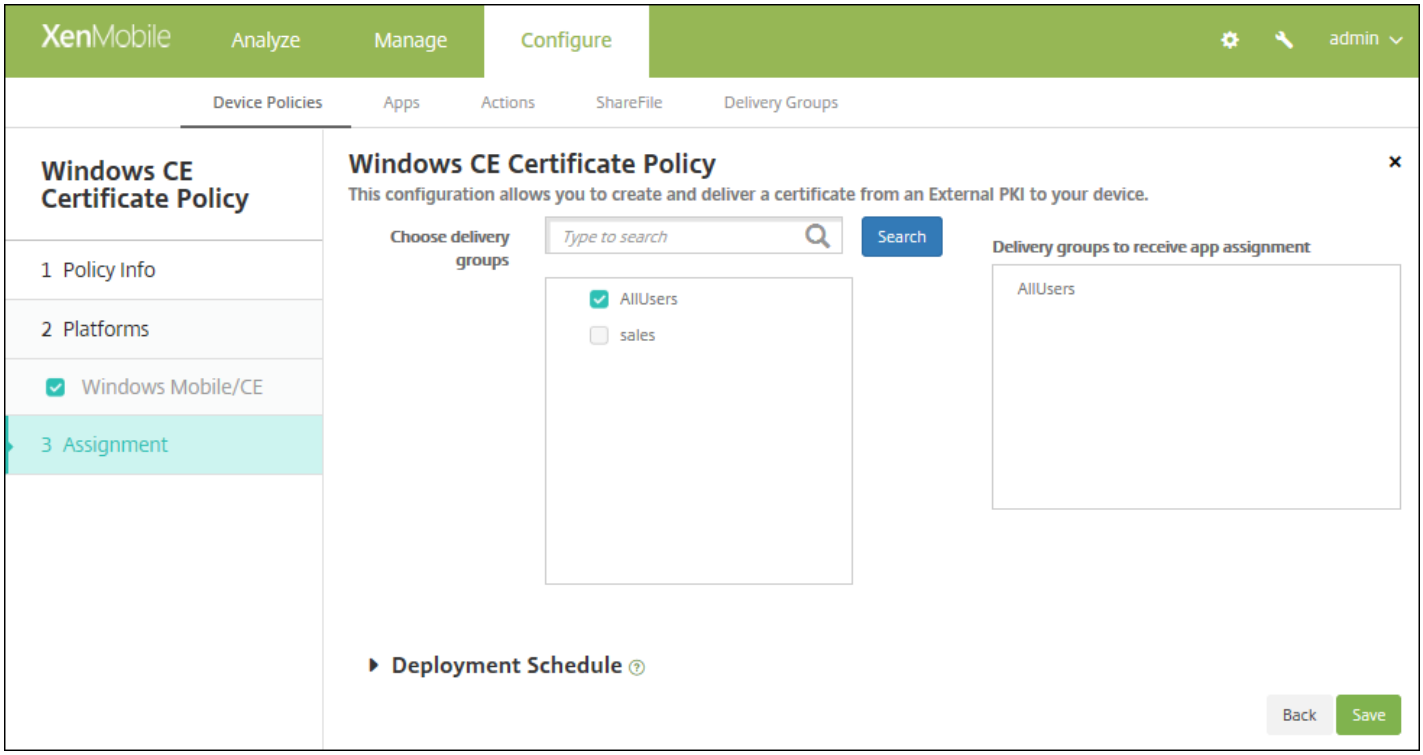


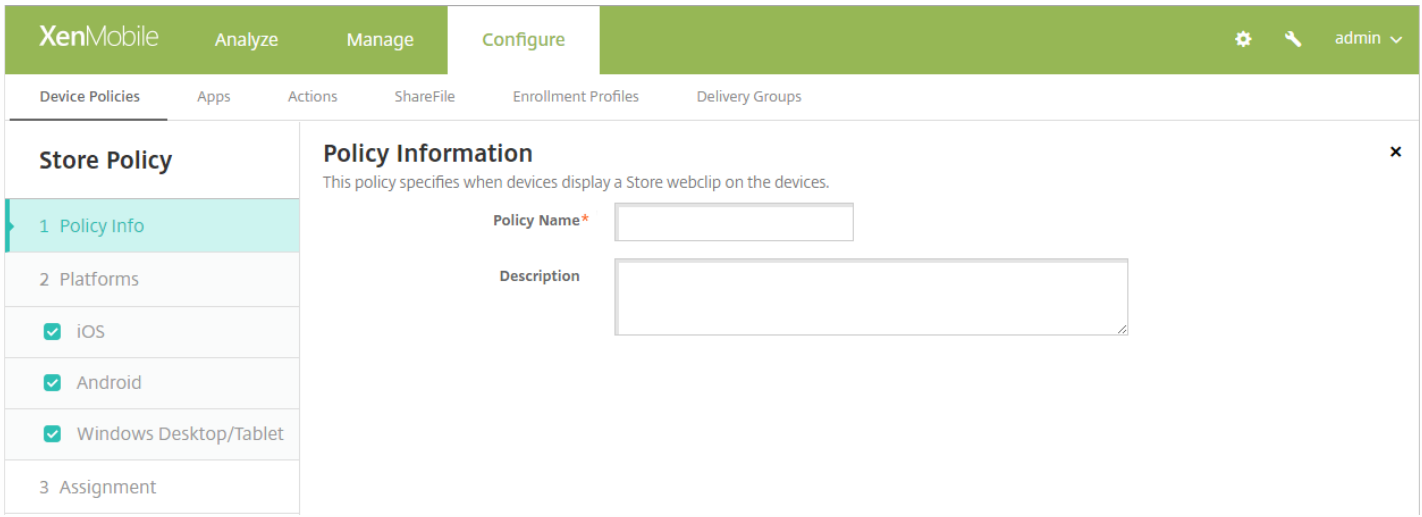
-
-



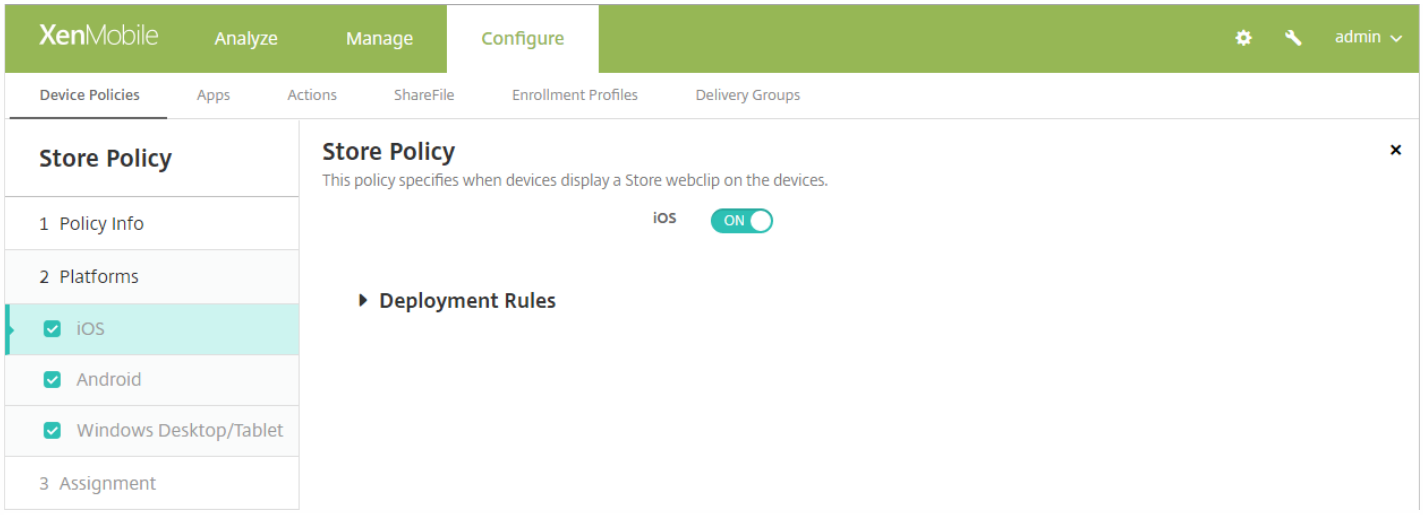
-
-
-
  -
  -
  -
  -
  -
-

7. Configurez les règles de déploiement.



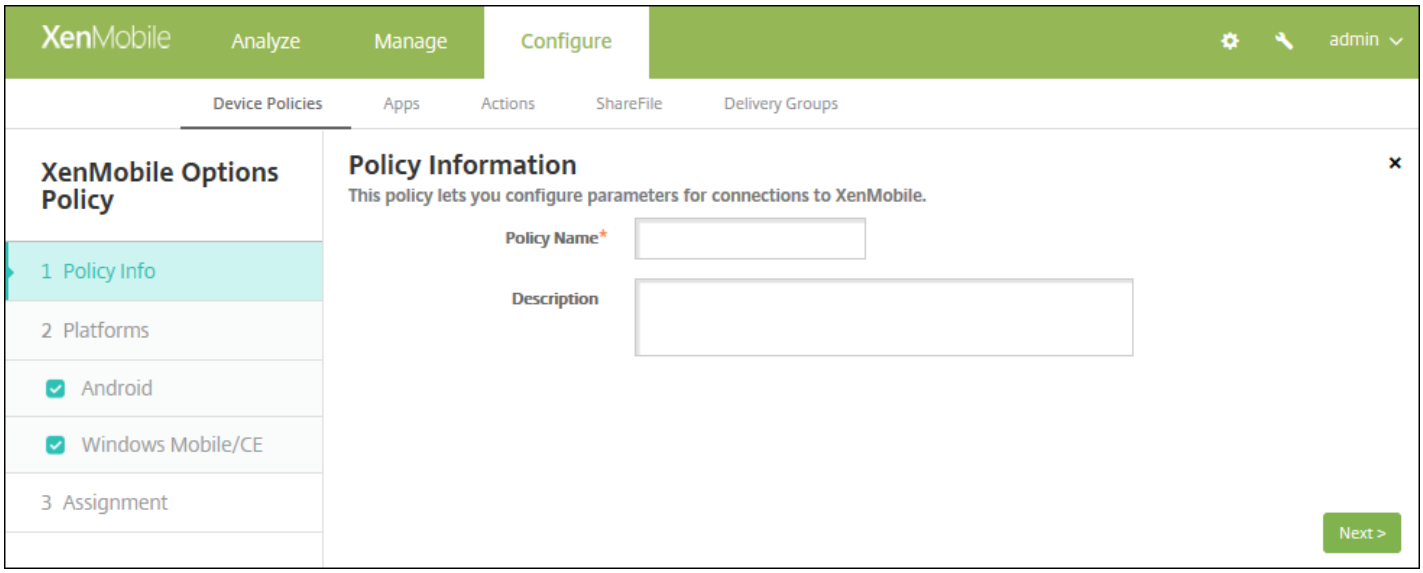


-
-



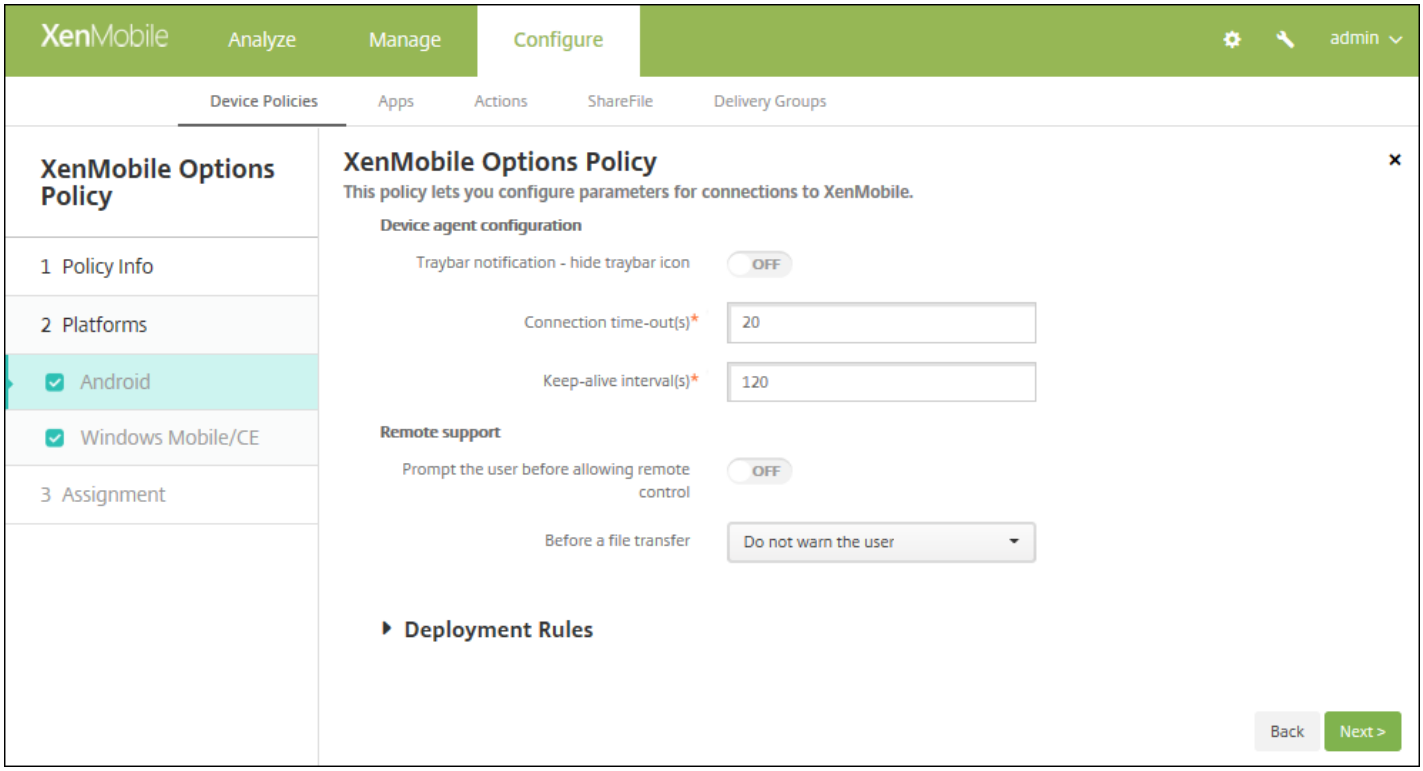
8. Configurer les règles de déploiement

-



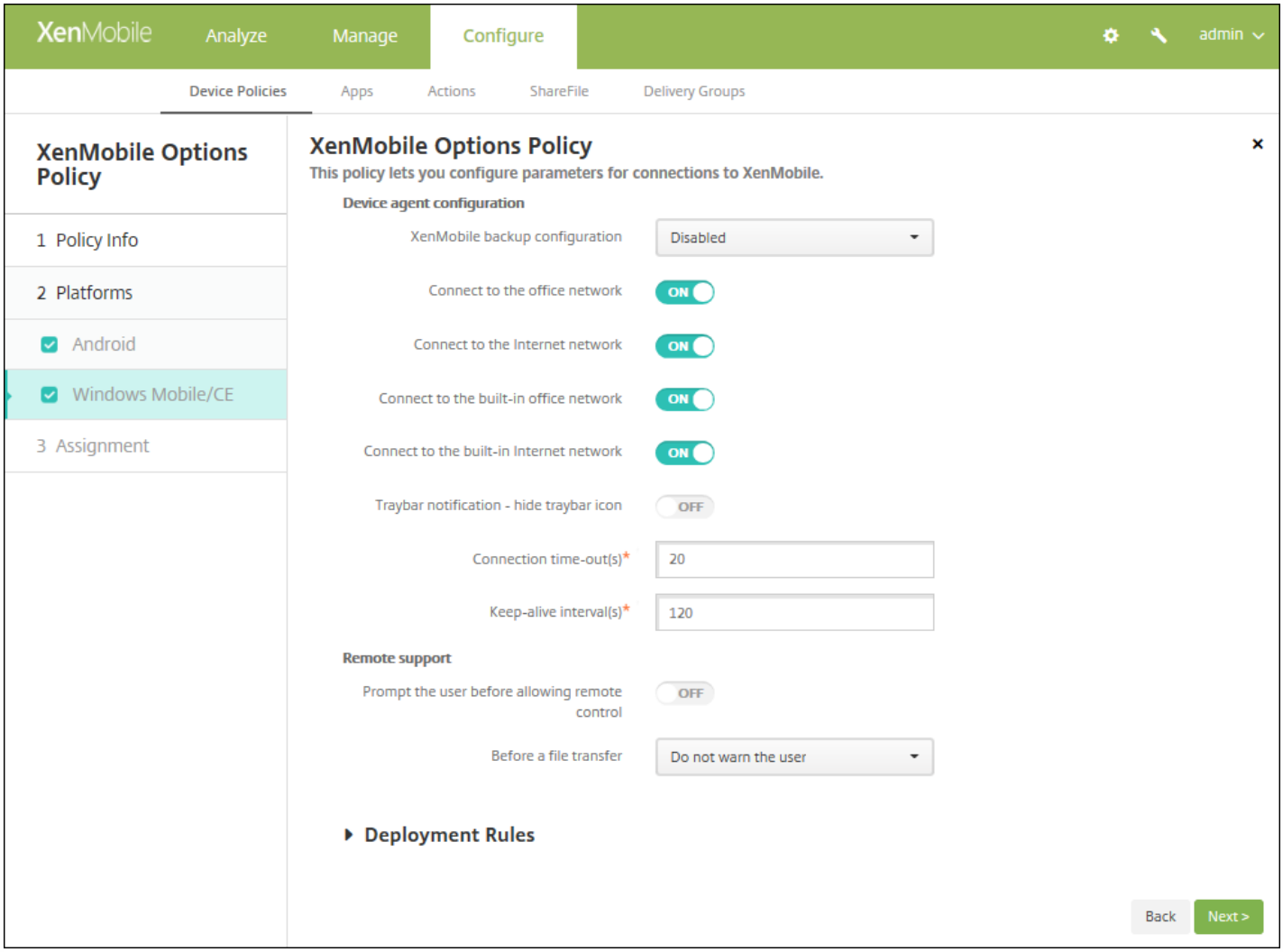
-
-

Configurer les paramètres pour Android



-
-
-
-
-

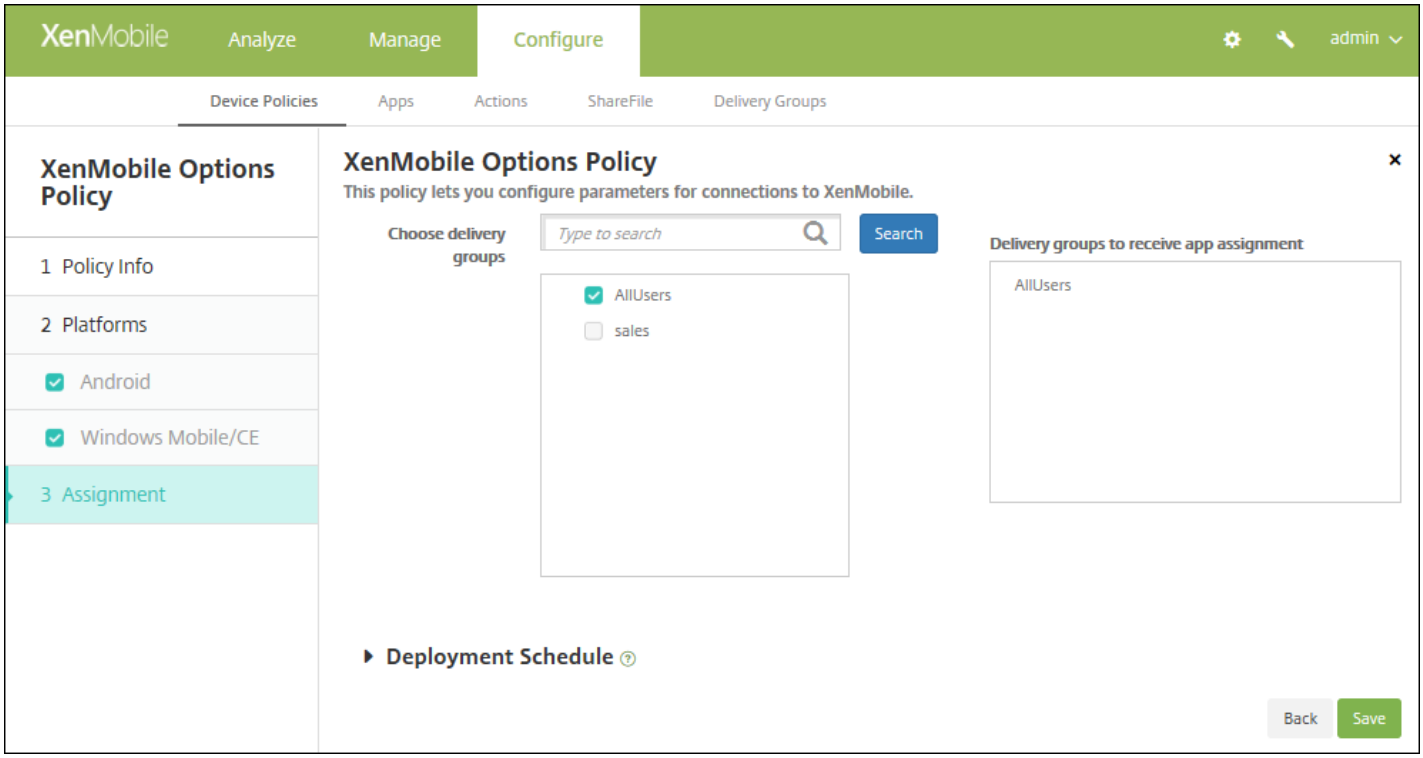
Configurer les paramètres pour Windows Mobile/CE



-
  -
    -
    -
    -
  -
  -
  -
  -
  -
  -

-
-
-
-

7. Configurez les règles de déploiement.



-
-
-

-
-
-
-

Stratégies de désinstallation de XenMobile

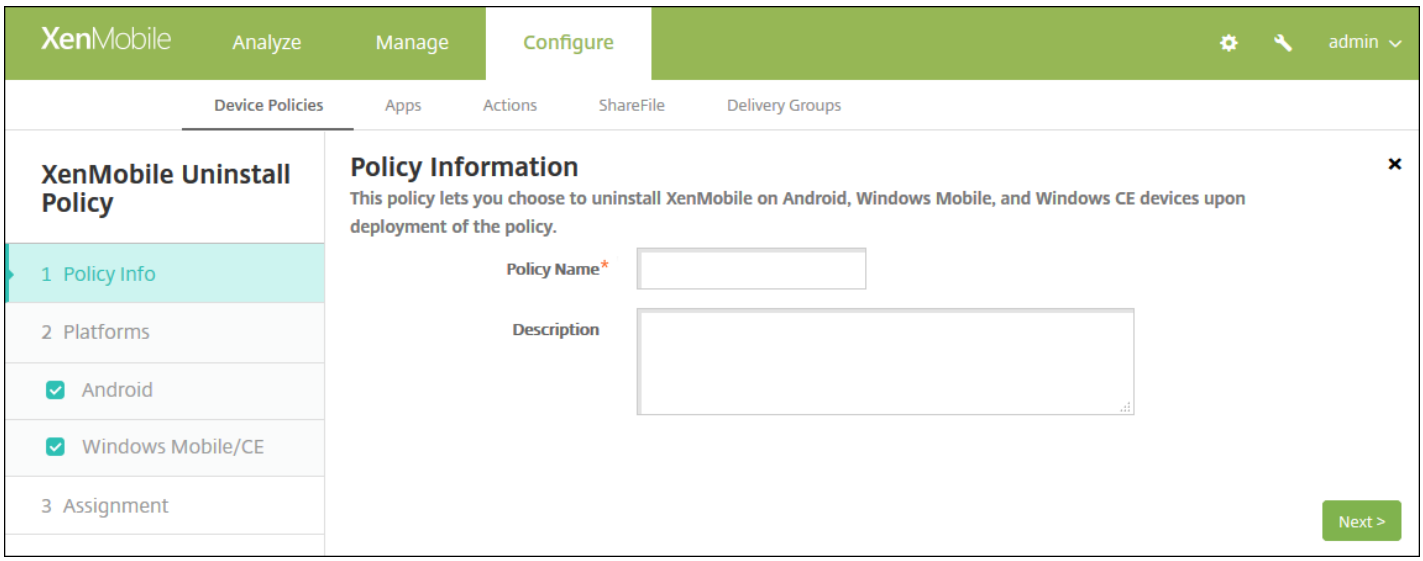
Feb 23, 2017

Vous pouvez ajouter une stratégie dans XenMobile afin de désinstaller XenMobile des appareils Android et Windows Mobile/CE. Lorsqu'elle est déployée, cette stratégie supprime XenMobile sur tous les appareils du déploiement.

1. Dans la console XenMobile, cliquez sur **Configurer > Stratégies d'appareil**. La page **Stratégies d'appareil** s'affiche.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une nouvelle stratégie** apparaît.

3. Développez **Plus**, puis, sous **Agent XenMobile**, cliquez sur **Désinstallation de XenMobile**. La page **Stratégie de désinstallation de XenMobile** s'affiche.



4. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

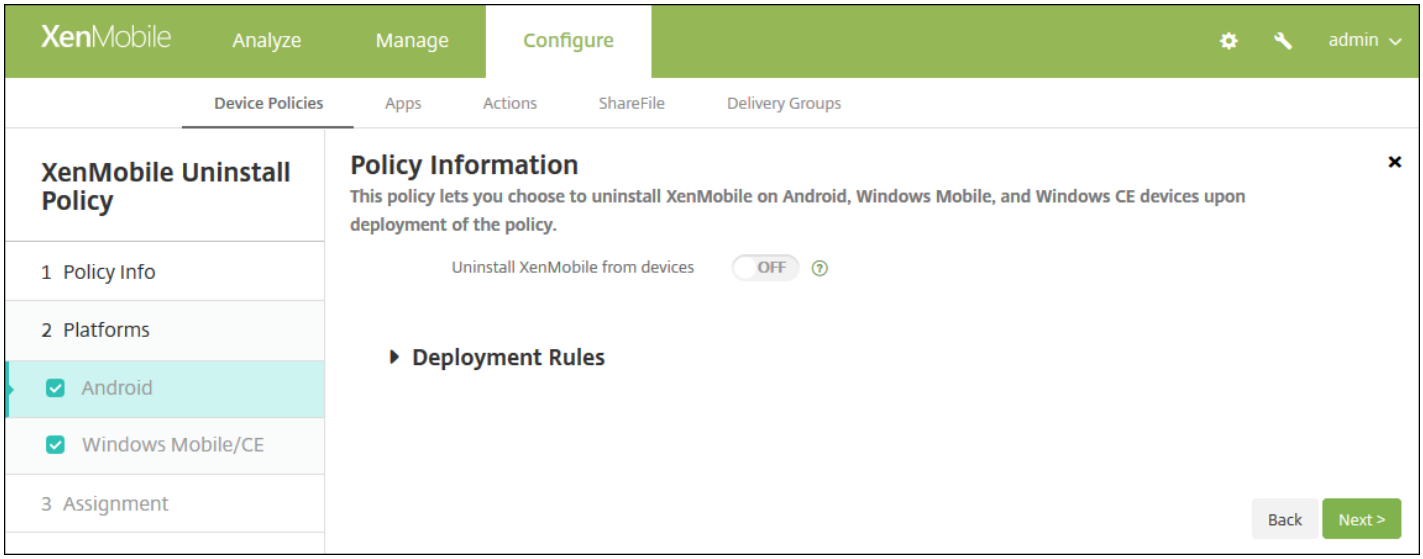
- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

5. Cliquez sur **Next**. La page d'informations **Stratégie par plate-forme** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 7 pour savoir comment définir les règles de déploiement de cette plate-forme.

Configurer les paramètres pour Android et Windows Mobile/CE

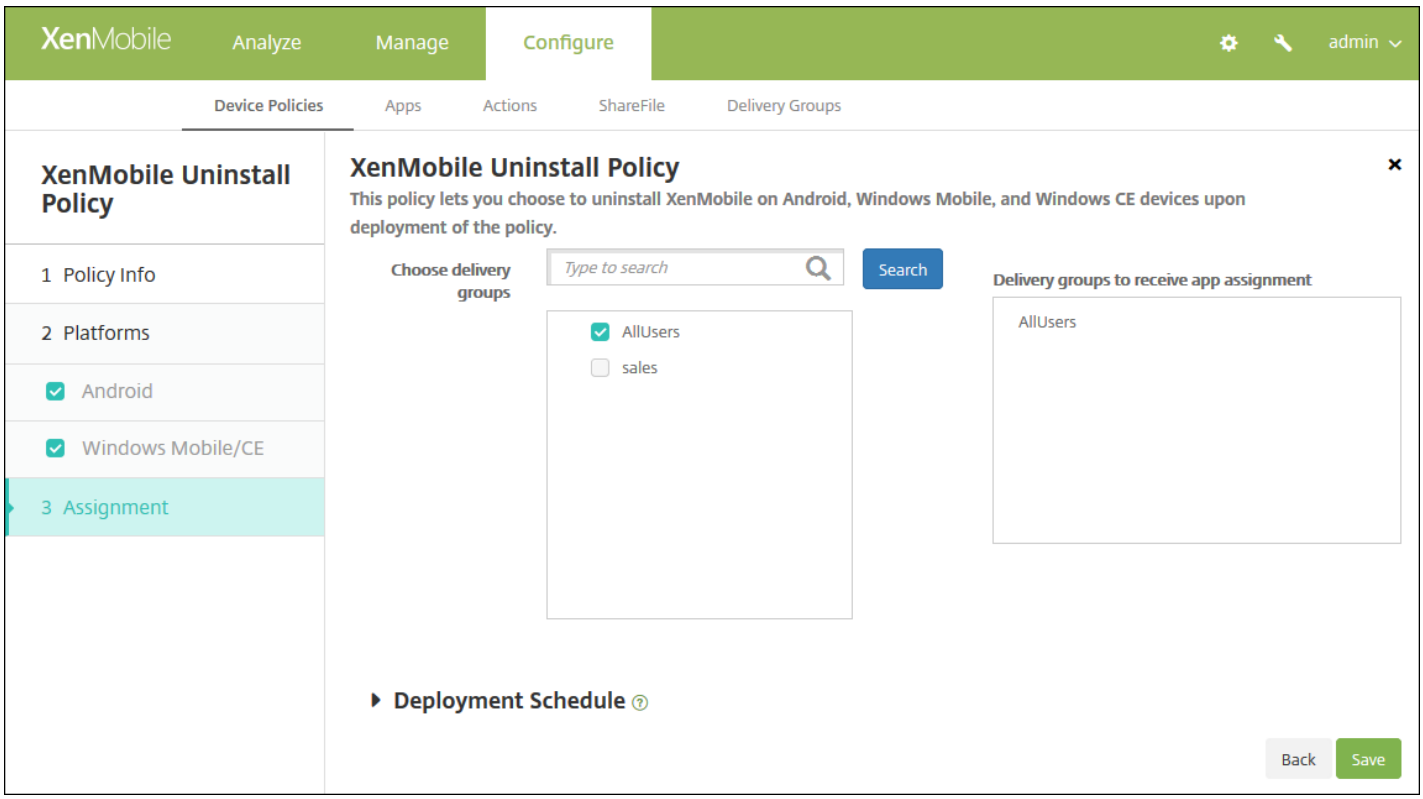


Configurez ce paramètre pour chaque plate-forme que vous sélectionnez :

- **Désinstaller XenMobile des appareils** : sélectionnez cette option pour désinstaller XenMobile de chaque appareil sur lequel vous déployez cette stratégie. La valeur par défaut est **OFF**.

7. Configurez les règles de déploiement.

8. Cliquez sur **Suivant**. La page d'attribution de la **Stratégie de désinstallation de XenMobile** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou

sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

Ajouter des applications à XenMobile

Feb 23, 2017

Vous pouvez ajouter des applications à XenMobile pour en assurer la gestion. Vous ajoutez les applications à la console XenMobile, où vous pouvez organiser les applications par catégorie et les déployer auprès des utilisateurs.

Vous pouvez ajouter les types suivants d'applications à XenMobile :

- **MDX**. Ce sont des applications wrappées avec le MDX Toolkit (et les stratégies associées). Vous déployez des applications MDX que vous avez obtenues depuis des magasins internes et publics.
- **Magasin d'applications public**. Ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin d'applications public, tel que iTunes ou Google Play. Par exemple : GoToMeeting.
- **Web et SaaS**. Ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). Vous pouvez créer vos propres applications, ou faire votre choix parmi un ensemble de connecteurs d'applications pour l'authentification unique aux applications Web existantes. Par exemple : GoogleApps_SAML.
- **Entreprise**. Ces applications sont des applications natives qui ne sont pas wrappées avec le MDX Toolkit et qui ne contiennent aucune des stratégies associées aux applications MDX.
- **Lien Web**. Il s'agit d'une adresse Web (URL) à un site public ou privé, ou à une application Web qui ne requiert pas d'authentification unique (SSO).

> ## Remarque
>
> Citrix prend en charge l'installation silencieuse d'applications iOS et Samsung Android. Une installation silencieuse signifie que les utilisateurs ne sont pas invités à installer les applications que vous déployez sur l'appareil ; les applications sont installées de manière silencieuse en arrière-plan. Vous devez remplir les conditions suivantes pour pouvoir effectuer une installation silencieuse :
>
> - Pour les applications iOS, l'appareil iOS géré doit être en mode supervisé. Pour de plus amples informations, consultez la section Importer des stratégies de profil iOS et Mac OS X.
> - Pour les applications Android, des stratégies Samsung for Enterprise (SAFE) ou KNOX doivent être activées sur l'appareil. Pour ce faire, vous devez définir la stratégie de clé de licence MDM Samsung pour générer des clés de licence KNOX et SamsungELM. Pour de plus amples informations, consultez la section Stratégies de clé de licence MDM Samsung.

Fonctionnement des applications mobiles et MDX

XenMobile prend en charge les applications iOS, Mac OS X, Android et Windows, y compris les applications XenMobile, telles que Secure Hub, Secure Mail et Secure Web, ainsi que l'utilisation de stratégies MDX. Grâce à la console XenMobile, vous pouvez charger des applications et les mettre à disposition sur les appareils des utilisateurs. En plus des applications XenMobile, vous pouvez ajouter les types suivants d'applications :

- Applications que vous développez pour vos utilisateurs.
- Applications dans lesquelles vous souhaitez autoriser ou interdire des fonctionnalités d'appareils à l'aide de stratégies MDX.

Pour distribuer des applications XenMobile pour iOS et Android, vous devez télécharger les fichiers MDX à partir d'un magasin public, les charger sur la console XenMobile (**Configurer > Applications**), mettre à jour les stratégies MDX en

fonction de vos besoins, puis charger les fichiers MDX sur les magasins d'applications publics.Pour de plus amples informations, consultez la section Ajouter une application MDX dans cet article.

Pour distribuer des applications XenMobile pour Windows, vous devez télécharger les fichiers des applications à partir de Citrix, les wrapper avec le MDX Toolkit, les charger sur la console XenMobile, modifier les stratégies MDX en fonction de vos besoins, et mettre à disposition les applications sur les appareils des utilisateurs à l'aide de groupes de mise à disposition. Pour de plus amples informations, consultez la section Mise à disposition d'applications XenMobile via un magasin d'applications public dans la documentation des applications XenMobile.

Citrix fournit le MDX Toolkit qui wrappe les applications pour iOS, Mac OS X, Android et Windows avec une logique et des stratégies Citrix. L'outil peut wrapper une application qui a été créée au sein de votre organisation ou une application créée par des tiers de manière sécurisée.

Fonctionnement des applications Web et SaaS

XenMobile est fourni avec un ensemble de connecteurs d'applications constituant des modèles qu'il est possible de configurer en vue de l'authentification unique (SSO) pour des applications Web et Software as a Service (SaaS) et, dans certains cas, pour la création et la gestion de comptes d'utilisateur. XenMobile inclut des connecteurs SAML (Security Assertion Markup Language). Les connecteurs SAML sont prévus pour les applications Web qui prennent en charge le protocole SAML en vue de l'authentification unique et de la gestion des comptes d'utilisateur. XenMobile prend en charge les protocoles SAML 1.1 et SAML 2.0.

Vous pouvez également construire vos propres connecteurs SAML d'entreprise.

Pour de plus amples informations, consultez la section Ajouter une application Web ou SaaS dans cet article.

Fonctionnement des applications d'entreprise

Les applications d'entreprise résident généralement dans votre réseau interne. Les utilisateurs peuvent se connecter aux applications à l'aide de Secure Hub. Lorsque vous ajoutez une application d'entreprise, XenMobile crée le connecteur d'application pour cette dernière. Pour de plus amples informations, consultez la section Ajouter une application d'entreprise dans cet article.

Fonctionnement du magasin d'applications public

Vous pouvez configurer des paramètres afin de récupérer les noms et descriptions des applications depuis l'App Store d'Apple, Google Play et Windows Store. Lorsque vous récupérez les informations d'application dans le magasin, XenMobile remplace le nom et la description existants. Pour de plus amples informations, consultez la section Ajouter l'application d'un magasin d'applications public dans cet article.

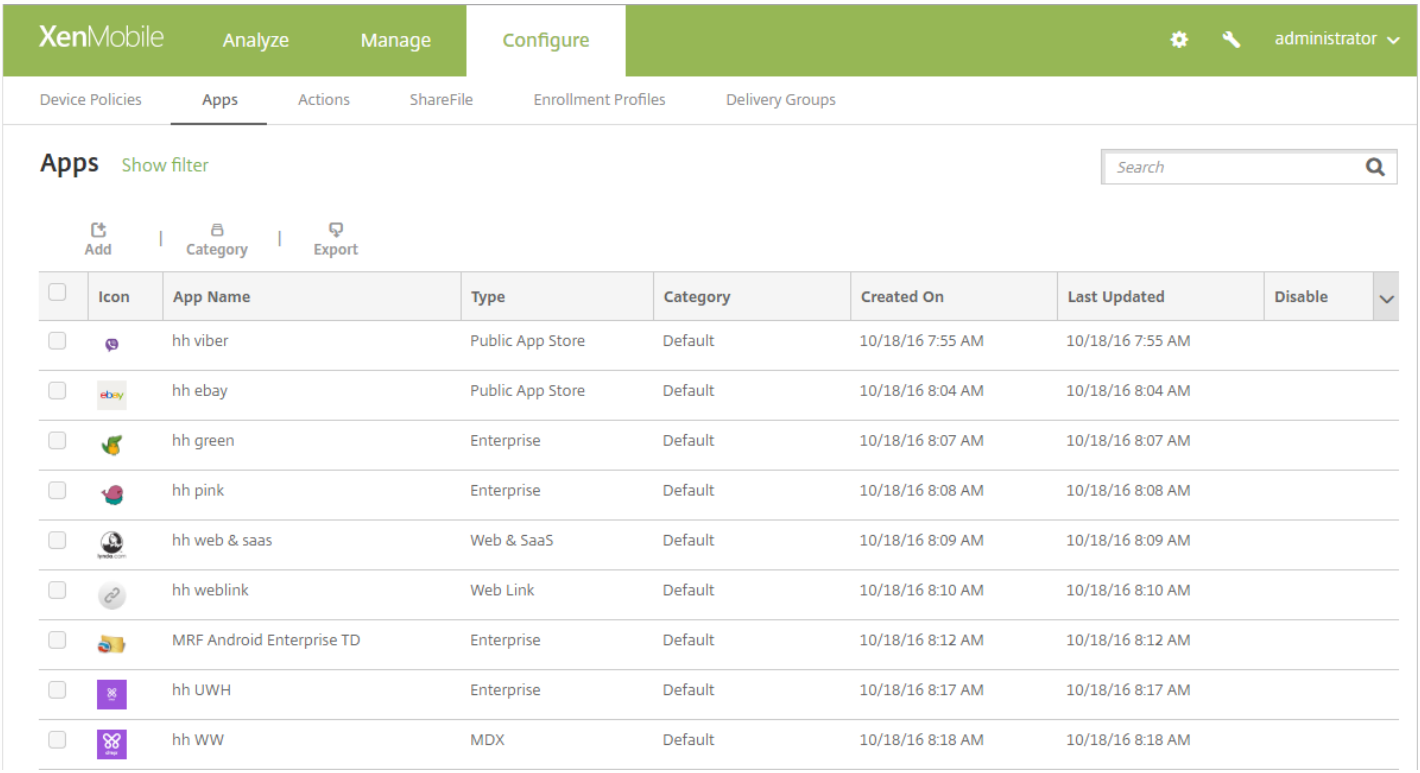
Fonctionnement des liens Web

Un lien Web est une adresse Web permettant d'accéder à un site Internet ou intranet. Un lien Web permet également d'accéder à une application Web qui ne requiert pas d'authentification unique (SSO). Une fois que vous avez terminé de configurer un lien Web, celui-ci s'affiche sous forme d'icône dans le XenMobile Store. Lorsque les utilisateurs ouvrent une session avec Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles. Pour de plus amples informations, consultez la section Ajouter un lien Web applicatif dans cet article.

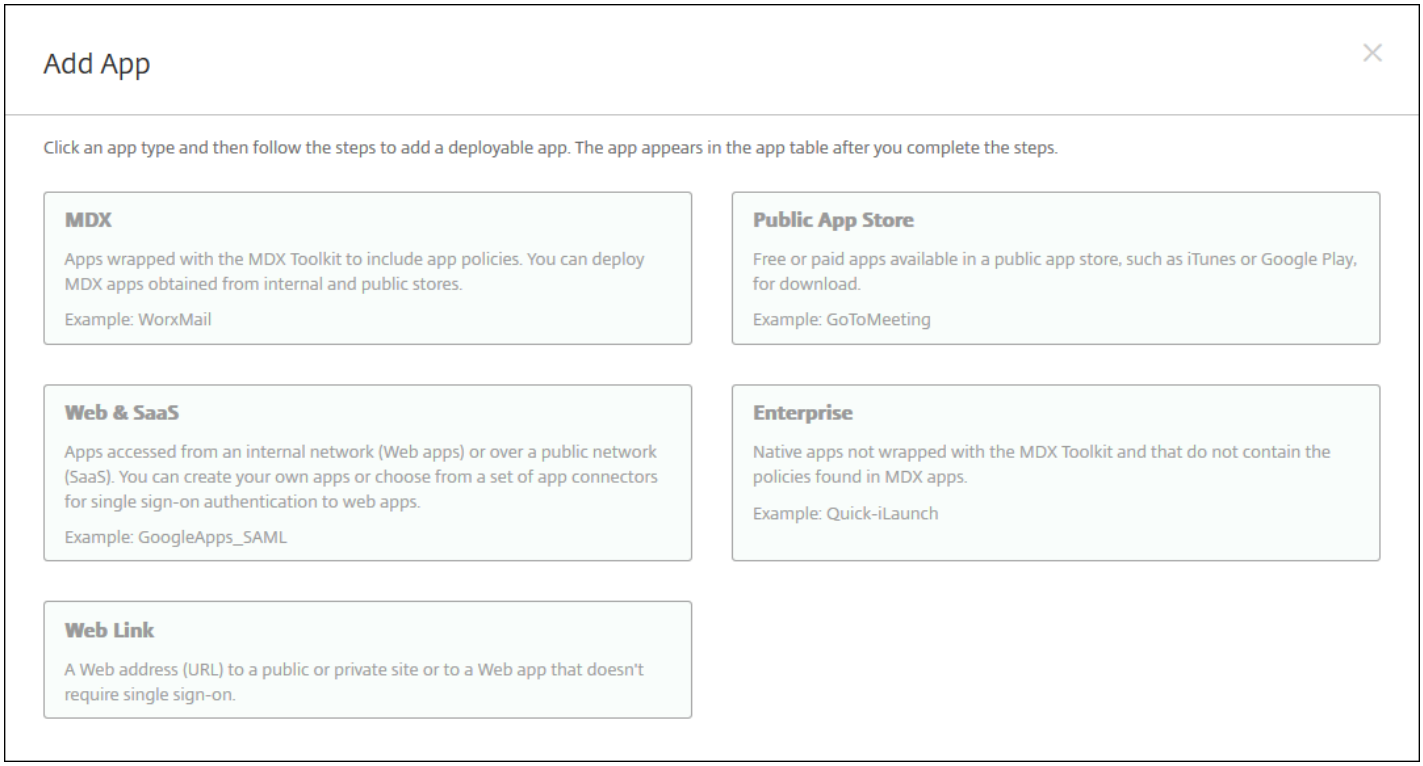
Ajouter une application MDX

Lorsque vous recevez une application mobile MDX wrappée pour iOS, Android, ou Windows Phone, vous pouvez charger l'application sur XenMobile. Après le chargement de l'application, vous pouvez configurer les détails de l'application et les paramètres de stratégie. Pour plus d'informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez la section Synopsis des stratégies MDX. Des descriptions détaillées des stratégies sont également proposées dans cette section.

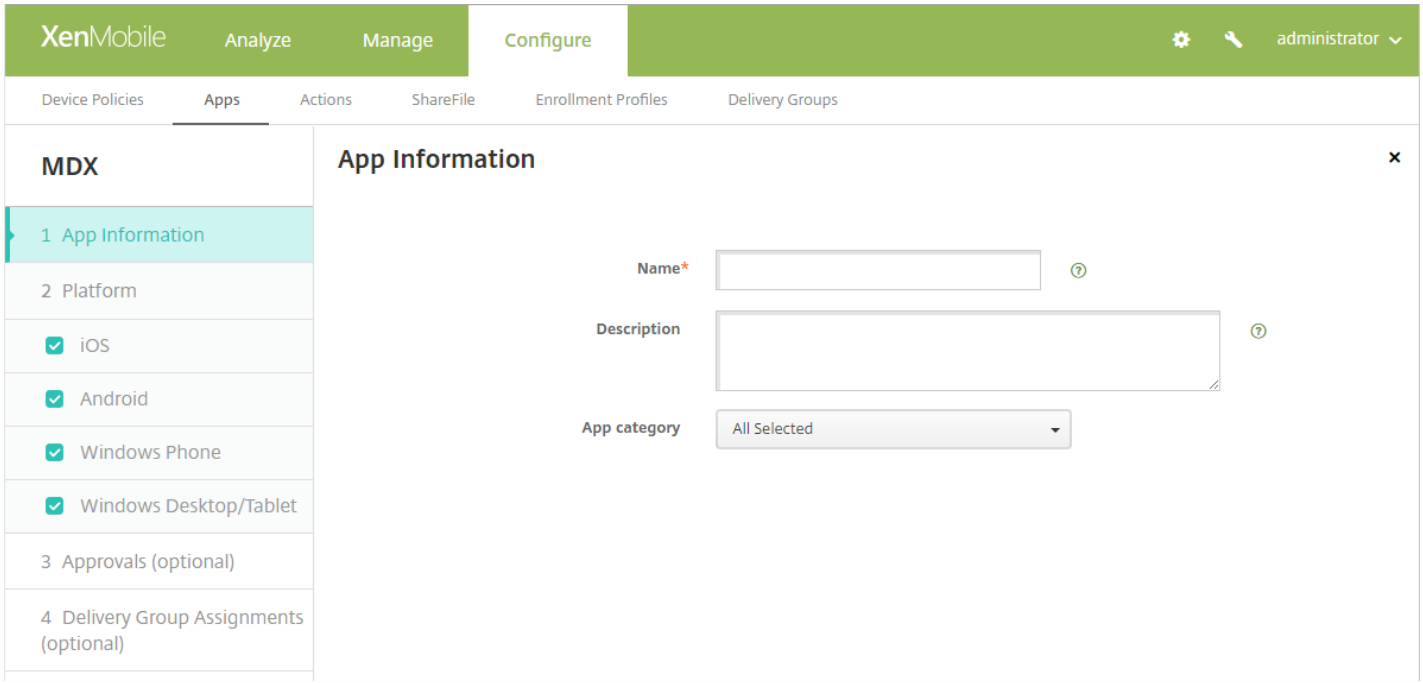
1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'affiche.



2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **MDX**. La page **Informations sur l'application** s'affiche.



4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour l'application. Il apparaît sous **Nom de l'application** dans le tableau **Applications**.
- **Description** : entrez une description pour l'application (facultatif).
- **Catégorie d'application** : si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section Créer des

catégories d'applications.

5. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 11 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Sélectionnez un fichier .mdx à charger en cliquant sur le bouton **Charger** et en accédant à l'emplacement du fichier.

- Si vous ajoutez une application VPP B2B iOS, cliquez sur **Votre application est-elle une application VPP B2B ?** et, dans la liste, cliquez sur le compte VPP B2B à utiliser.

8. Cliquez sur **Suivant**. La page sur les détails de l'application s'affiche.

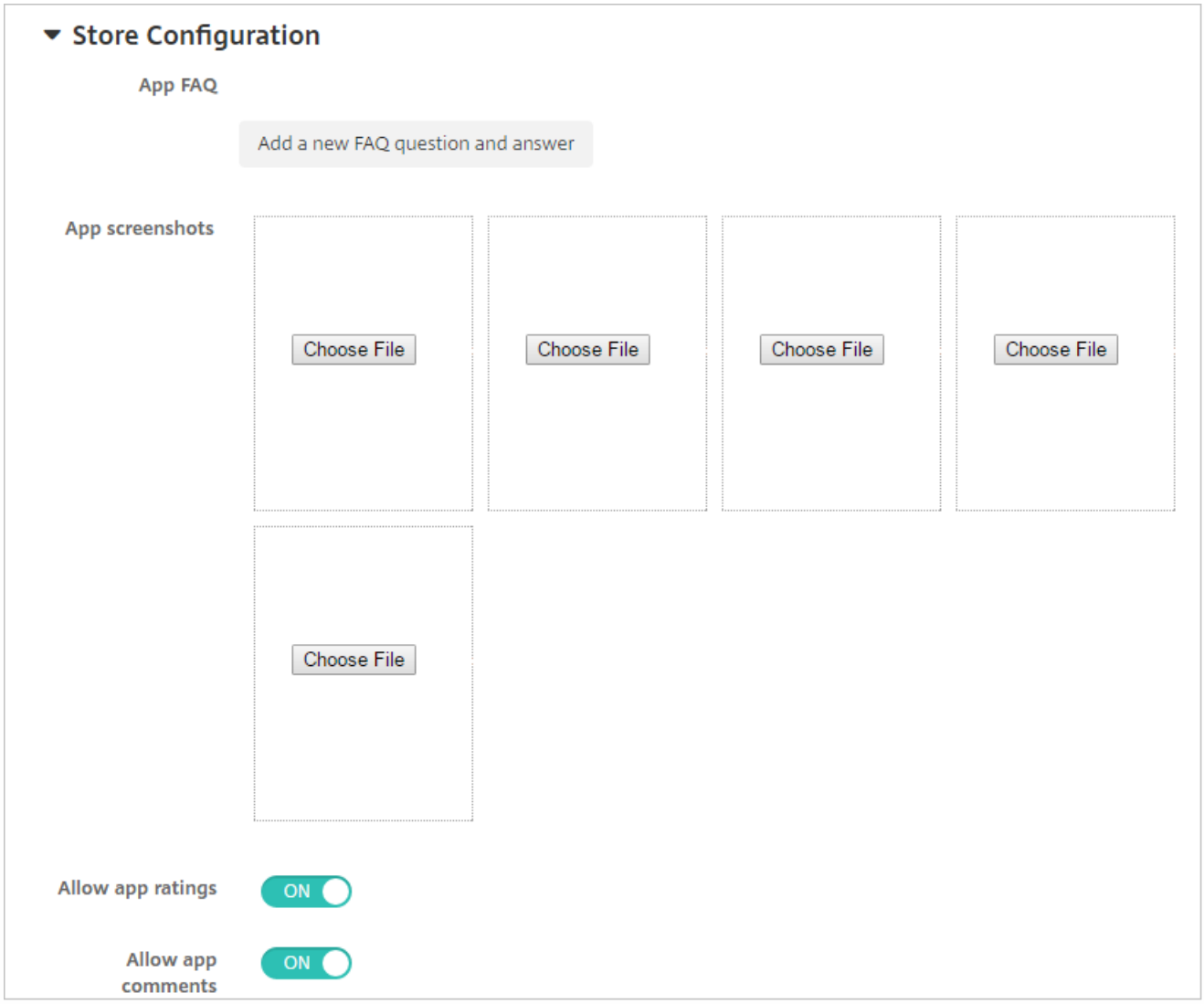
9. Configurez les paramètres suivants :

- **Nom du fichier** : entrez le nom du fichier associé à l'application.
- **Description de l'application** : entrez une description pour l'application.
- **Version de l'application** : si vous le souhaitez, entrez le numéro de version de l'application.
- **Version d'OS minimum** : si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
- **Version d'OS maximum** : si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus** : si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
- **Supprimer l'application si le profil MDM est supprimé** : sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est **ON**.
- **Empêcher la sauvegarde des données d'application** : sélectionnez cette option si vous souhaitez empêcher les utilisateurs de sauvegarder les données de l'application. La valeur par défaut est **ON**.
- **Forcer l'application à être gérée** : sélectionnez cette option pour spécifier si, lors de l'installation d'une application non gérée, vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **ON**. Disponible dans iOS 9.0 et version ultérieure.

10. Configurez les **stratégies MDX**. Les stratégies MDX varient selon la plate-forme et incluent des options dans des domaines de stratégie tels que l'authentification, la sécurité de l'appareil, la configuration réseau requise, l'accès divers, le cryptage, l'interaction de l'application, les restrictions applicatives, l'accès au réseau d'entreprise, les journaux d'applications et le géofencing. Dans la console, les stratégies ont une info-bulle qui décrit chacune d'entre elles. Pour de plus amples informations sur les stratégies applicatives pour les applications MDX, telles qu'un tableau répertoriant les stratégies s'appliquant à chaque type de plate-forme, consultez la section Synopsis des stratégies MDX.

11. Configurez les règles de déploiement.

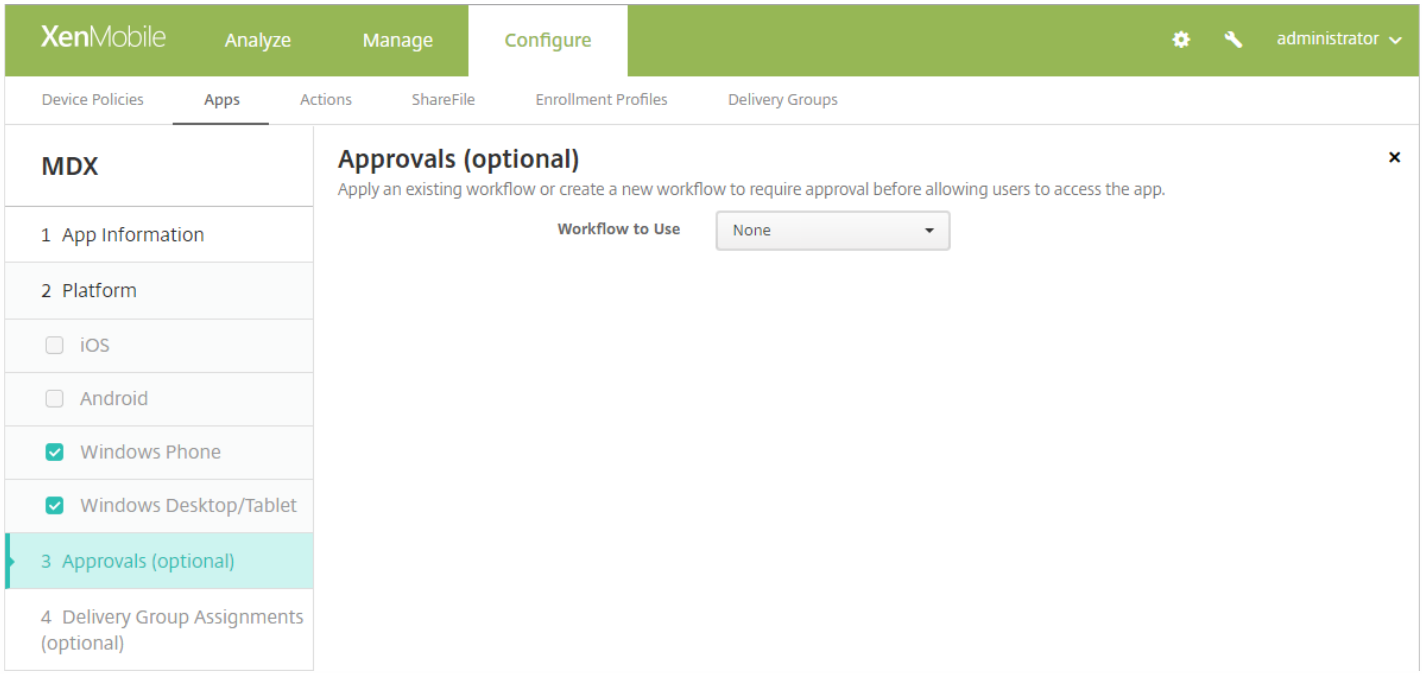
12. Développez **XenMobile Store Configuration**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

13. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 15.

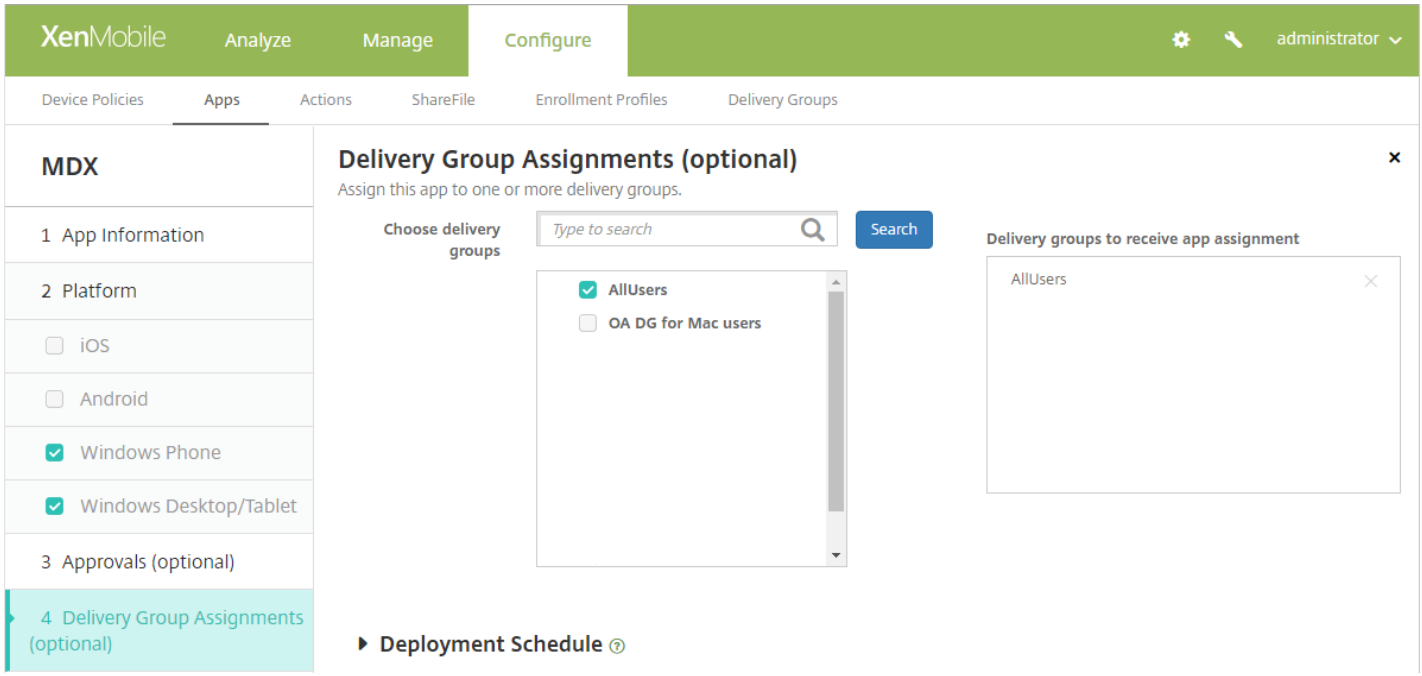
Configurez ce paramètre si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucune**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants :
  - **Nom** : entrez un nom unique pour le workflow.
  - **Description** : entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
    - Pas nécessaire
    - 1 niveau
    - 2 niveaux
    - 3 niveaux
  - **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
  - Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
    - Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
      - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
      - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats

de la recherche.

- Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

14. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

16. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de Calendrier de déploiement, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

17. Cliquez sur **Enregistrer**.

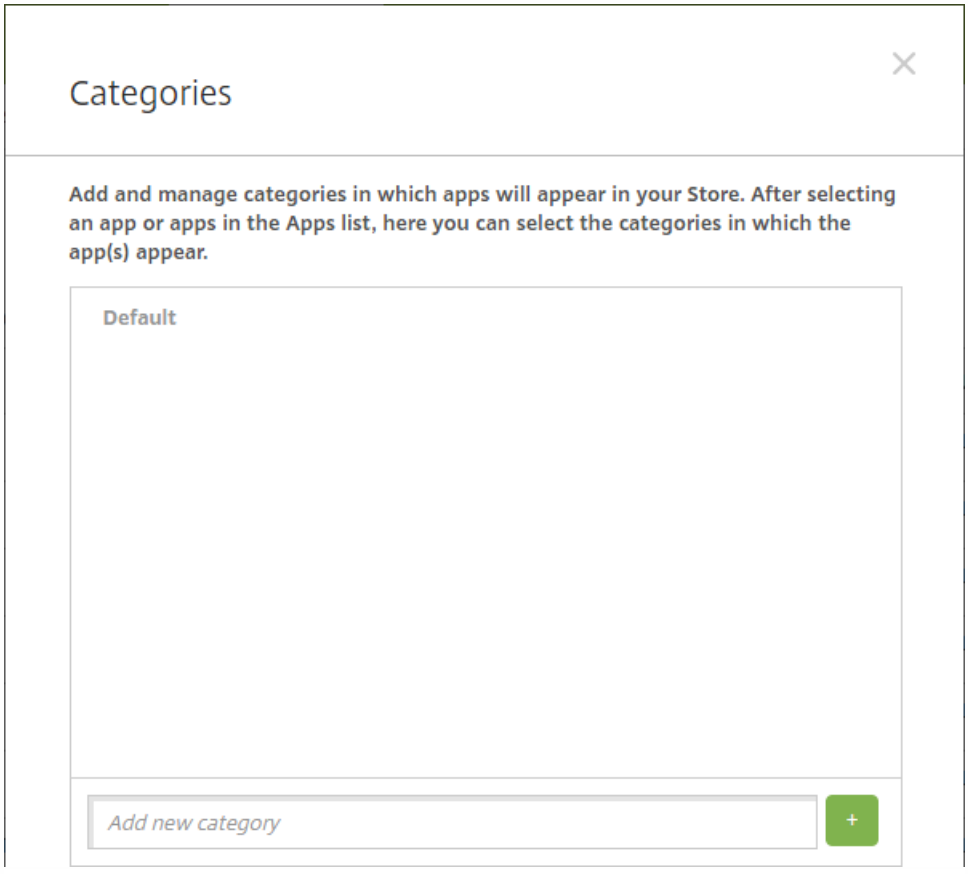
Créer des catégories d'applications

Lorsque les utilisateurs se connectent à Secure Hub, ils obtiennent une liste des applications, des liens Web et des magasins que vous avez ajoutés et configurés dans XenMobile. Vous pouvez utiliser les catégories d'applications pour permettre aux utilisateurs d'accéder uniquement aux applications, liens Web ou magasins auxquels vous souhaitez autoriser l'accès. Par exemple, il est possible de créer une catégorie Finance et d'y ajouter des applications ayant trait uniquement au secteur de la finance. Ou vous pouvez configurer une catégorie Ventes à laquelle vous attribuez des applications de ventes.

Vous configurez les catégories sur la page **Applications** dans la console XenMobile. Ensuite, lorsque vous ajoutez ou modifiez une application, un lien Web ou un magasin, vous pouvez ajouter l'application à l'une ou plusieurs des catégories que vous avez configurées.

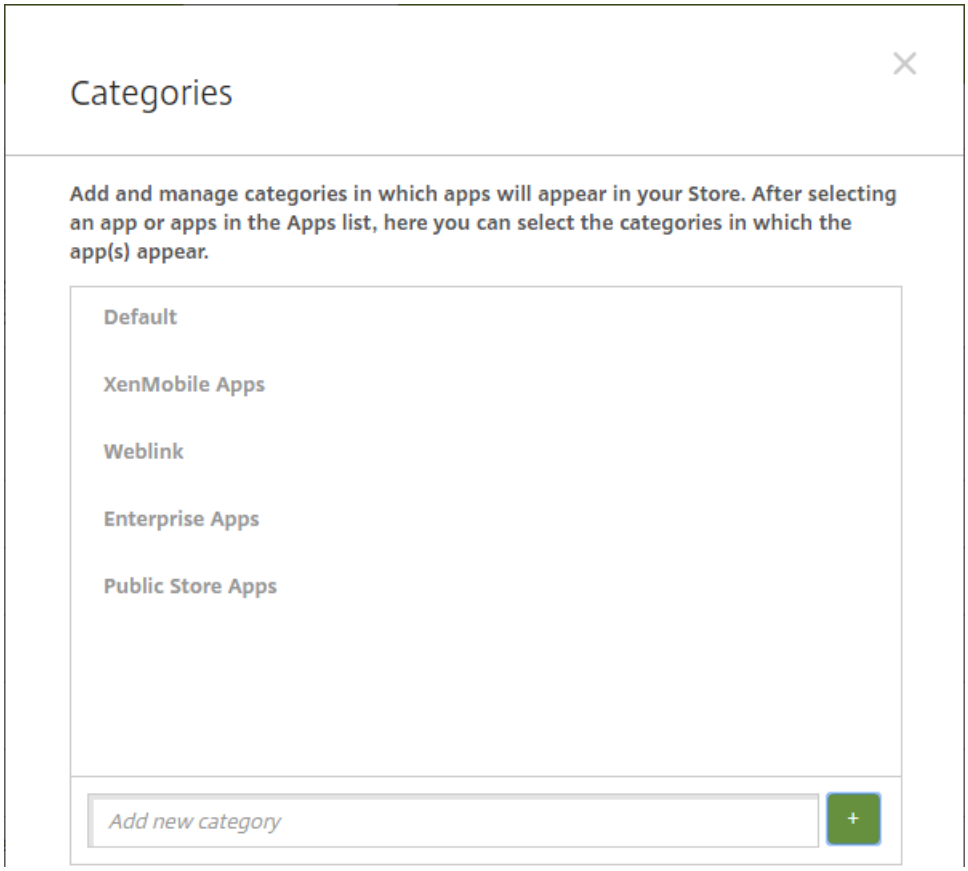
1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'affiche.

2. Cliquez sur **Catégorie**. La boîte de dialogue **Catégories** s'affiche.



3. Pour chaque catégorie que vous voulez ajouter, procédez comme suit :

- Tapez le nom de la catégorie que vous souhaitez ajouter dans le champ **Ajouter une nouvelle catégorie** en bas de la boîte de dialogue. Par exemple, vous pouvez entrer Applications d'entreprise pour créer une catégorie pour les applications d'entreprise.
- Cliquez sur le signe plus (+) pour ajouter la catégorie. La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue **Catégories**.



4. Lorsque vous avez terminé d'ajouter des catégories, fermez la boîte de dialogue **Catégories**.

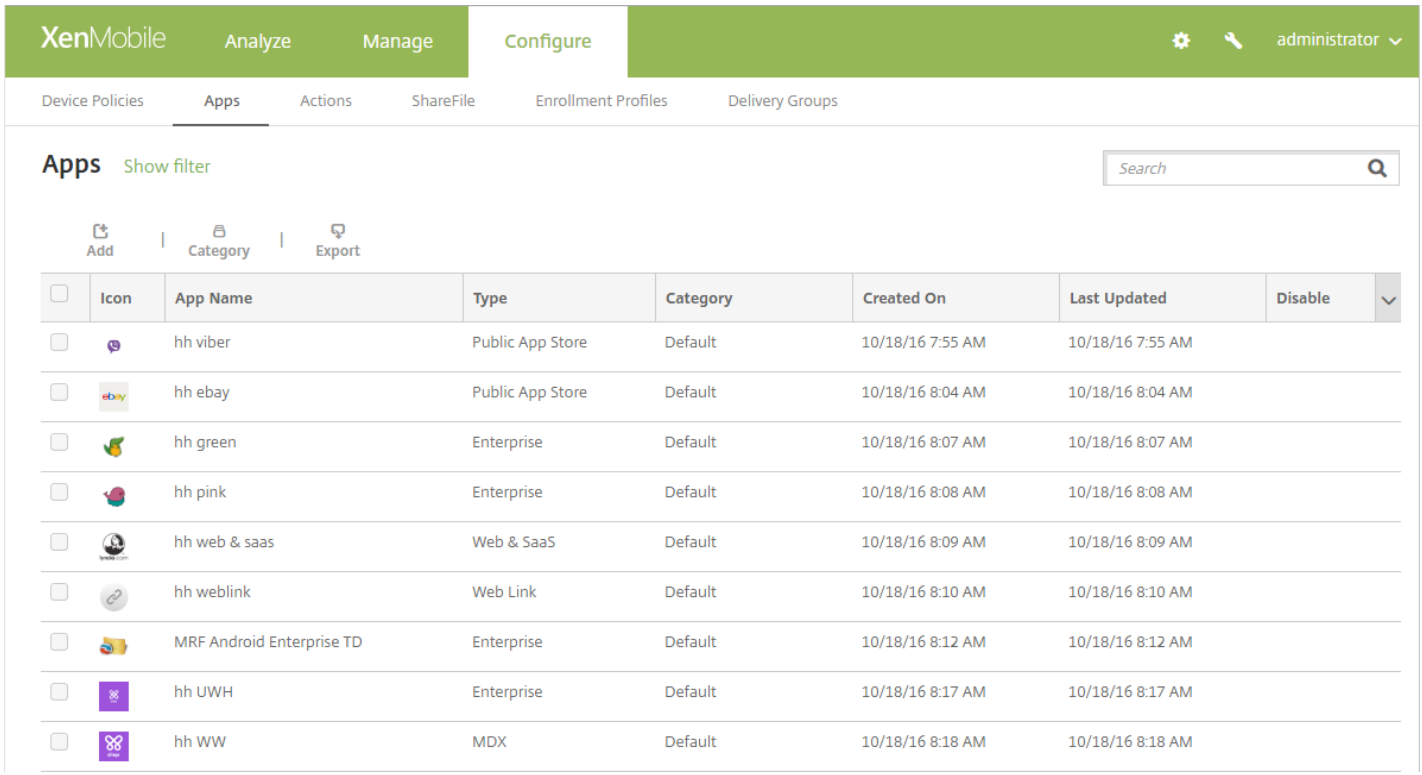
5. Sur la page **Applications**, vous pouvez placer une application existante dans une nouvelle catégorie.

- Sélectionnez l'application que vous souhaitez classer.
- Cliquez sur **Modifier**. La page **Informations sur l'application** s'affiche.
- Dans la liste **Catégorie d'application**, appliquez la nouvelle catégorie en sélectionnant la case à cocher appropriée. Désélectionnez les cases à cocher pour les catégories que vous ne souhaitez pas appliquer à l'application.
- Cliquez sur l'onglet **Attribution de groupes de mise à disposition** ou cliquez sur **Suivant** sur chacune des pages suivantes pour compléter les autres pages de configuration de l'application.
- Cliquez sur **Enregistrer** sur la page **Attribution de groupes de mise à disposition** pour appliquer la catégorie. La nouvelle catégorie est appliquée à l'application et l'application s'affiche dans le tableau **Applications**.

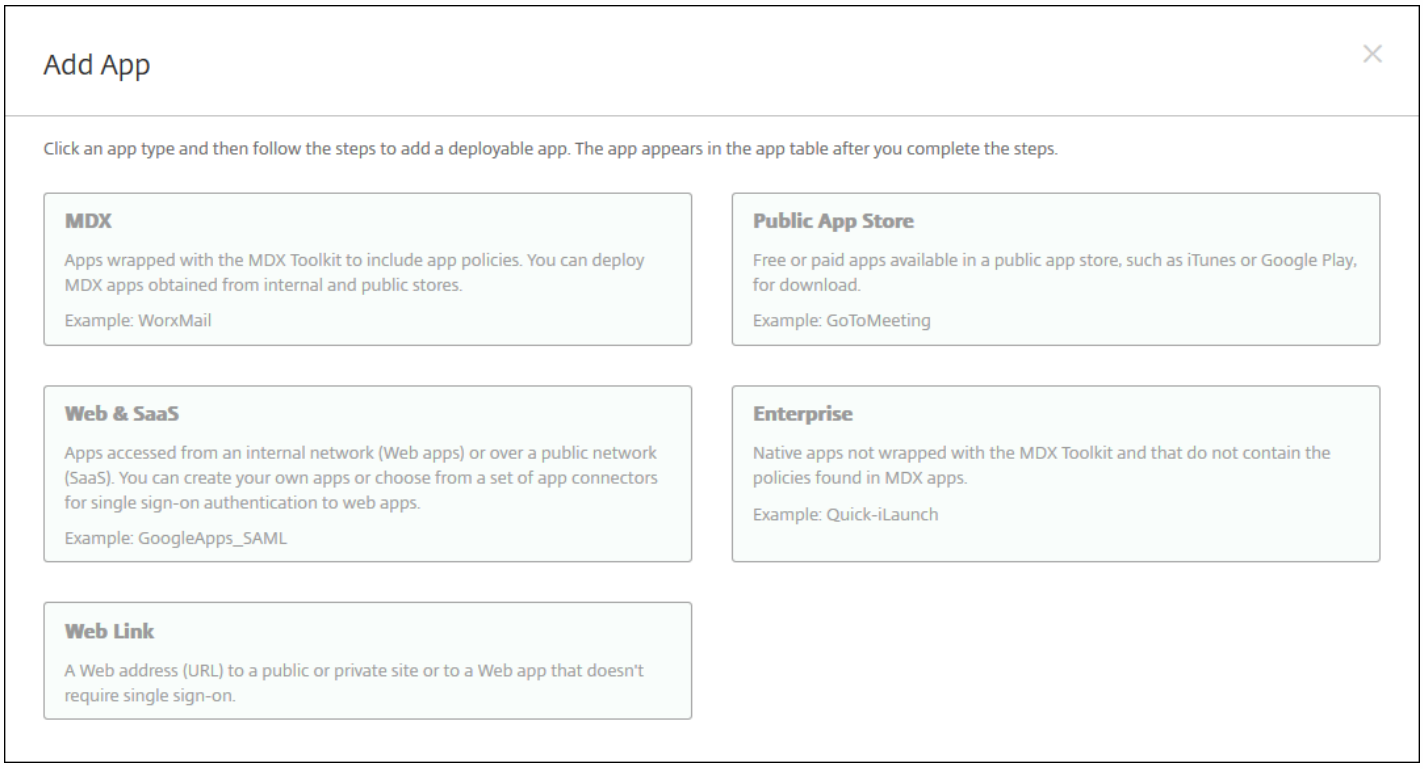
Ajouter une application d'un magasin d'applications public

Vous pouvez ajouter des applications gratuites ou payantes à XenMobile qui sont disponibles dans un magasin d'applications public, tel que iTunes où Google Play. Par exemple : GoToMeeting. Également, lorsque vous ajoutez une application payante provenant d'un magasin d'applications public pour un Android for Work, vous pouvez vérifier l'état de la licence d'achat groupé : le nombre total de licences disponibles, ainsi que l'adresse e-mail de chaque utilisateur qui consomme les licences. Le plan Achat groupé pour Android for Work simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation.

1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'affiche.



2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Magasin d'applications public**. La page **Informations sur l'application** s'affiche.

4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

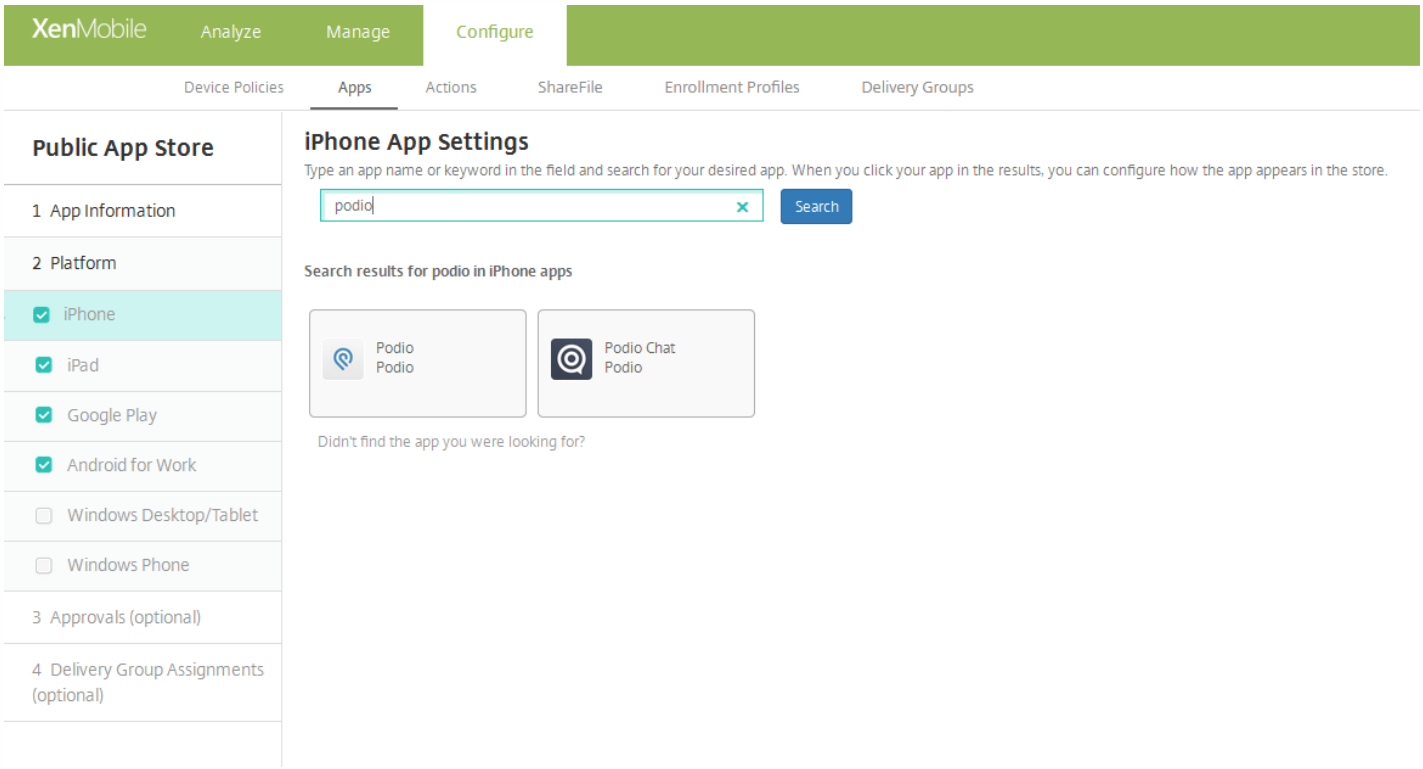
- **Nom** : entrez un nom descriptif pour l'application. Il apparaît sous **Nom de l'application** dans le tableau **Applications**.
- **Description** : entrez une description pour l'application (facultatif).
- **Catégorie d'application** : si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section Créer des catégories d'applications.

