À propos du serveur XenMobile 10.1

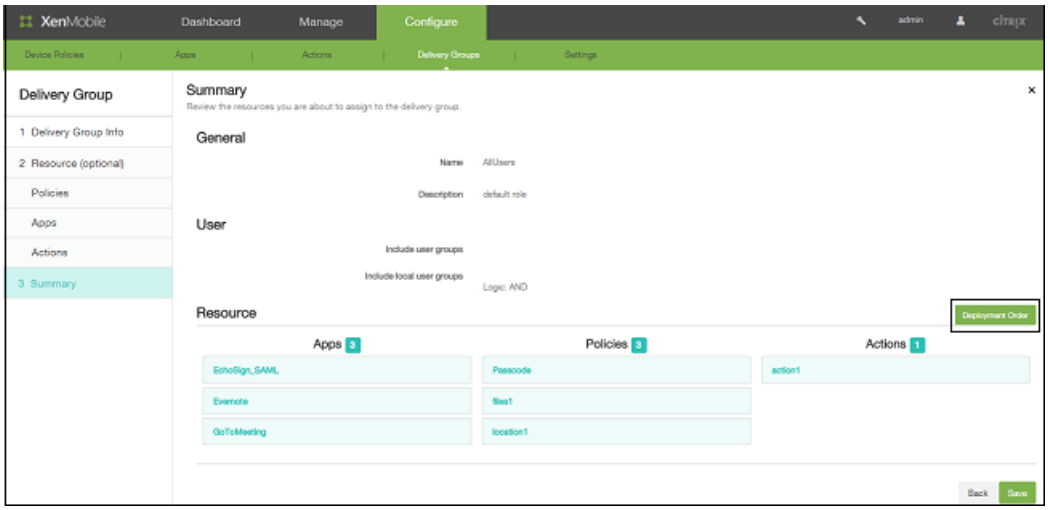
Oct 11, 2016

Vous pouvez effectuer la mise à niveau de XenMobile 10 vers XenMobile 10.1 dans la console XenMobile. Pour effectuer la mise à niveau, vous devez utiliser xms_10.1.0.62986.bin. Dans la console XenMobile, accédez à **Paramètres** > **Gestion des versions**. Cliquez sur **Mettre à niveau** et chargez ensuite le fichier xms_10.1.0.62986.bin. Pour plus d'informations sur la mise à niveau de la console, veuillez consulter la rubrique Mise à niveau de XenMobile.

> ## Remarque
>
> Le client d'assistance à distance n'est pas disponible dans XenMobile Cloud versions 10.x pour Windows CE et pour appareils Samsung Android.

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.

Ordre de déploiement des ressources. Dans XenMobile MDM Edition, vous pouvez modifier l'ordre dans lequel les ressources sont déployées dans un groupe de mise à disposition. Dans la console XenMobile, vous modifiez l'ordre de déploiement dans Configurer > Groupes de mise à disposition. Lorsque vous ajoutez ou modifiez un groupe de mise à disposition, sur la page Résumé, à côté de Ressources, vous cliquez sur Ordre de déploiement, d'où vous pouvez modifier la position des ressources qui s'affichent dans la liste pour définir l'ordre de votre choix.



Remarques :

- Les ressources dont vous pouvez trier l'ordre de déploiement doivent être des ressources gérées par XenMobile, telles que des stratégies et des applications. Toutefois, dans cette version de XenMobile MDM Edition, vous ne pouvez pas encore trier d'actions.
- Cette fonctionnalité n'est pas prise en charge pour Windows Phone et Windows Tablet. Pour appliquer un calendrier de déploiement de ressources sur ces appareils, vous devez exécuter plusieurs déploiements.

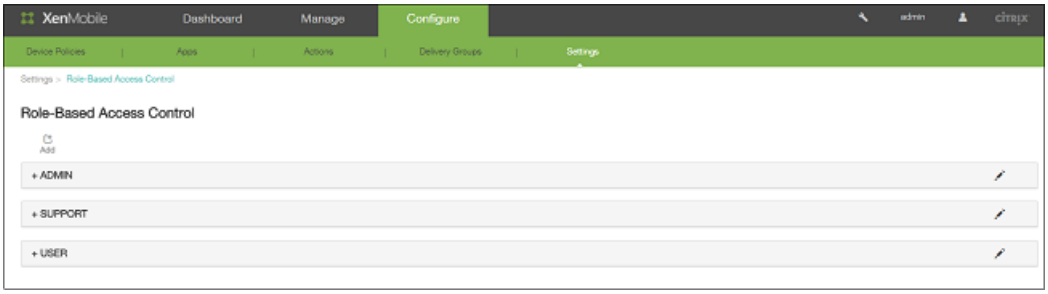
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exportation des données du tableau. Pour chaque tableau dans la console XenMobile - Applications, Stratégies, Actions, Groupes de mise à disposition, Utilisateurs et groupes locaux, Inscription et Appareils, cliquez sur Exporter pour créer un fichier .csv contenant toutes les colonnes affichées.

API REST. XenMobile prend en charge les API publiques pour les services REST pour vous permettre d'appeler les services qui sont exposés par le biais de XenMobile directement via un client REST. Vous pouvez effectuer les opérations suivantes à l'aide des API prises en charge dans XenMobile 10.1 :

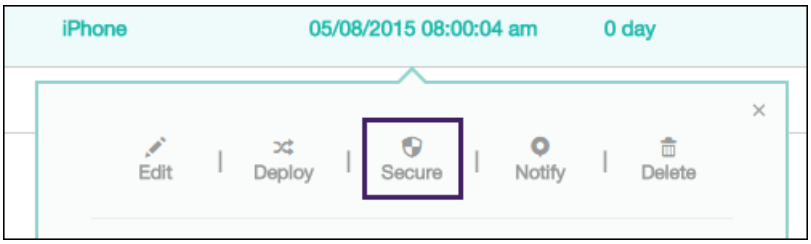
- Configurer des licences, NetScaler Gateway, LDAP et la gestion des certificats lors de l'installation initiale.
- Récupérer les détails d'un groupe de mise à disposition avec les ressources et les groupes attribués.
- Réinitialiser le mot de passe administrateur.
- Exporter un certificat PKI.
- Configurer les paramètres du serveur de notification, tels que l'ajout et la modification du serveur SMS et SMTP, la suppression et l'activation du serveur.
- Récupérer les détails de l'application et supprimer des applications.
- Définir le nom de domaine complet de l'hôte.

RBAC. Le rôle DEVICE_PROVISIONING a été supprimé de XenMobile 10.1, et la fonctionnalité de console d'assistance a été ajoutée. Dans XenMobile 10, cette fonctionnalité était disponible automatiquement pour le rôle ADMIN ; dans XenMobile 10.1, la fonctionnalité est uniquement disponible lorsque vous sélectionnez Support pour le rôle.



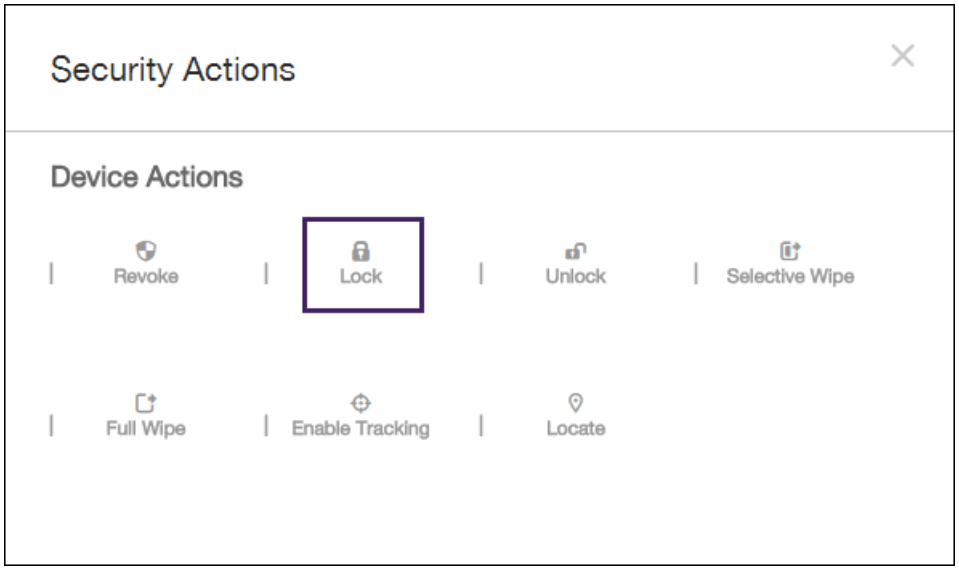
Action de sécurisation au verrouillage de l'appareil. Vous pouvez verrouiller un appareil avec l'affichage d'un message et d'un numéro de téléphone sur l'écran de verrouillage. Vous pouvez verrouiller un appareil dans la console XenMobile dans Gérer > Appareils.

Lorsque vous sélectionnez un appareil iOS dans la liste, dans la boîte de dialogue qui s'affiche, cliquez sur Sécurité.

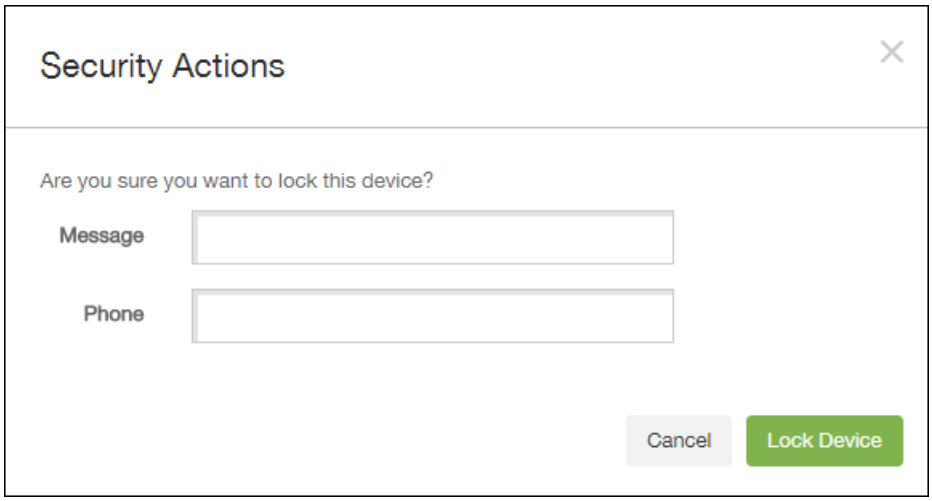


Dans la boîte de dialogue Actions de sécurisation, cliquez sur Verrouiller.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ensuite, dans le message de confirmation, vous pouvez, si vous le souhaitez, entrez un message et un numéro de téléphone, puis cliquer sur Verrouiller un appareil. Cette fonctionnalité est prise en charge sur iOS 7 et 8.



Remarque : le message et le numéro de téléphone ne s'affichent sur un appareil verrouillé que si vous avez également défini la stratégie Code secret dans la console XenMobile, ou si les utilisateurs ont activé le code secret manuellement sur l'appareil.

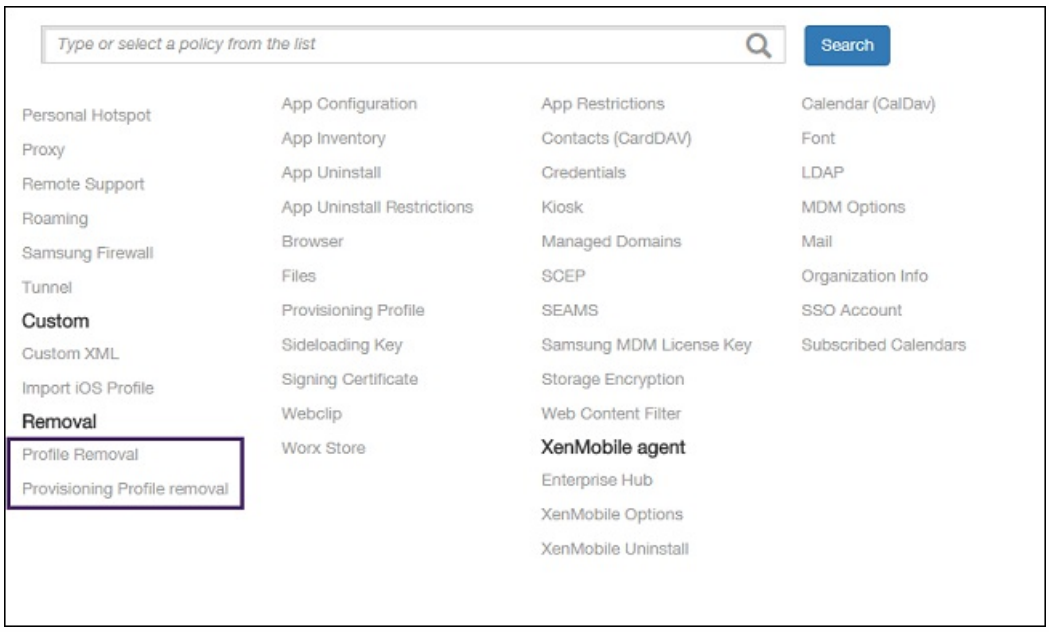
Améliorations apportées à VPP. Les fonctionnalités suivantes étendent les capacités du programme d'achats en volume (VPP) dans XenMobile.

- Permet d'importer plusieurs jetons VPP dans XenMobile ; par exemple, pour les jetons achetés dans plusieurs emplacements ou dans le cas d'organisations, d'unités organisationnelles ou de divisions qui nécessitent des jetons VPP différents.
- Les partenaires peuvent créer et déployer des applications B2B pour les utilisateurs d'appareils iOS depuis des magasins d'applications business-to-business (B2B) en ajoutant les informations d'identification d'ouverture de session à la configuration VPP dans la console XenMobile, sous Paramètres.
- Prise en charge de la gestion de plusieurs applications VPP/B2B pour les organisations qui utilisent XenMobile pour gérer les applications et les appareils de plusieurs clients VPP et sociétés multinationales. Les applications provenant de tous les comptes VPP/B2B sont automatiquement téléchargées vers XenMobile et sont automatiquement mises à jour. Vous pouvez attribuer des applications VPP/B2B spécifiques aux utilisateurs dans la console XenMobile, où vous pouvez

© 1999-2017 Citrix Systems, Inc. All rights reserved.

également afficher le compte VPP/B2B auquel une application s'applique.

Stratégies de profils de provisioning et détails des appareils. Dans XenMobile 10 et versions antérieures, vous devez distribuer le profil aux appareils utilisateur en tant que pièce jointe à un e-mail ; les utilisateurs ajoutent le profil sur leur appareil iOS en cliquant sur la pièce jointe. XenMobile 10.1 prend en charge les stratégies de profil de provisioning et les détails d'appareil suivants, ce qui facilite le suivi de l'état des profils de provisioning pour les applications d'entreprise sur appareils iOS et ne nécessite plus que les utilisateurs installent manuellement les profils sur leurs appareils.



- **Stratégie de profil de provisioning iOS**. Permet d'installer un profil de provisioning à distance sur un appareil iOS. Lorsque vous configurez la stratégie, vous devez charger un profil de provisioning iOS, puis déployer le profil sur les appareils utilisateur.
- **Stratégie de suppression de profil de provisioning iOS**. Permet de supprimer un profil de provisioning d'un appareil iOS. Vous configurez ces stratégies dans la console XenMobile depuis Configurer > Stratégies d'appareil.
- **Listes des profils de provisioning iOS**. Vous pouvez afficher un inventaire de profils iOS pour l'appareil et une liste des profils de provisioning qui sont installés sur l'appareil, indiquant l'identificateur unique universel (UUID), la date d'expiration et l'état de gestion de chaque profil. Vous pouvez afficher ces détails dans la console XenMobile sous Gérer > Appareils.

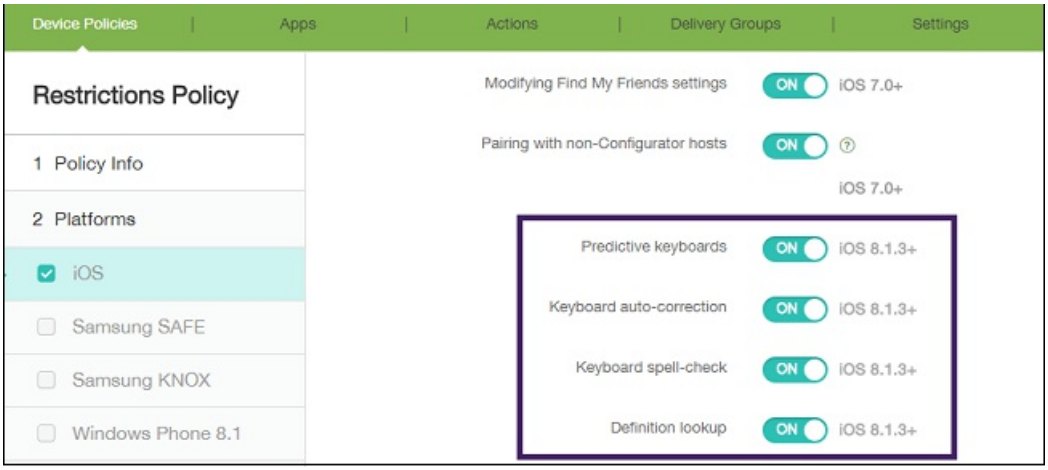
Pré-inscription à Apple Device Enrollment Program (DEP). Permet aux revendeurs de pré-inscrire les appareils dans DEP pour installer des applications gérées sur les appareils avant de distribuer ces derniers aux utilisateurs.

Intégration avec Apple Configurator. Simplifie l'inscription à grande échelle des appareils appartenant à l'entreprise. Les appareils peuvent se connecter à un Apple Configurator et sont automatiquement configurés pour installer un profil XenMobile pré-généré.

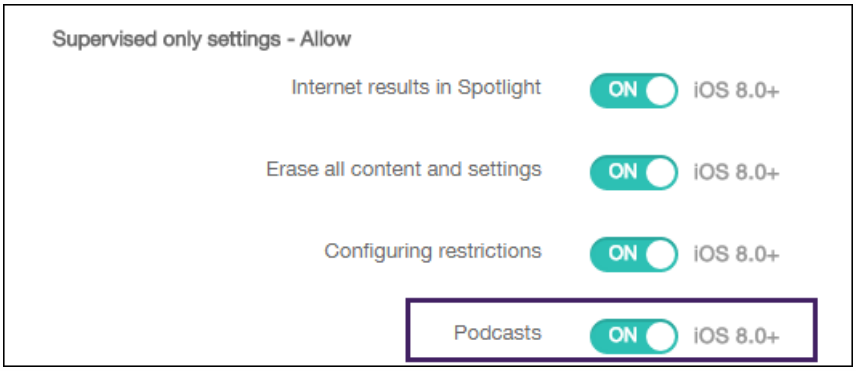
Nouvelles stratégies de restriction pour les appareils supervisés iOS.

- Autorise ou non les claviers prédictifs, avec correction automatique, avec vérification orthographique et avec recherche de définitions. Disponible sur iOS 8.1.3 sur les appareils supervisés uniquement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



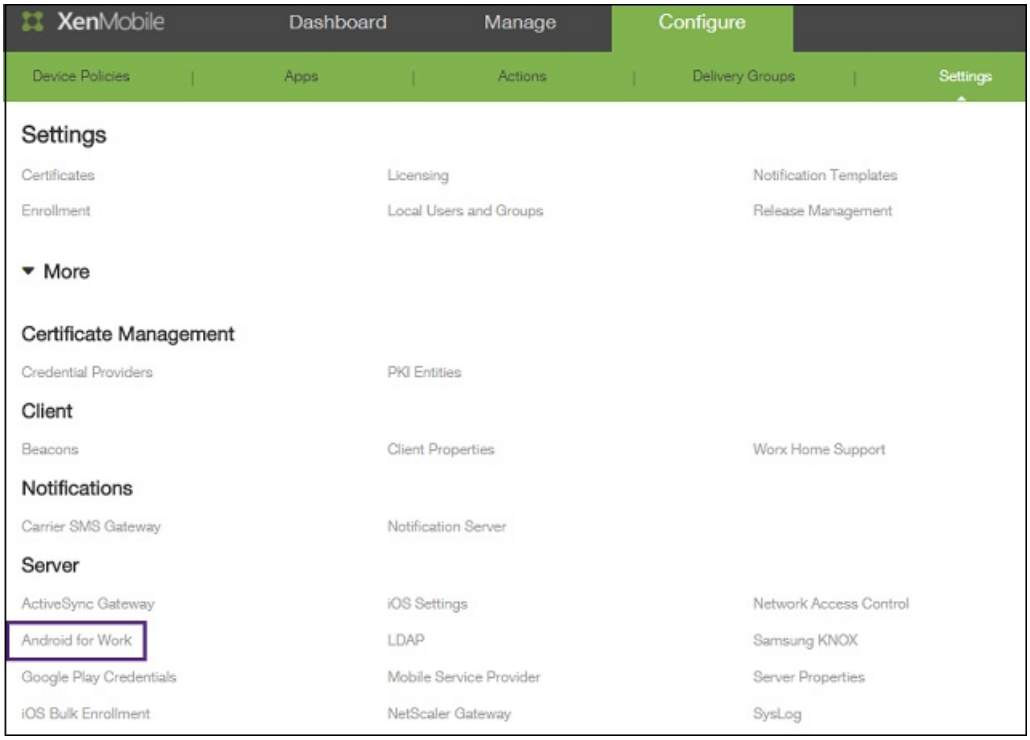
- Autorise ou non les podcasts. Disponible sur iOS 8.0 et versions ultérieures sur les appareils supervisés uniquement.

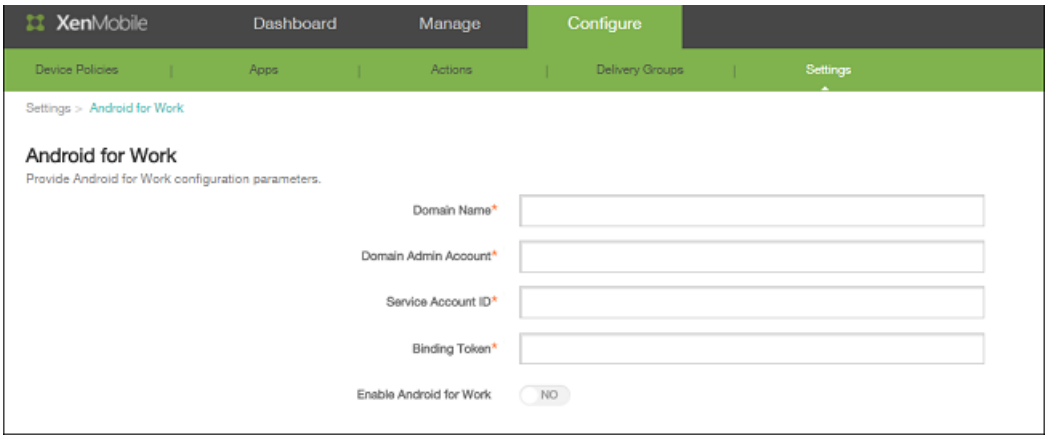


Android for Work. Espace de travail sécurisé sur les appareils qui séparent les applications et données d'entreprise des applications et données personnelles. Les organisations peuvent configurer un compte Android for Work avec Google. Vous pouvez ensuite déployer des applications approuvées à partir du magasin Google Play for Work sur des appareils utilisateur. Vous pouvez également définir des stratégies de restriction d'application pour contrôler l'accès et les fonctionnalités. Configurez les paramètres Android for Work dans la console XenMobile sous Paramètres > Serveur > Android for Work et sous Stratégies d'appareil > Sécurité > Restrictions applicatives Android for Work.

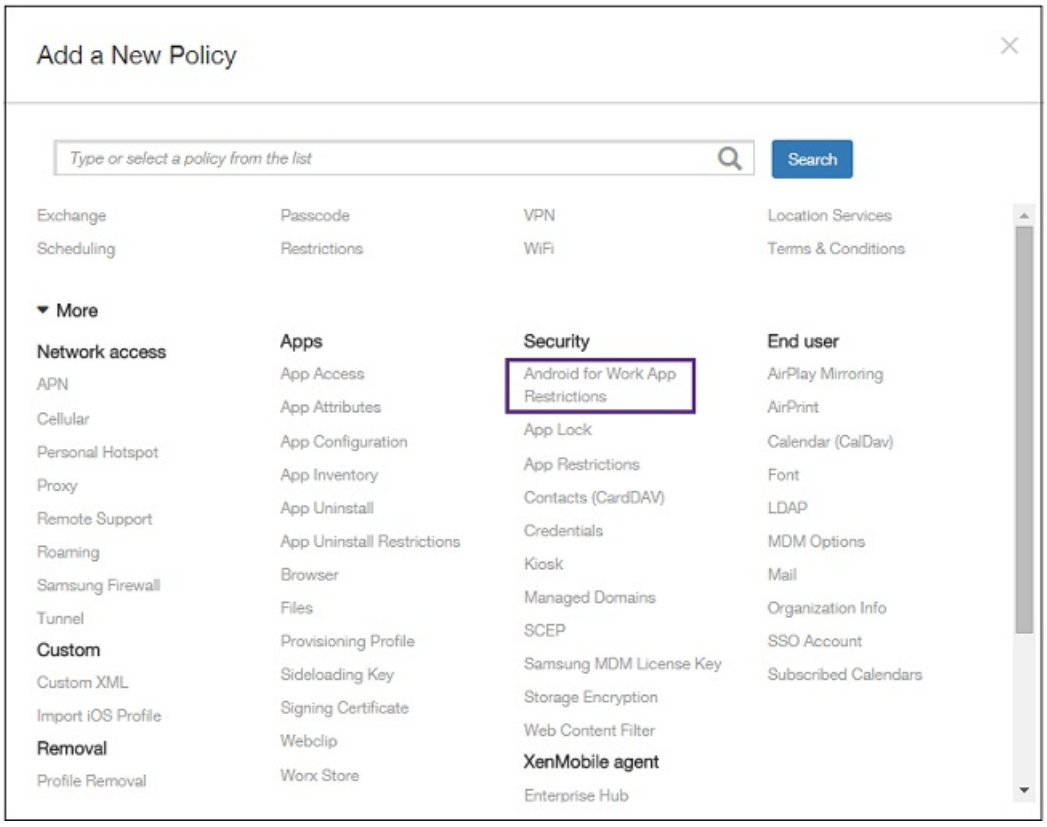
> ## Remarque
>
> Android for Work ne prend pas en charge les applications wrappées. Les utilisateurs doivent installer Worx Home sur leur appareil Android, puis ajouter des applications Android for Work à Worx Home.

© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.



Conteneur Samsung KNOX. Le tableau suivant répertorie les stratégies MDM pour le conteneur Samsung KNOX et le système d'exploitation auxquels elles s'appliquent. Le conteneur Samsung KNOX est un espace de travail sur les appareils qui sépare les applications et données d'entreprise des applications et données personnelles. Vous configurez ces paramètres de stratégie dans la console XenMobile depuis Configurer > Stratégies d'appareil > Restrictions.

Stratégie	**S'applique à Samsung KNOX Standard ; s'appliquait auparavant à Samsung SAFE**	**S'applique à Samsung KNOX Premium (KNOX 2.0)**
Permet l'utilisation de l'API Samsung SAFE pour la configuration des paramètres Nom de point d'accès (APN) et Service GPRS sur un appareil Android.	X	X
Active ou désactive l'utilisation de l'authentification CAC (Common Access Card) dans le conteneur KNOX, qui comprend les authentifications nécessaires pour l'utilisation de la messagerie et du navigateur dans le conteneur.		X
Définit la combinaison d'une empreinte digitale et d'un mot de passe comme méthode de déverrouillage.		X
Active ou désactive la capacité des utilisateurs à déplacer des applications dans le conteneur KNOX.		X
Active ou désactive l'utilisation d'un clavier non sécurisé dans le		X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégie	S'applique à Samsung KNOX Standard ; s'appliquait auparavant à Samsung SAFE	S'applique à Samsung KNOX Premium (KNOX 2.0)
conteneur KNOX. Active ou désactive le partage via une liste dans le conteneur KNOX. Autorise ou non les utilisateurs à envoyer ou recevoir des SMS et des MMS.	X	X
Autorise ou non les utilisateurs à modifier la date et l'heure manuellement.	X	
Autorise les utilisateurs à installer des applications qui sont déjà installées dans leur zone personnelle sur le conteneur KNOX.		X
Active ou désactive les applications GMS dans le conteneur KNOX.		X
Active ou désactive le placement de l'appareil en configuration Critères communs.		X
Active ou désactive le magasin de clés TIMA qui fournit un stockage de clés sécurisé basé sur TrustZone pour les clés symétriques.		X
Active ou désactive la journalisation des événements de l'appareil à des fins d'analyses poussées de l'appareil.		X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problèmes résolus de XenMobile 10.1

Jul 25, 2016

Comparaison avec : XenMobile Server 10.

Les problèmes suivants ont été résolus dans XenMobile 10.1 :

- Lorsque vous ajoutez une entité de protocole PKI générique (GPKI) avec le type d'authentification client, l'URL de WSDL n'est pas envoyée au serveur de certificats pour effectuer l'authentification.

  [#501945]

- Pour supprimer des groupes Active Directory déjà configurés dans un groupe de mise à disposition, vous devez d'abord effectuer une recherche sur les groupes Active Directory, puis désactiver les cases à cocher pour ces groupes.

  [#512990]

- Vous pouvez maintenant configurer l'autorité de certification Microsoft à l'aide de l'authentification de base.

  [#526705]

- Vous ne pouvez pas ajouter un seul appareil BlackBerry ou Windows dans la console XenMobile.

  [#532844]

- Vous pouvez maintenant installer des profils VPN sur des appareils iOS.

  [#533770]

- Lors de l'utilisation du sujet ou de la macro SAN $user.distinguishedname, un CN= supplémentaire n'est plus ajouté au nom qui est importé dans le certificat client.

  [#533837]

- RBAC : les administrateurs avec des droits en lecture seule sont maintenant uniquement autorisés à afficher. Ils ne peuvent plus afficher les options qui ne sont pas disponibles pour eux.

  [#534184]

- La création de compte échoue sur iOS lorsque NetScaler Gateway est à l'écoute sur un port autre que celui par défaut.

  [#537368]

- Dans la console XenMobile, dans les stratégies MDX, sous Authentification, le paramètre Code secret d'application ou Session en ligne requise est désormais enregistré.

  [#543397]

- La stratégie Compte SSO et VPN pour iOS fonctionne maintenant.

  [#549924]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Vous pouvez maintenant publier des applications Android personnalisées.

  [#550111]

- Les caractères spéciaux tels que $, @ et " ne sont pas reconnus dans les mots de passe pour l'interface de ligne de commande (CLI) lors de l'installation de XenMobile 10 et dans les mots de passe attribués aux certificats ; le caractère spécial et tous les caractères suivants sont ignorés et l'ouverture de session échoue. Après l'installation, le mot de passe de la CLI ne peut pas être modifié pour inclure des caractères spéciaux.

  [#541997, #542436]

- Sur les appareils Windows Phone 8.1 inscrits, aucune application gérée ne figure dans la liste d'inventaires logiciels.

  [#506143]

- Si vous configurez un nom d'affichage de Delivery Controller StoreFront comportant un caractère spécial, comme un point (.), les utilisateurs ne peuvent pas souscrire à des applications et les ouvrir avec XenApp via Worx Home. L'erreur « Impossible de traiter votre demande » s'affiche. Pour contourner le problème, supprimez les caractères spéciaux dans le nom.

  [#535497]

- La synchronisation automatique avec le cloud ShareFile ne s'effectue pas à l'heure prévue chaque jour. Par conséquent, les utilisateurs que l'administrateur ShareFile a provisionnés manuellement dans le cloud depuis la dernière synchronisation ne sont pas rapprochés.

  [#542494]

- Lorsque vous configurez une stratégie Background network services, le caractère espace est limité pour votre liste de noms de domaine complet et le port des adresses de services.

  [#542891]

- Lorsque XenMobile est installé sur un hyperviseur, l'heure sur le serveur XenMobile peut être décalée de plusieurs heures.

  [#543668]

- Lorsqu'un nom de groupe d'utilisateurs Active Directory contient un point (.), vous ne pouvez pas enregistrer le groupe de mise à disposition.

  [#547957]

- Les applications d'entreprise, telles que les applications XenDesktop et XenApp, ne s'affichent pas lorsque les utilisateurs tentent d'y accéder depuis Worx Store via Worx Home en s'inscrivant avec un autre nom principal de l'utilisateur (UPN).

  [#548339]

- Si la liste des groupes Active Directory compte plus de 255 caractères, elle est tronquée et les appartenances au groupe d'utilisateurs ne sont pas enregistrées. En conséquence, il se peut que les utilisateurs ne puissent pas s'inscrire et que les groupes de mise à disposition ne puissent pas être déployés.

  [#548762, #557918]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Sur un appareil Android ou iOS exécutant Citrix Receiver, dans certains cas, les utilisateurs ne peuvent pas ouvrir les applications StoreFront à partir de Worx Home.

  [#549824]

- Lorsque vous configurez une stratégie VPN dans la console XenMobile avec le Type de connexion IPSec, vous ne pouvez pas configurer un secret partagé. En outre, si vous définissez le paramètre Activer VPN sur demande sur ON, dans la liste Action sur demande, vous ne pouvez pas spécifier d'action.

  [#550560, #550844, #553296]

- Dans la console XenMobile, lorsque vous configurez une option de verrouillage des actions sécurisées iOS, les champs de message et de numéro de téléphone autorisent des chaînes trop longues pour être affichées correctement sur l'appareil. En outre, si vous cliquez sur le bouton Verrouiller, vous recevez un message d'erreur si le champ du message contient un point d'interrogation (?). Enfin, après configuration des champs de message et de numéro de téléphone et d'une autre commande de verrouillage, les champs de message et de numéro de téléphone contiennent parfois les informations de configuration précédentes.

  [#551200, #551201, #554811]

- Vous ne pouvez ni créer ni déployer une stratégie Exchange ActiveSync lorsque le numéro de port suit l'adresse du serveur, comme dans mail.exemple.com:8443.

  [#551313]

- Lorsque vous configurez l'authentification LDAP, si la longueur du nom d'utilisateur et du mot de passe est supérieure à 76 caractères, une erreur se produit lorsque vous demandez un certificat CA.

  [#553276]

- Lorsque vous configurez une entité PKI, si vous utilisez un nom unique dans le nom d'objet du certificat que vous chargez vers XenMobile, le nom du certificat inclut « CN », comme dans CN = CN=Admin, Jean.

  [#553280]

- Lors de la création d'un modèle de confirmation d'inscription, si vous configurez une macro pour le destinataire de ${device.imei} afin de renvoyer l'IMEI du périphérique, la macro renvoie continuellement l'IMEI du premier appareil inscrit par les utilisateurs et non l'IMEI des appareils suivants. Le problème se produit lorsque les utilisateurs ont défini les mêmes informations d'identification de connexion pour chaque appareil inscrit.

  [#553282]

- Lorsque vous configurez une nouvelle instance de NetScaler Gateway, si vous définissez le Type d'ouverture de session sur Domaine uniquement, vous ne pouvez pas définir le paramètre Mot de passe requis sur OFF.

  [#553628]

- Les stratégies de restriction Samsung pour Autoriser le contrôle du matériel et Ajouter des profils sous Wi-Fi n'ont aucun effet sur les appareils.

  [#555938]

- Vous ne pouvez pas wrapper les fichiers Android .apk dont le développement a été personnalisé. Lorsque vous tentez de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

charger l'application .apk sur XenMobile, une erreur de type de paquetage non valide se produit.

[#557089]

- Dans la console XenMobile, le filtre pour Android for Work est absent de la page Stratégies d'appareil.

  [#558298]

- Dans la console XenMobile, lorsque vous utilisez un verrou sur un appareil inscrit dans Android for Work, vous voyez une option permettant de verrouiller l'appareil avec un code secret.

  [#559098]

- Lorsque vous réinscrivez un appareil avec un autre utilisateur dans Android for Work, le champ E-mail principal Google Directory n'est pas mis à jour avec les nouvelles informations de l'utilisateur.

  [#559161]

- La distribution de l'application Google Play sur un appareil Android for Work échoue.

  [#559174]

- Après le déploiement d'une stratégie de restrictions applicatives Android for Work, l'onglet Appareils de la console XenMobile est inaccessible. De plus, vous ne pouvez pas modifier la nouvelle stratégie.

  [#560225]

- Vous êtes en mesure de charger une application publique non approuvée sur la plate-forme Android for Work.

  [#560390]

- Lorsque vous sélectionnez la condition de déploiement Uniquement lorsque le déploiement précédent a échoué, après que vous déployez des applications wrappées qui sont alors installées sur des appareils inscrits, les applications ne s'affichent pas lorsque les utilisateurs accèdent à Worx Store ultérieurement. L'icône de l'application ne s'affiche plus sur le springboard de l'appareil.

  [#560500]

- Dans la console XenMobile, lorsque vous configurez une entité GPKI générique, si vous définissez le serveur d'adaptateur PKI principal sans authentification, le GPKI ne se connecte pas aux ports HTTPS. Le message d'erreur suivant s'affiche : Impossible de localiser le WSDL avec l'URL que vous avez fournie. Vérifiez l'URL WSDL et réessayez.

  [#560707]

- Lorsque les paramètres de serveur Android for Work sont incorrects, vous pouvez activer Android for Work.

  [#561475]

- Vous pouvez ajouter une application Android for Work auto-hébergée à un groupe de mise à disposition comme application requise.

  [#561485]

- Dans la console XenMobile, lorsque vous configurez une option de verrouillage d'actions sécurisées iOS, le champ de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

numéro de téléphone permet d'entrer plusieurs signe plus (+).

[#561792]

- Dans la console XenMobile, lorsque vous enregistrez une stratégie de restriction d'appareil Samsung KNOX, un message d'erreur s'affiche.

  [#562607]

- Lorsque vous enregistrez une configuration Android for Work sans avoir importé un certificat Android for Work, une erreur de configuration se produit.

  [#562983]

- Lorsque vous créez une stratégie de désinstallation d'application pour Samsung KNOX, puis déployez la stratégie pour supprimer une application spécifique, l'application est supprimée du conteneur KNOX et l'icône est supprimée du springboard de l'appareil, mais l'application s'affiche de nouveau après environ 3 à 4 secondes.

  [#562713]

- Lorsque vous configurez une stratégie de navigateur Samsung Android for Work, les URL des signets ne sont pas validées.

  [#565379]

- Dans la console XenMobile, lorsque vous créez une stratégie de restriction d'appareil Samsung SAFE, un message d'erreur s'affiche lorsque vous enregistrez la stratégie.

  [#565697]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problèmes connus de XenMobile Server 10.1

Jul 25, 2016

Les problèmes suivants sont connus dans XenMobile 10.1.

- Dans XenMobile 10.x, vous pouvez rechercher des noms de groupes uniquement à l'aide de noms antérieurs à Windows 2000, car la console XenMobile affiche le sAMAccountName au lieu du nom commun.
- Étant donné que les services IIS sur les serveurs exécutant Windows 2008 ont un défaut de négociation SSL dans la mise en œuvre de TLS v1, des problèmes se produisent avec Java 8 :

  [#492269]

- XenMobile Server 10.1 est pris en charge par les autorités de certification Windows 2008 R2 à condition d'appliquer une solution de contournement. Pour activer la prise en charge de TLSv1.1 et de TLSv1.2, suivez les instructions de l'article de base de données Microsoft https://support.microsoft.com/en-us/kb/245030, dans la section « SCHANNEL\Protocols subkey ».
- XenMobile Server 10.1 n'est pas pris en charge avec les autorités de certification « vanilla » de Windows 2008.
- Pendant l'inscription, les appareils iOS peuvent rencontrer des erreurs pendant ou après l'installation du profil de gestion de la flotte mobile (MDM). Les messages « Cocoa erreur 4097 » ou « Le profil ne peut pas être déchiffré » peuvent s'afficher respectivement sur les appareils exécutant iOS 8.1 ou les appareils exécutant des versions antérieures de iOS. Si cela se produit, les utilisateurs doivent essayer de s'inscrire à nouveau. Dans certains cas, plusieurs tentatives sont nécessaires.
  [#507948]
- Lors de la réinscription d'un appareil, l'inscription peut échouer si les utilisateurs se réinscrivent trop tôt après s'être désinscrits.
  [#516567]
- L'énumération d'applications échoue lorsque des groupes de mise à disposition sont définis avec des groupes Active Directory appartenant à des domaines parent et enfant utilisant l'opérateur ET. Pour éviter ce problème, utilisez l'opérateur OU lors de la définition des groupes de mise à disposition.
  [#518084]
- Lorsque vous créez une action dans laquelle Disabled user est True, lorsque le problème est déclenché, l'action que vous configurez ne se produit pas.
  [#531024]
- Lorsque vous configurez le serveur XenMobile avec une lettre majuscule dans le nom d'hôte, par exemple ABC.Xms.com, Worx Store ne s'ouvre pas sur les appareils après l'inscription des appareils.
  [#545527]
- Sur un appareil Android en mode Android for Work, lorsque vous ajoutez une entité PKI avec un fournisseur d'informations d'identification de protocole PKI générique ou les Services de certificats Microsoft, et que vous associez les informations d'identification d'une stratégie d'informations d'identification avec une autre stratégie, le certificat est révoqué et régénéré par erreur lorsque les utilisateurs actualisent les stratégies d'appareils à partir de Worx Home. Pour contourner le problème, déployez le certificat une seule fois.
  [#547905]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Lorsque vous créez une stratégie Exchange pour Windows Phone 8.1 et que vous avez configuré le niveau de journalisation sur De base, le déploiement échoue. Il s'agit d'un problème de tiers.
  [#555923]

- Dans la console XenMobile, lorsque vous configurez une stratégie de navigateur pour Android for Work, pour les adresses URL figurant dans la liste noire, la stratégie est appliquée pour les correspondances exactes. Par exemple, si vous accédez à http://www.exemple.com, seule cette URL est bloquée, mais pas https://www.exemple.com ou http://www.exemple.com.pk.
  [#560963]

- Les appareils Windows Phone 8.1 ne peuvent pas se connecter au serveur XenMobile après le renouvellement du certificat. Il s'agit d'un problème de tiers.
  [#561511]

- Vous pouvez choisir une action d'effacement complète dans la console XenMobile à partir du tableau de bord pour les appareils Android for Work, mais les appareils ne prennent pas en charge cette action. Lorsque vous choisissez cette action, les appareils Android for Work sont sélectivement effacés et les utilisateurs ne peuvent pas se réinscrire dans XenMobile, sauf si vous supprimez l'appareil de XenMobile.
  [#562642]

- Dans Worx Home pour iOS, lorsque vous lancez une application Windows hébergée sur un Delivery Controller XenApp avec un nom d'affichage contenant des caractères spéciaux (#% ^), il se peut que le message d'erreur « Accès à votre réseau d'entreprise non disponible » s'affiche.
  [#564069]

- Lorsque vous créez une stratégie de mot de passe et définissez la complexité sur Alphanumérique ou Numérique, après le déploiement de la stratégie sur des appareils Windows Phone 8.1, les utilisateurs ne peuvent pas choisir de lettres sur le clavier. Il s'agit d'un problème de tiers.
  [#565682]

- Sur les appareils Windows Phone 8.1, si les utilisateurs choisissent de ne pas installer Worx Home lors de l'inscription, les applications d'entreprise requises sont automatiquement déployées et installées par erreur sur l'appareil.
  [#566166]

- Dans la console XenMobile, lors de la configuration des paramètres RBAC, lorsque vous ajoutez un rôle, en Accès autorisé, vous devez désactiver la case à cocher d'accès à la console d'administration ou sélectionner une ou plusieurs options dans les fonctionnalités de la console. Si ce n'est pas le cas, vous pouvez toujours ajouter le rôle, mais une erreur s'affiche lorsque les utilisateurs ouvrent une session sur la console.
  [#567076]

- L'obligation d'utiliser des mots de passe iTunes sur les appareils iOS 8.3 + n'est pas appliquée.
  [#567434]

- L'inscription basée sur certificat de Worx Home échoue sur Windows Phone 8.1. Pour résoudre ce problème, consultez l'article http://support.citrix.com/article/CTX141541.

  [#567812]

- Après la migration des données dans un déploiement d'entreprise XenMobile vers XenMobile 10.1, les problèmes suivants se produisent sur les appareils Windows Phone 8.1 inscrits :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Les utilisateurs disposant d'appareils Windows Phone 8.1 ne peuvent pas se connecter à Worx Store.
- Les utilisateurs ne peuvent pas ouvrir les applications d'entreprise installées à partir de Worx Home, mais ils peuvent les ouvrir à partir du menu principal.
- Les utilisateurs ne peuvent pas ouvrir Worx Store.

[#568316]

- Lors de la création de règles de déploiement avancées, si vous ajoutez une règle pour Limiter par nom de propriété d'appareil connu et que vous définissez la valeur de la propriété sur True ou False, la règle ne fonctionne pas comme prévu. Par exemple, la règle Supervisé égal à False ne fonctionne pas. Pour contourner le problème, la valeur de la propriété à choisir pour Limiter par nom de propriété d'appareil connu doit être une valeur booléenne : 0 pour indiquer False et un -1 pour indiquer True.
  [#568964]

- Toutes les applications iOS requises ne sont pas transmises à tous les utilisateurs après l'inscription de Worx Home à cause d'un délai du service APNS.
  [#569978]

- Lorsque vous fournissez un nom d'hôte pour l'interface de ligne de commande, aucune erreur n'est signalée lorsque vous entrez des caractères non valides. Le nom d'hôte ne peut pas commencer par le caractère **-** et ne peut pas contenir les caractères suivants : **$? /**

  [#570147]

- Dans la console XenMobile, lorsque vous ouvrez Paramètres > NetScaler Gateway, les instructions suivantes s'affichent : « Si vous utilisez NetScaler Gateway avec StoreFront en tant que serveur d'authentification, vous devez également activer StoreFront ». Ceci est incorrect. Vous n'avez pas besoin d'activer StoreFront.
  [#570820]

- Lorsque vous configurez une seule stratégie pour les plates-formes Android et Android for Work, la stratégie pour l'appareil Android prend également effet sur un appareil Android for Work. Pour contourner le problème, configurez une stratégie distincte pour chaque plate-forme et attribuez des utilisateurs différents pour chaque stratégie. En d'autres termes, attribuez la stratégie Android aux utilisateurs d'appareils Android et attribuez la stratégie Android for Work aux utilisateurs d'appareils Android for Work.
  [#570828]

- Dans la console XenMobile, lors de la configuration de votre connexion à ShareFile, si le mot de passe d'administrateur ShareFile contient les caractères **%** ou **^**, vous obtenez une erreur ou observez d'autres comportements erronés. Pour éviter ce problème, modifiez le mot de passe du compte d'administrateur ShareFile de façon à ce qu'il ne contienne pas les caractères **%** ou **^** .
  [#571283]

- Les utilisateurs ne peuvent pas inscrire d'appareils exécutant Android for Work avec la méthode d'inscription « Nom d'utilisateur + PIN ». Ce paramètre s'affiche dans la console XenMobile dans Configurer > Paramètres > Inscription > Nom d'utilisateur + PIN.

  [#571919]

- Lorsque vous configurez l'authentification LDAP avec sAMAccountName comme méthode de recherche d'utilisateurs, les appareils Android ne peuvent pas effectuer d'inscription en mode Android for Work. Il s'agit d'un problème de tiers.
  [#571927]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Dans les déploiements cloud, les contrôles de connectivité NetScaler Gateway de la page Support peuvent afficher l'état Fail (Échec) par erreur.
  [#573564]
- Les appareils exécutant Android M peut rencontrer des problèmes de réinscription. Il s'agit d'un problème de tiers.

  [#574746]
- Si vous utilisez le protocole SSL sur le serveur SQL Server, chargez le certificat d'autorité de certification racine de confiance depuis la console XenMobile 10.0 avant la mise à niveau. Sinon, une boucle de redémarrage se met en œuvre.

  [#574751]
- Planifiez l'arrêt des nœuds de cluster en mode de maintenance car une panne de deux minutes peut se produire.
  [#575644]
- Rejoignez de nouveaux nœuds uniquement après avoir fait apparaître le premier nœud dans le cluster.

  [#575671]
- Une erreur de profil non valide se produit lorsque vous essayez de configurer le programme Device Enrollment Program (DEP) iOS dans la console XenMobile. Il s'agit d'un problème de tiers.

  [#607143]
- 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]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Aperçu de l'architecture

Oct 11, 2016

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 Worx Home.
- 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 une application qui a été créée au sein de votre organisation ou une application mobile développée par des tiers, telle que les applications Citrix Worx. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Configuration de la mise en cluster pour XenMobile 10.

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. Pour accéder à des diagrammes d'architecture de référence, consultez les articles Reference Architecture for On-Premises Deployments et Reference Architecture for Cloud Deployments du Manuel de déploiement de XenMobile. Pour obtenir une liste complète des ports, consultez la section Exigences requises par XenMobile en matière de port.

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). 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 (voir Plates-formes prises en charge dans XenMobile). Vous déployez XenMobile en mode MAM (également appelé mode MAM exclusif) si vous prévoyez d'utiliser uniquement les fonctionnalités MAM de XenMobile sans inscrire d'appareils 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). Vous déployez XenMobile en mode ENT (enterprise) 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile dans le réseau interne

Vous pouvez déployer une architecture avec XenMobile dans le réseau interne, plutôt que dans la zone démilitarisée (DMZ), afin de répondre à une ou plusieurs des exigences suivantes :

- Vous ne disposez pas d'un hyperviseur dans la zone démilitarisée (DMZ) ou vous n'êtes pas autorisé à disposer d'un hyperviseur dans la DMZ.
- Votre DMZ peut uniquement contenir des appliances de réseau.

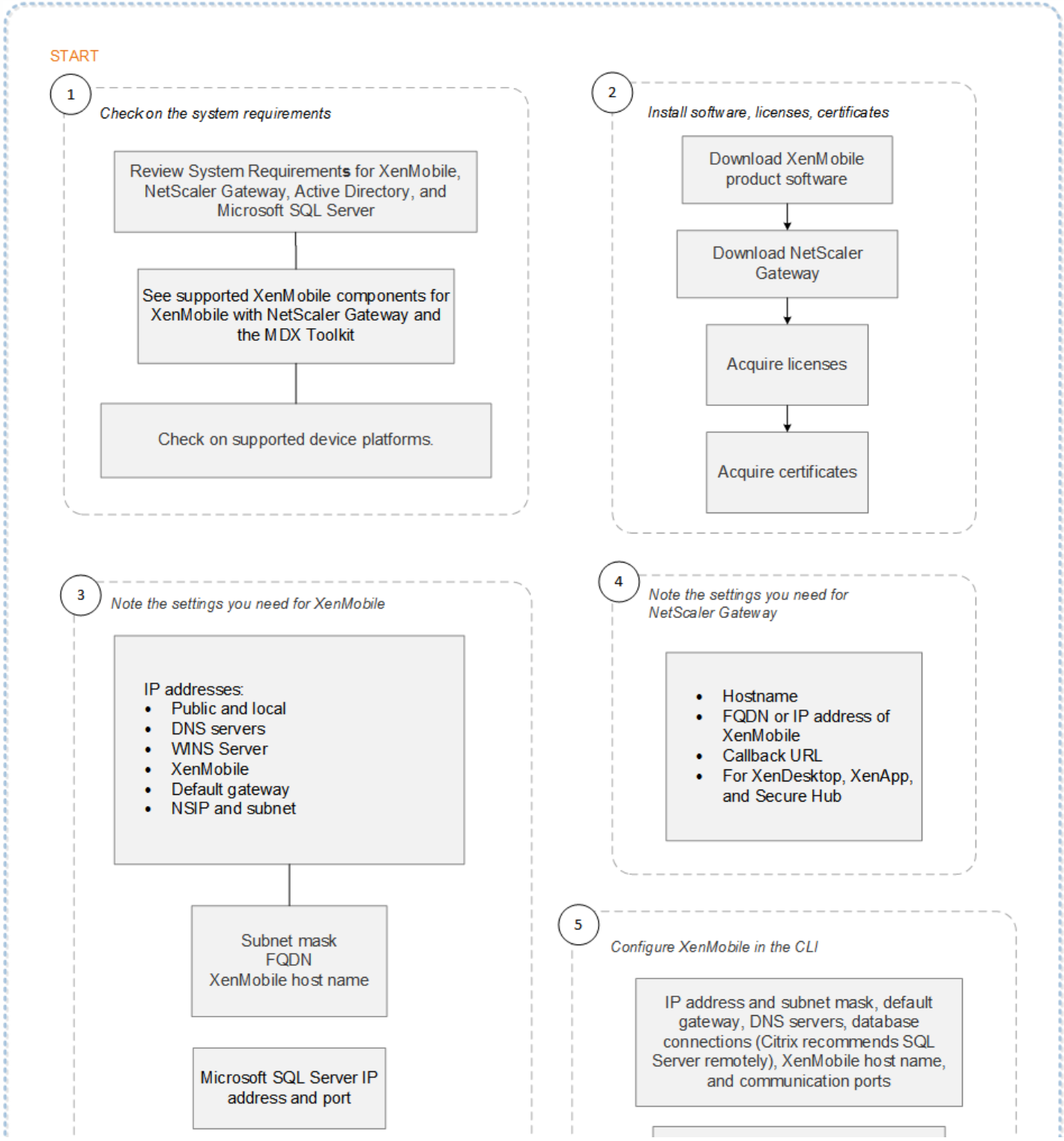
Étant donné que le serveur XenMobile n'est pas dans la DMZ, vous n'avez pas besoin d'ouvrir de ports sur le pare-feu interne pour autoriser l'accès à SQL Server et aux serveurs PKI depuis la DMZ.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

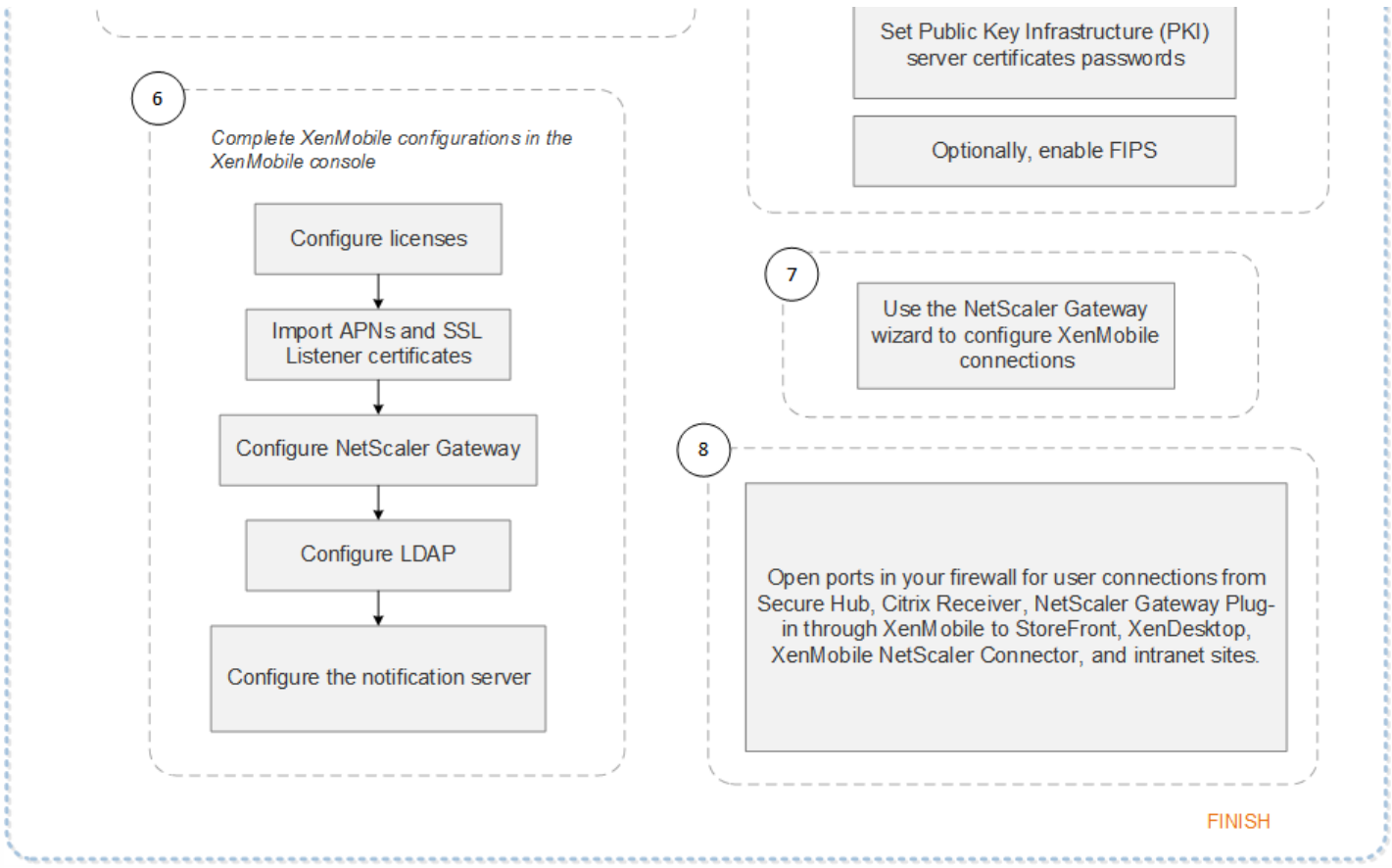
Organigramme du déploiement de XenMobile avec NetScaler Gateway

Jul 25, 2016

Vous pouvez utiliser cet organigramme pour vous guider dans les étapes principales du déploiement XenMobile 10.1 avec NetScaler Gateway. Vous trouverez des liens vers des rubriques liées à chaque étape après la figure.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



1

- Configuration système requise pour XenMobile 10.1
- Compatibilité XenMobile
- Plates-formes prises en charge dans XenMobile 10.1

2

- Installation de XenMobile
- Certificats dans XenMobile
- Licences pour XenMobile

3

- Check-list de pré-installation XenMobile

4

- Check-list de pré-installation XenMobile

5

- Configuration de XenMobile dans la fenêtre d'invite de commande

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6

- Configuration de XenMobile dans un navigateur Web

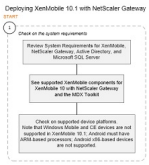
7

- Configuration des paramètres de votre environnement XenMobile

8

- Exigences requises par XenMobile en matière de port

Cliquez sur l'image miniature pour télécharger l'organigramme au format PDF.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Capacité à monter en charge de XenMobile

Jul 25, 2016

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 fournit les réponses aux questions les plus courantes quant à la configuration requise pour les déploiements à petite et grande échelle.

Les données de cet article offrent des directives permettant de déterminer les performances et la capacité à monter en charge d'une infrastructure XenMobile. Les deux facteurs clés pour déterminer la manière de configurer votre serveur et la base de données sont la capacité à monter en charge (nombre maximal d'utilisateurs/d'appareils) et le taux d'ouverture de session.

- La capacité à monter en charge est définie comme le nombre maximal d'utilisateurs exécutant simultanément une charge de travail déterminée. Pour de plus amples informations sur les flux utilisés pour charger l'infrastructure XenMobile, reportez-vous à la section Charges de travail.
- Ouverture de session est défini comme l'intégration de nouveaux utilisateurs et l'authentification des utilisateurs existants.
  - Le taux d'intégration est le nombre maximal d'appareils pouvant être inscrits dans l'environnement pour la première fois. Appelé Première utilisation ou FTU dans cet article, ce point de données est important lors de l'orchestration d'une stratégie de déploiement.
  - Le taux d'utilisateur existant est le nombre maximal d'utilisateurs authentifiés dans l'environnement et qui se sont déjà inscrits et connectés avec leur appareil. Ces tests englobent la création de sessions pour les utilisateurs déjà inscrits et l'exécution des applications WorxMail et WorxWeb.

Le tableau suivant affiche des directives relatives à la capacité à monter en charge basées sur les résultats de test pour l'environnement XenMobile correspondant.

Tableau 1. XenMobile Enterprise avec inscription

Capacité à monter en charge	Jusqu'à 100 000 appareils	
Taux d'ouverture de session	Intégration (FTU)	Jusqu'à 2 777 appareils par heure
	Utilisateurs existants	Jusqu'à 16 667 appareils par heure
Configuration	NetScaler Gateway	MPX 20500
	XenMobile Enterprise Edition	Cluster à 10 nœuds du serveur XenMobile
	Base de données	Base de données externe Microsoft SQL Server

Cette section décrit la configuration matérielle utilisée et les résultats de l'exécution des charges de travail intégrées (FTU)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

et des tests de capacité à monter en charge de la charge de travail utilisateur existante.

Le tableau suivant définit les recommandations matérielles et de configuration pour XenMobile lors de la montée en charge de 1 000 à 100 000 appareils. Ces directives sont basées sur les résultats des tests et leurs charges de travail associées. Les recommandations tiennent compte de la marge d'erreur acceptable comme défini dans les critères de sortie.

L'analyse des résultats des tests a mené à ces conclusions :

- Le taux d'ouverture de session est un facteur important pour déterminer la capacité à monter en charge d'un système. Outre l'ouverture de sessioninitiale, les taux d'ouverture de session dépendent des valeurs d'expiration de l'authentification configurées dans votre environnement. Par exemple, si vous avez défini une valeur d'expiration de l'authentification trop faible, les utilisateurs doivent exécuter des demandes de connexion plus fréquentes. Par conséquent, vous devez comprendre clairement la manière dont ces valeurs d'expiration affectent votre environnement.
- Une base de données externe (SQL Server) avec 128 Go de RAM, 300 Go d'espace disque et 24 processeurs virtuels a été utilisée pour conduire les tests et est recommandée pour les environnements de production.
- Pour atteindre une montée en charge maximale, les ressources en matière d'UC et de RAM ont été augmentées sur XenMobile.
- La configuration du cluster à 10 nœuds a été la plus grande configuration validée. La montée en charge au-delà de 10 nœuds requiert une implémentation supplémentaire de XenMobile.

Tableau 2. XenMobile Enterprise avec résultats de montée en charge d'inscription

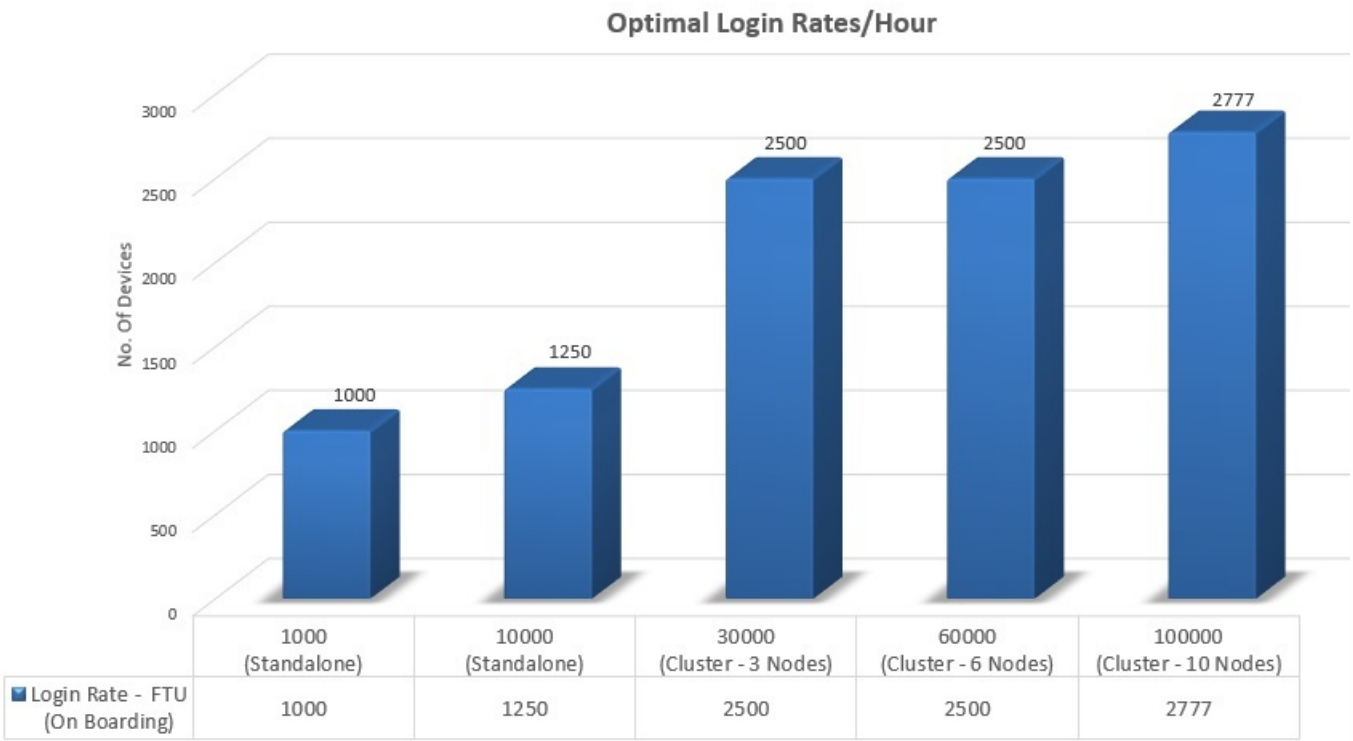
Nombre d'appareils	**1 000**	**10 000**	**30 000**	**60 000**	**100 000**
Taux d'ouverture de session					
Intégration (FTU)	125	1 250	2 500	2 500	2 777
Utilisateurs existants	1 000	2 500	7 500	15 000	16 667
Configuration					
Environnement de référence	VPX-XenMobile en mode autonome	MPX-XenMobile en mode autonome	MPX-XenMobile en cluster (3)	MPX-XenMobile en cluster (6)	MPX-XenMobile en cluster (10)
NetScaler Gateway	VPX avec 2 Go de RAM Deux processeurs virtuels	MPX-10500		MPX-20500	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile - mode	Autonome	Autonome	Cluster		
XenMobile - cluster	S.O.	S.O.	3	6	10
XenMobile - boîtier virtuel	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels			
Base de données	Externe				

Le tableau précédent présente les taux d'ouverture de session recommandés pour les nouveaux clients et les clients existants basés sur la configuration XenMobile, le boîtier NetScaler Gateway, les paramètres de cluster et la base de données. Utilisez les données de ce tableau pour planifier un calendrier d'inscriptions optimal pour les nouveaux déploiements et les taux d'utilisateurs/d'appareils déjà inscrits pour les déploiements existants. La section Configuration associe les données de performances d'inscription et d'ouverture de session aux recommandations matérielles appropriées.

Figure 1. XenMobile Enterprise avec inscription : taux d'ouverture de session par heure

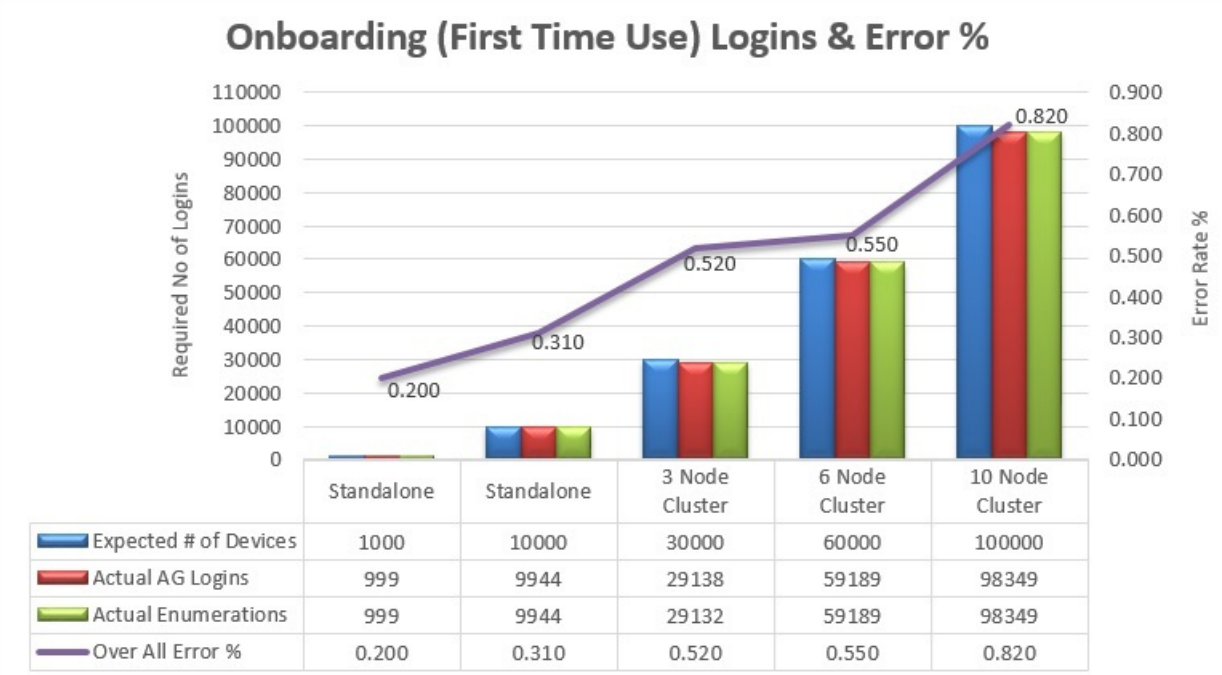


Remarque : vous allez rencontrer les situations suivantes si vous dépassez les recommandations en termes de taux ou de matériel lors du dimensionnement de votre système.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Latence d'inscription ou d'ouverture de session (durée aller-retour)
  - Latence moyenne totale : > 1,5 seconde
  - Latence moyenne pour une ouverture de session NetScaler Gateway : > 440 ms
  - Latence moyenne pour une demande Worx Store : > 3 secondes
- Une détérioration de la performance physique, telle qu'une insuffisance des ressources d'UC et de mémoire, a été observée sur les composants de l'infrastructure lorsque les limites de la montée en charge ont été atteintes.
  - Réponses non valides sur les boîtiers NetScaler Gateway et XenMobile.
  - Réponse lente de la console XenMobile.

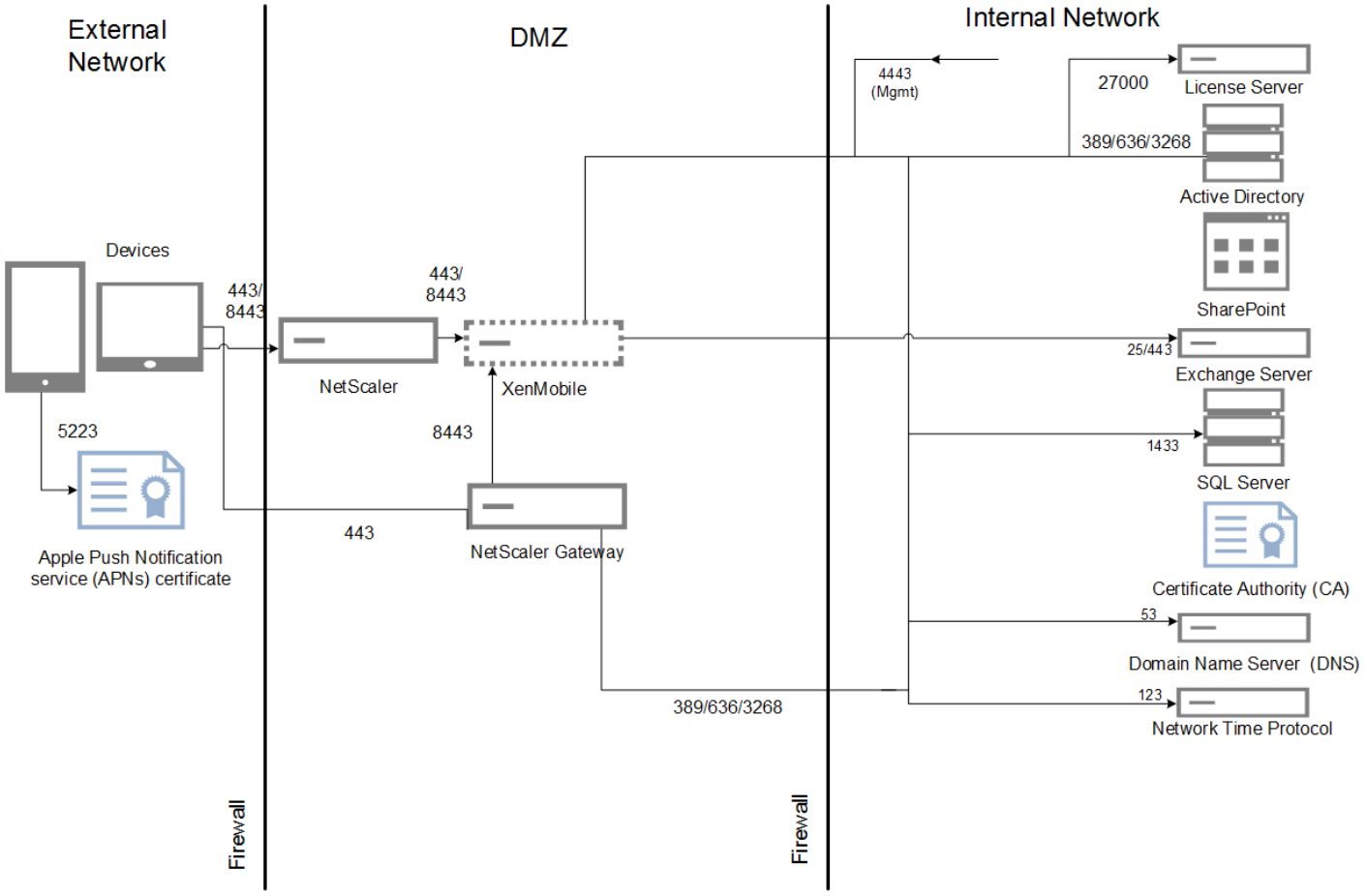
Figure 2. Ouvertures de session intégrées (FTU) et pourcentage d'erreur avec inscription



Le pourcentage d'erreur dans la figure précédente comprend l'ensemble des erreurs rencontrées relatives aux demandes correspondant à chaque opération et n'est pas limité aux ouvertures de session. Le pourcentage d'erreur se situe dans la limite autorisée pour chaque série de tests comme défini dans les critères de sortie.

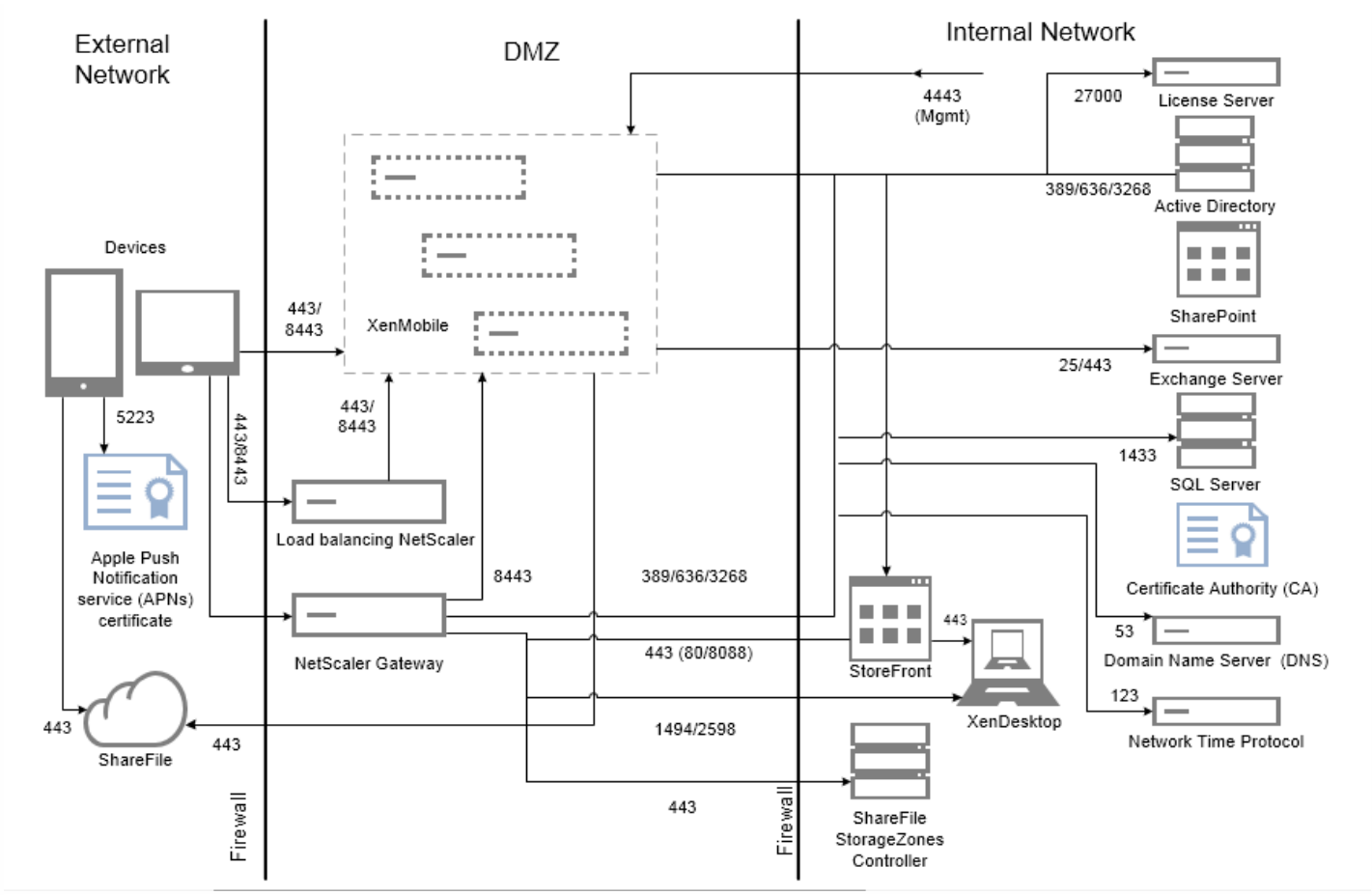
La figure suivante montre l'architecture de référence pour un déploiement à petite échelle. Il s'agit d'une architecture autonome qui prend en charge jusqu'à 10 000 appareils.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La figure suivante montre l'architecture de référence pour un déploiement d'entreprise. Il s'agit d'une architecture en cluster avec déchargement SSL pour MAM sur HTTP qui prend en charge 10 000 appareils ou plus.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les tests ont été exécutés sur XenMobile Enterprise pour établir un banc d'essai. En vue de cibler les déploiements à petite et à grande échelle, 1 000 à 100 0000 appareils ont été utilisés pour les mesures.

Des charges de travail ont été créées pour simuler des cas d'utilisation réels. Ces charges de travail ont été exécutées pour chaque test afin d'étudier les effets sur l'inscription et les taux d'ouverture de session. L'objectif de ces tests était d'obtenir un taux d'ouverture de session optimal compris dans la marge d'erreur autorisée, comme détaillé dans les critères de sortie. Les taux d'ouverture de session sont un facteur critique pour déterminer la configuration matérielle recommandée pour les composants d'infrastructure.

Les demandes d'ouverture de session des charges de travail intégrées (FTU) comprenaient les opérations de détection automatique, d'authentification et d'enregistrement des appareils. Les abonnements aux applications, ainsi que les opérations d'installation et de démarrage ont été réparties de manière uniforme au cours de la période de test, ce qui a réuni les meilleures conditions pour une simulation réelle des actions de l'utilisateur. Au terme du test, la session a été fermée. Les demandes d'ouverture de session pour la charge de travail des utilisateurs existants comprenaient uniquement des demandes d'authentification.

Les charges de travail des utilisateurs sont définies comme suit :

Tableau 3. Définitions de la charge de travail de l'utilisateur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sessions utilisateur et appareils	Inclut les ouvertures de session NetScaler Gateway, les énumérations, l'enregistrement des appareils, et ainsi de suite pour chaque session.
Worx Store démarre	Les utilisateurs lancent Worx Store à plusieurs reprises et chaque fois qu'ils s'abonnent à une ou à plusieurs applications, ou qu'ils les installent, qu'il s'agisse d'applications mobiles (Web/SaaS/MDX) ou Windows (HDX).
Authentification unique des applications Web ou SaaS par appareil	Permet de lancer une séquence d'applications Web/SaaS jusqu'à ce que XenMobile exécute l'authentification unique et renvoie l'URL de l'application réelle. Le trafic n'a pas été envoyé aux applications réelles.
Téléchargements d'applications MDX par appareil	Compte le nombre de téléchargements d'applications MDX (peut se produire sur les lancements Worx Store). Pour iOS, cela comprend également l'automatisation de l'installation d'applications depuis Apple ITMS, qui utilise les nouvelles API du service de jeton/tms sur NetScaler Gateway.

Notes et hypothèses

Afin d'étendre les capacités de XenMobile au-delà de 30 000 appareils, vous devez régler les paramètres de serveur suivants :

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

-

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

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

Vous devez effectuer ces modifications sur tous les nœuds XenMobile, puis redémarrer le serveur.

Les scénarios suivants ne sont pas couverts dans le cadre des tests de capacité à monter en charge. Ces scénarios seront pris en compte pour l'amélioration des tests :

- La transmission de stratégies aux appareils n'est pas testée.
- Les appareils connectés Android ne sont pas testés.
- Le déploiement de paquetage n'est pas testé.
- La plate-forme Windows n'est pas testée.

Chaque XenMobile prend en charge un maximum de 10 000 connexions simultanées.

Les tests ont été exécutés dans des conditions idéales sur un réseau local pour ignorer les problèmes de latence réseau. Dans un environnement réel, la capacité à monter en charge dépend également de la bande passante disponible, plus particulièrement pour les téléchargements d'applications.

Charge de travail intégrée (FTU)

La charge de travail intégrée (FTU) est définie comme la première fois qu'un utilisateur accède à l'environnement XenMobile. Les opérations comprises dans cette charge de travail étaient les suivantes :

- Découverte automatique

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Inscription
- Authentification
- Enregistrement de l'appareil
- Mise à disposition d'applications (Web, SaaS et mobiles MDX)
  - Abonnement aux applications (y compris les téléchargements d'images et d'icônes)
  - Installation des applications MDX souscrites
- Lancement des applications (Web, SaaS et mobiles MDX)
- Nombre minimal de connexions WorxMail et WorxWeb (tunnels VPN) : deux connexions
- Installation des applications requises via XenMobile

Paramètres de charge de travail inclus :
- 1 enregistrement d'appareil par appareil
- 1 énumération par appareil
- 14 applications énumérées par appareil
- 4 lancements de Worx Store par appareil
- 4 authentifications uniques d'applications Web/SaaS par appareil
- 1 application MDX téléchargée par appareil
- 2 téléchargements d'applications requises

Charge de travail des utilisateurs existants
Le tableau suivant présente la charge de travail des utilisateurs existants. Cette charge de travail simulait un utilisateur utilisant les applications WorxMail et WorxWeb. Cette simulation a été utilisée pour mesurer la capacité à monter en charge du port NetScaler Gateway dans la configuration XenMobile. Pour l'application WorxWeb, les utilisateurs avaient accès aux sites Web internes, ce qui ne déclenche pas l'authentification unique XenMobile. Les opérations dans ce mode étaient les suivantes :
- Authentification (NetScaler Gateway et XenMobile)
- Nombre de connexions WorxMail et WorxWeb (tunnels VPN) : quatre connexions

Profils de connexion WorxApps
Le tableau suivant présente les paramètres de charge de travail pour les utilisateurs existants.

Tableau 4. Profils de connexion WorxApps

Connexion d'appareils	Type de connexion	Données envoyées par session[1]	Données reçues par session[1]
Connexion WorxMail n° 1	Type 1[2]	4,1 Mo	4,1 Mo
Connexion WorxMail n° 2	Type 1	6,3 Mo	12,5 Mo
Connexion WorxWeb n° 1	Type 2[3]	5,2 Mo	15,7 Mo
Connexion WorxWeb n° 2	Type 2	4,1 Mo	3,4 Mo
Nombre total d'octets transférés par session[1]		~ 19,7 Mo	~ 40,7 Mo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. **Par session** : 8 heures.

2. **Type 1** : envoi et réception asymétriques avec des connexions à long terme (WorxMail avec une connexion à une boîte aux lettres Microsoft Exchange dédiée).

3. **Type 2** : envoi et réception asymétriques avec des connexions qui se ferment et s'ouvrent de nouveau après un certain délai (connexions WorxWeb).

Remarque : les modifications apportées aux détails de connexion affectent les résultats de l'analyse. Par exemple, si le nombre de connexions par utilisateur est augmenté, le nombre de sessions de NetScaler Gateway prises en charge peut être réduit.

Profils WorxMail et WorxWeb

Les tableaux suivants présentent les détails des profils WorxMail et WorxWeb.

Tableau 5. Profil WorxMail pour une charge de travail moyenne

Messages envoyés par jour	20
Messages reçus par jour	80
Messages lus par jour	80
Messages supprimés par jour	20
Taille moyenne des messages (Ko)	200

Tableau 6. Profil WorxWeb pour charge de travail moyenne

Nombre d'applications Web lancées	10
Nombre de pages Web ouvertes manuellement	10
Nombre moyen de paires demande–réponse par application Web	100
Taille moyenne de la demande (octets)	300
Taille moyenne de la réponse (octets)	1000

Configuration et paramètres

Les configurations suivantes ont été utilisées lors de l'exécution des tests de capacité à monter en charge :

- Les serveurs virtuels de NetScaler Gateway et d'équilibrage de charge coexistaient sur le même boîtier NetScaler Gateway.
- Une clé de 2 048 bits a été utilisée sur NetScaler Gateway pour les transactions SSL.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les taux d'ouverture de session constituent la base de cette analyse. Ils servent de ligne directive pour les composants d'infrastructure et leur configuration respective. Il est important de noter que les taux d'ouverture de session prennent en compte une marge d'erreur qui se compose des éléments suivants :

- Réponses non valides
  - Une réponse avec le code d'état 401/404 à la place de 200 est considérée comme non valide.
- Délais d'expiration des demandes
  - Une réponse est attendue dans les 120 secondes.
- Erreurs de connexion
  - Une réinitialisation de la connexion s'est produite.
  - Un arrêt brutal de connexion s'est produit.

Le taux d'ouverture de session est acceptable si le taux d'erreur global est inférieur à 1 % du nombre total de demandes envoyées à partir d'un appareil donné. Le taux d'erreur inclut les erreurs correspondant à chaque opération de charge de travail individuelle, ainsi que la performance physique du composant d'infrastructure, comme l'insuffisance des ressources d'UC et de mémoire.

Le tableau suivant dresse la liste des logiciels d'infrastructure XenMobile utilisés pour ces tests.

Tableau 8. Composants d'infrastructure XenMobile

Composant	Version
NetScaler Gateway	10.5-57.4.nc
XenMobile	10.1.0.63030
Base de données externe	MS SQL Server 2014 R2 (128 Go de RAM, 300 Go d'espace disque, 24 processeurs virtuels)

Les tests de capacité à monter en charge ont été exécutés sur une plate-forme XenServer comme décrit dans le tableau suivant.

Tableau 9. Matériel XenServer

Fournisseur	Genuine Intel
Modèle	UC Intel Xeon — E5645 @ 2,40 GHz (nombre d'UC = 24)

Cela comprend les services de base d'infrastructure (par exemple, Active Directory, Windows Domain Name Service (DNS), autorité de certification, Microsoft Exchange, etc.), ainsi que les composants XenMobile (boîtier virtuel XenMobile et boîtier virtuel NetScaler Gateway VPX, le cas échéant).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour obtenir des informations ou poser des questions techniques concernant cet article ou les produits mentionnés ici, visitez le site Citrix.com, effectuez une recherche sur le site de la documentation XenMobile pour consulter la documentation produit la plus récente, ou contactez votre représentant Citrix local.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À propos de XenMobile Cloud

Oct 11, 2016

XenMobile Cloud est un service qui offre un environnement de gestion de la mobilité d'entreprise (EMM) XenMobile permettant de gérer les applications et les appareils, ainsi que les utilisateurs ou les groupes d'utilisateurs. Avec XenMobile Cloud, Citrix gère la configuration et la maintenance de l'infrastructure sur site via le groupe Citrix Cloud Operations. La séparation vous permet de vous concentrer uniquement sur l'expérience utilisateur et sur la gestion des appareils, des stratégies et des applications. XenMobile Cloud remplace également le besoin d'acheter et de gérer des licences avec des frais d'abonnement.

Les administrateurs de Cloud Operations peuvent gérer la maintenance et la configuration de la connectivité réseau, ainsi que l'intégration de produits Citrix tels que NetScaler, XenApp, XenDesktop, StoreFront et ShareFile. L'environnement de cloud est hébergé dans des centres de données Amazon situés dans le monde entier pour assurer des performances élevées, une réponse et une assistance rapides.

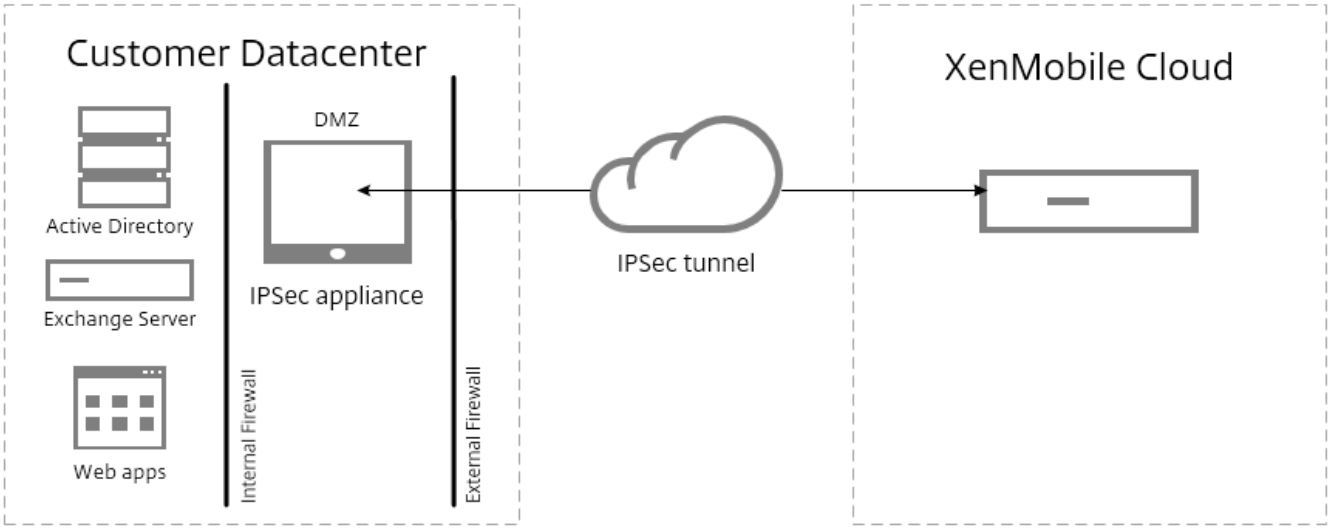
Pour commencer à utiliser XenMobile Cloud, accédez à https://www.citrix.com/products/xenmobile/tech-info/cloud.html

Remarque

- Le client d'assistance à distance n'est pas disponible dans XenMobile Cloud versions 10.x pour Windows CE et pour appareils Samsung Android.
- Les composants côté serveur de XenMobile Cloud ne sont pas conformes à la norme FIPS 140-2.
- Citrix ne prend pas en charge l'intégration de syslog dans XenMobile Cloud avec un serveur syslog sur site. 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.

L'architecture de base de XenMobile Cloud est illustrée dans la figure suivante : Pour accéder à des diagrammes d'architecture de référence détaillés, consultez la section « Reference Architecture for Cloud Deployments » du Manuel de déploiement de XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Vous pouvez intégrer l'architecture XenMobile Cloud au sein de votre infrastructure en installant et en déployant Citrix CloudBridge ou à l'aide d'une passerelle IPsec existante dans votre centre de données.

Cette architecture vous permet de bénéficier de l'utilisation de NetScaler dans le cloud, géré par le groupe Cloud Operations, ou dans votre centre de données. Lorsqu'il est utilisé dans le centre de données, NetScaler vous offre un point de gestion unique pour contrôler l'accès et limiter les actions au cours des sessions en fonction de l'identité de l'utilisateur et du périphérique de point de terminaison. Ce déploiement améliore la sécurité des applications, la protection des données et la gestion de la conformité.

Pour télécharger et installer Citrix CloudBridge, accédez à https://www.citrix.com/downloads/cloudbridge.html

Rôles dans XenMobile Cloud

XenMobile Cloud utilise le même contrôle d'accès basé sur un rôle (RBAC) qu'un déploiement de XenMobile. La différence avec XenMobile Cloud est que le groupe Citrix Cloud Operations gère tout rôle, y compris le provisioning, lié à l'infrastructure.

La figure suivante illustre la console RBAC pour XenMobile Cloud.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile implémente quatre rôles utilisateur par défaut de façon à séparer logiquement l'accès aux fonctions système. Les rôles par défaut sont les suivants :

- **Administrateur**. Accorde un accès complet au système.
- **Assistance**. Accorde l'accès à l'assistance à distance.
- **Utilisateur**. Accorde aux utilisateurs l'accès à l'inscription d'appareils et à l'utilisation du portail en libre-service.
- **Provisioning**. Accorde aux administrateurs la capacité de provisionner tous les appareils Windows Mobile/CE en tant que groupe à l'aide de l'outil de provisioning d'appareil. Ce rôle est géré par le groupe Cloud Operations.

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.

Vous pouvez attribuer des rôles à des utilisateurs (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.

Vous pouvez attribuer les rôles suivants. Le groupe Citrix Cloud Operations gère tout rôle qui ne se trouve pas sur cette liste.

Section principale	Section	Page	Page visible pour
Tableau de bord	ALL	ALL	Administrateur informatique
Gérer	Appareils	ALL	Administrateur informatique
Gérer	Inscription	ALL	Administrateur informatique
Configurer	Stratégies applicatives	ALL	Administrateur informatique
Configurer	Applications	ALL	Administrateur informatique
Configurer	Actions	ALL	Administrateur informatique
Configurer	Groupes de mise à disposition	ALL	Administrateur informatique

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer	Settings	Certificats	Administrateur cloud et administrateur informatique
Configurer	Settings	Modèles de notification	Administrateur informatique
Configurer	Settings	Contrôle d'accès basé sur un rôle	Administrateur cloud et administrateur informatique
Configurer	Settings	Inscription	Administrateur informatique
Configurer	Settings	Utilisateurs et groupes locaux	Administrateur cloud et administrateur informatique
Configurer	Settings	Gestion des versions	Administrateur cloud et administrateur informatique
Configurer	Settings	Workflows	Administrateur informatique
Configurer	Settings	Fournisseurs d'informations d'identification	Administrateur informatique
Configurer	Settings	Entités PKI	Administrateur informatique
Configurer	Settings	Propriétés de client	Administrateur informatique
Configurer	Settings	NetScaler Gateway	Administrateur cloud uniquement Ou administrateur informatique uniquement
Configurer	Settings	Passerelle SMS opérateur	Administrateur informatique
Configurer	Settings	Serveur de notification	Administrateur cloud et administrateur informatique
Configurer	Settings	ActiveSync Gateway	Administrateur informatique
Configurer	Settings	VPP iOS	Administrateur informatique
Support	Opérations de journal	Paramètres du journal	Administrateur cloud et administrateur informatique et support technique

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer	Settings	Propriétés du serveur	Administrateur cloud et administrateur informatique et support technique
Configurer	Settings	Informations d'identification Google Play	Administrateur informatique
Configurer	Settings	LDAP	Administrateur informatique
Configurer	Settings	Contrôle d'accès réseau	Administrateur informatique
Support	Pack de support	Créer des packs d'assistance	Administrateur cloud et support technique
Configurer	Settings	iOS Device Enrollment Program	Administrateur informatique
Configurer	Settings	Fournisseur de services mobiles	Administrateur informatique
Configurer	Settings	Samsung KNOX	Administrateur informatique
Configurer	Settings	XenApp/ XenDesktop	Administrateur informatique
Configurer	Settings	ShareFile	Administrateur informatique
Support	Advanced	Informations de cluster	Administrateur cloud et support technique
Support	Advanced	Nettoyage de la mémoire	Administrateur cloud et support technique
Support	Advanced	Propriétés de la mémoire Java	Administrateur cloud et support technique
Support	Advanced	Macros	Administrateur informatique
Assistant FTU	Configuration initiale	NetScaler Gateway	Administrateur cloud uniquement Ou administrateur informatique uniquement
Configurer	Settings	Assistance Worx Home	Administrateur informatique

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer	Settings	Personnalisation Worx Store	Administrateur informatique
Support	Diagnostics	Contrôles de connectivité dans NetScaler Gateway	Administrateur cloud et administrateur informatique et support technique
Support	Diagnostics	Contrôles de connectivité dans XenMobile	Administrateur cloud et administrateur informatique et support technique
Support	Opérations de journal	Journaux	Administrateur cloud et administrateur informatique et support technique
Support	Advanced	Configuration du PKI	Administrateur cloud et administrateur informatique
Support	Outils	Utilitaire de signature APNS	Support technique
Support	Outils	Citrix Insight Services	Administrateur cloud et administrateur informatique et support technique
Assistant FTU	Configuration initiale	Certificat SSL	Administrateur cloud et administrateur informatique
Assistant FTU	Configuration initiale	Configuration du LDAP	Administrateur informatique
Assistant FTU	Configuration initiale	Serveur de notification	Administrateur cloud et administrateur informatique
Assistant FTU	Configuration initiale	Récapitulatif	Administrateur cloud et administrateur informatique
Support	Liens	Centre de connaissances de Citrix	Administrateur cloud et administrateur informatique et support technique
Support	Outils	État NetScaler Connector de l'appareil	Administrateur informatique

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Support	Opérations de journal	Paramètres de journal->Taille du journal	Administrateur cloud et support technique

Pour obtenir des instructions détaillées sur la personnalisation des rôles, veuillez consulter la section Configuration de rôles avec RBAC.

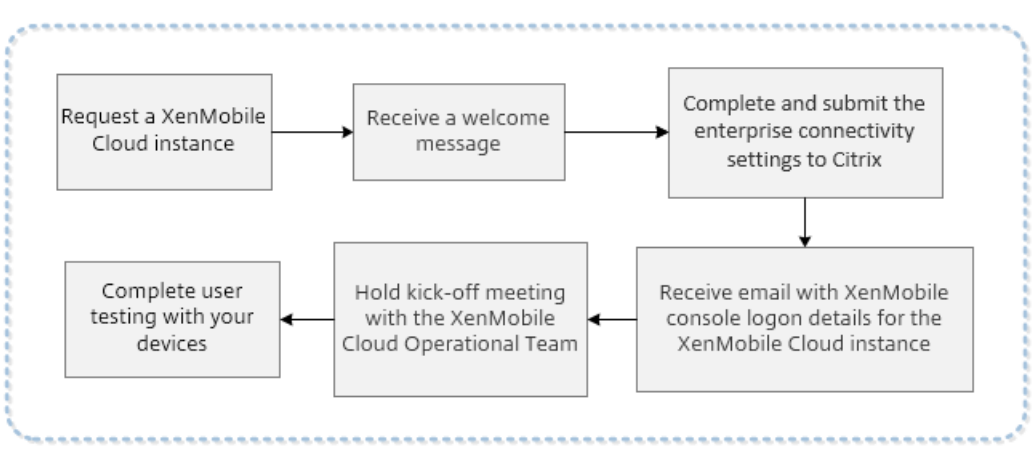
Pour demander un redémarrage des nœuds du serveur, contactez le support technique à l'adresse https://www.citrix.com/contact/technical-support.html

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Administration et conditions requises par XenMobile Cloud

Jul 25, 2016

Les étapes qui composent le processus d'intégration à partir du moment où vous demandez une instance de XenMobile Cloud jusqu'aux tests utilisateur avec les appareils dans votre organisation sont illustrées dans la figure suivante. Lors de l'évaluation ou de l'achat de XenMobile Cloud, l'équipe XenMobile Cloud Operational offre un soutien constant tant au niveau de l'intégration que de la communication afin de s'assurer que les services XenMobile Cloud essentiels sont opérationnels et configurés correctement.



Citrix héberge et met à disposition votre solution XenMobile Cloud. Certaines exigences en matière de port et de communication, cependant, sont requises pour se connecter à l'infrastructure XenMobile Cloud pour les services d'entreprise, tels que Active Directory. Consultez les sections suivantes pour préparer votre déploiement XenMobile Cloud.

Passerelles de tunnel IPSec XenMobile Cloud

Vous pouvez utiliser un connecteur d'entreprise XenMobile, un tunnel IPsec pour connecter l'infrastructure XenMobile Cloud avec les services d'entreprise, tels que Active Directory.

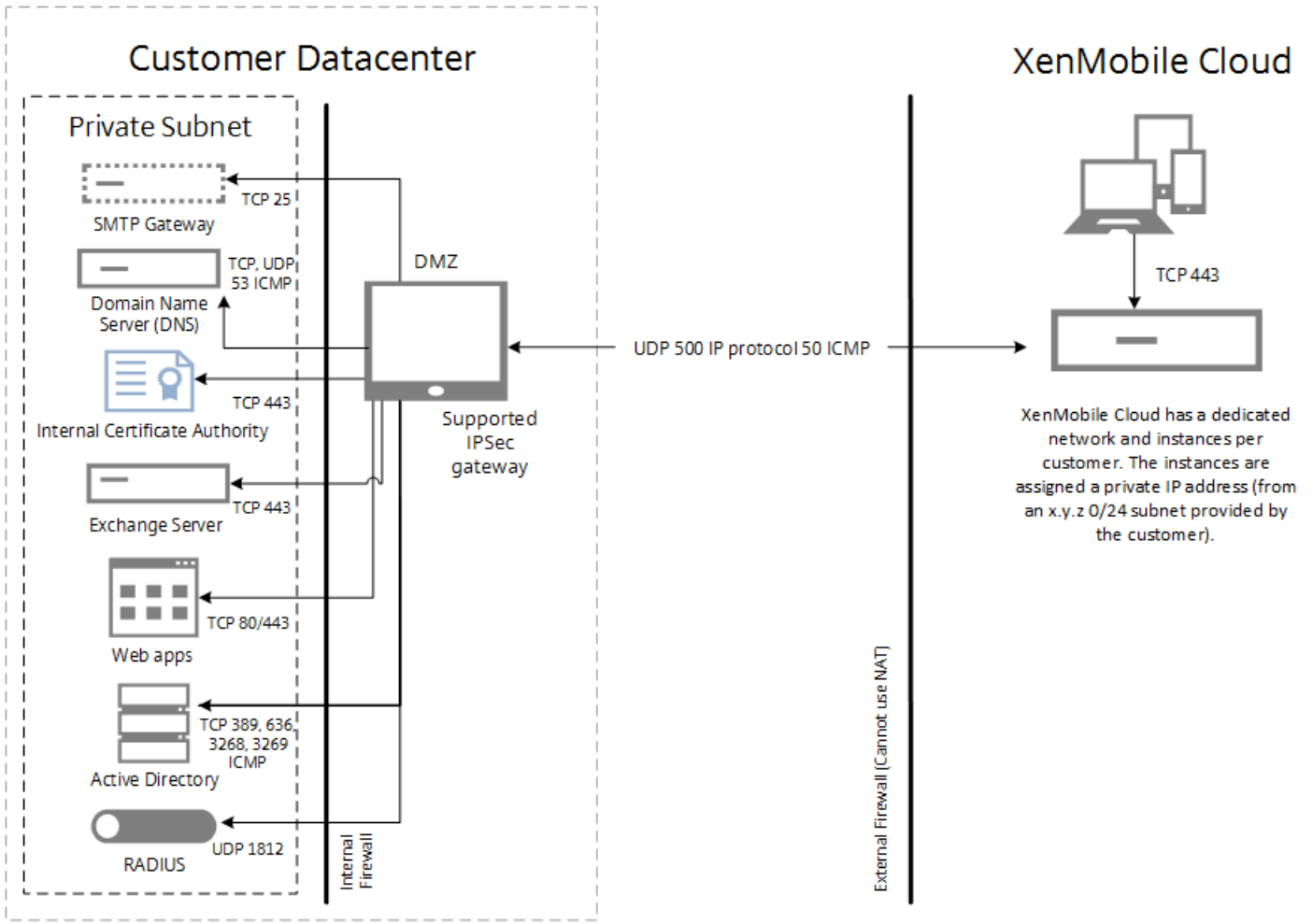
Les passerelles IPsec répertoriées dans le site Web Amazon Web Services suivant ont été officiellement testées et sont prises en charge avec la solution XenMobile Cloud : http://aws.amazon.com/vpc/faqs/. Accédez à « Q : Quels sont les périphériques de passerelle client dont la compatibilité avec Amazon VPC a été vérifiée ? » pour trouver la liste des passerelles prises en charge.

> ## Remarque
>
> Si votre passerelle IPSec ne figure pas dans la liste, il est possible qu'elle fonctionne avec XenMobile Cloud, mais elle prendra plus de temps à configurer, et vous devrez peut-être utiliser l'une des passerelles IPSec officiellement prises en charge comme solution de secours.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Votre passerelle IPSec doit disposer d'une adresse IP publique qui lui a été attribuée directement et l'adresse ne peut pas utiliser la traduction d'adresse réseau (NAT).

La figure suivante montre comment le tunnel IPsec est configuré dans la solution XenMobile Cloud pour se connecter aux services de votre entreprise via plusieurs ports.



Le tableau suivant présente les exigences en matière de port et de communication pour un déploiement XenMobile Cloud, y compris les exigences du tunnel IPSec.

Source	Destination	Protocoles	Port	Description
Pare-feu externe (edge) : règles de trafic entrant				
Adresses IP publiques de XenMobile Cloud (AWS) IPCSEC VPN [1]	Appliance IPSec client	UPD	500	Configuration IPSec IKE.
Adresses IP publiques de XenMobile Cloud	Appliance IPSec client	ID du protocole IP	50	Protocole ESP IPSec.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

(AWS) IPCSEC VPN [1]				
Adresses IP publiques de XenMobile Cloud (AWS) IPCSEC VPN [1]	Appliance IPSec client	ICMP		Pour la résolution des problèmes (peut être supprimé après la configuration).
Pare-feu externe (edge) : règles de trafic sortant				
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [1]	UDP	500	Configuration IPSec IKE.
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [1]	ID du protocole IP	50, 51	Protocole ESP IPSec.
Sous-réseau de la zone démilitarisée (DMZ) cliente	Adresses IP publiques de XenMobile Cloud (AWS) IPSec VPN [2]	ICMP		Pour la résolution des problèmes (peut être supprimé après la configuration).
Pare-feu internet : règles de trafic entrant				
Sous-réseau client /24 inutilisé et routable [2]	Serveurs DNS internes dans le data center client	TCP, UPP, ICMP	53	Résolution DNS.
Sous-réseau client /24 inutilisé et routable [2]	Contrôleurs de domaine Active Directory dans le data center client	LDAP (TCP)	389, 636 3268, 3269	Pour l'authentification de l'utilisateur Active Directory et les requêtes d'annuaire aux contrôleurs de domaine.
Sous-réseau client /24 inutilisé et routable [2]	Contrôleurs de domaine Active Directory dans le data center client	ICMP		Pour la résolution des problèmes (peut être supprimé une fois l'installation complète terminée).
Sous-réseau client /24 inutilisé et routable [2]	Serveurs Exchange dans le data center client	SMTP (TCP)	25	Facultatif : pour les notifications par e-mail XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sous-réseau client /24 inutilisé et routable [2]	Serveurs Exchange dans le data center client	HTTP, HTTPS (TCP)	80, 443	Exchange ActiveSync, qui est nécessaire si le trafic ActiveSync est envoyé depuis l'appareil vers l'infrastructure XenMobile Cloud (via le tunnel IPSec) aux serveurs Exchange. Ceci n'est PAS nécessaire si l'appareil utilisateur communique avec un nom de domaine complet ActiveSync public via Internet et qu'il n'utilise pas le tunnel IPSec XenMobile pour accéder aux serveurs Exchange.
Sous-réseau client /24 inutilisé et routable [2]	Serveurs d'application, tels que des serveurs intranet/Web, des serveurs SharePoint, et ainsi de suite.	HTTP, HTTPS (TCP)	80, 443	Accès aux serveurs intranet et/ou d'application à partir d'appareils mobiles via le tunnel IPSec XenMobile. Chaque serveur d'application doit être ajouté aux règles de pare-feu avec le numéro de port nécessaire pour accéder à l'application (généralement le port 80 et/ou 443).
Sous-réseau client /24 inutilisé et routable [2]	Serveur PKI (si une PKI sur site est utilisée)	HTTPS (TCP)	443	Facultatif (non utilisé pour les POC XenMobile) : Cela peut être utilisé pour établir une intégration entre l'infrastructure de XenMobile Cloud et une infrastructure PKI sur site (telle qu'une autorité de certification Microsoft) pour établir une authentification par certificat au sein de la solution XenMobile.
Sous-réseau client /24 inutilisé et routable [2]	Serveur RADIUS	UDP	1812	Facultatif (non utilisé pour les POC XenMobile) : Cela peut être utilisé pour établir une authentification à deux facteurs dans la solution XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pare-feu internet : règles de trafic sortant				
Sous-réseaux clients internes, à partir desquels la console XenMobile doit être disponible	Sous-réseau client /24 inutilisé et routable [2]	TCP	4443	Console XenMobile App Controller (MAM) dans l'infrastructure de XenMobile Cloud.

[1] Sera fourni par l'équipe de XenMobile Cloud lorsque l'instance de XenMobile Cloud et les composants IPSec sont provisionnés dans l'infrastructure de XenMobile Cloud.

[2] Sous-réseau /24 inutilisé fourni par le client dans le cadre du processus de provisioning, qui n'entre pas en conflit avec les sous-réseaux internes du data center du client ; il est routable.

Si vous prévoyez de déployer XenMobile Mail Manager ou XenMobile NetScaler Connector pour filtrer la messagerie native, par exemple pour bloquer ou autoriser la connectivité à la messagerie à partir de clients de messagerie natifs sur les appareils mobiles des utilisateurs, veuillez consulter les exigences supplémentaires suivantes.

Certificat APNs Apple XenMobile

Si vous envisagez de gérer des appareils iOS avec votre déploiement XenMobile Cloud, vous avez besoin d'un certificat APNS d'Apple. Vous devez préparer le certificat avant de déployer la solution XenMobile Cloud. Pour obtenir des instructions détaillées, consultez la section Faire une demande de certificat APNs.

Certificat de notification push WorxMail pour iOS

Si vous souhaitez utiliser la notification push pour votre déploiement WorxMail, vous devez préparer un certificat APNS Apple pour la notification push iOS WorxMail. Pour de plus amples informations, veuillez consulter la section Notifications push pour WorxMail pour iOS.

MDX Toolkit XenMobile

Le MDX Toolkit est une technologie de wrapping d'application qui prépare les applications en vue de les déployer en toute sécurité avec XenMobile. Si vous voulez wrapper des applications, telles que Citrix WorxMail, WorxMail, WorxNotes, QuickEdit, etc., vous devez installer le MDX Toolkit. Pour de plus amples informations, consultez la section À propos du MDX Toolkit.

Si vous envisagez de wrapper des applications iOS, vous devez disposer d'un compte Apple Developer pour créer les profils de distribution Apple nécessaires. Pour de plus amples informations, consultez la section Configuration système requise par le MDX Toolkit et le site Web Apple Developer.

Si vous envisagez de wrapper des applications pour des appareils Windows Phone 8.1, consultez la section Configuration système requise.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Découverte automatique XenMobile pour l'inscription d'appareils Windows Phone

Si vous souhaitez utiliser le service de découverte automatique de XenMobile pour votre Windows Phone 8.1, assurez-vous que vous disposez d'un certificat SSL public. Pour de plus amples informations, consultez la section Pour activer la découverte automatique pour l'inscription utilisateur dans XenMobile.

Console XenMobile

La solution XenMobile Cloud utilise la même console Web qu'un déploiement XenMobile sur site. L'administration quotidienne de votre solution Cloud, telle que la gestion des stratégies, la gestion des applications, la gestion des appareils, etc., est donc similaire à l'administration d'un déploiement XenMobile sur site. Pour de plus amples informations sur la gestion des applications et des appareils dans la console XenMobile, consultez la section Prise en main de la console XenMobile.

Inscription d'appareils XenMobile

Pour de plus amples informations sur les options d'inscription de XenMobile pour les différentes plates-formes, consultez la section Inscription d'utilisateurs et d'appareils.

Prise en charge de XenMobile

Pour de plus amples informations sur la manière d'accéder à des informations et outils de support dans la console XenMobile, consultez la section Support et maintenance de XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Prise en charge des plates-formes dans XenMobile Cloud

Jul 25, 2016

Après avoir demandé une instance de XenMobile Cloud, vous pouvez, si vous le souhaitez, commencer la préparation de la prise en charge des plates-formes Android, iOS et Windows. À mesure que vous effectuez les étapes qui s'appliquent à votre environnement, conservez les informations à portée de façon à pouvoir les utiliser lors de la configuration des paramètres dans la console XenMobile.

Notez que ces exigences sont un sous-ensemble des exigences en matière de port et de communication que constitue le processus d'intégration de XenMobile Cloud. Pour de plus amples informations, consultez la section Administration et conditions requises par XenMobile Cloud.

- 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 Gestion des appareils avec Android for Work dans XenMobile.
- 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 Google for Work Android.

- 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). Pour de plus amples informations, consultez le portail Apple Push Certificates Portal.
- Créer un jeton d'entreprise VPP (Volume Purchase Program). Pour de plus amples informations, consultez la section Programme d'achat en volume d'Apple.

- 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.
- Créer un jeton d'inscription d'application (AET). Pour de plus amples informations, consultez la section Microsoft Windows Dev Center.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration système requise

Jul 25, 2016

Pour exécuter XenMobile 10.1, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.5.x, 6.2.x, 6.1.x ou 6.0.x) ; pour de plus amples informations, voir XenServer
  - VMWare (versions prises en charge : ESXi 4.1, ESXi 5.1 ou ESXi 5.5) ; 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
- Deux processeurs virtuels
- 4 Go de RAM
- 50 Go d'espace disque

La configuration recommandée pour 10 000 périphériques est la suivante :

- Processeur quadruple cœur
- 16 Go de RAM

Pour exécuter NetScaler Gateway avec XenMobile 10.1, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.2.x, 6.1.x ou 6.0.x)
  - VMWare (versions prises en charge : ESXi 4.1, ESXi 5.1 ou ESXi 5.5)
  - 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.

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

  XenMobile 10.1 prend en charge les groupes de disponibilité AlwaysOn SQL Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**) :
Server Configuration - Service Accounts

Configure Windows Service Accounts and Permissions

Server-Level Roles

- 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 9.3.11 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

XenMobile prend en charge les serveurs de messagerie suivants :

- Exchange 2013
- Exchange 2010

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Compatibilité XenMobile

Jul 25, 2016

Pour un résumé des composants XenMobile que vous pouvez intégrer, consultez la section Compatibilité XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Plates-formes prises en charge

Jul 25, 2016

Vous pouvez trouver la liste complète des appareils pris en charge par XenMobile 10.x pour la gestion de la mobilité d'entreprise dans la section Plates-formes prises en charge dans XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration requise pour les ports

Oct 11, 2016

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.

Vous devez ouvrir les ports suivants pour autoriser les connexions utilisateur à partir de Worx Home, 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 de NetScaler Gateway. Pour plus d'informations sur les adresses IP appartenant à NetScaler, telles que l'adresse IP NetScaler (NSIP), l'adresse IP du serveur virtuel (VIP) et l'adresse IP du sous-réseau (SNIP), consultez la section How a NetScaler Communicates with Clients and Servers dans la documentation de 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	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 vous recommande d'utiliser le port 443.	Trafic réseau XML de StoreFront et l'Interface Web STA NetScaler Gateway	XenDesktop ou XenApp
123	Utilisé pour les services NTP (Network Time Protocol).	NetScaler Gateway	Serveur NTP
389	Utilisé pour les connexions LDAP non sécurisées.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Microsoft Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 l'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	NetScaler Gateway	XenApp ou XenDesktop

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	fiabilité de session. Citrix recommande de conserver ce port ouvert.		
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 télécharger les journaux et les packs d'assistance pour tous les nœuds du cluster XenMobile à partir d'un 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 ou Windows Phone Store. Utilisé pour la publication d'applications à partir des magasins d'application via Citrix Mobile Self-Serve sur iOS, Worx Home pour Android, ou Worx Home 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)
	Utilisé pour les connexions sortantes entre XenMobile et Nexmo SMS Notification Relay.		Serveur Nexmo SMS Relay
443	Utilisé pour les connexions sortantes vers le serveur de découverte automatique.	XenMobile	https://discovery.mdm.zenprise.com
	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	
	Utilisé pour l'inscription et l'installation de l'agent pour Android et Windows Mobile.	Internet	XenMobile
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.		
		Appareils	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5223	Utilisé pour les connexions sortantes APNS à partir d'appareils iOS sur les réseaux Wi-Fi sur *.push.apple.com.	iOS sur les réseaux WiFi	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
8443	Utilisé pour l'inscription d'appareils iOS et Windows Phone.	Internet Réseau local et Wi-Fi	XenMobile

La configuration de ce port permet de s'assurer que les appareils Android qui se connectent à partir de Worx Home pour Android, versions 10.2 et 10.3, peuvent accéder au service de découverte 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 Worx Home dispose des dernières informations de sécurité pour l'environnement dans lequel l'appareil s'inscrit. Worx Home 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 Worx Home 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
	54.225.219.53
	54.243.185.79
	107.22.184.230
	107.20.173.245
discovery.mdm.zenprise.com	184.72.219.144

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conformité FIPS 140-2

Jul 25, 2016

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 : 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 dans XenMobile Device Manager utilisent des modules de chiffrement fournis par OpenSSL et certifiés FIPS. (Pour vous tenir au courant des dernières informations, consultez les détails suivants.) 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 de bout en bout.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Prise en charge des langues dans XenMobile

Jul 25, 2016

Les applications Citrix Worx et la console XenMobile sont conçues pour être utilisées dans des langues autres que l'anglais. Cela inclut la prise en charge des caractères étendus ainsi que des claviers non anglais même lorsque l'application n'est pas traduite dans la langue préférée des utilisateurs.

Le tableau suivant affiche les langues dans lesquelles les versions les plus récentes des applications Worx sont traduites. Un X indique que la langue est prise en charge.

Langue de l'interface utilisateur	**Japonais**	**Chinois simplifié**	**Allemand**	**Français**	**Espagnol**	**Coréen**	**Portugais**	**Néerlandais**	**Italien**	**Danois**	**Suédois**
Apple iPhone/iPad											
Worx Home	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X			
Android Phone/Tablet											
Worx Home	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X			
WinPhone											

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Worx Home	X	X	X		X	X	X
WorxMail	X	X	X		X	X	X
WorxWeb	X	X	X		X	X	X

Pour connaître l'état de globalisation des produits Citrix, consultez le centre de connaissances Citrix.

Le tableau suivant résume l'état de traduction de la console XenMobile. Un X indique qu'elle est disponible dans cette langue.

Langues	**Chinois simplifié**	**Français**
Console XenMobile	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Check-list d'installation

Jul 25, 2016

Cette check-list dresse la liste des prérequis 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. Pour les étapes d'installation, consultez la section Installation de XenMobile.

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.	XenMobile	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Prérequis ou paramètre	Composant ou fonction	Prendre note du paramètre
	Réservez une adresse IP si vous installez une instance d'XenMobile. Si vous configurez un cluster, prenez note de toutes les adresses IP dont vous avez besoin.		
	• 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 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 Worx Home ou NetScaler Gateway Plug-in lorsque le split tunneling est défini sur Activé.	NetScaler Gateway	
	Vérifiez que le serveur XenMobile, NetScaler Gateway, le serveur externe Microsoft SQL et le serveur DNS peuvent communiquer entre eux.	XenMobile NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de plus amples informations, consultez la section Installation des licences NetScaler Gateway.	NetScaler Gateway XenMobile Serveur de licences Citrix	

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 dans XenMobile.

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

Vous devez ouvrir les ports pour autoriser la communication avec les composants XenMobile. Pour obtenir une liste complète des ports que vous devez ouvrir, consultez la section Exigences requises par XenMobile en matière de port.

	Configuration requise	Composant	Remarques
	Ouvrez les ports pour XenMobile	XenMobile NetScaler Gateway	

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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. Avant d'installer un serveur XenMobile en mode FIPS, vous devez vous assurer que les conditions préalables exigées par SQL Server sont remplies. Pour de plus amples informations, consultez la section Configuration de FIPS avec XenMobile.	XenMobile	

	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, cn=users,dc=ace,dc=com. NetScaler Gateway et XenMobile l'utilisent pour interroger Active Directory.	XenMobile NetScaler Gateway	
	Notez le nom unique de base du groupe.	XenMobile	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Configuration requise	Composant	Prendre note du paramètre
	Il s'agit du niveau d'arborescence sous lequel se trouvent les groupes. NetScaler Gateway et XenMobile l'utilisent pour interroger Active Directory.	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	

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 Worx Home. Vous créez un serveur virtuel pour autoriser les connexions utilisateur à partir de 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	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Configuration requise	Composant	Prendre note du paramètre
	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 Worx Home.	NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installation de XenMobile

Oct 11, 2016

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.

Avant de démarrer : 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. Consultez également la Configuration système requise pour XenMobile 10.1 et la Check-list de pré-installation de XenMobile.

Remarque : assurez-vous que l'hyperviseur est configuré avec l'heure correcte car XenMobile utilise cette heure. Assurez-vous également que la machine virtuelle XenMobile est configurée pour synchroniser l'heure de l'invité avec l'hôte dans les propriétés de la machine virtuelle.

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 du mode FIP : avant d'installer un serveur XenMobile en mode FIPS, vous devez vous assurer que les conditions préalables exigées par SQL Server sont remplies. Pour de plus amples informations, consultez la section Configuration de FIPS avec XenMobile.

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.
- Si vous installez Windows Server 2008 R2 ou Windows Server 2012, effectuez les opérations suivantes :
  - Supprimez le fichier Virtual Machines/<UUID spécifique à la version>.xml
  - Déplacez le fichier Legacy/<UUID spécifique à la version>.exp dans Virtual Machines

  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.

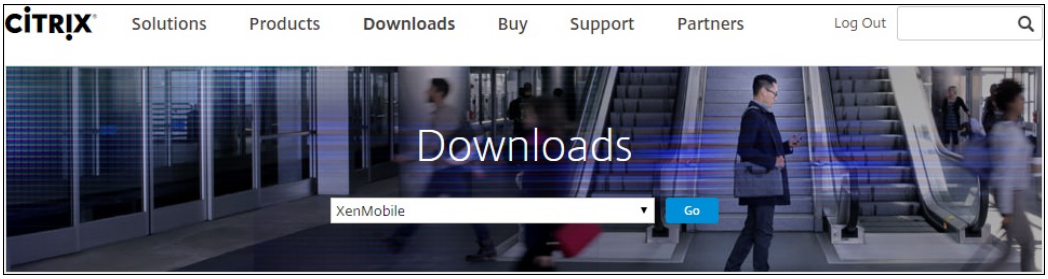
  Windows Server 2012 R2 ne requiert pas ces étapes supplémentaires.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 10.5.
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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

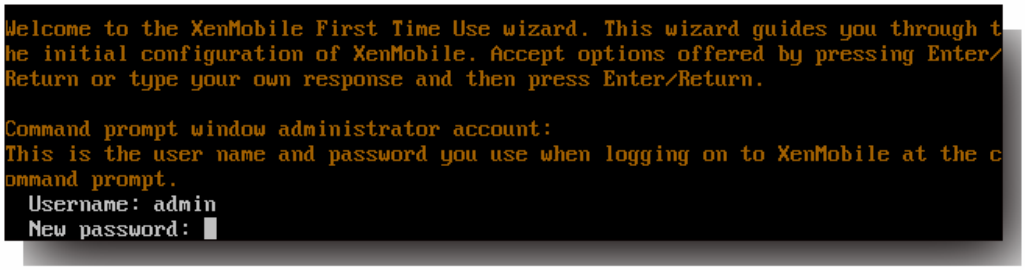
XenMobile à l'aide de la console de ligne de commande de XenCenter ou de vSphere.

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.

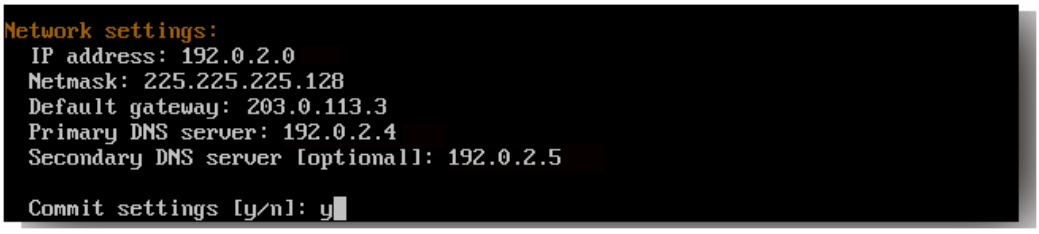
Configuration de XenMobile dans la fenêtre d'invite de commande

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 tapezy pour valider les paramètres suivants :
   1. Adresse IP
   2. Masque réseau
   3. Passerelle par défaut
   4. Serveur DNS principal
   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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

d'exemple.

5. Typey pour renforcer la sécurité en générant une phrase secrète de cryptage aléatoire oun pour fournir votre propre phrase secrète. Citrix vous recommande d'utilisery 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.

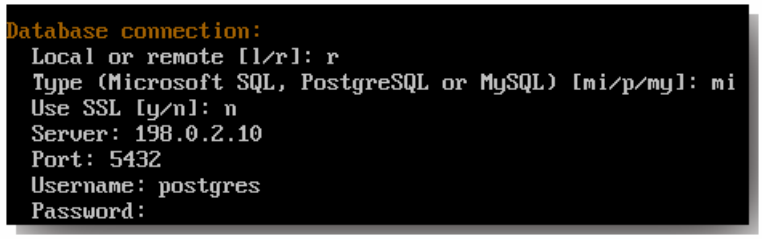
   Remarque : si vous souhaitez étendre votre environnement et configurer des serveurs supplémentaires, vous devez fournir votre propre phrase secrète. Il n'est pas possible d'afficher la phrase secrète si vous avez sélectionné une phrase secrète aléatoire.



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 Conformité FIPS 140-2 de XenMobile. Vous devez également vous assurer que certaines conditions sont respectées, comme abordé dans la section Configuration de FIPS avec XenMobile.



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



   1. Votre base de données peut être locale ou distante. Typel pour local our pour distant.
   2. Sélectionnez le type de base de données. Typemi pour Microsoft SQL ou tapezp 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, tapezy pour utiliser l'authentification SSL pour votre base de données.
   4. Fournissez le nom de domaine complet (FQDN) du serveur de base de données. 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 le mot de passe d'administrateur de votre 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, tapezy pour activer la mise en cluster des nœuds ou instances XenMobile.
   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.
9. Tapez le nom de domaine complet (FQDN) du serveur XenMobile. Le FQDN du serveur XenMobile doit être identique au nom commun du certificat d'écoute SSL.

   Remarque : le FQDN du serveur XenMobile est le DNS public pour l'inscription auprès de XenMobile.

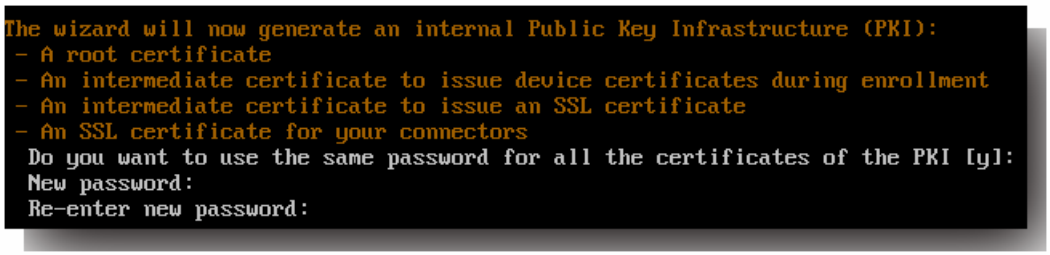


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 par XenMobile en matière de port.
    Remarque : acceptez les ports par défaut en appuyant sur Entrée (ou Retour sur un Mac).



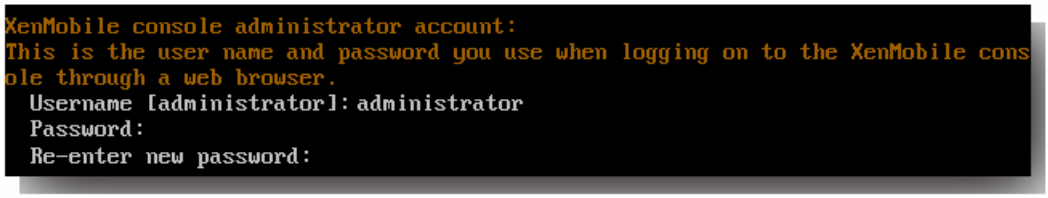
12. Ignorez la question suivante sur la mise à niveau à partir d'une version précédente de XenMobile, car vous installez XenMobile pour la première fois.
13. Typey si vous souhaitez utiliser le même mot de passe pour chaque certificat PKI. Pour plus d'informations sur la fonctionnalité PKI de XenMobile,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



    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.

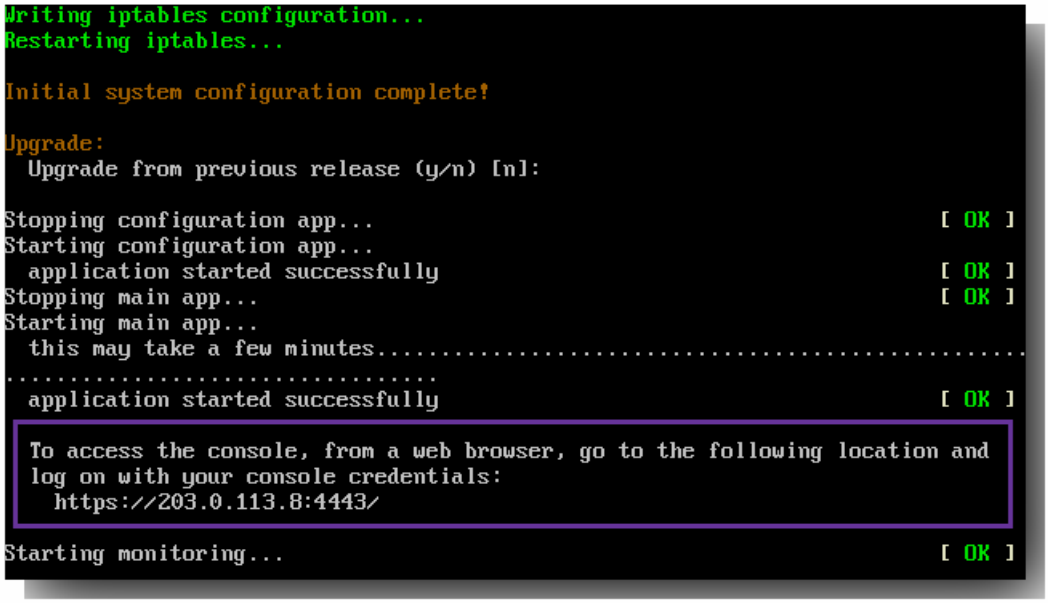
15. Appuyez sur Entrée pour valider les paramètres.
16. Créez un compte d'administrateur pour la connexion à la console XenMobile avec un navigateur Web. Retenez bien ces informations d'identification car vous devrez les réutiliser ultérieurement.



    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, tapezn 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.

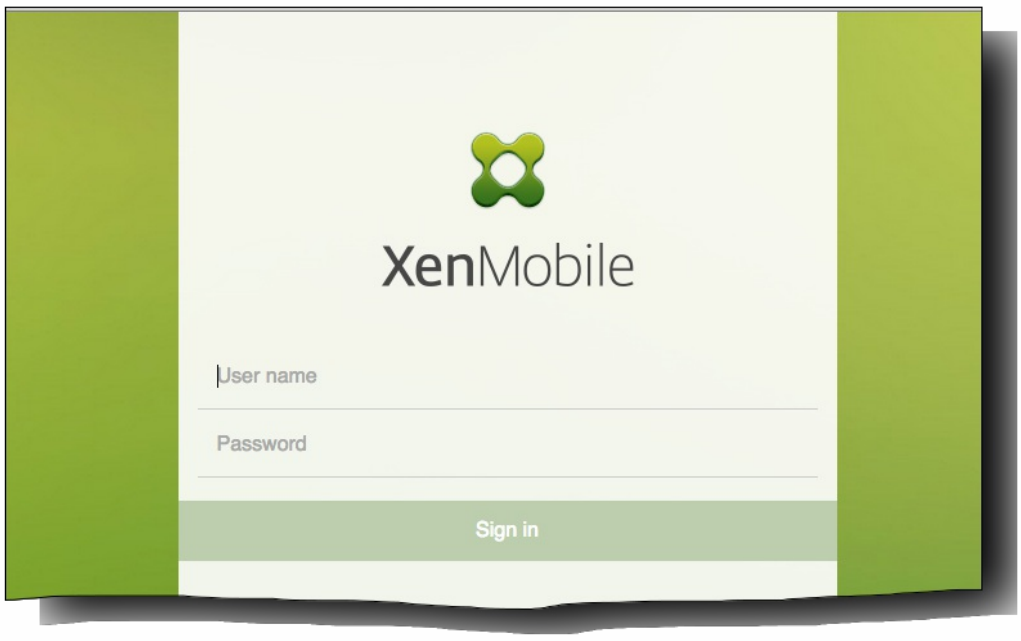
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configuration de 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. XenMobile est fourni avec une licence d'évaluation valide pendant 30 jours. Pour plus d'informations sur l'ajout et la configuration de licences et la configuration de notifications d'expiration, veuillez consulter la section Licences pour XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

5. Sur la page Certificat, cliquez sur Importer. La boîte de dialogue Importer apparaît.
6. Importez votre certificat APNS et d'écoute SSL. Pour de plus amples informations sur l'utilisation de certificats, consultez la section Chargement de certificats dans XenMobile.
   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 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 dans XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de FIPS avec XenMobile

Jul 25, 2016

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mise à niveau de XenMobile

Jul 25, 2016

Lorsque de nouvelles versions du logiciel XenMobile sont disponibles, vous pouvez mettre à niveau vers une nouvelle version. Vous disposez de deux options de mise à niveau en fonction de votre scénario :

- Pour installer les nouvelles versions du logiciel XenMobile 10.1, les Service Packs et les correctifs système, utilisez la page Gestion des versions dans la console XenMobile, comme décrit plus loin dans cet article.
- Pour mettre à niveau XenMobile 9.0 - MDM Edition, App Edition et Enterprise Edition - vers XenMobile 10.1, utilisez l'outil de mise à niveau. Pour plus de détails, consultez les articles de cette section. Vous pouvez télécharger l'outil de mise à niveau depuis la page de téléchargements de Citrix.com.

Remarque

- Citrix vous recommande d'utiliser la dernière version de l'outil de mise à niveau. Cette version vous permet de mettre à jour les modes MAM, MDM et Enterprise de votre environnement XenMobile 9.0 à l'aide d'un seul outil. Lorsque de nouvelles versions ou des mises à jour importantes sont disponibles, elles sont publiées sur Citrix.com, et une notification est envoyée au point de contact de chaque client.
- Si votre configuration XenMobile 9.0 est basée sur des instances SQL nommées, vous devez suivre les étapes spécifiques à cette situation. Pour plus de détails, consultez la section Prise en charge des instances SQL nommées.

Important

- Tenez compte de ce problème connu dans XenMobile 10.1 car il est probable que votre nom d'hôte XenMobile 9.0 comporte une majuscule. Dans ce cas, après la mise à niveau vers XenMobile 10.1, les appareils ne peuvent pas accéder à Worx Store. Lorsque vous configurez le serveur XenMobile avec une lettre majuscule dans le nom d'hôte, par exemple ABC.Xms.com, Worx Store ne s'ouvre pas sur les appareils après l'inscription des appareils. [#545527]
- Après la mise à niveau vers XenMobile 10.1, lorsque vous mettez à jour dans XenMobile 10.1 les applications mobiles Worx que vous avez configurées dans une version antérieure, les paramètres des applications ne s'affichent plus dans la console XenMobile. Vous devez modifier et configurer à nouveau les paramètres de ces applications. Il est cependant inutile de les réinstaller. Vous ne devez effectuer cette opération qu'une seule fois ; les valeurs seront conservées lors des prochaines mises à jour de l'application ou du serveur.

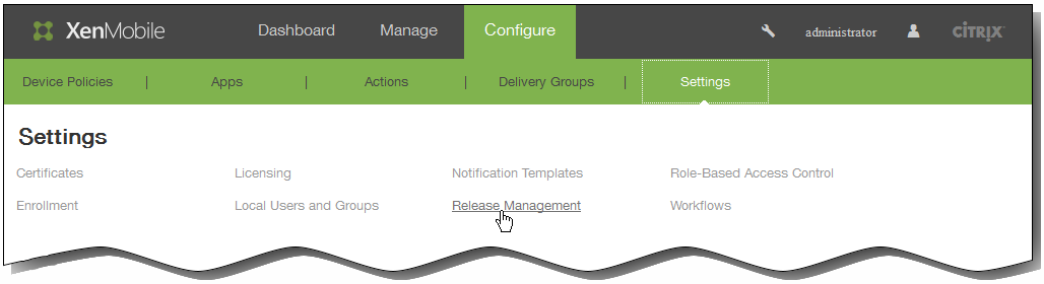
Configuration requise :

- 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.
- Vérifiez la configuration système requise.

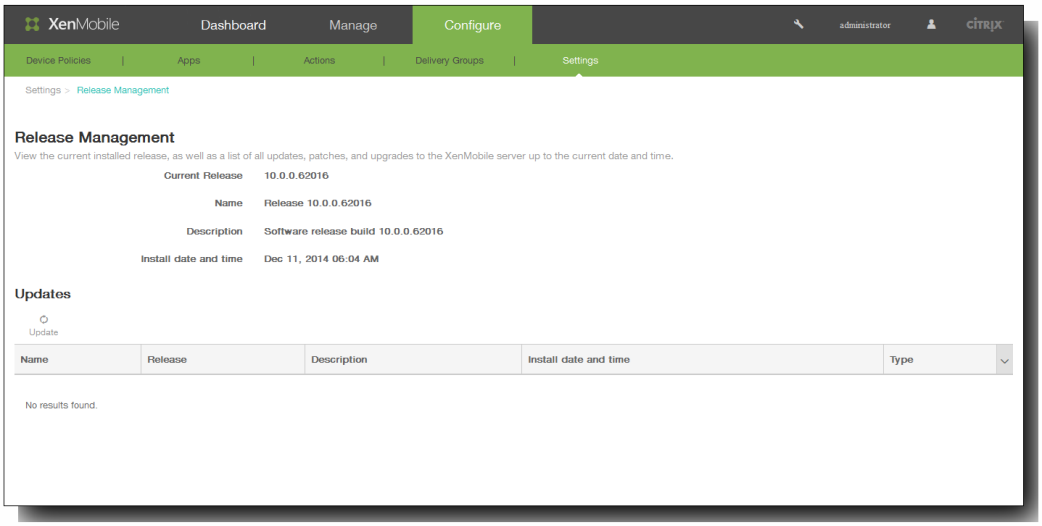
1. Ouvrez une session sur votre compte sur le site Web de Citrix et téléchargez le fichier XenMobile Upgrade (.bin) sur un emplacement approprié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Gestion des versions.



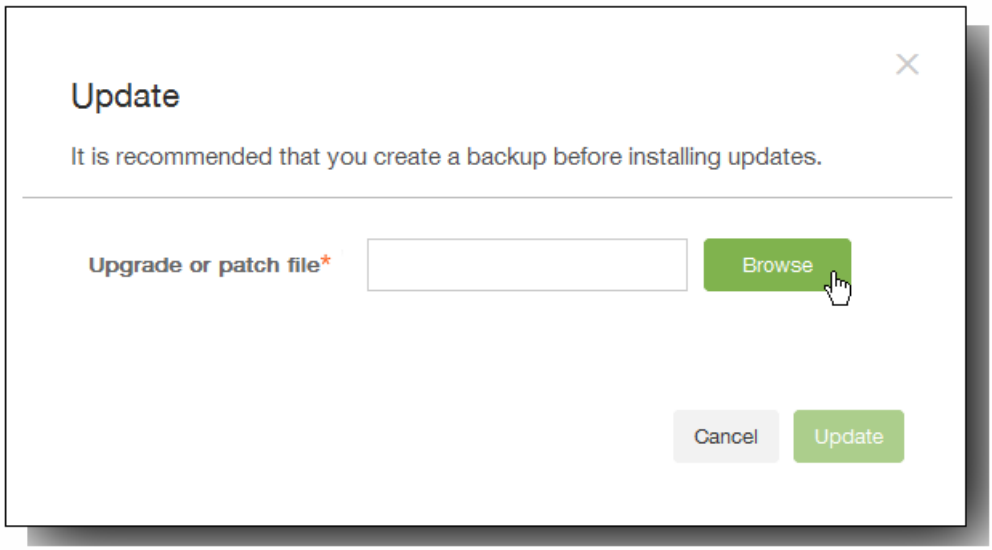
La page Gestion des versions s'affiche. Cette dernière affiche la version du logiciel actuellement installé, ainsi qu'une liste des mises à jour, correctifs et mises à niveau que vous avez déjà téléchargés.



3. Sous Mises à jour, cliquez sur Mettre à jour. La boîte de dialogue Mettre à jour s'affiche.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



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, toutefois, XenMobile nécessite un redémarrage, vous devez utiliser la ligne de commande.
   Important : si votre système est configuré en mode cluster, suivez les étapes suivantes pour mettre à jour chaque nœud :
   - Arrêtez tous les nœuds sauf un.
   - Mettez à jour ce nœud.
   - 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 mise à jour est restauré.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À propos de l'outil de mise à niveau

Jul 25, 2016

Pour effectuer une mise à niveau depuis XenMobile 9.0 (MDM Edition, App Edition et Enterprise Edition) vers XenMobile 10.1, vous devez utiliser l'outil de mise à niveau. Vous pouvez télécharger cet outil sur la page des téléchargements du site Citrix.com. Les problèmes connus et résolus dans cette version sont répertoriés plus loin dans cet article :

- Problèmes résolus dans l'outil de mise à niveau dans cette version
- Problèmes connus dans l'outil de mise à niveau dans cette version

La dernière version de l'outil de mise à niveau comprend des améliorations de l'interface, la prise en charge de Remote PostgreSQL 9.3.11, et la prise en charge de Device Manager 9.0 RP3 et d'App Controller RP7.

L'outil de mise à niveau est intégré à la machine virtuelle XenMobile 10.1. Vous activez l'assistant à usage unique via la console de ligne de commande lors de l'installation initiale de XenMobile 10.1.

Chemins de mise à niveau

Un chemin de mise à niveau est une séquence recommandée destinée à garantir que vos données sont correctement migrées. Cette section contient les chemins de mise à niveau pour chaque type d'appareil et les combinaisons de mode d'inscription :

- Appareils iOS et Android (tous les modes d'inscription), ainsi que téléphones et tablettes Windows inscrits en mode MDM
- Téléphones Windows inscrits dans en mode Enterprise

> Il n'existe pas de chemin de mise à niveau pour les téléphones ou tablettes Windows inscrits en mode MAM ou pour les tablettes Windows inscrites en mode Enterprise.

Pour mettre à niveau, suivez la séquence en démarrant par l'étape qui correspond à la version que vous mettez à niveau.

1. Si vous utilisez XenMobile 8.6 ou 8.7, vous devez d'abord mettre à niveau vers XenMobile 9.0.

> Vous ne pouvez pas utiliser l'outil de mise à niveau pour passer de XenMobile 8.6 ou 8.7 à XenMobile 10.1.

2. Utilisez l'outil de mise à niveau pour mettre à niveau XenMobile 9.0 vers XenMobile 10.1.

- Après la mise à niveau de XenMobile 9 vers XenMobile 10.1, certains clients ont signalé des problèmes d'accès à WorxStore, d'ouverture d'applications, ainsi que des problèmes avec d'autres fonctionnalités. Pendant que Citrix s'emploie activement à résoudre ces problèmes, vous pouvez temporairement annuler la mise à niveau de manière à restaurer XenMobile 9. Pour de plus amples informations, consultez la section Restauration des mises à niveau de XenMobile.
- Lorsque la Multi-Tenant Console (MTC) est activée sur XenMobile 9.0, vous pouvez migrer la MTC vers XenMobile 10.1. Pour obtenir des instructions détaillées, consultez la section Mise à niveau du serveur locataire de la console MTC vers XenMobile 10.1.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Mettez à jour XenMobile 10.1 vers XenMobile 10.3 (ou 10.3.5).

    Lorsque cette mise à jour suit une mise à niveau de XenMobile 9.0 vers 10.1, vous pouvez migrer les données des appareils Android, iOS et Windows pris en charge.

4. Mettez à jour XenMobile 10.3 vers XenMobile 10.3.5.

Les étapes suivantes sont recommandées 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 10.3.

1. Installez les derniers correctifs pour Device Manager et App Controller.

2. Téléchargez la dernière version de l'outil de mise à niveau.

3. Mettez à niveau Worx Home sur Device Manager vers la version 10.2, puis déployez Worx Home.

    Si les utilisateurs exécutent Worx Home 9.x et qu'ils ont inscrit des téléphones Windows, nous recommandons de mettre à niveau Worx Home vers 10.2 avant de procéder à la mise à niveau. Ensuite, dès que la mise à niveau vers 10.1 est terminée, le serveur XenMobile doit être mis à niveau vers 10.3 avant de connecter les appareils.

4. Désinstallez manuellement Worx Home 9.x des appareils des utilisateurs.

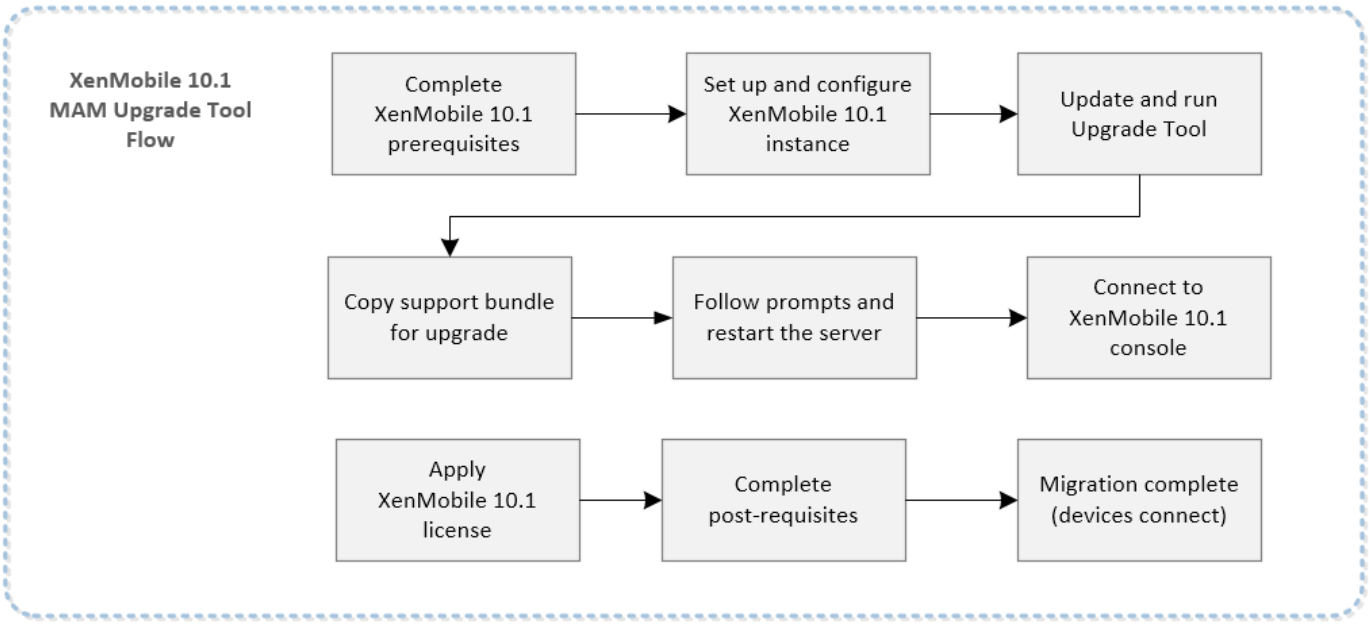
5. Demandez aux utilisateurs d'accéder au Download Hub sur leur téléphone pour installer Worx Home 10.2, que vous avez déployé à partir de Device Manager.

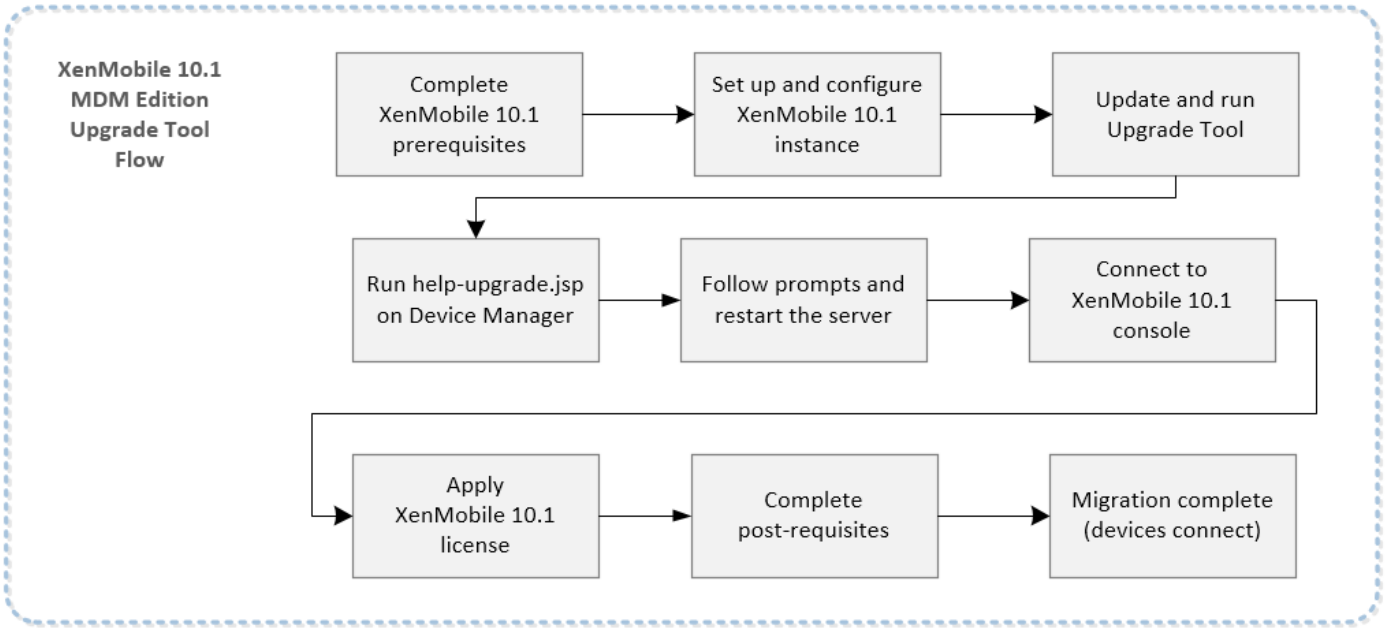
6. Mettez à niveau vers XenMobile 10.1, puis mettez à niveau immédiatement vers XenMobile 10.3 avant de connecter des appareils au serveur XenMobile mis à niveau.

7. 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.

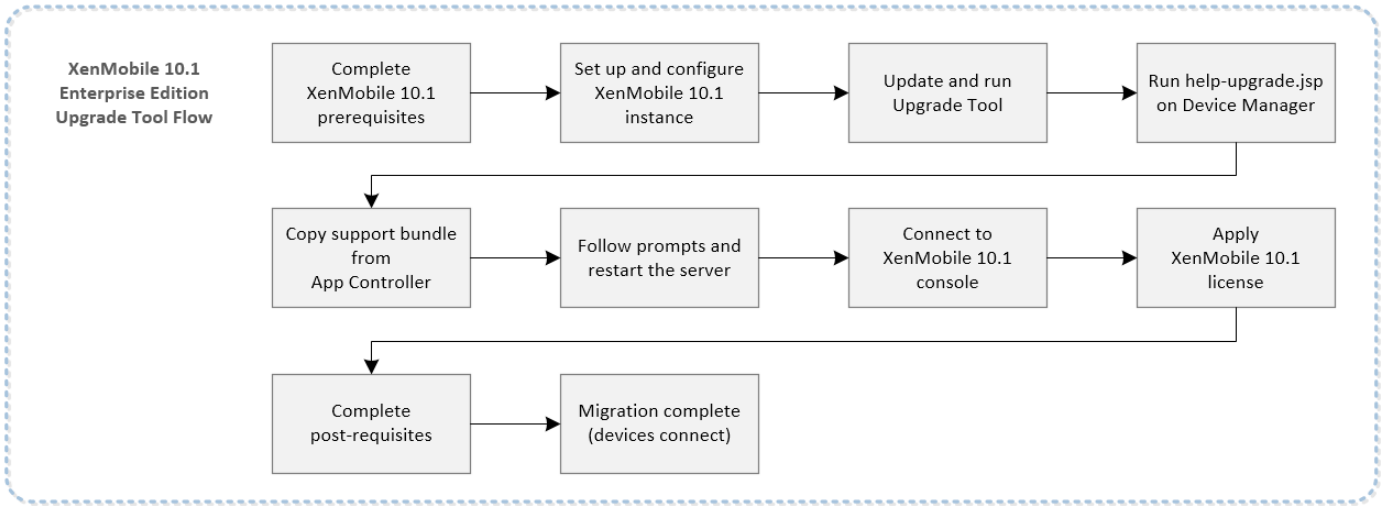
Les figures suivantes illustrent les étapes de base nécessaires pour effectuer la mise à niveau de XenMobile 9.0 vers XenMobile 10.1.

© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.



Consultez les sections Conditions préalables et Problèmes connus et problèmes résolus de XenMobile 10.1, ainsi que les problèmes connus et résolus dans l'outil de mise à niveau décrits ici avant de commencer la migration vers XenMobile 10.1.

Problèmes résolus dans l'outil de mise à niveau dans cette version

> **Remarque**
>
> Pour obtenir une liste des problèmes résolus dans les versions précédentes de l'outil de migration, téléchargez ce PDF.

Après la mise à niveau de XenMobile 9 vers XenMobile 10.1, puis la mise à jour vers XenMobile 10.3, les stratégies de clip Web ne sont pas déployées sur les appareils Windows 10 qui étaient inscrits dans XenMobile 9. Les stratégies de clip Web sont déployées sur les appareils Windows 10 inscrits dans XenMobile 10.3. [#610101]

Après la mise à niveau de XenMobile 9 vers XenMobile 10.1, les licences VPP en gros volumes ne fonctionnent pas. [#610418]

Les abonnements utilisateur ne sont pas migrés si les informations d'abonnement incluent le nom de domaine en majuscules. [#620542]

Une application préparée à l'aide du SDK Worx App n'est pas migrée si elle contient une adresse URL non standard, par exemple si vous ne formatez pas l'ID du magasin dans l'adresse URL en tant que id*app-ID*?mt=8. [#625920]

Problèmes connus dans l'outil de mise à niveau dans cette version

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important

Tenez compte de ce problème connu dans XenMobile 10.1 car il est probable que votre nom d'hôte XenMobile 9.0 comporte une majuscule. Dans ce cas, après la mise à niveau vers XenMobile 10.1, les appareils ne peuvent pas accéder à WorxStore.

- Lorsque vous configurez le serveur XenMobile avec une lettre majuscule dans le nom d'hôte, par exemple ABC.Xms.com, WorxStore ne s'ouvre pas sur les appareils après l'inscription des appareils. [#545527]

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]
- 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]
- Lorsque les utilisateurs mettent à niveau un déploiement XenMobile 9 basé sur des instances SQL nommées en suivant les étapes recommandées dans l'article Prise en charge des instances SQL nommées pour résoudre un problème de nom de domaine complet, le pack d'assistance est chargé avec succès, mais une erreur de connexion à la base de données s'affiche. Par conséquent, les utilisateurs ne peuvent pas poursuivre la mise à niveau. [#605775]
- Certaines configurations de stratégie de restriction sont obsolètes dans 10.1. Par conséquent, XenMobile ne parvient pas à déployer la stratégie de restriction en entier sur les téléphones Windows 10 après la mise à niveau de XenMobile 9 vers XenMobile 10.1, puis la mise à jour vers XenMobile 10.3. Toutefois, si vous affichez et enregistrez les paramètres de stratégie dans XenMobile 10.3, la stratégie est déployée avec succès. [#608541]
- 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]

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

- L'outil de mise à niveau ne prend pas en charge les instances nommées des bases de données SQL Server de XenMobile 9.0. L'outil fournit un numéro de port, mais aucun nom d'instance. La mise à niveau échoue avec une erreur java.sql.SQLException si l'outil tente d'établir une connexion avec l'instance inattendue plutôt que l'instance par défaut. Pour corriger les problèmes, consultez la section Prise en charge des instances SQL nommées. [#575679]
- 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]
- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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]

RBAC

Problèmes avec les paramètres RBAC après la mise à niveau :

- 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.
- 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. [#569350, #569395, #569423]

Windows CE

- Les appareils Windows CE ne sont pas pris en charge dans XenMobile 10.1.

Worx Home et WorxStore

- Après la mise à jour de XenMobile 10.1 vers XenMobile 10.3, lorsque les utilisateurs ouvrent Worx Home sur des appareils iOS et Android, le WorxStore est vide. Pour contourner le problème, redémarrez NetScaler ou effacez le cache de NetScaler. [#609706]
- Avant la mise à niveau de XenMobile 9 vers XenMobile 10.1, 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. [#619458]
  Pour de plus amples informations sur les conditions préalables requises, consultez la section Conditions préalables requises.
- Les utilisateurs équipés d'appareils en mode MAM exclusif ne peuvent pas s'authentifier auprès de Worx Home après une mise à niveau de XenMobile 9.0 vers XenMobile 10.1, si vous définissez ensuite l'option LDAP **Recherche utilisateur par** sur **sAMAccountName** puis que vous mettez à niveau vers XenMobile 10.3.x. [#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 10.3, puis chargez-le sur le domaine Android for Work.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ce que fait l'outil de mise à niveau

L'outil de mise à niveau XenMobile 10.1 permet de migrer les données utilisateur et de configuration d'un serveur XenMobile 9.0 vers une nouvelle instance de XenMobile 10.1 avec le même nom de domaine complet (FQDN).

- Quelle que soit votre édition de XenMobile, vous pouvez effectuer une mise à niveau test à l'aide de données de configuration de production pour comparer XenMobile 9.0 et XenMobile 10.1 sans affecter votre environnement de production.
- Vous pouvez procéder à une mise niveau de production complète pour déplacer tous les éléments de XenMobile 9.0 vers XenMobile 10.1. Vous ne pouvez cependant pas effectuer de déplacement à partir de l'environnement test pour mettre à niveau un environnement de production. Vous devez recommencer depuis le début pour la mise à niveau de l'environnement de production.

Vous trouverez des diagrammes d'architecture des déploiements de XenMobile 10.1 dans la section Aperçu de l'architecture.

Lorsque vous choisissez **Test Drive** dans l'outil, seules les données de configuration sont migrées vers XenMobile 10.1 ; aucune donnée utilisateur (dans le cas de déploiements XenMobile Enterprise Edition) ou d'appareil n'est migrée.

Lorsque vous choisissez **Upgrade** dans l'outil, toutes les configurations, tous les appareils et toutes les données utilisateur sont migrées. Lorsque vous ouvrez une session sur la console XenMobile 10.1 après la mise à niveau, vous pouvez voir toutes les données utilisateur et de l'appareil qui ont été migrées depuis XenMobile 9.0.

Remarque : il ne s'agit pas d'une migration sur place ; toutes les données sont *copiées* durant la migration et non déplacées vers XenMobile 10.1. XenMobile 9.0 reste inchangé jusqu'à ce que vous déplaciez le serveur XenMobile 10.1 dans l'environnement de production. Lorsque des utilisateurs sont connectés à XenMobile 10.1 en environnement de production, si pour une raison quelconque, vous souhaitez revenir à XenMobile 9.0, ces utilisateurs doivent se réinscrire dans XenMobile 9.0.

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 fois la mise à niveau test effectuée, vous pouvez effectuer une mise à niveau de production sur un environnement isolé pour des tests plus poussés. Une fois que vous avez validé la mise à niveau, vous pouvez effectuer une autre mise à niveau de production sur votre environnement de production.

Après la réussite de la mise à niveau de production, pour basculer XenMobile 10.1 en mode production, vous devez effectuer les opérations suivantes :

1. Si NetScaler répartit la charge des serveurs XenMobile Device Manager, vous devez :

- Créer un nouveau service d'équilibrage de charge XenMobile 10.1.
- Basculer le service XenMobile 9.0 vers le service XenMobile 10.1.

2. Pour les environnements autonomes, mettre à jour l'entrée DNS pour mapper le nom de domaine complet (FQDN) de XenMobile 9.0 sur la nouvelle adresse IP du serveur XenMobile 10.1. Cette étape n'est pas nécessaire pour les environnements en cluster.

Pour de plus amples informations, consultez la section Post-requis de l'outil de mise à niveau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Lorsque vous utilisez l'outil de mise à niveau, les informations suivantes **ne sont pas** migrées vers XenMobile 10.1 :

- Les informations de licence.
- Les rapports de données.
- Les stratégies de groupes de serveurs et les déploiements associés (non pris en charge dans XenMobile 10.1).
- Le groupe MSP (Managed Service Provider).
- Les stratégies et les paquetages associés à Windows CE et 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 migration.log.
- CXM Web (remplacé par Citrix WorxWeb).
- 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 migrée. XenMobile 10.1 prend en charge une seule stratégie de marque ; vous devez laisser une stratégie de marque dans XenMobile 9.0 pour que votre migration vers XenMobile 10 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 10.1 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 10.1).

Veuillez également noter les nouveautés suivantes dans XenMobile 10.1 :

- XenMobile 10.1 ne prend pas en charge les utilisateurs Active Directory qui sont assignés à des groupes locaux.
- La hiérarchie des groupes locaux est aplatie.

Planification de votre mise à niveau

> ### Important
>
> Pour chacune des étapes, suivez les instructions dans Activation et exécution de l'outil de mise à niveau et Conditions préalables. Le processus de mise à niveau est complexe ; assurez-vous que les conditions préalables sont remplies avant de commencer. Si vous entrez un mot de passe incorrect pour le certificat, par exemple, la mise à niveau échoue. En cas d'échec, vous devez configurer une nouvelle instance de XenMobile 10.1 dans la console de ligne de commande et démarrer l'outil de mise à niveau.

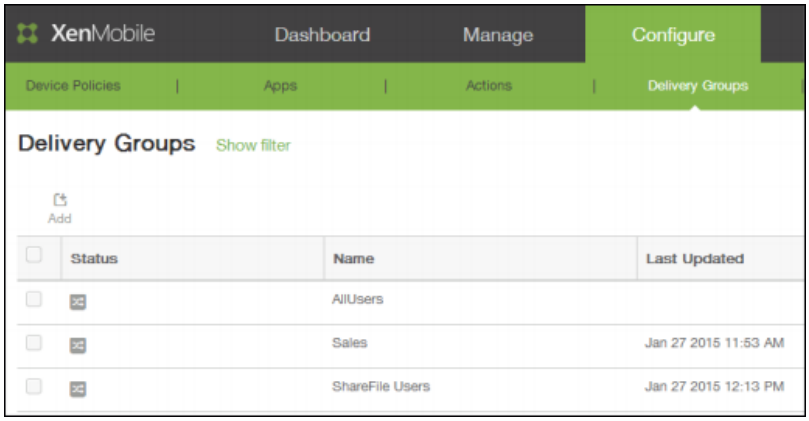
Citrix vous conseille de suivre les étapes suivantes pour procéder à la mise à niveau :

1. Testez la mise à niveau dans un environnement de simulation.
    1. Configurez NetScaler 10.5 avec NetScaler Gateway et des serveurs virtuels d'équilibrage de charge NetScaler, de préférence configurés à l'aide de l'utilitaire de XenMobile 10.
    2. Apportez les modifications appropriées au pare-feu et au DNS.
2. Effectuez une mise à niveau de production dans un environnement de simulation.
    1. Ajustez la configuration de NetScaler en suivant les étapes requises après l'installation.
    2. Apportez les modifications appropriées au pare-feu et au DNS.
3. Effectuez une mise à niveau de production dans votre environnement de production et passez en mode opérationnel.
    1. Planifiez les temps d'arrêt lors de l'exécution de la migration.

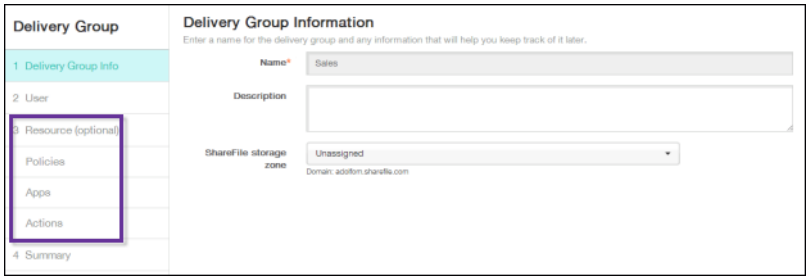
© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Ajustez la configuration de NetScaler en suivant les étapes requises après l'installation.
3. Apportez les modifications appropriées au pare-feu et au DNS.

Notez qu'une fois la mise à niveau effectuée, les paquetages de déploiement dans Device Manager sont appelés groupes de mise à disposition dans XenMobile 10.1, comme le montre la figure suivante. Pour de plus amples informations, consultez la section Gestion des groupes de mise à disposition.



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.



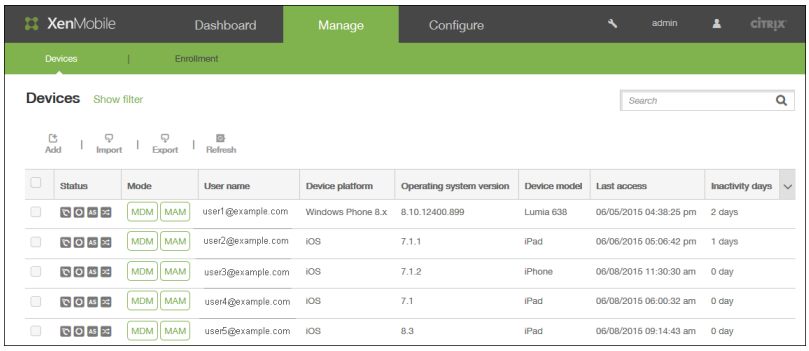
Les utilisateurs n'ont pas besoin de réinscrire leurs appareils après une mise à niveau de production vers XenMobile 10.1. Les appareils doivent se connecter automatiquement au serveur XenMobile 10.1 en fonction de l'intervalle de pulsation. Les utilisateurs peuvent toutefois être invités à s'authentifier à nouveau avant que l'appareil puisse se reconnecter.

Si vous souhaitez connecter immédiatement un appareil à XenMobile 10.1, utilisez WorxHome > Infos sur l'appareil > Actualiser la stratégie sur l'appareil.

Une fois les appareils des utilisateurs connectés, vérifiez que les appareils sont affichés dans la console XenMobile, comme

© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'illustre la figure suivante.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conditions préalables

Jul 25, 2016

Vous devez remplir les pré-requis suivants avant d'exécuter l'outil de mise à niveau de XenMobile. Pour consulter la liste des problèmes connus, consultez la section À propos de l'outil de mise à niveau.

> ## Important
>
> Tenez compte de ce problème connu dans XenMobile 10.1 car il est probable que votre nom d'hôte XenMobile 9.0 comporte une majuscule. Dans ce cas, après la mise à niveau vers XenMobile 10.1, les appareils ne peuvent pas accéder à Worx Store.
>
> - Lorsque vous configurez le serveur XenMobile avec une lettre majuscule dans le nom d'hôte, par exemple ABC.Xms.com, Worx Store ne s'ouvre pas sur les appareils après l'inscription des appareils. [#545527]

Correctif App Controller

Téléchargez le dernier fichier de correctif pour XenMobile 9.0 App Controller depuis la page Downloads (Téléchargements) sur Citrix.com. 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 **Télécharger** et redémarrez App Controller.

Nom du magasin

> ## Remarque
>
> Avant d'effectuer la mise à niveau de XenMobile 9 vers XenMobile 10.1, vous devez rétablir le nom par défaut du 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.



Serveur de licences Citrix

Assurez-vous d'avoir installé le serveur de licences Citrix 11.12.1 (disponible sur la page Système de licences Citrix) et d'avoir

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configuré le serveur avec la dernière licence V6 pour votre édition de XenMobile. Assurez-vous que les ports de serveur de licences 27000 et 7279 sont ouverts sur le serveur. Cette étape est primordiale pour éviter que les utilisateurs soient forcés à réinscrire leurs appareils.

NetScaler 10.5 et XenMobile 10.1

Citrix vous recommande d'utiliser Netscaler 10.5 avec XenMobile 10.1. Avant de mettre à niveau vers NetScaler 10.5, enregistrez une copie de votre configuration Netscaler (ns.conf). La version Netscaler 10.5 comprend un utilitaire de déploiement simple et rapide qui vous guide à travers les étapes requises pour intégrer NetScaler 10.5 et XenMobile 10. Pour de plus amples informations, consultez la section FAQ : Intégration de XenMobile 10 et NetScaler 10.5.

Serveur LDAP

Assurez-vous que le nouveau serveur XenMobile 10.1 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.

Ouvrir les ports du pare-feu

Ouvrez les mêmes ports de pare-feu pour la nouvelle adresse IP du serveur XenMobile 10.1 que ceux ouverts pour l'adresse IP du serveur XenMobile 9.0.

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 10.1.

De XenMobile 9.0		**à XenMobile 10.1**
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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

PostgreSQL local	MS SQL
MDM Edition	
PostgreSQL local	PostgreSQL local
MS SQL	MS SQL
Remote PostgreSQL	Remote PostgreSQL

Durant le processus de migration des 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"
Remplacez cette ligne par "host all all 0.0.0.0/32 md5"

2. Enregistrez le fichier.

3. Arrêtez et redémarrez le service.

4. Recherchez et ouvrez le fichier postgresql.conf et changez cette ligne :
"#listen_addresses = 'localhost'" to "listen_addresses = '*'"

> ## Remarque
>
> cette opération peut être rendue restrictive en autorisant uniquement les adresses IP des serveurs XenMobile 9.0 et XenMobile 10.1 à accéder à la base de données PostgreSQL (listen_addresses = '10.x.x.1,10.x.x.2).

5. Arrêtez et redémarrez le service PostgreSQL pour que les modifications prennent effet.

Si un port personnalisé a été assigné à la 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 10.1 de se connecter à la base de données et de migrer les informations requises.

Certificat SSL externe

Les certificats SSL externes doivent respecter les critères indiqués dans la section Comment configurer un certificat SSL externe. Veillez à consulter votre pki.xml avant de démarrer la migration pour vous assurer que le certificat SSL remplit ces conditions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom d'utilisateur du compte d'administrateur

Le compte d'administrateur utilisé pour se connecter à la console XenMobile 10.1 peut contenir uniquement des lettres en minuscules ; vous ne pourrez pas vous connecter à la console XenMobile 10.1 après la migration si le compte contient des lettres majuscules. Créez un compte d'utilisateur administrateur avec uniquement des lettres en minuscules et disposant de toutes les autorisations afin qu'une fois la migration effectuée, vous puissiez utiliser ce compte pour ouvrir une session sur la console XenMobile 10.1.

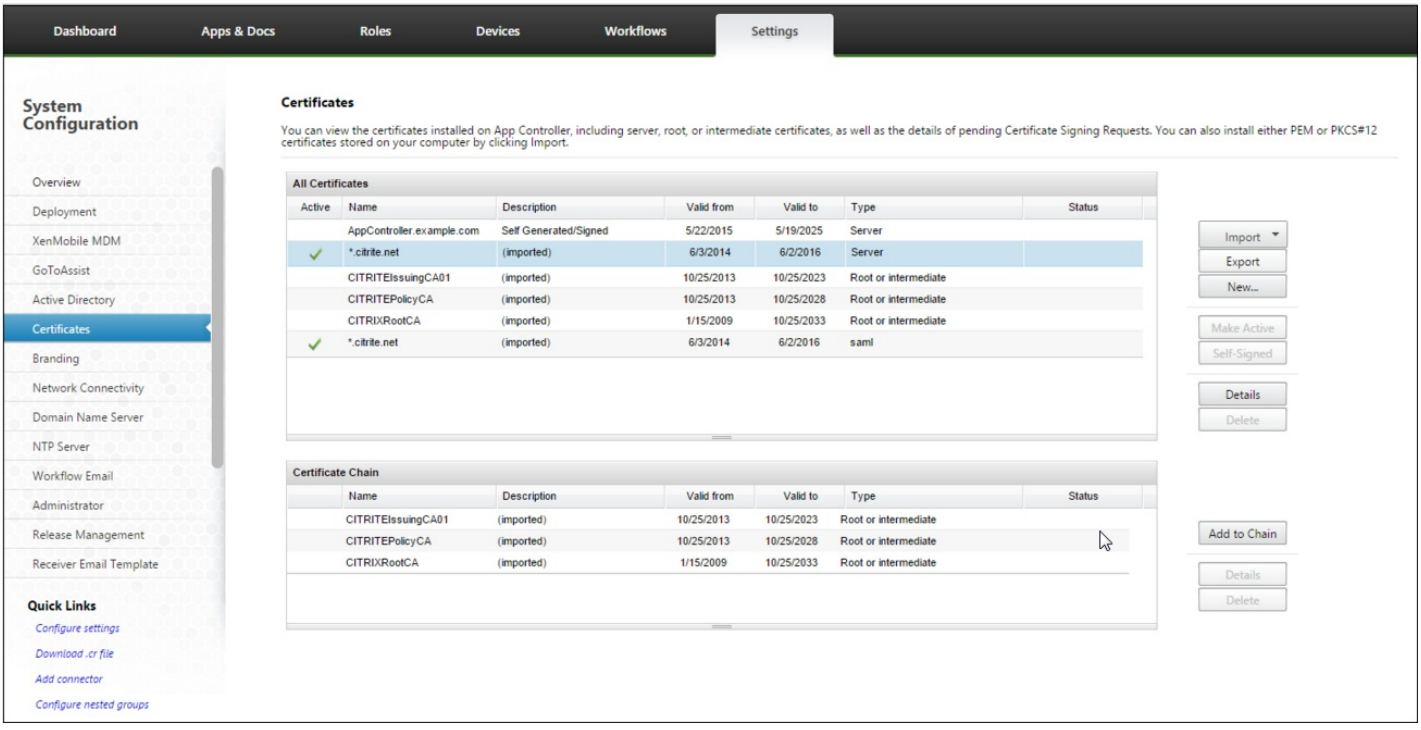
Noms de paquetages de déploiement avec caractères spéciaux

Les noms de paquetages de déploiement dans XenMobile 9.0 qui contiennent des caractères spéciaux (!, $(),#,%, +,*, ~,?, |,} {, []) sont migrés, mais les groupes de mise à disposition dans XenMobile 10.1 ne peuvent pas être modifiés après la migration. En outre, les utilisateurs locaux et les groupes locaux créés dans XenMobile 9.0 qui contiennent un crochet ouvrant ([) causent des problèmes lors de la création d'invitations d'inscription dans XenMobile 10.1. Avant la migration, supprimez tous les caractères spéciaux des noms de paquetages de déploiement et les crochets ouverts des noms d'utilisateurs locaux et de groupes locaux.

Exporter le certificat de serveur XenMobile 9.0

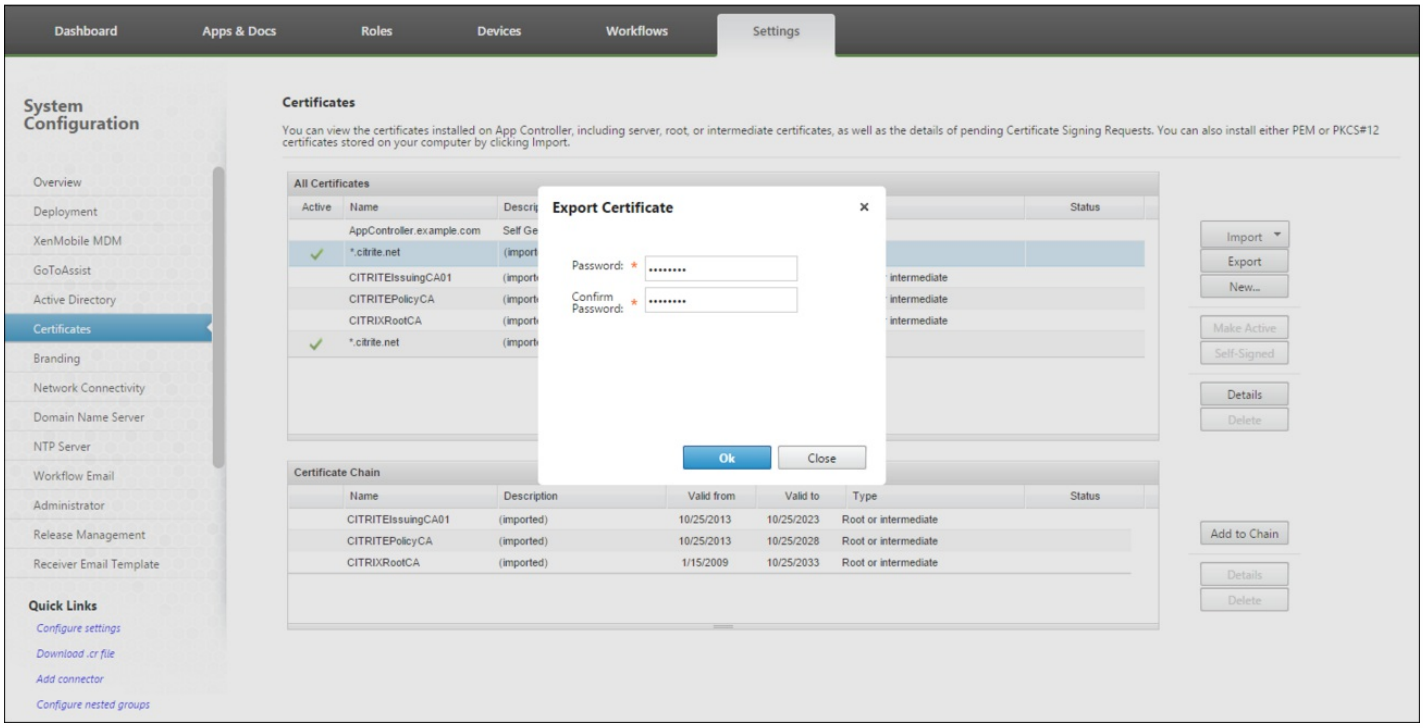
Si vous effectuez la mise à niveau d'un déploiement XenMobile 9.0 Enterprise Edition, vous devez exporter le certificat de serveur App Controller et l'importer dans NetScaler Gateway. Ouvrez une session sur XenMobile 9.0 App Controller et cliquez sur **Certificats**. Suivez ces étapes pour exporter le certificat de serveur :

1. Dans la liste des certificats, cliquez sur le certificat de serveur que vous souhaitez exporter, puis cliquez sur **Exporter**.



2. Dans la boîte de dialogue **Exporter certificat**, entrez le mot de passe de votre certificat dans les deux champs et cliquez sur **OK**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Importez le certificat de serveur dans le boîtier NetScaler Gateway.

Serveur pour le chargement du pack de support crypté

Serveur où vous pouvez télécharger le pack de support crypté à partir de l'interface de ligne de commande à l'aide du protocole FTP (File Transfer Protocol) ou du protocole SCP (Secure Copy Protocol).

Après avoir passé en revue les problèmes connus et rempli toutes les conditions préalables, démarrez la mise à niveau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Activation et exécution de l'outil de mise à niveau de XenMobile 10.1

Oct 11, 2016

Les étapes suivantes sont les étapes de base à suivre pour mettre à niveau les déploiements XenMobile Enterprise Edition et MAM de XenMobile 9.0 vers XenMobile 10.1 :

1. Configurez l'instance de XenMobile 10.1 à l'aide de la console de ligne de commande.
2. Conformez-vous à tous les pré-requis de l'outil de mise à niveau. Pour plus de détails, consultez la section Conditions préalables.
3. Démarrez l'outil de mise à niveau dans un navigateur.
4. Exécutez help-upgrade.jsp. XenMobile Enterprise Edition uniquement.
5. Mettez à jour App Controller.
6. Créez un pack d'assistance.
7. Entrez l'adresse URL de l'emplacement des fichiers de XenMobile 9.0. XenMobile Enterprise Edition uniquement.
8. Chargez le pack d'assistance pour l'outil de mise à niveau.
9. Mettez à jour la configuration de la base de données.
10. Démarrez la mise à niveau. **Remarque :** si vous mettez à jour l'outil de mise à niveau, vous devez effacer le cache de votre navigateur avant de démarrer la mise à niveau.
11. Redémarrez le serveur XenMobile 10.1.
12. Ouvrez une session sur la console XenMobile 10.1.
13. Appliquez les licences XenMobile 10.1 pour autoriser les utilisateurs à se connecter.
14. Pour mettre à niveau un environnement XenMobile Enterprise Edition de production, si vous utilisez l'équilibrage de charge NetScaler, supprimez l'adresse IP du serveur XenMobile 9.0, puis ajoutez celle du serveur XenMobile 10.1.
15. Pour une mise à niveau de production, modifiez le DNS externe XenMobile pour pointer vers le nouveau serveur XenMobile 10.1.

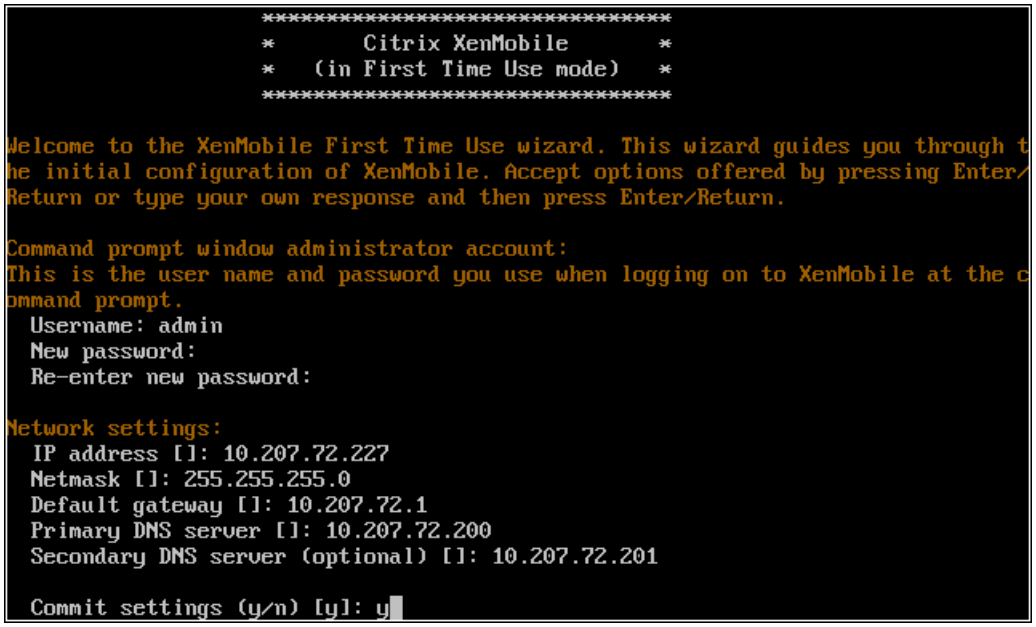
Pour installer une instance de XenMobile 10.1 et activer l'outil de mise à niveau

Activez l'outil de mise à niveau à l'aide de l'interface de ligne de commande lors de l'installation initiale de XenMobile 10.1, comme illustré dans les figures suivantes.

> ## Important
>
> si vous voulez prendre un instantané de votre système, faites-le après la configuration initiale de XenMobile 10.1 et *avant* d'accéder à l'outil de mise à niveau.

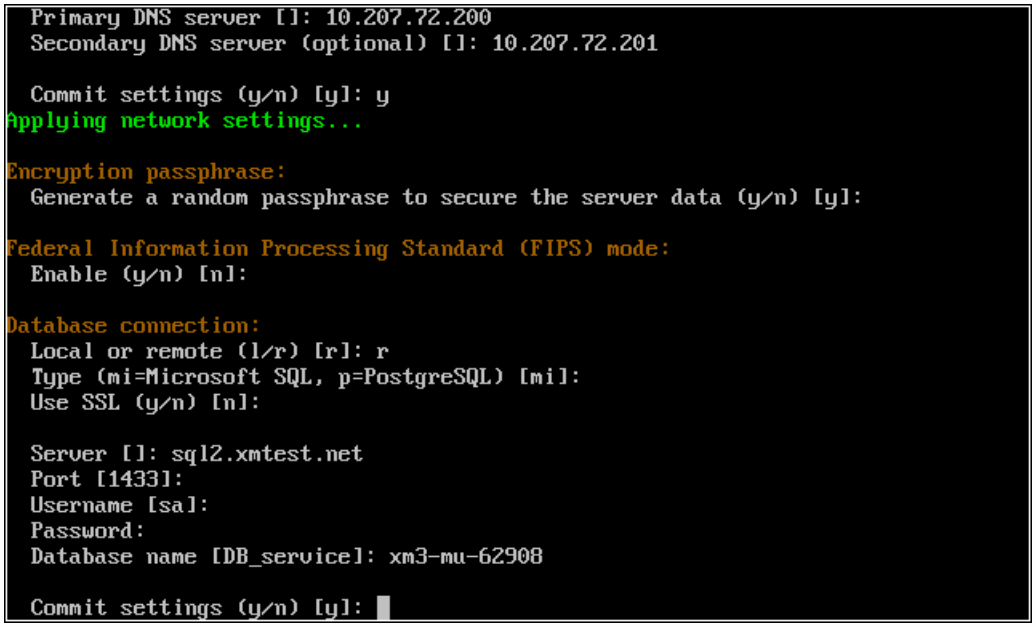
1. Dans l'interface de ligne de commande, tapez votre nom d'utilisateur et votre mot de passe d'administrateur, puis entrez vos paramètres réseau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



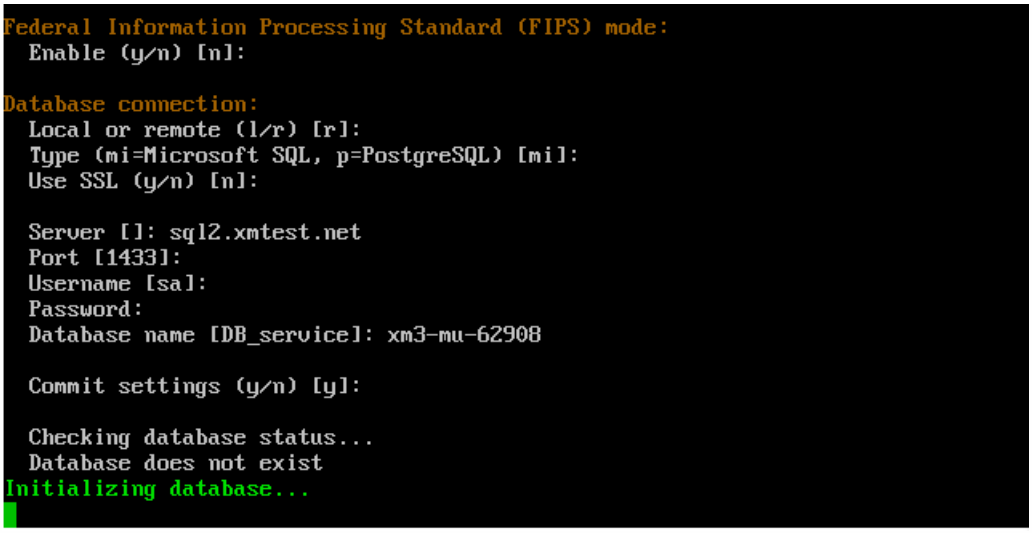
2. Tapez **y** pour valider les paramètres.

3. 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.



4. Tapez **y** pour valider les paramètres.XenMobile initialise la base de données.

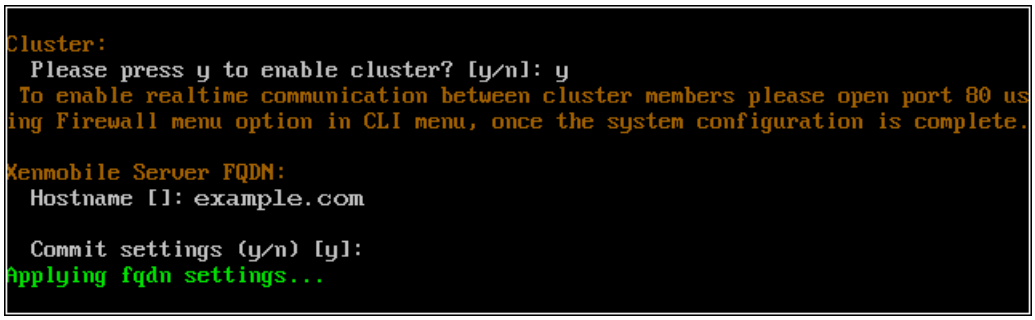
© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. 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.

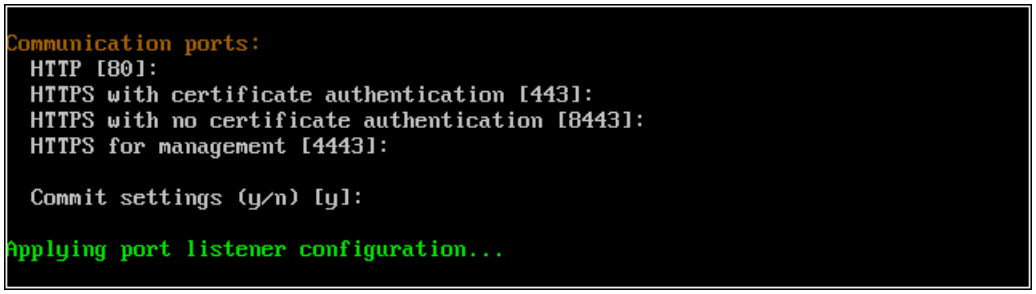
> ## Important
>
> Les noms de domaine complets pour les environnements 9.0 et 10.1 doivent correspondre.



6. Tapez **y** pour valider les paramètres.

7. Définissez les ports de communication.

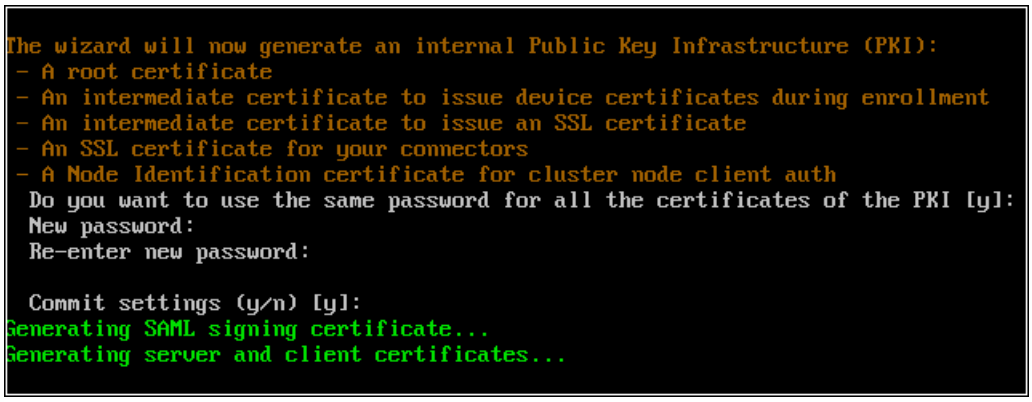
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Après avoir défini les ports, une invite s'affiche pour le nom de l'instance Device Manager qui indique : si vous effectuez une mise à niveau à partir d'une version précédente, le nom doit correspondre au nom configuré précédemment. Veuillez noter que les installations par défaut utilisent le nom *zdm*. Si le nom par défaut a été modifié, vous devez entrer le nouveau nom.

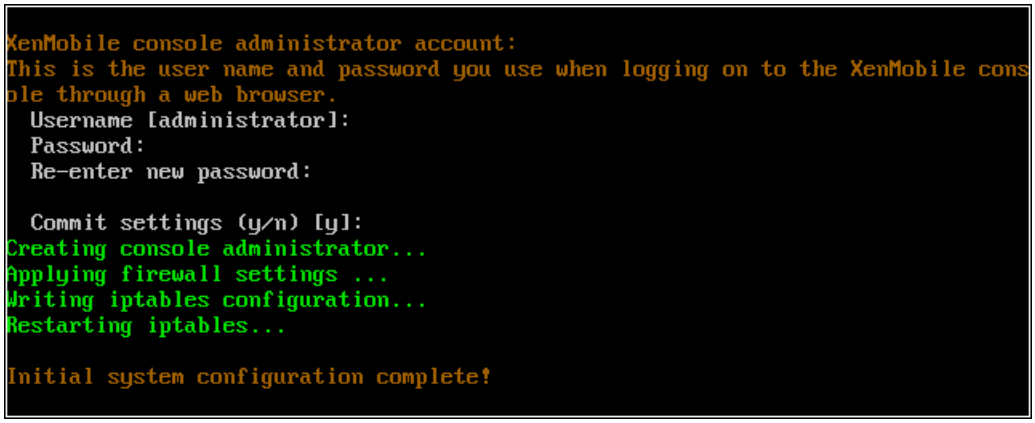
8. Tapez **y** pour valider les paramètres.

9. Tapez le mot de passe à utiliser pour les certificats, puis sélectionnez s'il faut utiliser le même mot de passe pour tous les certificats.



10. Tapez **y** pour valider les paramètres.

11. Entrez le nom d'utilisateur et le mot de passe de l'administrateur de la console de XenMobile.

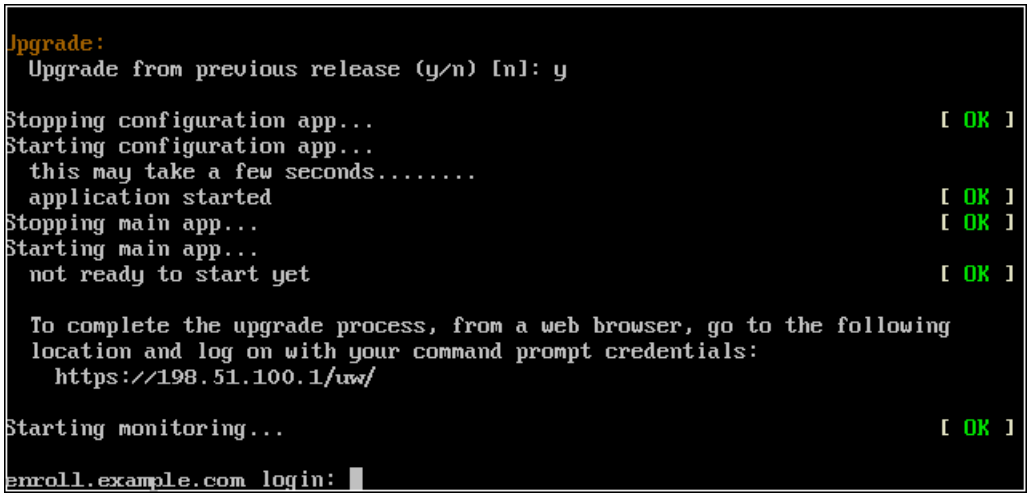


12. Tapez **y** pour valider les paramètres.

13. Tapez **y** pour mettre à niveau. **Remarque :** si vous ne tapez pas y ici, vous devez configurer une nouvelle instance de

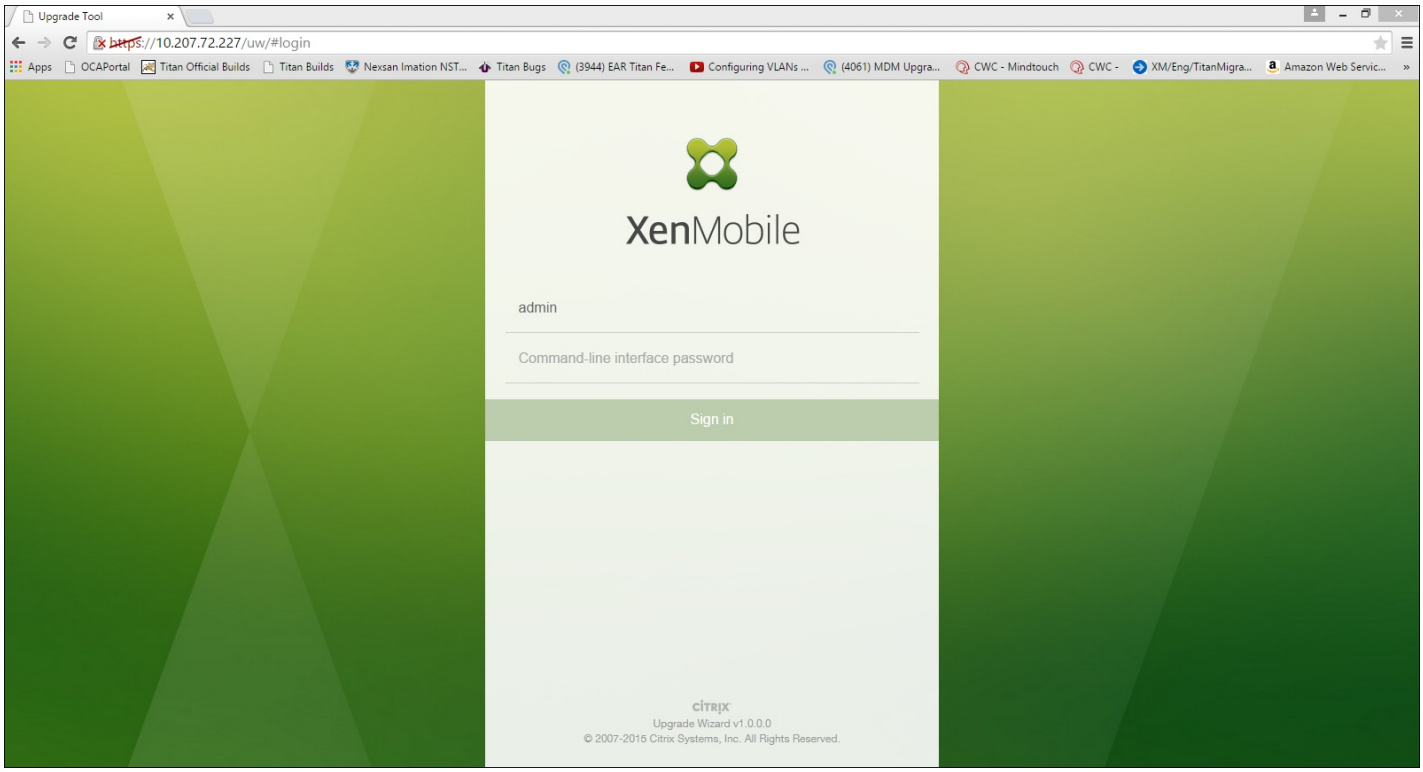
 © 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 10.1 dans la console de ligne de commande et démarrer l'outil de mise à niveau.



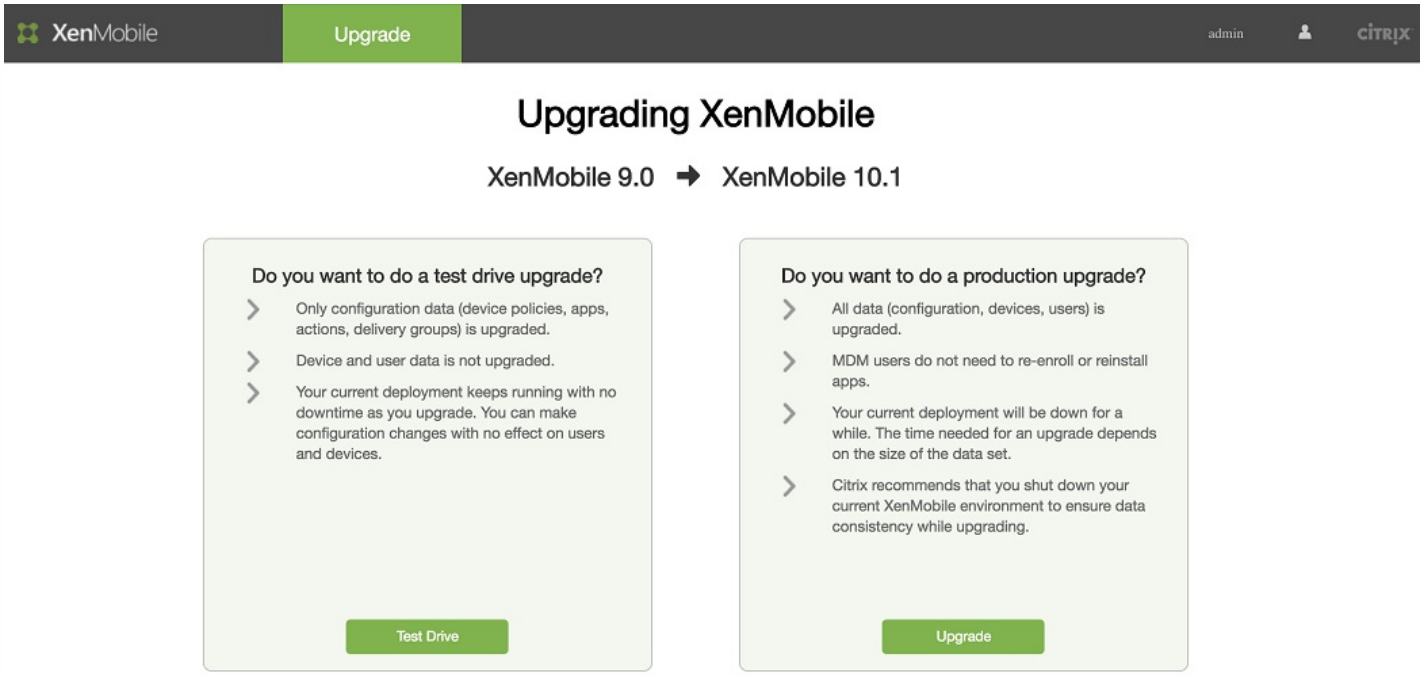
XenMobile 10.1 active l'outil de mise à niveau à usage unique.

14. Accédez à l'outil de mise à niveau dans un navigateur Web à l'adresse https:///uw/.

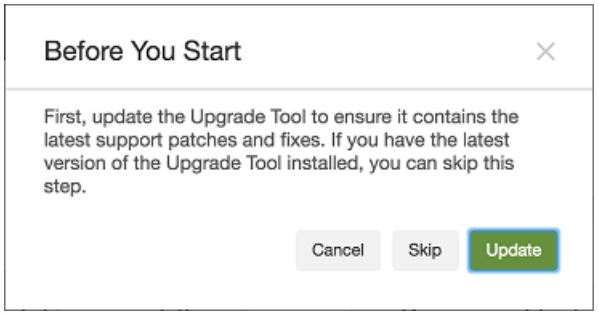


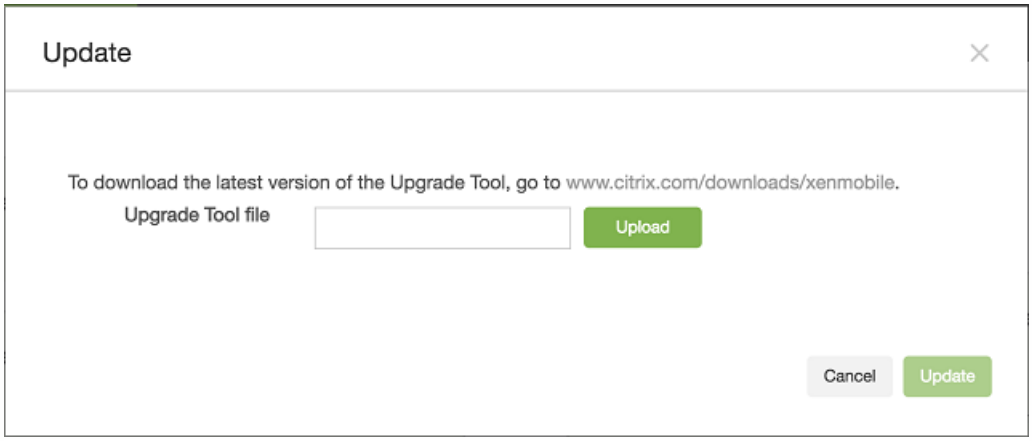
15. Vous pouvez maintenant choisir entre un environnement de test et une mise à niveau de l'environnement de production. Ces instructions font référence à la mise à niveau d'un environnement de production. Dans la page **Upgrading XenMobile**, cliquez sur **Upgrade**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



16. Dans la boîte de dialogue **Before You Start**, cliquez sur **Update**, et utilisez la boîte de dialogue **Update** pour installer la dernière version de l'outil.





Une fois que vous avez mis à jour l'outil, l'outil redémarre votre système.

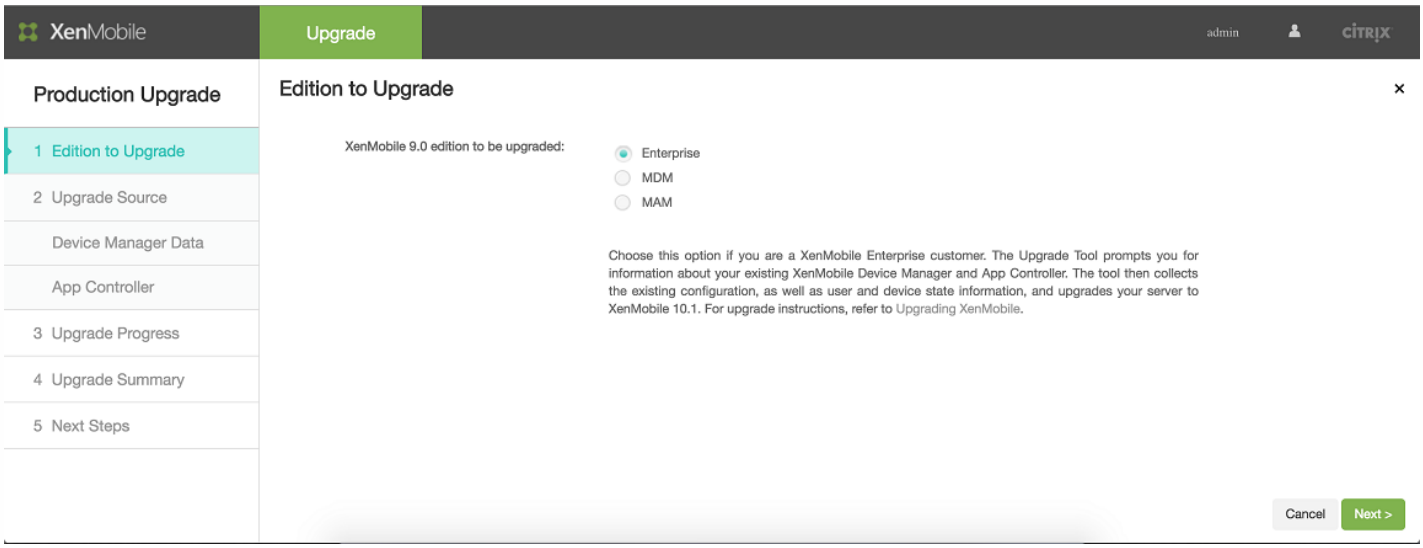
17. Avant de continuer, effacez le cache de votre navigateur et entrez de nouveau l'adresse URL pour accéder à l'outil de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

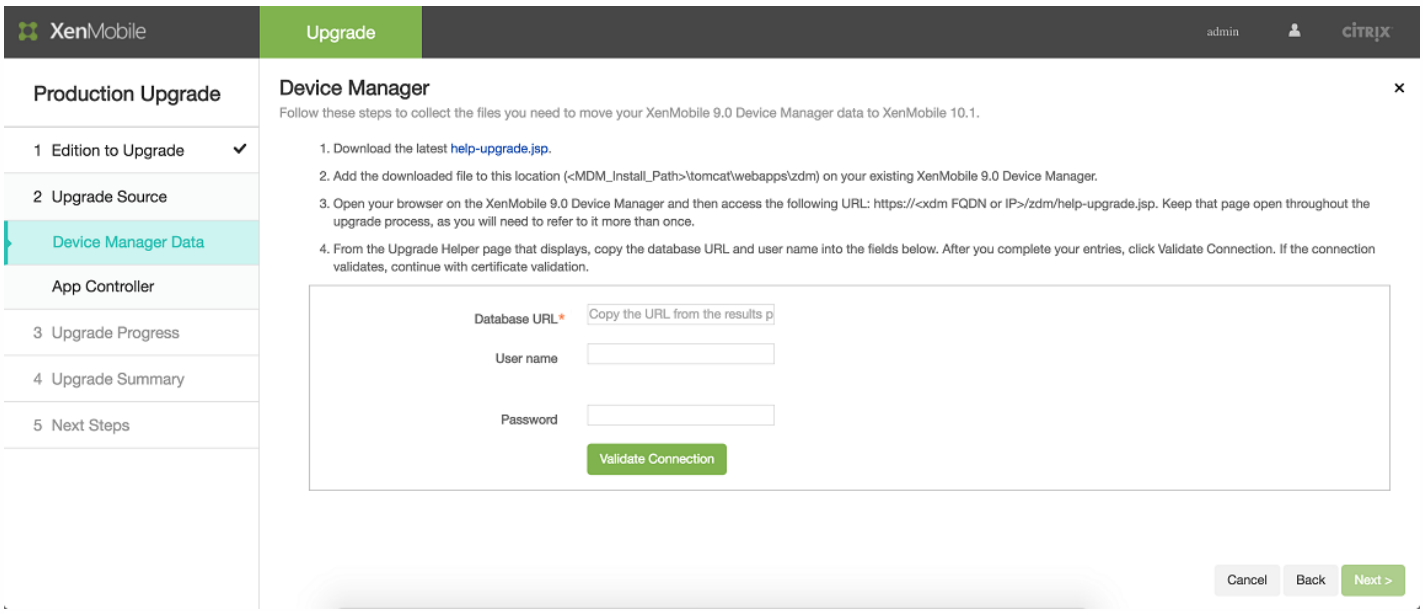
mise à niveau (https:///uw/).

18. Dans la page **Upgrading XenMobile**, cliquez sur **Upgrade**. Dans la boîte de dialogue **Before You Start**, cliquez sur **Skip**.

19. Dans la page **Edition to Upgrade** , sélectionnez votre édition. Dans cet exemple, l'édition sélectionnée est **Enterprise**.



20. Cliquez sur **Suivant**.



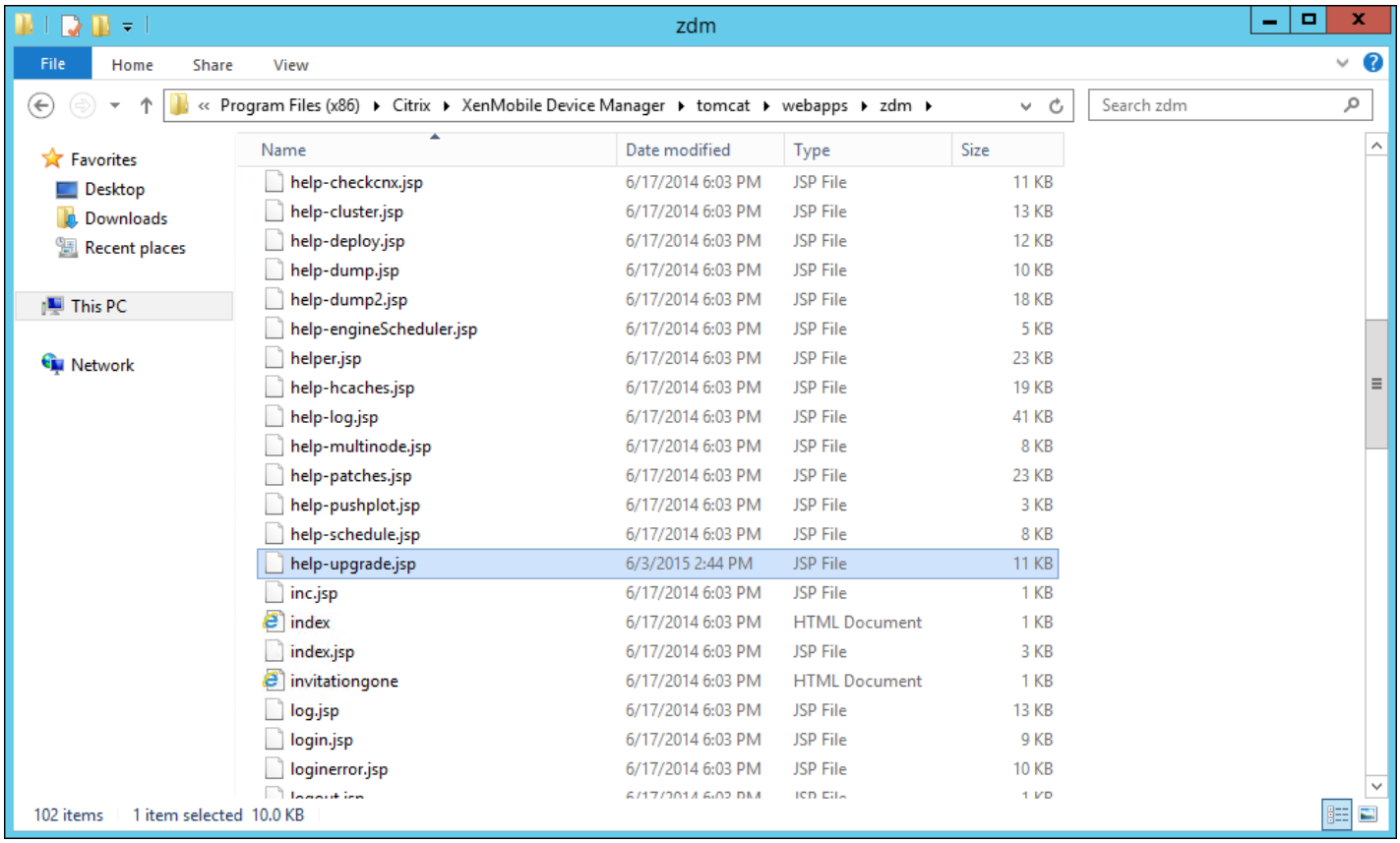
La page de **Device Manager** s'affiche pour les migrations de XenMobile Enterprise Edition. Cette étape n'est pas nécessaire pour les migrations MAM. Si vous effectuez une migration MAM, la page Update App Controller s'affiche ; ignorez les instructions jusqu'à l'étape 24 pour mettre à jour App Controller.

21. Suivez ces instructions pour collecter 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

a. Cliquez sur le lien dans l'étape 1 de la page de **Device Manager**, puis enregistrez le fichier téléchargé help-upgrade.zip.

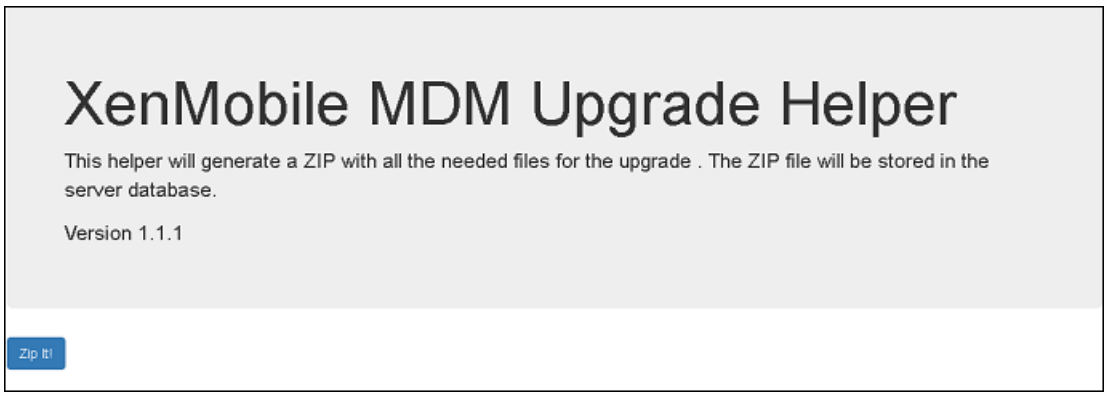
b. Extrayez le fichier help-upgrade.jsp dans \tomcat\webapps\zdm sur votre XenMobile 9.0 Device Manager existant.



c. Dans une fenêtre de navigateur, connectez-vous au serveur XenMobile 9.0.

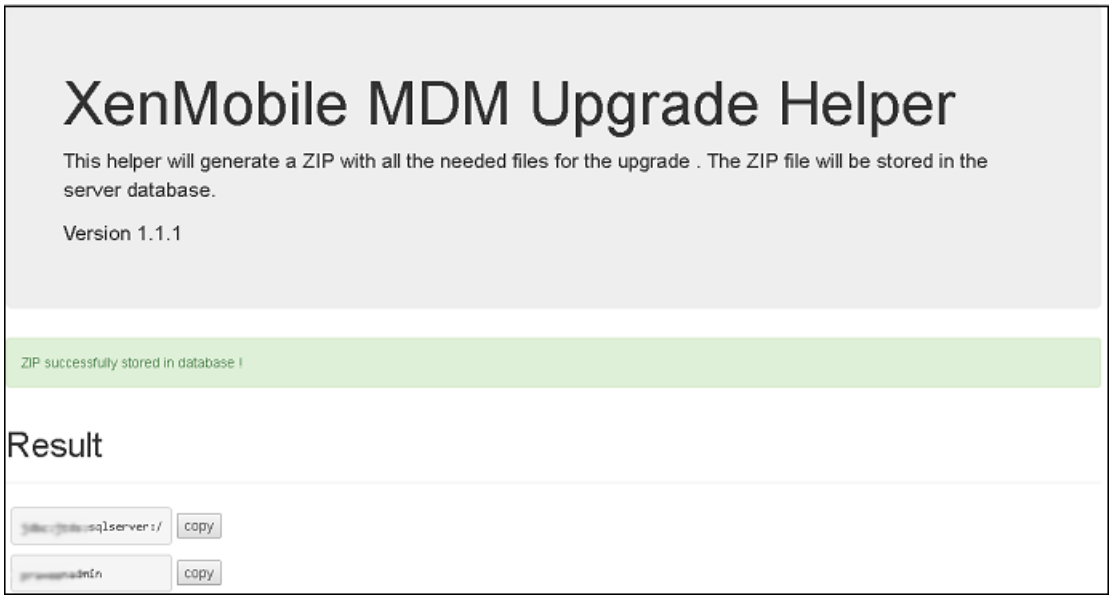
d. Dans un onglet de navigateur distinct, entrez cette URL : https://localhost/zdm/help-upgrade.jsp. Cette entrée ouvre la page **XenMobile MDM Upgrade Helper**, qui collecte et compresse tous les fichiers de XenMobile 9.0 qui sont requis pour la mise à niveau vers XenMobile 10.1. Le fichier compressé est stocké dans la base de données du serveur à partir de laquelle il est extrait. Il se peut que vous deviez ouvrir une session sur la page help-upgrade.jsp.

e. Cliquez sur **Zip it** et suivez les instructions à l'écran pour collecter les fichiers requis pour la mise à niveau.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

22. 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**.



23. Dans l'outil de mise à niveau :

a. Entrez le mot de passe et cliquez sur **Validate Connection**.

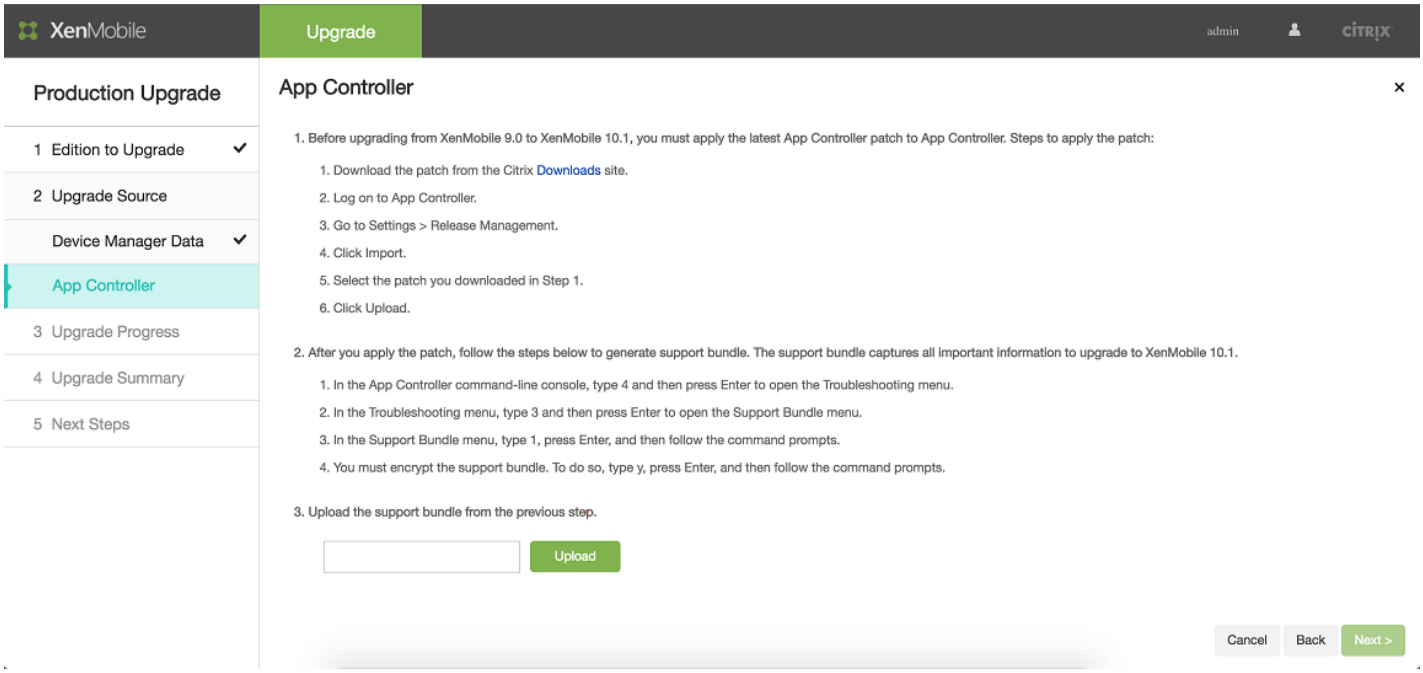
b. Entrez le mot de passe pour chaque certificat et cliquez sur **Validate Password**.

c. Cliquez sur **Next**.

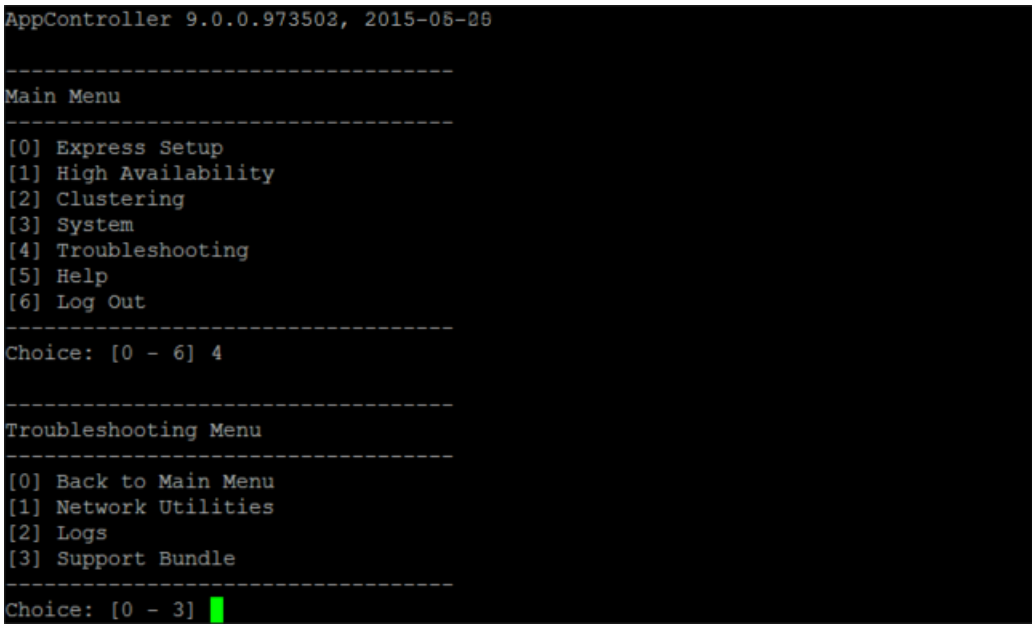
24. Si vous avez changé le fichier ew-config.properties, redémarrez le service xdm sur XenMobile 9 MDM et accédez à https://localhost/zdm/help-upgrade.jsp pour exécuter de nouveau le fichier zip. Cela permet de relire le fichier ew-config.properties et de l'enregistrer dans la base de données XenMobile MDM 9 pour préparer la migration.

25. 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 page **App Controller** pour mettre à niveau App Controller. Suivez ensuite ces étapes pour créer un pack d'assistance :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

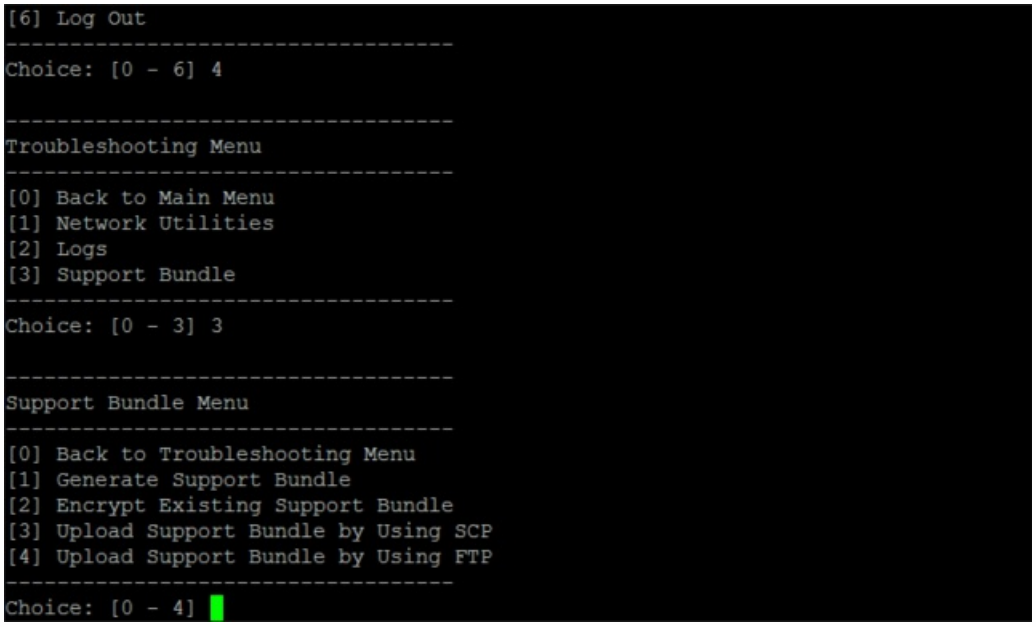


a. Dans la console de ligne de commande d'App Controller, tapez **4** , puis appuyez sur ENTRÉE pour ouvrir le menu Troubleshooting.

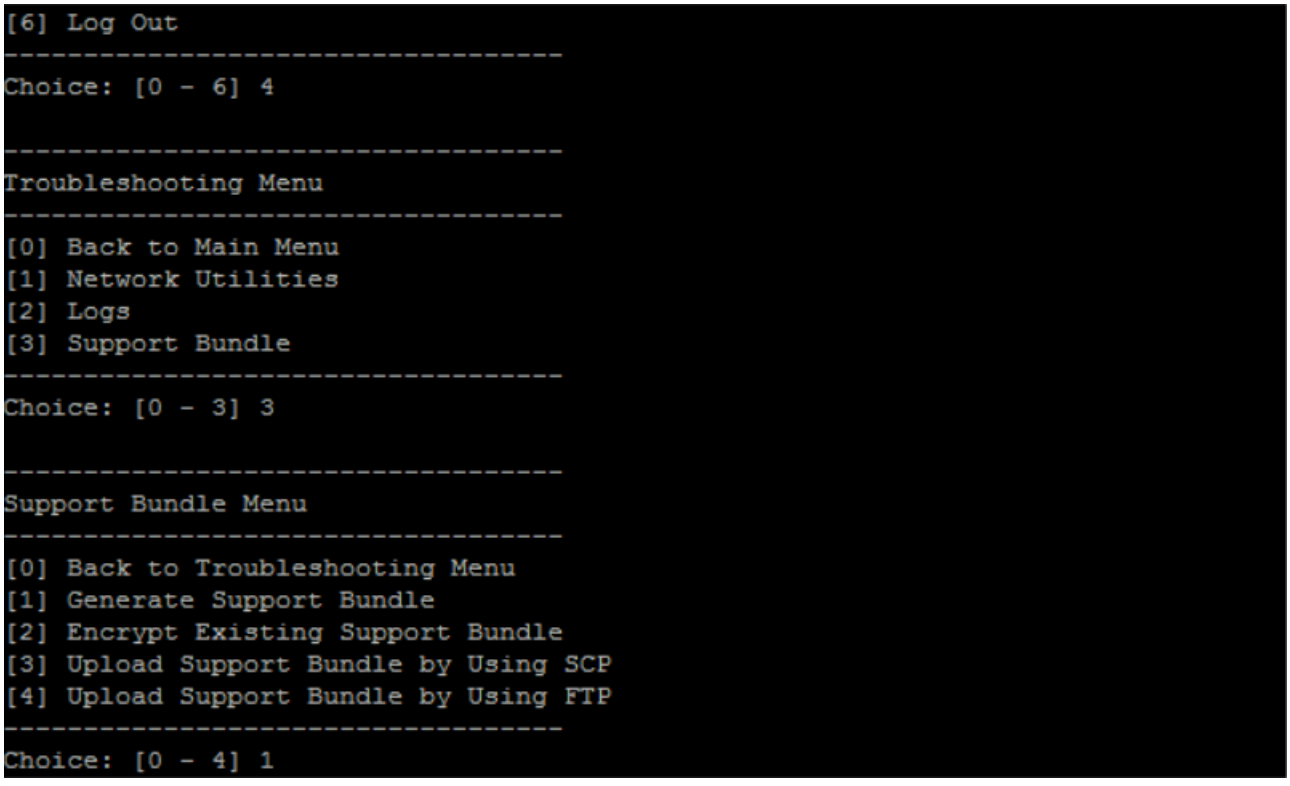


b. Dans le menu Troubleshooting, tapez **3**, puis appuyez sur ENTRÉE pour ouvrir le menu Support Bundle.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

d. Tapez **y**, appuyez sur ENTRÉE, puis suivez les invites de commande.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

---------------------------------
Support Bundle Menu
---------------------------------
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Encrypt Existing Support Bundle
[3] Upload Support Bundle by Using SCP
[4] Upload Support Bundle by Using FTP
---------------------------------
Choice: [0 - 4] 1
Do you want to encrypt the support bundle? [y/n] y

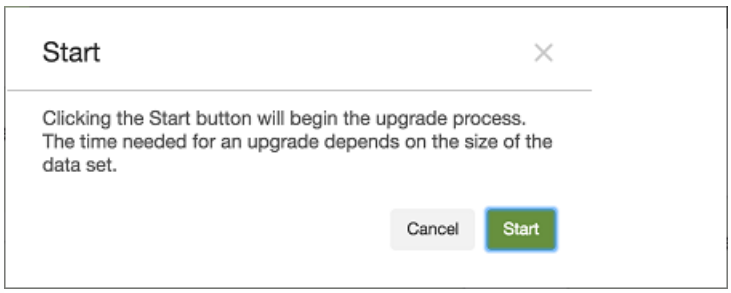
Please wait while AppController creates the support bundle.
```

e. Dans le menu Support Bundle, tapez **3**, puis appuyez sur ENTRÉE et suivez les invites de commande.

26. Dans la page **App Controller**, spécifiez le pack d'assistance, puis cliquez sur **Upload**.

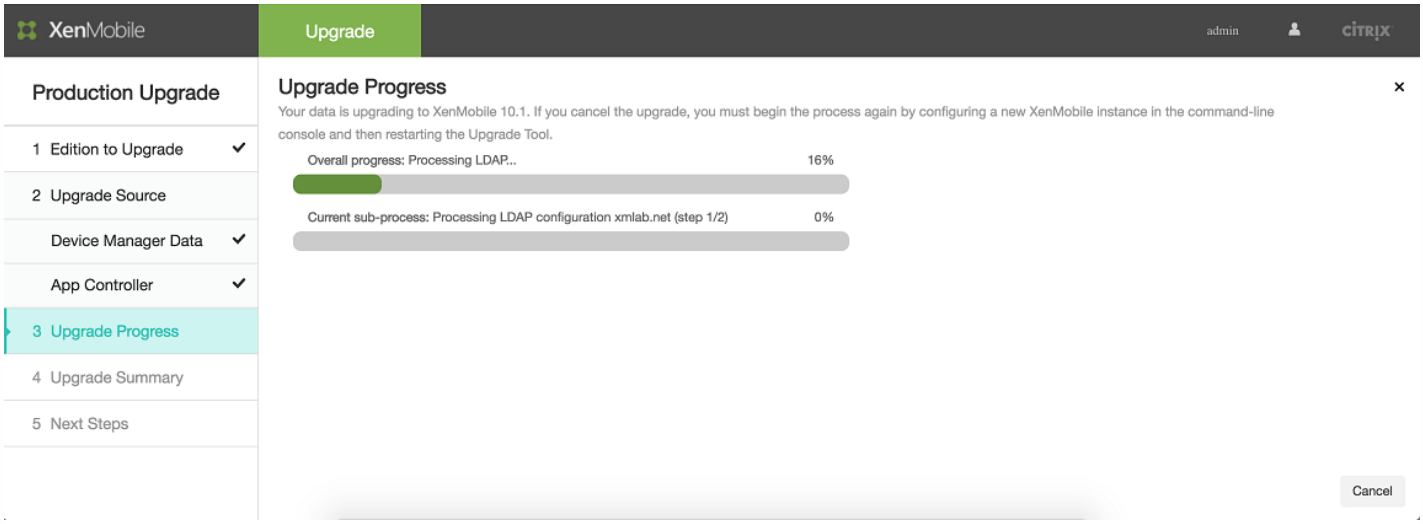
L'outil de mise à niveau traite les fichiers collectés (pour XenMobile Enterprise Edition) et le pack d'assistance. Cette étape peut prendre plus de 15 minutes si vous migrez un grand nombre d'utilisateurs.

27. Cliquez sur **Next**. La boîte de dialogue de confirmation **Start** s'affiche.



28. Cliquez sur **Start**. La page **Upgrade** 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.

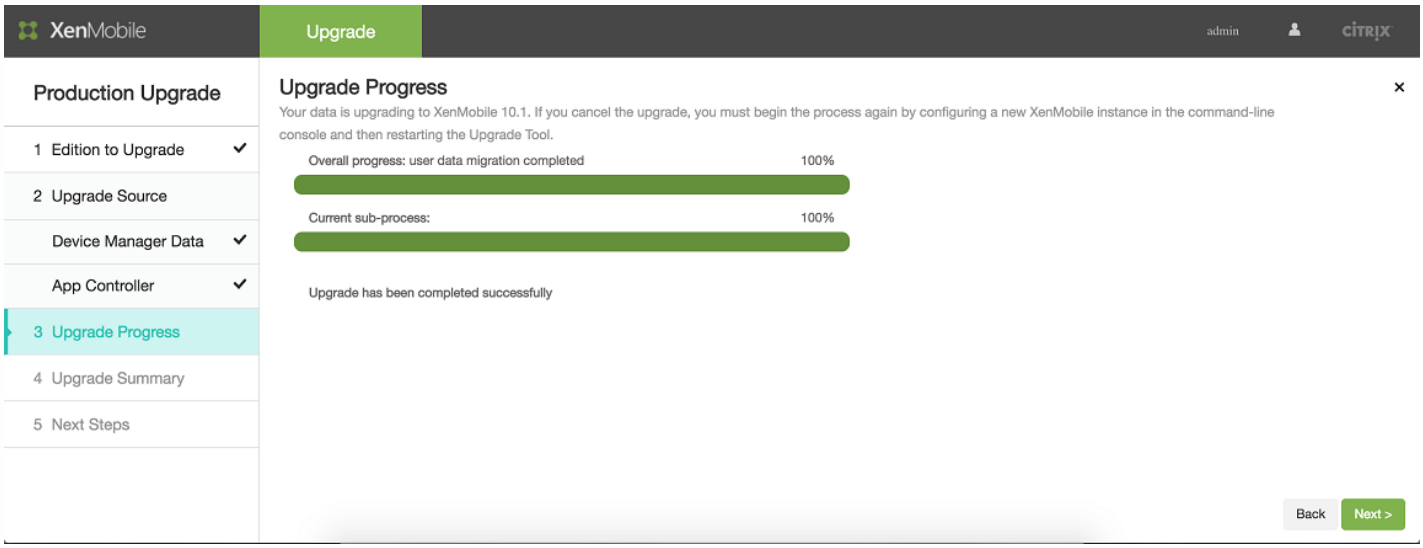
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Remarque

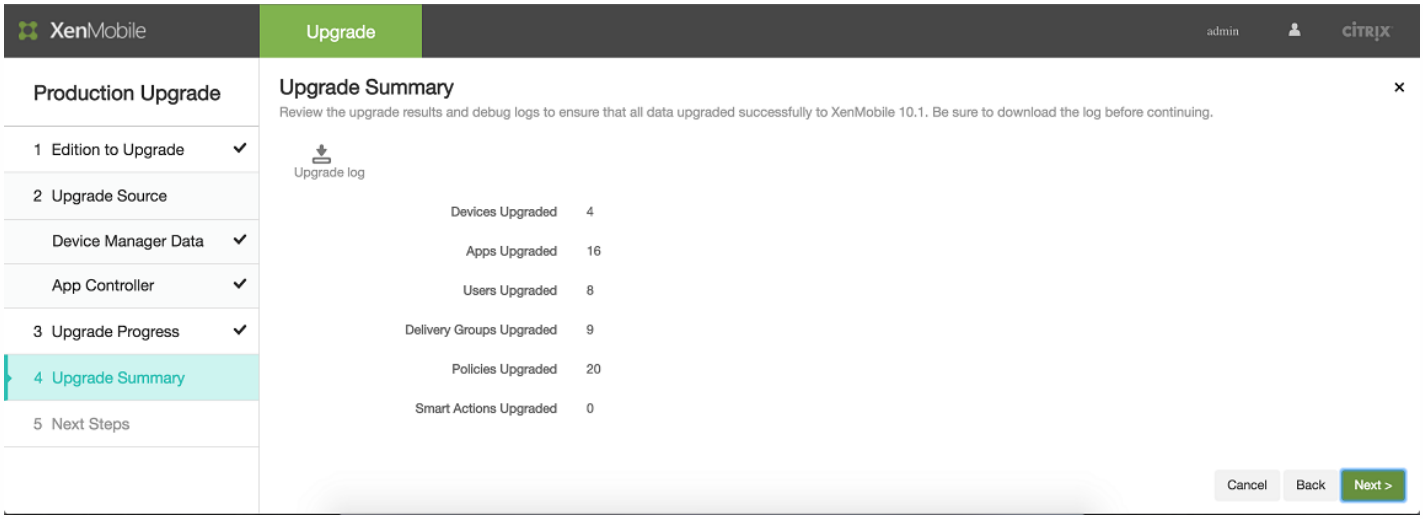
Si la mise à niveau échoue, vous pouvez afficher les journaux pour comprendre la raison de l'erreur. Ensuite, vous devez importer une nouvelle instance de XenMobile 10.1 et redémarrer le processus de mise à niveau. Vous ne pouvez pas utiliser le bouton **Précédent** du navigateur pour revenir sur les pages précédentes et corriger les informations.

La page Upgrade Progress vous indique quand la mise à niveau est terminée.



29. Cliquez sur **Next**. La page **Upgrade Summary** s'affiche.

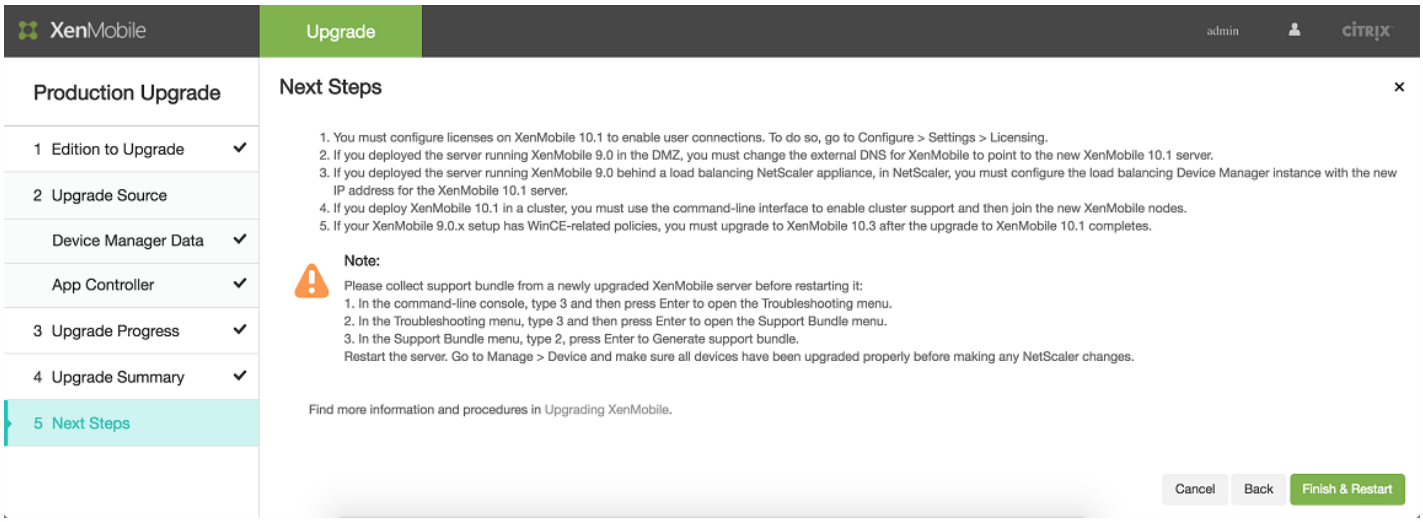
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 10.1.

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.

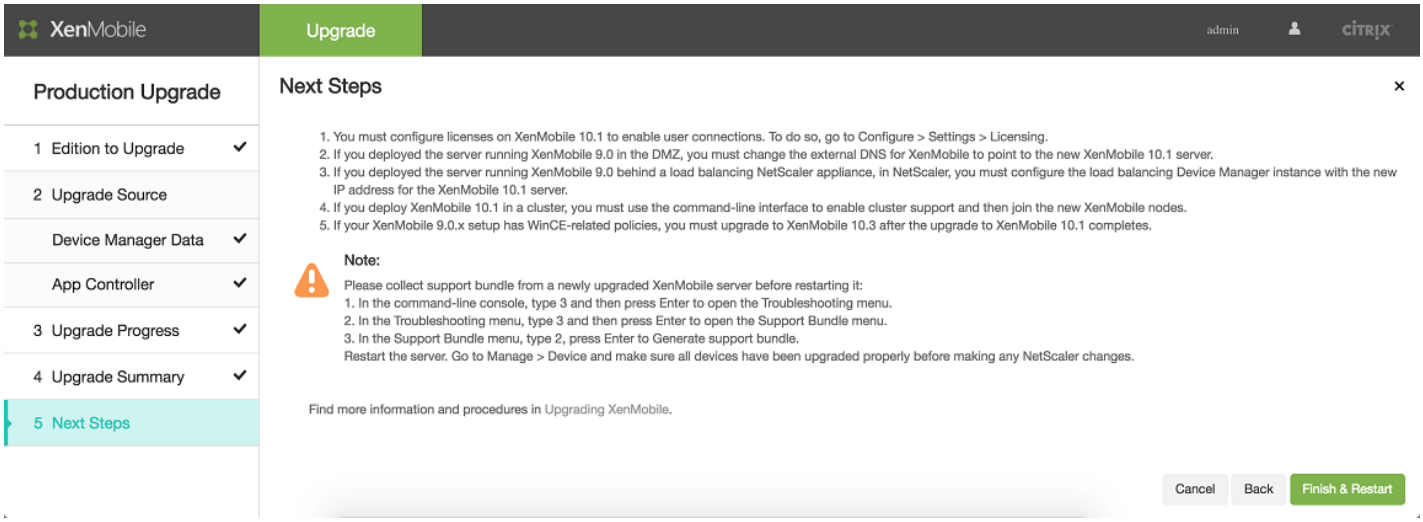
© 1999-2017 Citrix Systems, Inc. All rights reserved.

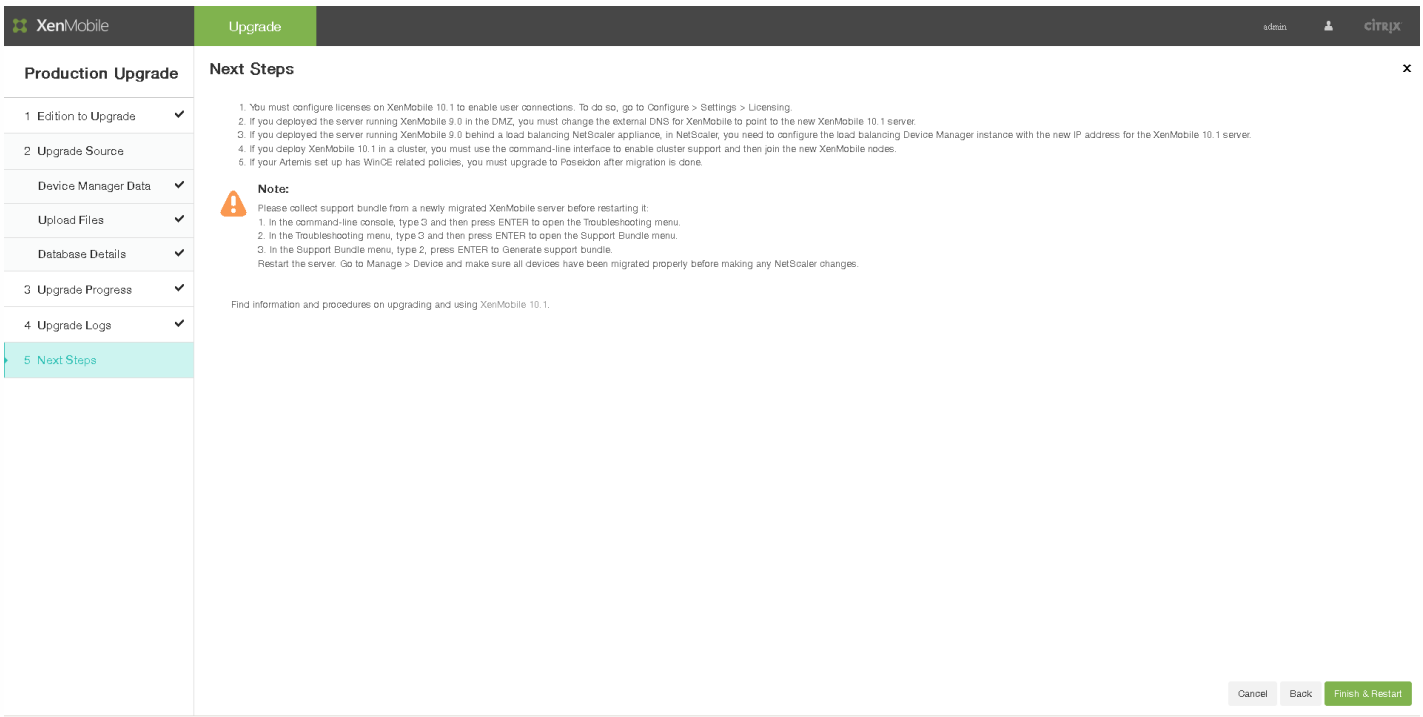
Post-requis de l'outil de mise à niveau

Oct 11, 2016

Après avoir effectué la mise à niveau, assurez-vous que vous avez effectué les post-requis suivants. Lorsque vous cliquez sur **Finish & Restart**, le serveur redémarre.

Remarque : ouvrez une session sur la console XenMobile à l'aide de https://:4443 avec vos informations d'identification d'administrateur de XenMobile 9.0 Device Manager. (Si vous avez effectué une mise à niveau de MAM, entrez vos informations d'identification d'administrateur de XenMobile 9.0 App Controller.)

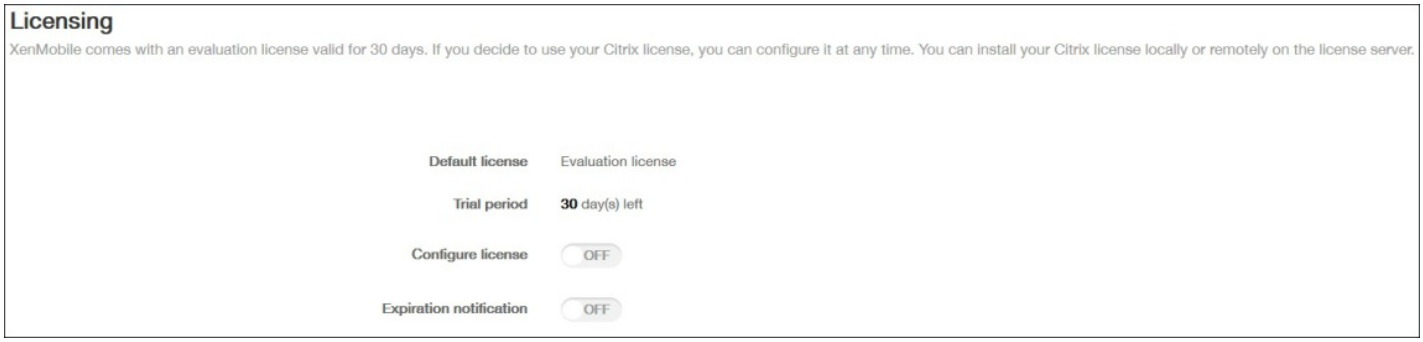




Système de licences

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 10.1 prend uniquement en charge le système de licences Citrix V6. Assurez-vous de définir la configuration de licence distante ou locale dans la console XenMobile, comme illustré dans la figure suivante, et téléchargez le fichier de licences sur Système de licences Citrix. Pour plus de détails, consultez la section Licences pour XenMobile.



Vous devez configurer des licences sur XenMobile 10.1 pour activer les connexions utilisateur. Pour ce faire, accédez à **Configuration** > **Paramètres** > **Gestion Licences**. Si vous utilisez un serveur autonome exécutant XenMobile 10.1, vous pouvez charger la licence dans la console XenMobile.

NetScaler

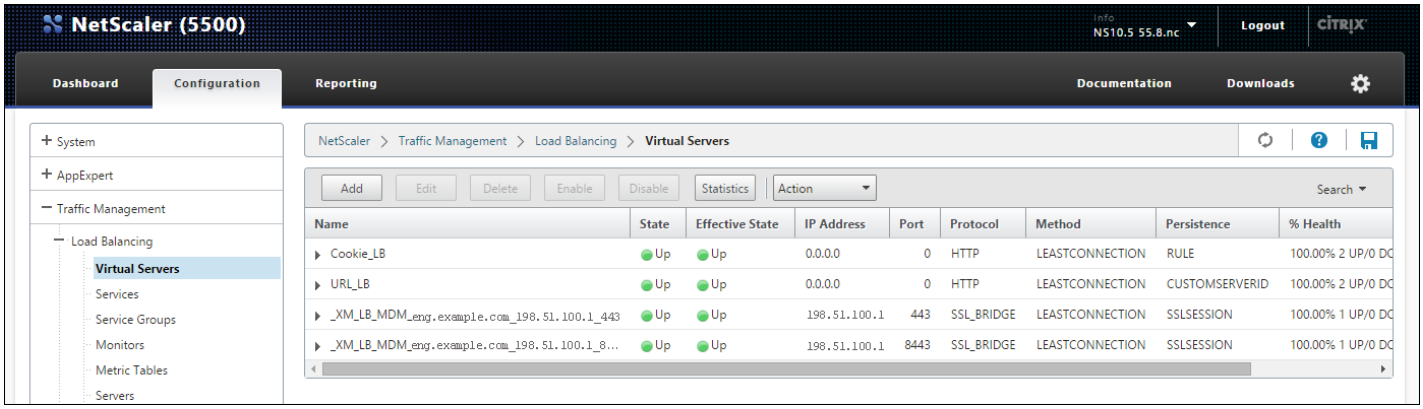
> ## Remarque
>
> Ce post-requis s'applique uniquement lorsque vous mettez à niveau une mise à niveau de production de XenMobile Enterprise Edition ; il ne concerne pas les mises à niveau de MAM ou MDM.

Les étapes à suivre dans NetScaler entraînent la création d'un nouveau serveur virtuel d'équilibrage de charge pour le nom de domaine complet de XenMobile 9.0 App Controller. Les principales étapes sont les suivantes :

1. Configurez un serveur virtuel d'équilibrage de charge pour la migration.
2. Créez une entrée hôte pour le nom de domaine complet d'App Controller qui pointe vers le nouveau serveur virtuel d'équilibrage de charge.
3. Changez NetScaler Gateway pour pointer vers le nouveau nom de domaine complet du serveur XenMobile : 8443.
4. Changez le serveur virtuel d'équilibrage de charge de Device Manager pour pointer vers la nouvelle adresse IP du serveur XenMobile.
5. Créez un nouveau serveur virtuel d'équilibrage de charge MAM basé sur un pont SSL ou une configuration MDM de déchargement SSL.
6. Créez une entrée hôte pour le nom de domaine complet du serveur XenMobile vers le nouveau serveur virtuel d'équilibrage de charge MAM.

1. Ouvrez une session sur NetScaler, puis cliquez sur **Traffic Management** > **Load Balancing** > **Virtual Servers**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Cliquez sur **Add**.

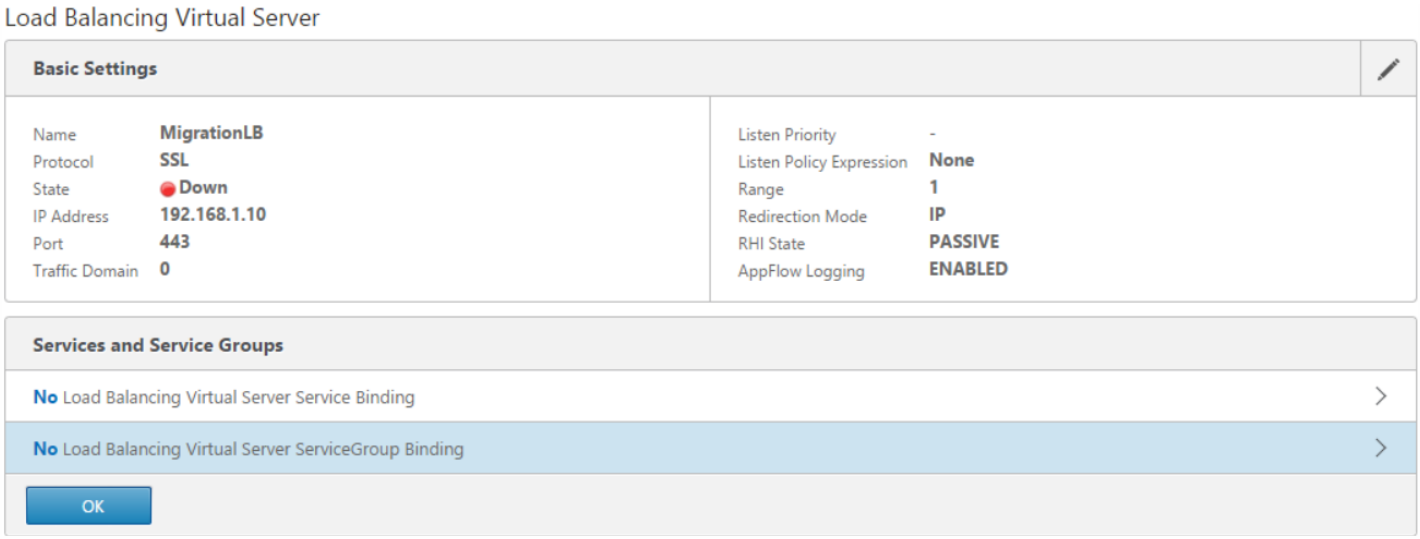
3. Sur la page **Load Balancing Virtual Server**, configurez les paramètres suivants, puis cliquez sur **OK**.



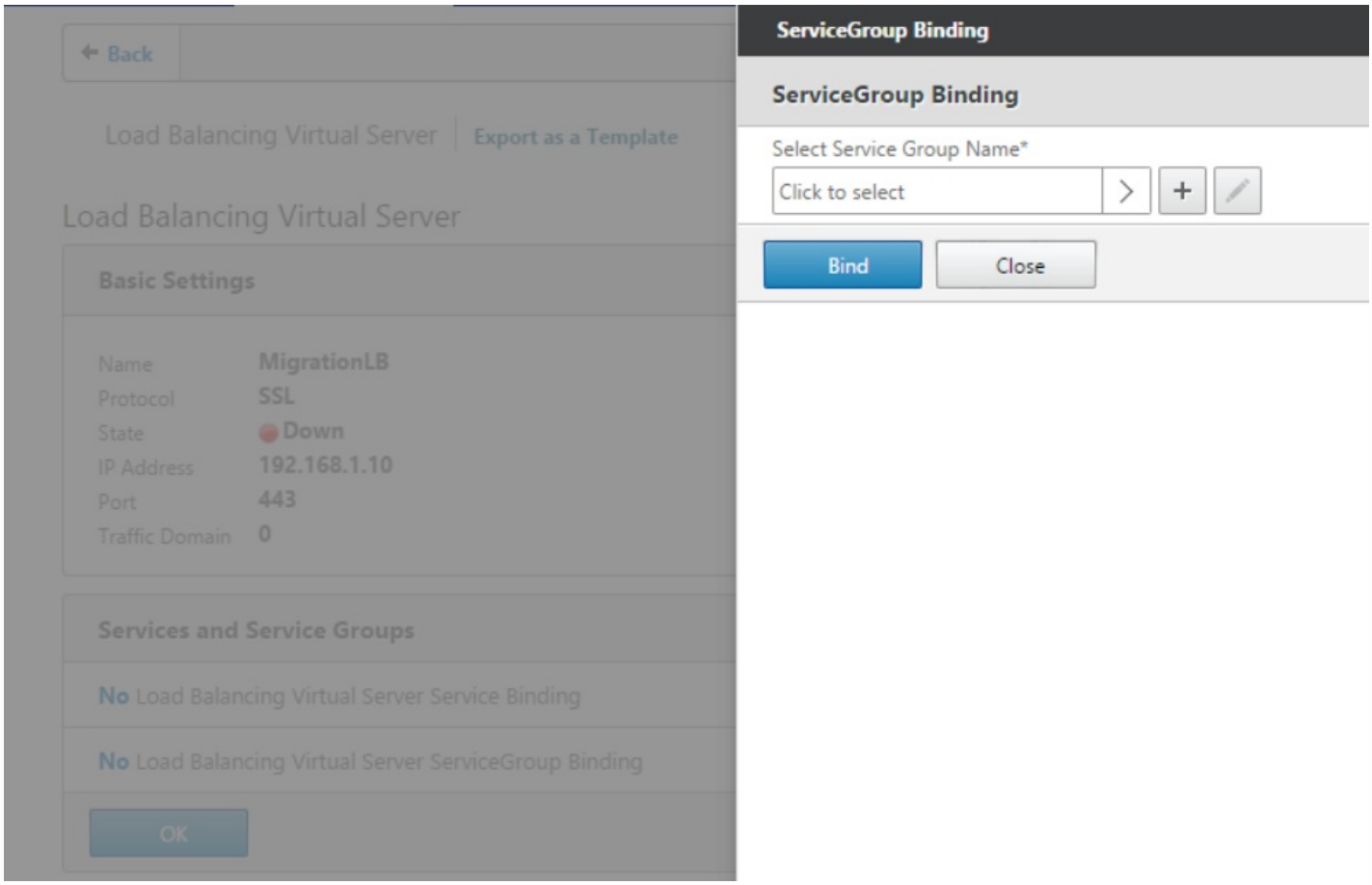
- **Name** : tapez un nom pour le nouvel équilibrage de charge.
- **Protocol** : doit être défini sur SSL. La valeur par défaut est HTTP.
- **IP Address** : entrez une adresse IP pour le nouvel équilibrage de charge, en respectant la norme RFC 1918 ; par exemple 192.168.1.10.
- **Port** : vérifiez que le numéro de port est 443.

4. Sous **Services and Service Groups**, cliquez sur **No Load Balancing Virtual Server Service Group Binding**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

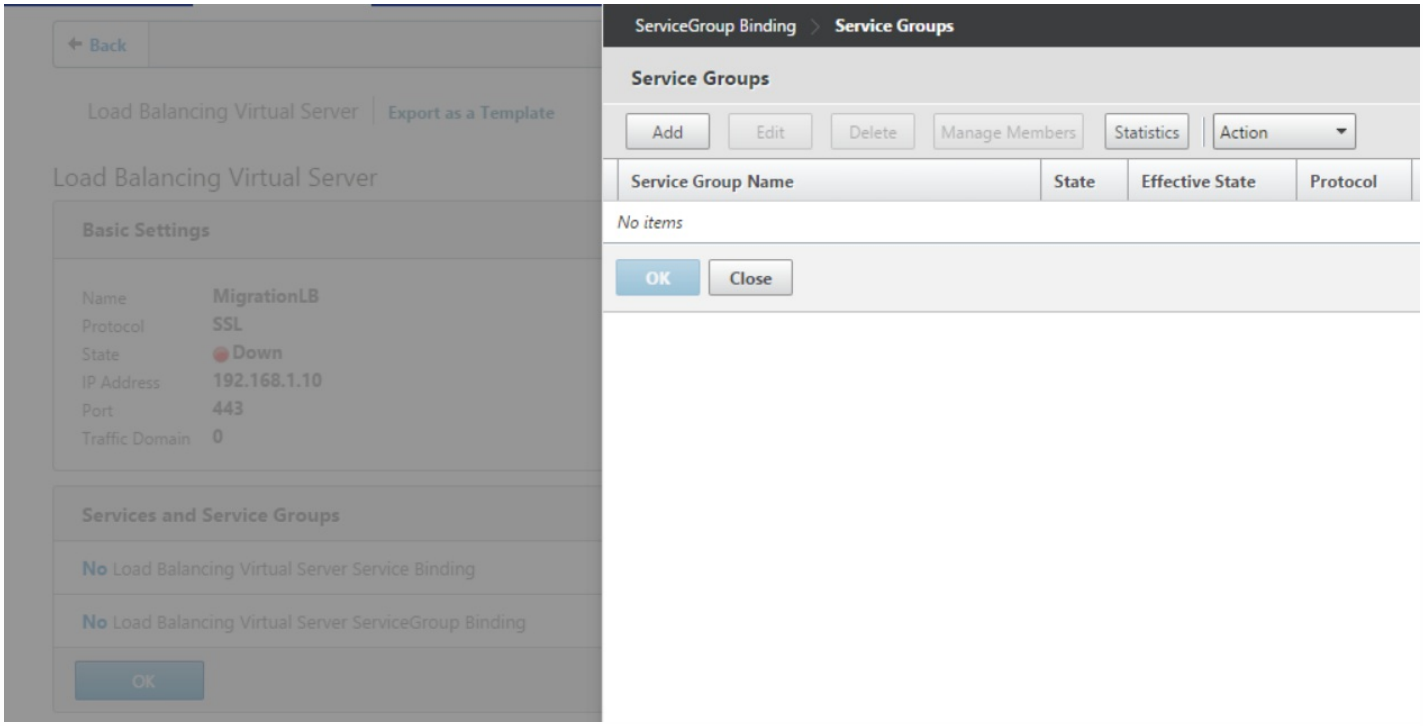


5. Sous **Select Service Group Name**, cliquez sur **Click to Select**.

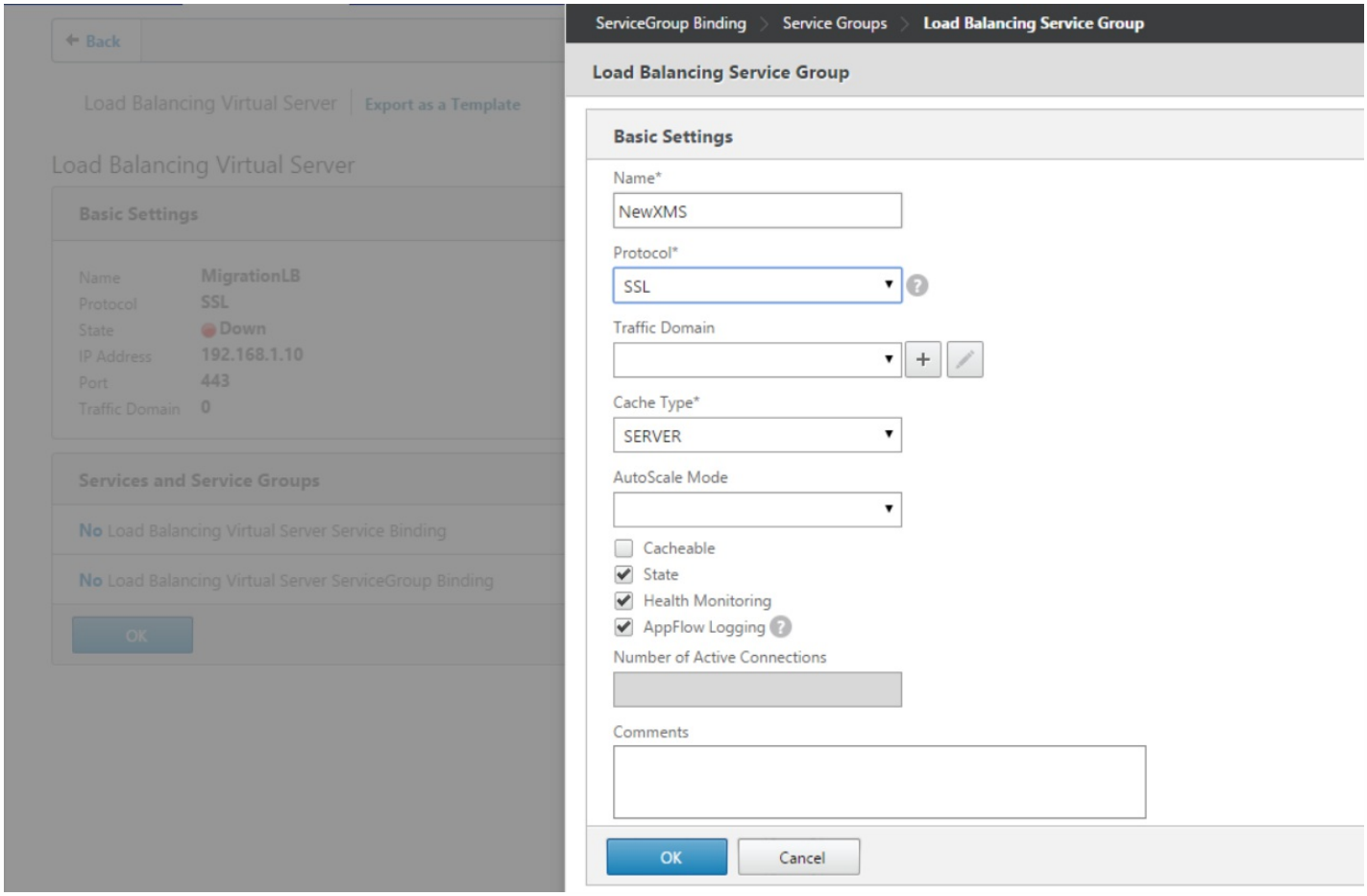


6. Cliquez sur **Add** pour créer un groupe de services.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

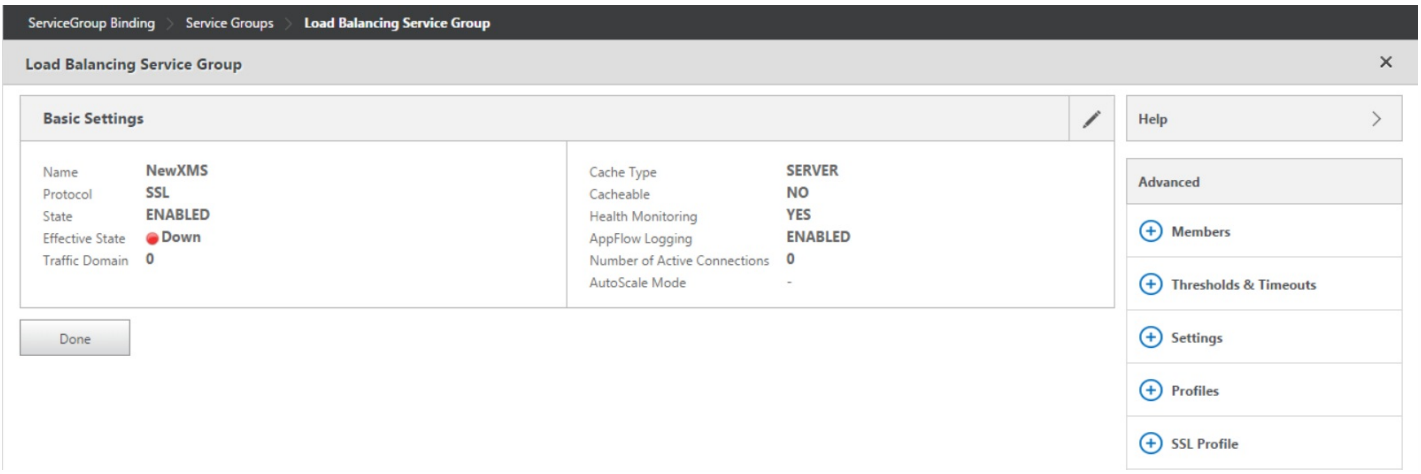


7. Sur la page **Load Balancing Service Group**, entrez un nom pour le nouveau groupe de services, vérifiez que le protocole est défini sur **SSL**, puis cliquez sur **OK**.

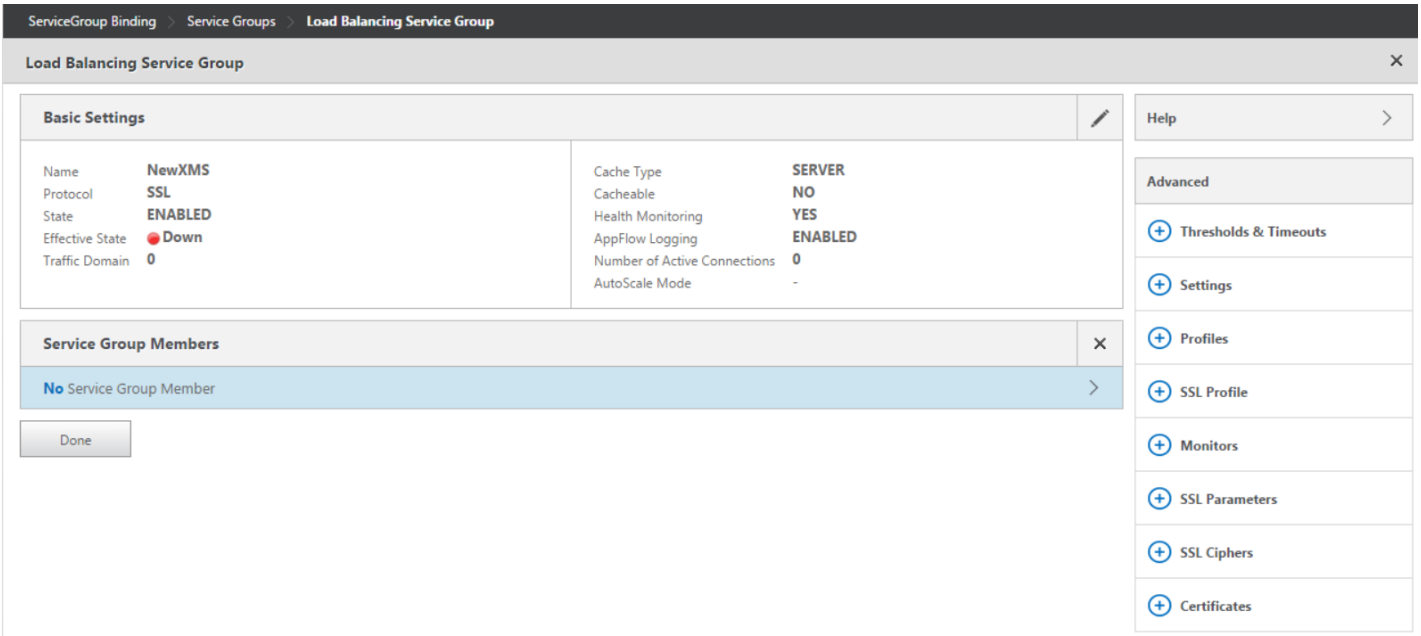


© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. Cliquez sur **Members**.



9. Cliquez sur l'entrée **No Service Group Member** mise en surbrillance.



10. Sur la page **Create Service Group Member**, configurez les paramètres suivants :

- **IP Address/IP Address Range*** : entrez l'adresse IP du serveur XenMobile 10.1.
- **Port** : définissez sur 8443.
- **Server ID** : si vous migrez d'un environnement XenMobile 9.0 en cluster vers un environnement XenMobile 10.1 en cluster, entrez l'ID du nœud de serveur (Server Node ID) du serveur XenMobile actuel.

> ## Remarque
>
> Vous pouvez obtenir l'ID du nœud de serveur en vous connectant à l'interface de ligne de commande du serveur XenMobile 10.1 et en tapant 1 pour accéder au menu Clustering. L'ID du nœud de serveur est appelé ID du nœud actuel (Current Node ID).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

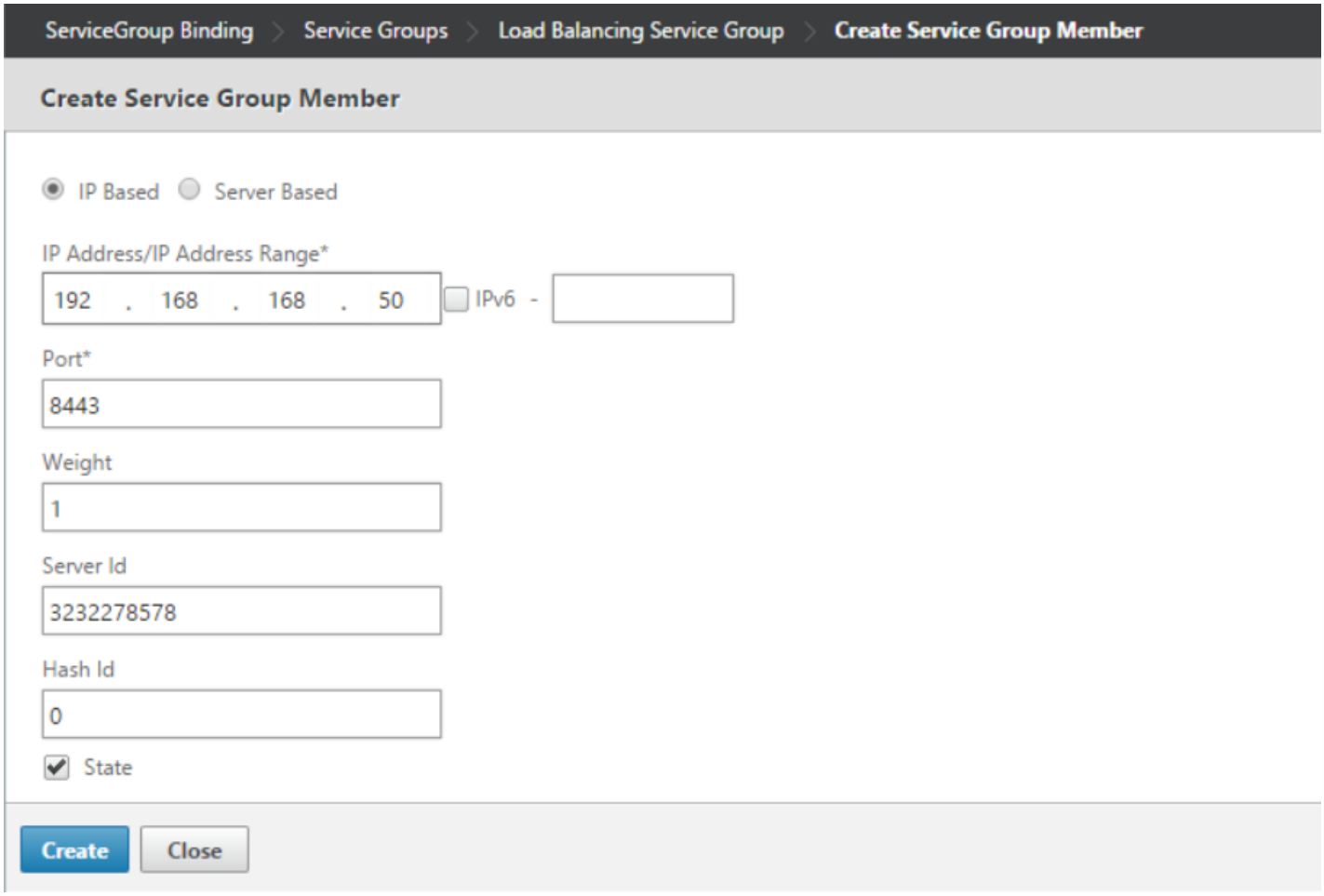
```
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
---------------------------------
Choice: [0 - 5] 1

Current Node ID: 181356771

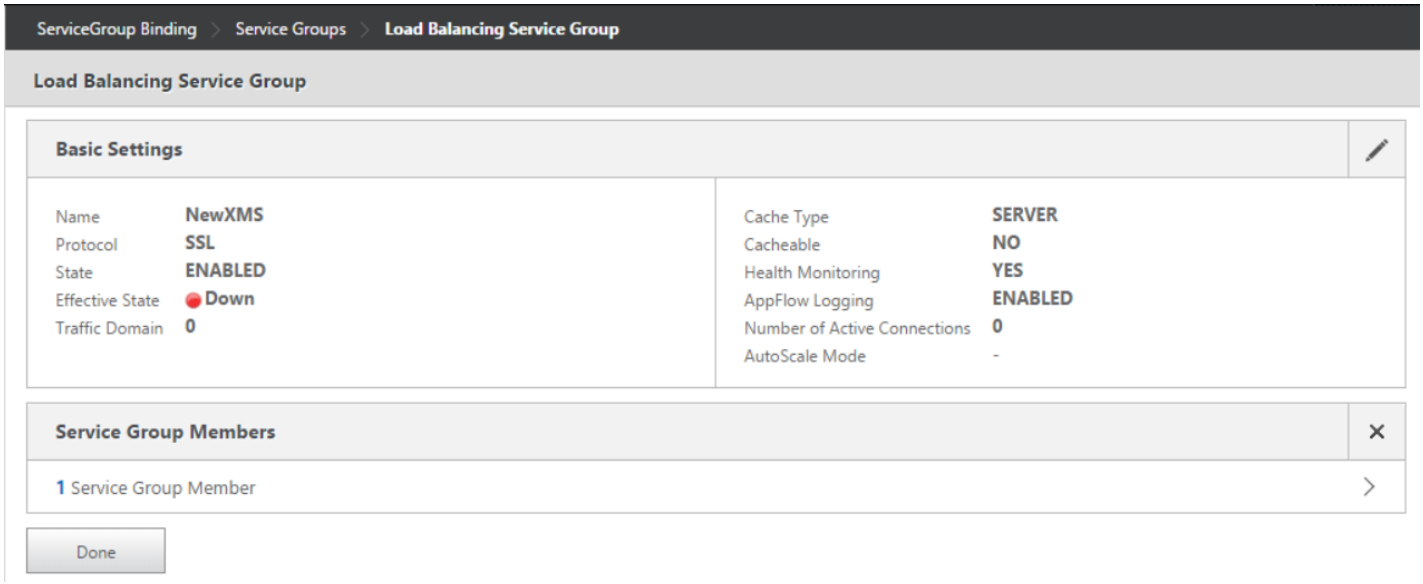
Cluster Members:
node: 192.0.2.0 status: ACTIVE  role: OLDEST


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

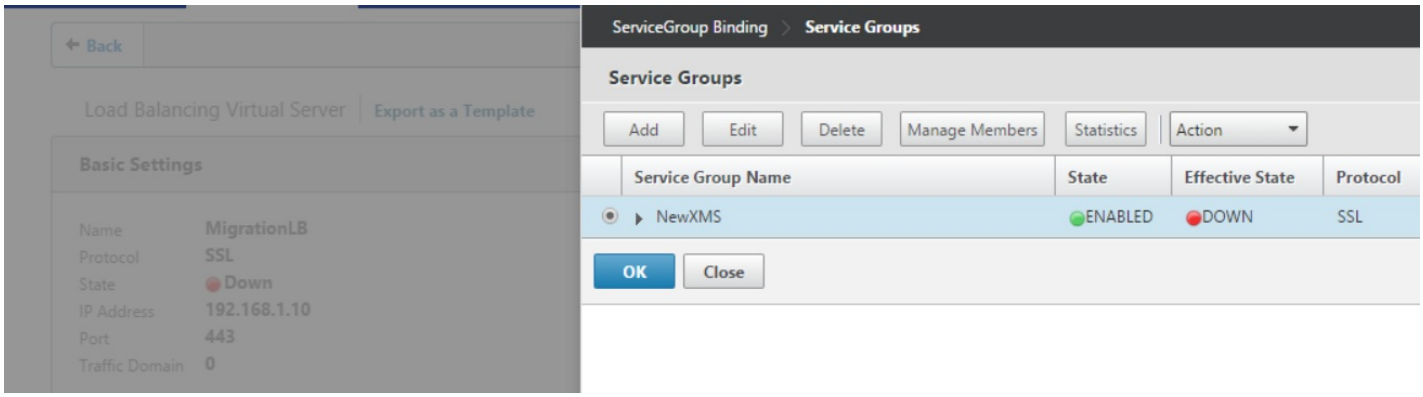
11. Cliquez sur **Create**, puis cliquez sur **Done**.



