À propos de XenMobile 10

Oct 11, 2016

XenMobile 10 combine les composants App Controller et Device Manager de XenMobile 9 et des versions précédentes au sein d'un outil de gestion unifié à partir duquel vous pouvez configurer et gérer des applications et des appareils utilisateur.

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.

Nouveautés

Pour obtenir une liste des problèmes résolus dans cette version, consultez l'article http://support.citrix.com/article/CTX141722. Pour obtenir une liste des problèmes connus dans XenMobile 10.0, consultez la section Problèmes connus.

- **Infrastructure unifiée**. La gestion de la flotte (MDM) et des applications mobiles (MAM) est unifiée au sein d'une seule infrastructure de serveur.
  - Vous pouvez déployer XenMobile plus rapidement en raison du nombre restreint d'étapes de configuration nécessaires.
  - Vous pouvez gérer des applications et des appareils à partir d'un seul serveur virtuel.
- **Nouvelle console XenMobile unifiée.**
  - Interface utilisateur conviviale conçue pour faciliter les tâches administratives, telles que l'inscription, le déploiement, la configuration et le dépannage de l'environnement mobile complet.
  - Configuration de stratégie d'application et d'appareil simplifiée. Vous pouvez configurer une stratégie sur toutes les plates-formes d'appareils disponibles.
- **Intégration avec NetScaler Gateway à partir de la même console.** Vous pouvez gérer les contrôles de connectivité automatisés pour de multiples systèmes qui font partie de l'environnement mobile.
- **Prise en charge des balises abandonnée.** Les balises ne sont pas prises en charge dans XenMobile 10, bien que leurs options apparaissent dans la console XenMobile. Citrix vous recommande de vous connecter au serveur XenMobile via NetScaler Gateway ou, directement au serveur XenMobile derrière votre pare-feu.
- **Prise en charge améliorée de l'authentification applicative.** Permet de crypter les communications entre les appareils et le réseau interne, entre le réseau interne et le serveur XenMobile, et pour les connexions à la console XenMobile.
  - Authentification adaptative RSA
  - Prise en charge du cryptage avancé FIPS 140.2

Prise en main de XenMobile 10

Commencez par télécharger et installer l'image virtuelle pour XenMobile 10.0 Edition sur un hyperviseur, tel que XenServer, VMware ESXi ou Hyper-V, puis procédez à la configuration initiale de XenMobile sur la console de ligne de commande de l'hyperviseur. Pour de plus amples informations, reportez-vous aux sections Configuration système requise, Check-list de pré-installation et Installation de XenMobile.

Ouvrez ensuite la console XenMobile Web à l'aide du compte administrateur que vous avez créé durant la configuration initiale.

Pour de plus amples informations sur les autres étapes à suivre, consultez la section Prise en main de la console. La première série de recommandations couvre les paramètres initiaux que vous avez peut-être ignorés durant les étapes d'installation.

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.
- 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.

Les sections suivantes décrivent différentes architectures de référence pour le déploiement XenMobile. Pour accéder à des

diagrammes d'architecture de référence, consultez les sections 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.

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.

Mode de gestion de la flotte mobile (MDM)

XenMobile MDM Edition permet de gérer les appareils mobiles pour iOS, Android, Amazon et Windows Phone (voir Plates-formes prises en charge dans XenMobile 10). Vous déployez XenMobile en mode MDM si vous projetez 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 10). Vous déployez XenMobile en mode MAM (également appelé mode MAM exclusif) si vous projetez 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 10). 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.

Capacité à monter en charge de XenMobile 10

Oct 11, 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.
- Le taux d'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 de la charge de travail d'intégration (FTU), ainsi que les tests de capacité à monter en charge pour la charge de travail des utilisateurs existants.

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 :

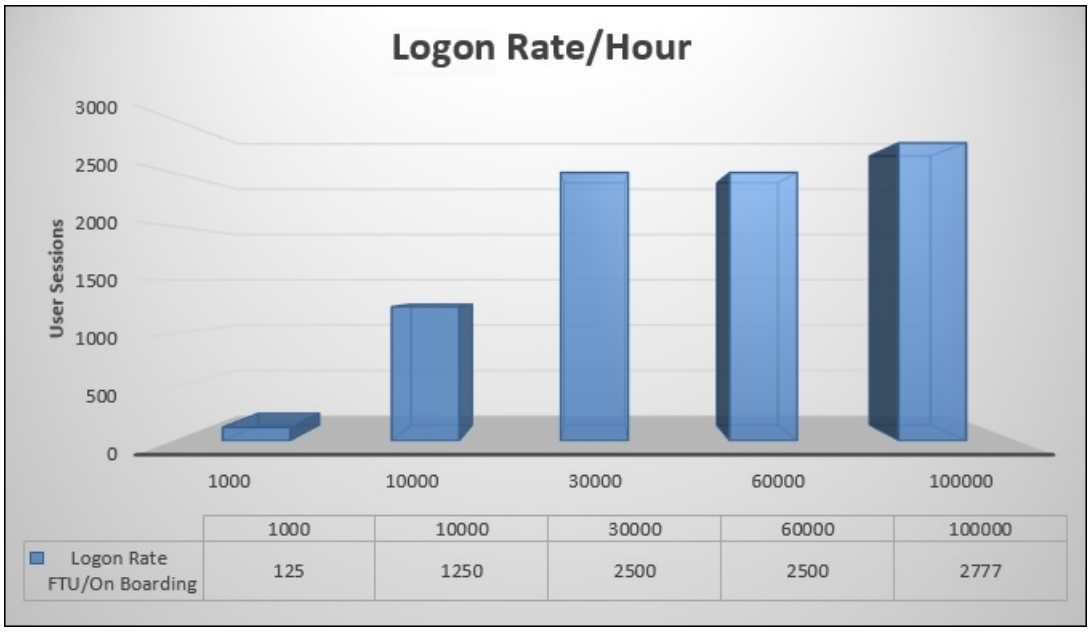
- Le taux d'ouverture de session est un facteur important pour déterminer la capacité à monter en charge d'un système. Outre l'ouverture de session initiale, les taux d'ouverture de session dépendent des valeurs d'expiration de l'authentification configurées dans votre environnement. Par exemple, si 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	
XenMobile - mode	Autonome	Autonome	Cluster		

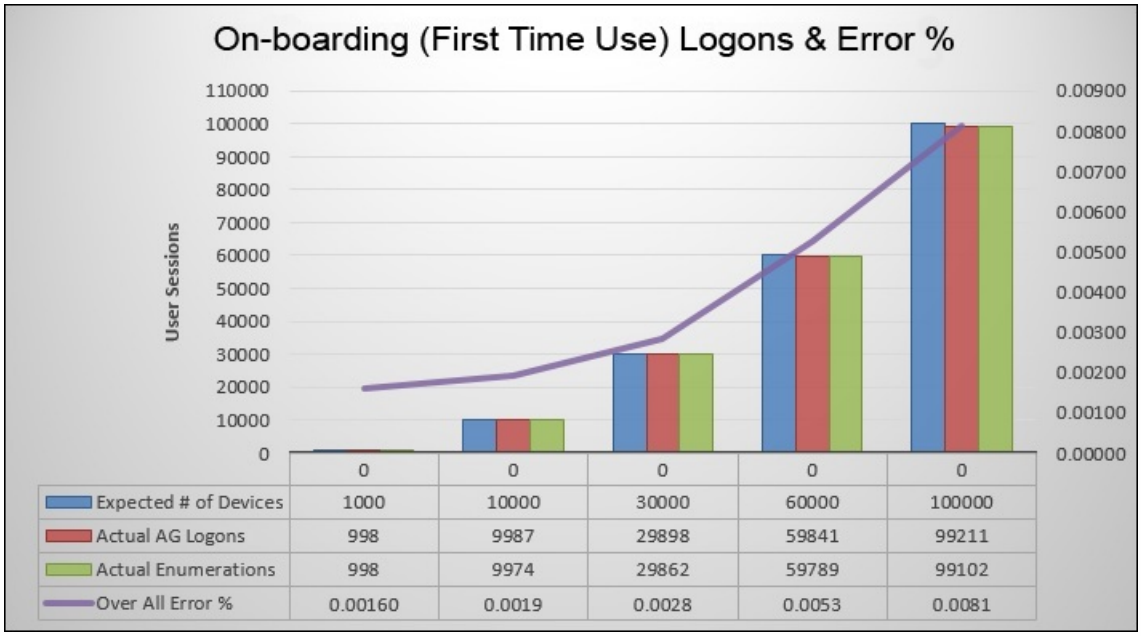
XenMobile - cluster	S.O.	S.O.	3	6	10
XenMobile - boîtier virtuel	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	8 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels	16 Go de RAM et 4 processeurs virtuels
Base de données	Externe				

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.



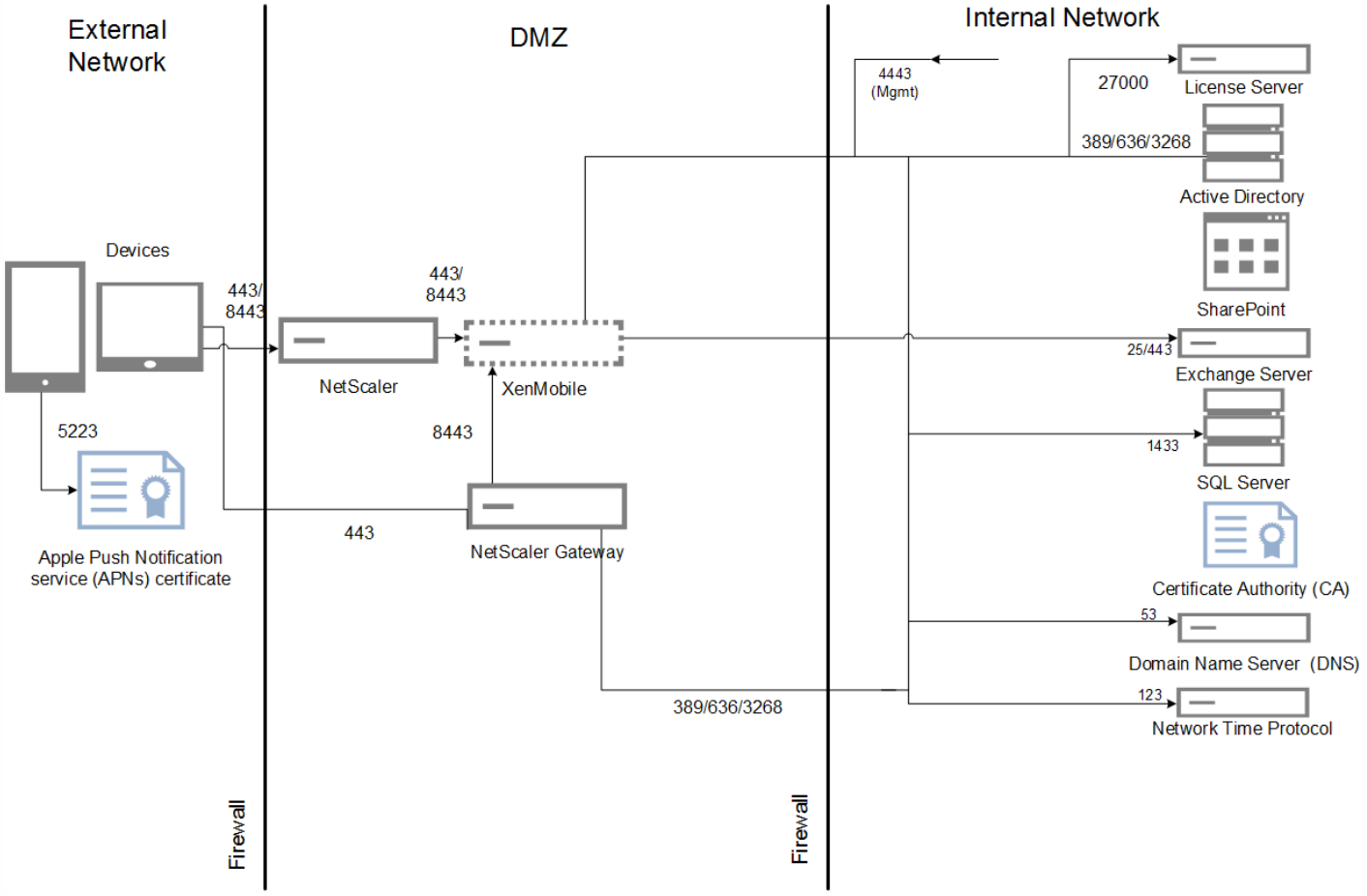
Remarque : vous allez rencontrer les situations suivantes si vous dépassez les recommandations en termes de taux ou de matériel lors du dimensionnement de votre système.

- 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.

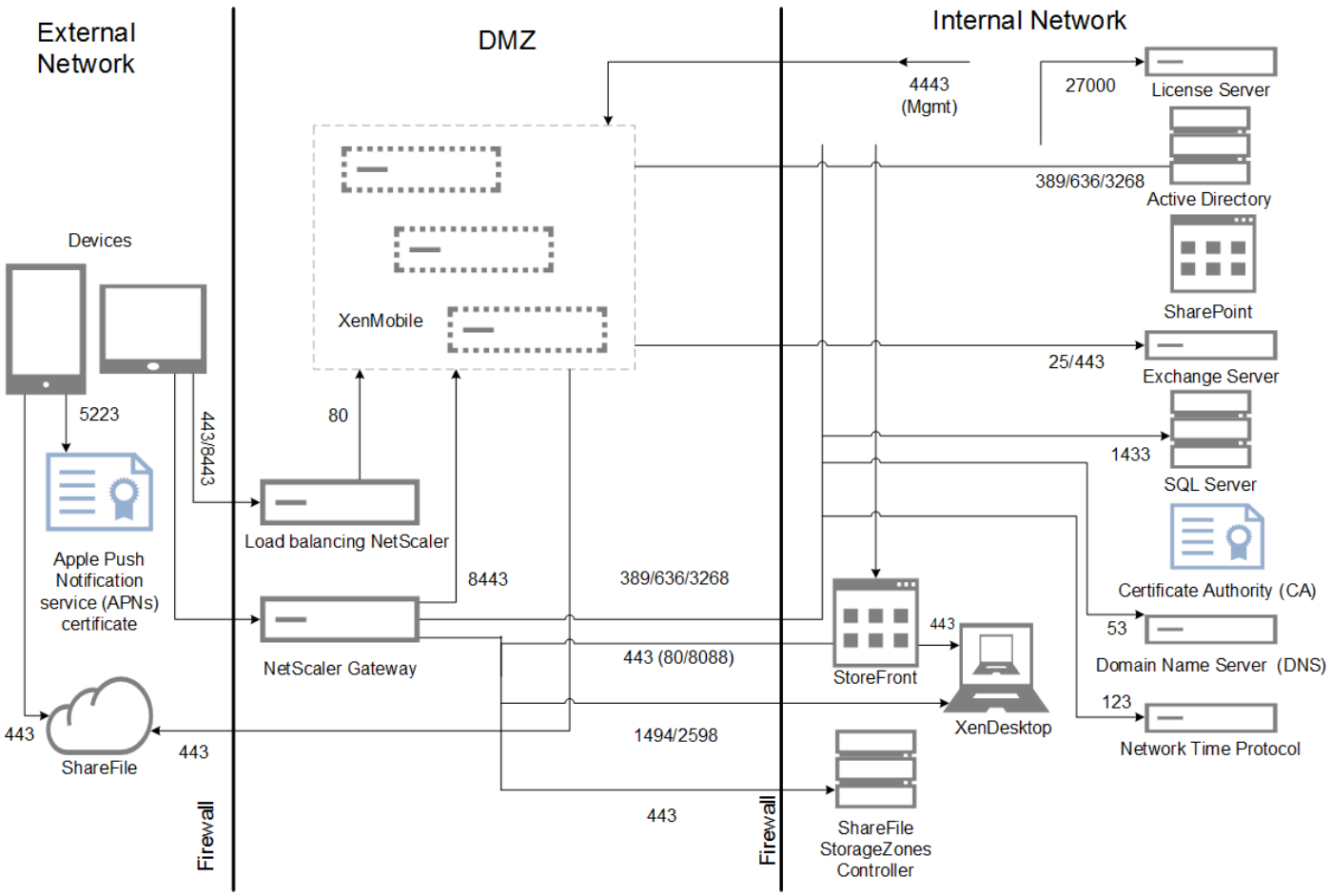


Le pourcentage d'erreur dans la figure précédente comprend l'ensemble des erreurs rencontrées relatives aux demandes correspondant à chaque opération et n'est pas limité aux ouvertures de session. Le pourcentage d'erreur se situe dans la limite autorisée pour chaque série de tests comme défini dans les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



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 MDM sur HTTP qui prend en charge 10 000 appareils ou plus.



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 10 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.

Charges de travail

Les charges de travail des utilisateurs sont définies comme suit :

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

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.

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
- 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

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.

Critères de sortie

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 7. Composants d'infrastructure XenMobile

Composant	Version
NetScaler Gateway	10.5.55.8.nc
XenMobile	10.0,62300.0.0
Base de données externe	MS SQL Server 2008 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 8. Matériel XenServer

Fournisseur	GenuineIntel
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).

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.

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.

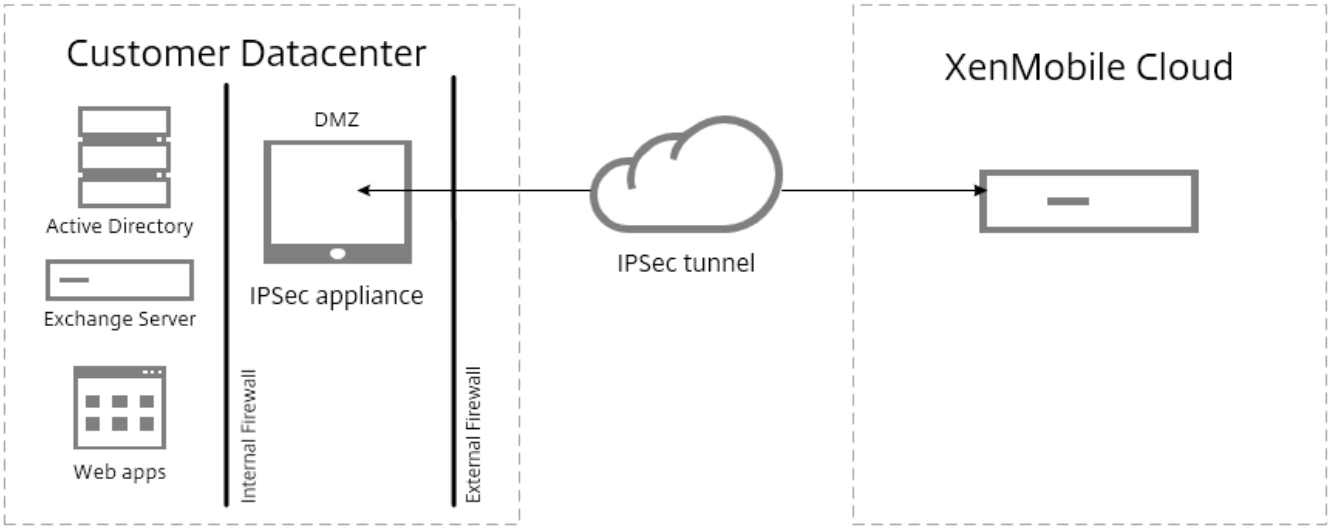
Les administrateurs de Cloud Operations peuvent gérer la maintenance et la configuration de la connectivité réseau, ainsi que l'intégration de produits Citrix tels que NetScaler, XenApp, XenDesktop, StoreFront et ShareFile. L'environnement de cloud est hébergé dans des centres de données Amazon situés 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.



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.

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

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

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

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

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

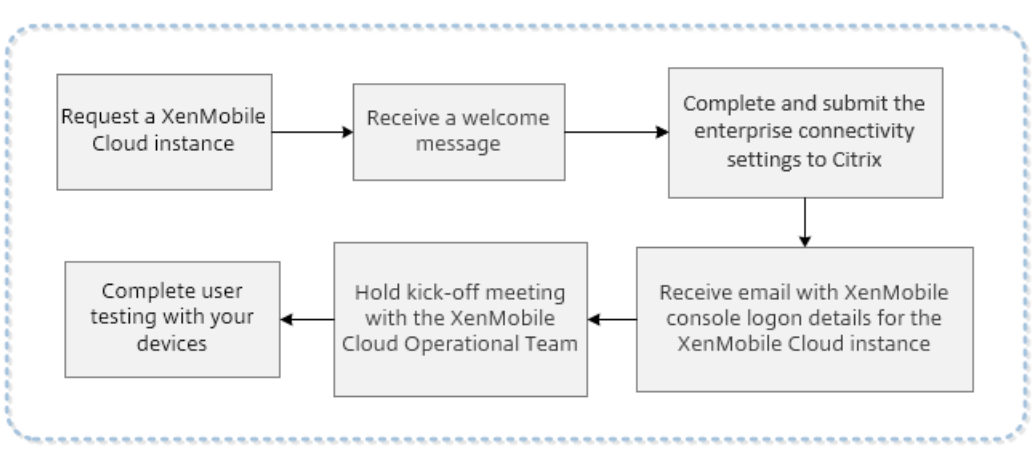
Pour obtenir des instructions détaillées sur la personnalisation des rôles, veuillez consulter la section Configuration de rôles avec RBAC.

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

Administration et conditions requises par XenMobile Cloud

May 06, 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

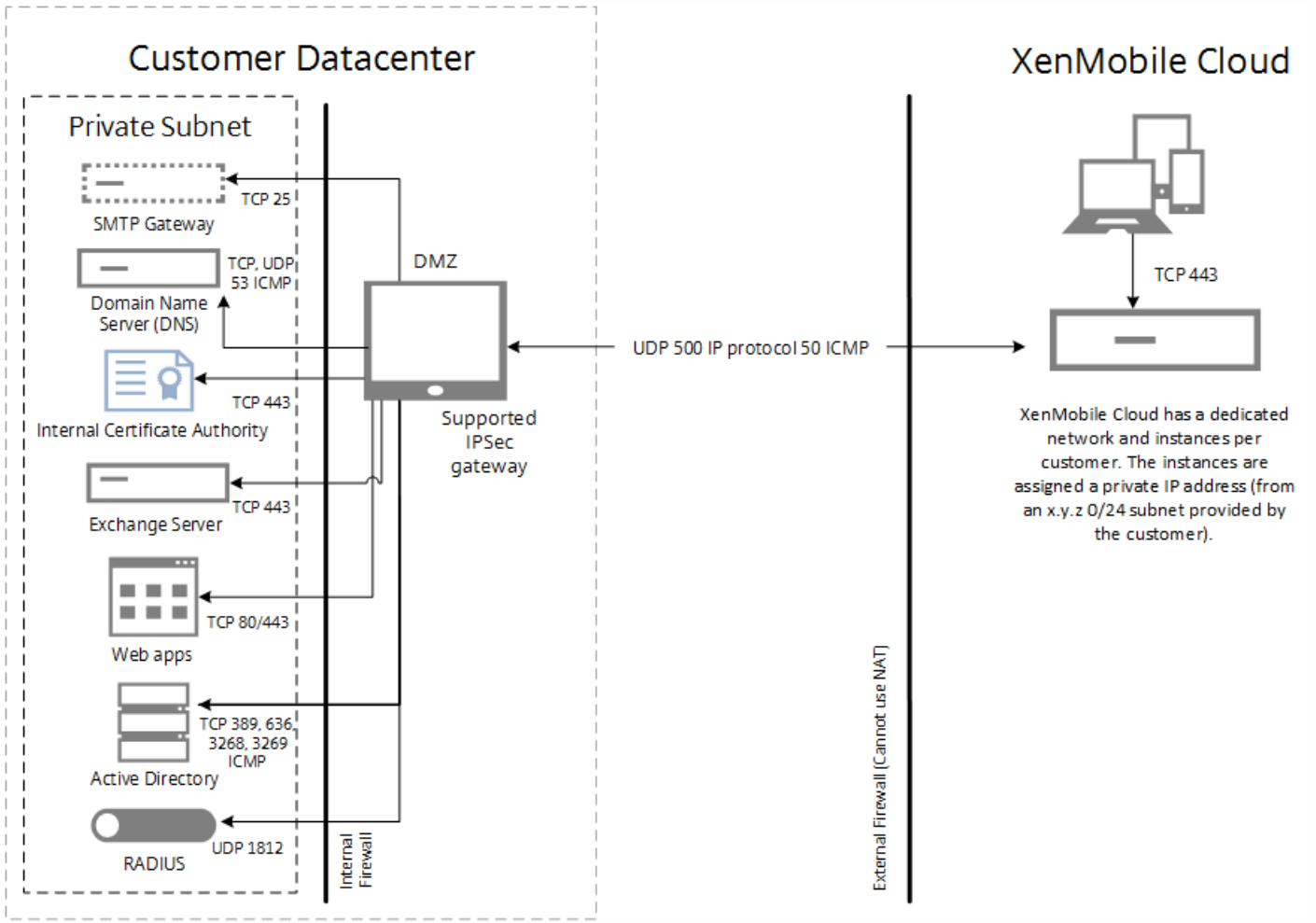
Vous pouvez utiliser un connecteur d'entreprise XenMobile, un tunnel IPsec pour connecter l'infrastructure XenMobile Cloud avec les services d'entreprise, tels que Active Directory.

Les passerelles IPsec répertoriées sur le site Web des services Web Amazon 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.

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.

(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.

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.

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.

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.

Prise en charge des plates-formes dans XenMobile Cloud

May 06, 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.

Configuration système requise

Oct 11, 2016

Pour exécuter XenMobile 10, vous avez besoin de la configuration système minimale suivante :

- L'un des suivants :
  - XenServer (versions prises en charge : 6.2.x, 6.1.x, or 6.0.x) ; pour plus de détails, reportez-vous à XenServer
  - VMWare (versions prises en charge : ESXi 5.5, ESXi 5.1, ESXi 4.1) ; 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
- 8 Go de RAM
- 50 Go d'espace disque

La configuration recommandée pour 10 000 périphériques est la suivante :

- Processeur quadruple cœur
- 8 Go de RAM

Pour exécuter NetScaler Gateway avec XenMobile 10, vous avez besoin de la configuration système minimale suivante :

- XenServer, VMware ou Hyper-V
- 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.

Le référentiel Device Manager nécessite une base de données Microsoft SQL Server exécutée sur l'une des versions prises en charge suivantes :

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

Citrix XenMobile prend en charge les groupes de disponibilité SQL Always ainsi que la mise en cluster SQL pour assurer une haute disponibilité de la base de données. Citrix ne prend pas en charge la mise en miroir de bases de données pour la haute disponibilité de la base de données de XenMobile. Citrix prend en charge la haute disponibilité de la base de données en mode actif/actif ou actif/inactif avec le déploiement MS SQL Cluster.

Remarque : si la base de données est hors connexion, le serveur XenMobile n'établira pas de connexions à partir des appareils car il sera également hors connexion.

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.

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

Compatibilité XenMobile

Oct 11, 2016

> **Important**
>
> À compter de la version 10.4, les applications mobiles Worx sont renommées Applications XenMobile. La plupart des applications XenMobile ont été renommées, mais pas toutes. Pour de plus amples informations, consultez la section À propos des applications XenMobile.

Cet article dresse la liste des versions des composants XenMobile pris en charge que vous pouvez intégrer, y compris NetScaler Gateway, ainsi que la version du MDX Toolkit requise pour wrapper, configurer et distribuer des applications mobiles Worx/XenMobile.

XenMobile 10.x

Versions NetScaler Gateway prises en charge :

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

Citrix prend en charge la version actuelle et les deux dernières versions antérieures de XenMobile. À titre d'exemple, si la version actuelle est XenMobile 10.4, Citrix prend également en charge XenMobile 10.3.6 (qui est un Service Pack plutôt qu'une version complète) et XenMobile 10.3.5.

Les composants du client XenMobile doivent satisfaire aux exigences de compatibilité suivantes :

- Les dernières versions de Secure Hub et du MDX Toolkit sont compatibles avec la dernière version du serveur XenMobile et les deux versions les plus récentes avant celle-ci.
- La dernière version de Secure Hub, et la version la plus récente avant celle-ci, sont compatibles avec les dernières versions du MDX Toolkit et des applications XenMobile.
- La dernière version des applications XenMobile a été testée avec la dernière version du MDX Toolkit.

Pour tirer parti des nouvelles fonctionnalités, des correctifs et des mises à jour de stratégie, Citrix vous recommande d'installer la dernière version de MDX Toolkit, de Secure Hub et des applications XenMobile.

Pour bénéficier des nouvelles fonctionnalités, des corrections et des stratégies mises à jour, Citrix vous recommande d'installer la version la plus récente du MDX Toolkit, de Worx Home et des applicati

Versions Android et iOS du MDX Toolkit	**Versions de Worx Home/Secure Hub**	
	Android	**iOS**
10.4	10.4	10.4
10.3.10	10.3.10	10.3.10
10.3.9	10.3.9	10.3.9
10.3.6	10.3.8	10.3.8
10.3.5	10.3.6	10.3.6
10.3.1	10.3.5	10.3.5
10.2.1	10.3.1	10.3.1
10.7.0	10.3	
10.0.5	10.2.1	10.2.1
10.0.3	10.8.0	10.8.0
	10.0.3	10.0.3

MDX Toolkit pour Windows Phone	**Versions Worx Home compatibles***
10.7.0	10.0.3
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

* Les versions de Worx Home antérieures à 10.0.3 sont compatibles mais non prises en charge.

> **Remarque**
>
> Windows Phone 10 est uniquement pris en charge pour XenMobile 10 et 10.3.x. Il n'est pas pris en charge pour XenMobile 10.1. Pour XenMobile 9, vous devez installer un correctif pour que les applications fonctionnent

correctement. Pour de plus amples informations, consultez l'article CTX215497.

XenMobile 10.x prend en charge les versions des applications mobiles Worx/XenMobile répertoriées dans le tableau ci-dessous.

App	Android	iOS	Windows Phone 8.1/10[1]
Secure Hub	10.4	10.4	
Worx Home	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3.1 10.2.1 10.8.0 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2.1 10.8.0 10.0.3 10.0.0	10.0.3 10.0.0
Secure Forms		10.4 10.3.10 10.3.9 10.3.8 10.3.6	
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.2 10.7.0
Secure Notes	10.4	10.4	
Worx Notes	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10,3 10.2 10.7.0 10.0.0	
Secure Tasks	10.4	10.4	

WorxTasks	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.7.0	10.3.10 10.3.9 10.3.6 10.3.5 10,3 10.2 10.7.0	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.3.10 10.3.9 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[2]	6.5	6.4	
ShareConnect	3.6	3.8	
ShareFile	4.9	4.7.1	

1 Windows Phone 10 n'est pas pris en charge sur XenMobile 10.1.

2 Seules les versions plus récentes de QuickEdit, ShareConnect et ShareFile sont prises en charge.

Prise en charge des navigateurs

XenMobile 10.x prend en charge les navigateurs suivants :

- Internet Explorer (mais pas la version 9 ou les versions antérieures)
- Chrome
- Firefox
- Safari sur les appareils mobiles pour accéder au portail en libre-service.

XenMobile 10.x est compatible avec la version la plus récente du navigateur ainsi qu'avec une version antérieure à la version actuelle.

XenMobile 9

XenMobile 9 inclut Device Manager 9.0 et App Controller 9.0.

Versions NetScaler Gateway prises en charge :

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

Les composants du client XenMobile doivent généralement satisfaire aux exigences de compatibilité suivantes :

- La dernière version de Secure Hub et du MDX Toolkit est compatible avec les deux dernières versions du serveur XenMobile.
- La dernière version du MDX Toolkit est compatible avec les dernières applications XenMobile.
- Les versions récentes du MDX Toolkit sont compatibles avec les versions suivantes de Secure Hub :

	Versions de Worx Home/Secure Hub*

Versions Android et iOS du MDX Toolkit		
	Android	**iOS**
10.4	10.4	10.4
10.3.6	10.3.6	10.3.6
10.3.5	10.3.5	10.3.5
10.3.1	10.3.1	
10.3	10.3	10.3
10.2.1	10.2.1	10.2.1
10.7.0	10.8.0	10.8.0
10.0.5	10.0.3	10.0.3
10.0.3		

MDX Toolkit pour Windows Phone 10[1]	**Versions de Secure Hub compatibles**
10.4	10.4
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2	10.2

[1]Dans XenMobile 9, Windows 10 requiert un correctif disponible ici.

MDX Toolkit for Windows Phone 8.1	**Versions de Secure Hub compatibles***
10.3.5	10.3.5
10.3.1	10.3
10.3	10.3
10.2.1	10.2.1
10.0.5 - 10.0.3	10.0.3
10.0.0	10.0.0

*Les versions de Secure Hub antérieures à 10.0.3 sont compatibles mais non prises en charge.

XenMobile 9 prend en charge les versions des applications mobiles Worx/XenMobile répertoriées dans le tableau ci-dessous.

App	**Android**	**iOS**	**Windows Phone 8.1**
Secure Hub	10.4	10.4	

Worx Home	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3.1 10.2.1 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2.1 10.8.0 10.0.3 10.0.0	10.0.3 10.0.0
Secure Mail	10.4	10.4	
WorxMail	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.2 10.7.0
Secure Notes	10.4	10.4	
WorxNotes*	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.0	
Secure Tasks	10.4	10.4	
WorxTasks	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2	

		10.7.0	
Secure Web	10.4	10.4	
WorxWeb	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.0.3 10.0.0	10.3.10 10.3.9 10.3.8 10.3.7 10.3.6 10.3.5 10.3 10.2 10.7.0 10.0.3 10.0.0	10.2 10.0.3
QuickEdit[1]	6.0.2	6.3.10	
ShareConnect	3.2	3.6	
ShareFile	4.6.5	4.5	

[1]Seules les versions les plus récentes de QuickEdit, ShareConnect et ShareFile sont prises en charge.

* MDX Toolkit 2.3 et 2.2.1 ne prennent pas en charge WorxNotes/Secure Notes.

Plates-formes prises en charge

Oct 11, 2016

XenMobile prend en charge les appareils exécutant les plates-formes suivantes pour la gestion de la mobilité d'entreprise, y compris la gestion d'applications et d'appareils. En raison de restrictions spécifiques à la plate-forme et de fonctionnalités de sécurité, les fonctionnalités ne sont pas toutes prises en charge sur toutes les plates-formes.

Pour prendre en charge les anciennes versions de systèmes d'exploitation mobiles, tels que Android 4.1 et iOS 7, consultez l'article CTX204192 dans le centre de connaissances Citrix.

Les informations sur les plates-formes prises en charge dans cet article s'appliquent également à XenMobile Mail Manager et à XenMobile NetScaler Connector.

Remarque

- Citrix prend en charge, au minimum, la version actuelle et une version antérieure des principales plates-formes de système d'exploitation. Les fonctionnalités de la nouvelle version de XenMobile ne fonctionneront pas toutes sur les anciennes versions de plates-formes. Cet article décrit en détail ce que Citrix prend en charge pour chaque système d'exploitation. Il contient également les modèles d'appareils testés par Citrix. Si vous rencontrez des problèmes avec d'autres modèles d'appareils, veuillez contacter le service d'assistance technique de Citrix.
- À compter de la version 10.4, les applications mobiles Worx sont renommées Applications XenMobile. La plupart des applications XenMobile ont été renommées, mais pas toutes. Pour de plus amples informations, consultez la section À propos des applications XenMobile.

XenMobile 10.4 et 10.3.x

Systèmes d'exploitation pris en charge pour tous les modes : Android 4.4.x, 5.x, 6.x, 7

Systèmes d'exploitation pris en charge pour le mode MDM uniquement : Android 4.1.x, 4.2.x, 4.3

Worx Home/Secure Hub sont pris en charge sur les appareils Android x86 pour les fonctions MDM.

Les applications XenMobile/Worx wrappées MDX sont prises en charge sur les appareils Android x64.

Appareils Android utilisés pour tester XenMobile 10.3.x et 10.4 sur les systèmes d'exploitation répertoriés précédemment :

- Nexus 6, 7, 9, 10
- Samsung Galaxy S4 et Note 3, 4, 5
- Galaxy Tablet P750
- Galaxy Tab-A
- Galaxy Tab 2 - S3, S4, S5
- HTC One
- Samsung Tablet P750
- Samsung S6, S6 Edge et S7
- OnePlus X

- Xiaomi Mi 4
- Huawei Honor 6
- Huawei Ascend Mate 7
- HTC One M9
- Motorola Moto-X
- Sony Experia Z
- Note 2, 3, 4

XenMobile 10 et 10.1

Systèmes d'exploitation pris en charge pour tous les modes : 4.4.x, 5.x, 6.x, 7

Systèmes d'exploitation pris en charge pour le mode MDM uniquement : 4.1.x

Android 4.2 et 4.3 ne sont pas pris en charge.

Worx Home est pris en charge sur les appareils Android x86 pour les fonctions MDM. La gestion des applications est uniquement disponible sur les appareils Android équipés de processeurs ARM. Les applications wrappées MDX ne sont pas prises en charge sur les appareils Android x86.

Les applications Worx wrappées MDX sont prises en charge sur les appareils Android x64.

Appareils Android utilisés lors des tests avec XenMobile 10 et 10.1 sur les systèmes d'exploitation répertoriés ci-dessus :

- Nexus 10, 7, 5, 9
- Galaxy S4 et Note 2, 3
- Galaxy Tablet 2, S3, S4, S5
- Moto X
- HTC One
- HTC Desire, LG
- Samsung Tablet P750

SAFE et KNOX

Sur les appareils Samsung compatibles, XenMobile 10.x prend en charge et étend les stratégies Samsung KNOX et Samsung for Enterprise (SAFE). Vous devez activer les API SAFE en déployant la clé Samsung ELM (Enterprise License Management) intégrée sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. Pour activer les API Samsung KNOX, vous devez acheter une licence Samsung KNOX à l'aide du Samsung KNOX License Management System (KLMS) en plus de déployer la clé Samsung ELM.

Pour les stratégies HTC, XenMobile prend en charge HTC API version 0.5.0. Dans le cas des stratégies spécifiques aux appareils Sony, XenMobile prend en charge Sony Enterprise SDK 2.0.

Remarque : toutes les applications Worx/XenMobile sont compatibles avec iOS 10 à compter de la version 10.3.10. Vous devez utiliser le MDX Toolkit 10.3.10 ou ultérieur pour wrapper des applications mobiles ou d'entreprise pour garantir leur compatibilité avec iOS 10. Lorsque les utilisateurs mettent à niveau vers iOS 10, ils doivent également mettre à niveau vers Worx Home 10.3.10 ou une version supérieure (Secure Hub) pour pouvoir ouvrir des applications MDX. Pour de plus amples informations, consultez cet article du centre de connaissances.

XenMobile 10.3.x et 10.4

- iOS 10
- iOS 9.x
- iOS 8.x (Worx Home/Secure Hub uniquement dans les déploiements en mode MDM exclusif)

Appareils iOS pris en charge par XenMobile 10.3.x et 10.4 :

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

XenMobile 10 et 10.1

- iOS 10
- iOS 9.x
- iOS 8.x (Worx Home uniquement dans les déploiements en mode MDM exclusif)

Appareils iOS pris en charge par XenMobile 10 et 10.1 :

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

XenMobile 10.3.x et 10.4

- Windows 10, 8.1 Tablet
  - Windows 10 Tablet n'est pas pris en charge lorsque XenMobile est en mode MAM uniquement.
- Windows Tablet Surface Pro 3, Surface 2, RT
- Windows Phone 10, 8.1
  - Pour Windows Phone 10, vous devez installer un correctif depuis la page des téléchargements de XenMobile.
  - Windows Phone 8.1 et 10 ne sont pas pris en charge lorsque XenMobile est en mode MAM uniquement.
- Compatibilité de Windows Phone 8.1 avec Worx Home :
  - Worx Home 10.0 lorsque XenMobile est en mode Enterprise
  - Worx Home 9.1.0 lorsque XenMobile est en mode MDM-only
- Windows 8.1 éditions Professionnel et Entreprise (32 bits et 64 bits)
- Windows RT 8.1
- Windows Mobile/CE
  - Windows CE n'est pas pris en charge lorsque XenMobile est en mode MAM uniquement.

Appareils Windows pris en charge par XenMobile 10.3 :

- Windows Tablet 10, 8.1
- Windows Phone 10, 8.1
- HTC (Windows Phone 8.1)
- Nokia 920, 925, 1020, 1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3

- Windows Tablet Surface 2
- Windows Tablet RT

XenMobile 10 et 10.1

- Windows 10 Tablet
- Windows Phone 8.1 / 10 :
  - Windows Phone 8.1 n'est pas pris en charge lorsque XenMobile est en mode MAM uniquement.
  - Windows Phone 10 est pris en charge sur XenMobile 10.3 et versions ultérieures.
  - Windows Phone 10 est pris en charge sur XenMobile 9, mais vous devez installer un correctif Device Manager, comme traité dans cet article du centre de connaissances. Prenez également note du correctif pour Windows 10 Anniversary Update version 1607 pour Windows Phones. Pour de plus amples informations, consultez cet article du centre de connaissances.
- Compatibilité de Windows Phone 8.1 avec Worx Home :
  - WorxHome 10.0 lorsque XenMobile est en mode Enterprise
  - WorxHome 9.0.3 lorsque XenMobile est en mode MDM-only
- Windows 8.1 éditions Professionnel et Entreprise (32 bits et 64 bits)
- Windows RT 8.1
- Windows Mobile : XenMobile 10.1 ne prend pas en charge les appareils Windows Mobile. Les utilisateurs d'appareils exécutant Windows Mobile ou Windows CE doivent continuer à utiliser XenMobile 9.

Appareils Windows pris en charge par XenMobile 10 et 10.1 :

- Windows Tablet 8.1
- HTC (Windows Phone 8.1)
- Nokia 920, 925, 1020, 1520 (Windows Phone 8.1)
- Windows Tablet Surface Pro 3
- Windows Tablet Surface 2
- Windows Tablet RT

La gestion des appareils Windows Phone 7 est assurée via XenMobile Mail Manager. Pour de plus amples informations, consultez la section Installation de XenMobile Mail Manager.

XenMobile 10.3.x et 10.4

XenMobile 10.3.x et 10.4 ne prennent pas en charge Symbian.

XenMobile 10 et 10.1

Exemples d'appareils Symbian pris en charge par XenMobile 10.1 et 10. Ces appareils sont uniquement pris en charge pour la gestion des appareils dans XenMobile 10 :

- Symbian 3
- Symbian S60 5ème édition
- Symbian S60 3éme édition, Feature Pack 2
- Symbian S60 3éme édition, Feature Pack 1
- Symbian S60 3éme édition
- Symbian S60 2ème édition, Feature Pack 3

- Symbian S60 2ème édition, Feature Pack 2

La gestion des appareils BlackBerry est assurée via XenMobile Mail Manager. Pour de plus amples informations, consultez la section Installation de XenMobile Mail Manager.

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.

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

Vous devez ouvrir les ports suivants pour autoriser les connexions utilisateur à partir de 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
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 fiabilité de session. Citrix recommande de conserver ce port ouvert.	NetScaler Gateway	XenApp ou XenDesktop
3268	Utilisé pour les connexions LDAP non sécurisées au Microsoft Global Catalog.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Active Directory
3269	Utilisé pour les connexions LDAP sécurisées au Microsoft Global Catalog.	NetScaler Gateway XenMobile	Serveur d'authentification LDAP ou Active Directory
9080	Utilisé pour le trafic HTTP entre NetScaler et XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
9443	Utilisé pour le trafic HTTPS entre NetScaler et XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
45000 80	Utilisé pour la communication entre deux VM XenMobile lors du déploiement dans un cluster.	XenMobile	XenMobile
8443	Utilisé pour l'inscription, XenMobile Store et la gestion des applications mobiles (MAM).	XenMobile NetScaler Gateway Appareils Internet	XenMobile
4443	Utilisé pour l'accès à la console XenMobile par un administrateur via le navigateur.	Point d'accès (navigateur)	XenMobile
	Utilisé pour 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	XenMobile	Démon vendeur Citrix

	l'obtention de licences Citrix.		

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

Port TCP	Description	Source	Destination
25	Port SMTP par défaut du service de notification XenMobile. Si votre serveur SMTP utilise un port différent, assurez-vous que votre pare-feu ne bloque pas ce port.	XenMobile	Serveur SMTP
80 et 443	Connexion de l'App Store d'entreprise à Apple iTunes App Store (ax.itunes.apple.com), Google Play (doit utiliser 80) ou Windows Phone Store. Utilisé pour la publication d'applications à partir des magasins d'application via Citrix Mobile Self-Serve sur iOS, 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)
80 ou 443	Utilisé pour les connexions sortantes entre XenMobile et Nexmo SMS Notification Relay.	XenMobile	Serveur Nexmo SMS Relay
443	Utilisé pour les connexions sortantes vers le serveur de découverte automatique.	XenMobile	https://discovery.mdm.zenprise.com
443	Utilisé pour l'inscription et l'installation de l'agent pour Android et Windows Mobile.	Internet	XenMobile
	Utilisé pour l'inscription et l'installation de l'agent pour appareils Android et Windows, la console Web XenMobile et le client d'assistance à distance MDM.	Réseau local interne et WiFi	
1433	Utilisé par défaut pour les connexions à un serveur de base de données distant (facultatif).	XenMobile	SQL Server

Port TCP	Description	Source	Destination
2195	Utilisé pour les connexions sortantes Apple Push Notification Service (APNS) à gateway.push.apple.com pour les notifications sur les appareils iOS et la transmission de stratégies aux appareils.	XenMobile	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
2196	Utilisé pour les connexions sortantes APNS à feedback.push.apple.com pour les notifications sur les appareils iOS et la transmission de stratégies aux appareils.		
5223	Utilisé pour les connexions sortantes APNS à partir d'appareils iOS sur les réseaux Wi-Fi sur *.push.apple.com.	Appareils iOS sur les réseaux WiFi	Internet (hôtes APNs utilisant l'adresse IP publique 17.0.0.0/8)
8443	Utilisé pour l'inscription d'appareils iOS et Windows Phone.	Internet	XenMobile
		Réseau local et Wi-Fi	

La configuration de ce port permet de s'assurer que les appareils Android qui se connectent à partir de Worx Home pour Android 10.2 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 cas, 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
	184.73.241.73
	54.243.233.48
	204.236.239.233
	107.20.198.193

Conformité FIPS 140-2

May 06, 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 sur iOS utilisent des modules de chiffrement certifiés FIPS fournis par le OpenSSL et Apple. Sur Android, toutes les opérations de chiffrement de données au repos et données en transit provenant de l'appareil mobile vers NetScaler Gateway utilisent des modules de chiffrement certifiés FIPS fournis par OpenSSL.

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

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

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

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

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

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

Prise en charge des langues dans XenMobile

May 06, 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 les caractères étendus ainsi que les 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 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**	**Hébreu**
Apple iPhone/iPad												
Worx Home	X	X	X	X	X	X	X	X	X	X	X	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	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	X
WorxMail	X	X	X	X	X	X	X	X	X	X	X	X
WorxWeb	X	X	X	X	X	X	X	X	X	X	X	X
WorxNotes	X	X	X	X	X	X	X	X	X	X	X	X
WorxTasks	X	X	X	X	X	X	X	X	X	X	X	X
QuickEdit	X	X	X	X	X	X	X	X				
Windows Phone												
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.

Langue de l'interface utilisateur	**Chinois simplifié**	**Allemand**	**Français**	**Coréen**	**Portugais**
Console XenMobile	X	X	X	X	X

Le tableau suivant dresse la liste des langues du Moyen-Orient qui sont prises en charge pour chaque application. Un **X** indique que la fonctionnalité est disponible pour cette plate-forme.

App	**iOS**	**Android**	**Windows Phone**
Worx Home	X	X	
WorxMail	X	X	
WorxWeb	X	X	
WorxTasks	X	X	
WorxNotes	X	X	
QuickEdit	X	X	

Check-list d'installation

May 06, 2016

Cette check-list dresse la liste des prérequis et des paramètres nécessaires à l'installation de XenMobile 10. 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	

	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	

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.

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

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

	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	
	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	

	Configuration requise	Composant	Prendre note du paramètre
•	Notez le nom de domaine complet public de Worx Home.	Gateway NetScaler Gateway	

Problèmes connus

May 06, 2016

Vous trouverez ci-dessous les problèmes connus dans XenMobile 10.0.

Pour obtenir une liste des problèmes résolus dans cette version, consultez l'article http://support.citrix.com/article/CTX141722.

- Worx Home peut afficher des espaces réservés gris à la place d'icônes lorsqu'un appareil iOS est mis à jour de la version iOS 7 vers iOS 8, puis qu'il est redémarré. Il s'agit d'un problème de tiers. [#502879]
- 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]
- Vous ne pouvez pas effectuer d'appels SOAP checkUserPassword et addGroup dans la classe de groupe USER dans XenMobile 10. Les modifications apportées à l'API User apparaissent dans la base de données, mais pas sur les appareils. [#511551, #511822]
- Il n'est pas possible de modifier l'ordre de déploiement des ressources du groupe de mise à disposition à partir de la console Web XenMobile. Si vous souhaitez contrôler l'ordre de déploiement, renommez vos ressources de manière à suivre le protocole de déploiement utilisé par XenMobile : numérique (1, 2, 3,...), caractères alphabétiques en majuscule (A, B, C,...) et caractères alphabétiques en minuscule (a, b, c,...). Une ressource portant un nom commençant par 24 sera déployée avant une ressource dont le nom commence par WM et ces deux ressources seraient déployées avant une ressource dont le nom commence par tw. [#512566]
- SafeSearch est désactivé et défini sur modéré sur les appareils Windows Phone 8.1 lorsque la restriction Filtrer le contenu réservé aux adultes est activée. [#513605]
- Lorsque vous déployez des stratégies Windows 8.1 Tablet, avant que XenMobile reçoive confirmation par l'appareil que la stratégie a été exécutée, il se peut que les stratégies soient répertoriées dans l'onglet Déployé(e) dans Détails de l'appareil sur la console XenMobile. [#514749]
- Lors de la réinscription d'un appareil, l'inscription peut échouer si les utilisateurs se réinscrivent trop tôt après s'être désinscrits. [#516567]
- Parfois, lorsque des utilisateurs se réinscrivent dans Worx Home, XenMobile présente une session SSL mise en cache et l'écran d'inscription s'affiche de nouveau. Lorsque cela se produit, les utilisateurs doivent se réinscrire. [#517301]
- 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]
- Si vous configurez un paramètre ou une stratégie dans la console XenMobile au sein duquel/de laquelle vous chargez un fichier (certificat, PDF, police, etc.), et que vous affichez ultérieurement les détails de la stratégie ou du paramètre, le nom de fichier ne s'affiche pas. [#519552]
- XenMobile ne prend pas en charge l'authentification avec code PIN en mode de gestion des applications mobiles (MAM) sur iOS et Android. Si vous configurez ce mode en tant que mode par défaut dans la console XenMobile, les utilisateurs doivent entrer leurs informations d'identification à deux reprises dans Worx Home. [#519572]
- Si vous désactivez le groupe AllUsers en tant que groupe de mise à disposition dans la console XenMobile, les utilisateurs qui n'appartiennent à aucun groupe de mise à disposition ne peuvent pas inscrire d'appareil, mais peuvent ouvrir une session sur le Portail en libre-service . [#521393]
- Worx Home pour Windows Phone 8.x, en mode de gestion de la flotte mobile, prend uniquement en charge les

applications provenant de magasins publics lorsqu'elles sont déployées de façon facultative. Si ces applications sont ajoutées au groupe de mise à disposition approprié, elles ne s'affichent pas dans Worx Home. [#521524]

- La page d'informations sur le contrôle d'accès basé sur rôle (RBAC) s'affiche pour vous permettre de modifier le modèle d'administration par défaut. Quelles que soient les modifications que vous apportez au champ de modèle RBAC et à d'autres champs, ces modifications ne sont pas enregistrées dans le modèle d'administration. Le modèle d'administration ne peut pas être modifié. [#521540]
- Sur les appareils iOS, le provisioning du jeton SAML lorsque les utilisateurs s'inscrivent auprès de Worx Home et configurent leurs comptes ShareFile peut ne pas être synchronisé. Pour contourner le problème, les utilisateurs peuvent fermer leur session Worx Home et la rouvrir puis se connecter à l'application ShareFile de façon à déclencher une nouvelle demande de jeton SAML. [#521934]
- Sur la plupart des machines, lorsque les utilisateurs exécutant des appareils Android tapotent sur l'icône Menu, les options de menu Accepter et Refuser s'affichent, ce qui permet aux utilisateurs de continuer le processus d'inscription. Sur certains appareils exécutant des systèmes d'exploitation antérieurs à la version 4.0, tels que le Samsung Tablet GT-P7510, l'icône Menu ne s'affiche pas sur la page Termes et conditions dans l'affichage par défaut, et les utilisateurs ne peuvent pas terminer le processus d'inscription. Pour contourner le problème, vous pouvez exclure le déploiement des termes et conditions sur ces appareils. [#524039]
- Worx Home sur des appareils iOS ne peut pas se connecter à Worx Store si le nom du magasin par défaut est modifié sur la page Balises de la console XenMobile (Configurer > Paramètres > Plus > Balises). Le paramètre par défaut est Magasin. Si ce paramètre est modifié, le service de découverte échoue lors d'ouverture de session et Worx Store ne peut pas être trouvé. Pour éviter ce problème, laissez le paramètre Nom du magasin dans la page Balises sur Magasin. [#523306]
- Dans une configuration XenMobile dotée d'un équilibrage de charge et du déchargement SSL, lorsque vous configurez des applications SAML, pour que le SSO fonctionne lorsque des utilisateurs installent WorxWeb et qu'ils ouvrent une application initiée par le fournisseur de services, toutes les références au serveur XenMobile doivent pointer vers le port 8443 au lieu du port 443. [#528680]
- Lorsque vous créez une stratégie de code secret Samsung KNOX et que vous configurez le paramètre Verrouiller l'appareil après (minutes d'inactivité), bien que le paramètre dans la console affiche des minutes en tant qu'unité, le serveur verrouille l'appareil après quelques secondes. [#531204]
- Vous ne pouvez pas configurer votre propre service SAML et fournisseur d'identité dans XenMobile 10 pour authentifier les utilisateurs et leurs appareils. [#530892]
- Vous ne pouvez pas ajouter un seul appareil BlackBerry ou Windows dans la console XenMobile. [#532844]
- Si vous configurez un jeton SAML avec le signe dièse (#) dans le nom, l'authentification unique (SSO) à partir de Worx Home ne fonctionne pas et un message d'erreur s'affiche. [#533078]
- Lorsque vous ajoutez une entité générique PKI (GPKI) dans la console XenMobile, vous ne pouvez pas tester la connexion à l'adaptateur de l'URL WSDL (Web Services Description Language) durant la configuration. [#533871]
- Les stratégies de mot de passe Windows Tablet ne prennent pas effet immédiatement sur les appareils et les nouvelles exigences en matière de longueur minimale du mot de passe ne sont pas toujours appliquées de façon uniforme. Il s'agit d'un problème de tiers. [#534088]
- Lorsque les utilisateurs inscrivent un appareil iOS en mode de gestion de la flotte mobile (MDM), les options de Sécurité disponibles dans la console XenMobile sur la page Gérer > Appareils qui permettent de localiser et suivre l'appareil n'apparaissent immédiatement. Les options apparaissent après un bref délai. [#534672]
- 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]
- Les applications ne s'affichent pas dans le Worx Store pour appareils iOS antérieurs à iOS 8 si vous entrez une valeur dans le champ Appareils exclus dans la console XenMobile lorsque vous ajoutez et configurez l'application. Pour

contourner le problème, vous pouvez configurer une règle de déploiement afin de spécifier les appareils autorisés à installer l'application. [#537631]

- Lorsque vous configurez des connexions NetScaler Gateway avec XenMobile sur un port autre que le port par défaut 443, l'inscription à la gestion d'applications mobiles (MAM) échoue sur les appareils iOS, tout comme Worx Home sur les appareils Windows. [#537368]
- Les caractères spéciaux tels que $, @ et " ne sont pas reconnus dans les mots de passe pour les 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]
- Une erreur de profil non valide se produit lorsque vous essayez de configurer le iOS Device Enrollment Program dans la console XenMobile. Il s'agit d'un problème de tiers. [#608213]

Vous trouverez ci-dessous les problèmes connus dans XenMobile Mail Manager 10.0.

- 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.

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 et la Check-list de pré-installation de XenMobile 10.
Remarque : assurez-vous que l'hyperviseur est configuré avec l'heure correcte car XenMobile utilise cette heure.
Prérequis XenServer ou VMware ESXi : avant d'installer XenMobile sur XenServer ou VMware ESXi, vous devez effectuer les opérations suivantes. Pour de plus amples informations, reportez-vous à votre documentation XenServer ou VMware.

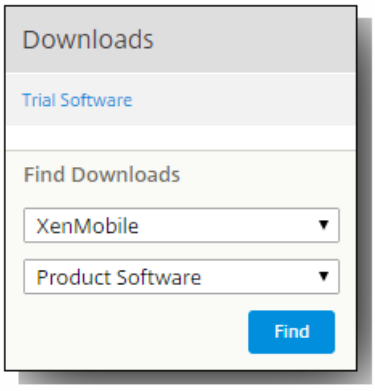
- Installez XenServer ou VMware ESXi sur un ordinateur doté des ressources matérielles appropriées.
- Installez XenCenter ou vSphere sur un autre ordinateur. L'ordinateur qui héberge XenCenter ou vSphere se connecte à l'hôte XenServer ou VMware ESXi via le réseau.

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

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

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

Vous pouvez télécharger le logiciel à partir du site Web de Citrix. Vous devez vous connecter au site puis cliquer sur le lien Downloads (Téléchargements) disponible sur la page Web Citrix. Vous pouvez ensuite sélectionner le produit que vous voulez télécharger. À titre d'exemple, la figure suivante affiche XenMobile et Product Software sélectionnés dans les listes :



Lorsque vous cliquez sur Find (Rechercher), une page répertoriant les téléchargements disponibles s'affiche avec la version la plus récente en haut de la liste. Vous pouvez sélectionner votre logiciel dans la liste des options disponibles.

Pour télécharger le logiciel pour XenMobile

1. Accédez au site Web Citrix.
2. Cliquez sur My Account (Se connecter) et connectez-vous.
3. Cliquez sur Downloads (Téléchargements).
4. Sous Find Downloads (Recherche de téléchargements), dans la liste des produits, cliquez sur XenMobile.
5. Dans Téléchargements de fichiers, sur la liste des types de téléchargements, sélectionnez Logiciel, puis cliquez sur Chercher.
6. Sur la page XenMobile Product Software, cliquez sur l'édition de XenMobile que vous voulez télécharger, c'est-à-dire XenMobile 10.0.
7. Sur la page XenMobile 10.0 App Edition, cliquez sur le bouton Download de l'image virtuelle appropriée pour installer XenMobile sur XenServer, VMware ou Hyper-V.
8. 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. Cliquez sur My Account (Se connecter) et connectez-vous.
3. Cliquez sur Downloads (Téléchargements).
4. Sous Find Downloads (Recherche de téléchargements), dans la liste des produits, cliquez sur NetScaler Gateway.
5. Dans Téléchargements de fichiers, sur la liste des types de téléchargements, sélectionnez Logiciel, puis cliquez sur Chercher.
   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.
6. Sur la page NetScaler Gateway, développez 10.5(4).
7. Cliquez sur la version du logiciel d'appliance que vous voulez télécharger.
8. 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.
9. Suivez les instructions affichées à l'écran pour télécharger le logiciel.