5. Cliquez sur **Suivant**. La page **Plates-formes d'applications** s'affiche.

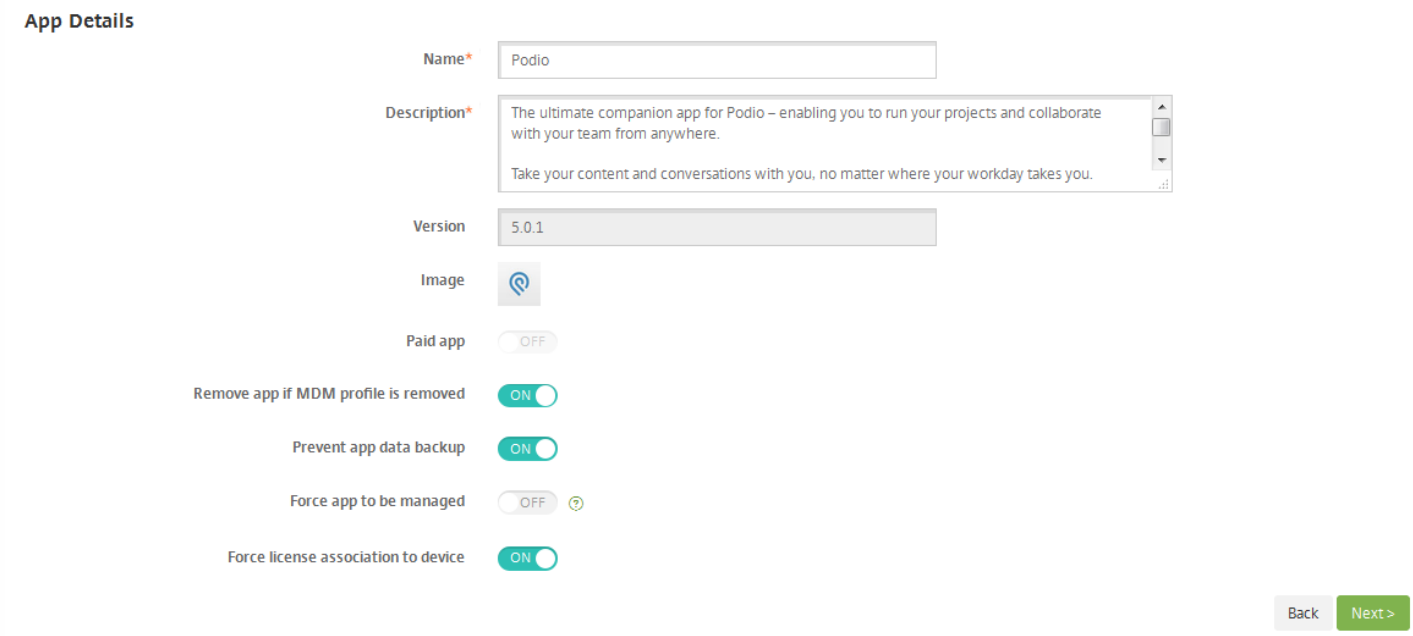
6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 10 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Sélectionnez une application à ajouter en tapant le nom de l'application dans la zone de recherche et en cliquant sur **Rechercher**. Les applications correspondant aux critères de recherche s'affichent. La figure suivante illustre le résultat de la recherche pour « podio ».



8. Cliquez sur chaque application que vous souhaitez ajouter. Les champs **Détails sur l'application** sont pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image).

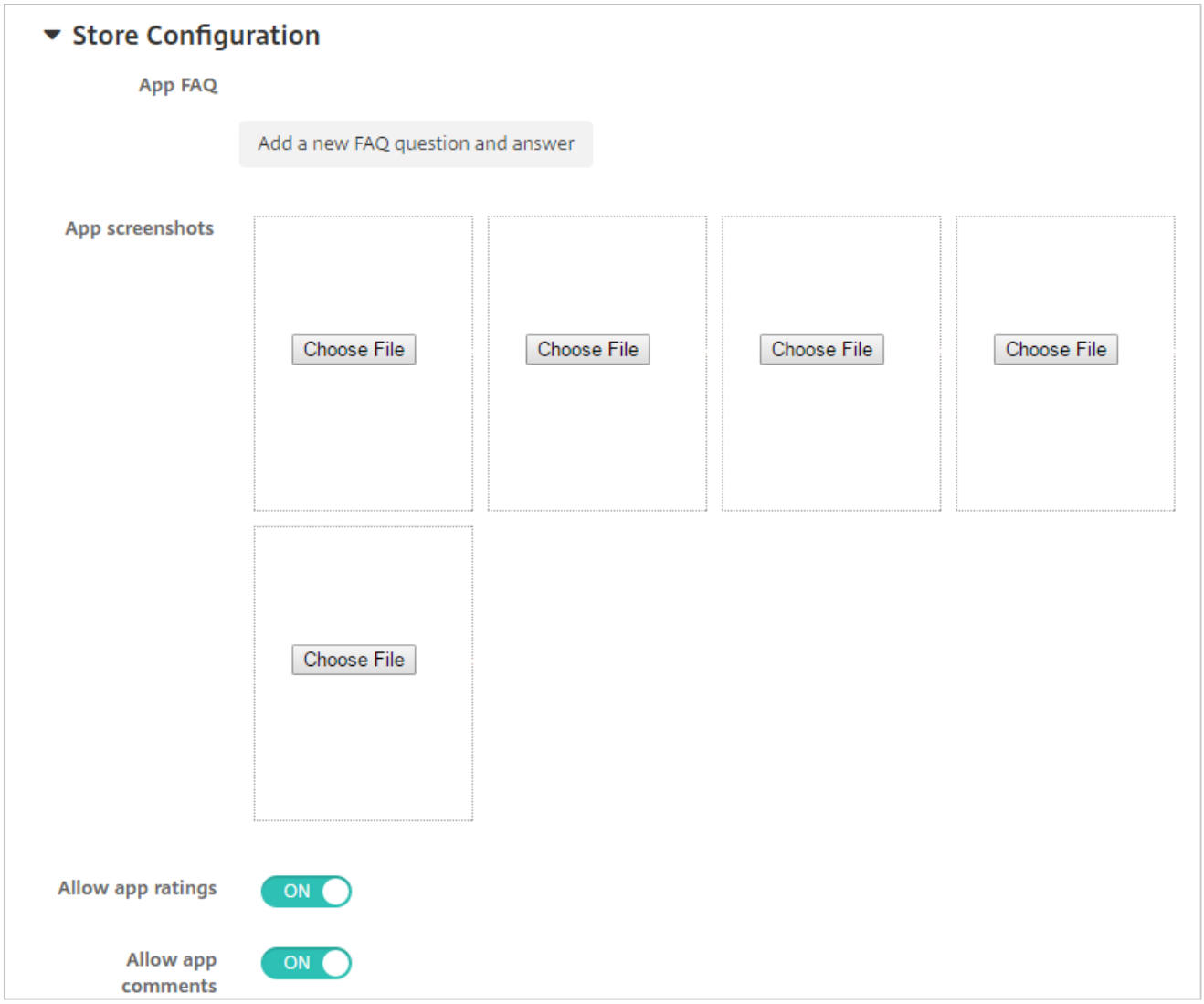


9. Configurez les paramètres suivants :

- Si nécessaire, modifiez le nom et la description de l'application.
- **Application payante** : ce champ est préconfiguré et ne peut pas être modifié.
- **Supprimer l'application si le profil MDM est supprimé** : sélectionnez cette option si vous souhaitez supprimer l'application lorsque le profil MDM est supprimé. La valeur par défaut est **ON**.
- **Empêcher la sauvegarde des données d'application** : sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **ON**.
- **Forcer l'application à être gérée** : sélectionnez cette option pour spécifier si, lors de l'installation d'une application non gérée, vous souhaitez inviter les utilisateurs à autoriser l'application à être gérée sur les appareils non supervisés. La valeur par défaut est **OFF**. Disponible dans iOS 9.0 et version ultérieure.
- **Forcer l'association de licence avec l'appareil** : sélectionnez cette option si vous voulez associer une application qui a été développée en association avec un périphérique à un périphérique plutôt qu'à un utilisateur. Disponible sur iOS 9 et version ultérieure. Si l'application que vous avez choisie ne prend pas en charge l'attribution à un appareil, ce champ ne peut pas être modifié.

10. Configurez les règles de déploiement.

11. Développez **XenMobile Store Configuration**.

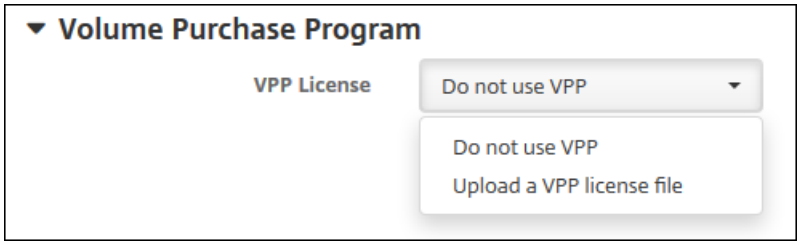


Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est ON.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée.

12. Développez **Programme d'achat en volume** ou dans le cas d'Android for Work, développez **Achat groupé**.

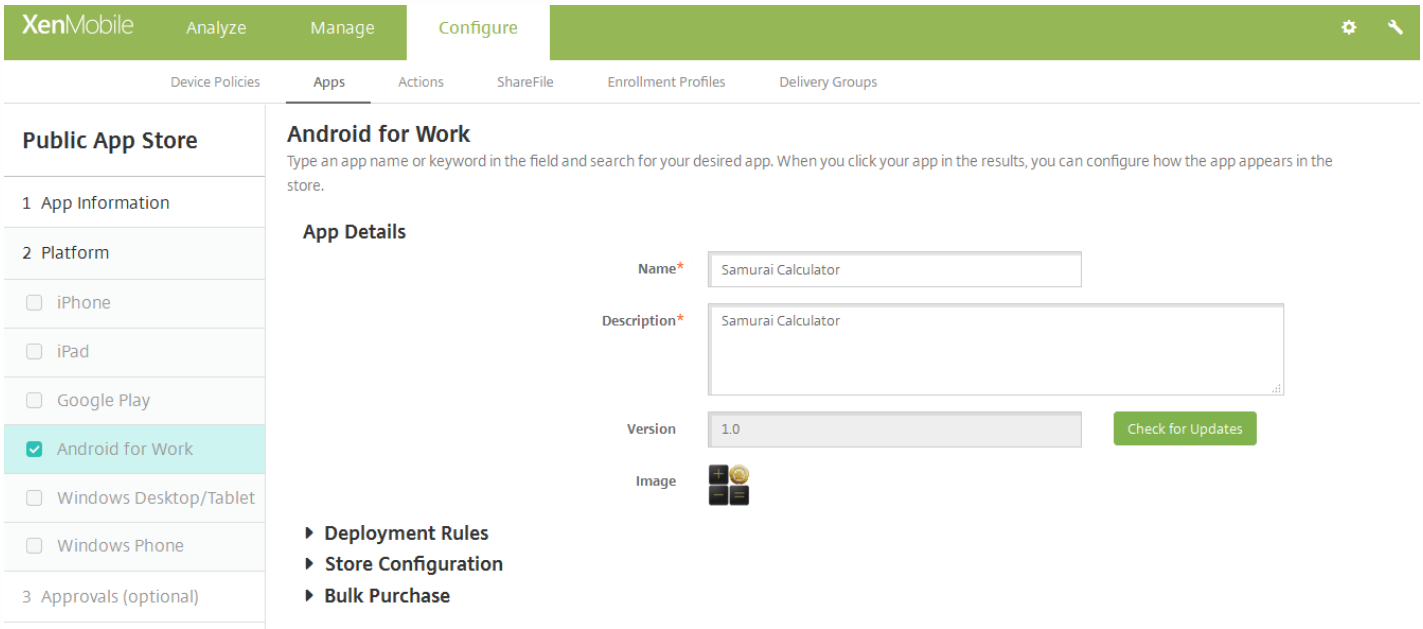
Pour le Programme d'achat en volume, suivez les étapes suivantes.



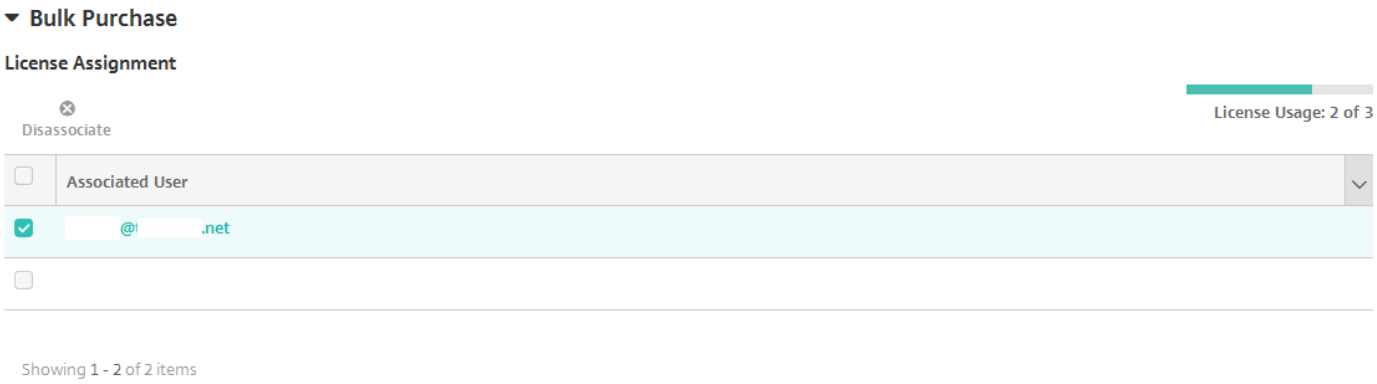
a. 9. Dans la liste **Licences VPP**, cliquez sur **Charger un fichier de licences VPP** si vous voulez autoriser XenMobile à appliquer une licence VPP pour l'application.

b. Dans la boîte de dialogue qui s'affiche, importez la licence.

Pour les achats groupés Android for Work, développez la section **Achat groupé**.



Le tableau Attribution de licences affiche le nombre de licences actuellement en cours d'utilisation pour l'application par rapport au nombre total disponible. Vous pouvez sélectionner un utilisateur et cliquer sur **Dissocier** pour libérer sa licence afin qu'elle puisse profiter à un autre utilisateur. Veuillez toutefois noter que vous ne pouvez dissocier des licences que si l'utilisateur ne fait pas partie d'un groupe de mise à disposition qui contient l'application spécifique.



13. Cliquez sur **Suivant**. La page **Approbations** s'affiche.

Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape suivante.

Configurez ces paramètres si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucune**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants :
  - **Nom** : entrez un nom unique pour le workflow.
  - **Description** : entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
    - Pas nécessaire
    - 1 niveau
    - 2 niveaux
    - 3 niveaux
  - **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
  - Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
    - Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
    - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    - Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

14. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

16. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.

- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

17. Cliquez sur **Enregistrer**.

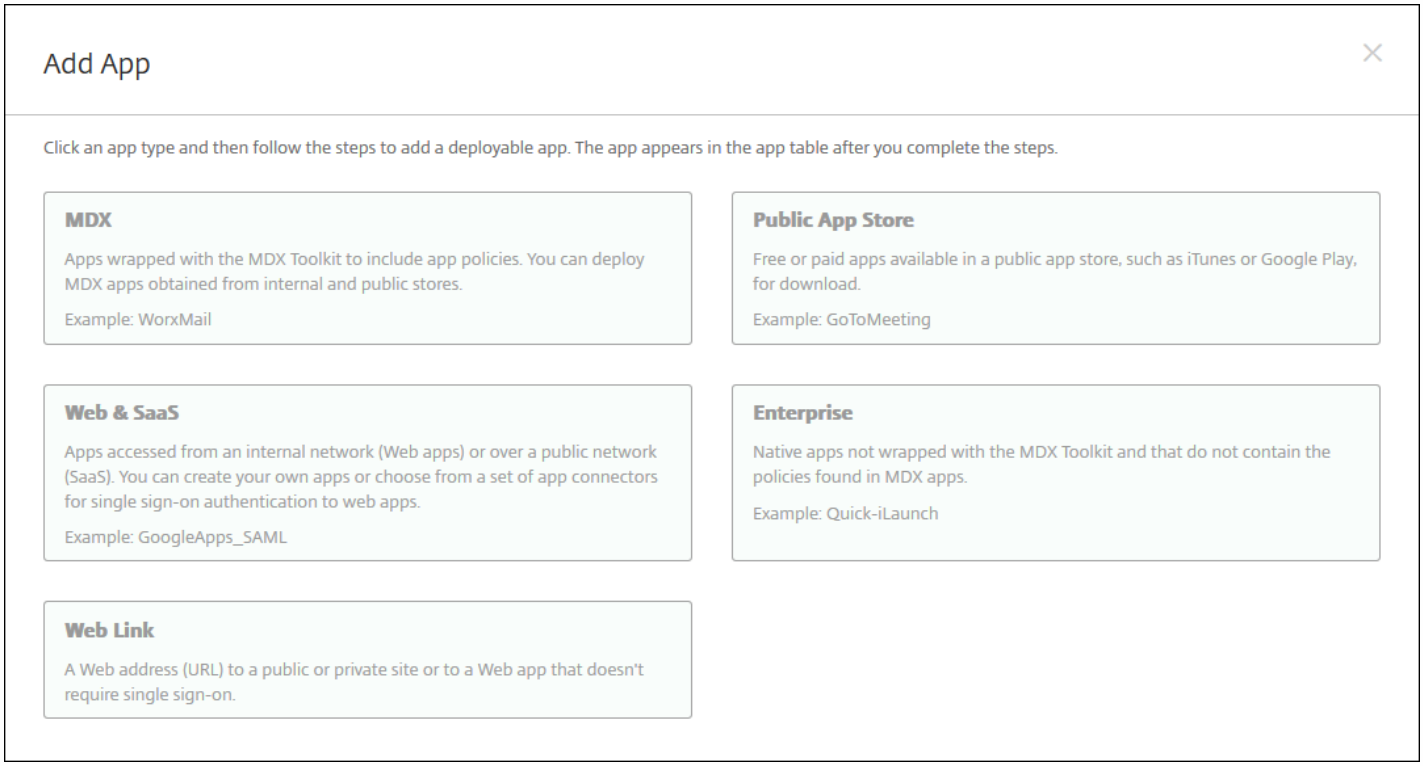
Ajouter une application Web ou SaaS

Grâce à la console XenMobile, vous pouvez fournir aux utilisateurs une autorisation d'authentification unique (SSO) à vos applications mobiles, d'entreprise, Web et SaaS. Vous pouvez activer des applications pour l'authentification unique (SSO) à l'aide des modèles de connecteurs d'applications. Pour obtenir une liste des types de connecteurs disponibles dans XenMobile, consultez la section Types de connecteur d'applications. Vous pouvez également créer votre propre connecteur dans XenMobile lorsque vous ajoutez une application Web ou SaaS.

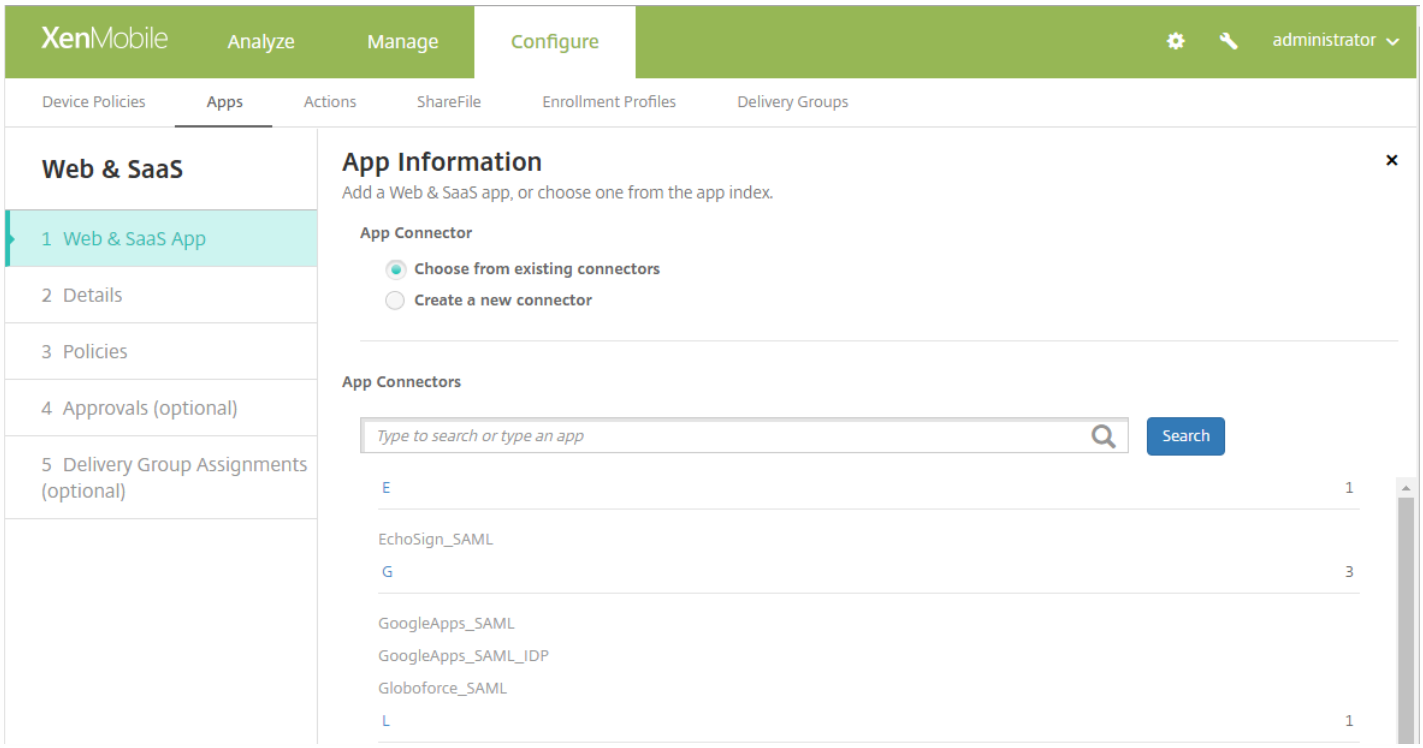
Si une application est uniquement disponible en authentification unique, enregistrez les paramètres lorsque vous terminez la configuration des paramètres précédents ; l'application s'affiche alors dans l'onglet **Applications** de la console XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'ouvre.

2. Cliquez sur **Ajouter**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Web et SaaS**. La page **Informations sur l'application** s'affiche.



4. Configurez un nouveau connecteur d'applications ou un connecteur existant comme suit.

Pour configurer un connecteur d'applications existant

Dans la page **Informations sur l'application**, l'option **Choisir parmi les connecteurs existants** est déjà sélectionnée, comme illustré ci-dessus. Cliquez sur le connecteur que vous souhaitez utiliser dans la liste **Connecteurs d'applications**. Les informations sur le connecteur d'applications s'affichent.

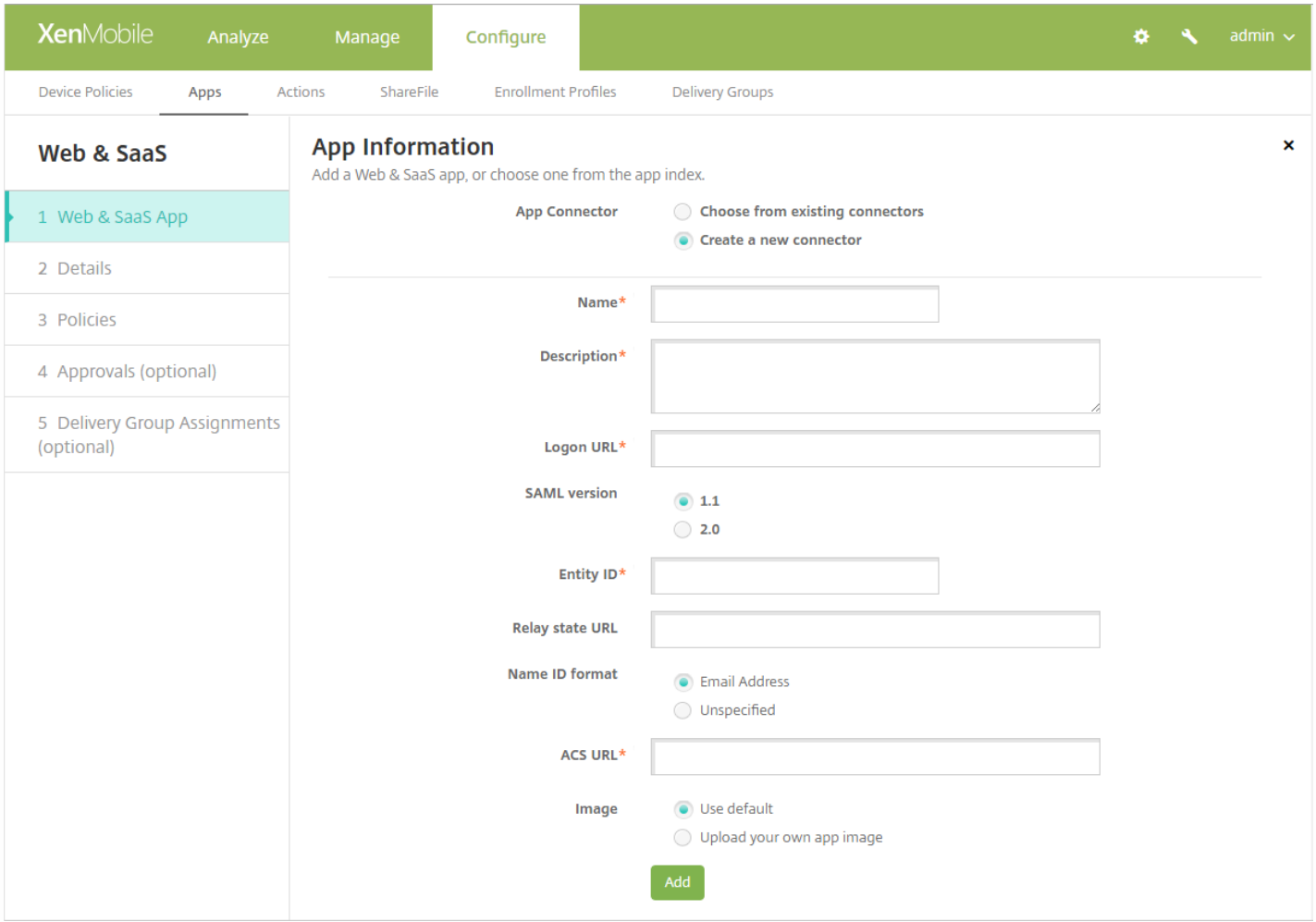
Pour configurer ces paramètres :

- **Nom de l'application** : acceptez le nom attribué ou entrez un nouveau nom.
- **Description de l'application** : acceptez la description existante ou choisissez la vôtre.
- **URL** : acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
- **Nom de domaine** : le cas échéant, entrez le nom de domaine de l'application. Ce champ est obligatoire.
- **L'application est hébergée dans le réseau interne** : indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de NetScaler Gateway. En réglant cette option sur **ON**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **OFF**.
- **Catégorie d'application** : dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
- **Provisioning du compte utilisateur** : sélectionnez cette option si vous souhaitez créer des comptes utilisateur pour l'application. Si vous utilisez le connecteur Globoforce_SAML, vous devez activer cette option pour assurer une intégration SSO transparente.
- Si vous activez **Provisioning du compte utilisateur**, configurez les paramètres suivants :

- **Compte de service**
  - **Nom d'utilisateur** : entrez un nom pour l'administrateur de l'application. Ce champ est obligatoire.
  - **Mot de passe** : tapez le mot de passe d'administrateur de l'application. Ce champ est obligatoire.
- **Compte utilisateur**
  - **Lorsque les droits de l'utilisateur prennent fin** : dans la liste, cliquez sur l'action à effectuer lorsque les utilisateurs ne sont plus autorisés à accéder à l'application. La valeur par défaut est Désactiver le compte. Les options possibles sont les suivantes :
    - Désactiver le compte
    - Conserver le compte
    - Supprimer le compte
- **Règle de nom d'utilisateur**
  - Pour chaque règle de nom d'utilisateur que vous souhaitez ajouter, procédez comme suit :
    - **Attributs utilisateur** : dans la liste, cliquez sur l'attribut utilisateur à ajouter à la règle.
    - **Longueur (caractères)** : dans la liste, cliquez sur le nombre de caractères (de l'attribut utilisateur) à inclure dans la règle de nom d'utilisateur. Le paramètre par défaut est **All**
    - **Règle** : chaque attribut utilisateur que vous ajoutez est automatiquement ajouté à la règle de nom d'utilisateur.
- **Exigences de mot de passe**
  - **Longueur** : entrez la longueur minimale du mot de passe de l'utilisateur. La valeur par défaut est de **8**.
- **Expiration du mot de passe**
  - **Validité (jours)** : tapez le nombre de jours pendant lequel le mot de passe est valable. Les valeurs valides sont **0**-**90**. La valeur par défaut est 90.
  - **Réinitialiser le mot de passe automatiquement après son expiration** : sélectionnez cette option si vous voulez réinitialiser le mot de passe automatiquement lors de l'expiration. La valeur par défaut est **OFF**. Si vous n'activez pas ce champ, les utilisateurs ne peuvent pas ouvrir l'application après que leur mot de passe expire.

Pour configurer un nouveau connecteur d’applications

Dans la page **Informations sur l'application**, sélectionnez **Créer un nouveau connecteur**. Les champs du connecteur d’applications s’affichent.

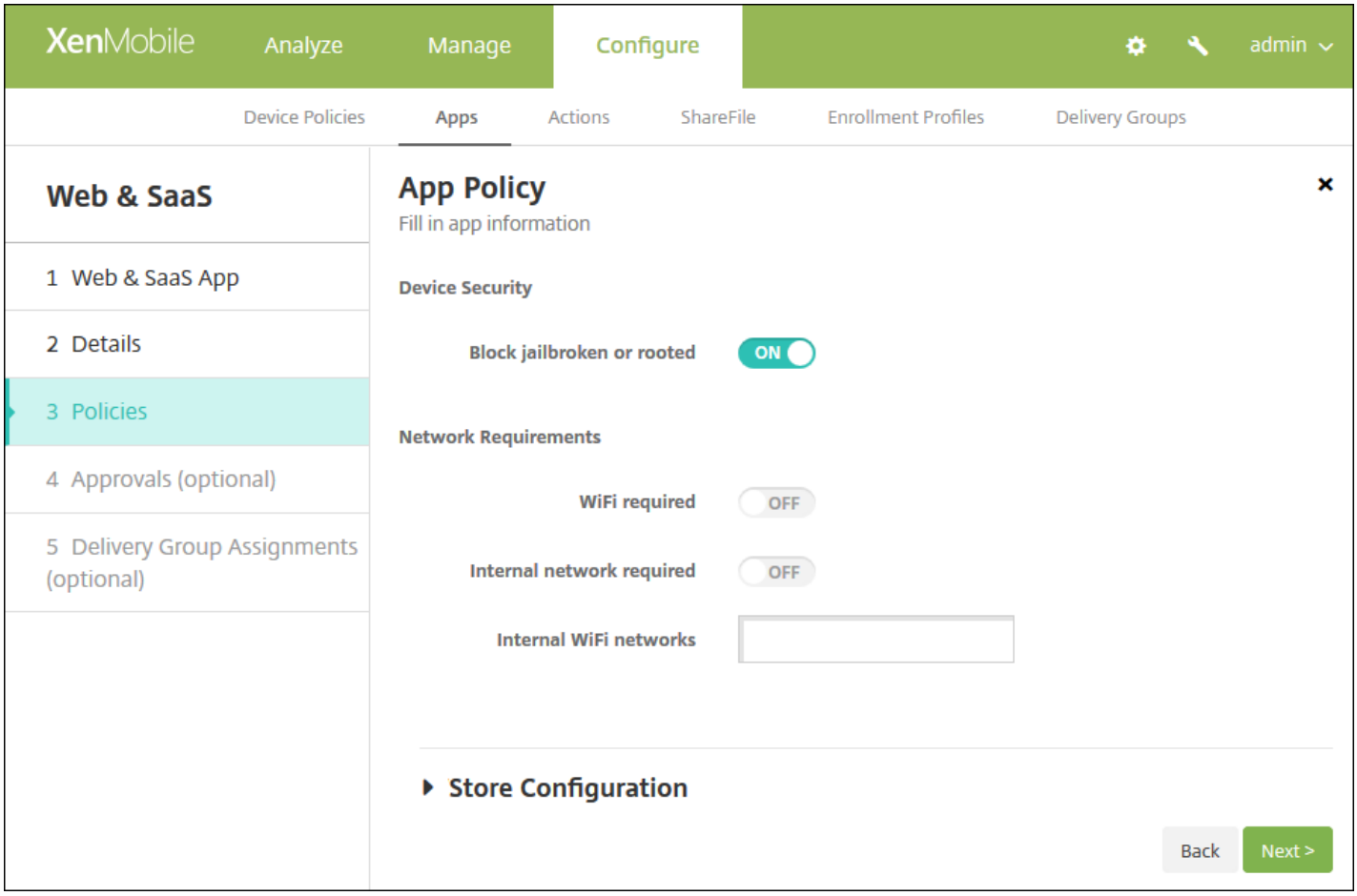


Pour configurer ces paramètres :

- **Nom** : entrez un nom pour le connecteur. Ce champ est obligatoire.
- **Description** : entrez une description pour le connecteur. Ce champ est obligatoire.
- **URL de connexion** : entrez, ou copiez et collez, l'adresse URL de l'emplacement sur lequel les utilisateurs ouvrent une session sur le site. Par exemple, si l'application que vous souhaitez ajouter possède une page d'ouverture de session, ouvrez un navigateur Web et accédez à la page d'ouverture de session de l'application. Par exemple, http://www.exemple.com/logon. Ce champ est obligatoire.
- **Version SAML** : sélectionnez **1.1** ou **2.0**. La valeur par défaut est de **1,1**.
- **ID de l'entité** : entrez l'identité de l'application SAML.
- **URL d'état du relais** : entrez l'adresse Web de l'application SAML. L'URL d'état du relais représente l'URL de réponse de l'application.
- **Format de l'ID de nom** : sélectionnez **Adresse e-mail** ou **Non spécifié**. Le paramètre par défaut est **Email Address**.
- **URL ACS** : entrez l'URL du service ACS (consommateur d'assertion) du fournisseur de services ou d'identités. L'URL ACS offre aux utilisateurs une fonctionnalité d'authentification unique (SSO).
- **Image** : indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.
  - Si vous souhaitez télécharger votre propre image, sélectionnez-la en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Le fichier doit être un fichier .PNG ; vous ne pouvez pas charger une image GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

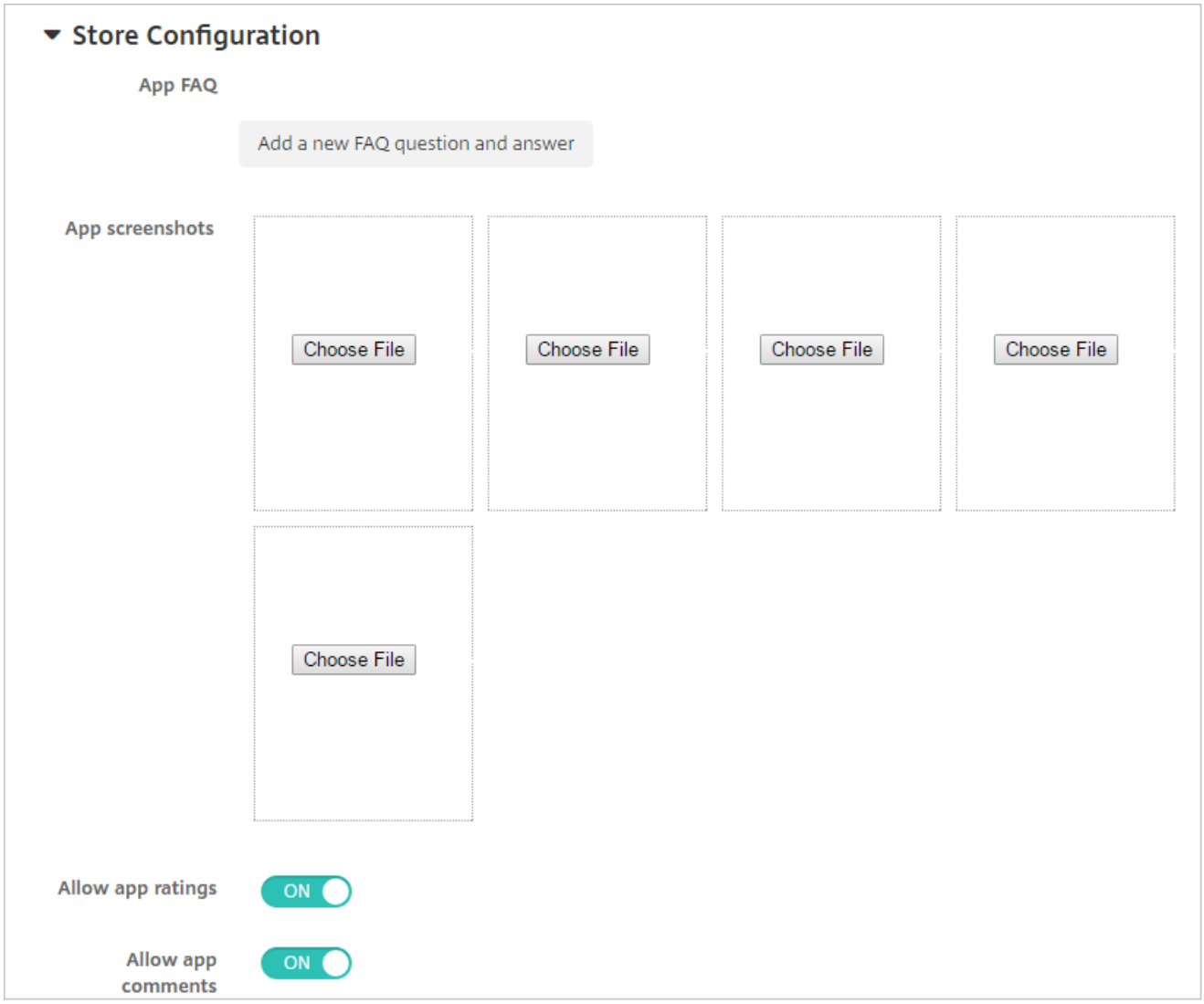
- Lorsque vous avez terminé, cliquez sur **Ajouter**. La page **Détails** s'affiche.

5. Cliquez sur **Suivant**. La page **Stratégie d'application** s'affiche.



- Pour configurer ces paramètres :
  - **Sécurité de l'appareil**
    - **Bloquer les appareils jailbreakés ou rootés** : sélectionnez cette option pour empêcher les appareils jailbreakés ou rootés d'accéder à l'application. La valeur par défaut est **ON**.
  - **Configuration réseau requise**
    - **Wi-Fi requis** : sélectionnez cette option pour spécifier qu'une connexion WiFi est requise pour exécuter l'application. La valeur par défaut est **OFF**.
    - **Réseau interne requis** : sélectionnez cette option si un réseau interne est requis pour exécuter l'application. La valeur par défaut est **OFF**.
    - **Réseaux Wi-Fi internes**: si vous avez activé « Wi-Fi requis », saisissez les réseaux Wi-Fi internes à utiliser.

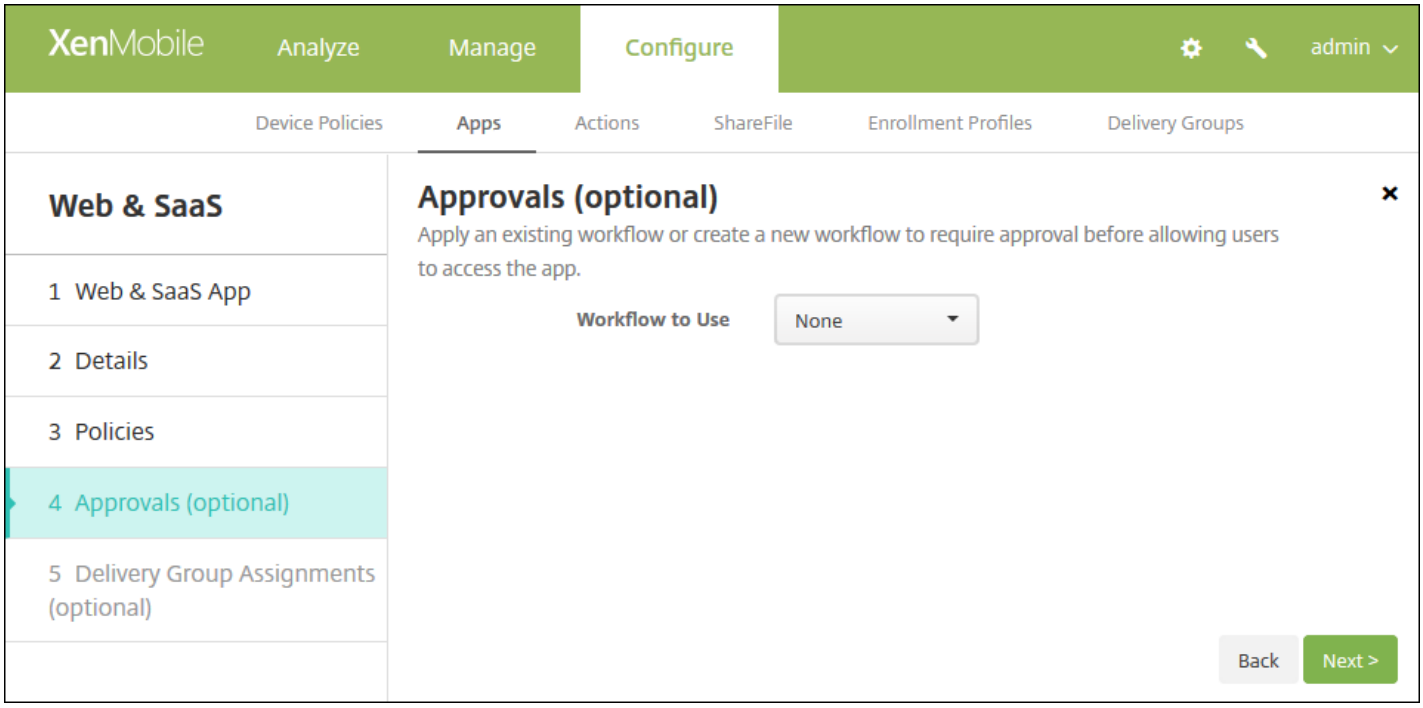
6. Développez **XenMobile Store Configuration**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

7. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



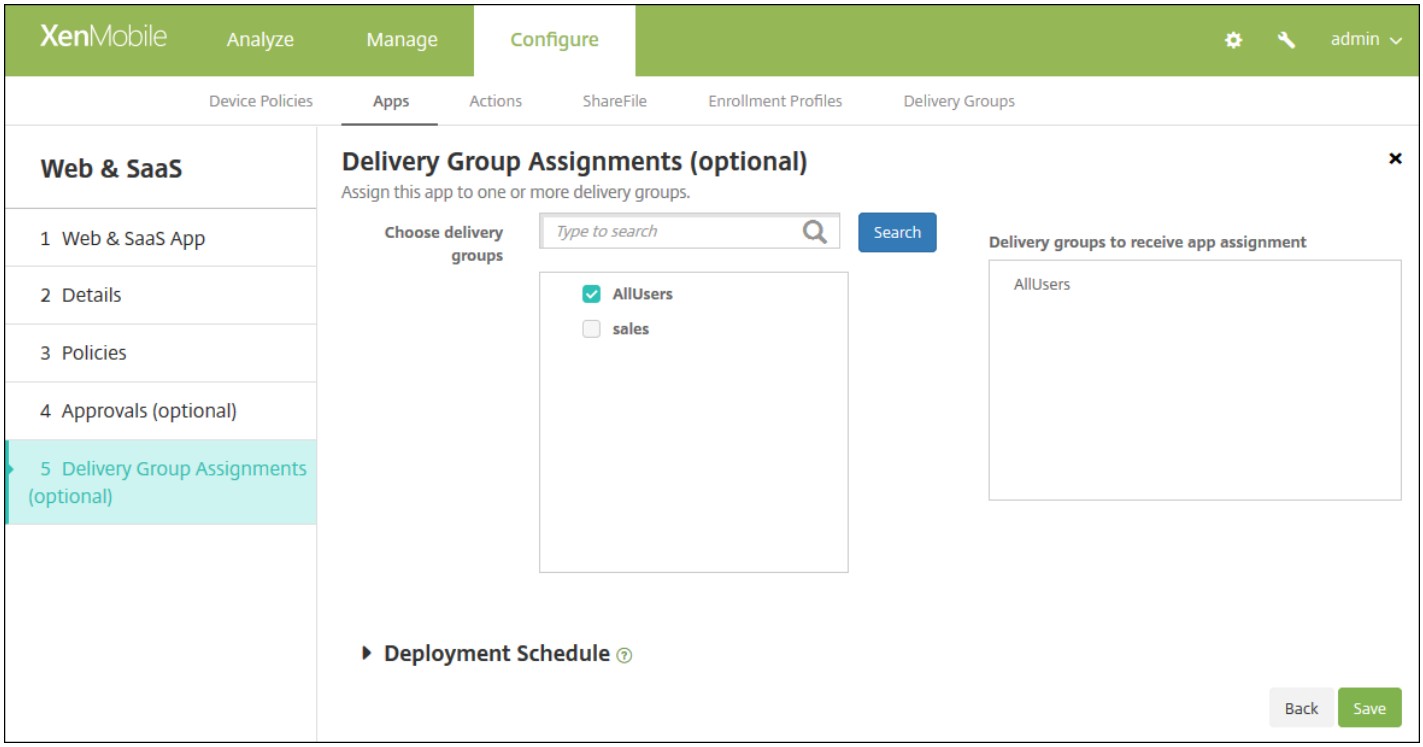
Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 8.

Configurez ces paramètres si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucune**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants :
  - **Nom** : entrez un nom unique pour le workflow.
  - **Description** : entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
    - Pas nécessaire
    - 1 niveau
    - 2 niveaux
    - 3 niveaux
  - **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
  - Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
    - Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
      - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.

- Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
- Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

8. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



9. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**,

qui ne s'applique pas à iOS.

11. Cliquez sur **Enregistrer**.

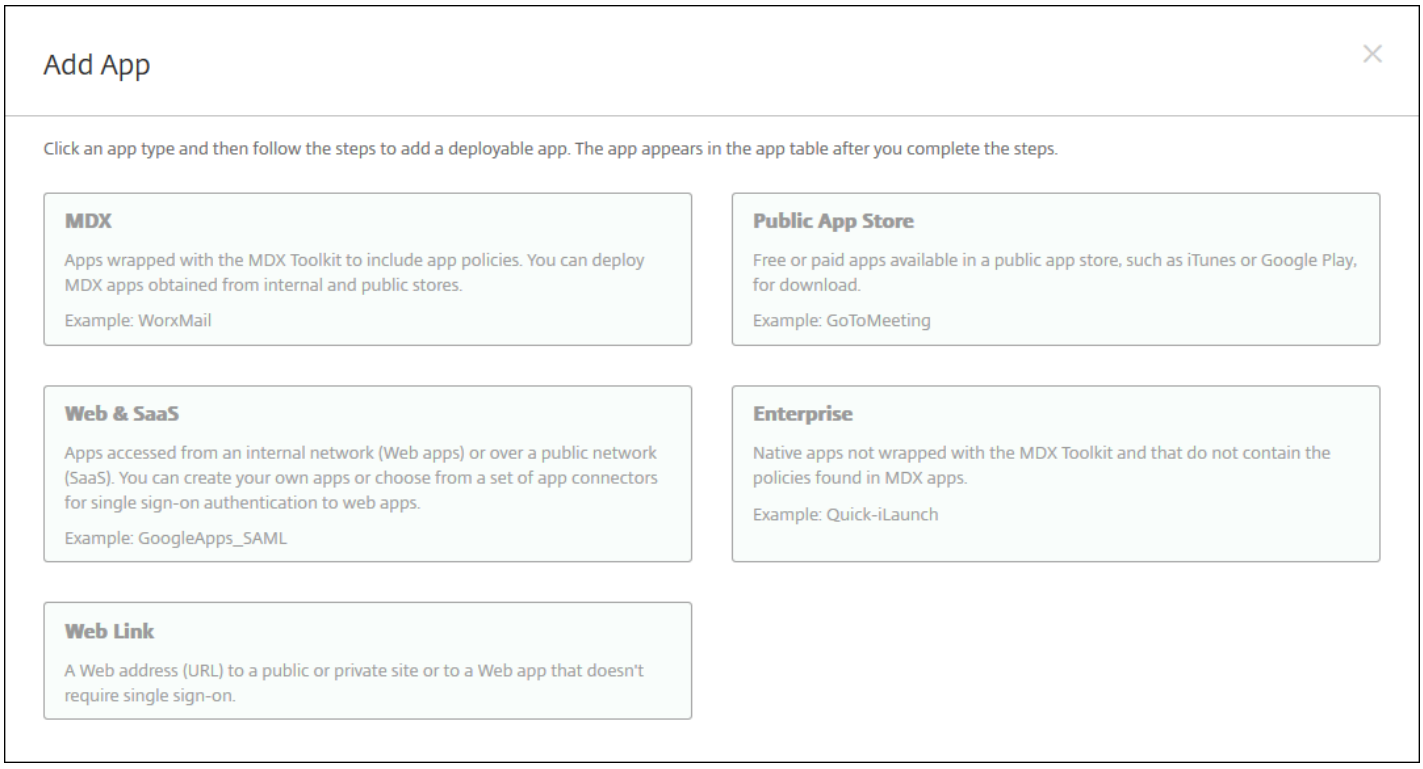
Ajouter une application d'entreprise

Les applications d'entreprise dans XenMobile représentent des applications natives qui ne sont pas wrappées avec le MDX Toolkit et qui ne contiennent aucune des stratégies associées aux applications MDX. Vous pouvez charger une application d'entreprise sur l'onglet **Applications** dans la console XenMobile. Les applications d'entreprise prennent en charge les plates-formes suivantes (et les types de fichiers correspondant) :

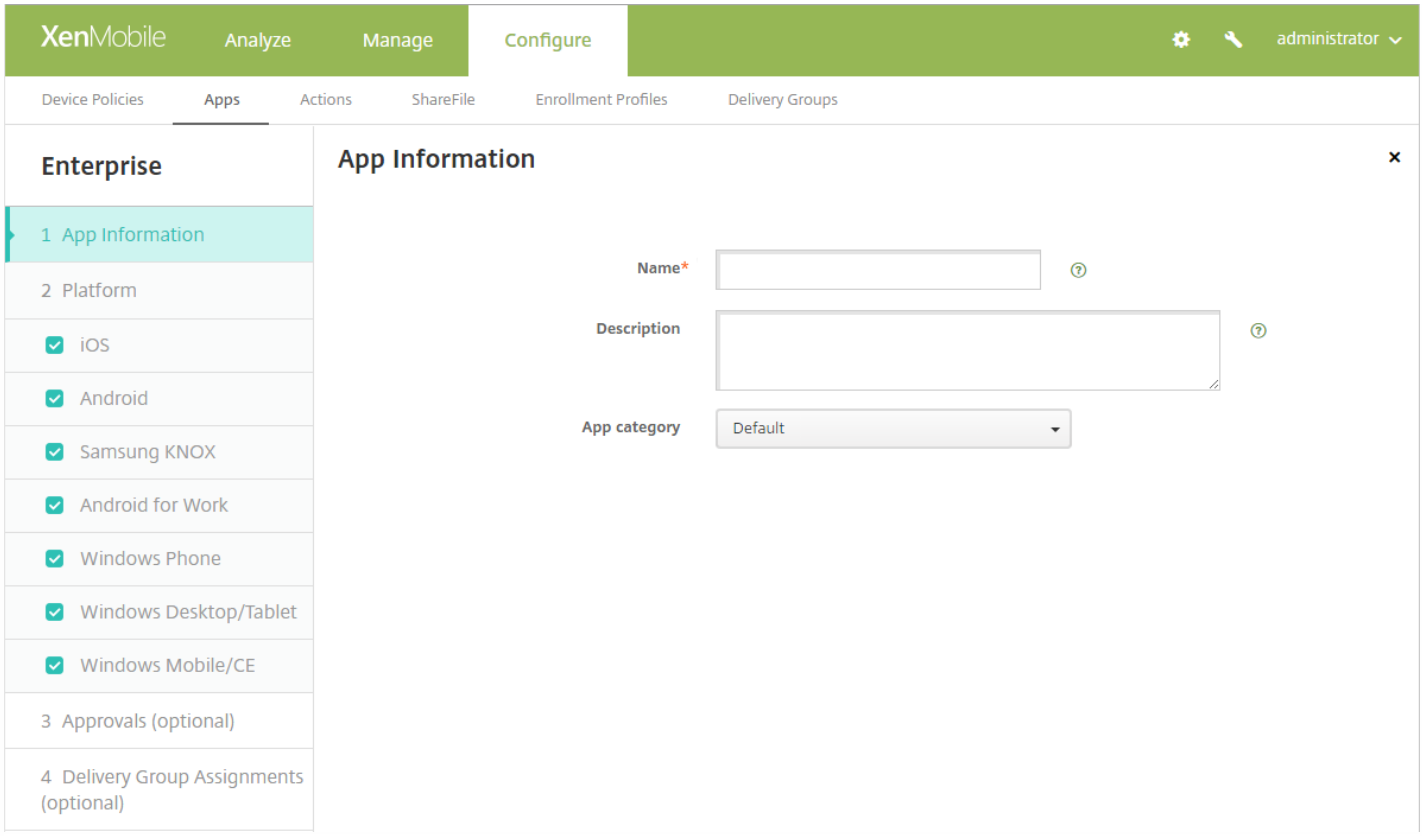
- iOS (fichier .ipa)
- Android (fichier .apk)
- Samsung KNOX (fichier .apk)
- Android for Work (fichier .apk)
- Windows Phone (fichier .xap ou .appx)
- Windows Tablet (fichier .appx)
- Windows Mobile/CE (fichier .cab)

1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'ouvre.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.



3. Cliquez sur **Enterprise**. La page **Informations sur l'application** s'affiche.



4. Dans le panneau **Informations sur l'application**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour l'application. Il est répertorié sous Nom de l'application dans le tableau Applications.
- **Description** : entrez une description pour l'application (facultatif).
- **Catégorie d'application** : si vous le souhaitez, dans la liste, cliquez sur la catégorie dans laquelle vous souhaitez ajouter l'application. Pour de plus amples informations sur les catégories d'applications, veuillez consulter la section Création de catégories d'applications dans XenMobile.

5. Cliquez sur **Next**. La page **Plates-formes d'applications** s'affiche.

6. Sous **Plates-formes**, sélectionnez les plates-formes que vous souhaitez ajouter. Si vous configurez une seule plate-forme, désélectionnez les autres.

Lorsque vous avez terminé de configurer les paramètres pour une plate-forme, référez-vous à l'étape 10 pour savoir comment définir les règles de déploiement de cette plate-forme.

7. Pour chaque plate-forme que vous avez choisie, sélectionnez le fichier à charger en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

8. Cliquez sur **Next**. La page d'informations sur l'application pour la plate-forme s'affiche.

9. Configurez les paramètres pour le type de plate-forme, notamment :

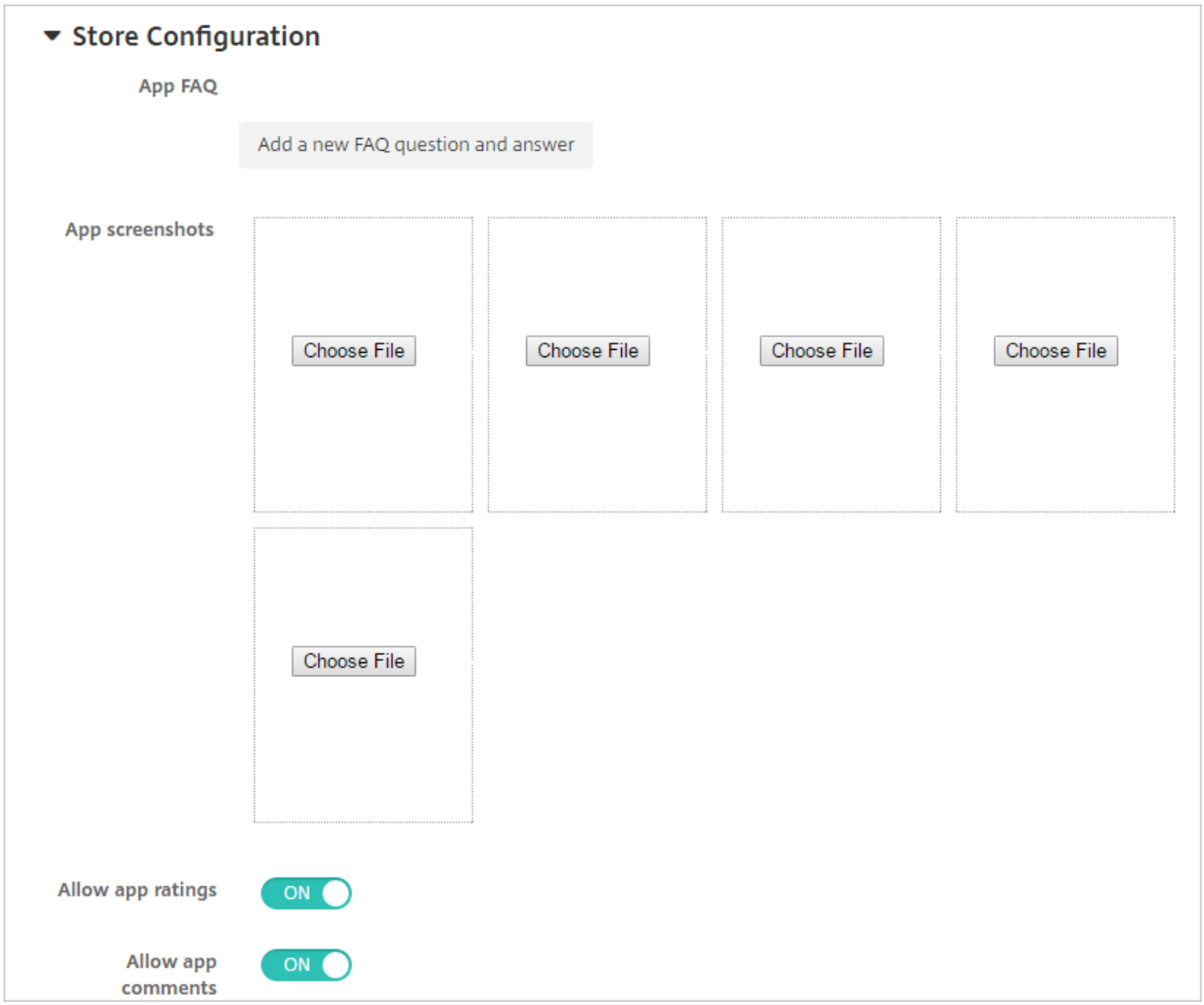
- **Nom du fichier** : entrez un nouveau nom pour l'application (facultatif).
- **Description de l'application** : entrez une nouvelle description pour l'application (facultatif).
- **Version de l'application** : vous ne pouvez pas modifier ce champ.
- **Version d'OS minimum** : si vous le souhaitez, entrez la version la plus ancienne du système d'exploitation que l'appareil

peut exécuter pour pouvoir utiliser l'application.

- **Version d'OS maximum** : si vous le souhaitez, entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
- **Appareils exclus** : si vous le souhaitez, entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
- **Supprimer l'application si le profil MDM est supprimé** : sélectionnez cette option si vous souhaitez supprimer l'application d'un appareil lorsque le profil MDM est supprimé. La valeur par défaut est **ON**.
- **Empêcher la sauvegarde des données d'application** : sélectionnez cette option si vous souhaitez empêcher l'application de sauvegarder les données. La valeur par défaut est **ON**.
- **Forcer l'application à être gérée** : si vous installez une application non gérée, sélectionnez **ON** si vous souhaitez que les utilisateurs sur des appareils non supervisés soient invités à autoriser la gestion de l'application. S'ils acceptent l'invite, l'application est gérée. Ce paramètre s'applique aux appareils iOS 9.x.

10. Configurez les règles de déploiement.

11. Développez **XenMobile Store Configuration**.

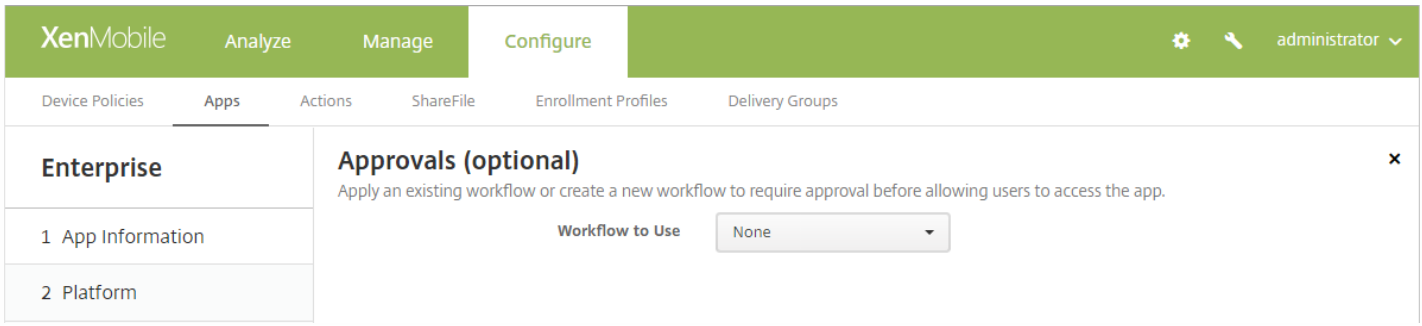


Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le

XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

12. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



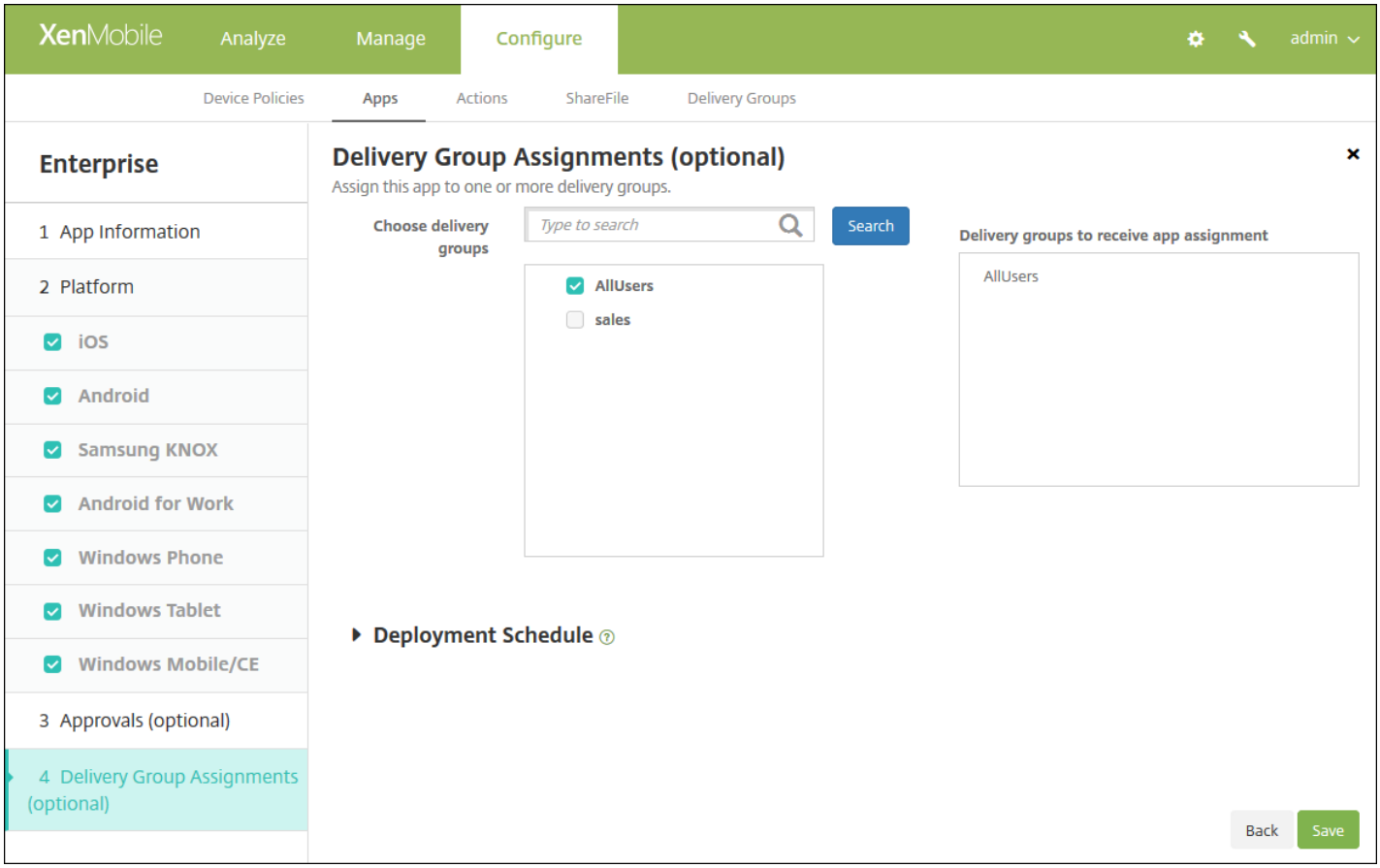
Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 13.

Configurez ces paramètres si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucune**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants :
  - **Nom** : entrez un nom unique pour le workflow.
  - **Description** : entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
    - Pas nécessaire
    - 1 niveau
    - 2 niveaux
    - 3 niveaux
  - **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.

- Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
    - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    - Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

13. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



14. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

15. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement**

précédent a échoué. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

16. Cliquez sur **Enregistrer**.

Ajouter un lien Web

Dans XenMobile, vous pouvez créer une adresse Web (URL) à un site public ou privé, ou à une application Web qui ne requiert pas d'authentification unique (SSO).

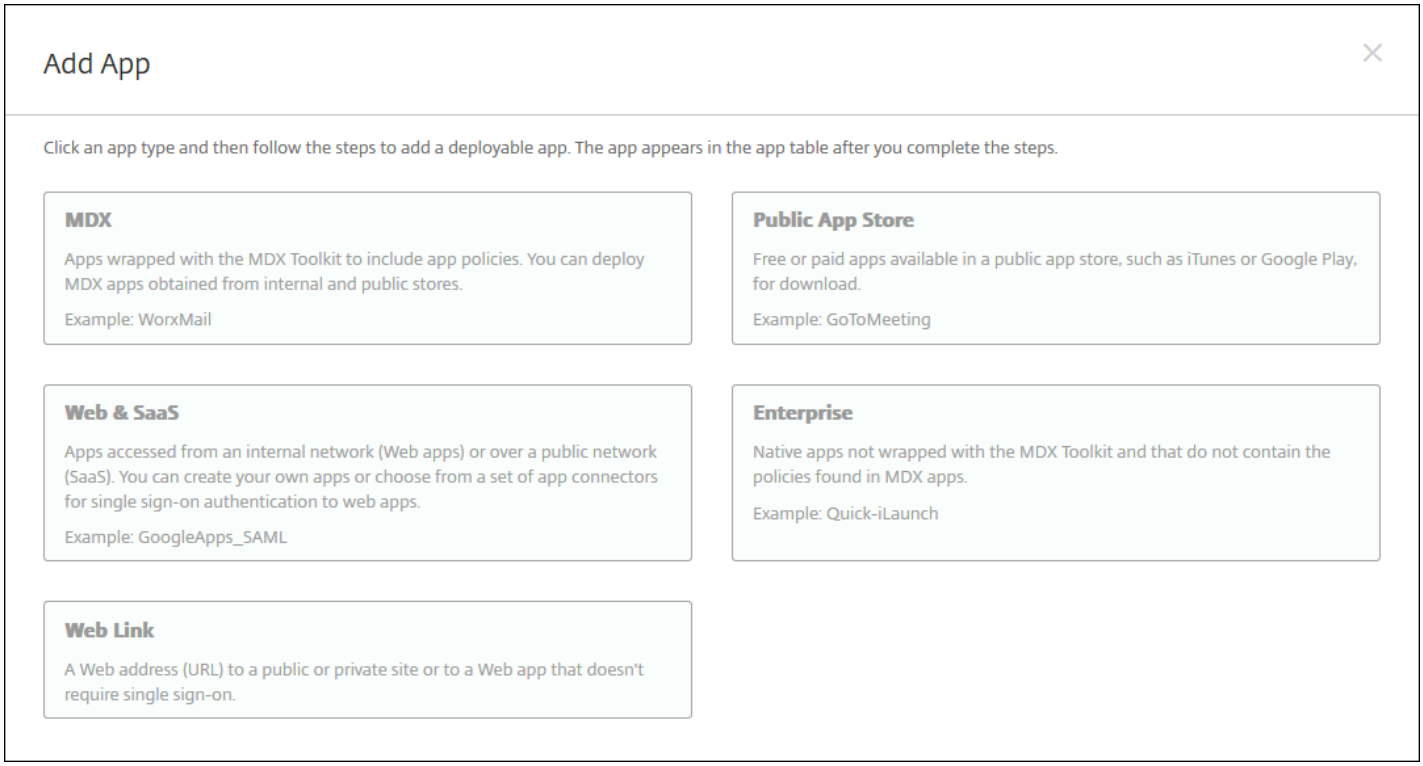
Vous pouvez configurer des liens Web dans l'onglet **Applications** de la console XenMobile. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau **Applications**. Lorsque les utilisateurs ouvrent une session avec Secure Hub, le lien s'affiche avec la liste des applications et bureaux disponibles.

Pour ajouter le lien, vous devez fournir les informations suivantes :

- Nom du lien
- Description du lien
- Adresse Web (URL)
- Catégorie
- Rôle
- Image au format .png (facultatif)

1. Dans la console XenMobile, cliquez sur **Configurer** > **Applications**. La page **Applications** s'affiche.

2. Cliquez sur **Add**. La boîte de dialogue **Ajouter une application** s'affiche.

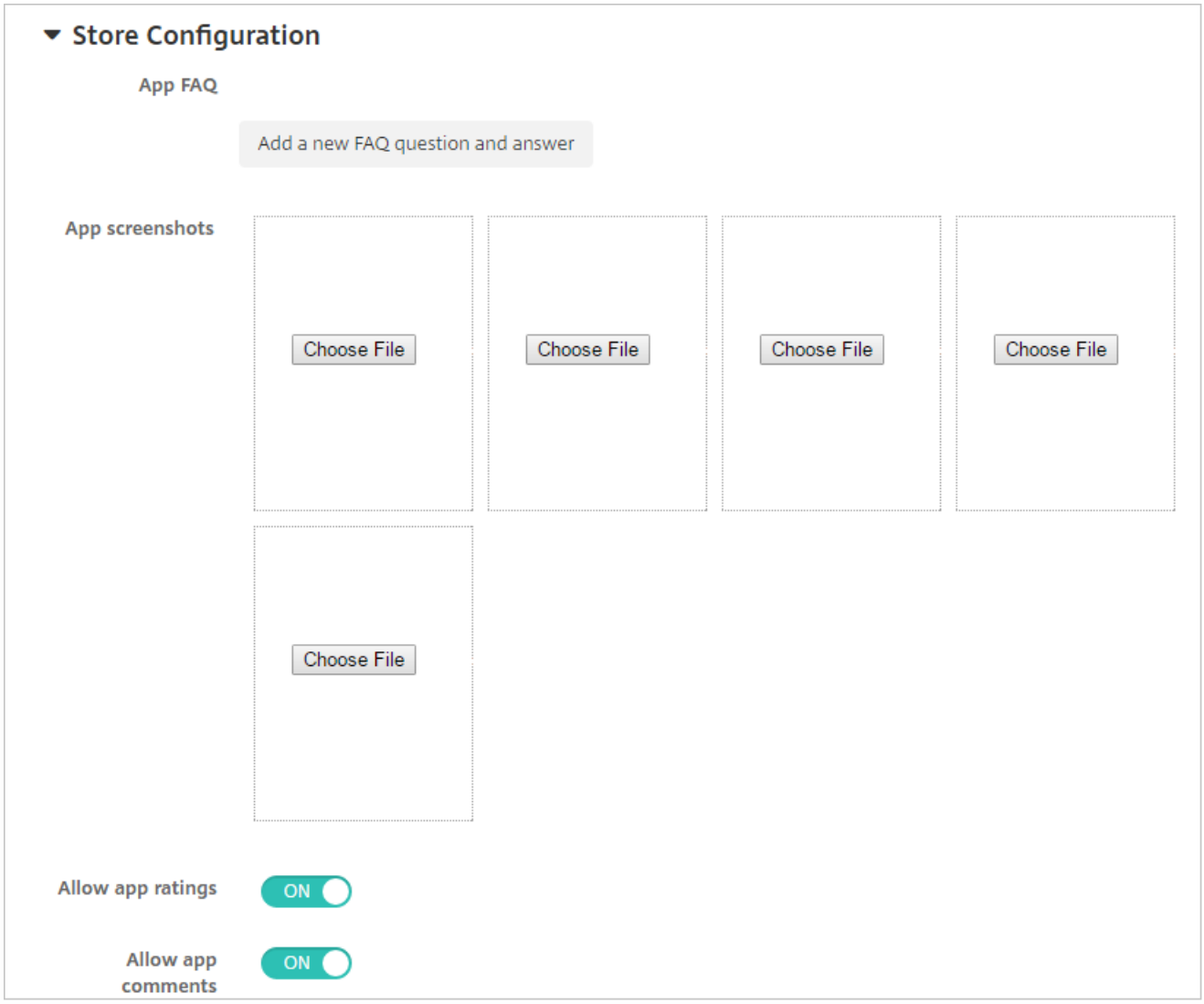


3. Cliquez sur **Lien Web**. La page **Informations sur l'application** s'affiche.

4. Configurez les paramètres suivants :

- **Nom de l'application** : acceptez le nom attribué ou entrez un nouveau nom.
- **Description de l'application** : acceptez la description existante ou choisissez la vôtre.
- **URL** : acceptez l'URL attribuée ou entrez l'adresse Web de l'application. Selon le connecteur que vous choisissez, ce champ peut contenir un paramètre fictif que vous devez remplacer avant de pouvoir passer à la page suivante.
- **L'application est hébergée dans le réseau interne** : indiquez si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à l'application interne à partir d'un site distant, ils doivent se connecter par l'intermédiaire de NetScaler Gateway. En réglant cette option sur **ON**, le mot-clé VPN est ajouté à l'application et permet aux utilisateurs de se connecter via NetScaler Gateway. La valeur par défaut est **OFF**.
- **Catégorie d'application** : dans la liste, cliquez sur une catégorie à appliquer à l'application (facultatif).
- **Image** : indiquez si vous souhaitez utiliser l'image Citrix par défaut ou charger votre propre image d'application. La valeur par défaut est Utiliser valeur par défaut.
  - Si vous souhaitez télécharger votre propre image, sélectionnez-la en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier. Le fichier doit être un fichier .PNG ; vous ne pouvez pas charger une image GIF ou JPEG. Lorsque vous ajoutez un graphique personnalisé, vous ne pouvez pas le modifier ultérieurement.

5. Développez **XenMobile Store Configuration**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

6. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.

7. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous

sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

8. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- Cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

9. Cliquez sur **Enregistrer**.

Activer les applications Microsoft 365

Vous pouvez ouvrir le conteneur MDX pour autoriser Secure Mail, Secure Web et ShareFile à transférer des documents et données à des applications Microsoft Office 365. Pour de plus amples informations, consultez la section Autoriser l'interaction sécurisée avec les applications Office 365.

Créer et gérer des workflows

Vous pouvez appliquer des workflows pour gérer la création et la suppression des comptes d'utilisateur. Avant de pouvoir utiliser un workflow, vous devez identifier les personnes de votre organisation chargées d'approuver les demandes d'ouverture de comptes d'utilisateur. Vous pouvez ensuite utiliser le modèle de workflow pour créer et approuver les demandes.

Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres d'e-mail de workflow, qui doivent être définis avant que vous puissiez utiliser des workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert une approbation.

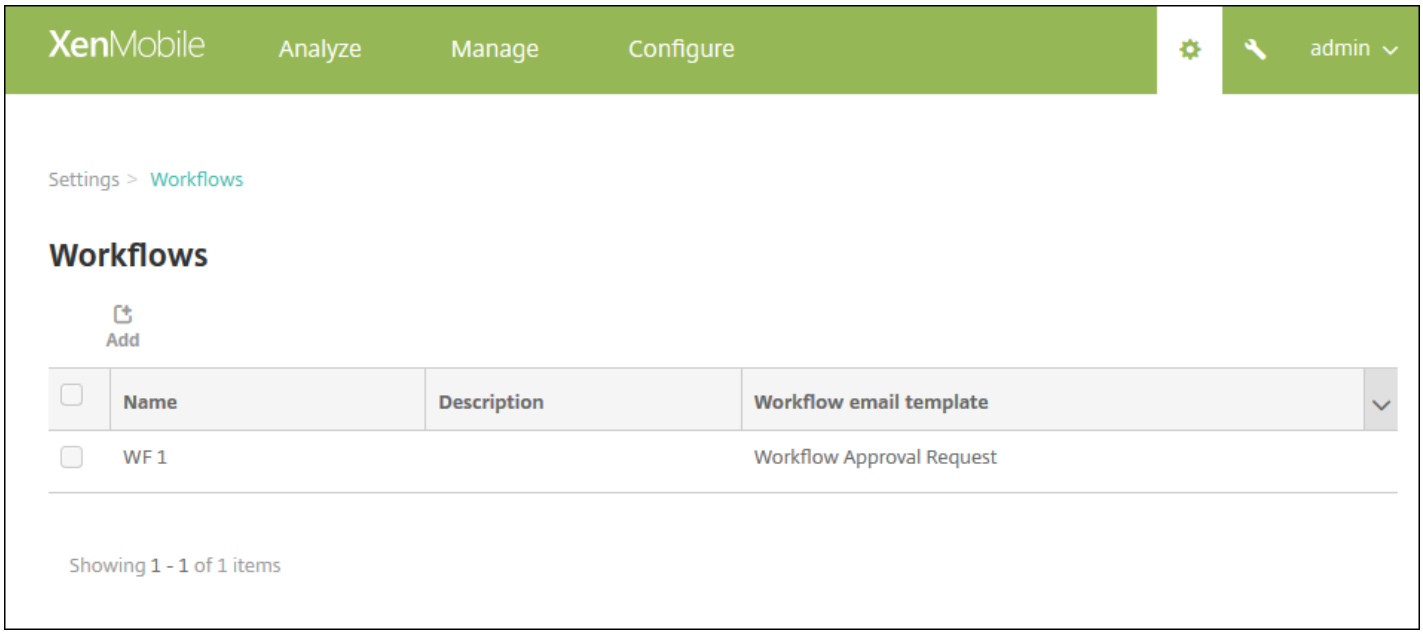
Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

- Dans la page Workflows sur la console XenMobile. Sur la page Workflows, vous pouvez configurer plusieurs workflows à utiliser pour la configuration d'applications. Lorsque vous configurez des workflows sur la page Workflows, vous pouvez sélectionner le workflow lors de la configuration de l'application.
- Lorsque vous configurez un connecteur d'application, dans l'application, vous devez fournir un nom de workflow, puis configurer les personnes qui peuvent approuver la demande de compte utilisateur.