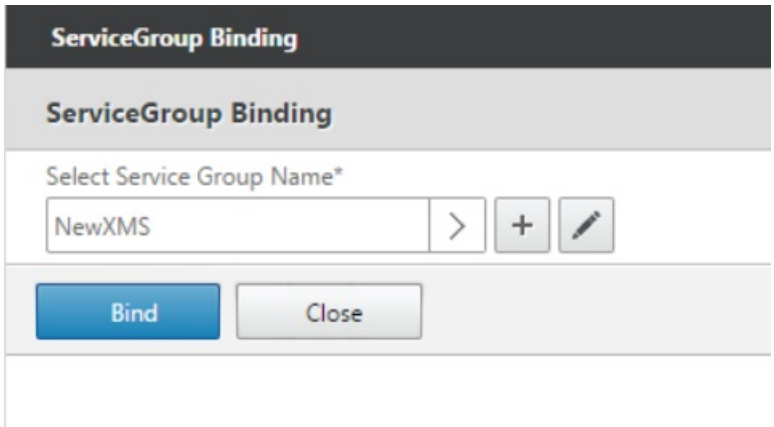
© 1999-2017 Citrix Systems, Inc. All rights reserved.



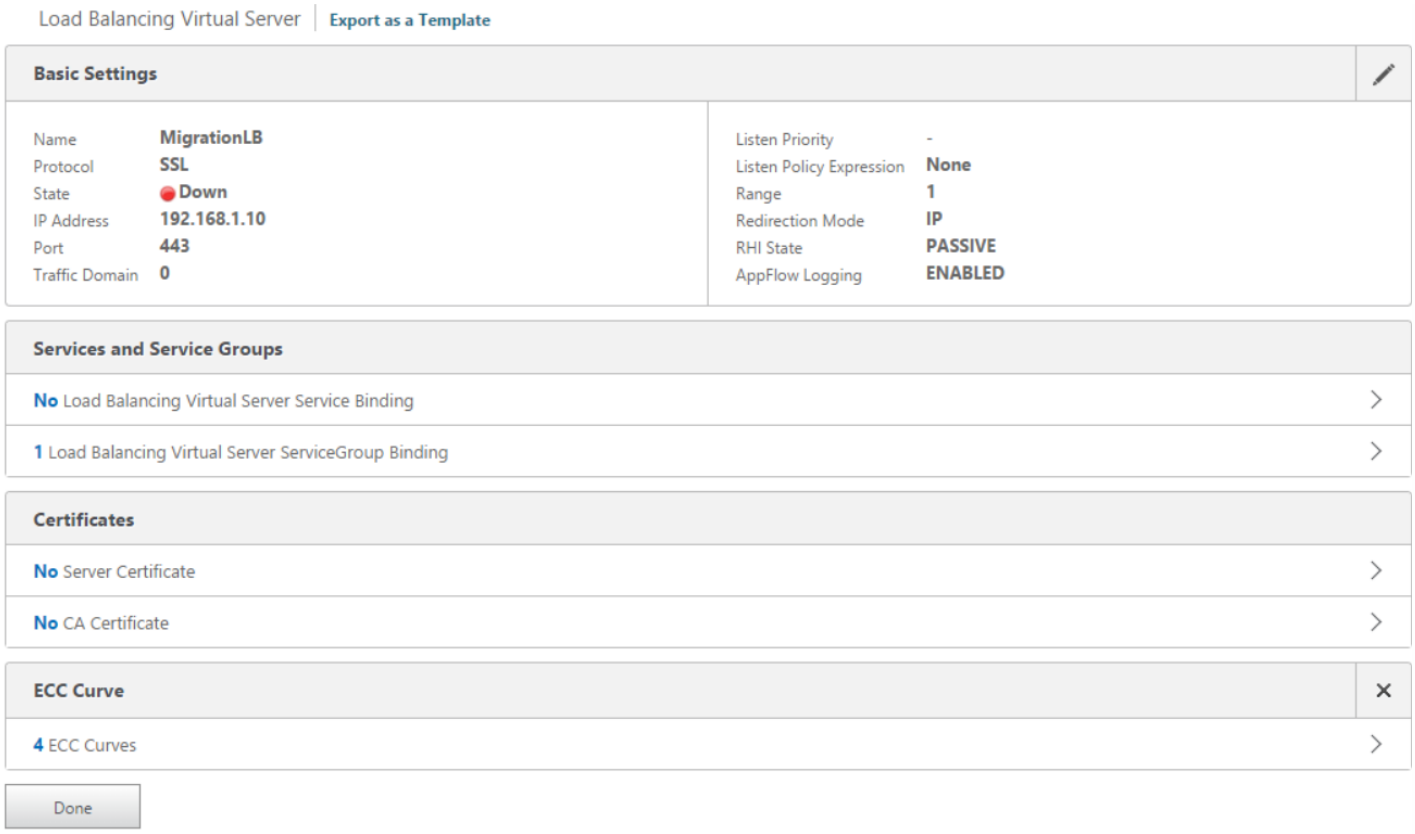
12. Cliquez sur **OK**.



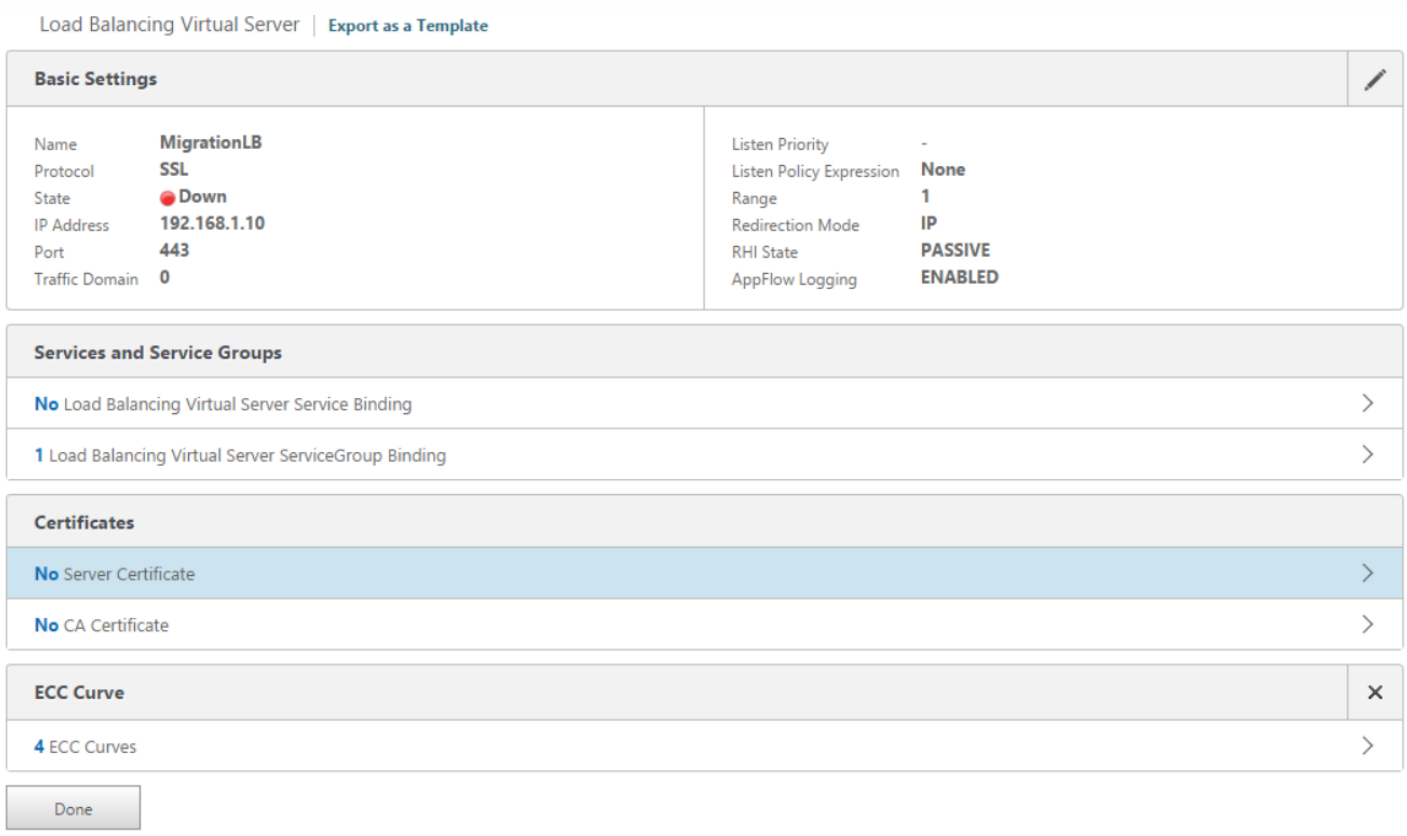
13. Cliquez sur **Bind**, puis sur l'écran suivant, cliquez sur **Done**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

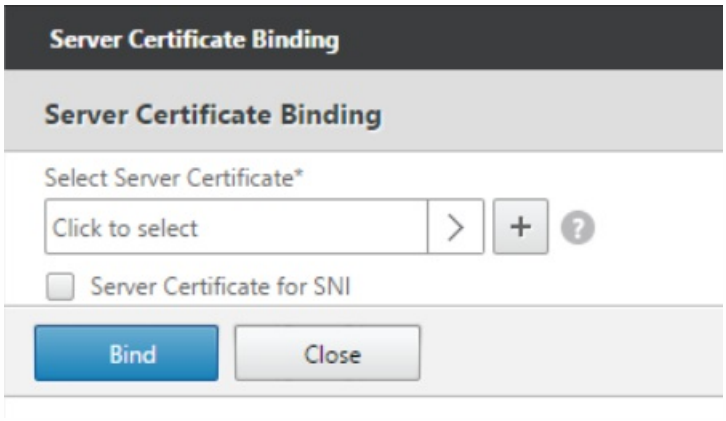


14. Sous **Certificates**, cliquez sur **No Server Certificate**.

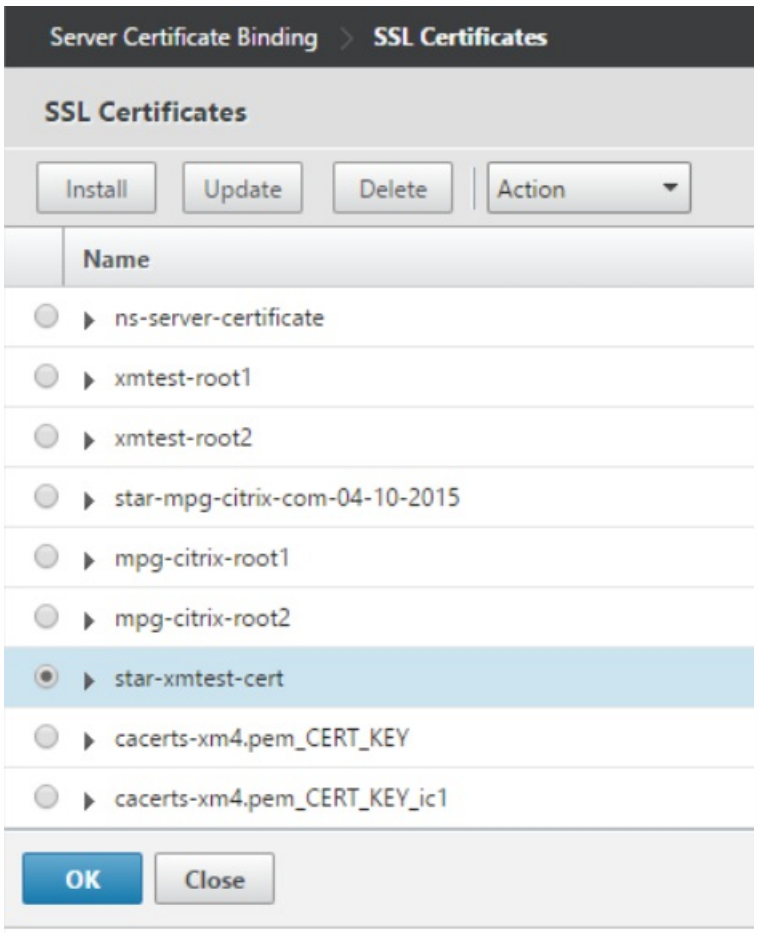


© 1999-2017 Citrix Systems, Inc. All rights reserved.

15. Sous **Server Certificate Binding**, cliquez sur **Click to Select**.

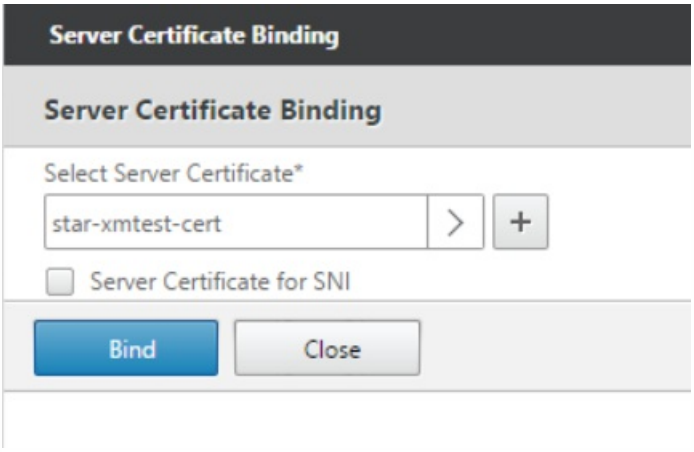


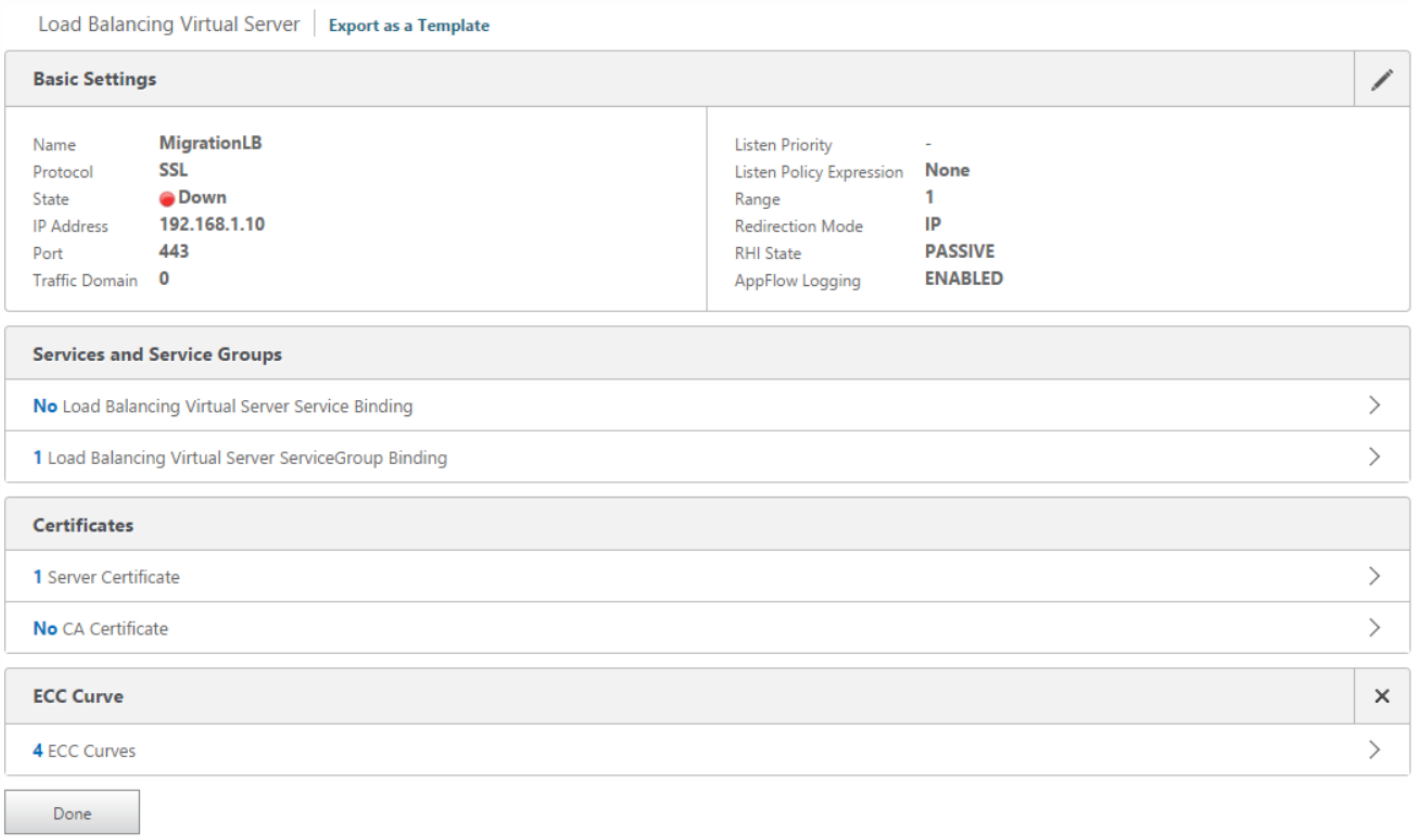
16. Sous **Certificates**, cliquez sur le certificat de serveur que vous avez exporté au cours des Prérequis, cliquez sur **OK**.



17. Cliquez sur **Bind**, puis sur l'écran suivant, cliquez sur **Done**.

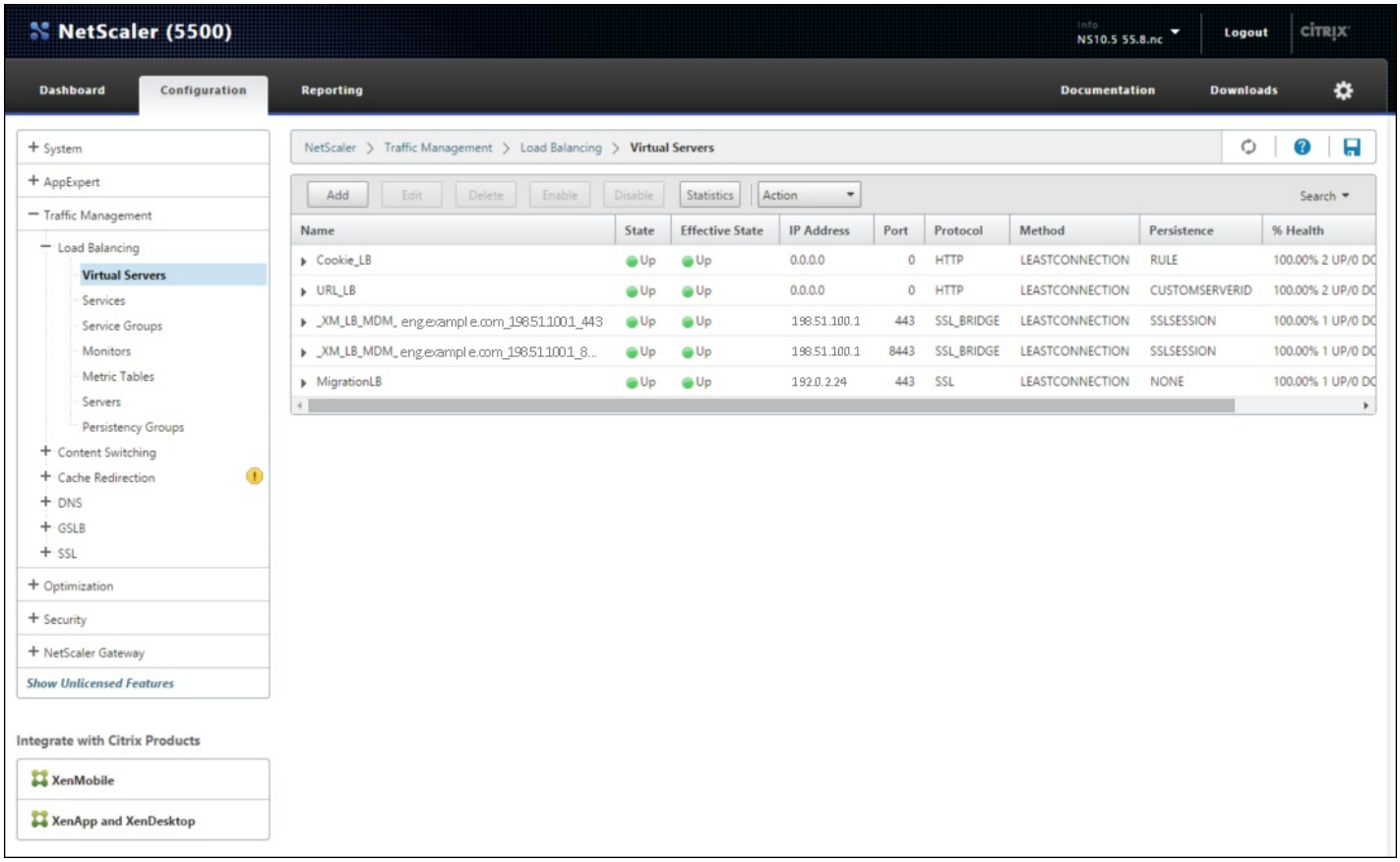
© 1999-2017 Citrix Systems, Inc. All rights reserved.





18. Cliquez sur le bouton d'actualisation pour confirmer que le serveur est en fonctionnement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



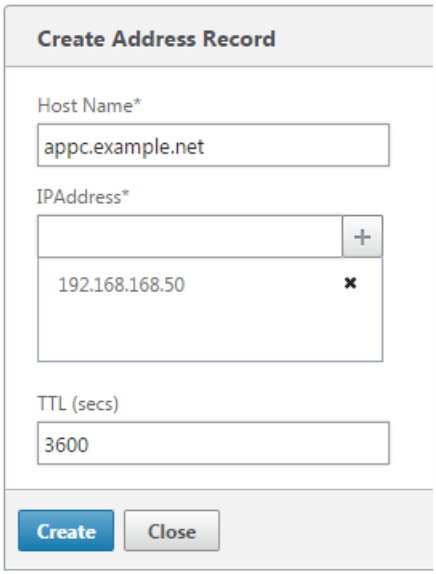
Configurer un enregistrement d'adresse pour le nom de domaine complet du serveur App Controller pointant vers le nouvel équilibrage de charge de migration

Cliquez sur **Traffic Management** > **DNS** > **Records** > **Address Records**, puis cliquez sur **Add** pour créer un enregistrement d'adresse pour le nom de domaine complet du serveur App Controller pointant vers le nouvel équilibrage de charge de migration.

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.

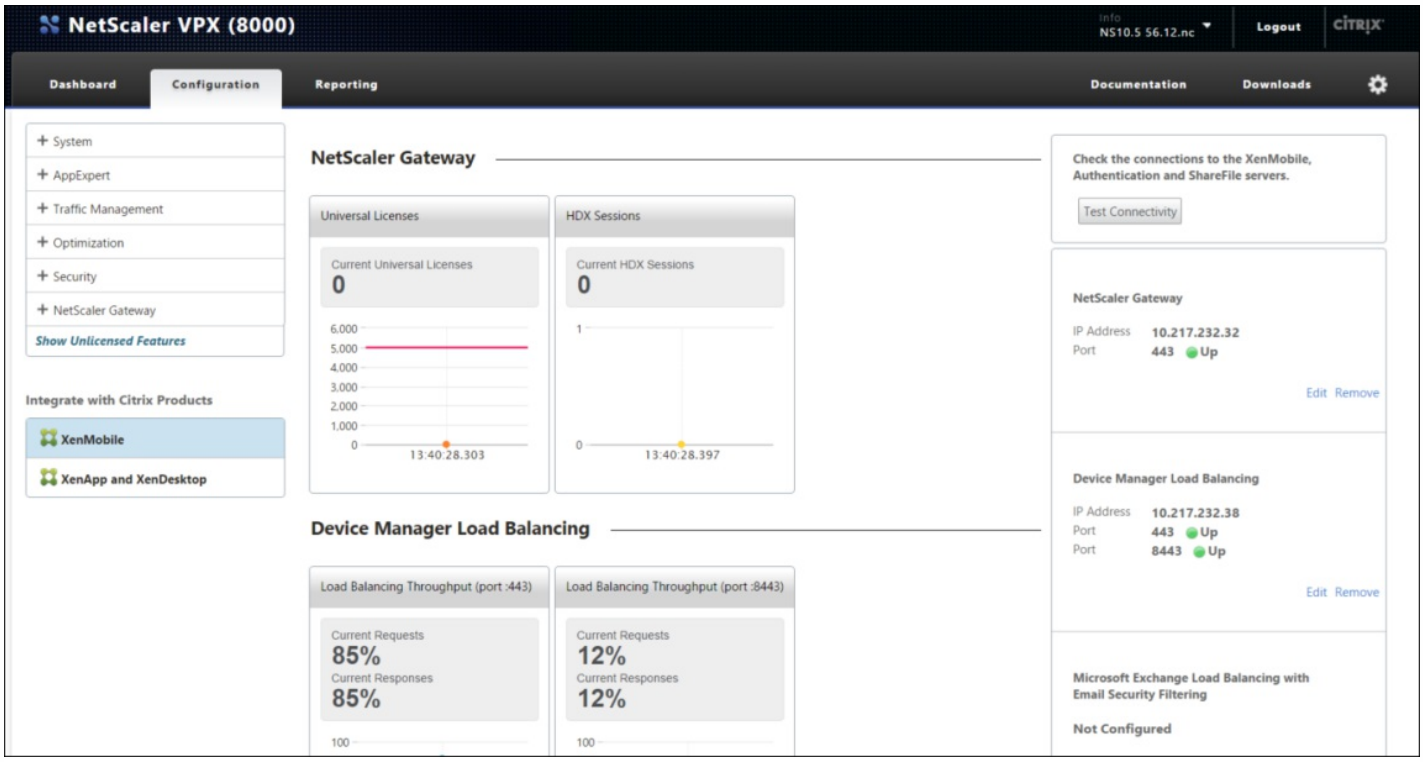
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mettre à jour l'équilibrage de charge XenMobile 9.0 MDM pour pointer vers la nouvelle adresse IP du serveur XenMobile 10.1

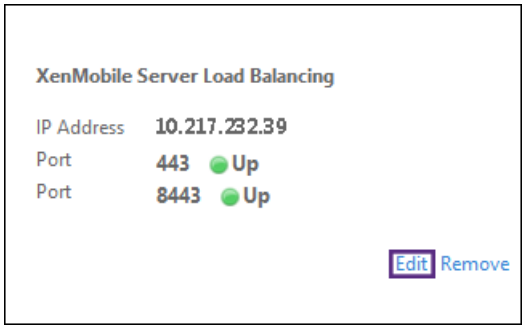
Si vous avez déployé le serveur exécutant XenMobile 9.0 derrière un boîtier d'équilibrage de charge NetScaler, vous devez configurer l'instance d'équilibrage de charge de XenMobile 9.0 Device Manager dans NetScaler avec la nouvelle adresse IP du serveur XenMobile 10.1, et aussi charger le certificat du serveur XenMobile 9.0 sur le serveur XenMobile 10.1.

1. Démarrez l'utilitaire de configuration NetScaler XenMobile.



2. Dans la partie droite de l'écran, sous **XenMobile Server Load Balancing**, cliquez sur **Edit**.

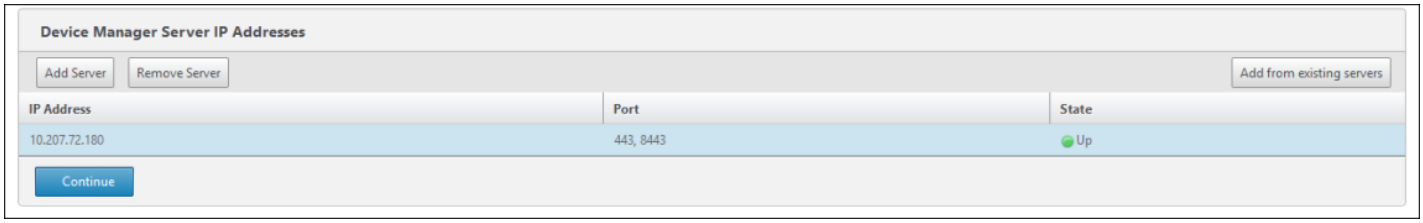
© 1999-2017 Citrix Systems, Inc. All rights reserved.



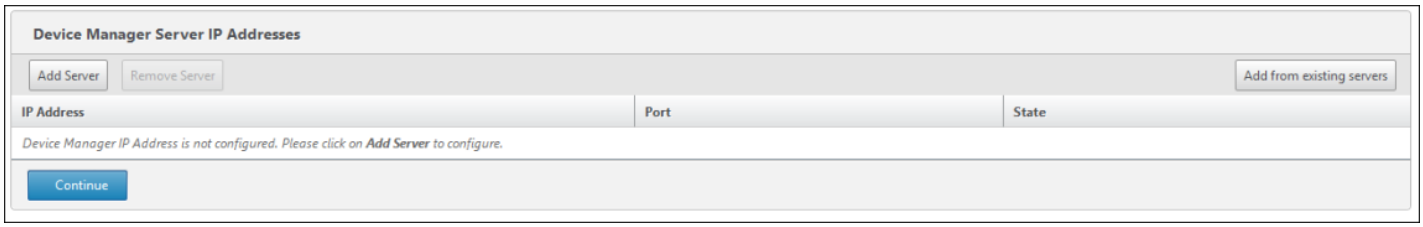
3. Cliquez sur l'icône de stylo pour modifier l'**adresse IP de Device Manager Server (Device Manager Server IP Address)**.



4. Sélectionnez l'adresse IP du serveur XenMobile 9.0 Device Manager et cliquez sur **Remove Server**.



5. Cliquez sur **Add Server** et ajoutez l'adresse IP du nouveau serveur XenMobile 10.1. **Remarque** : vous ne pouvez pas définir les numéros de port ici. Le serveur est créé sur le port 80 et son état est défini sur Down. Vous devez créer des services pour les ports 443 et 8443 et lier ces services au serveur virtuel d'équilibrage de charge approprié.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



Modifier le nom de domaine complet d'App Controller sur NetScaler Gateway

Dans XenMobile 10.1, le composant App Controller écoute sur le port 8443 plutôt que sur le port 443. Vous devez modifier le nom de domaine complet d'App Controller en fonction de l'édition que vous migrez.

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 10.1, qui est le nom de domaine complet de XenMobile 9.0 Device Manager suivi du port 8443. Le tableau suivant présente un exemple.

Composant de XenMobile 9.0	Nom de domaine complet du composant	Nom de domaine complet de XenMobile 10.1 Enterprise Edition
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

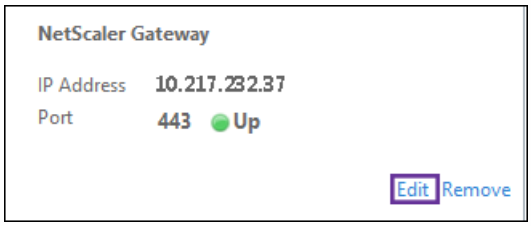
Modifiez le nom de domaine complet d'App Controller de manière à pointer vers le nouveau nom de domaine complet de XenMobile 10.1, à savoir le nom de domaine complet de XenMobile 9.0 App Controller suivi du port 8443. Le tableau suivant présente un exemple.

Composant de XenMobile 9.0	Nom de domaine complet du composant	Nom de domaine complet de XenMobile 10.1 Enterprise Edition
App Controller	appc.example.net	appc.example.net:8443
NetScaler Gateway	access.example.com	S.O.

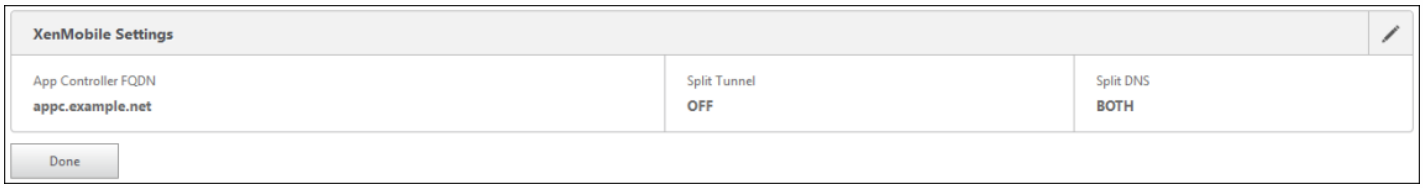
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour modifier le nom de domaine complet d'App Controller

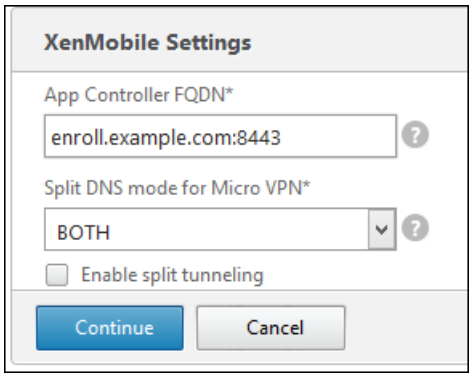
1. Sous **NetScaler Gateway**, cliquez sur **Edit**.



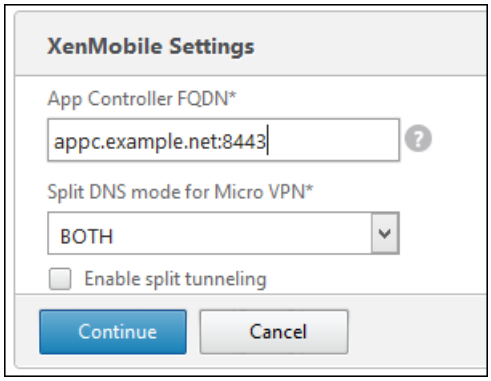
2. Cliquez sur l'icône de stylo en regard de **XenMobile Settings**.



3. Modifiez le nom de domaine complet d'App Controller : XenMobile Enterprise Edition: enroll.example.com:8443



XenMobile App Edition: appc.example.net:8443



4. Cliquez sur **Continue** et **Finish**. Ensuite, vous devez mettre à jour votre DNS pour résoudre le nom de domaine complet de l'adresse IP du serveur XenMobile 10.1.

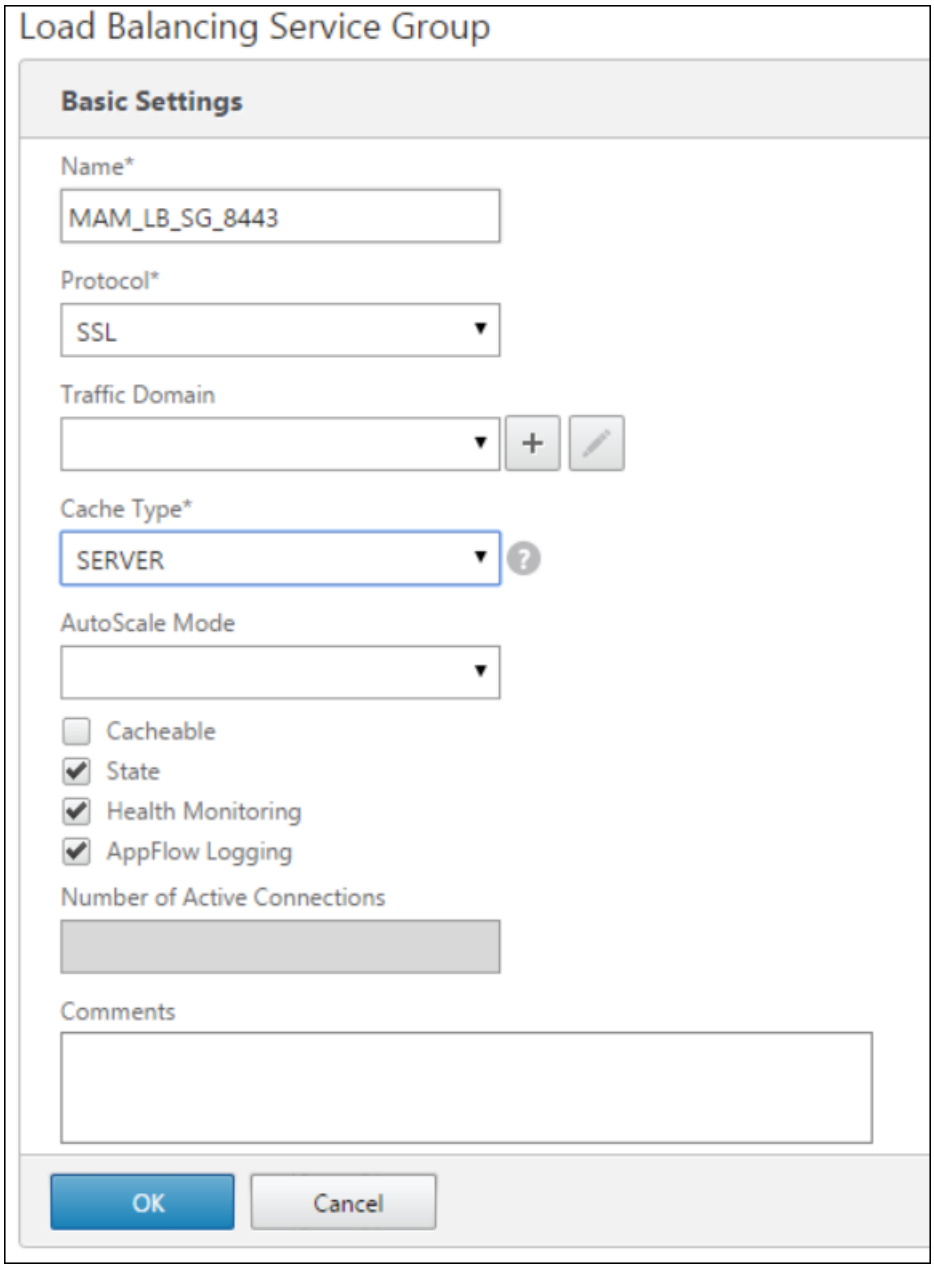
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Créer un nouveau serveur virtuel d'équilibrage de charge MAM basé sur une configuration MDM de pont SSL

Vous devez créer un nouveau serveur virtuel d'équilibrage de charge MAM pour équilibrer la charge du trafic de MAM sur la base de la configuration du serveur virtuel d'équilibrage de charge MDM existant. La procédure suivante explique comment procéder si vous avez un pont SSL configuré. Si votre serveur virtuel d'équilibrage de charge est configuré avec le déchargement SSL, veuillez consulter les étapes de cette procédure.

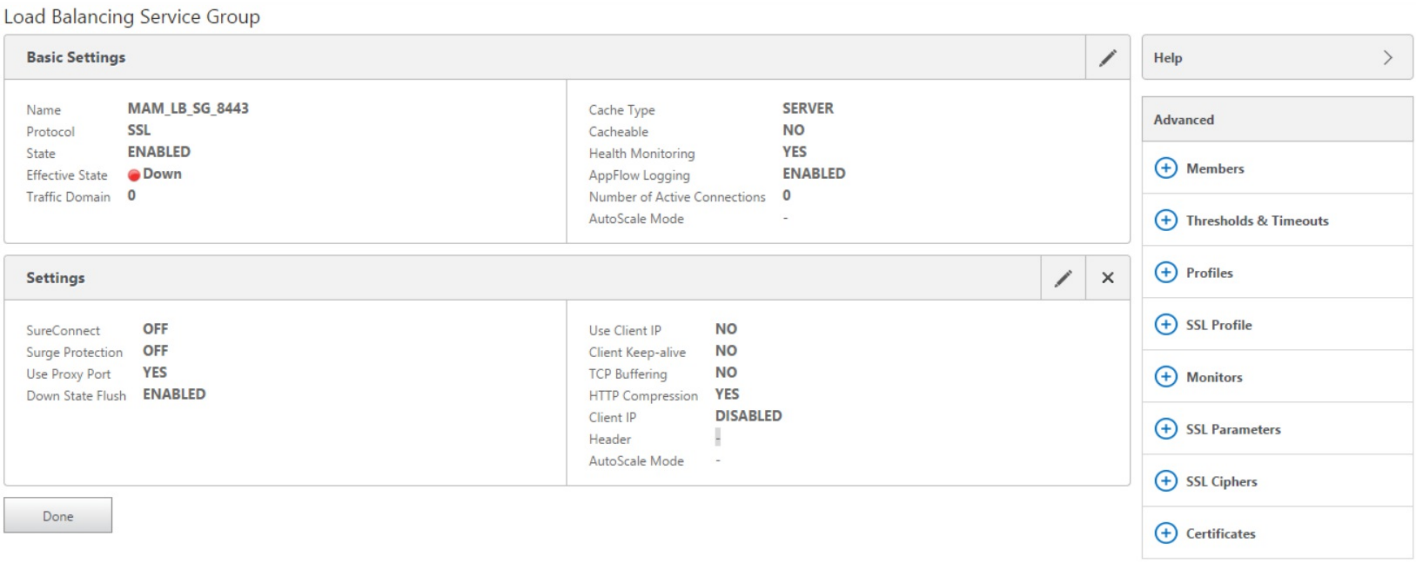
Créez un serveur virtuel d'équilibrage de charge MAM et liez les services du groupe de services au serveur virtuel d'équilibrage de charge.

1. Cliquez sur **Traffic Management** > **Load Balancer** > **Service Groups**.
2. Cliquez sur Add, puis configurez les paramètres comme illustré dans la figure suivante :

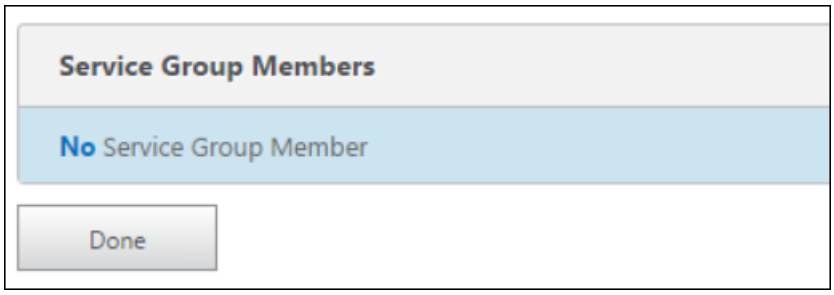


3. Cliquez sur **OK**, puis sur **Members**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

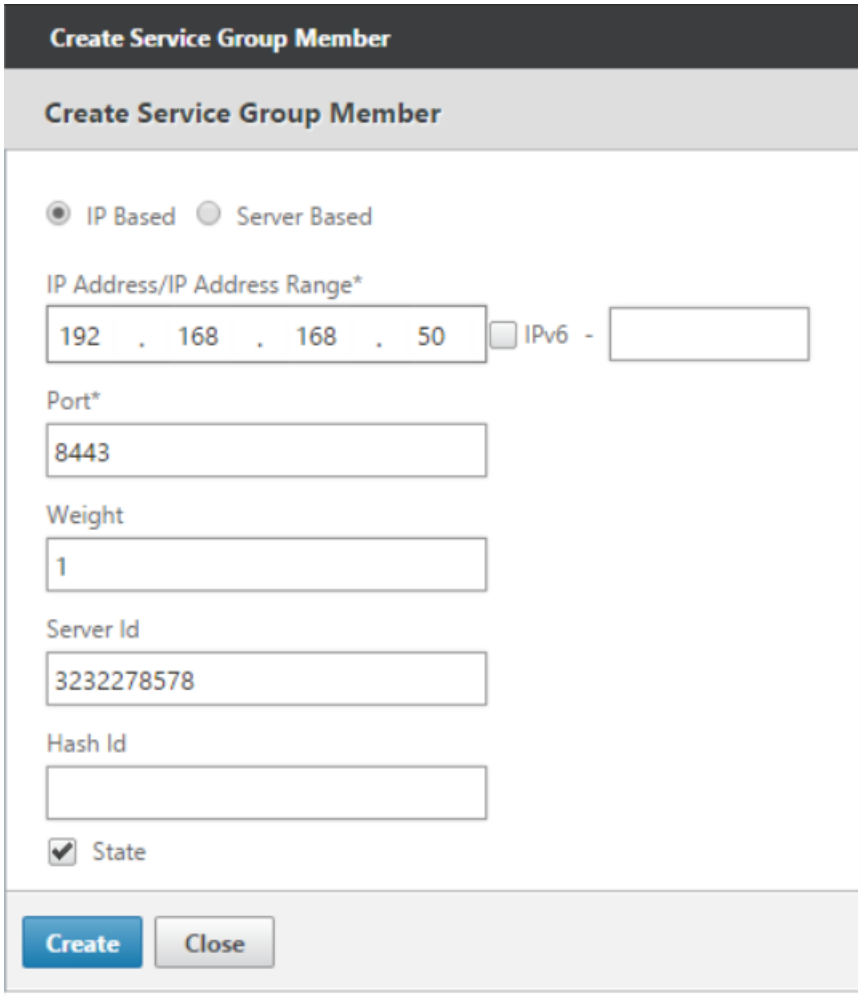


4. Cliquez sur **No Service Group Member** pour ajouter un nouveau membre.



5. Entrez l'adresse IP du serveur XenMobile, le port 8443 et l'ID du serveur, puis cliquez sur **Create**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

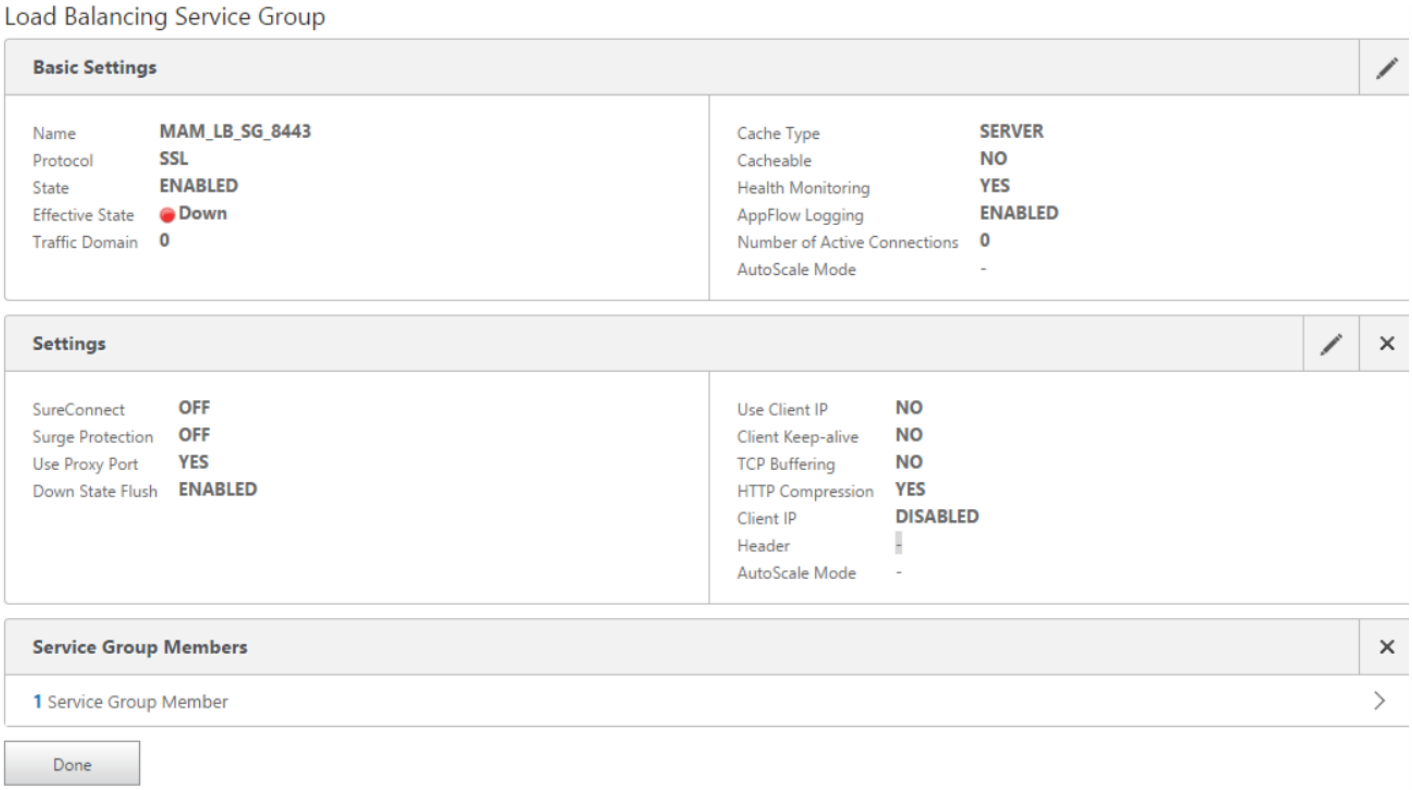


Remarque

- Vous pouvez obtenir l'ID du serveur à partir de l'interface de ligne de commande de XenMobile 10.1 sous l'option de menu Afficher l'état du cluster.
- Si vous disposez de plusieurs nœuds XenMobile, recommencez cette étape pour chaque nœud, en ajoutant chaque nœud au groupe de services MAM_LB_SG_8443.

6. Cliquez sur **Done**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

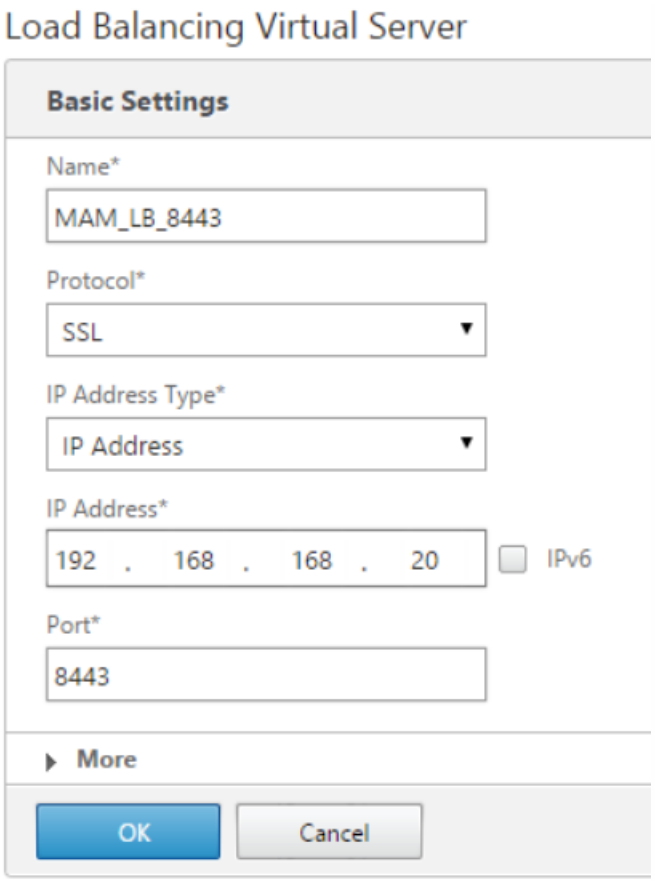


7. Cliquez sur **Traffic Management** > **Load Balancer** > **Virtual Server**, puis cliquez sur **Add**.

> ## Remarque
>
> vous créez cet équilibrage de charge pour acheminer le trafic de NetScaler Gateway vers les nœuds du serveur XenMobile.

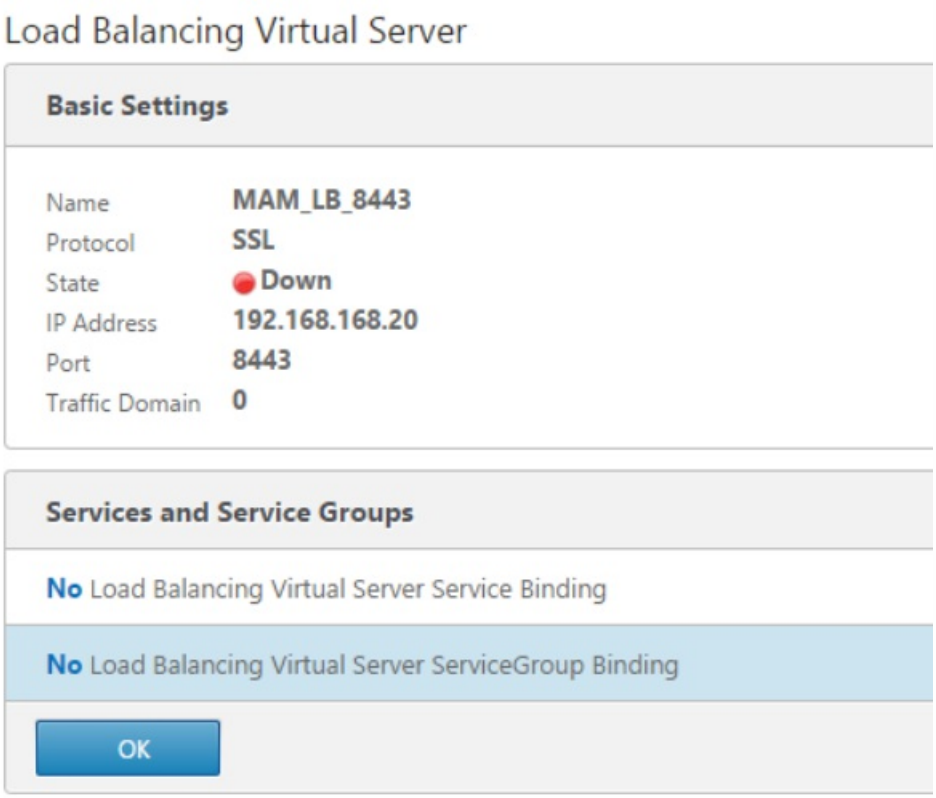
8. Tapez un nom pour l'équilibrage de charge MAM, le port 8443 et les adresses IP privées inutilisées comme indiqué dans la figure suivante.

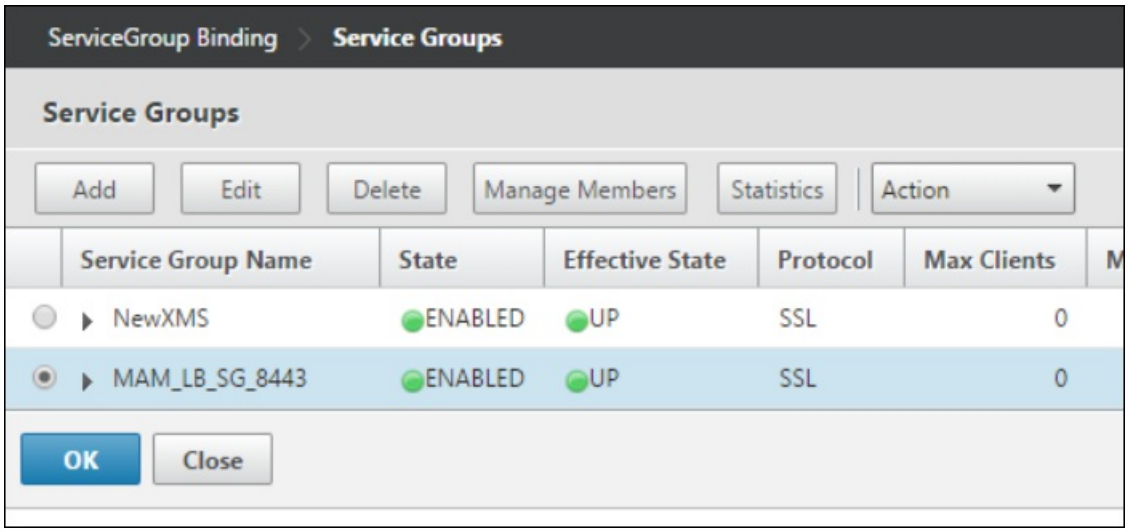
© 1999-2017 Citrix Systems, Inc. All rights reserved.



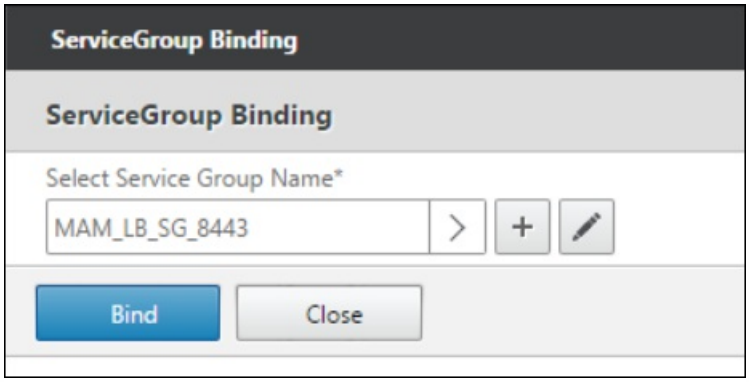
9. Cliquez sur **No Load Balancing Virtual Server ServiceGroup Binding** pour lier le groupe de services MAM_LB_SG_8443 comme indiqué dans les figures suivantes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

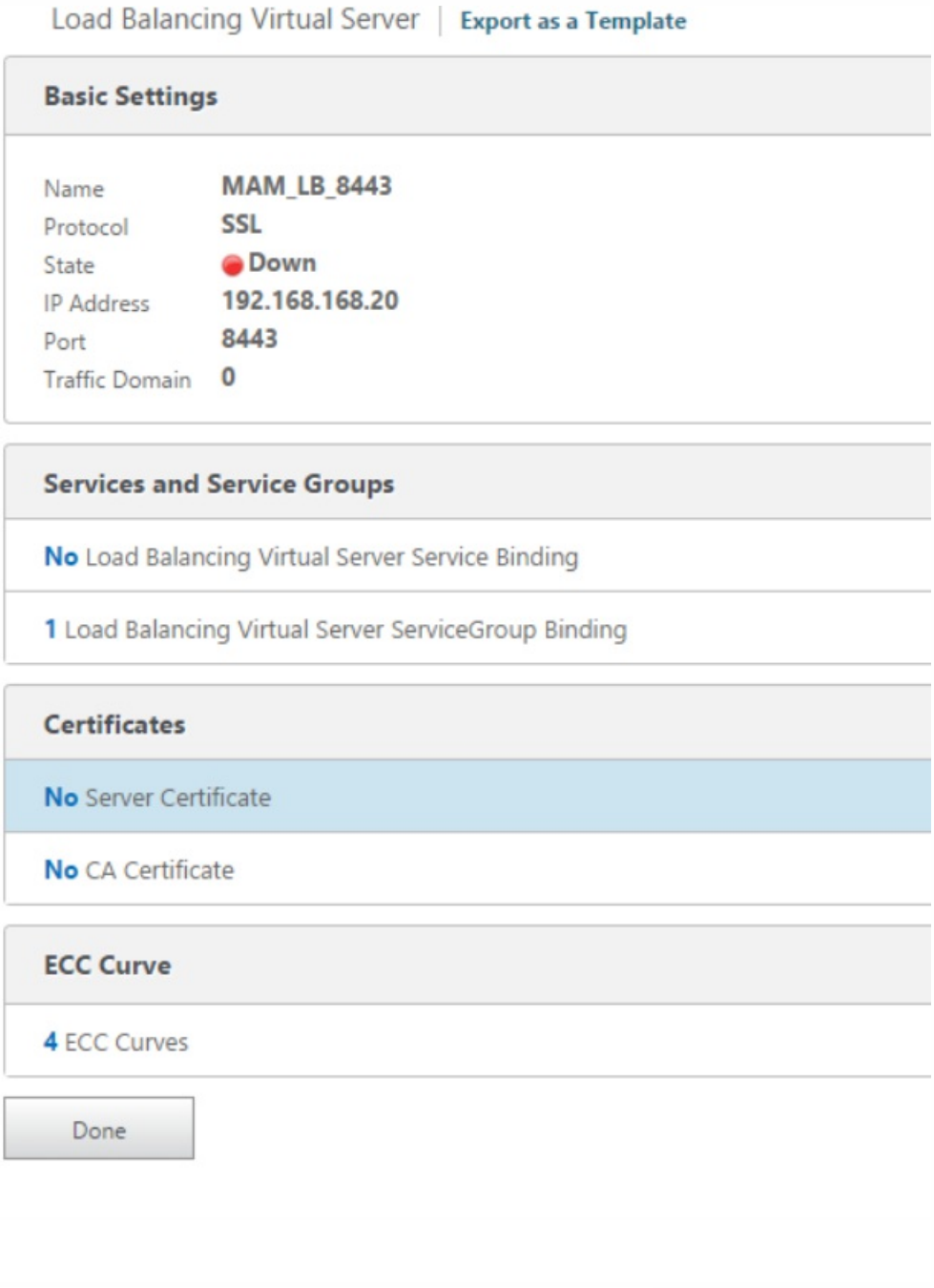




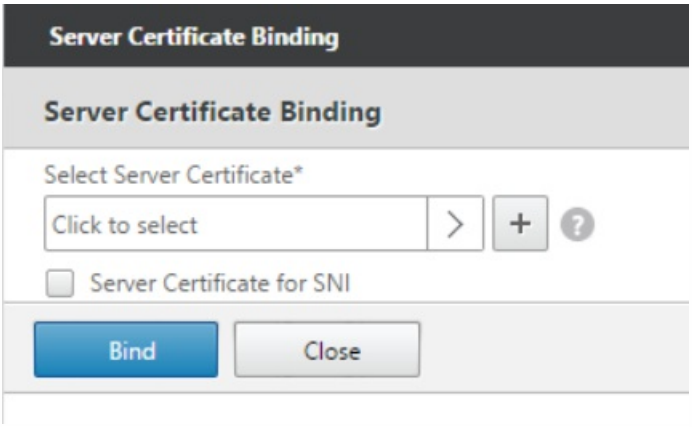
© 1999-2017 Citrix Systems, Inc. All rights reserved.

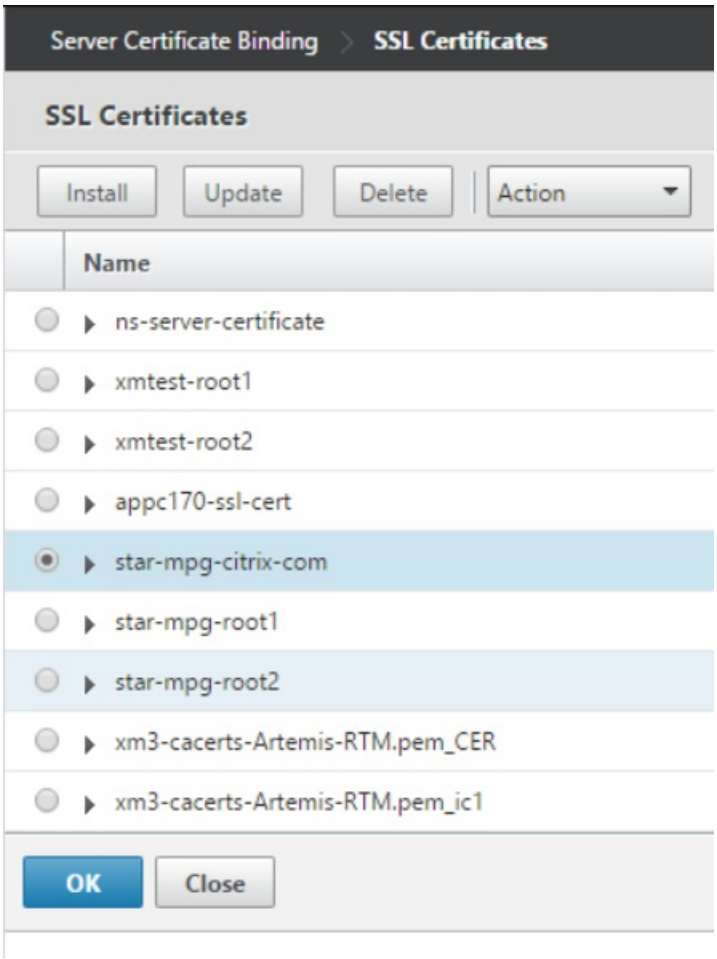


10. Liez le certificat du serveur au serveur virtuel MAM_LB_8443 comme indiqué dans les figures suivantes.

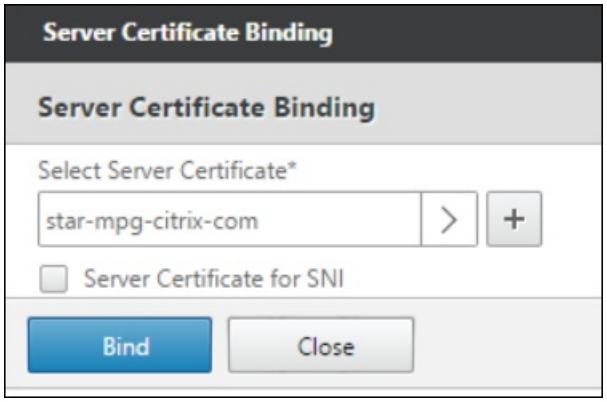


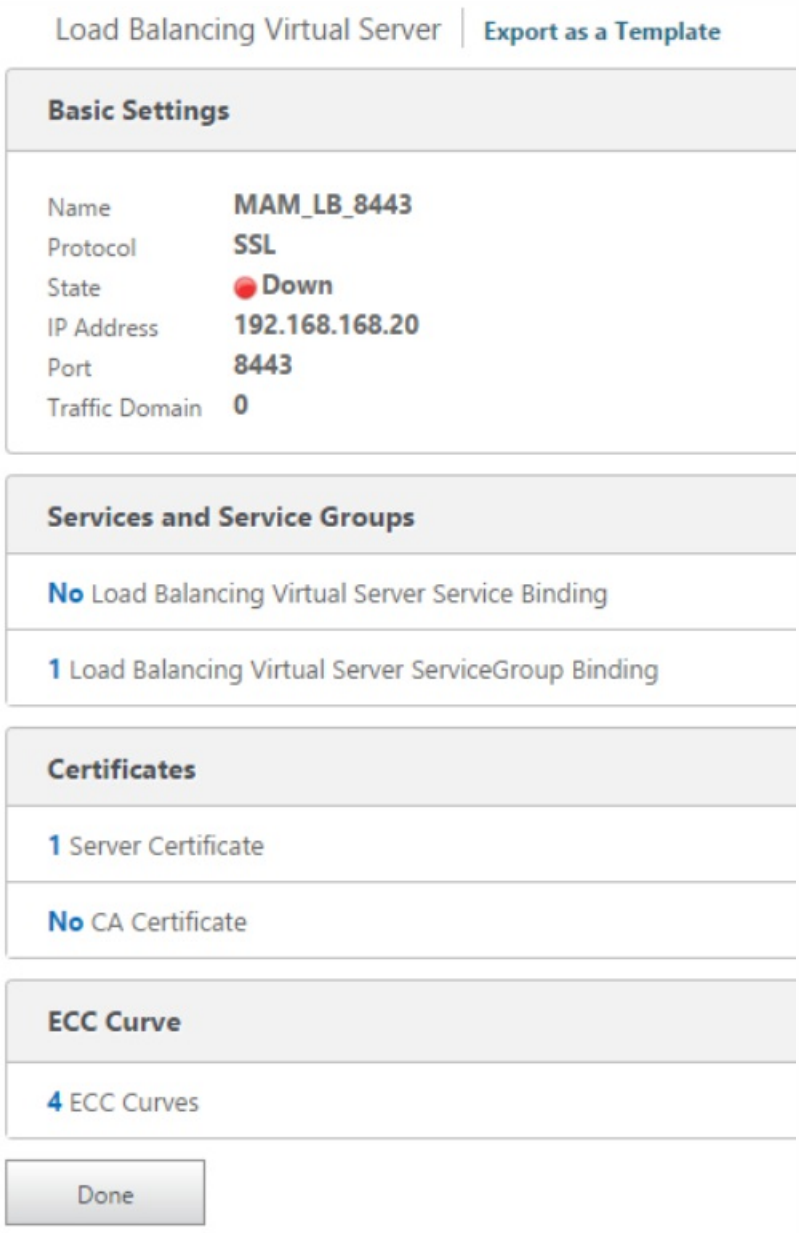
© 1999-2017 Citrix Systems, Inc. All rights reserved.





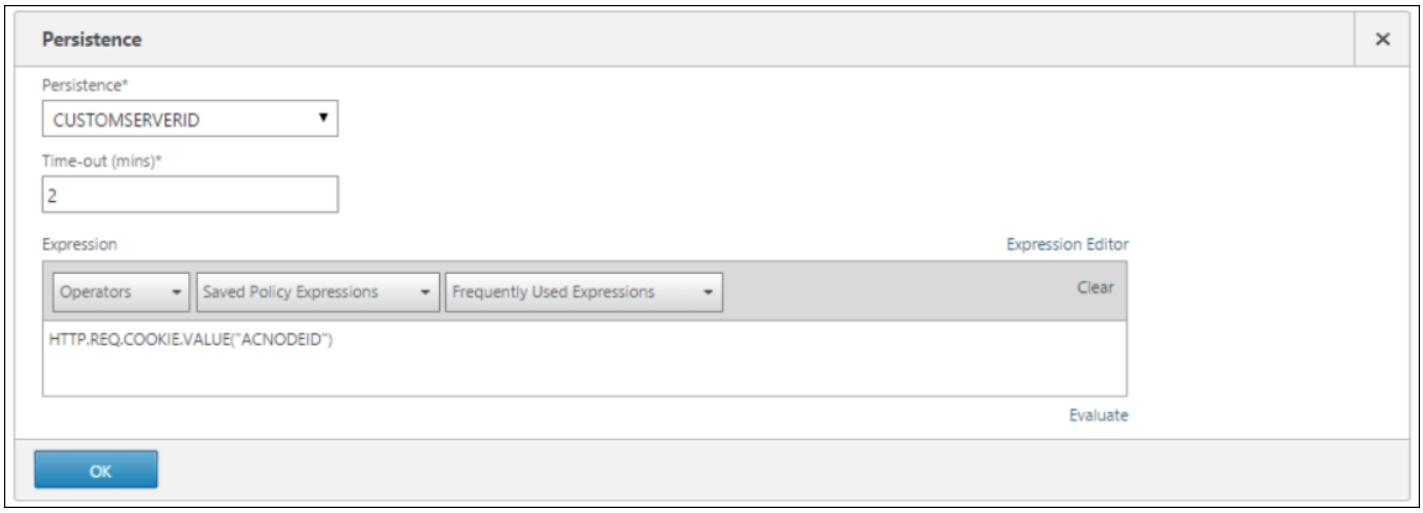
© 1999-2017 Citrix Systems, Inc. All rights reserved.





11. Sous **Persistence**, dans la liste **Persistence**, cliquez sur **CUSTOMSERVERID**, puis dans le champ **Expression**, tapez HTTP.REQ.COOKIE.VALUE(“ACNODEID”), puis cliquez sur **OK**.

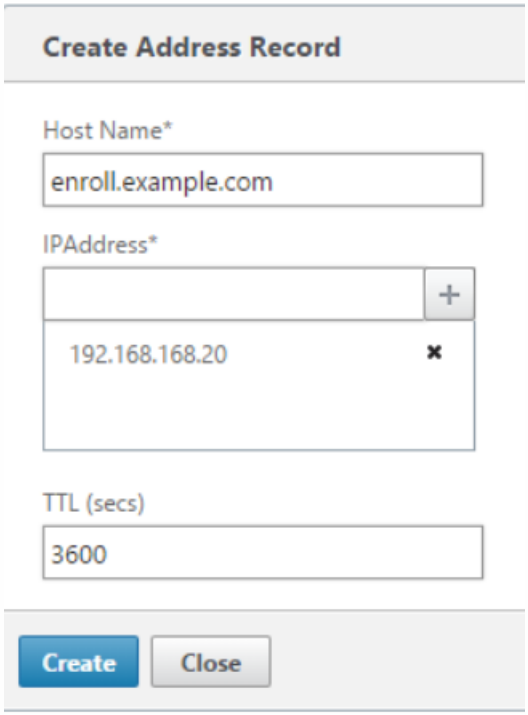
 © 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur**Traffic Management** > **DNS** > **Records** > **Address Records** pour créer un enregistrement d'adresse pour le nom de domaine complet du serveur XenMobile 10.1 pointant vers le nouveau serveur virtuel MAM_LB_8443.

Remarque

Le nom de domaine complet du serveur XenMobile 10.1 est enroll.example.com.

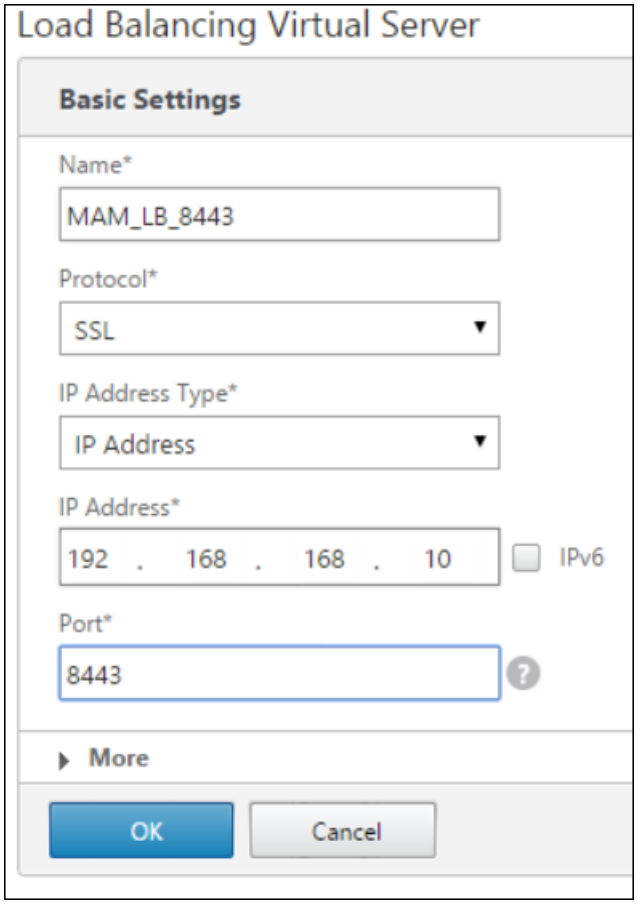


Créer un nouveau serveur virtuel d'équilibrage de charge MAM basé sur une configuration MDM de déchargement SSL

1. Cliquez sur **Traffic Management** > **Load Balancer** > **Virtual Server**, puis cliquez sur **Add**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

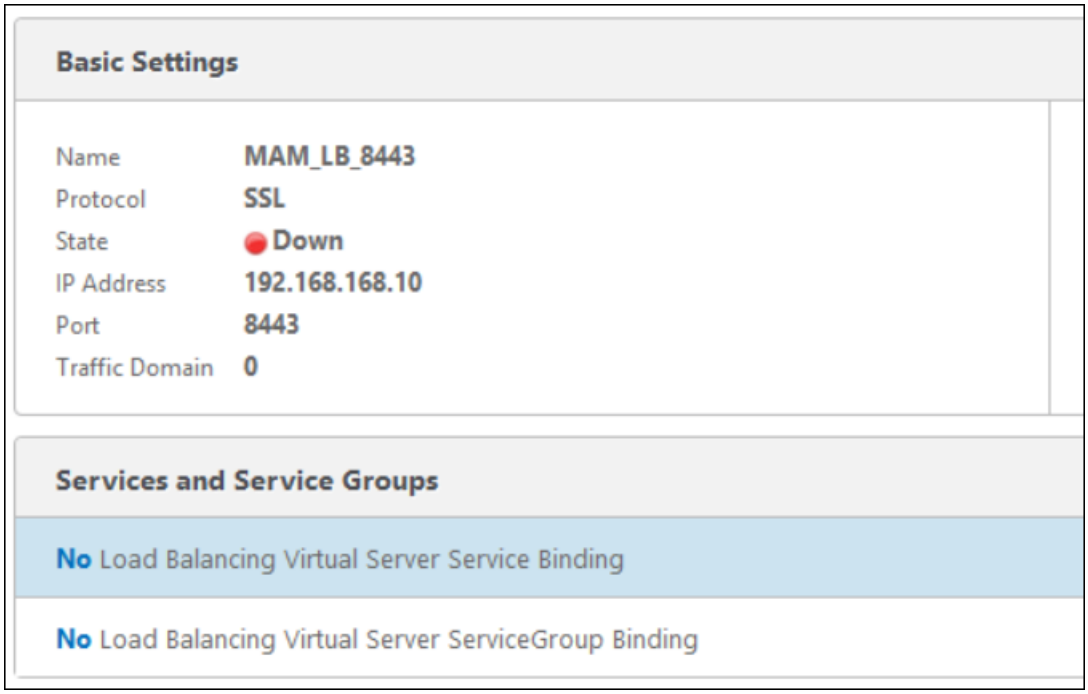
2. Tapez un nom pour l'équilibrage de charge MAM, le port 8443 et les adresses IP privées inutilisées comme indiqué dans l'image suivante.



3. Cliquez sur **OK**.

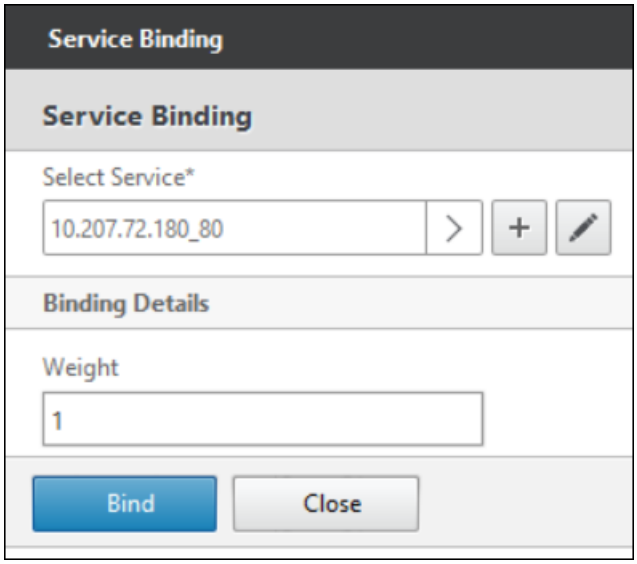
4. Cliquez sur **No Load Balancing Virtual Server Service Binding** pour lier le serveur virtuel du groupe de services MAM_LB_8443 comme indiqué dans les figures suivantes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



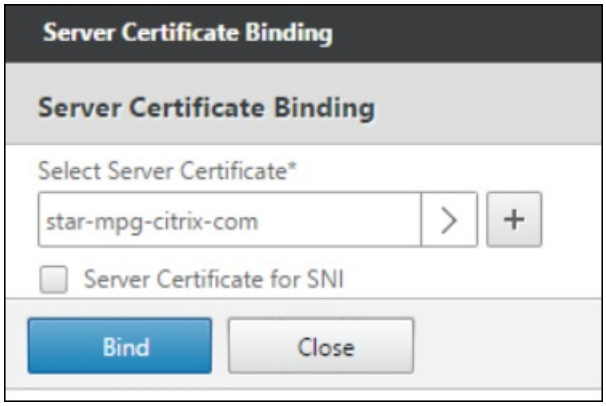
Remarque

Le service est déjà présent puisqu'il a été configuré à l'aide de l'assistant d'équilibrage de charge MDM.

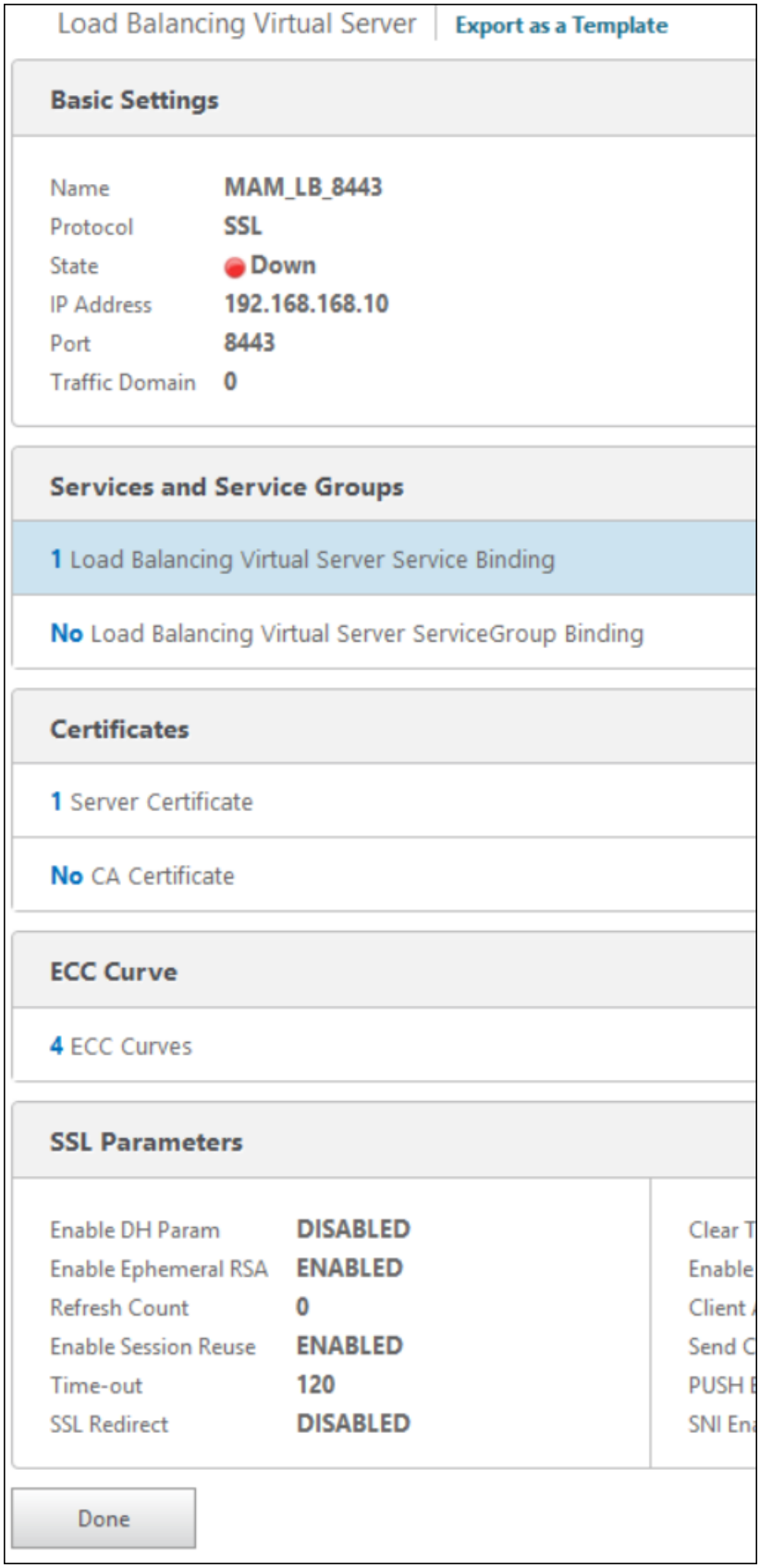


5. Liez le certificat du serveur au serveur virtuel MAM _LB_8443 comme indiqué dans les figures suivantes, puis cliquez sur **Done**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

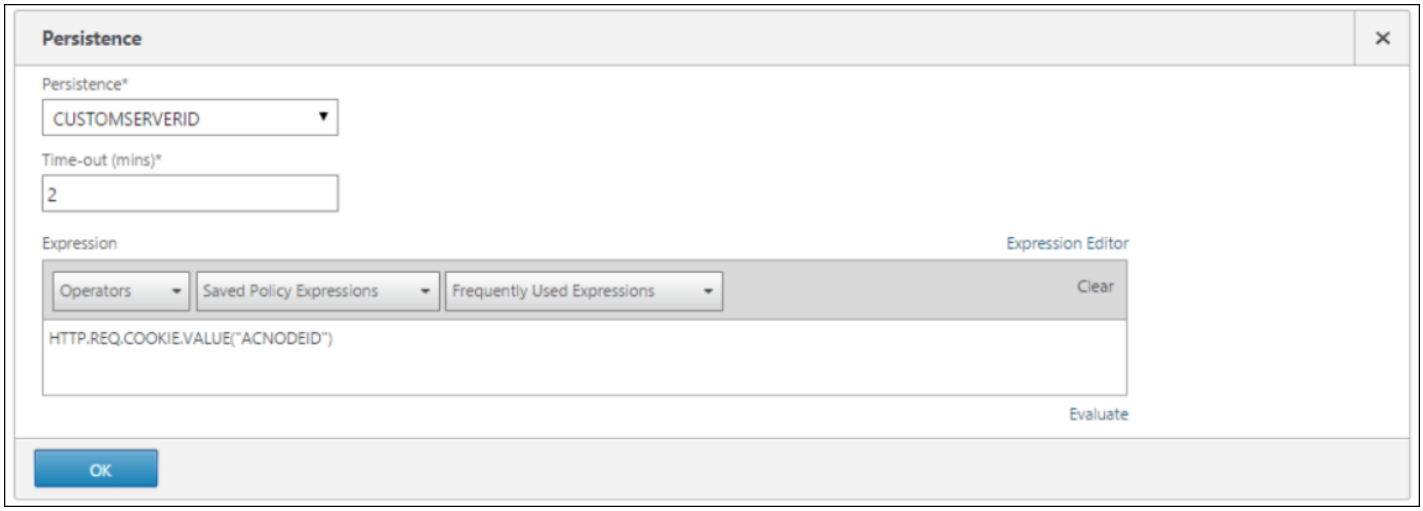


© 1999-2017 Citrix Systems, Inc. All rights reserved.



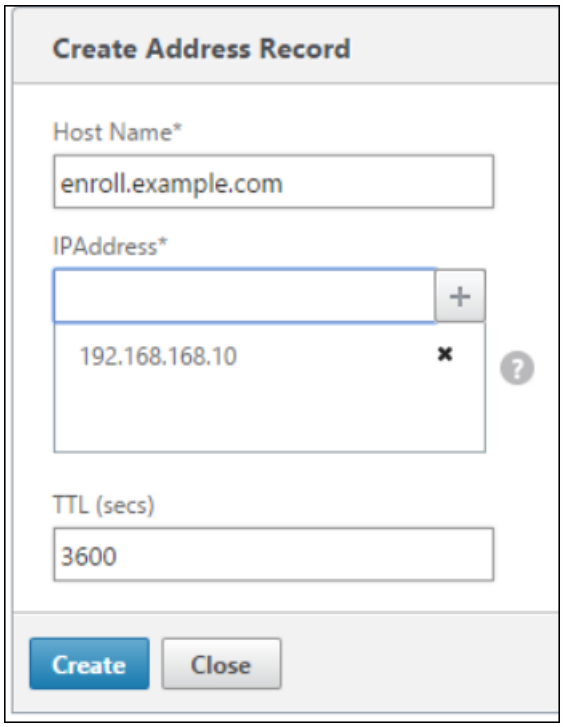
6. Sous **Persistence**, dans la liste **Persistence**, cliquez sur **CUSTOMSERVERID**, puis dans le champ **Expression**, tapez HTTP.REQ.COOKIE.VALUE("ACNODEID").

 © 1999-2017 Citrix Systems, Inc. All rights reserved.



7. Configurez un enregistrement d'adresse pour le nom de domaine complet du serveur XenMobile pointant vers le nouveau serveur virtuel d'équilibrage de charge MAM.

8. Cliquez sur **Traffic Management** > **DNS** > **Records** > **Address Records**, puis cliquez sur **Add** pour créer un enregistrement d'adresse pour le nom de domaine complet du serveur XenMobile 10.1 pointant vers le nouveau serveur virtuel d'équilibrage de charge MAM.

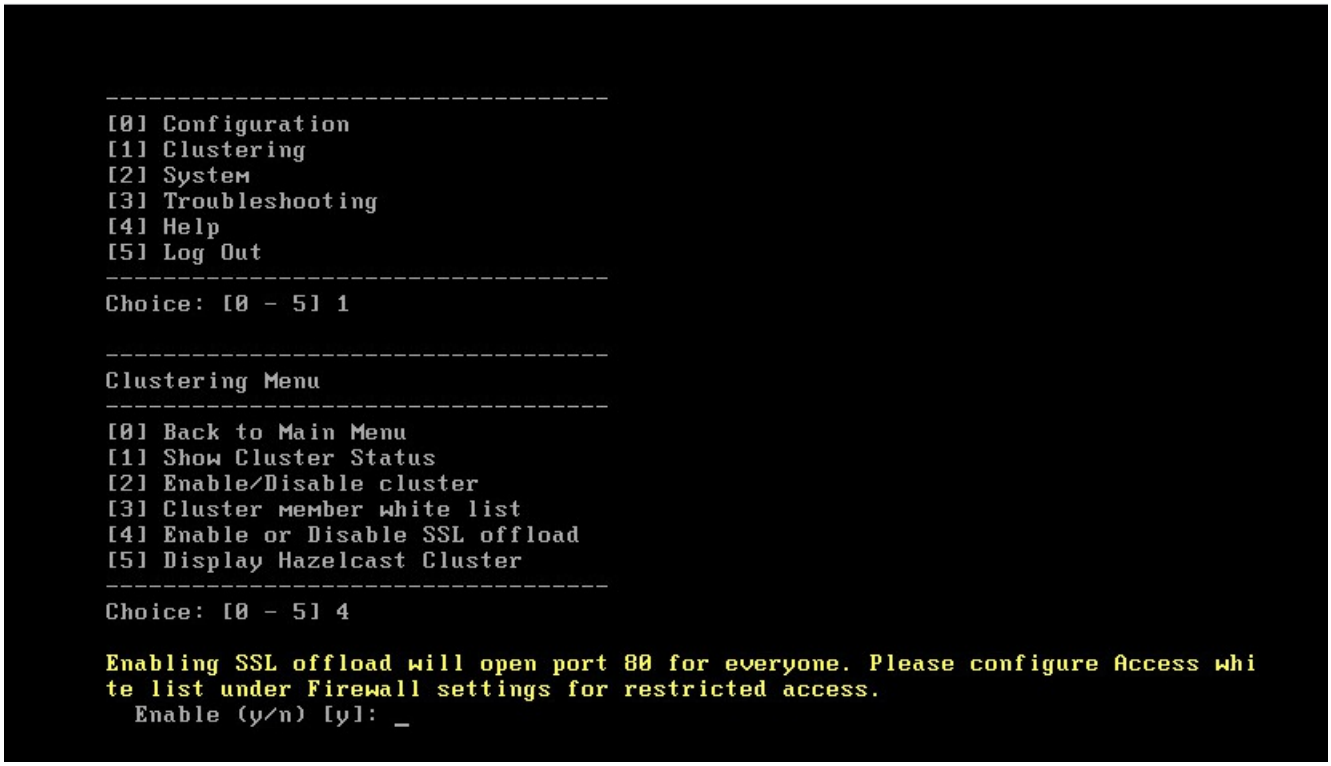


Remarque

Le nom de domaine complet du serveur XenMobile 10.1 est enroll.example.com.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

9. Si vous utilisez le déchargement SSL, dans l'interface de ligne de commande, activez le port 80 pour le déchargement SSL.



Reconfigurer la STA sur NetScaler Gateway

Dans NetScaler Gateway, vous devez également ajouter l'adresse IP ou le nom de domaine complet du serveur exécutant la STA. Pour ce faire, suivez cette procédure :

1. Cliquez sur **Netscaler Gateway**.
2. Cliquez sur **Virtual Servers**.
3. Sélectionnez la configuration du serveur virtuel NetScaler Gateway, puis cliquez sur **Modifier**.
4. Sous **Published Applications**, cliquez sur **STA server**.
5. Notez l'adresse URL, puis sélectionnez le serveur Secure Ticket Authority dans la liste.
6. Cliquez sur **Unbind** , puis cliquez sur **Add Binding**.
7. Dans le champ **Secure Ticket Authority Server**, tapez l'URL notée à l'étape 5.
8. 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.

Mise en cluster

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Si vous déployez XenMobile 10.1 dans un cluster, vous devez utiliser l'interface de ligne de commande pour activer la prise en charge de cluster et rejoindre les nouveaux nœuds XenMobile. Vous pouvez réutiliser les adresses IP du nœud XenMobile 9.0 en configurant la nouvelle instance de XenMobile 10.1 avec la même adresse IP et la joindre au nœud (administrateur) le plus ancien.

Mise à jour des informations qui n'ont pas été migrées

Mettez à jour les informations suivantes, selon les besoins :

- Groupe de fournisseurs de services gérés (MSP)
- Attributs Active Directory personnalisés
- Rôles RBAC
- Paramètres de journal
- Toutes les données de configuration ou d'utilisateur répertoriées dans le fichier migration.log
- Toutes les configurations de serveur Syslog
- Pour une migration sur site, les rôles RBAC sont migrés, mais il existe des problèmes connus.

Considérations à prendre en compte lors de l'utilisation d'un nom de magasin WorxStore personnalisé

Avant la mise à niveau, l'une des étapes préalables consistait à contourner ce problème :

> Problème connu du WorxStore : avant la mise à niveau de XenMobile 9 vers XenMobile 10.1, 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. [#619458]

Si vous n'avez pas rempli cette condition préalable, vous devez suivre l'une de ces étapes préalables avant d'utiliser XenMobile Server 10.1 :

- Si vous disposez d'une flotte importante d'appareils Windows, rétablissez le nom par défaut du magasin. Après cela, les utilisateurs qui se sont inscrits avec des appareils iOS et Android doivent se déconnecter et se reconnecter à WorxHome.
- Si vous possédez moins d'appareils Windows que d'appareils iOS et Android, il est recommandé aux utilisateurs Windows de réinscrire leurs appareils.

Pour de plus amples informations sur ce problème, veuillez consulter l'article http://support.citrix.com/article/CTX214553.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Restauration des mises à niveau de XenMobile

Oct 11, 2016

Après la mise à niveau de XenMobile 9 vers XenMobile 10.1, certains clients ont signalé des problèmes d'accès à WorxStore, d'ouverture d'applications, ainsi que des problèmes avec d'autres fonctionnalités. Citrix fournissait préalablement des instructions permettant de restaurer temporairement une mise à niveau. Il est maintenant recommandé de *ne plus* essayer de restaurer une mise à niveau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mise à niveau du serveur locataire de la console MTC vers XenMobile 10.1

Jul 25, 2016

Si la Multi-Tenant Console (MTC) est activée sur XenMobile 9.0, vous pouvez migrer les instances XenMobile 9 gérées par MTC vers des instances XenMobile 10 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.

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 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. Pour le nom de l'instance, utilisez zdm.

5. Durant l'installation du serveur XenMobile, sélectionnez **Oui** lorsque vous êtes invité à confirmer que vous procédez à une mise à niveau.

6. Copiez les fichiers suivants depuis le serveur sur lequel vous procédez à la mise à niveau : 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. Copiez et modifiez : C:\Program Files (x86)\Citrix\XenMobile Device Manager for Multi-Tenant\tomcat\conf\server.xml

9. Supprimez tous les connecteurs de port utilisés par l'autre locataire dans le fichier server.xml. Vous pouvez laisser 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 :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 changés aux étapes 10 et 11.

13. Ouvrez https://10.215.199.42:1433/uw/?cloudMode, où l'adresse IP est suivie par le port de la connexion HTTPS avec certificat.

14. Ouvrez le dossier Mettre à niveau (Upgrade).

15. Installez le fichier 63110upgrade.bin.

16. Sélectionnez MDM et cliquez sur **Suivant** dans les écrans qui suivent jusqu'à ce que vous soyez invité à sélectionner le fichier .zip.

17. Assurez-vous que la base de données est correcte, entrez le mot de passe du certificat d'autorité de certification et cliquez sur **Suivant** à deux reprises.

18. 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.

19. Dans la console XenMobile, installez une nouvelle licence.

20. Changez la traduction d'adresses réseau afin de pointer vers un nouveau serveur.

21. Apportez les modifications nécessaires au pare-feu afin d'autoriser les ports utilisés par le serveur XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

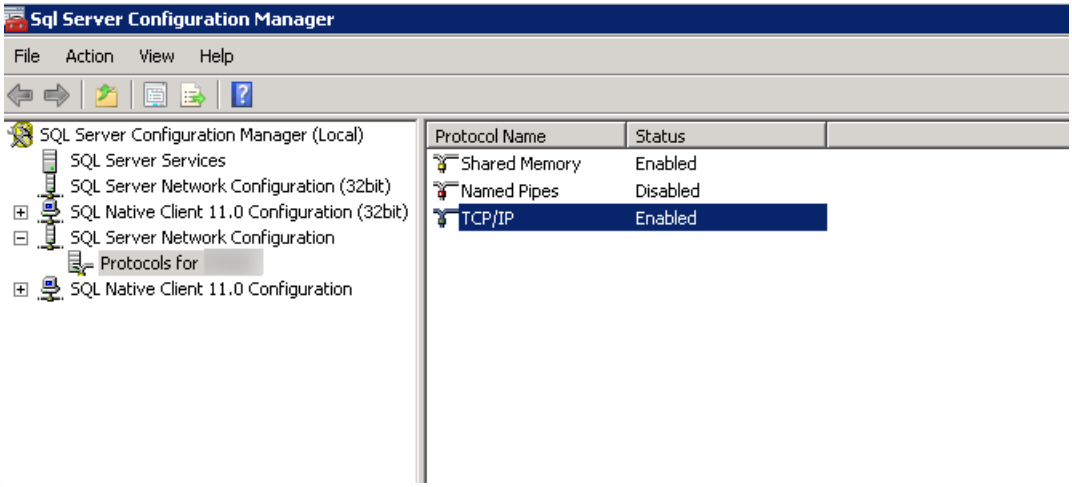
Prise en charge des instances SQL nommées

Jul 25, 2016

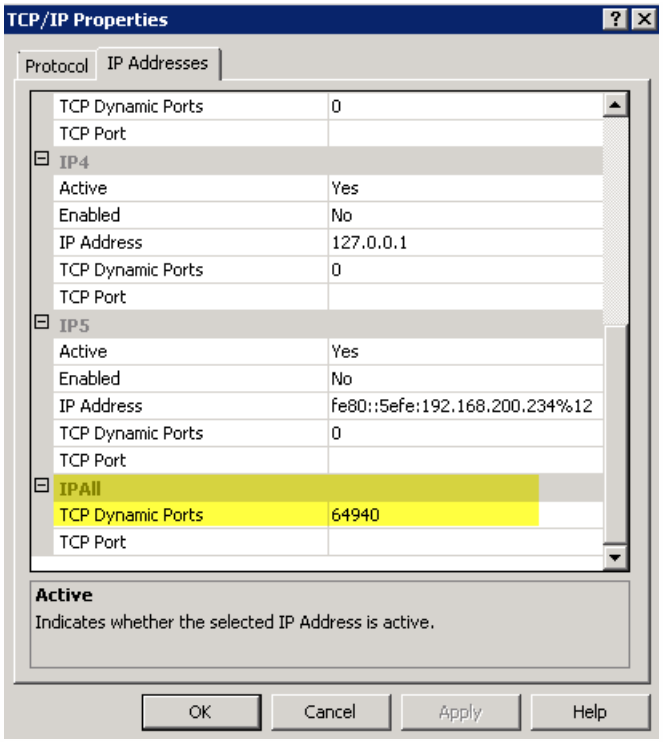
Vous pouvez utiliser l'outil de mise à niveau pour mettre à niveau XenMobile 9 vers XenMobile 10 et mettre à niveau XenMobile 9 vers XenMobile 10.1. Si votre installation XenMobile 9 est basée sur des instances SQL nommées, vous devez suivre les étapes spécifiques à cette situation. Si votre environnement XenMobile 9 répond aux conditions préalables suivantes, suivez les étapes dans cet article pour procéder à la mise à niveau.

- XenMobile 9 MDM Edition ou Enterprise Edition configuré avec une base de données SQL Server externe.
- Base de données SQL Server exécutée sur une instance nommée autre que celle par défaut.
- Instance nommée SQL Server écoutant 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.

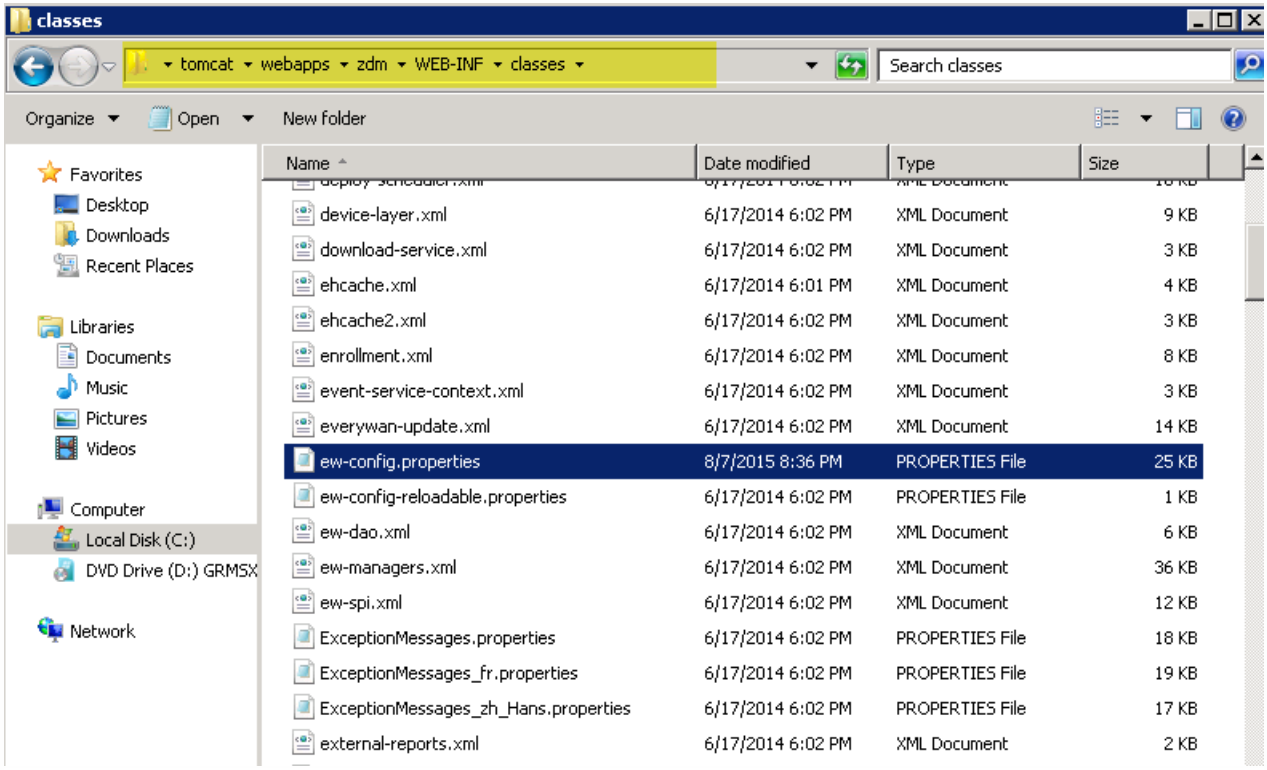


© 1999-2017 Citrix Systems, Inc. All rights reserved.



Étapes à suivre pour mettre à niveau XenMobile avec une instance nommée SQL Server

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.

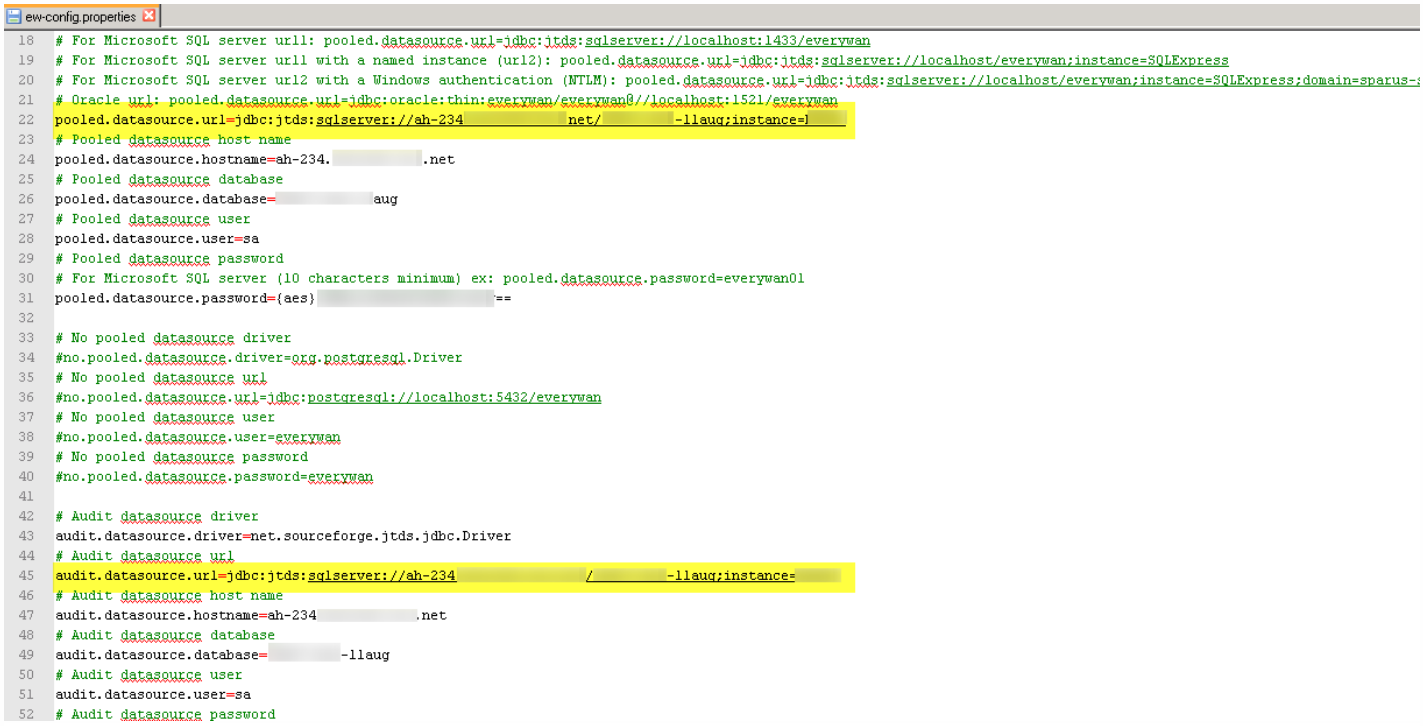


2. Dans le fichier ew-config.properties, recherchez les URL suivantes dans la section DATASOURCE Configuration :

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

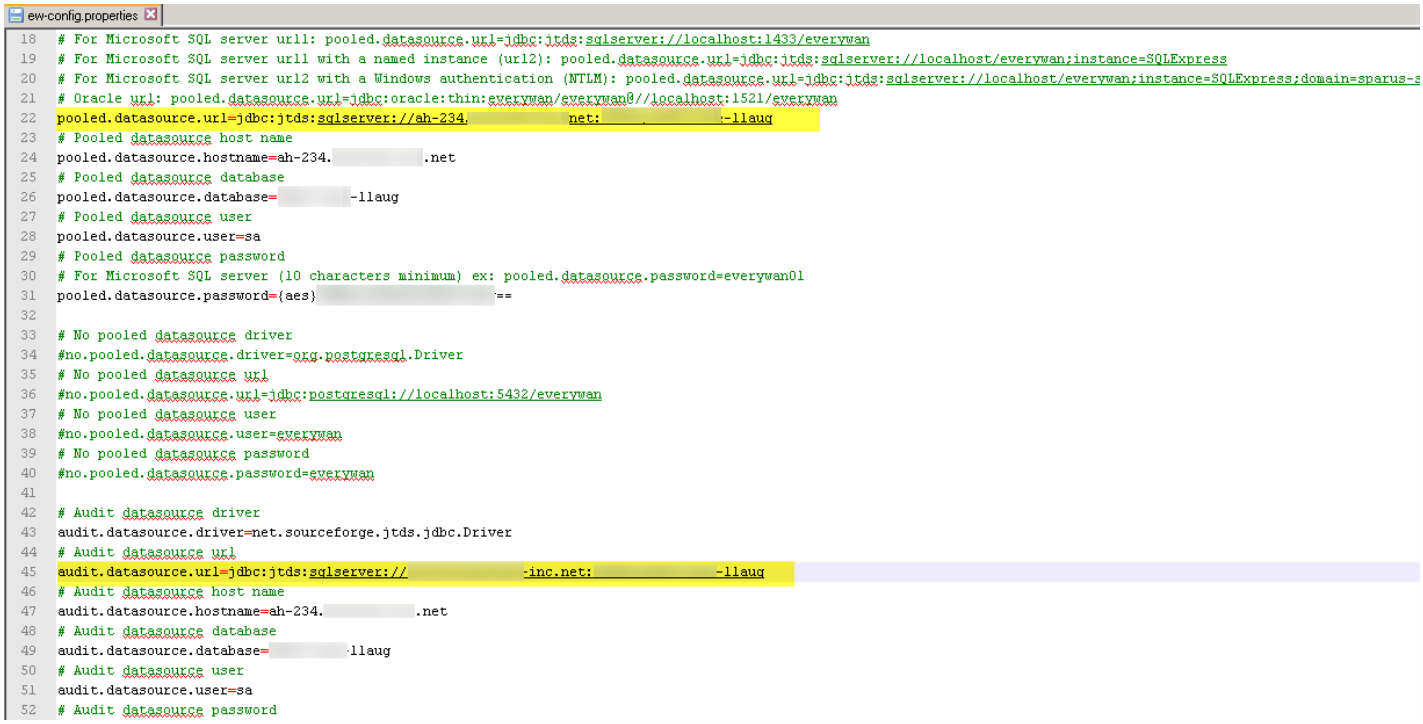
pooled.datasource.url=jdbc:jtds:sqlserver:// :64940/

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

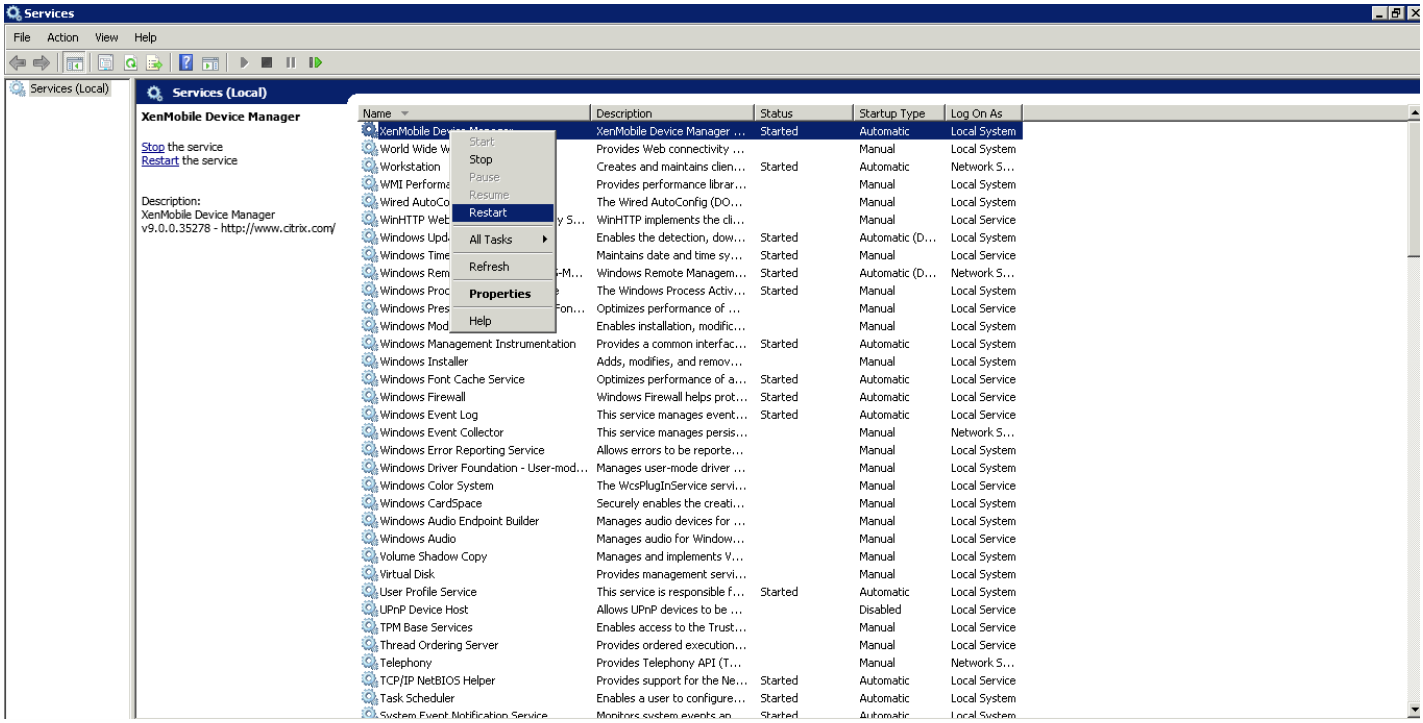
Ajoutez ";domain=" à la fin de l'adresse URL si le compte utilisateur appartient à un domaine.

> ## Remarque
>
> Citrix vous recommande d'effectuer une sauvegarde, une copie ou de prendre note des modifications que vous apportez au fichier ew-config.properties. Ces informations s'avèrent utiles si la migration échoue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

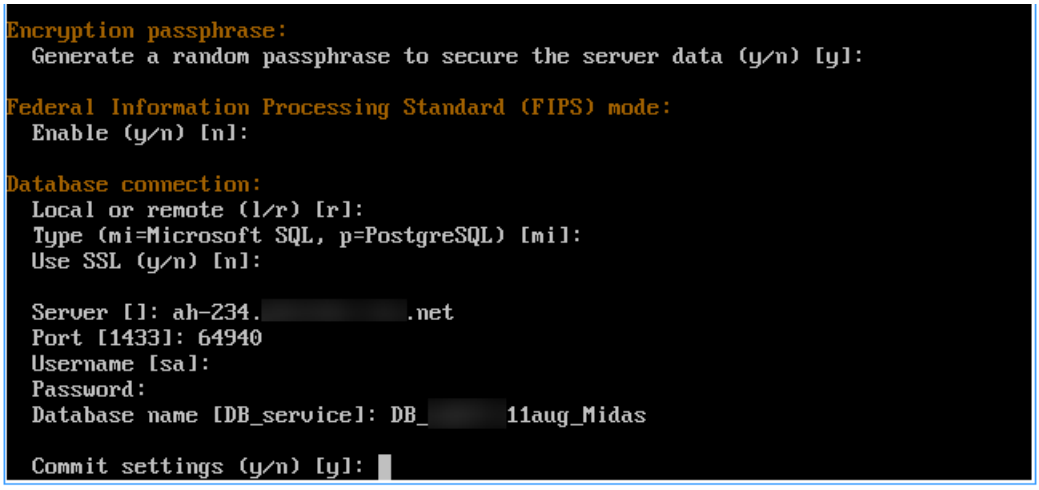


4. Redémarrez le service Device Manager. Actualisez les connexions aux appareils une fois l'instance de Device Manager redémarrée.



5. Déterminez si le nouveau serveur XenMobile 10 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 ; configurez ensuite le port statique sur le nouveau serveur XenMobile dans le cadre de la configuration de la base de données.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Suivez les étapes dans ces articles pour poursuivre la mise à niveau de votre environnement XenMobile :

- Pour mettre à niveau XenMobile 9.0 App Edition ou Enterprise Edition vers XenMobile 10.1, vous devez utiliser l'outil de mise à niveau de XenMobile Server App Edition, Enterprise Edition. Pour de plus amples informations, consultez la section Activation et exécution de l'outil de mise à niveau de XenMobile 10.1.
- Pour effectuer la mise à niveau de XenMobile 9.0 MDM Edition uniquement vers XenMobile 10.1, consultez la section Outil de mise à niveau de XenMobile 10 MDM.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de la mise en cluster pour XenMobile 10

Jul 25, 2016

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.

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 MDM bande L et une adresse IP privée pour 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 Aperçu de l'architecture.

Installation des nœuds de cluster XenMobile

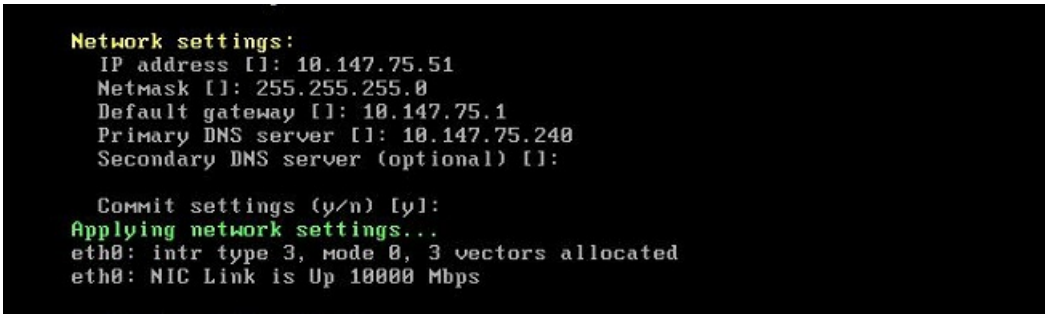
En fonction du nombre de nœuds requis, vous pouvez créer de nouvelles VM XenMobile. Pointez la nouvelle VM vers la même base de données et fournissez les mêmes mots de passe de certificat PKI.

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



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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



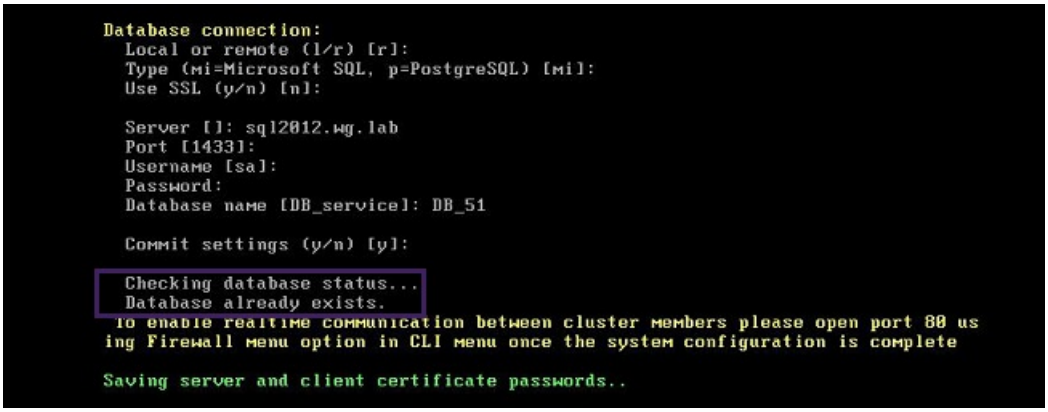
3. Si vous souhaitez utiliser le mot de passe par défaut pour la protection des données, tapezyou tapezn et entrez un nouveau mot de passe.



4. Si vous souhaitez utiliser la norme FIPS, tapezyou tapezn.

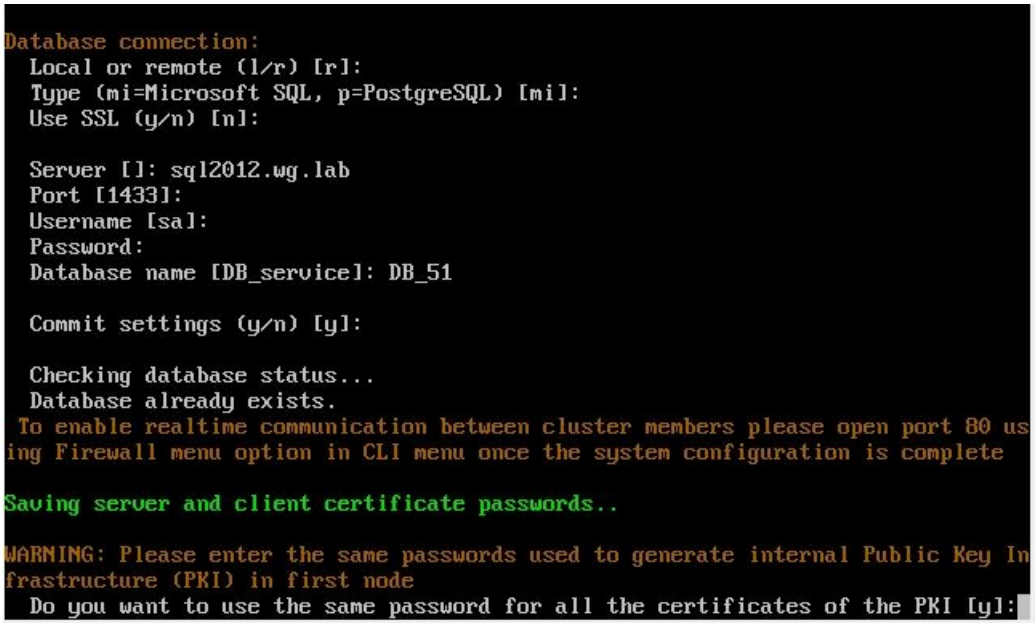


5. Configurez la base de données en pointant vers la base de données vers laquelle pointait la VM entièrement configurée auparavant. Le message suivant s'affiche : La base de données existe déjà.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

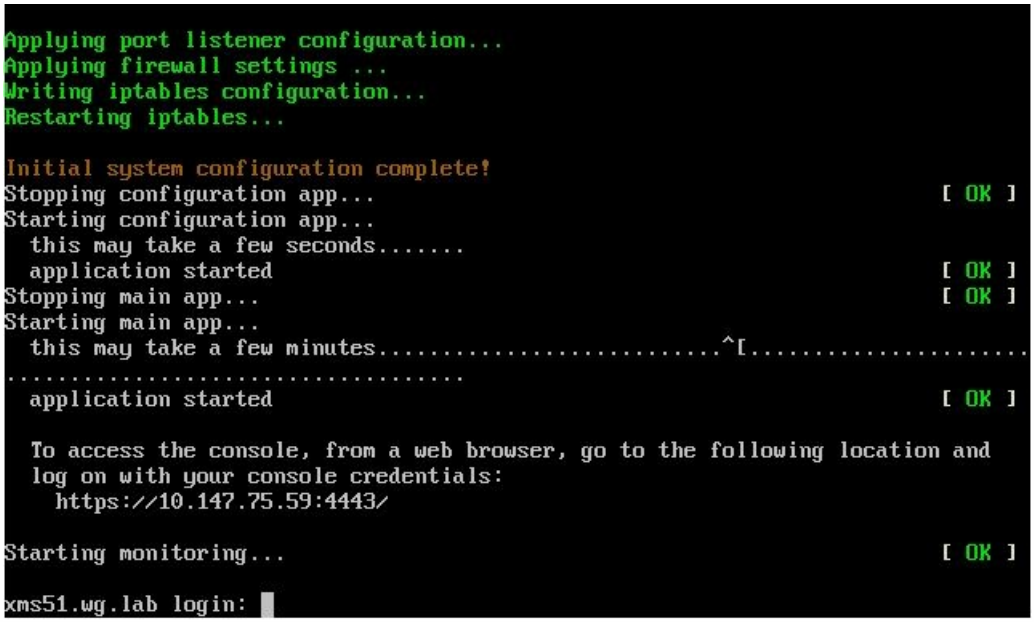


Une fois que vous avez entré le mot de passe, la configuration initiale sur le second nœud se termine.



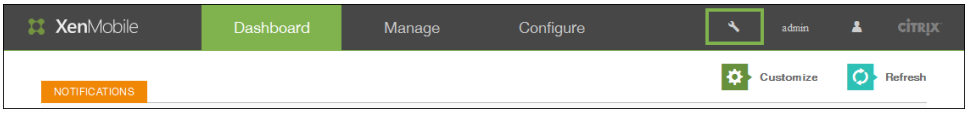
7. Une fois la configuration terminée, le serveur redémarre et la boîte de dialogue d'ouverture de session s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

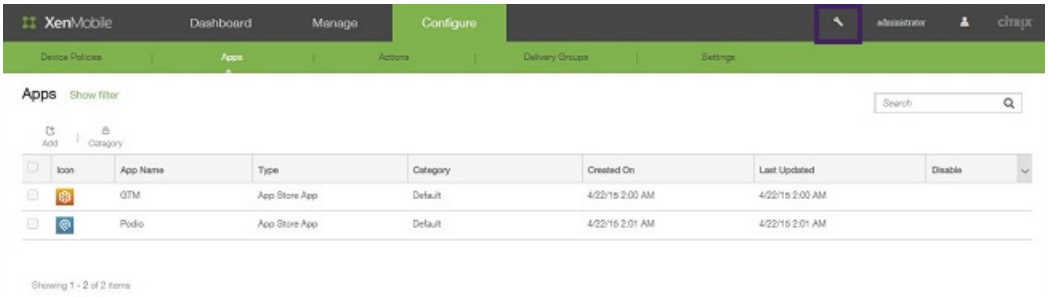


Remarque : la boîte de dialogue d'ouverture de session est identique à la boîte de dialogue d'ouverture de session de la première VM. Cette correspondance vous permet de vérifier que les deux VM utilisent le même serveur de base de données.

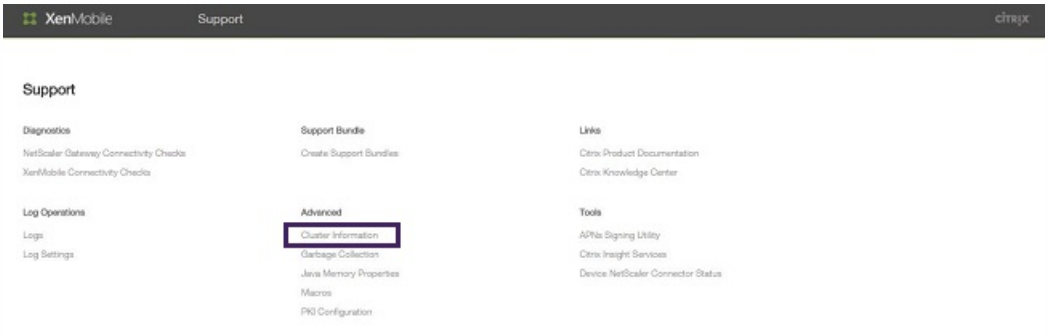
8. Utilisez le nom de domaine complet (FQDN) de XenMobile pour ouvrir la console XenMobile dans un navigateur Web.
9. Sur le tableau de bord, cliquez sur l'icône d'outils dans le coin supérieur droit de l'écran.



La page Support s'ouvre.

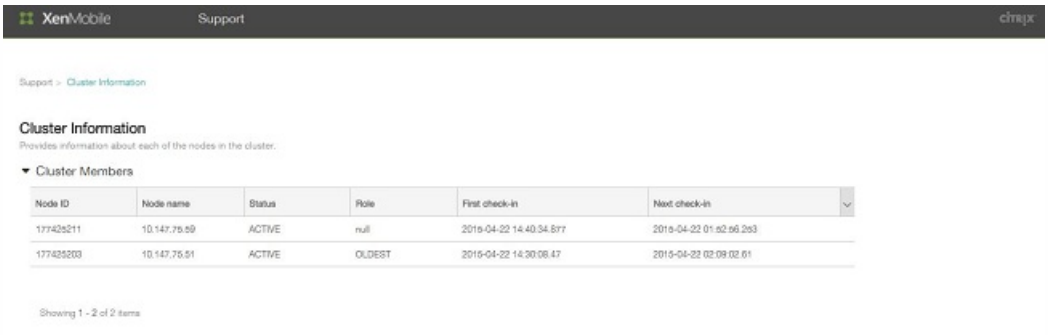


10. Sous Avancé, cliquez sur Informations de cluster.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

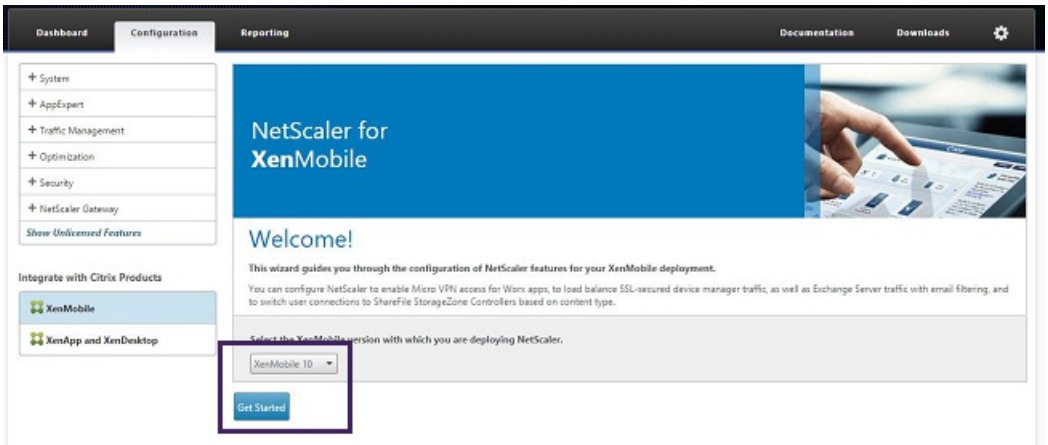
Pour configurer l'équilibrage de charge pour le cluster XenMobile dans NetScaler

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.

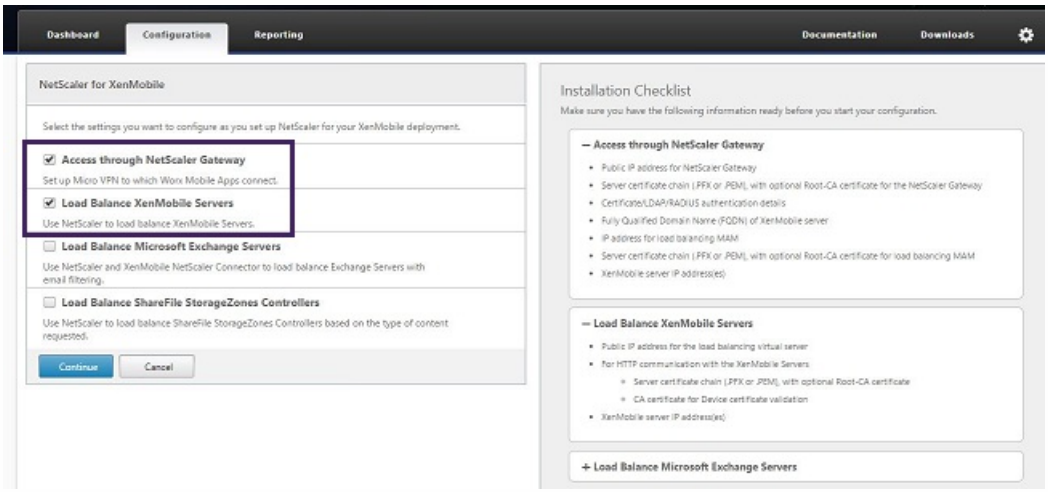


2. Sur l'onglet Configuration, cliquez sur XenMobile, puis sur Get Started.

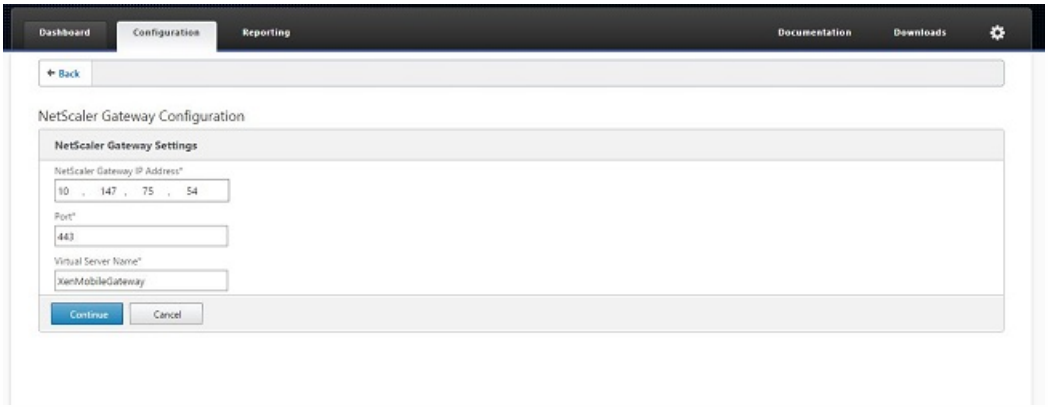


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

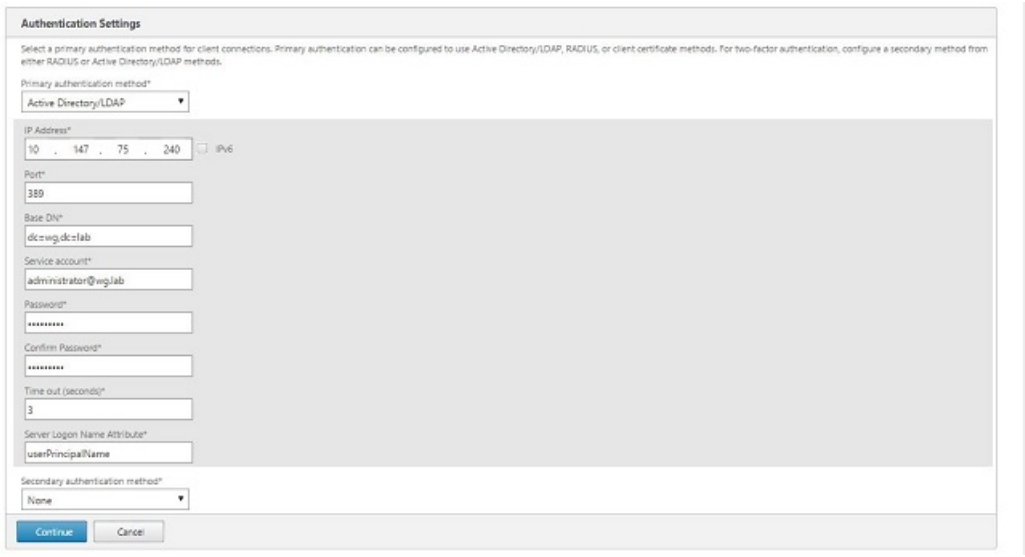


5. Liez le certificat de serveur à l'adresse IP virtuelle de NetScaler Gateway en effectuant l'une des opérations suivantes, puis cliquez sur Continue.
   - Dans Use existing certificate, sélectionnez le certificat de serveur dans la liste.
   - Cliquez sur l'onglet Install Certificate pour charger un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



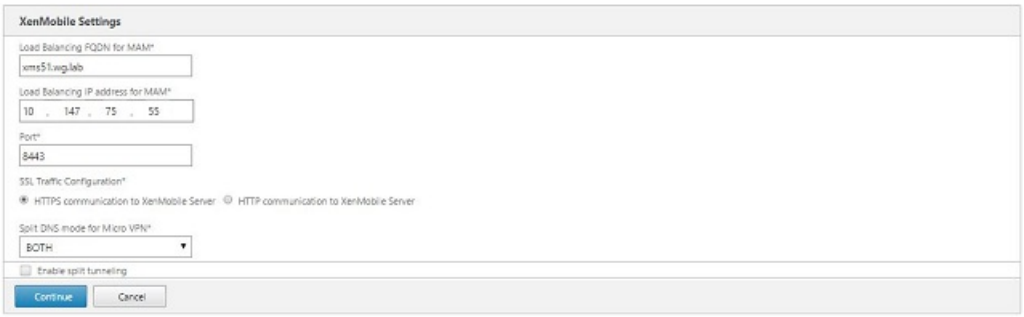
6. Entrez les détails du serveur d'authentification, puis cliquez sur Continue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

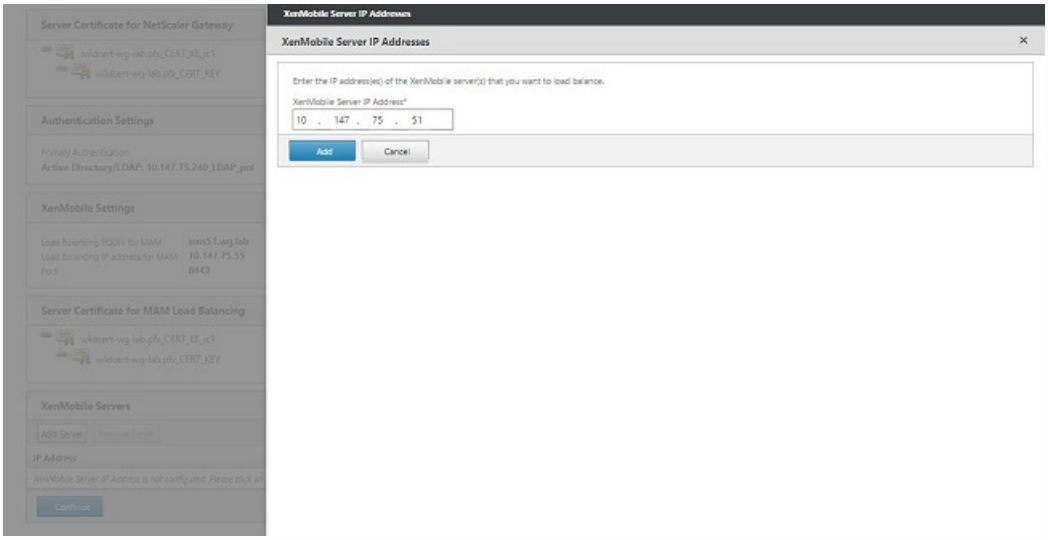


10. Sous XenMobile Servers, cliquez sur Add Server pour ajouter les nœuds XenMobile.

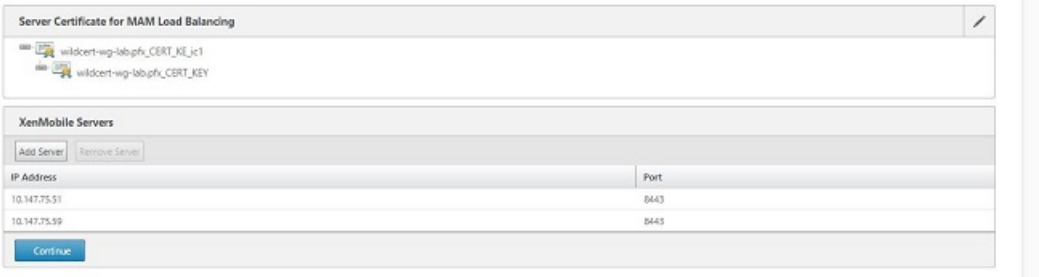
© 1999-2017 Citrix Systems, Inc. All rights reserved.



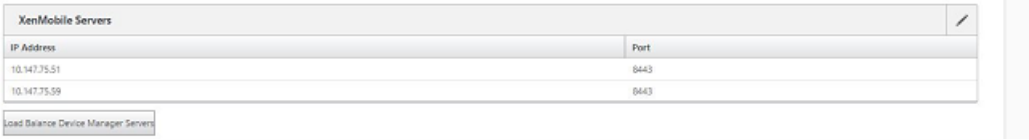
11. Entrez l'adresse IP du nœud XenMobile, puis cliquez sur Add.



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 sur Continuer.

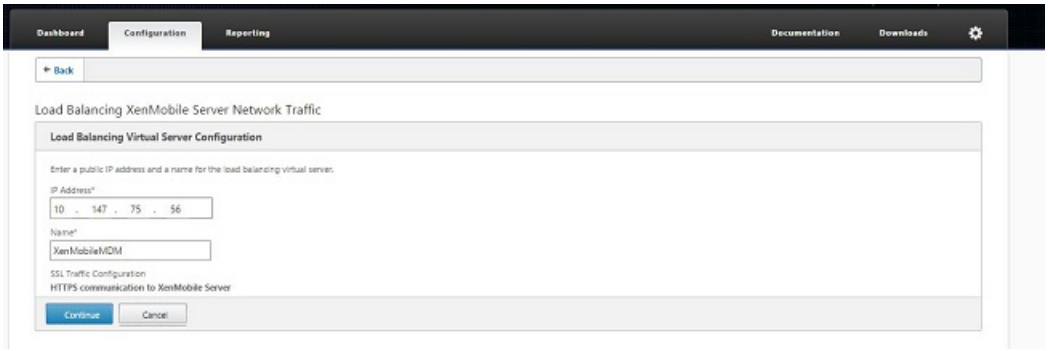


13. Cliquez sur Load Balance Device Manager Servers pour continuer la configuration de l'équilibrage de charge MDM.

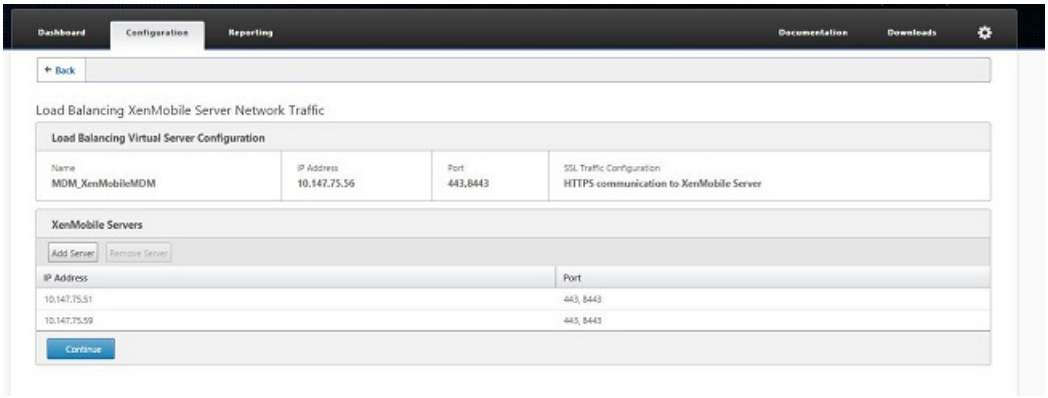


14. Entrez l'adresse IP à utiliser pour l'équilibrage de charge MDM, puis cliquez sur Continue.

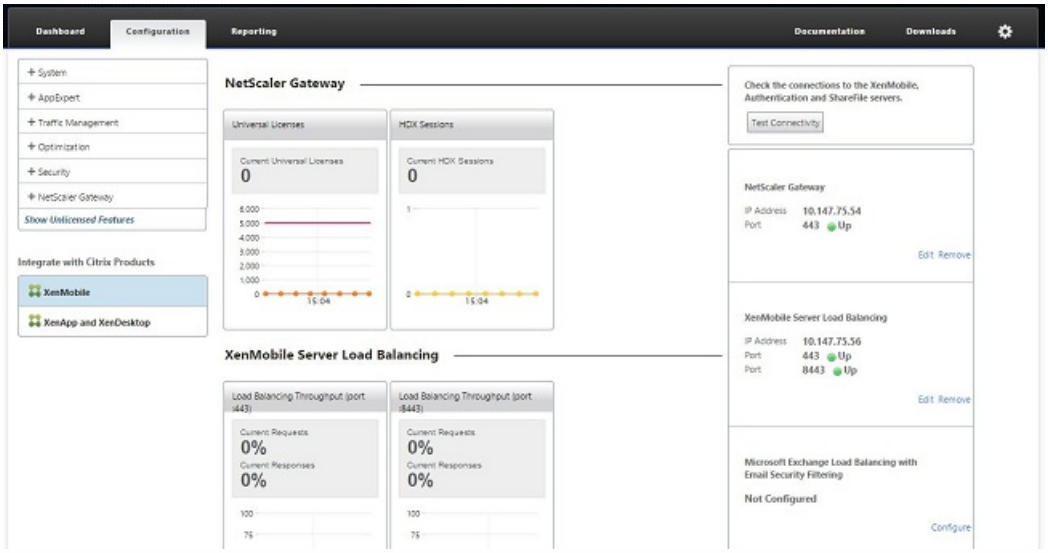
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

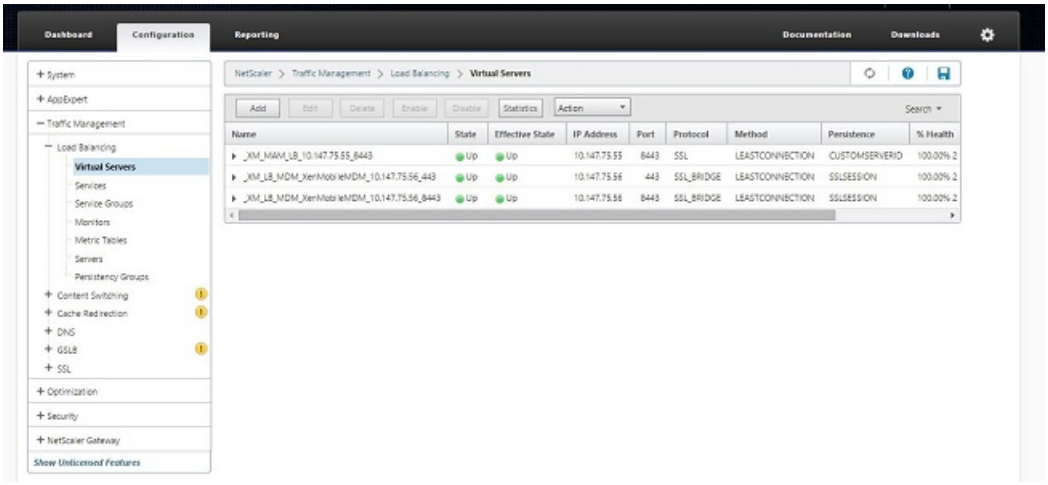


Vous verrez l'état de l'adresse IP virtuelle sur la page XenMobile.

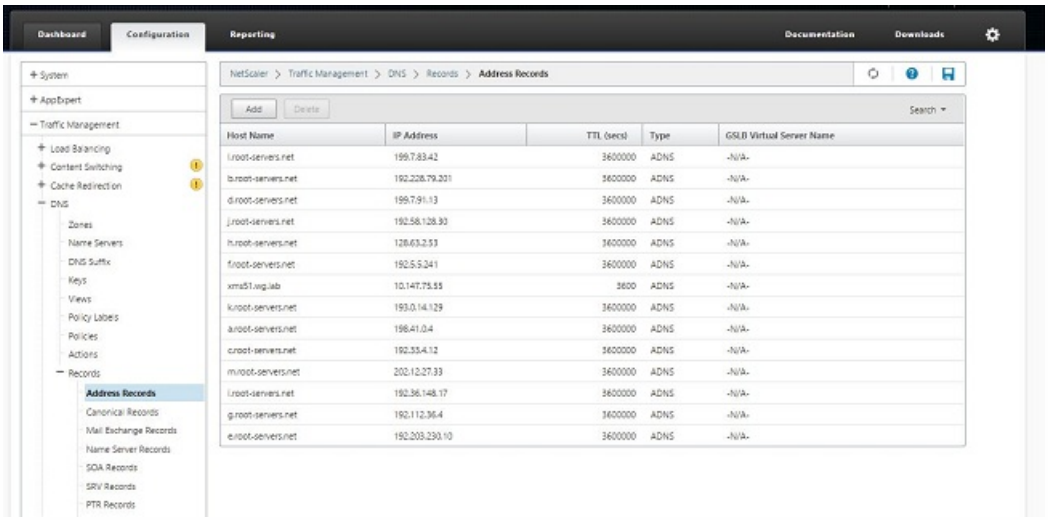


16. Pour vérifier que les adresses IP virtuelles sont opérationnelles, cliquez sur l'onglet Configuration, puis accédez à Traffic Management > Load Balancing > Virtual Servers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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



© 1999-2017 Citrix Systems, Inc. All rights reserved.

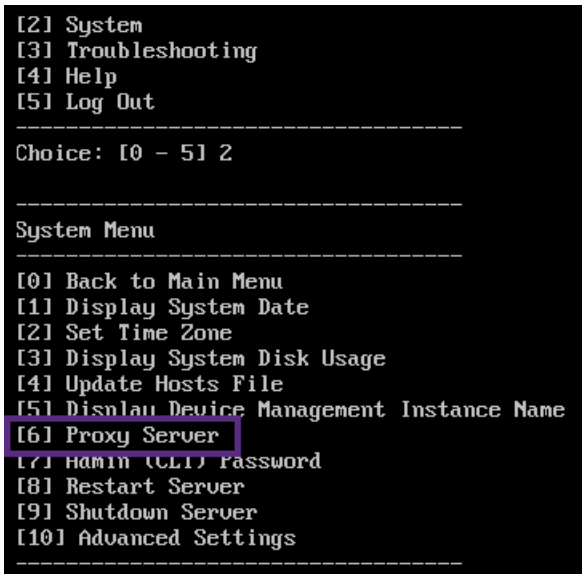
Activation des serveurs proxy dans XenMobile

Jul 25, 2016

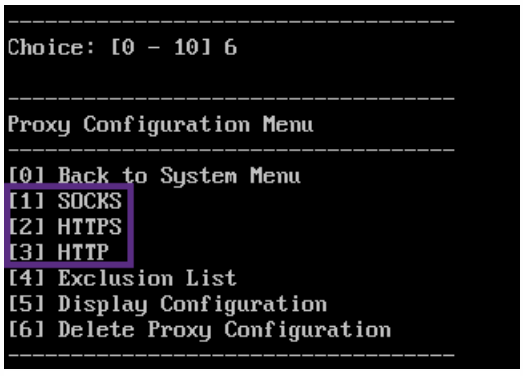
Lorsque vous souhaitez contrôler le trafic Internet sortant, vous pouvez configurer un serveur proxy dans XenMobile pour acheminer ce trafic. Pour ce faire, vous devez configurer le serveur proxy par le biais de l'interface de ligne de commande (CLI). Veuillez noter que la configuration du serveur proxy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

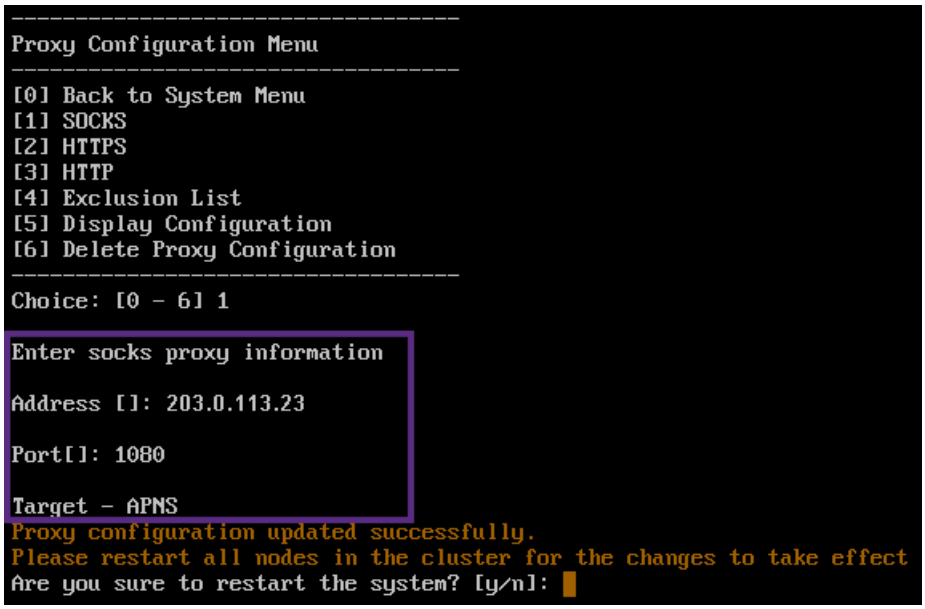


4. Entrez l'adresse IP de votre serveur proxy, le numéro de port et une cible. Reportez-vous au tableau suivant pour consulter la liste des types de cibles prises en charge pour chaque type de serveur proxy.

Type de proxy	Cibles prises en charge

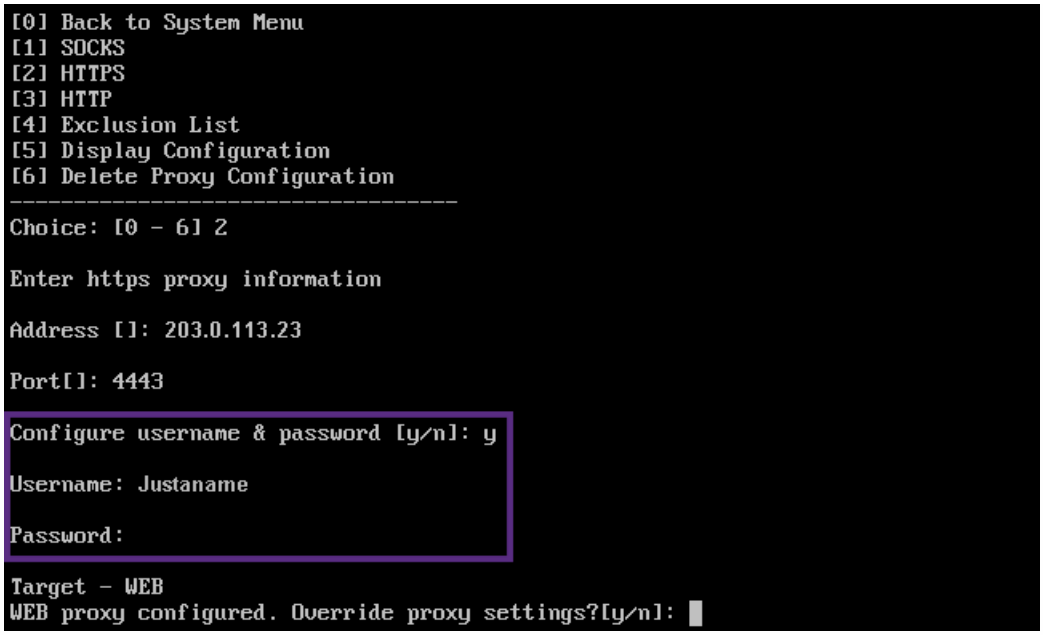
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Système de licences

Jul 25, 2016

XenMobile et NetScaler Gateway requièrent des licences. Pour plus d'informations sur le système de licences NetScaler Gateway, consultez la section Installation de licences sur 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**
>
> XenMobile 10.1 requiert le serveur de licences Citrix 11.12.1 ou une version ultérieure ; les versions antérieures du serveur ne fonctionnent pas avec XenMobile 10.1.

> **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 après l'installation. L'accès à la console Web XenMobile n'est jamais bloqué, qu'une licence XenMobile valide soit disponible ou non.

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

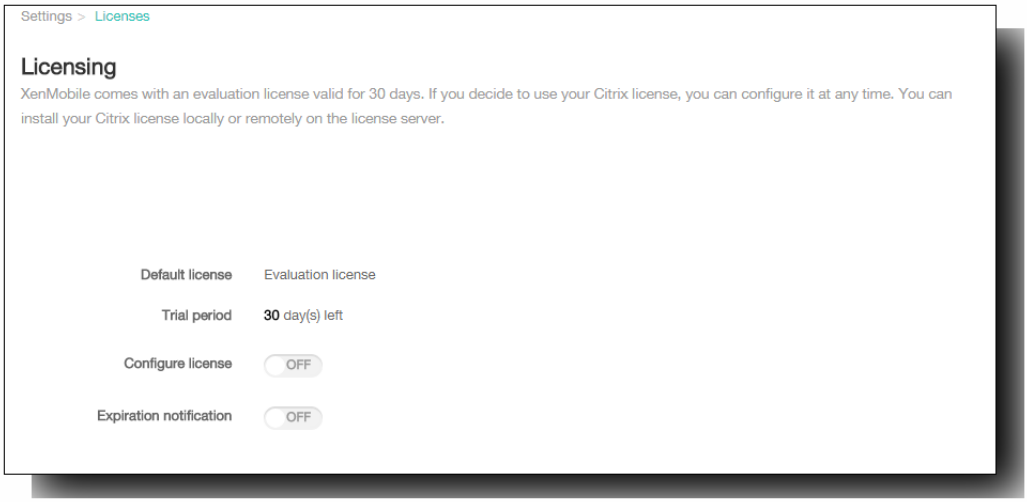
Lorsqu'une licence XenMobile expire, toutes les fonctionnalités de gestion d'appareil deviennent indisponibles. Par exemple, de nouveaux utilisateurs ou de nouveaux appareils ne peuvent pas être inscrits et les applications et les configurations

© 1999-2017 Citrix Systems, Inc. All rights reserved.

déployées sur les appareils inscrits ne peuvent pas être mises à jour.

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 Configurer > Paramètres.
2. Cliquez sur Licences. La page Licences s'ouvre.

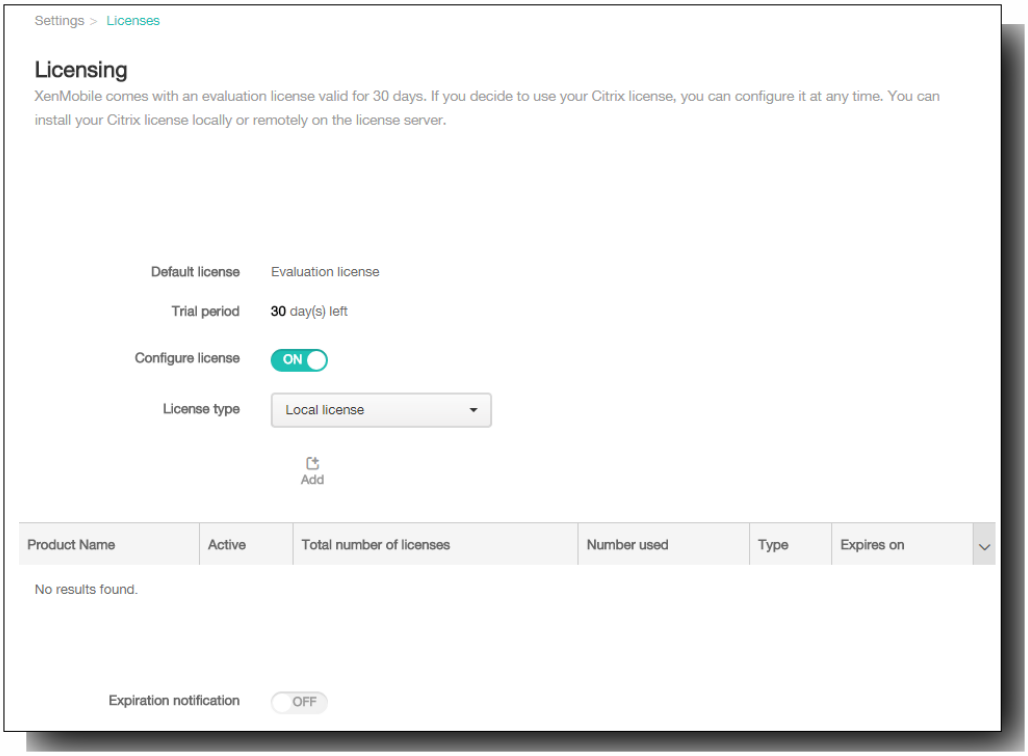
Pour ajouter une licence locale

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.

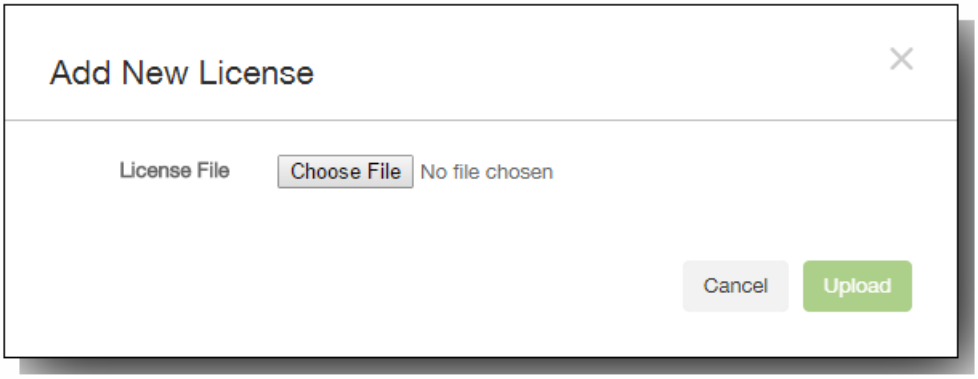
Vous pouvez gérer toutes les licences locales via la console XenMobile.

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, cliquez sur Configurer > Paramètres > Licences. La page Licences s'ouvre.
3. Définissez Configurer licence sur On. La liste Type de licence, le bouton Ajouter, et le tableau des licences apparaissent. Le tableau des licences contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

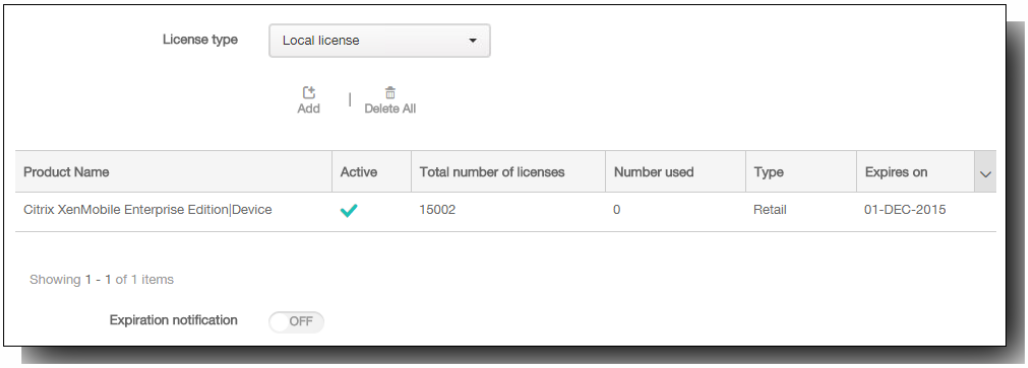


4. Vérifiez que le type de licence est défini sur licence locale, puis cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle licence apparaît.



5. Dans la boîte de dialogue Ajouter une nouvelle licence, cliquez sur Choisir un fichier, puis recherchez votre licence.
6. Cliquez sur Charger. Les licences sont chargées localement et s'affichent dans le tableau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

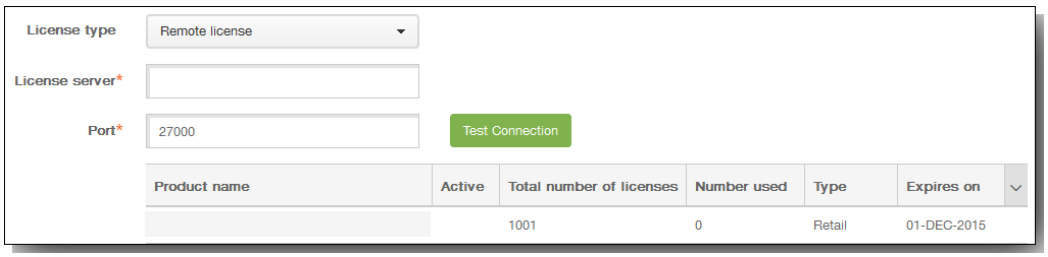


7. Lorsque la licence s'affiche dans le tableau sur la page Licences, activez-la. S'il ne s'agit pas de la première licence dans le tableau, la licence est activée automatiquement.

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 des licences apparaissent. Le tableau des licences contient les licences que vous avez utilisées avec XenMobile. Si vous n'avez pas encore ajouté de licence Citrix, le tableau est vide.
2. 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.



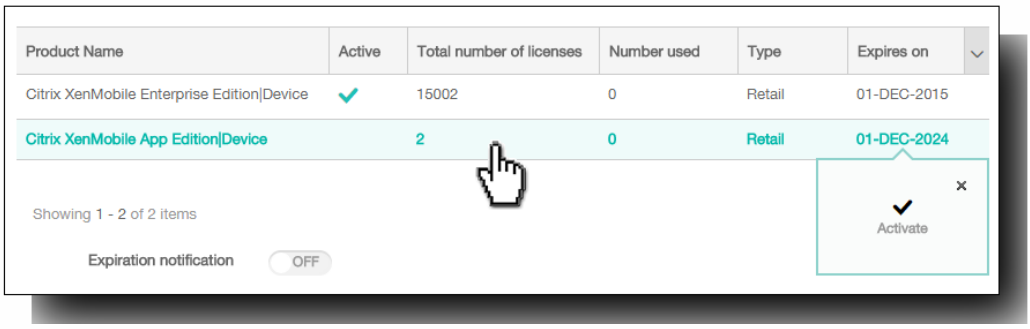
3. Dans Serveur de licences, entrez l'adresse IP ou le nom de domaine complet (FQDN) de votre serveur de licences distant.
4. Dans le champ Port, acceptez le port par défaut ou saisissez le numéro de port utilisé pour communiquer avec le serveur de licences.
5. Cliquez sur Tester la connexion. Si la connexion est établie, XenMobile se connecte au serveur de licences et le tableau des licences est renseigné avec les licences disponibles. Si la connexion échoue, vérifiez que vous avez fourni les informations correctes et que toutes les connexions sont actives.
   Remarque : s'il n'existe qu'une seule licence, elle est activée automatiquement.

Pour activer une autre licence

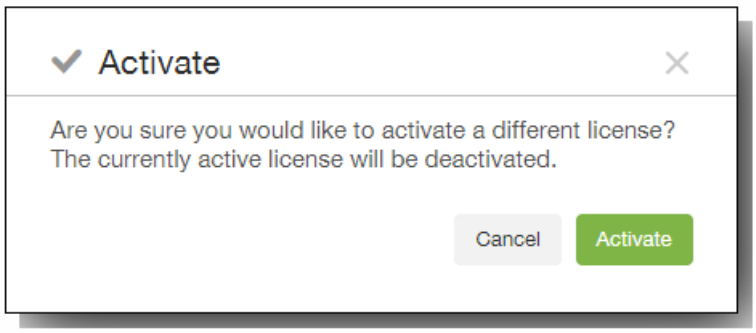
Si vous disposez de plusieurs licences, vous pouvez choisir la licence que vous souhaitez activer. Vous ne pouvez disposer que d'une seule licence active à la fois.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

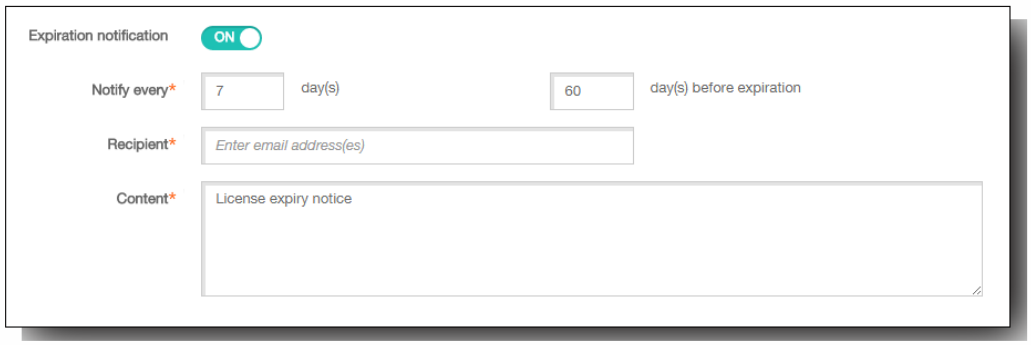


3. Cliquez sur Activer.
   Important : si vous activez la licence sélectionnée, la licence actuellement active est désactivée.
   La licence sélectionnée est activée.

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. Dans Notifier chaque, entrez :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

3. Dans le champ Destinataire, entrez votre adresse e-mail ou l'adresse e-mail de la personne responsable de la licence.
4. Dans le champ Contenu, entrez un message de notification d'expiration à l'attention du destinataire.
5. Cliquez sur Enregistrer. En se basant sur le nombre de jours avant l'expiration, XenMobile commence à envoyer des messages contenant le texte que vous avez fourni lors de ce processus aux destinataires que vous avez spécifiés. Les notifications sont répétées en fonction de la fréquence que vous avez définie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

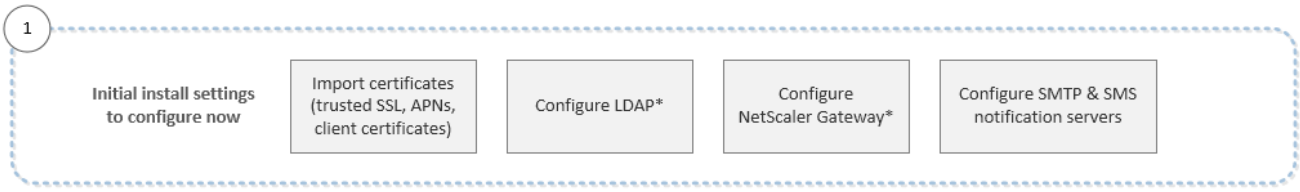
Prise en main de la console XenMobile

Jul 25, 2016

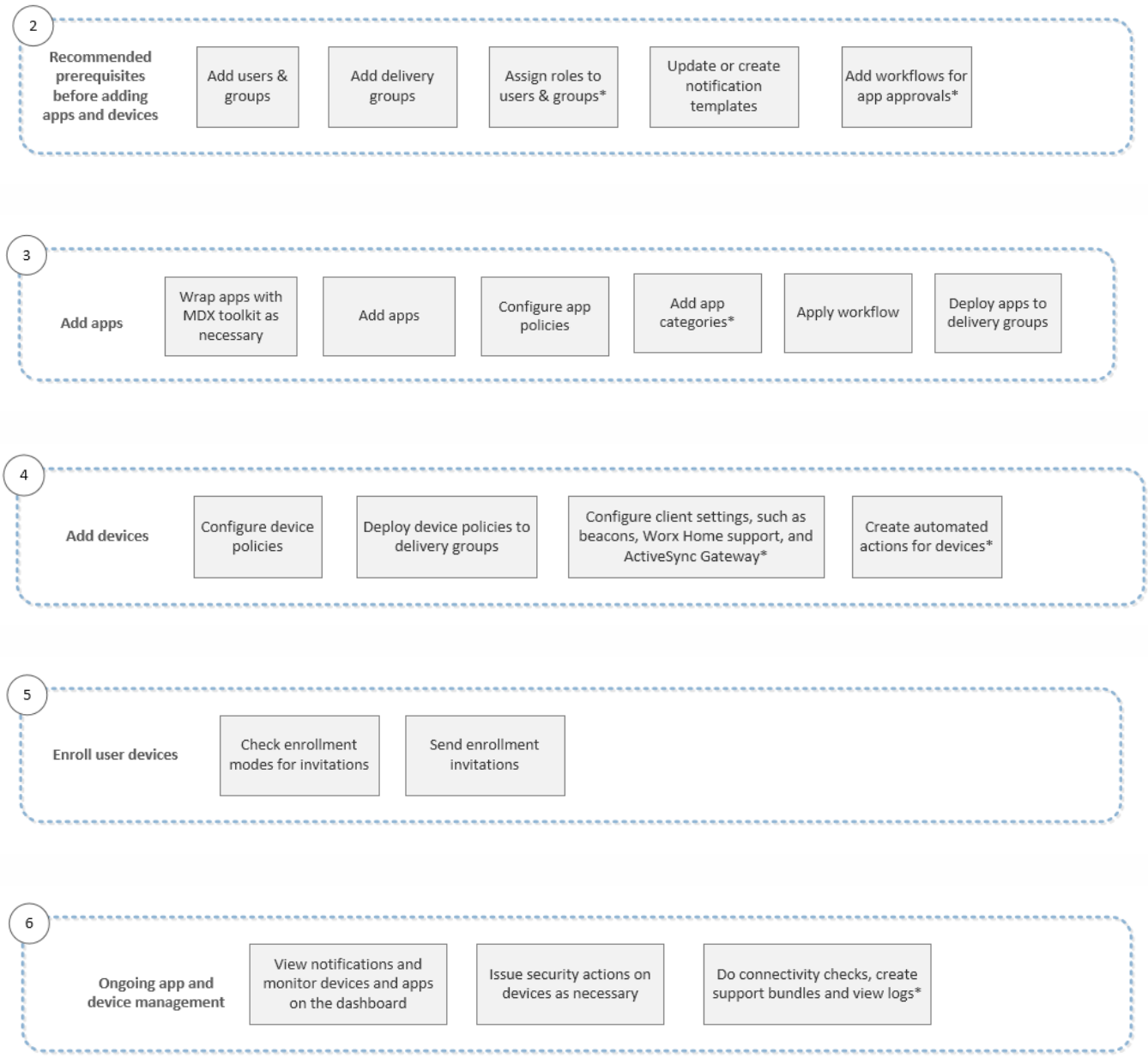
La console XenMobile est l'outil de gestion unifiée dans XenMobile qui combine les composants App Controller et Device Manager de XenMobile 9 et des versions antérieures. Cette rubrique suppose que vous avez installé XenMobile et que vous êtes prêt à travailler dans la console. Si vous devez installer XenMobile, consultez la section Installation de XenMobile.
la console XenMobile est prise en charge dans les deux versions les plus récentes de Firefox, Chrome et Internet Explorer.
La figure suivante montre un exemple du tableau de bord qui s'affiche lorsque vous vous connectez à la console Web XenMobile.



Pour de plus amples informations sur les autres étapes à suivre dans la console, l'illustration suivante affiche un workflow recommandé conçu pour vous préparer à gérer des applications et des appareils. La première série de recommandations couvre les paramètres initiaux que vous avez peut-être ignorés durant les étapes d'installation.
Conseil : cliquez sur chaque ligne pour ouvrir une rubrique avec plus de détails et des liens vers les procédures.
Remarque : les éléments marqués d'un astérisque sont facultatifs.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



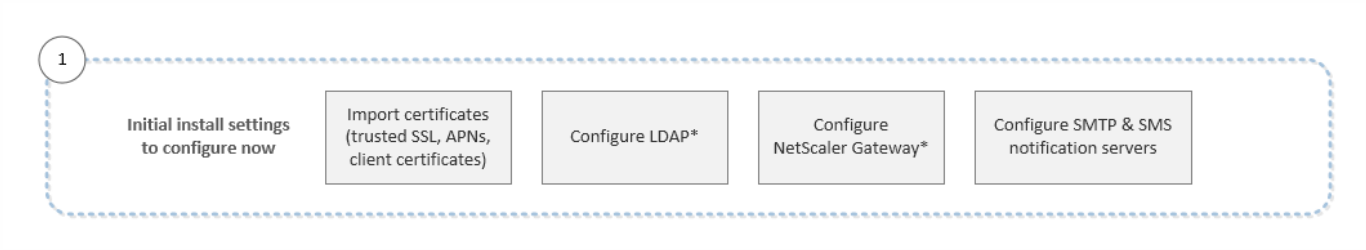
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow des paramètres initiaux

Jul 25, 2016

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 **Configurer** > **Paramètres**. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console 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 suivants de la documentation des produits Citrix :

- Certificats dans XenMobile
- Configuration du LDAP
- NetScaler Gateway et XenMobile
- Notifications dans XenMobile

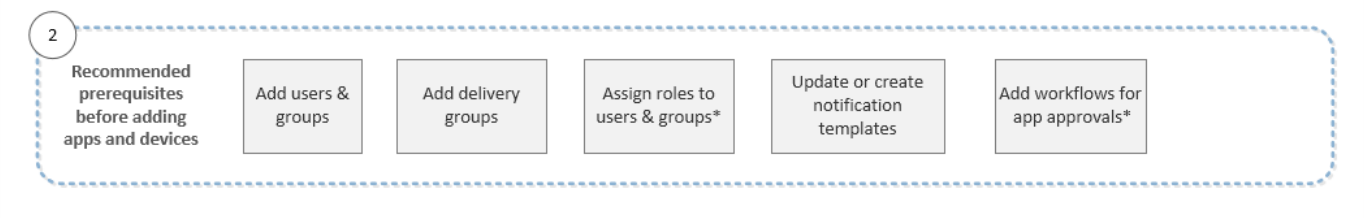
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow de la configuration requise pour la console

Jul 25, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

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 suivants de la documentation des produits Citrix :

- Configuration de comptes utilisateur, de rôles et de paramètres d'inscription
- Gestion des groupes de mise à disposition dans XenMobile
- Pour créer ou mettre à jour des rôles personnalisés dans XenMobile avec RBAC
- Pour créer ou mettre à jour des modèles de notification dans XenMobile
- Pour configurer des modes d'inscription et activer le portail en libre-service
- Création et gestion de workflows

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow d'ajout d'applications

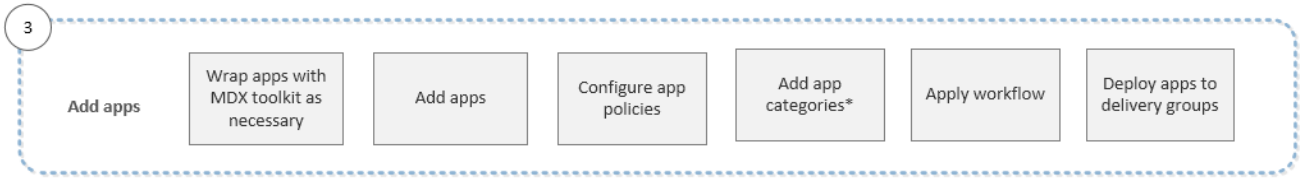
Jul 25, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux.

Ensuite, vous pouvez configurer certains prérequis avant d'ajouter des applications et des appareils en suivant le Workflow de la configuration requise pour la console. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

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 suivants de la documentation des produits Citrix :

- À propos de MDX Toolkit
- Ajout d'applications à XenMobile
- Synopsis des stratégies MDX pour iOS, Android et Windows Phone 8.1
- Pour ajouter des catégories d'applications
- Création et gestion de workflows
- Gestion des groupes de mise à disposition dans XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow d'ajout d'appareils

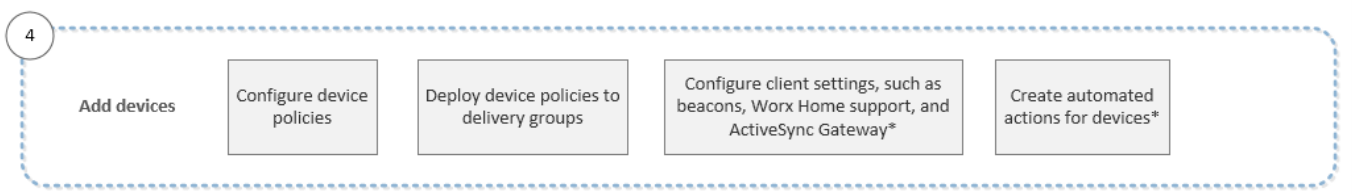
Jul 25, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux.

Ensuite, vous pouvez configurer certains prérequis avant d'ajouter des applications et des appareils en suivant le Workflow de la configuration requise pour la console. Ensuite, vous pouvez ajouter des applications en suivant les instructions de la section Workflow d'ajout d'applications. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

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 suivants de la documentation des produits Citrix :

- Ajout d'appareils et affichage des détails des appareils dans XenMobile
- Stratégies XenMobile par plate-forme
- Gestion des groupes de mise à disposition dans XenMobile
- Configuration des paramètres du client XenMobile
- Création d'actions automatisées dans XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

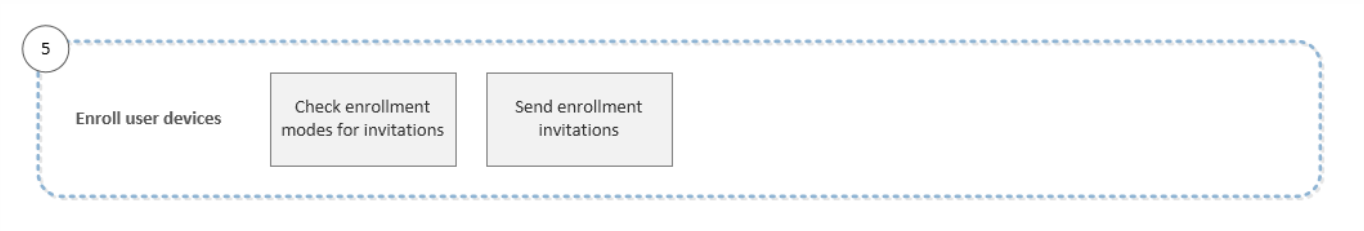
Workflow d'inscription d'appareils utilisateur

Jul 25, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux.

Ensuite, vous pouvez configurer certains prérequis avant d'ajouter des applications et des appareils en suivant le Workflow de la configuration requise pour la console. Ensuite, vous pouvez ajouter des applications en suivant les instructions de la section Workflow d'ajout d'applications et ajouter et enregistrer des appareils en suivant les instructions de la section Workflow d'ajout d'appareils. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

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 :

- Configuration de comptes utilisateur, de rôles et de paramètres d'inscription
- Pour configurer des modes d'inscription et activer le portail en libre-service

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Workflow de gestion des applications et appareils

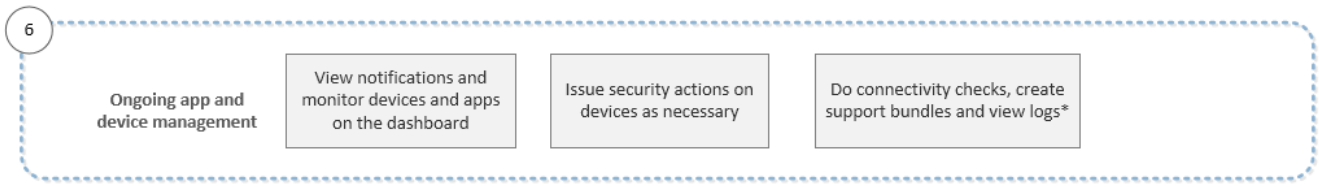
Jul 25, 2016

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. Si vous avez ignoré certaines configurations, vous pouvez afficher les paramètres initiaux recommandés dans Workflow des paramètres initiaux.

Ensuite, vous pouvez configurer certains prérequis avant d'ajouter des applications et des appareils en suivant le Workflow de la configuration requise pour la console. Ensuite, vous pouvez ajouter des applications en suivant les instructions de la section Workflow d'ajout d'applications et ajouter et enregistrer des appareils en suivant les instructions de la section Workflow d'ajout d'appareils. Une fois que vous avez terminé les quatre premiers workflows, inscrivez les appareils utilisateur en suivant les instructions de la section Workflow d'inscription d'appareils utilisateur. Pour afficher l'ensemble du workflow, reportez-vous à la section Prise en main de la console XenMobile.

Ce sixième et dernier 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 Support et maintenance de XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Filtres et tableaux dans la console XenMobile

Jul 25, 2016

Vous pouvez rechercher des filtres et des tableaux dans la console XenMobile. Ils figurent sur les onglets principaux Appareils, Inscription, Stratégies d'appareil, Applications, Actions et Groupes de mises à disposition, ainsi que sur la plupart des pages sous l'onglet Paramètres, telles que Groupes et utilisateurs locaux. Les filtres vous permettent d'affiner les informations dans toutes ces zones de la console afin de localiser les informations exactes que vous voulez afficher ou pour lesquelles vous souhaitez entreprendre une action. Dans les tableaux, vous pouvez cliquer sur un ou plusieurs éléments afin d'afficher les options que vous pouvez effectuer sur les éléments sélectionnés. Les options peuvent changer en fonction du nombre d'éléments que vous sélectionnez.

Le tableau suivant répertorie les options les plus courantes ainsi que leur emplacement.

Option de menu	Action	Tableau où l'option apparaît
Ajouter	Ajouter un nouvel élément au tableau.	Tous
Catégorie	Ajouter et gérer des catégories pour les applications.	Applications
Copier l'URL	Copier l'URL dans le Presse-papiers.	Inscription
Supprimer ou Tout supprimer	Supprimer définitivement les éléments sélectionnés.	Tous
Déployer	Déployer des ressources auprès d'utilisateurs et d'appareils.	Appareils et groupes de mise à disposition
Désactiver	Désactiver une application ou le groupe de mise à disposition AllUsers.	Applications et groupes de mise à disposition
Modifier	Apporter des modifications à un élément existant.	Tous, sauf Inscription
Exporter	Envoyer le contenu du tableau dans un fichier .csv.	Tous
Importer	Ajouter des appareils à partir d'un fichier de provisioning.	Appareils
	Ajouter des utilisateurs et des groupes locaux à partir d'un fichier.	Utilisateurs et groupes locaux
Gérer les groupes locaux	Ajouter un groupe local pour la gestion.	Utilisateurs et groupes locaux
Notifier	Envoyer une notification aux utilisateurs et appareils sélectionnés.	Inscription et appareils
Actualiser	Mettre à jour le tableau.	Appareils

© 1999-2017 Citrix Systems, Inc. All rights reserved.

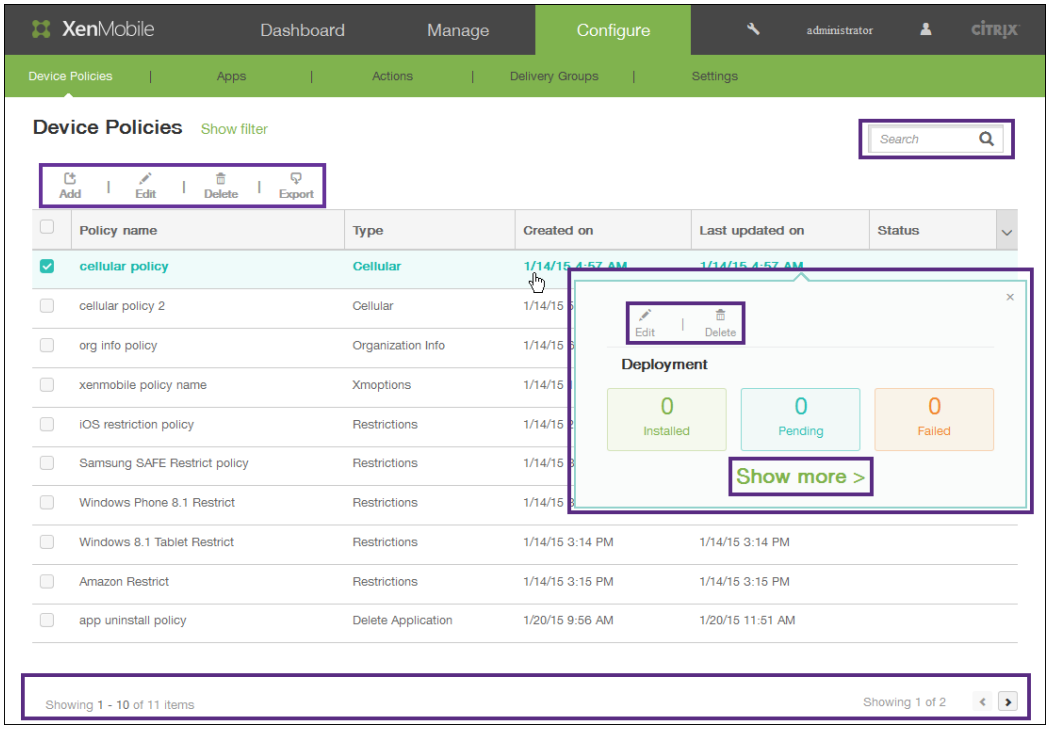
Option de menu	Action	Tableau où l'option apparaît
Sécuriser	Appeler des actions sur l'appareil sélectionné.	Appareils
Portail en libre-service	Activer le portail libre-service en tant que mode d'inscription.	Inscription
Mettre à jour	Mettre à jour les valeurs dans un tableau.	Gestion des versions

Pour afficher les options dans les tableaux de la console XenMobile

Pour réaliser des actions sur les informations présentes dans les tableaux de la console, vous pouvez afficher les différentes options de plusieurs manières différentes :

- Vous pouvez sélectionner la case à cocher en regard d'un élément pour afficher le menu d'options au-dessus de la liste.
- Vous pouvez sélectionner la case à cocher en regard de plusieurs éléments pour exécuter une action sur tous ces éléments simultanément. Les actions que vous pouvez exécuter sur plusieurs éléments dépendent du tableau que vous consultez.
- Vous pouvez cliquer sur un élément dans la liste pour afficher le menu d'options sur le côté droit de la liste. Lorsque vous cliquez sur Afficher plus, des détails sur cet élément s'afficheront. Ce que vous voyez dépend du tableau que vous consultez.
- Vous pouvez entrer un nom complet ou partiel dans la zone Rechercher pour limiter le nombre d'éléments répertoriés.

La figure suivante montre comment les options apparaissent dans la zone Stratégies d'appareil de la console. Seuls 10 éléments sont affichés par page. Cliquez sur les triangles dans la partie inférieure droite de la page pour vous déplacer d'une page à l'autre.



Pour filtrer les informations dans la console XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

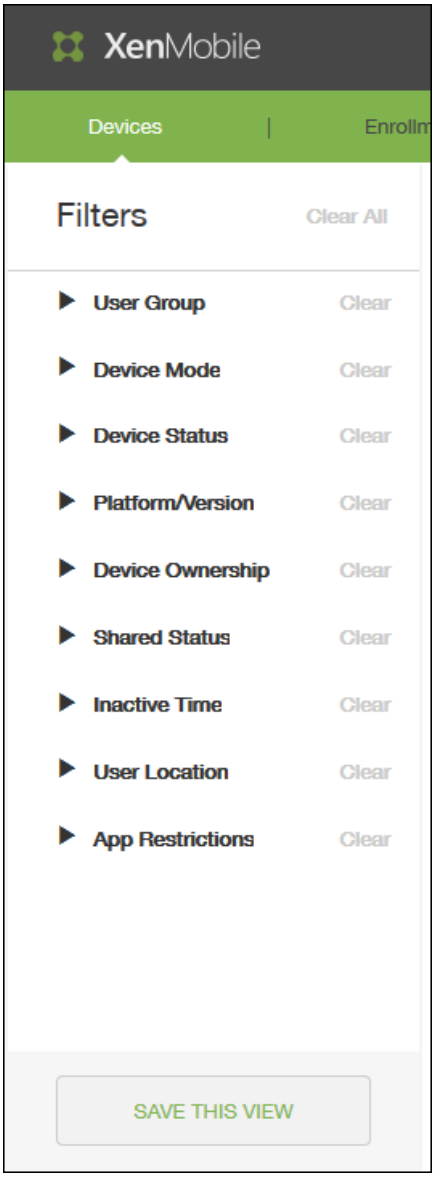
Lorsque vous voulez afficher un sous-ensemble spécifique d'informations dans une zone de la console, tel que Appareils, Inscription, Stratégies d'appareil, Applications, Actions, Groupes de mise à disposition et Groupes et utilisateurs locaux, vous pouvez filtrer la liste en fonction de critères que vous sélectionnez. Cette procédure utilise la page Appareils comme exemple, mais les étapes permettant de filtrer les résultats sont identiques dans toute la console.

1. Sur la page Appareils, cliquez sur Afficher le filtre.



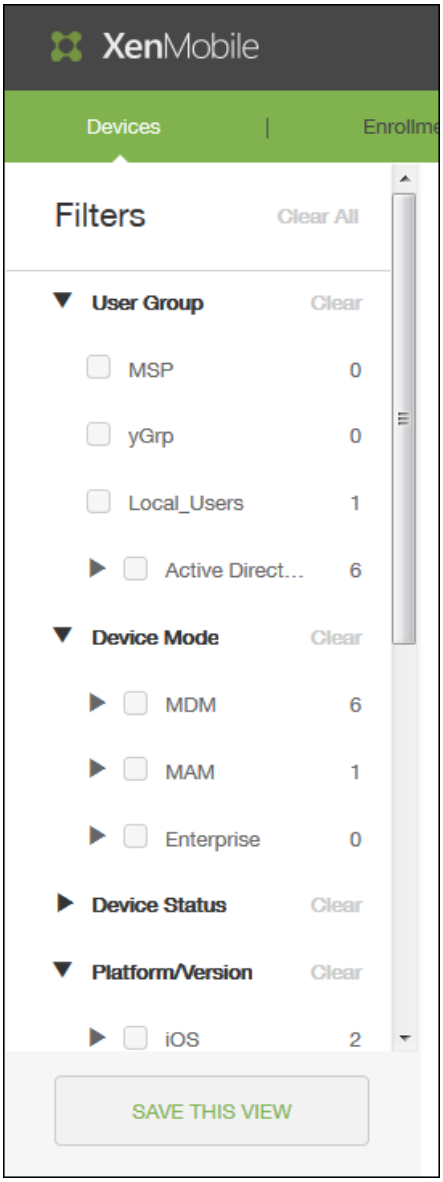
Le panneau de filtre apparaît et répertorie les critères que vous pouvez appliquer pour filtrer la liste Appareils. Lorsque vous affichez le filtre pour la première fois, tous les critères sont réduits.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



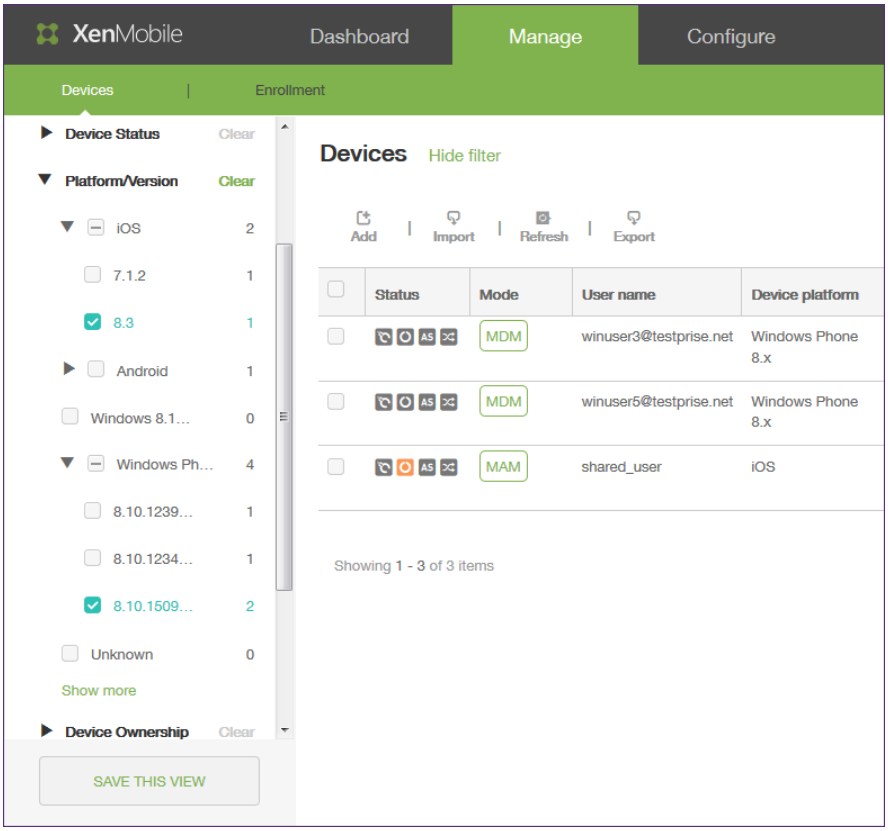
2. Cliquez sur le triangle à gauche d'un filtre pour afficher les critères disponibles pour ce filtre. Les chiffres à droite de chaque critère représentent le nombre d'appareils qui remplissent ce critère.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

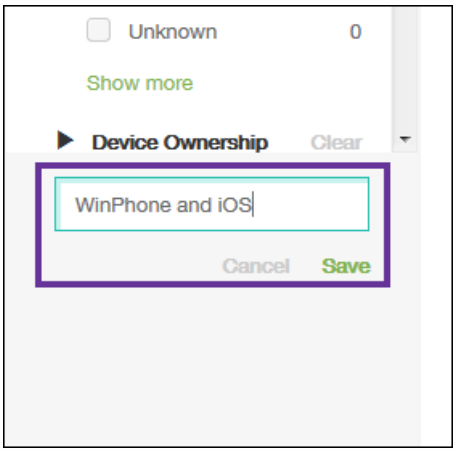


3. Sélectionnez le critère de filtration à utiliser. La liste Appareils est limitée aux appareils qui répondent aux critères sélectionnés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Procédez comme suit :
   - Cliquez sur Masquer le filtre pour continuer à travailler avec la liste filtrée.
   - Cliquez sur Tout effacer pour revenir à la liste complète.
   - Cliquez sur Effacer en regard d'un critère spécifique pour supprimer ce filtre et supprimer ces éléments dans la liste filtrée.
5. Si vous voulez enregistrer les critères sélectionnés en tant que filtre personnalisé, dans le champ Enregistrer le filtre en bas du panneau Filtrer, tapez un nom descriptif et cliquez sur Enregistrer. Si vous décidez de ne pas enregistrer le filtre, cliquez sur Annuler.



6. Après avoir enregistré le filtre, vous pouvez le sélectionner en bas du panneau Filtre pour filtrer les informations dans le tableau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : si vous cliquez sur le triangle à droite du nom de filtre, vous pouvez renommer ou supprimer le filtre.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Notifications

Jul 25, 2016

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. Il 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 cette section expliquent comment ajouter un serveur SMTP, une passerelle SMS, et une passerelle SMS opérateur.

Pour configurer un serveur SMTP et une passerelle SMS

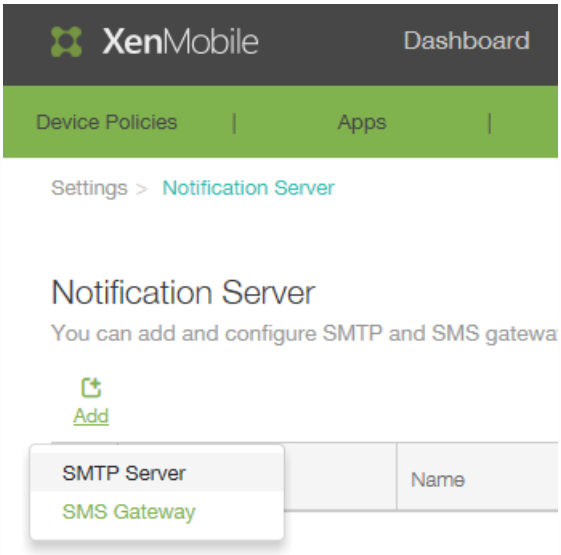
Configuration requise :

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

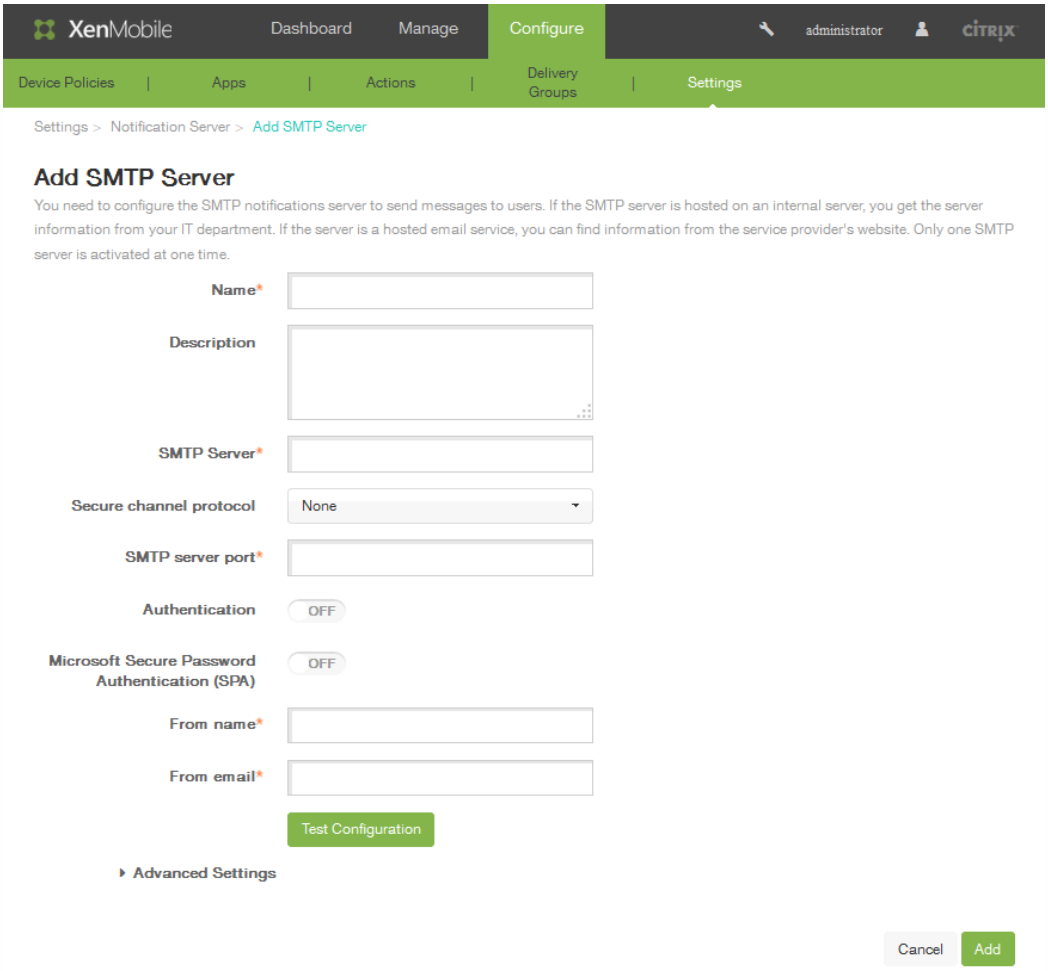
serveur SMTP sur votre réseau interne pour que les notifications soient envoyées avec succès.

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > Serveur de notification.
   La page de configuration Serveur de notification s'affiche.



2. Cliquez sur Ajouter, cliquez sur Serveur SMTP ou Passerelle SMS et suivez les procédures détaillées pour chaque choix dans les étapes suivantes.
   - Pour ajouter un serveur SMTP, suivez les étapes 3 à 6.
   - Pour ajouter une passerelle SMS, suivez les étapes 7 à 9.
3. Si vous cliquez pour ajouter un serveur SMTP, la page Ajouter un serveur SMTP s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

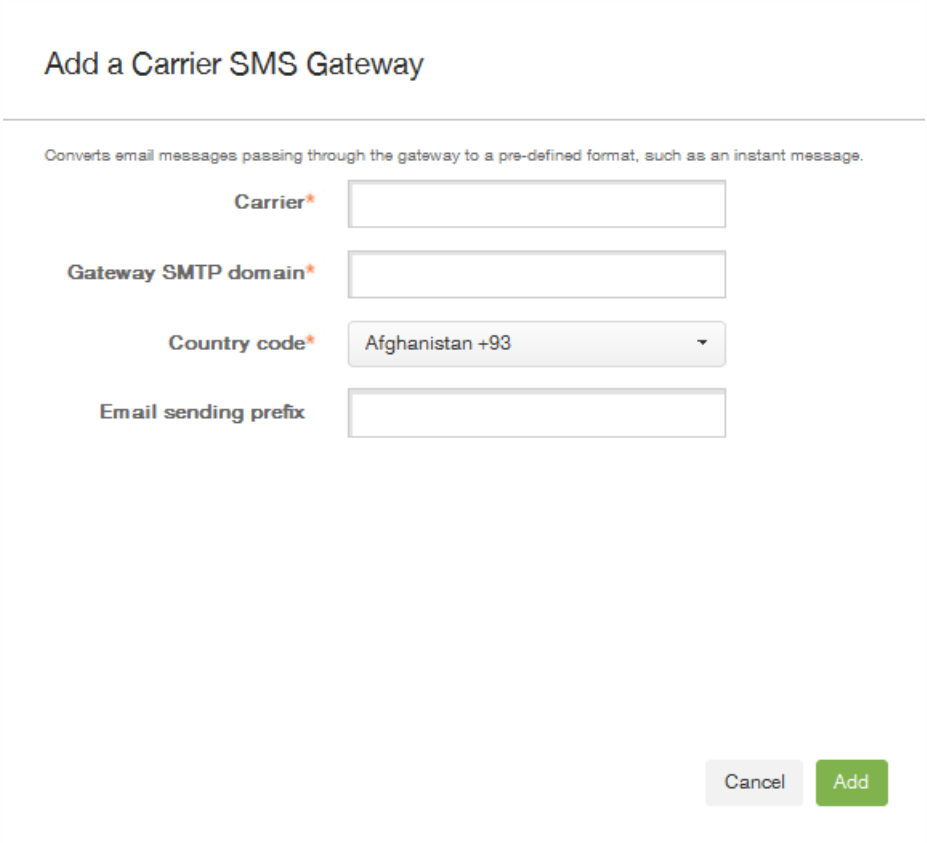


4. Configurez les paramètres suivants :
   - Nom : entrez le nom associé à ce compte de serveur SMTP.
   - Description : entrez une description pour le serveur (facultatif).
   - Serveur SMTP : entrez le nom d'hôte du serveur. Le nom d'hôte peut être un nom de domaine complet (FQDN) ou une adresse IP.
   - 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. Par défaut, ce champ est défini sur 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. Cette fonctionnalité est désactivée par défaut.
   - Authentification par mot de passe sécurisé (SPA) Microsoft : si le serveur SMTP utilise la SPA, cliquez sur ON. Cette fonctionnalité est désactivée par défaut.
   - 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.
   - Tester la configuration : cliquez pour envoyer une notification par e-mail test.
5. 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. Par défaut, ce champ est défini sur 5.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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. Par défaut, ce champ est défini sur 30 secondes.
- Nombre max de destinataires SMTP : entrez le nombre maximal de destinataires par message envoyés par le serveur SMTP. Par défaut, cette valeur est définie sur 100.

6. Après avoir configuré le serveur SMTP, cliquez sur **Ajouter**.
7. Sur la page de configuration Serveur de notification, pour configurer une passerelle SMS, cliquez sur Ajouter, puis sur Passerelle SMS.
   La page Ajouter une passerelle SMS s'affiche.



   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.
8. Configurez les paramètres suivants :
   - Nom : identifiez la configuration de la passerelle SMS.
   - Description : entrez une description pour la configuration (facultatif).
   - Clé : entrez l'identificateur numérique fourni par l'administrateur système lors de l'activation du compte.
   - 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.
   - 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 ; sinon, entrez une étiquette ou un nom significatif. Vous pouvez acheter des numéros de téléphone virtuels sur le site Web Nexmo.
   - HTTPS : sélectionnez cette option si vous souhaitez utiliser le protocole HTTPS pour transmettre des requêtes SMS à Nexmo.
   - 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 +.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

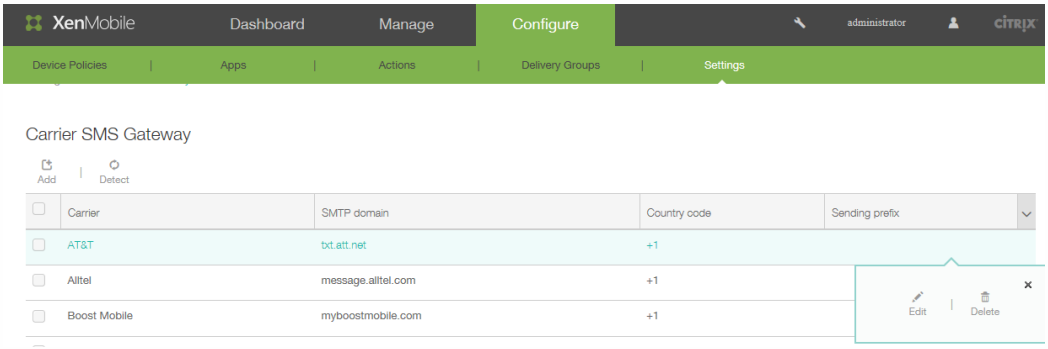
- Tester la configuration : cliquez pour envoyer un message test à l'aide de la configuration actuelle. Les erreurs de connexion sont détectées et apparaissent immédiatement, telles que les erreurs d'authentification ou les numéros de téléphone erronés. Les messages sont reçus dans les mêmes délais que ceux envoyés entre téléphones portables.

9. Cliquez sur Ajouter.

Pour ajouter une passerelle SMS d'opérateur

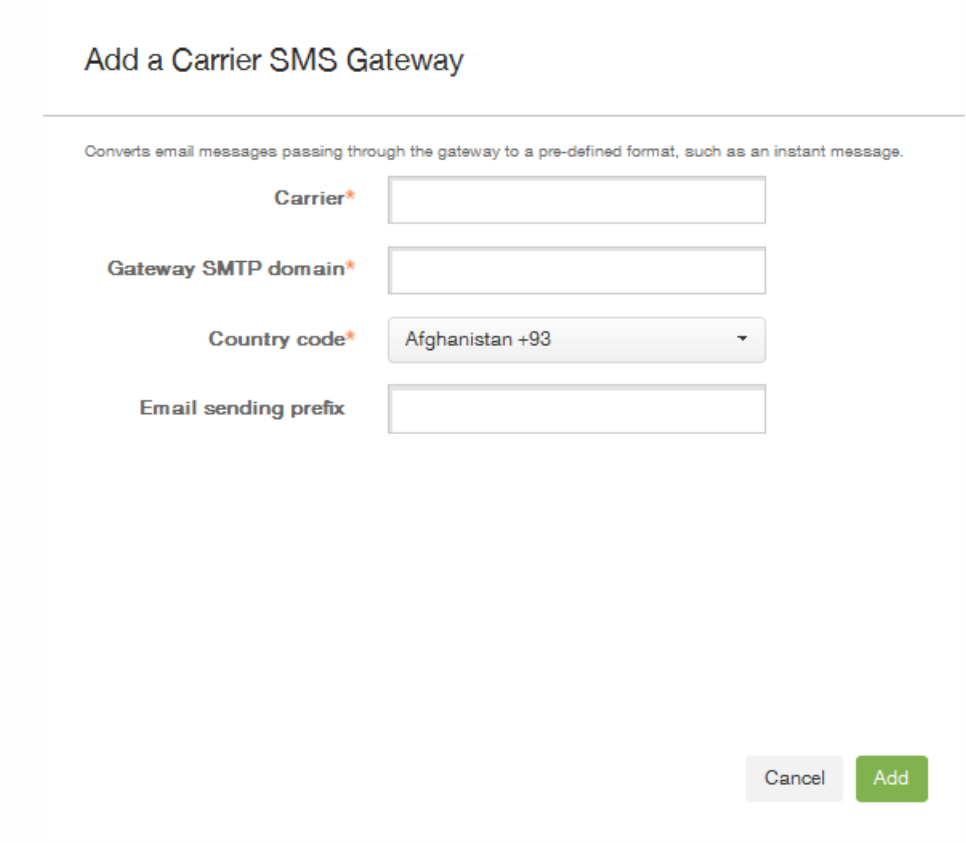
Vous pouvez configurer une passerelle SMS d'opérateur dans XenMobile pour configurer les notifications qui sont envoyées via la passerelle SMS d'un opérateur. Les opérateurs utilisent les passerelles SMS pour envoyer ou recevoir des transmissions SMS vers ou à partir d'un réseau de télécommunications. 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 Web XenMobile, cliquez sur Configurer > Paramètres > Plus > Passerelle SMS de l'opérateur. La page de configuration Passerelle SMS opérateur s'ouvre.



2. Cliquez sur Ajouter pour ajouter un nouvel opérateur. Cliquez sur le bouton Détecter pour découvrir automatiquement une passerelle. La boîte de dialogue Ajouter la passerelle SMS d'un opérateur apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Entrez les informations suivantes : 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. Opérateur : entrez le nom de l'opérateur.
   2. Domaine SMTP de la passerelle : entrez le domaine associé à la passerelle SMTP.
   3. Indicatif du pays : dans la liste, cliquez sur l'indicatif de pays pour l'opérateur.
   4. Préfixe d'envoi d'e-mail : si vous le souhaitez, vous pouvez spécifier un préfixe pour l'envoi d'e-mail.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificats

Oct 11, 2016

Dans XenMobile, les certificats permettent d'établir des connexions sécurisées et d'authentifier les utilisateurs.

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).

Pour inscrire et gérer des appareils iOS avec XenMobile, vous devez configurer et créer un certificat Apple Push Notification Service (APNS). Pour obtenir des instructions détaillées, consultez la section Faire une demande de certificat 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	PEM ou PFX (PKCS#12)	SSL, SAML, APNS XenMobile génère également une PKI complète durant le processus d'installation. Le serveur XenMobile ne prend pas en charge les certificats avec une extension .pem. Utilisez la commande openssl pour générer un fichier PFX à partir d'un fichier PEM : openssl pkcs12 -export -out certificate.pfx -in certificate.pem
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration des certificats clients pour l'authentification

NetScaler Gateway prend en charge l'utilisation de certificats clients pour l'authentification. Les utilisateurs qui ouvrent une session sur NetScaler Gateway peuvent également être authentifiés en fonction des attributs du certificat client qui est présenté au serveur virtuel. L'authentification du certificat client peut également être utilisée avec un autre type d'authentification, tel que LDAP ou RADIUS pour fournir une authentification à deux facteurs.

Pour authentifier les utilisateurs en fonction des attributs du certificat du côté client, l'authentification du client doit être activée sur le serveur virtuel et le certificat client doit être demandé. Vous devez lier un certificat racine au serveur virtuel sur NetScaler Gateway.

L'authentification des appareils avec NetScaler Gateway n'est pas prise en charge pour les certificats obtenus via une autorité de certification discrétionnaire.

Lorsque les utilisateurs ouvrent une session sur NetScaler Gateway, après l'authentification, les informations relatives au nom d'utilisateur sont extraites à partir du champ spécifié du certificat. Ce champ est généralement Subject:CN. Si le nom d'utilisateur est extrait avec succès, l'utilisateur est authentifié. S'il ne fournit pas de certificat valide durant la négociation SSL ou si l'extraction du nom d'utilisateur échoue, l'authentification échoue.

Vous pouvez authentifier les utilisateurs en fonction du certificat client en définissant le type d'authentification par défaut de manière à utiliser le certificat client. Vous pouvez également créer une action de certificat dont la tâche est de définir les opérations à réaliser durant l'authentification basée sur un certificat client SSL.

PKI XenMobile

La fonctionnalité d'intégration de l'infrastructure de clé publique (PKI) XenMobile vous permet de gérer la distribution et le cycle de vie des certificats de sécurité utilisés sur vos appareils.

XenMobile crée une PKI interne pour l'authentification de l'appareil lors du processus d'installation.

Les PKI externes peuvent également être utilisées pour émettre des certificats sur les appareils que vous pouvez utiliser dans les stratégies de configuration ou pour l'authentification des clients à NetScaler Gateway.

La fonction principale du système PKI est l'entité PKI. Une entité PKI présente un composant backend pour les opérations PKI. Ce composant fait partie de votre infrastructure d'entreprise, telle que Microsoft, RSA, Entrust Symantex ou OpenTrust PKI. L'entité PKI gère l'émission et la révocation de certificats backend. Elle représente la source de référence pour le statut du certificat. La configuration XenMobile doit normalement contenir une entité PKI par composant PKI backend.

La fonction secondaire du système PKI est le fournisseur d'identités. Un fournisseur d'identités est une configuration particulière d'émission et de cycle de vie de certificat. Il contrôle des éléments comme le format du certificat (sujet, clé, algorithmes) et les conditions de sa révocation ou de son renouvellement, le cas échéant. Les fournisseurs d'identités délèguent des opérations aux entités PKI. En d'autres termes, bien que les fournisseurs d'identités contrôlent le moment où les opérations PKI sont exécutées et la nature des données avec lesquelles elles sont effectuées, les entités PKI contrôlent la manière dont ces opérations sont réalisées. La configuration XenMobile contient normalement plusieurs fournisseurs d'identités par entité PKI.

Administration des certificats XenMobile

Nous vous recommandons d'effectuer un suivi des certificats que vous utilisez dans votre déploiement XenMobile, et plus

© 1999-2017 Citrix Systems, Inc. All rights reserved.

particulièrement leurs dates d'expiration et mots de passe associés. Cette section vise à faciliter l'administration des certificats dans XenMobile.

Votre environnement peut inclure une partie ou l'ensemble des certificats suivants :

Serveur XenMobile
Certificat SSL pour le nom de domaine complet MDM
Certificat SAML (pour ShareFile)
Certificats d'autorité de certification racine et intermédiaire pour les certificats ci-dessus et toute autre ressource interne (StoreFront / Proxy etc)
Certificat APNS pour la gestion des appareils iOS
Certificat APNS interne pour les notifications XMS WorxHome
Certificat utilisateur PKI pour la connectivité aux infrastructures de clé publique (PKI)

MDX Toolkit
Certificat Apple Developer
Profil de provisioning Apple (par application)
Certificat APNS Apple (à utiliser avec WorxMail)
Fichier keyStore Android
Windows Phone – Certificat Symantec

NetScaler
Certificat SSL pour le nom de domaine complet MDM
Certificat SSL pour le nom de domaine complet de la passerelle
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 des certificats XenMobile

Si vous laissez un certificat expirer, ce certificat n'est plus valide. Par conséquent vous ne pouvez plus effectuer de transactions sécurisées sur votre environnement ni accéder aux ressources XenMobile.

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

Certificats APNS pour WorxMail

Étant donné que les certificats du service de notification push d'Apple (APNS) expirent tous les ans, n'oubliez pas de créer de nouveaux certificats SSL pour le service de notification push d'Apple et de les mettre à niveau sur le portail Citrix avant que les certificats n'expirent. Si le certificat expire, les utilisateurs rencontreront des incohérences dans les notifications push de WorxMail. En outre, vous ne pourrez plus envoyer de notifications push pour vos applications.

Certificats APNS pour la gestion des appareils iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Vous pouvez afficher l'état et la date d'expiration du certificat APNS en vous connectant au portail Apple Push Certificates Portal. Vous devez vous connecter à l'aide du même utilisateur que celui qui a créé le certificat.

Apple vous enverra également une notification par e-mail 30 et 10 jours avant la date d'expiration avec les informations suivantes :

« The following Apple Push Notification Service certificate, created for AppleID CustomersID will expire on Date. Revoking or allowing this certificate to expire will require existing devices to be re-enrolled with a new push certificate.

Please contact your vendor to generate a new request (a signed CSR), then visit https://identity.apple.com/pushcert to renew your Apple Push Notification Service certificate.

Thank You,

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.

Veuillez noter qu'un certificat et un profil de provisioning iOS Developer for Enterprise existants peuvent ne pas être compatibles avec iOS 9. Pour de plus amples informations, consultez la section Wrapping d'applications Worx pour iOS 9.

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. Un exemple d'ID d'application acceptable est : com.NomSociété.NomProduit.
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 de plus amples informations, consultez la section Wrapping des applications mobiles iOS.

Pour confirmer que 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.

Certificats d'entreprise Symantec pour Windows Phone

Symantec est le fournisseur exclusif des certificats de signature de code du service Microsoft App Hub. Les développeurs et les éditeurs de logiciels rejoignent le App Hub pour distribuer des applications Windows Phone et Xbox 360 en vue de leur téléchargement via le Windows Marketplace. Pour de plus amples informations, consultez Symantec Code Signing

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificates for Windows Phone dans la documentation de Symantec.

Si le certificat expire, les utilisateurs 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 de plus amples informations sur la façon de gérer l'expiration des certificats pour NetScaler, consultez l'article How to handle certificate expiry on NetScaler dans le centre de connaissances Citrix.

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

Le Expiry Monitor et le Command Center peuvent vous aider à suivre vos certificats NetScaler et vous informerons lorsque le certificat expire. Ces deux outils permettent d'assurer le suivi des certificats Netscaler suivants :

Certificat SSL pour le nom de domaine complet MDM
Certificat SSL pour le nom de domaine complet de la passerelle
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 précédents

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Chargement de certificats dans XenMobile

Jul 25, 2016

Les certificats sont utilisés par le serveur XenMobile. Vous devez charger des certificats sur XenMobile via la zone Certificats de la console XenMobile. Ces certificats 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 la zone Certificats en tant que stockage pour les certificats que vous voulez déployer sur des appareils. Cette utilisation s'applique particulièrement aux autorités de certification utilisées pour établir une relation de confiance sur l'appareil.

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.

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 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.

XenMobile prend en charge les formats d'entrée suivants pour les certificats :

- fichiers de certificat codés PEM ou DER ;
- fichiers de certificat codés PEM ou DER avec un fichier de clé privée associé au format codé PEM ou DER ;
- keystores PKCS#12 (P12 ; également connus sous le nom de fichier PFX sous Windows).

Important : le serveur XenMobile ne prend pas en charge les certificats avec une extension .pem. Utilisez la commande openssl pour générer un fichier PFX à partir d'un fichier PEM :

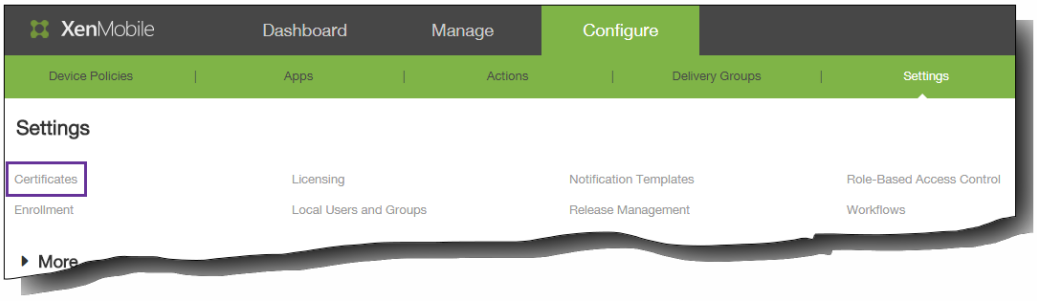
openssl pkcs12 -export -out certificate.pfx -in certificate.pem

Pour importer un keystore

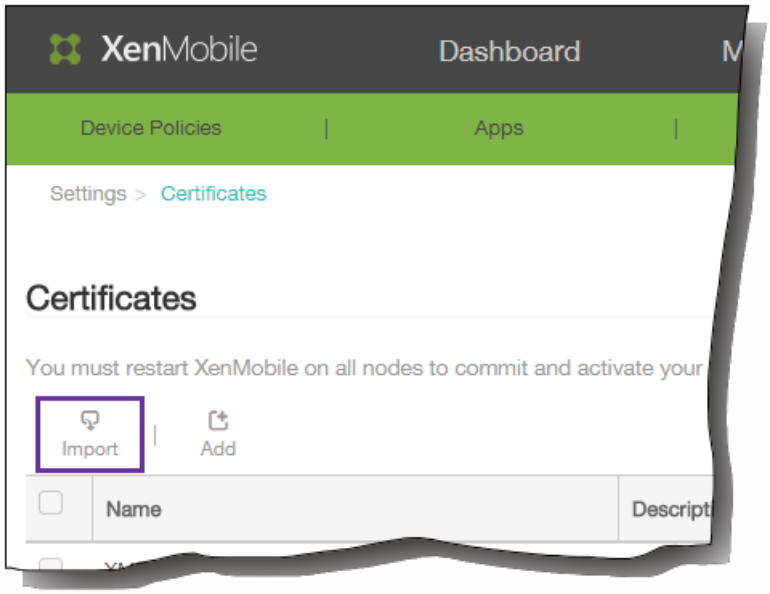
Les keystores, de par leur conception, peuvent comporter plusieurs entrées. Lors du chargement à partir d'un keystore, par conséquent, vous êtes invité à indiquer l'alias d'entrée qui identifie l'entrée à charger. Si vous ne spécifiez pas d'alias, la première entrée du magasin est chargée. Étant donné 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 Configurer > Paramètres > Certificats.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



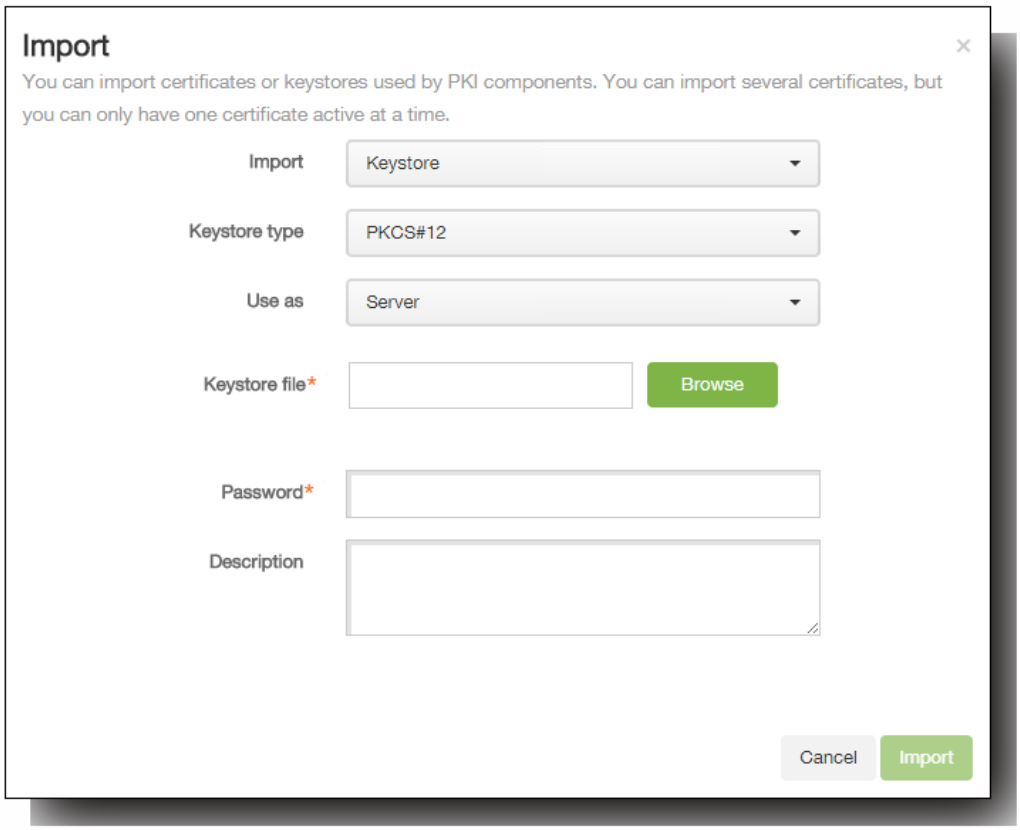
2. Sur la page Certificats, cliquez sur Importer.



La boîte de dialogue Importer apparaît.

3. Dans la boîte de dialogue Importer, dans Importer, cliquez sur Keystore.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La boîte de dialogue Importer change pour refléter les options de keystore disponibles, comme illustré dans la figure précédente.

4. Dans le type Keystore, cliquez sur PKCS#12.
5. 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 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.
6. Parcourez pour trouver le keystore que vous voulez importer.
7. Dans Mot de passe, entrez le mot de passe affecté au certificat.
8. Entrez une description pour le keystore (facultatif) vous permettant de le distinguer de vos autres keystores.
9. Cliquez sur Importer. Le keystore est ajouté au tableau Certificats.

Pour importer un certificat

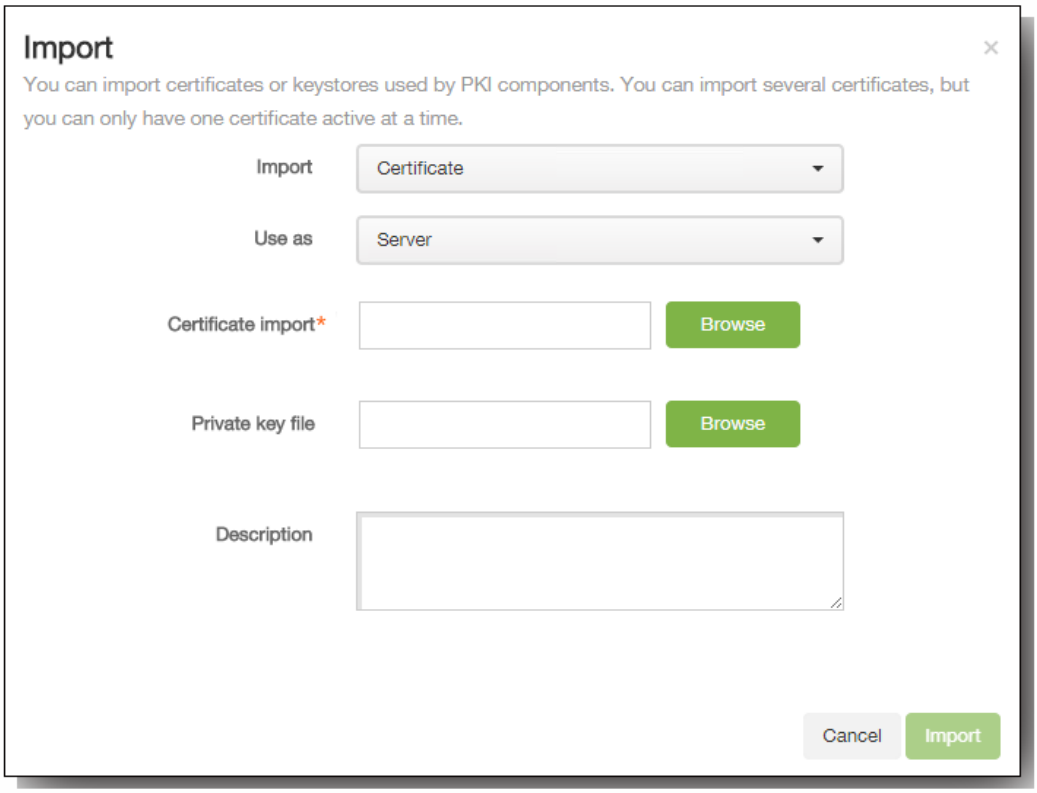
Lors de l'importation d'un certificat, soit à partir d'un fichier, soit depuis une entrée de keystore, XenMobile tente de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Configurer > Paramètres > 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.



La boîte de dialogue Importer change pour refléter les options de certificat disponibles.

4. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Écouteur SSL**. L'écouteur SSL notifie XenMobile de l'activité cryptographique SSL.

5. Parcourez pour trouver le certificat que vous voulez importer.
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 mettre à jour vos certificats de manière plus efficace, dans la console XenMobile, sous Configurer > Paramètres > 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entités PKI

Jul 25, 2016

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

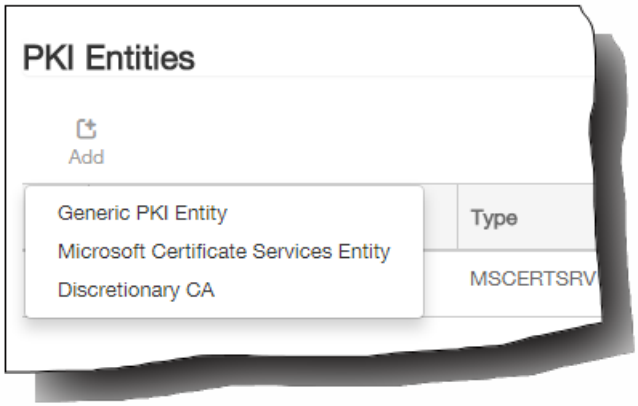
La carte GPKI, en tant que point de terminaison des services Web SOAP, publie une définition WSDL auto-descriptive. La création d'une entité GPKI PKI équivaut à fournir cette définition WSDL à XenMobile, soit par le biais d'une adresse URL soit en chargeant le fichier lui-même.

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.

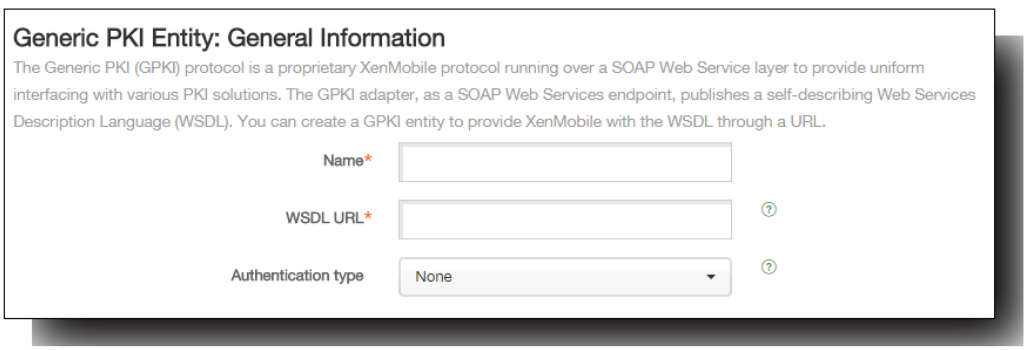
Les paramètres utilisateur sont des paramètres qui sont définis par l'adaptateur GPKI pour une opération spécifique et dont vous avez besoin pour fournir des valeurs à XenMobile. XenMobile détermine les opérations prises en charge par la carte (quelles capacités elle possède) et les paramètres requis 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Sur la page Entité PKI générique : informations générales, procédez comme suit :
   1. Nom : entrez un nom descriptif pour l'entité PKI.
   2. URL du WSDL : entrez l'emplacement du WSDL décrivant la carte.
   3. 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.
   4. Cliquez sur Suivant.
      La page Entité PKI générique : capacité de l'adaptateur s'affiche.

5. 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.

6. 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.
7. 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).

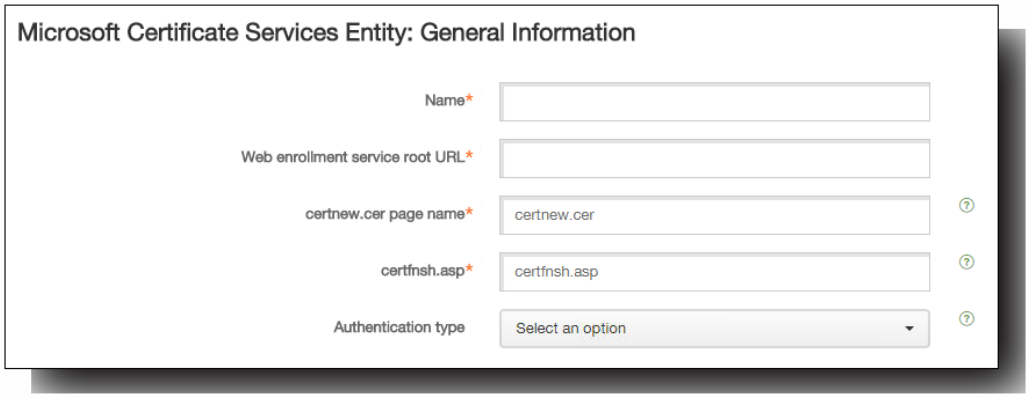
Pour créer une entité PKI Microsoft CA dans XenMobile, vous devez spécifier l'adresse URL de base de l'interface Web des services de certificats. Si vous le souhaitez, utilisez l'authentification de client SSL pour sécuriser la connexion entre XenMobile et l'interface Web des services de certificats.

Pour ajouter une entité Services de certificats Microsoft

1. Dans la console 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 Services de certificats Microsoft.
   La page Entité Services de certificats Microsoft : informations générales s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Sur la page Entité Services de certificats Microsoft : informations générales, procédez comme suit :
   1. 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.
   2. 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.
   3. 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.
   4. certfnsh.asp : nom de la page certfnsh.asp. Utilisez le nom par défaut sauf si vous l'avez renommé pour une raison quelconque.
   5. 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.
      - Certificat client : sélectionnez le certificat client SSL correct.
      - 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.

5. 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.
6. 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.

7. 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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

9. Cliquez sur Enregistrer.
   L'entité s'affiche sur le tableau Entités PKI.

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://serveur/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 :

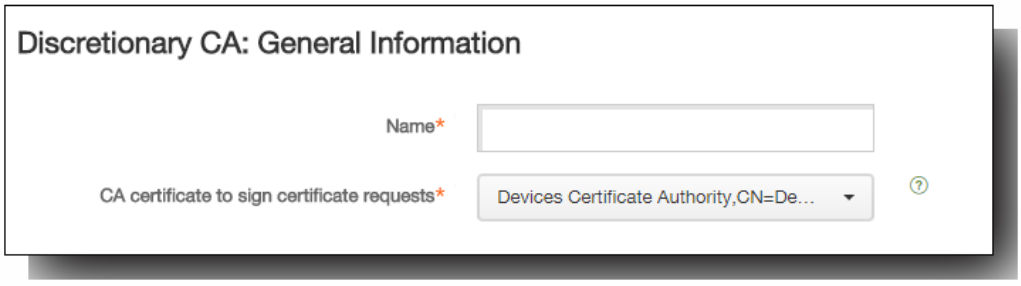
- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

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 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.

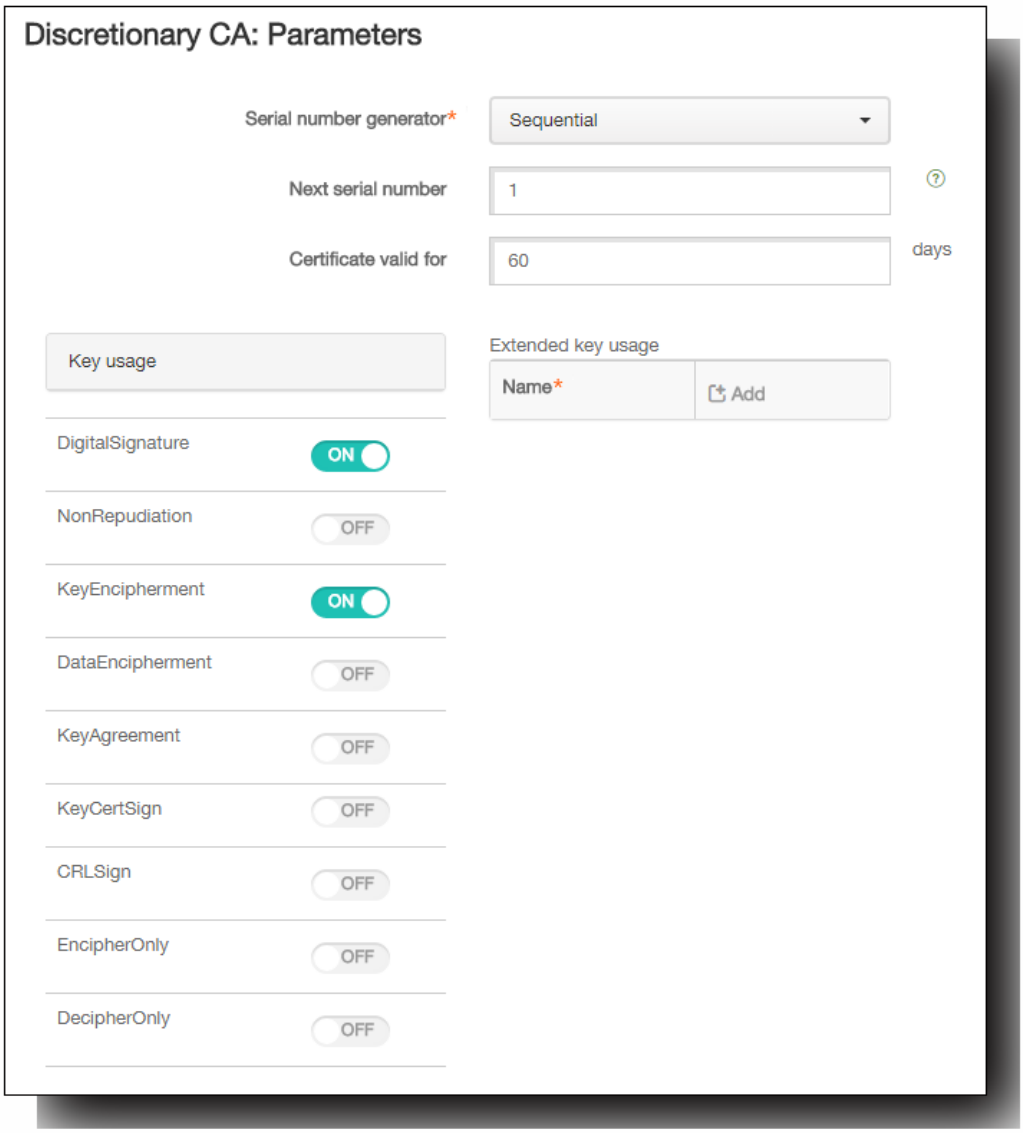
3. Cliquez sur CA discrétionnaire.
   La page CA discrétionnaire : informations générales s'affiche.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Nom : entrez un nom descriptif pour la CA discrétionnaire.
2. 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.
3. Cliquez sur Suivant.
   La page CA discrétionnaire : paramètres s'affiche.



5. Sur la page CA discrétionnaire : paramètres, procédez comme suit :
   1. 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.
   2. Numéro de série suivant : entrez une valeur pour déterminer le numéro suivant émis.
   3. Certificat valide pour : entrez le nombre de jours pendant lesquels le certificat est valide.
   4. 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.
   5. Utilisation de clé étendue : pour ajouter d'autres paramètres, cliquez sur Ajouter, entrez le nom de clé, puis cliquez sur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Enregistrer.

6. Cliquez sur Suivant.
   La page CA discrétionnaire : distribution s'affiche.

6. 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 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.
7. Cliquez sur Suivant.
   La page CA discrétionnaire : protocole OCSPs'affiche.

8. Sur la page CA discrétionnaire : protocole OCSP, procédez comme suit :
   1. 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.
   2. 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 > Configure > Paramètres > Certificats.
9. Cliquez sur Enregistrer.
   L'autorité de certification discrétionnaire s'affiche sur le tableau Entités PKI.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Fournisseurs d’informations d’identification

Jul 25, 2016

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 8	Non	Non

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contexte	SCEP pris en charge	SCEP requis
Configuration de Windows Phone	Non	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.

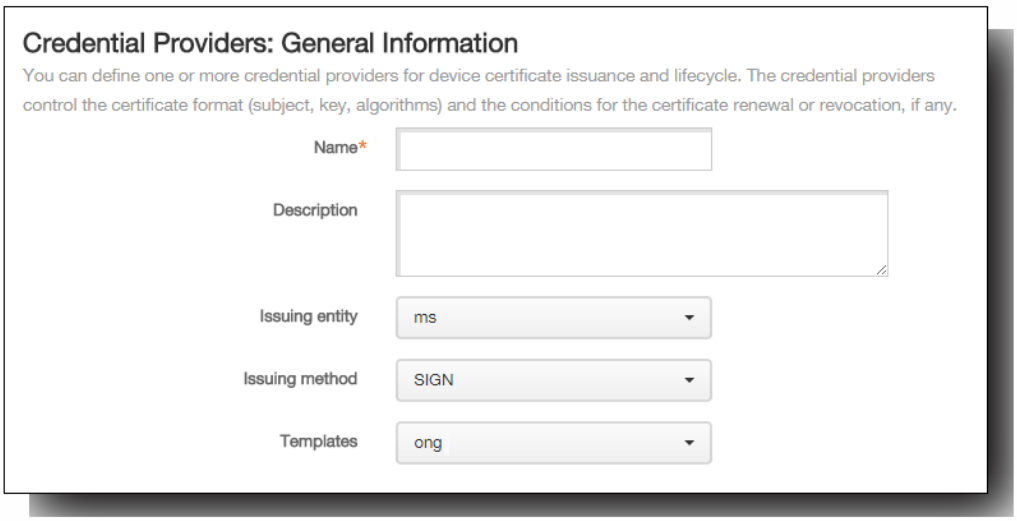
La configuration de la révocation nécessite que vous spécifiiez une certaine durée (en jours). Lorsque l'appareil se connecte, le serveur vérifie que la date du certificat NotAfter est postérieure à la date actuelle, moins la durée spécifiée. Si c'est le cas, un renouvellement est tenté.

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.

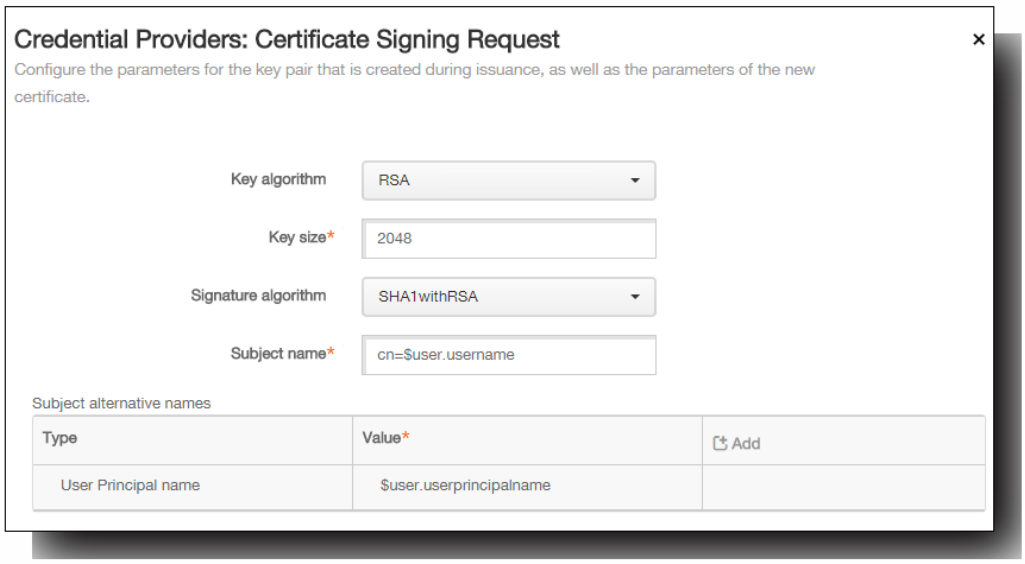
© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > 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 :
   1. 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.
   2. 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.
   3. Entité émettrice : cliquez sur l'entité qui émet le certificat.
   4. 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.
   5. Si la liste des modèles est disponible, sélectionnez un modèle pour le fournisseur d'identités.
      Remarque : ces modèles deviennent disponibles lorsque les entités Services de certificats Microsoft sont ajoutées sur Configurer > Paramètres > Plus > Entités PKI.
   6. Cliquez sur Suivant.
      La page Fournisseur d'identités : demande de signature de certificat s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Sur la page Fournisseur d'identités : demande de signature de certificat, procédez comme suit :
    1. Algorithme de clé : cliquez sur l'algorithme de clé pour la nouvelle paire de clés. Les valeurs disponibles sont RSA, DSA et ECDSA.
    2. 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.
    3. Algorithme de signature : cliquez sur une valeur pour le nouveau certificat. Les valeurs dépendent de l'algorithme de clé.
    4. 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.
    5. 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.
    Remarque : comme avec le nom du sujet, vous pouvez utiliser les macros XenMobile dans le champ de valeur.
    6. Cliquez sur Suivant.
    La page Fournisseurs d'identités : distribution s'affiche.

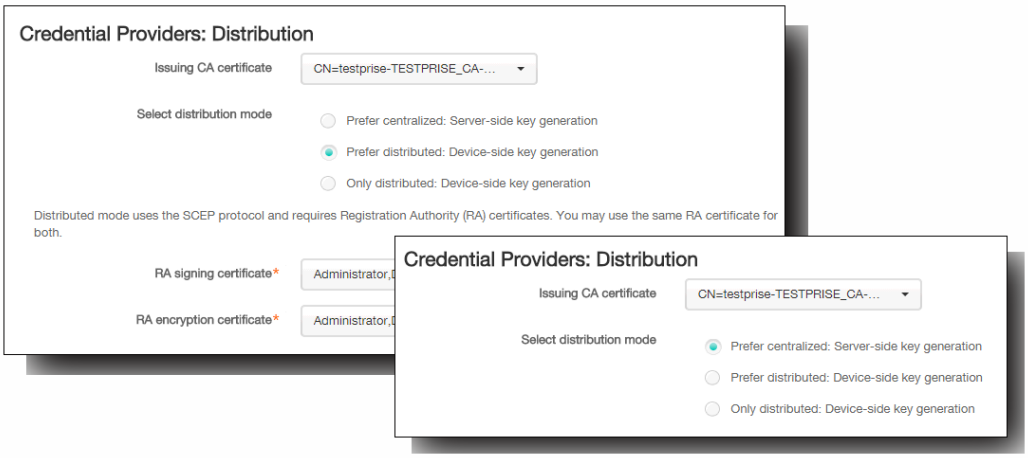
5. Sur la page Fournisseurs d'identités : distribution, procédez comme suit :
    1. Dans la liste Certificat émis par l'autorité de certification, cliquez sur le certificat d'autorité de certification proposé. Étant donné que le fournisseur d'identités utilise une entité d'autorité de certification 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.
    2. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

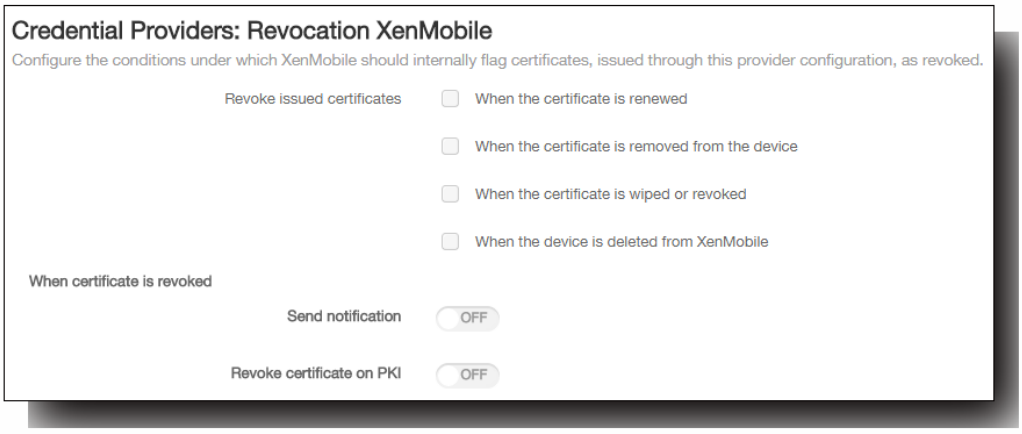
être utilisé pour le chiffrement et la signature.

- 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 sélectionnez Préférer mode distribué : génération de la clé sur l'appareil ou Distribué uniquement : génération de la clé sur l'appareil, vous devez également sélectionner un certificat de signature RA et un certificat de chiffrement RA. De nouveaux champs apparaissent pour ces certificats.

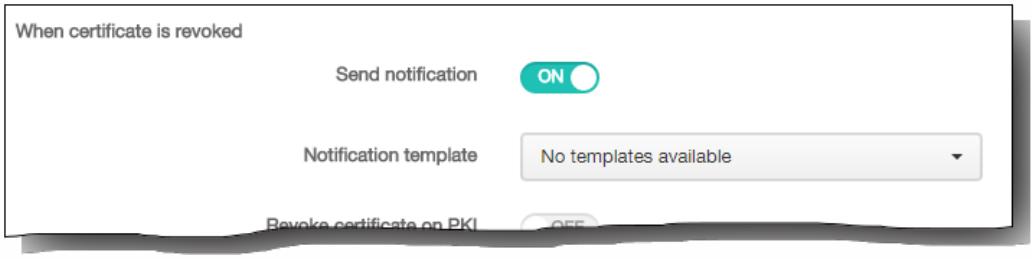


3. Si vous avez sélectionné Préférer mode distribué : génération de la clé sur l'appareil ou Distribué uniquement : génération de la clé sur l'appareil, cliquez sur le certificat de signature RA et le certificat de chiffrement RA. Le même certificat peut être utilisé pour les deux modes.
4. Cliquez sur 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.

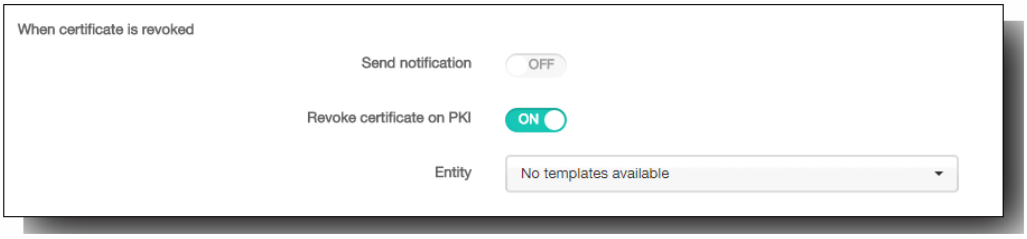


6. Sur la page Fournisseurs d'identités : révocation XenMobile, procédez comme suit :
   1. Dans Révoquer les certificats émis, sélectionnez l'une des options qui indique quand les certificats doivent être révoqués.
   2. Si vous voulez que XenMobile envoie une notification lorsque le certificat est révoqué, définissez la valeur de Envoyer une notification sur On et choisissez un modèle de notification.

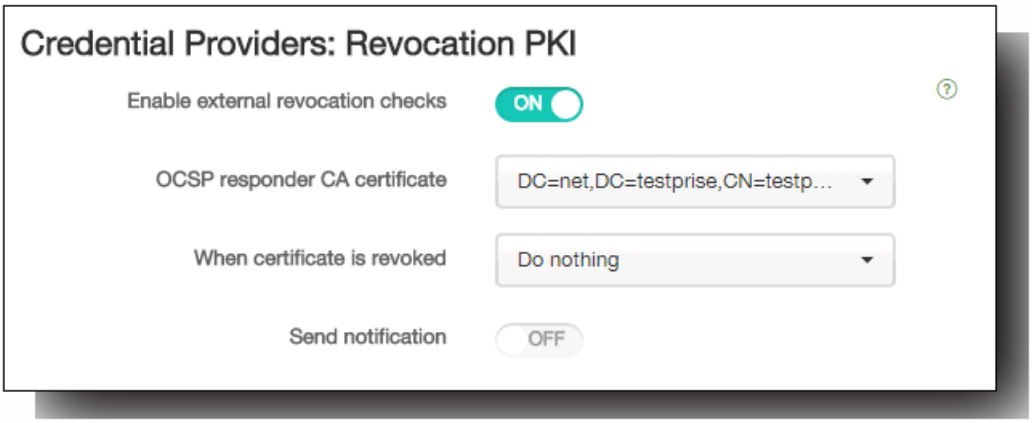
© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. 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.



4. 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.



7. Sur la page Fournisseurs d'identités : révocation PKI, procédez comme suit si vous souhaitez révoquer les certificats de la PKI :
   1. Modifiez le paramètre Activer les vérifications de révocation externe sur On.

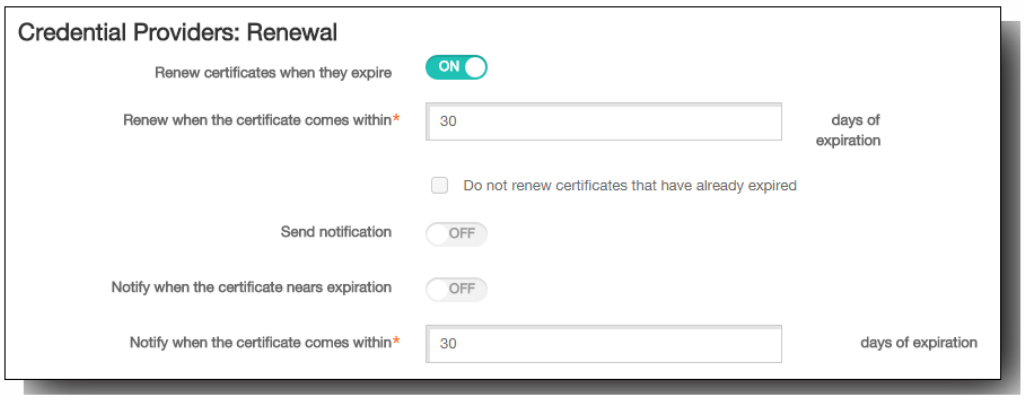
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Des champs supplémentaires liés à la PKI de révocation apparaissent.

2. 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
3. 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.
4. 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.
5. 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).

8. Sur la page Fournisseurs d'identités : renouvellement, procédez comme suit si vous souhaitez renouveler les certificats lorsqu'ils expirent :
   1. Réglez Renouveler les certificats lorsqu'ils expirent sur On.
      Des champs supplémentaires s'affichent.



   2. Dans le champ Renouveler lorsque le certificat expire dans, entrez quand le renouvellement doit être effectué, en nombre de jours avant l'expiration.
   3. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 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.

5. 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.

6. 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.

9. Cliquez sur Enregistrer.
   Le fournisseur d'identités est ajouté à la table Fournisseur d'identités.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Faire une demande de certificat APNS

Jul 25, 2016

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	Envoyez la demande de signature de certificat (CSR) signée à Apple sur le portail Apple Push certificat Portal (Apple ID obligatoire), puis téléchargez 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.

   Country Name (2 letter code) [AU]:FR
   State or Province Name (full name) [Some-State]:Province
   Locality Name (eg, city) []:Paris
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:Citrix
   Organizational Unit Name (eg, section) []:Marketing
   Common Name (eg, YOUR name) []:Guillaume Martin
   Email Address []:guillaume.martin@client.com

3. Dans le message suivant, entrez un mot de passe pour la clé privée de la demande de signature de certificat.
   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:
   An optional company name []:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 ou utilisateur disposant d'un accès à l'onglet **À**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

propos de.

9. Cliquez sur l'onglet **À propos de**, puis cliquez sur **Mettre à jour le certificat APNS**.
10. Dans la boîte de dialogue **Mettre à jour le certificat APNS**, recherchez le fichier certificat APNS .pfx sur votre ordinateur, puis entrez un nouveau mot de passe.
11. Cliquez sur **Charger le certificat APNs**.
12. Cliquez sur **Mettre à jour**.

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. Ouvrez une session sur la console XenMobile en tant qu'administrateur.
2. Cliquez sur **Configurer** > **Paramètres** > **Certificats**.
3. Sur la page **Certificats**, cliquez sur **Importer**. La boîte de dialogue **Import** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Accédez au fichier .p12 sur votre ordinateur.
5. 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.

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 sur XenMobile dans **Configurer** > **Paramètres** > **Certificats**.
7. Dans la boîte de dialogue **Importer**, importez le nouveau certificat.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway et XenMobile

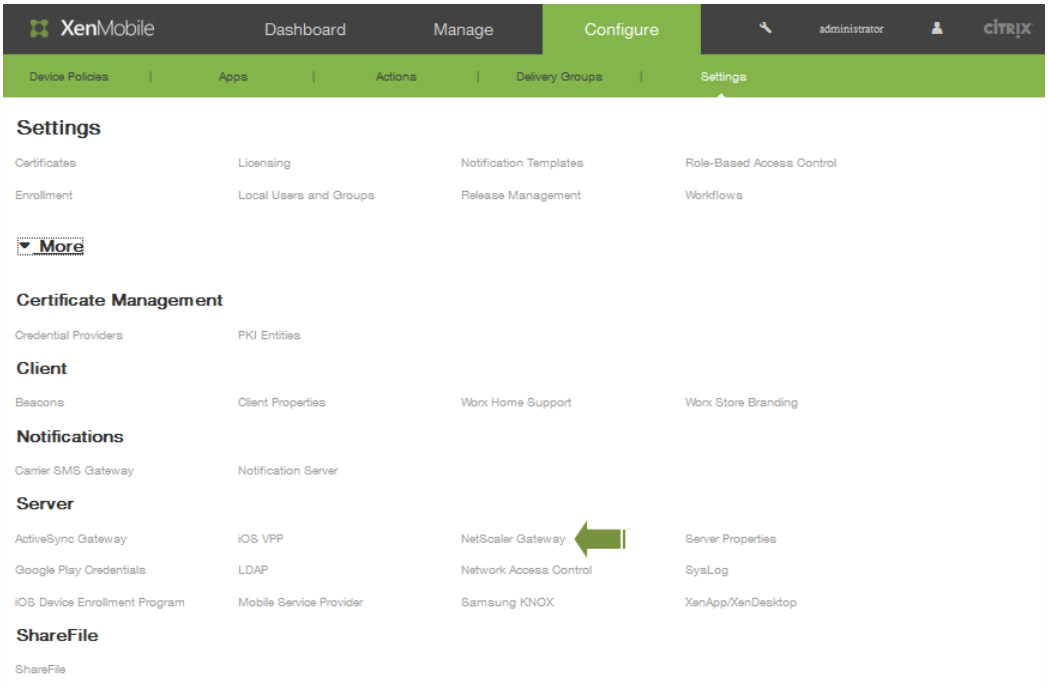
Jul 25, 2016

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.

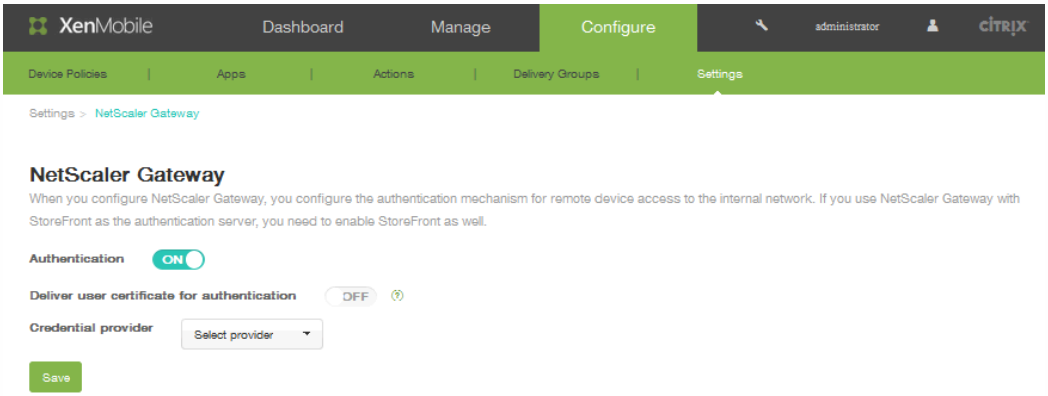
Remarque : pour de plus amples informations sur la configuration de NetScaler Gateway pour XenMobile sur NetScaler, consultez la section Configuration de paramètres pour votre environnement XenMobile.

Pour configurer NetScaler Gateway

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > NetScaler Gateway.



2. Dans Authentification, sélectionnez ON.



3. Si vous voulez que XenMobile partage le certificat d'authentification avec Worx Home afin que NetScaler Gateway gère

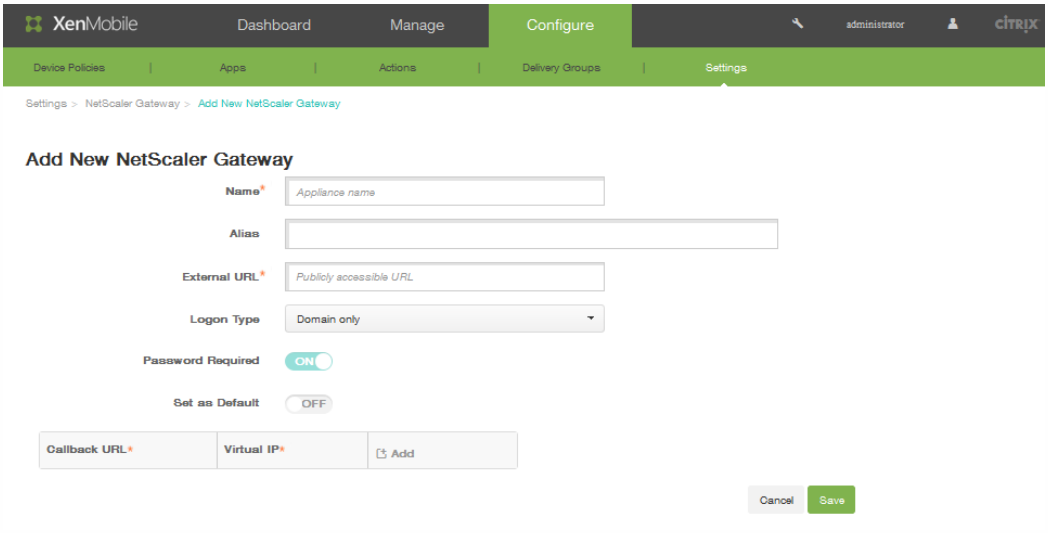
© 1999-2017 Citrix Systems, Inc. All rights reserved.

l'authentification du certificat client, dans Délivrer un certificat utilisateur pour l'authentification, sélectionnez ON.

4. Dans la liste Fournisseur d'identités, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseur d'identités.
5. Cliquez sur Enregistrer.

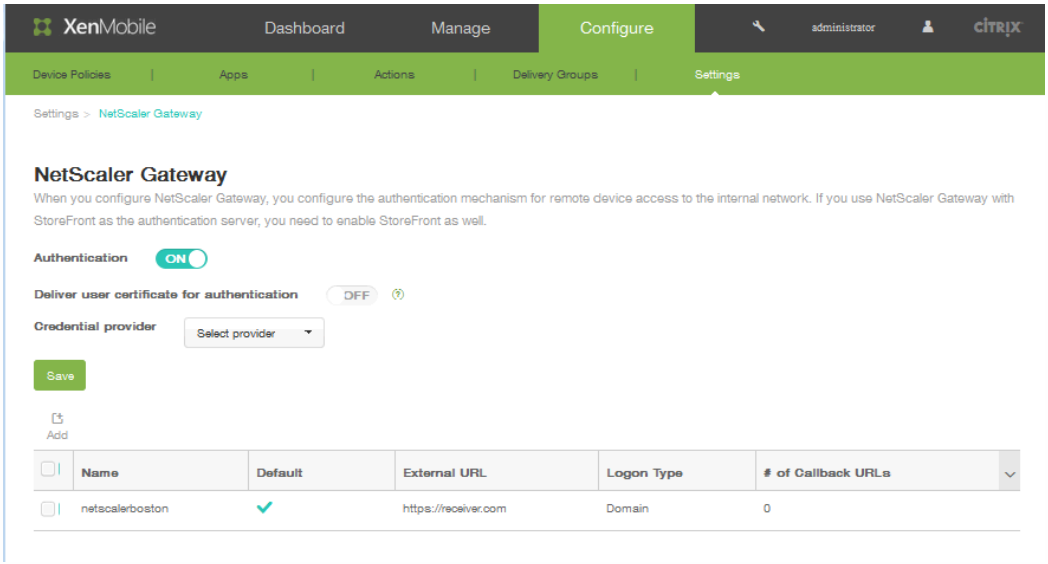
Pour ajouter une nouvelle instance NetScaler Gateway

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > NetScaler Gateway.
2. Au-dessus du tableau, cliquez sur Ajouter. La page Ajouter une nouvelle passerelle NetScaler Gateway s'affiche.



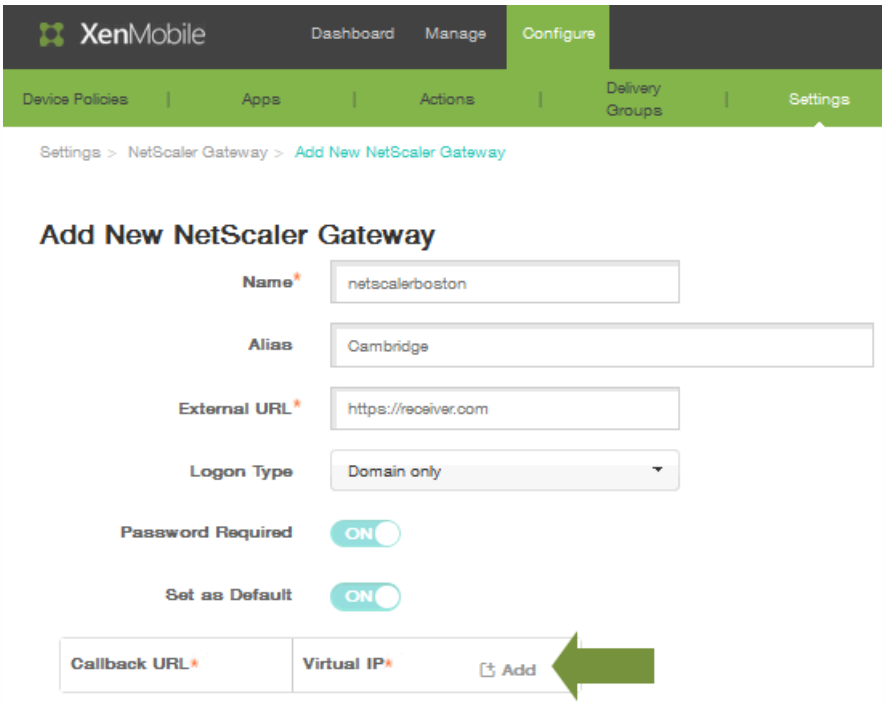
3. Dans le champ Nom, entrez un nom pour l'instance NetScaler Gateway.
4. Dans Alias, entrez un alias (facultatif).
5. Dans URL externe, entrez l'adresse URL publiquement accessible de NetScaler Gateway. Par exemple, https://receiver.com.
6. Dans la liste Type d'ouverture de session, cliquez sur un type d'ouverture de session. 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. Par défaut, le type d'ouverture de session est défini sur **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.
7. Dans **Mot de passe requis**, sélectionnez ON si vous souhaitez demander l'authentification par mot de passe.
8. Dans **Définir par défaut**, sélectionnez ON pour utiliser cette passerelle NetScaler Gateway par défaut.
9. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.
2. Sur la page Ajouter une nouvelle passerelle NetScaler Gateway, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration du LDAP

Jul 25, 2016

Dans XenMobile, vous pouvez configurer une connexion à un ou plusieurs annuaires, tels que Active Directory. Vous pouvez ensuite utiliser la configuration LDAP pour importer des groupes, des comptes d'utilisateurs et les propriétés associées. 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.

Comment fonctionne LDAP

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 configurer des connexions LDAP dans XenMobile

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > LDAP.
   La page de configuration de LDAP s'affiche.

2. Cliquez sur Ajouter.
   La page Ajouter LDAP s'affiche.

3. Configurez les paramètres suivants :
   - Type d'annuaire : cliquez sur le type d'annuaire approprié. Par défaut, Microsoft Active Directory est sélectionné.
   - 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 : entrez le nom de 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 : cliquez sur OUI pour activer les connexions sécurisées.

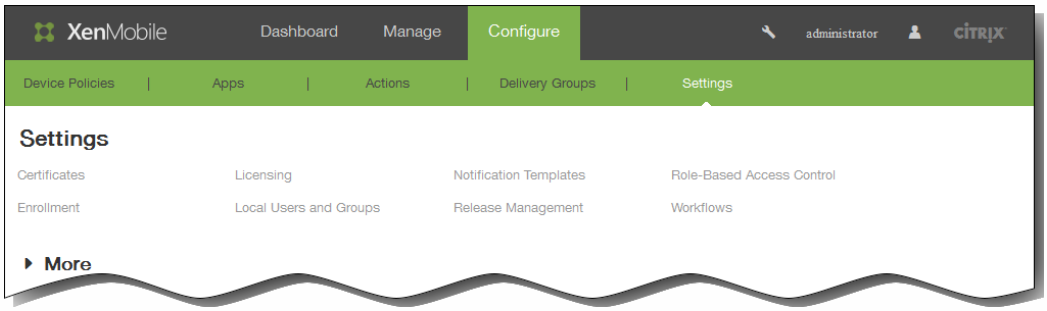
4. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Comptes utilisateur, rôles et paramètres d'inscription

Jul 25, 2016

Dans XenMobile, vous configurez des utilisateurs et des groupes, des rôles pour les utilisateurs et les groupes, ainsi que le mode d'inscription et les invitations dans la page Paramètres de la console XenMobile.



Depuis la page Paramètres, vous pouvez effectuer ce qui suit :

- Cliquez sur Utilisateurs et groupes locaux pour ajouter des comptes utilisateur manuellement ou utilisez un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux. Consultez les informations suivantes pour obtenir plus d'informations :
  - Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile
  - 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
- Cliquez sur Inscription pour configurer jusqu'à sept modes, chacun disposant 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. Consultez les informations suivantes pour obtenir plus d'informations :
  - Pour configurer des modes d'inscription et activer le portail en libre-service
  - Pour activer la découverte automatique pour l'inscription utilisateur dans XenMobile
- 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. Consultez les informations suivantes pour obtenir plus d'informations :
  - Pour créer ou mettre à jour des rôles personnalisés dans XenMobile 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 : Worx Home, SMTP ou SMS. Consultez les informations suivantes pour obtenir plus d'informations :
  - Pour créer ou mettre à jour des modèles de notification dans XenMobile

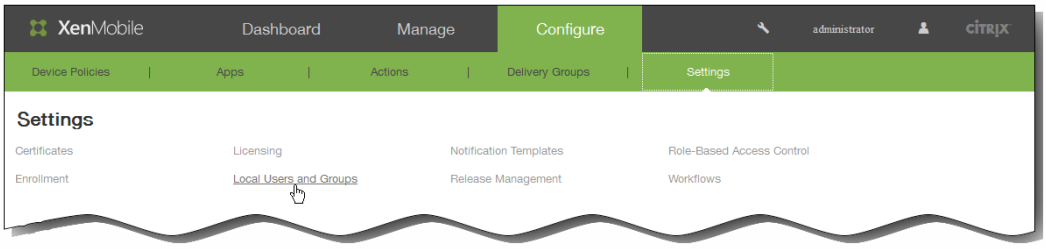
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile

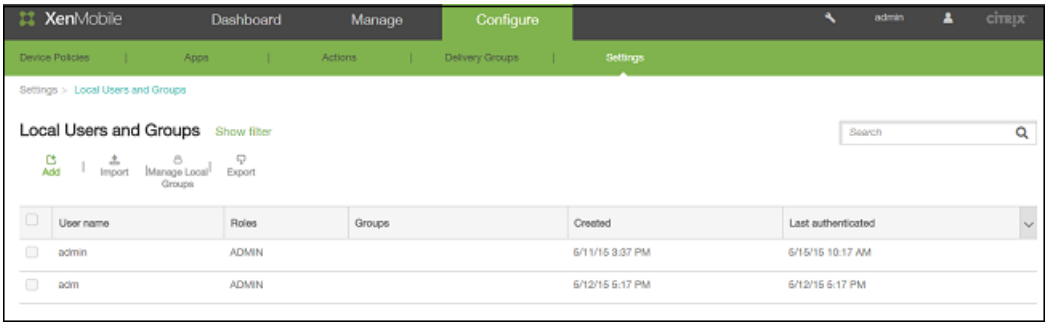
Jul 25, 2016

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 des utilisateurs à partir d'un fichier de provisioning.

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Groupes et utilisateurs locaux.



La page Groupes et utilisateurs locaux s'affiche.

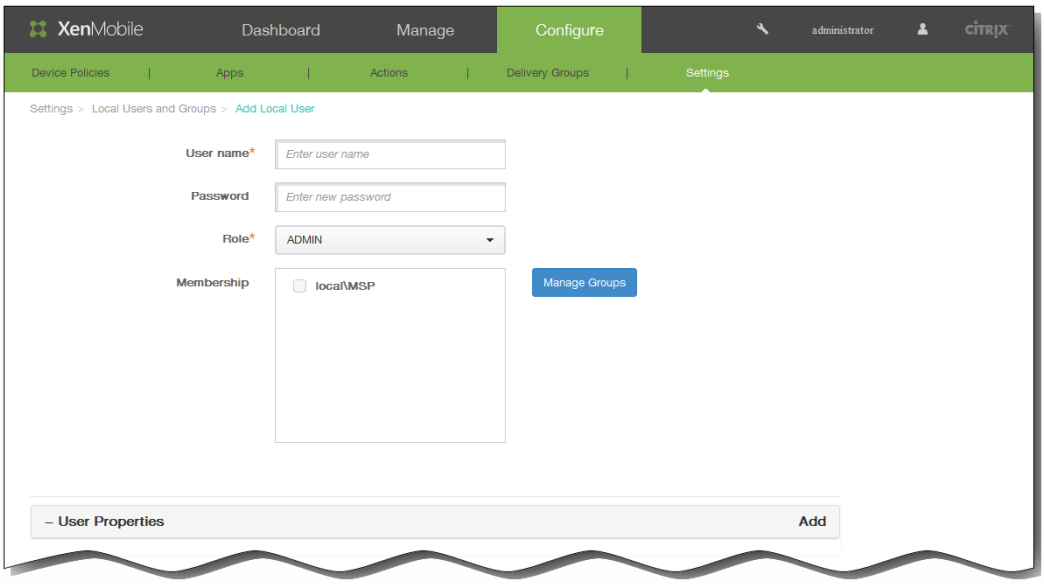


Pour ajouter un utilisateur local

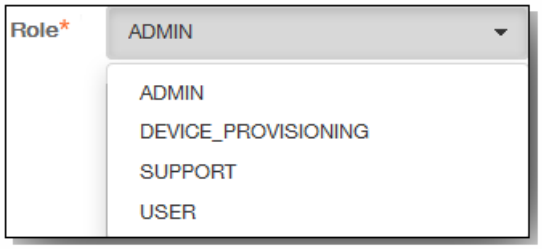
Cette procédure ajoute un seul utilisateur à la fois à XenMobile. Pour ajouter plusieurs utilisateurs, consultez la section Pour importer des comptes utilisateur à l'aide d'un fichier de provisioning .csv.

1. Sur la page Groupes et utilisateurs locaux, cliquez sur Ajouter. La page Ajouter un utilisateur local s'affiche.

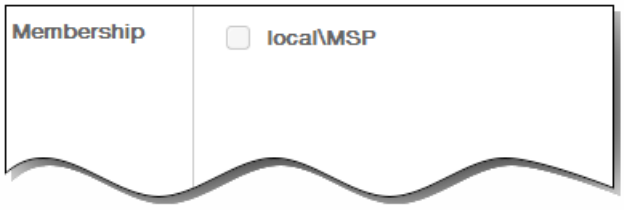
© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Entrez les informations suivantes pour ajouter un nouvel utilisateur local :
   1. Nom d'utilisateur : entrez le nom de l'utilisateur. Il s'agit d'un champ obligatoire.
   2. Mot de passe : entrez un mot de passe utilisateur (facultatif).
   3. Rôle : Dans la liste Rôle, cliquez sur le rôle d'utilisateur. Pour plus d'informations sur les rôles, consultez la section Pour créer ou mettre à jour des rôles personnalisés dans XenMobile avec RBAC.