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

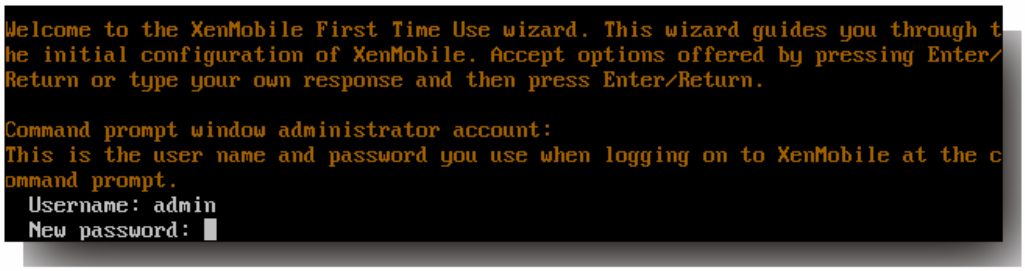
1. Configurez l'adresse IP et le masque de sous-réseau, la passerelle par défaut et les serveurs DNS pour XenMobile à l'aide de la console de ligne de commande de XenCenter ou de vSphere.
2. Ouvrez une session sur la console de gestion XenMobile et suivez les étapes des écrans d'ouverture de session.

Remarque

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

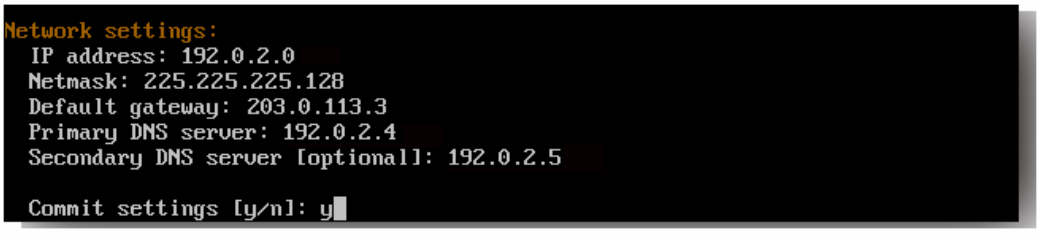
Configuration de XenMobile dans la fenêtre d'invite de commande

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 console de l'hyperviseur, créez un compte d'administrateur pour XenMobile dans la fenêtre d'invite de commandes.



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 suivantes :
   1. Adresse IP
   2. Masque réseau
   3. Passerelle par défaut
   4. Serveur DNS principal
   5. Serveur DNS secondaire (facultatif)



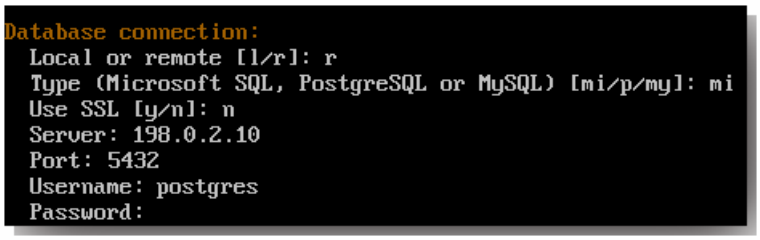
Remarque : les adresses illustrées dans cette image ne sont pas réelles et sont fournies uniquement à titre d'exemple.

5. Typey pour renforcer la sécurité en générant une phrase secrète 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. Le phrase secrète ne peut pas être affichée.

Remarque : si vous avez l'intention d'étendre votre environnement et de 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. Configurez la connexion à la base de données. Votre base de données peut être locale ou distante. Lorsque vous êtes invité à faire un choix entre Locale ou distante, tapezr oul.
   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.



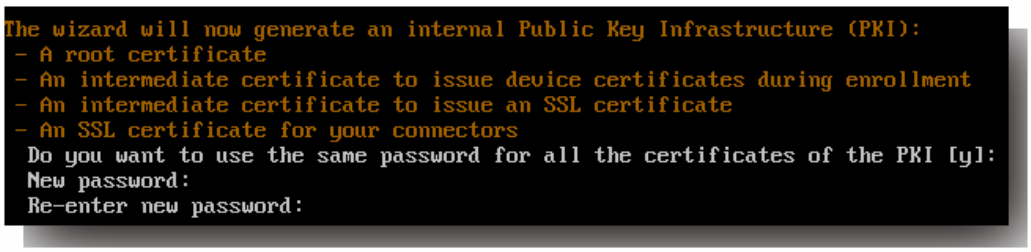
   Important : le port par défaut pour PostgreSQL est 5432.

   Remarque : les adresses illustrées dans cette image ne sont pas réelles et sont fournies uniquement à titre d'exemple.
8. Fournissez le nom de domaine complet (FQDN) du serveur hébergeant XenMobile. Ce serveur hôte fournit à lui seul les services de gestion des appareils et des applications.

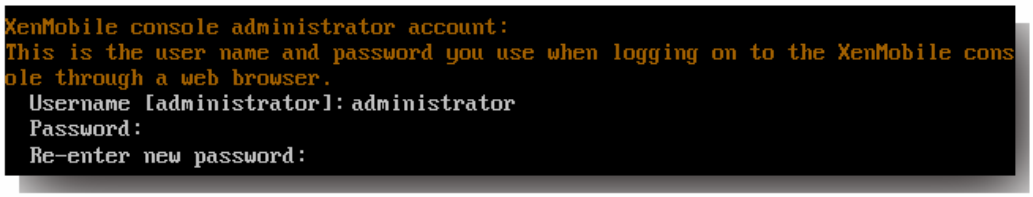
   Important : vous ne pourrez pas modifier le nom de domaine complet sans réinstaller complètement le serveur.

9. 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).

10. Vous êtes invité à fournir des mots de passe pour tous les certificats de serveur PKI. Vous pouvez choisir le même mot de passe pour chaque certificat. 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 devrez fournir les mêmes mots de passe pour chaque nœud.



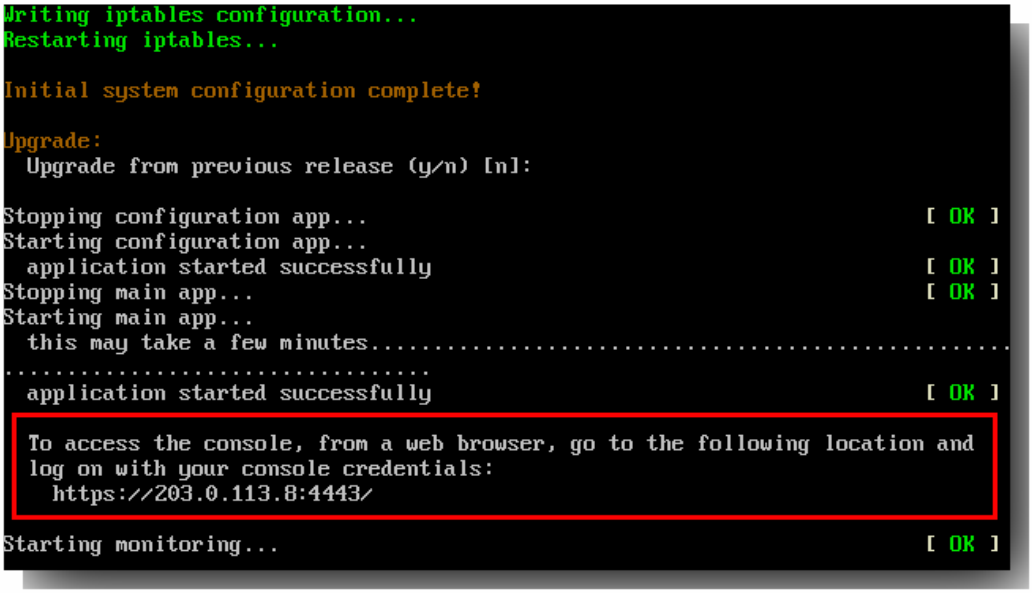
    Remarque : aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe. Rien ne s'affiche.
11. Créez un compte d'administrateur pour la connexion à la console XenMobile avec un navigateur Web. Retenez bien ces informations d'identification car vous devrez les réutiliser ultérieurement.



    Remarque : aucun caractère, par exemple un astérisque, ne s'affiche lorsque vous entrez le nouveau mot de passe. Rien ne s'affiche.
12. Lorsque vous êtes invité à indiquer si vous procédez à une mise à niveau, tapezn car il s'agit d'une nouvelle installation.

13. Copiez l'URL complète qui s'affiche sur l'écran et continuez la configuration initiale de XenMobile dans votre navigateur

Web.



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.
   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 : le certificat d'écoute SSL requiert 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.
   Ressources : 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.
   Remarque : 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.

Configuration de FIPS avec XenMobile

May 06, 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

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.

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.

Outil de mise à niveau de XenMobile 10 MDM

May 06, 2016

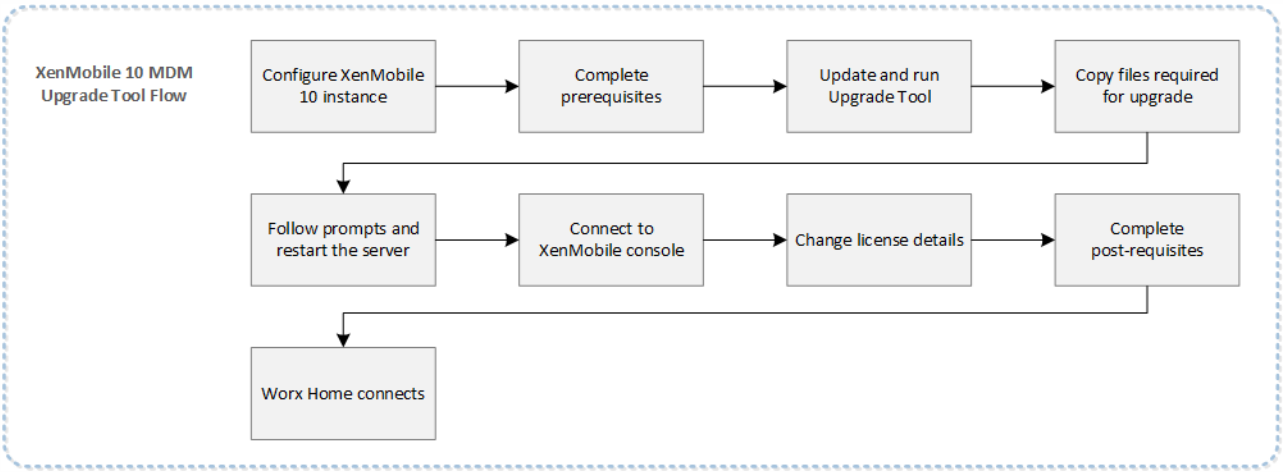
> ## Remarque
>
> Citrix vous recommande d'utiliser la dernière version de l'outil de mise à niveau. La dernière version disponible vous permet de mettre à jour les modes MAM, MDM et Enterprise de votre environnement XenMobile 9.0 à l'aide d'un seul outil. Vous pouvez télécharger l'outil de mise à niveau depuis la page de téléchargements de Citrix.com.

Utilisez l'outil de mise à niveau XenMobile 10 MDM pour mettre à niveau XenMobile 9.0 vers XenMobile 10. L'outil est pris en charge pour les mises à niveau des déploiements de l'édition XenMobile MDM.

Important : l'utilisation de l'outil de mise à niveau pour les éditions XenMobile App ou XenMobile Enterprise n'est pas pris en charge. De même, vous ne pouvez pas utiliser l'outil de mise à niveau pour passer de XenMobile 8.6 ou 8.7 à XenMobile 10. En outre, si la console Multi-Tenant console (MTC) est activée sur XenMobile 9.0, la MTC ne peut pas être migrée vers XenMobile 10.
Si votre installation XenMobile 9.0 est basée sur des instances SQL nommées, vous devez suivre les étapes spécifiques à cette situation. Pour de plus amples informations, consultez la section Prise en charge des instances SQL nommées.

L'outil de mise à niveau est intégré à la machine virtuelle XenMobile 10. Vous activez l'assistant à usage unique via la console de ligne de commande lors de l'installation initiale de XenMobile 10.

Le diagramme suivant illustre les étapes de base nécessaires pour effectuer la mise à niveau de XenMobile 9.0 vers XenMobile 10.



Consultez Conditions préalables et Problèmes connus avant de démarrer la migration vers XenMobile 10.

L'outil de mise à niveau XenMobile 10 MDM permet de migrer la configuration et les données de l'utilisateur d'un serveur XenMobile 9.0 vers une nouvelle instance de XenMobile 10 avec le même nom de domaine complet (FQDN).

Vous pouvez choisir de tester la mise à niveau ou d'effectuer une mise à niveau complète de l'environnement de production. Lorsque vous choisissez Test Drive dans l'outil, seules les données de configuration sont migrées vers XenMobile 10 ; aucune donnée utilisateur ou de l'appareil ne sont migrées. Cette option vous permet de comparer XenMobile 9.0 et XenMobile 10 sans affecter votre environnement de production.

Lorsque vous choisissez Production 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 après la mise à niveau, vous pouvez voir toutes les données utilisateur et de l'appareil qui ont été migrées depuis XenMobile 9.

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. XenMobile 9.0 reste inchangé jusqu'à ce que vous déplaciez le serveur XenMobile 10 dans l'environnement de production. Lorsque des utilisateurs sont connectés à XenMobile 10 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.
Après la réussite de la mise à niveau de l'environnement de production, pour passer XenMobile 10 en production, vous devez effectuer les opérations suivantes :

1. Mettre à jour l'entrée DNS pour mapper le nom de domaine complet (FQDN) XenMobile 9.0 sur la nouvelle IP du serveur XenMobile 10.
2. Si NetScaler répartit la charge des serveurs XenMobile Device Manager, vous devez basculer le service XenMobile 9.0 vers le service XenMobile 10.

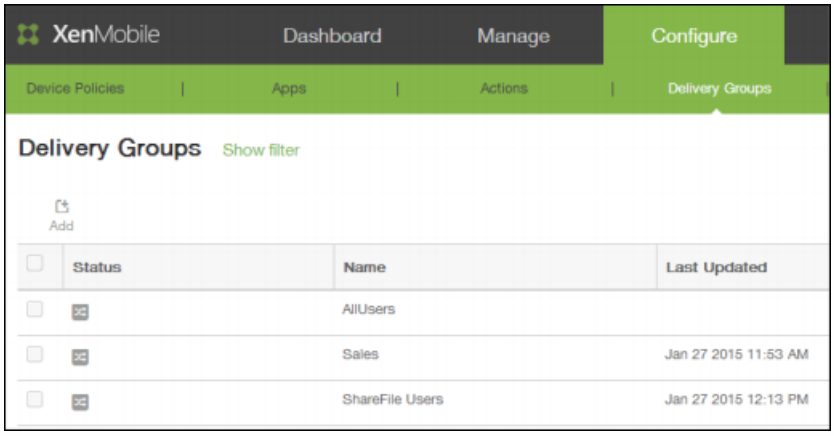
Lorsque vous utilisez l'outil de mise à niveau, les informations suivantes **ne sont pas** migrées vers XenMobile 10 :

- Les informations de licence.
- Les rapports de données.
- Les actions automatisées
- Les stratégies de groupes de serveurs et les déploiements associés.
- Le groupe MSP.
- 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 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 sont des paramètres de pare-feu que vous pouvez configurer dans l'interface de ligne de commande.

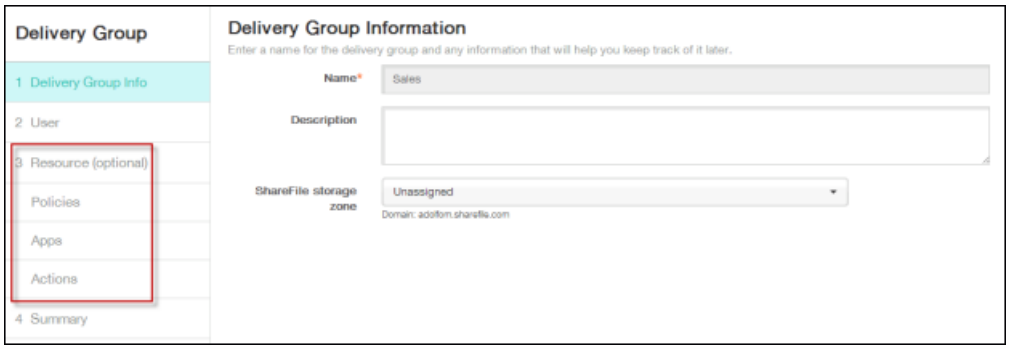
Veuillez également noter les nouveautés suivantes de XenMobile 10 :

- XenMobile 10 ne prend pas en charge les utilisateurs Active Directory qui sont assignés à des groupes locaux.
- La hiérarchie des groupes locaux est aplatie.

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



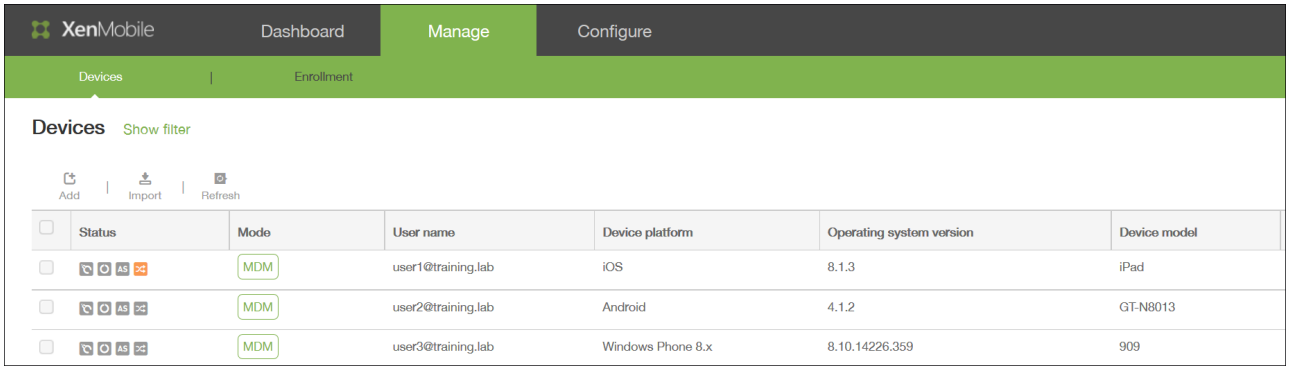
Dans le groupe de mise à disposition, vous pouvez voir les stratégies MDM, les actions et les applications requises par le groupe d'utilisateurs qui requiert des ressources.



Les utilisateurs n'ont pas besoin de réinscrire leurs appareils après la mise à niveau vers XenMobile 10. Les appareils doivent se connecter automatiquement au serveur XenMobile 10 en fonction de l'intervalle de pulsation.

Si vous souhaitez connecter immédiatement un appareil à XenMobile 10, 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 l'illustre la figure suivante.



Conditions préalables

May 06, 2016

Vous devez remplir les pré-requis suivants avant d'exécuter l'outil de mise à niveau de XenMobile 10 MDM.

Serveur de licences Citrix

Assurez-vous d'avoir installé la licence de serveur Citrix 11.12.1 (disponible sur la page Système de licences Citrix et d'avoir configuré le serveur avec la dernière licence exclusive MDM V6. Assurez-vous que les ports de serveur de licences 27000 et 7279 sont ouverts sur le serveur. Cette étape est primordiale pour empêcher la mise à niveau involontaire des appareils utilisateurs vers le mode XenMobile Enterprise, qui pourrait provoquer une violation de licence et également obliger les utilisateurs à réinscrire leurs appareils.

Base de données

La migration peut uniquement être effectuée entre bases de données de même type. Par exemple :

Prise en charge

- De PostgreSQL à PostgreSQL
- De MSSQL à MSSQL

Non pris en charge

- De MSSQL à PostgreSQL
- De PostgreSQL à MSSQL

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"
2. Ajoutez une nouvelle ligne host all all [XMS address/external address]/32 md5
3. Enregistrez le fichier.
4. Arrêtez et démarrez le service.
5. Recherchez et ouvrez le fichier postgresql.conf et changez cette ligne :

   "#listen_addresses = 'localhost'"

   sur

   "listen_addresses = '*'"

   Remarque : la ligne ne doit contenir aucune marque de commentaire. Cette opération peut être rendue restrictive en autorisant uniquement les adresses IP des serveurs XenMobile 9.0 et XenMobile 10 à accéder à la base de données PostgreSQL (listen_addresses = '10.x.x.1,10.x.x.2').
6. Arrêtez et redémarrez le service PostgreSQL pour que les modifications prennent effet.
7. Assurez-vous que XMS et la base de données peuvent communiquer. (Cela vérifie également que la base de données peut accepter les connexions distantes.)

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 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 fichier pki.xmlavant de démarrer la migration pour vous assurer que le certificat SSL remplit ces conditions.

Nom d'utilisateur du compte d'administrateur

Le compte d'administrateur utilisé pour se connecter à la console XenMobile 10 peut contenir uniquement des lettres ; vous ne pourrez pas vous connecter à la console XenMobile 10 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.

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 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. 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.

Copier des fichiers depuis XenMobile 9.0 Device Manager

En supposant que Device Manager est installé à l'emplacement par défaut (C:\Program Files (x86)\Citrix XenMobile Device Manager\tomcat), copiez les fichiers suivants dans un dossier temporaire :

Depuis le dossier C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\conf :

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

Remarque : si des certificats de serveur SSL personnalisés (.p12) ont été utilisés sur le serveur exécutant Device Manager, vérifiez d'avoir copié ce certificat à la place de https.p12 dans le dossier temporaire.
Depuis le dossier C:\Program Files (x86)\Citrix\XenMobile Device Manager\tomcat\webapps\zdm\WEB-INF\classes\, copiez les fichiers suivants dans le même dossier temporaire :

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

Après avoir copié tous ces fichiers, ouvrez le dossier temporaire et compressez les fichiers ; ne compressez pas le dossier, seulement les fichiers. Les fichiers compressés seront chargés lors de la mise à niveau.

Après avoir passé en revue les problèmes connus et rempli toutes les conditions préalables, démarrez la mise à niveau. Pour de plus amples informations, consultez la section Activation et exécution de l'outil de mise à niveau de XenMobile 10 MDM.

Problèmes connus

May 06, 2016

Vous trouverez ci-dessous les problèmes connus de l'outil de mise à niveau de XenMobile 10 MDM :

- La valeur du nombre limite de verrouillage de XenMobile n'est pas migrée. Réinitialisez la valeur après la migration. [#545770]
- Les options de rôles RBAC (contrôle d'accès basé sur un rôle) ne sont pas migrées correctement. Après la migration, examinez les rôles RBAC et apportez les modifications nécessaires. [#543183]
- Les paramètres de journal ne sont pas migrés. Après la migration, configurez à nouveau les paramètres de journal dans la console XenMobile. [#541869]
- Lorsqu'une configuration comportant plusieurs configurations LDAP dans laquelle seule une configuration LDAP prenant en charge les groupes imbriqués est migrée, la prise en charge des groupes imbriqués est activée sur tous les LDAP que vous avez configurés après la migration. En outre, la synchronisation des groupes se produit sur tous les serveurs LDAP lors du démarrage du serveur. [#540713]
- Lorsqu'une stratégie de filtre de contenu Web contient des URL sans HTTP/HTTPS, l'adresse URL est supprimée lorsque les utilisateurs modifient l'adresse URL puis annulent l'opération. Après la migration, vérifiez que toutes les adresses URL contiennent HTTP ou HTTPS pour empêcher la suppression lors de l'annulation d'une modification. [#540025]
- Lorsque des stratégies, des applications ou des actions sont incluses dans plusieurs paquetages avec des règles différentes, les règles de déploiement ne sont pas migrées. Ce comportement est normal. [#539517]
- L'administrateur XenMobile 9.0 ne peut pas se connecter à la console XenMobile 10 après une migration réussie si le nom d'utilisateur de l'administrateur contient une majuscule. Avant la migration, créez un compte d'utilisateur administrateur contenant 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. [#547422]
- Si la console Multi-Tenant Console (MTC) est activée sur XenMobile 9, MTC ne peut pas être migrée vers XenMobile 10. [#549969]
- Plusieurs des paramètres et autorisations du rôle de super administrateur crée dans XenMobile 9.0 ne sont pas migrées vers XenMobile 10. Après la migration, dans la console XenMobile 10, cliquez sur Configurer > Paramètres > Contrôle d'accès basé sur rôle et recréez le rôle de super administrateur XenMobile 9.0 avec les autorisations du rôle administrateur de XenMobile 10. [#553079]
- Les noms des paquetages de déploiement créés dans XenMobile 9.0 avec des caractères spéciaux (!, $(),#,%, +,*, ~,?, |,} {, []) 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. 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. [#538639]

Activation et exécution de l'outil de mise à niveau de XenMobile 10 MDM

May 06, 2016

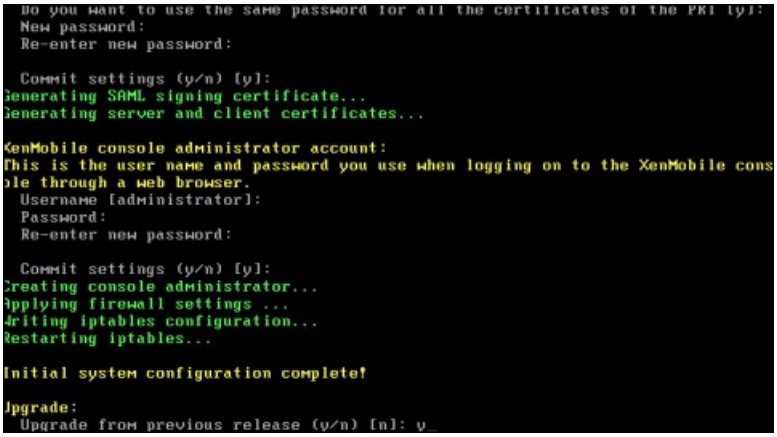
Les étapes suivantes sont les étapes de base à suivre pour mettre à niveau XenMobile 9.0 vers XenMobile 10 :

1. Configurez l'instance XenMobile 10 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. Mettez à jour l'outil de mise à niveau vers la version la plus récente.
   Important : effacez le cache de votre navigateur après le redémarrage du système.
4. Démarrez l'outil de mise à niveau dans Firefox ou Chrome.
5. Téléchargez les fichiers copiés XenMobile 9.0 dans l'outil de mise à niveau.
6. Entrez le mot de passe du certificat XenMobile 9.0.
7. Autorisez l'exécution de l'outil de mise à niveau.
8. Redémarrez le serveur XenMobile 10.
9. Ouvrez une session sur la console XenMobile 10.
10. Configurez des licences sur XenMobile 10 pour autoriser les utilisateurs à se connecter.
11. Pour mettre à niveau un environnement de production, modifiez le DNS externe XenMobile pour pointer vers le nouveau serveur XenMobile 10.
12. Pour mettre à niveau un environnement de production si vous utilisez l'équilibrage de charge NetScaler, supprimez l'IP du serveur XenMobile 9.0 puis ajoutez l'IP du serveur XenMobile 10.

Pour installer une instance de XenMobile 10 et activer l'outil de mise à niveau

Activez l'outil de mise à niveau à l'aide de la console de ligne de commande lors de l'installation initiale de XenMobile 10, comme illustré dans la figure suivante.

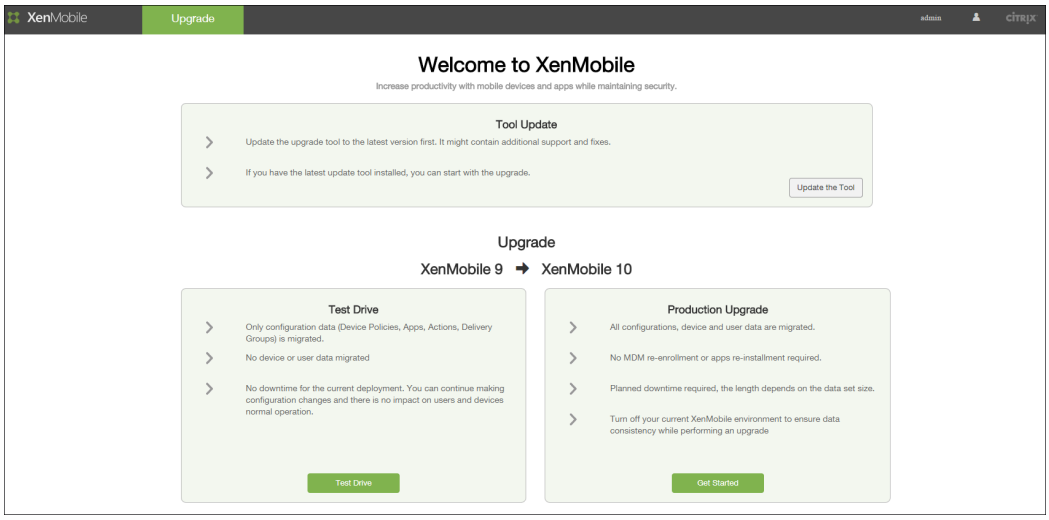
Important : si vous voulez prendre un instantané de votre système, faites-le après la configuration initiale de XenMobile 10 et *avant* d'accéder à l'outil de mise à niveau.



Si vous tapez **y** pour la mise à niveau, XenMobile 10 active l'outil de mise à niveau. Ensuite, vous pouvez accéder à l'outil de mise à niveau via https:///uw/.

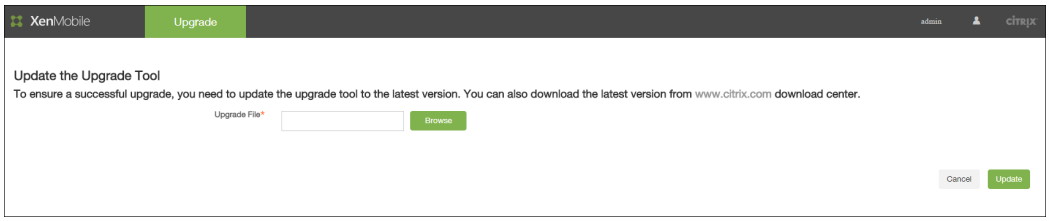
Conseil : Citrix vous recommande d'utiliser Firefox ou Chrome pour accéder à l'outil de mise à niveau ; Internet Explorer n'est

pas recommandé.
Lorsque vous migrez vers le nouveau serveur, assurez-vous que le nom d'hôte du nouveau serveur correspond au nom d'hôte du serveur à partir duquel vous effectuez la migration. Cela garantit que Worx Home peut se connecter avec le même nom d'hôte à XenMobile 10 que celui que Worx Home utilisait pour se connecter à XenMobile 9.0. Dans ce cas, les utilisateurs n'ont pas besoin de se réinscrire auprès de XenMobile 10.



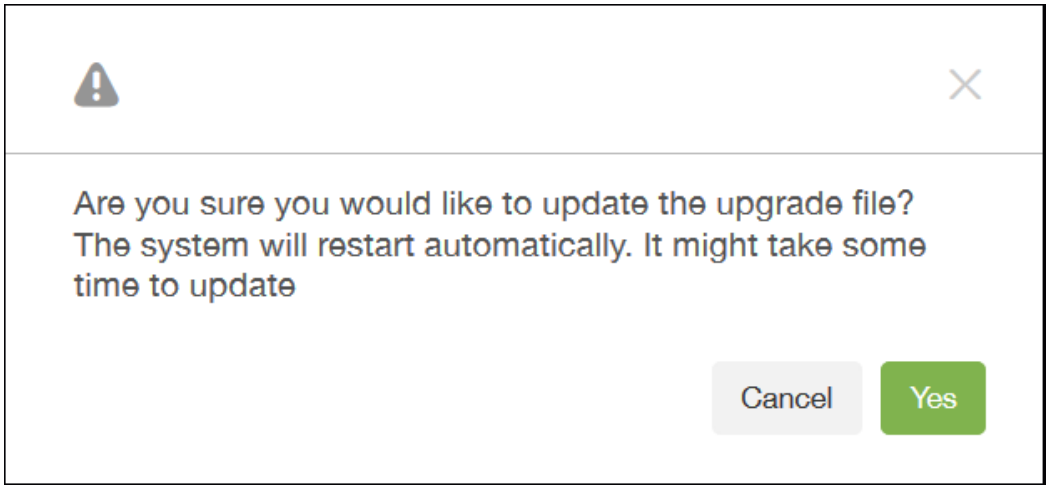
Pour mettre à jour l'outil de mise à niveau et commencer la migration

Vous trouverez des mises à jour de l'outil de mise à niveau sur la page de téléchargement de XenMobile. Pour les migrations MDM, utilisez la dernière version de l'outil à télécharger sur Citrix.com.



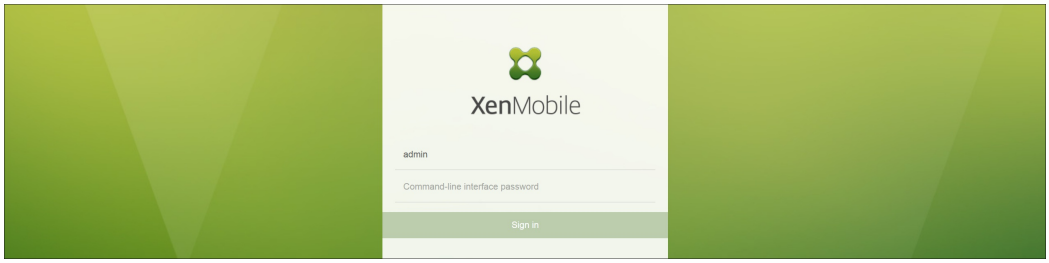
Le message suivant s'affiche pour confirmer le début du processus de mise à jour.

Remarque : après avoir cliqué sur Yes, vous ne verrez pas d'indicateur de progression, mais vous pouvez regarder l'interface de ligne de commande pour voir lorsque le système redémarre. La mise à jour devrait prendre approximativement 30 secondes.

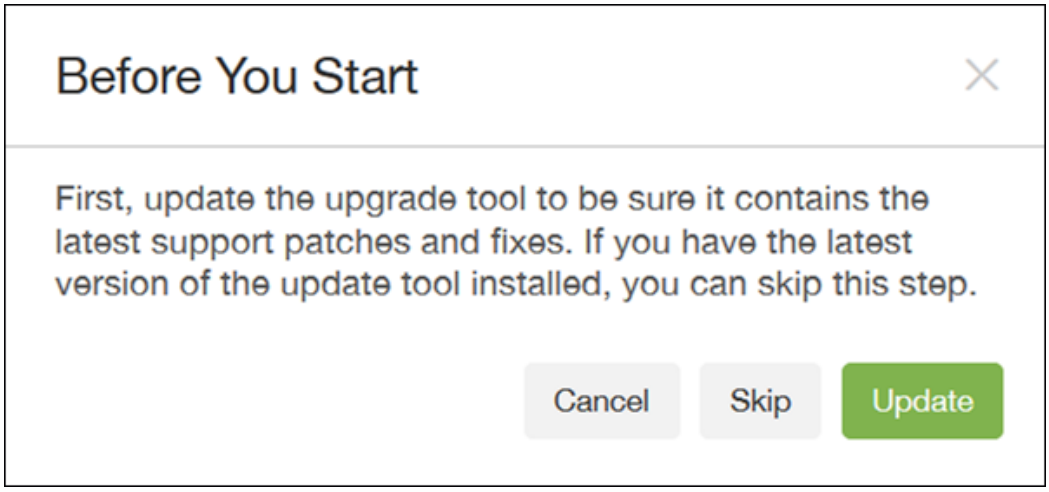


Remarque :

- Une fois le système redémarré, effacez le cache de votre navigateur avant d'accéder à nouveau à l'URL de l'outil de mise à niveau, https:///uw.
- Si vous n'utilisez pas le port par défaut pour la communication HTTPS (443), l'URL de l'outil de mise à niveau est https://:/uw.



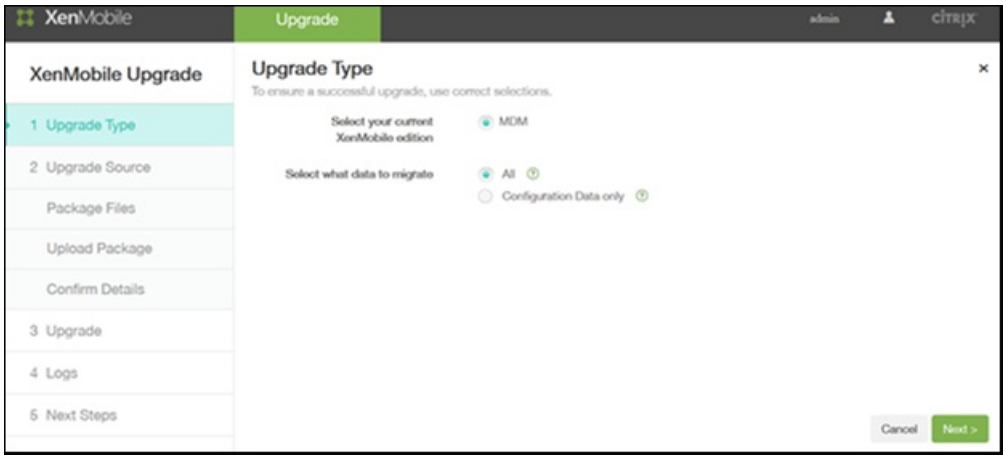
Dans ce cas, après avoir ouvert une session sur l'outil de mise à niveau, vous pouvez cliquer sur **Skip**, car vous avez déjà mis à jour l'outil de mise à niveau.



Sélectionnez Test Drive ou Production Upgrade puis procédez à la migration.

Une fois l'outil de mise à niveau ouvert, vous pouvez choisir d'effectuer la migration de toutes les données ou uniquement des données de configuration. Si vous choisissez Configuration Data only, les utilisateurs doivent réinscrire leurs appareils.

Cliquez sur Next pour charger les fichiers que vous avez copiés et compressés dans le dossier temporaire.

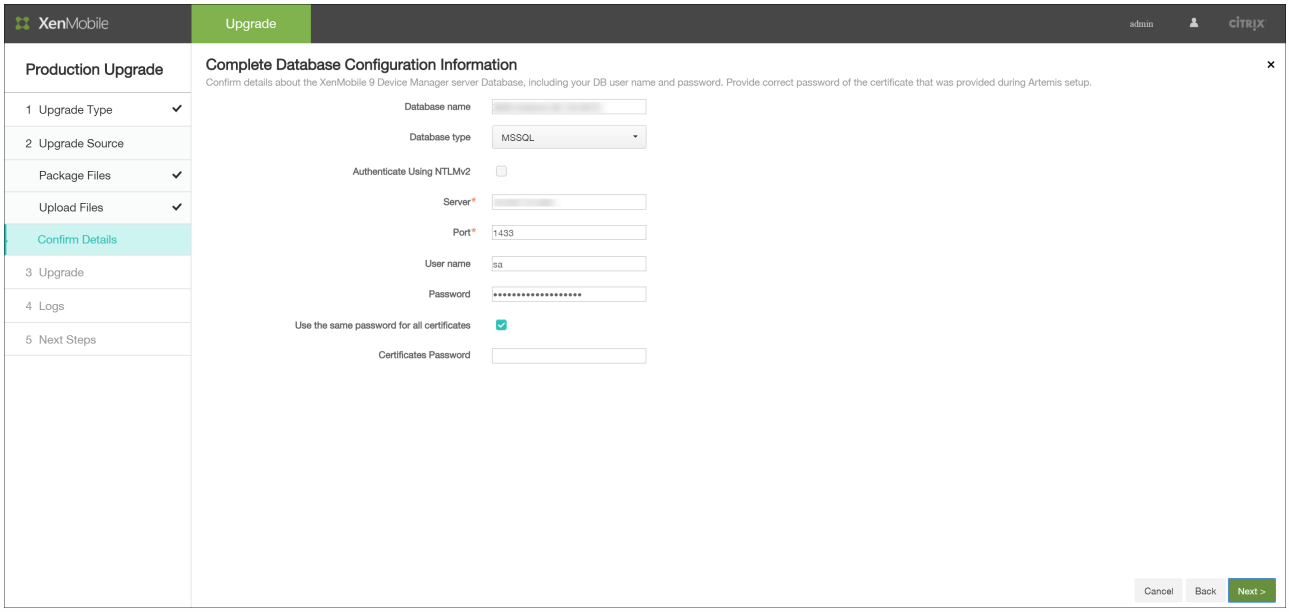


Cliquez sur Next une fois le chargement terminé.

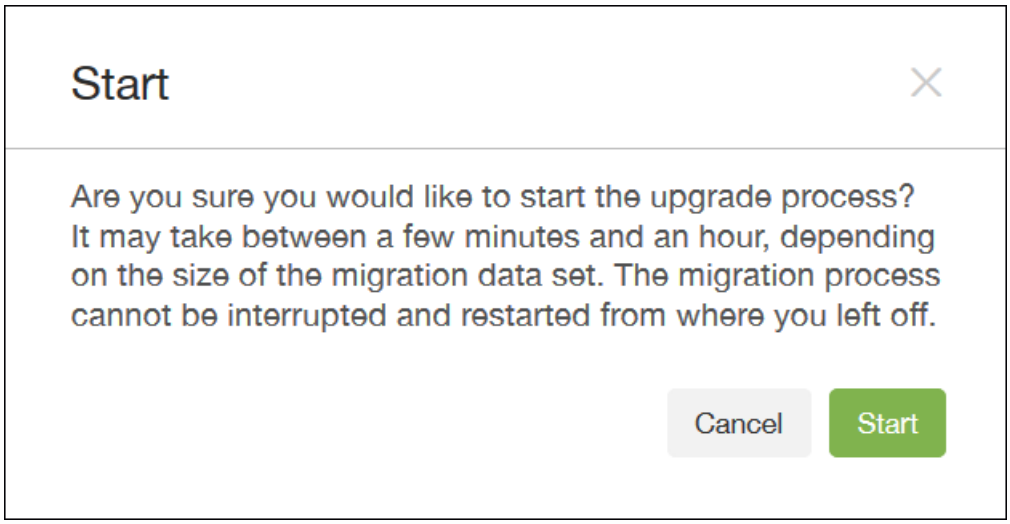
Lorsque vous migrez une base de données PostgreSQL et que le nom du serveur est « localhost », vous devez remplacer « localhost » par l'adresse IP du serveur.

Vérifiez que les informations collectées depuis XenMobile 9.0 Device Manager 9.0 sont correctes. Vous devez également entrer le mot de passe du certificat.

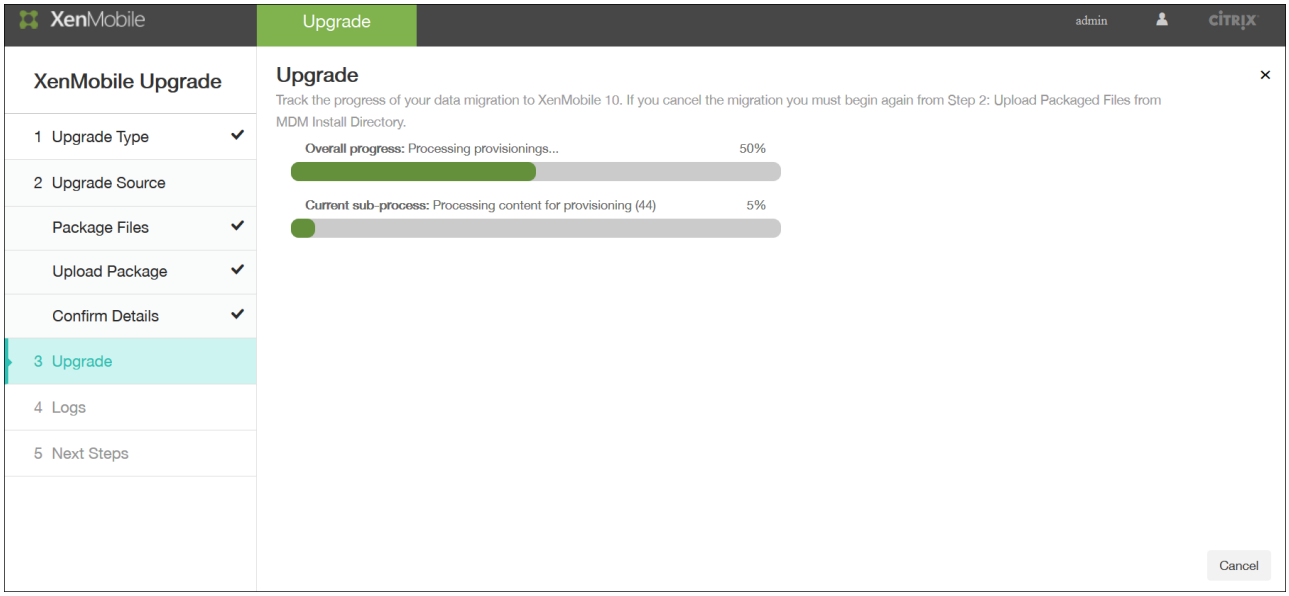
Important : tous les mots de passe des certificats doivent être entrés correctement ou la migration échouera.

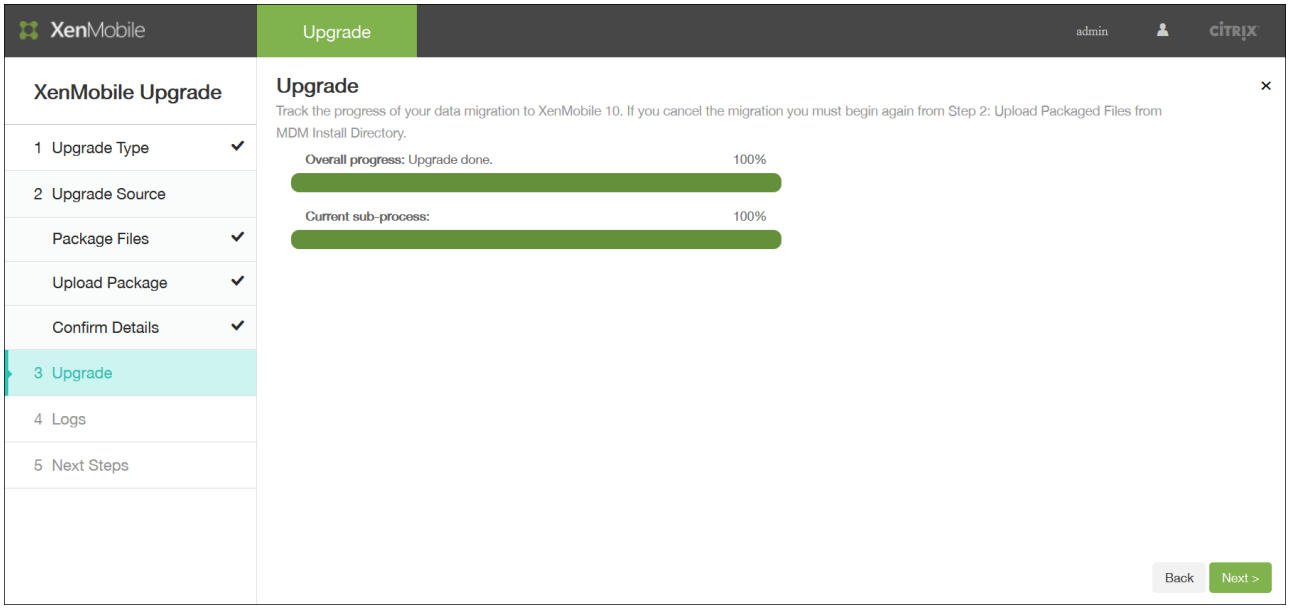


Lorsque vous cliquez sur Next, le message de confirmation suivant s'affiche.



Puis, la page Upgrade affiche des indicateurs de progression pour vous permettre d'effectuer le suivi de la migration des données depuis XenMobile 9.0.



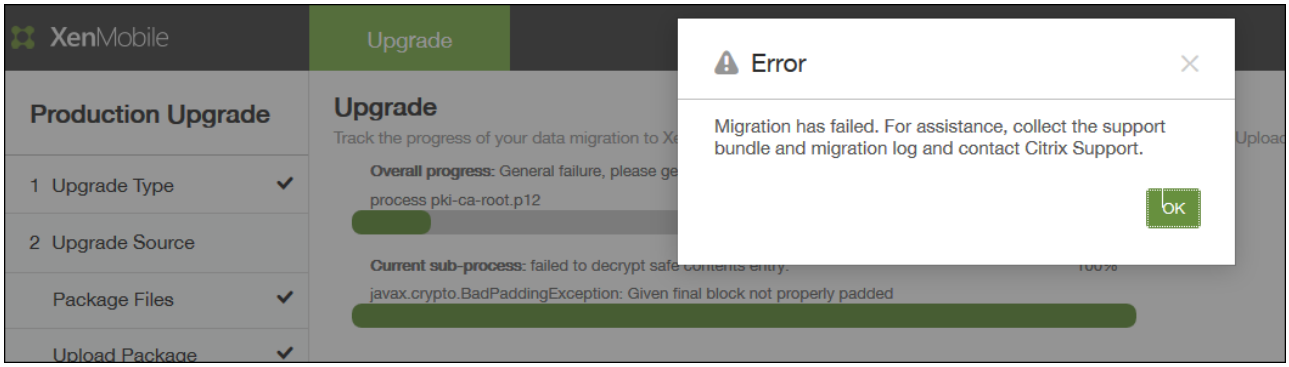


Si vous n'avez pas copié tous les fichiers Device Manager requis dans le dossier.zip, l'outil de mise à niveau affiche le ou les fichiers manquants. Ensuite, l'outil reprend après vous ayez ajouté le ou les fichiers manquants.

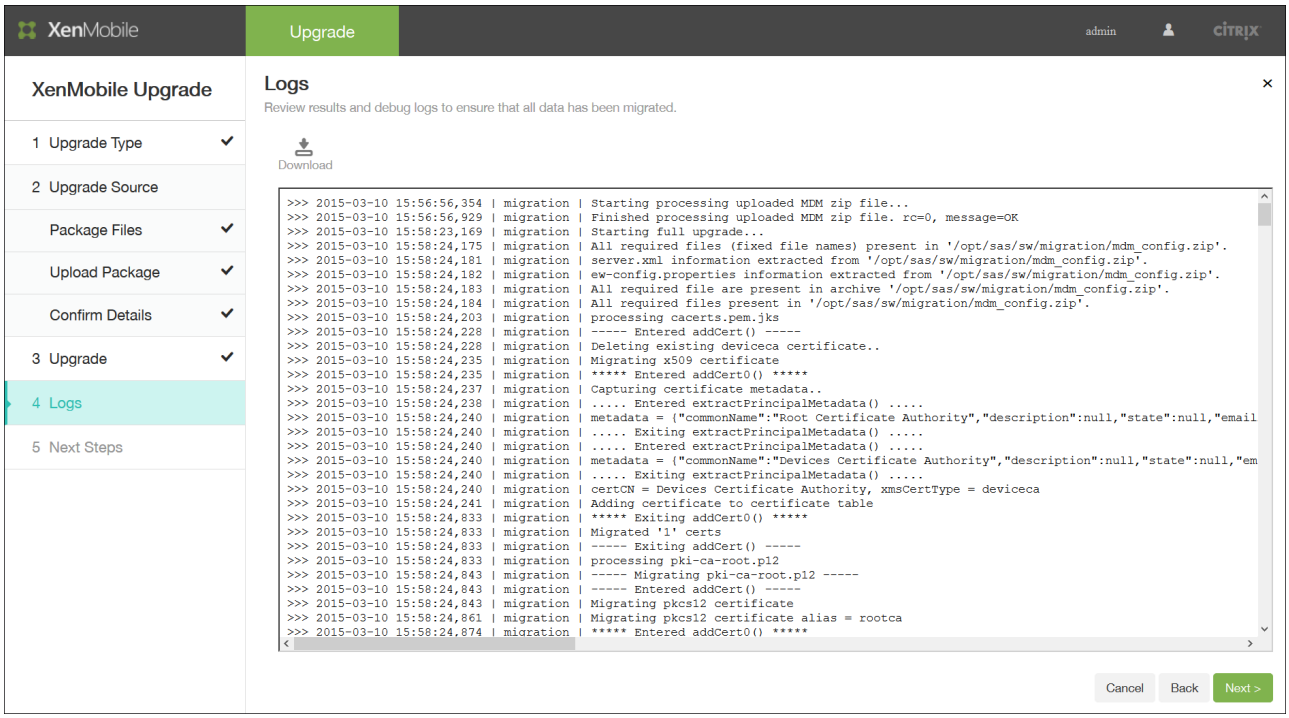
Si vous ne pouvez pas résoudre un problème, un message d'erreur s'affiche vous indiquant de générer un pack d'assistance XenMobile, de collecter le journal de migration et de contacter le support technique Citrix.

Remarque :

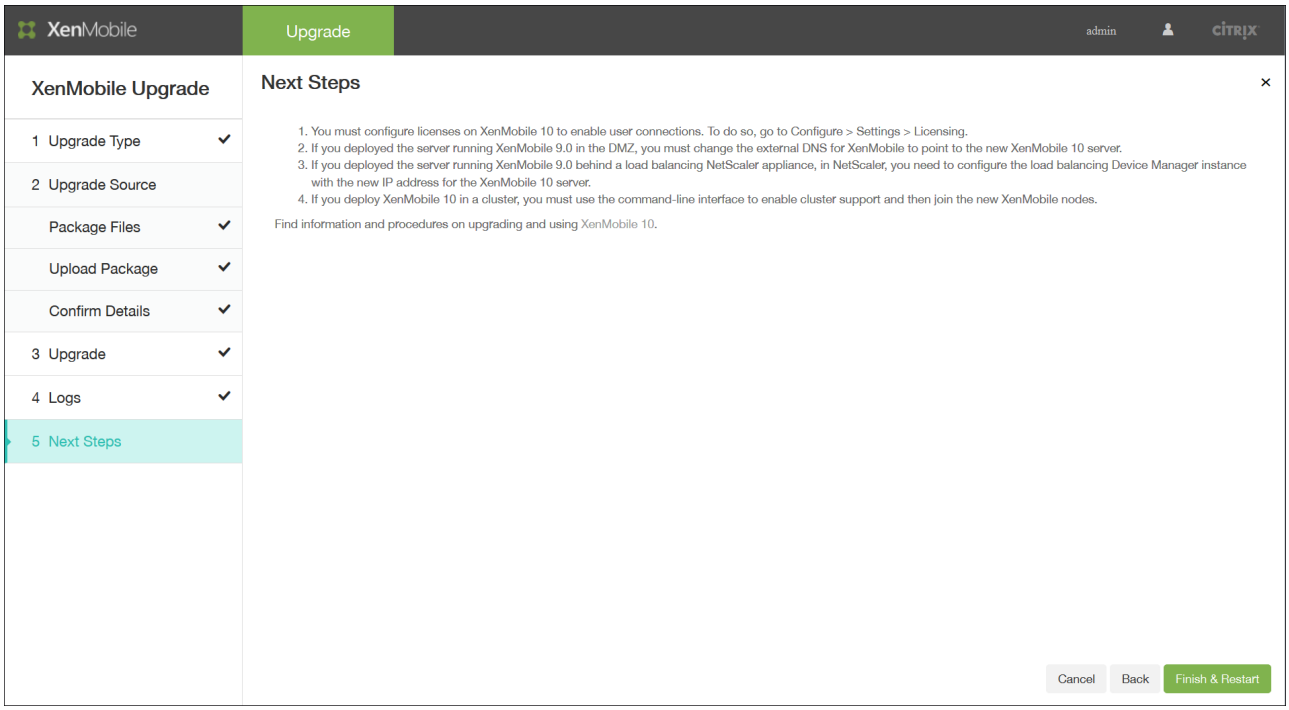
- Si la migration échoue, vous devez importer une nouvelle instance XenMobile 10 et recommencer la migration.
- Une fois la migration terminée (réussite ou échec), vous ne pourrez plus utiliser le bouton Back pour corriger ces informations. Vous devez importer une nouvelle instance XenMobile 10 et redémarrer la migration.

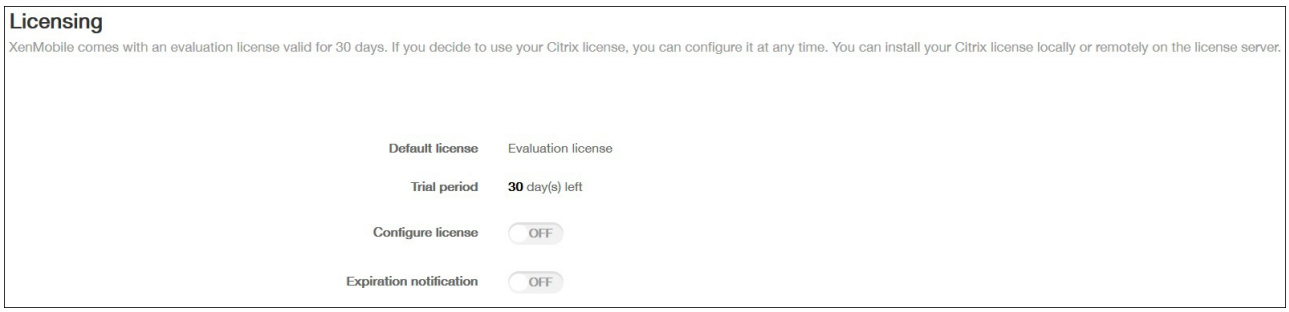


Lorsque vous mettez à niveau vers XenMobile 10, l'outil de mise à niveau XenMobile génère un fichier journal – migration.log – à télécharger et à consulter, comme le montre la figure suivante. Citrix vous recommande de consulter le fichier pour déterminer les stratégies, paramètres, données utilisateur et ainsi de suite qui ont été migrés ou non vers XenMobile 10.



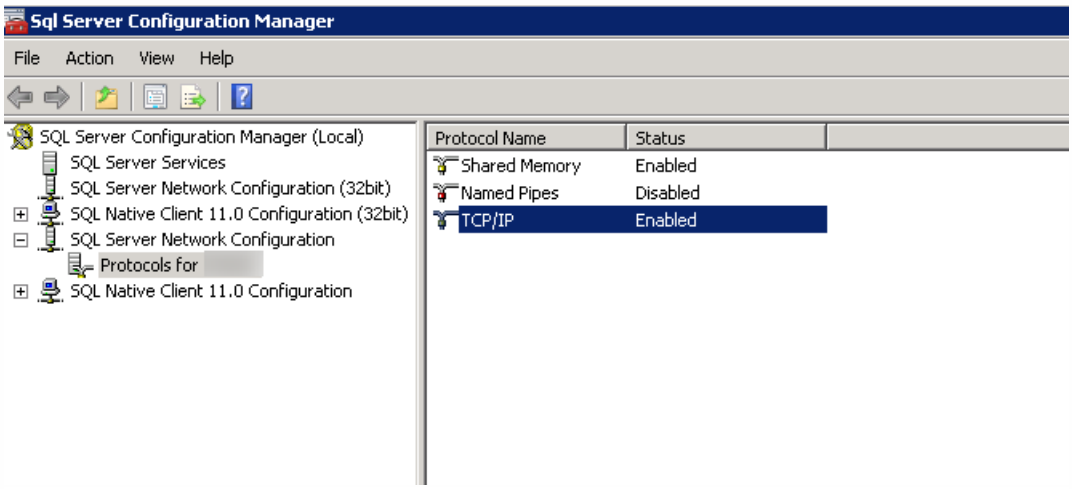
Après avoir téléchargé et consulté les journaux de migration, cliquez sur Next pour passer à la page suivante, Next Steps. Consultez la section Post-requis de l'outil de mise à niveau pour de plus amples informations.