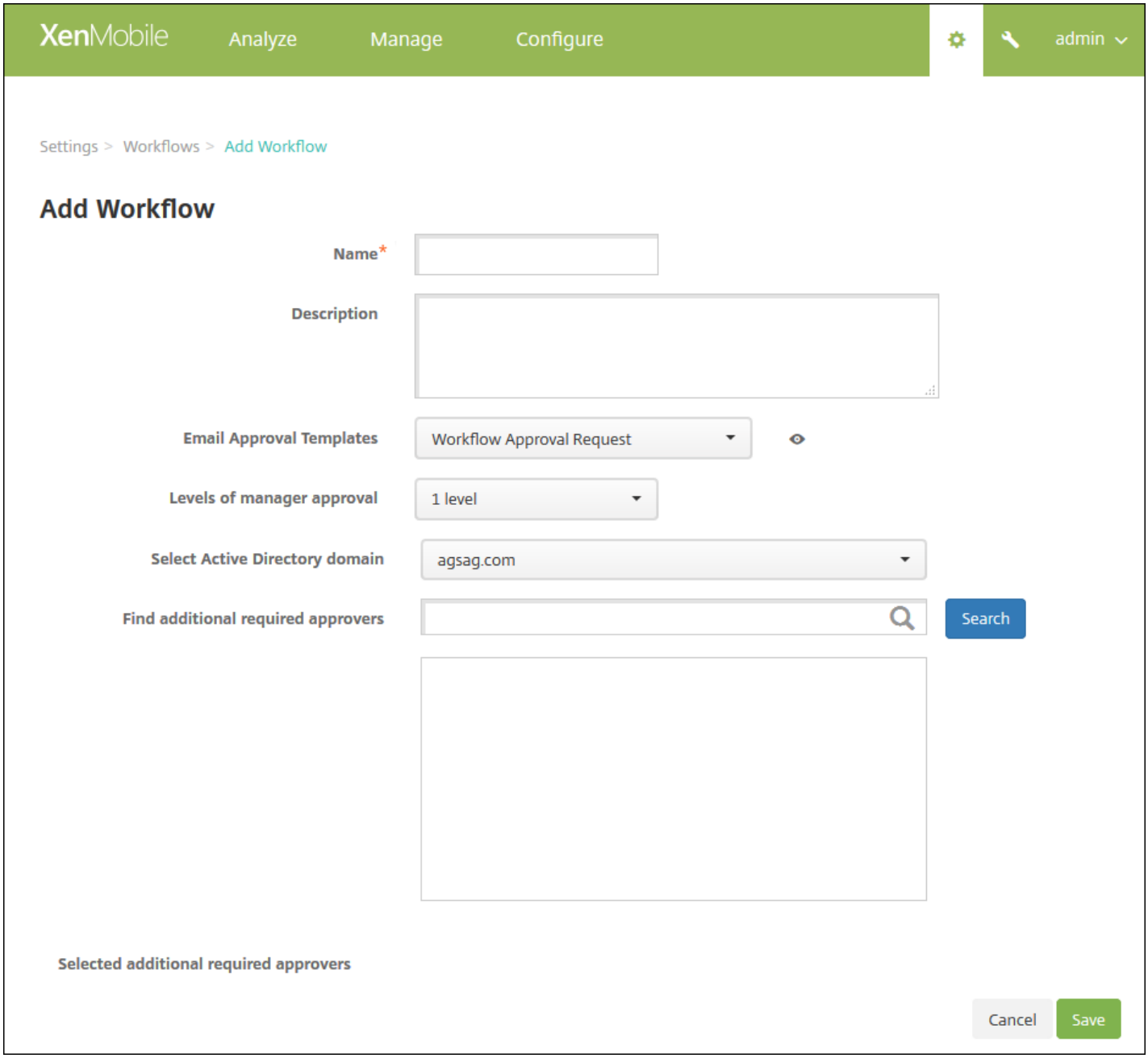
Vous pouvez désigner jusqu'à trois niveaux pour l'approbation du responsable des comptes d'utilisateur. Si vous voulez faire approuver le compte utilisateur par d'autres personnes, vous pouvez rechercher, puis sélectionner leur nom ou leur adresse e-mail. Lorsque XenMobile trouve la personne concernée, vous pouvez l'ajouter au workflow. Toutes les personnes figurant dans le workflow reçoivent un e-mail afin d'approuver ou de refuser l'ouverture du nouveau compte d'utilisateur.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Workflows**. La page **Workflows** s'affiche.

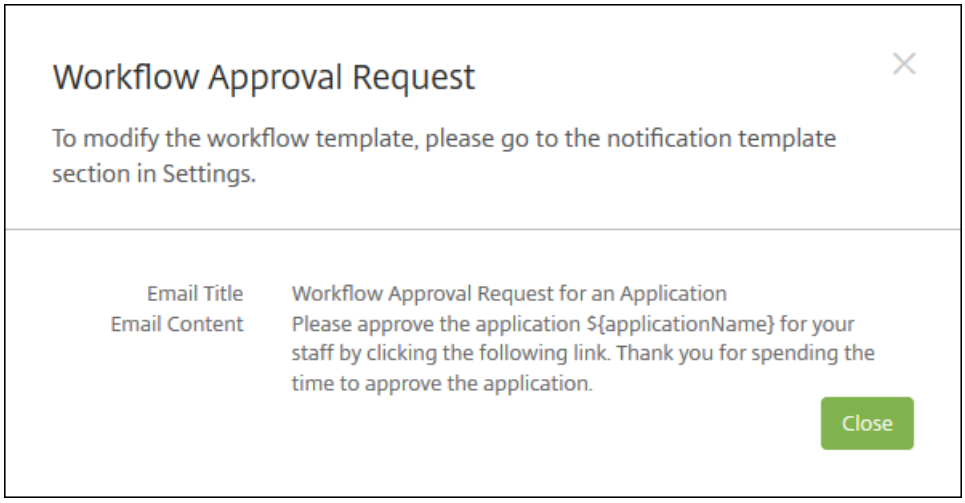


3. Cliquez sur **Ajouter**. La page **Ajouter un workflow** s'affiche.



4. Configurez les paramètres suivants :

- **Nom** : entrez un nom unique pour le workflow.
- **Description** : entrez une description pour le workflow (facultatif).
- **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Vous créez des modèles d'e-mail dans la section Modèles de notification sous Paramètres dans la console XenMobile. Lorsque vous cliquez sur l'icône d'œil à droite de ce champ, la boîte de dialogue suivante s'affiche.



- **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est 1 niveau. Les options possibles sont les suivantes :
  - Pas nécessaire
  - 1 niveau
  - 2 niveaux
  - 3 niveaux
- **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
- **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur Rechercher. Les noms proviennent d'Active Directory.
- Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer une personne de la liste **Approbateurs supplémentaires requis sélectionnés**, procédez comme suit :
    - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la recherche.
    - Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

5. Cliquez sur **Enregistrer**. Le workflow créé s'affiche sur la page **Workflows**.

Après avoir créé le workflow, vous pouvez afficher les détails du workflow, voir les applications associées au workflow ou supprimer le workflow. Vous ne pouvez pas modifier un workflow après sa création. Si vous avez besoin d'un workflow avec différents niveaux d'approbation ou approbateurs, vous devez créer un nouveau workflow.

Pour afficher les détails d'un workflow et le supprimer

1. Sur la page **Workflows**, dans la liste des workflows, sélectionnez un workflow en cliquant sur la ligne dans le tableau ou en cochant la case à cocher en regard du workflow.

2. Pour supprimer un workflow, cliquez sur **Supprimer**. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur **Delete** .

Important : vous ne pouvez pas annuler cette opération.

Types de connecteur d'application

Feb 23, 2017

Le tableau suivant dresse la liste des connecteurs et des types de connecteurs disponibles dans XenMobile lorsque vous ajoutez une application Web ou SaaS. Vous pouvez également ajouter un nouveau connecteur à XenMobile lorsque vous ajoutez une application Web ou SaaS.

Il indique si le connecteur prend en charge la gestion des comptes d'utilisateur, ce qui permet de créer de nouveaux comptes, de façon automatique ou à l'aide d'un workflow.

Nom du connecteur	SSO SAML	Prend en charge la gestion des comptes d'utilisateur
EchoSign_SAML	O	O
Globoforce_SAML		**Remarque** : lorsque vous utilisez ce connecteur, vous devez Activer la gestion des utilisateurs pour le provisioning pour assurer une intégration SSO transparente.
GoogleApps_SAML	O	O
GoogleApps_SAML_IDP	O	O
Lynda_SAML	O	O
Office365_SAML	O	O
Salesforce_SAML	O	O
Salesforce_SAML_SP	O	O
SandBox_SAML	O	
SuccessFactors_SAML	O	
ShareFile_SAML	O	
ShareFile_SAML_SP	O	
WebEx_SAML_SP	O	O

Mettre à niveau les applications MDX ou Enterprise

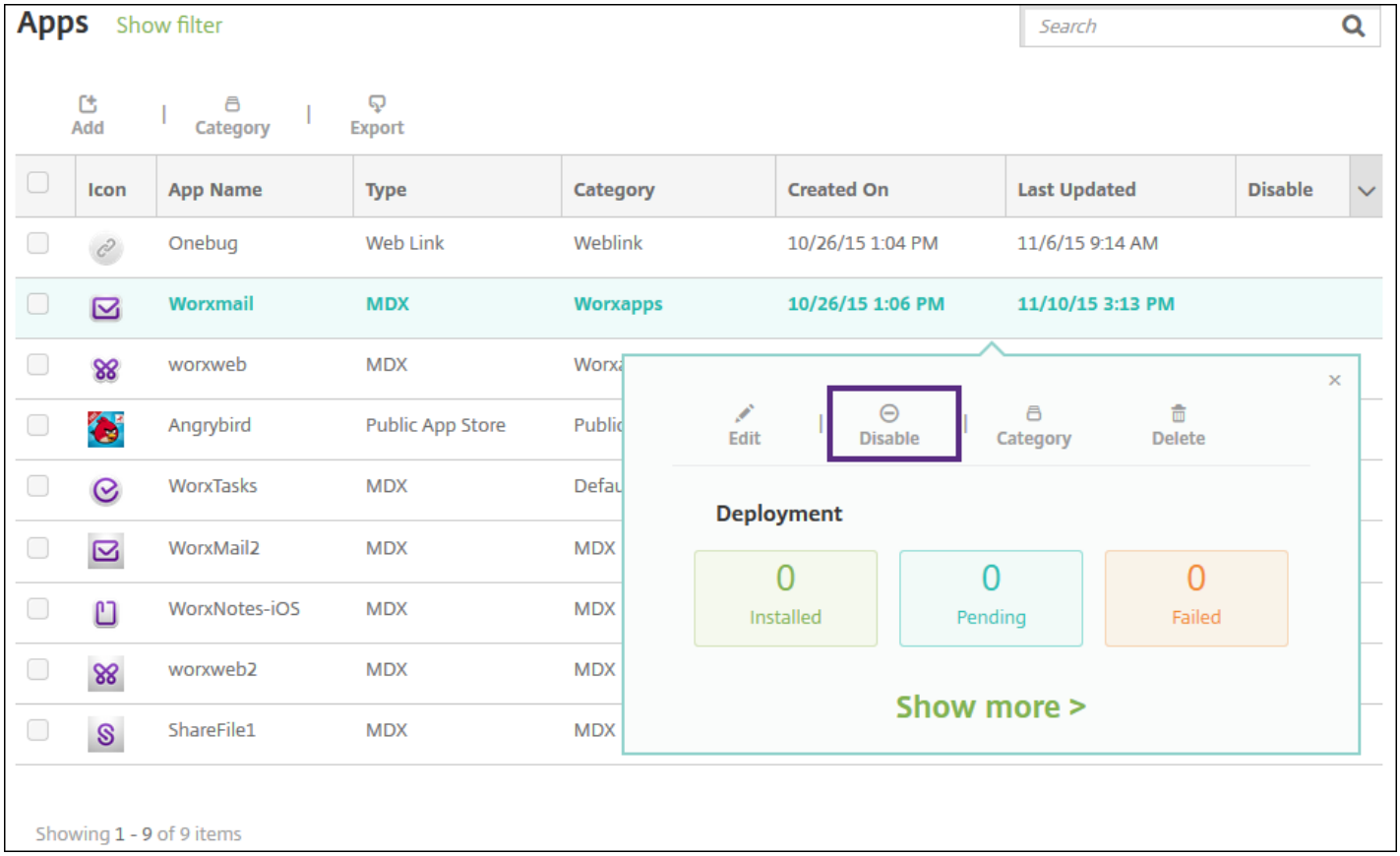
Feb 23, 2017

Pour mettre à niveau une application MDX ou Enterprise dans XenMobile, désactivez-la dans la console XenMobile, puis téléchargez la nouvelle version de l'application.

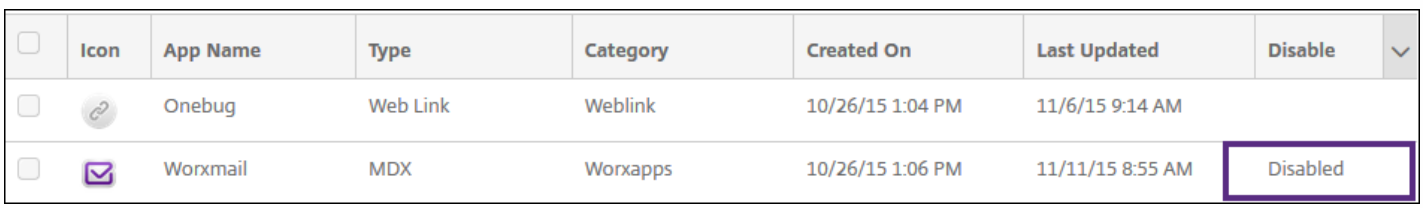
1. Dans la console XenMobile, cliquez sur **Configurer > Applications**. La page **Applications** s'affiche.

2. Pour les appareils gérés (appareils inscrits dans XenMobile pour la gestion des appareils mobiles), passez à l'étape 3. Pour les appareils non gérés (appareils inscrits dans XenMobile uniquement à des fins de gestion des applications d'entreprise), procédez comme suit :

- Dans le tableau **Applications**, cliquez sur la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.
- Cliquez sur **Désactiver** dans le menu qui s'affiche.



- Cliquez sur **Désactiver** dans la boîte de dialogue de confirmation. *Désactivé* s'affiche dans la colonne **Désactiver** pour l'application.



Remarque : l'application désactivée passe en mode de maintenance. Lorsque l'application est désactivée, les utilisateurs ne peuvent pas se reconnecter à l'application après avoir fermé leur session. La désactivation d'applications est un paramètre facultatif, mais nous recommandons de désactiver l'application pour éviter les problèmes avec la fonctionnalité de l'application. Les problèmes peuvent survenir en raison des mises à jour de stratégies, par exemple, ou si des utilisateurs effectuent une requête de téléchargement en même temps que vous chargez l'application sur XenMobile.

3. Dans le tableau **Applications**, cliquez sur la case à cocher en regard de l'application, ou cliquez sur la ligne contenant l'application que vous souhaitez mettre à jour.

4. Cliquez sur **Modifier** dans le menu qui s'affiche. La page **Informations sur l'application** s'affiche avec la liste des plates-formes que vous avez choisies pour l'application sélectionnée.

5. Configurez les paramètres suivants :

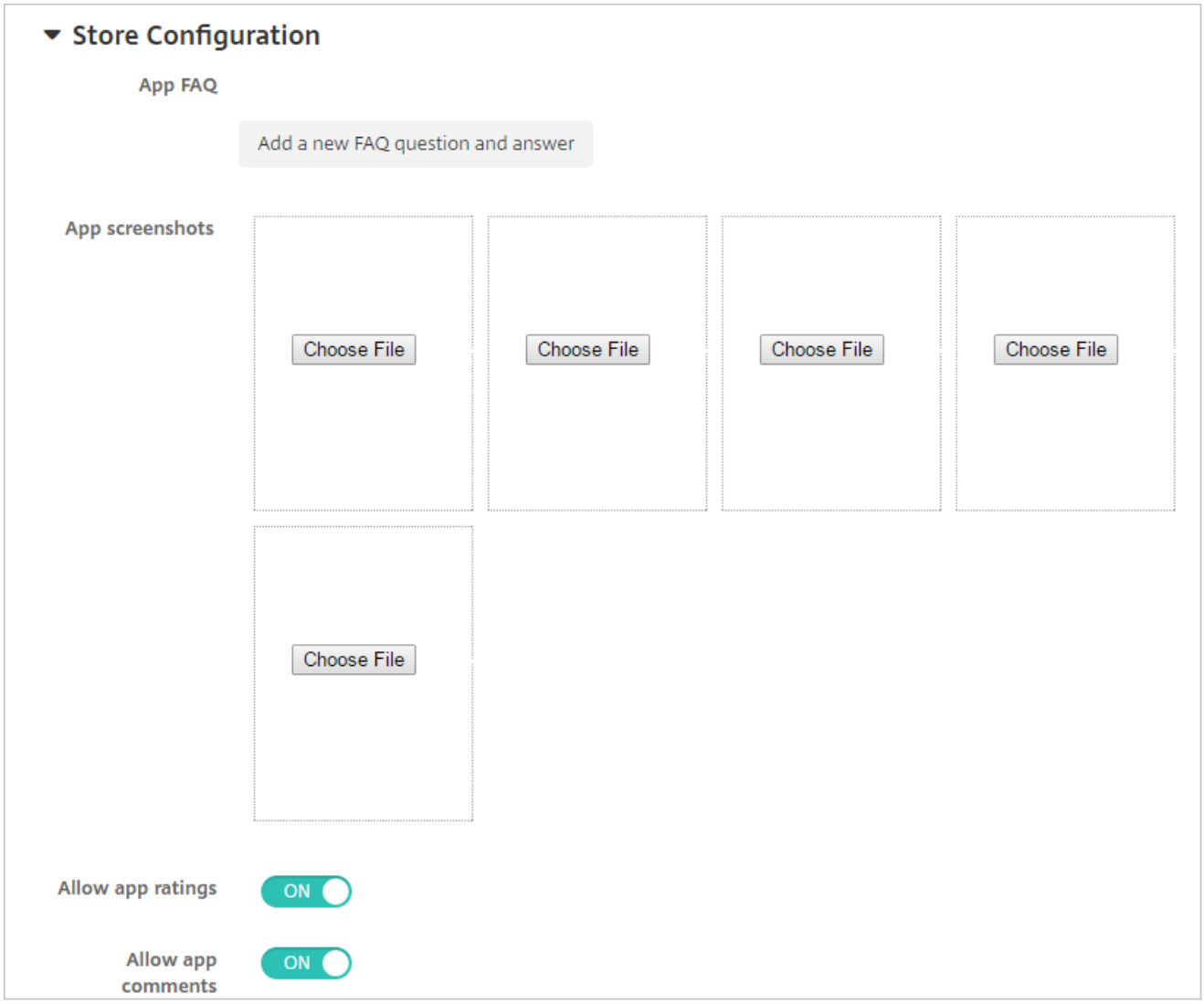
- **Nom** : si vous le souhaitez, vous pouvez modifier le nom de l'application.
- **Description** : si vous le souhaitez, vous pouvez modifier la description de l'application.
- **Catégorie d'application** : si vous le souhaitez, vous pouvez modifier la catégorie.

6. Cliquez sur **Suivant**. La première page de plate-forme sélectionnée s'affiche. Effectuez les opérations suivantes pour chaque plate-forme sélectionnée :

- Choisissez le fichier de remplacement que vous voulez charger en cliquant sur le bouton **Charger** et accédez à l'emplacement du fichier. L'application se charge dans XenMobile.
- Si vous le souhaitez, vous pouvez modifier les détails de l'application et les paramètres de stratégie pour la plate-forme.
- Si vous le souhaitez, vous pouvez configurer des règles de déploiement (voir l'étape 7) et XenMobile Store (voir l'étape 8).

7. Configurez les règles de déploiement.

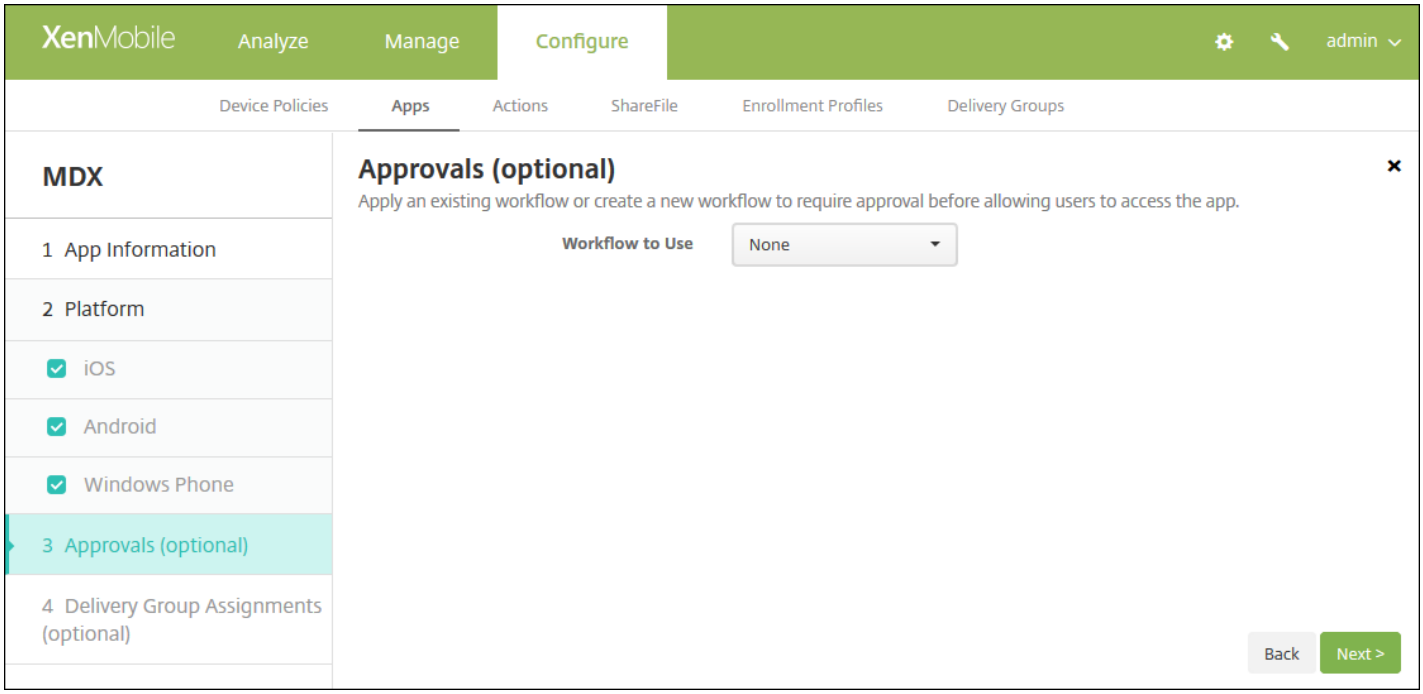
8. Développez **Configuration du magasin**.



Si vous le souhaitez, vous pouvez ajouter un FAQ pour l'application ou des captures d'écran qui s'affichent dans le XenMobile Store. Vous pouvez également indiquer si les utilisateurs peuvent évaluer ou ajouter des commentaires sur l'application.

- Pour configurer ces paramètres :
  - **FAQ sur les applications** : ajoutez des questions et réponses pour l'application.
  - **Copies d'écran des applications** : ajoutez des captures d'écran pour faciliter le classement de l'application dans le XenMobile Store. L'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.
  - **Autoriser notation des applications** : indiquez si un utilisateur peut évaluer l'application. La valeur par défaut est **ON**.
  - **Autoriser commentaires sur les applications** : indiquez si les utilisateurs peuvent laisser des commentaires sur l'application sélectionnée. La valeur par défaut est **ON**.

9. Cliquez sur **Suivant**. La page **Approbations** s'affiche.



10. Vous utilisez des workflows lorsque vous avez besoin d'une approbation pour créer des comptes d'utilisateur. S'il n'est pas nécessaire de configurer des workflows d'approbation, vous pouvez passer à l'étape 11.

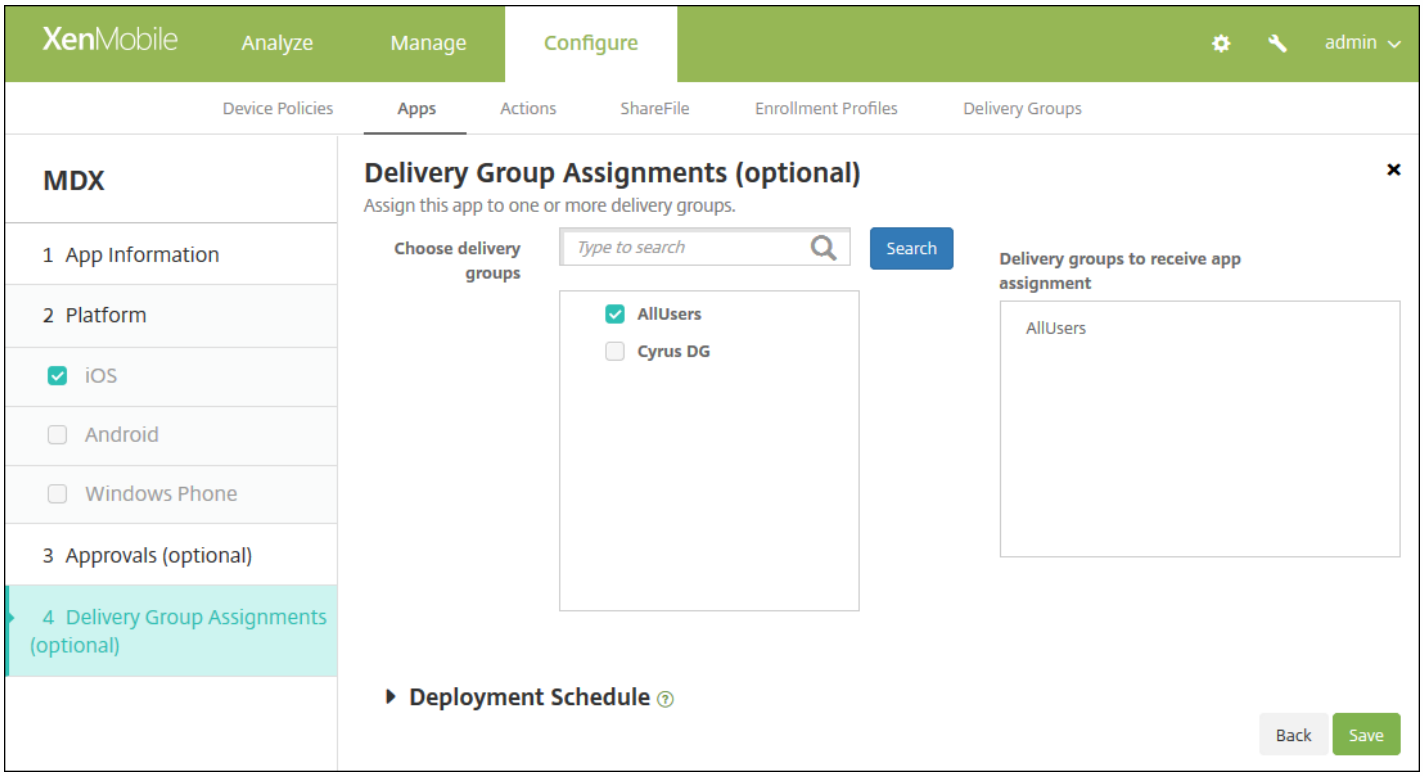
Configurez ce paramètre si vous devez attribuer ou créer un workflow :

- **Workflow à utiliser** : dans la liste, cliquez sur un workflow existant ou cliquez sur **Créer un nouveau workflow**. La valeur par défaut est **Aucune**.
- Si vous sélectionnez **Créer un nouveau workflow**, configurez les paramètres suivants :
  - **Nom** : entrez un nom unique pour le workflow.
  - **Description** : entrez une description pour le workflow (facultatif).
  - **Modèles d'approbation d'e-mail** : dans la liste, sélectionnez le modèle d'e-mail d'approbation à attribuer. Lorsque vous cliquez sur l'icône d'œil à droite du champ, une boîte de dialogue s'affiche dans laquelle vous pouvez afficher un aperçu du modèle.
  - **Niveaux d'approbation par un responsable** : dans la liste, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow. La valeur par défaut est **1 niveau**. Les options possibles sont les suivantes :
    - Pas nécessaire
    - 1 niveau
    - 2 niveaux
    - 3 niveaux
  - **Sélectionner un domaine Active Directory** : dans la liste, sélectionnez le domaine Active Directory à utiliser pour le workflow.
  - **Rechercher des approbateurs supplémentaires requis** : tapez le nom de la personne dans le champ de recherche et cliquez sur **Rechercher**. Les noms proviennent d'Active Directory.
  - Lorsque le nom de la personne s'affiche dans le champ, sélectionnez la case à cocher en regard de son nom. Le nom et l'adresse e-mail de cette personne s'affichent dans la liste **Approbateurs supplémentaires requis sélectionnés**.
  - Pour supprimer une personne de la liste Approbateurs supplémentaires requis sélectionnés, procédez comme suit :
    - Cliquez sur **Rechercher** pour afficher une liste de toutes les personnes dans le domaine sélectionné.
    - Tapez un nom complet ou partiel dans la zone de recherche et cliquez sur **Rechercher** pour limiter les résultats de la

recherche.

- Les personnes figurant dans la liste **Approbateurs supplémentaires requis sélectionnés** ont des coches en regard de leur nom dans la liste des résultats qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque nom à supprimer.

11. Cliquez sur **Suivant**. La page **Attribution de groupes de mise à disposition** s'affiche.



12. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer l'application. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

13. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**. Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**.

Remarque :

- cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres > Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.
- Le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

14. Cliquez sur **Enregistrer**. La page **Applications** s'affiche.

15. Si vous avez désactivé l'application à l'étape 2, effectuez les opérations suivantes :

- Dans le tableau des **Applications**, choisissez l'application que vous avez mis à jour puis dans le menu qui s'affiche, cliquez sur **Activer**.
- Dans la boîte de dialogue de confirmation qui s'affiche, cliquez sur **Activer**. Les utilisateurs peuvent désormais accéder à l'application et recevoir une notification les invitant à mettre l'application à niveau.

Synopsis des stratégies applicatives MDX

Feb 23, 2017

Pour consulter une liste des stratégies applicatives MDX pour iOS, Android et Windows Phone accompagnée de notes sur les restrictions et des recommandations de Citrix, consultez la section Synopsis des stratégies applicatives MDX dans la documentation du MDX Toolkit.

Personnalisation de XenMobile Store et de Citrix Secure Hub

Feb 23, 2017

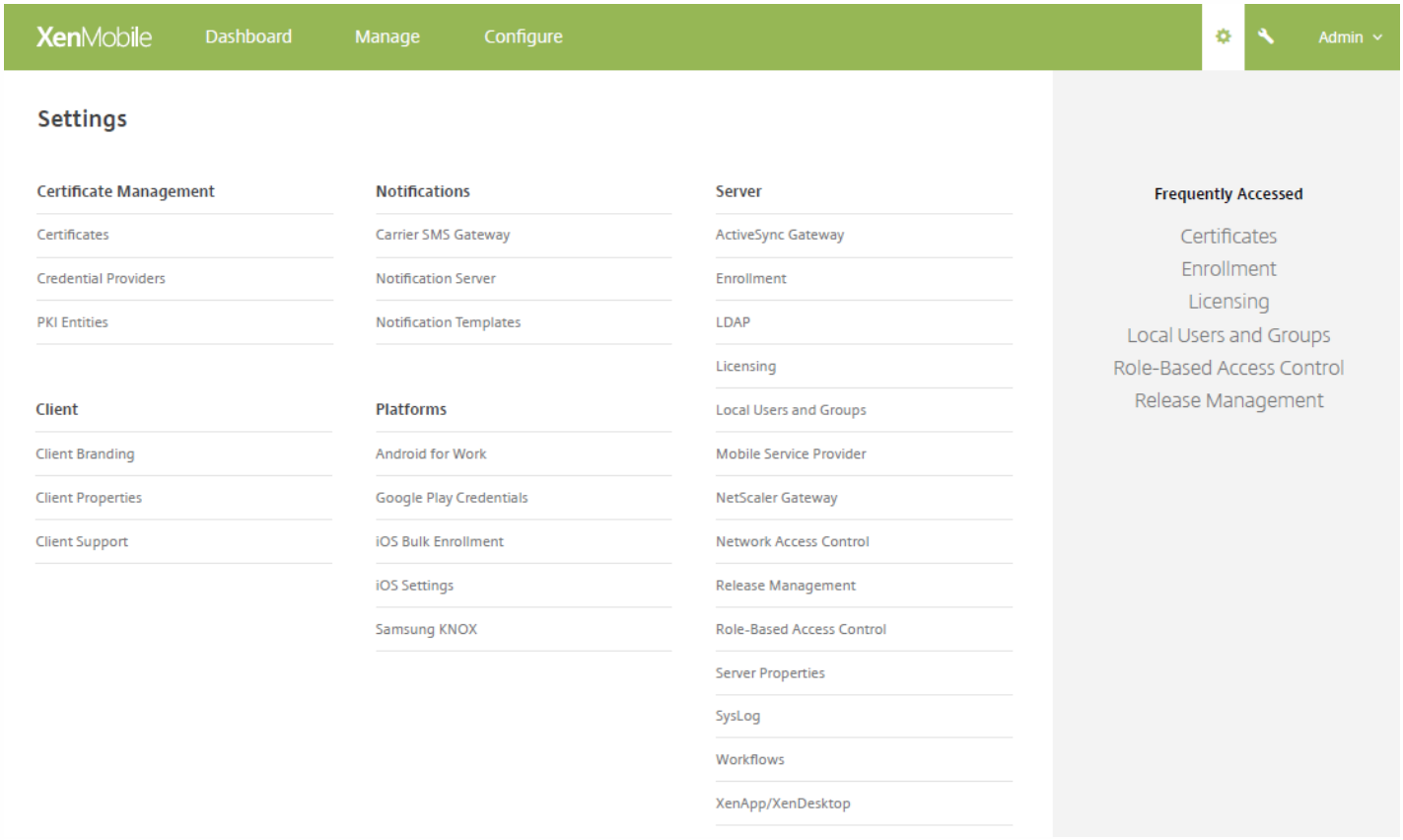
Vous pouvez configurer la manière dont les applications s'affichent dans le magasin et ajouter un logo pour personnaliser Secure Hub et XenMobile Store sur les appareils mobiles iOS et Android.

Remarque : avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

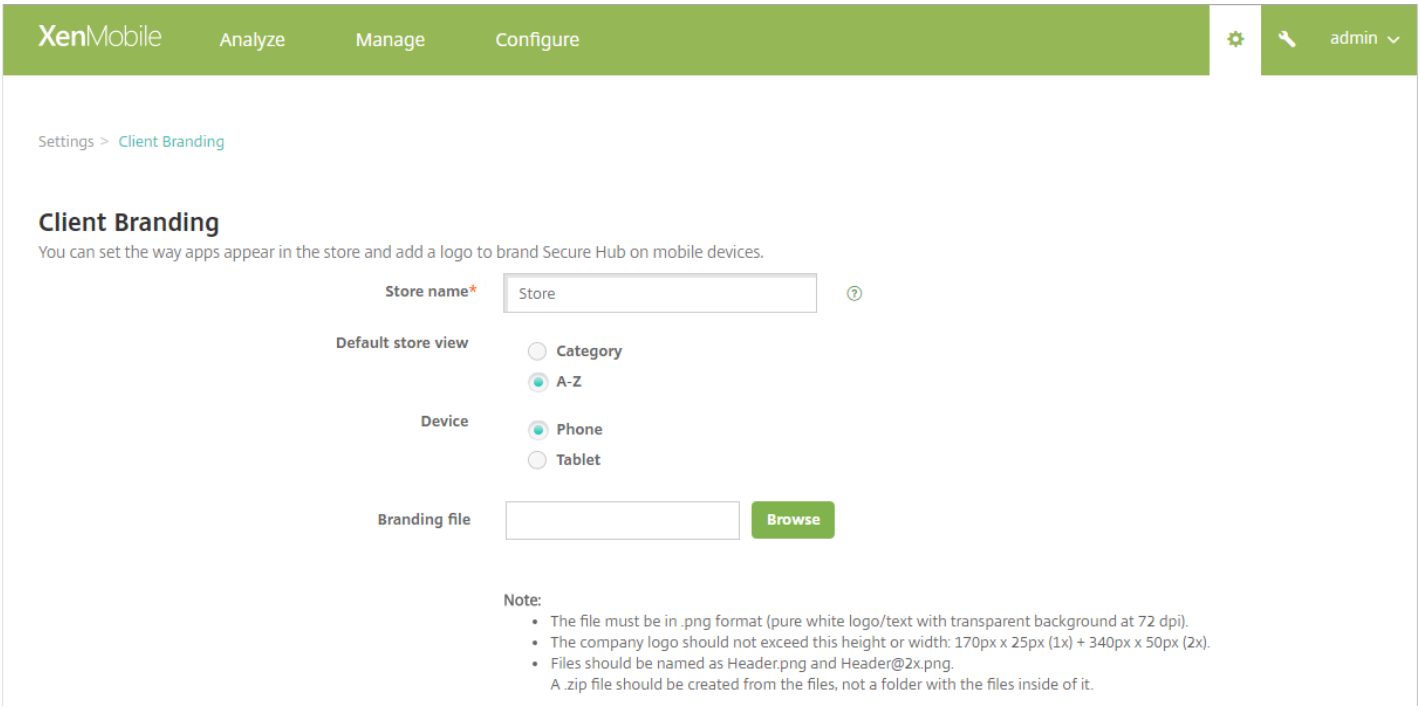
L'image personnalisée doit répondre à ces exigences :

- Le fichier doit être au format .png.
- Utilisez un logo blanc pur ou du texte avec un arrière-plan transparent à 72 ppp.
- Le logo de la société ne doit pas dépasser cette hauteur ou largeur : 170 px x 25 px (1x) et 340 px x 50 px (2x).
- Appelez les fichiers Header.png et Header@2x.png
- Créez un fichier .zip à partir des fichiers, et non un dossier contenant les fichiers.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.



2. Sous **Client**, cliquez sur **Personnalisation du client**. La page **Personnalisation du client** s'affiche.



Configurez les paramètres suivants :

- **Nom du magasin** : le nom s'affiche dans les informations de compte de l'utilisateur. La modification du nom change également l'adresse URL utilisée pour accéder aux services du magasin. Il n'est généralement pas nécessaire de modifier le nom par défaut.
- **Vue du magasin par défaut** : sélectionnez **Catégorie** ou **A-Z**. La valeur par défaut est **A-Z**.
- **Appareil** : sélectionnez **Téléphone** ou **Tablette**. La valeur par défaut est **Téléphone**.
- **Fichier de personnalisation** : sélectionnez une image ou un fichier .zip d'images à utiliser pour la personnalisation en cliquant sur **Parcourir** et en accédant à l'emplacement du fichier.

3. Cliquez sur **Enregistrer**.

Pour déployer ce paquetage auprès des appareils de vos utilisateurs, vous devez créer un paquetage de déploiement et le déployer sur les appareils des utilisateurs.

Citrix Launcher

Mar 31, 2017

Citrix Launcher vous permet de personnaliser l'expérience de l'utilisateur pour les appareils Android déployés par XenMobile. La version Android minimale prise en charge pour la gestion par Secure Hub de Citrix Launcher est Android 4.0.3. Vous pouvez ajouter la **stratégie Configuration du Launcher** pour contrôler ces restrictions au niveau de l'appareil de Citrix Launcher :

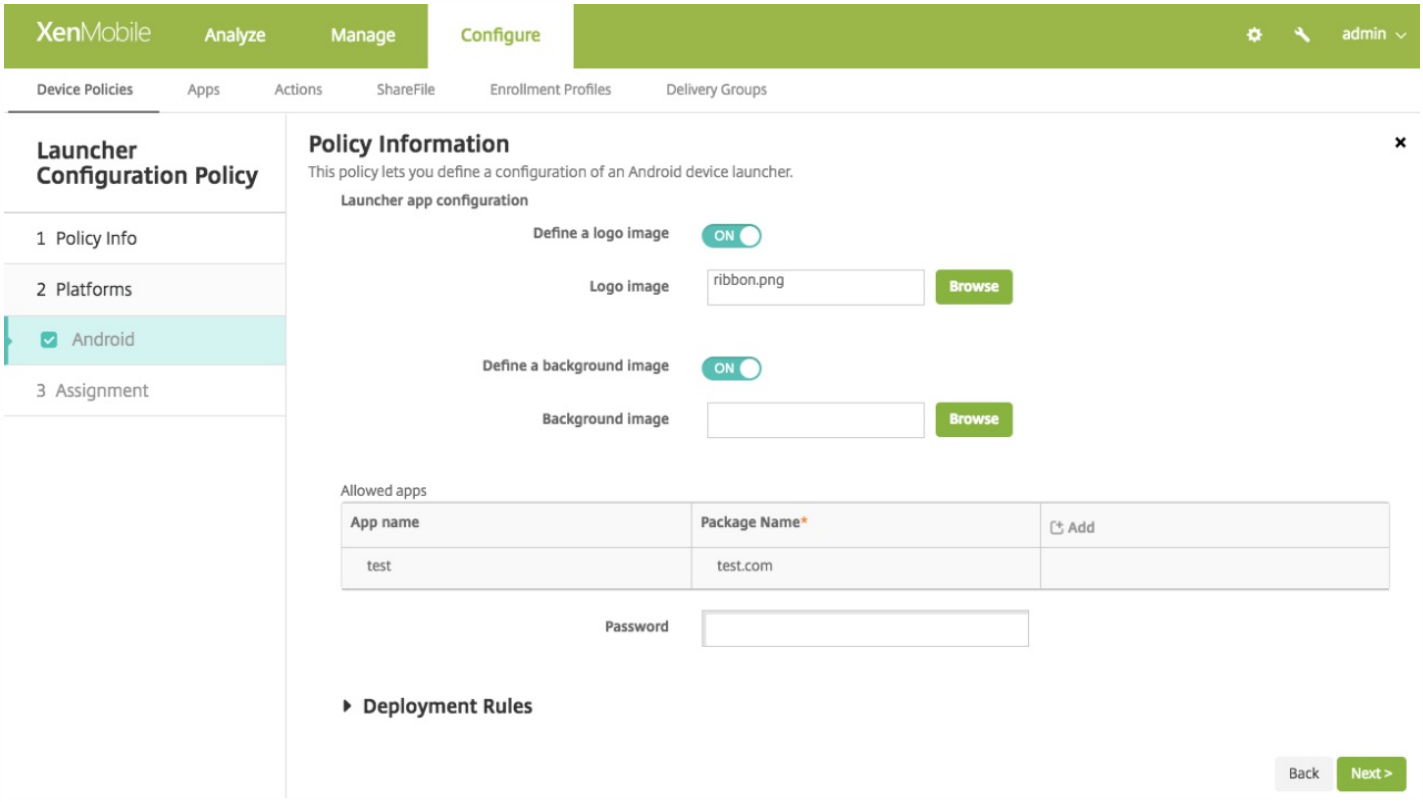
- Gérez les appareils Android, de façon à ce que les utilisateurs puissent uniquement accéder aux applications que vous spécifiez.
- Si vous le souhaitez, vous pouvez spécifier une image de logo personnalisé pour l'icône Citrix Launcher et une image d'arrière-plan personnalisée pour Citrix Launcher.
- Spécifiez un mot de passe que les utilisateurs doivent entrer pour quitter le Launcher.

Le Lanceur d'appareils fournit un accès intégré aux paramètres de l'appareil tels que Wi-Fi, Bluetooth, code secret et d'autres paramètres. Citrix Launcher n'est pas destiné à être une couche de sécurité supplémentaire venant s'ajouter à ce que la plate-forme de l'appareil offre déjà.

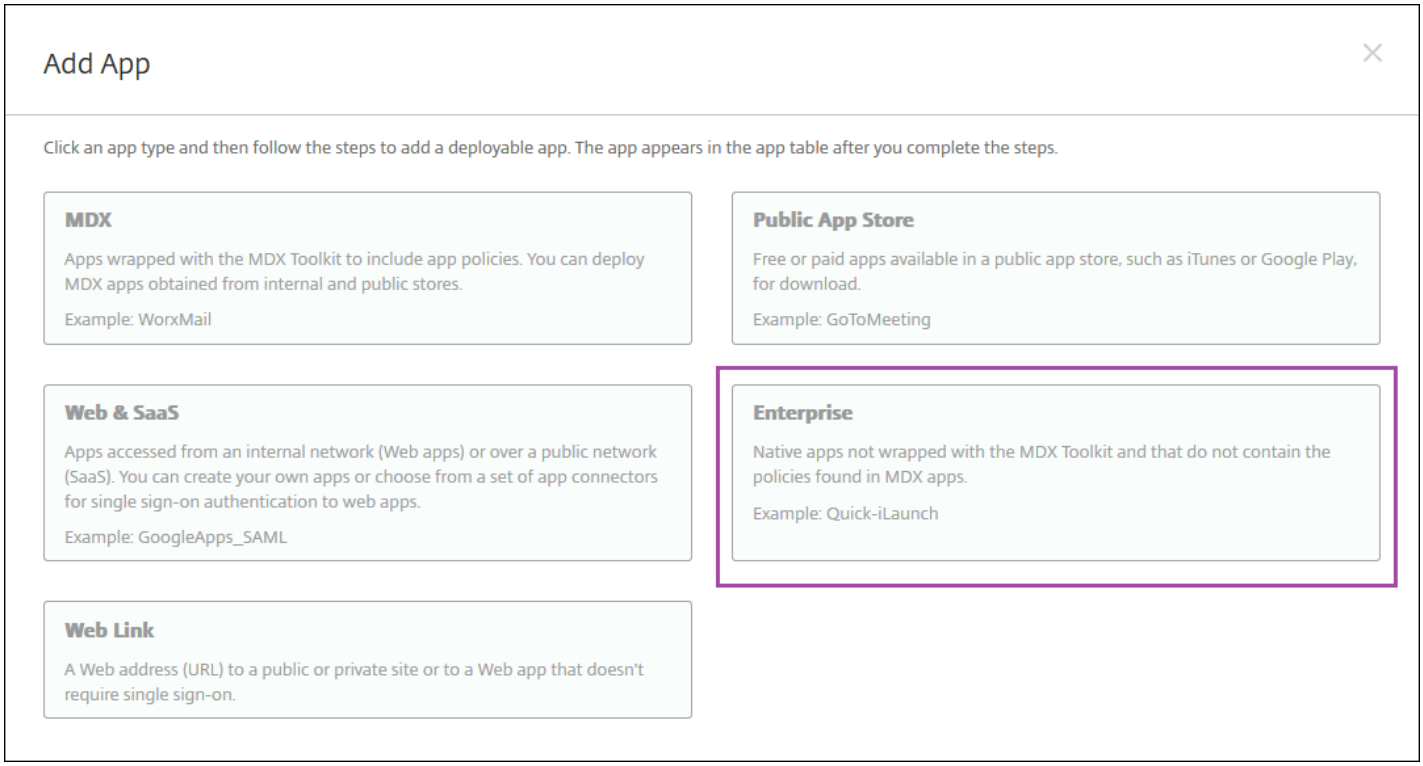
Pour fournir le Citrix Launcher aux appareils Android, suivez ces étapes.

1. Téléchargez l'application Citrix Launcher depuis la page des téléchargements de Citrix XenMobile pour votre édition de XenMobile. Le nom du fichier est CitrixLauncher.apk. Le fichier est prêt à être chargé dans XenMobile et ne nécessite pas de wrapping.

2. Ajoutez la stratégie d'appareil **Configuration du Launcher** : accédez à **Configurer > Stratégies d'appareil**, cliquez sur **Ajouter**, puis dans la boîte de dialogue **Ajouter une nouvelle stratégie**, commencez à taper **Launcher**. Pour de plus amples informations, consultez la section Stratégie de configuration du Launcher.

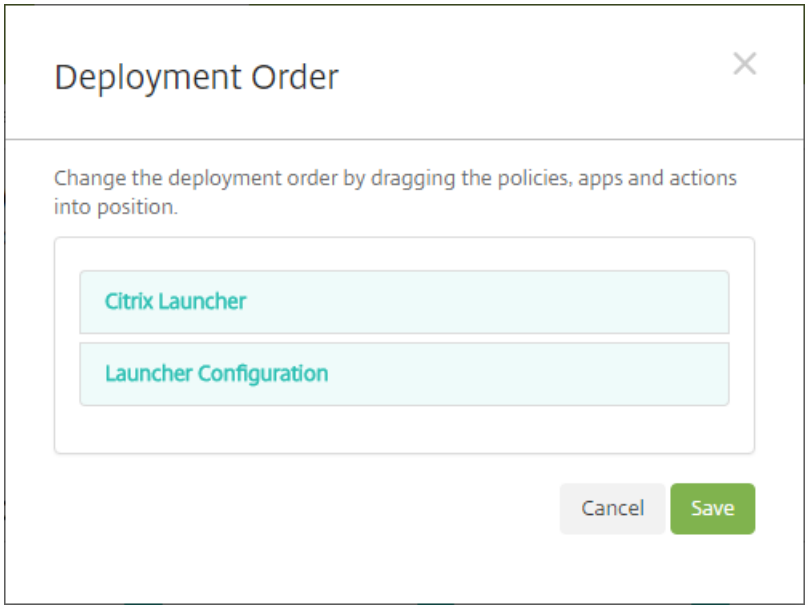


3. Ajoutez l'application Citrix Launcher à XenMobile en tant qu'application d'entreprise. Dans **Configurer > Applications**, cliquez sur **Ajouter**. Cliquez sur **Entreprise**. Pour de plus amples informations, consultez la section Ajouter une application d'entreprise.



4. Créez un groupe de mise à disposition pour Citrix Launcher avec la configuration suivante dans **Configurer > Groupes de mise à disposition** :

- Sur la page **Stratégies**, ajoutez la **Stratégie de configuration du Launcher**.
- Sur la page **Applications**, faites glisser **Citrix Launcher** vers **Applications requises**.
- Sur la page **Résumé**, cliquez sur **Ordre de déploiement** et assurez-vous que l'application **Citrix Launcher** précède la stratégie **Configuration du Launcher**.



Pour de plus amples informations, consultez la section Déployer des ressources.

Programme d'achat en volume iOS

Feb 23, 2017

Vous pouvez gérer les licences applicatives iOS à l'aide du Programme d'achat en volume d'Apple (VPP), une solution simple et évolutive destinée à gérer les besoins de votre organisation en matière de contenu. Le programme VPP simplifie la recherche, l'achat et la distribution d'applications et d'autres données en bloc pour une organisation.

Avec VPP, vous pouvez utiliser XenMobile pour distribuer des applications, y compris des applications XenMobile et d'autres applications MDX, directement sur vos appareils ou attribuer du contenu auprès de vos utilisateurs à l'aide de codes de téléchargement. Vous configurez des paramètres spécifiques au Programme d'achat en volume iOS (VPP) dans XenMobile.

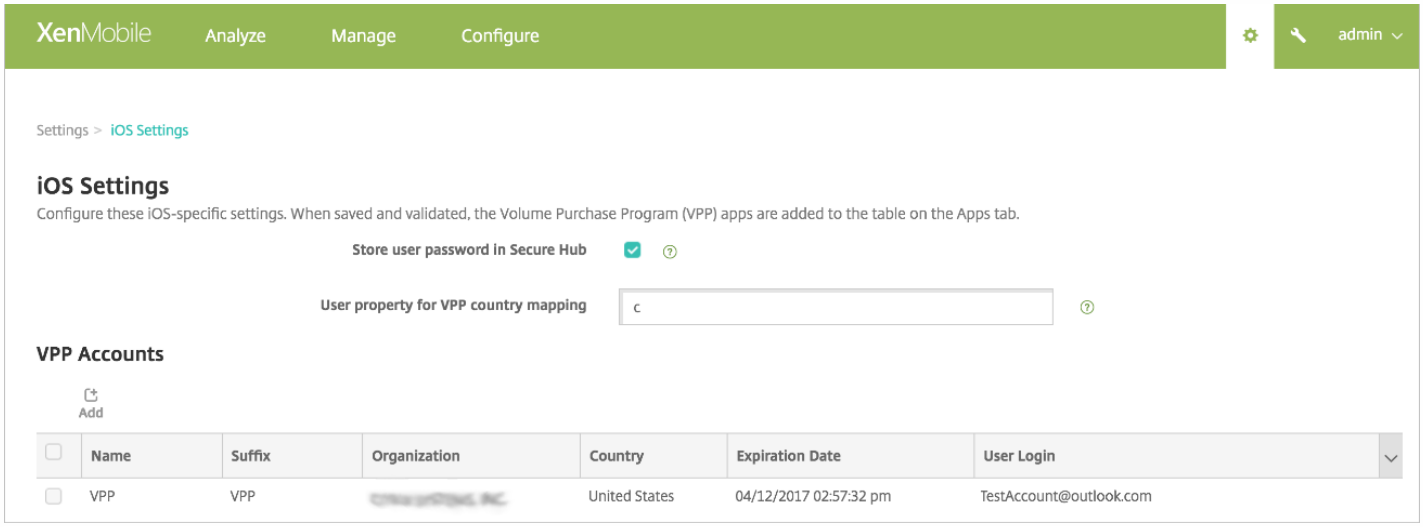
Cet article se concentre sur l'utilisation du programme VPP avec des licences gérées, ce qui vous permet d'utiliser XenMobile pour distribuer des applications. Si vous utilisez actuellement des codes de téléchargement et que vous souhaitez changer au profit d'une distribution gérée, consultez le document de support Apple, Passage du système de codes de téléchargement au système de distribution gérée, dans le cadre du programme d'achat en volume.

Pour plus d'informations sur le programme d'achat en volume iOS, consultez le site http://www.apple.com/business/vpp/. Pour vous inscrire auprès du programme VPP, accédez à https://deploy.apple.com/qforms/open/register/index/avs. Pour accéder à votre magasin VPP dans iTunes, accédez à https://vpp.itunes.apple.com/?l=en.

Après avoir enregistré et validé les paramètres VPP iOS dans XenMobile, les applications achetées sont ajoutées au tableau de la page **Configurer > Applications** dans la console XenMobile.

1. Dans la console Web de XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Sous **Plate-forme**, cliquez sur **Paramètres iOS**. La page de configuration **Paramètres iOS** s'affiche.



3. Pour configurer ces paramètres :

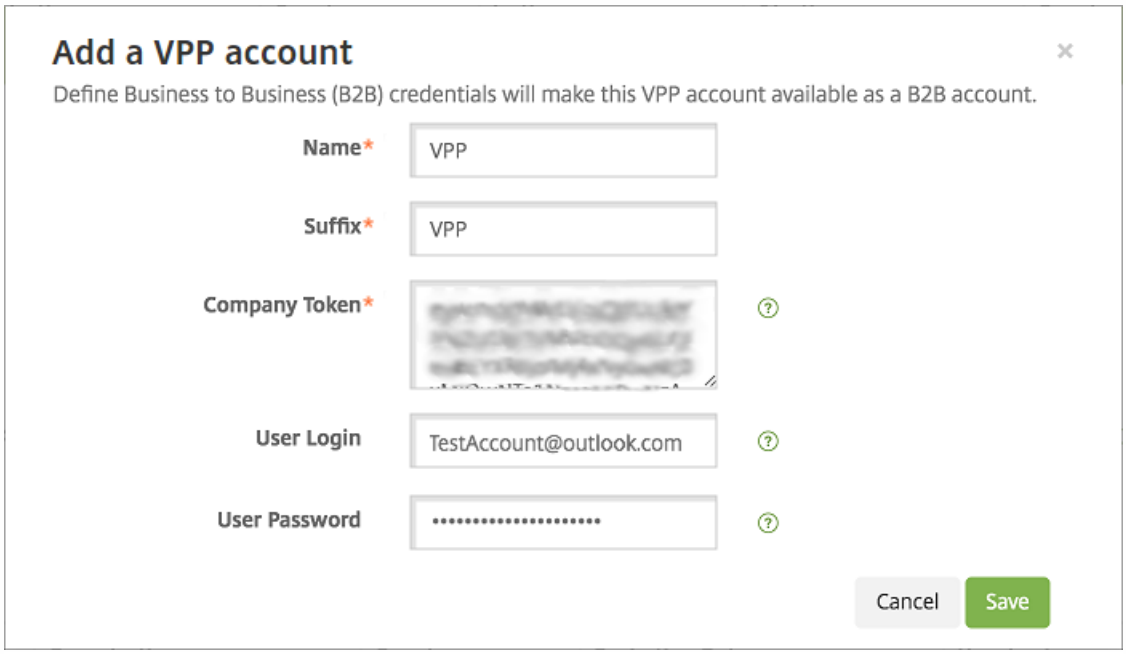
- **Stocker le mot de passe utilisateur dans Secure Hub** : indiquez si un nom d'utilisateur et un mot de passe doivent être stockés dans Secure Hub en vue de l'authentification sur XenMobile. La valeur par défaut est de stocker les informations à l'aide de cette méthode sécurisée.

- **Propriété utilisateur pour le choix du pays VPP** : entrez un code pour autoriser les utilisateurs à télécharger des applications à partir de magasins d'applications spécifiques à un pays.

    XenMobile utilise ce mappage pour choisir le pool de propriété du code VPP. Par exemple, si la propriété de l'utilisateur est États-Unis, l'utilisateur ne peut pas télécharger d'applications si le code VPP de l'application est pour le Royaume-Uni. Contactez votre administrateur de plan VPP pour plus d'informations sur le choix du code de pays.

Comptes VPP

- Pour chaque compte VPP que vous souhaitez ajouter, cliquez sur **Ajouter**. La boîte de dialogue **Ajouter un compte VPP** apparaît.



Configurez ces paramètres pour chaque compte à ajouter :

Remarque : si vous utilisez Apple Configurator 1, chargez un fichier de licences comme suit : accédez à **Configurer > Applications**, accédez à une page de plate-forme et développez **Programme d'achat en volume**.

- **Nom** : entrez le nom du compte VPP.
- **Suffixe** : entrez le suffixe qui s'affiche avec les noms des applications obtenues via le compte VPP. Par exemple, si vous entrez **VPP**, l'application Secure Mail s'affiche dans la liste des applications en tant que **Secure Mail - VPP**.
- **Jeton d'entreprise** : copiez et collez le jeton de service VPP obtenu auprès de Apple. Pour obtenir le jeton, dans la page de **résumé** de compte du portail Apple VPP, cliquez sur le bouton **Télécharger** pour générer et télécharger le fichier VPP. Le fichier contient le jeton de service, ainsi que d'autres informations telles que le code de pays et l'expiration. Enregistrez le fichier dans un emplacement sécurisé.
- **Connexion utilisateur** : entrez un nom d'administrateur de compte VPP autorisé facultatif utilisé pour importer des applications B2B personnalisées.
- **Mot de passe utilisateur** : entrez le mot de passe d'administrateur du compte VPP.

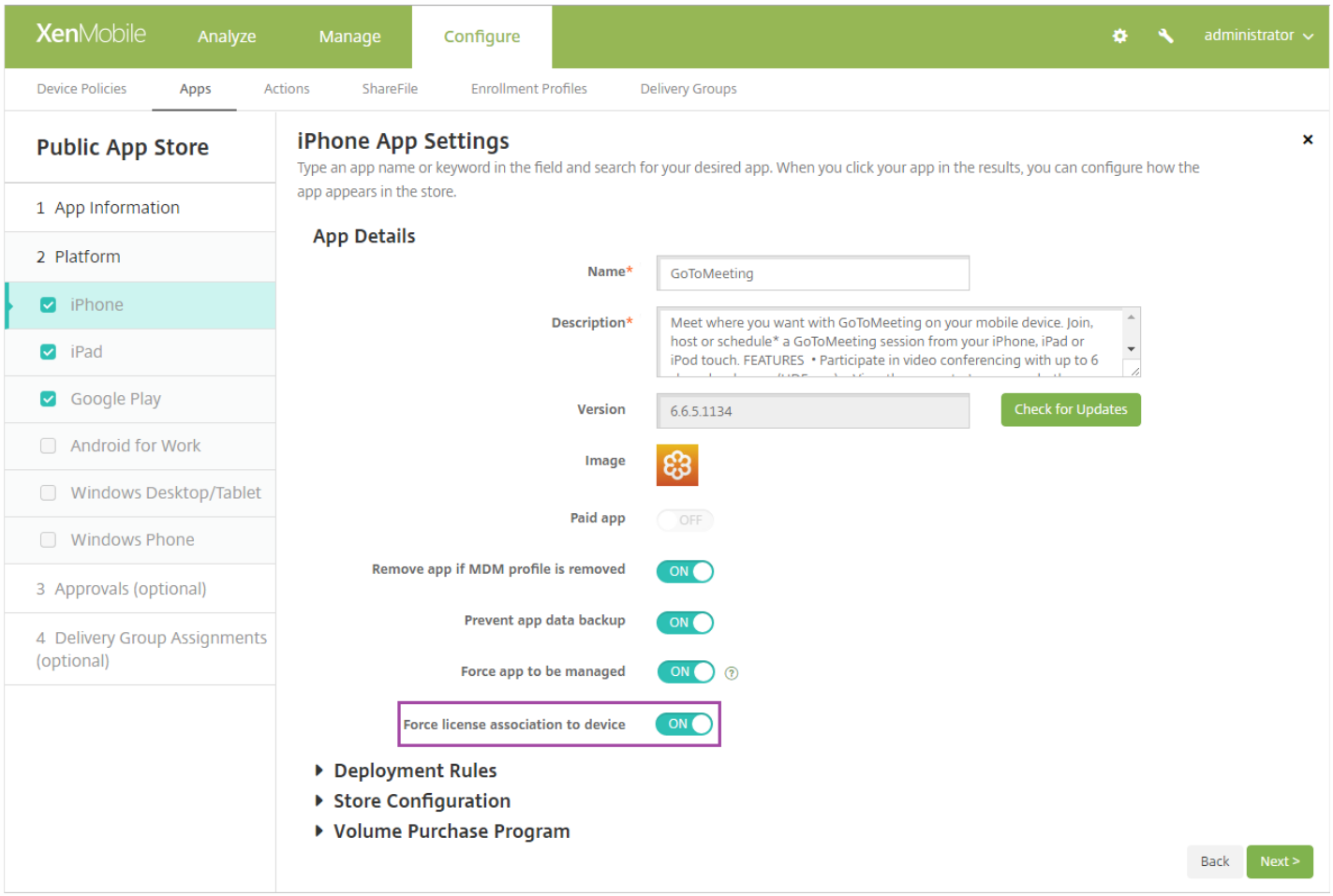
5. Cliquez sur **Enregistrer** pour fermer la boîte de dialogue.

6. Cliquez sur **Enregistrer** pour enregistrer les paramètres iOS.

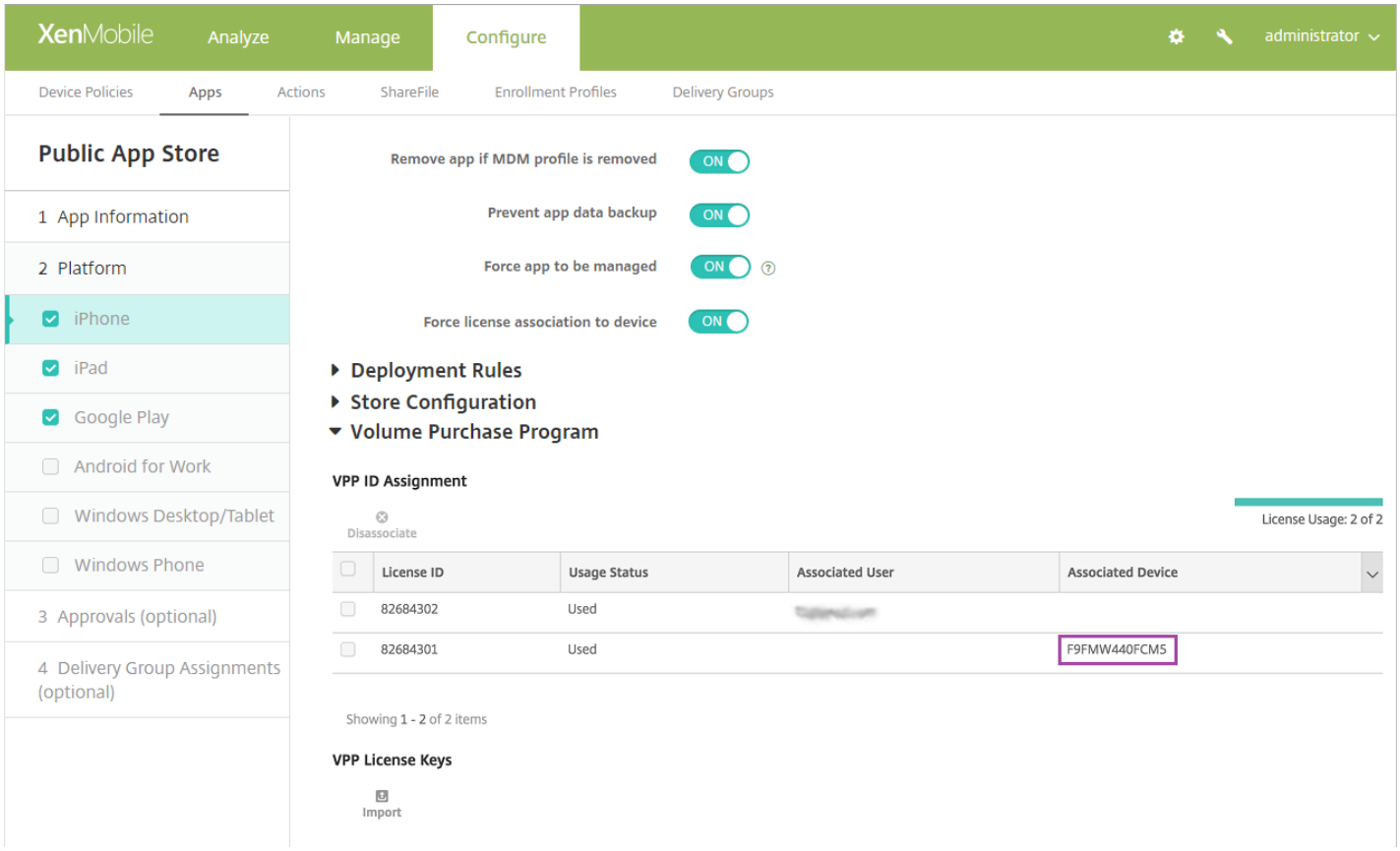
Un message s'affiche pour vous informer que XenMobile va ajouter des applications à la liste sur la page **Configurer > Applications**. Sur la page **Configurer > Applications** page, notez que le nom des applications collectées depuis votre compte VPP inclut le suffixe que vous avez spécifié dans la configuration ci-dessus.

Vous pouvez maintenant configurer les paramètres d'application VPP puis ajuster les paramètres de votre groupe mise à disposition et de vos stratégies pour les applications VPP. Une fois que vous avez terminé ces configurations, les utilisateurs peuvent inscrire leurs appareils. Les remarques suivantes fournissent des informations sur ces processus.

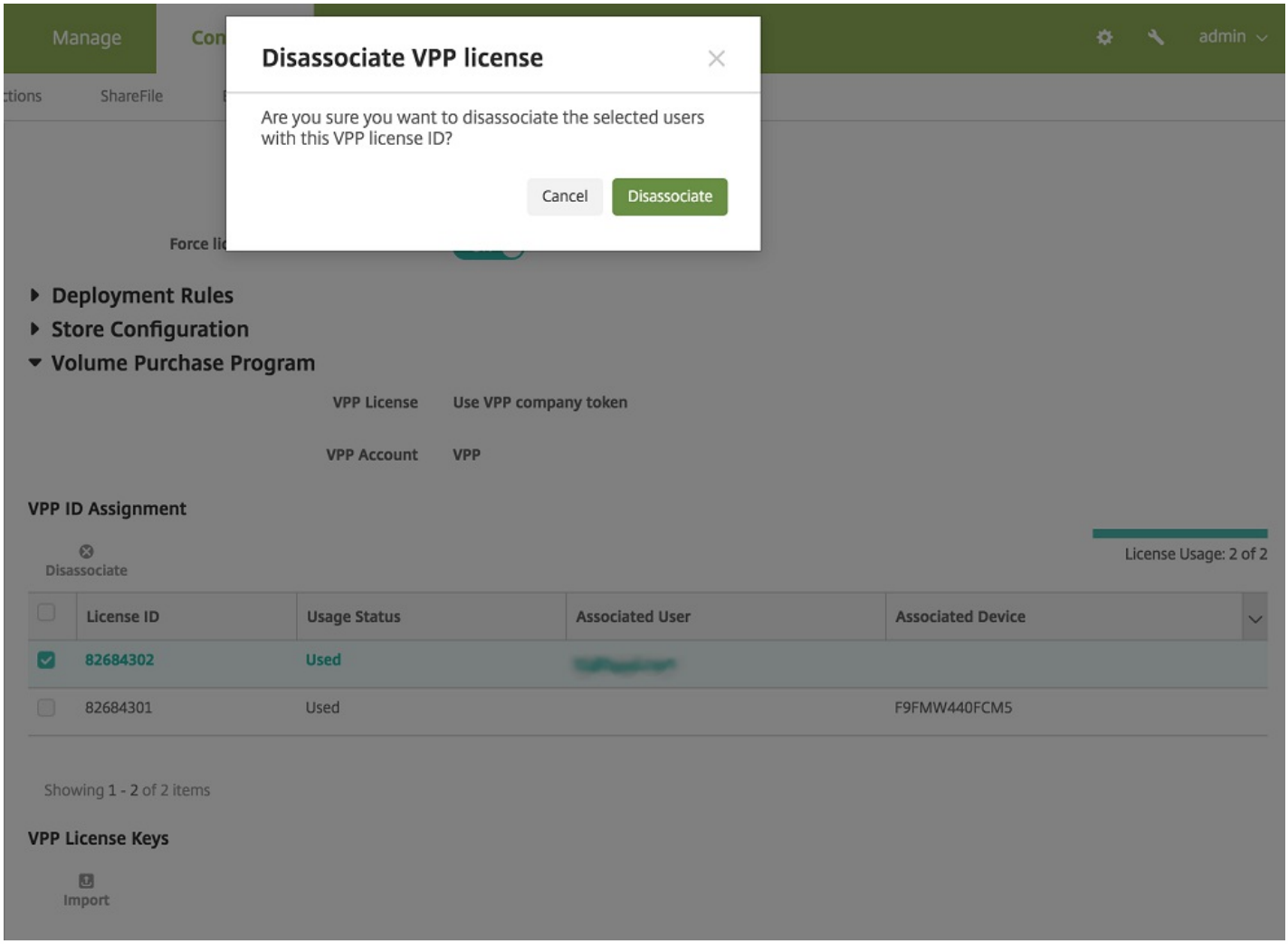
- Lors de la configuration des paramètres applicatifs VPP (**Configurer > Applications**), activez **Forcer l'association de licence avec l'appareil**. L'un des avantages des programmes Apple VPP et DEP avec des appareils supervisés est la possibilité d'utiliser XenMobile pour attribuer l'application au niveau de l'appareil (plutôt qu'au niveau de l'utilisateur). Par conséquent, vous n'avez pas besoin d'utiliser un appareil Apple ID, les utilisateurs ne reçoivent pas de message les invitant à rejoindre le programme VPP et les utilisateurs peuvent télécharger les applications sans se connecter à leur compte iTunes.



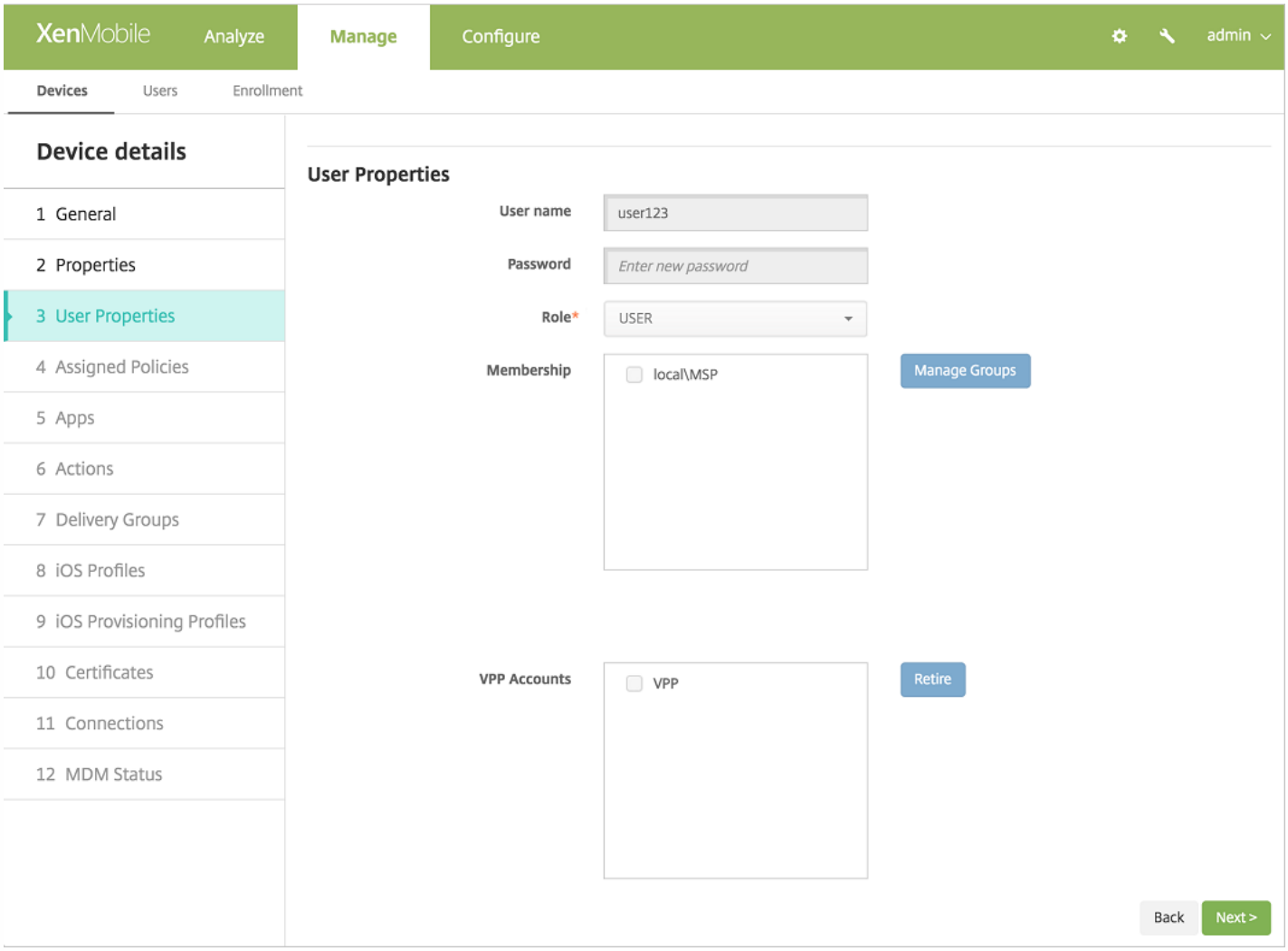
Pour afficher les informations du programme VPP pour cette application, développez **Programme d'achat en volume**. Veuillez noter que dans le tableau **Attribution de l'IP VPP**, la licence est associée à un appareil. Le numéro de série de l'appareil s'affiche dans la colonne **Appareil associé**. Si l'utilisateur supprime le jeton, puis l'importe à nouveau, le mot **Masqué** s'affiche au lieu du numéro de série, en raison de restrictions de confidentialité d'Apple.



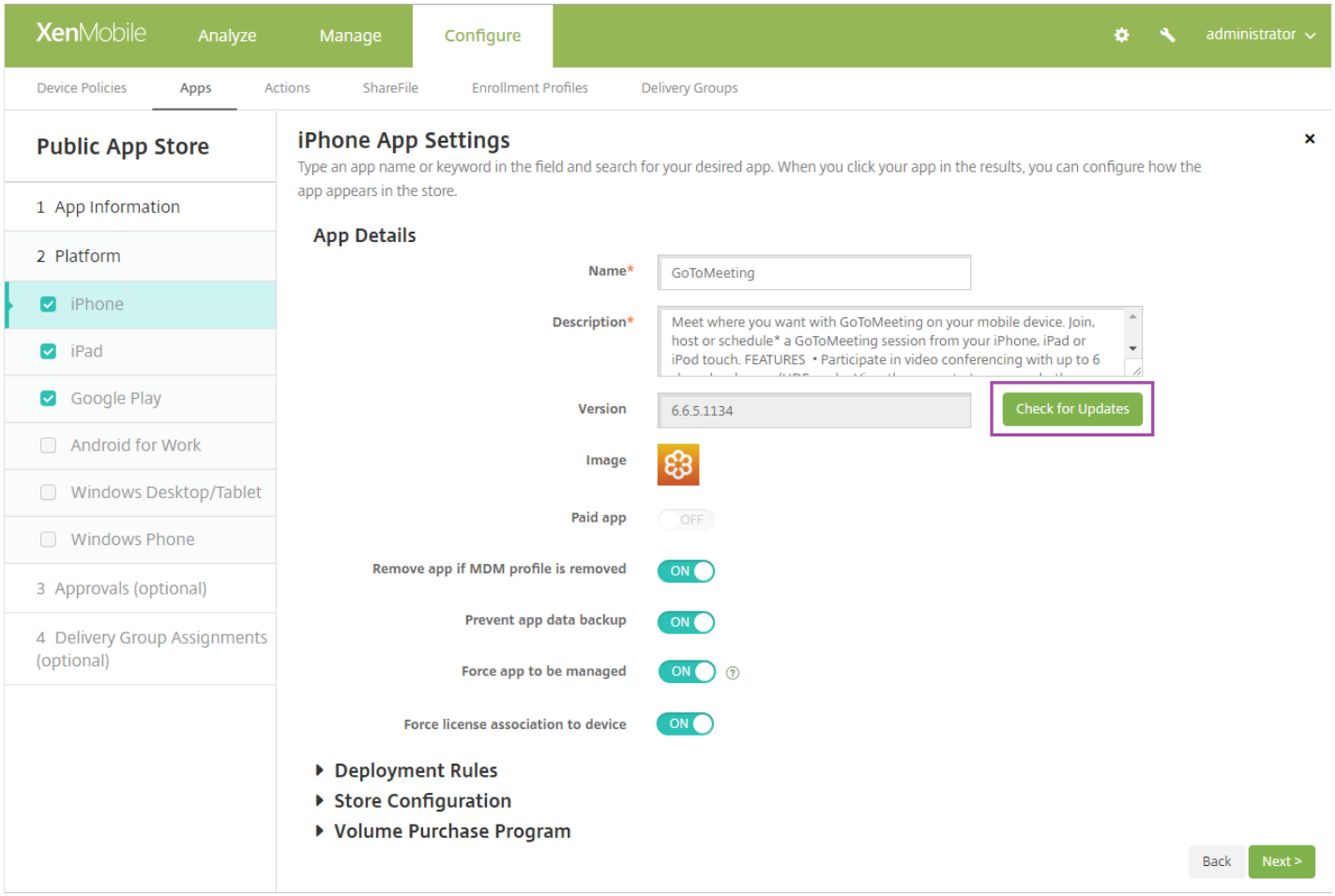
Pour dissocier une licence, cliquez sur la ligne en regard de la licence et cliquez sur **Dissocier**.