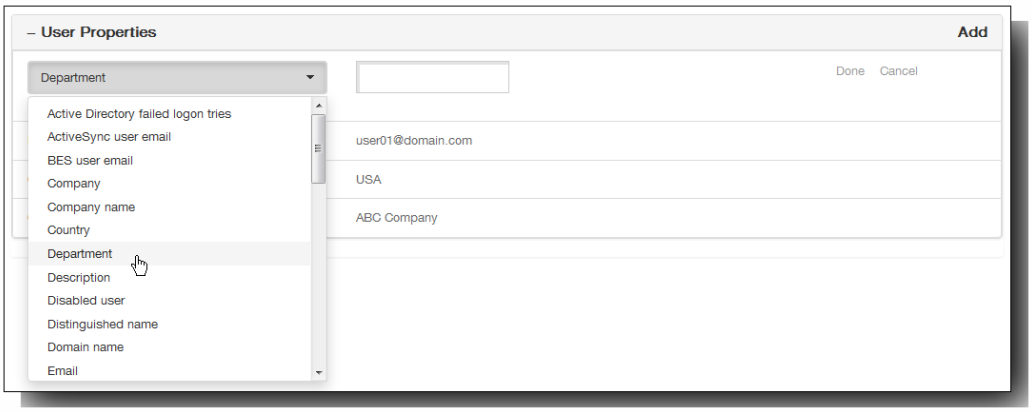


   4. Adhésion : dans la liste Adhésion, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur.



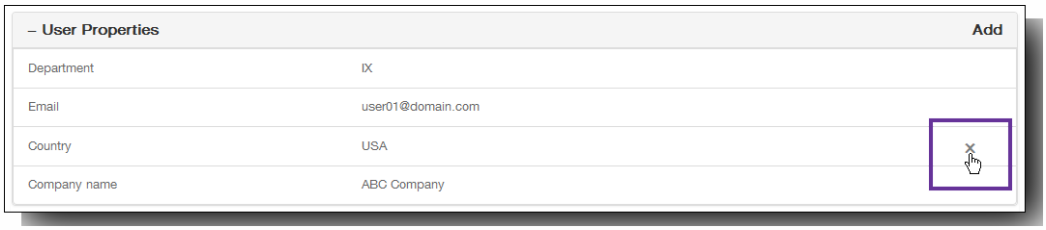
3. Pour ajouter des propriétés utilisateur (facultatif), suivez ces étapes :
   1. Cliquez sur Ajouter en regard de Propriétés utilisateur.
   2. Dans la liste Propriétés utilisateur, cliquez sur une propriété.
   3. Entrez l'attribut de propriété utilisateur dans le champ à côte de la liste.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Cliquez sur Terminé pour enregistrer la propriété utilisateur ou cliquez sur Annuler pour annuler l'opération.
5. Répétez les étapes b, c, et d pour les autres propriétés que vous souhaitez ajouter.

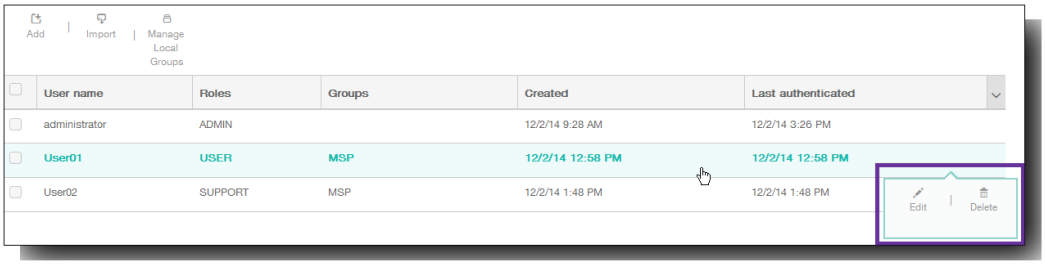
4. Éventuellement, pour modifier une propriété utilisateur, effectuez les opérations suivantes :
   1. Cliquez sur la propriété utilisateur que vous voulez modifier.
   2. Modifiez l'attribut de la propriété utilisateur.
   3. Cliquez sur Terminé pour enregistrer la modification ou cliquez sur Annuler pour annuler la modification.
5. Éventuellement, pour supprimer une propriété utilisateur, effectuez les opérations suivantes :
   1. Placez le pointeur de la souris sur la ligne contenant la propriété utilisateur que vous souhaitez supprimer.
   2. Cliquez sur le X qui apparaît à droite de la ligne.



   La propriété est immédiatement supprimée.
6. Cliquez sur Enregistrer pour enregistrer le nouvel utilisateur.

Pour modifier un utilisateur local

1. Sur la page Groupes et utilisateurs locaux, dans la liste des utilisateurs, cliquez pour sélectionner un utilisateur.



   La page Modifier un utilisateur local apparaît.
2. Modifiez les informations suivantes le cas échéant :
   1. Nom d'utilisateur : entrez le nom de l'utilisateur. Il s'agit d'un champ obligatoire.
   2. Mot de passe : entrez un mot de passe utilisateur (facultatif).

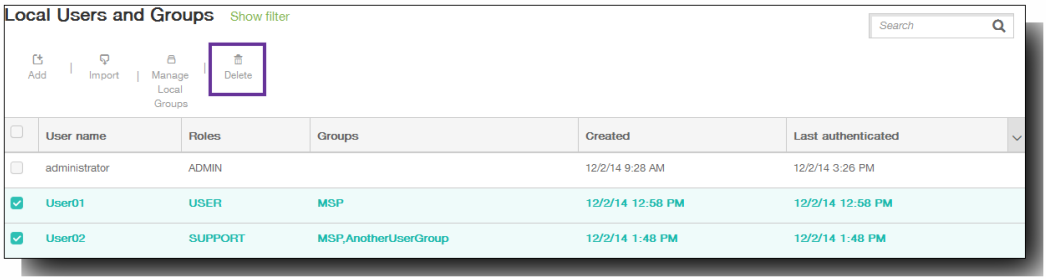
© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Rôle : Dans la liste Rôle, cliquez sur le rôle d'utilisateur.
4. Adhésion : dans la liste Adhésion, cliquez sur le groupe ou les groupes auxquels ajouter l'utilisateur.
5. Propriétés utilisateur : ajoutez de nouvelles propriétés utilisateur ou modifiez des propriétés existantes.

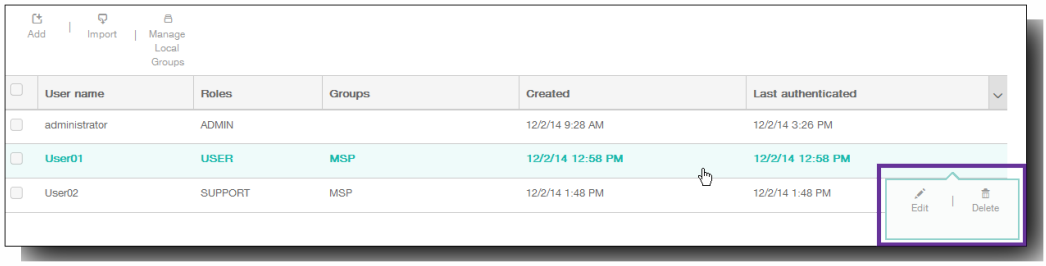
3. Cliquez sur Enregistrer pour enregistrer vos modifications.

Pour supprimer un utilisateur local

1. Sur la page Groupes et utilisateurs locaux, dans la liste des utilisateurs, effectuez l'une des opérations suivantes :
   - Sélectionnez la case à cocher en regard de l'utilisateur ou des utilisateurs que vous souhaitez supprimer, puis cliquez sur Supprimer.



   - Cliquez sur la ligne de l'utilisateur que vous souhaitez supprimer, puis dans le menu qui s'affiche sur la droite, cliquez sur Supprimer.



Un dialogue de confirmation s'affiche. Cliquez sur Supprimer pour confirmer l'opération et supprimer le ou les utilisateurs. Important : vous ne pouvez pas annuler cette opération.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Importation de comptes utilisateur

Jul 25, 2016

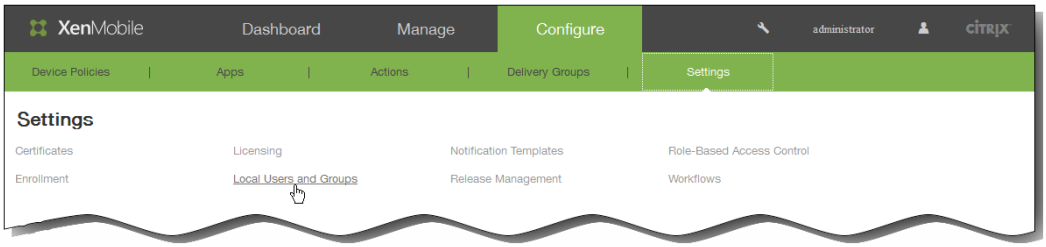
Vous pouvez importer des comptes utilisateur et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

Remarque :

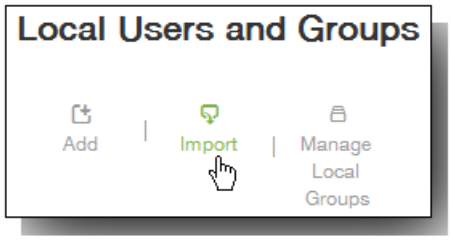
- Si vous importez des utilisateurs à partir d'un annuaire LDAP, utilisez le nom de domaine et le nom d'utilisateur dans le fichier d'importation. Par exemple, spécifiez le nomd'utilisateur@domaine.com. Cette syntaxe empêche d'autres recherches qui ralentiraient la vitesse d'importation.
- Si vous importez des utilisateurs sur l'annuaire utilisateur interne XenMobile, désactivez le domaine par défaut pour accélérer le processus d'importation. Vous pouvez réactiver le domaine par défaut après l'importation des utilisateurs internes.
- Les utilisateurs locaux peuvent être au format « Nom d'utilisateur principal (UPN) », mais Citrix vous recommande 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 Web XenMobile, cliquez sur Configurer > Paramètres > Groupes et utilisateurs locaux.



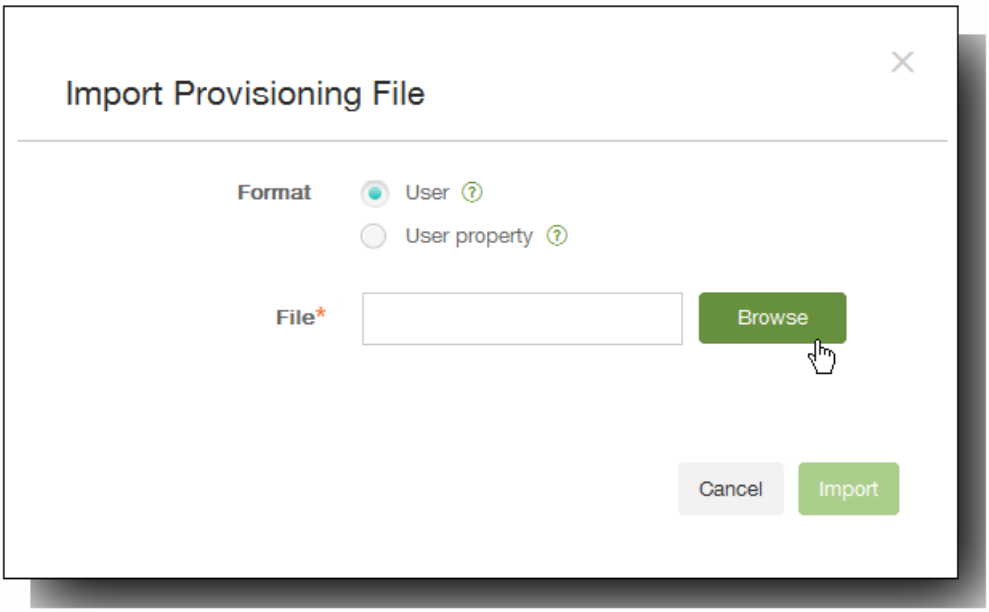
2. Sur la page Groupes et utilisateurs locaux, cliquez sur Importer.



La boîte de dialogue Importer le fichier de provisioning apparaît.

3. Dans la boîte de dialogue Importer le fichier de provisioning, sélectionnez le format du fichier de provisioning que vous importez.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. En regard de Fichier, cliquez sur Parcourir pour accéder à l'emplacement du fichier de provisioning, puis cliquez sur Importer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Formats des fichiers de provisioning

Jul 25, 2016

Un fichier de provisioning que vous créez manuellement et utilisez pour l'importation de comptes utilisateur et de propriétés sur Device Manager doit être au format suivant :

- Champs des fichiers de provisioning utilisateur : `user;password;role;group1;group2`
- Champs d'attributs des fichiers de provisioning 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 au format `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

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 : prop 2 value

© 1999-2017 Citrix Systems, Inc. All rights reserved.

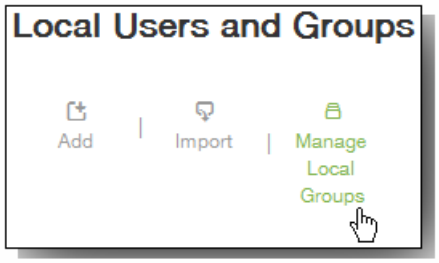
Ajout ou suppression de groupes

Jul 25, 2016

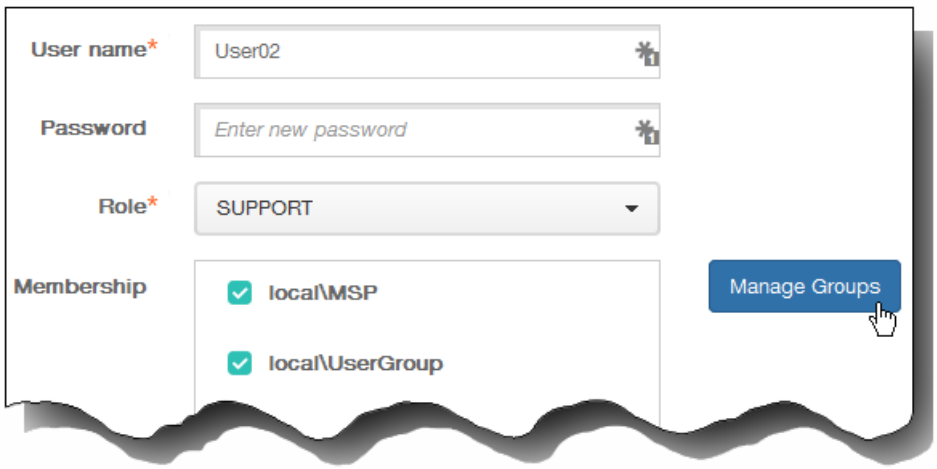
Vous gérez les groupes dans la boîte de dialogue Gérer les groupes dans la console XenMobile, que vous pouvez trouver sur la page Groupes et utilisateurs locaux, la page Ajouter un utilisateur local où la page Modifier un utilisateur local. Aucune commande ne permet de modifier un groupe. Si vous supprimez un groupe, n'oubliez pas que la suppression d'un groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association des utilisateurs 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.

Pour ajouter un groupe local

1. Procédez comme suit :
   - Sur la page Groupes et utilisateurs locaux, cliquez sur Gérer les groupes locaux.

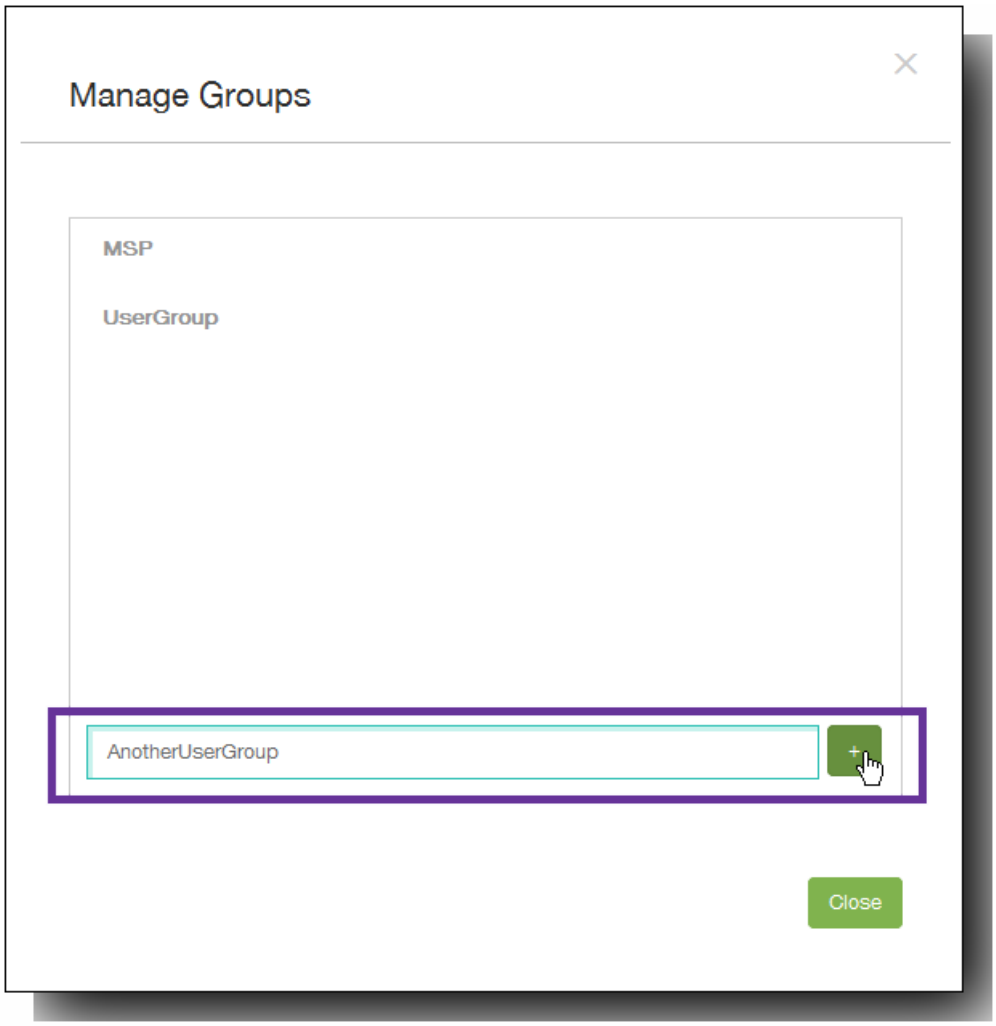


   - Sur la page Ajouter un utilisateur local ou la page Modifier un utilisateur local, cliquez sur Gérer les groupes.



   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 (+).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Le groupe d'utilisateurs est ajouté à la liste.

3. Cliquez sur Fermer.

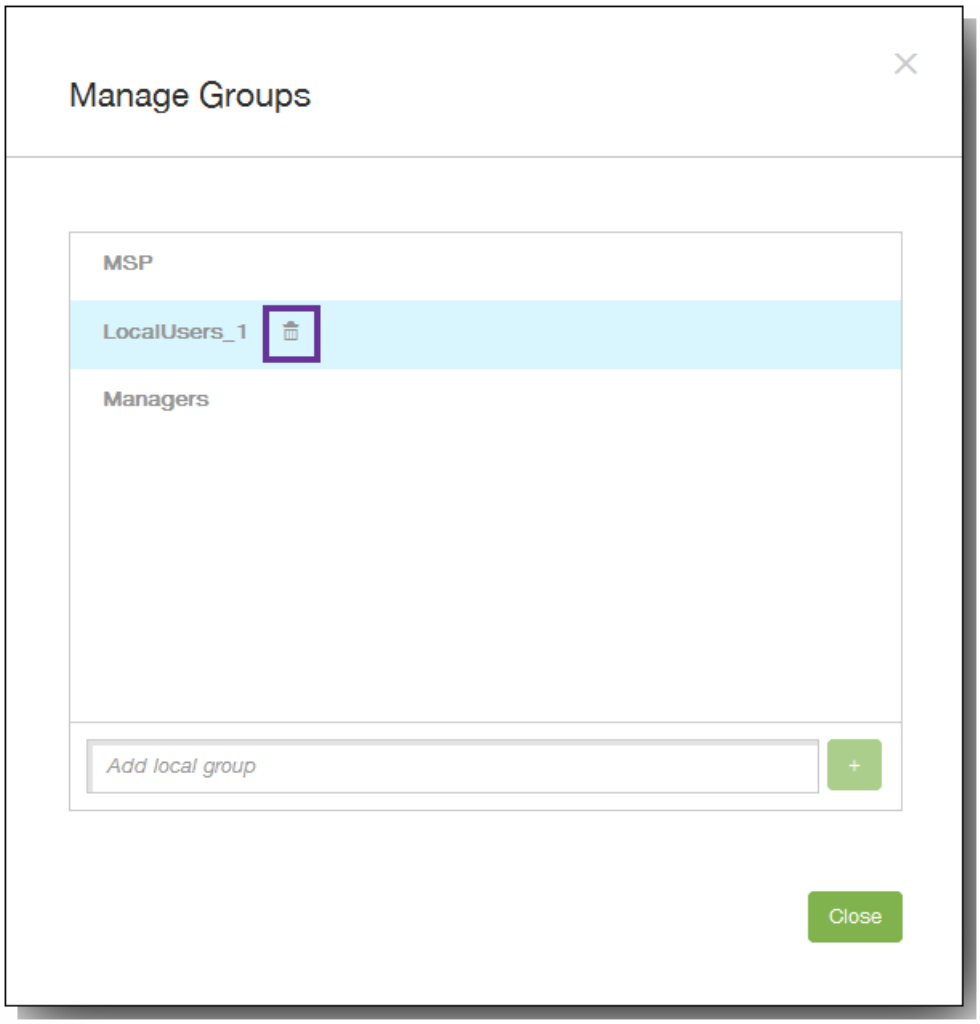
Pour supprimer un groupe

Remarque : la suppression d'un groupe n'a aucun effet sur les comptes d'utilisateur. La suppression d'un groupe supprime simplement l'association des utilisateurs 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 Groupes et utilisateurs locaux, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour configurer des modes d'inscription et activer le portail en libre-service

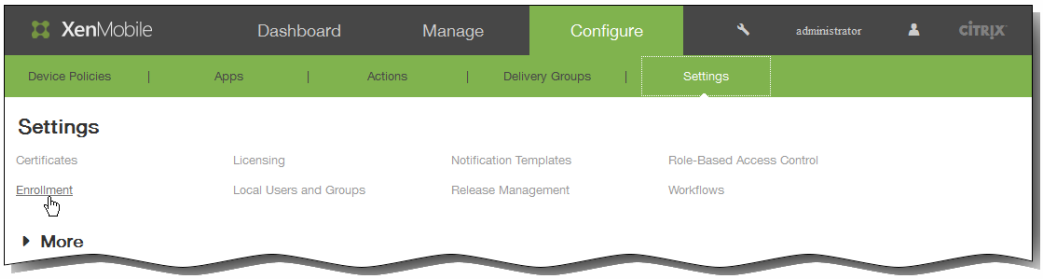
Jul 25, 2016

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, 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 console XenMobile, à partir de la page Gérer > Inscription (voir Inscription d'utilisateurs et d'appareils dans XenMobile).

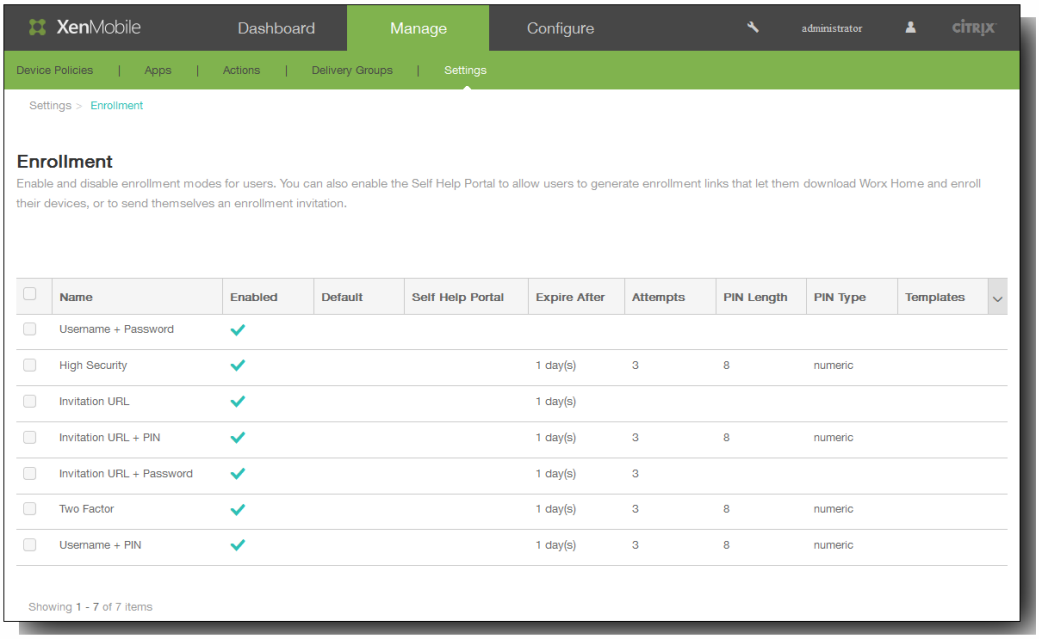
Remarque : si vous prévoyez d'utiliser des modèles de notification personnalisés, vous devez définir les modèles avant de configurer des modes d'inscription. Pour de plus amples informations sur les modèles de notification, consultez la section Pour créer ou mettre à jour des modèles de notification dans XenMobile.

1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Inscription.

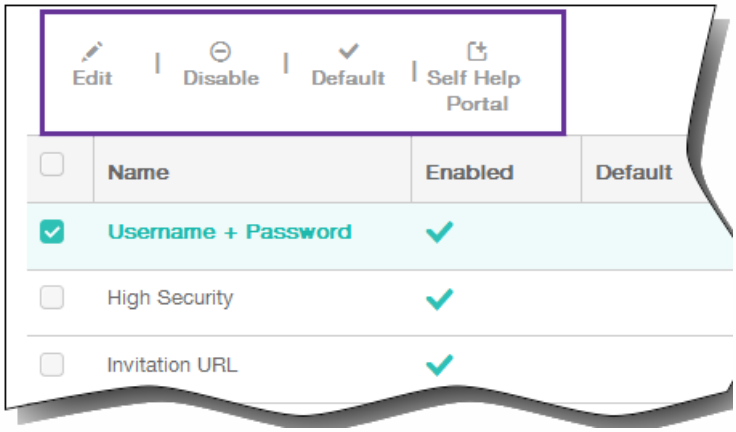


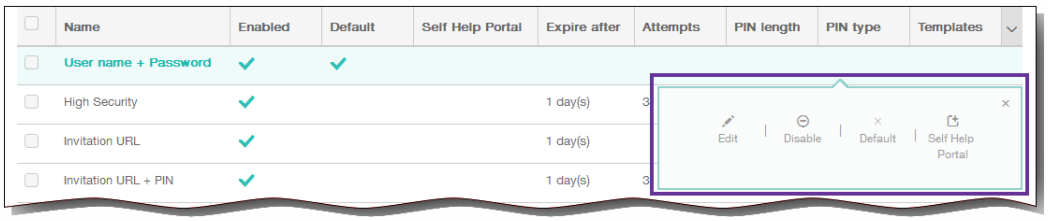
La page Inscription s'affiche. Elle contient un tableau de tous les modes d'inscription disponibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Sélectionnez un mode d'inscription à modifier dans la liste, puis définissez le mode comme le mode par défaut, supprimez le mode ou autorisez l'accès des utilisateurs via le portail en libre-service.
   Remarque : lorsque vous activez 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 ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

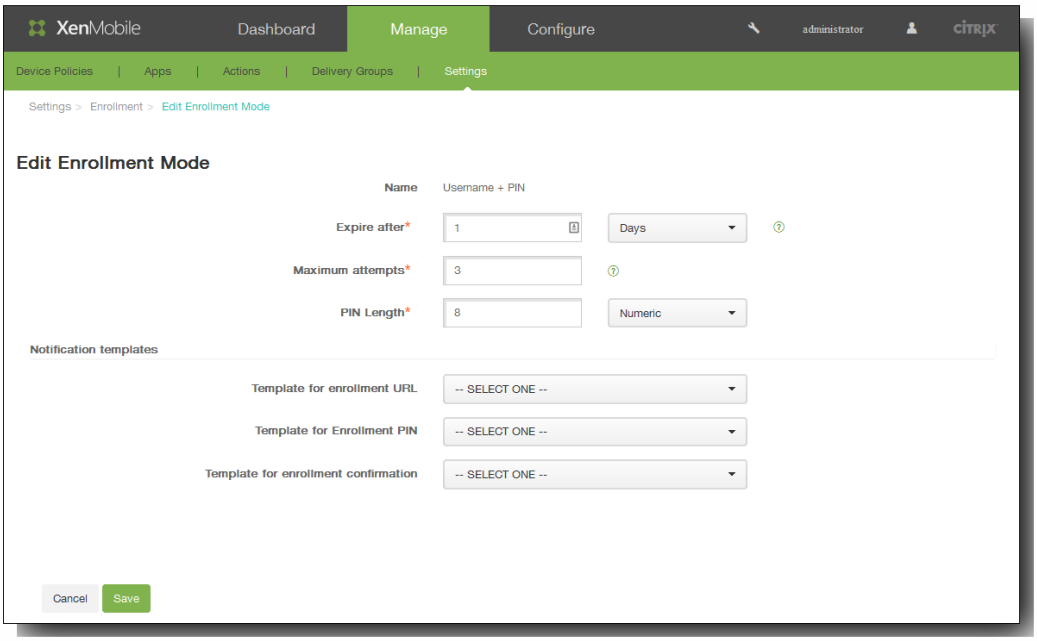




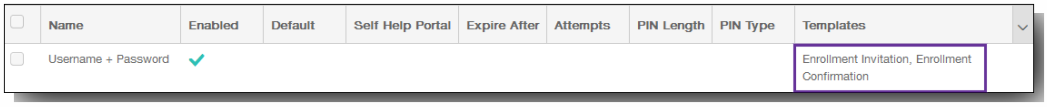
Pour modifier un mode d'inscription

1. Dans la liste Inscription, sélectionnez un mode d'inscription, puis cliquez sur Modifier. En fonction du mode que vous sélectionnez, vous pouvez voir d'autres options que les options illustrées dans la figure suivante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Modifiez les informations suivantes le cas échéant :
   1. Expire après : entrez un délai d'expiration au-delà duquel les utilisateurs ne peuvent pas inscrire leurs appareils.
      Remarque : entrez 0 pour empêcher l'invitation d'expirer.
   2. Jours : sélectionnez Jours ou Heures afin qu'ils correspondent au délai d'expiration que vous avez entré dans Expire après.
   3. 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.
      Remarque : entrez 0 pour autoriser un nombre illimité de tentatives.
   4. Longueur du code PIN : entrez le nombre de chiffres ou de caractères que le code PIN généré doit contenir.
   5. Numérique : sélectionnez Numérique ou Alphanumérique pour le type de PIN.
3. Sous Modèles de notification, modifiez les paramètres suivants le cas échéant :
   1. 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 Pour créer ou mettre à jour des modèles de notification dans XenMobile.
   2. Modèle pour la confirmation d'inscription : sélectionnez un modèle à utiliser pour informer un utilisateur que l'inscription a réussi.
4. Cliquez sur Enregistrer pour valider vos modifications.



Pour définir un mode d'inscription comme mode par défaut

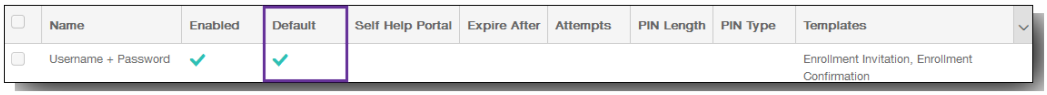
Lorsque vous définissez un mode d'inscription en tant que mode par défaut, le mode est utilisé pour toutes les demandes d'inscription d'appareil, sauf si vous sélectionnez un autre mode d'inscription. Si aucun mode d'inscription n'est défini par

© 1999-2017 Citrix Systems, Inc. All rights reserved.

défaut, vous devez créer une demande d'inscription pour chaque inscription d'appareil.

Remarque : seuls Nom d'utilisateur + mots de passe, Deux facteurs ou Nom d'utilisateur + PIN peuvent être définis en tant que mode d'inscription par défaut.

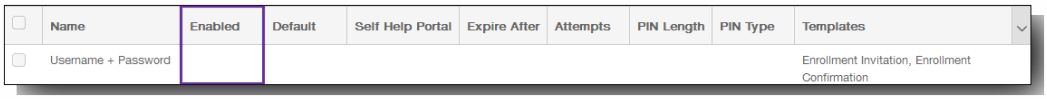
1. Sélectionnez l'un des trois modes suivants à définir comme mode d'inscription par défaut : Nom d'utilisateur + mots de passe, Deux facteurs ou Nom d'utilisateur + PIN.
   Remarque : le mode sélectionné doit être activé pour être défini comme mode par défaut.
2. Cliquez sur Mode par défaut. Le mode 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.



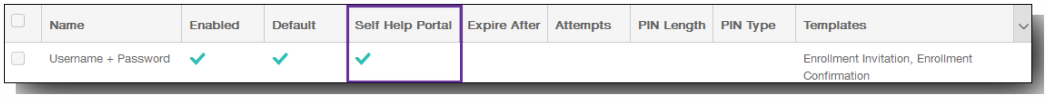
Pour activer un mode d'inscription sur le portail en libre-service

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de rôles avec RBAC

Jul 25, 2016

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.
- **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 également créer de nouveaux rôles utilisateur dotés d'autorisations permettant d'accéder à des fonctions système spécifiques au-delà des fonctions définies par ces rôles par défaut en utilisant les rôles par défaut en tant que modèles que vous personnalisez.

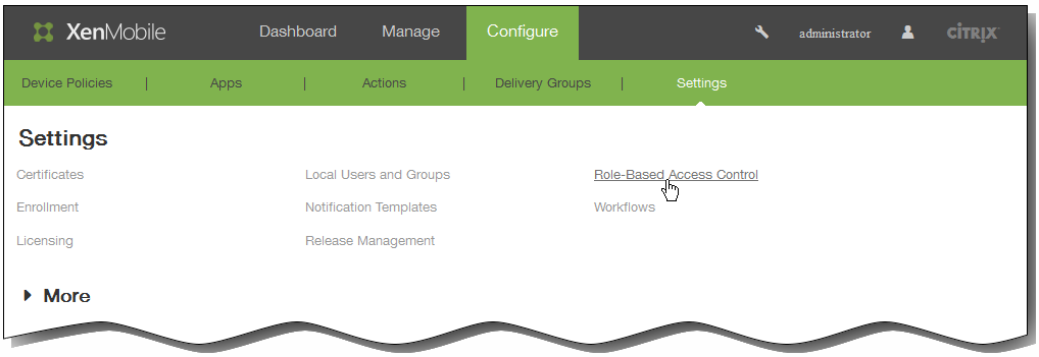
Les rôles peuvent être attribués à des utilisateurs locaux (au niveau de l'utilisateur) ou à des groupes Active Directory (tous les utilisateurs de ce groupe ont les mêmes autorisations). Si un utilisateur appartient à plusieurs groupes Active Directory, les autorisations sont fusionnées pour définir 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 :

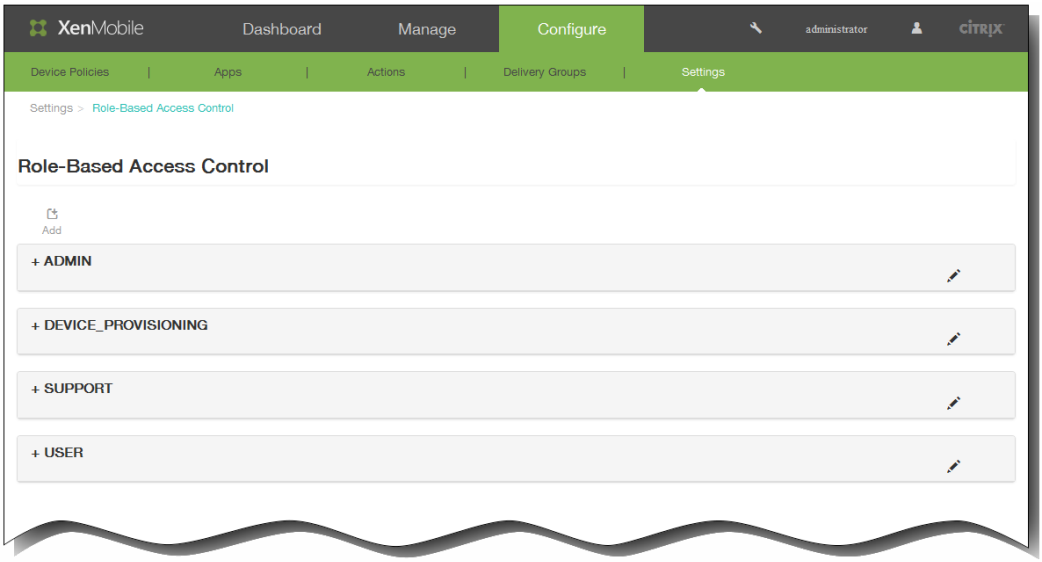
- Créer un nouveau rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Contrôle d'accès basé sur un rôle.

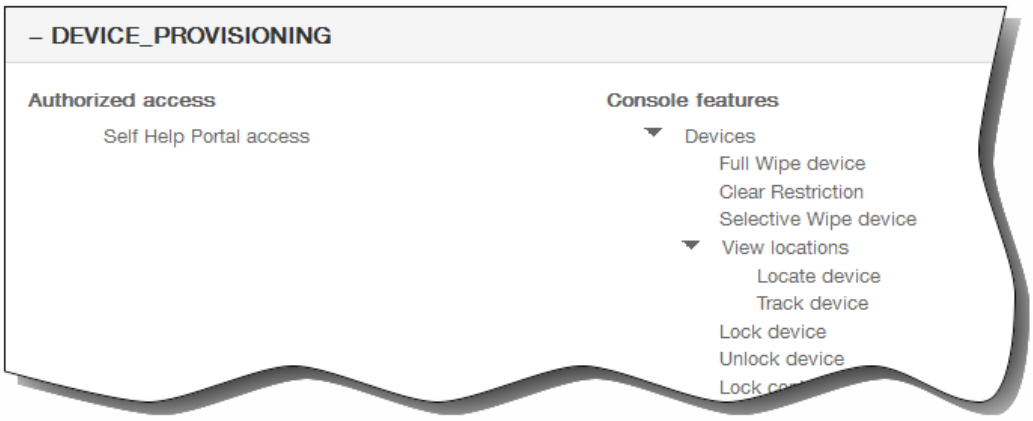


La page Rôle qui apparaît affiche les quatre rôles utilisateur par défaut, ainsi que tout rôle que vous avez déjà ajouté.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

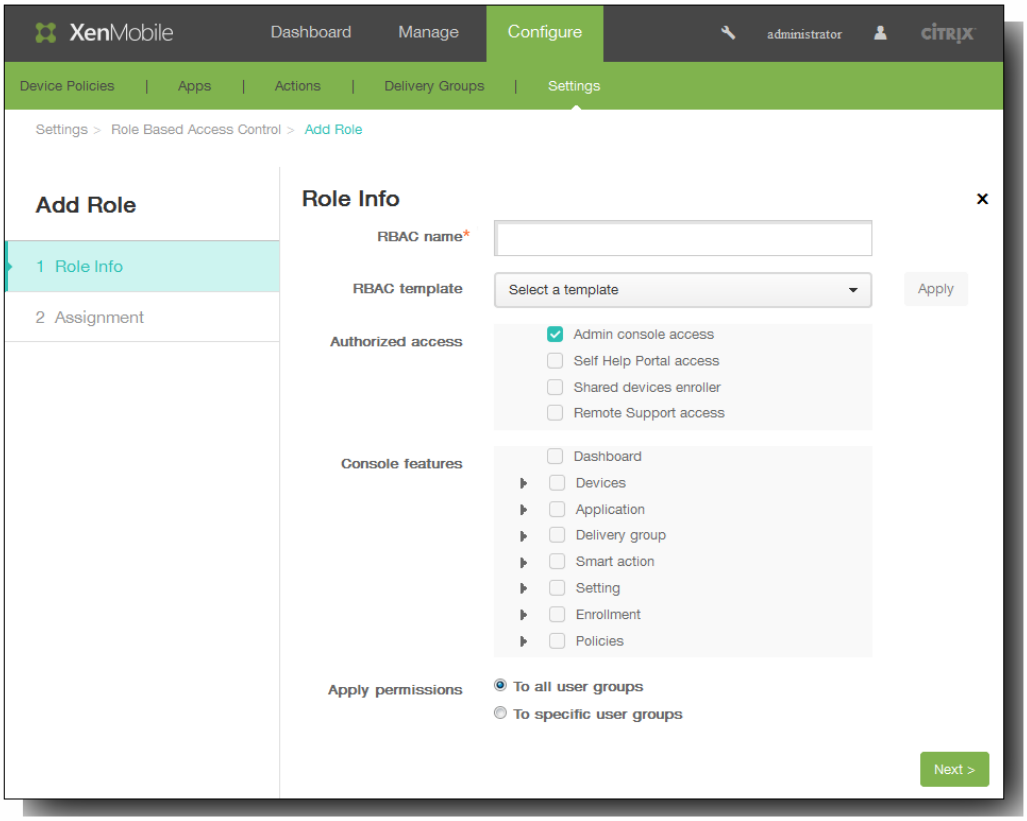


Remarque : si vous cliquez sur le signe plus (+) à côté d'un rôle, celui-ci se développe pour afficher toutes les autorisations pour ce rôle, comme illustré dans la figure suivante.



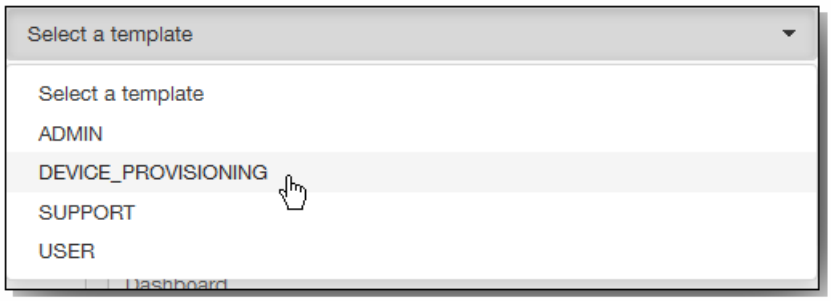
2. Cliquez sur Ajouter pour ajouter un nouveau rôle utilisateur, cliquez sur l'icône de crayon à droite d'un rôle existant pour modifier le rôle, ou cliquez sur l'icône de corbeille à droite d'un rôle que vous avez précédemment défini pour supprimer le rôle. Vous ne pouvez pas supprimer les rôles utilisateur par défaut.
   - Lorsque vous cliquez sur Ajouter ou l'icône de crayon, la page Ajouter un rôle ou Modifier le rôle s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



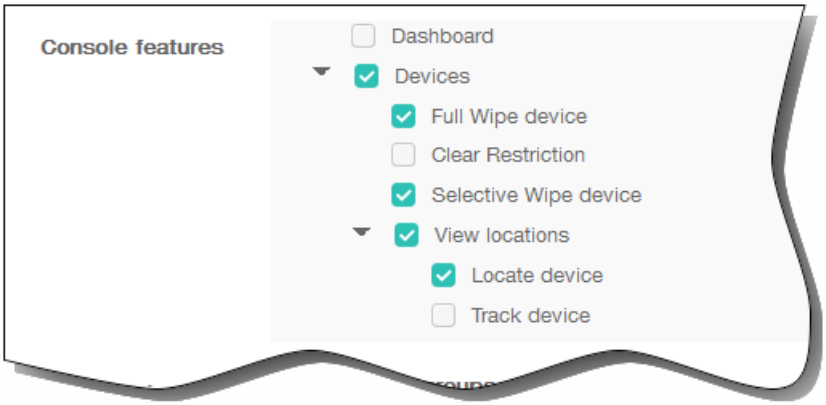
- Lorsque vous cliquez sur l'icône de corbeille, une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer le rôle sélectionné.

3. Entrez les informations suivantes pour créer un nouveau rôle utilisateur ou pour modifier un rôle utilisateur existant :
   1. Nom RBAC : entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle existant.
   2. Modèle RBAC : cliquez sur un modèle à partir duquel créer le nouveau rôle ou cliquez sur un nouveau modèle pour un rôle existant.
      Remarque : les modèles RBAC sont les rôles utilisateur par défaut, ainsi que les rôles que vous avez précédemment définis. Ils définissent les fonctions système auxquelles les utilisateurs associés à ce rôle ont accès. 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.

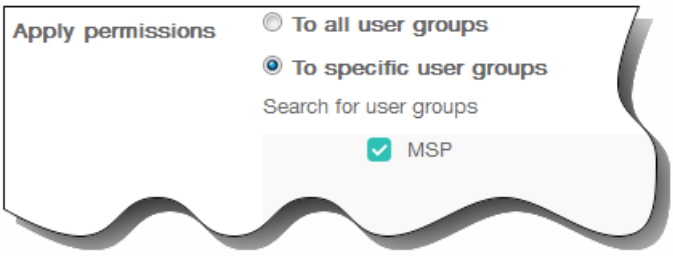


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cliquez sur Appliquer pour renseigner les cases Accès autorisé et Fonctionnalités de la console avec les autorisations d'accès prédéfinies pour le modèle sélectionné.
- Sélectionnez et décochez les cases à cocher appropriées dans Accès autorisé et Fonctionnalités de la console pour personnaliser le rôle.
  Remarque : 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 permet d'accéder en lecture seule à cette partie de la console ; vous devez sélectionner des options individuelles en-dessous du niveau supérieur pour activer l'accès en écriture/mise à jour pour cette option. Par exemple, dans la figure suivante, l'utilisateur dispose d'un accès en lecture seule à l'option Effacer les restrictions.



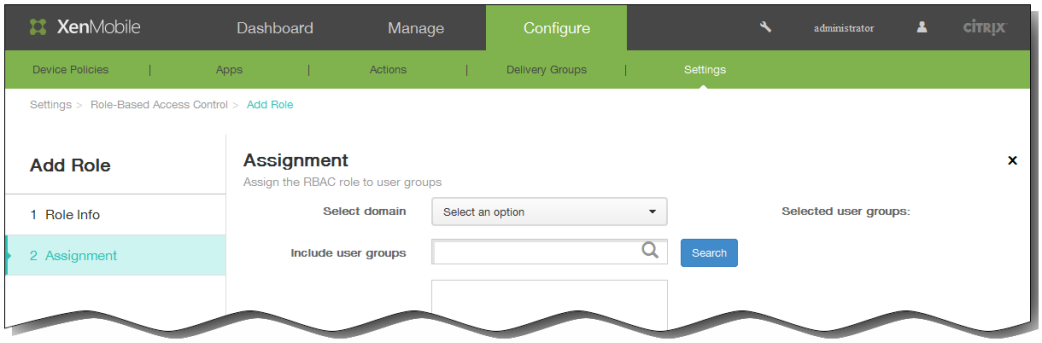
3. Appliquer les autorisations : sélectionnez les groupes auxquels vous voulez appliquer les autorisations sélectionnées.



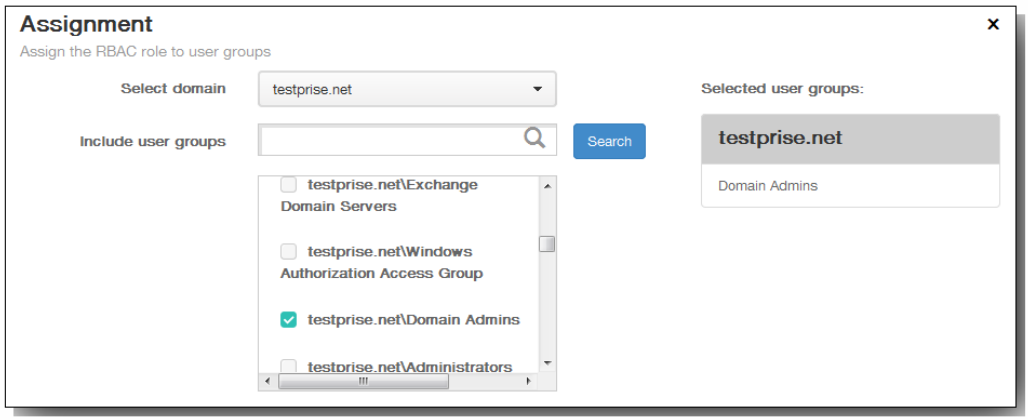
Si vous cliquez sur À des groupes d'utilisateurs spécifiques, une liste des groupes s'affiche à partir de laquelle vous pouvez sélectionner un ou plusieurs groupes.

4. Cliquez sur Suivant. La page Attribution s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Entrez les informations suivantes pour attribuer le rôle à des groupes d'utilisateurs, puis cliquez sur Enregistrer.
   1. Sélectionner un domaine : cliquez sur un domaine dans la liste.
   2. 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.
   3. 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.



Pour supprimer un groupe d'utilisateurs de la liste Groupes d'utilisateurs sélectionnés, effectuez l'une des opérations suivantes :

- 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.

Les groupes d'utilisateurs dans la liste ont des coches en regard de leur nom dans la liste qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Rôles et autorisations RBAC

Jul 25, 2016

Chaque rôle RBAC prédéfini dispose de certains accès et de certaines autorisations associés à ce rôle. Cet article explique chacune de ces autorisations. Pour plus d'informations sur la manière de configurer les rôles RBAC, consultez la section Configuration de rôles avec RBAC.

- Rôle d'administrateur
- Rôle Support
- Rôle Utilisateur

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour activer la découverte automatique pour l'inscription utilisateur dans XenMobile

Jul 25, 2016

La découverte 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 des 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 sur https://xenmobiletools.citrix.com. Pour plus d'informations sur le portail Autodiscovery Service, consultez la rubrique relative à XenMobile Autodiscovery Service.

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 :
   1. 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.
   2. 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 découverte 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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Les SAN appropriés pour les domaines restants (par exemple, enterpriseenrollment.masociété2.com, enterpriseenrollment.masociété3.com, etc).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

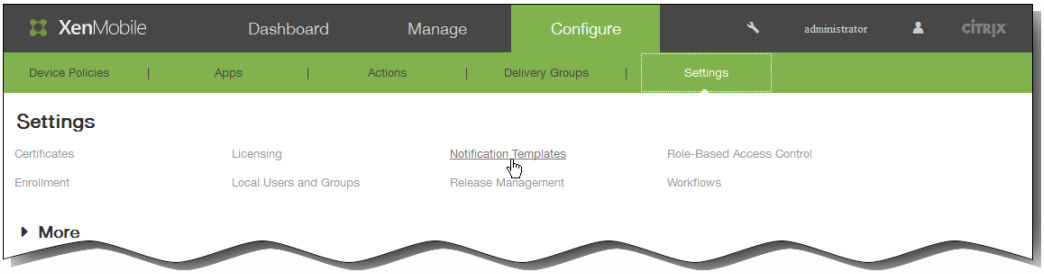
Création et mise à jour de modèles de notification

Jul 25, 2016

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 : Worx Home, SMTP ou SMS.

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. Pour de plus amples informations, consultez la section Notifications dans XenMobile

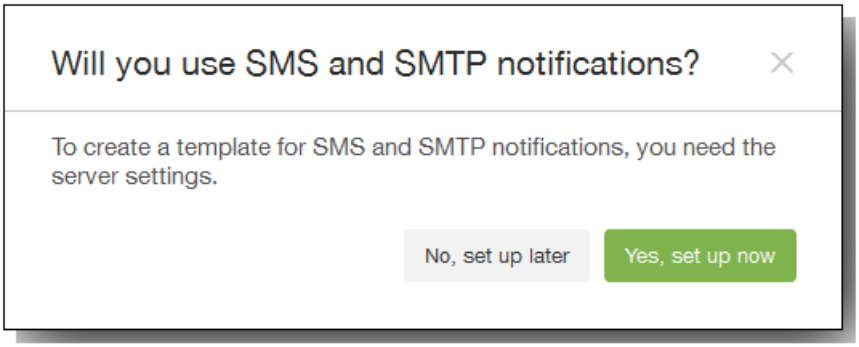
1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Modèles de notification.



2. Procédez comme suit :
   - Cliquez sur Ajouter pour ajouter un nouveau modèle de notification. 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. Pour de plus amples informations, consultez la section Notifications dans XenMobile

     Remarque : si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP maintenant, vous serez redirigé vers la page Configurer > Paramètres > Serveur de notification. Après avoir configuré les canaux que vous souhaitez utiliser, vous pouvez retourner sur la page Configurer > Paramètres > 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.

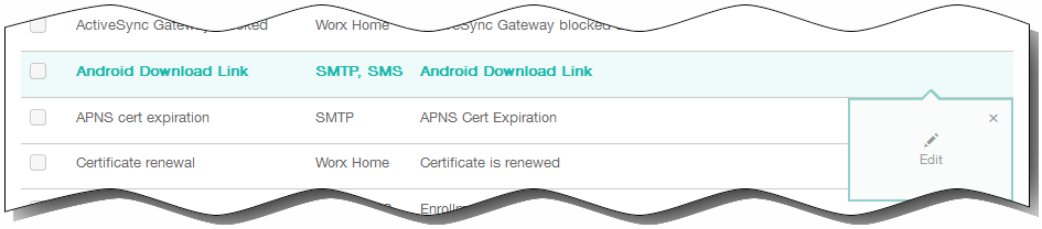


   - Sélectionnez un modèle existant à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

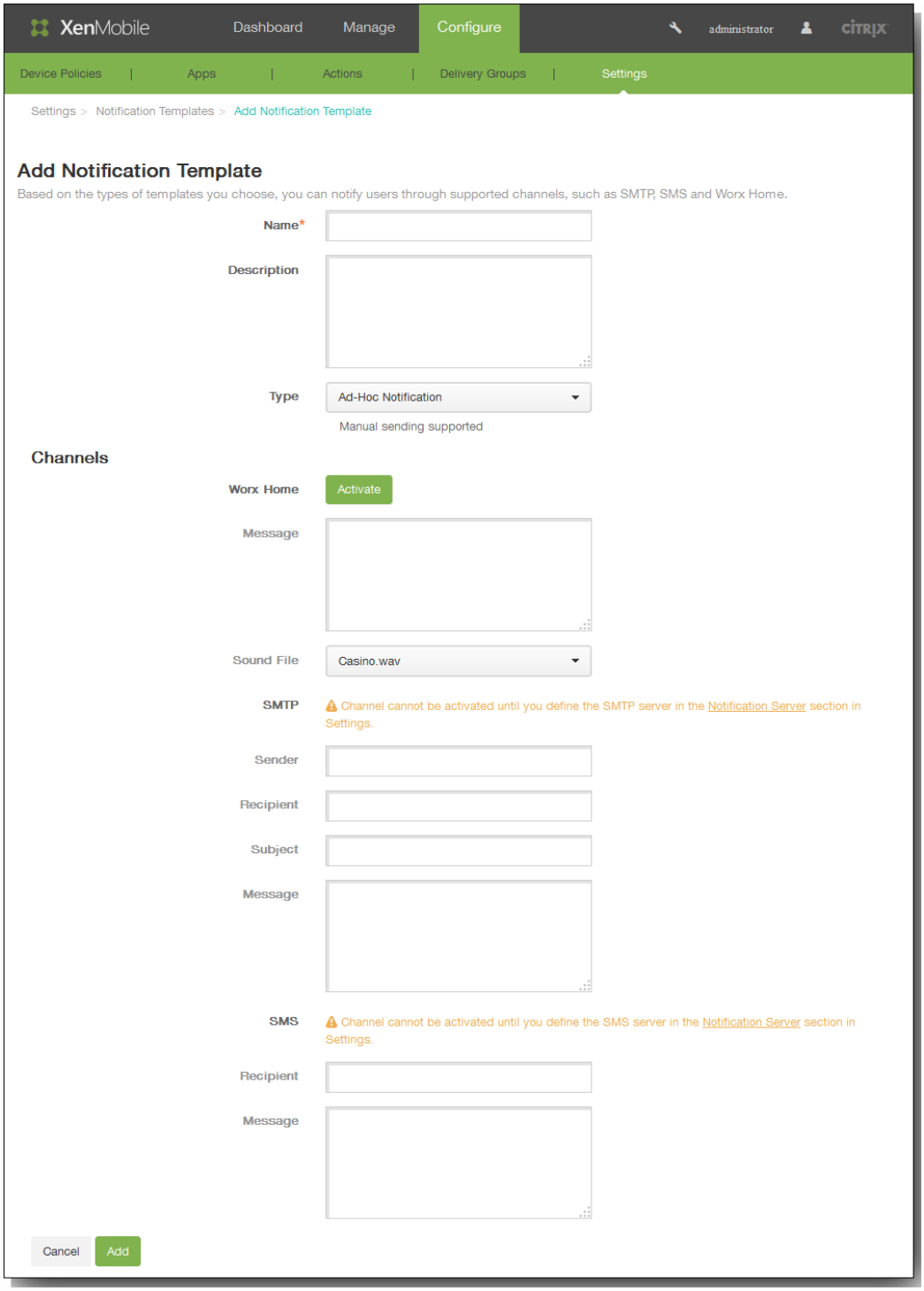
Remarque :

- Vous ne pouvez supprimer que les modèles de notification que vous avez ajoutés ; vous ne pouvez pas supprimer des modèles de notification prédéfinis.
- Lorsque vous sélectionnez la case à cocher en regard d'un modèle de notification, le menu d'options s'affiche au-dessus de la liste de modèles de notification ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.
- XenMobile comprend plusieurs modèles de notification prédéfinis qui reflètent les différents types d'événements auxquels XenMobile répond automatiquement pour chaque appareil dans le système.



Lorsque vous cliquez sur le bouton pour ajouter un modèle, la page Ajouter un modèle de notification s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sur la page Ajouter un modèle de notification (ou Modifier le modèle de notification si vous modifiez un modèle de notification), entrez ou modifier les informations suivantes :
   1. Nom : entrez un nom descriptif pour le modèle.
   2. Description : entrez une description pour le modèle.
   3. Type : sélectionnez le type de notification. Seuls les canaux pris en charge pour le type sélectionné s'affichent. 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 :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- ${outofcompliance.reason(whitelist_blacklist_apps_name)}
- ${outofcompliance.reason(smg_block)}

Attention : 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.

4. 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 Worx Home, seuls les appareils iOS et Android reçoivent des notifications ; elles apparaissent dans la barre de notification de l'appareil.
- Si vous choisissez SMS, seuls les utilisateurs d'appareils équipés d'une carte SIM reçoivent la notification.
- Si vous choisissez SMTP, la plupart des utilisateurs recevront le message, car ils se sont inscrits avec leurs adresses e-mail.

Worx Home

1. Activer : cliquez pour activer le canal de notification.
2. Message : entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez Worx Home.
3. Fichier son : sélectionnez le son de notification que l'utilisateur entend lorsque la notification est reçue.

SMTP

1. Cliquez sur Activer pour activer le canal de notification.
   Important : vous ne pouvez activer la notification SMTP que si vous avez déjà configuré le serveur SMTP. Pour de plus amples informations, consultez la section Notifications dans XenMobile
2. Expéditeur : entrez un expéditeur (facultatif) pour la notification, qui peut être un nom, une adresse e-mail, ou les deux.
3. 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 Ajout d'appareils et affichage des détails des appareils dans XenMobile.
4. Sujet : entrez un sujet pour la notification. Ce champ est obligatoire si vous utilisez des SMTP.
5. Message : entrez le message à envoyer à l'utilisateur.

SMS

1. Cliquez sur Activer pour activer le canal de notification.
   Important : vous ne pouvez activer la notification SMTP que si vous avez déjà configuré le serveur SMTP. Pour de plus amples informations, consultez la section Notifications dans XenMobile
2. 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. 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. Pour de plus amples informations, consultez la section Ajout d'appareils et affichage des détails des appareils dans XenMobile.
3. Message : entrez le message à envoyer à l'utilisateur. Ce champ est obligatoire si vous utilisez des SMS.
   Important : vous ne pouvez activer la notification SMS que si vous avez déjà configuré la passerelle SMS. Pour de plus

© 1999-2017 Citrix Systems, Inc. All rights reserved.

amples informations, consultez la section Notifications dans XenMobile

5. Cliquez sur Ajouter pour ajouter le nouveau modèle ou cliquez sur Enregistrer pour enregistrer vos modifications. Lorsque tous les canaux sont correctement configurés, ils apparaissent dans cet ordre sur la page Modèles de notification : SMTP, SMS et Worx Home. Tout canal qui n'est pas correctement configuré apparaît après les canaux correctement configurés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gestion des groupes de mise à disposition

Jul 25, 2016

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. 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.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 délivre uniquement la première ressource dans cette liste. En supprimant les ressources dupliquées 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 :

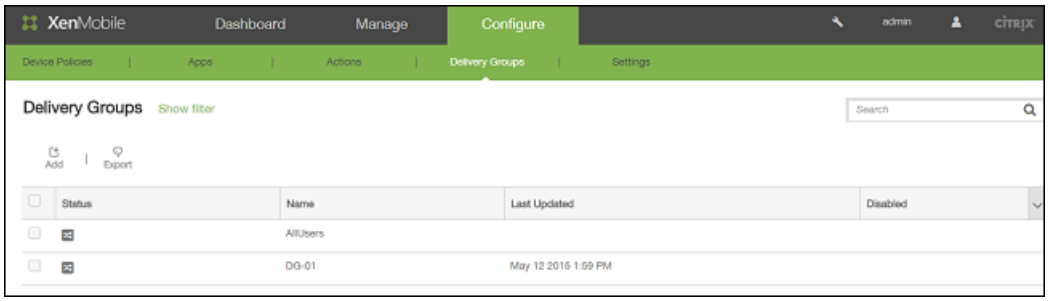
- Groupe de mise à disposition A : avec un ordre **non spécifié** pour les ressources (RES) ; contient RES1 et RES2.
- Groupe de mise à disposition B : avec un ordre **spécifié** pour les ressources (RES) ; contient RES3 et RES2. Dans ce cas, vous souhaitez mettre à disposition RES3 avant RES2.

Si l'algorithme de calcul classe uniquement les groupes de déploiement par nom, XenMobile réaliserait le déploiement dans cet ordre : RES1, RES2, RES3. XenMobile ignorerait RES2, un doublon, du groupe de mise à disposition B.

Toutefois, l'algorithme de calcul place les ressources du groupe de mise à disposition B plus haut dans la liste que celles provenant du groupe de mise à disposition A, donc XenMobile effectue le déploiement dans cet ordre : RES3, RES2, RES1. XenMobile ignore RES2 du groupe de mise à disposition A, car il en double. Par conséquent, cet algorithme respecte l'ordre spécifié par l'administrateur XenMobile.

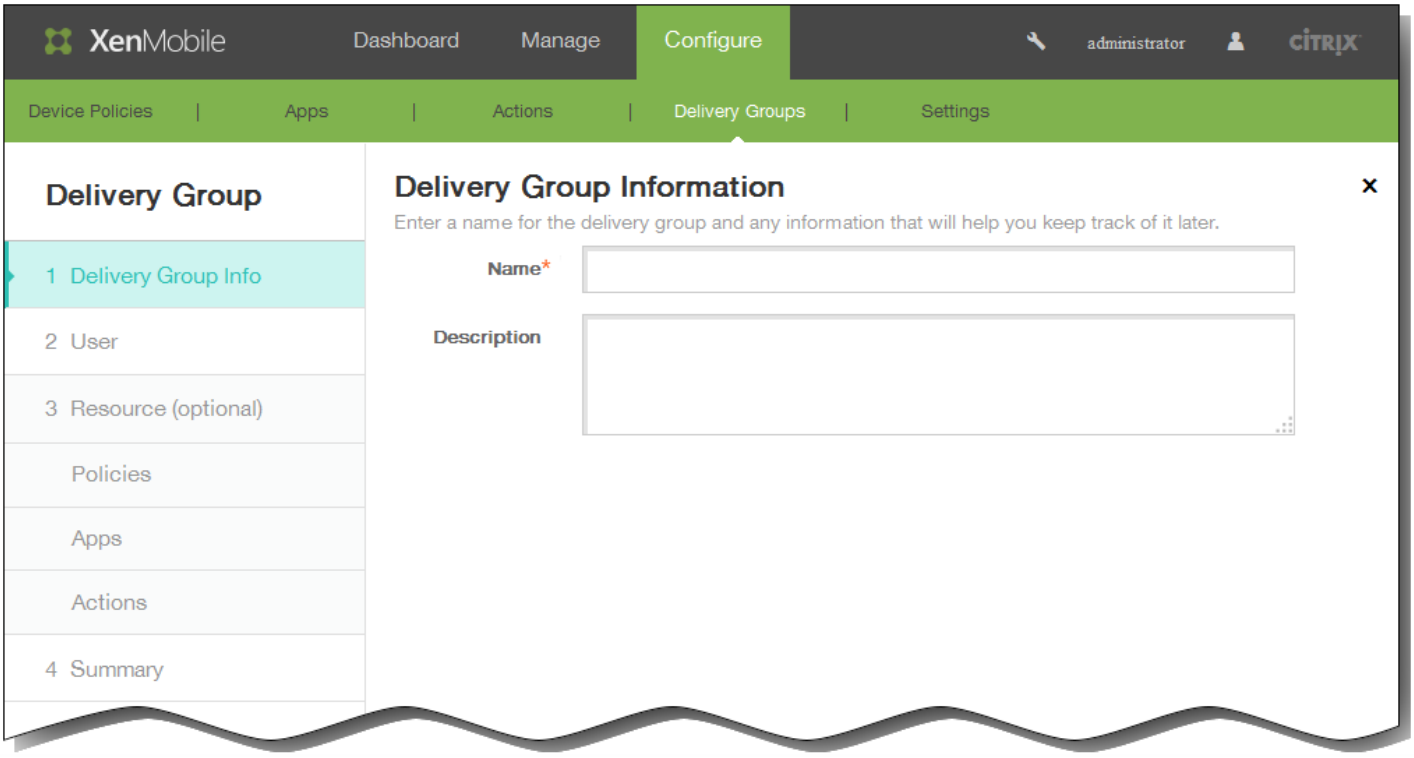
Pour ajouter un groupe de mise à disposition

1. Dans la console XenMobile, cliquez sur **Configurer > Groupes de mise à disposition**. La page **Groupes de mise à disposition** s'affiche.



2. Depuis la page **Groupes de mise à disposition** , cliquez sur **Ajouter**. La page **Informations sur le groupe de mise à disposition** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



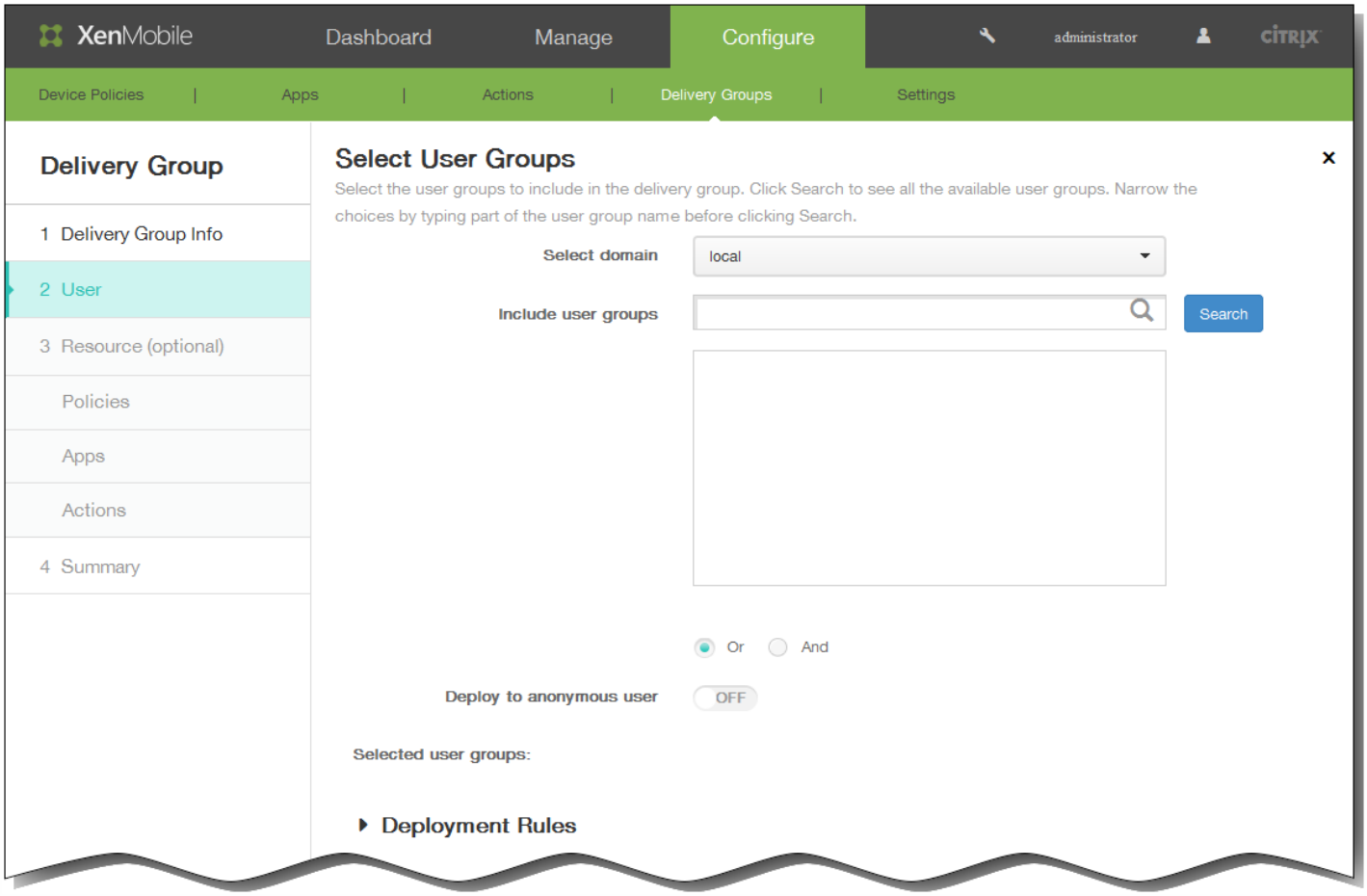
3. Sur la page **Informations sur le groupe de mise à disposition**, entrez les informations suivantes :

   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 **Utilisateur du groupe de mise à disposition** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Sur la page **Sélectionner des groupes d'utilisateurs**, entrez les informations suivantes :

    a. **Sélectionner un domaine** : sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.

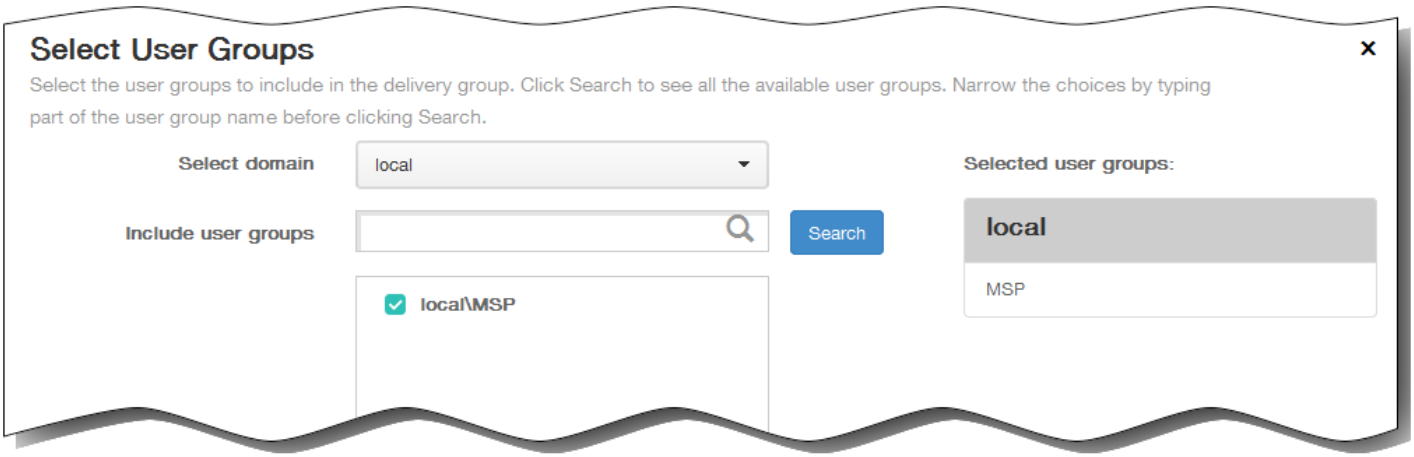
    b. **Inclure des groupes d'utilisateurs** : effectuez l'une des opérations suivantes :

        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.

    c. 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour supprimer un groupe d'utilisateurs de la liste **Groupes d'utilisateurs sélectionnés**, effectuez l'une des opérations suivantes :

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.

Les groupes d'utilisateurs figurant dans la liste **Groupes d'utilisateurs sélectionnés** ont des coches en regard de leur nom dans la liste qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.

d. **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.

e. **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. Développez **Règles de déploiement**, puis configurez les paramètres suivants : l'onglet **Base** s'affiche par défaut.



a. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.

(1) Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est **Toutes**.

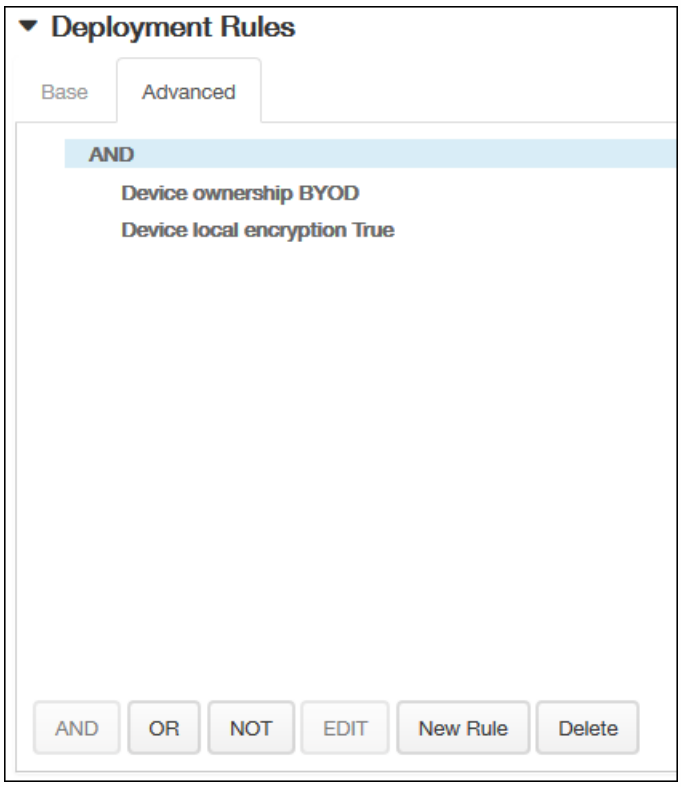
© 1999-2017 Citrix Systems, Inc. All rights reserved.

(2) Cliquez sur **Nouvelle règle** pour définir les conditions.

(3) Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**, comme illustré dans la figure qui précède.

(4) Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

b. Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes.



Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.

c. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.

(1) Cliquez sur **ET**, **OU** ou **SAUF**.

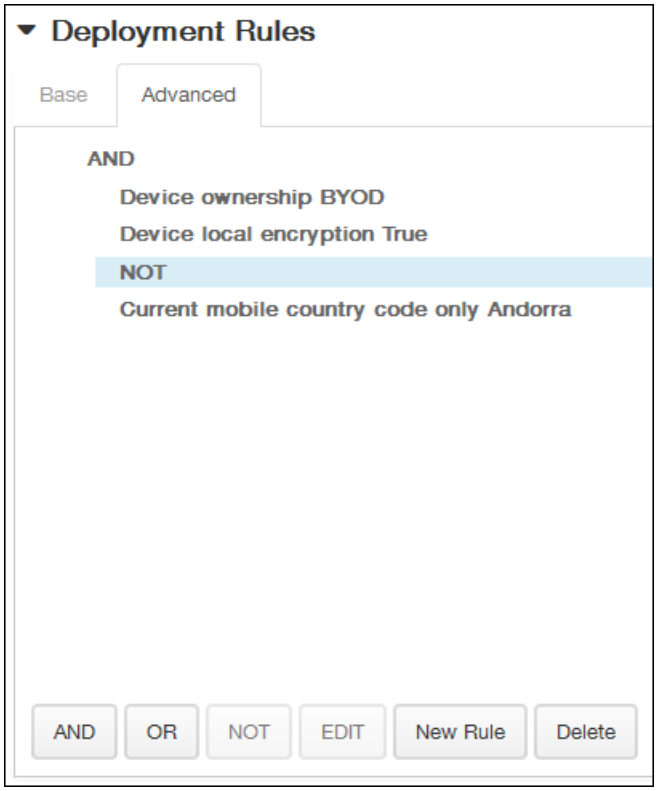
(2) Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.

Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.

(3) Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions.

Dans cet exemple, le propriétaire doit être **BYOD**, le chiffrement sur l'appareil local doit être **Vrai** et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement **Andorre**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

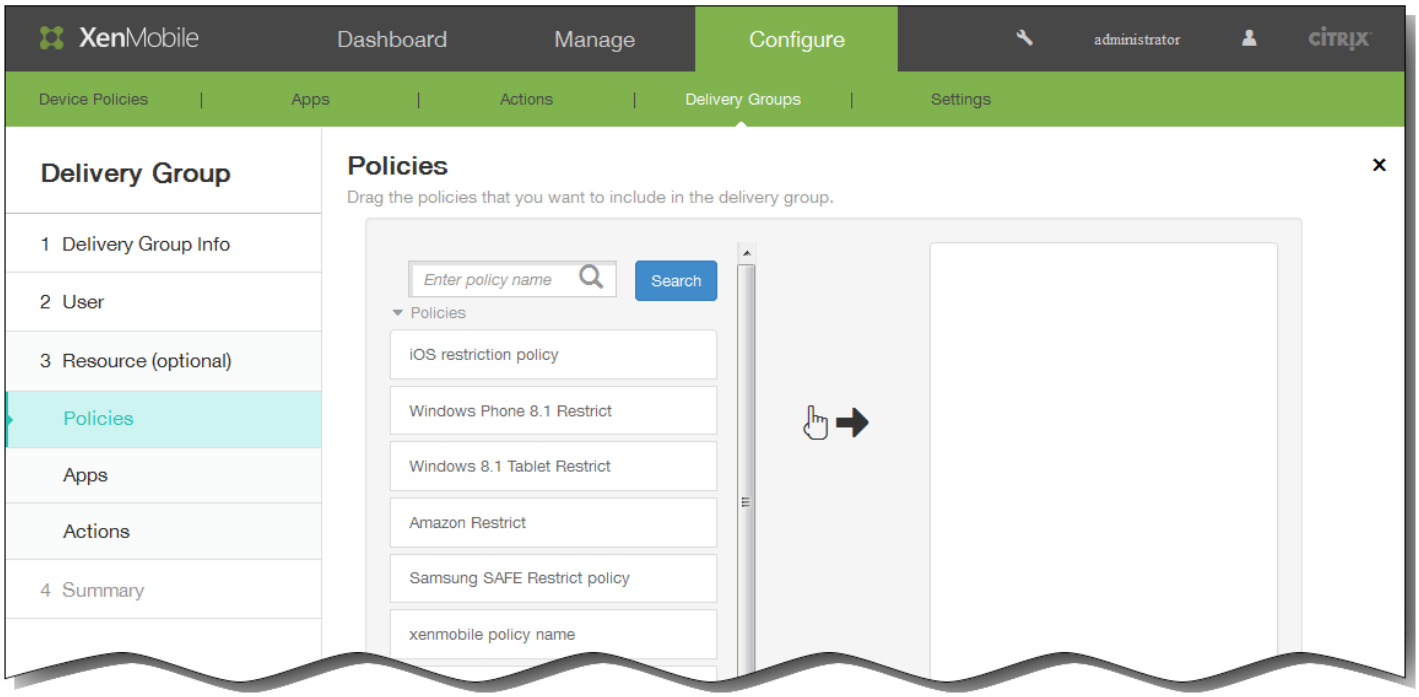


7. Cliquez sur **Suivant**. La page **Ressources du groupe de mise à disposition** s'affiche. Vous pouvez éventuellement ajouter des stratégies, des applications ou des actions pour le groupe de mise à disposition. Pour ignorer cette étape, sous **Groupe de mise à disposition**, cliquez sur **Résumé** pour afficher un résumé de la configuration du groupe de mise à disposition ; sinon, procédez comme suit :

Remarque : pour ignorer une ressource, sous **Ressources (facultatif)**, cliquez sur la ressource que vous souhaitez ajouter et suivez les étapes pour cette ressource.

Pour ajouter des stratégies

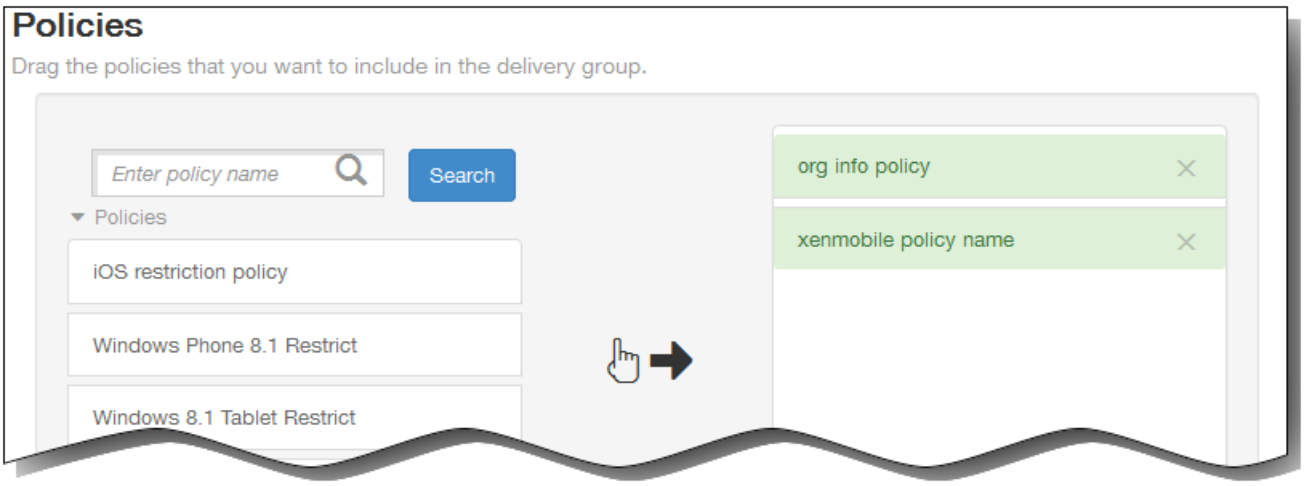
© 1999-2017 Citrix Systems, Inc. All rights reserved.



a. Parcourez la liste des stratégies disponibles pour trouver la stratégie que vous souhaitez ajouter, ou pour limiter la liste des stratégies, tapez un nom de stratégie complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.

b. Cliquez sur une stratégie et faites-la glisser dans la zone de droite.

c. Répétez les étapes a et b pour ajouter d'autres stratégies.

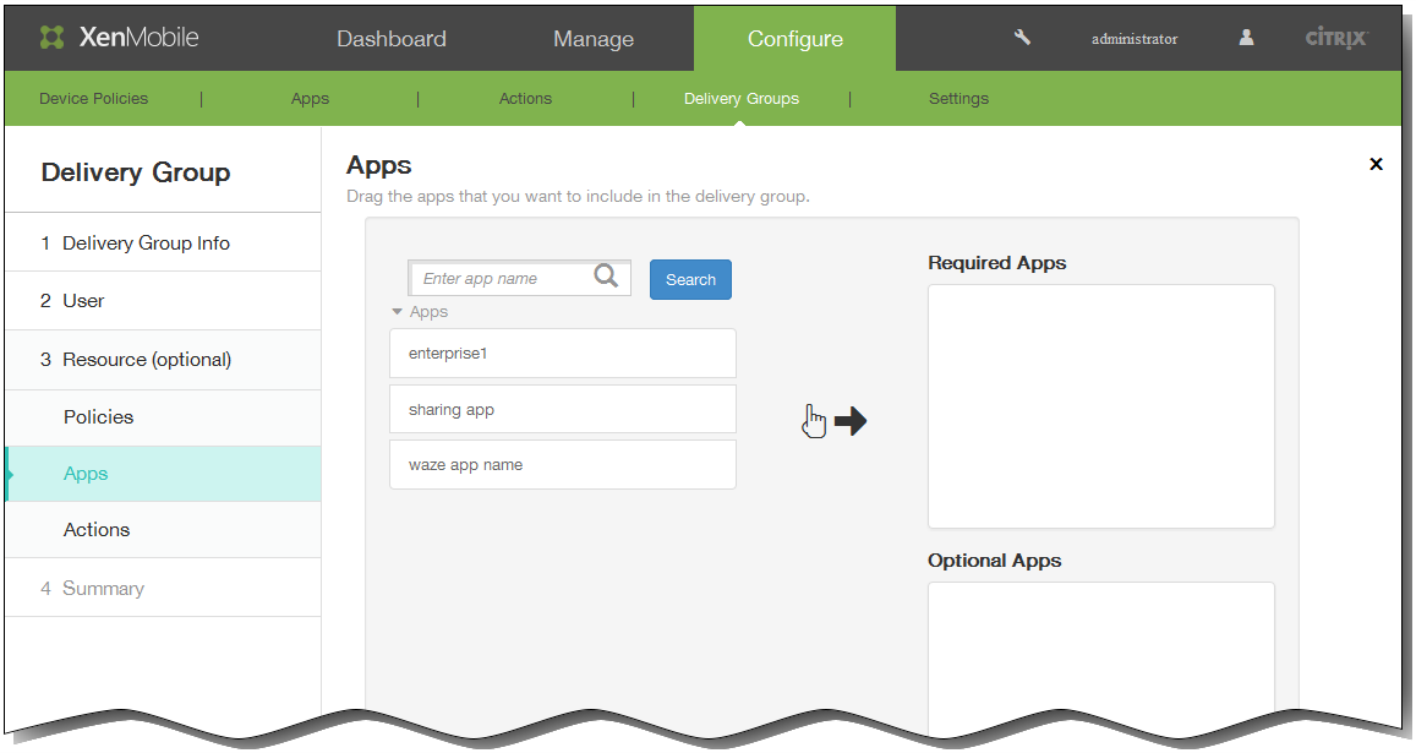


d. Pour supprimer une ressource de stratégie, cliquez sur le **X** en regard du nom de la stratégie.

e. Cliquez sur **Suivant** pour passer à la page de ressource **Applications**. Si vous n'ajoutez plus de ressources, sous **Groupe de mise à disposition**, cliquez sur **Résumé**. La page de **ressources Applications** ou la page **Résumé** s'affiche.

Pour ajouter des applications

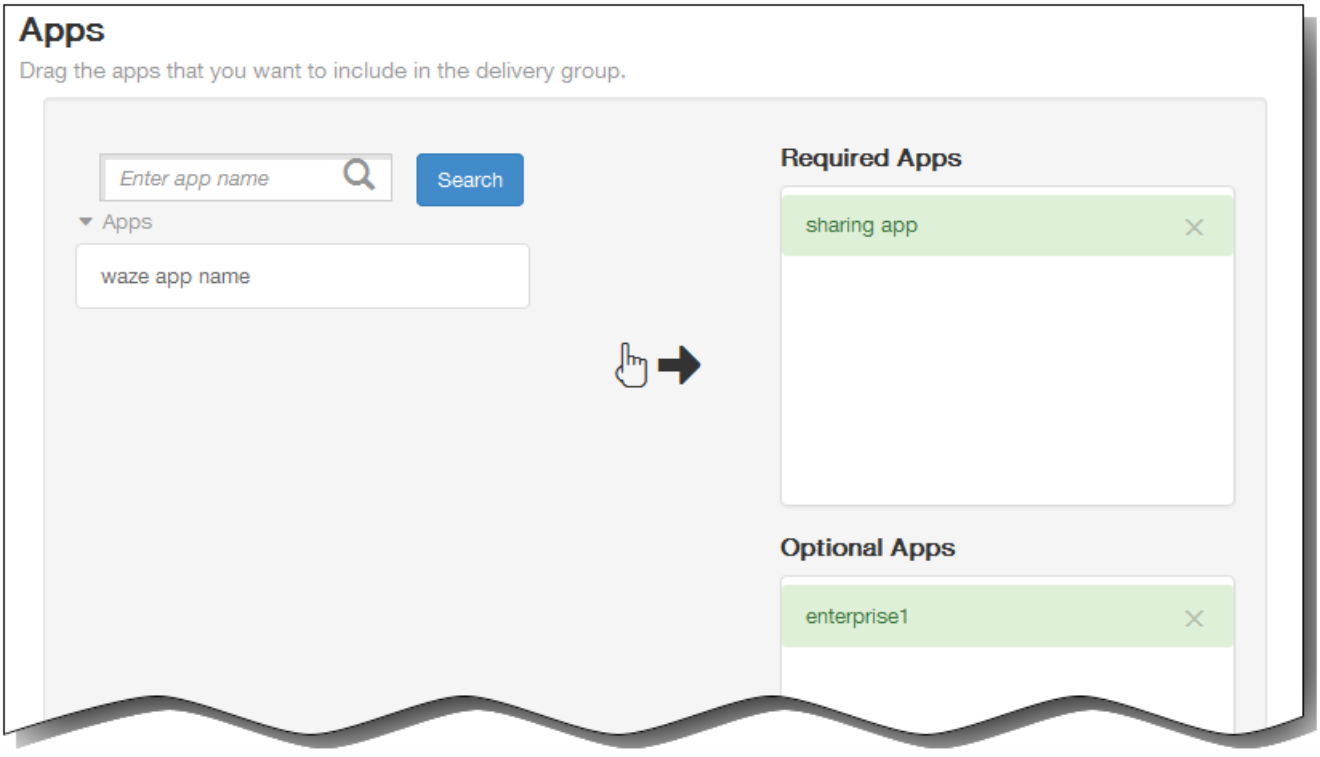
© 1999-2017 Citrix Systems, Inc. All rights reserved.



a. Parcourez la liste des applications disponibles pour trouver l'application que vous souhaitez ajouter, ou pour limiter la liste des applications, tapez un nom d'application complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.

b. Cliquez sur une application et faites-la glisser dans la zone **Applications requises** ou **Applications facultatives**.

c. Répétez les étapes a et b pour ajouter plus d'applications.

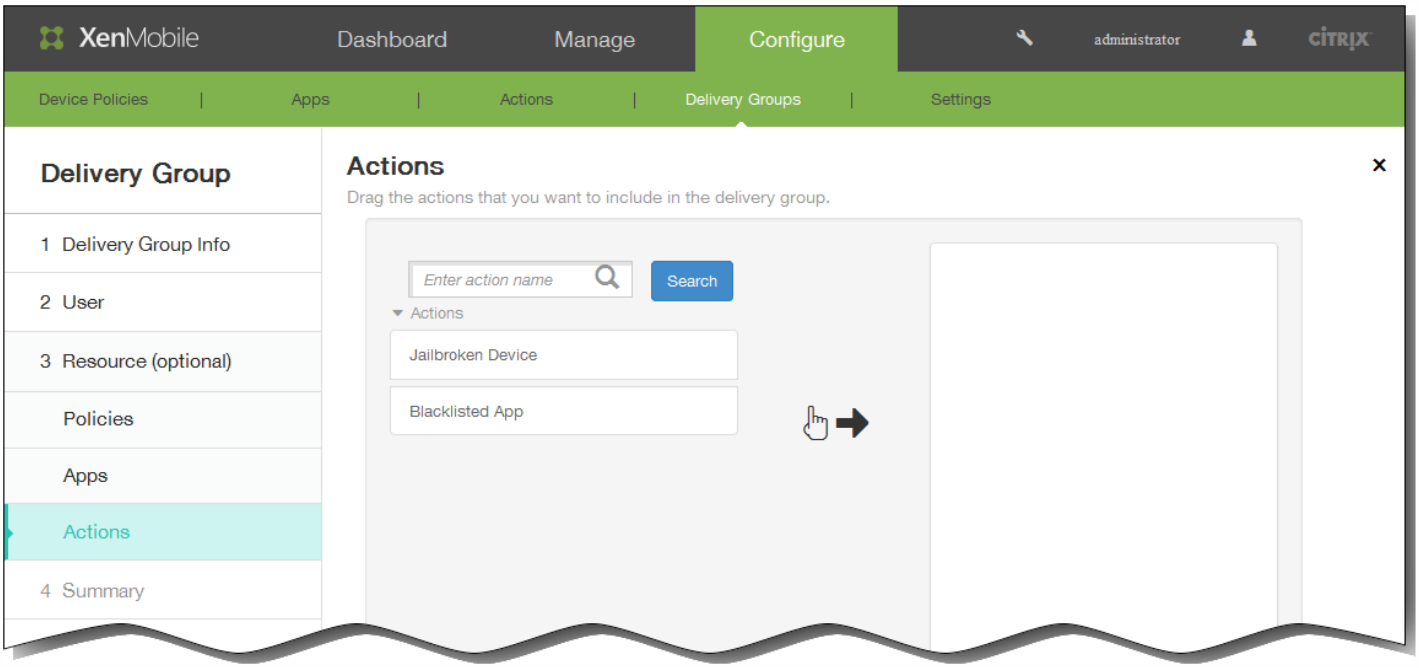


© 1999-2017 Citrix Systems, Inc. All rights reserved.

d. Pour supprimer une ressource d'application, cliquez sur le **X** en regard du nom de l'application.

e. Cliquez sur **Suivant** pour passer à la page de ressource **Actions**. Si vous n'ajoutez plus de ressources, sous **Groupe de mise à disposition**, cliquez sur **Résumé**. La page de **ressources Actions** ou la page **Résumé** s'affiche.

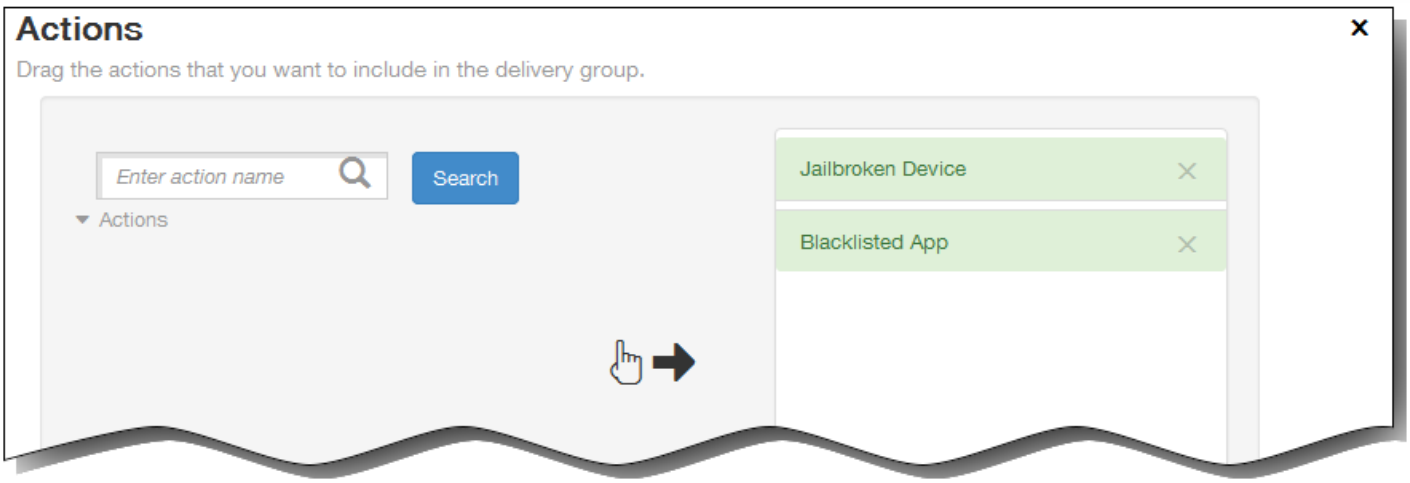
Pour ajouter des actions



a. Parcourez la liste des actions disponibles pour trouver l'action que vous souhaitez ajouter, ou pour limiter la liste des actions, tapez un nom d'action complet ou partiel dans la zone de recherche et cliquez sur **Rechercher**.

b. Cliquez sur une action et faites-la glisser dans la zone de droite.

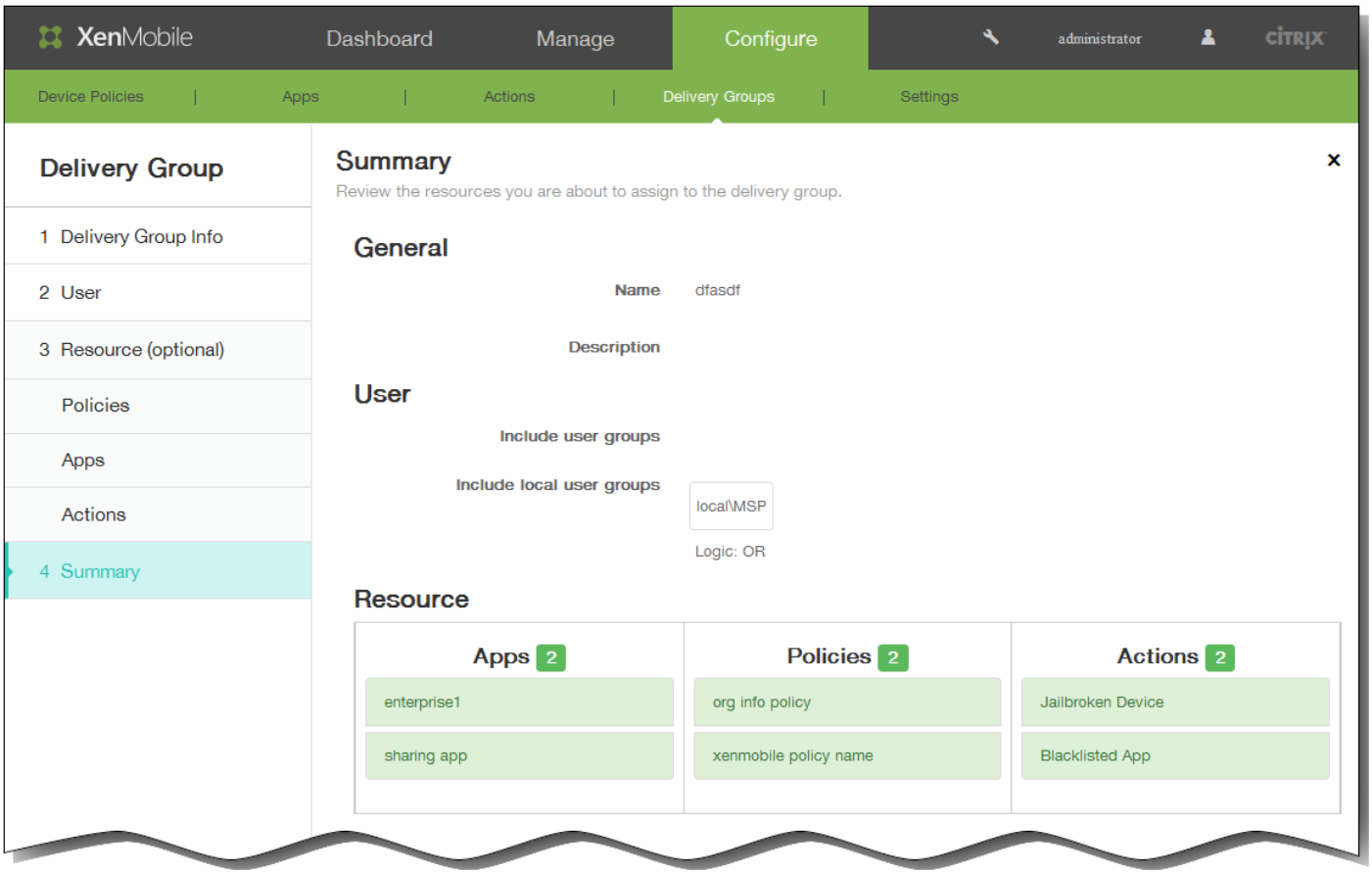
c. Répétez les étapes a et b pour ajouter plus d'actions.



d. Pour supprimer une ressource d'action, cliquez sur le **X** en regard du nom de l'action.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

e. Cliquez sur **Suivant**. La page **Résumé** s'affiche.



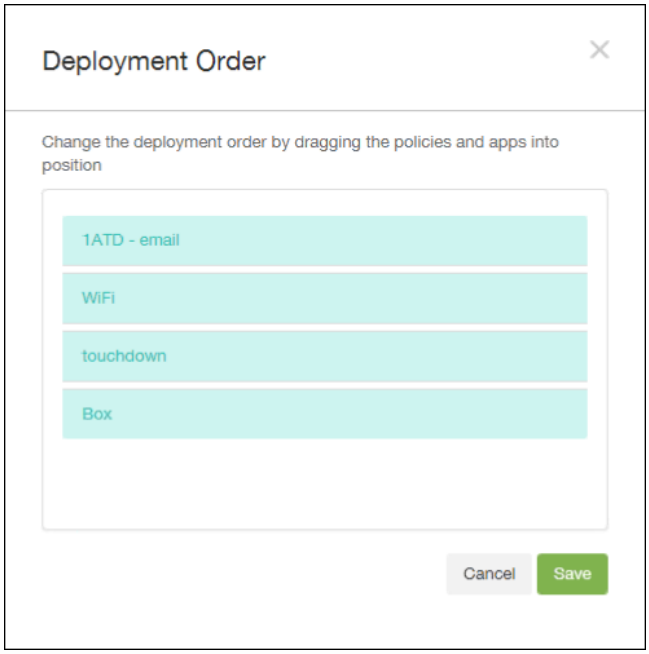
8. Sur la page **Résumé**, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources. Cliquez sur **Précédent** pour revenir sur les pages précédentes pour modifier la configuration le cas échéant. Cliquez sur **Ordre 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.

9. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

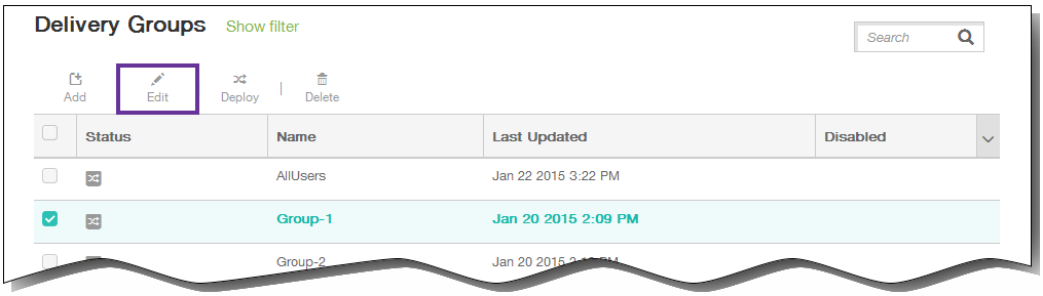


2. Cliquez sur une ressource et faites-la glisser vers l'emplacement à partir duquel vous voulez la déployer. Lorsque vous modifiez l'ordre de déploiement, XenMobile déploie les ressources dans la liste de haut en bas.

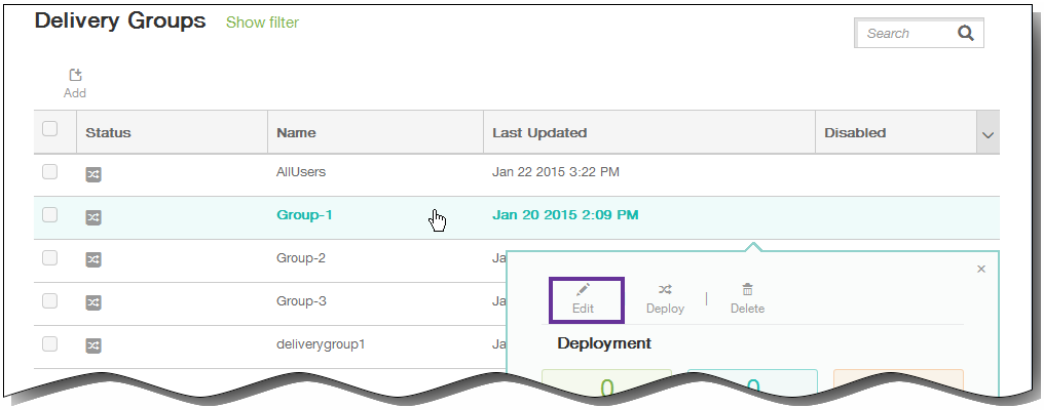
3. Cliquez sur **Enregistrer** pour enregistrer l'ordre de déploiement.

Pour modifier un groupe de mise à disposition

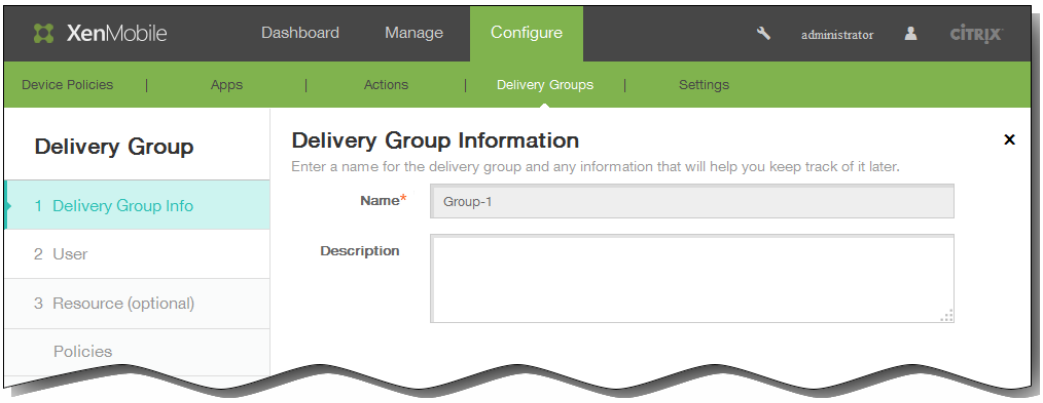
1. Sur la page Groupes de mise à disposition, sélectionnez le groupe de mise à disposition que vous souhaitez modifier en sélectionnant la case en regard de son nom ou en cliquant sur la ligne contenant son nom.
2. Cliquez sur Modifier.
   Remarque : en fonction de la manière dont vous avez sélectionné le groupe de mise à disposition, la commande Modifier apparaît au-dessus ou à droite du groupe de mise à disposition.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

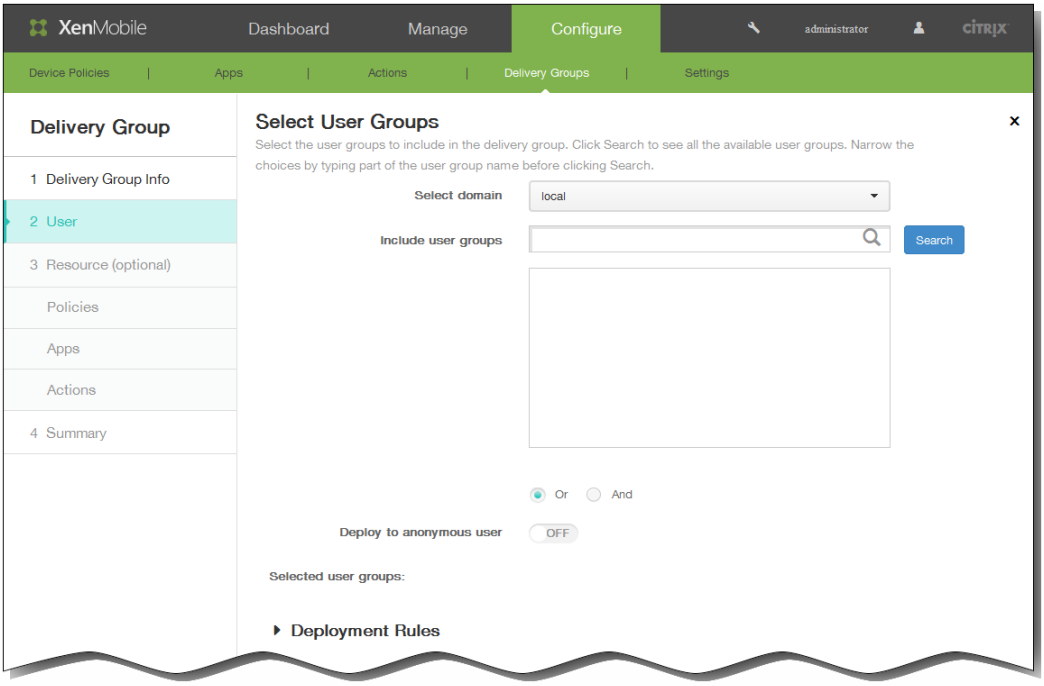


La page de modification des Informations sur le groupe de mise à disposition s'affiche.

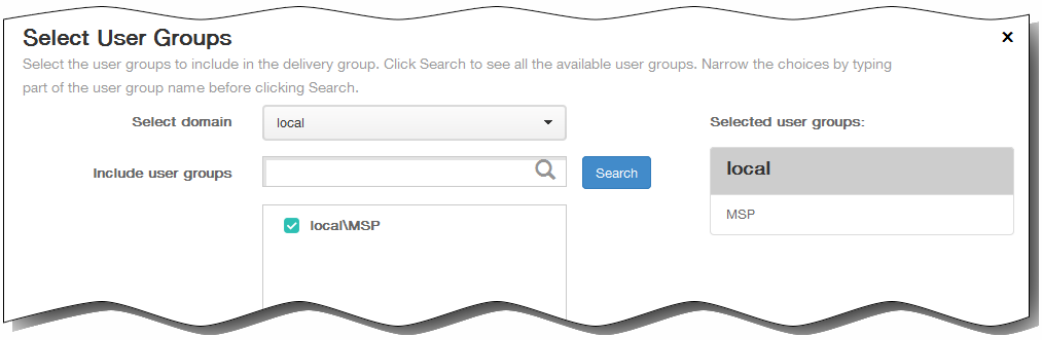


3. Ajoutez ou modifiez la description.
   Remarque : vous ne pouvez pas modifier le nom d'un groupe existant.
4. Cliquez sur Suivant. La page Sélectionner des groupes d'utilisateurs s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Dans le panneau Sélectionner des groupes d'utilisateurs, entrez ou modifiez les informations suivantes :
   1. Sélectionner un domaine : sélectionnez le domaine à partir duquel choisir les utilisateurs dans la liste.
   2. Inclure des groupes d'utilisateurs : effectuez l'une des opérations suivantes :
      - 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.
   3. 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.



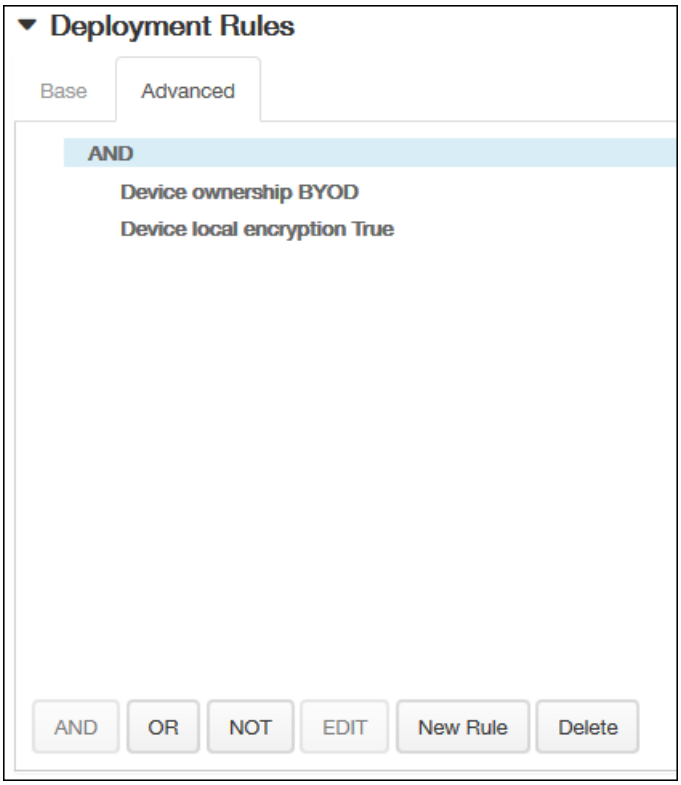
   Remarque : pour supprimer des groupes d'utilisateurs, cliquez sur Rechercher, puis dans la liste des groupes d'utilisateurs, décochez la case à cocher en regard du groupe ou des groupes que vous souhaitez supprimer. Vous pouvez taper un nom de groupe complet ou partiel dans la zone de recherche, puis cliquez sur Rechercher pour limiter le nombre de groupes d'utilisateurs affichés dans la liste.
   4. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. 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. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

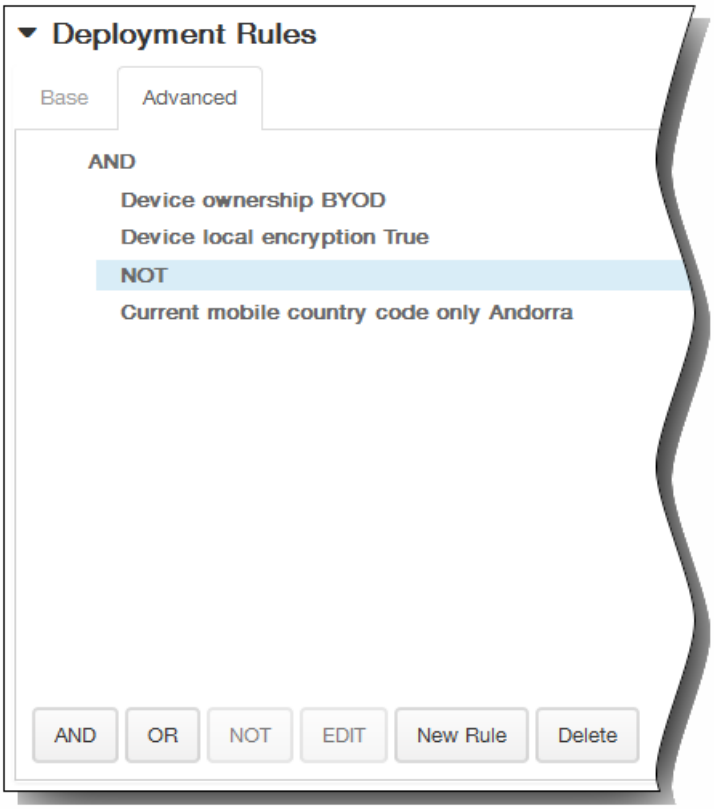


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

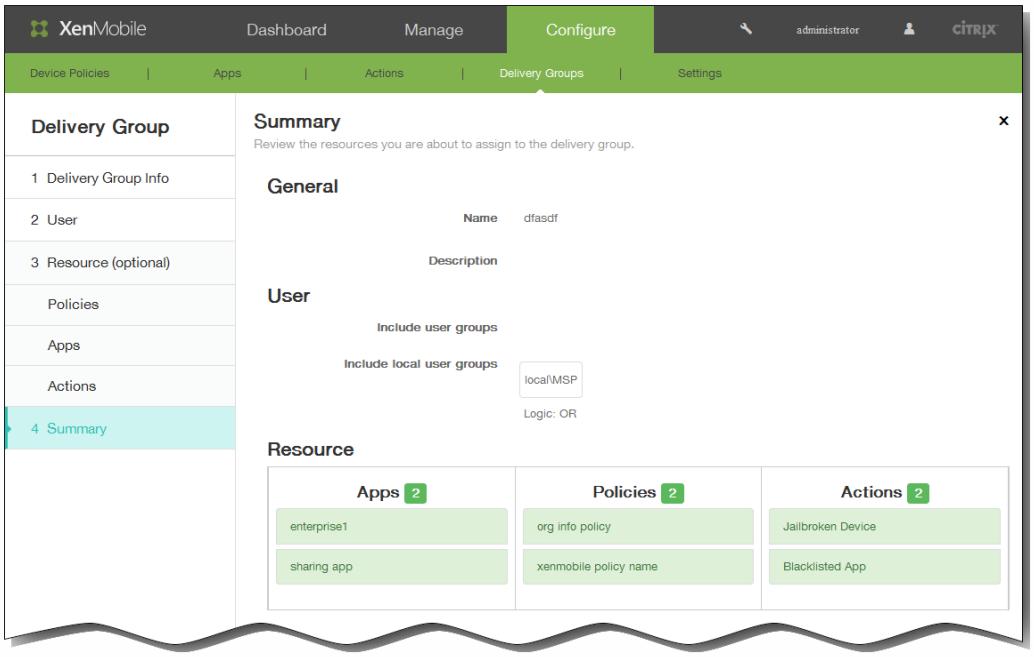
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



7. 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.
   Lorsque vous avez terminé de modifier une ressource, cliquez sur Suivant ou sous Groupe de mise à disposition, cliquez sur Résumé.

   La page de ressource suivante s'affiche ou la page Résumé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

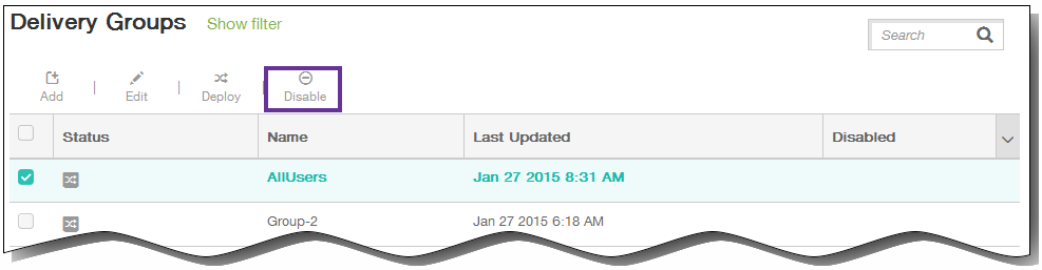


8. Sur la page Résumé, vous pouvez vérifier les options que vous avez configurées pour le groupe de mise à disposition et modifier l'ordre de déploiement des ressources. Cliquez sur Précédent pour revenir sur les pages précédentes pour modifier la configuration le cas échéant. Cliquez sur Ordre de déploiement 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.
9. Cliquez sur Enregistrer pour enregistrer vos modifications.

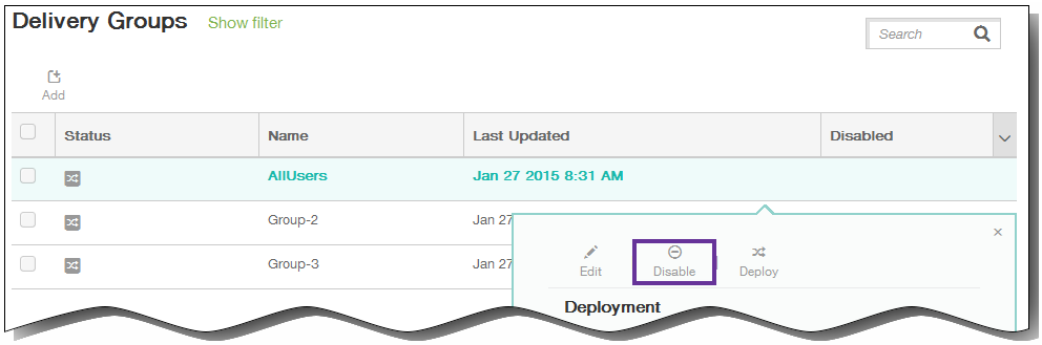
Pour activer et désactiver le groupe de mise à disposition AllUsers

Remarque : AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver.

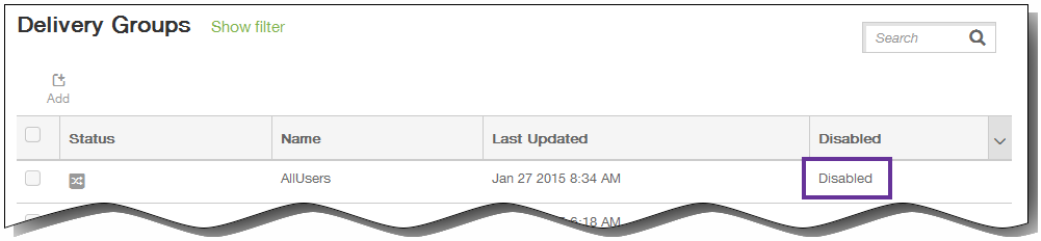
1. Dans la page Groupes de mise à disposition, sélectionnez le groupe de mise à disposition AllUsers en sélectionnant la case à cocher en regard de AllUsers ou en cliquant sur la ligne contenant AllUsers. Procédez ensuite comme suit :
   Remarque : en fonction de la manière dont vous avez sélectionné AllUsers, la commande Activer ou Désactiver apparaît au-dessus ou à droite du groupe de mise à disposition AllUsers.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 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.

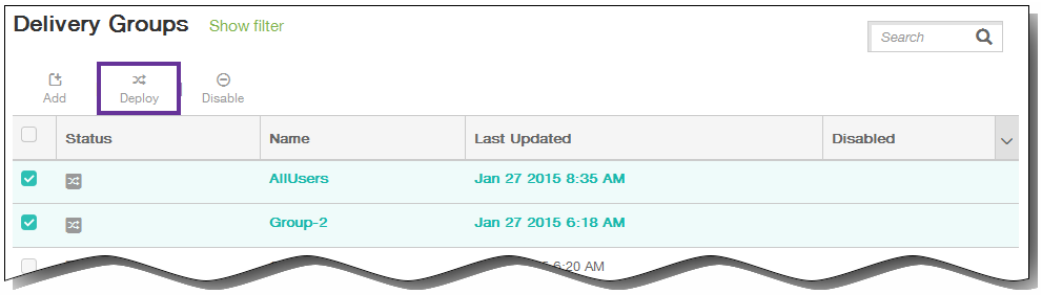
Pour déployer des groupes de mise à disposition

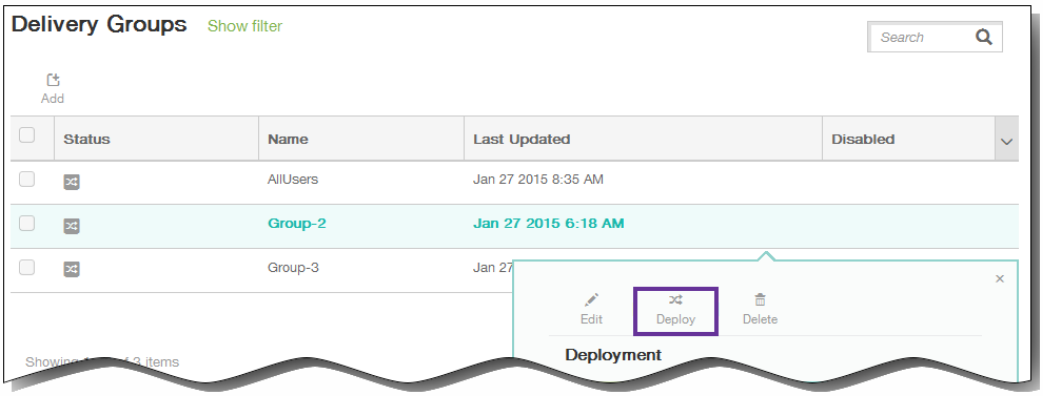
Le déploiement sur un groupe de mise à disposition implique l'envoi d'une notification de type push à tous les utilisateurs équipés d'appareils iOS, Windows Phone 8.1 et Windows 8.1 Tablet qui appartiennent au groupe de mise à disposition les invitant à se reconnecter à XenMobile, ce qui permet de réévaluer 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.

Remarque : pour mettre à jour les applications affichées dans la liste des applications disponibles dans le Worx 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.

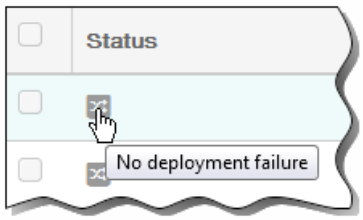
© 1999-2017 Citrix Systems, Inc. All rights reserved.





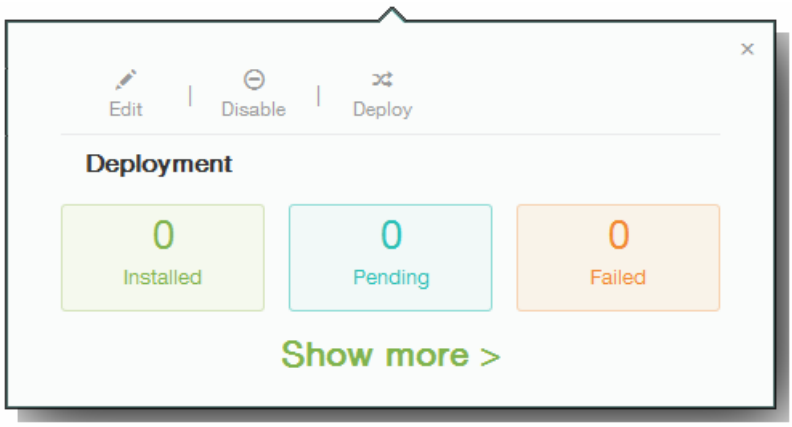
La boîte de dialogue Déployer des appareils apparaît.

3. 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.

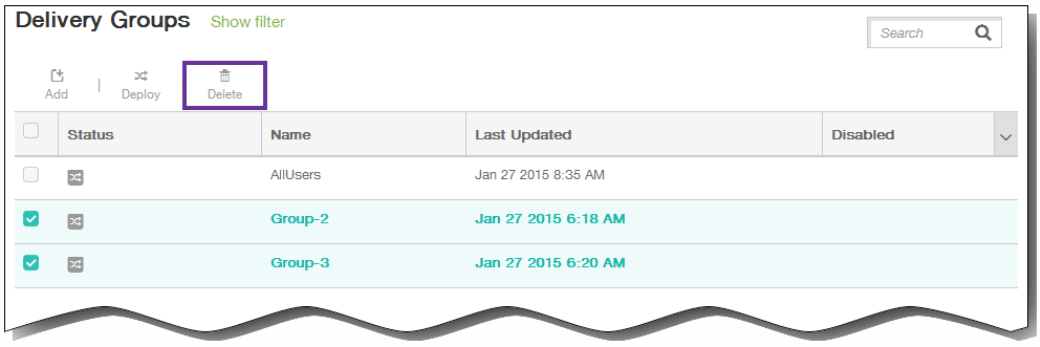
© 1999-2017 Citrix Systems, Inc. All rights reserved.

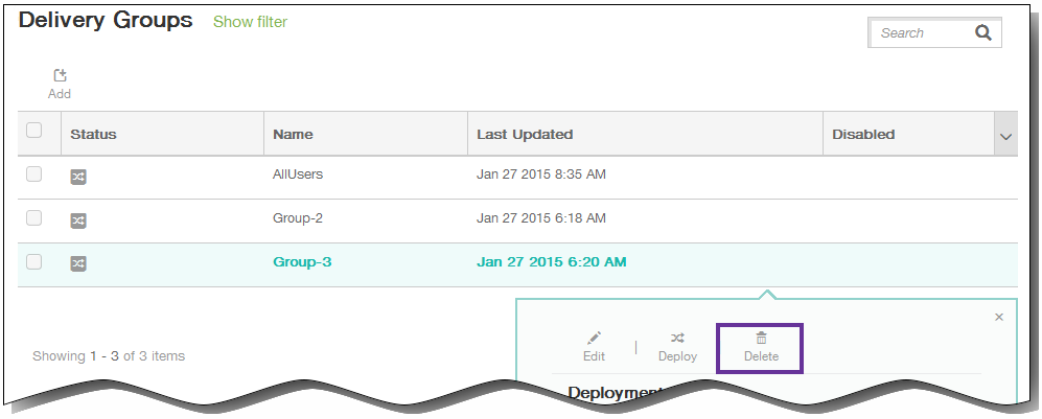


Pour supprimer des groupes de mise à disposition

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.
   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.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

La boîte de dialogue Supprimer s'affiche.

3. Cliquez sur Supprimer dans la boîte de dialogue Supprimer.
   Important : vous ne pouvez pas annuler cette opération.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Inscription d'utilisateurs et d'appareils

Jul 25, 2016

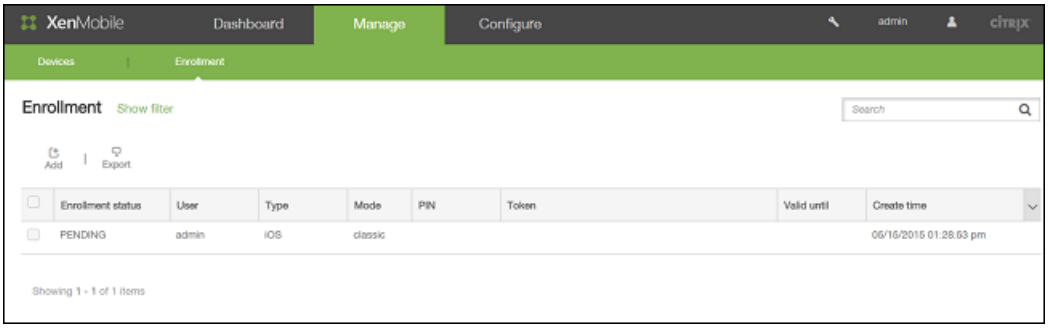
Pour gérer les appareils utilisateur à distance et de manière sécurisée, ces derniers doivent être inscrits dans XenMobile. Le logiciel client XenMobile est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée, suivi de XenMobile et du profil de l'utilisateur. Une fois que les appareils sont inscrits dans la console XenMobile, vous pouvez effectuer des tâches de gestion sur l'appareil, telles que l'application de stratégies, le déploiement d'applications, l'envoi de données sur l'appareil, le verrouillage, l'effacement, et la localisation des appareils perdus ou volés.

Pour inscrire des utilisateurs, vous devez d'abord ajouter des utilisateurs à XenMobile si vous n'avez pas encore établi une connexion à Active Directory. Les rubriques de cette section décrivent les autres étapes requises pour l'inscription d'utilisateurs :

- Configurer les modes d'inscription (par défaut, SHP).
- Configurer les serveurs de notification (SMTP et SMS).
- Configurer le modèle de notification d'inscription.
- Envoyer une notification d'inscription.

Remarque : avant de pouvoir inscrire des utilisateurs d'appareils iOS, vous devez demander un certificat APNS. Consultez la section Certificats dans XenMobile pour plus d'informations.

Pour accéder aux options de configuration pour les utilisateurs et appareils dans la console XenMobile, cliquez sur **Configurer > Inscription** :



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Appareils Android

Jul 25, 2016

1. Accédez au magasin Google Play ou Amazon App sur votre Android et téléchargez l'application Citrix Worx Home, puis tapotez sur l'application.
2. Lorsque vous êtes invité à installer l'application, cliquez sur Suivant, puis cliquez sur Installer.
3. Après l'installation de Worx Home, 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 Worx, que vous pouvez utiliser pour vous connecter à Worx Home et à d'autres applications Worx, telles que WorxMail, WorxWeb, ShareFile, et bien plus encore. Vous devez entrer votre code PIN Worx deux fois. Sur l'écran Créer un code PIN Worx, entrez un code PIN contenant une série de six chiffres.
8. Entrez de nouveau le code PIN. Worx Home s'ouvre. Vous pouvez ensuite accéder à Worx 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 de vos utilisateurs après l'inscription, des messages les inviteront à installer les applications. Cliquez sur Installer pour installer les applications.

Pour désinscrire et réinscrire un appareil Android

Mis à jour : 12-02-2015

Avant de réinscrire un appareil, il doit d'abord être désinscrit. Durant la période pendant laquelle l'appareil est désinscrit mais pas encore réinscrit, ce dernier n'est pas géré par XenMobile, bien qu'il apparaisse toujours dans l'inventaire des appareils dans la console XenMobile. Vous ne pouvez pas suivre l'appareil ni vérifier s'il respecte les exigences de conformité lorsqu'il n'est pas géré par XenMobile.

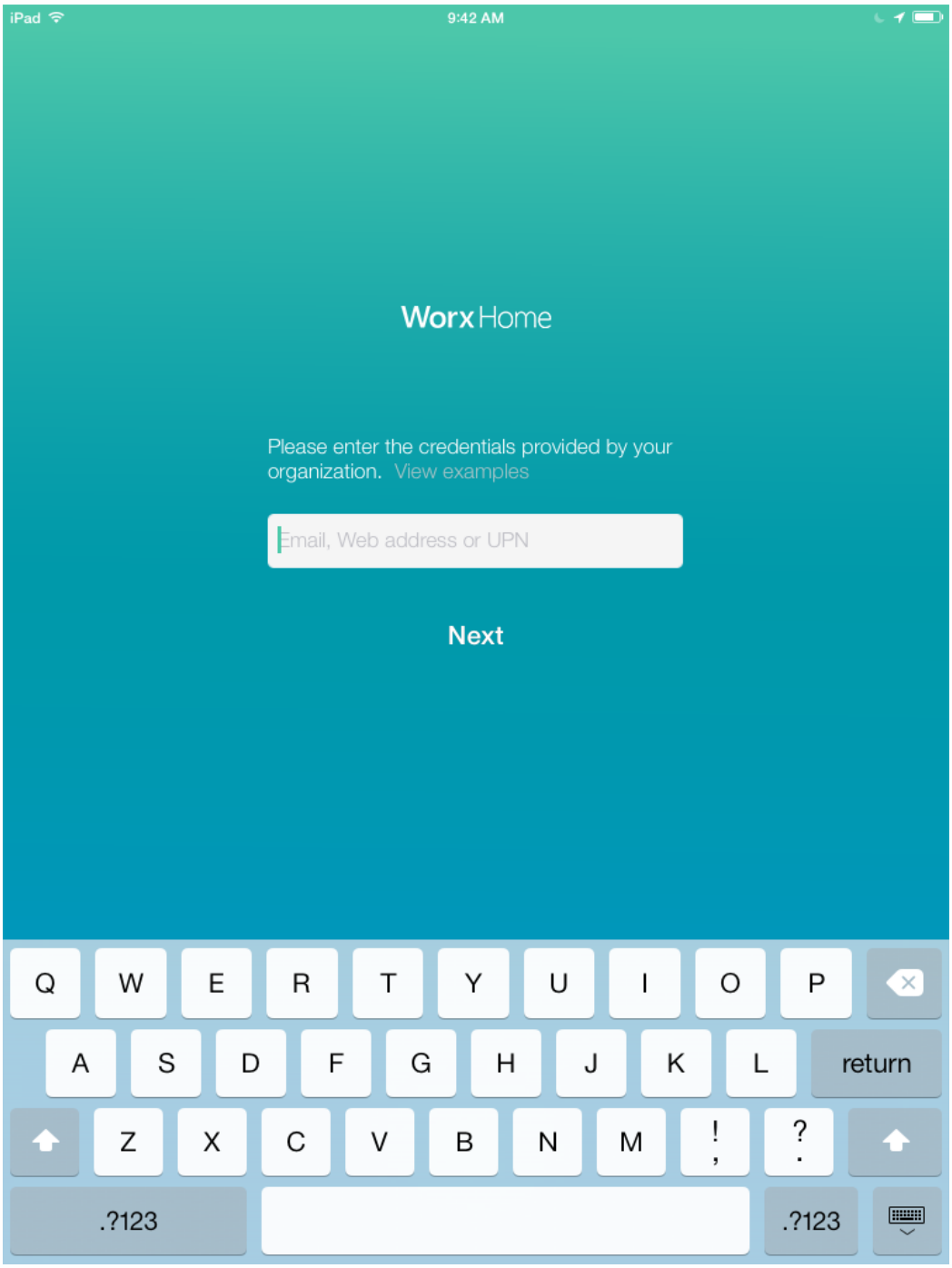
1. Touchez pour ouvrir l'application Worx Home.
2. Touchez l'icône Paramètres en haut à gauche de la fenêtre d'application.
3. Touchez Re-Enroll. Un message s'affiche afin de confirmer que vous souhaitez réinscrire votre appareil.
4. Touchez OK. Cela entraîne la désinscription de l'appareil.
5. Suivez les instructions à l'écran pour réinscrire votre appareil.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Appareils iOS

Jul 25, 2016

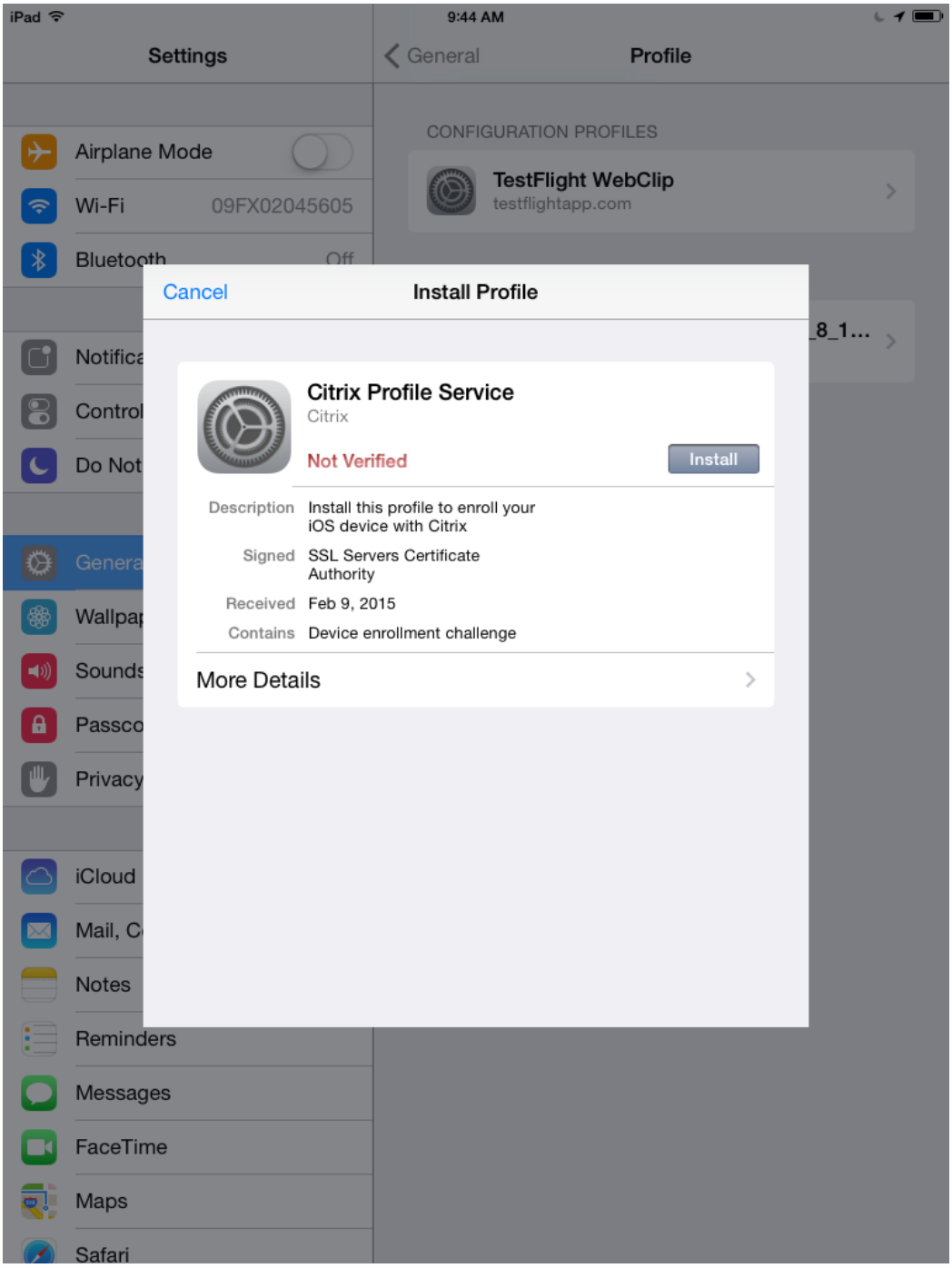
1. Téléchargez l'application Worx Home à partir de l'App Store Apple iTunes sur l'appareil, puis installez l'application sur l'appareil.
2. Sur l'écran d'accueil de l'appareil iOS, tapotez l'application Worx Home.
3. Lorsque l'application Worx Home s'affiche, entrez vos informations d'identification d'entreprise, telles que le nom du serveur XenMobile de votre entreprise, le nom d'utilisateur principal (UPN), ou votre adresse e-mail et cliquez sur Suivant.



4. Entrez votre nom d'utilisateur et votre mot de passe. Un navigateur s'ouvre pour commencer le processus d'inscription.

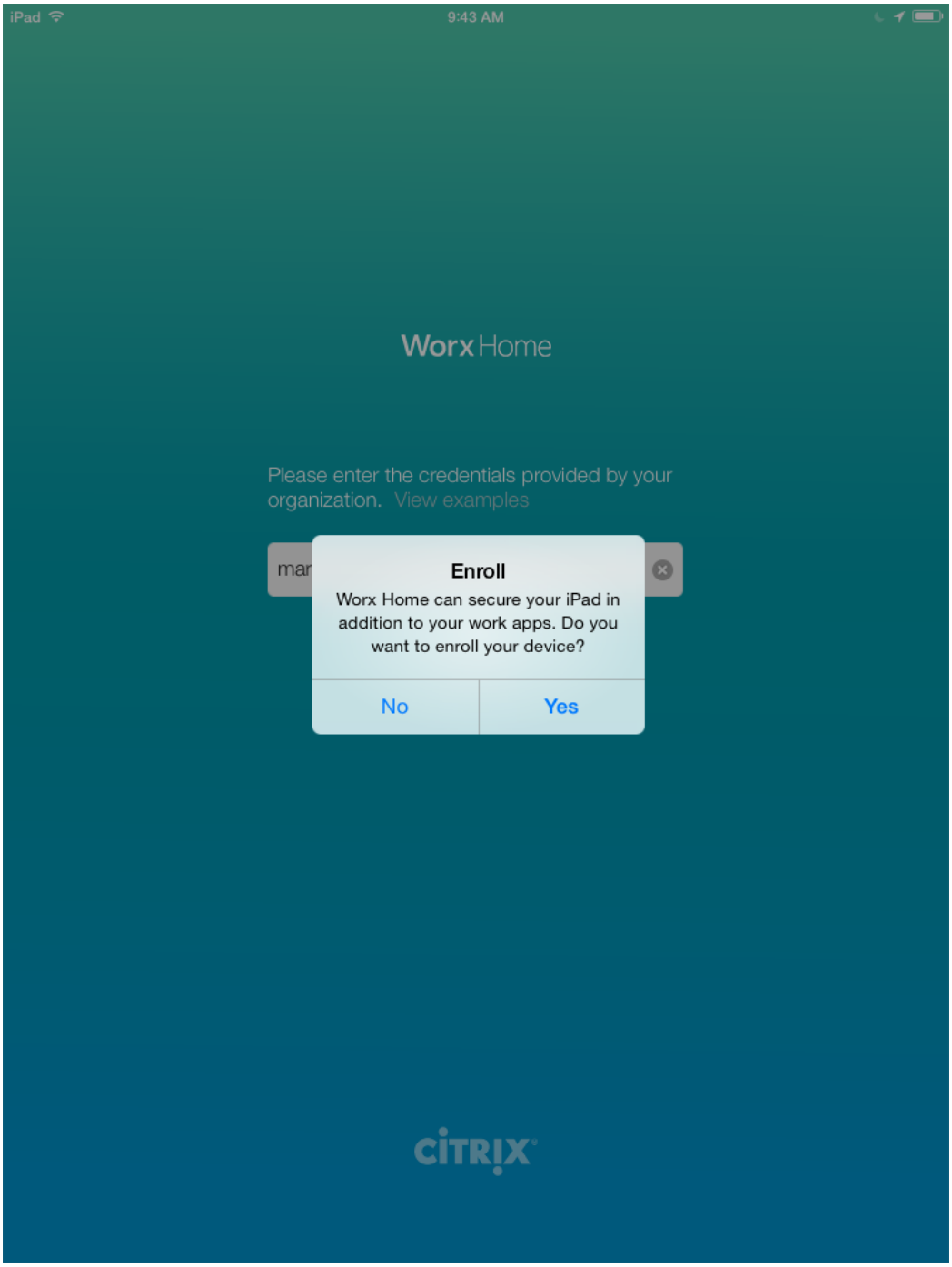
© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Cliquez sur Installer pour installer Citrix Profile Services.



6. Cliquez sur Installer maintenant si vous y êtes invité par un message d'avertissement.
7. Si votre appareil est configuré avec un code secret, vous serez invité à l'entrer pour installer le profil.
8. Touchez Installer.
9. Une fois l'installation du profil terminée, touchez Terminé pour terminer le processus d'installation du profil de la société.
10. Lorsque Worx Home s'affiche, appuyez sur Oui pour permettre à Worx Home d'utiliser votre emplacement actuel.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. En fonction de la manière dont XenMobile est configuré, vous pouvez être invité à créer un code PIN Worx, que vous pouvez utiliser pour vous connecter à Worx Home et à d'autres applications Worx, telles que WorxMail, WorxWeb, ShareFile, et bien plus encore. Vous devez entrer votre code PIN Worx deux fois. Worx Home s'ouvre. Vous pouvez ensuite accéder à Worx Store pour afficher les applications que vous pouvez installer sur votre appareil iOS.
12. Appuyez sur Worx Store pour ouvrir le magasin d'applications d'entreprise.
13. Si vous avez configuré XenMobile pour distribuer automatiquement des applications sur les appareils de vos utilisateurs après l'inscription, des messages les inviteront à installer les applications. Cliquez sur Installer pour installer les applications.

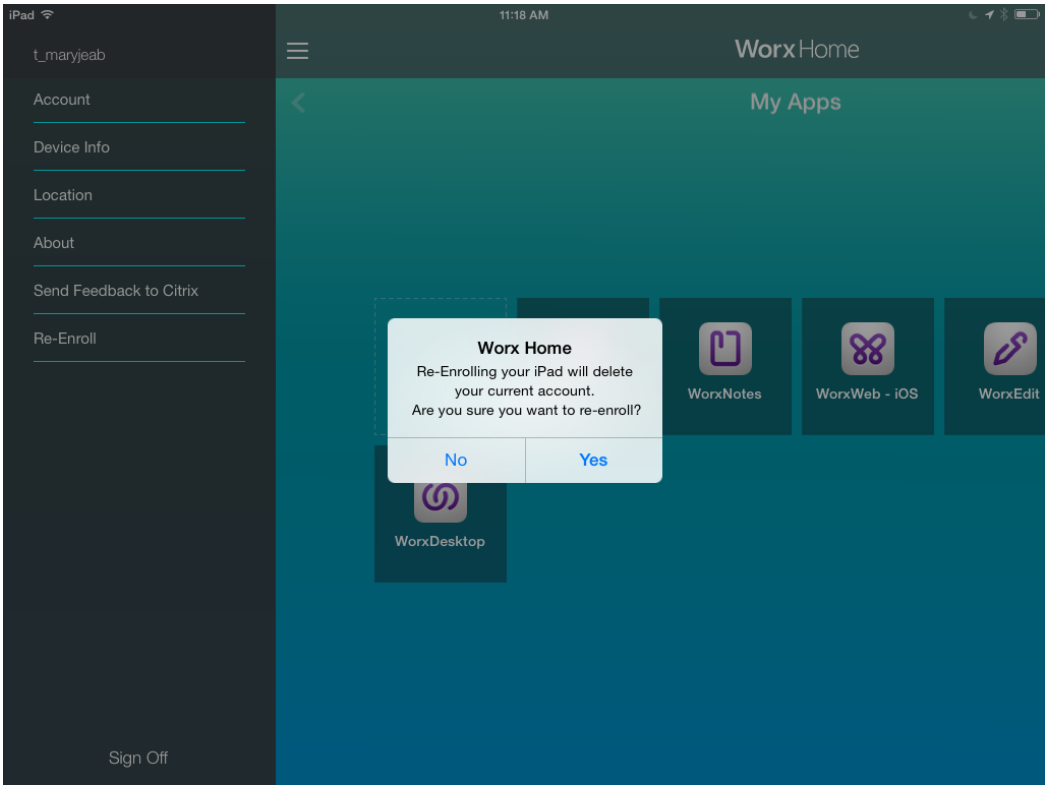
Pour réinscrire un appareil iOS

Mis à jour : 13-02-2015

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Avant de réinscrire un appareil, il doit d'abord être désinscrit. Durant la période pendant laquelle l'appareil est désinscrit mais pas encore réinscrit, ce dernier n'est pas géré par XenMobile, bien qu'il apparaisse toujours dans l'inventaire des appareils dans la console XenMobile. Vous ne pouvez pas effectuer le suivi de l'appareil ni vérifier s'il respecte les exigences de conformité s'il n'est pas géré par XenMobile.

1. Touchez pour ouvrir l'application Worx Home.
2. Touchez l'icône Paramètres en haut à gauche de la fenêtre d'application.
3. Touchez Réinscription. Un message s'affiche afin de confirmer que vous souhaitez réinscrire votre appareil.



4. Touchez Oui. Cela entraîne la désinscription de l'appareil.
5. Suivez les instructions à l'écran pour réinscrire votre appareil.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Appareils Windows

Jul 25, 2016

XenMobile prend en charge l'inscription d'appareils exécutant les systèmes d'exploitation Windows suivants :

- Windows
- Windows Phone

Les utilisateurs Windows et Windows Phone s'inscrivent directement au travers de leurs appareils.

Vous devez configurer la découverte automatique 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 8.1 à l'aide de la découverte automatique

Les utilisateurs peuvent inscrire des appareils exécutant Windows RT 8.1, et les versions 32 bits et 64 bits de Windows 8.1 Professionnel et Windows 8.1 Entreprise. Pour activer la gestion des appareils Windows 8.1, Citrix vous recommande de configurer la découverte automatique. Pour de plus amples informations, consultez la section Pour activer la découverte 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 touchez Paramètres du PC > Réseau > Lieu de travail.
3. Entrez votre adresse de messagerie d'entreprise, puis touchez Activer. 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. 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. 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 inscrire les appareils Windows 8.1 sans découverte automatique

Il est possible d'inscrire des appareils Windows 8.1 sans découverte automatique. Cependant, Citrix vous recommande de configurer la découverte automatique. Étant donné que l'inscription sans découverte 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 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 touchez Paramètres du PC > Réseau > Lieu de travail.
3. Entrez votre adresse de messagerie d'entreprise.
4. Si l'option Détecter automatiquement l'adresse du serveur est activée, tapotez pour la désactiver.
5. Dans le champ Entrer l'adresse du serveur, tapez l'adresse du serveur au format suivant : https://*serverfqdn:8443/serverInstance*/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.
6. Entrez votre mot de passe.
7. 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 inscrire des appareils Windows Phone 8.1

Pour inscrire des appareils Windows Phone 8.1 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 découverte 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'applications 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 Citrix Worx Home Windows Phone 8 signée).

1. Sur l'écran principal de Windows 8.1 Phone, tapotez l'icône Paramètres.
2. Tapotez Lieu de travail.
3. Sur l'écran Lieu de travail, tapotez Ajouter un compte.
4. Dans l'écran suivant, entrez une adresse de messagerie et un mot de passe et touchez s'inscrire. Si la découverte automatique est configurée pour votre domaine, les informations requises dans les étapes suivantes sont automatiquement renseignées. Passez à l'étape 8. Si la découverte 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.
5. 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.
6. 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 s'inscrire.
7. 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, touchez Annuler.
8. 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 tapotez sur Terminé. Si vous désactivez cette option, vous devrez vous réinscrire afin de recevoir le magasin d'applications d'entreprise.
9. Sur l'écran Compte ajouté, touchez terminé.
10. 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, Worx Home s'inscrit en arrière-plan. Aucun

© 1999-2017 Citrix Systems, Inc. All rights reserved.

indicateur n'apparaît lorsque l'installation est terminée. Ouvrez Worx Home à partir de l'écran Toutes les applications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Appareils Symbian

Jul 25, 2016

1. Accédez à l'adresse Web XenMobile pour votre organisation. L'adresse Web est au format suivant : https://.domaine.com//setup
   Remarque : vous pouvez utiliser le préfixe HTTPS uniquement si vous disposez d'un certificat émis par une autorité de confiance, telle que Verisign ou Thawte.
2. Sur l'écran Install, touchez OK.
3. Touchez Phone Memory en tant qu'emplacement où installer l'agent XenMobile.
4. Lorsque l'installation est terminée, touchez Yes pour ouvrir XenMobile.
5. Sur l'écran Security Details, touchez OK pour autoriser XenMobile à accéder au téléphone.
6. Entrez les quatre premiers chiffres du code du serveur comme 2831 puis touchez OK.
7. Sur l'écran Control Request Accepted, touchez OK.
8. Entrez le nom d'utilisateur et le mot de passe, le nom de serveur, le port et le nom de l'instance pour le serveur XenMobile, puis touchez OK. Les informations de connexion s'affichent.
9. Cliquez sur Options pour passer en revue les détails de connexion au serveur, puis touchez Close pour terminer l'installation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Envoi d'une invitation d'inscription dans XenMobile

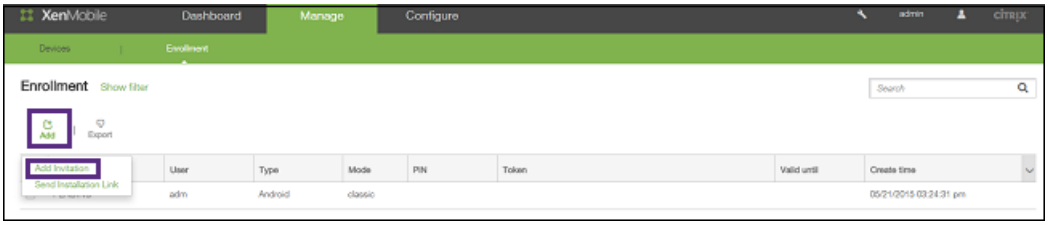
Jul 25, 2016

Dans la console XenMobile, vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS, Android et Windows.

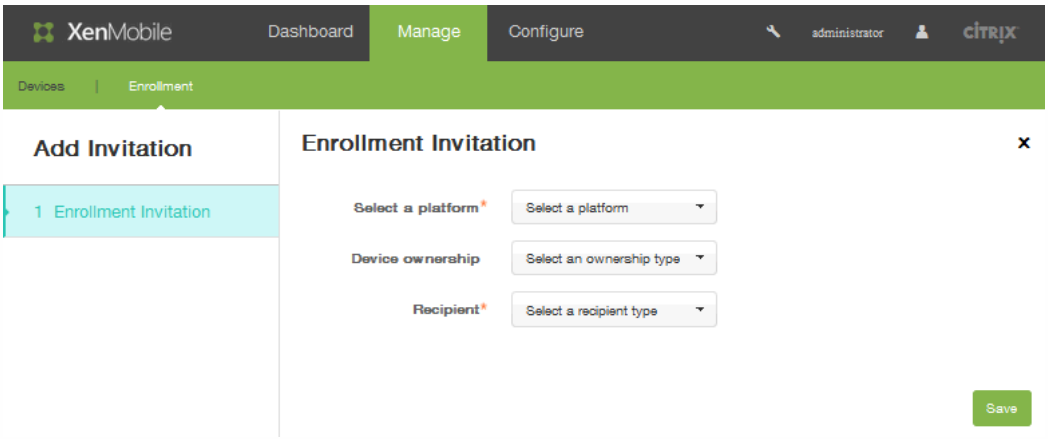
1. Dans la console XenMobile, cliquez sur Gérer > Inscription.



2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu répertoriant les options permettant d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.
3. Cliquez sur Ajouter une invitation.

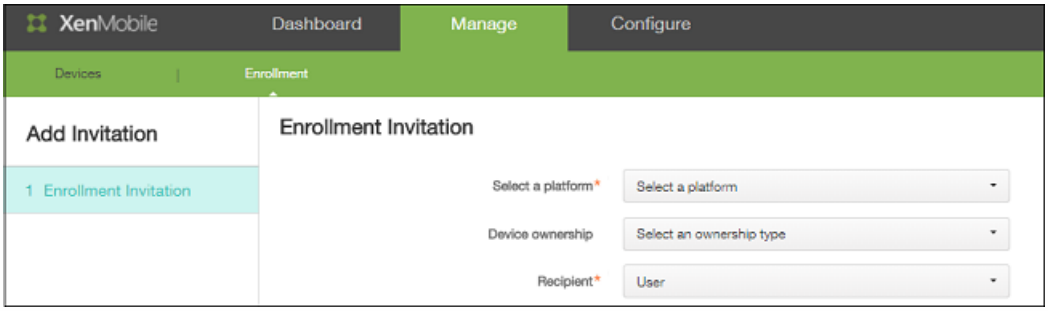


L'écran Invitation d'inscription s'affiche.



4. Dans la liste Sélectionner une plate-forme, cliquez sur iOS ou Android.
5. Dans la liste Propriétaire, cliquez sur Entreprise ou Employé.
6. Dans la liste Destinataire, cliquez sur Utilisateur ou Groupe.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Lorsque vous sélectionnez un utilisateur en tant que destinataire, d'autres options de configuration s'affichent. Suivez les étapes dans ces rubriques pour spécifier les paramètres d'invitation en fonction du type de destinataire sélectionné.

Pour envoyer une invitation d'inscription à un utilisateur

1. Dans la console XenMobile, cliquez sur Gérer > Inscription.

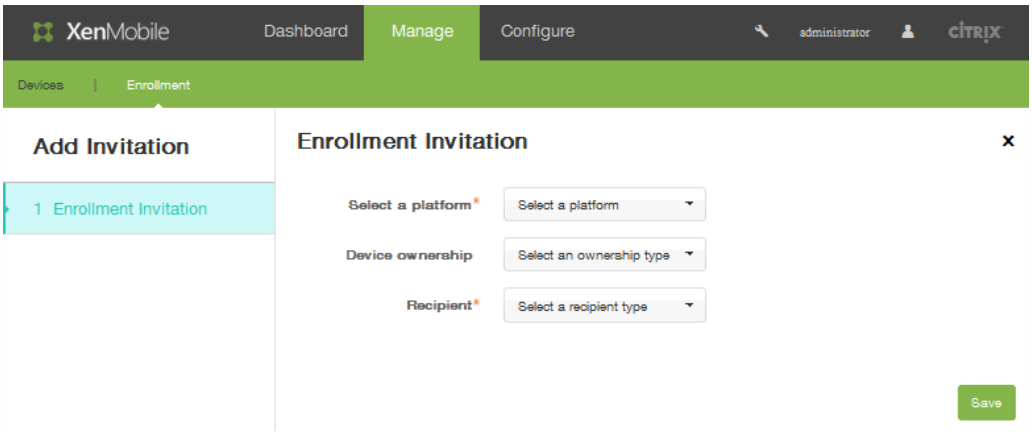


2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.

3. Cliquez sur Ajouter une invitation.

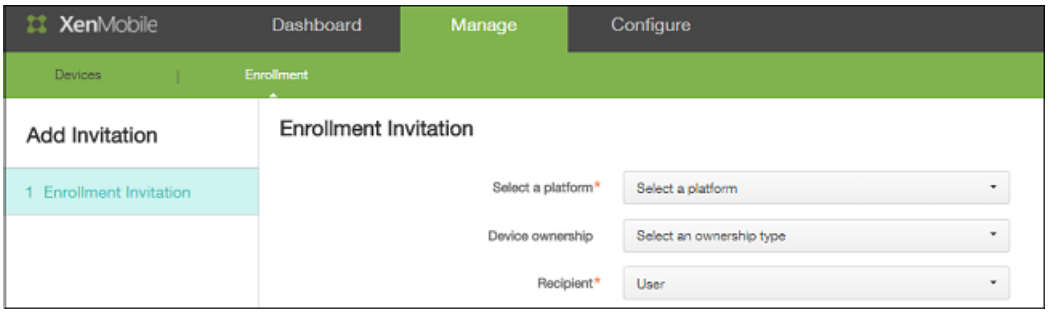


L'écran Invitation d'inscription s'affiche.



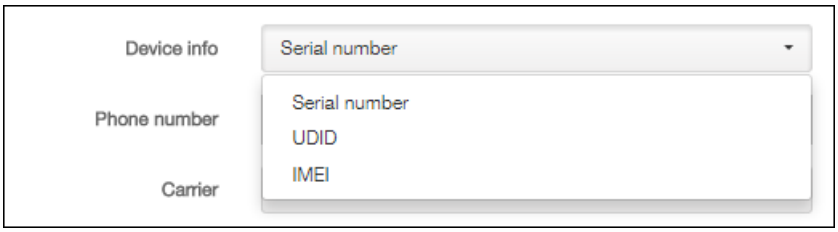
4. Dans la liste Sélectionner une plate-forme, cliquez sur iOS ou Android.
5. Dans la liste Propriétaire, cliquez sur Entreprise ou Employé.
6. Dans la liste Destinataire, cliquez sur Utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



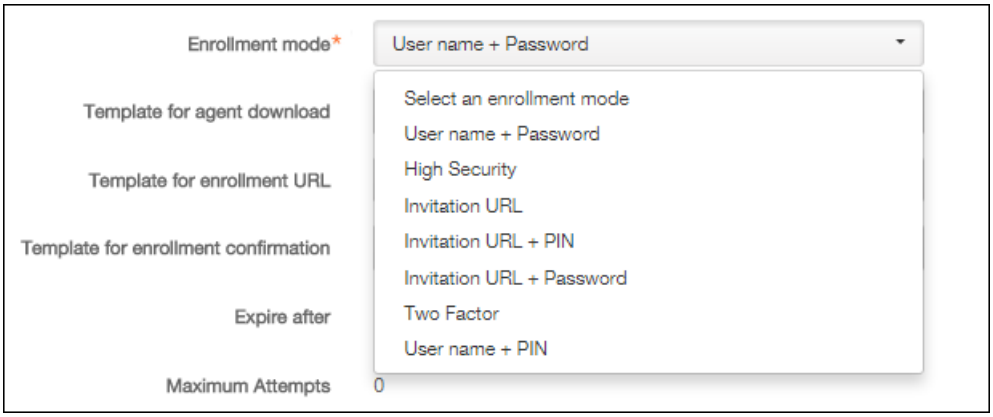
Des options de configuration supplémentaires liées à l'inscription de l'utilisateur s'affichent.

7. Dans Nom d'utilisateur, entrez un nom d'utilisateur.
   Remarque : 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 envoyer des notifications. S'il s'agit d'un utilisateur Active Directory, assurez-vous que LDAP est configuré.
8. Dans la liste Infos appareil, sélectionnez Numéro de série, UDID ou IMEI.

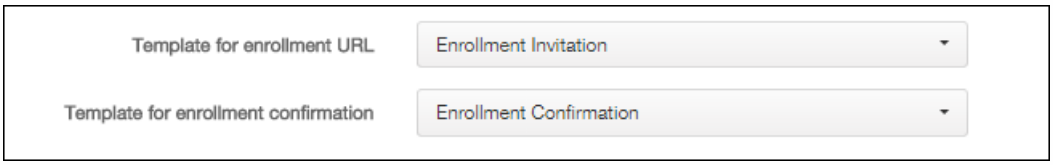


Après avoir choisi une option, un champ s'affiche dans lequel vous pouvez entrer la valeur correspondante à l'appareil.

9. Dans Numéro de téléphone, entrez le numéro de téléphone de l'utilisateur (facultatif).
10. Dans la liste Opérateur, sélectionnez un opérateur auquel associer le numéro de téléphone de l'utilisateur.
11. Dans la liste Mode d'inscription, sélectionnez Nom d'utilisateur + mot de passe (valeur par défaut), Haute sécurité, URL d'invitation, URL d'invitation + PIN, URL d'invitation + mot de passe, Deux facteurs ou Nom d'utilisateur + PIN.



12. Dans la liste Modèle pour téléchargement de l'agent, 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 dans l'étape 1.

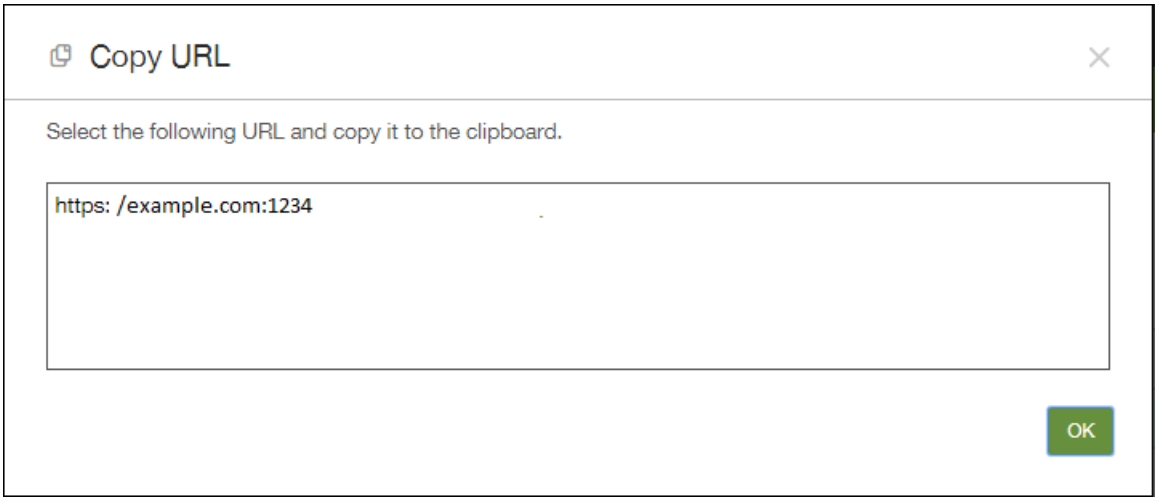


© 1999-2017 Citrix Systems, Inc. All rights reserved.

13. Dans la liste Modèle pour l'URL d'inscription, sélectionnez Invitation d'inscription.
14. Dans la liste Modèle pour la confirmation d'inscription, cliquez sur Confirmation d'inscription. L'invitation d'inscription expire après un certain temps. Le champ Expire après indique quand l'inscription expire. Le champ Nbre max de tentatives indique le nombre maximal de tentatives d'inscription autorisées.
15. Dans Envoyer invitation, effectuez l'une des opérations suivantes :
    - Cliquez sur ON, puis sur Enregistrer et envoyer.
    - Laissez l'option désactivée (OFF), puis cliquez sur Enregistrer.
16. L'invitation que vous avez ajoutée apparaît dans le tableau sur la page Inscription. À partir de cette fenêtre, si vous cliquez pour sélectionner une invitation, plusieurs nouvelles options s'affichent au-dessus du tableau : Notifier, Copier l'URL et Supprimer.



1. Cliquez sur Notifier pour envoyer une invitation en attente.
2. Cliquez sur Copier l'URL pour copier l'URL d'invitation dans le cas où vous souhaitez envoyer l'invitation dans un e-mail. Lorsque la notification s'affiche, sélectionnez l'URL, copiez-la et cliquez sur OK.



3. Cliquez sur Supprimer pour supprimer l'invitation.

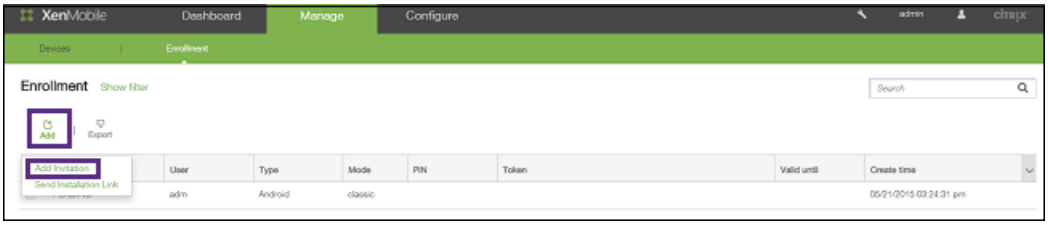
Pour envoyer une invitation d'inscription à un groupe

1. Dans la console XenMobile, cliquez sur Gérer > Inscription.

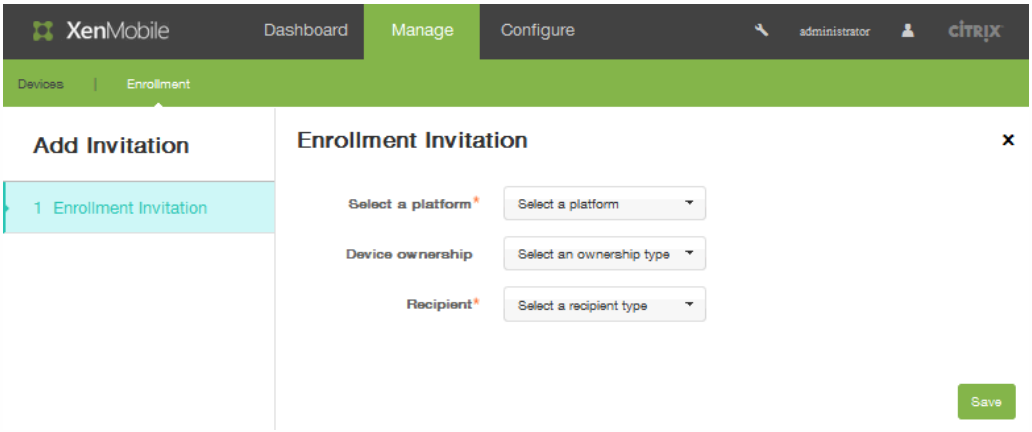


2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.
3. Cliquez sur Ajouter une invitation.

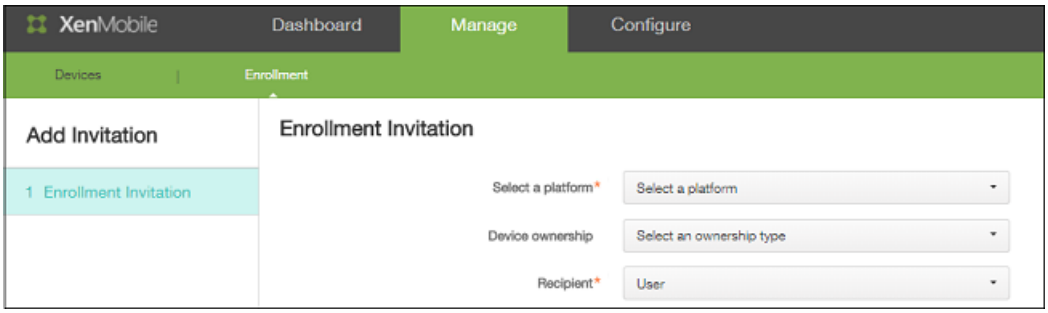
© 1999-2017 Citrix Systems, Inc. All rights reserved.



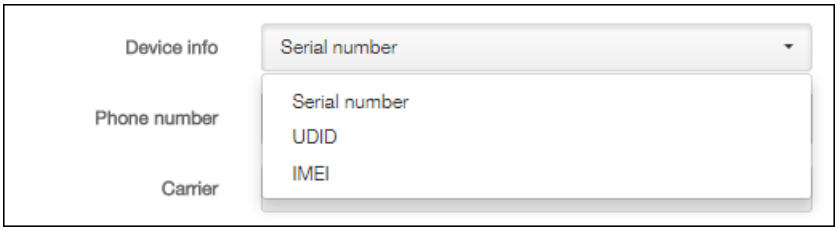
L'écran Invitation d'inscription s'affiche.



4. Dans la liste Sélectionner une plate-forme, sélectionnez iOS ou Android.
5. Dans la liste Propriétaire, sélectionnez Entreprise ou Employé.
6. Dans la liste Destinataire, sélectionnez Groupe. Des options de configuration s'affichent pour l'inscription d'un groupe.



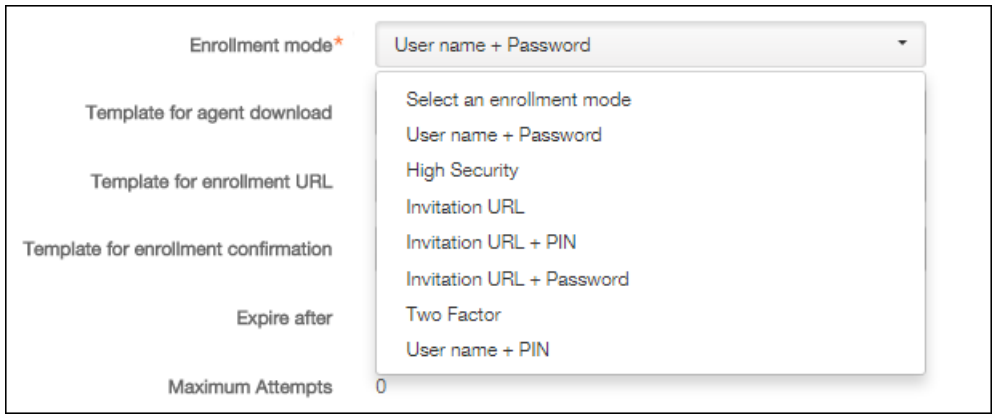
7. Dans Nom d'utilisateur, entrez un nom d'utilisateur.
   Remarque : l'utilisateur doit exister dans le serveur XenMobile en tant qu'utilisateur local ou en tant qu'utilisateur dans Active Directory. Si l'utilisateur est local, assurez-vous que la propriété Email de l'utilisateur est configurée pour envoyer des notifications. S'il s'agit d'un utilisateur Active Directory, assurez-vous que LDAP est configuré.
8. Dans la liste Infos appareil, sélectionnez 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.



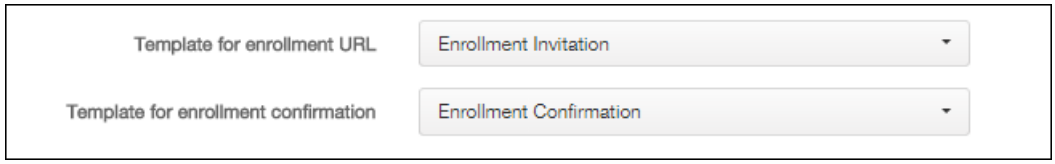
9. Dans Numéro de téléphone, entrez le numéro de téléphone de l'utilisateur (facultatif).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Dans la liste Opérateur, sélectionnez un opérateur auquel associer le numéro de téléphone de l'utilisateur.
11. Dans Mode d'inscription, sélectionnez Nom d'utilisateur + mot de passe valeur par défaut), Haute sécurité, URL d'invitation + PIN, URL d'invitation + mot de passe, Deux facteurs ou Nom d'utilisateur + PIN.



12. Dans la liste Modèle pour téléchargement de l'agent, 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 dans l'étape 1.



13. Dans Modèle pour l'URL d'inscription, sélectionnez Invitation d'inscription.
14. Dans la liste Modèle pour la confirmation d'inscription, sélectionnez Invitation d'inscription. L'invitation d'inscription expire après un certain temps. Le champ Expire après indique quand l'inscription expire. Le champ Nbre max de tentatives indique le nombre maximal de tentatives d'inscription autorisées.
15. Dans Envoyer invitation, cliquez sur ON puis sur Enregistrer et envoyer.

Pour envoyer un lien d'installation d'inscription

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 Configurer > Paramètres > Serveur de notification. Pour de plus amples informations, consultez la section Notifications dans XenMobile.

1. Dans la console XenMobile, cliquez sur Gérer > Inscription.

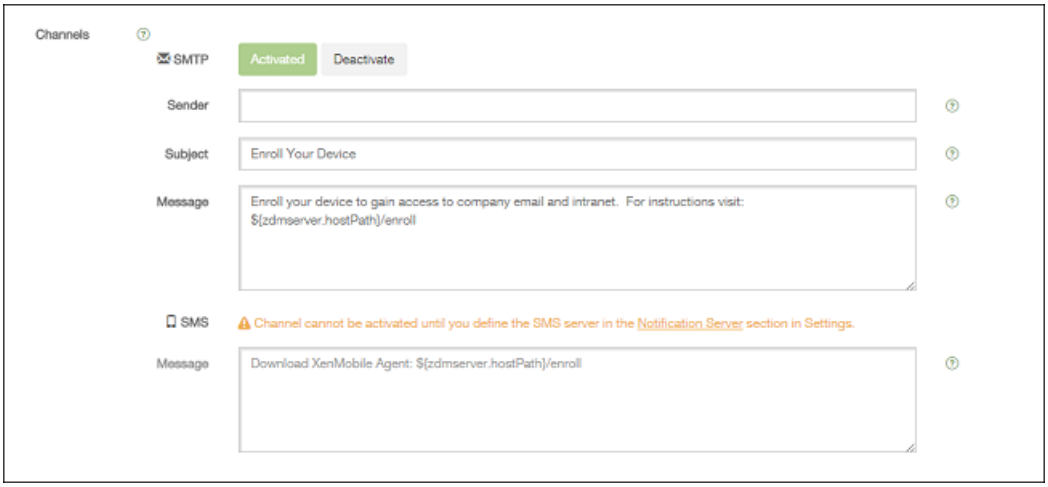


2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.
3. Cliquez sur Envoyer lien d'installation. Les options Envoyer lien d'installation s'affichent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Dans Destinataire, cliquez sur Ajouter pour ajouter l'adresse e-mail et le numéro de téléphone d'un destinataire auquel vous souhaitez envoyer un lien d'installation de l'inscription, puis cliquez sur Enregistrer. Vous pouvez répéter cette étape pour ajouter des destinataires supplémentaires un par un.
5. Dans Canaux, sélectionnez un canal à utiliser pour envoyer le lien d'installation de l'inscription. Les notifications sont envoyées via SMTP ou SMS.



Remarque : ces canaux (SMTP ou SMS) ne peuvent pas être activés tant que vous n'avez pas configuré les paramètres du serveur dans Configurer > Paramètres > Serveur de notification. Pour de plus amples informations, consultez la section Notifications dans XenMobile

6. Si vous configurez le champ SMTP, spécifiez l'expéditeur. Ce champ facultatif est utilisé dans le champ de formulaire d'un message SMTP. Si vous ne spécifiez pas d'expéditeur ici, la valeur spécifiée dans le champ Paramètres > Serveur de notification est utilisée.
7. Pour les notifications SMTP, dans Sujet, incluez l'objet du message (facultatif). Par exemple, « inscription de votre appareil ».
8. Dans Message, ajoutez le contenu du message à envoyer au destinataire. Par exemple, « Inscrivez votre appareil pour accéder à la messagerie et aux applications de l'entreprise ».
9. Pour envoyer des notifications via SMS, tapez un message qui sera envoyé au destinataire. 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.
10. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Gestion des appareils avec Android for Work dans XenMobile

Jul 25, 2016

Android for Work est un espace de travail disponible sur les appareils Android exécutant Android 5.0 et version ultérieure qui isole les comptes, applications et données d'entreprise des comptes, applications et données personnels. Dans XenMobile 10.1, vous pouvez gérer les appareils BYOD et les appareils Android appartenant à l'entreprise en demandant aux utilisateurs de créer un profil professionnel séparé sur leurs appareils qui, combiné avec le cryptage du matériel et les stratégies que vous déployez, sépare de manière sécurisée les zones professionnelles et personnelles d'un appareil. Vous pouvez gérer toutes les stratégies, applications et données d'entreprise à distance et vous pouvez effacer les stratégies, applications et données de l'appareil sans affecter la zone personnelle de l'utilisateur. Pour de plus amples informations sur la prise en charge des appareils Android, consultez la page appareils de Google.

Dans XenMobile 10.1, vous pouvez également gérer les appareils exécutant Android 4.0 - 4.4 en demandant aux utilisateurs de télécharger et d'installer l'application Android for Work, qui fournit les fonctionnalités d'espace de travail sécurisé intégrées dans les appareils exécutant Android 5.0 et version ultérieure.

Vous utilisez Google Play for Work pour ajouter, acheter et approuver les applications pour le déploiement vers l'espace de travail d'un appareil Android for Work. Vous pouvez utiliser la console Google Play for Work pour déployer vos applications Android privées, ainsi que des applications tierces et publiques.

Configuration requise pour Android for Work :

- Un domaine publiquement accessible
- Un compte d'administrateur Google
- Des appareils exécutant Android 5.0+ Lollipop avec prise en charge de profils gérés ou des appareils exécutant Android 4.0 - 4.4 (Ice Cream Sandwich, Jelly Bean et KitKat) avec l'application Android for Work
- Un compte Google avec Google Play installé dans le profil personnel de l'utilisateur
- Un profil de travail configuré sur l'appareil.

Avant de pouvoir définir des restrictions applicatives Android for Work, vous devez effectuer les opérations suivantes :

- Effectuer les tâches de configuration d'Android for Work sur Google.
- Créer des informations d'identification Google Play.
- Configurer les paramètres de serveur Android for Work.
- Créer au moins une stratégie Android for Work.
- Ajouter, acheter et approuver des applications Android for Work dans le magasin d'applications Google Play for Work.

Vous pouvez utiliser les liens suivants lorsque vous gérez Android for Work :

- Console d'administration Google : https://admin.google.com/AdminHome
- Console d'administration Play for Work : https://play.google.com/work/apps
- Publication sur Play pour les applications de chaînes privées et auto-hébergées : https://play.google.com/apps/publish
- Console Google Developer pour la création de compte de service : https://console.developers.google.com

Conditions préalables pour Android for Work

Avant de pouvoir administrer Android for Work dans XenMobile, vous devez effectuer les opérations suivantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Créer un compte Android for Work
- Configurer un compte de service
- Télécharger un certificat Android for 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 for Work et gérer les applications Android for Work dans XenMobile.

Créer un compte Android for Work

Vous devez remplir les conditions préalables suivantes avant de pouvoir configurer un compte Android for Work :

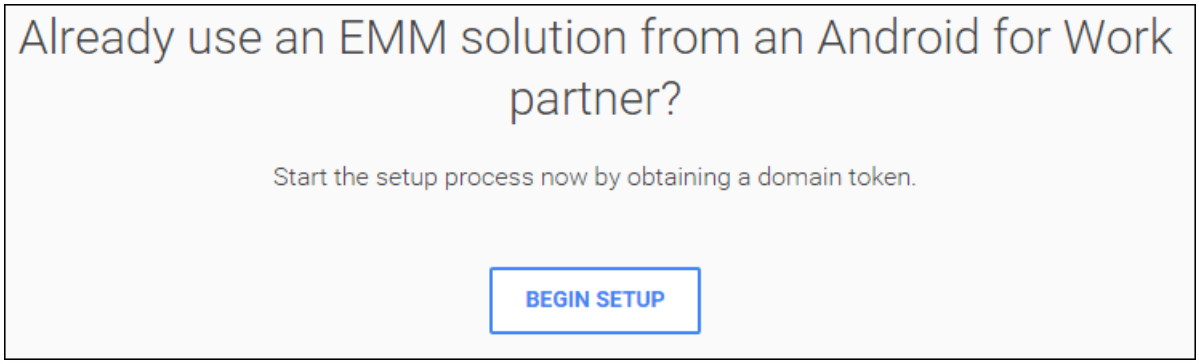
- Vous devez disposer d'un nom de domaine ; par exemple, exemple.com.
- Vous devez autoriser Google à vérifier que le domaine vous appartient.
- Vous devez activer et administrer Android for Work par le biais d'un fournisseur de gestion de la mobilité d'entreprise (EMM) (XenMobile 10.0 ou version ultérieure).

Si vous avez déjà vérifié votre nom de domaine auprès de Google, vous pouvez passer à la section Configurer un compte de service Android for Work et télécharger un certificat Android for Work.

1. Accédez au portail Google Android for Work (https://www.google.com/work/android/partners/) et accédez à la page **Partners**.

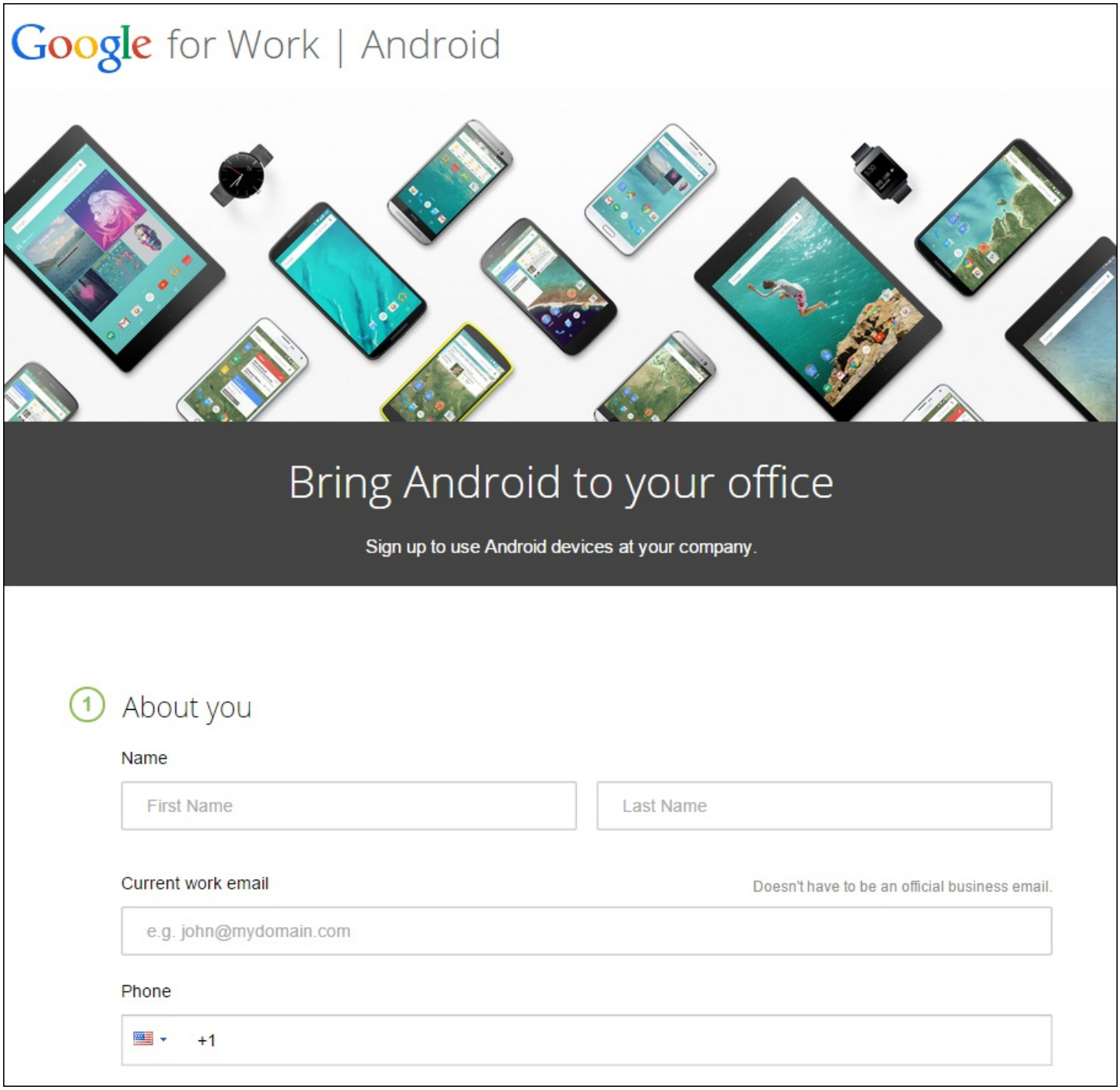


2. Cliquez sur **Begin Setup**.



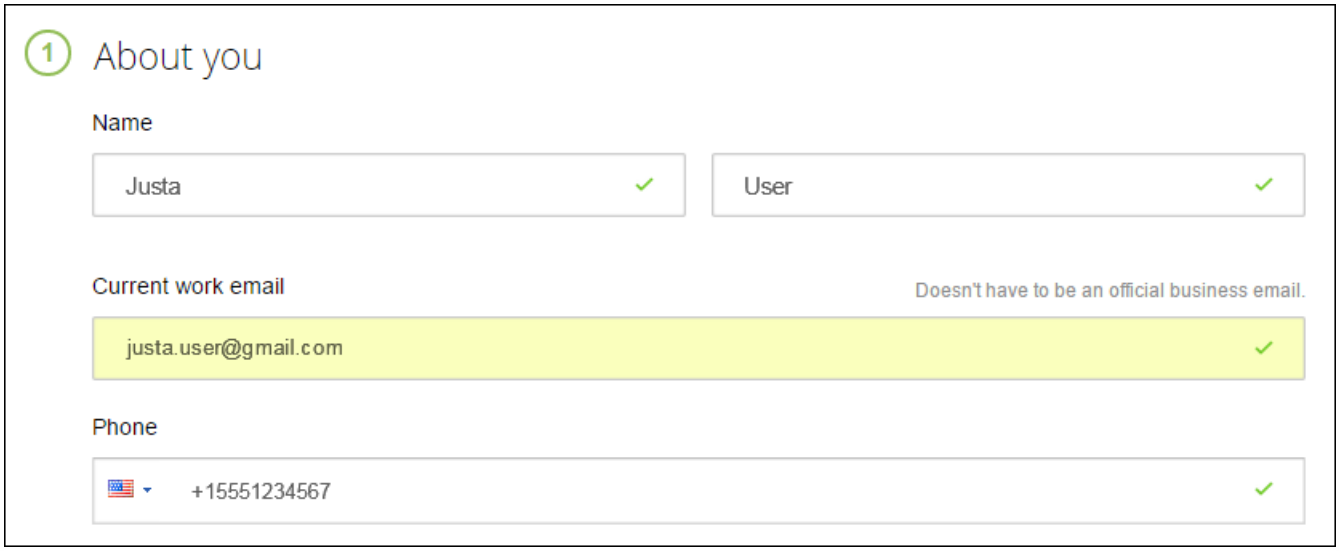
Vous serez redirigé vers la page suivante où vous entrez vos informations d'administrateur et les informations sur l'entreprise.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

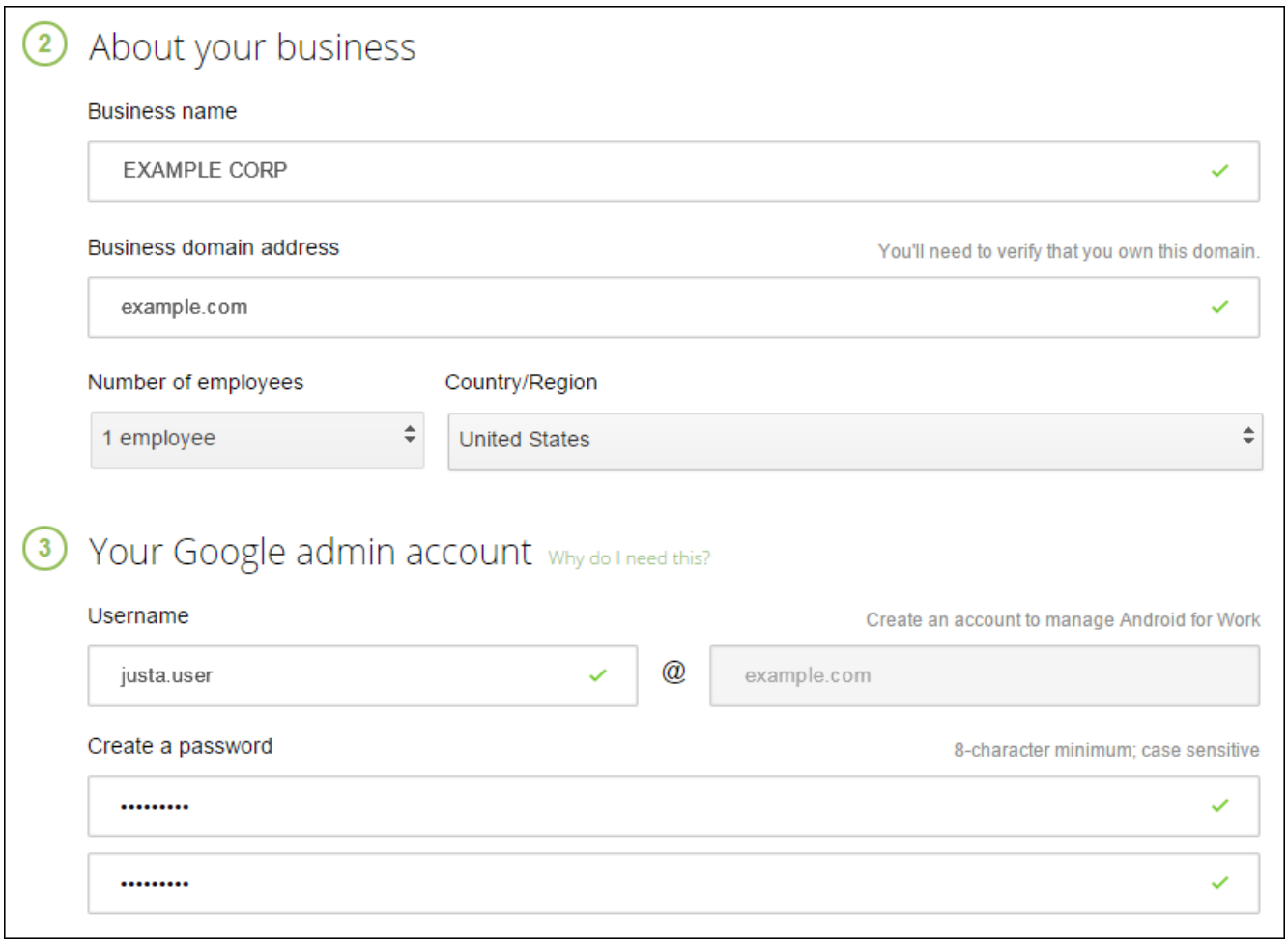


2. Entrez vos informations d'utilisateur administrateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

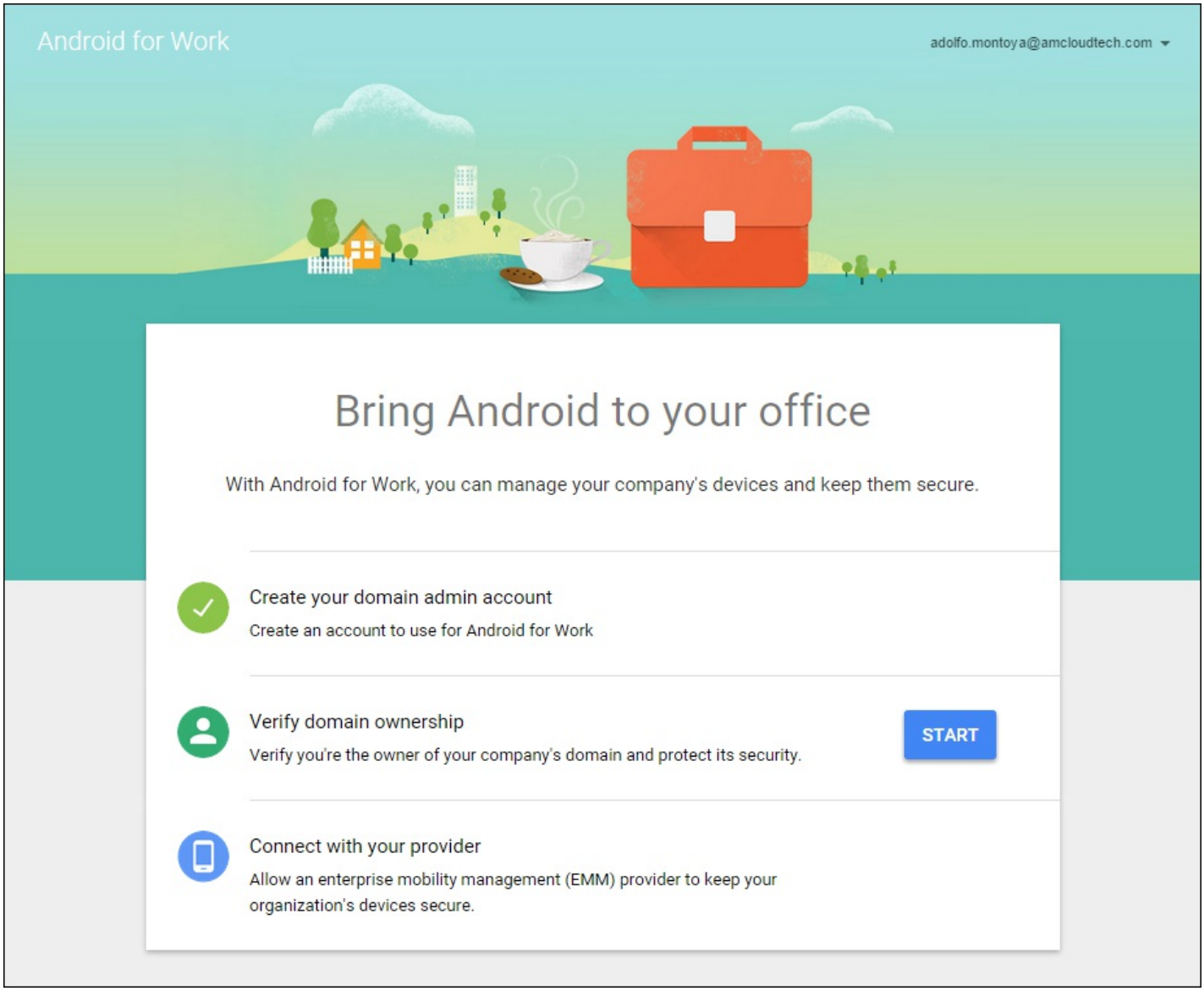


3. Entrez les informations de votre entreprise, ainsi que les informations sur votre compte d'administrateur.



La première étape de ce processus est terminée et la page suivante s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



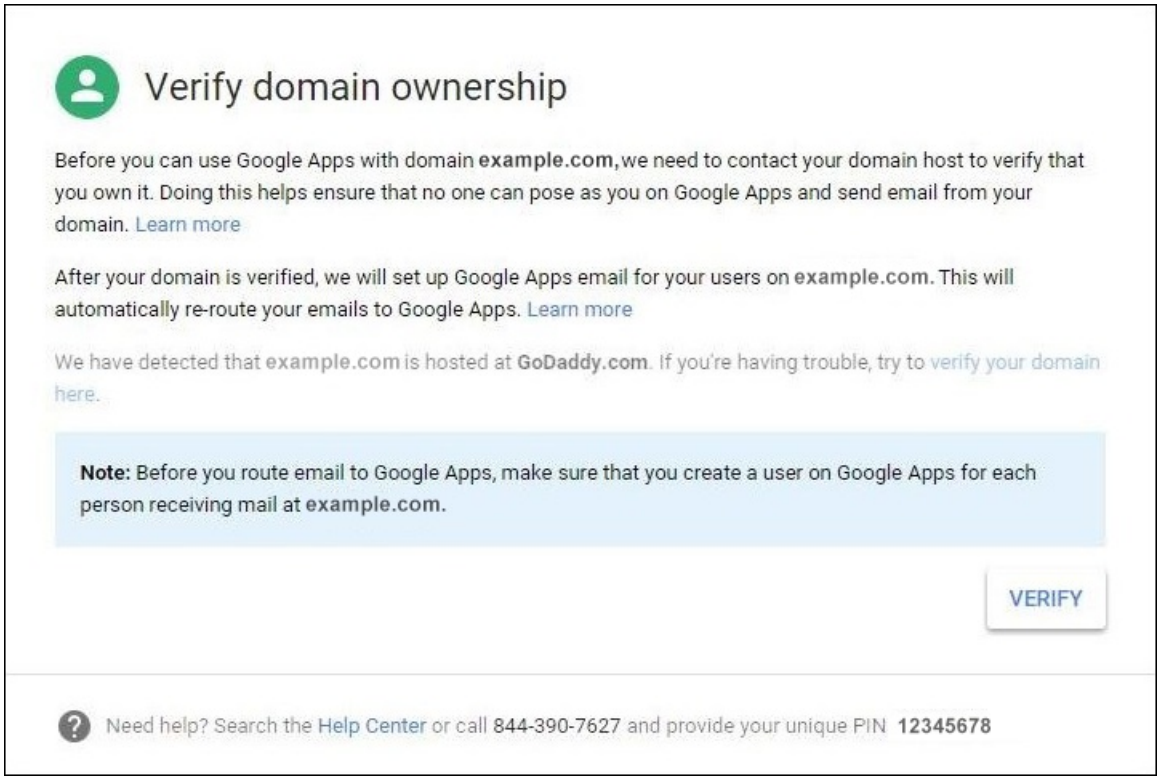
Vérifier le propriétaire du domaine

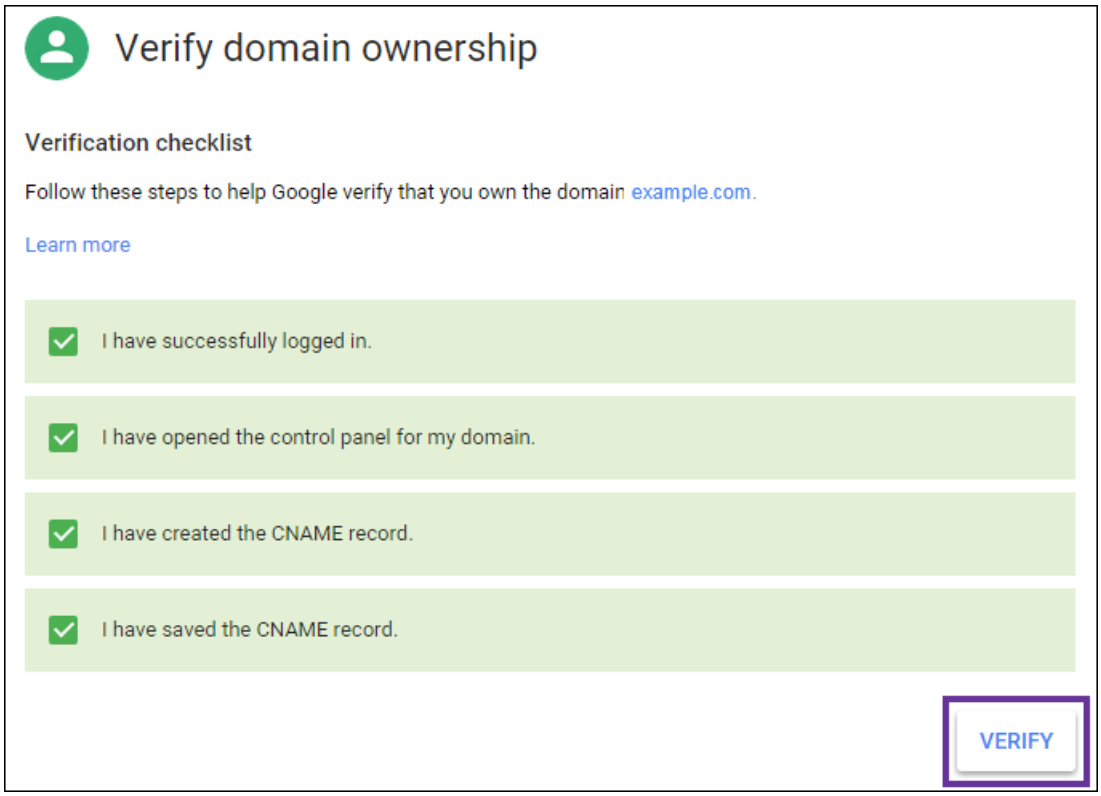
Vous devez maintenant autoriser Google à vérifier votre domaine. Il existe trois méthodes différentes pour vérifier votre domaine : ajouter un enregistrement TXT ou CNAME au site Web de l'hôte de votre domaine, charger un fichier HTML sur le serveur Web de votre domaine, ou ajouter une balise à votre page d'accueil. Google recommande la première méthode. Les étapes permettant de vérifier que votre domaine vous appartient ne sont pas couvertes dans cet article, 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 pour vérifier votre domaine.

2. Lorsque vous avez terminé, cliquez sur **Vérifier**.

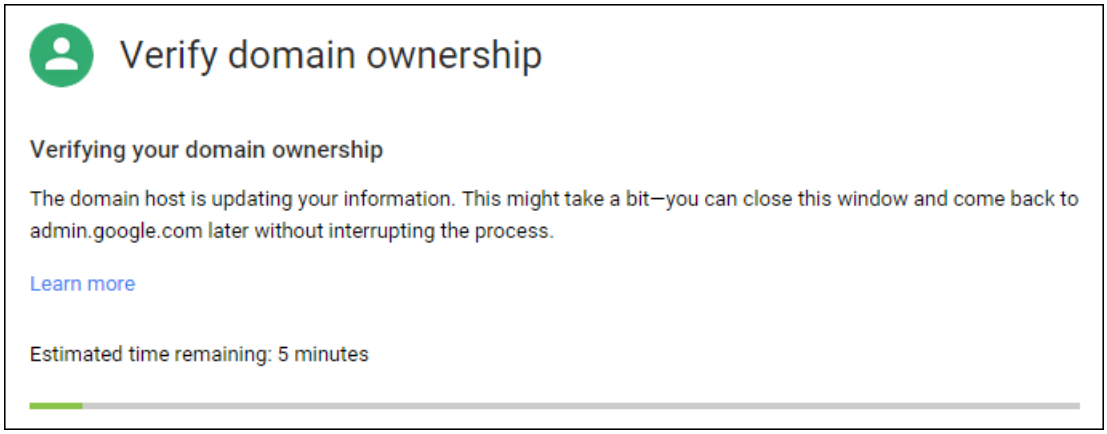
© 1999-2017 Citrix Systems, Inc. All rights reserved.



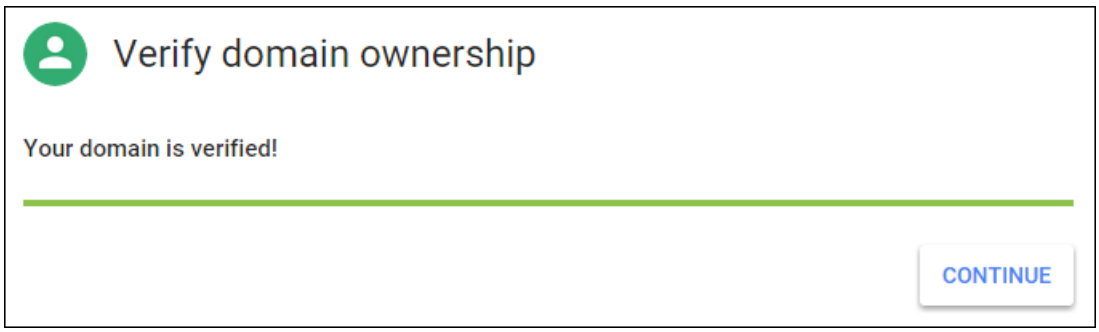


7. Google vérifie que vous êtes le propriétaire du domaine.

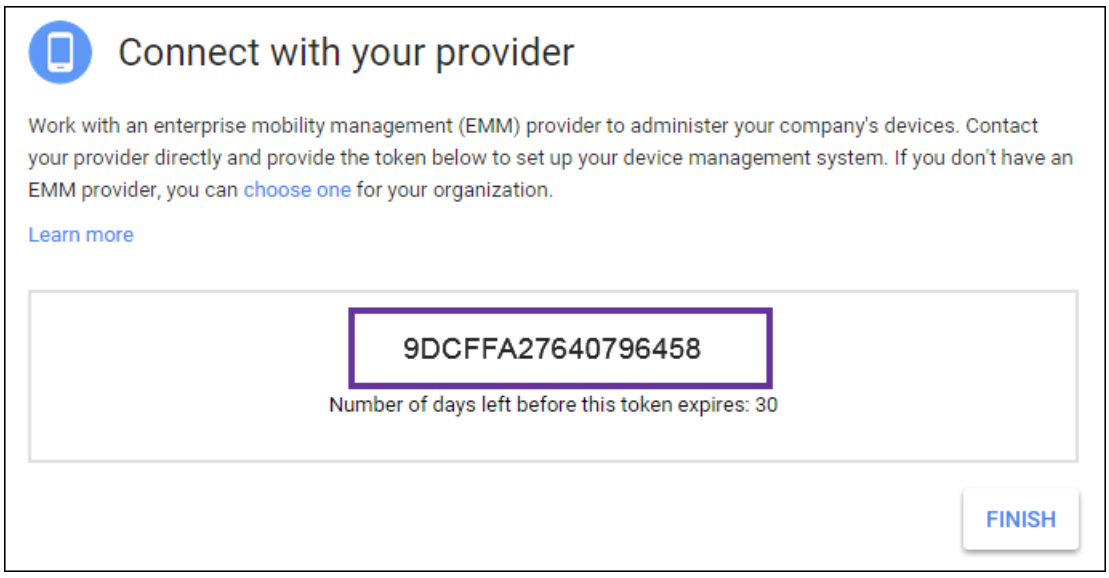
© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. La page suivante s'affiche si la vérification réussit. Cliquez sur **Continuer**.

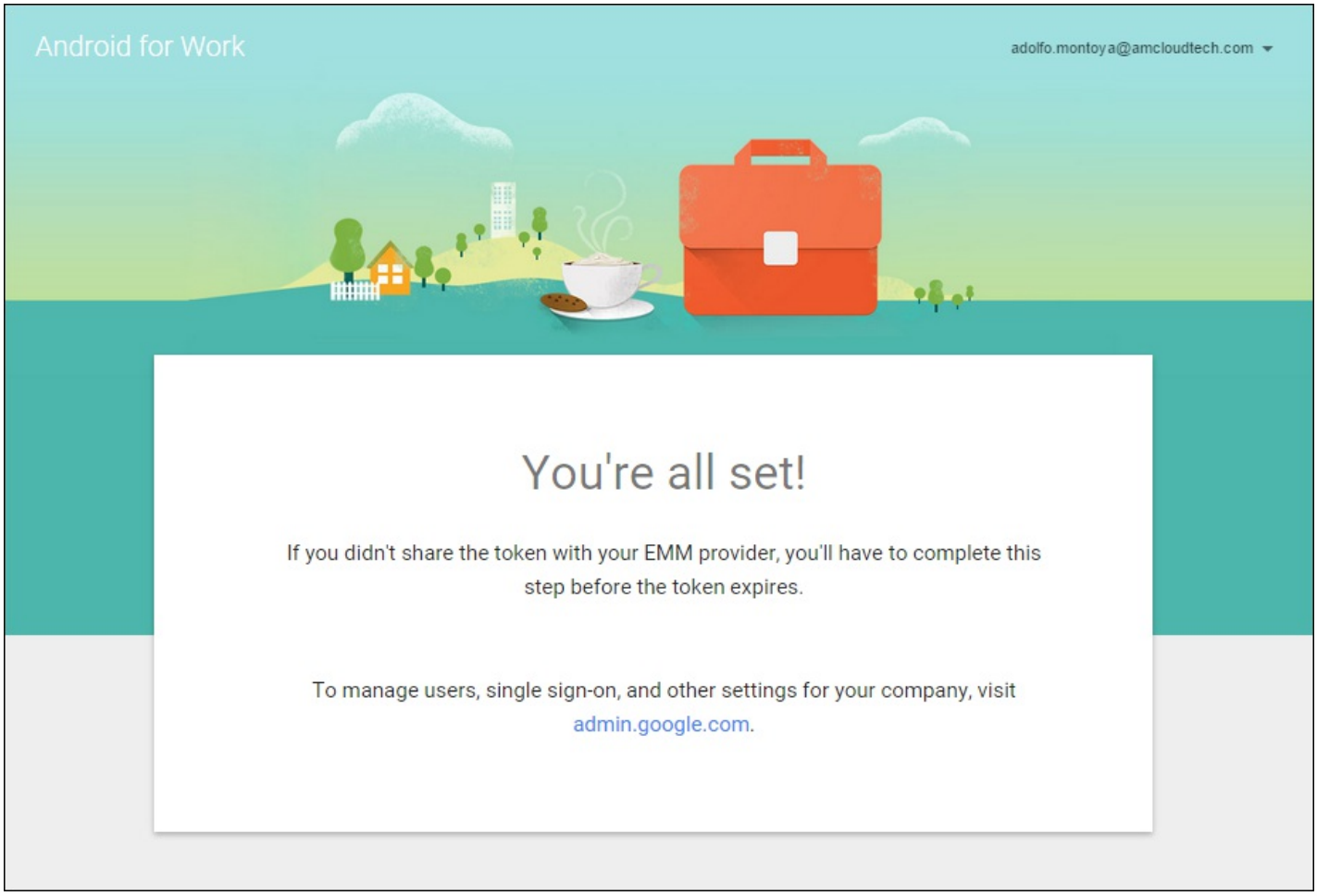


9. Google crée un jeton de liaison EMM que vous fournissez à Citrix lorsque vous configurez les paramètres d'Android for Work. Copiez et enregistrez le jeton ; vous en aurez besoin plus tard lors de la configuration.



10. Cliquez sur **Finish** pour terminer la configuration Android for Work.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



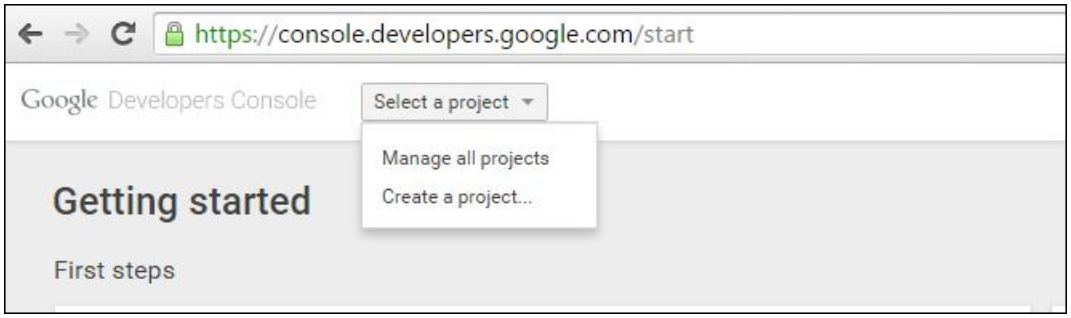
11. Une fois que vous avez créé un compte de service Android for Work, vous pouvez ouvrir une session sur la console d'administration Google pour gérer vos paramètres de gestion de la mobilité Android for Work.

Définissez un compte de service Android for Work et téléchargez un certificat Android for Work

Pour autoriser XenMobile à contacter les services Google Play et Directory, vous devez créer un nouveau 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 for Work. Pour de plus amples informations sur le protocole d'authentification utilisé, accédez à https://developers.google.com/identity/protocols/OAuth2ServiceAccount.

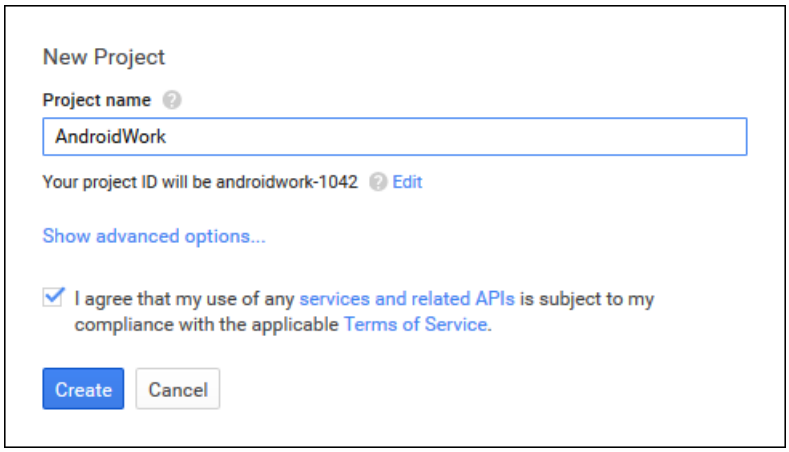
1. Dans un navigateur Web, accédez à https://console.developers.google.com/project et ouvrez une session à l'aide de vos informations d'identification d'administrateur Google.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

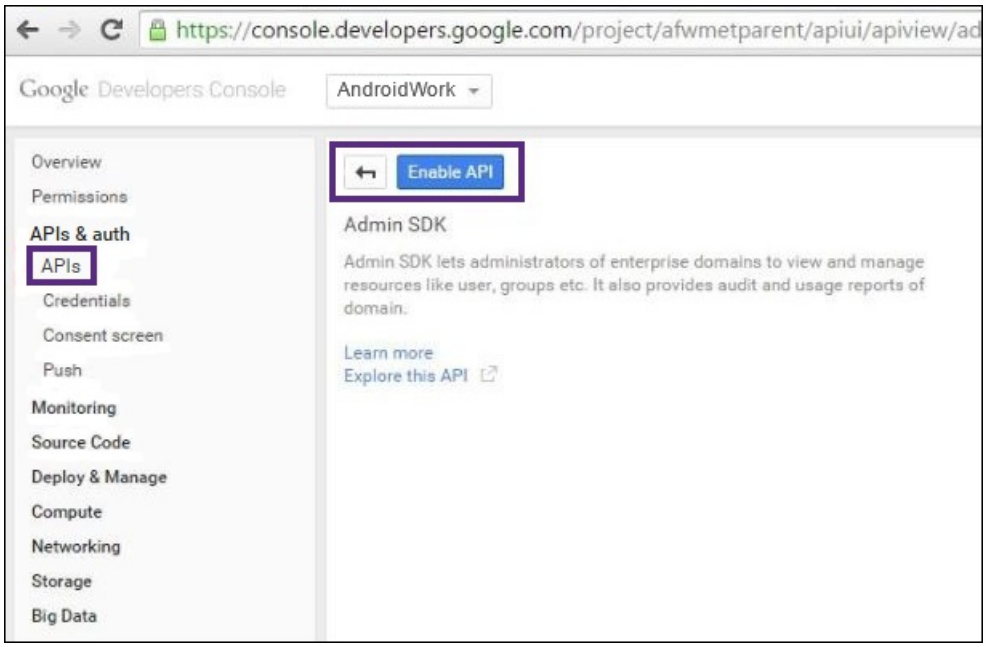


3. Dans la liste **Sélectionnez un projet**, cliquez sur **Créer un projet**.

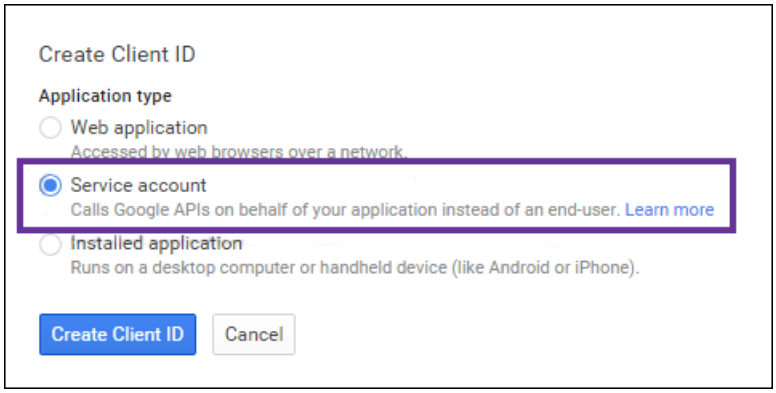
4. Entrez un nom de projet, cliquez sur la case à cocher pour accepter les conditions d'utilisation du service, et cliquez sur **Créer**.



5. Dans le panneau de gauche, cliquez sur **API et authentification**, puis cliquez sur **API**.



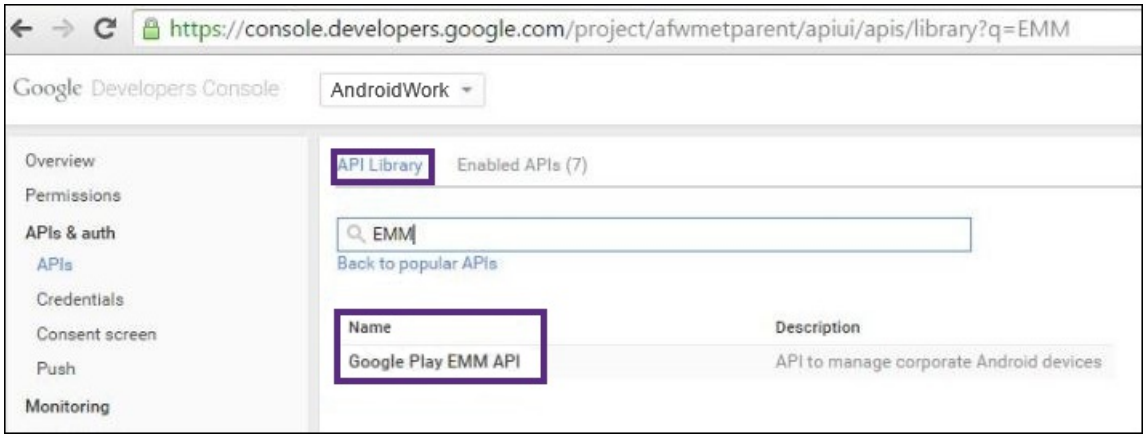
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans **API Google Apps**, cliquez sur **Admin SDK**. Vous pouvez également taper « Admin SDK » dans le champ de recherche, puis cliquer sur **Admin SDK** sur la page des résultats de la recherche.

7. Cliquez sur **Activer l'API**.

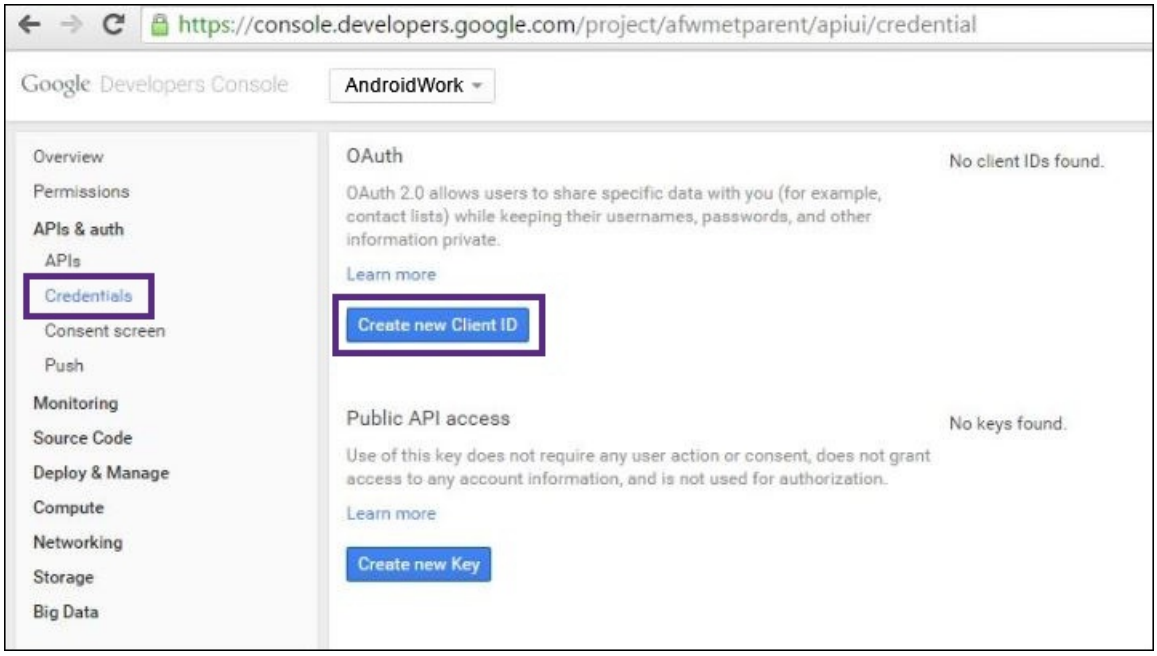
8. Sous **Bibliothèque API**, recherchez **EMM** et sélectionnez **Google Play EMM API**.



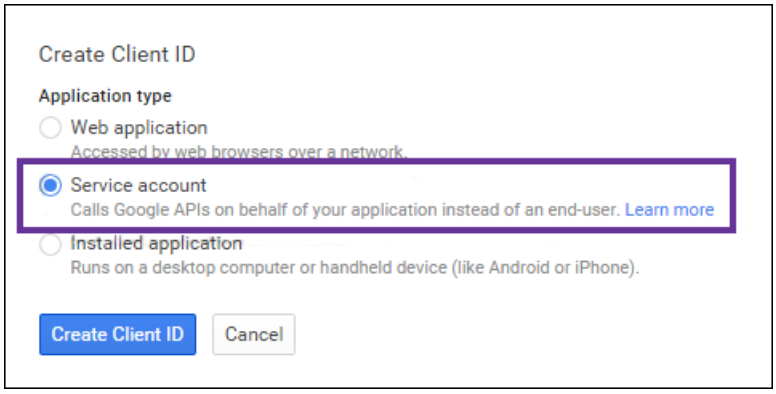
9. Cliquez sur **Activer l'API**.

10. Sur la même page, dans le panneau de gauche, sous **API et authentification**, cliquez sur **Certificats**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. Dans le panneau de droite, cliquez sur **Créer un nouvel identifiant client**. La boîte de dialogue **Créer un identifiant client** s'affiche.



12. Sélectionnez **Compte de service** et cliquez sur **Créer un identifiant client**.

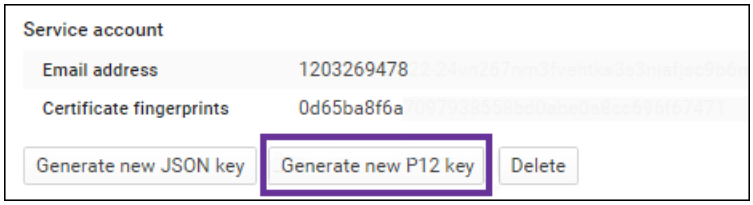
13. Cliquez sur **OK, j'ai compris**. Après avoir cliqué sur OK, j'ai compris, un fichier json est téléchargé sur votre ordinateur. Veillez à enregistrer le fichier dans un emplacement sécurisé.

Sous **Compte de service**, prenez note de l'adresse e-mail et des empreintes digitales du certificat (mot de passe). Vous en aurez besoin dans les prochaines étapes.

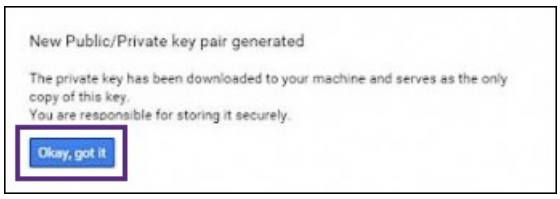
L'adresse e-mail est le compte de service que vous utilisez lors de la liaison de XenMobile en tant que fournisseur EMM et pour activer l'accès au client API.

14. Sous **Compte de service**, cliquez sur **Générer nouvelle clé P12**. Le certificat (fichier P12) est téléchargé sur votre ordinateur. Veillez à enregistrer le certificat dans un emplacement sécurisé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

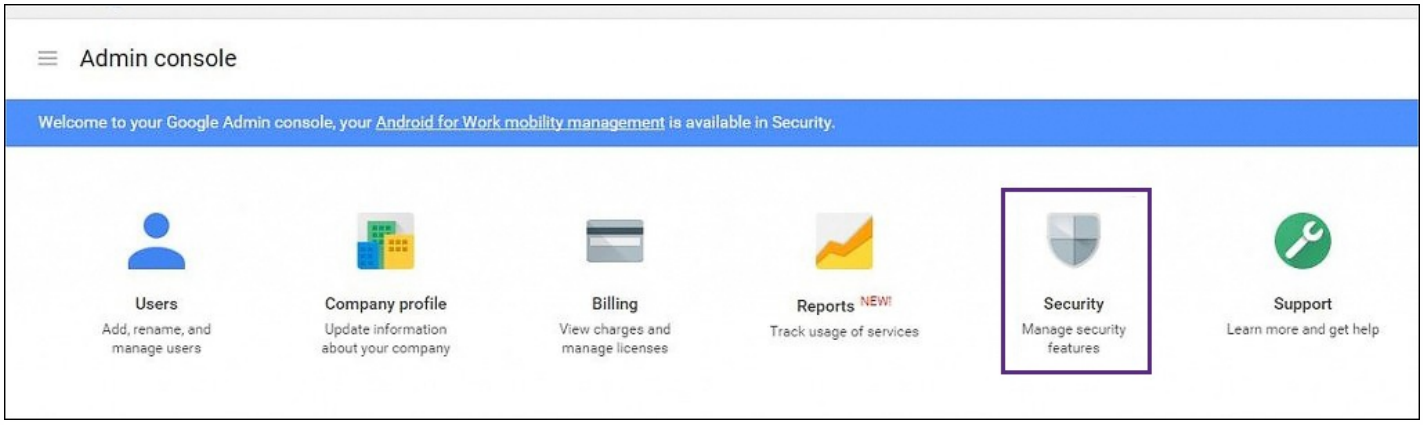


15. Cliquez sur **OK, j'ai compris**.

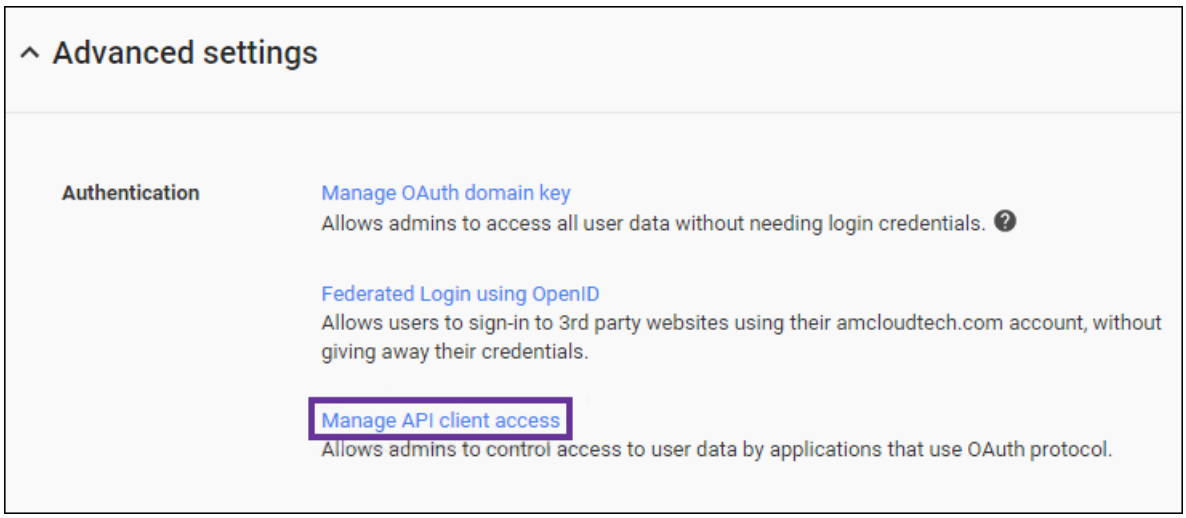


16. Ouvrez une session sur le portail de la console d'administration Google à l'adresse https://admin.google.com avec vos identifiants d'administrateur Google Android for Work.

17. Cliquez sur **Sécurité**.



18. Cliquez sur **Paramètres avancés** et cliquez sur **Gérer l'accès au client d'API**.



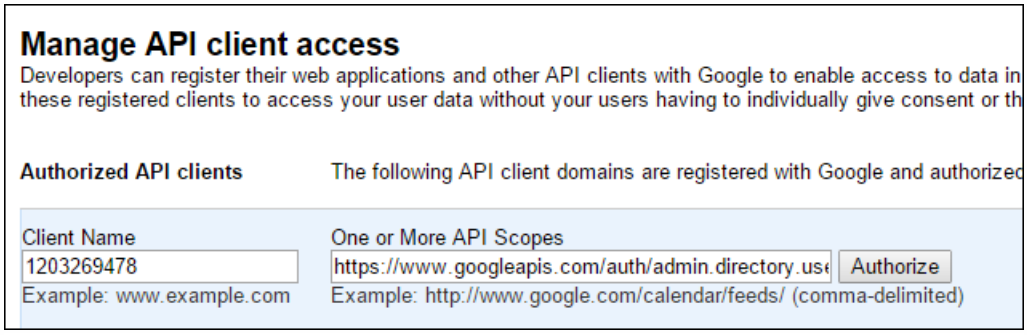
© 1999-2017 Citrix Systems, Inc. All rights reserved.

19. Cliquez sur **Clients API autorisés**. La page **Gérer l'accès au client d'API** s'affiche.

20. Dans le champ **Nom du client**, entrez l'ID client généré à l'étape 14.

21. Dans **Une ou plusieurs étendues d'API**, entrez « https://www.googleapis.com/auth/admin.directory.user » (sans les guillemets).

22. Cliquez sur **Autoriser**.

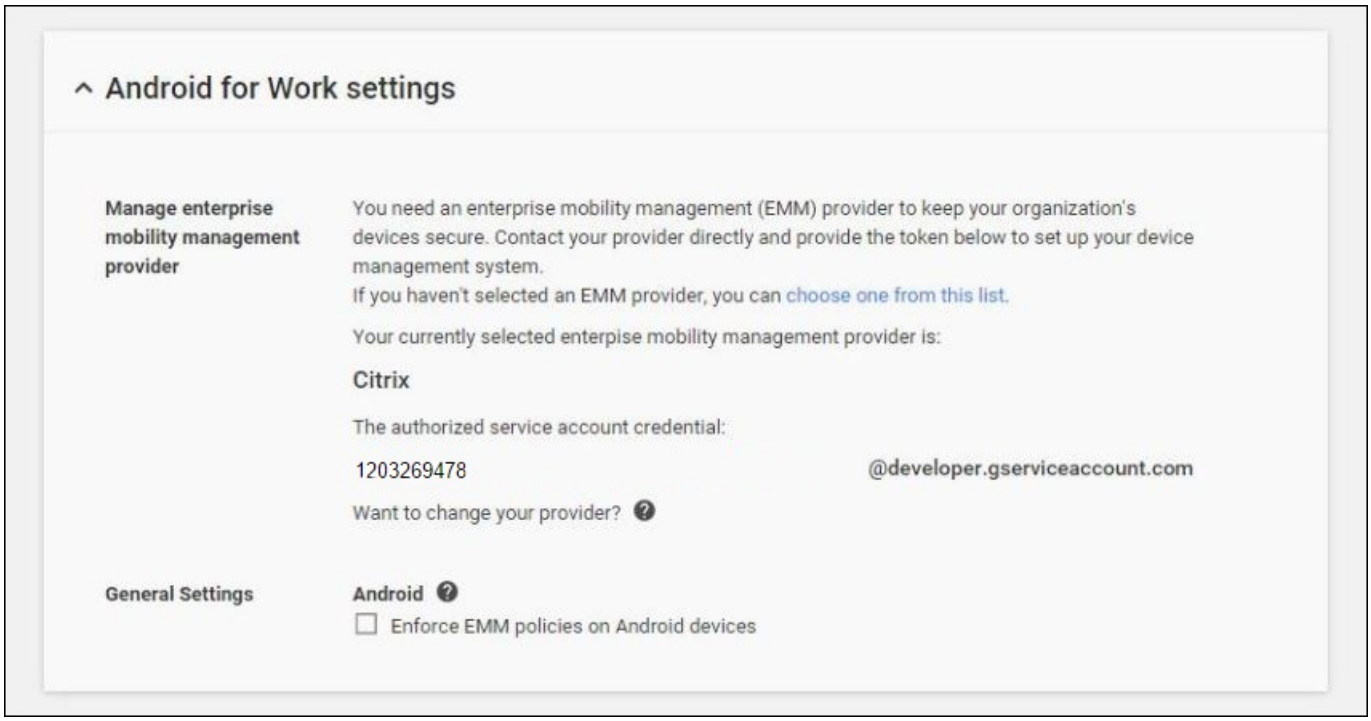


Liaison à EMM

Avant de pouvoir utiliser XenMobile pour gérer vos appareils Android for Work, vous devez contacter l'assistance technique de Citrix (https://www.citrix.com/contact/technical-support.html) et fournir votre nom de domaine, compte de service et jeton de liaison. Citrix liera le jeton à XenMobile en tant que fournisseur de gestion de la mobilité d'entreprise (EMM).

1. Pour confirmer la liaison, ouvrez une session sur le portail de la console d'administration Google et cliquez sur **Sécurité**.

2. Cliquez sur **Paramètres Android for Work**. Vous verrez que votre compte Google Android for Work est lié à Citrix en tant que fournisseur EMM.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Après avoir confirmé la liaison du jeton, vous pouvez commencer à utiliser XenMobile pour gérer vos appareils Android for Work. Vous devez importer le certificat P12 que vous avez généré à l'étape 14, configurer les paramètres du serveur Android for Work, activer l'authentification unique SAML et définir au moins une stratégie d'appareil Android for Work.

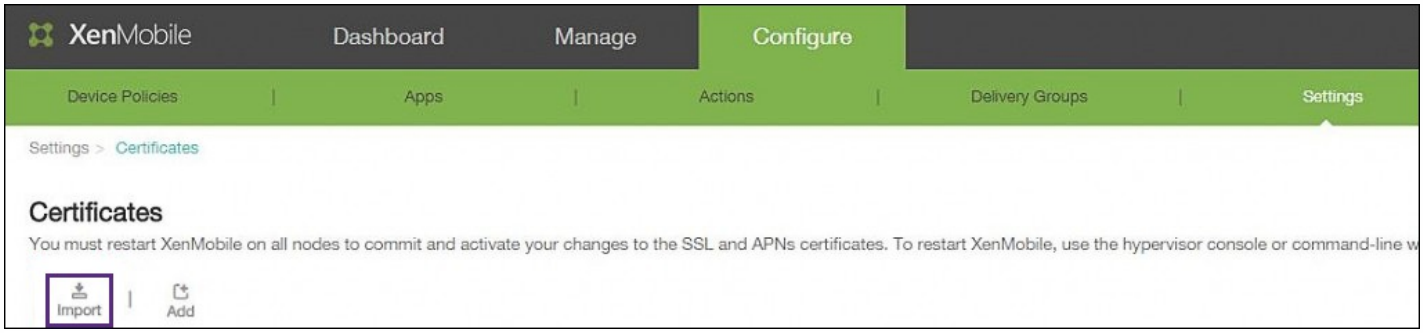
Importer le certificat P12

Suivez ces étapes pour importer votre certificat P12 Android for Work :

Ouvrez une session sur la console XenMobile 10.1.

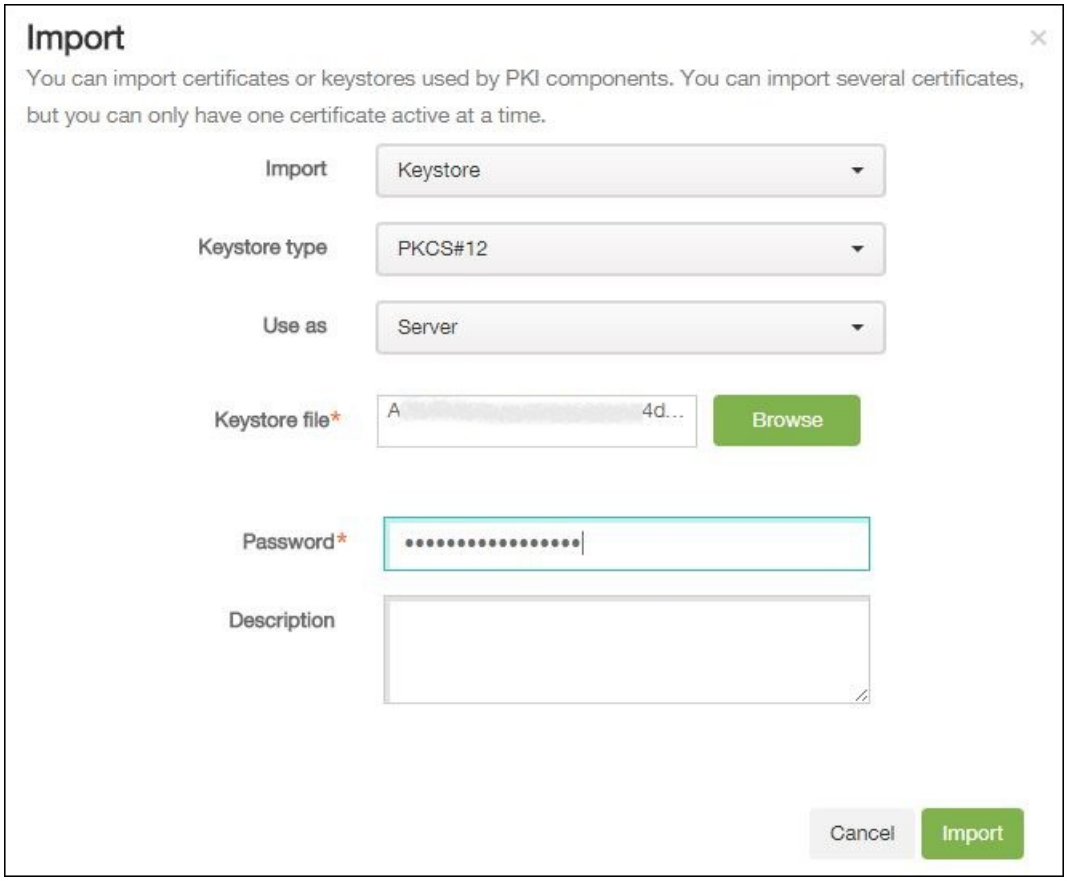
2. Cliquez sur **Configurer -> Paramètres -> Certificat**. La page **Certificats** s'affiche.





3. Cliquez sur **Importer**. La boîte de dialogue **Importer** apparaît. Configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



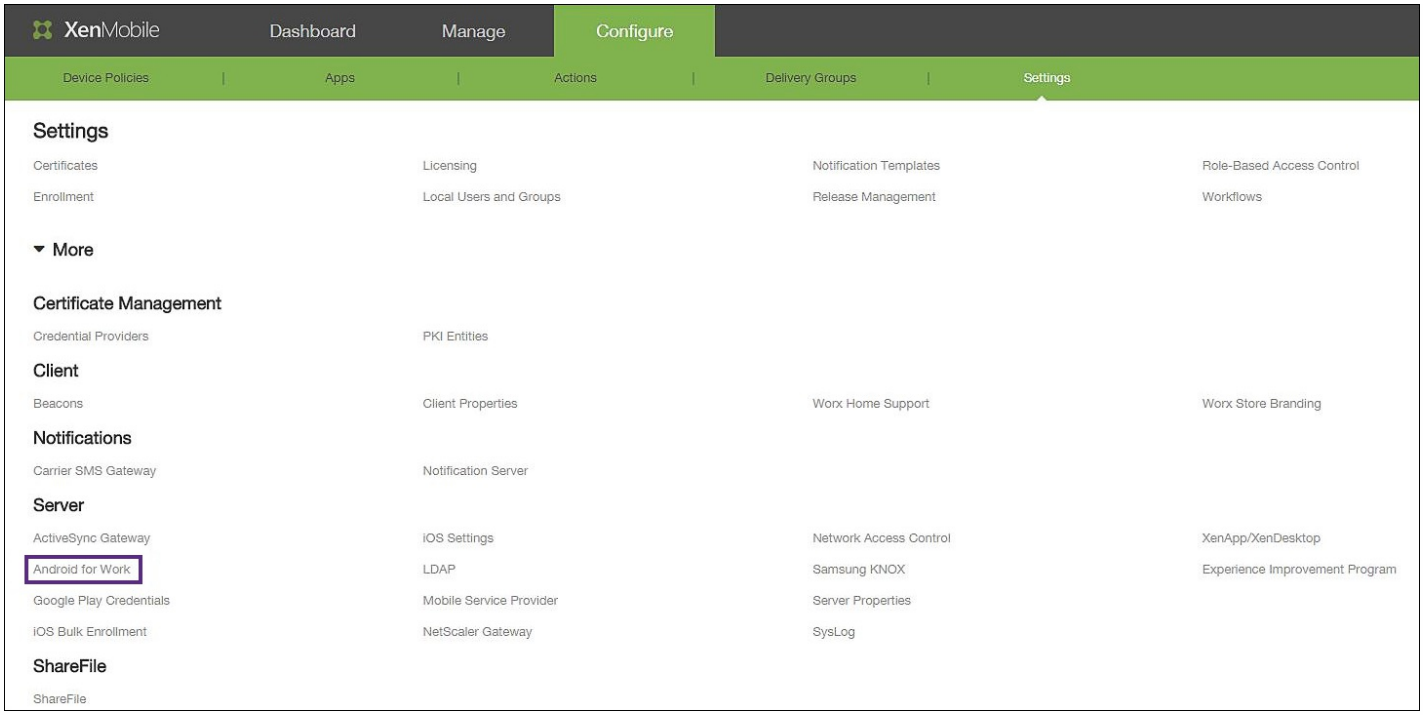
- **Importer** : dans la liste, cliquez sur Keystore.
- **Type de keystore** : dans la liste, cliquez sur PKCS#12.
- **Utiliser en tant que** : dans la liste, cliquez sur Serveur.
- **Fichier de keystore** : cliquez sur Parcourir et accédez au certificat P12.
- **Mot de passe** : entrez le mot de passe du keystore.
- **Description** : entrez une description pour le certificat.

4. Cliquez sur **Importer**.

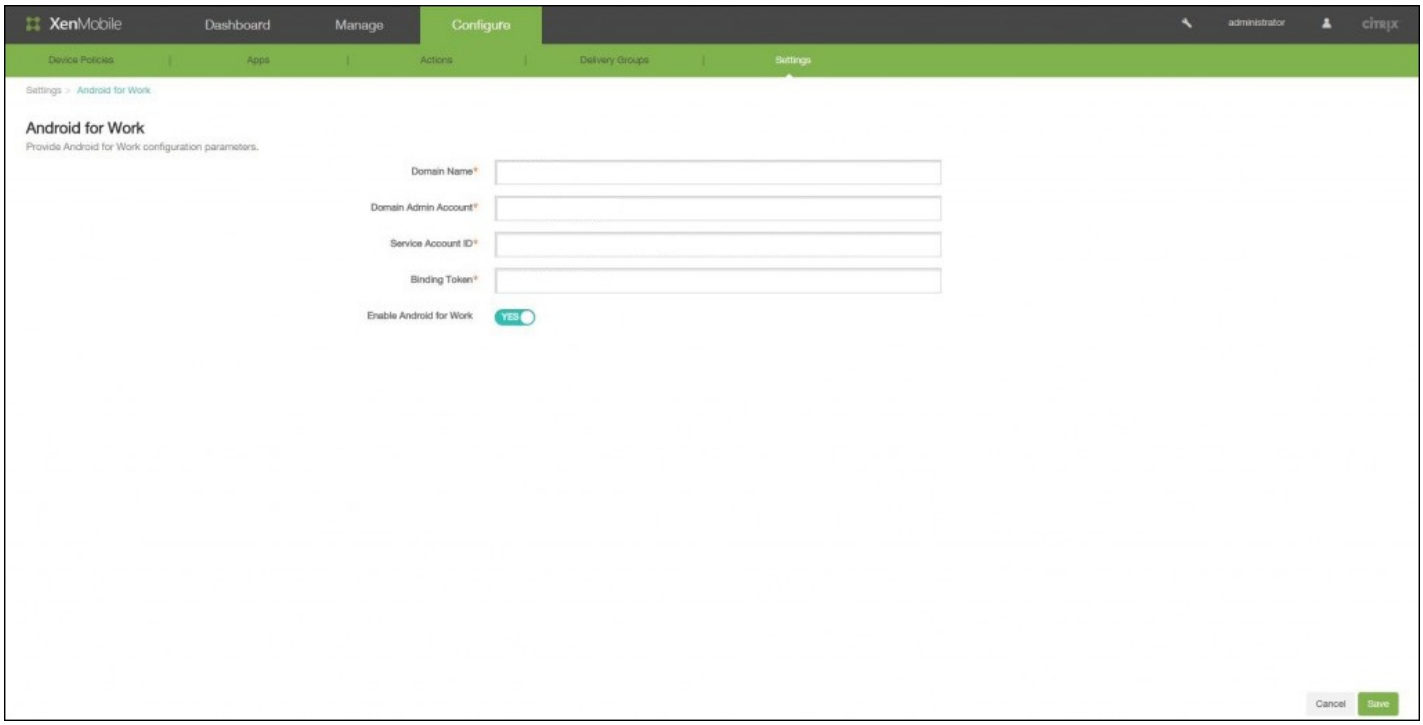
Configurer les paramètres du serveur Android for Work

1. Cliquez sur **Configurer -> Paramètres** et développez **Plus**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Sous **Serveur**, cliquez sur **Android for Work**. La page **Android for Work** s'affiche. Configurez les paramètres suivants :



- **Nom de domaine** : entrez votre nom de domaine Android for Work.
- **Compte d'administrateur de domaine** : entrez le nom d'utilisateur de votre administrateur de domaine.
- **ID du compte de service** : entrez l'ID de votre compte de service.
- **Jeton de liaison** : entrez, ou copiez et collez le jeton de liaison.
- **Activer Android for Work** : cliquez pour activer ou désactiver Android for Work.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur **Enregistrer**.

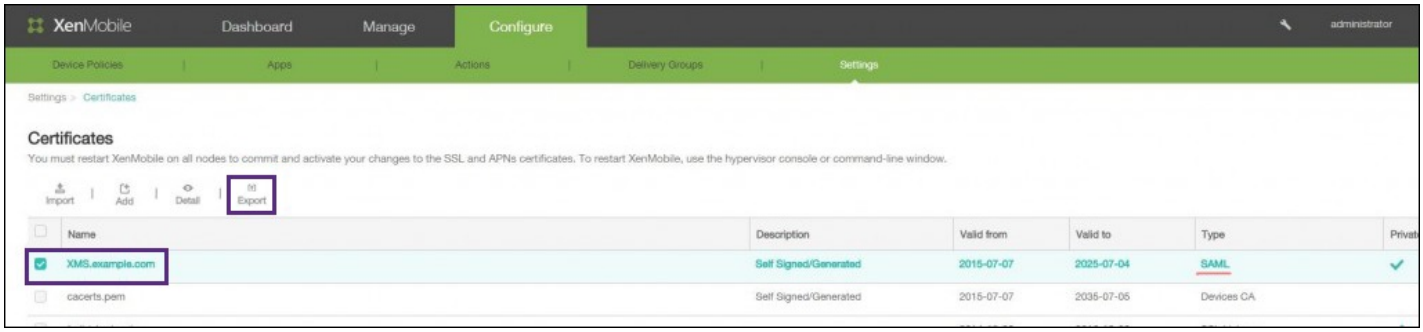
Activer l'authentification unique SAML

Ouvrez une session sur la console XenMobile 10.1.

2. Cliquez sur **Configurer -> Paramètres -> Certificat**. La page **Certificats** s'affiche.



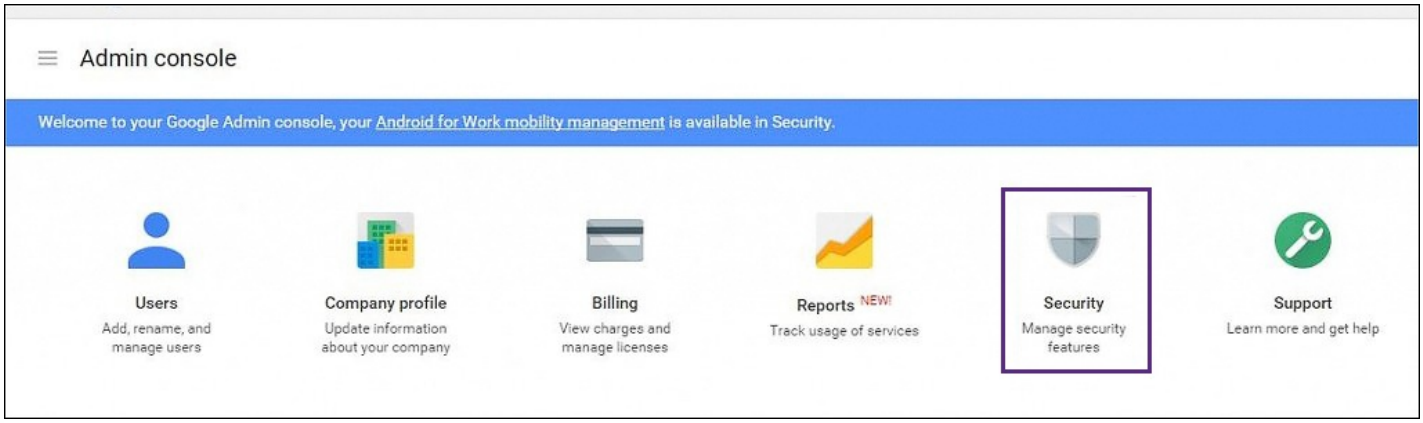
3. Sur la page **Certificats**, dans la liste des certificats, cliquez sur le certificat SAML.



Cliquez sur **Exporter** et enregistrez le certificat sur votre ordinateur.

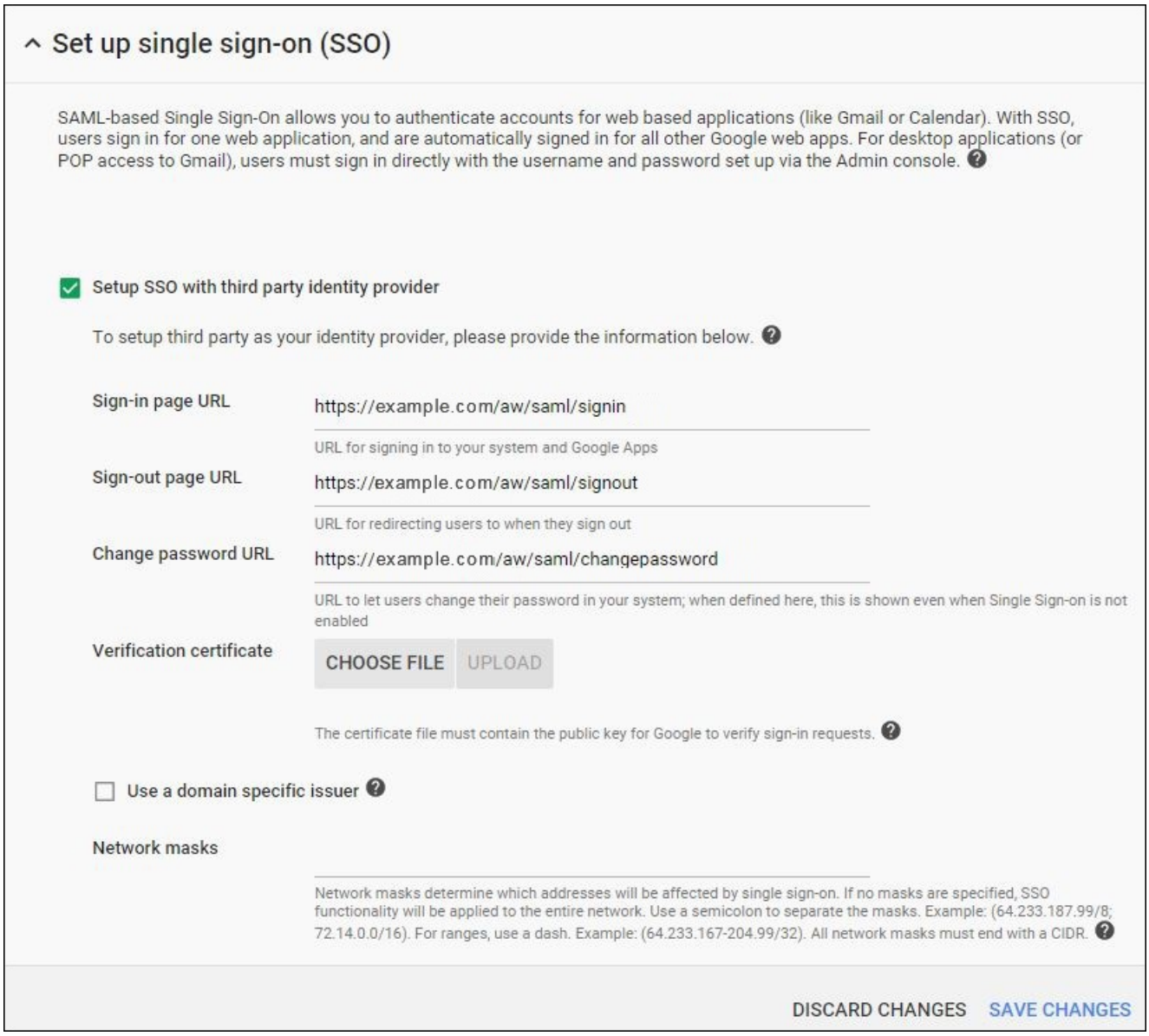
5. Ouvrez une session sur le portail de la console d'administration Google (https://admin.google.com) avec vos identifiants d'administrateur Android for Work.

6. Cliquez sur **Sécurité**.



7. Dans **Sécurité**, cliquez sur **Configurer l'authentification unique (SSO)** et configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



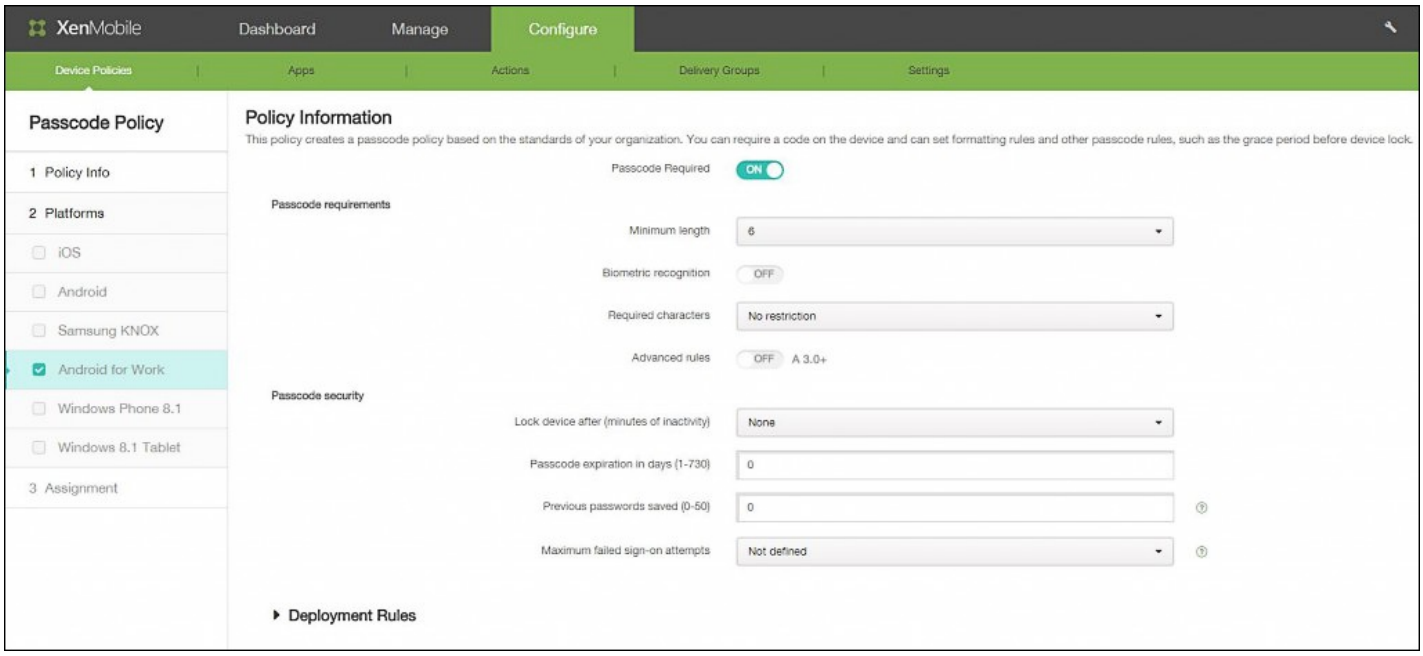
- **URL de la page de connexion** : entrez l'adresse URL des utilisateurs qui se connectent à votre système et Google Apps. Par exemple : https:///aw/saml/signin.
- **URL de la page de déconnexion** : entrez l'adresse URL vers laquelle les utilisateurs sont redirigés lorsqu''ils se déconnectent. Par 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. Lorsque cette option est définie ici, les utilisateurs voient cette fonctionnalité même si 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 for Work

Vous pouvez configurer n'importe quelle stratégie, mais 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les étapes de base pour configurer une stratégie sont les suivantes :

1. Ouvrez une session sur la console XenMobile 10.1.

2. Cliquez sur **Configurer -> 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 de stratégies d'appareil, consultez la section Stratégies d'appareil.

Vos utilisateurs peuvent désormais télécharger l'application Worx Home à partir du magasin Google Play et inscrire leurs appareils dans XenMobile (veillez à utiliser le nom d'utilisateur principal (UPN) pour l'inscription). Une fois les appareils inscrits avec succès, Worx Home va installer le profil Android for Work de façon à ce que les utilisateurs puissent accéder à leurs applications Android for Work. Les utilisateurs peuvent être invités à crypter leurs appareils lors de ce processus avant de pouvoir continuer.

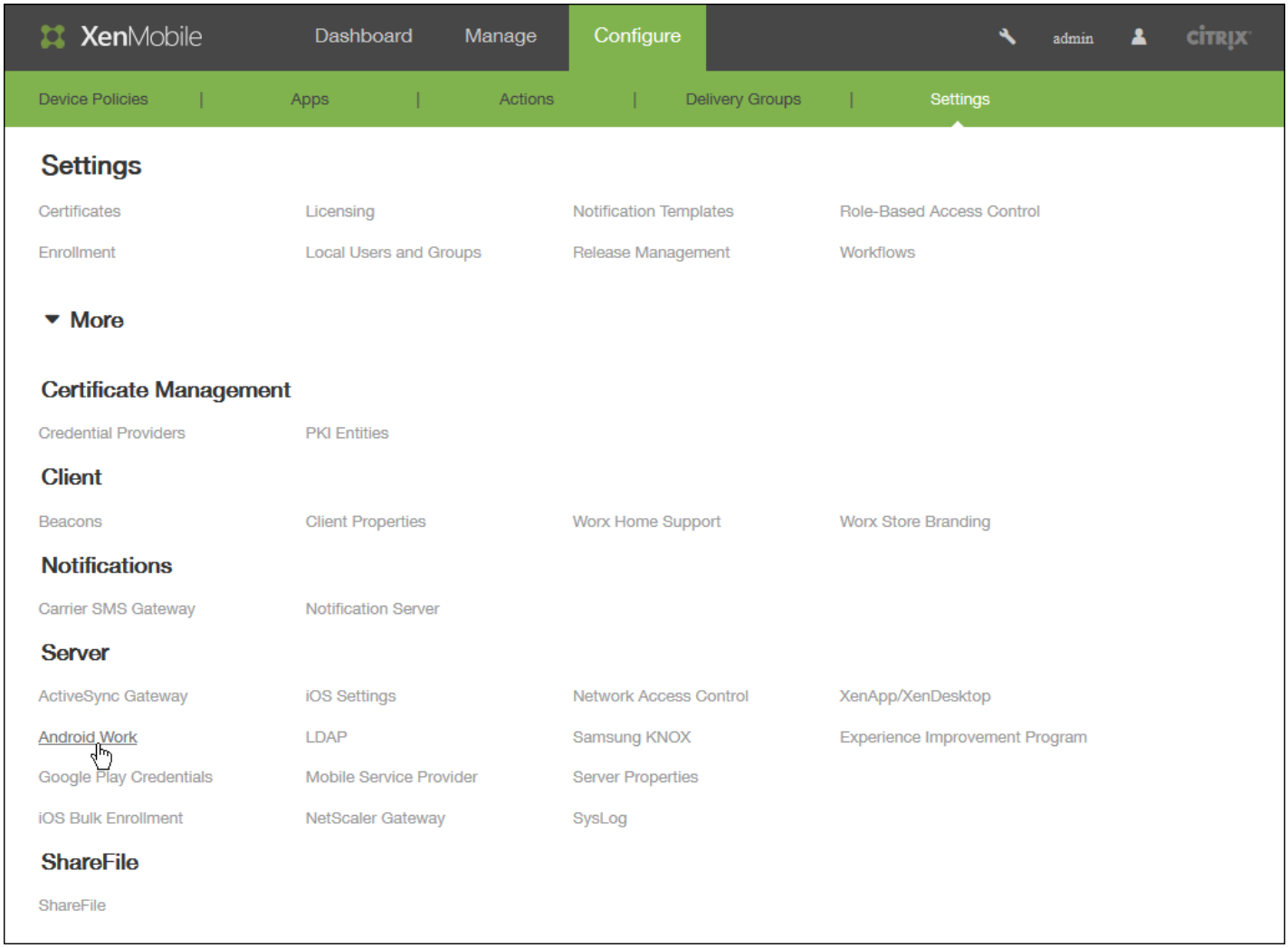
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurer les paramètres de compte Android for Work.

Jul 25, 2016

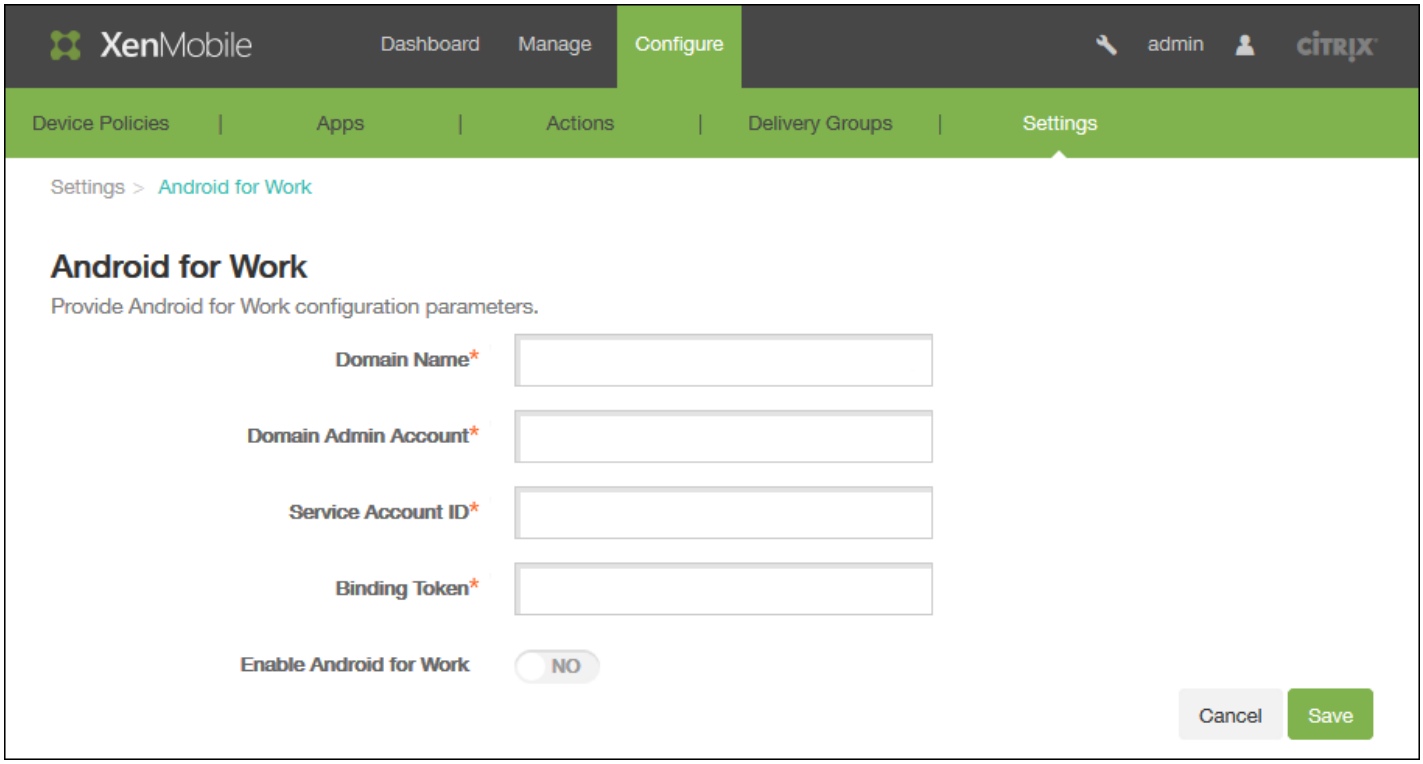
Avant de démarrer la gestion des applications et des stratégies Android for Work sur les appareils des utilisateurs, vous devez définir les informations de domaine et de compte Android for Work dans XenMobile. Avant de procéder, toutefois, vous devez effectuer les tâches de configuration Android for Work sur Google pour configurer un administrateur de domaine et obtenir un ID de compte de service et un jeton de liaison. Pour de plus amples informations sur les tâches de configuration Android for Work sur Google, consultez la section Gestion des appareils avec Android for Work.

1. Dans la console XenMobile, cliquez sur **Configurer > Paramètres**.



2. Développez **Plus**, puis sous **Serveur**, cliquez sur **Android for Work**. La page **Android for Work** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.
- **Jeton de liaison** : entrez ou collez le jeton de liaison que vous avez reçu depuis Google lorsque vous avez configuré votre compte Android for Work.
- **Activer Android for Work** : sélectionnez cette option pour activer Android for Work.

4. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

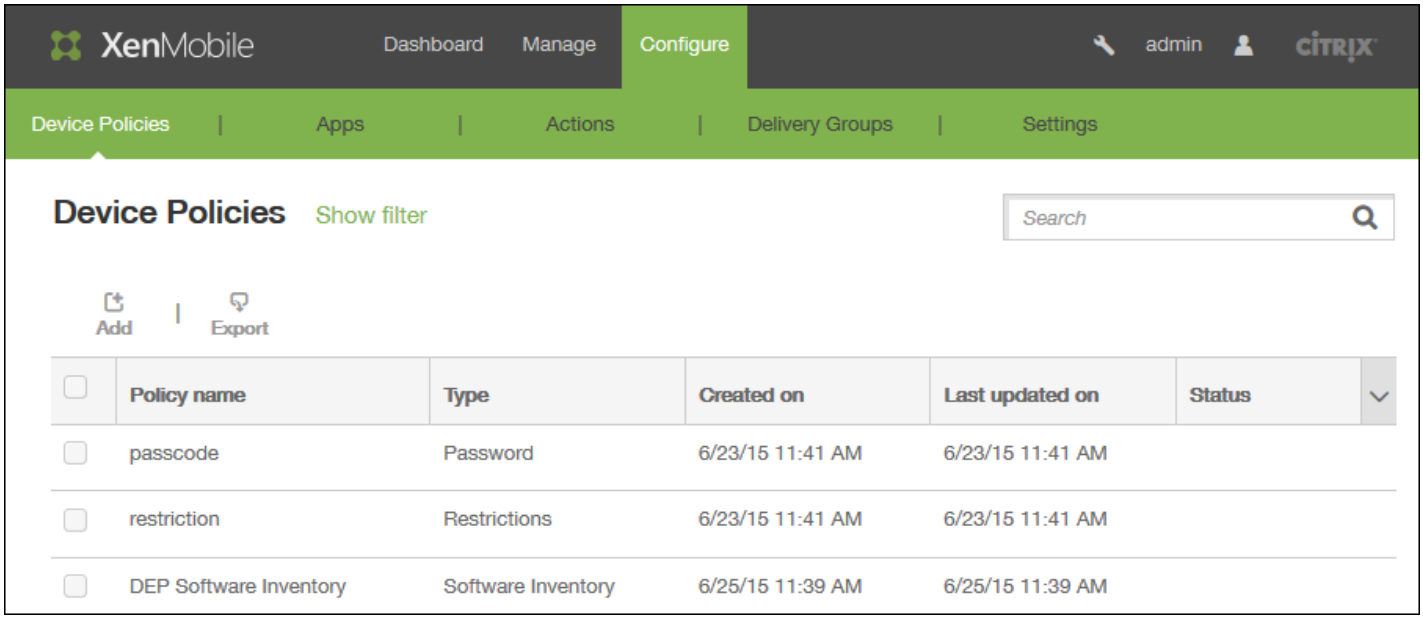
Stratégie de restrictions applicatives Android for Work

Jul 25, 2016

Vous pouvez modifier les restrictions associées avec les applications Android for Work, mais vous devez avant cela effectuer les actions suivantes :

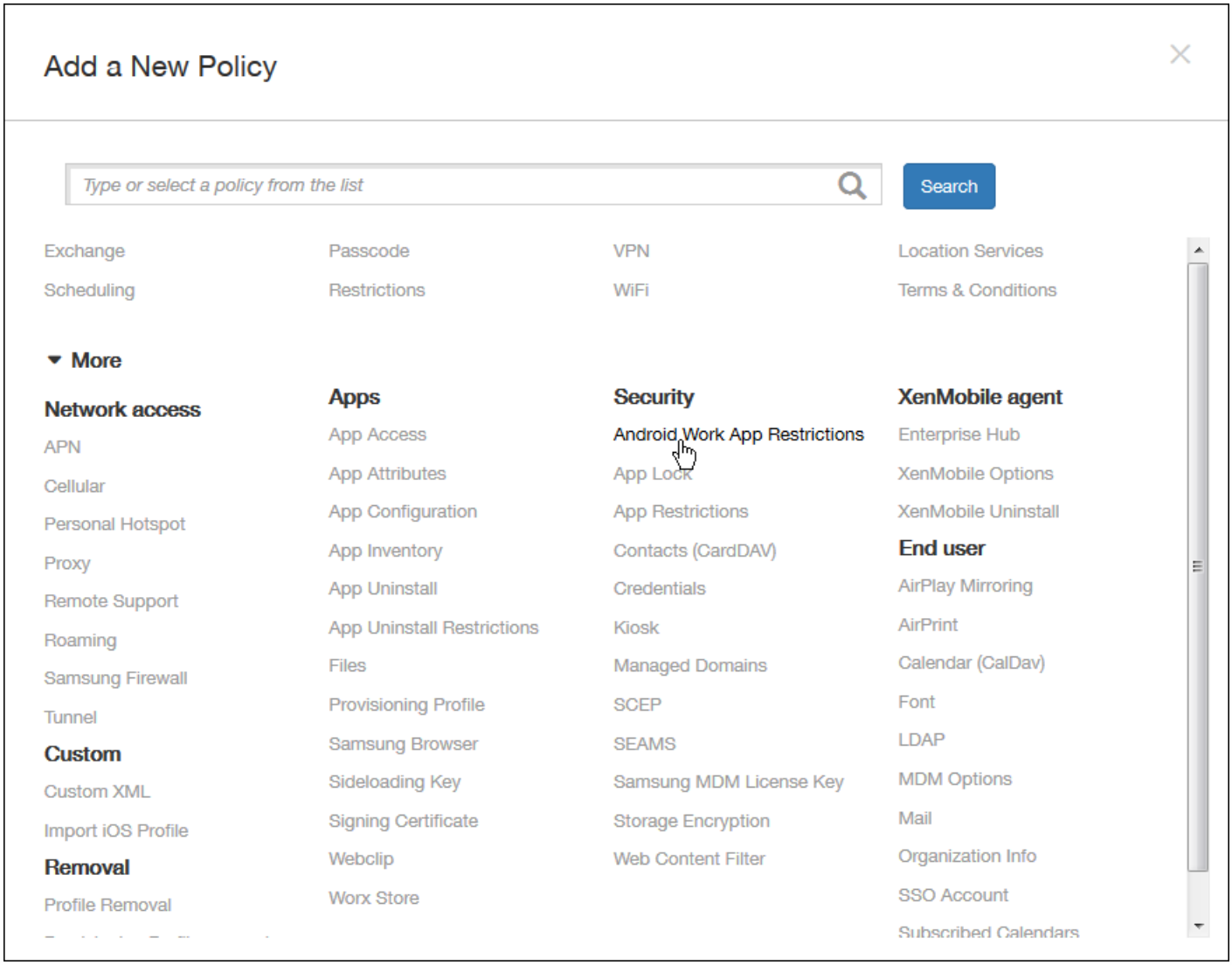
- Effectuer les tâches de configuration d'Android for Work sur Google. Pour de plus amples informations, consultez la section Gestion d'appareils avec Android for Work.
- Créer des informations d'identification Google Play. Pour de plus amples informations, consultez la section Informations d'identification Google Play.
- Configurer les paramètres de compte Android for Work. Pour de plus amples informations, consultez la section Configurer les paramètres de 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.



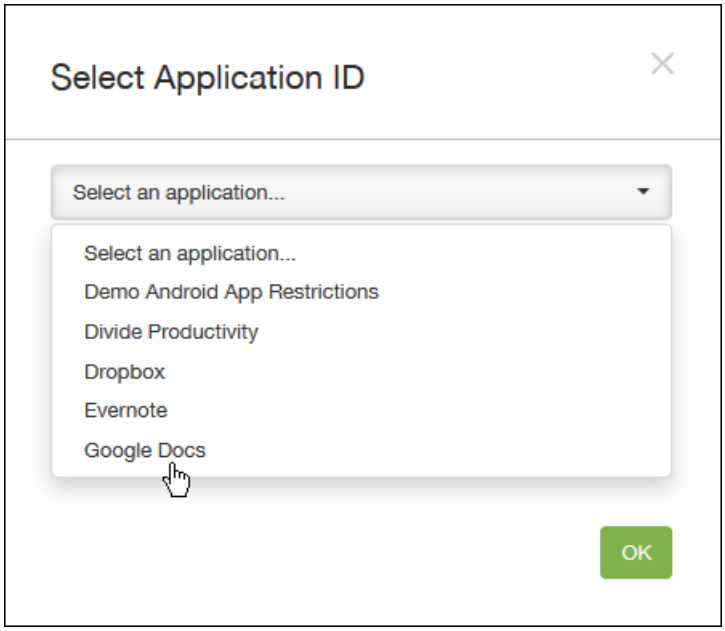
2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La page **Ajouter une nouvelle stratégie** apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



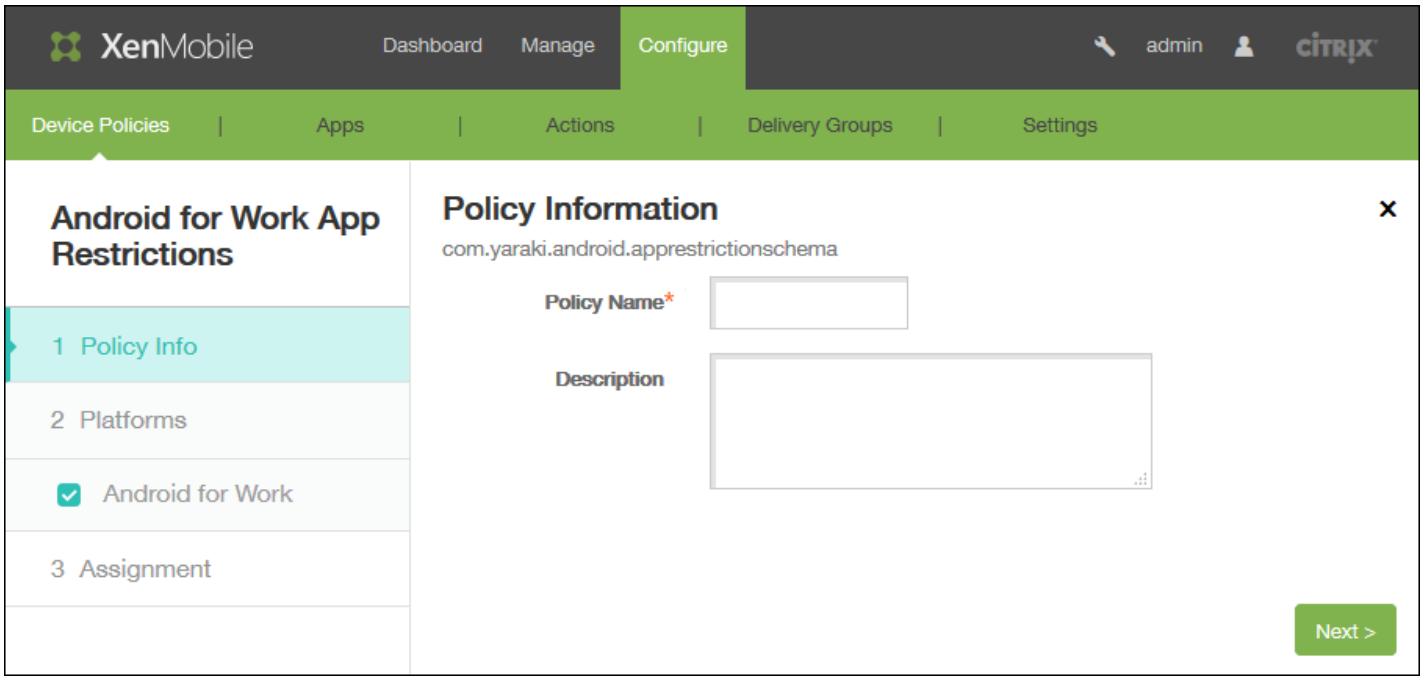
3. Sur la page **Ajouter une nouvelle stratégie**, cliquez sur **Plus** puis sous **Sécurité**, cliquez sur **Restrictions applicatives Android for Work**. Une boîte de dialogue s'affiche, vous invitant à sélectionner une application.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



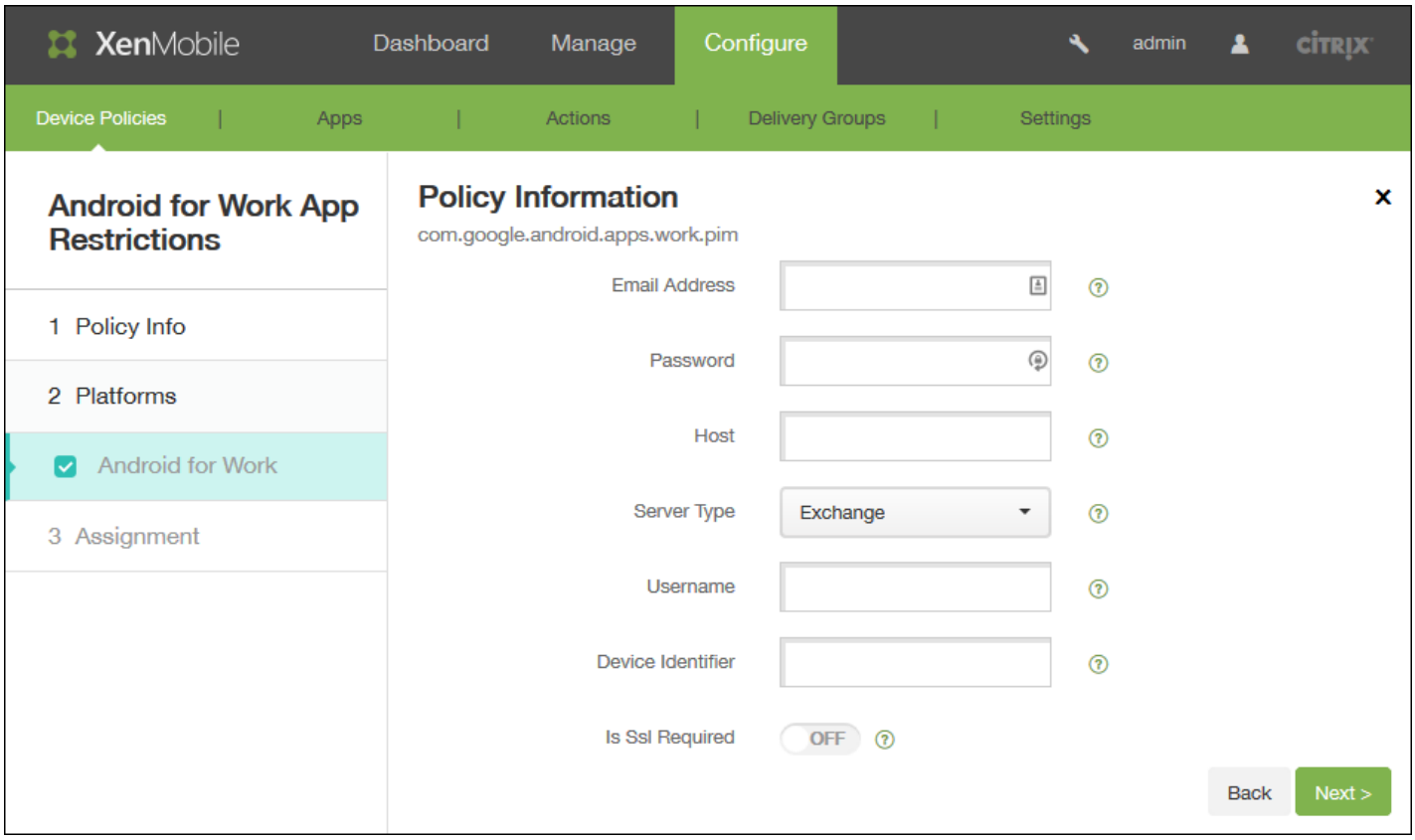
5. Dans la section **Informations sur la stratégie**, entrez les informations suivantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Nom de la stratégie** : entrez un nom descriptif pour la stratégie.
- **Description** : entrez une description pour la stratégie (facultatif).