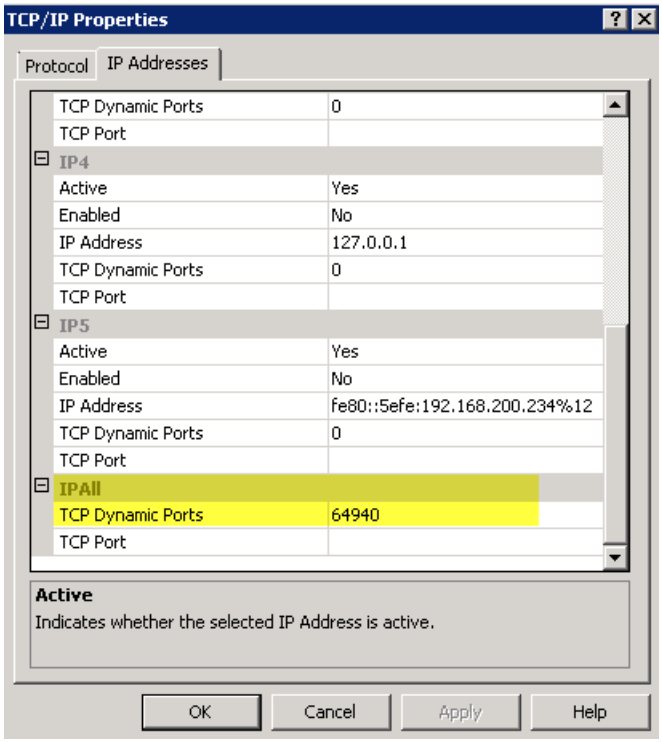




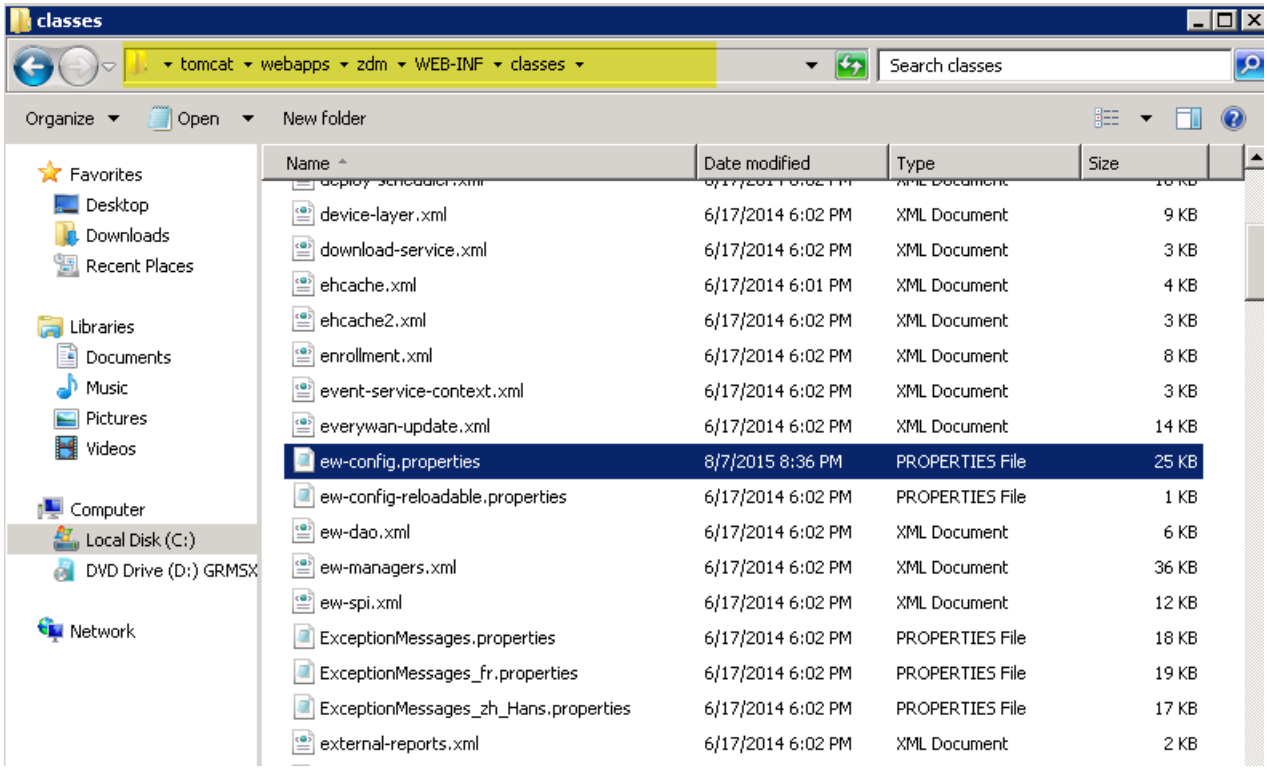
-
-
-
-
-
-
-
-
-

-
-
-





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

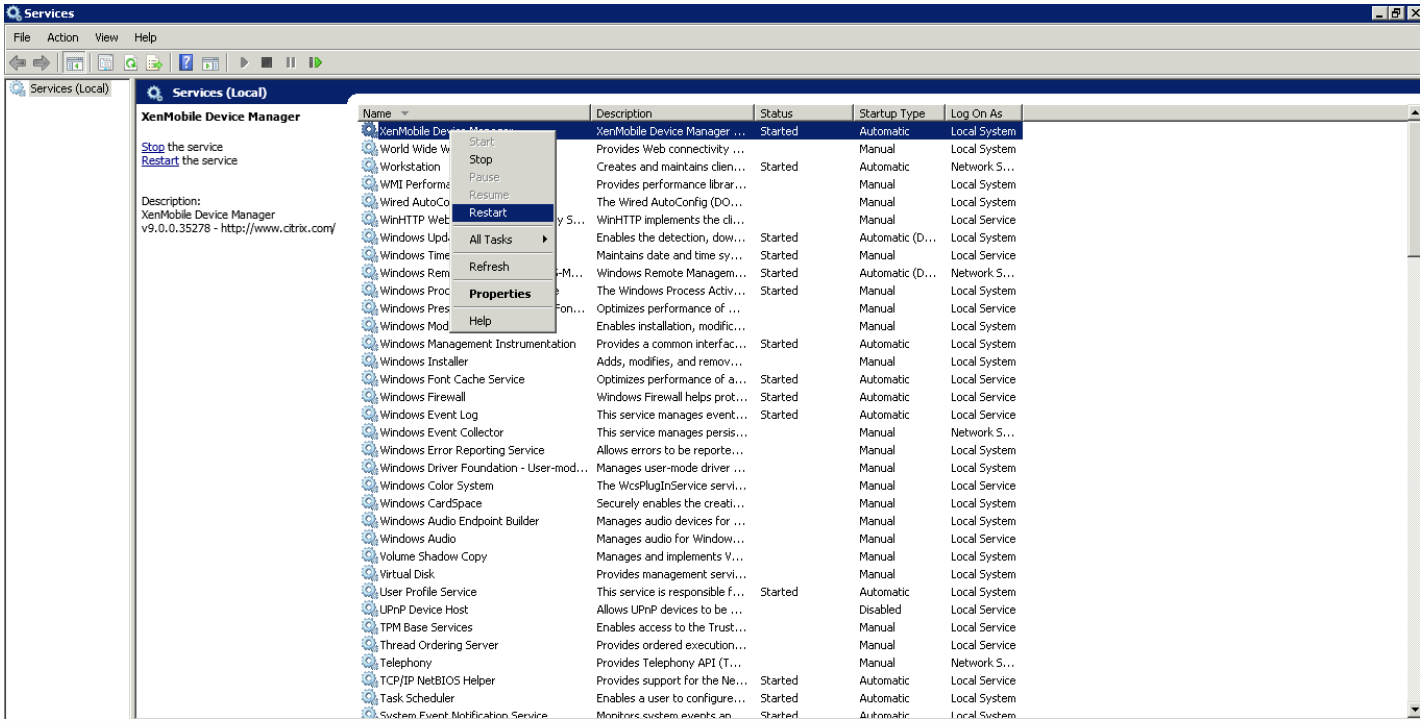


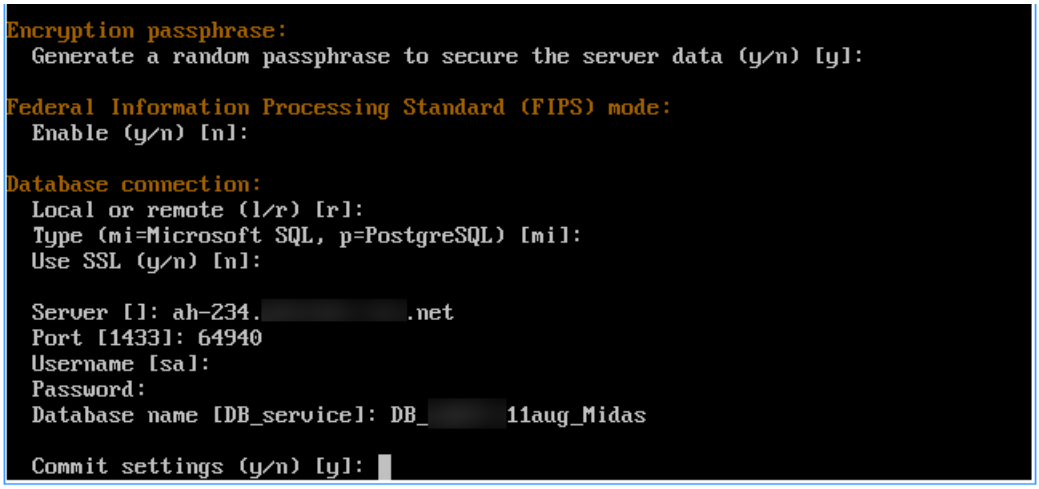
ew-config.properties

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

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

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

ew-config.properties

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

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

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



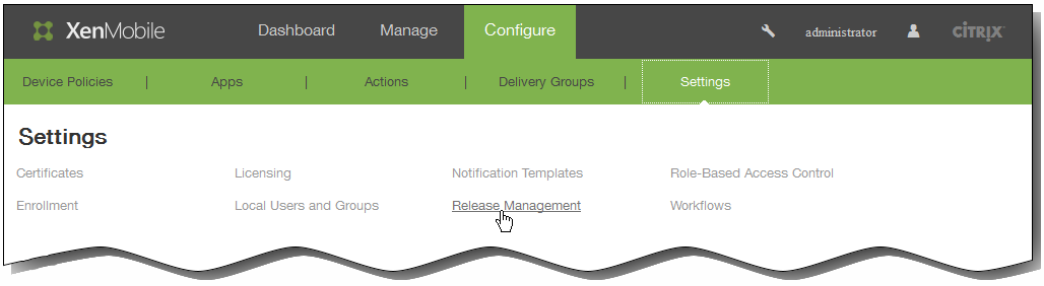


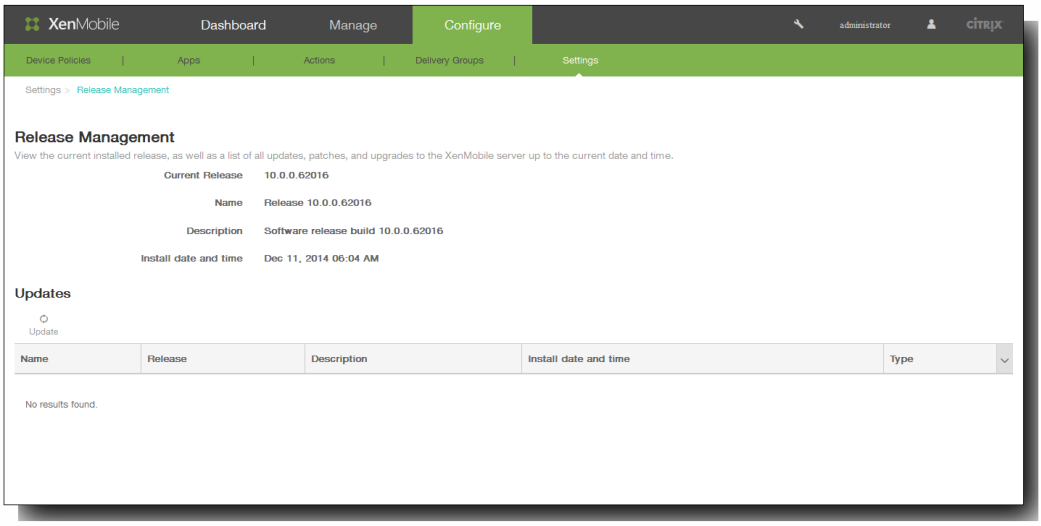
-
-

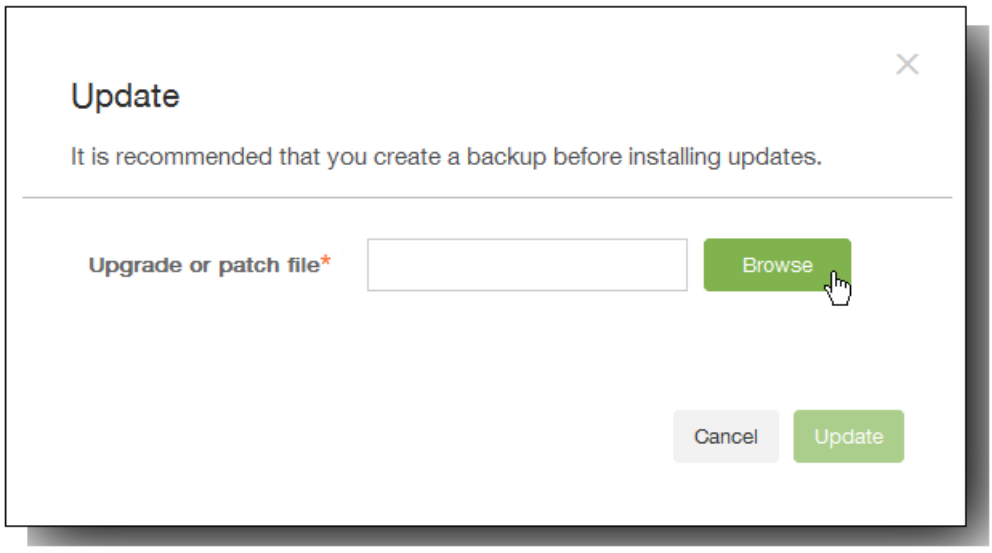
-
-
-

  -
  -
  -

Pour mettre à niveau XenMobile







-
-
-

-
-
-
-
-

Installation des nœuds de cluster XenMobile


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

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

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

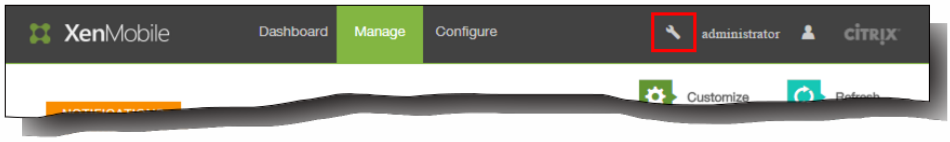
```
Federal Information Processing Standard (FIPS) mode:
  Enable (y/n) [n]:
```

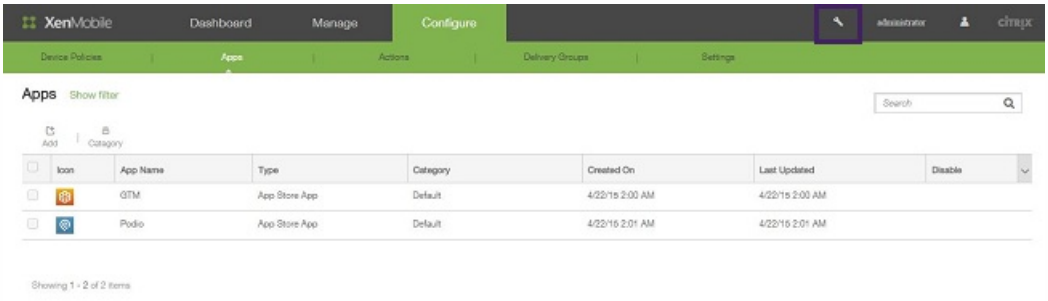
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

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

  Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..
```

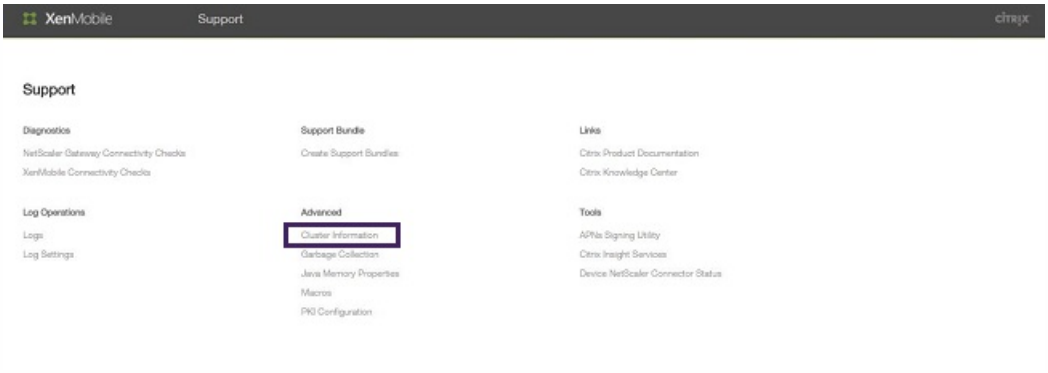
```
Database connection:
  Local or remote (l/r) [r]:
  Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
  Use SSL (y/n) [n]:

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

  Commit settings (y/n) [y]:

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

Saving server and client certificate passwords..

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

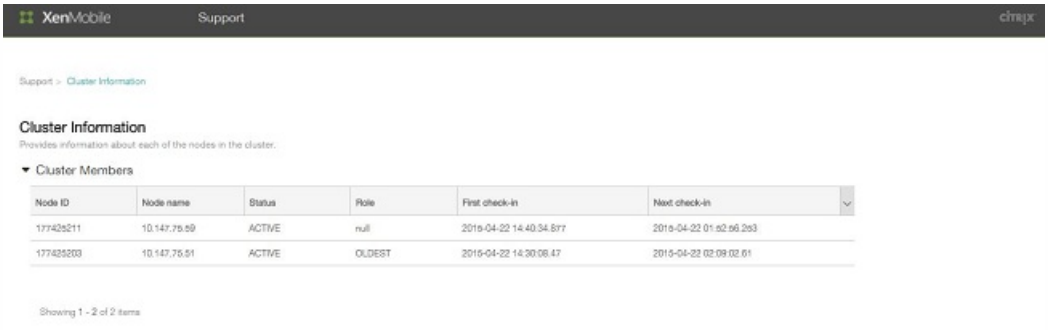
```
      Saving server and client certificate passwords..

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

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

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

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

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

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

Starting monitoring...                                           [ OK ]

xms51.wg.lab login:
```

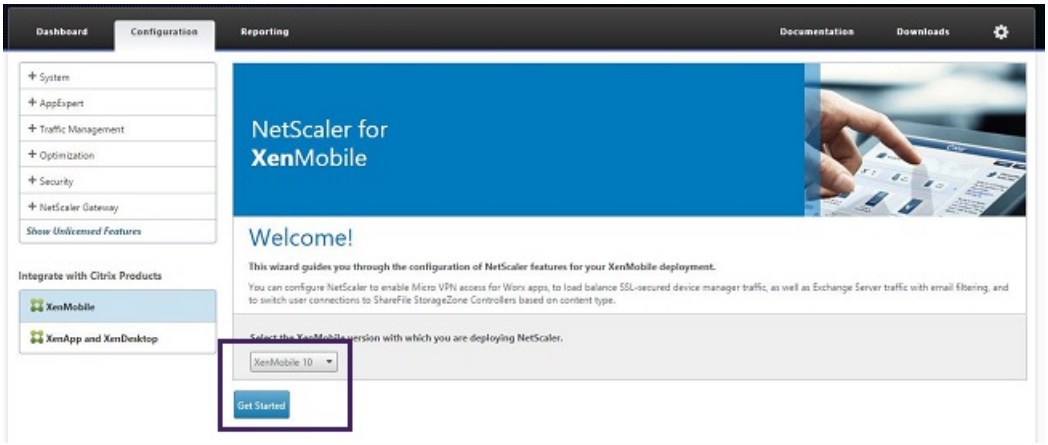


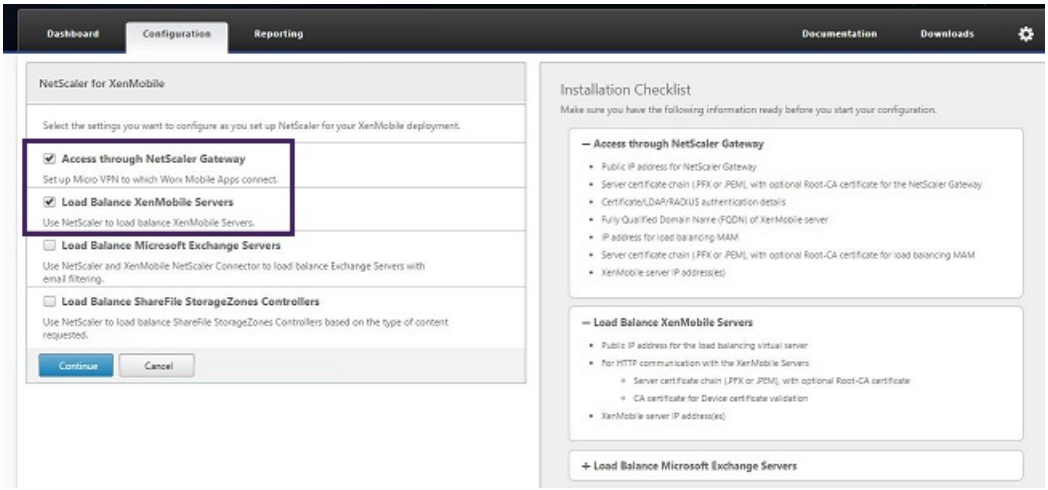


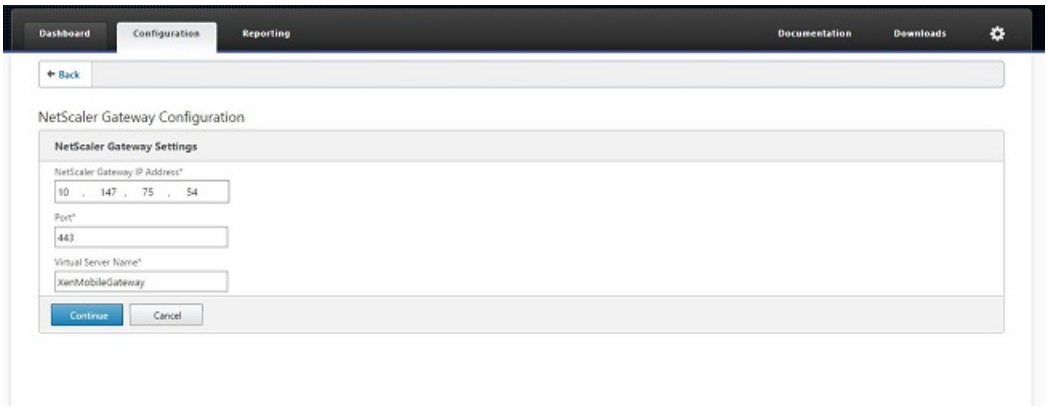




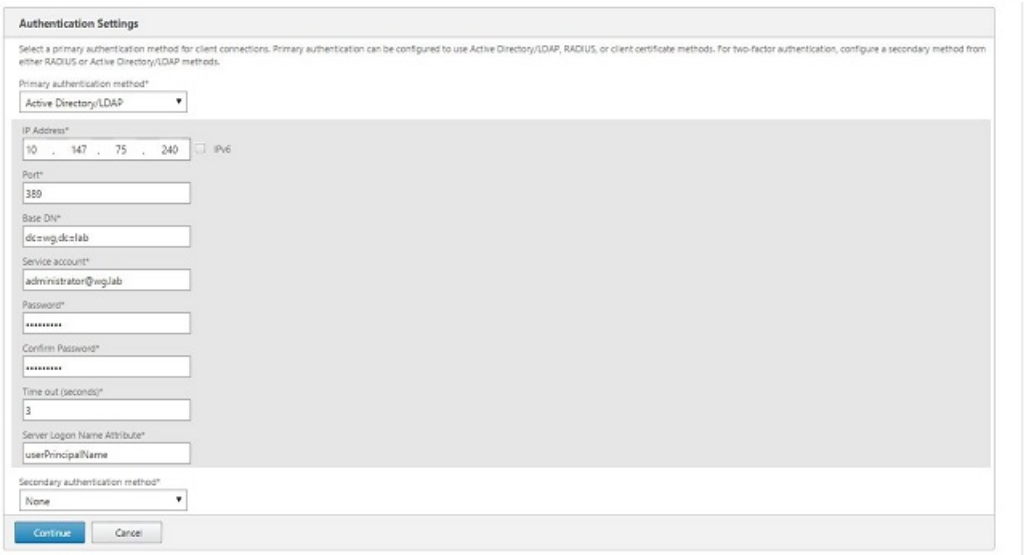
Pour configurer l'équilibrage de charge pour le cluster XenMobile dans NetScaler

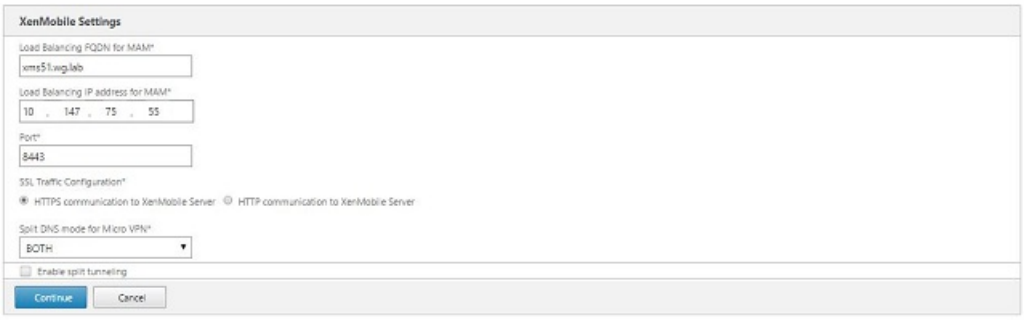


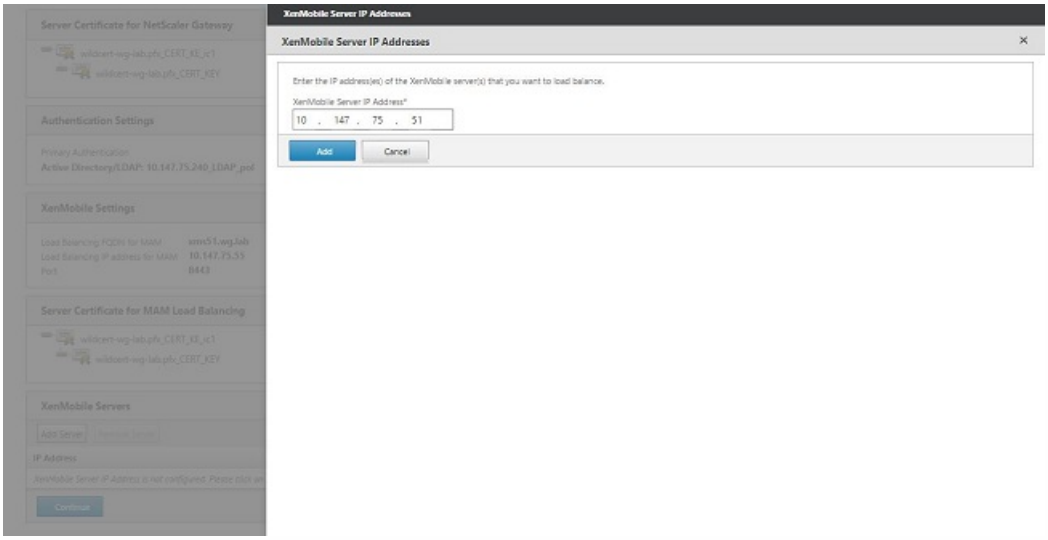


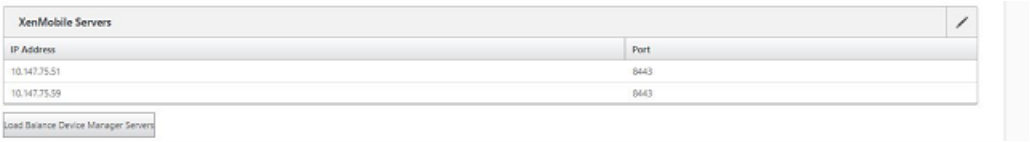


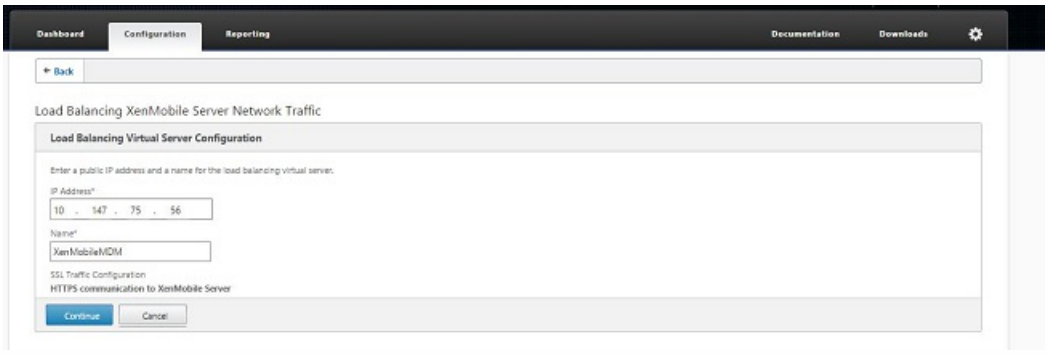
-
-

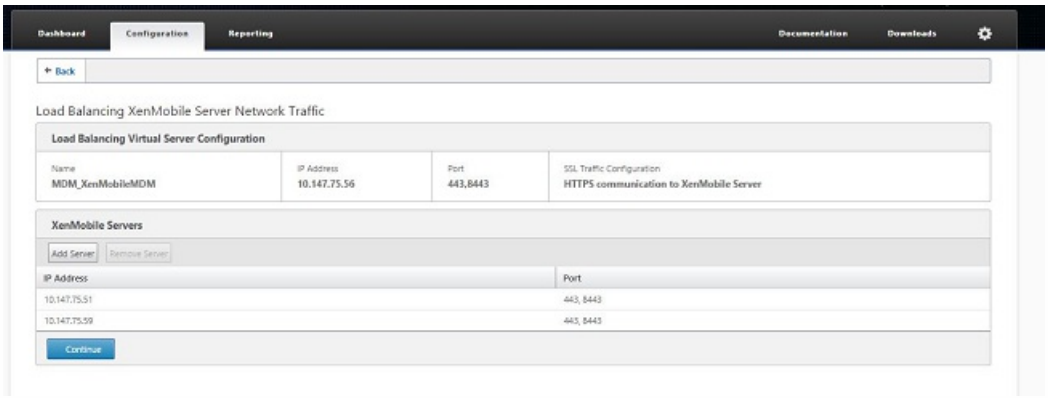


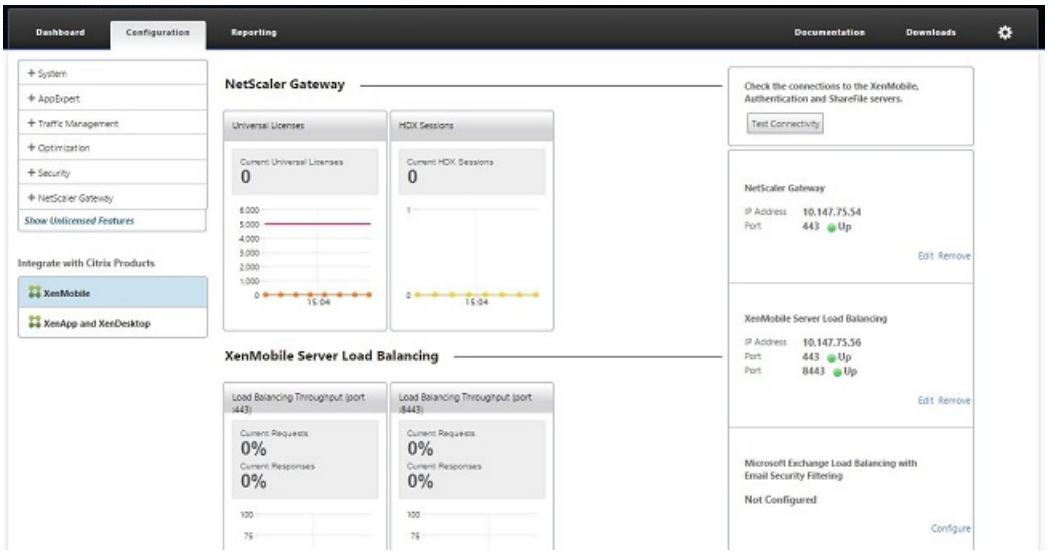


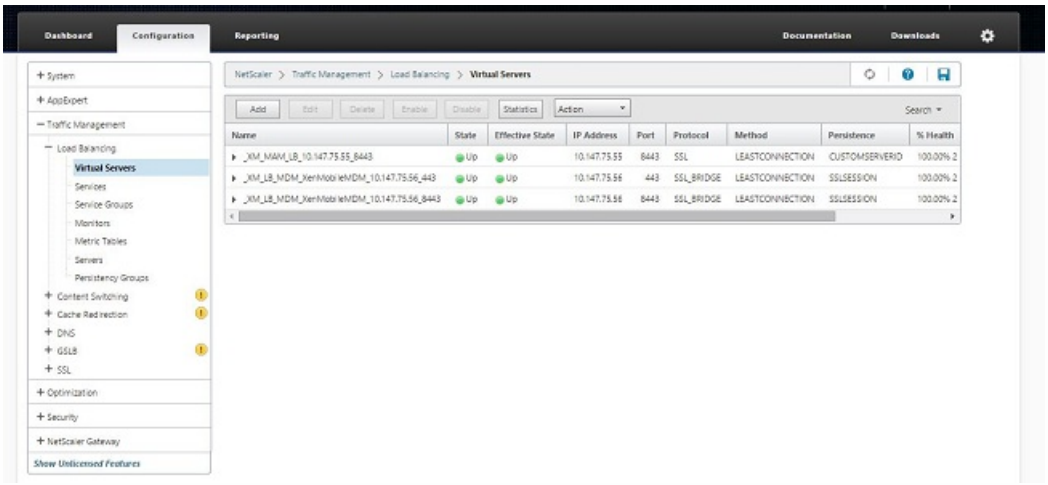


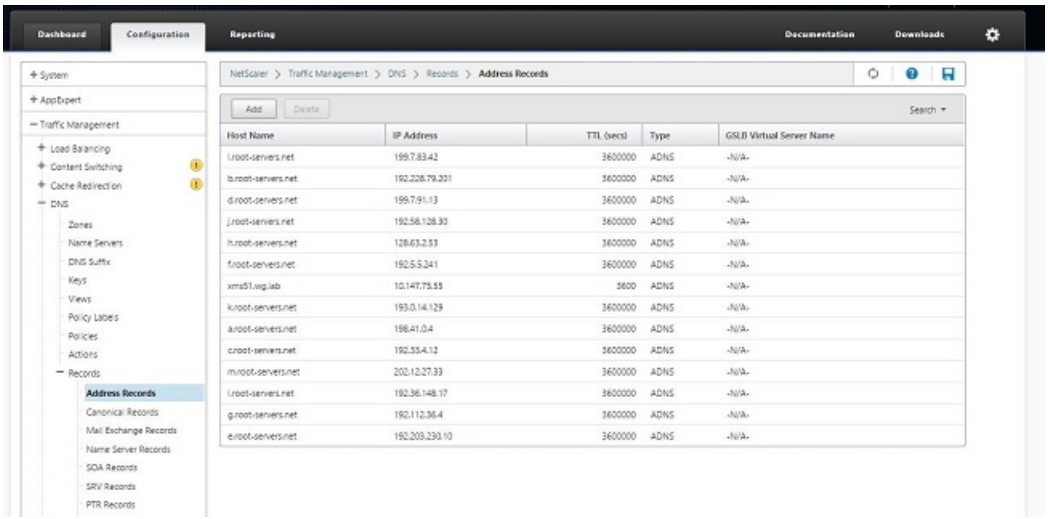


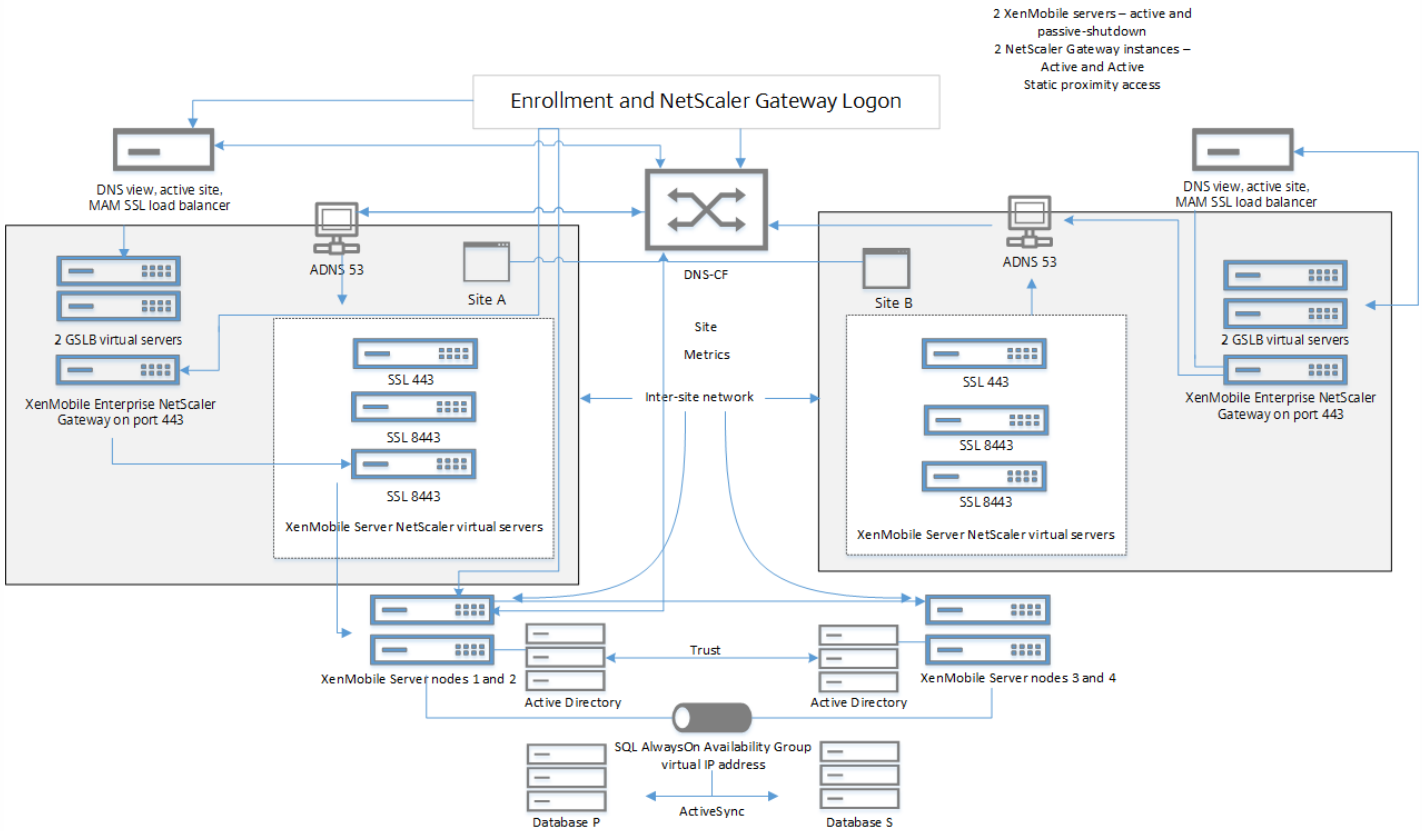






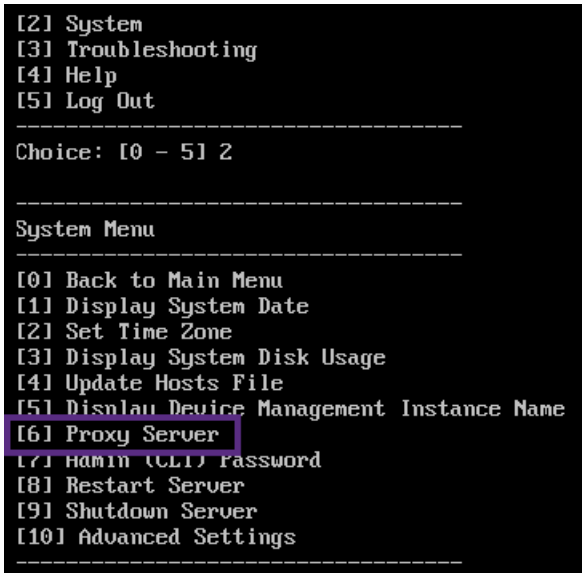


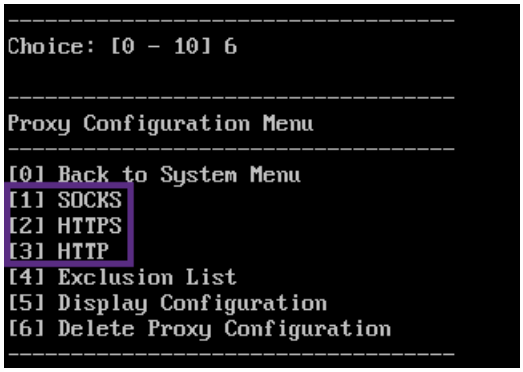


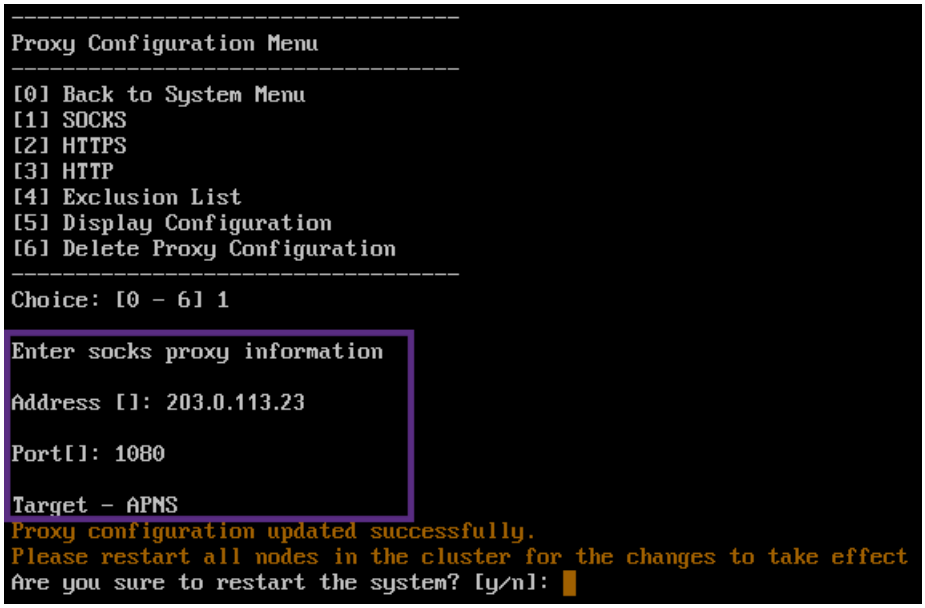


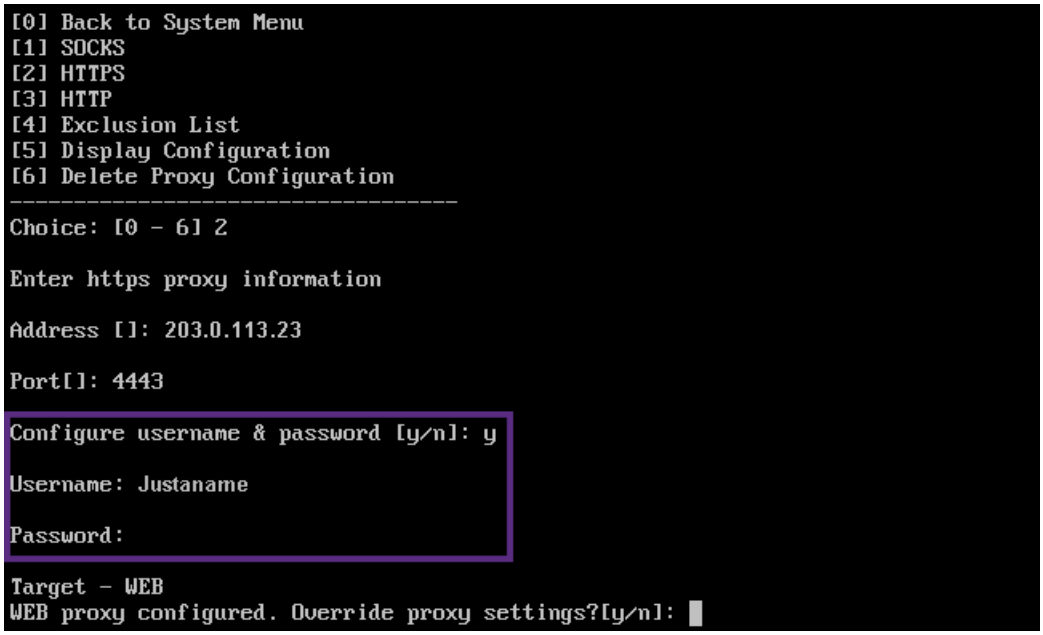
PDF

PDF



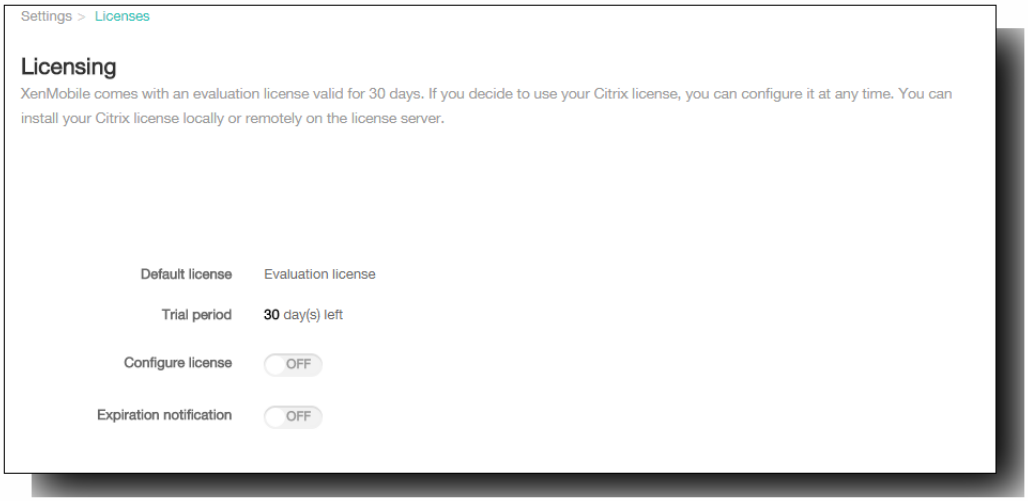




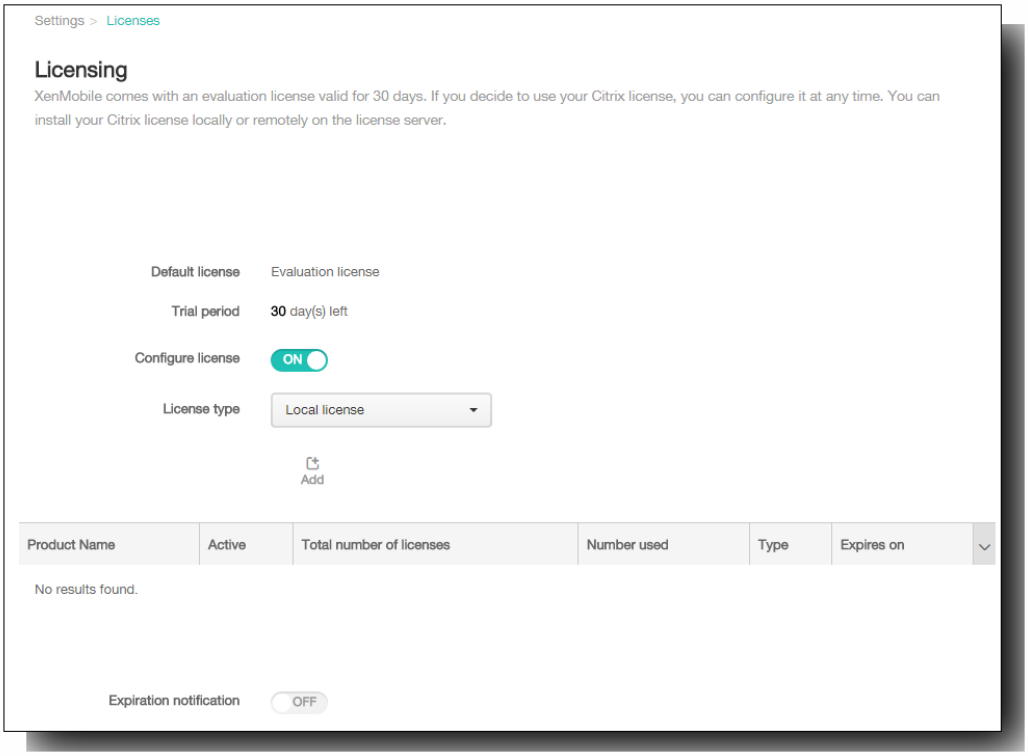


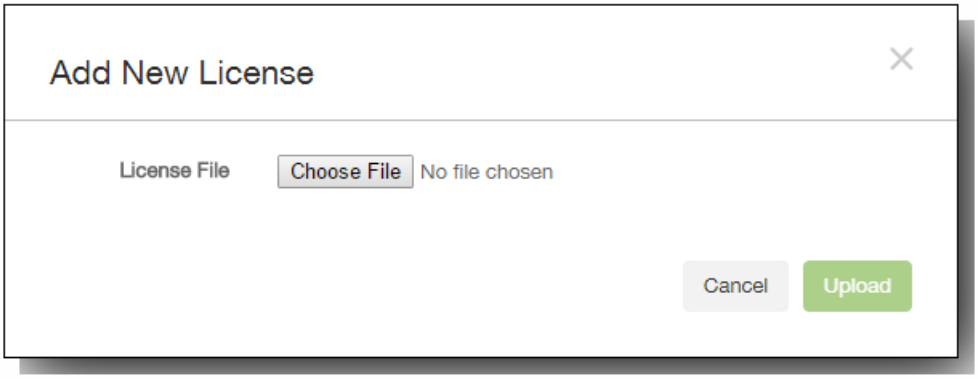
Considérations sur les licences de XenMobile

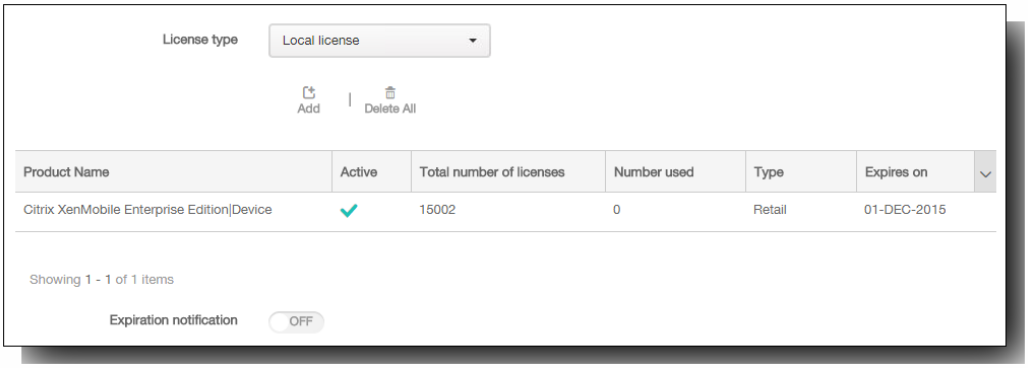
Pour trouver la page Licences sur la console XenMobile