Si vous associez des licences VPP à des utilisateurs, XenMobile intègre les utilisateurs à votre compte VPP et associe leur ID iTunes avec le compte VPP. L'ID iTunes des utilisateurs n'est pas visible par votre entreprise ou le serveur XenMobile. Apple crée l'association de manière à protéger la confidentialité des utilisateurs. Vous pouvez retirez un utilisateur du programme VPP afin de dissocier toutes les licences du compte utilisateur. Pour retirer un utilisateur, accédez à **Gérer > Appareils**.



- Lorsque vous attribuez une application à un groupe de mise à disposition, XenMobile identifie par défaut l'application en tant qu'application facultative. Pour vous assurer que XenMobile déploie une application sur les appareils, accédez à **Configurer > Groupes de mise à disposition** et, sur la page **Applications**, déplacez l'application sur la liste **Applications requises**.
- Lorsqu'une mise à jour est disponible pour l'application d'un magasin d'applications public, et que cette application est transmise via le programme VPP, l'application ne se met pas à jour automatiquement sur les appareils. Vous devez rechercher les mises à jour et les appliquer. Par exemple, pour distribuer une mise à jour de Secure Hub (si elle est attribuée à un appareil et non un utilisateur), dans **Configurer > Applications**, sur une page de plate-forme, cliquez sur **Rechercher les mises à jour** et appliquez la mise à jour.



XenApp et XenDesktop via Citrix Secure Hub

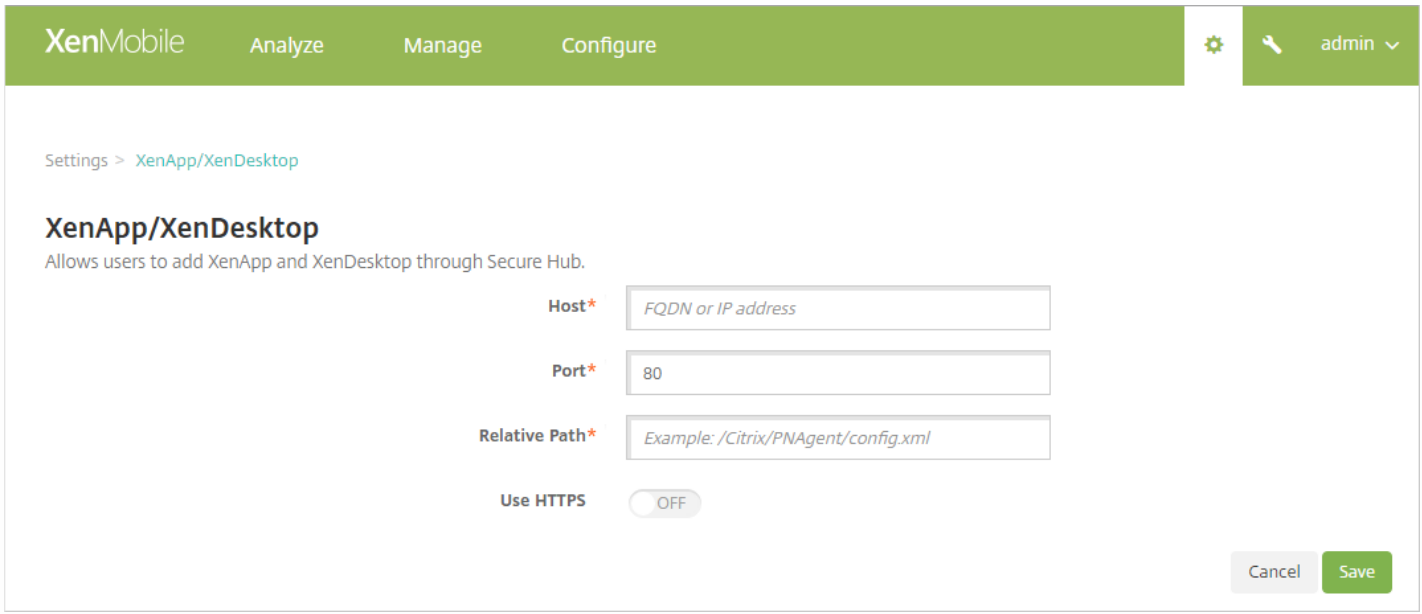
Feb 23, 2017

XenMobile peut collecter des applications depuis XenApp et XenDesktop et les rendre disponibles aux utilisateurs d'appareils mobiles dans XenMobile Store. Les utilisateurs s'abonnent directement aux applications dans XenMobile Store et les lancent depuis Secure Hub. Citrix Receiver doit être installé sur les appareils des utilisateurs pour lancer des applications, mais n'a pas besoin d'être configuré.

Pour configurer ce paramètre, vous devez connaître le nom de domaine complet (FQDN) ou l'adresse IP et le numéro de port du site Interface Web ou StoreFront.

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **XenApp/XenDesktop**. La page **XenApp/XenDesktop** s'affiche.



3. Configurez les paramètres suivants :

- **Hôte** : entrez le nom de domaine complet (FQDN) ou l'adresse IP pour StoreFront ou le site Interface Web.
- **Port** : entrez le numéro de port pour StoreFront ou le site Interface Web. La valeur par défaut est 80.
- **Chemin relatif** : entrez le chemin d'accès. Par exemple, /Citrix/PNAgent/config.xml
- **Utiliser HTTPS**: sélectionnez cette option si vous souhaitez activer l'authentification sécurisée entre le site Interface Web ou StoreFront et l'appareil client. La valeur par défaut est **OFF**.

4. Cliquez sur **Enregistrer**.

Déployer des ressources

Feb 23, 2017

La gestion et la configuration d'appareils impliquent généralement la création de ressources (stratégies et applications) et d'actions dans la console XenMobile, puis le packaging de ces dernières à l'aide de groupes de mise à disposition. L'ordre dans lequel XenMobile transmet les ressources et les actions dans un groupe de mise à disposition aux appareils est appelé *ordre de déploiement*. Cet article explique comment ajouter, gérer et déployer des groupes de mise à disposition, comment changer l'ordre de déploiement des ressources et des actions dans les groupes de mise à disposition, et la façon dont XenMobile détermine l'ordre de déploiement lorsqu'un utilisateur figure dans plusieurs groupes de mise à disposition qui comportent des stratégies conflictuelles ou en double.

Les groupes de mise à disposition définissent la catégorie d'utilisateurs pour lesquels vous déployez des combinaisons de stratégies, d'applications et d'actions. L'inclusion dans un groupe de mise à disposition est basée sur les caractéristiques des utilisateurs, telles que l'entreprise, le pays, le département, l'adresse, la fonction, etc. Les groupes de mise à disposition vous permettent de mieux contrôler les personnes qui reçoivent les ressources et à quel moment. Vous pouvez déployer un groupe de mise à disposition à tout le monde ou à un groupe d'utilisateurs défini de manière plus précise.

Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils iOS, Windows Phone et Windows Tablet qui appartiennent au groupe de mise à disposition les invitant à se reconnecter à XenMobile, ce qui permet de réévaluer les appareils et de déployer des applications, des stratégies et des actions ; les utilisateurs équipés d'autres plates-formes reçoivent les ressources immédiatement s'ils sont déjà connectés, ou en fonction de leur stratégie de planification, la prochaine fois qu'ils se connectent.

Le groupe de mise à disposition par défaut AllUsers est créé lorsque vous installez et configurez XenMobile. Il contient à tous les utilisateurs locaux et utilisateurs Active Directory. Vous ne pouvez pas supprimer le groupe AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs.

Ordre de déploiement

L'ordre de déploiement est la séquence dans laquelle XenMobile transmet les ressources aux appareils. La fonctionnalité d'ordre de déploiement est uniquement prise en charge avec le mode MDM.

Pour déterminer l'ordre de déploiement, XenMobile applique des filtres et des critères de contrôle, tels que des règles de déploiement et un calendrier de déploiement, aux stratégies, applications, actions et groupes de mise à disposition. Avant d'ajouter des groupes de mise à disposition, considérez la façon dont les informations de cette section se rapportent à vos objectifs de déploiement.

Voici un résumé des concepts principaux liés à l'ordre de déploiement :

- **Ordre de déploiement** : séquence dans laquelle XenMobile transmet les ressources (stratégies et applications) et actions à un appareil. L'ordre de déploiement de certaines stratégies, telles que les termes et conditions et l'inventaire logiciel, n'a aucun effet sur les autres ressources. L'ordre dans lequel les actions sont déployées n'a aucun effet sur les autres ressources, leur position est donc ignorée lorsque XenMobile déploie les ressources.
- **Règles de déploiement :** XenMobile utilise les règles de déploiement que vous spécifiez pour les propriétés d'appareil pour filtrer les stratégies, les applications, les actions et les groupes de mise à disposition. Par exemple, une règle de déploiement peut spécifier la distribution du paquetage de déploiement lorsqu'un nom de domaine correspond à une

valeur particulière.

- **Calendrier de déploiement :** XenMobile utilise le calendrier de déploiement que vous spécifiez pour les actions, les applications et les stratégies d'appareil pour contrôler le déploiement de ces éléments. Vous pouvez spécifier un déploiement immédiat, à une date et heure particulières, ou en fonction de conditions de déploiement.

Le tableau suivant présente ces conditions et d'autres critères que vous pouvez associer à des objets ou ressources spécifiques pour les filtrer ou contrôler leur déploiement.

Objet/Ressource	**Filtre/Critères de contrôle**
Stratégies d'appareil	La plate-forme de l'appareil Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
App	La plate-forme de l'appareil Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
Action	Règle de déploiement (basée sur les propriétés d'appareil) Une planification du déploiement
Groupe de mise à disposition	Utilisateur/ groupes Règle de déploiement (basée sur les propriétés d'appareil)

Il est très probable que dans un environnement standard, plusieurs groupes de mise à disposition soient attribués à un seul utilisateur, avec les résultats possibles suivants :

- Des objets dupliqués existent dans les groupes de mise à disposition.
- Une stratégie spécifique est configurée différemment dans plus d'un groupe de mise à disposition qui est attribué à un utilisateur.

Lorsque l'une de ces situations se produit, XenMobile calcule un ordre de déploiement pour tous les objets qu'il doit délivrer sur un appareil ou pour lesquels il doit intervenir. Les étapes de calcul sont indépendantes de la plate-forme de l'appareil.

Étapes de calcul :

1. Déterminez tous les groupes de mise à disposition d'un utilisateur spécifique, en fonction des filtres de groupes/d'utilisateurs et des règles de déploiement.
2. Créez une liste ordonnée de toutes les ressources (stratégies, actions et applications) dans les groupes de mise à disposition sélectionnés qui s'appliquent en fonction des filtres de la plate-forme de l'appareil, des règles de déploiement et du calendrier de déploiement. L'algorithme utilisé est le suivant :

a. Placez les ressources provenant des groupes de mise à disposition qui ont un ordre de déploiement défini par l'utilisateur avant celles ne disposant pas d'un ordre de déploiement. Le principe derrière ce raisonnement est décrit après ces étapes.

b. Pour départager les groupes de mise à disposition, classez les ressources provenant de groupes de mise à disposition par nom de groupe de mise à disposition. Par exemple, placez les ressources provenant du groupe de mise à disposition A avant celles provenant du groupe de mise à disposition B.

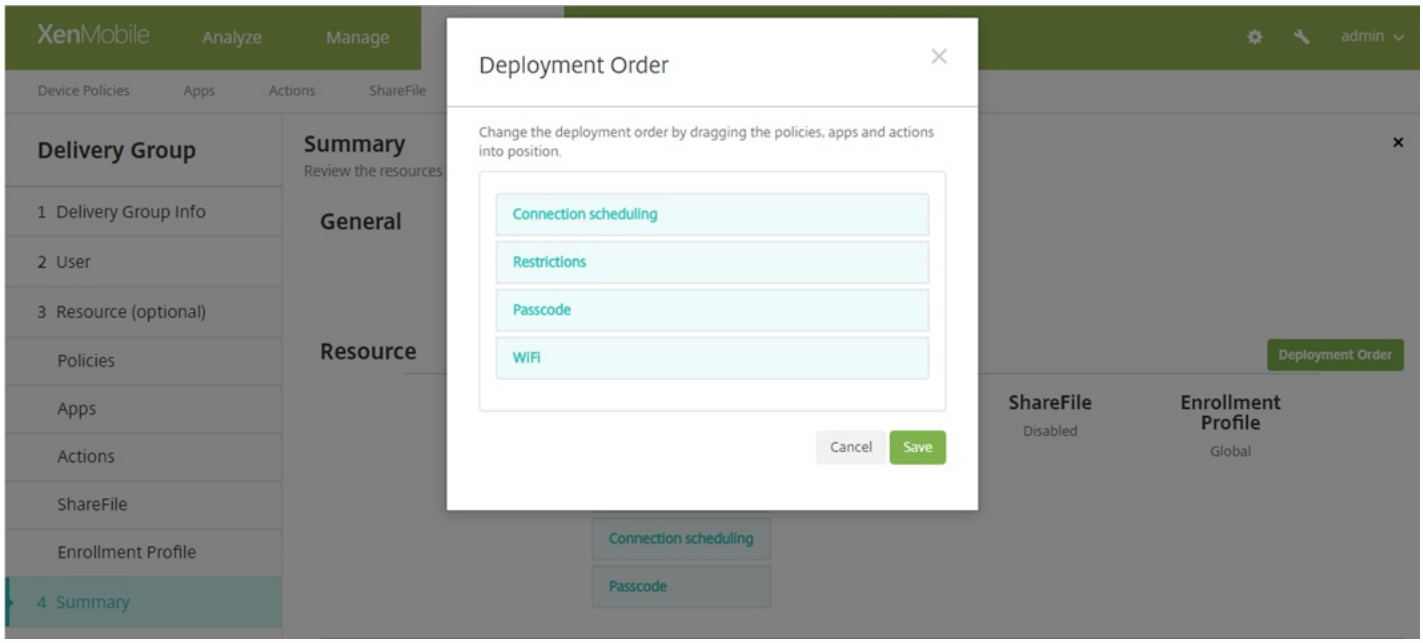
c. Tout en effectuant le tri, si un ordre de déploiement défini par un utilisateur est spécifié pour les ressources d'un groupe de mise à disposition, conservez cet ordre. Sinon, triez les ressources dans ce groupe de mise à disposition par nom de ressource.

d. Si la même ressource apparaît plus d'une fois, supprimez la ressource dupliquée.

Les ressources pour lesquelles un ordre a été défini par un utilisateur sont déployées avant les ressources pour lesquelles aucun ordre n'a été défini par un utilisateur. Une ressource peut exister dans plusieurs groupes de mise à disposition attribués à un utilisateur. Comme indiqué dans les étapes ci-dessus, l'algorithme de calcul supprime les ressources redondantes et met uniquement à disposition la première ressource de la liste. En supprimant les ressources en double de cette façon, XenMobile applique l'ordre défini par l'administrateur XenMobile.

Supposons par exemple que vous disposiez de deux groupes de mise à disposition comme suit :

- Groupe de mise à disposition, Gestionnaires de comptes 1: avec un ordre **non spécifié** pour les ressources ; contient les stratégies **Wi-Fi** et **Code secret**.
- Groupe de mise à disposition, Gestionnaires de comptes 2 : avec un ordre **spécifié** pour les ressources ; contient les stratégies **Planification de connexion**, **Restrictions**, **Code secret** et **Wi-Fi**. Dans ce cas, vous souhaitez mettre à disposition la stratégie **Code secret** avant la stratégie **Wi-Fi**.



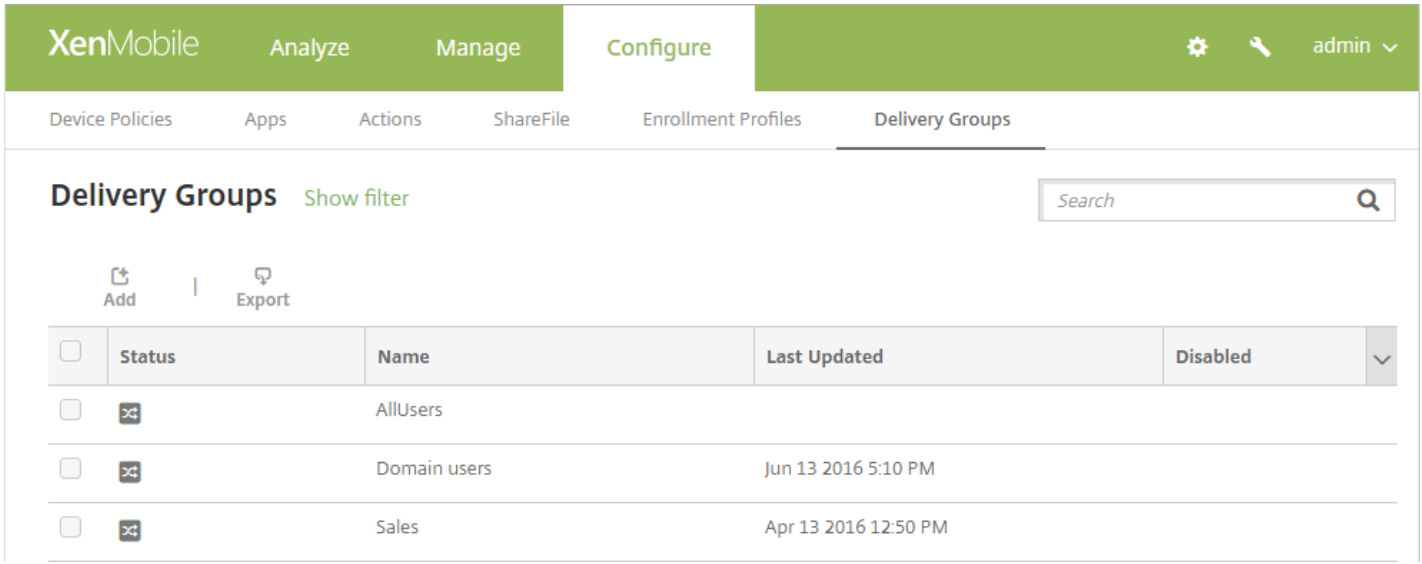
Si l'algorithme de calcul classait uniquement les groupes de déploiement par nom, XenMobile réaliserait le déploiement dans cet ordre, en commençant par le groupe de mise à disposition Gestionnaires de comptes 1 : **Wi-Fi**, **Code secret**, **Planification de connexion** et **Restrictions**. XenMobile ignorerait **Code secret** et **Wi-Fi**, des doublons du groupe de mise à

disposition Gestionnaires de comptes 2.

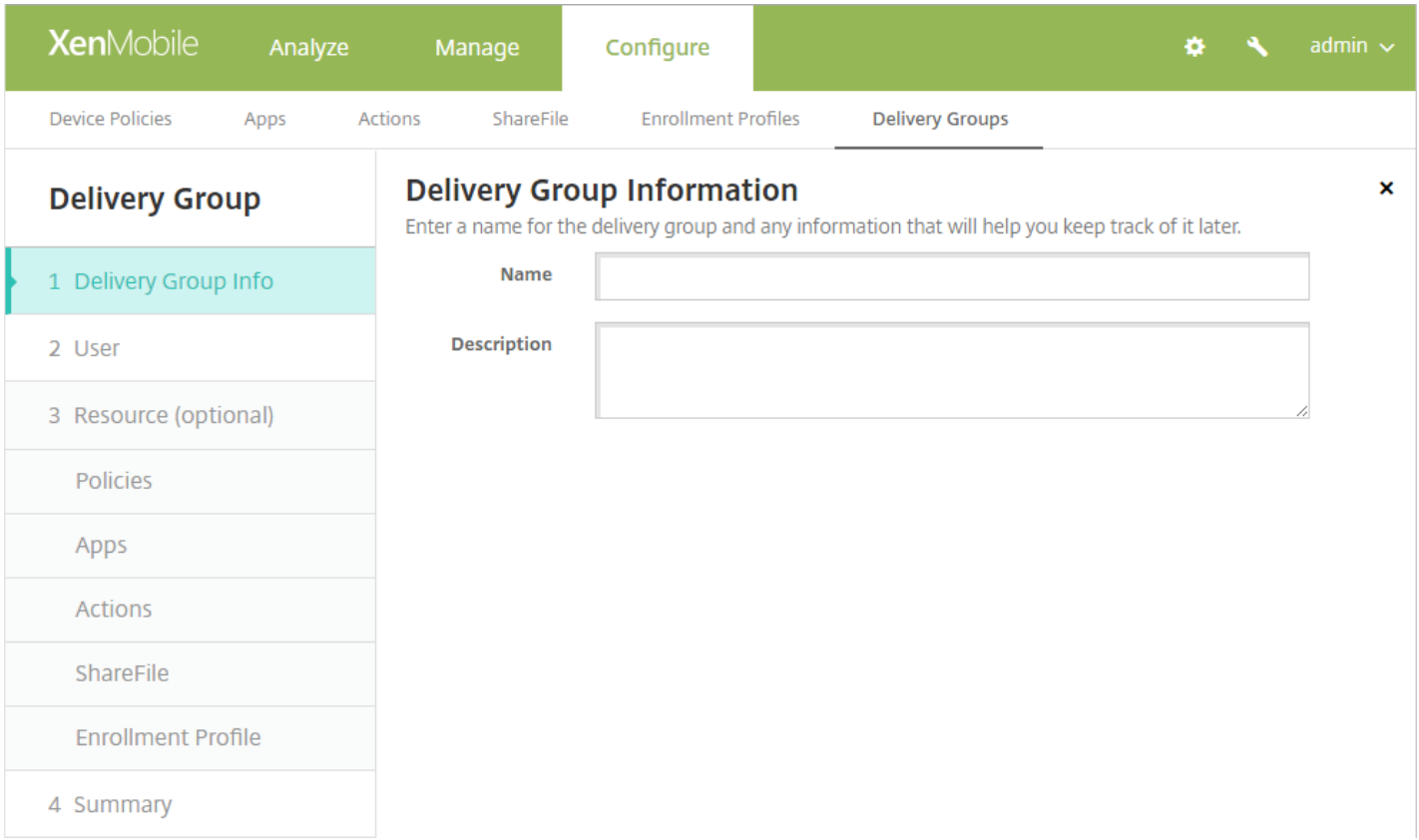
Toutefois, étant donné que l'ordre de déploiement du groupe Gestionnaires de comptes 2 a été spécifié par un administrateur, l'algorithme de calcul place les ressources du groupe de mise à disposition Gestionnaires de comptes 2 plus haut dans la liste que celles du groupe de mise à disposition Gestionnaires de comptes 1. Par conséquent, XenMobile déploie les stratégies dans cet ordre : **Planification de connexion**, **Restrictions**, **Code secret** et **Wi-Fi**. XenMobile ignore les stratégies **Wi-Fi** et **Code secret** du groupe de mise à disposition Gestionnaires de comptes 1, car elles sont dupliquées. Par conséquent, cet algorithme respecte l'ordre spécifié par l'administrateur XenMobile.

Pour ajouter un groupe de mise à disposition

1. Dans la console XenMobile, cliquez sur **Configurer > Groupes de mise à disposition**. La page **Groupes de mise à disposition** s'affiche.



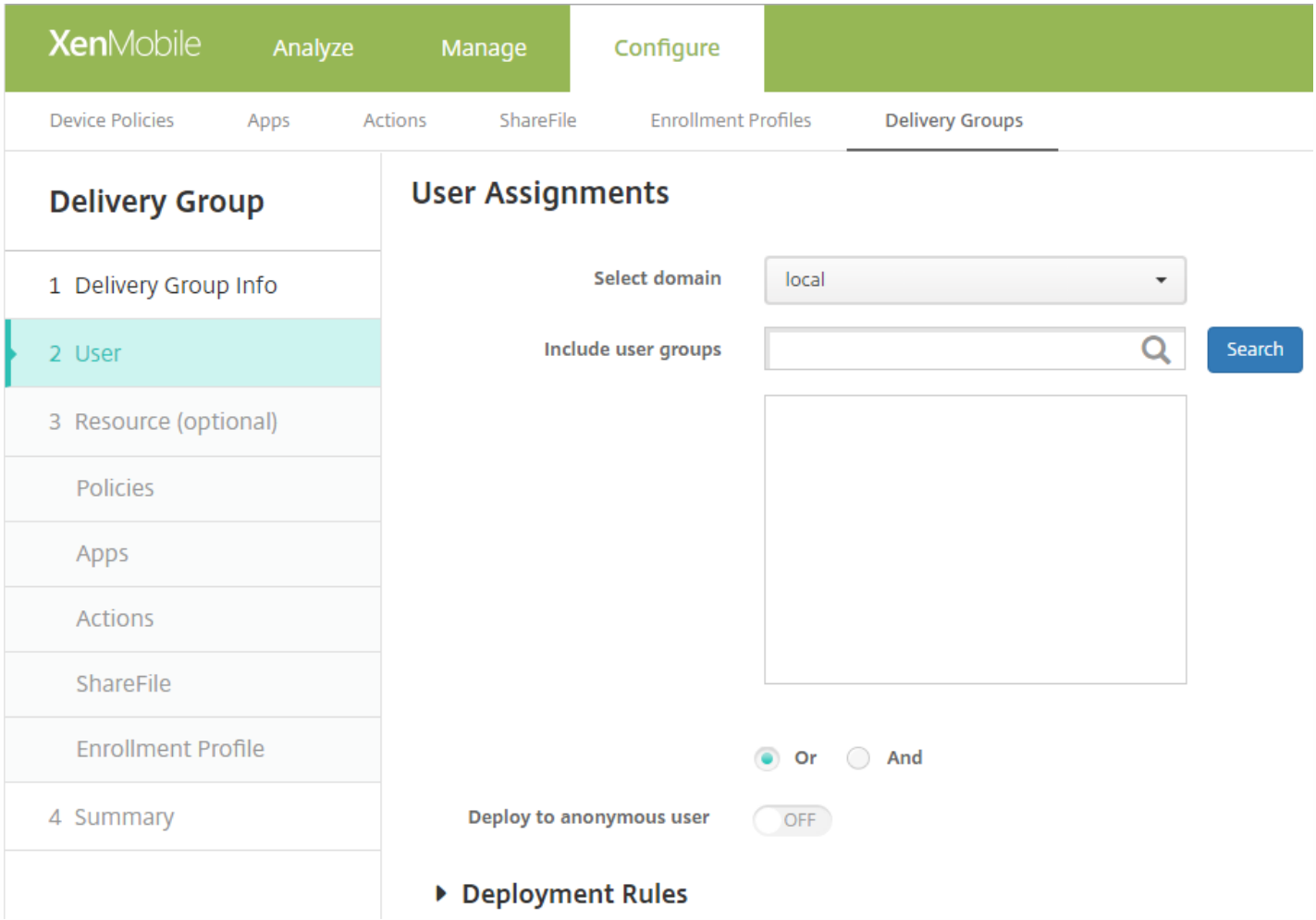
2. Sur la page **Groupes de mise à disposition**, cliquez sur **Ajouter**. La page **Informations sur le groupe de mise à disposition** s'affiche.



3. Sur la page **Informations sur le groupe de mise à disposition**, entrez les informations suivantes :

- **Nom** : entrez un nom descriptif pour le groupe de mise à disposition.
- **Description** : entrez une description pour le groupe de mise à disposition (facultatif).

4. Cliquez sur **Suivant**. La page **Attributions utilisateur** apparaît.



5. Configurez les paramètres suivants :

- **Sélectionner un domaine** : sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.
- **Inclure des groupes d'utilisateurs** : effectuez l'une des opérations suivantes :
  - Dans la liste des groupes d'utilisateurs, cliquez sur les groupes que vous souhaitez ajouter. Les groupes sélectionnés s'affichent dans la liste **Groupes d'utilisateurs sélectionnés**.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné.
  - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs.
    - Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, effectuez l'une des opérations suivantes :
      - Dans la liste **Groupes d'utilisateurs sélectionnés**, cliquez sur le **X** en regard de chaque groupe que vous souhaitez supprimer.
      - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.
      - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.
- **Ou/Et** : sélectionnez cette option pour spécifier si les utilisateurs peuvent appartenir à n'importe quel groupe (Ou) ou s'ils doivent figurer dans tous les groupes (Et) pour que la ressource puisse leur être déployée.

- **Déployer auprès d'un utilisateur anonyme** : sélectionnez cette option si vous voulez déployer auprès d'utilisateurs non authentifiés dans le groupe de mise à disposition.

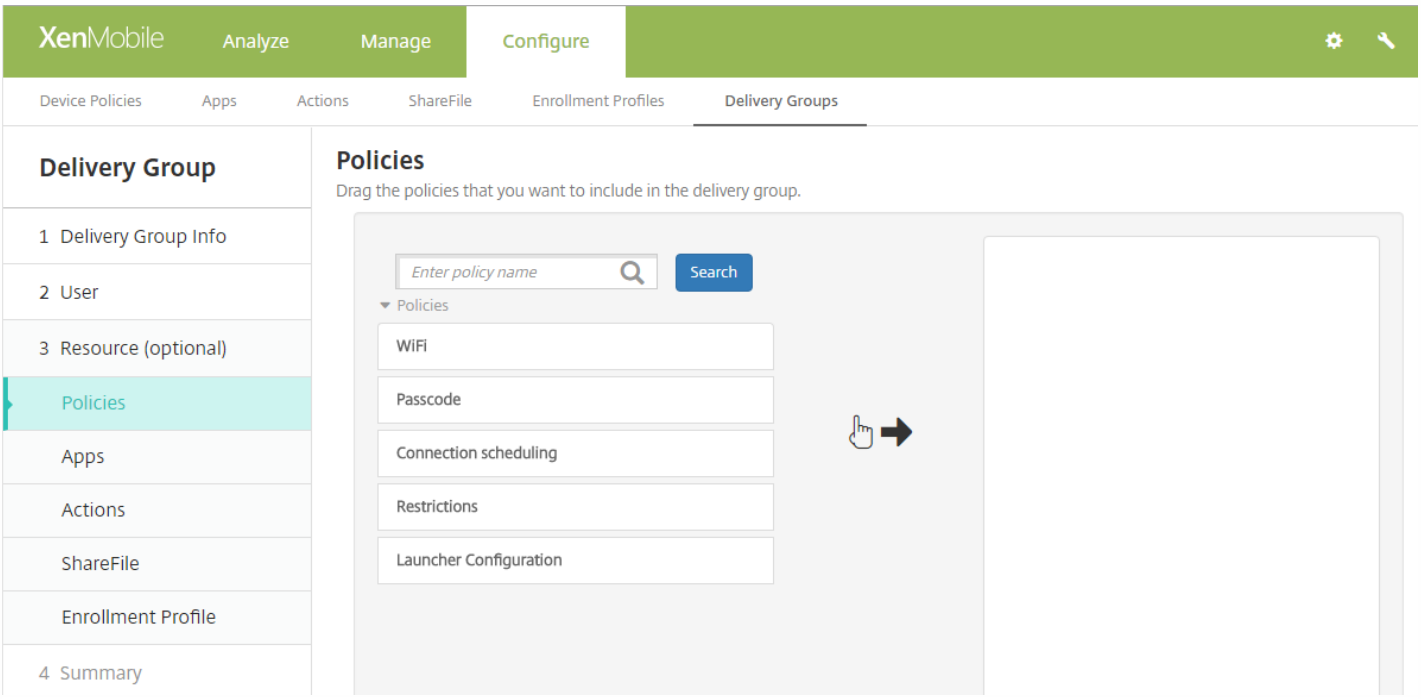
  Remarque : les utilisateurs non authentifiés sont des utilisateurs que vous n'avez pas réussi à authentifier, mais dont les appareils sont autorisés à se connecter à XenMobile.

6. Configurez les règles de déploiement.

Pour ajouter des ressources supplémentaires pour les groupes de mise à disposition

Vous pouvez ajouter des ressources supplémentaires pour les groupes de mise à disposition pour appliquer des stratégies spécifiques, fournir les applications obligatoires et facultatives, ajouter des actions automatiques et activer ShareFile pour l'authentification unique pour le contenu et les données. Les sections suivantes décrivent comment ajouter des stratégies, des applications et des actions et comment activer ShareFile. Vous pouvez ajouter n'importe quelle de ces ressources, toutes ou aucune pour le groupe de mise à disposition. Pour ne pas ajouter de ressource, cliquez sur **Résumé**.

Ajouter des stratégies



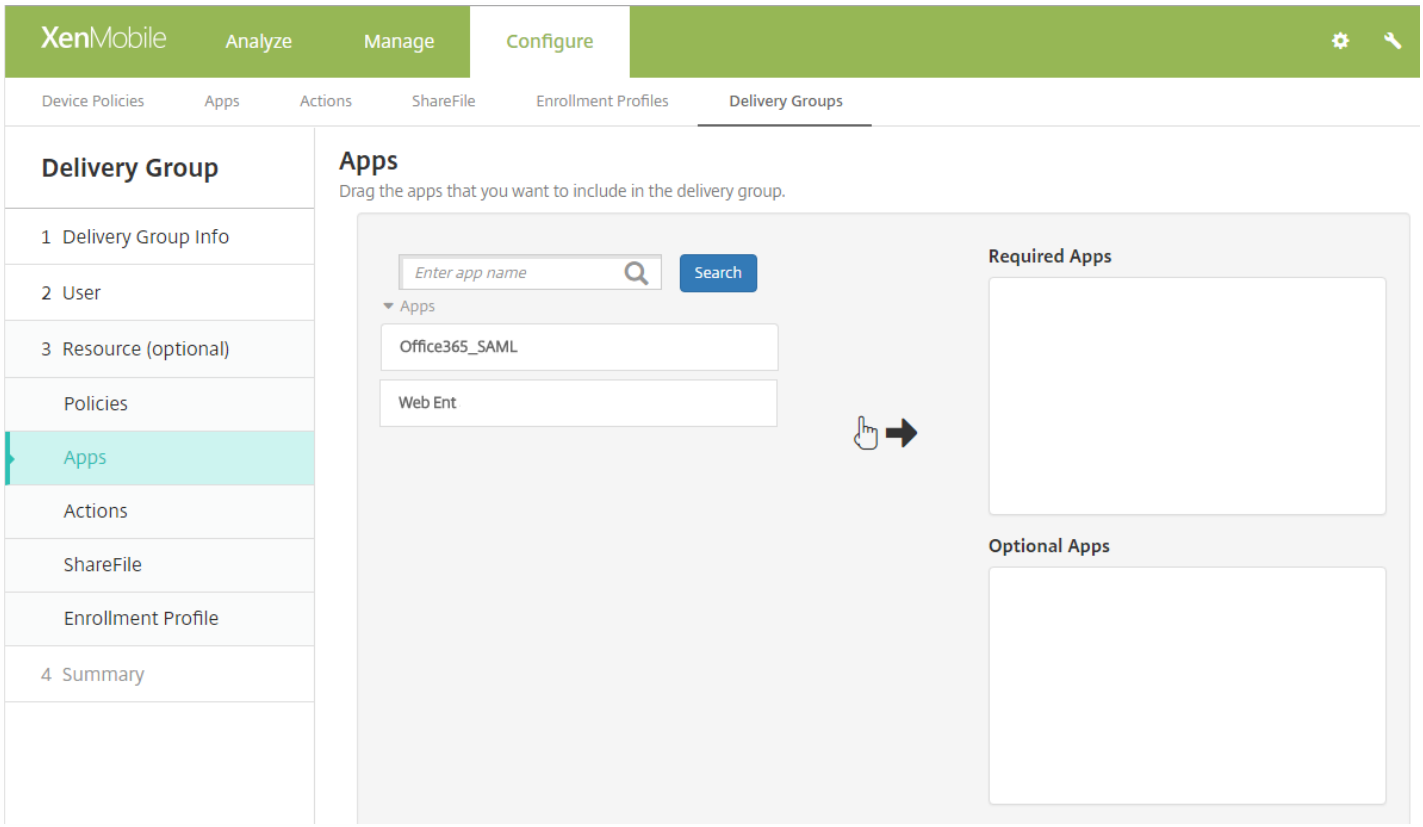
1. Pour chaque stratégie que vous voulez ajouter, procédez comme suit :

- Parcourez la liste des stratégies disponibles pour trouver la stratégie que vous souhaitez ajouter.
- Ou pour limiter la liste des stratégies, entrez un nom de stratégie complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
- Cliquez sur la stratégie que vous souhaitez ajouter et faites-la glisser dans la zone de droite.

Remarque : pour supprimer une stratégie, cliquez sur le **X** en regard du nom de la stratégie dans la zone de droite.

2. Cliquez sur **Next**. La page **Applications** s'affiche.

Ajouter des applications.



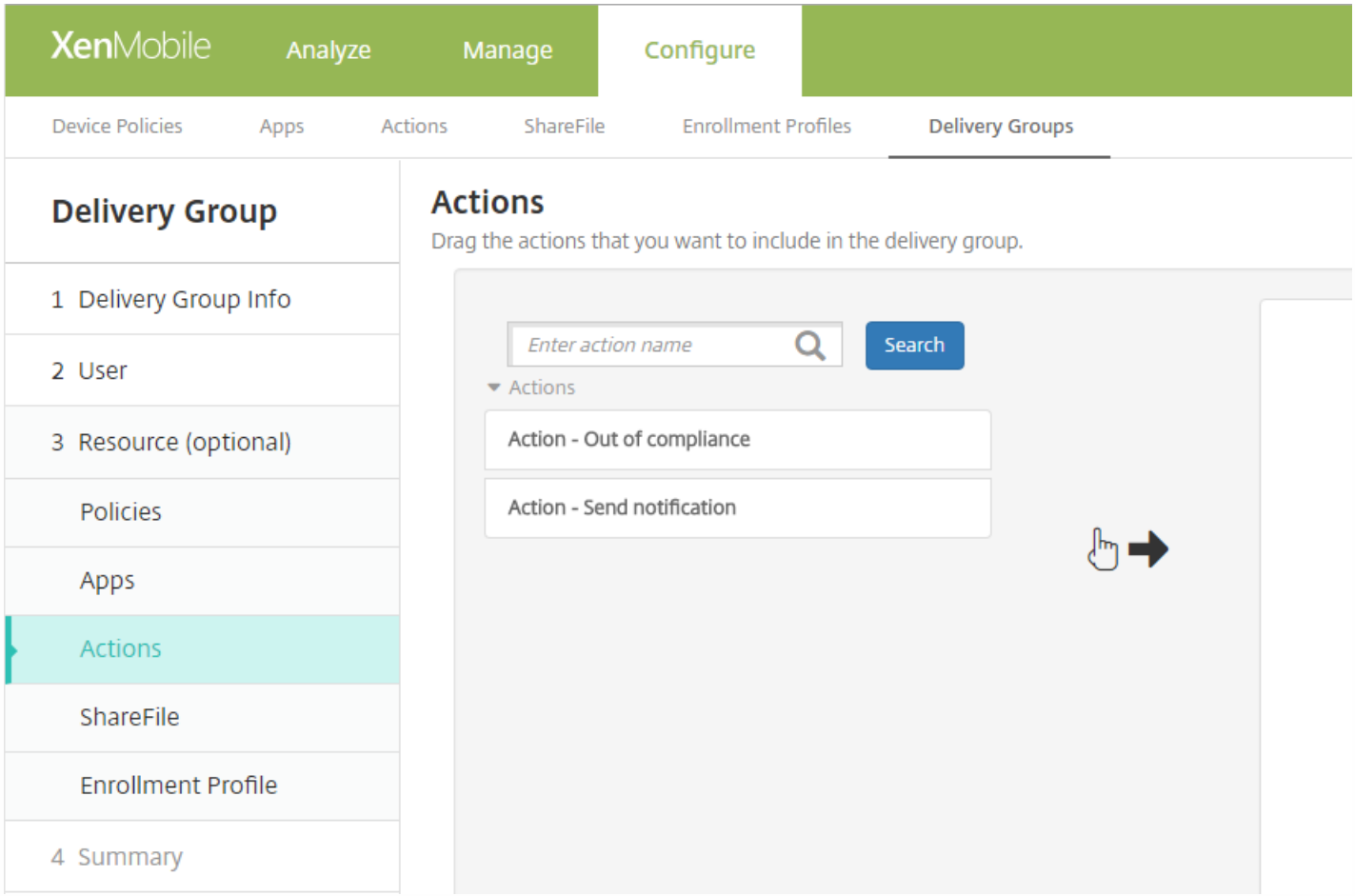
1. Pour chaque application que vous voulez ajouter, procédez comme suit :

- Parcourez la liste des applications disponibles pour trouver l'application que vous souhaitez ajouter.
- Ou pour limiter la liste des applications, entrez un nom d'application complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
- Cliquez sur l'application que vous souhaitez ajouter et faites-la glisser dans la zone **Applications requises** ou **Applications facultatives**.

Remarque : pour supprimer une application, cliquez sur le **X** en regard du nom de l'application dans la zone de droite.

2. Cliquez sur **Next**. La page **Actions** s'affiche.

Ajouter des actions



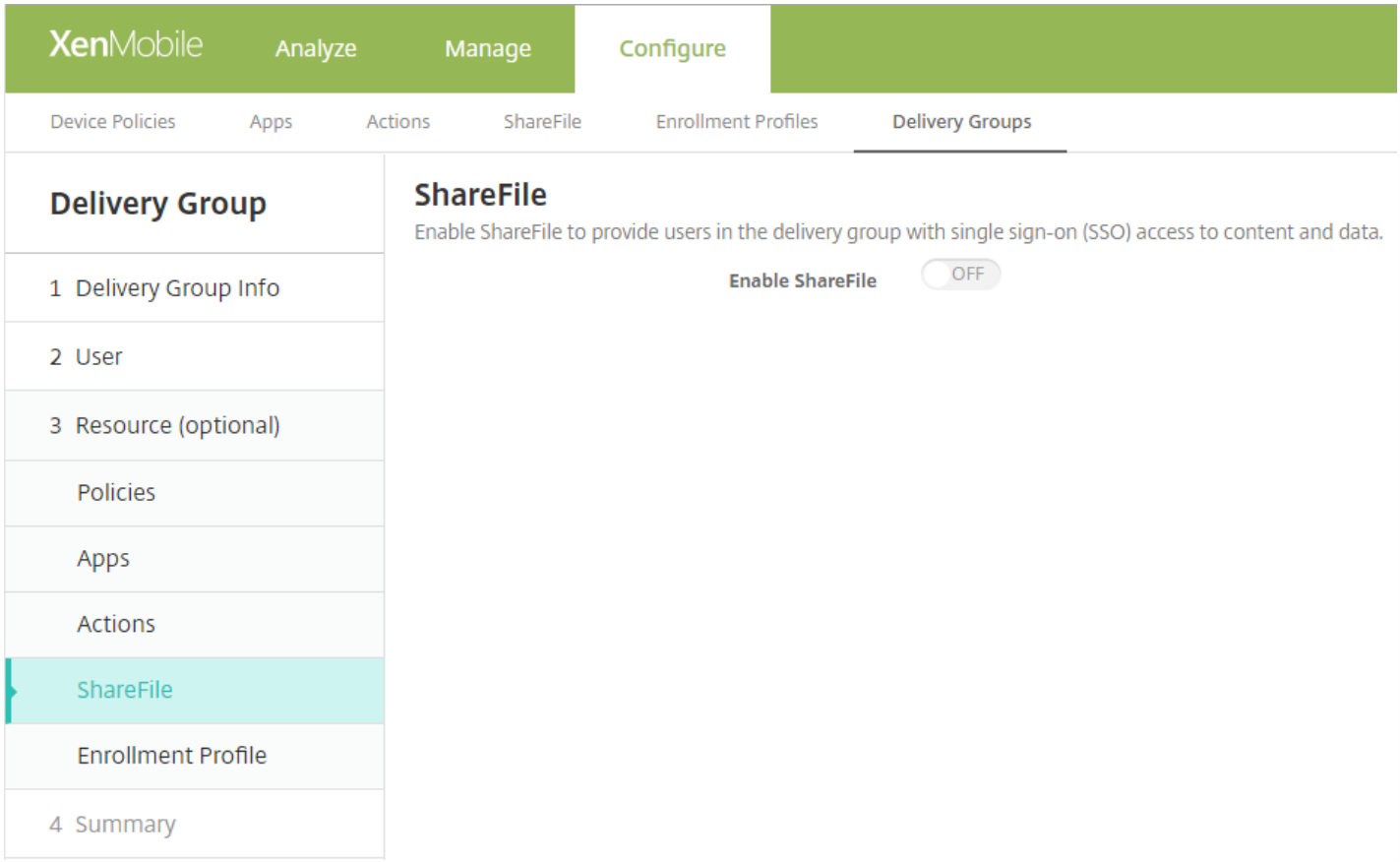
1. Pour chaque action que vous voulez ajouter, procédez comme suit :

- Parcourez la liste des actions disponibles pour trouver l'action que vous souhaitez ajouter.
- Ou pour limiter la liste des actions, entrez un nom d'action complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.
- Cliquez sur l'action que vous souhaitez ajouter et faites-la glisser dans la zone de droite.

Remarque : pour supprimer une action, cliquez sur le **X** en regard du nom de l'action dans la zone de droite.

2. Cliquez sur **Next**. La page **ShareFile** s'ouvre.

Activer ShareFile

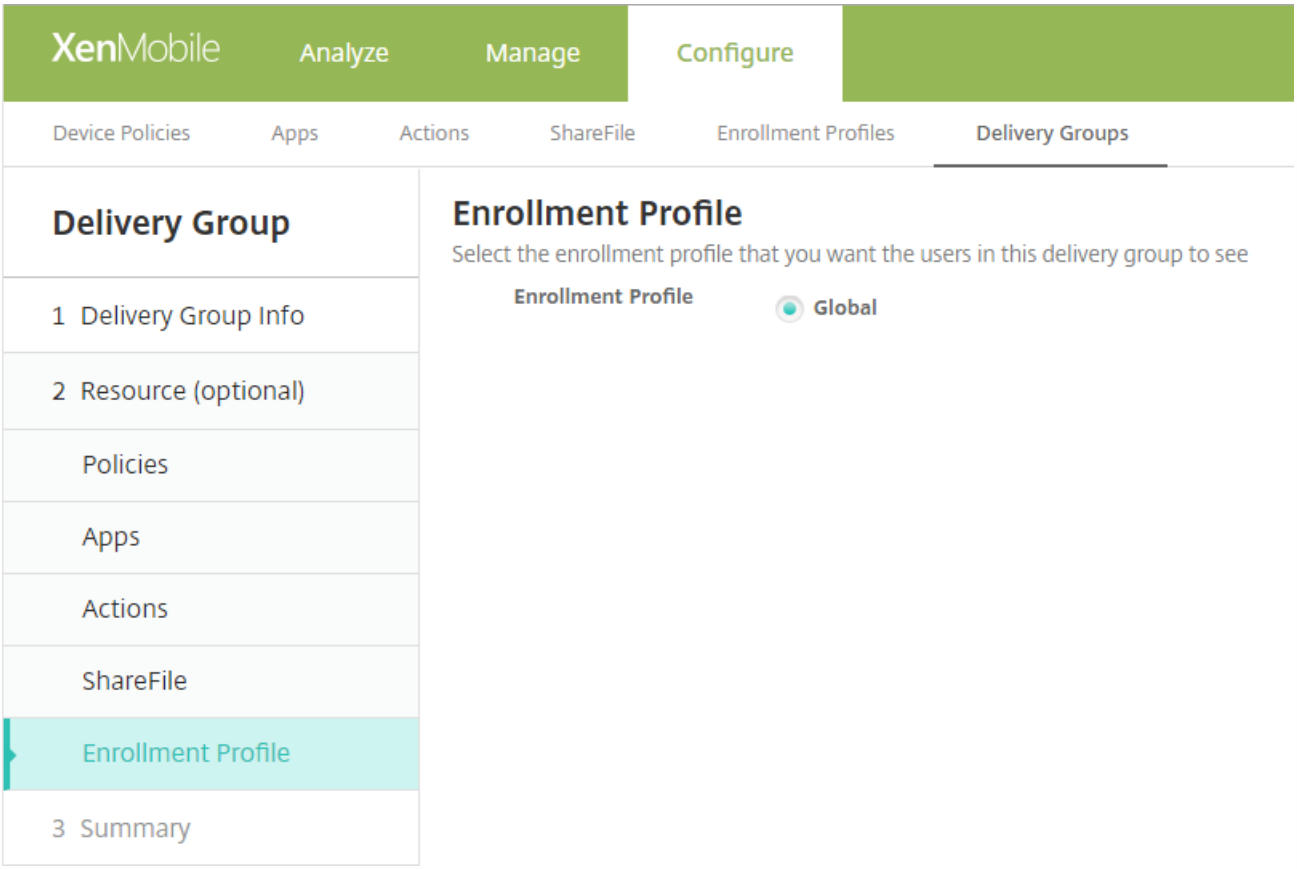


1. Configurez ce paramètre :

- **Activer ShareFile** : cliquez sur **ON** pour activer l'accès par authentification unique ShareFile au contenu et aux données.

2. Cliquez sur **Next**. La page **Résumé** s'affiche.

Profil d'inscription

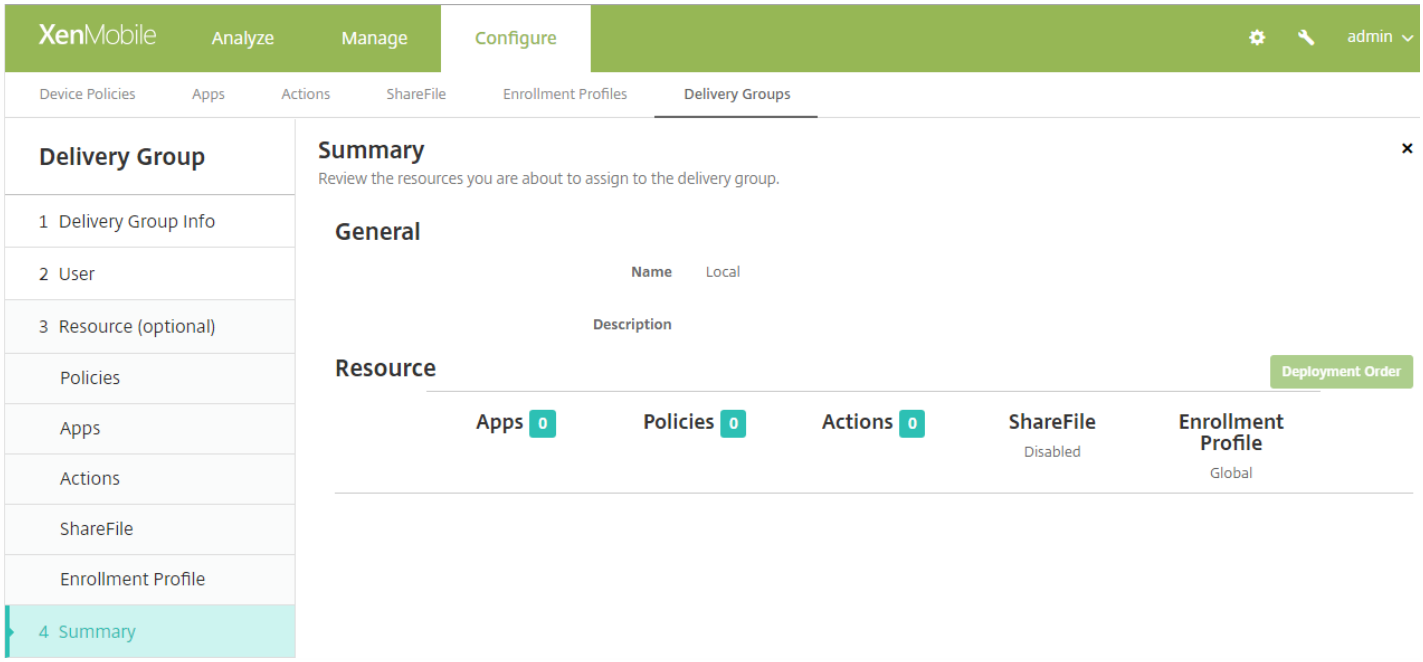


1. Configurez ce paramètre :

- **Profil d'inscription** : sélectionnez un profil d'inscription. Pour créer un profil d'inscription, consultez la section Limite d'inscription d'appareils.

2. Cliquez sur **Suivant**. La page **Résumé** s'affiche.

Consulter les options configurées et modifier l'ordre de déploiement



Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources. La page Résumé affiche vos ressources par catégorie ; elle ne pas reflète pas l'ordre de déploiement.

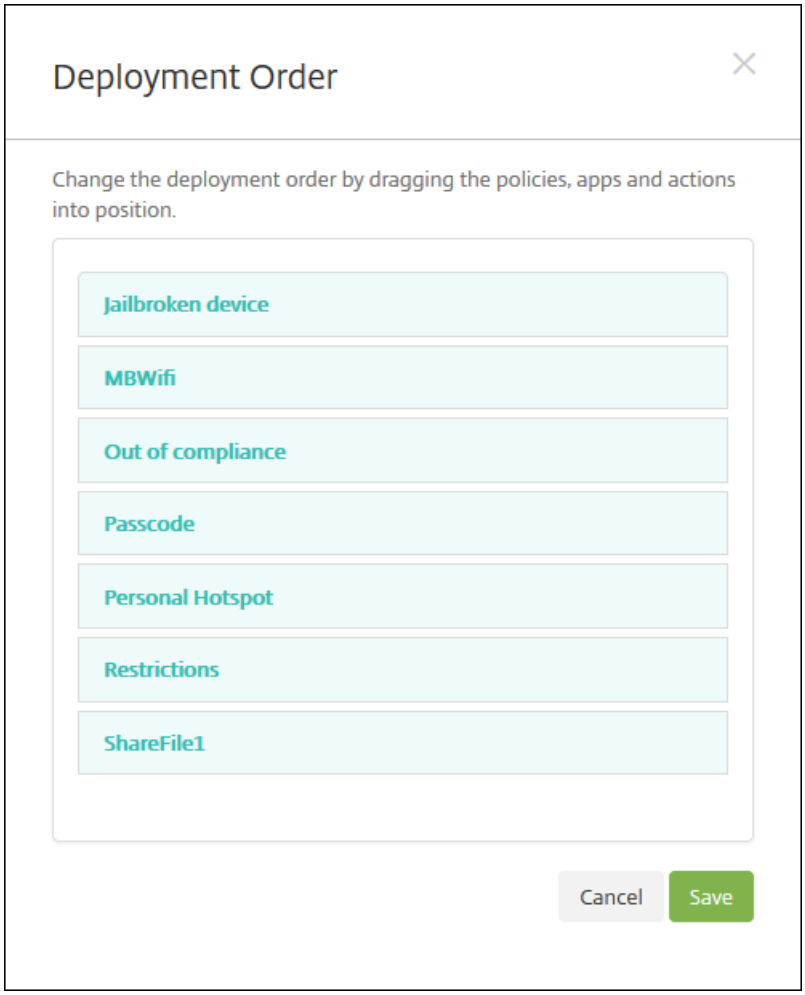
1. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.

2. Cliquez sur **Ordre de déploiement** pour afficher l'ordre de déploiement ou réorganiser l'ordre de déploiement.

3. Cliquez sur **Enregistrer** pour enregistrer le groupe de mise à disposition.

Pour modifier l'ordre de déploiement

1. Cliquez sur le bouton **Ordre de déploiement**. La boîte de dialogue **Ordre de déploiement** s'affiche.



2. Cliquez sur une ressource et faites-la glisser vers l'emplacement à partir duquel vous voulez la déployer. Lorsque vous modifiez l'ordre de déploiement, XenMobile déploie les ressources dans la liste de haut en bas.

3. Cliquez sur **Enregistrer** pour enregistrer l'ordre de déploiement.

Pour modifier un groupe de mise à disposition

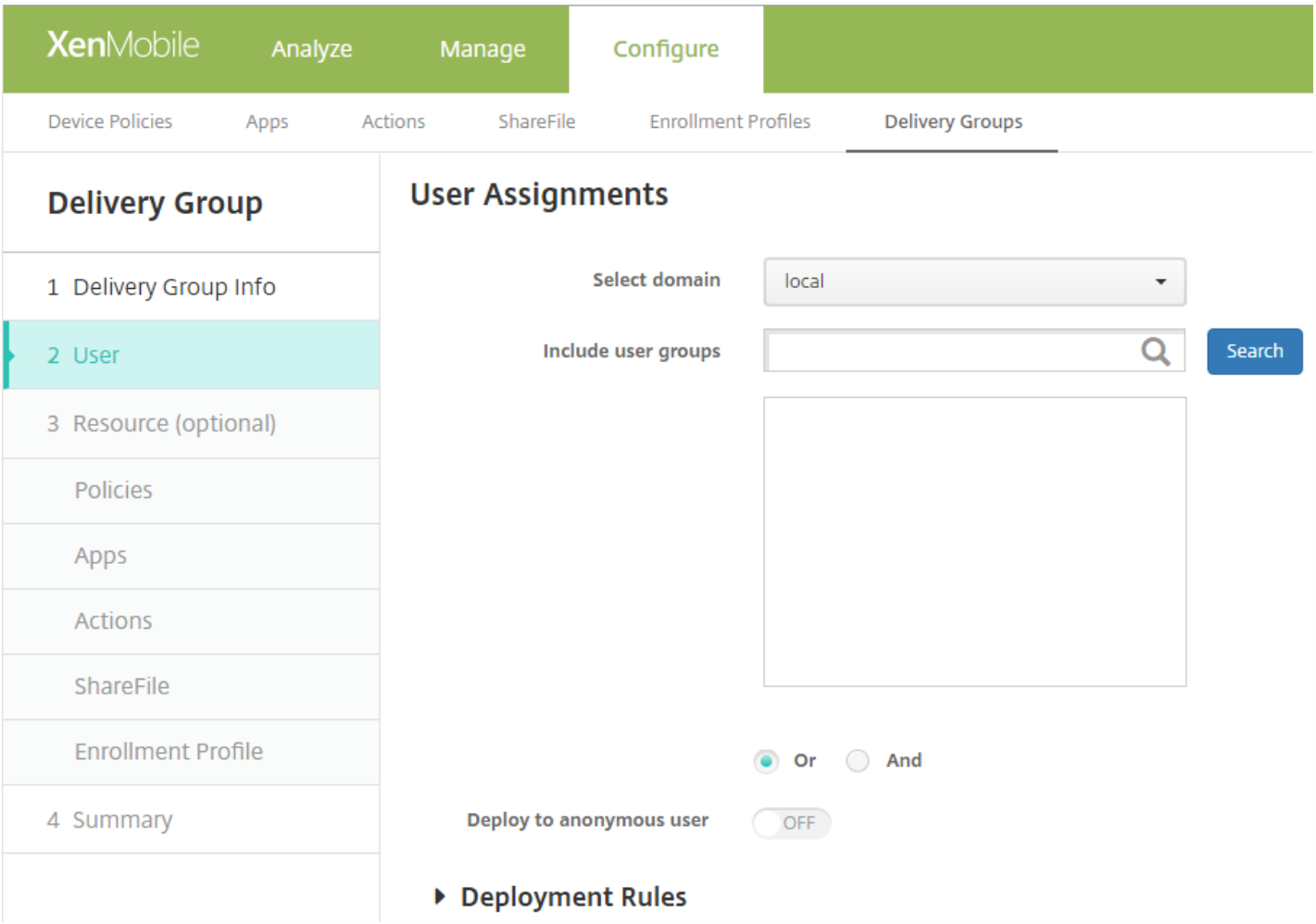
1. Sur la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition que vous souhaitez modifier en sélectionnant la case en regard de son nom ou en cliquant sur la ligne contenant son nom, puis cliquez sur **Modifier**. La page de modification des **Informations sur le groupe de mise à disposition** s'affiche.

> **Remarque**
>
> En fonction de la manière dont vous avez sélectionné le groupe de mise à disposition, la commande **Modifier** apparaît au-dessus ou à droite du groupe de mise à disposition.

2. Ajoutez ou modifiez la **description**.

Remarque : vous ne pouvez pas modifier le nom d'un groupe de mise à disposition existant.

3. Cliquez sur **Suivant**.La page **Attributions utilisateur** apparaît.



4. Sur la page **Sélectionner des groupes d'utilisateurs**, entrez ou modifiez les informations suivantes :

- **Sélectionner un domaine** : sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.
- **Inclure des groupes d'utilisateurs** : effectuez l'une des opérations suivantes :
  - Dans la liste des groupes d'utilisateurs, cliquez sur les groupes que vous souhaitez ajouter. Les groupes sélectionnés s'affichent dans la liste **Groupes d'utilisateurs sélectionnés**.
  - Cliquez sur **Rechercher** pour afficher une liste de tous les groupes d'utilisateurs dans le domaine sélectionné.
  - Tapez un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter la liste des groupes d'utilisateurs.

    Remarque : pour supprimer des groupes d'utilisateurs, cliquez sur **Rechercher**, puis dans la liste des groupes d'utilisateurs, décochez la case à cocher en regard du groupe ou des groupes que vous souhaitez supprimer. Vous pouvez taper un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur **Rechercher** pour limiter le nombre de groupes d'utilisateurs affichés dans la liste.

- **Ou/Et** : sélectionnez cette option pour spécifier si les utilisateurs peuvent appartenir à n'importe quel groupe (Ou) ou s'ils doivent figurer dans tous les groupes (Et) pour le déploiement.
- **Déployer auprès d'un utilisateur anonyme** : sélectionnez cette option si vous voulez déployer auprès d'utilisateurs non authentifiés dans le groupe de mise à disposition.

Remarque : les utilisateurs non authentifiés sont des utilisateurs que vous n'avez pas réussi à authentifier, mais dont les appareils sont autorisés à se connecter à XenMobile.

5. Développez **Règles de déploiement** et configurez les paramètres comme à l'étape 5 de cette procédure.

6. Cliquez sur **Suivant**. La page **Ressources du groupe de mise à disposition** s'affiche. Ajoutez ou supprimez des stratégies, des applications ou des actions. Pour ignorer cette étape, sous **Groupe de mise à disposition**, cliquez sur **Résumé** pour afficher un résumé de la configuration du groupe de mise à disposition.

7. Lorsque vous avez terminé de modifier une ressource, cliquez sur **Suivant** ou sous **Groupe de mise à disposition**, cliquez sur **Résumé**.

8. Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources.

9. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.

10. Cliquez sur **Ordre de déploiement** pour réorganiser l'ordre de déploiement des ressources ; pour plus d'informations sur la modification de l'ordre de déploiement, consultez la section Pour modifier l'ordre de déploiement.

11. Cliquez sur **Enregistrer** pour enregistrer le groupe de mise à disposition.

Pour activer et désactiver le groupe de mise à disposition AllUsers

> **Remarque**
>
> AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver.

1. Dans la page **Groupes de mise à disposition**, sélectionnez le groupe de mise à disposition AllUsers en sélectionnant la case à cocher en regard de **AllUsers** ou en cliquant sur la ligne contenant AllUsers. Procédez ensuite comme suit :

Remarque : en fonction de la manière dont vous avez sélectionné AllUsers, la commande **Activer** ou **Désactiver** apparaît au-dessus ou à droite du groupe de mise à disposition AllUsers.

- Cliquez sur **Désactiver** pour désactiver le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est activé (paramètre par défaut). **Désactivé** s'affiche sous le titre **Désactivé** dans le tableau des groupes de mise à disposition.
- Cliquez sur **Activer** pour activer le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est désactivé. **Désactivé** disparaît du titre **Désactivé** dans le tableau des groupes de mise à disposition.

Pour déployer sur des groupes de mise à disposition

Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils iOS, Windows Phone et Windows Tablet qui appartiennent au groupe de mise à disposition les invitant à se reconnecter à XenMobile. Cela permet de réévaluer les appareils et de déployer des applications, des stratégies et des actions. Les utilisateurs équipés d'autres plates-formes reçoivent les ressources immédiatement s'ils sont déjà connectés, ou en fonction de leur stratégie de planification, la prochaine fois qu'ils se connectent.

Remarque : pour mettre à jour les applications affichées dans la liste des applications disponibles dans le XenMobile Store sur les appareils Android des utilisateurs, vous devez d'abord déployer une stratégie d'inventaire des applications sur les

appareils des utilisateurs.

1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :

- Pour déployer sur plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes sur lesquels vous voulez déployer.
- Pour déployer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.

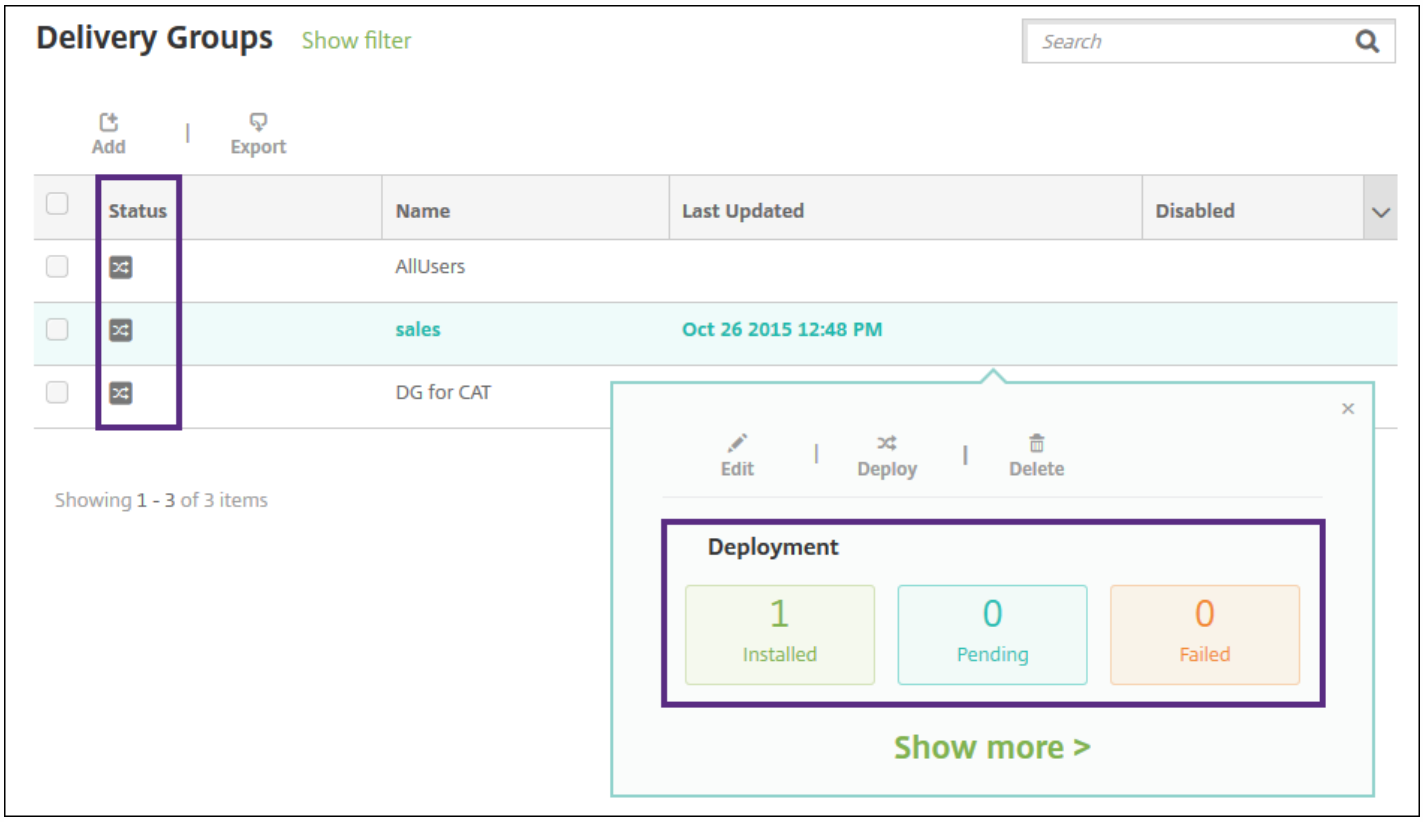
2. Cliquez sur **Déployer**.

Remarque : en fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Déployer** apparaît au-dessus ou à droite du groupe de mise à disposition.

Vérifiez que les groupes auprès desquels vous souhaitez déployer des applications, des stratégies et des actions sont répertoriés et cliquez sur **Déployer**. Les applications, stratégies et actions sont déployées auprès des groupes sélectionnés en fonction de la plate-forme d'appareil et de la stratégie de planification.

Vous pouvez vérifier l'état du déploiement sur la page **Groupes de mise à disposition** de l'une des façons suivantes :

- Examinez l'icône de déploiement sous l'en-tête **État** pour le groupe de mise à disposition, qui indique les échecs de déploiement.
- Cliquez sur la ligne contenant le groupe de mise à disposition pour afficher une superposition indiquant si les déploiements sont **installés**, **en attente** ou qu'ils ont **échoué**.



Pour supprimer des groupes de mise à disposition

> **Remarque**
>
> vous ne pouvez pas supprimer le groupe de mise à disposition AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs.

1. Sur la page **Groupes de mise à disposition**, effectuez l'une des opérations suivantes :

- Pour supprimer plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes que vous voulez supprimer.
- Pour supprimer sur un seul groupe de mise à disposition, sélectionnez la case à cocher en regard de son nom ou cliquez sur la ligne contenant son nom.

2. Cliquez sur **Supprimer**. La boîte de dialogue **Supprimer** s'affiche.

Remarque : en fonction de la manière dont vous sélectionnez un groupe de mise à disposition, la commande **Supprimer** apparaît au-dessus ou à droite du groupe de mise à disposition.

3. Cliquez sur **Supprimer**.

> **Important**
>
> vous ne pouvez pas annuler cette opération.

Pour exporter le tableau des groupes de mise à disposition

1. Cliquez sur le bouton **Exporter** au-dessus du tableau **Groupes de mise à disposition**. XenMobile extrait les informations du tableau **Groupes de mise à disposition** et les convertit en fichier .csv.

2. Ouvrez ou enregistrez le fichier .csv. Cette opération dépend du navigateur que vous utilisez. Vous pouvez également annuler l'opération.

Macros

Feb 23, 2017

XenMobile fournit des macros puissantes qui permettent de renseigner les données de propriété d'utilisateur ou d'appareil dans le champ de texte d'un profil, d'une stratégie, d'une notification, ou d'un modèle d'inscription (pour certaines actions), pour ne citer que quelques exemples d'utilisations. Grâce aux macros, vous pouvez configurer une stratégie et la déployer auprès d'un grand nombre d'utilisateurs et de manière à ce que des valeurs spécifiques à l'utilisateur s'affichent pour chaque utilisateur ciblé. Par exemple, vous pouvez pré-remplir la valeur boîte aux lettres pour un utilisateur dans un profil Exchange pour des milliers d'utilisateurs.

Cette fonctionnalité est disponible uniquement dans le contexte de configurations et de modèles pour iOS et Android.

Définition des macros utilisateur

Les macros utilisateur suivantes sont toujours disponibles :

- loginname (nom d'utilisateur + nom de domaine)
- username (nom d'ouverture de session moins le domaine, si présent)
- domainname (nom de domaine, ou domaine par défaut)

Il se peut que les propriétés suivantes définies par l'administrateur soient disponibles :

- 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 (remplace la propriété décrite ci-dessus)

En outre, si l'utilisateur est authentifié à l'aide d'un serveur d'authentification, tel que LDAP, toutes les propriétés associées à l'utilisateur dans le magasin sont disponibles.

Syntaxe des macros

Une macro pouvez prendre la forme suivante :

- ${type.PROPERTYNAME}
- ${type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]}

De manière générale, toute syntaxe suivie du symbole dollar ($) doit être placée entre accolades ({ }).

- Les noms de propriétés qualifiés font référence à une propriété utilisateur, à une propriété d'appareil ou à une propriété personnalisée.
- Les noms de propriétés qualifiés consistent en un préfixe, suivi par le nom de propriété réel.
- Les propriétés de l'utilisateur prennent la forme ${user.[PROPERTYNAME] (prefix="user.")}.
- Les propriétés d'appareil prennent la forme ${device.[PROPERTYNAME] (prefix="device.")}.

Par exemple,${user.username} remplit la valeur de nom d'utilisateur dans le champ de texte d'une stratégie. Ceci est utile pour la configuration des profils Exchange ActiveSync et d'autres profils utilisés par plusieurs utilisateurs.

Pour les macros personnalisées (propriétés que vous définissez), le préfixe est ${custom}. Vous pouvez ignorer le préfixe.

Remarque : les noms de propriétés sont sensibles à la casse.

Actions automatisées

Mar 31, 2017

Vous créez des actions automatisées dans XenMobile pour programmer des réactions à des événements, à des propriétés utilisateur/appareil ou l'existence d'applications sur les appareils utilisateur. Lorsque vous créez une action automatisée, vous devez définir son effet sur l'appareil de l'utilisateur lorsqu'il est connecté à XenMobile en fonction de déclencheurs. Lorsqu'un événement est déclenché, vous pouvez envoyer une notification à l'utilisateur pour résoudre un problème avant qu'une action plus sérieuse ne soit nécessaire.

Par exemple, si vous souhaitez détecter une application que vous avez déjà mise dans une liste noire (par exemple, Scrabble), vous pouvez spécifier un déclencheur qui rend l'appareil utilisateur non-conforme lorsque l'application Scrabble est détectée sur leur appareil. L'action les avertit qu'ils doivent supprimer l'application pour que leurs appareils soient à nouveau conformes. Vous pouvez définir un délai au cours duquel l'utilisateur doit se conformer aux exigences avant d'entreprendre d'autres actions plus sérieuses, comme l'effacement des données d'entreprise de l'appareil.

Dans les cas où l'appareil d'un utilisateur est placé dans un état de non conformité, puis que l'utilisateur répare l'appareil de façon à ce qu'il soit conforme, vous devez configurer une stratégie destinée à déployer un paquetage qui réinitialise l'appareil dans un état de conformité.

Les effets automatiques que vous pouvez paramétrer sont :

- Effacement complet ou effacement des données d'entreprise de l'appareil.
- Rendre l'appareil non-conforme.
- Révoquer l'appareil.
- Envoyer un message à l'utilisateur pour qu'il résolve un problème avant que des actions plus sévères ne soient entreprises.

Cet article explique comment ajouter, modifier et filtrer les actions automatisées dans XenMobile, ainsi que la manière de configurer les actions d'effacement et de verrouillage des applications pour le mode MAM exclusif.

> ## Remarque
>
> Pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans Paramètres pour SMTP et SMS afin que XenMobile puisse envoyer des messages, consultez Notifications dans XenMobile. Vous devez également configurer les modèles de notification que vous prévoyez d'utiliser avant de continuer. Pour de plus amples informations sur la configuration des modèles de notification, consultez la section Pour créer ou mettre à jour des modèles de notification dans XenMobile.

1. Dans la console XenMobile, cliquez sur **Configurer** > **Actions**.La page **Actions** s'affiche.

2. Sur la page **Actions**, effectuez l'une des actions suivantes :

- Cliquez sur **Ajouter** pour ajouter une nouvelle action.
- Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.

Remarque : lorsque vous activez la case à cocher en regard d'une action, le menu d'options s'affiche au-dessus de la liste d'actions ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

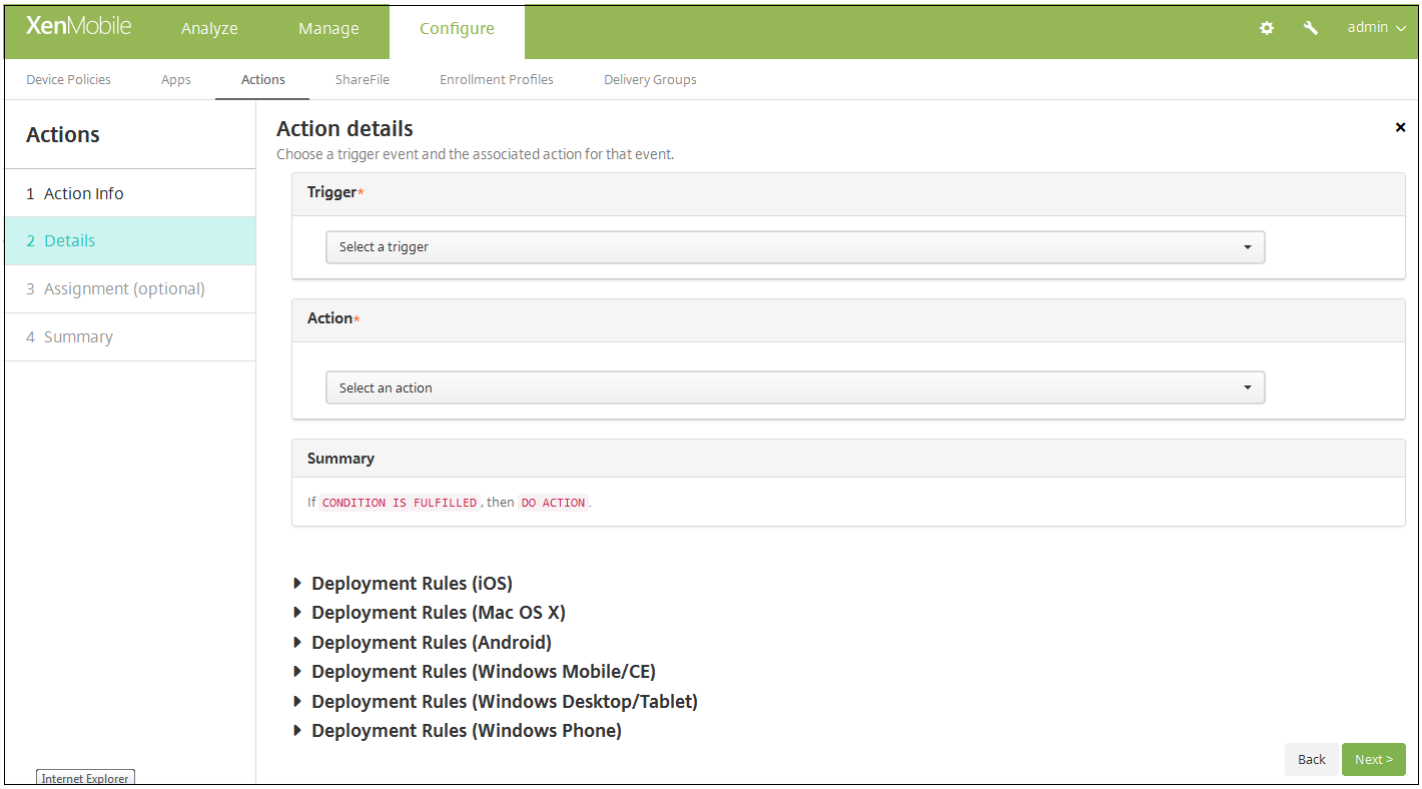
3. La page **Informations sur l'action** s'affiche.

4. Sur la page **Informations sur l'action**, entrez ou modifiez les informations suivantes :

- **Nom** : entrez un nom permettant d'identifier de façon unique l'action. Ce champ est obligatoire.
- **Description** : décrivez ce que l'action doit faire.

5. Cliquez sur **Suivant**.La page sur les **Détails de l'action** s'affiche.

Remarque : l'exemple suivant illustre comment configurer un **déclencheur d'événement**. Si vous sélectionnez un autre déclencheur, les options sont différentes de celles affichées ici.



6. Sur la page **Détails de l'action**, entrez ou modifiez les informations suivantes :

- Dans la liste des **Déclencheurs**, cliquez sur le type de déclencheur d'événements pour cette action.Signification des déclencheurs :
  - **Événement** : réagit à un événement prédéfini.
  - **Propriété de l'appareil** : recherche un attribut d'appareil sur l'appareil en mode MDM et y réagit.
  - **Propriété utilisateur** : réagit à un attribut utilisateur, généralement à partir d'Active Directory.
  - **Nom de l'application installée** : réagit à une application installée. Ne s'applique pas au mode MAM exclusif. Requiert que la stratégie d'inventaire des applications soit activée sur l'appareil. Par défaut, la stratégie d'inventaire des applications est activée sur toutes les plates-formes. Pour de plus amples informations, consultez la section Pour ajouter une stratégie d'inventaire des applications.