6. Cliquez sur **Suivant**. La page **Stratégie par plate-forme** s'affiche.

7. Sous **Plates-formes**, dans la section d'informations sur la stratégie **Android for Work**, configurez les paramètres de l'application que vous avez sélectionnée. Les paramètres que vous voyez dépendent des restrictions associées à l'application sélectionnée. La figure suivante présente certaines des options disponibles pour l'application Google Docs.



8. Développez **Règles de déploiement** et configurez les paramètres suivants :

L'onglet **Base** s'affiche par défaut.



- Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.

  i. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est

© 1999-2017 Citrix Systems, Inc. All rights reserved.

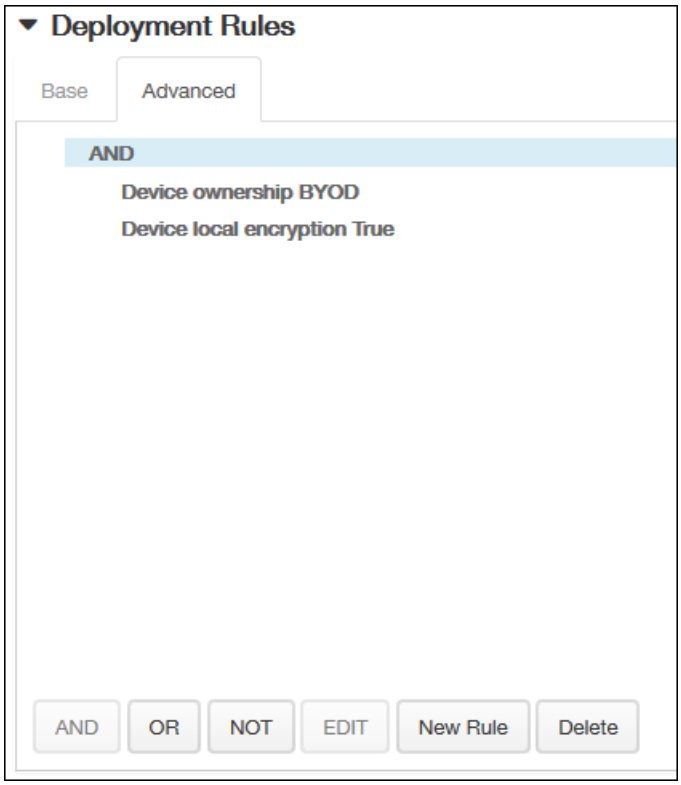
remplie. L'option par défaut est **Toutes**.

ii. Cliquez sur **Nouvelle règle** pour définir les conditions.

iii. Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**, comme illustré dans la figure qui précède.

iv. Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

- Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes.



Les conditions que vous avez choisies sur l'onglet Base s'affichent.

- Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.

i. Cliquez sur **ET**, **OU** ou **SAUF**.

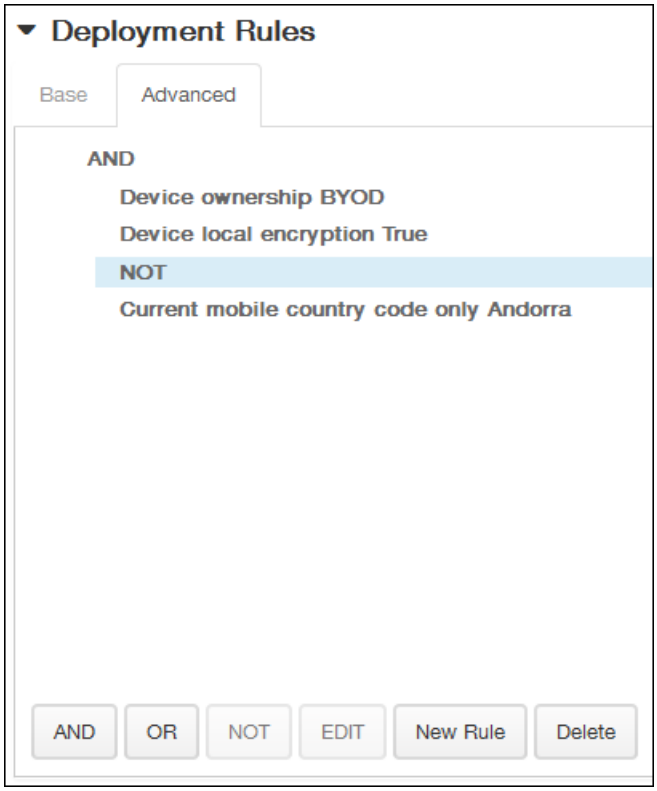
ii. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.

Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.

iii. Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions.

Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

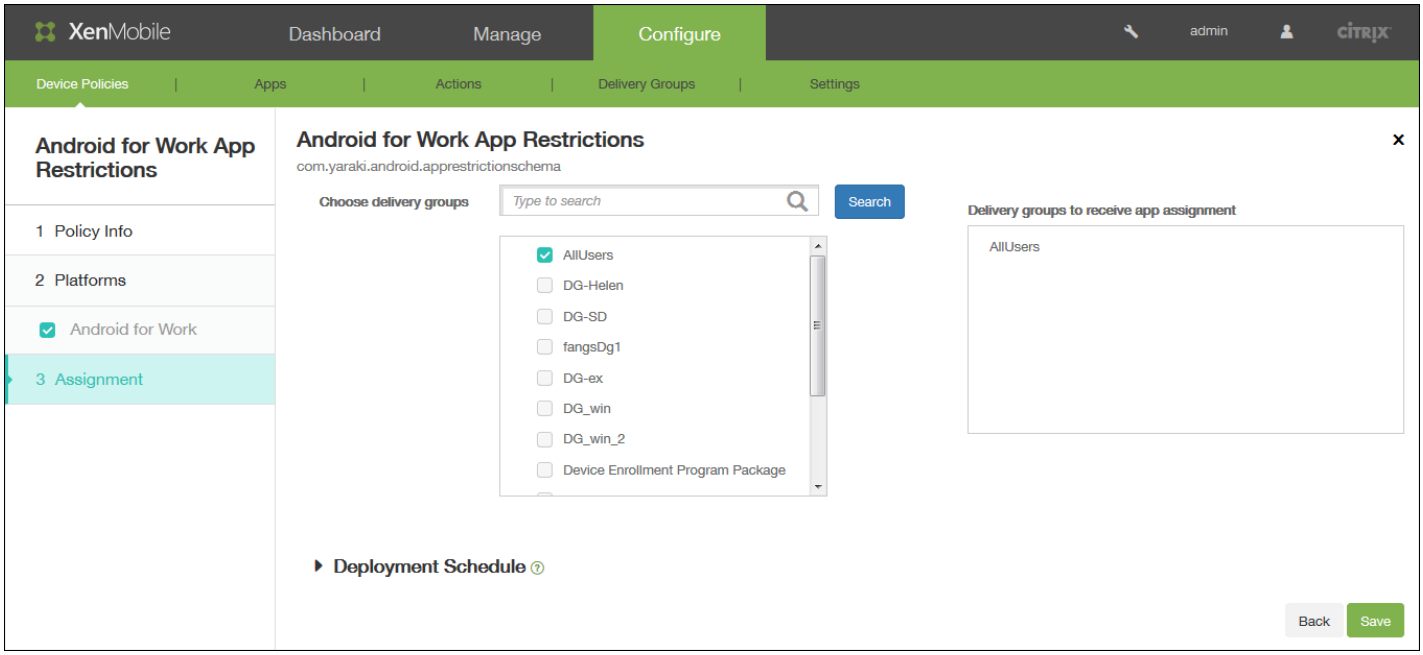


9. Cliquez sur **Suivant**.

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**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Veuillez noter que 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration des règles de déploiement

Jul 25, 2016

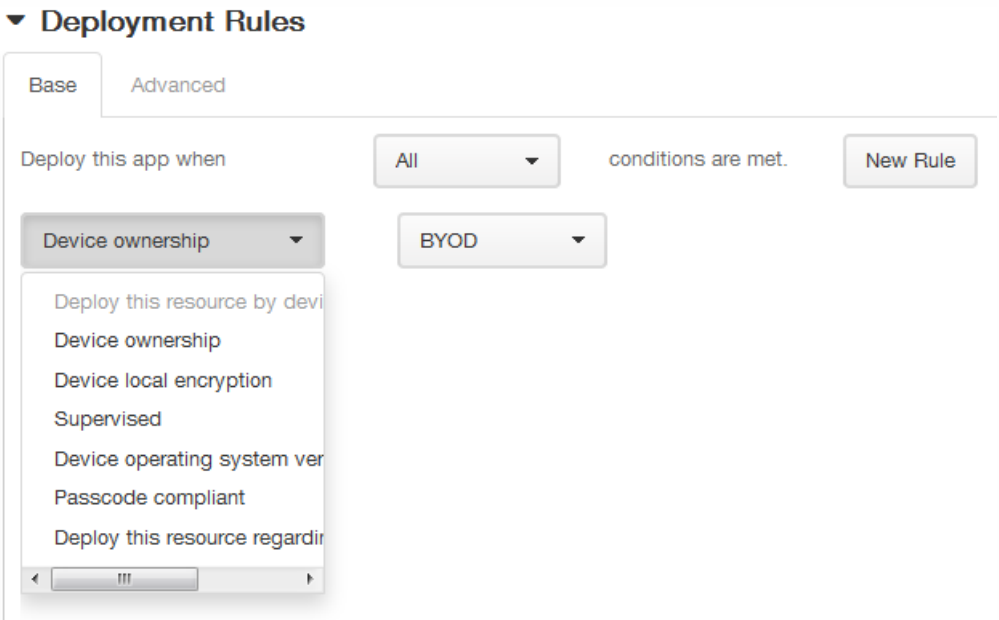
Cette section décrit :

- Les règles de déploiement : paramètres qui affectent le déploiement d'un paquetage.
- Les calendriers de déploiement : options qui spécifient quand XenMobile transmet les paquetages à un appareil.

Configuration des règles de déploiement

Les règles de déploiement sont des paramètres qui affectent le résultat du déploiement d'un paquetage. Vous pouvez spécifier des règles de déploiement pour des propriétés d'appareil, des applications et des actions. 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 afin de déterminer l'ordre de déploiement d'un paquetage. Pour de plus amples informations, consultez la section Ordre de déploiement.

Vous pouvez baser le déploiement d'un paquetage sur une version spécifique d'un système d'exploitation, sur une plate-forme matérielle particulière, ou une autre combinaison. Dans cet assistant utilisé pour ajouter et modifier les propriétés d'appareil, les applications et les actions sont un éditeur de règles de base et avancé. Le mode Avancé est un éditeur à format libre. L'image ci-dessous illustre l'écran Règles de déploiement accessible lors de l'ajout ou de la modification d'une application :



Règles de déploiement de base

Les règles de déploiement de base comprennent des tests prédéfinis et les actions résultantes. Lorsque cela est possible, les résultats sont préconfigurés dans des tests exemples. Par exemple, lorsque vous basez un déploiement de paquetage sur une plate-forme matérielle, toutes les plates-formes connues existantes sont entrées dans un test résultant, réduisant de manière drastique la durée de création de vos règles, et limitant les erreurs possibles.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cliquez sur **Nouvelle règle** pour ajouter une règle au paquetage.

Remarque : le créateur de règles contient davantage d'informations, spécifiques à chaque test.

Pour créer une nouvelle règle, sélectionnez un modèle de règle, sélectionnez le type de condition, puis personnalisez la règle. La personnalisation de la règle inclut la modification de la description. Lorsque vous avez terminé les paramètres de configuration, vous devez ajouter la règle pour le paquetage.

Vous pouvez ajouter autant de règles que vous voulez. Le paquetage est déployé lorsque toutes les règles correspondent.

Règles de déploiement avancées

Si vous cliquez sur l'onglet **Avancé**, l'**Éditeur des règles avancées** s'affiche.

Dans ce mode, vous pouvez spécifier la relation définie entre les règles. Les opérateurs **AND**, **OR** et **NOT** sont disponibles.

Configuration de calendriers 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 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.

Si vous ne modifiez pas les options de planification du déploiement, les déploiements se produisent immédiatement sur chaque connexion. Les options de planification du déploiement sont les suivantes :

Déployer: la valeur par défaut est **ON**. Pour empêcher le déploiement, modifiez ce paramètre sur **OFF**.

Calendrier de déploiement : la valeur par défaut est **Maintenant**. Pour spécifier une date de déploiement, sélectionnez **Plus tard**, puis choisissez une date et une heure.

Conditions de déploiement : la valeur par défaut est **À chaque connexion**. Pour limiter les déploiements, modifiez ce paramètre sur **Uniquement lorsque le déploiement précédent a échoué**.

Déployer pour les connexions permanentes : la valeur par défaut est **OFF**. Pour les appareils iOS et Windows Mobile : si vous définissez l'option **Stratégie de planification de connexion** sur **Toujours**, vous devez changer **Déployer pour les connexions permanentes** sur **ON**. Pour les appareils Android : la propriété de serveur XenMobile, **Déploiement en arrière-plan**, nécessite que vous définissiez **Déployer pour les connexions permanentes** sur **ON** pour chaque stratégie déployée sur des appareils Android.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

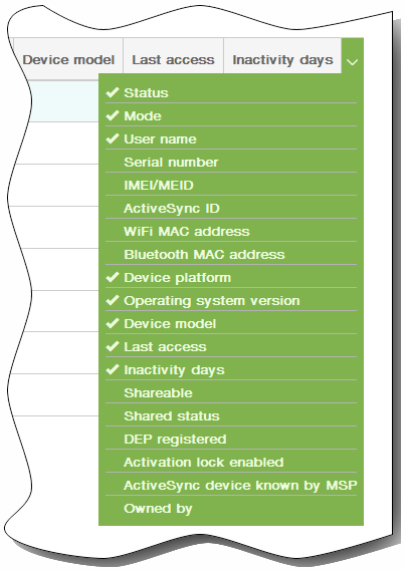
Ajout d'appareils et affichage des détails des appareils

Jul 25, 2016

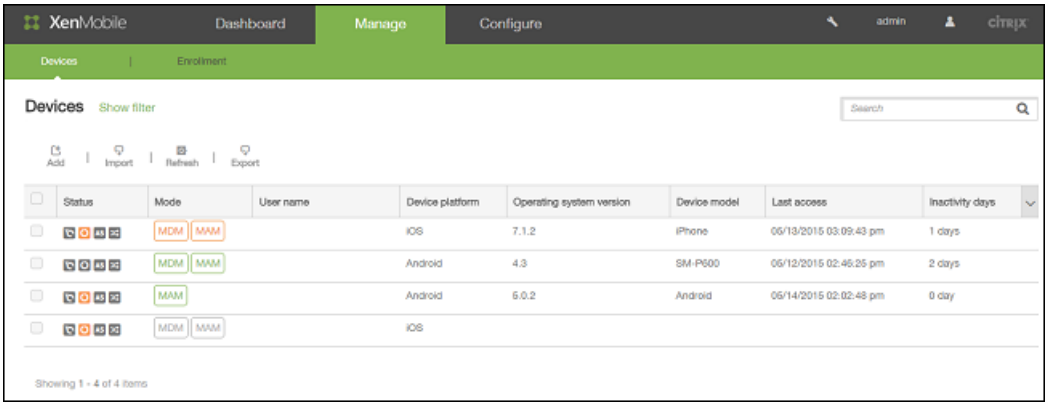
La base de données de référentiel du serveur de la console XenMobile stocke une liste des appareils mobiles. Chaque appareil mobile est défini par un numéro de série unique et/ou un numéro IMEI (identité internationale d'équipement mobile)/MEID (identifiant de l'équipement mobile). Pour renseigner la console XenMobile avec vos appareils, vous pouvez ajouter les appareils manuellement ou importer une liste d'appareils à partir d'un fichier. Voir Formats des fichiers de provisioning.

Sur la page Appareils dans la console, vous trouverez un tableau répertoriant tous les appareils, avec les informations suivantes : État (appareil non débloqué, appareil non géré, Active Sync Gateway indisponible, pas d'échec du déploiement), Mode, (MDM, MAM), Nom d'utilisateur, Plate-forme de l'appareil, Version du système d'exploitation, Modèle d'appareil, Dernier accès et Jours d'inactivité.

Remarque : les en-têtes précédents sont les valeurs par défaut. Vous pouvez personnaliser les éléments affichés dans le tableau en cliquant sur la flèche vers le bas sur le dernier en-tête, puis en cliquant parmi les nombreux en-têtes possibles sur ceux que vous voulez voir dans le tableau ou en supprimant ceux que vous ne souhaitez pas voir.



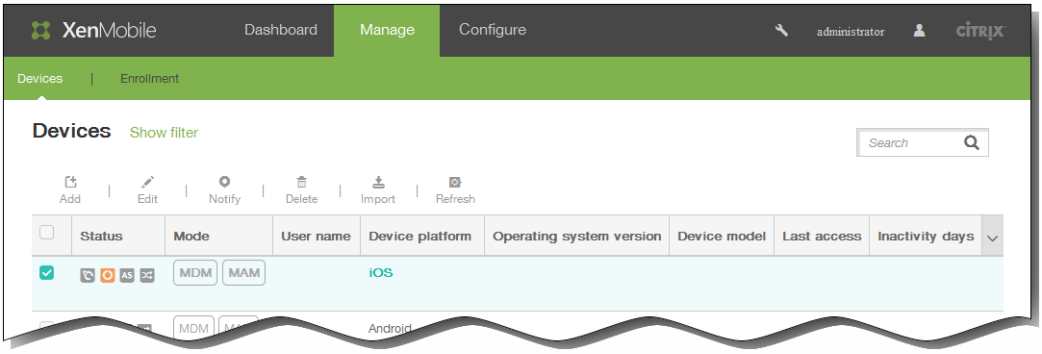
Vous pouvez ajouter un nouvel appareil manuellement en cliquant sur Ajouter, ou vous pouvez importer un fichier de provisioning en cliquant sur Importer. Pour mettre à jour le tableau, cliquez sur Actualiser.



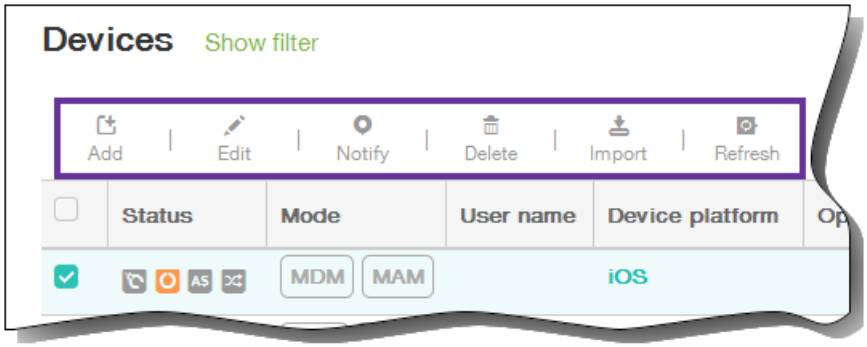
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter des appareils manuellement.

1. Dans la console XenMobile, cliquez sur Gérer > Appareils et cliquez sur Ajouter. La page Ajouter un appareil s'affiche.
2. Dans Sélectionner une plate-forme, cliquez sur iOS, Android ou Symbian.
3. Entrez les informations suivantes :
   1. iOS : entrez le numéro de série.
   2. Android : entrez le numéro de série et le numéro IMEI/MEID.
   3. Symbian : entrez le numéro IMEI/MEID.
4. Cliquez sur Ajouter. Le tableau Appareils s'affiche avec l'appareil ajouté en bas de la liste.
5. 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.

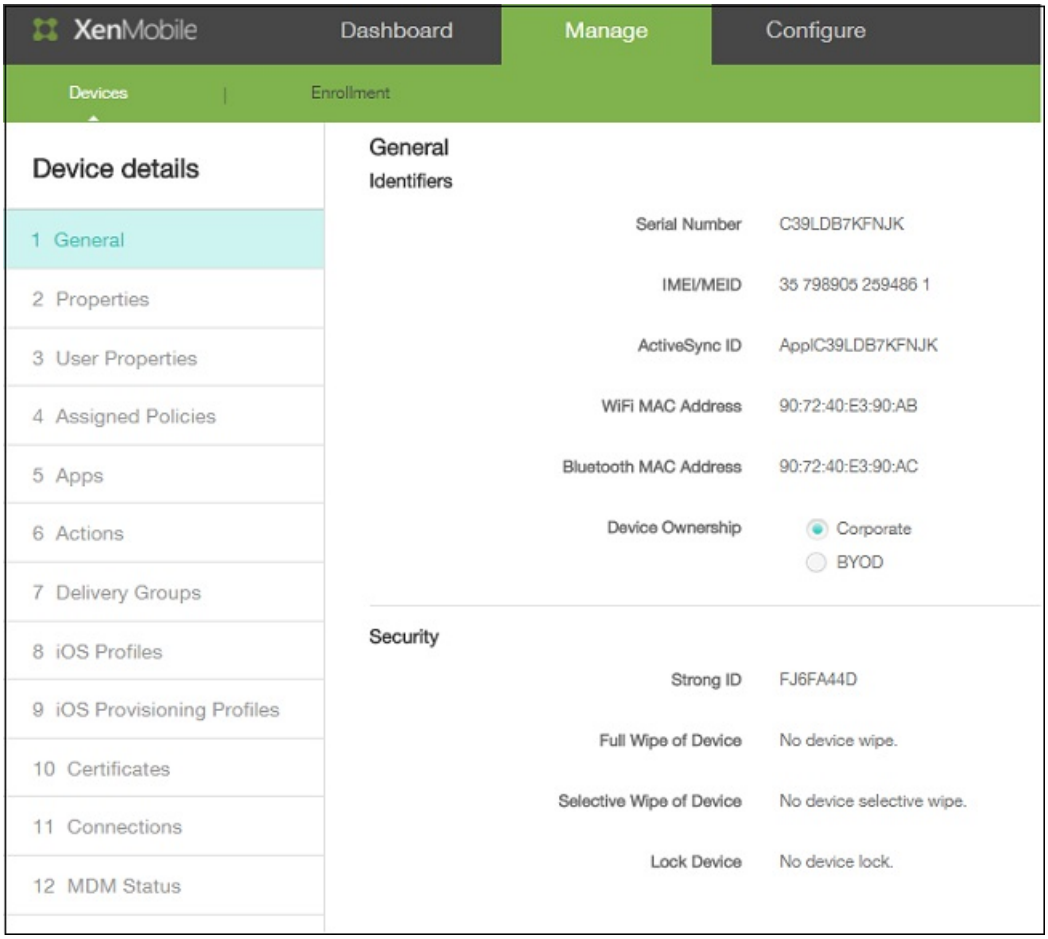


Remarque : lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



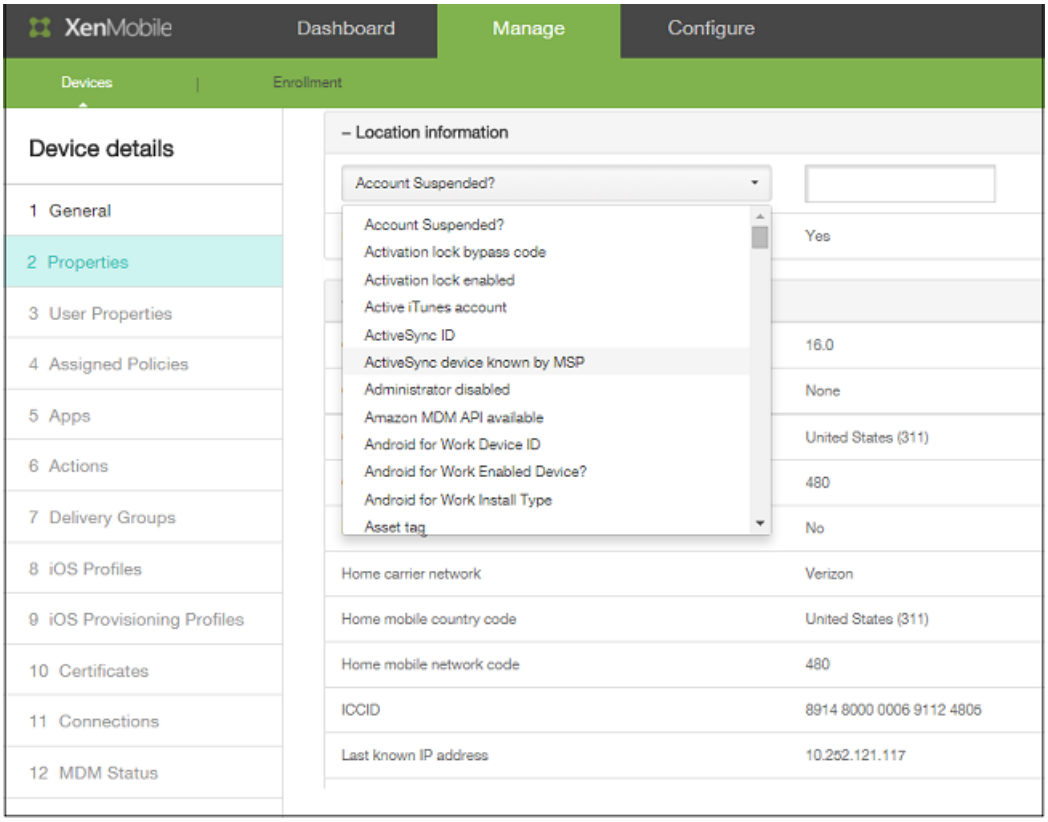
6. Sous Général : identificateurs, confirmez les informations affichées (la liste de paramètres varie en fonction du type de plate-forme) : numéro de série, IMEI/MEID, ID ActiveSync, adresse MAC Wi-Fi, adresse MAC Bluetooth, Propriétaire : entreprise ou BYOD.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



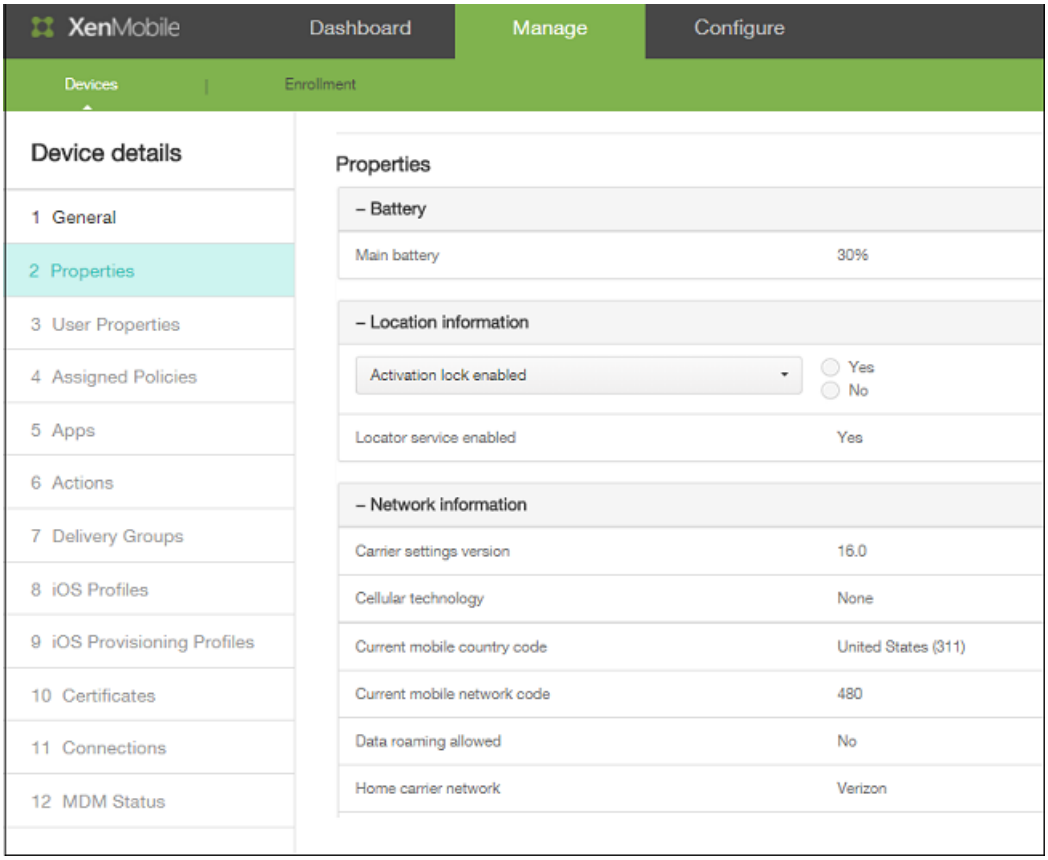
7. Sous Sécurité, confirmez les informations qui s'affichent (la liste de paramètres varie en fonction du type de plate-forme) : identifiant fort, effacement complet de l'appareil, effacer les données d'entreprise d'un appareil, verrouiller l'appareil, déverrouiller l'appareil, exclusion de l'appareil, contourner le verrouillage d'activation, effacer les restrictions sur l'appareil.
8. Cliquez sur Suivant pour ajouter des propriétés.
9. Sur la page Propriétés, cliquez sur Ajouter pour afficher une liste des propriétés que vous pouvez provisionner pour l'appareil. Une liste des propriétés disponibles s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



10. Dans la liste, cliquez sur la propriété à provisionner et définissez sa valeur. Par exemple, vous pouvez sélectionner la propriété Verrouillage d'activation activé et définir la valeur sur Oui ou Non.
11. Une fois la configuration d'une propriété terminée, cliquez sur Terminé.
12. Répétez les étapes 9 à 11 pour chaque propriété que vous souhaitez provisionner et cliquez sur Suivant.
    Remarque : lorsque vous ajoutez des propriétés, elles sont répertoriées sous Propriétés. Lorsque vous revenez sur la page propriétés ultérieurement, les propriétés sont séparées dans différentes catégories.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



La section **Stratégies attribuées** et les sections suivantes contiennent toutes des informations récapitulatives sur l'appareil.

- Stratégies attribuées : affiche le nombre des stratégies attribuées, y compris le nombre de stratégies déployées, en attente ou ayant échoué. Les informations relatives au nom, au type et à la dernière date de déploiement s'affichent également pour chaque stratégie.
- Applications : affiche le nombre d'applications lors du dernier inventaire, ce qui comprend le nombre d'applications installées, en attente et ayant échoué.
  - Pour Installé, les informations suivantes s'affichent : nom, propriétaire, version, auteur, taille, installé, identifiant et type.
  - Pour les applications En attente et Échec, les informations suivantes s'affichent : nom, dernier déploiement, identifiant et type.
- Actions : affiche le nombre d'actions, ce qui comprend le nombre d'actions déployées, en attente et qui ont échoué. Chaque action affiche le nom du déploiement et la date à laquelle il a été déployé pour la dernière fois.
- Groupes de mise à disposition : affiche le nombre de groupes de mise à disposition ayant réussi, en attente et qui ont échoué. Les groupes de mise à disposition et des informations sur l'heure s'affichent pour chaque action. En outre, des informations plus détaillées s'affichent pour le groupe de mise à disposition, comprenant notamment l'état, le propriétaire et la date de l'action.
- Profils iOS (appareils iOS uniquement) : affiche le dernier inventaire de profil iOS et comprend notamment le nom, le type, l'organisation et une description.
- Certificats : affiche le nombre de certificats valides et de certificats révoqués ou ayant expiré, y compris le type, le fournisseur, l'émetteur, le numéro de série et la date de validité.
- Connexions : affiche l'état de la première connexion et de la dernière connexion. Pour chaque connexion, le nom d'utilisateur, l'avant-dernière authentification et la dernière authentification s'affichent.
- TouchDown (appareils Android uniquement) : affiche la dernière authentification de l'appareil et le dernier utilisateur à s'être authentifié. Chaque nom de stratégie et valeur de stratégie applicables s'affiche.

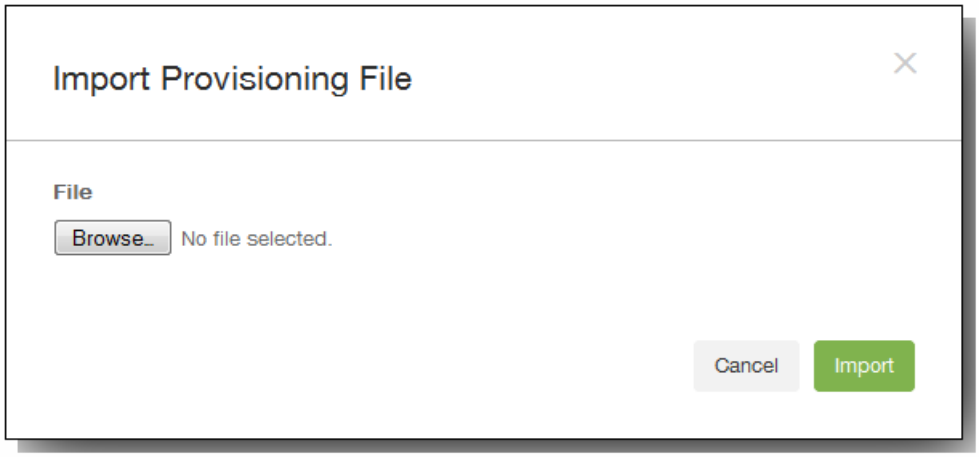
© 1999-2017 Citrix Systems, Inc. All rights reserved.

13. Cliquez sur Enregistrer.

Pour 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. Voir Formats des fichiers de provisioning.

1. Dans le menu au-dessus du tableau Appareils, cliquez sur Importer. La boîte de dialogue Importer le fichier de provisioning apparaît.

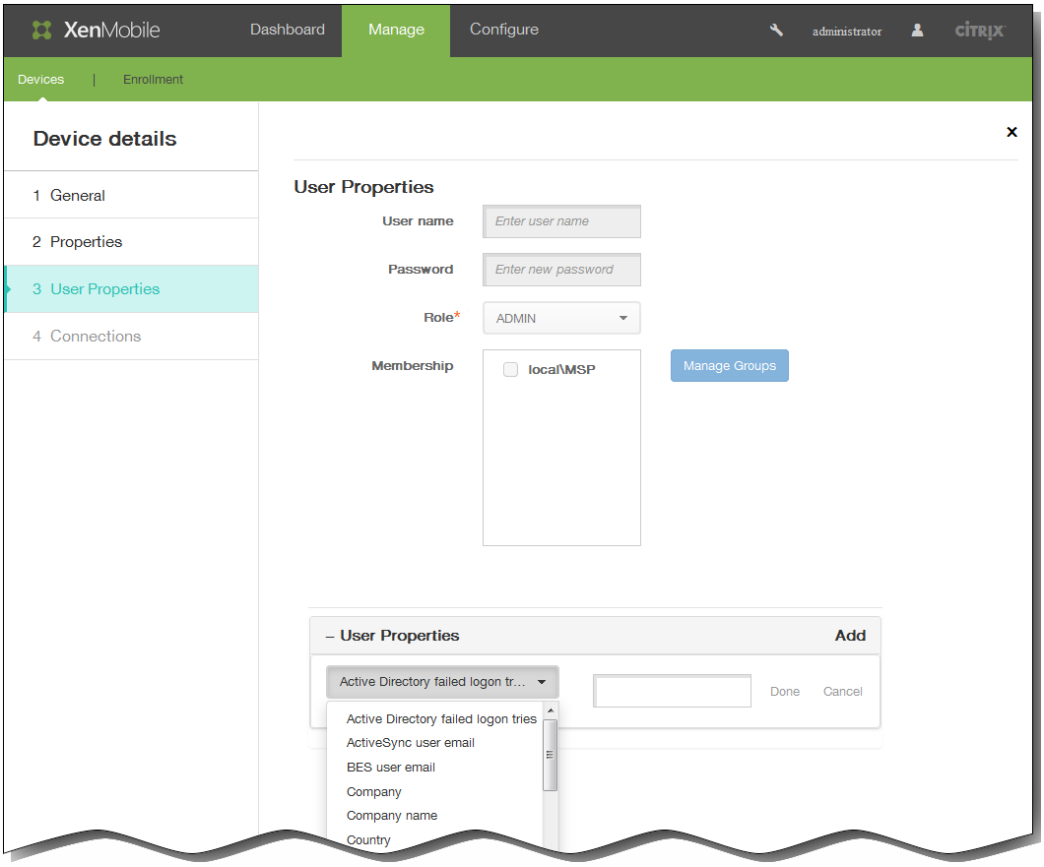


2. Sélectionnez le fichier à importer en cliquant sur Parcourir et accédez à l'emplacement du fichier.
3. Cliquez sur Importer. Les fichiers importés sont ajoutés au tableau Appareils.

Pour modifier des appareils

1. Sélectionnez l'appareil à modifier et cliquez sur Modifier. La page Détails de l'appareil s'affiche.
2. Sous Général : identifiants, le seul champ que vous pouvez modifier est Propriétaire, que vous pouvez définir sur Entreprise ou BYOD.
3. Cliquez sur Suivant. La page Propriétés s'affiche.
4. Sur la page Propriétés, ajoutez, modifiez ou supprimez des propriétés suivant vos besoins.
   - Pour modifier une propriété, cliquez sur la propriété, modifiez ses paramètres, puis cliquez sur Terminé ou Annuler.
   - Pour supprimer une propriété, placez le curseur sur la liste et cliquez sur le X sur le côté droit. L'élément est supprimé immédiatement.
5. Cliquez sur Suivant. La page qui s'affiche ensuite dépend de l'appareil sélectionné. Pour certains appareils, la page Propriétés utilisateur s'affichera, et pour d'autres, c'est la page Propriétés attribuées qui s'affichera.
6. Si la page Propriétés utilisateur s'affiche, ajoutez, modifiez ou supprimez des propriétés utilisateur comme suit ; sinon, les pages restantes contiennent des informations récapitulatives sur l'appareil. Pour obtenir une description détaillée de ces pages, reportez-vous à Pour ajouter des appareils manuellement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Remarque : la partie supérieure de la page Propriétés utilisateur ne peut pas être modifiée.

- Pour ajouter une propriété utilisateur, cliquez sur Ajouter.
  - Dans la liste, cliquez sur la propriété que vous voulez ajouter, entrez la valeur pour la propriété, puis cliquez sur Terminé ou Annuler. Répétez cette étape pour chaque propriété à ajouter.
- Pour modifier une propriété, cliquez sur la propriété, modifiez ses paramètres, puis cliquez sur Terminé ou Annuler.
- Pour supprimer une propriété, placez le curseur sur la liste et cliquez sur le X sur le côté droit. L'élément est supprimé immédiatement.

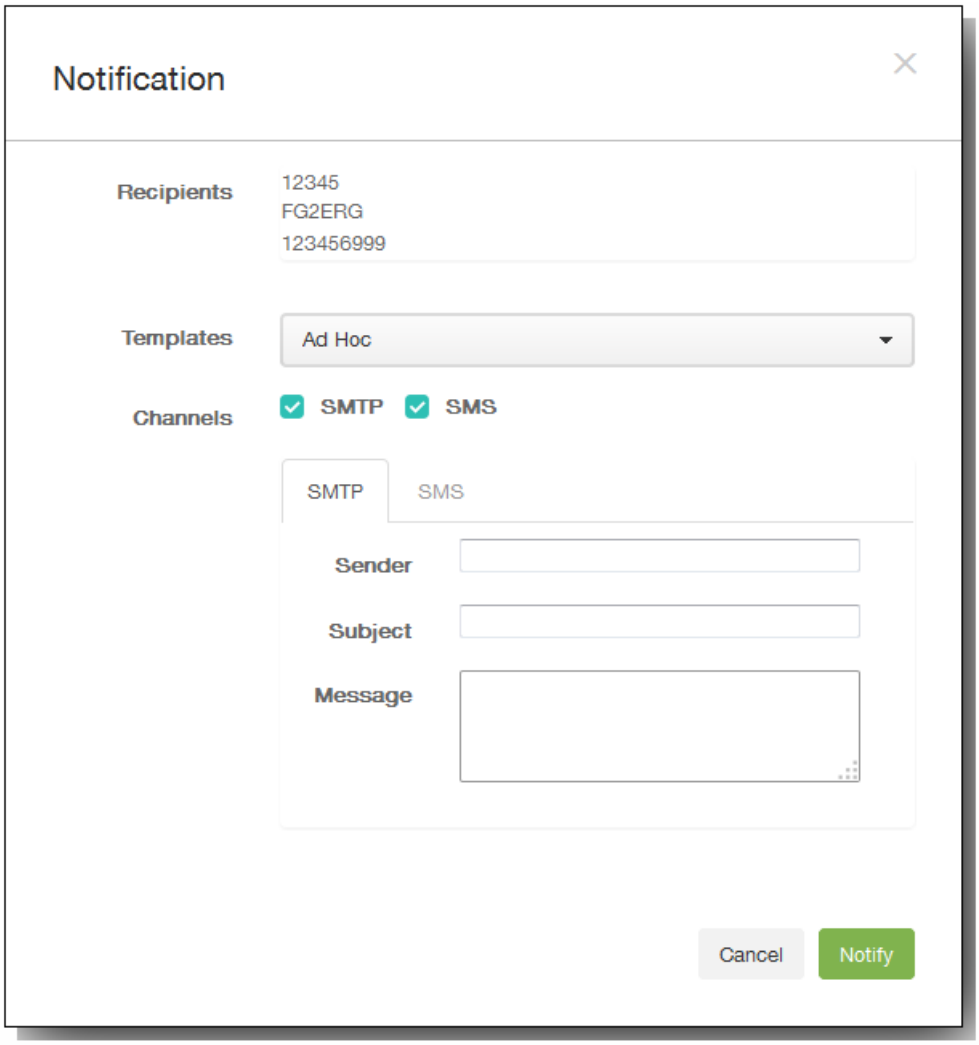
7. Cliquez sur Suivant sur chacune des pages suivantes pour afficher des informations de synthèse.
8. Sur la page finale, cliquez sur Enregistrer pour enregistrer les modifications sur l'appareil.

Pour envoyer une notification aux appareils

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour de plus amples informations sur les notifications, consultez la section Pour créer ou mettre à jour des modèles de notification dans XenMobile.

1. Sélectionnez l'appareil ou les appareils auxquels vous souhaitez envoyer une notification.
2. Cliquez sur Notifier. La boîte de dialogue Notification s'affiche. Destinataires répertorie tous les appareils sélectionnés pour recevoir pour la notification.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Renseignez les informations suivantes :
   1. Modèles : dans la liste, cliquez sur le type de notification que vous souhaitez envoyer.
      Les champs Sujet et Message sont renseignés avec le texte configuré pour le modèle que vous avez choisi, sauf pour le modèle Ad Hoc.
   2. Canaux : sélectionnez la méthode à utiliser pour envoyer le message. La valeur par défaut est SMTP
      — et
      SMS.
      Vous pouvez cliquer sur les onglets SMTP et SMS pour afficher le format du message pour chaque option.
   3. Expéditeur : entrez un expéditeur (facultatif).
   4. Sujet : entrez un sujet pour un message ad hoc.
   5. Message : entrez le message pour un message ad hoc.
4. Cliquez sur Notifier.

Pour 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.
   Important : vous ne pouvez pas annuler cette opération.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

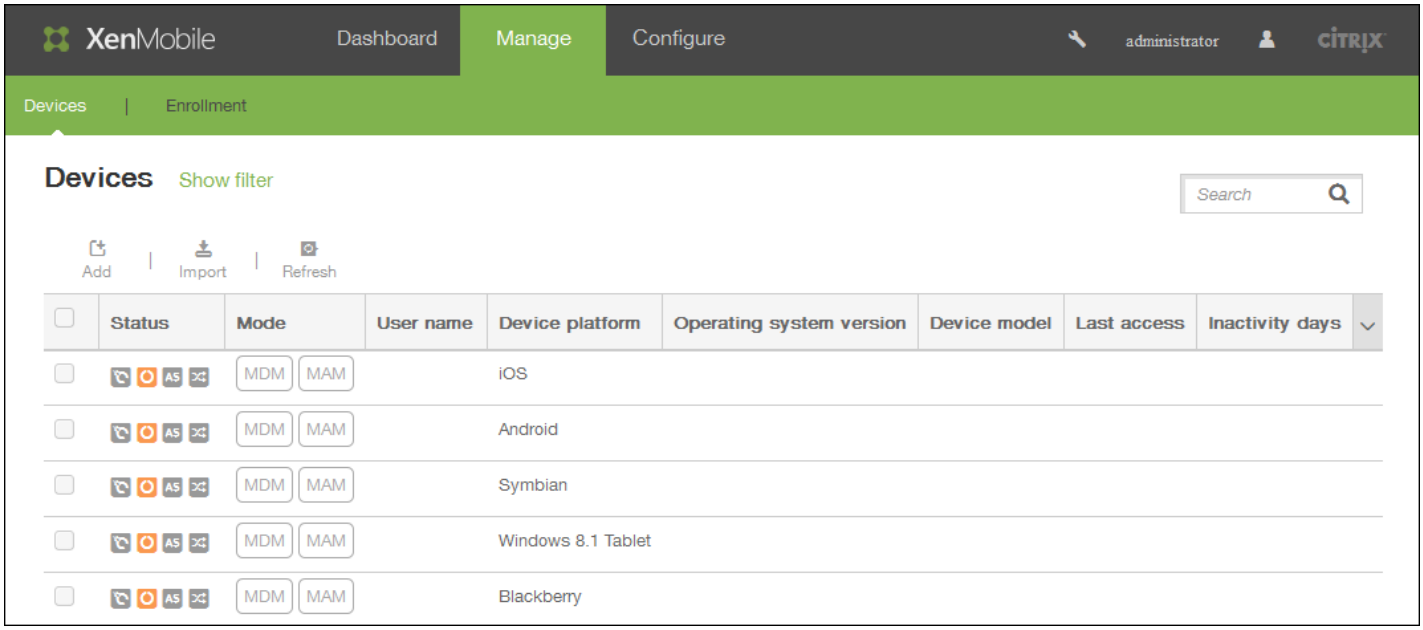
Pour verrouiller un appareil iOS

Jul 25, 2016

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 iOS 7 et 8.

Si vous choisissez d'inclure un message et un numéro de téléphone sur l'écran de verrouillage, le message et le numéro de téléphone ne s'affichent sur un appareil verrouillé que si vous avez également défini la stratégie Code secret dans la console XenMobile, ou si les utilisateurs ont activé le code secret manuellement sur l'appareil.

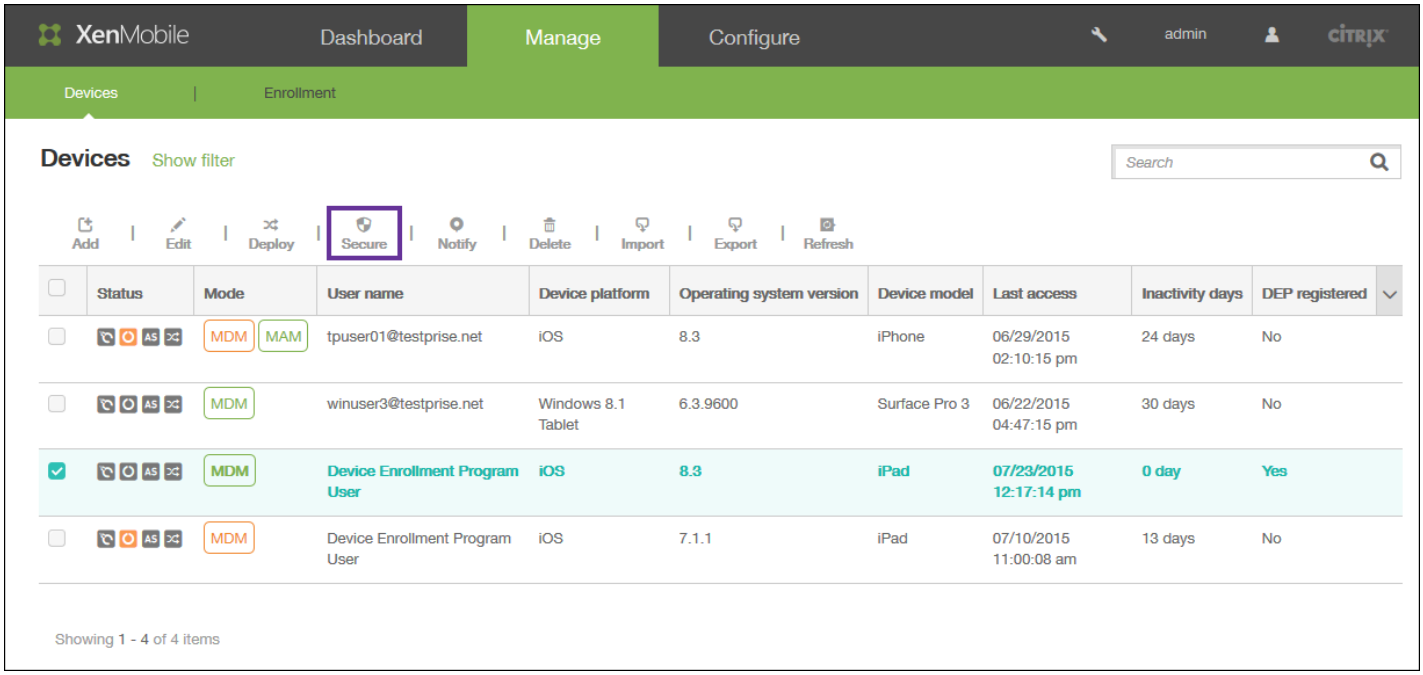
Dans la console XenMobile, cliquez sur **Gérer > Appareils**. La page **Appareils** s'ouvre.

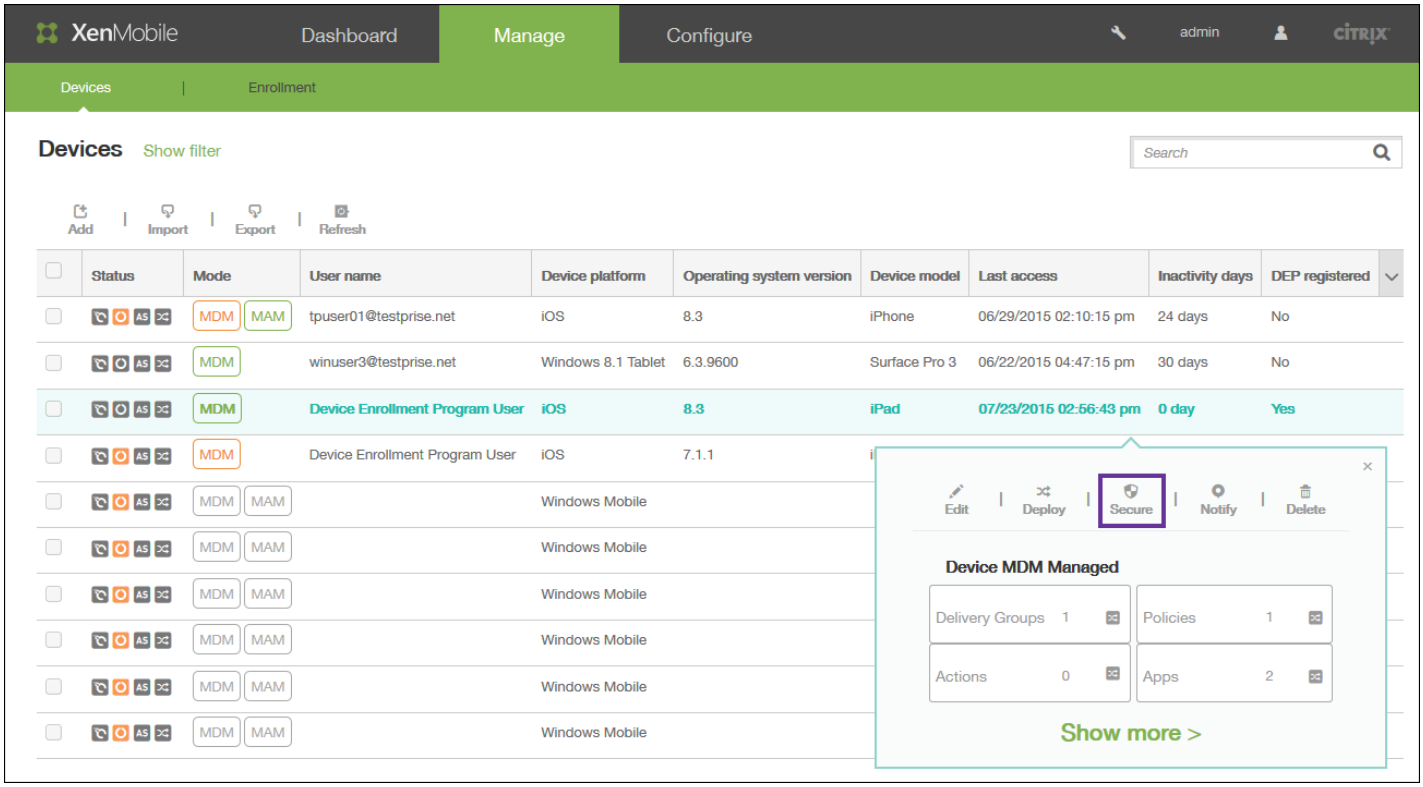


2. Sélectionnez l'appareil iOS que vous voulez verrouiller.

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 ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.

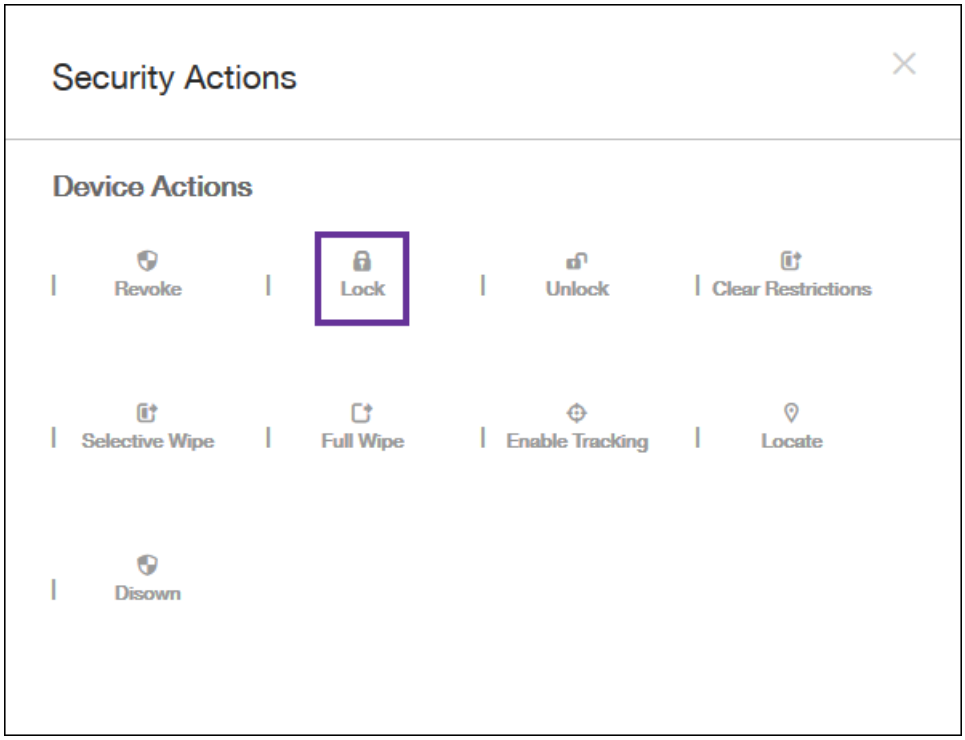
© 1999-2017 Citrix Systems, Inc. All rights reserved.



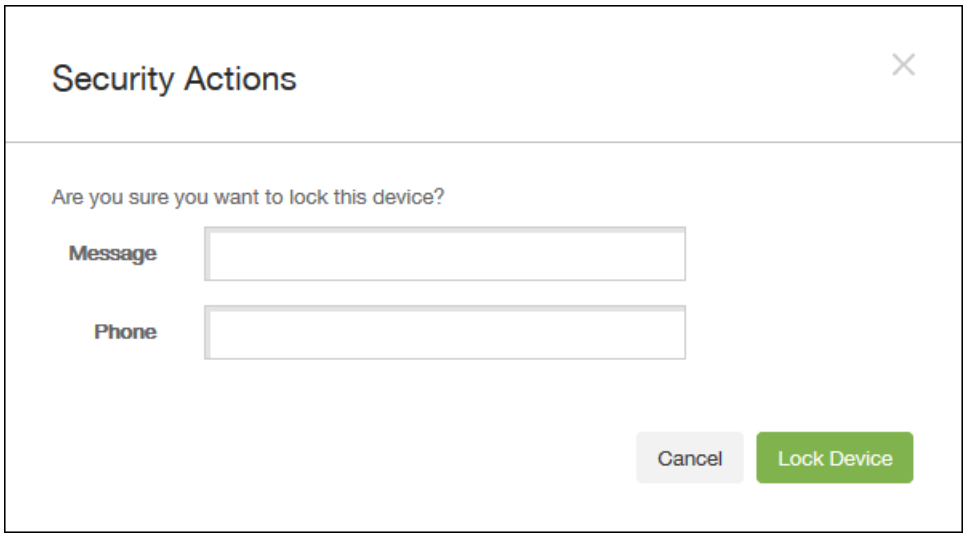


3. Dans le menu d'options, sélectionnez **Sécurité**. La boîte de dialogue **Actions de sécurisation** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Sélectionnez **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.

6. Cliquez sur **Verrouiller un appareil**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

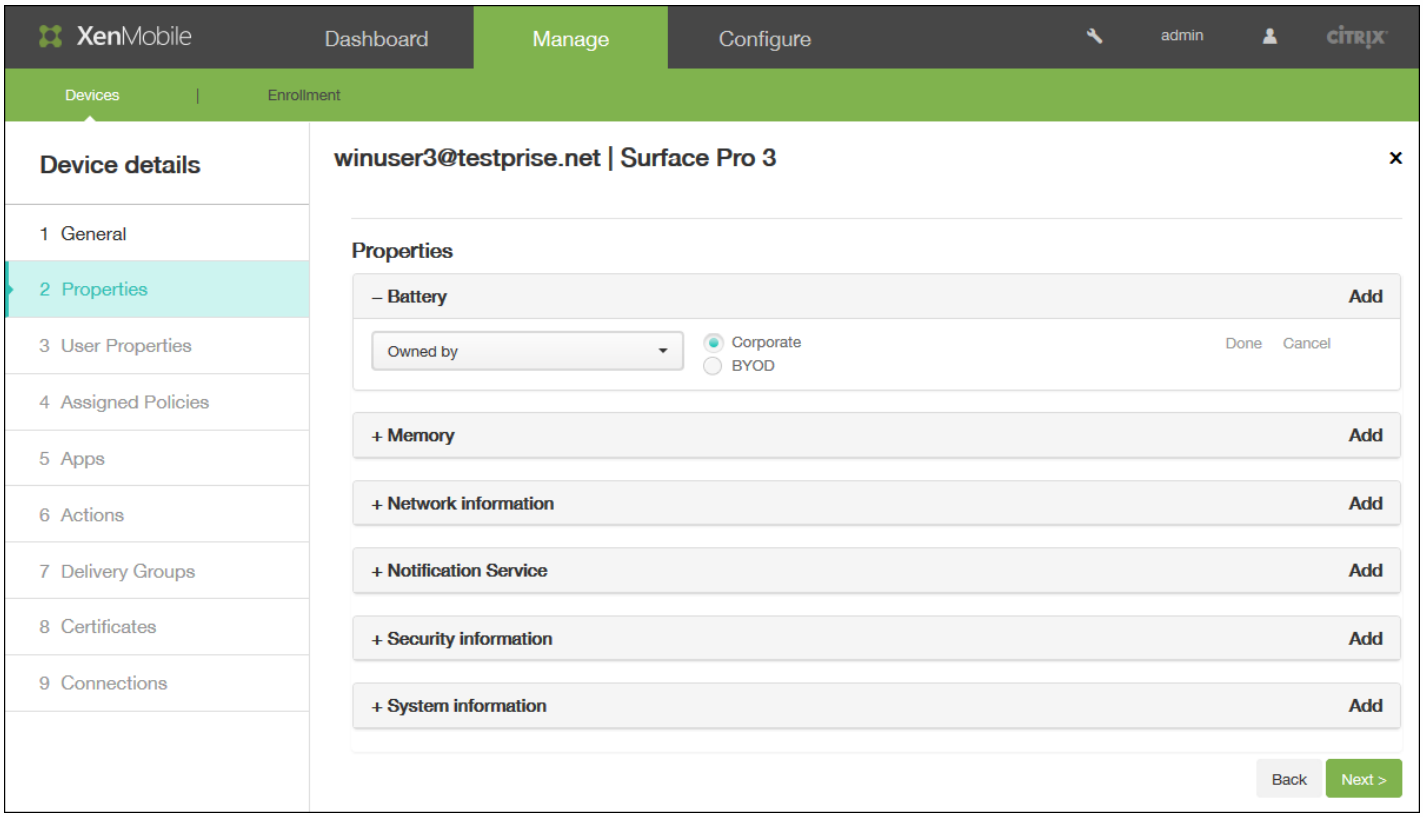
Identification manuelle des appareils utilisateur

Jul 25, 2016

Vous pouvez manuellement identifier un appareil dans XenMobile de l'une des trois manières suivantes :

- Identifier l'appareil pendant le processus d'inscription basé sur invitation.
- Identifier l'appareil durant processus d'inscription sur portail d'aide en libre-service.
- Identifier l'appareil 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).



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Formats des fichiers de provisioning

Jul 25, 2016

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

Remarque :

- Le jeu de caractères du fichier doit être au format UTF-8.
- 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 au format propertyV\;test\;1\;2 dans le fichier de provisioning.
- SerialNumber est requis si IMEI n'est pas spécifié.
- SerialNumber est requis pour les appareils iOS car le numéro de série est l'identifiant de l'appareil iOS.
- IMEI est requis si SerialNumber n'est pas spécifié.
- Les valeurs autorisées pour OperatingSystemFamily sont : WINDOWS, ANDROID ou iOS.

Exemple de fichier de provisioning d'appareil

Les lignes suivantes décrivent chacune un appareil dans un fichier de provisioning.

1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;

La première entrée signifie ce qui suit :

- SerialNumber : 1050BF3F5173010816100655105903 91
- IMEI : 15244201625379901
- OperatingSystemFamily : WINDOWS
- PropertyName : propertyN
- PropertyValue : propertyV\;test\;1\;2;prop 2

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Macros dans XenMobile

Jul 25, 2016

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies applicatives

Jul 25, 2016

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 appareils iOS, Android et Windows et même entre différents fournisseurs d'appareils exécutant Android.

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).

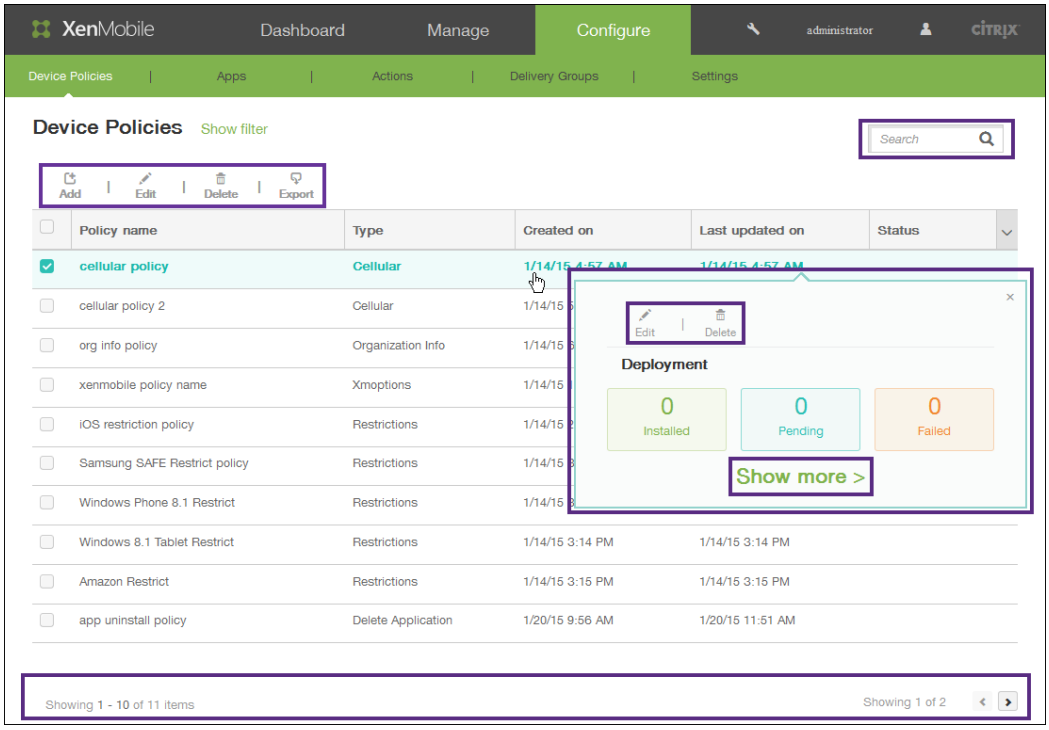
Page Stratégies d'appareil dans la console

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.

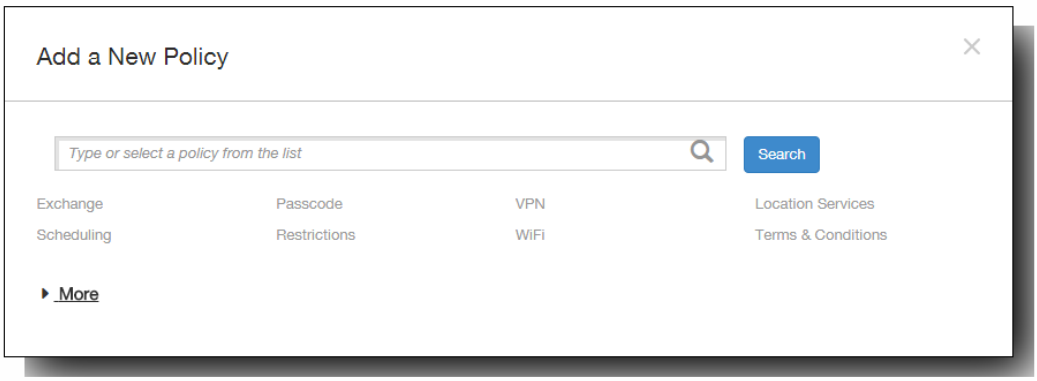
Pour modifier ou supprimer une stratégie sur la page Stratégies d'appareil, vous pouvez sélectionner la case à cocher en regard d'une stratégie pour afficher les options de menu au-dessus de la liste de stratégie, ou vous pouvez cliquer sur une stratégie dans la liste pour afficher le menu d'options sur le côté droit de la liste. Si vous cliquez sur Afficher plus, les détails de stratégie s'affichent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



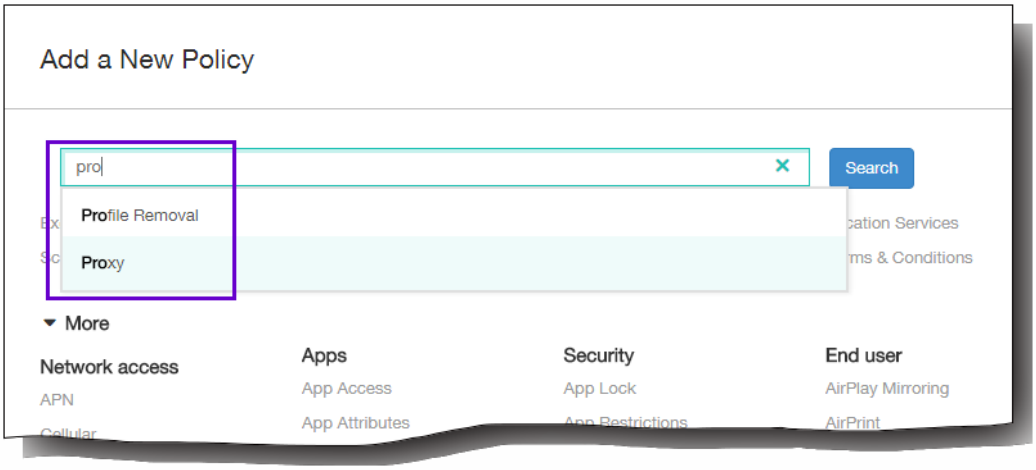
Pour ajouter une stratégie d'appareil

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.

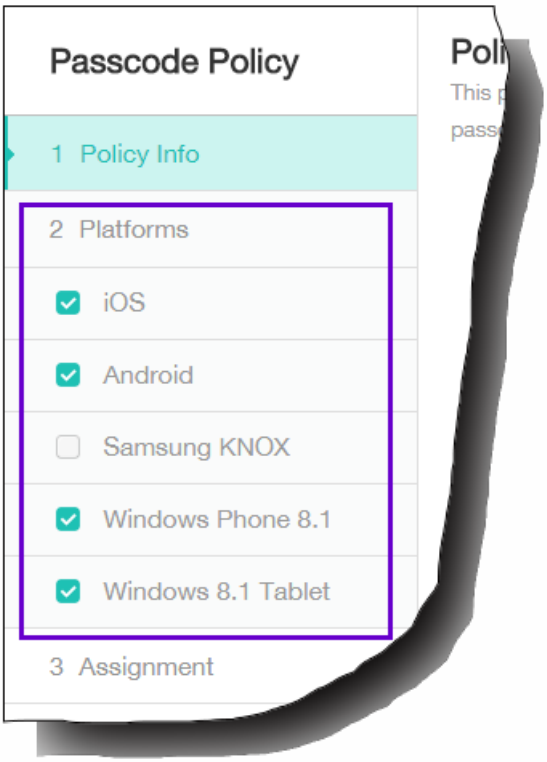


2. Pour trouver la stratégie que vous souhaitez ajouter, effectuez l'une des opérations suivantes :
   - Cliquez sur la stratégie.
     La page Informations sur la stratégie pour la stratégie sélectionnée s'affiche.
   - Entrez le nom de la stratégie dans le champ de recherche. À mesure que vous tapez, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



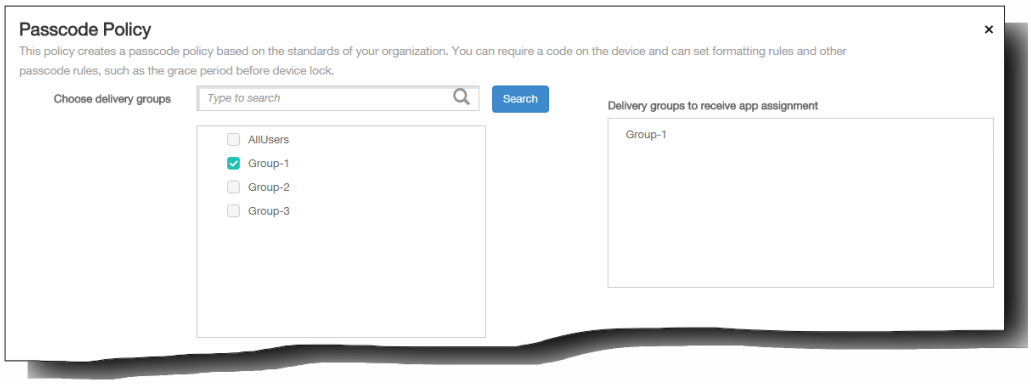
3. Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour les plates-formes sélectionnées s'affichent dans l'étape 5.
   Remarque : seules les plates-formes prises en charge par la stratégie sont répertoriées.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 des 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies XenMobile par plate-forme

Jul 25, 2016

Vous pouvez configurer des stratégies d'appareil dans XenMobile pour Amazon, iOS, Android, Android for Work, Samsung SAFE, Samsung KNOX, Symbian, Windows Phone 8.1 et Windows 8.1 Tablet. Vous ajoutez et configurez les stratégies dans la console XenMobile depuis Configurer > Stratégies d'appareil.

Remarque : Sony Android prend uniquement en charge la stratégie de chiffrement du stockage. Android HTC prend uniquement en charge la stratégie Exchange.

Stratégie d'appareil	**Amazon**	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
Communes									
Exchange		X	X	X	X	X		X	
Planification			X	X			X		
Code secret		X	X	X		X		X	X
Restrictions	X	X			X			X	X
VPN	X	X	X		X	X			X
Wi-Fi		X	X					X	X
Services de localisation		X	X						
Termes et conditions	X	X	X		X	X	X		
Accès réseau									
APN		X	X			X			
Cellulaire		X	X						
Personal Hotspot		X							

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Hotspot									
Proxy		X							
Assistance à distance						X			
Itinérance		X							
Pare-feu Samsung					X				
Tunnel			X						
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
Personnalisées									
XML personnalisé							X	X	X
Importer profil iOS		X							
Suppression									
Suppression de profil		X							
Suppression du profil de provisioning		X							
Applications									
Accès applicatif		X	X				X		
Attributs d'application		X							

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de l'application		X							
Inventaire des applications		X	X			X	X	X	X
Désinstallation d'applications		X	X	X		X			X
Restriction de désinstallation d'applications	X				X				
Fichiers			X						
Navigateur				X	X	X			
Profil de provisioning		X							
Clé de sideloading									X
Certificat de signature									X
Clip Web		X	X						X
Worx Store		X	X						X
	Amazon	**iOS**	**Android**	**Android for Work**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
Sécurité									
Restrictions applicatives Android for				X					

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Work									
Mode kiosque		X	X						
Restrictions applicatives						X			
Contacts (CardDAV)		X							
Informations d'identification		X	X	X					X
Kiosque					X				
Domaines gérés		X							
SCEP		X							
Clé de licence MDM Samsung					X	X			
Chiffrement du stockage			X		X			X	
Filtre de contenu Web		X							
Agent XenMobile									
Hub d'entreprise								X	
Options XenMobile			X				X		
Désinstallation de XenMobile			X						

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Utilisateur final									
Mise en miroir AirPlay		X							
AirPrint		X							
Calendrier (CalDav)		X							
Police		X							
LDAP		X							
Options MDM		X							
Messagerie		X							
Info organisation		X							
Compte SSO		X							
Abonnements calendriers		X							

© 1999-2017 Citrix Systems, Inc. All rights reserved.

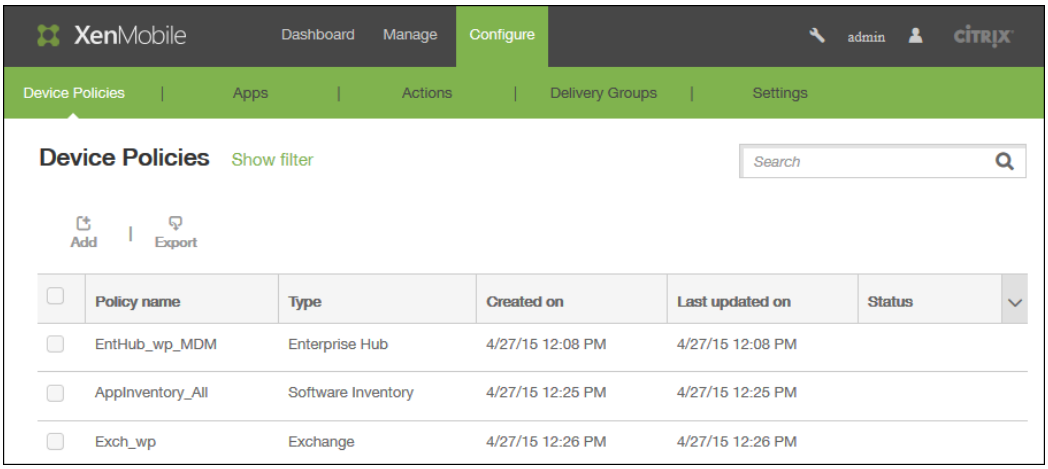
Pour ajouter une stratégie d'accès aux applications

Jul 25, 2016

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 ou Symbian.

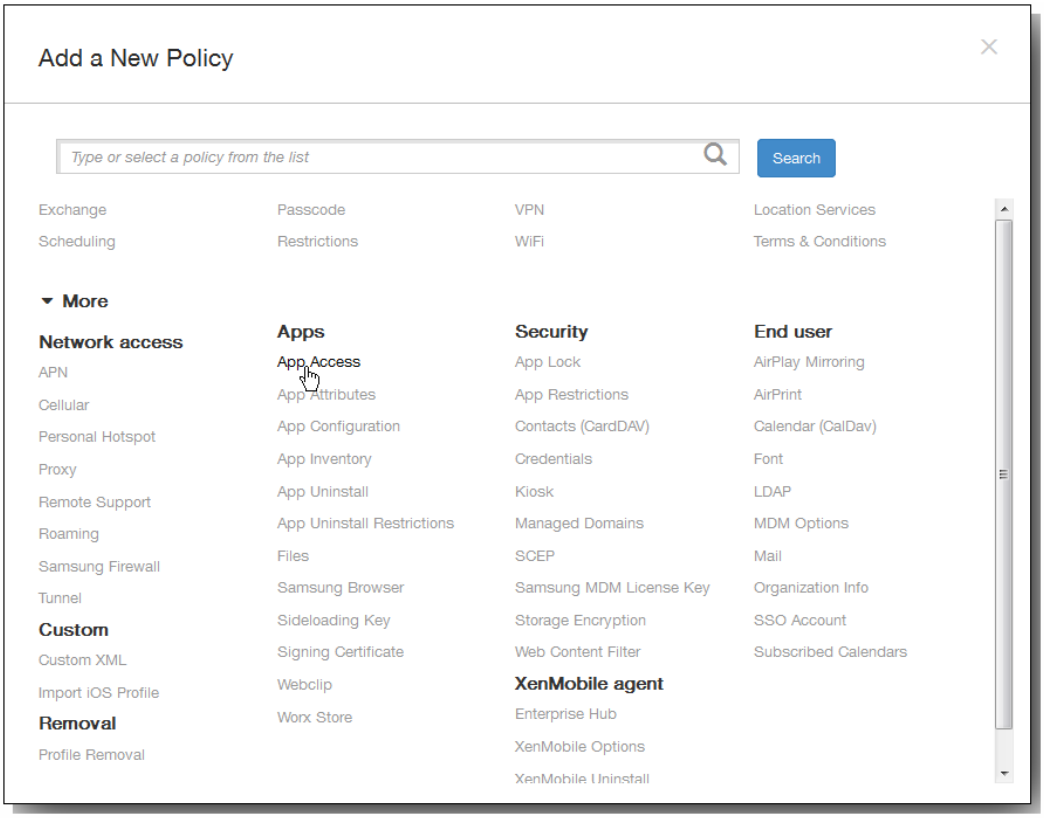
Vous ne pouvez configurer qu'un type de stratégie d'accès à la fois. Vous pouvez ajouter une stratégie pour une liste d'applications obligatoires, d'applications suggérées ou d'applications interdites, mais vous ne pouvez pas combiner ces trois types de liste au sein de la même stratégie d'accès. Si 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.

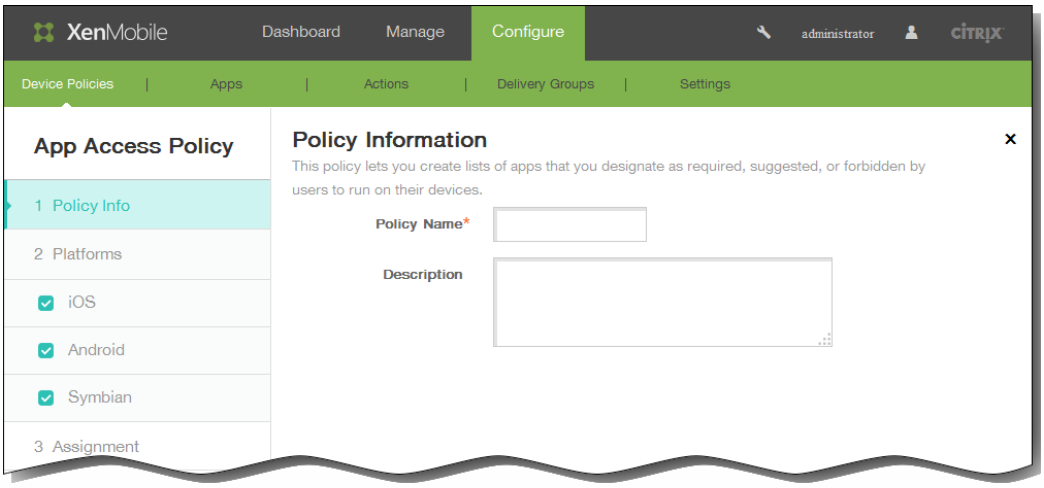


2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

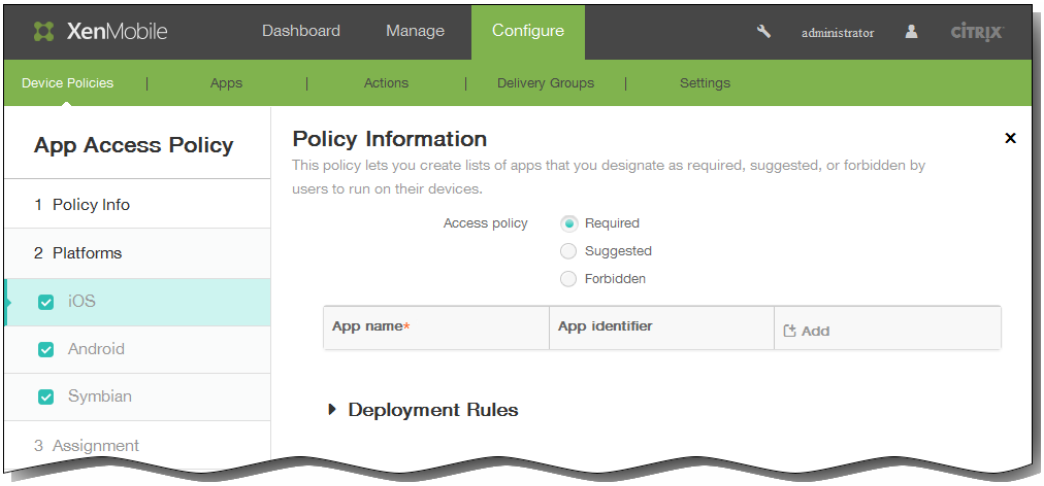


3. Cliquez sur Plus > Accès aux applications. La page d'informations sur la Stratégie d'accès aux applications s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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 page de configuration de la plate-forme iOS s'affiche en premier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes à ajouter, puis effectuez les opérations suivantes pour chaque plate-forme :
   1. Stratégie d'accès : cliquez sur Requise, Suggérée ou Interdite. La valeur par défaut est Requise.
   2. Pour ajouter une ou plusieurs applications à la liste, cliquez sur Ajouter, puis procédez comme suit :
      1. Nom app : entrez un nom pour l'application.
      2. Identifiant app : entrez un identifiant pour l'application (facultatif).
      3. Cliquez sur Enregistrer ou sur Annuler.
      4. Répétez les étapes i à iii pour chaque application que vous souhaitez 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.

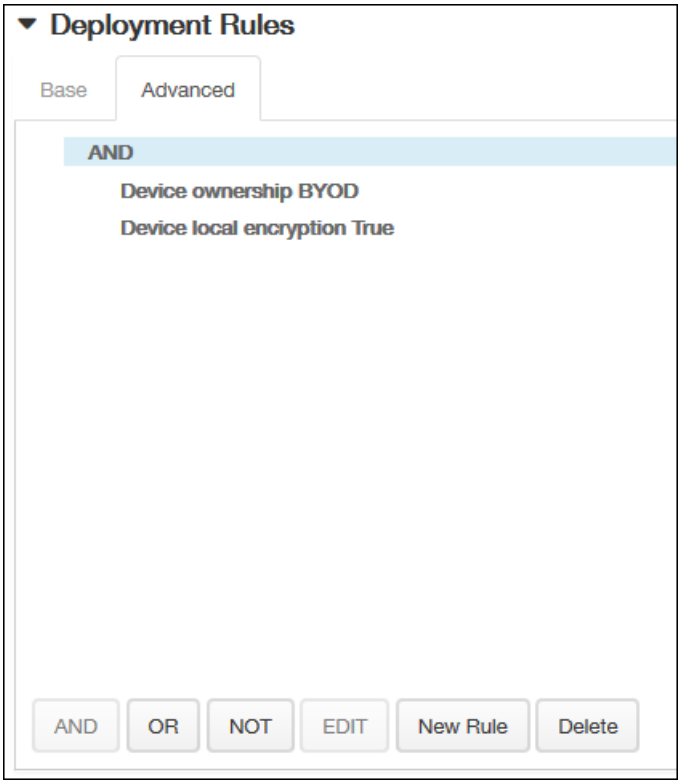
      Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour définir les conditions.
      3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
      4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
   2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

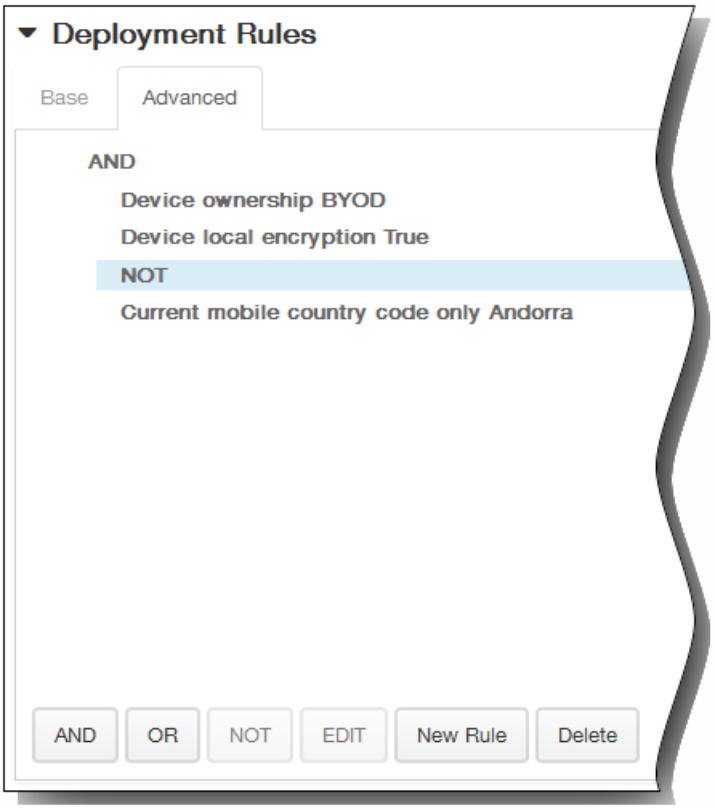


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

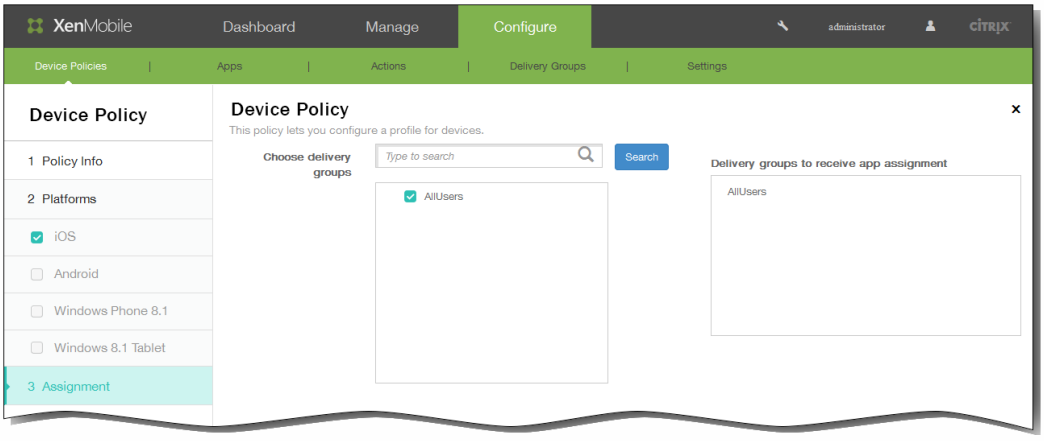
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. Cliquez sur Suivant. 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.



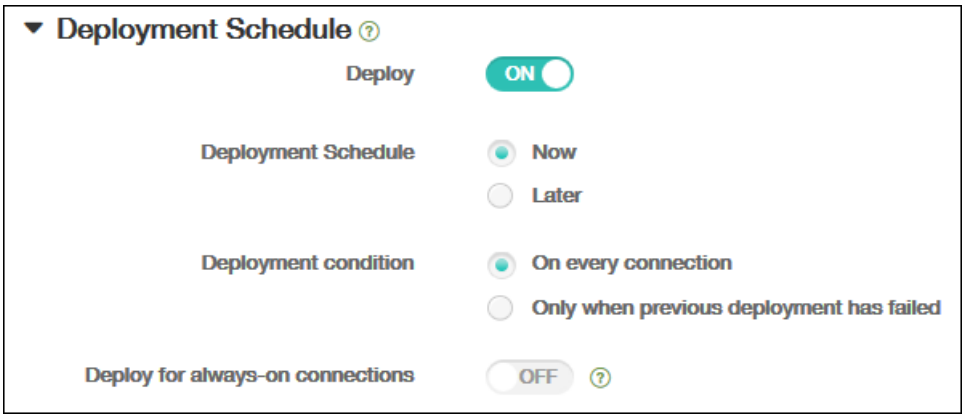
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

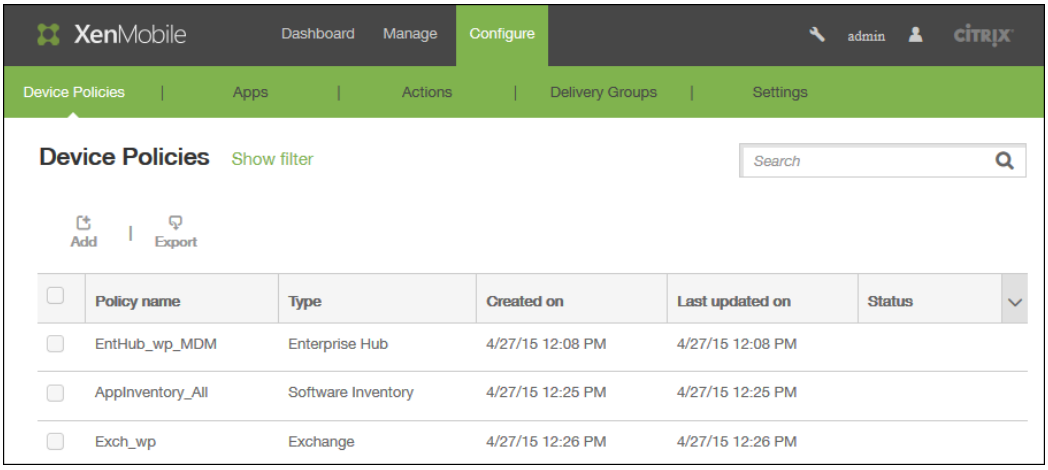
Pour ajouter une stratégie d'inventaire des applications

Jul 25, 2016

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.

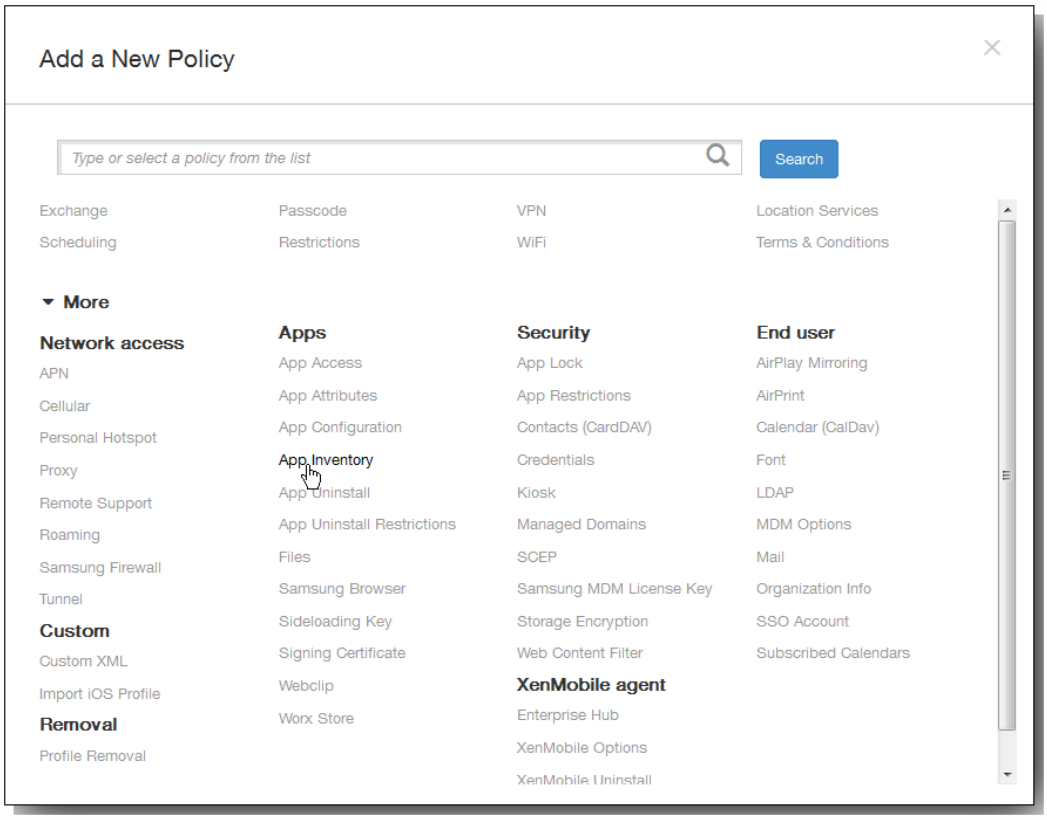
Important : pour mettre à jour les applications affichées dans la liste des applications disponibles dans le Worx Store sur les appareils Android des utilisateurs, vous devez d'abord déployer cette stratégie sur les appareils des utilisateurs.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

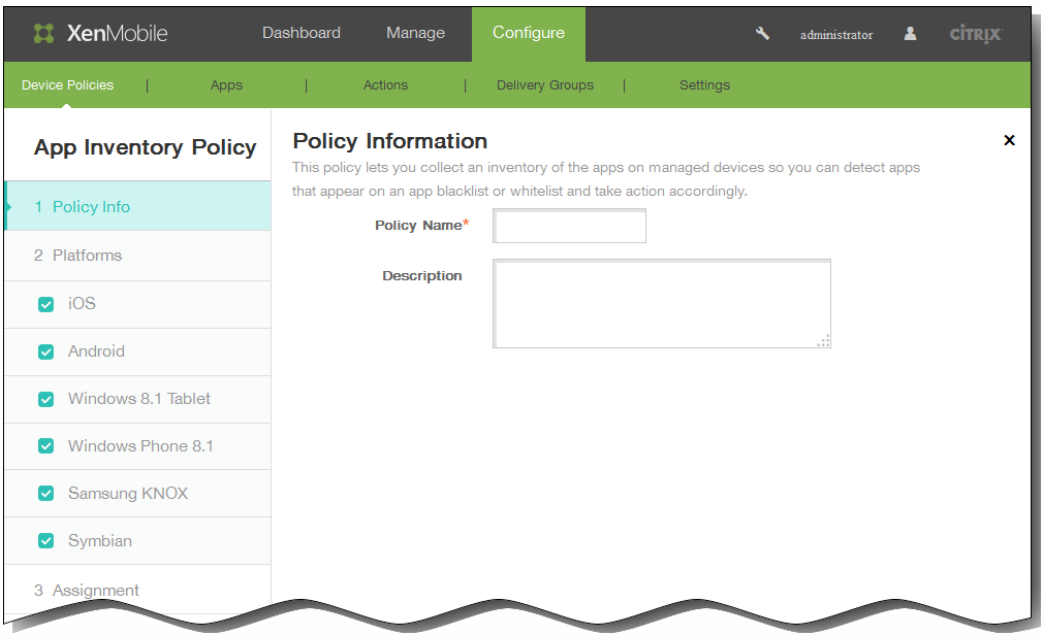


2. Cliquez sur Ajouter. La page Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



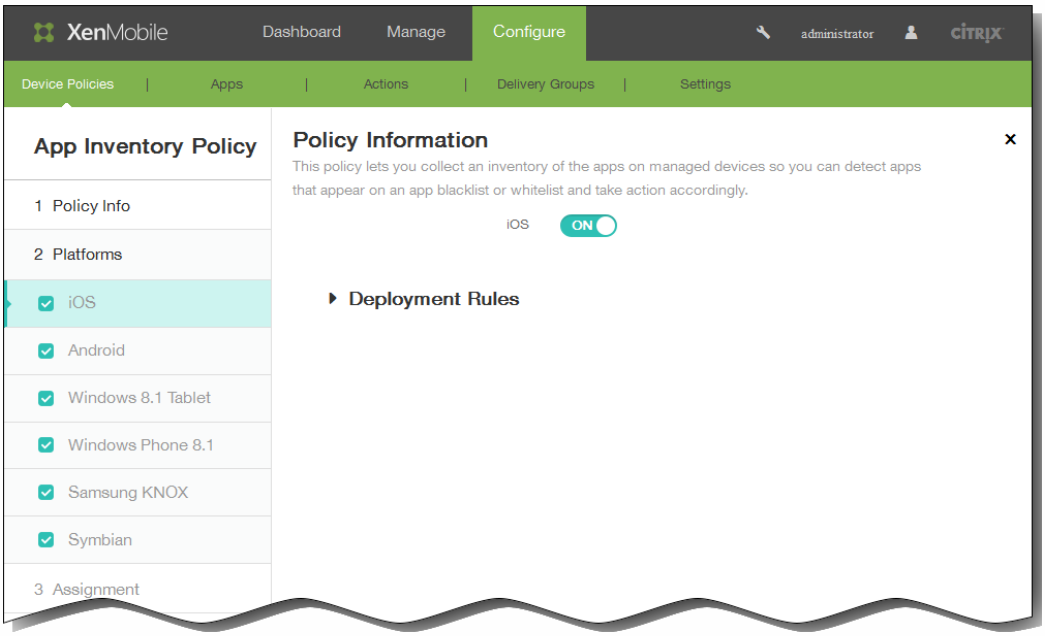
3. Cliquez sur Plus > Inventaire des applications. La page Stratégie d'inventaire des applications s'affiche.



4. Dans le panneau Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Stratégie par plate-forme s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : lorsque la page Stratégie par plate-forme s'affiche, toutes les plates-formes sont sélectionnées et le panneau de configuration de la plate-forme iOS s'affiche en premier.



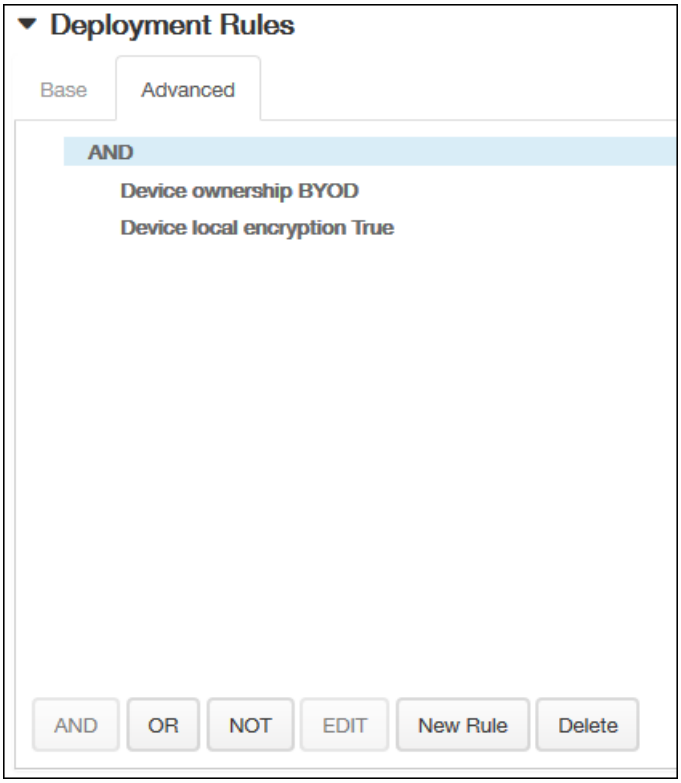
Sélectionnez la ou les plates-formes que vous souhaitez ajouter, puis pour chaque plate-forme, procédez comme suit :

6. Conservez le paramètre par défaut ou modifiez la valeur du paramètre sur OFF. La valeur par défaut est ON.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

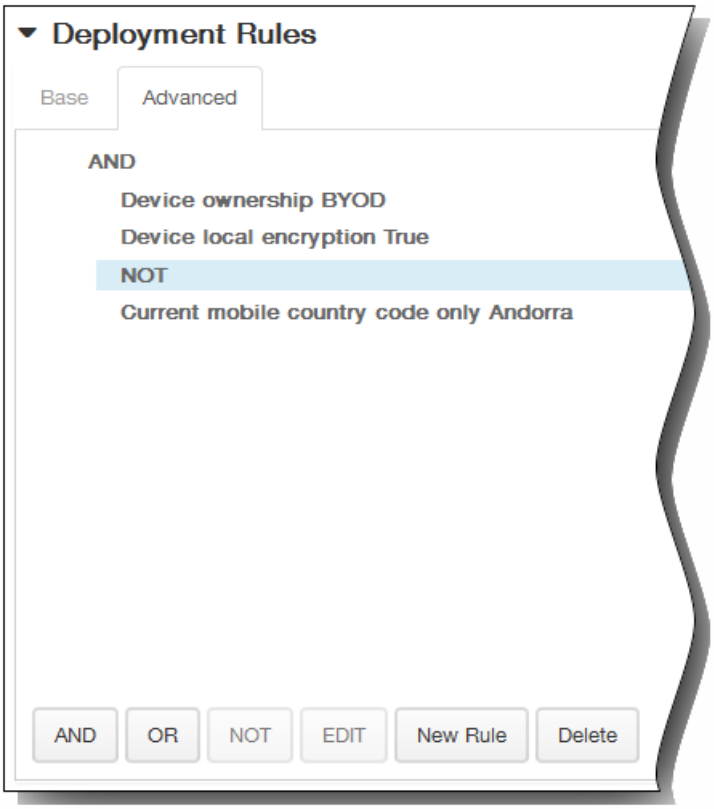


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

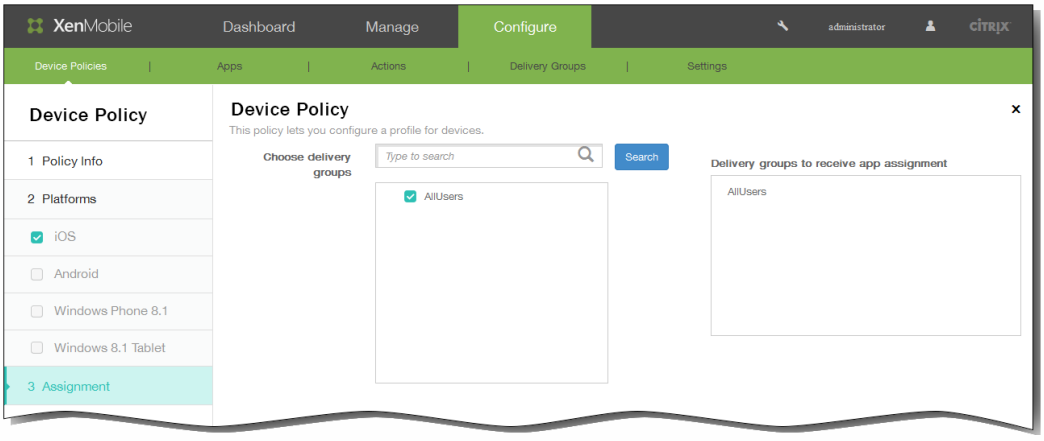
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. Cliquez sur Suivant. La page de la plate-forme suivante s'affiche ou la page de stratégie Attribution.
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.



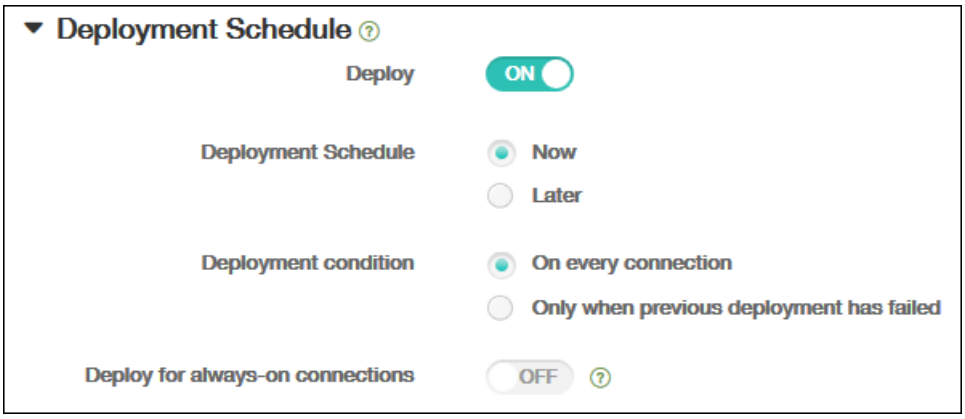
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

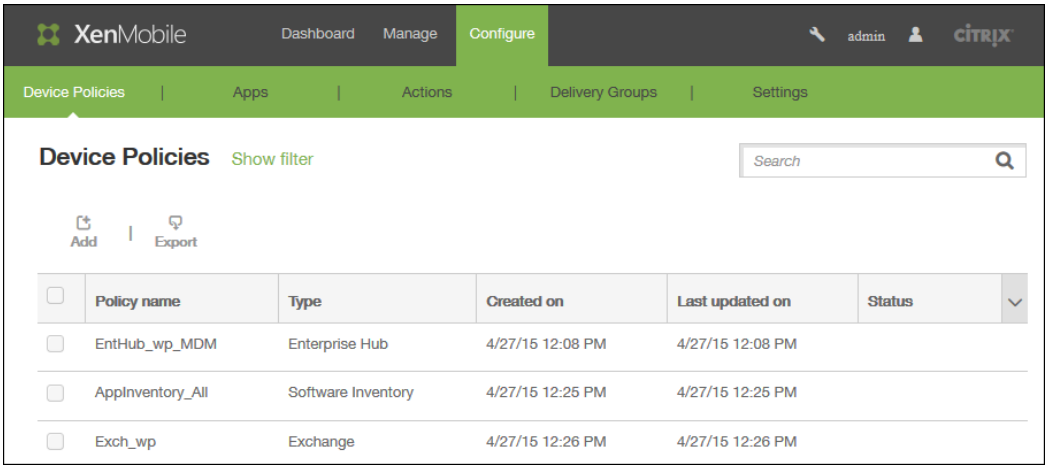
Pour ajouter une stratégie de tunnel applicatif pour Android

Jul 25, 2016

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.

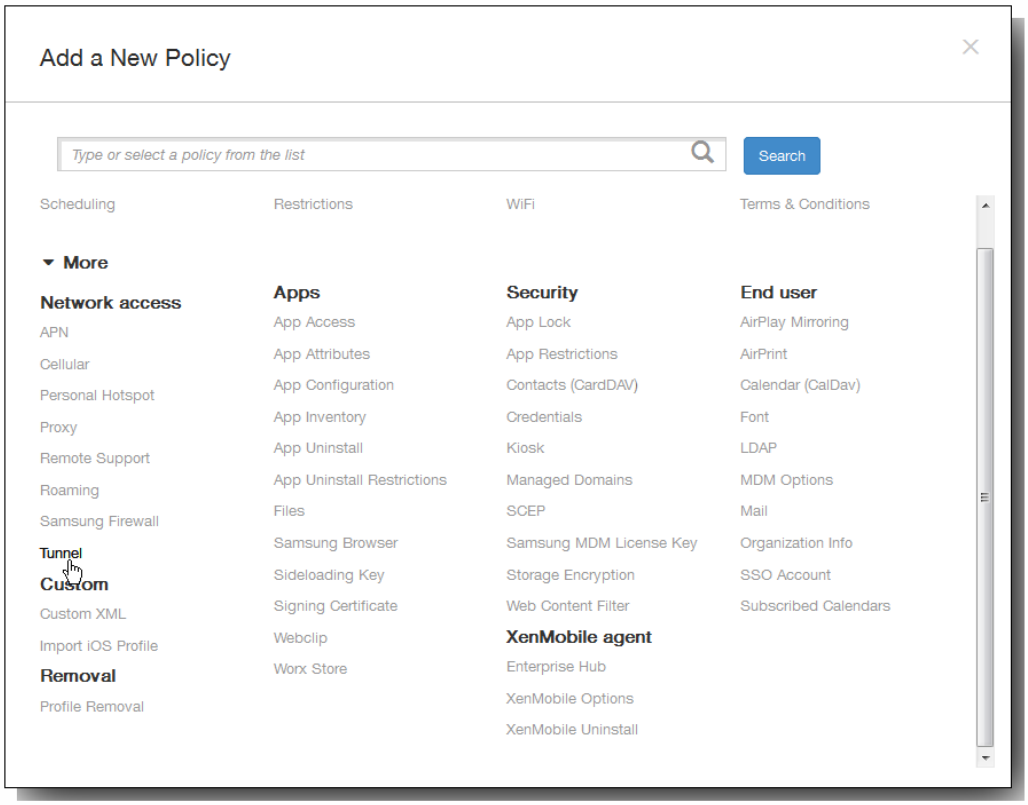
Remarque : tout trafic applicatif envoyé via un tunnel que vous définissez dans cette stratégie transite via XenMobile avant d'être redirigé vers le serveur exécutant l'application.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

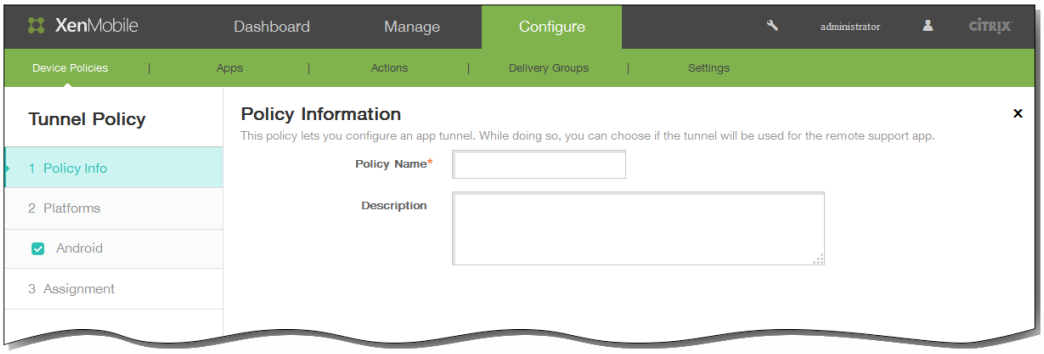


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

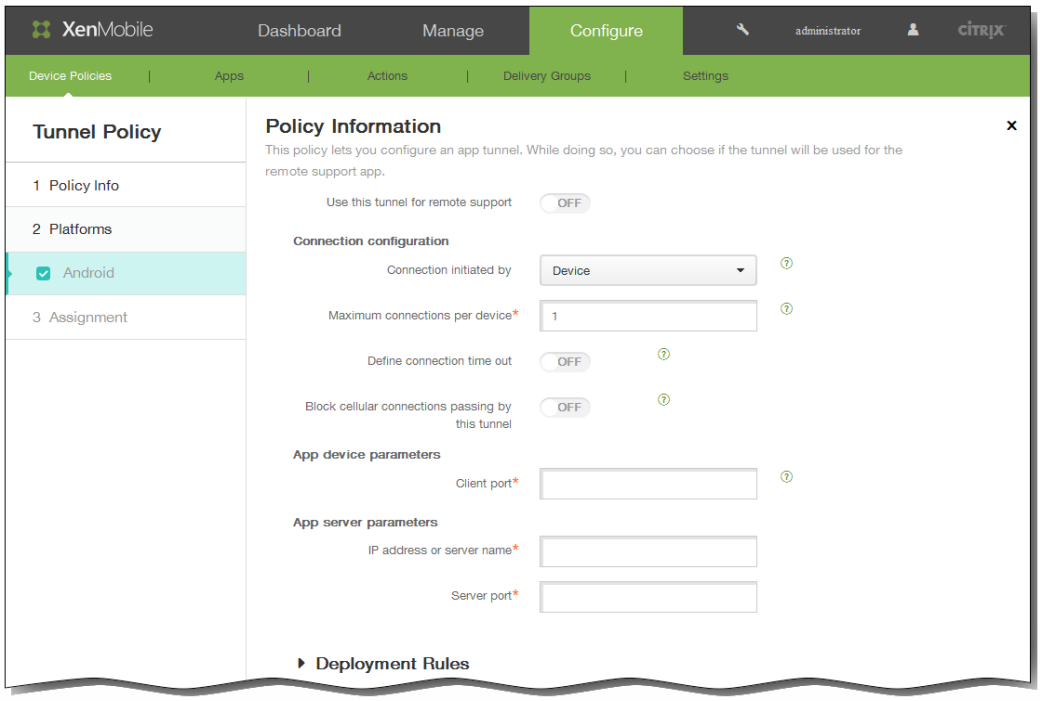


3. Cliquez sur Plus, puis, sous Accès réseau, cliquez sur Tunnel. La page Stratégie de tunnel s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page de plate-forme Stratégie Android s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans 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 :
   1. Connexion initiée par : Cliquez sur Appareil ou Serveur pour spécifier la source lançant la connexion.
   2. 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.
   3. 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.
   4. 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.
   5. 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.
   6. Port client : entrez le numéro du port du client. Dans la plupart des cas, cette valeur est la même que celle du port serveur.
   7. 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.
   8. Port serveur : entrez le numéro de port du serveur.

   Si vous **sélectionnez** l'assistance à distance, procédez comme suit :
   1. Utiliser ce tunnel pour l'assistance à distance : définissez cette option sur On.
   2. 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.
   3. 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.
   4. Utiliser une connexion SSL : indiquez si vous souhaitez utiliser une connexion SSL sécurisée pour ce tunnel.
   5. Bloquer les connexions cellulaires transitant par ce tunnel : sélectionnez cette option pour spécifier si ce tunnel est bloqué en itinérance.

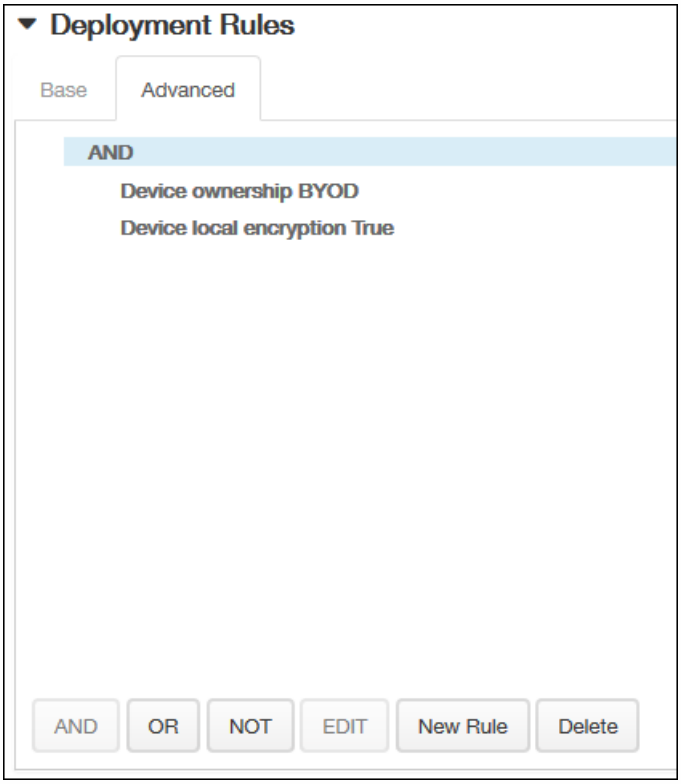
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remarque : les connexions Wi-Fi et USB ne sont pas bloquées.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



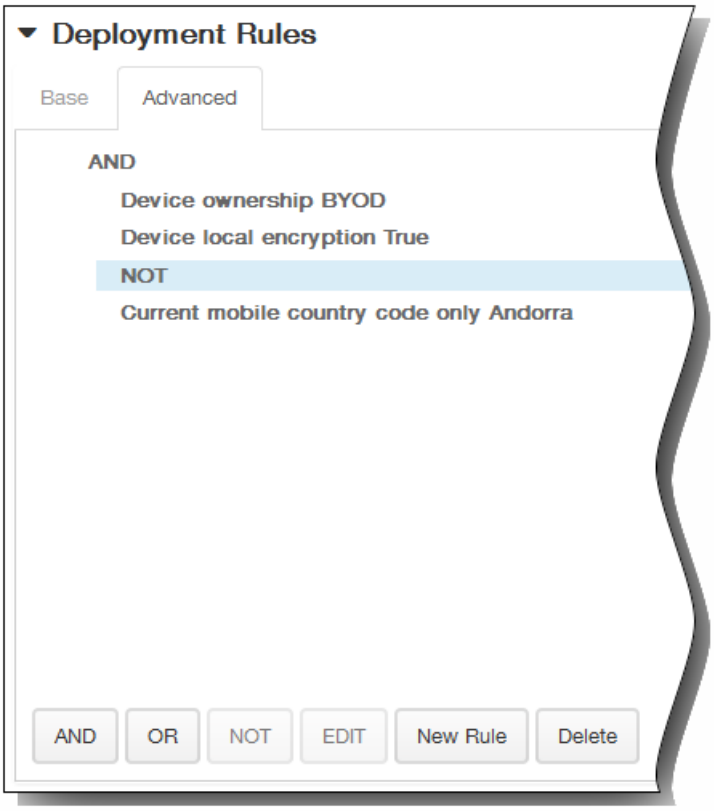
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
    1. Cliquez sur ET, OU ou SAUF.
    2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.

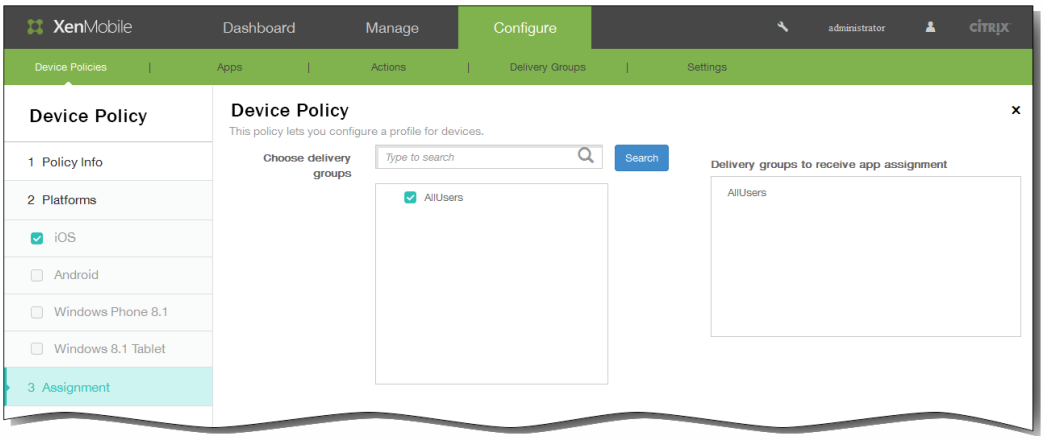
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
   Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



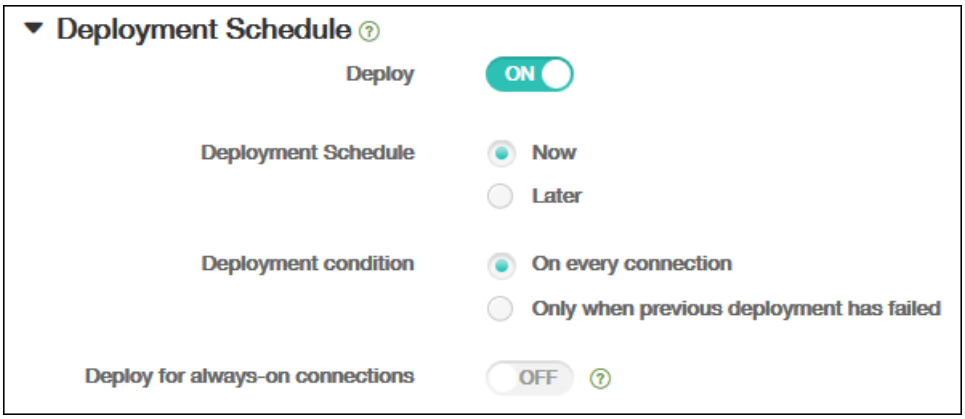
8. Cliquez sur Suivant. La page d'attribution de la Stratégie de tunnel s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies XML personnalisées

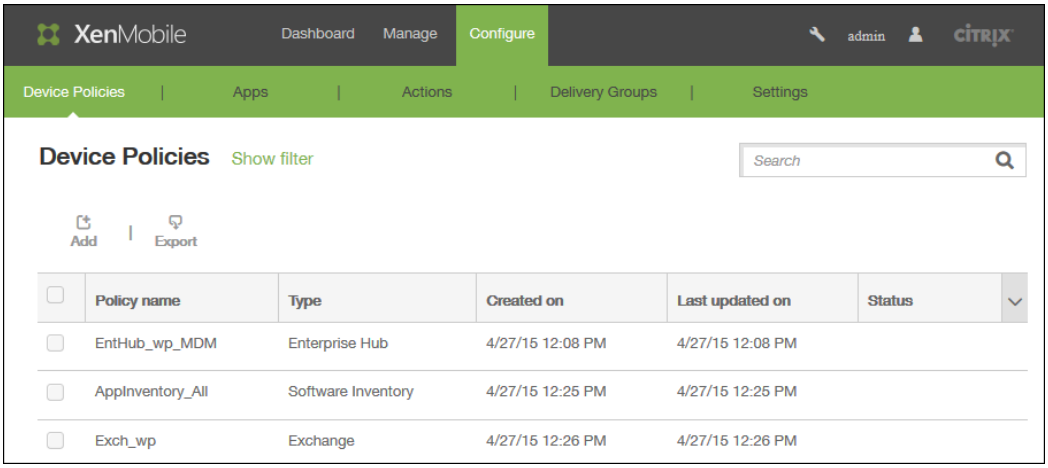
Jul 25, 2016

Vous pouvez créer des stratégies XML personnalisées dans XenMobile pour personnaliser les fonctionnalités suivantes sur Windows Phone 8.1, Windows 8.1 tablet et Symbian :

- 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.

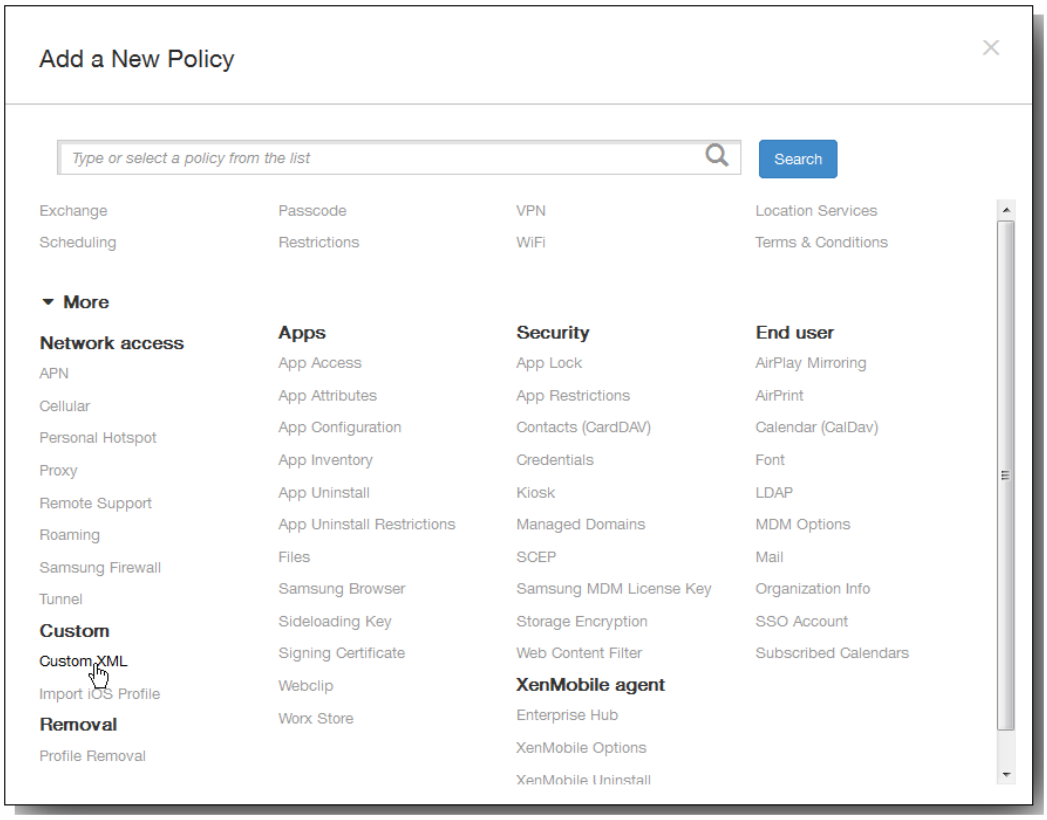
Vous créez votre propre configuration XML personnalisée à l'aide de l'API Open Mobile Alliance Device Management (OMA DM) dans Windows 8.1. La création de code XML personnalisé avec l'API OMA DM n'est pas couverte dans cette rubrique. Pour de plus amples informations sur l'utilisation de l'API OMA DM, 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.

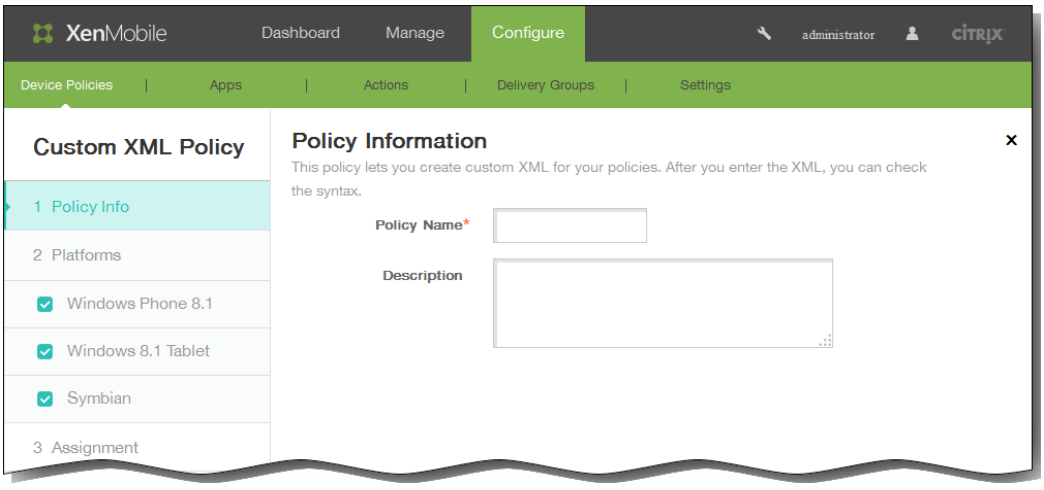


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

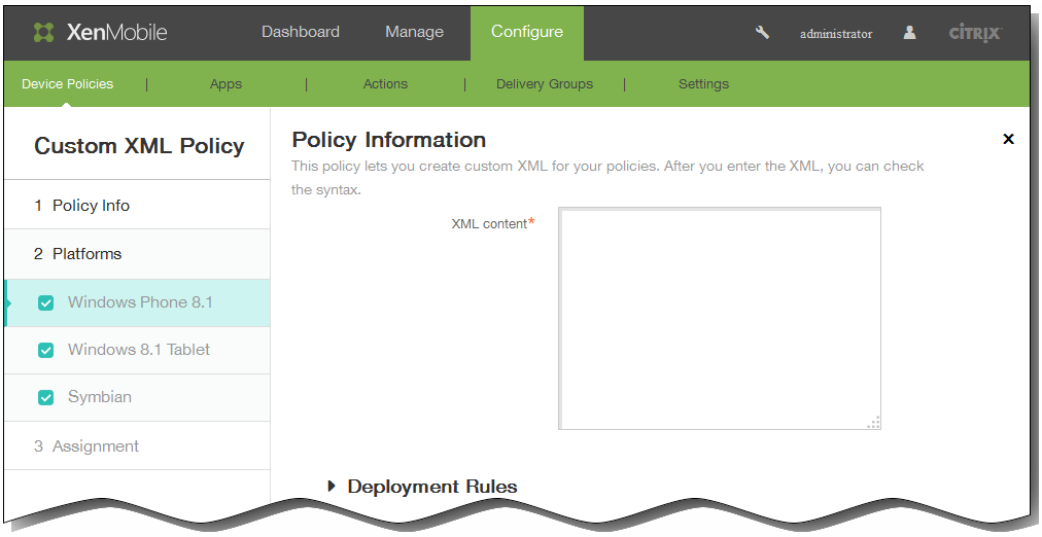


3. Cliquez sur Plus puis, sous Sécurité, cliquez sur XML personnalisé. La page d'informations Stratégie XML personnalisée s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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 le panneau de configuration de la plate-forme Windows Phone 8.1 s'affiche en premier.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

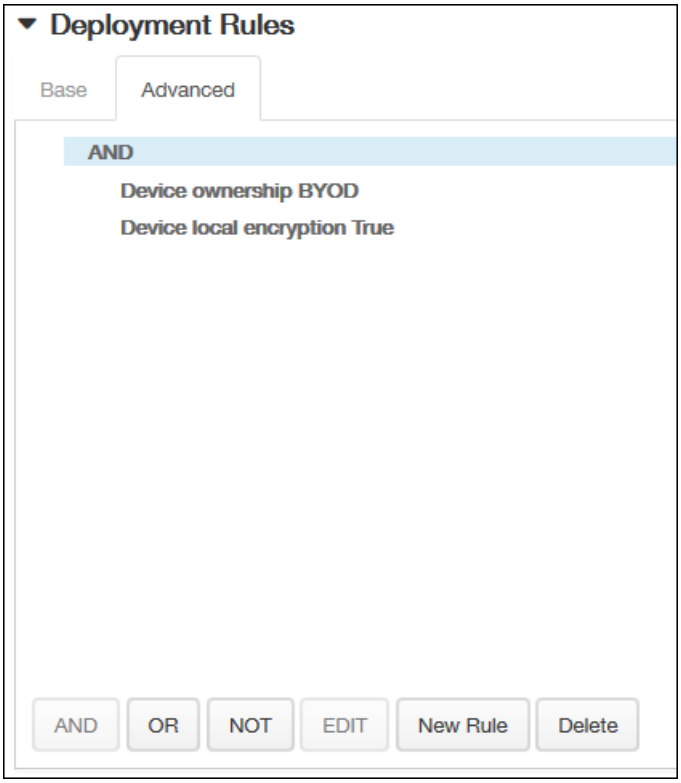


6. Sous Plates-formes, assurez-vous que les plates-formes que vous voulez ajouter sont sélectionnées.
7. Dans Contenu XML, entrez le code XML personnalisé que vous souhaitez ajouter à la stratégie. Si le contenu est trop long, vous pouvez couper et coller le code à partir du fichier source.
8. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

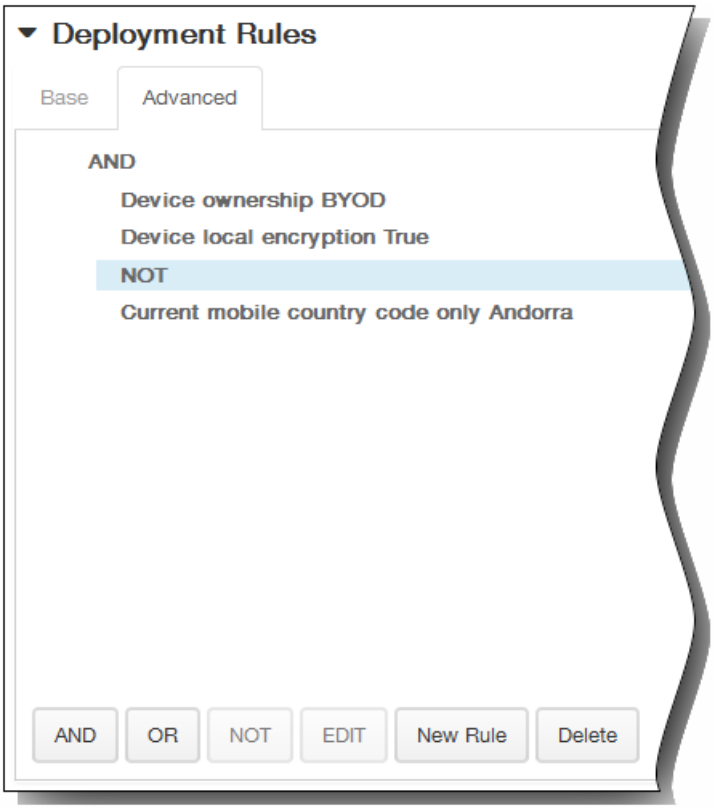


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

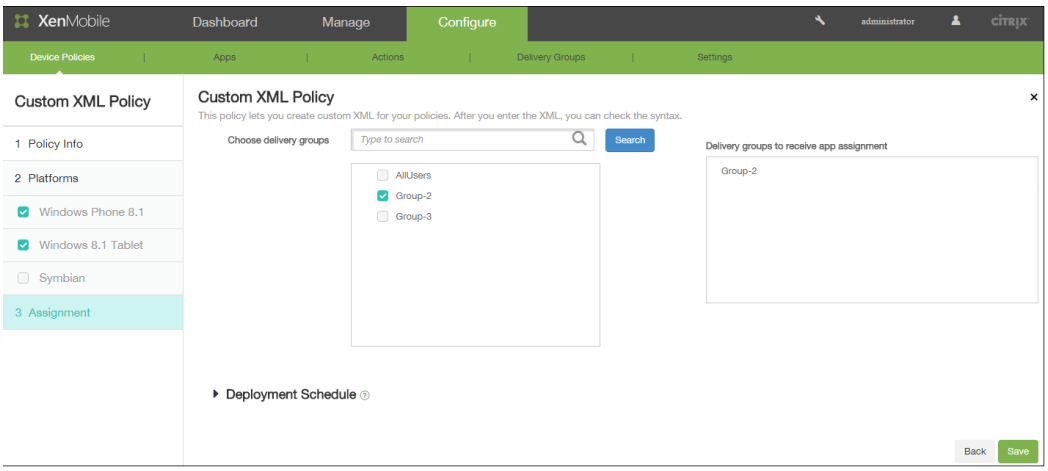
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

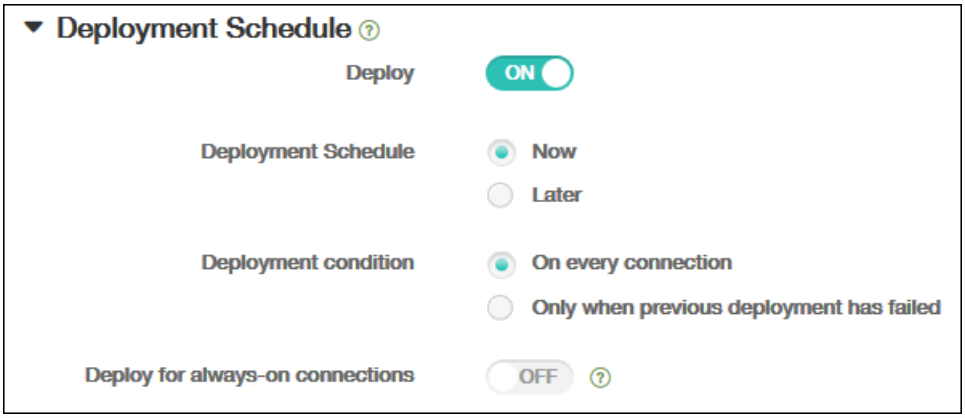


11. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 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.
5. 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.

Remarque : 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 pour enregistrer la stratégie.

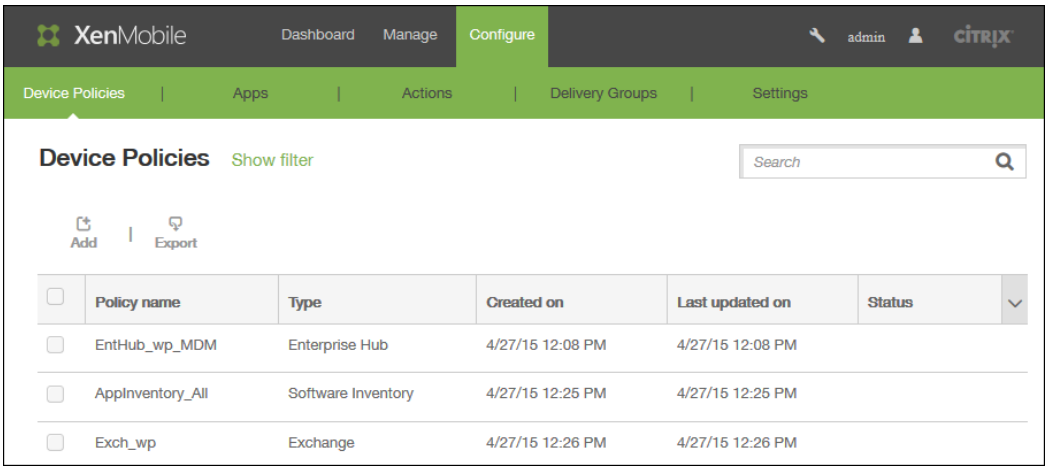
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies de désinstallation d'application

Jul 25, 2016

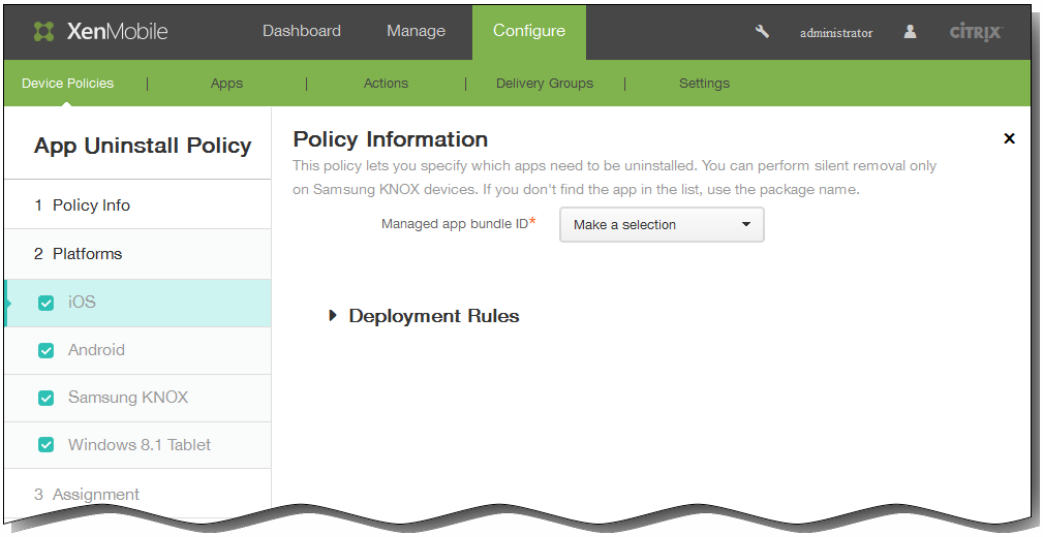
Vous pouvez créer une stratégie de désinstallation d'application pour les plates-formes iOS, Android, Samsung KNOX, Android for Work et Windows 8.1 Tablet. Une stratégie de désinstallation d'application vous permet de supprimer des applications des appareils utilisateur pour un certain nombre de raisons. 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. Sur la page Stratégies d'appareil, cliquez sur Ajouter.

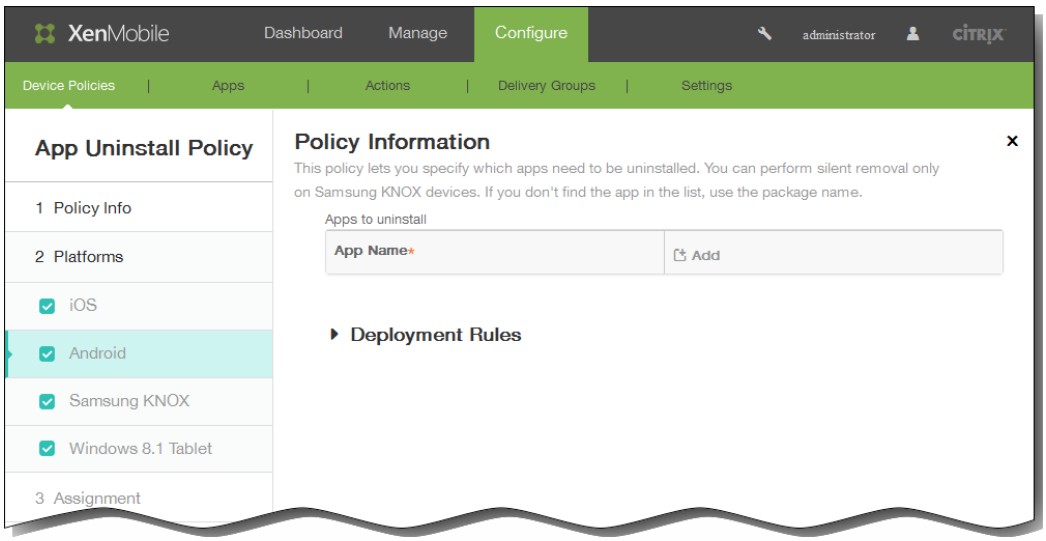


2. Dans la boîte de dialogue Ajouter une nouvelle stratégie, cliquez sur Plus puis dans Applications, cliquez sur Désinstallation des applications.
3. Dans le panneau d'informations Stratégie de désinstallation des applications, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
   3. Cliquez sur Suivant.
4. lorsque la page Stratégie par plate-forme s'affiche, toutes les plates-formes sont sélectionnées et le panneau de configuration de la plate-forme iOS s'affiche en premier. Dans Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter et désélectionnez celles que vous ne souhaitez pas ajouter.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Configurez les paramètres suivants en fonction des plates-formes que vous avez sélectionnées.
   1. Si vous avez sélectionné iOS, dans la liste Bundle ID d'application gérée, cliquez sur une application existante ou cliquez sur Ajouter.
      Remarque : 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.
   2. Si vous optez pour Android, Samsung KNOX, Android for Work ou Windows 8.1 Tablet :



Dans Applications à désinstaller, cliquez sur Ajouter, puis procédez comme suit :

1. Nom app : dans la liste, cliquez sur une application existante ou sur Ajouter pour entrer un nouveau nom d'application.
   Remarque : s'il n'existe aucune application configurée pour cette plate-forme, la liste est vide et vous devez ajouter de nouvelles applications.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

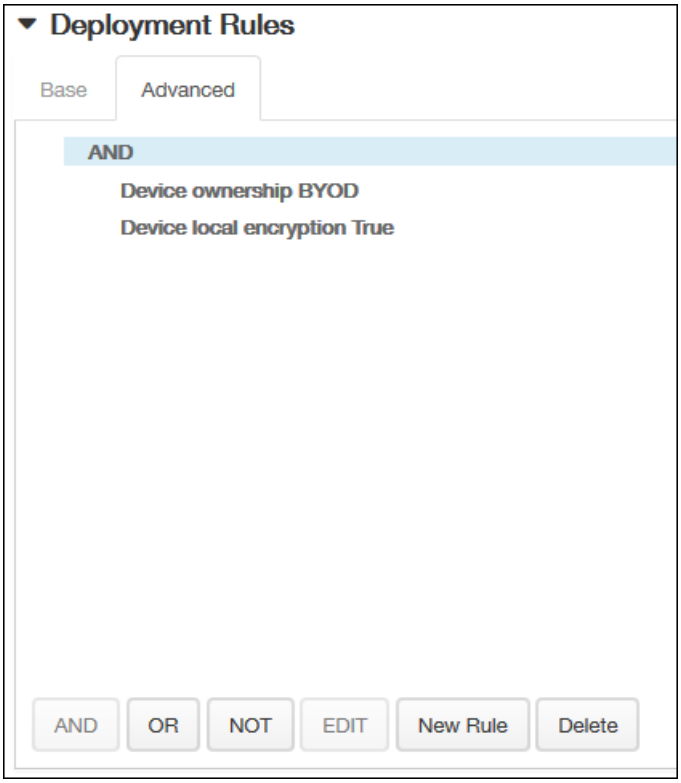
2. Cliquez sur Ajouter pour ajouter l'application, ou cliquez sur Annuler pour annuler l'ajout de l'application.
3. Répétez les étapes i. et ii. pour chaque application que vous voulez ajouter à la stratégie de désinstallation.
   Remarque : pour supprimer une application existante de la stratégie de 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.

6. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

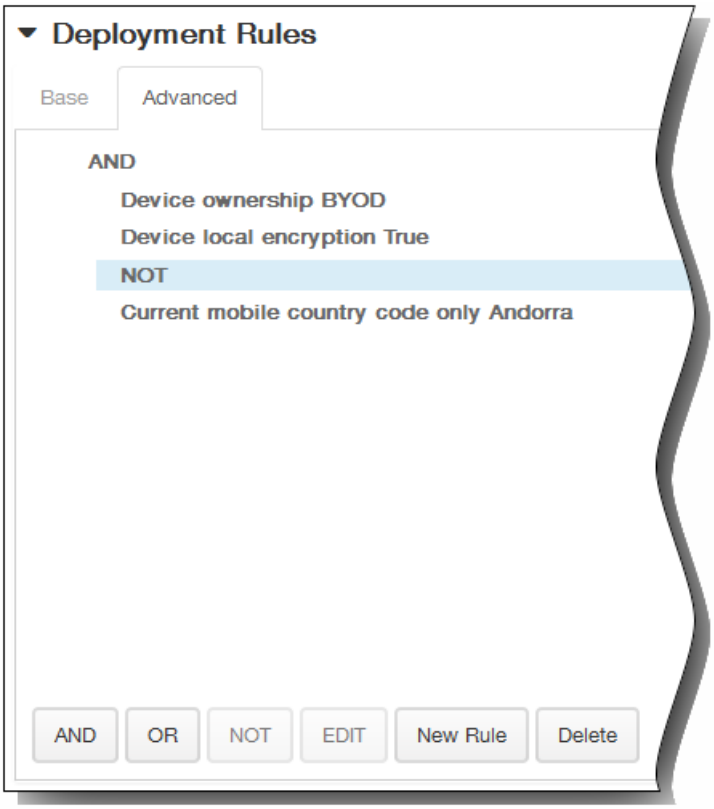
© 1999-2017 Citrix Systems, Inc. All rights reserved.



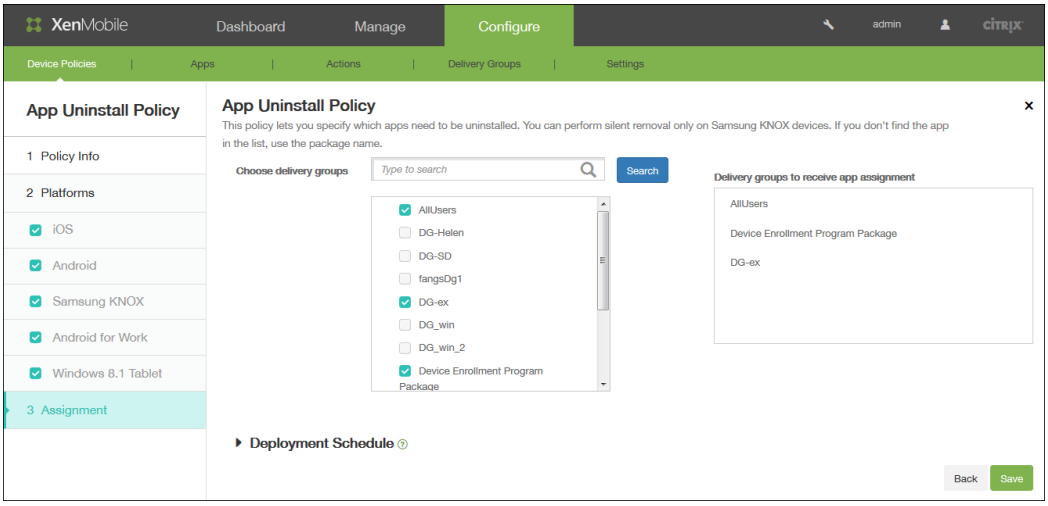
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. Cliquez sur Suivant. La page d'attribution de la Stratégie de désinstallation des applications 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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

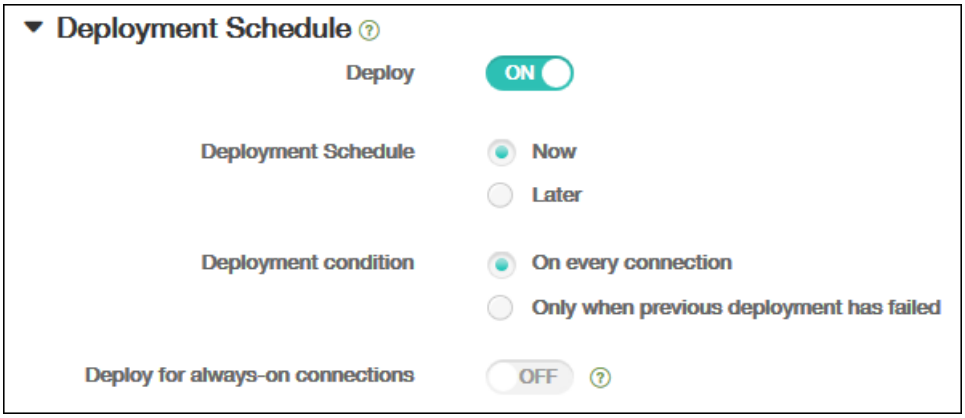


9. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
4. 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.
5. 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.



10. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de fichiers pour Android

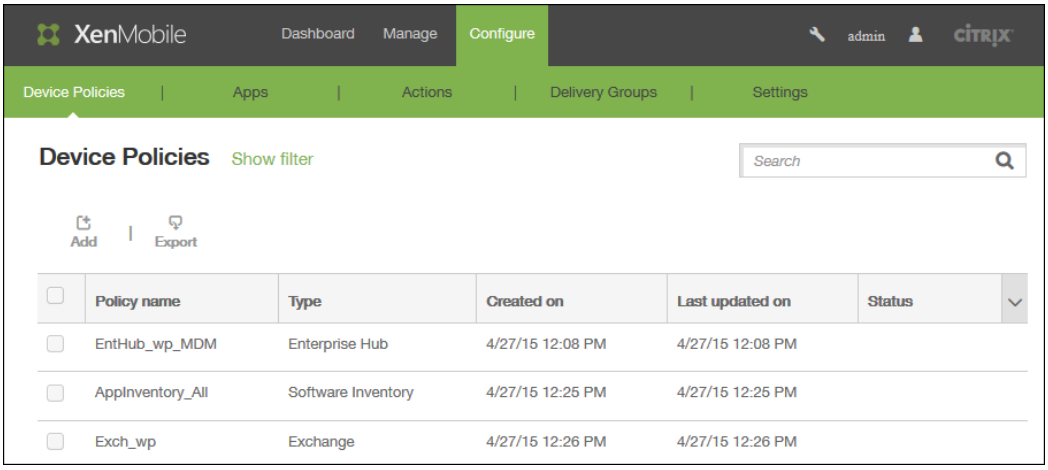
Jul 25, 2016

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 :

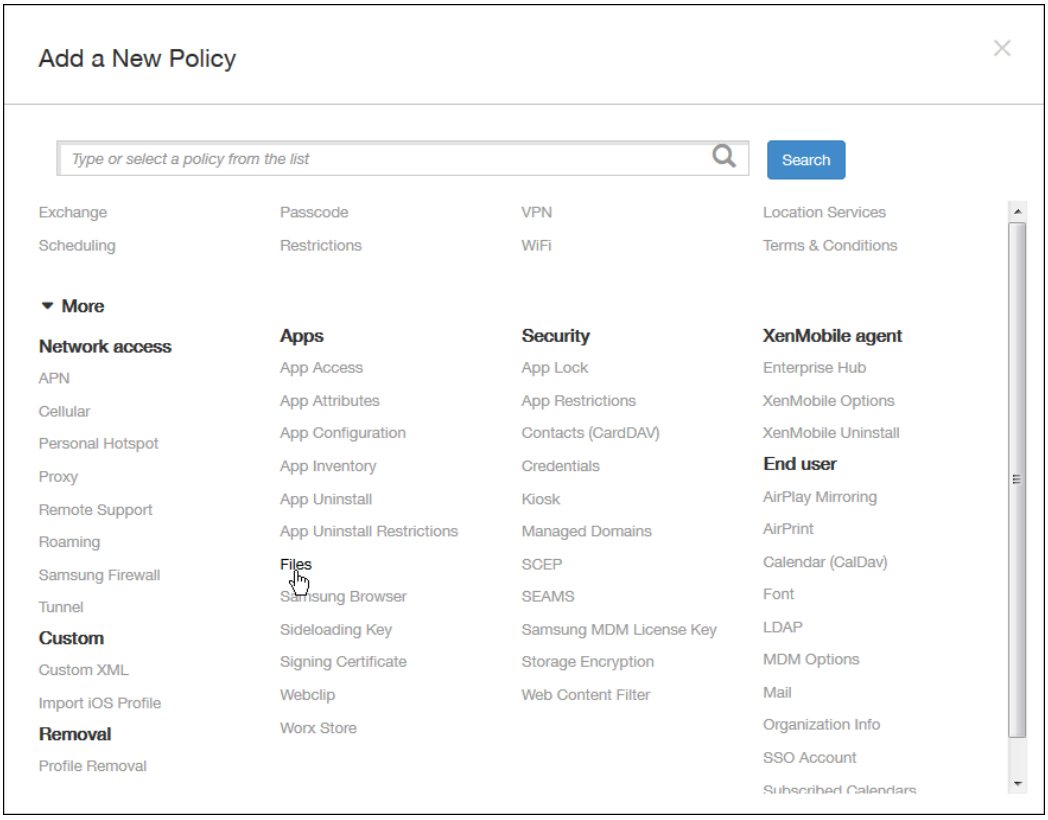
- Fichiers texte (.xml, .html, .py, etc.)
- Autres fichiers tels que des documents, images, feuilles de calcul ou présentations
- Pour Windows Mobile and Windows CE uniquement : fichiers de script créés avec MortScript

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

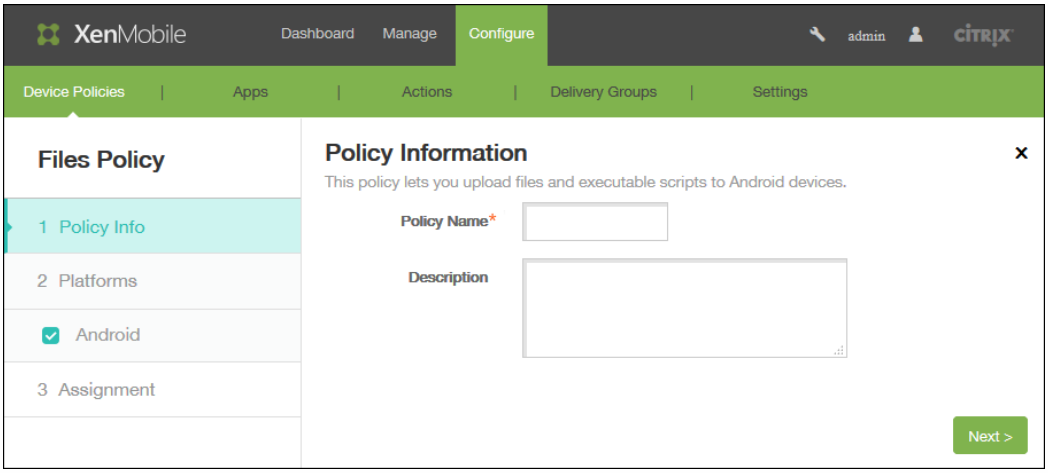


2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

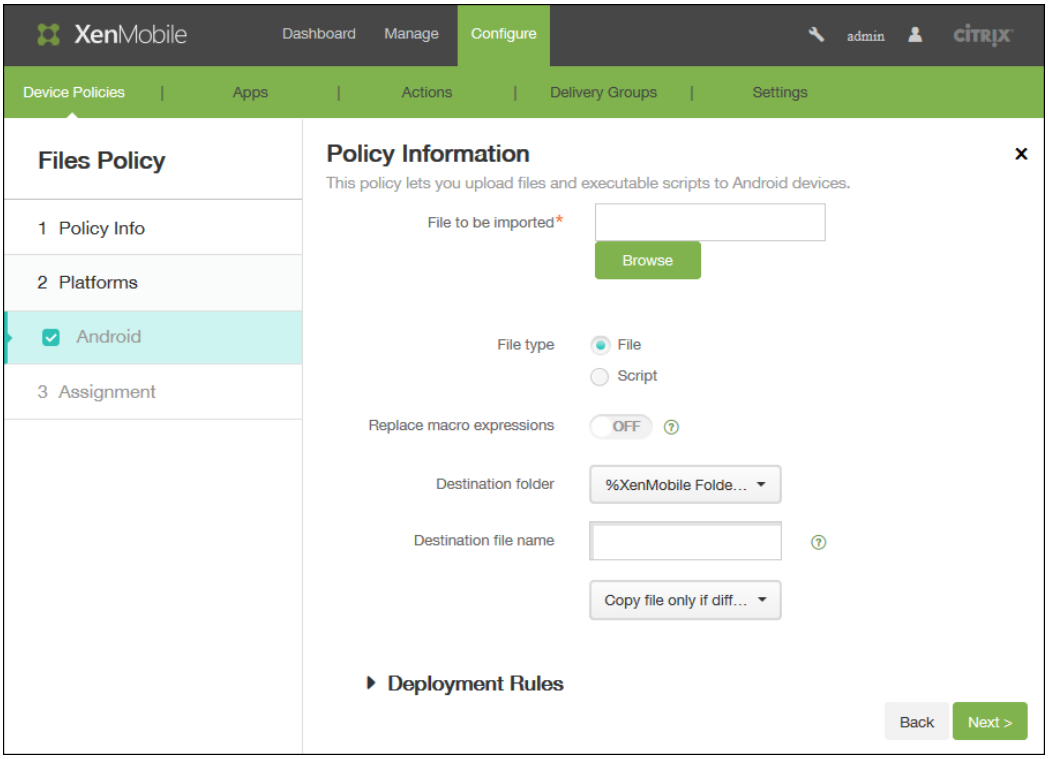


3. Cliquez sur Plus puis, sous Applications, cliquez sur Fichiers. La page d'informations Stratégie de fichiers s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Plate-forme Android s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans la page d'informations Plate-forme Android, entrez les informations suivantes :
   1. Fichier à importer : sélectionnez le fichier à importer en cliquant sur Parcourir et en accédant à l'emplacement du fichier.
   2. 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.
   3. 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.
   4. Dossier de destination : dans la liste, sélectionnez l'emplacement dans lequel stocker le fichier chargé.
   5. 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.
   6. Copier le fichier s'ils sont différents : dans la liste, sélectionnez si vous souhaitez copier le fichier s'il est différent du fichier existant ou remplacer le fichier existant.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



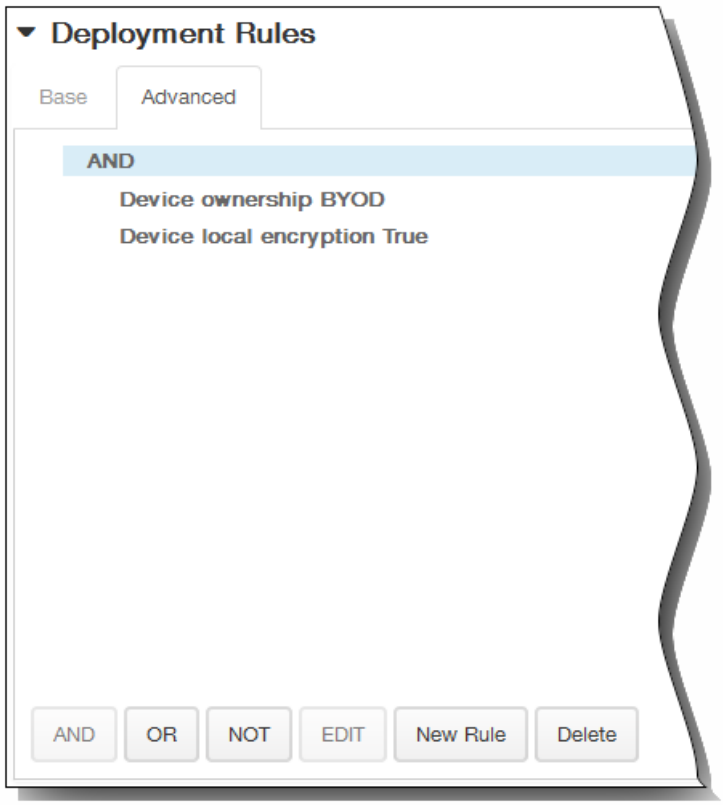
   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est

© 1999-2017 Citrix Systems, Inc. All rights reserved.

remplie. L'option par défaut est Toutes.

2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

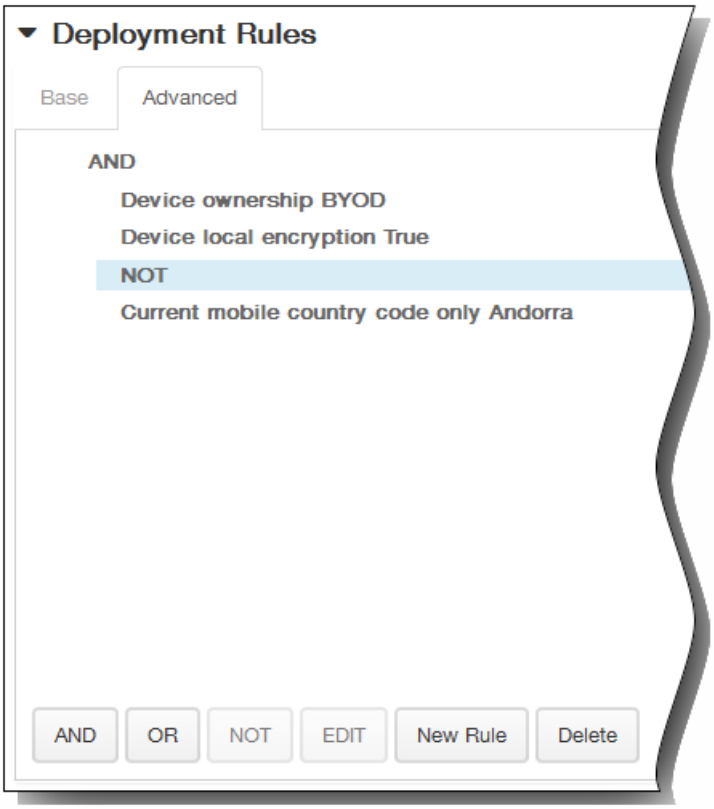
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



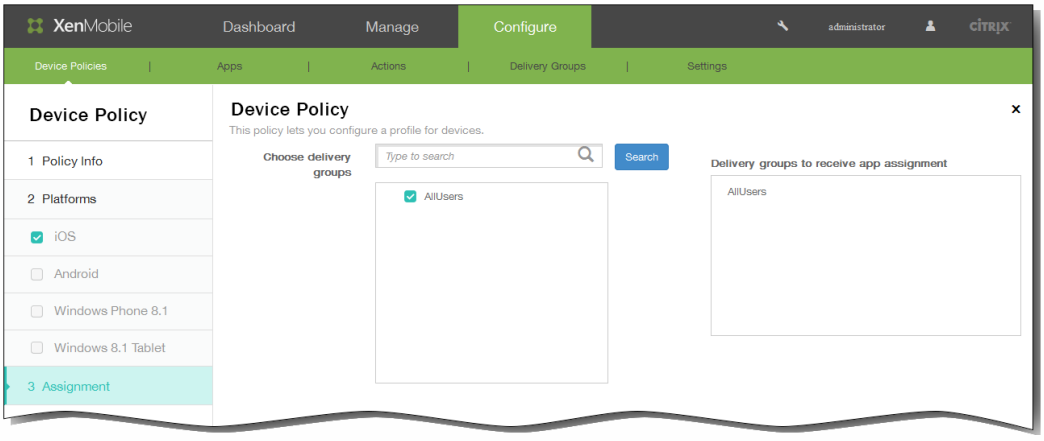
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



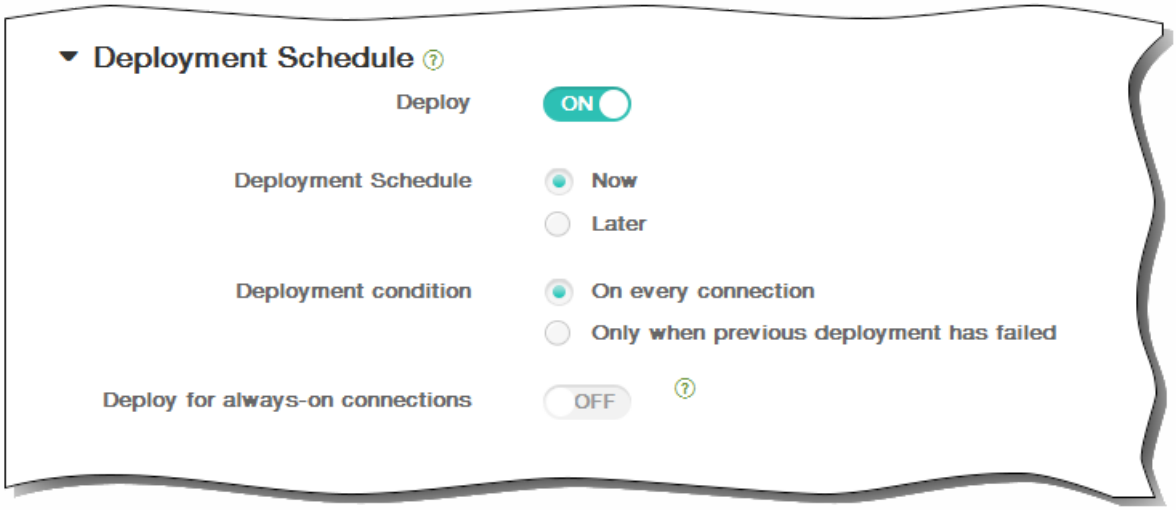
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies APN

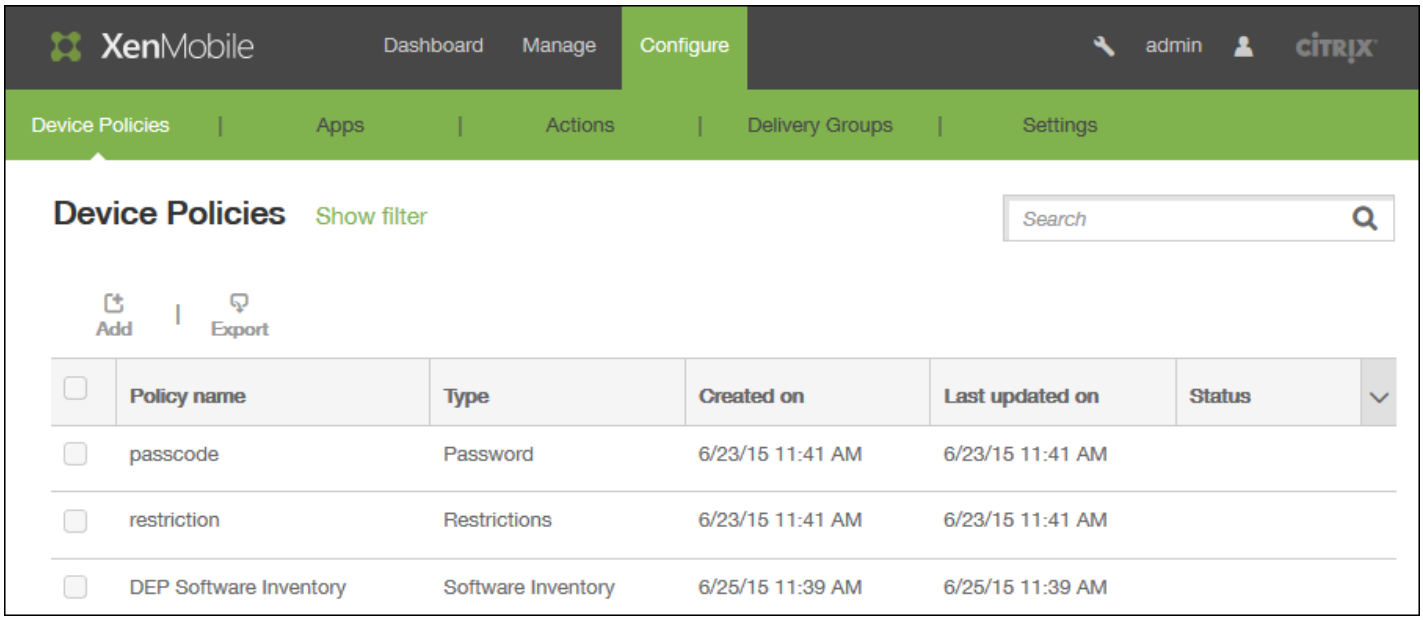
Jul 25, 2016

Vous pouvez ajouter une stratégie de nom de point d'accès (APN) personnalisée pour iOS et Android. 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

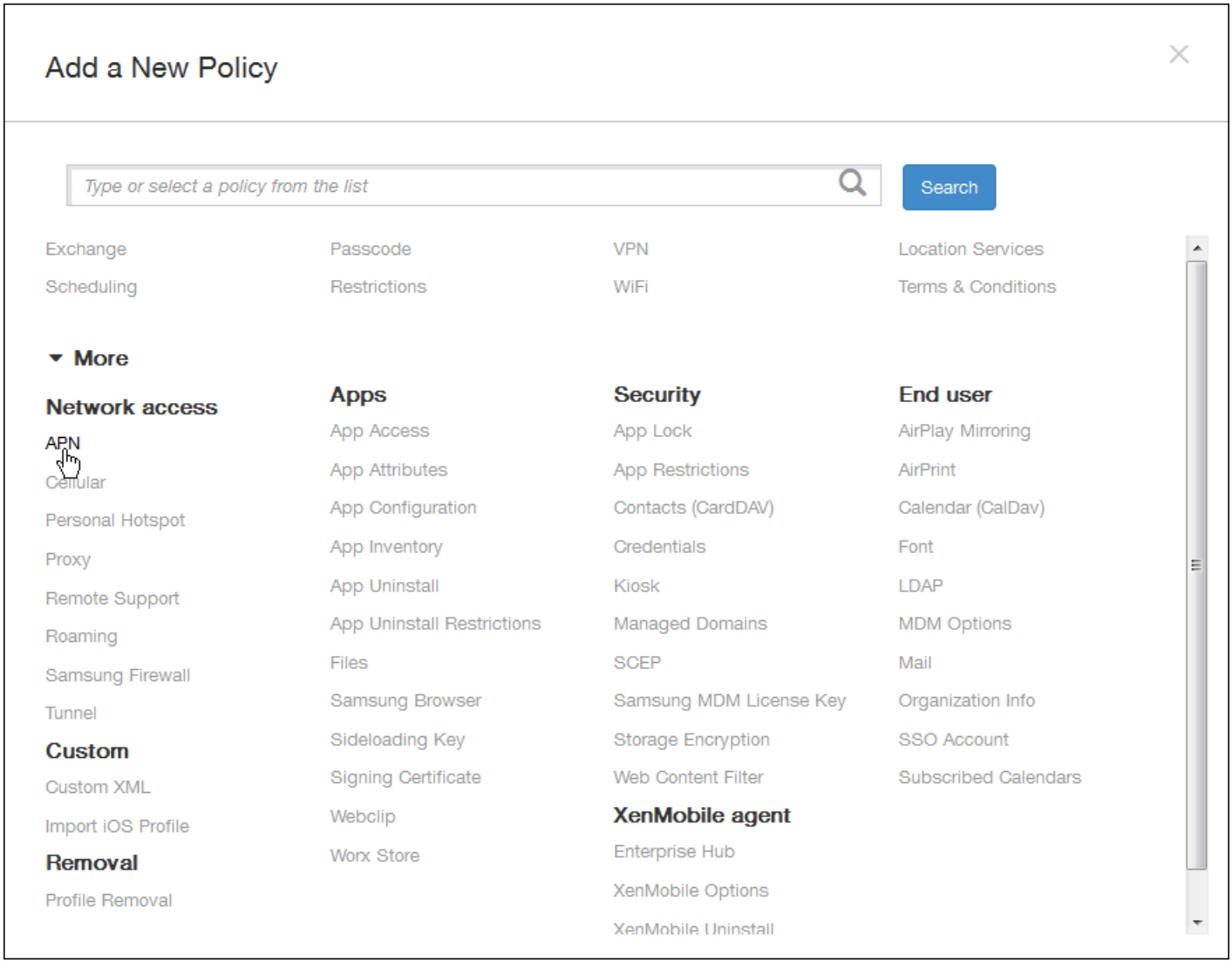
Paramètres Android

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



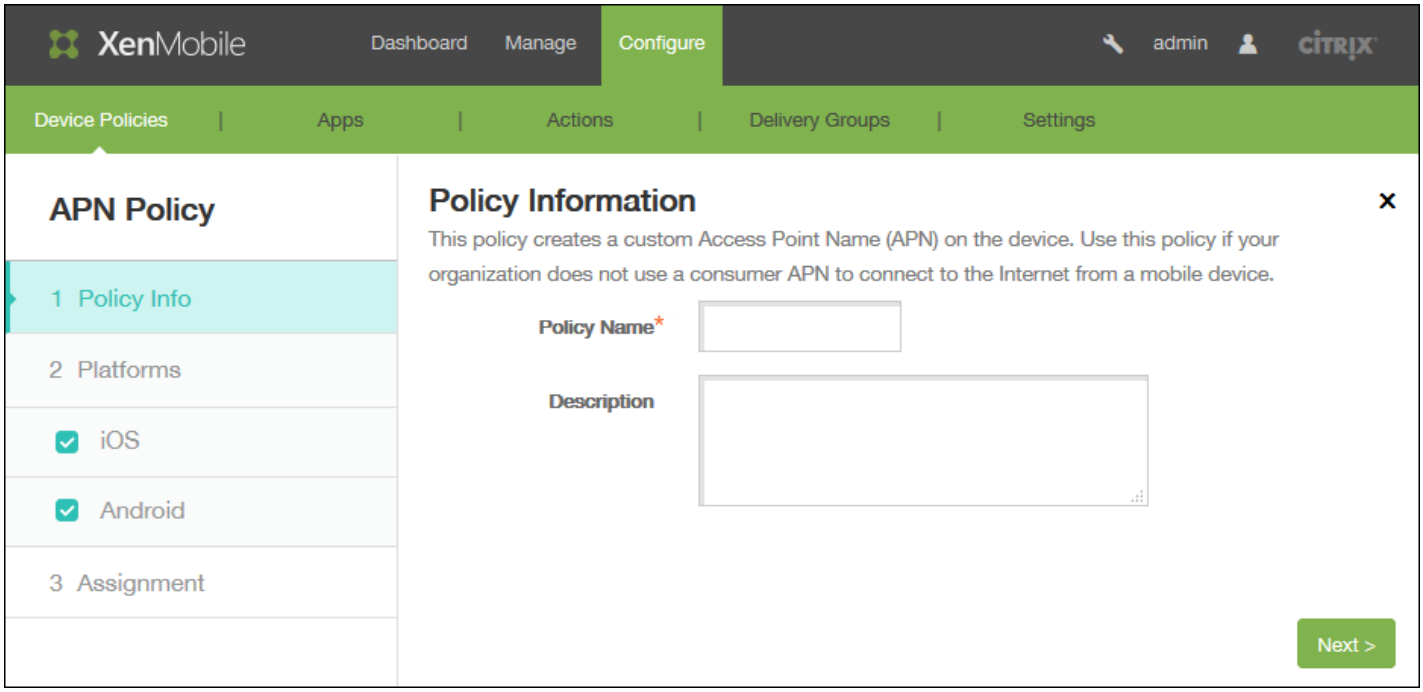
2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La page **Ajouter une nouvelle stratégie** apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sur la page **Ajouter une nouvelle stratégie**, cliquez sur **Plus** puis sous **Accès réseau**, cliquez sur **APN**. La page d'informations **Stratégie APN** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

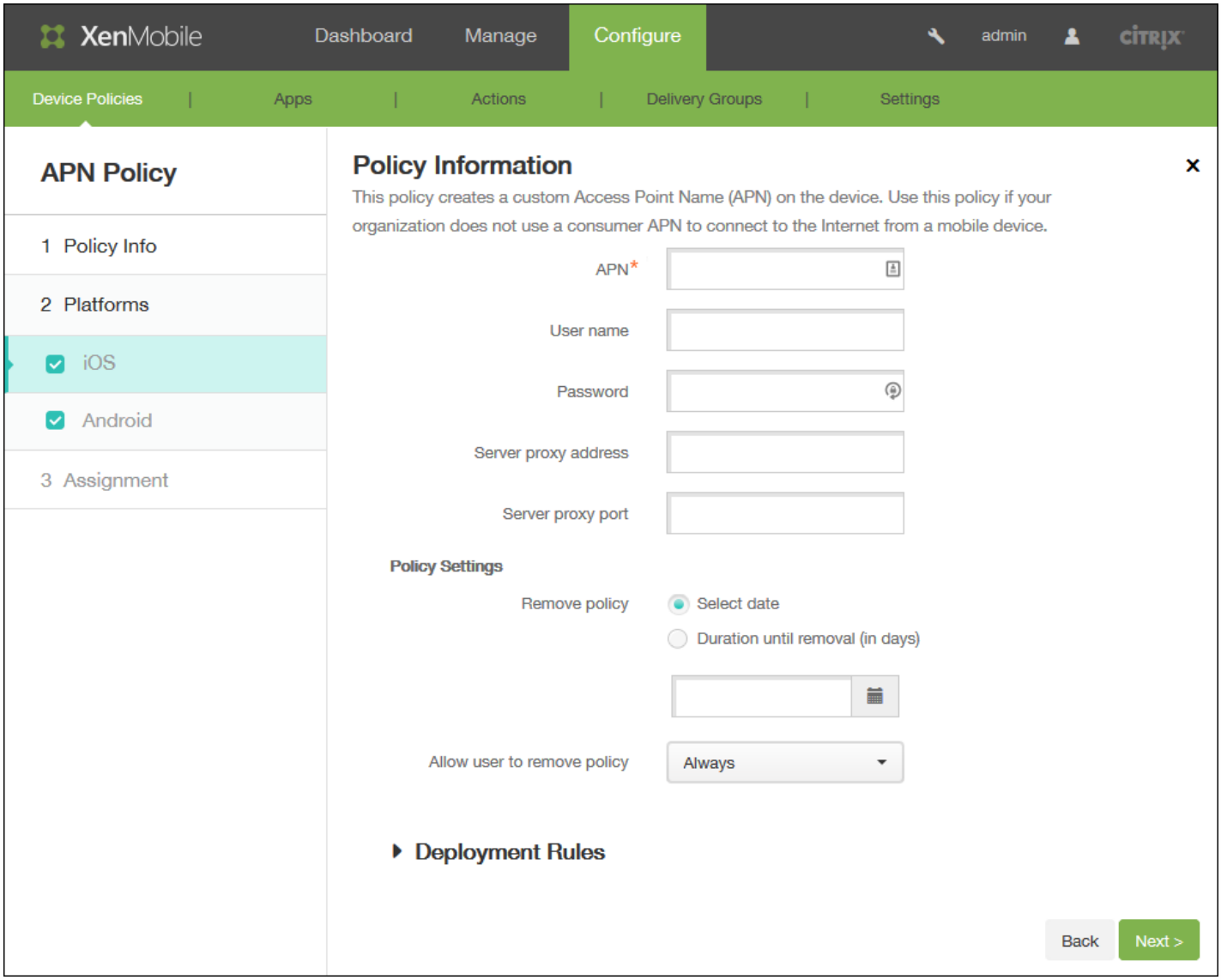
Remarque : lorsque la page **Stratégie par plate-forme** s'affiche, toutes les plates-formes sont sélectionnées et la plate-forme iOS s'affiche en premier.

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.

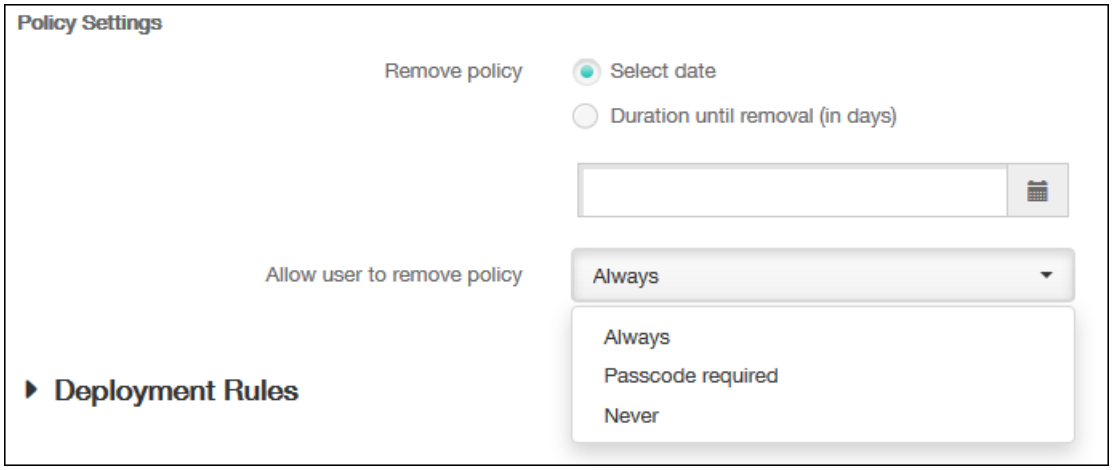
Paramètres iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



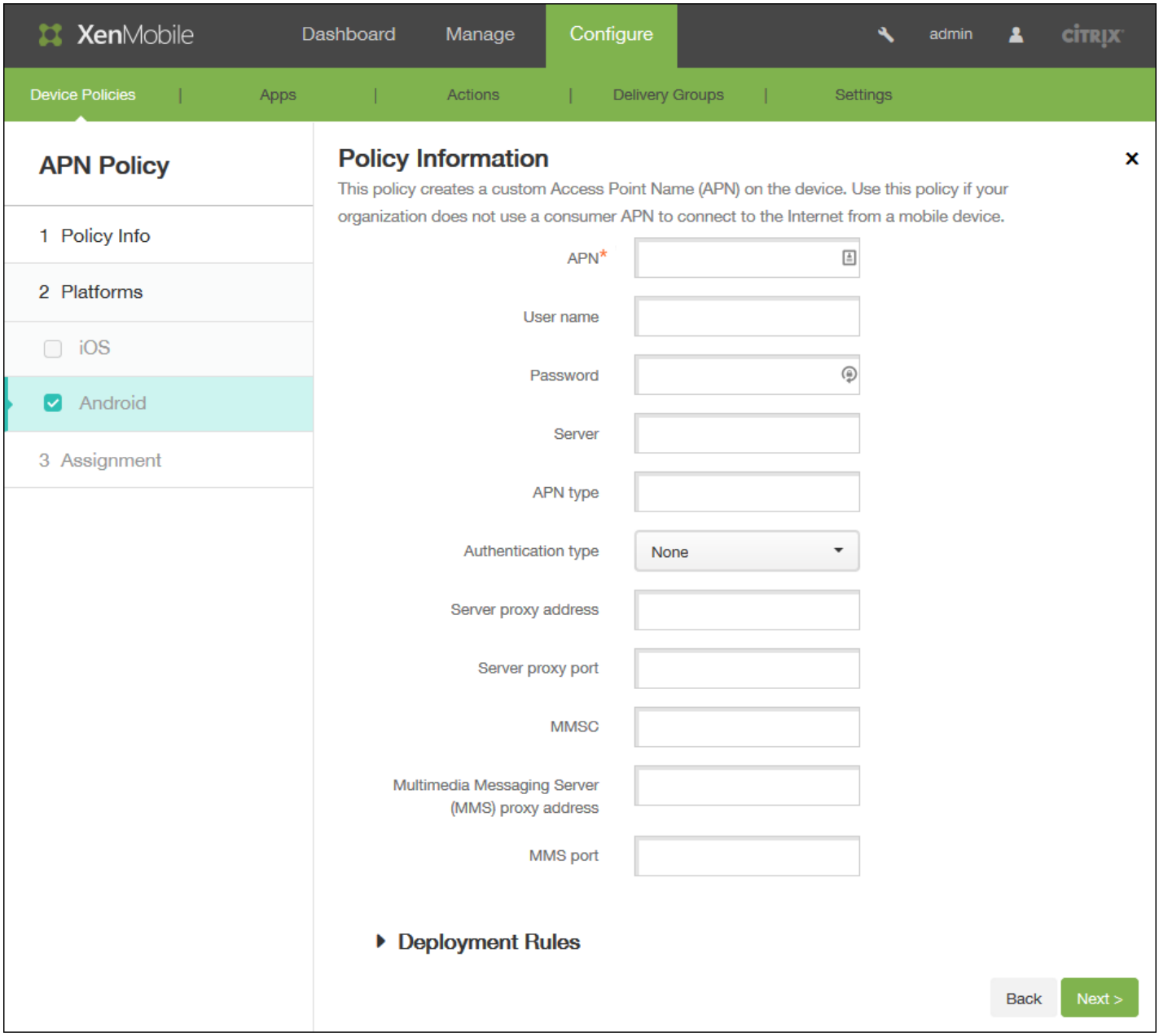
- **APN** : entrez le nom du point d'accès. Ce dernier doit correspondre à un APN iOS accepté ou la stratégie échouera.
- **Nom d'utilisateur**: cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. Si l'argument nom d'utilisateur est manquant, l'appareil invite à saisir la chaîne lors de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Paramètres Android

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

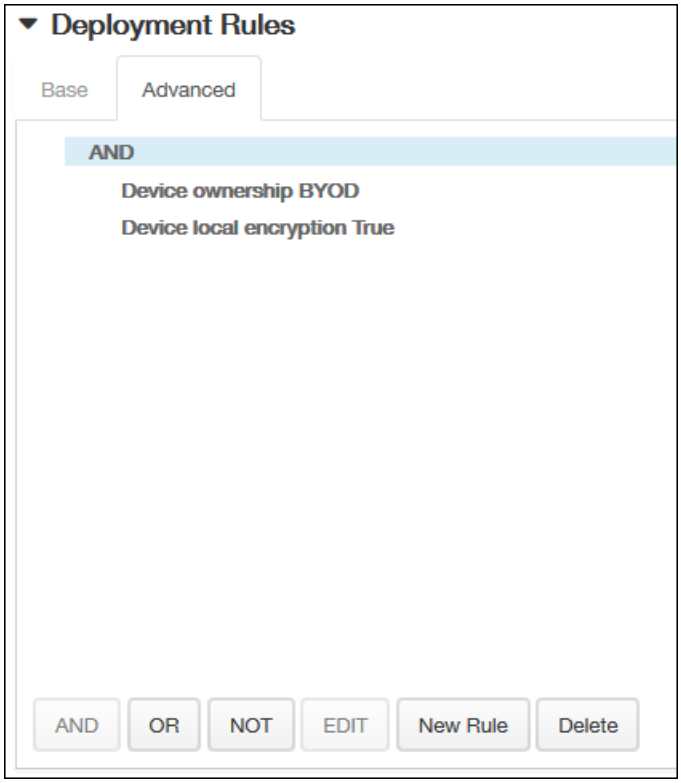
- **Type d'authentification** : dans la liste, cliquez sur le type d'authentification à utiliser. Valeur par défaut Aucun.
- **Adresse du serveur proxy** : adresse IP ou adresse URL du proxy HTTP APN de l'opérateur.
- **Port du serveur proxy** : numéro de port du proxy APN. Nécessaire que si vous avez 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.

7. Développez **Règles de déploiement**, puis configurez les paramètres suivants : L'onglet **Base** s'affiche par défaut.



- Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
  - Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est **Toutes**.
  - Cliquez sur **Nouvelle règle** pour définir les conditions.
  - Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**, comme illustré dans la figure qui précède.
  - Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
- Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes. Les conditions que vous avez choisies sur l'onglet Base s'affichent.

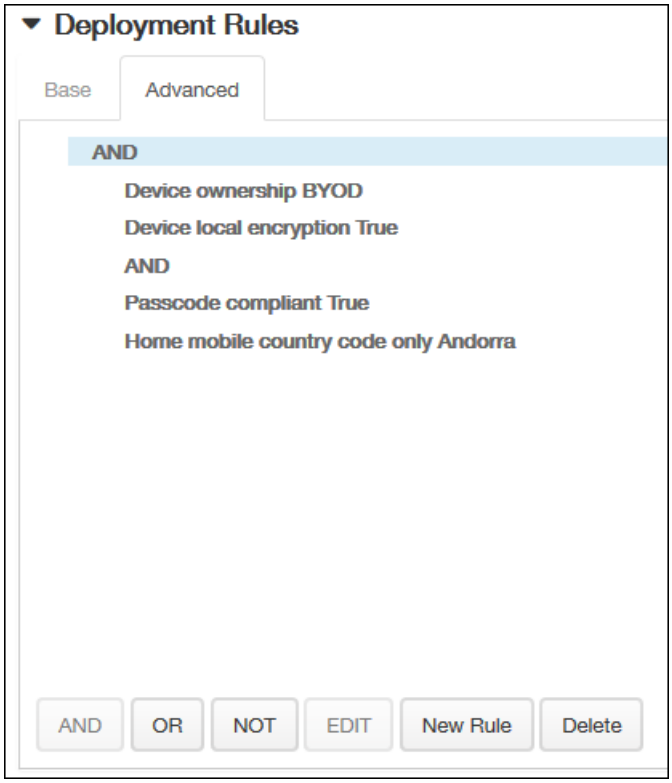
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
  - Cliquez sur **ET**, **OU** ou **SAUF**.
  - Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
    Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.
  - Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions.

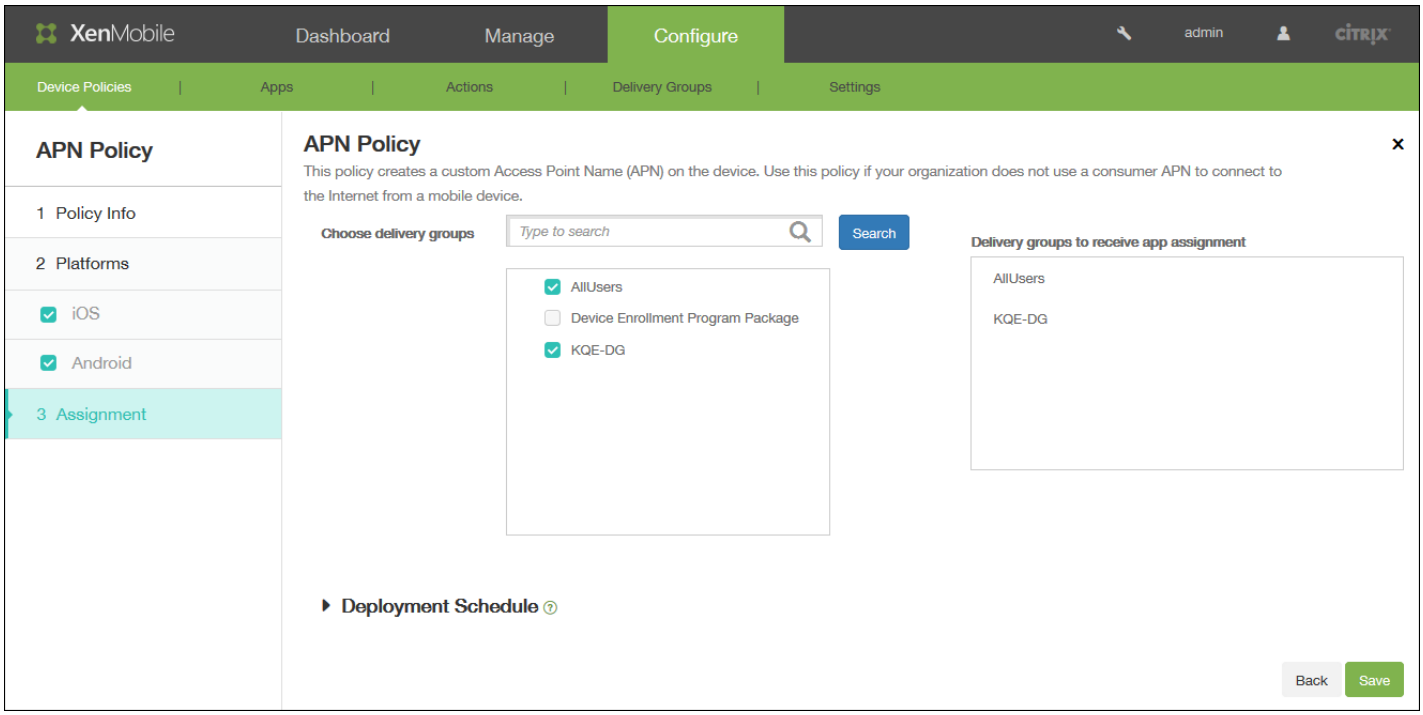
    Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

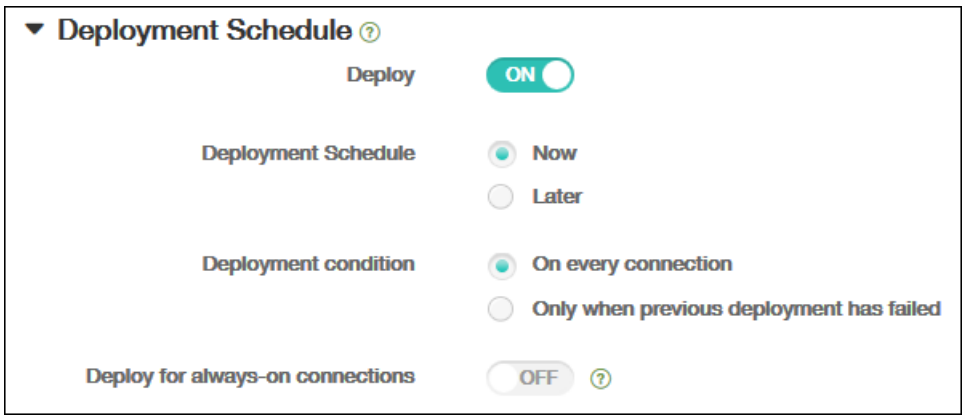
10. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- 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.

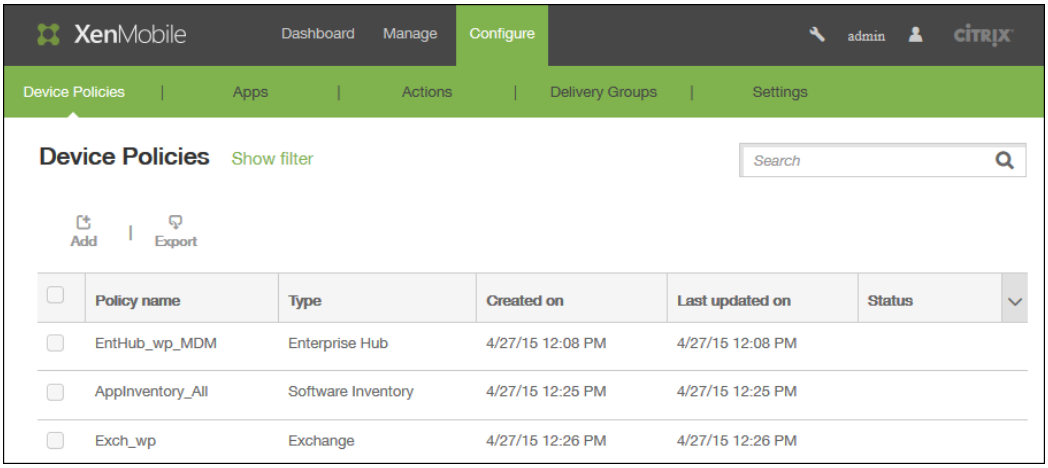
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie cellulaire pour iOS

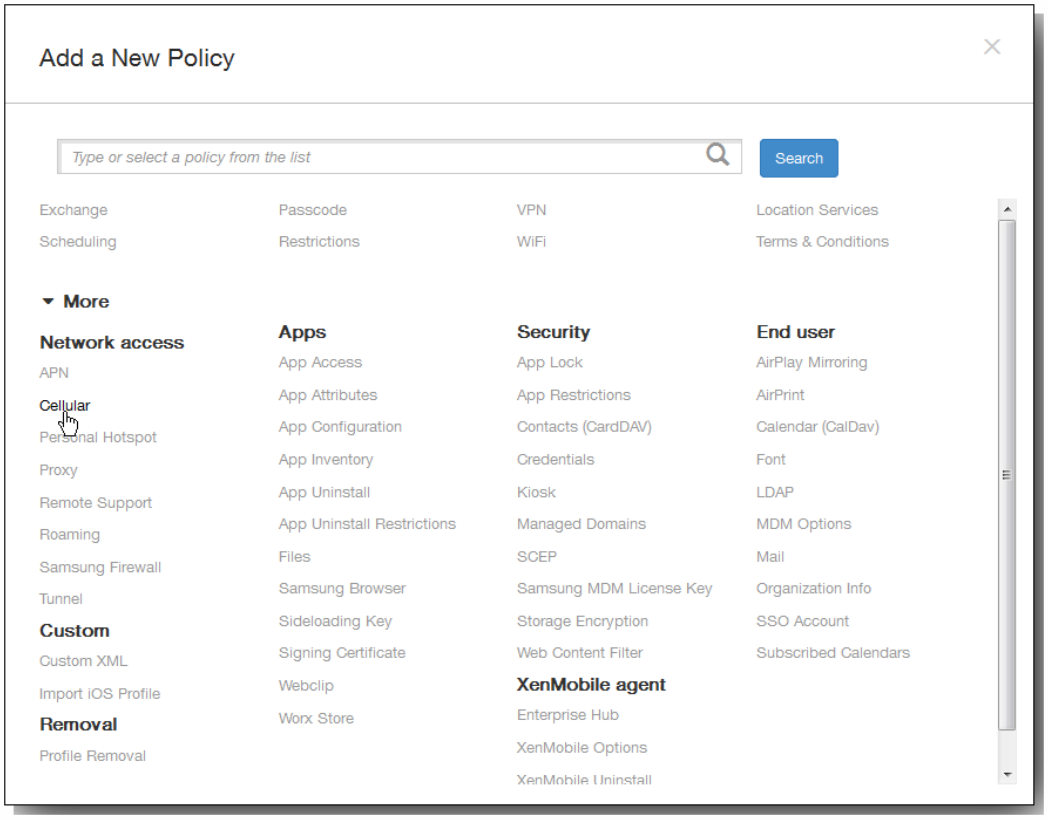
Jul 25, 2016

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.

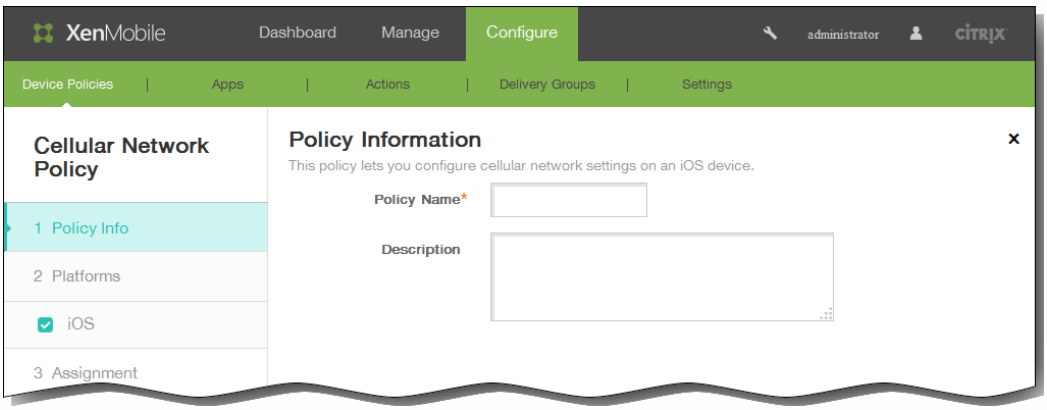


2. Cliquez sur Ajouter.
   La page Ajouter une nouvelle stratégie apparaît.



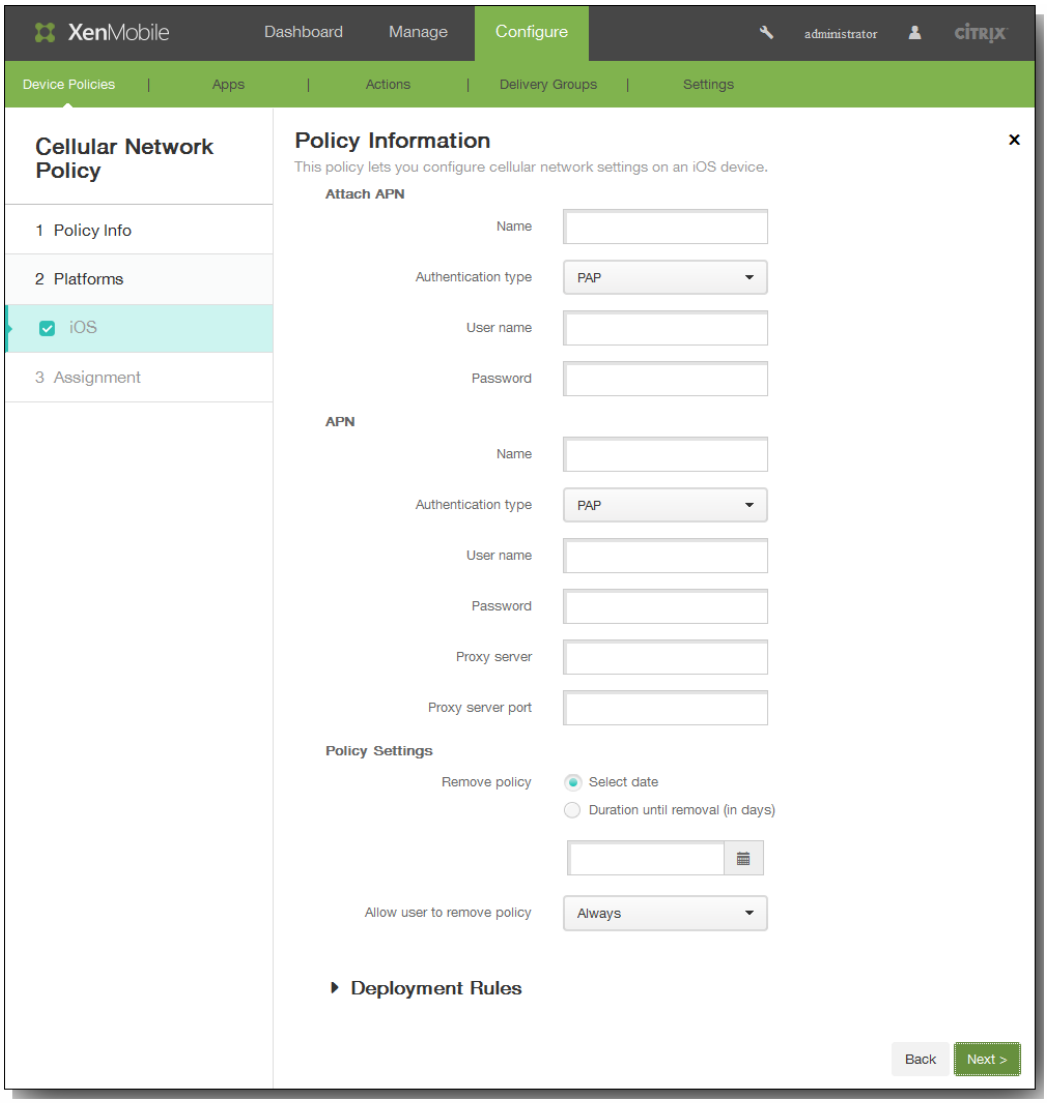
© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Sur la page Ajouter une nouvelle stratégie, cliquez sur 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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

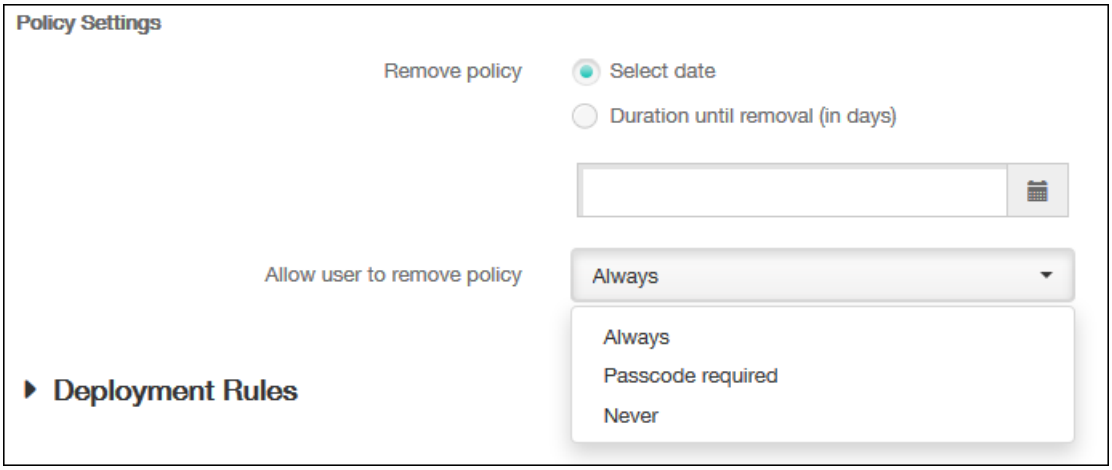


6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes : Sous **Attacher APN** :
   1. Nom : entrez un nom pour cette configuration.
   2. Type d'authentification : dans la liste, cliquez sur CHAP (Challenge Handshake Authentication Protocol) ou PAP (Password Authentication Protocol). La valeur par défaut est PAP.
   3. Nom d'utilisateur : entrez un nom d'utilisateur à utiliser pour l'authentification.
   4. Mot de passe : entrez un mot de passe à utiliser pour l'authentification.

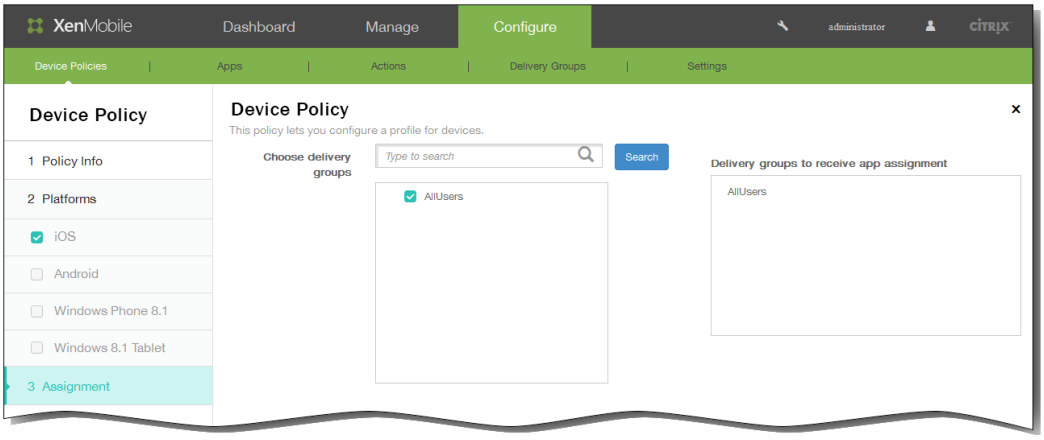
   Sous **APN** :
   1. Nom : entrez un nom pour la configuration du nom du point d'accès (APN).
   2. Type d'authentification : dans la liste, cliquez sur CHAP ou PAP. La valeur par défaut est PAP.
   3. Nom d'utilisateur : entrez un nom d'utilisateur à utiliser pour l'authentification.
   4. Mot de passe : entrez un mot de passe à utiliser pour l'authentification.
   5. Serveur proxy : entrez l'adresse réseau du serveur proxy.
   6. Port du serveur proxy : entrez le port du serveur proxy.
7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.



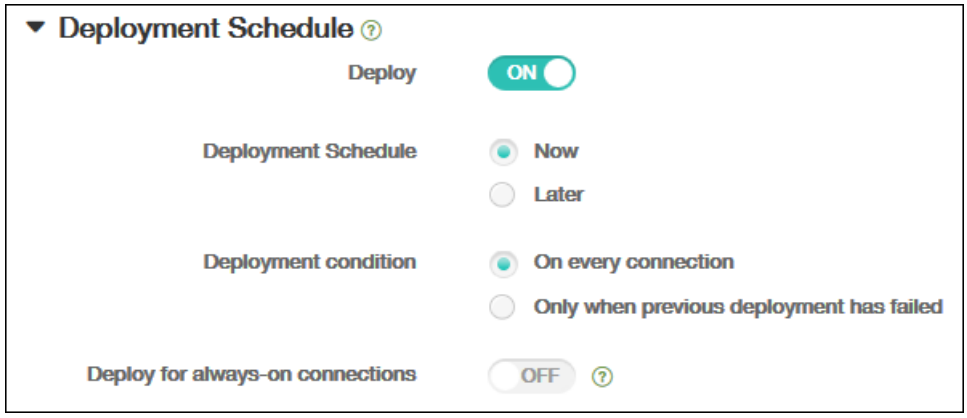
11. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



12. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



13. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour créer une stratégie d'hub d'entreprise pour Windows Phone 8.1

Jul 25, 2016

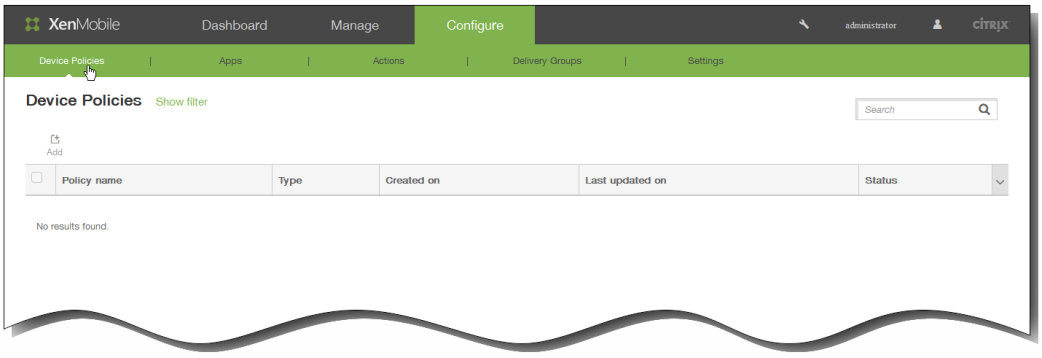
Une stratégie d'hub d'entreprise pour Windows Phone 8.1 vous permet de distribuer des applications d'entreprise via le magasin hub d'entreprise.

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)

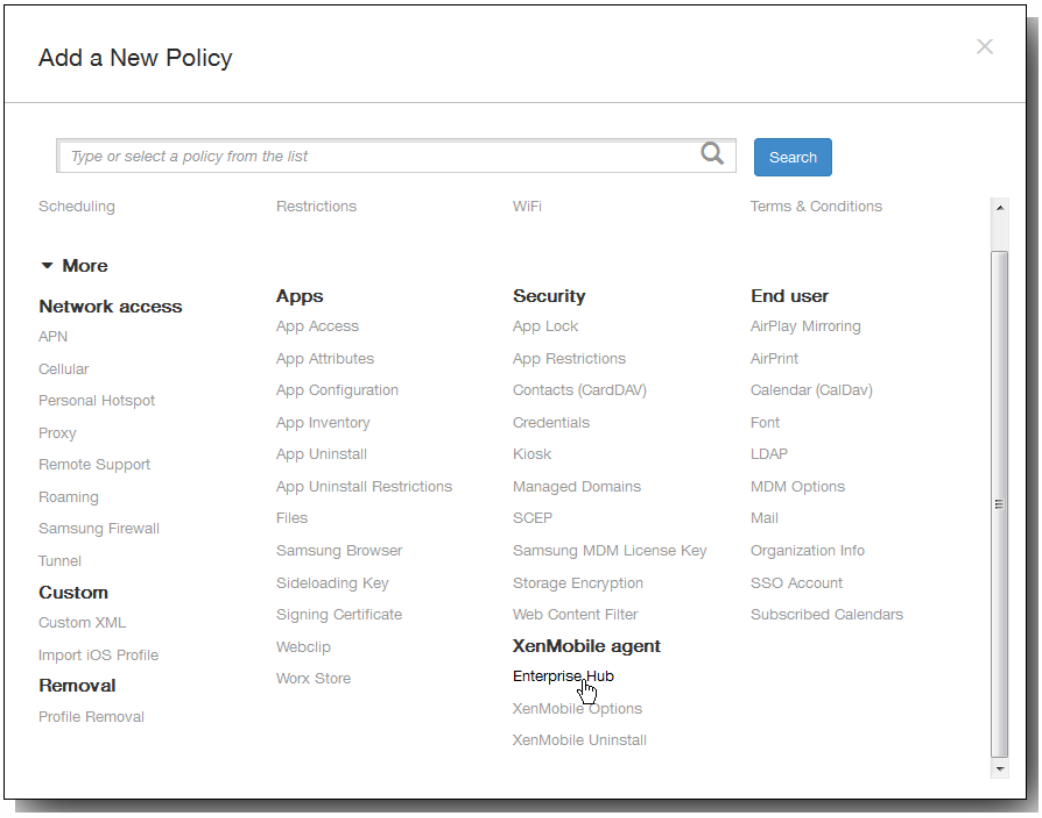
Remarque : XenMobile prend en charge une seule stratégie d'hub d'entreprise pour un mode Windows Phone 8.1 Worx Home. Par exemple, pour télécharger Windows Phone 8.1 Worx Home pour XenMobile Enterprise Edition, vous ne devez pas créer de multiples stratégies d'hub d'entreprise avec différentes versions 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.

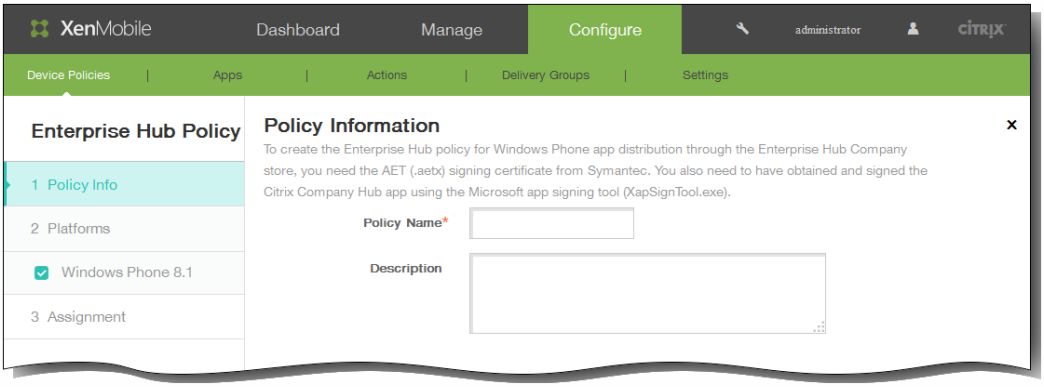


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

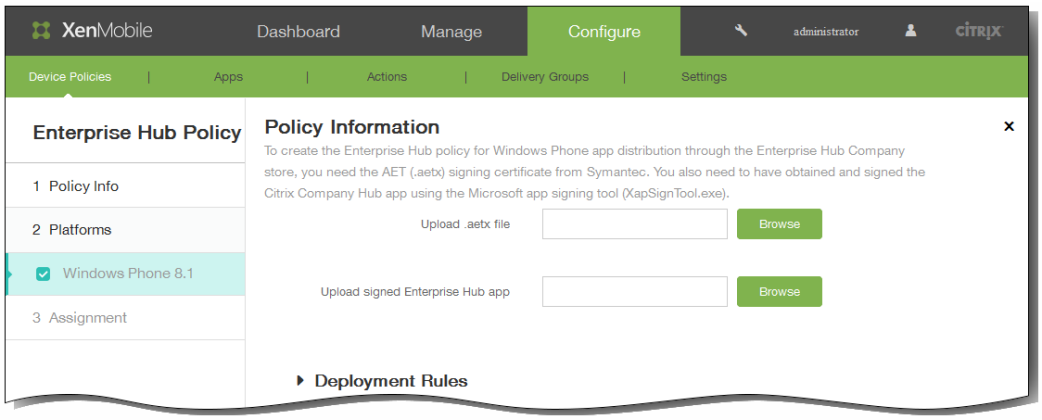


3. Cliquez sur Plus, puis, sous Agent XenMobile, cliquez sur Hub d'entreprise. La page Stratégie d'hub d'entreprise s'affiche.

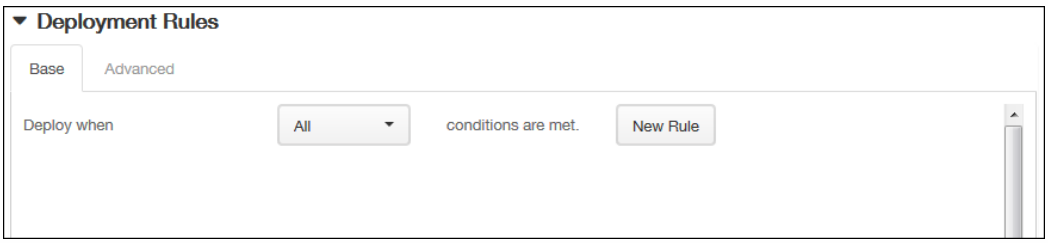


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
    1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
    2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page de plate-forme Windows Phone 8.1 s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

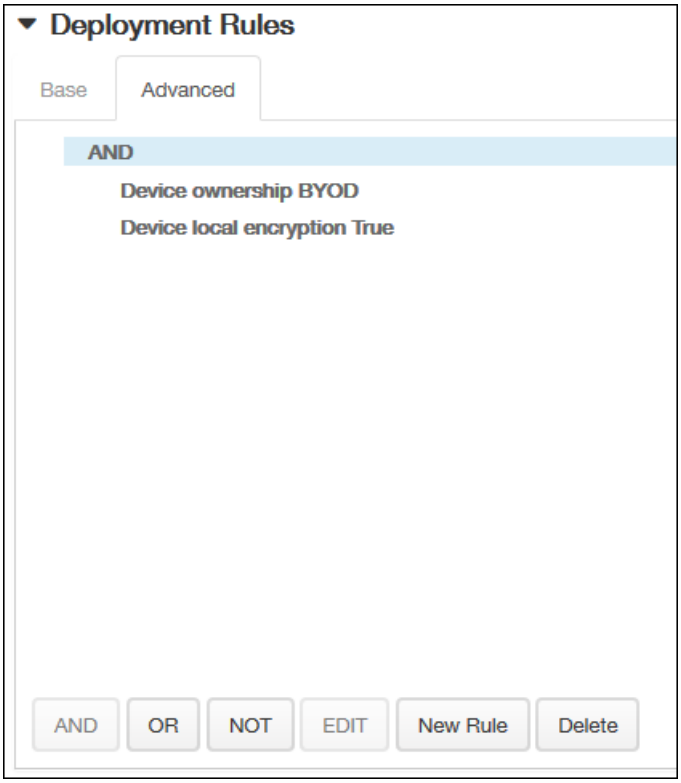


6. Configurez les paramètres suivants :
   1. Charger fichier .aetx : naviguez jusqu'à l'emplacement du fichier .aetx et sélectionnez le fichier.
   2. Charger application d'hub d'entreprise signée : naviguez jusqu'à l'emplacement de l'application d'hub d'entreprise et sélectionnez l'application.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour définir les conditions.
      3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
      4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
   2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

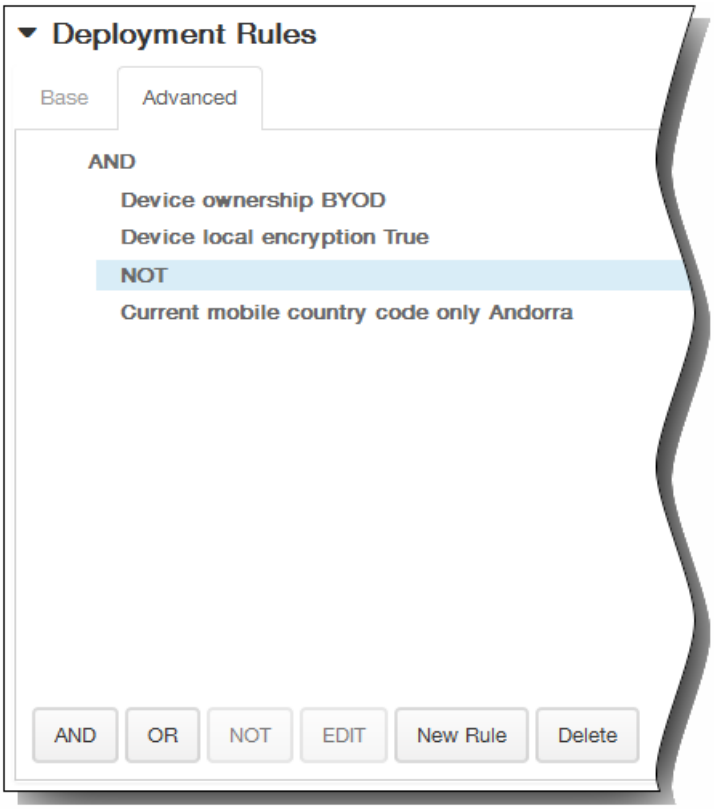


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

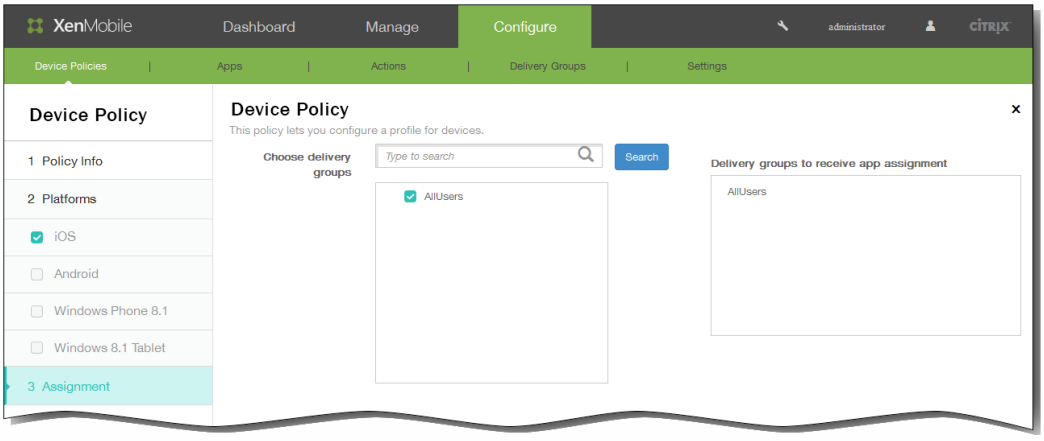
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



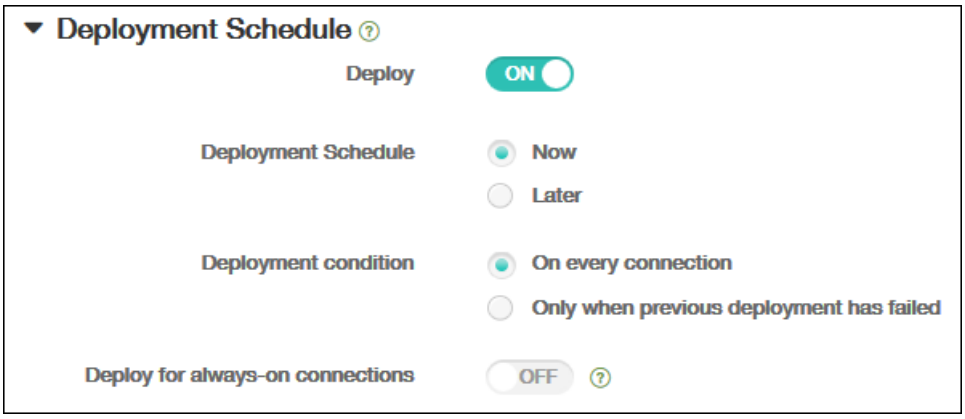
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

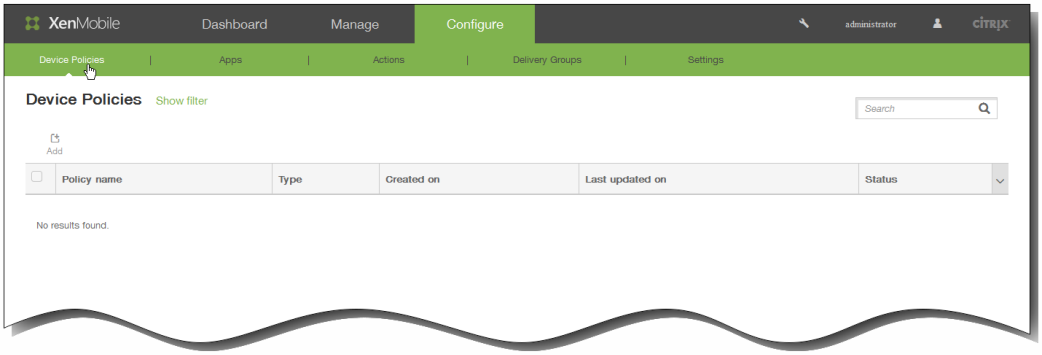
Stratégies Microsoft Exchange ActiveSync

Jul 25, 2016

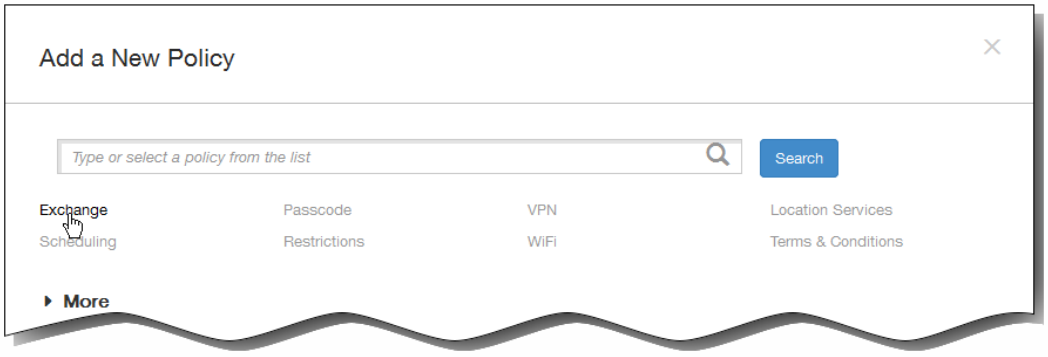
Vous pouvez utiliser la stratégie Exchange ActiveSync pour configurer un client de messagerie sur les appareils des utilisateurs pour leur permettre d'accéder à leur messagerie d'entreprise hébergée sur Exchange. Vous pouvez créer des stratégies pour iOS, Android HTC, Android TouchDown, Android for Work, Samsung SAFE, Samsung KNOX et Windows Phone 8.1. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans les rubriques 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.

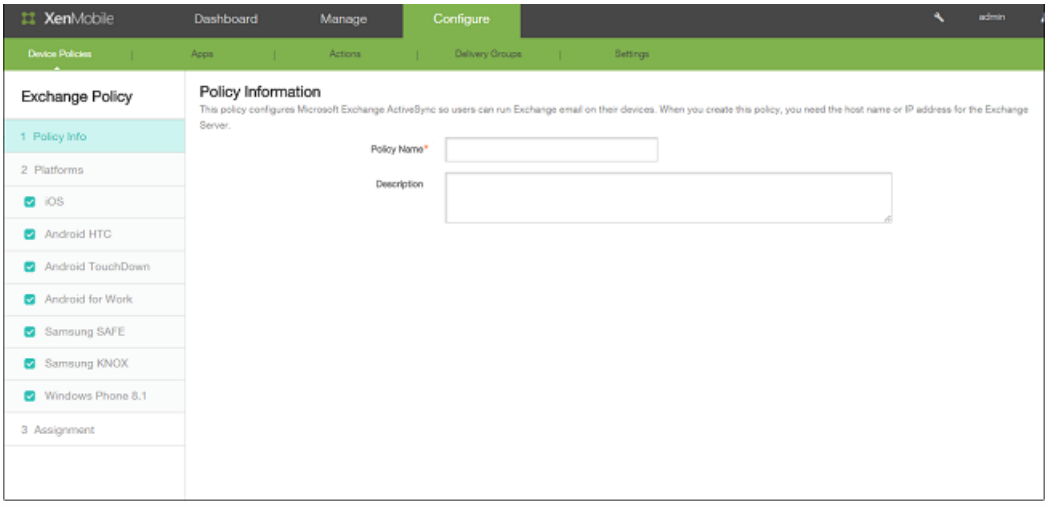


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie s'affiche.



3. Cliquez sur Exchange. La page d'informations Stratégie Exchange s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Dans le panneau Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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 le panneau de configuration de la plate-forme iOS s'affiche en premier.
6. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter.
   - Si vous sélectionnez iOS, configurez les paramètres suivants :

     Nom du compte Exchange ActiveSync : entrez un nom de compte Exchange Server.

     Exchange ActiveSync nom d'hôte: entrez le nom d'hôte du serveur Exchange Server ou son adresse IP.

     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.
     Remarque : 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.
     Remarque : 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.
     Remarque : 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 : sélectionnez un intervalle dans la zone de liste déroulante.

     Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) : facultatif. Sélectionnez les informations d'identification Cert/PKI configurées dans la zone déroulante.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autoriser le déplacement des e-mails entre les comptes : facultatif. Sélectionnez On/Off. La valeur par défaut est Off.

N'envoyer le courrier que depuis l'application de messagerie : facultatif. Sélectionnez On/Off. La valeur par défaut est Off.

Désactiver la synchronisation des courriers récents : facultatif. Sélectionnez On/Off. La valeur par défaut est Off.

Activer S/MIME : facultatif. Sélectionnez On/Off. La valeur par défaut est Off.

Activer commutateur de chiffrement S/MIME par message : facultatif. Sélectionnez On/Off. La valeur par défaut est Off.

- Si vous sélectionnez Android HTC, configurez les paramètres suivants :

  Nom d'affichage de la configuration : entrez le nom de cette stratégie qui s'affiche sur les appareils des utilisateurs.

  Adresse du serveur : tapez le nom d'hôte du serveur Exchange Server ou son adresse IP.

  ID utilisateur : spécifiez le nom d'utilisateur du compte utilisateur Exchange.
  Remarque : 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.
  Remarque : 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.
  Remarque : 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.

- Si vous sélectionnez Android TouchDown, configurez les paramètres suivants :

  Nom du serveur ou adresse IP : tapez le nom d'hôte du serveur Exchange Server ou son adresse IP.

  Domaine : entrez le domaine dans lequel réside le serveur Exchange.
  Remarque : 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.
  Remarque : 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.
  Remarque : vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes de messagerie des utilisateurs.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 None.

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.

- Si vous avez sélectionné **Android for Work**, configurez les paramètres suivants :

  Nom du serveur ou adresse IP : entrez le nom d'hôte du serveur Exchange Server ou son adresse IP.

  Domaine : entrez le domaine dans lequel le serveur Exchange réside.
  Remarque : vous pouvez utiliser la macro système **${user.domainname}** dans ce champ pour rechercher automatiquement les noms de domaine d'utilisateurs.

  ID utilisateur : spécifiez le nom d'utilisateur du compte utilisateur Exchange.
  Remarque : vous pouvez utiliser la macro système **${user.username}** dans ce champ pour rechercher automatiquement les noms d'utilisateur.

  Mot de passe : entrez un mot de passe pour le compte utilisateur Exchange.

  Adresse e-mail : spécifiez l'adresse complète de l'utilisateur.
  Remarque : vous pouvez utiliser la macro système **${user.mail}** dans ce champ pour rechercher automatiquement les comptes e-mail 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 None.

- Si vous sélectionnez Samsung SAFE ou Samsung KNOX, configurez les paramètres suivants :

  Nom du serveur ou adresse IP : tapez le nom d'hôte du serveur Exchange Server ou son adresse IP.

  Domaine : entrez le domaine dans lequel le serveur Exchange réside.
  Remarque : vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaine d'utilisateurs.

  ID utilisateur : spécifiez le nom d'utilisateur du compte utilisateur Exchange.
  Remarque : vous pouvez utiliser la macro système ${user.username} dans ce champ pour rechercher automatiquement les noms d'utilisateur.

  Mot de passe : entrez un mot de passe pour le compte utilisateur Exchange.

  Adresse e-mail : spécifiez l'adresse complète de l'utilisateur.
  Remarque : vous pouvez utiliser la macro système ${user.mail} dans ce champ pour rechercher automatiquement les comptes e-mail 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exchange requiert l'authentification du certificat client. La valeur par défaut est None.

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.

- Si vous sélectionnez Windows Phone 8.1, configurez les paramètres suivants.

  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 : tapez le nom d'hôte du serveur Exchange Server ou son adresse IP.

  Domaine : entrez le domaine dans lequel réside le serveur Exchange.
  Remarque : 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.
  Remarque : 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.
  Remarque : 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.

  Périodicité : dans la liste, cliquez sur le calendrier à utiliser lors de la synchronisation des données envoyées à partir du serveur Exchange.

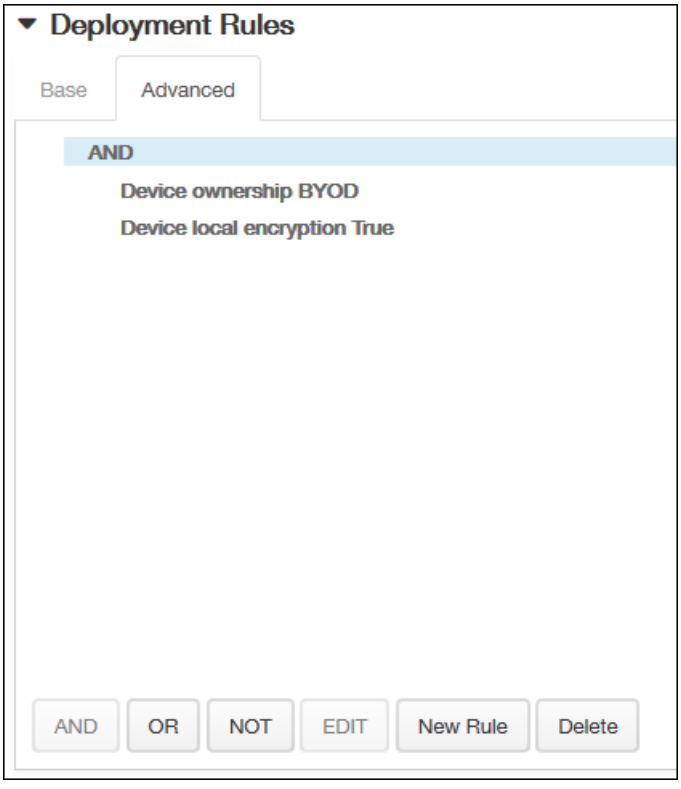
  Niveau d'enregistrement : dans la liste, cliquez sur Désactivé, De base ou Avancé pour spécifier le niveau de détail lors de la journalisation des activités Exchange.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

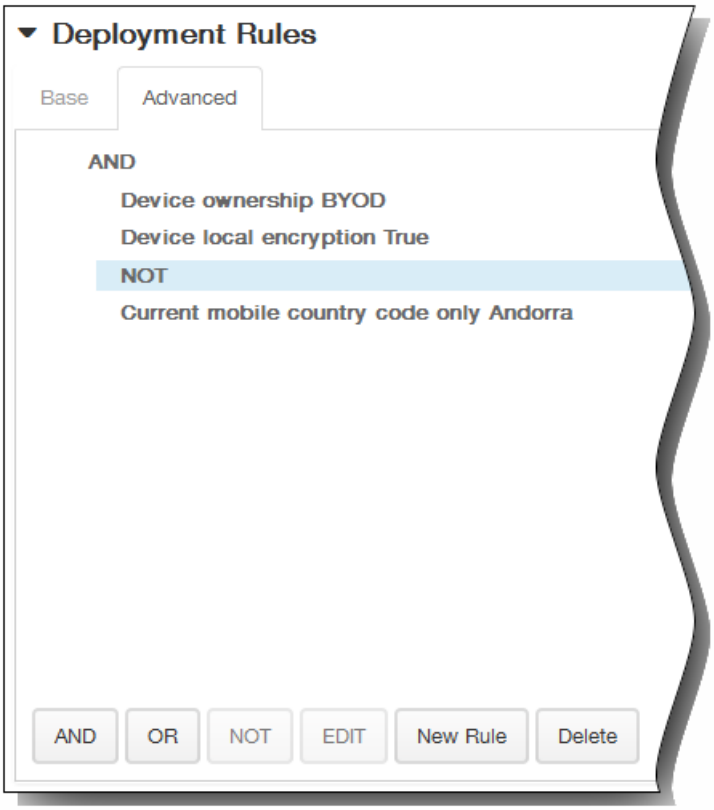


   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la

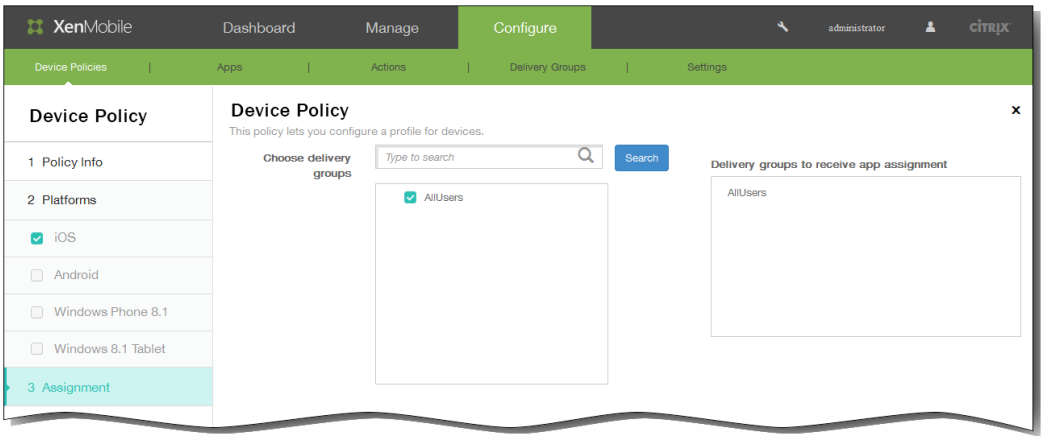
© 1999-2017 Citrix Systems, Inc. All rights reserved.

condition ou sur Supprimer pour supprimer la condition.

3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
   Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



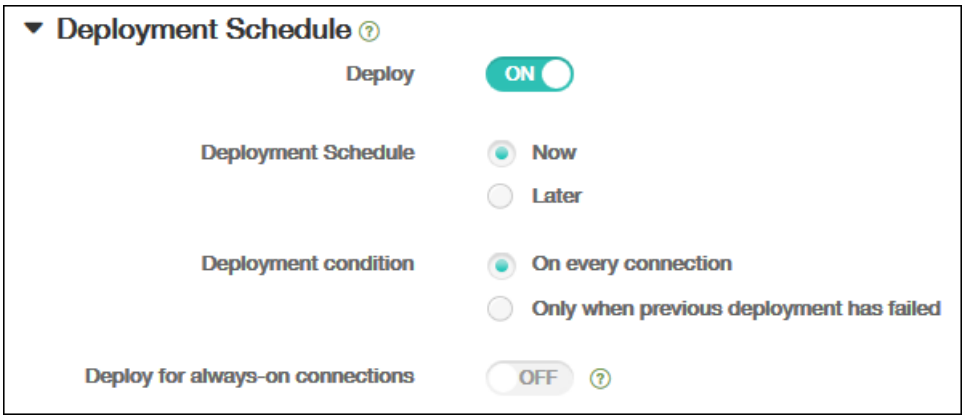
8. Cliquez sur Suivant. La page d'attribution de la Stratégie Exchange s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.



11. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

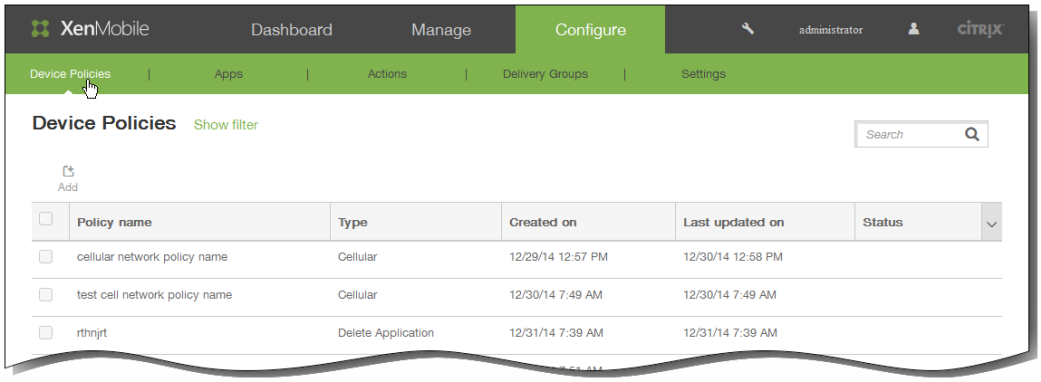
Stratégies d'emplacement

Jul 25, 2016

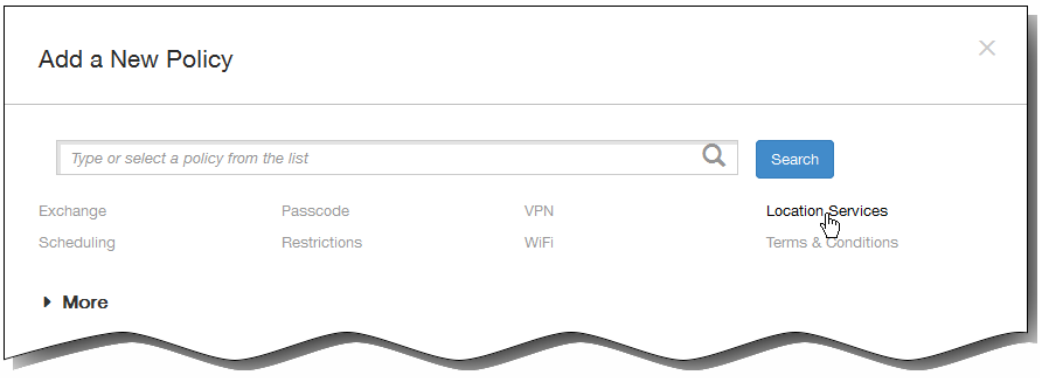
Vous pouvez créer des stratégies d'emplacement dans XenMobile pour imposer des limites géographiques, et suivre l'emplacement et les déplacements des appareils des utilisateurs. Lorsque les utilisateurs violent le périmètre défini, également appelé géofencing, XenMobile peut effacer immédiatement toutes 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.

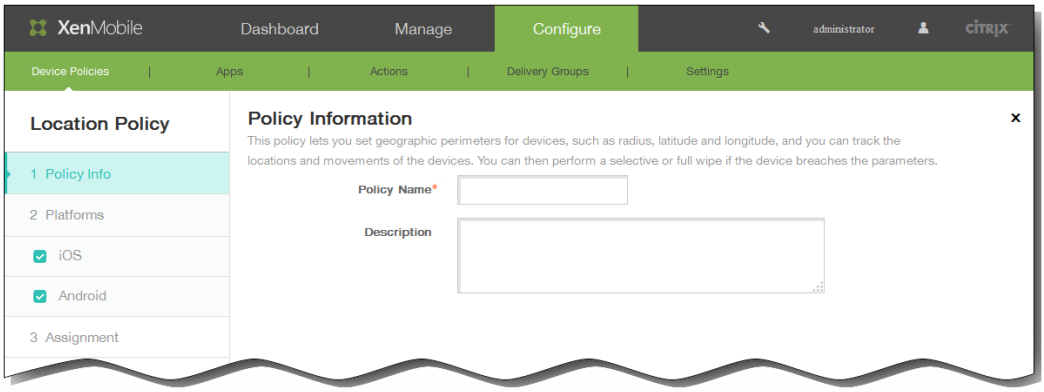


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

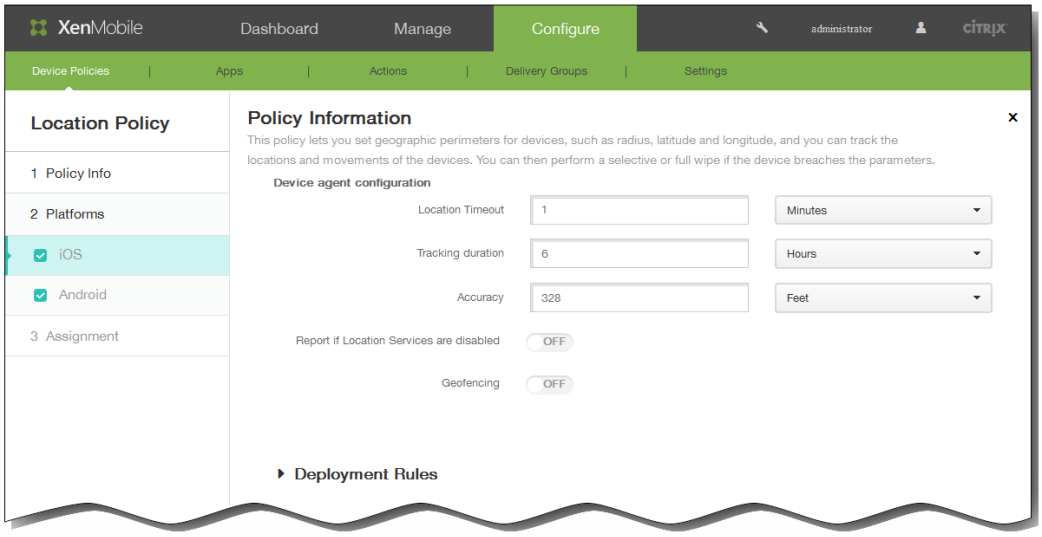


3. Cliquez sur Services de localisation. La page d'informations Stratégie d'emplacement s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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, les deux plates-formes sont sélectionnées et le panneau de configuration de la plate-forme iOS s'affiche en premier.



6. Sous Plates-formes, sélectionnez les plates-formes que vous souhaitez ajouter.
   - Si vous sélectionnez iOS, configurez les paramètres suivants :
     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.

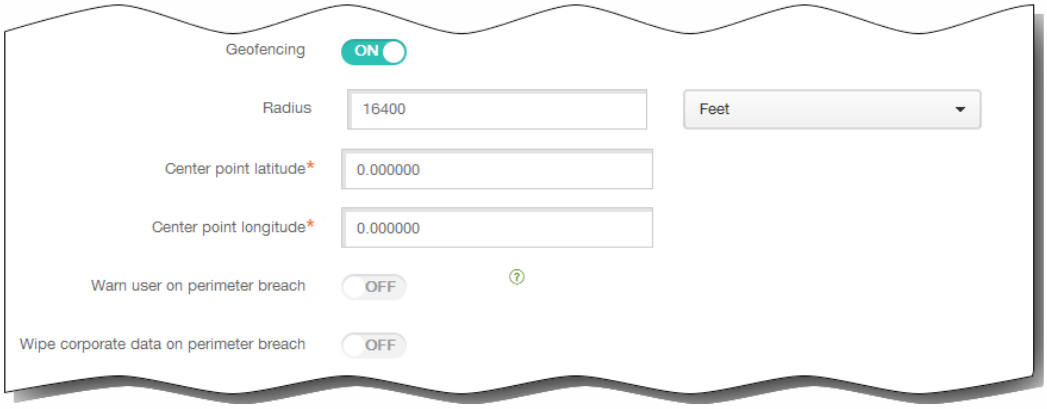
     Durée du suivi : entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée pendant laquelle XenMobile suit l'appareil. Les valeurs valides sont 1 à 6 heures ou 10 à 360 minutes. La valeur par défaut est 6 heures.

     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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 : sélectionnez cette option pour configurer 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.
- 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.

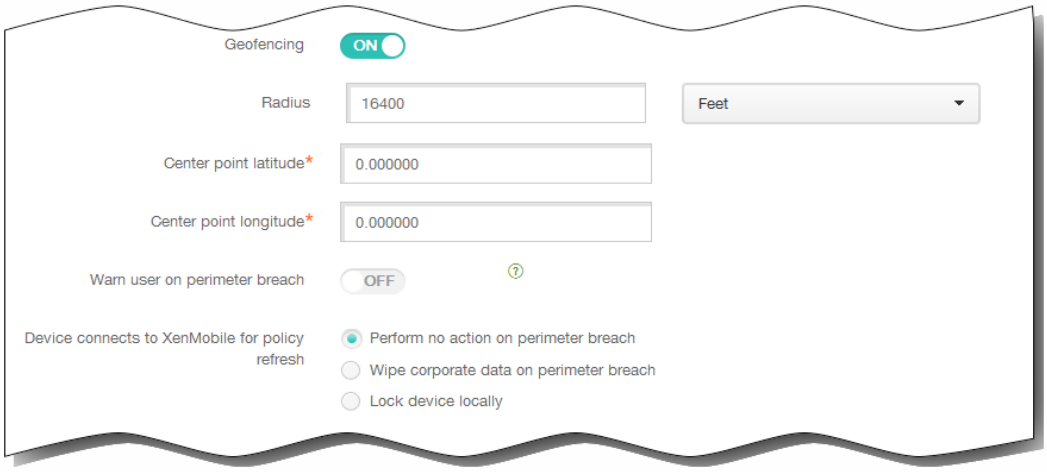
  Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant l'effacement des données d'entreprise sur les appareils des utilisateurs. Cela offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile n'efface leurs appareils. La durée par défaut est de 0 secondes.

- Si vous avez sélectionné Android, configurez les paramètres suivants :
  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.
  Remarque : si la valeur définie est inférieure à 10 minutes, cela peut avoir un impact négatif sur l'autonomie de la

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 : sélectionnez cette option pour configurer 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Délai du verrouillage : verrouille les appareils des utilisateurs après une période spécifiée. Lorsque vous activez cette option, le champ Délai du verrouillage s'affiche.

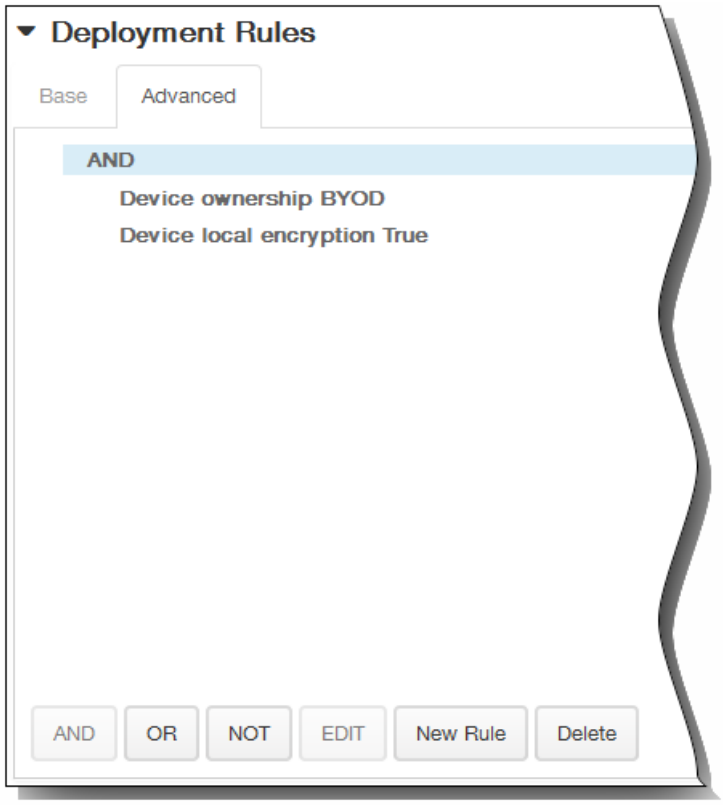
  Entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la durée du délai avant le verrouillage des appareils des utilisateurs. Cela offre aux utilisateurs la possibilité de revenir à l'emplacement autorisé avant que XenMobile ne verrouille leurs appareils. La durée par défaut est de 0 secondes.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

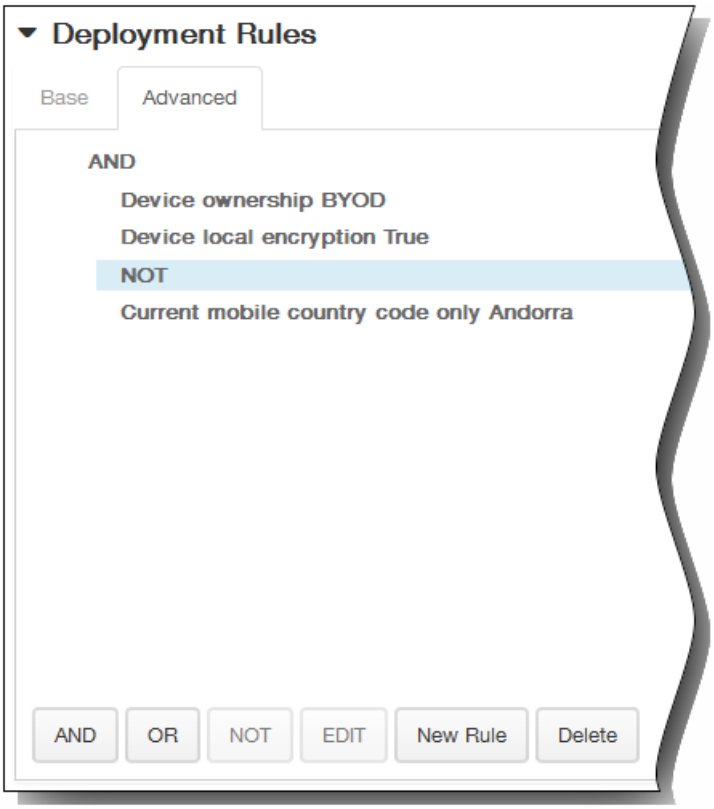


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

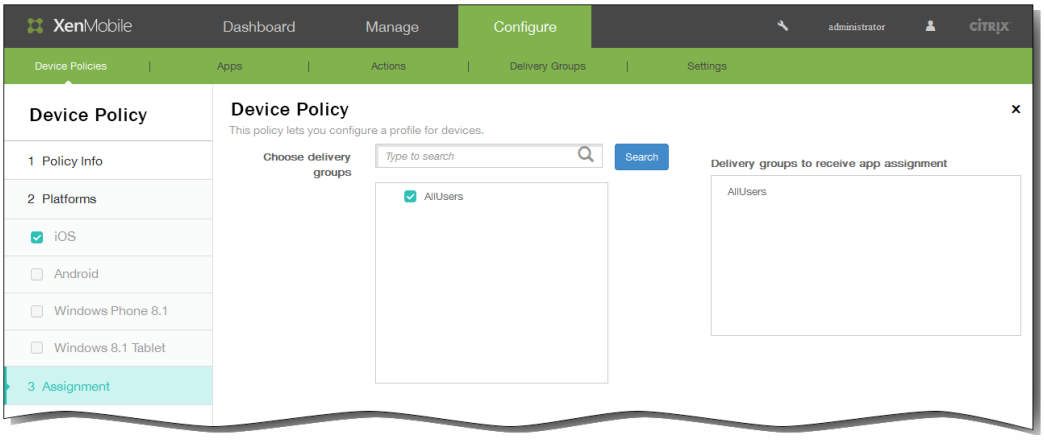
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



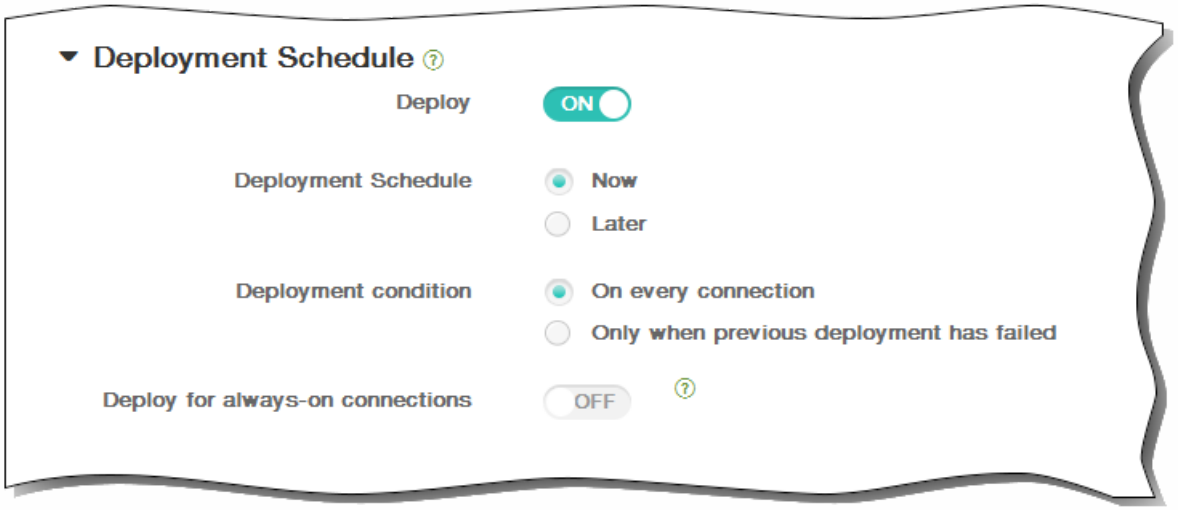
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

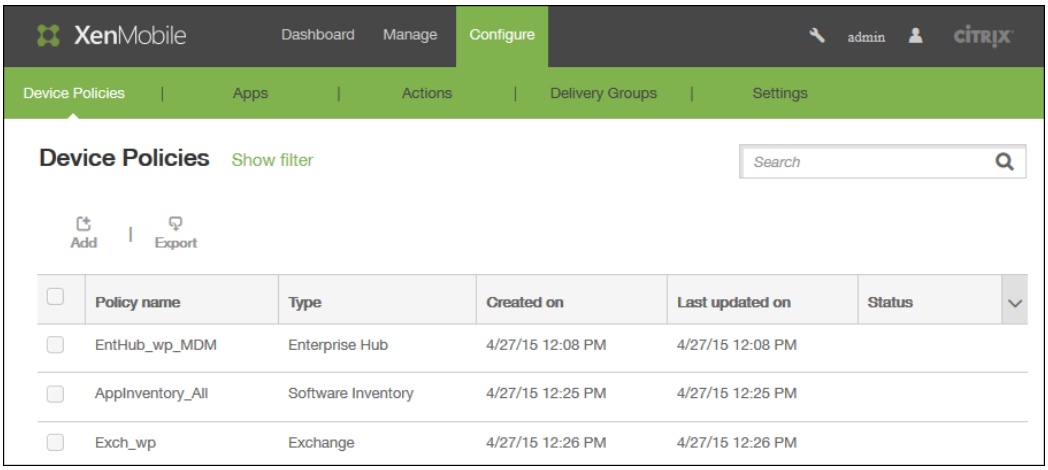
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies de planification de connexion

Jul 25, 2016

Vous pouvez créer des stratégies de planification de connexion afin de contrôler comment et quand les appareils Android et Symbian se connectent à XenMobile. 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 pour ajouter une nouvelle stratégie. 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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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, les deux plates-formes sont sélectionnées et le panneau de configuration de la plate-forme Android s'affiche en premier.
6. Sous Plates-formes, sélectionnez les plates-formes que vous souhaitez ajouter.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
     Cette option n'est pas recommandée car elle décharge la batterie et génère un trafic réseau important.

   - Jamais : connexion manuelle. Les utilisateurs doivent lancer la connexion depuis XenMobile sur leurs appareils.
   - Toutes les : se connecte à l'intervalle défini. Les appareils se connectent automatiquement après un nombre défini de minutes.
     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 20.

   - Définir un calendrier : 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. La section suivante décrit comment définir un délai de connexion.
     Pour définir 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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).

8. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

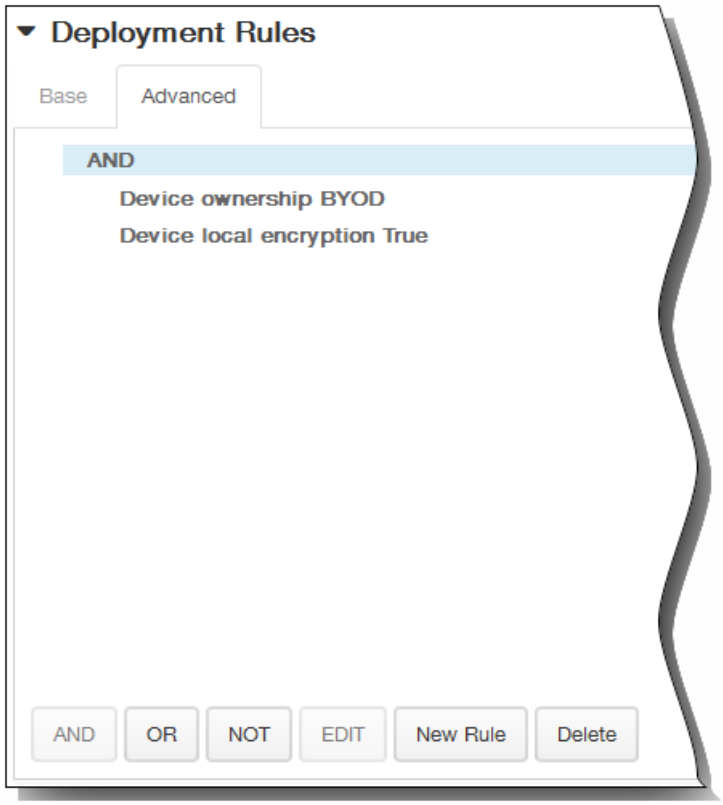


1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

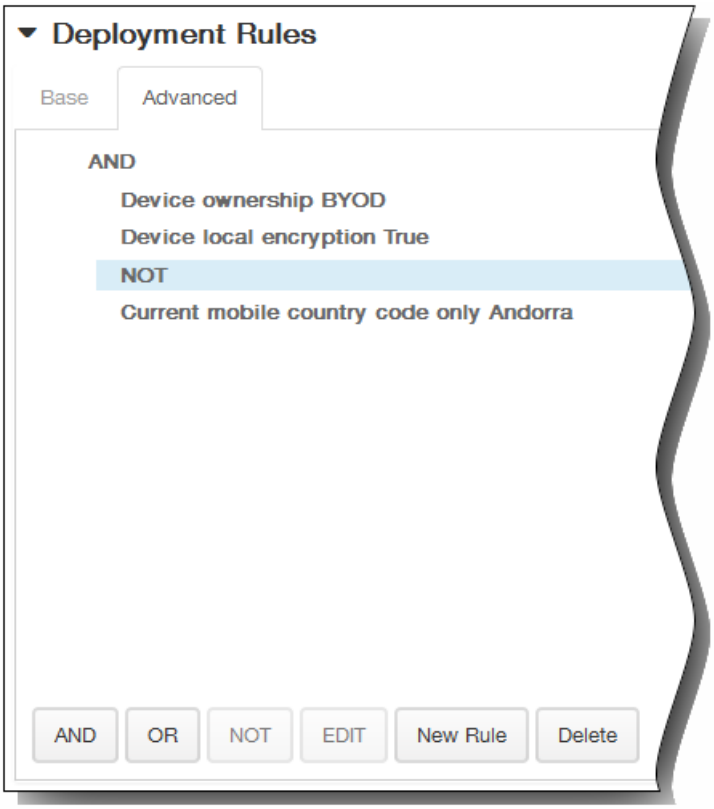
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

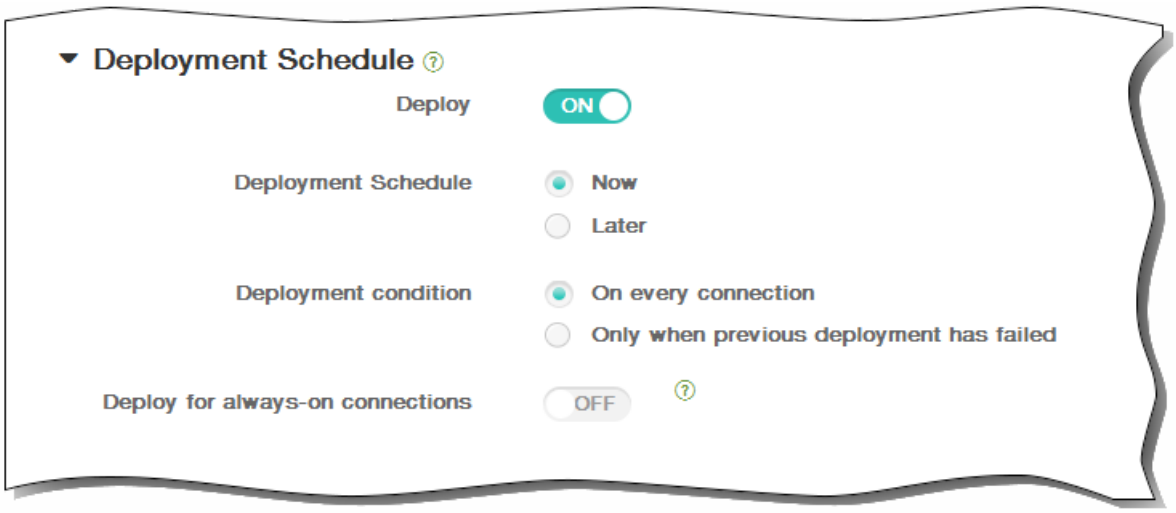
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.
11. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de mise en miroir AirPlay pour iOS

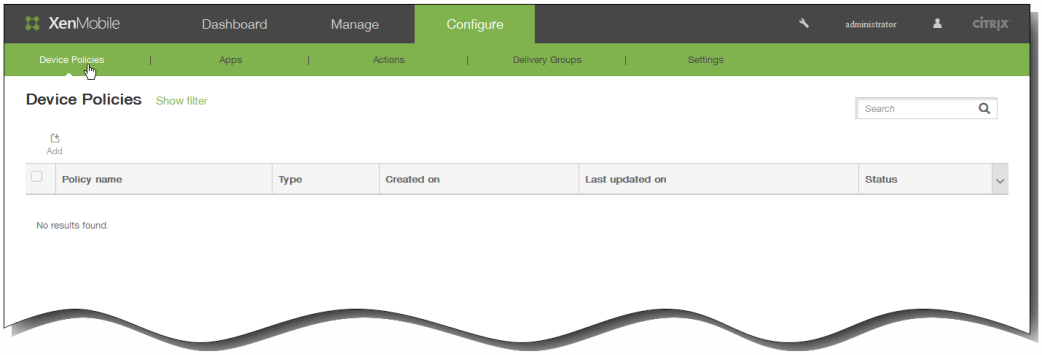
Jul 25, 2016

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.

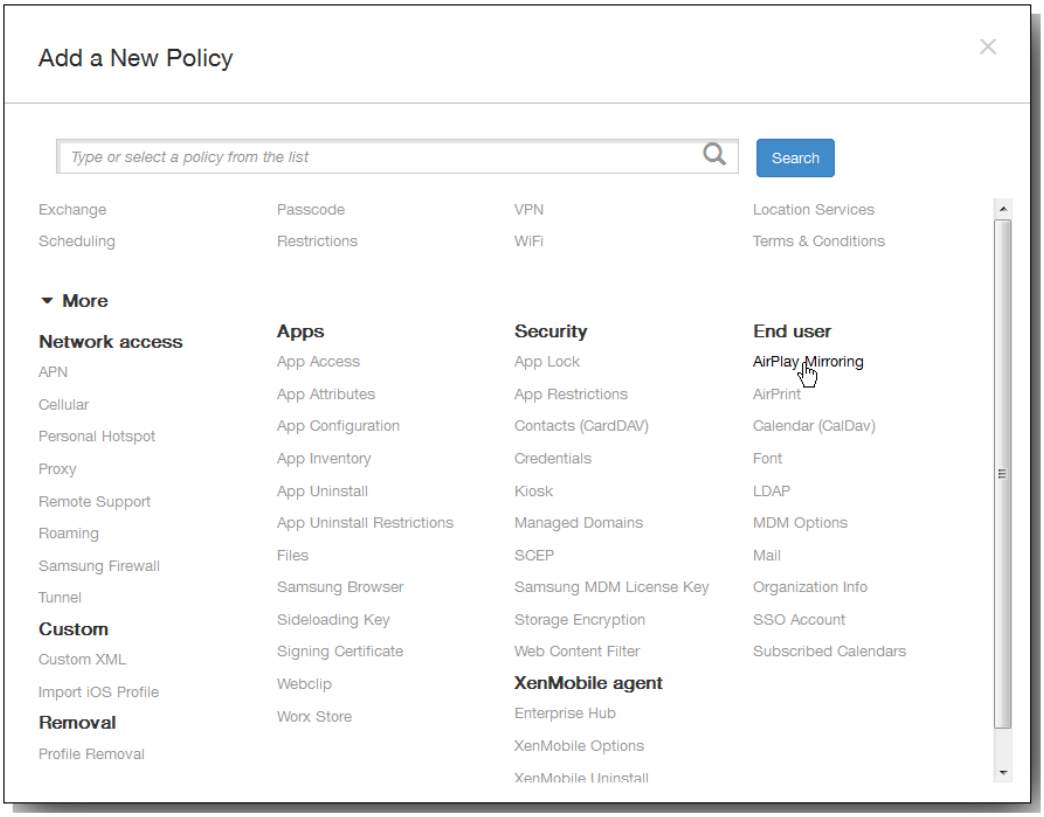
Remarque : avant de continuer, vérifiez que vous disposez des ID et des mots de passe de tous les appareils que vous voulez ajouter.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

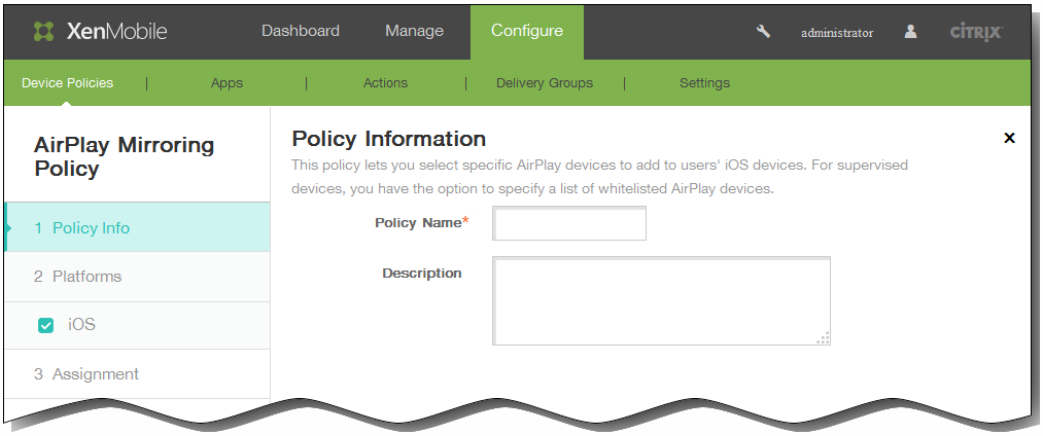


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

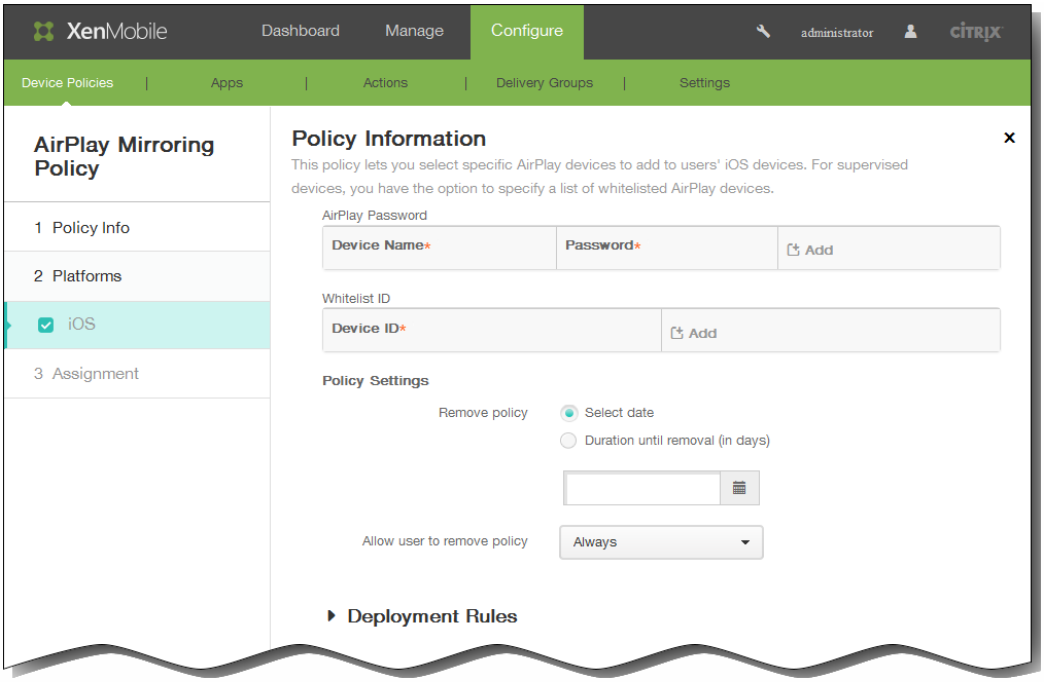


3. Cliquez sur Plus, puis sous Utilisateur final, cliquez sur Mise en miroir AirPlay. La page Stratégie de mise en miroir AirPlay s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



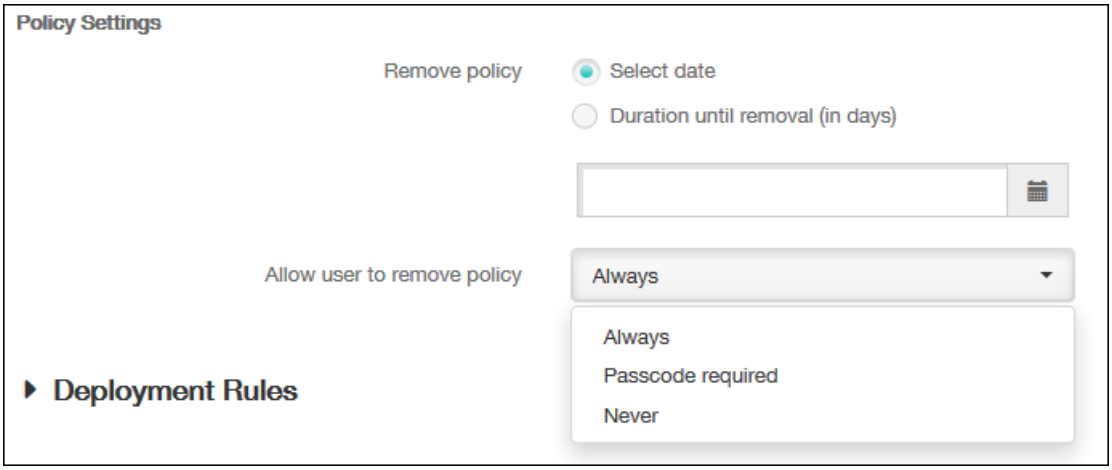
6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Mot de passe AirPlay : cliquez sur Ajouter et procédez comme suit :
      1. ID de l'appareil : entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
      2. Mot de passe : entrez un mot de passe pour l'appareil (facultatif).
      3. Cliquez sur Ajouter pour ajouter l'appareil ou cliquez sur Annuler pour annuler l'ajout de l'appareil.
      4. Répétez les étapes i à iii pour chaque appareil que vous souhaitez ajouter.
   2. ID de liste blanche : cliquez sur Ajouter, puis procédez comme suit pour limiter les appareils supervisés aux ID d'appareils figurant sur la liste blanche :
      Remarque : cette liste est ignorée pour les appareils non supervisés.
      1. 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.
      2. Cliquez sur Ajouter pour ajouter l'appareil ou cliquez sur Annuler pour annuler l'ajout de l'appareil.
      3. Répétez les étapes i et ii pour chaque appareil que vous voulez ajouter à la liste blanche.