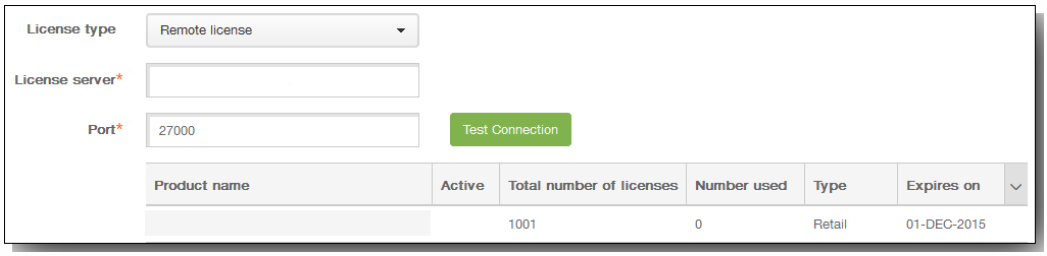
Pour ajouter une licence locale



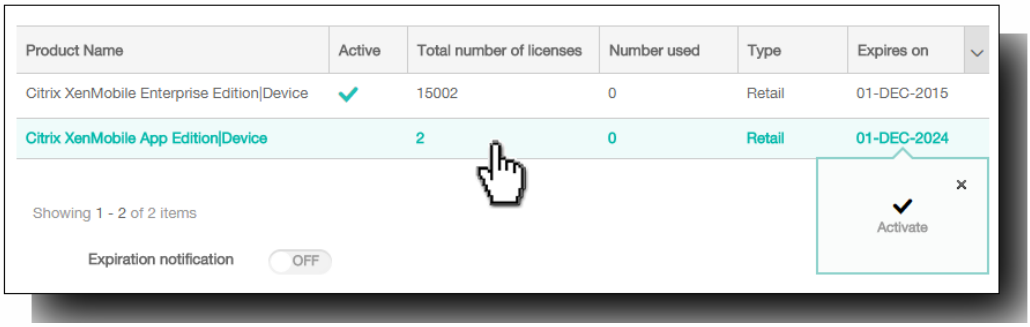


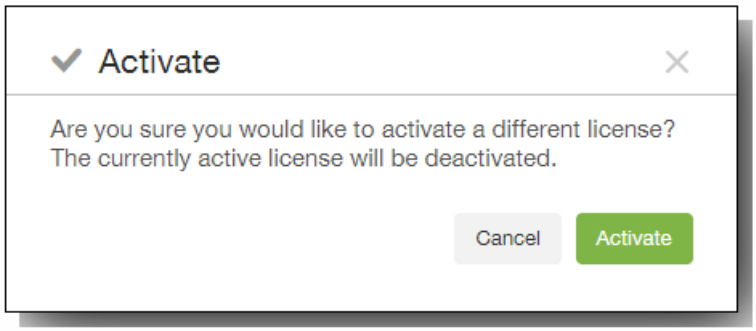


Pour ajouter une licence à distance

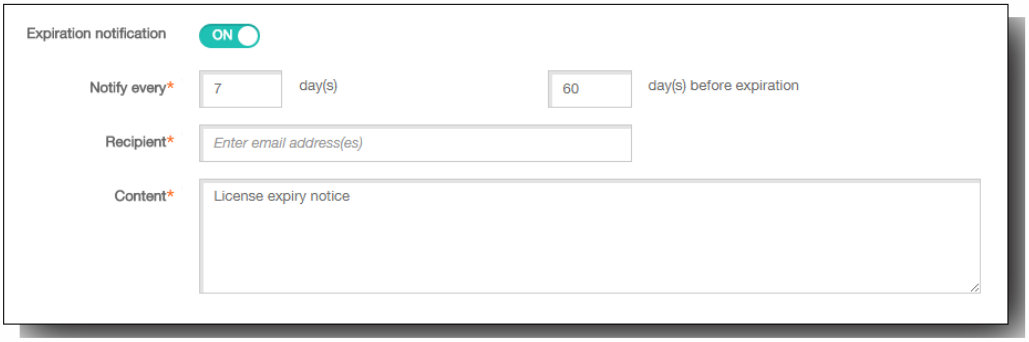


Pour activer une autre licence

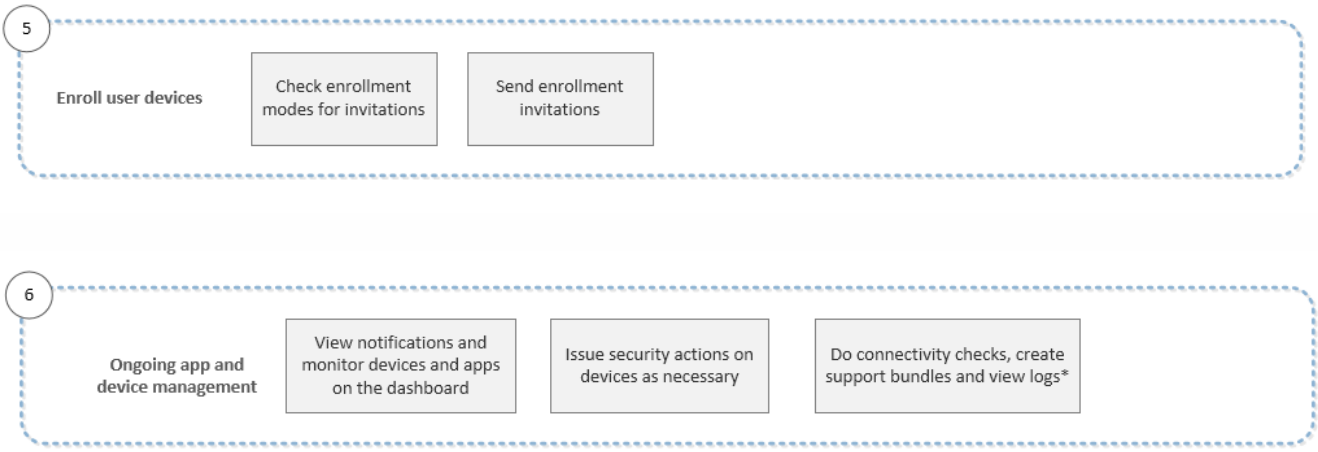


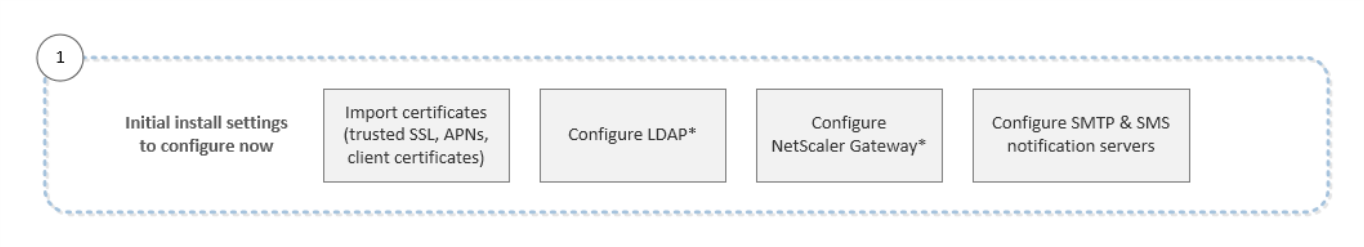


Pour automatiser une notification d'expiration



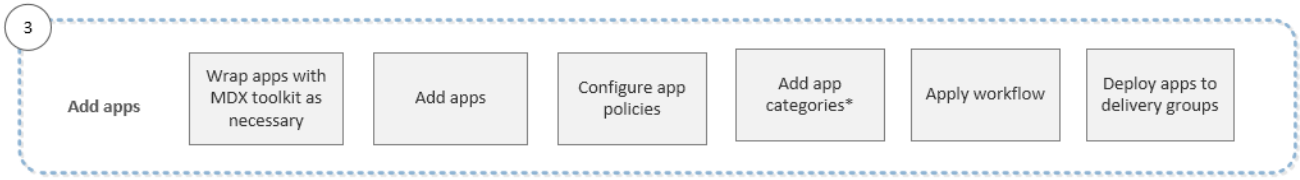
-
-



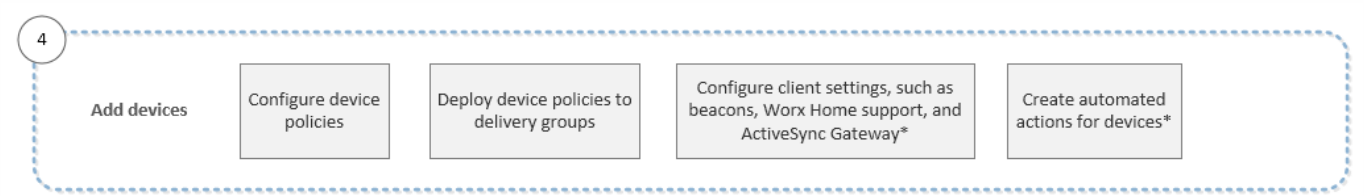


-
-
-
-

-
-
-
-
-
-

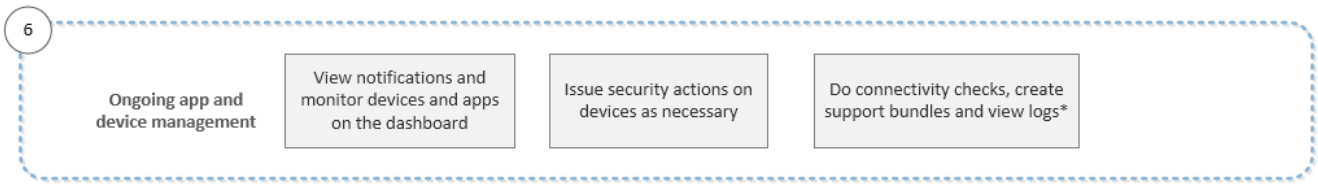


-
-
-
-
-
-



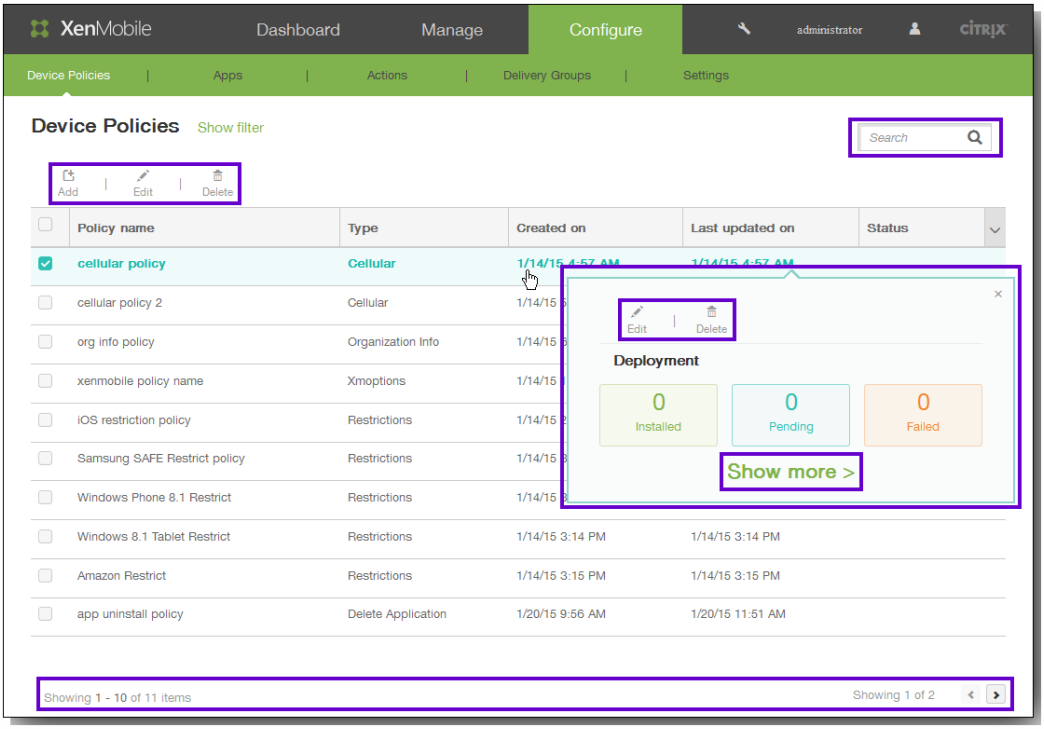
-
-
-
-
-

-
-

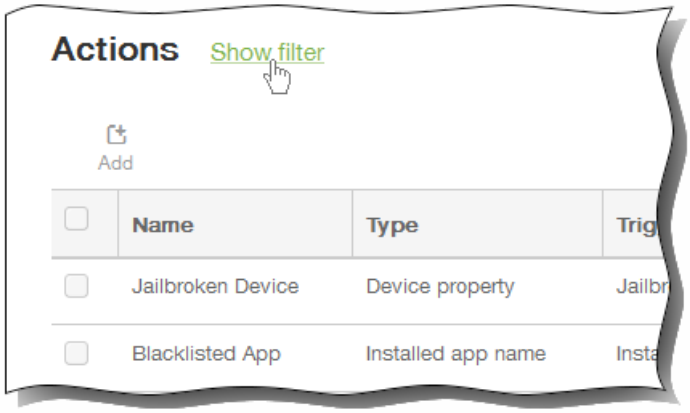


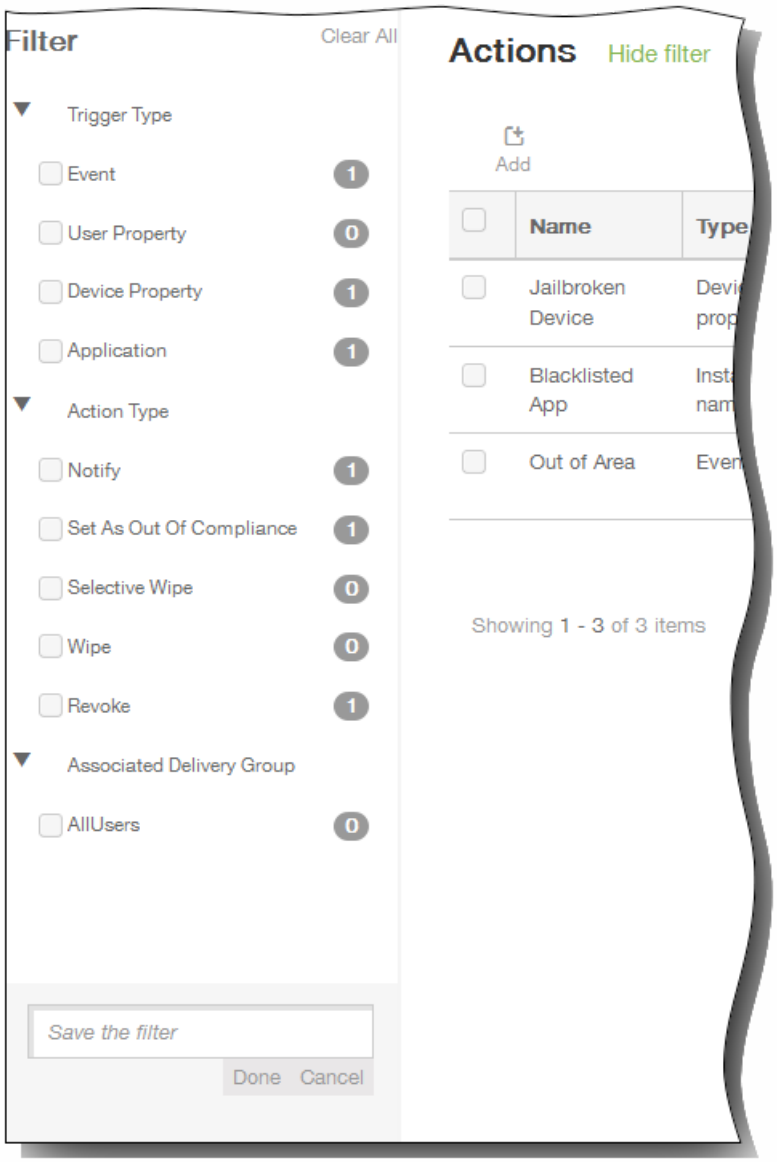
Pour afficher les options dans les tableaux de la console XenMobile

-
-
-
-

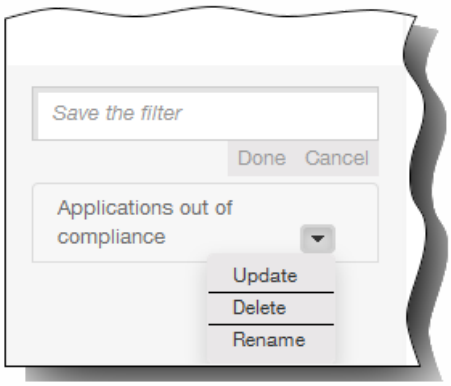


Pour filtrer les informations dans la console XenMobile



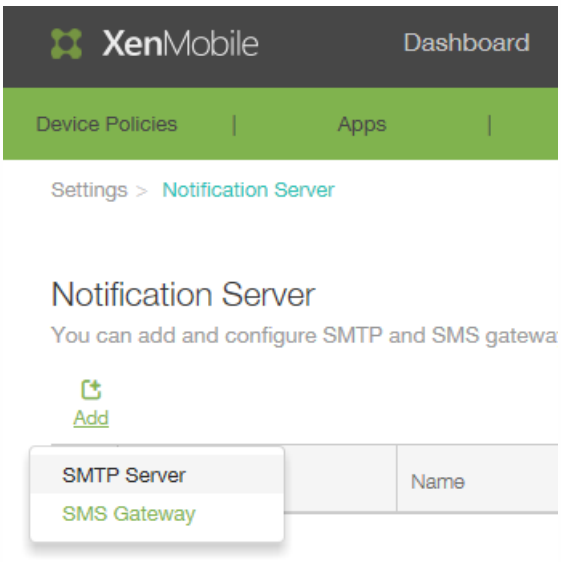


-
-

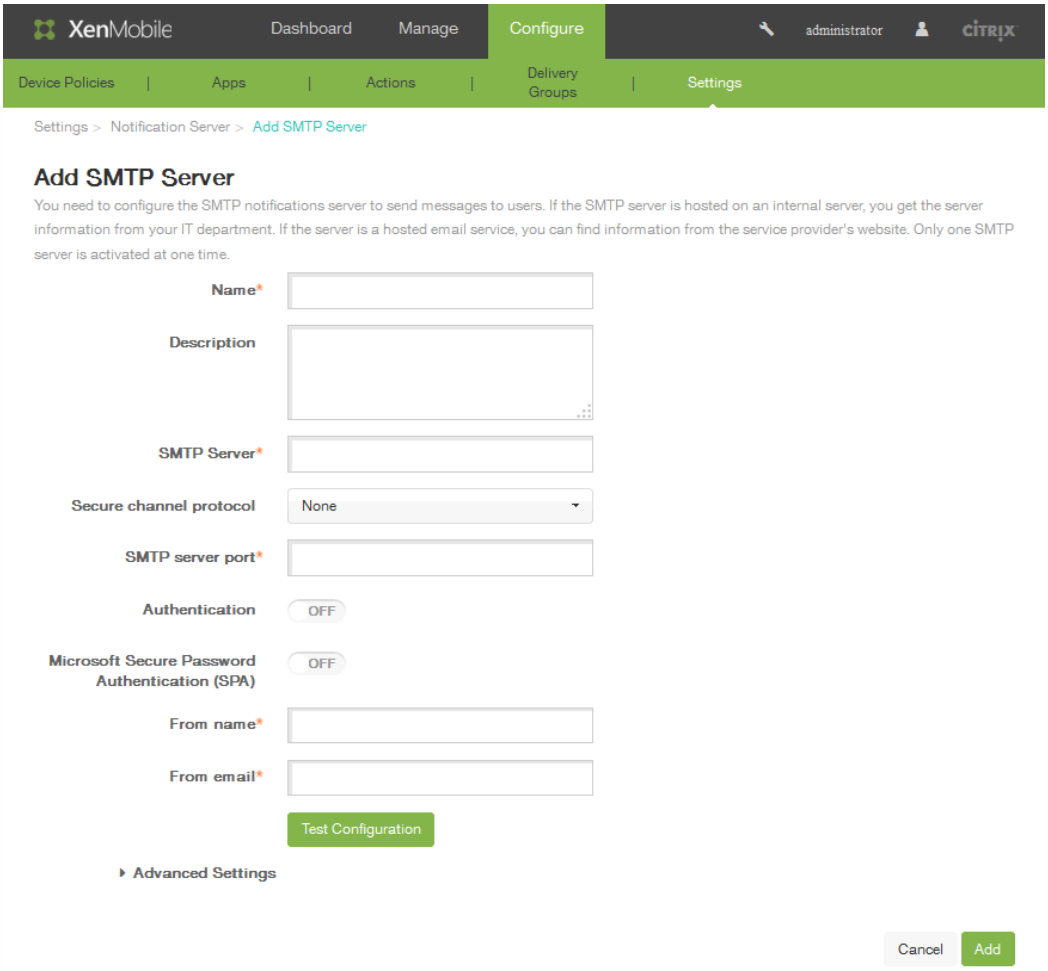


-
-
-
-
-
-
-
-

-
-

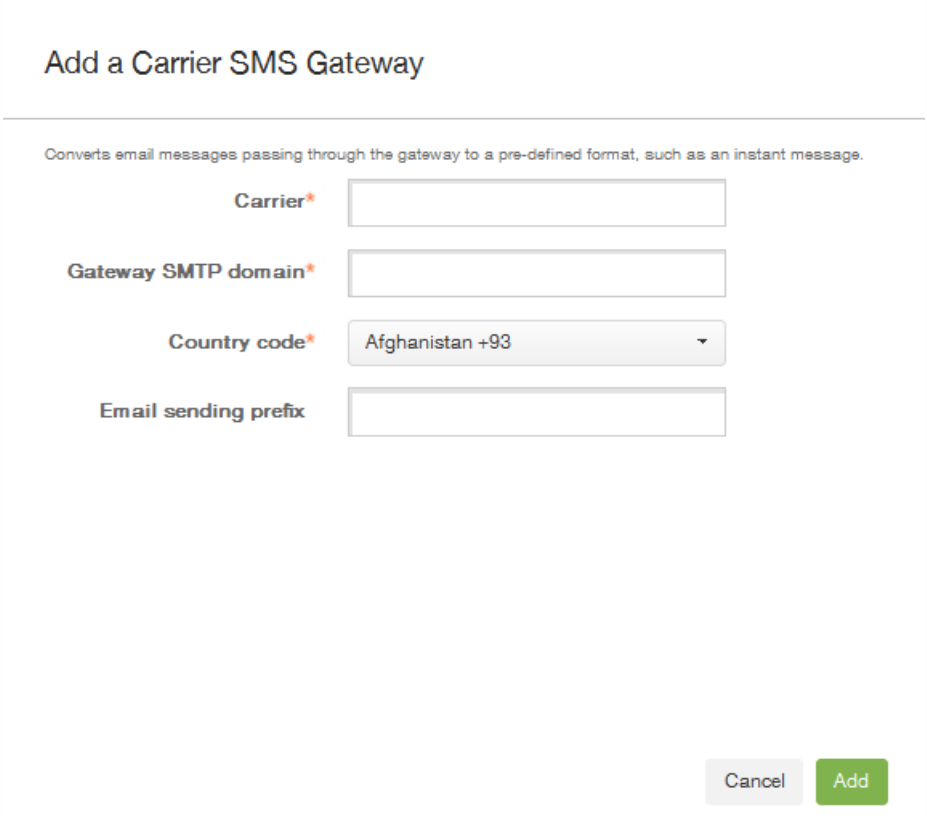


-
-



-
-
-
-
-
-
-
-
-
-
-

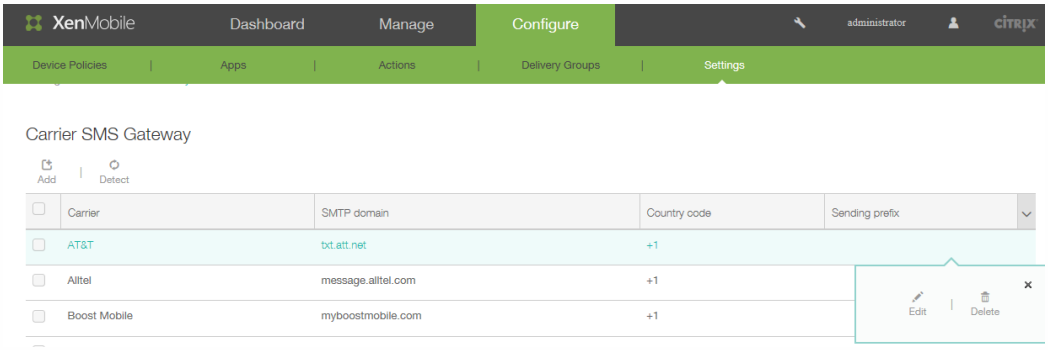
-
-

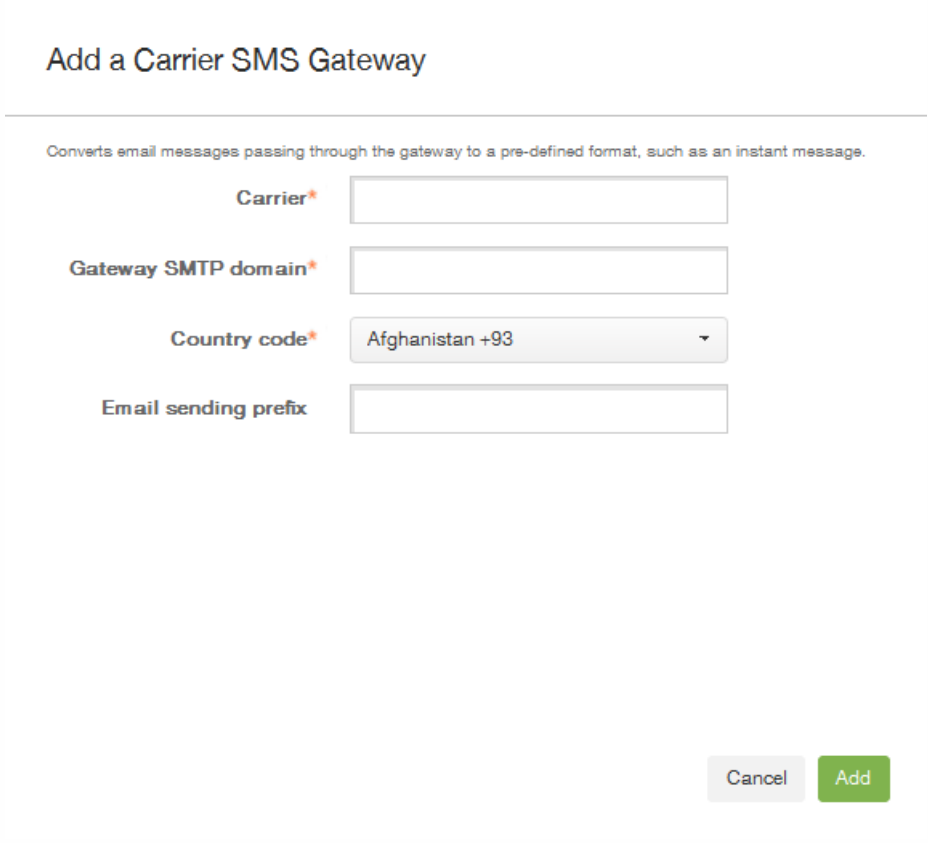


-
-
-
-
-
-

-
-

Pour ajouter une passerelle SMS d'opérateur





Configuration des certificats clients pour l'authentification

PKI XenMobile

Stratégie d'expiration des certificats XenMobile

Certificats APNS pour WorxMail

Certificats APNS pour la gestion des appareils iOS

MDX Toolkit (certificat de distribution iOS)

Keystore Android

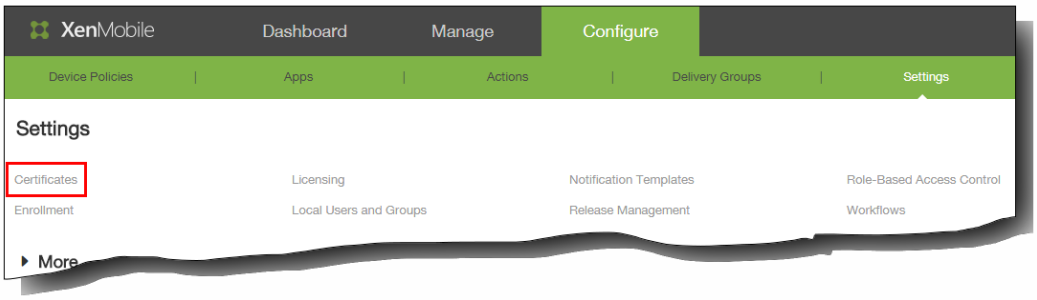
Certificats d'entreprise Symantec pour Windows Phone

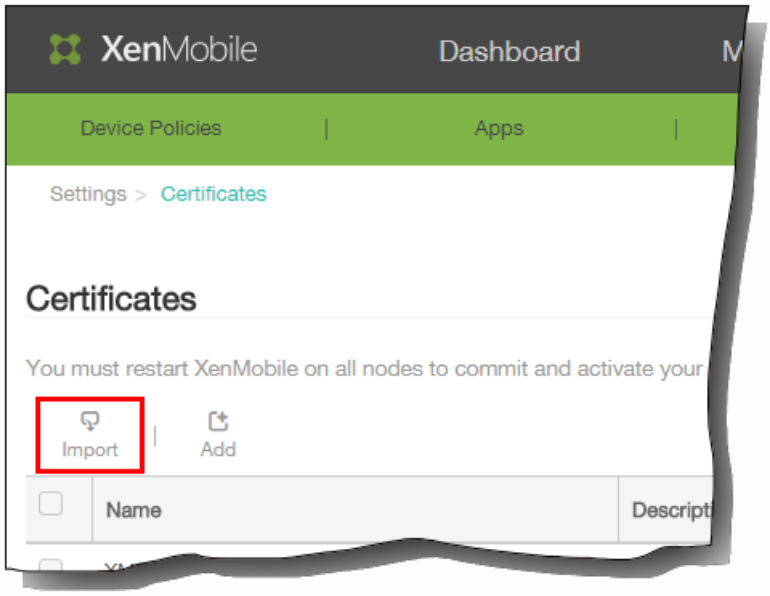
NetScaler

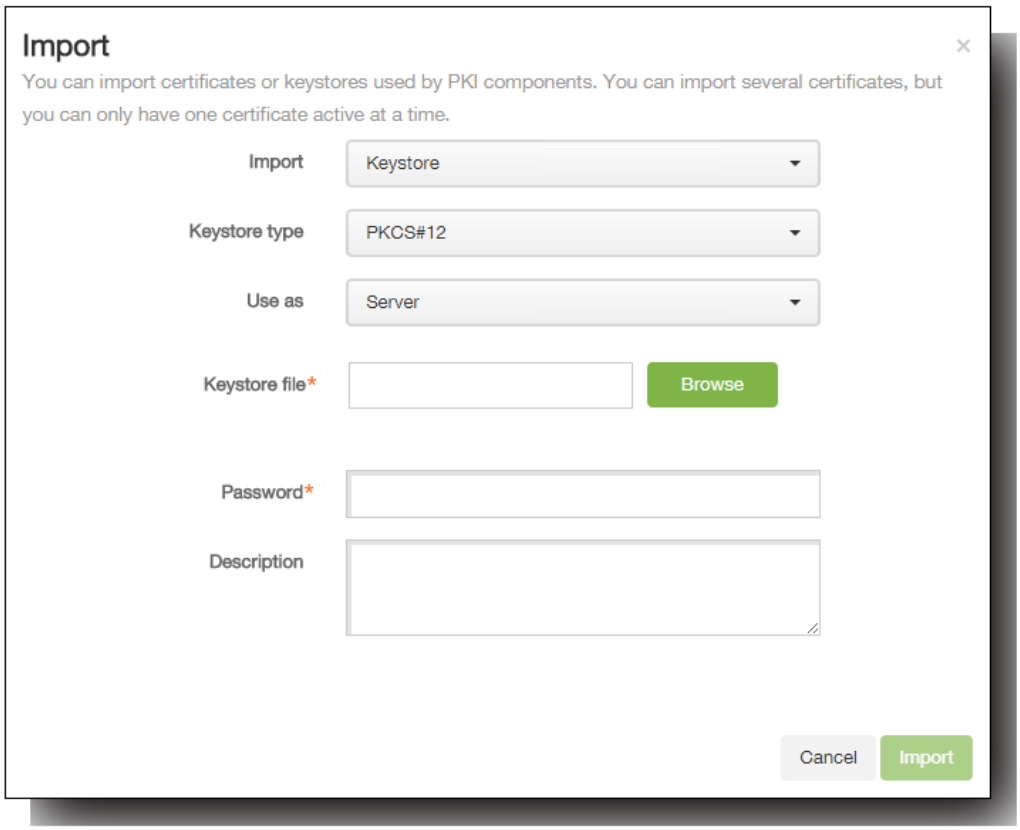
-
-

-

Pour importer un keystore

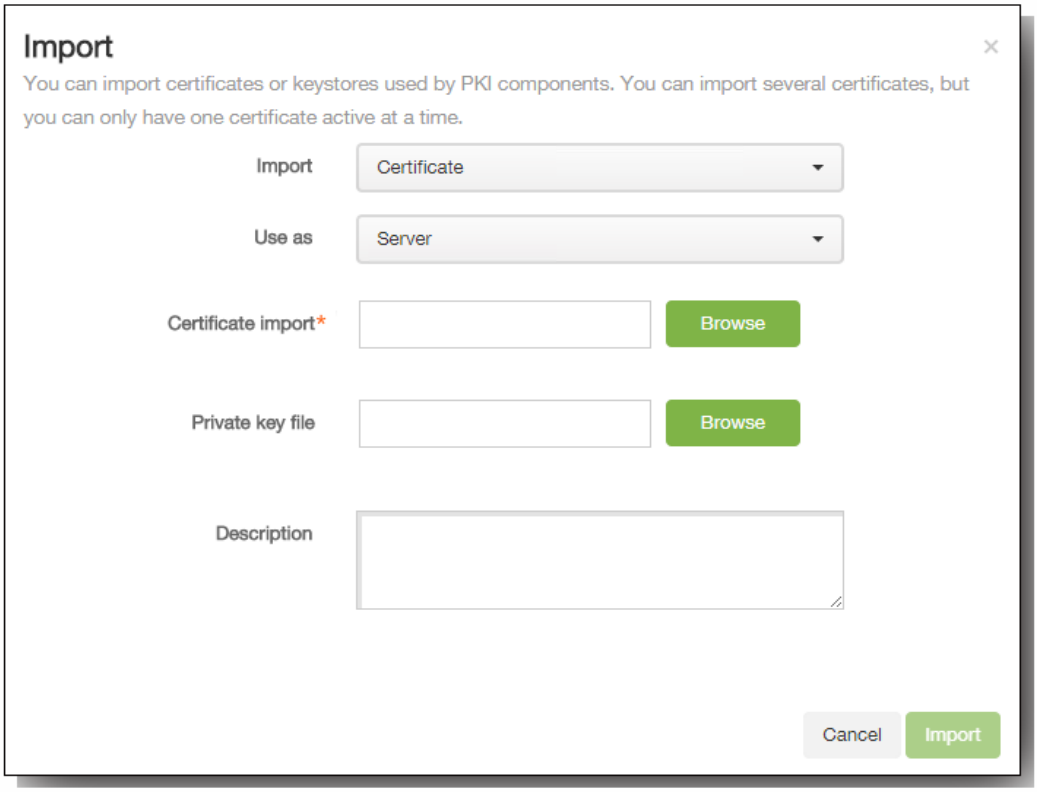






-
-
-
-

Pour importer un certificat



-
-

Mise à jour d'un certificat

-
-
-

-
-
-

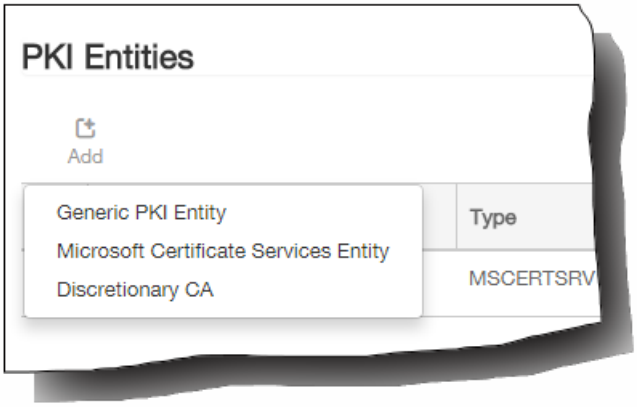
Concepts de PKI communs

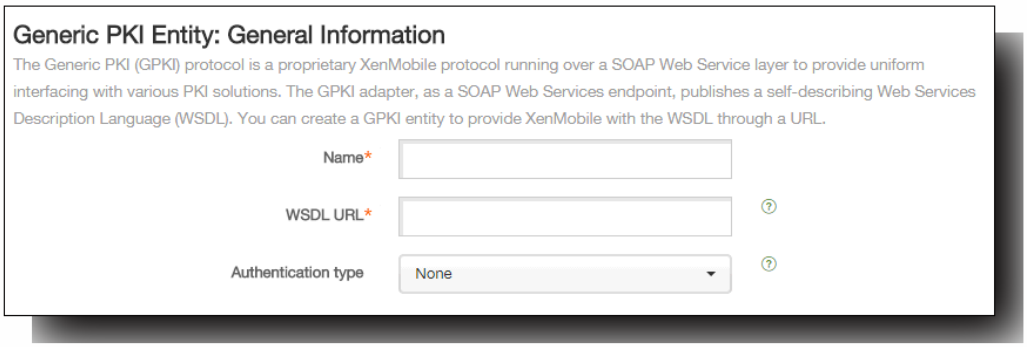
-
-
-

PKI générique

-
-
-

Pour ajouter une PKI générique

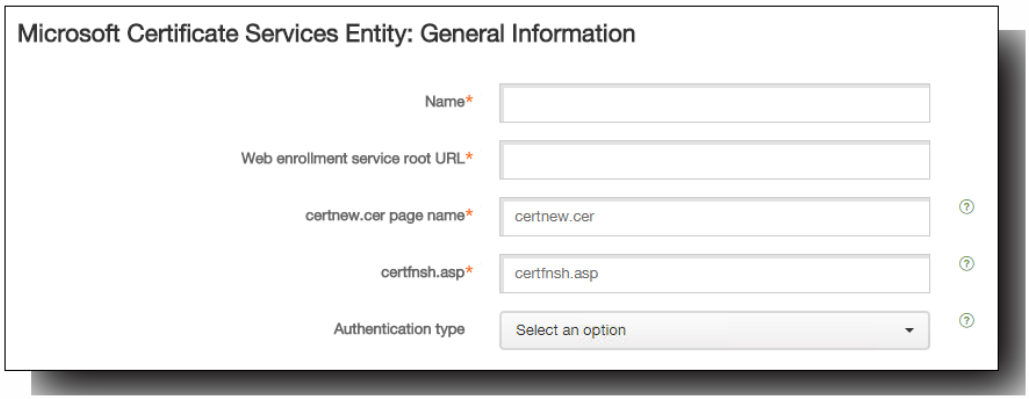




-
-
-

Services de certificats Microsoft

Pour ajouter une entité Services de certificats Microsoft



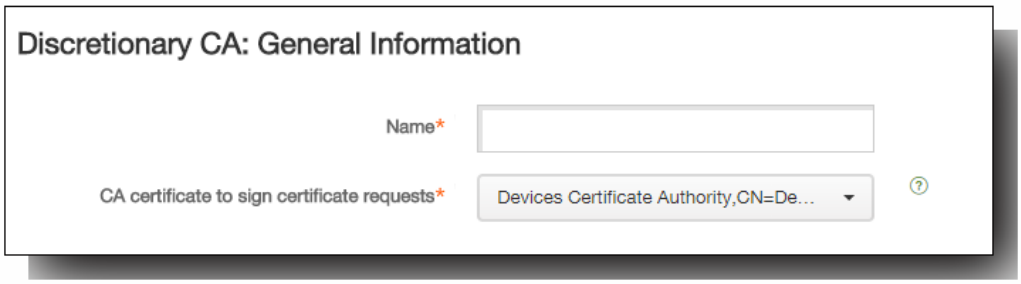
-
-
-
-

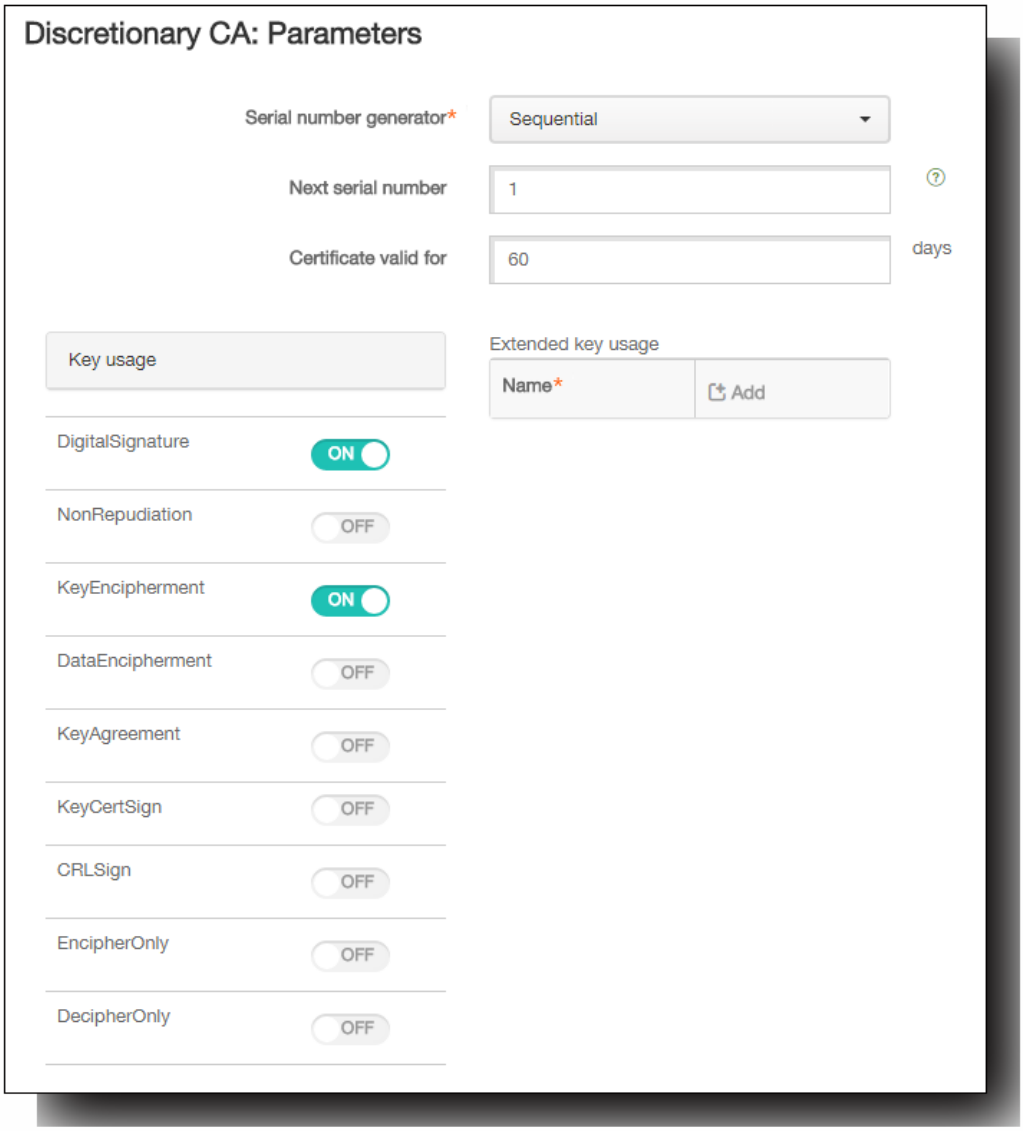
Autorités de certification discrétionnaires

https://serveur/instance/ocsp

-
-
-
-
-

Pour ajouter des autorités de certification discrétionnaires





-

-
-
-
-
-
-

Méthodes d’émission de certificats

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

- Signature. Avec cette méthode, l'émission implique la création d'une nouvelle clé privée, la création d'une demande de signature de certificat (CSR) et la soumission de la demande de signature de certificat à une autorité de certification (CA) pour signature. XenMobile

prend en charge la méthode de signature des trois entités PKI (Entité Services de certificats Microsoft, PKI générique et CA discrétionnaire).
- Récupération. Dans le cadre de XenMobile, cette méthode implique la récupération d'une paire de clés. XenMobile prend en charge la méthode de récupération uniquement pour l'entité PKI générique.

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

Mise à disposition de certificats

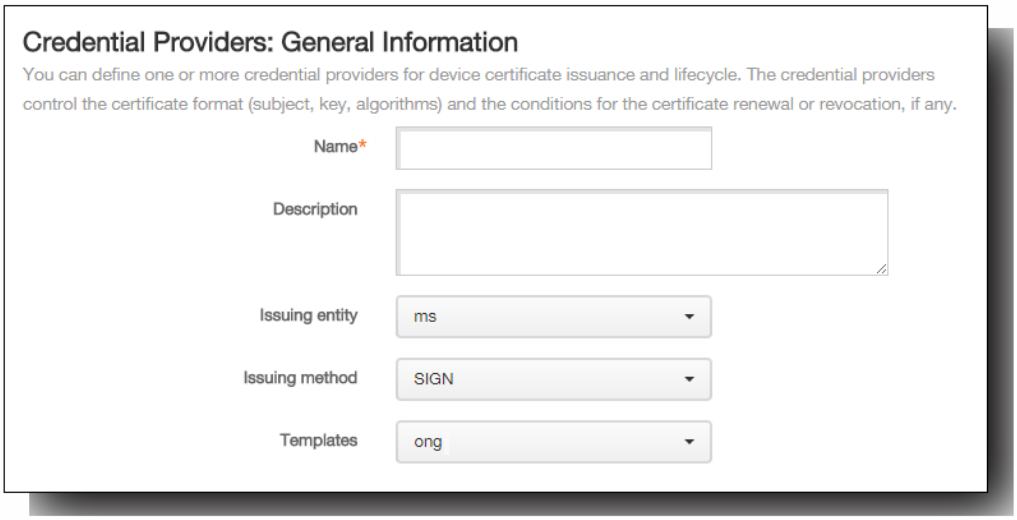
-
-

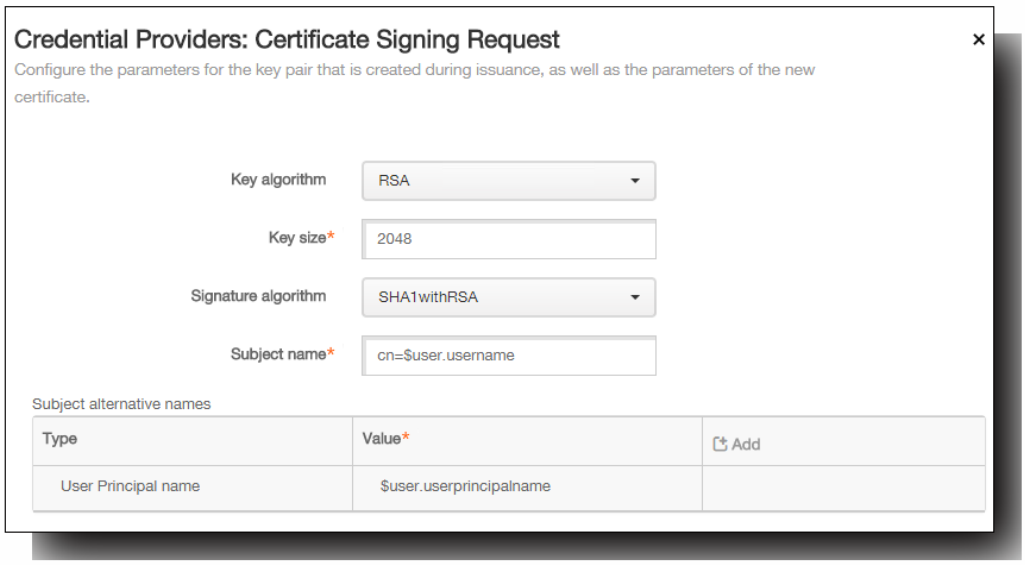
Révocation de certificats

-
-
-

Renouvellement de certificat

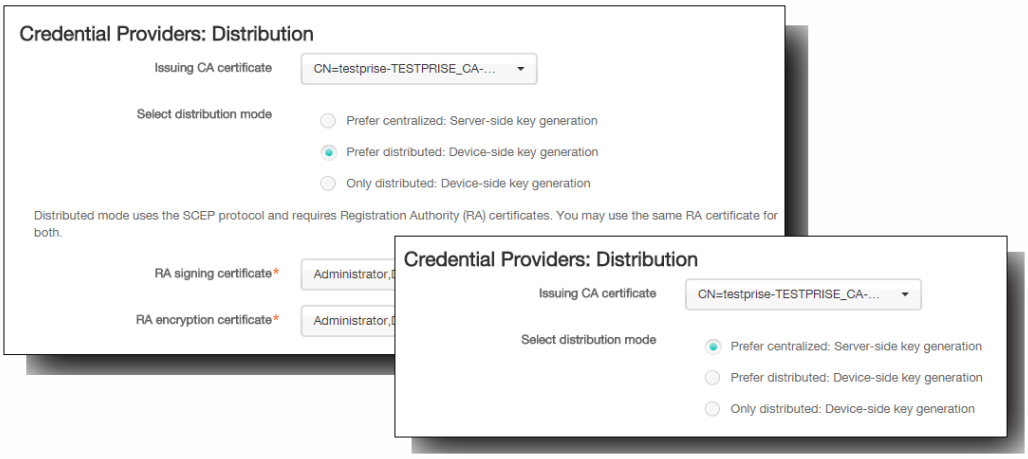
Pour créer un fournisseur d'identités

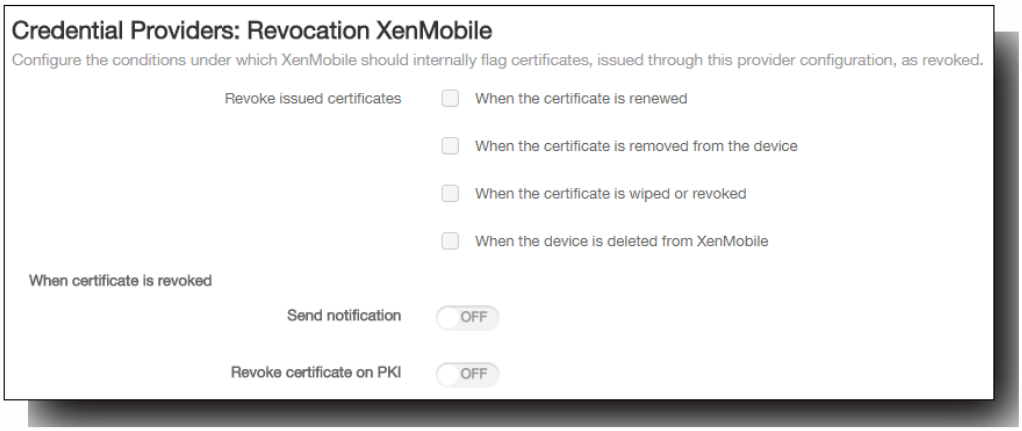


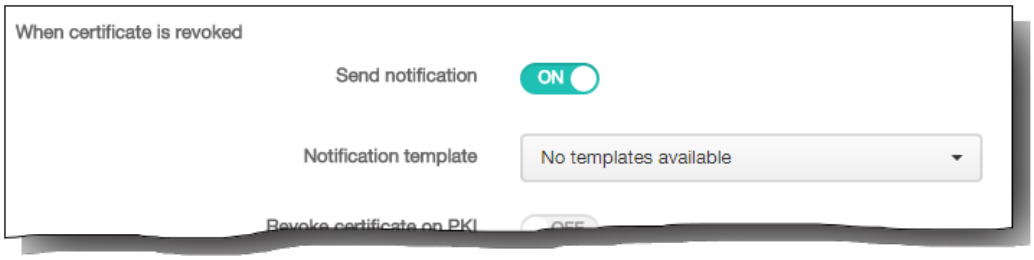


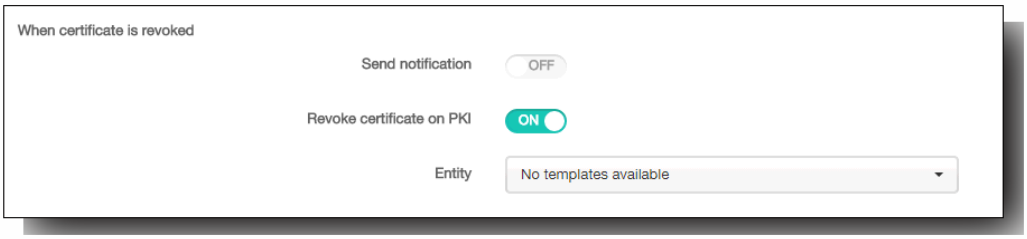
CN=${user.username} OU=${user.department} O=${user.companyname} C=${user.c}\endquotation

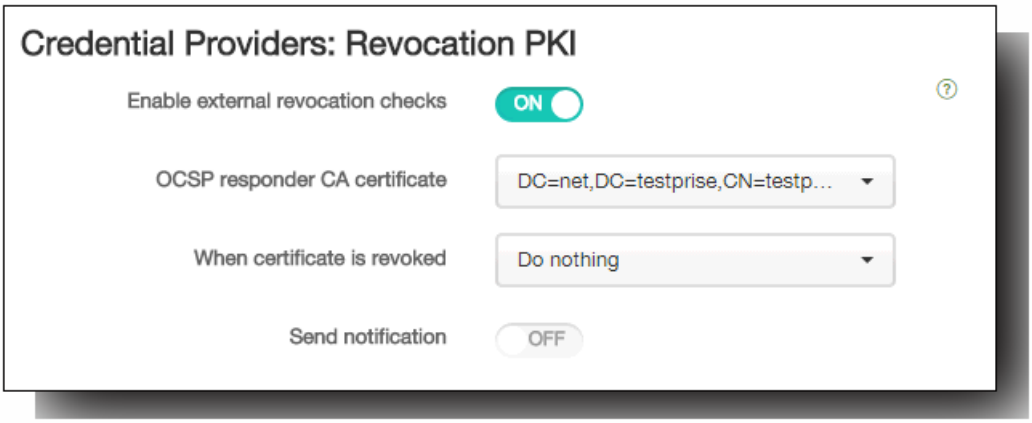
-
-



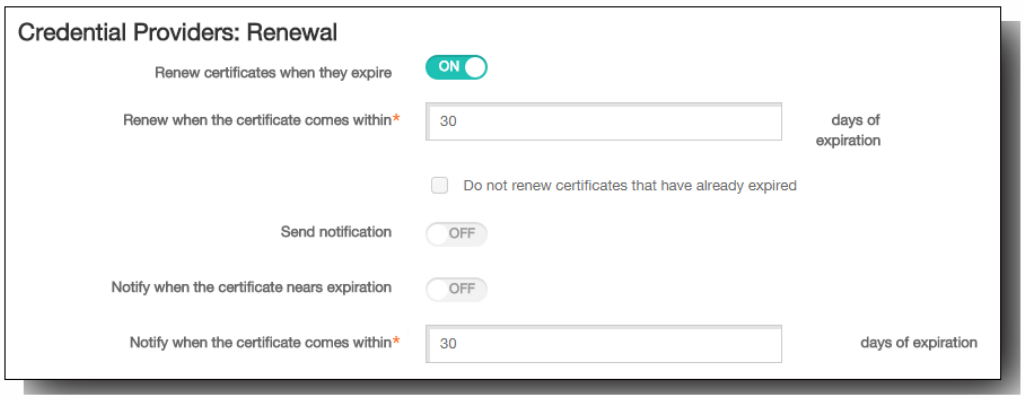








-
-
-
-
-
-



-
-
-
-

Faire une demande de certificat APNS

May 06, 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).

	APNS .pfx en utilisant OpenSSL	
Étape 5	Importer un certificat APNS dans XenMobile	Importez le certificat dans XenMobile.

Informations de migration du certificat Push MDM Apple

Les certificats push MDM (gestion des appareils mobiles) créés dans le iOS Developer Enterprise Program ont été migrés vers le portail Apple Push Certificats Portal. Cette migration affecte la création de nouveaux certificats push MDM, ainsi que le renouvellement, la révocation et le téléchargement de certificats push MDM existants. La migration n'affecte pas les autres certificats APNS (non MDM).

Si votre certificat push MDM a été créé dans le iOS Developer Enterprise Program, les situations suivantes s'appliquent :

- Le certificat a été migré automatiquement pour vous.
- Vous pouvez renouveler le certificat dans le portail Apple Push Certificats Portal sans affecter vos utilisateurs.
- Vous devez utiliser le programme iOS Developer Enterprise Program pour révoquer ou télécharger un certificat préexistant.

Si aucun de vos certificats push MDM n'est proche de l'expiration, vous n'avez rien à faire. Si vous disposez d'un certificat push MDM dont l'expiration est proche, contactez le fournisseur de votre solution MDM. Ensuite, demandez à votre iOS Developer Program Agent de se connecter au portail Apple Push Certificates Portal avec son Apple ID.

Tous les nouveaux certificats push MDM doivent être créés dans le portail Apple Push Certificats Portal. Le programme iOS Developer Enterprise Program n'autorisera plus la création d'un Apple ID avec un identificateur de bundle (section APNS) contenant com.apple.mgmt.

Remarque : vous devez conserver l'Apple ID utilisé pour créer le certificat. En outre, l'Apple ID doit être un ID d'entreprise et non un ID personnel.

Pour créer une demande de signature de certificat à l'aide de Microsoft IIS

La première étape de génération d'une demande de certificat APNS pour les appareils iOS consiste à créer une demande de signature de certificat (CSR). Sur un serveur Windows 2012 R2 où Windows 2008 R2, vous pouvez générer une demande de signature de certificat à l'aide de Microsoft IIS.

1. Ouvrez Microsoft IIS.
2. Double-cliquez sur l'icône Certificats de serveur pour IIS.
3. Dans la fenêtre Certificats de serveur, cliquez sur **Créer une demande de certificat**.
4. Tapez les informations de nom unique (DN) appropriées, puis cliquez sur **Suivant**.
5. Sélectionnez le **Fournisseur de services de chiffrement Microsoft RSA SChannel** pour le fournisseur de services de chiffrement et **2048** pour la longueur en bits, puis cliquez sur **Suivant**.
6. Entrez un nom de fichier et spécifiez un emplacement pour enregistrer la CSR, puis cliquez sur **Terminer**.

Pour créer une demande de signature de certificat sur un Mac

1. Sur un Mac exécutant Mac OS X, sous **Applications** > **Utilitaires**, démarrez l'application Trousseau d'accès.
2. Ouvrez le menu **Trousseau d'accès** et cliquez sur **Préférences**.

3. Cliquez sur l'onglet **Certificats**, définissez les options **OCSP** et **CRL** sur **Désactivé**, puis fermez la fenêtre Préférences.
4. Dans le menu **Trousseau d'accès**, cliquez sur **Assistant de certification** > **Demander un certificat à une autorité de certification**.
5. L'Assistant de certification vous invite à entrer les informations suivantes :
   1. **Adresse e-mail**. Adresse de messagerie de la personne ou du compte de rôle qui est responsable de la gestion du certificat.
   2. **Nom commun**. Nom commun de la personne ou compte de rôle qui est responsable de la gestion du certificat.
   3. **Adresse e-mail de l'AC**. Adresse de messagerie de l'autorité de certification.
6. Sélectionnez **Enregistrée sur le disque** et **Me laisser indiquer les informations sur la bi-clé** et cliquez sur **Continuer**.
7. Entrez un nom pour le fichier CSR, enregistrez le fichier sur votre ordinateur, puis cliquez sur **Enregistrer**.
8. Spécifiez les informations de bi-clé en sélectionnant la **Dimension de clé** de 2048 bits et **Algorithme RSA**, puis cliquez sur **Continuer**. Le fichier CSR est prêt à être chargé dans le cadre du processus de certificat APNS.
9. Cliquez sur **Terminé** lorsque l'Assistant de certification termine le processus de demande de signature de certificat.

Pour créer une demande de signature de certificat avec OpenSSL

Si vous ne pouvez pas utiliser un serveur Windows 2012 R2 ou Windows 2008 R2 et Microsoft Internet Information Server (IIS) ou un ordinateur Mac pour générer une demande de signature de certificat (CSR) à soumettre à Apple afin d'obtenir le certificat Apple Push Notification Service (APNS), vous pouvez utiliser OpenSSL.

Remarque : pour pouvoir utiliser OpenSSL pour créer une demande de signature de certificat, vous devez télécharger et installer OpenSSL à partir du site Web OpenSSL.

1. Sur l'ordinateur sur lequel vous avez installé OpenSSL, exécutez la commande suivante à partir d'une invite de commandes ou de shell.
   openssl req -new -keyout Customer.key.pem –out CompanyAPNScertificate.csr -newkey rsa:2048

2. Le message suivant s'affiche pour les informations de nom du certificat. Entrez les informations demandées.
   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 []:

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**

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 **Importer** apparaît.

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.

NetScaler Gateway et XenMobile

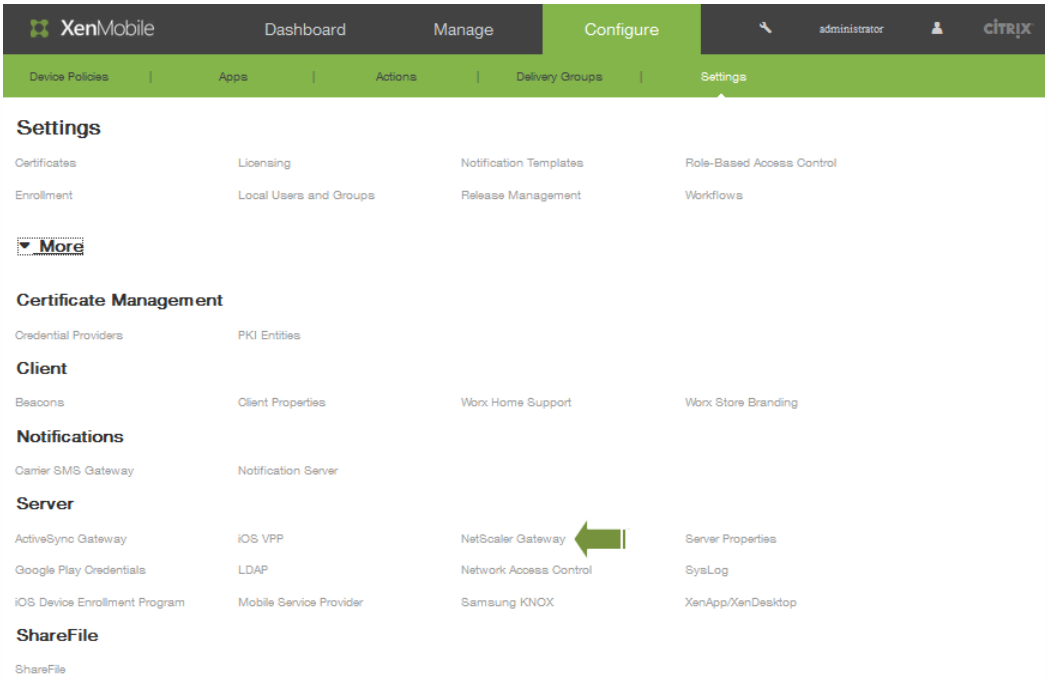
May 06, 2016

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.

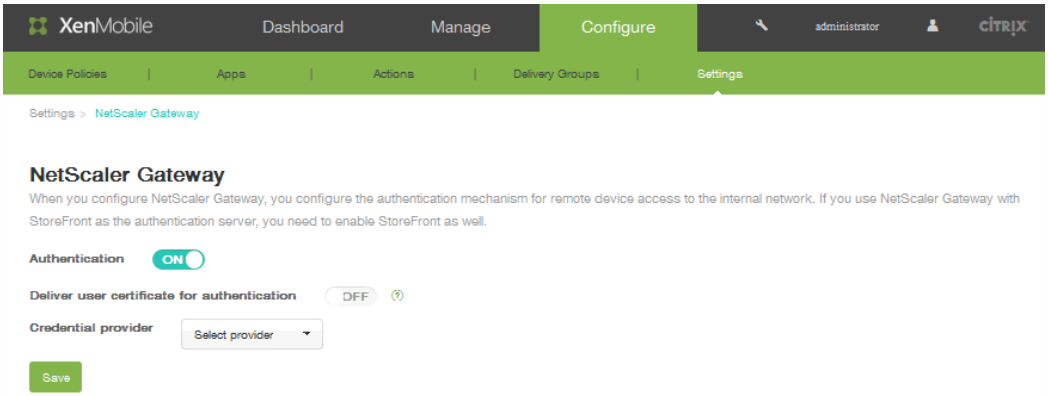
Remarque : pour de plus amples informations sur la configuration de NetScaler Gateway pour XenMobile sur NetScaler, consultez la section Configuration de paramètres pour votre environnement XenMobile.

Pour configurer NetScaler Gateway

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > NetScaler Gateway.