7. Dans la liste suivante, cliquez sur la réponse au déclencheur.

8. Dans la liste **Action**, cliquez sur l'action à effectuer lorsque le critère du déclencheur est rencontré. À l'exception de **Envoyer une notification**, vous choisissez un délai au cours duquel les utilisateurs devront avoir résolu le problème qui a activé le déclencheur. Si le problème n'est pas résolu dans ce délai, l'action sélectionnée est entreprise. Les actions

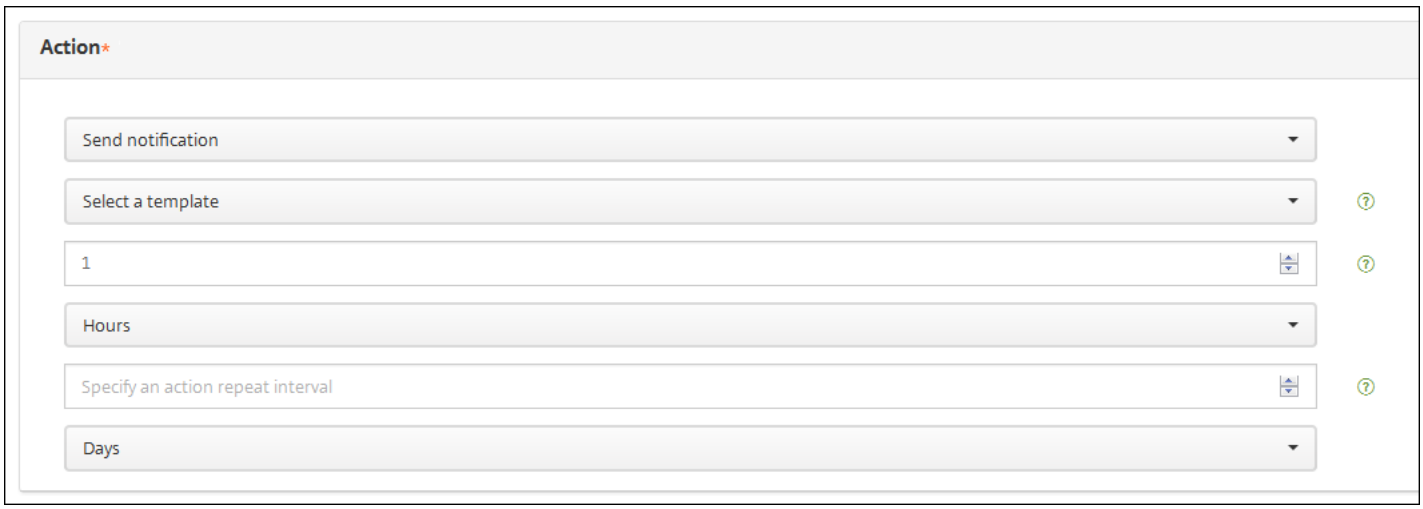
disponibles sont les suivantes :

- **Effacer les données d'entreprise de l'appareil** : permet d'effacer toutes les données et applications d'entreprise d'un appareil, sans toucher aux données et applications personnelles.
- **Effacer toutes les données de l'appareil** : permet d'effacer toutes les données et applications d'un appareil, y compris des cartes mémoire si l'appareil en est doté.
- **Révoquer l'appareil** : permet d'empêcher un appareil de se connecter à XenMobile.
- **Mode kiosque** : permet de refuser l'accès à toutes les applications sur un appareil. Sur Android, les utilisateurs ne pourront pas se connecter à XenMobile. Sur iOS, les utilisateurs pourront se connecter, mais ils ne pourront pas accéder aux applications. Pour de plus amples informations, consultez la section « Actions de verrouillage et d'effacement des applications en mode MAM uniquement » plus loin dans cet article.
- **Effacement des applications** : sur Android, cette option supprime le compte XenMobile de l'utilisateur. Sur iOS, cette option supprime les clés de cryptage dont les utilisateurs ont besoin pour pouvoir accéder aux fonctionnalités de XenMobile.Pour de plus amples informations, consultez la section « Actions de verrouillage et d'effacement des applications en mode MAM uniquement » plus loin dans cet article.
- **Marquer l'appareil comme non conforme** : permet de définir l'appareil comme non conforme.
- **Envoyer une notification** : permet d'envoyer un message à l'utilisateur.

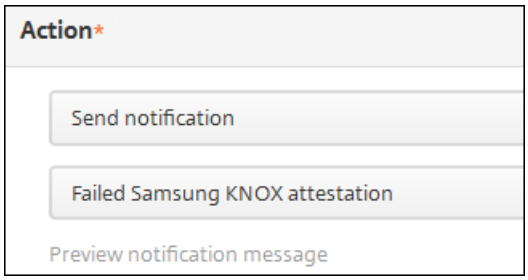
Si vous sélectionnez **Envoyer une notification**, le reste de cette procédure décrit comment envoyer une action de notification.

9. Dans la liste suivante, sélectionnez le modèle à utiliser pour la notification.Les modèles de notification correspondant à l'événement sélectionné apparaissent, sauf si aucun modèle n'existe pour le type de notification. Dans ce cas, le message suivant vous invite à configurer un modèle : Aucun modèle de notification pour ce type d'événement. Créez un modèle à l'aide de **Modèles de notification** dans **Paramètres**.

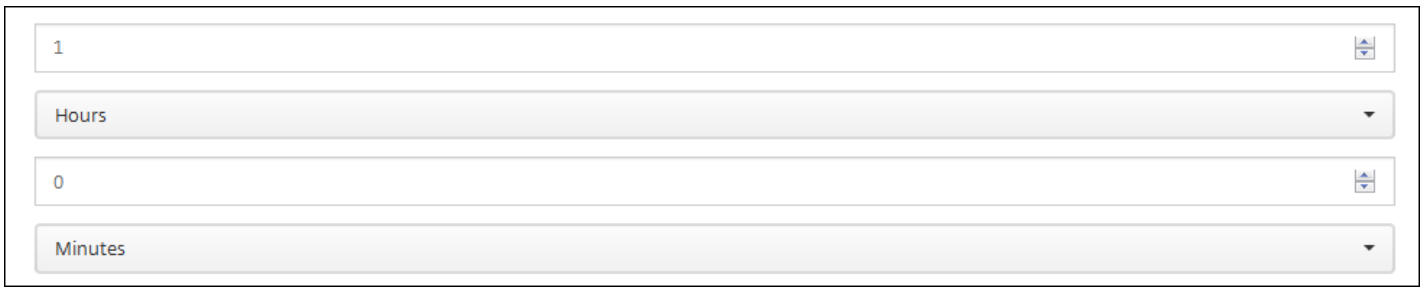
Remarque : pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans Paramètres pour SMTP et SMS afin que XenMobile puisse envoyer des messages, consultez Notifications dans XenMobile. Vous devez également configurer les modèles de notification que vous prévoyez d'utiliser avant de continuer. Pour de plus amples informations sur la configuration des modèles de notification, consultez la section Pour créer ou mettre à jour des modèles de notification dans XenMobile.



Remarque : après avoir sélectionné le modèle, vous pouvez afficher un aperçu de la notification en cliquant sur **Aperçu du message de notification**.



10. Dans les champs suivants, définissez le délai en jours, heures ou minutes avant d'effectuer une action et l'intervalle auquel l'action doit se répéter jusqu'à ce que l'utilisateur résolve le problème ayant activé le déclencheur.



11. Dans **Résumé**, vérifiez que vous avez créé les actions automatisées comme prévu.

12. près avoir configuré les détails de l'action, vous pouvez configurer des règles de déploiement pour chaque plate-forme individuellement. Pour ce faire, suivez l'étape 13 pour chacune des plates-formes que vous choisissez.

13. Configurez les règles de déploiement

14. Lorsque vous avez terminé de configurer les règles de déploiement par plate-forme pour l'action, cliquez sur **Suivant**.La page d'**attribution d'actions** s'affiche. Sur cette page, vous pouvez attribuer l'action à un ou plusieurs groupes de mise à disposition. Cette étape est facultative.

15. En regard de **Choisir des groupes de mise à disposition**, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie.Les groupes que vous sélectionnez s'affichent dans liste de droite **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

16. Développez Calendrier de déploiement et configurez les paramètres suivants :

- En regard de **Déployer**, cliquez sur **ON** pour planifier le déploiement ou cliquez sur **OFF** pour empêcher le déploiement. L'option par défaut est **ON**.Si vous choisissez **OFF**, aucune autre option ne doit être configurée.
- En regard de **Calendrier de déploiement**, cliquez sur **Maintenant** ou **Plus tard**. L'option par défaut est **Maintenant**.
- Si vous cliquez sur **Plus tard**, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.

- En regard de **Conditions de déploiement**, cliquez sur **À chaque connexion** ou **Uniquement lorsque le déploiement précédent a échoué**. L'option par défaut est **À chaque connexion**.
- En regard de **Déployer pour les connexions permanentes**, cliquez sur **ON** ou **OFF**. L'option par défaut est **OFF**. **Remarque** : cette option s'applique lorsque vous avez configuré la clé de déploiement d'arrière-plan de planification dans **Paramètres** > **Propriétés du serveur**. L'option de calendrier permanent n'est pas disponible pour iOS.

Remarque : le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de **Déployer pour les connexions permanentes**, qui ne s'applique pas à iOS.

17. Cliquez sur **Suivant**.La page **Résumé** s'affiche, où vous pouvez vérifier la configuration de l'action.

18. Cliquez sur **Enregistrer** pour enregistrer l'action.

Actions de verrouillage et d'effacement des applications en mode MAM uniquement

Vous pouvez effacer ou verrouiller les applications d'un appareil en réponse à quatre catégories de déclencheurs répertoriées dans la console XenMobile : événement, propriété de l'appareil, propriété utilisateur et nom de l'application installée.

Pour configurer le déclenchement automatique de l'effacement des applications ou du mode kiosque

1. Dans la console XenMobile, cliquez sur **Configurer > Actions**.

2. Sur la page **Actions**, cliquez sur **Ajouter**.

3. Sur la page **Informations sur l'action**, entrez un nom pour l'action et une description facultative.

4. Sur la page **Détails de l'action**, sélectionnez le déclencheur de votre choix.

5. Dans **Action**, sélectionnez une action.

Pour cette étape, tenez compte des conditions suivantes :

Lorsque le type de déclencheur est **Événement** et que la valeur n'est pas **Utilisateur Active Directory désactivé**, les actions **Effacement des applications** et **Mode kiosque** ne s'affichent pas.

Lorsque le type de déclencheur est **Propriété de l'appareil** et que la valeur est **Mode perdu MDM activé**, les actions suivantes ne s'affichent pas :

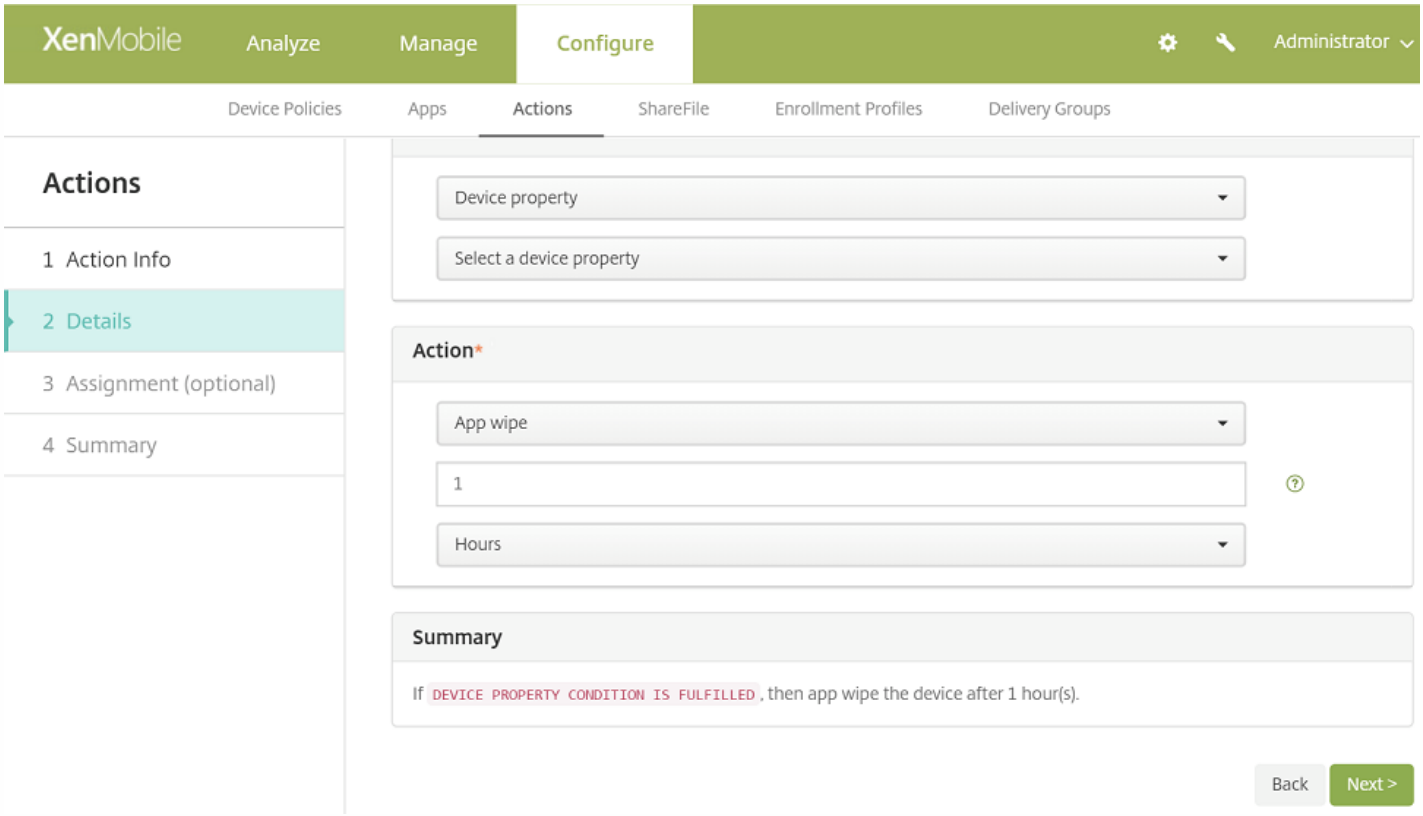
- Effacer les données d'entreprise de l'appareil
- Effacer toutes les données de l'appareil
- Révoquer l'appareil

Pour chaque option, un délai de 1 heure est automatiquement défini, mais vous pouvez sélectionner la durée de ce délai en minutes, heures ou jours. Le délai donne aux utilisateurs la possibilité de tenter de résoudre un problème avant l'exécution de l'action. Vous pouvez en apprendre davantage sur les actions Effacement des applications et Mode kiosque dans la rubrique Configuration de rôles avec RBAC.

> **Remarque**
>
> Si vous définissez le déclencheur sur **Événement**, l'intervalle de répétition est réglé automatiquement sur un minimum d'1 heure.

L'appareil doit actualiser les stratégies pour se synchroniser avec le serveur pour que la notification soit envoyée. En règle générale, un appareil se synchronise avec le serveur lorsque les utilisateurs se connectent ou actualisent manuellement leurs stratégies Secure Hub.

Un délai supplémentaire d'environ une heure avant l'exécution de l'action est également possible, afin de permettre la synchronisation de la base de données Active Directory avec XenMobile.



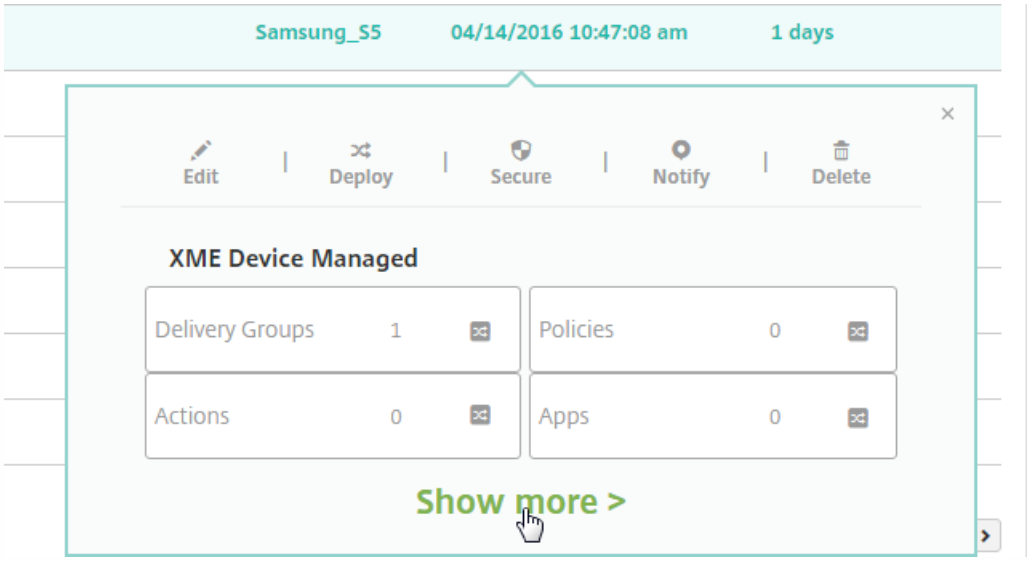
6. Configurez les règles de déploiement, puis cliquez sur **Suivant**.

7. Configurez les attributions de groupe de mise à disposition et un calendrier de déploiement, puis cliquez sur **Suivant**.

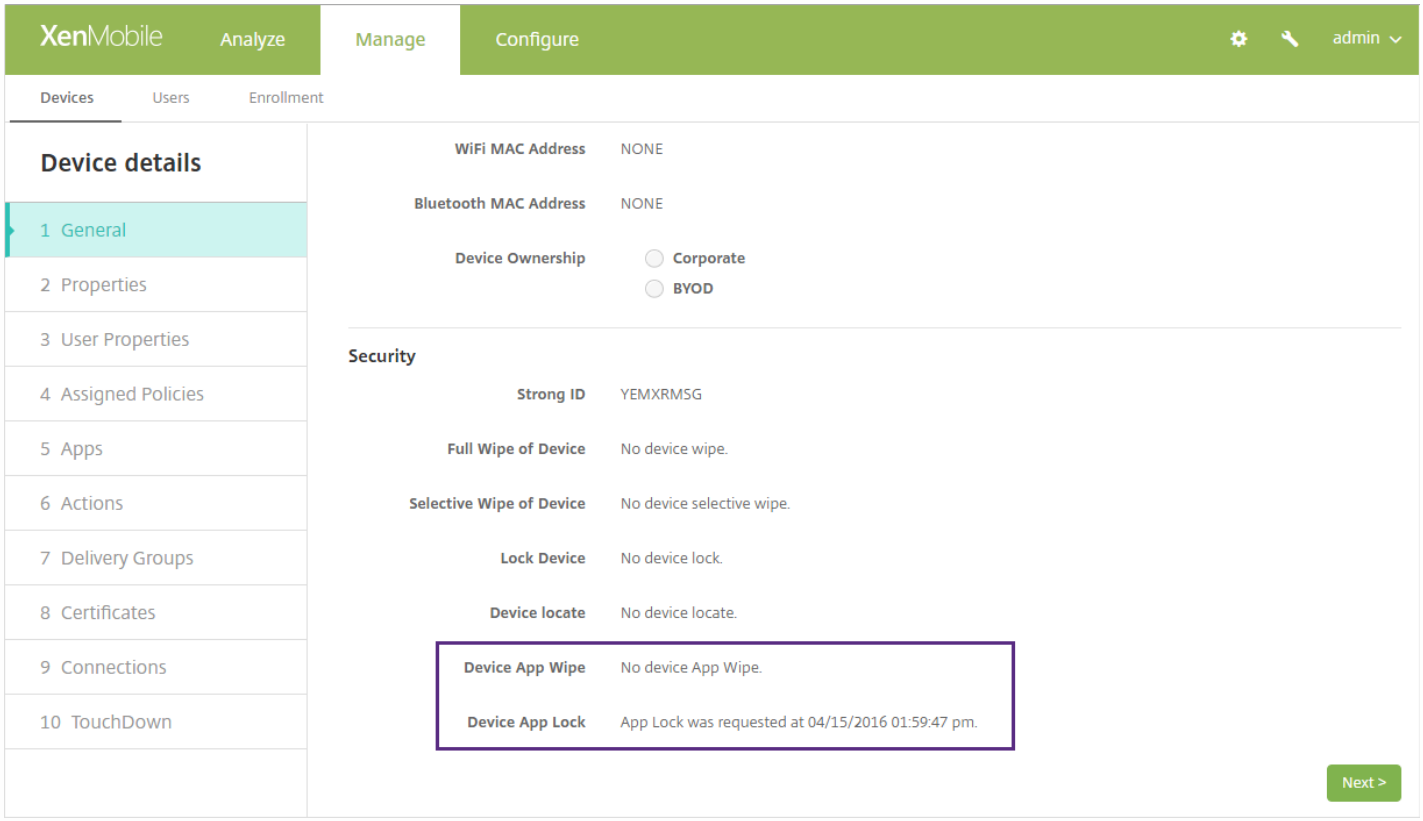
8. Cliquez sur **Enregistrer**.

Pour vérifier l'état de verrouillage ou d'effacement d'une application

1. Accédez à **Gérer > Appareils**, cliquez sur un appareil et sur **Afficher plus**.



2. Faites défiler jusqu'à **Effacement des applications sur l'appareil** et **Mode kiosque sur l'appareil**.



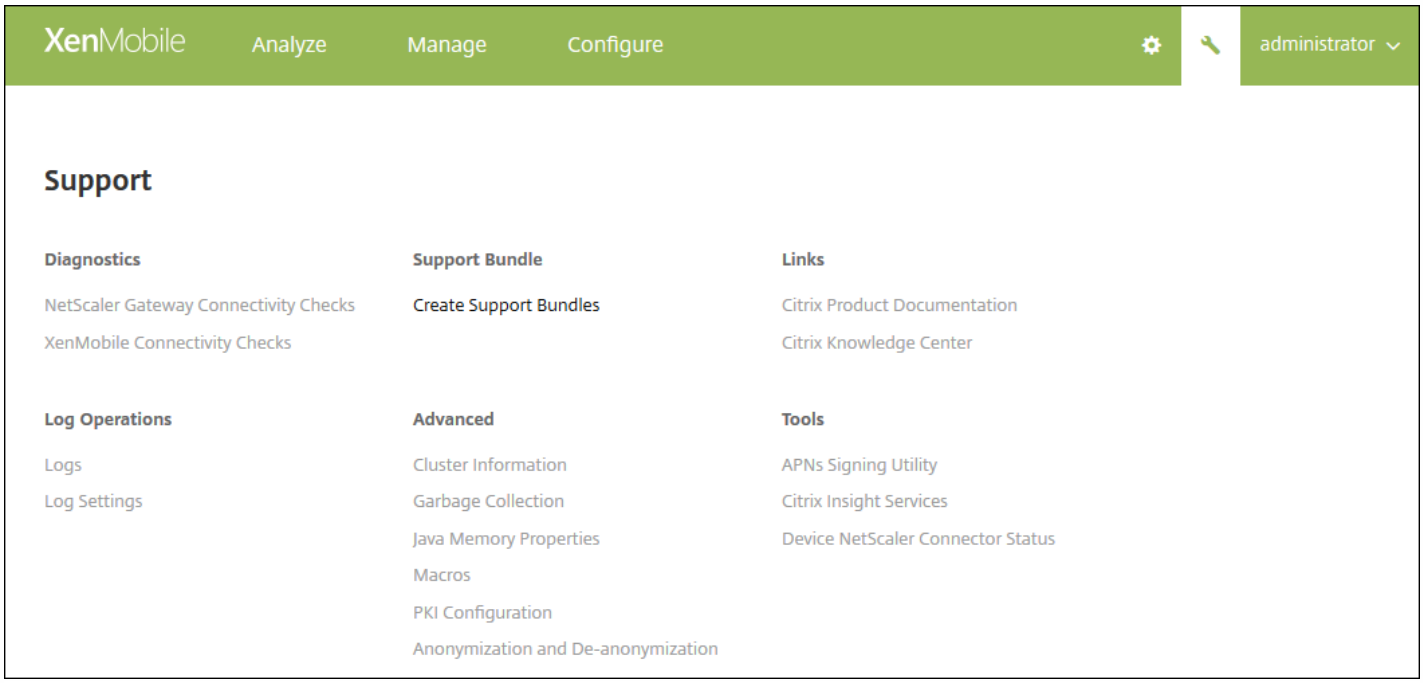
Surveillance et support

Feb 23, 2017

Utilisez la page Support de XenMobile pour accéder à des informations et outils de support. Vous pouvez également effectuer des actions à partir de l'interface de ligne de commande. Pour de plus amples informations, consultez la section Options d'interface de ligne de commande.

Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit.

La page Support s'affiche.



Utilisez la page **Support** de XenMobile pour :

- Accéder aux diagnostics.
- Créer des packs d'assistance.
- Accéder aux liens de la documentation produit et du centre de connaissances Citrix.
- Accéder au journal des opérations.
- Sélectionner un ensemble d'options de configuration et d'informations avancées.
- Accéder à un ensemble d'outils et d'utilitaires.

Rapports

Mar 31, 2017

XenMobile propose les rapports prédéfinis suivants qui vous permettent d'analyser vos déploiements d'applications et d'appareils :

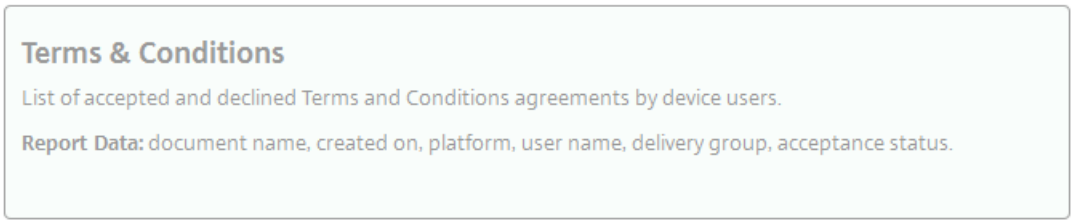
- **Applications par appareils et utilisateur** : répertorie les applications gérées que les utilisateurs ont sur leur appareil. Ce rapport ne comprend pas les applications personnelles installées sur un appareil.
- **Termes et conditions** : répertorie les utilisateurs qui ont accepté et refusé les conditions générales.
- **Top 25 des applications** : répertorie jusqu'à 25 applications que la plupart des utilisateurs ont sur leurs appareils.
- **Appareils jailbreakés/rootés** : répertorie les appareils iOS rootés et les appareils Android jailbreakés.
- **Top 10 des applications** : échec du déploiement : répertorie les applications dont le déploiement a échoué.
- **Appareils inactifs** : répertorie les appareils qui sont inactifs depuis une période de temps spécifiée.
- **Application par type et catégorie** : répertorie les applications par version, type et catégorie.
- **Inscription d'appareils** : répertorie tous les appareils inscrits.
- **Applications par plate-forme** : répertorie les applications et les versions de l'application par plate-forme et version de l'appareil.
- **Applications sur liste noire par appareil et utilisateur** : répertorie les applications sur liste noire que les utilisateurs ont sur leur appareil.
- **Appareils et applications** : dresse la liste des appareils qui exécutent des applications gérées.

Les rapports sont au format .csv, que vous pouvez ouvrir avec des programmes tels que Microsoft Excel.

Suivez les instructions ci-dessous pour créer un rapport :

1. Dans la console XenMobile, cliquez sur l'onglet **Analyser**, puis cliquez sur **Rapports**. La page **Rapports** s'affiche.

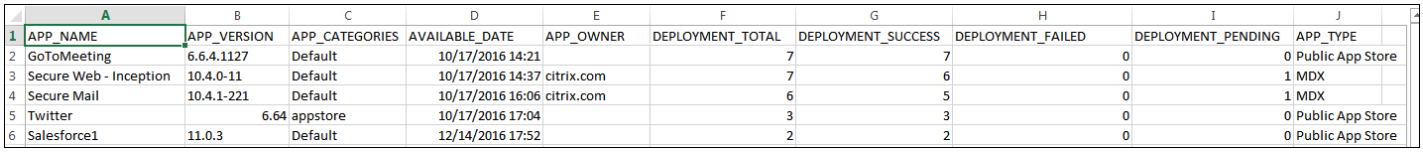
Chaque type de rapport contient une description des informations recueillies par le rapport, ainsi que les données spécifiques du rapport, comme illustré dans l'exemple suivant :



2. Cliquez sur le rapport que vous souhaitez créer. En fonction du navigateur que vous utilisez, le fichier est automatiquement téléchargé ou vous êtes invité à enregistrer le fichier.

3. Répétez l'étape 2 pour chaque rapport que vous souhaitez créer.

La figure suivante montre une partie d'un rapport des top 25 des applications tel qu'il apparaît dans Microsoft Excel :



	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

Bien qu'il soit possible d'utiliser SQL Server pour créer des rapports personnalisés, Citrix ne recommande pas cette méthode. L'utilisation de la base de données SQL Server de cette façon peut avoir des conséquences imprévues sur votre déploiement XenMobile. Si vous décidez d'utiliser cette méthode de création de rapports, assurez-vous que les requêtes SQL sont exécutées à l'aide d'un compte en lecture seule.

Fournisseur de services mobiles

Feb 23, 2017

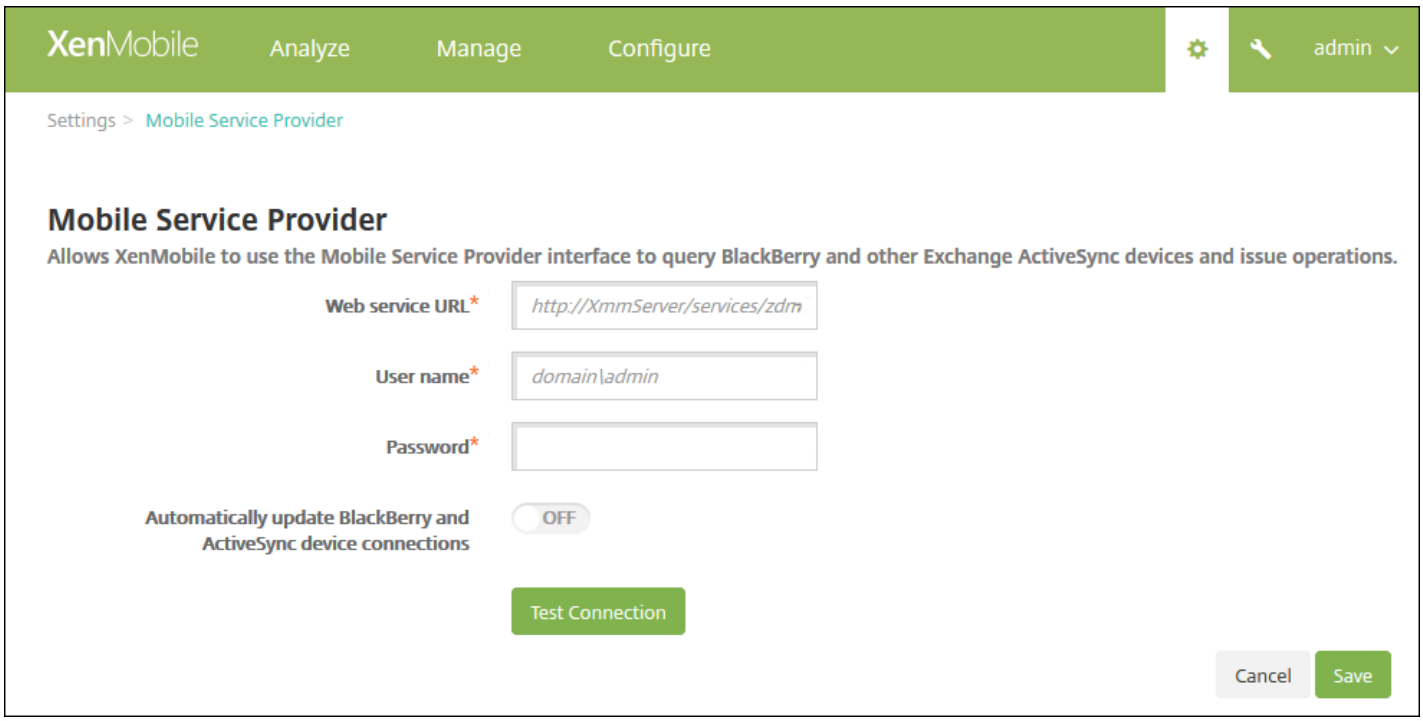
Vous pouvez configurer XenMobile de manière à ce qu'il utilise l'interface du fournisseur de services mobiles pour interroger les appareils BlackBerry et des appareils Exchange ActiveSync et effectuer des opérations.

Par exemple, votre entreprise peut compter plus de 1 000 utilisateurs et chaque utilisateur peut utiliser un ou plusieurs appareils. Lorsque vous signalez à chaque utilisateur qu'il doit inscrire ses appareils auprès de XenMobile à des fins de gestion, la console XenMobile indique le nombre d'appareils que les utilisateurs inscrivent. Si vous configurez ce paramètre, vous pouvez déterminer le nombre d'appareils qui se connectent au serveur Exchange. Cela vous permet d'effectuer ce qui suit :

- Déterminer si certains utilisateurs n'ont pas encore inscrit leurs appareils.
- Émettre des commandes sur les appareils utilisateur se connectant à un serveur Exchange, telles que l'effacement de données.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Dans **Serveur**, cliquez sur **Fournisseur de services mobiles**. La page **Fournisseur de services mobiles** s'affiche.



3. Configurez les paramètres suivants :

- **URL du service Web** : entrez l'adresse URL du service Web, par exemple, http://ServeurXmm/services/xdmservice
- **Nom d'utilisateur** : entrez le nom d'utilisateur au format domaine\administrateur
- **Mot de passe** : entrez le mot de passe.
- **Mettre à jour automatiquement les connexions aux appareils BlackBerry et ActiveSync** : activez cette option si vous souhaitez mettre à jour automatiquement les connexions aux appareils. La valeur par défaut est **OFF**.
- Cliquez sur **Tester la connexion** pour vérifier la connexion.

4. Cliquez sur **Enregistrer**.

SysLog

Feb 23, 2017

Vous pouvez configurer XenMobile de manière à envoyer les fichiers journaux à un serveur syslog. Vous avez besoin du nom d'hôte ou de l'adresse IP du serveur.

Syslog est un protocole de journalisation standard constitué de deux composants : un module d'audit (qui s'exécute sur le boîtier) et un serveur, qui peut être exécuté sur un système distant. Le protocole Syslog utilise le protocole UDP pour le transfert des données. Les événements d'administrateur et les événements d'utilisateur sont enregistrés.

Vous pouvez configurer le serveur afin de collecter les informations suivantes :

- Les journaux système qui contiennent un enregistrement des actions effectuées par XenMobile.
- Les journaux d'audit qui contiennent un enregistrement chronologique des activités système d'XenMobile.

Les informations de journal collectées par un serveur syslog à partir d'un boîtier sont stockées dans un fichier journal sous forme de messages. Ces messages contiennent généralement les informations suivantes :

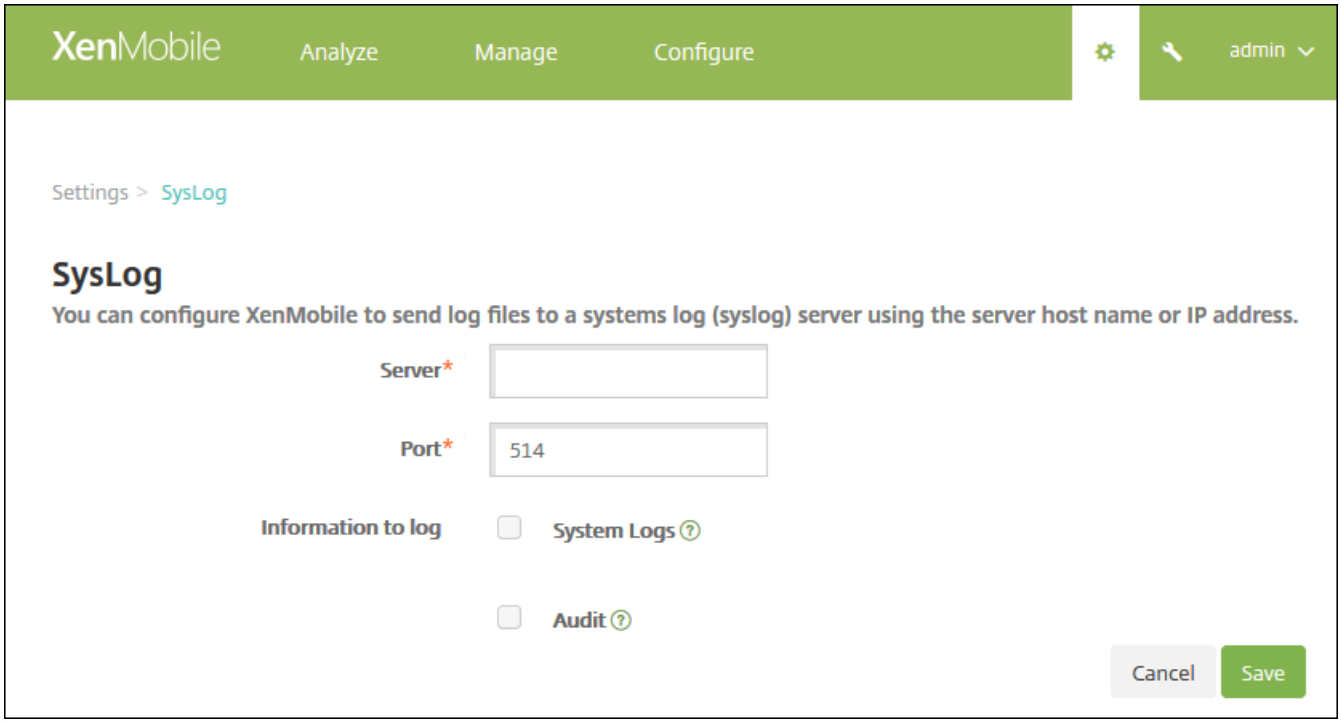
- L'adresse IP du boîtier qui a généré le message de journal
- Un horodatage
- Le type de message
- Le niveau de journalisation associé à un événement (critique, erreur, remarque, avertissement, informatif, débogage, alerte ou urgence)
- Les informations de message

Vous pouvez utiliser ces informations pour analyser la source de l'alerte et prendre des mesures correctives si nécessaire.

> ## Remarque
>
> Dans les déploiements XenMobile Service (cloud), Citrix ne prend pas en charge l'intégration syslog avec un serveur syslog local. Au lieu de cela, vous pouvez télécharger les journaux à partir de la page de support dans la console XenMobile. Ce faisant, vous devez cliquer sur **Tout télécharger** pour obtenir les journaux système. Pour de plus amples informations, consultez la section Visualisation et analyse des fichiers journaux dans XenMobile.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.

2. Cliquez sur **Syslog**. La page **Syslog** s'affiche.



3. Pour configurer ces paramètres :

- **Serveur** : entrez une adresse IP ou le nom de domaine complet (FQDN) de votre serveur syslog.
- **Port** : saisissez le numéro du port. Le port est défini par défaut sur 514.
- **Informations à consigner** : sélectionnez ou désélectionnez **Journaux système** et **Audit**.
  - Les journaux système contiennent les actions effectuées par XenMobile.
  - Les journaux d'audit contiennent un enregistrement chronologique des activités système de XenMobile.

4. Cliquez sur **Enregistrer**.

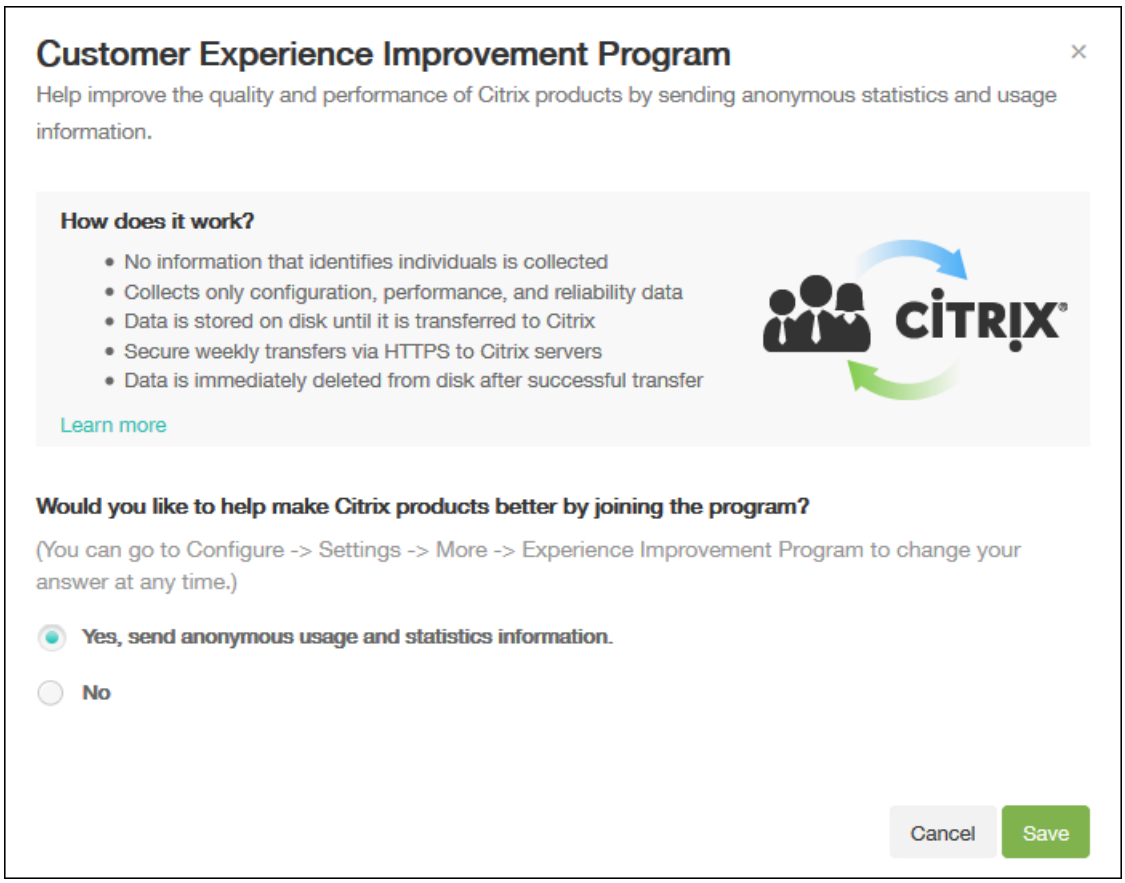
Programme d'amélioration de l'expérience utilisateur

Feb 23, 2017

Le Programme d'amélioration de l'expérience utilisateur Citrix (CEIP) rassemble des données de configuration et d'utilisation anonymes à partir de XenMobile et les envoie automatiquement à Citrix. Ces données permettent à Citrix d'améliorer la qualité, la fiabilité et les performances de XenMobile. La participation au programme CEIP est complètement volontaire. Lorsque vous installez XenMobile pour la première fois, ou lorsque vous installez une mise à jour, vous avez la possibilité de participer au programme CEIP. Lorsque vous acceptez de participer, les données de configuration sont généralement recueillies chaque semaine, et les données relatives aux performances et à l'utilisation sont recueillies toutes les heures. Les données sont stockées sur disque et transférées de manière sécurisée via HTTPS à Citrix une fois par semaine. Vous pouvez modifier votre participation au programme CEIP dans la console XenMobile. Pour plus d'informations sur le programme CEIP, veuillez consulter la section À propos du Programme d'amélioration de l'expérience utilisateur Citrix (CEIP).

Choisir de participer au programme CEIP

La première fois que vous installez XenMobile ou lorsque vous effectuez une mise à jour, la boîte de dialogue suivante vous invite à participer au programme.

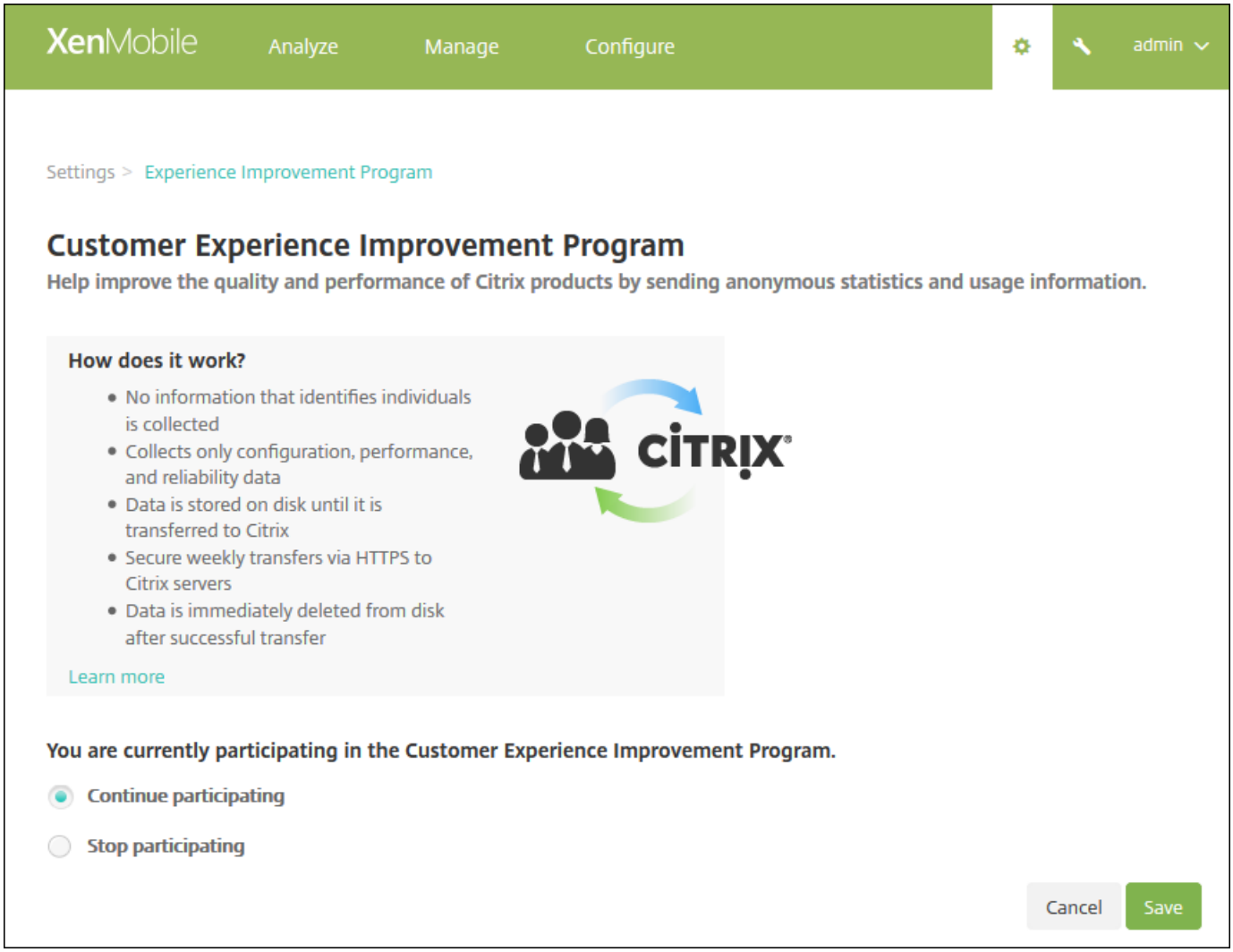


Modification de votre paramètre de participation au programme CEIP

1. Pour modifier votre paramètre de participation au programme CEIP, dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit de la console pour ouvrir la page **Paramètres**.

2. Dans **Serveur**, cliquez sur **Programme d'amélioration de l'expérience utilisateur**. La page **Programme d'amélioration**

de l'expérience utilisateur s'affiche. La page exacte qui s'affiche change selon que vous participez au programme CEIP ou non.



3. Si vous participez actuellement au programme CEIP et que vous voulez arrêter, cliquez sur **Ne plus participer au programme**.

4. Si vous ne participez pas actuellement au programme CEIP et que vous voulez y adhérer, cliquez sur **Participer au programme**.

5. Cliquez sur **Enregistrer**.

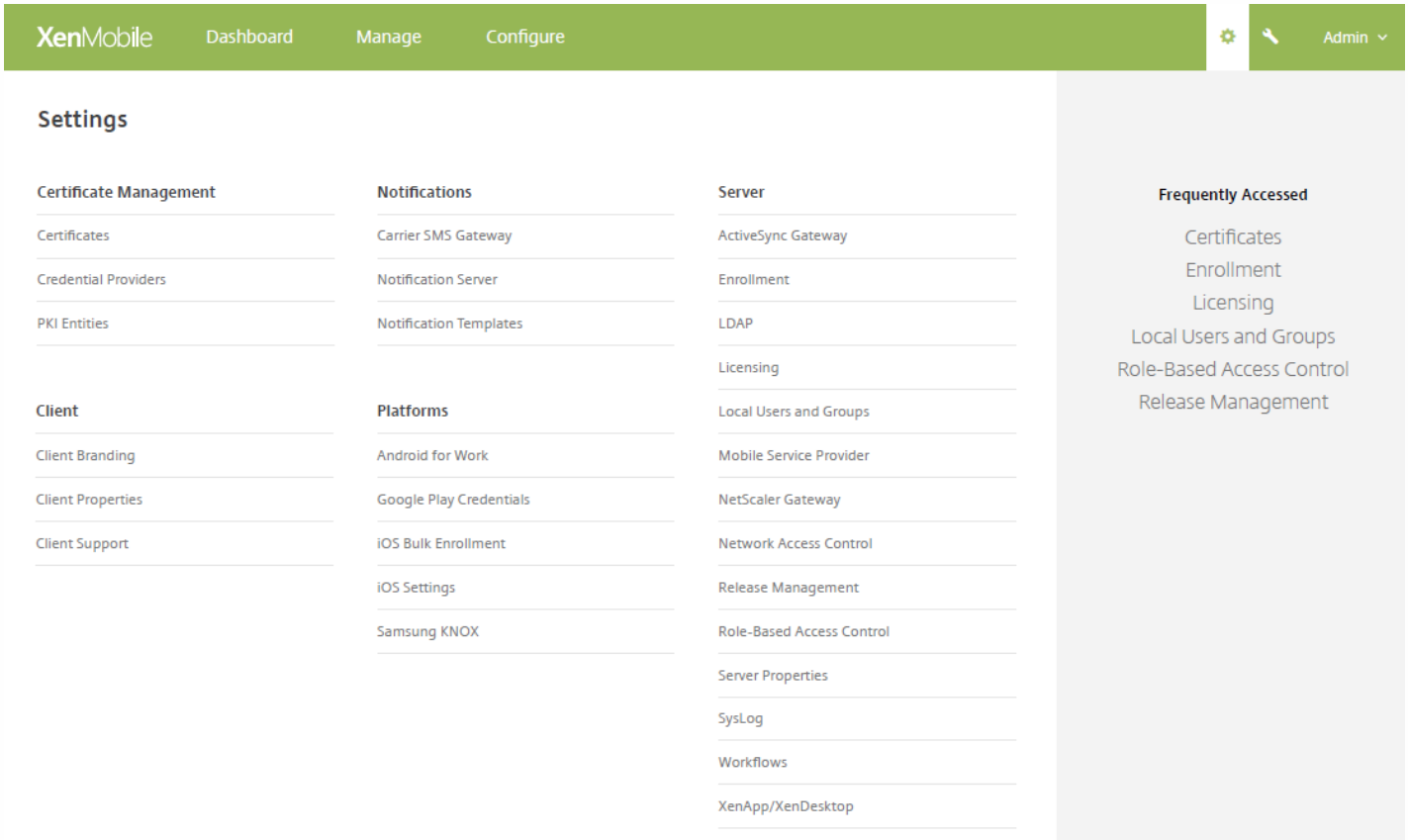
GotoAssist et Assistance à distance

Mar 31, 2017

Vous pouvez fournir aux utilisateurs différentes méthodes pour contacter le personnel d'assistance en fournissant des adresses e-mail et des numéros de téléphone. Lorsque des utilisateurs demandent une assistance depuis leurs appareils, ils voient les options que vous avez définies.

Vous pouvez également configurer la manière dont les utilisateurs envoient les journaux à l'assistance technique depuis leurs appareils. Vous pouvez configurer les journaux de manière à les envoyer directement ou par e-mail.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.



2. Sous **Client**, cliquez sur **Support client**. La boîte de dialogue **Support client** s'affiche.

3. Configurez les paramètres suivants pour configurer une adresse e-mail et numéro de téléphone et pour indiquer la façon dont l'appareil envoie les journaux à l'assistance technique.

- **Téléphone de l'assistance (support technique)** : entrez le numéro de téléphone pour votre service d'assistance.
- **E-mail de l'assistance (support technique)** : entrez l'adresse e-mail pour le contact de votre service d'assistance informatique.
- **Envoyer les journaux de l'appareil au service d'assistance** : indiquez si vous souhaitez que les journaux de l'appareil soient envoyés **directement** ou **par e-mail**. La valeur par défaut est **par e-mail**.

  - Lorsque vous sélectionnez **directement**, les paramètres liés au stockage des journaux sur ShareFile s'affichent. Si vous

activez l'option Stocker les journaux sur ShareFile, les journaux sont envoyés directement à ShareFile. Sinon, les journaux sont envoyés à XenMobile, puis envoyés par e-mail à l'assistance technique. L'option **Si l'envoi direct échoue, utiliser e-mail** s'affiche également ; elle est activée par défaut. Vous pouvez désactiver cette option si vous ne voulez pas utiliser la messagerie du client pour envoyer les journaux en cas de problème avec le serveur. Si vous désactivez cette option et qu'un problème serveur se produit, les journaux ne sont pas envoyés.

- Lorsque vous activez **par e-mail**, la messagerie du client est toujours utilisée pour envoyer les journaux.

4. Cliquez sur **Enregistrer**.

Assistance à distance

L'Assistance à distance permet aux représentants du service d'assistance de contrôler à distance des appareils mobiles Windows et Android gérés.

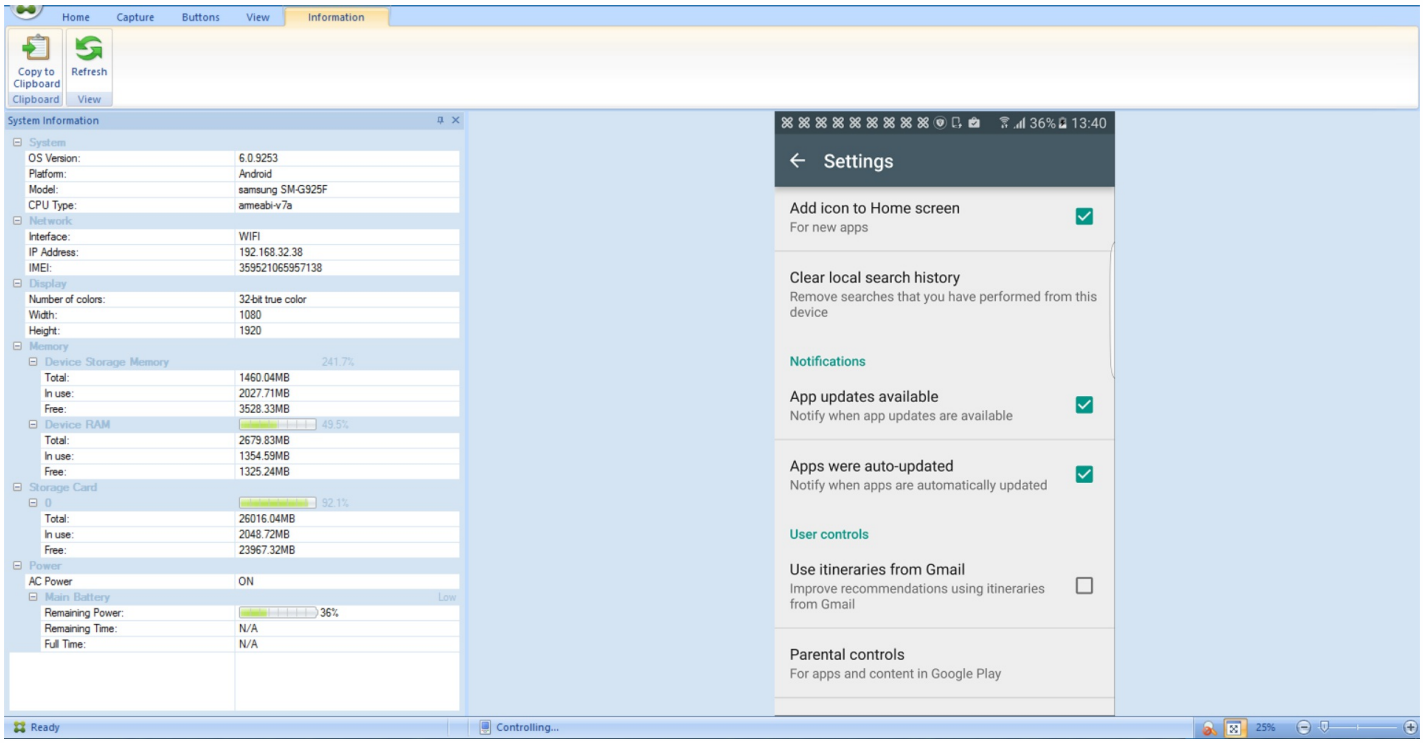
L'application Assistance à distance est disponible sur tous les appareils mobiles Windows et sur les appareils Android Samsung SAFE et les appareils autres que Samsung.

La capture d'écran est uniquement prise en charge sur les appareils Samsung KNOX.

Le contrôle à distance des appareils iOS n'est pas pris en charge.

Pendant une session de contrôle à distance :

- Les utilisateurs voient une icône sur leur appareil mobile indiquant qu'une session de contrôle à distance est active.
- Les utilisateurs de l'Assistance à distance voient la fenêtre de l'application Assistance à distance et une fenêtre de contrôle à distance qui affiche un rendu de l'appareil contrôlé.



Avec l'Assistance à distance, vous pouvez effectuer les opérations suivantes :

- Vous connecter à distance à l'appareil mobile d'un utilisateur et contrôler l'écran de l'utilisateur. Les utilisateurs peuvent

vous voir parcourir leur écran, ce qui peut s'avérer utile dans le cadre de formations.
- Parcourir et réparer un appareil distant en temps réel. Vous pouvez modifier les configurations, résoudre les problèmes liés au système d'exploitation, et désactiver ou arrêter les applications ou les processus qui posent problème.
- Isoler et contenir les menaces avant qu'elles ne se propagent sur d'autres appareils mobiles en désactivant à distance l'accès réseau, en arrêtant les processus indésirables et en supprimant les applications et les logiciels malveillants.
- Activer à distance la sonnerie et appeler le téléphone, pour aider l'utilisateur à localiser l'appareil. Si un utilisateur ne peut pas trouver l'appareil, vous pouvez effacer toutes les données qu'il contient pour vous assurer que vos données confidentielles ne sont pas compromises.

L'Assistance à distance permet également au personnel du service d'assistance technique d'effectuer ce qui suit :

- Afficher une liste de tous les appareils connectés à une ou plusieurs instances de XenMobile.
- Afficher des informations sur le système, notamment le modèle de l'appareil, niveau de système d'exploitation, numéro d'identité internationale d'équipement mobile (IMEI) et numéro de série, mémoire, état de la batterie et connectivité.
- Afficher les utilisateurs et les groupes pour XenMobile.
- Exécuter le gestionnaire des tâches de l'appareil afin de pouvoir afficher et mettre fin à des processus actifs et redémarrer l'appareil mobile.
- Exécuter le transfert de fichiers à distance, notamment le transfert de fichiers bidirectionnel entre les appareils mobiles et un serveur de fichiers central.
- Télécharger et installer des logiciels par lots sur un ou plusieurs appareils mobiles.
- Configurer des paramètres de clé de registre sur l'appareil.
- Optimiser le temps de réponse sur les réseaux cellulaires à faible bande passante à l'aide d'un contrôle à distance de l'écran de l'appareil en temps réel.
- Afficher le thème de l'appareil de la plupart des marques et modèles d'appareils mobiles. Afficher un éditeur de thème afin d'ajouter de nouveaux modèles d'appareils et de mapper les touches physiques.
- Activer la capture d'écran sur l'appareil, enregistrer et lire avec la possibilité de capturer une séquence d'interactions sur l'appareil afin de créer un fichier vidéo AVI.
- Tenir des réunions en direct à l'aide d'un tableau blanc partagé, utiliser des communications audio VoIP et effectuer des chats entre utilisateurs mobiles et l'équipe d'assistance.

Configuration système requise pour l'Assistance à distance

Le logiciel Assistance à distance est installé sur les ordinateurs Windows qui répondent aux conditions suivantes. Pour les exigences en matière de port, consultez la section Configuration requise pour les ports.

Plates-formes prises en charge :

- Intel Xeon/Pentium 4 - 1 GHz minimum
- 512 Mo minimum de RAM
- 100 Mo minimum d'espace disque libre

Systèmes d'exploitation pris en charge :

- Microsoft Windows Server 2003 Standard Edition ou Enterprise Edition SP1 ou version ultérieure
- Microsoft Windows 2000 Professionnel SP4
- Microsoft Windows XP SP2 ou version ultérieure
- Microsoft Windows Vista SP1 ou version ultérieure
- Microsoft Windows 10
- Microsoft Windows 8

- Microsoft Windows 7

Pour installer le logiciel Assistance à distance

1. Pour télécharger le programme d'installation de l'assistance à distance, accédez à la page de téléchargement de XenMobile 10 et connectez-vous à votre compte.
2. Développez **Tools** et téléchargez XenMobile Remote Support v9.
   Le nom de fichier de l'Assistance à distance est XenMobileRemoteSupport-9.0.0.35265.exe.
3. Cliquez deux fois sur le programme d'installation de l'Assistance à distance et suivez les instructions de l'assistant d'installation.

Pour installer l'Assistance à distance à partir de la ligne de commande :

Exécutez la commande suivante :

RemoteSupport.exe /S

où *RemoteSupport* correspond au nom du programme d'installation. Par exemple :

XenMobileRemoteSupport-9.0.0.35265.exe/S

Vous pouvez utiliser les variables suivantes lors de l'installation du logiciel Assistance à distance :

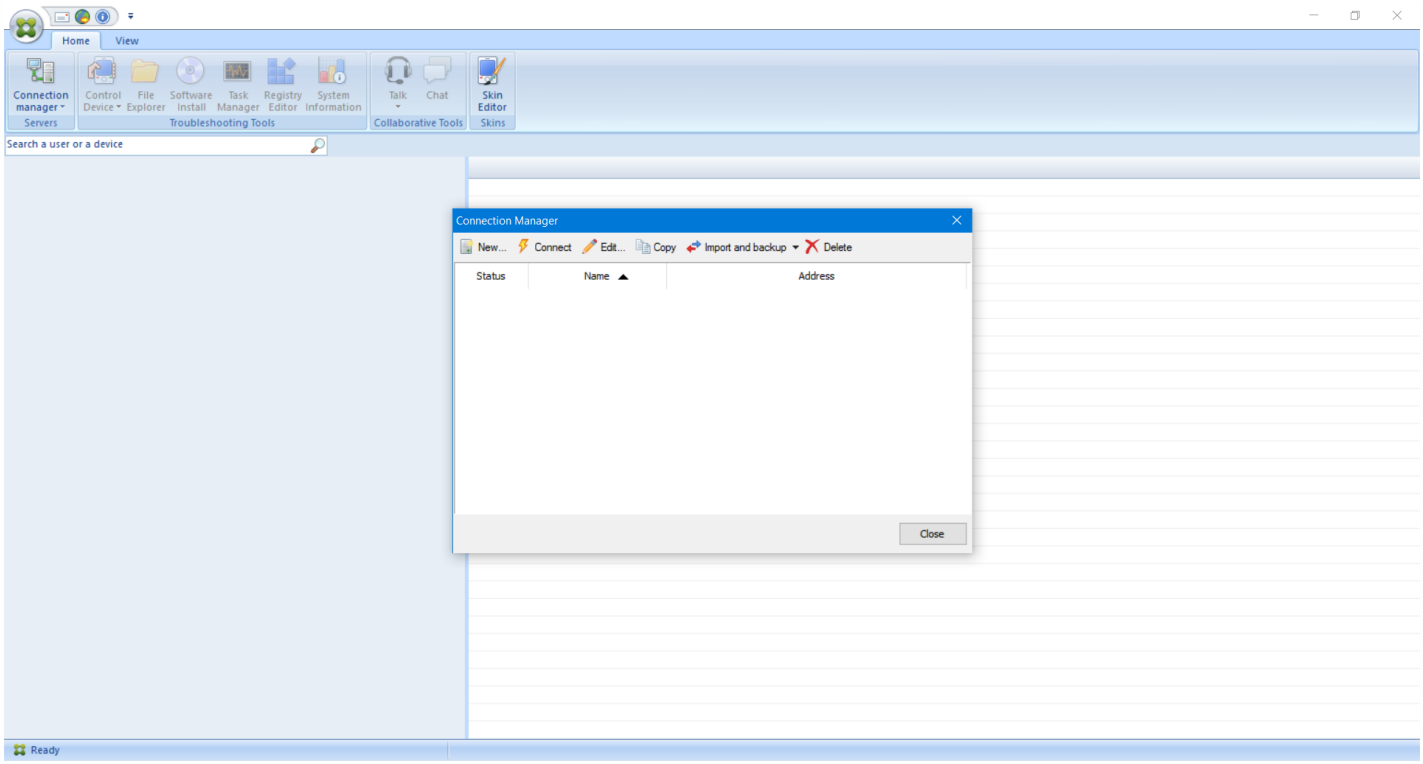
- /S: pour installer le logiciel Assistance à distance de manière silencieuse avec les paramètres par défaut.
- /D=dir: pour spécifier un répertoire d'installation personnalisé.

Pour connecter l'Assistance à distance à XenMobile

Pour établir des connexions d'assistance à distance avec des appareils gérés, vous devez ajouter une connexion depuis l'Assistance à distance vers un ou plusieurs serveurs XenMobile qui gèrent les appareils. Cette connexion s'exécute sur un tunnel applicatif que vous définissez dans la stratégie de tunnel MDM, une stratégie pour appareils Android et Windows Mobile/CE. Définissez le tunnel applicatif avant de pouvoir connecter l'Assistance à distance à XenMobile. Pour plus de détails, consultez la section Stratégies de tunnel applicatif.

1. Démarrez le logiciel Assistance à distance et utilisez vos informations d'identification XenMobile pour ouvrir une session.

2. Dans **Gestionnaire de connexions**, cliquez sur **Nouveau**.



3. Dans la boîte de dialogue **Connection Configuration**, sur l'onglet **Server**, entrez les valeurs suivantes :

    a. Dans **Configuration name**, entrez un nom pour l'entrée de configuration.

    b. Dans **Server IP address or name**, entrez l'adresse IP ou le nom DNS du serveur XenMobile.

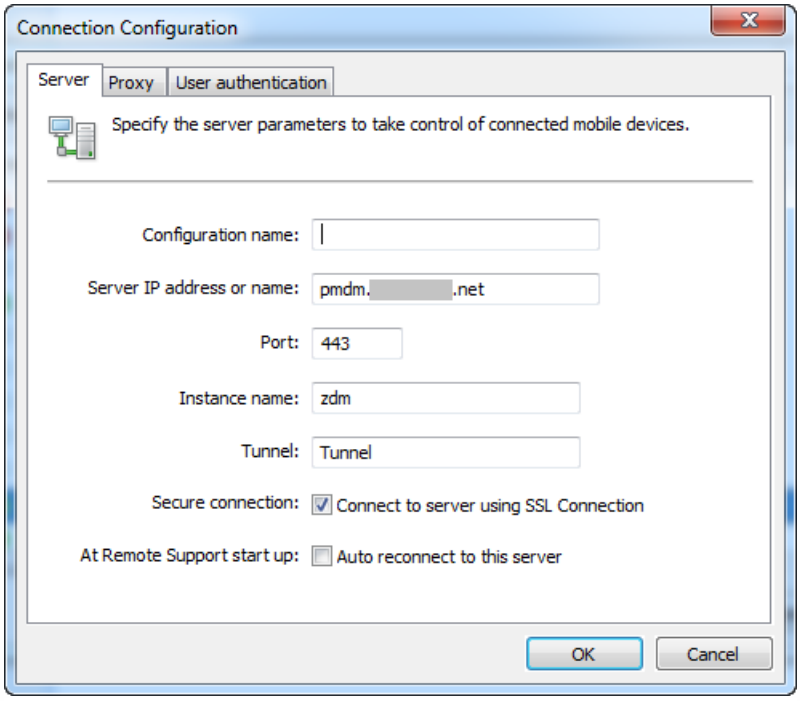
    c. Dans **Port**, entrez un numéro de port TCP, comme défini dans la configuration du serveur XenMobile.

    d. Dans **Instance name**, si XenMobile fait partie d'un déploiement Multi-Tenant, entrez un nom d'instance.

    e. Dans **Tunnel**, entrez le nom de la Stratégie de tunnel.

    f. Sélectionnez la case **Connect to server using SSL Connection**.

    g. Sélectionnez la case **Auto reconnect to this server** pour vous connecter au serveur XenMobile configuré chaque fois que l'application Assistance à distance démarre.



4. Sur l'onglet **Proxy**, sélectionnez **Use a http proxy server** et entrez les informations suivantes :

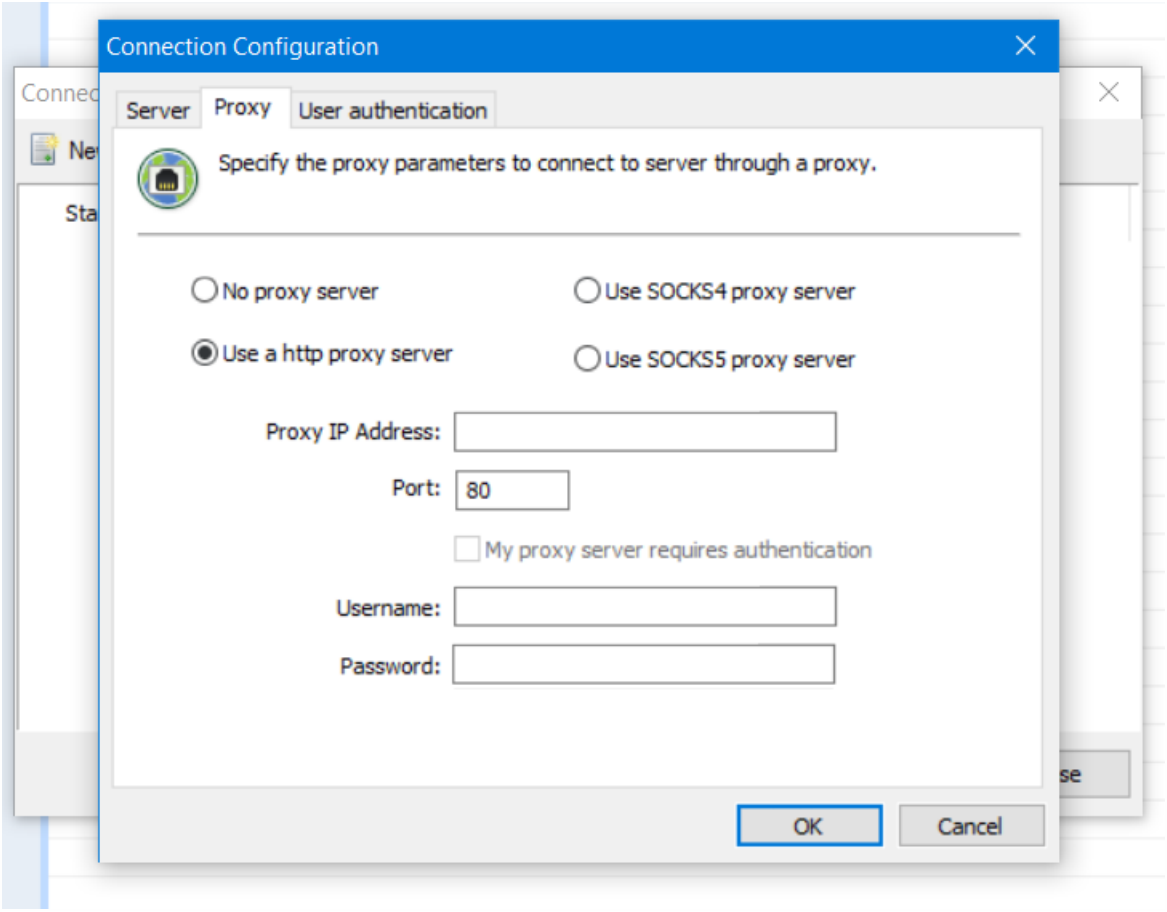
    a. Dans **Proxy IP Address**, saisissez l'adresse IP du serveur proxy.

    b. Dans **Port**, saisissez le numéro de port TCP utilisé par le proxy.

    c. Sélectionnez la case **My proxy server requires authentication** si le serveur proxy requiert une authentification pour autoriser le trafic.

    d. Dans **Username**, saisissez le nom de l'utilisateur qui doit être authentifié sur le serveur proxy.

    e. Dans **Password**, saisissez le mot de passe qui doit être authentifié sur le serveur proxy.



5. Sur l'onglet **User Authentication**, sélectionnez la case **Remember my login and password** et entrez les informations d'identification.

6. Cliquez sur **OK**.

Pour vous connecter à XenMobile, double-cliquez sur la connexion que vous avez créée, puis entrez le nom d'utilisateur et le mot de passe que vous avez configurés pour la connexion.

Pour activer l'assistance à distance des appareils Samsung KNOX

Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX. Vous pouvez configurer deux types d'assistance :

- Assistance à distance de base : cette option vous permet d'afficher des informations de diagnostic sur l'appareil, telles que les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés, etc.
- Assistance à distance premium : cette option vous permet de contrôler à distance l'écran de l'appareil, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.

  Avec l'assistance Premium, vous devez configurer la stratégie de clé de licence MDM Samsung dans la console XenMobile. Lorsque vous configurez cette stratégie, sélectionnez uniquement la plate-forme **Samsung KNOX**. Vous n'avez pas

besoin configurer la plate-forme Samsung SAFE pour ce scénario, étant donné que la clé ELM est déployée automatiquement sur les appareils Samsung lorsqu'ils s'inscrivent dans XenMobile. Pour de plus amples informations, consultez la section Clé de licence MDM Samsung.

Pour de plus amples informations sur la configuration de la stratégie Assistance à distance, consultez la Stratégie d'assistance à distance.

Pour utiliser une session d'Assistance à distance

Lorsque vous démarrez l'Assistance à distance, la partie gauche de la fenêtre de l'application Assistance à distance présente des groupes d'utilisateurs XenMobile, comme défini dans la console XenMobile. Par défaut, seuls les groupes contenant des utilisateurs qui sont actuellement connectés sont affichés. Vous pouvez afficher l'appareil pour chaque utilisateur en regard de l'entrée de l'utilisateur.

1. Pour afficher tous les utilisateurs, développez chaque groupe à partir de la colonne de gauche.
   Les utilisateurs actuellement connectés au serveur XenMobile sont indiqués par une icône verte.
2. Pour afficher tous les utilisateurs, y compris ceux qui ne sont pas actuellement connectés, cliquez sur **View** et sélectionnez **Non-connected devices.**
   Les utilisateurs non connectés s'affichent sans la petite icône verte.

Les appareils connectés au serveur XenMobile, mais non affectés à un utilisateur s'affichent en mode anonyme. (La chaîne **Anonymous** s'affiche dans la liste). Vous pouvez contrôler ces appareils de la même façon que l'appareil d'un utilisateur connecté.

Pour contrôler un appareil, sélectionnez l'appareil en cliquant sur sa ligne, puis cliquez sur **Control Device**. Un rendu de l'appareil s'affiche dans la fenêtre de l'Assistance à distance. Vous pouvez interagir avec un appareil contrôlé de l'une des manières suivantes :

- Contrôler l'écran de l'appareil, y compris les couleurs, dans la fenêtre principale, où dans une fenêtre séparée flottante.
- Établir une session VoIP entre le support technique et l'utilisateur. Configurer les paramètres VoIP.
- Établir une session de chat avec l'utilisateur.
- Accéder au Gestionnaire des tâches de l'appareil pour gérer des éléments tels que l'utilisation de la mémoire, l'utilisation d'UC et les applications en cours d'exécution.
- Explorer les répertoires locaux de l'appareil mobile. Transférer des fichiers.
- Modifier le registre de l'appareil sur des appareils mobiles Windows.
- Afficher les informations système de l'appareil et tous les logiciels installés.
- Mettre à jour de l'état de connexion de l'appareil mobile avec le serveur XenMobile.

Créer les options d'assistance Secure Hub et GoToAssist

Feb 23, 2017

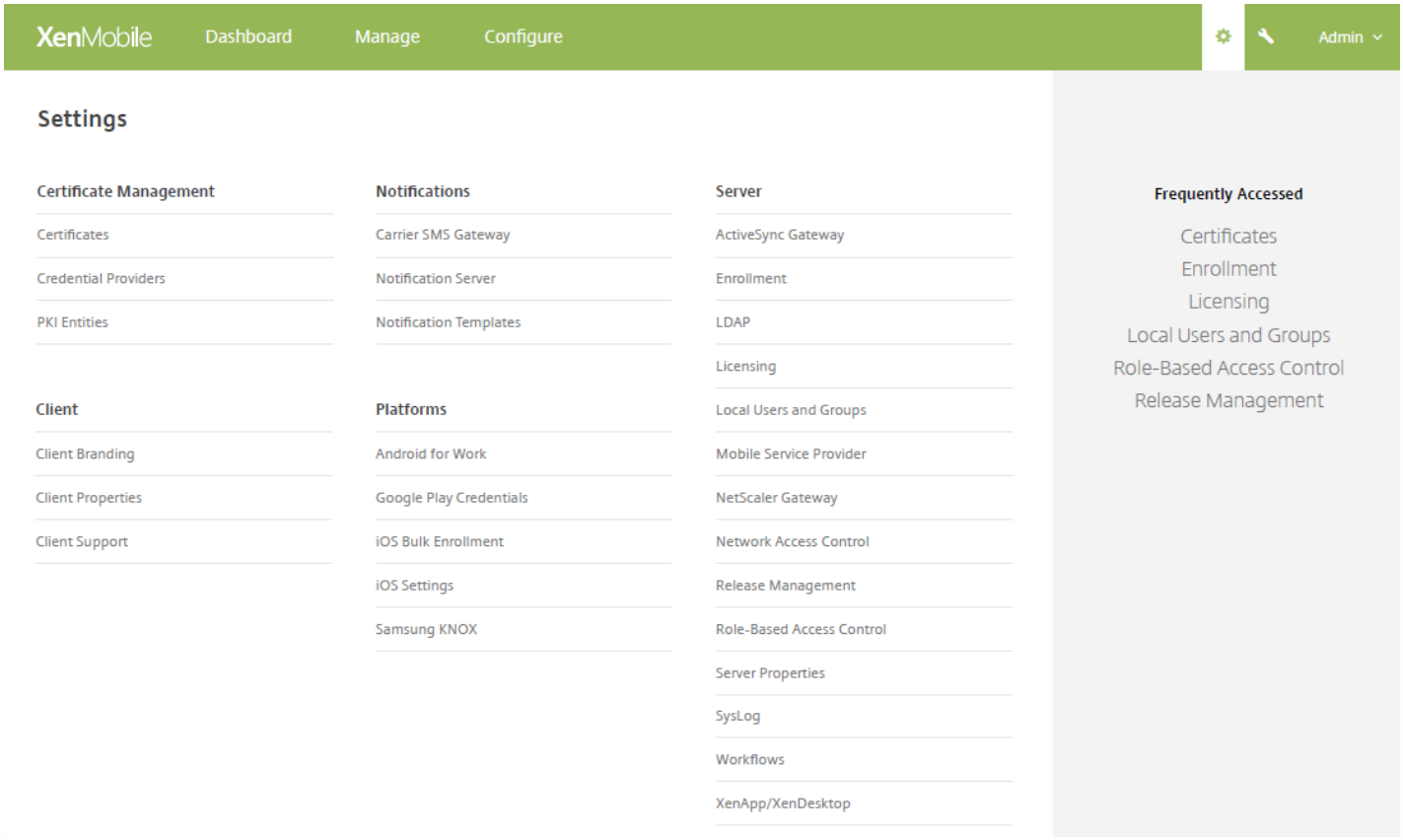
Vous pouvez configurer la manière dont les applications s'affichent dans le magasin et ajouter un logo pour personnaliser Secure Hub et XenMobile Store sur les appareils mobiles iOS et Android.