      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.

7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

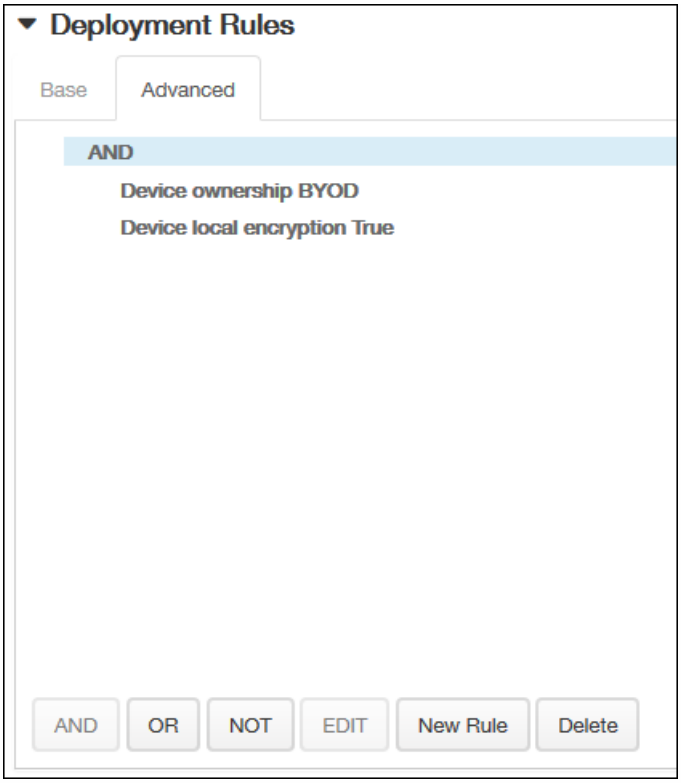


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

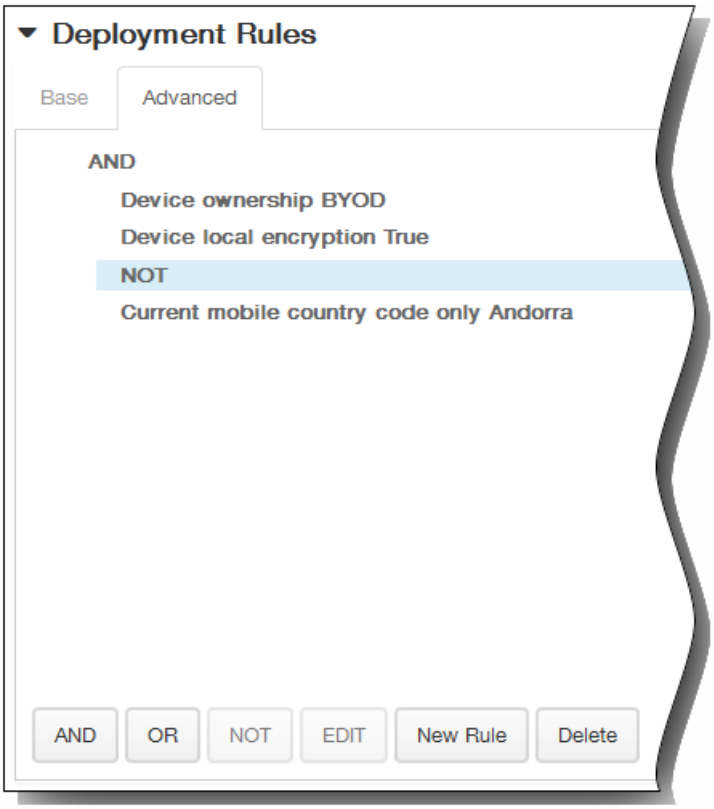


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

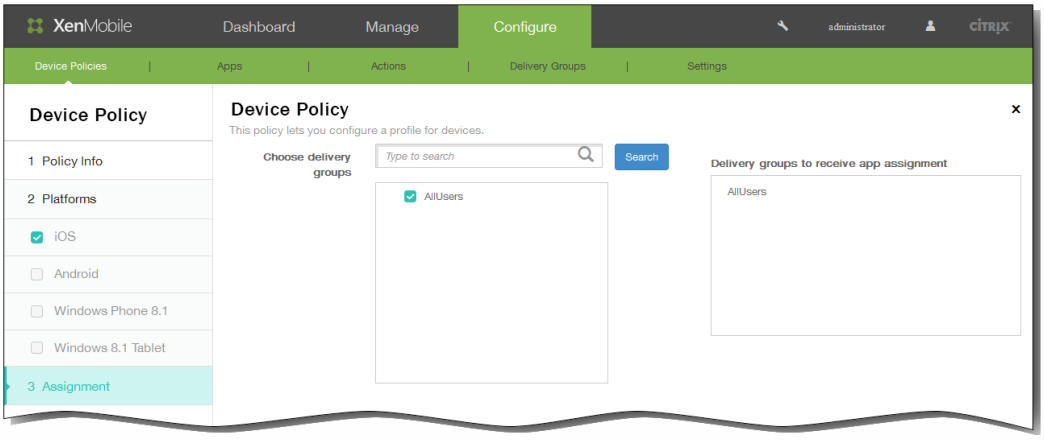
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de mise en miroir AirPlay s'affiche.
13. 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.



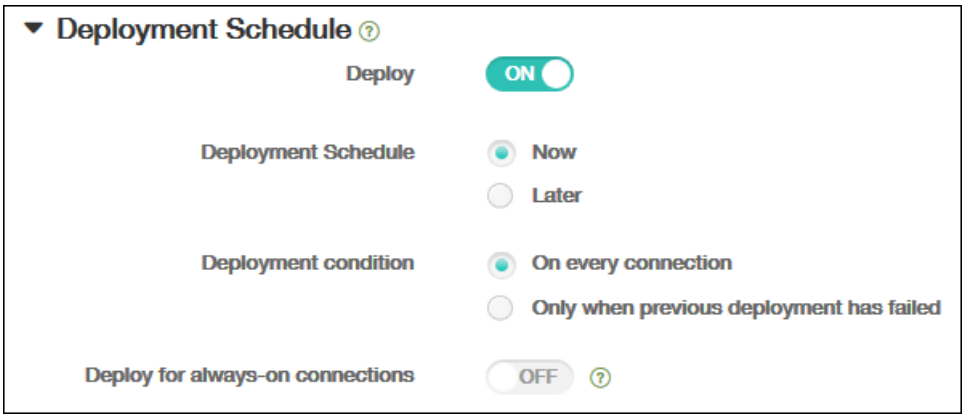
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie AirPrint pour iOS

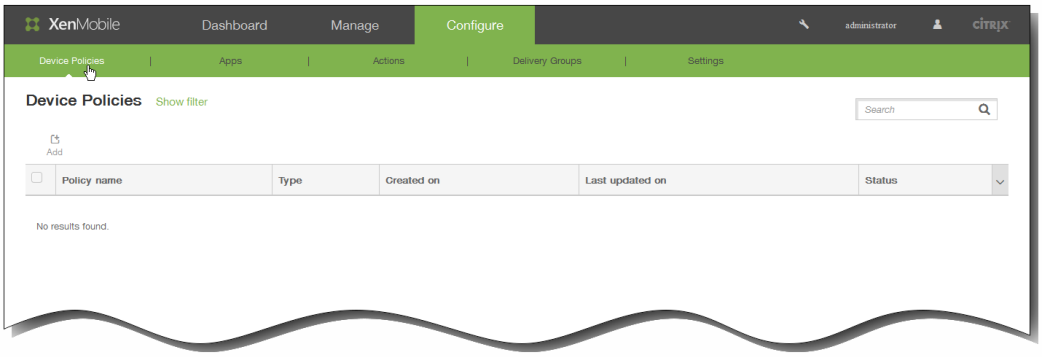
Jul 25, 2016

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.

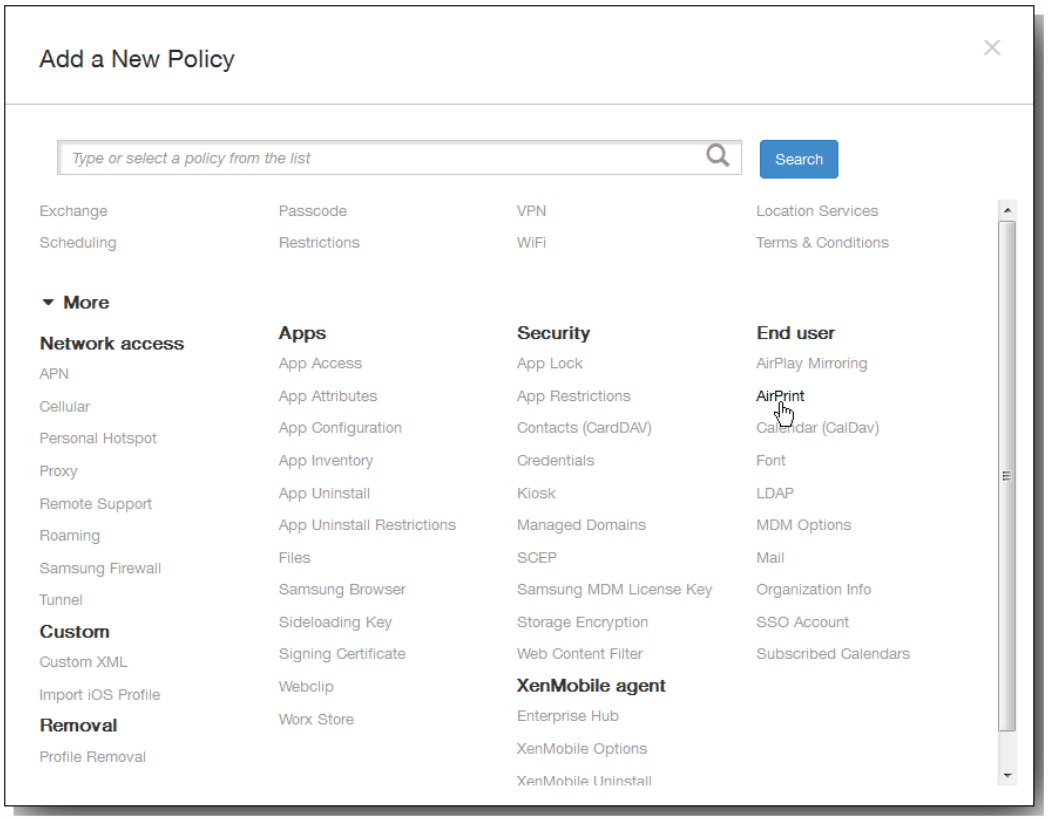
Remarque :

- 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.

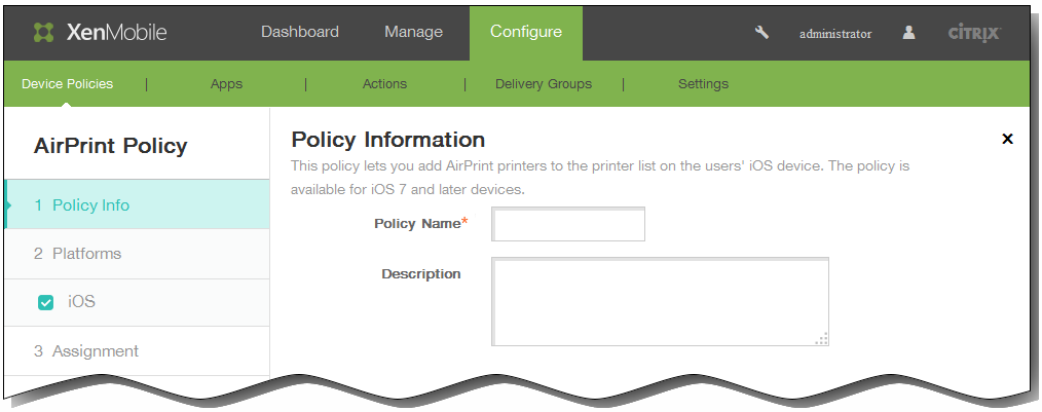


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

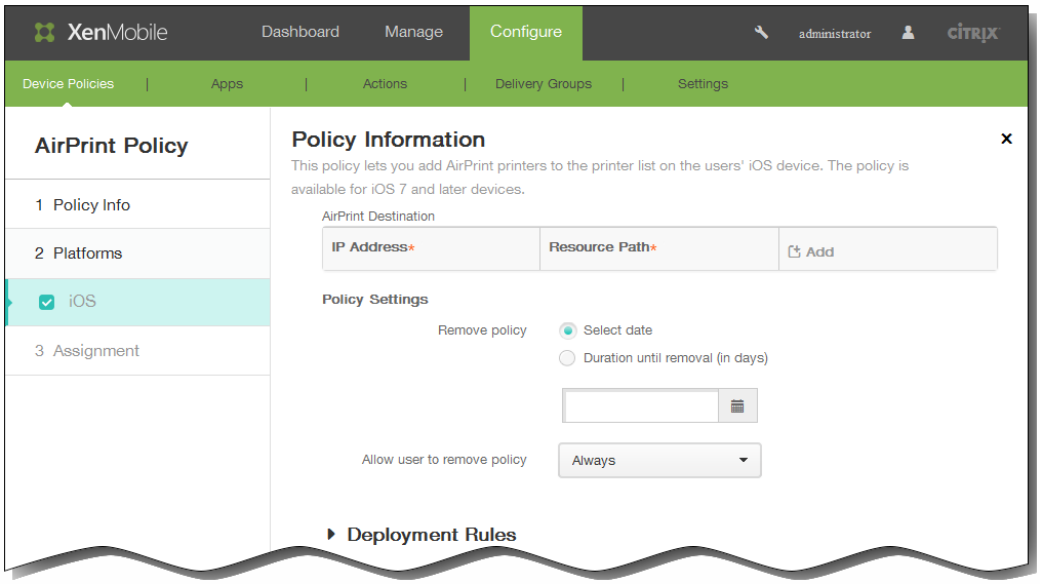


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

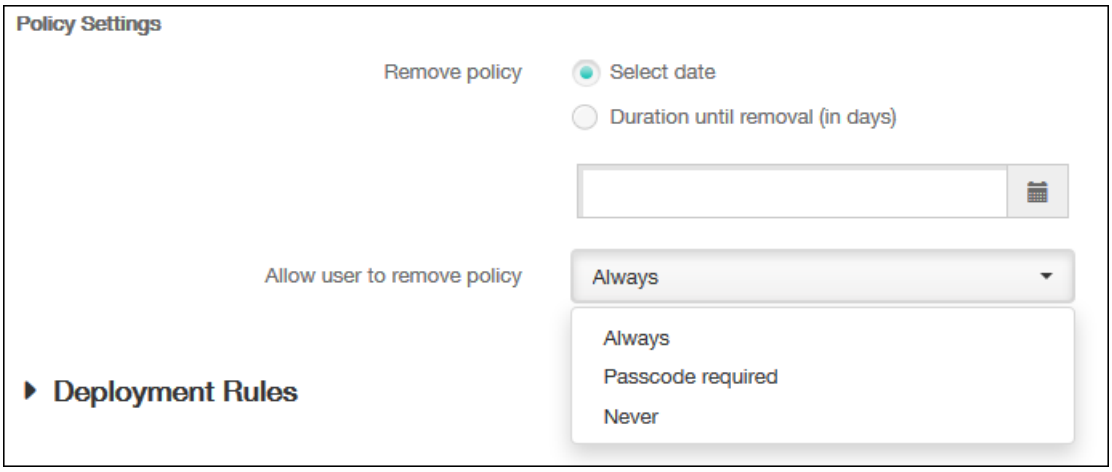


6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Destination AirPrint : cliquez sur Ajouter et procédez comme suit :
      1. Adresse IP : entrez l'adresse IP de l'imprimante AirPrint.
      2. Chemin d'accès à la ressource : entrez le chemin d'accès à la 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.
      3. Cliquez sur Ajouter pour ajouter l'imprimante ou sur Annuler pour annuler l'ajout de l'imprimante.
      4. Répétez les étapes i à iii pour chaque appareil que vous souhaitez ajouter.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

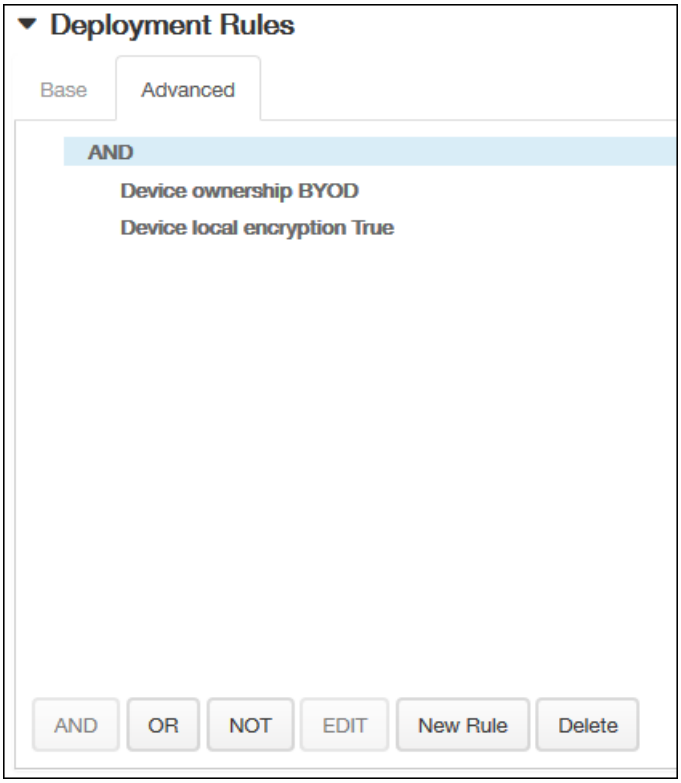


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

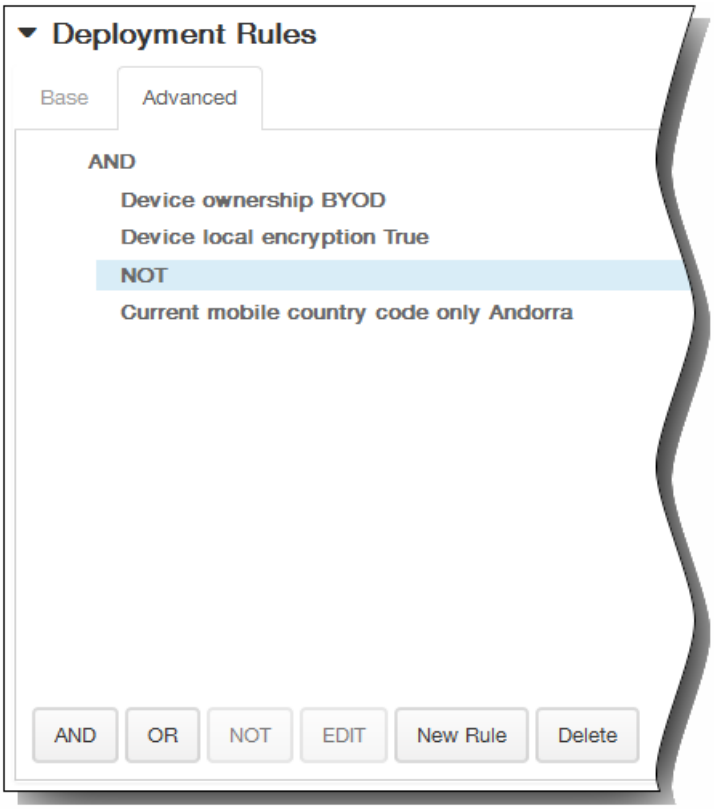


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

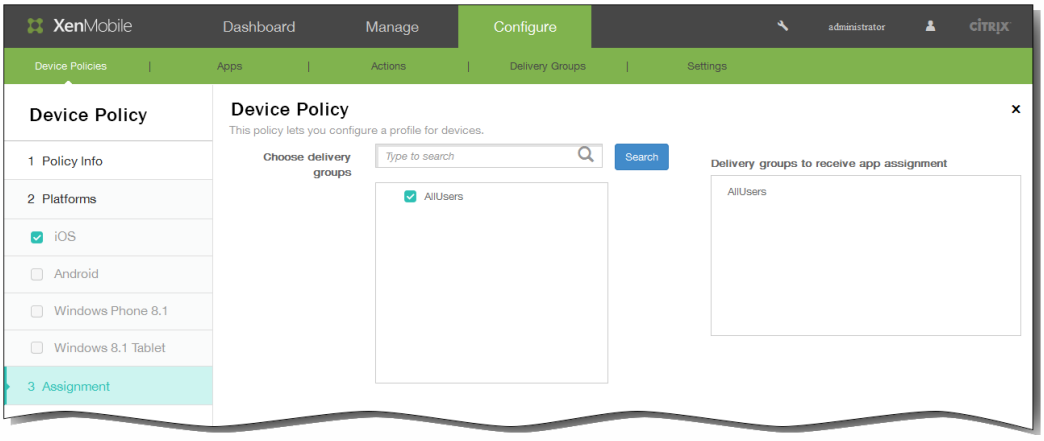
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie AirPrint s'affiche.
13. 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.



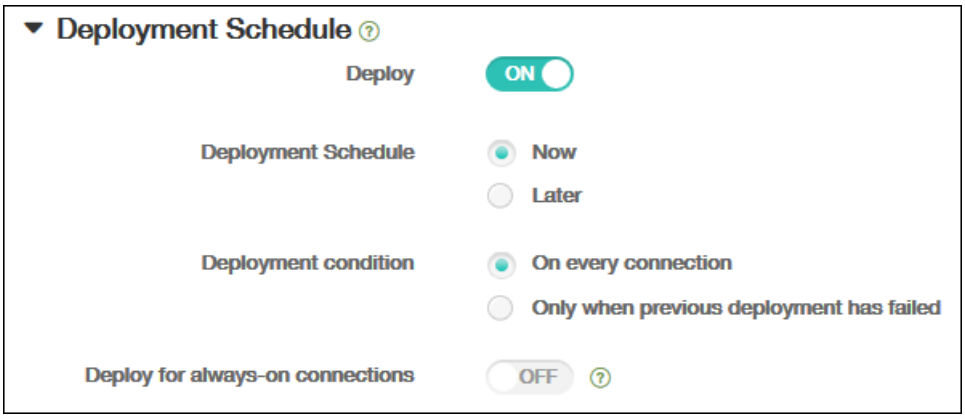
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

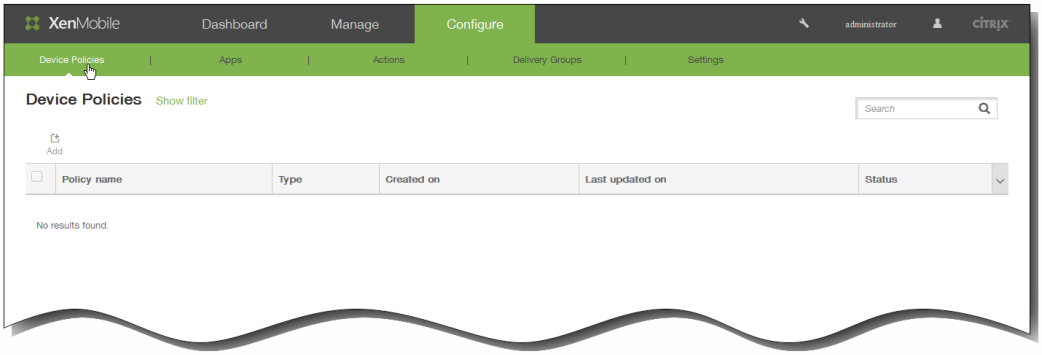
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de calendrier (CalDAV) pour iOS

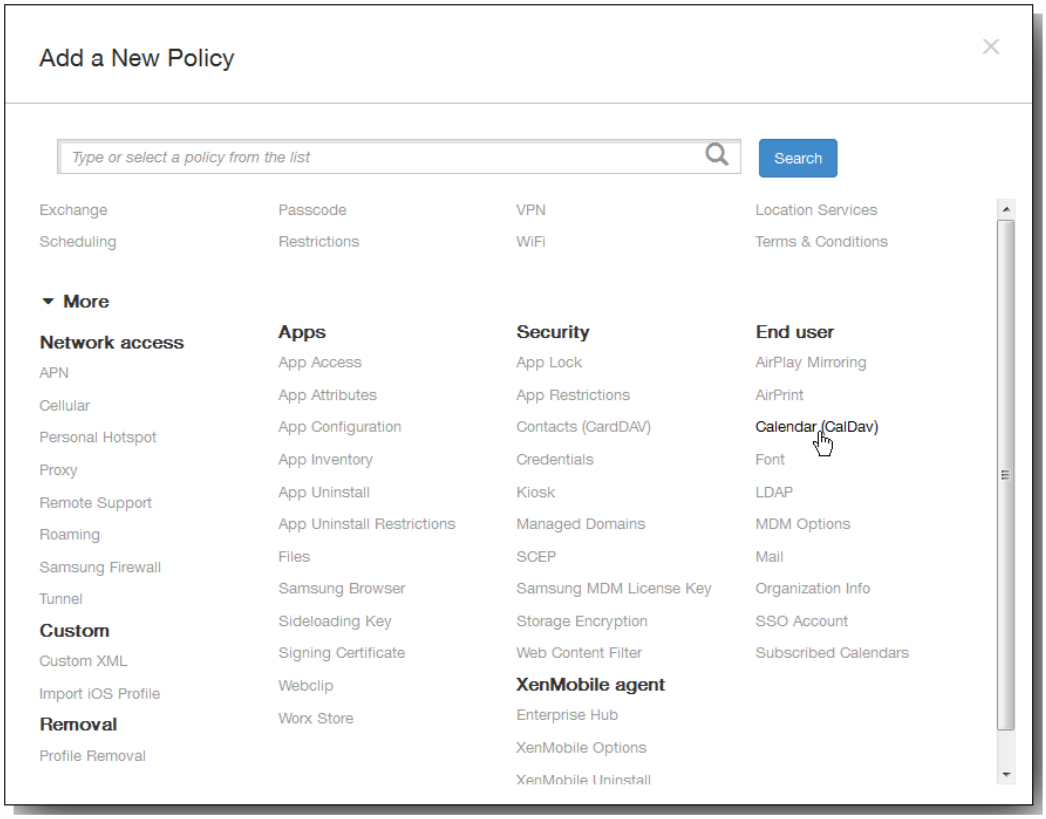
Jul 25, 2016

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de calendrier iOS (CalDAV) sur des appareils iOS 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.

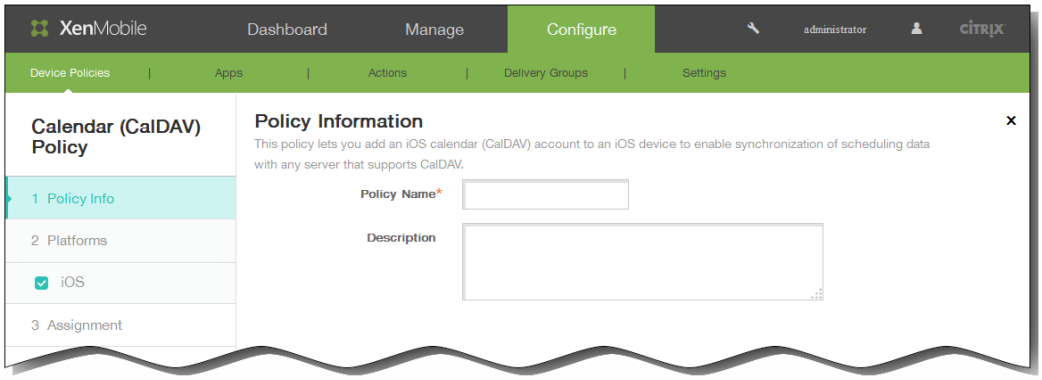


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

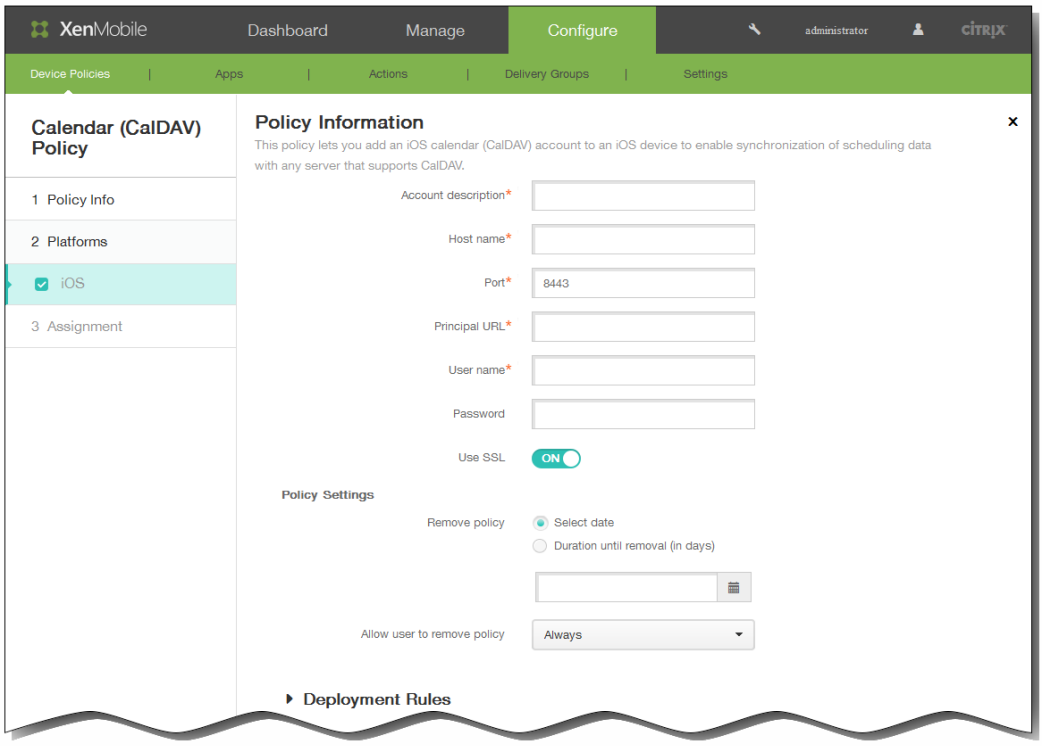


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

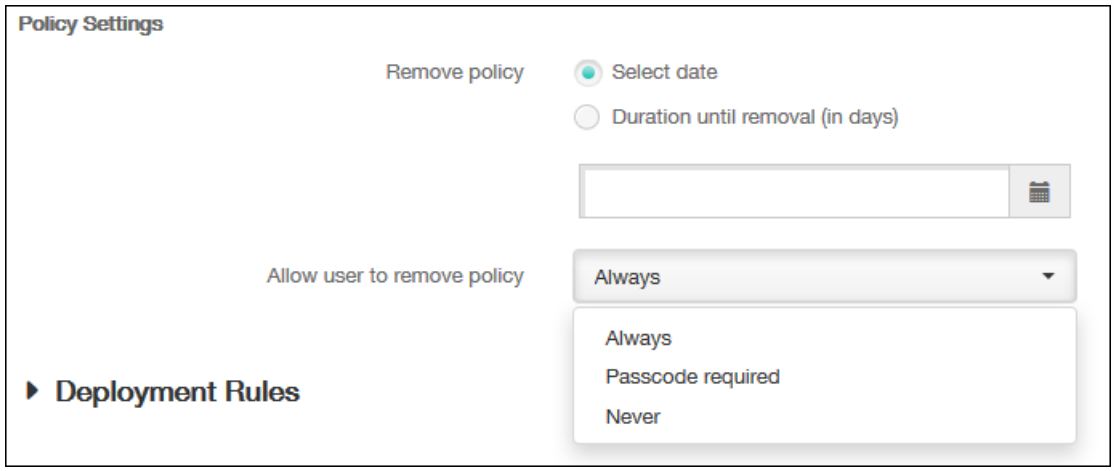


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Description du compte : entrez une description du compte. Ce champ est obligatoire.
   2. Nom d'hôte : entrez l'adresse du serveur CalDAV. Ce champ est obligatoire.
   3. Port : entrez le port sur lequel se connecter au serveur CalDAV. Ce champ est obligatoire. La valeur par défaut est 8443.
   4. URL principale : entrez l'adresse URL du calendrier de l'utilisateur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Nom d'utilisateur : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
6. Mot de passe : entrez un mot de passe utilisateur (facultatif).
7. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est On.

7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

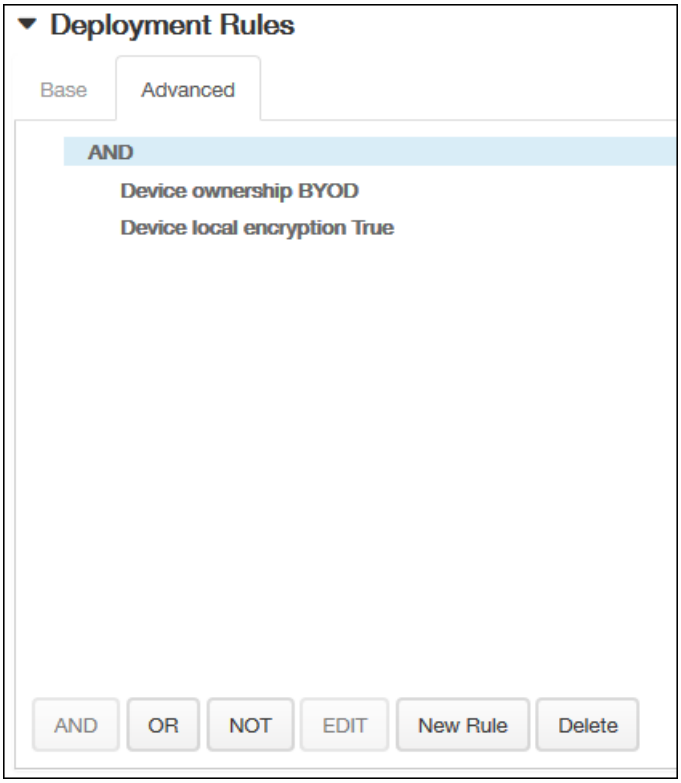


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

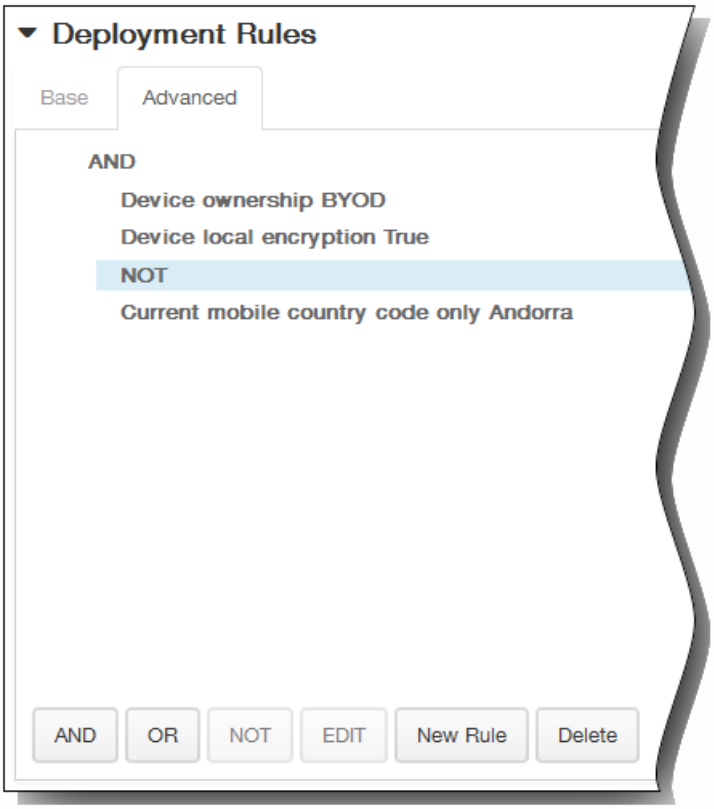


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

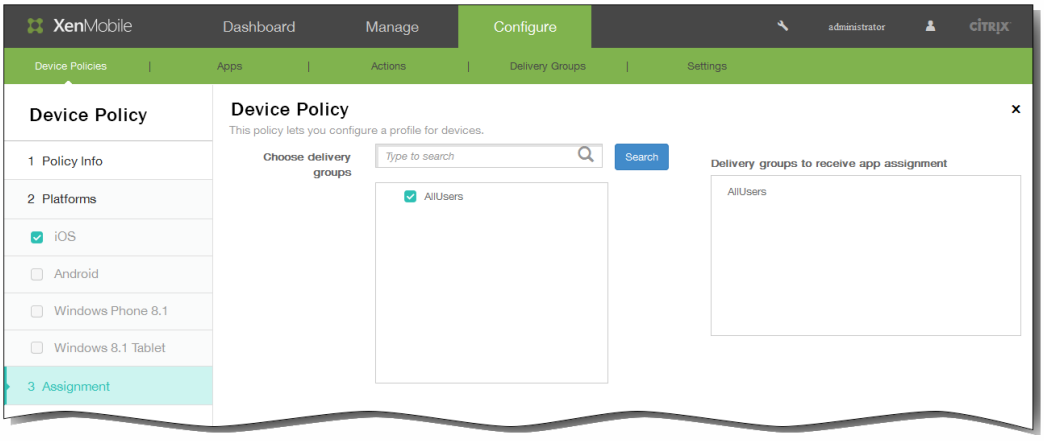
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de calendrier (CalDAV) s'affiche.
13. 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.



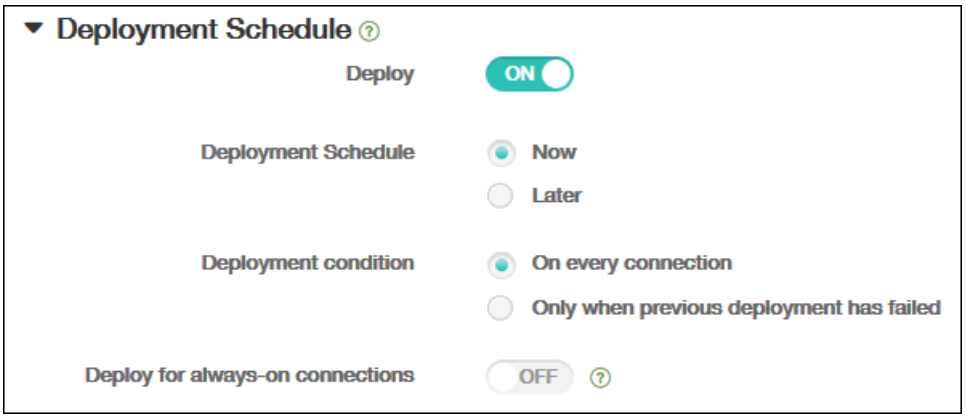
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

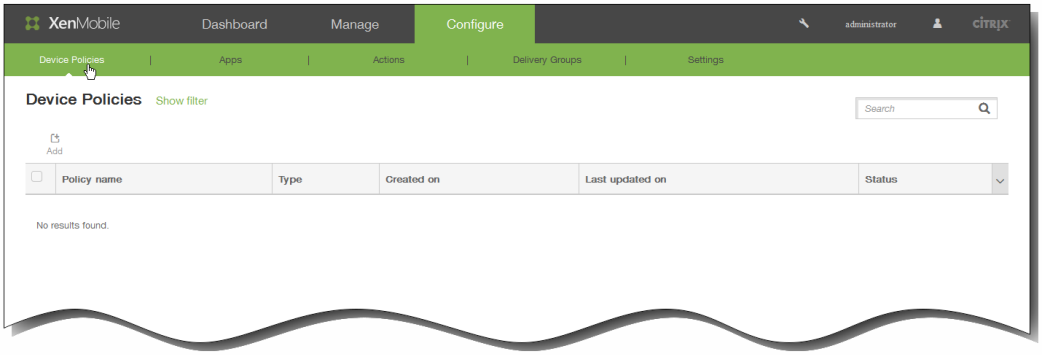
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de contacts (CardDAV) pour iOS

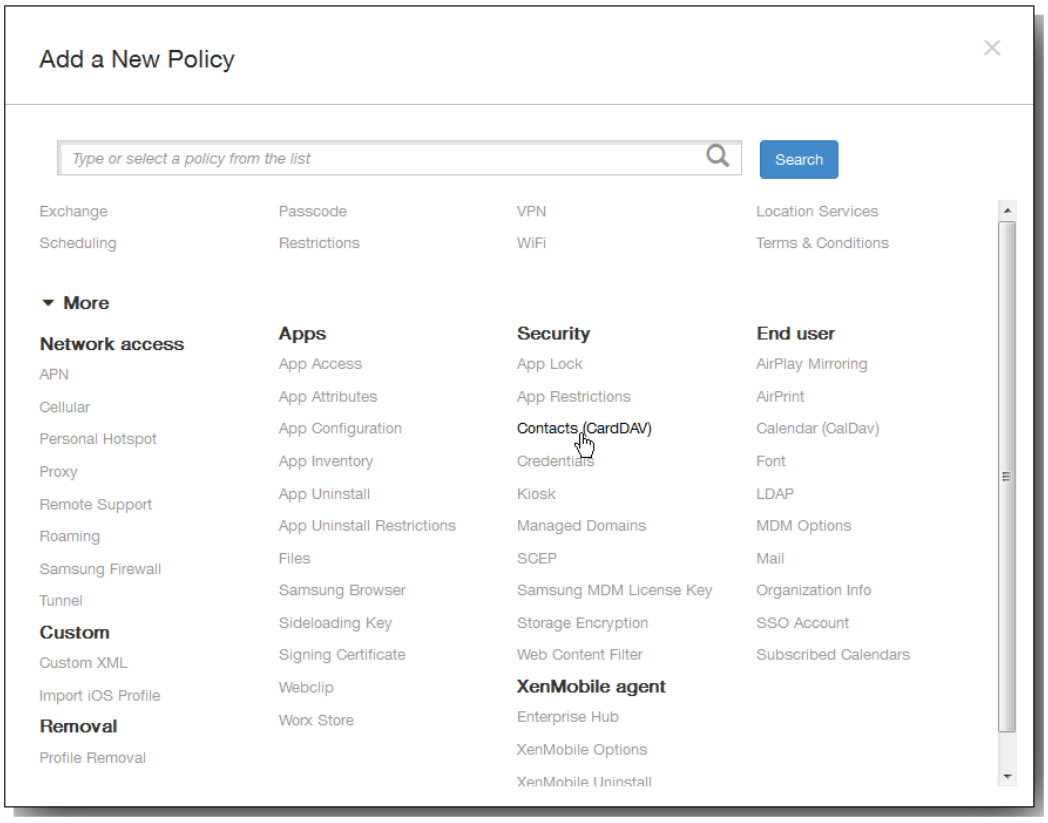
Jul 25, 2016

Vous pouvez ajouter une stratégie dans XenMobile afin d'ajouter un compte de contacts iOS (CalDAV) sur des appareils iOS 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.

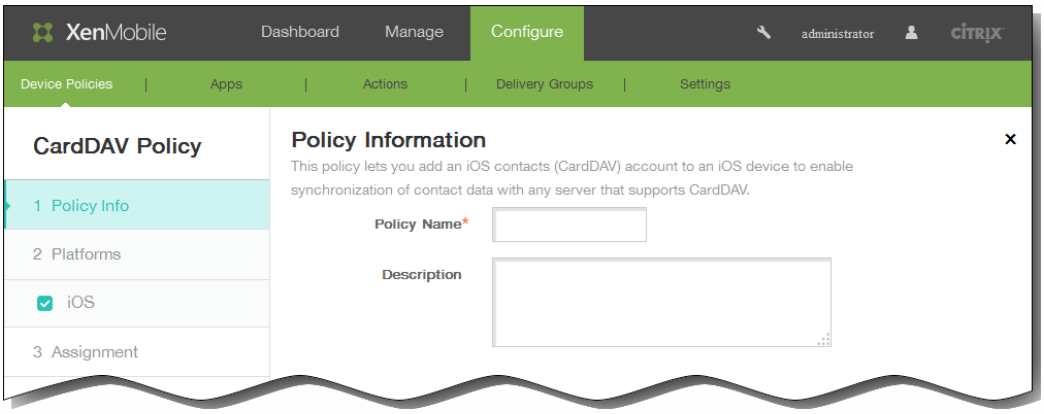


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

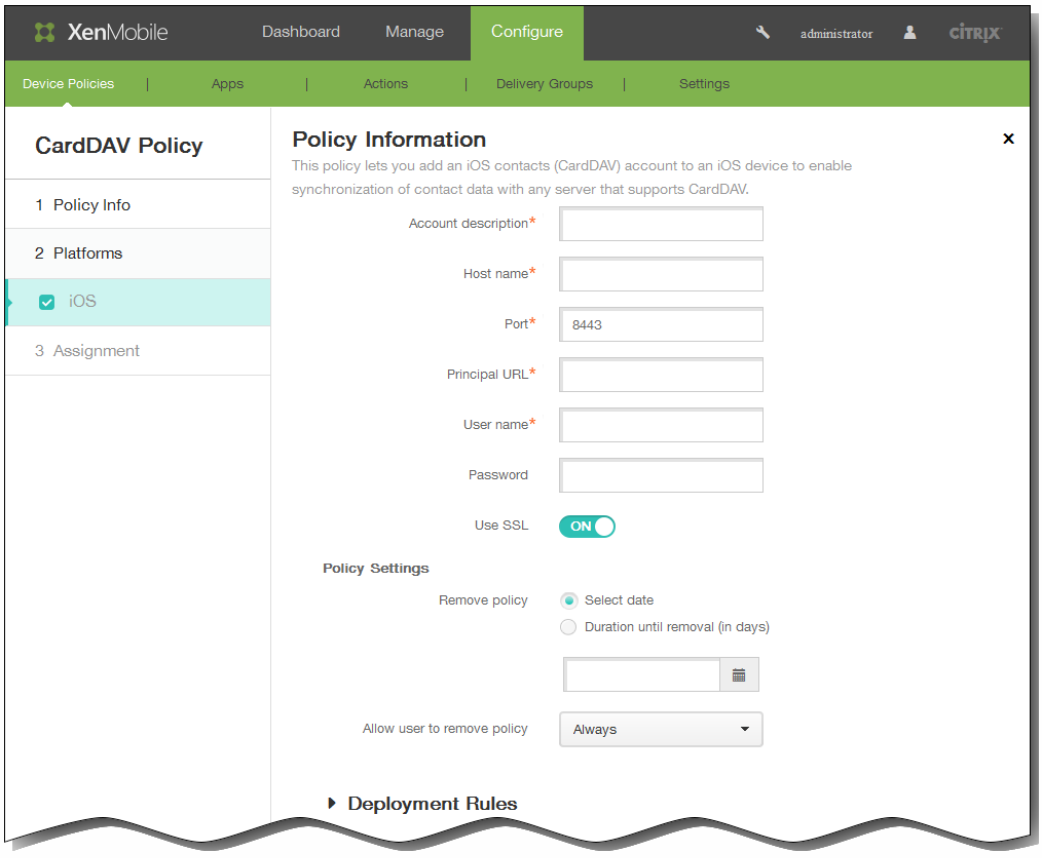


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Contacts (CardDAV). La page Stratégie CardDAV s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

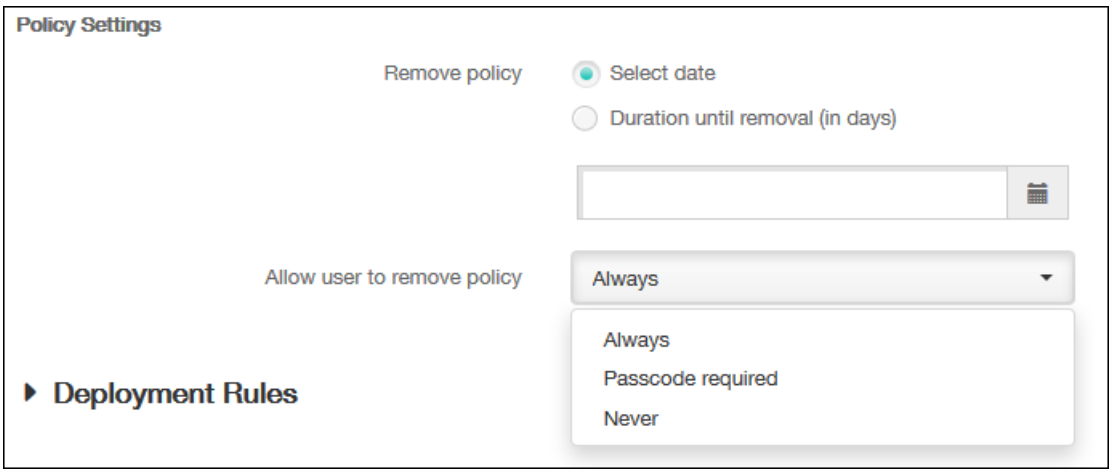


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Description du compte : entrez une description pour le compte. Ce champ est obligatoire.
   2. Nom d'hôte : entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Port : entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est 8443.
4. URL principale : entrez l'adresse URL du calendrier de l'utilisateur.
5. Nom d'utilisateur : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
6. Mot de passe : entrez un mot de passe utilisateur (facultatif).
7. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CardDAV. La valeur par défaut est ON.

7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

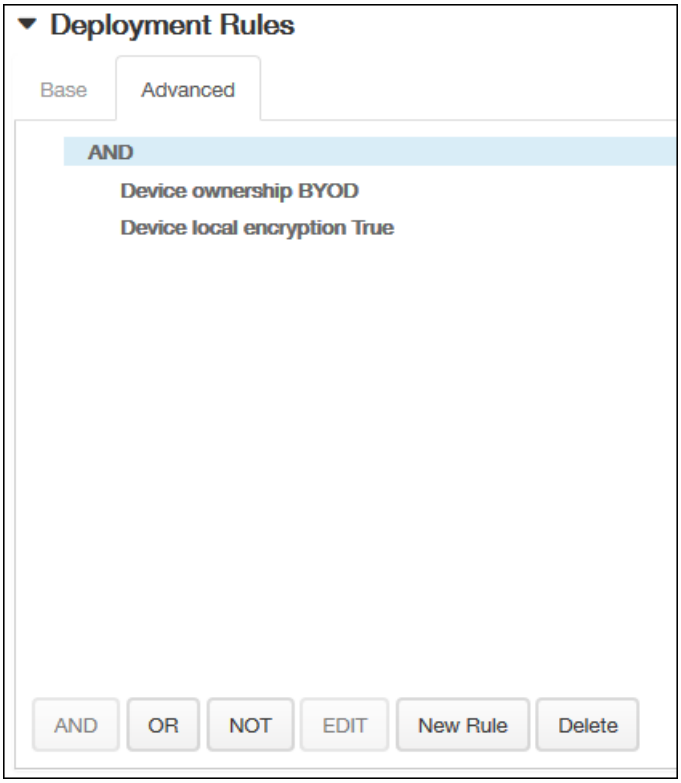


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

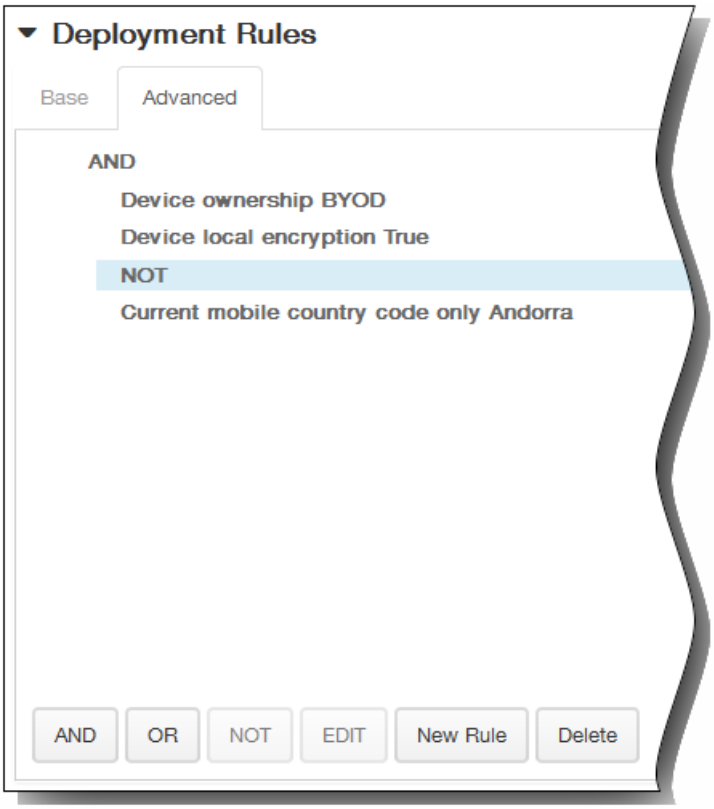


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

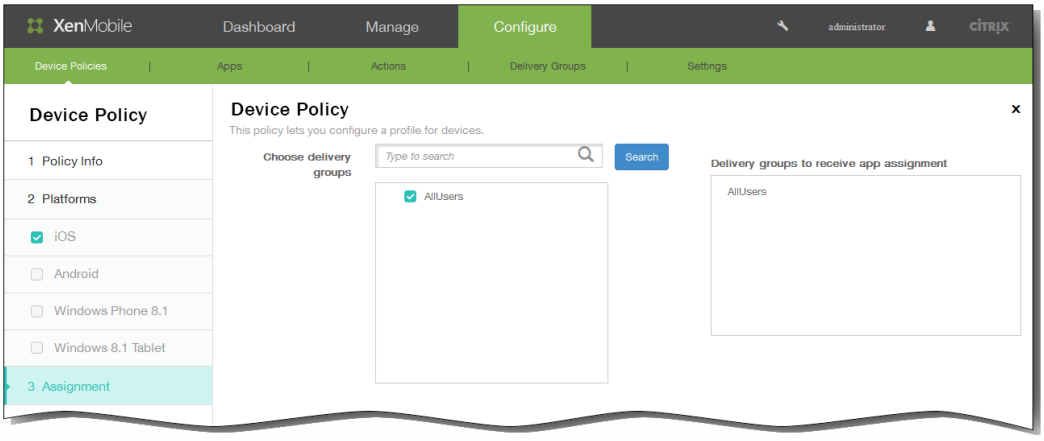
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie CardDAV s'affiche.
13. 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.



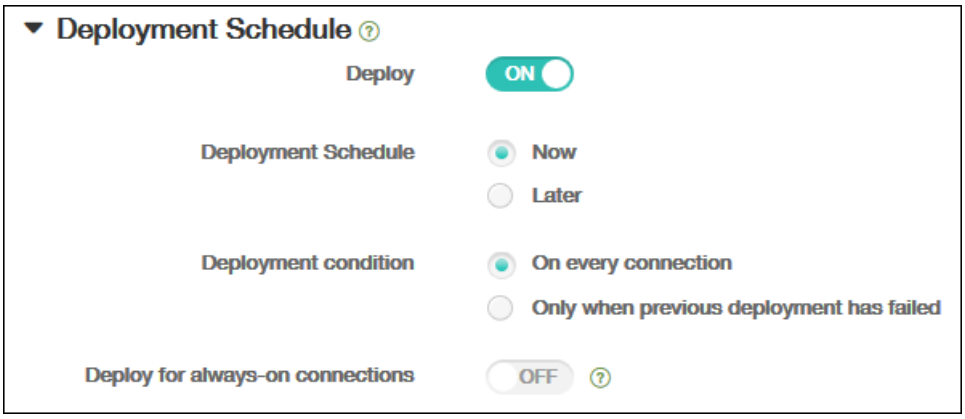
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de profil de provisioning pour iOS

Jul 25, 2016

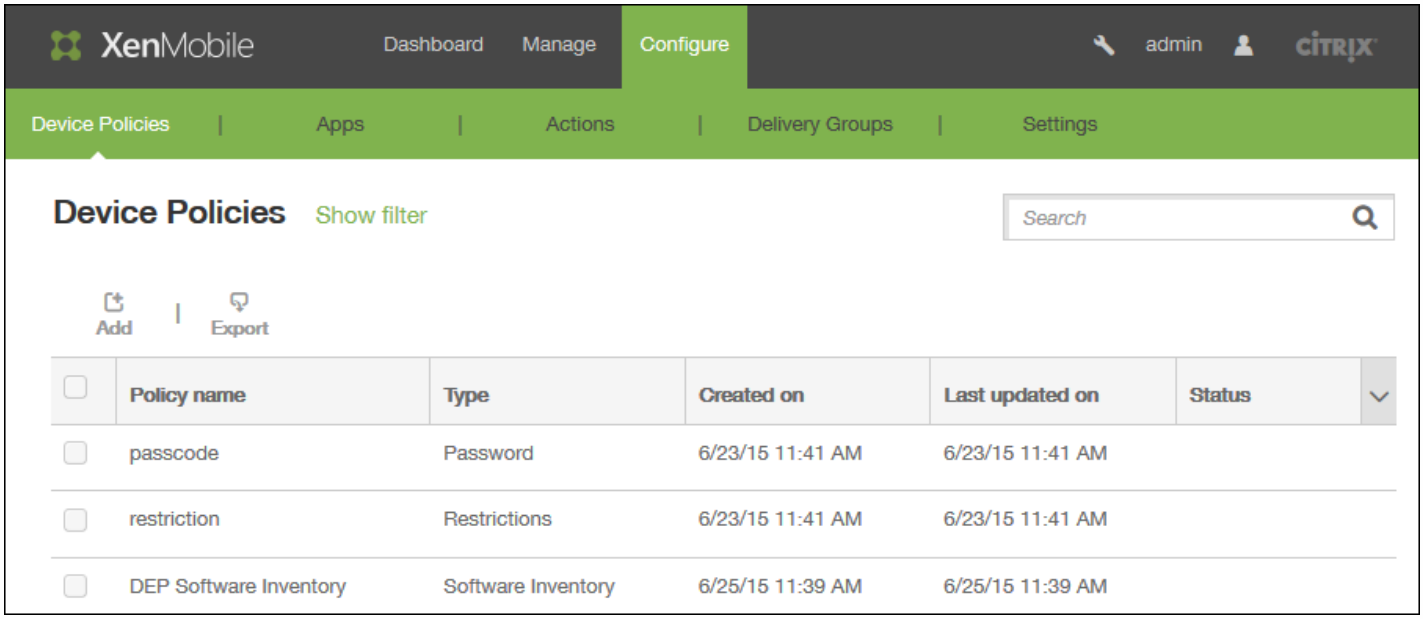
Lorsque vous développez et codez une application d'entreprise iOS, vous incluez généralement un profil de provisioning de distribution d'entreprise, dont Apple a besoin pour que l'application s'exécute sur un appareil iOS. Si un profil de provisioning est manquant, ou s'il a expiré, l'application se 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.

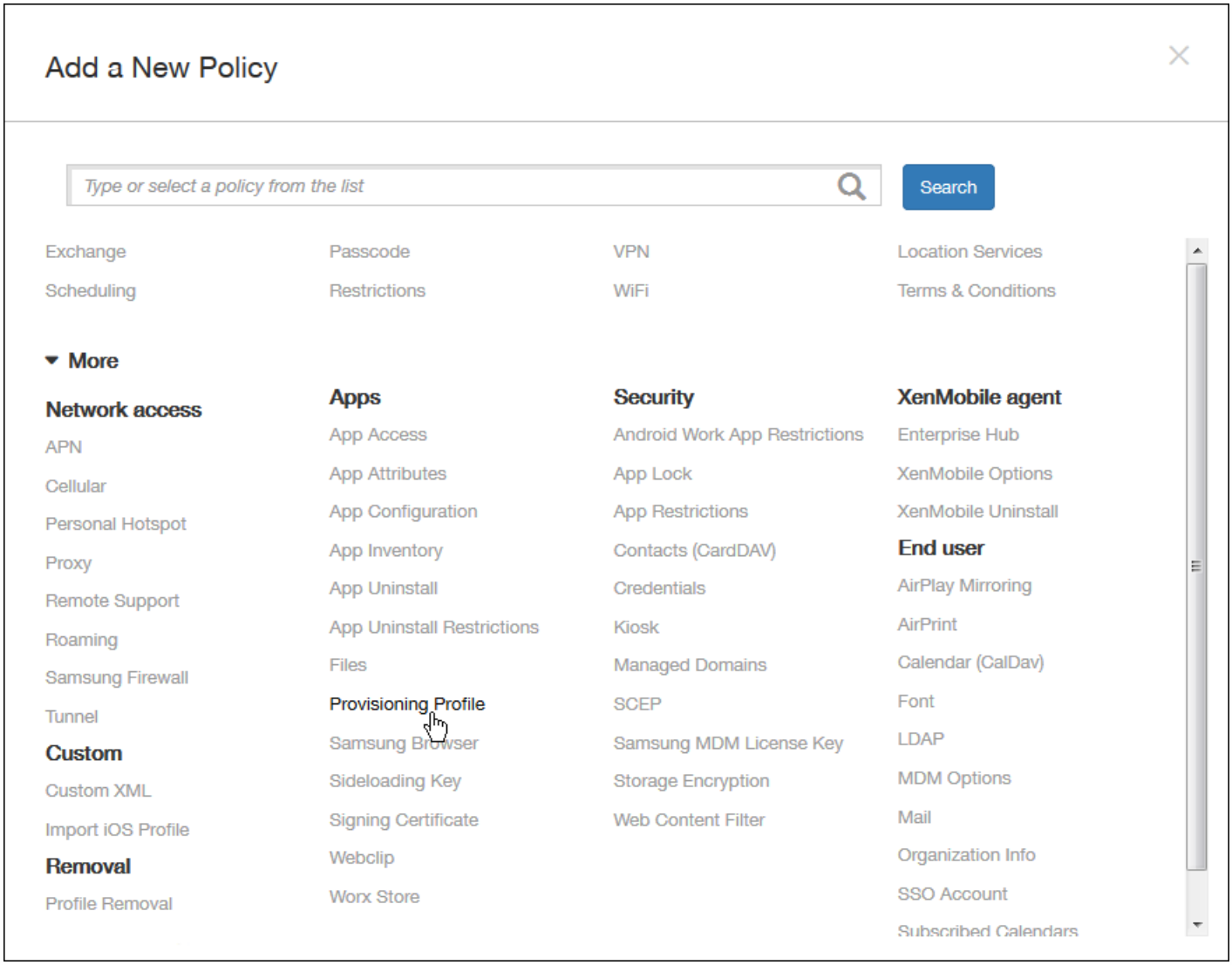
Avant de pouvoir créer une stratégie de profil de provisioning, vous devez créer un fichier de profil de provisioning. Pour plus d'informations, veuillez consulter la section Création de profils de provisioning sur le site Apple Developer.

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



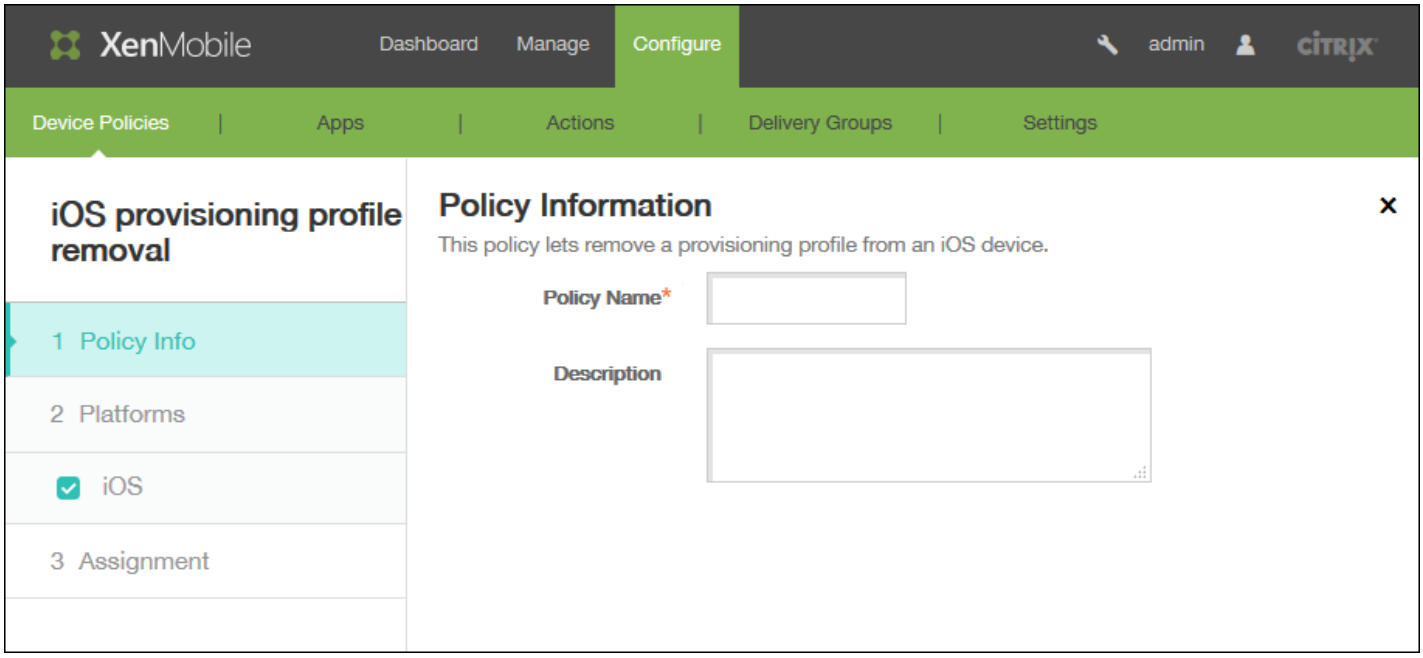
2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La page **Ajouter une nouvelle stratégie** apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sur la page **Ajouter une nouvelle stratégie**, cliquez sur **Plus** puis sous **Applications**, cliquez sur **Profil de provisioning**. La page d'informations **Stratégie de profil de provisioning iOS** s'affiche.

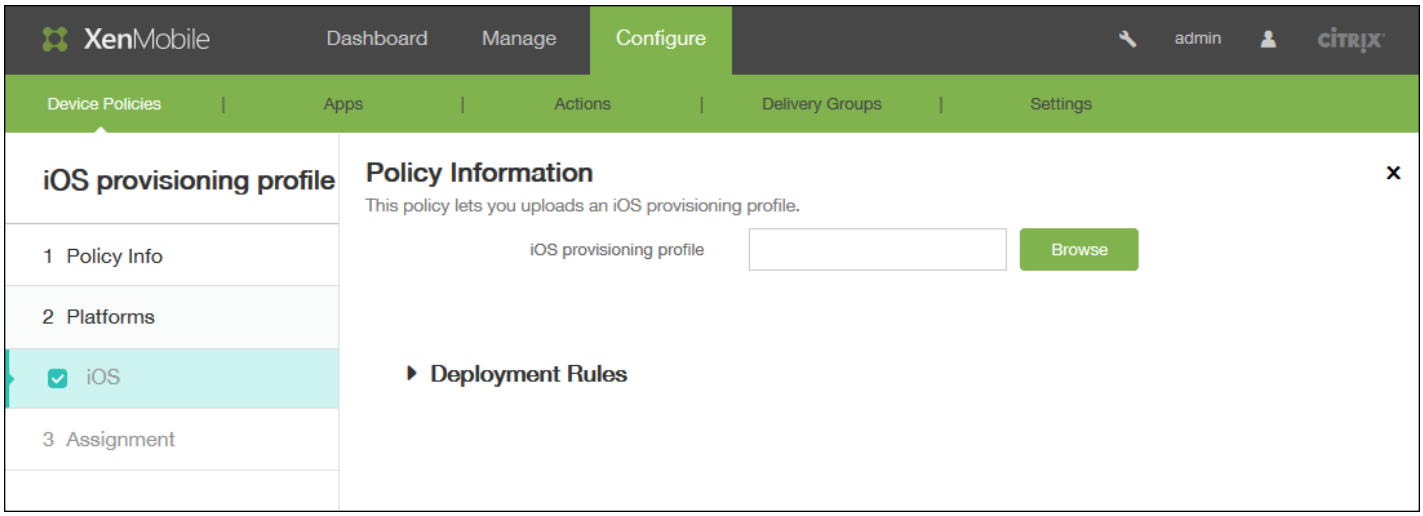
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. Dans la page **Informations sur la plate-forme iOS**, sélectionnez le fichier de profil de provisioning à importer en cliquant sur **Parcourir** et accédez à l'emplacement du fichier.

7. Développez **Règles de déploiement** et configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

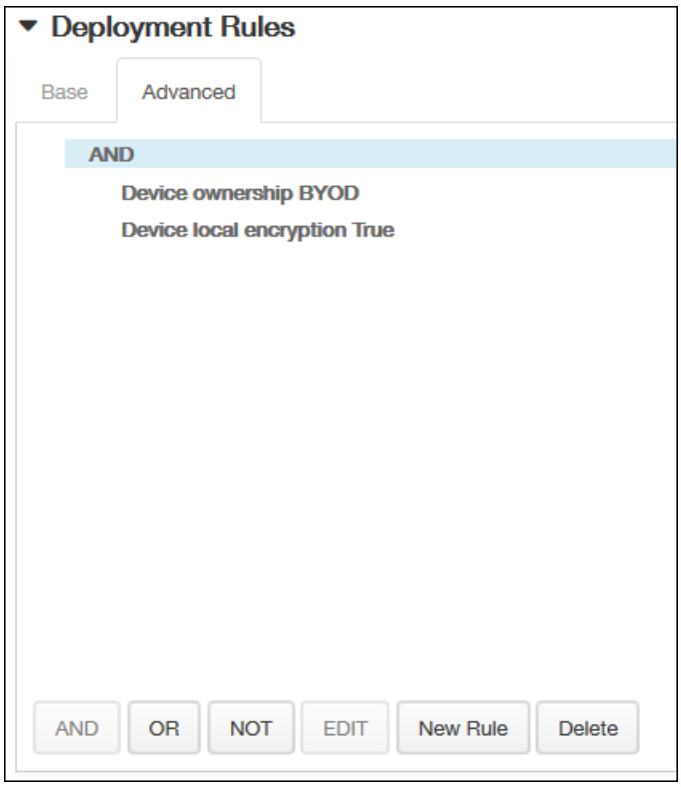


L'onglet **Base** s'affiche par défaut.

8. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.

- Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est **Toutes**.
- Cliquez sur **Nouvelle règle** pour définir les conditions.
- Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**, comme illustré dans la figure qui précède.
- Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

9. Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes.



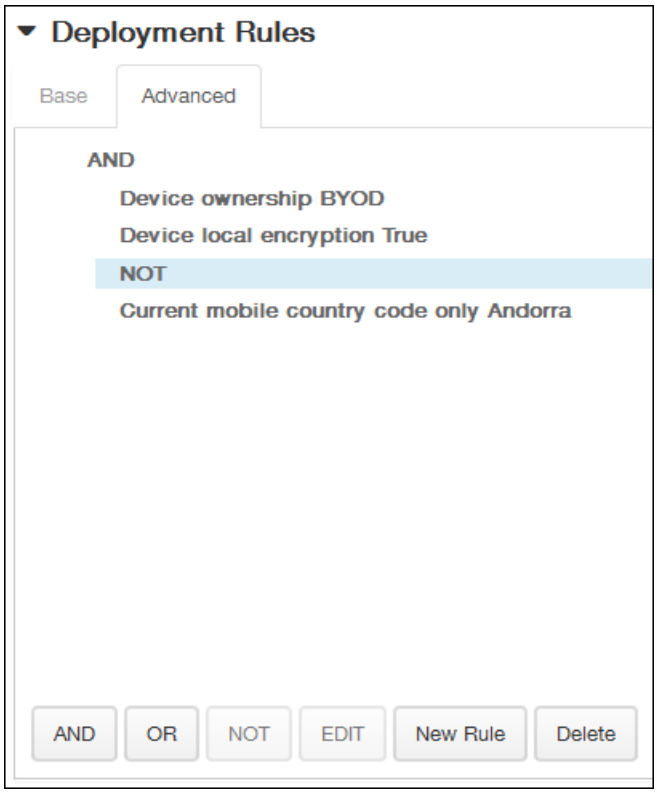
Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.

10. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.

- Cliquez sur **ET**, **OU** ou **SAUF**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
- Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.
- Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions.

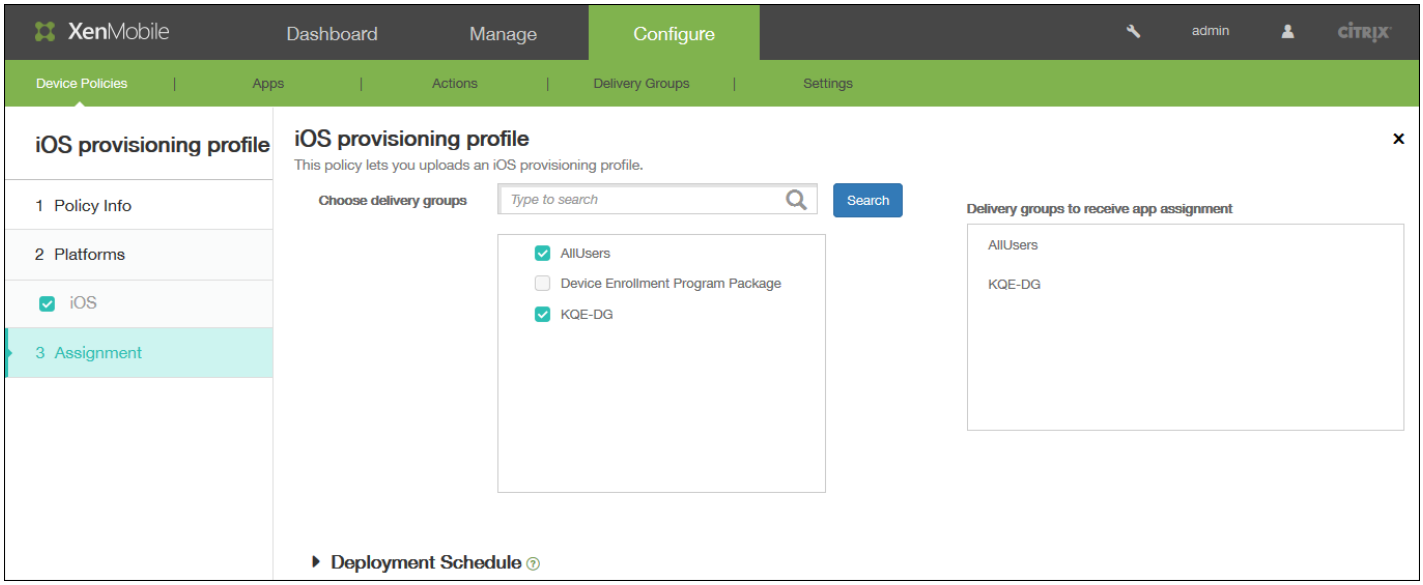


Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

11. Cliquez sur **Suivant**. La page d'attribution **Stratégie de profil de provisioning iOS** 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 la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

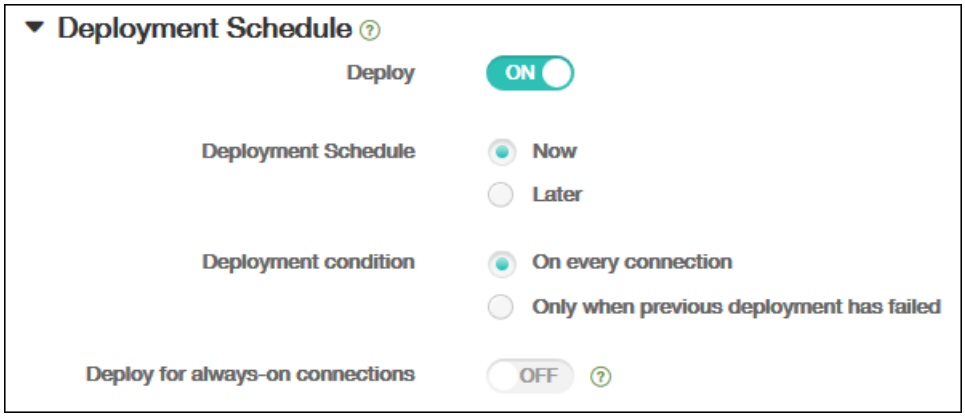


13. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- 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**. Notez que 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

14. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

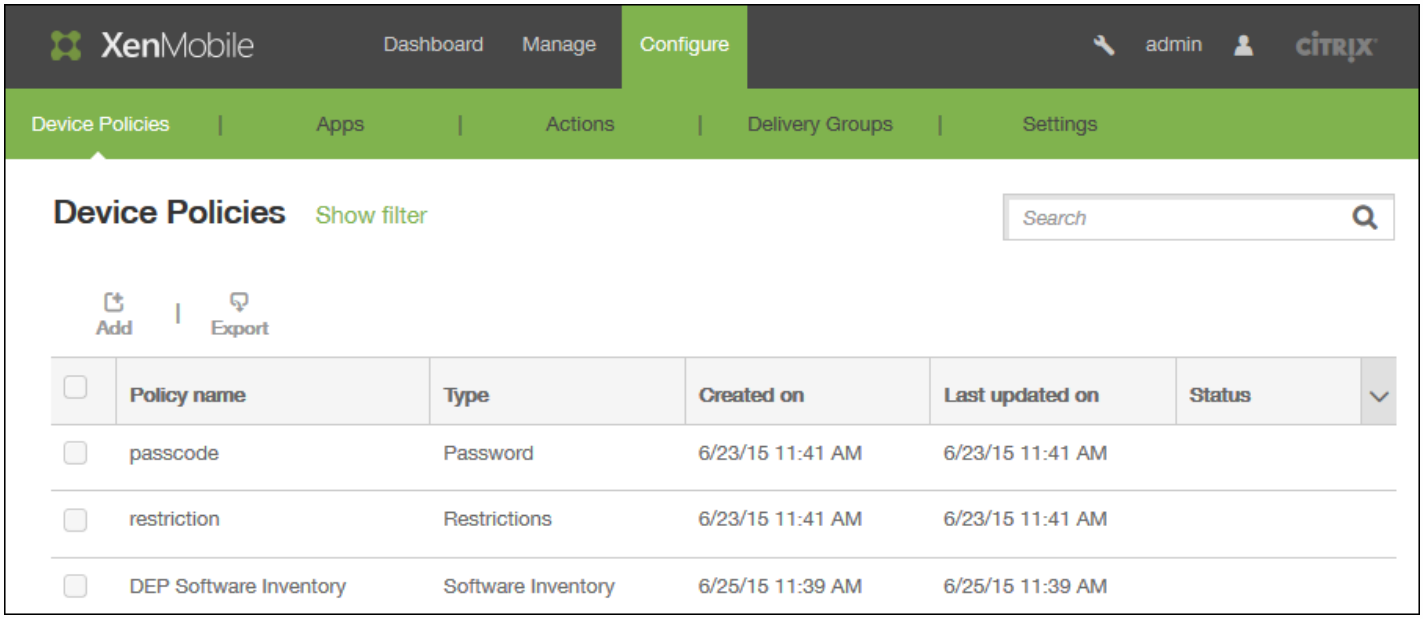
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de suppression de profil de provisioning pour iOS

Jul 25, 2016

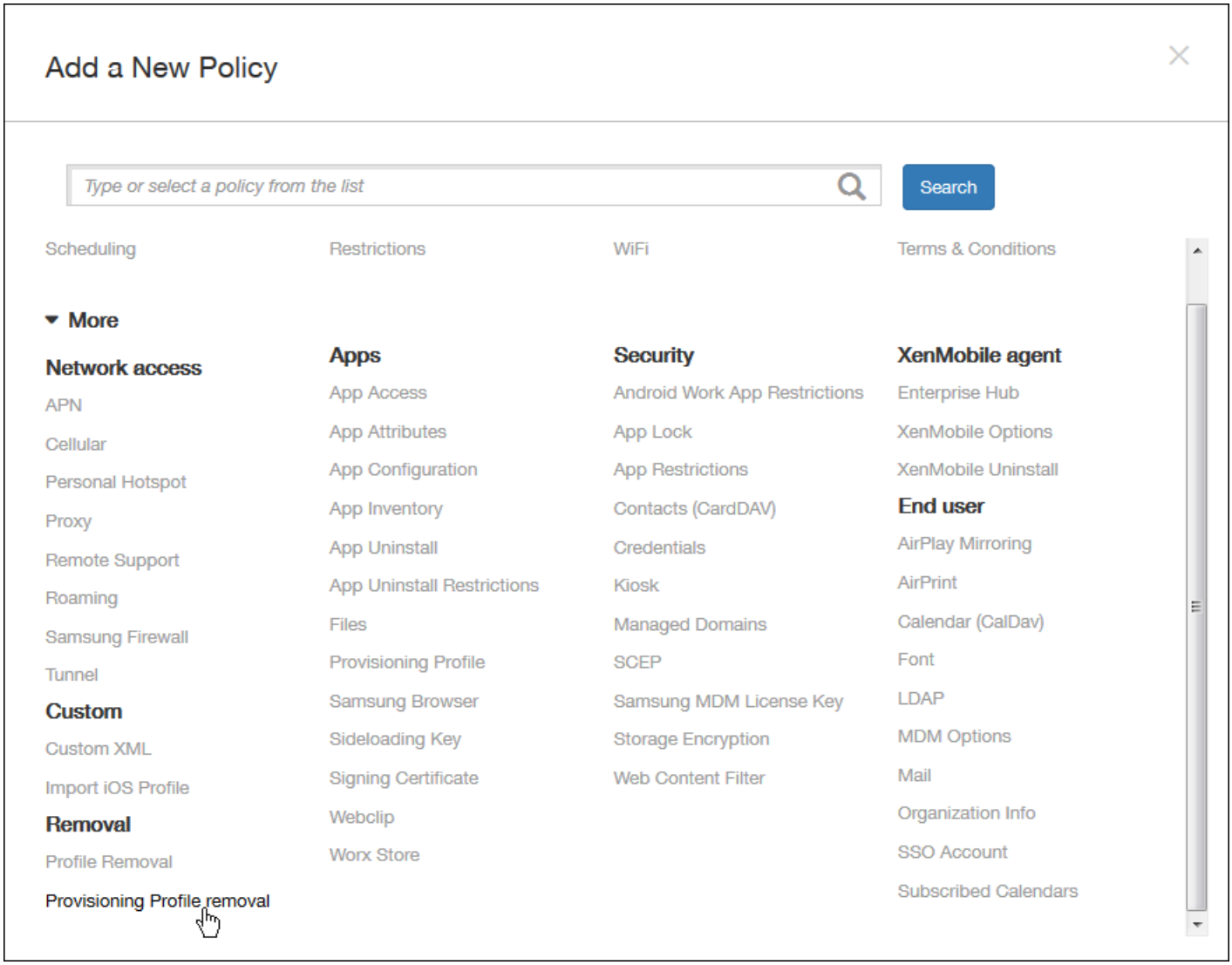
Vous pouvez supprimer des profils de provisioning iOS avec des stratégies d'appareil. Pour de plus amples informations sur les profils de provisioning, consultez la section Ajout d'un profil de provisioning.

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



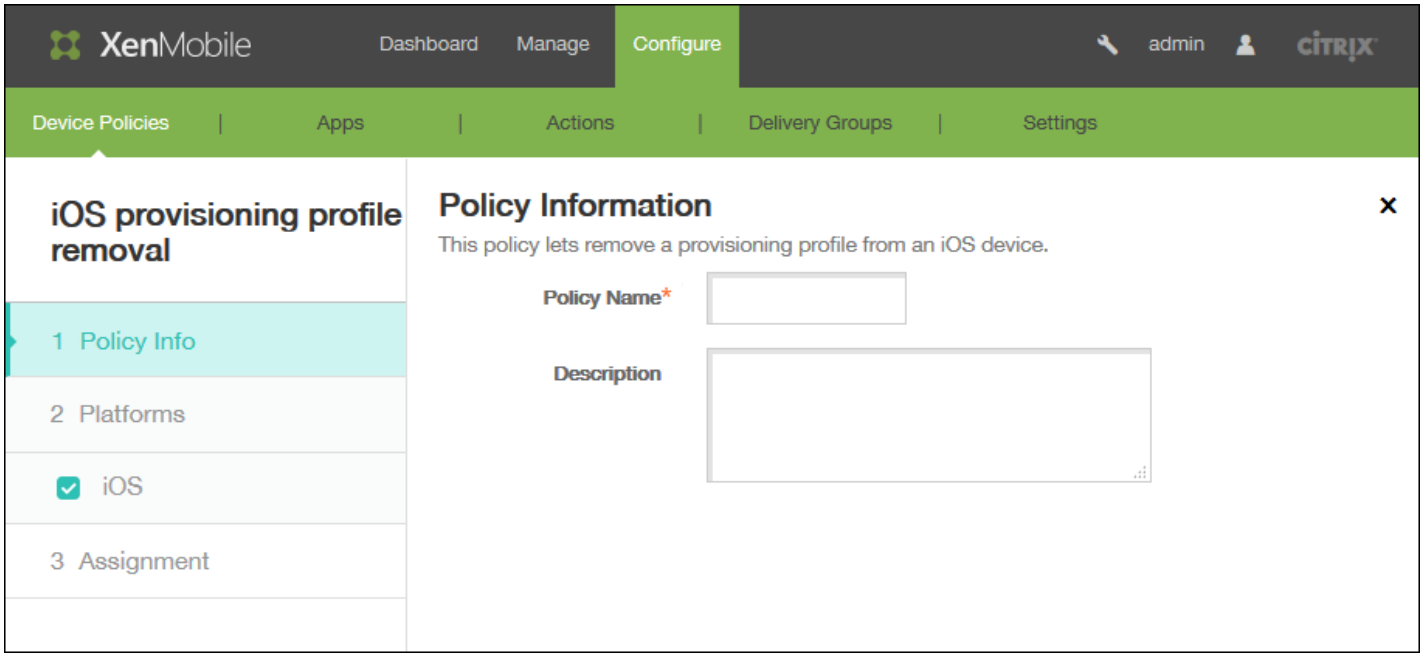
2. Cliquez sur **Ajouter** pour ajouter une nouvelle stratégie. La page **Ajouter une nouvelle stratégie** apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sur la page **Ajouter une nouvelle stratégie**, cliquez sur **Plus** puis sous **Suppression**, cliquez sur **Suppression du profil de provisioning**. La page d'informations **Stratégie de suppression de profil de provisioning iOS** s'affiche.

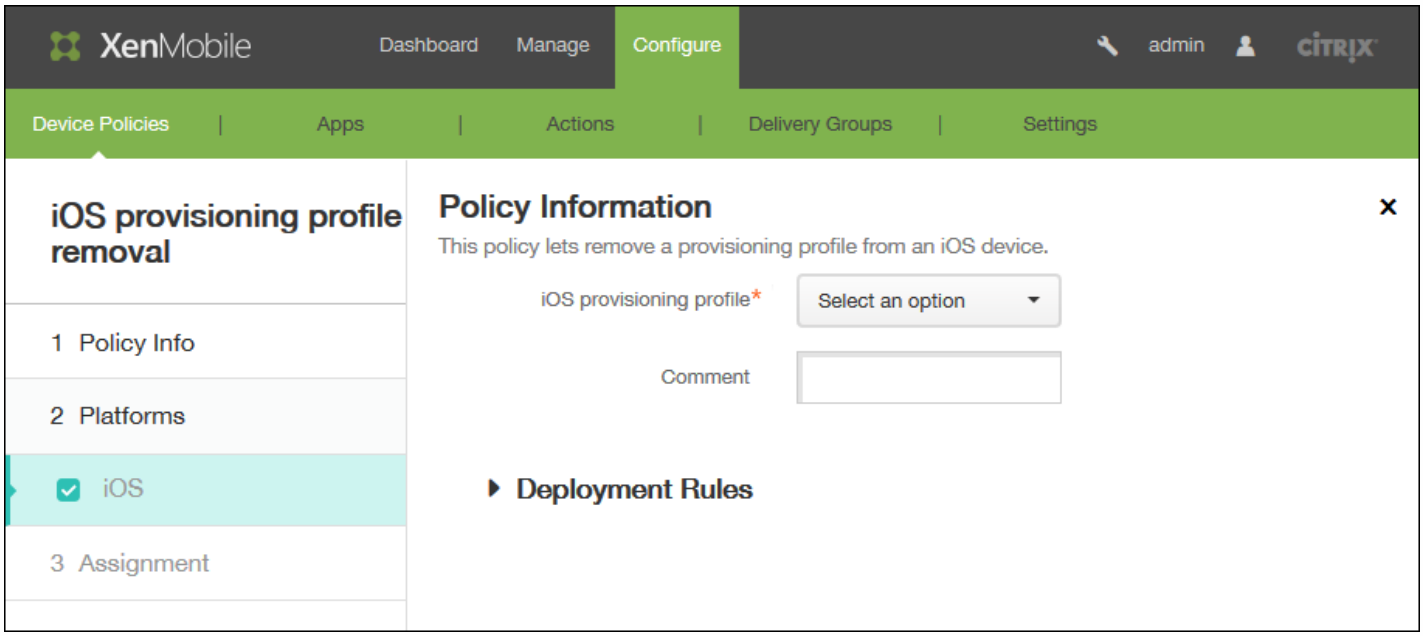
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. Dans la section **Informations sur la plate-forme iOS**, 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. Développez **Règles de déploiement** et configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

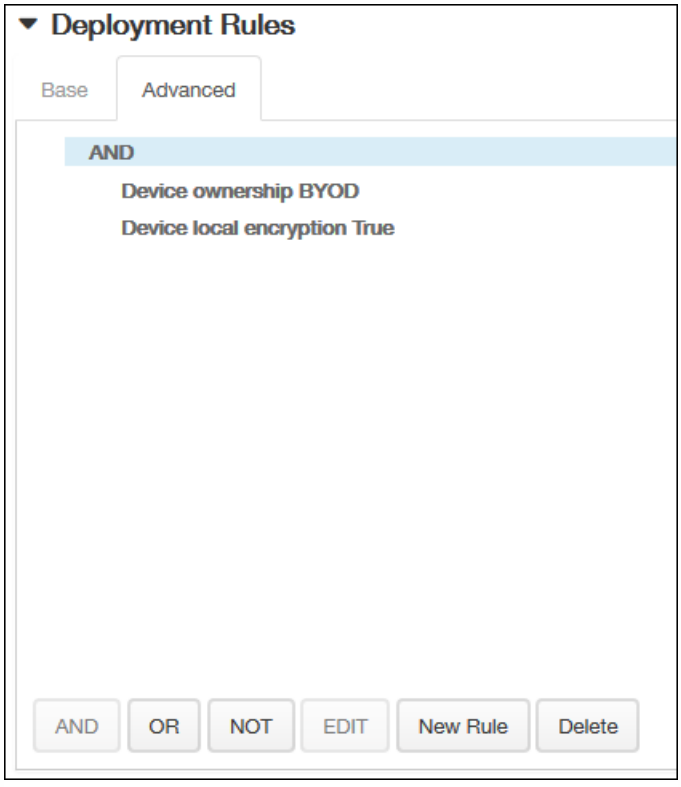


L'onglet **Base** s'affiche par défaut.

8. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.

- Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est **Toutes**.
- Cliquez sur **Nouvelle règle** pour définir les conditions.
- Dans la liste, cliquez sur les conditions, telles que **Propriétaire** et **BYOD**, comme illustré dans la figure qui précède.
- Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

9. Cliquez sur l'onglet **Avancé** pour combiner les règles avec des options booléennes.



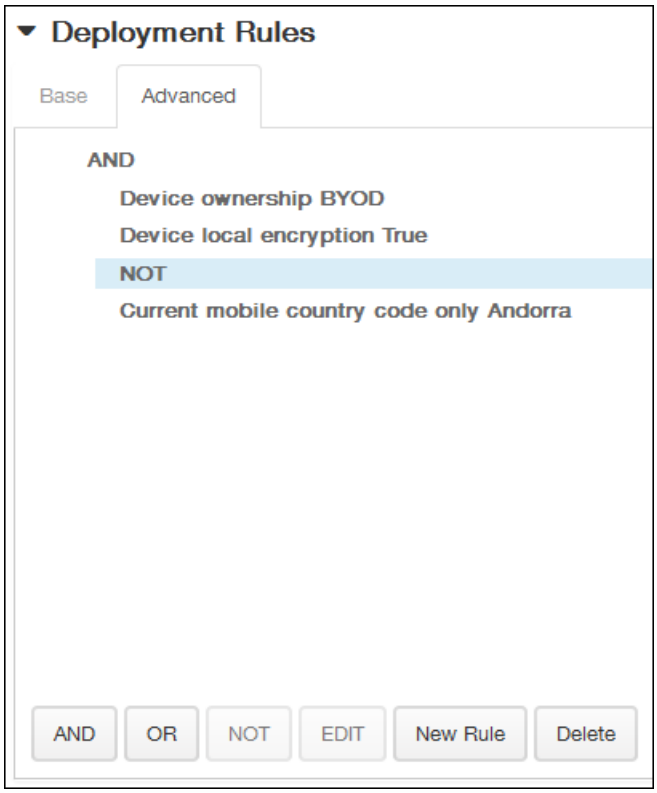
Les conditions que vous avez choisies sur l'onglet **Base** s'affichent.

10. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.

- Cliquez sur **ET**, **OU** ou **SAUF**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
- Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur **MODIFIER** pour modifier la condition ou sur **Supprimer** pour supprimer la condition.
- Cliquez sur **Nouvelle règle** de nouveau pour ajouter davantage de conditions.

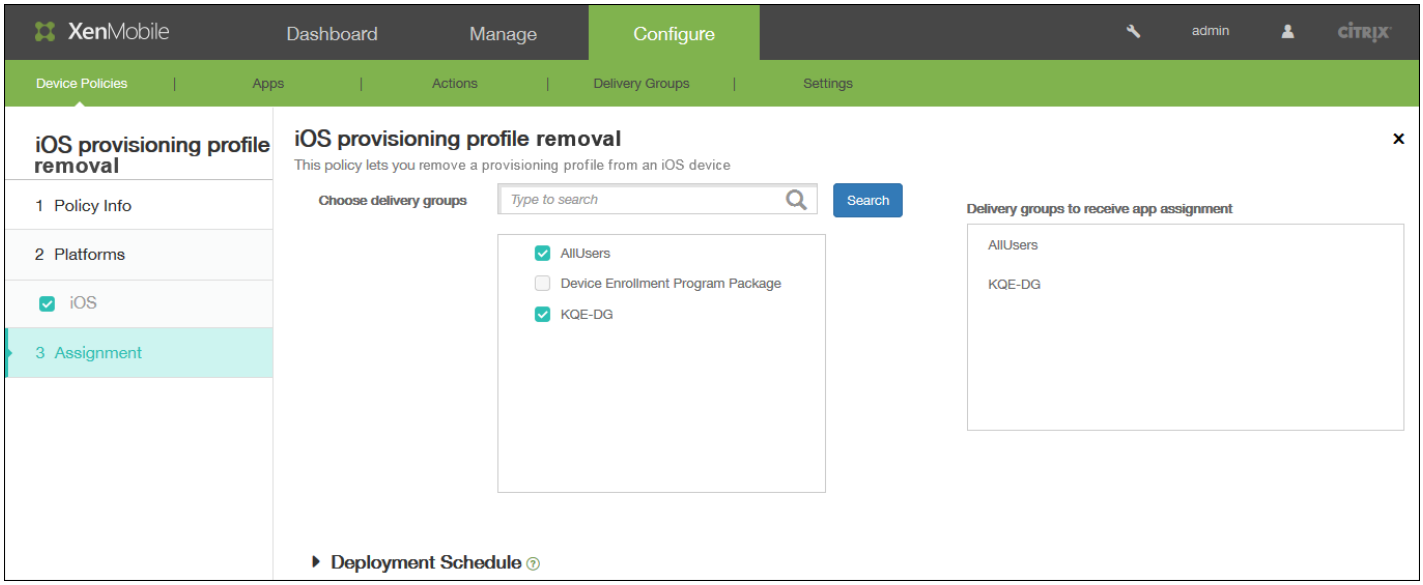


Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

11. Cliquez sur **Suivant**. La page d'attribution **Stratégie de profil de provisioning iOS** 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 la stratégie. Les groupes que vous sélectionnez s'affichent dans liste **Groupes de mise à disposition qui vont recevoir l'attribution d'applications**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

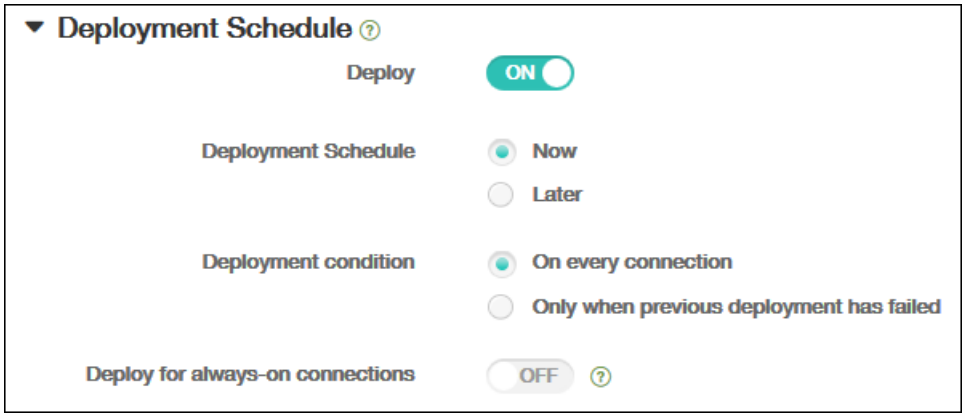


13. Développez **Calendrier de déploiement** et configurez les paramètres suivants :

- 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**. Notez que 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

14. Cliquez sur **Enregistrer** pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies d'informations d’identification

Jul 25, 2016

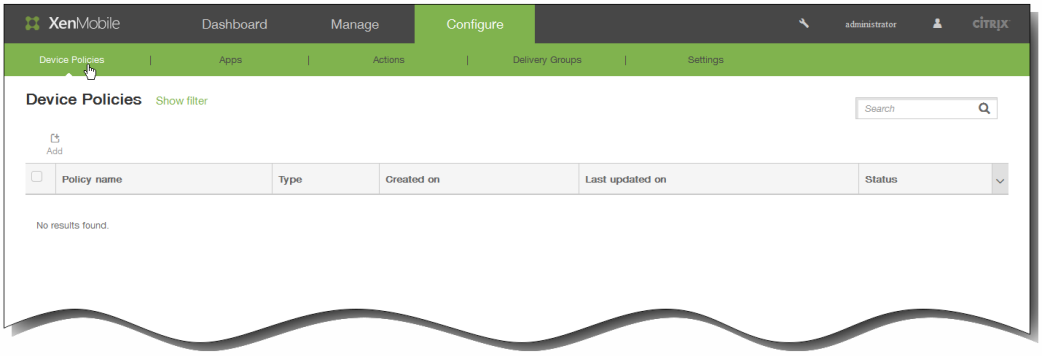
Vous pouvez créer des stratégies d'informations d'identification dans XenMobile afin d'intégrer l'authentification à votre configuration PKI dans XenMobile, comme une entité PKI, un keystore, un fournisseur d'informations d'identification ou un certificat de serveur. Pour plus d'informations sur les informations d’identification, veuillez consulter la section Certificats dans XenMobile.

Vous pouvez créer des stratégies d'informations d'identification pour iOS, Android, Android for Work et Windows 8.1 Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie :

- Informations d'identification que vous prévoyez d'utiliser pour chaque plate-forme, ainsi que les certificats et les mots de passe.

1. Dans la console XenMobile, cliquez sur ConfigurerStratégies d'appareil. La page Stratégies d'appareil s'affiche.



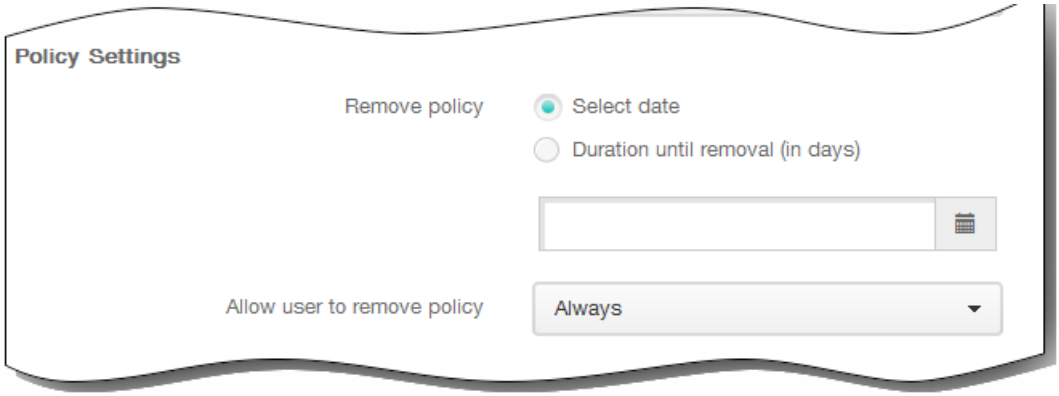
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.
3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Informations d'identification. La page Stratégie d'informations d'identification s'affiche.
4. Dans le panneau Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. 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 le panneau de configuration de la plate-forme iOS s'affiche en premier.
6. Sous Plates-formes, sélectionnez les plates-formes que vous souhaitez ajouter.
   - Si vous sélectionnez iOS, configurez les paramètres suivants :
     Type de certificat : dans la liste, cliquez sur le type d'informations d'identification à utiliser avec cette stratégie.

     Entrez les informations suivantes pour les informations d'identification 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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



1. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
2. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
3. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
4. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

- Si vous avez sélectionné Android, configurez les paramètres suivants :
  Type de certificat : dans la liste, cliquez sur le type d'informations d'identification à utiliser avec cette stratégie.

  Entrez les informations suivantes pour les informations d'identification 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

- Si vous avez sélectionné Windows Phone 8.1 Tablet, 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 les informations d'identification. Mon magasin stocke les certificats dans les magasins de certificats des utilisateurs.

  Type de certificat : le certificat est le seul type d'informations d'identification pour tablettes Windows 8.1.

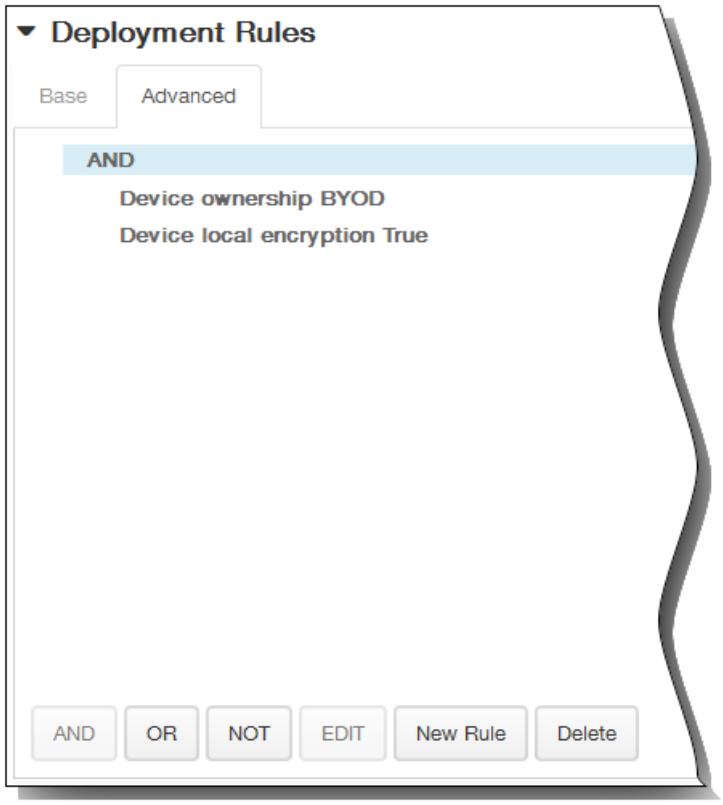
  Emplacement du certificat : sélectionnez le fichier de certificat en cliquant sur Parcourir et accédez à l'emplacement du fichier.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

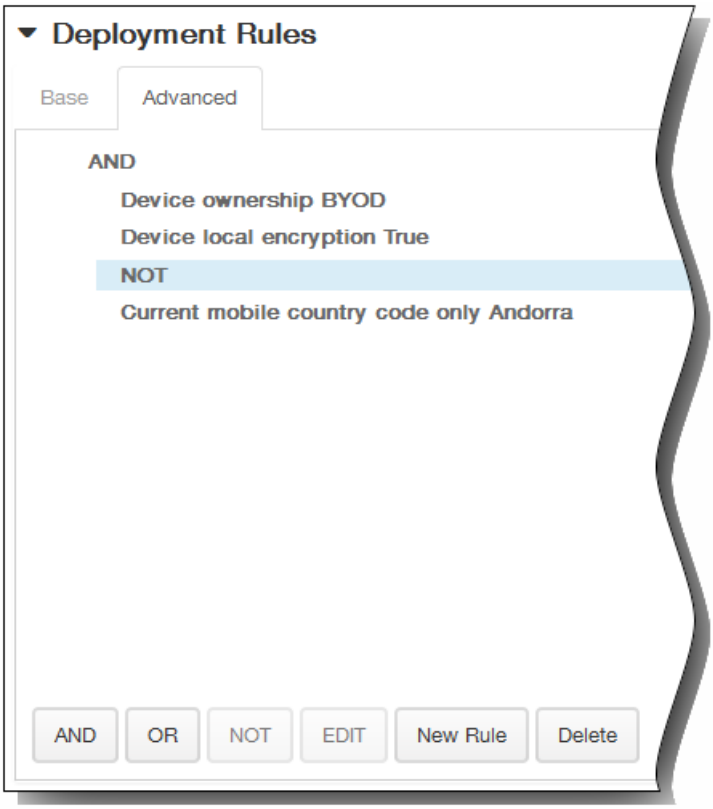
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

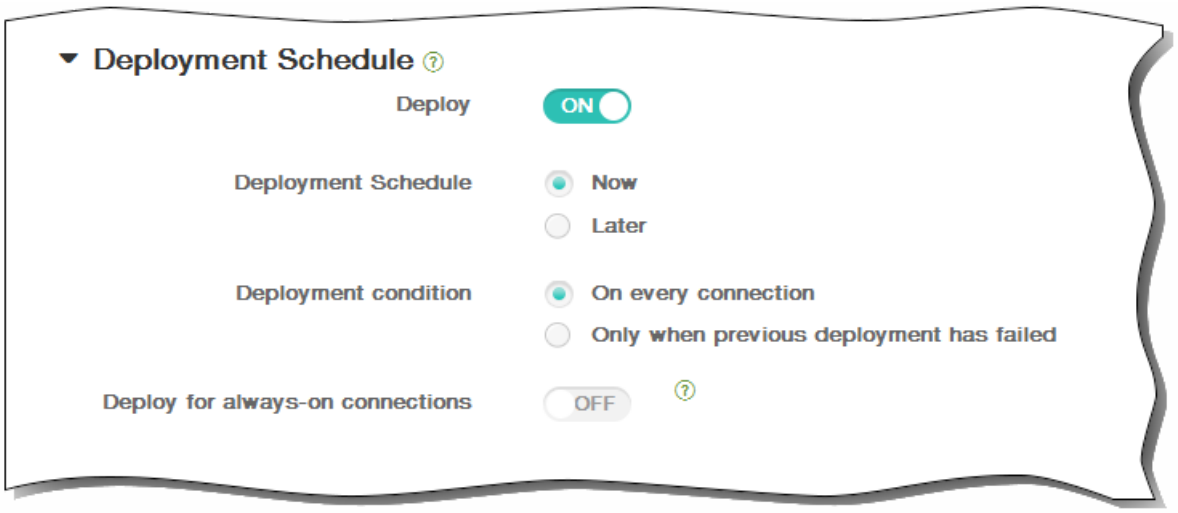
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie kiosque pour Samsung SAFE

Jul 25, 2016

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.

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.

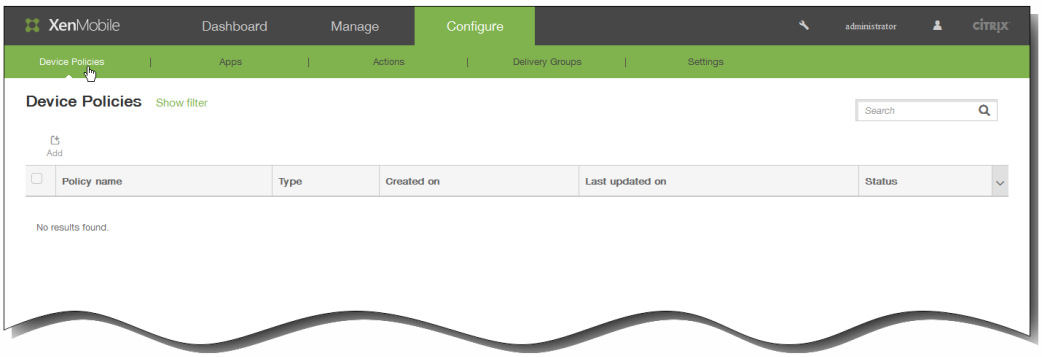
Si vous souhaitez supprimer les appareils du mode kiosque ultérieurement, créez une nouvelle stratégie kiosque pour laquelle le **mode kiosque** est défini sur **Désactiver**. Mettez à jour le ou les groupes de mise à disposition pour supprimer la stratégie kiosque qui activait le mode kiosque et pour ajouter la stratégie kiosque qui désactive le mode kiosque.

Pour ajouter une stratégie kiosque

Remarque :

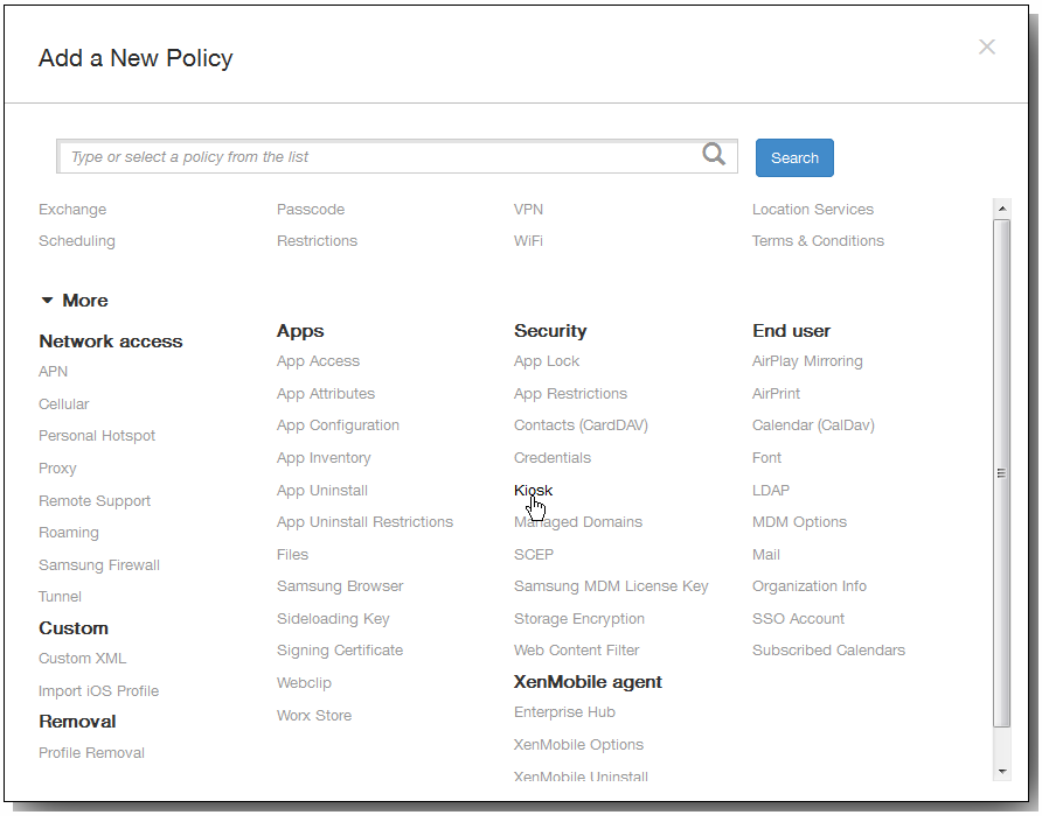
- Toutes les applications que vous spécifiez pour le mode kiosque doivent déjà être installées sur les appareils des utilisateurs.
- Certaines options ne s'appliquent qu'à l'API Samsung Mobile Device Management 4.0 et versions ultérieures.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

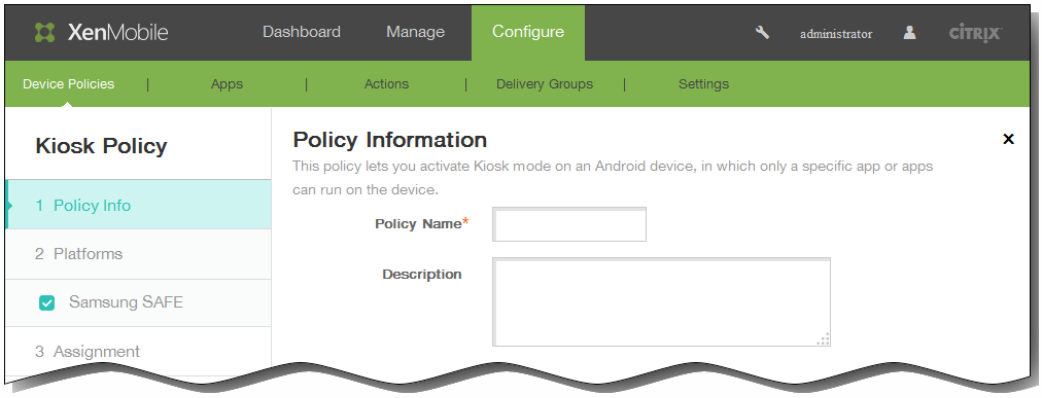


© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

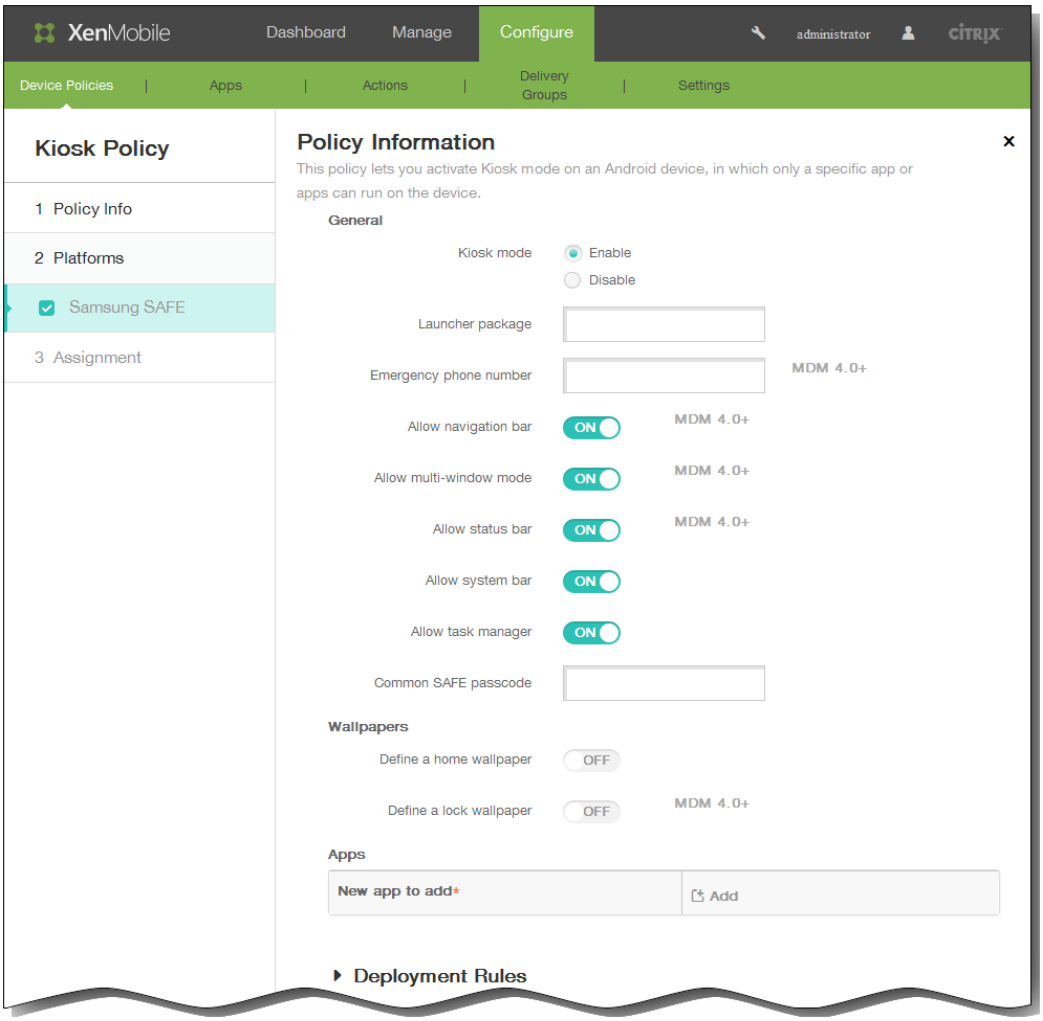


3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Kiosque. La page Stratégie kiosque s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations sur la plate-forme Samsung SAFE s'affiche.

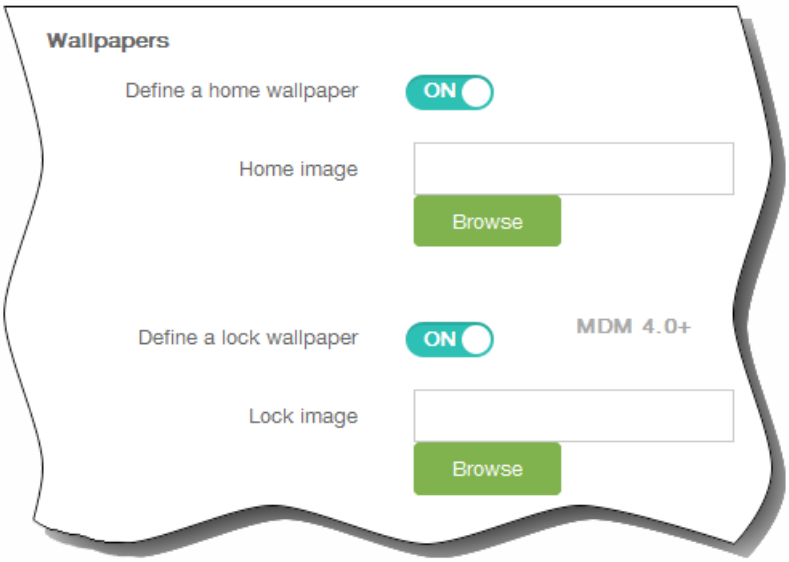
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Sur la page d'informations de la plate-forme Samsung SAFE, entrez les informations suivantes :
    1. Mode kiosque : cliquez sur Activer ou Désactiver. La valeur par défaut est Activer. Lorsque vous cliquez sur Désactiver, toutes les options suivantes disparaissent.
    2. 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.
    3. 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 l'API Samsung Mobile Device Management 4.0 et versions ultérieures.
    4. 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.
    5. 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.
    6. 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.
    7. Autoriser la barre système : sélectionnez cette option pour permettre aux utilisateurs de voir la barre système en mode Kiosque.
    8. Autoriser le gestionnaire de tâches : sélectionnez cette option pour permettre aux utilisateurs de voir et utiliser le gestionnaire de tâches en mode Kiosque.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

9. 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.
10. 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.
11. 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. Lorsque l'une des options précédentes est activée, un champ s'affiche pour vous permettre de choisir l'image personnalisée en cliquant sur Parcourir et en accédant à l'emplacement de l'image.



12. Applications : cliquez sur Ajouter, puis procédez comme suit :
    1. 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.
    2. Cliquez sur Ajouter pour ajouter l'application, ou cliquez sur Annuler pour annuler l'ajout de l'application.
    3. Répétez les étapes i et ii pour chaque application que vous souhaitez 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.

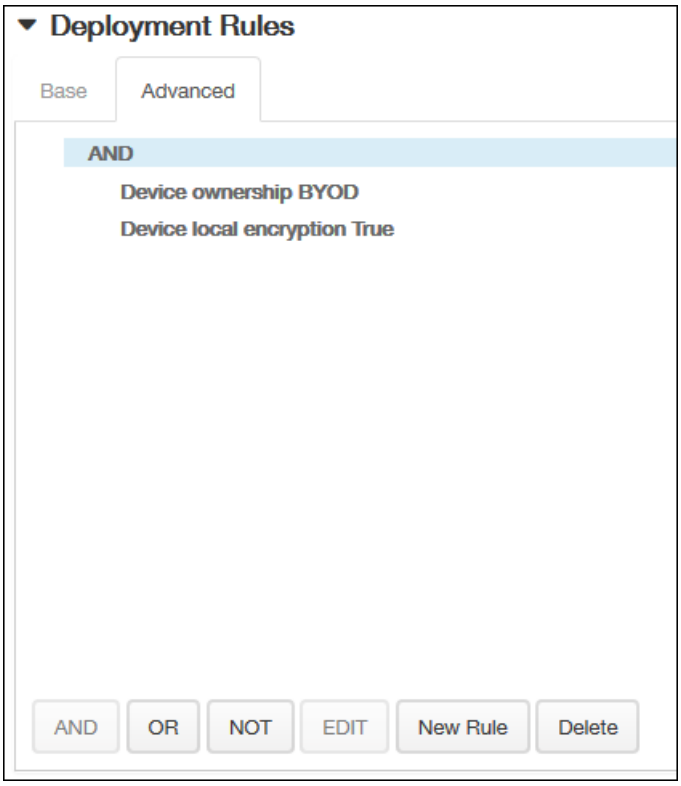
    Pour modifier une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

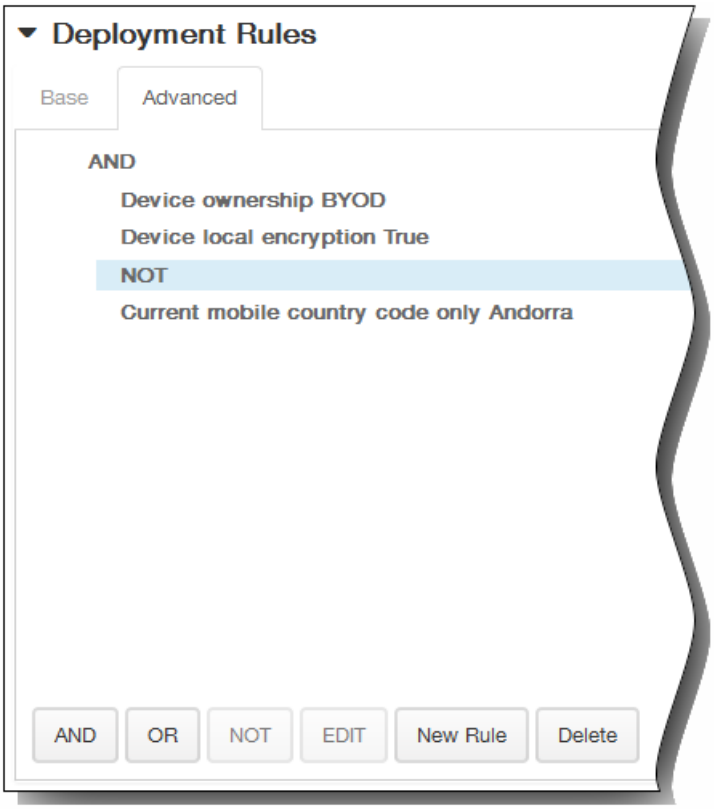
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



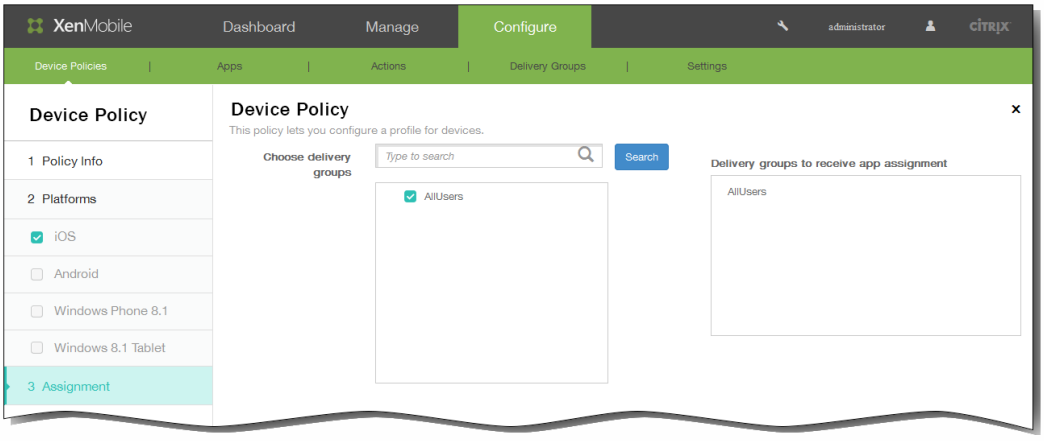
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
    1. Cliquez sur ET, OU ou SAUF.
    2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
       Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
    3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
       Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. Cliquez sur Suivant. 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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



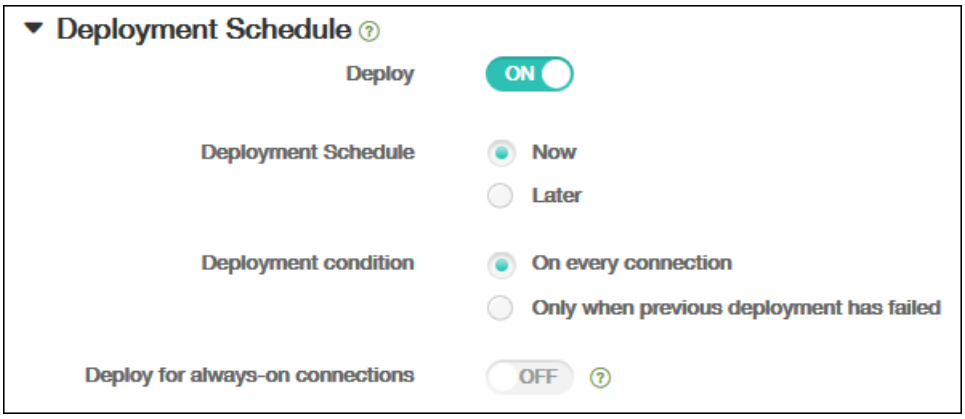
10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

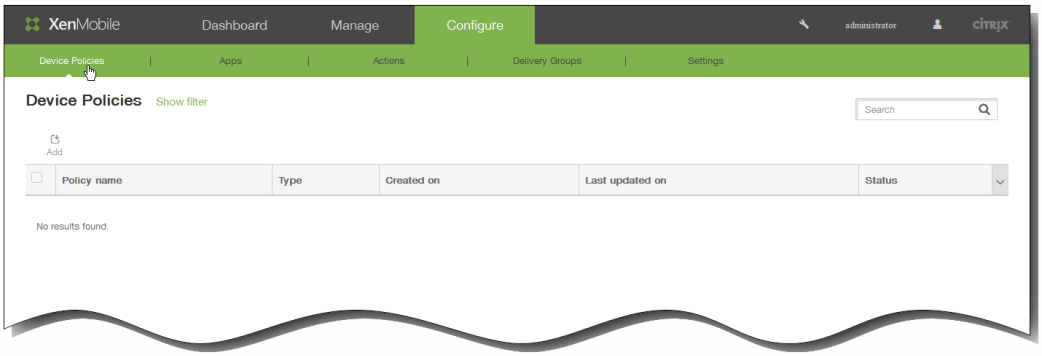
Pour ajouter une stratégie de police pour iOS

Jul 25, 2016

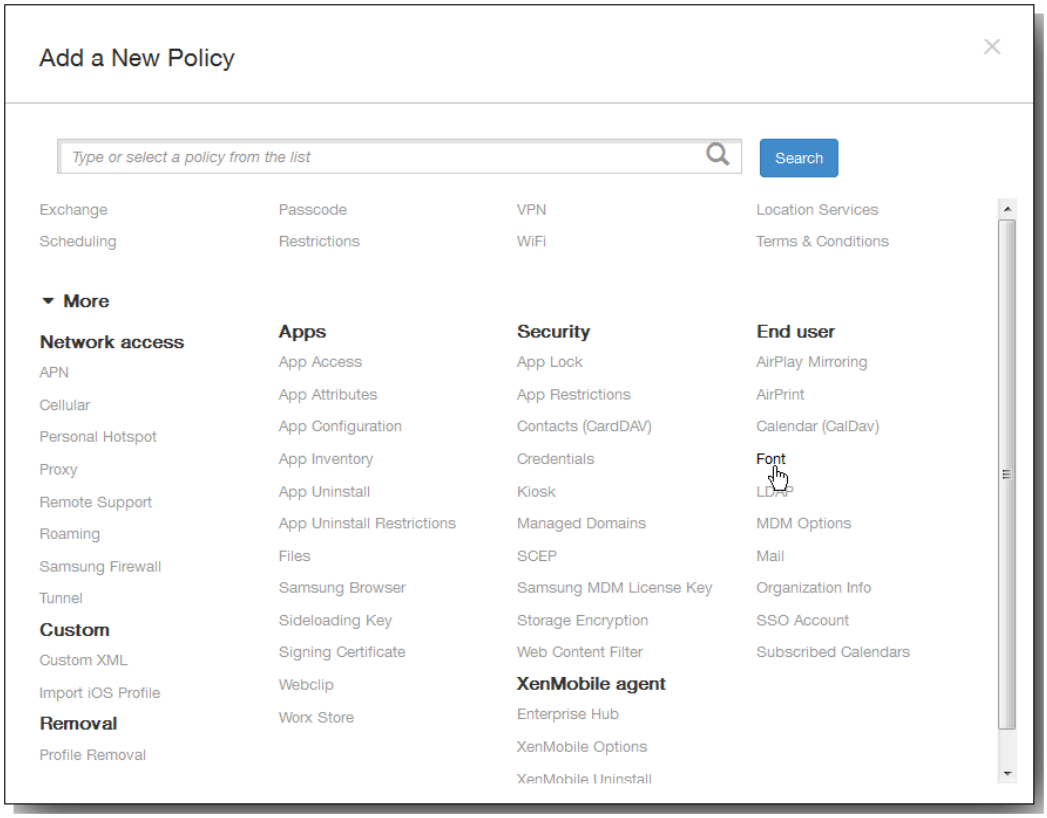
Vous pouvez ajouter une stratégie de police dans XenMobile pour ajouter des polices supplémentaires sur les appareils des utilisateurs. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge.

Remarque : 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.

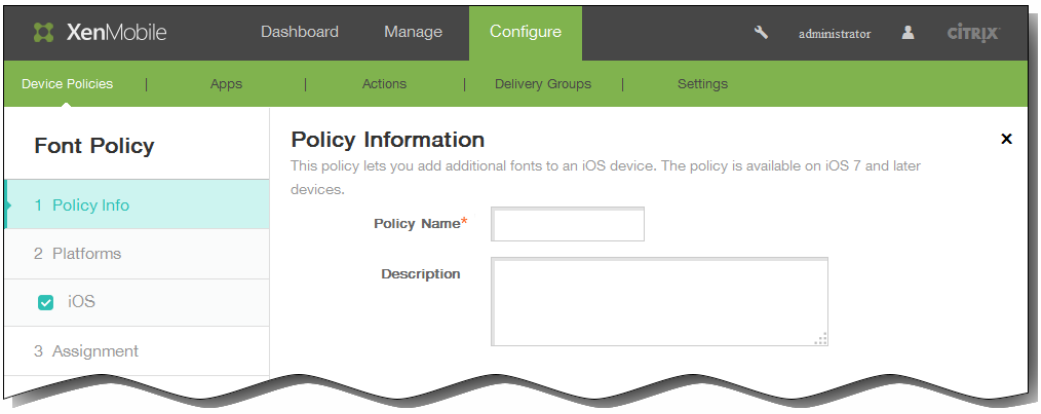


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

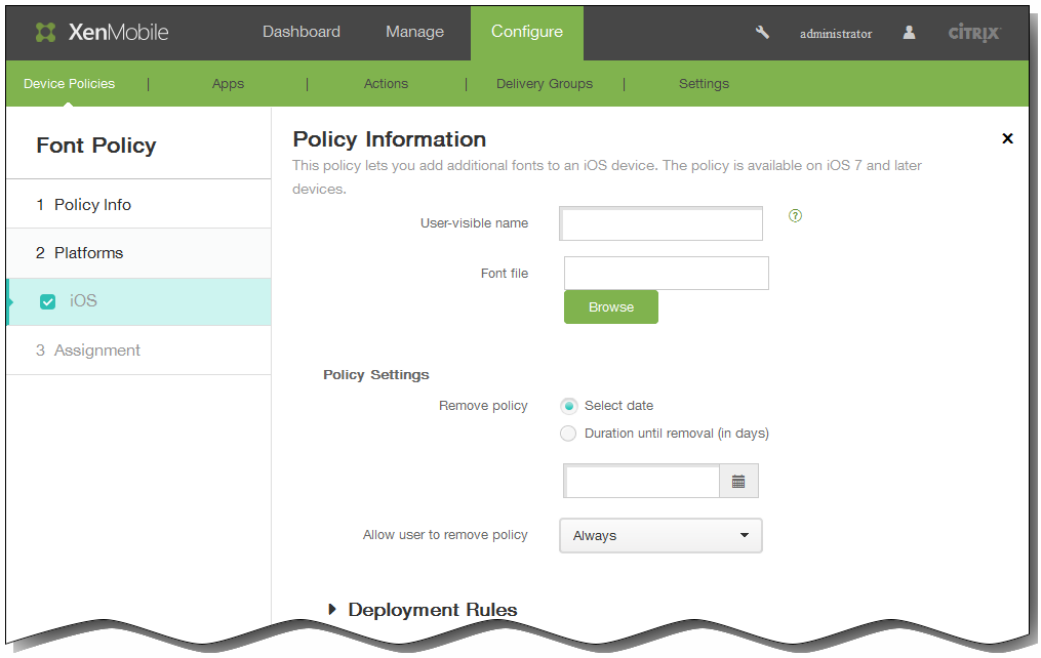


3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Police. La page Stratégie de police s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

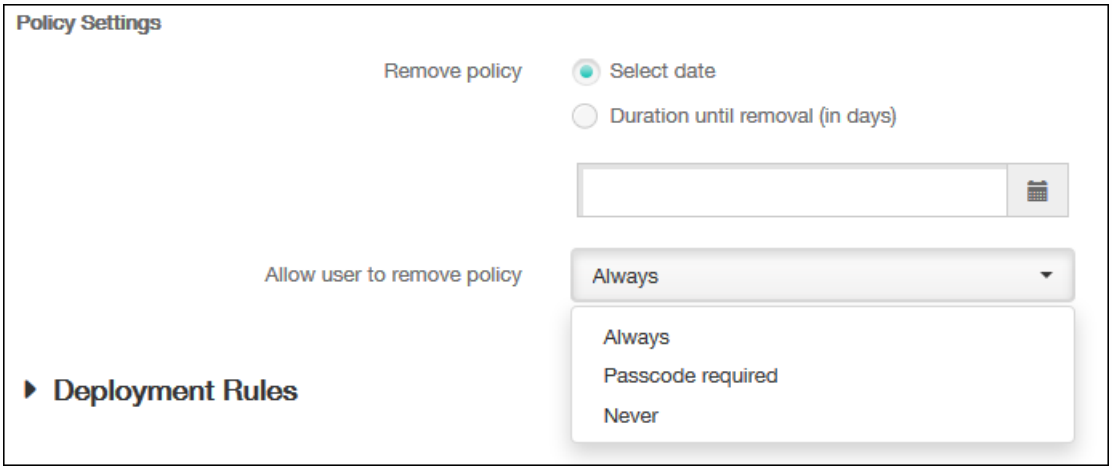


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

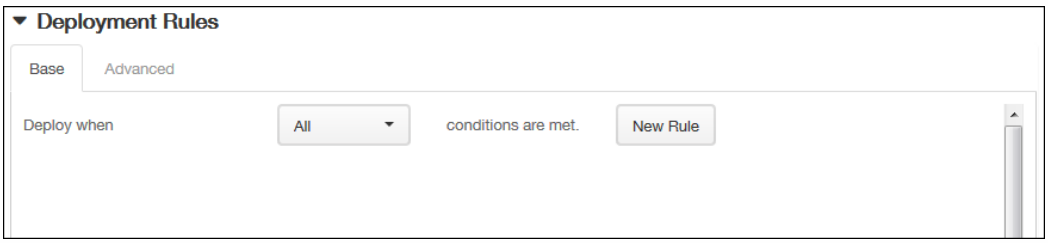


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Nom visible par l'utilisateur : entrez le nom que les utilisateurs voient dans leurs listes de polices.
   2. Fichier de police : sélectionnez le fichier de police à ajouter aux périphériques utilisateur en cliquant sur Parcourir, puis accédez à l'emplacement du fichier.
7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

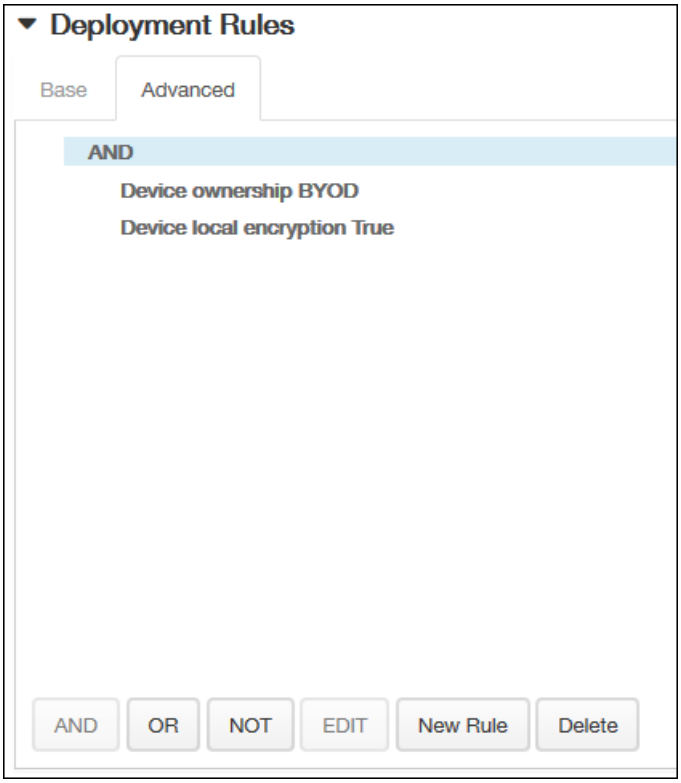


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

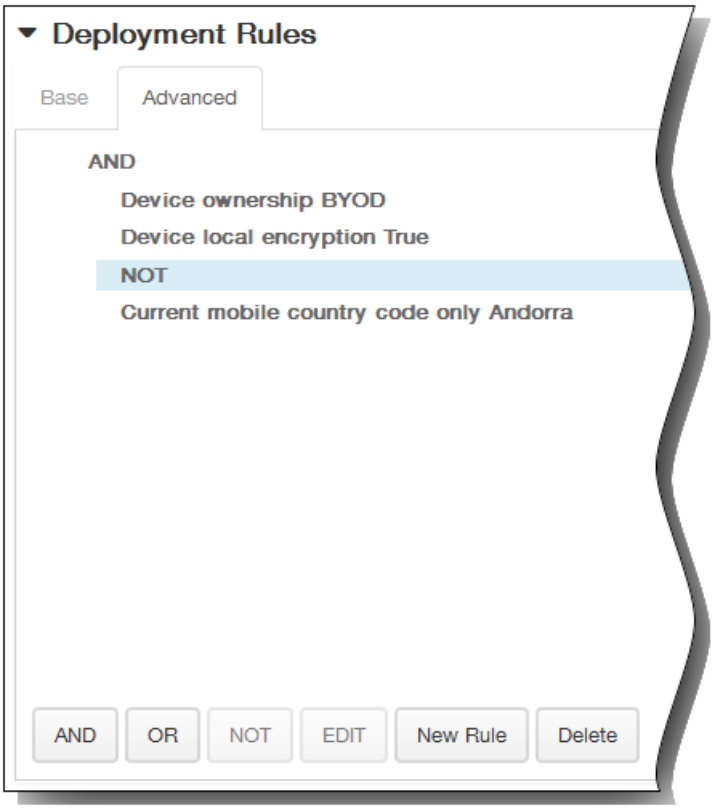


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

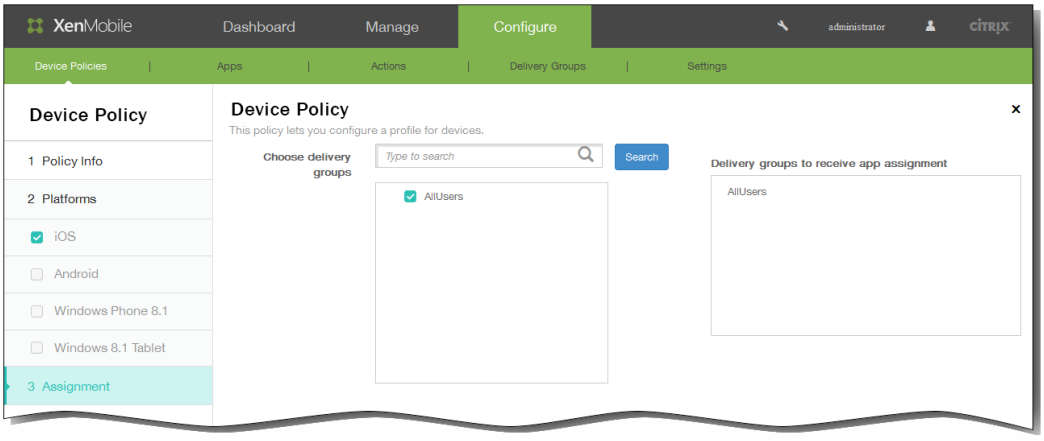
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de police s'affiche.
13. 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.



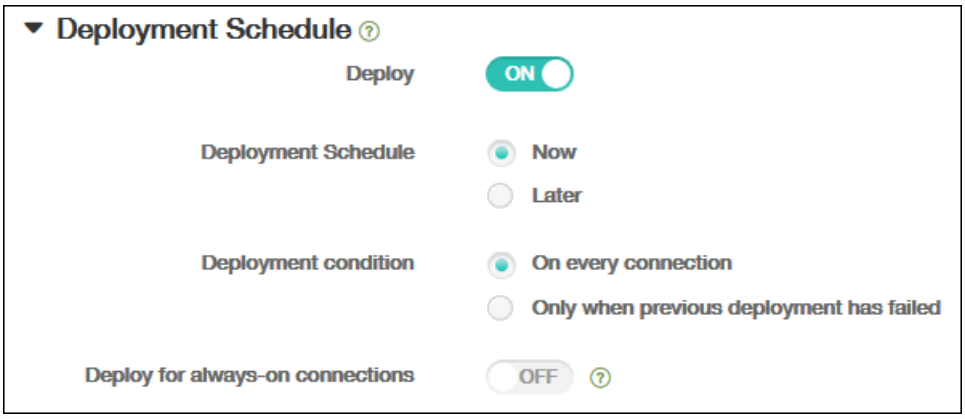
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

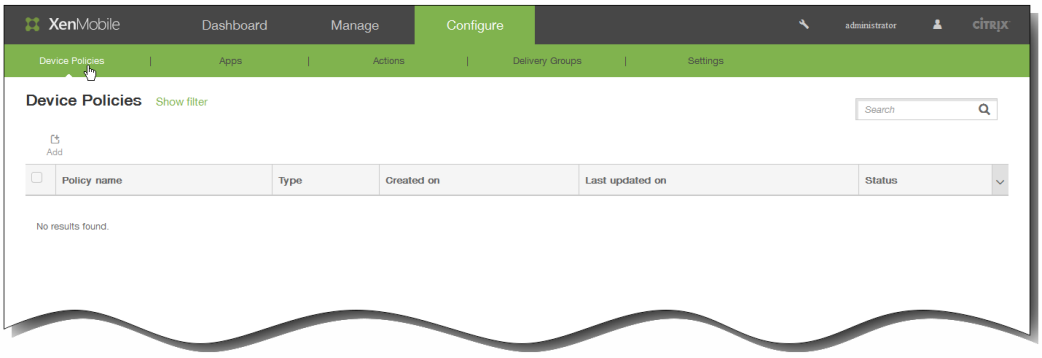
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie de messagerie pour iOS

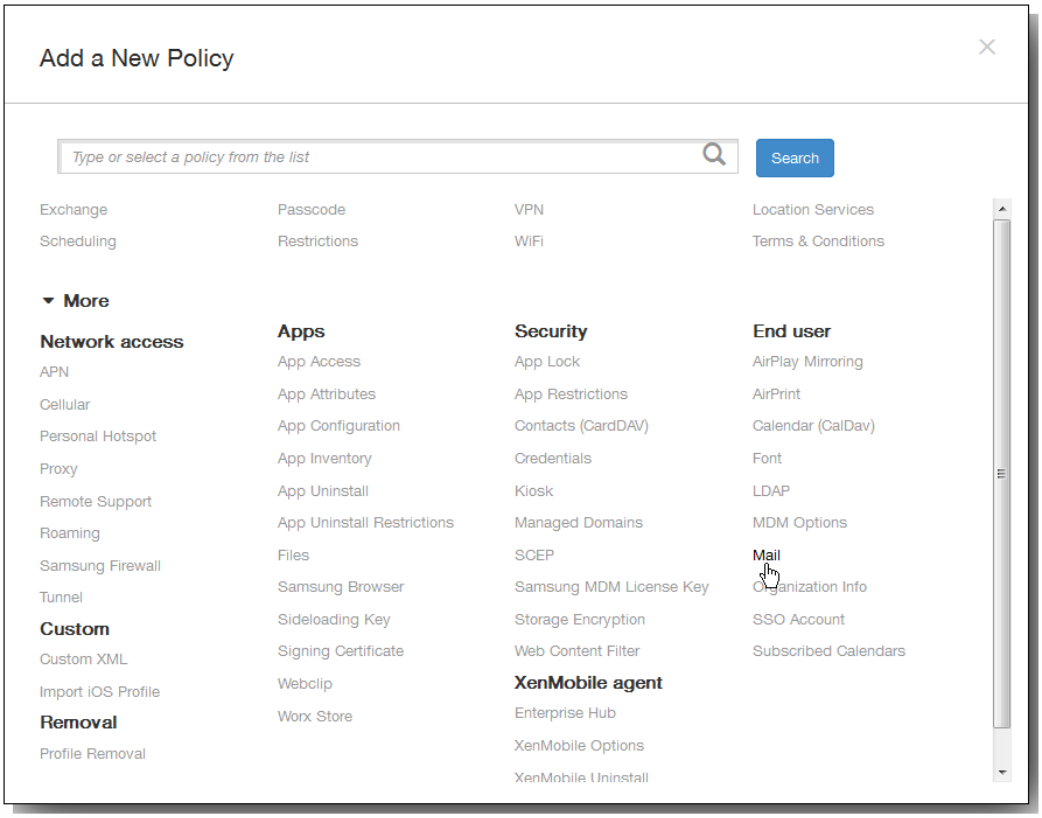
Jul 25, 2016

Vous pouvez ajouter une stratégie de messagerie dans XenMobile pour configurer un compte de messagerie sur les appareils iOS des utilisateurs.

1. Dans la console XenMobile, cliquez sur ConfigurerStratégies d'appareil. La page Stratégies d'appareil s'affiche.

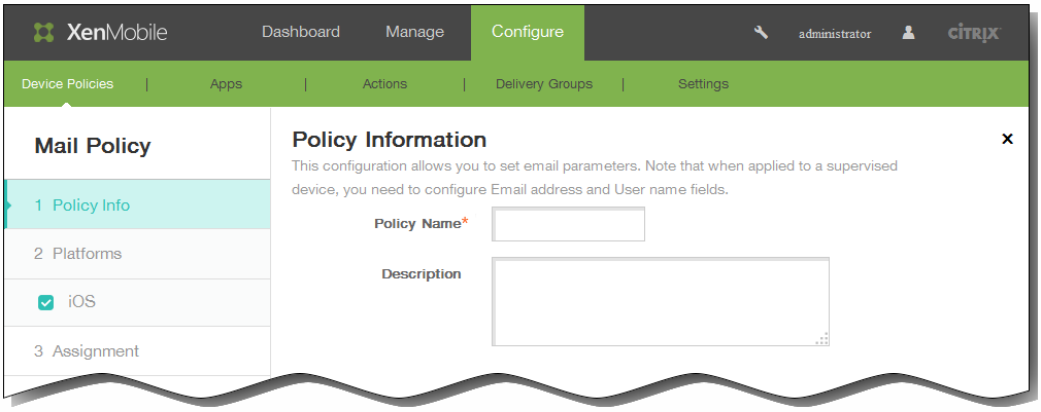


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



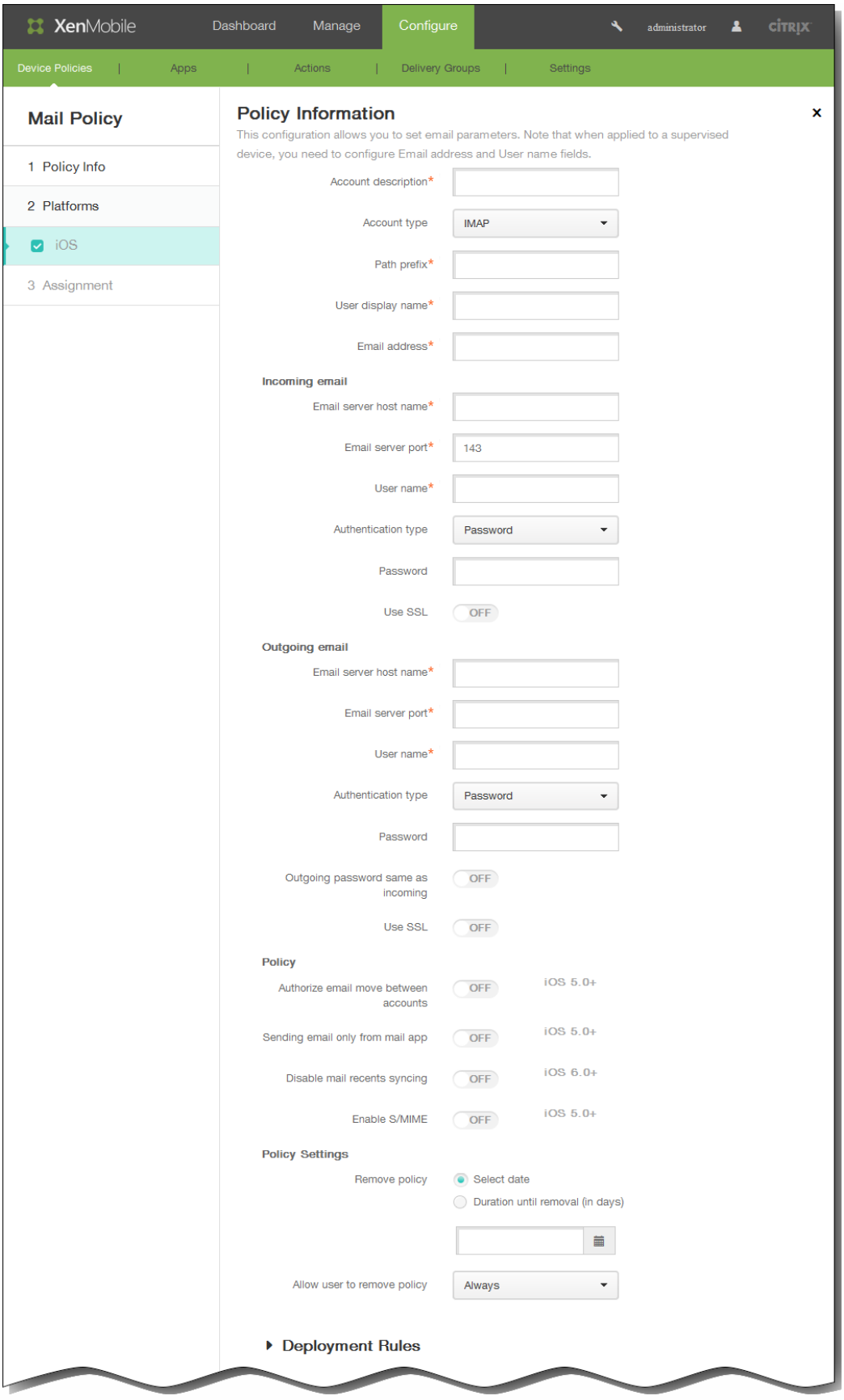
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Description du compte : entrez une description pour le compte ; elle apparaît dans les applications de messagerie et de paramètres. Ce champ est obligatoire.
2. 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.
3. 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.
4. Nom d'affichage de l'utilisateur : entrez le nom d'utilisateur à utiliser dans les messages, etc. Ce champ est obligatoire.
5. Adresse électronique : entrez l'adresse e-mail du compte. Ce champ est obligatoire.

Paramètres du courrier entrant

6. Nom d'hôte du serveur de messagerie : entrez le nom d'hôte ou l'adresse IP du serveur de courrier entrant. Ce champ est obligatoire.
7. 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.
8. 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.
9. 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.
10. Mot de passe : entrez un mot de passe pour le serveur de messagerie du courrier entrant.
11. 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

12. 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.
13. Port du serveur de messagerie : entrez le numéro de port du serveur de messagerie du courrier sortant. Si vous n'entrez pas de numéro de port, le port par défaut du protocole donné est utilisé.
14. 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.
15. 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.
16. Mot de passe : entrez un mot de passe (facultatif) pour le serveur de messagerie pour courrier sortant.
17. 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.
18. Utiliser SSL : sélectionnez cette option pour que le serveur de messagerie du courrier sortant utilise l'authentification SSL. La valeur par défaut est OFF.

Paramètres de stratégie

Remarque : les options s'appliquent uniquement à iOS 5.0 ou versions ultérieures.

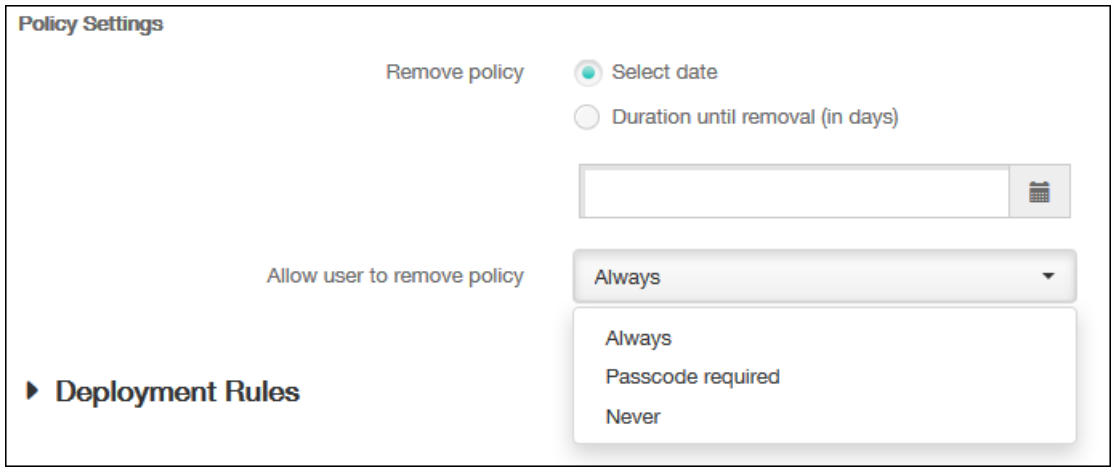
19. Autoriser le déplacement des e-mails entre les comptes : sélectionnez cette option pour autoriser les utilisateurs à déplacer les messages de ce compte vers un autre compte et à transférer des messages et y répondre à partir d'un autre compte. La valeur par défaut est OFF, ce qui permet aux utilisateurs de déplacer des messages vers un autre compte et de les transférer et y répondre à partir d'un autre compte.
20. N'envoyer des e-mails que depuis l'application de messagerie : sélectionnez cette option si vous voulez que les

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

utilisateurs soient uniquement autorisés à envoyer des e-mails avec l'application de messagerie iOS.

21. 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.
22. 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.
23. Informations d'identification de l'identité de signature : dans la liste, sélectionnez les informations d'identification de signature à utiliser.
24. Informations d'identification de l'identité de chiffrement : dans la liste, sélectionnez les informations d'identification de chiffrement à utiliser.

7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.



11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

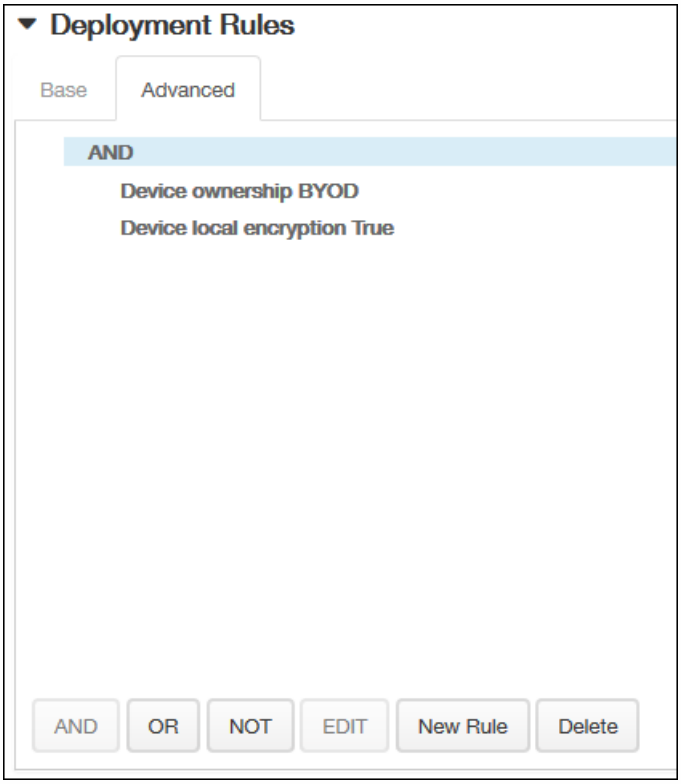


1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

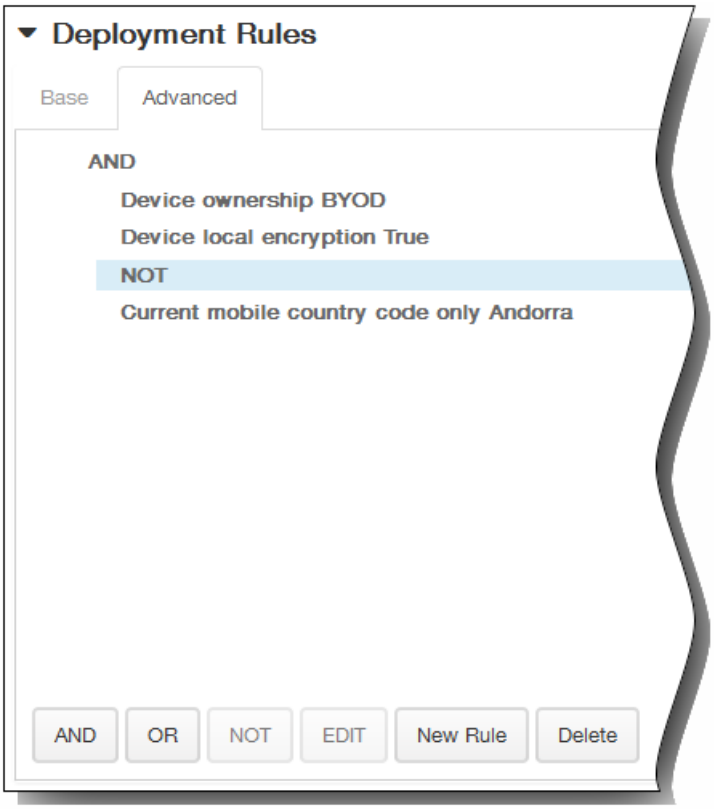
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



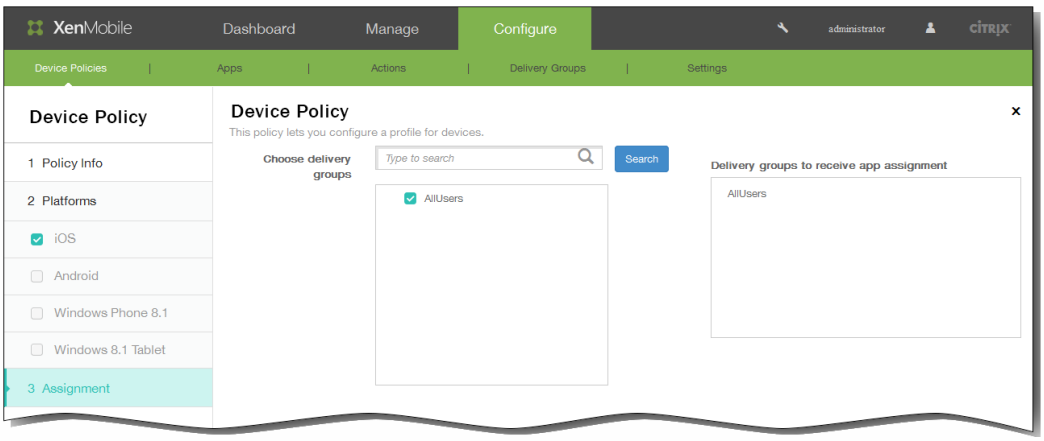
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de messagerie s'affiche.
13. 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.

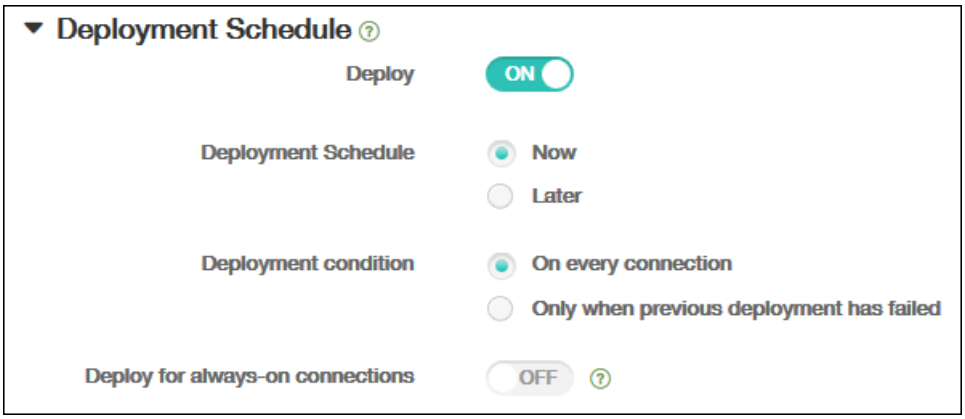


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
4. 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.
5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Stratégies de domaines gérés

Jul 25, 2016

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.

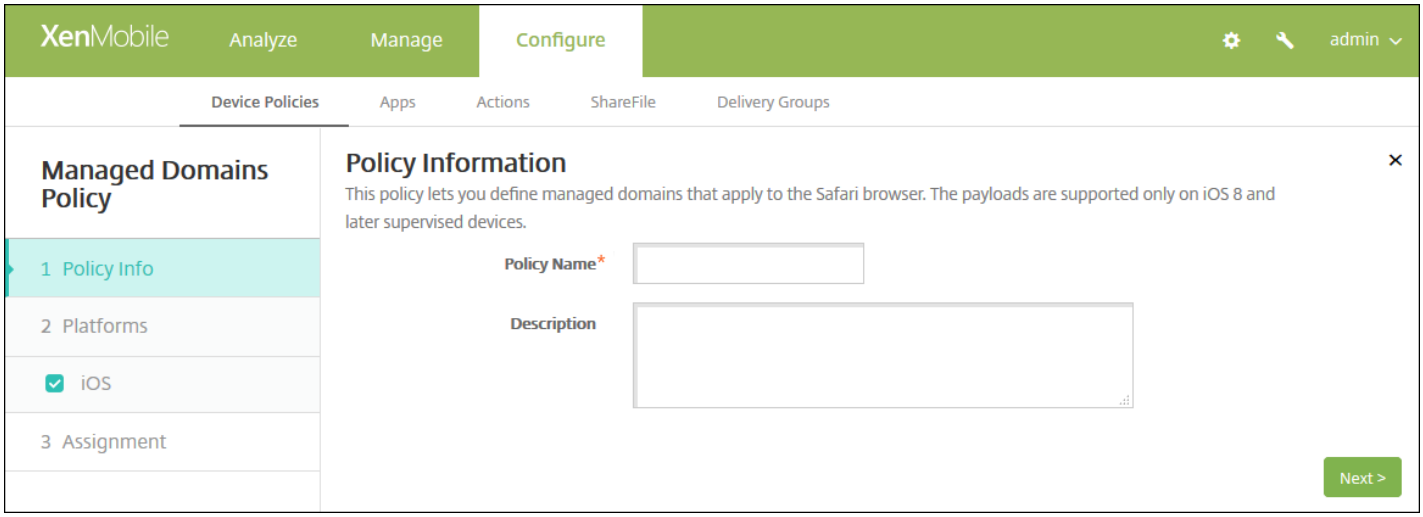
Lorsqu'un utilisateur envoie un e-mail à un destinataire dont le domaine n'est pas sur la liste des domaines de messagerie gérés, un message s'affiche sur l'appareil de l'utilisateur pour l'avertir qu'il envoie un message à un utilisateur en dehors de votre domaine d'entreprise.

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.

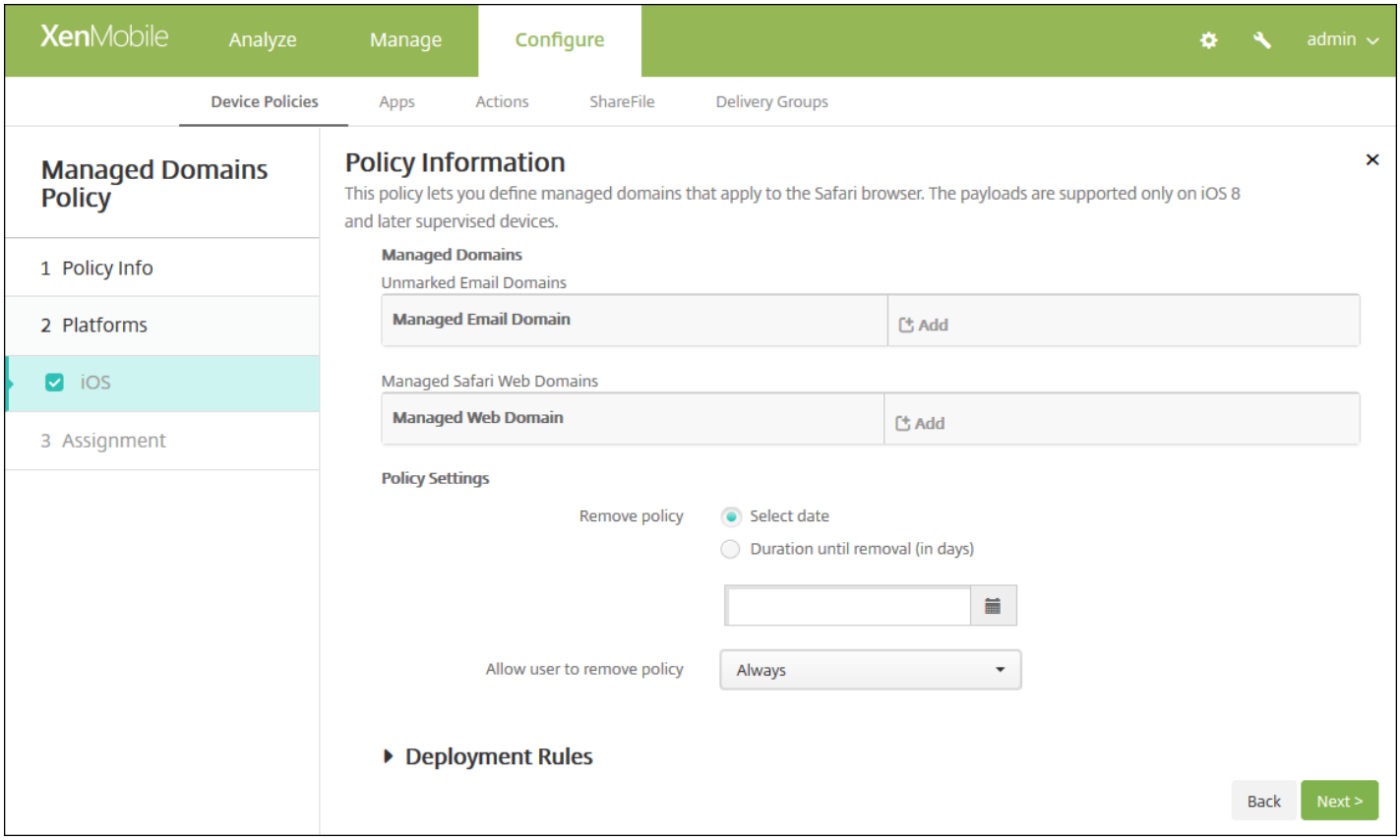


4. Dans la page **Informations sur la stratégie**, entrez les informations suivantes :

- **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 **Plate-forme iOS** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

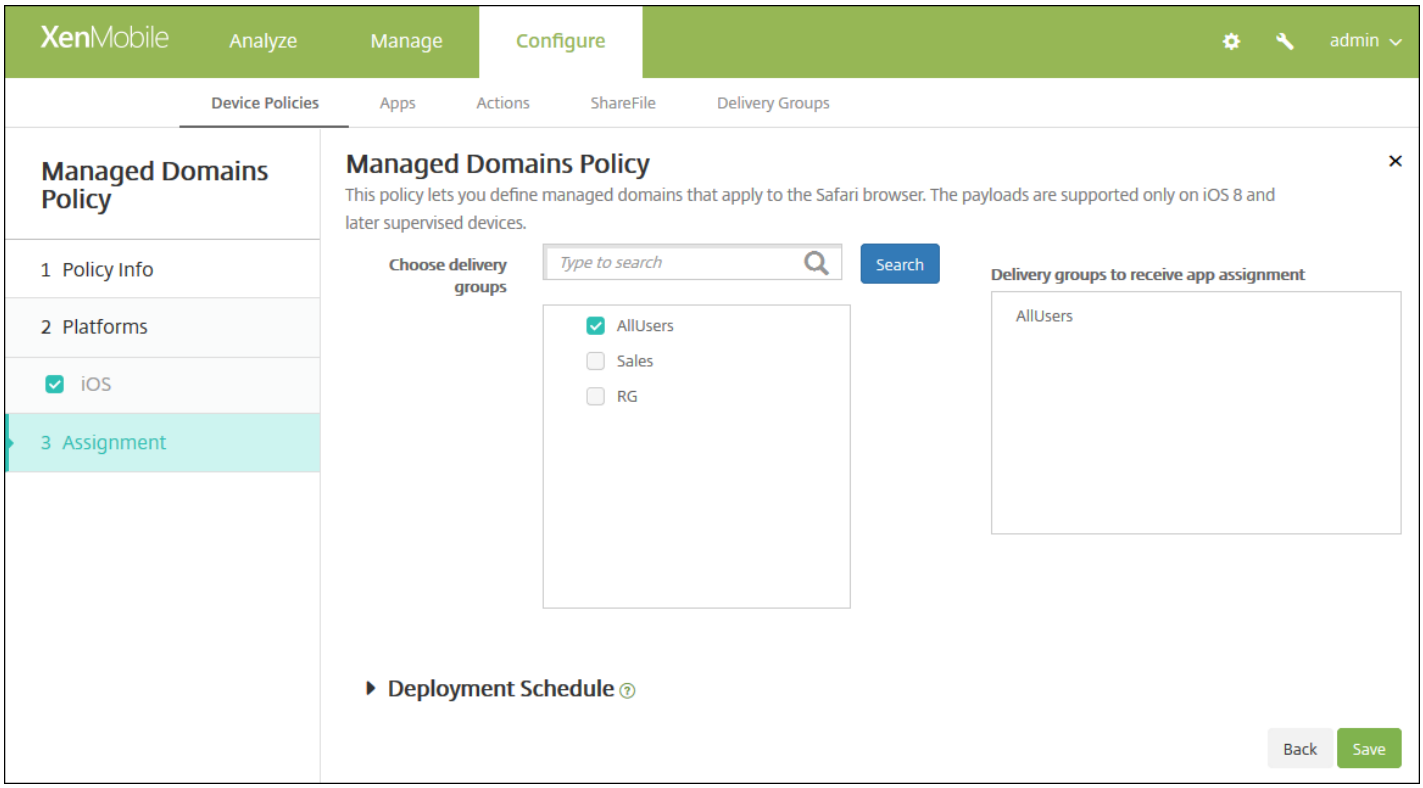
- **Paramètres de stratégie**
  - Sous **Paramètres de stratégie**, à côté de **Supprimer la stratégie**, cliquez sur **Sélectionner une date** ou **Délai avant suppression (en jours)**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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**.

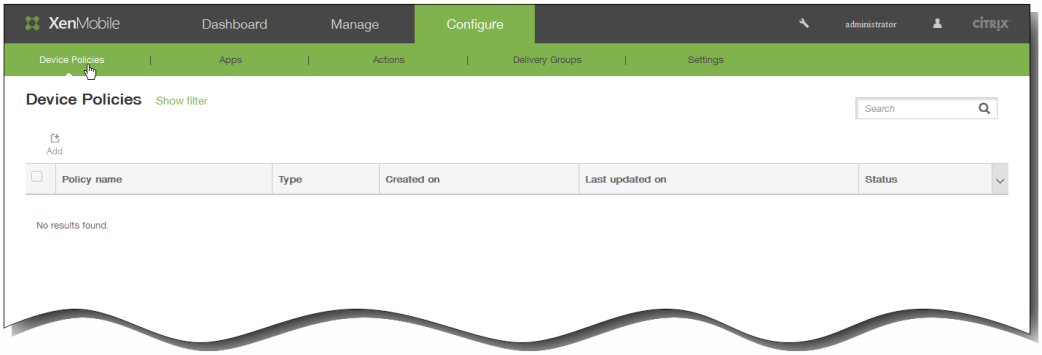
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une stratégie d'informations sur l'organisation pour iOS

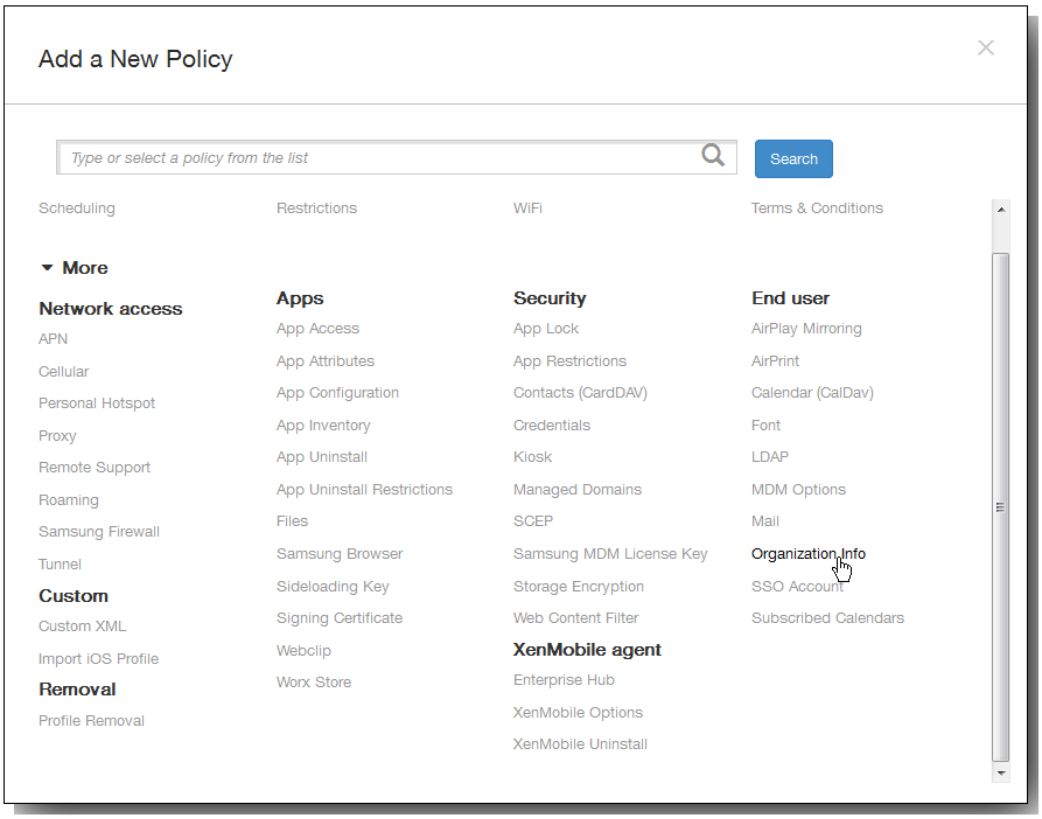
Jul 25, 2016

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.

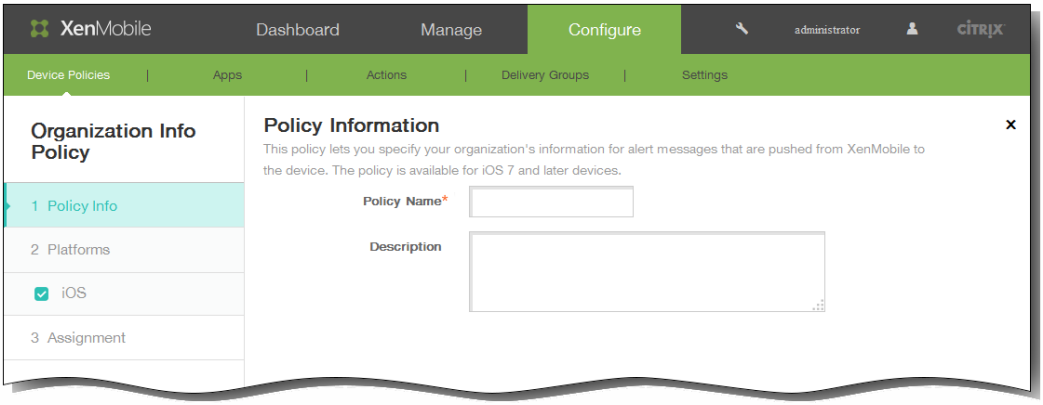


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

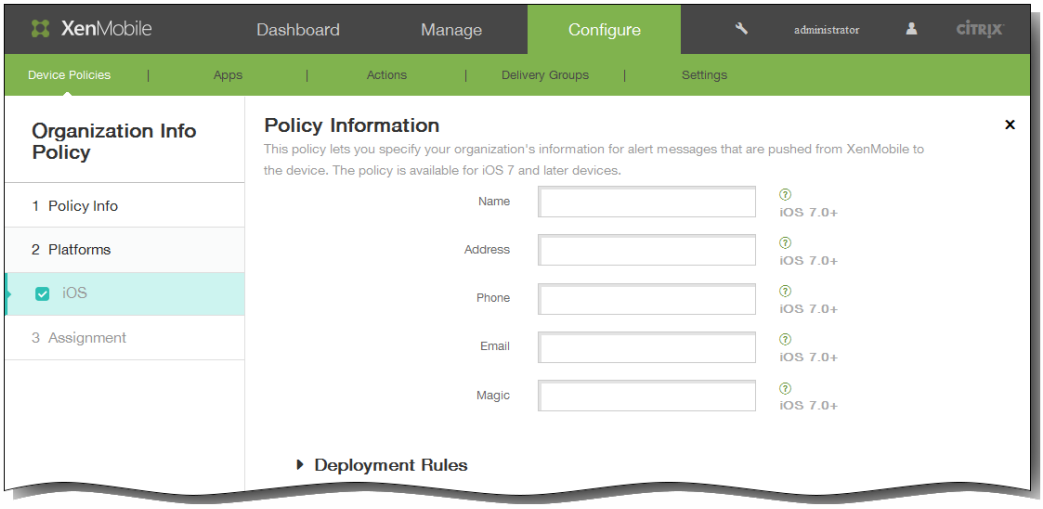


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

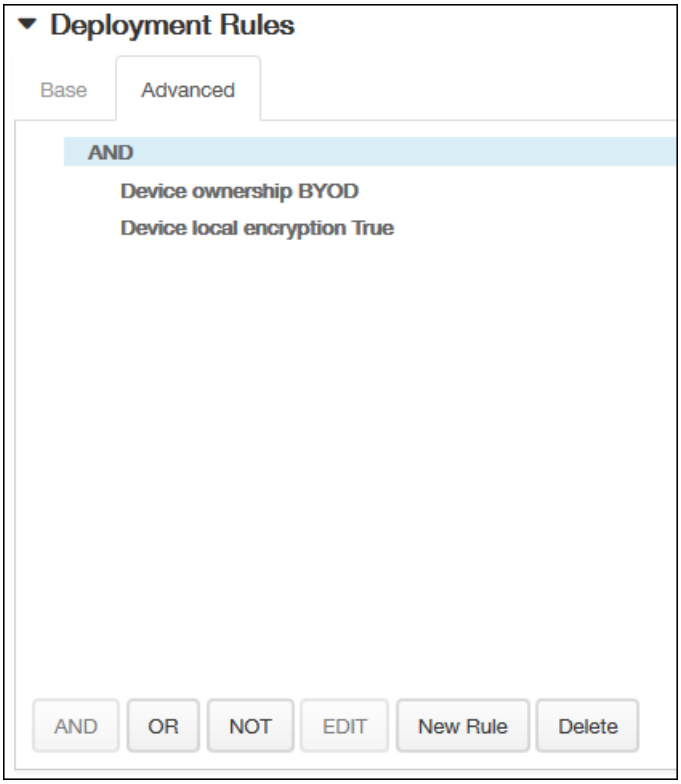


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Nom : entrez le nom de l'organisation exécutant XenMobile.
   2. Adresse : entrez l'adresse de l'organisation.
   3. Téléphone : entrez le numéro de téléphone d'assistance de l'organisation.
   4. Adresse électronique : entrez l'adresse e-mail d'assistance.
   5. Magic : entrez un mot ou une phrase décrivant les services gérés par l'organisation.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



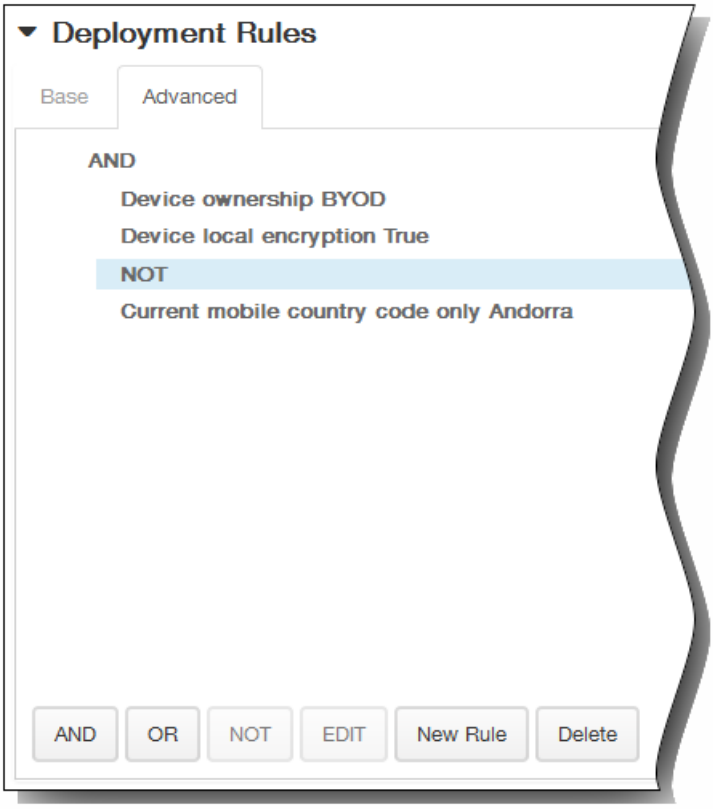
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



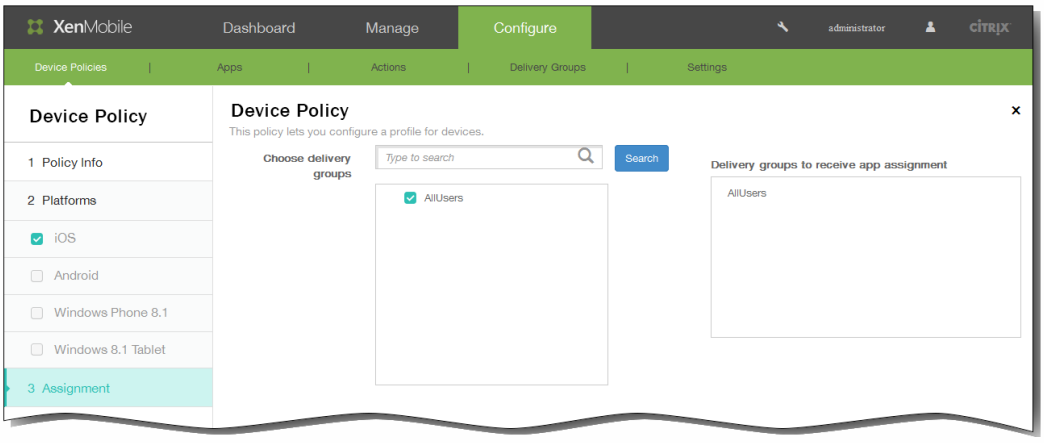
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

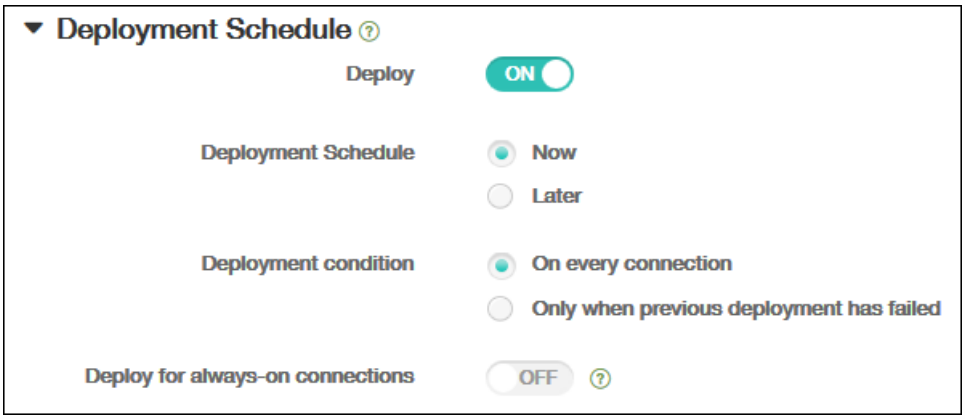


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
4. 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.
5. 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

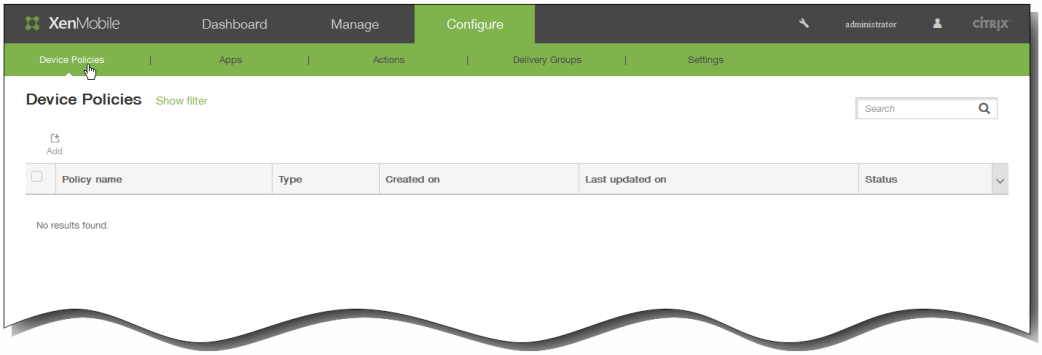
Pour ajouter une stratégie LDAP pour iOS

Jul 25, 2016

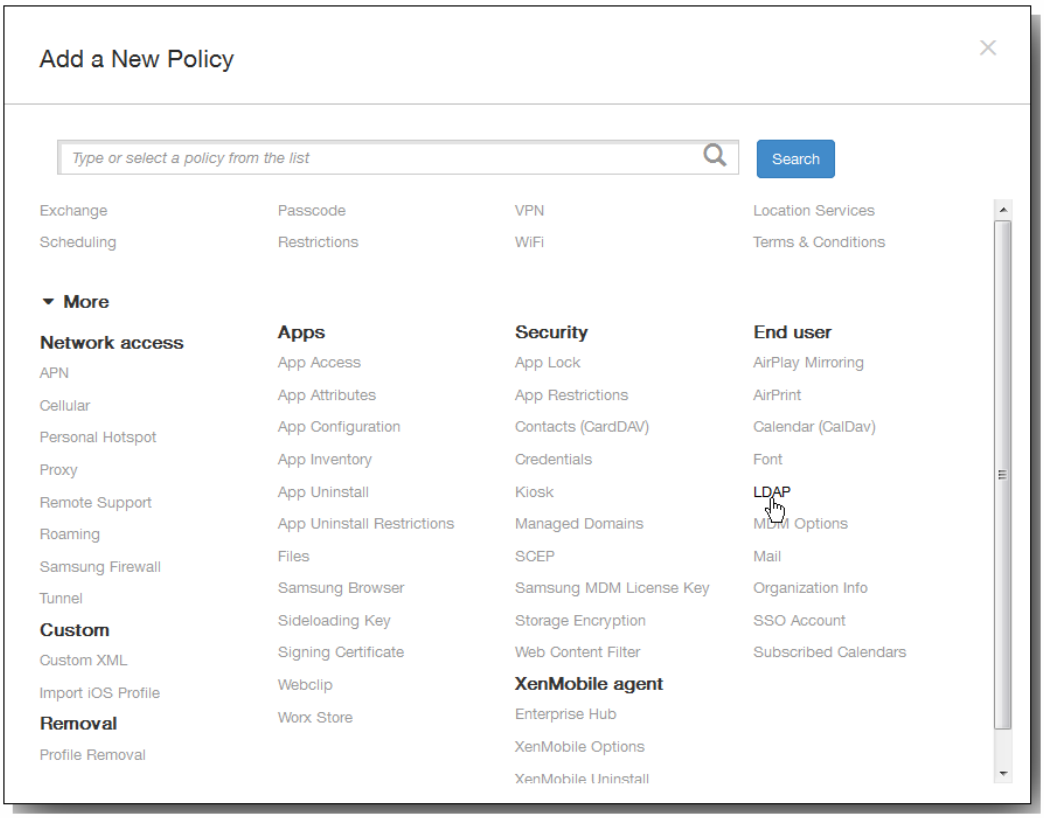
Vous créez une stratégie LDAP pour appareils iOS dans XenMobile pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information sur le compte nécessaires. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.

Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

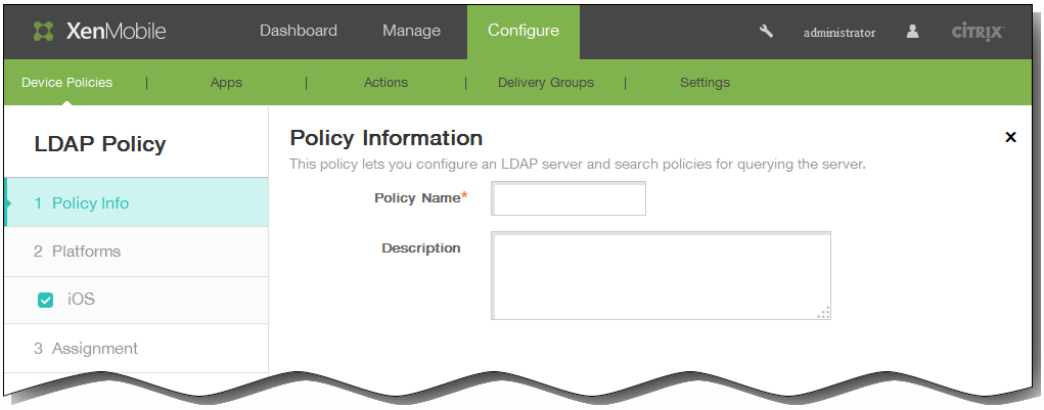


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

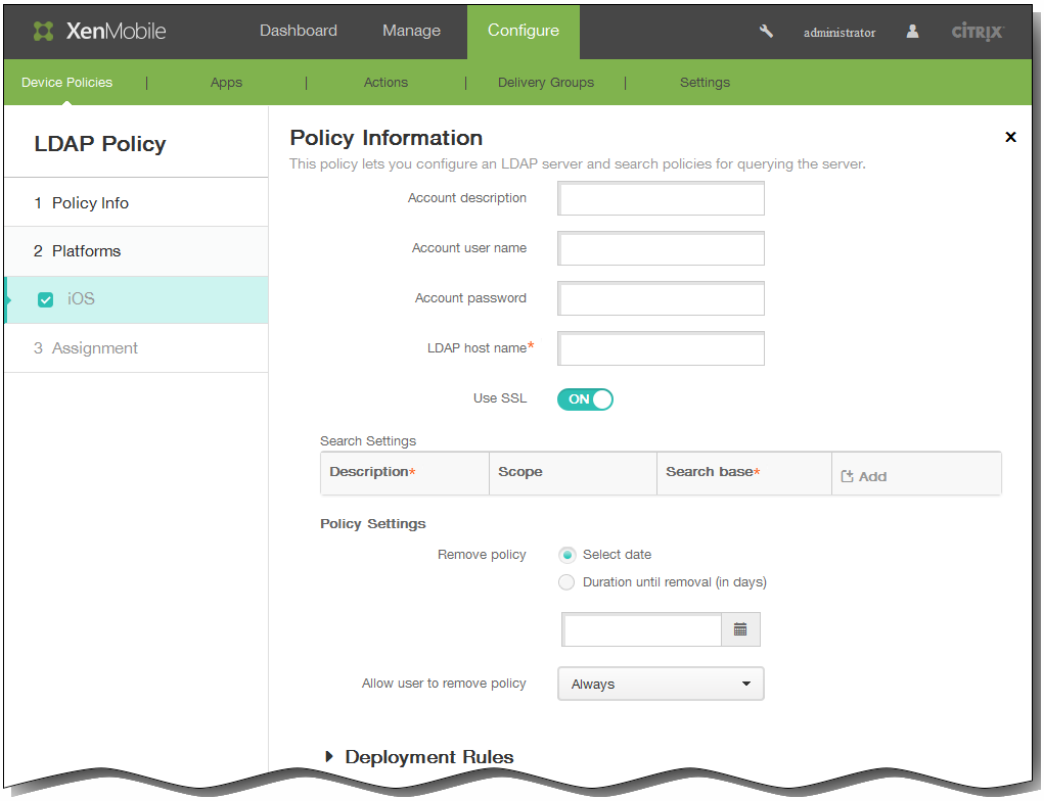


© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur 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 :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Plate-forme iOS s'affiche.

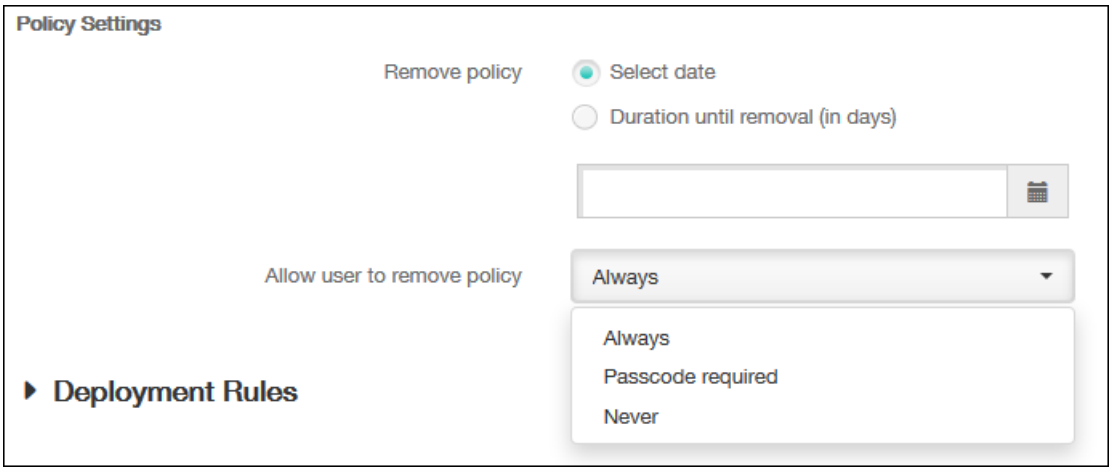


6. Sur la page d'informations Plate-forme iOS, entrez les informations suivantes :
   1. Description du compte : entrez une description du compte (facultatif).
   2. Nom d'utilisateur du compte : entrez un nom d'utilisateur (facultatif).
   3. Mot de passe du compte : entrez un mot de passe (facultatif). À utiliser uniquement avec des profils chiffrés.
   4. Nom d'hôte LDAP : entrez le nom d'hôte du serveur LDAP. Ce champ est obligatoire.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est ON.
6. Paramètres de recherche : cliquez sur Ajouter et procédez comme suit :
   Remarque : 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.
   1. Description : entrez une description pour le paramètre de recherche. Ce champ est obligatoire.
   2. 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.
   3. Base de recherche : entrez le chemin d'accès au nœud à partir duquel démarrer une recherche. Exemple : `ou=people` ou `0=example corp`. Ce champ est obligatoire.
   4. Cliquez sur Ajouter pour ajouter le paramètre de recherche ou cliquez sur Annuler pour annuler l'ajout du paramètre de recherche.
   5. Répétez les étapes i à iv 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.
7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

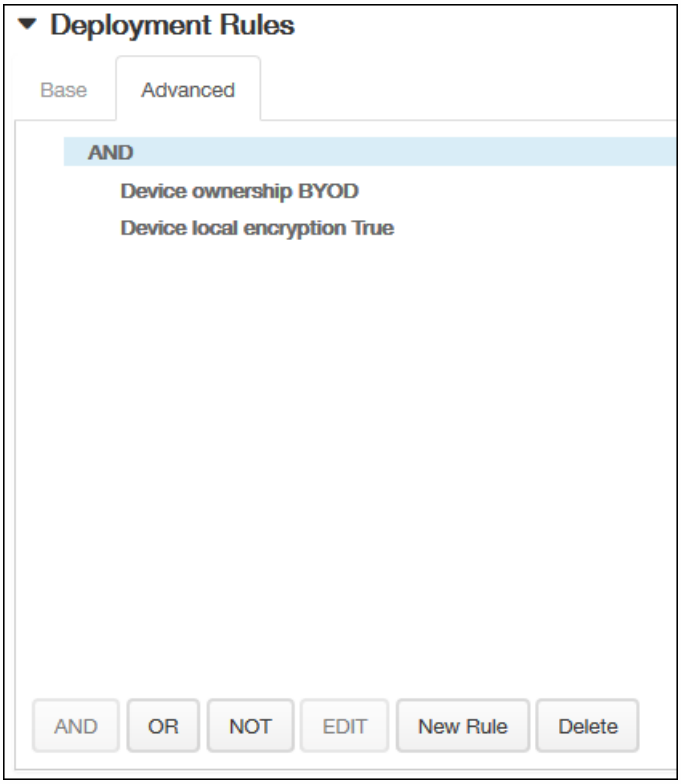


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



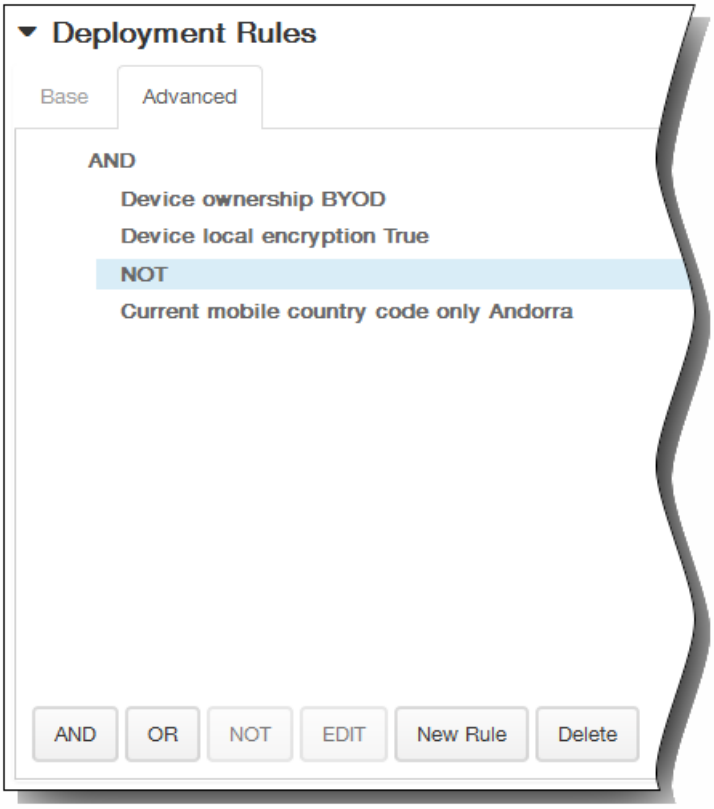
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



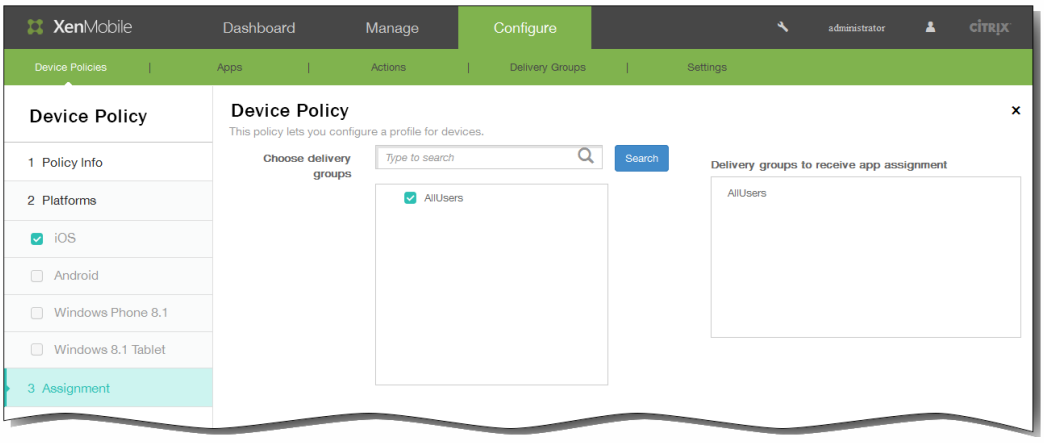
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie LDAP s'affiche.
13. 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.

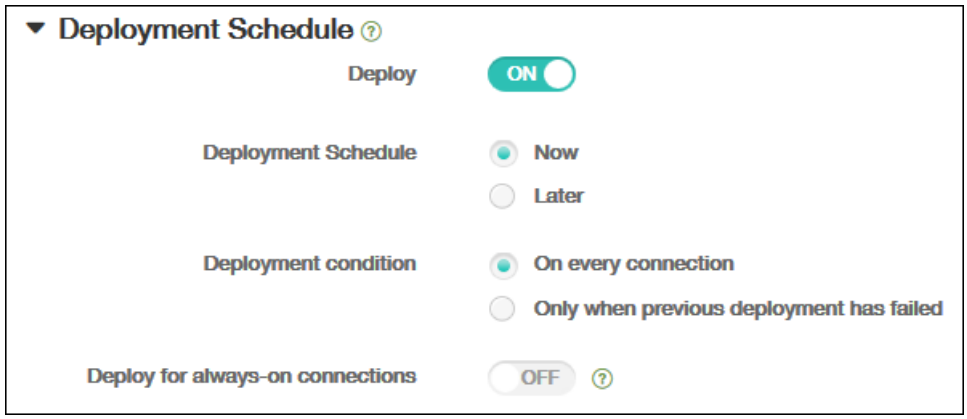


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
4. 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.
5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

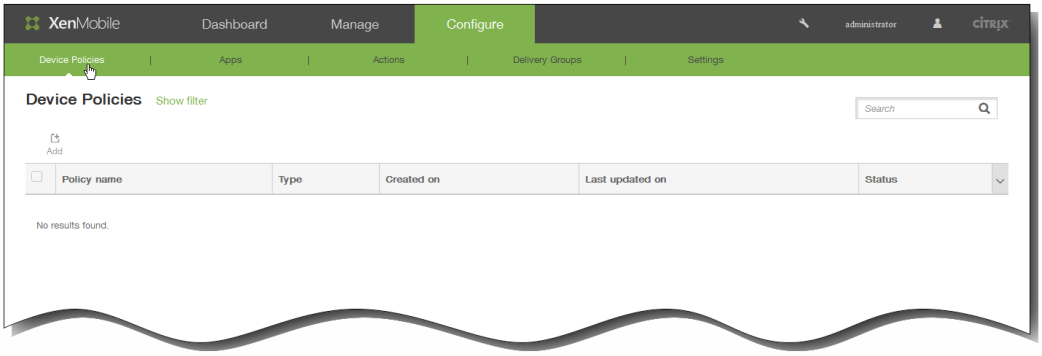
Pour ajouter une stratégie de compte SSO pour iOS

Jul 25, 2016

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.

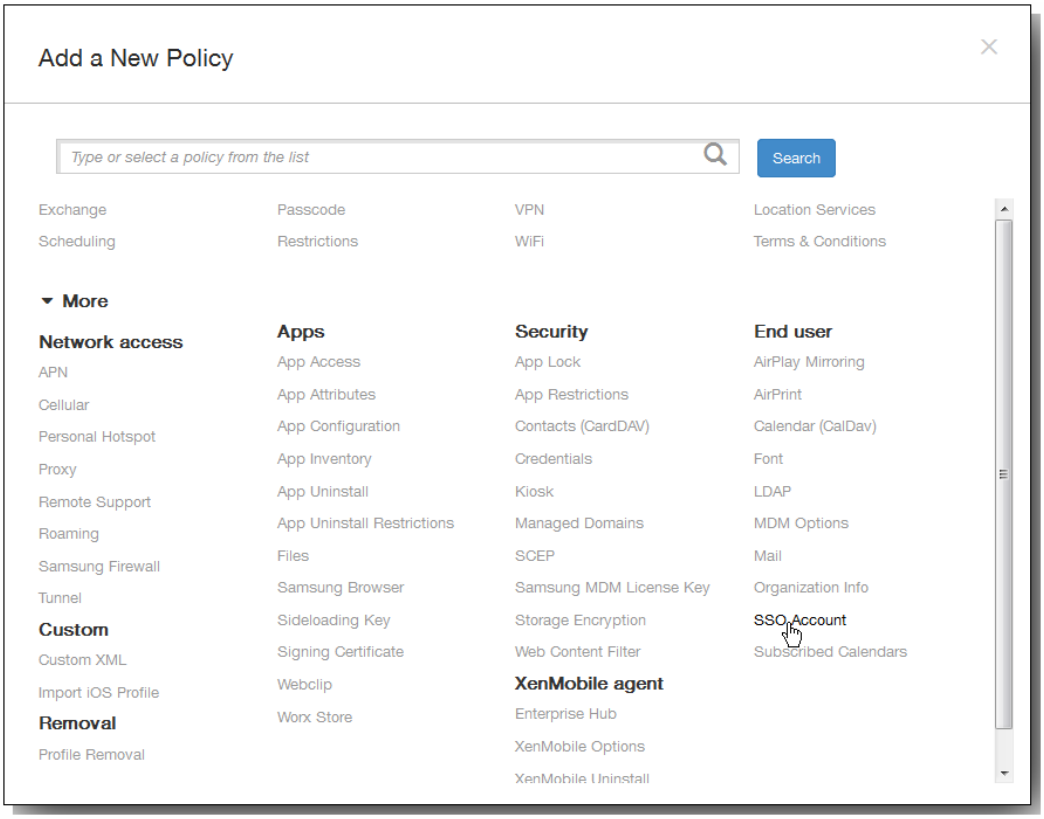
Remarque : cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

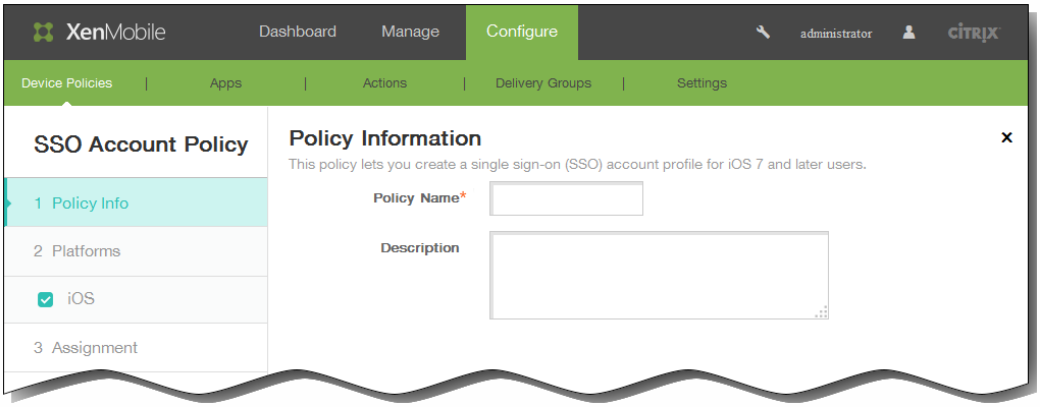


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

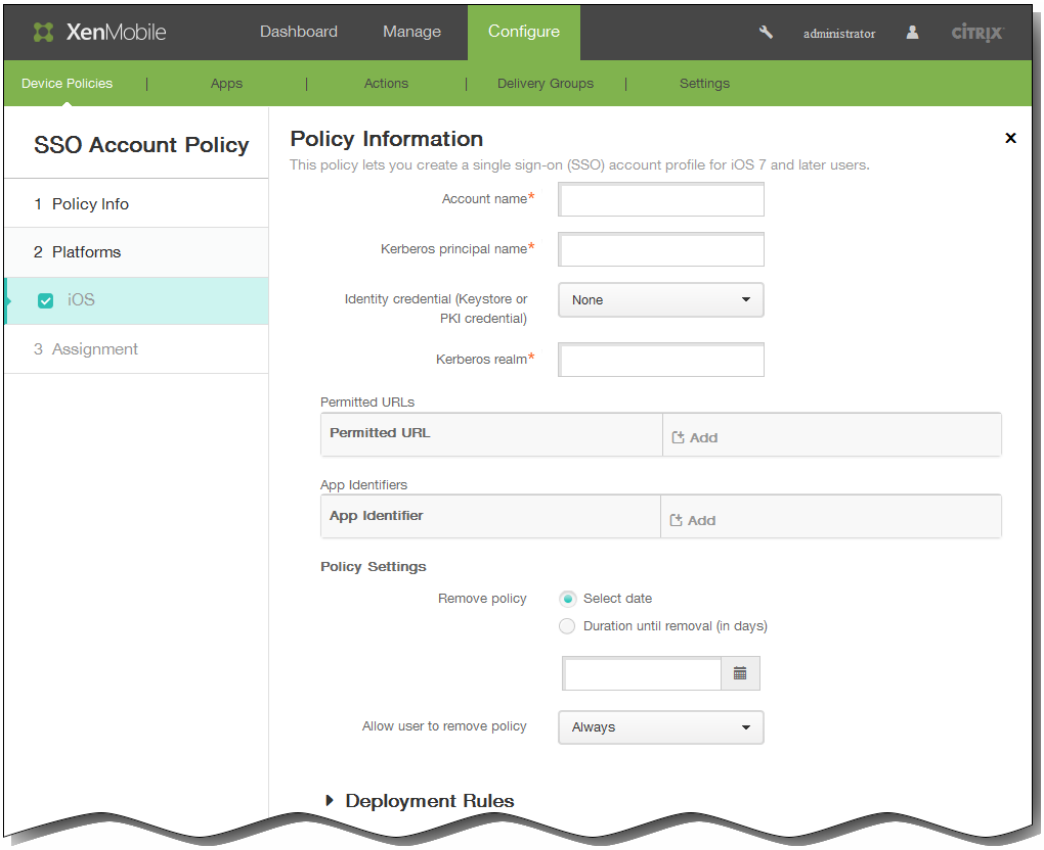


3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Compte SSO. La page Stratégie de compte SSO s'affiche.



4. Dans le panneau d'informations Stratégie de compte SSO, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Plate-forme iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Sur la page d'informations Plate-forme iOS, entrez les informations suivantes :
    1. Nom du compte : entrez le nom du compte SSO Kerberos qui s'affiche sur les appareils des utilisateurs. Ce champ est obligatoire.
    2. Nom principal Kerberos : entrez le nom principal Kerberos. Ce champ est obligatoire.
    3. Infos d'identification de l'identité (infos d'identification magasin de clés ou PKI) : dans la liste, cliquez sur des infos d'identification de l'identité qui peuvent être utilisées pour renouveler les infos d'identification Kerberos sans intervention de l'utilisateur.
    4. Domaine Kerberos : entrez le domaine Kerberos pour cette stratégie. Il s'agit généralement de votre nom de domaine en lettres majuscules (par exemple, EXAMPLE.COM). Ce champ est obligatoire.
    5. URL autorisées : cliquez sur Ajouter, puis effectuez les opérations suivantes :
        1. URL autorisée : entrez une adresse URL pour laquelle vous souhaitez demander l'authentification unique (SSO) lorsqu'un utilisateur visite l'URL à partir d'un appareil iOS.
           Par exemple, lorsqu'un utilisateur tente d'accéder à un site dans Safari et que le site Web lance une demande d'authentification Kerberos, si ce site ne figure pas dans la liste des URL, l'appareil iOS ne tentera pas une authentification unique en fournissant le jeton Kerberos qui a été mis en cache sur l'appareil lors d'une précédente ouverture de session Kerberos. La correspondance doit être exacte sur la partie hôte de l'URL, par exemple : http://shopping.apple.com est valide, mais http://*.apple.com ne l'est pas. De même, si Kerberos n'est pas activé en fonction d'une correspondance à l'hôte, l'URL utilise un appel HTTP standard. Cela peut signifier presque tout, y compris un défi de mot de passe standard ou une erreur HTTP si l'URL est uniquement configurée pour l'authentification unique (SSO) à l'aide de Kerberos.

        2. Cliquez sur Ajouter pour ajouter l'URL, ou cliquez sur Annuler pour annuler l'ajout de l'URL.
        3. Répétez les étapes i et ii pour chaque adresse URL que vous souhaitez ajouter.
    6. Identifiants application : cliquez sur Ajouter, puis effectuez les opérations suivantes :

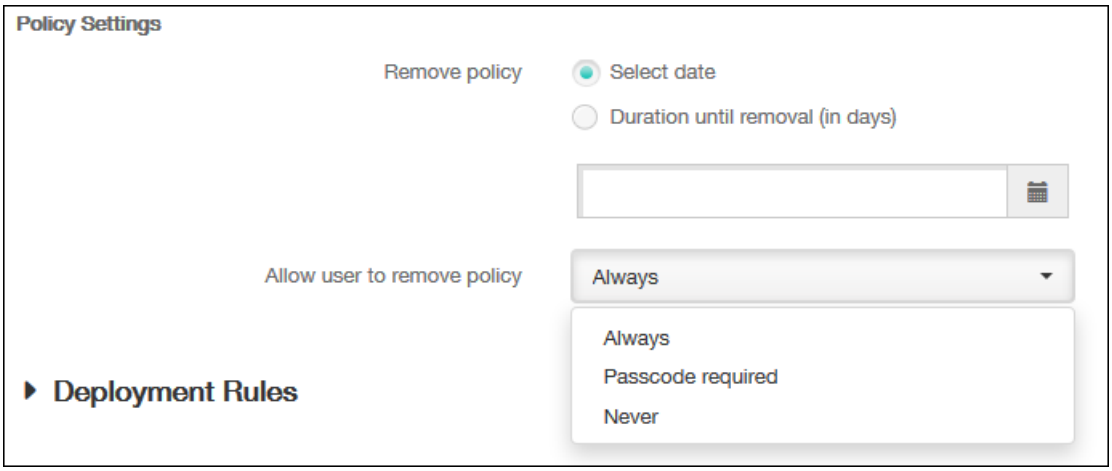
© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Identifiant app : entrez un identifiant d'application pour une application qui est autorisée à utiliser cette connexion. Remarque : si vous n'ajoutez aucun identifiant d'application, cette connexion correspond à **tous** les identifiants d'application.
2. Cliquez sur Ajouter pour ajouter l'identifiant d'application, ou cliquez sur Annuler pour annuler l'ajout de l'identifiant d'application.
3. Répétez les étapes i et ii pour chaque identifiant d'application que vous souhaitez ajouter.

Remarque : pour supprimer une URL ou un identifiant d'application, placez le curseur sur la ligne contenant la liste, puis 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 URL ou un identifiant d'application, placez le curseur sur la ligne contenant la liste, puis 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. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.



11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

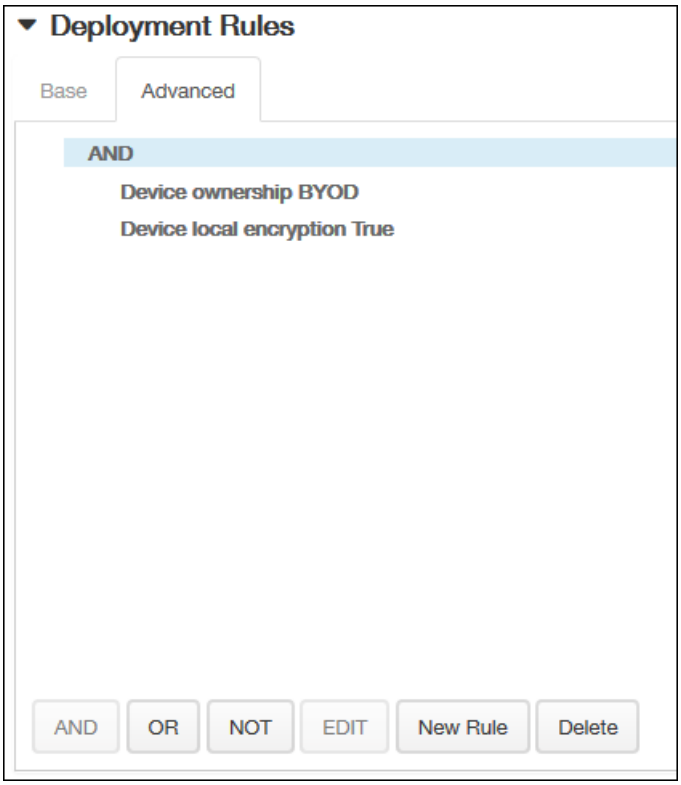


1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.

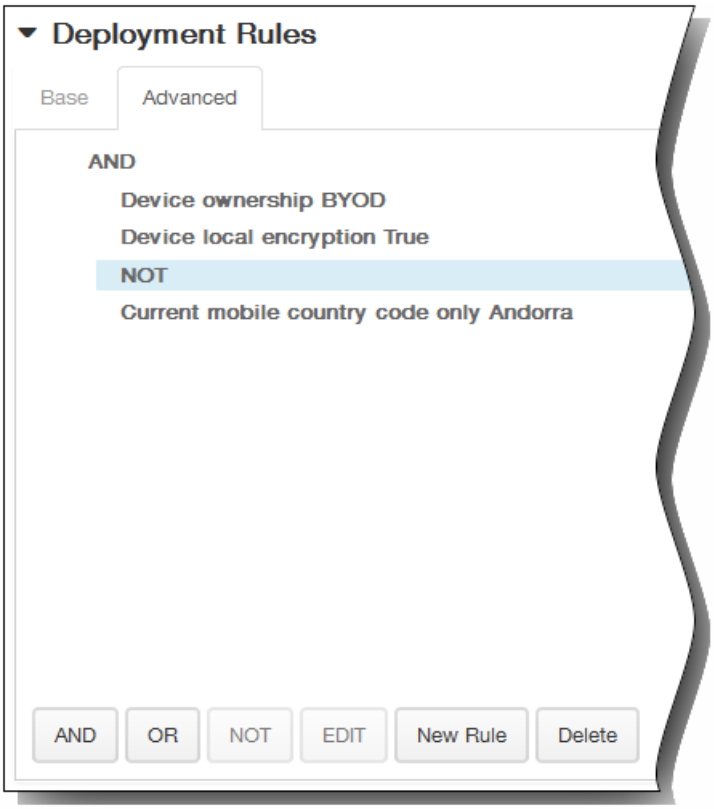
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



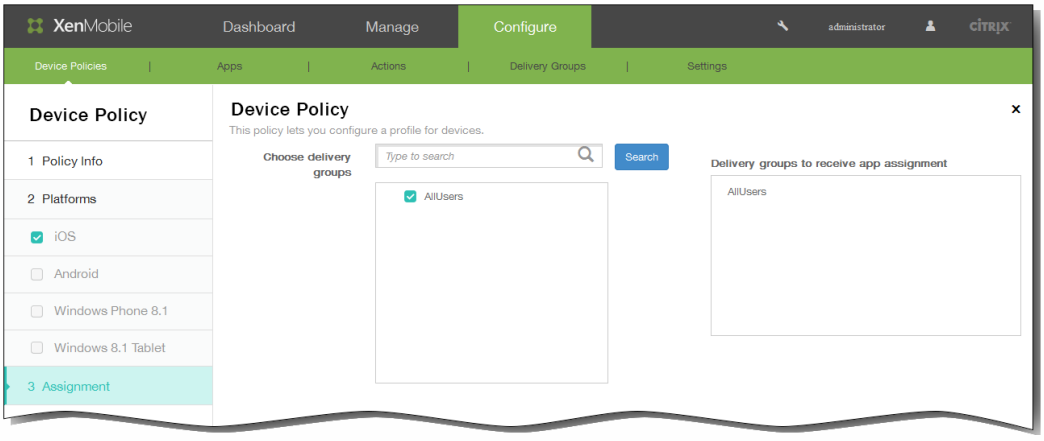
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de compte SSO s'affiche.
13. 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.



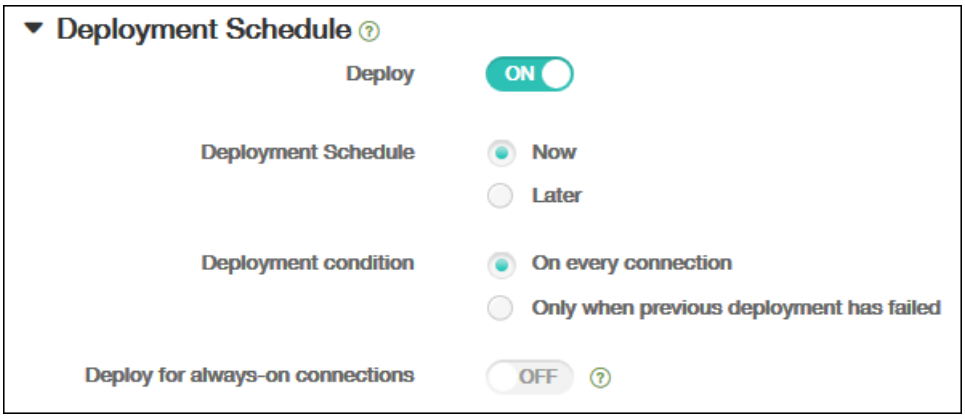
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

© 1999-2017 Citrix Systems, Inc. All rights reserved.

précédent a échoué. L'option par défaut est À chaque connexion.

5. 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.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

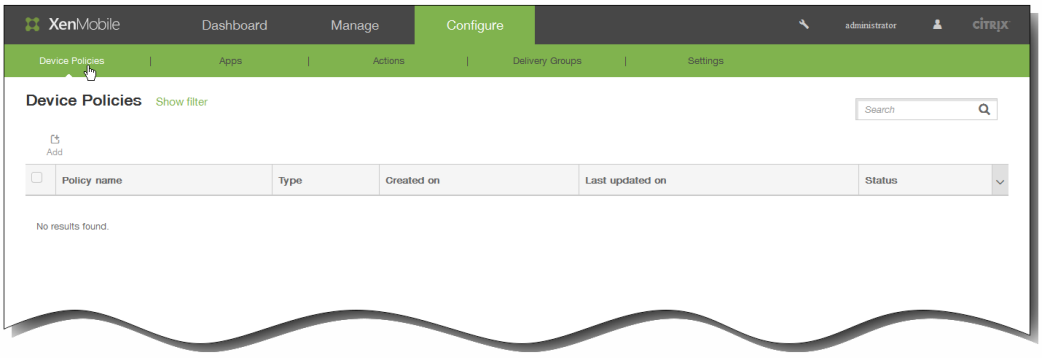
Pour ajouter une stratégie d'abonnements calendriers pour iOS

Jul 25, 2016

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.

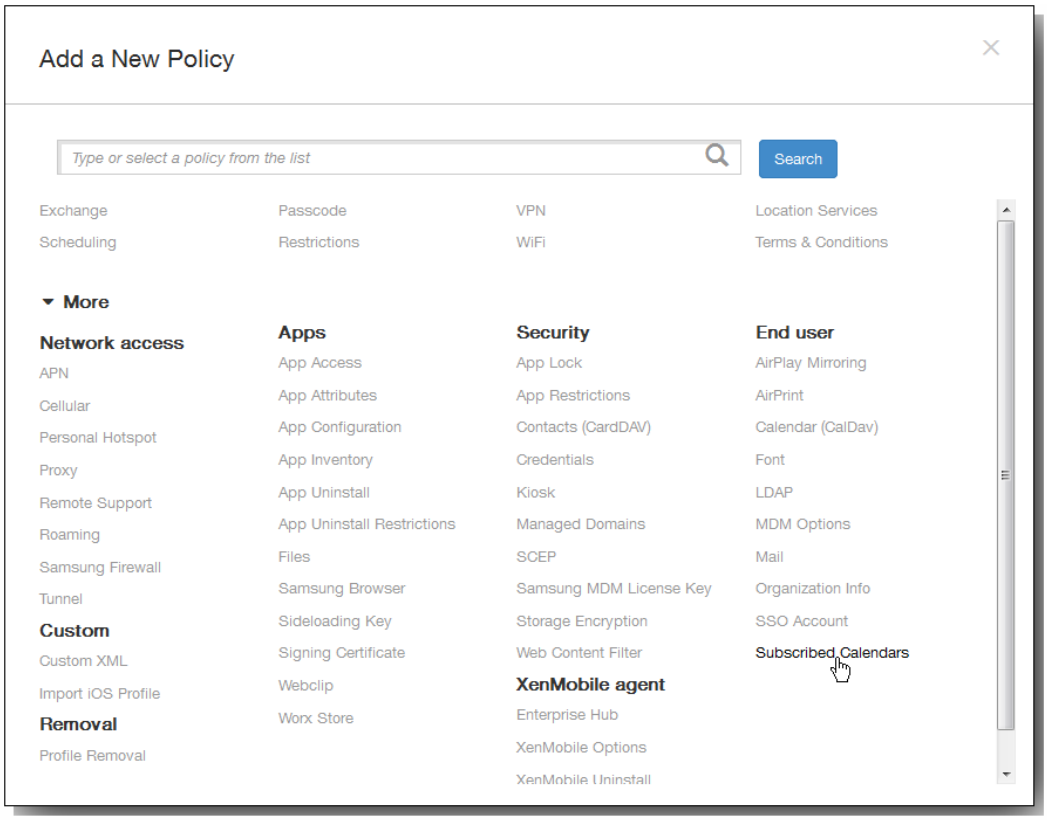
Remarque : vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

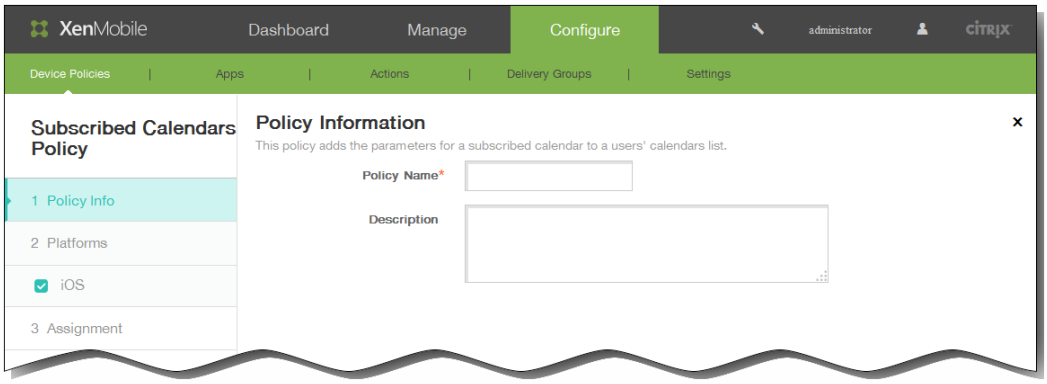


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

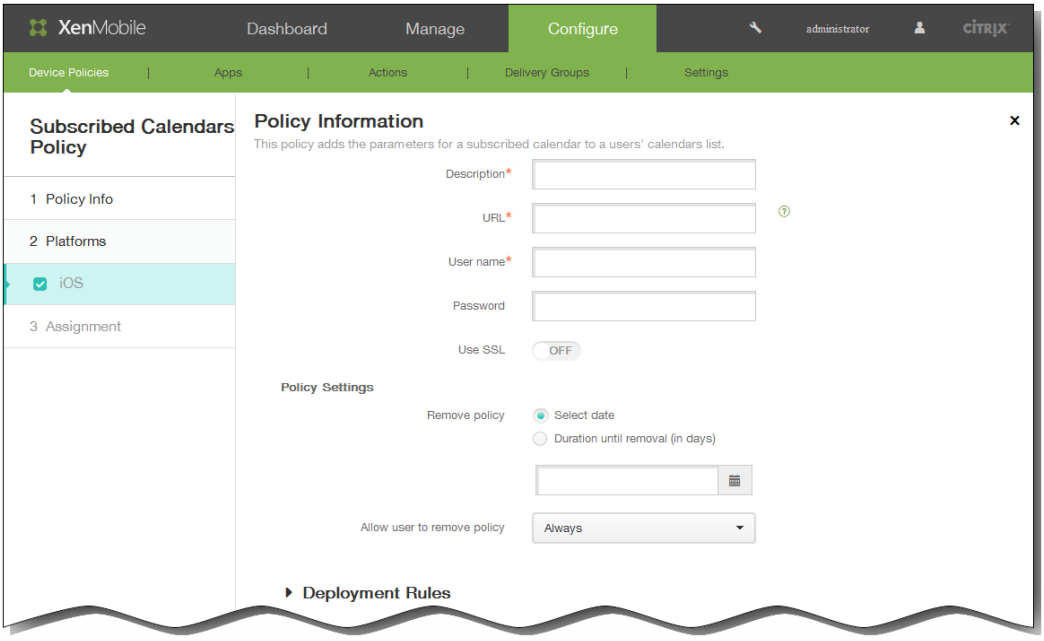


3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Abonnements calendriers. La page Stratégie d'abonnements calendriers s'affiche.

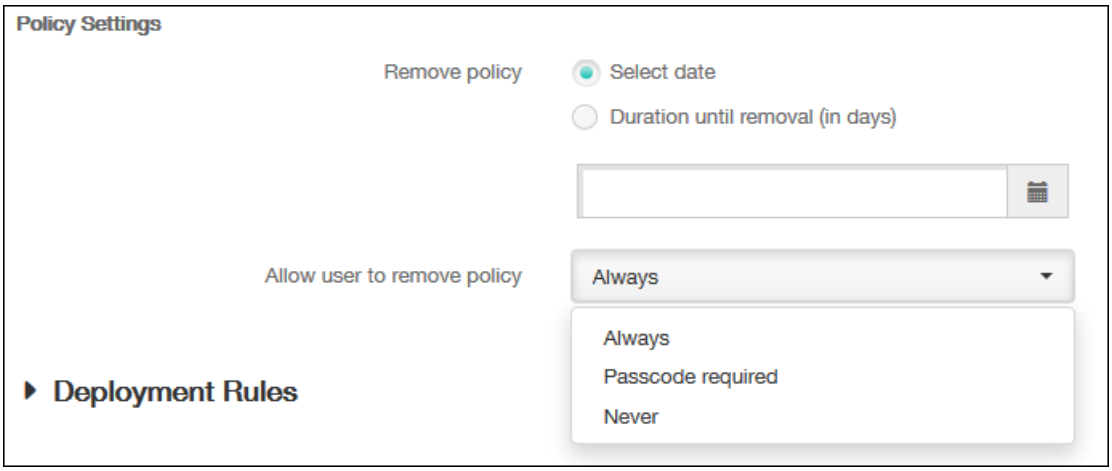


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Description : entrez une description pour le calendrier. Ce champ est obligatoire.
   2. URL : entrez l'URL du calendrier. Vous pouvez entrer une URL webcal:// ou un lien http:// vers un fichier iCalendar (.ics). Ce champ est obligatoire.
   3. Nom d'utilisateur : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
   4. Mot de passe : entrez un mot de passe utilisateur (facultatif).
   5. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au calendrier. La valeur par défaut est Off.
7. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
8. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
9. Dans la liste Autoriser l'utilisateur à supprimer la stratégie, cliquez sur Toujours, Mot de passe requis ou Jamais.
10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

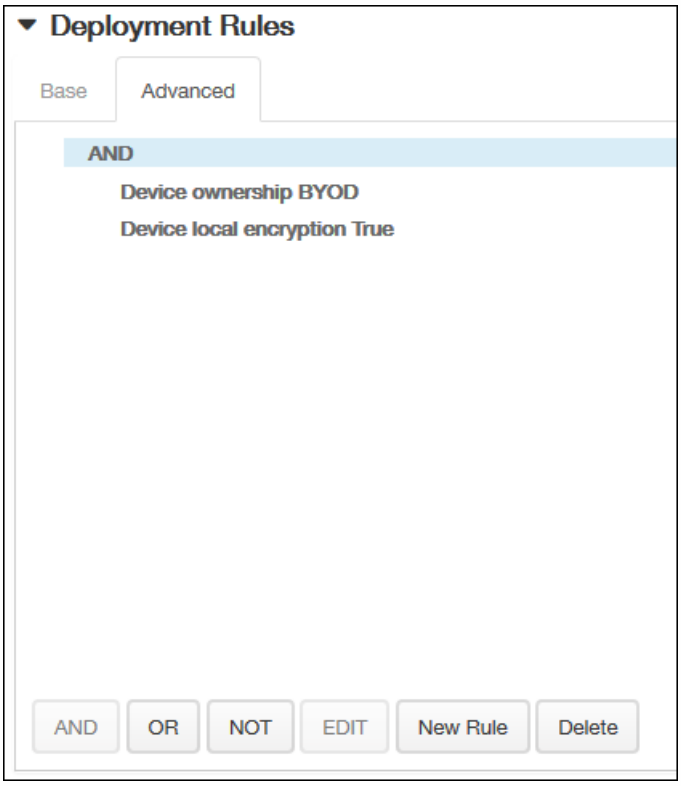


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



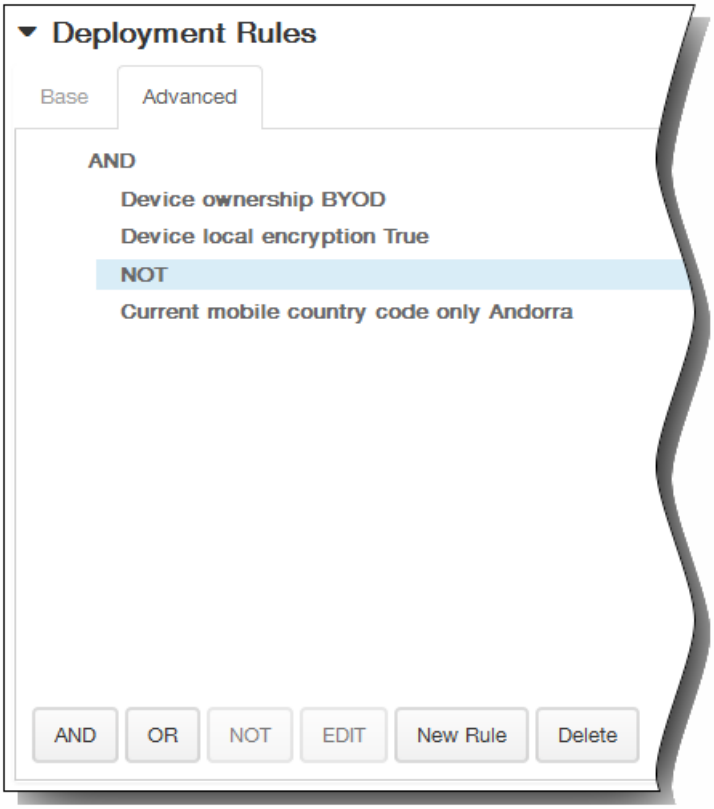
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir les conditions.
   3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
   4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



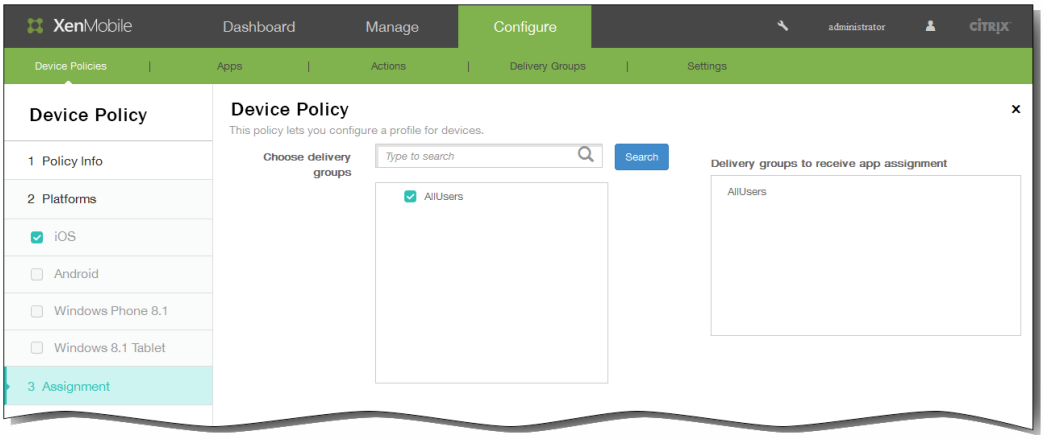
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
   Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie d'abonnements calendriers s'affiche.
13. 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.



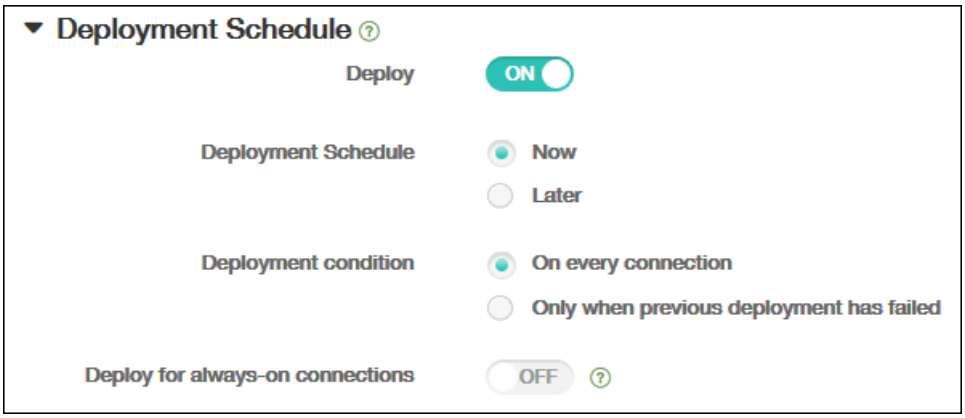
14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.

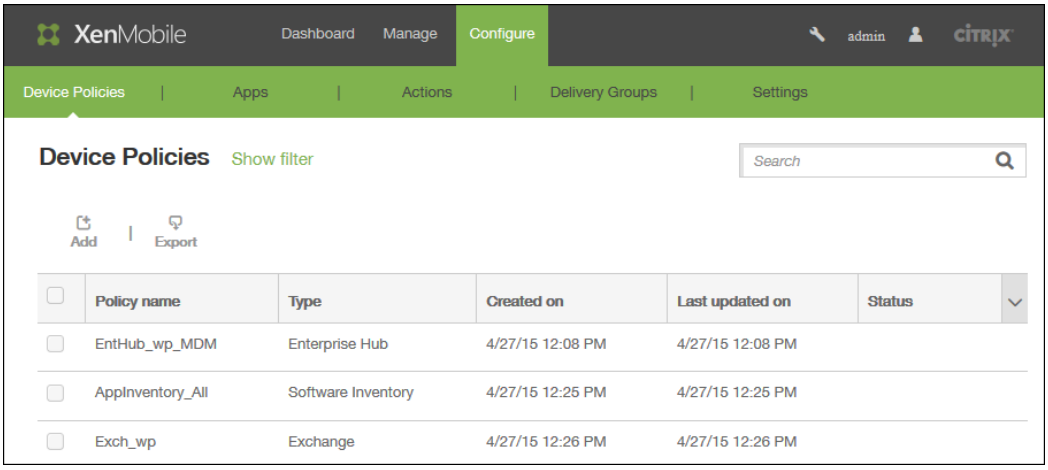
2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement précédent a échoué. L'option par défaut est À chaque connexion.
5. 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.

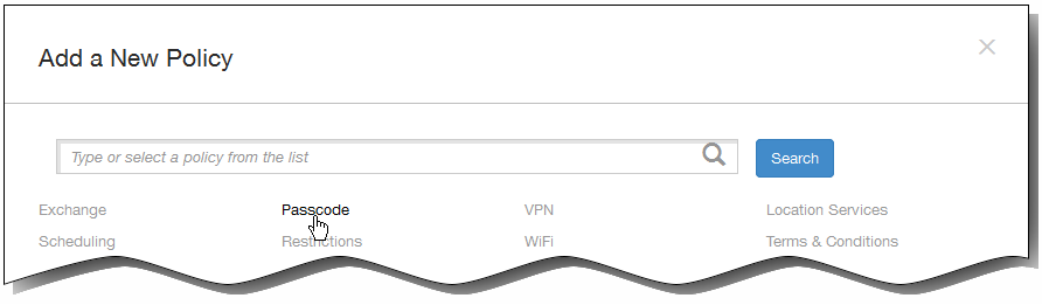
Remarque : le calendrier de déploiement que vous configurez est identique pour toutes les plates-formes. Les modifications que vous apportez s'appliquent à toutes les plates-formes, à l'exception de Déployer pour les connexions permanentes, qui ne s'applique pas à iOS.



15. Cliquez sur Enregistrer pour enregistrer la stratégie.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



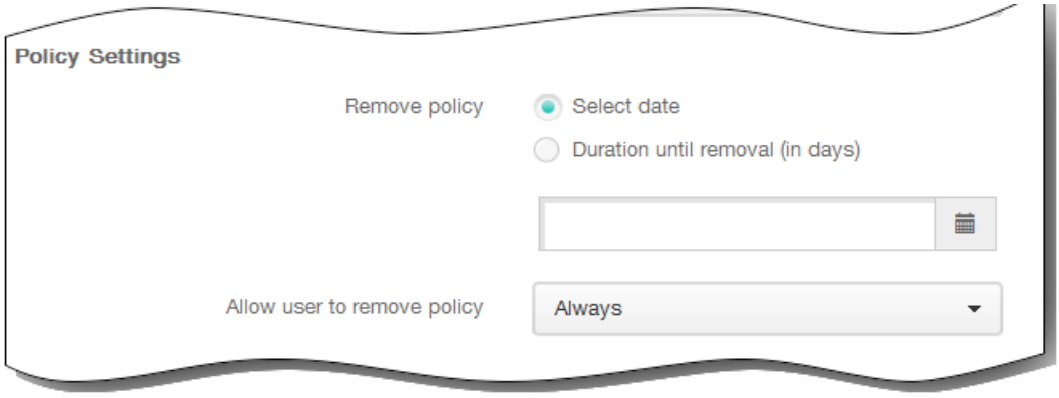


© 1999-2017 Citrix Systems, Inc. All rights reserved.

- _____

_____

© 1999-2017 Citrix Systems, Inc. All rights reserved.



 © 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

_____

_____

-
  _____

-
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

•

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

- _____

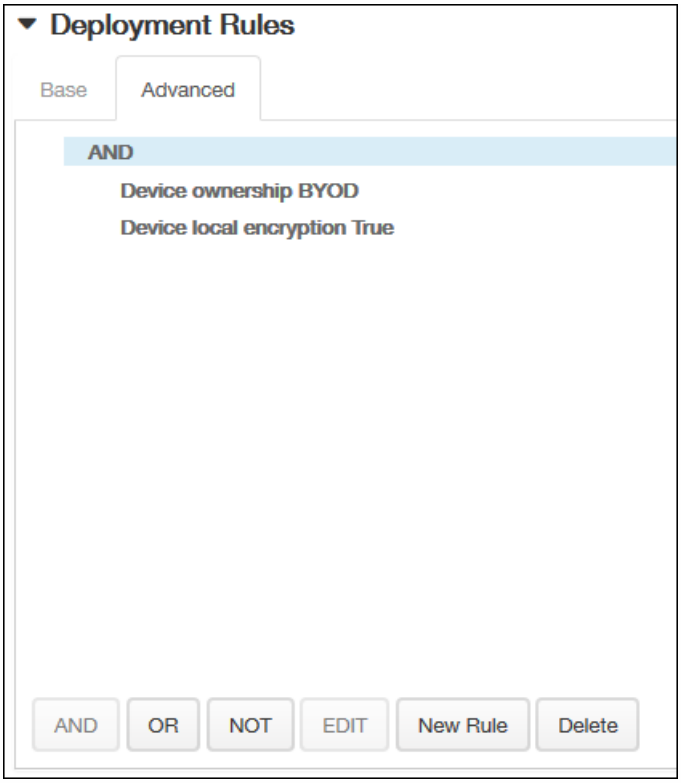
_____

-

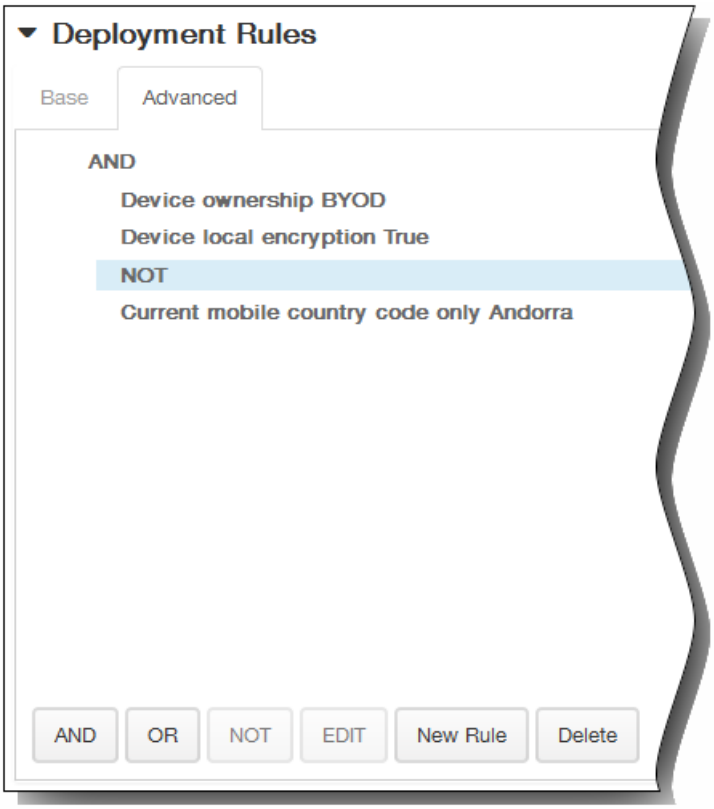
© 1999-2017 Citrix Systems, Inc. All rights reserved.

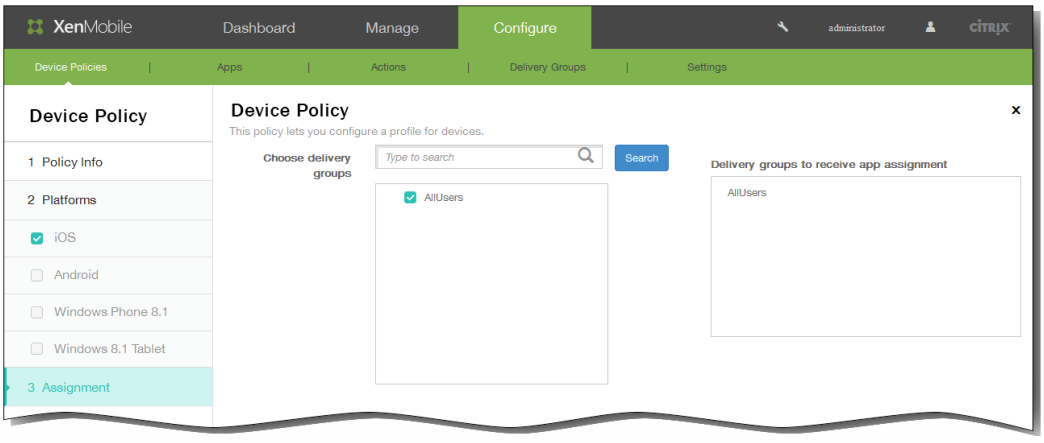


© 1999-2017 Citrix Systems, Inc. All rights reserved.

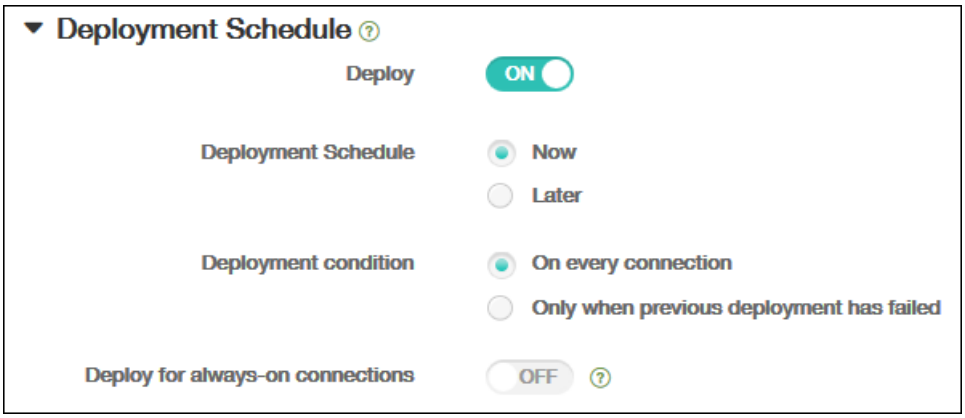


© 1999-2017 Citrix Systems, Inc. All rights reserved.

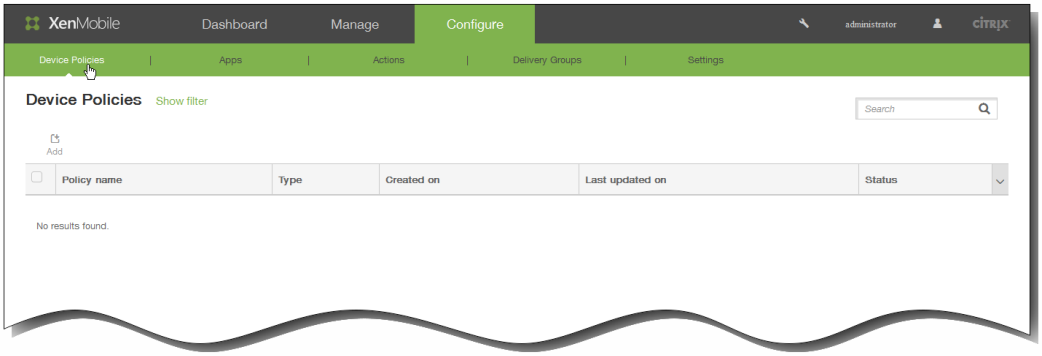




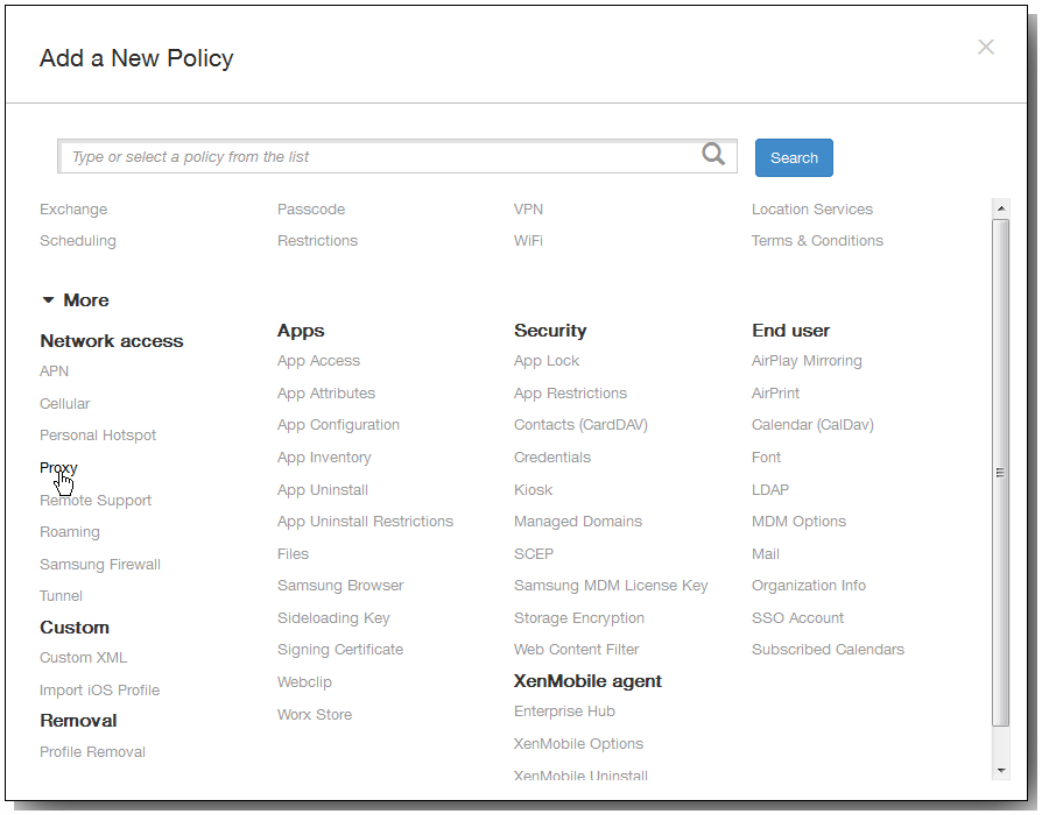
© 1999-2017 Citrix Systems, Inc. All rights reserved.

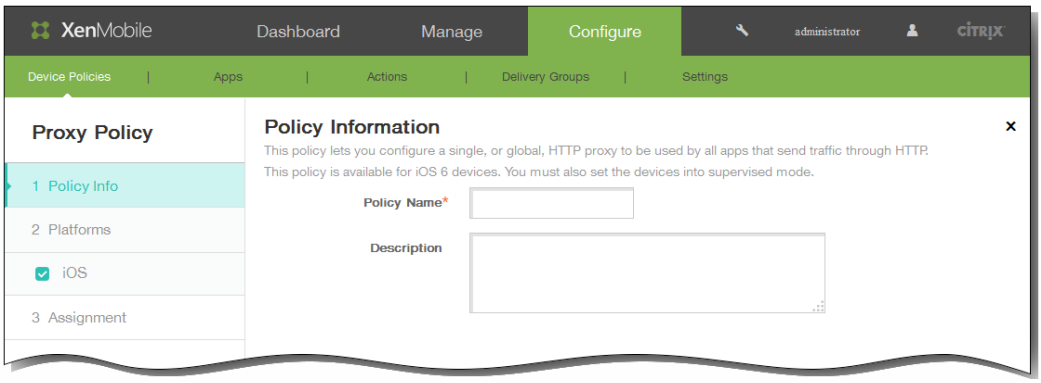


© 1999-2017 Citrix Systems, Inc. All rights reserved.

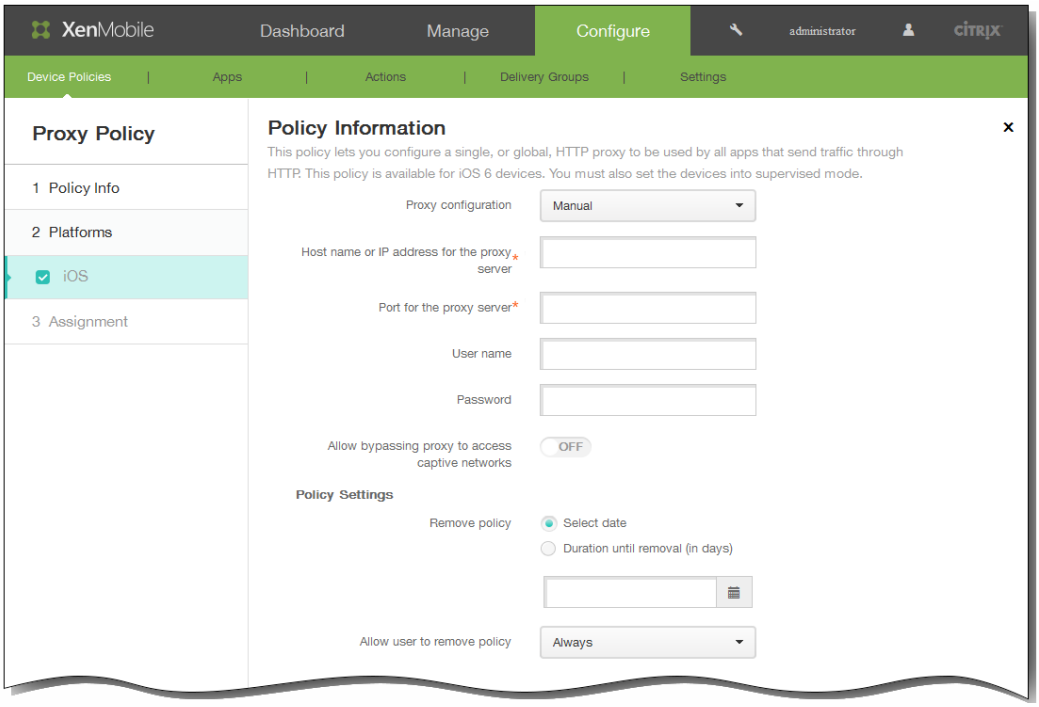


© 1999-2017 Citrix Systems, Inc. All rights reserved.

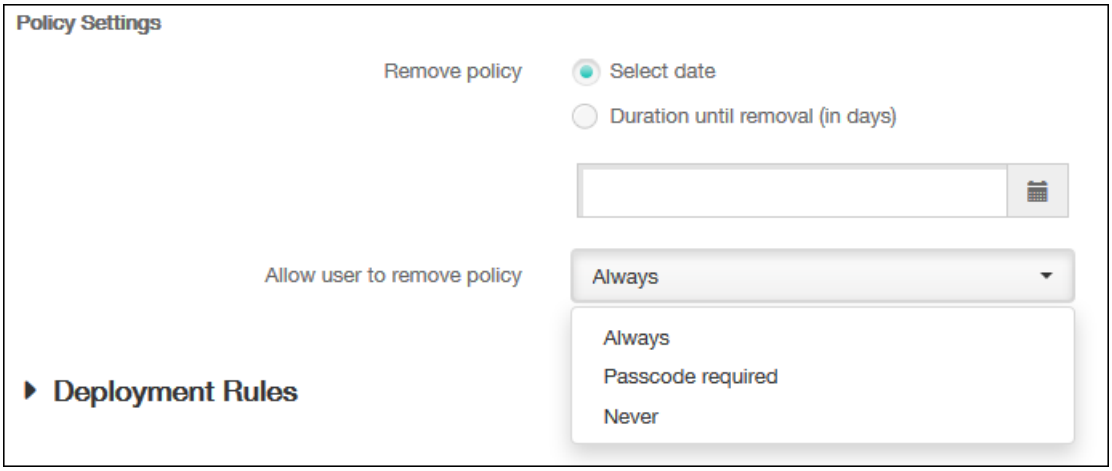


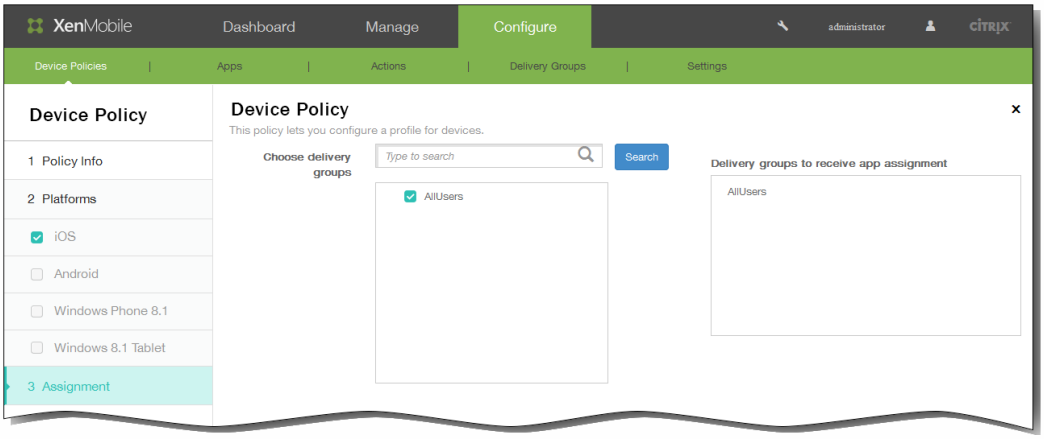


© 1999-2017 Citrix Systems, Inc. All rights reserved.

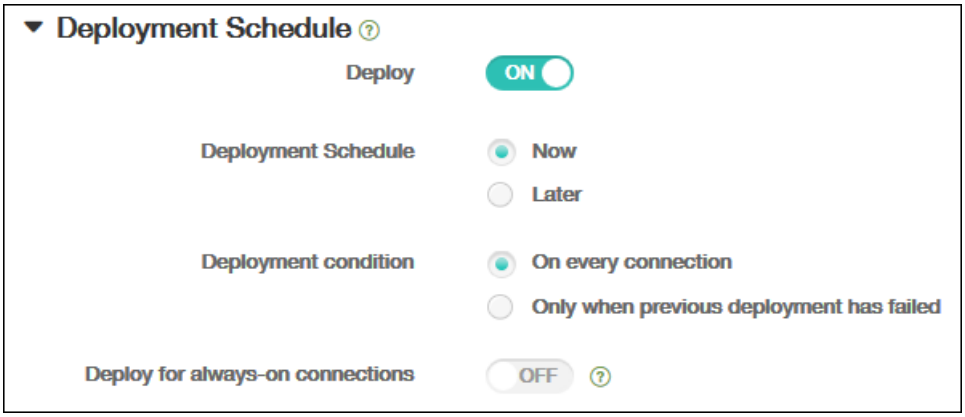


© 1999-2017 Citrix Systems, Inc. All rights reserved.



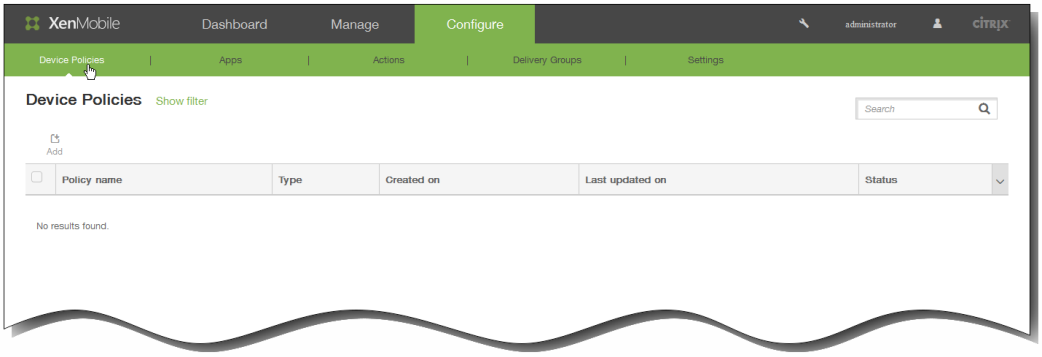


© 1999-2017 Citrix Systems, Inc. All rights reserved.

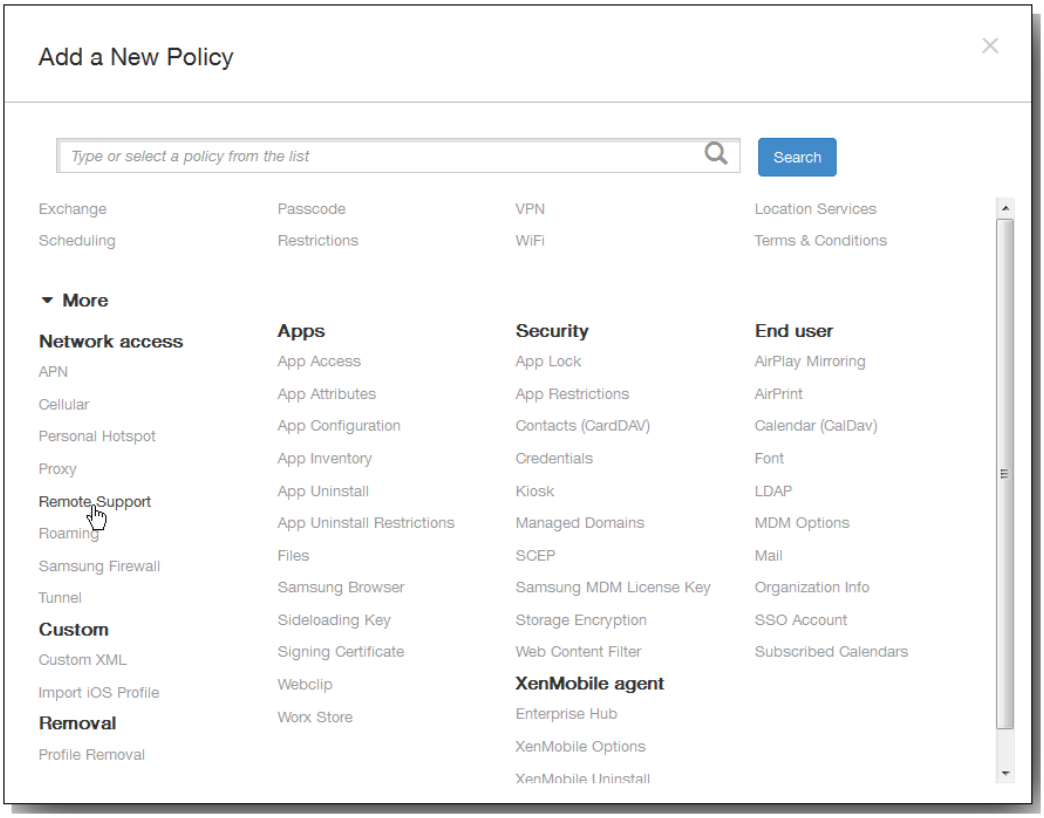


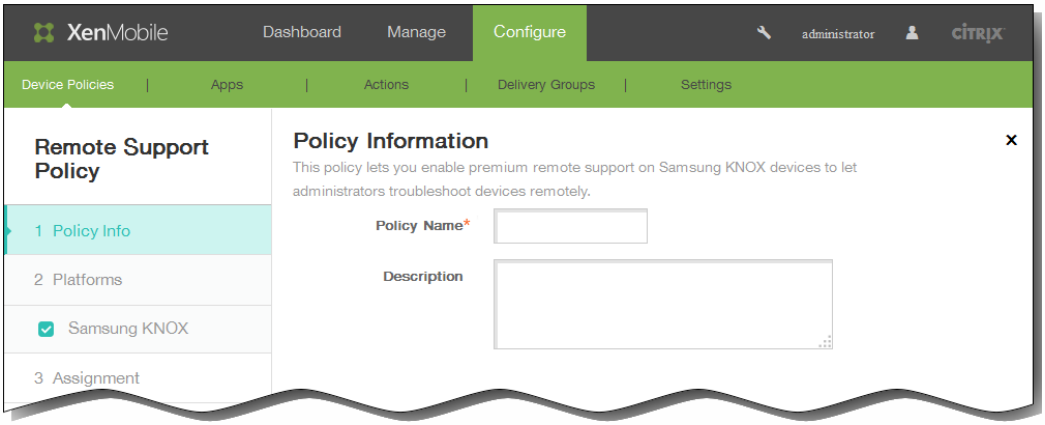
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-

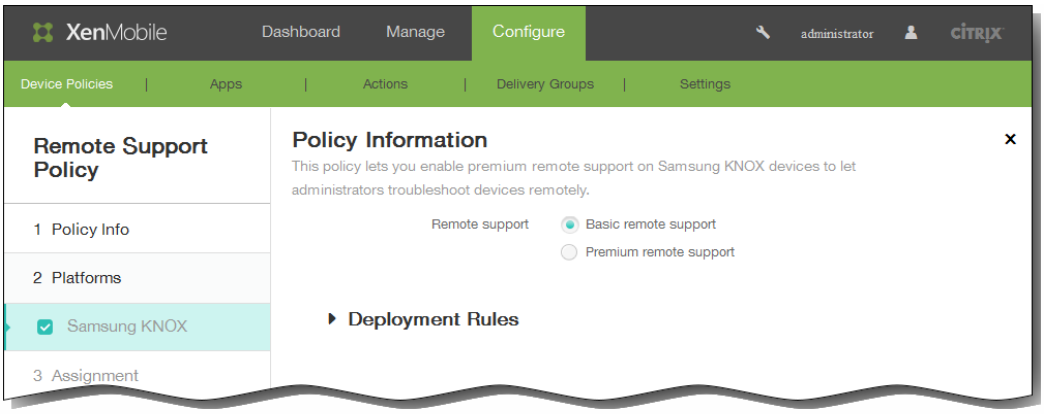


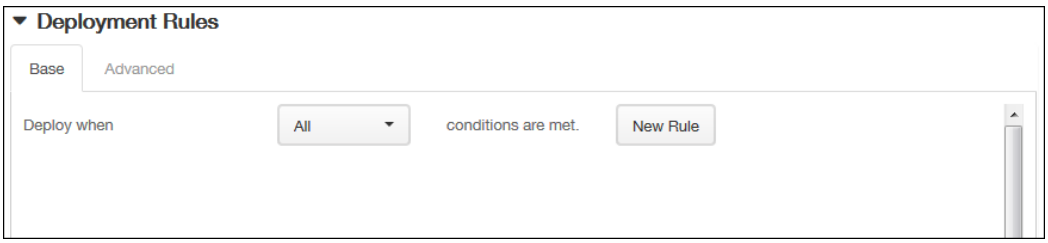
© 1999-2017 Citrix Systems, Inc. All rights reserved.



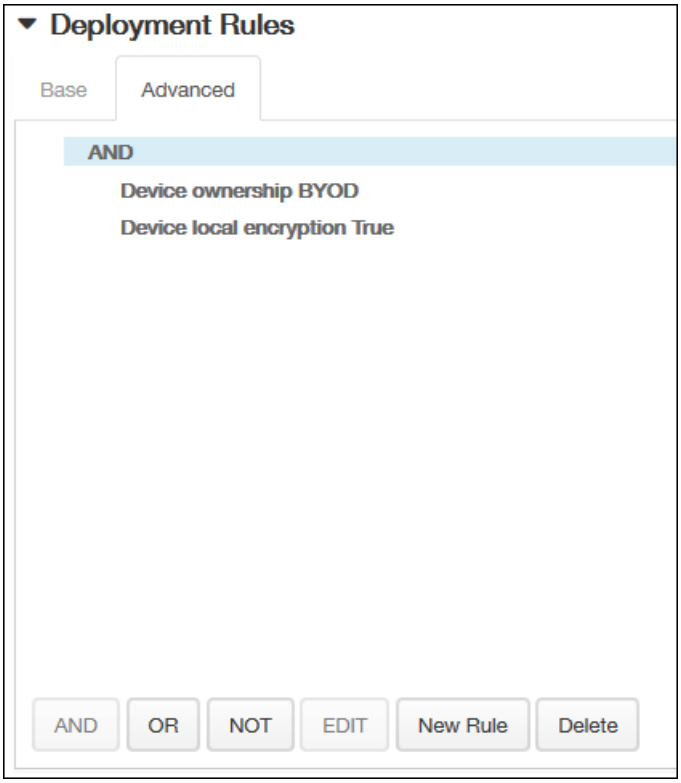


© 1999-2017 Citrix Systems, Inc. All rights reserved.

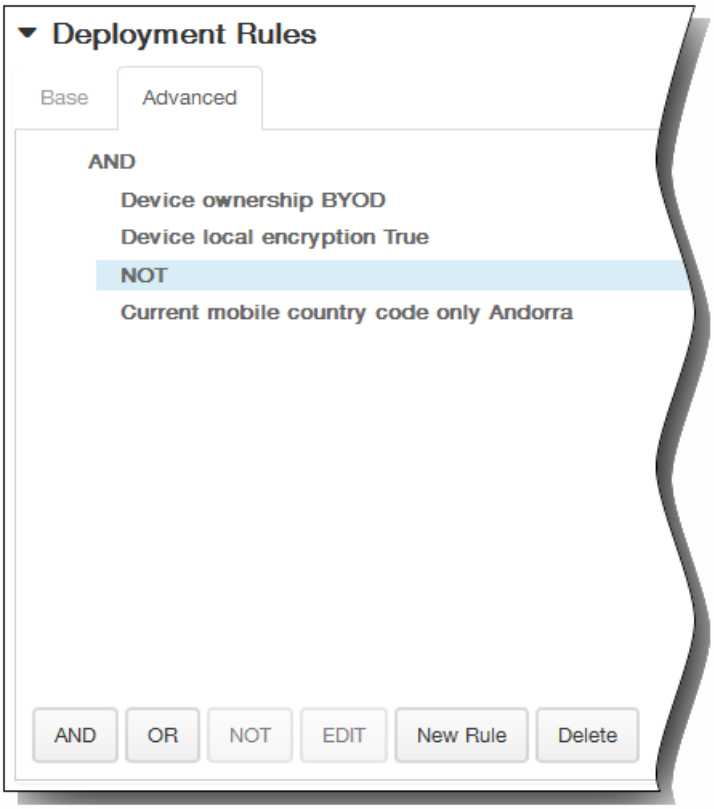


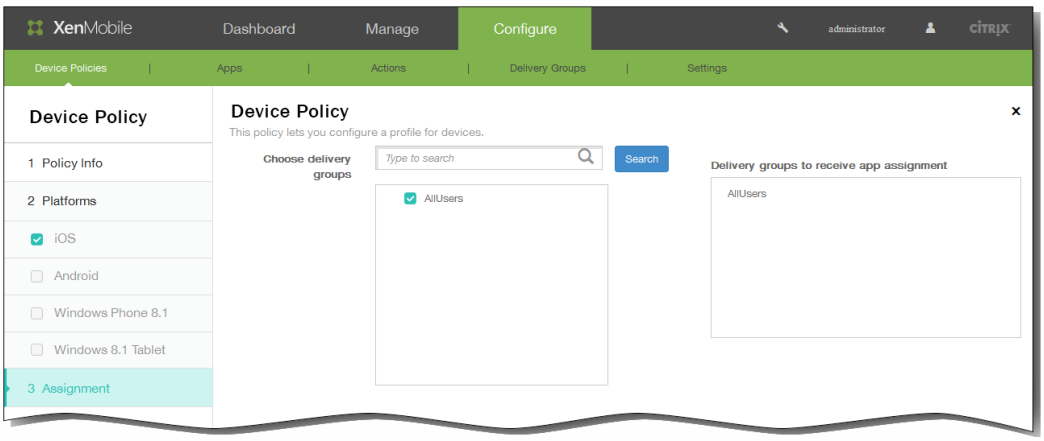


© 1999-2017 Citrix Systems, Inc. All rights reserved.

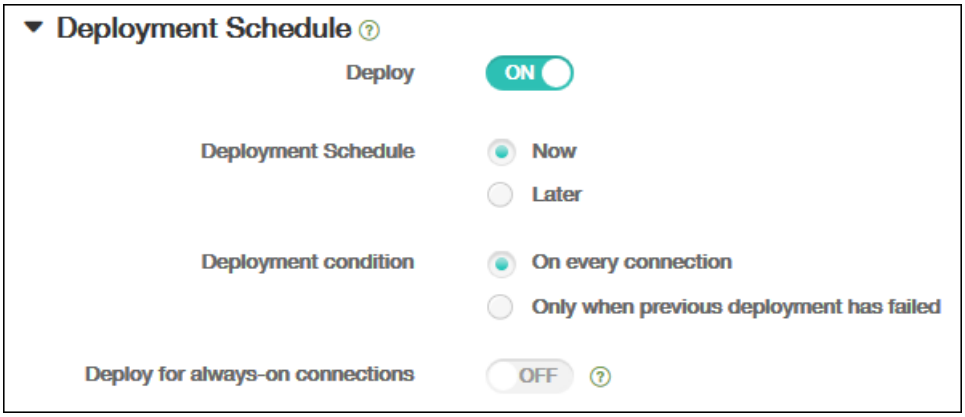


© 1999-2017 Citrix Systems, Inc. All rights reserved.



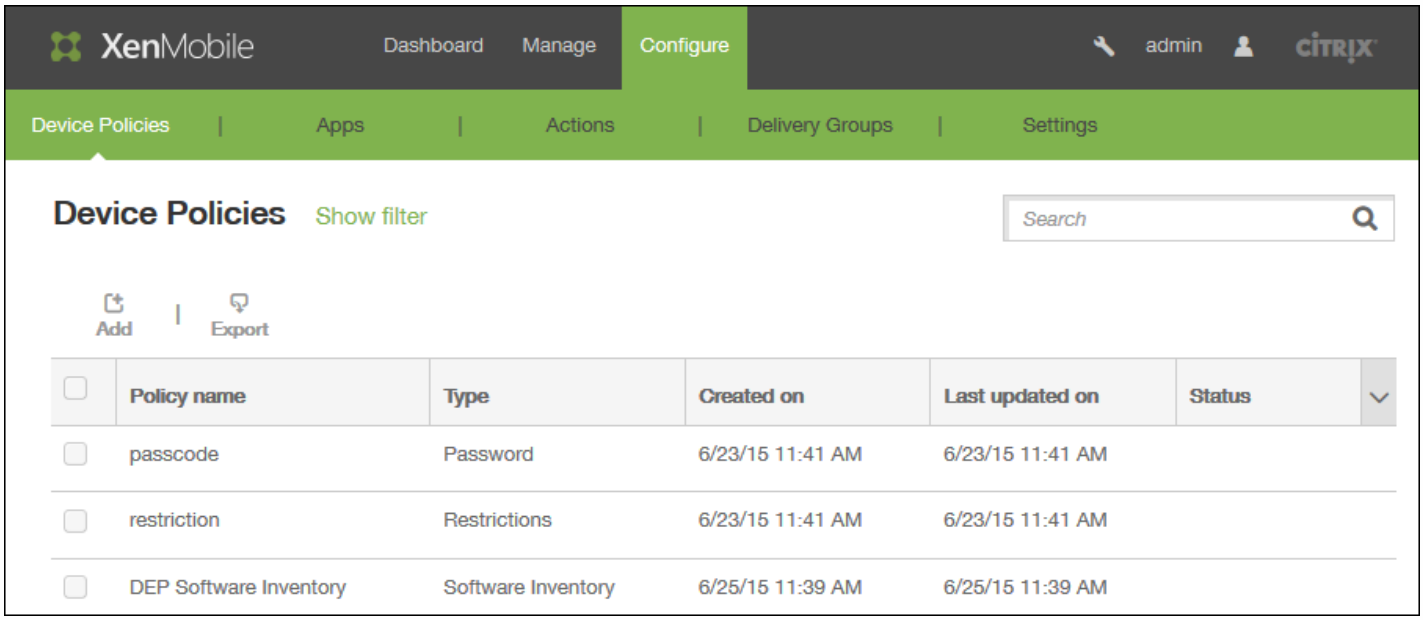


© 1999-2017 Citrix Systems, Inc. All rights reserved.