2. Dans Authentification, sélectionnez ON.



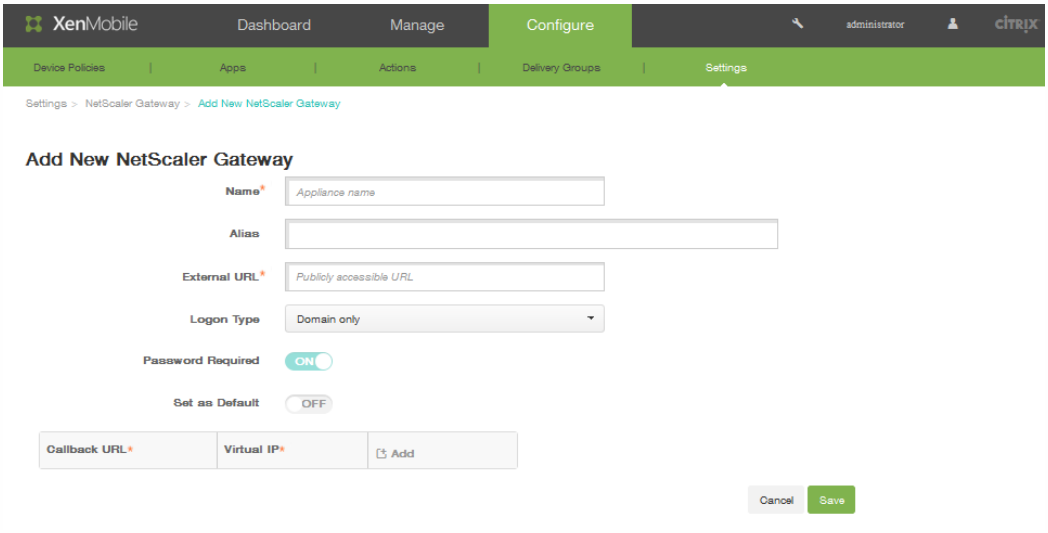
3. Si vous voulez que XenMobile partage le certificat d'authentification avec Worx Home afin que NetScaler Gateway gère

l'authentification du certificat client, dans Délivrer un certificat utilisateur pour l'authentification, sélectionnez ON.

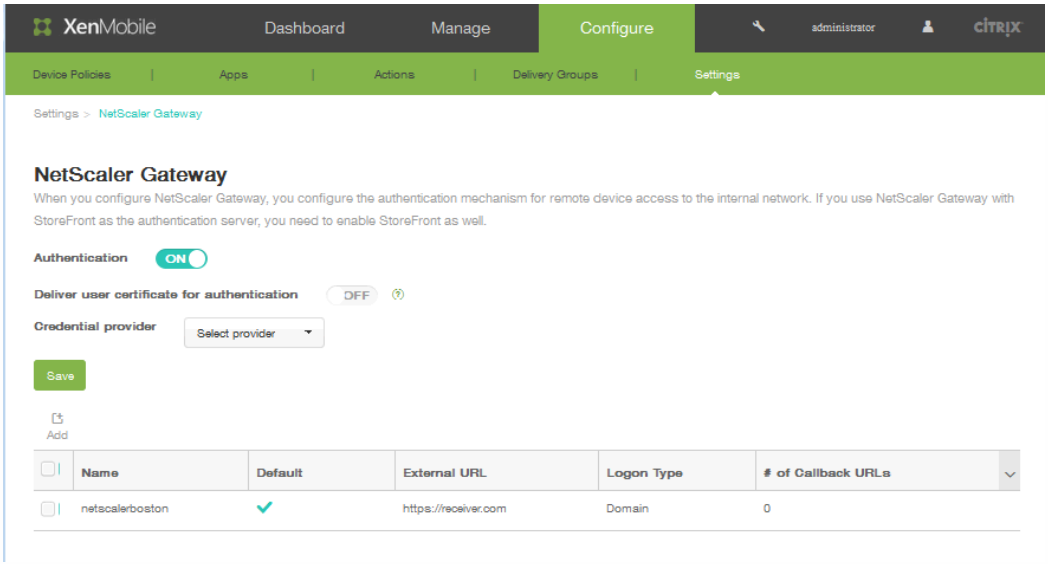
4. Dans la liste Fournisseur d'identités, cliquez sur le fournisseur d'identités. Pour de plus amples informations, consultez la section Fournisseur d'identités.
5. Cliquez sur Enregistrer.

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.

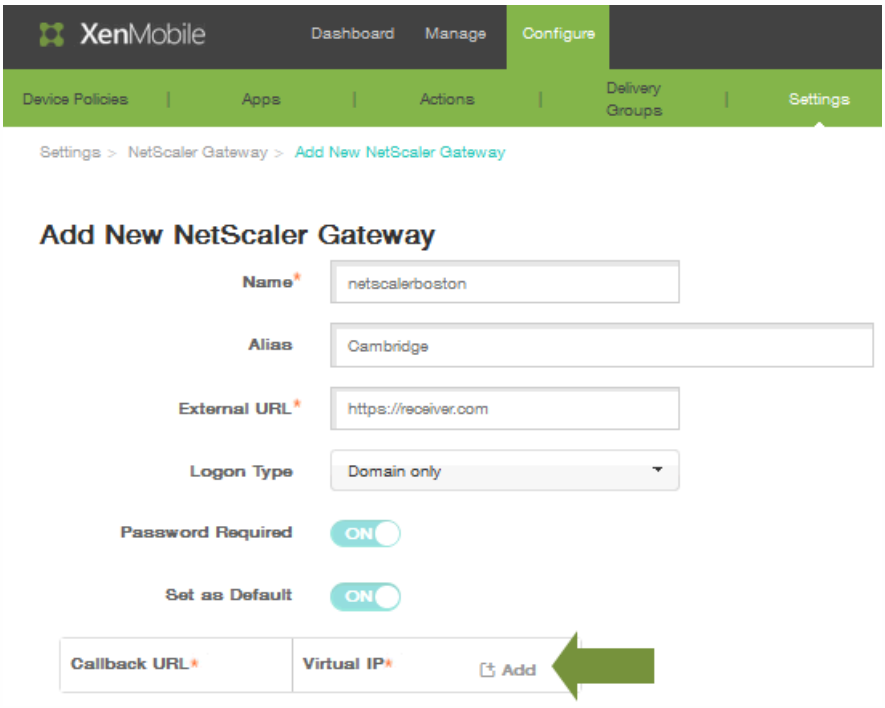


3. Dans le champ Nom, entrez un nom pour l'instance NetScaler Gateway.
4. Dans Alias, entrez un alias (facultatif).
5. Dans URL externe, entrez l'adresse URL publiquement accessible de NetScaler Gateway. Par exemple, https://receiver.com.
6. Dans la liste Type d'ouverture de session, cliquez sur un type 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 donc 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.



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.

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

Configuration du LDAP

May 06, 2016

Vous pouvez configurer une connexion dans XenMobile à un ou plusieurs annuaires, tels que Active Directory, qui sont compatibles avec le protocole LDAP (Lightweight Directory Access Protocol). 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 sur 0, l'utilisateur n'est pas obligé d'attendre après un verrouillage.

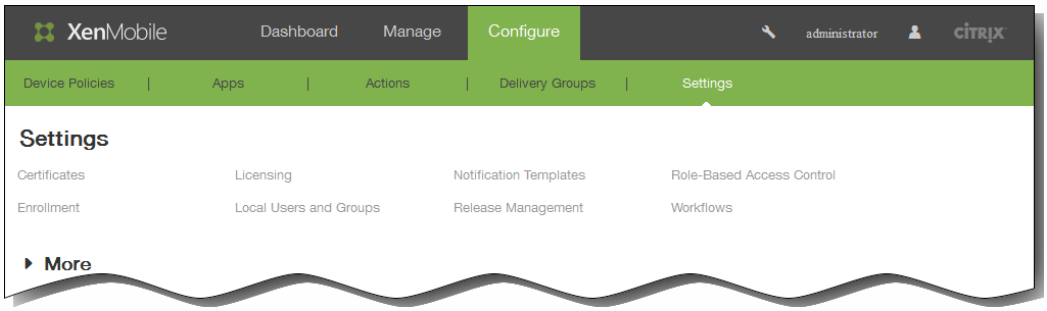
- Port TCP du catalogue global : entrez le numéro de port TCP du serveur du catalogue global. Par défaut, le numéro de port TCP est défini sur 3268 ; pour les connexions SSL, utilisez le numéro de port 3269.
- Base de recherche du catalogue global : si vous le souhaitez, entrez la valeur de base de recherche 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.

Comptes utilisateur, rôles et paramètres d'inscription

May 06, 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 :

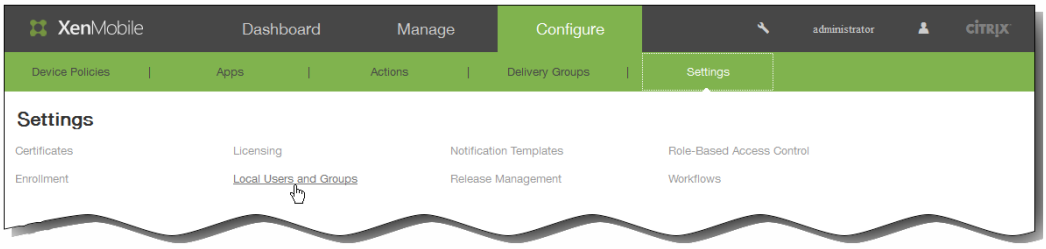
- Cliquez sur Utilisateurs et groupes locaux pour ajouter des comptes utilisateur manuellement ou utilisez un fichier de provisioning .csv pour importer des comptes et gérer des groupes locaux. Consultez les informations suivantes pour obtenir plus d'informations :
  - Pour ajouter, modifier ou supprimer 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

Pour ajouter, modifier ou supprimer des utilisateurs locaux dans XenMobile

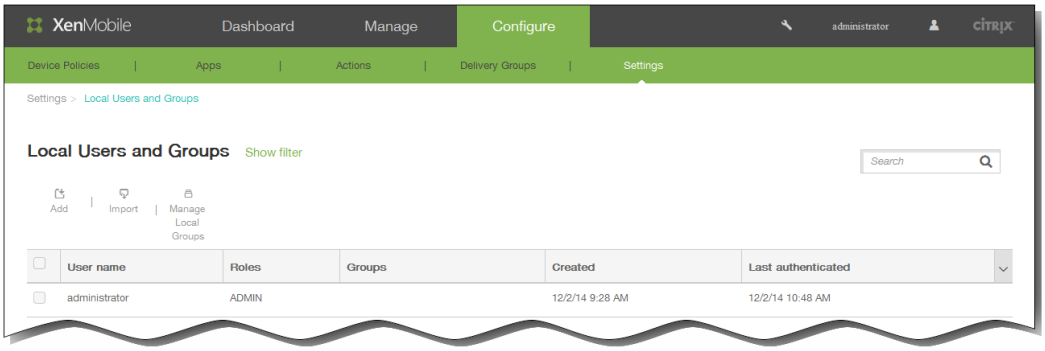
May 06, 2016

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.



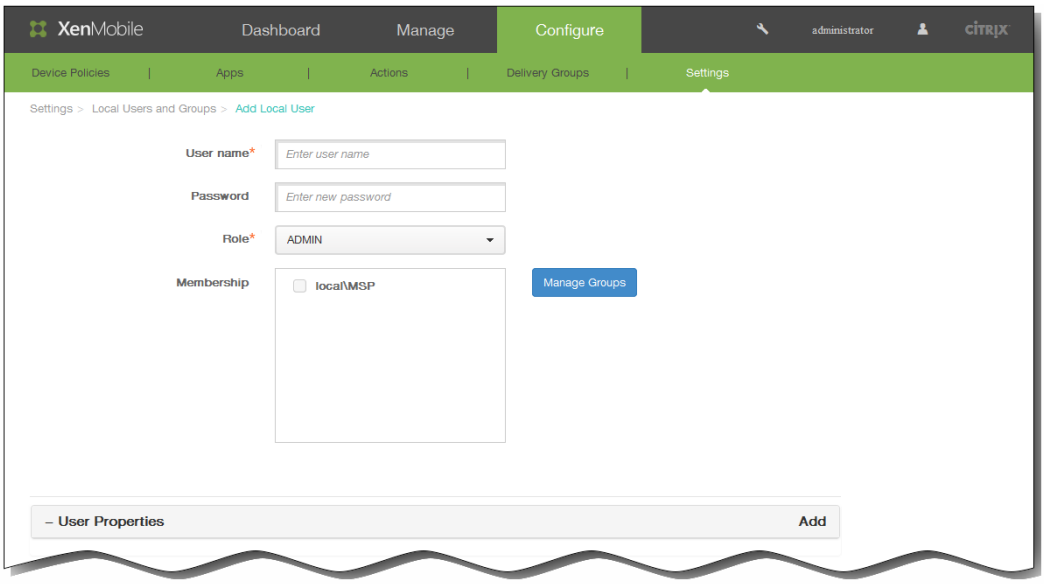
La page Groupes et utilisateurs locaux s'affiche.



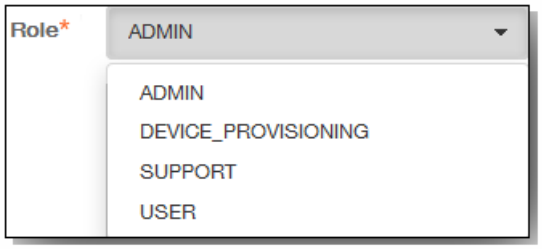
Pour ajouter un utilisateur local

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.

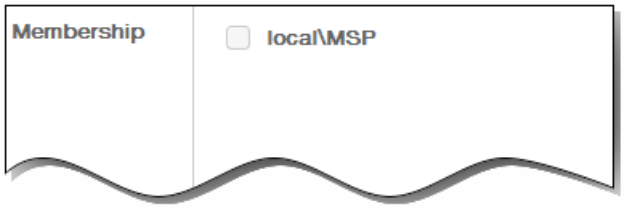
1. Sur la page Groupes et utilisateurs locaux, cliquez sur Ajouter. La page Ajouter un utilisateur local s'affiche.



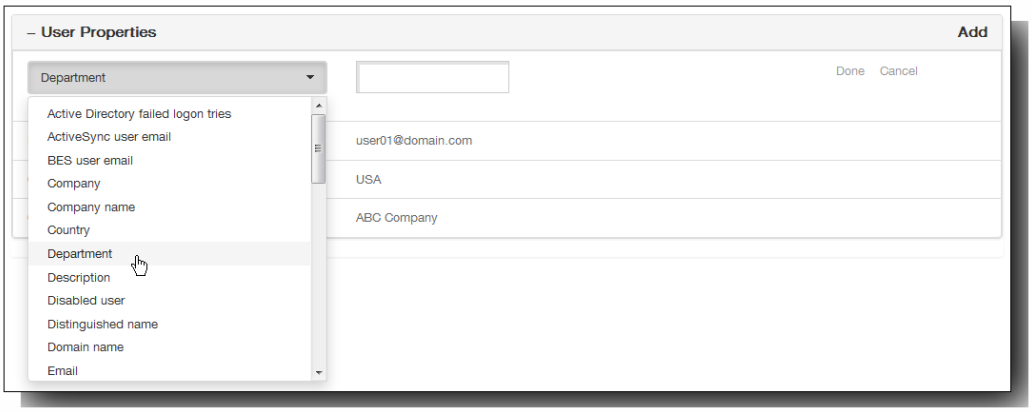
2. Entrez les informations suivantes pour ajouter un nouvel utilisateur local :
   1. Nom d'utilisateur : entrez le nom de l'utilisateur. Il s'agit d'un champ obligatoire.
   2. Mot de passe : entrez un mot de passe utilisateur (facultatif).
   3. Rôle : Dans la liste Rôle, cliquez sur le rôle d'utilisateur. 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.

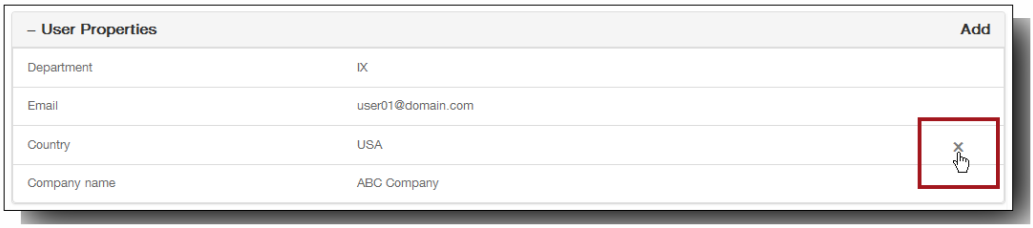


3. Pour ajouter des propriétés utilisateur (facultatif), suivez ces étapes :
   1. Cliquez sur Ajouter en regard de Propriétés utilisateur.
   2. Dans la liste Propriétés utilisateur, cliquez sur une propriété.
   3. Entrez l'attribut de propriété utilisateur dans le champ à côte de la liste.



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.

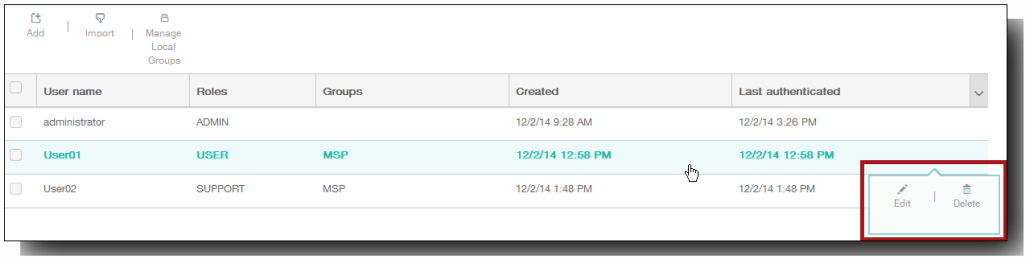
4. Éventuellement, pour modifier une propriété utilisateur, effectuez les opérations suivantes :
   1. Cliquez sur la propriété utilisateur que vous voulez modifier.
   2. Modifiez l'attribut de la propriété utilisateur.
   3. Cliquez sur Terminé pour enregistrer la modification ou cliquez sur Annuler 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.



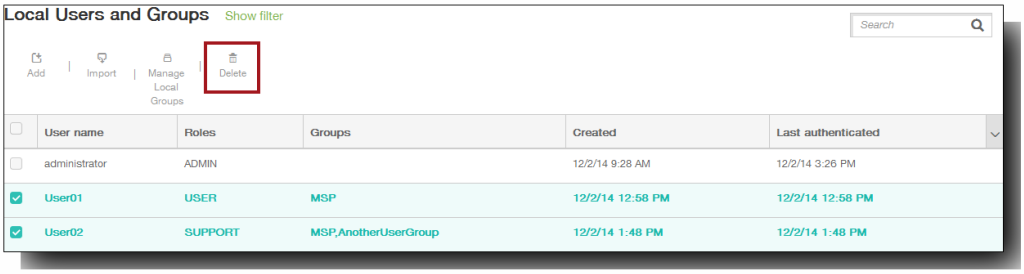
   La page Modifier un utilisateur local apparaît.
2. Modifiez les informations suivantes le cas échéant :
   1. Nom d'utilisateur : entrez le nom de l'utilisateur. Il s'agit d'un champ obligatoire.

2. Mot de passe : entrez un mot de passe utilisateur (facultatif).
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.

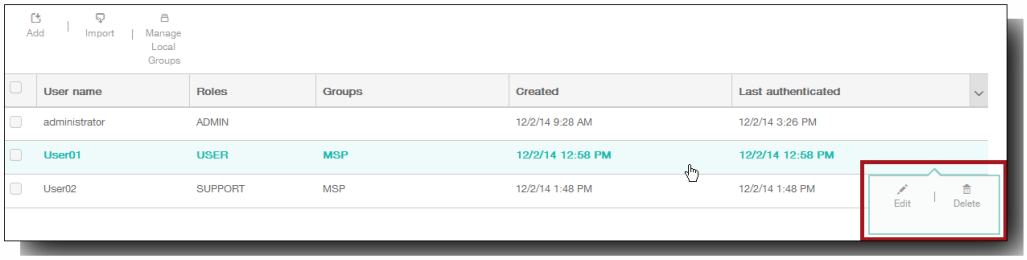
3. Cliquez sur Enregistrer pour enregistrer vos modifications.

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.

Importation de comptes utilisateur

May 06, 2016

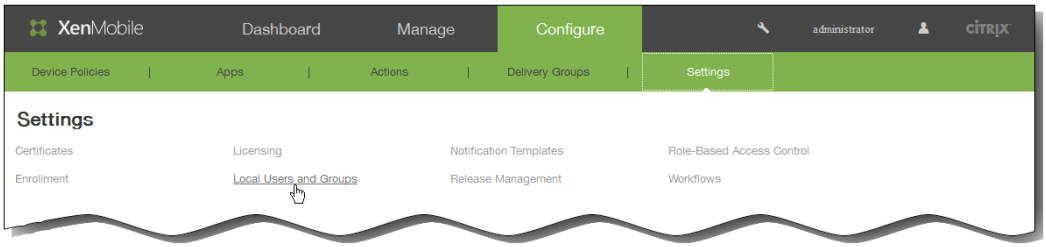
Vous pouvez importer des comptes utilisateur et des propriétés à partir d'un fichier .csv appelé fichier de provisioning, que vous pouvez créer manuellement. Pour de plus amples informations sur la mise en forme des fichiers de provisioning, consultez Formats des fichiers de provisioning.

Remarque :

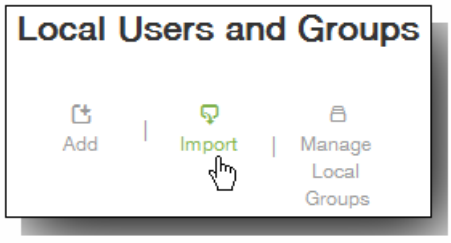
- Si vous importez des utilisateurs à partir d'un annuaire LDAP, utilisez le nom de domaine et le nom d'utilisateur dans le fichier d'importation. Par exemple, spécifiez le nomd'utilisateur@domaine.com. Cette syntaxe empêche d'autres recherches qui ralentiraient la vitesse d'importation.
- Si vous importez 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.

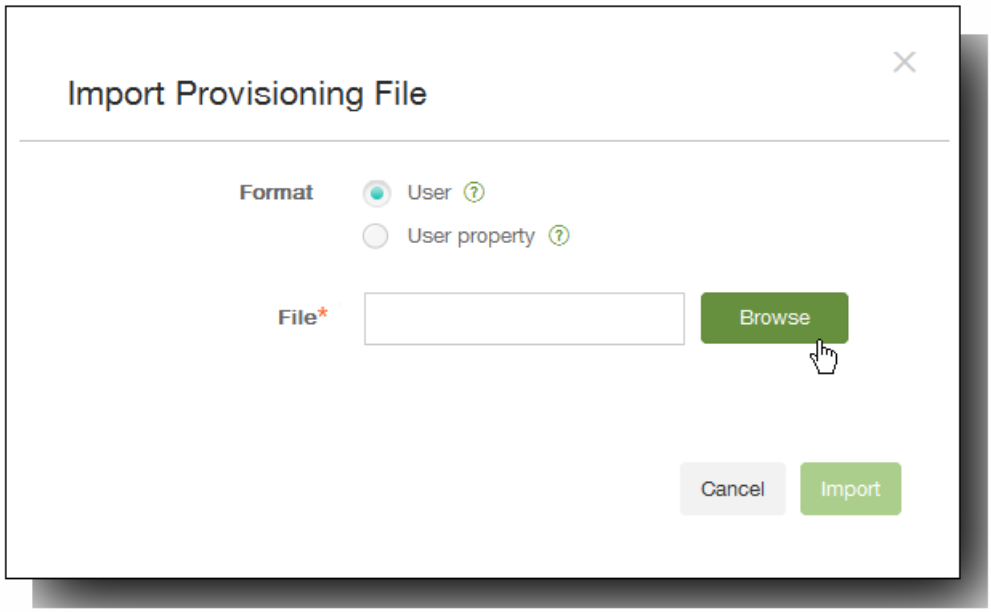


2. Sur la page Groupes et utilisateurs locaux, cliquez sur Importer.



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.



4. En regard de Fichier, cliquez sur Parcourir pour accéder à l'emplacement du fichier de provisioning, puis cliquez sur Importer.

Formats des fichiers de provisioning

May 06, 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

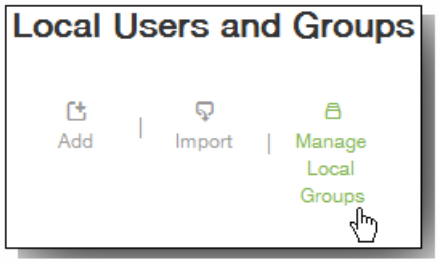
Ajout ou suppression de groupes

May 06, 2016

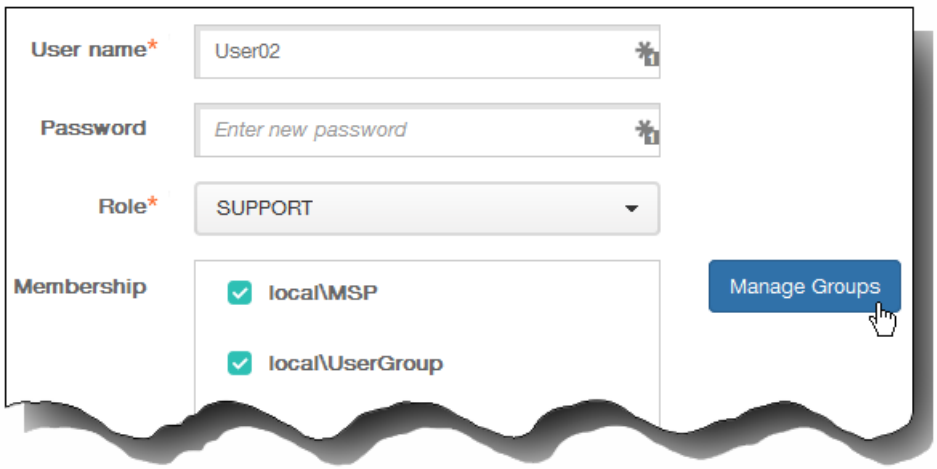
Vous gérez les groupes dans la boîte de dialogue Gérer les groupes dans la console XenMobile, que vous pouvez trouver sur la page Groupes et utilisateurs locaux, la page Ajouter un utilisateur local où la page Modifier un utilisateur local. Aucune commande ne permet de modifier un groupe. Si vous supprimez 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

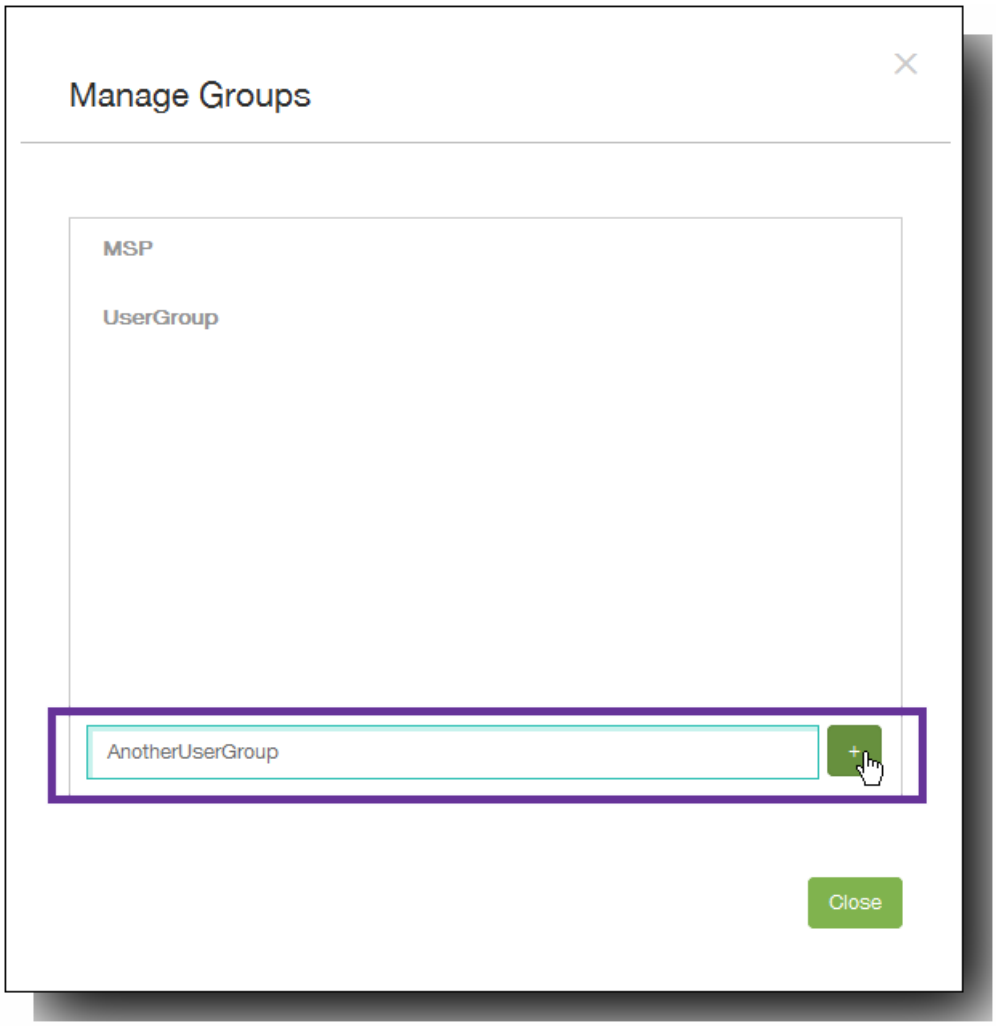
1. Procédez comme suit :
   - Sur la page Groupes et utilisateurs locaux, cliquez sur Gérer les groupes locaux.



   - 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 (+).



Le groupe d'utilisateurs est ajouté à la liste.

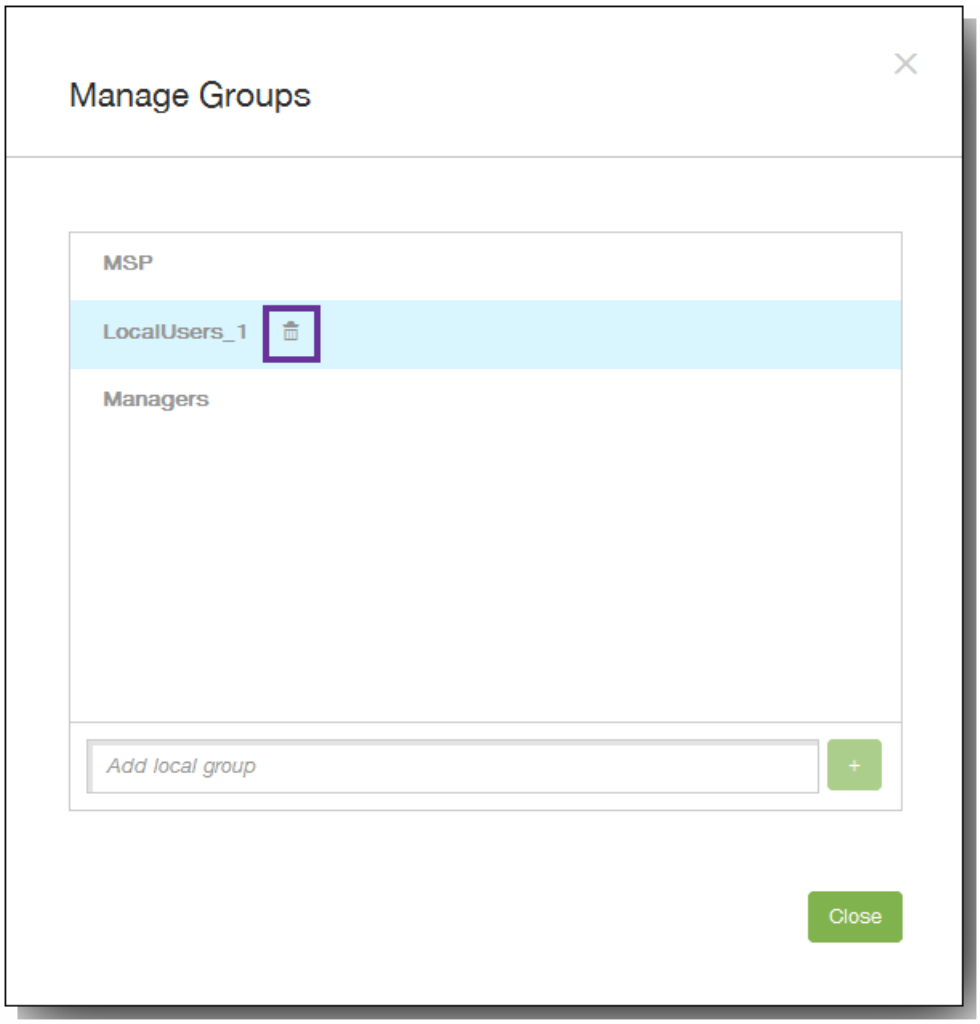
3. Cliquez sur Fermer.

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.



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.

Pour configurer des modes d'inscription et activer le portail en libre-service

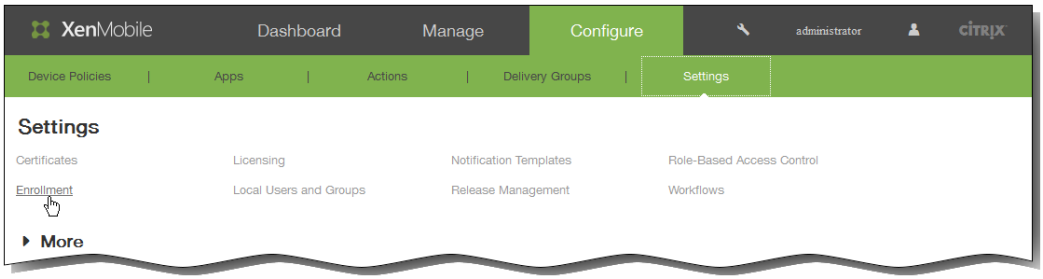
May 06, 2016

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.

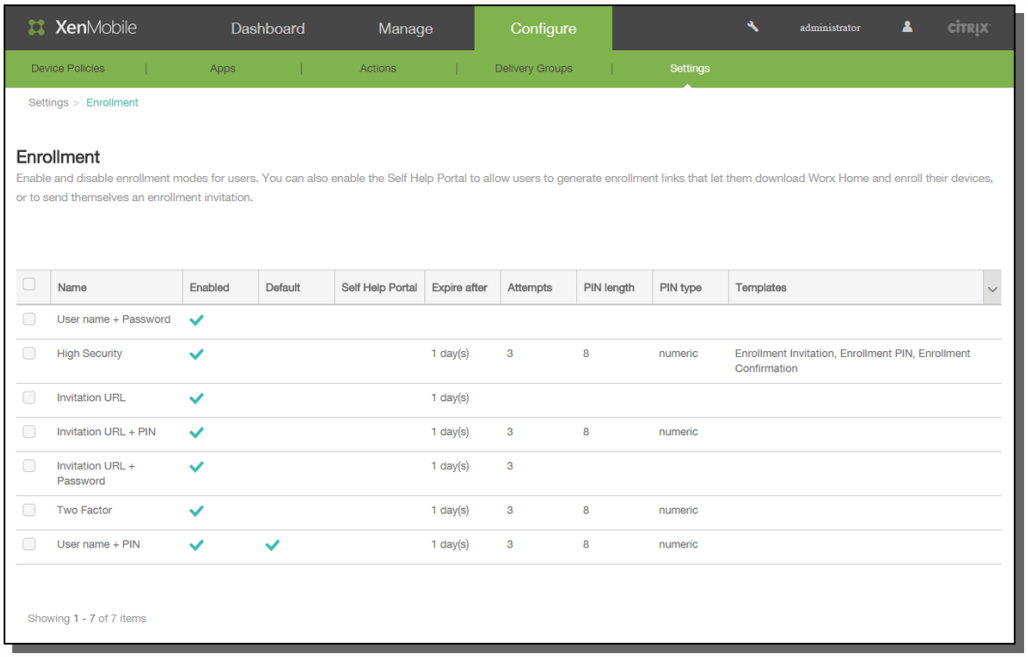
Vous configurez les modes d'inscription dans la console XenMobile sur la page Paramètres > Inscription. Vous envoyez des invitations d'inscription depuis la console XenMobile, à partir de la page Gérer > Inscription (voir Inscription d'utilisateurs et d'appareils dans XenMobile).

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.

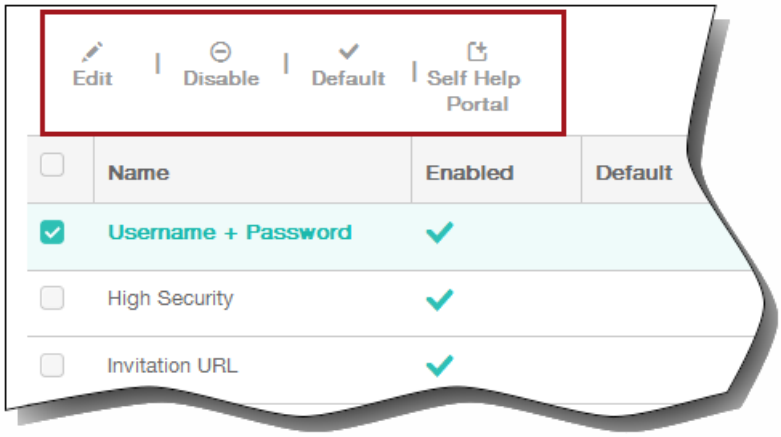
1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Inscription.

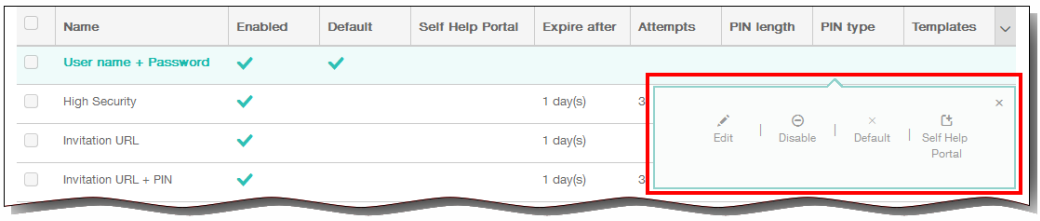


La page Inscription s'affiche. Elle contient un tableau de tous les modes d'inscription disponibles.



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.

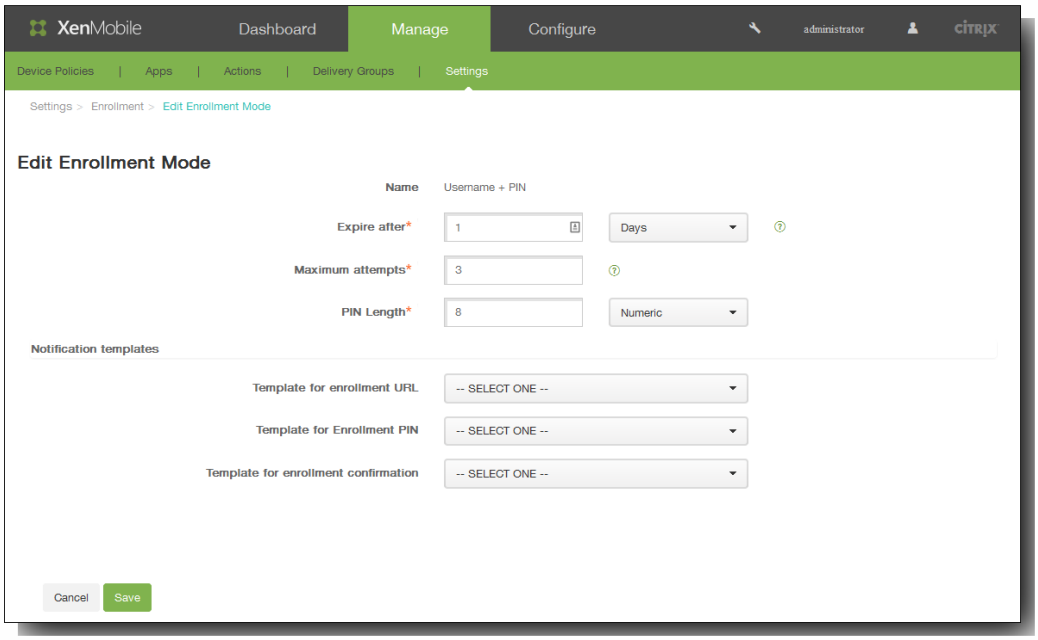




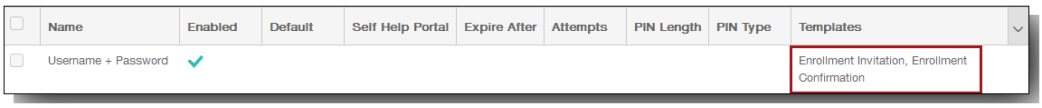
Pour modifier un mode d'inscription

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.



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.



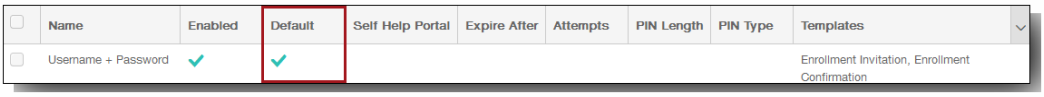
Pour définir un mode d'inscription comme mode par défaut

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 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.

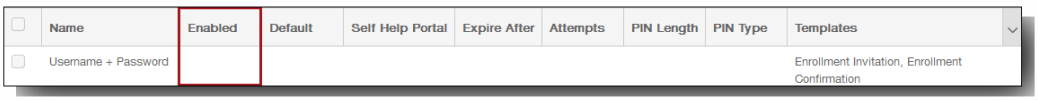
1. Sélectionnez l'un des trois modes suivants à définir comme mode d'inscription par défaut : Nom d'utilisateur + mots de passe, Deux facteurs ou Nom d'utilisateur + PIN.
   Remarque : le mode sélectionné doit être activé pour être défini comme mode par défaut.
2. Cliquez sur Mode par défaut. Le mode 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.



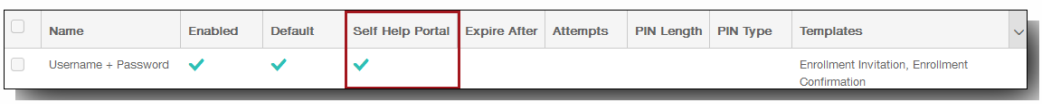
Pour activer un mode d'inscription sur le portail en libre-service

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.



Configuration de rôles avec RBAC

May 06, 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.
- **Provisioning**. Utilisé par les administrateurs pour provisionner tous les appareils Windows Mobile/CE en tant que groupe à l'aide de l'outil de provisioning d'appareil.
- **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.

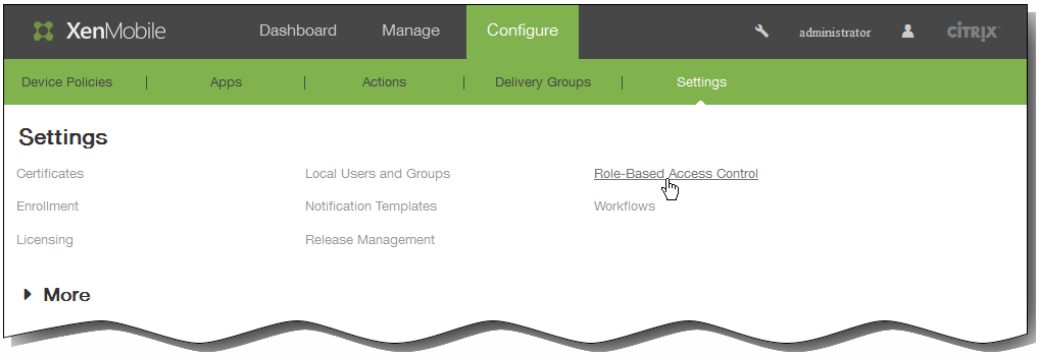
Les rôles peuvent être attribués à des utilisateurs locaux (au niveau de l'utilisateur) ou à des groupes Active Directory (tous les utilisateurs de ce groupe ont les mêmes autorisations). Si un utilisateur appartient à plusieurs groupes Active Directory, les autorisations sont fusionnées pour définir 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.

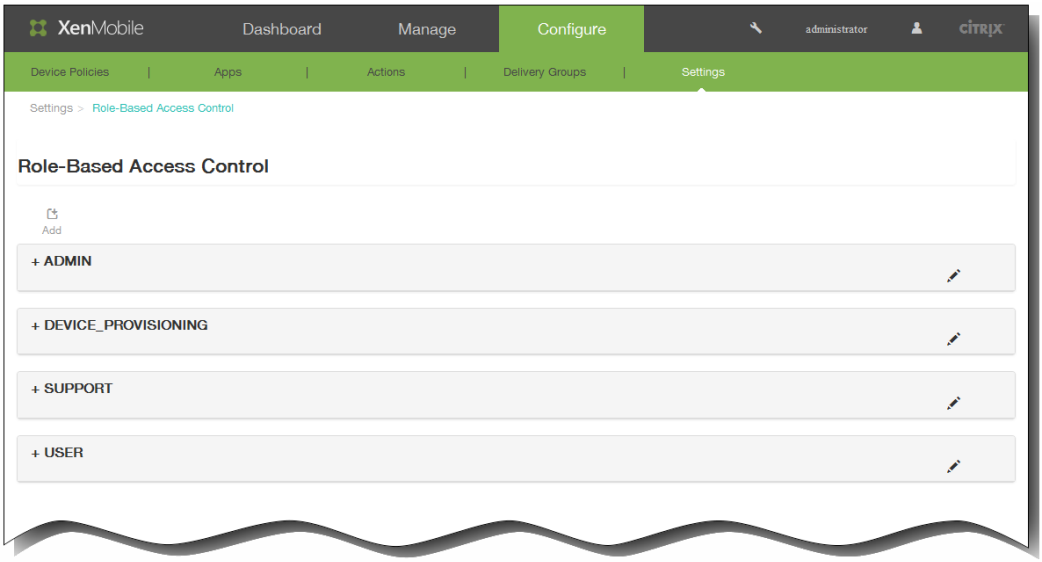
Vous pouvez utiliser la fonctionnalité RBAC dans XenMobile pour effectuer les opérations suivantes :

- Créer un nouveau rôle.
- Ajouter des groupes à un rôle.
- Associer des utilisateurs locaux aux rôles.

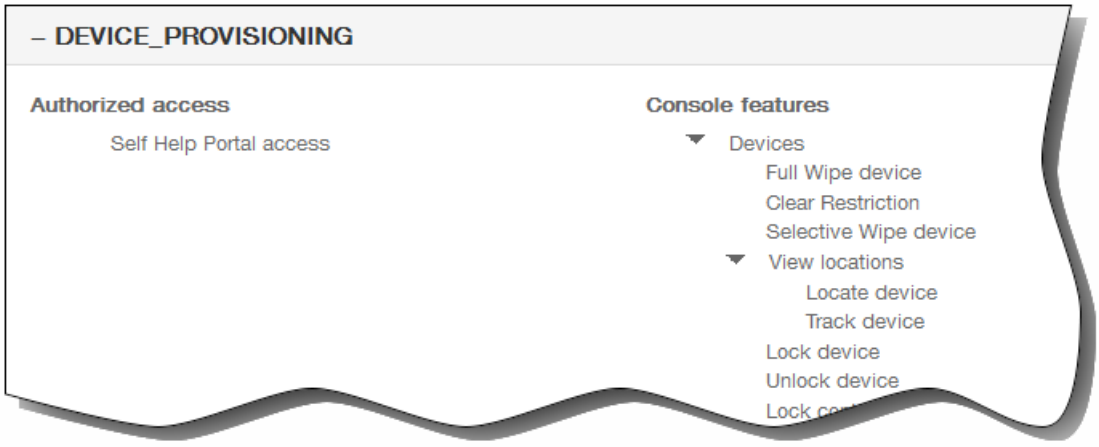
1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Contrôle d'accès basé sur un rôle.



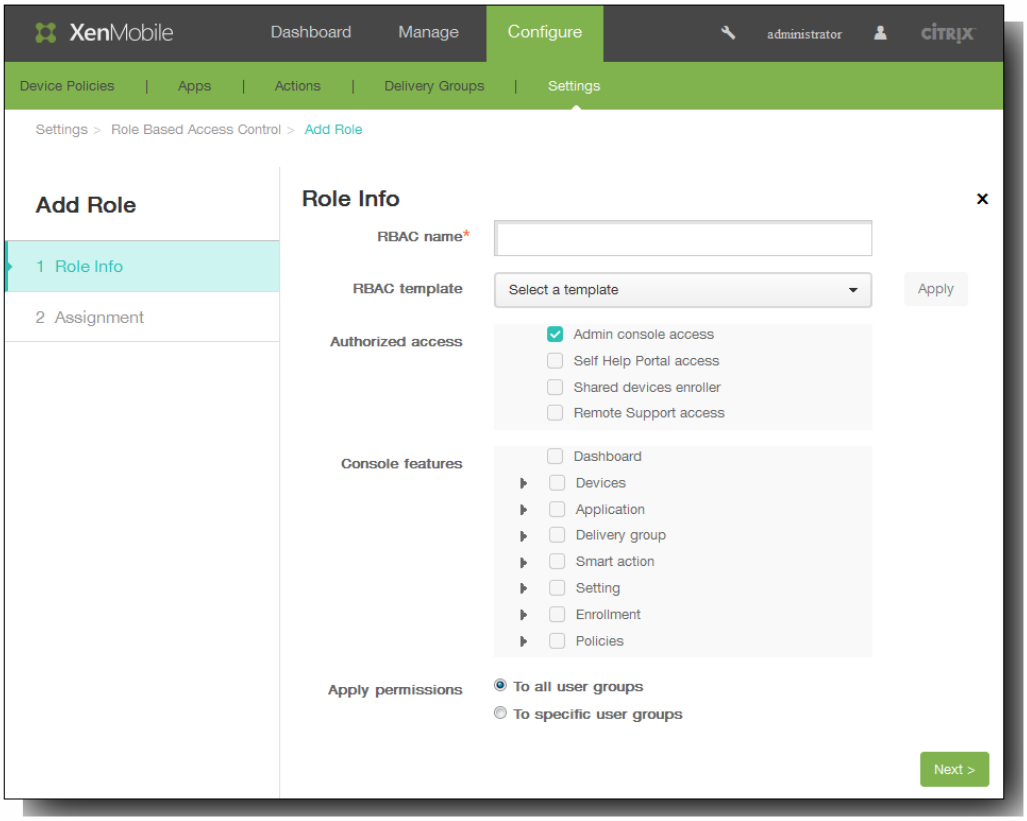
La page Rôle qui apparaît affiche les quatre rôles utilisateur par défaut, ainsi que tout rôle que vous avez déjà ajouté.



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.

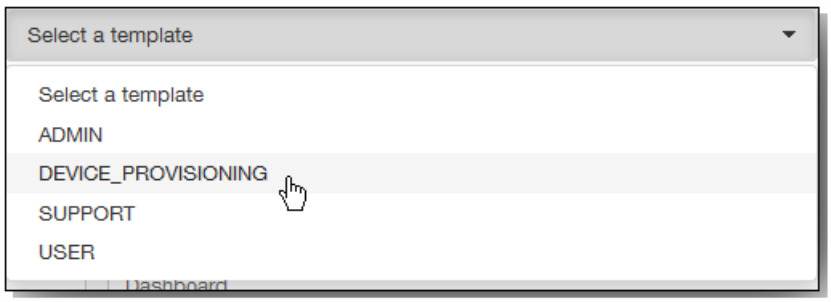


2. Cliquez sur Ajouter pour ajouter un nouveau rôle utilisateur, cliquez sur l'icône de crayon à droite d'un rôle existant pour modifier le rôle, ou cliquez sur l'icône de corbeille à droite d'un rôle que vous avez précédemment défini pour supprimer le rôle. Vous ne pouvez pas supprimer les rôles utilisateur par défaut.
   - Lorsque vous cliquez sur Ajouter ou l'icône de crayon, la page Ajouter un rôle ou Modifier le rôle s'affiche.

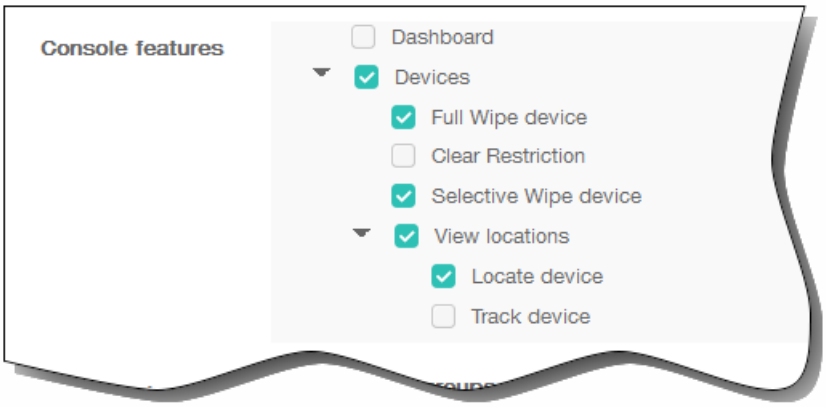


- Lorsque vous cliquez sur l'icône de corbeille, une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer le rôle sélectionné.

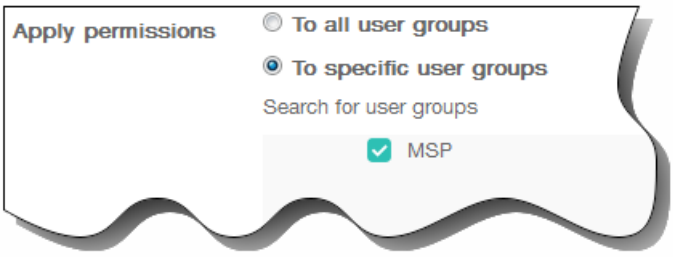
3. Entrez les informations suivantes pour créer un nouveau rôle utilisateur ou pour modifier un rôle utilisateur existant :
    1. Nom RBAC : entrez un nom descriptif pour le nouveau rôle utilisateur. Vous ne pouvez pas modifier le nom d'un rôle existant.
    2. Modèle RBAC : cliquez sur un modèle à 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.



- 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.

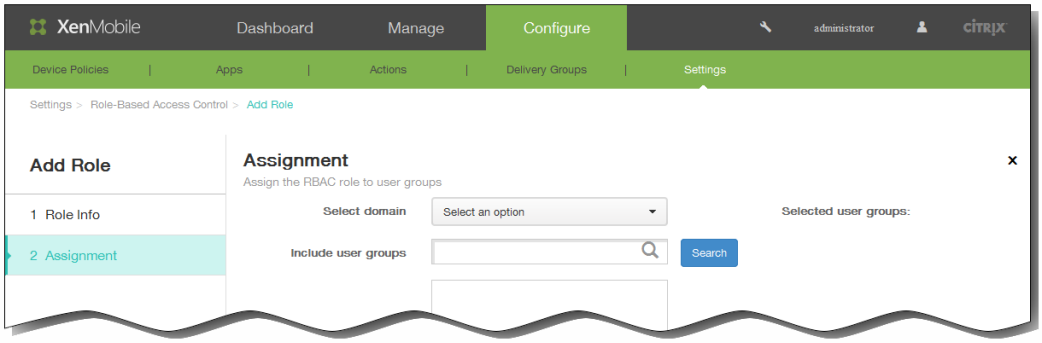


3. Appliquer les autorisations : sélectionnez les groupes auxquels vous voulez appliquer les autorisations sélectionnées.

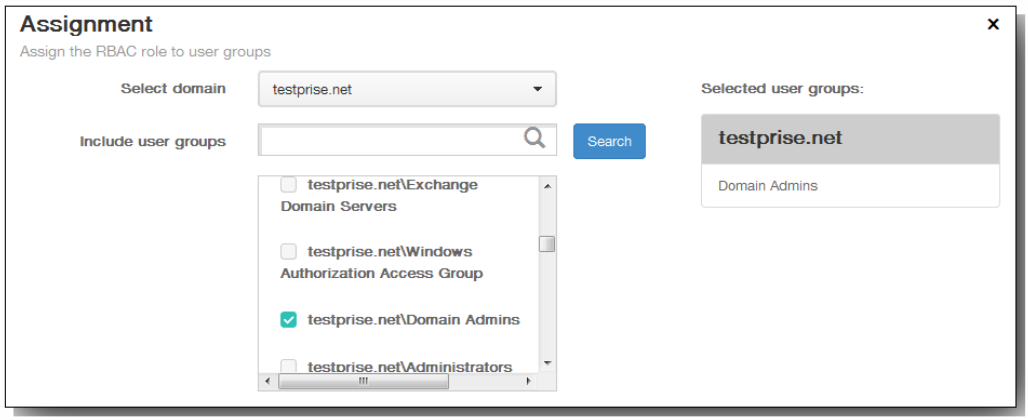


Si vous cliquez sur À des groupes d'utilisateurs spécifiques, une liste des groupes s'affiche à partir de laquelle vous pouvez sélectionner un ou plusieurs groupes.

4. Cliquez sur Suivant. La page Attribution s'affiche.



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 une liste des groupes sélectionnés à droite de la zone de recherche.



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.

Pour activer la découverte automatique pour l'inscription utilisateur dans XenMobile

Oct 11, 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 ces détails sur le serveur XenMobile. Le nom d'utilisateur doit être entré au format UPN (nom d'utilisateur principal) ; par exemple, utilisateur@monentreprise.com.

Pour activer la détection automatique, vous pouvez accéder au portail Autodiscovery Service 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).

- Les SAN appropriés pour les domaines restants (par exemple, enterpriseenrollment.masociété2.com, enterpriseenrollment.masociété3.com, etc).

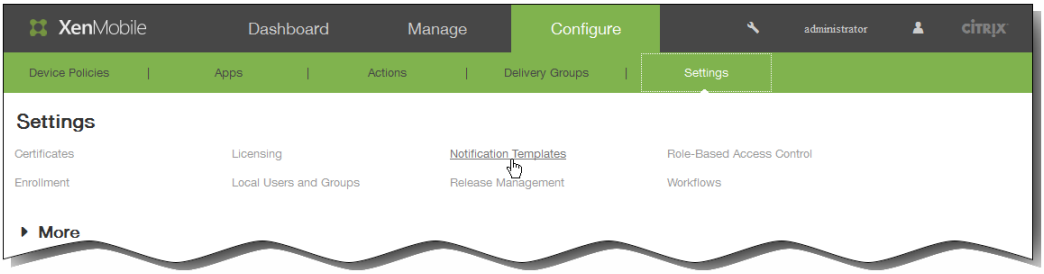
Création et mise à jour de modèles de notification

May 06, 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

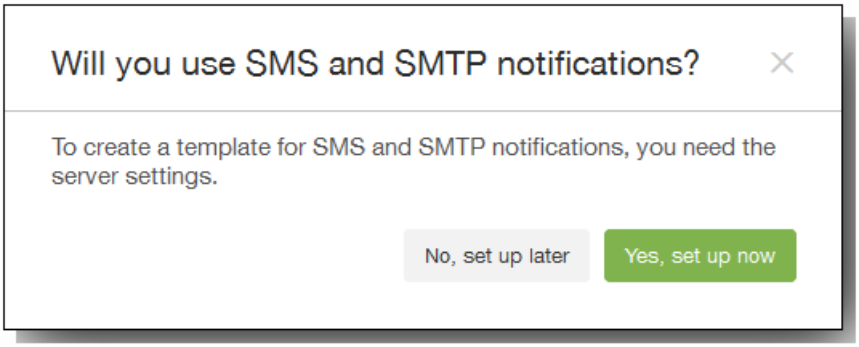
1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Modèles de notification.



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.