Remarque : avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

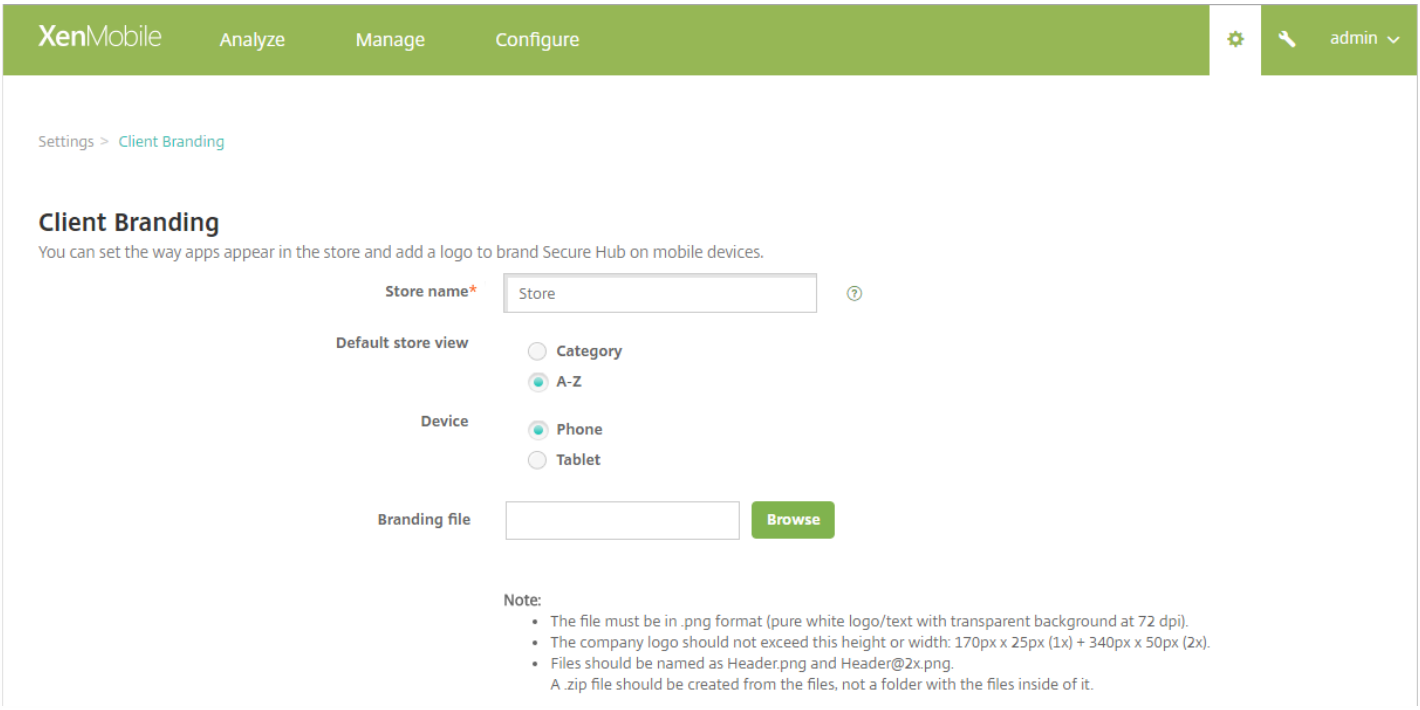
L'image personnalisée doit répondre à ces exigences :

- Le fichier doit être au format .png.
- Utilisez un logo blanc pur ou du texte avec un arrière-plan transparent à 72 ppp.
- Le logo de la société ne doit pas dépasser cette hauteur ou largeur : 170 px x 25 px (1x) et 340 px x 50 px (2x).
- Appelez les fichiers Header.png et Header@2x.png
- Créez un fichier .zip à partir des fichiers, et non un dossier contenant les fichiers.

1. Dans la console XenMobile, cliquez sur l'icône d'engrenage dans le coin supérieur droit. La page **Paramètres** s'affiche.



2. Sous **Client**, cliquez sur **Personnalisation du client**. La page **Personnalisation du client** s'affiche.



3. Configurez les paramètres suivants :

- **Nom du magasin** : le nom s'affiche dans les informations de compte de l'utilisateur. La modification du nom change également l'adresse URL utilisée pour accéder aux services du magasin. Il n'est généralement pas nécessaire de modifier le nom par défaut.
- **Vue du magasin par défaut** : sélectionnez **Catégorie** ou **A-Z**. La valeur par défaut est **A-Z**.
- **Appareil** : sélectionnez **Téléphone** ou **Tablette**. La valeur par défaut est **Téléphone**.
- **Fichier de personnalisation** : pour sélectionner une image ou un fichier .zip d'images à utiliser pour la personnalisation, cliquez sur **Parcourir** et accédez à l'emplacement du fichier.

4. Cliquez sur **Enregistrer**.

Pour déployer ce paquetage auprès des appareils de vos utilisateurs, vous devez créer un paquetage de déploiement et le déployer.

Tests de connectivité

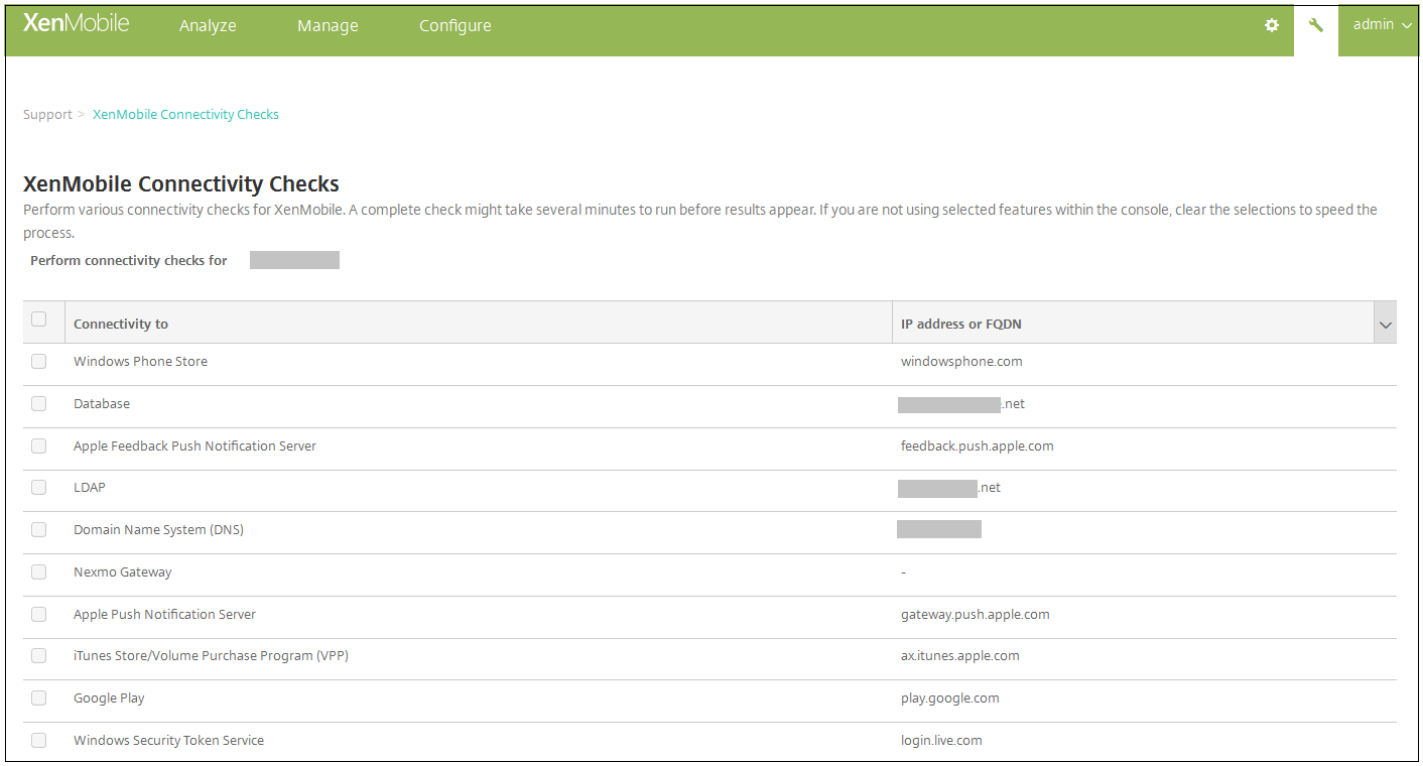
Mar 31, 2017

Depuis la page **Support** de XenMobile, vous pouvez vérifier la connexion de XenMobile à NetScaler Gateway et à d'autres serveurs et emplacements.

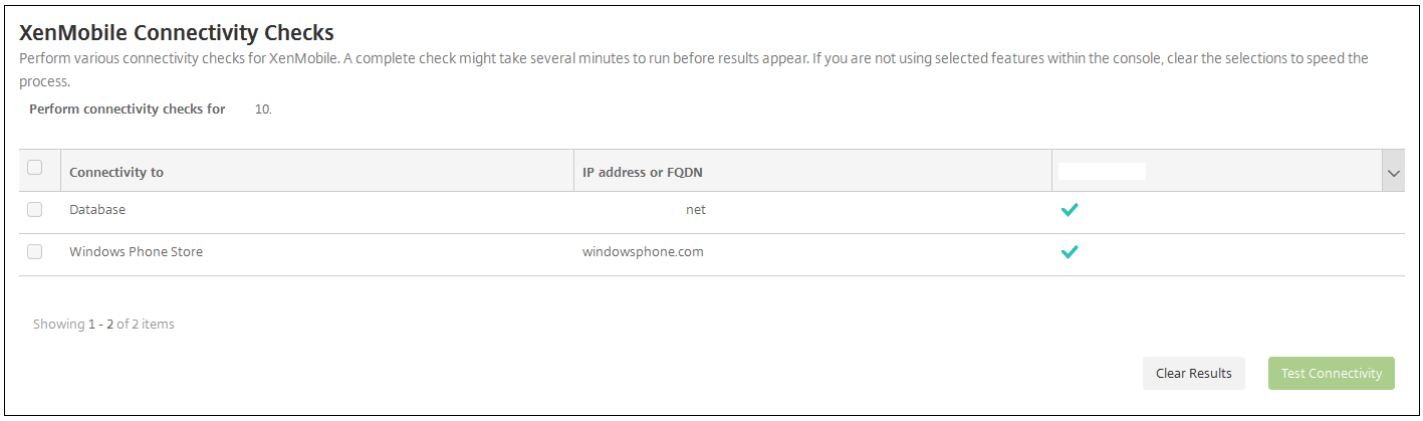
Réalisation de contrôles de connectivité dans XenMobile

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page **Support** s'affiche.

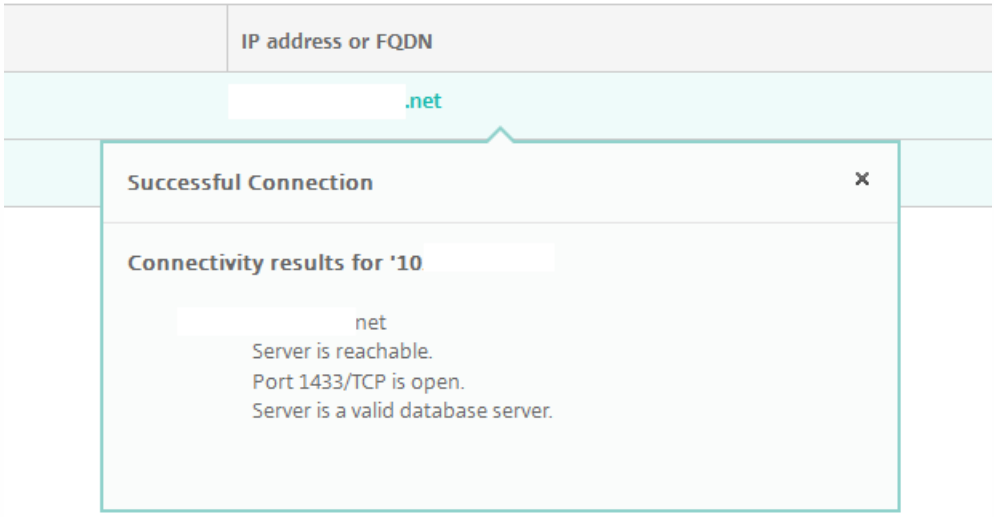
2. Sous **Diagnostics**, cliquez sur **Test de la connectivité XenMobile**.La page **Test de la connectivité XenMobile** s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



2. Sélectionnez les serveurs que vous souhaitez inclure dans le test de connectivité, puis cliquez sur **Tester la connectivité**.La page des résultats du test s'affiche.

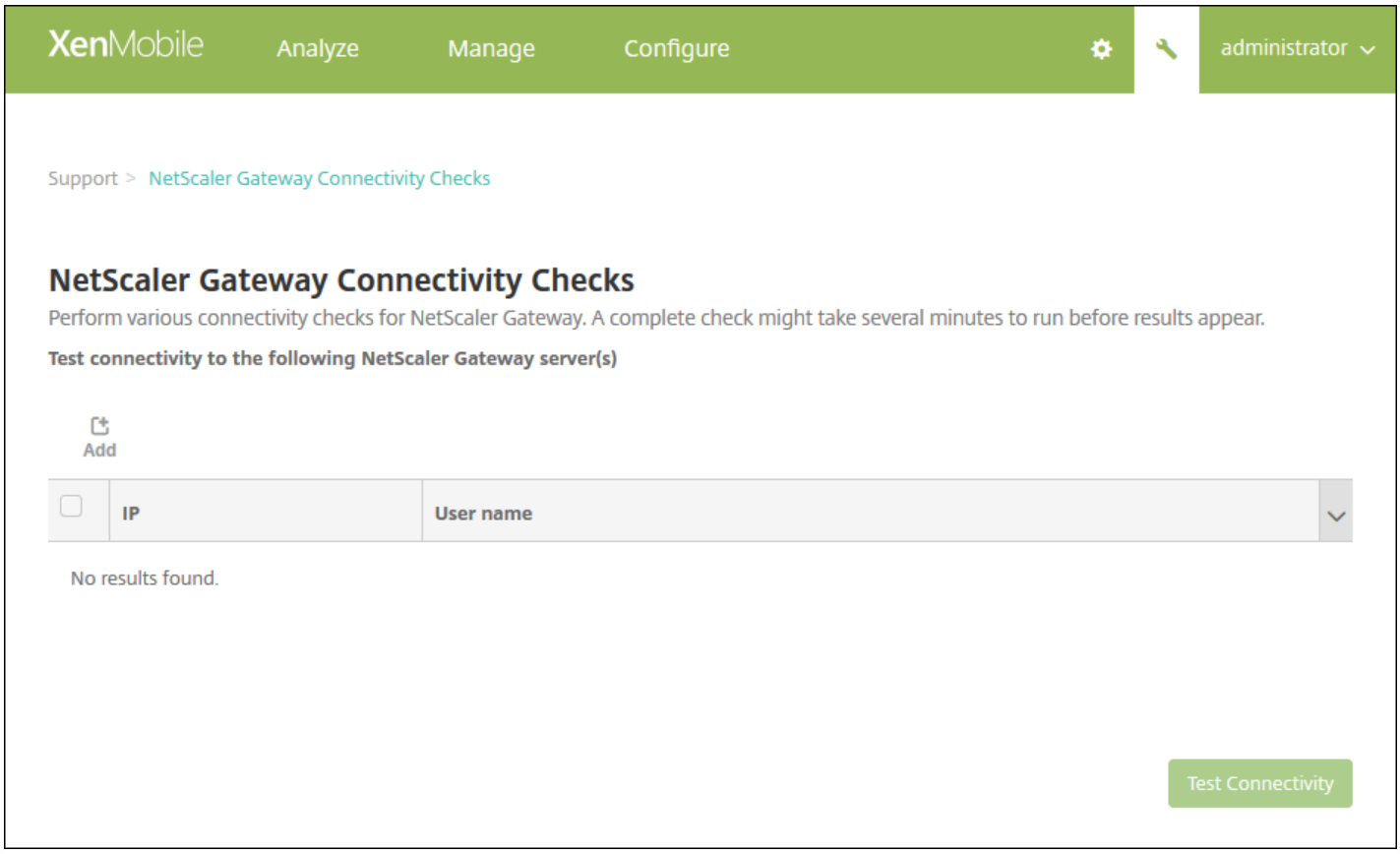


3. Sélectionnez un serveur dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.

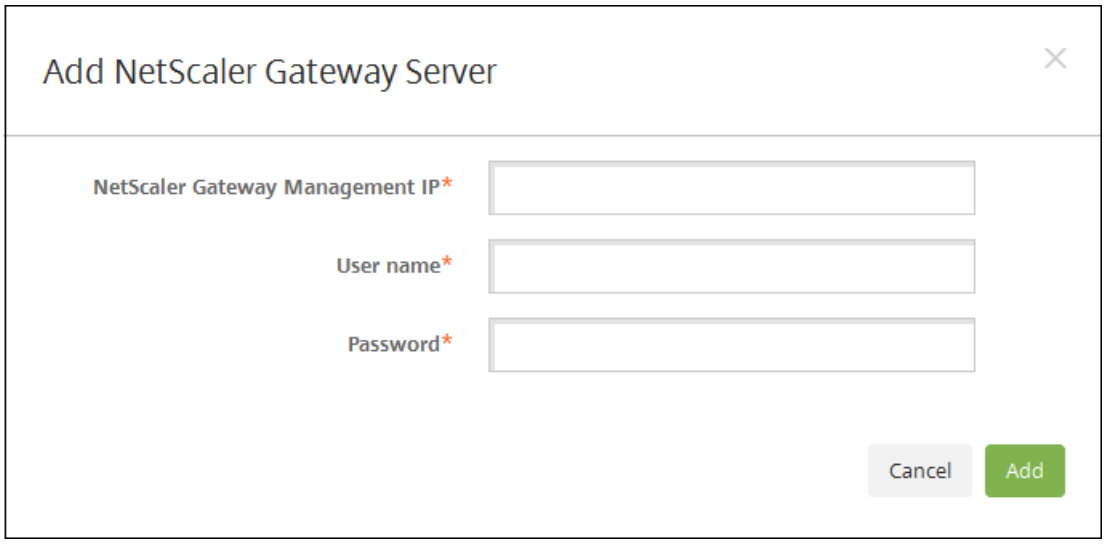


Réalisation de contrôles de connectivité pour NetScaler Gateway

1. Sur la page **Support**, sous **Diagnostics**, cliquez sur **Test de la connectivité NetScaler Gateway**.La page **Test de la connectivité NetScaler Gateway** s'affiche. Le tableau est vide si vous n'avez pas ajouté de serveurs NetScaler Gateway.



2. Cliquez sur **Ajouter**.La boîte de dialogue **Ajouter un serveur NetScaler Gateway** s'affiche.



3. Dans **Adresse IP de gestion de NetScaler Gateway**, entrez l'adresse IP de gestion du serveur exécutant NetScaler Gateway que vous voulez tester.

Remarque : si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui est déjà ajouté, l'adresse IP est renseignée.

4. Tapez vos informations d'identification d'administrateur pour ce NetScaler Gateway.

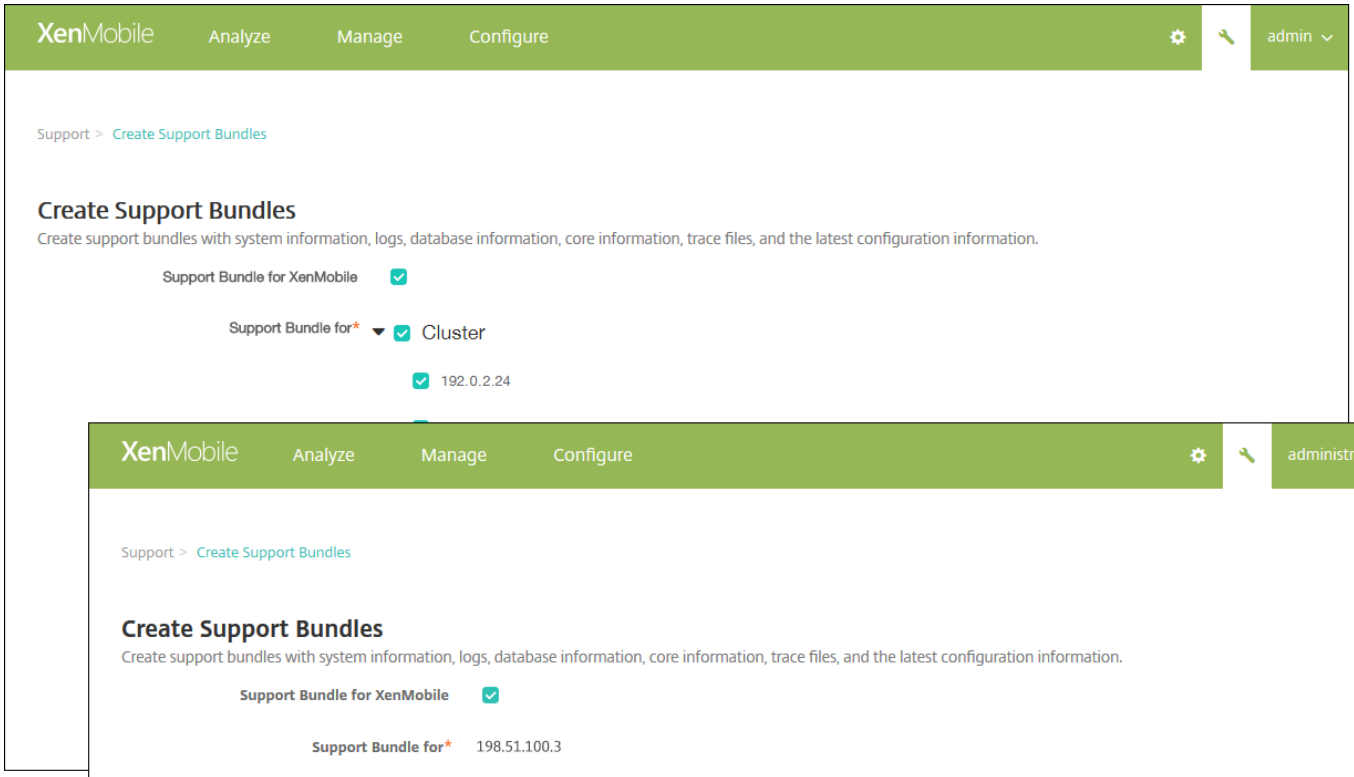
Remarque : si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui a déjà été ajouté, le nom d'utilisateur est renseigné.

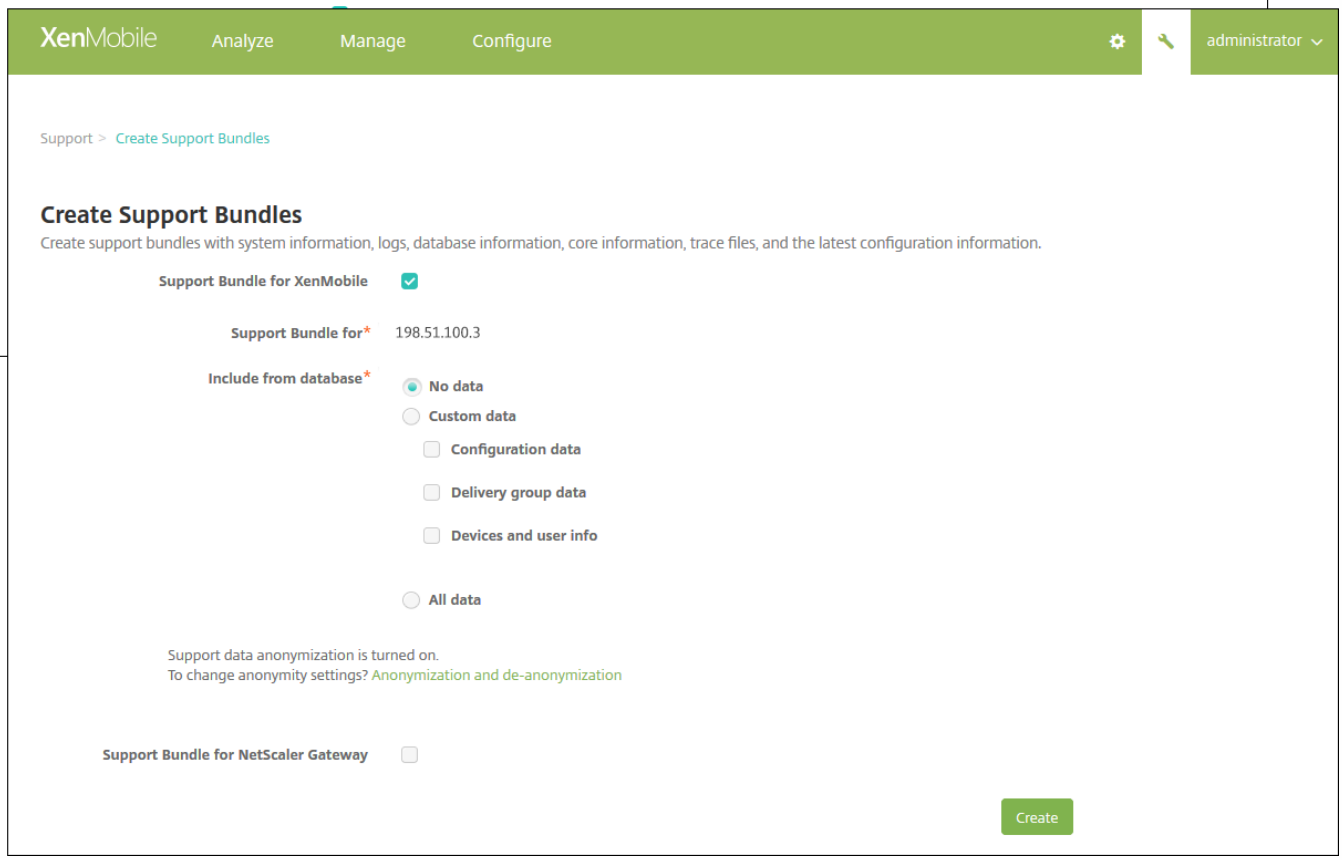
5. Cliquez sur **Ajouter**.La passerelle NetScaler Gateway est ajoutée au tableau sur la page **Test de la connectivité NetScaler Gateway**.

6. Sélectionnez le serveur NetScaler Gateway et cliquez sur **Tester la connectivité**.

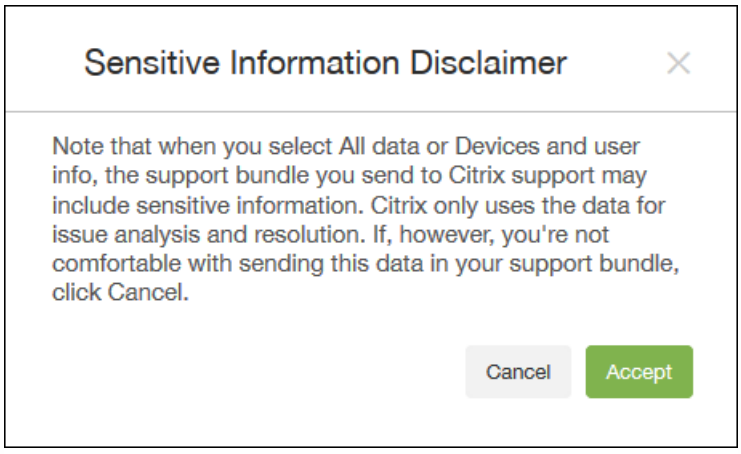
Les résultats s'affichent dans la table Résultats du test.

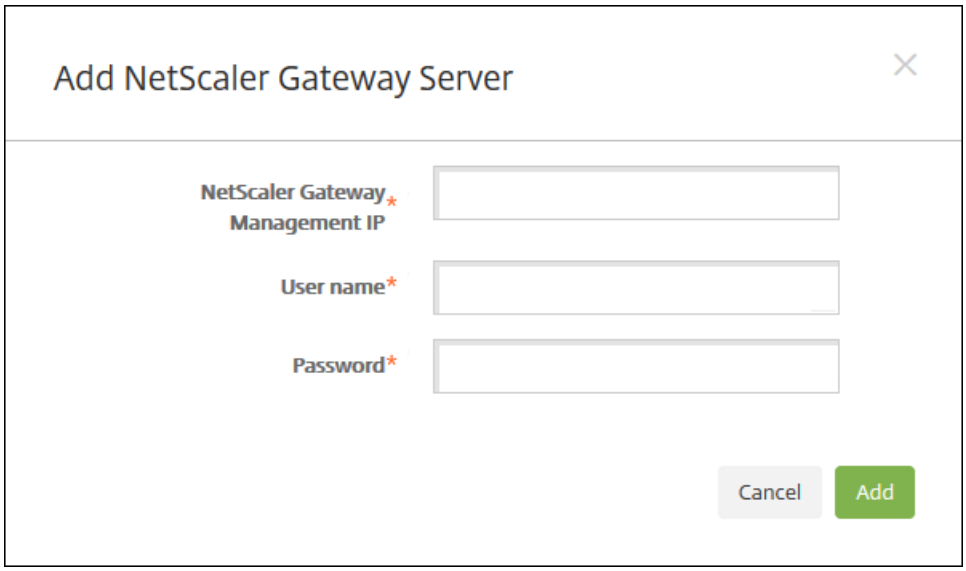
7. Sélectionnez un serveur dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.