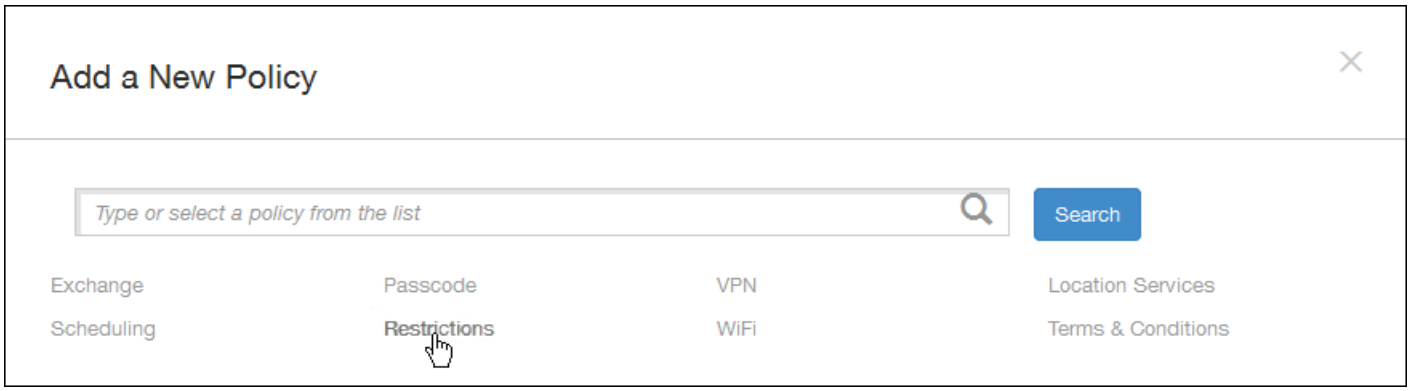


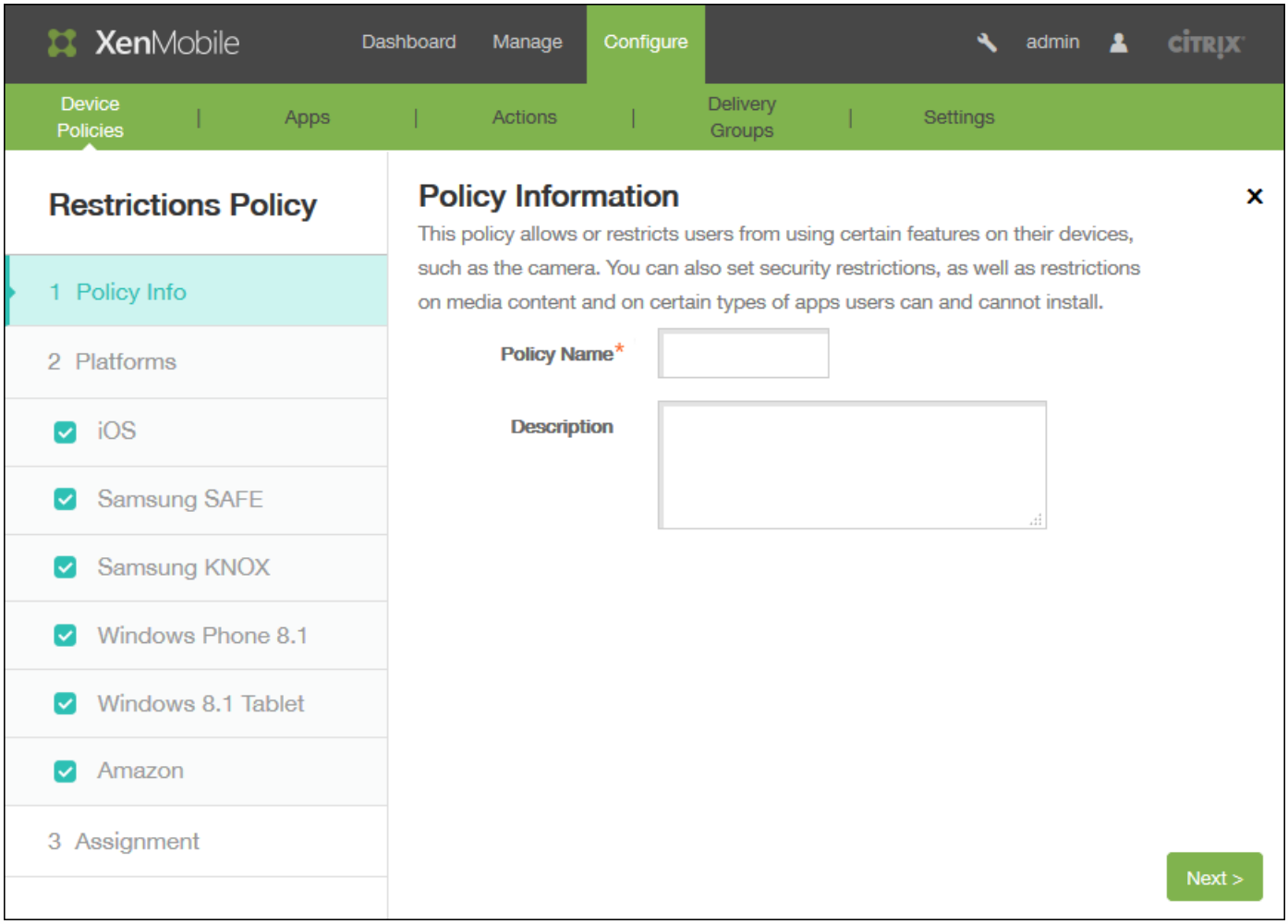
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-



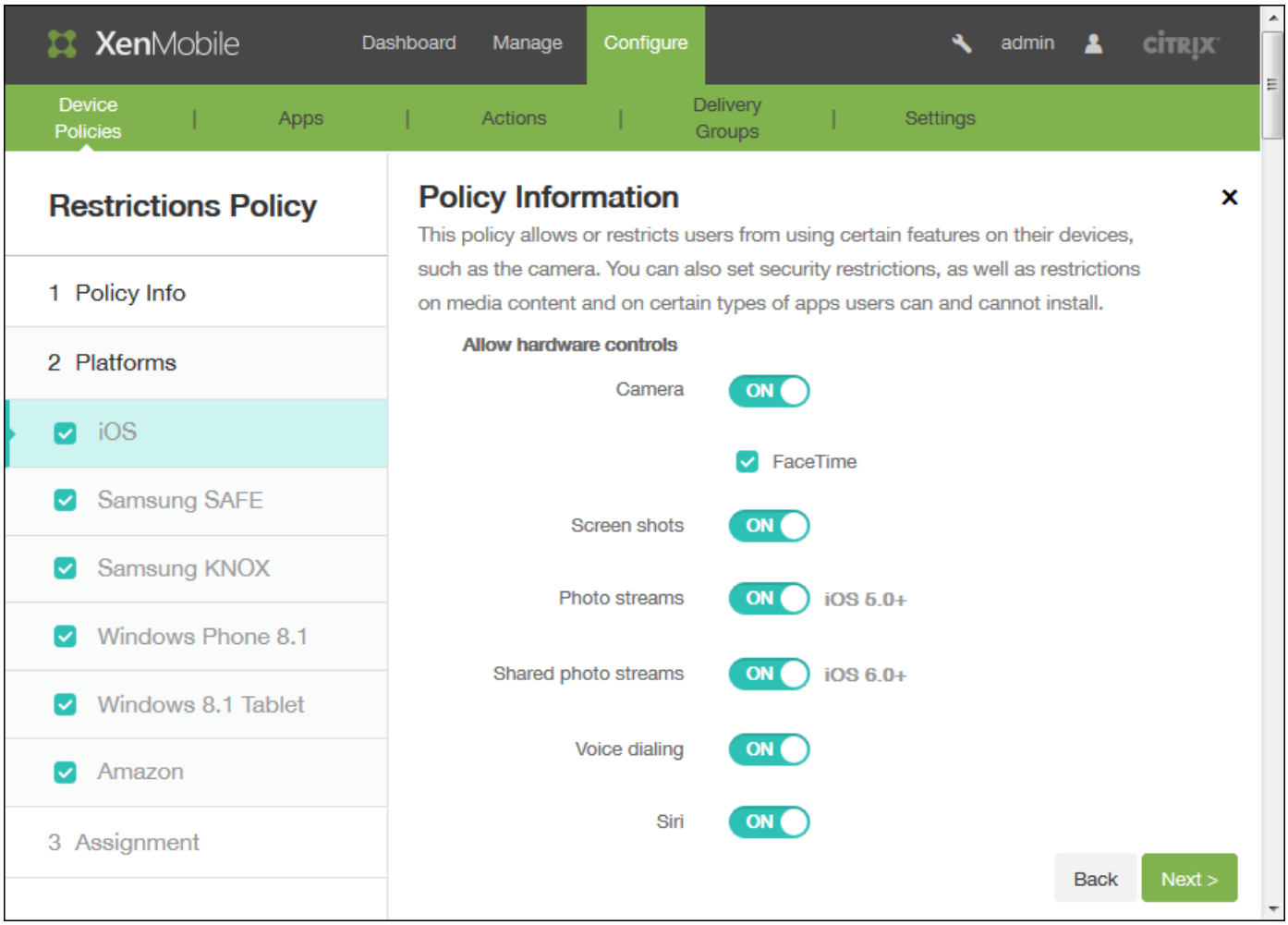
© 1999-2017 Citrix Systems, Inc. All rights reserved.





-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

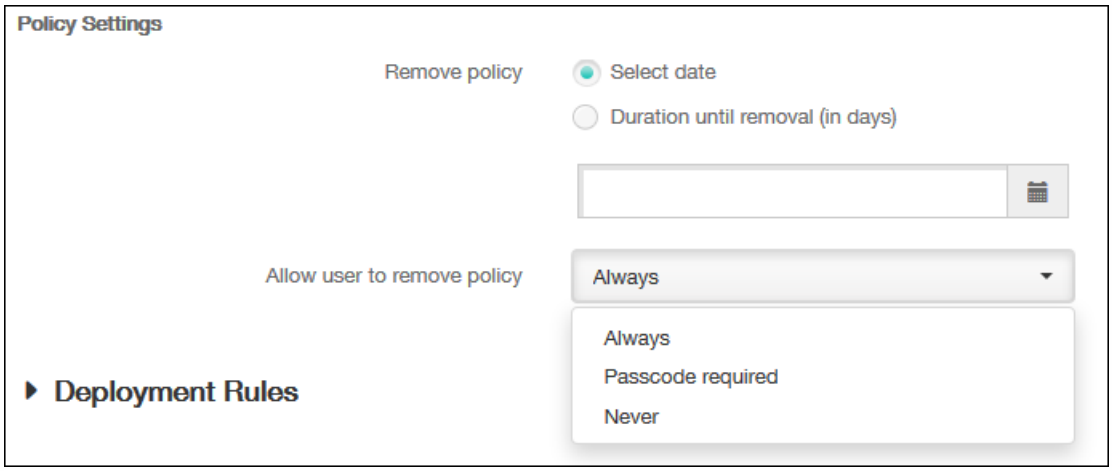
 © 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

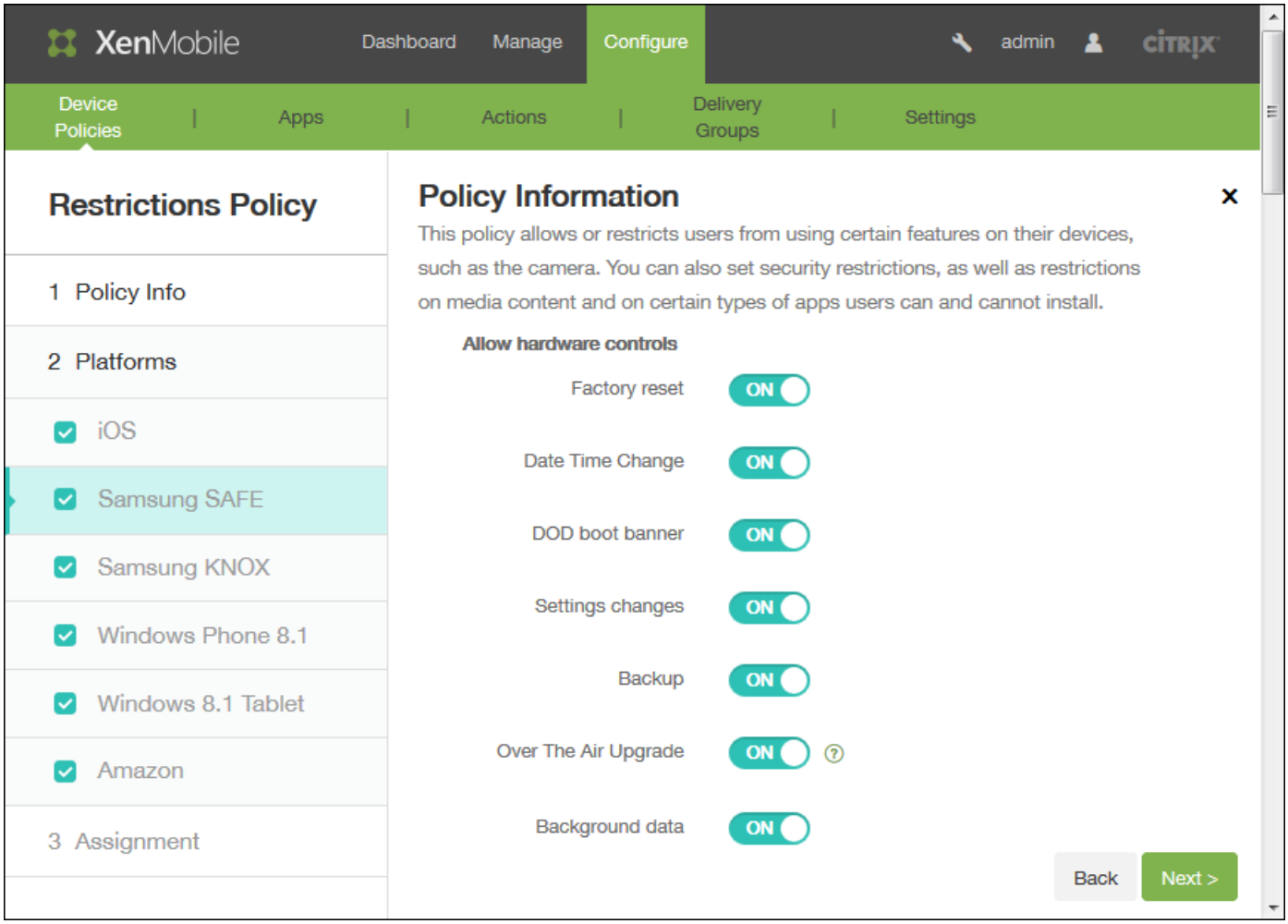
-
-
-
-
-
  -
  -
  -
-
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-



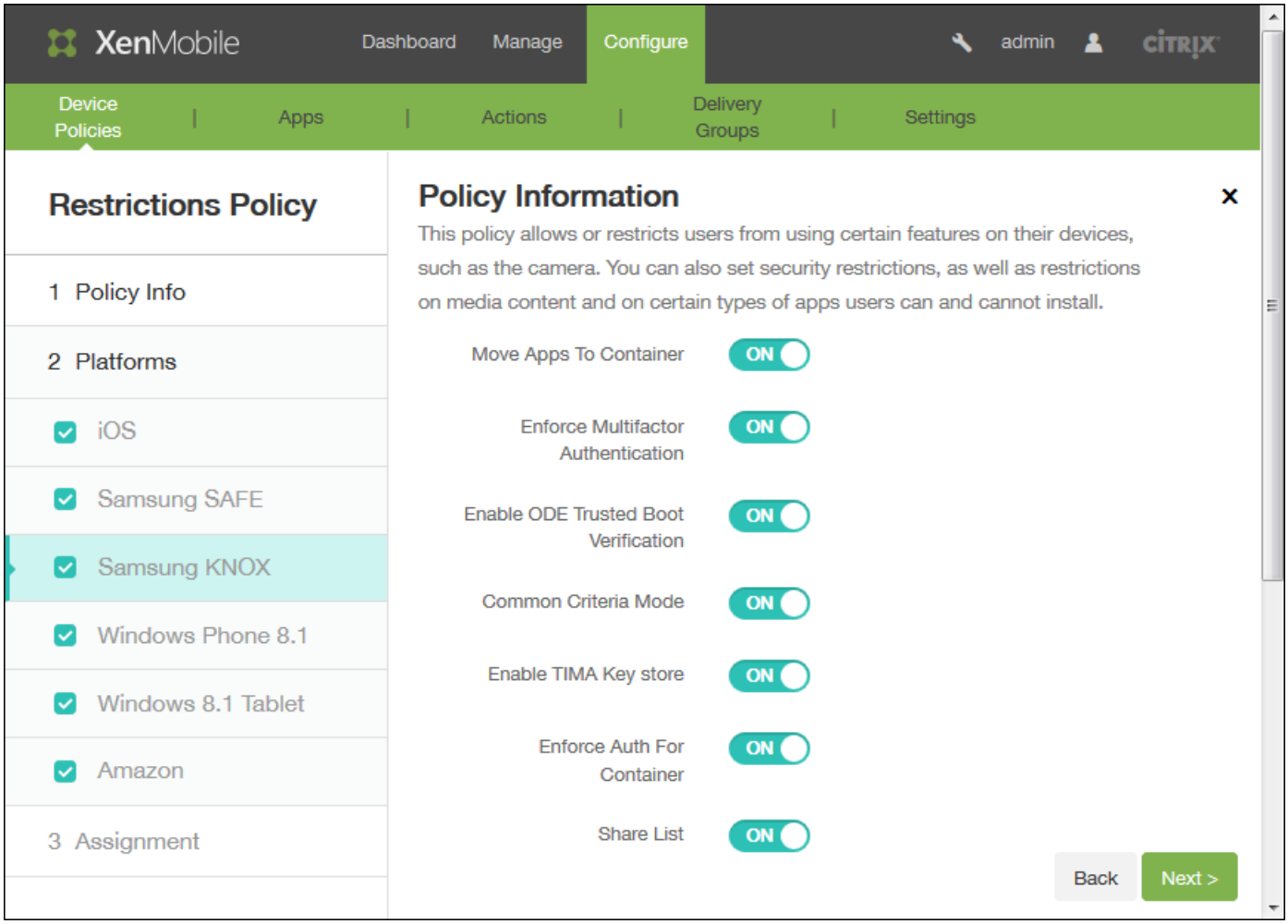
© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

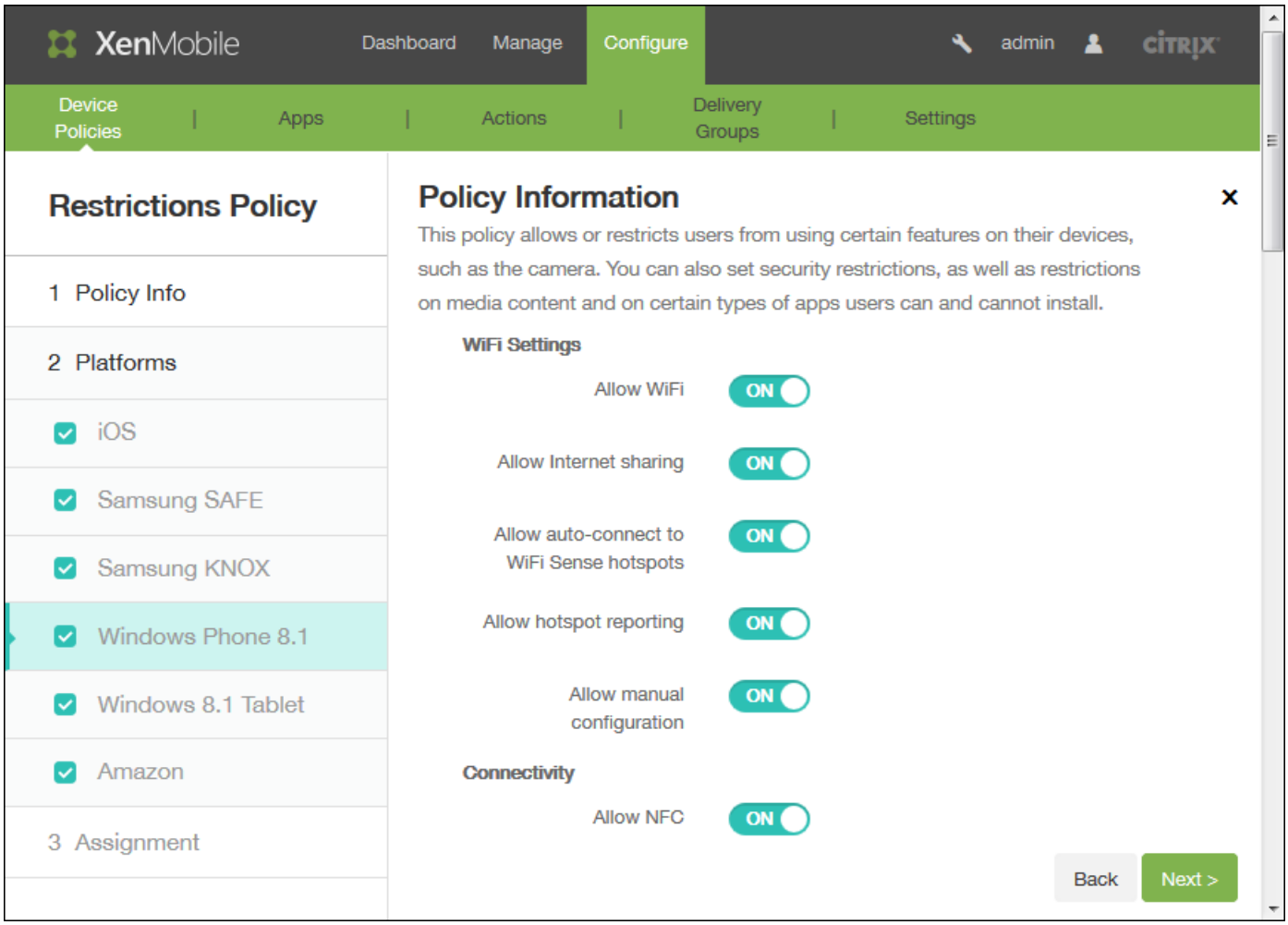
 © 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-



-
-
-
-
-
-

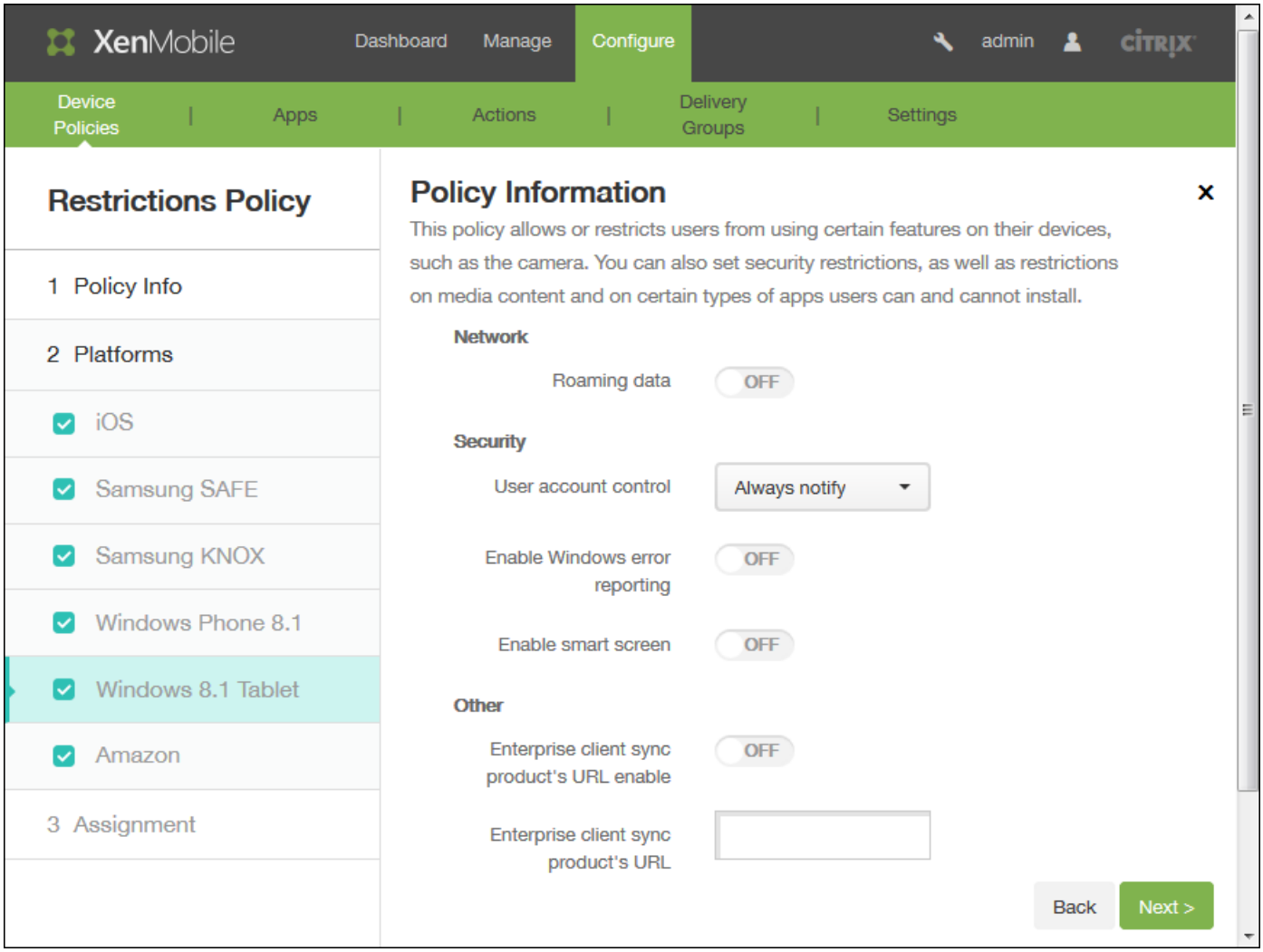
© 1999-2017 Citrix Systems, Inc. All rights reserved.



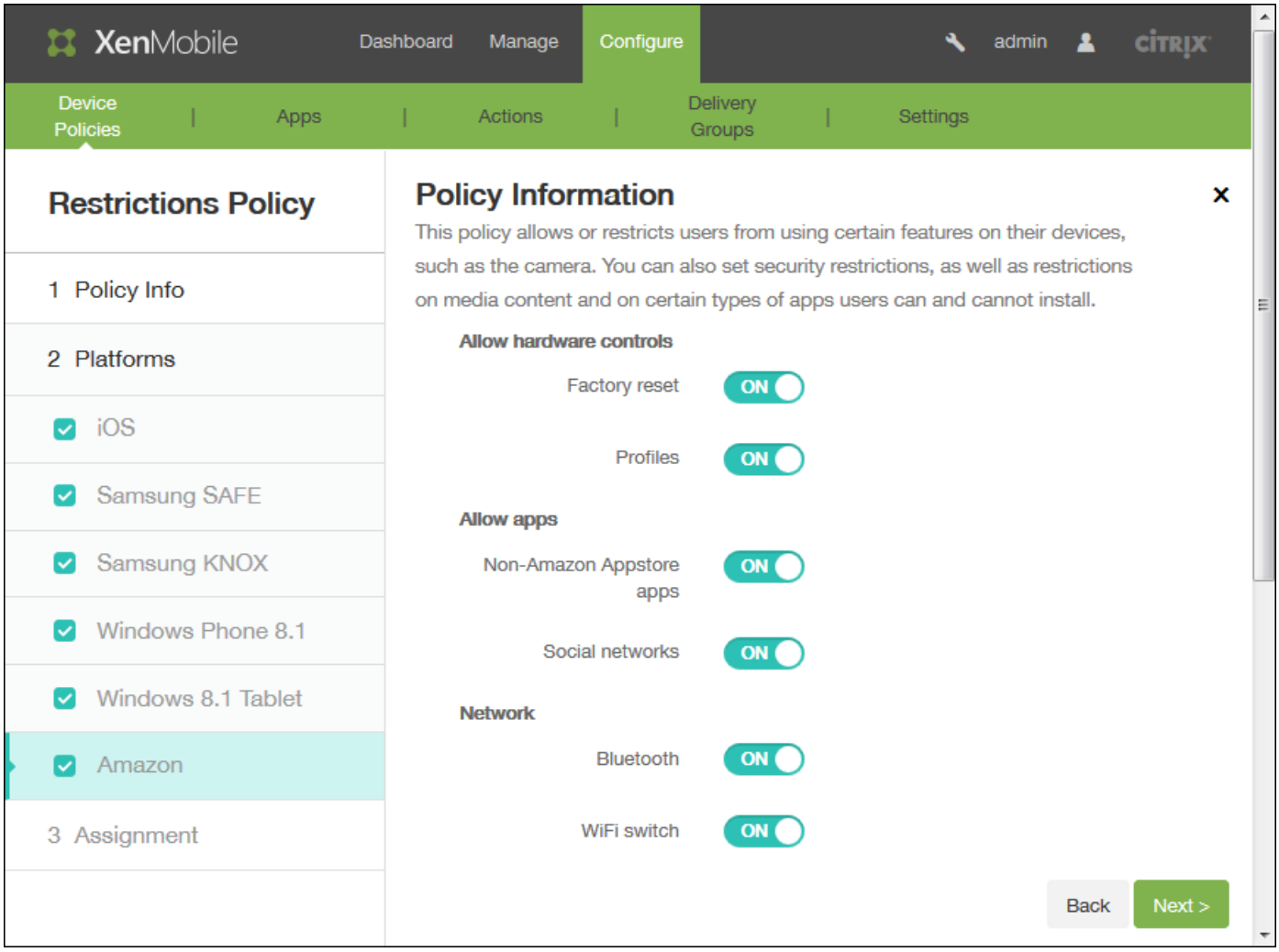
© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
  -
  -
    -
    -
    -
    -
    -
    -
  -
    -
    -
    -
    -
    -
    -
  -
    -
    -
    -
    -
    -



© 1999-2017 Citrix Systems, Inc. All rights reserved.



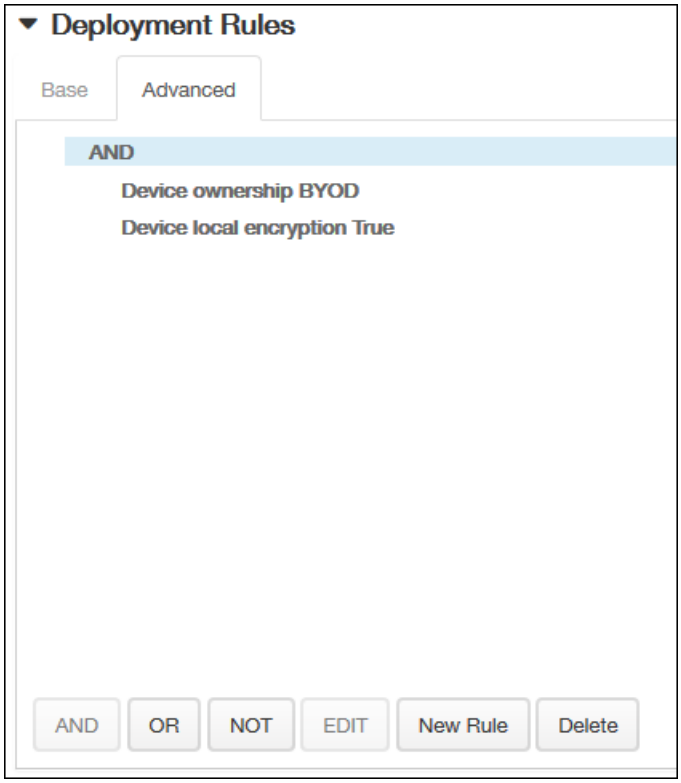
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
  -
  -
  -
  -
  -
  -
  -
-
  -



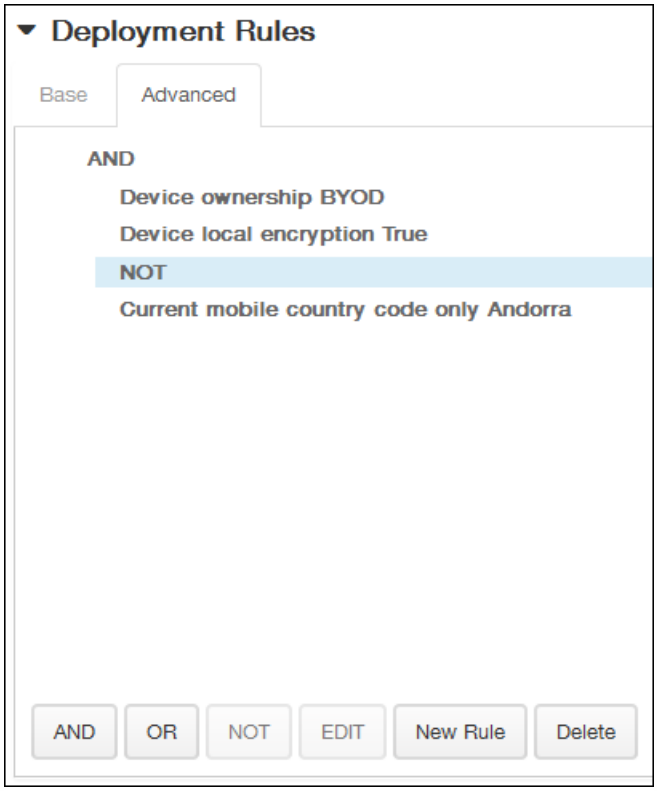
-
  -
  -
  -
  -
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

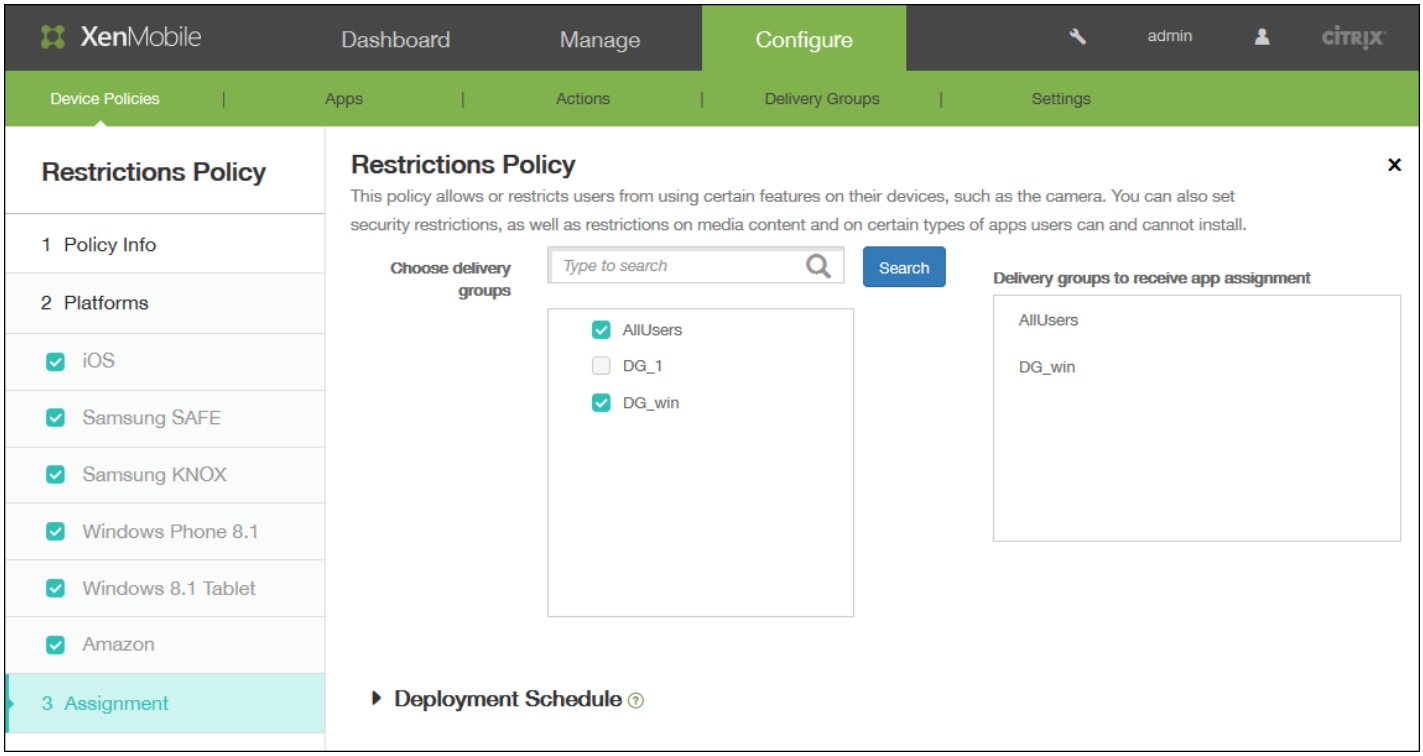


-
  -
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

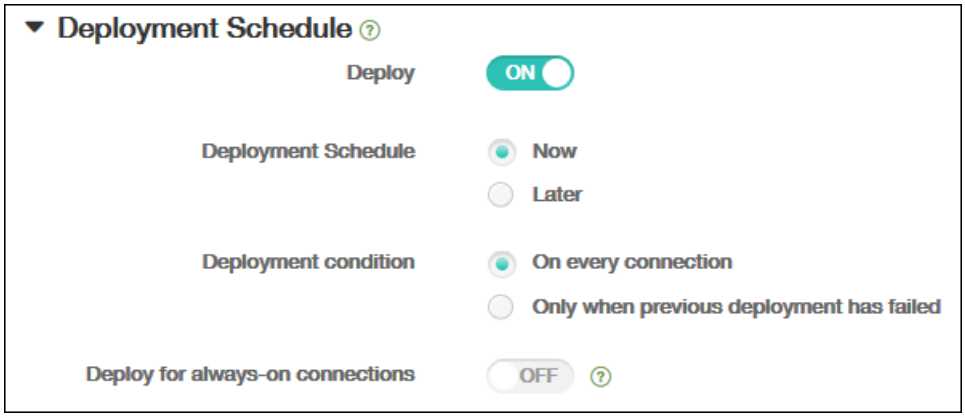


© 1999-2017 Citrix Systems, Inc. All rights reserved.

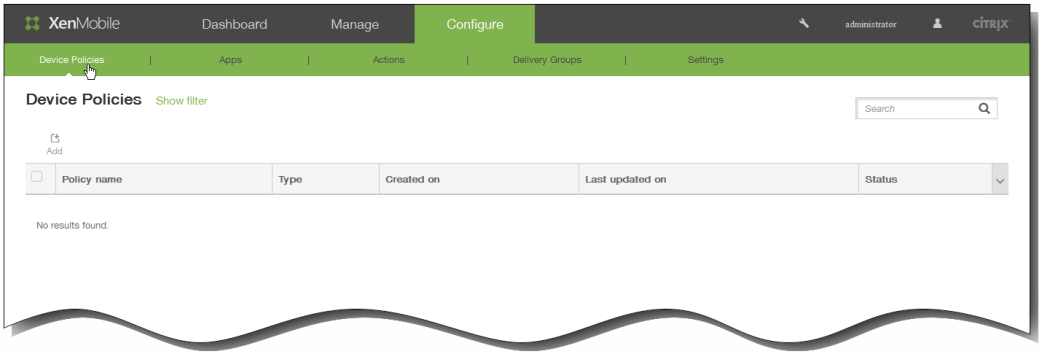


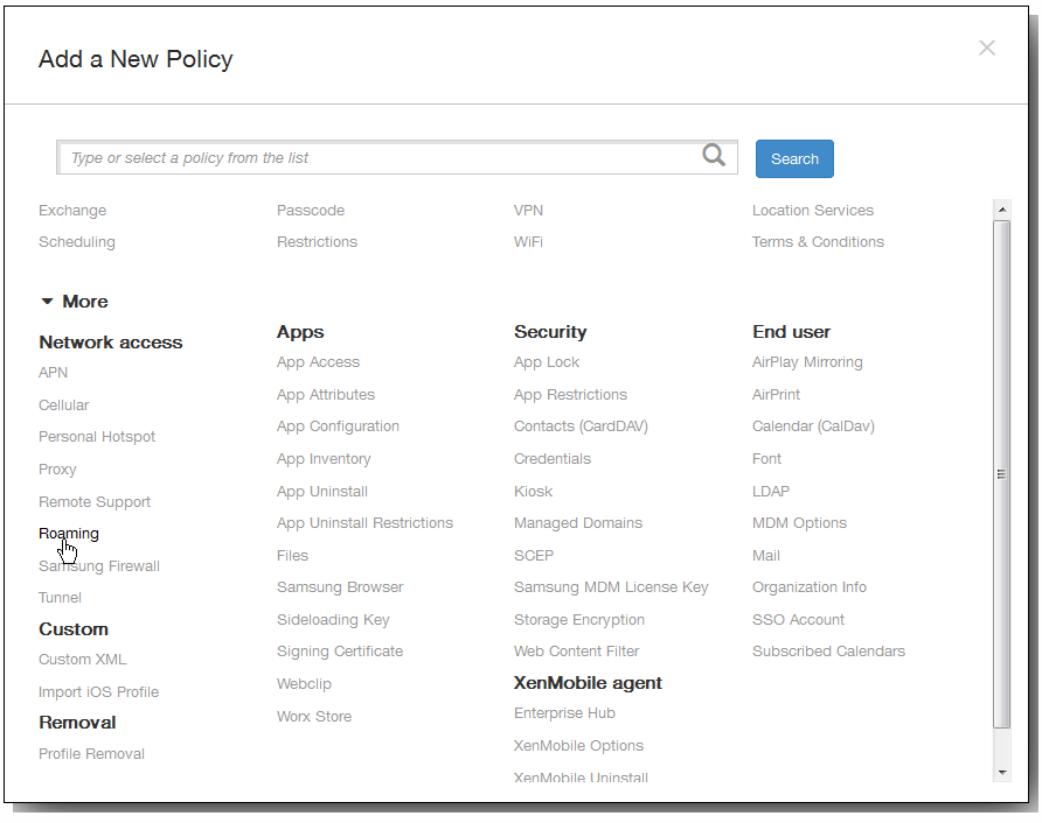
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

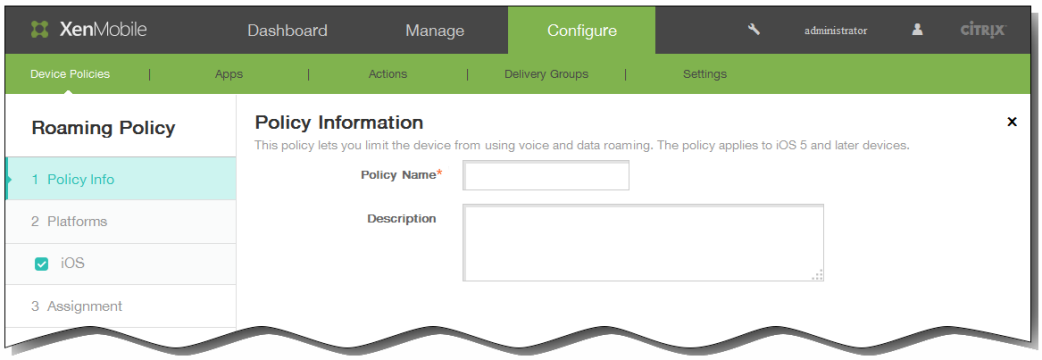


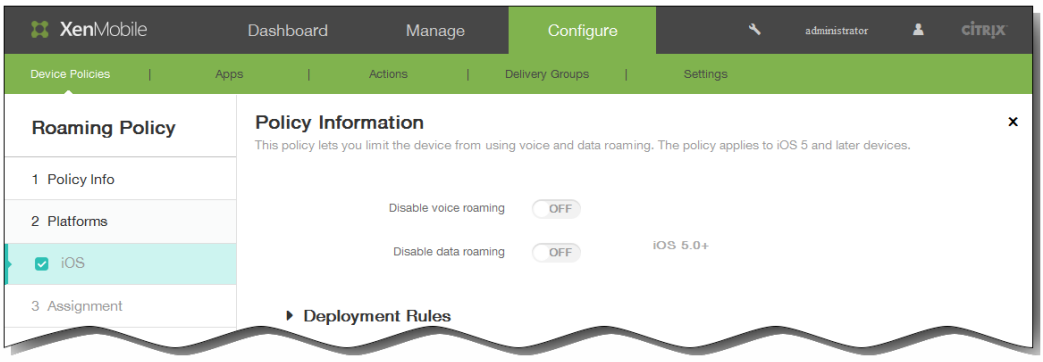
© 1999-2017 Citrix Systems, Inc. All rights reserved.





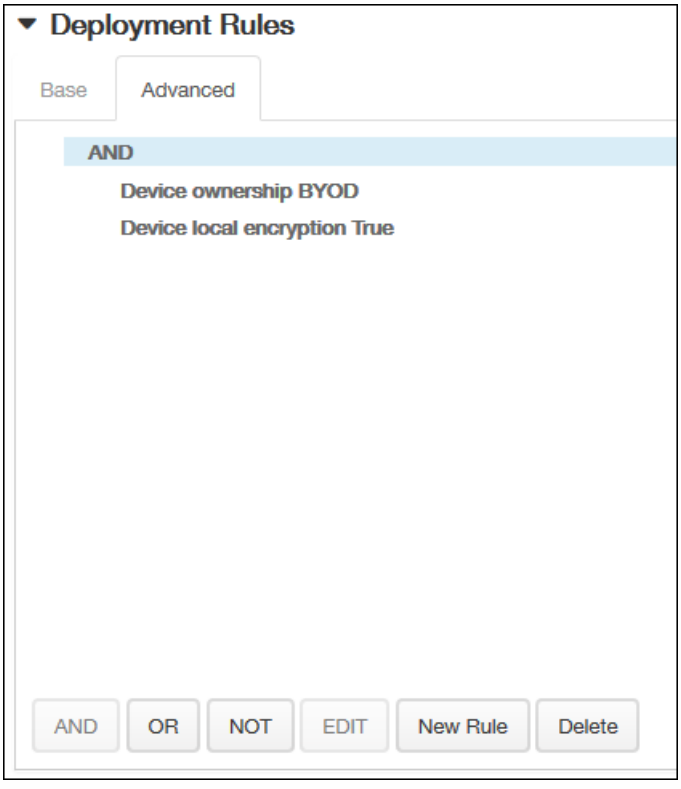
© 1999-2017 Citrix Systems, Inc. All rights reserved.



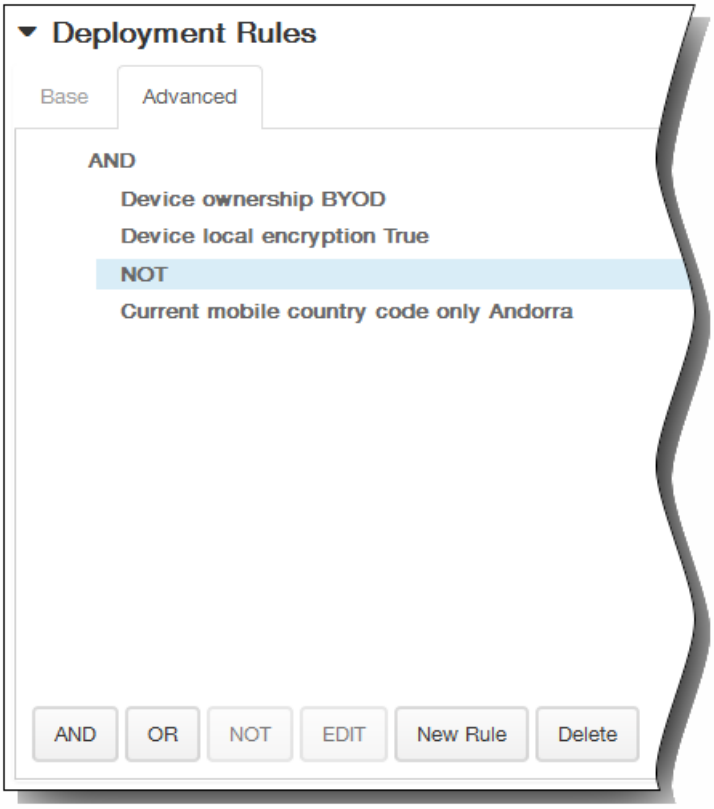


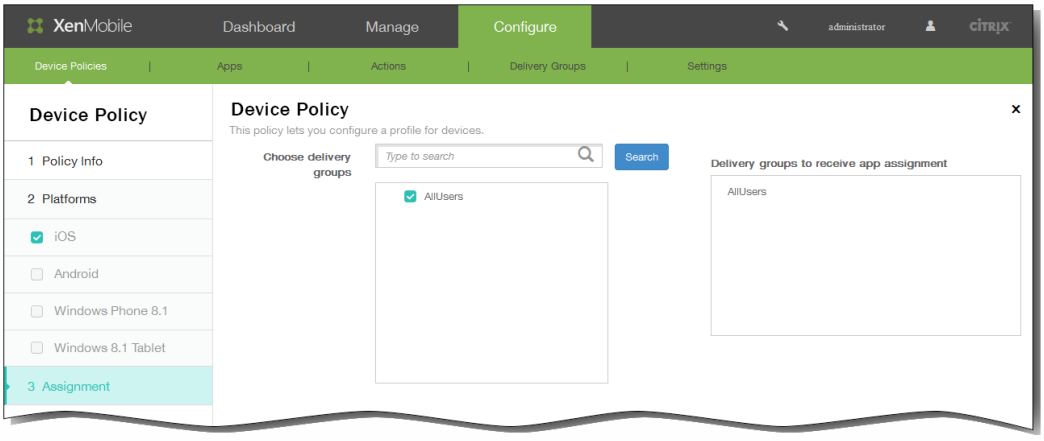
© 1999-2017 Citrix Systems, Inc. All rights reserved.



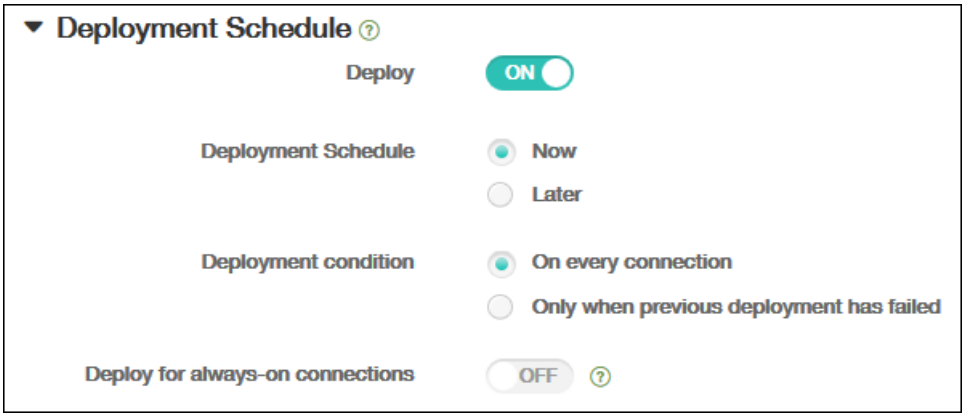


© 1999-2017 Citrix Systems, Inc. All rights reserved.

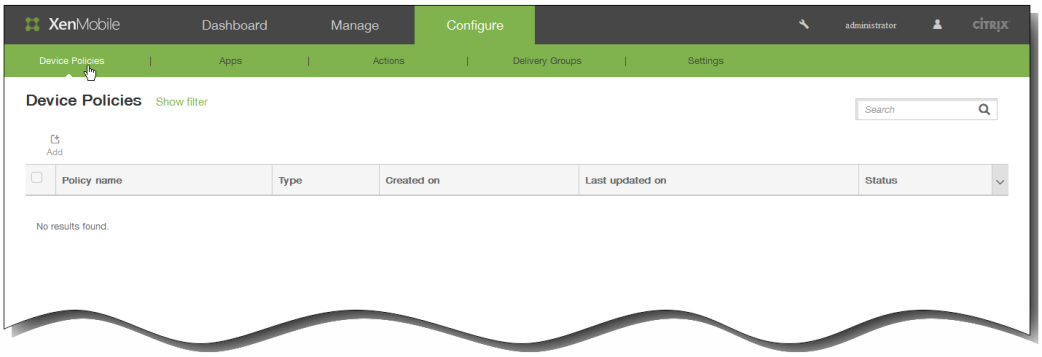




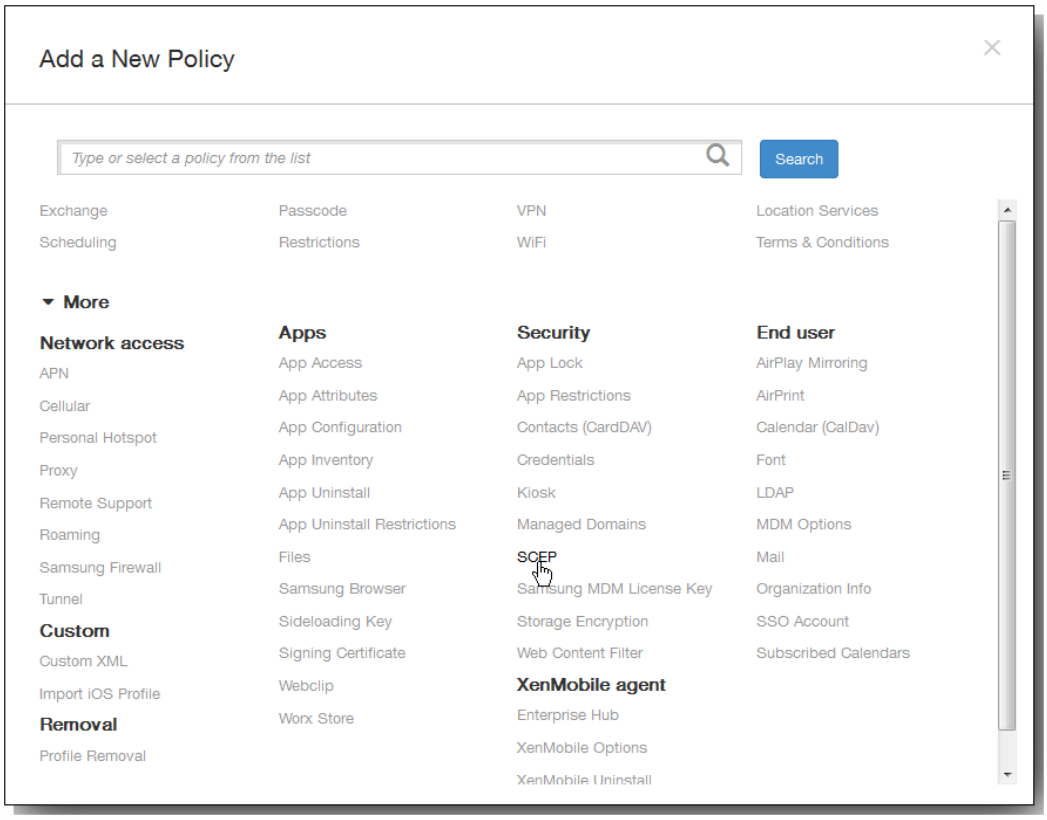
© 1999-2017 Citrix Systems, Inc. All rights reserved.

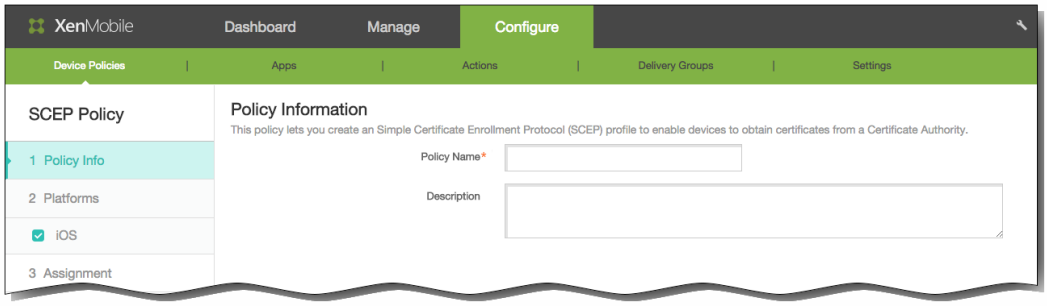


© 1999-2017 Citrix Systems, Inc. All rights reserved.

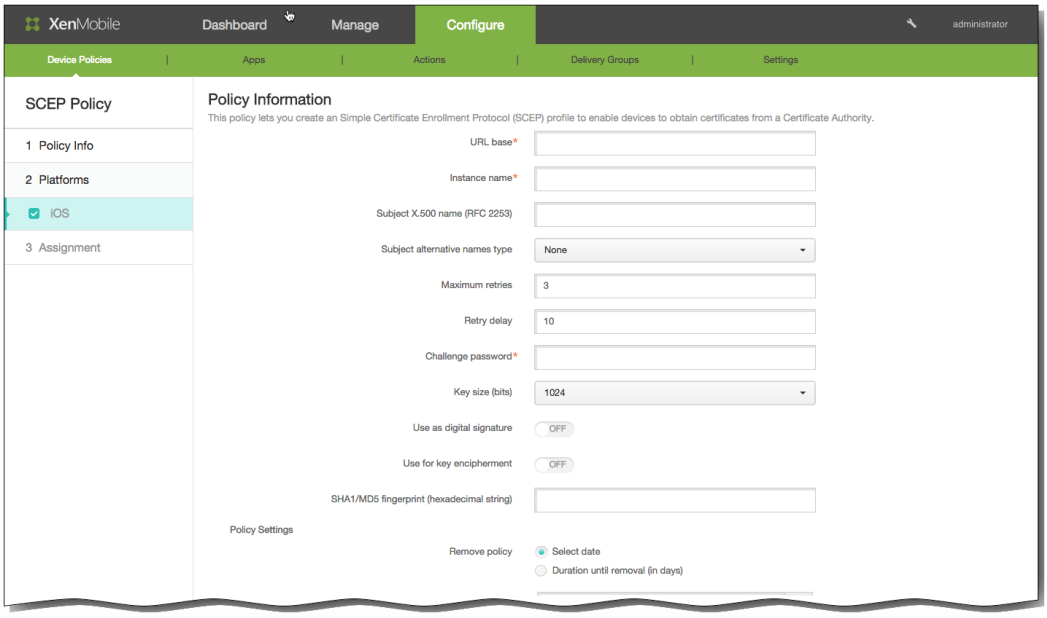


© 1999-2017 Citrix Systems, Inc. All rights reserved.

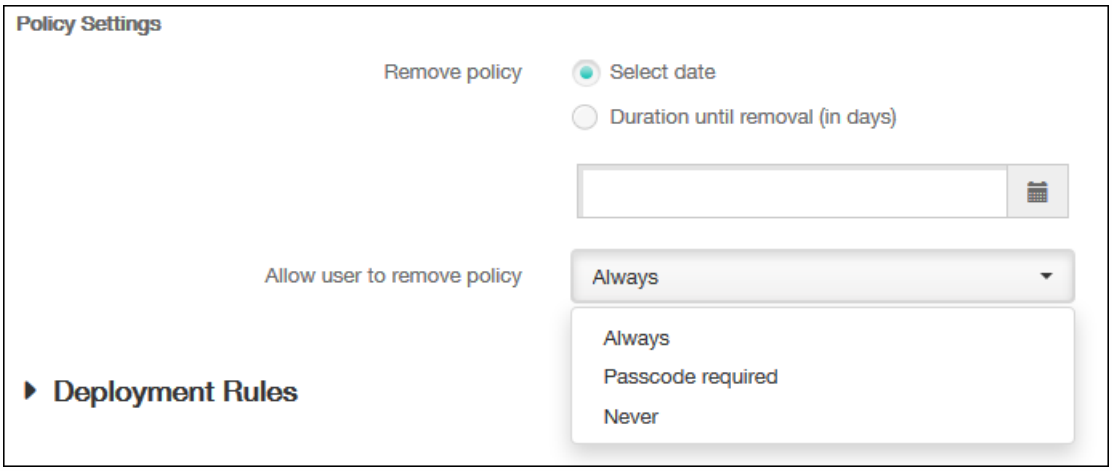




© 1999-2017 Citrix Systems, Inc. All rights reserved.

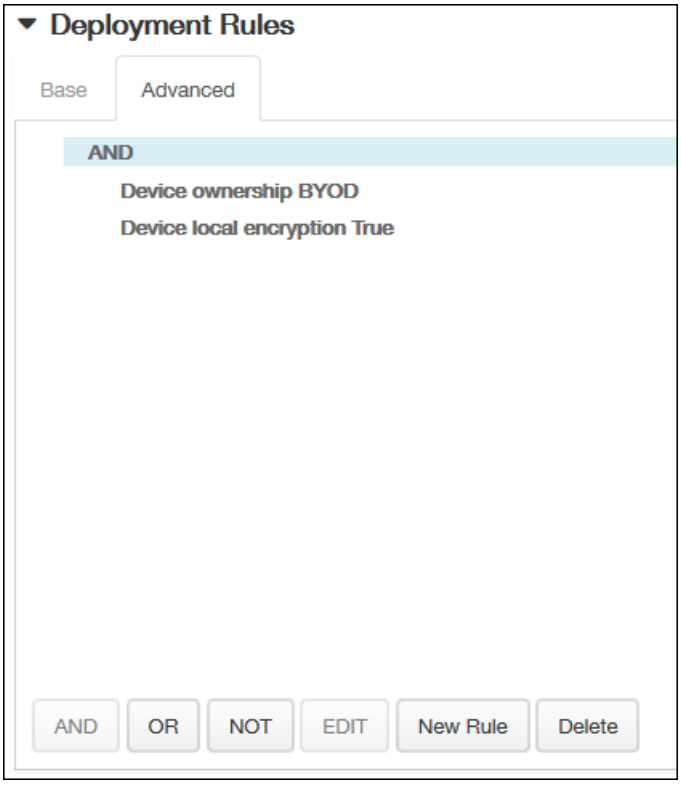


© 1999-2017 Citrix Systems, Inc. All rights reserved.

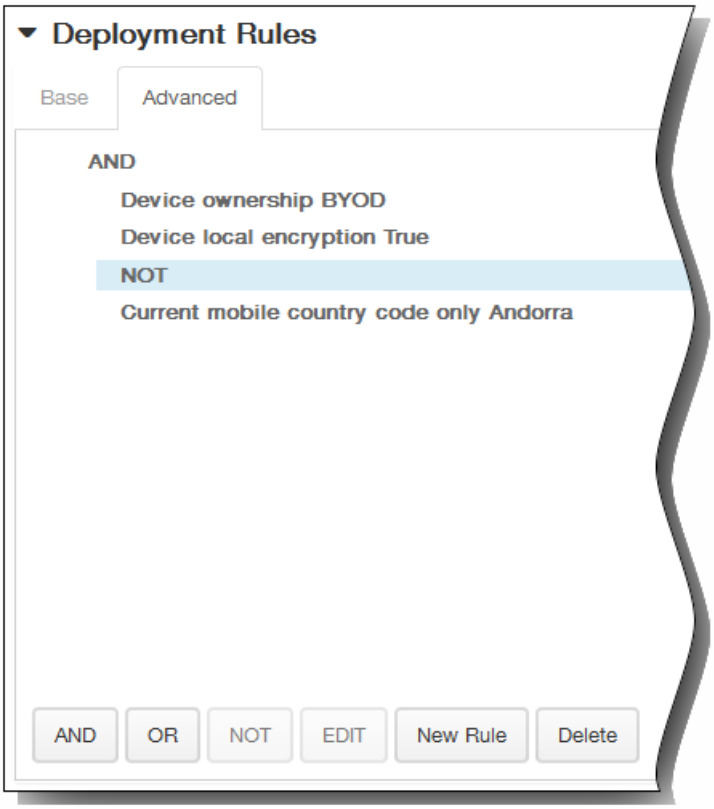


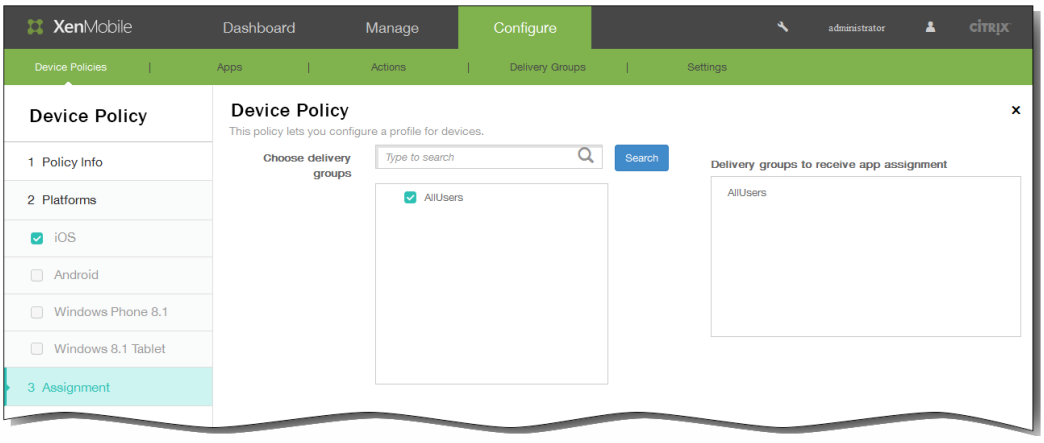


© 1999-2017 Citrix Systems, Inc. All rights reserved.

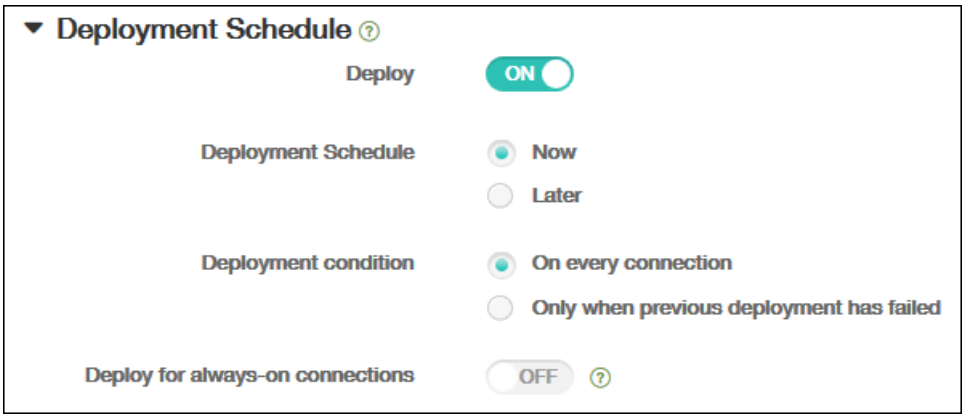


© 1999-2017 Citrix Systems, Inc. All rights reserved.

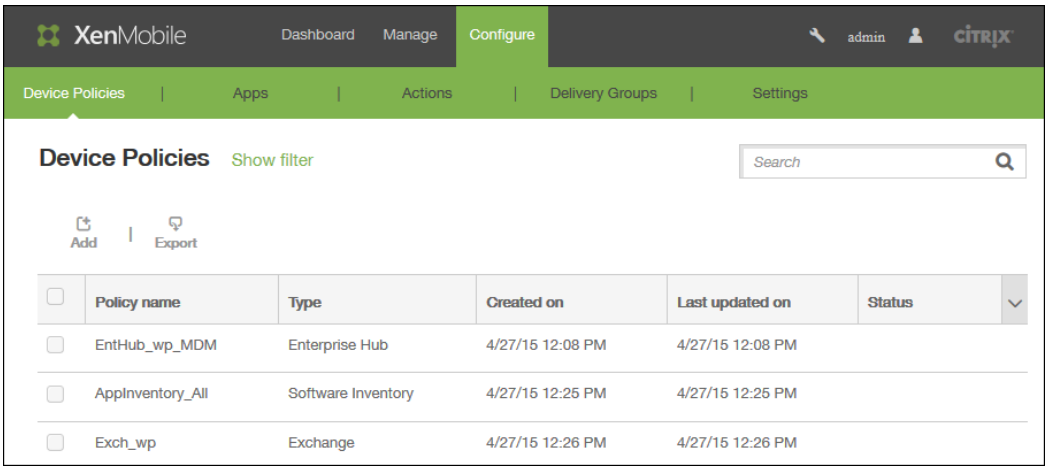




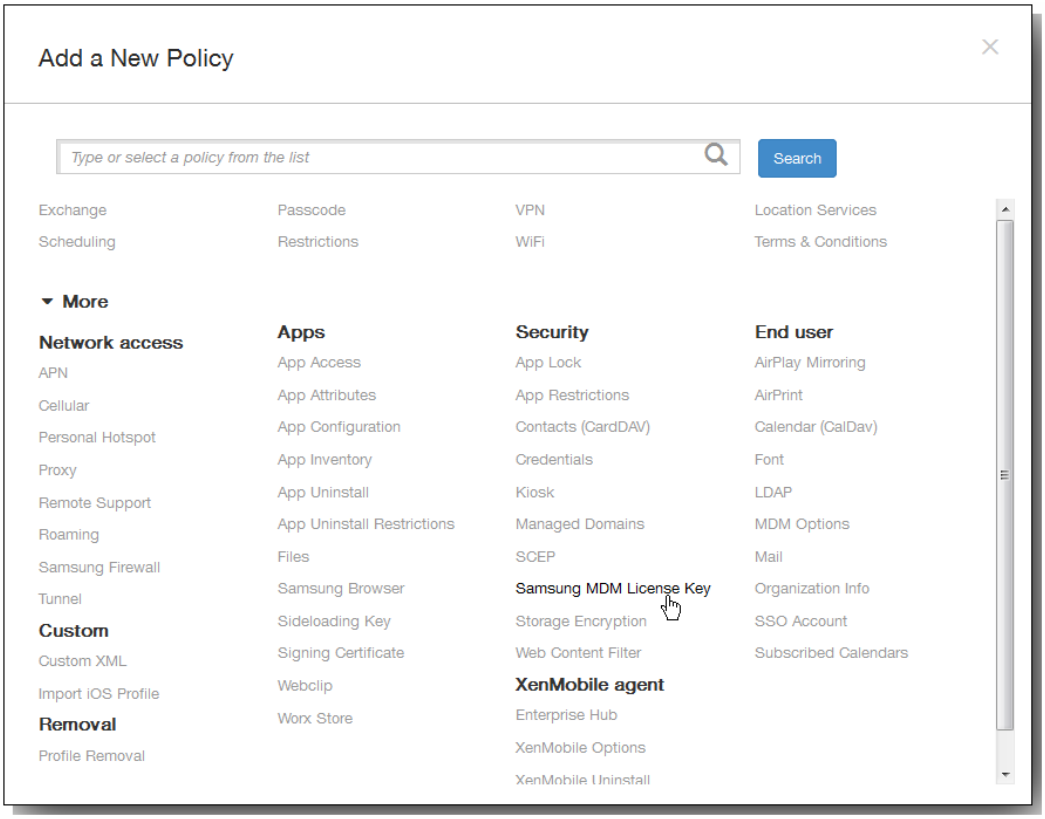
© 1999-2017 Citrix Systems, Inc. All rights reserved.

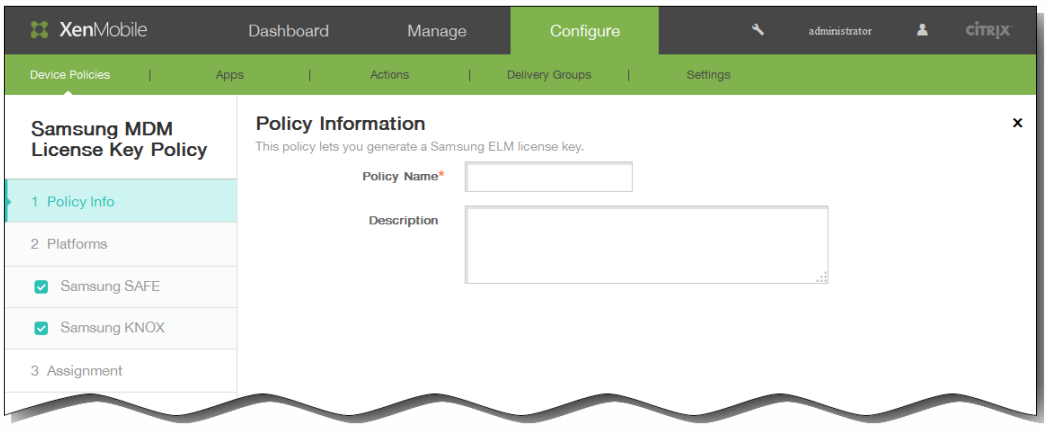


© 1999-2017 Citrix Systems, Inc. All rights reserved.

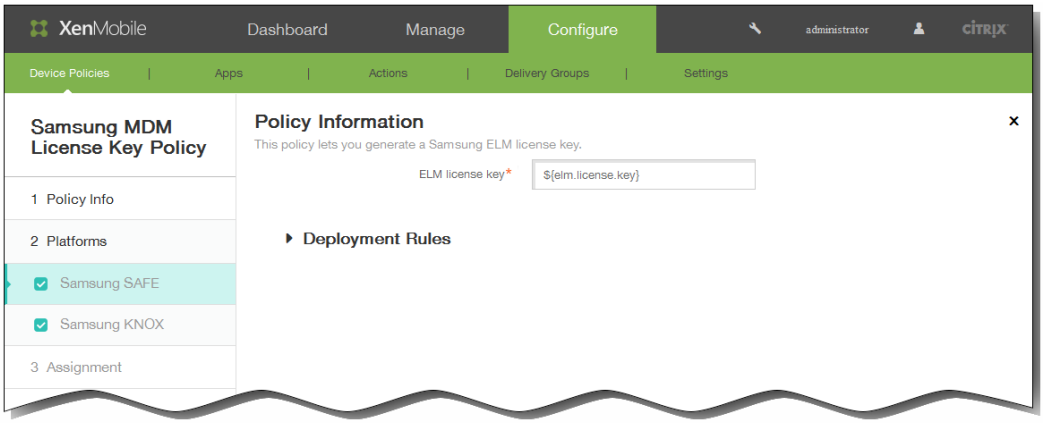


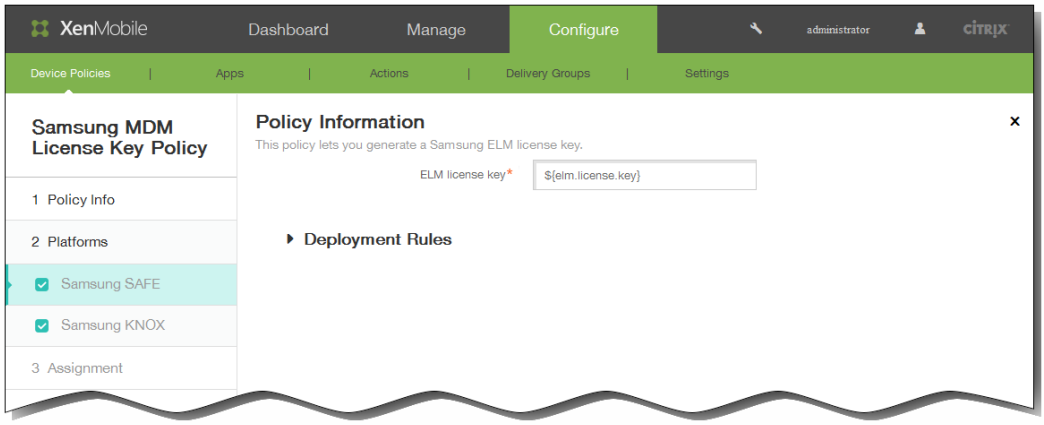
© 1999-2017 Citrix Systems, Inc. All rights reserved.

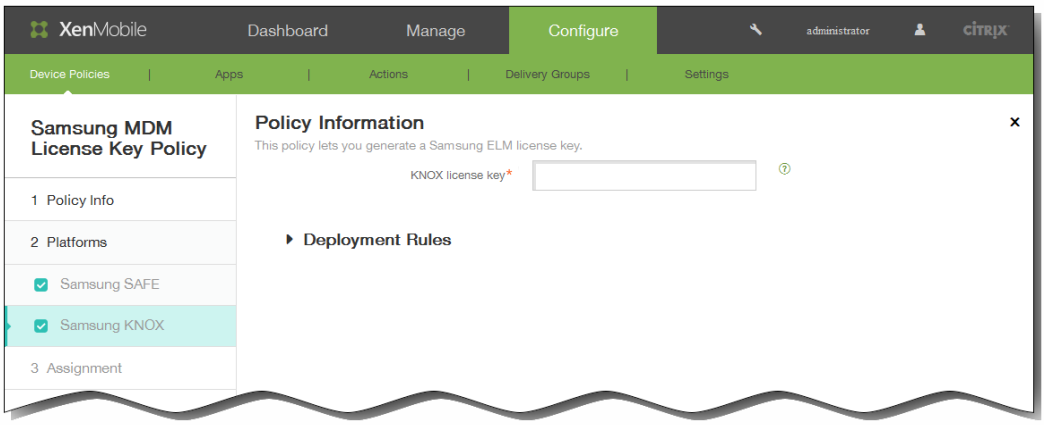




© 1999-2017 Citrix Systems, Inc. All rights reserved.

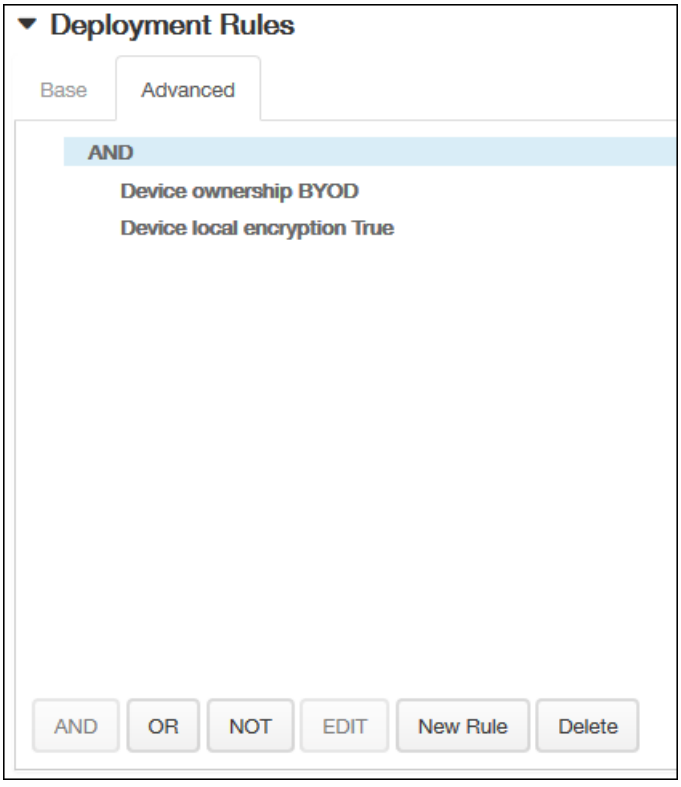




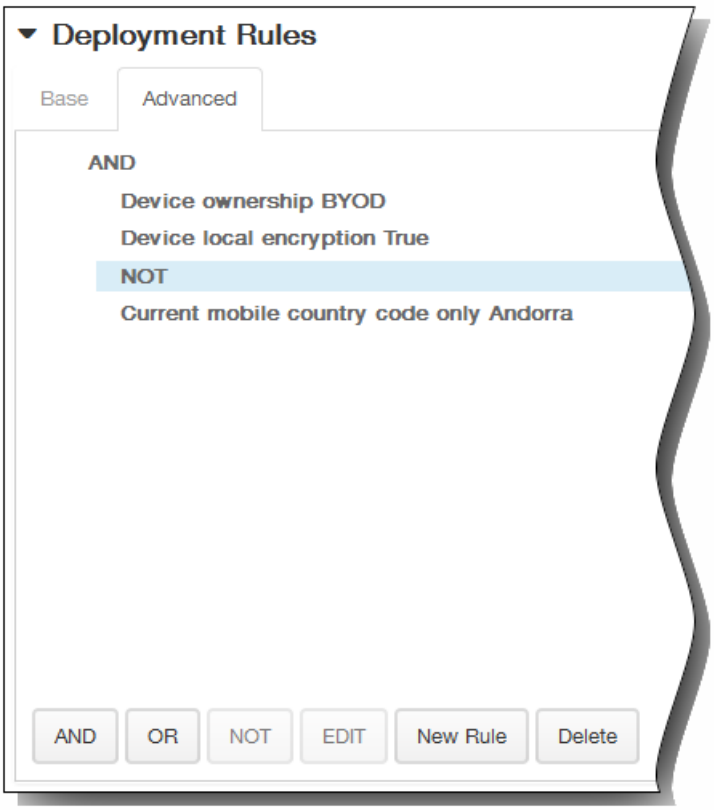


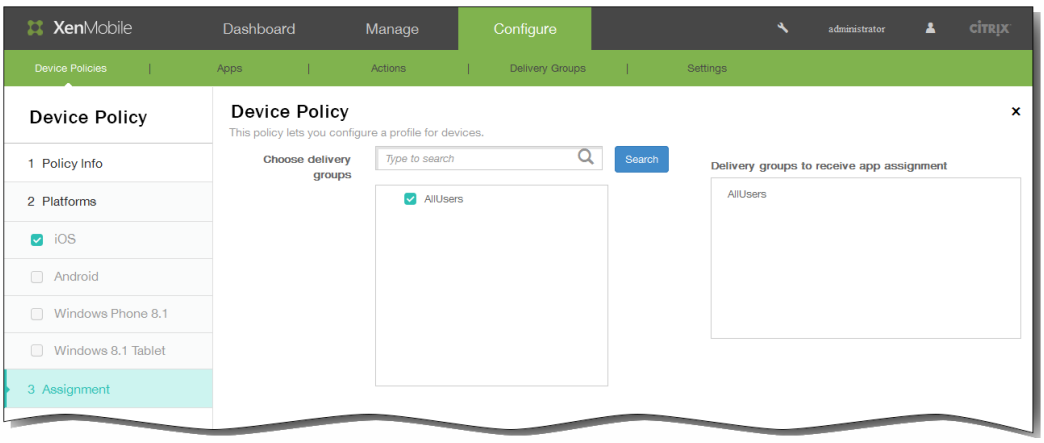
© 1999-2017 Citrix Systems, Inc. All rights reserved.



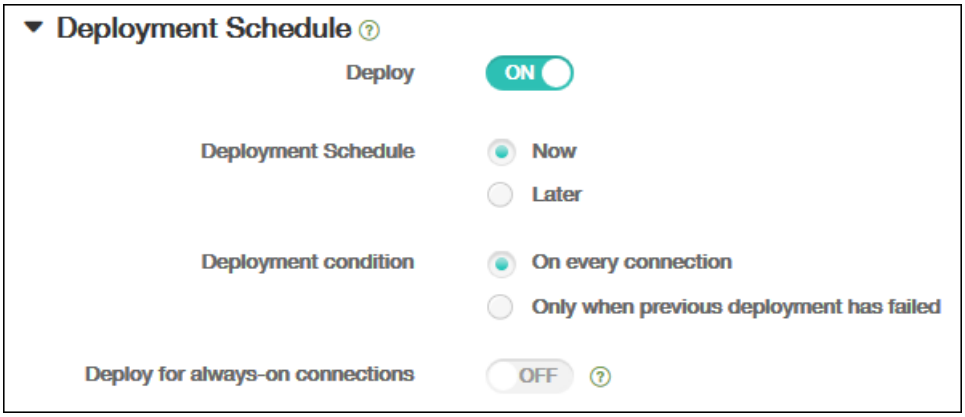


© 1999-2017 Citrix Systems, Inc. All rights reserved.



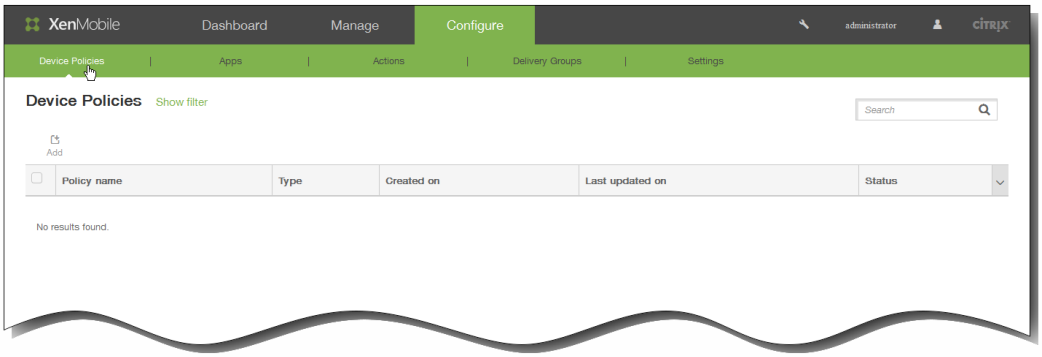


© 1999-2017 Citrix Systems, Inc. All rights reserved.

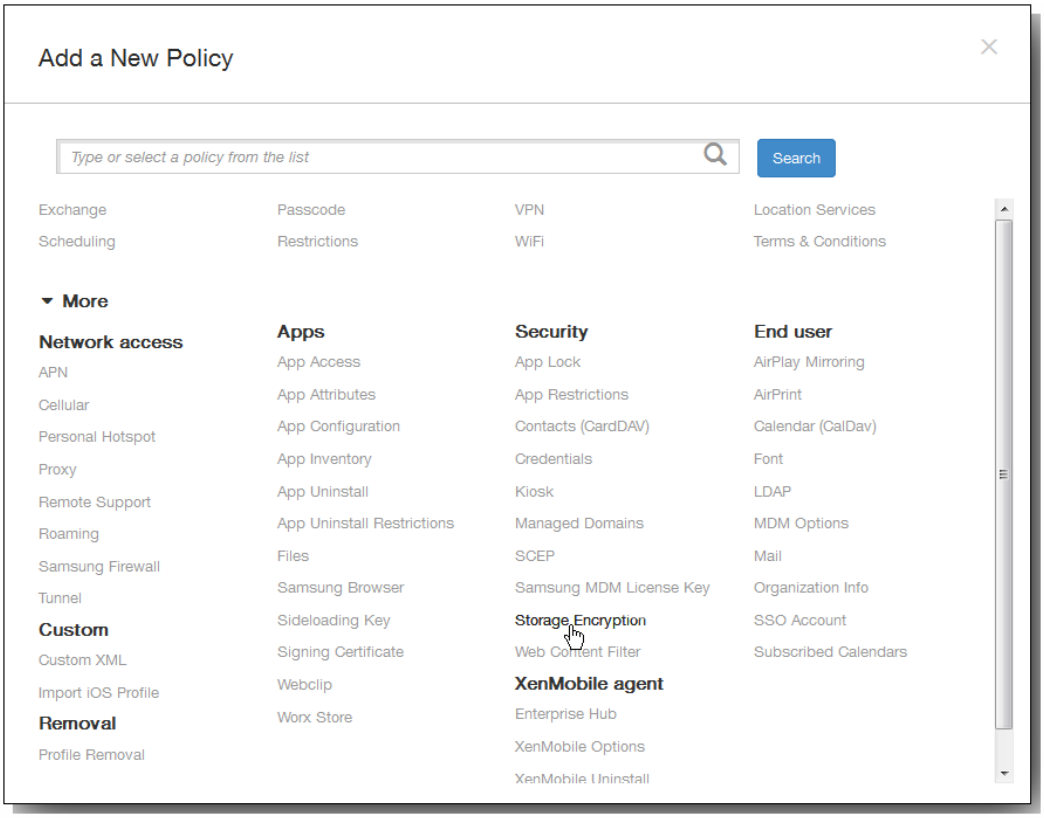


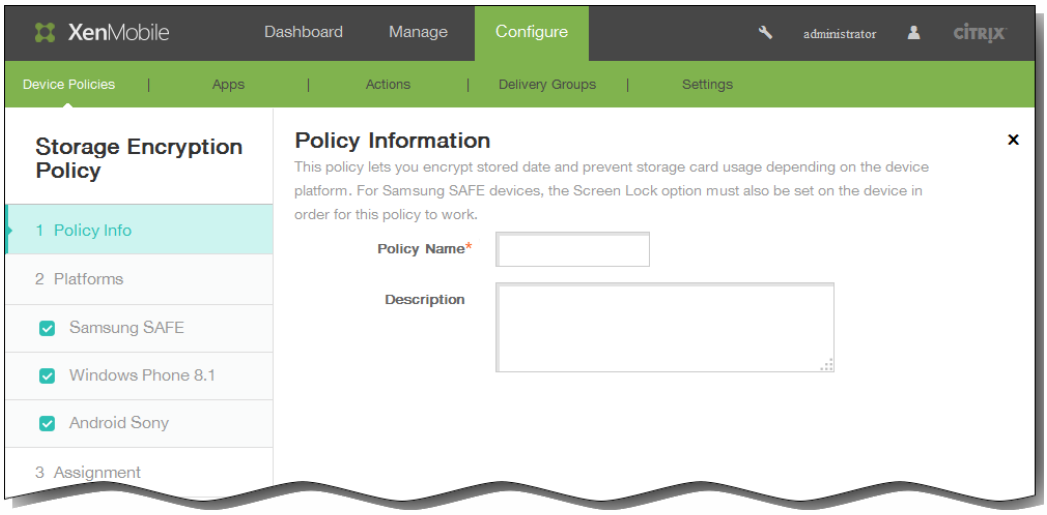
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-



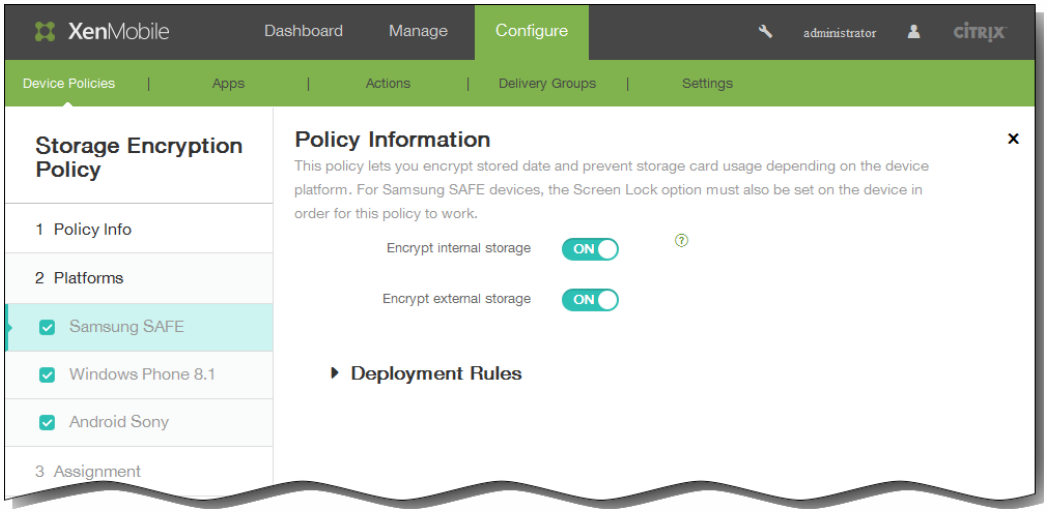
© 1999-2017 Citrix Systems, Inc. All rights reserved.



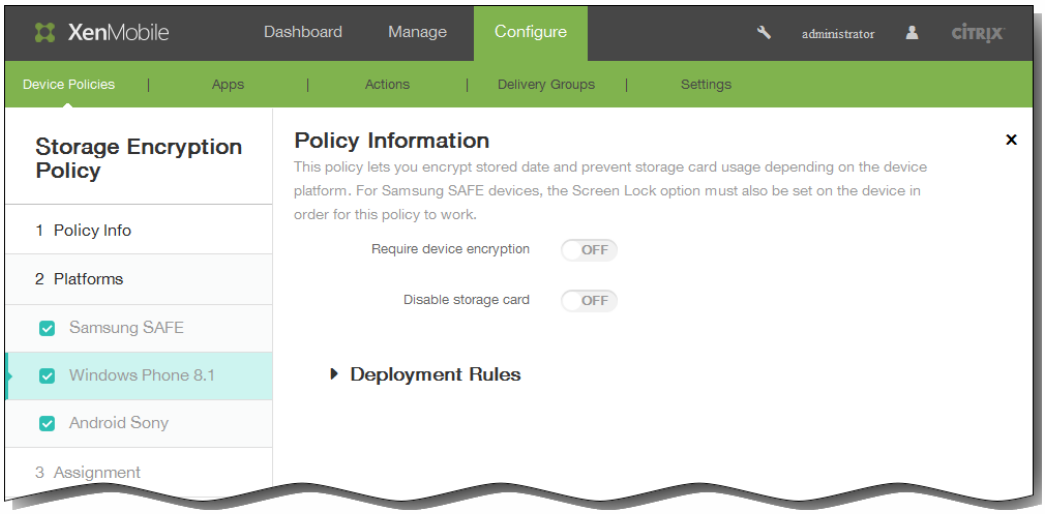


© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
  -
  -

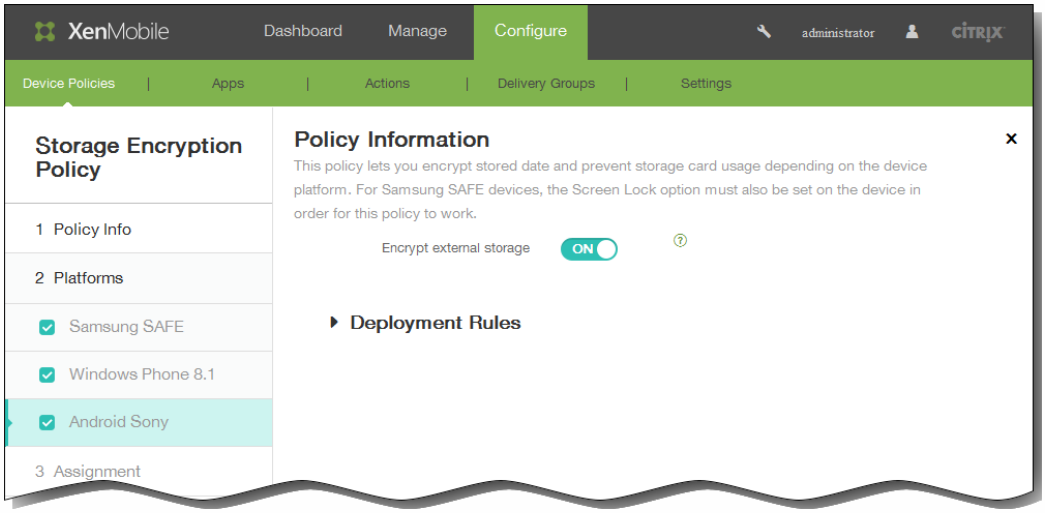


-
  -
  -



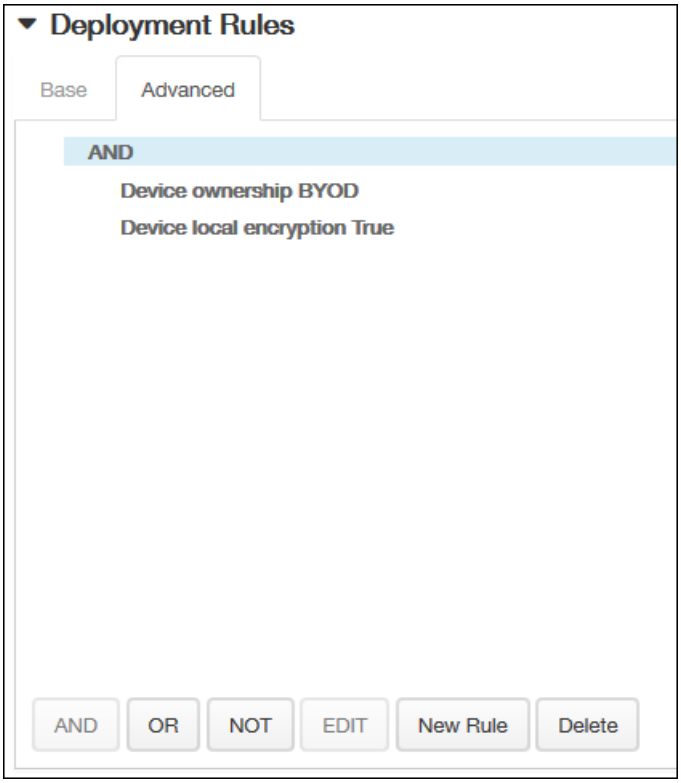
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

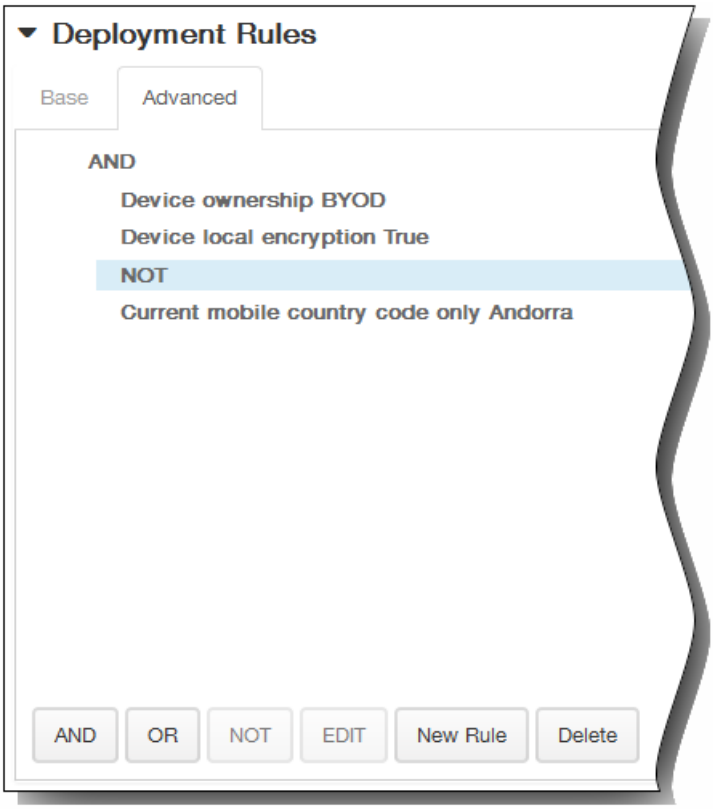


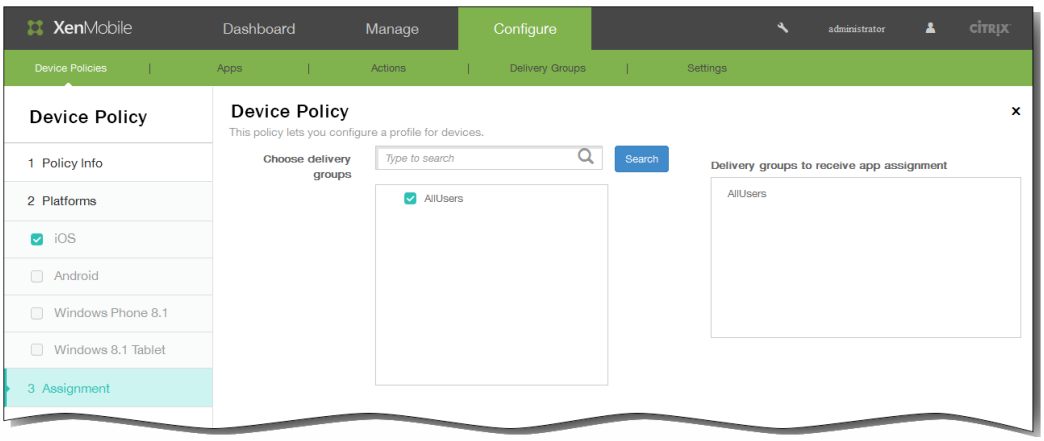


© 1999-2017 Citrix Systems, Inc. All rights reserved.

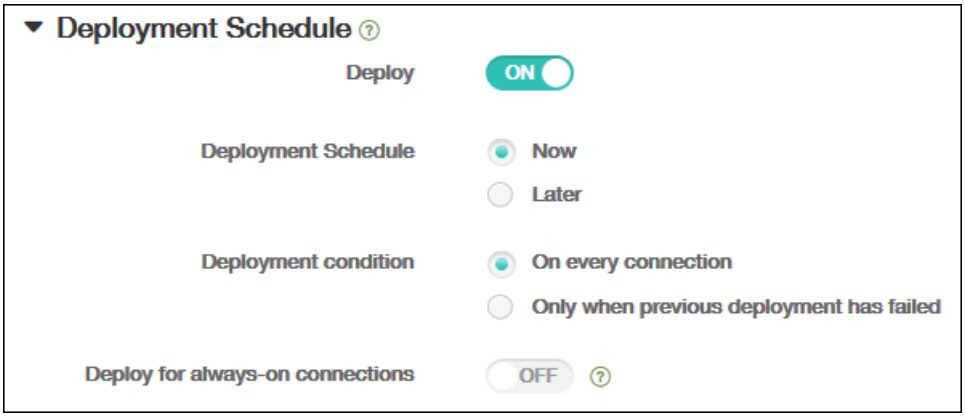


© 1999-2017 Citrix Systems, Inc. All rights reserved.

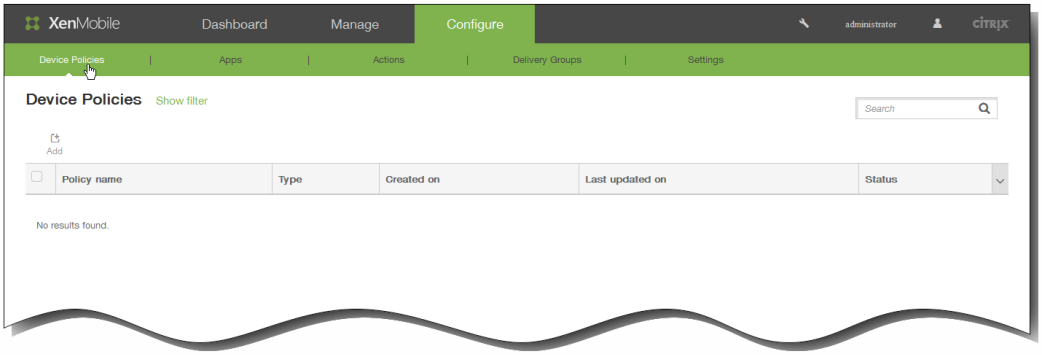




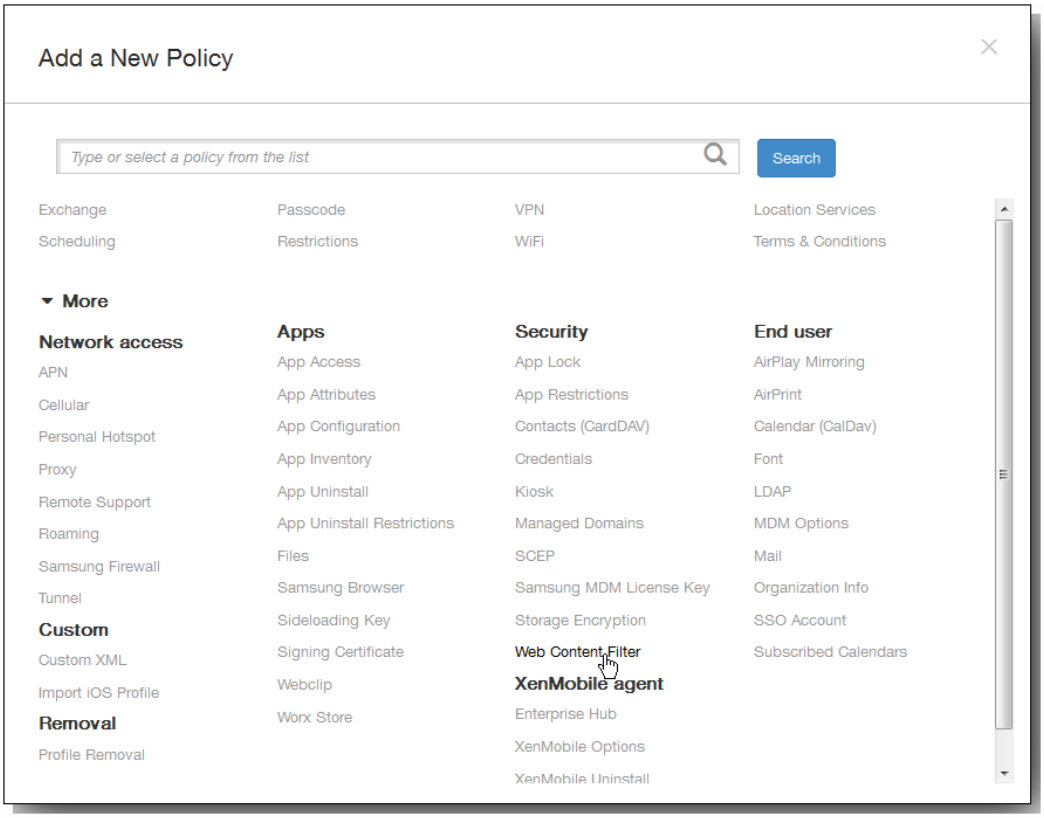
© 1999-2017 Citrix Systems, Inc. All rights reserved.

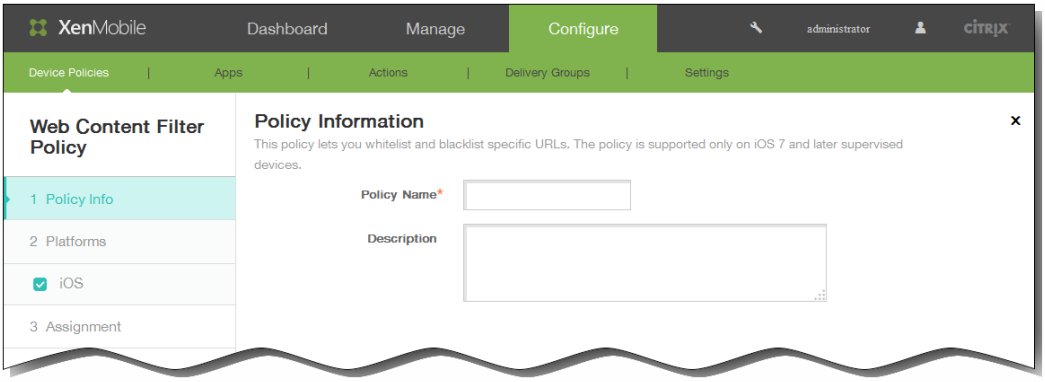


© 1999-2017 Citrix Systems, Inc. All rights reserved.

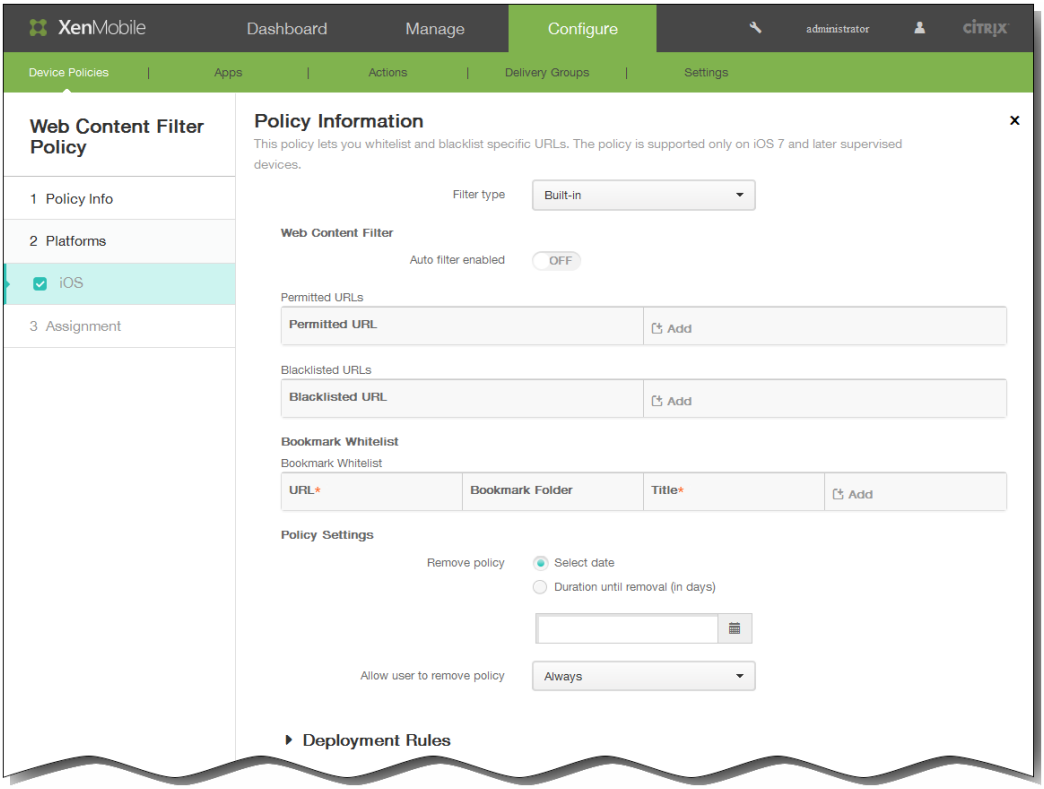


© 1999-2017 Citrix Systems, Inc. All rights reserved.



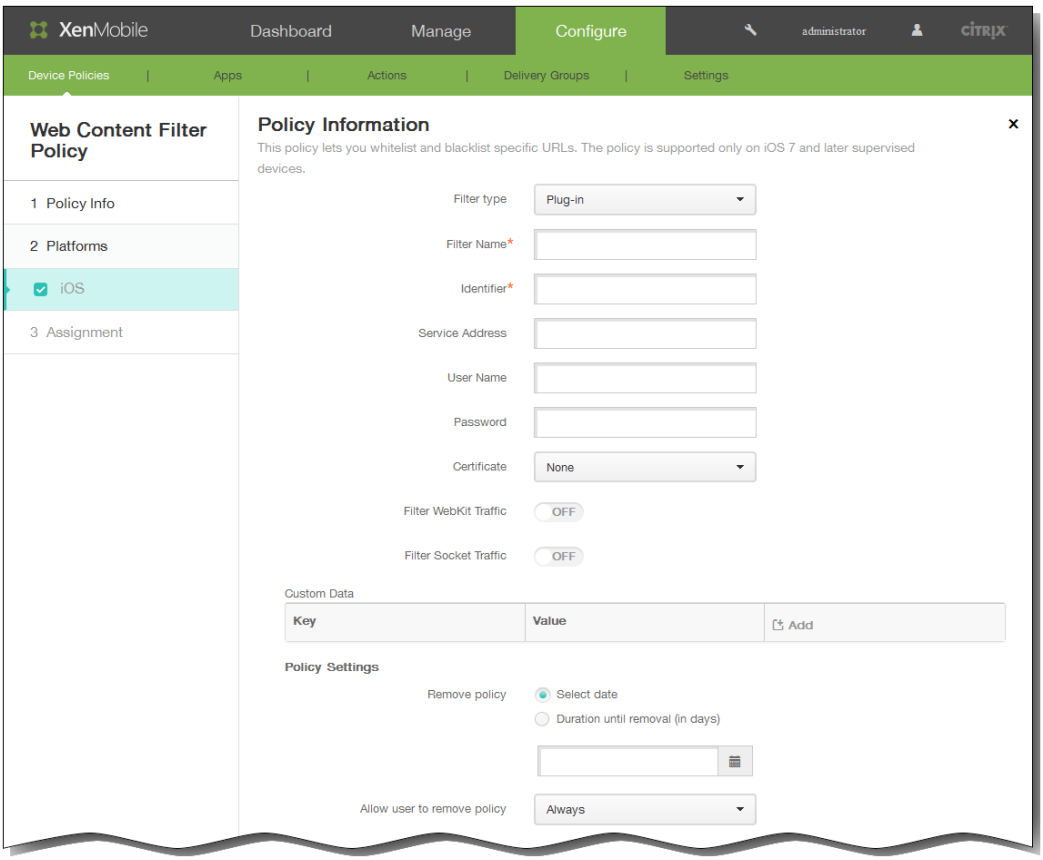


© 1999-2017 Citrix Systems, Inc. All rights reserved.

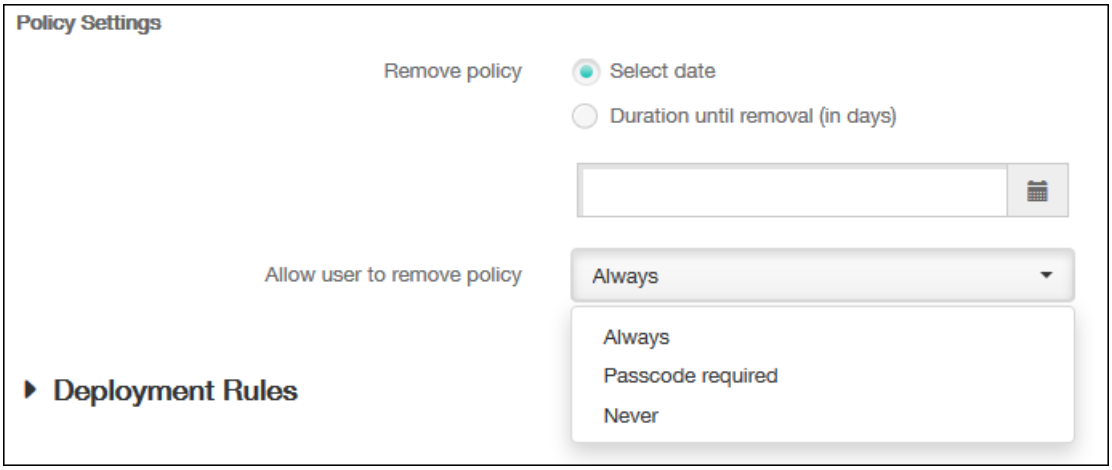


-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

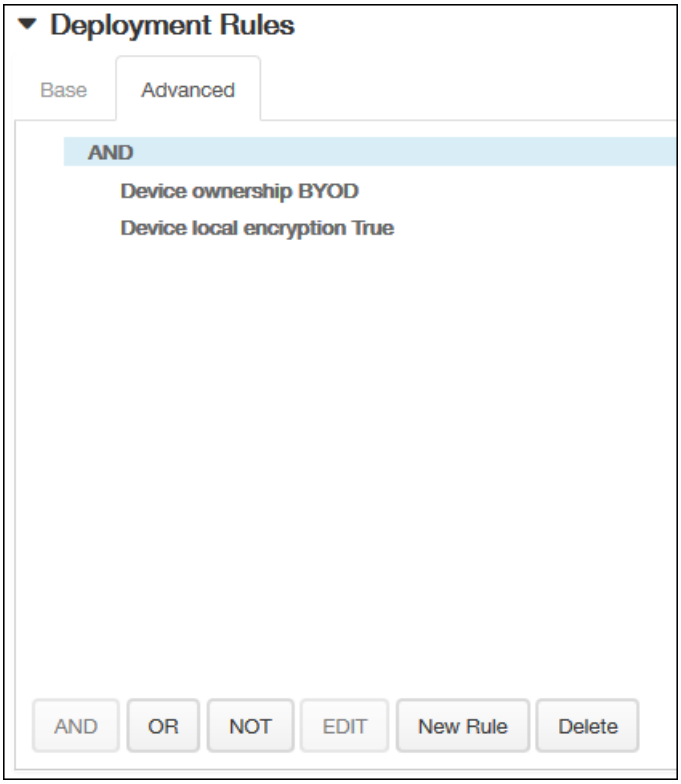


© 1999-2017 Citrix Systems, Inc. All rights reserved.

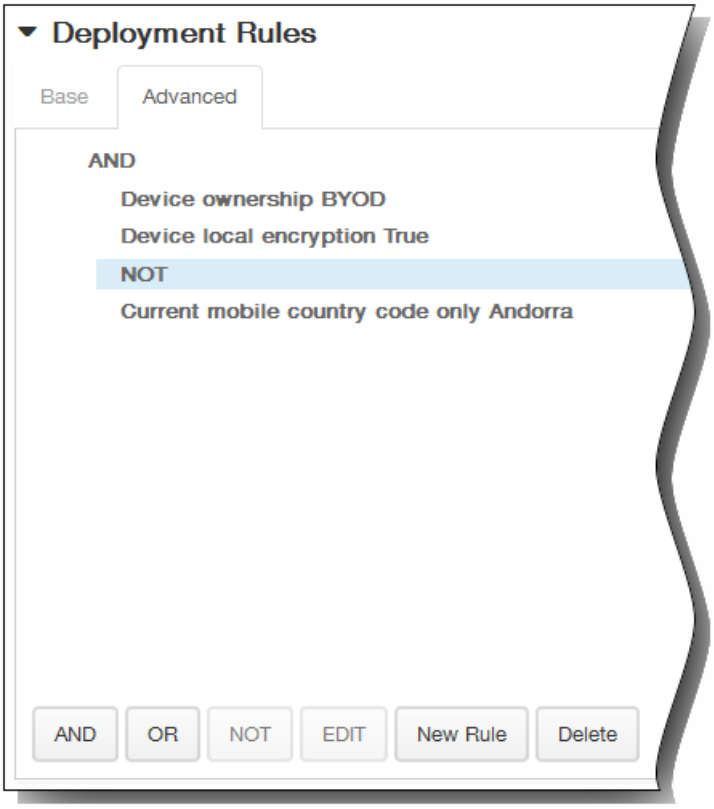


© 1999-2017 Citrix Systems, Inc. All rights reserved.

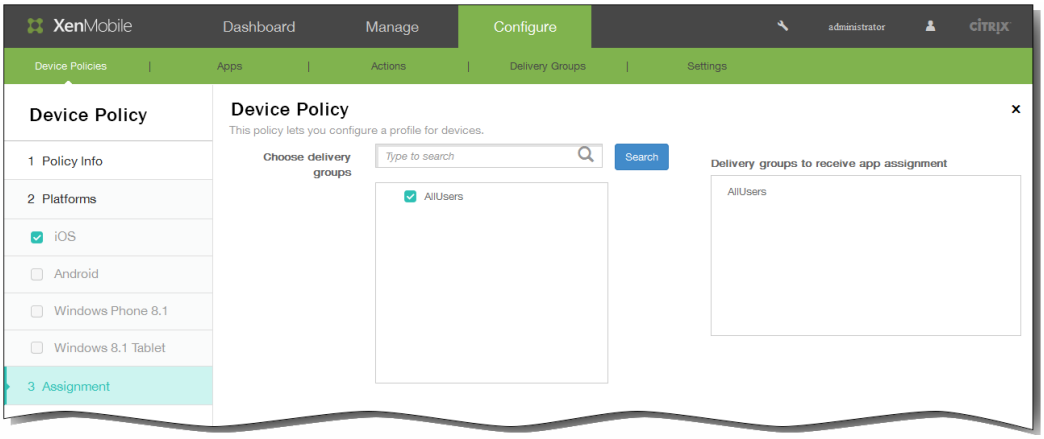


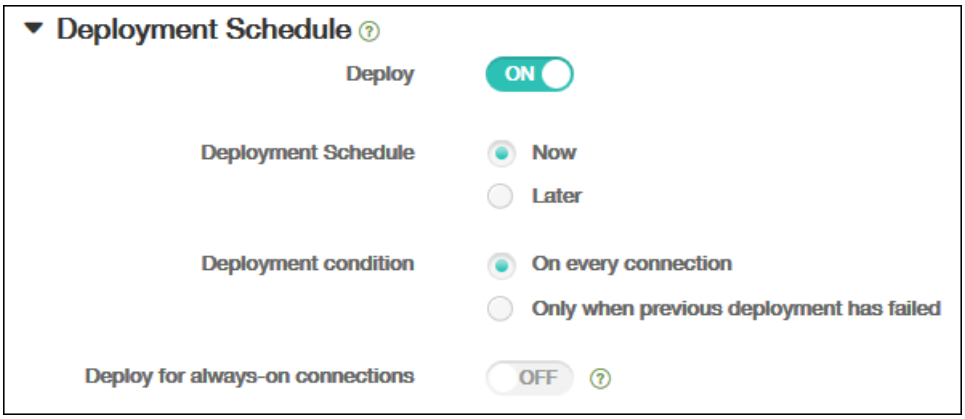


© 1999-2017 Citrix Systems, Inc. All rights reserved.

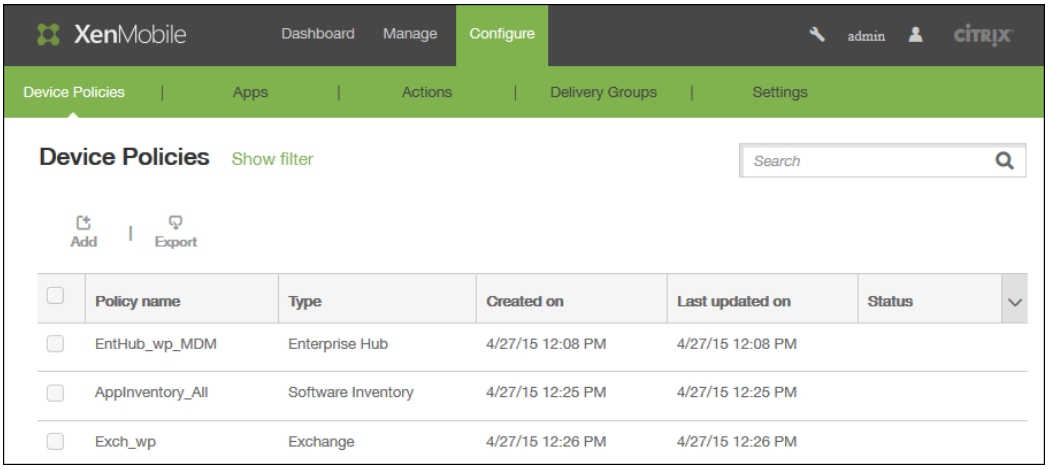


© 1999-2017 Citrix Systems, Inc. All rights reserved.

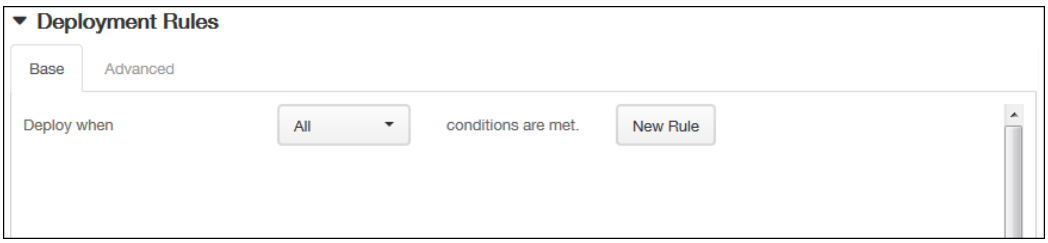


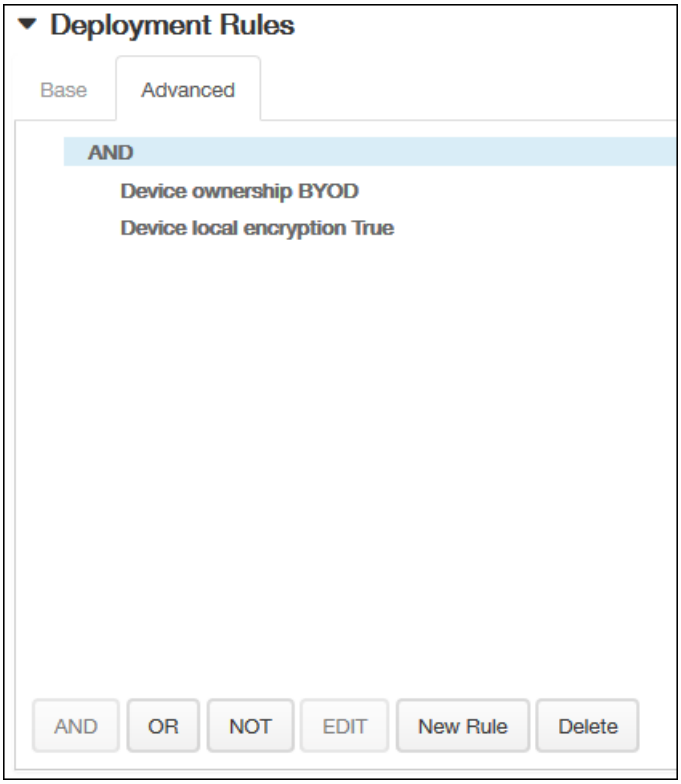


© 1999-2017 Citrix Systems, Inc. All rights reserved.

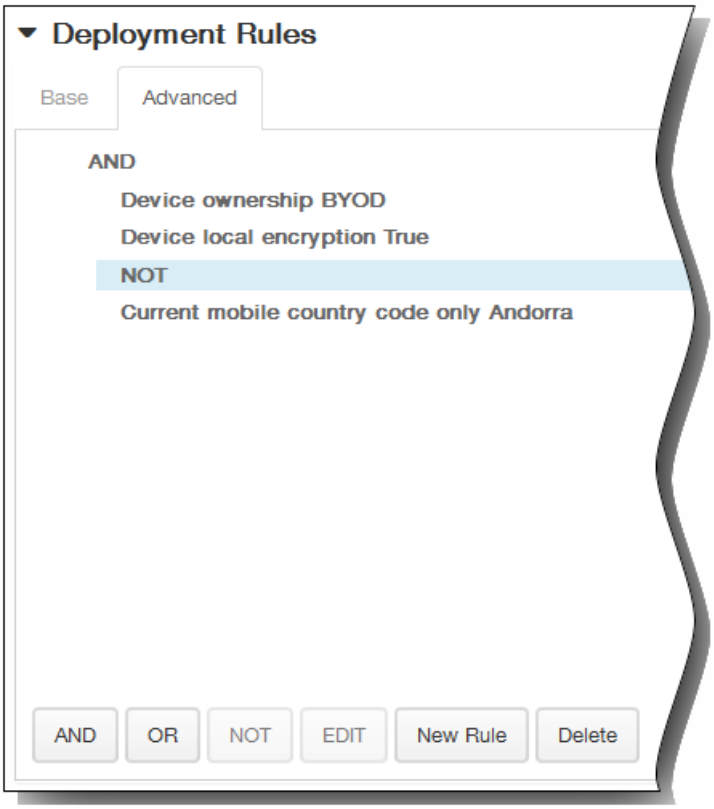


© 1999-2017 Citrix Systems, Inc. All rights reserved.

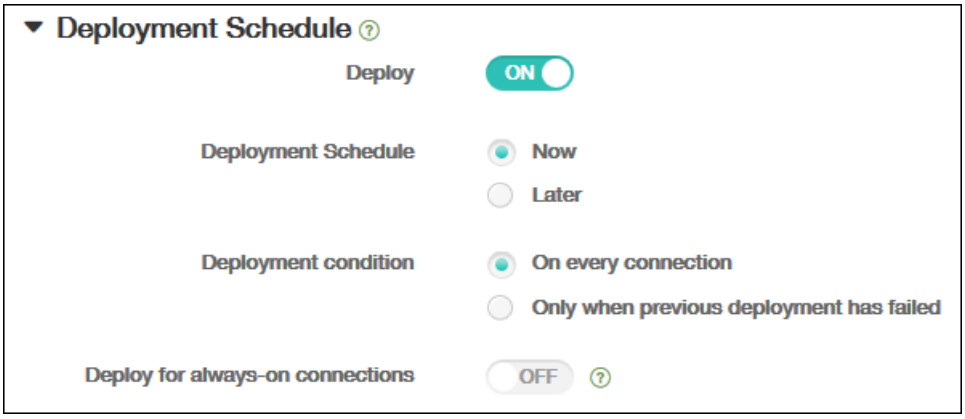




© 1999-2017 Citrix Systems, Inc. All rights reserved.

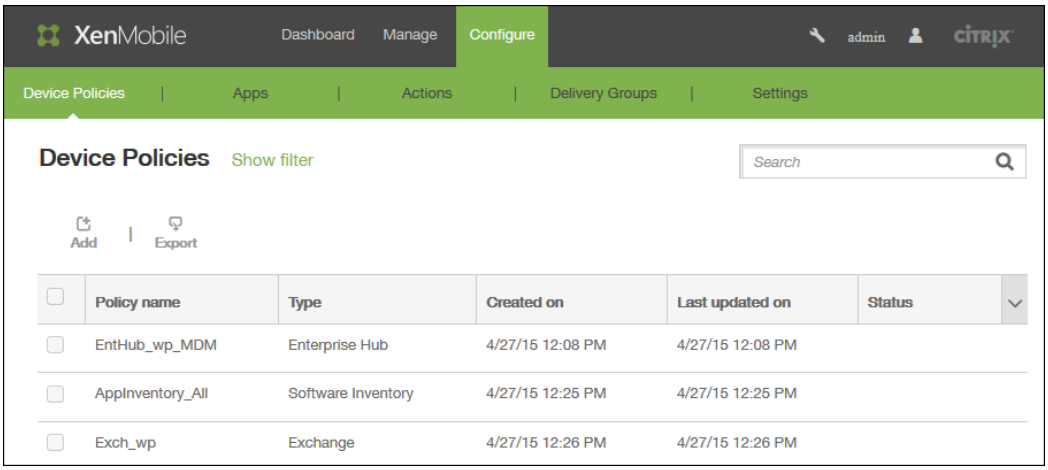


© 1999-2017 Citrix Systems, Inc. All rights reserved.

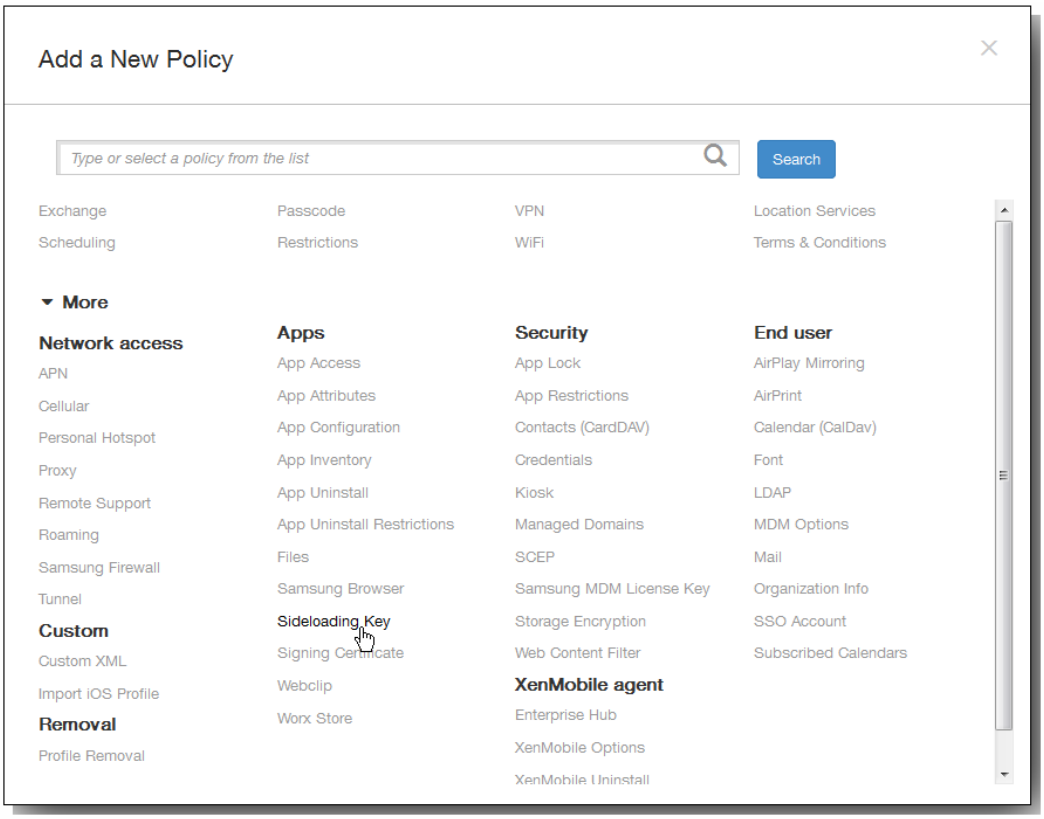


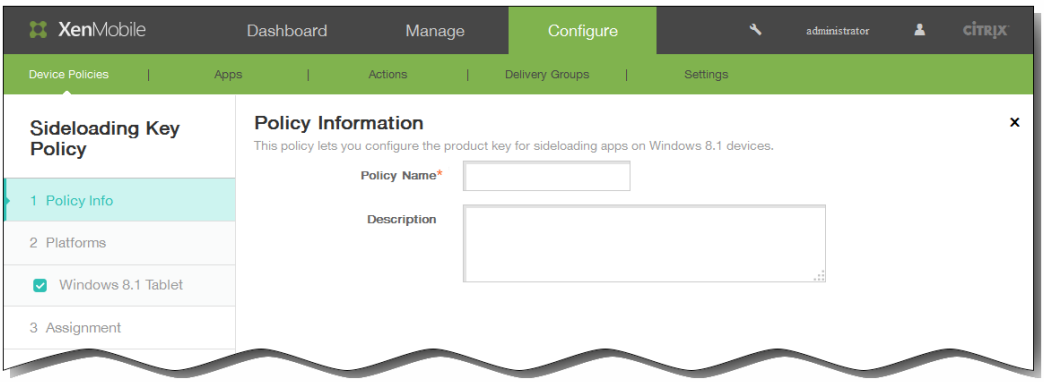
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

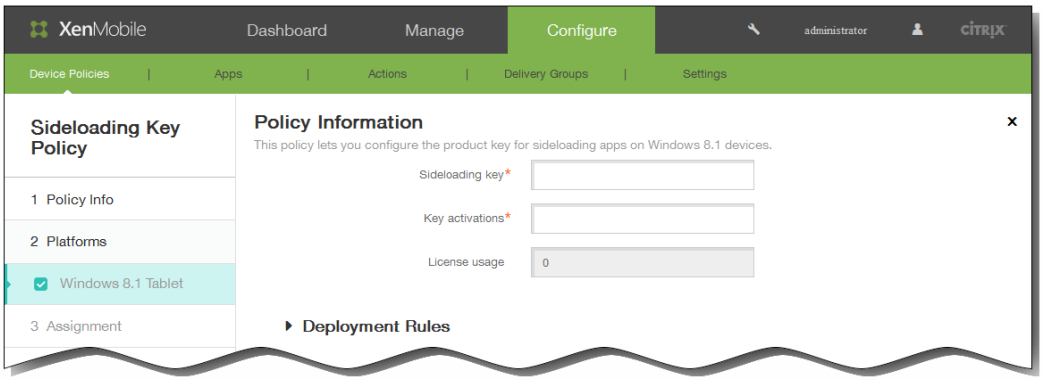


© 1999-2017 Citrix Systems, Inc. All rights reserved.



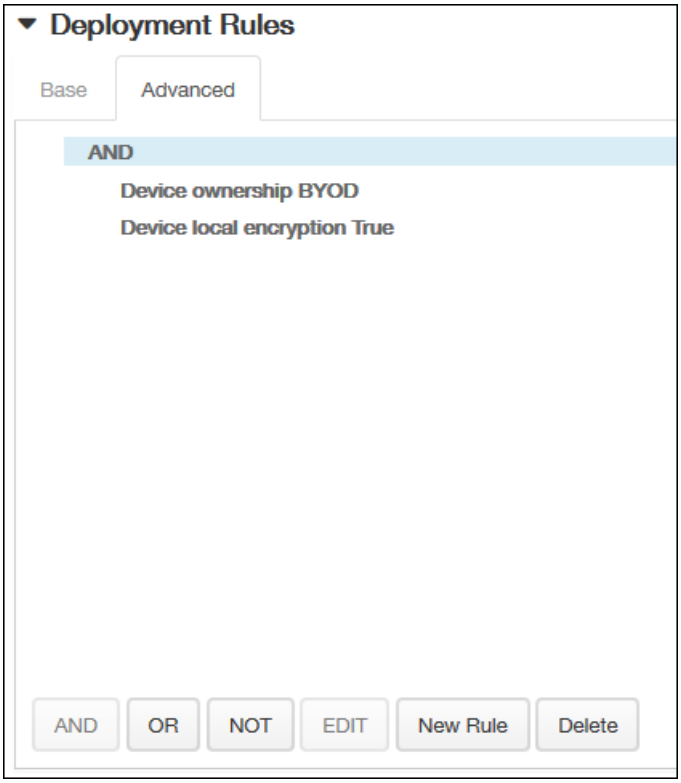


© 1999-2017 Citrix Systems, Inc. All rights reserved.

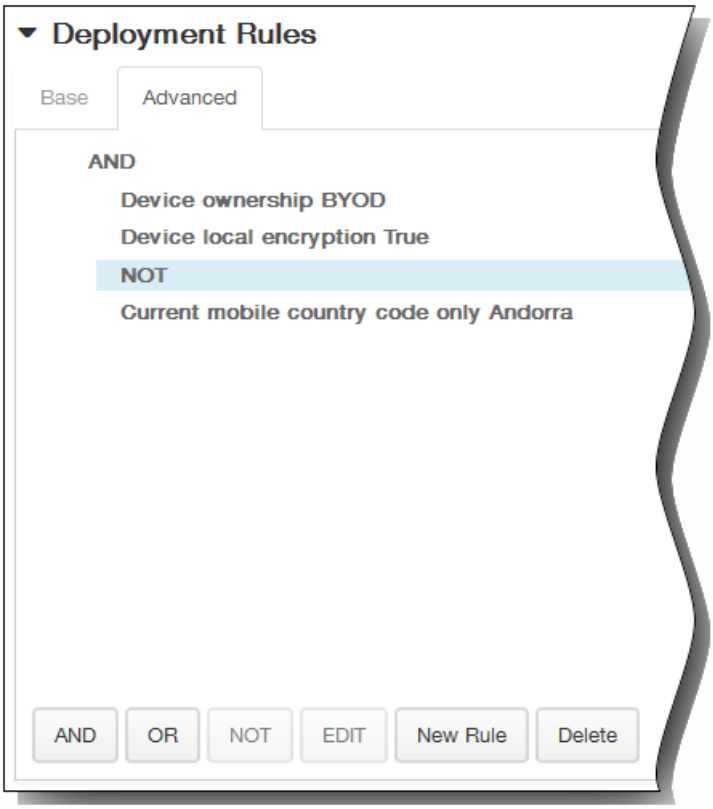


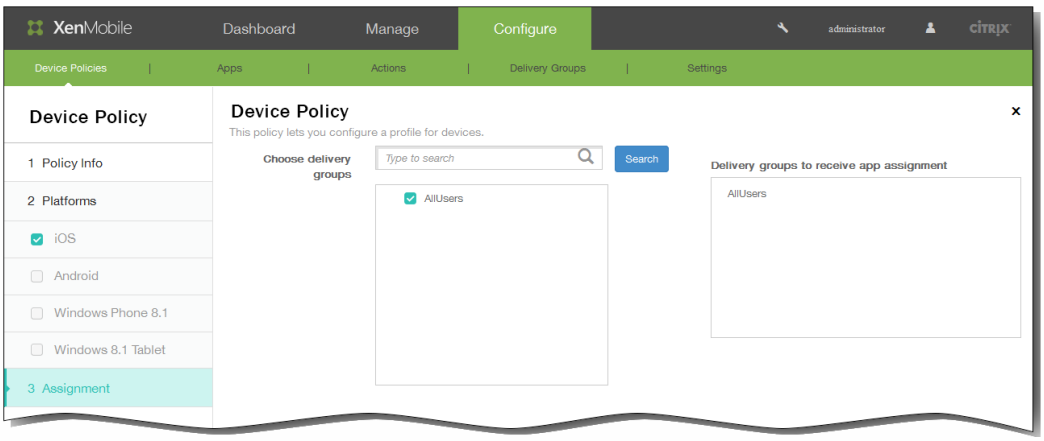


© 1999-2017 Citrix Systems, Inc. All rights reserved.

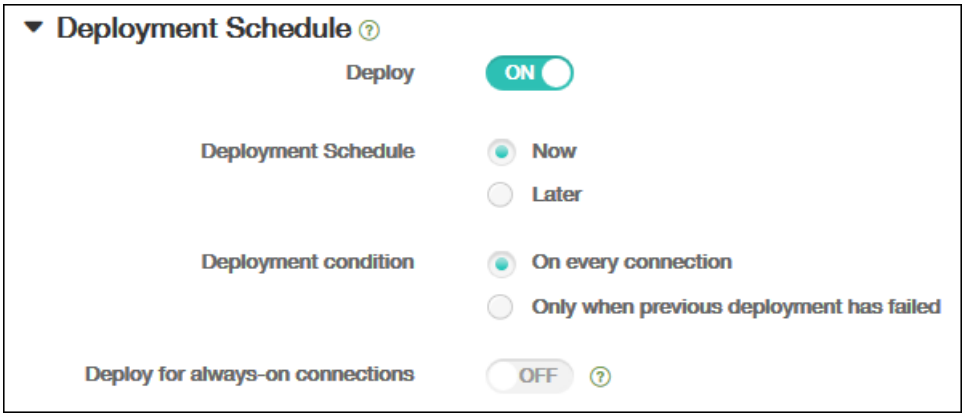


© 1999-2017 Citrix Systems, Inc. All rights reserved.

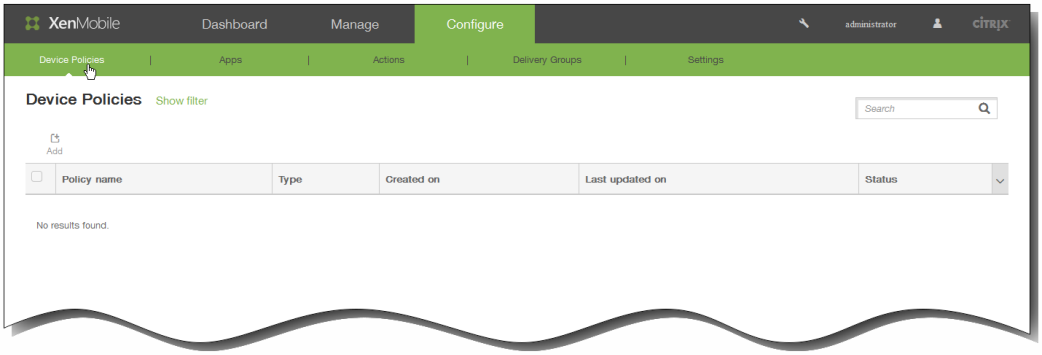




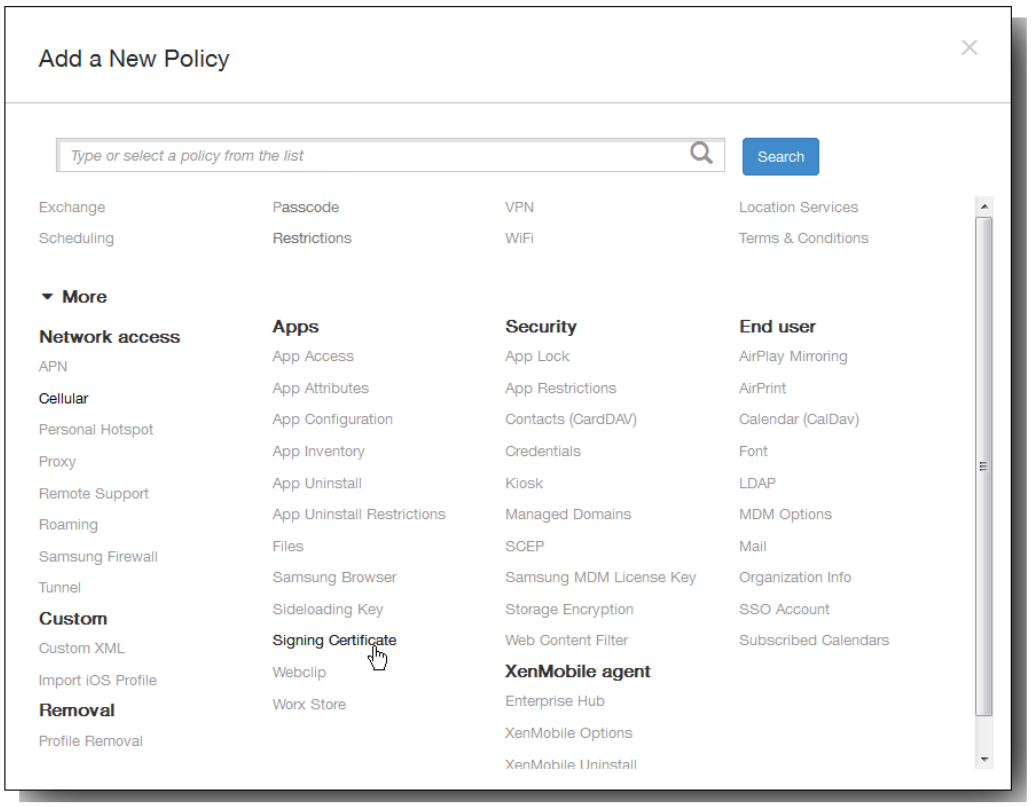
© 1999-2017 Citrix Systems, Inc. All rights reserved.

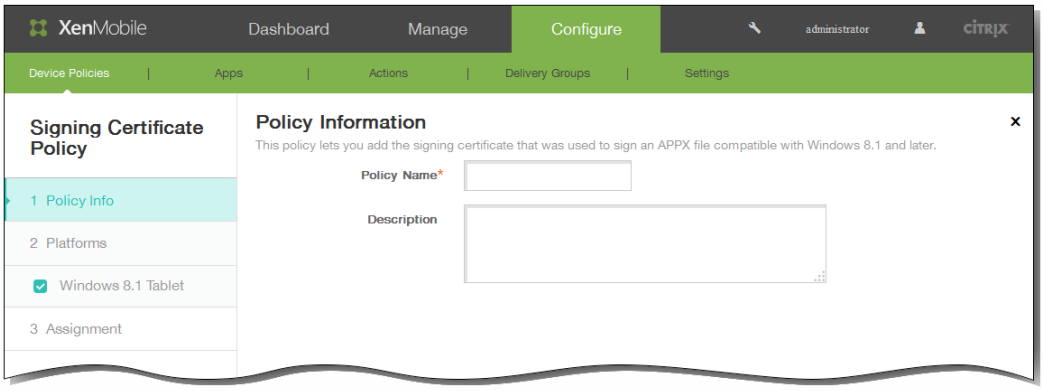


© 1999-2017 Citrix Systems, Inc. All rights reserved.

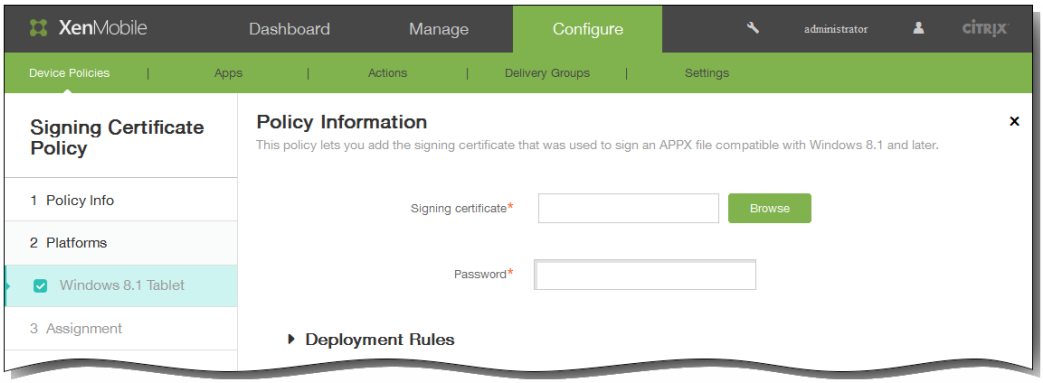


© 1999-2017 Citrix Systems, Inc. All rights reserved.



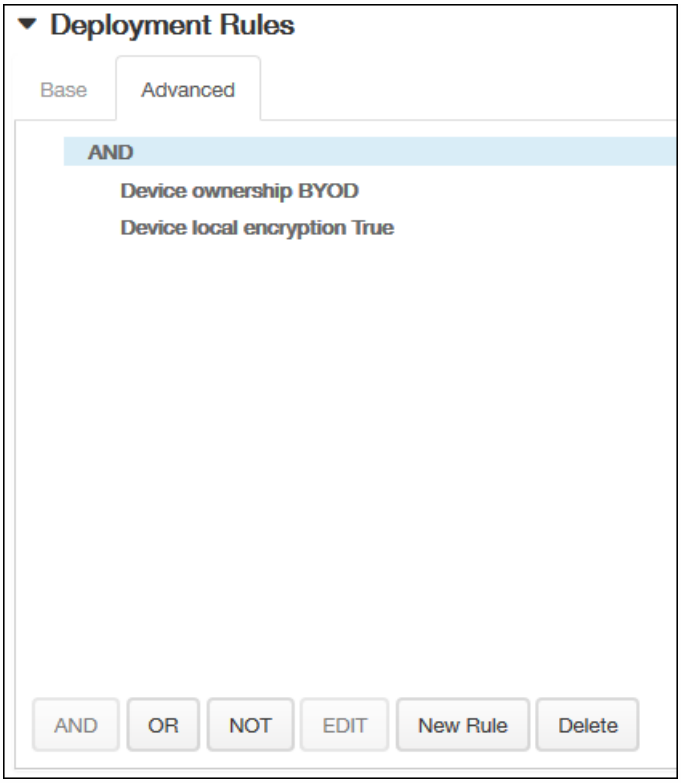


© 1999-2017 Citrix Systems, Inc. All rights reserved.

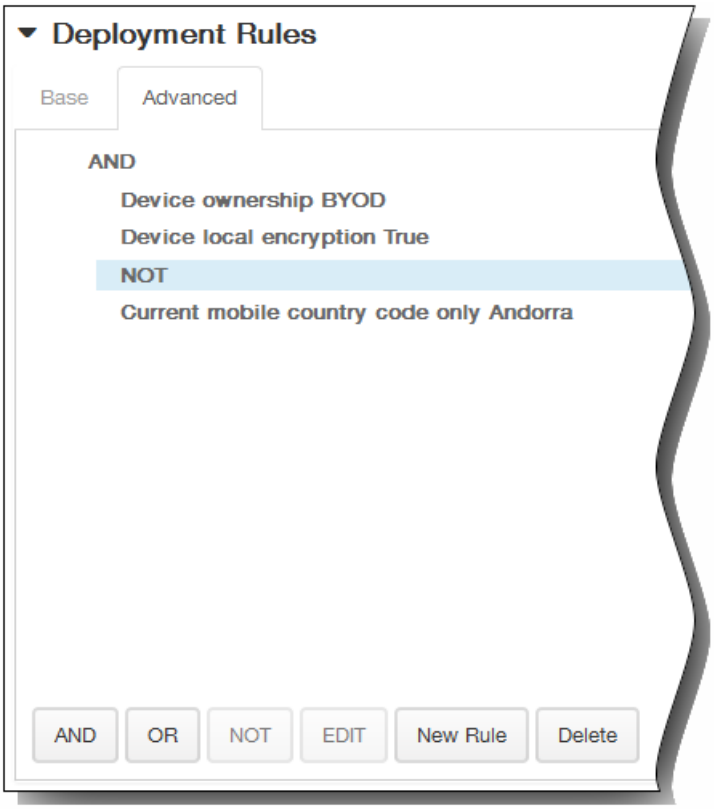


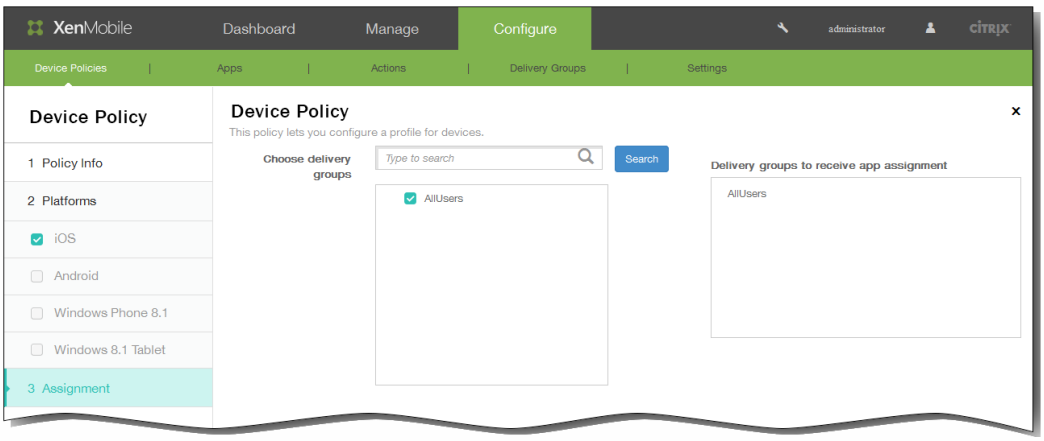


© 1999-2017 Citrix Systems, Inc. All rights reserved.

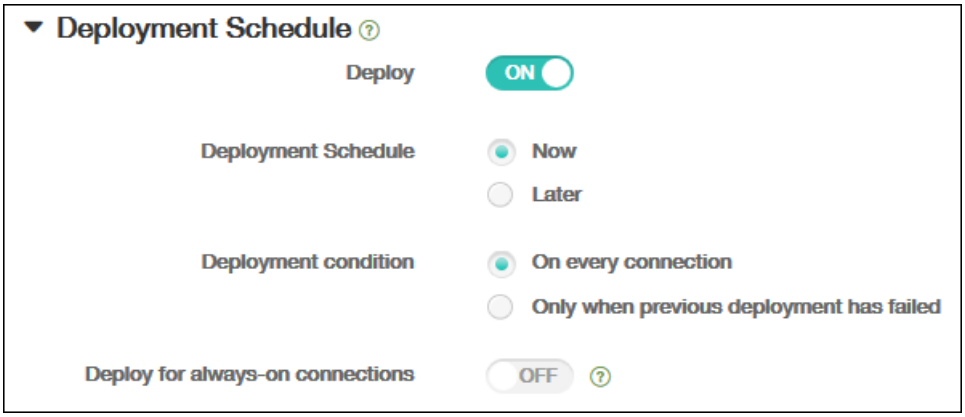


© 1999-2017 Citrix Systems, Inc. All rights reserved.

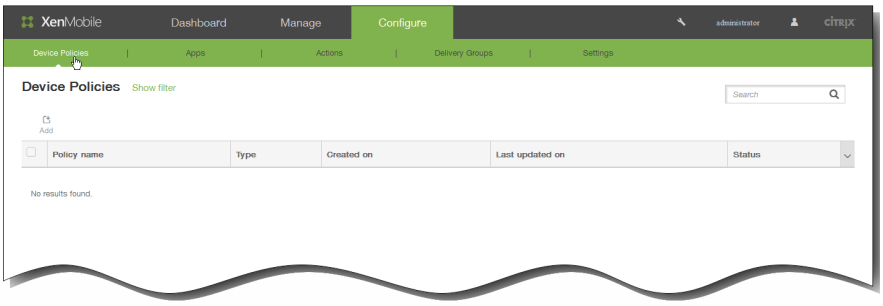


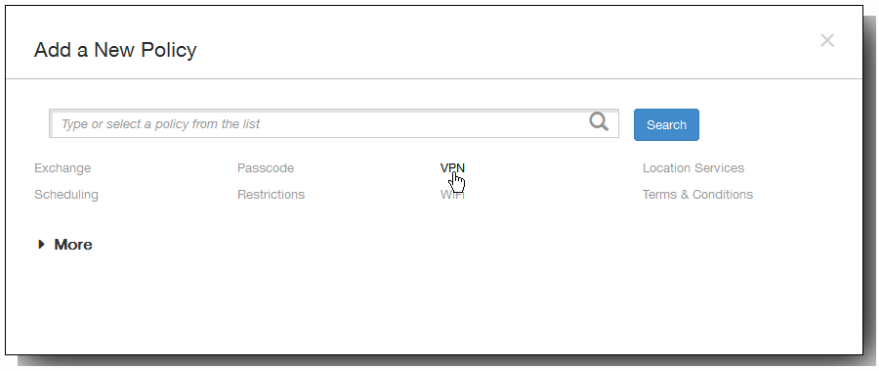


© 1999-2017 Citrix Systems, Inc. All rights reserved.

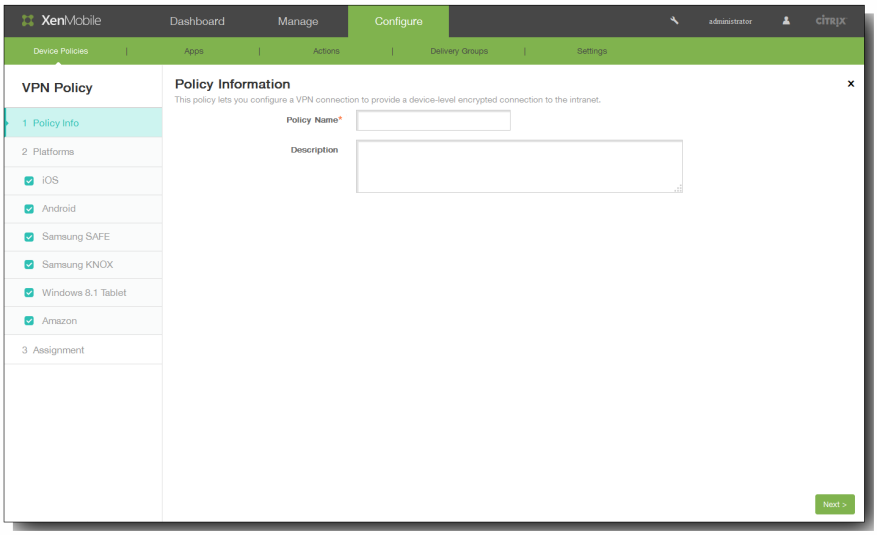


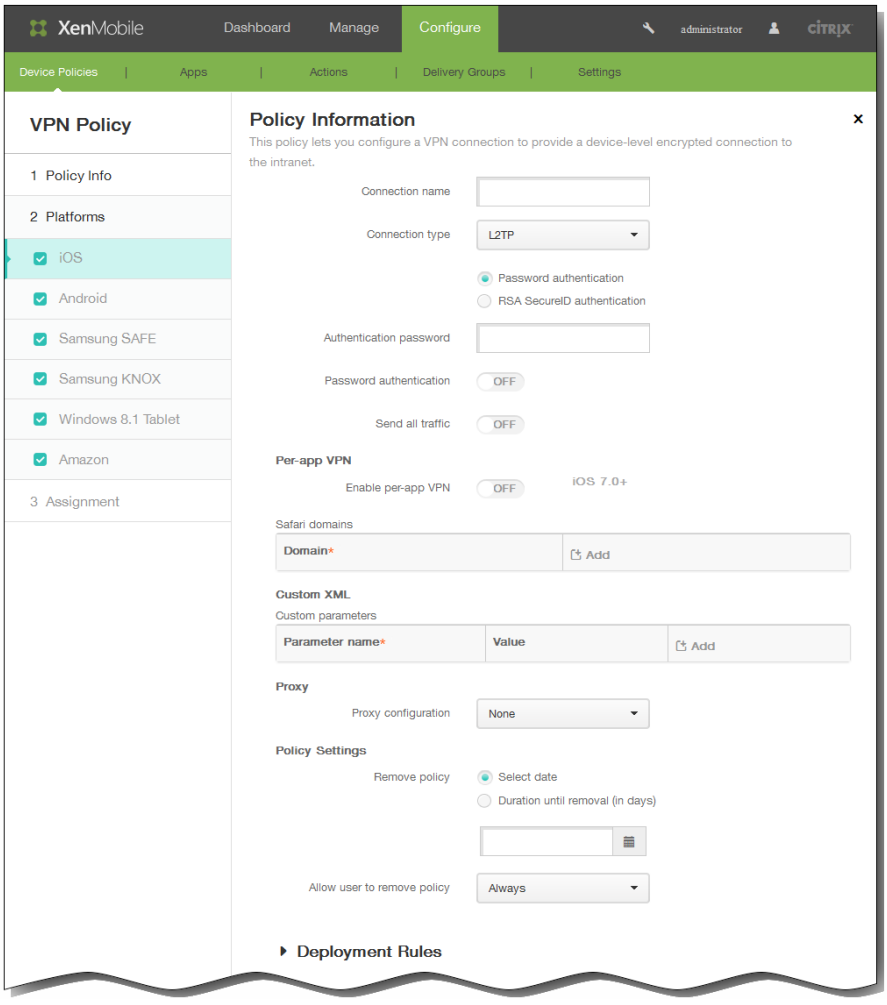
© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

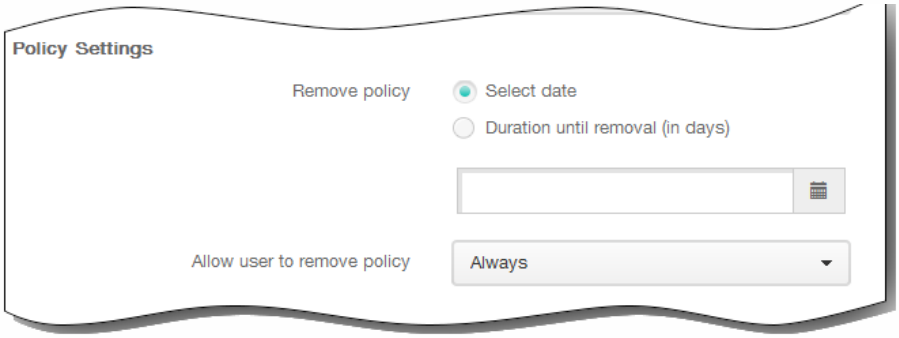
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

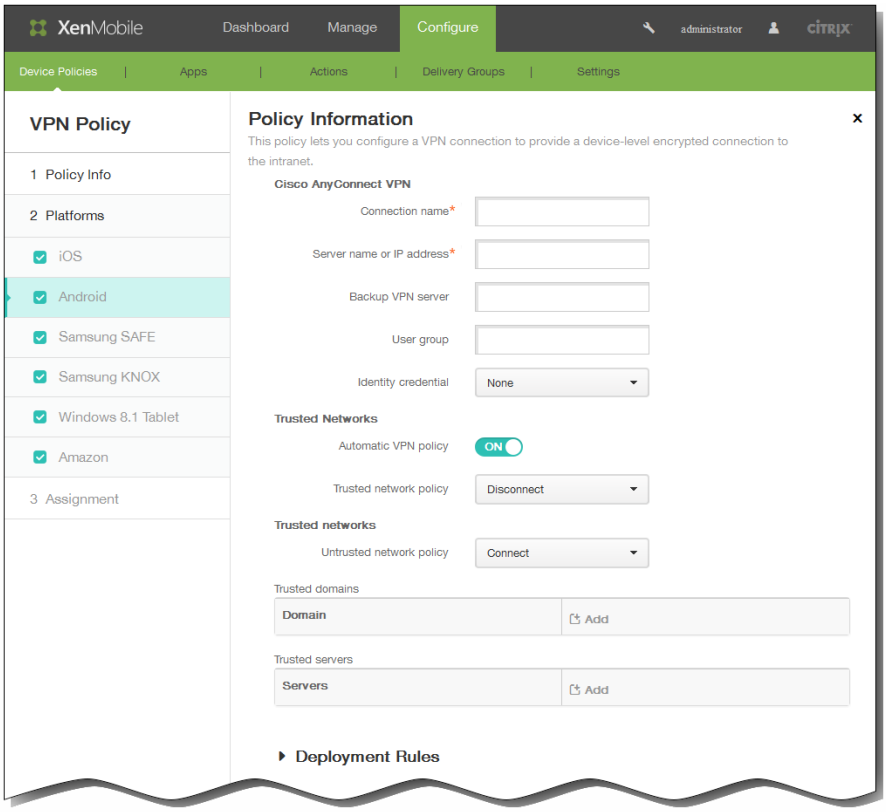
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

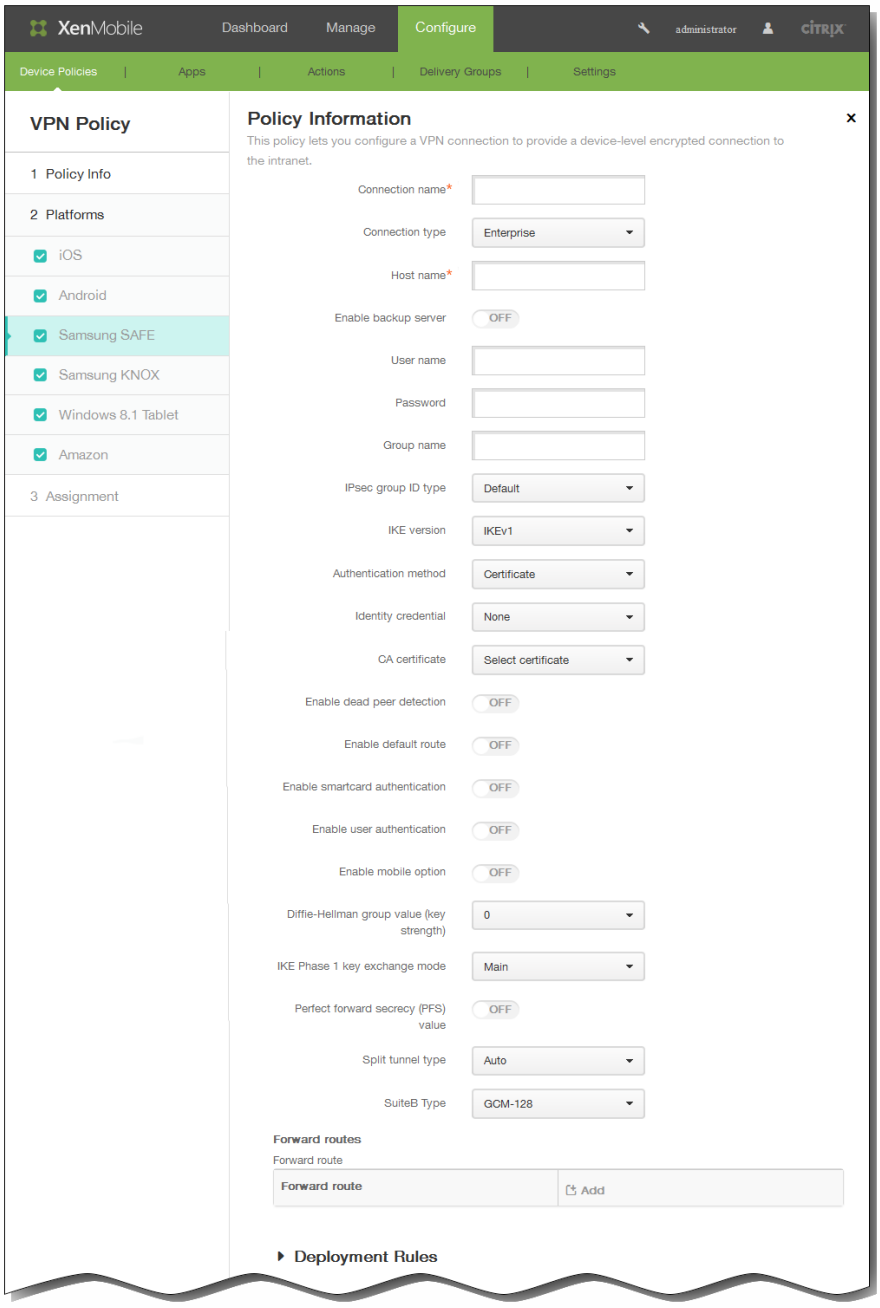


© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

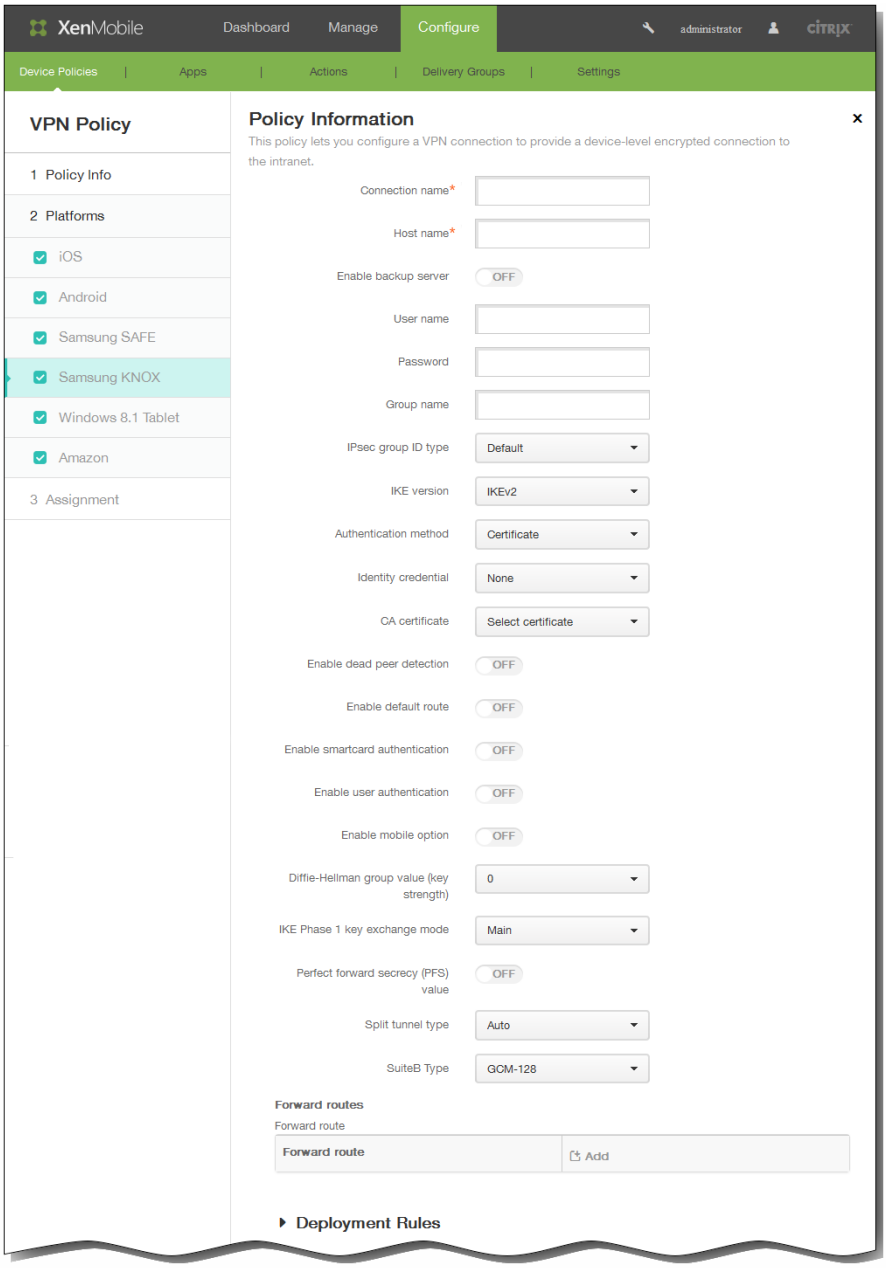


-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

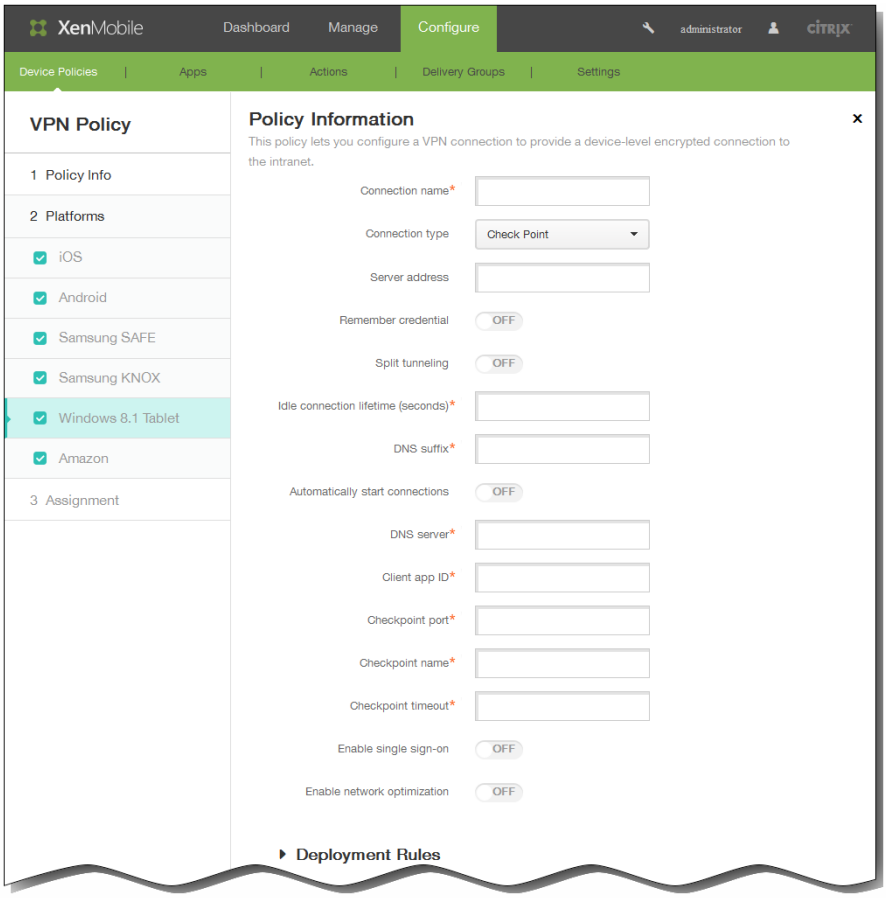
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

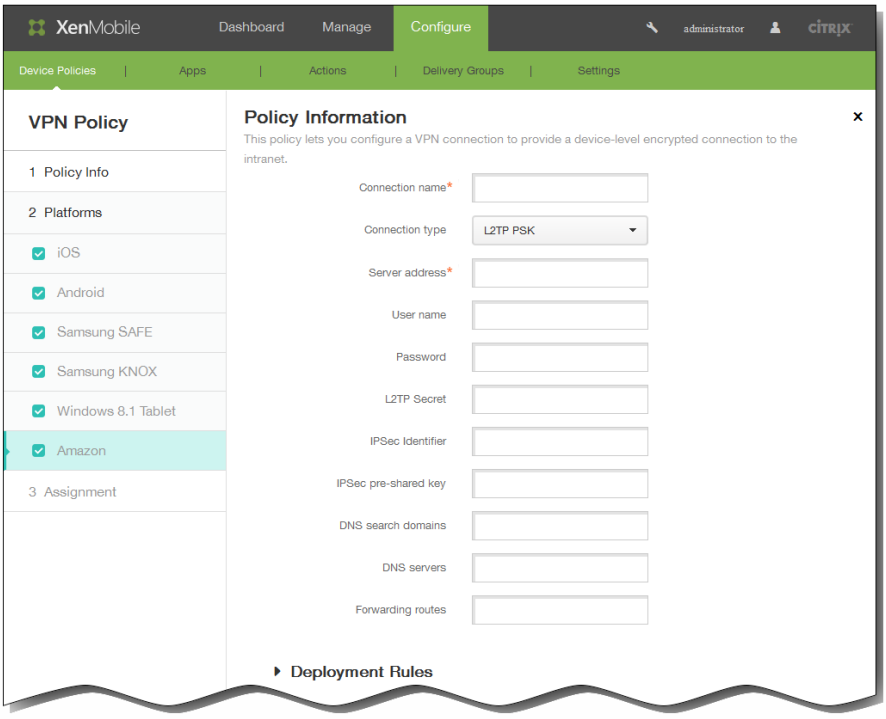
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-
-

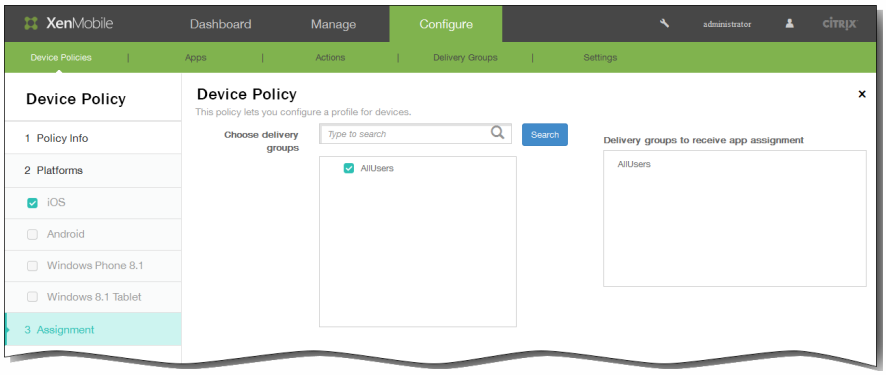
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

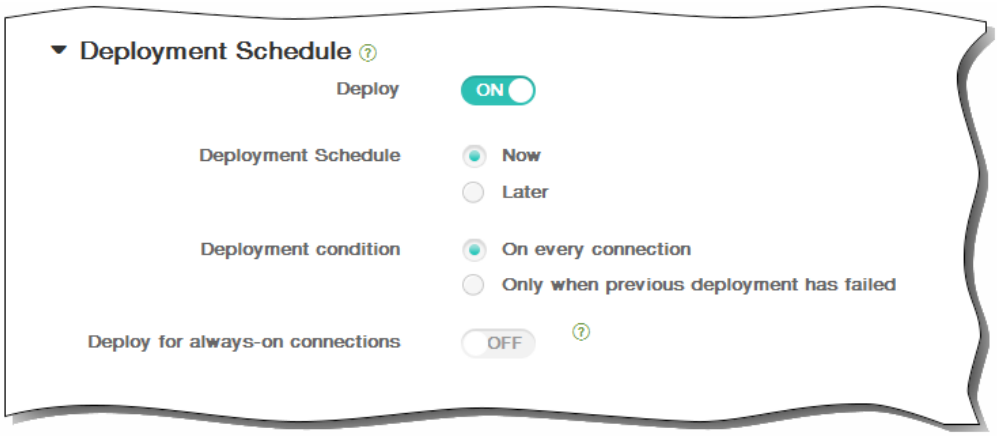


-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

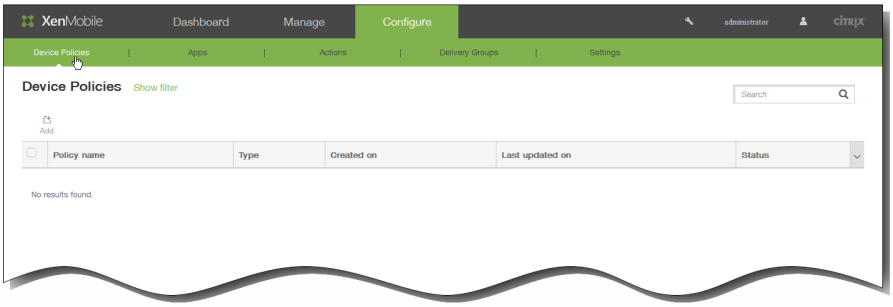


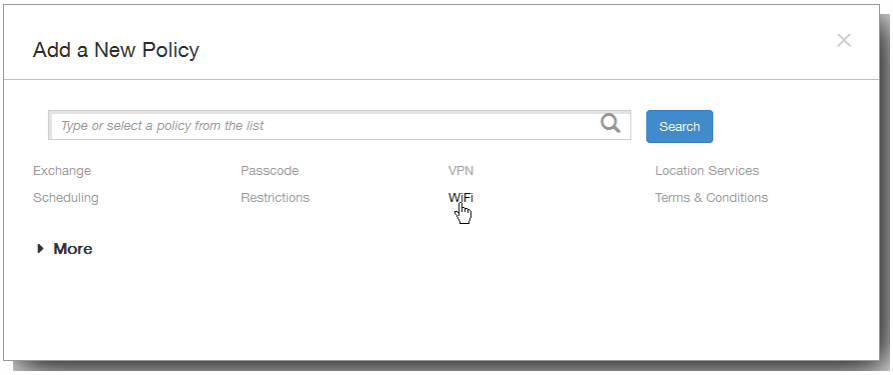
© 1999-2017 Citrix Systems, Inc. All rights reserved.



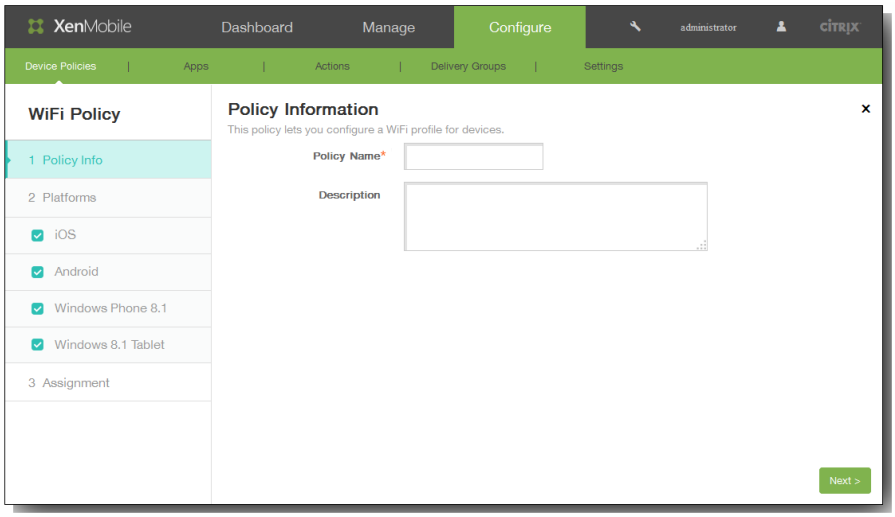
© 1999-2017 Citrix Systems, Inc. All rights reserved.

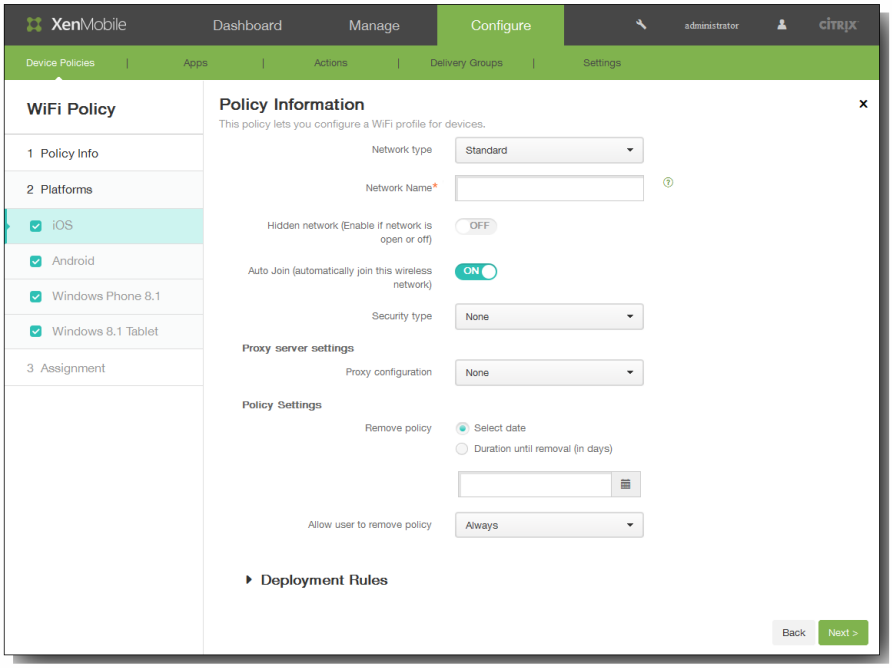
-
-
-
-
-
-





© 1999-2017 Citrix Systems, Inc. All rights reserved.



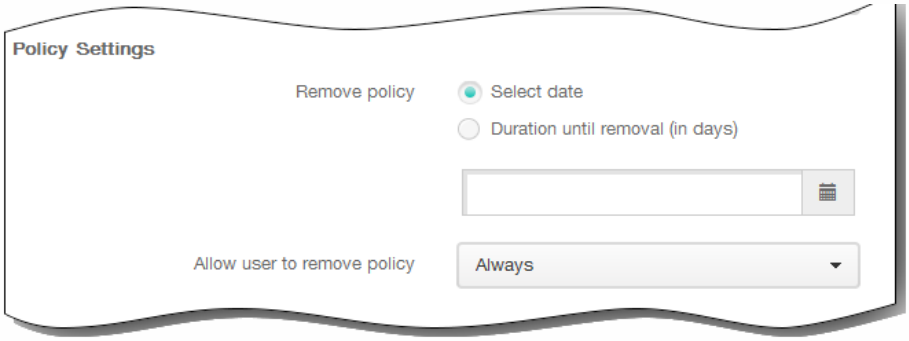


© 1999-2017 Citrix Systems, Inc. All rights reserved.

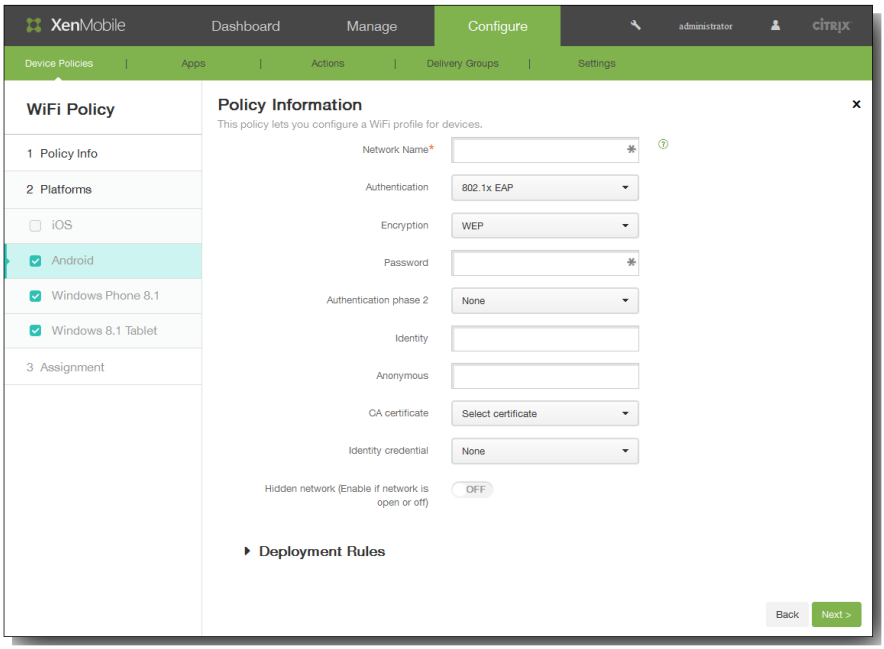
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

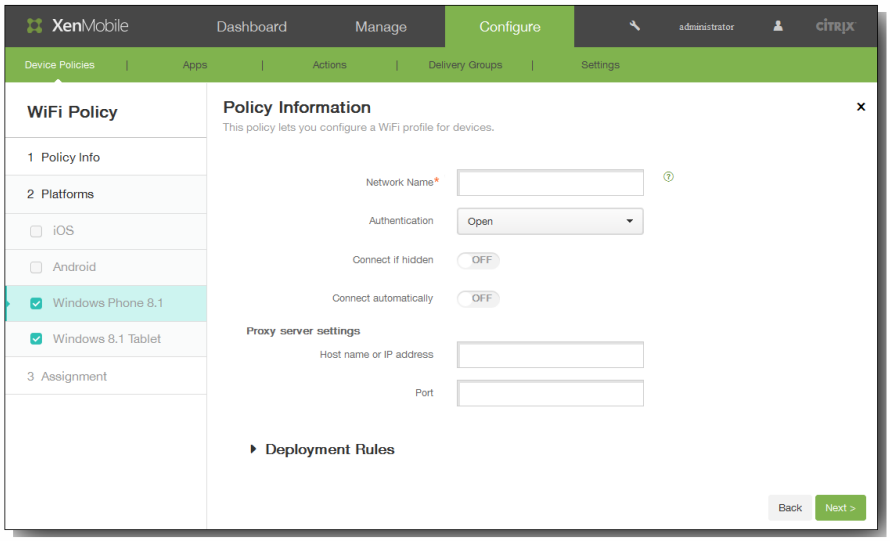


© 1999-2017 Citrix Systems, Inc. All rights reserved.



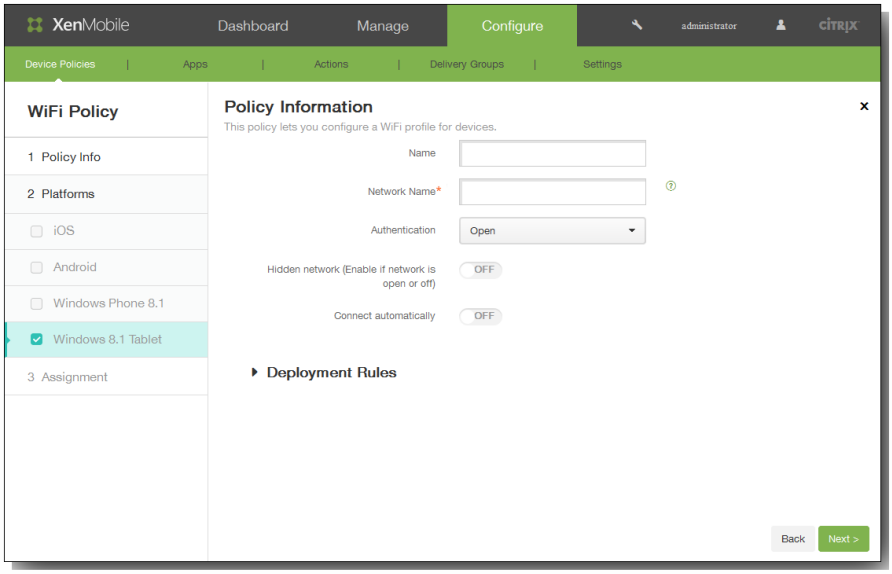
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

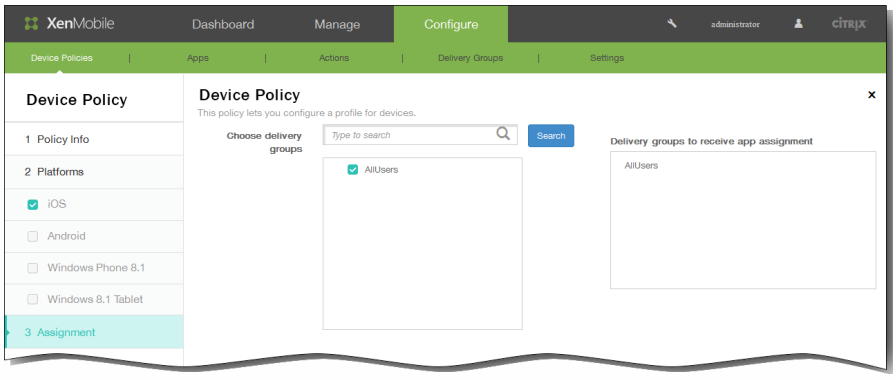


-
-
-
-

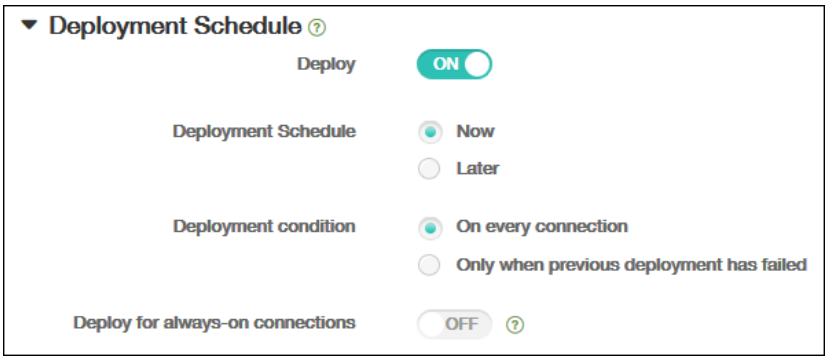
© 1999-2017 Citrix Systems, Inc. All rights reserved.



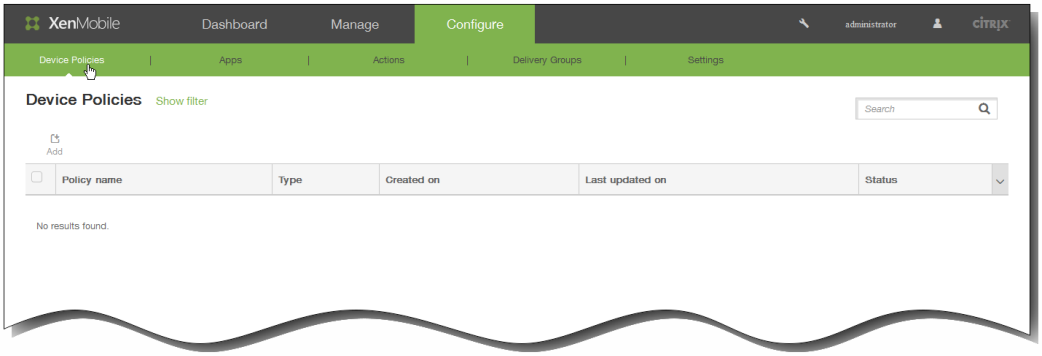
-
-
-
-
-

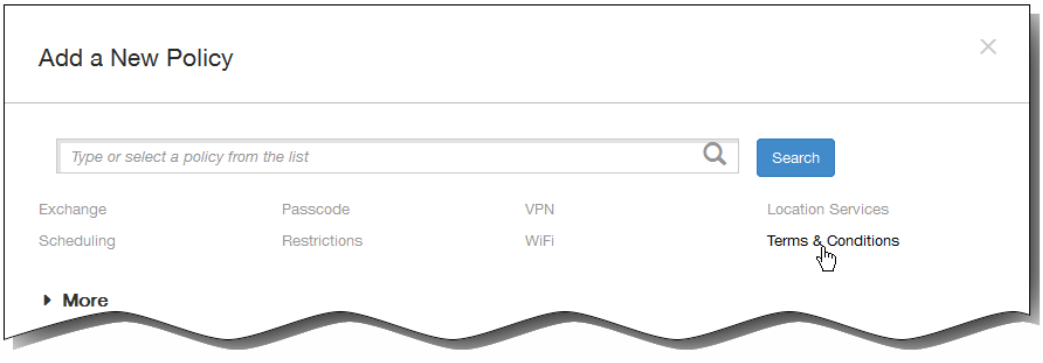


© 1999-2017 Citrix Systems, Inc. All rights reserved.

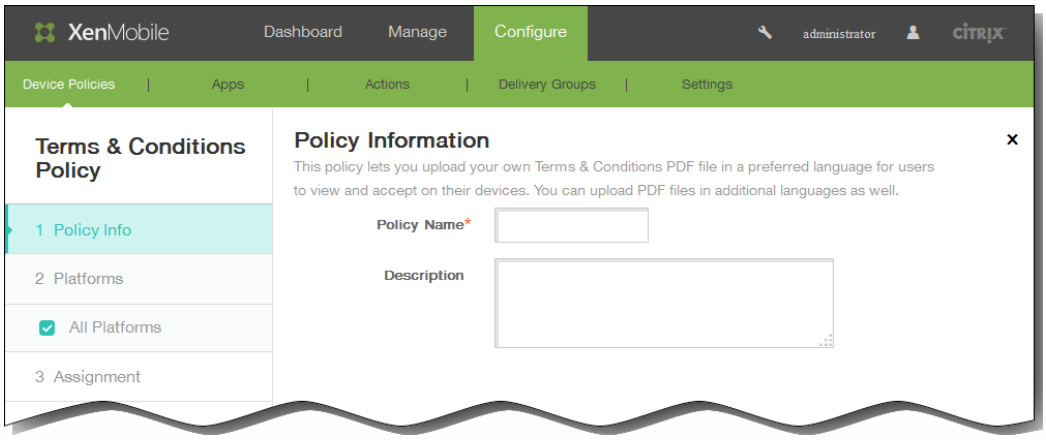


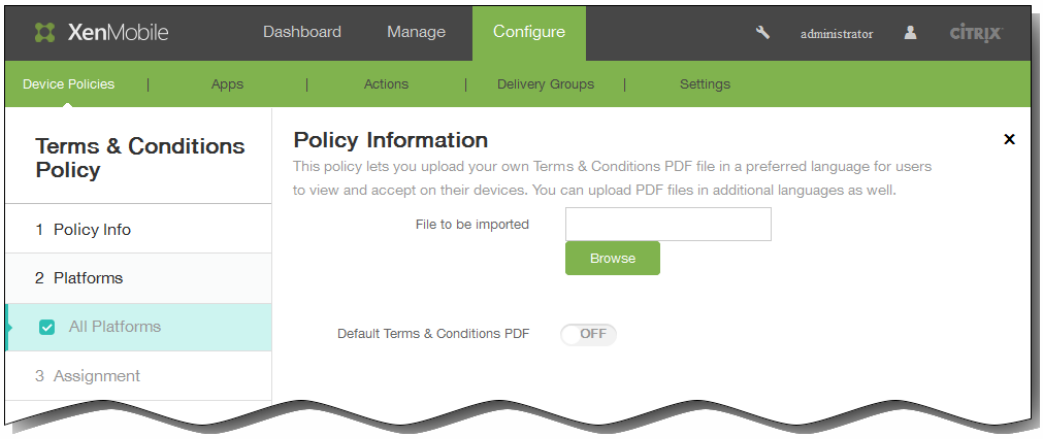
© 1999-2017 Citrix Systems, Inc. All rights reserved.





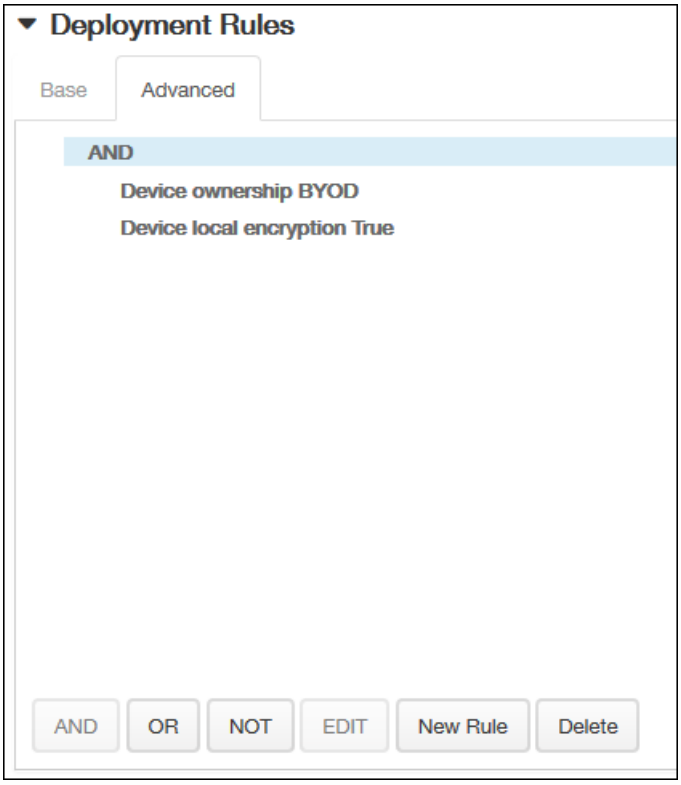
© 1999-2017 Citrix Systems, Inc. All rights reserved.



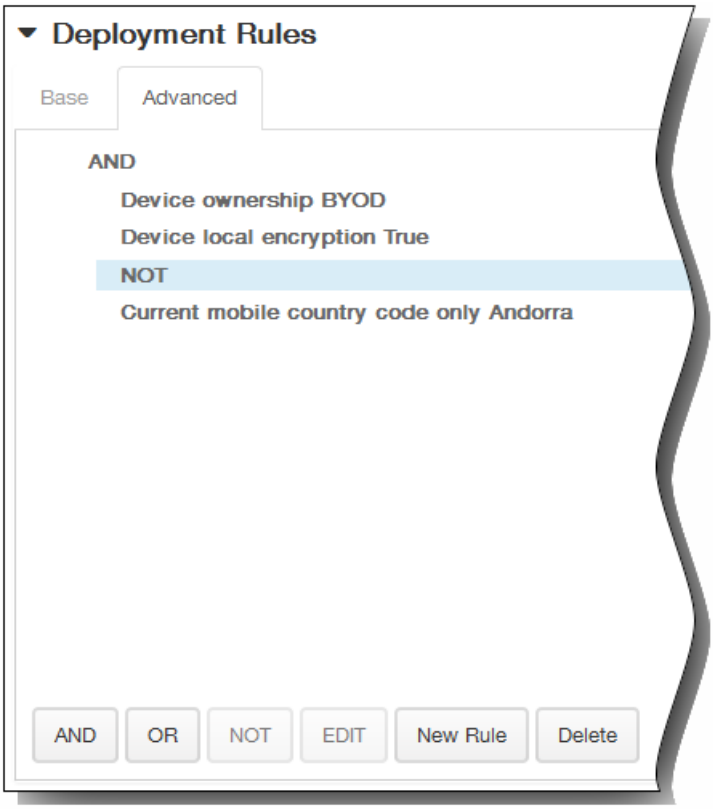


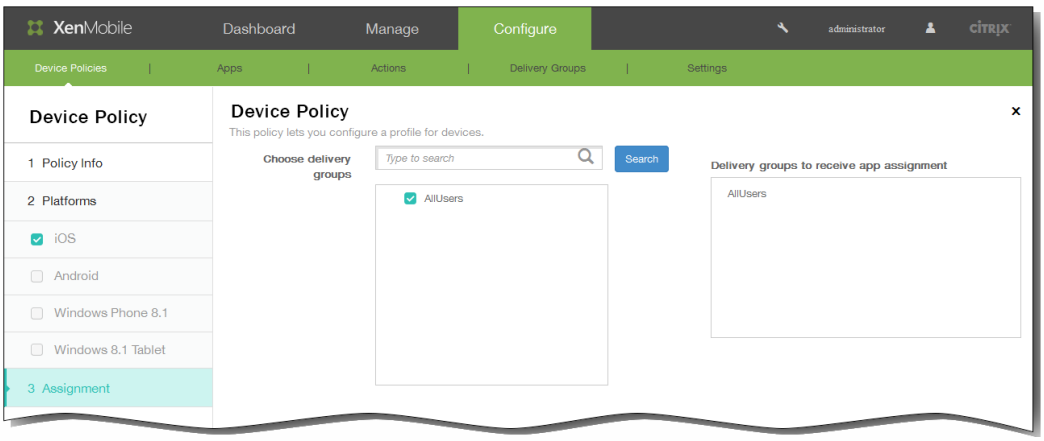


© 1999-2017 Citrix Systems, Inc. All rights reserved.

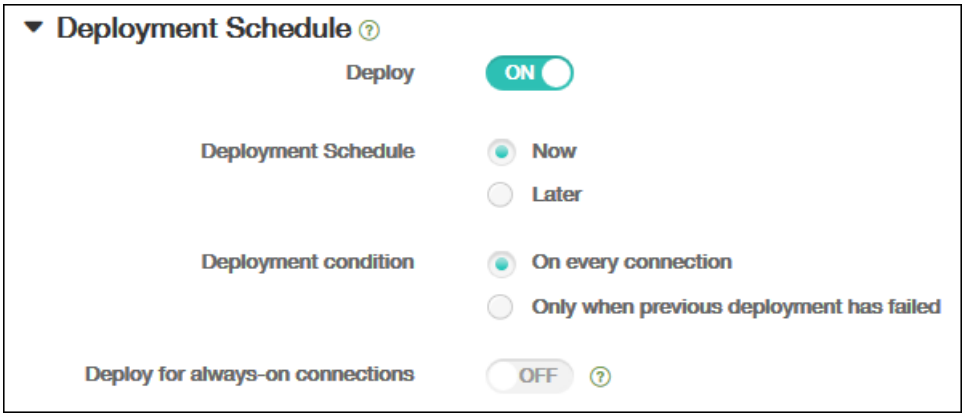


© 1999-2017 Citrix Systems, Inc. All rights reserved.

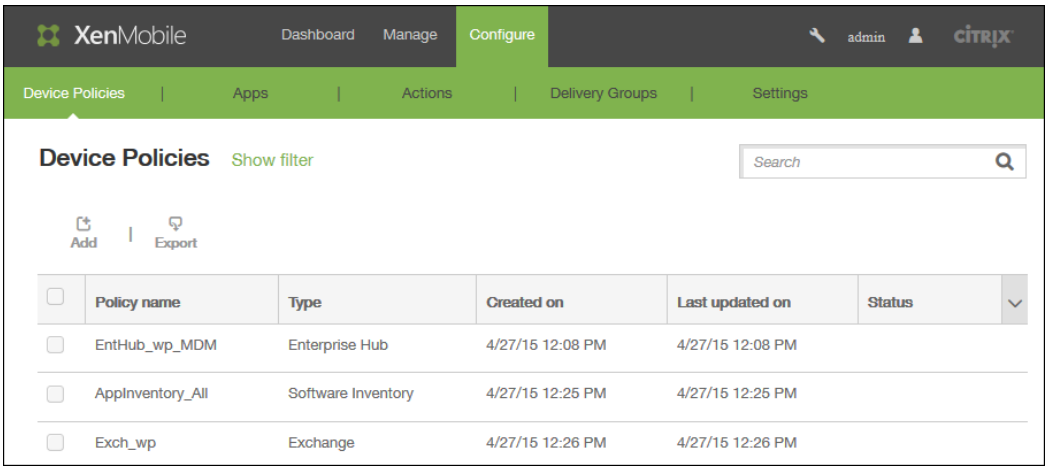




© 1999-2017 Citrix Systems, Inc. All rights reserved.

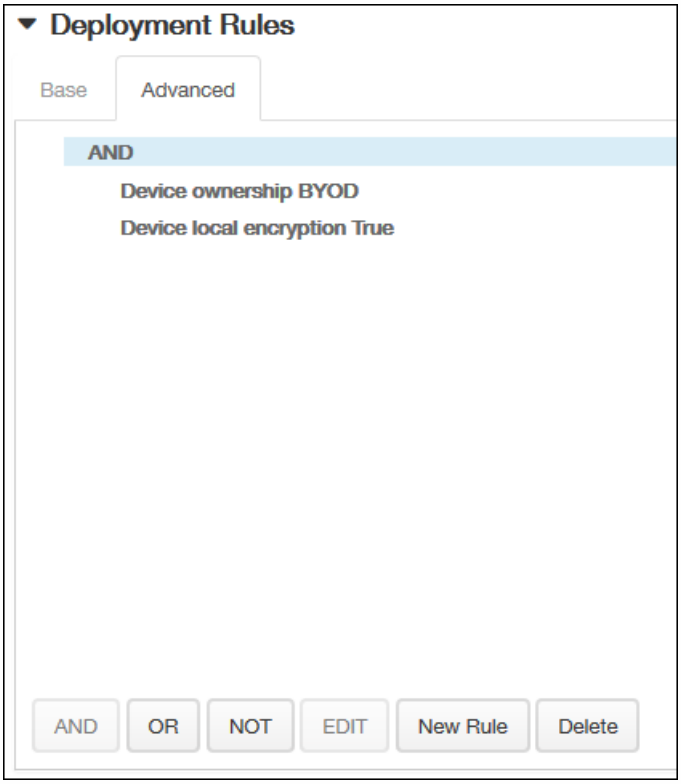


© 1999-2017 Citrix Systems, Inc. All rights reserved.

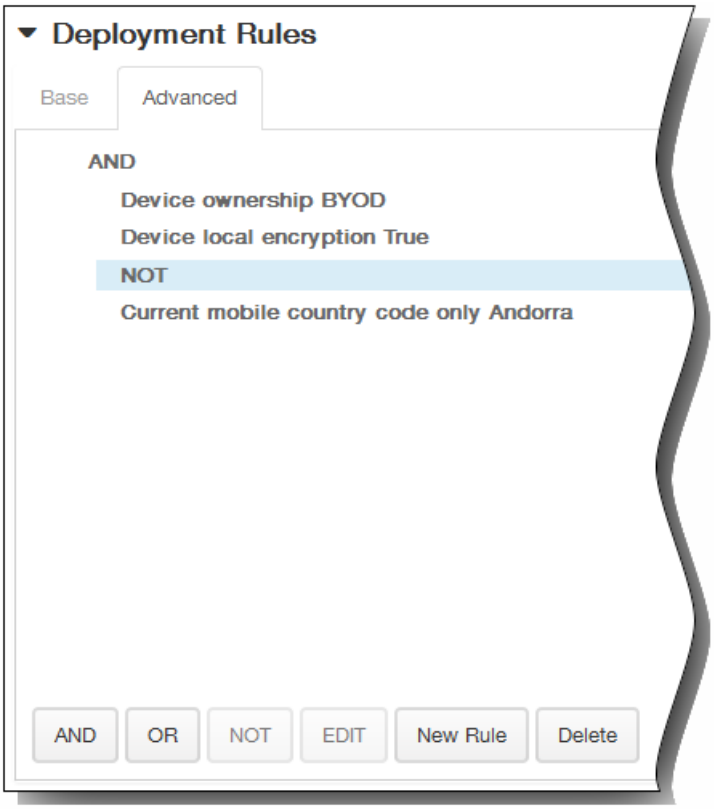


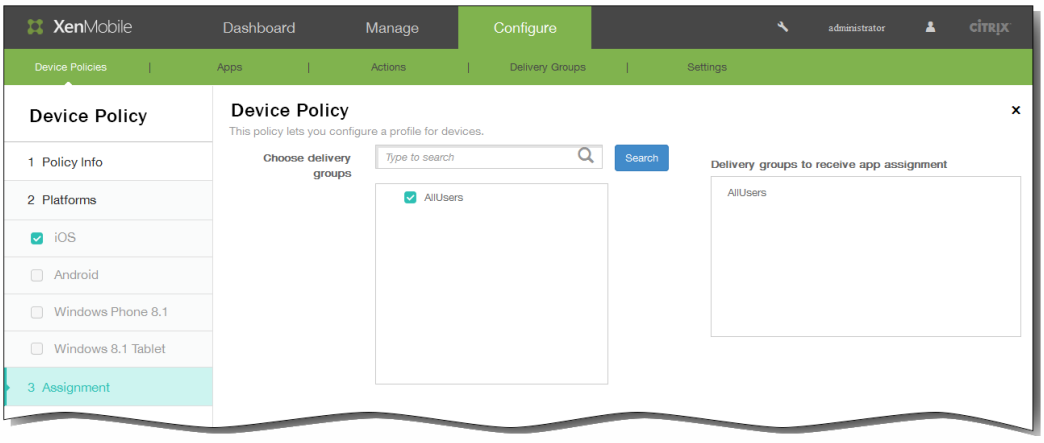


© 1999-2017 Citrix Systems, Inc. All rights reserved.

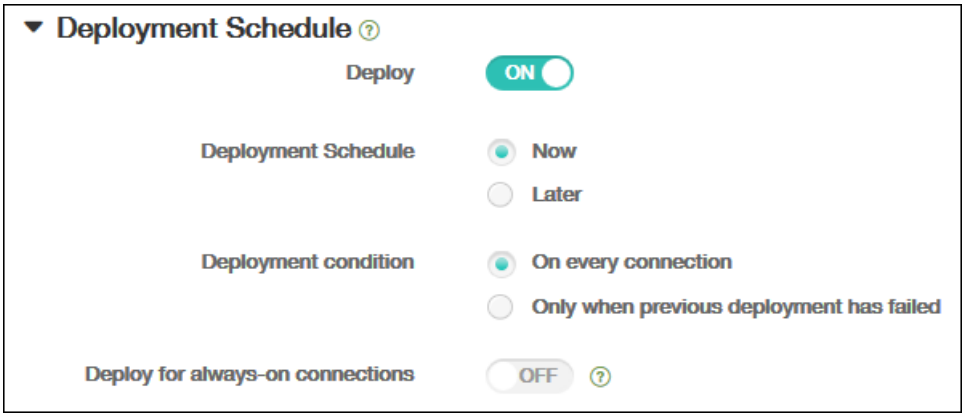


© 1999-2017 Citrix Systems, Inc. All rights reserved.

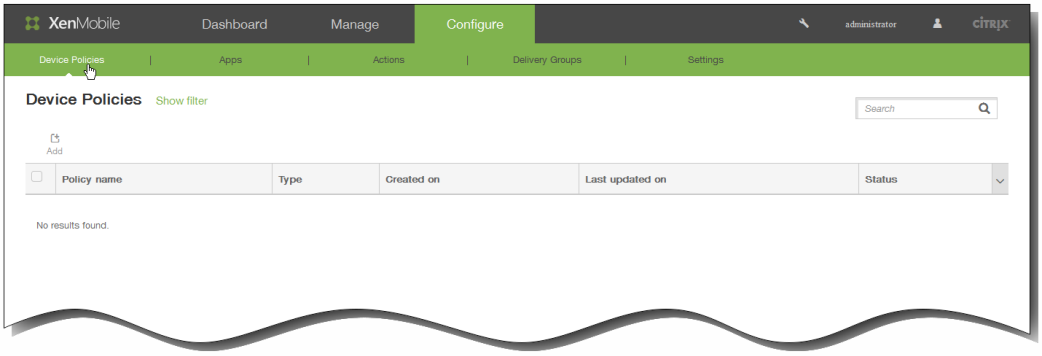


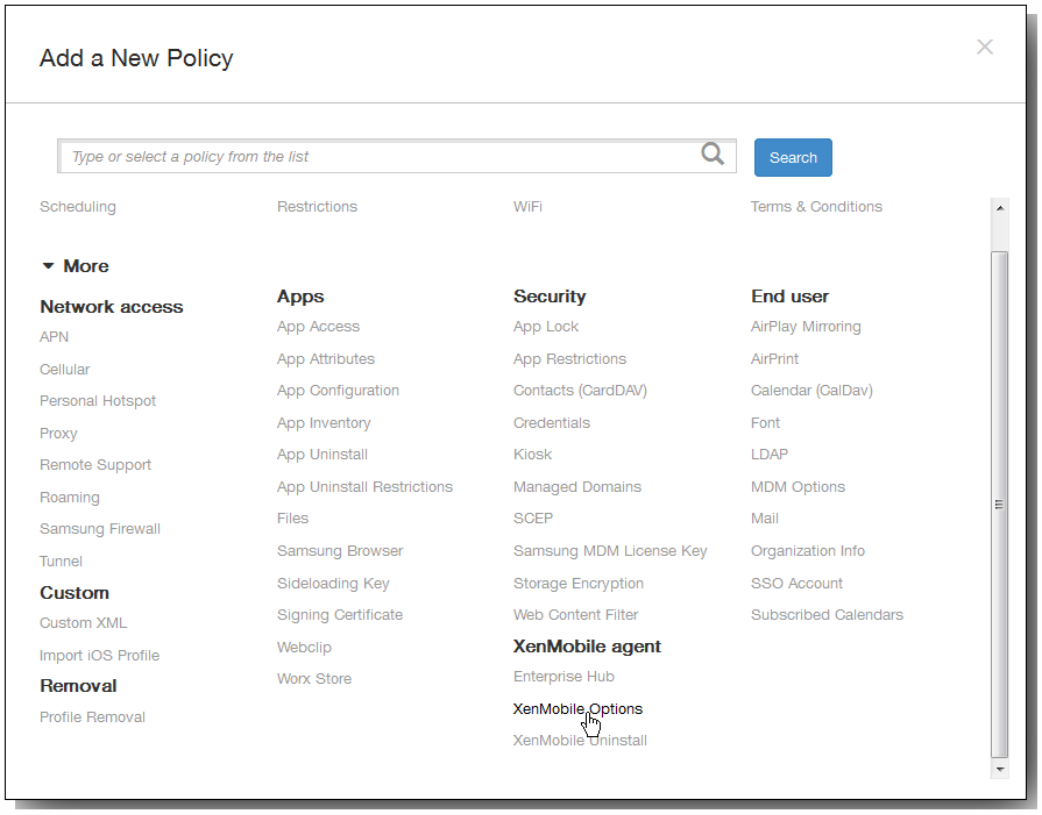


© 1999-2017 Citrix Systems, Inc. All rights reserved.

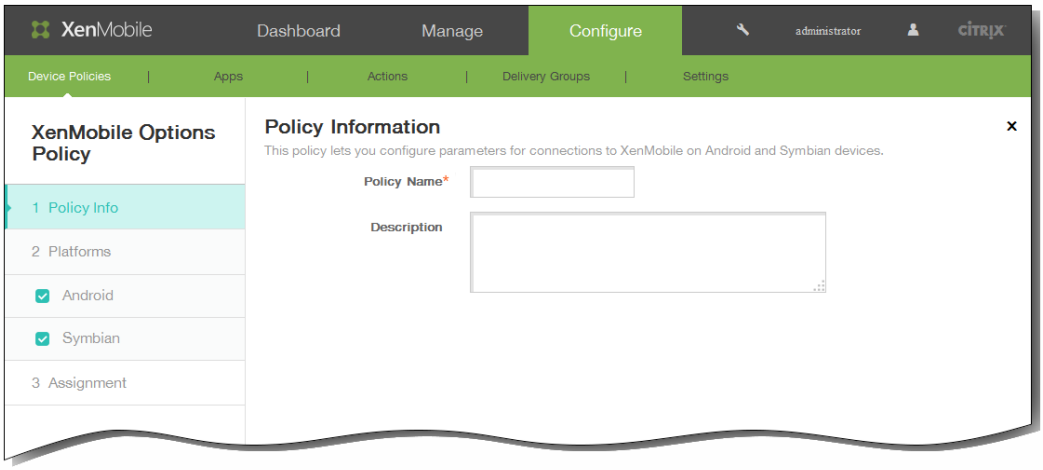


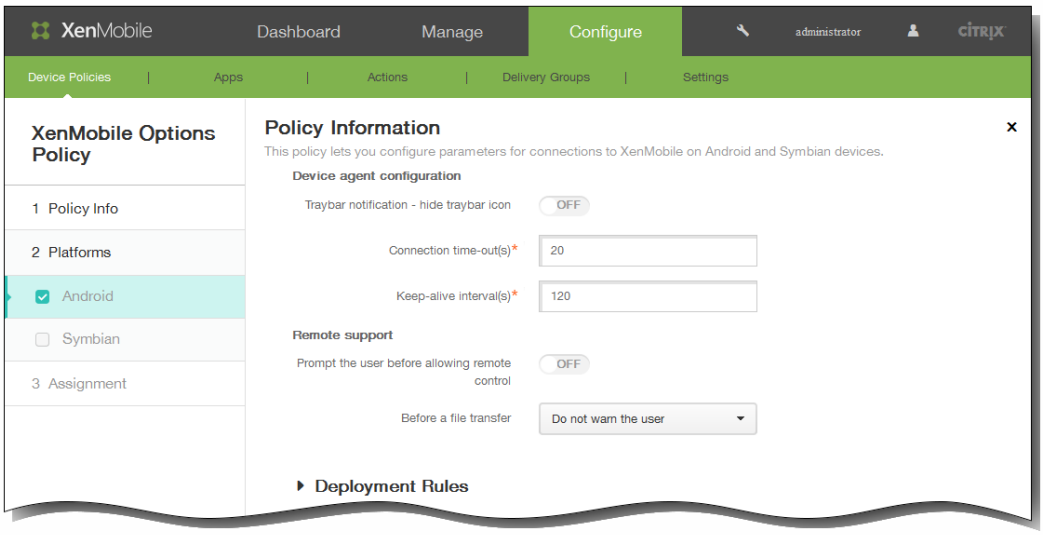
© 1999-2017 Citrix Systems, Inc. All rights reserved.



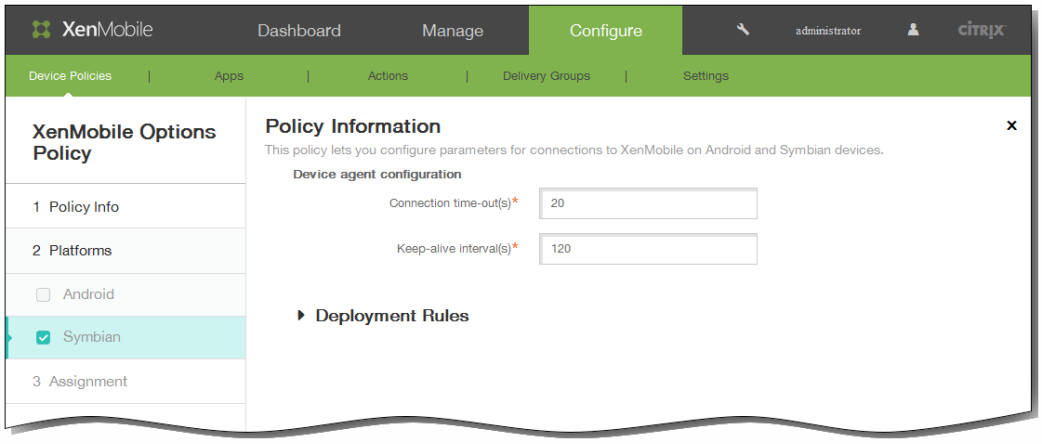


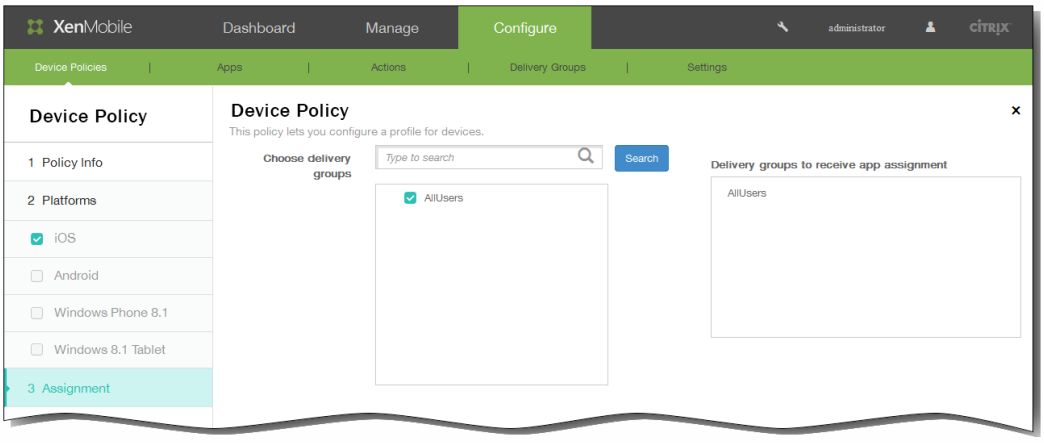
© 1999-2017 Citrix Systems, Inc. All rights reserved.



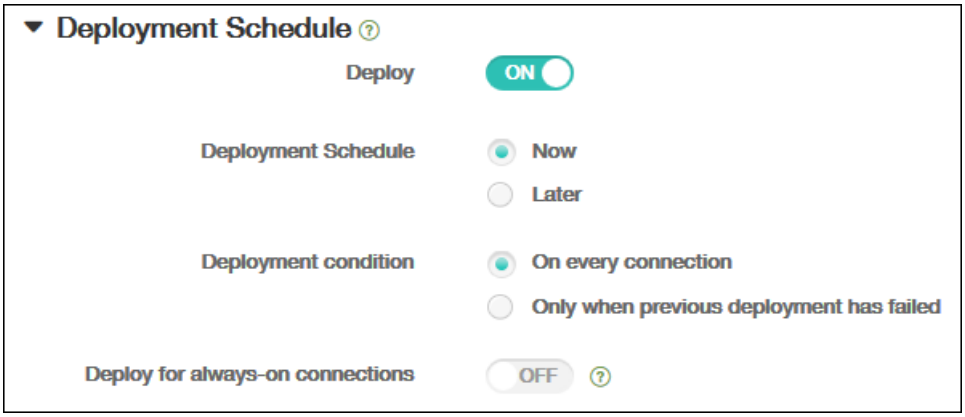


© 1999-2017 Citrix Systems, Inc. All rights reserved.

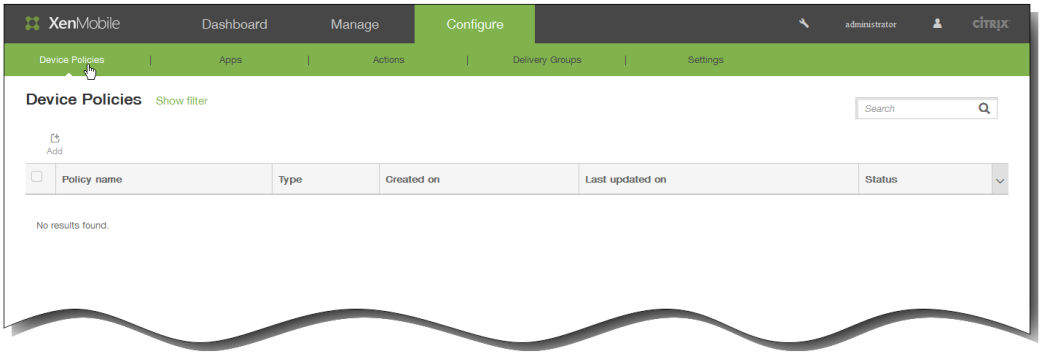


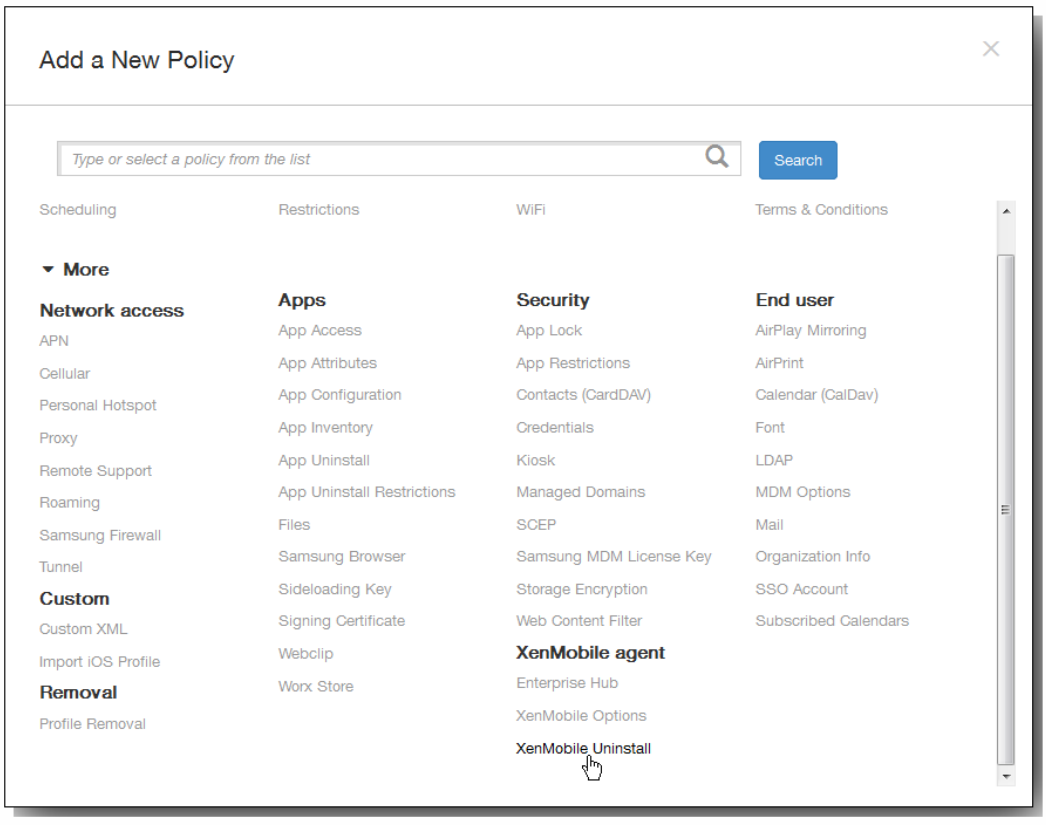


© 1999-2017 Citrix Systems, Inc. All rights reserved.

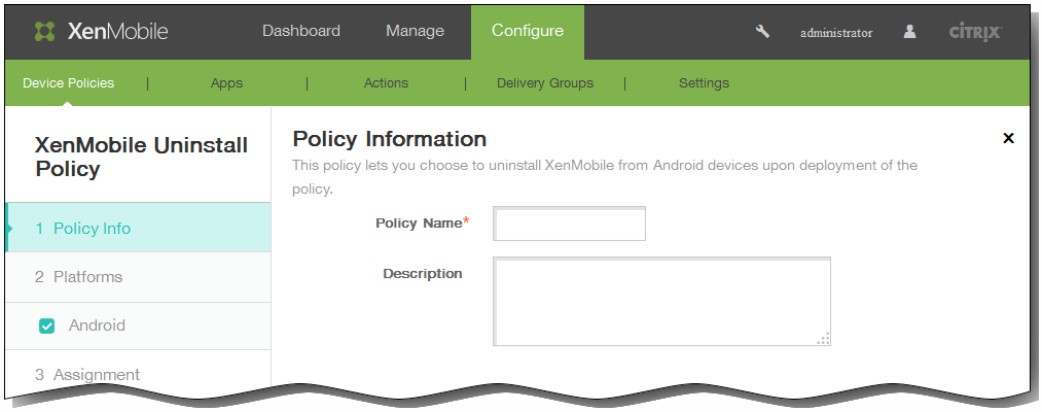


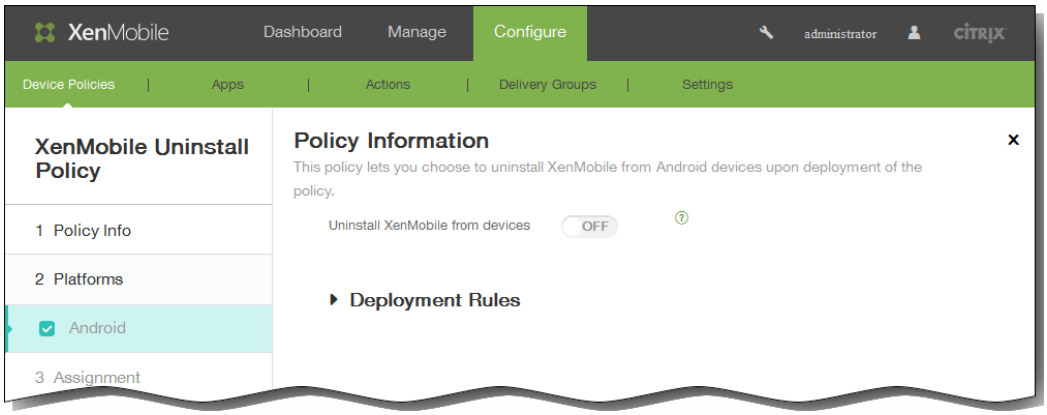
© 1999-2017 Citrix Systems, Inc. All rights reserved.





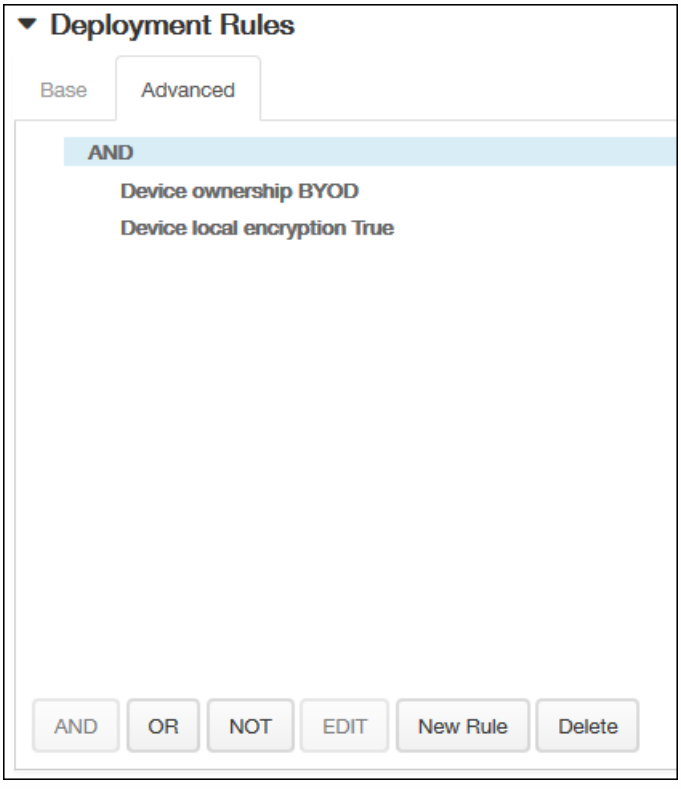
© 1999-2017 Citrix Systems, Inc. All rights reserved.



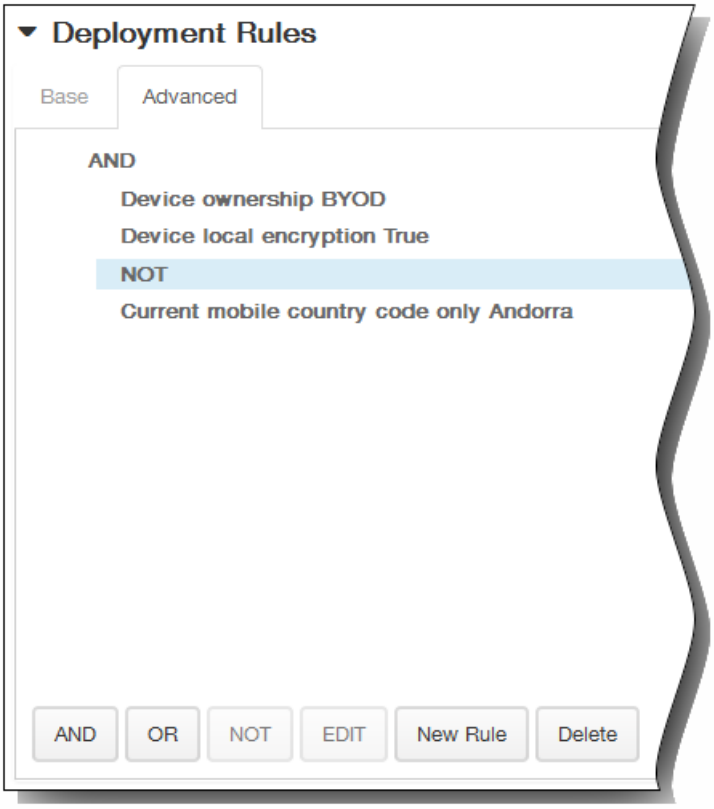


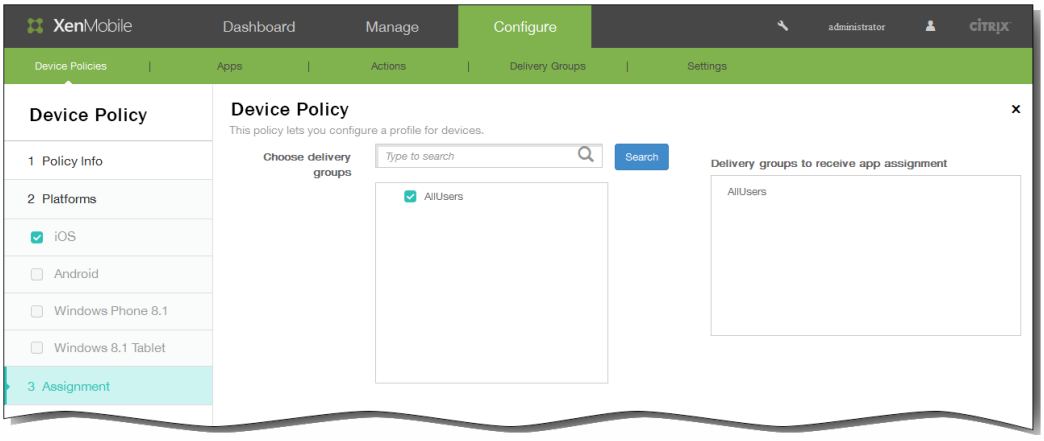
© 1999-2017 Citrix Systems, Inc. All rights reserved.



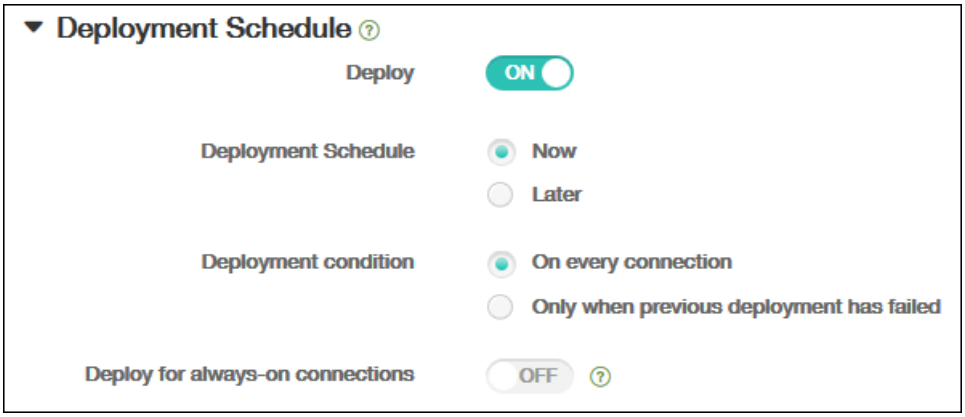


© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.



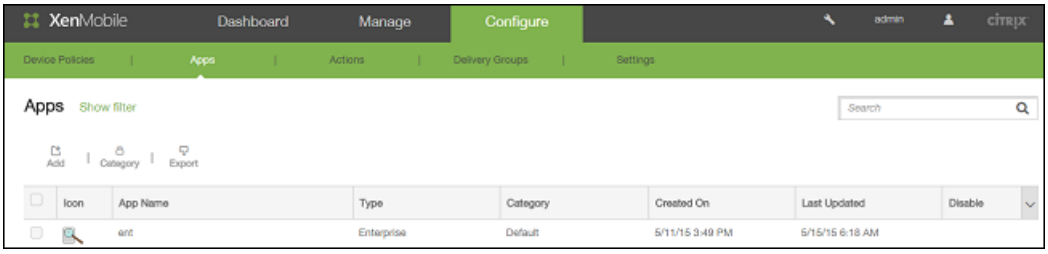
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-



-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

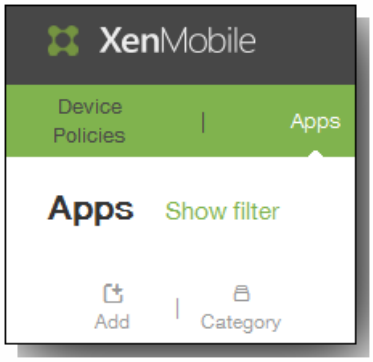
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une application MDX à XenMobile

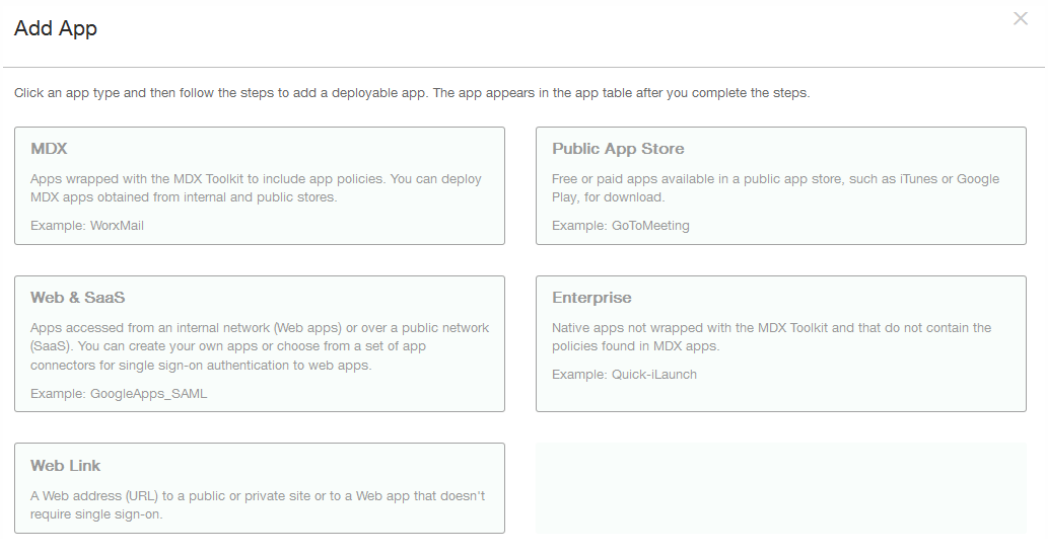
Jul 25, 2016

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 de plus amples informations sur les stratégies applicatives disponibles pour chaque type de plate-forme, consultez la section Synopsis des stratégies MDX pour iOS, Android, et Windows Phone. 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 Ajouter.

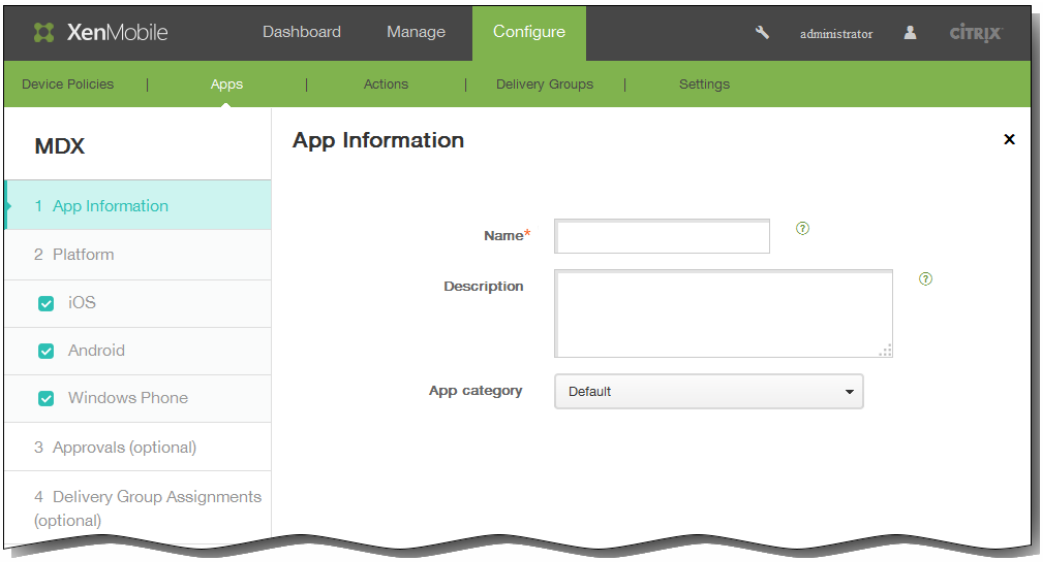


3. Dans l'écran Ajouter une application, cliquez sur MDX.

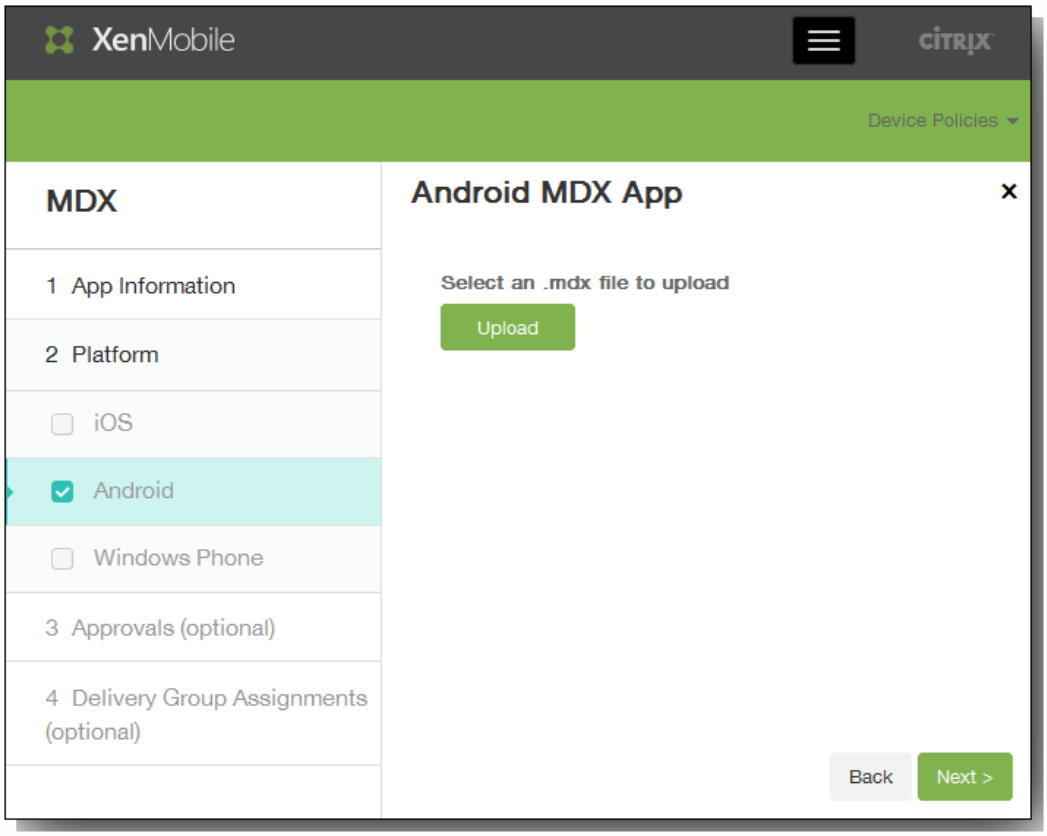


4. Sur la page Informations sur l'application, entrez un nom et une description facultative pour l'application. Ces champs sont utilisés à des fins internes. Si vous ajoutez des applications à de multiples appareils, utilisez les cases à cocher dans la partie gauche de l'écran pour les sélectionner.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

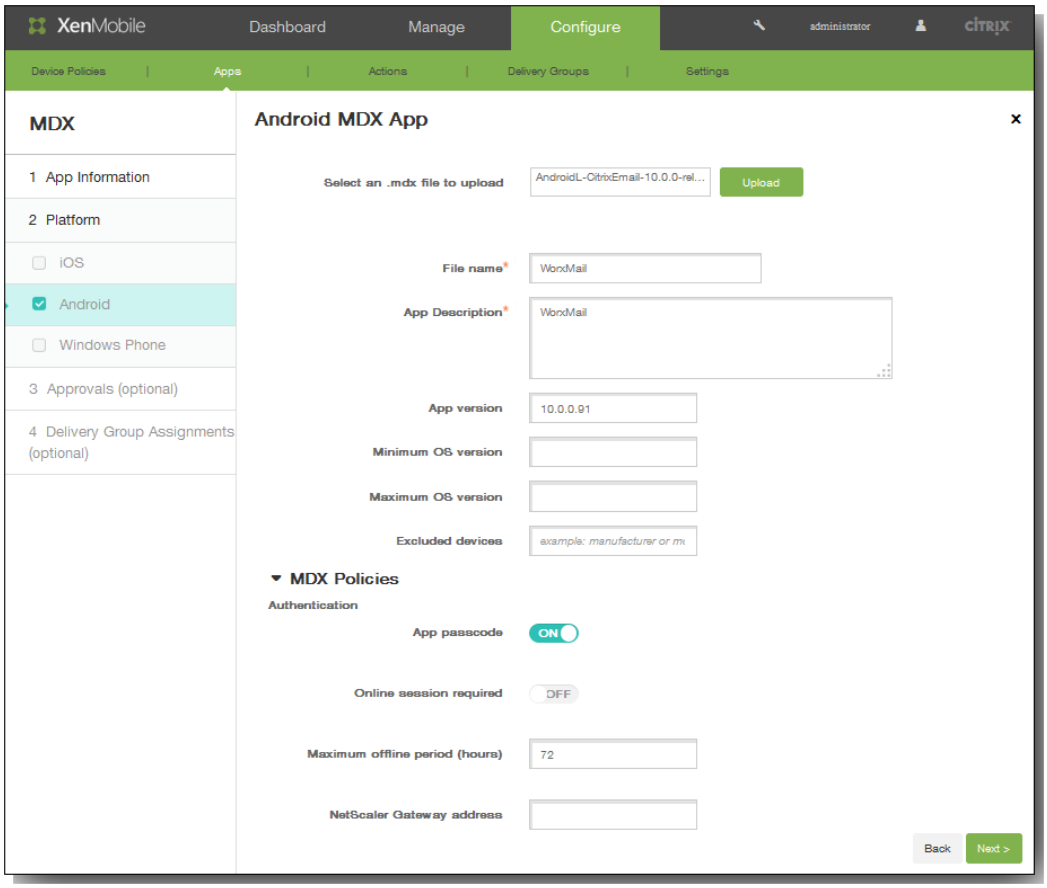


5. Dans la liste Catégorie d'application, cliquez sur Catégorie d'application. Consultez la section Ajout d'une catégorie pour plus d'informations.
6. Cliquez sur Suivant.
7. Cliquez sur Charger pour sélectionner un fichier .mdx à charger, puis cliquez sur Suivant.

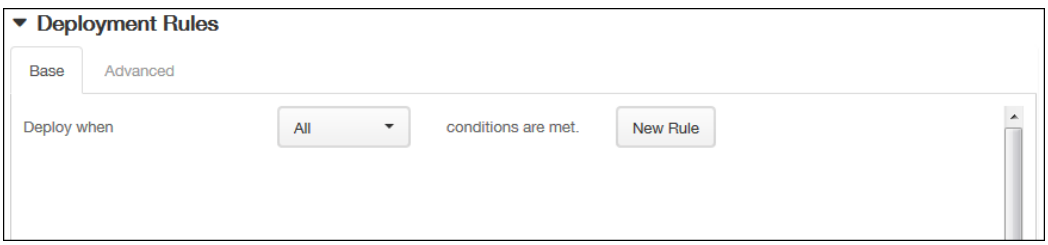


Les champs de détails sur l'application et de stratégies MDX apparaissent.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

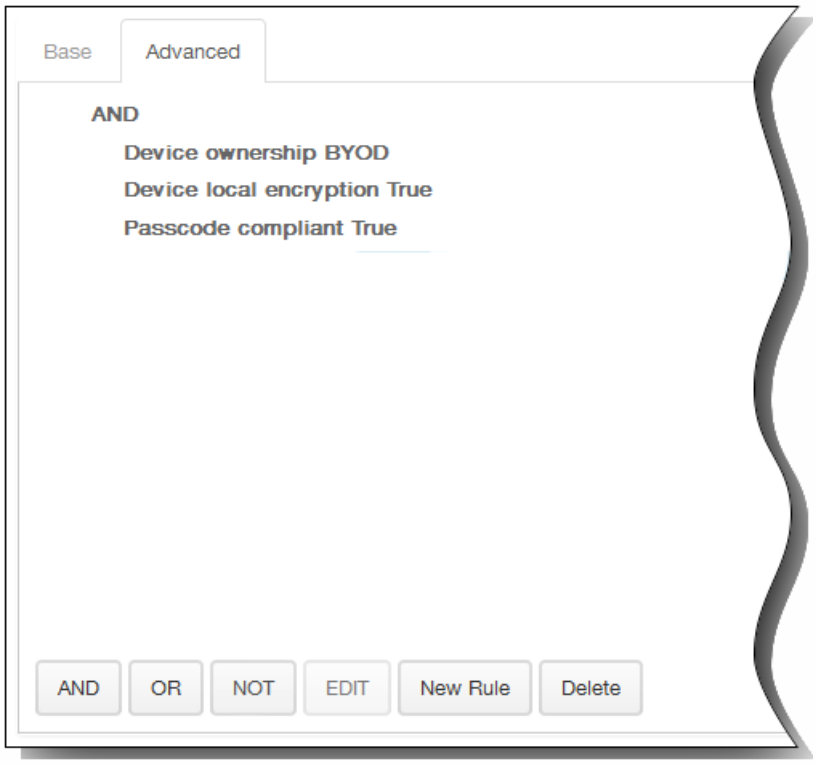


8. Configurez les paramètres suivants :
   1. Nom du fichier : entrez le nom du fichier associé à l'application.
   2. Description de l'application : entrez une description pour l'application.
   3. Version d'OS minimum : entrez la version la plus ancienne du système d'exploitation que l'appareil peut exécuter pour pouvoir utiliser l'application.
   4. Version d'OS maximum : entrez la version la plus récente du système d'exploitation que l'appareil doit exécuter pour pouvoir utiliser l'application.
   5. Appareils exclus : entrez le fabricant ou modèles d'appareils qui ne peuvent pas exécuter l'application.
9. Dans Stratégies MDX, configurez les paramètres de stratégie que le Worx Store applique en matière d'authentification, de sécurité sur l'appareil, d'exigences de réseau et d'accès, de cryptage, d'interaction avec l'application, de restrictions applicatives et plus.
   Remarque : dans la console, placez le curseur sur le nom de la stratégie pour en afficher une description. 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 pour iOS, Android et Windows Phone.
10. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

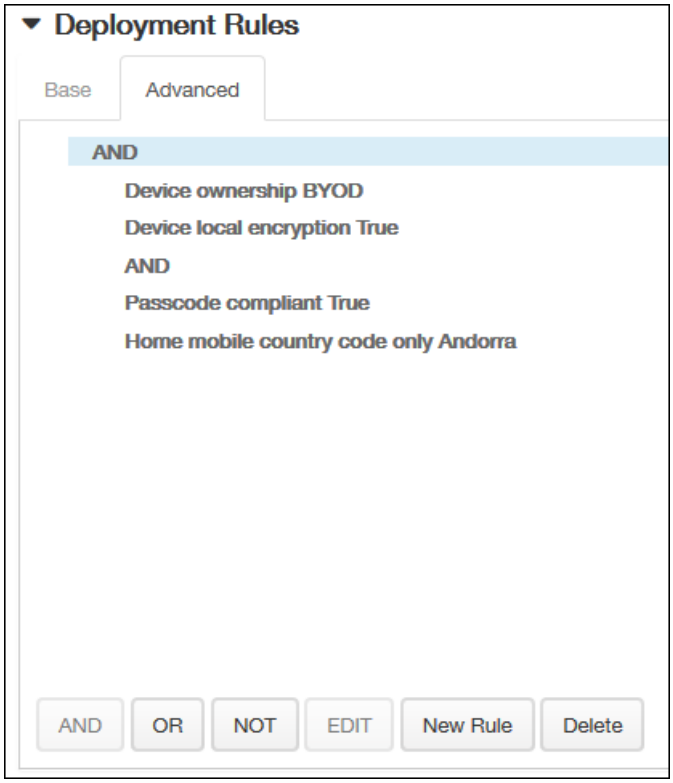
1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



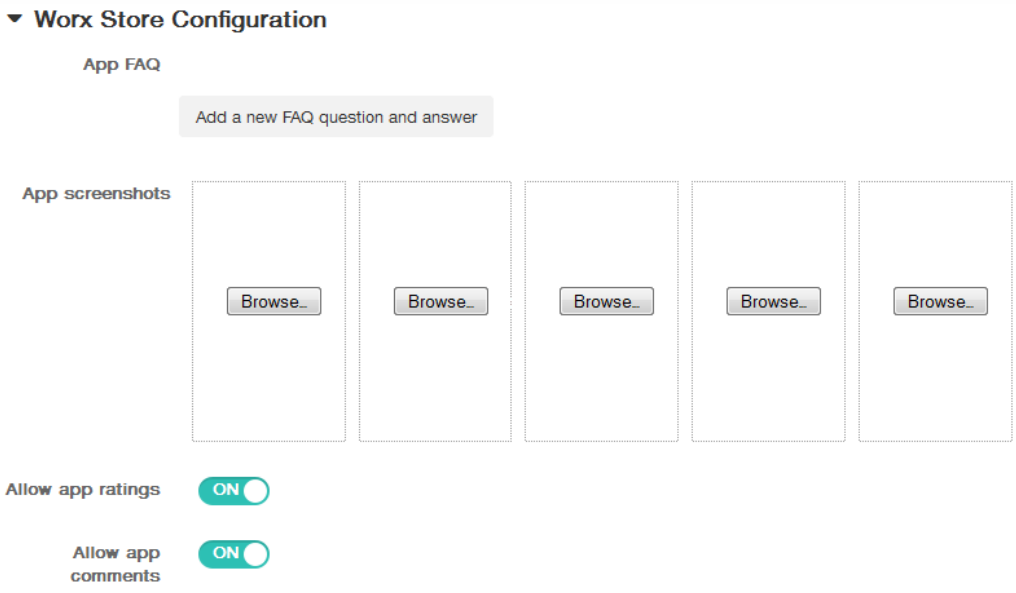
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
    1. Cliquez sur ET, OU ou SAUF.
    2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
       Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
    3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
       Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai, l'appareil doit se conformer aux exigences en matière de code secret et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



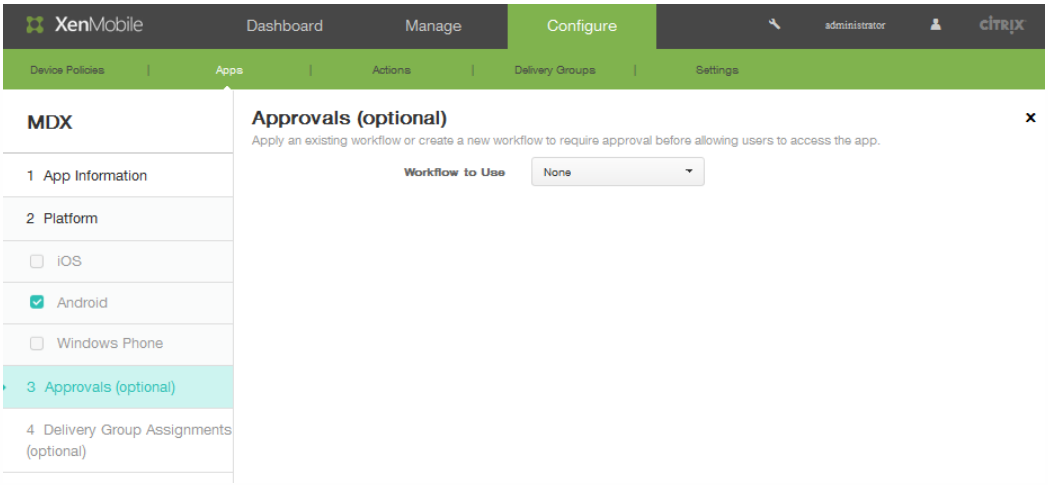
11. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



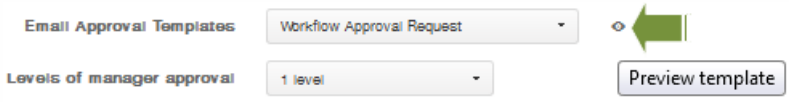
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

12. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
13. Cliquez sur Suivant. L'écran Approbations s'affiche.

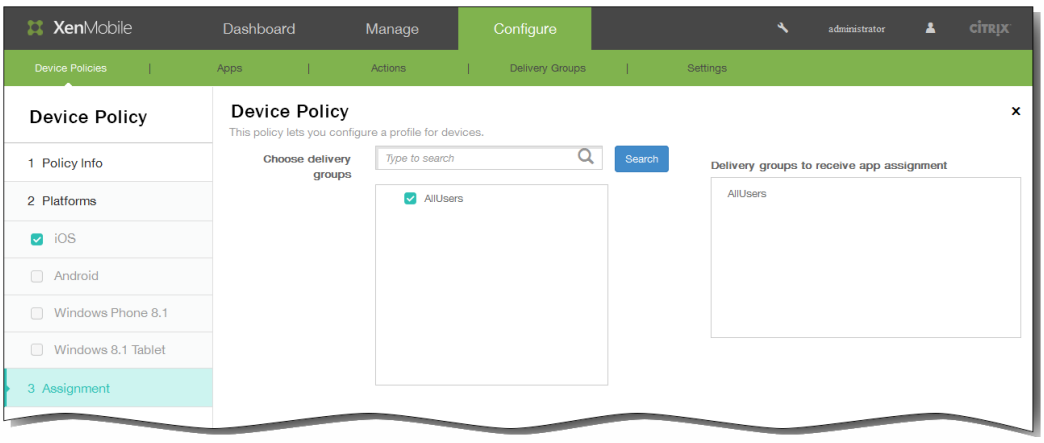
© 1999-2017 Citrix Systems, Inc. All rights reserved.



14. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur.
    1. Spécifiez un **nom** pour le workflow.
    2. Éventuellement, entrez une **description**.
    3. Dans le champ **Modèles d'approbation d'e-mail**, cliquez sur une option de notification. Cliquez sur **l'icône** d'œil pour afficher un aperçu du modèle choisi.



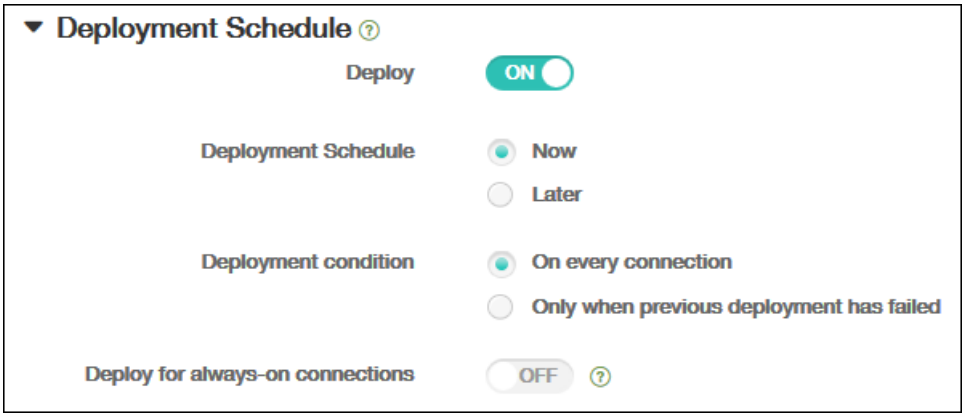
    4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3. .
    5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
    6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.
15. Cliquez sur Suivant.
16. 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

17. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. 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.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. 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.



18. Cliquez sur Enregistrer. La console XenMobile applique les informations d'application.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Création de catégories d'applications dans XenMobile

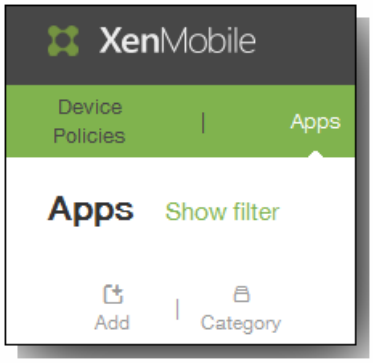
Jul 25, 2016

Lorsque les utilisateurs se connectent à Worx Home, 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 pouvez également configurer une catégorie Apple pour l'App Store.

Vous configurez les catégories sur la page Applications dans la console XenMobile. Ensuite, lorsque vous configurez ou modifiez une application, un lien Web ou un magasin, vous pouvez ajouter l'application à l'une des catégories que vous avez configurées.

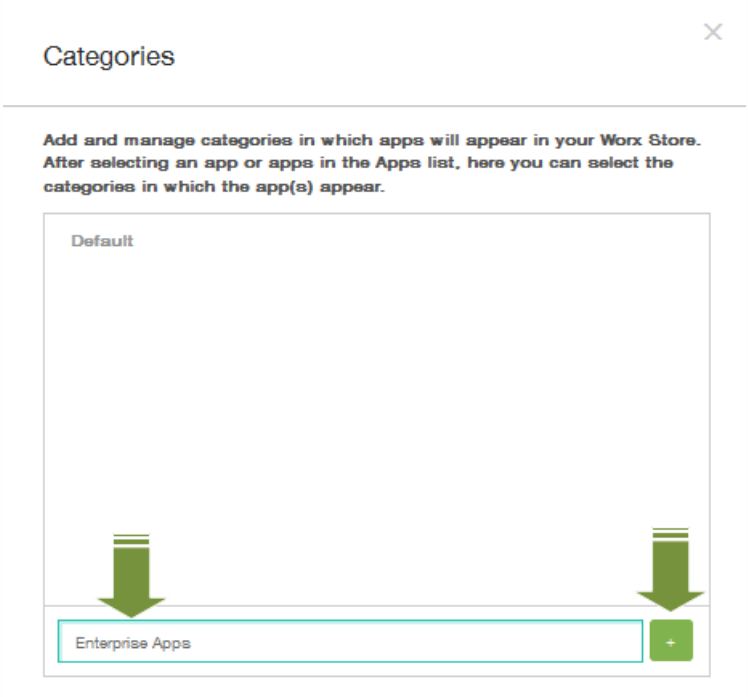
Pour ajouter une catégorie

1. Dans la console XenMobile, cliquez sur Configurer > Applications. La page Applications s'affiche.
2. Sur la page Applications, cliquez sur Catégorie.



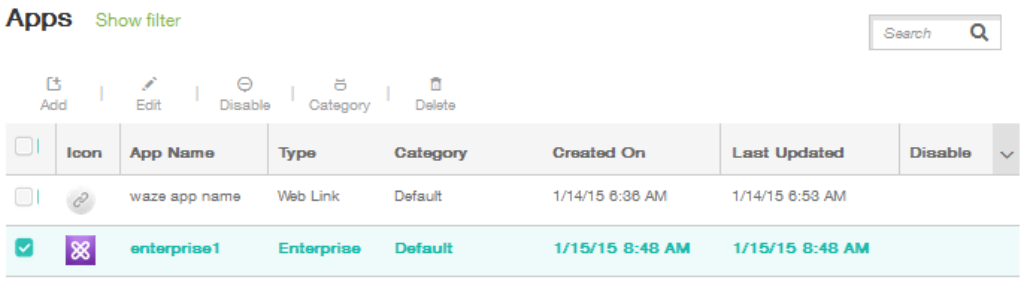
3. Dans la boîte de dialogue Catégories, entrez le nom de la catégorie que vous souhaitez ajouter, puis cliquez sur le signe plus (+). Par exemple, entrez *Applications d'entreprise*, puis cliquez sur le signe plus (+).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

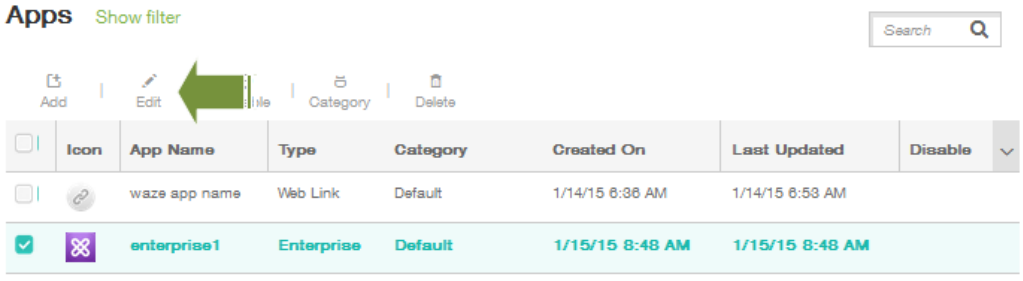


La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue Catégories. Si aucune catégorie n'est configurée, seule la catégorie **par défaut** s'affiche.

4. Répétez l'étape 3 pour ajouter autant de nouvelles catégories que vous le souhaitez, puis fermez la boîte de dialogue Catégories.
5. Sur la page Applications, vous pouvez classer une application existante dans une nouvelle catégorie. Sélectionnez l'application que vous souhaitez classer.



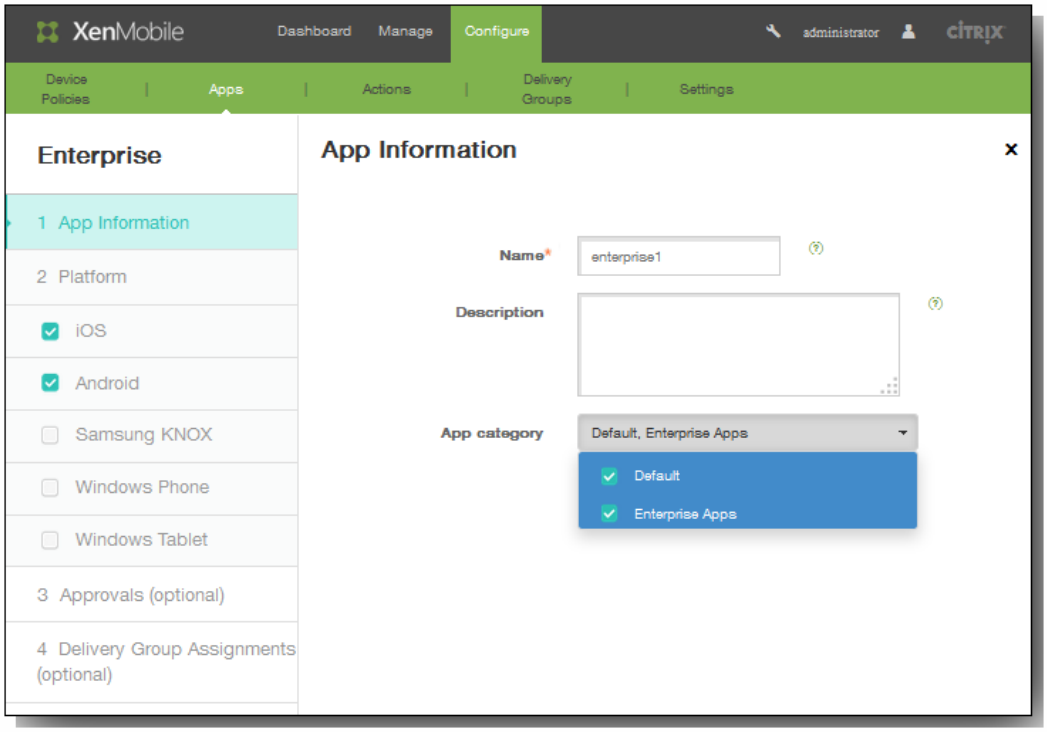
6. Cliquez sur Modifier pour classer l'application.



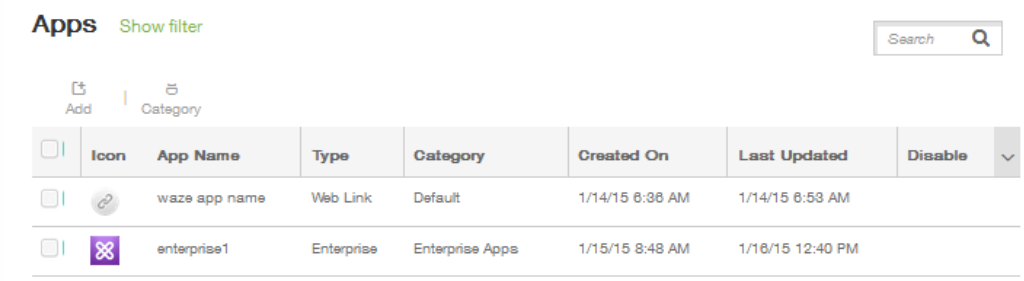
© 1999-2017 Citrix Systems, Inc. All rights reserved.

La page Informations sur l'application s'affiche.

7. Dans la liste Catégorie d'application, appliquez la catégorie en sélectionnant la case à cocher appropriée.



8. Cliquez sur Suivant pour compléter les autres pages de configuration de l'application.
9. Cliquez sur Enregistrer sur la dernière page pour appliquer la catégorie. La nouvelle catégorie créée est appliquée à l'application et l'application s'affiche dans le tableau des applications.



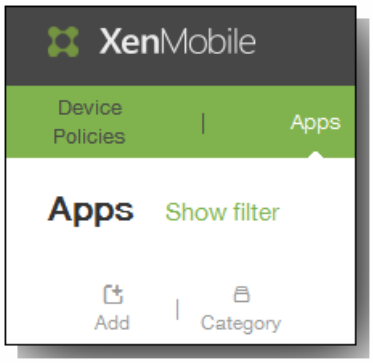
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter un magasin d'applications public à XenMobile

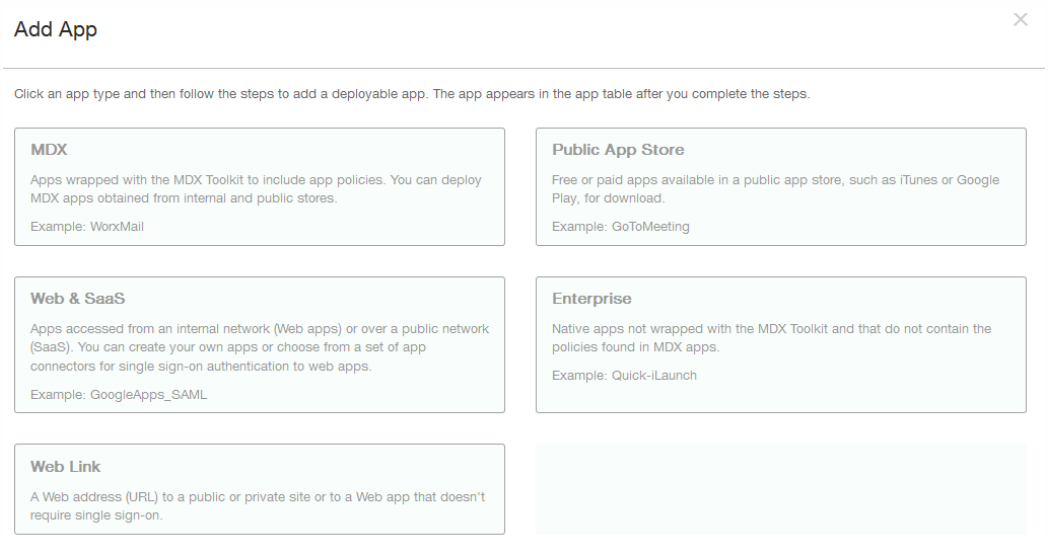
Jul 25, 2016

Vous pouvez ajouter des applications gratuites ou payantes à XenMobile qui sont disponibles dans un magasin d'applications public, tel que iTunes où GooglePlay. Par exemple : GoToMeeting.

1. Dans la console XenMobile, cliquez sur Configurer > Applications. L'écran Applications s'affiche.

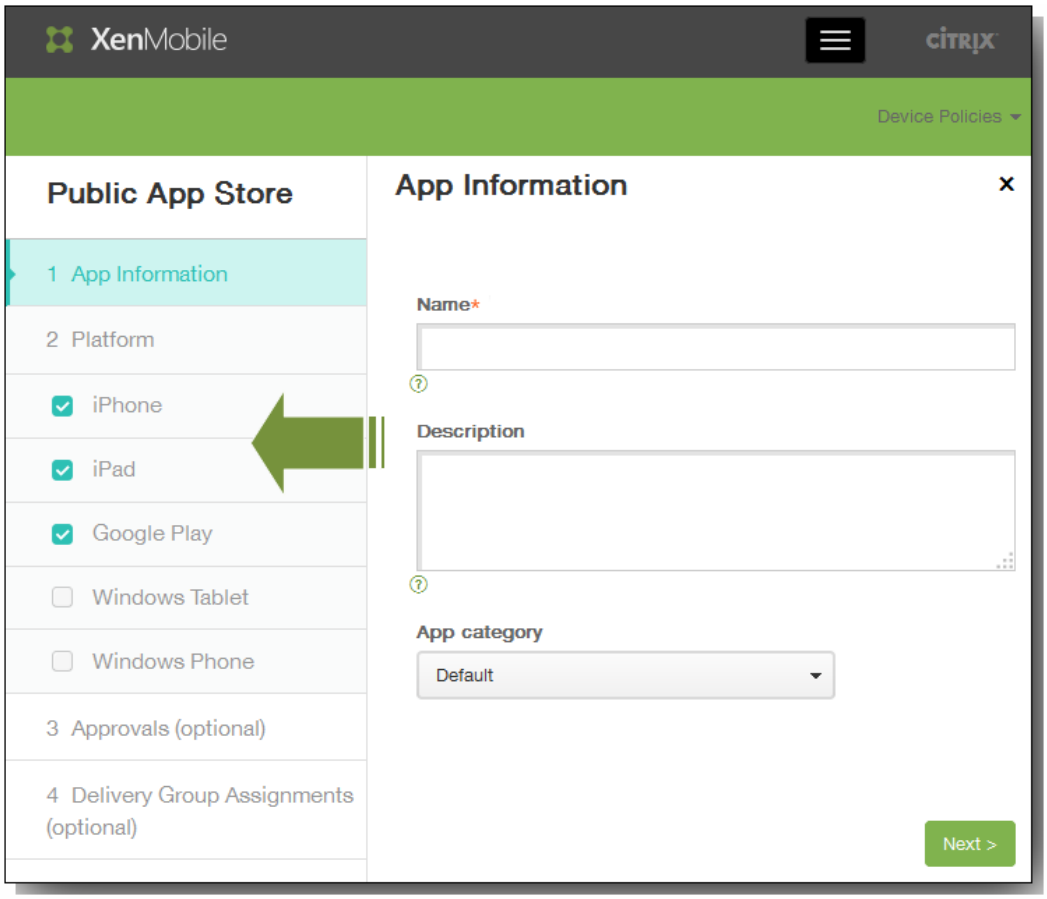


2. Cliquez sur Ajouter.
3. Dans l'écran Ajouter une application, cliquez sur Magasin d'applications public.

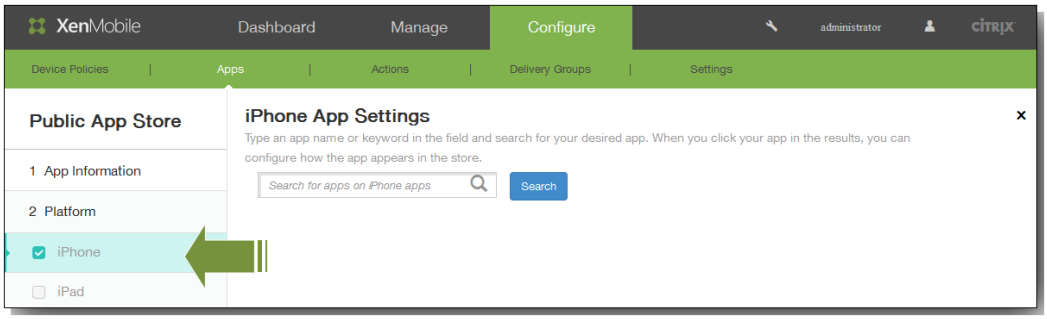


4. Sur la page Informations sur l'application, entrez un nom et une description pour l'application. Ces champs sont utilisés à des fins internes. Si vous ajoutez des applications pour de multiples appareils (par exemple, iPhone, iPad et GooglePlay), utilisez les cases à cocher dans la partie gauche de l'écran pour les sélectionner.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

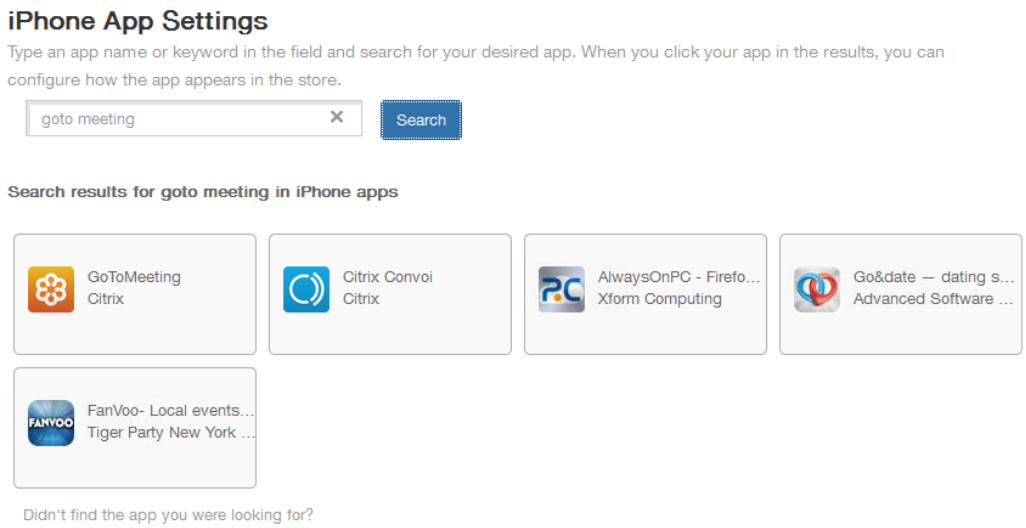


5. Dans la liste Catégorie d'application, cliquez sur Catégorie d'application.
6. Cliquez sur Suivant.
7. Sur l'écran Plate-forme de sélection du type de plate-forme, dans le champ de recherche, tapez le nom d'une application ou un mot clé pour localiser l'application que vous souhaitez ajouter. Par exemple, si vous avez choisi d'ajouter une application iPhone, la console XenMobile recherche toutes les applications iPhone. Si vous avez choisi d'ajouter des applications pour de multiples plates-formes, des résultats s'affichent pour chaque plate-forme.