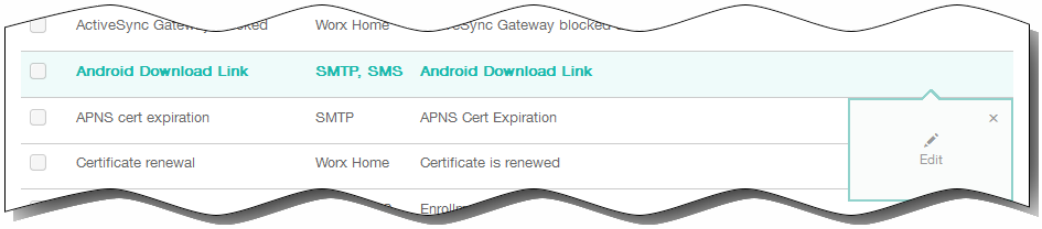
     Important : si vous choisissez de configurer les paramètres de passerelle SMS ou de serveur SMTP ultérieurement, vous ne pourrez pas activer ces canaux lorsque vous ajoutez ou modifiez un modèle de notification, ce qui signifie que ces canaux ne seront pas disponibles pour l'envoi de notifications aux utilisateurs.



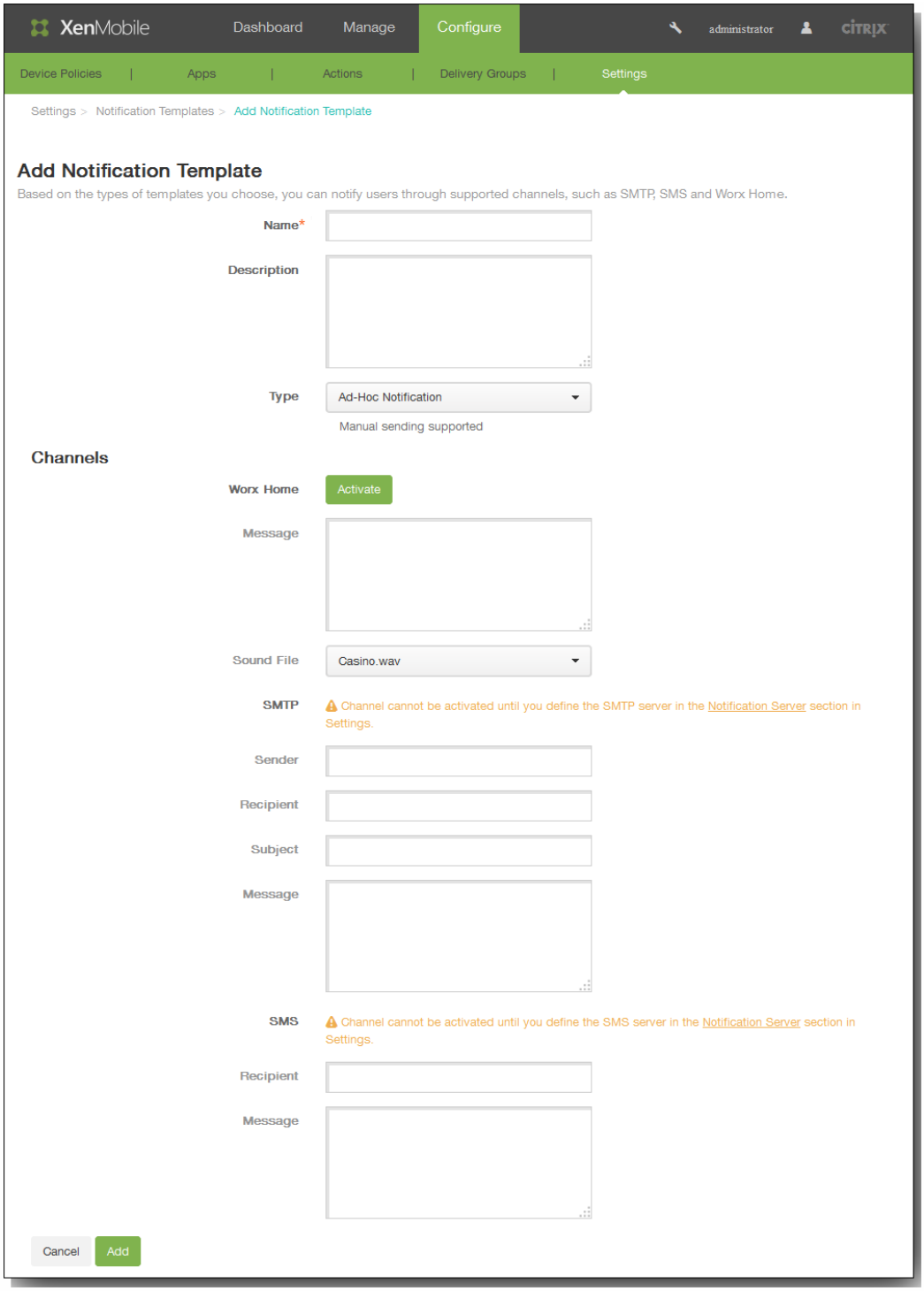
   - Sélectionnez un modèle existant à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.

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.



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 :

- ${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 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.

Gestion des groupes de mise à disposition

May 06, 2016

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 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.

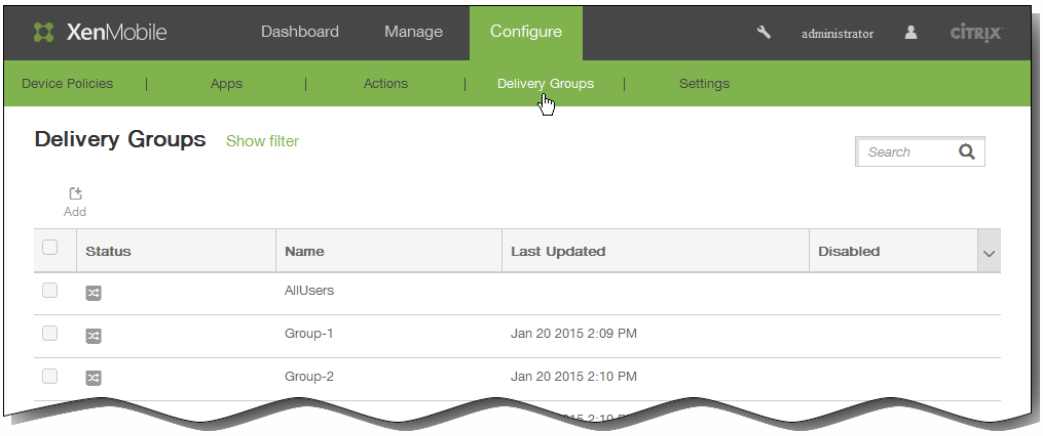
Le groupe de mise à disposition par défaut AllUsers est créé lorsque vous installez et configurez XenMobile. Il contient à tous les utilisateurs locaux et utilisateurs Active Directory. Vous ne pouvez pas supprimer le groupe AllUsers, mais vous pouvez le désactiver si vous ne souhaitez pas envoyer des ressources à tous les utilisateurs.

Vous pouvez ajouter, modifier, désactiver, activer, déployer et supprimer des groupes de mise à disposition dans XenMobile pour gérer la manière dont les stratégies, les applications et les actions sont déployées auprès de vos utilisateurs. Chacune de ces actions est décrite en détail dans les sections suivantes de cette rubrique :

- Pour ajouter un groupe de mise à disposition
- Pour modifier un groupe de mise à disposition
- Pour activer et désactiver le groupe de mise à disposition AllUsers
- Pour déployer des groupes de mise à disposition
- Pour supprimer des groupes de mise à disposition

Pour commencer à gérer vos groupes de mise à disposition, ouvrez la page Groupes de mise à disposition comme suit :

1. Dans la console XenMobile, cliquez sur Configurer > Groupes de mise à disposition.

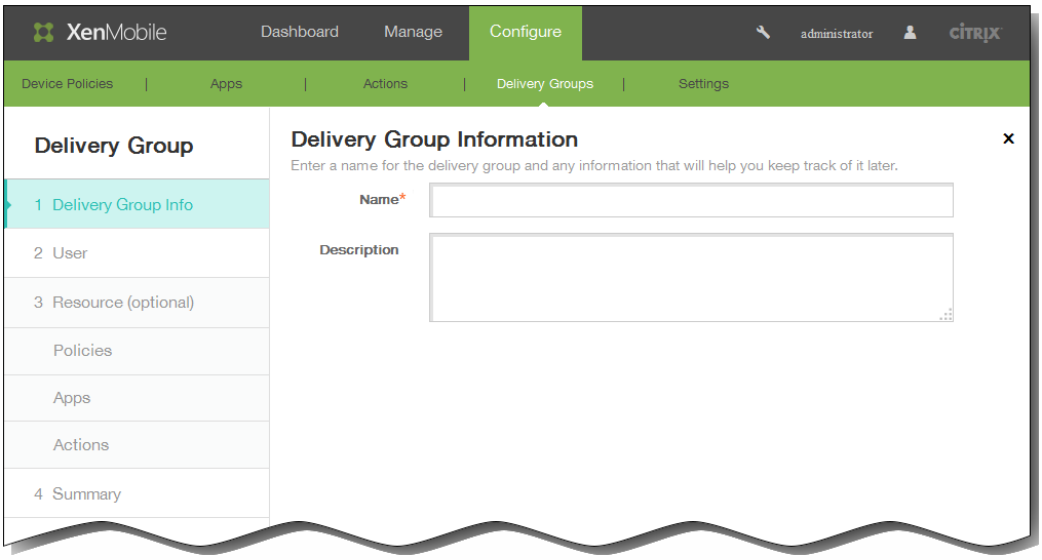


La page Groupes de mise à disposition s'affiche. Reportez-vous ensuite à la rubrique eDocs correspondant à l'action que

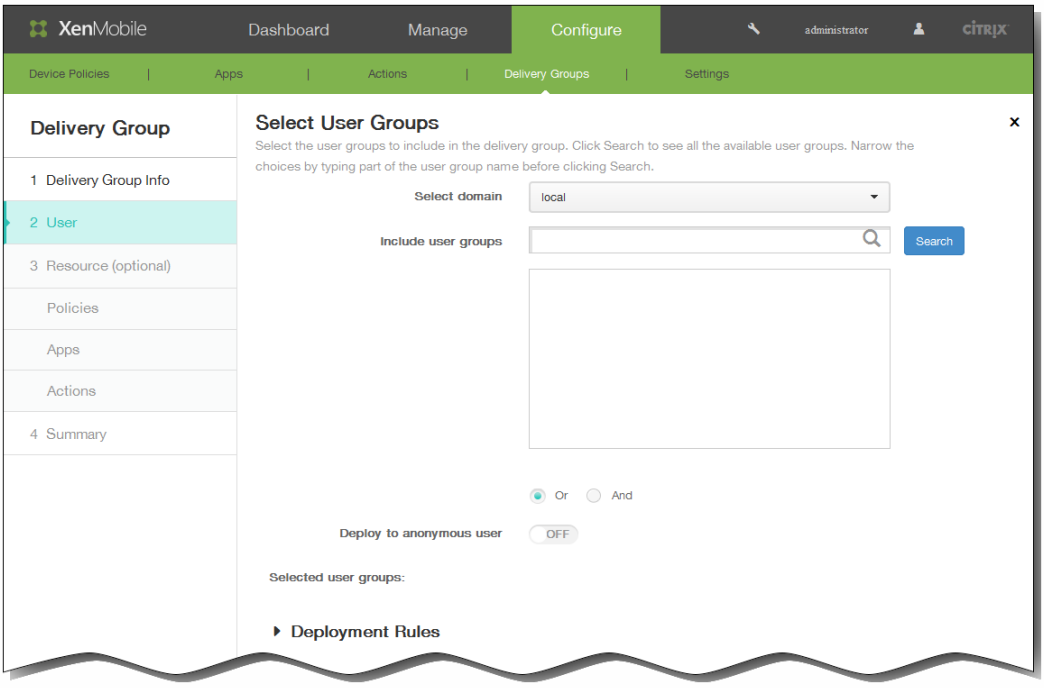
vous souhaitez effectuer.

Pour ajouter un groupe de mise à disposition

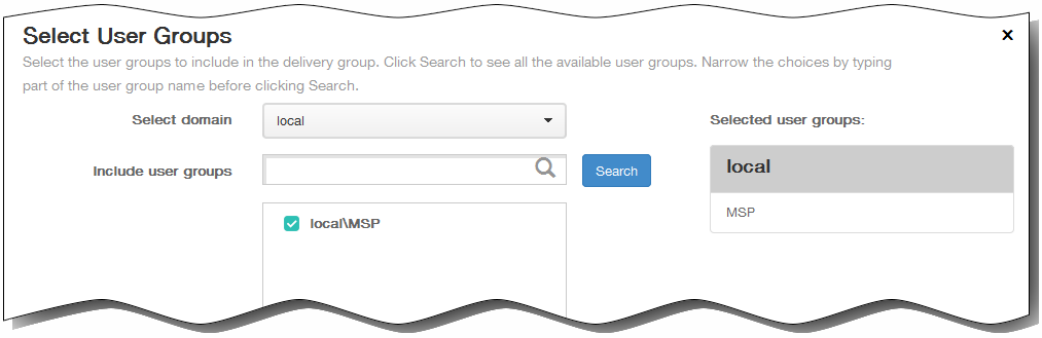
1. Sur la page Groupes de mise à disposition, cliquez sur Ajouter. La page Informations sur le groupe de mise à disposition s'affiche.



2. Dans le panneau Informations sur le groupe de mise à disposition, entrez les informations suivantes :
   1. Nom : entrez un nom descriptif pour le groupe de mise à disposition.
   2. Description : entrez une description pour le groupe de mise à disposition (facultatif).
3. Cliquez sur Next. La page Utilisateur du groupe de mise à disposition s'affiche.



4. Dans le panneau Sélectionner des groupes d'utilisateurs, entrez 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.



    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.

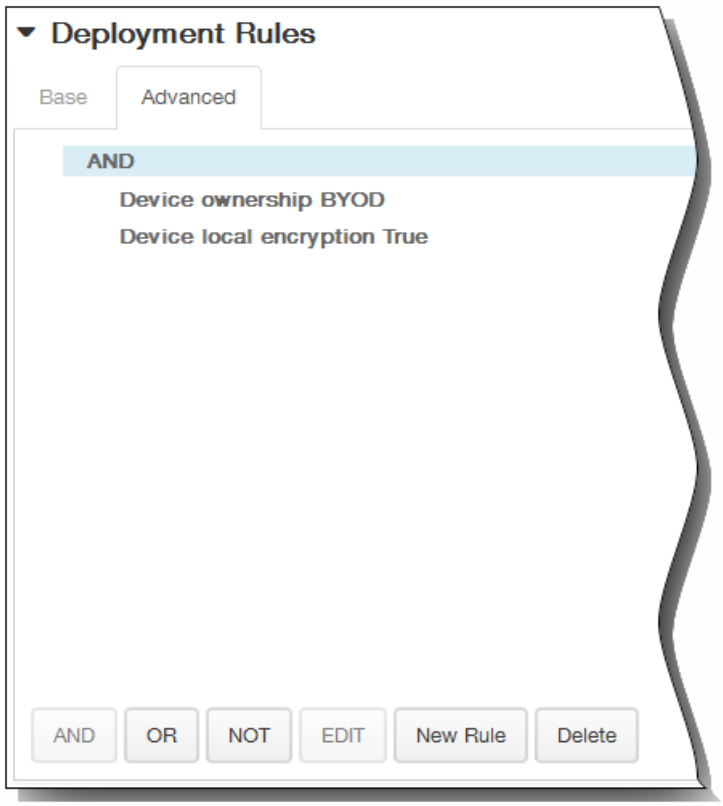
    Les groupes d'utilisateurs figurant dans la liste Groupes d'utilisateurs sélectionnés ont des coches en regard de leur nom dans la liste qui s'affiche. Parcourez la liste et décochez la case à cocher en regard de chaque groupe à supprimer.

    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 que la ressource puisse leur être déployée.
    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.
5. 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.

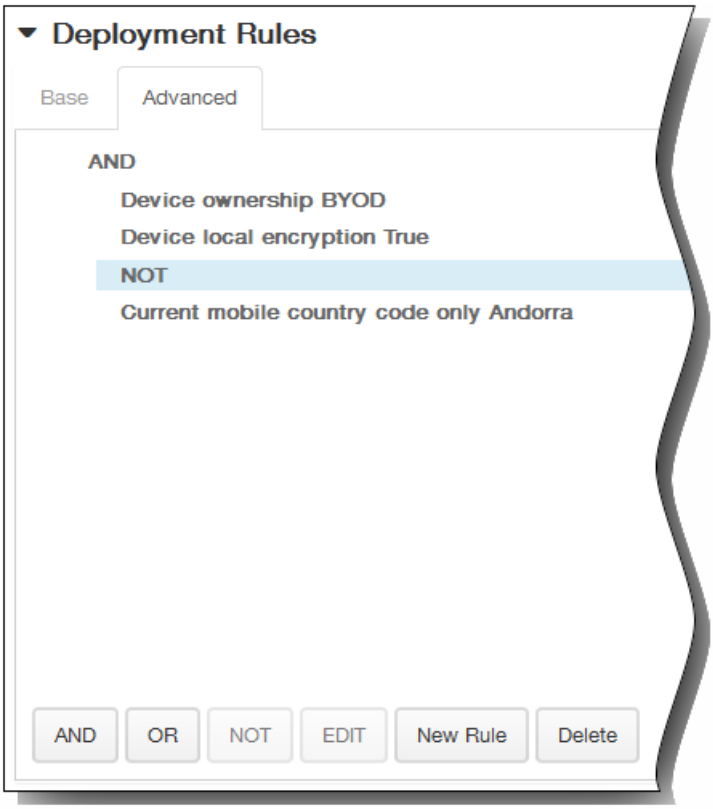
1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme 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.

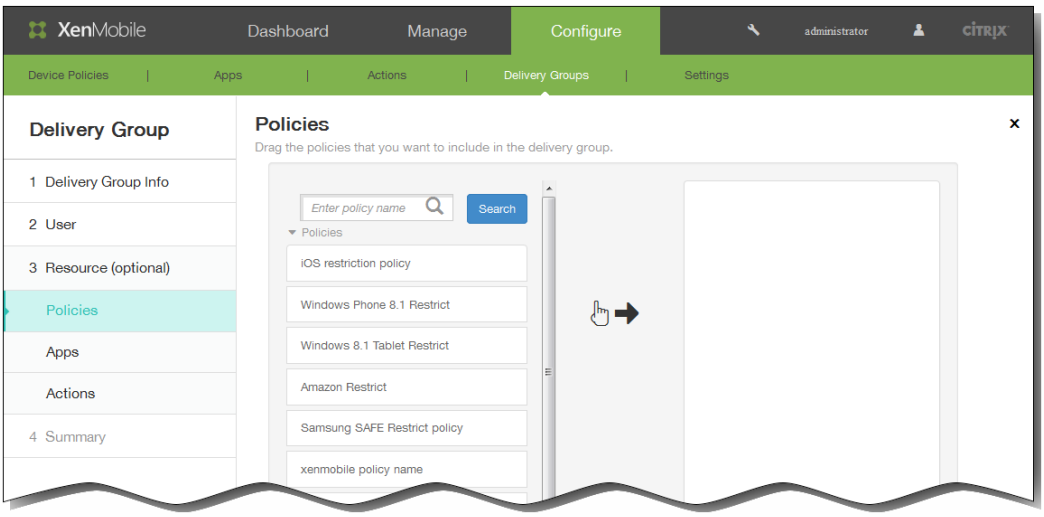


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
      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.

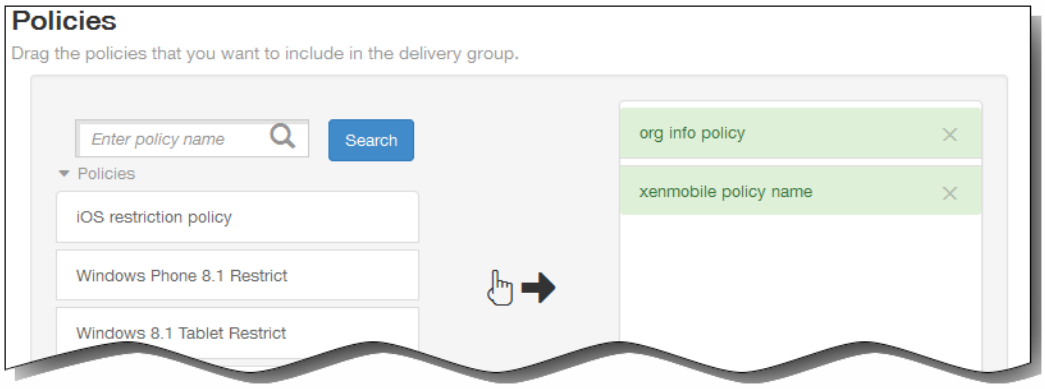


6. Cliquez sur Next. La page Ressources du groupe de mise à disposition s'affiche. Vous pouvez éventuellement ajouter des stratégies, des applications ou des actions pour le groupe de mise à disposition. Pour ignorer cette étape, sous Groupe de mise à disposition, cliquez sur Résumé pour afficher un 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



1. 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.

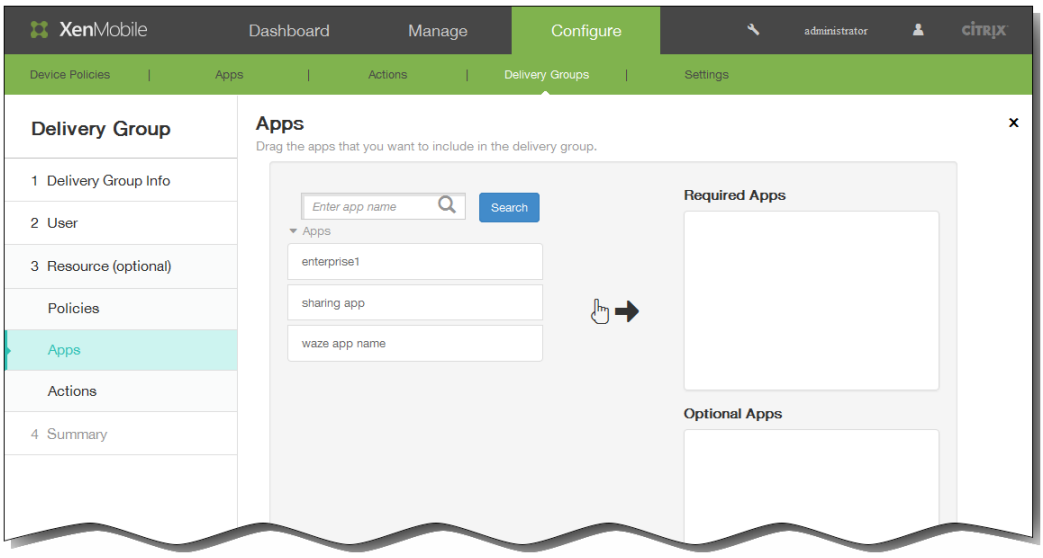
2. Cliquez sur une stratégie et faites-la glisser dans la zone de droite.
3. Répétez les étapes a et b pour ajouter d'autres stratégies.



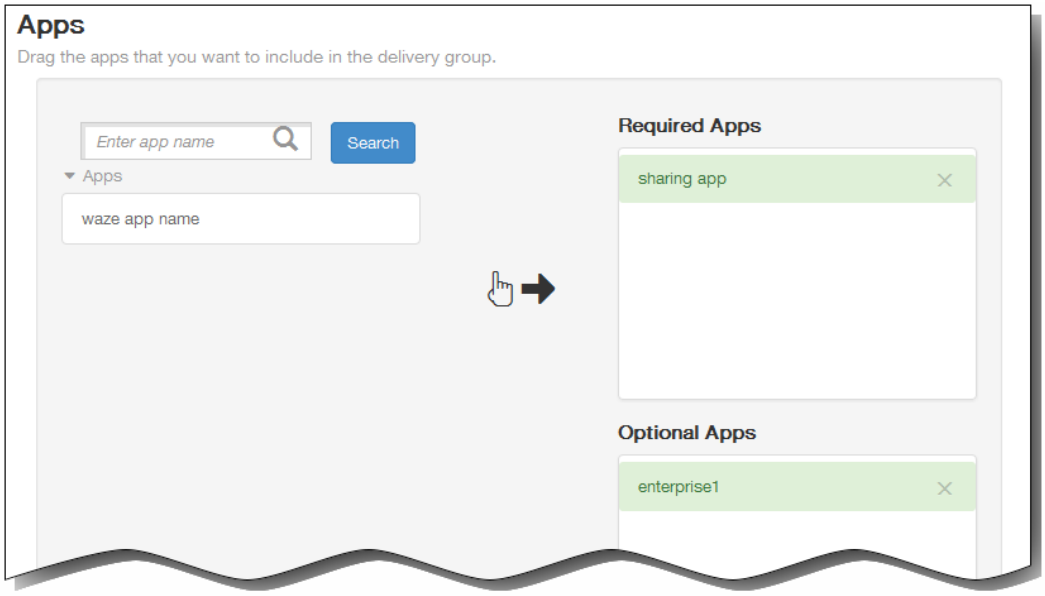
Pour supprimer une ressource de stratégie, cliquez sur le X en regard du nom de la stratégie.

4. 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. L'une ou l'autre de la page de ressource Applications ou de la page Résumé s'affiche.

Pour ajouter des applications



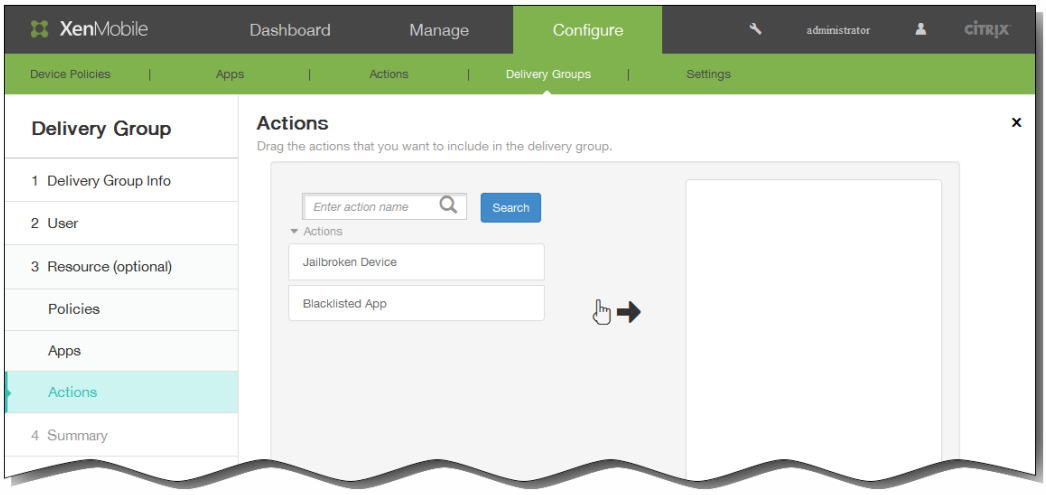
1. Parcourez la liste des applications disponibles pour trouver l'application que vous souhaitez ajouter, ou pour limiter la liste des applications, tapez un nom d'application complet ou partiel dans la zone de recherche et cliquez sur Rechercher.
2. Cliquez sur une application et faites-la glisser dans la zone Applications requises ou Applications facultatives.
3. Répétez les étapes a et b pour ajouter plus d'applications.



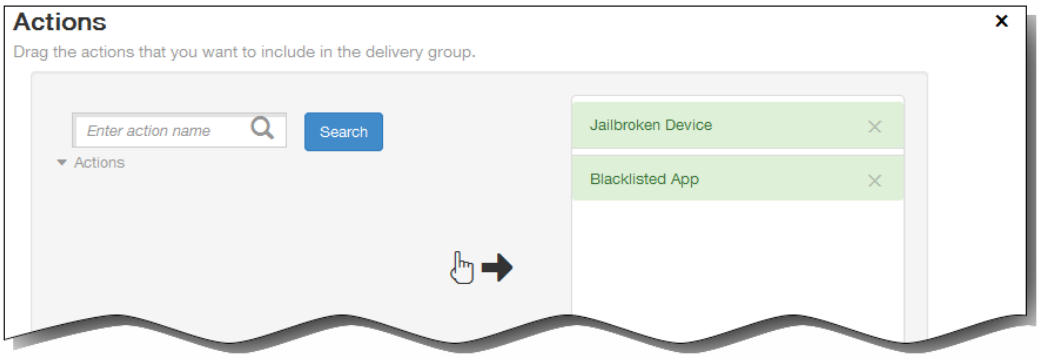
Pour supprimer une ressource d'application, cliquez sur le X en regard du nom de l'application.

4. 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. L'une ou l'autre de la page de ressource Actions ou de la page Résumé s'affiche.

Pour ajouter des actions

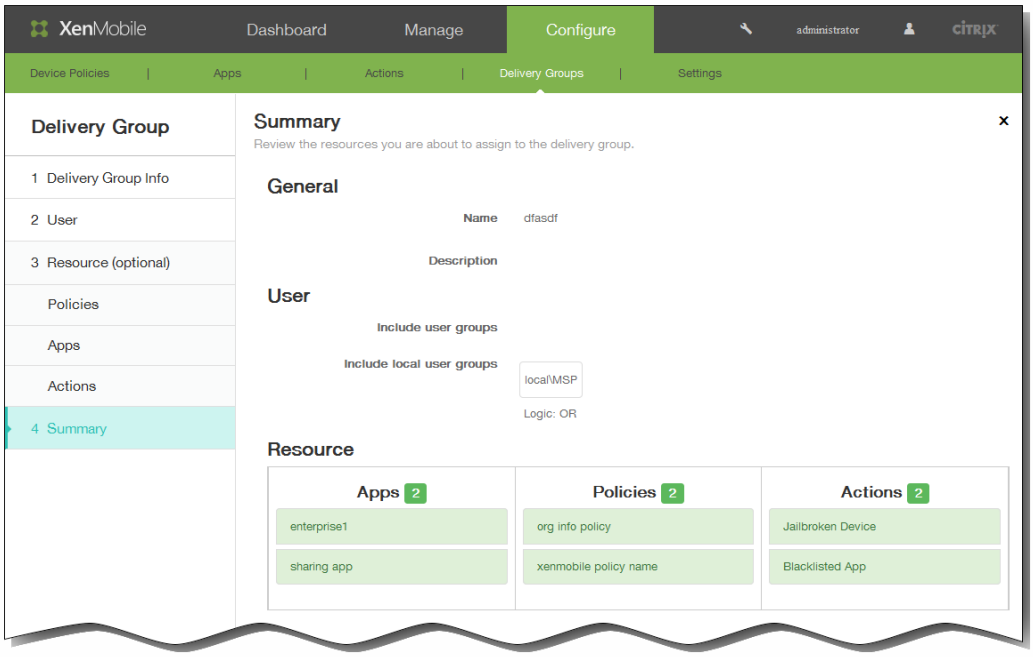


1. Parcourez la liste des actions disponibles pour trouver l'action que vous souhaitez ajouter, ou pour limiter la liste des actions, tapez un nom d'action complet ou partiel dans la zone de recherche et cliquez sur Rechercher.
2. Cliquez sur une action et faites-la glisser dans la zone de droite.
3. Répétez les étapes a et b pour ajouter plus d'actions.



Pour supprimer une ressource d'action, cliquez sur le X en regard du nom de l'action.

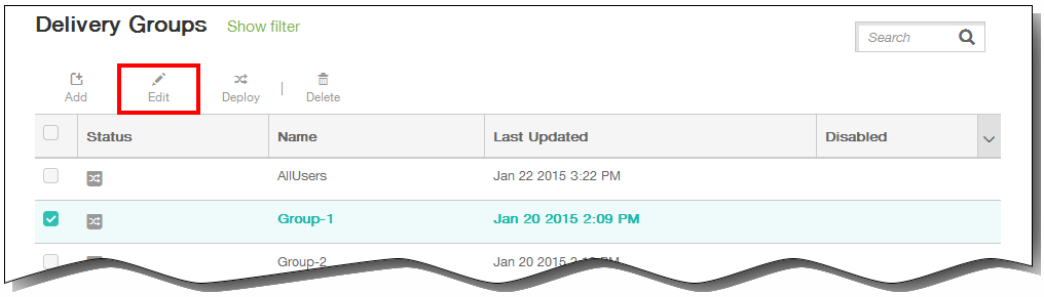
4. Cliquez sur Suivant. La page Résumé s'affiche.

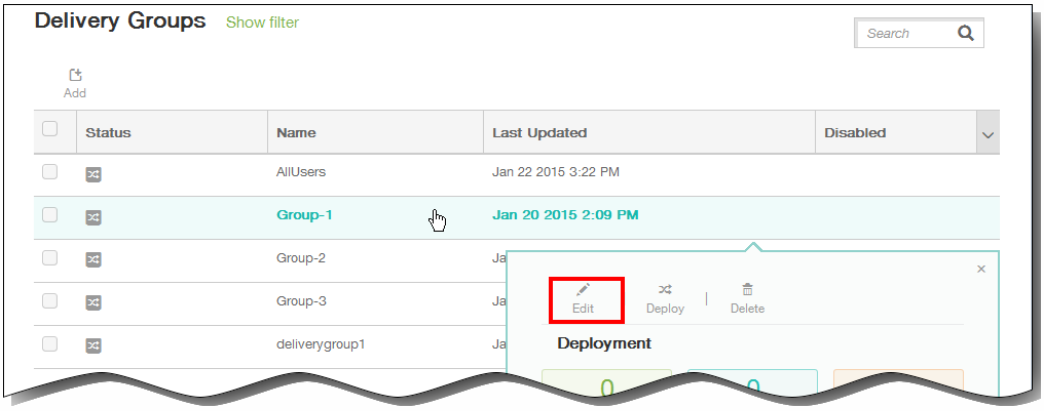


7. Sur la page Résumé, vérifiez les options que vous avez configurées pour le groupe de mise à disposition. Cliquez sur Précédent pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.
8. Cliquez sur Enregistrer pour enregistrer le groupe de mise à disposition.

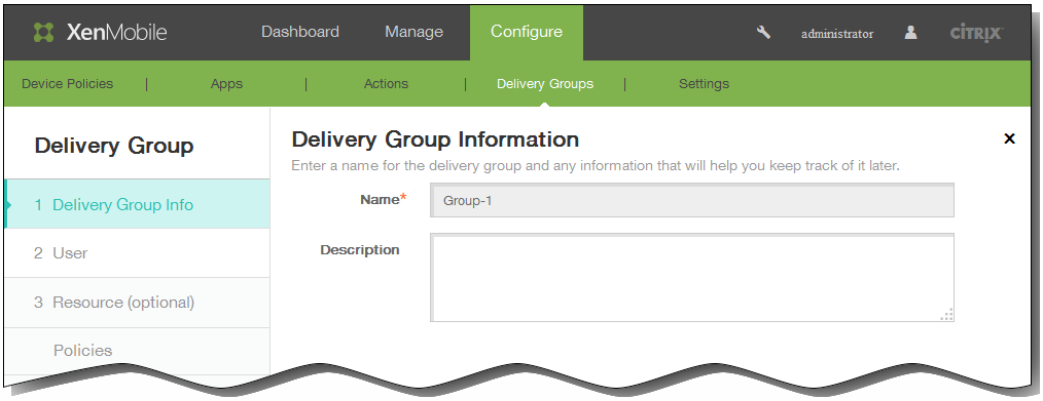
Pour modifier un groupe de mise à disposition

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.

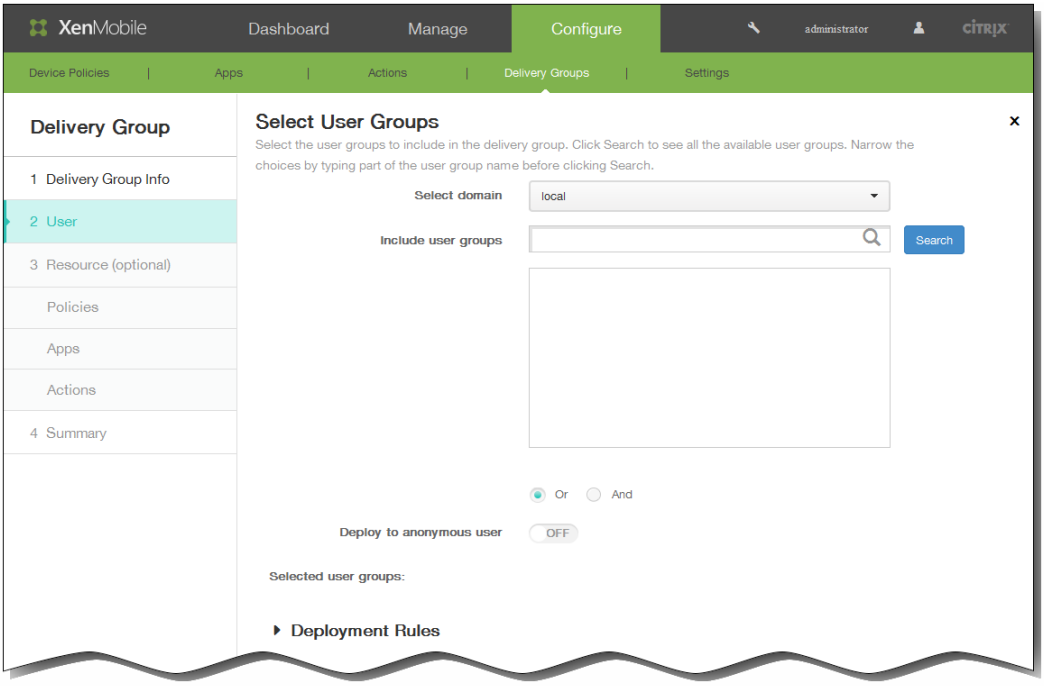




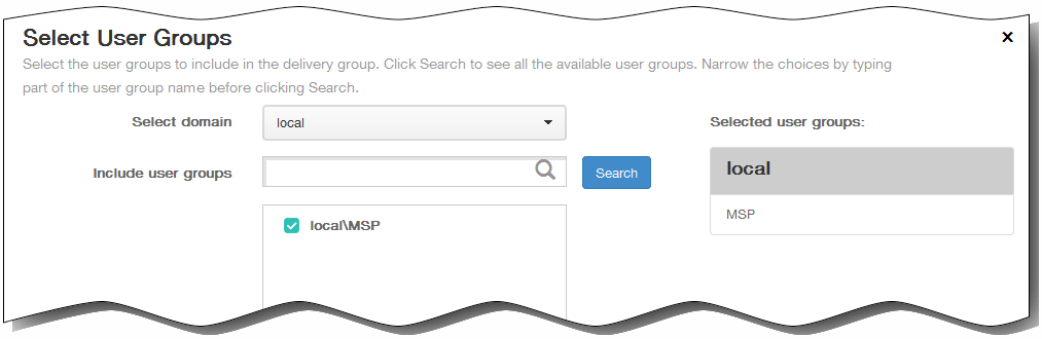
La page de modification des Informations sur le groupe de mise à disposition s'affiche.



3. Ajoutez ou modifiez la description.
   Remarque : vous ne pouvez pas modifier le nom d'un groupe existant.
4. Cliquez sur Next. La page Sélectionner des groupes d'utilisateurs s'affiche.



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.

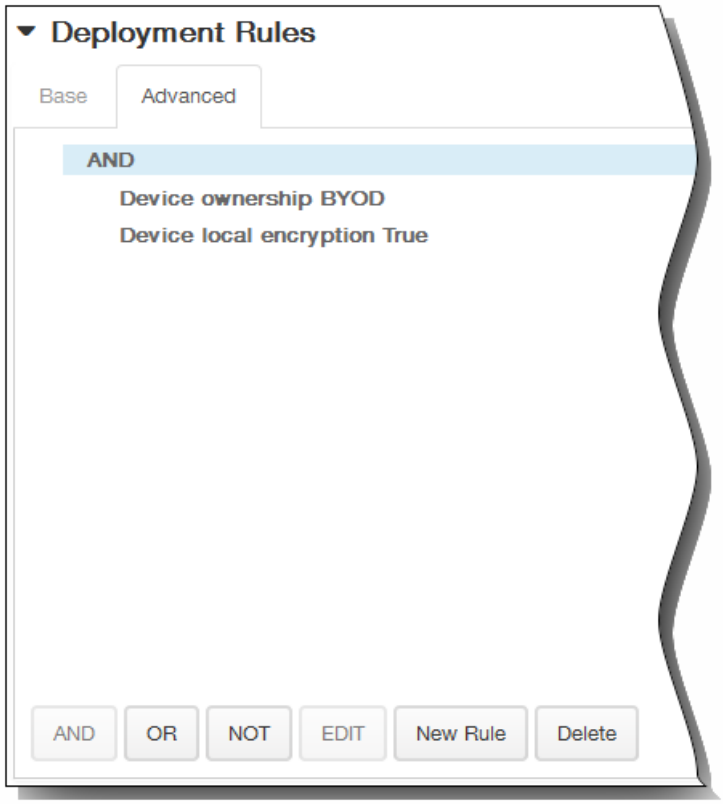


   Remarque : pour supprimer des groupes d'utilisateurs, cliquez sur Rechercher, puis dans la liste des groupes d'utilisateurs, décochez la case à cocher en regard du groupe ou des groupes que vous souhaitez supprimer. Vous pouvez taper un nom de groupe complet ou partiel dans la zone de recherche, puis 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.
   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.

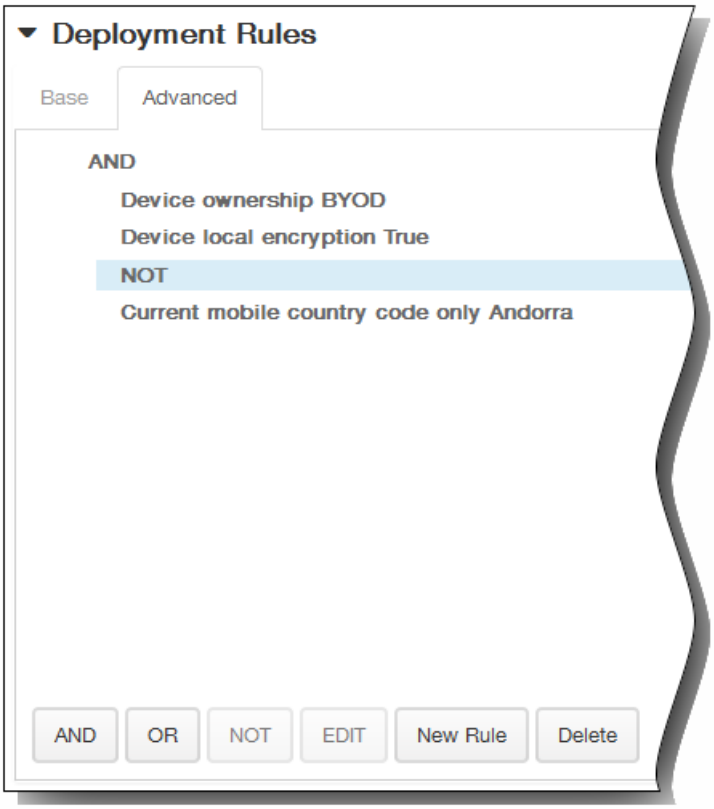
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



Les conditions que vous avez choisies sur l'onglet Base s'affichent.

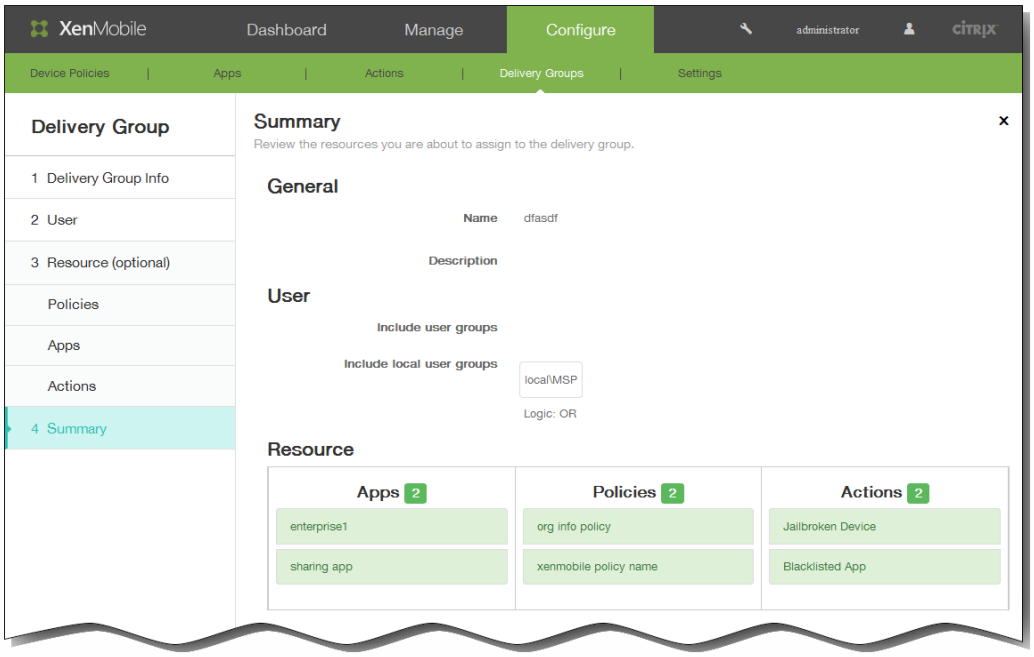
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter 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 Next. 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.

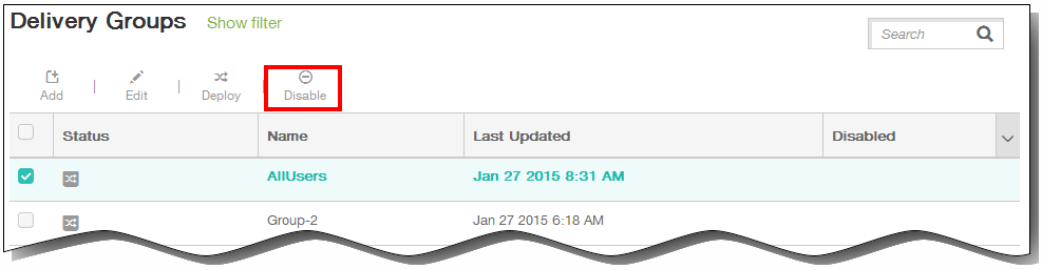


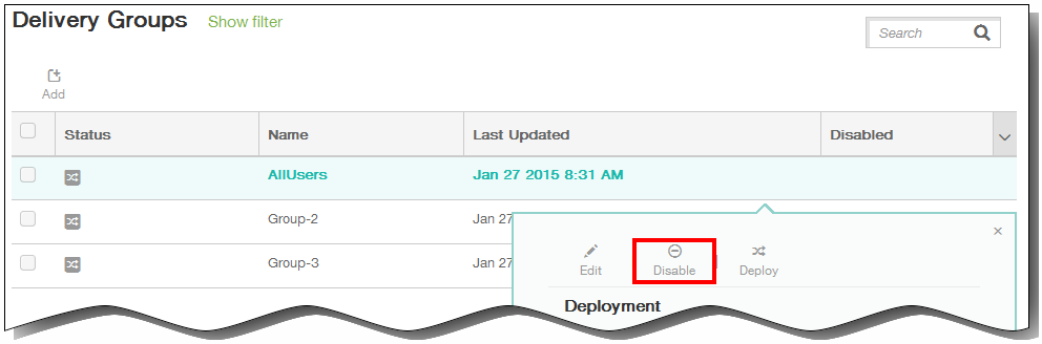
8. Sur la page Résumé, vérifiez les modifications que vous avez apportées. Cliquez sur Précédent pour revenir sur les pages précédentes pour modifier la configuration le cas échéant.
9. Cliquez sur Enregistrer pour enregistrer vos modifications.

Pour activer et désactiver le groupe de mise à disposition AllUsers

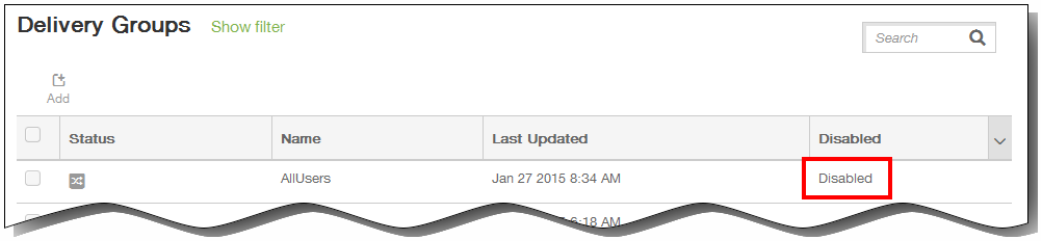
Remarque : AllUsers est le seul groupe de mise à disposition que vous pouvez activer ou désactiver.

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.





- 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.



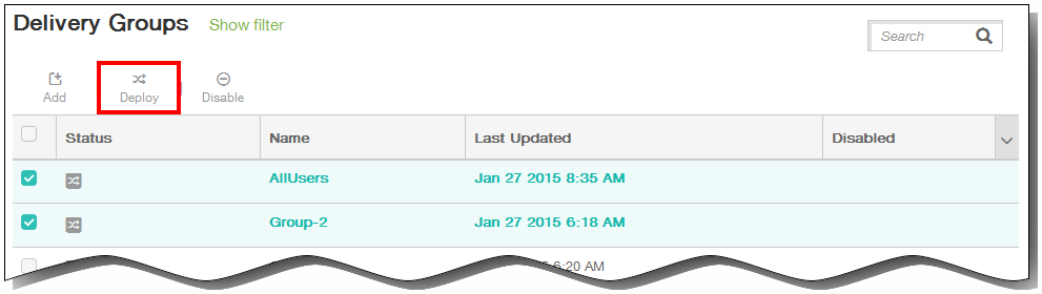
- Cliquez sur Activer pour activer le groupe de mise à disposition AllUsers. Cette commande est uniquement disponible si AllUsers est désactivé.
  Désactivé disparaît du titre Désactivé dans le tableau des groupes de mise à disposition.

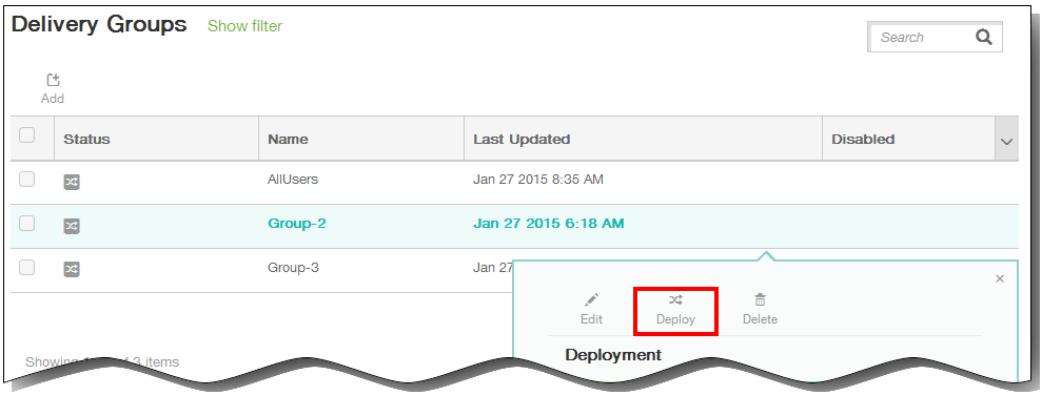
Pour déployer des groupes de mise à disposition

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.

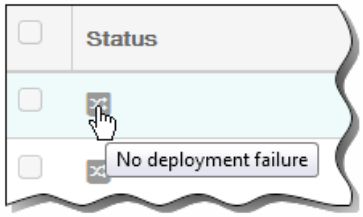
1. Sur la page Groupes de mise à disposition, effectuez l'une des opérations suivantes :
   - Pour déployer sur plus d'un groupe de mise à disposition à la fois, sélectionnez les cases à cocher en regard des groupes sur lesquels vous voulez déployer.
   - Pour déployer sur un seul groupe de mise à disposition, 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.



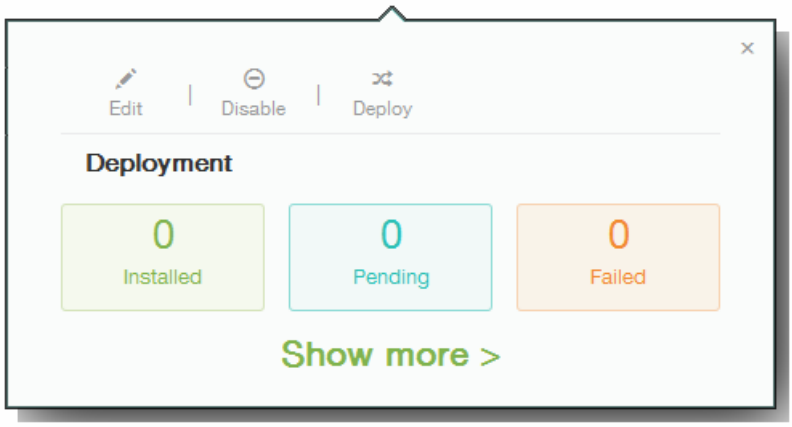


La boîte de dialogue Déployer des appareils apparaît.

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.



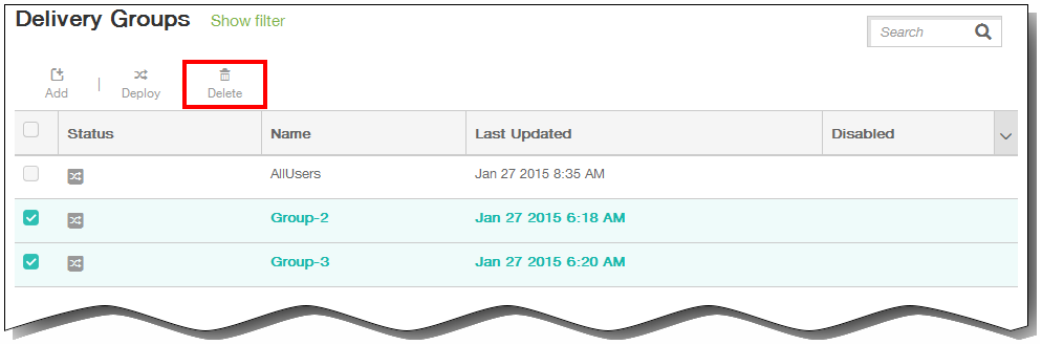
   - Cliquez sur la ligne contenant le groupe de mise à disposition pour afficher une superposition indiquant si les déploiements sont installés, en attente ou qu'ils ont échoué.

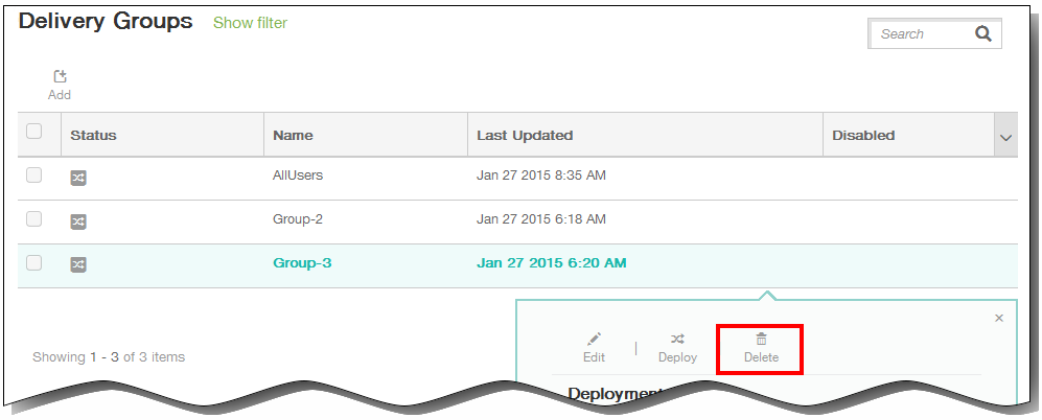


Pour supprimer des groupes de mise à disposition

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.





   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.

Inscription d'utilisateurs et d'appareils

May 06, 2016

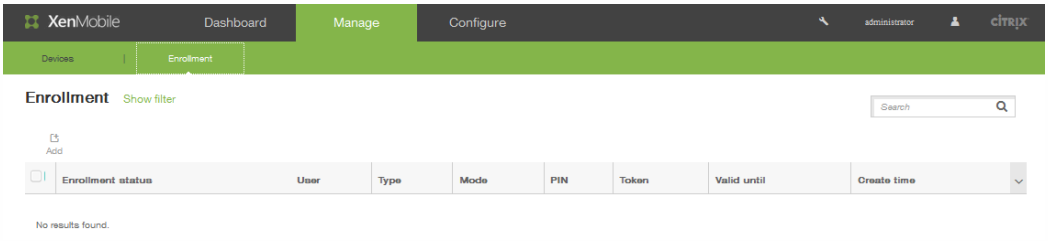
Pour gérer les appareils utilisateur à distance et de manière sécurisée, ces derniers doivent être inscrits dans XenMobile. Le logiciel client XenMobile est installé sur l'appareil utilisateur et l'identité de l'utilisateur est authentifiée, suivi de XenMobile et du profil de l'utilisateur. Une fois 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** :



Appareils Android

May 06, 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. 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.

Vous avez maintenant inscrit votre appareil Android. Touchez le Worx Store pour accéder à votre magasin d'applications d'entreprise, ainsi qu'aux applications Worx, telles que WorxMail, WorxWeb, ShareFile, et bien plus encore.