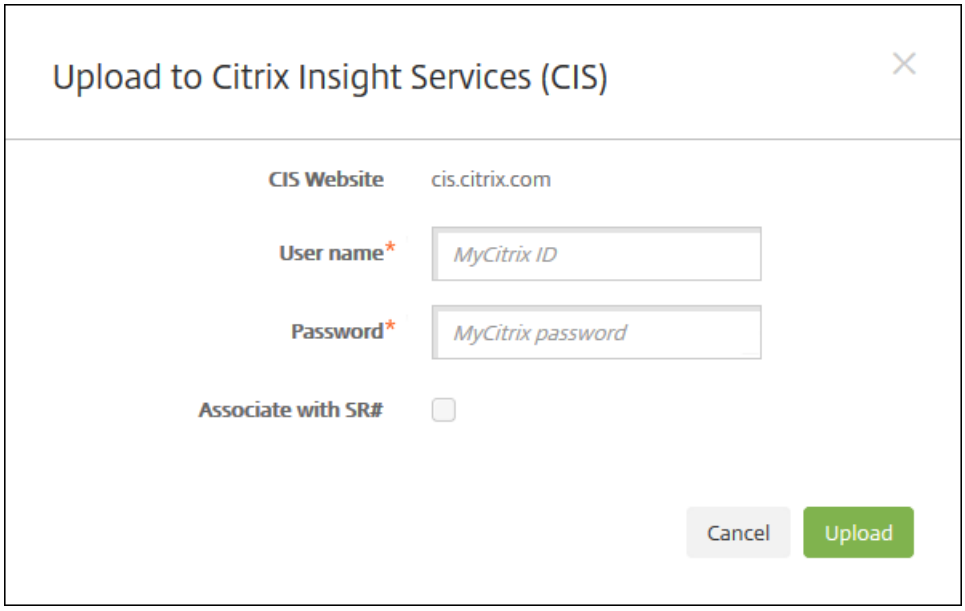




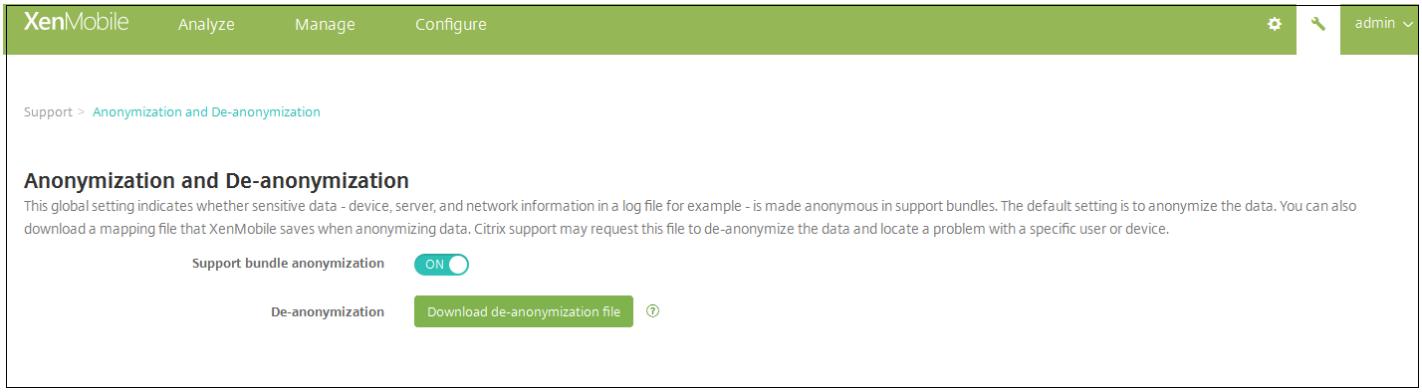
-
-
  -
  -
  -
-

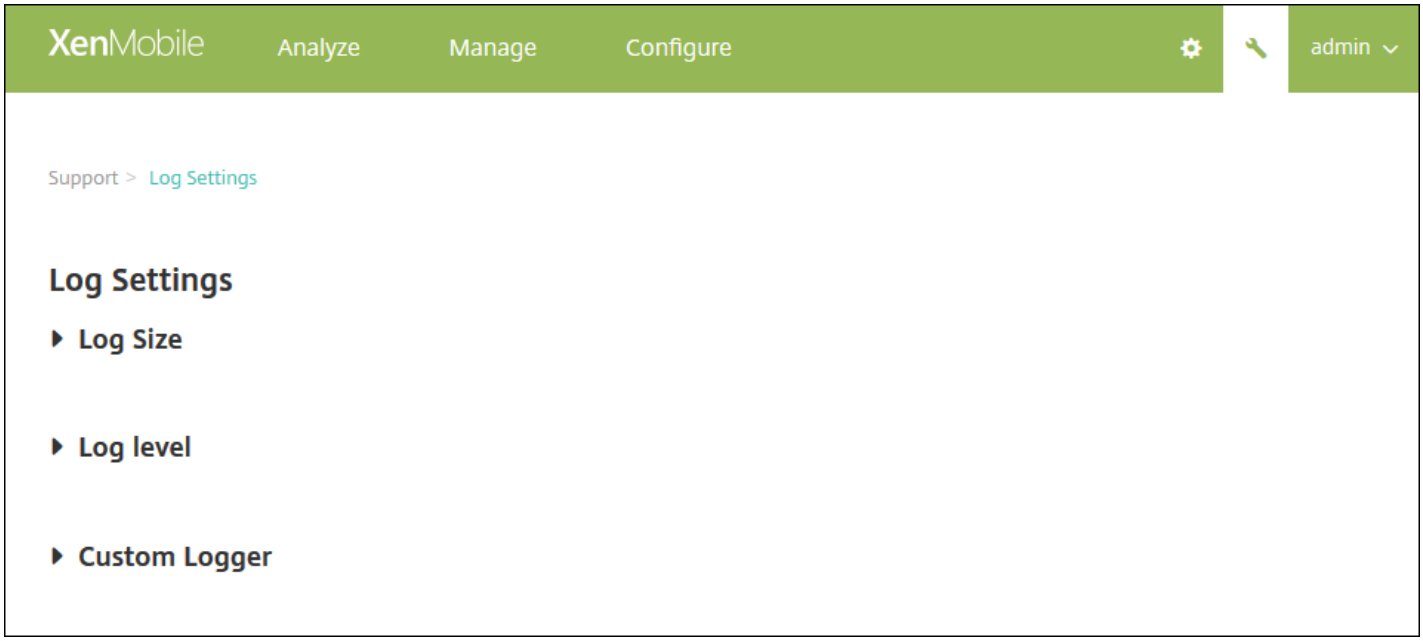




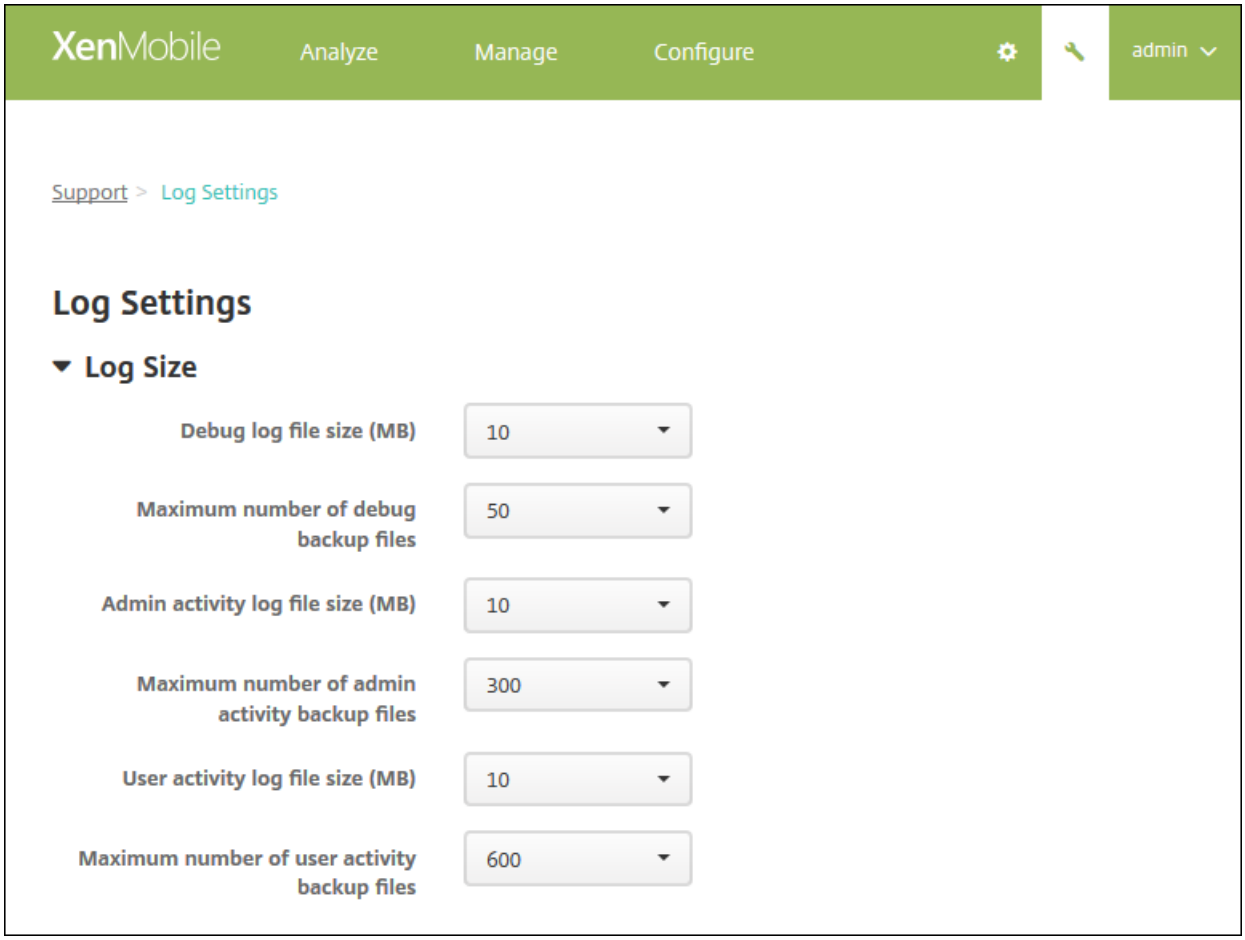


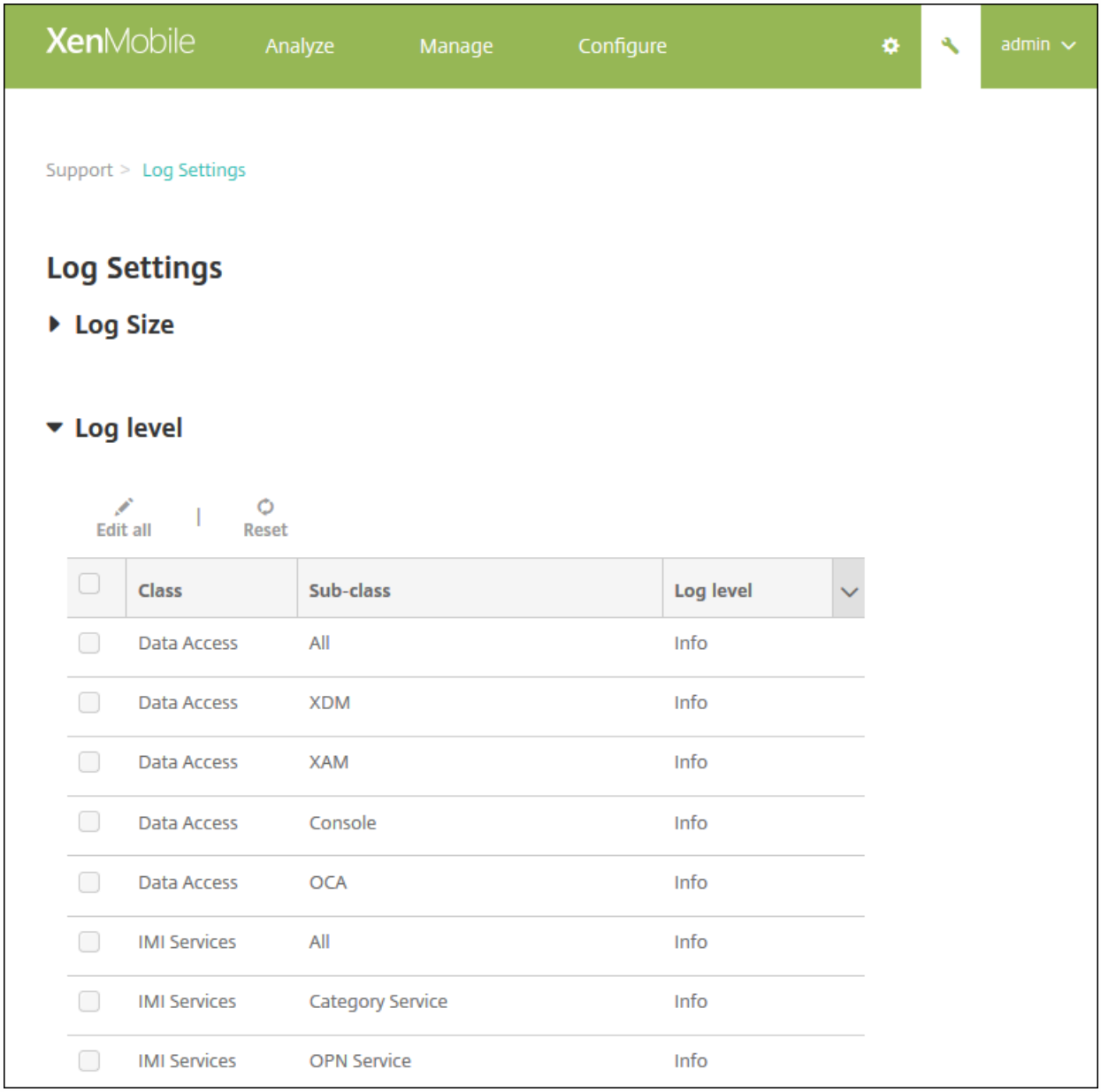
-
-



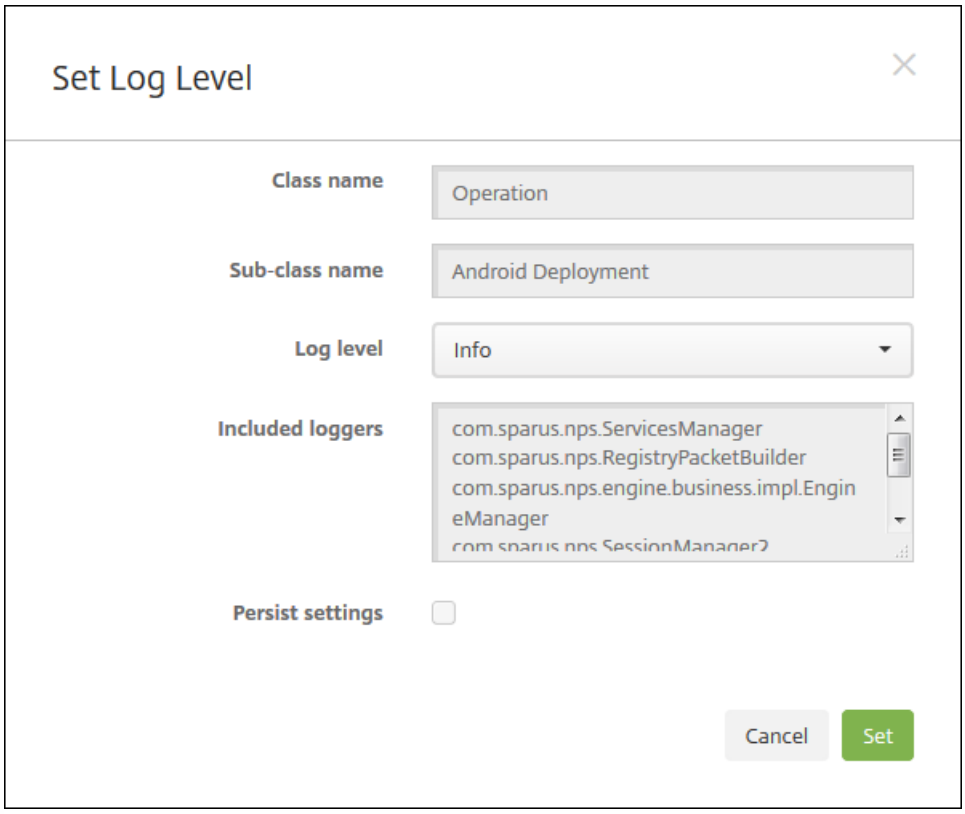


-
-
-

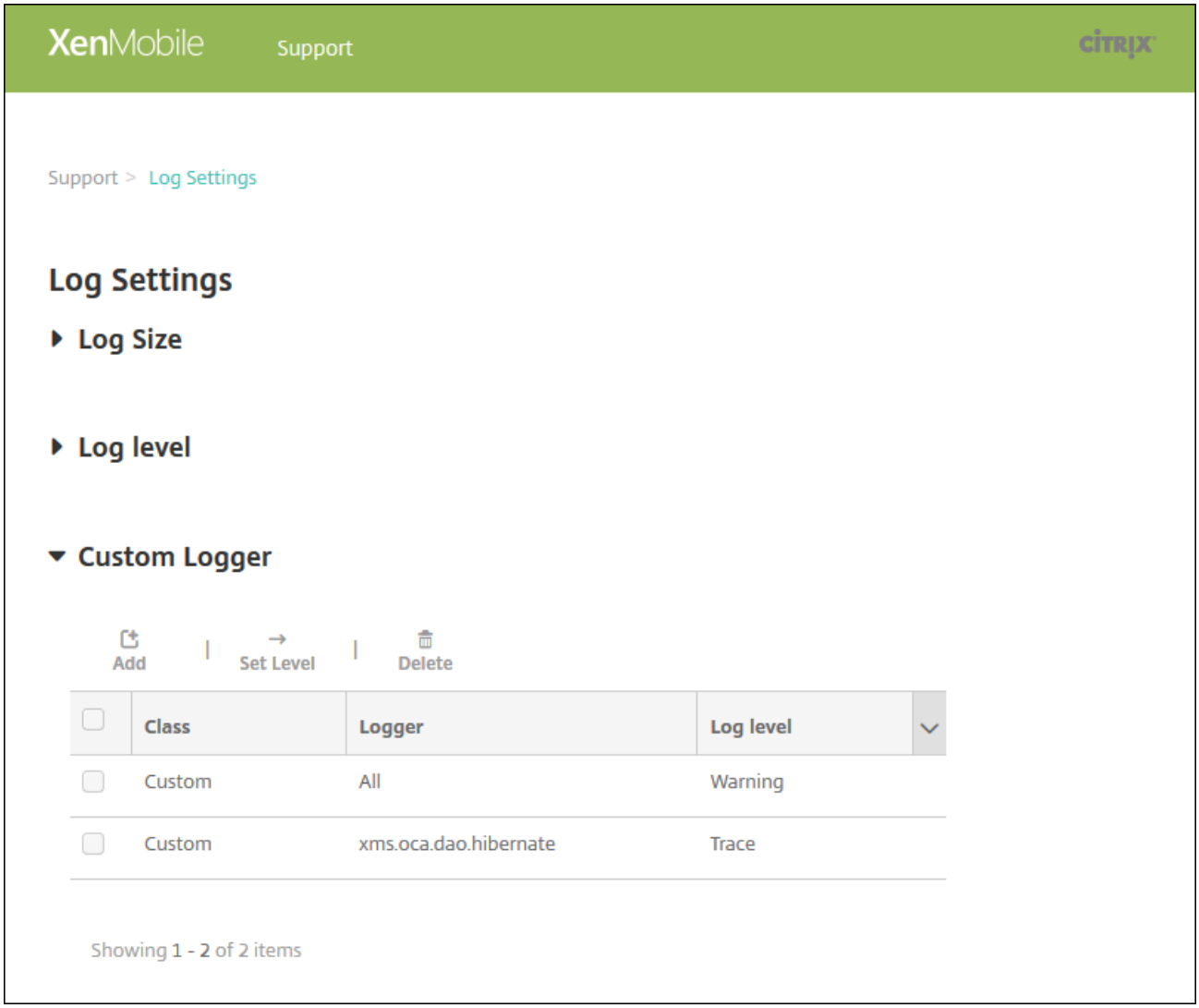


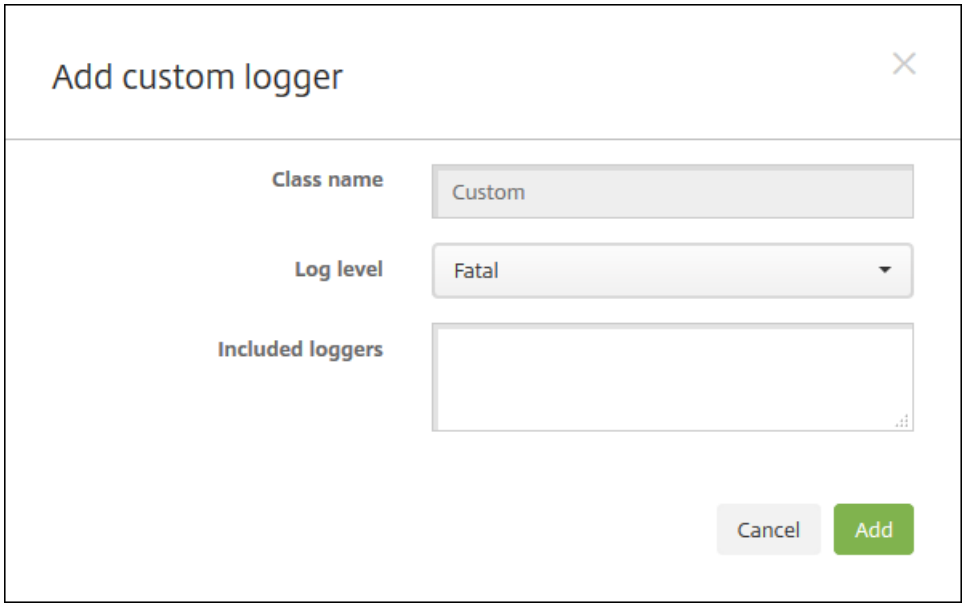


-
-

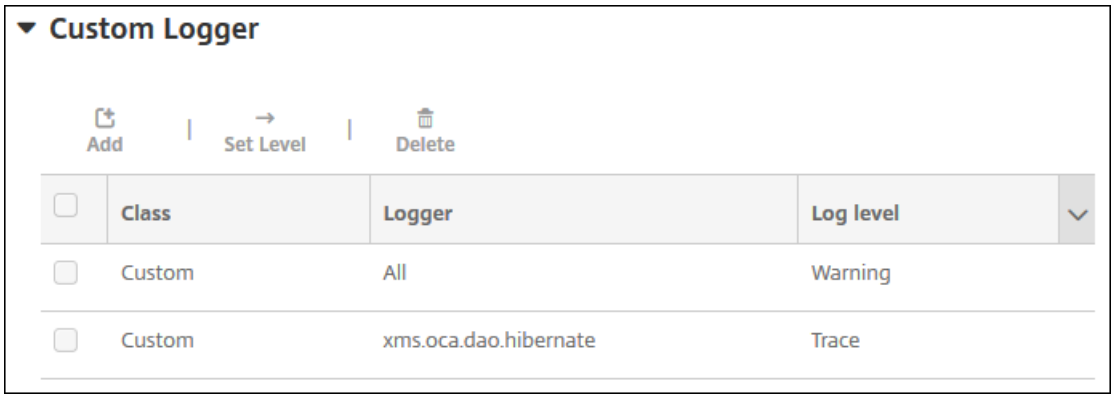


-
-
-
  -
  -
  -
  -
  -
  -
  -
-
-

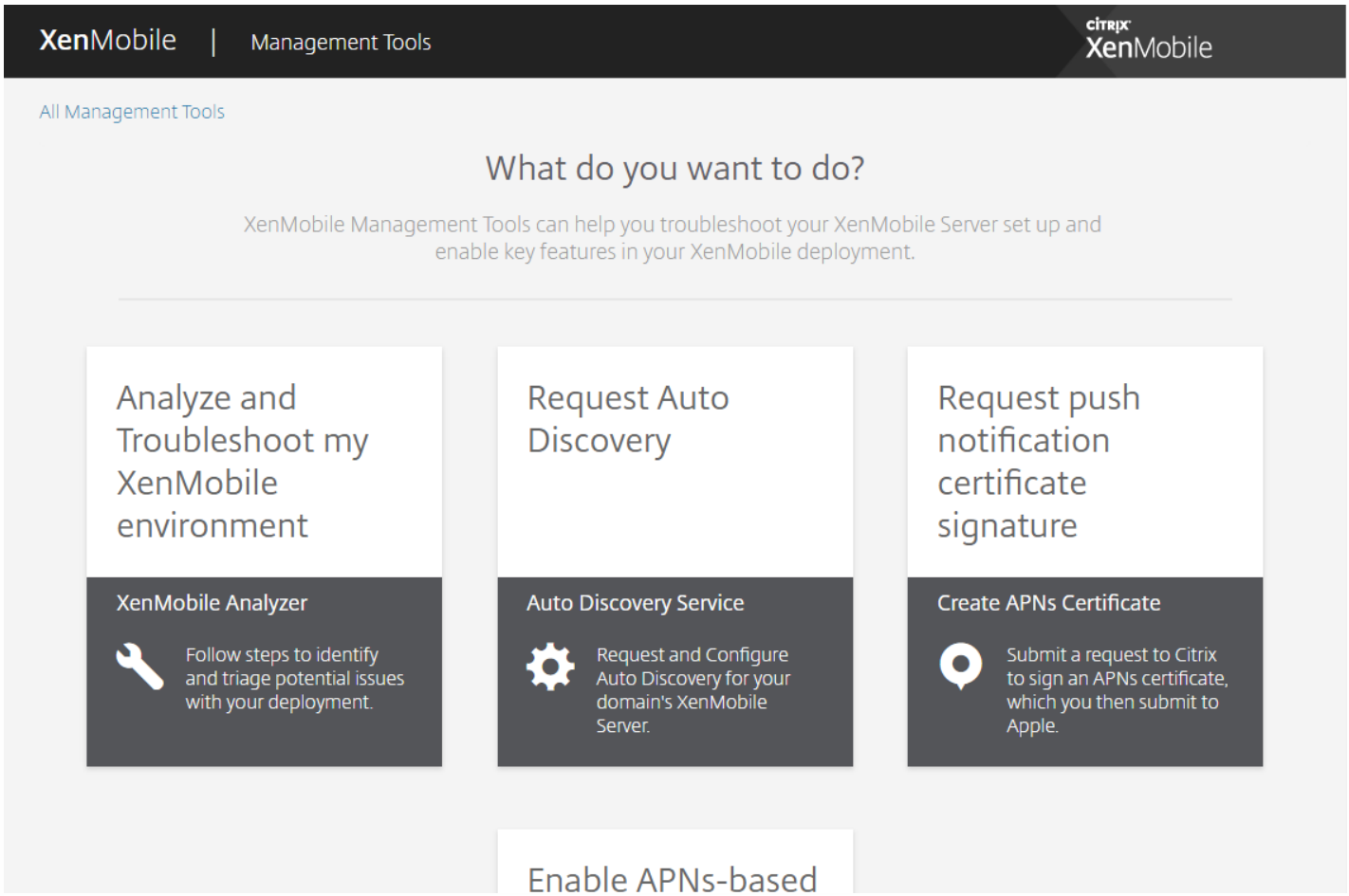


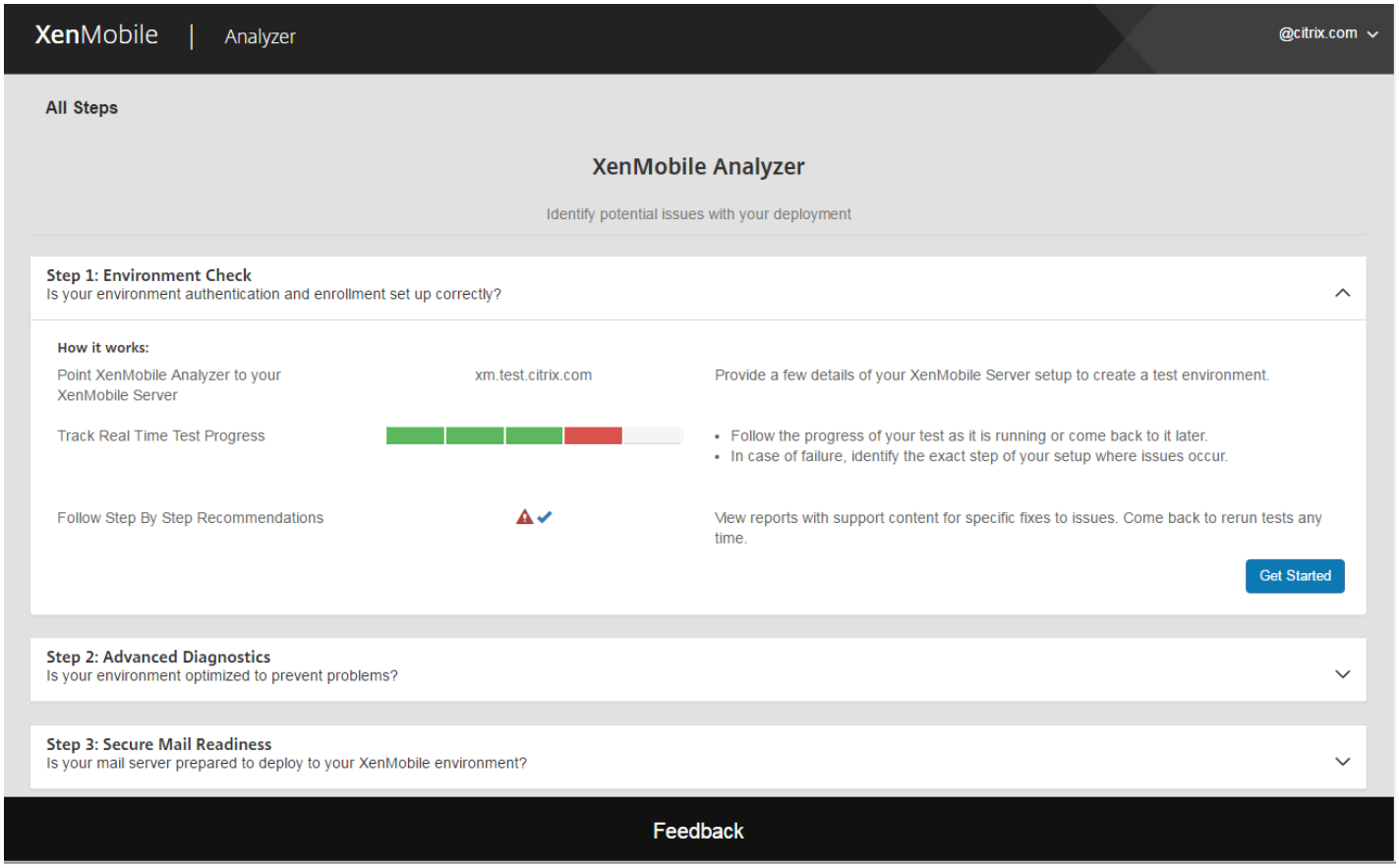


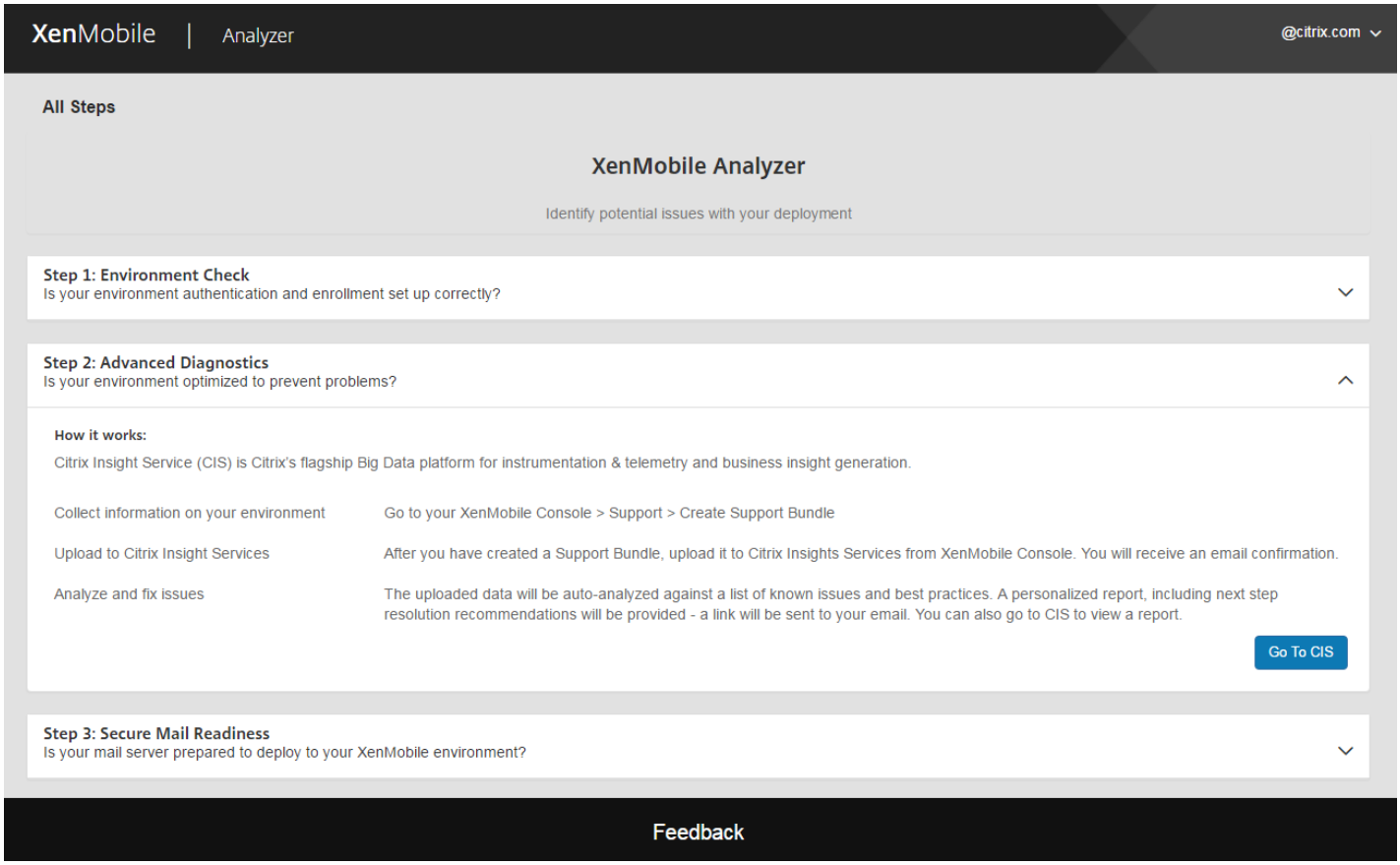
-
-
  -
  -
  -
  -
  -
  -
  -
-

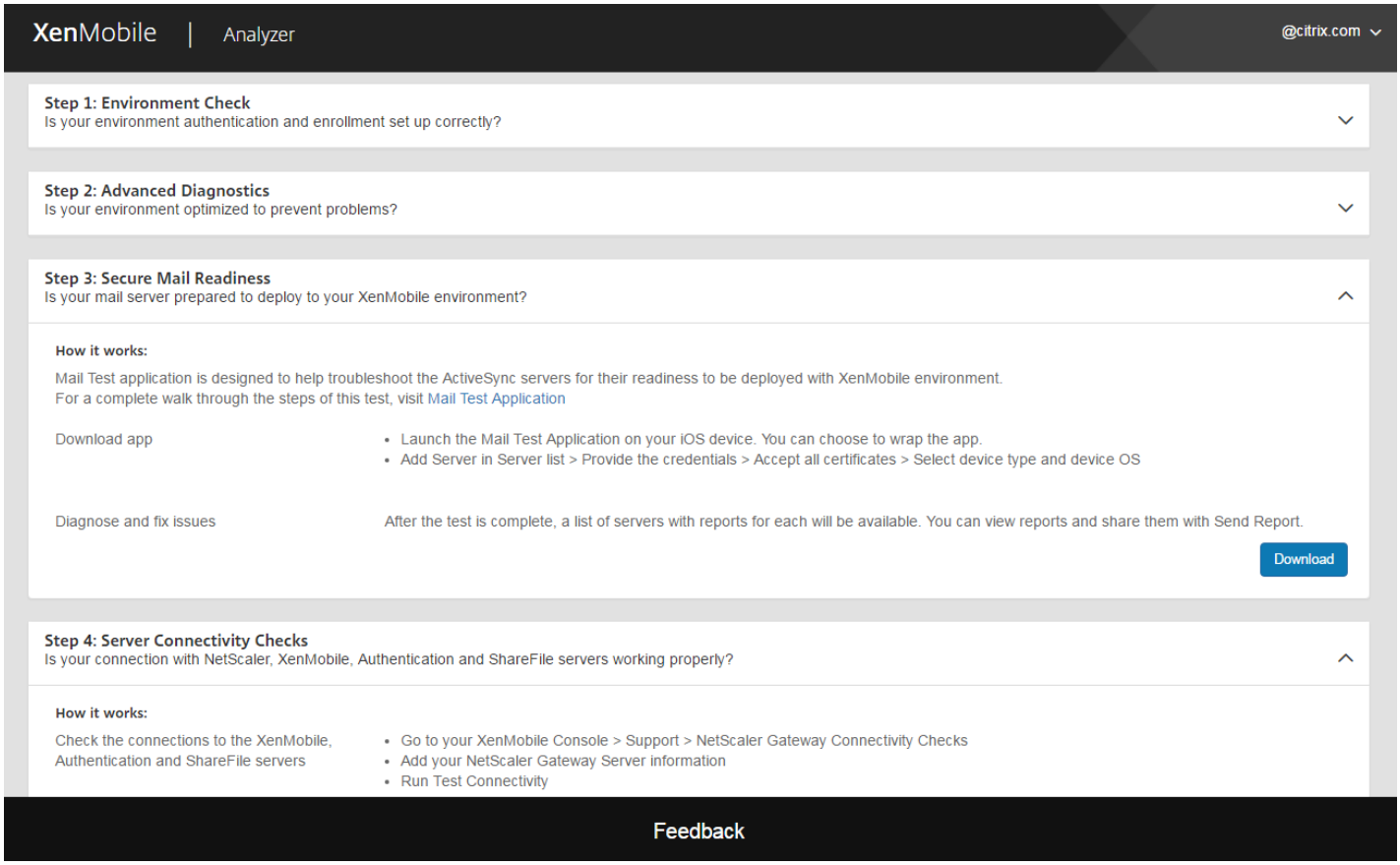


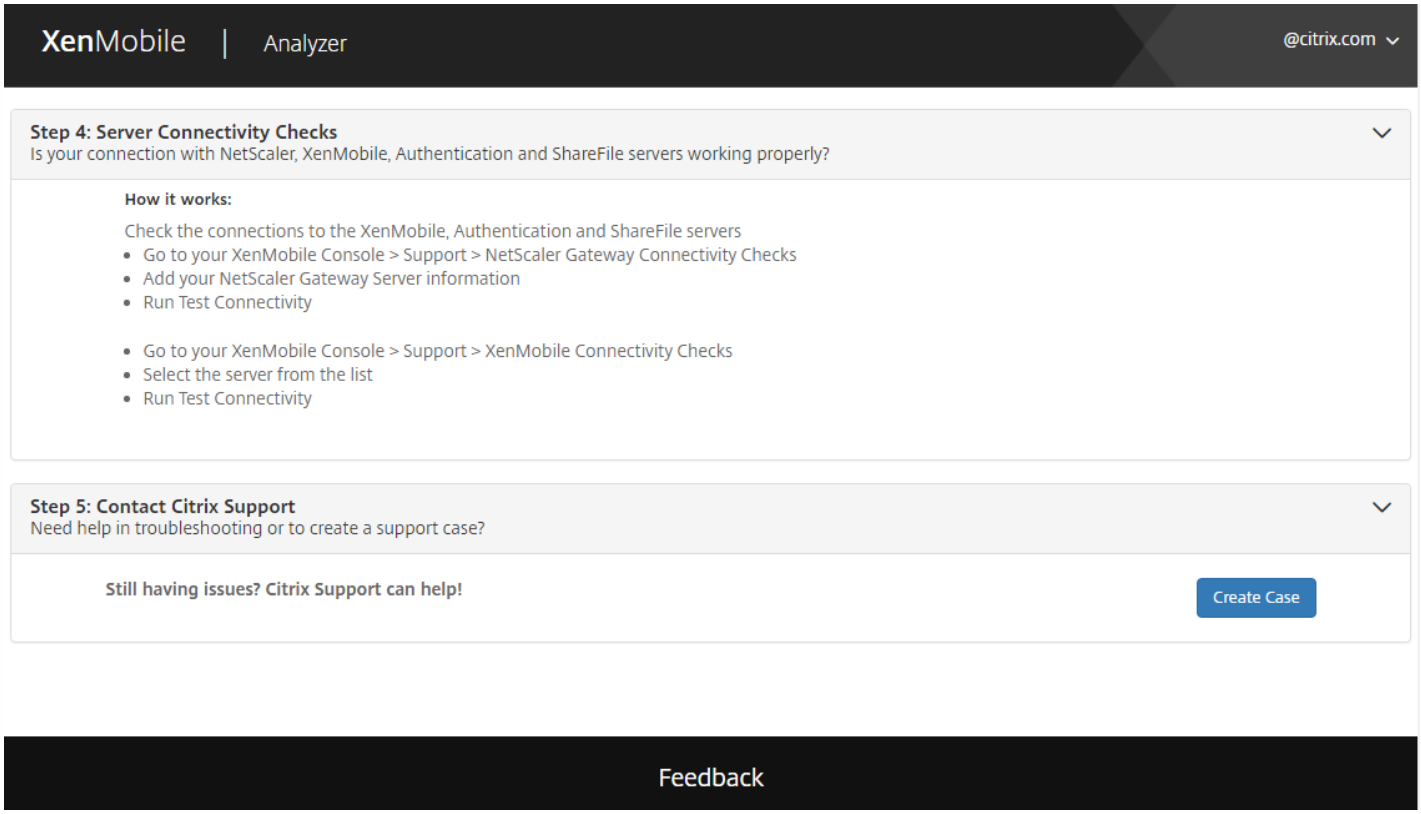
-
-
-
-
-
-
-
-
-
-
-
-

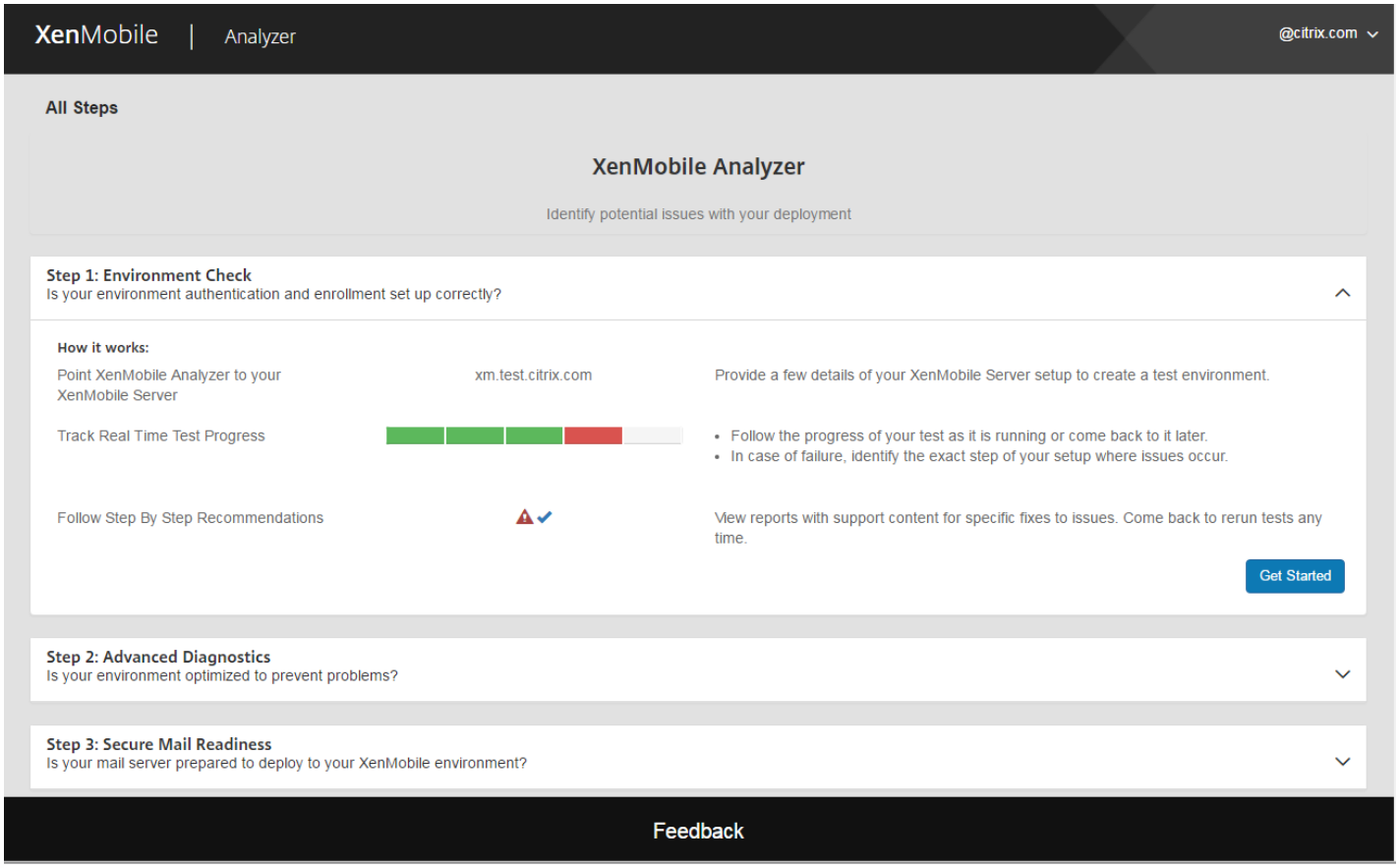


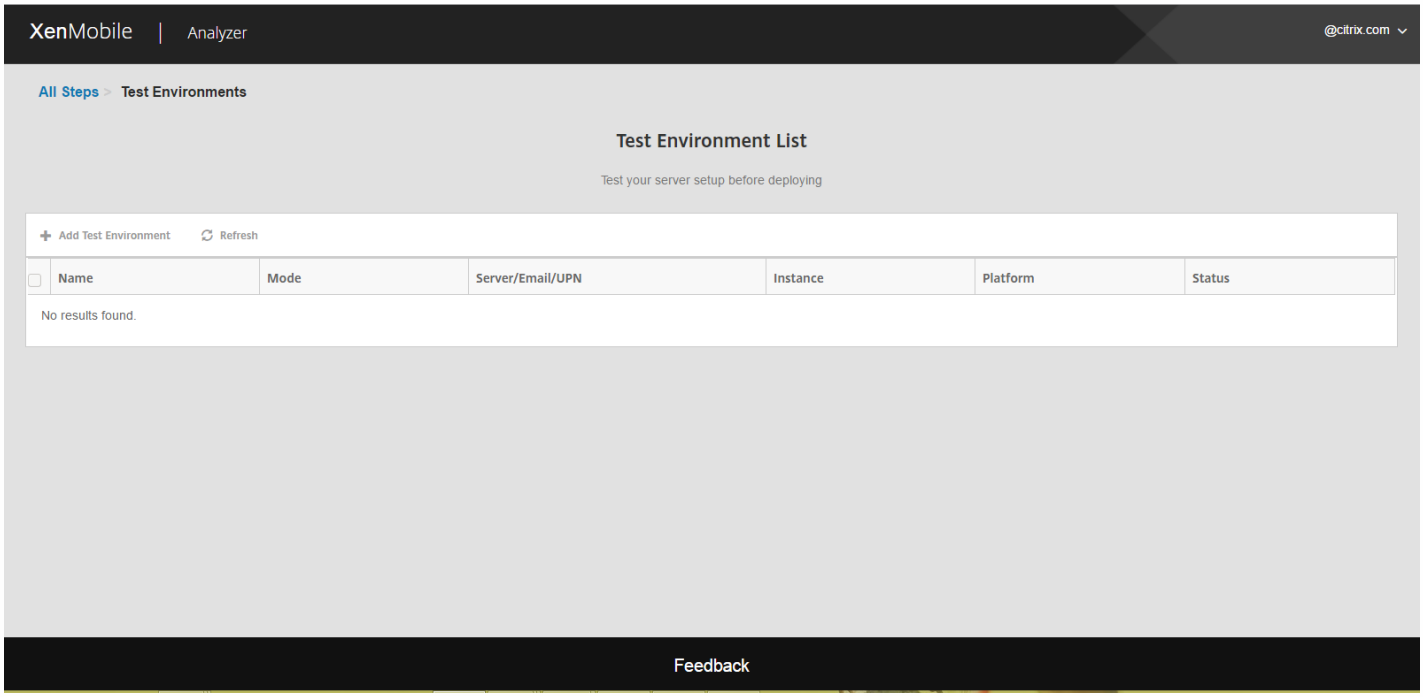


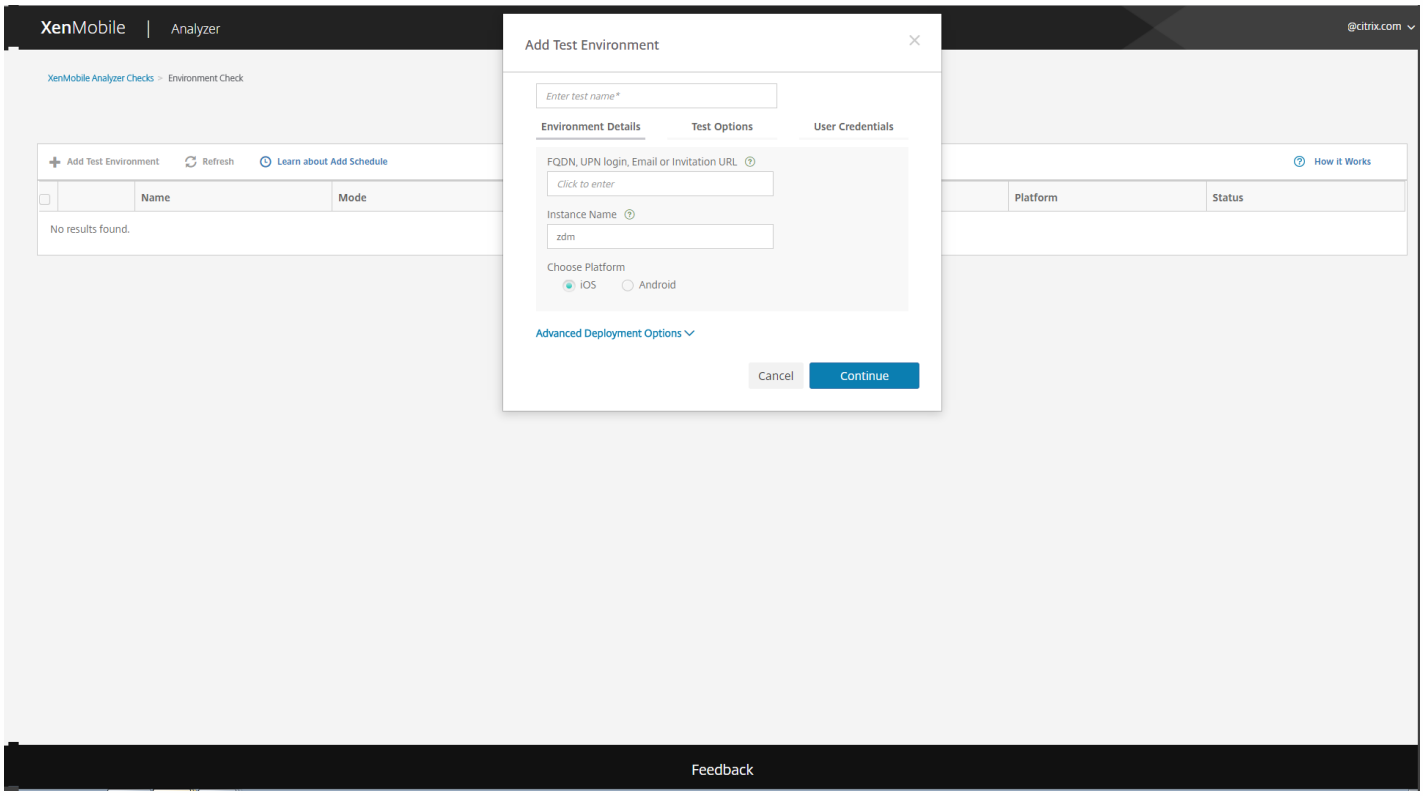


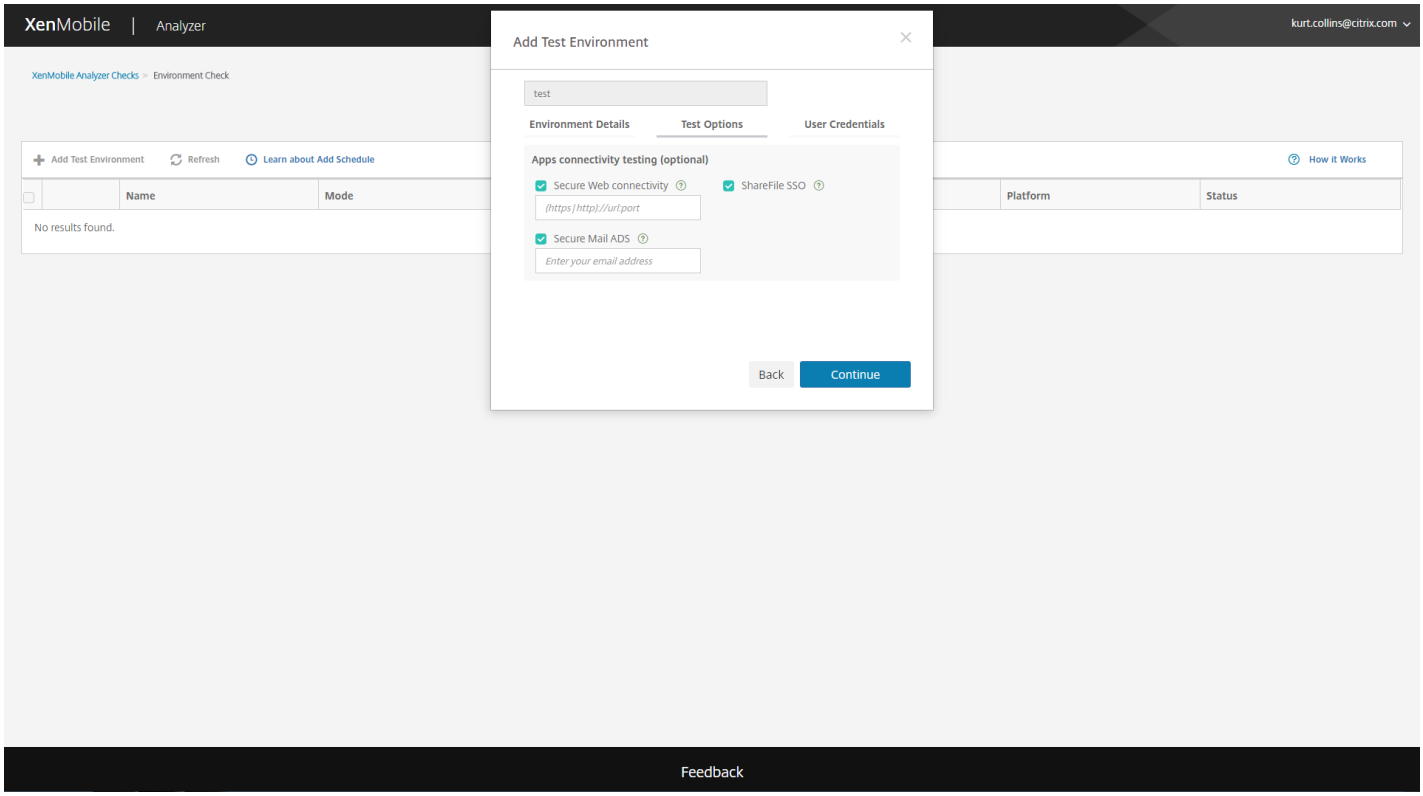


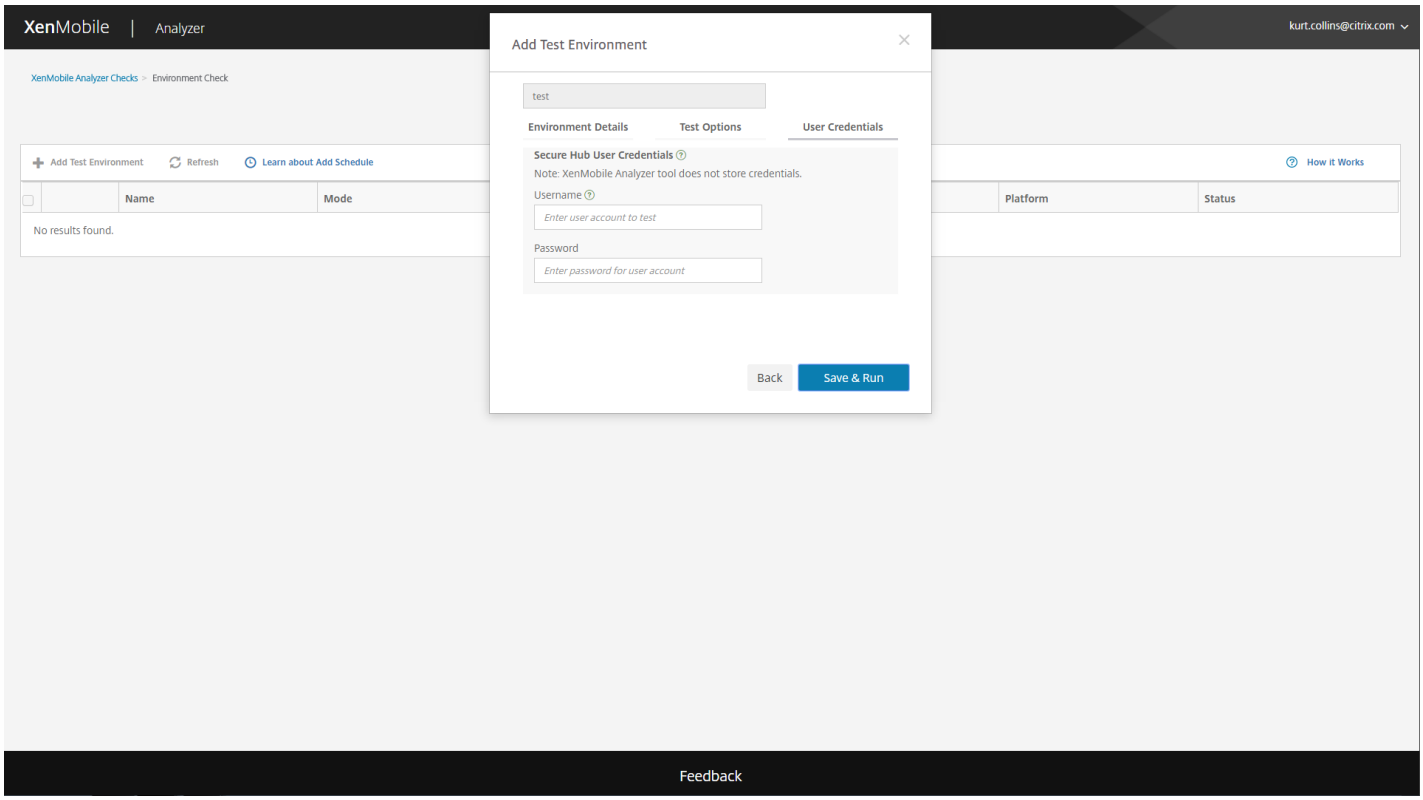


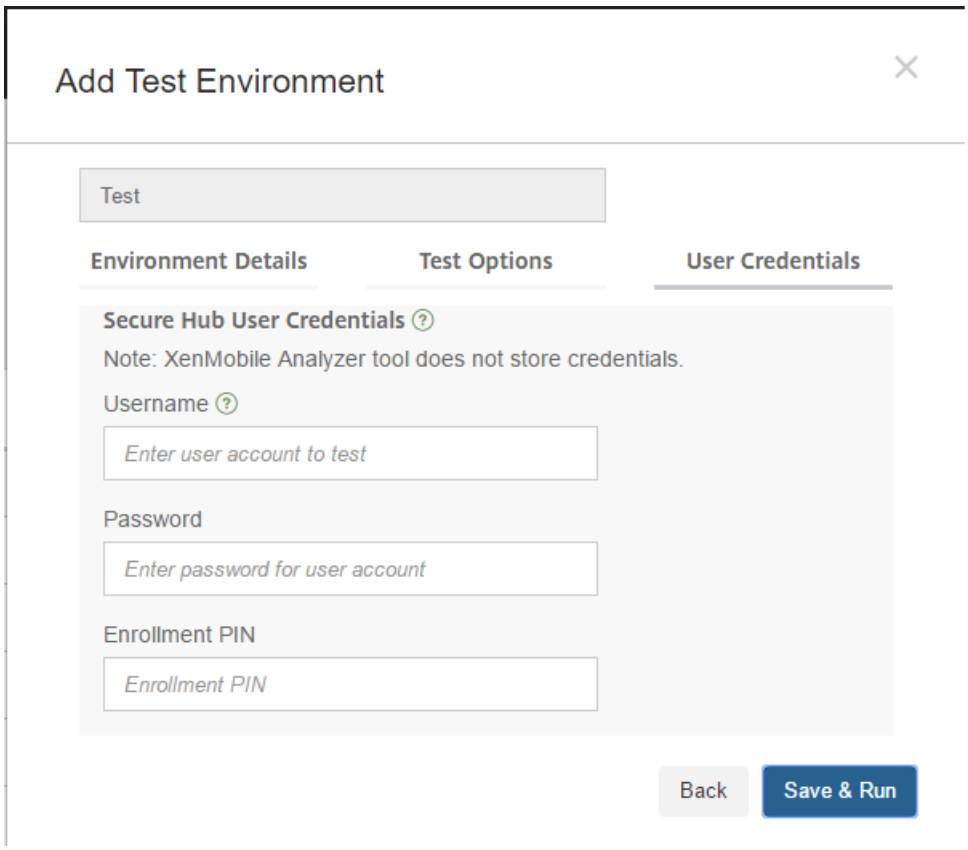


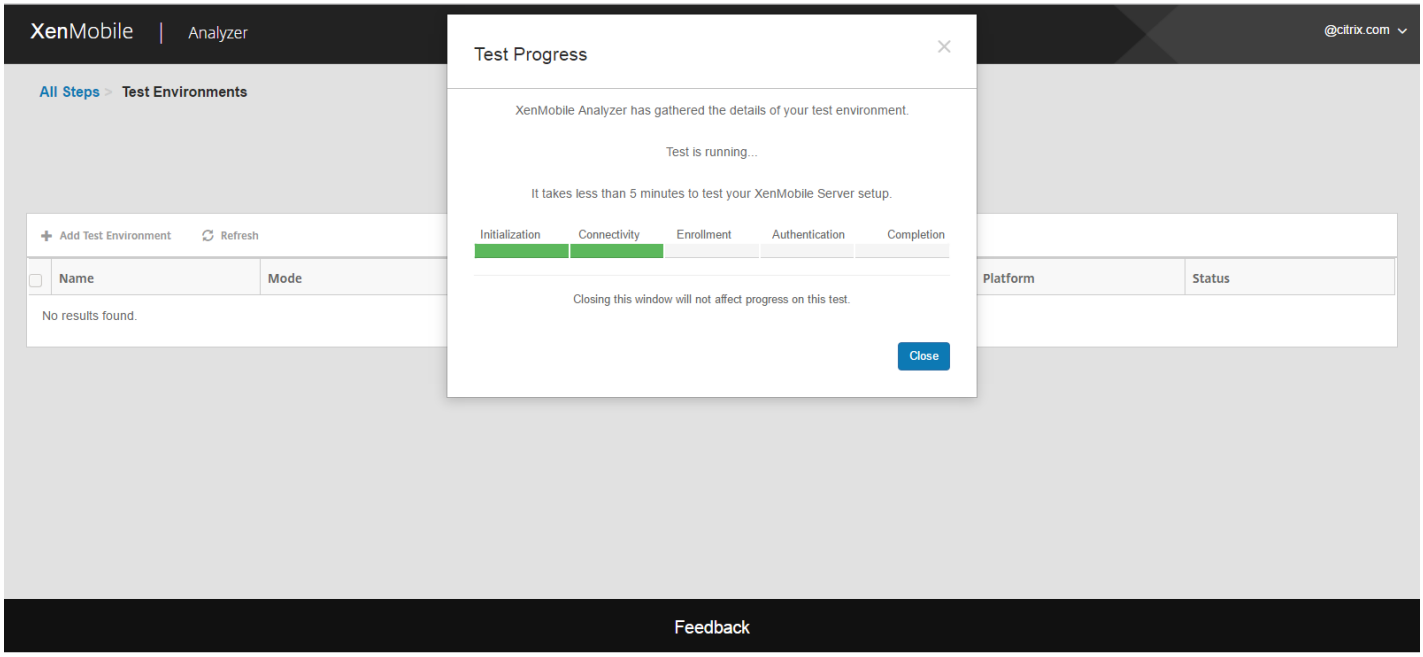


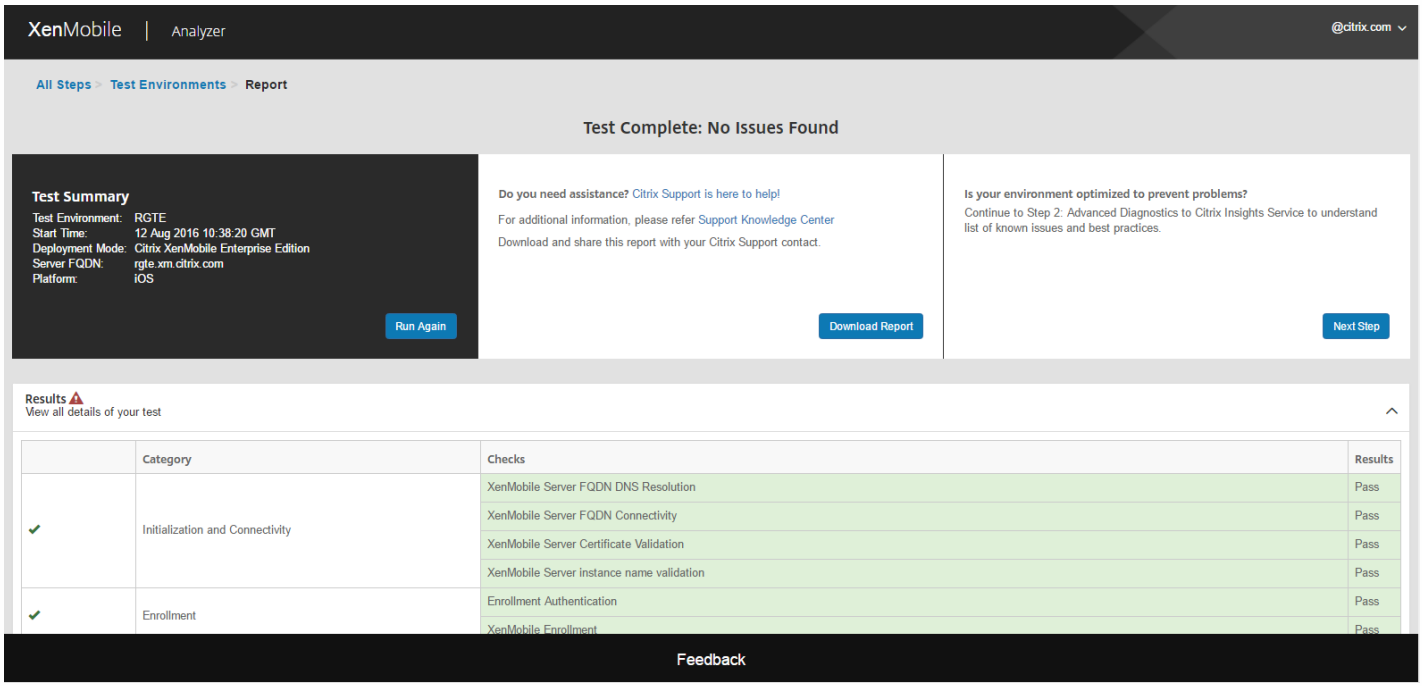


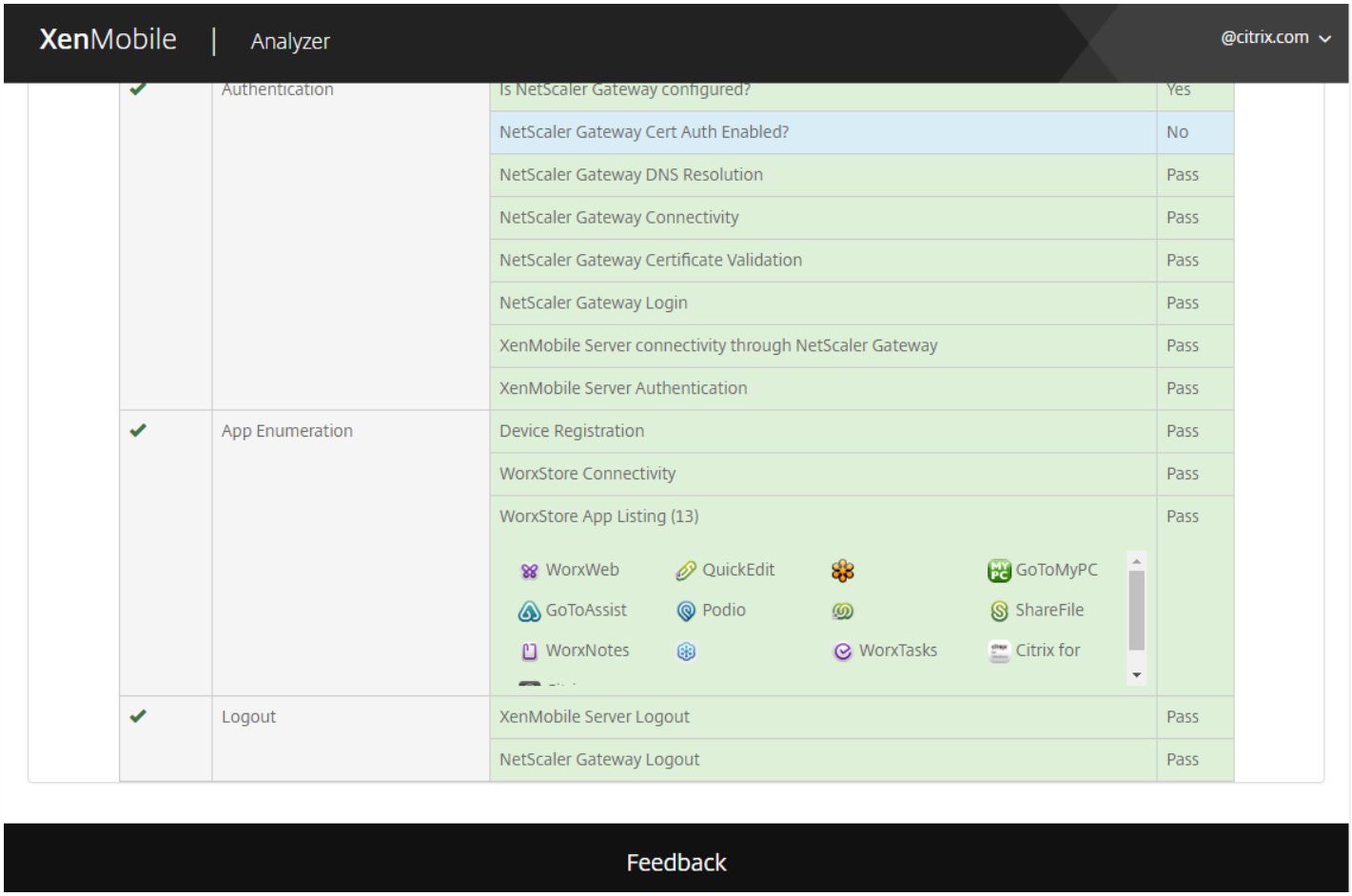


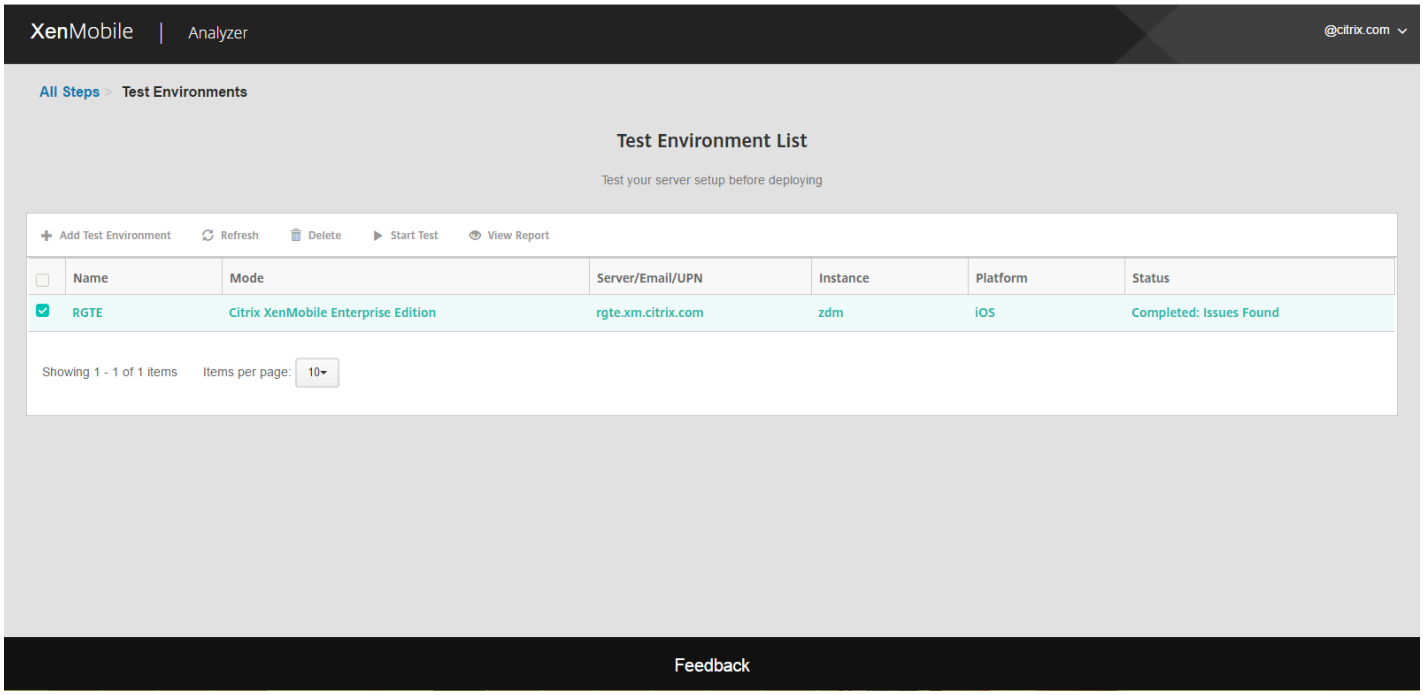


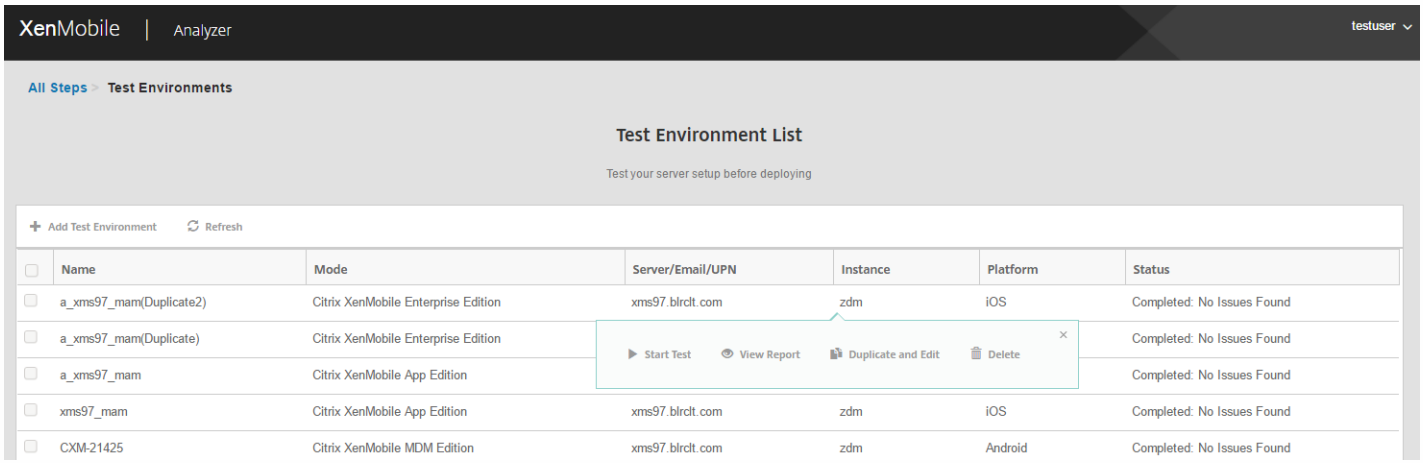


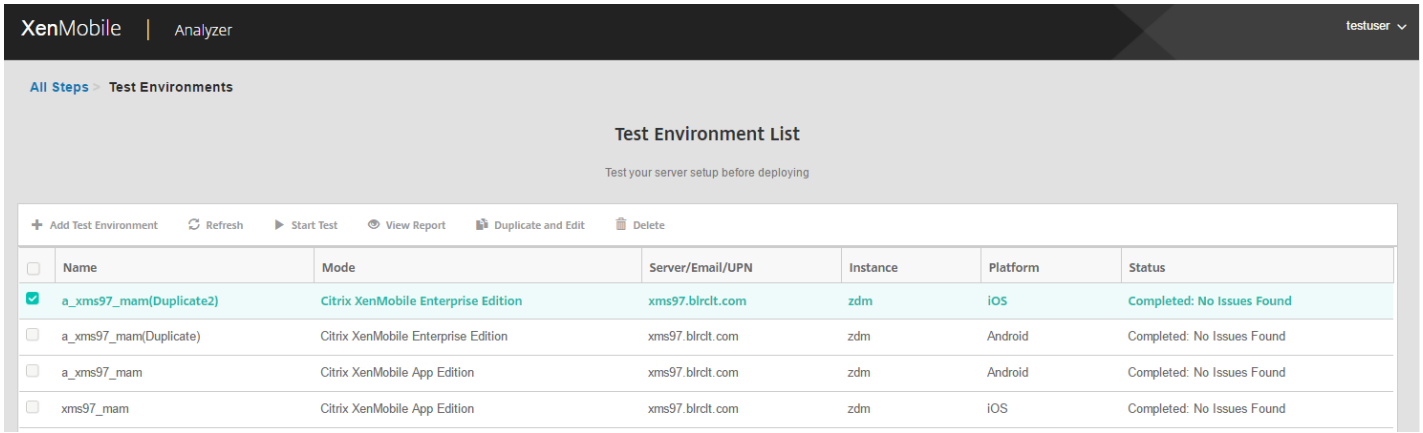


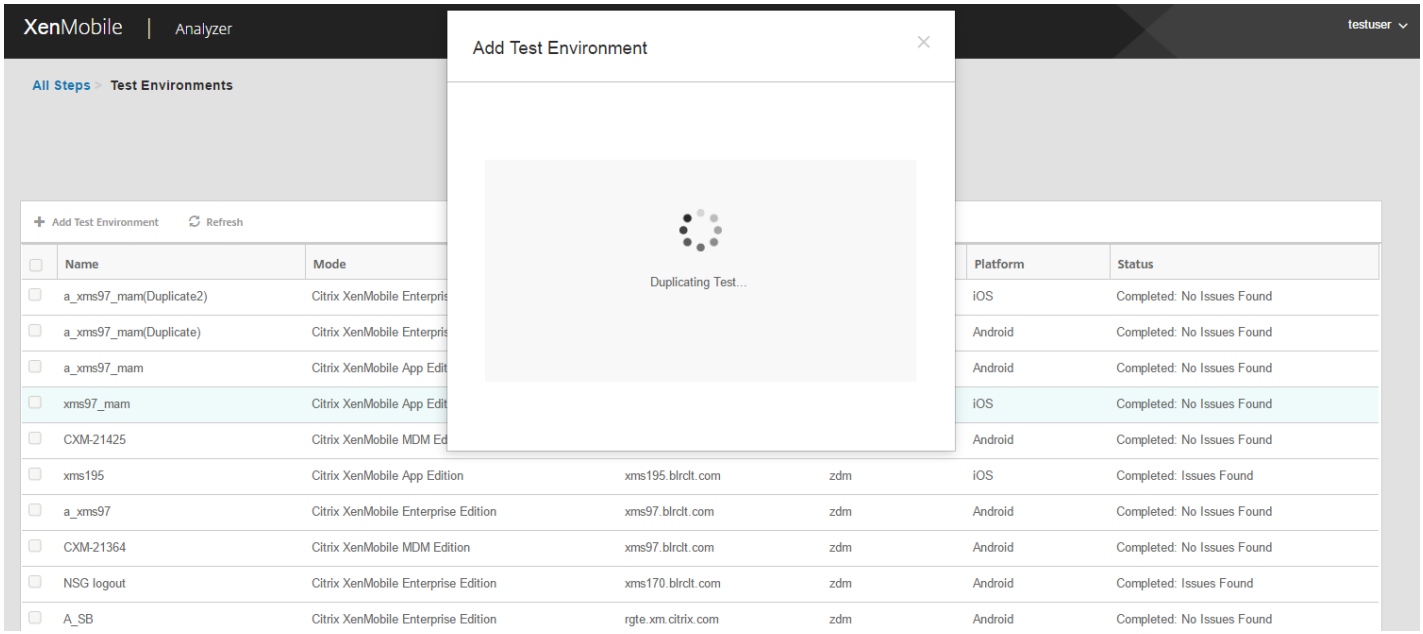


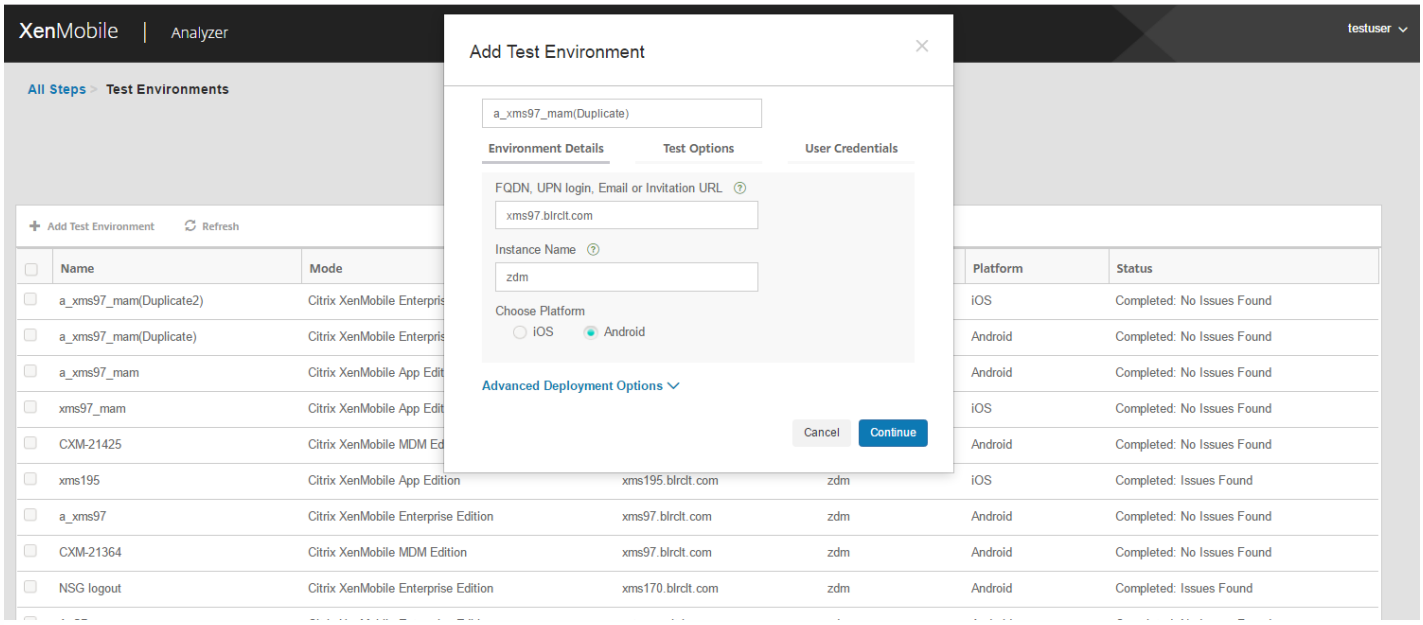




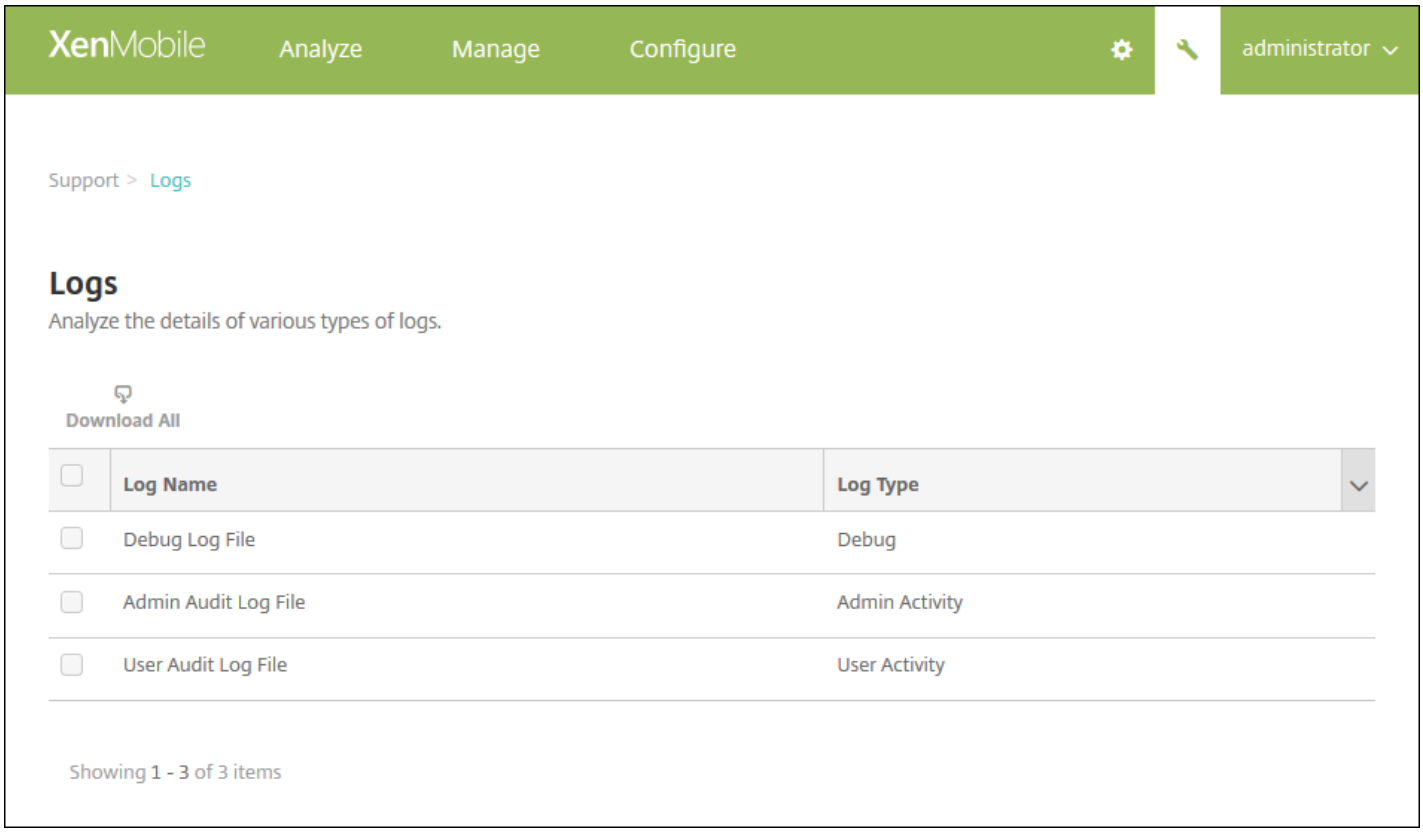




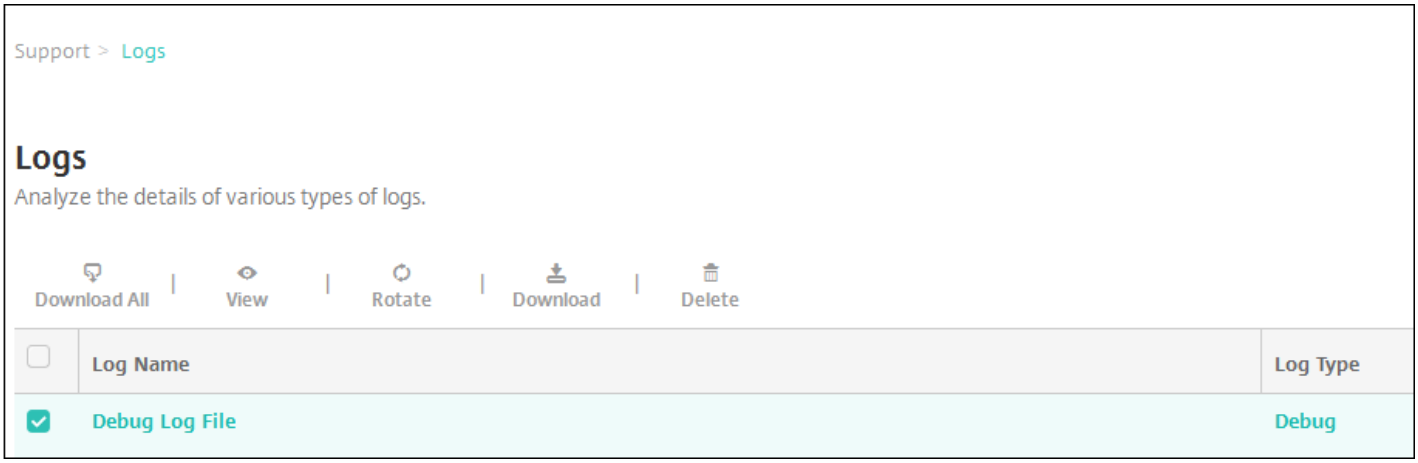




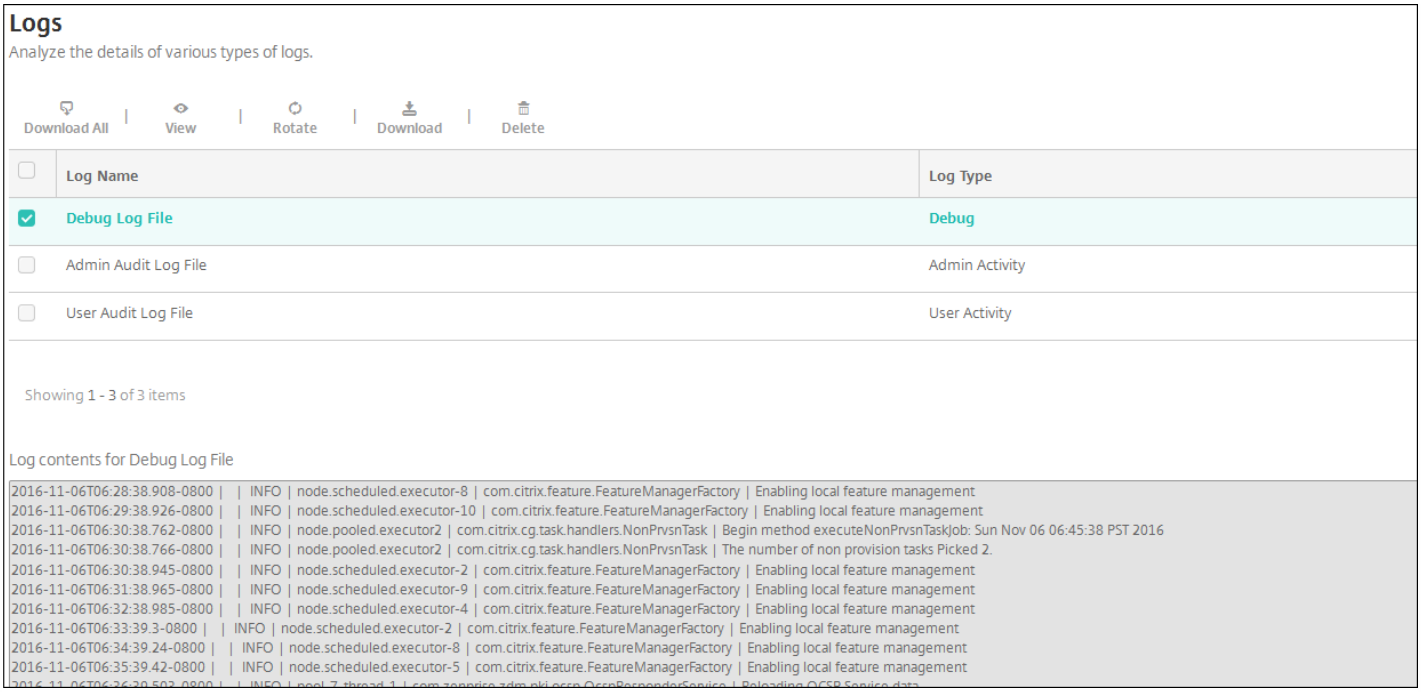
-
-
-
-
-
-
-
-
-
-



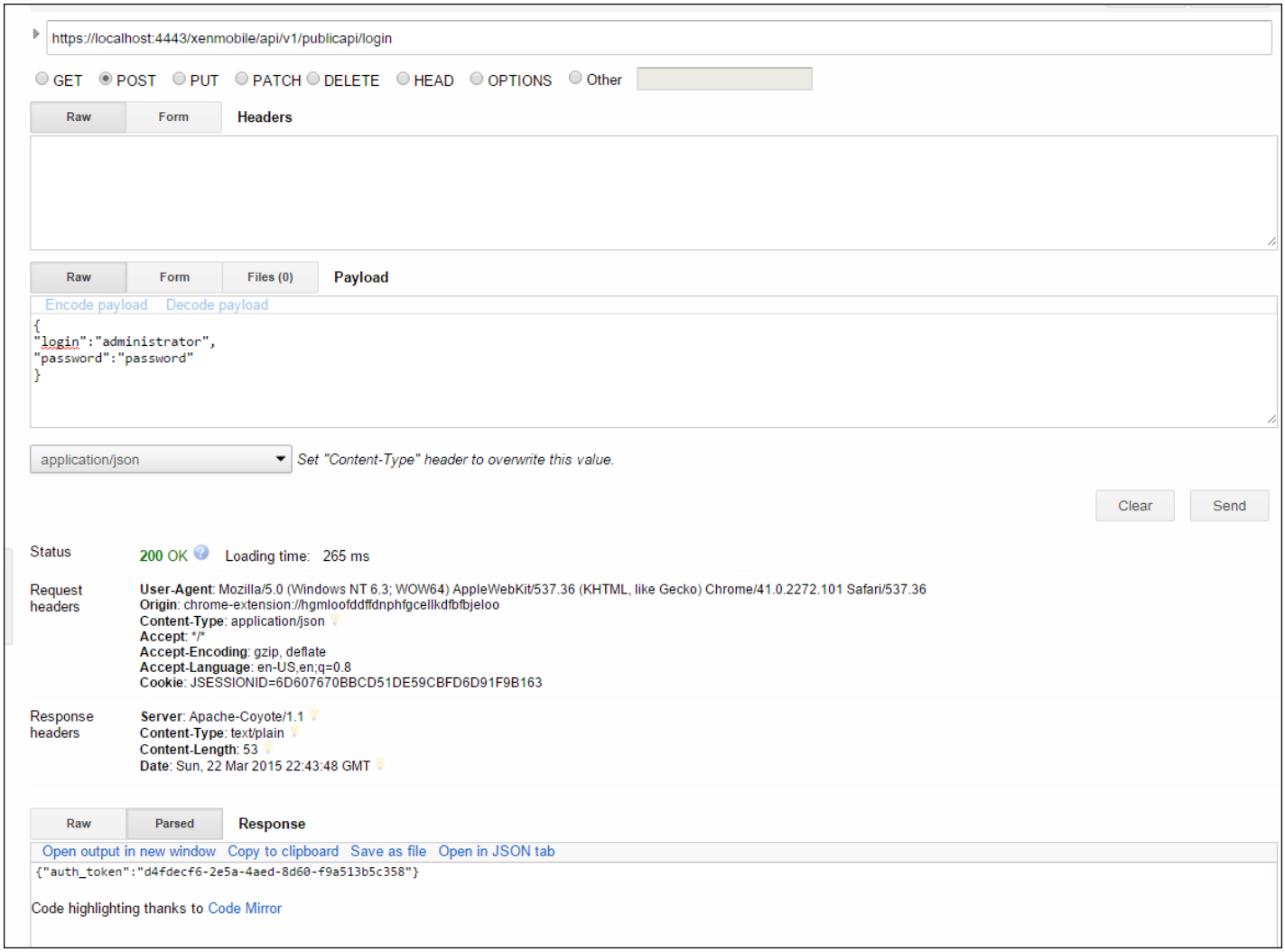
-
-
-



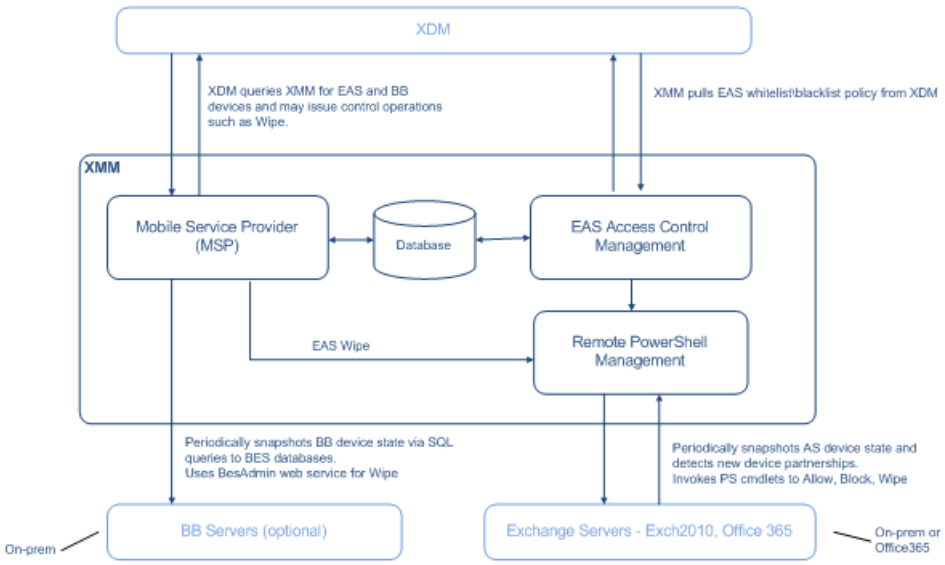
-
-
-
-
-
-
-



-
-



-
-
-
-
-
-
-



-
-
-

- **Pour Exchange Server 2010 SP2 :**
  - Get-CASMailbox
  - Set-CASMailbox

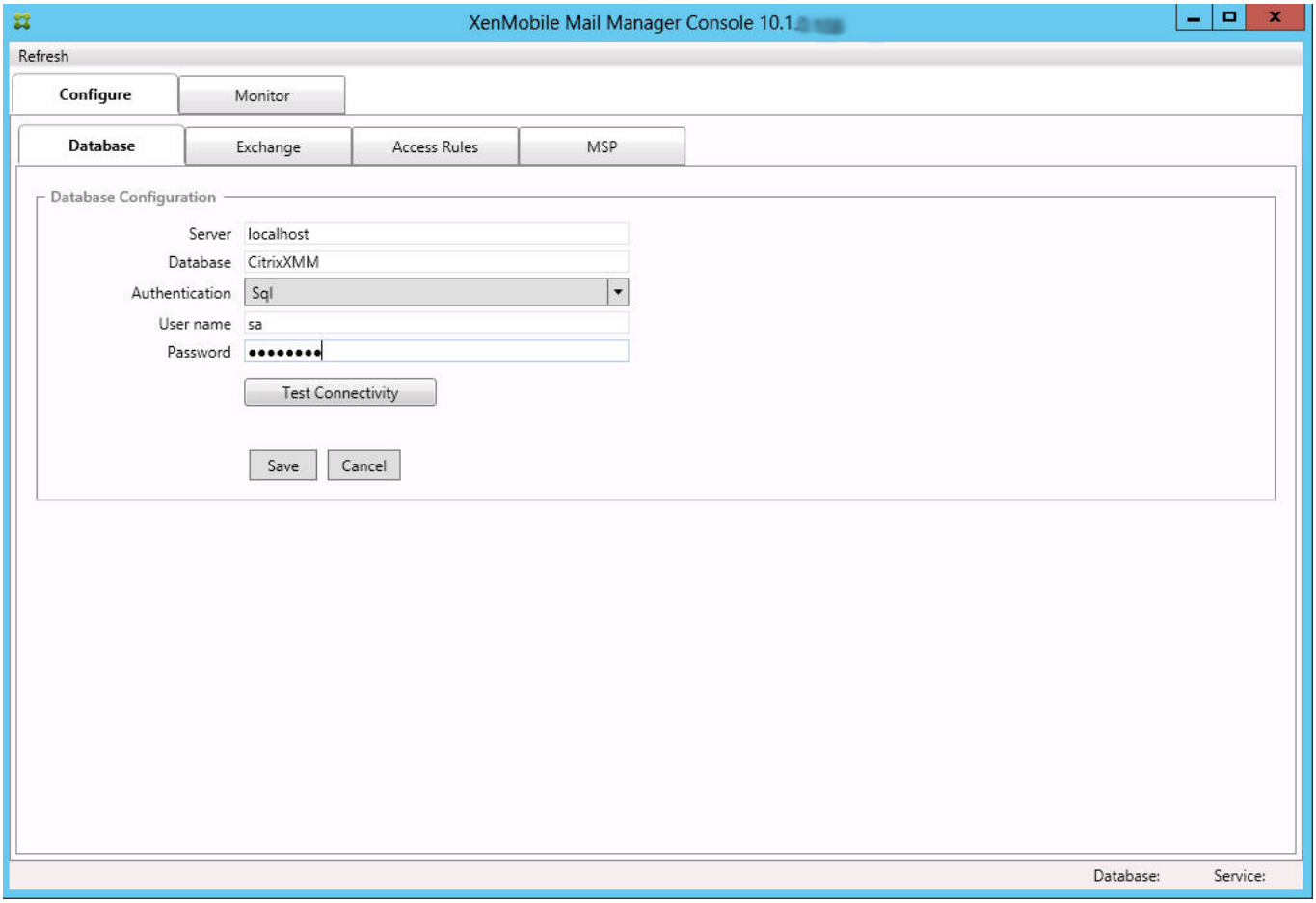
- Get-Mailbox
- Get-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Clear-ActiveSyncDevice
- Get-ExchangeServer
- Get-ManagementRole
- Get-ManagementRoleAssignment

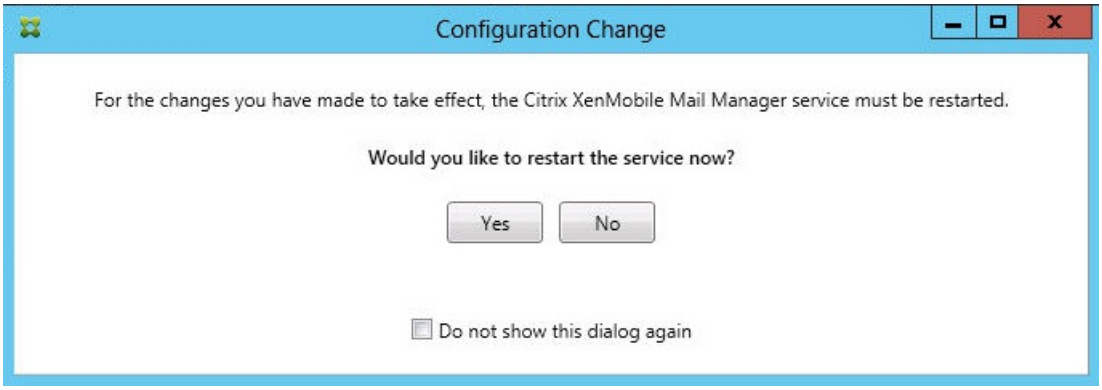
- **Pour Exchange Server 2013 et Exchange Server 2016 :**
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment

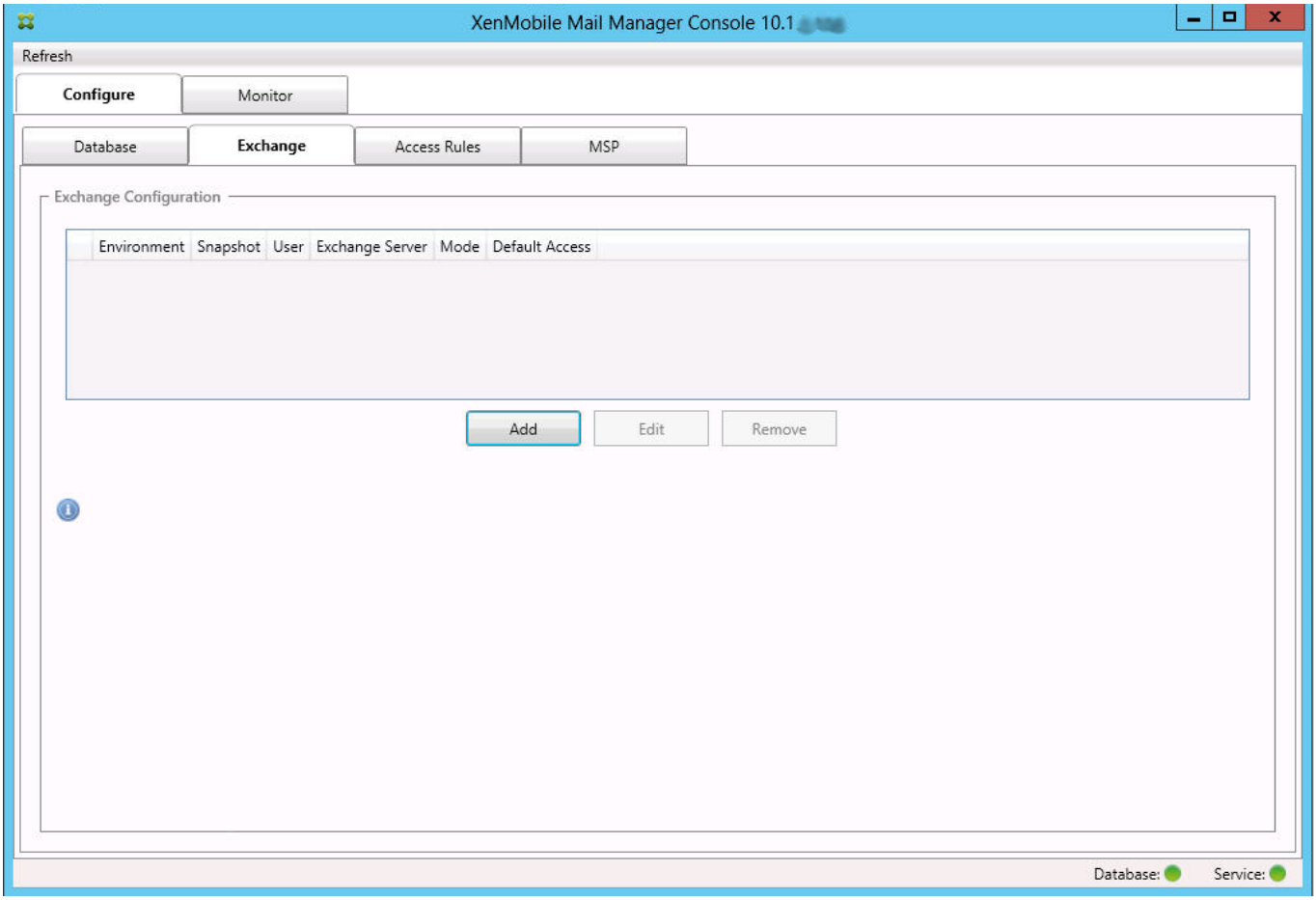
- Si XenMobile Mail Manager est configuré pour afficher l'ensemble de la forêt, l'autorisation doit avoir été accordée pour exécuter : Set-AdServerSettings -ViewEntireForest $true
- Les informations d'identification fournies doivent avoir été autorisées à se connecter au serveur Exchange Server via le Shell distant. Par défaut, l'utilisateur qui a installé Exchange possède ce droit.
- Conformément à l'article Microsoft TechNet about_Remote_Requirements, afin d'établir une connexion à distance et exécuter les commandes distantes, les informations d'identification doivent correspondre à un utilisateur qui est un administrateur sur l'appareil distant. Conformément à ce billet de blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands, Set-PSSessionConfiguration peut être utilisé pour éliminer les exigences d'administration, mais le support et les discussions spécifiques à cette commande sont hors de portée de ce document.
- Le serveur Exchange doit être configuré pour prendre en charge les requêtes PowerShell distantes via HTTP. En règle générale, un administrateur exécutant la commande PowerShell suivante sur le serveur Exchange est la seule exigence requise : WinRM QuickConfig.
- Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de 18 sur Exchange 2010. Lorsque la limite de connexion est atteinte, XenMobile Mail Manager ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

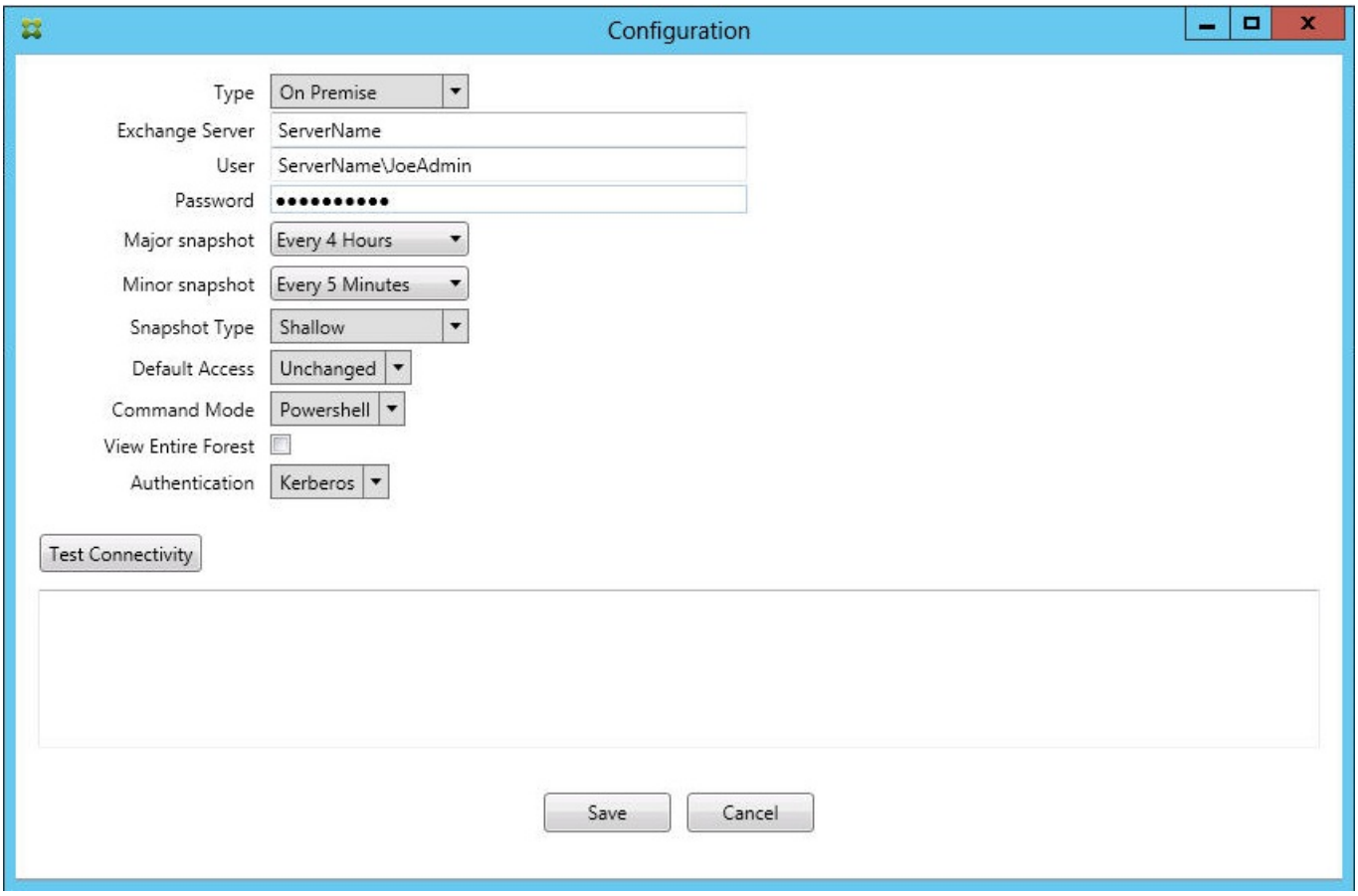
- **Autorisations**. Les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent être en mesure de se connecter à Office 365 et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-MobileDevice
  - Get-MobileDeviceStatistics
  - Clear-MobileDevice
  - Get-ExchangeServer
  - Get-ManagementRole
  - Get-ManagementRoleAssignment
- **Privilèges**. Les informations d'identification fournies doit avoir été autorisées à se connecter au serveur Office 365 via le Shell distant. Par défaut, l'administrateur d'Office 365 Online possède les privilèges requis.
- **Stratégies de limitation**. Exchange possède de nombreuses stratégies de limitation. L'une de ces stratégies contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de trois sur Office 365. Lorsque la limite de connexion est atteinte, XenMobile Mail Manager ne peut pas se connecter au serveur Exchange. Il existe plusieurs méthodes pour changer le nombre maximal de connexions simultanées autorisées via PowerShell qui ne sont pas couvertes dans cette documentation. Si vous êtes intéressé, renseignez-vous au sujet des stratégies de limitation d'Exchange relatives à la gestion à distance avec PowerShell.