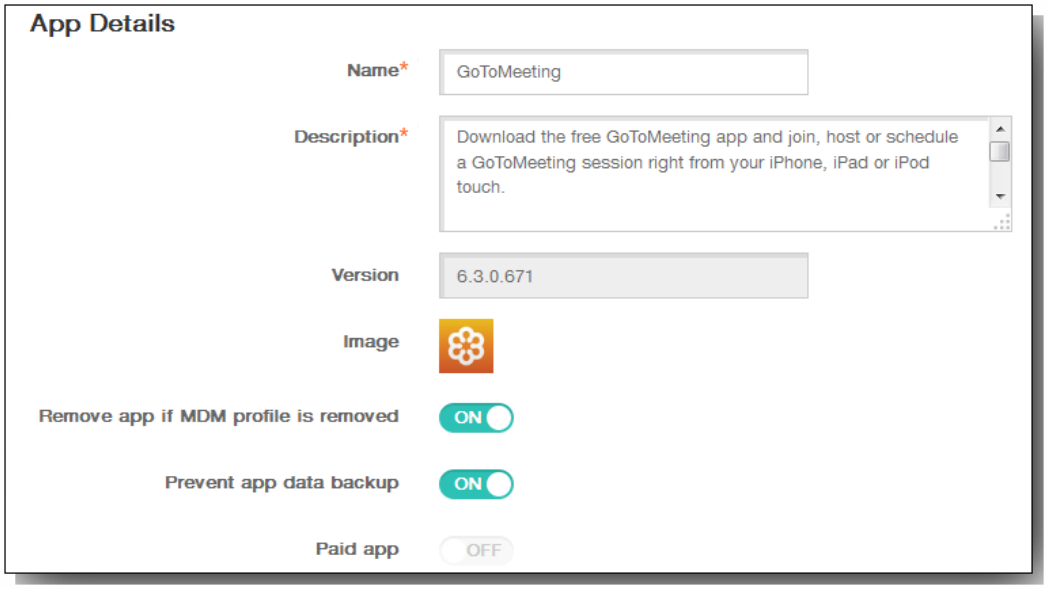


Dans la figure suivante, les applications correspondant aux critères de recherche s'affichent (par exemple, GoToMeeting).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. Cliquez sur une application dans les résultats pour configurer la manière dont elle s'affiche dans le magasin. Sur l'écran Détails sur l'application, les champs sont préremplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image). Si nécessaire, modifiez le nom et la description de l'application.



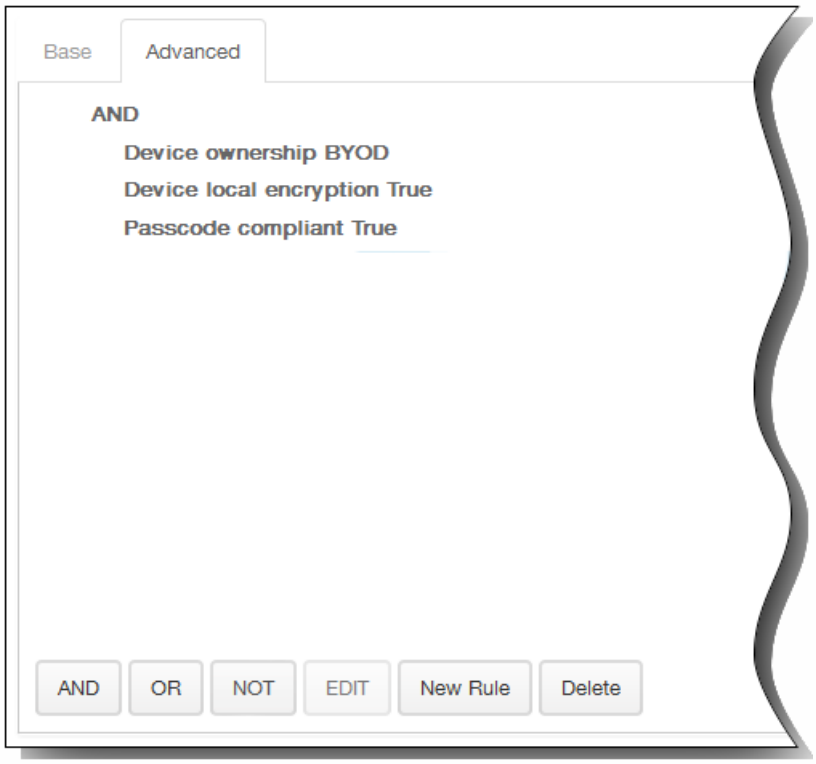
1. Dans Supprimer l'application si le profil MDM est supprimé, cliquez sur ON pour supprimer l'application lorsque le profil MDM est supprimé. Par défaut, cette option est réglée sur ON.
2. Dans Empêcher la sauvegarde des données d'application, cliquez sur ON pour empêcher l'application de sauvegarder des données. Par défaut, cette option est réglée sur ON.
3. Dans **Application payante**, le champ est préconfiguré et ne peut pas être modifié.

9. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.



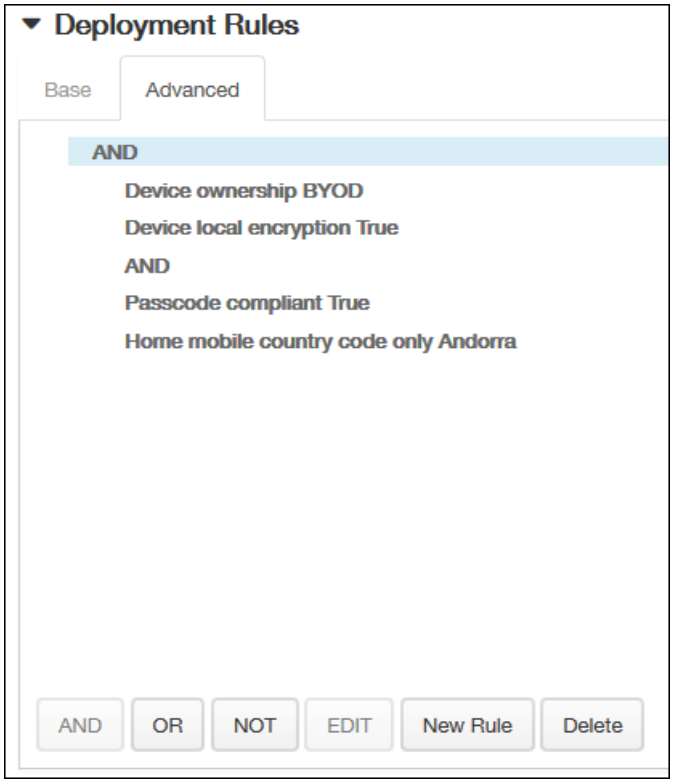
© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

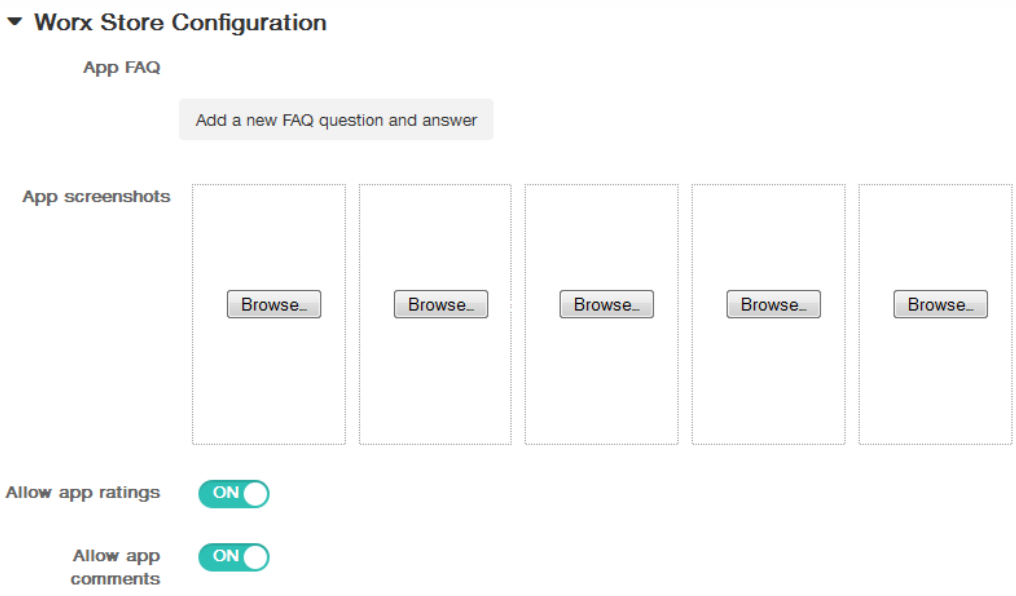


   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
    1. Cliquez sur ET, OU ou SAUF.
    2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
       Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
    3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
       Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai, l'appareil doit se conformer aux exigences en matière de code secret et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



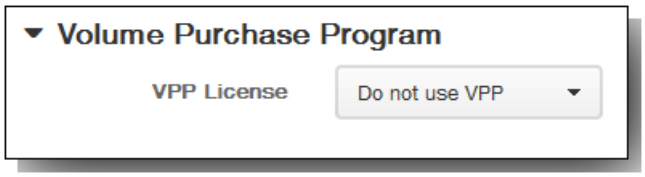
10. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



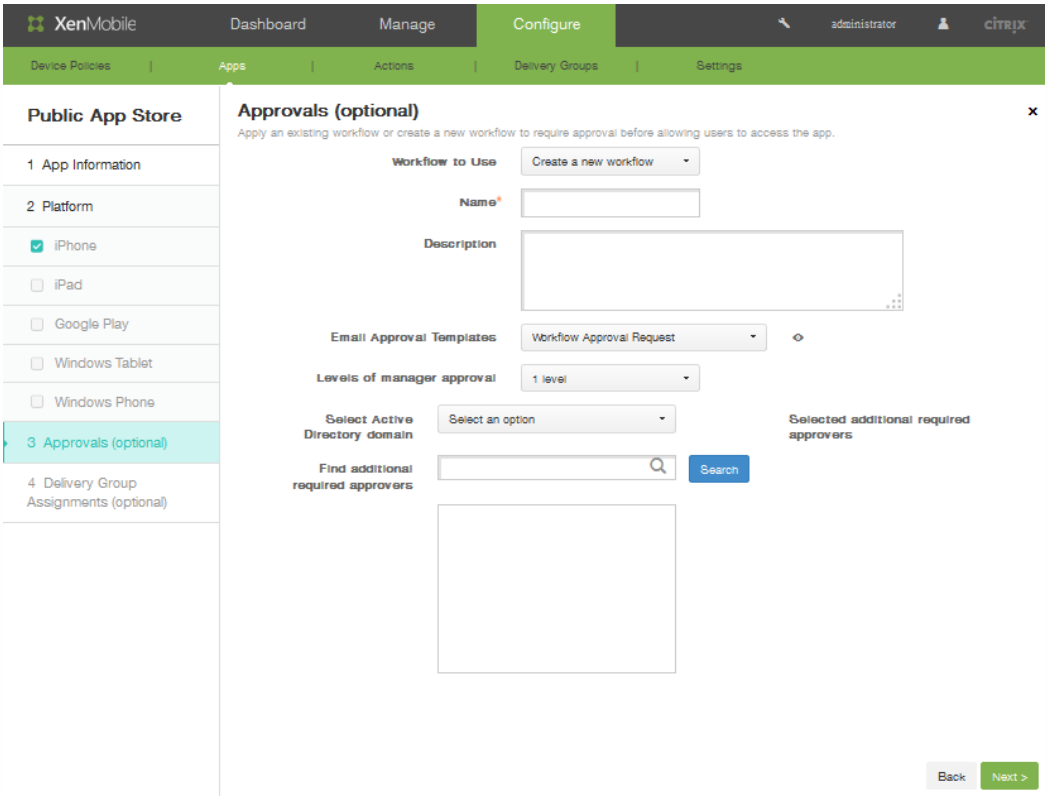
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

11. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
12. Développez Programme d'achat en volume, puis 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.

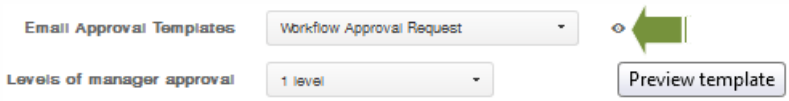
© 1999-2017 Citrix Systems, Inc. All rights reserved.



13. Cliquez sur Suivant et répétez les étapes 7 à 16 pour chaque type de plate-forme pour laquelle vous souhaitez ajouter des applications publiques.
14. Sur la page **Approbations**, dans la liste **Workflow à utiliser**, cliquez sur un workflow ou sur **Créer un nouveau workflow**.



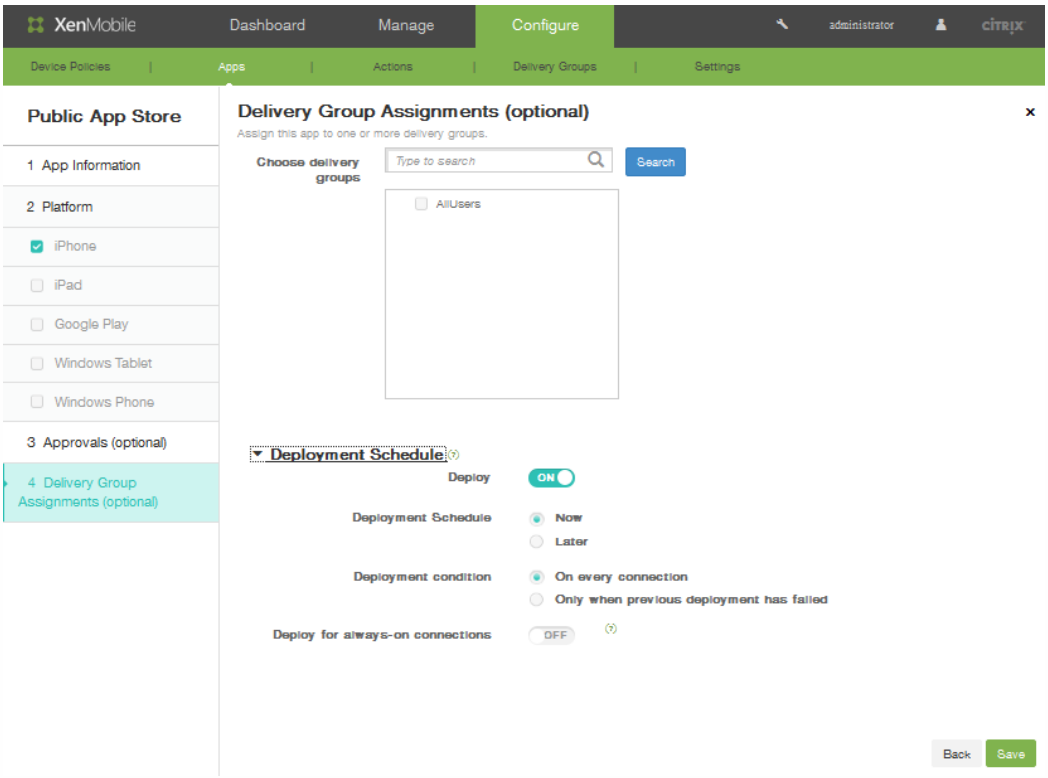
15. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes.
    1. Spécifiez un **nom** pour le workflow.
    2. Éventuellement, entrez une **description**.
    3. Dans le champ **Modèles d'approbation d'e-mail**, cliquez sur une option de notification. Cliquez sur **l'icône** d'œil pour afficher un aperçu du modèle choisi.



    4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3. .
    5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
    6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

16. Cliquez sur **Suivant**.
17. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez l'application à un ou plusieurs groupes de mise à disposition.



18. Dans Choisir des groupes de mise à disposition, recherchez un groupe de mise à disposition (ou des groupes.) Sélectionnez la case à cocher **Tous les utilisateurs** pour attribuer l'application à chaque utilisateur XenMobile.
19. Développez Calendrier de déploiement pour affiner le groupe de mise à disposition.
    1. Déployer : cliquez sur ON pour activer un calendrier de déploiement.
    2. Calendrier de déploiement : cliquez sur Maintenant ou Plus tard pour définir la planification du déploiement.
    3. Conditions de déploiement : cliquez pour déployer l'application sur chaque connexion, ou uniquement lorsque le déploiement précédent a échoué.
    4. Dans Déployer pour les connexions permanentes, cliquez sur ON pour procéder au déploiement lorsque la stratégie de connexion permanente est définie.
       Remarque : cette option s'applique lorsque vous avez également configuré des clés de déploiement d'arrière-plan globales dans la section Paramètres des propriétés du serveur de la console XenMobile. La stratégie de calendrier permanent n'est pas disponible pour iOS.
20. Cliquez sur Enregistrer. La console XenMobile applique les informations d'application.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une application Web et SaaS à XenMobile

Jul 25, 2016

Grâce à la console XenMobile, vous pouvez fournir aux utilisateurs une 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 Liste des types de connecteur d'applications.

Vous pouvez également créer votre propre connecteur dans XenMobile.

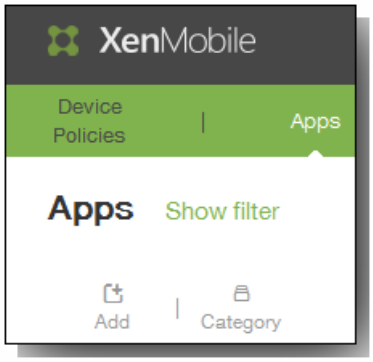
Pour configurer un connecteur, spécifiez les paramètres suivants :

- Noms différents (facultatif). Utilisez tout connecteur affiché dans la console. Le connecteur de zone n'est plus pris en charge.
- Description de l'application.
- Adresse Web en utilisant le nom de domaine complet (FQDN). Par exemple, si vous voulez ajouter LinkedIn à votre liste d'applications, vous accédez à http://www.linkedin.com, puis vous cliquez sur Sign in (Se connecter). Lorsque la page d'ouverture de session s'affiche, vous utilisez l'adresse Web https://www.linkedin.com lors de la configuration de l'application.
- Emplacement de l'application (Internet où votre réseau interne).
- Informations d'identification pour l'authentification unique. Les utilisateurs peuvent utiliser les informations d'identification de l'application.
- Catégorie à laquelle l'application appartient. Les catégories vous permettent d'organiser les applications dans Worx Home.
- Stratégies d'application pour chaque application que vous configurez dans XenMobile.
- Paramètres d'approbation de workflow pour toutes les applications, ce qui comprend la spécification des individus qui peuvent approuver le compte utilisateur.
- Groupe de mise à disposition d'utilisateurs auxquels vous voulez attribuer l'application.

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.

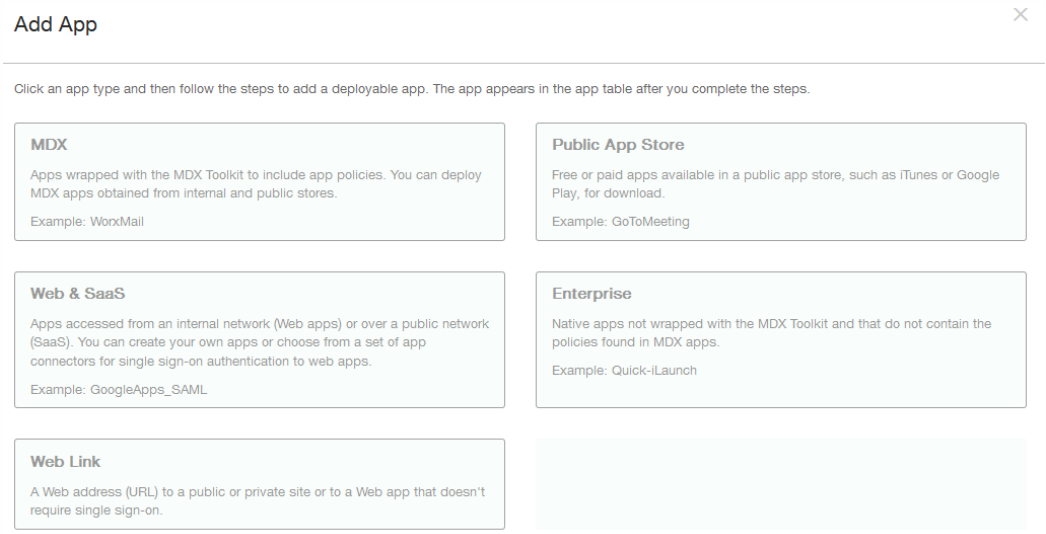
Pour ajouter un connecteur d'applications dans XenMobile

1. Dans la console Web XenMobile, cliquez sur Configurer > Applications. La page Applications s'ouvre.
2. Sur la page Applications, cliquez sur **Ajouter**.

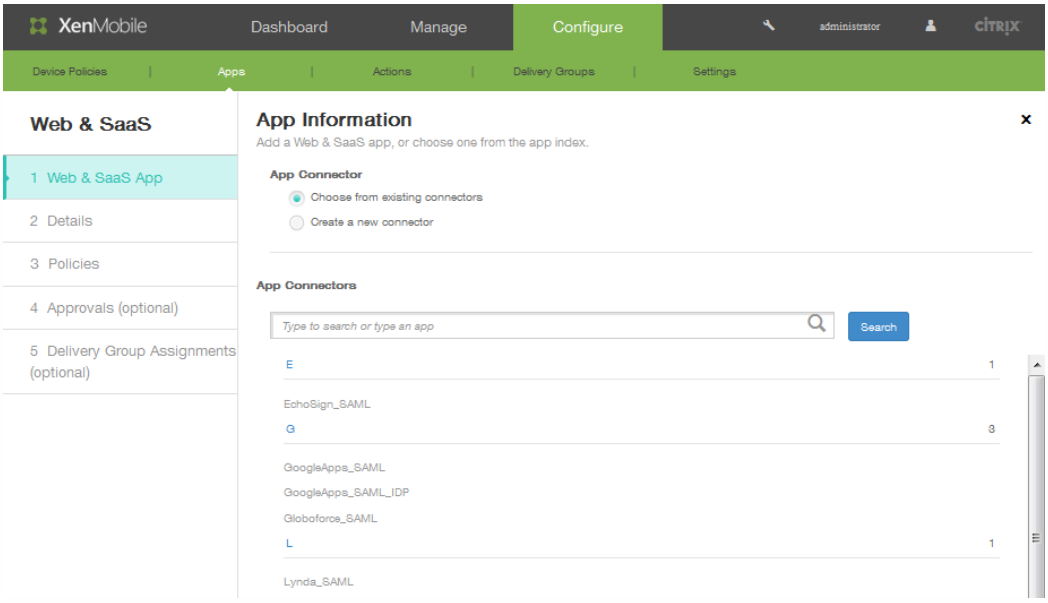


3. Sur la page **Ajouter une application**, cliquez sur **Web et SaaS**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

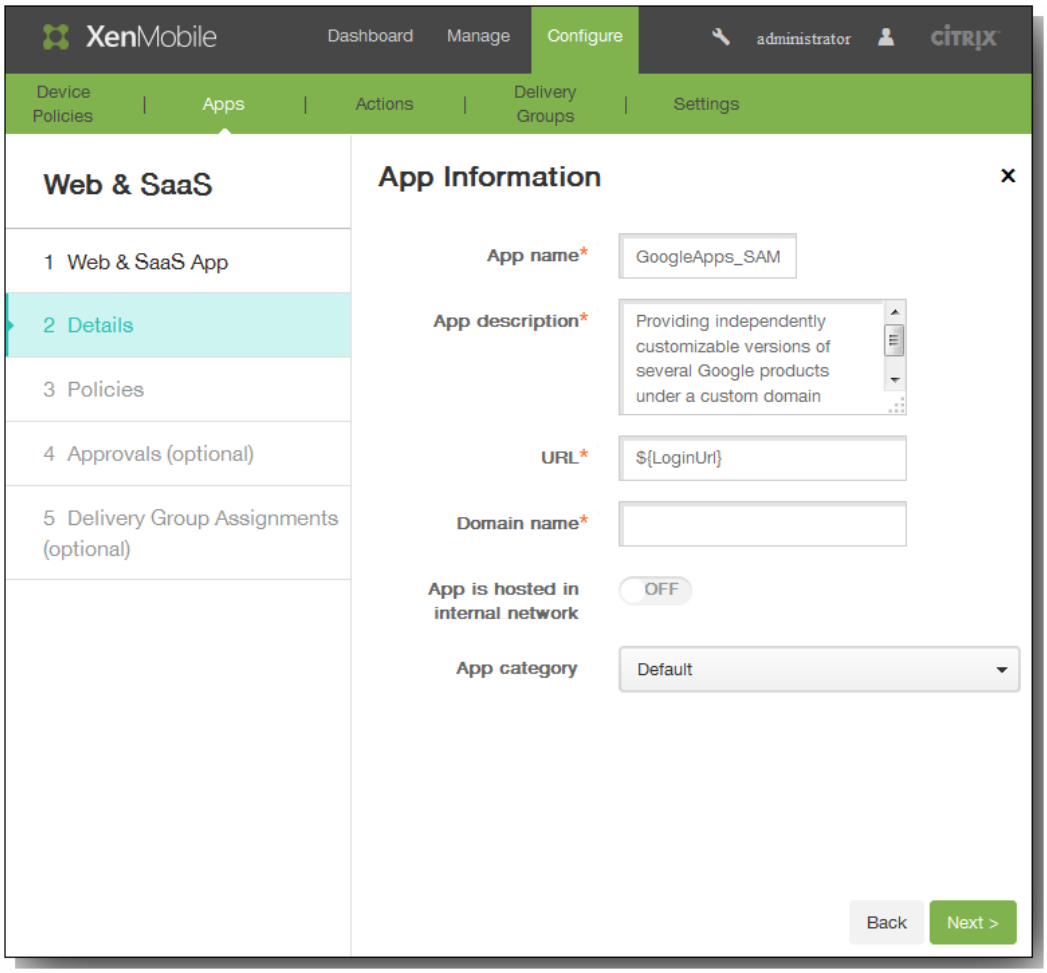


4. Sur la page Informations sur l'application, cliquez sur Choisir parmi les connecteurs existants ou Créer un nouveau connecteur.



5. Si vous cliquez sur une application dans la liste, la page Détails s'ouvre. Les champs Nom app, Description et URL sont pré-remplis.

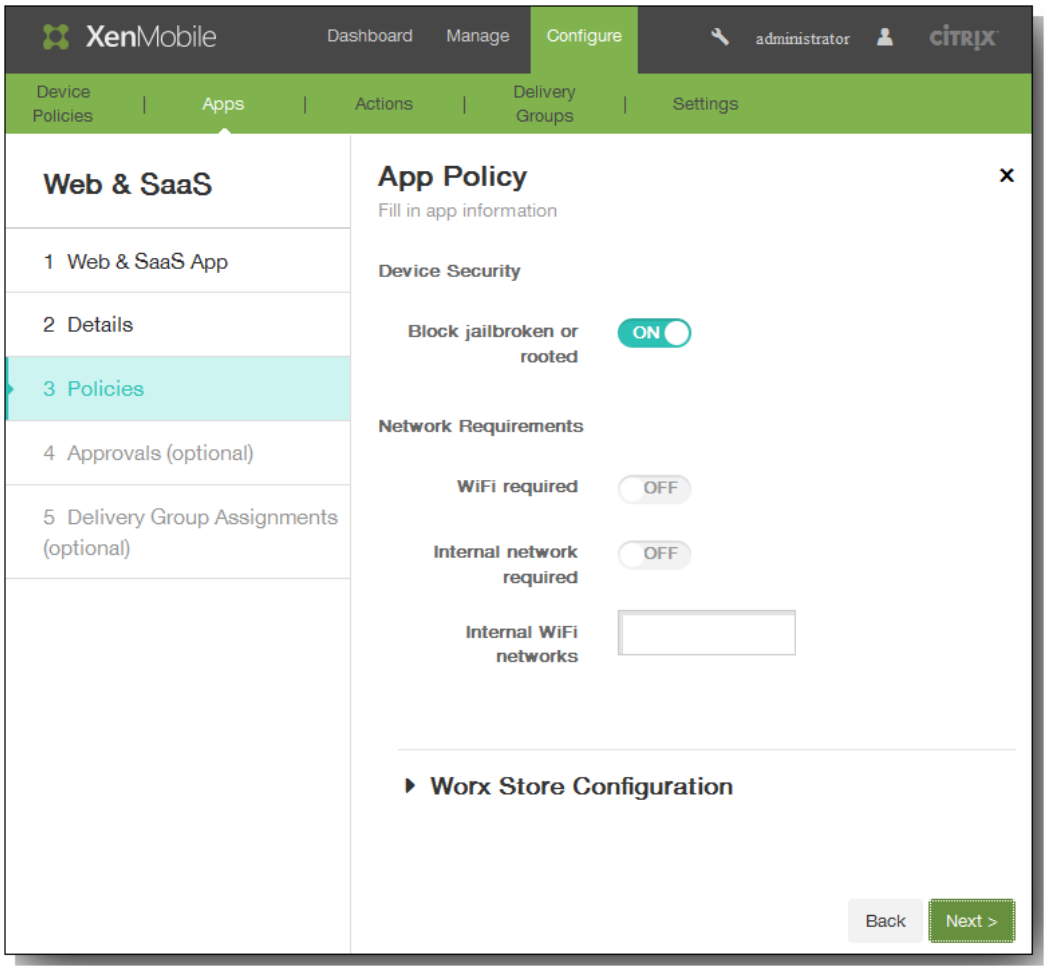
© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Le cas échéant, dans le champ URL, entrez l'adresse Web de l'application ou conservez l'adresse par défaut.
2. Sélectionnez L'application est hébergée dans le réseau interne et cliquez sur ON 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.
3. Dans la liste Catégorie d'application, cliquez sur une catégorie.
4. Dans la case Activer la gestion des utilisateurs pour le provisioning, cliquez sur On. Si vous utilisez le connecteur Globalforce_SAML, vous devez Activer la gestion des utilisateurs pour le provisioning pour assurer une intégration SSO transparente.

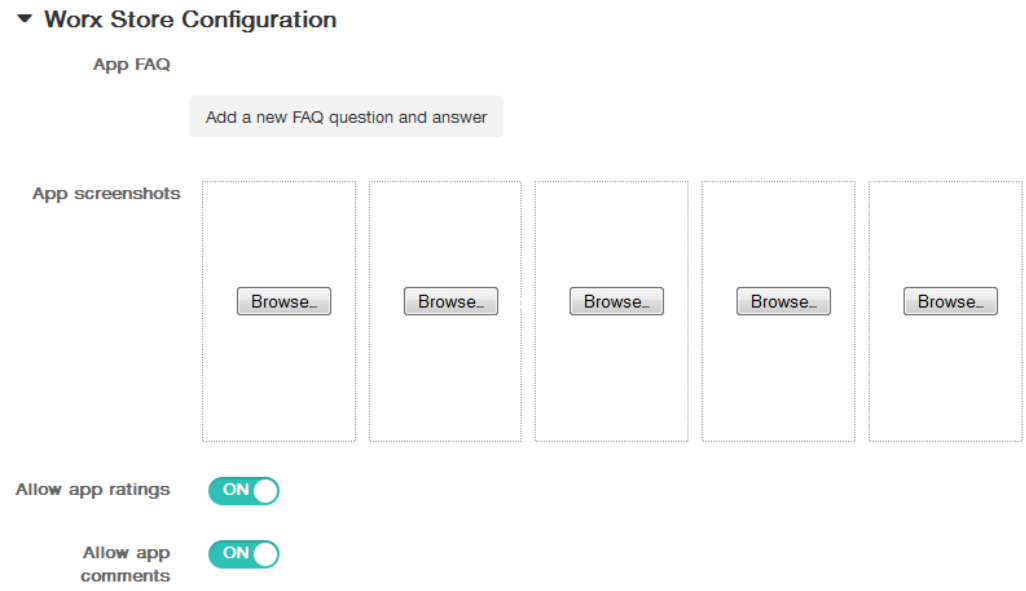
6. Cliquez sur Suivant. La page Stratégies s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



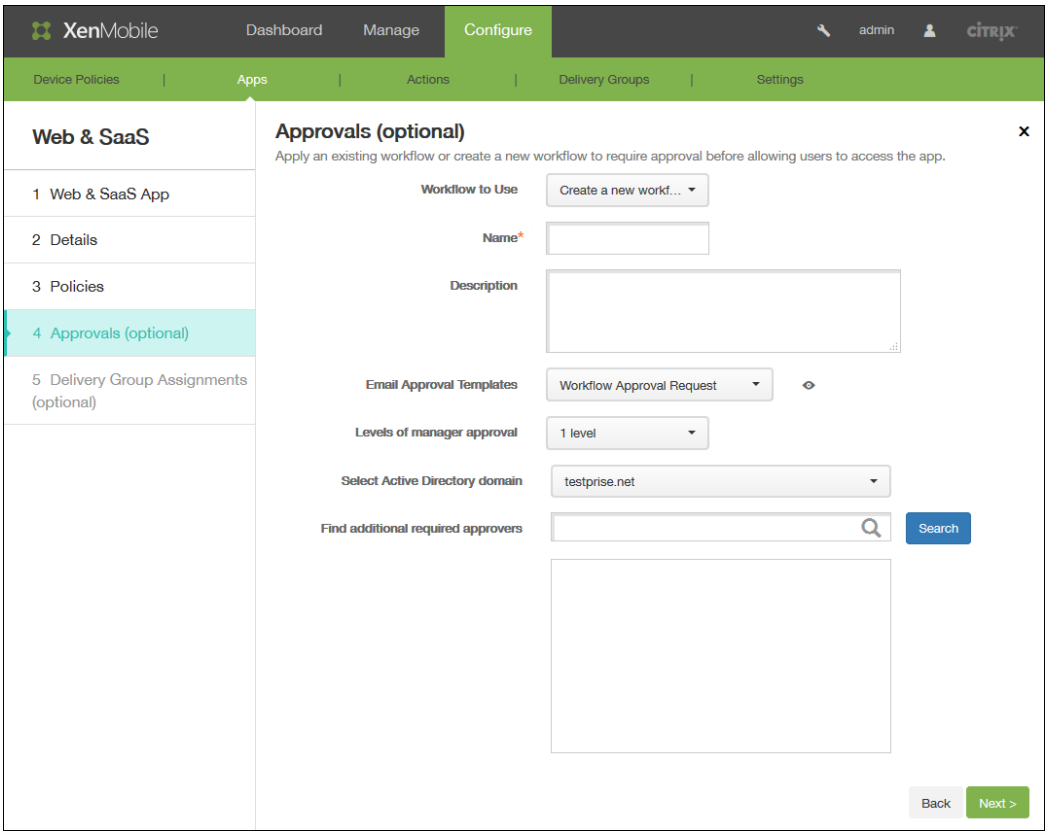
7. Dans Sécurité de l'appareil, dans Bloquer les appareils jailbreakés ou rootés, cliquez sur ON.
8. Dans Exigences du réseau, configurez les paramètres suivants :
   1. Dans Wi-Fi requis, cliquez sur Activé, puis spécifiez des réseaux Wi-Fi internes.
   2. Dans Réseau interne requis, cliquez sur ON si un réseau interne est requis pour exécuter l'application.
9. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

10. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
11. Cliquez sur Suivant.
12. Sur la page Approbations, dans la liste Workflow à utiliser, cliquez sur un workflow ou sur Créer un nouveau workflow.

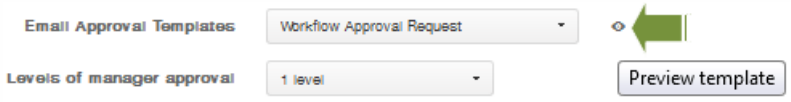


13. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin

© 1999-2017 Citrix Systems, Inc. All rights reserved.

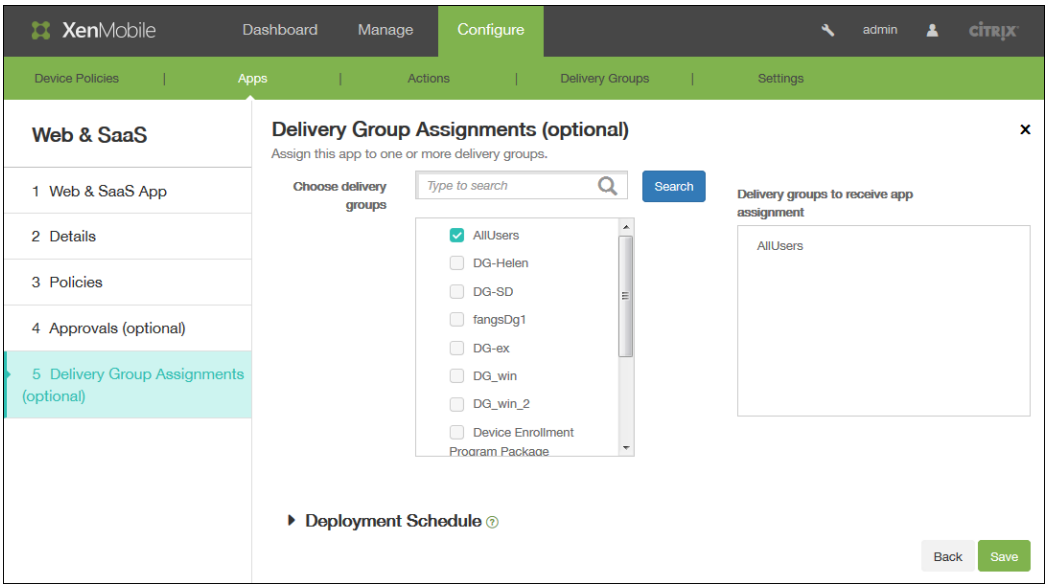
d'une approbation pour créer un compte d'utilisateur.

1. Spécifiez un **nom** pour le workflow.
2. Éventuellement, entrez une **description**.
3. Dans le champ **Modèles d'approbation d'e-mail**, cliquez sur une option de notification. Cliquez sur **l'icône** d'œil pour afficher un aperçu du modèle choisi.



4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3.
5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

14. Cliquez sur Suivant.
15. Éventuellement, sur la page **Attribution de groupes de mise à disposition**, 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.

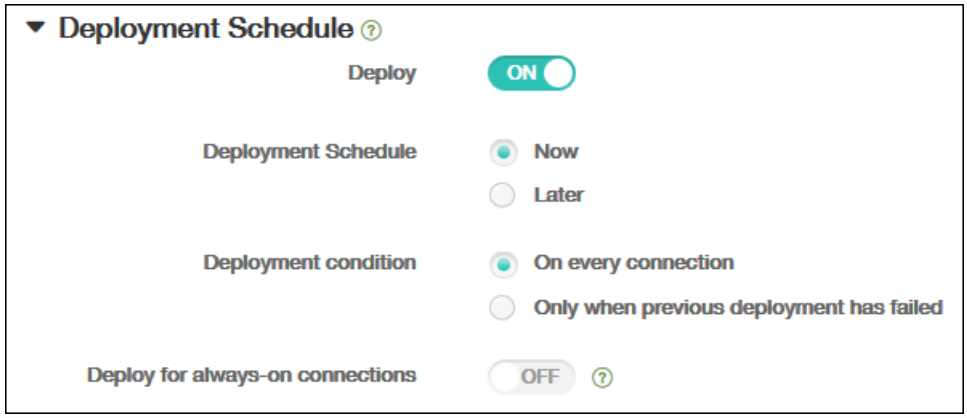


16. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.
    4. 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.
    5. En regard de Déployer pour les connexions permanentes, cliquez sur ON ou OFF. L'option par défaut est OFF.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Liste des types de connecteur d'applications

Jul 25, 2016

Le tableau suivant dresse la liste des connecteurs et des types de connecteurs disponibles avec XenMobile. Il indique également 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter une application d'entreprise à XenMobile

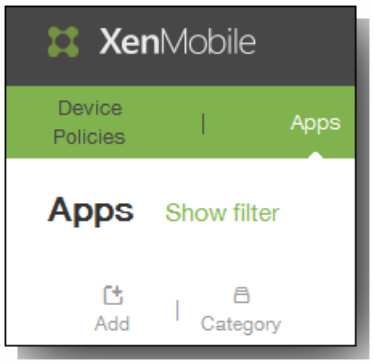
Jul 25, 2016

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) :

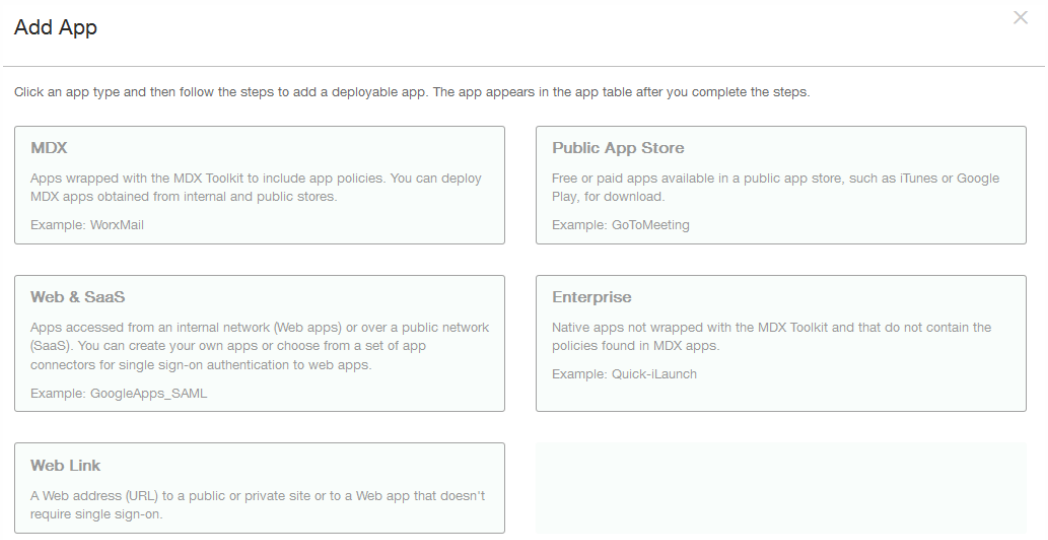
- iOS (fichier .ipa)
- Android (fichier .apk)
- Samsung KNOX (fichier .apk)
- Android for Work (fichier .apk)
- Windows Phone (fichier .xap ou .appx)
- Windows Tablet (fichier .appx)

Pour créer une application d'entreprise

1. Dans la console XenMobile, cliquez sur Configurer > Applications.
2. Sur la page Applications, cliquez sur **Ajouter**.

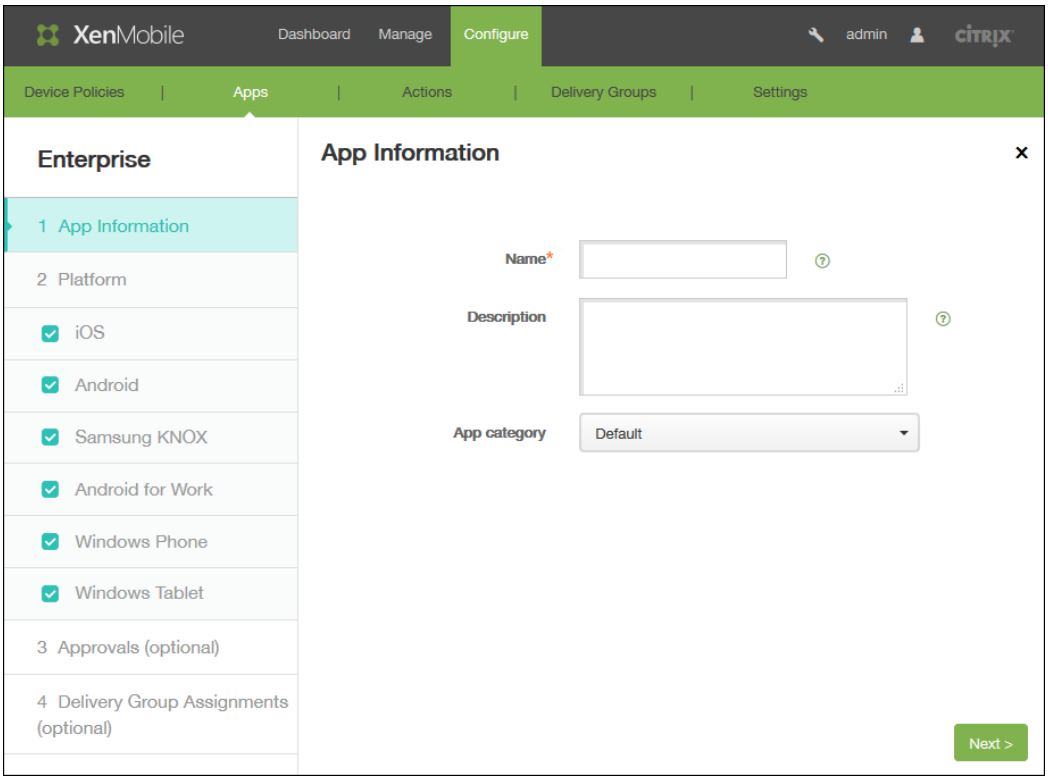


3. Sur la page Ajouter une application, cliquez sur **Entreprise**.



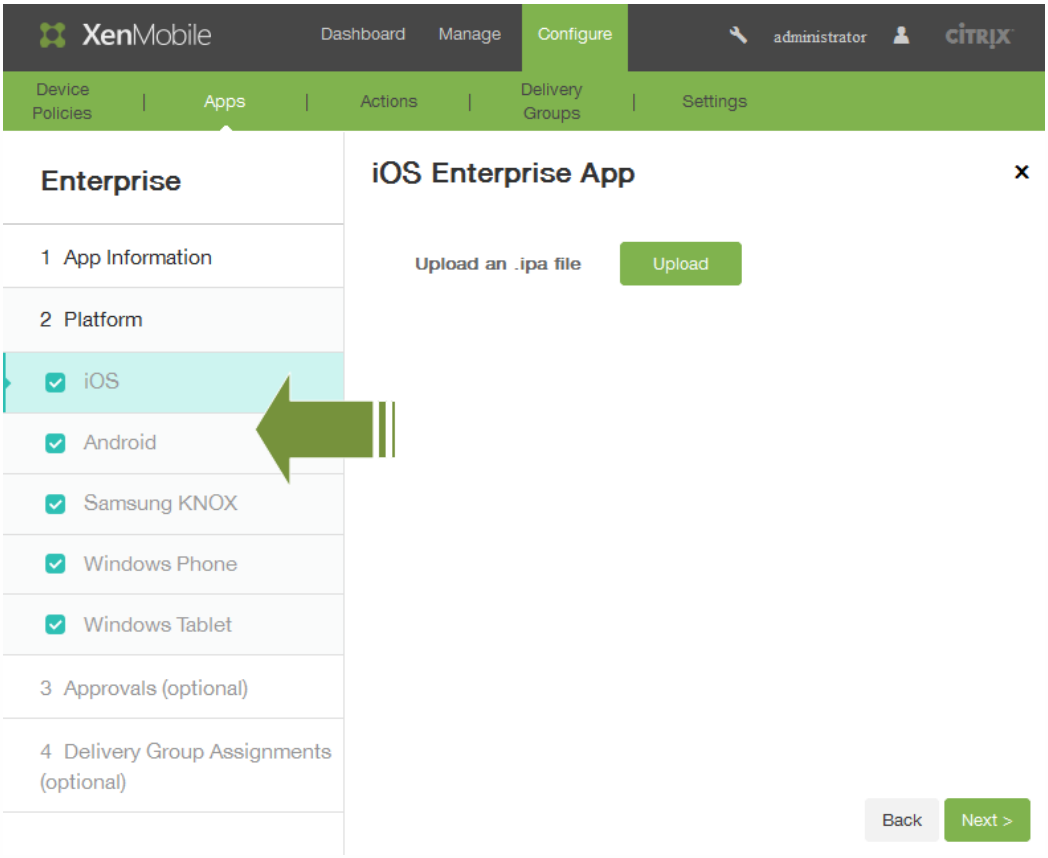
© 1999-2017 Citrix Systems, Inc. All rights reserved.

La page Informations sur l'application s'affiche.

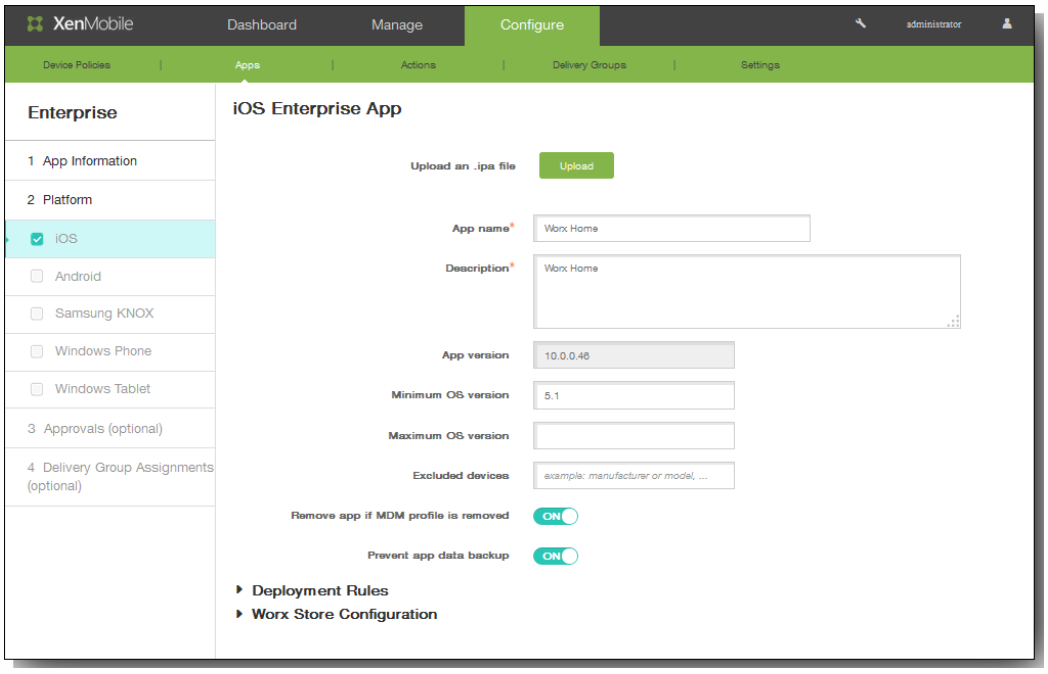


4. Sur la page Informations sur l'application, complétez les éléments suivants :
   1. Nom : entrez un nom pour l'application.
   2. Description : entrez une description pour l'application.
   3. Dans **Catégorie d'application**, cliquez sur une catégorie, puis sur Suivant.
5. Dans la zone Plate-forme sur le côté gauche de la page, sélectionnez les plates-formes auxquelles vous souhaitez ajouter l'application (par exemple, iOS ou Android).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Cliquez sur Charger pour accéder à l'emplacement du fichier, puis cliquez sur Suivant. La page d'informations sur l'application s'affiche pour le type de plate-forme. Les champs sont pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image). Si nécessaire, modifiez le nom et la description de l'application.

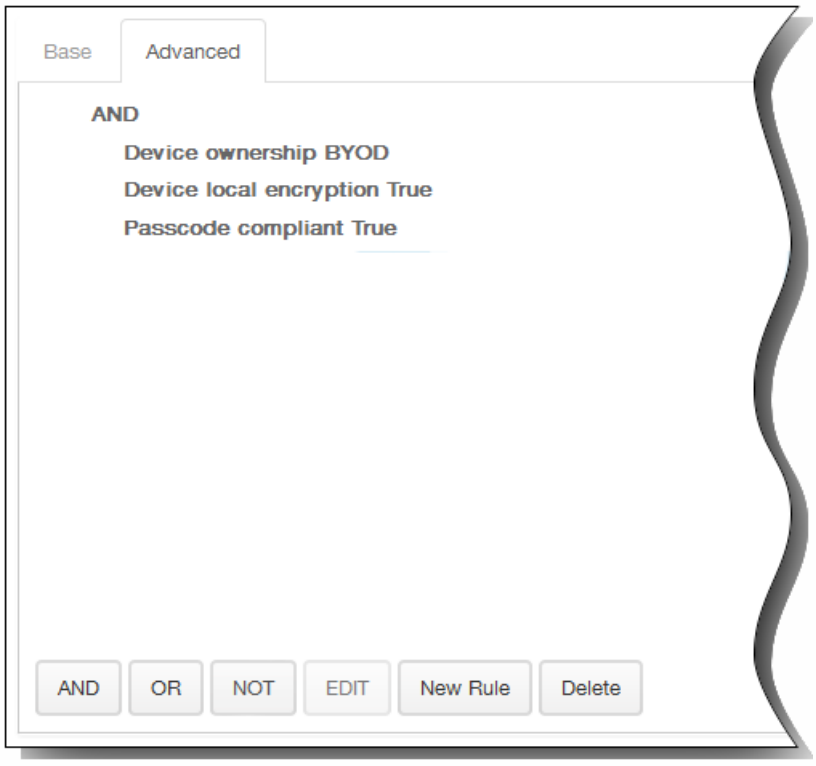


© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. Dans Supprimer l'application si le profil MDM est supprimé, cliquez sur ON pour supprimer l'application lorsque le profil MDM est supprimé. Par défaut, cette option est réglée sur ON.
8. Dans Empêcher la sauvegarde des données d'application, cliquez sur ON pour empêcher l'application de sauvegarder des données. Par défaut, cette option est réglée sur ON.
9. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

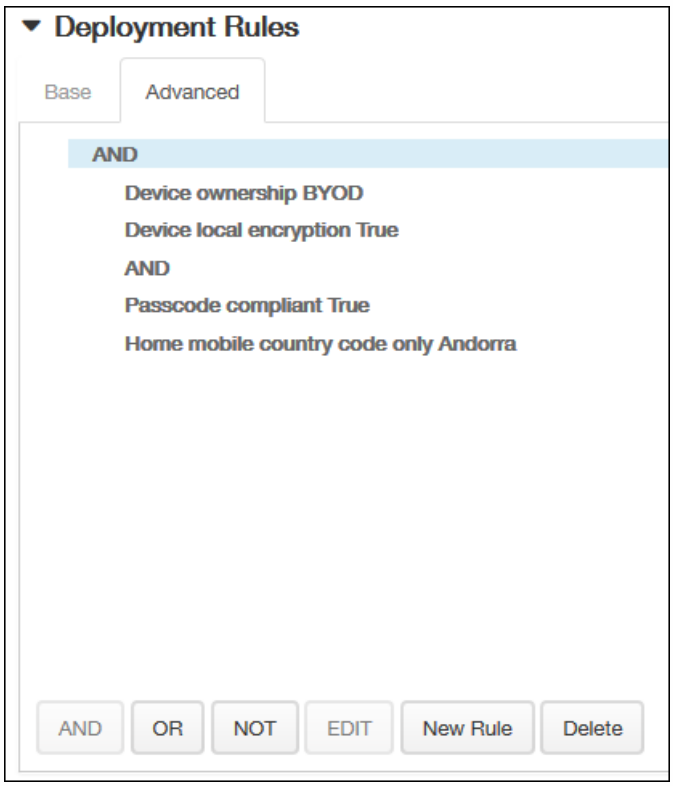


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Les conditions que vous avez choisies sur l'onglet Base s'affichent.

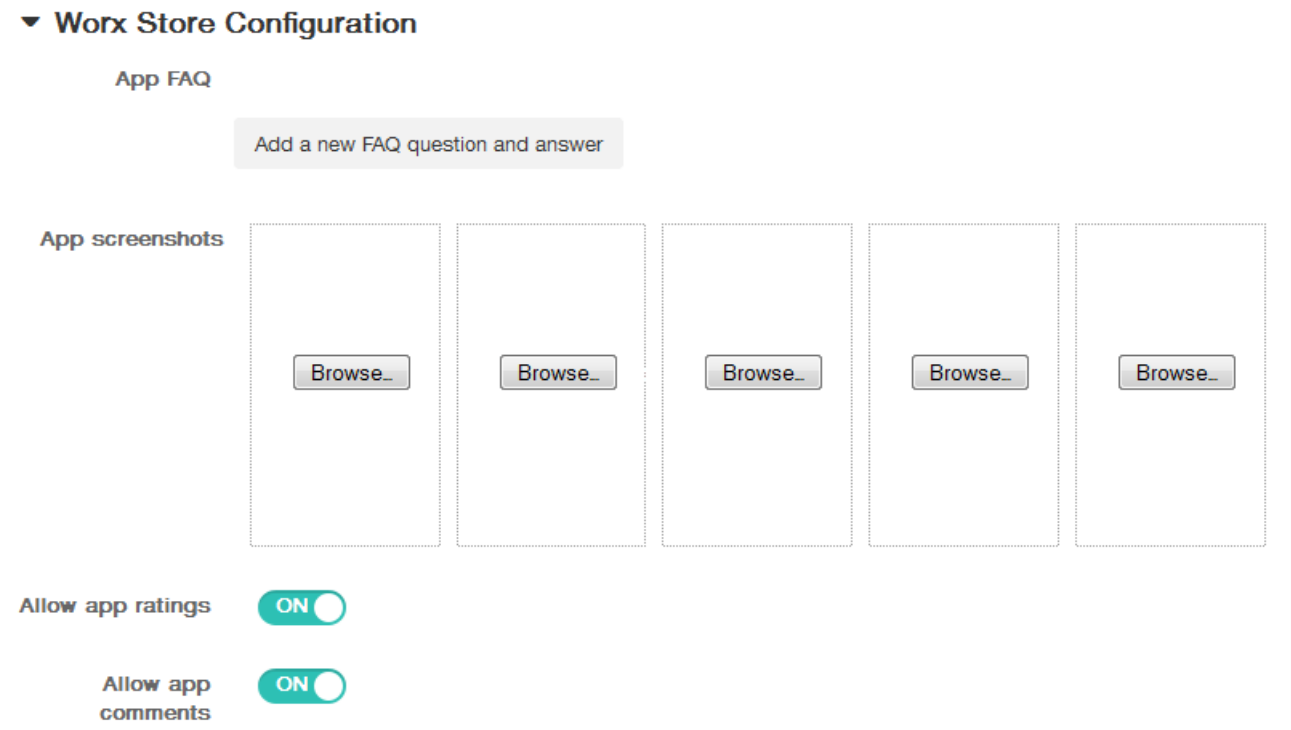
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai, l'appareil doit se conformer aux exigences en matière de code secret et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.



10. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.

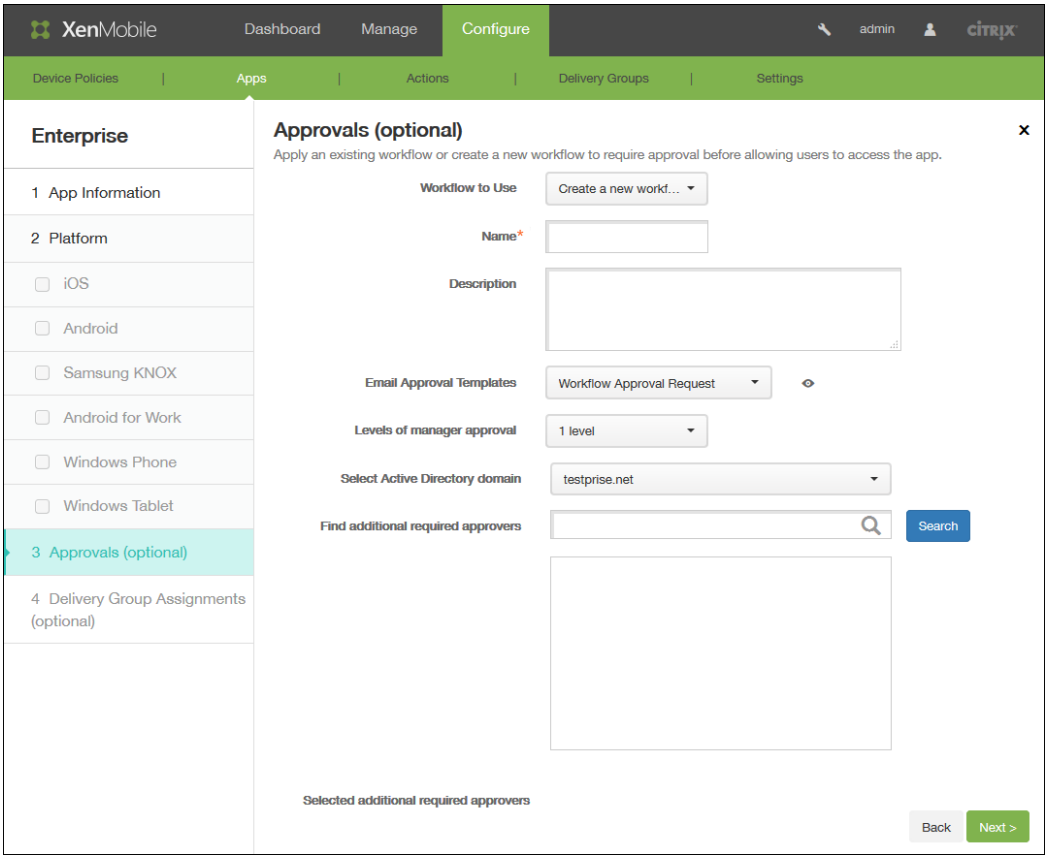
© 1999-2017 Citrix Systems, Inc. All rights reserved.



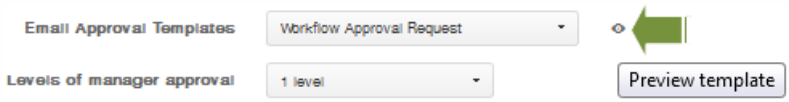
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

11. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
12. Cliquez sur Suivant.
13. Sur la page Approbations, dans la liste Workflow à utiliser, cliquez sur un workflow ou sur Créer un nouveau workflow.

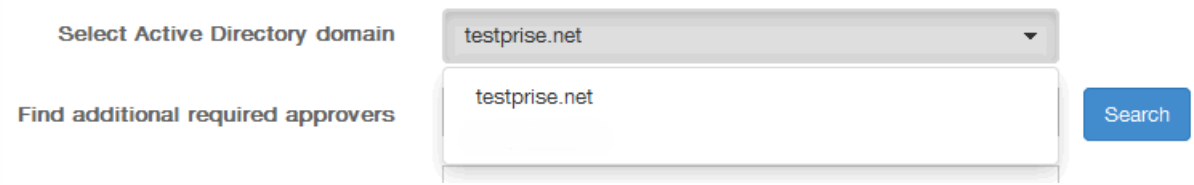
© 1999-2017 Citrix Systems, Inc. All rights reserved.



14. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur.
    1. Spécifiez un **nom** pour le workflow.
    2. Éventuellement, entrez une **description**.
    3. Dans le champ **Modèles d'approbation d'e-mail**, cliquez sur une option de notification. Cliquez sur l'icône d'œil pour afficher un aperçu du modèle choisi.



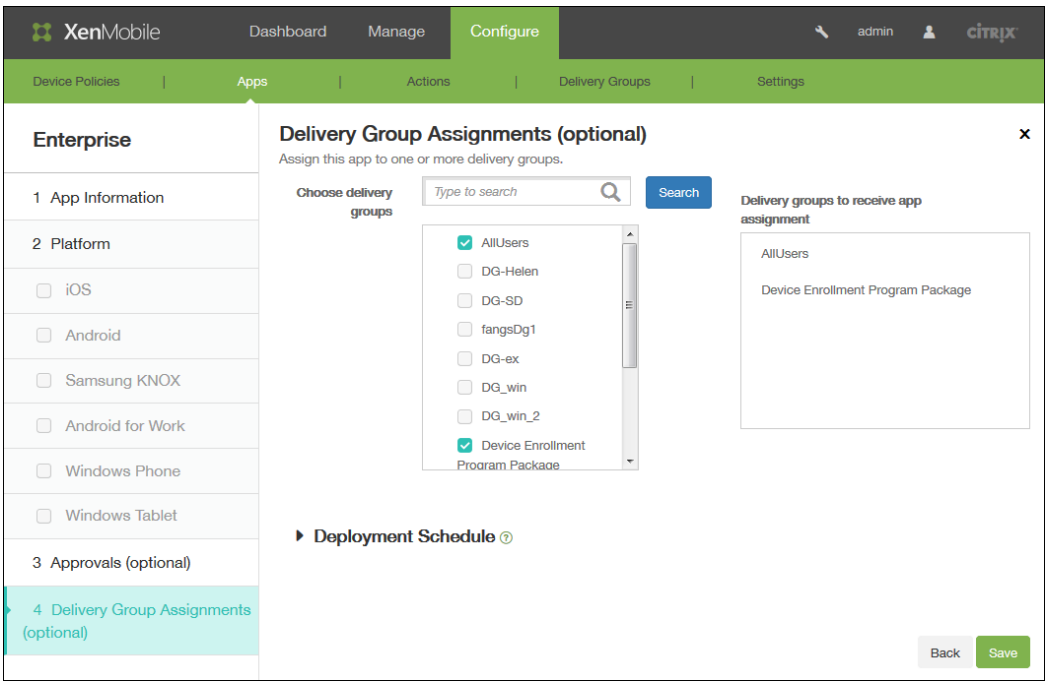
    4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3.
    5. Dans **Sélectionner un domaine Active Directory**, sélectionnez le domaine dans le menu déroulant ; seuls les domaines Active Directory apparaissent dans cette liste (par exemple, testprise.net) :



© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

15. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez l'application à un ou plusieurs groupes de mise à disposition.



16. Dans Choisir des groupes de mise à disposition, recherchez un groupe de mise à disposition (ou des groupes.) Sélectionnez la case à cocher **Tous les utilisateurs** pour attribuer l'application à chaque utilisateur XenMobile.
17. Développez Calendrier de déploiement pour affiner le groupe de mise à disposition.
    1. Déployer : cliquez sur ON pour activer un calendrier de déploiement.
    2. Calendrier de déploiement : cliquez sur Maintenant ou Plus tard pour définir la planification du déploiement.
    3. Conditions de déploiement : cliquez pour déployer l'application sur chaque connexion, ou uniquement lorsque le déploiement précédent a échoué.
    4. Dans Déployer pour les connexions permanentes, cliquez sur ON pour procéder au déploiement lorsque la stratégie de connexion permanente est définie.
       Remarque : cette option s'applique lorsque vous avez également configuré des clés de déploiement d'arrière-plan globales dans la section Paramètres des propriétés du serveur de la console XenMobile. La stratégie de calendrier permanent n'est pas disponible pour iOS.
18. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour ajouter un lien Web applicatif à XenMobile

Jul 25, 2016

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).

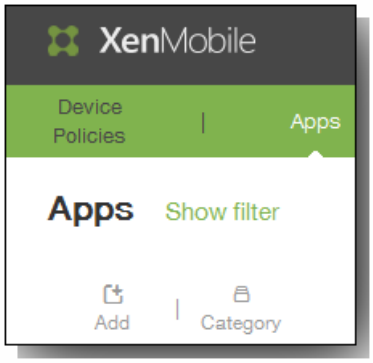
Vous pouvez configurer des liens Web dans l'onglet Applications de la console XenMobile. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau répertoriant les applications. Lorsque les utilisateurs ouvrent une session avec Worx Home, le lien 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)

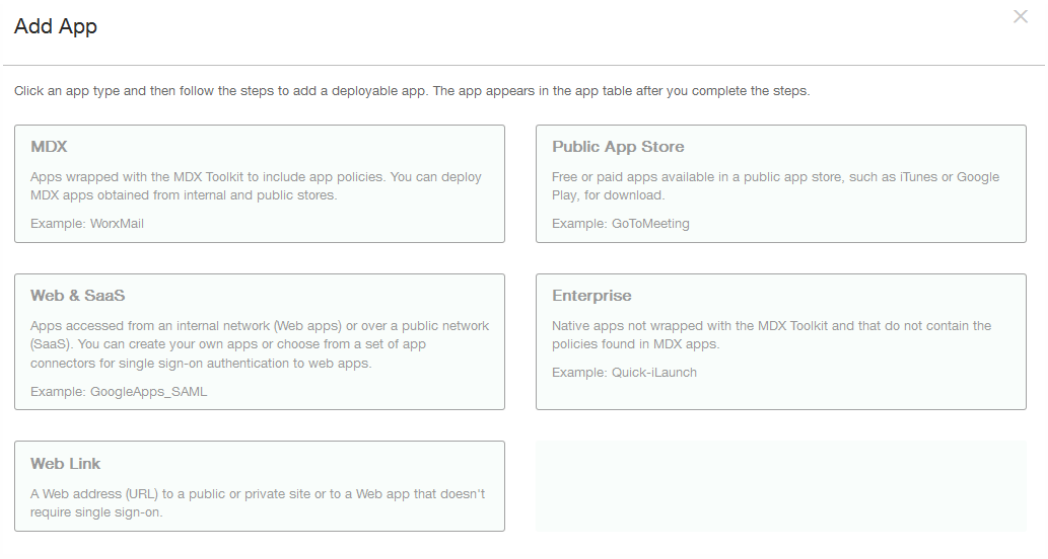
Pour ajouter un lien Web dans XenMobile

1. Configurer > Applications. La page Applications s'ouvre.
2. Sur la page Applications, cliquez sur Ajouter.



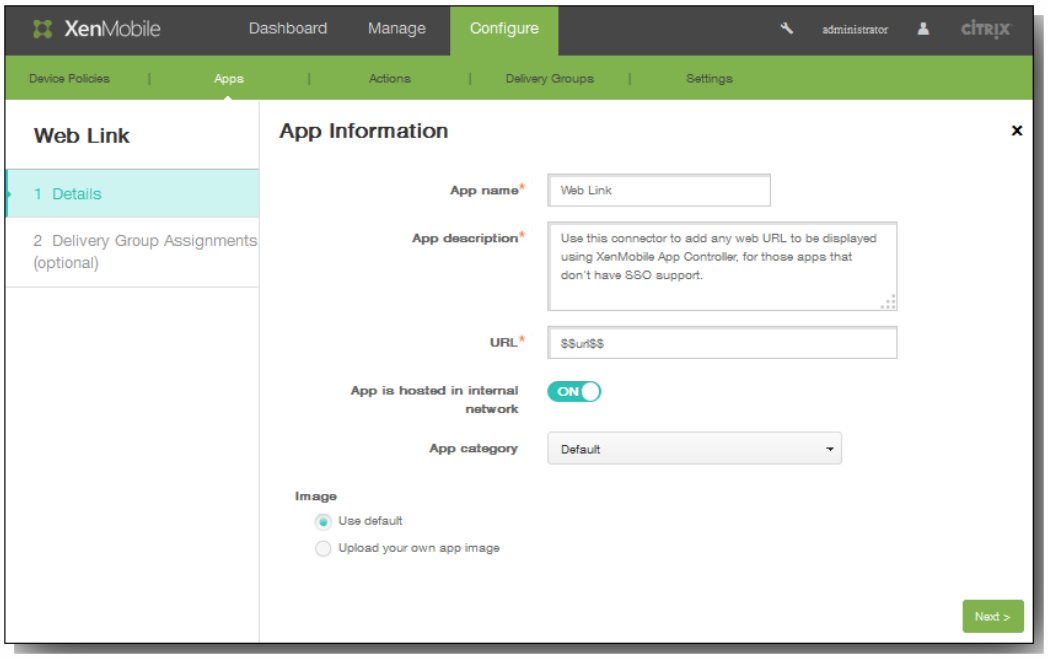
3. Sur la page Ajouter une application, cliquez sur Lien Web.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



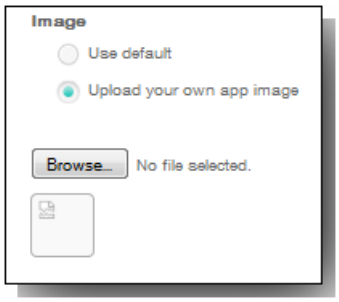
La page Informations sur l'application s'affiche.

4. Les champs Nom app, Description et URL sont pré-remplis.



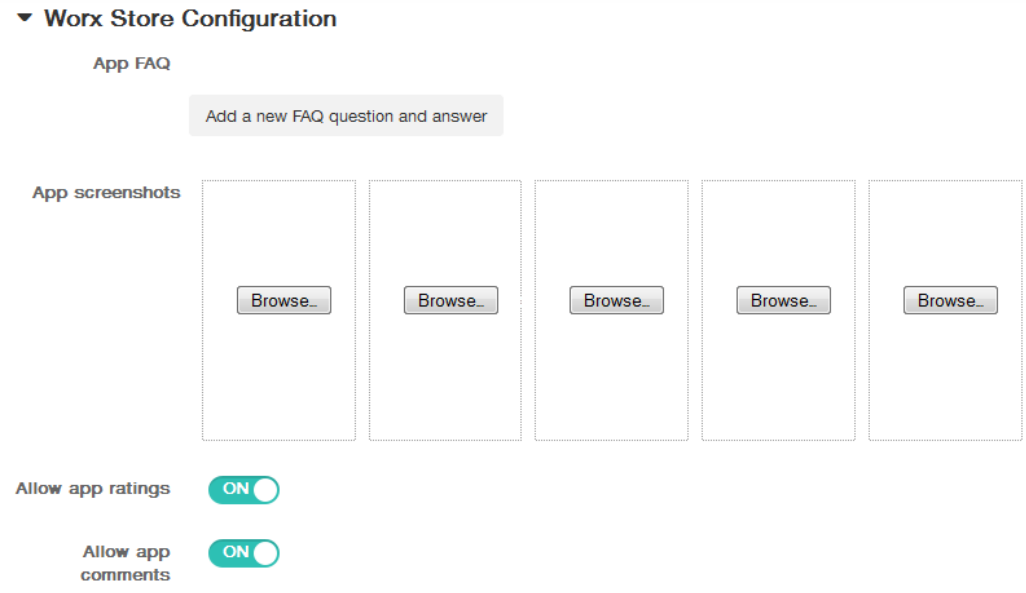
1. Le cas échéant, dans le champ URL, entrez l'adresse Web de l'application ou conservez l'adresse par défaut.
2. Sélectionnez L'application est hébergée dans le réseau interne et cliquez sur ON si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à 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.
3. Dans la liste Catégorie d'application, cliquez sur une catégorie.
4. Si vous souhaitez associer votre propre image miniature au connecteur, sélectionnez Charger votre propre image d'application. Cliquez sur Parcourir pour accéder à l'image voulue :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Les images doit être de type PNG.

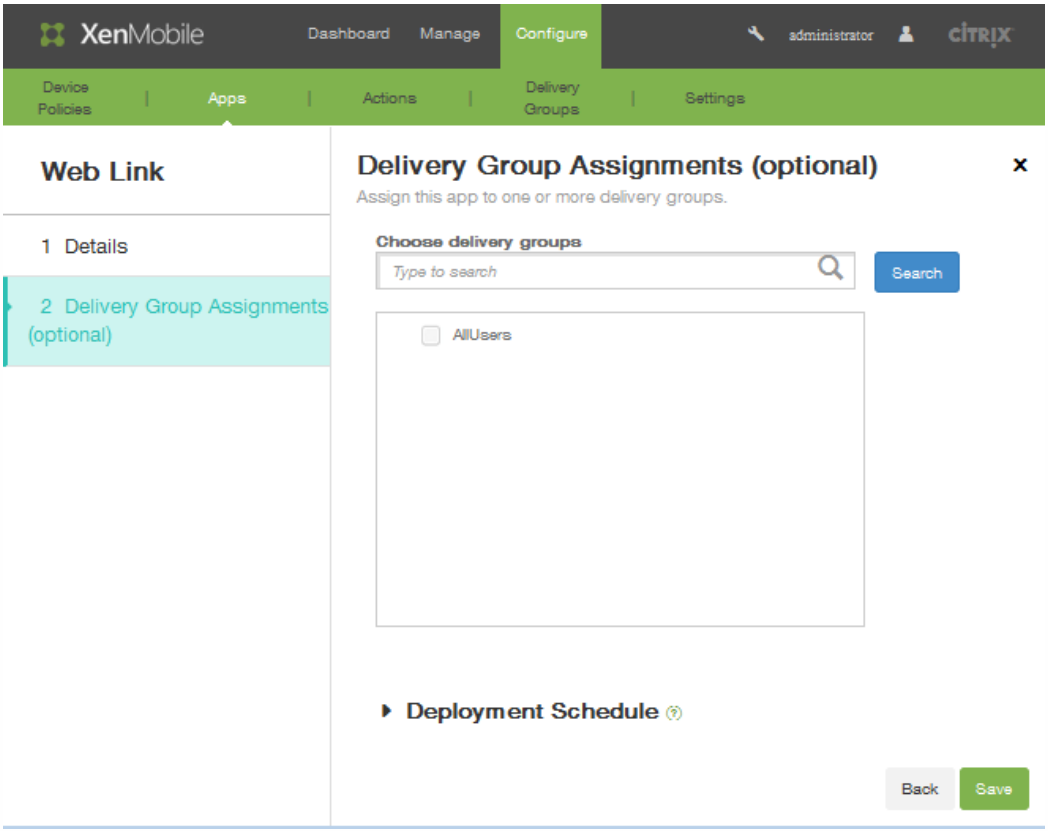
5. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



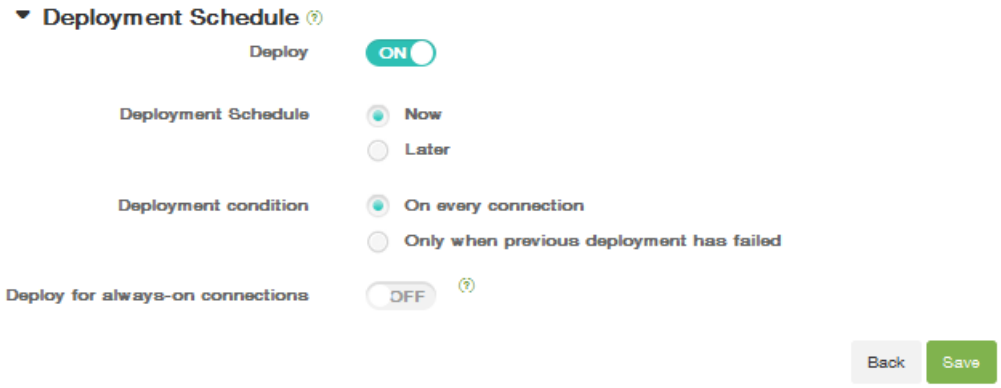
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

6. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
7. Cliquez sur Suivant.
8. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez l'application à un ou plusieurs groupes de mise à disposition.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. Dans Choisir des groupes de mise à disposition, recherchez un groupe de mise à disposition (ou des groupes.) Sélectionnez la case à cocher **Tous les utilisateurs** pour attribuer l'application à chaque utilisateur XenMobile.
10. Développez Calendrier de déploiement pour affiner le groupe de mise à disposition.



1. Déployer : cliquez sur ON pour activer un calendrier de déploiement.
2. Calendrier de déploiement : cliquez sur Maintenant ou Plus tard pour définir la planification du déploiement.
3. Conditions de déploiement : cliquez pour déployer l'application sur chaque connexion, ou uniquement lorsque le déploiement précédent a échoué.
4. Dans Déployer pour les connexions permanentes, cliquez sur ON pour procéder au déploiement lorsque la stratégie de connexion permanente est définie.
   Remarque : cette option s'applique lorsque vous avez également configuré des clés de déploiement d'arrière-plan globales dans la section Paramètres des propriétés du serveur de la console XenMobile. La stratégie de calendrier permanent n'est pas disponible pour iOS.
11. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Création et gestion de workflows

Jul 25, 2016

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.

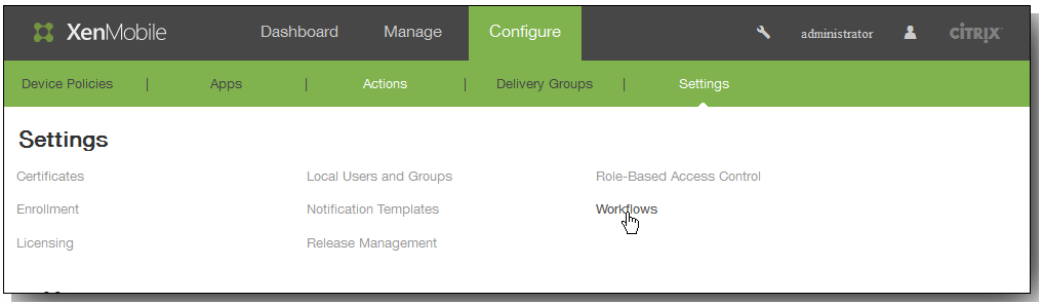
Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres de messagerie de workflow. Il est indispensable de configurer les paramètres de messagerie de workflow pour utiliser les workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces paramètres incluent le serveur de messagerie, le port, l'adresse e-mail et si la demande de création du compte utilisateur requiert ou non une approbation.

Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

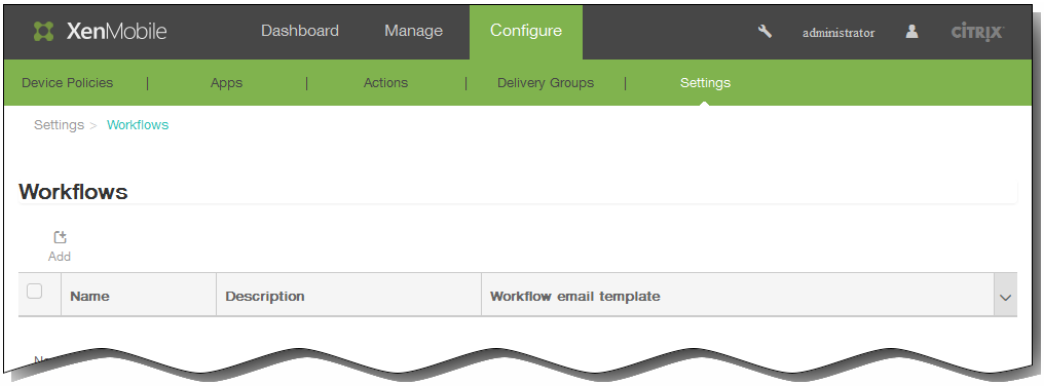
- Dans la page Workflows sur la console XenMobile. Sur la page Workflows, vous pouvez configurer plusieurs workflows à utiliser pour la configuration d'applications. Lorsque vous configurez des workflows sur la page Workflows, vous pouvez sélectionner le workflow lors de la configuration de l'application.
- 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 les rechercher et les sélectionner. 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 Configurer > Paramètres > Workflows.

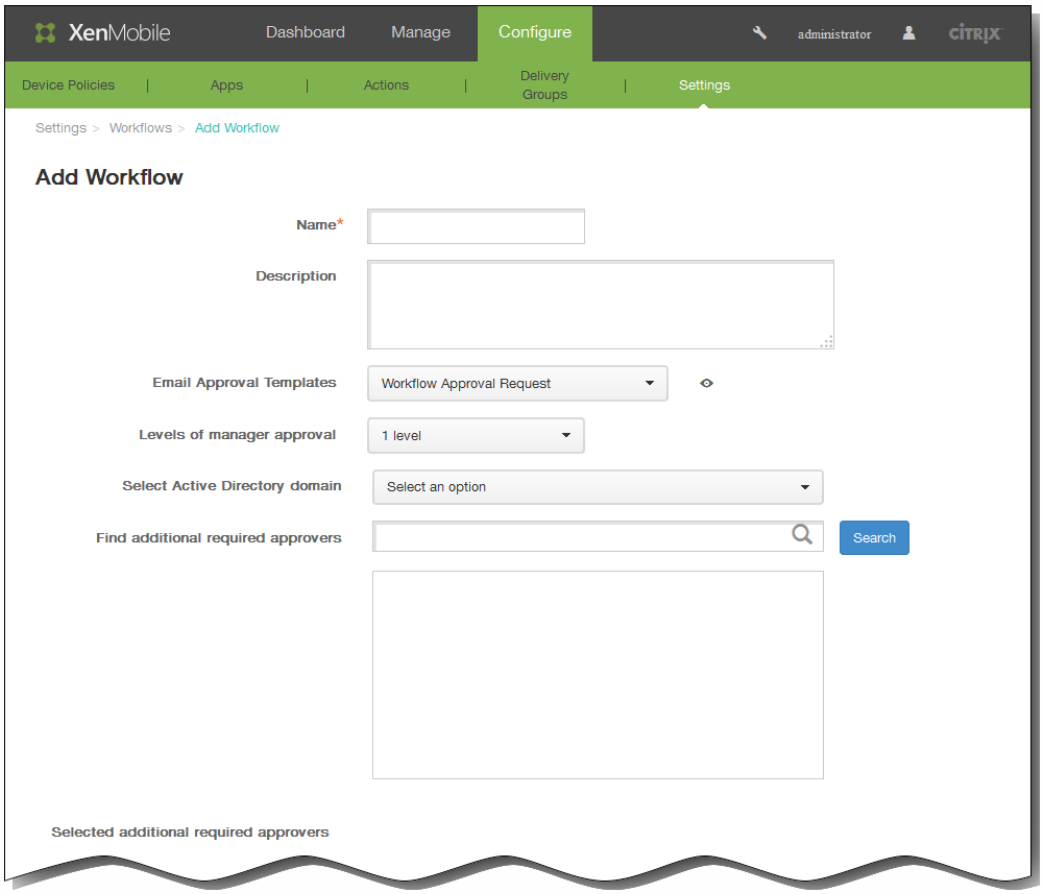


© 1999-2017 Citrix Systems, Inc. All rights reserved.



La page Workflows s'affiche.

2. Sur la page Workflows, cliquez sur Ajouter. La page Ajouter un workflow s'affiche.



3. Sur la page Ajouter un workflow, dans le champ Nom, entrez un nom unique pour le workflow.
4. Dans le champ Description, entrez une description pour le workflow (facultatif).
5. Dans la liste Modèles d'approbation d'e-mail, 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, le conseil suivant s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Dans la liste Niveaux d'approbation par un responsable, sélectionnez le nombre de niveaux d'approbation par un responsable requis pour ce workflow.
7. Dans la liste Sélectionner un domaine Active Directory, sélectionnez le domaine Active Directory à utiliser pour le workflow.
8. En regard de 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.
9. 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.
10. 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 Supprimer.
   Important : vous ne pouvez pas annuler cette opération.

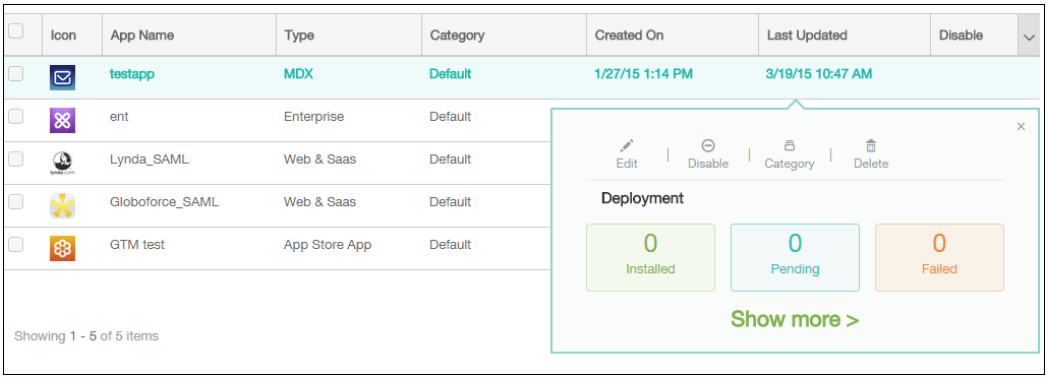
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Mise à niveau d'une application dans XenMobile

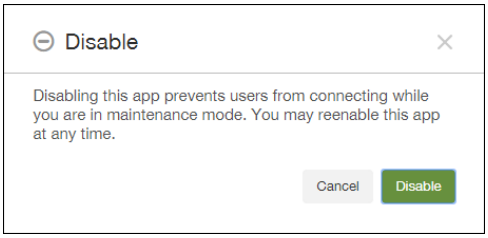
Jul 25, 2016

Pour mettre à niveau une application 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.
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 :
   1. Dans le tableau des applications, choisissez l'application que vous souhaitez mettre à jour puis dans le menu qui s'affiche, cliquez sur Désactiver.



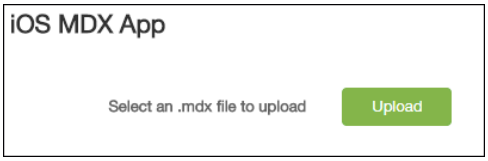
   2. Dans la boîte de dialogue de confirmation, cliquez sur Désactiver.



   Dans le tableau des applications, l'application est marquée Désactivée.

   Remarque : l'application désactivée passe en mode de maintenance. Quand l'application est désactivée, les utilisateurs ne pourront plus s'y connecter une fois la session fermée. La désactivation d'applications est un paramètre facultatif, mais Citrix recommande de désactiver l'application pour éviter les problèmes avec la fonctionnalité de l'application. Le problème peut 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. Cliquez pour sélectionner l'application, puis dans le menu qui s'affiche, cliquez sur Modifier. La plate-forme que vous avez choisie pour l'application apparaît comme étant sélectionnée.
4. Sur la page Informations sur l'application, vous pouvez modifier le Nom, la Description ou la Catégorie d'application, puis cliquez sur Suivant.
5. Cliquez sur Charger pour sélectionner le fichier que vous souhaitez charger pour remplacer l'application actuelle, puis cliquez sur Suivant.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



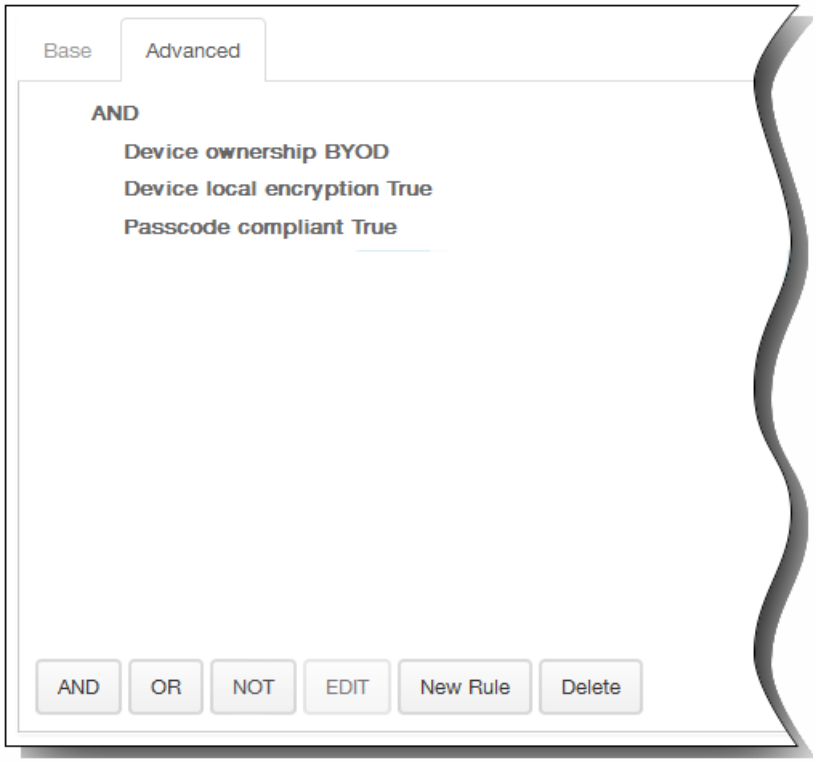
L'application se charge dans XenMobile. Si vous le souhaitez, vous pouvez modifier les détails de l'application et les paramètres de stratégie.

6. Cliquez sur Suivant, puis dans les étapes 8 à 14, laissez les paramètres par défaut ou modifiez ceux liés à la mise à niveau.
7. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

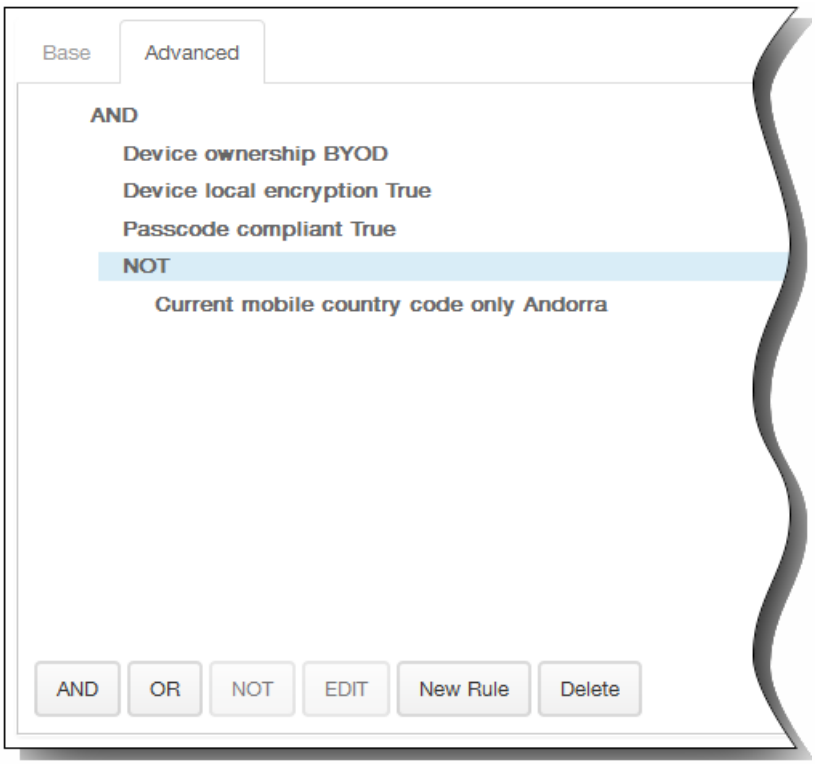
© 1999-2017 Citrix Systems, Inc. All rights reserved.



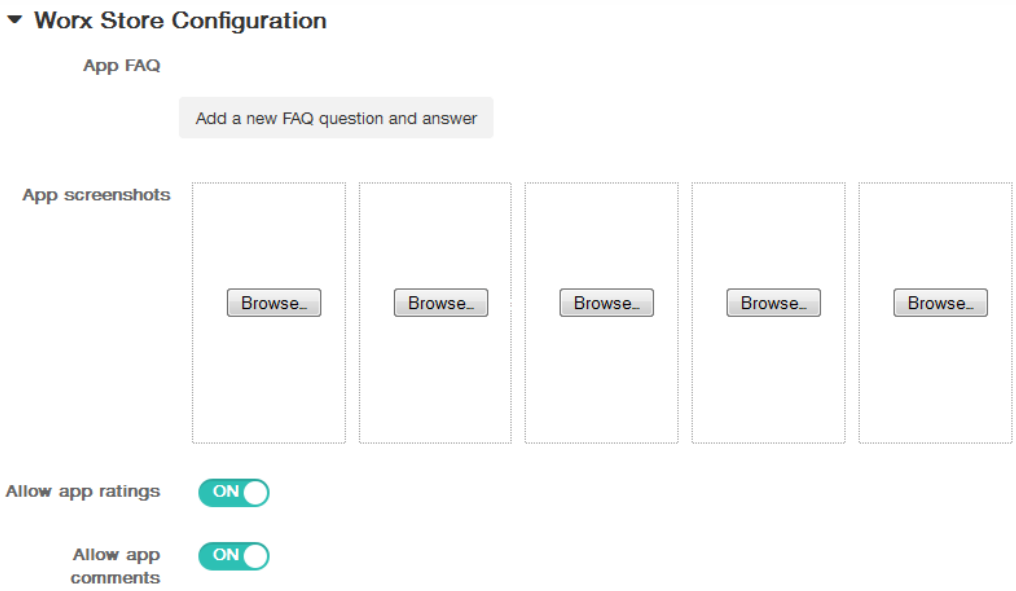
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.
   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai, l'appareil doit se conformer aux exigences en matière de code secret et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



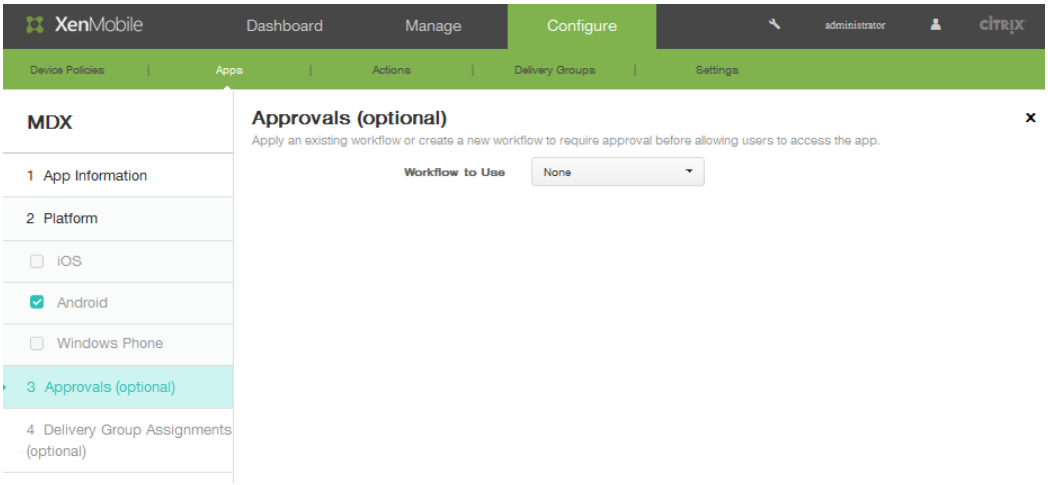
8. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



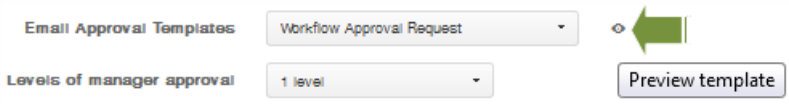
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

9. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
10. Cliquez sur Suivant. L'écran Approbations s'affiche.

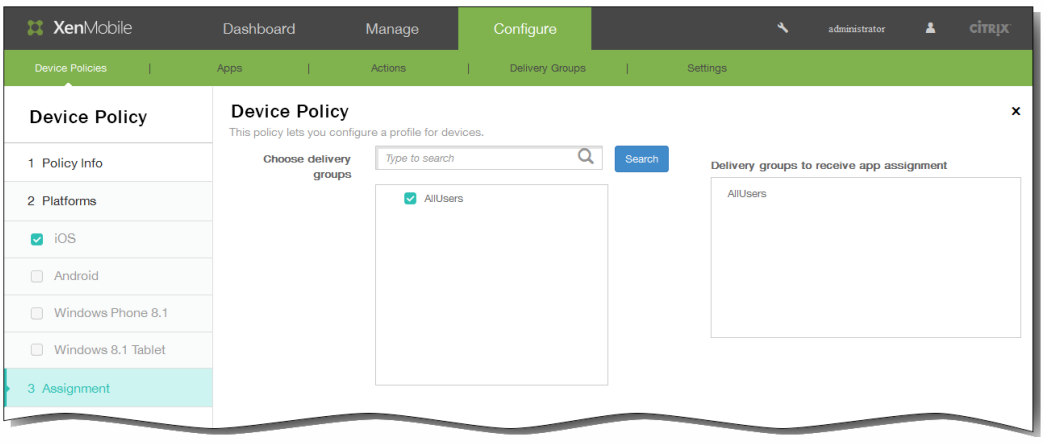
© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer des comptes d'utilisateurs.
    1. Spécifiez un **nom** pour le workflow.
    2. Éventuellement, entrez une **description**.
    3. Dans le champ **Modèles d'approbation d'e-mail**, cliquez sur une option de notification. Cliquez sur **l'icône** d'œil pour afficher un aperçu du modèle choisi.

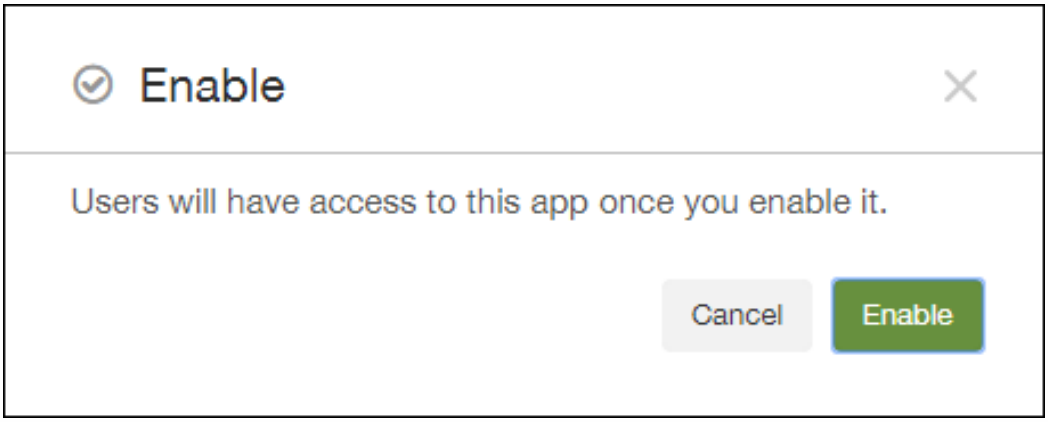


    4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3. .
    5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
    6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.
12. Cliquez sur Suivant.
13. 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

14. Cliquez sur Enregistrer. La page Applications s'affiche.
15. Si vous avez désactivé l'application à l'étape 2, effectuez les opérations suivantes :
    1. Dans le tableau des Applications, choisissez l'application que vous avez mis à jour puis dans le menu qui s'affiche, cliquez sur Activer.
    2. Dans le message 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Synopsis des stratégies applicatives MDX

Jul 25, 2016

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.

Remarque : Worx Home actualise les stratégies au cours de certaines actions. Pour de plus amples informations, consultez la section Worx Home.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration de XenMobile et de l'application ShareFile pour l'authentification unique à l'aide de SAML

Oct 11, 2016

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 Worx Home 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 WorxMail 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 guide 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
- Worx Home 9.0 (pour applications mobiles ShareFile)
  Installez la version iOS ou Android appropriée.
- Compte d'administrateur ShareFile

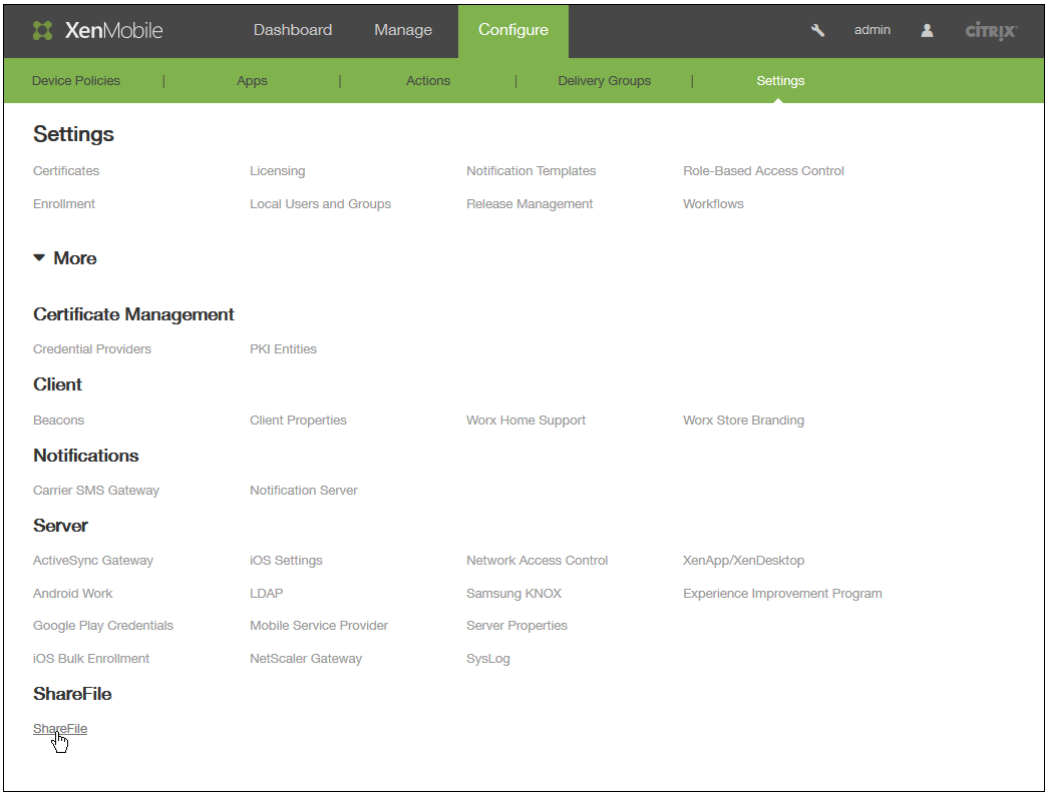
Assurez-vous que XenMobile et ShareFile peuvent se connecter. Pour de plus amples informations sur la vérification de la connectivité, consultez la section Réalisation de contrôles de connectivité.

Configurer l'accès à ShareFile

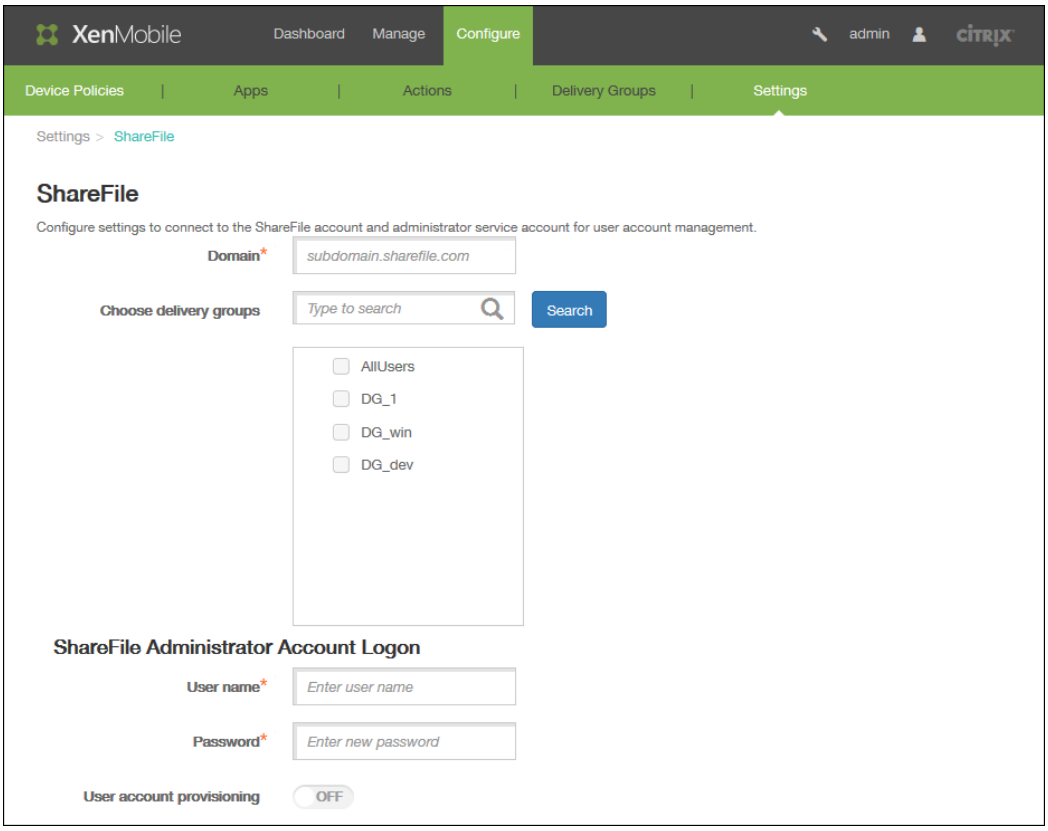
Avant de configurer SAML pour ShareFile, indiquez les informations d'accès à ShareFile comme suit :

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres. La page Paramètres s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Cliquez sur Plus, puis sous ShareFile, cliquez sur ShareFile. La page de configuration de ShareFile s'affiche.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Configurez les paramètres suivants :
   - Domaine : tapez votre nom de sous-domaine ShareFile, par exemple exemple.sharefile.com.
   - Choisir des 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.
   - 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.
4. 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 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 dans Configurer l'accès à ShareFile.
4. Assurez-vous que le même fuseau horaire est configuré pour ShareFile et XenMobile.
   Remarque : des fuseaux horaires différents peuvent se traduire par des horodatages incohérents, ce qui entraîne l'échec de l'authentification unique.

Valider l'application mobile ShareFile

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Worx Home.
2. À partir de Worx 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 WorxMail

1. Sur la machine utilisateur, si cela n'a pas déjà été fait, installez et configurez Worx Home.
2. À partir de Worx Store, téléchargez, installez et configurez WorxMail.
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.

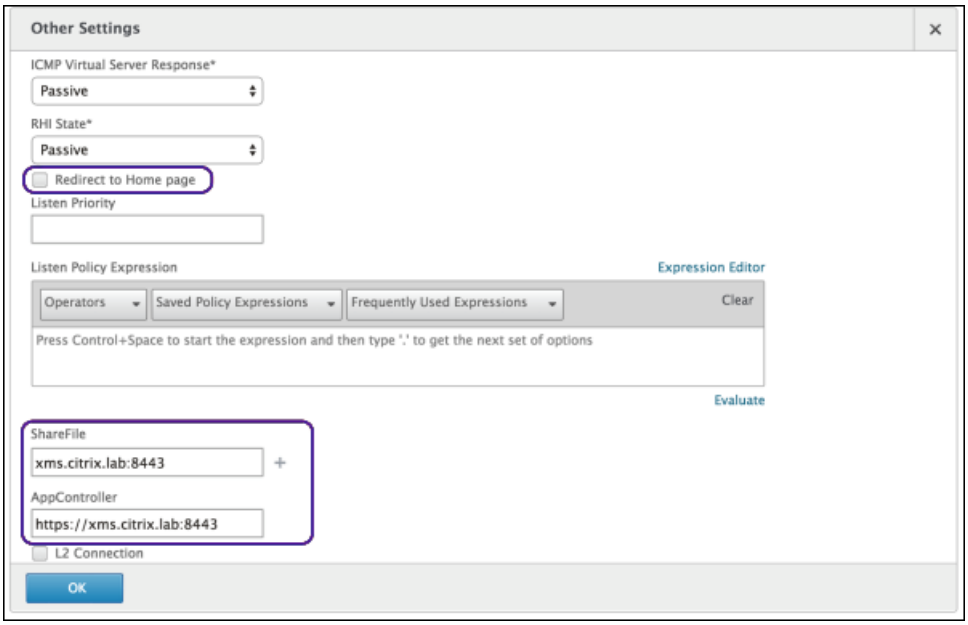
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.



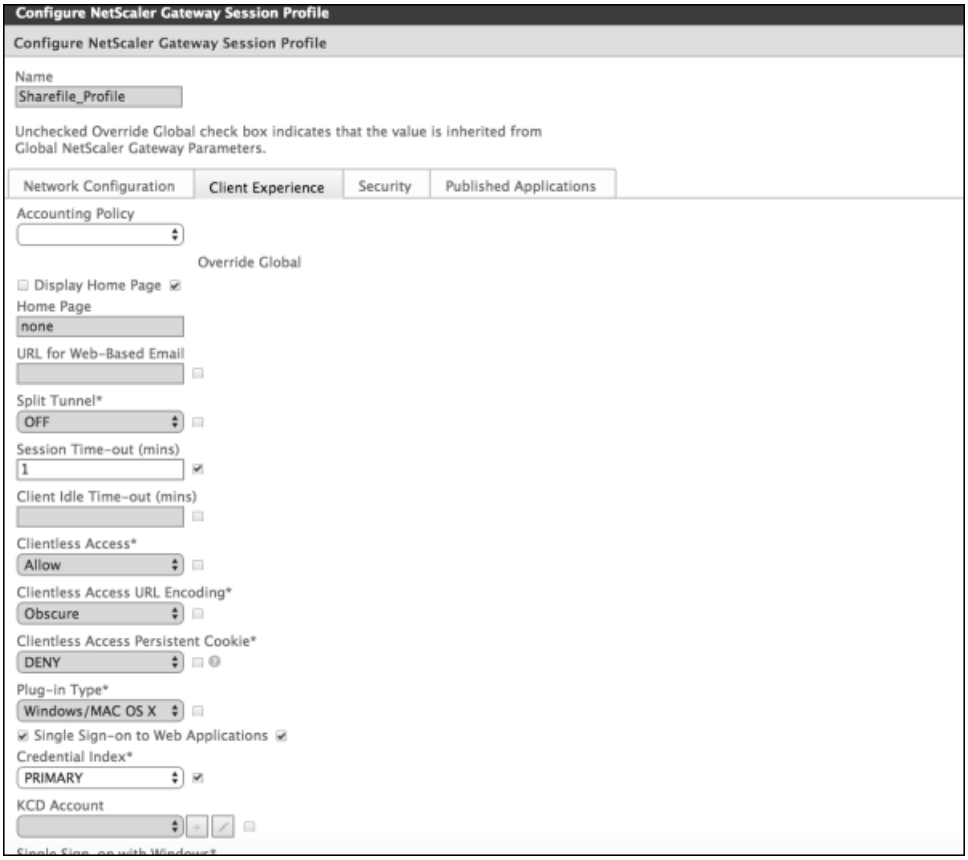
2. Sous ShareFile, tapez le nom de votre serveur interne XenMobile et le numéro de port.
3. Sous AppController, tapez l'URL de votre serveur XenMobile.
   Cette configuration autorise les demandes pour l'URL indiquée via le chemin d'accès /cginfra.

Créer une stratégie et un profil de demande de session ShareFile

Configurez les paramètres suivants pour créer une stratégie et un profil de demande de session ShareFile :

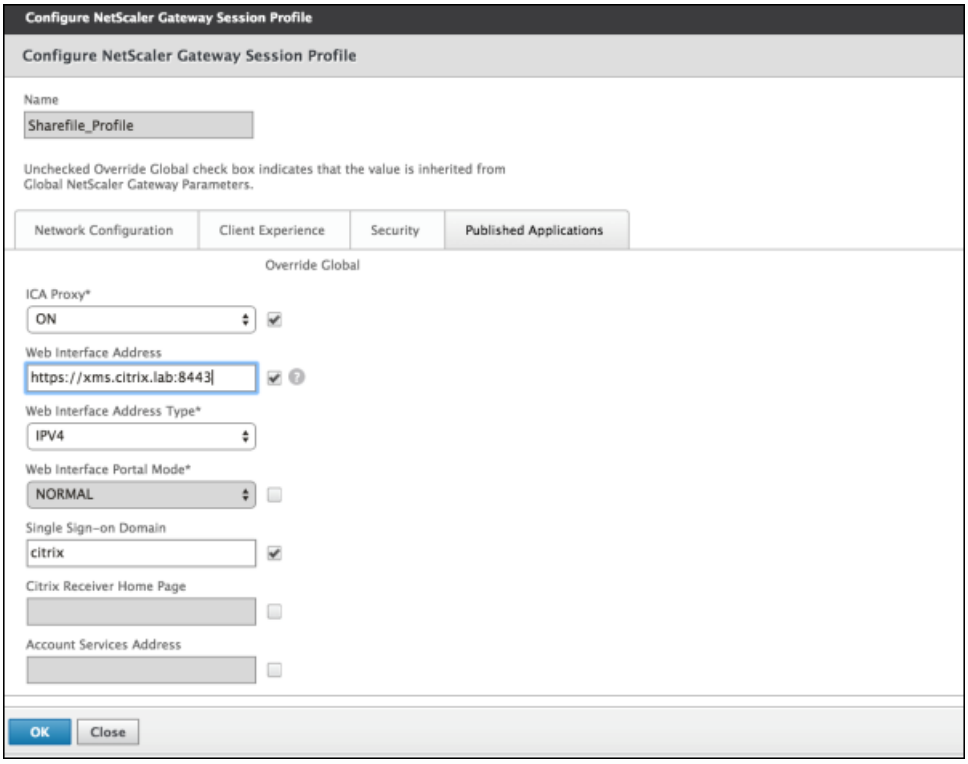
1. Dans l'utilitaire de configuration de NetScaler Gateway, dans le volet de navigation de gauche, cliquez sur NetScaler Gateway > Policies > Session.
2. Créez une stratégie de session. Dans l'onglet Policies, cliquez sur Add.
3. Dans le champ Name, tapez ShareFile_Policy.
4. Créez une action en cliquant sur le bouton +.
   L'écran Create NetScaler Gateway Session Profile s'affiche. Configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



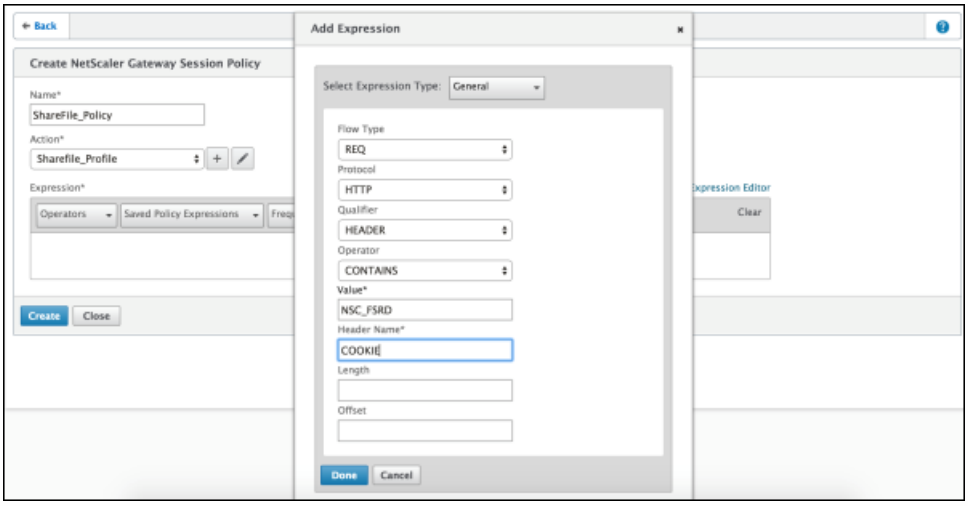
1. Name : tapez ShareFile_Profile.
2. Cliquez sur l'onglet Client Experience, puis configurez les paramètres suivants :
    1. Home Page : tapez none.
    2. Session Time-out (mins) : tapez 1.
    3. Single Sign-on to Web Applications : sélectionnez ce paramètre.
    4. Credential Index : dans la liste, cliquez sur PRIMARY.
3. Cliquez sur l'onglet Published Applications, puis configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Proxy ICA : dans la liste, sélectionnez ON.
2. Web Interface Address : entrez l'URL de votre serveur XenMobile.
3. 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, puis configurez les paramètres suivants :



1. Value : tapez NSC_FSRD.
2. Header Name : tapez COOKIE.
3. Cliquez sur Done.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

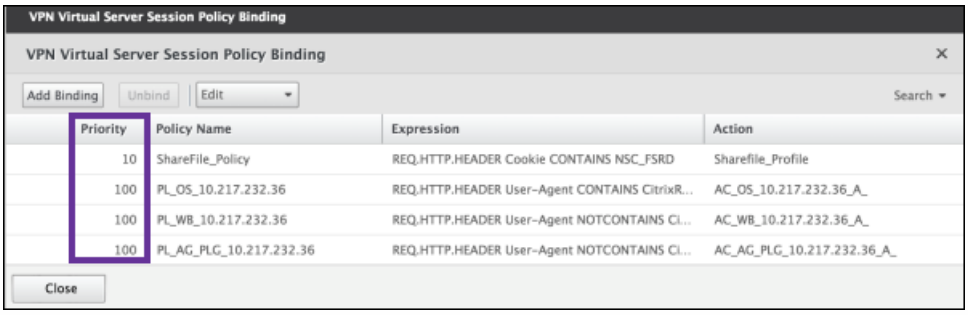
7. Cliquez sur Create, puis sur Close.



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 Détails, cliquez sur votre serveur virtuel NetScaler Gateway.
3. Cliquez sur Modifier.
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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

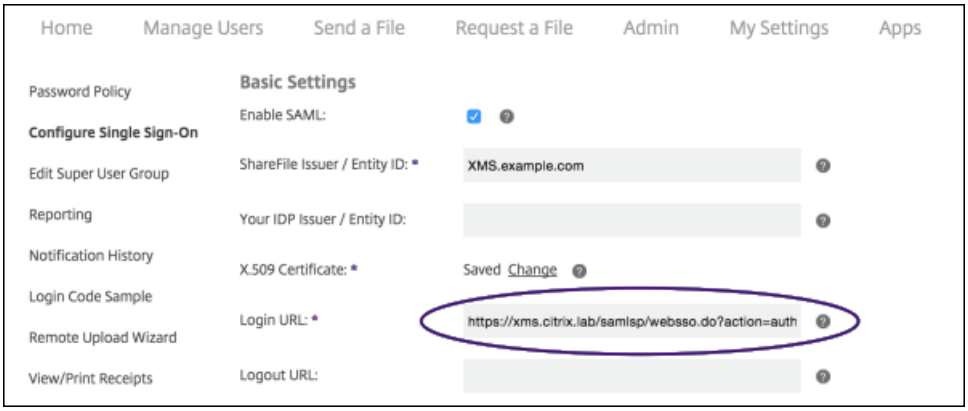


3. Cliquez sur Applications > Applications et notez le nom de l'application (Application Name) correspondant à l'application avec le nom d'affichage (Display Name) « ShareFile ».



Modifier les paramètres d'authentification unique de ShareFile.com

1. Ouvrez une session sur votre compte ShareFile (https://.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.



1. Insérez le nom de domaine complet (FQDN) externe du serveur virtuel de NetScaler Gateway et « /cginfra/https/ »

© 1999-2017 Citrix Systems, Inc. All rights reserved.

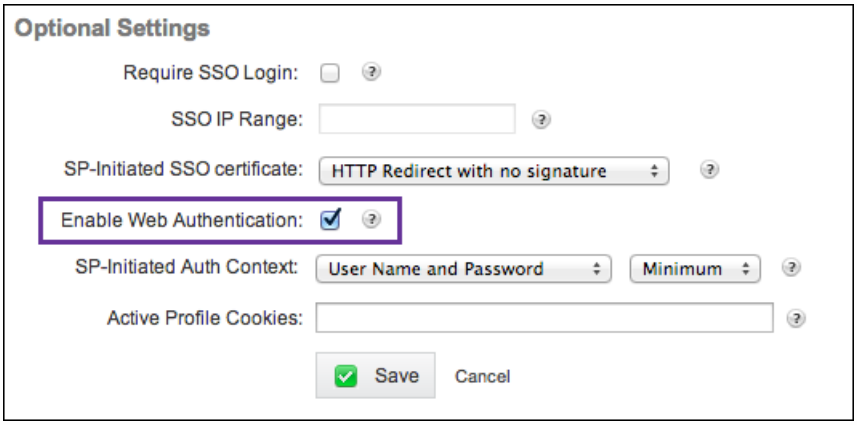
devant le nom de domaine complet du serveur XenMobile, puis ajoutez « 8443 » après le nom de domaine complet de XenMobile.
L'URL doit maintenant ressembler à ce qui suit :
https://**nsgateway.acme.com/cginfra/https**/xms.citrix.lab:**8443**/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

2. Remplacez le paramètre **&app=ShareFile_SAML_SP** par le nom interne de l'application ShareFile indiqué à l'étape 3 dans Configurer SAML pour les applications ShareFile non MDX. 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

3. 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.



5. Cliquez sur Enregistrer.

Valider la configuration

Procédez comme suit pour valider la configuration.

1. Dans votre navigateur, accédez à https://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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configuré.
Vos dossiers ShareFile à l'adresse .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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Actions automatisées

Jul 25, 2016

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.

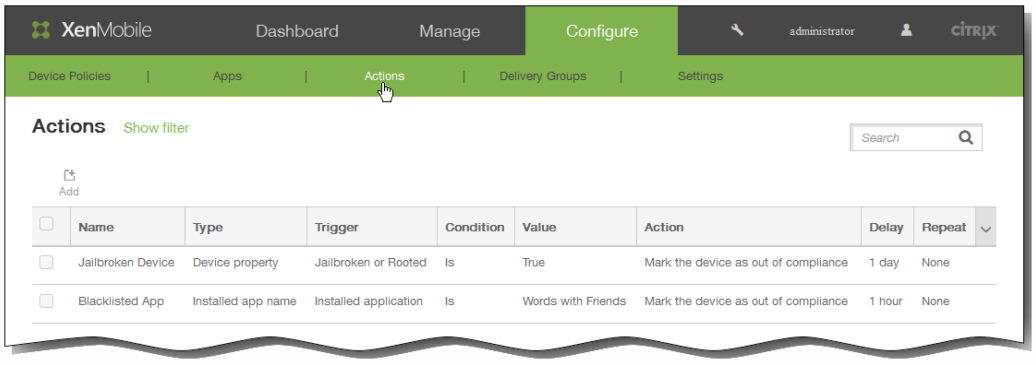
Les effets automatiques que vous pouvez paramétrer sont :

- 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.

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 la section 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.

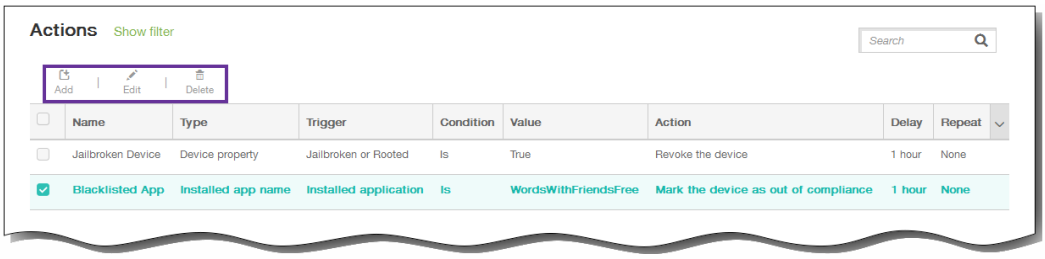
Cette rubrique explique comment ajouter, modifier et filtrer des actions automatisées dans XenMobile.

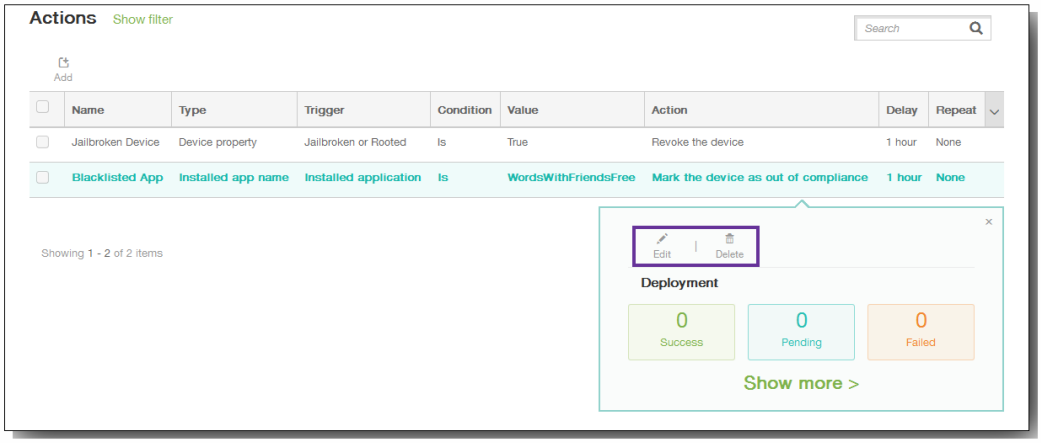
1. Dans la console XenMobile, cliquez sur Configurer > Actions. La page Actions s'affiche.



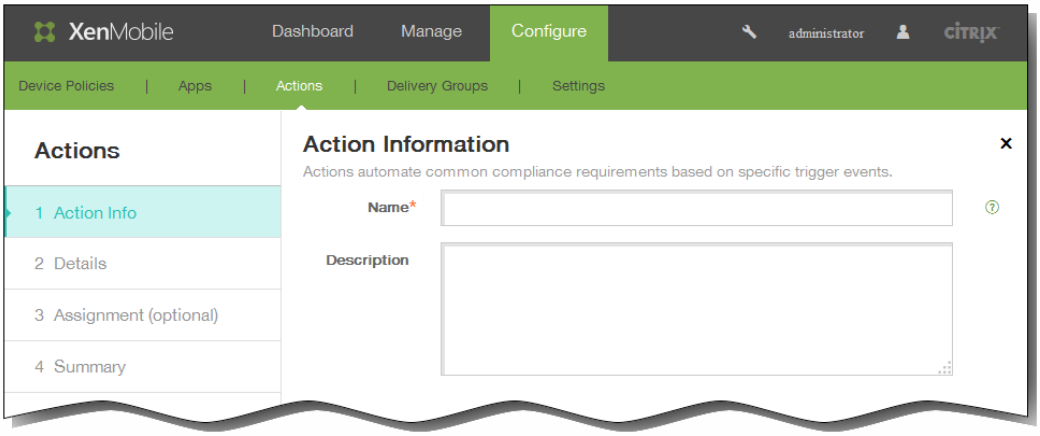
2. Sur la page Actions, effectuez l'une des actions suivantes :
   - Cliquez sur Ajouter pour ajouter une nouvelle action.
   - Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.
     Remarque : lorsque vous activez la case à cocher en regard d'une 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



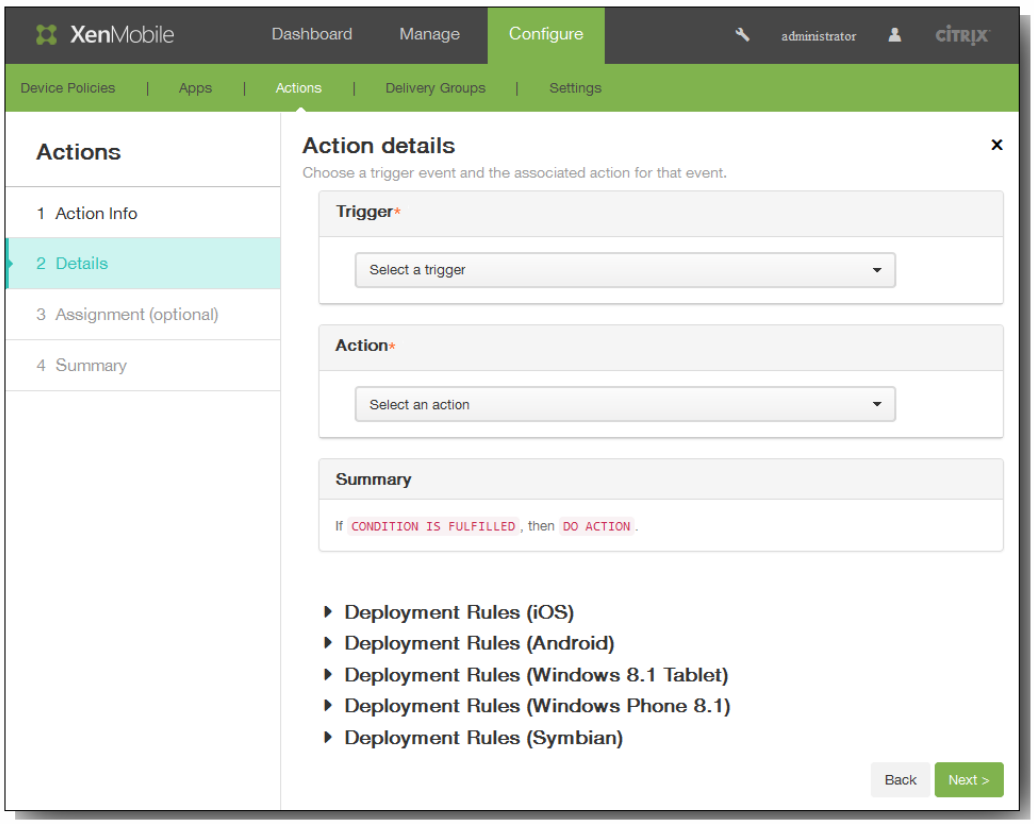


La page Informations sur l'action s'affiche.

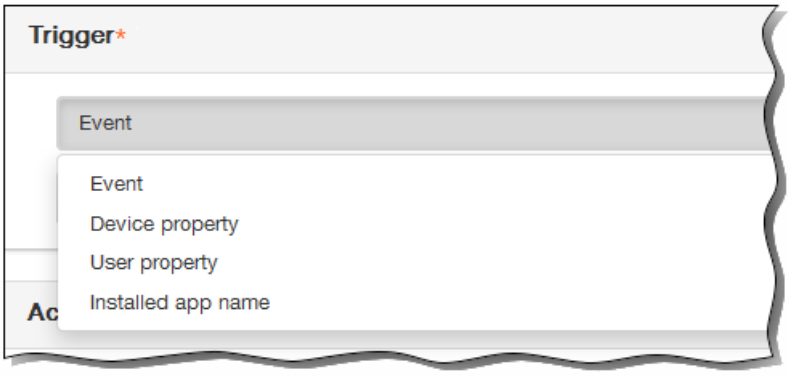


3. Sur la page Informations sur l'action, entrez ou modifiez les informations suivantes :
   1. Nom : entrez un nom permettant d'identifier de façon unique l'action. Ce champ est obligatoire.
   2. Description : décrivez ce que l'action doit faire.
4. Cliquez sur Suivant. La page sur les Détails de l'action 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

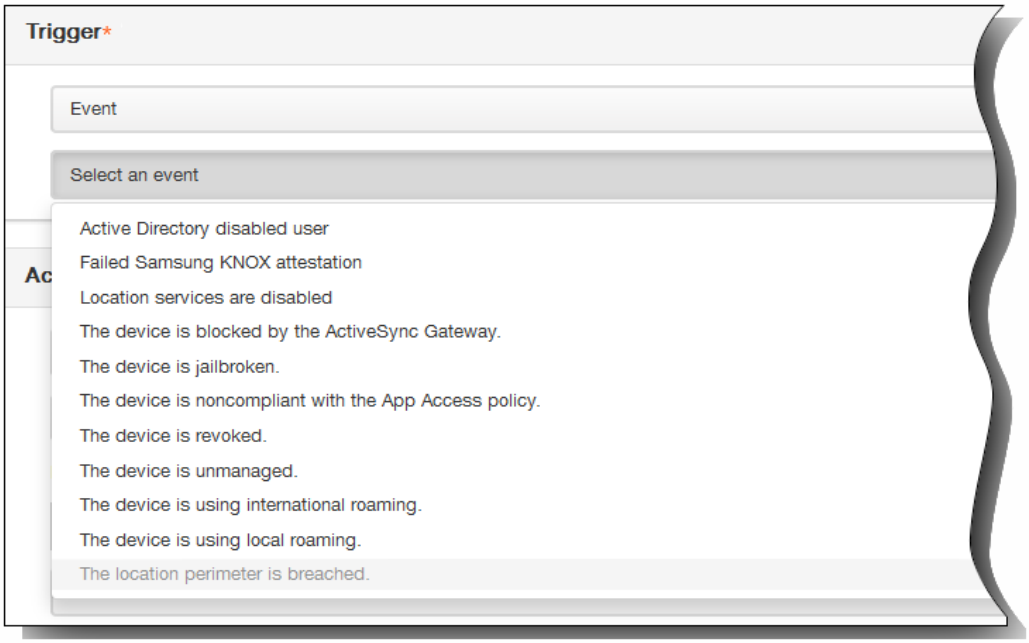


5. Sur la page Détails de l'action, entrez ou modifiez les informations suivantes :
   1. Dans la liste des Déclencheurs, cliquez sur le type de déclencheur d'événements pour cette action. Signification des déclencheurs :
      - Événement : réagit à un événement prédéfini.
      - Propriété de l'appareil : 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. 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.

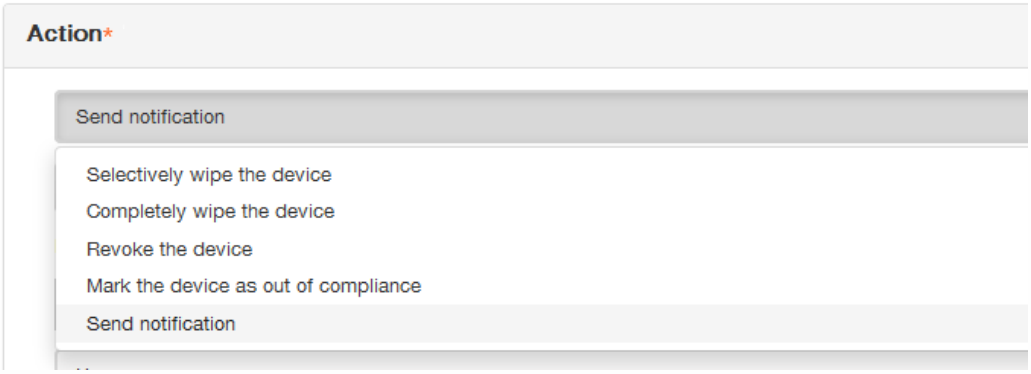


   2. Dans la liste suivante, cliquez sur la réponse au déclencheur.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



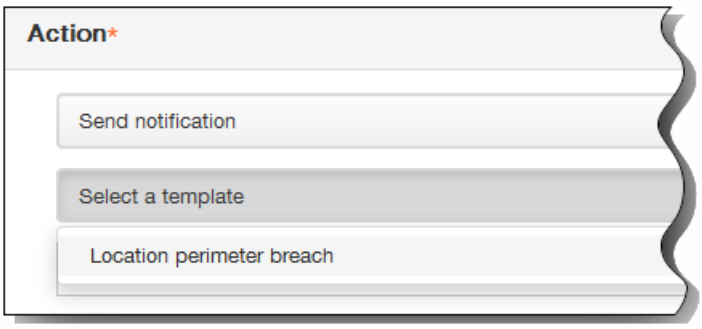
3. Dans la liste Action, cliquez sur l'action à effectuer lorsque le critère du déclencheur est rencontré. À l'exception de Envoyer une notification, vous choisissez un délai au cours duquel les utilisateurs devront avoir résolu le problème qui a activé le déclencheur. Si le problème n'est pas résolu dans ce délai, l'action sélectionnée est entreprise.



Le reste de cette procédure décrit comment envoyer une action de notification.

4. Dans la liste suivante, sélectionnez le modèle à utiliser pour la notification. Les modèles de notification correspondant à l'événement sélectionné apparaissent.
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 la section 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

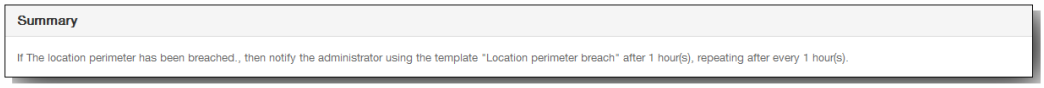


Remarque : après avoir sélectionné le modèle, vous pouvez afficher un aperçu de la notification en cliquant sur Aperçu du message de notification.

5. 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.

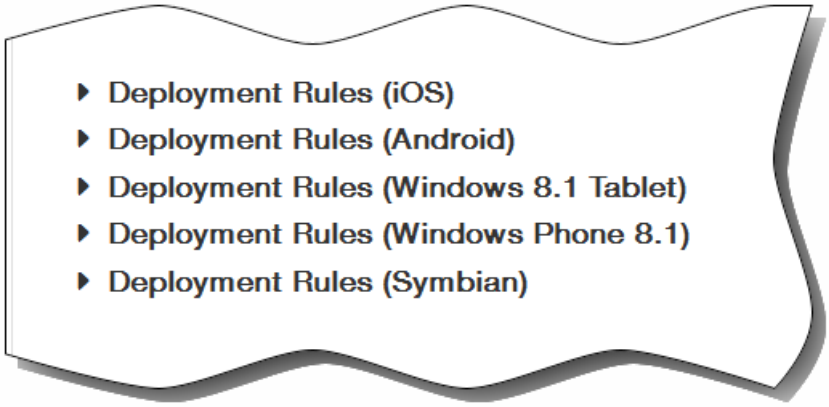


6. Dans Résumé, vérifiez que vous avez créé les actions automatisées comme prévu.



Après avoir configuré les détails de l'action, vous pouvez configurer des règles de déploiement pour chacune des plates-formes, iOS, Android, Windows 8.1 Tablet, Windows Phone 8.1 et Symbian. Pour ce faire, suivez les étapes 6 à 9 pour chacune des plates-formes que vous choisissez.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

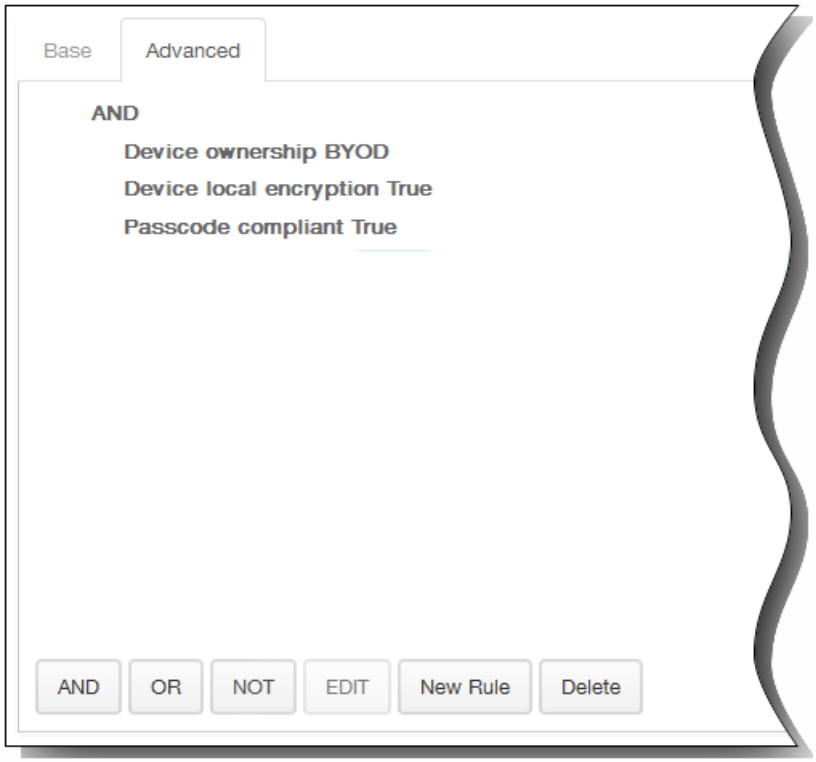


6. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.



1. Dans la liste, cliquez sur les options pour déterminer quand l'action doit être déployée.
    1. Vous pouvez déployer l'action lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les conditions.
    3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme illustré dans la figure qui précède.
    4. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions. Vous pouvez ajouter autant de conditions que vous le souhaitez.
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

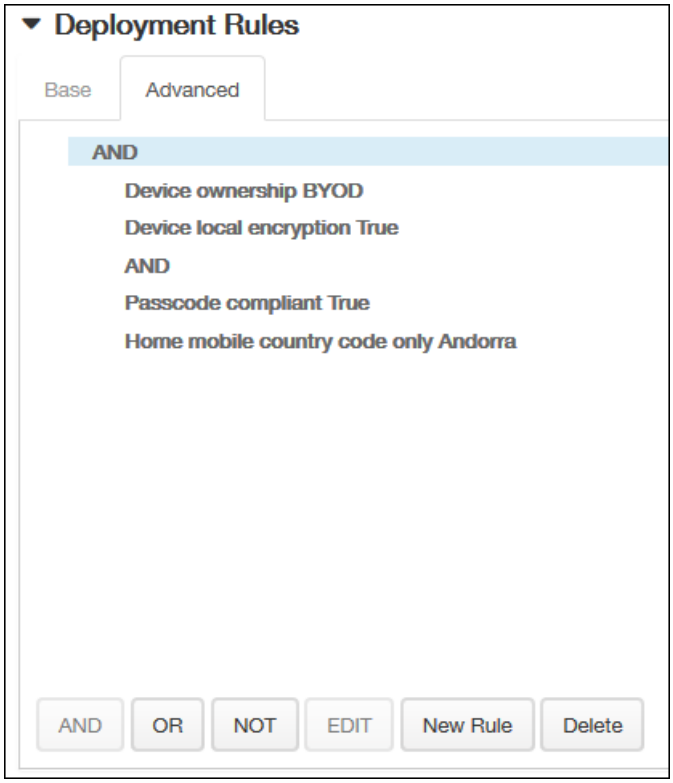


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

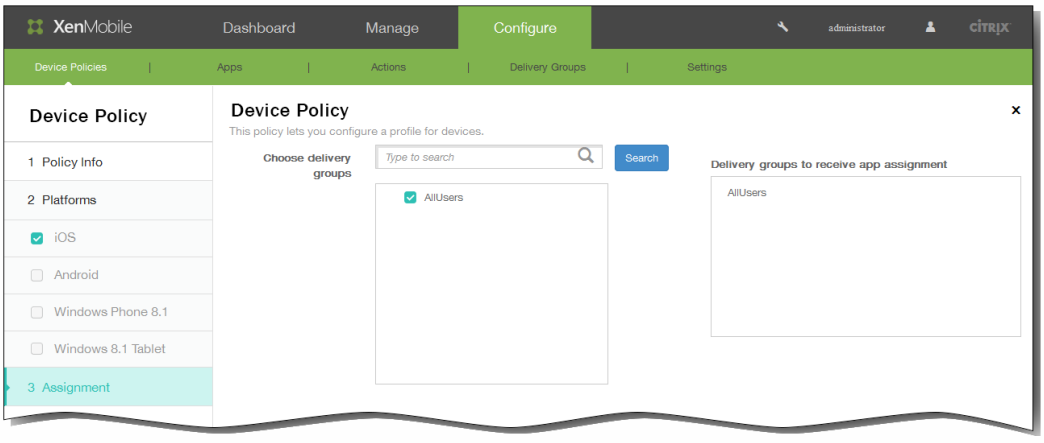
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      Vous pouvez à tout moment cliquer pour sélectionner une condition et cliquer sur MODIFIER pour modifier la condition ou sur Supprimer pour supprimer la condition.

   3. Cliquez sur Nouvelle règle de nouveau pour ajouter davantage de conditions.
      Dans cet exemple, le propriétaire doit être BYOD, le chiffrement sur l'appareil local doit être Vrai, l'appareil doit se conformer aux exigences en matière de code secret et l'indicatif de pays de l'appareil mobile ne peut pas être uniquement Andorre.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. 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.
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 de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

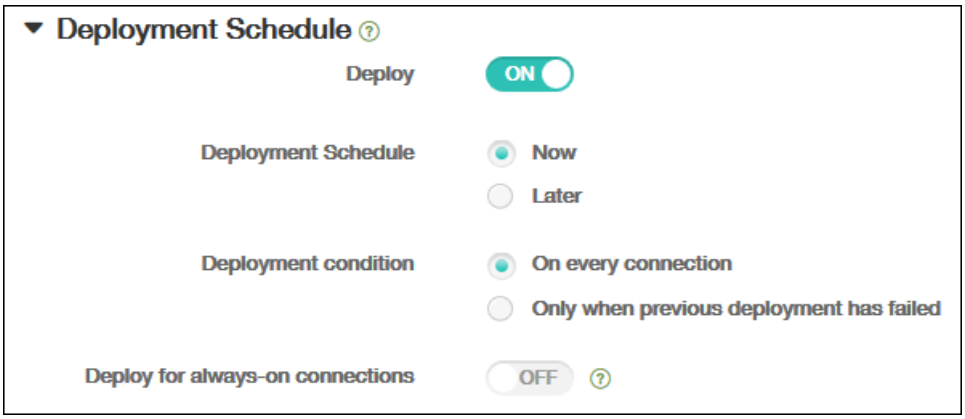


9. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    2. En regard de Calendrier de déploiement, cliquez sur Maintenant ou Plus tard. L'option par défaut est Maintenant.
    3. Si vous cliquez sur Plus tard, cliquez sur l'icône du calendrier, puis sélectionnez la date et l'heure pour le déploiement.

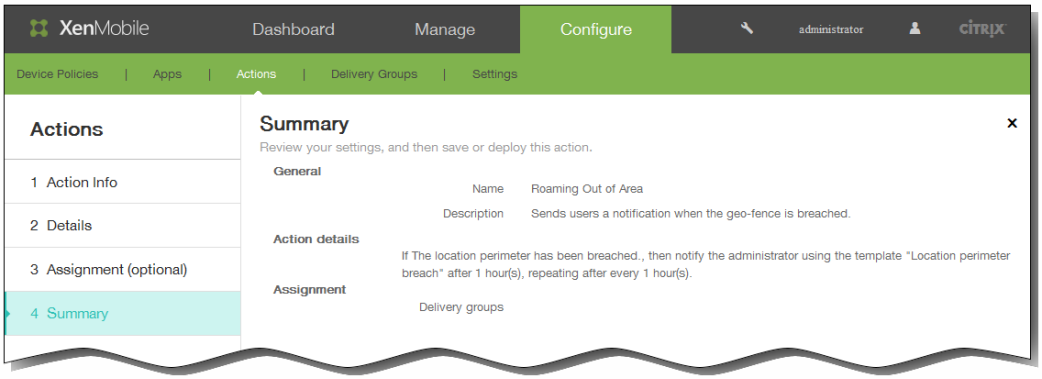
© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. 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.
5. 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.



10. Cliquez sur Suivant. La page Résumé s'affiche, où vous pouvez vérifier la configuration de l'action.



11. Cliquez sur Enregistrer pour enregistrer l'action.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Paramètres du client XenMobile

Jul 25, 2016

Vous pouvez configurer les paramètres du client XenMobile dans la console Web XenMobile.

1. Dans la console XenMobile, cliquez sur Configurer et sur Paramètres.
   La page Paramètres s'affiche.
2. Cliquez sur Plus.
3. Sous **Client**, cliquez sur l'option que vous souhaitez configurer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriété client

Jul 25, 2016

Les propriétés client prédéfinies de XenMobile et leurs paramètres par défaut sont comme suit.

ENABLE_PASSCODE_AUTH

Nom complet : Activer l'authentification du code PIN Worx

Cette clé permet d'activer la fonctionnalité de code PIN Worx. Avec le code PIN ou code secret Worx, 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 Worx 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 Worx 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 complet : Activer la mise en cache du mot de passe de l'utilisateur

Cette clé 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 clé sur true, les utilisateurs sont invités à créer un code PIN ou code secret Worx. La clé ENABLE_PASSCODE_AUTH doit être définie sur true lorsque vous définissez cette clé sur true.

Valeurs possibles : true ou false

Valeur par défaut : false

ENCRYPT_SECRETS_USING_PASSCODE

Nom complet : Chiffrer les secrets à l'aide d'un code secret

Cette clé 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 clé 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 clé de manière à fournir une sécurité plus élevée sur les appareils des utilisateurs.

Remarque : l'activation de cette clé affecte l'expérience utilisateur car le nombre d'invites de saisie du code PIN Worx est plus important.

Valeurs possibles : true ou false

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Valeur par défaut : false

PASSCODE_TYPE

Nom complet : Type de code PIN Worx

Cette clé définit si les utilisateurs peuvent définir un code PIN Worx numérique ou un code secret Worx alphanumérique. Lorsque vous sélectionnez la valeur Numérique, l'utilisateur peut définir uniquement un code PIN Worx numérique. Lorsque vous sélectionnez la valeur Alphanumérique, l'utilisateur peut utiliser une combinaison de lettres et de chiffres pour le code secret Worx.

Remarque : lorsque vous modifiez le paramètre, les utilisateurs sont invités à créer un nouveau code PIN ou code secret Worx la prochaine fois qu'ils sont invités à s'authentifier.

Valeurs possibles : Numeric ou Alphanumeric

Valeur par défaut : Numeric

PASSCODE_EXPIRY

Nom complet : Exigences en matière d'expiration du code PIN Worx

Cette clé définit la durée (en jours) pendant laquelle le code PIN ou code secret Worx est valide, et après laquelle l'utilisateur est obligé de modifier son code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie uniquement lorsque le code PIN ou code secret Worx de l'utilisateur expire.

Valeurs possibles : 1-99

Valeur par défaut : 90

PASSCODE_HISTORY

Nom complet : Historique du code PIN Worx

Cette clé définit le nombre de codes PIN ou codes secrets Worx précédemment utilisés que les utilisateurs ne sont pas autorisés à réutiliser lorsqu'ils changent leur code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, la nouvelle valeur est définie la prochaine fois que les utilisateurs réinitialisent leur code PIN ou code secret Worx.

Valeurs possibles : 1-99

Valeur par défaut : 5

PASSCODE_MAX_ATTEMPTS

Nom complet : Nombre maximal de tentatives de saisie du code PIN Worx

Cette clé définit le nombre de tentatives de saisie infructueuses du code PIN ou code secret Worx 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 Worx.

Valeurs possibles : tout entier positif

Valeur par défaut : 15

© 1999-2017 Citrix Systems, Inc. All rights reserved.

INACTIVITY_TIMER

Nom complet : Délai d'inactivité

Cette clé 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 Worx. Pour activer ce paramètre pour une application MDX, vous devez définir le paramètre App Passcode sur On. Si le paramètre App Passcode est défini sur Off, les utilisateurs sont redirigés vers Worx Home 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 à Worx Home et pas seulement aux applications MDX.

Valeurs possibles : tout entier positif

Valeur par défaut : 15

PASSCODE_STRENGTH

Nom complet : Exigences en matière de sûreté du code PIN Worx

Cette clé définit le niveau de sécurité du code PIN ou code secret Worx. Lorsque vous modifiez ce paramètre, les utilisateurs sont invités à définir un nouveau code PIN ou code secret Worx 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 que vous sélectionnez pour PASSCODE_TYPE :

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
Taille moyenne (Valeur par défaut)	1. Tous les nombres ne peuvent pas être identiques. Par exemple, 444444 n'est pas autorisé. 2. Tous les nombres ne peuvent pas être consécutifs. Par exemple, 123456 ou 654321 n'est pas autorisé. **Autorisé** : 444333, 124567, 136790, 555556, 788888	En plus des règles de sécurité de niveau Low pour un code secret : 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 consécutifs. Par exemple, abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123 ne sont pas autorisés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		Autorisé : aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~
Strong	Identique au niveau de sécurité Medium du code secret Worx.	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#

ENABLE_CRASH_REPORTING

Nom d'affichage : Enable Crash reporting

Cette clé active ou désactive les rapports de plantage à l'aide des applications Crashlytics for Worx.

Valeurs possibles : true ou false

Valeur par défaut : true

DISABLE_LOGGING

Nom d'affichage : Disable logging

Cette clé 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 Worx Home 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 Worx Home et MDX.

Lorsque cette clé est définie sur true, Worx Home 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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Personnalisation du Worx Store pour appareils iOS

Jul 25, 2016

Vous pouvez configurer la manière dont les applications s'affichent dans le magasin et ajouter un logo pour personnaliser Worx Home et WorxStore sur les appareils mobiles iOS et Android.

Remarque : avant de commencer, assurez-vous que votre image personnalisée est prête et accessible.

- Le nom de 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) + 340 px x 50 px (2x).
- Appelez le fichier Header.png et Header@2x.png
- Créez un fichier .zip des fichiers, et non un dossier contenant les fichiers.

1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Plus > Personnalisation de Worx Store.
2. En regard de Vue du magasin par défaut, sélectionnez Catégorie ou A-Z.
3. En regard de Appareil, sélectionnez Téléphone ou Tablette.
4. En regard de Fichier de personnalisation, cliquez sur Parcourir pour sélectionner une image ou un fichier .zip d'images à utiliser pour la personnalisation, puis cliquez sur Enregistrer.

Pour déployer ce paquetage auprès des appareils de vos utilisateurs, vous devez créer un paquetage de déploiement et le déployer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Création d'options d'assistance Worx Home et GoToAssist

Jul 25, 2016

1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Plus > Assistance Worx Home.
2. Sur la page Assistance Worx Home, entrez une valeur pour les champs suivants :
    1. E-mail de l'assistance (support technique)
    2. Téléphone de l'assistance (support technique)
    3. Jeton pour chat GoToAssist
    4. E-mail de ticket d'assistance GoToAssist

Les informations d'assistance Worx Home que vous créez s'affichent dans la liste Propriétés du client dans la console XenMobile et sont associées aux clés suivantes : SUPPORT_EMAIL, SUPPORT_PHONE, GTA_CHAT et GTA_TICKET.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

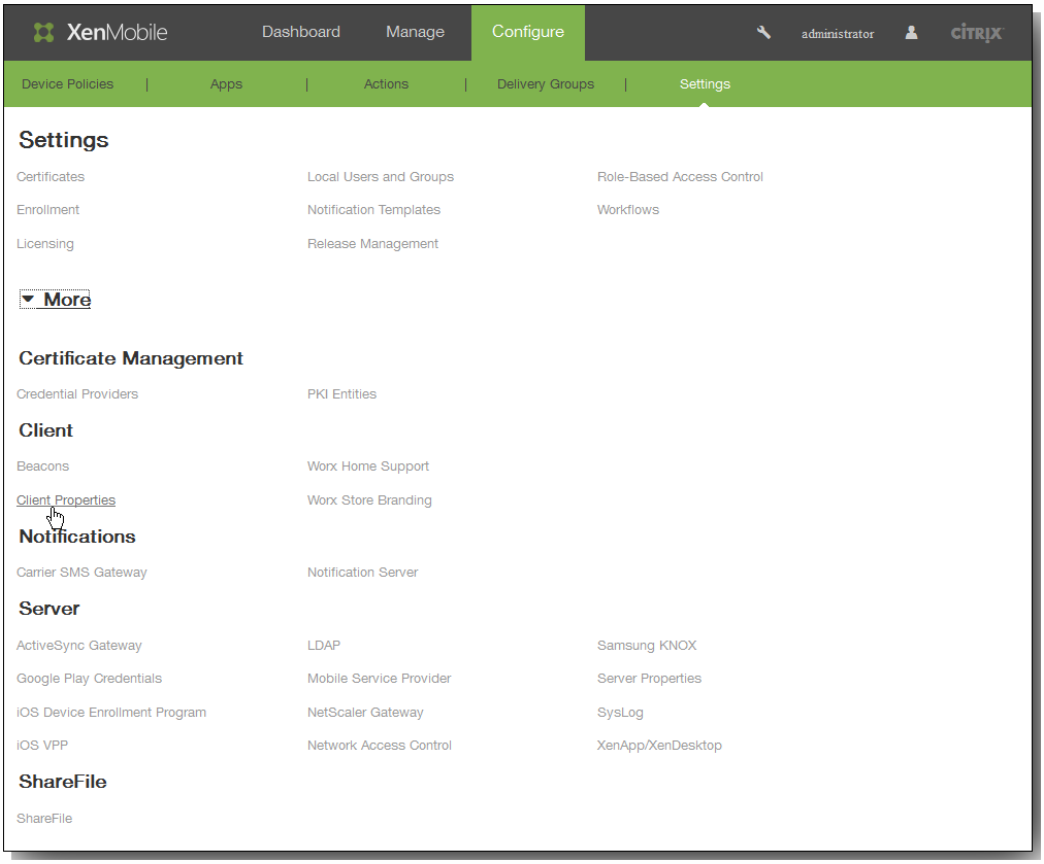
Pour ajouter, modifier ou supprimer des propriétés de client

Jul 25, 2016

Les propriétés du client contiennent des informations qui sont fournies directement à Worx Home sur les appareils des utilisateurs. Les propriétés du client sont utilisées pour configurer des paramètres avancés tels que le code PIN Worx. Vous obtenez les propriétés du client à partir du support de Citrix.

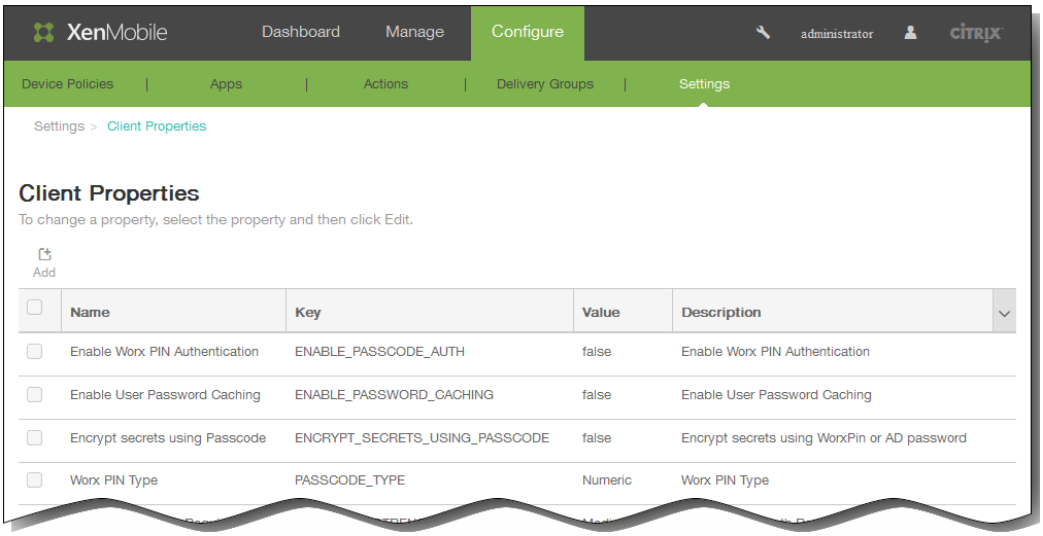
Remarque : les propriétés du client sont susceptibles d'être modifiées avec chaque nouvelle version des applications clientes, et plus particulièrement Worx Home.

1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Plus > Propriétés du client.



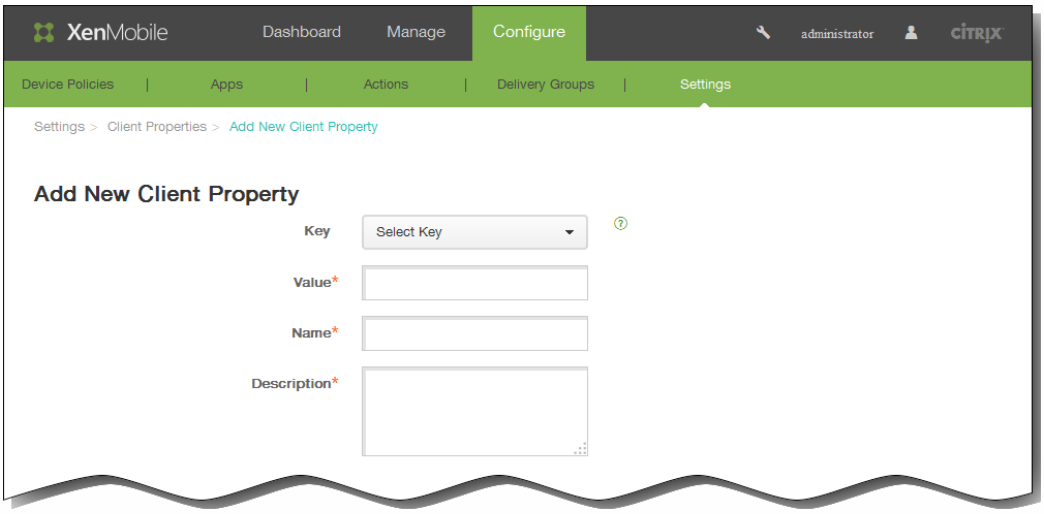
La boîte de dialogue Propriétés du client s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Pour ajouter une propriété de client

1. Dans la page Propriétés du client, cliquez sur Ajouter. La page Ajouter une nouvelle propriété de client s'affiche.



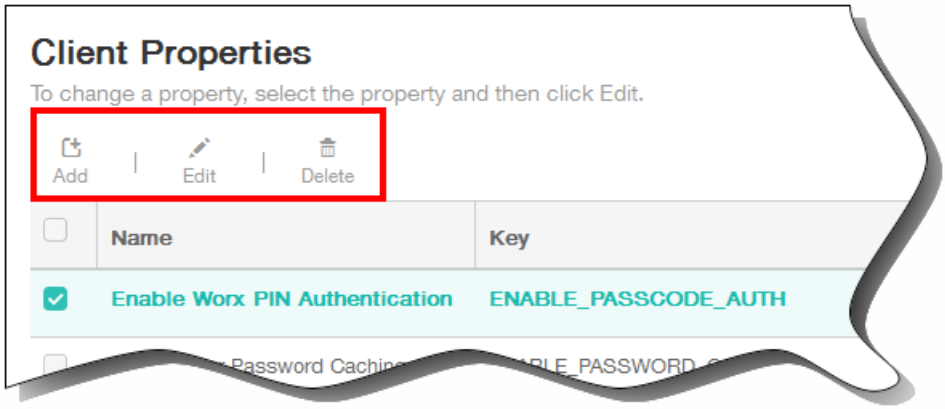
2. Dans la boîte de dialogue Ajouter une nouvelle propriété de client, entrez les informations suivantes :
   Remarque : tous les champs sont obligatoires.
   1. Clé : dans la liste, cliquez sur la clé de propriété que vous souhaitez ajouter.
      Important : contactez le support Citrix avant d'apporter des modifications ou pour demander une clé spéciale pour effectuer une modification.
   2. Valeur : entrez la valeur de la propriété sélectionnée.
   3. Nom : entrez un nom pour la propriété.
   4. Description : entrez une description pour la propriété.

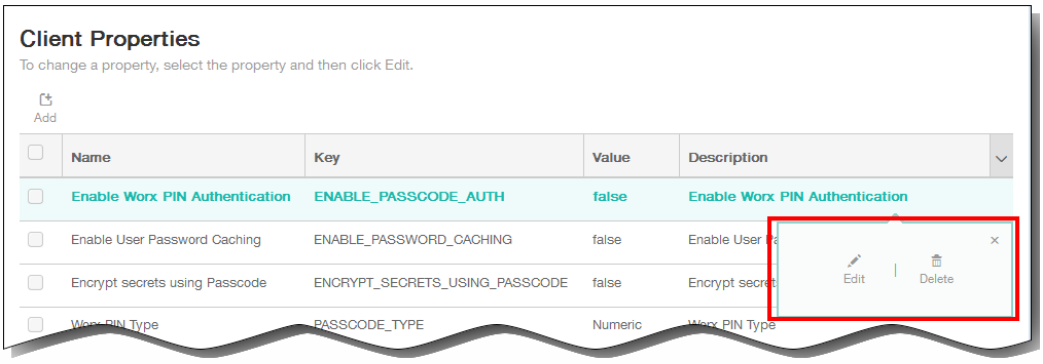
Pour modifier une propriété de client

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

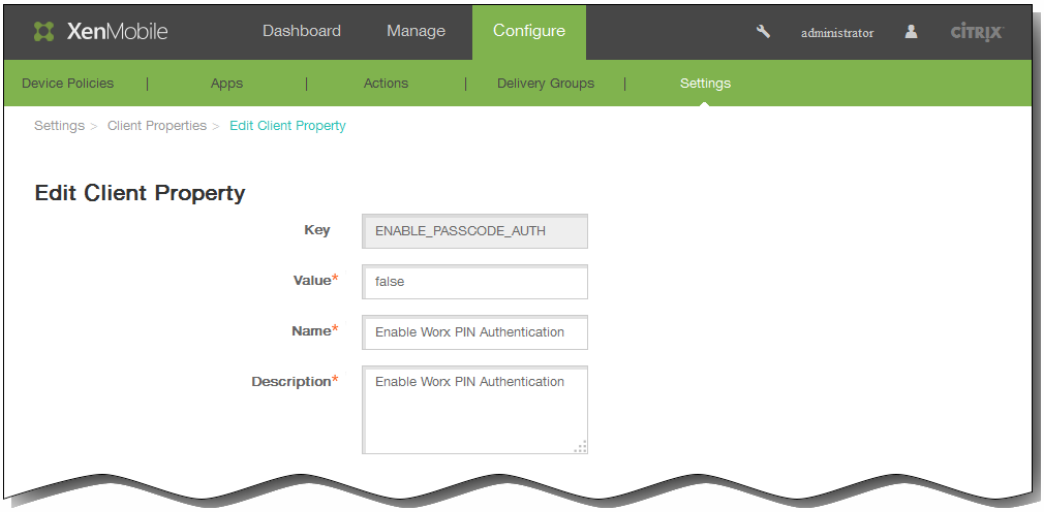
© 1999-2017 Citrix Systems, Inc. All rights reserved.

droit de la liste.





2. Cliquez sur Modifier. La page Modifier la propriété client s'affiche.



3. Modifiez les informations suivantes le cas échéant :
   1. Valeur : valeur de la propriété sélectionnée.
   2. Nom : nom de la propriété.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

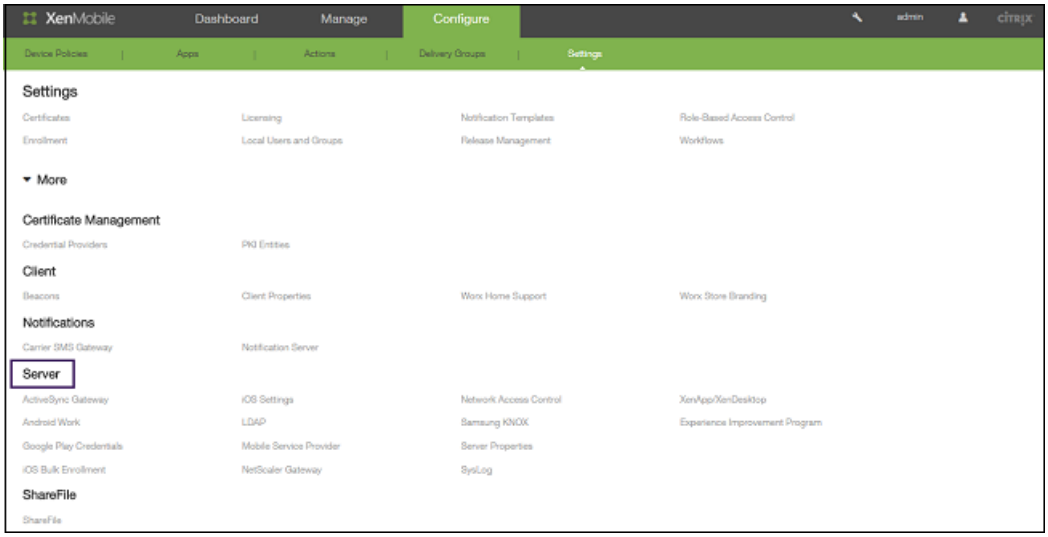
Paramètres du serveur XenMobile

Jul 25, 2016

Les paramètres du serveur XenMobile que vous configurez dans la console Web XenMobile comprennent :

- ActiveSync Gateway
- Android for Work
- Informations d'identification Google Play
- Inscription en bloc iOS
- Paramètres iOS
- LDAP
- Fournisseur de services mobiles
- NetScaler Gateway
- Contrôle d'accès réseau
- Samsung KNOX
- Propriétés du serveur
- SysLog
- XenApp/XenDesktop
- Programme d'amélioration de l'expérience

1. Dans la console XenMobile, cliquez sur Configurer et sur Paramètres.
   La page Paramètres s'affiche.



2. Cliquez sur Plus.
3. Sous **Serveur**, cliquez sur l'option que vous souhaitez configurer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ActiveSync Gateway dans XenMobile

Jul 25, 2016

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.

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.

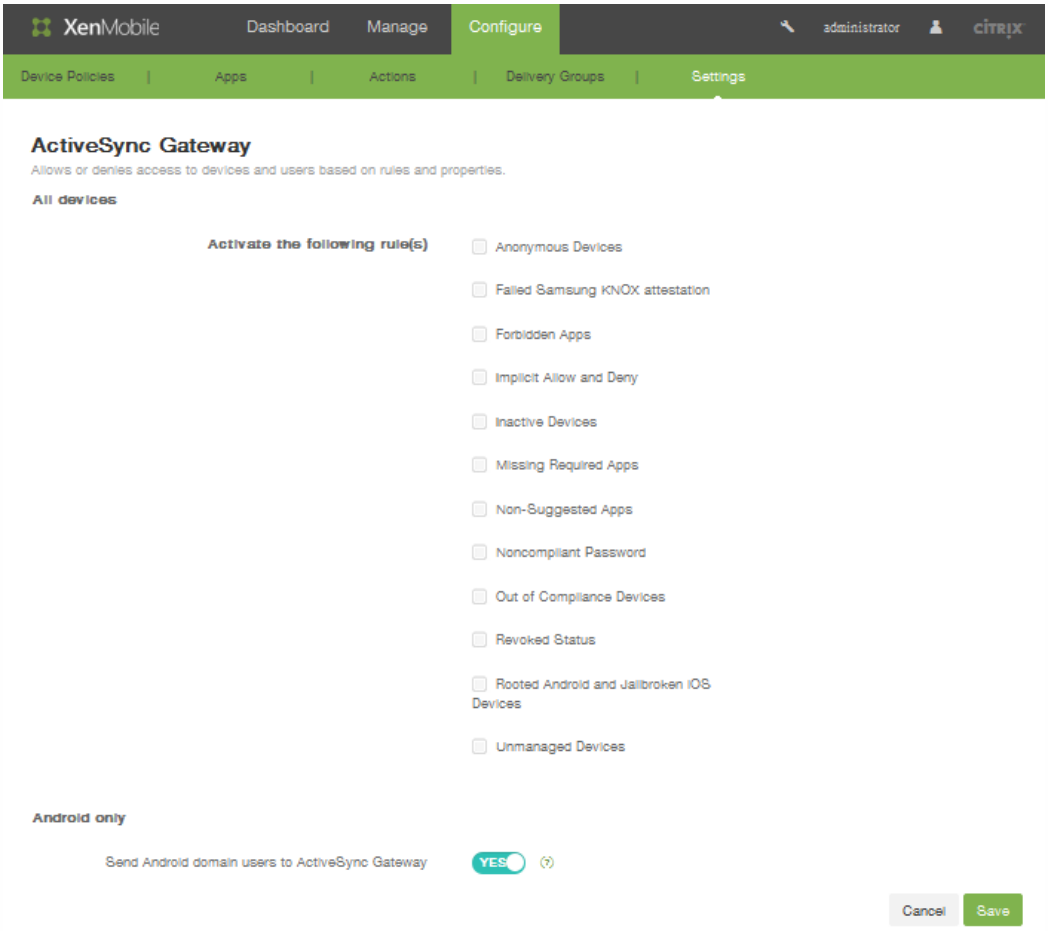
Appareils non gérés : vérifie si un appareil est toujours dans un état géré, sous le contrôle de XenMobile. Par exemple, un appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 ActiveSync Gateway dans XenMobile

1. Dans la console XenMobile, cliquez sur **Configurer > Paramètres > Plus > ActiveSync Gateway**.
   La page de configuration **ActiveSync Gateway** s'affiche.



2. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.
3. Dans **Android uniquement**, dans **Envoyer les utilisateurs de domaine Android vers ActiveSync Gateway**, cliquez sur **Oui** pour vous assurer que XenMobile envoie les informations de l'appareil Android à Secure Mobile Gateway.
4. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Informations d'identification Google Play

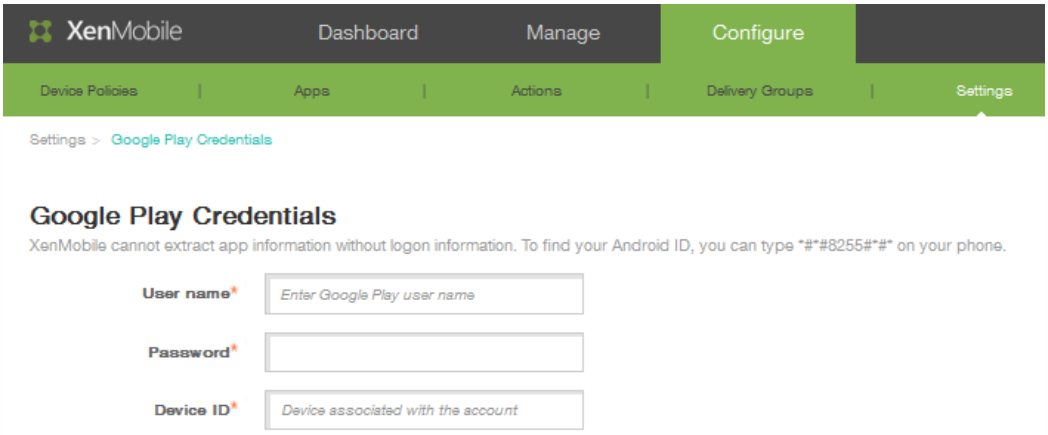
Jul 25, 2016

XenMobile utilise les informations d'identification Google Play pour extraire les informations applicatives pour l'appareil.

Remarque : pour trouver votre ID Android, entrez *#*#8255#*#*sur votre téléphone.
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.

Pour configurer XenMobile de manière à utiliser les informations d'identification Google Play

1. Dans la console Web XenMobile, cliquez Configurer > Paramètres > Plus > Identifiants Google Play.
   L'écran de configuration Identifiants Google Play s'affiche.



2. Dans Nom d'utilisateur, entrez le nom associé au compte Google Play.
3. Dans Mot de passe, entrez le mot de passe utilisateur.
4. Dans ID de l'appareil, entrez votre ID Android.
   Entrez *#*#8255#*#*sur votre téléphone pour déterminer l'ID Android.
5. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

iOS Device Enrollment Program

Jul 25, 2016

Vous pouvez configurer un iOS Device Enrollment Program dans XenMobile pour les appareils mobiles exécutant iOS. Cette fonctionnalité permet aux appareils iOS de notifier les serveurs Apple de l'existence d'un profil qui personnalise l'utilisation de l'assistant d'installation de l'appareil qui peut être attribué à des appareils spécifiques.

Pour configurer le programme iOS Device Enrollment Program dans XenMobile

1. Dans la console Web XenMobile, cliquez Configurer > Paramètres > Plus > iOS Bulk Enrollment Program > Configuration DEP.
   La page de configuration DEP (Device Enrollment Program) s'affiche.

2. Dans Détails, configurez les paramètres suivants :
   - Inscription d'appareils : cliquez sur OUI.
   - Clé key: Entrez la clé du client.
   - Secret du client : entrez un secret de client.
   - Jeton d'accès : spécifiez le jeton d'accès.
   - Secret d'accès : entrez le secret du jeton d'accès.
   - Expiration du jeton d'accès : si vous le souhaitez, spécifiez la date d'expiration du jeton d'accès.
3. Cliquez sur Tester la connexion pour vérifier la connexion.
4. Développez Installation de l'appareil et configurez les paramètres suivants :
   - Division : entrez le nom associé à la division.
   - Numéro de téléphone de l'assistance : entrez le numéro de téléphone de l'assistance.
   - Adresse e-mail du support : entrez l'adresse e-mail de l'assistance (facultatif).
   - ID de service unique : spécifiez un ID de service unique (facultatif).
5. Dans Paramètres de l'appareil, configurez les paramètres suivants qui sont associés au programme iOS Device Enrollment Program :
   - Autoriser ou refuser le couplage : cliquez sur Autoriser pour permettre à l'appareil d'être géré par des outils Apple, tels que iTunes et Apple Configurator.
     Remarque : si vous autorisez le couplage, et que vous utilisez Apple Configurator, dans Mode supervisé, sélectionnez OUI.
   - Suppression du profil des appareils : si vous souhaitez que l'appareil utilise un profil qui puisse être supprimé à distance, cliquez sur Autoriser.
   - Exiger l'inscription des appareils : sélectionnez cette case pour empêcher les utilisateurs de passer outre le processus d'inscription.
6. Dans Étapes de configuration de l'appareil, configurez les paramètres suivants :
   - Emplacement Services: Cliquez sur Configuration afin d'autoriser l'appareil à partager son emplacement ou cliquez sur Ignorer pour empêcher l'appareil de partager son emplacement.
   - Restaurer à partir de la copie de sauvegarde : cliquez sur Configuration pour autoriser un appareil à restaurer les données à partir d'une copie de sauvegarde.
   - Apple ID et iCloud: cliquez sur Configuration si vous souhaitez que l'appareil utilise Apple ID et iCloud.
   - Termes et conditions : cliquez sur Configuration.
   - Code secret : cliquez sur Configuration pour utiliser un code secret pour l'inscription d'appareil.
   - Siri : cliquez sur Configuration pour qu'un appareil utilise Siri.
   - Touch ID : cliquez sur Configuration pour utiliser la fonction Touch ID sur l'appareil.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Apple Pay : cliquez sur Configuration pour activer Apple Pay sur l'appareil.
- Zoom : cliquez sur Configuration pour activer zoom.
- Diagnostics : cliquez sur Configuration pour autoriser l'appareil à partager les diagnostics.

7. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Déploiement d'appareils iOS via le programme DEP d'Apple

Jul 25, 2016

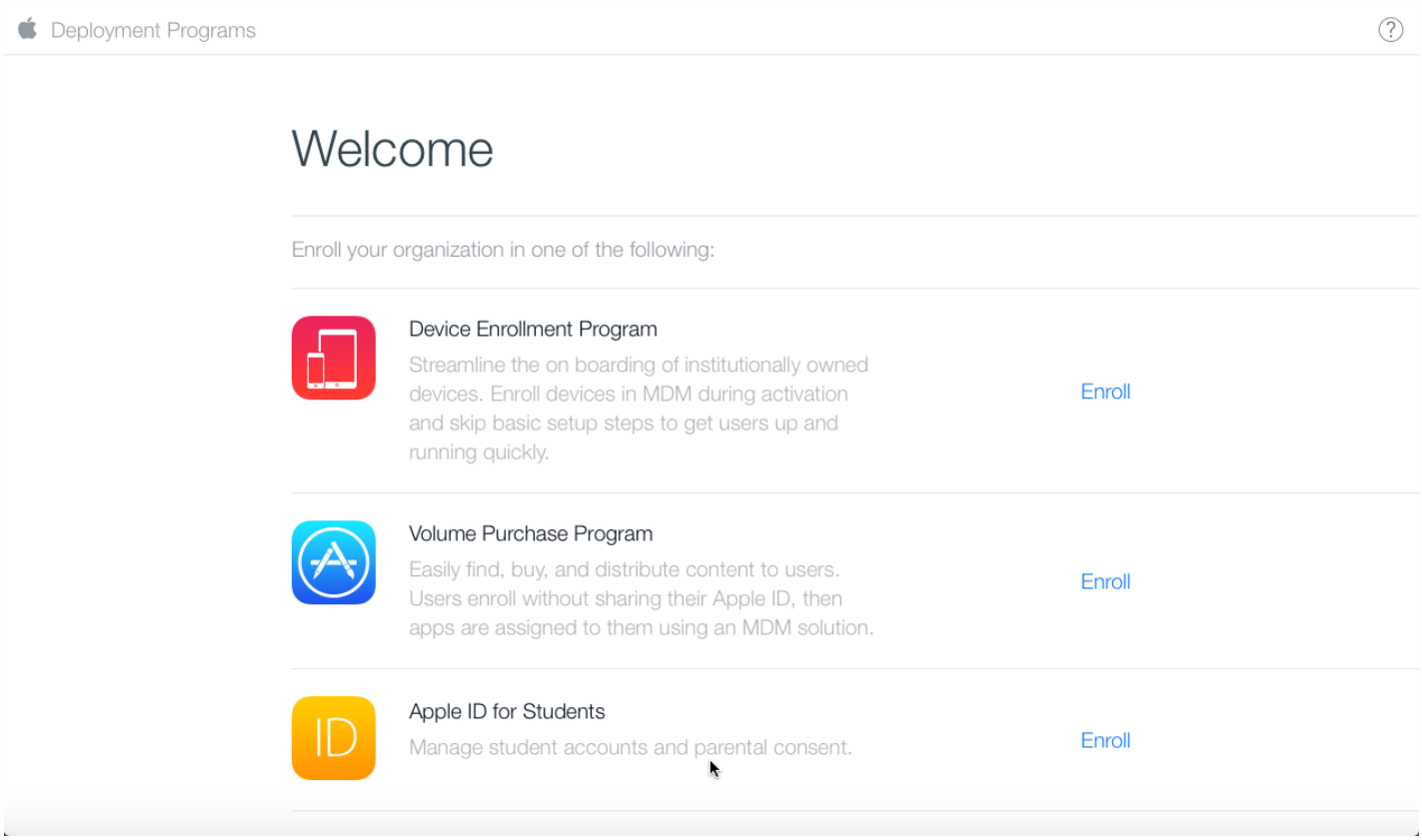
Vous avez besoin d'un compte Apple Developer Enterprise Program (DEP) pour bénéficier du programme DEP d'Apple pour inscrire et gérer des appareils iOS dans XenMobile. Les conditions principales que les organisations doivent respecter pour s'inscrire au programme DEP d'Apple sont les suivantes.

- 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.

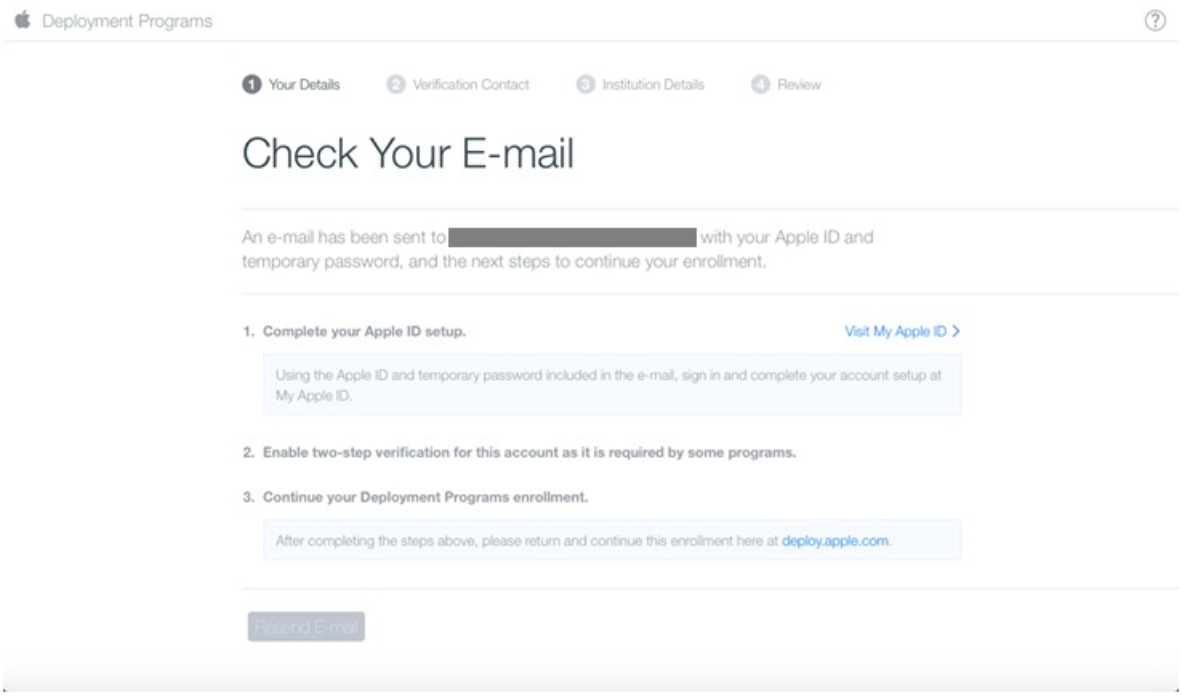
Demander l'ouverture d'un compte Apple DEP

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.

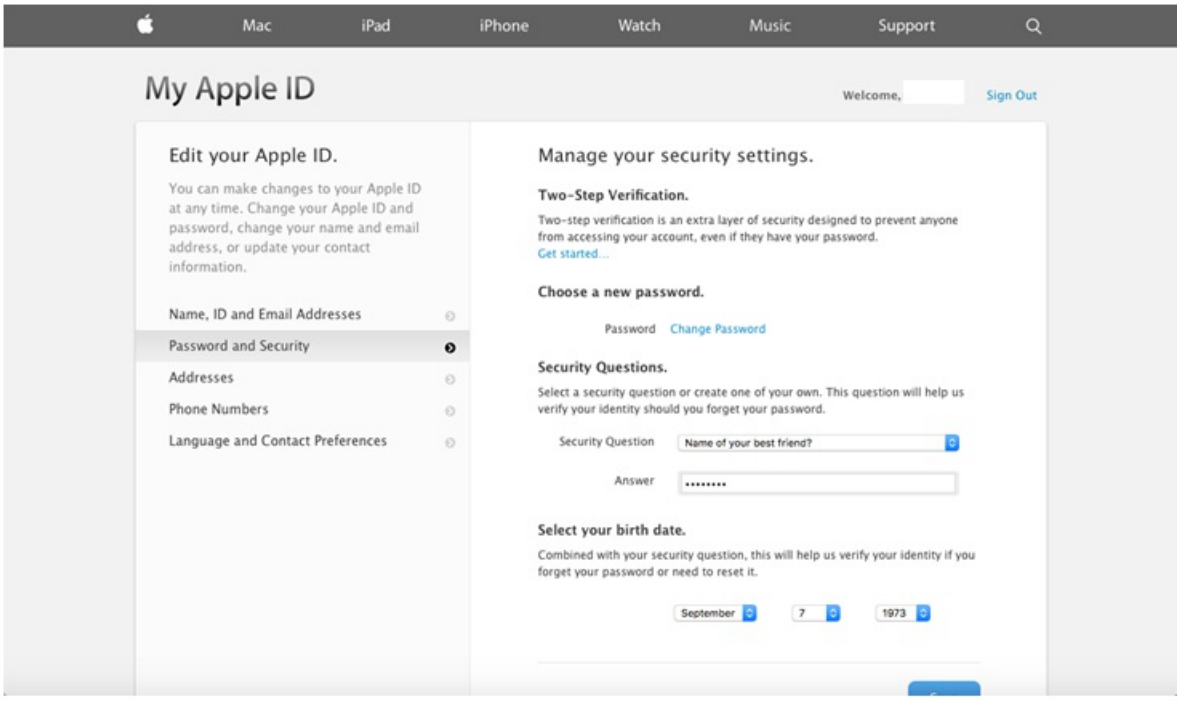


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

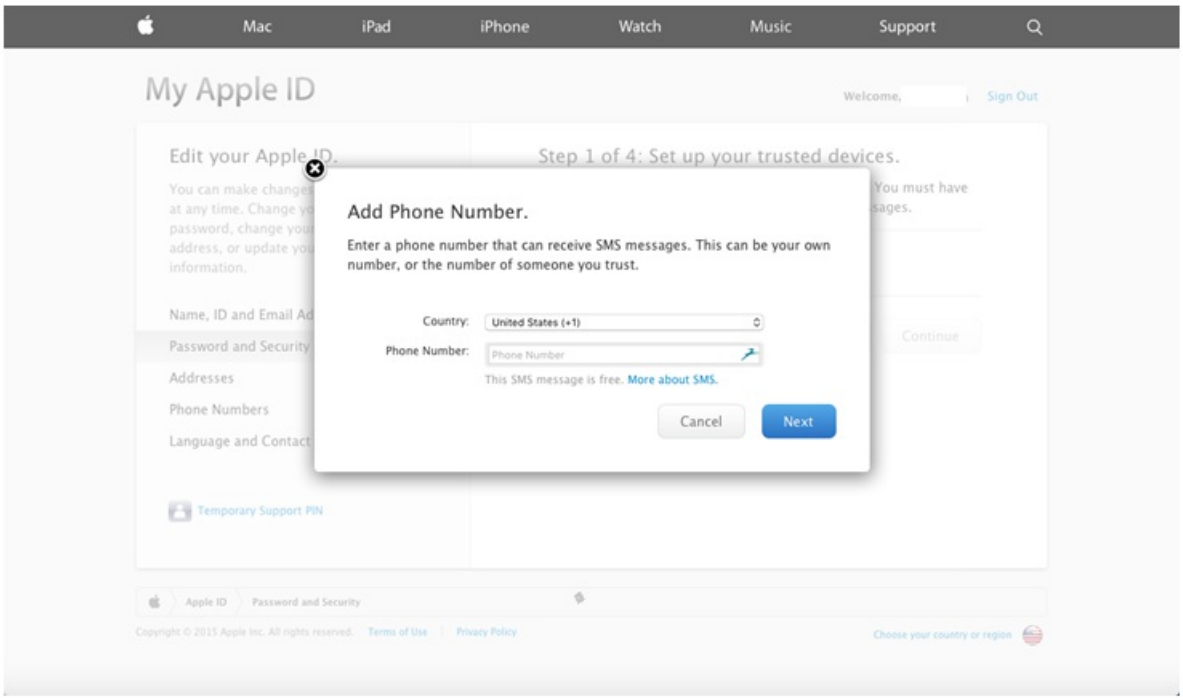


2. Connectez-vous à l'aide de cet identifiant Apple et configurez les paramètres de sécurité du compte.

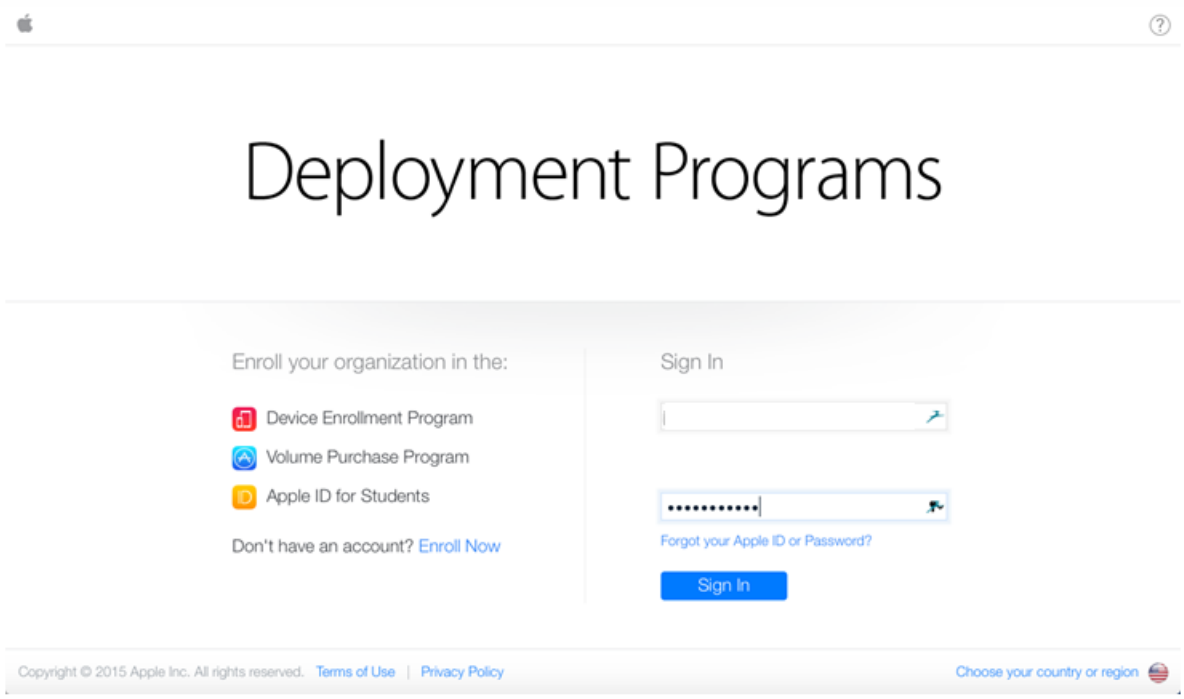


3. Configurez et activez la validation en deux étapes, ce qui est nécessaire pour utiliser le portail DEP. Durant ces étapes, vous ajoutez un numéro de téléphone par le biais duquel vous recevrez le code PIN à 4 chiffres requis pour la validation en deux étapes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

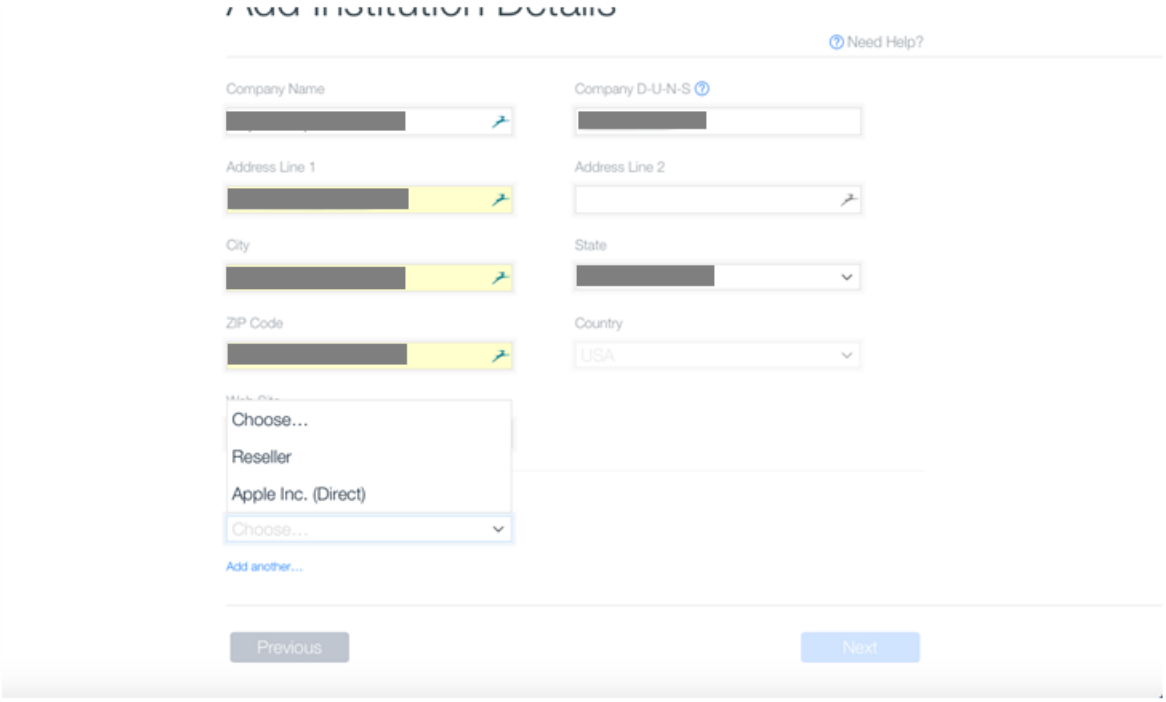


4. Connectez-vous au portail DEP pour terminer la configuration du compte à l'aide de la validation en deux étapes que vous venez de configurer.

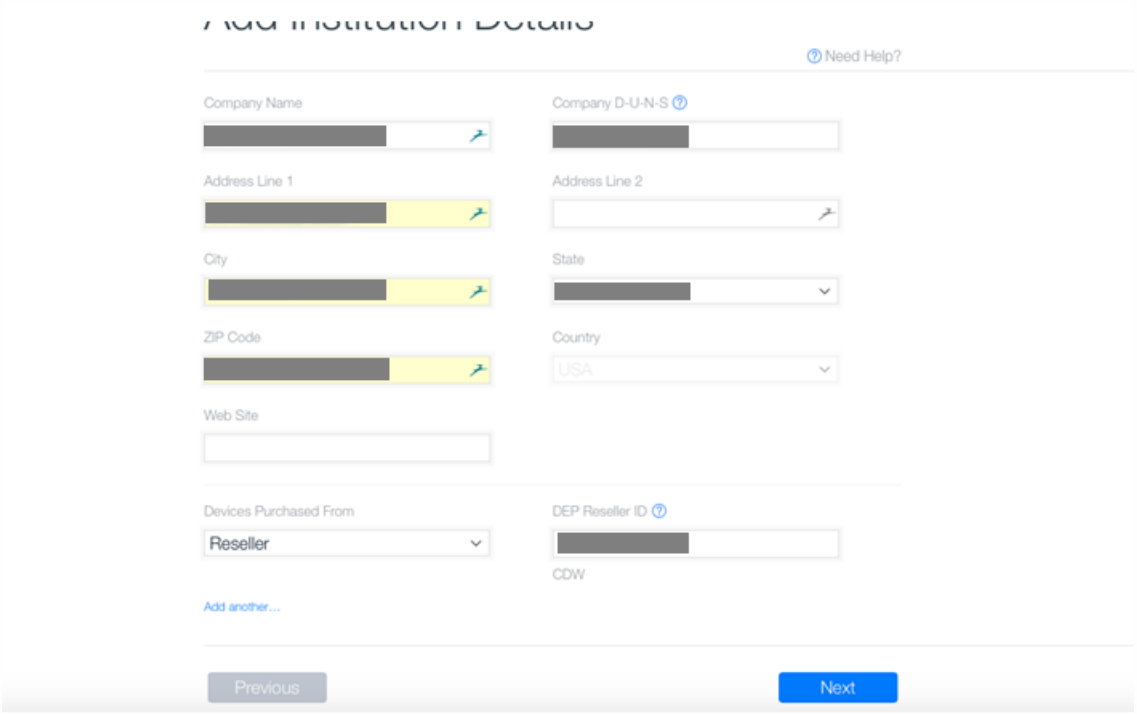


5. Ajoutez les détails de votre entreprise et sélectionnez là où vous avez acheté vos appareils. Pour de plus amples informations sur les options, consultez la section suivante, Commander des appareils compatibles avec le programme DEP.

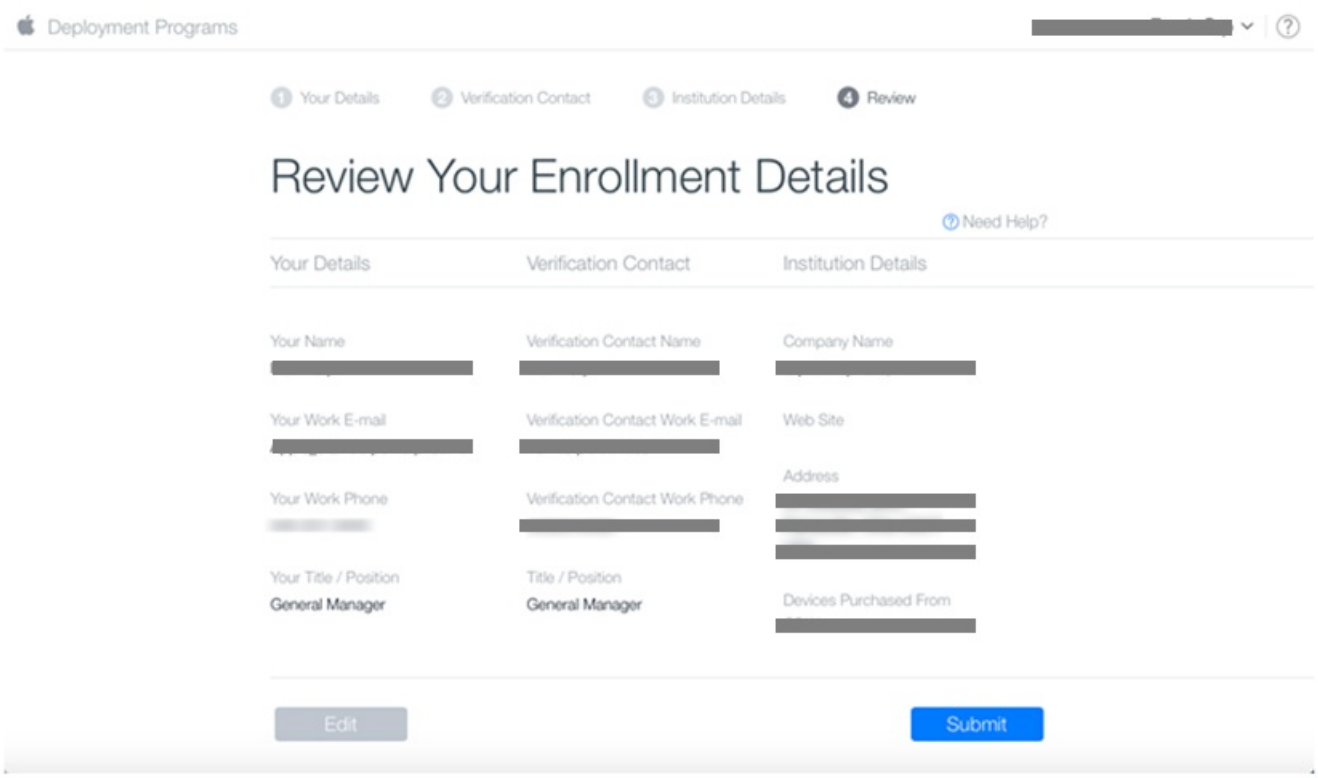
© 1999-2017 Citrix Systems, Inc. All rights reserved.



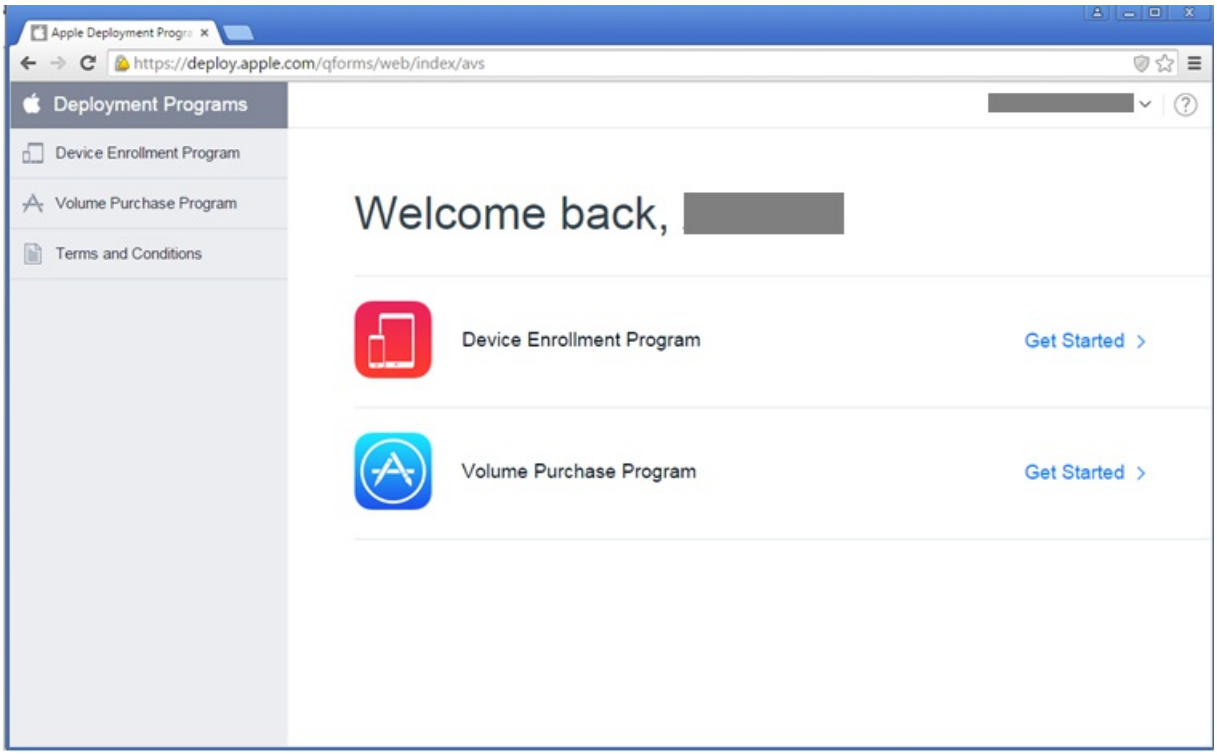
6. Ajoutez le numéro de client Apple ou l'ID du revendeur DEP, vérifiez vos détails d'inscription et attendez que Apple approuve votre compte.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

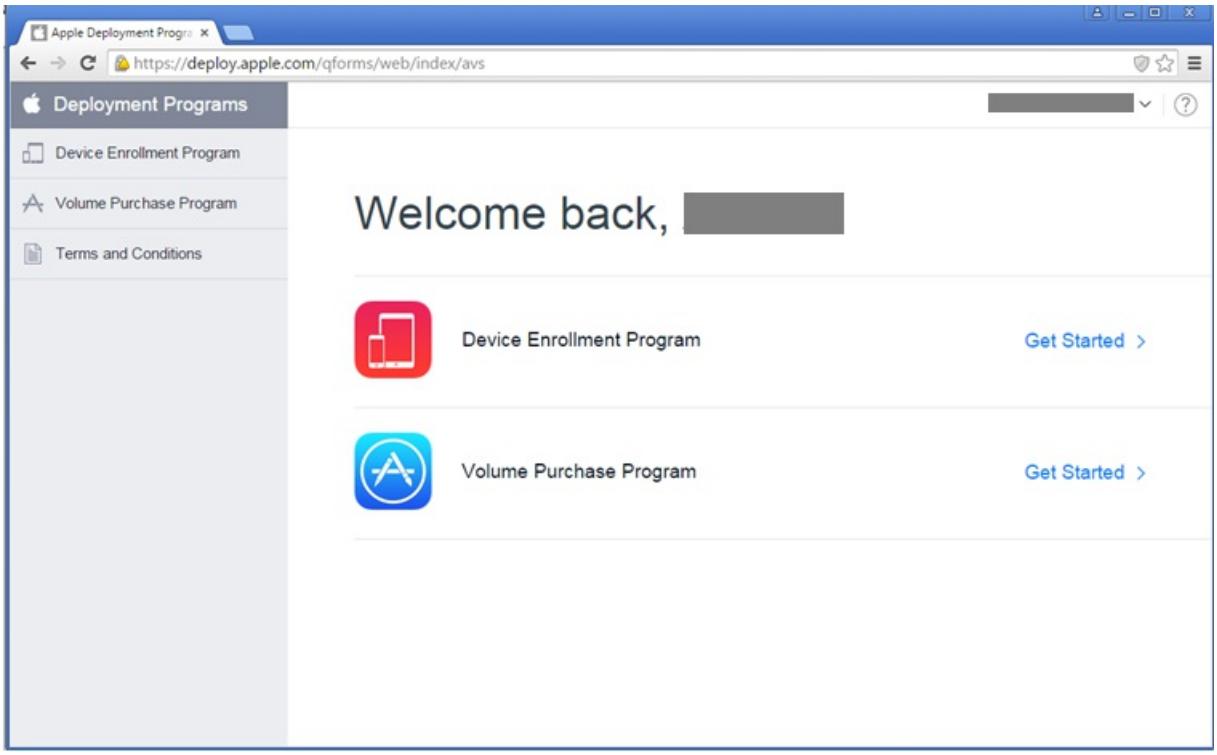


Intégration de votre compte DEP avec XenMobile

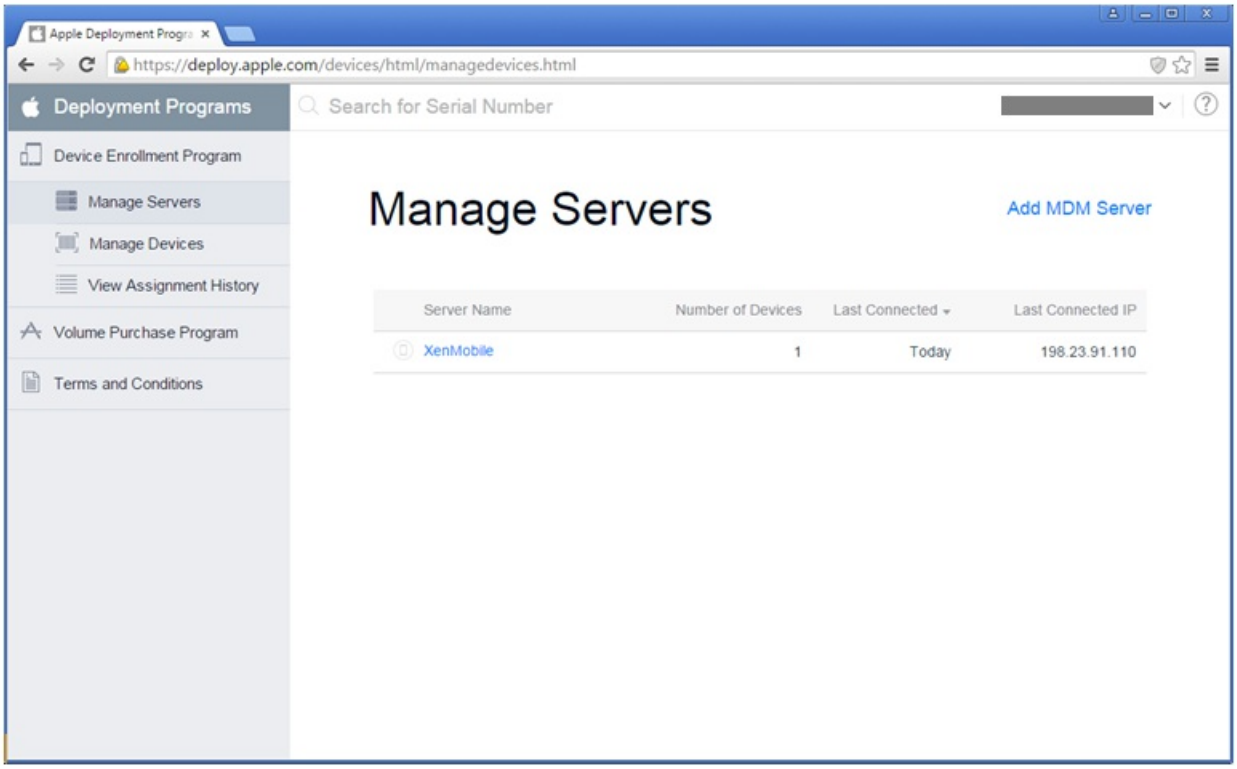
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

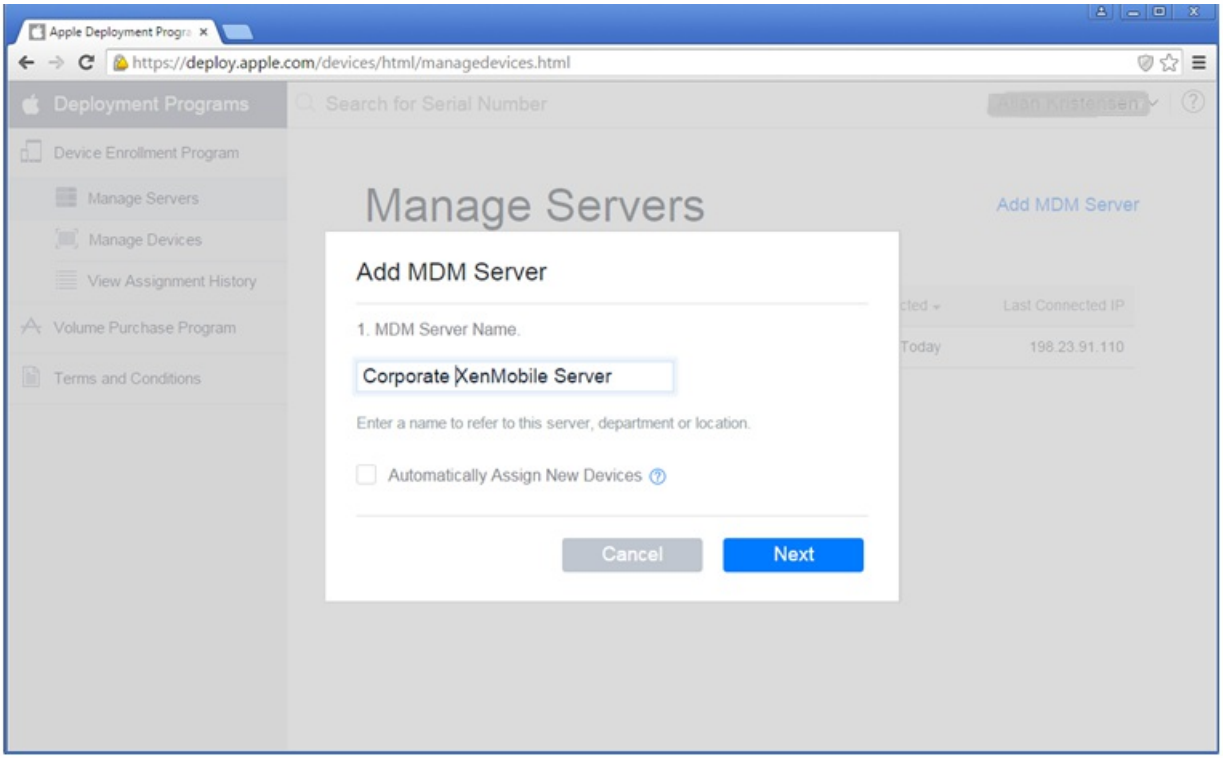


2. Cliquez sur **Gérer les serveurs** et sur le côté droit, cliquez sur **Ajouter un serveur MDM**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

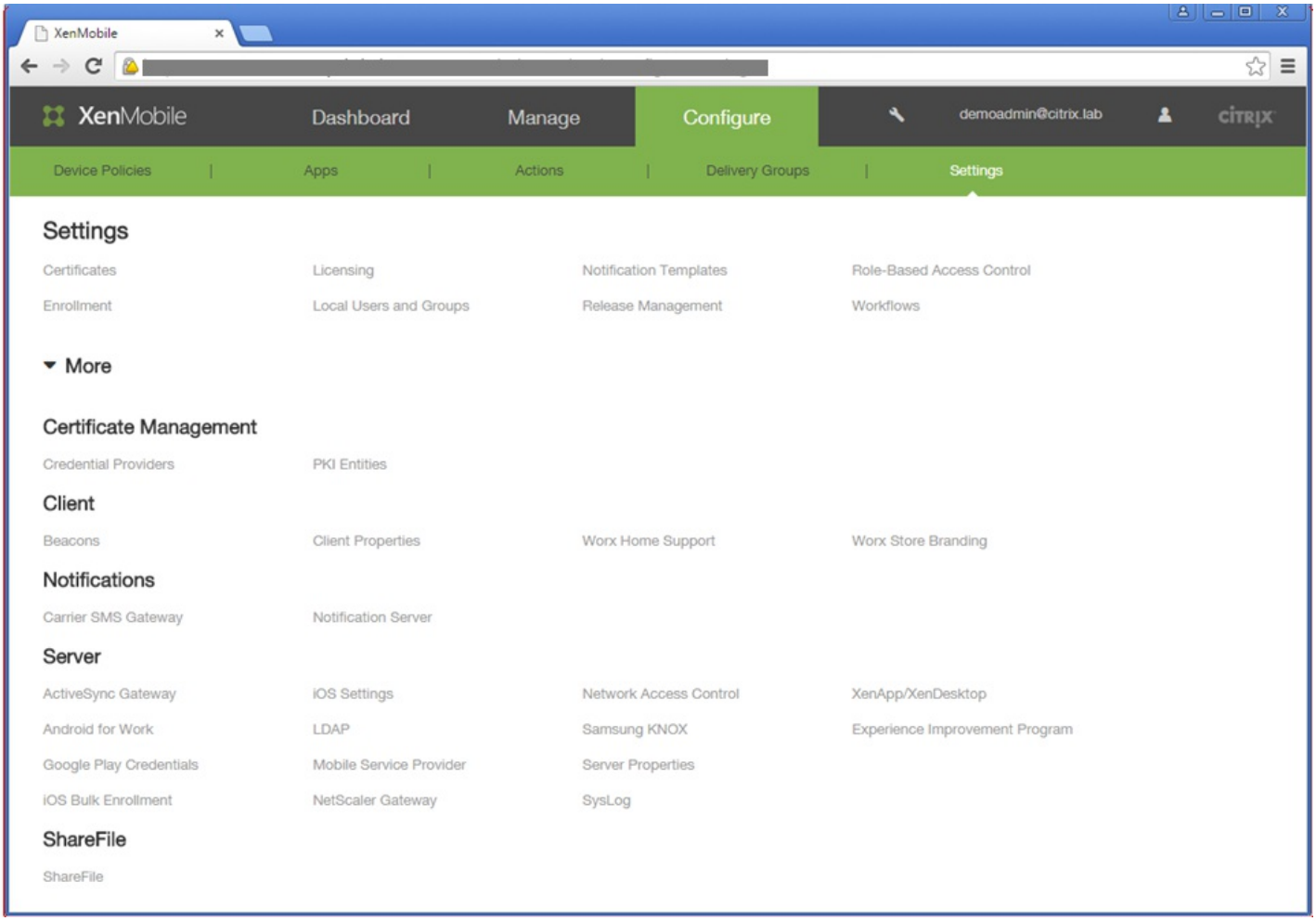
3. Dans **Ajouter un serveur MDM**, entrez un nom pour votre serveur XenMobile et cliquez sur **Suivant**.



4. Chargez une clé publique depuis votre serveur XenMobile. Pour générer la clé depuis XenMobile, procédez comme suit :

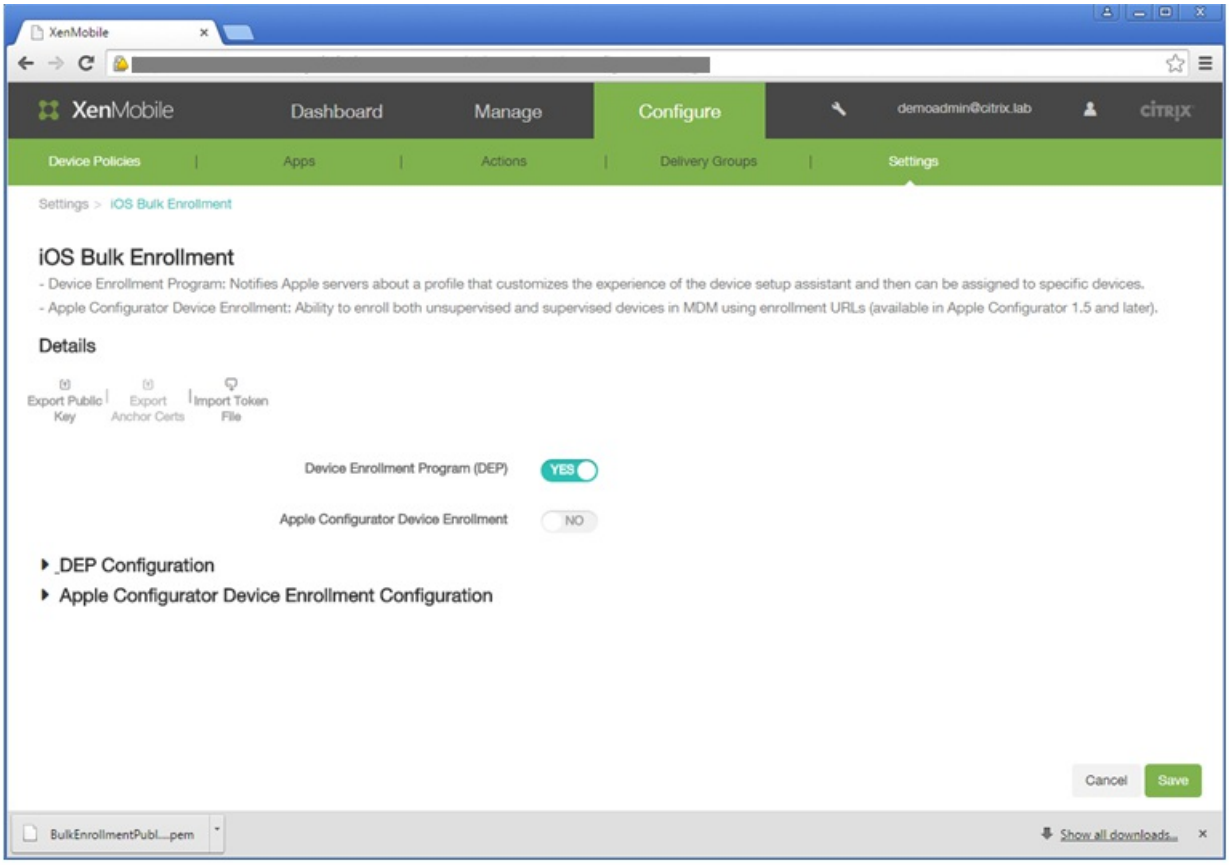
a. Connectez-vous à la console XenMobile, cliquez sur **Configurer**, **Paramètres** et sous **Plus**, cliquez sur **Inscription en bloc iOS**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

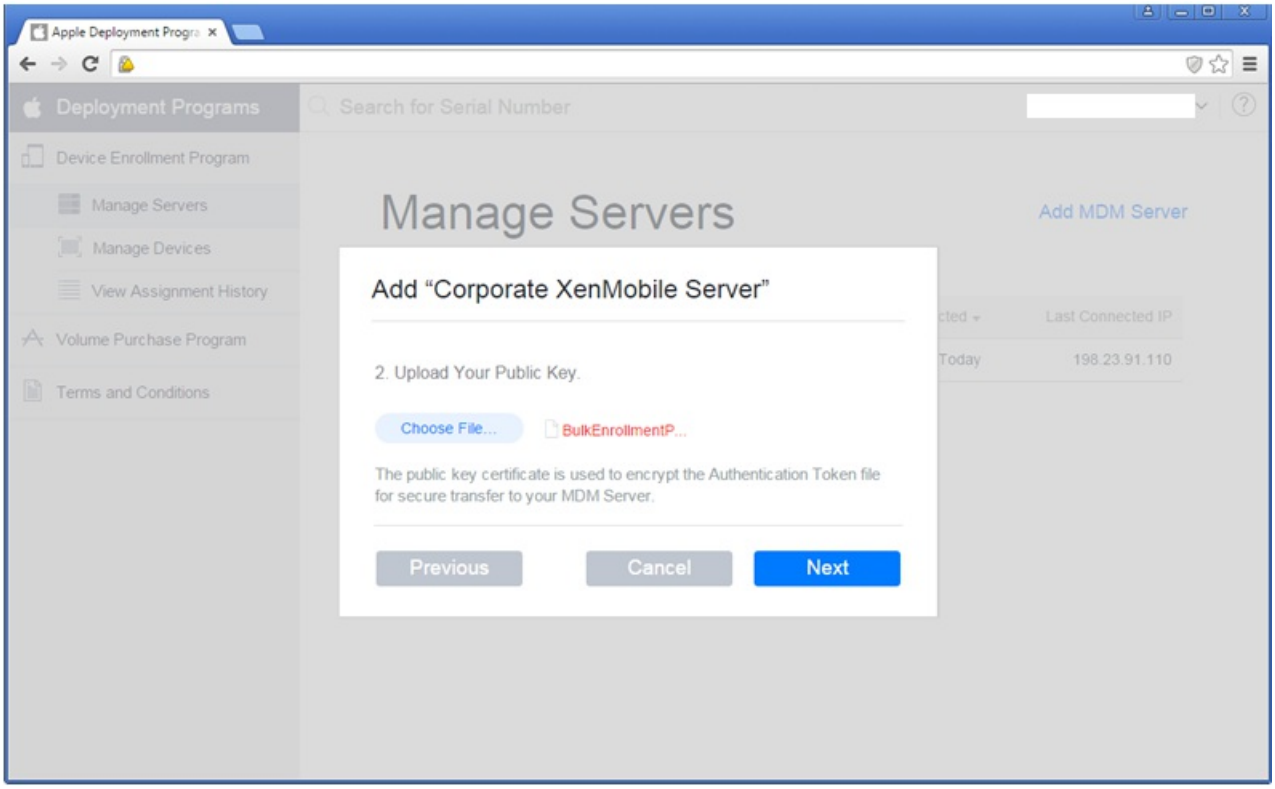


b. Sur la page **Inscription en bloc iOS**, cliquez sur **Exporter la clé publique**. La clé publique est téléchargée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

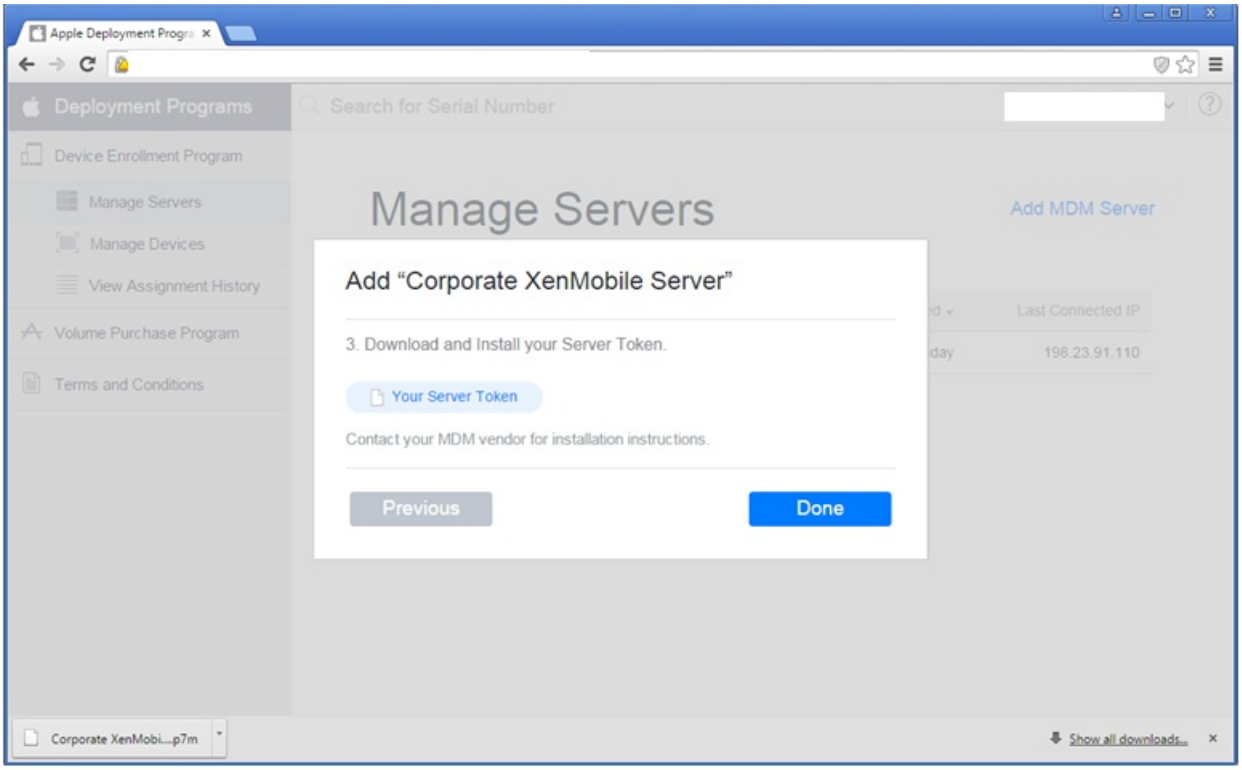


5. Sur le portail Apple DEP, cliquez **Choisir un fichier**, sélectionnez la clé publique que vous venez de télécharger et cliquez sur **Suivant**.



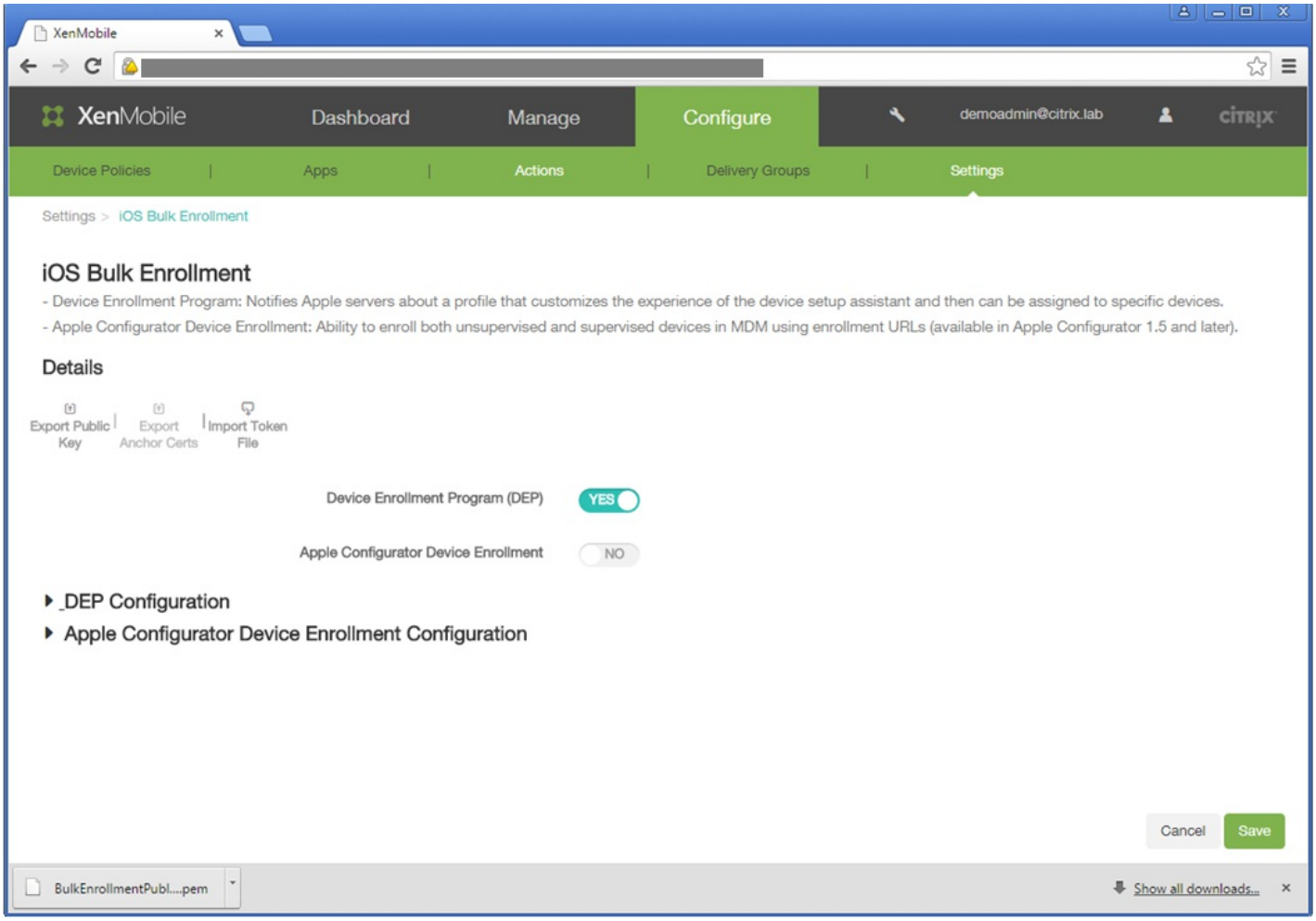
© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. Cliquez sur **Votre jeton de serveur** pour générer un jeton de serveur, lequel est téléchargé depuis le navigateur, et cliquez sur **Terminé**.

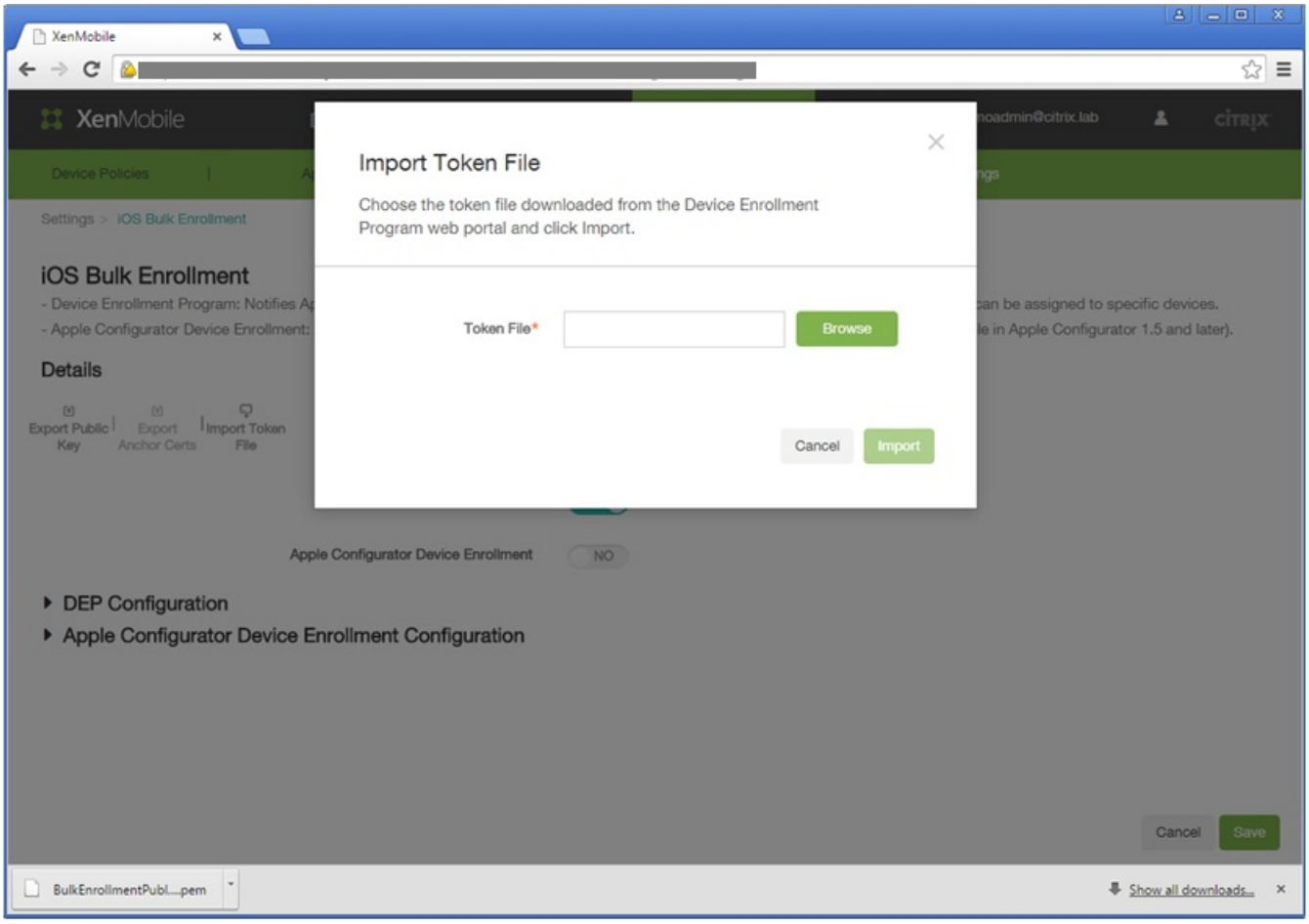


7. Sur la page **Inscription en bloc iOS** de la console XenMobile, cliquez sur **Importer un fichier jeton** et chargez le fichier de jeton que vous avez téléchargé à l'étape précédente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



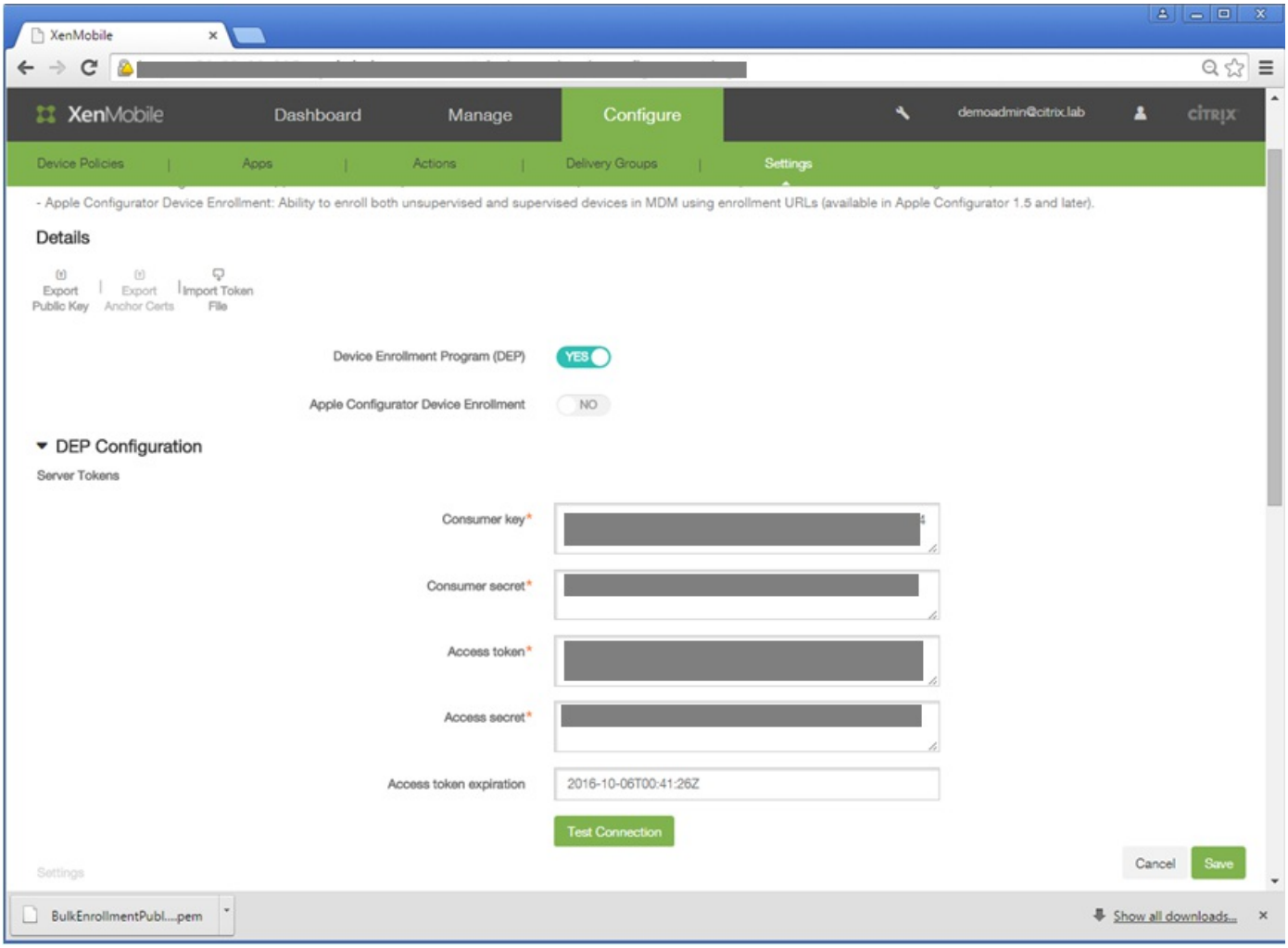
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

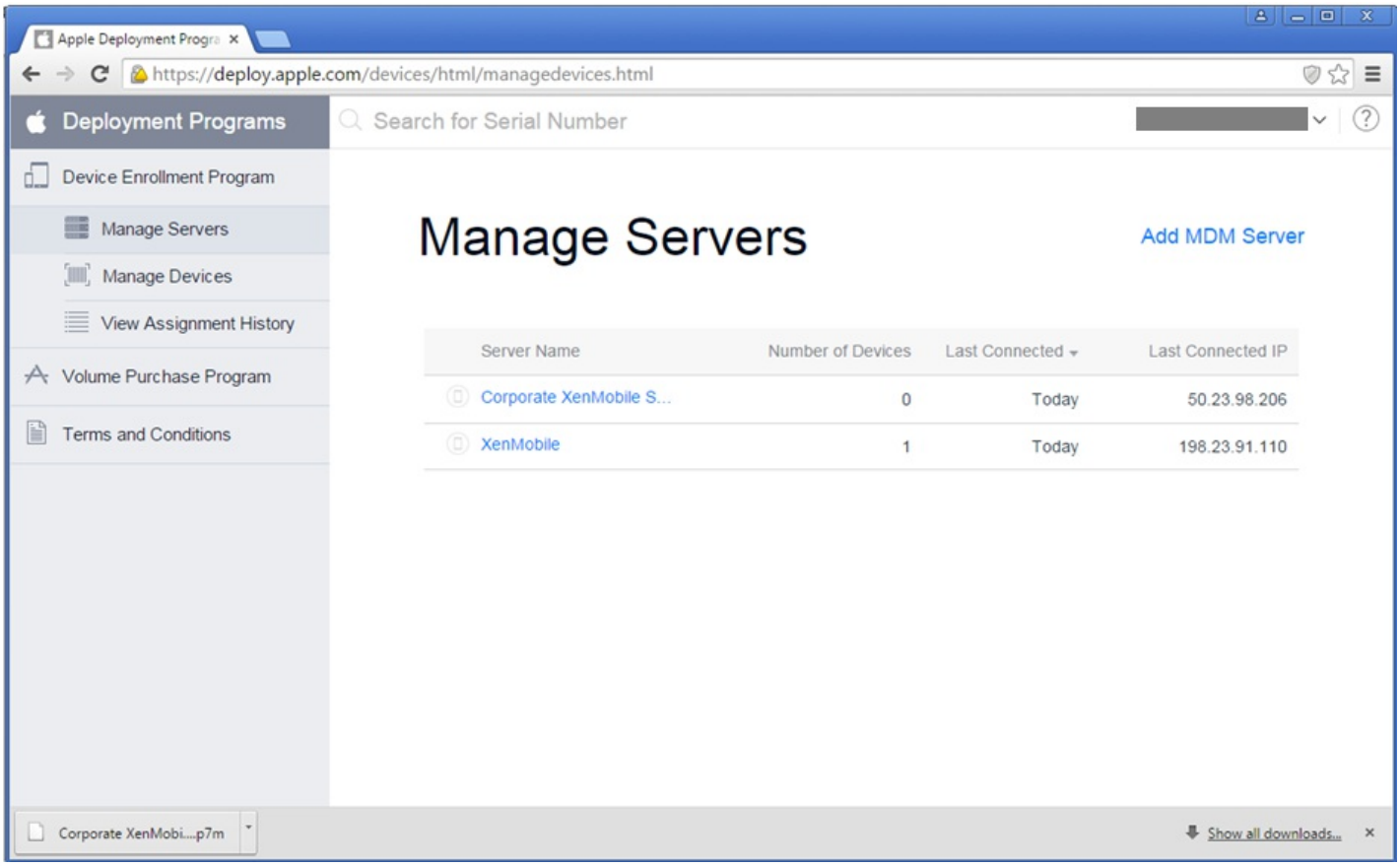
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

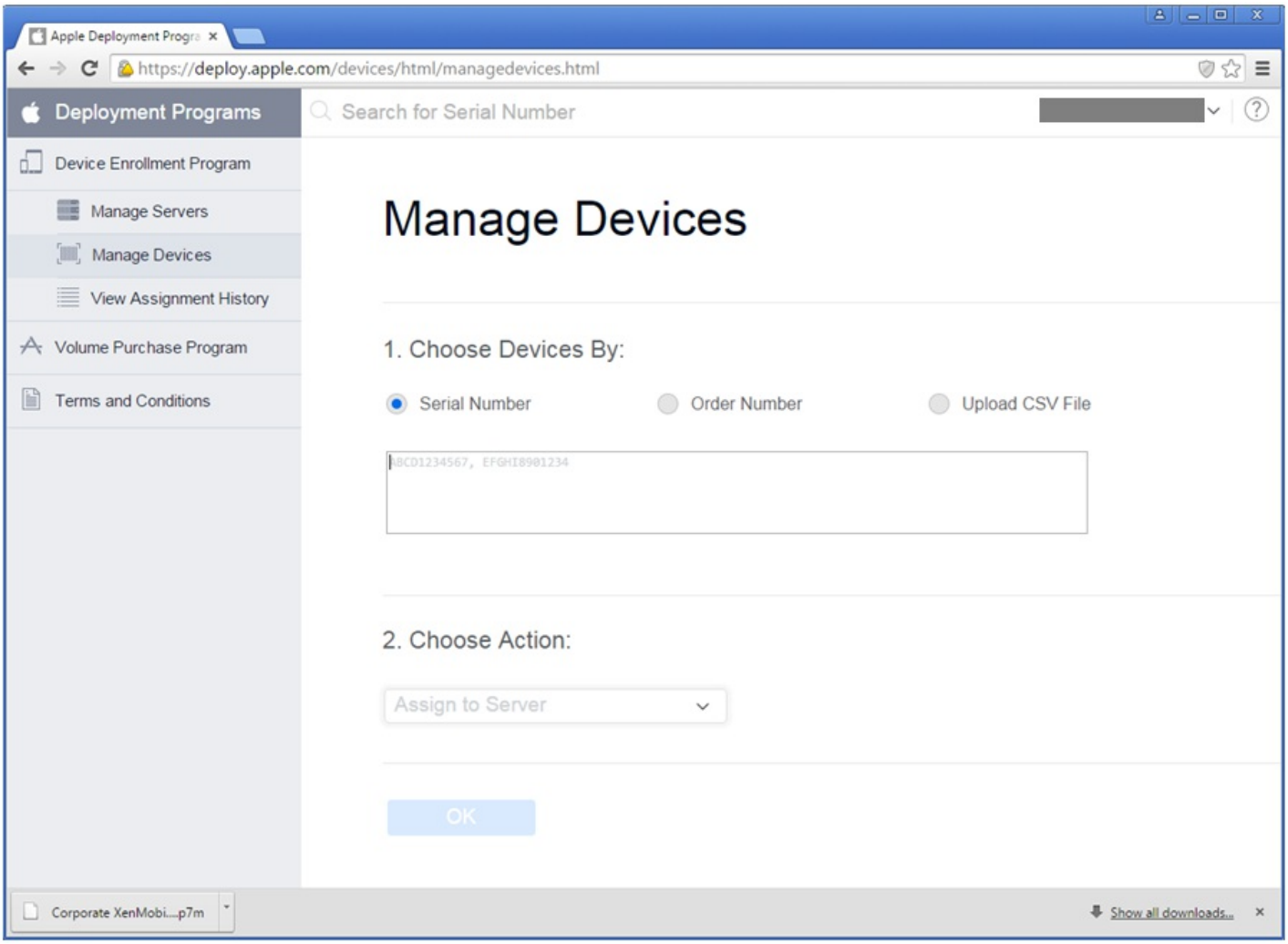
Gestion des appareils compatibles avec le programme DEP

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.

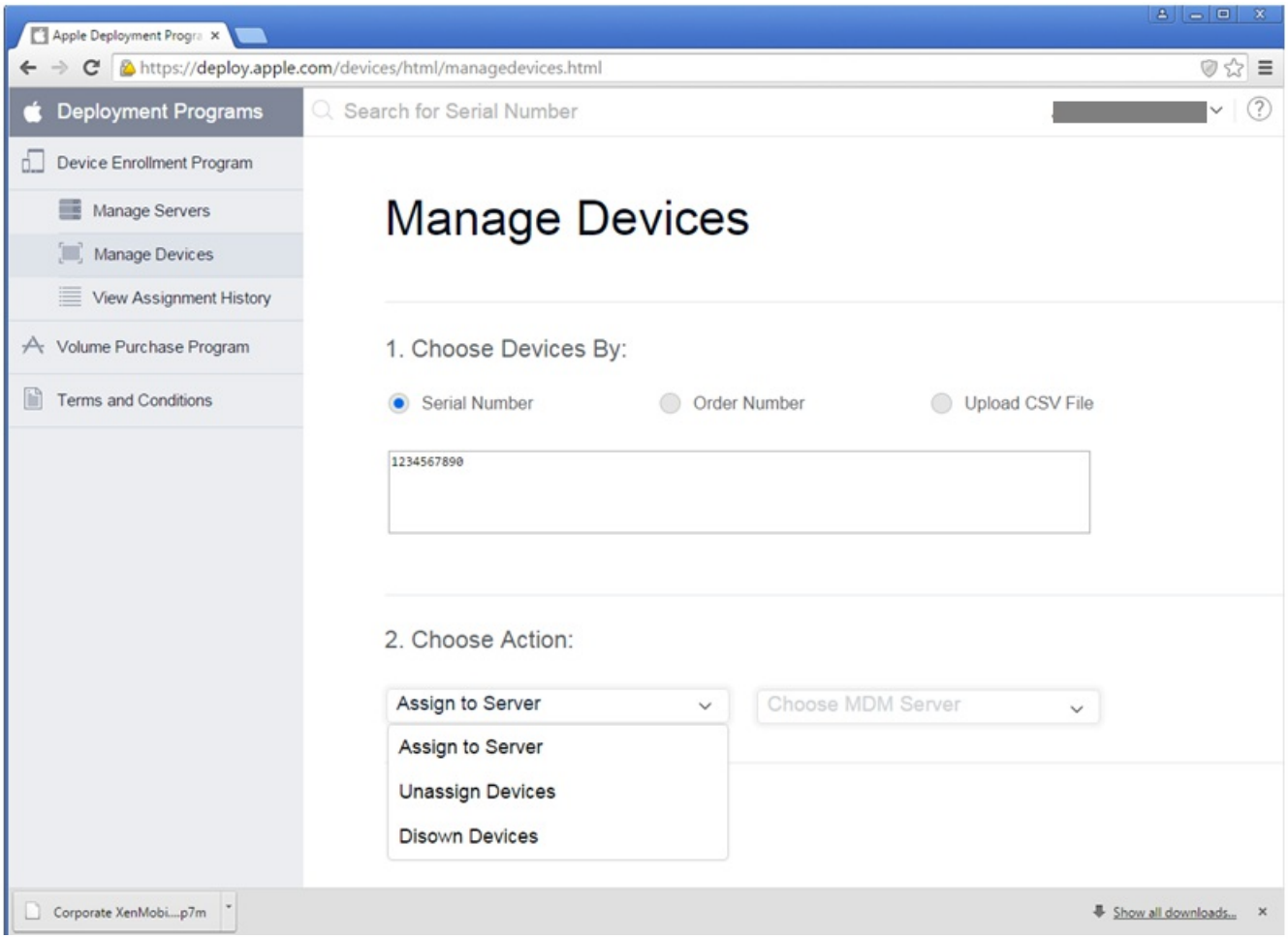
2. Cliquez sur **Programme d'inscription d'appareils**, sur **Gérer les appareils** et dans **Choisir des appareils**, sélectionnez l'option à utiliser pour charger et définir les appareils compatibles avec le programme DEP : **Numéro de série**, **Numéro de commande** ou **Télécharger un fichier CSV**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

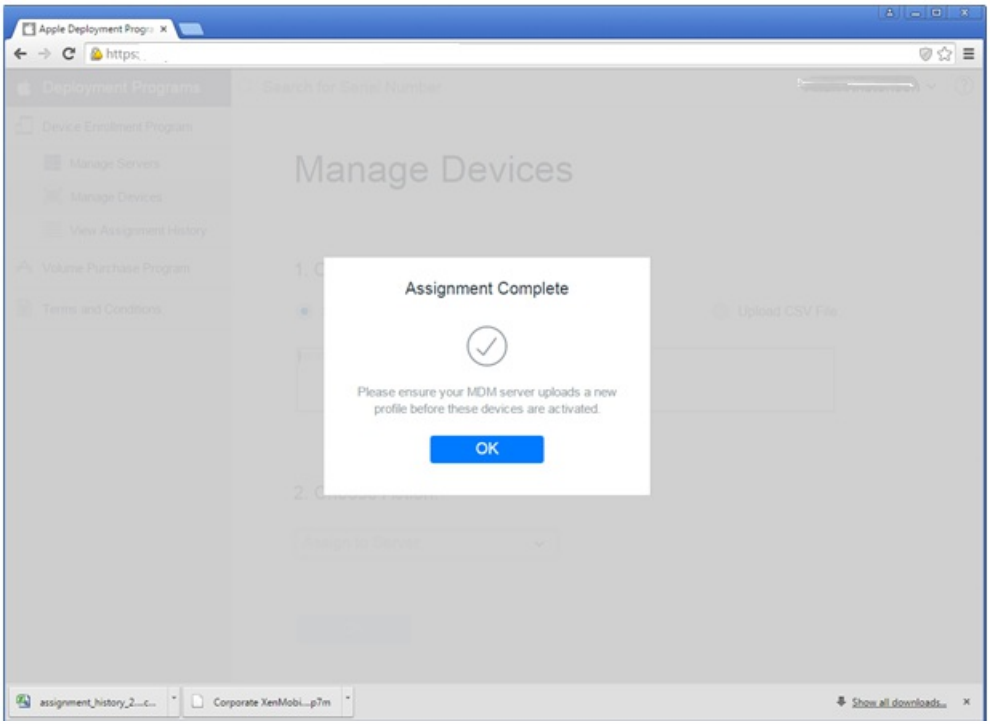


3. Sous **Choisir une action**, pour attribuer vos appareils à un serveur XenMobile, cliquez sur **Attribuer au serveur**, et dans la liste, cliquez sur le nom de votre serveur XenMobile et cliquez sur **OK**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Vos appareils DEP sont maintenant associés au serveur XenMobile sélectionné.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

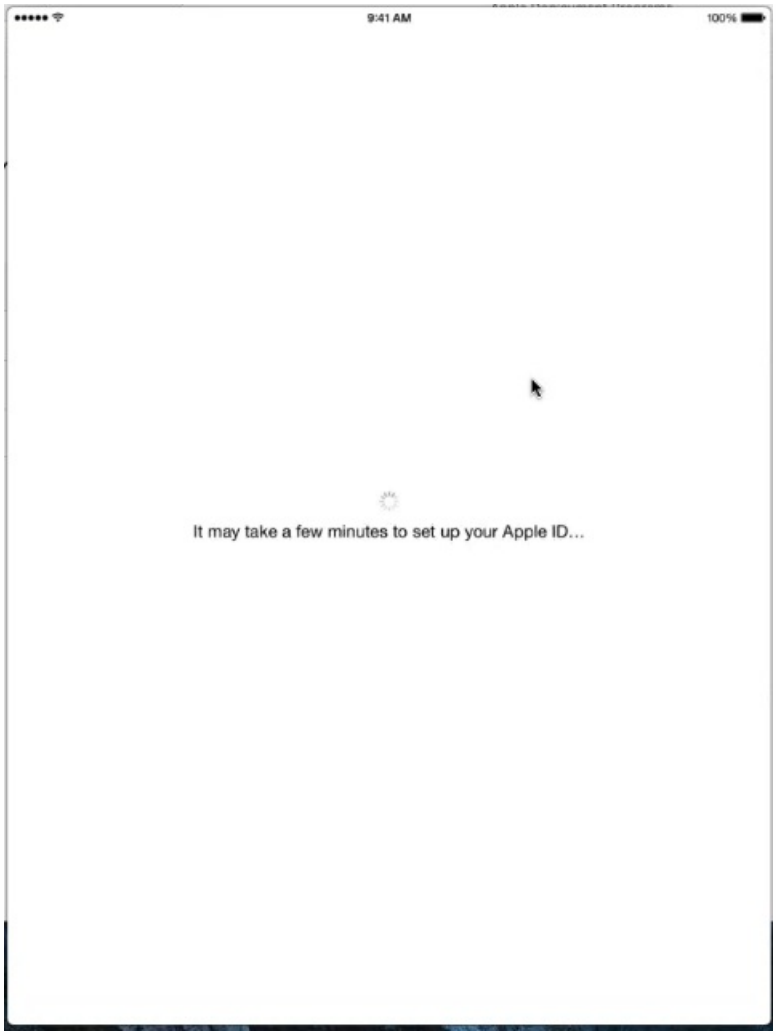
3. L'appareil démarre automatiquement le processus d'inscription d'appareils de XenMobile. Ils suivent l'assistant pour inscrire l'appareil auprès du serveur XenMobile associé à l'appareil compatible avec le programme DEP.

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.



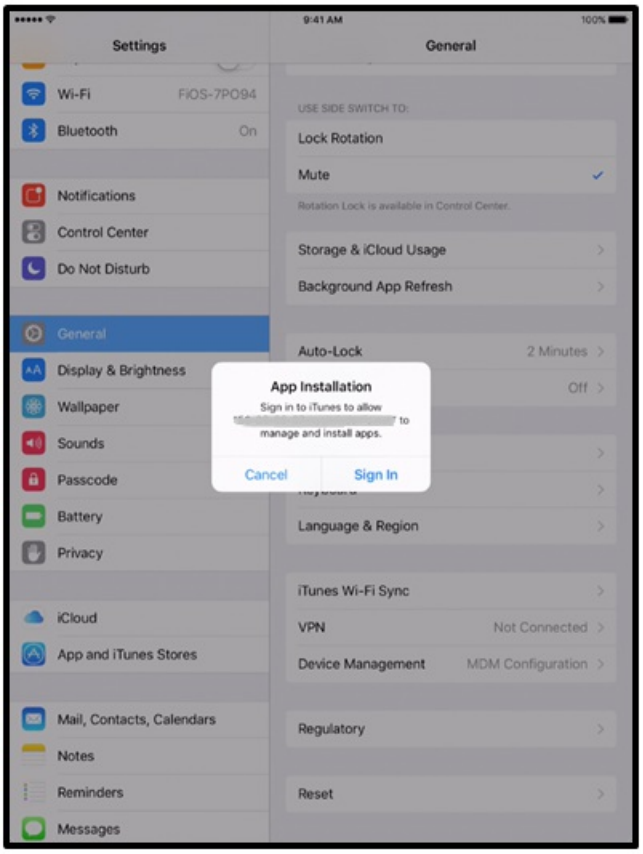
4. La configuration DEP que vous avez configurée dans la console XenMobile est transmise à l'appareil. Les utilisateurs suivent l'assistant pour configurer l'appareil.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Il est possible qu'ils soient invités à se connecter à iTunes de façon à ce que Worx Home puisse être téléchargé.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Ils ouvrent Worx Home 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 Worx.

Le reste des applications requises est transmis à l'appareil.

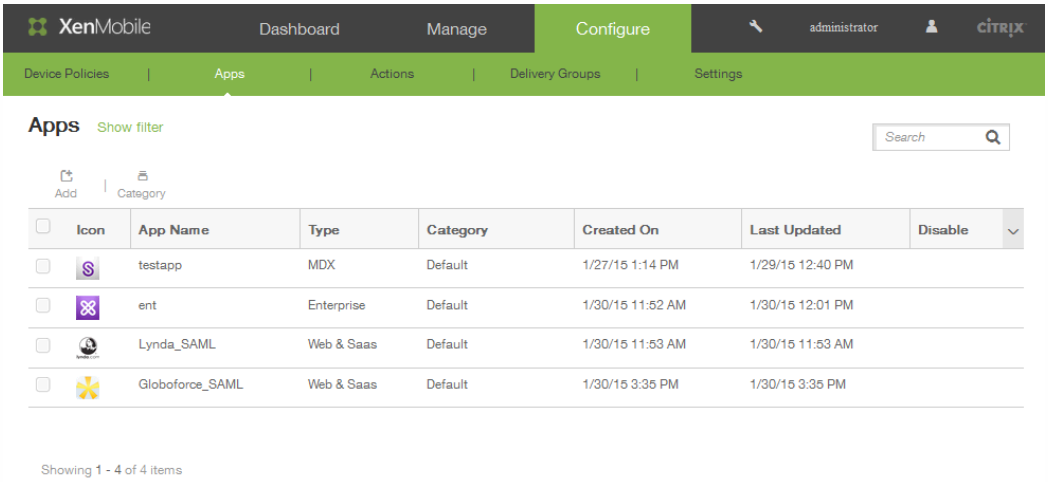
© 1999-2017 Citrix Systems, Inc. All rights reserved.

VPP iOS

Jul 25, 2016

Vous pouvez configurer des paramètres spécifiques au Programme d'achat en volume iOS (VPP) dans XenMobile. Le programme VPP iOS simplifie la recherche, l'achat et la distribution d'applications en bloc pour une organisation. Le programme VPP fournit une solution simple et évolutive destinée à gérer les besoins en contenu de l'organisation.

Après avoir enregistré et validé les paramètres VPP iOS dans XenMobile, les applications achetées sont ajoutées au tableau de l'onglet Applications dans la console XenMobile.

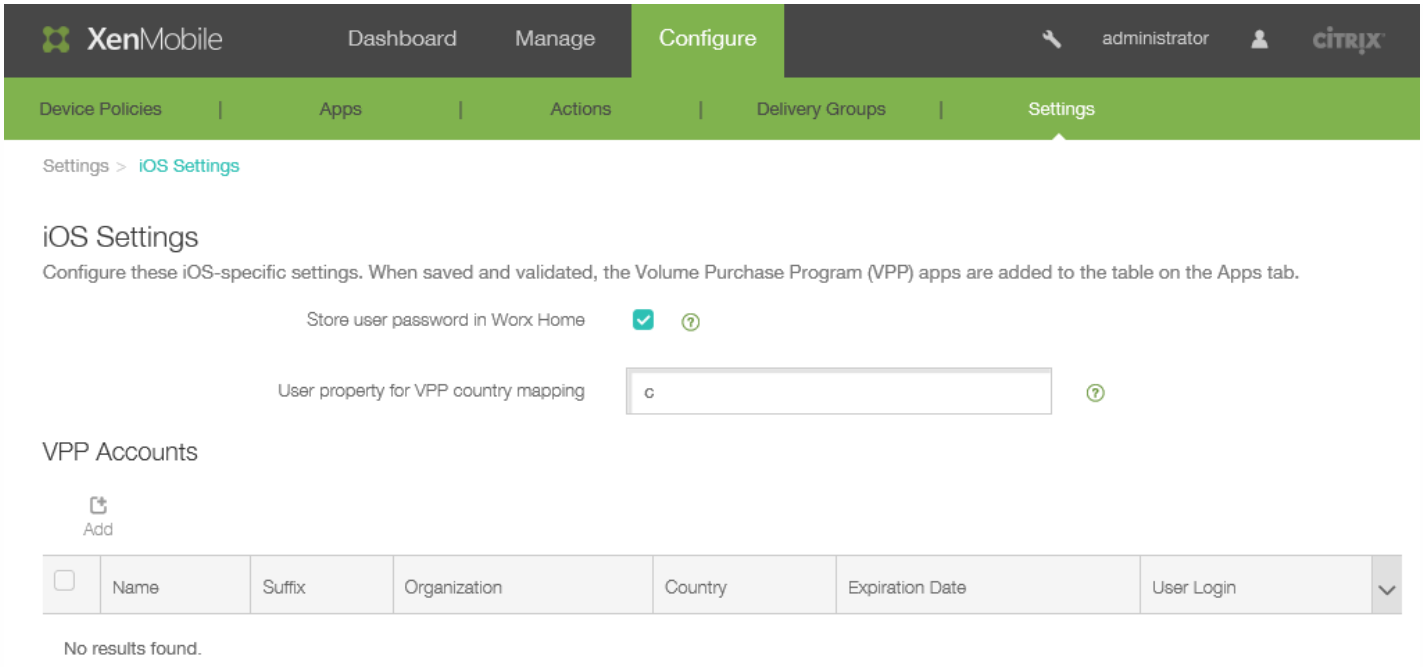


Pour configurer VPP iOS dans XenMobile

Dans la console Web XenMobile, cliquez sur **Configurer** > **Paramètres** > **Plus** > **Paramètres iOS**.

L'écran de configuration VPP iOS s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

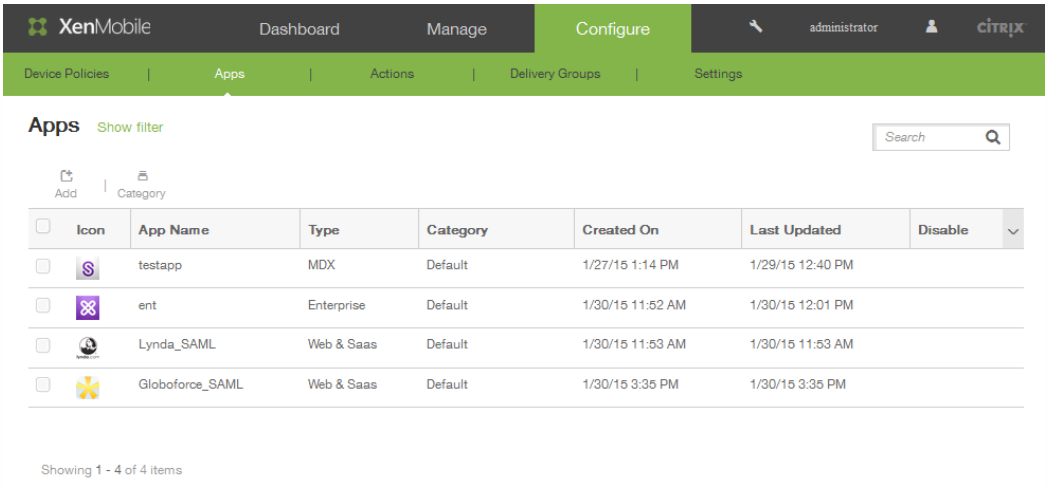


1. Dans Stocker le mot de passe utilisateur dans Worx Home, sélectionnez la case à cocher pour stocker de façon sécurisée un nom d'utilisateur et un mot de passe dans Worx Home en vue de l'authentification sur XenMobile.
2. Dans Propriété utilisateur du choix de pays pour le Volume Purchasing Program (VPP), entrez un code pour autoriser les utilisateurs à télécharger des applications à partir de magasins d'applications spécifiques à un pays.

   Ce mappage est utilisé 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 distribué au Royaume-Uni. Contactez votre administrateur de plan VPP pour plus d'informations sur le choix du code de pays.

3. Cliquez sur **Ajouter** sous **Comptes VPP**.
4. Ajoutez un nom et un suffixe.
5. Dans Jeton d'entreprise, entrez un jeton qui représente le jeton de service VPP généré quand un utilisateur effectue des achats dans l'App Store d'Apple via un compte d'entreprise. Le jeton est utilisé pour valider la licence VPP. Par exemple, si vous disposez d'un compte Apple VPP d'entreprise, accédez à https://vpp.itunes.com, cliquez sur **Business**, et connectez-vous avec votre identifiant de compte Apple VPP pour récupérer les informations appropriées.
6. Cliquez sur Enregistrer. Les informations sont alors affichées dans le tableau Applications :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

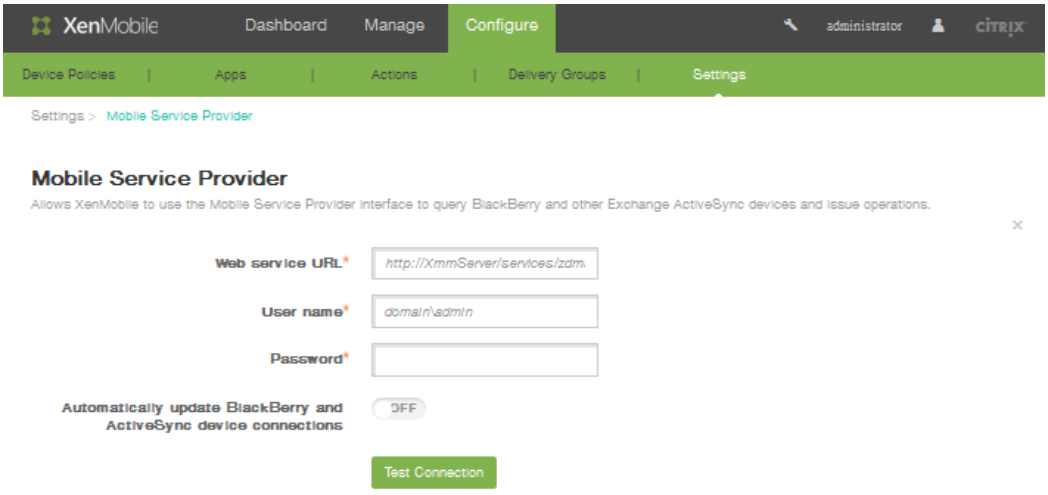
Fournisseur de services mobiles

Jul 25, 2016

Vous pouvez configurer XenMobile de manière à ce qu'il utilise l'interface du fournisseur de services mobiles pour interroger les appareils BlackBerry et d'autres appareils Exchange ActiveSync et effectuer des opérations.

Pour configurer le fournisseur de services mobiles

1. Dans la console Web XenMobile, cliquez Configurer > Paramètres > Plus > Fournisseur de services mobiles.
   La page de configuration Fournisseur de services mobiles s'affiche.



2. Dans URL du service Web, entrez l'adresse URL du service Web, par exemple, http://ServeurXmm/services/xdmservice
3. Dans Nom d'utilisateur, entrez le nom d'utilisateur au format domaine\administrateur
4. Dans Mot de passe, entrez le mot de passe.
5. Dans Mettre à jour automatiquement les connexions aux appareils BlackBerry et ActiveSync, cliquez sur ON si vous souhaitez activer cette option. Le paramètre par défaut est OFF.
6. Cliquez sur Tester la connexion pour vérifier la connexion.
7. Cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contrôle d'accès réseau

Jul 25, 2016

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

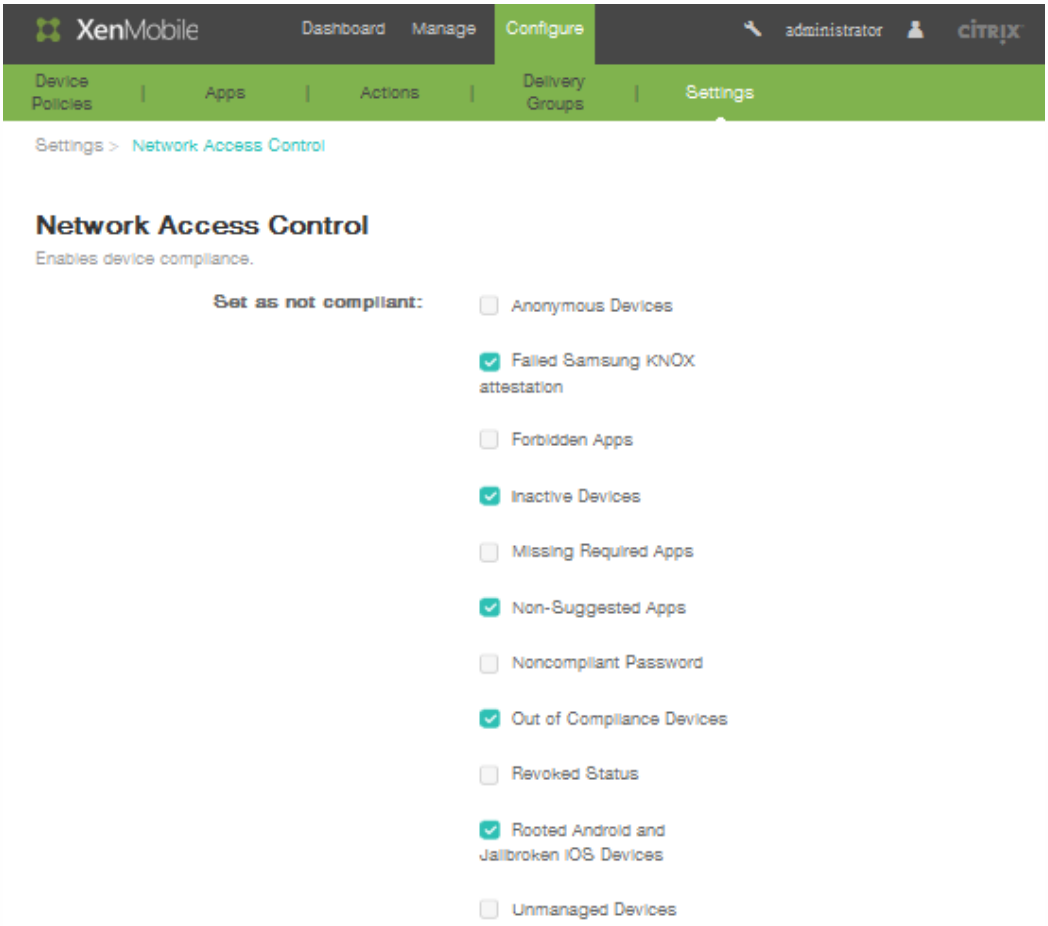
appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

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.

> ## 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 et/ou qui ne sont pas inscrits sont marqués comme Non conformes et seront bloqués sur votre réseau par le boîtier NAC.

Pour configurer le contrôle d'accès réseau dans XenMobile

1. Dans la console Web XenMobile, cliquez **Configurer > Paramètres > Plus > Contrôle d'accès réseau**. La page de configuration **Contrôle d'accès réseau** s'affiche.



2. 3. Cochez les cases correspondant aux filtres **Définir comme non conforme**que vous souhaitez activer.
3. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Samsung KNOX

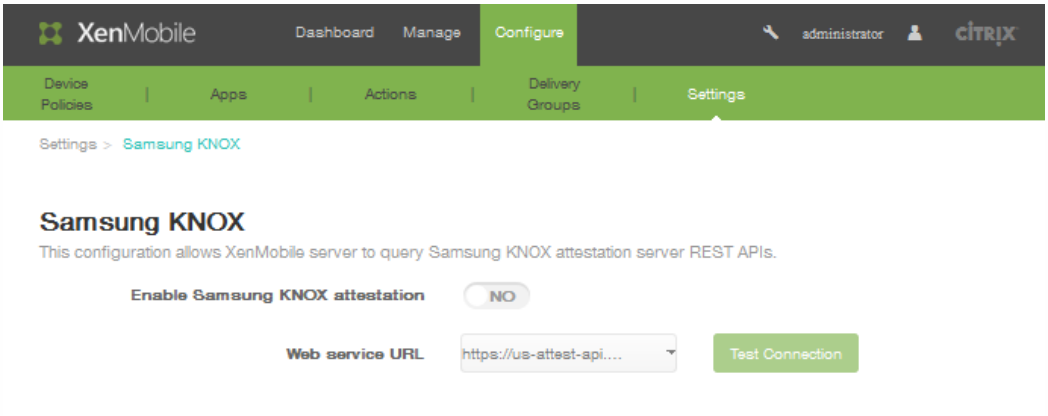
Jul 25, 2016

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.

Pour activer l'attestation Samsung KNOX

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > Samsung KNOX.
   La page de configuration Samsung KNOX s'affiche.



2. Dans Activer la certification Samsung KNOX, cliquez sur **OUI**.
3. Lorsque vous cliquez sur OUI dans l'étape 2, l'option **URL du service Web** est activée. Dans la liste, cliquez sur le serveur d'attestation approprié.
4. Cliquez sur **Tester la connexion** pour vérifier la connexion.
5. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriétés du serveur

Jul 25, 2016

XenMobile dispose de plus de 100 propriétés qui s'appliquent aux opérations du serveur. Cet article décrit certaines des propriétés de serveur les plus importantes et décrit en détail comment ajouter, modifier ou supprimer des propriétés de serveur.

Définitions des propriétés du serveur

Heure d'exécution du nettoyage du journal d'audit

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**.

Intervalle de nettoyage du journal d'audit (en jours)

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

Enregistreur d'audit

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

Rétention du journal d'audit (en jours)

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

Nettoyage du journal de déploiement (en jours)

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

Désactiver la vérification de serveur SSL

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**.

Délai d'inactivité en minutes

Nombre de minutes après lequel un administrateur inactif qui utilise l'API publique du serveur XenMobile pour accéder à la console XenMobile ou une application tierce, est déconnecté. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **5**.

Single Sign-On à NetScaler

Si la valeur est **False**, elle désactive la fonctionnalité de rappel de XenMobile durant le Single Sign-On depuis NetScaler vers le serveur XenMobile. La fonctionnalité de rappel est utilisée 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nettoyage du journal de session (en jours)

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

Téléchargement d'applications non authentifiées pour appareils Android

Si la valeur est **True**, vous pouvez télécharger des applications auto-hébergées sur des appareils Android exécutant Android for Work. Cette propriété est nécessaire 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**.

Téléchargement d'applications non authentifiées pour appareils Windows

Utilisé uniquement pour les anciennes versions de Worx Home 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**.

Ticket à usage unique XAM

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. La valeur par défaut est **3600000**.

Intervalle maximale d'inactivité (minutes) du portail en libre-service de XenMobile MDM

Nombre de minutes après lequel un utilisateur inactif est déconnecté du portail en libre-service de XenMobile. Un délai d'expiration de **0** signifie qu'un utilisateur inactif reste connecté. La valeur par défaut est **30**.