Pour désinscrire et réinscrire un appareil Android

Mis à jour : 12-02-2015

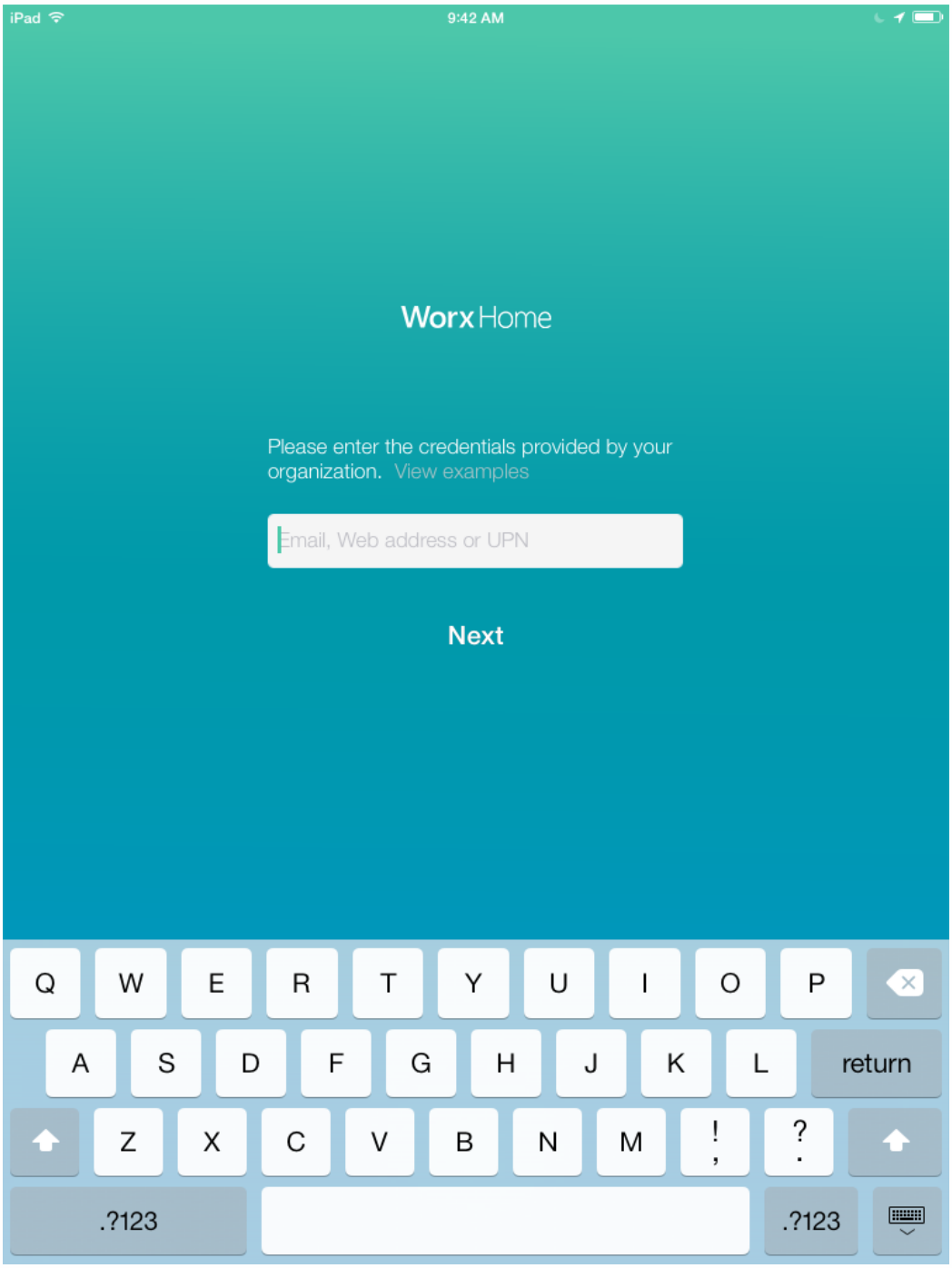
Avant de réinscrire un appareil, il doit d'abord être désinscrit. Durant la période pendant laquelle l'appareil est désinscrit mais pas encore réinscrit, ce dernier n'est pas géré par XenMobile, bien qu'il apparaisse toujours dans l'inventaire des appareils dans la console XenMobile. Vous ne pouvez pas 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.

Appareils iOS

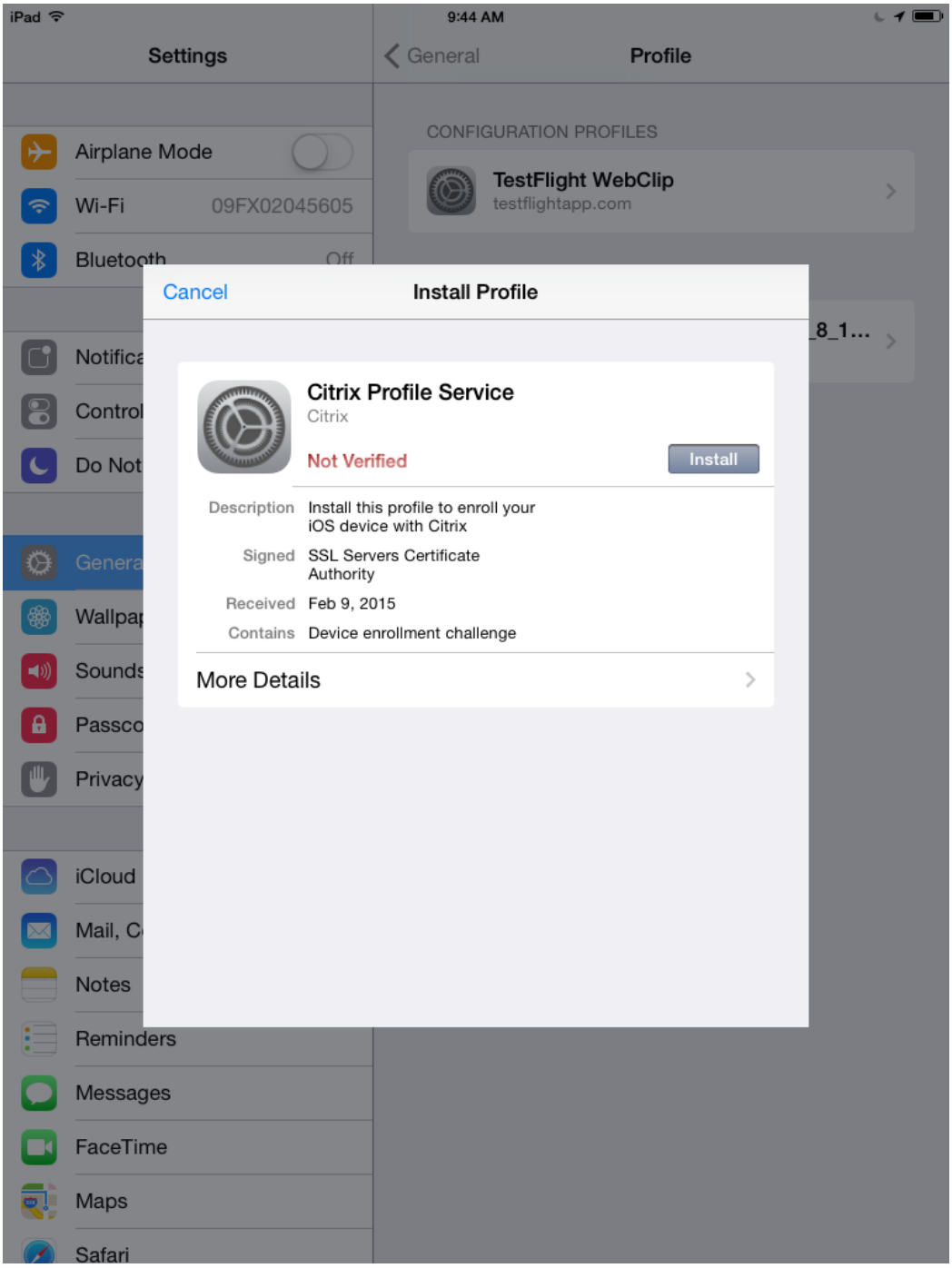
May 06, 2016

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.

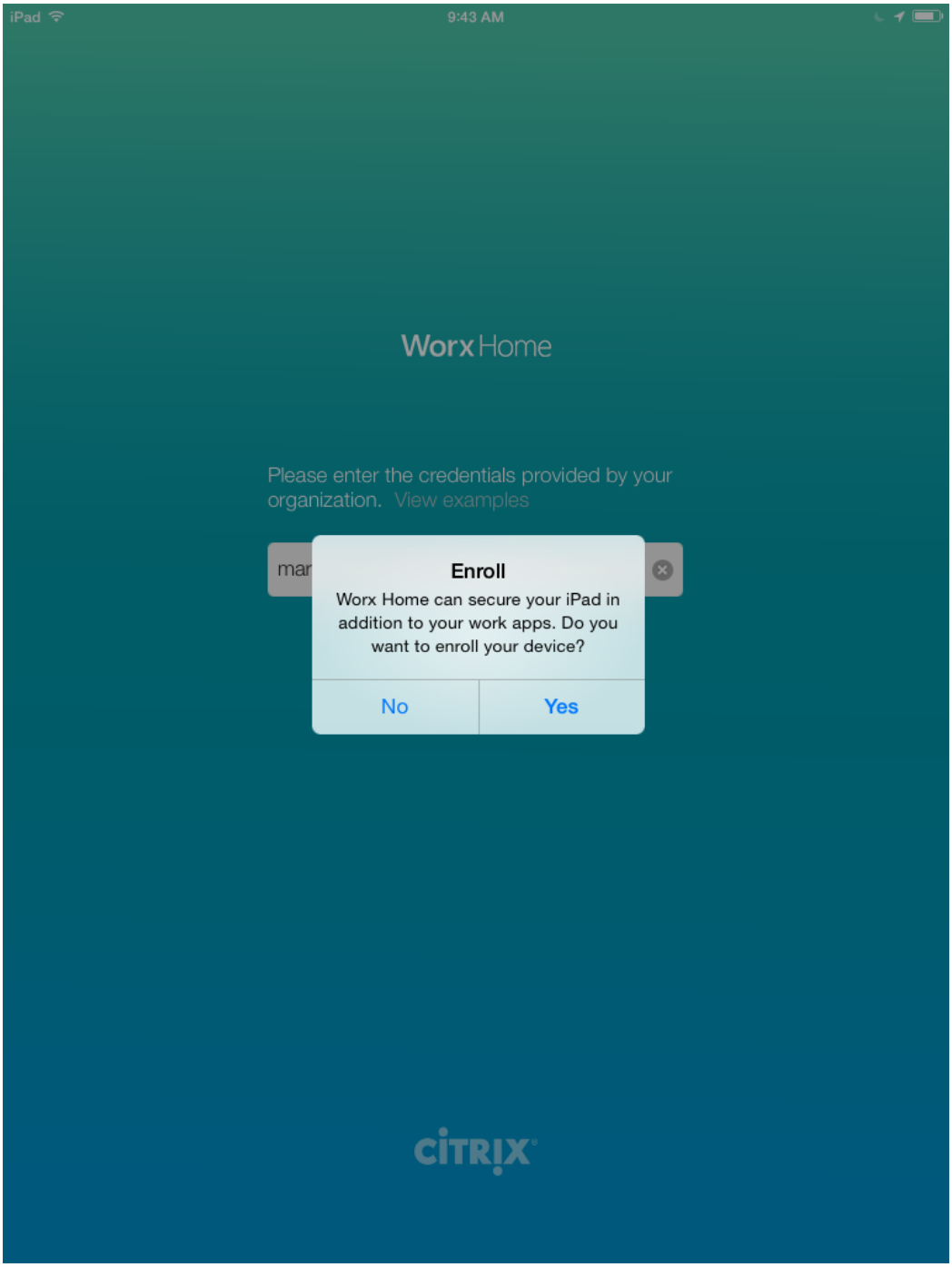


4. Entrez votre nom d'utilisateur et votre mot de passe. Un navigateur s'ouvre pour commencer le processus d'inscription.

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.



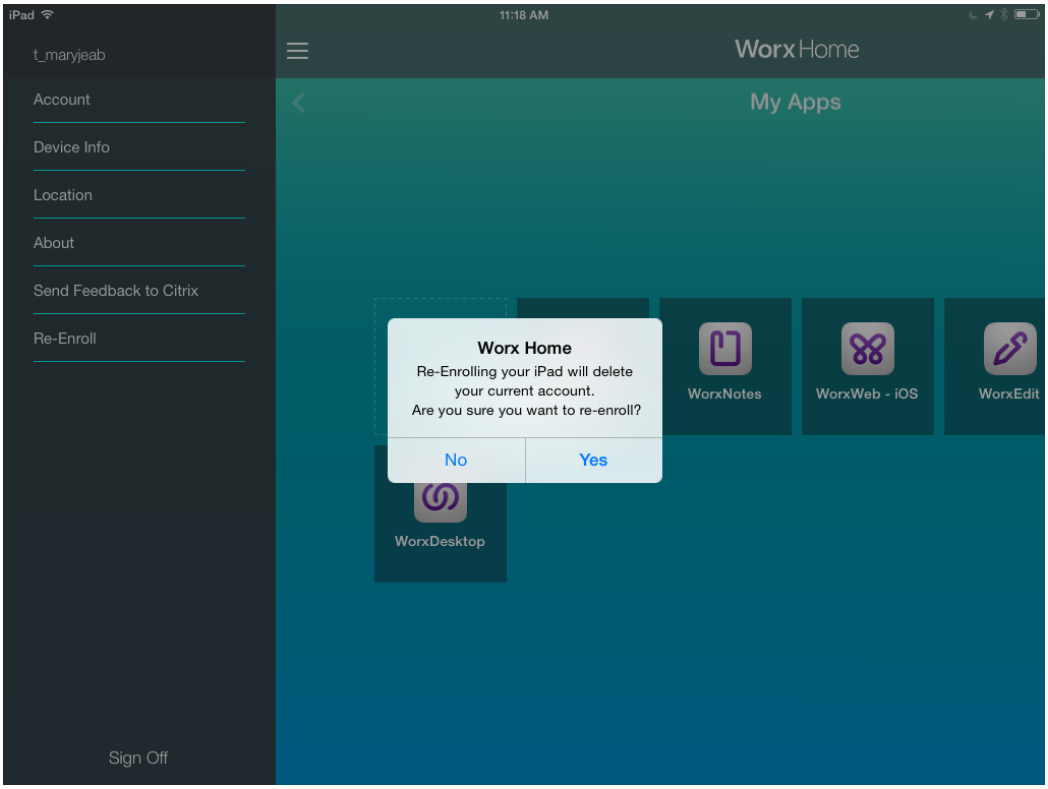
11. En fonction de la manière dont XenMobile est configuré, vous pouvez être invité à créer un code PIN Worx, que vous pouvez utiliser pour vous connecter à Worx Home et à d'autres applications Worx, telles que WorxMail, WorxWeb, ShareFile, et bien plus encore. Vous devez entrer votre code PIN Worx deux 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

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.

Inscription d'appareils Windows dans XenMobile

May 06, 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.

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

Mis à jour : 11-02-2015

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 indicateur n'apparaît lorsque l'installation est terminée. Ouvrez Worx Home à partir de l'écran Toutes les applications.

Appareils Symbian

May 06, 2016

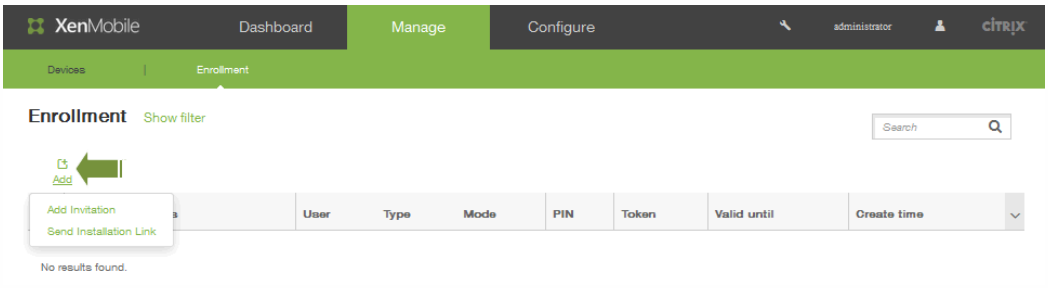
1. Accédez à l'adresse Web XenMobile pour votre organisation. L'adresse Web est au format suivant : https://.domaine.com//setup
   Remarque : vous pouvez utiliser le préfixe HTTPS uniquement si vous disposez d'un certificat émis par une autorité de confiance, telle que Verisign ou Thawte.
2. Sur l'écran 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.

Envoi d'une invitation d'inscription dans XenMobile

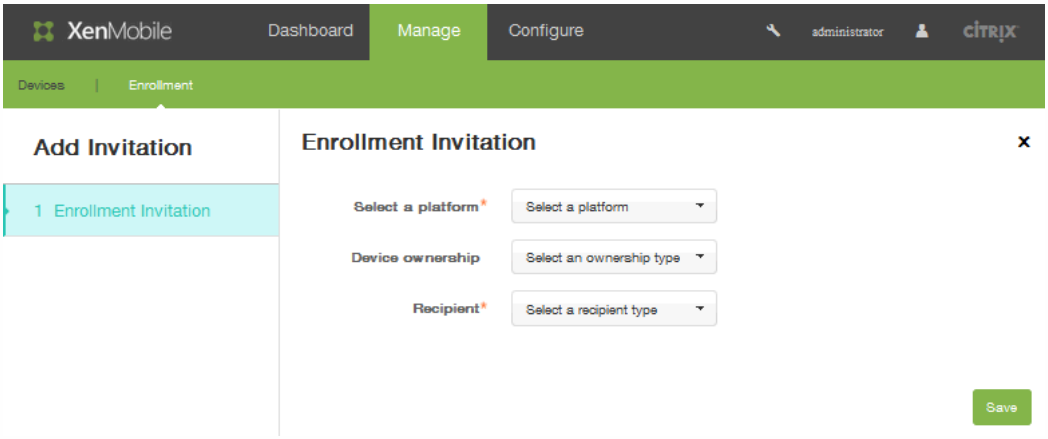
May 06, 2016

Dans la console XenMobile, vous pouvez envoyer une invitation d'inscription aux utilisateurs d'appareils iOS et Android.

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.



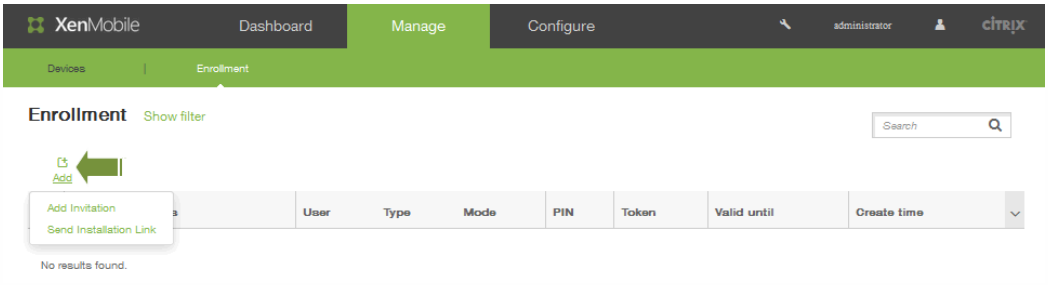
3. Cliquez sur Ajouter une invitation. L'écran Invitation d'inscription s'affiche.



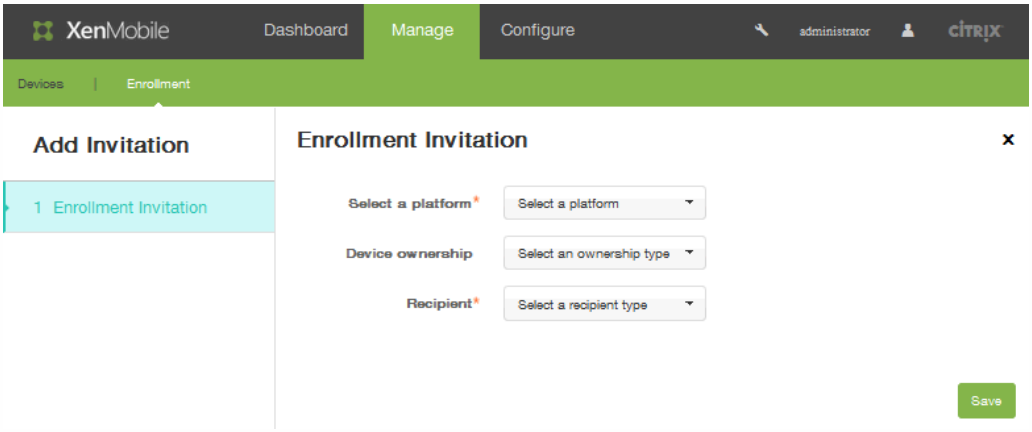
4. Dans la liste Sélectionner une plate-forme, cliquez sur iOS ou Android.
5. Dans la liste Propriétaire, cliquez sur Entreprise ou Employé.
6. Dans la liste Destinataire, cliquez sur Utilisateur ou Groupe. Lorsque vous sélectionnez un utilisateur en tant que destinataire, l'interface change pour afficher d'autres options de configuration. 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

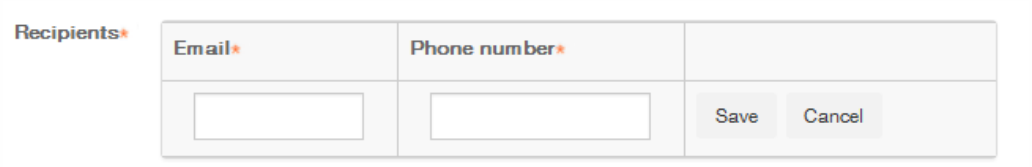
1. Dans la console XenMobile, cliquez sur Gérer > Inscription.
2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.



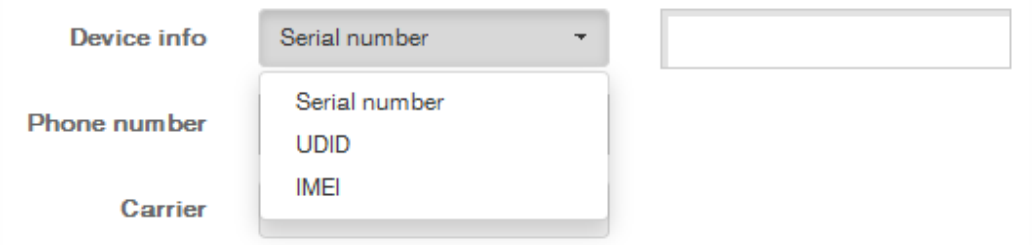
3. Cliquez sur Ajouter une invitation. L'écran Invitation d'inscription s'affiche.



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. L'interface change pour afficher les options de configuration liées à l'inscription d'utilisateurs.



7. Dans Nom d'utilisateur, entrez un nom d'utilisateur. L'utilisateur doit exister dans le serveur XenMobile en tant qu'utilisateur local ou en tant qu'utilisateur dans Active Directory. Si l'utilisateur est local, assurez-vous que la propriété Email de l'utilisateur est configurée pour 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, l'interface change pour afficher un champ dans lequel vous pouvez entrer la valeur correspondante à l'appareil :

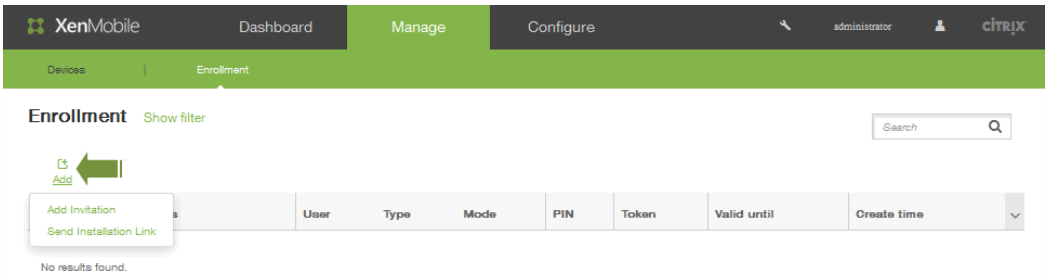


9. Dans Numéro de téléphone, entrez le numéro de téléphone de l'utilisateur (facultatif).

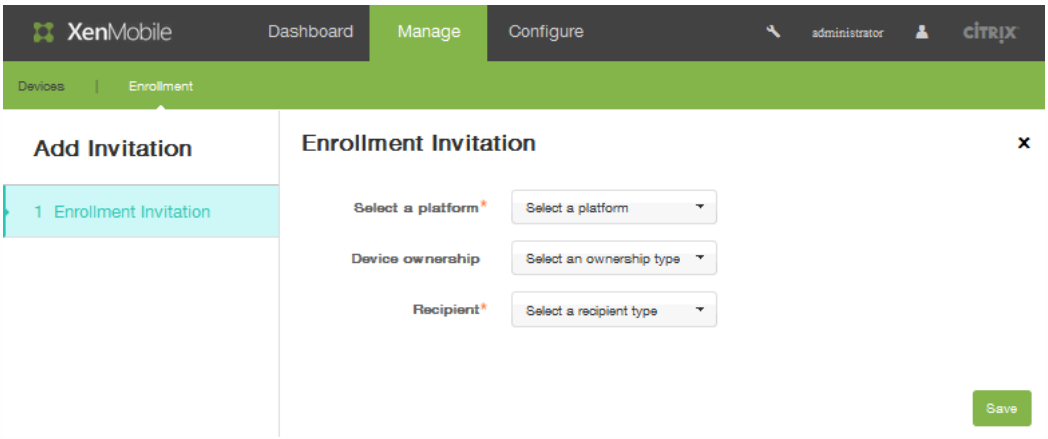
10. Dans la liste Opérateur, sélectionnez un opérateur auquel associer le numéro de téléphone de l'utilisateur.
11. Dans la liste Mode d'inscription, sélectionnez Nom d'utilisateur + mot de passe (valeur par défaut), Haute sécurité, URL d'invitation, URL d'invitation + PIN, URL d'invitation + mot de 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.
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, cliquez sur ON.
16. Cliquez sur Enregistrer.

Pour envoyer une invitation d'inscription à un groupe

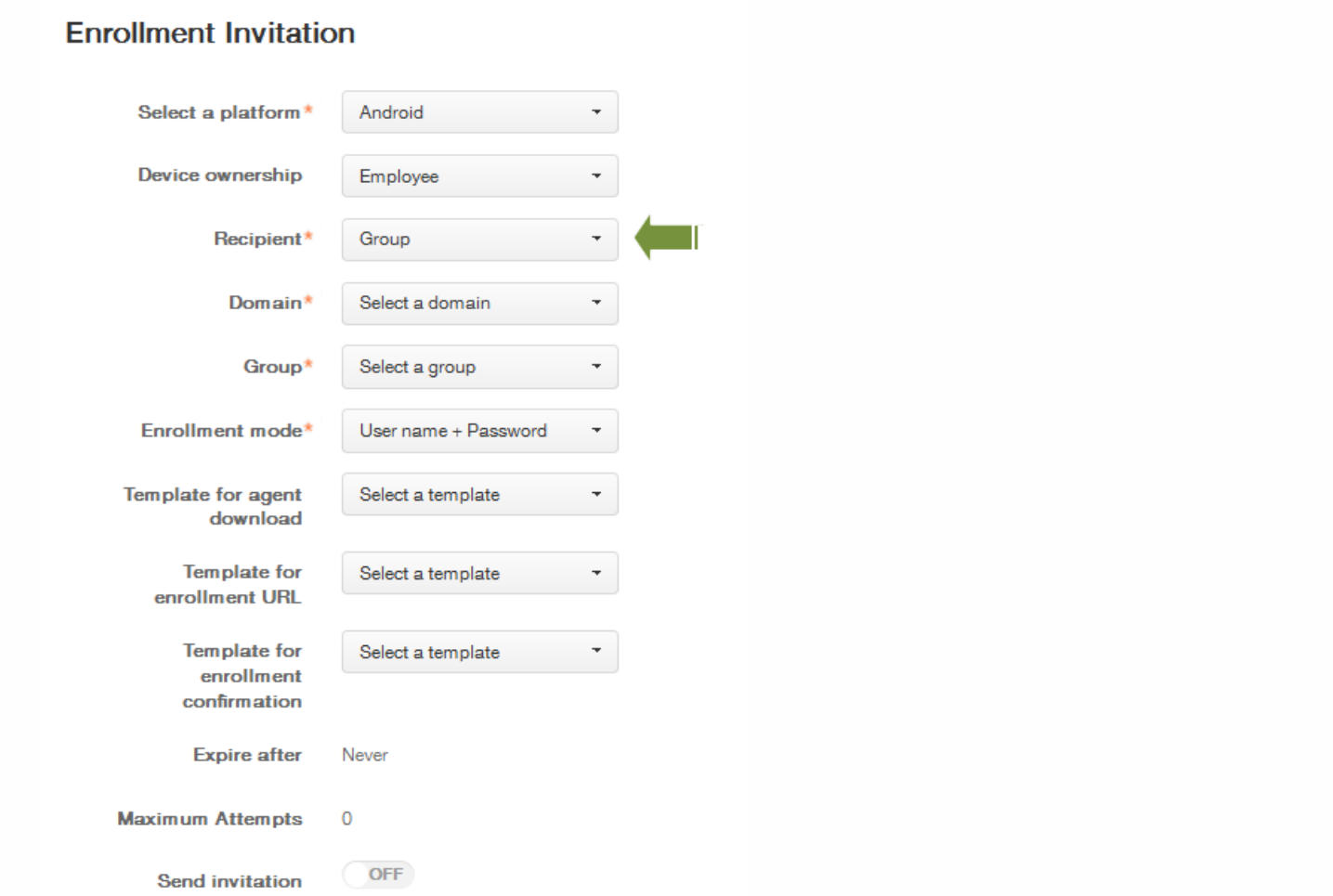
1. Dans la console XenMobile, cliquez sur Gérer > Inscription.
2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.



3. Cliquez sur Ajouter une invitation. 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. L'interface change pour afficher les options de configuration pour l'inscription de groupe :

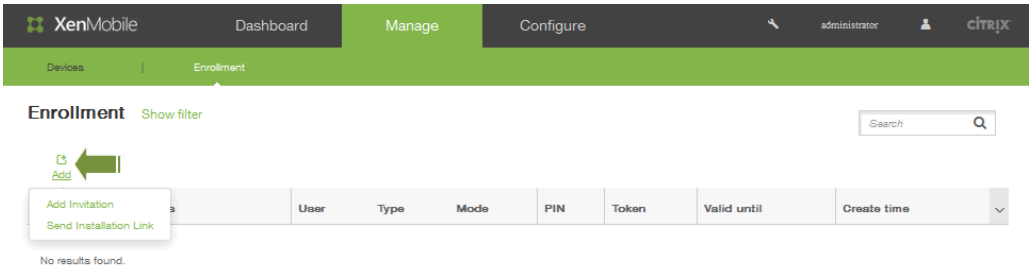


7. Pour Domaine, sélectionnez le domaine dans lequel le groupe de destinataires réside.
8. Pour Groupe, sélectionnez le groupe auquel vous souhaitez envoyer une notification d'inscription.
9. Dans Mode d'inscription, sélectionnez Nom d'utilisateur + mot de passe valeur par défaut), Haute sécurité, URL d'invitation + PIN, URL d'invitation + mot de passe, Deux facteurs ou Nom d'utilisateur + PIN.
10. 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.
11. Dans Modèle pour l'URL d'inscription, sélectionnez Invitation d'inscription.
12. 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.
13. Dans Envoyer invitation, cliquez sur ON pour envoyer l'invitation d'inscription au groupe sélectionné.
14. Cliquez sur Enregistrer.

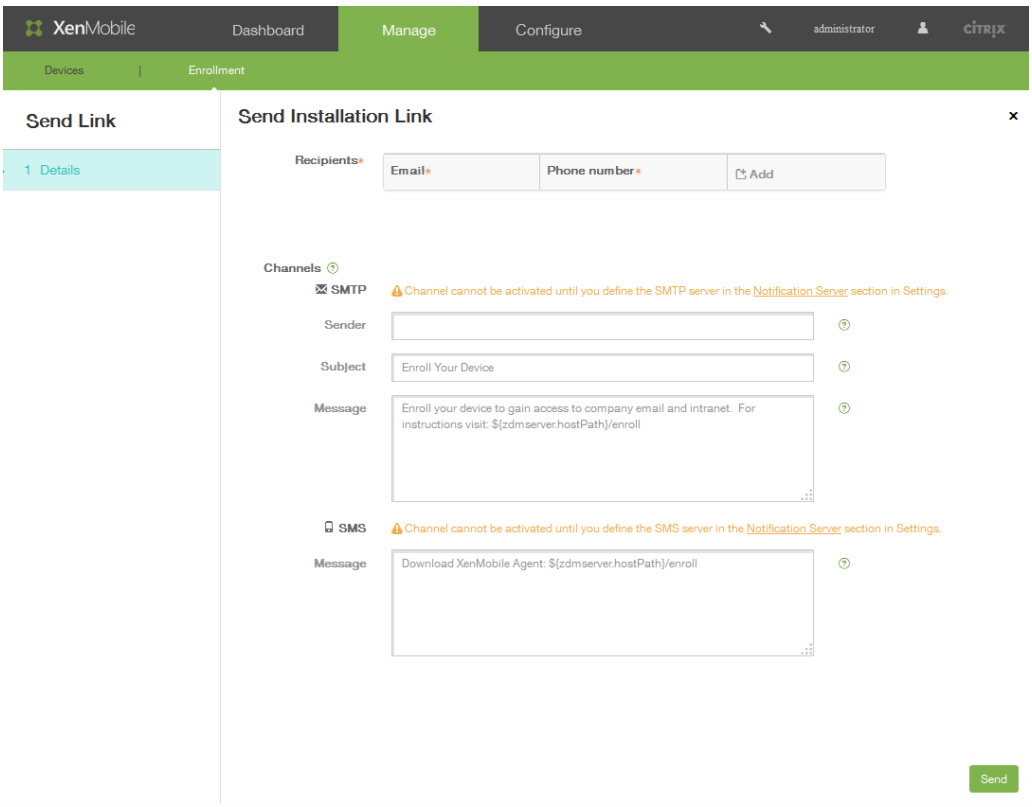
Pour envoyer un lien d'installation d'inscription

Avant de pouvoir envoyer un lien d'installation de l'inscription, vous devez configurer les canaux (SMTP ou SMS) sur le serveur de notification : Configurer > Paramètres > Serveur de notification. Pour de plus amples informations, consultez la section Notifications dans XenMobile.

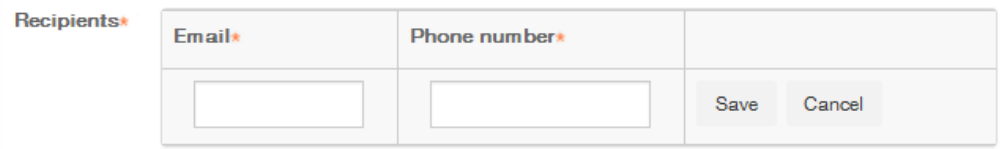
1. Dans la console XenMobile, cliquez sur Gérer > Inscription.
2. Sur l'écran Inscription, cliquez sur Ajouter. Un menu dans lequel vous pouvez choisir d'ajouter une invitation ou d'envoyer un lien d'installation s'affiche.



3. Cliquez sur Envoyer lien d'installation. L'interface change pour afficher les options Envoyer lien d'installation.



4. Dans Destinataire, cliquez sur Ajouter pour identifier un destinataire auquel vous souhaitez envoyer un lien d'installation de l'inscription. Le champ Destinataire se développe pour vous permettre d'ajouter une adresse e-mail et un numéro de téléphone.



5. Entrez une adresse e-mail et un numéro de téléphone pour l'utilisateur qui reçoit le lien d'invitation à s'inscrire. Ces champs sont obligatoires.
6. 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.

7. 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.
8. Pour les notifications SMTP, vous pouvez également inclure le sujet si vous le souhaitez. Par exemple, « inscription de votre appareil ».
9. Entrez un message à utiliser pour le contenu du message envoyé au destinataire. Par exemple, « Inscrivez votre appareil pour accéder à la messagerie et à l'intranet de l'entreprise ».
10. 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.
11. 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.

Configuration des règles de déploiement

Oct 11, 2016

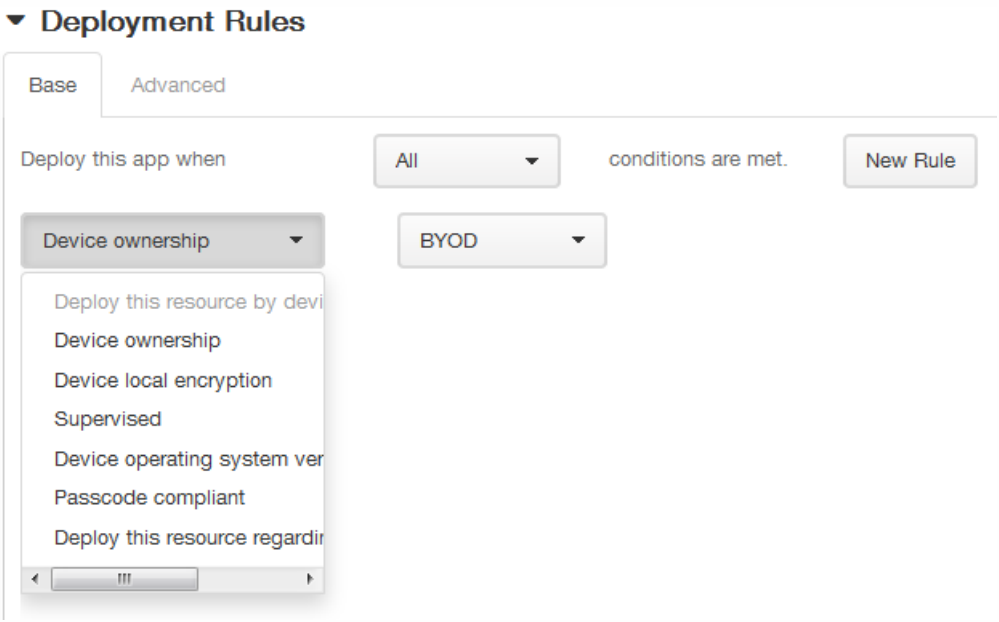
Cette section décrit :

- 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

Vous pouvez définir un nombre de paramètres qui affecte le résultat du déploiement d'un paquetage.

Par exemple, le paquetage de votre déploiement peut être basé sur une version spécifique d'un système d'exploitation, sur une plate-forme matérielle particulière, ou toute autre combinaison. Dans cet assistant, vous trouverez un éditeur de règles de base et avancées. Le mode Avancé est un éditeur à format libre. L'image ci-dessous illustre l'écran des règles de déploiement accessibles 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.

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 **ET**, **OU** et **SAUF** appropriés 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.

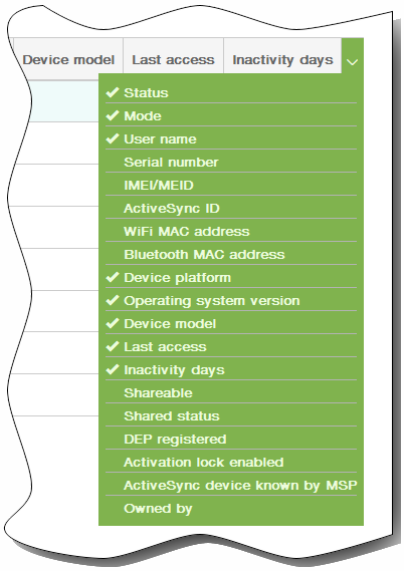
Ajout d'appareils et affichage des détails des appareils

May 06, 2016

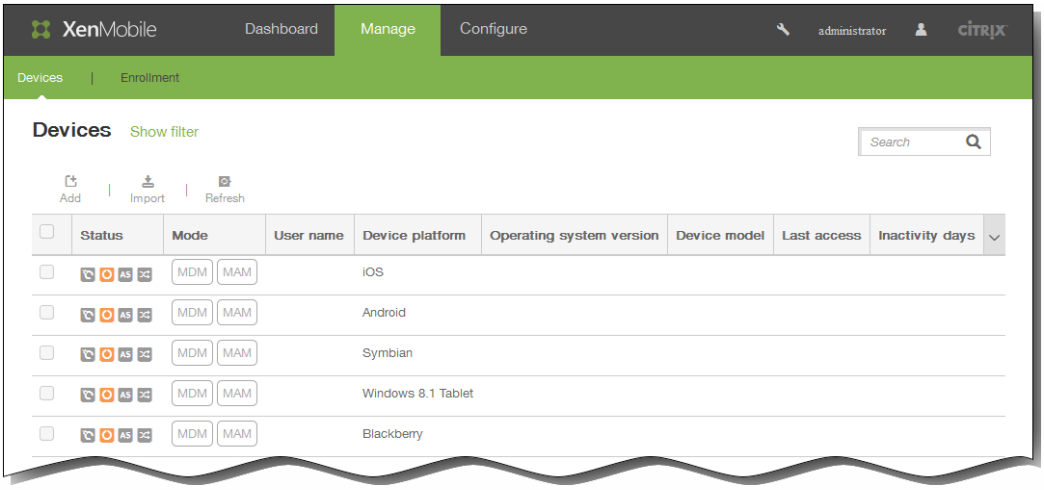
La base de données de référentiel du serveur de la console XenMobile stocke une liste des appareils mobiles. Chaque appareil mobile est défini par un numéro de série unique et/ou un numéro IMEI (identité internationale d'équipement mobile)/MEID (identifiant de l'équipement mobile). Pour renseigner la console XenMobile avec vos appareils, vous pouvez ajouter les appareils manuellement ou importer une liste d'appareils à partir d'un fichier. Consultez la section 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 jailbreaké, 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.

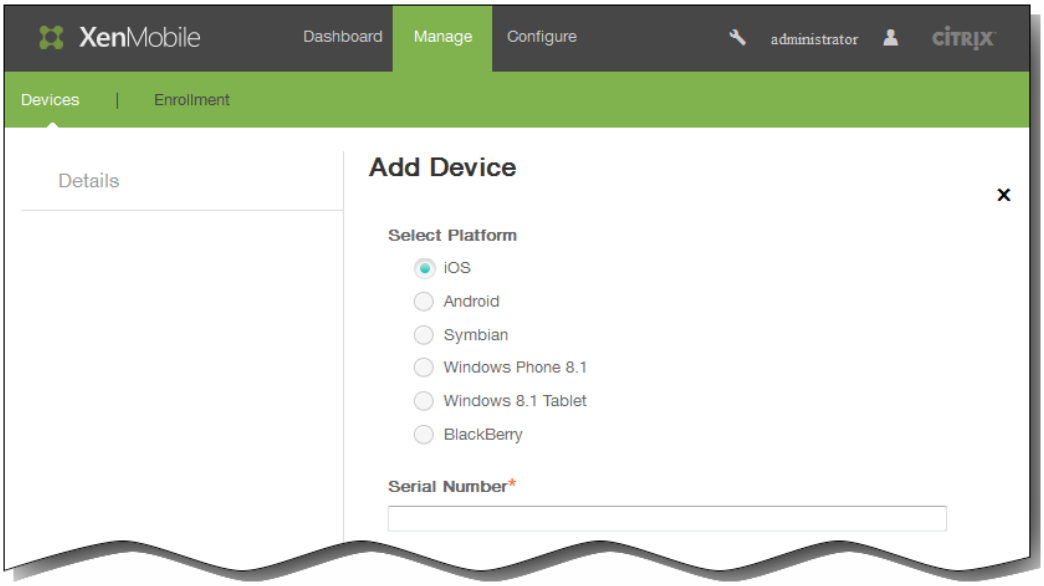
Remarque : les en-têtes précédents sont les valeurs par défaut. Vous pouvez personnaliser les éléments affichés dans le tableau en cliquant sur la flèche vers le bas sur le dernier en-tête, puis en cliquant sur les en-têtes que vous voulez voir ou en supprimant ceux que vous ne souhaitez pas voir.



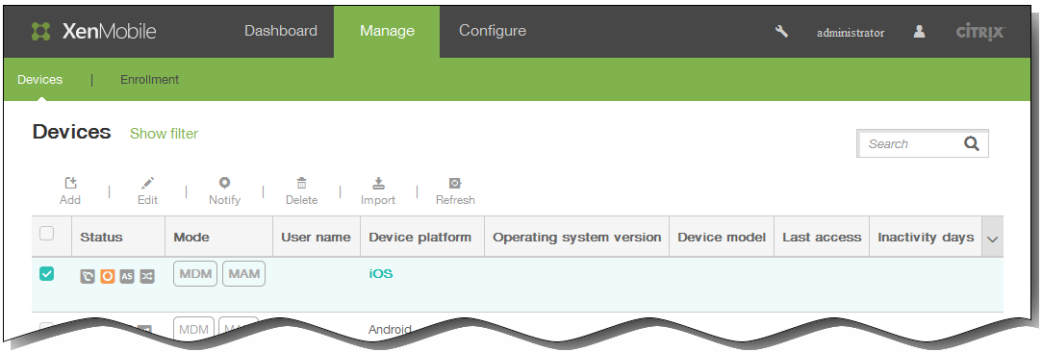
Vous pouvez ajouter un nouvel appareil manuellement en cliquant sur Ajouter, ou vous pouvez importer un fichier de provisioning en cliquant sur Importer. Pour mettre à jour le tableau, cliquez sur Actualiser.



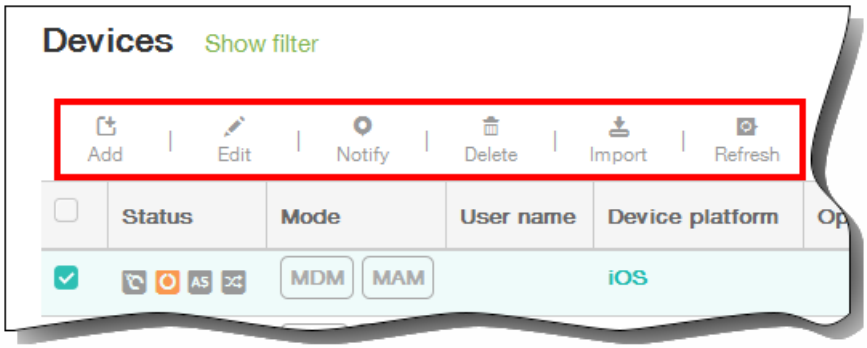
1. Dans la console XenMobile, cliquez sur GérerAppareils et cliquez sur Ajouter. La page Ajouter un appareil s'affiche.

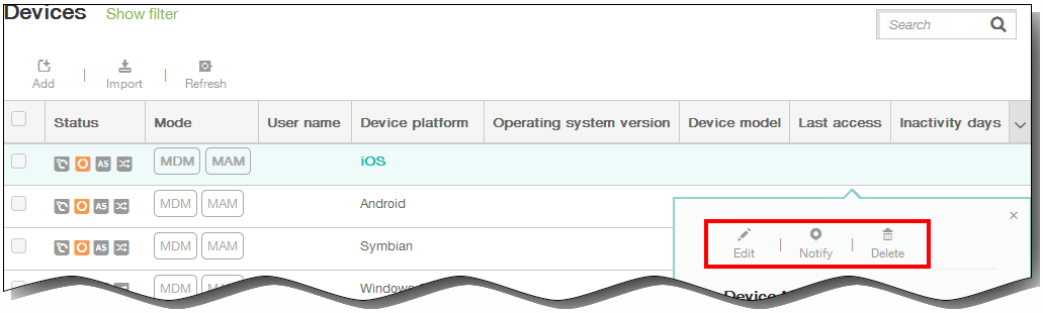


2. Dans Sélectionner une plate-forme, cliquez sur iOS, Android, Symbian, Windows Phone 8.1, Windows 8.1 Tablet ou BlackBerry.
3. Entrez les informations suivantes :
   1. iOS : entrez le numéro de série.
   2. Android : entrez le numéro de série et le numéro IMEI/MEID.
   3. Symbian : entrez le numéro IMEI/MEID.
   4. Windows Phone 8.1 : entrez le numéro de série et le numéro IMEI/MEID.
   5. Windows 8.1 Tablet : entrez le numéro de série et le numéro IMEI/MEID.
   6. BlackBerry : entrez le numéro de série et 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.

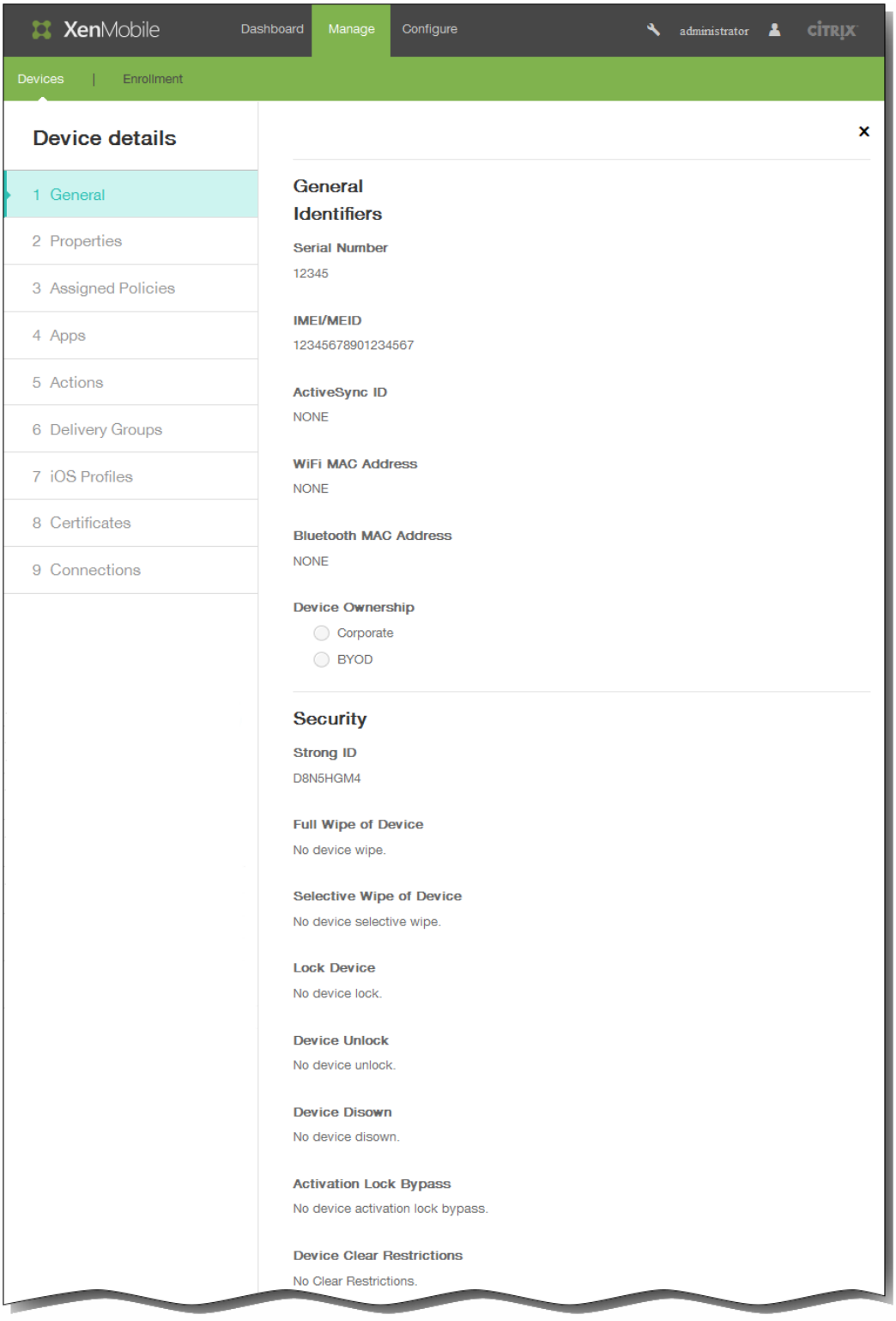


Remarque : lorsque vous sélectionnez la case à cocher en regard d'un appareil, le menu d'options s'affiche au-dessus de la liste des appareils ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté droit de la liste.



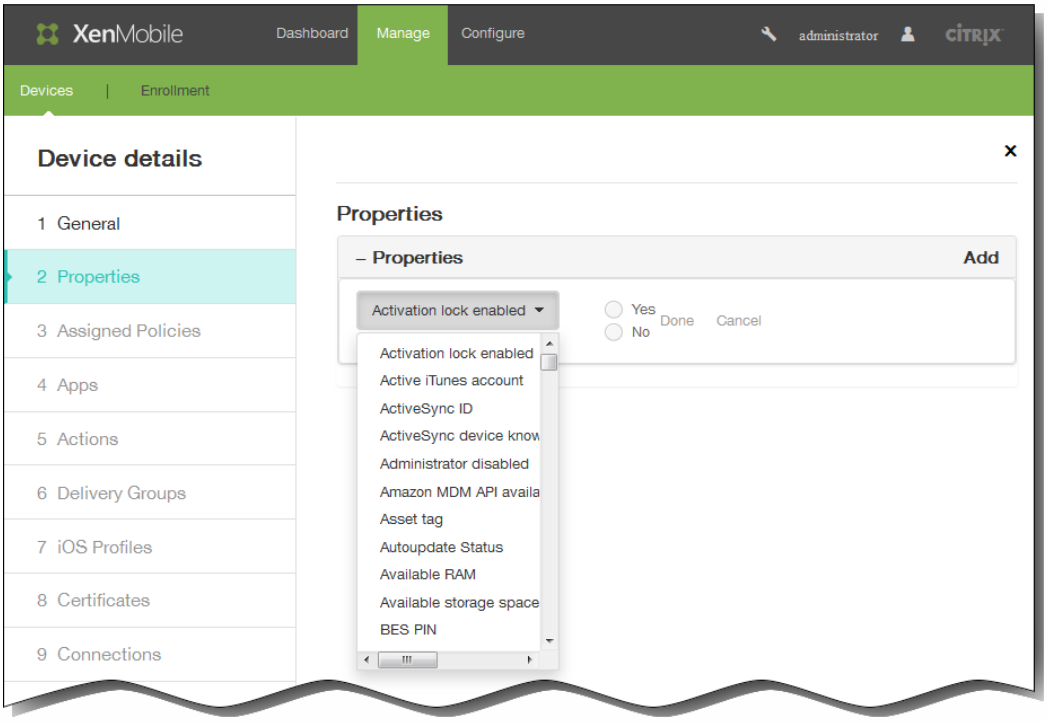


6. Sous Général : identificateurs, confirmez les informations affichées (la liste de paramètres varie en fonction du type de plate-forme) : numéro de série, IMEI/MEID, ID ActiveSync, adresse MAC Wi-Fi, adresse MAC Bluetooth, Propriétaire : entreprise ou BYOD.

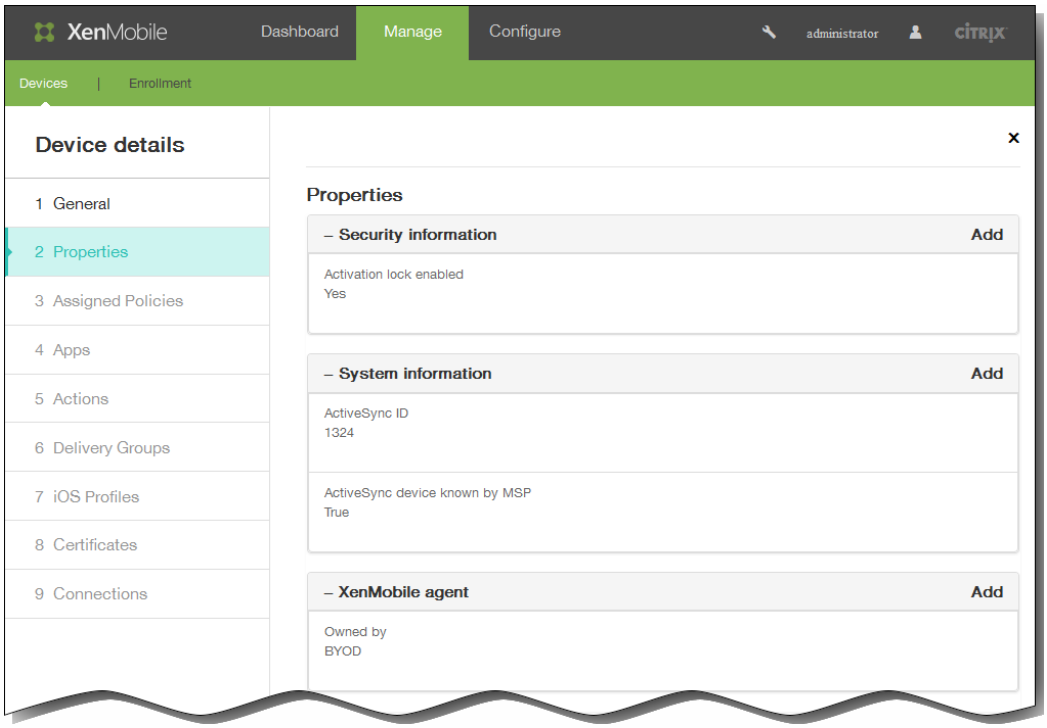


7. Sous Sécurité, confirmez les informations qui s'affichent (la liste de paramètres varie en fonction du type de plate-forme) : identifiant fort, effacement complet de l'appareil, effacer les données d'entreprise d'un appareil, verrouiller l'appareil, déverrouiller l'appareil, exclusion de l'appareil, 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.



10. Dans la liste, cliquez sur la propriété à provisionner et définissez sa valeur. Par exemple, dans l'image précédente, la propriété Verrouillage d'activation activé est sélectionnée avec une valeur que vous pouvez définir 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.



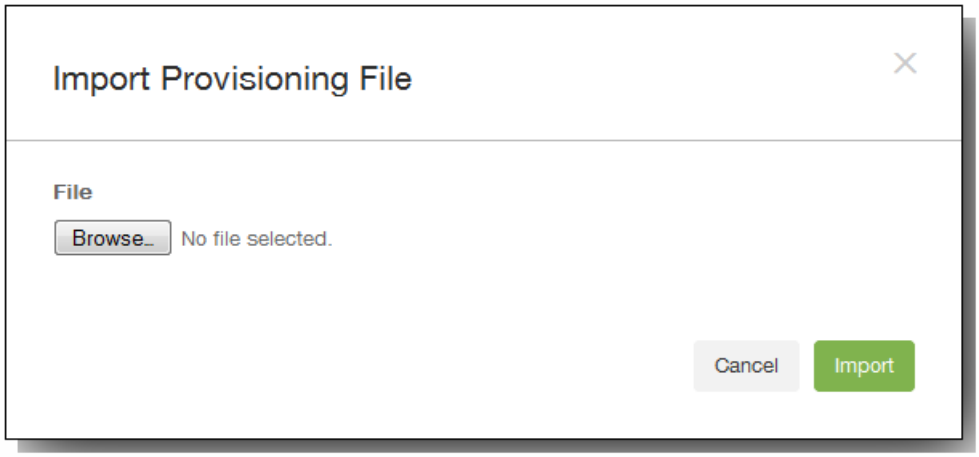
La section **Stratégies attribuées** et les sections suivantes contiennent toutes des informations récapitulatives sur l'appareil.

- 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.

13. Cliquez sur Enregistrer.

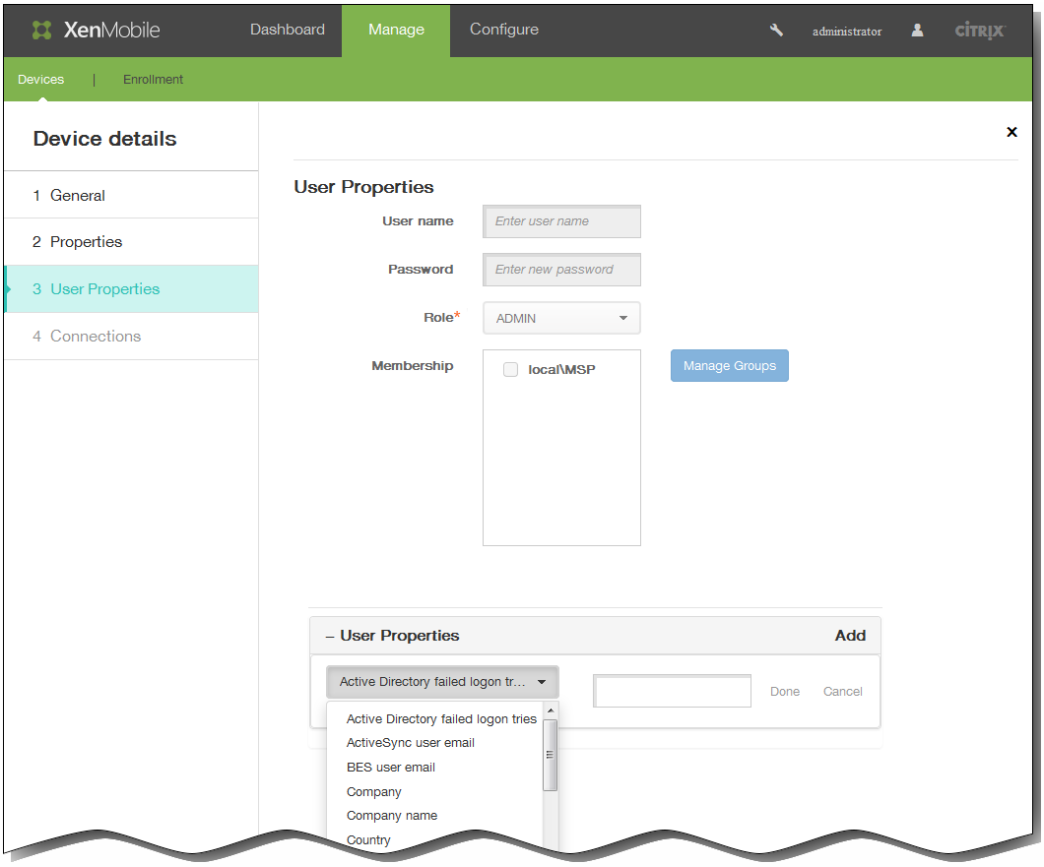
Vous pouvez importer un fichier fourni par les opérateurs mobiles ou les fabricants de l'appareil, ou vous pouvez créer votre propre fichier de provisioning. Consultez la section Formats des fichiers de provisioning.