-
-

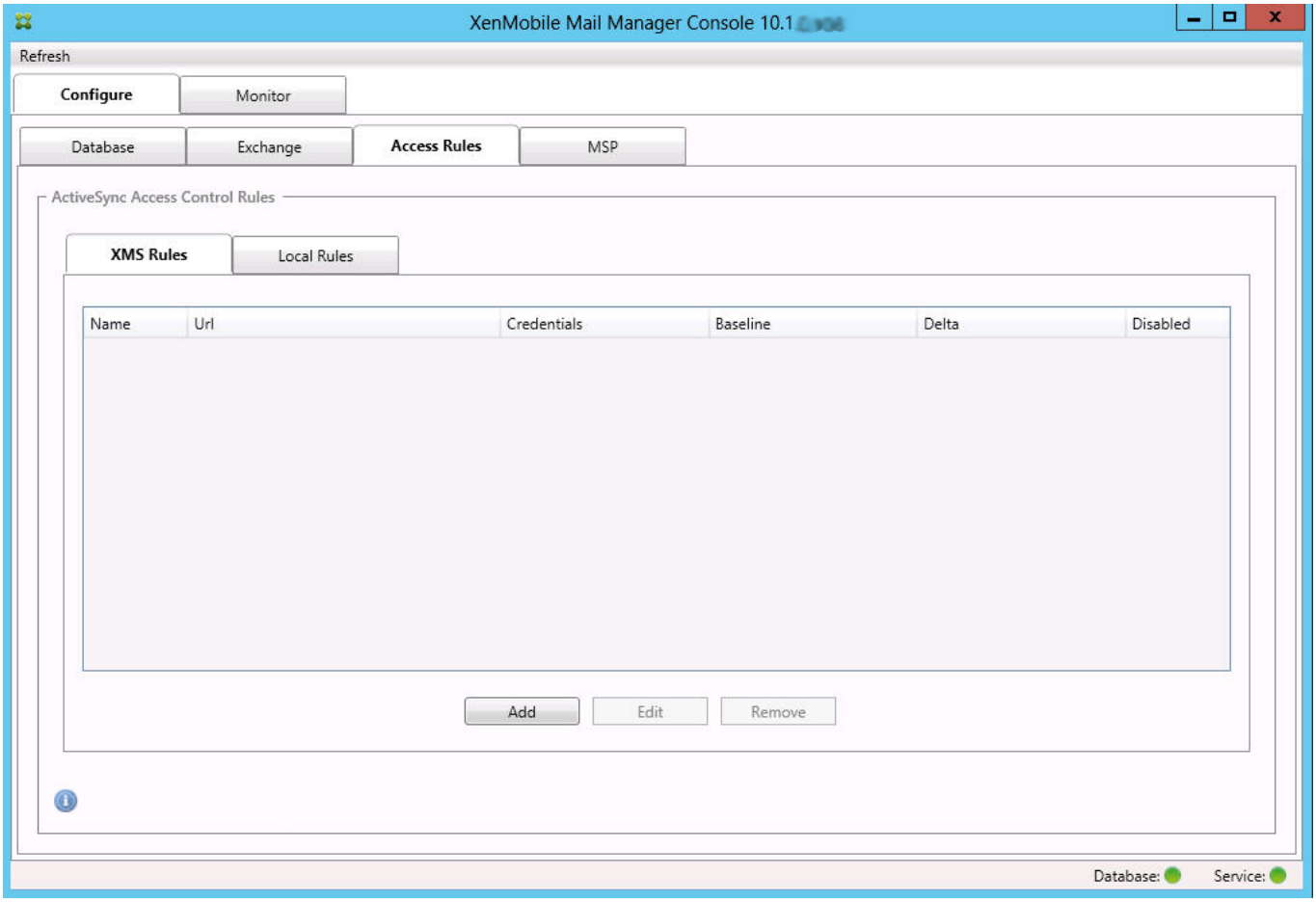


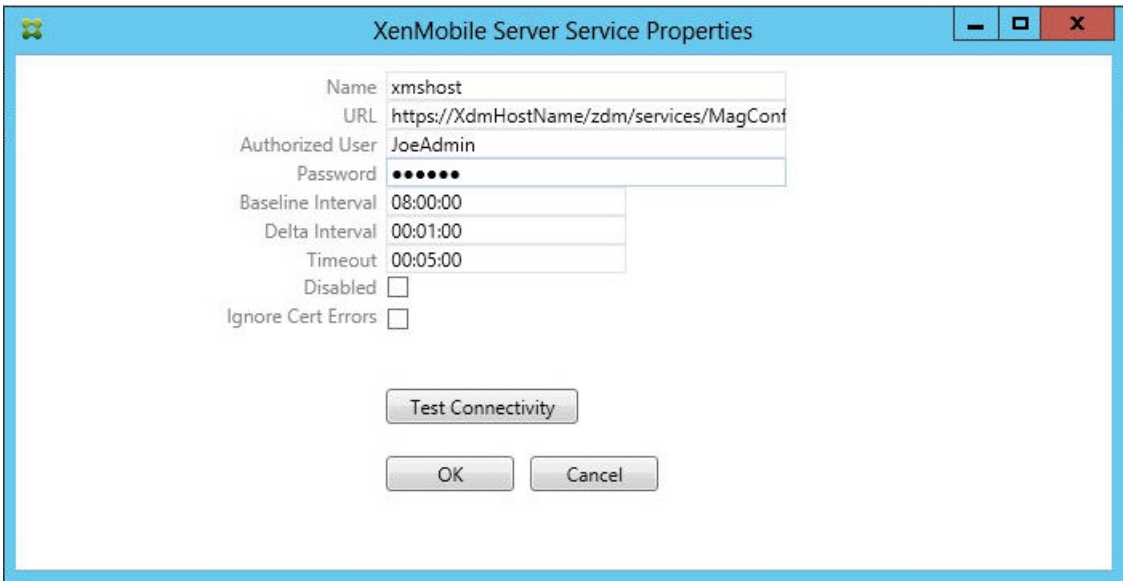


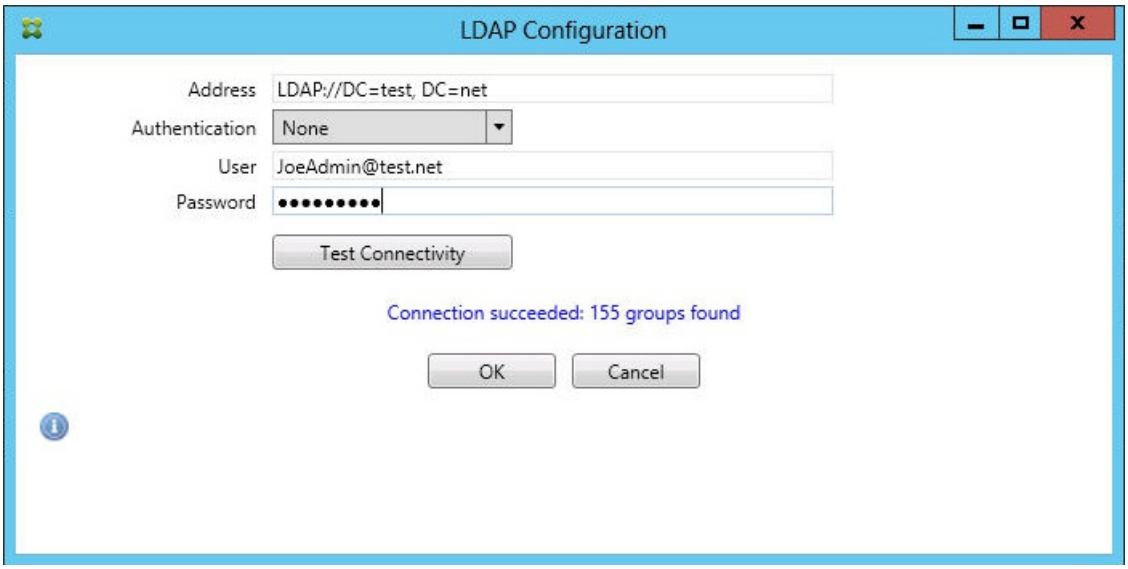


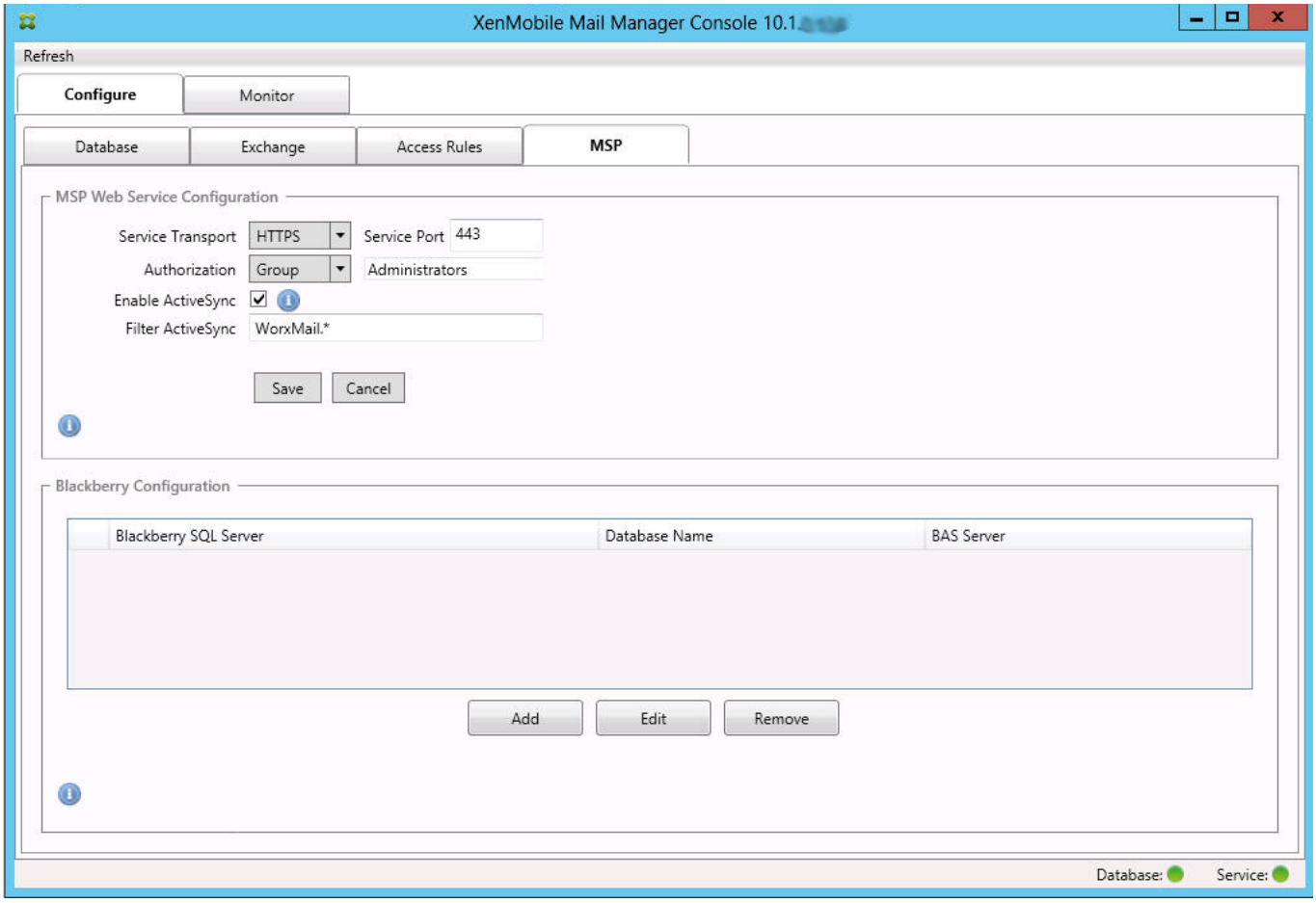


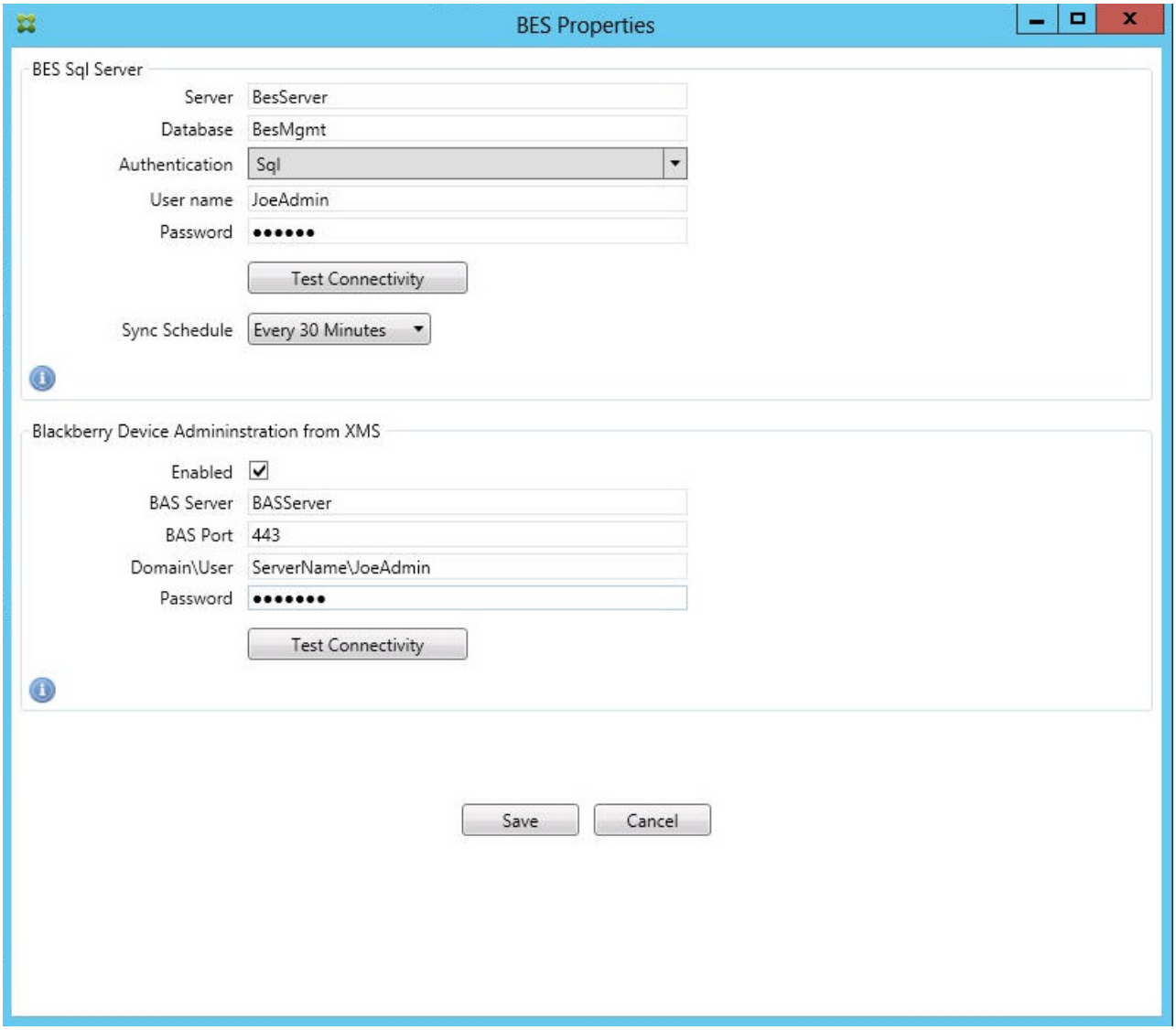
-
-

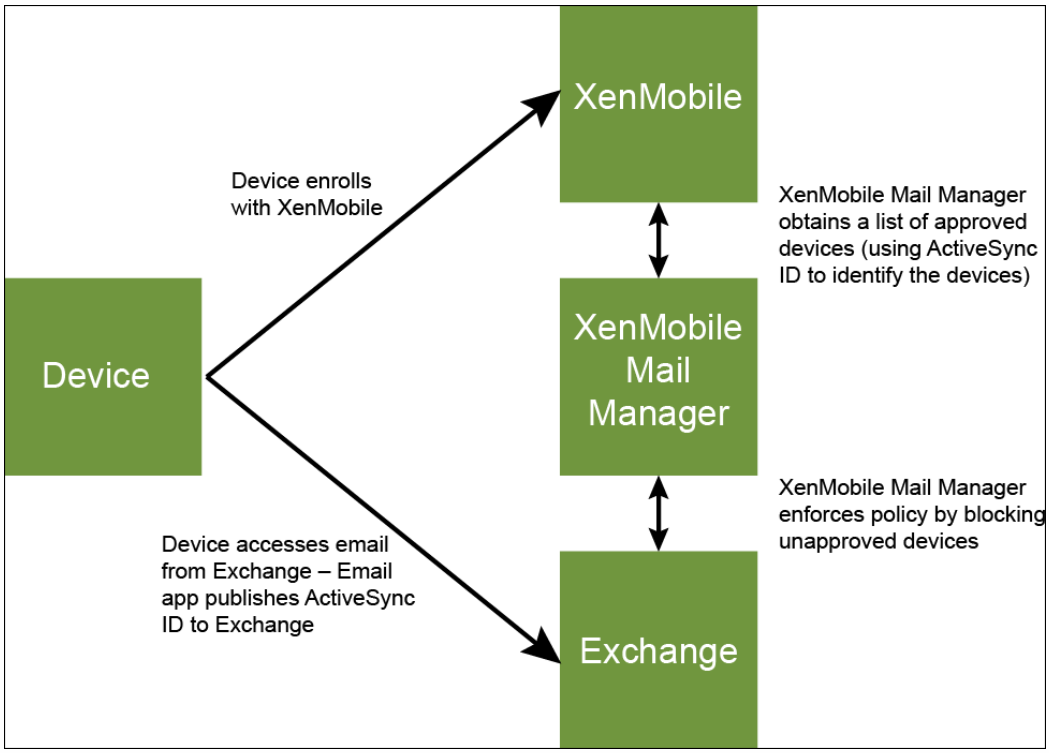










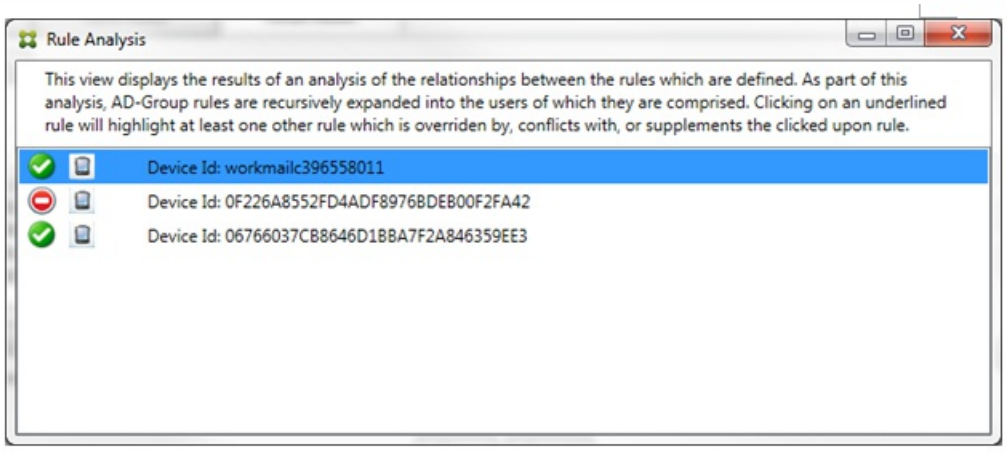


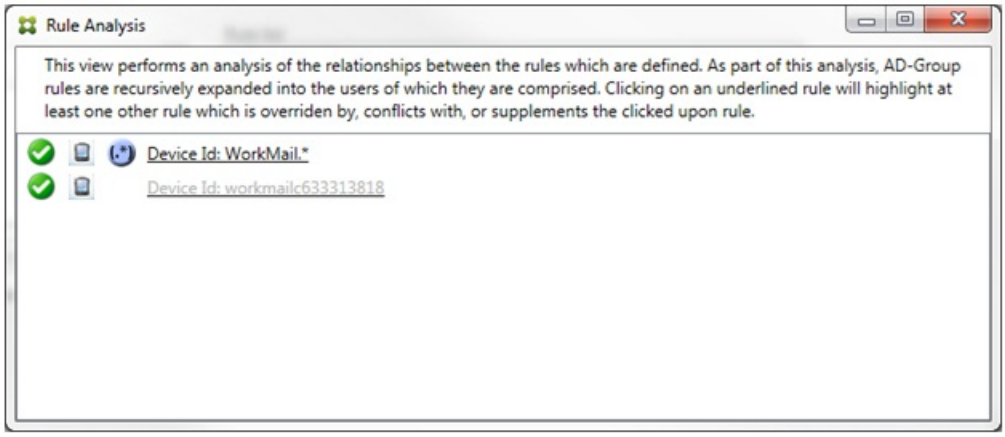
-
-

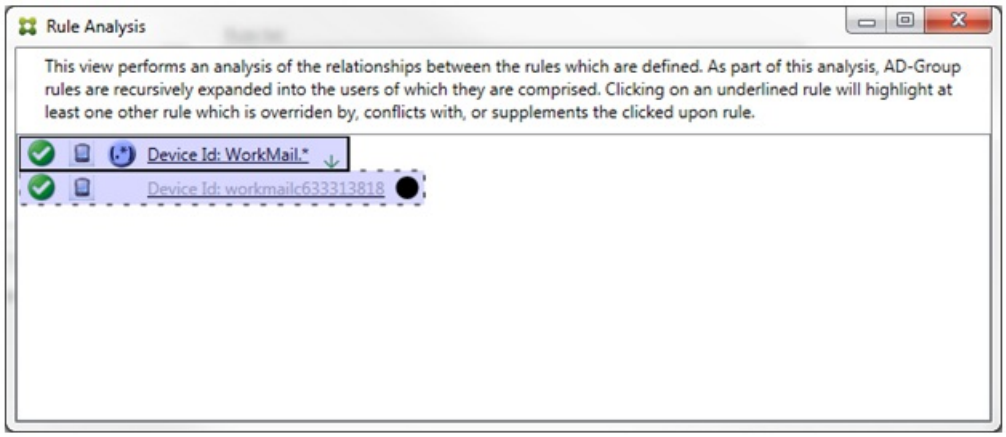
-
-
-
-

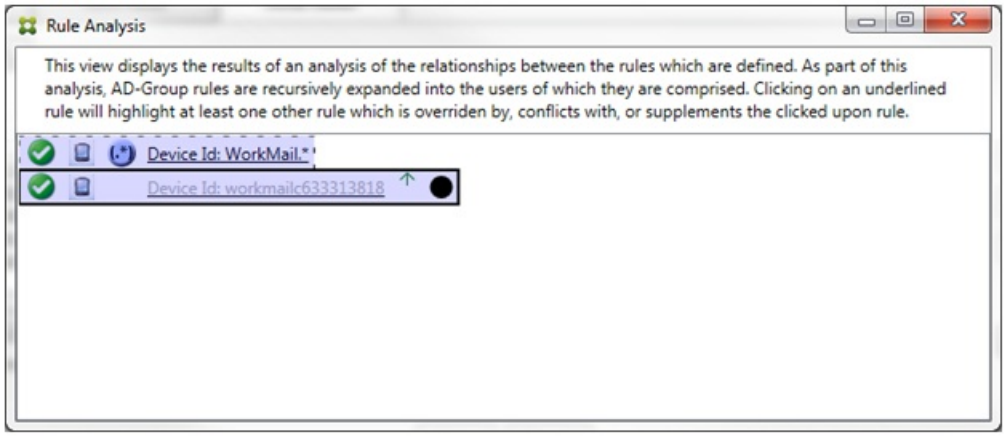
-
-
-
-
-
-
-

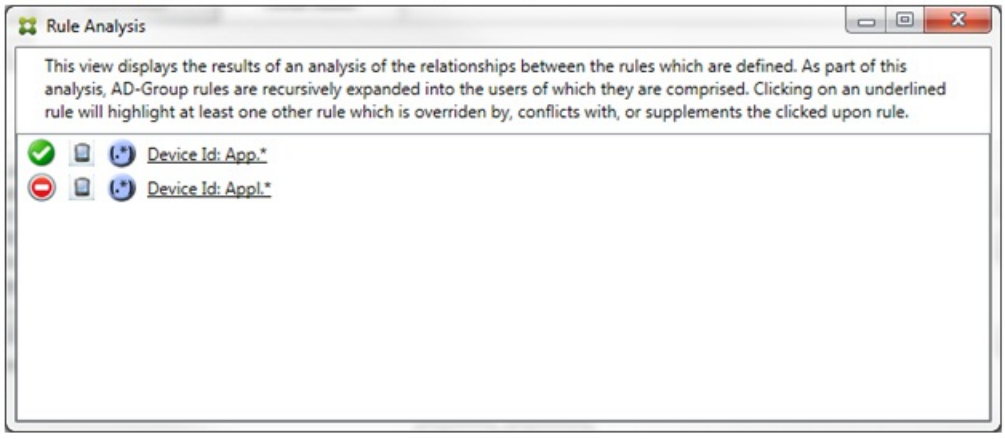
-
-
-
-

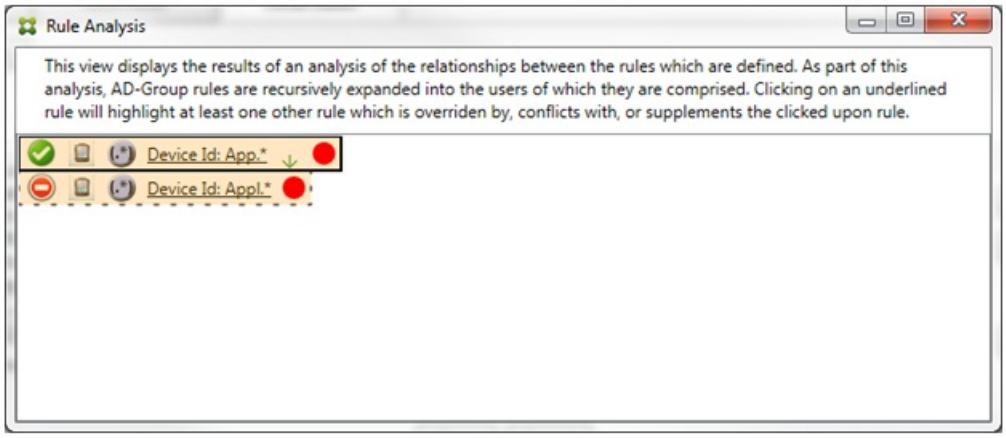


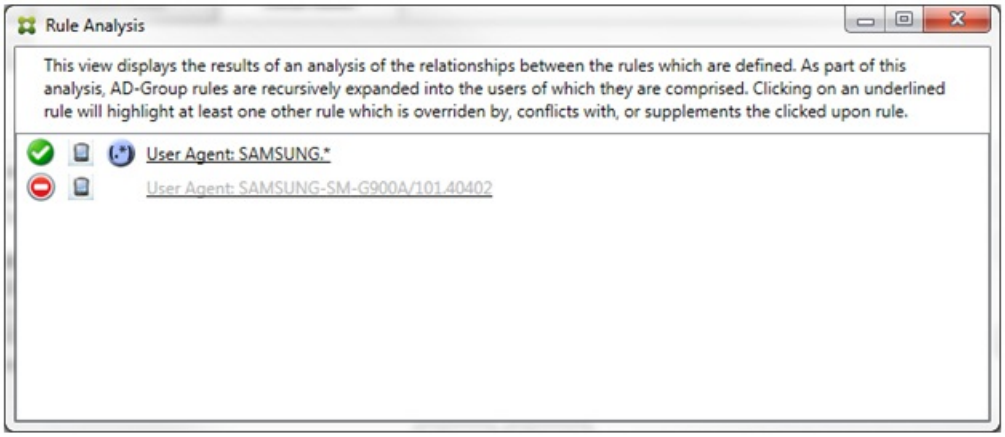


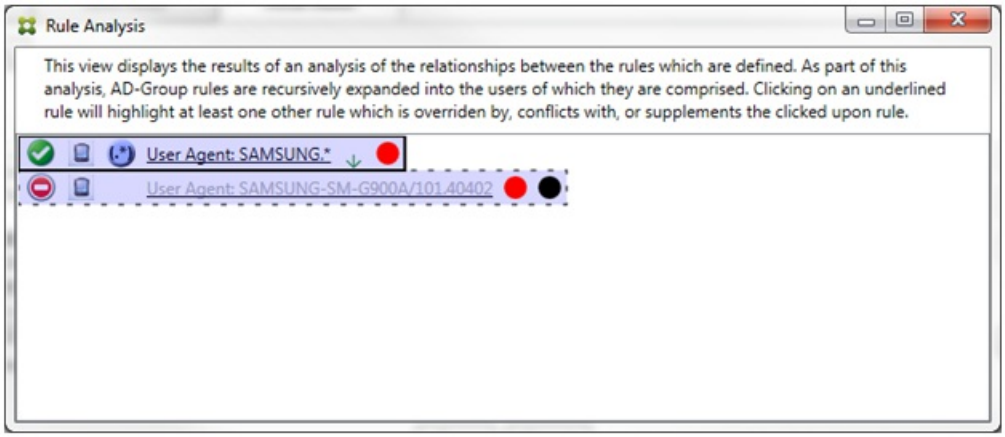


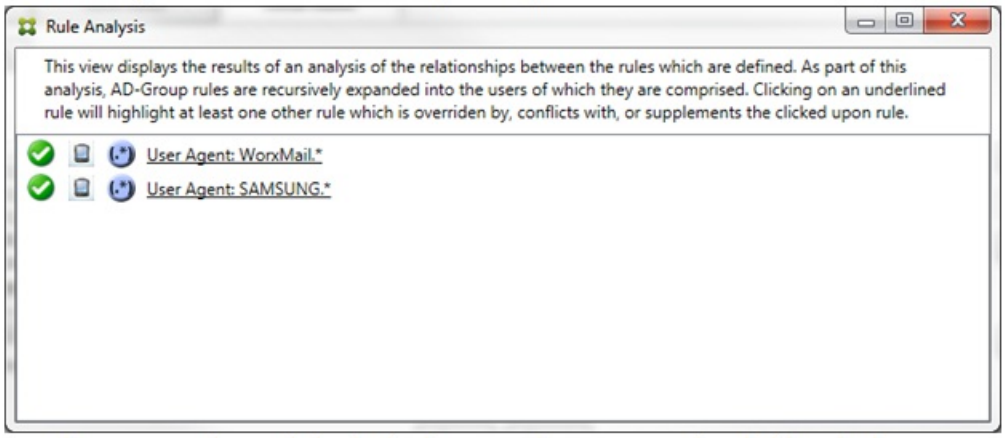


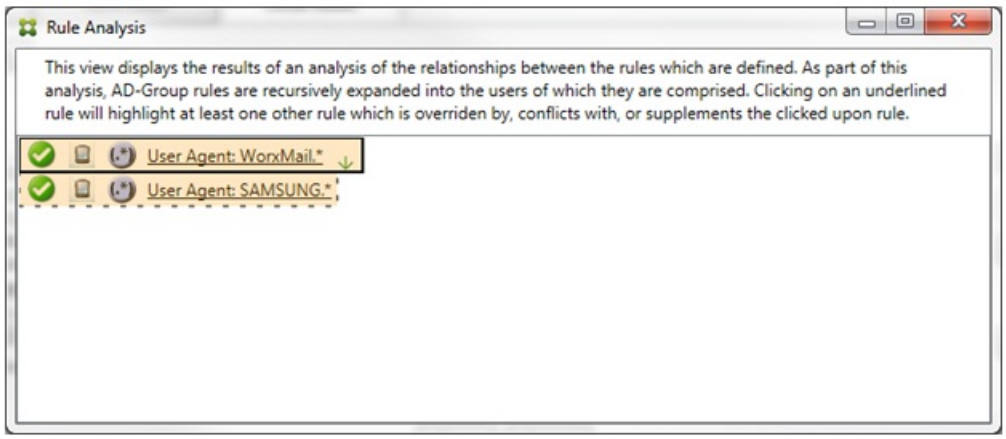


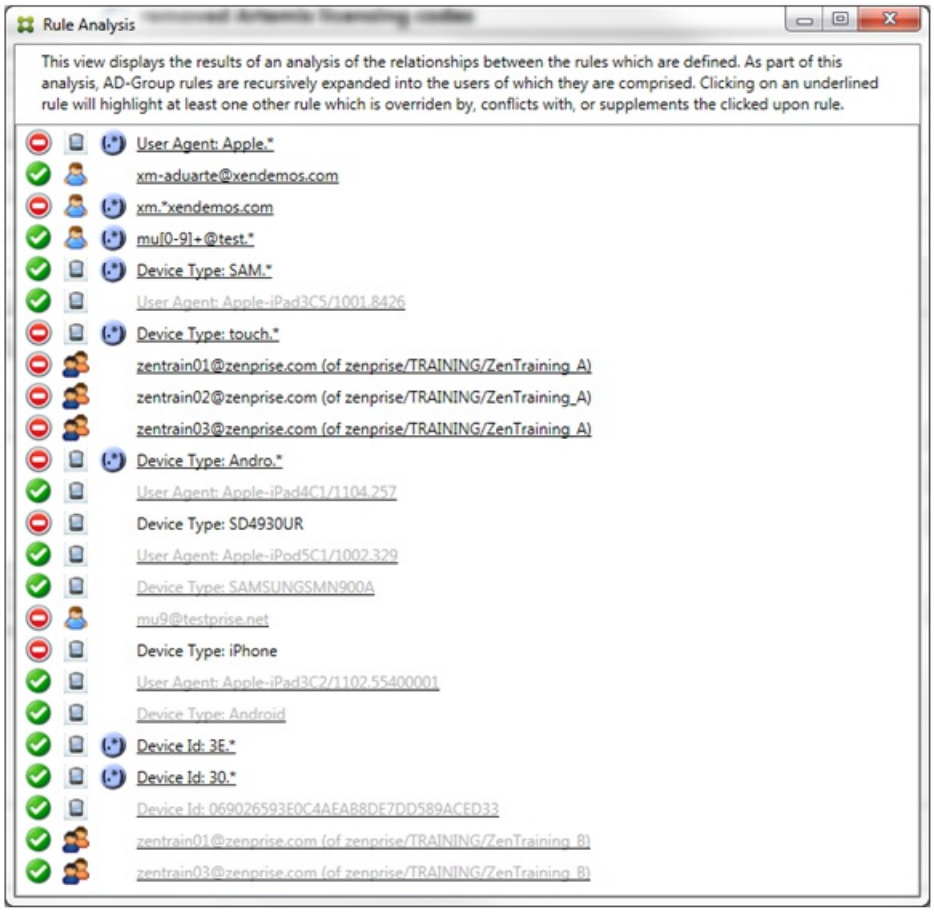


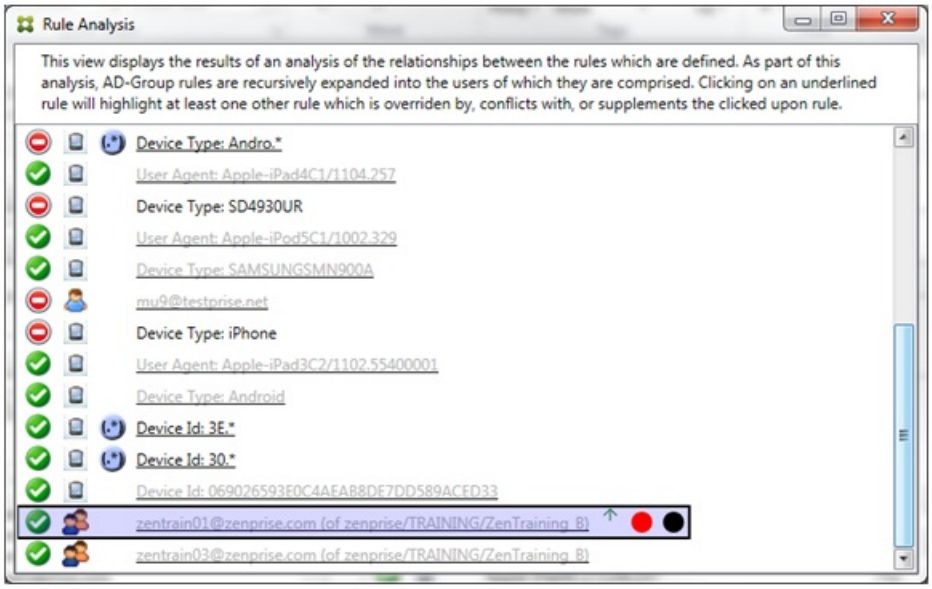




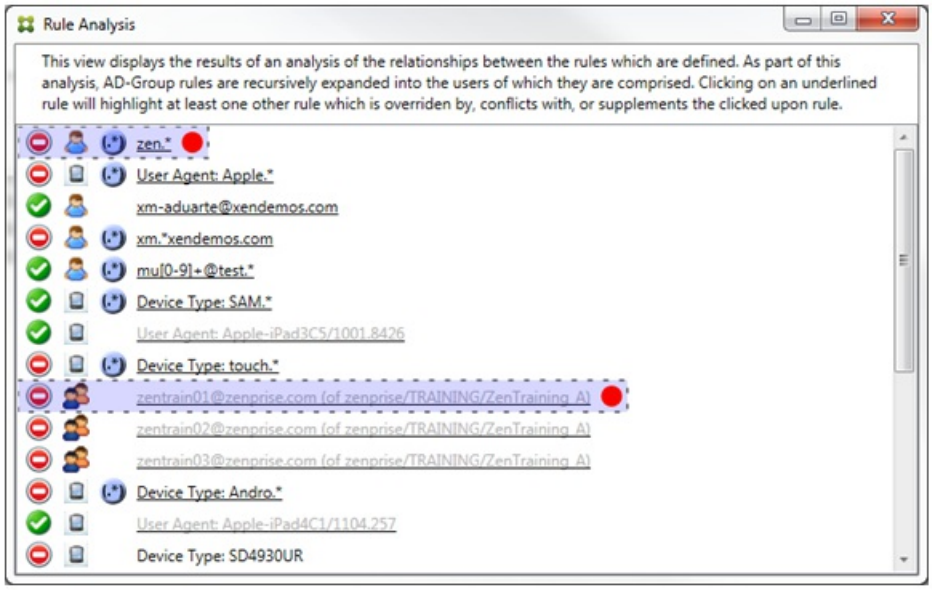


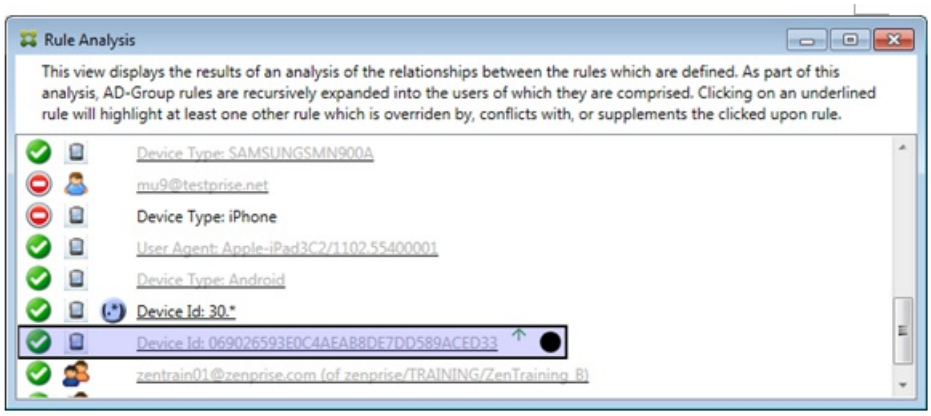




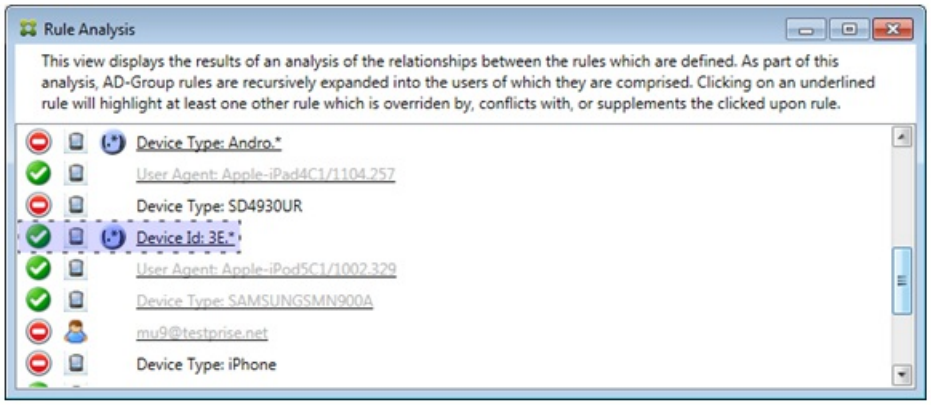


-
-
-



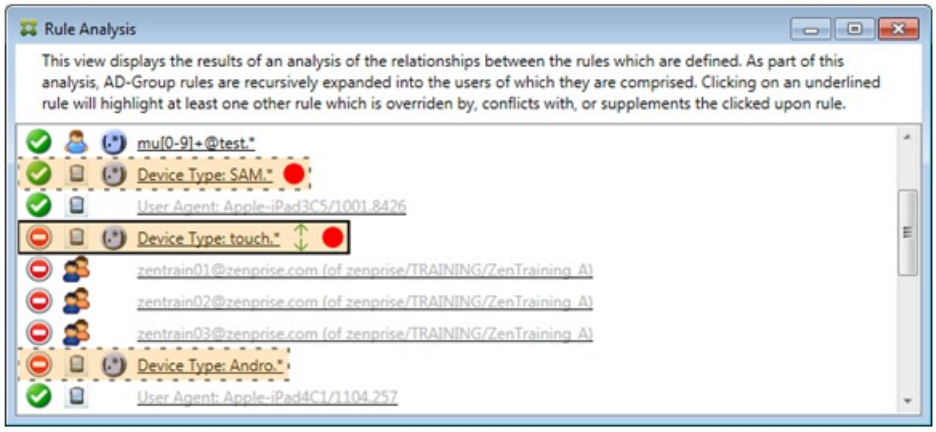


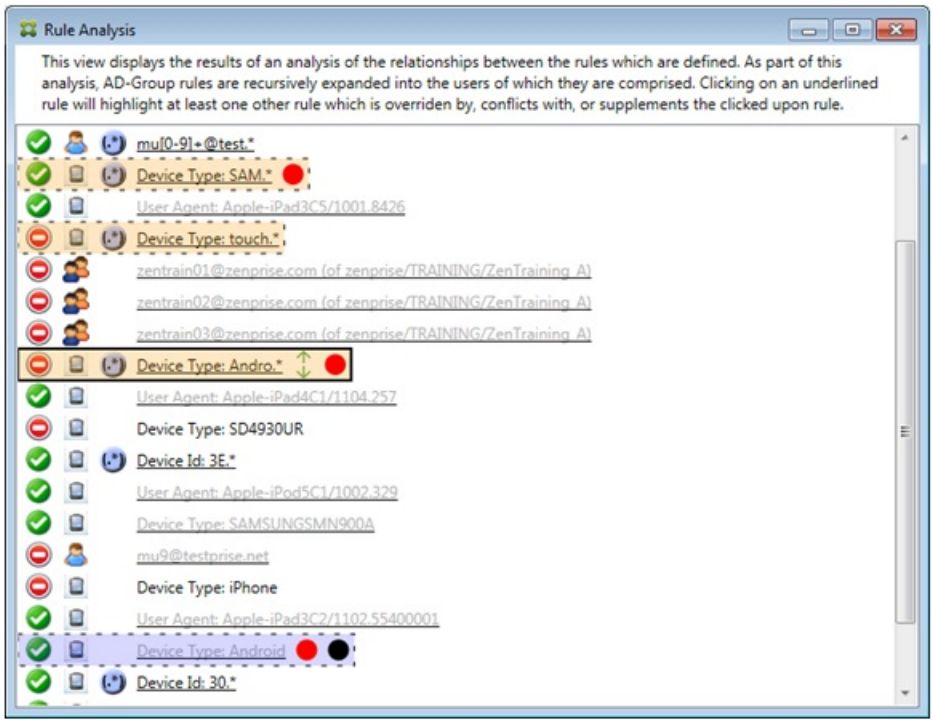
-
-
-

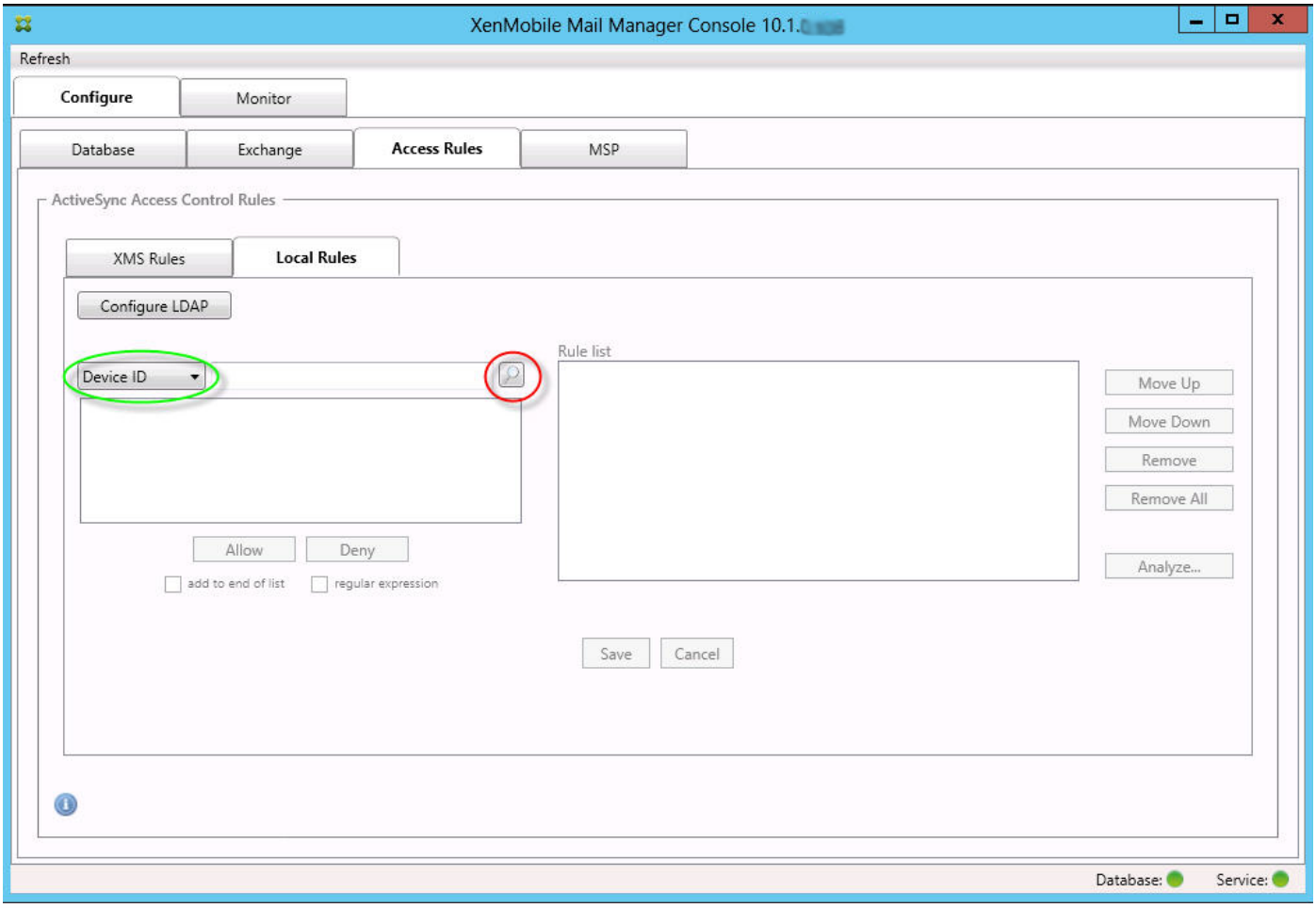


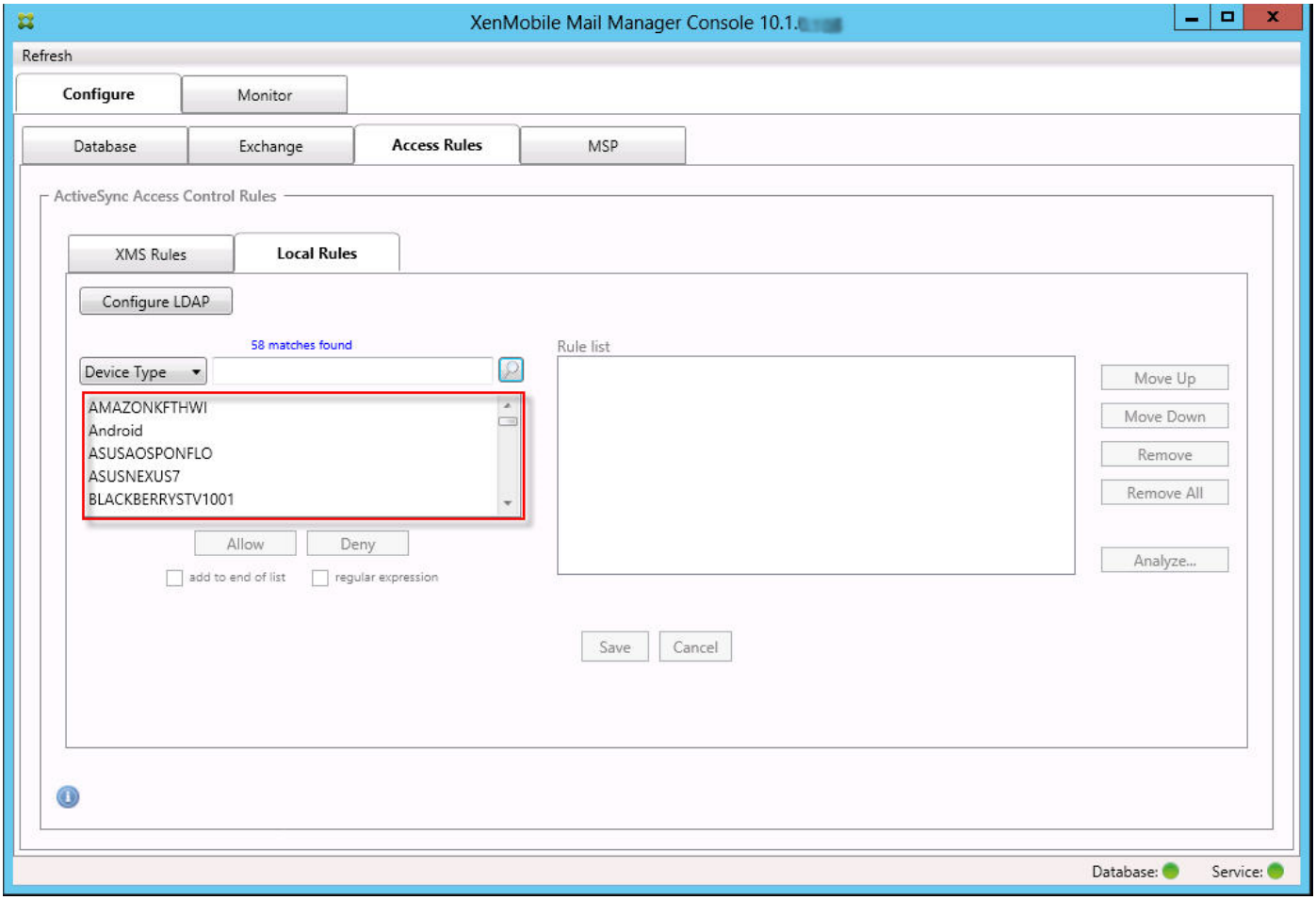
-
-

-
-
-
-
-

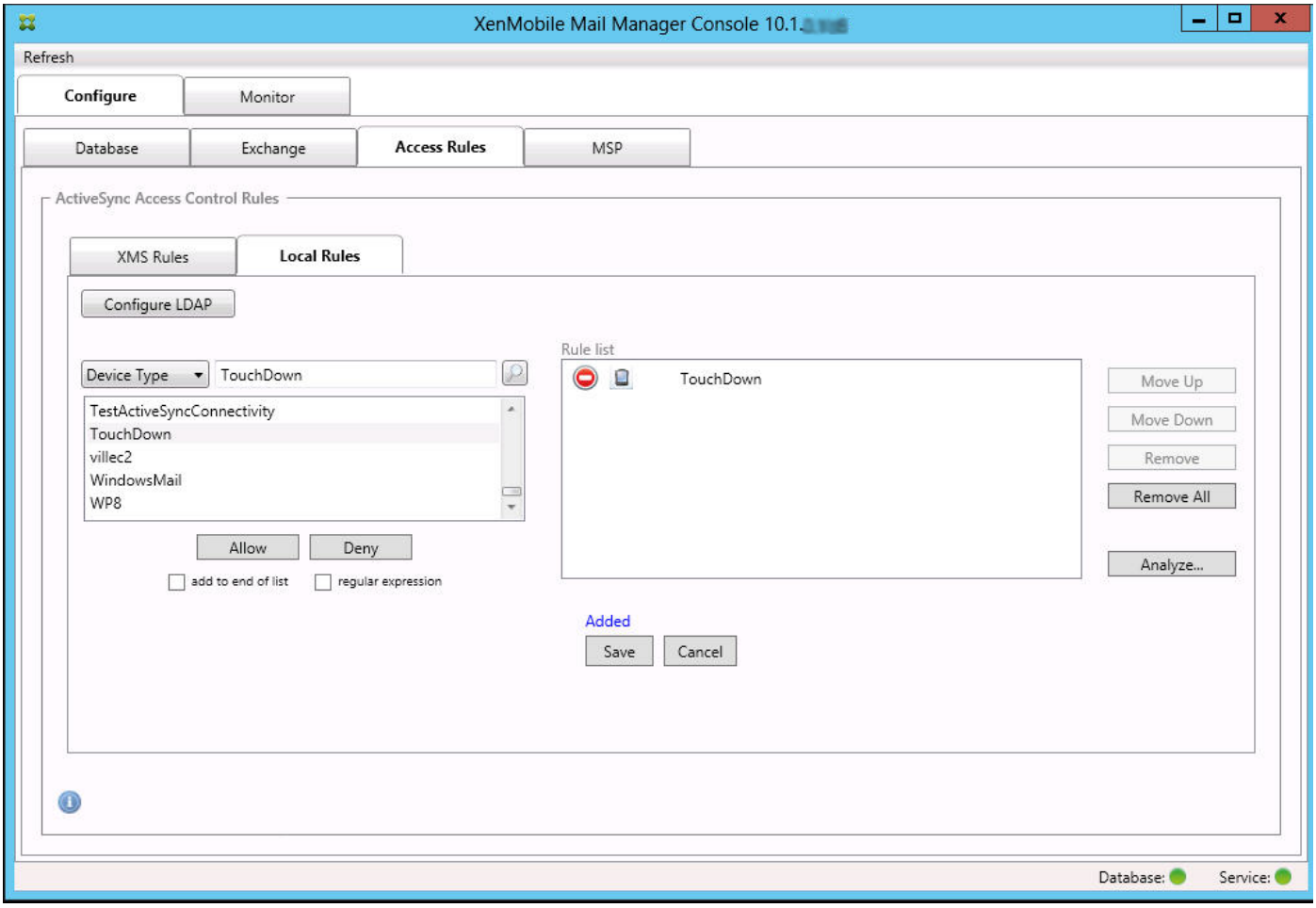


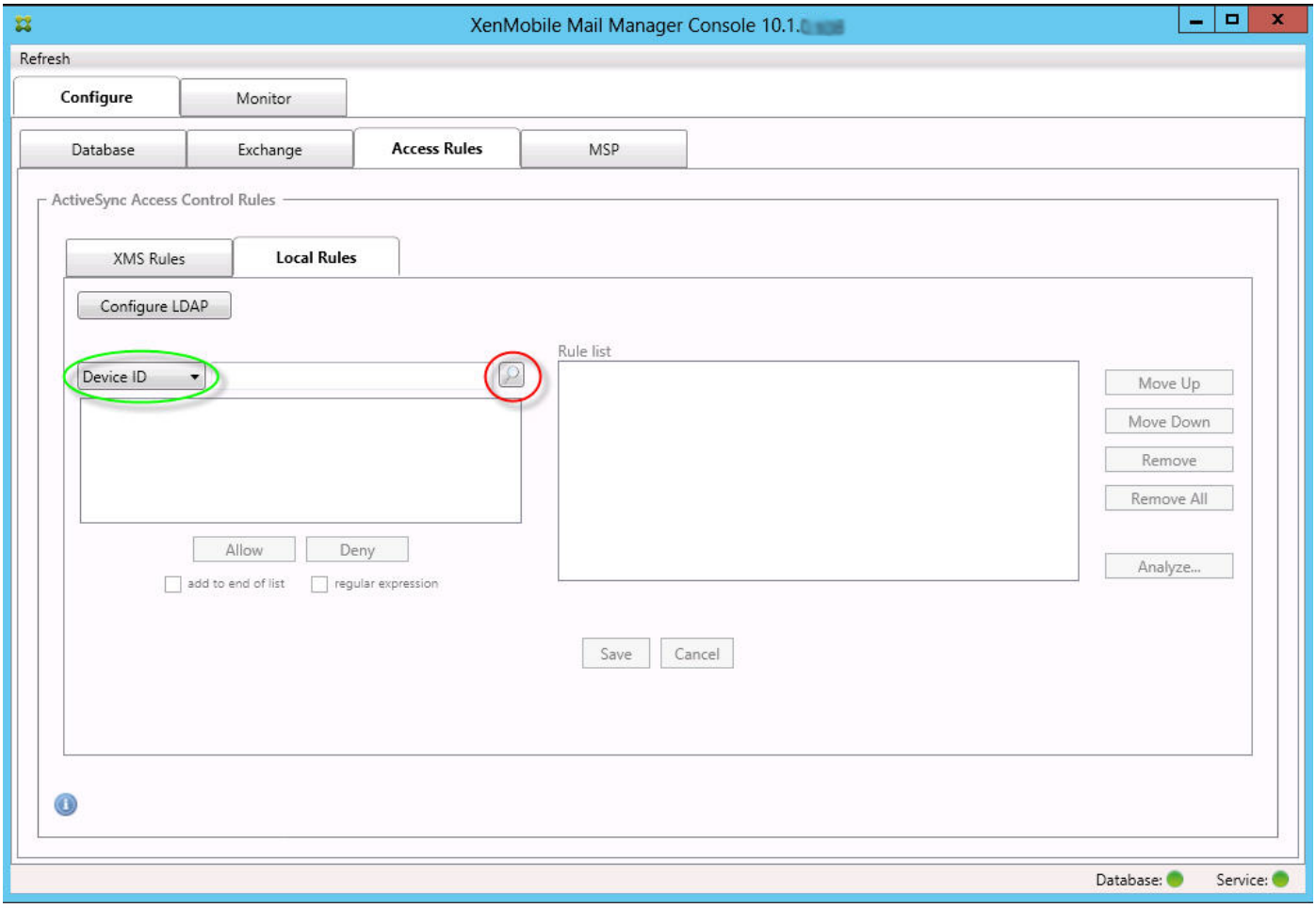


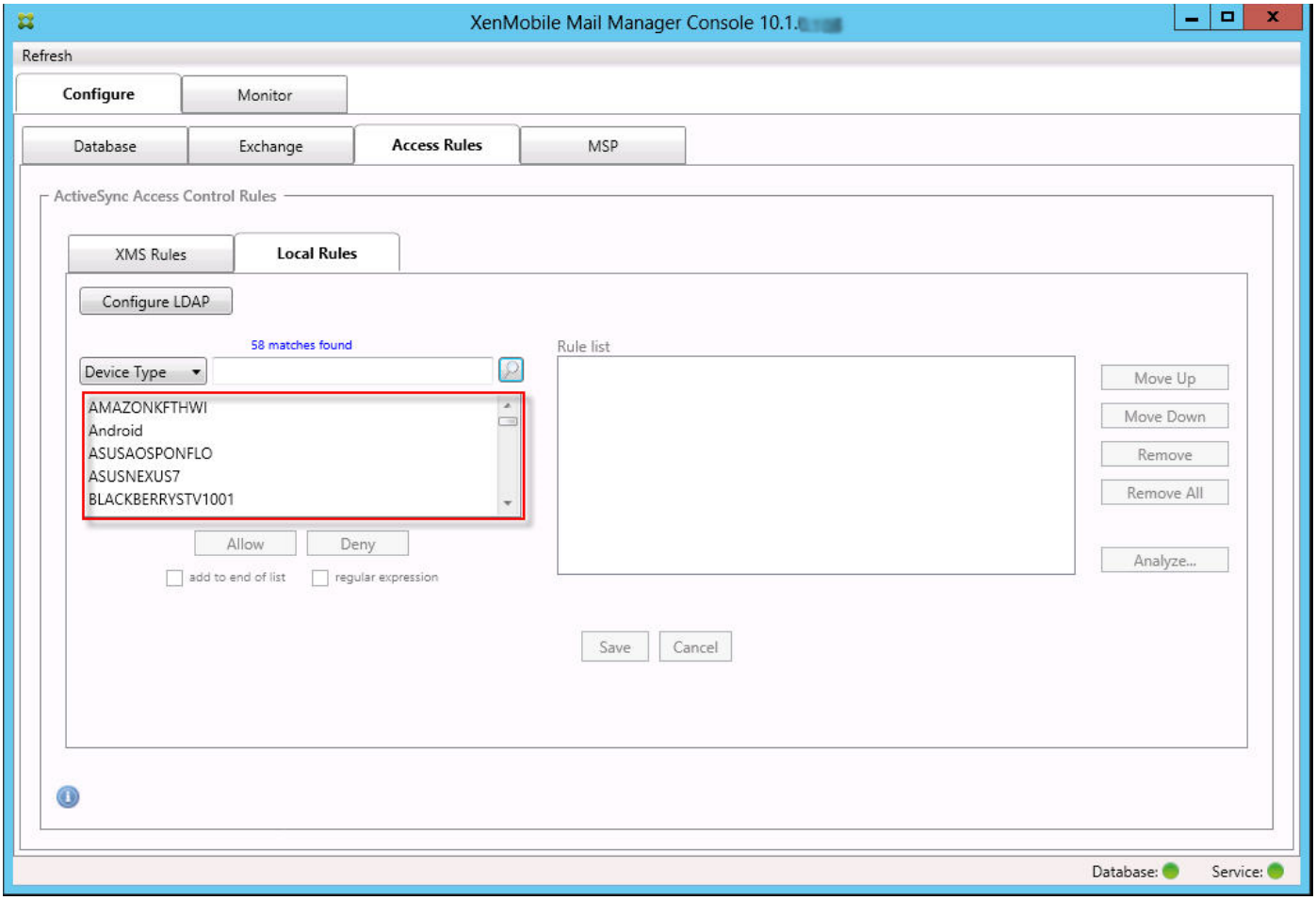


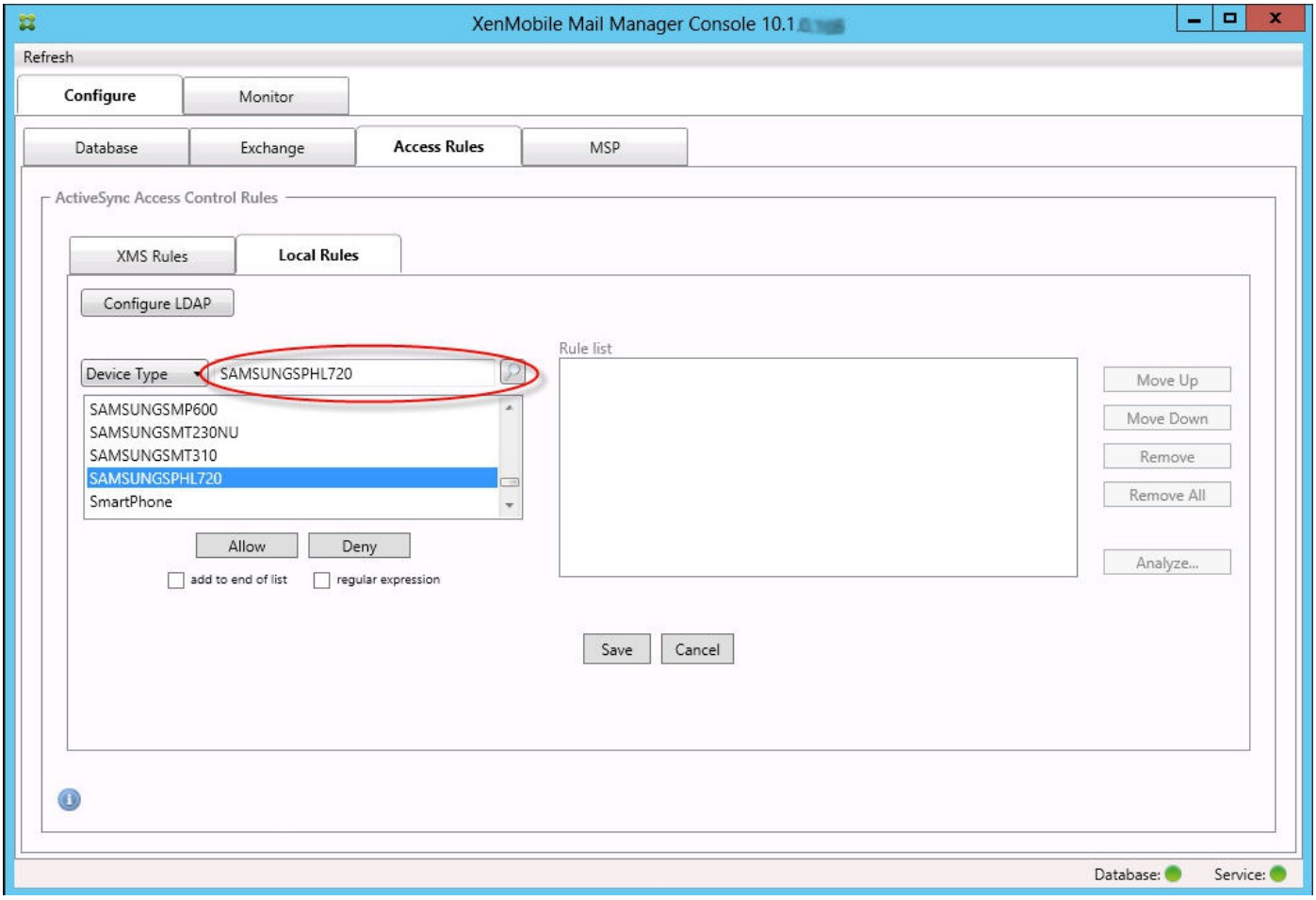


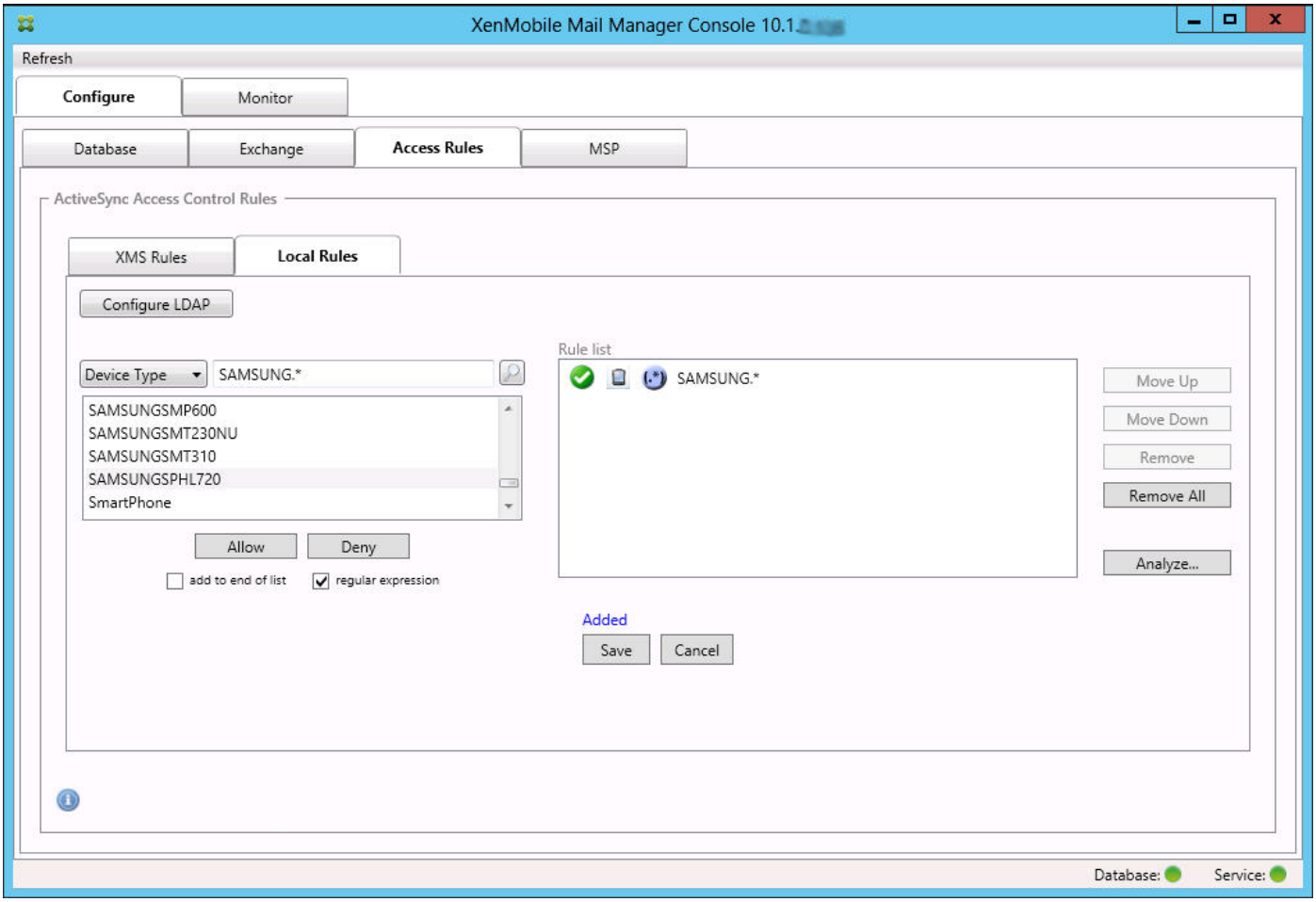
-
-

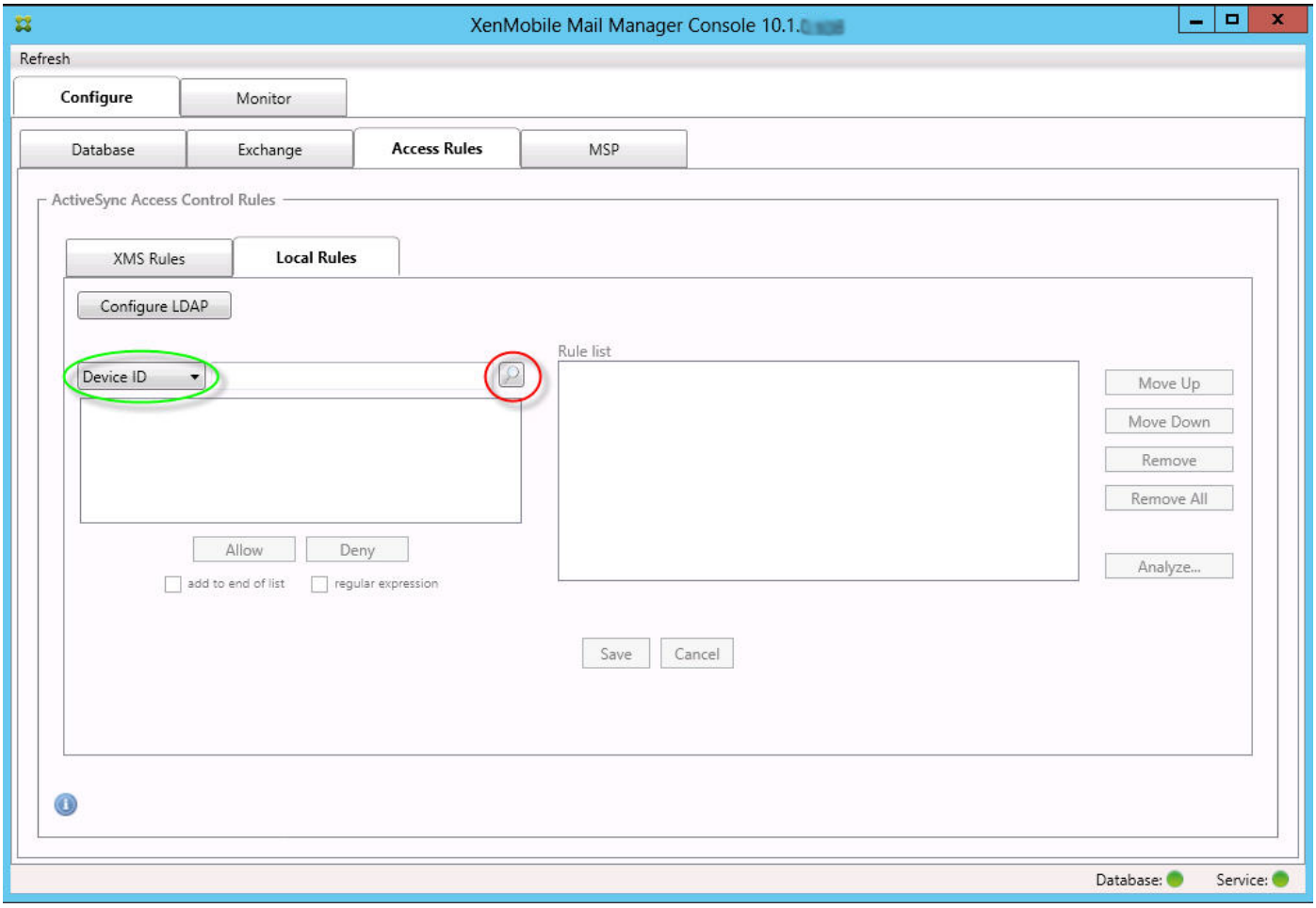


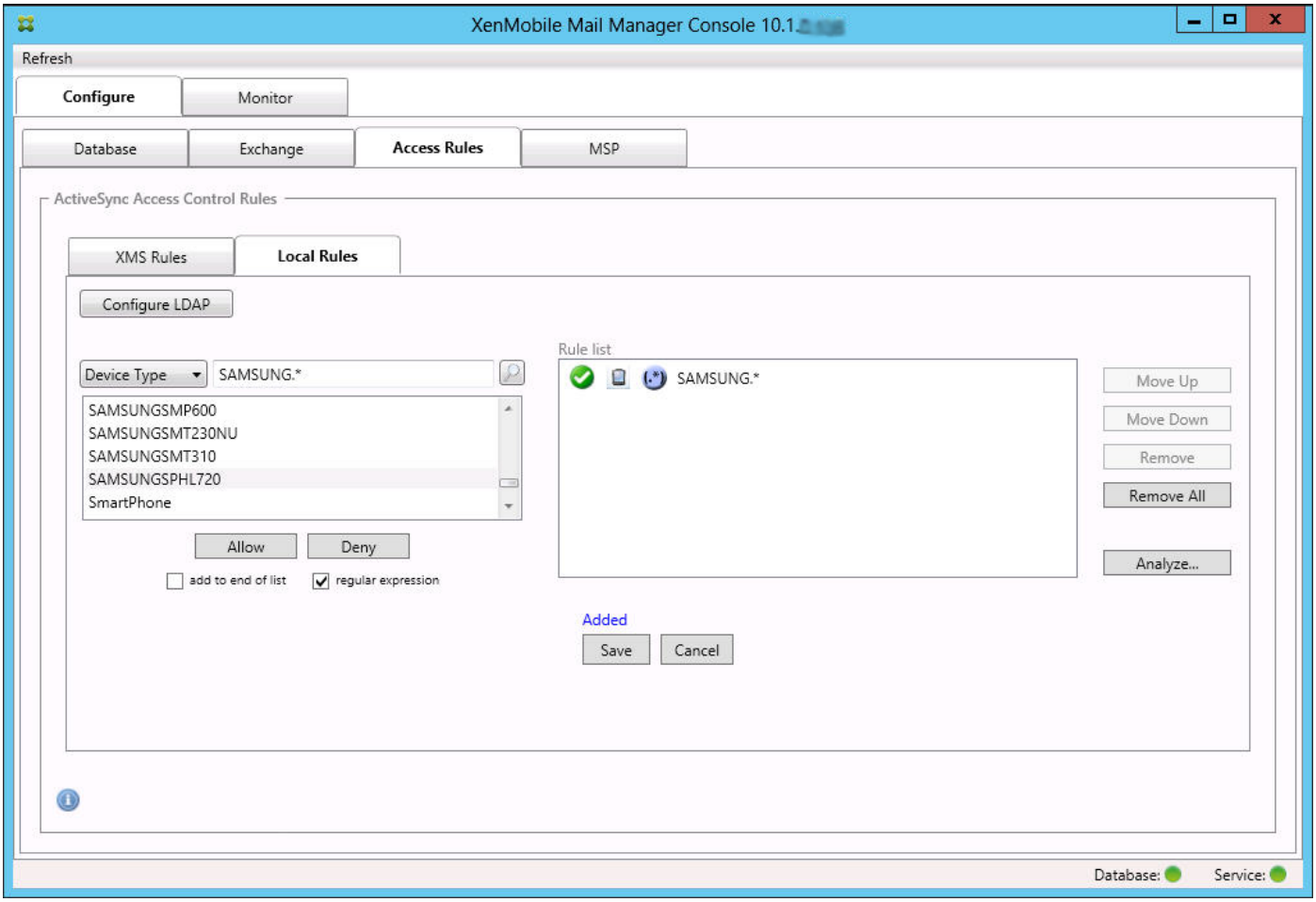


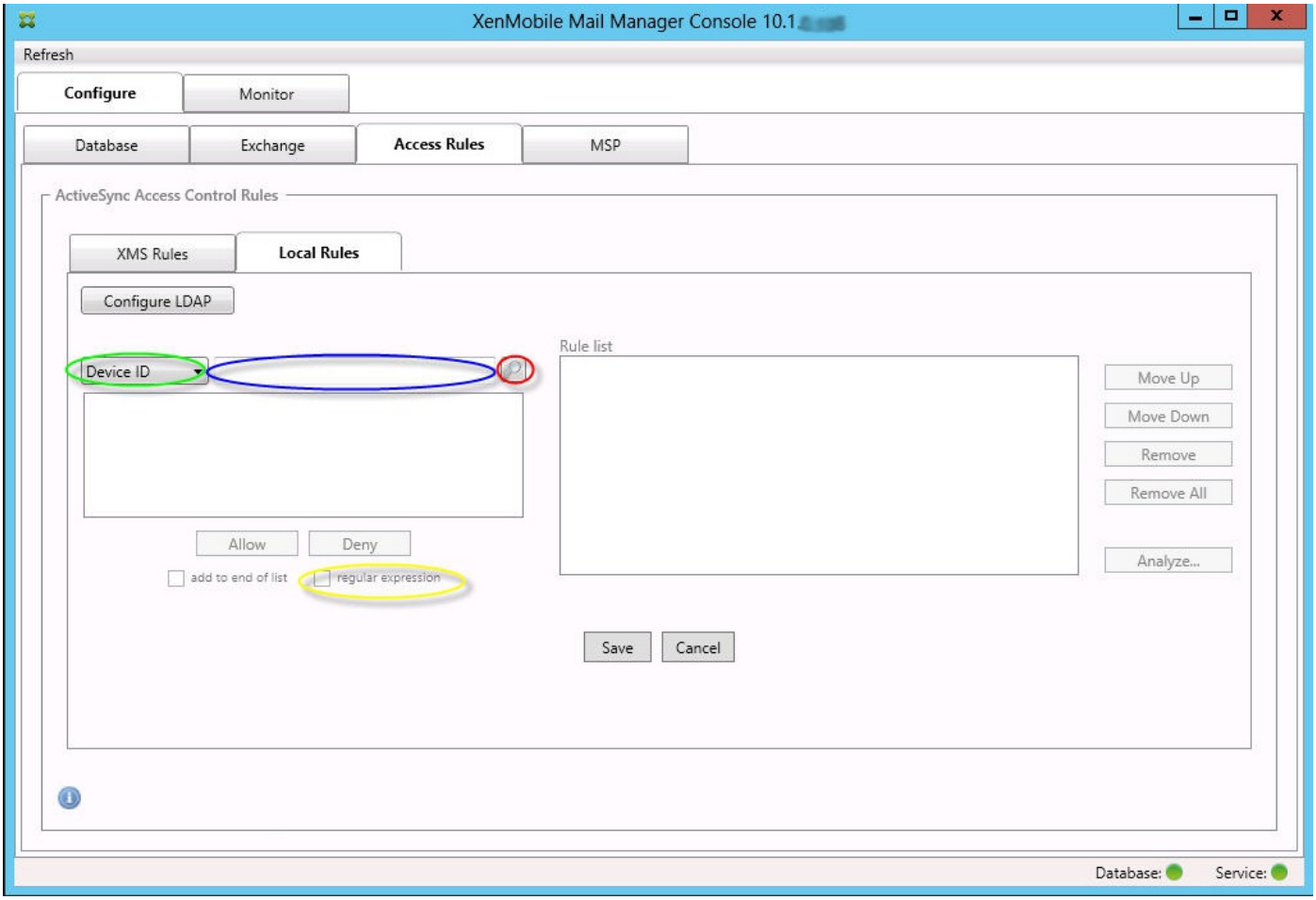


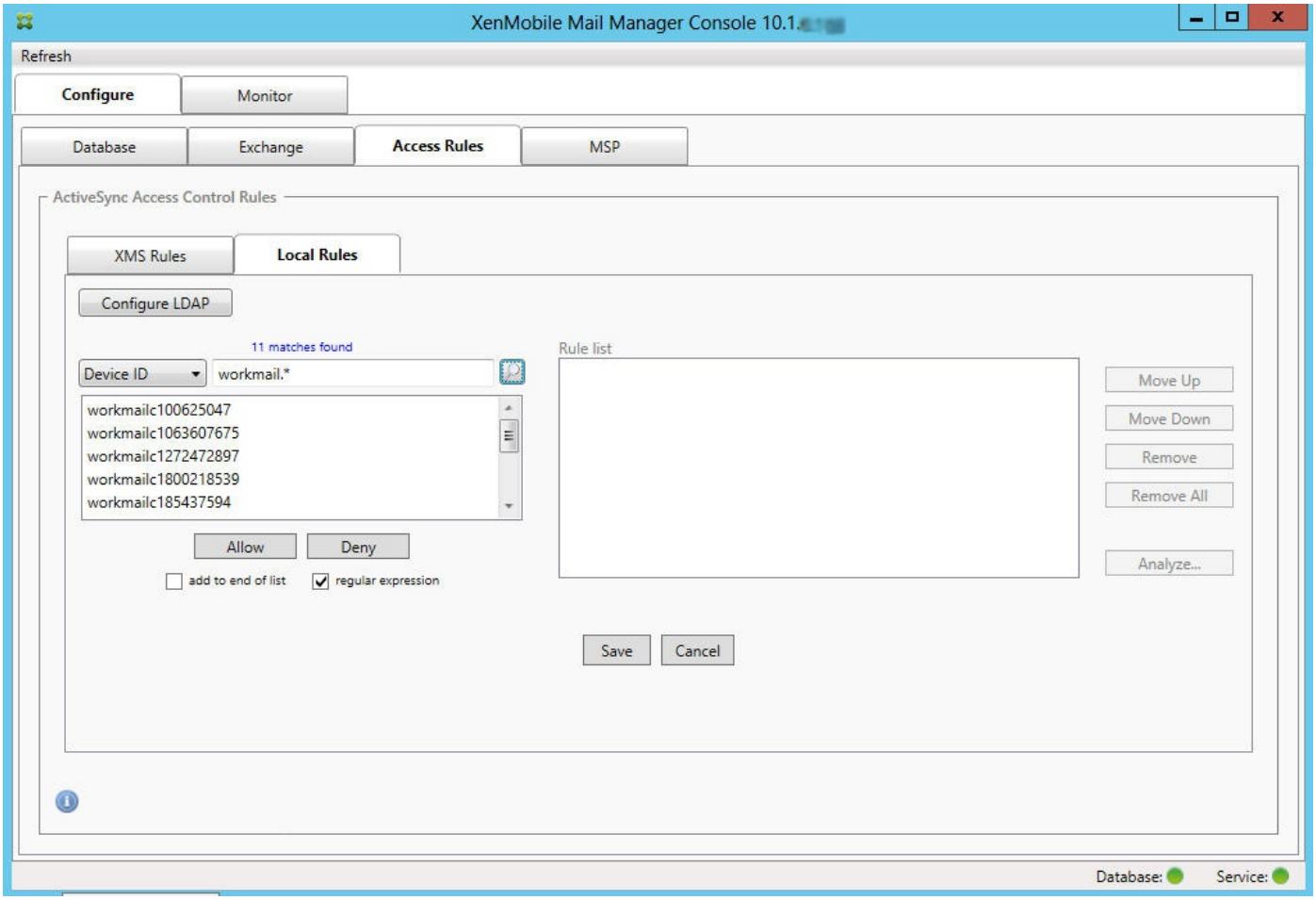


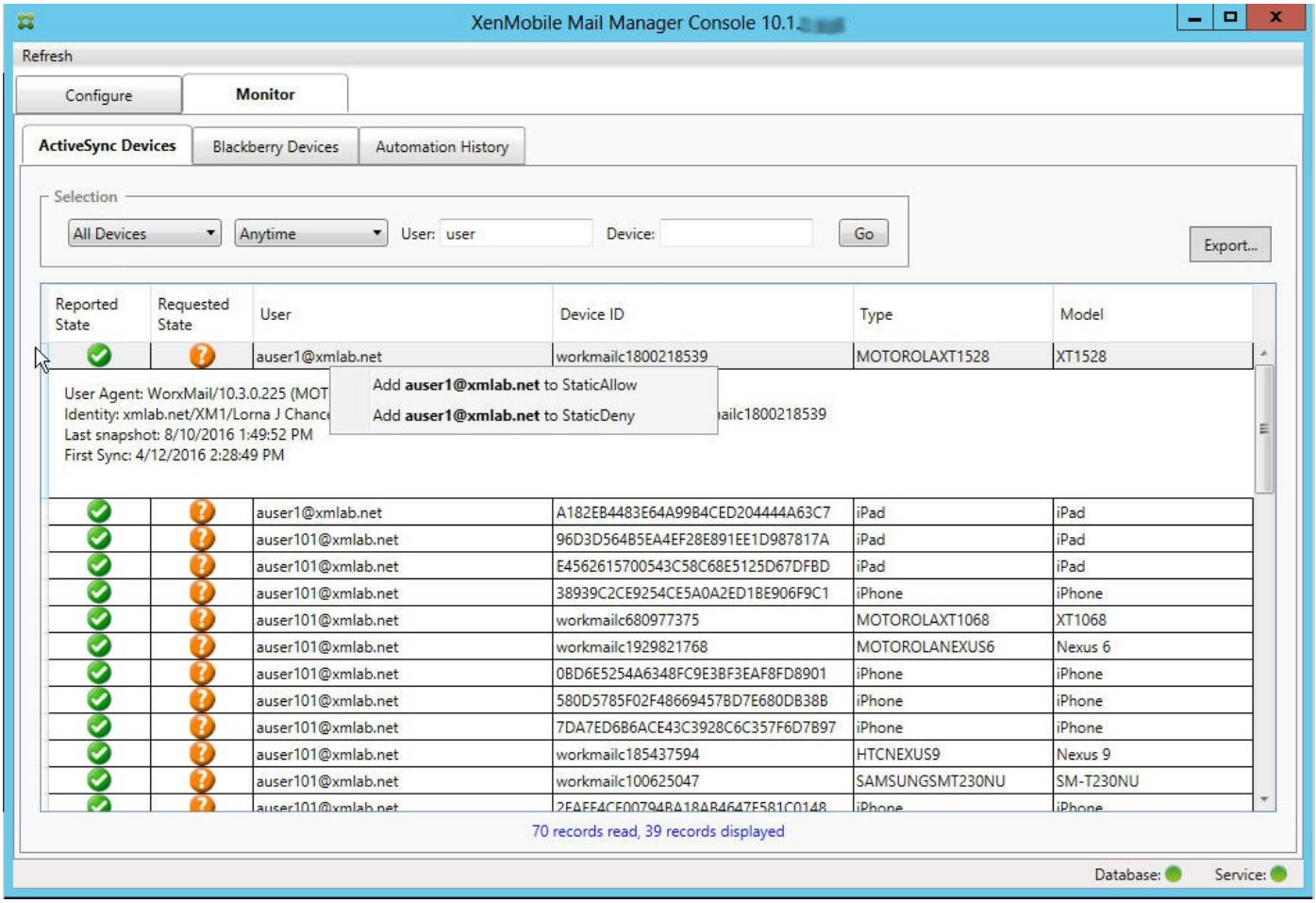






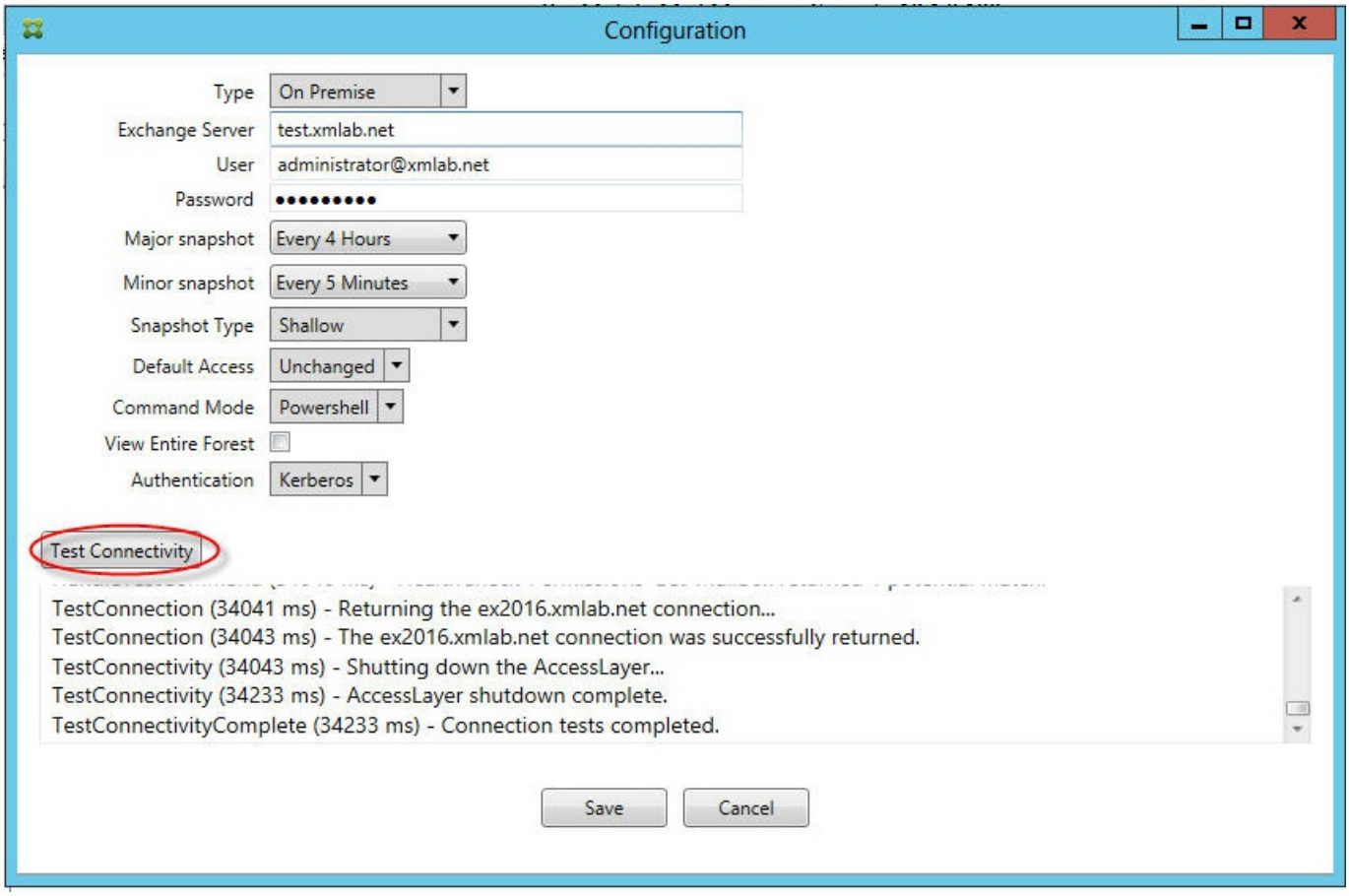






-
  -
  -
  -
-
-
-
-

-
  -
  -
-



-
-