Ajout, modification ou suppression de propriétés de serveur

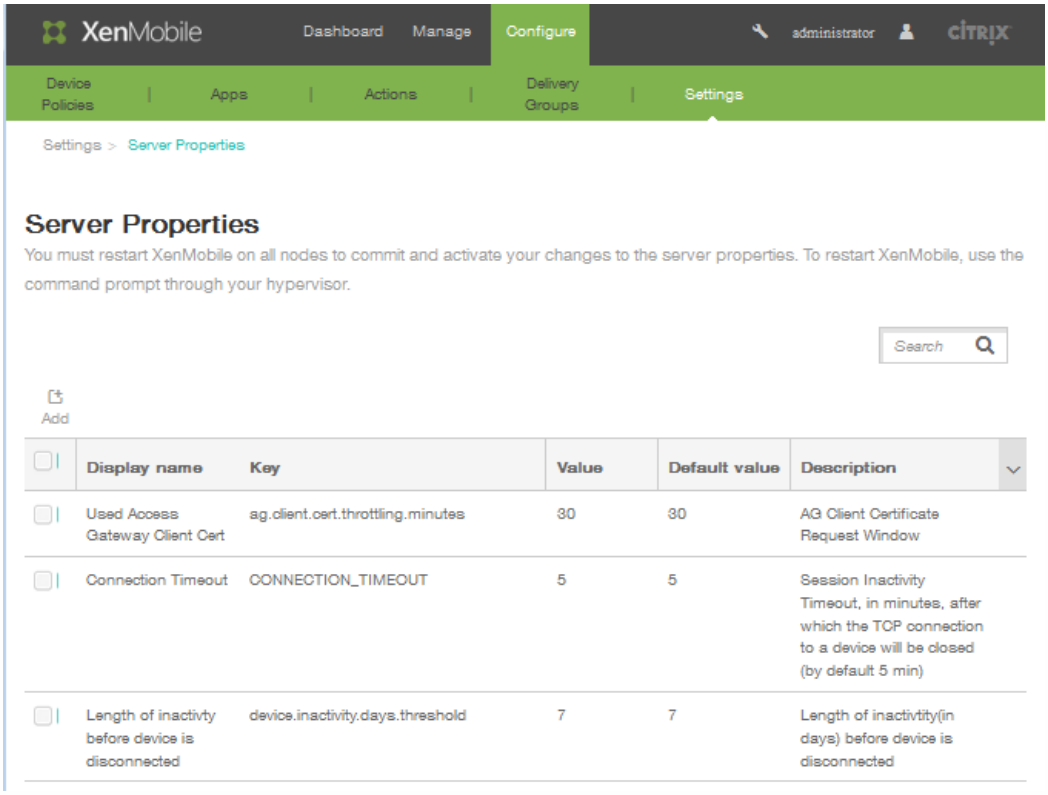
Dans XenMobile, vous pouvez appliquer des propriétés au serveur. Après avoir effectué des modifications, vous devez redémarrer XenMobile sur tous les nœuds pour valider et activer les modifications.

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

Pour configurer les propriétés de serveur dans XenMobile

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > Propriétés du serveur.
   La page de configuration Propriétés du serveur s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Procédez comme suit :
   - Cliquez sur Ajouter pour ajouter une nouvelle propriété de serveur.
   - Dans le tableau, cliquez pour sélectionner une propriété existante, puis dans le menu qui s'affiche, cliquez sur Modifier.
3. Si vous avez cliqué sur Ajouter dans l'étape 2, configurez les champs suivants :

- Clé : dans la liste, sélectionnez la clé appropriée.
  Remarque : 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** : ajoutez une description pour la nouvelle propriété de serveur (facultatif), puis cliquez sur Enregistrer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration du mode de serveur efficace XenMobile

Jul 25, 2016

Le mode de serveur XenMobile est la valeur définie dans les propriétés de serveur. Vous pouvez définir la valeur sur MAM, MDM ou ENT 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.

Pour plus d'informations sur la configuration du mode de serveur, veuillez consulter la section Propriétés du serveur.

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.

Le mode de serveur efficace est ajouté au journal du serveur à chaque fois qu'une licence est activée ou supprimée et lorsque le mode du serveur est modifié dans les propriétés du serveur. Pour de plus amples informations sur la création et l'affichage des fichiers journaux, consultez la section Support et maintenance de XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SysLog

Jul 25, 2016

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 seront enregistrés.

Vous pouvez configurer le serveur afin de collecter les informations suivantes :

- Les journaux système consignent les actions effectuées par XenMobile.
- Les journaux d'audit contiennent un enregistrement chronologique des activités système de 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

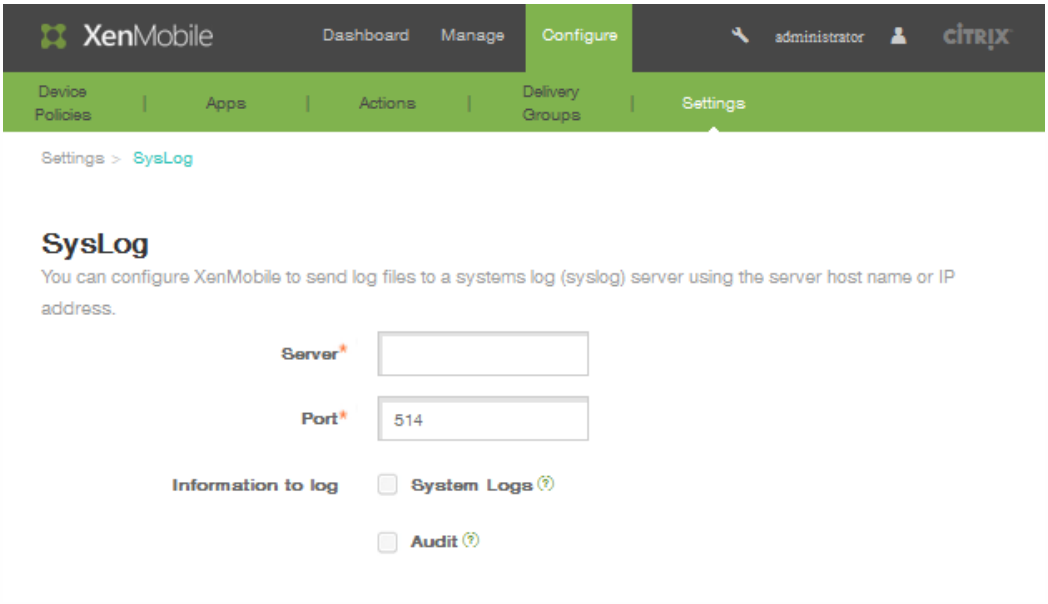
Vous pouvez utiliser ces informations pour analyser la source de l'alerte et prendre des mesures correctives si nécessaire.

> ## Remarque
>
> Dans les déploiements XenMobile 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.

Pour configurer un serveur syslog dans XenMobile

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > Syslog.
   La page de configuration Syslog s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Dans le champ Nom, entrez une adresse IP ou le nom de domaine complet (FQDN) de votre serveur syslog.
3. Dans Port, saisissez le numéro de port. Le port est défini par défaut sur 514.
4. Dans Informations à consigner, sélectionnez ou désélectionnez Journaux système et Audit.
   - Les journaux système consignent les actions effectuées par XenMobile.
   - Les journaux d'audit contiennent un enregistrement chronologique des activités système de XenMobile.
5. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

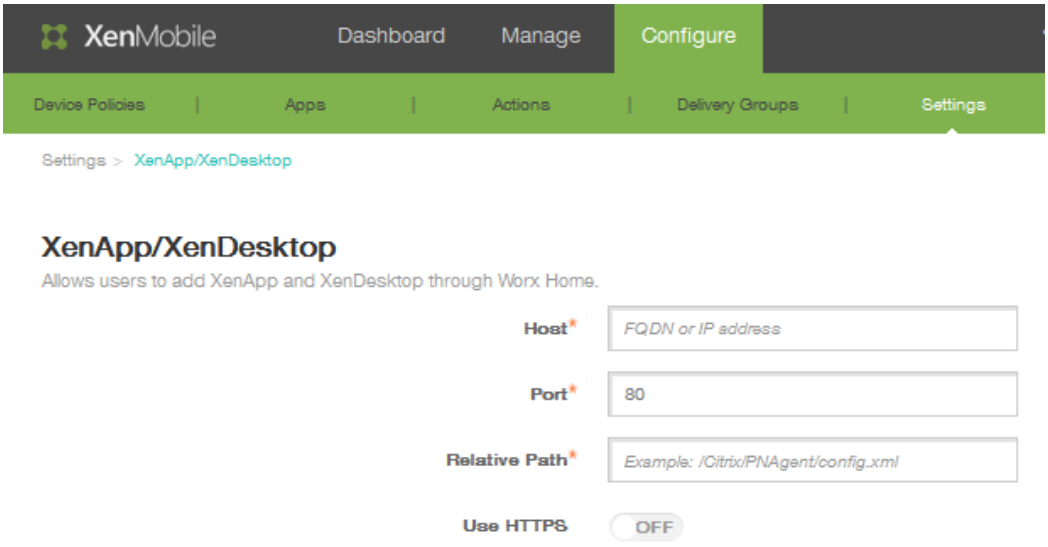
Pour configurer XenApp et XenDesktop

Jul 25, 2016

XenMobile peut collecter des applications depuis XenApp et XenDesktop et les rendre disponibles aux utilisateurs d'appareils mobiles dans Worx Store. Les utilisateurs s'abonnent directement aux applications dans Worx Store et les lancent depuis WorxHome. 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 pour StoreFront ou le site Interface Web.

1. Dans la console Web XenMobile, cliquez sur **Configurer > Paramètres > Plus > XenApp/XenDesktop**.
   La page de configuration de **XenApp/XenDesktop** s'affiche.



2. Dans **Hôte**, entrez le nom de domaine complet (FQDN) ou l'adresse IP pour StoreFront ou le site Interface Web.
3. Dans **Port**, saisissez le numéro de port pour StoreFront ou le site Interface Web. La valeur par défaut est 80.
4. Dans **Chemin relatif**, entrez le chemin d'accès. Par exemple, /Citrix/Store/PNAgent/config.xml
5. Dans **Utiliser HTTPS**, sélectionnez **ON** pour activer l'authentification sécurisée entre StoreFront ou le site Interface Web et l'appareil client. La valeur par défaut est **OFF**.
6. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

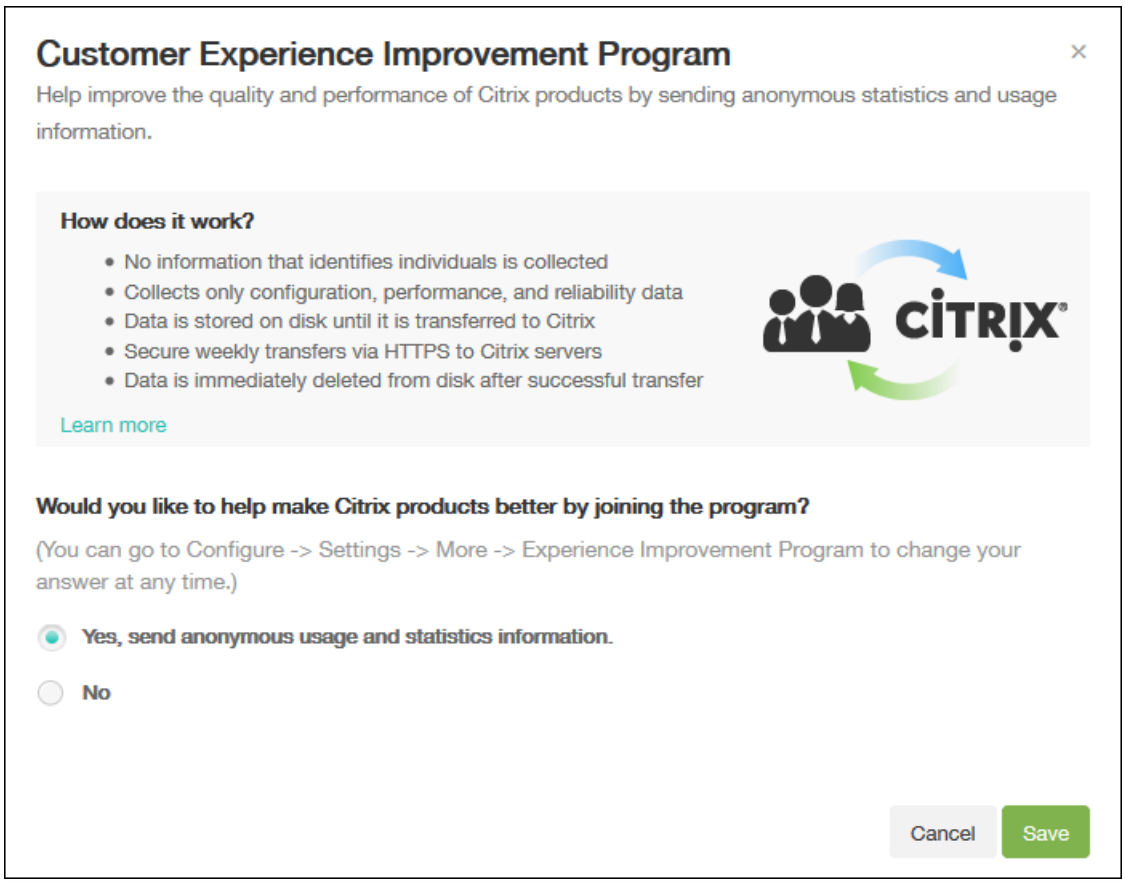
Programme d'amélioration de l'expérience utilisateur

Jul 25, 2016

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).

CEIP lors de l'installation ou la mise à niveau de XenMobile

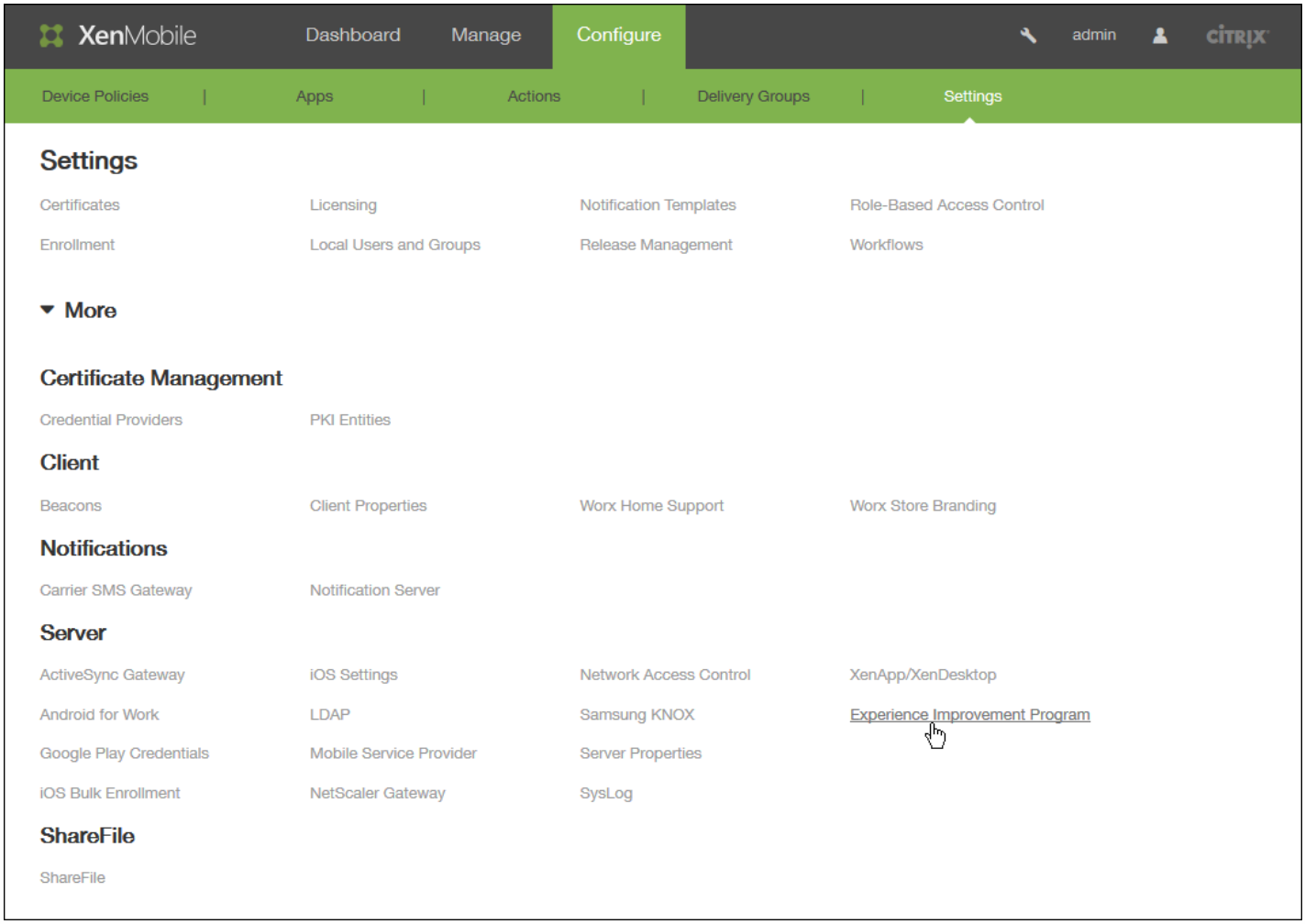
La première fois que vous installez XenMobile ou lorsque vous effectuez une mise à jour, vous pouvez voir la boîte de dialogue suivante, dans laquelle vous devez indiquer si vous voulez participer, puis cliquez sur **Enregistrer**.



Modification de votre paramètre de participation au programme CEIP

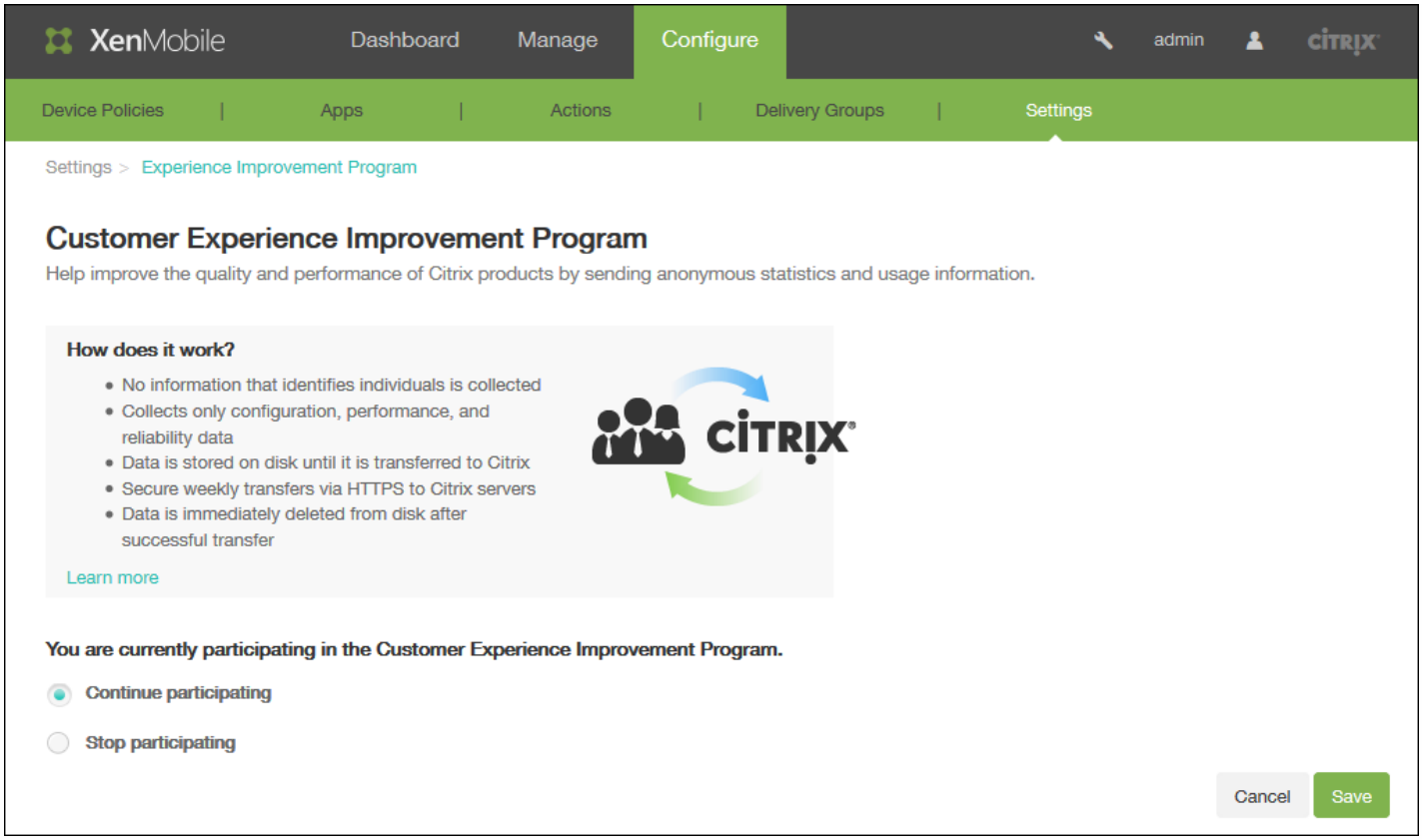
1. Pour modifier votre paramètre de participation au programme CEIP, dans la console XenMobile, cliquez sur **Configurer -> Paramètres**. La page **Paramètres** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. La figure suivante illustre la page d'un utilisateur participant au programme.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Si vous participez actuellement au programme CEIP et que vous voulez arrêter, cliquez sur **Ne plus participer au programme**.

3. Si vous ne participez pas actuellement au programme CEIP et que vous voulez y adhérer, cliquez sur **Participer au programme**.

4. Cliquez sur **Enregistrer**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Inscription en bloc d'appareils iOS

Jul 25, 2016

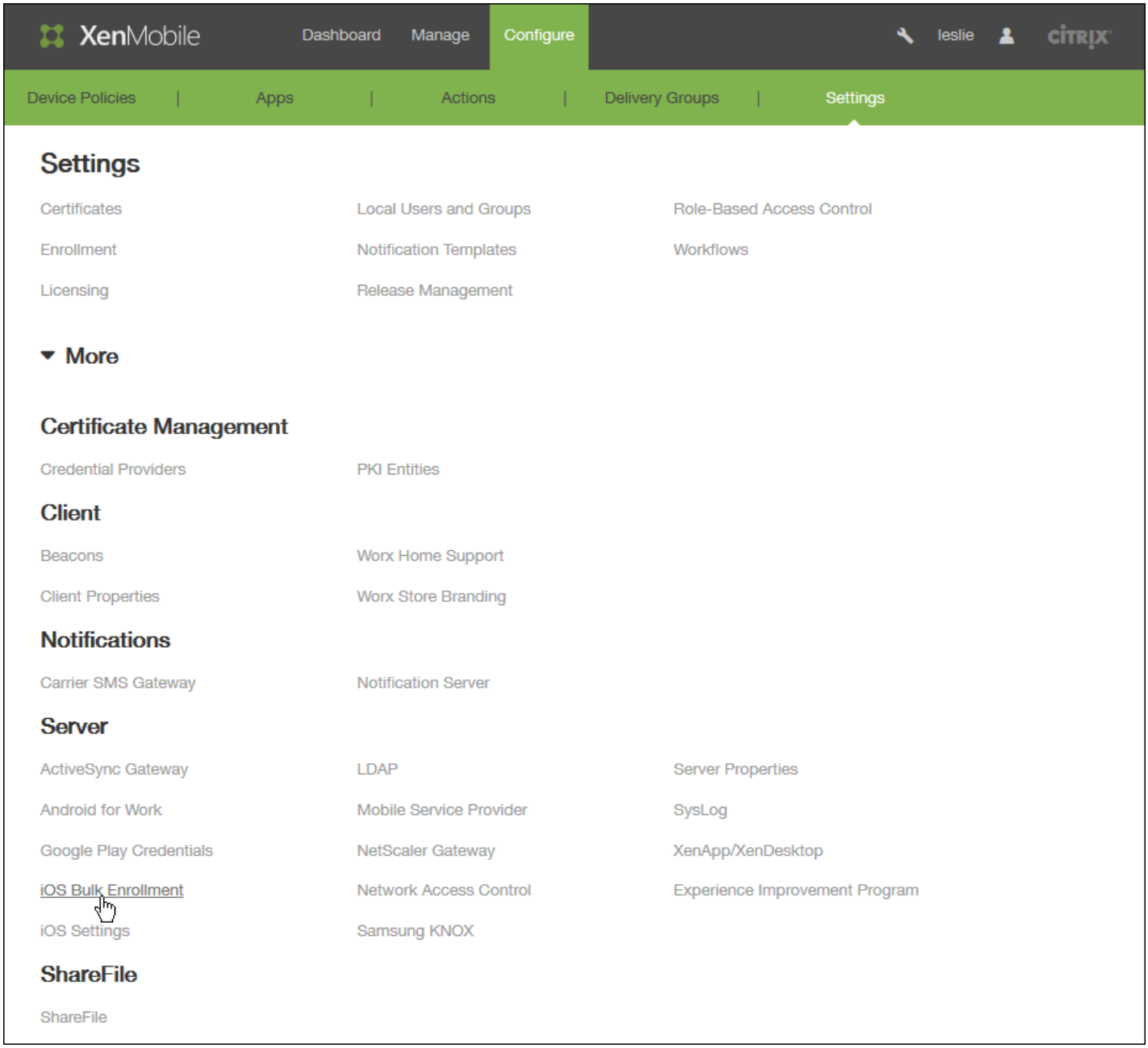
Vous pouvez inscrire un grand nombre d'appareils iOS dans XenMobile de deux façons. Vous pouvez utiliser le programme Device Enrollment Program (DEP) d'Apple pour inscrire les appareils que vous achetez directement depuis Apple ou auprès d'un revendeur Apple agréé, ou vous pouvez utiliser Apple Configurator pour inscrire des appareils, qu'ils aient été achetés directement ou non auprès d'Apple.

Avec le programme DEP, vous n'avez aucune tâche de préparation à effectuer sur les appareils ; vous envoyez les numéros de série des appareils ou les numéros de commande via le programme DEP et les appareils sont configurés et inscrits dans XenMobile. Une fois les appareils inscrits, ils sont prêts à l'emploi et peuvent être distribués aux utilisateurs. Par ailleurs, lorsque vous configurez des appareils avec le programme DEP, vous pouvez supprimer certaines des étapes de l'assistant d'installation que les utilisateurs doivent d'habitude réaliser la première fois qu'ils démarrent leurs appareils. Pour de plus amples informations sur la configuration du programme DEP, reportez-vous à la page Device Enrollment Program d'Apple.

Avec Apple Configurator, vous associez des appareils à un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure et à 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, la première fois 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'aide de Apple Configurator, consultez la page Apple Configurator d'Apple.

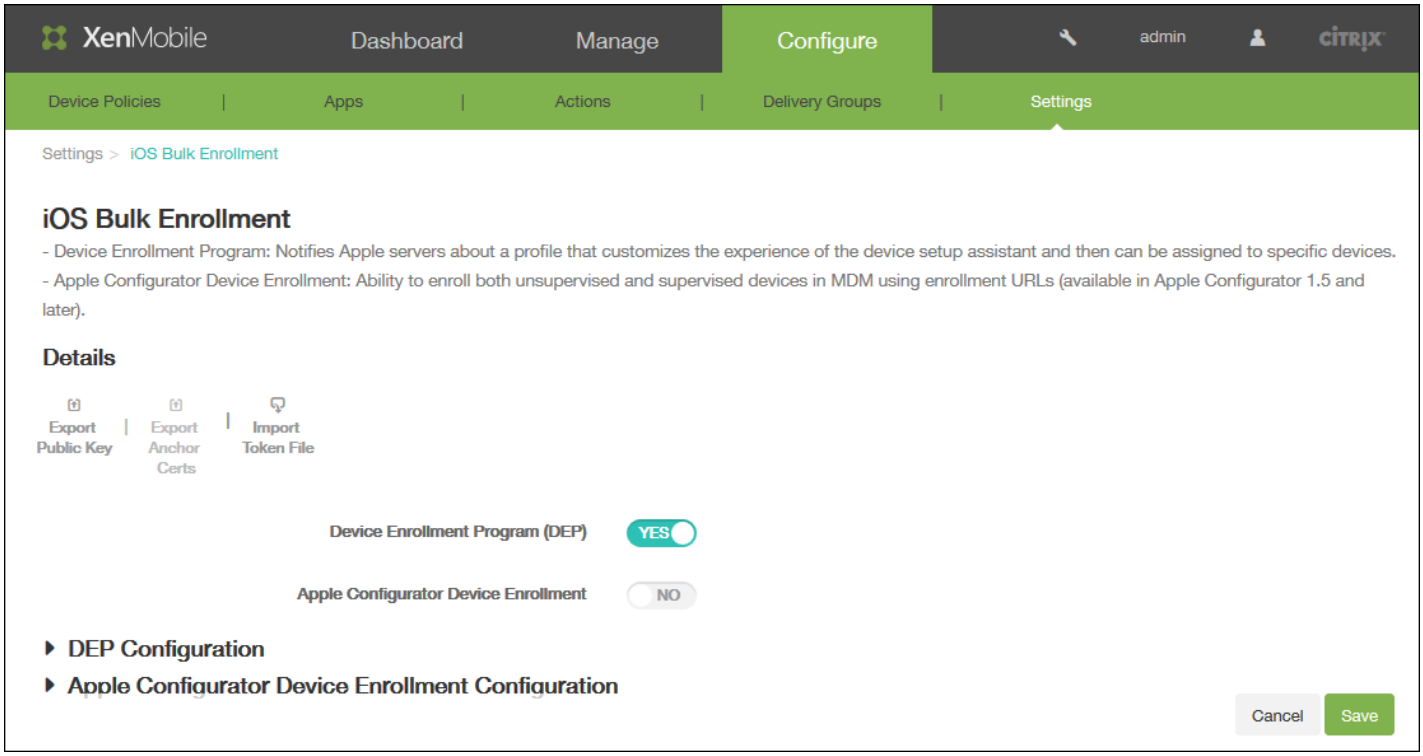
1. Dans la console XenMobile, cliquez sur **Configurer > Paramètres**. La page **Paramètres** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



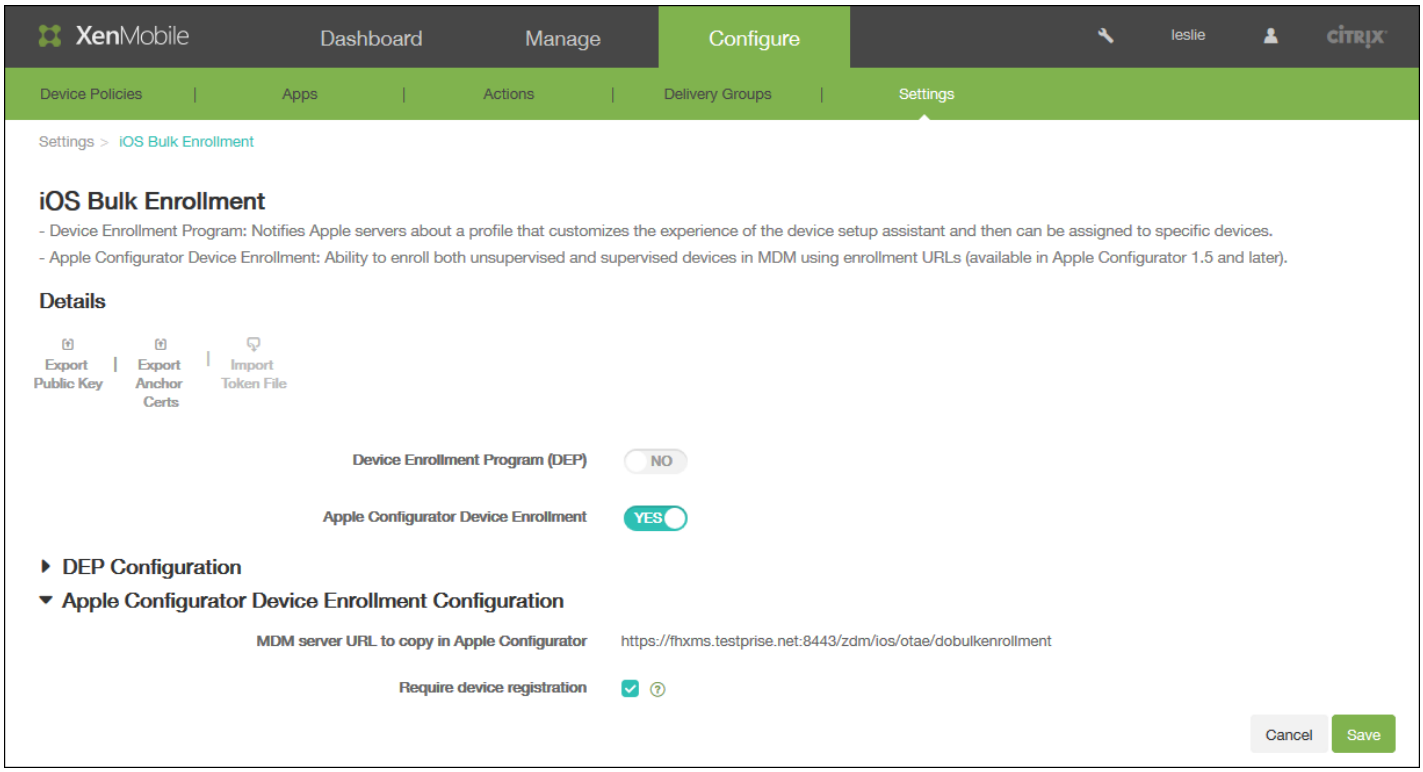
2. Sous **Serveur**, cliquez sur **Inscription en bloc iOS**. La page **Inscription en bloc iOS** s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Si vous configurez les paramètres du programme DEP, veuillez consulter la section Configuration des paramètres du programme DEP ; si vous configurez les paramètres d'Apple Configurator, veuillez consulter la section Configuration des paramètres d'Apple Configurator.

Configuration des paramètres d'Apple Configurator



© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Définissez **Device Enrollment Program** sur **Non**.

2. Définissez **Autoriser Apple Configurator Device Enrollment** sur **Oui**.

3. Développez **Configuration du DEP Apple Configurator** et prenez note des paramètres suivants et configurez-les :

- **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.
- **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.

> ## 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 5 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 **Anchor**, si XenMobile n'utilise pas un certificat SSL approuvé.

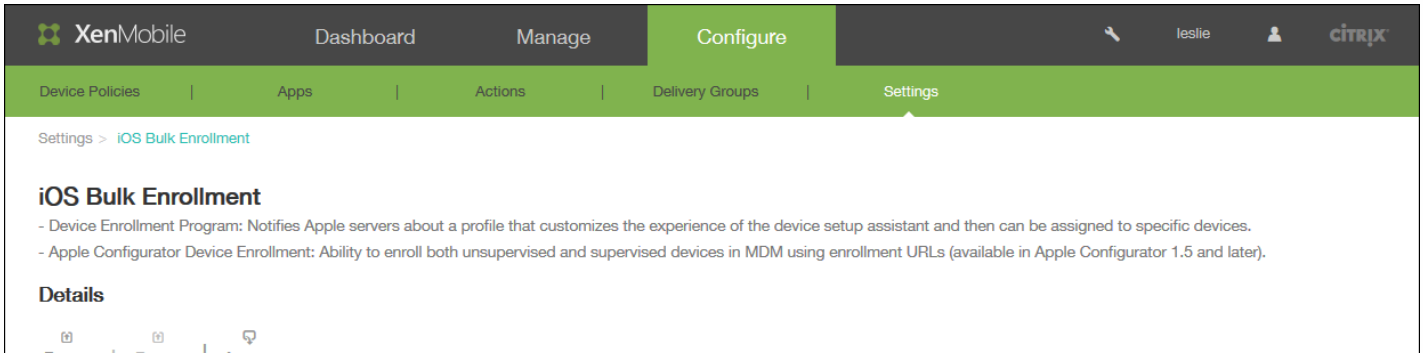
8. Utilisez un câble Dock Connector vers USB pour connecter des appareils au Mac exécutant Apple Configurator pour configurer simultanément jusqu'à 30 appareils connectés. Si vous ne disposez pas d'un Dock Connector, utilisez un ou plusieurs hubs (alimentés) USB 2.0 haute vitesse pour connecter les appareils.

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.

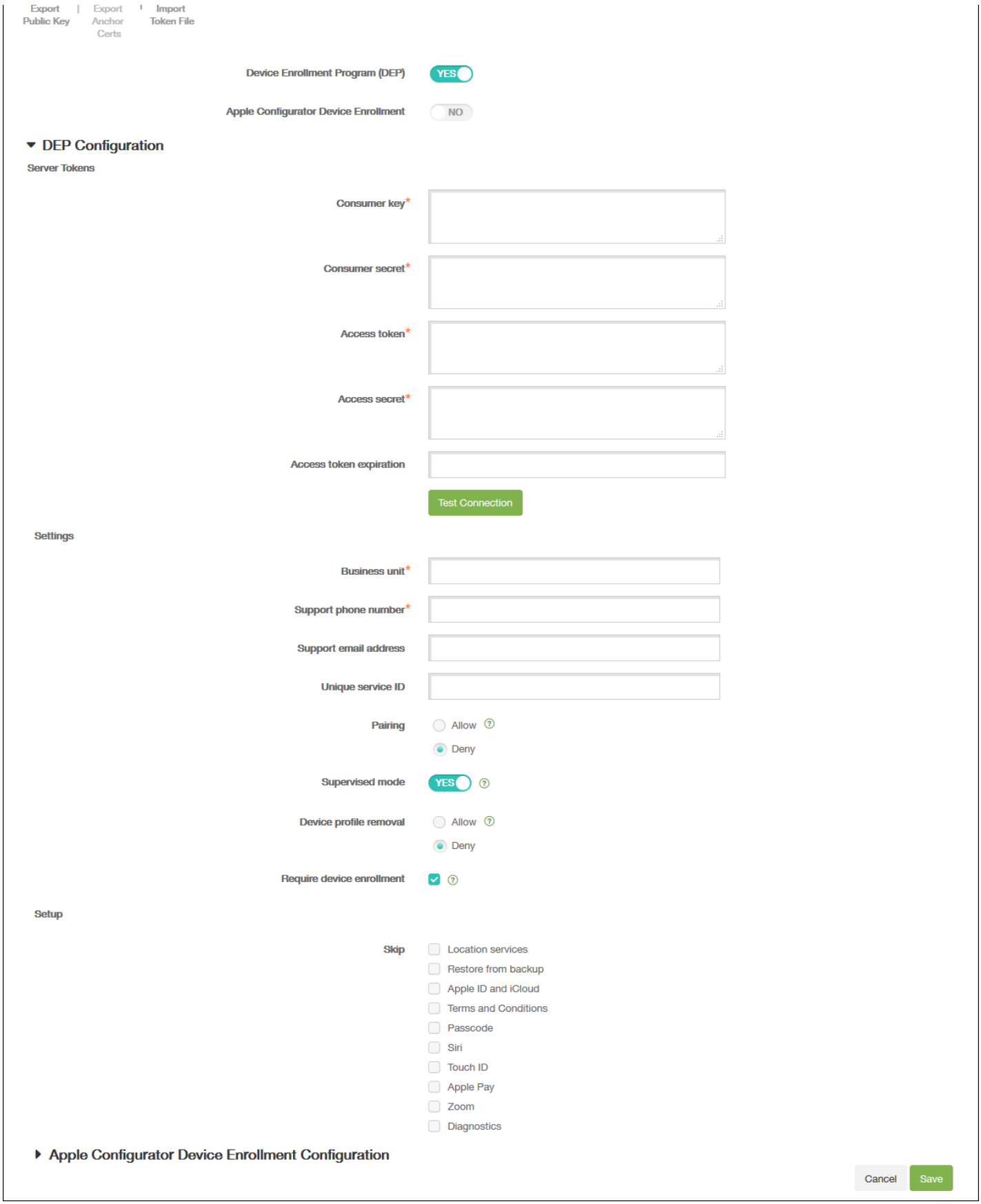
10. Dans Apple Configurator, configurez les stratégies dont vous avez besoin.

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.

Configuration des paramètres DEP



© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Définissez **Device Enrollment Program** sur **Oui**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Définissez **Autoriser Apple Configurator Device Enrollment** sur **Non**.

3. Développez **Configuration DEP** et configurez les paramètres suivants :

Jetons de serveur

- **Clé du client** :
- **Secret du client** :
- **Jeton d'accès** :
- **Secret d'accès** :
- **Expiration du jeton d'accès** :

Paramètres

- **Division** :
- **Numéro de téléphone de l'assistance** :
- **Adresse e-mail de l'assistance** :
- **ID de service unique** :
- **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 **Autoriser**.
- **Mode supervisé** : doit être défini sur **Oui** si vous utilisez Apple Configurator pour gérer les appareils inscrits via le programme DEP. La valeur par défaut est **Oui**.
- **Suppression de profil** : sélectionnez cette option pour autoriser les appareils à utiliser un profil qui peut être supprimé à distance. La valeur par défaut est **Autoriser**.
- **Exiger l'inscription des appareils** : sélectionnez cette option pour obliger les utilisateurs à inscrire leurs appareils. La valeur par défaut n'exige pas d'inscription.

Installation

Sélectionnez les étapes de l'Assistant de configuration iOS que vos utilisateurs ne devront *pas* utiliser lorsqu'ils démarrent leurs appareils pour la première fois.

- **Ignorer**
  - **Emplacement** : configurez le service de localisation sur 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.
  - **Apple ID et iCloud** : configurez un Apple ID et un compte iCloud pour l'appareil.
  - **Termes et conditions** : exigez que l'utilisateur accepte les termes et conditions pour utiliser l'appareil.
  - **Code secret** : créez un code secret pour l'appareil.
  - **Siri** : utilisez ou non Siri sur l'appareil.
  - **Touch ID** : configurez la fonction Touch ID sur l'appareil.
  - **Apple Play** : configurez l'accès à Apple Play sur l'appareil.
  - **Zoom** : configurez la résolution d'affichage (standard ou zoom).
  - **Diagnostics** : configurez cette option si vous souhaitez partager les données d'incidents et les statistiques d'utilisation avec Apple.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

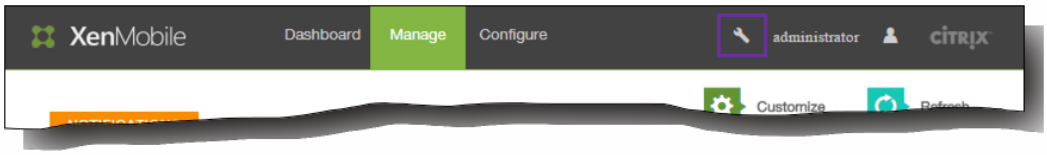
Support et maintenance de XenMobile

Jul 25, 2016

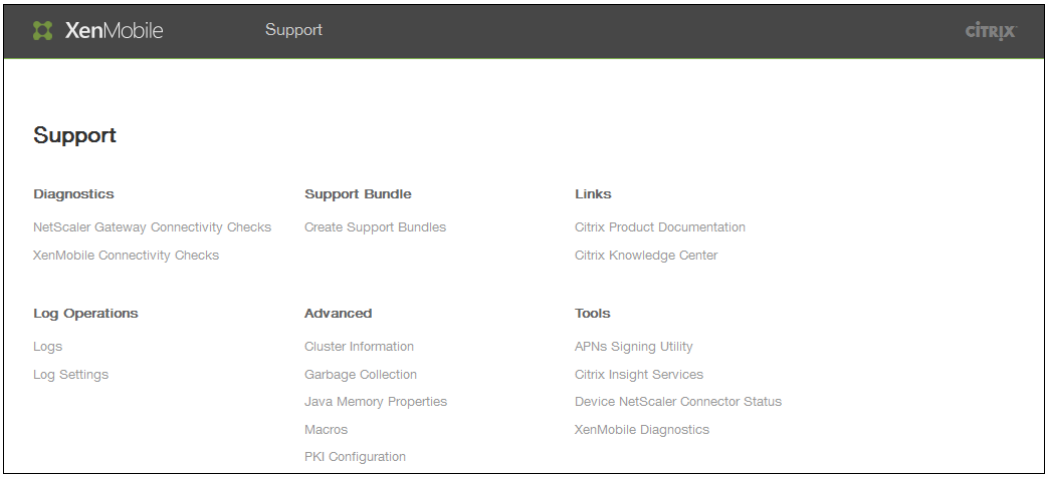
Utilisez la page Support de XenMobile pour accéder à des informations et outils de support. Vous pouvez également effectuer des actions à partir de l'interface de ligne de commande. Pour de plus amples informations, consultez la section Options d'interface de ligne de commande XenMobile.

Pour accéder à la page Support

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



La page Support s'affiche dans un autre onglet de navigateur :



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

API REST XenMobile : références

Jul 25, 2016

Vous pouvez appeler les services REST à l'aide de n'importe quel client REST et l'API REST de XenMobile pour appeler les services qui sont exposés au travers de la console XenMobile. L'API n'exige pas de connexion à la console XenMobile pour appeler les services décrits dans cet article.

Vous devez utiliser l'une des autorisations suivantes pour accéder à l'API REST :

- Autorisation d'accès à l'API publique définie dans le cadre de la configuration d'accès basé sur un rôle (pour plus d'informations sur la configuration d'accès basé sur un rôle, consultez la section Configuration de rôles avec RBAC)
- Autorisation de super utilisateur

Vous pouvez appeler les services d'API REST à l'aide d'un client REST.

Pour appeler les services D'API REST

Les éléments ci-dessous sont des exemples illustrant comment appeler l'API REST à l'aide de chacune des méthodes précédentes.

> **Remarque**
>
> dans les exemples suivants, modifiez le nom de l'hôte et le numéro de port afin qu'ils correspondent à votre environnement.

À l'aide d'un client REST

Cet exemple utilise le client Advanced REST pour Chrome.

Connexion

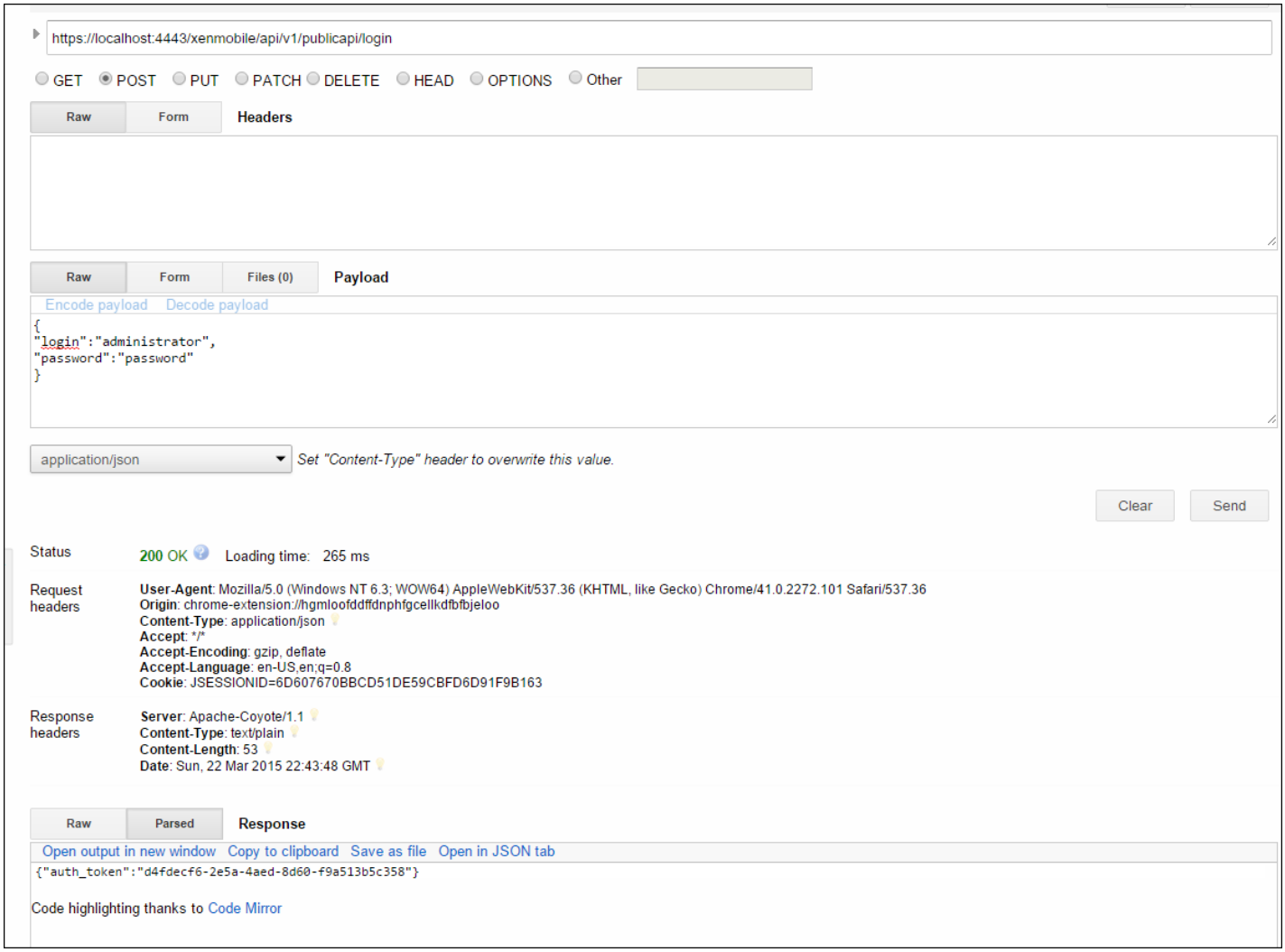
URL : https://:/xenmobile/api/v1/authentication/login

Requête : { "login":"administrator", "password":"password" }

Type de méthode : POST

Content-type : application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Obtenir les groupes de mise à disposition par filtre

URL : /xenmobile/api/v1/deliverygroups/filter

Requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn":"id",

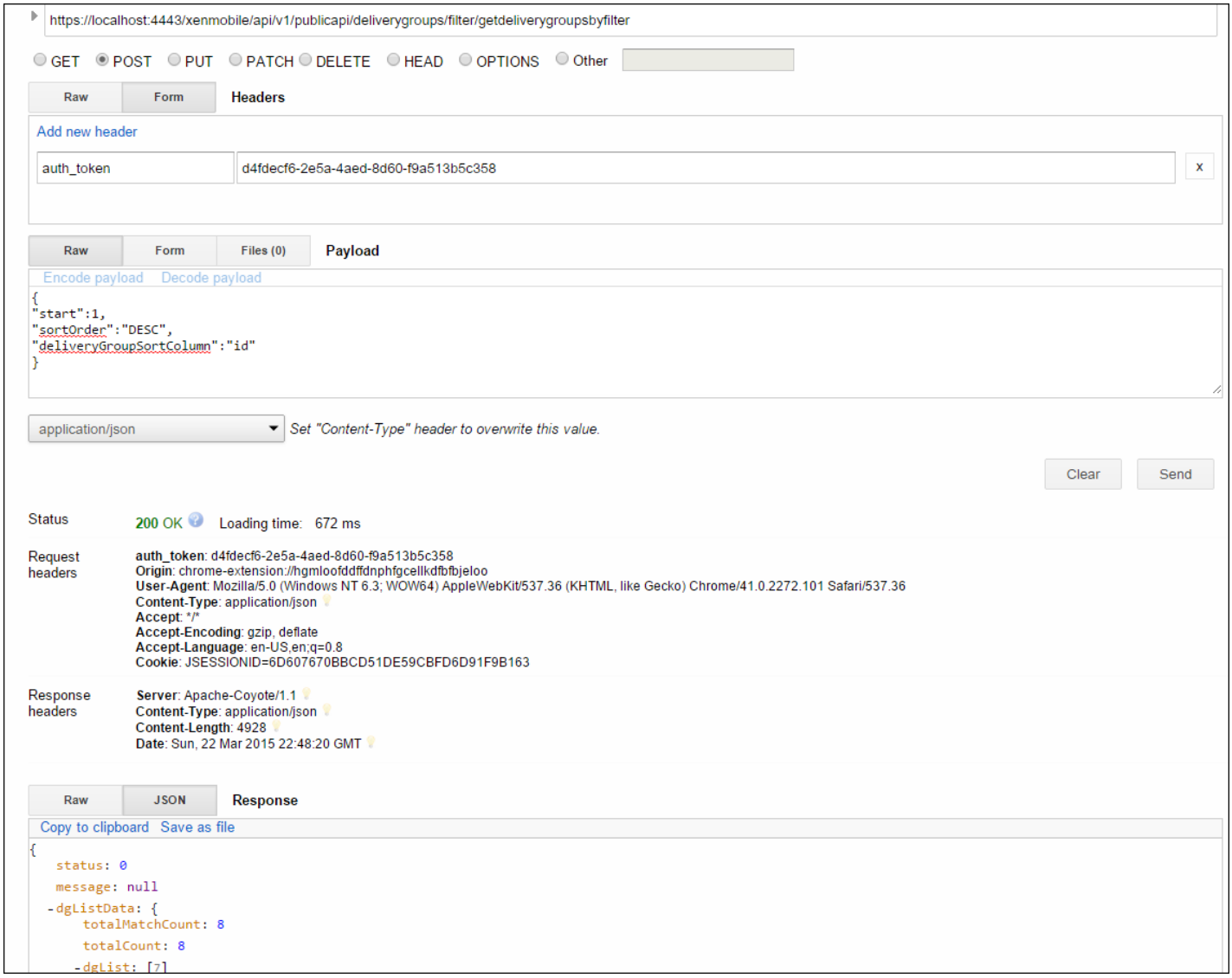
    "search":"add"

}
```

Type de méthode : POST

Content-type : application/json

 © 1999-2017 Citrix Systems, Inc. All rights reserved.



Services de l'API REST publique

Le tableau suivant répertorie les services REST disponibles :

Fonction	Service REST	URL
Connexion	Connexion	/xenmobile/api/v1/authentication/login
	Déconnexion	/xenmobile/api/v1/authentication/logout
Certificats	Obtenir tous les certificats	xenmobile/api/v1/certificates
	Supprimer les certificats	xenmobile/api/v1/certificates/

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Importer le certificat en tant que SAML	xenmobile/api/v1/certificates/import/certificate/saml
	Importer le certificat en tant que serveur	xenmobile/api/v1/certificates/import/certificate/server
	Importer le certificat en tant qu'écouteur	xenmobile/api/v1/certificates/import/certificate/listener
	Créer un certificat	xenmobile/api/v1/certificates/csr
	Exporter un certificat	xenmobile/api/v1/certificates/export
Keystore	Importer le keystore en tant que serveur	xenmobile/api/v1/certificates /import/keystore/server
	Importer le keystore en tant qu'SAML	xenmobile/api/v1/certificates /import/ keystore/saml
	Importer le keystore en tant qu'APNS	xenmobile/api/v1/certificates /import/ keystore/apns
	Importer le keystore en tant qu'écouteur	xenmobile/api/v1/certificates /import/ keystore/listener
Licences	Obtenir les informations de licence	xenmobile/api/v1/licenses
	Enregistrer les informations de licence	xenmobile/api/v1/licenses
	Charger des licences	xenmobile/api/v1/licenses/upload
	Supprimer des licences	xenmobile/api/v1/licenses/remove
	Activer une licence	xenmobile/api/v1/licenses/activate/{licenseType}
	Tester le serveur	xenmobile/api/v1/licenses/testserver
	Obtenir la date d'expiration	xenmobile/api/v1/licenses/getexpirationdate

© 1999-2017 Citrix Systems, Inc. All rights reserved.

LDAP	Obtenir la liste de configuration LDAP	xenmobile/api/v1/ldap
	Ajouter un nouveau protocole LDAP	xenmobile/api/v1/ldap/msactivedirectory
	Modifier un nouveau protocole LDAP	xenmobile/api/v1/ldap/msactivedirectory/{name}
	Définir la configuration LDAP par défaut	xenmobile/api/v1/ldap/default/{name}
	Supprimer LDAP	configxenmobile/api/v1/ldap/{name}
NetScaler	Obtenir NetScaler Gateway	xenmobile/api/v1/netscaler
	Ajouter NetScaler Gateway	xenmobile/api/v1/netscaler
	Mettre à jour NetScaler Gateway	xenmobile/api/v1/netscaler/{id}
	Définir NetScaler Gateway par défaut	xenmobile/api/v1/netscaler/default/{id}
	Supprimer des NetScaler Gateway	xenmobile/api/v1/netscaler
Notification	Obtenir les serveurs de notification	xenmobile/api/v1/notificationserver
	Obtenir le serveur de notification par ID	xenmobile/api/v1/notificationserver/{id}
	Ajouter/modifier un serveur SMTP	xenmobile/api/v1/notificationserver/smtp
	Ajouter/modifier une passerelle SMS	xenmobile/api/v1/notificationserver/sms

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Définir le serveur SMTP comme valeur par défaut (activation)	xenmobile/api/v1/notificationserver/activate/smtp/{id}
	Supprimer un serveur de notification	xenmobile/api/v1/notificationserver/{id}
	Définir la passerelle SMS comme valeur par défaut (activation)	xenmobile/api/v1/notificationserver/activate/sms/{id}
Utilisateurs et groupes locaux	Obtenir des utilisateurs locaux	xenmobile/api/v1/localusersgroups
	Obtenir un utilisateur spécifique	xenmobile/api/v1/localusersgroups/{name}
	Ajouter un utilisateur	xenmobile/api/v1/localusersgroups
	Importer un fichier de provisioning	xenmobile/api/v1/localusersgroups/importprovisioningfile
	Mettre à jour un utilisateur	xenmobile/api/v1/localusersgroups
	Supprimer des utilisateurs	xenmobile/api/v1/localusersgroups/deletelocalusers
	Supprimer un utilisateur	xenmobile/api/v1/localusersgroups/{name}
	Obtenir des utilisateurs locaux par filtre	xenmobile/api/v1/localusersgroups/filter
	Réinitialiser le mot de passe de l'utilisateur	xenmobile/api/v1/localusersgroups/password
Gestion des applications	Supprimer un conteneur d'applications	xenmobile/api/v1/application/{id conteneur}
	Supprimer des conteneurs d'applications	xenmobile/api/v1/application
	Obtenir les conteneurs	xenmobile/api/v1/application/filter

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	d'applications par filtre	
	Obtenir le conteneur d'applications Weblink par ID de conteneur	xenmobile/api/v1/application/weblink/{container id}
	Obtenir le conteneur d'applications Web et SaaS par ID de conteneur	xenmobile/api/v1/application/saas/{id conteneur}
	Obtenir le conteneur d'applications Appstore par ID de conteneur	xenmobile/api/v1/application/appstore/{id conteneur}
	Obtenir le conteneur d'applications mobiles par ID de conteneur	xenmobile/api/v1/application/mobile/{id conteneur}
Groupes de mise à disposition	Ajouter des groupes de mise à disposition	xenmobile/api/v1/deliverygroups
	Modifier des groupes de mise à disposition	xenmobile/api/v1/deliverygroups
	Obtenir un groupe de mise à disposition spécifique	xenmobile/api/v1/deliverygroups/{nom du rôle}
	Obtenir les groupes de mise à disposition par filtre	xenmobile/api/v1/deliverygroups/filter
	Obtenir tous les groupes de mise à disposition	xenmobile/api/v1/deliverygroups
	Supprimer des groupes de mise à disposition	xenmobile/api/v1/deliverygroups
	Obtenir l'état du déploiement	xenmobile/api/v1/deliverygroups/getdeploymentstatus/{nom}
Propriétés du serveur	Obtenir les propriétés du serveur	xenmobile/api/v1/serverproperties/

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Obtenir les propriétés du serveur par filtre	xenmobile/api/v1/serverproperties/filter/
Ajouter des propriétés de serveur	xenmobile/api/v1/serverproperties/
Modifier les propriétés de serveur	xenmobile/api/v1/serverproperties/
Réinitialiser les propriétés de serveur	xenmobile/api/v1/serverproperties/reset
Supprimer les propriétés de serveur	xenmobile/api/v1/serverproperties/

Définition des API REST

Les sections suivantes décrivent les API répertoriées dans le tableau précédent.

Rappel : dans les exemples suivants, modifiez le nom de l'hôte et le numéro de port afin qu'ils correspondent à votre environnement.

Pour ouvrir une session sur l'API publique

Accepte les informations d'identification de l'utilisateur et utilise l'AuthenticationManager existant pour authentifier l'utilisateur. La première fois que AuthenticationManager authentifie un utilisateur, il génère un jeton d'authentification qui est placé dans l'en-tête de la requête.

URL : https://:/xenmobile/api/v1/authentication/login

Type de requête : POST

Paramètres de requête COPIER

```
{ "login":"administrator", "password":"password" }
```

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "auth-token":"q483409eu82mkfrcdiv90iv0gc:q483409eu82mkfrcdiv90iv0gc"

}
```

Pour se déconnecter de l'API publique

Supprime le jeton d'authentification émis lorsque l'utilisateur se connecte et déconnecte l'utilisateur actuel. Nécessite le nom d'utilisateur et le jeton d'authentification.

URL : https://:/xenmobile/api/v1/authentication/logout

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête COPIER

```
{“login”:”administrator”}
```

Exemple de réponse COPIER

```
{"Status":"user administrator logged out successfully."}
```

Pour gérer les certificats

Les opérations de gestion des certificats vous permettent d'afficher, de supprimer, d'importer et d'ajouter des certificats via l'API publique.

Obtenir tous les certificats

Retourne tous les certificats dans la base de données.

URL : https://:/xenmobile/api/v1/certificates

Type de requête : GET

© 1999-2017 Citrix Systems, Inc. All rights reserved.

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête : None

Exemple de réponse COPIER


```
{
    "status": 0,
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": null,
    "certificate": [
        {
            "name": "ent-root-ca",
            "description": "test description server 1",
            "validFrom": "2012-02-22",
            "validTo": "2017-02-21",
            "type": "chain",
            "isActive": false,
            "privateKey": "false",
            "ca": null,
            "id": 4656,
            "certDetails": {
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certDetails": {
    "signatureAlgo": "SHA1WithRSAEncryption",
    "version": null,
    "serialNum": "348237881800118418457268346483687164l3",
    "issuerName": {
        "certString": "DC=com,DC=example,CN=ent-root-ca",
        "emailAddress": null,
        "commonName": "ent-root-ca",
        "orgUnit": null,
        "org": null,
        "locality": null,
        "state": null,
        "country": null,
        "description": null
    },
    "subjectName": {
        "certString": "DC=com,DC=example,CN=ent-root-ca",
        "emailAddress": null,
        "commonName": "ent-root-ca",
        "orgUnit": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                        "org": null,

                        "locality": null,

                        "state": null,

                        "country": null,

                        "description": null

                    }

                }

            }

        ],

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

}
```


Supprimer les certificats

Supprime les certificats spécifiés. Requiert l'ID du certificat pour chaque certificat à supprimer.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/publicapi/certificates

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Paramètres de requête COPIER

```
{“certificateIds”:[“<certificate_id_1>”,”<certificate_id_2>”, ..., "<certificate_id_n>"]}
```

Importer le certificat en tant que certificat SAML

Importe le certificat spécifié en tant que certificat SAML.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/saml

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'saml',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Importer le certificat en tant que certificat de serveur

Importe le certificat spécifié en tant que certificat de serveur.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/server

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'none',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        },

        "certificate": null,

        "apnsCheckObj": {

            "topicNameMismatch": false,

            "certExpired": false,

            "certNotYetValid": false,

            "malformed": false

        }

    }
```

Importer le certificat en tant que certificat d'écoute

Importe le certificat spécifié en tant que certificat d'écoute SSL.

URL : https://:/xenmobile/api/v1/certificates/import/certificate/listener

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
certImportData = {

    'type':'cert',

    'checkTopicName':true,

    'password':'1111',

    'alias':'',

    'useAs':'listener',

    'keystoreType':'PKCS12',

    'uploadType':'certificate',

    'description':'test description'

}

uploadFile = <the actual file to be uploaded>
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "csrRequest": null,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

    "certificate": null,

    "apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```

Créer un certificat

Crée un certificat auto-signé ou une demande de signature de certificat (CSR) qui requiert une signature de l'autorité de certification.

URL : https://:/xenmobile/api/v1/certificates/csr

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Content-type : Application/form_url_encoded

Paramètres de requête COPIER

```
{
    "isSelfSign":true,
    "csrRequest":{
    "commonName":"your certificate name",
    "description":"certificate description",
    "org":"organization",
    "orgUnit":"organization unit",
    "locality":"location",
    "state":"CA",
    "country":"US",
    "isSelfSign":true
    },
"validDays":"60",
"keyLength":"1024",
"useAs":"none"
}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemple de réponse COPIER

```
{
    status: 0
    message: "Success"
    csrRequest: ""
    apnsCheck: null
    certificate: null
    apnsCheckObj:
    {
    topicNameMismatch: false
    certExpired: false
    certNotYetValid: false
    malformed: false
    }
}
```

Exporter un certificat

Télécharge le certificat spécifié. Le tableau suivant dresse la liste des paramètres pour cette opération.

Paramètre	Requis	Description

© 1999-2017 Citrix Systems, Inc. All rights reserved.

id	Oui	ID du certificat numérique
password		Mot de passe associé au certificat exporté.
exportPrivateKey		Indicateur qui spécifie si la clé privée doit être exportée.

URL : https://:/xenmobile/api/v1/certificates/export

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "id": "300",
    "password": "1111",
    "exportPrivateKey": true
}
```

Exemple de réponse : affiche la chaîne de certificat suite à une requête fructueuse.

Pour gérer les keystores

Vous pouvez importer des keystores par le biais de l'API publique

Importer un keystore serveur

Importe un keystore serveur.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/server

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore SAML

Importe un keystore SAML.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/saml

Type de requête : POST

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':'none',
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
}
    uploadFile = <certificate file>
    uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore APNS

Importe un keystore APNS.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/apns

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':apns,
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "message": "Success",
    "csrRequest": null,
    "apnsCheck": {
            "topicNameMismatch": false,
            "certExpired": false,
            "certNotYetValid": false,
            "malformed": false
    },
    "certificate": null,
    "apnsCheckObj": {
        "topicNameMismatch": false,
        "certExpired": false,
        "certNotYetValid": false,
        "malformed": false
    }
}
```


Importer un keystore d'écoute SSL

Importe un keystore d'écoute SSL.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/certificates/import/keystore/listener

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête COPIER

```
certImportData = {
    'type':'cert',
    'checkTopicName':true,
    'password':'1111',
    'alias':'',
    'useAs':"listener",
    'keystoreType':'PKCS12',
    'uploadType':'keystore',
    'description':'test description'
    }
uploadFile = <certificate file>
uploadFile = <private key file>
```

Exemple de réponse COPIER

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "status": 0,

    "message": "Success",

    "csrRequest": null,

    "apnsCheck": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    },

"certificate": null,

"apnsCheckObj": {

        "topicNameMismatch": false,

        "certExpired": false,

        "certNotYetValid": false,

        "malformed": false

    }

}
```


Pour gérer les licences

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Vous permet de gérer les licences par le biais de l'API publique.

Obtenir les informations de licences

Affiche des informations sur les licences.

URL : https://:/xenmobile/api/v1/licenses

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    status: 0
    message: "Success"
    cpLicenseServer: {
        serverAddress: "192.0.2.20"
        localPort: 0
        remotePort: 27000
        serverType: "remote"
        licenseType: "none"
        isServerConfigured: true
        gracePeriodLeft: 0
        isRestartLpeNeeded: null
        isScheduleNotificationNeeded: null
            licenseList: []
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    sadate: "2015.1210"
    notice: "Example Systems Inc."
    vendorString: ";LT=Retail;GP=720;UDM=U;LP=90;CL=STD,ADV,ENT;SA=1;ODP=0"
    licensesInUse: 0
    licensesAvailable: 102
    overdraftLicenseCount: 2
    p_E_M: "CXM_ENTU_UD"
    serialNumber: "cxmretailent1000user"
    licenseType: "Retail"
    expirationDate: "01-DEC-2015"
}
licenseNotification:
{
    id: 1
    notificationEnabled: false
    notifyFrequency: 7
    notifyNumberDaysBeforeExpire: 60
    recepientList: ""
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            emailContent: "License expiry notice"

        }

    }

}
```

Enregistrer les informations de licences

Enregistre toutes les informations sur les licences.

URL : https://:/xenmobile/api/v1/licenses

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "serverAddress": "192.0.2.20",

    "localPort": 0,

    "remotePort": 27000,

    "serverType": "remote",

    "licenseType": "none",

    "isServerConfigured": true,

    "gracePeriodLeft": 0,

    "isRestartLpeNeeded": true,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "isScheduleNotificationNeeded": true,
    "licenseList": [],
    "licenseNotification": {
        "id": 1,
        "notificationEnabled": true,
        "notifyFrequency": 20,
        "notifyNumberDaysBeforeExpire": 60,
        "recepientList": "justa.name123@example.com",
        "emailContent": "Licenseexpirynotice"
    }
}
```


Exemple de réponse COPIER


```
{
    "status": 0,
    "message": "Success"
}
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Charger le fichier de licences

Charge le fichier de licences spécifié.

URL : https://:/xenmobile/api/v1/licenses/upload

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : Multipart/form-data

Paramètres de requête : uploadFile =

Exemple de réponse COPIER

```
{

   "status": 0,

   "message": "Success"

}
```

Activer une licence

Active la licence spécifiée.

URL : https://:/xenmobile/api/v1/licenses/activate/{type de licence}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête : ajoutez le type de licence pour activer l'URL de la licence.

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success"

    "cpLicenseServer": null

}
```

Supprimer toutes les licences

Supprime toutes les licences.

URL : https://:/xenmobile/api/v1/licenses/remove

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "isConnected": null

}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tester le serveur de licences

Vérifie la connectivité sur le serveur de licences.

URL : https://:/xenmobile/api/v1/licenses/testserver/

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "serverAddress": "192.0.2.7",
    "localPort": 0,
    "remotePort": 27000,
    "serverType": null,
    "licenseType": null,
    "isServerConfigured": null,
    "gracePeriodLeft": 0,
    "isRestartLpeNeeded": null,
    "isScheduleNotificationNeeded": null,
    "licenseList": [],
    "licenseNotification": null
}
```


Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success",

    "isConnected": true

}
```


Obtenir la première date d'expiration

Trouve la licence avec la première date d'expiration.

URL : https://:/xenmobile/api/v1/licenses/getexpirationdate

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success",

    "expiredDate": 1448956800000,

    "daysBeforeExpire": 229,

    "daysInPOC": 0

}
```

Pour gérer les configurations LDAP

Le tableau suivant dresse la liste des paramètres utilisés dans les opérations de configuration LDAP.

Paramètre	Requis	Description
primaryHost	Oui	Adresse IP du serveur LDAP principal ou nom d'hôte. Entrez en tant qu'Adresse IP ou FQDN.
secondaryHost	Non	Adresse IP du serveur LDAP secondaire ou nom d'hôte. Entrez en tant qu'Adresse IP ou FQDN.
port	Oui	Numéro de port du serveur LDAP
username	Oui	Serveur LDAP valide nom d'utilisateur
password	Oui	Mot de passe pour username
userBaseDN	Oui	
lockoutLimit	Non	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

lockoutTime	Non	
useSecure	Non	
userSearchBy	Oui	Rechercher les utilisateurs par upn ou samaccount
domain	Oui	Nom de domaine unique du serveur LDAP
domainAlias	Oui	Alias pour le domaine LDAP
globalCatalogPort	Non	
gcRootContext	Non	
groupBaseDN	Oui	
isDefault	Non	Partie de la réponse GET qui indique si la configuration LDAP est la configuration par défaut.
name	Non	Partie de la réponse GET qui est un identificateur unique utilisé pour mettre à jour ou supprimer la configuration LDAP.

Répertorier la configuration LDAP

Répertorie la configuration LDAP entière dans XenMobile.

URL : https://:/xenmobile/api/v1/ldap

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    “result”: [

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"aaa@example.com","password":"1.pwd","userB

    { "primaryHost":"192.0.2.7","secondaryHost":"","port":"389","username":"test@xmexample.com","password":"1.pwd","us

    ]

}
```

Ajouter une nouvelle configuration LDAP

Ajoute une nouvelle configuration LDAP. Le nom de domaine doit être unique et ne peut pas être le même qu'une autre configuration LDAP.

URL : https://:/xenmobile/api/v1/ldap/msactivedirectory

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    “status”: 0,

    “message”: “LDAP configuration created”

}
```

Modifier une configuration LDAP

Modifie une configuration LDAP, mais vous ne pouvez pas modifier le domaine avec l'opération de modification.

URL : https://:/xenmobile/api/v1/ldap/msactivedirectory/{nom}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "primaryHost":"192.0.2.7",

    "secondaryHost":"",

    "port":"389",

    "username":"aaa@example.com",

    "password":"1.pwd",

    "userBaseDN":"dc=example,dc=com",

    "groupBaseDN":"dc=example,dc=com",

    "lockoutLimit":"0",

    "lockoutTime":"1",

    "useSecure":"false",

    "userSearchBy":"upn",

    "domain":"example.com",

    "domainAlias":"exampleAlias",

    "globalCatalogPort":"0",

    "gcRootContext":""

}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Définir la configuration LDAP par défaut

Définit la configuration LDAP spécifiée en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/ldap/default/{nom}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Supprimer une configuration LDAP

Supprime la configuration LDAP spécifiée.

URL : https://:/xenmobile/api/v1/ldap/{nom}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations NetScaler Gateway

Vous permet de gérer les configurations de NetScaler Gateway. Le tableau suivant dresse la liste des paramètres utilisés dans les opérations NetScaler Gateway.

Paramètre	Requis	Description
name	Oui	Nom unique de NetScaler Gateway
alias	Non	
url	Oui	URL publiquement accessible pour NetScaler Gateway
passwordRequired	Oui	
logonType	Oui	Valeurs valides : domain-only, domain-token, domain-certificate, certificate-only, certificate-token et token-only
callback	Non	
default	Oui	Définissez ce paramètre sur true ou false lors de l'ajout ou de la modification d'une configuration de NetScaler Gateway. Si ce paramètre n'est pas transmis, la valeur par défaut est false.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

id	Non	Partie de la réponse GET qui est un identificateur unique utilisé pour mettre à jour ou supprimer la configuration NetScaler Gateway.

Répertorier toutes les configurations NetScaler Gateway

Répertorie la configuration NetScaler Gateway entière dans XenMobile.

URL : https://:/xenmobile/api/v1/netscaler

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    “result”: [

        { "name":"displayName",

        "alias":"",

        "url":"https://externalURl.com",

        "passwordRequired":"false",

        "logonType":"domain",

        "default":"false","id":"",

        “callback”: [{“callbackUrl”:http://example.com,

        “ip”:”192.0.2.8”}]

        },

        { "name":"displayName",

        "alias":"",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "url":"https://externalURl.com",

            "passwordRequired":"false",

            "logonType":"domain",

            "default":"false",

            "id":"",

            “callback”: [{“callbackUrl”:http://example.com,

            “ip”:”192.0.2.8”}]

            }

      ]

}
```

Ajouter une nouvelle configuration NetScaler Gateway

Ajoute une nouvelle configuration NetScaler Gateway.

URL : https://:/xenmobile/api/v1/netscaler

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "alias":"",

    “default”:true, "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “callback”: [{“callbackUrl”:http://example.com,

    “ip”:”192.0.2.8”}]

}
```

Modifier une configuration NetScaler Gateway

Modifie la configuration NetScaler Gateway spécifiée.

URL : https://:/xenmobile/api/v1/netscaler/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "alias":"",

    "url":"https://externalURl.com",

    "passwordRequired":"false",

    "logonType":"domain”,

    “default”: true,

    “callback”: [{“callbackUrl”:http://ag.com,

    “ip”:”192.0.2.8”}]

}
```

Supprimer une configuration NetScaler Gateway

Supprime la configuration NetScaler Gateway spécifiée.

URL : https://:/xenmobile/api/v1/netscaler/{id}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration NetScaler Gateway par défaut

Définit la configuration NetScaler Gateway spécifiée en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/netscaler/default/{id}

Type de requête : PUT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations du serveur de notifications SMS et SMTP

Vous pouvez ajouter, modifier, activer (définir comme valeur par défaut) et supprimer les configurations du serveur SMS et SMTP. Le tableau suivant dresse la liste des paramètres utilisés dans les opérations de configuration du serveur SMS et SMTP.

Paramètre	Requis	Description
name	Oui	Nom unique de configuration SMS/SMTP.
serverType	Non	Type de serveur de notification (SMS ou SMTP) envoyé par le serveur dans la requête GET.
active	Non	Indique si le serveur est utilisé pour les notifications. Un seul serveur peut être actif pour chaque type.
id	Non	Identificateur unique utilisé pour mettre à jour, supprimer et activer le serveur.
description	Non	Description du serveur.
Paramètres SMS		
key	Oui	
secret	Oui	
virtualPhoneNumber	Oui	Doit utiliser un format de numéro de téléphone.
https	Oui	La valeur par défaut est false
country	Oui	
carrierGateway	Oui	La valeur par défaut est false
Paramètres SMTP		
secureChannelProtocol	Oui	Type de protocole de sécurité à utiliser. Les valeurs valides sont : None,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		SSL et TLS. La valeur par défaut est none.
port	Oui	
authentication	Oui	Indique s'il faut utiliser l'authentification. Les valeurs valides sont true et false.
username	Oui, si l'authentification est true.	
password	Oui, si l'authentification est true.	
msSecurePasswordAuth	Oui	La valeur par défaut est false
fromName	Oui	
fromEmail	Oui	
numOfRetries	Non	Un nombre entier. La valeur par défaut est 5.
timeout	Non	Un nombre entier. La valeur par défaut est 30.
maxRecipients	Non	Un nombre entier. La valeur par défaut est 100.

Répertorier tous les serveurs SMS et SMTP

Répertorie tous les serveurs SMS et SMTP dans XenMobile.

URL : https://:/xenmobile/api/v1/notificationserver

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Accept : application/json

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    “result”: [

        { "name":"serverName","serverType":"SMS,"active":"true","id":"10"},

        { "name":"serverName2","serverType":"SMTP,"active":"true","id":"10"},

        { "name":"serverName3","serverType":"SMS,"active":"false","id":"10"}

    ]

}
```

Obtenir les détails du serveur

Obtient des informations sur le serveur par ID de serveur.

URL : https://:/xenmobile/api/v1/notificationserver/{id}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Accept : application/json

Exemple de réponse SMS COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Exemple de réponse SMTP COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.12",

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Ajouter une configuration de serveur SMS

Ajoute une configuration de serveur SMS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/notificationserver/sms

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Modifier la configuration du serveur SMS

Modifie la configuration du serveur SMS spécifié.

URL : https://:/xenmobile/api/v1/notificationserver/sms/{id}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name":"displayName",

    "description":"",

    "server":"192.0.2.9",

    "carrierGateway":"true",

    "country":"+93",

    "https":"false”,

    “key”: “123456”,

    "secret":"secretKey",

    "virtualPhoneNumber":"4085552222",

    "carrierGateway":"true"

}
```

Ajouter une configuration de serveur SMTP

Ajoute une configuration de serveur SMTP.

URL : https://:/xenmobile/api/v1/notificationserver/smtp

Type de requête : POST

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Modifier une configuration SMTP

Modifie la configuration SMTP spécifiée.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/notificationserver/smtp/{id}

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    name":"displayName",

    "description":"Edited description",

    "server":"192.0.2.9"

    "secureChannelProtocol":"true",

    "port":"345",

    "authentication":"false”,

    “username”: “test”,

    “password”: “testPassword”,

    "msSecurePasswordAuth":"true",

    "fromName":"Email name",

    "fromEmail":test@example.com,

    "numOfRetries":5,

    "timeout":30,

    "maxRecipients":100

}
```

Supprimer la configuration du serveur

Supprime la configuration du serveur SMS ou SMTP spécifié.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/notificationserver/{id}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration SMS par défaut

Définit la configuration du serveur SMS spécifié en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/notificationserver/activate/sms/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Définir la configuration SMTP par défaut

Définit la configuration du serveur SMTP spécifié en tant que configuration par défaut.

URL : https://:/xenmobile/api/v1/notificationserver/activate/smtp/{id}

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les utilisateurs et groupes locaux

Vous pouvez gérer les utilisateurs et groupes locaux en utilisant les services suivants.

Obtenir tous les utilisateurs

Obtient tous les utilisateurs locaux.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"status": 0,

"message": "Success",

"result": [

    {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"

        },

        "role": "ADMIN",

        "roles": null,

        "createdOn": "1/10/15 11:42 AM",

        "lastAuthenticated": "1/10/15 11:42 AM",

        "domainName": null,

        "adUser": false,

        "vppUser": false

    }
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    ]

}
```

Obtenir un utilisateur

Obtient l'utilisateur local spécifié.

URL : https://:/xenmobile/api/v1/localusersgroups/{nom}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "result": {

        "userid": 8,

        "username": "admin",

        "password": null,

        "confirmPassword": null,

        "groups": [],

        "attributes": {

            "company": "example"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            company": "Example
        },
        "role": "ADMIN",
        "roles": null,
        "createdOn": "1/10/15 11:42 AM",
        "lastAuthenticated": "1/10/15 11:42 AM",
        "domainName": null,
        "adUser": false,
        "vppUser": false
    }
}
```

Ajouter un utilisateur

Ajoute un utilisateur avec les attributs spécifiés.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "attributes": {

          "badpwdcount": "4",

          "asuseremail": "justa.name@example.com",

          "company": "example",

          "mobile": "4695557854"

          },

    "groups": [

          "MSP"

          ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Exemple de réponse COPIER

```
{

    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"message": "Success",

"user": {

    "userid": 0,

    "username": "justaname_XX",

    "password": "password",

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": null,

    "lastAuthenticated": null,

    "domainName": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "adUser": false,

        "vppUser": false

    }

}
```

Mettre à jour un utilisateur

Met à jour les attributs utilisateur.

URL : https://:/xenmobile/api/v1/localusersgroups

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "attributes": {

          "badpwdcount": "4",

          "asuseremail": "justa.name@example.com",

          "company": "example",

          "mobile": "4695557854"

          },

    "groups": [

          "MSP"

          ],

    "role": "USER",

    "username": "justaname_XX",

    "password": "password"

}
```

Exemple de réponse COPIER

```
{

    "status": 0,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"message": "Success",

"user": {

    "userid": 108,

    "username": "justaname_XX",

    "password": null,

    "confirmPassword": null,

    "groups": [

        "MSP"

    ],

    "attributes": {

        "badpwdcount": "4",

        "asuseremail": "justa.name@example.com",

        "company": "example",

        "mobile": "4695557854"

    },

    "role": "USER",

    "roles": null,

    "createdOn": "3/27/15 1:10 PM",

    "lastAuthenticated": "3/27/15 1:10 PM",

    "domainName": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "adUser": false,

        "vppUser": false

    }

}
```

Changer le mot de passe utilisateur

Réinitialise le mot de passe d'un utilisateur ; vous pouvez également modifier le mot de passe d'un utilisateur dans l'appel « update local user ».

URL : https://:/xenmobile/api/v1/localusersgroups/resetpassword

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "username": “administrator”,

    “password”: “newPassword”

}
```

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
Response Errors:

1250 – User id not found

1252 – Failed to reset the password

Password can also be changed in the update local user call.
```

Supprimer des utilisateurs

Supprime les utilisateurs spécifiés.

URL : https://:/xenmobile/api/v1/localusersgroups/resetpassword

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{ justaname XX }
```

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```

Supprimer un utilisateur

Supprime l'utilisateur spécifié.

URL : https://:/xenmobile/api/v1/localusersgroups/

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "user": null

}
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Importer un fichier de provisioning

Charge un fichier contenant les données de l'utilisateur local. Le fichier à charger doit être au format .csv. Pour de plus amples informations sur les fichiers de provisioning, consultez la section Formats des fichiers de provisioning.

URL : https://:/xenmobile/api/v1/localusersgroups/importprovisioningfile

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
importdata={"fileType:"user"}

uploadfile=<file to be uploaded.csv>
```

Exemple de réponse COPIER

```
{

   "status": 0,

   "message": "Success",

   "user": null

}
```

Pour gérer les applications

Vous pouvez gérer les applications avec les services suivants.

Obtenir toutes les applications par filtre

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Obtient les applications en fonction des paramètres de filtre spécifiés.

URL : https://:/xenmobile/api/v1/application/filter

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "start": 0,
    "limit": 10,
    "orderBy": "name",
    "sortOrder": "desc",
    "searchStr": "justaserver1"
}
```

Obtenir des applications mobiles par conteneur

Obtient des applications mobiles dans le conteneur spécifié.

URL : https://:/xenmobile/api/v1/application/mobile/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"status": 0,

"message": "Success",

"result": {

    "id": 14,

    "name": "testApp",

    "description": "",

    "createdOn": null,

    "lastUpdated": null,

    "disabled": false,

    "nbSuccess": 0,

    "nbFailure": 0,

    "nbPending": 0,

    "schedule": {

        "enableDeployment": true,

        "deploySchedule": "NOW",

        "deployScheduleCondition": "EVERYTIME",

        "deployDate": null,

        "deployTime": null,

        "deployInBackground": false

    },
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"iconData": "",
"appType": "MDX",
"categories": [
    "Default"
],
"roles": [],
"workflow": null,
"ios": {
    "displayName": "GoToMeeting",
    "description": "G2MW_IOS_5.3.3_075_01",
    "paid": false,
    "removeWithMdm": true,
    "preventBackup": true,
    "appVersion": "5.3.3.075",
    "minOsVersion": "",
    "maxOsVersion": "",
    "excludedDevices": "",
    "avppParams": null,
    "avppTokenParams": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"rules": null,
"appType": "mobile_ios",
"uuid": "8e69d397-48bb-4f29-a95c-dd7b16665c1c",
"id": 0,
"store": {
    "rating": {
        "rating": 0,
        "reviewerCount": 0
    },
    "screenshots": [],
    "faqs": [],
    "storeSettings": {
        "rate": true,
        "review": true
    }
},
"policies": [
    {
        "policyName": "ReauthenticationPeriod",
        "policyValue": "480",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "policyType": "integer",

            "policyCategory": "Authentication",

            "title": "Reauthentication period (minutes)",

            "description": "\nDefines the period before a user is challenged to authenticate again. ",

            "units": "minutes",

            "explanation": null

        },

        {

            "policyName": "BlockJailbrokenDevices",

            "policyValue": "true",

            "policyType": "boolean",

            "policyCategory": "Device Security",

            "title": "Block jailbroken or rooted",

            "description": "\nIf On, the application is locked when the device is jailbroken or rooted.",

            "units": null,

            "explanation": null

        },

        {

            "policyName": "CertificateLabel",

            "policyValue": "",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                    "policyType": "string",

                    "policyCategory": "Network Access",

                    "title": "Certificate label",

                    "description": "\nThe label for the certificate.\n                                                    Default value is er

                    "units": null,

                    "explanation": null

                }

            ]

        },

        "android": null,

        "android_knox": null,

        "android_work": null,

        "windows": null,

        "windows_tab": null

    }

}
```


Obtenir applications SaaS par conteneur

Obtient des applications SaaS à partir du conteneur spécifié.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

URL : https://:/xenmobile/api/v1/application/mobile/saas/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Obtenir applications d'un magasin public par conteneur

Obtient les applications d'un magasin public depuis le conteneur spécifié.

URL : https://:/xenmobile/api/v1/application/mobile/appstore/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Obtenir applications Web Link par conteneur

Obtient des applications Web Link depuis le conteneur spécifié.

URL : https://:/xenmobile/api/v1/application/mobile/weblink/{Idconteneur}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Supprimer un conteneur d'application

Supprime le conteneur d'application spécifié.

URL: https://:/xenmobile/api/v1/application/{Idconteneur}

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Pour gérer les configurations de groupe de mise à disposition

Vous pouvez gérer les configurations de groupe de mise à disposition avec les services suivants.

Obtenir des groupes de mise à disposition par filtre

Utilise les paramètres de filtre spécifiés pour obtenir les groupes de mise à disposition.

URL : https://:/xenmobile/api/v1/deliverygroups/filter

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "start": 1,

    "sortOrder": "DESC",

    "deliveryGroupSortColumn": "id",

    “limit”:10,

    "search": "add"

}
```

Exemple de réponse COPIER

```
{

     "status": 0,

     "message": "Success",

     "dgListData": {

         "totalMatchCount": 7,

         "totalCount": 10,

         "dgList": [
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "id": null,
    "name": "add delivery group 6.0",
    "description": "testing add delivery group 6.0",
    "groups": [
        {
            "id": 1,
            "userListId": 1,
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": 0
        }
    ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"
    "disabled": false,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"lastUpdated": 1427144713353,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "Web Link",

        "required": false

    },

    {

        "name": "GoogleApps_SAML",

        "required": true

    }

],

"devicePolicies": [

    "test terms conditions"

],

"smartActions": [

    "shankar ganesh"

],

"nbSuccess": 0,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "nbFailure": 0,

        "nbPending": 0

    },

    {

        "id": null,

        "name": "add delivery group 5.0",

        "description": "testing add delivery group 5.0",

        "groups": [

            {

                "id": 1,

                "userListId": 1,

                "name": "MSP",

                "uniqueName": "MSP",

                "uniqueId": "MSP",

                "domainName": "local",

                "primaryToken": 0

            }

        ],

        "zoneId": null,

        "zoneDomain": null,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"shankar.ganesh@citrix.com\"},\"ruleId\"

"disabled": false,

"lastUpdated": 1426891345698,

"anonymousUser": true,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "GoogleApps_SAML",

        "required": true

    },

    {

        "name": "Web Link",

        "required": false

     }

],

"devicePolicies": [

    "test terms conditions"

],

"smartActions": [

    "shankar ganesh"
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                    ],
                    "nbSuccess": 0,
                    "nbFailure": 0,
                    "nbPending": 0
                }
            ]
        }
}
```

Obtenir un groupe de mise à disposition par nom

URL : https://:/xenmobile/api/v1/deliverygroups/{nom}

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": null,
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"name": "AllUsers",

"description": "default role",

"groups": [],

"zoneId": null,

"zoneDomain": null,

"rules": null,

"disabled": false,

"lastUpdated": null,

"anonymousUser": false,

"roledefLangVersionId": 1,

"applications": [

    {

        "name": "test mdx",

        "required": false

    },

    {

        "name": "test all",

        "required": false

    },

    {
```

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        {
            "name": "justa test",
            "required": false
        },
        {
            "name": "test enterprise",
            "required": false
        },
        {
            "name": "name test",
            "required": false
        }
    ],
    "devicePolicies": [
        "test terms conditions"
    ],
    "smartActions": [
        "justa name"
    ],
    "nbSuccess": 0,
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "nbFailure": 0,

        "nbPending": 0

    }

}
```

Modifier un groupe de mise à disposition

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "name": "add delivery group 2",

    "description": "Changing the description of the delivery group xxx",

    "groups": [

        {

            "name": "MSP",

            "uniqueName": "MSP",

            "uniqueId": "MSP",

            "domainName": "local"
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        },
        {
            "name":"CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId":"a4169204-45f6-48fb-8a0d-847a3200d47e",
            "domainName": "example.com"
        }
        ],
    "disabled": false,
    "anonymousUser": false,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "test mdx",
            "required": false
        }
        ],
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
    "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-restrictU
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"role": {
    "id": null,
    "name": "add delivery group 2",
    "description": "Changing the description of the delivery group xxx",
    "groups": [
        {
            "id": null,
            "userListId": null,
            "name": "MSP",
            "uniqueName": "MSP",
            "uniqueId": "MSP",
            "domainName": "local",
            "primaryToken": null
        },
        {
            "id": null,
            "userListId": null,
            "name": "CN=Users,CN=Builtin,DC=example,DC=com",
            "uniqueName": "Users",
            "uniqueId": "a4169204-45f6-48fb-8a0d-847a3200d47e"
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "uniqueId": "a4169204-45f6-48fb-8a0d-847a5200d47e",
            "domainName": "example.com",
            "primaryToken": null
          }
        ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"values\":{\"stringOperator\":\"eq\",\"value\":\"justa.name@example.com\"},\"ruleId\":\"001-rest
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": false,
    "roledefLangVersionId": null,
    "applications": [
        {
         "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "test mdx",
            "required": false
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            }

            ],

        "devicePolicies": [

            "test terms conditions"

            ],

        "smartActions": [

            "justa name"

            ],

        "nbSuccess": 0,

        "nbFailure": 0,

        "nbPending": 0

    }

}
```

Ajouter un groupe de mise à disposition

Ajoute un groupe de mise à disposition.

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "name": "add delivery group 4.0",
    "description": "testing add delivery group 4.0",
    "anonymousUser": true,
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
        "applications": [
            {
                "name": "GoogleApps_SAML",
                "required": true
            },
            {
                "name": "Web Link",
                "required": false
            }
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        ],
    "devicePolicies": [
        {
            "name":"test terms conditions",
            "priority":-1
        }
        ],
     "smartActions": [
        {
            "name":"Smart Action Name 1",
            "priority":-1
        }
        ],
    "groups": [
        {
            "uniqueName": "MSP",
            "domainName": "local",
            "name": "MSP",
            "uniqueId": "MSP"
        }
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        ],
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\":\"ju
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "role": {
        "id": 16,
        "name": "add delivery group 11.0",
        "description": "testing add delivery group 4.0",
        "groups": [
            {
                "id": null,
                "userListId": null,
                "name": "MSP",
                "uniqueName": "MSP",
                "uniqueId": "MSP",
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
            "domainName": "local",
            "primaryToken": null
        }
       ],
    "zoneId": null,
    "zoneDomain": null,
    "rules": "{\"AND\":[{\"eq\":{\"property\":{\"type\":\"USER_PROPERTY\",\"name\":\"mail\"},\"type\":\"STRING\",\"value\"
    "disabled": false,
    "lastUpdated": null,
    "anonymousUser": true,
    "roledefLangVersionId": null,
    "applications": [
        {
            "name": "GoogleApps_SAML",
            "required": true
        },
        {
            "name": "Web Link",
            "required": false
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
                }

                ],

            "devicePolicies": [

                "test terms conditions"

                ],

            "smartActions": [

                "justa name"

                ],

            "nbSuccess": 0,

            "nbFailure": 0,

            "nbPending": 0

        }

    }
```

Supprimer un groupe de mise à disposition

Supprime les groupes de mise à disposition spécifiés.

URL : https://:/xenmobile/api/v1/deliverygroups

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
[ "add delivery group 11.0" ]
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "roleNames": [
        "add delivery group 11.0"
    ]
}
```

Pour gérer les propriétés du serveur

Vous pouvez gérer les propriétés du serveur XenMobile à l'aide des services suivants.

Obtenir toutes les propriétés du serveur

Obtient tous les propriétés du serveur XenMobile.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : GET

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Exemple de réponse COPIER

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
"status": 0,

"message": "Success",

"allEwProperties": [

    {

        "id": 1,

        "name": "ios.mdm.pki.ca-root.certificatefile",

        "value": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayName": "ios.mdm.pki.ca-root.certificatefile",

        "description": "",

        "defaultValue": "c:/opt/sas/sw/tomcat/inst1/conf/pki-ca-root.crt.pem",

        "displayFlag": false,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    } ,

    {

        "id": 2,

        "name": "ios.mdm.https.host",

        "value": "192.0.2.4",
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
        "displayName": "ios.mdm.https.host",

        "description": "",

        "defaultValue": "192.0.2.4",

        "displayFlag": false,

        "editFlag": false,

        "deleteFlag": false,

        "markDeleted": false

    },

    {

        "id": 3,

        "name": "ios.mdm.enrolment.checkRemoteAddress",

        "value": "false",

        "displayName": "iOS Device Management Enrollment - Check Remote Address",

        "description": "",

        "defaultValue": "false",

        "displayFlag": true,

        "editFlag": true,

        "deleteFlag": false,

        "markDeleted": false

    },
```


 © 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    ]

}
```

Obtenir les propriétés du serveur par filtre

Obtient les propriétés du serveur à l'aide des paramètres de filtre spécifiés.

URL : https://:/xenmobile/api/v1/serverproperties/filter

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{

    "start": 0,

    "limit": 1000,

    "orderBy": "name",

    "sortOrder": "desc",

    "searchStr": "justaserver1"

}
```

Exemple de réponse COPIER

```
{
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
    "status": 0,

    "message": "Success",

    "allEwProperties": [

        {

            "id": 154,

            "name": "justaserver123",

            "value": "justaserver1",

            "displayName": "justarserver display name",

            "description": "justaserver description",

            "defaultValue": "justaserver1",

            "displayFlag": true,

            "editFlag": true,

            "deleteFlag": true,

            "markDeleted": false

        }

    ]

}
```


Ajouter une propriété de serveur

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Ajoute la propriété de serveur spécifiée.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 1",
    "description": "Description 1"
}
```

Exemple de réponse COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```


Modifier des propriétés de serveur

Modifie la propriété de serveur spécifiée.

URL : https://:/xenmobile/api/v1/serverproperties

Type de requête : PUT

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

Content-type : application/json

Paramètres de requête COPIER

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
    "name": "Key 2",
    "value": "Value 1",
    "displayName": "Display Name 2",
    "description": "Description 2"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

Réinitialiser des propriétés de serveur

Réinitialise les propriétés de serveur spécifiées.

URL : https://:/xenmobile/api/v1/serverproperties/reset

Type de requête : POST

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Content-type : application/json

Paramètres de requête COPIER

```
{

    "names": [,

        "justaname7"

        ]

}
```

Exemple de réponse COPIER

```
{

    "status": 0,

    "message": "Success",

    "allEwProperties": null

}
```

Supprimer des propriétés de serveur

URL: https://hostname:4443 /xenmobile/api/v1/serverproperties

Type de requête : DELETE

En-tête de requête : auth_token – le jeton d'authentification obtenu lorsque l'utilisateur s'est connecté

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Content-type : application/json

Paramètres de requête COPIER

```
{
    "justaname3",
    "justaname4"
}
```

Exemple de réponse COPIER

```
{
    "status": 0,
    "message": "Success",
    "user": null
}
```

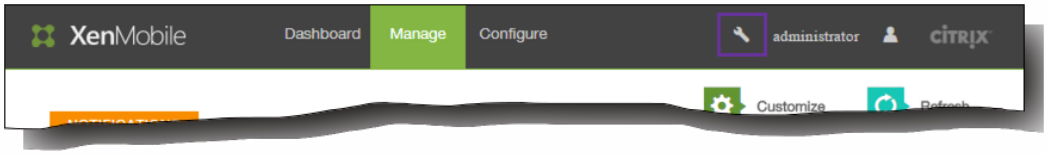

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Réalisation de contrôles de connectivité

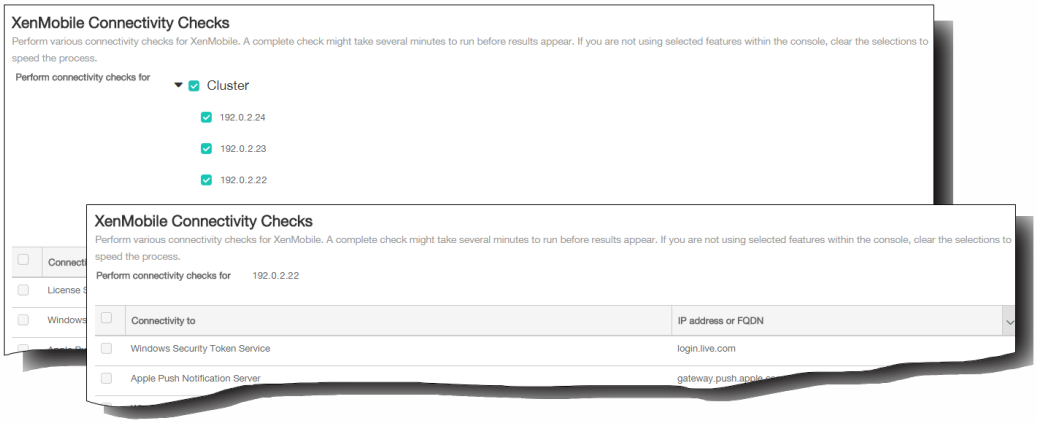
Jul 25, 2016

Depuis la page Support de XenMobile, vous pouvez vérifier la connexion de XenMobile à NetScaler Gateway et à d'autres serveurs et emplacements. Pour accéder à la page de support, procédez comme suit :

1. À partir de la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. L'icône de clé est disponible dans toutes les pages de la console XenMobile. Vous pouvez être invité à entrer votre nom d'utilisateur et votre mot de passe.



Un nouvel onglet de navigateur, **Support XenMobile**, s'ouvre. Si votre environnement XenMobile contient des nœuds en cluster et qu'ils ne sont pas tous affichés, cliquez sur la case à cocher en regard de **Permet de tester la connectivité de** pour développer la liste des nœuds. Si votre environnement contient un seul serveur, il est répertorié en regard de **Permet de tester la connectivité de**.



Réalisation de contrôles de connectivité dans XenMobile

1. Sur la page Support, cliquez sur Test de la connectivité XenMobile. La page Test de la connectivité XenMobile s'affiche.
2. Sélectionnez les serveurs que vous souhaitez inclure dans le test de connectivité, puis cliquez sur Tester la connectivité. Les résultats s'affichent.
3. Cliquez sur la liste d'un serveur (et non pas la case à cocher en regard du serveur) dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.
4. Lorsque vous avez terminé, cliquez sur **Effacer les résultats** pour revenir sur la table des serveurs.

Réalisation de contrôles de connectivité pour NetScaler Gateway

1. Sur la page Support, cliquez sur Test de la connectivité NetScaler Gateway. La page Test de la connectivité NetScaler Gateway s'affiche.
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 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 est déjà 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. 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.

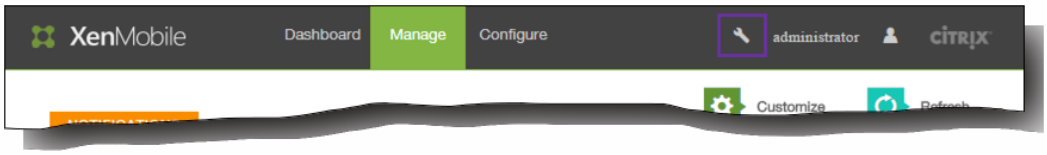
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Création de packs d'assistance dans XenMobile

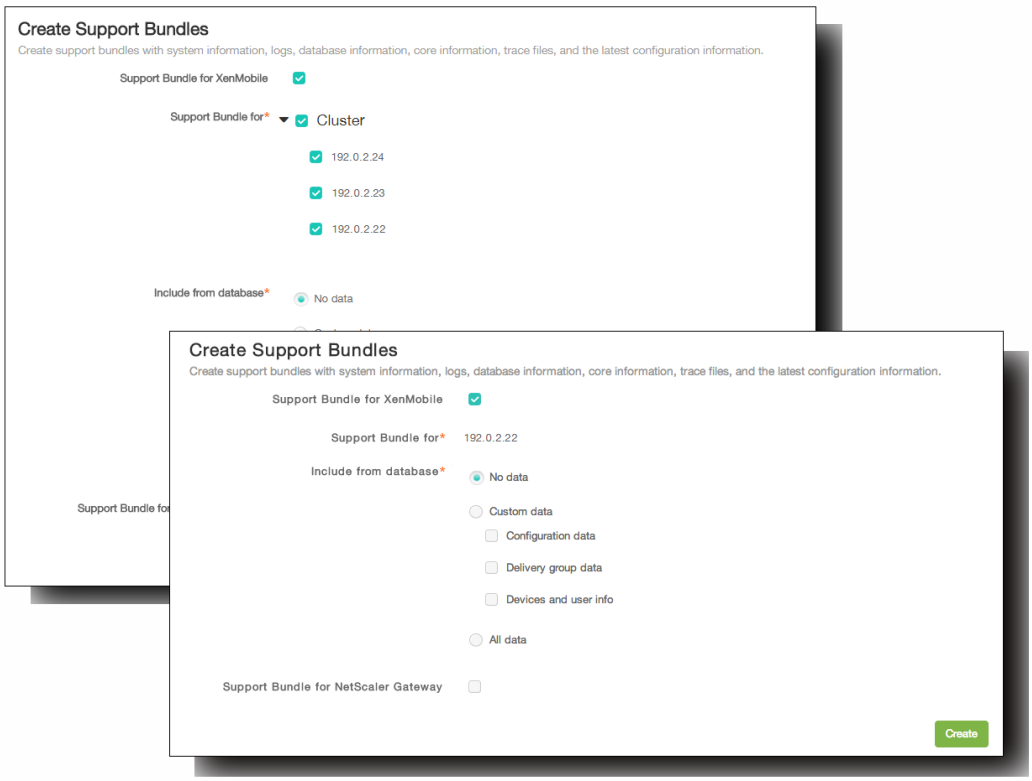
Jul 25, 2016

Si vous voulez signaler un problème à Citrix ou résoudre un problème, vous pouvez créer un pack d'assistance, puis le charger sur Citrix Insight Services (CIS).

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. L'icône de clé est disponible dans toutes les pages de la console XenMobile.
   Remarque : vous serez peut-être invité à entrer votre nom d'utilisateur et mot de passe.



   L'assistance XenMobile s'ouvre dans un nouvel onglet de navigateur.
2. Sur la page Support, cliquez sur Créer des packs d'assistance. La page Créer des packs d'assistance s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.

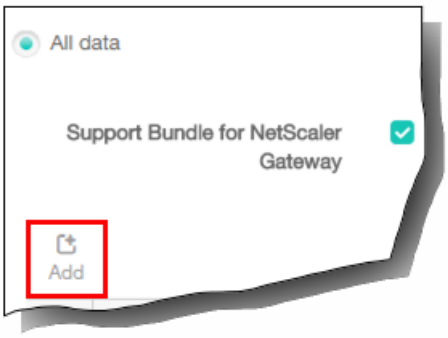


3. Assurez-vous que la case à cocher Pack d'assistance pour XenMobile est sélectionnée.
4. Si votre environnement XenMobile contient des nœuds en cluster, dans Pack d'assistance pour, vous pouvez sélectionner tous les nœuds ou une combinaison de nœuds à partir desquels extraire des données.
5. Dans Inclure depuis la base de données, effectuez l'une des opérations suivantes :
   - Cliquez sur Aucune donnée.

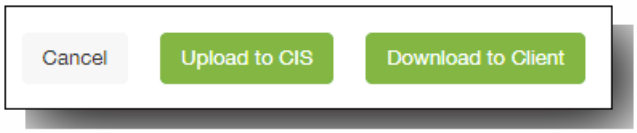
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Cliquez sur Données personnalisées, puis sélectionnez tout ou partie des éléments suivants :
  - Données de configuration. Comprend les configurations de certificat et les stratégies de gestionnaire d'appareils.
  - Données du groupe de mise à disposition. Comprend des informations sur les groupes de mise à disposition d'applications ; contient des détails sur les types d'applications et la stratégie de mise à disposition.
  - Infos sur l'utilisateur et les appareils. Comprend les stratégies d'appareil, les applications, les actions et les groupes de mise à disposition.
- Cliquez sur Toutes les données.

6. Sélectionnez le Pack d'assistance pour NetScaler Gateway si vous souhaitez inclure des packs d'assistance NetScaler Gateway, puis procédez comme suit :
   1. Cliquez sur Ajouter.



   La boîte de dialogue Ajouter un serveur NetScaler Gateway s'affiche.
   2. Dans Adresse IP de gestion de NetScaler Gateway, entrez l'adresse IP de gestion de NetScaler Gateway à partir de laquelle vous voulez extraire votre pack d'assistance.
      Remarque : si vous créez un pack à partir d'un serveur NetScaler Gateway qui est déjà ajouté, l'adresse IP est renseignée.
   3. Dans Nom d'utilisateur et Mot de passe, entrez les informations d'identification utilisateur requises pour accéder au serveur exécutant NetScaler Gateway.
      Remarque : si vous créez un pack à partir d'un serveur NetScaler Gateway qui est déjà ajouté, le nom d'utilisateur est renseigné.
   4. Cliquez sur Ajouter. Le nouveau pack d'assistance NetScaler Gateway est ajouté au tableau.
   5. Répétez l'étape 6 pour ajouter des packs d'assistance NetScaler Gateway supplémentaires le cas échéant.
7. Cliquez sur Créer. Le pack d'assistance est créé et deux nouveaux boutons, Charger sur CIS et Télécharger sur le client s'affichent.



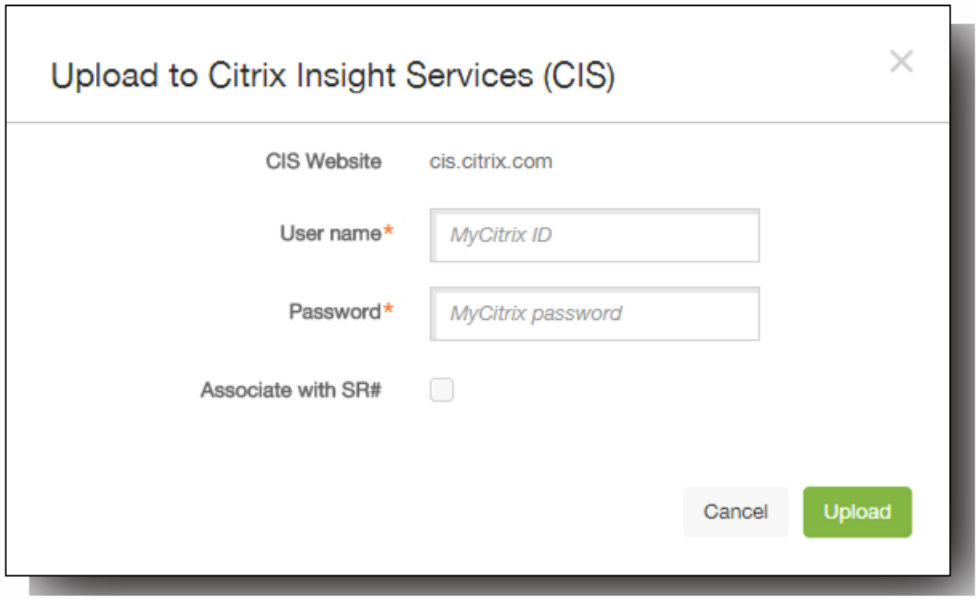
Poursuivez les procédures de **Chargement de packs d'assistance sur Citrix Insight Services** ou de **Téléchargement de packs d'assistance sur un client**.

Chargement de packs d'assistance sur Citrix Insight Services

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Après la création d'un pack d'assistance, vous pouvez le charger sur Citrix Insight Services (CIS) ou télécharger le pack sur votre ordinateur. Ces étapes vous montrent comment charger le pack sur CIS.

1. Sur la page Créer des packs d'assistance, cliquez sur Charger sur CIS. La boîte de dialogue Charger sur Citrix Insight Services (CIS) s'affiche.



2. Dans le champ Nom d'utilisateur, entrez votre ID MyCitrix.
3. Dans le champ Mot de passe, entrez votre mot de passe MyCitrix.
4. Si vous souhaitez associer ce pack à un numéro de demande de service existant, sélectionnez la case à cocher Associer avec la SR n° et dans les deux nouveaux champs qui apparaissent, procédez comme suit :
    1. Dans N° de SR, entrez le numéro de demande de service à huit chiffres que vous souhaitez associer à ce pack.
    2. Dans le champ Description de la SR, entrez une description pour la SR.
5. Cliquez sur Charger. Le pack d'assistance est chargé sur CIS.

Téléchargement de packs d'assistance sur votre ordinateur

Après la création d'un pack d'assistance, vous pouvez le charger sur CIS ou le télécharger sur votre ordinateur. Si vous voulez résoudre le problème par vous-même, téléchargez le pack d'assistance sur votre ordinateur.
Sur la page Créer des packs d'assistance, cliquez sur Télécharger sur le client. Le pack est téléchargé sur votre ordinateur.

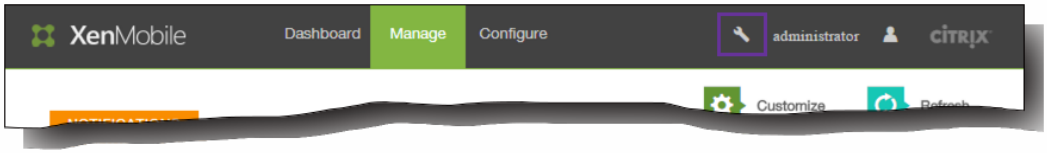
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour afficher le fichier journal de débogage

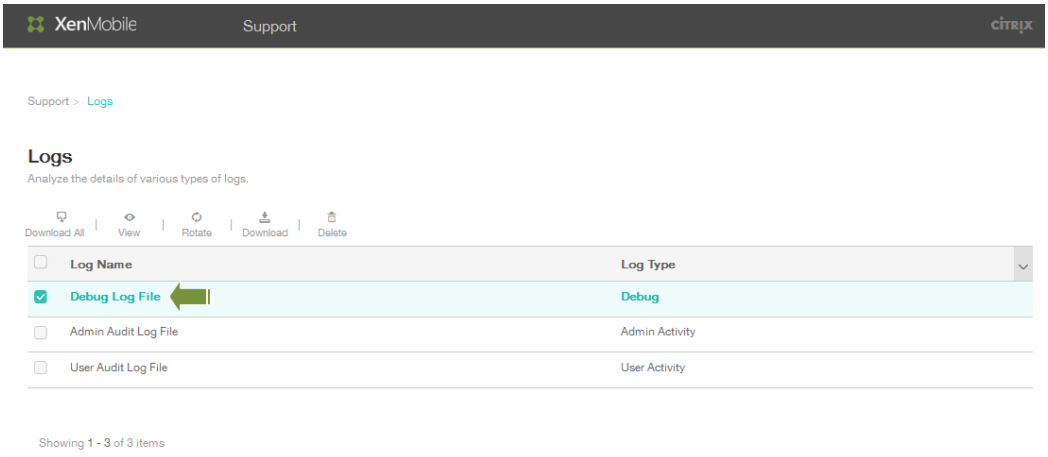
Jul 25, 2016

Suivez ces étapes pour afficher et télécharger le fichier journal de débogage :

1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. L'icône de clé est disponible dans toutes les pages de la console XenMobile.

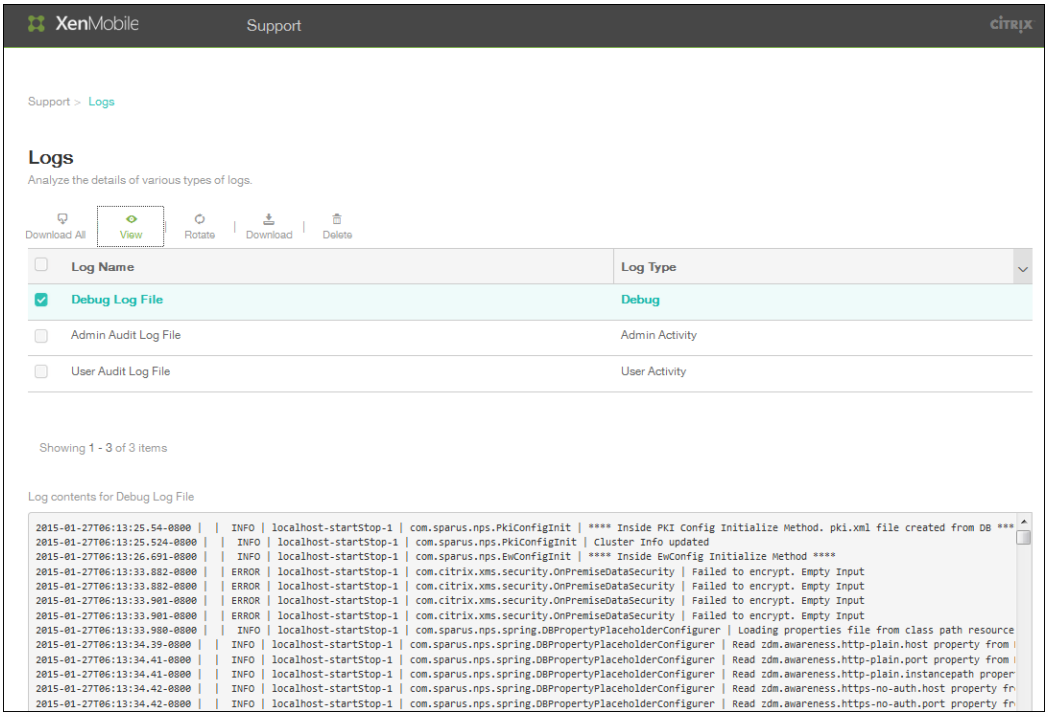


2. Sur la page Support, cliquez sur Journaux. L'écran Journaux s'affiche.



3. Sélectionnez Fichier journal de débogage, puis cliquez sur Afficher pour consulter le contenu du journal.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Après avoir analysé le fichier journal, utilisez l'option Télécharger un fichier pour enregistrer les données ou cliquez sur Supprimer pour supprimer le contenu du journal de la base de données.

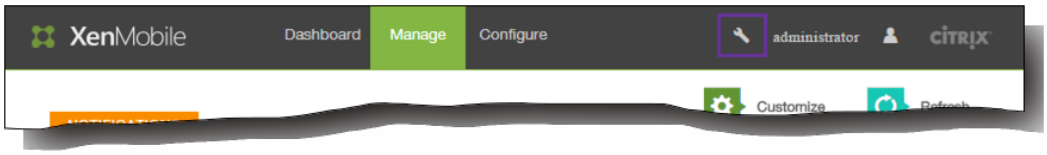
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pour configurer les paramètres du journal

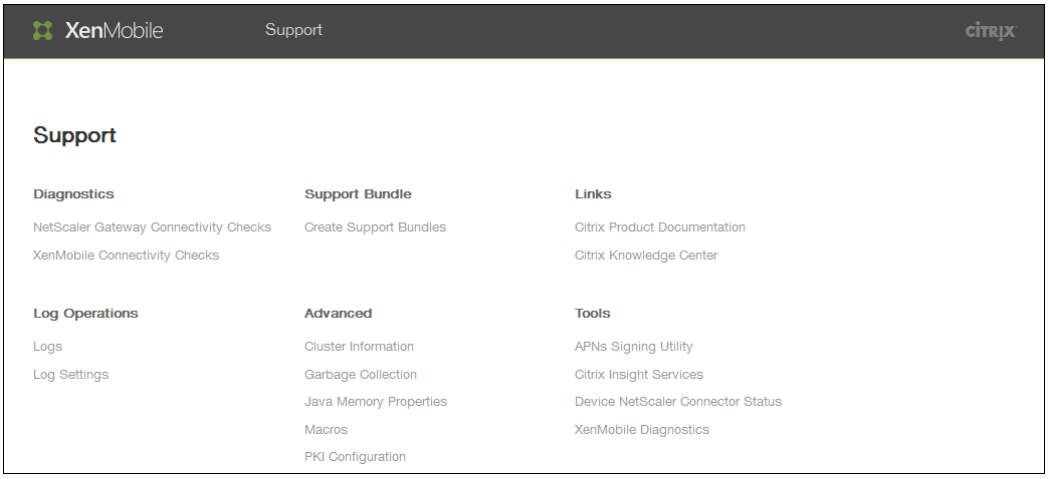
Jul 25, 2016

Vous pouvez configurer les paramètres du journal pour personnaliser les journaux générés par XenMobile. Si vous avez mis en cluster les serveurs XenMobile, lorsque vous configurez les paramètres de journal dans la console XenMobile, ces paramètres sont partagés avec tous les autres serveurs dans le cluster.

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

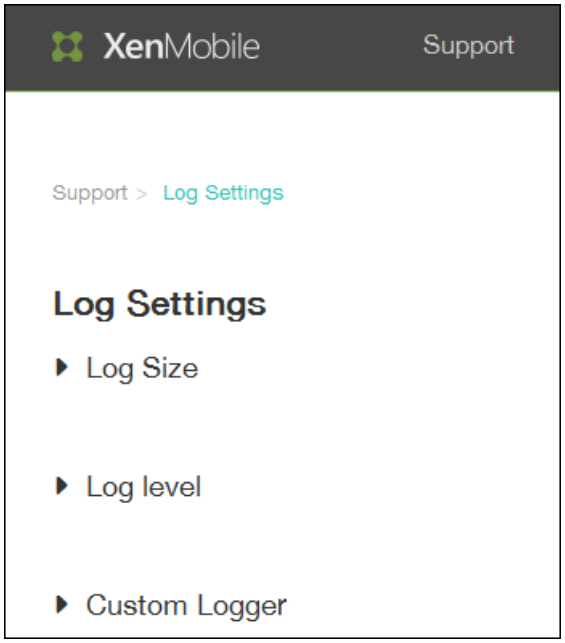


La page Support s'affiche dans un autre onglet de navigateur.



Sous Opérations du journal, cliquez sur Paramètres du journal pour accéder aux options suivantes :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

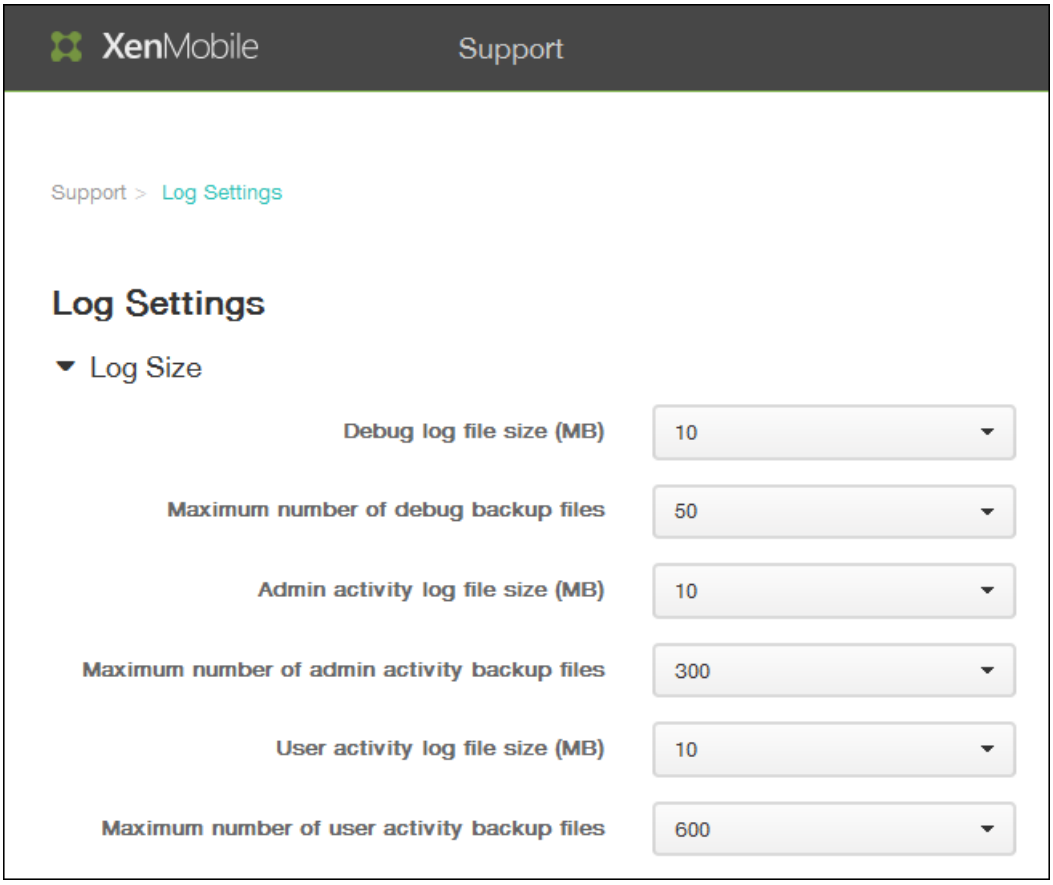


- Taille du journal. Utilisez cette option pour contrôler la taille du fichier journal et le nombre maximal de fichiers de sauvegarde du journal conservés dans la base de données. La taille du journal s'applique à tous les journaux pris en charge par XenMobile (journal de débogage, journal des activités de l'administrateur et journal des activités de l'utilisateur).
- Niveau du journal. Utilisez cette option pour modifier le niveau de journalisation ou pour conserver les paramètres.
- Enregistreur d'événements personnalisé. Utilisez cette option pour créer un enregistreur d'événements personnalisé ; un journal personnalisé requiert un nom de classe et un niveau de journalisation.

Pour configurer les options de taille du journal

1. Sur la page Paramètres du journal, développez Taille du journal et configurez les paramètres suivants :

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Taille du fichier journal de débogage (Mo): dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier de débogage. Par défaut, la taille du fichier est de 10 Mo.
2. Nombre maximum de fichiers de sauvegarde de débogage : dans la liste, cliquez sur le nombre maximal de fichiers de débogage conservés par le serveur. Par défaut, XenMobile conserve 50 fichiers de sauvegarde sur le serveur.
3. Taille du fichier journal des activités des administrateurs (Mo): dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier des activités des administrateurs. Par défaut, la taille du fichier est de 10 Mo.
4. Nombre maximum de fichiers de sauvegarde des activités des administrateurs : dans la liste, cliquez sur le nombre maximal des fichiers d'activités des administrateurs conservés par le serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.
5. Taille du fichier journal des activités des utilisateurs (Mo): dans la liste, sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier des activités des utilisateurs. Par défaut, la taille du fichier est de 10 Mo.
6. Nombre maximum de fichiers de sauvegarde des activités des utilisateurs : dans la liste, cliquez sur le nombre maximal des fichiers d'activités des utilisateurs conservés par le serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.

Pour configurer les options de niveau de journalisation

Le niveau de journalisation vous permet de spécifier le type d'informations que XenMobile collecte dans le journal. Vous pouvez définir le même niveau pour toutes les classes ou vous pouvez définir des niveaux spécifiques pour des classes individuelles.

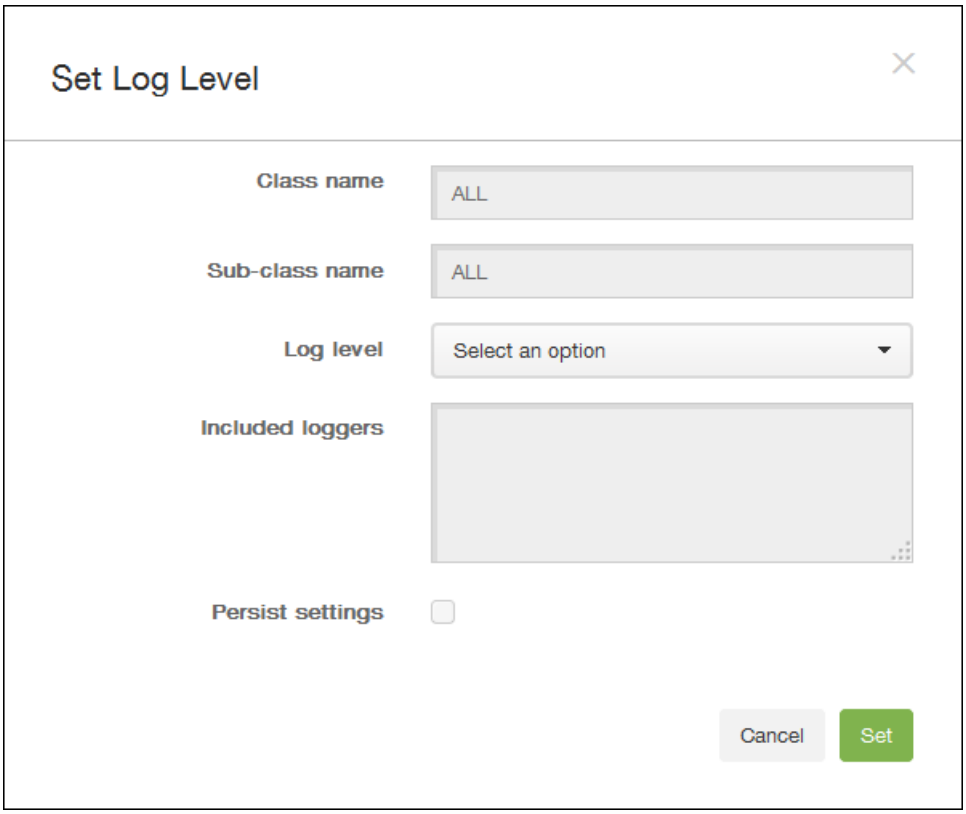
1. Sur la page Paramètres du journal, développez Niveau de journalisation. Un tableau de toutes les classes de journal s'affiche.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Procédez comme suit :
   - Cliquez sur la case à cocher en regard de Classe, puis cliquez sur Définir le niveau pour modifier uniquement le niveau de journalisation de cette classe.
   - Cliquez sur Tout modifier pour appliquer la modification apportée au niveau de journalisation à toutes les classes dans le tableau.

   L'écran des Définir le niveau du journal s'affiche.



1. Nom de la classe : ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche le nom de la classe individuelle ; il n'est pas modifiable.
2. Nom de la sous-classe : ce champ affiche Tout lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche le nom de la sous-classe individuelle ; il n'est pas modifiable.
3. Niveau de journalisation : dans la liste, cliquez sur un niveau de journalisation. Les niveaux de journalisation pris en

© 1999-2017 Citrix Systems, Inc. All rights reserved.

charge sont les suivants :

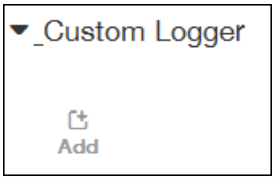
- Fatal
- Erreur
- Avertissement
- Info
- Débogage
- Trace
- Désactivé

4. Enregistreurs d'événements inclus : ce champ est vide lorsque vous modifiez le niveau de journalisation pour toutes les classes ou il affiche les enregistreurs d'événements actuellement configurés pour une classe individuelle ; il n'est pas modifiable.
5. Conserver les paramètres : si vous souhaitez conserver les paramètres de niveau de journalisation lorsque vous redémarrez le serveur, cochez cette case à cocher. Si vous ne sélectionnez pas cette case à cocher, cela indique que les paramètres de niveau de journalisation par défaut sont rétablis lorsque vous redémarrez le serveur.

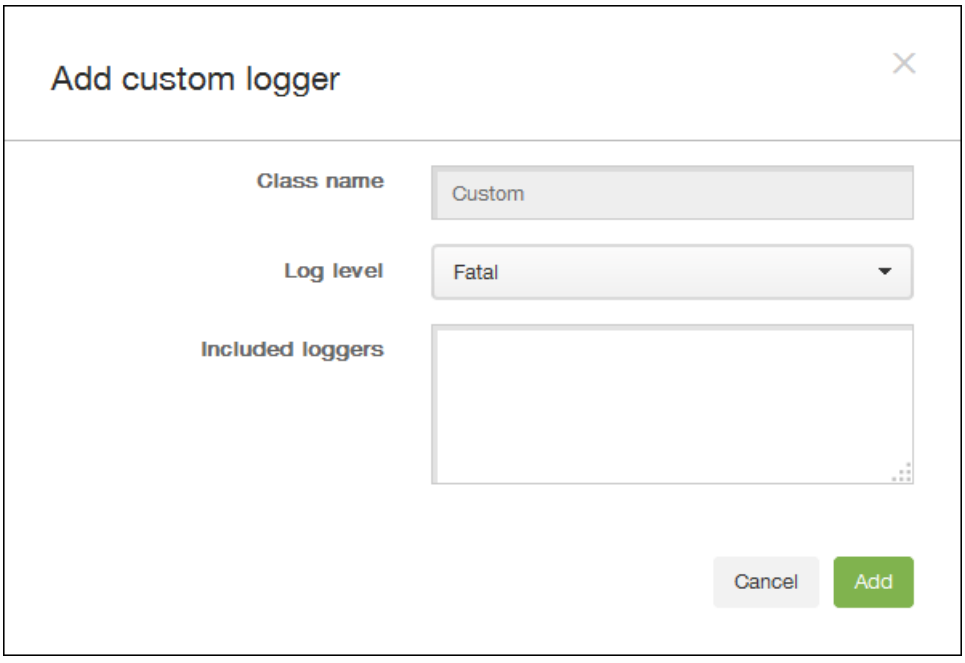
3. Cliquez sur Définir pour valider vos modifications.

Pour ajouter un enregistreur d'événements personnalisé

1. Sur la page Paramètres du journal, développez Enregistreur d'événements personnalisé et cliquez sur Ajouter.



L'écran Ajouter un enregistreur d'événements personnalisé s'affiche.

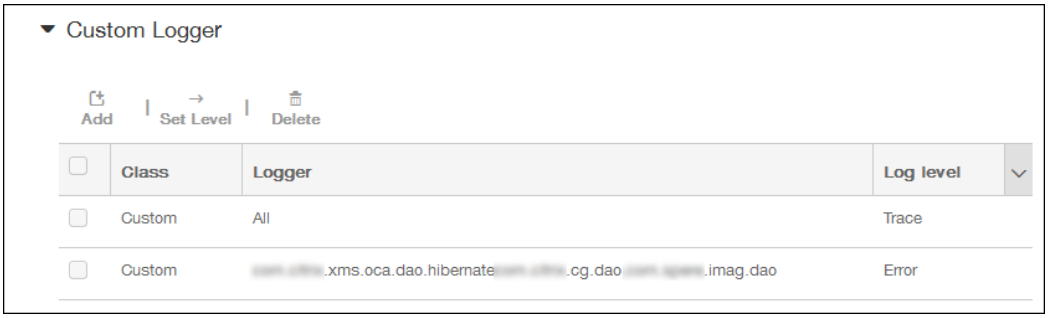


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurez les paramètres suivants :

1. Nom de la classe : ce champ affiche Personnaliser ; il n'est pas modifiable.
2. Niveau de journalisation : dans la liste, cliquez sur un niveau de journalisation. Les niveaux de journalisation pris en charge sont les suivants :
   - Fatal
   - Erreur
   - Avertissement
   - Info
   - Débogage
   - Trace
   - Désactivé
3. Enregistreurs d'événements inclus : ajoutez les enregistreurs d'événements à inclure dans ce journal personnalisé. Vous devez ajouter au moins un enregistreur d'événements.

2. Cliquez sur Ajouter. L'enregistreur d'événements personnalisé est ajouté au tableau Enregistreur d'événements personnalisé.



Pour supprimer un enregistreur d'événements personnalisé

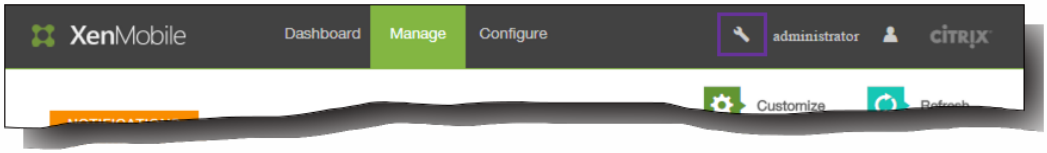
1. Sur la page Paramètres du journal, développez Enregistreur d'événements personnalisé et sélectionnez l'enregistreur d'événements personnalisé que vous souhaitez supprimer.
2. Cliquez sur Supprimer. Une boîte de dialogue s'affiche vous demandant si vous souhaitez supprimer l'enregistreur d'événements personnalisé. Cliquez sur OK.
   Important : vous ne pouvez pas annuler cette opération.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

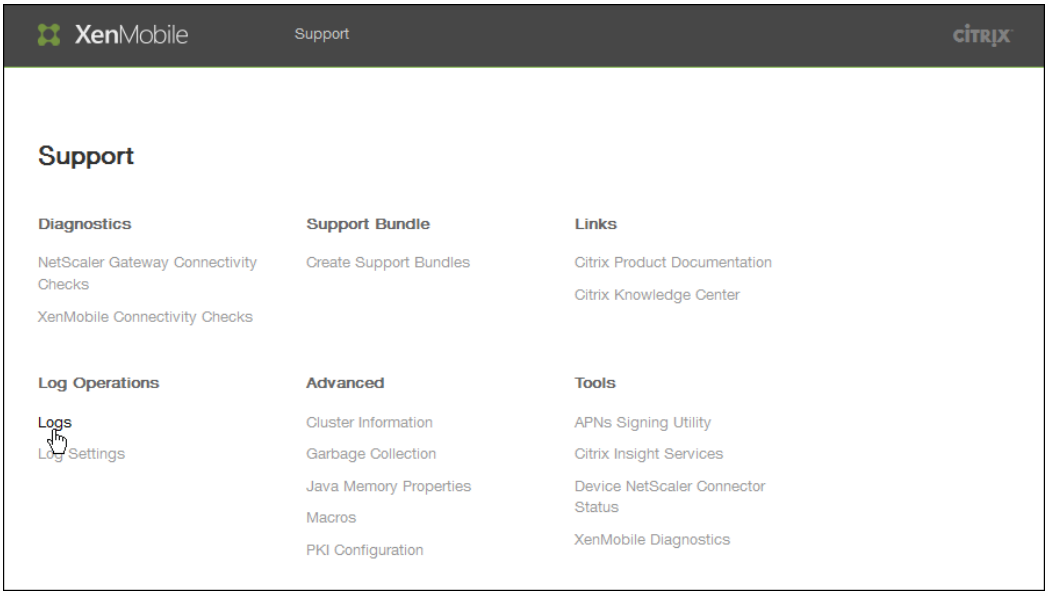
Visualisation et analyse des fichiers journaux dans XenMobile

Jul 25, 2016

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

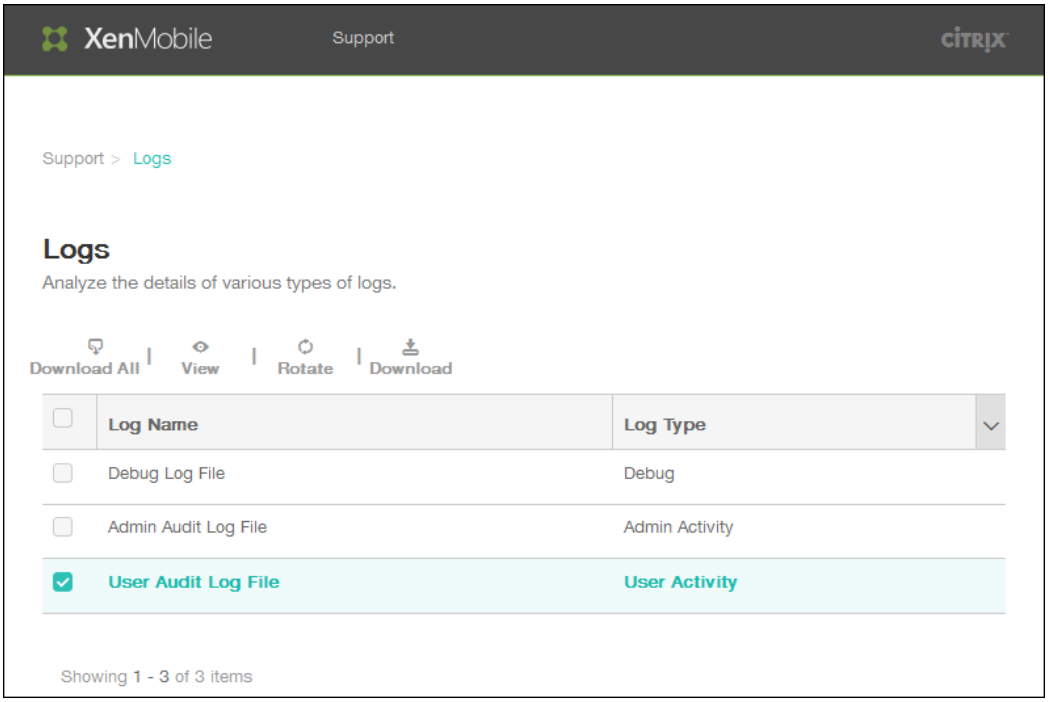


   La page Support s'ouvre dans une nouvelle fenêtre du navigateur.
2. Sous Opérations du journal, cliquez sur **Journaux**.

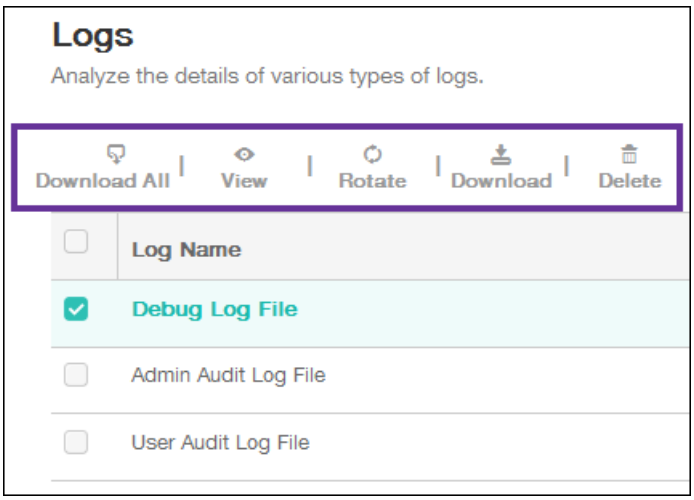


   L'écran **Journaux** s'affiche. Des journaux individuels apparaissent dans un tableau.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sélectionnez le journal que vous souhaitez afficher :
   - Les fichiers journaux de débogage contiennent des informations utiles pour le support Citrix, telles que des messages d'erreur et des actions liées au serveur.
   - Les fichiers journaux d'audit administrateur contiennent des informations d'audit relatives à l'activité sur la console XenMobile.
   - Les fichiers journaux d'audit utilisateur contiennent des informations relatives aux utilisateurs configurés.
4. Utilisez les actions en haut du tableau pour effectuer les opérations suivantes :
   Remarque :
   - Si vous sélectionnez plus d'un fichier journal, seules les options Tout télécharger et Supprimer sont disponibles.
   - Si vous avez mis en cluster des serveurs XenMobile, vous pouvez uniquement afficher les journaux pour le serveur auquel vous êtes connecté. Pour afficher les journaux d'autres serveurs, utilisez l'une des options de téléchargement.

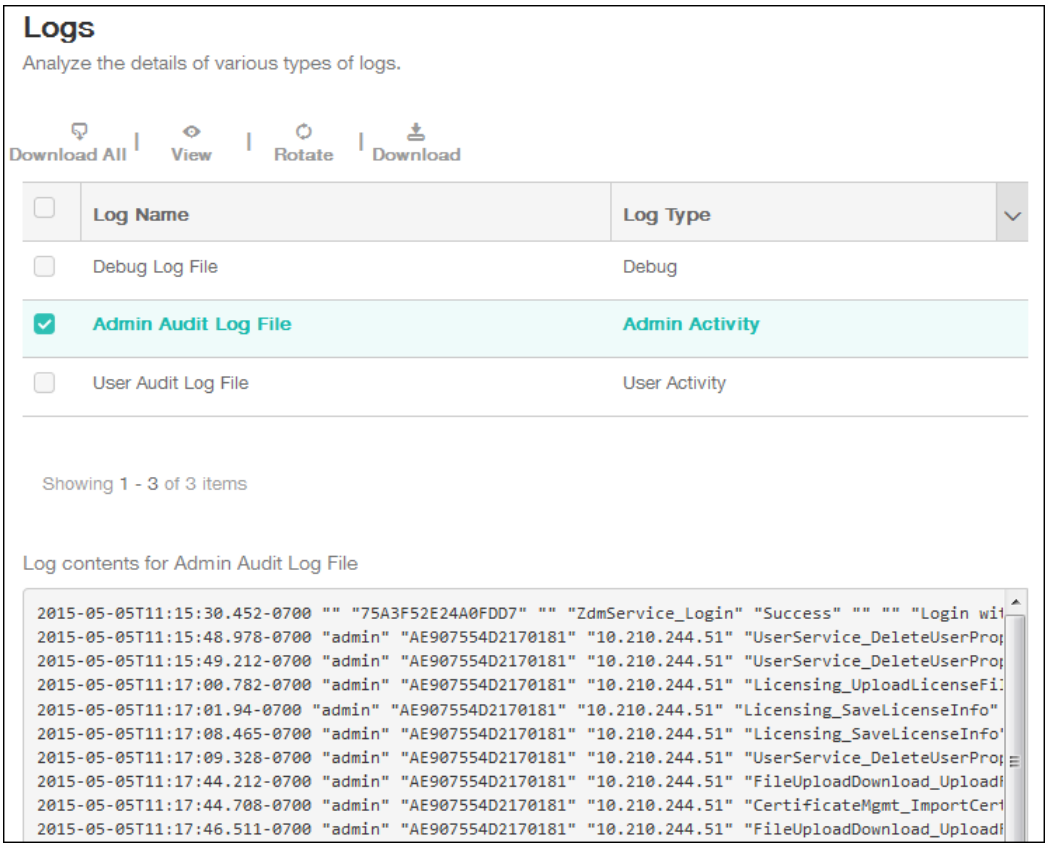


   - Tout télécharger : la console télécharge tous les journaux présents sur le système (y compris les journaux de

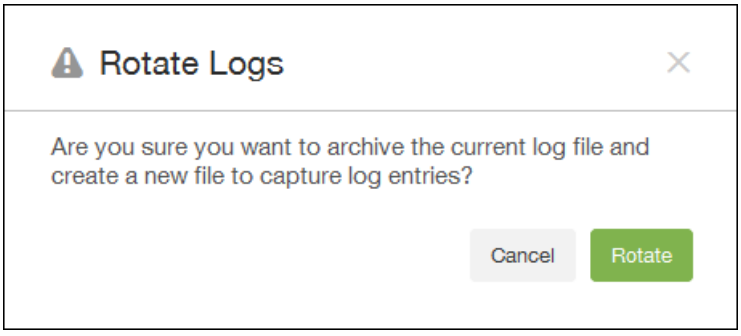
© 1999-2017 Citrix Systems, Inc. All rights reserved.

débogage, d'activité des utilisateurs/administrateurs, de serveur, etc.).

- Afficher : affiche le contenu du journal sélectionné en dessous du tableau.



- Alterner : archive le fichier journal actuel et crée un nouveau fichier pour capturer les entrées de journal. Une boîte de dialogue s'affiche lors de l'archivage d'un fichier journal ; cliquez sur Alterner pour continuer.



- Télécharger : la console télécharge uniquement le type de fichier journal sélectionné ; elle télécharge également tous les journaux archivés pour ce même type.
- Supprimer : supprime de manière définitive les fichiers journaux sélectionnés.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Options d'interface de ligne de commande XenMobile

Jul 25, 2016

Vous pouvez accéder à tout moment aux options d'interface de ligne de commande suivantes (CLI) sur l'hyperviseur sur lequel vous avez installé XenMobile : Citrix XenServer, Microsoft Hyper-V ou VMware ESXi.

Vous trouverez ci-après les choix que vous pouvez effectuer dans le menu principal et les menus qui s'affichent pour chacune des quatre premières options : Configuration, Mise en cluster, Système, et Dépannage.

Menu principal

---

[0] Configuration

[1] Mise en cluster

[2] Système

[3] Dépannage

[4] Aide

[5] Fermer la session

Choix : [0 - 5]

Options du menu de configuration

À partir du menu principal, lorsque vous sélectionnez l'option Configuration, les menus suivants s'affichent :

[0] Retour au menu principal

[1] Réseau

[2] Pare-feu

[3] Base de données

[4] Ports d'écoute

Choix : [0 - 4]

Lorsque vous choisissez l'option Réseau, vous êtes invité à redémarrer pour enregistrer les modifications.

Lorsque vous choisissez l'option Pare-feu, vous êtes invité à effectuer ce qui suit :

Configurer les services qui sont activés via le pare-feu.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Possibilité de configurer l'accès aux listes blanches :

- liste séparée par des virgules d'hôtes ou de réseaux

- par exemple 10.20.5.3, 10.20.6.0/24

- une valeur vide signifie aucune restriction d'accès

- entrez la valeur c pour effacer la liste

Service HTTP

Port : 80

Activer l'accès (y/n) [Y]:

Service HTTPS de gestion

Port : 4443

Activer l'accès (y/n) [Y]:

Service SSH

Port [22]:

Activer l'accès (y/n) [Y]:

Accès liste blanche []:

Service HTTPS de l'API de gestion (pour la gestion intermédiaire)

Port [30001]:

Activer l'accès (y/n) [Y]:

Accès liste blanche []:

Tunnel d'assistance à distance

Port [8081]:

Activer l'accès (y/n) [n]:

Lorsque vous choisissez l'option Base de données, vous êtes invité à effectuer ce qui suit :

Type: [mi]

Utiliser SSL (y/n) [y]:

Charger le certificat racine (y/n) [y]:

Copier ou Importer (c/i) [c]:

Options du menu de mise en cluster

© 1999-2017 Citrix Systems, Inc. All rights reserved.

À partir du menu principal, lorsque vous sélectionnez l'option Mise en cluster, les menus suivants s'affichent :

[0] Retour au menu principal

[1] Afficher l'état du cluster

[2] Activer/désactiver le cluster

[3] Liste blanche des membres du cluster

[4] Activer ou désactiver le déchargement SSL

[5] Afficher le cluster Hazelcast

Choix : [0 - 5]

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.

Lorsque vous sélectionnez la liste blanche de membre du cluster, et que vous avez désactivé la mise en cluster, le message suivant s'affiche :

Le cluster est désactivé. Veuillez l'activer.

Si la mise en cluster est activée, les options suivantes s'affichent :

Liste blanche actuelle :

- liste séparée par des virgules d'hôtes ou de réseaux

- par exemple 10.20.5.3, 10.20.6.0/24

- une valeur vide signifie aucune restriction d'accès

Veuillez entrer les hôtes ou réseaux à mettre sur liste blanche :

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.

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Membres du cluster Hazlecast :

[Adresse IP répertoriée]

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

Options du menu Système

À partir du menu principal, lorsque vous sélectionnez l'option Système, les menus suivants s'affichent :

---

[0] Retour au menu principal

[1] Afficher la date système

[2] Définir le fuseau horaire

[3] Afficher l'utilisation du disque système

[4] Mettre à jour le fichier d'hôtes

[5] Serveur proxy

[6] Mot de passe (CLI) administrateur

[7] Redémarrer le serveur

[8] Arrêter le serveur

[9] Paramètres avancés

Choix : [0 - 9]

Options du menu Dépannage

À partir du menu principal, lorsque vous sélectionnez l'option Dépannage, les menus suivants s'affichent :

---

[0] Retour au menu principal

[1] Utilitaires de réseau

[2] Journaux

[3] Pack d'assistance

Choix : [0 - 3]

Lorsque vous sélectionnez l'option Utilitaires de réseau, le menu suivant s'affiche :

© 1999-2017 Citrix Systems, Inc. All rights reserved.

[0] Retour au menu de dépannage

[1] Informations réseau

[2] Afficher la table de routage

[3] Afficher la table ARP (Protocole de résolution d'adresse)

[4] PING

[5] Détermination d'itinéraire

[6] Recherche DNS

[7] Trace réseau

Choix : [0 - 7]

Lorsque vous sélectionnez l'option Journaux, le menu suivant s'affiche :

Menu Journaux

---

[0] Retour au menu de dépannage

[1] Afficher le fichier journal

Choix : [0 - 1]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

APIs XenMobile

Jul 25, 2016

Vous pouvez utiliser les API des services Web suivants dans XenMobile pour gérer votre flotte mobile. Vous pouvez télécharger les API et les kits de développement pour XenMobile depuis le site XenMobile Developer Community.

Nom WSDL (Service Web Definition Language)	Appels
EveryWanDevice	addDevice
	addDevice
	authenticateUser
	authorize
	canCreateUser
	clearDeploymentHisto
	corporateDataWipeDevice
	createUser
	deploy
	deviceExists
	disableTrackingDevice
	enableTrackingDevice
	findDeviceByUdid
	getAllDevices
	getDeploymentHisto
	getDeploymentHisto

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom WSDL (Service Web Definition Language)	Appels
	getDeviceInfo
	getDeviceInformationForUser
	getDeviceProperties
	getLastUser
	getManagedStatus
	getMasterKeyList
	getSoftwareInventory
	getStrongID
	getUserDevices
	isEnforceSSL
	isEnforceStrongAuthentication
	locateDevice
	lockDevice
	putDeviceProperties
	registerDeviceForUser
	removeDevice
	resetDeploymentState
	revoke
	unlockDevice

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nom WSDL (Service Web Definition Language)	Appels
	wipeDevice
	addDevice
CiscoISE/NAC	action/pinlock
	/mdminfo
	/devices/0/all
	/devices/0/macaddress/
	/batchdevices/0/macaddress/all
OTPServices	createOTP
	getAvailableEnrollmentModes
	getOtpInfo
	triggerNotification

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Mail Manager 10

Jul 25, 2016

XenMobile Mail Manager permet d'étendre les capacités de XenMobile des façons suivantes :

- Contrôle d'accès dynamique des appareils EAS (Exchange Active Sync). L'accès des appareils EAS aux services Exchange peut être automatiquement autorisé ou bloqué.
- Permet à XenMobile d'accéder aux informations de partenariat d'appareil EAS fournies par Exchange.
- Permet à XenMobile d'effacer EAS sur un appareil mobile.
- Permet à XenMobile d'accéder à des informations sur des appareils Blackberry, et de réaliser des opérations de contrôle telles que l'effacement à distance (Wipe) et/ou la réinitialisation du mot de passe (ResetPassword).

Problèmes connus et résolus dans la version actuelle de XenMobile Mail Manager 10.0. Pour télécharger XenMobile Mail Manager, consultez la section Server Components (Composants serveur) dans la rubrique XenMobile 10 Server sur Citrix.com.

Problèmes connus

- La version installée de XenMobile Mail Manager affiche toujours la version 8.5 durant la mise à niveau vers XenMobile Mail Manager 10 ; toutefois, la mise à niveau de XenMobile Mail Manager se produit correctement. [#539520]
- L'affichage du message « devices found » dans l'instantané secondaire peut prêter à confusion. Le même périphérique ou les mêmes périphériques peuvent être signalés en tant que « new » dans les résumés d'instantanés secondaires lorsque les instantanés secondaires sont exécutés après le démarrage d'un instantané principal.

Problèmes résolus

Power Shell/Exchange Management

Dans certains environnements Microsoft Exchange (principalement Office 365), XenMobile Mail Manager subit une restriction qui limite la bande passante, empêchant ainsi les applications de lancer des requêtes ou des commandes PowerShell. Vous pouvez maintenant utiliser un autre chemin d'applet de commande PowerShell dans l'onglet de configuration Exchange, qui fait passer XenMobile Mail Manager à un autre mode de capture instantanée ; ce mode contourne le chemin d'accès aux données d'origine.

Un nouvel indicateur permet d'exposer l'indicateur **AllowRedirection** pour les environnements autres que Microsoft Office 365. Utilisez l'onglet de configuration de Microsoft Exchange pour activer cet indicateur.

Gestion des règles

Les règles locales LDAP prennent en charge un nombre indéterminé de groupes pour les environnements Active Directory larges.

XenMobile duplique les informations d'appareil pour les clients WorxMail. La résolution de ce problème requiert que vous activiez la prise en charge de l'expression régulière dans la partie Managed Service Provider (MSP) de XenMobile Mail Manager ; cela filtre les jeux d'enregistrements renvoyés à XenMobile. Les appareils correspondants au filtre ne sont pas renvoyés à XenMobile.

MSP

Les utilisateurs qui sont supprimés de la base de données Blackberry Enterprise Server (BES) sont désormais supprimés de la base de données locale.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Interface utilisateur

Vous pouvez désormais utiliser une classe de dialogue de progression pour les scénarios dans lesquels un processus persistant prend place. Dans un tel processus, XenMobile Mail Manager envoie des commentaires aux utilisateurs et leur offre la possibilité d'annuler le cas échéant.

La valeur par défaut pour les nouvelles instances de Microsoft Exchange est définie sur *Shallow*.

Programme d'installation

Les composants faisant référence à Zenprise ont été modifiés pour refléter XenMobile Mail Manager.

Le programme d'installation s'arrête s'il ne trouve pas le chemin d'installation.

Après l'installation les fichiers binaires et les scripts pris en charge se trouvent désormais dans le dossier Support.

Dans le menu Démarrer de Windows, les raccourcis XenMobile Mail Manager se trouvent désormais dans le dossier \Citrix\XenMobile Mail Manager.

Support

Le modèle de support offre la possibilité d'activer la fonction de dépannage grâce à l'ajout d'un fichier config.xml. Vous pouvez utiliser ce fichier pour aider Citrix à résoudre les problèmes. Dans cette version de XenMobile Mail Manager, cette fonction s'applique uniquement aux écrans Add et Edit de la configuration de Microsoft Exchange.
Remarque : vous pouvez également activer cette fonction de résolution des problèmes en maintenant la touche Maj lors de l'ouverture de l'utilitaire de configuration.

Journalisation

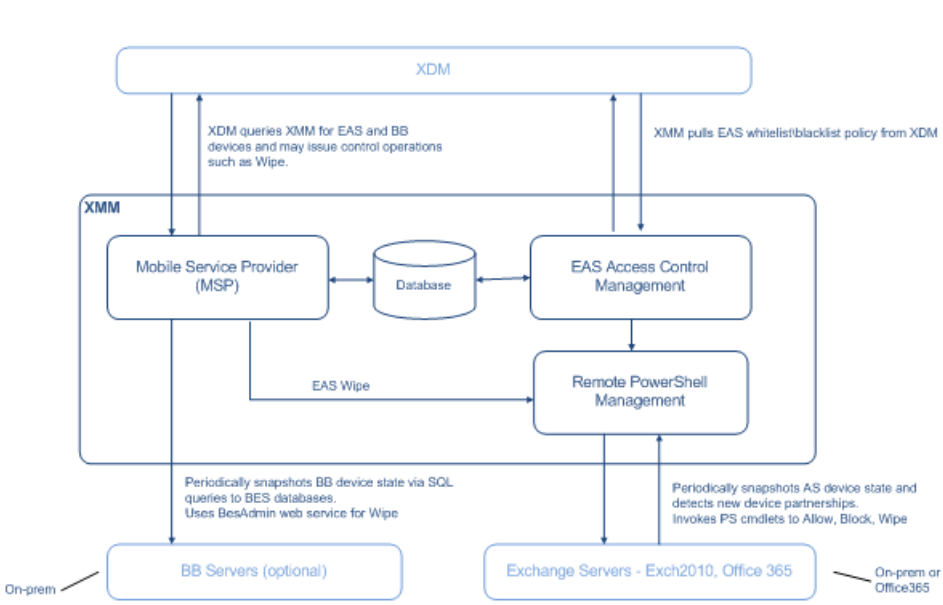
Les messages d'erreur renvoyés par PowerShell sont désormais accompagnés d'un GUID. Utilisez cette valeur pour contrôler ce qui s'affiche dans l'onglet Snapshot History.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Architecture

Oct 11, 2016

Le diagramme suivant illustre les composants principaux de XenMobile Mail Manager. 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.



Les trois composants principaux sont :

- **Exchange ActiveSync Access Control Management**. Communique avec XenMobile pour récupérer une stratégie Exchange ActiveSync depuis XenMobile, puis fusionne cette stratégie avec toutes les stratégies définies localement pour déterminer les appareils Exchange ActiveSync ayant le droit ou non d'accéder à Exchange. Les stratégies locales permettent d'étendre les règles de stratégie pour autoriser le contrôle d'accès par un groupe Active Directory, utilisateur, type d'appareil ou agent utilisateur de l'appareil (généralement la version de la plate-forme mobile).
- **Remote PowerShell Management**. Ce composant est responsable de la planification et de l'appel des commandes PowerShell à distance afin d'appliquer la stratégie compilée par la gestion du contrôle d'accès à Exchange ActiveSync. Il crée régulièrement un instantané de la base de données Exchange ActiveSync pour détecter de nouveaux périphériques ou des périphériques modifiés Exchange ActiveSync.
- Mobile Service Provider. Fournit une interface de service Web permettant à XenMobile d'interroger Exchange ActiveSync et/ou des appareils Blackberry, et également d'émettre des opérations de contrôle, telles que l'effacement.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration système requise et conditions préalables

Jul 25, 2016

La configuration système minimale suivante est nécessaire pour utiliser XenMobile Mail Manager :

- Windows Server 2008 R2 (doit être un serveur en anglais)
- Microsoft SQL Server 2008, SQL Server 2012, SQL Server Express 2008, SQL Server 2012 ou Microsoft SQL Server 2012 Express LocalDB
- Microsoft .NET Framework 4.5
- Blackberry Enterprise Service, version 5 (facultatif)

Versions minimales prises en charge de Microsoft Exchange Server

- Microsoft Office 365
- Exchange Server 2013
- Exchange Server 2010 SP2

Conditions préalables requises par XenMobile Mail Manager

- Windows Management Framework doit être installé.
  - PowerShell V4, V3 et V2
- La stratégie d'exécution de PowerShell doit être paramétrée sur RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- Le port TCP 80 doit être ouvert entre l'ordinateur exécutant XenMobile Mail Manager et le serveur Exchange distant.

Configuration requise pour l'ordinateur sur site exécutant Exchange

- **Autorisations**. Le contrôle d'accès basé sur rôle (RBAC) Exchange n'est pas couvert dans cette documentation. Cela dit, les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent, au minimum, être en mesure de se connecter au serveur Exchange Server et bénéficier d'un accès complet pour exécuter les applets de commande PowerShell spécifiques à Exchange suivantes :
  - Get-CASMailbox
  - Set-CASMailbox
  - Get-Mailbox
  - Get-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Clear-ActiveSyncDevice
- 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.
- Comme documenté dans l'article https://technet.microsoft.com/fr-fr/library/dd315349.aspx, 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 blog, http://blogs.msdn.com/b/powershell/archive/2009/11/23/you-don-t-have-to-be-an-administrator-to-run-remote-powershell-commands.aspx, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 d'entre elles 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. Une fois la limite de connexion atteinte, XenMobile Mail Manager ne sera plus en mesure de 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.

Configuration requise pour Office 365 Exchange

- **Autorisations**. Le contrôle d'accès basé sur rôle (RBAC) Exchange n'est pas couvert dans cette documentation. Cela dit, les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent, au minimum, 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-ActiveSyncDevice`
  - `Get-ActiveSyncDeviceStatistics`
  - `Clear-ActiveSyncDevice`
- Les informations d'identification fournies doit avoir été autorisées à se connecter au serveur Office 365 via le Shell distant. Par défaut, l'administrateur en ligne d'Office 365 possède les privilèges requis.
- Exchange possède de nombreuses stratégies de limitation. L'une d'entre elles contrôle combien de connexions PowerShell simultanées sont autorisées par utilisateur. Par défaut, le nombre de connexions simultanées autorisées pour un utilisateur est de 3 sur Office 365. Une fois la limite de connexion atteinte, XenMobile Mail Manager ne sera plus en mesure de 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.

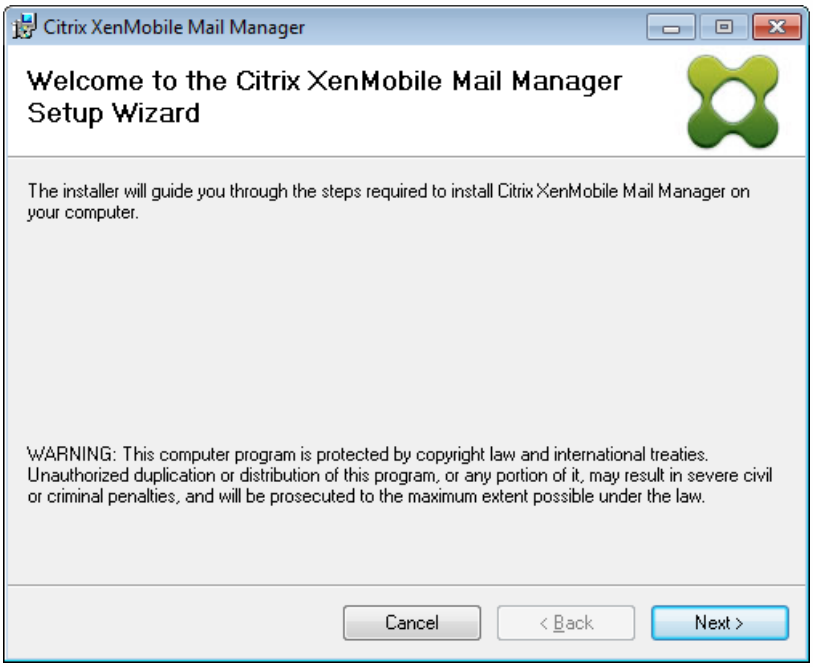
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Installation et configuration

Jul 25, 2016

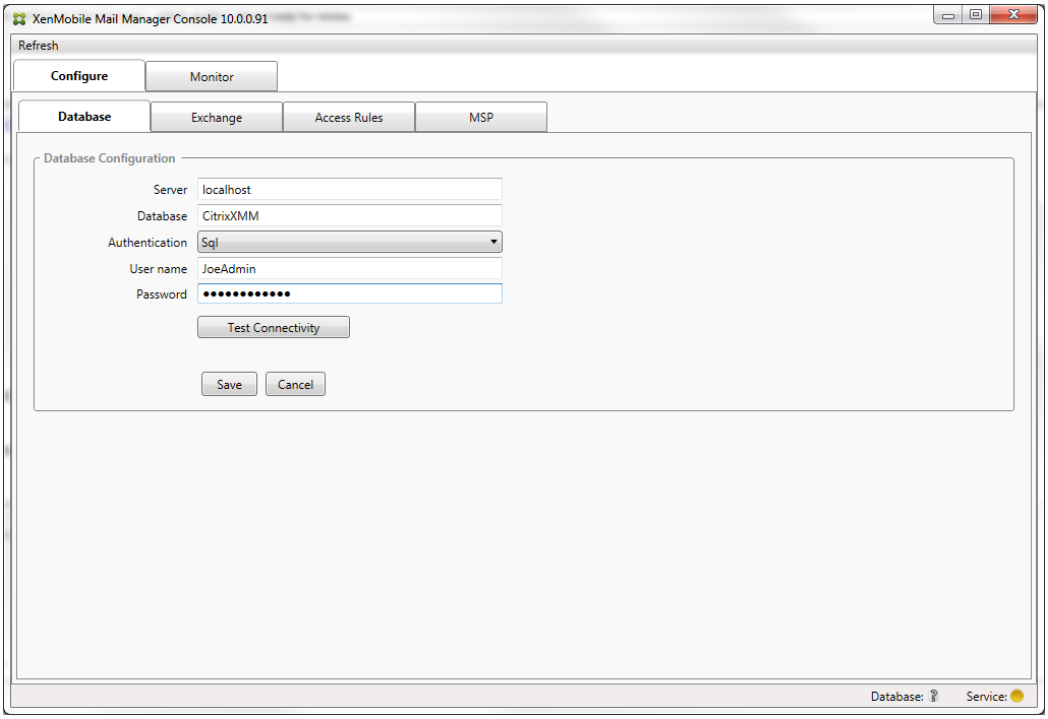
Suivez ces étapes pour installer et configurer XenMobile Mail Manager. Avant de commencer, assurez-vous d'avoir consulté la configuration système requise et les conditions préalables. Pour de plus amples informations, consultez la section Configuration système requise et conditions préalables pour XenMobile Mail Manager.

1. Cliquez sur le fichier XmmSetup.msi puis suivez les instructions de l'assistant pour installer XenMobile Mail Manager.



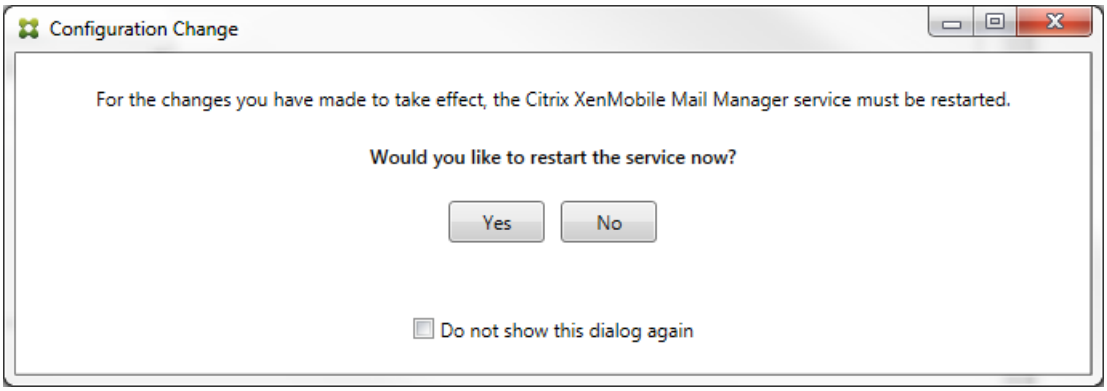
2. Dans le menu Démarrer, ouvrez XenMobile Mail Manager.
3. Configurez les propriétés de base de données suivantes :
   1. Sélectionnez l'onglet Configure > Database.
   2. Entrez le nom du serveur SQL (localhost par défaut).
   3. Conservez la base de données par défaut CitrixXmm.
   4. Sélectionnez l'un des modes d'authentification suivants utilisés pour SQL :
      - SQL. Entrez le nom d'utilisateur et le mot de passe d'un utilisateur SQL valide.
      - Windows Integrated. Si vous sélectionnez cette option, les informations d'identification d'ouverture de session du service XenMobile Mail Manager doivent être modifiées par un compte Windows disposant des autorisations nécessaires pour accéder au serveur SQL. Pour ce faire, ouvrez le Panneau de configurationOutils d'administrationServices, cliquez avec le bouton droit de la souris sur l'entrée du service XenMobile Mail Manager, puis sélectionnez l'onglet Ouverture de session.
        Remarque : si Windows Integrated est également choisi pour la connexion à la base de données BlackBerry, le compte Windows spécifié ici doit également pouvoir accéder à la base de données BlackBerry.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



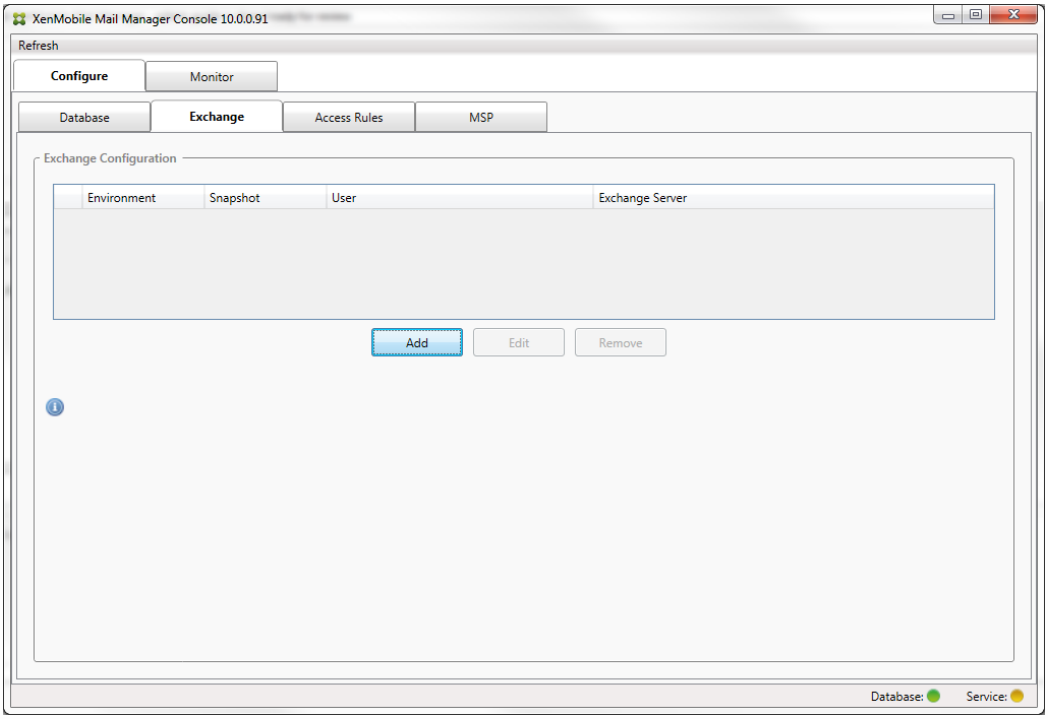
5. Cliquez sur Test Connectivity pour vérifier qu'une connexion peut être établie avec le serveur SQL, puis cliquez sur Save.

4. Un message vous invite à redémarrer le service. Cliquez sur Oui.

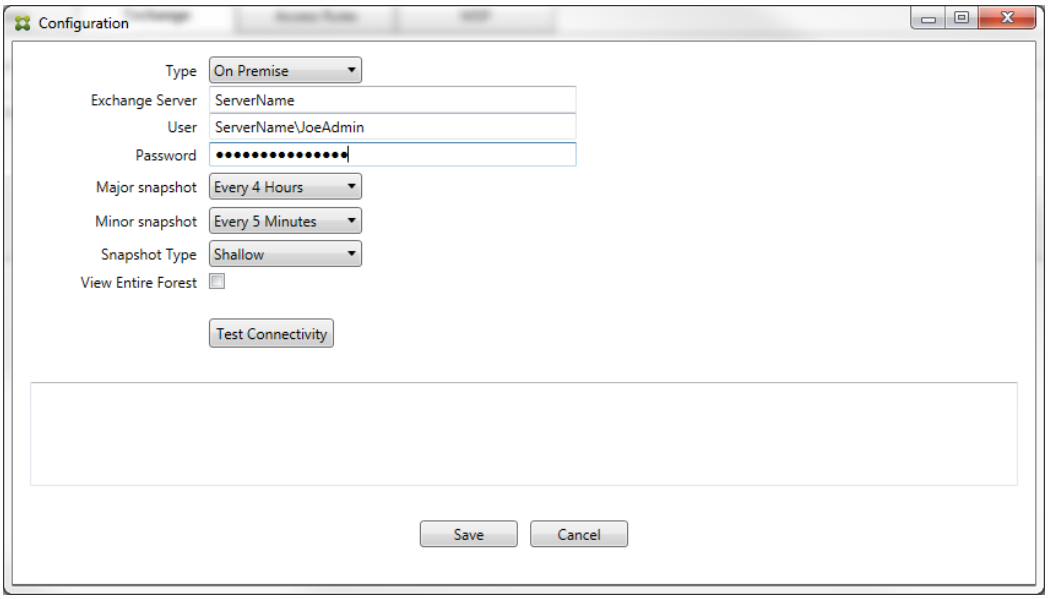


5. Configurez un ou plusieurs serveurs Exchange :
   1. Si vous ne gérez qu'un seul environnement Exchange, vous n'avez besoin que d'un seul serveur. Si vous gérez plusieurs environnements Exchange, vous avez besoin d'un seul serveur Exchange spécifié pour chaque environnement Exchange.
   2. Sélectionnez l'onglet Configure > Exchange.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Cliquez sur Ajouter.
4. Sélectionnez le type d'environnement de serveur Exchange, soit On Premise soit Office 365.



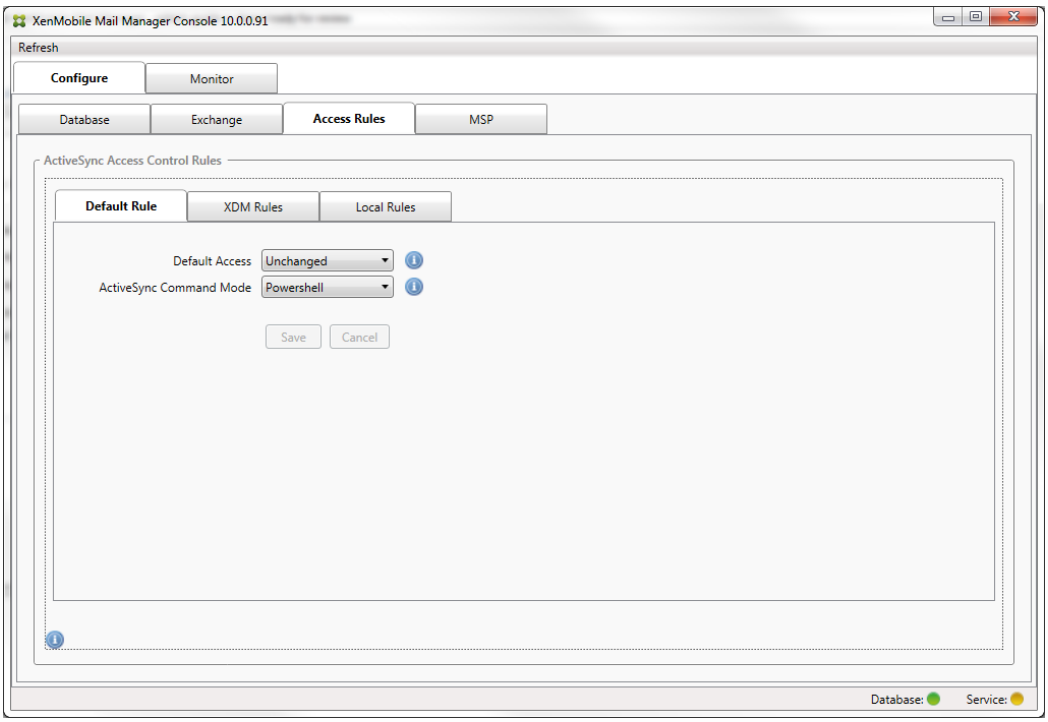
5. Si vous sélectionnez On Premise, entrez le nom du serveur Exchange qui sera utilisé pour les commandes PowerShell à distance.
6. Entrez le nom d'utilisateur d'une identité Windows disposant des droits appropriés sur le serveur Exchange comme indiqué dans la section Configuration requise.
7. Entrez le mot de passe (Password) de l'utilisateur.
8. Sélectionnez la planification d'exécution de captures d'instantanés principaux. Un instantané principal détecte tous les partenariats Exchange ActiveSync.
9. Sélectionnez la planification d'exécution des captures d'instantanés secondaires. Un instantané secondaire détecte les partenariats Exchange ActiveSync nouvellement créés.
10. Sélectionnez le type d'instantané : Deep ou Shallow. Les instantanés Shallow sont plus rapides et suffisants pour

© 1999-2017 Citrix Systems, Inc. All rights reserved.

exécuter toutes les fonctions de contrôle d'accès Exchange ActiveSync de XenMobile Mail Manager. Les instantanés Deep peuvent prendre beaucoup plus de temps et sont uniquement nécessaires si Mobile Service Provider est activé pour ActiveSync (ce qui permet à Device Manager d'interroger les appareils non gérés).

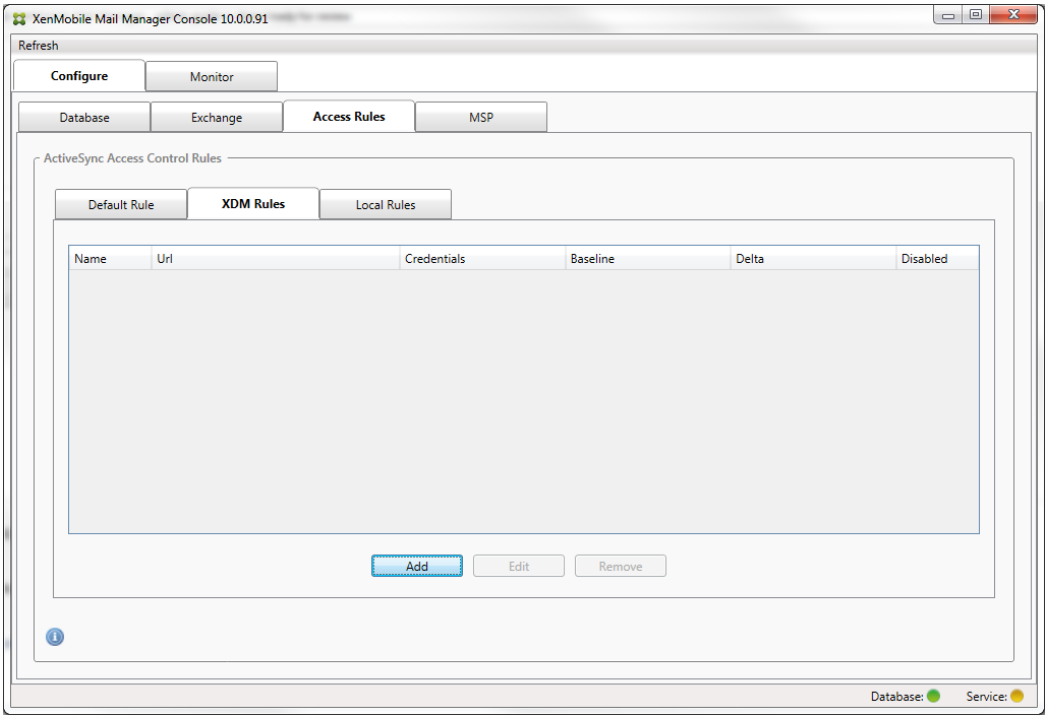
11. Cliquez sur Test Connectivity pour vérifier qu'une connexion peut être établie avec le serveur Exchange, puis cliquez sur Save.
12. Un message vous invite à redémarrer le service. Cliquez sur Oui.

6. Configurez les règles d'accès :
    1. Sélectionnez l'onglet ConfigureAccess Rules.

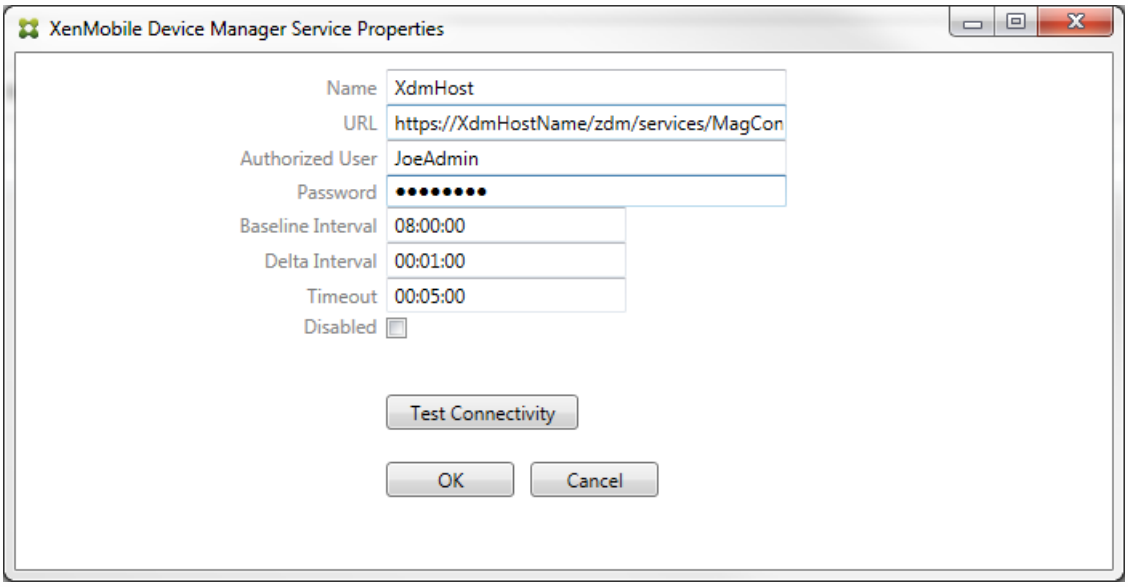


    2. Sélectionnez les paramètres d'accès par défaut : Allow, Block ou Unchanged. Cela contrôle la façon dont sont traités tous les appareils autres que ceux identifiés explicitement par des règles locales ou XenMobile. Si vous sélectionnez Allow, l'accès à ActiveSync sera autorisé à tous les appareils ; si vous sélectionnez Block, l'accès leur sera refusé. Si vous sélectionnez Unchanged, aucune modification ne sera apportée.
    3. Sélectionnez le mode de commande ActiveSync : PowerShell ou Simulation.
        - En mode PowerShell, XenMobile Mail Manager émet des commandes PowerShell afin d'appliquer le contrôle d'accès souhaité.
        - En mode Simulation, XenMobile Mail Manager n'émet pas de commandes PowerShell, mais consigne la commande prévue et les résultats escomptés dans la base de données. En mode Simulation, l'utilisateur peut alors utiliser l'onglet Monitor pour voir ce qui serait arrivé si le mode PowerShell était activé.
    4. Cliquez sur Save.
7. Cliquez sur l'onglet XDM Rules.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



1. Cliquez sur Ajouter.
2. Entrez un nom pour les règles XDM, comme XdmHost.

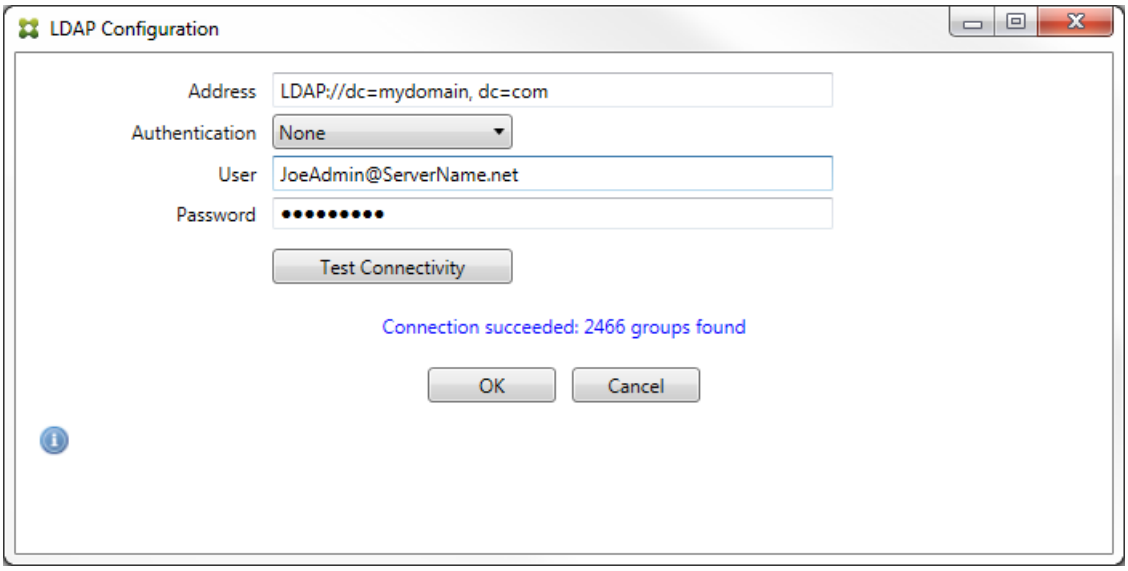


3. Modifiez l'URL pour qu'elle pointe vers le serveur XenMobile ; par exemple, si le nom du serveur est XdmHost, entrez http://NomHôteXdm/services/MagConfigService.
4. Entrez un utilisateur autorisé sur le serveur.
5. Entrez le mot de passe de l'utilisateur.
6. Conservez les valeurs par défaut Baseline Interval, Delta Interval, et Timeout values.
7. Cliquez sur Test Connectivity pour tester la connexion au serveur.
   Remarque : si la case Disabled est cochée, XenMobile Mail Service ne collectera pas de stratégie depuis le serveur XenMobile.
8. Cliquez sur OK.

8. Cliquez sur l'onglet Local Rules.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

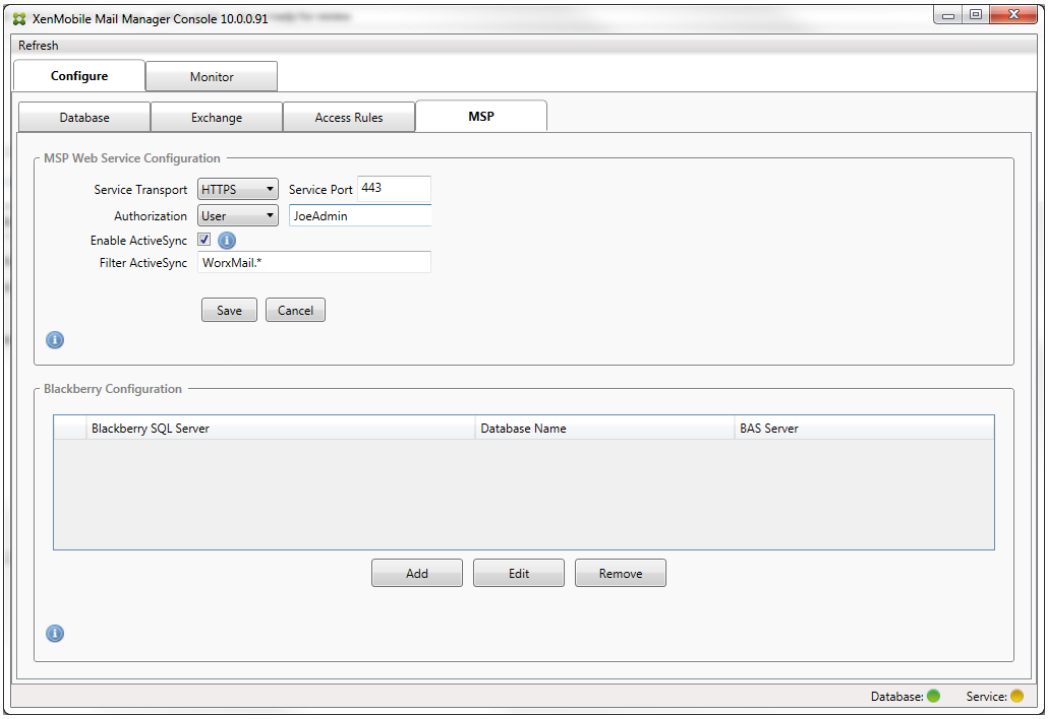
1. Si vous souhaitez créer des règles locales qui fonctionnent sur des groupes Active Directory, cliquez sur Configure LDAP, puis configurez les propriétés de connexion LDAP.



2. Vous pouvez ajouter des règles locales basées sur ActiveSync Device ID, Device Type, AD Group, User ou User Agent. Sélectionnez le type approprié dans la liste. Pour de plus amples informations, consultez la section Règles de contrôle d'accès à XenMobile Mail Manager.
3. Tapez le texte ou les fragments de texte dans la zone de texte. Si vous le souhaitez, cliquez sur le bouton de requête pour afficher les entités qui correspondent au fragment.
   Remarque : pour tous les types autres que Group, le système s'appuie sur les appareils qui ont été localisés dans un instantané. Par conséquent, si vous démarrez et que vous n'avez pas réalisé d'instantané, aucune entité ne sera disponible.
4. Sélectionnez une valeur de texte, puis cliquez sur Allow ou Deny pour l'ajouter à la Rule List sur le côté droit. Vous pouvez modifier l'ordre des règles ou les supprimer en utilisant les boutons situés à droite du panneau de Rule List. L'ordre est important car pour un utilisateur et un appareil donné, les règles sont évaluées dans l'ordre indiqué. Dans le cas d'une correspondance à une règle de niveau élevé (près du haut de la liste), les règles se trouvant plus bas dans la liste n'auront pas d'effet. Par exemple, si vous possédez une règle qui autorise tous les iPad, et une règle suivante bloquant l'utilisateur « Matt », l'iPad de Matt sera autorisé car la règle « iPad » possède une priorité plus élevée que la règle « Matt ».
5. Pour effectuer une analyse des règles dans la liste de règles pour rechercher des remplacements, des conflits ou des constructions supplémentaires potentiels, cliquez sur Analyze.
6. Cliquez sur Save.

9. Configurez le Mobile Service Provider.
   Remarque : l'option Mobile Service Provider est facultative et uniquement nécessaire si XenMobile est également configuré pour utiliser l'interface Mobile Service Provider pour interroger les appareils non gérés.
   1. Sélectionnez l'onglet Configure > MSP.

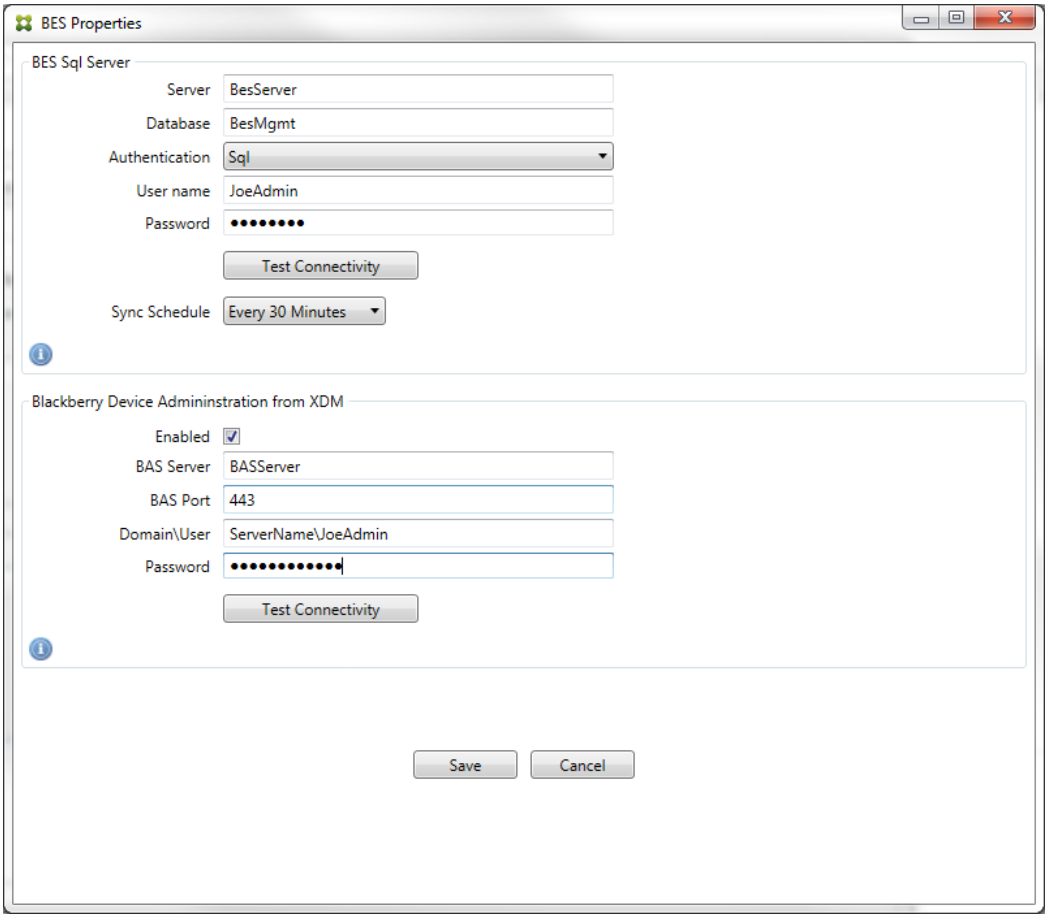
© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Définissez le type de transport de service sur HTTP ou HTTPS pour le service Mobile Service Provider service.
3. Définissez le port de service (généralement 80 ou 443) pour le service Fournisseur de services mobiles.
   Remarque : si vous utilisez le port 443, le port requiert un certificat SSL lié dans IIS.
4. Définissez le groupe ou l'utilisateur d'autorisation. Cela définit l'utilisateur ou l'ensemble des utilisateurs qui peuvent se connecter au service fournisseur de services mobiles XenMobile.
5. Paramétrer si les requêtes ActiveSync sont actives ou non.
   Remarque : si les requêtes ActiveSync sont activées pour le serveur XenMobile, le type de Snapshot pour un ou plusieurs serveurs Exchange doit être défini sur Deep ; cela peut avoir une influence significative sur les coûts des instantanés.
6. Par défaut, les appareils ActiveSync correspondants à l'expression régulière WorxMail.*ne seront pas envoyés à XenMobile. Pour changer ce comportement, vous pouvez modifier le champ Filter ActiveSync si nécessaire
   Remarque : s'il est laissé vide, cela signifie que tous les appareils seront transférés vers XenMobile.
7. Cliquez sur Save.

10. Si vous le souhaitez, vous pouvez configurer un ou plusieurs serveurs BlackBerry Enterprise Server (BES) :
    1. Cliquez sur Ajouter.
    2. Entrez le nom du serveur BES SQL.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Tapez le nom de la base de données de gestion BES.
4. Sélectionnez le mode Authentication. Si vous sélectionnez l'authentification intégrée Windows, le compte d'utilisateur du service XenMobile Mail Manager est le compte utilisé pour se connecter au serveur BES SQL.
   Remarque : si vous choisissez Windows Integrated pour la connexion à la base de données XenMobile Mail Manager, le compte Windows spécifié ici doit également pouvoir accéder à la base de données de XenMobile Mail Manager.
5. Si vous sélectionnez SQL authentication, entrez le nom d'utilisateur et le mot de passe.
6. Définissez Sync Schedule. Ceci est la planification utilisée pour se connecter au serveur BES SQL et rechercher toute mise à jour d'appareil.
7. Cliquez sur Test Connectivity pour vérifier la connectivité au serveur SQL.
   Remarque : si Windows Integrated est sélectionné, ce test utilise l'utilisateur actuellement connecté et non l'utilisateur du service XenMobile Mail Manager et par conséquent ne teste pas correctement l'authentification SQL.
8. Si vous souhaitez prendre en charge l'effacement à distance (Wipe) et/ou la réinitialisation du mot de passe (ResetPassword) d'appareils BlackBerry depuis XenMobile, cochez la case Enabled.
   1. Entrez le nom de domaine complet BES.
   2. Entrez le port BES utilisé par le service Web d'administration.
   3. Entrez le nom d'utilisateur complet et le mot de passe requis par le service BES.
   4. Cliquez sur Test Connectivity pour tester la connexion au serveur BES.
   5. Cliquez sur Enregistrer.

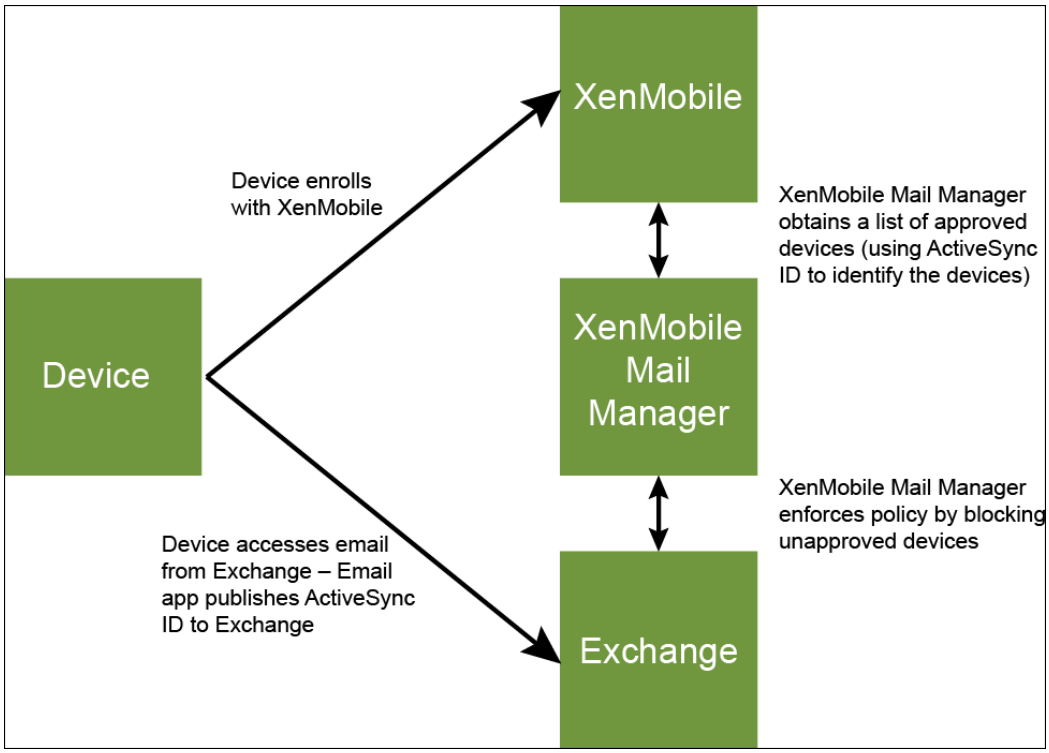
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Application des stratégies de messagerie avec des ID ActiveSync

Jul 25, 2016

Votre stratégie de messagerie d'entreprise peut refuser l'accès à la messagerie d'entreprise à certains appareils. Pour vous conformer à cette stratégie, vous devez vous assurer que les employés ne peuvent pas accéder à la messagerie d'entreprise à partir de tels appareils. XenMobile Mail Manager et XenMobile fonctionnent ensemble pour appliquer une telle stratégie de messagerie. XenMobile définit la stratégie d'accès à la messagerie d'entreprise, et lorsqu'un appareil non approuvé s'inscrit auprès de XenMobile, XenMobile Mail Manager applique la stratégie.

Le client de messagerie sur un appareil se fait connaître d'Exchange Server (ou Office 365) à l'aide de l'D d'appareil, également appelé ID ActiveSync, qui est utilisé pour identifier l'appareil de façon unique. Worx Home obtient un identificateur similaire et envoie l'identificateur à XenMobile lorsque l'appareil est inscrit. En comparant les ID des deux appareils, XenMobile Mail Manager peut déterminer si un appareil spécifique est autorisé à accéder à la messagerie d'entreprise. La figure suivante illustre ce concept :



Si XenMobile envoie un ID ActiveSync à XenMobile Mail Manager qui est différent de l'ID publié auprès de Exchange par l'appareil, XenMobile Mail Manager ne peut pas indiquer à Exchange l'action à exécuter avec l'appareil.

La correspondance des ID ActiveSync fonctionne de manière fiable sur la plupart des plates-formes ; cependant, Citrix a constaté que sur certaines implémentations Android, l'ID ActiveSync de l'appareil est différent de l'ID publié par le client de messagerie auprès d'Exchange. Pour pallier ce problème, vous pouvez effectuer les tâches suivantes :

- Sur la plate-forme Samsung SAFE, distribuez la configuration ActiveSync de l'appareil depuis XenMobile.
- Sur les autres plates-formes Android, distribuez l'application Touchdown et la configuration Touchdown ActiveSync

© 1999-2017 Citrix Systems, Inc. All rights reserved.

depuis XenMobile.

Cela n'empêche pas toutefois un employé d'installer un client de messagerie autre que Touchdown sur un appareil Android. Pour garantir que votre stratégie d'accès à la messagerie d'entreprise est appliquée correctement, vous pouvez adopter une approche de sécurité défensive et configurer XenMobile Mail Manager de manière à bloquer les e-mails en définissant la stratégie statique sur Deny by default. Cela signifie que si un employé configure un client de messagerie autre que Touchdown sur un appareil Android, et que la détection de l'ID ActiveSync ne fonctionne pas correctement, l'employé se voit refuser l'accès à la messagerie d'entreprise.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Règles de contrôle d'accès

Jul 25, 2016

XenMobile Mail Manager propose une approche basée sur des règles permettant de configurer dynamiquement le contrôle d'accès aux appareils Exchange ActiveSync. Une règle de contrôle d'accès à XenMobile Mail Manager se compose de deux parties : une expression correspondante et un état d'accès désiré (Autoriser ou Bloquer). Une règle doit être testée par rapport à un appareil ActiveSync Exchange donné pour déterminer si elle s'applique à l'appareil ou correspond à ce dernier. Il existe plusieurs types d'expressions correspondantes ; une règle peut, par exemple, correspondre à tous les appareils d'un type d'appareil donné ou à un ID d'appareil ActiveSync Exchange spécifique, ou encore à tous les appareils d'un utilisateur spécifique, etc.

À tout moment lors de l'ajout, la suppression et la réorganisation de règles dans la liste, si vous cliquez sur le bouton Cancel, l'état dans lequel se trouvait la liste lors de la première ouverture est rétabli. Si vous fermez l'outil de configuration sans cliquer sur Save, les modifications apportées sur cette fenêtre seront perdues.

XenMobile Mail Manager propose trois types de règles : les règles locales, les règles XDM, et la règle d'accès par défaut.

Local rules (Règles locales) : les règles locales ont la priorité la plus élevée : si un appareil est identifié par une règle locale, l'évaluation de la règle ne s'applique pas. Ni les règles XDM ni la règle d'accès par défaut ne seront consultées. Les règles locales se configurent localement sur XenMobile Mail Manager via l'onglet Configure/Access Rules/Local Rules. La prise en charge de correspondance se base sur l'appartenance des utilisateurs à un groupe Active Directory donné. La prise en charge de correspondance se base sur des expressions régulières pour les champs suivants :

- Active Sync Device ID
- ActiveSync Device Type
- User Principal Name (UPN)
- ActiveSync User Agent (généralement la plate-forme de l'appareil ou le client de messagerie)

Si un instantané principal a été effectué et qu'il a trouvé des appareils, vous pouvez ajouter une règle d'expressions normales ou régulières. Si aucun instantané principal n'a été effectué, vous pouvez uniquement ajouter des règles d'expressions régulières.

XDM rules (Règles XDM) : les règles XDM sont des références à un serveur XenMobile externe qui fournit des règles aux appareils gérés. Le serveur XenMobile peut être configuré avec ses propres règles de haut niveau qui identifient les appareils à autoriser ou à bloquer en fonction des propriétés connues par XenMobile, par exemple si l'appareil est jailbreaké ou s'il contient des applications interdites. XenMobile évalue les règles de haut niveau et génère un ensemble d'ID d'appareils ActiveSync autorisés ou bloqués, qui sont ensuite envoyés à XenMobile Mail Manager.

Default access rule (Règle d'accès par défaut) : la règle d'accès par défaut est unique car elle peut potentiellement s'appliquer à tous les appareils et elle est toujours évaluée en dernier. C'est la règle passe-partout, ce qui signifie que si un appareil donné ne correspond pas à une règle locale ou XDM, l'état d'accès souhaité de l'appareil est déterminé par l'état d'accès souhaité de la règle d'accès par défaut.

- Default Access – Allow (Accès par défaut - Autoriser). Tout appareil ne correspondant pas à une règle locale ou XDM sera autorisé.
- Default Access – Block (Accès par défaut - Bloquer). Tout appareil ne correspondant pas à une règle locale ou XDM sera bloqué.
- Default Access - Unchanged (Accès par défaut - Inchangé). L'état d'accès de tout appareil non associé à une règle locale ou XDM ne pourra pas être modifié par XenMobile Mail Manager. Si un appareil a été placé en quarantaine par Exchange,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

aucune action n'est prise ; par exemple, la seule manière de retirer un appareil en quarantaine est de posséder une règle locale ou XDM qui outrepasse explicitement la quarantaine.

À propos des évaluations de règles

Pour chaque appareil pour lequel Exchange remet des rapports à XenMobile Mail Manager, les règles sont évaluées dans l'ordre, de la priorité la plus élevée à la plus faible, comme suit :

- Règles locales
- Règle d'accès par défaut
- Règles XDM

Lorsqu'une correspondance est trouvée, l'évaluation s'arrête. Par exemple, si un appareil correspond à une règle locale, l'appareil ne sera pas évalué par rapport aux règles XDM ou à la règle d'accès par défaut. Cela reste aussi vrai pour un type de règle donné. Par exemple, s'il existe plus d'une correspondance pour un appareil donné dans la liste des règles locales, l'évaluation s'arrête dès la première correspondance.

XenMobile Mail Manager réévalue l'ensemble des règles déjà définies lorsque les propriétés d'un appareil sont modifiées, lorsque des appareils sont ajoutés ou supprimés ou lorsque les règles sont modifiées. Les instantanés principaux détectent la suppression d'appareils ainsi que les modifications apportées à leurs propriétés à intervalles configurables. Les instantanés secondaires détectent les nouveaux appareils à intervalles configurables.

Exchange ActiveSync possède aussi des règles régissant l'accès. Il est important de bien comprendre la façon dont ces règles fonctionnent dans l'environnement XenMobile Mail Manager. Exchange peut être configuré avec trois niveaux de règles : les exemptions personnelles, les règles d'appareil et les paramètres d'organisation. XenMobile Mail Manager automatise le contrôle d'accès en envoyant des requêtes PowerShell à distance via un programme pour modifier la liste des exemptions personnelles. Il s'agit de listes d'ID d'appareils Exchange ActiveSync autorisés ou bloqués associés à une boîte aux lettres donnée. Lorsqu'il est déployé, XenMobile Mail Manager prend en charge la gestion des listes d'exemptions dans Exchange. Pour plus d'informations, consultez cet article Microsoft.

L'analyse est particulièrement utile dans les situations dans lesquelles plusieurs règles ont été définies pour le même champ. Vous pouvez résoudre les relations entre les règles. Vous pouvez effectuer des analyses depuis la perspective des champs de règle ; par exemple, les règles sont analysées par groupes en fonction du champ remplissant la condition, tel que ActiveSync device ID, ActiveSync device type, User, User Agent, et ainsi de suite.

Terminologie relative aux règles :

- **Règle absolue**. Une substitution se produit lorsque plusieurs règles s'appliquent à un même appareil. Étant donné que les règles sont évaluées par priorité dans la liste, la ou les dernières instances de règle devant s'appliquer peuvent ne jamais être évaluées.
- **Règle conflictuelle**. Un conflit survient quand plusieurs règles s'appliquent à un même appareil et que l'accès (Autoriser/Bloquer) ne correspond pas. Si les règles conflictuelles ne sont pas des expressions régulières, un conflit se traduit toujours implicitement par une substitution.
- **Règle complémentaire**. Un complément a lieu lorsque plusieurs règles sont des expressions régulières et par conséquent, il peut s'avérer nécessaire de vérifier que les deux expressions régulières (ou plus) peuvent être combinées en une seule expression ou qu'il n'y ait pas duplication de fonctionnalités. Une règle complémentaire peut également causer des problèmes de conflit d'accès (Autoriser/Bloquer).
- **Règle principale**. La règle principale est la règle sur laquelle l'utilisateur a cliqué dans la boîte de dialogue. La règle est indiquée visuellement par une bordure. La règle aura également une ou deux flèches vertes pointant vers le haut ou vers le bas. Si une flèche pointe vers le haut, cela indique qu'il existe des règles secondaires qui précèdent la règle principale. Si

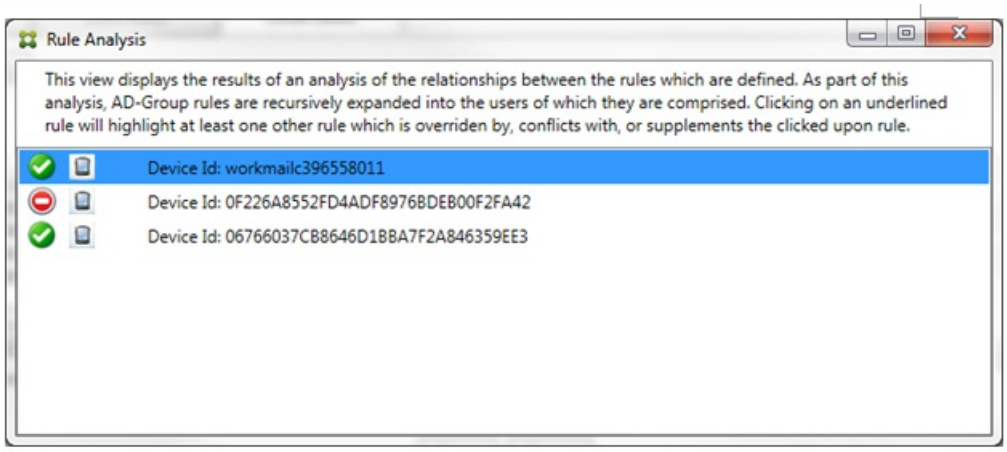
© 1999-2017 Citrix Systems, Inc. All rights reserved.

une flèche pointe vers le bas, cela indique qu'il existe des règles secondaires qui s'appliquent après la règle principale. Seule une règle principale peut être active à tout moment.

- **Règle secondaire**. Une règle secondaire est liée d'une certaine manière à la règle principale que ce soit via une relation de remplacement, de conflit ou supplémentaire. Les règles sont indiquées visuellement par une bordure en pointillés. Pour chaque règle principale, il peut y avoir une ou plusieurs règles secondaires. Lorsque vous cliquez sur une entrée soulignée, la ou les règles secondaires sélectionnées le sont toujours du point de vue de la règle principale. Par exemple, la règle secondaire sera remplacée par la règle principale et/ou la règle secondaire entrera en conflit avec la règle principale et/ou la règle secondaire complétera la règle principale.

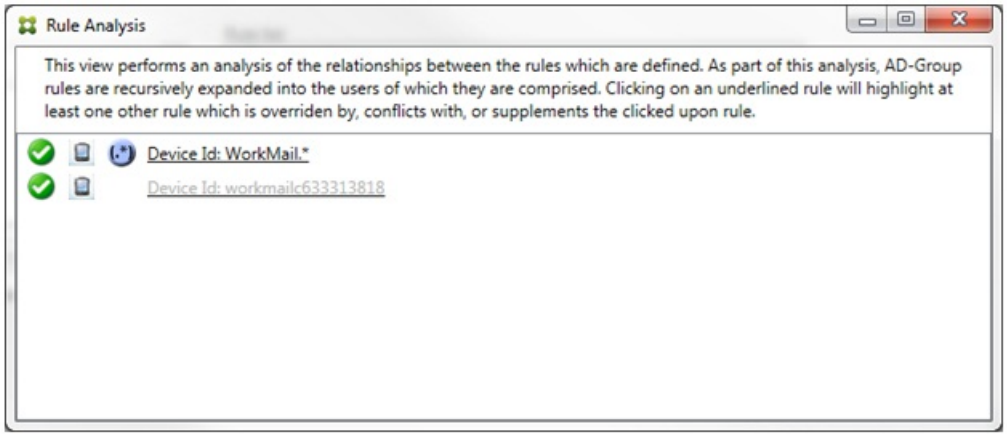
Apparence des types de règles dans la boîte de dialogue d'analyse des règles

Lorsqu'il n'y a aucun conflit, remplacement, ou complément, il n'y a pas d'entrées soulignées dans la boite de dialogue Rule Analysis. Par exemple, cliquer sur des éléments n'a pas d'impact, les éléments normaux sélectionnés seront mis en évidence.

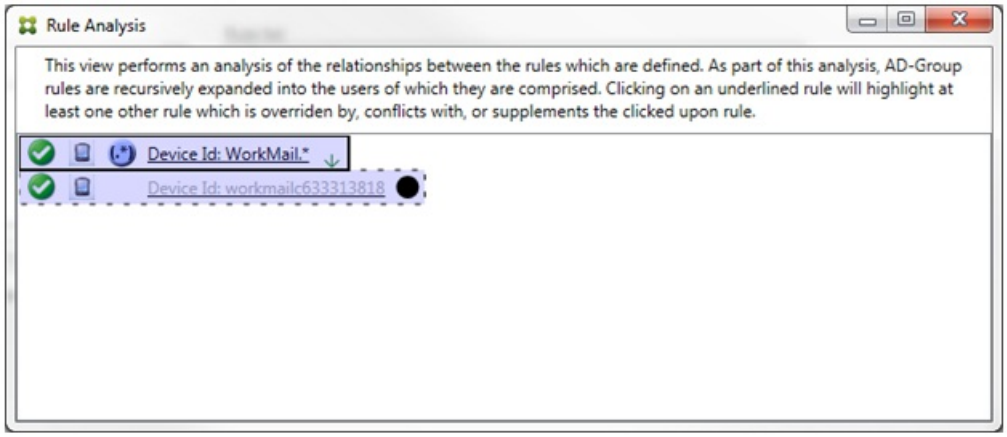


Lorsqu'une substitution se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Au moins une règle secondaire s'affichera dans une police plus claire pour indiquer que la règle a été remplacée par une règle de priorité plus élevée. Vous pouvez cliquer sur les règles remplacées pour déterminer la ou les règles qui ont remplacé la règle. Lorsqu'une règle remplacée a été soulignée que ce soit parce que la règle est une règle principale ou secondaire, un cercle noir apparaît à côté en guise d'indication visuelle signifiant que la règle est inactive. Par exemple, avant de cliquer sur la règle, la boîte de dialogue se présente comme suit :

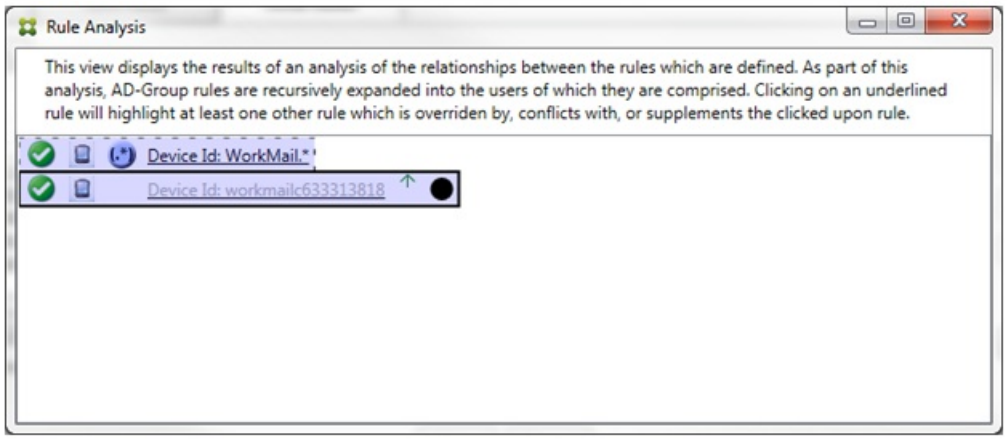
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Lorsque vous cliquez sur la règle prioritaire, la boîte de dialogue se présente comme suit :



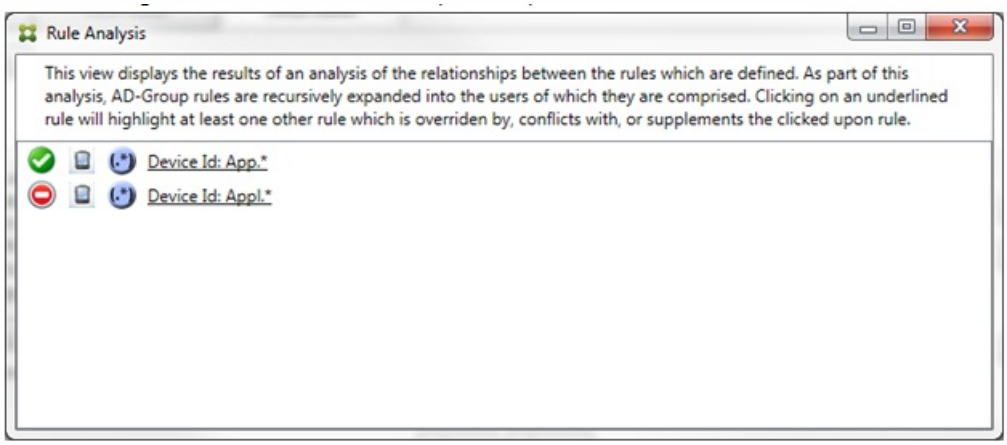
Dans cet exemple, la règle d'expression régulière WorkMail.* est la règle principale (indiquée par une bordure pleine) et la règle normale workmailc633313818 est une règle secondaire (indiquée par une bordure en pointillés). Le point noir à côté de la règle secondaire est une indication visuelle qui signifie que la règle est inactive (ne sera jamais évaluée) en raison de la règle d'expression régulière prioritaire. Après avoir cliqué sur la règle remplacée, la boîte de dialogue se présente comme suit :



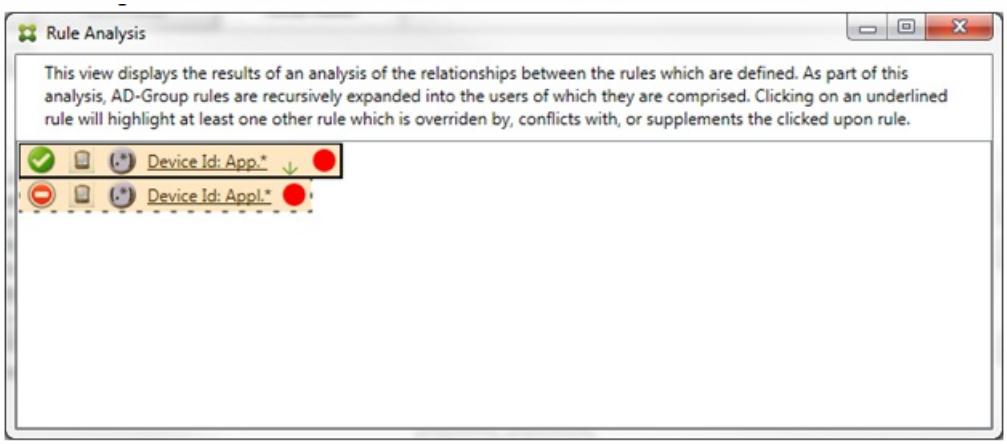
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans l'exemple précédent, la règle d'expression régulière WorkMail.* est la règle secondaire (indiquée par une bordure en pointillés) et la règle normale workmailc633313818 est une règle principale (indiquée par une bordure pleine). Pour cet exemple simple, il n'y a pas grande différence. Pour un exemple plus compliqué, consultez l'exemple d'expression complexe plus en avant dans cette rubrique. Dans un scénario avec de nombreuses règles définies, cliquer sur la règle remplacée permet d'identifier rapidement par quelles règles elle a été remplacée.

Lorsqu'un conflit se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Les règles en conflit sont indiquées par un point rouge. Le cas de règles qui entrent seulement en conflit avec une autre règle est uniquement possible avec deux ou plusieurs règles d'expressions régulières définies. Dans tous les autres cas de conflit, il y aura non seulement un conflit, mais aussi un remplacement. Avant de cliquer sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :



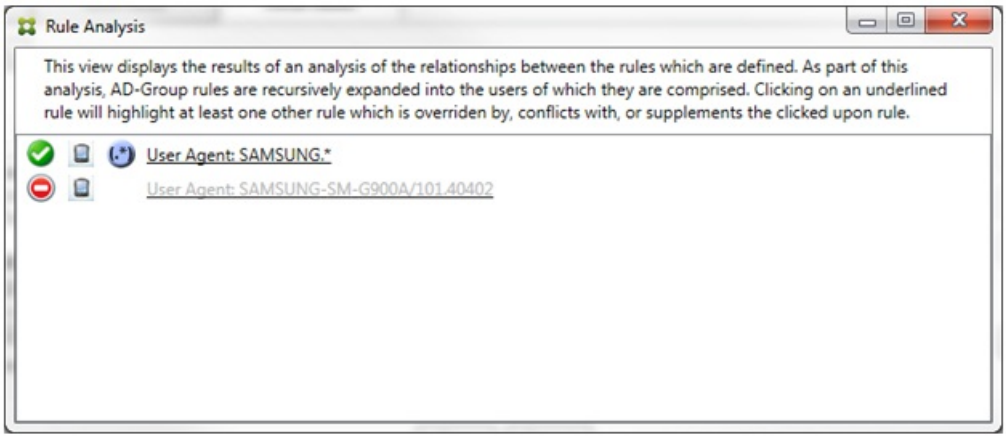
En inspectant les deux règles d'expressions régulières, il est évident que la première règle autorise tous les appareils avec un ID d'appareil contenant « App » et que la deuxième règle refuse tous les appareils avec un ID d'appareil contenant « Appl ». En outre, même si la deuxième règle refuse tous les appareils avec un ID d'appareil contenant « Appl », aucun appareil correspondant à ces critères ne verra son accès refusé en raison de la priorité plus élevée de la règle l'y autorisant. Après avoir cliqué sur la première règle, la boîte de dialogue se présente comme suit :



© 1999-2017 Citrix Systems, Inc. All rights reserved.

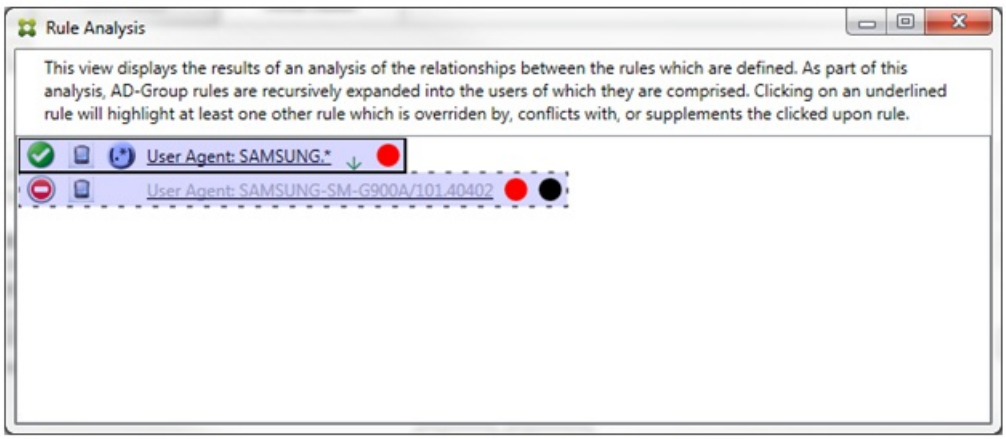
Dans le cas précédent, la règle principale (règle d'expression régulière App.*) et la règle secondaire (règle d'expression régulière Appl.*) sont toutes deux affichées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.

Dans un cas regroupant un conflit et un remplacement, la règle principale (règle d'expression régulière App.*) et la règle secondaire (règle d'expression régulière Appl.*) sont surlignées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière à un même champ de correspondance, ce qui peut entraîner un problème de redondance ou quelque chose de plus sérieux.



Il est facile de voir dans l'exemple précédent que la première règle (règle d'expression régulière SAMSUNG.*) ne remplace pas seulement la règle suivante (règle normale SAMSUNG-SM-G900A/101.40402), mais que l'accès des deux règles est différent (la règle principale indique Autoriser, la règle secondaire indique Bloquer). La deuxième règle (règle normale SAMSUNG-SM-G900A/101.40402) est affichée dans une police plus claire pour indiquer qu'elle a été remplacée et qu'elle n'est donc pas active.

Après avoir cliqué sur la règle d'expression régulière, la boîte de dialogue se présente comme suit :

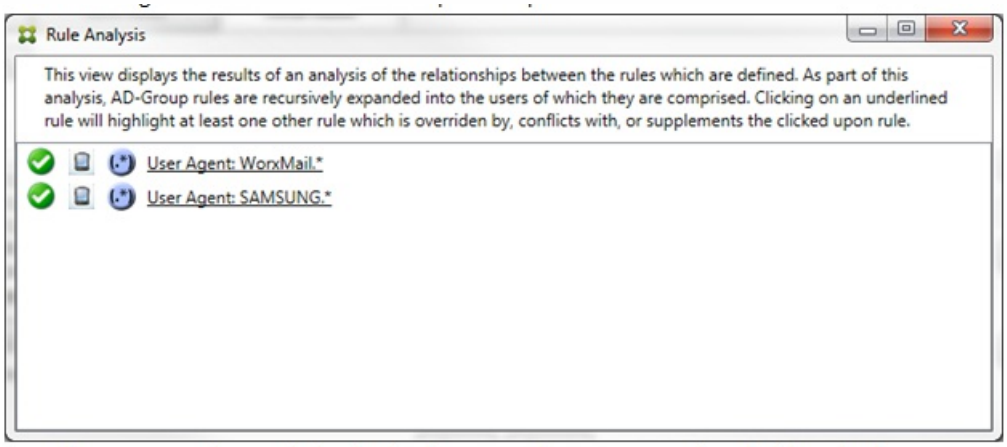


La règle principale (règle d'expression régulière SAMSUNG.*) est suivie d'un point rouge indiquant qu'elle entre en conflit avec

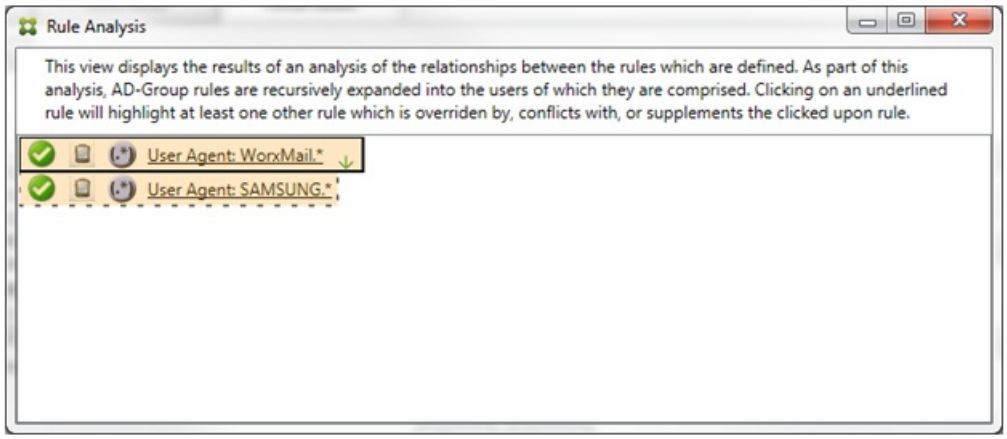
© 1999-2017 Citrix Systems, Inc. All rights reserved.

une ou plusieurs règles secondaires. La règle secondaire (règle normale SAMSUNG-SM-G900A/101.40402) est suivie d'un point rouge indiquant qu'elle entre en conflit avec la règle principale, ainsi que d'un point noir indiquant qu'elle a été remplacée et n'est donc pas active.

Au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Les règles qui se complètent uniquement entre elles n'impliquent que des règles d'expressions régulières. Lorsque des règles se complètent entre elles, elles sont surlignées en jaune. Avant de cliquer sur des règles dans un exemple simple, la boîte de dialogue se présente comme suit :



L'inspection visuelle révèle facilement que les deux règles sont des règles d'expressions régulières qui s'appliquent toutes les deux au champ ActiveSync device ID dans XenMobile Mail Manager. Après avoir cliqué sur la première règle, la boîte de dialogue se présente comme suit :

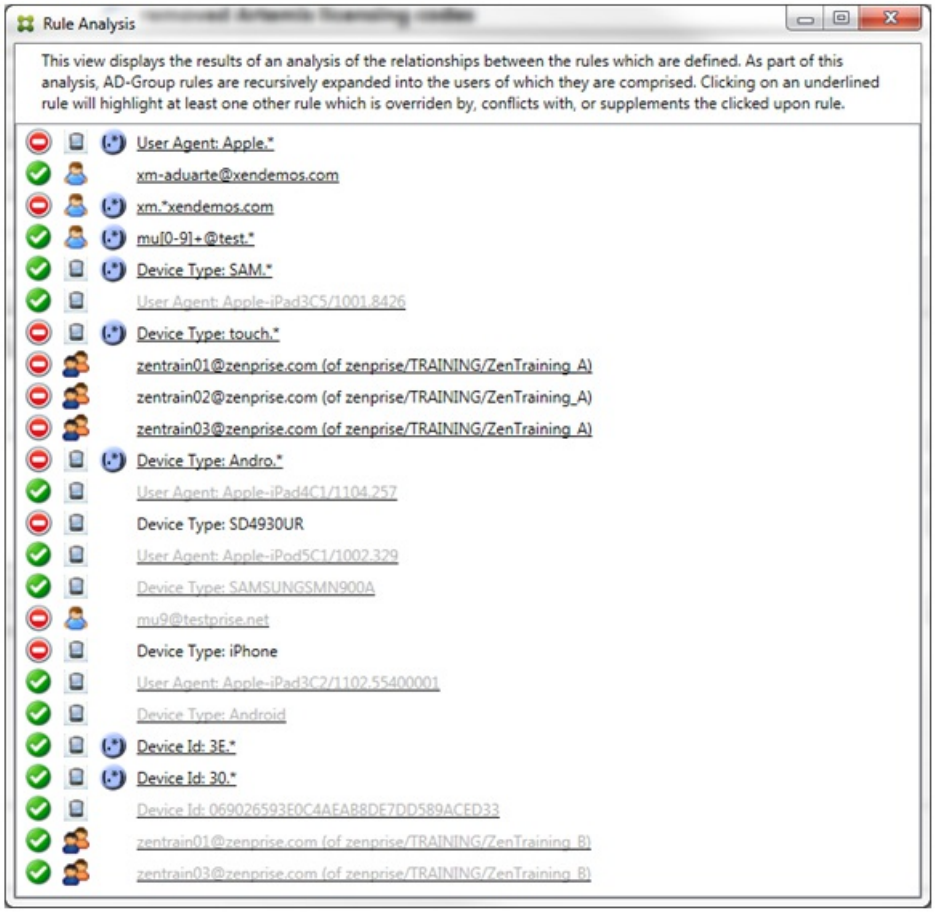


La règle principale (règle d'expression régulière WorxMail.*) est surlignée en jaune pour indiquer qu'il existe au moins une autre règle secondaire qui est une expression régulière. La règle secondaire (règle d'expression régulière SAMSUNG.*) est surlignée en jaune pour indiquer que celle-ci et la règle principale sont des règles d'expressions régulières qui s'appliquent à un même champ dans XenMobile Mail Manager ; dans ce cas, le champ ActiveSync device ID. Les expressions régulières peuvent ou non se chevaucher. C'est à vous de décider si vos expressions régulières sont correctement conçues.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemple d'expression complexe

De nombreux remplacements, conflits ou compléments sont susceptibles de se produire, c'est pourquoi il est impossible de fournir des exemples couvrant tous les scénarios envisageables. L'exemple suivant explique ce qu'il ne faut pas faire, et sert aussi à illustrer toute la portée de la présentation visuelle de l'analyse des règles. La plupart des éléments sont soulignés dans la figure ci-après. Plusieurs des éléments s'affichent dans une police plus claire, ce qui indique que la règle en question a été remplacée par une règle dont la priorité est plus élevée. Un certain nombre de règles d'expressions régulières sont incluses dans la liste, comme l'indique l'icône (.*).

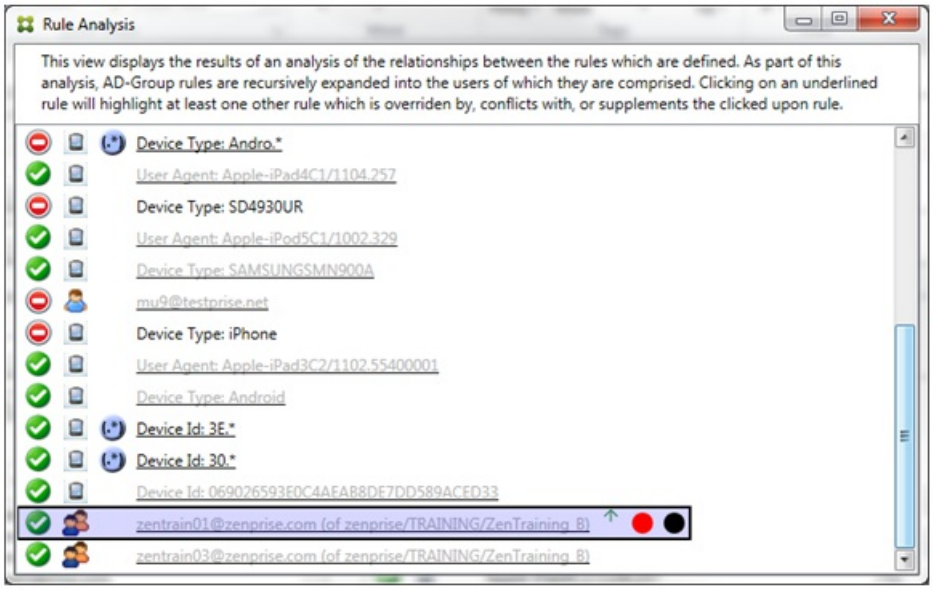


Comment analyser un remplacement

Pour afficher la ou les règles qui ont remplacé une règle particulière, cliquez sur cette dernière.

Exemple 1 : cet exemple explique pourquoi zentrain01@zenprise.com a été remplacée.

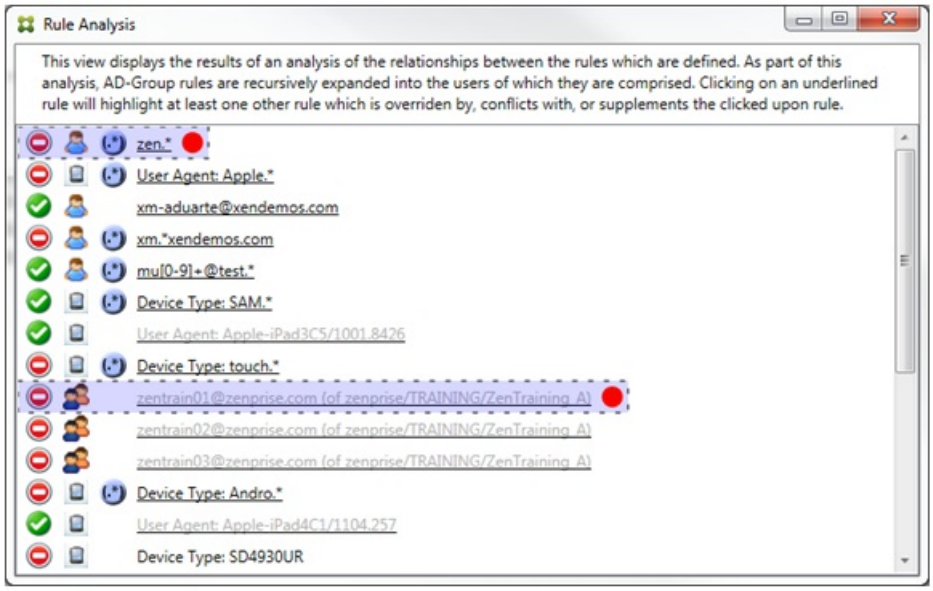
© 1999-2017 Citrix Systems, Inc. All rights reserved.



La règle principale (règle de groupe AD zenprise/TRAINING/ZenTraining B, dont zentrain01@zenprise.com est un membre) présente les caractéristiques suivantes :

- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire ou l'ensemble des règles se trouvent au-dessus).
- Est suivie d'un cercle rouge et d'un cercle noir pour indiquer respectivement qu'une ou plusieurs règles secondaires sont en conflit et que la règle principale a été remplacée et n'est donc pas active.

Si vous faites défiler vers le haut, vous pouvez voir ce qui suit :

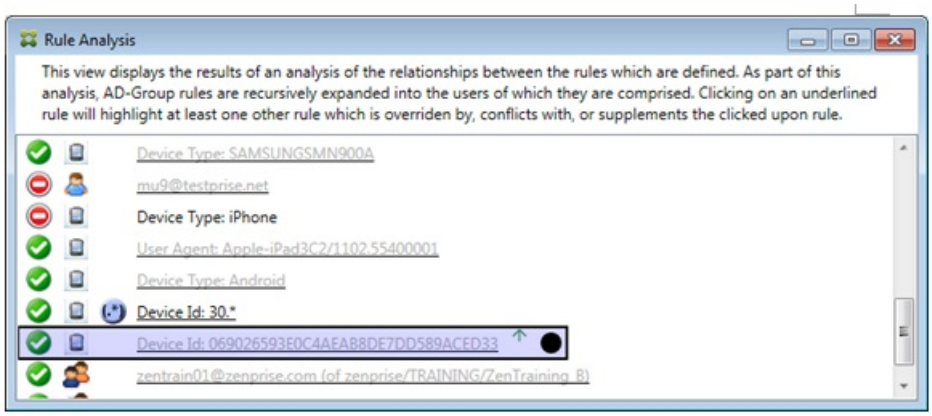


Dans ce cas, il existe deux règles secondaires qui remplacent la règle principale : la règle d'expression régulière zen.* et la règle normale zentrain01@zenprise.com (de zenprise/TRAINING/ZenTraining A). Dans le cas de la dernière règle secondaire,

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

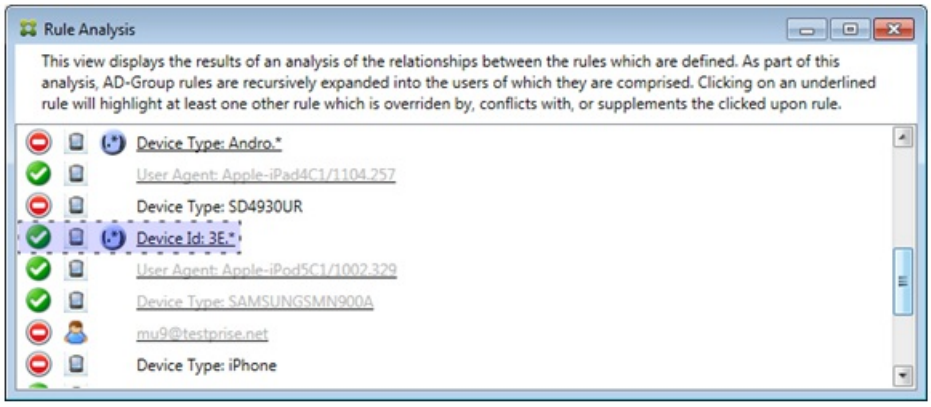
la règle de groupe Active Directory ZenTraining A contient l'utilisateur zentrain01@zenprise.com et la règle de groupe Active Directory ZenTraining B contient aussi l'utilisateur zentrain01@zenprise.com. Toutefois, étant donné que la règle secondaire a une priorité plus élevée que la règle principale, la règle principale a été remplacée. L'accès à la règle principale est Autoriser. Et comme l'accès des deux règles secondaires est Bloquer, toutes sont suivies d'un cercle rouge indiquant un conflit d'accès.

Exemple 2 : cet exemple illustre la raison pour laquelle l'appareil avec l'ID d'appareil ActiveSync 069026593E0C4AEAB8DE7DD589ACED33 a été remplacé :



La règle principale (règle d'ID d'appareil normale 069026593E0C4AEAB8DE7DD589ACED33) présente les caractéristiques suivantes :

- Est surlignée en bleu et encadrée par une bordure pleine.
- A une flèche verte pointant vers le haut (pour indiquer que la règle secondaire doit se trouver au-dessus).
- Est suivie par un cercle noir indiquant qu'une règle secondaire a remplacé la règle principale et que la règle est par conséquent inactive.



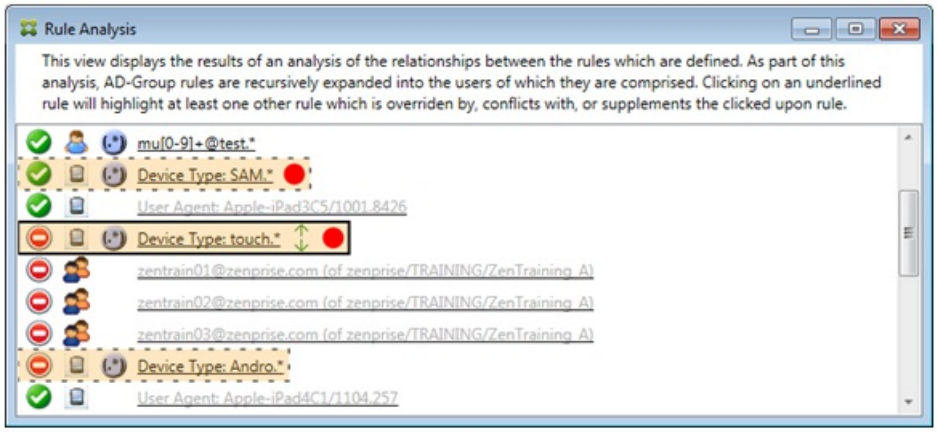
Dans ce cas, une seule règle secondaire remplace la règle principale : la règle d'expression régulière d'ID d'appareil ActiveSync 3E.* Comme l'expression régulière 3E.* correspond à 069026593E0C4AEAB8DE7DD589ACED33, la règle ne sera jamais évaluée.

Comment analyser un supplément et un conflit

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dans ce cas, la règle principale est la règle d'expression régulière ActiveSync Device Type touch.* Les caractéristiques sont les suivantes :

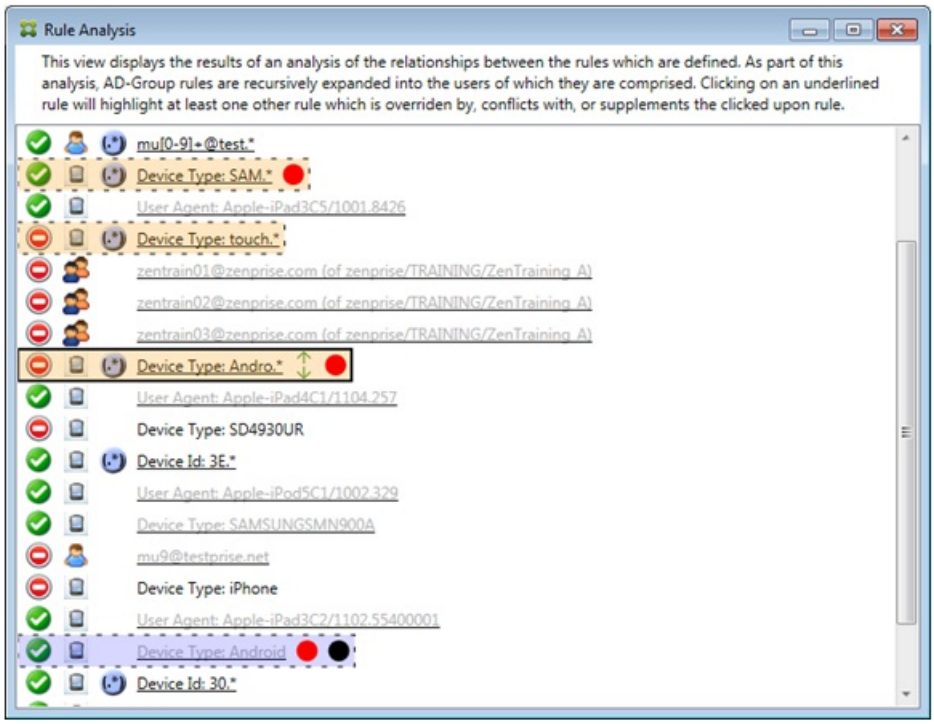
- Est signalée par une bordure pleine et surlignée en jaune indiquant qu'il y a plus d'une seule règle d'expression régulière appelant le même champ de règle, dans ce cas, ActiveSync device type.
- Deux flèches pointant vers le haut et vers le bas, ce qui indique qu'il existe au moins une règle secondaire avec une priorité plus élevée et au moins une règle secondaire avec une priorité inférieure.
- Le cercle rouge à côté indique qu'au moins une règle secondaire a son accès défini sur Autoriser ce qui entre en conflit avec l'accès de la règle principale qui est défini sur Bloquer.
- Il existe deux règles secondaires : la règle d'expression régulière ActiveSync Device Type SAM.*et la règle d'expression régulière ActiveSync Device Type Andro.*
- Les deux règles secondaires sont encadrées par des pointillés pour indiquer qu'elles sont secondaires.
- Les règles secondaires sont surlignées en jaune pour indiquer qu'elles s'appliquent en complément du champ de la règle ActiveSync Device Type.
- Vous devez vous assurer dans de tels scénarios que leurs règles d'expressions régulières ne sont pas redondantes.



Comment améliorer l'analyse des règles

Cet exemple explique pourquoi les relations entre les règles sont toujours abordées du point de vue de la règle principale. L'exemple précédent a montré comment un clic sur la règle d'expression régulière s'appliquait au champ de règle Device Type avec la valeur touch.* En cliquant sur la règle secondaire Andro.* vous mettrez en avant un autre ensemble de règles secondaires.

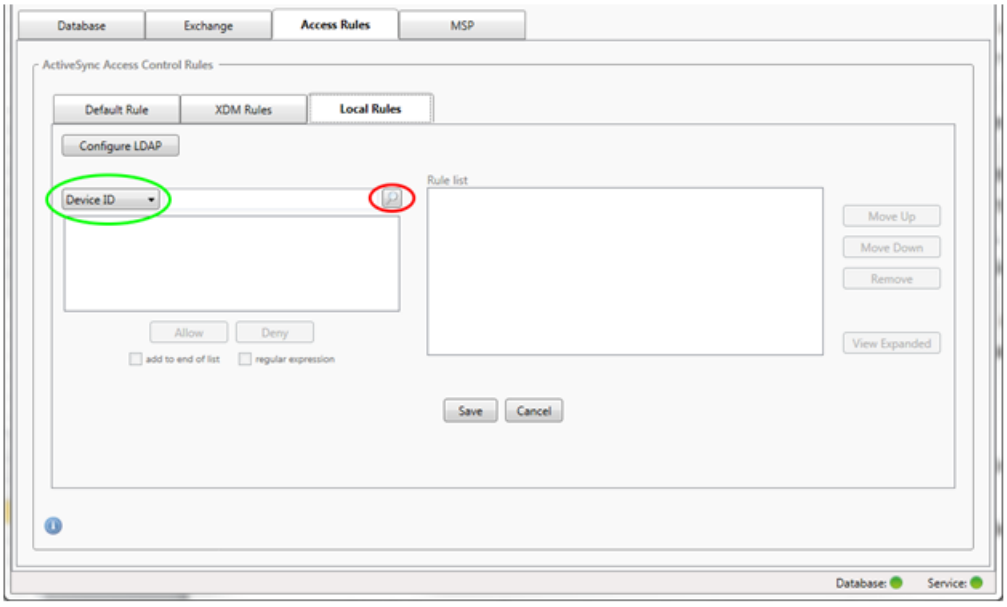
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Cet exemple présente une règle remplacée qui est inclue dans la relation de règle. Cette règle est la règle Android ActiveSync Device Type normale, qui est remplacée (indiquée par une police plus claire et un cercle noir à côté) et qui entre également en conflit avec la règle d'expression régulière principale ActiveSync Device Type Andro.* ; avant d'avoir été cliquée, cette règle était une règle secondaire. Dans l'exemple précédent, la règle Android ActiveSync Device Type normale n'était pas affichée en tant que règle secondaire, car du point de vue de la règle principale (règle d'expression régulière ActiveSync Device Type touch.*), elle n'était pas liée.

Pour configurer une règle locale d'expression normale

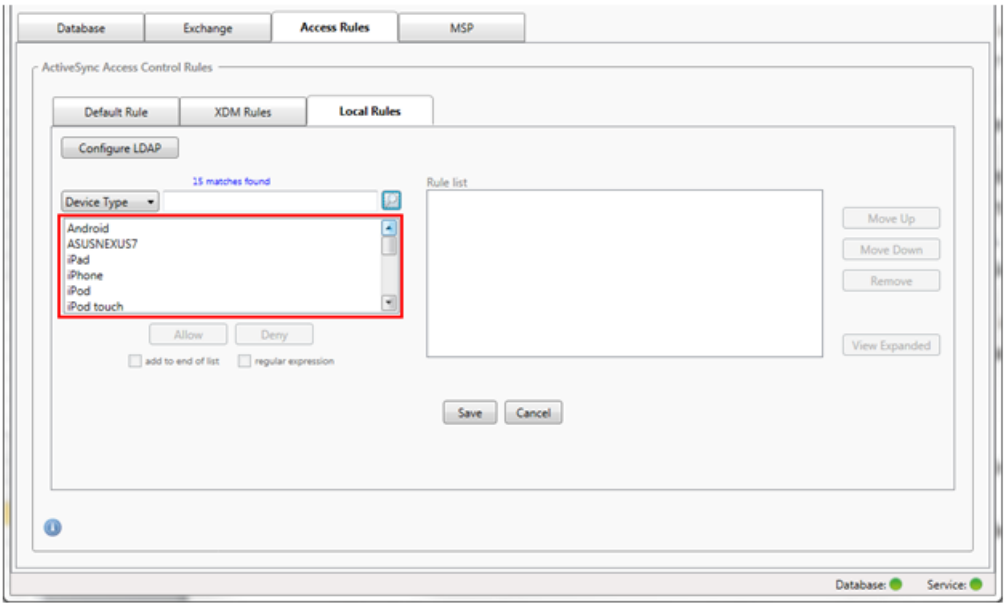
1. Cliquez sur l'onglet Access Rules.



2. Dans la listeDevice ID, sélectionnez le champ pour lequel vous souhaitez créer une règle locale.

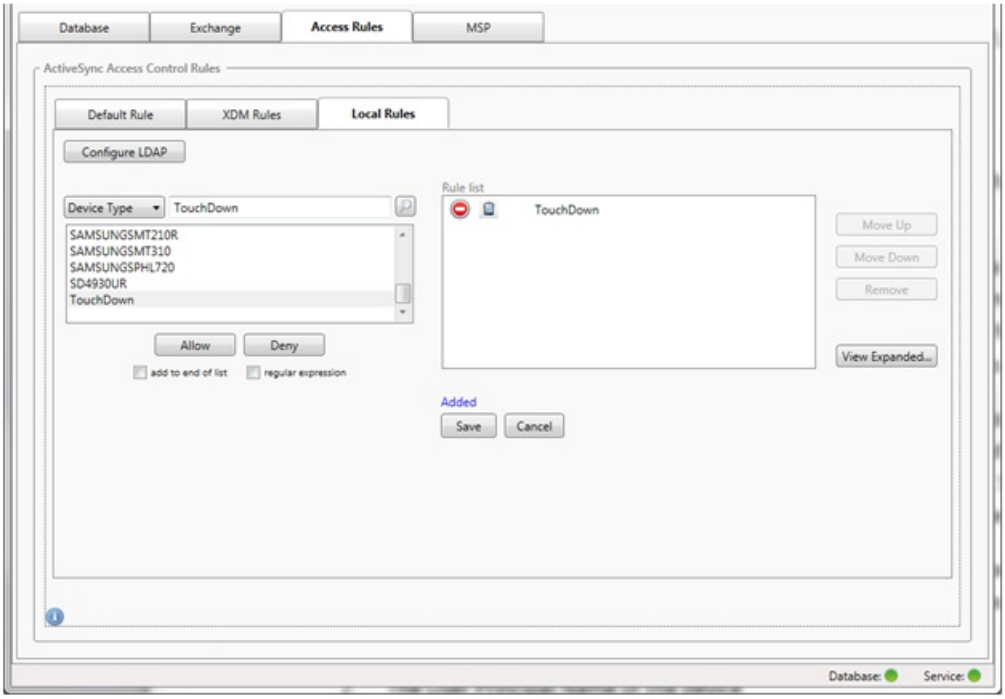
© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ Device Type a été choisi et les choix sont affichés ci-dessous dans la zone de liste.



4. Cliquez sur un des éléments dans la liste des résultats et cliquez sur l'une des options suivantes :
   - Allow signifie qu'Exchange sera configuré pour permettre le trafic ActiveSync pour tous les appareils correspondant.
   - Deny signifie que Exchange sera configuré de manière à refuser le trafic ActiveSync de tous les appareils correspondant.

   Dans cet exemple, les appareils dont le type est TouchDown se voient refuser l'accès.



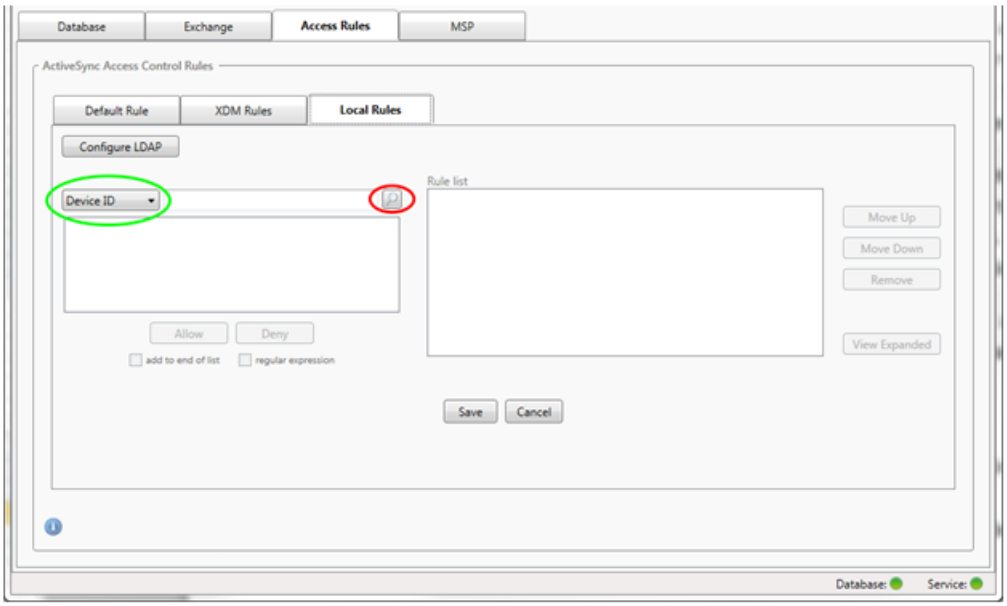
Pour ajouter une expression régulière

© 1999-2017 Citrix Systems, Inc. All rights reserved.

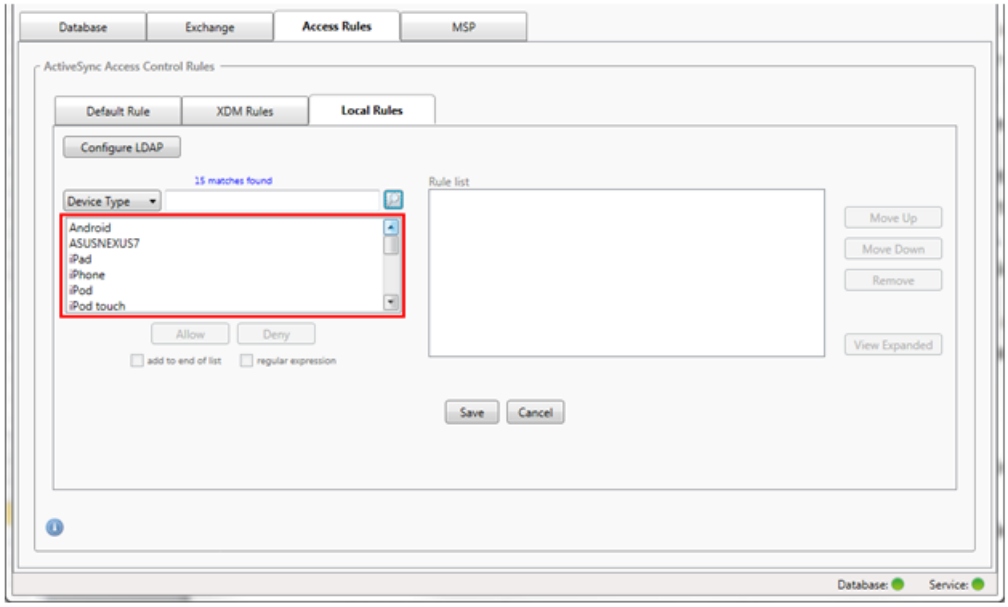
Les règles locales d'expressions régulières peuvent être différenciées par l'icône qui s'affiche à leur côté -  . Pour ajouter une règle d'expression régulière, vous pouvez créer une règle d'expression régulière à partir d'une valeur existante dans la liste des résultats pour un champ donné (si un instantané principal a été effectué), ou vous pouvez simplement saisir l'expression régulière que vous souhaitez.

Pour créer une expression régulière à partir d'une valeur de champ existant

1. Cliquez sur l'onglet Access Rules.

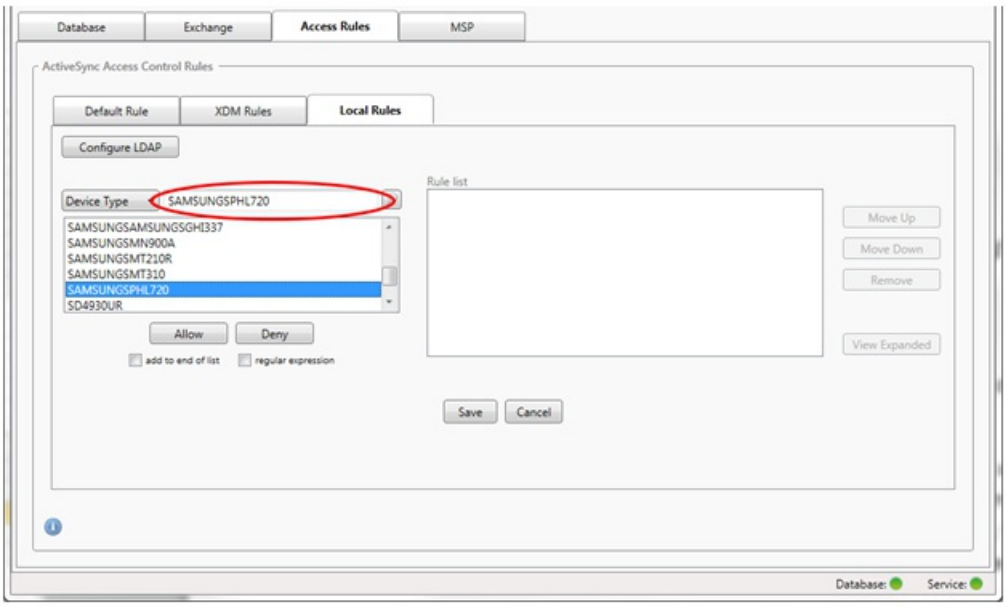


2. Dans la listeDevice ID, sélectionnez le champ pour lequel vous souhaitez créer une règle d'expression régulière locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ Device Type a été choisi et les choix sont affichés ci-dessous dans la zone de liste.

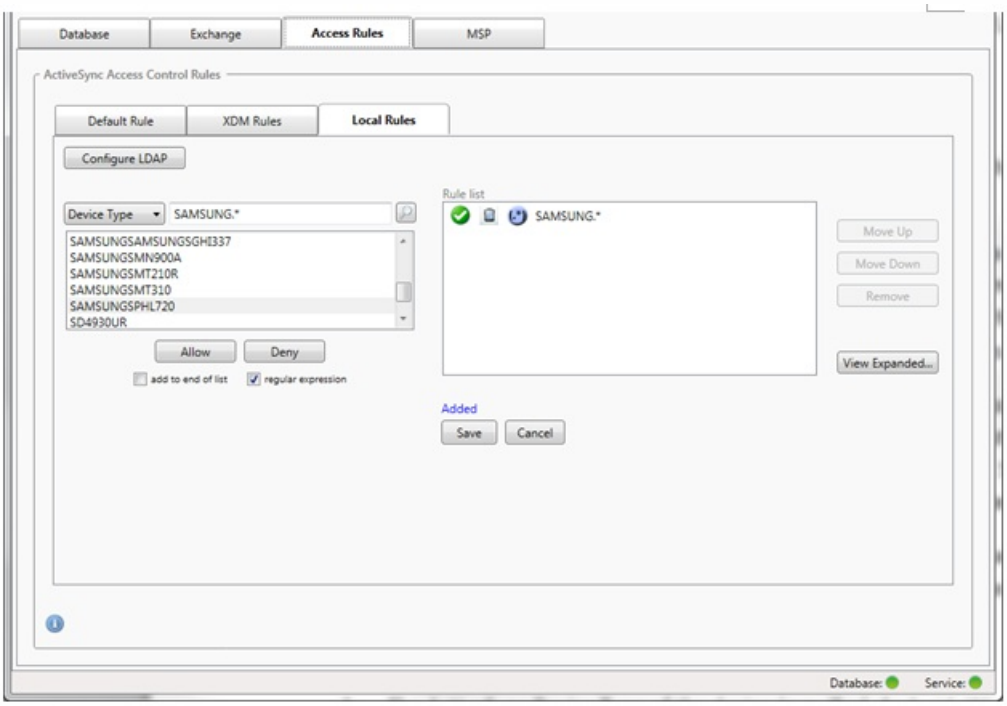


4. Cliquez sur un des éléments dans la liste des résultats. Dans cet exemple, SAMSUNGSPHL720 a été sélectionné et s'affiche dans la zone de texte adjacente à Device Type.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



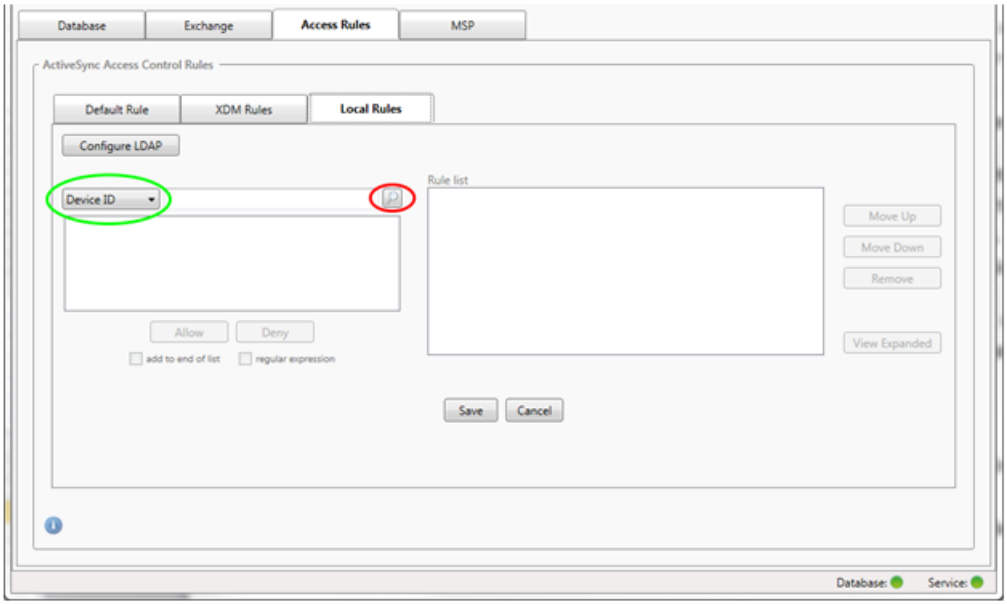
5. Pour autoriser tous les types d'appareils qui ont « Samsung » dans leur valeur Device Type, ajoutez une règle d'expression régulière en suivant les étapes suivantes :
   1. Cliquez dans la zone de texte de l'élément sélectionné.
   2. Modifiez le texte SAMSUNGSPHL720 par SAMSUNG.*
   3. Vérifiez que la case regular expression est cochée.
   4. Cliquez sur Allow.



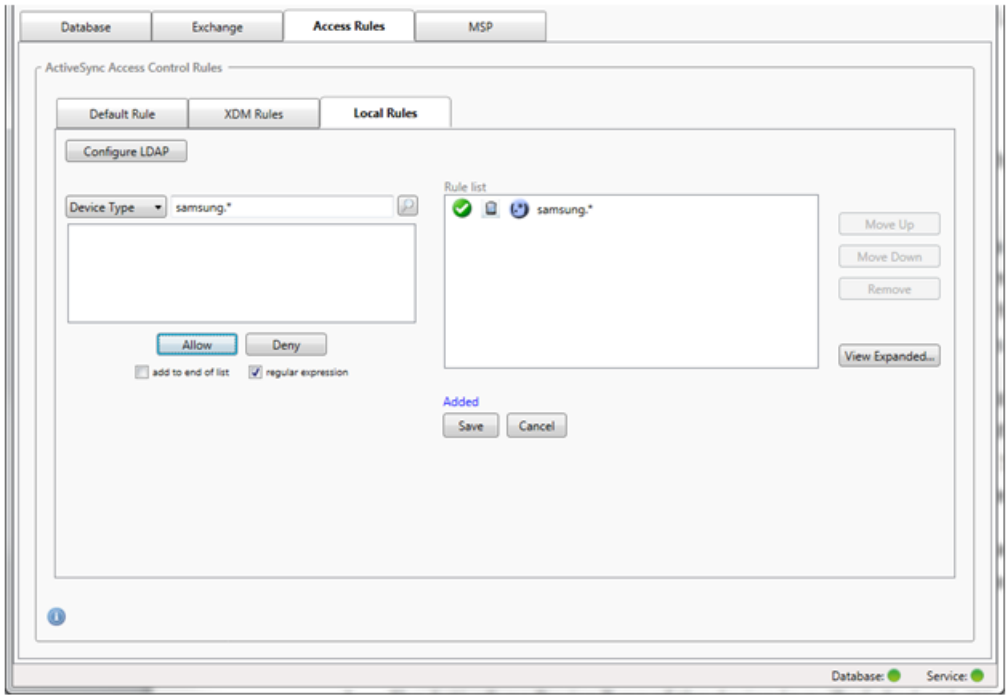
Pour créer une règle d'accès

1. Cliquez sur l'onglet Local Rules.
2. Pour entrer l'expression régulière, vous devez utiliser la liste Device ID et la zone de texte de l'élément sélectionné.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Sélectionnez le champ que vous voulez mettre en correspondance. Cet exemple utilise Device Type.
4. Entrez l'expression régulière. Cet exemple utilisesamsung.*
5. Assurez-vous que la case regular expression est cochée et cliquez sur Allow ou Deny. Dans cet exemple, le choix est Allow si bien que le résultat final est le suivant :

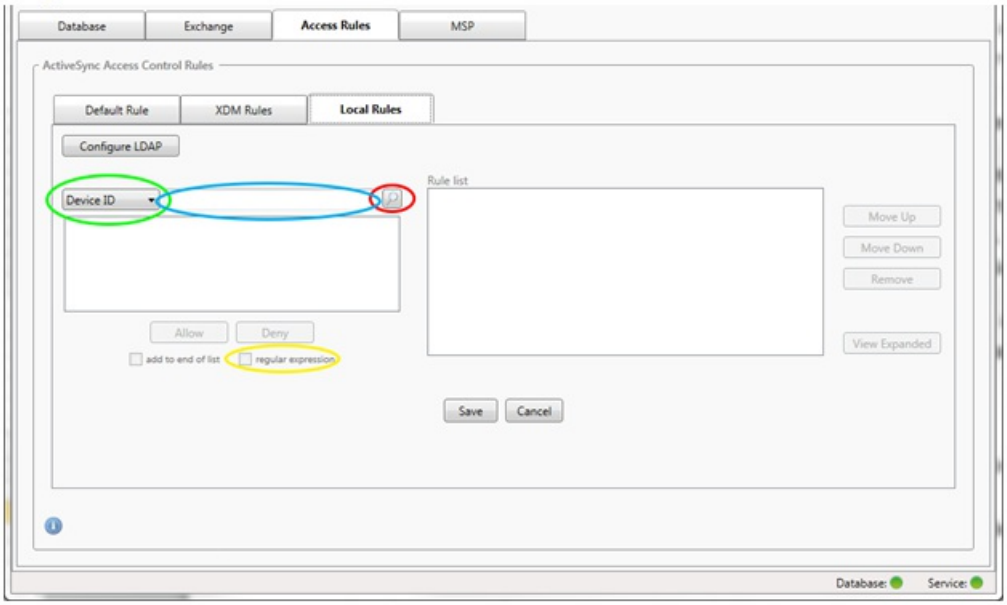


Pour rechercher des appareils

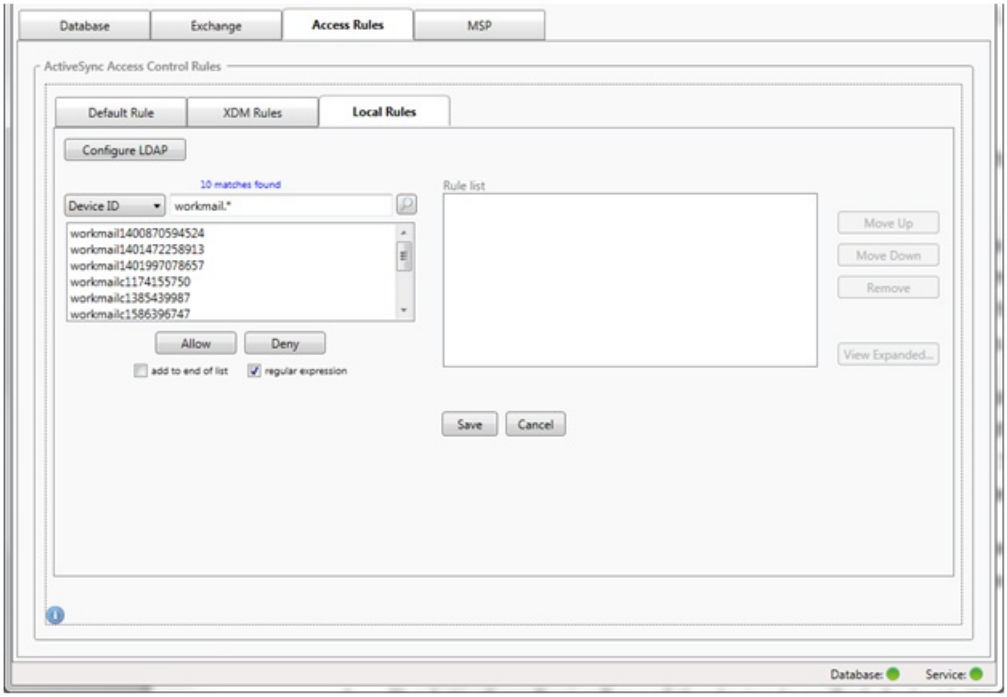
En cochant la case « regular expression », vous pouvez rechercher des appareils correspondant à l'expression donnée. Cette fonction est uniquement disponible si un instantané principal a été effectué. Vous pouvez utiliser cette fonction, même si vous ne prévoyez pas d'utiliser des règles d'expressions régulières. Imaginons que vous souhaitiez rechercher tous les appareils contenant « workmail » dans l'ID d'appareil ActiveSync. Pour ce faire, suivez cette procédure.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Cliquez sur l'onglet Access Rules.
2. Assurez-vous que le sélecteur de champ d'appareil est défini sur Device ID (valeur par défaut).



3. Cliquez sur la zone de texte de l'élément sélectionné (comme illustré en bleu dans la figure précédente) puis tapezworkmail.*.
4. Vérifiez que la case regular expression est cochée et cliquez sur l'icône de la loupe pour afficher les correspondances comme illustré dans la figure suivante.



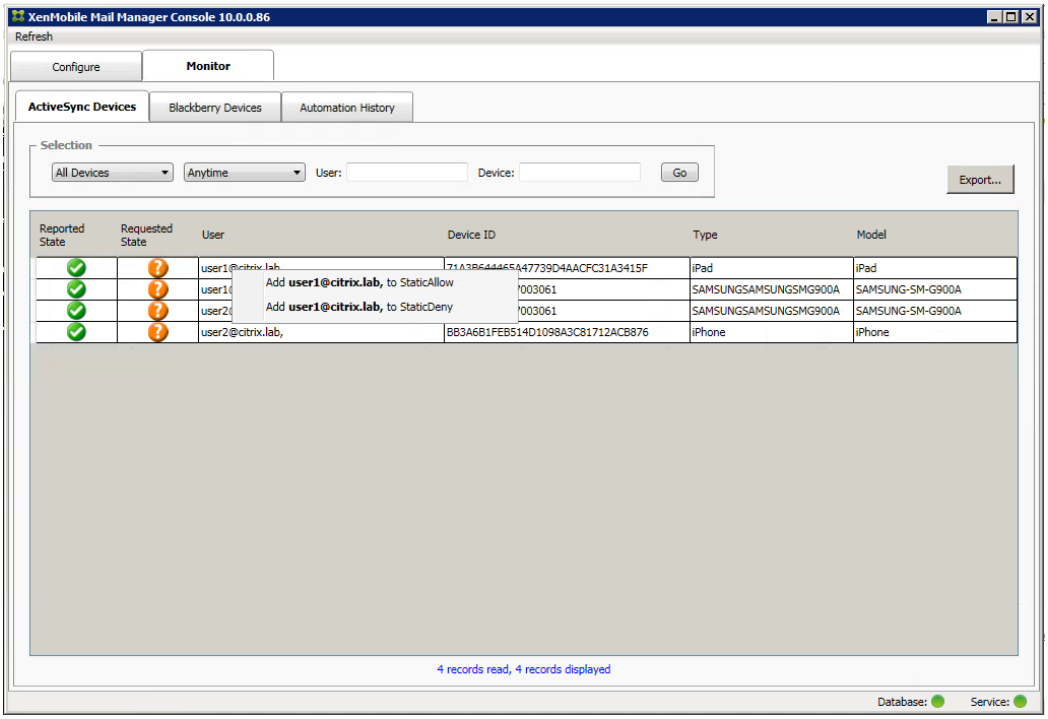
Pour ajouter un seul utilisateur, appareil ou type d'appareil à une règle statique

Vous pouvez ajouter des règles statiques basées sur l'utilisateur, l'ID d'appareil ou le type d'appareil sur l'onglet ActiveSync Devices.

1. Cliquez sur l'onglet ActiveSync Devices.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Dans la liste, cliquez avec le bouton droit sur un utilisateur, un appareil ou un type d'appareil et choisissez si vous souhaitez autoriser ou refuser votre sélection.
   L'image suivante montre l'option Allow/Deny lorsque user1 est sélectionné.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Surveillance des appareils

Jul 25, 2016

L'onglet Monitor de XenMobile Mail Manager permet de visualiser les appareils Exchange ActiveSync et BlackBerry qui ont été détectés et l'historique des commandes PowerShell automatisées qui ont été émises. L'onglet Monitor inclut les trois onglets suivants :

- ActiveSync Devices :
  - Vous pouvez exporter les partenariats d'appareils ActiveSync affichés en cliquant sur le bouton Export.
  - Vous pouvez ajouter des règles locales (statiques) en cliquant avec le bouton droit sur les colonnes User, Device ID où Type et en choisissant la règle d'autorisation ou de blocage appropriée.
  - Pour réduire une ligne développée, faites un Ctrl-clic sur la ligne développée.
- Blackberry Devices
- Automation History

L'onglet Configure affiche l'historique de tous les instantanés. L'historique d'instantané affiche le moment où l'instantané a été capturé, la durée nécessaire à la capture, le nombre d'appareils détectés et toutes les erreurs qui se sont produites :

- Sur l'onglet Exchange, cliquez sur l'icône d'information pour le serveur Exchange Server désiré.
- Sous l'onglet MSP, cliquez sur l'icône d'information pour le serveur BlackBerry désiré.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dépannage et diagnostics

Jul 25, 2016

XenMobile Mail Manager consigne erreurs et d'autres informations opérationnelles dans son fichier journal : \XmmWindowsService.log. XenMobile Mail Manager consigne également d'importants événements dans le journal d'événements Windows.

La liste suivante contient des erreurs courantes :

Le service XenMobile Mail Manager ne démarre pas

En cas d'erreurs, consultez le fichier journal et le journal des événements Windows. Les raisons habituelles sont les suivantes :

- Le service XenMobile Mail Manager ne peut pas accéder au serveur SQL. Cela peut être dû aux problèmes suivants :
  - Le service SQL Server n'est pas exécuté.
  - Échec de l'authentification.

  Si l'authentification Windows Integrated n'est pas configurée, le compte d'utilisateur du service XenMobile Mail Manager doit être une ouverture de session SQL autorisée. Le compte du service XenMobile Mail Manager utilise par défaut le compte système local, mais peut être modifié pour utiliser un autre compte disposant des privilèges d'administrateur local. Si l'authentification SQL est configurée, l'ouverture de session SQL doit être correctement configurée dans SQL.
- Le port configuré pour le fournisseur de services mobiles (MSP) n'est pas disponible. Le port d'écoute sélectionné ne doit pas être utilisé par un autre processus du système.

XenMobile ne peut pas se connecter au MSP

Vérifiez que le port du service MSP et le transport sont correctement configurés dans l'onglet Configure > MSP de la console XenMobile Mail Manager. Vérifiez qu'un groupe ou utilisateur d'autorisations est correctement défini.
Si le protocole HTTPS est configuré, vous devez installer un certificat de serveur SSL valide. Si IIS est installé, vous pouvez utiliser le gestionnaire IIS (Internet Information Services) pour installer le certificat. Si IIS n'est pas installé, consultez la section https://msdn.microsoft.com/fr-fr/library/ms733791.aspx pour plus d'informations sur l'installation de certificats.

XenMobile Mail Manager possède un utilitaire pour tester la connectivité au service MSP. Exécutez le programme MspTestServiceClient.exe et paramétrez l'URL et les informations d'identification afin qu'elles correspondent à celles qui seront configurées dans XenMobile, puis cliquez sur Test Connectivity. Cela simule les requêtes de service Web que le service XenMobile émet. Notez que si le protocole HTTPS est configuré, vous devez spécifier le nom d'hôte actuelle du serveur (le nom spécifié dans le certificat SSL).

Remarque : lors de l'utilisation de **Test Connectivity**, assurez-vous d'avoir au moins un enregistrement ActiveSyncDevice ou le test risque d'échouer.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile NetScaler Connector

Oct 11, 2016

XenMobile NetScaler Connector fournit un service d'autorisation au niveau de l'appareil des clients ActiveSync à NetScaler qui fait office de proxy inverse pour le protocole Exchange ActiveSync. L'autorisation est contrôlée par une combinaison de stratégies que vous définissez dans XenMobile et par des règles définies localement par XenMobile NetScaler Connector.

Pour plus d'informations, consultez les articles suivants :

- XenMobile NetScaler Connector
- ActiveSync Gateway dans XenMobile

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.