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.

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 la section Pour ajouter des appareils manuellement.



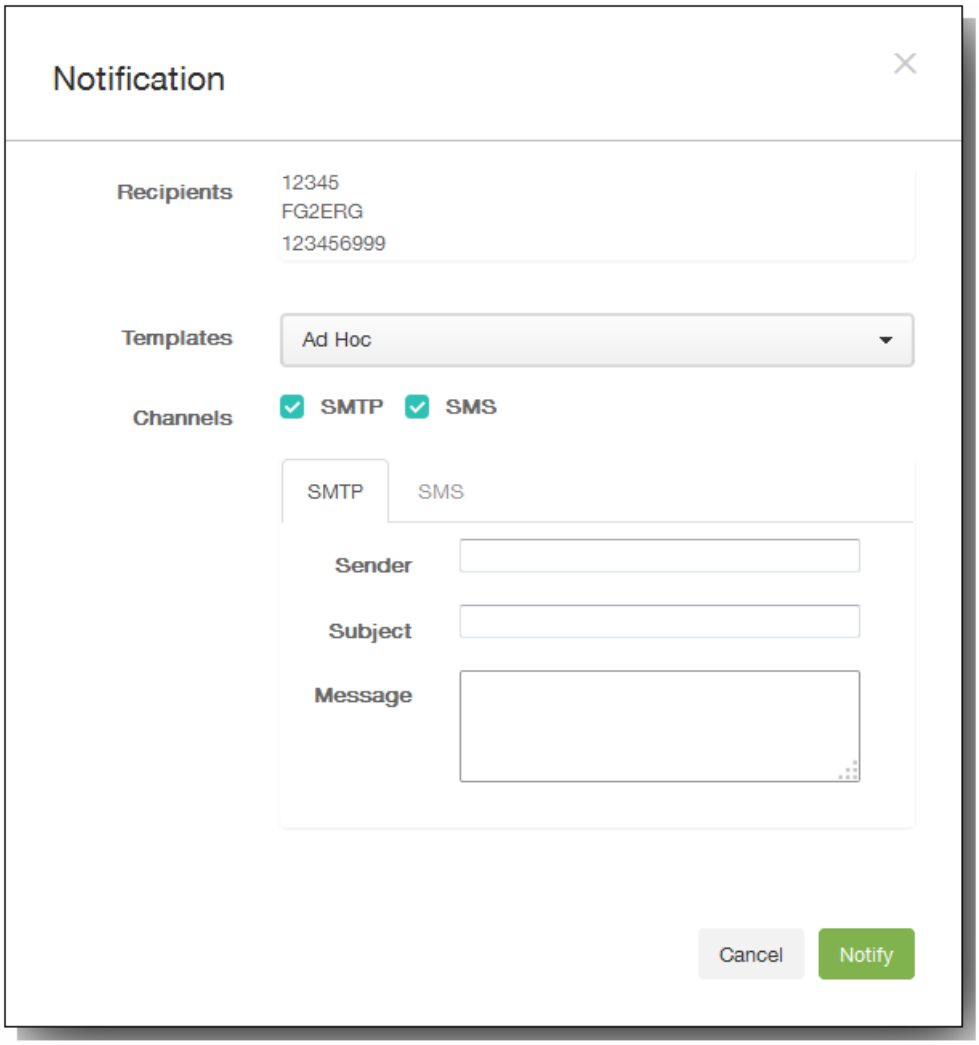
Remarque : la partie supérieure de la page Propriétés utilisateur ne peut pas être modifiée.

- 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.

Vous pouvez envoyer des notifications aux appareils à partir de la page Appareils. Pour plus d'informations sur les notifications, veuillez consulter 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.



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.

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.

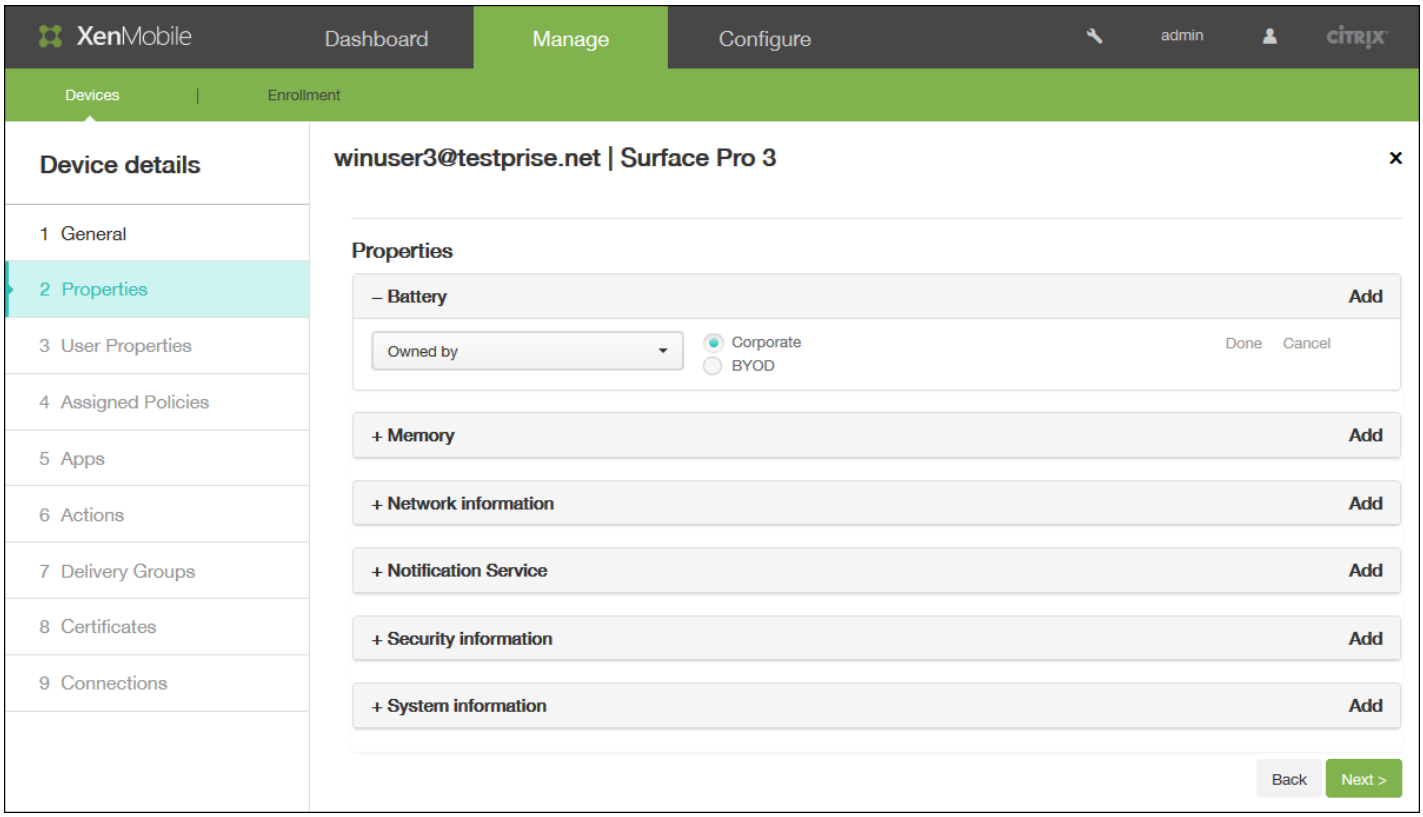
Identification manuelle des appareils utilisateur

May 06, 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 illustré 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 **Appartient à** et en choisissant **Entreprise** ou **BYOD** (appartient à l'employé).



Formats des fichiers de provisioning

May 06, 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.

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 : 1050BF3F51730108161006551059039 1
- IMEI : 15244201625379901
- OperatingSystemFamily : WINDOWS
- PropertyName : propertyN
- PropertyValue : propertyV\;test\;1\;2;prop 2

Macros dans XenMobile

May 06, 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.

Les macros utilisateur suivantes sont toujours disponibles :

- loginname (nom d'utilisateur + domainname)
- username (nom d'ouverture de session moins le domaine, si présent)
- domainname (nom de domaine, ou domaine par défaut)

Il se peut que les propriétés suivantes définies par l'administrateur soient disponibles :

- c
- cn
- company
- companyname
- department
- description
- displayname
- distinguishedname
- facsimiletelephonenumber
- givenname
- homecity
- homecountry
- homefax
- homephone
- homestate
- homestreetaddress
- homezip
- ipphone
- l
- mail
- middleinitial
- mobile
- officestreetaddress
- pager
- physicaldeliveryofficename

- postalcode
- postofficebox
- telephonenumber
- samaccountname
- sn
- st
- streetaddress
- title
- userprincipalname
- domainname (remplace la propriété décrite ci-dessus)

En outre, si l'utilisateur est authentifié à l'aide d'un serveur d'authentification, tel que LDAP, toutes les propriétés associées à l'utilisateur dans le magasin sont disponibles.

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.

Stratégies applicatives

May 06, 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.

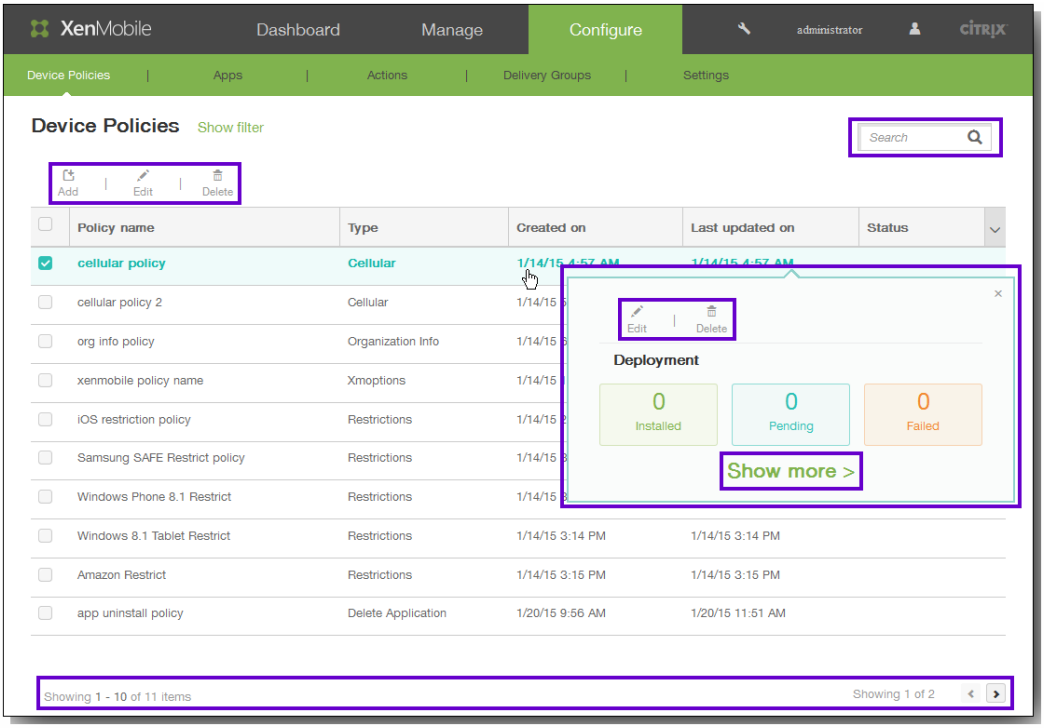
Les étapes de base pour créer une stratégie sont les suivantes :

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).

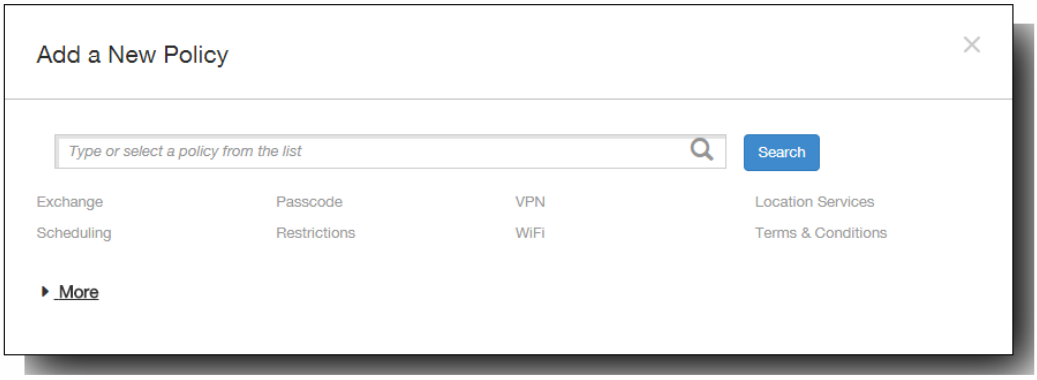
Les stratégies sont accessibles à partir de la page Stratégies d'appareil dans la console XenMobile. Pour accéder à la page Stratégies d'appareil, cliquez sur Configurer > Stratégies d'appareil. À partir de cette fenêtre, vous pouvez ajouter de nouvelles stratégies, consulter l'état de stratégies existantes, et modifier ou supprimer des stratégies.

La page Stratégies d'appareil contient une table répertoriant toutes les stratégies actuelles.

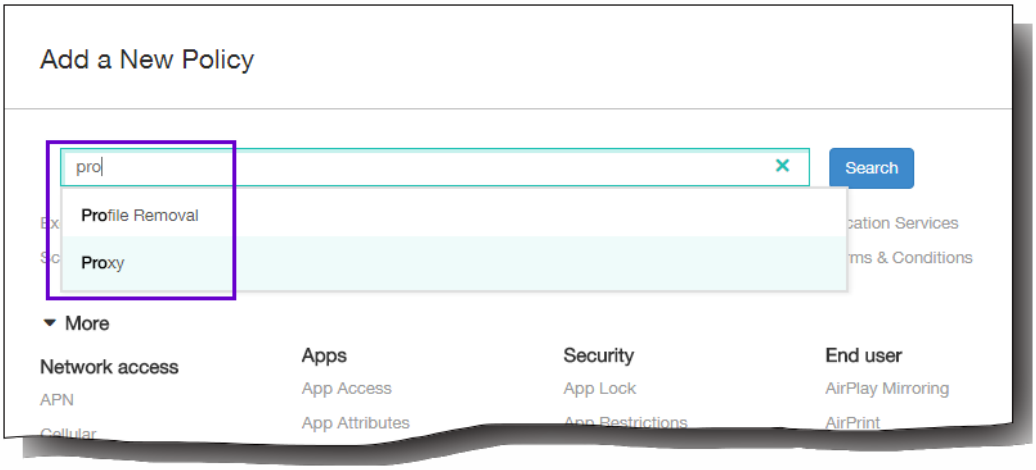
Pour modifier ou supprimer une stratégie sur la page Stratégies d'appareil, vous pouvez sélectionner la case à cocher en regard d'une stratégie pour afficher les options de menu au-dessus de la liste de stratégie, ou vous pouvez cliquer sur une stratégie dans la liste pour afficher le menu d'options sur le côté droit de la liste. Si vous cliquez sur Afficher plus, les détails de stratégie s'affichent.



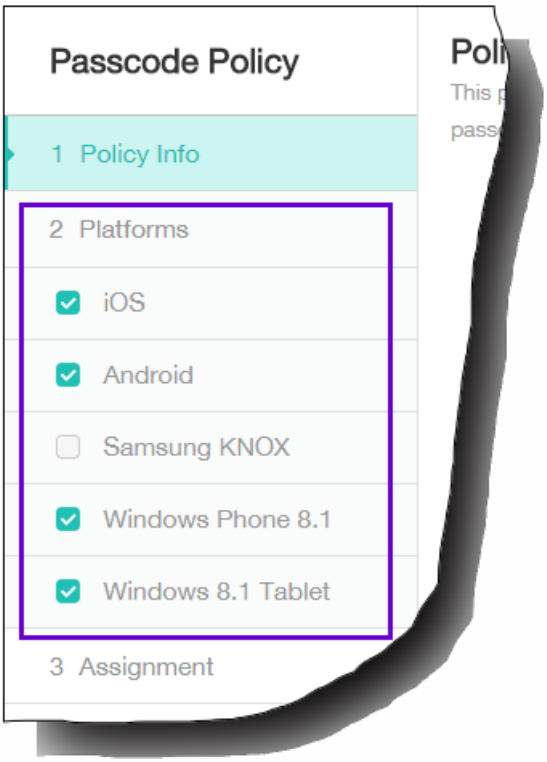
1. Sur la page Stratégies d'appareil, cliquez sur Ajouter.
   La boîte de dialogue Ajouter une nouvelle stratégie apparaît. Vous pouvez développer Plus pour afficher d'autres stratégies.



2. Pour trouver la stratégie que vous souhaitez ajouter, effectuez l'une des opérations suivantes :
   - Cliquez sur la stratégie.
     La page Informations sur la stratégie pour la stratégie sélectionnée s'affiche.
   - Entrez le nom de la stratégie dans le champ de recherche. À mesure que vous tapez, des correspondances potentielles s'affichent. Si votre stratégie figure dans la liste, cliquez dessus. Seule la stratégie sélectionnée reste dans la boîte de dialogue. Cliquez dessus pour ouvrir la page Informations de stratégie pour cette stratégie.
     Important : si votre stratégie sélectionnée figure dans la zone Plus, elle est uniquement visible si vous développez Plus.

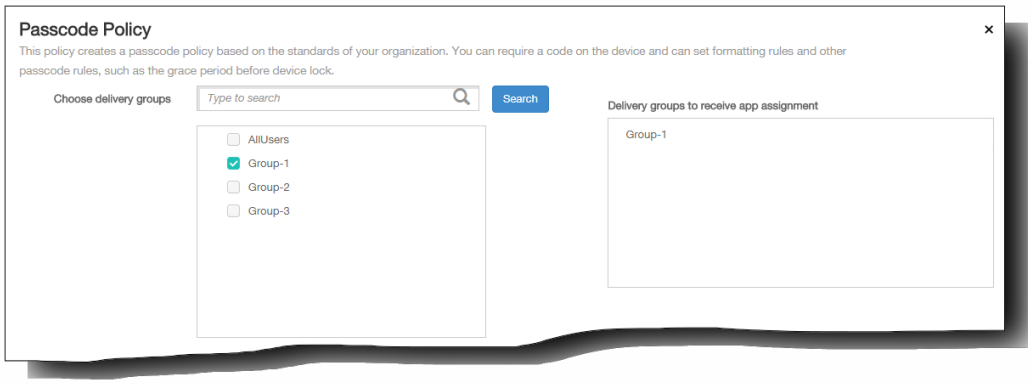


3. Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour les plates-formes sélectionnées s'affichent dans l'étape 5.
   Remarque : seules les plates-formes prises en charge par la stratégie sont répertoriées.



4. Remplissez la page Informations de stratégie puis cliquez sur Suivant. La page Informations de stratégie collecte des informations, comme le nom de la stratégie, pour vous aider à identifier et à suivre vos stratégies. Cette page est identique pour toutes les stratégies.
5. Renseignez les pages de plates-formes. Les pages de plates-formes s'affichent pour chaque plate-forme que vous avez sélectionnée dans l'étape 3. Ces pages sont différentes pour chaque stratégie. Chaque stratégie peut être différente entre les plates-formes. Les stratégies ne sont pas toutes prises en charge par toutes les plates-formes. Cliquez sur Suivant pour passer à la page de plate-forme suivante, ou lorsque toutes les pages de plate-forme sont remplies, à la page Attribution.
6. Sur la page Attribution, sélectionnez les groupes de mise à disposition auxquels vous voulez appliquer la stratégie.

Lorsque vous cliquez sur un groupe de mise à disposition, le groupe apparaît dans la zone Groupes de mise à disposition qui vont recevoir l'attribution d'applications.
Remarque : la zone Groupes de mise à disposition qui vont recevoir l'attribution d'applications n'apparaît pas tant que vous n'avez pas sélectionné un groupe de mise à disposition.



7. Cliquez sur Enregistrer.
   La stratégie est ajoutée au tableau des stratégies d'appareil.

1. Dans le tableau **Stratégies d'appareil**, sélectionnez la case à cocher en regard de la stratégie que vous souhaitez modifier ou supprimer.
2. Cliquez sur Modifier ou Supprimer.
   - Si vous cliquez sur Modifier, vous pouvez modifier tous les paramètres.
   - Si vous cliquez sur le bouton Supprimer, dans la boîte de dialogue de confirmation, cliquez de nouveau sur Supprimer.

Stratégies XenMobile par plate-forme

May 06, 2016

Le tableau suivant répertorie les stratégies d'appareils que vous pouvez ajouter et configurer dans XenMobile 10.0 pour Amazon, iOS, Android, 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.

Stratégies d'appareil	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
Communes								
Exchange		X	X	X	X		X	
Planification			X			X		
Code secret		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	X	X
Accès réseau								
APN		X	X		X			
Cellulaire			X					
Personal Hotspot		X						
Proxy		X						

Stratégies d'appareil	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
Assistance à distance					X			
Itinérance		X						
Pare-feu Samsung				X				
Tunnel			X					

	Amazon	iOS	Android	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						
Applications								
Accès applicatif		X	X			X		
Attributs d'application		X						
Configuration de l'application		X						
Inventaire des applications		X	X		X	X	X	X
Désinstallation d'applications		X	X		X			X
Restriction de désinstallation d'applications	X			X				
Fichiers			X					

Stratégies d'appareil	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
Navigateur Samsung				X	X			
Clé de sideloading								X
Certificat de signature								X
Clip Web		X	X					X
Worx Store		X	X					X
	Amazon	**iOS**	**Android**	**Samsung SAFE**	**Samsung KNOX**	**Symbian**	**Windows Phone 8.1**	**Windows 8.1 Tablet**
Sécurité								
Mode kiosque		X	X					
Restrictions applicatives					X			
Contacts (CardDAV)		X						
Informations d'identification		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	

Stratégies d'appareil	Amazon	iOS	Android	Samsung SAFE	Samsung KNOX	Symbian	Windows Phone 8.1	Windows 8.1 Tablet
Options XenMobile			X			X		
Désinstallation de XenMobile			X					
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						

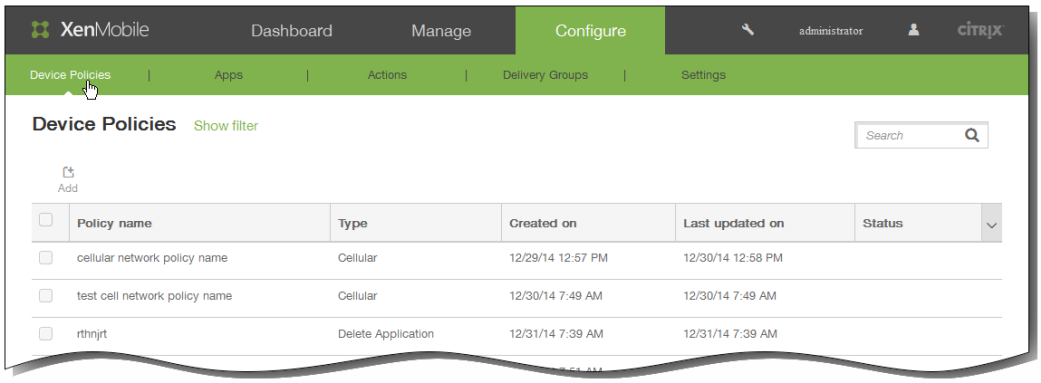
Pour ajouter une stratégie d'accès aux applications

May 06, 2016

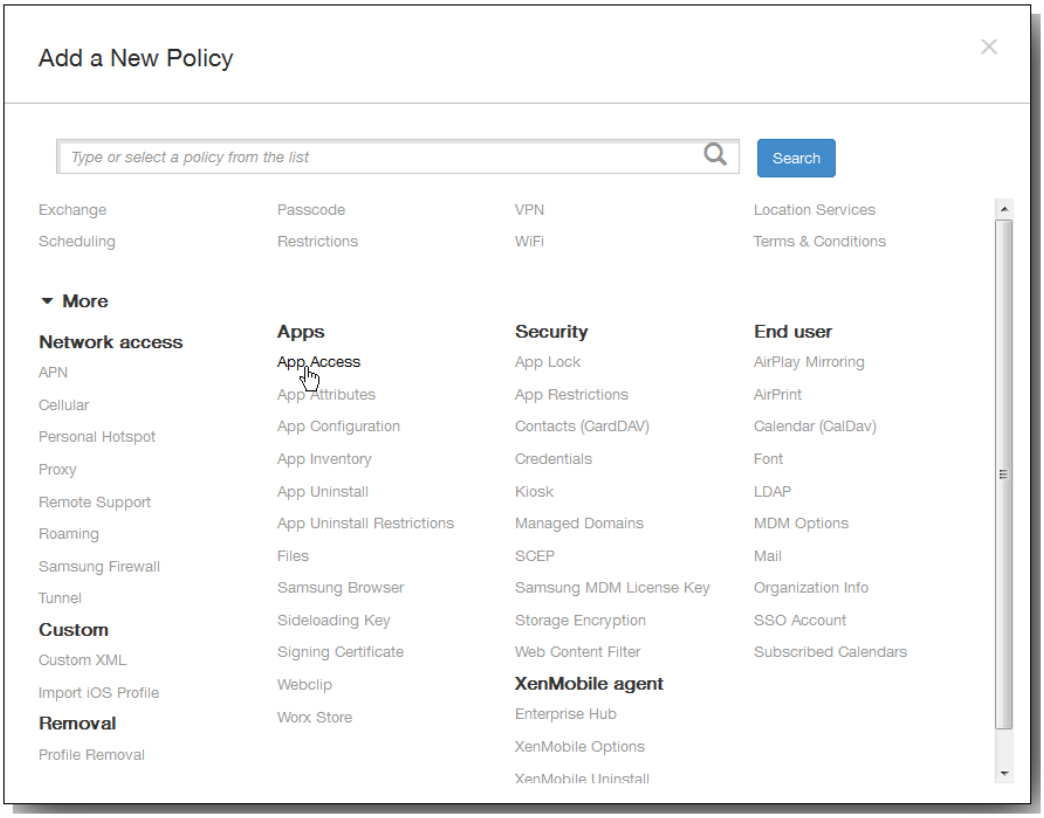
La stratégie d'accès aux applications dans XenMobile vous permet de définir une liste d'applications dont l'installation sur les appareils est obligatoire, facultative ou interdite. Vous pouvez ensuite créer une action automatisée dont la tâche consiste à vérifier la conformité de l'appareil par rapport 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.

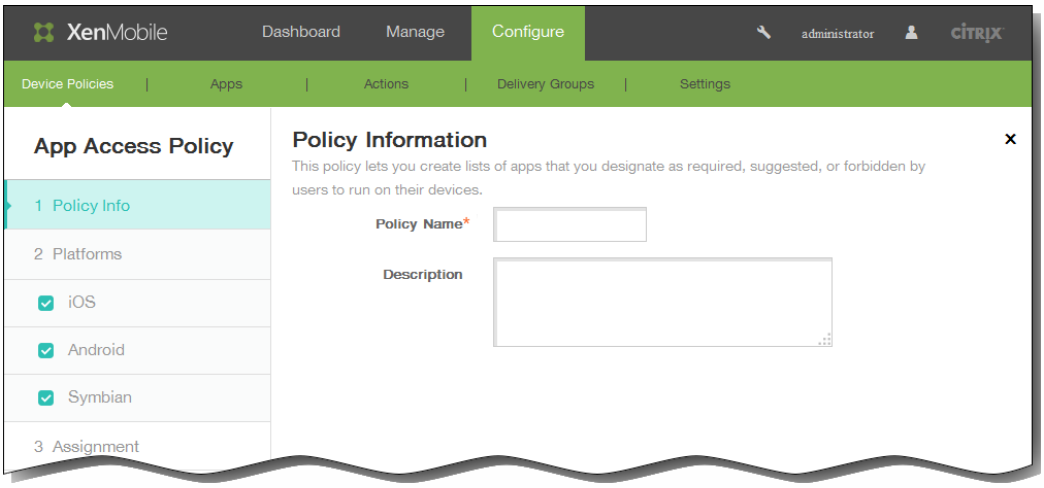
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil.



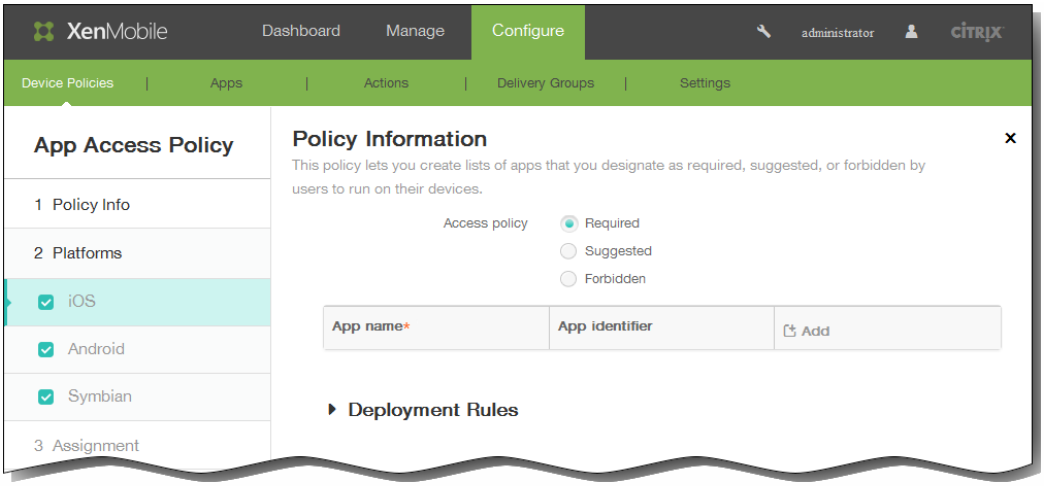
2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



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.



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.

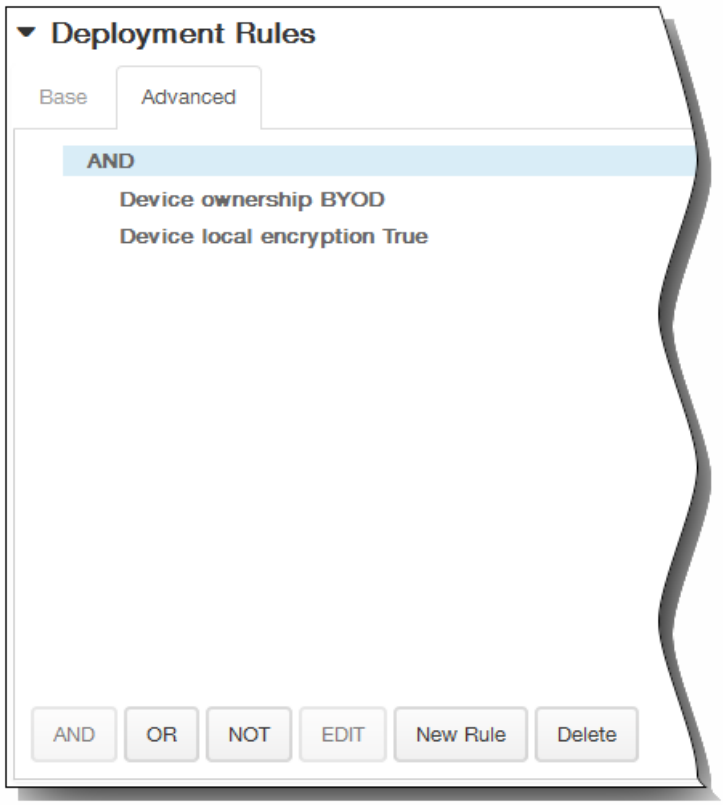
      Remarque : pour supprimer une application existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

      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.

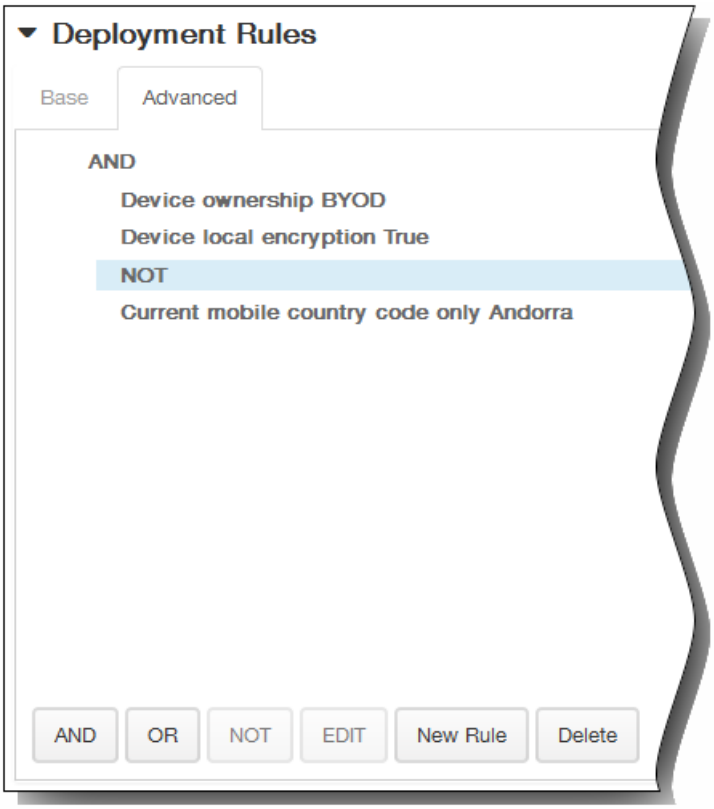
   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour 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.

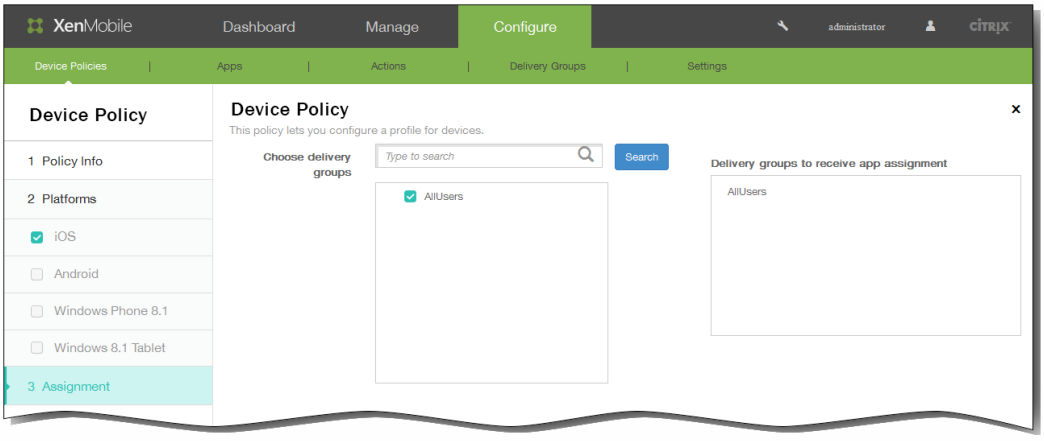


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

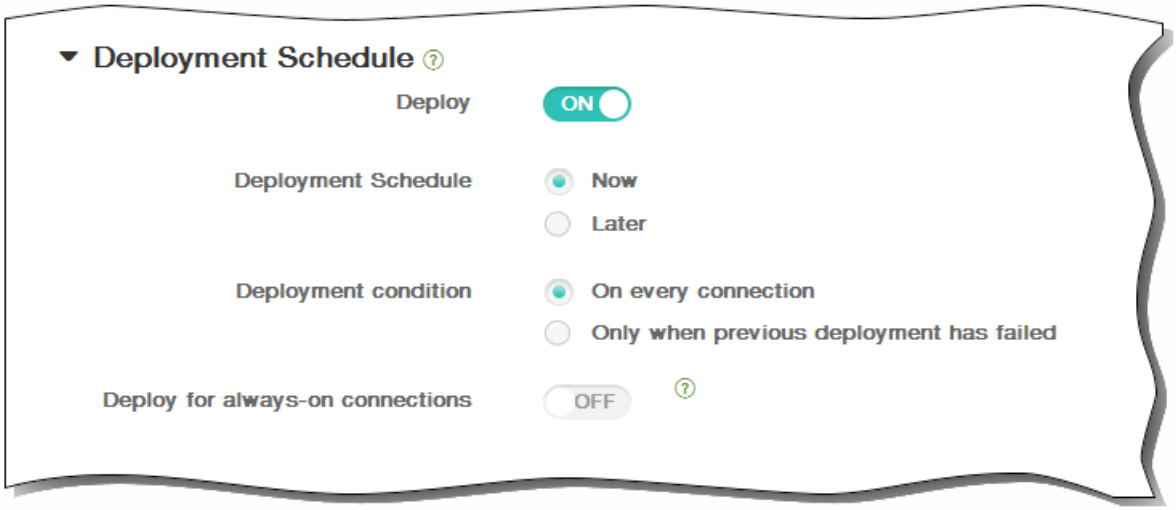


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

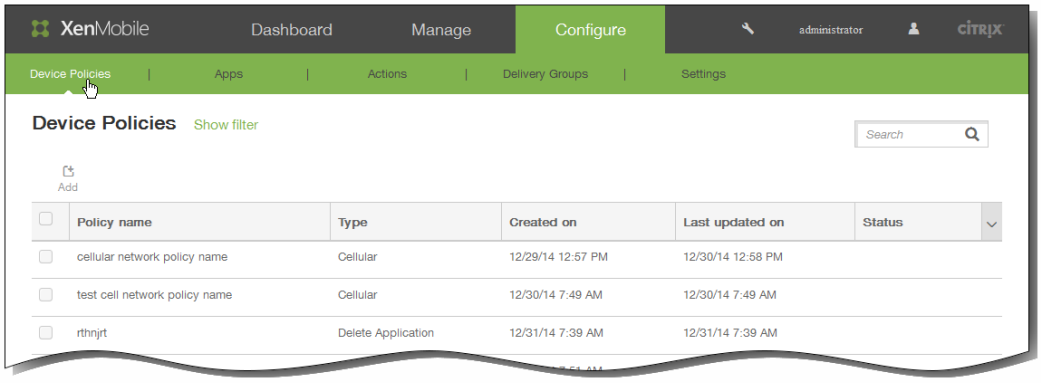
Pour ajouter une stratégie d'inventaire des applications

May 06, 2016

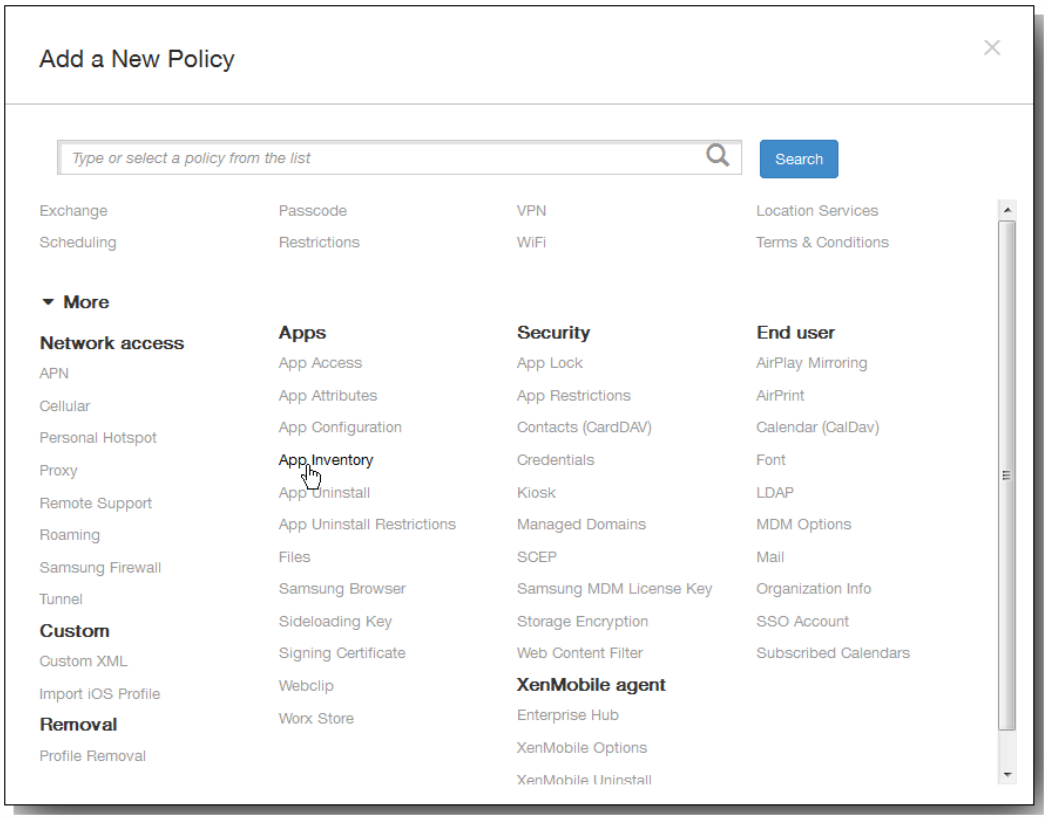
Une stratégie d'inventaire des applications dans XenMobile vous permet d'établir un inventaire des applications sur les appareils gérés, puis l'inventaire est comparé aux stratégies d'accès aux applications déployées sur ces appareils. Vous pouvez ainsi détecter les applications figurant sur une liste 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.

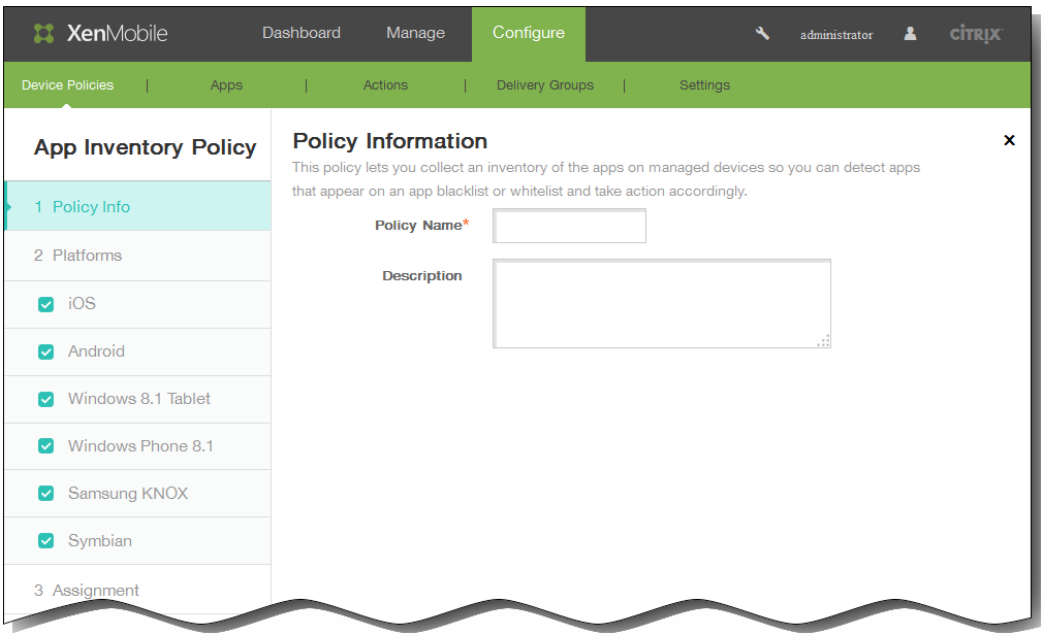
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



2. Cliquez sur Ajouter. La page Ajouter une nouvelle stratégie apparaît.

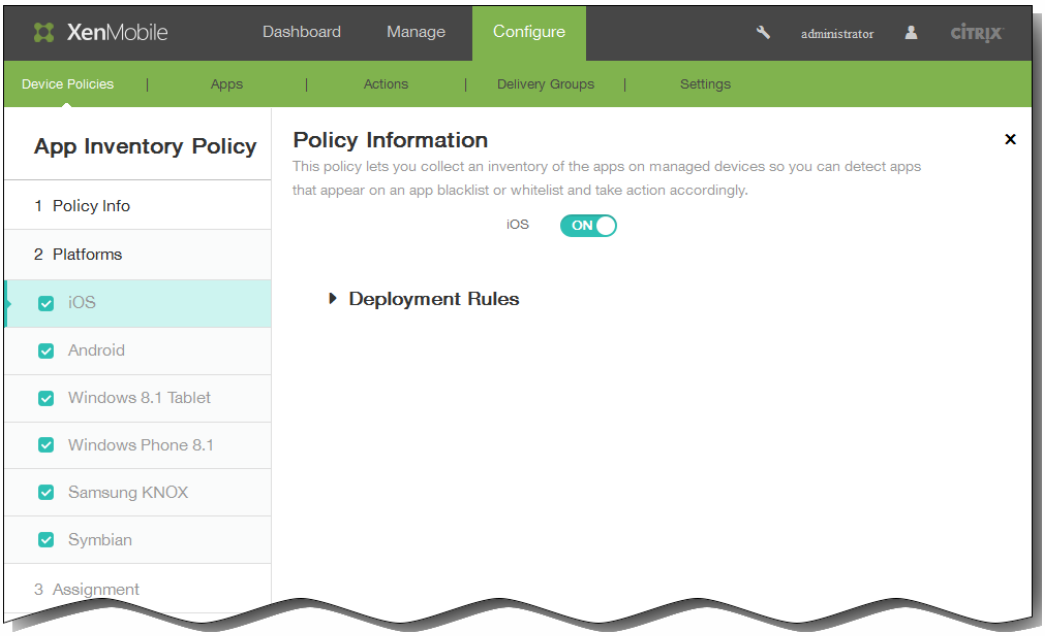


3. Cliquez sur Plus > Inventaire des applications. La page Stratégie d'inventaire des applications s'affiche.



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.

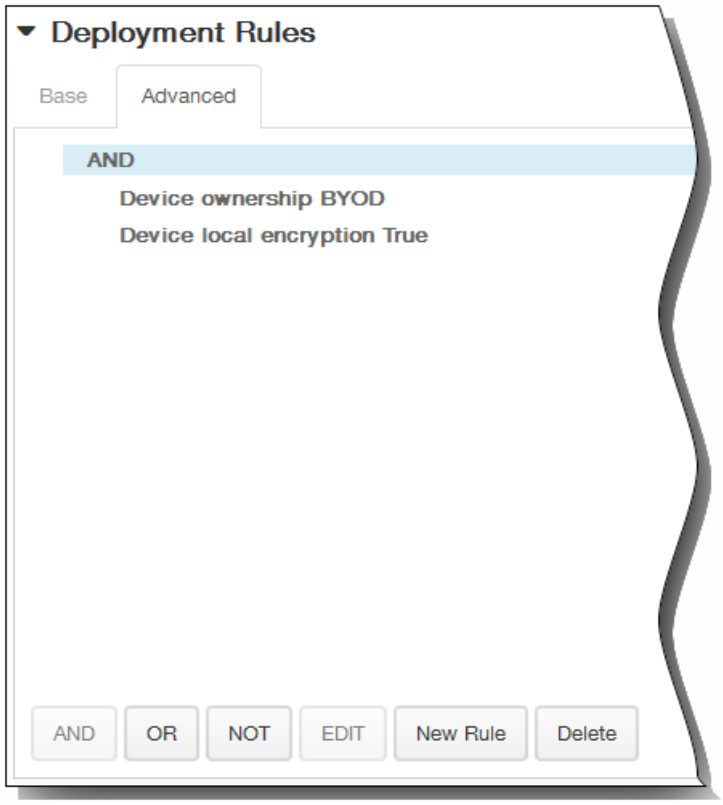
Remarque : lorsque la page Stratégie par plate-forme s'affiche, toutes les plates-formes sont sélectionnées et le panneau de configuration de la plate-forme iOS s'affiche en premier.



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.

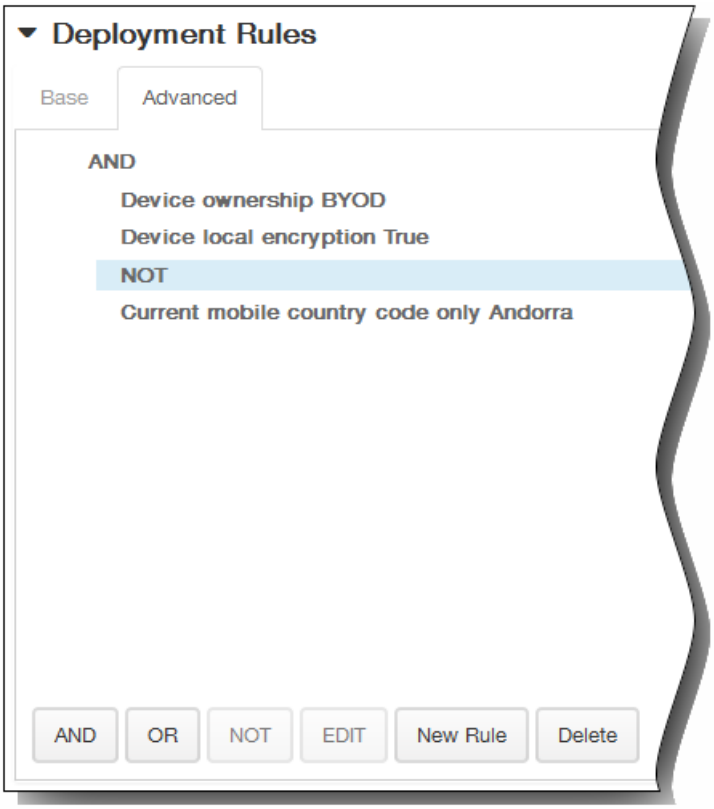
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



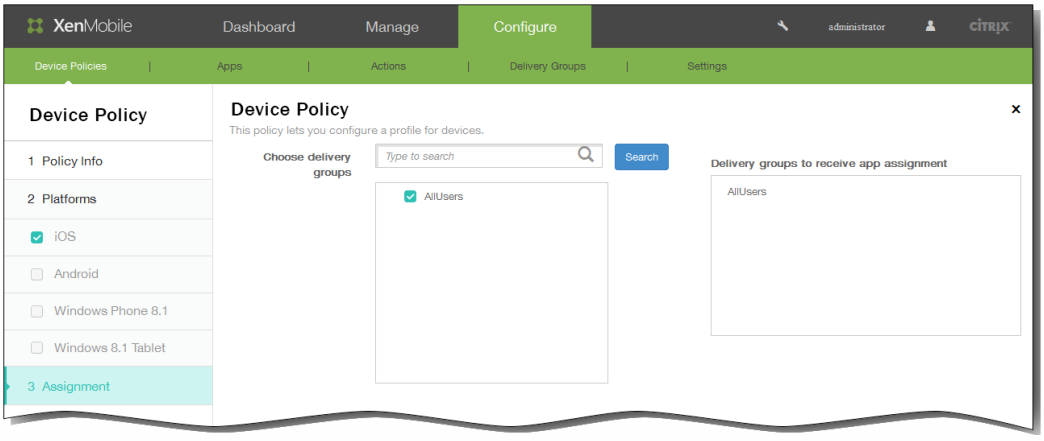
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

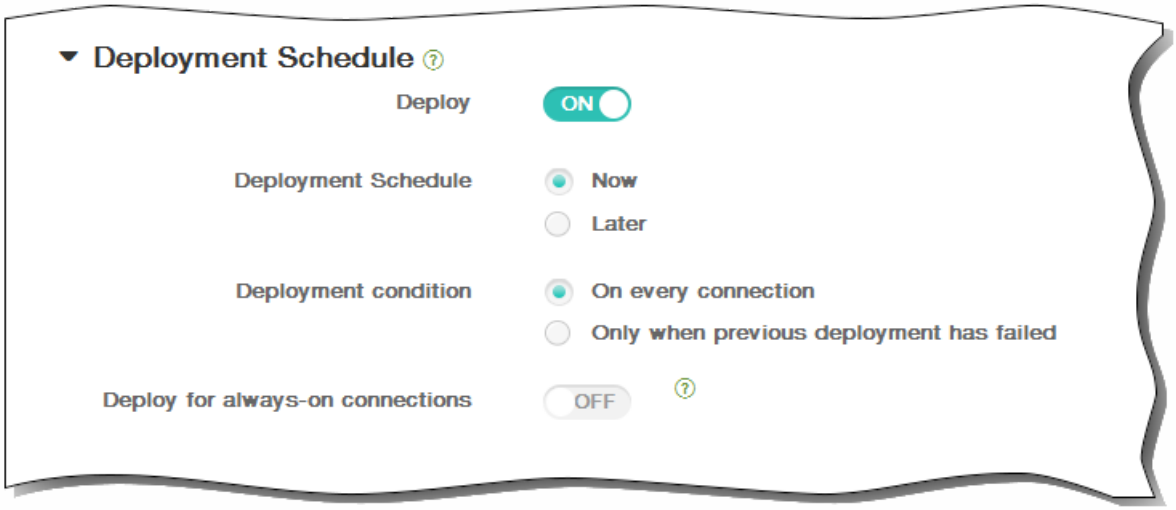


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

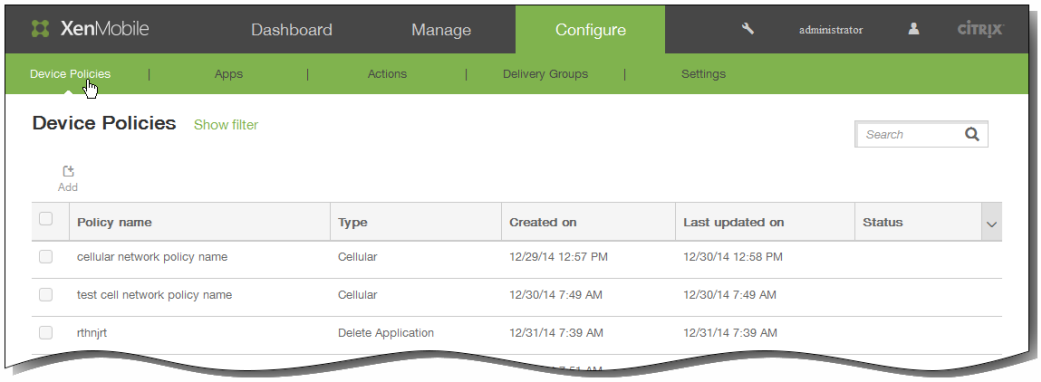
Pour ajouter une stratégie de tunnel applicatif pour Android

May 06, 2016

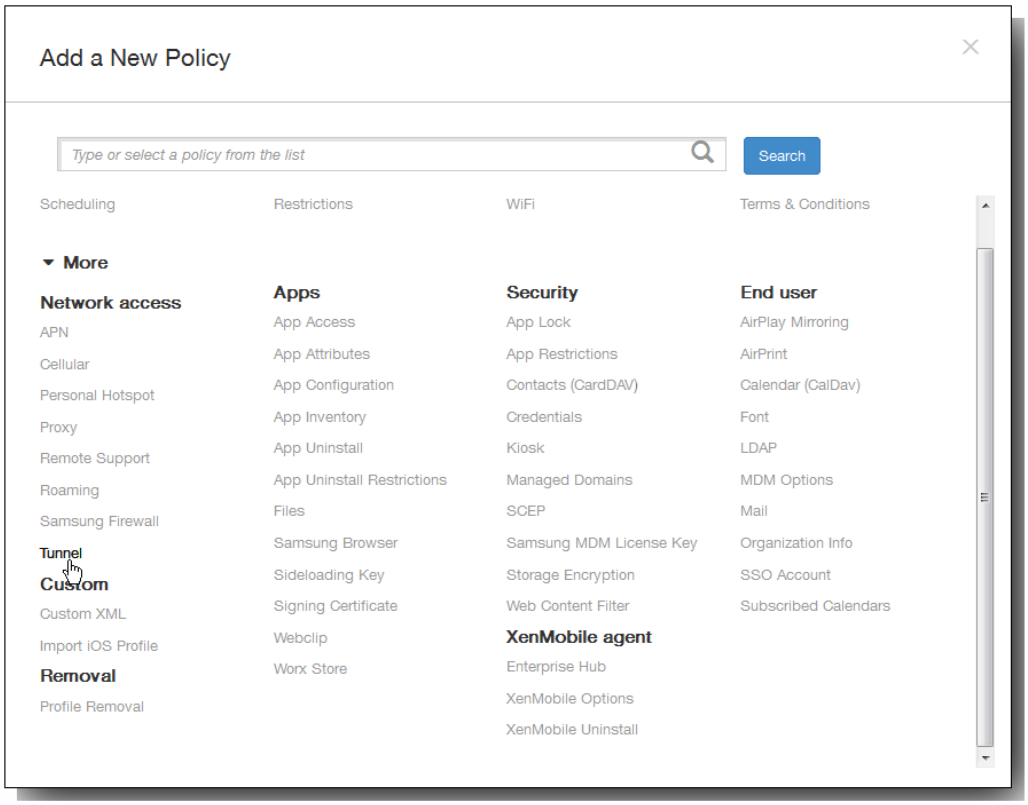
Les tunnels applicatifs sont conçus pour accroître la continuité du service et la fiabilité du transfert de données pour vos applications mobiles. Les tunnels applicatifs définissent les paramètres proxy entre le composant client de toute application d'appareil mobile et le composant de serveur d'applications. 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.

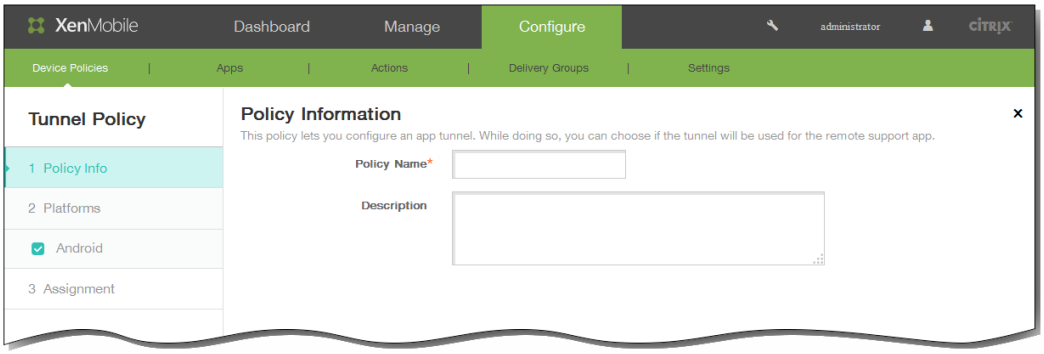
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



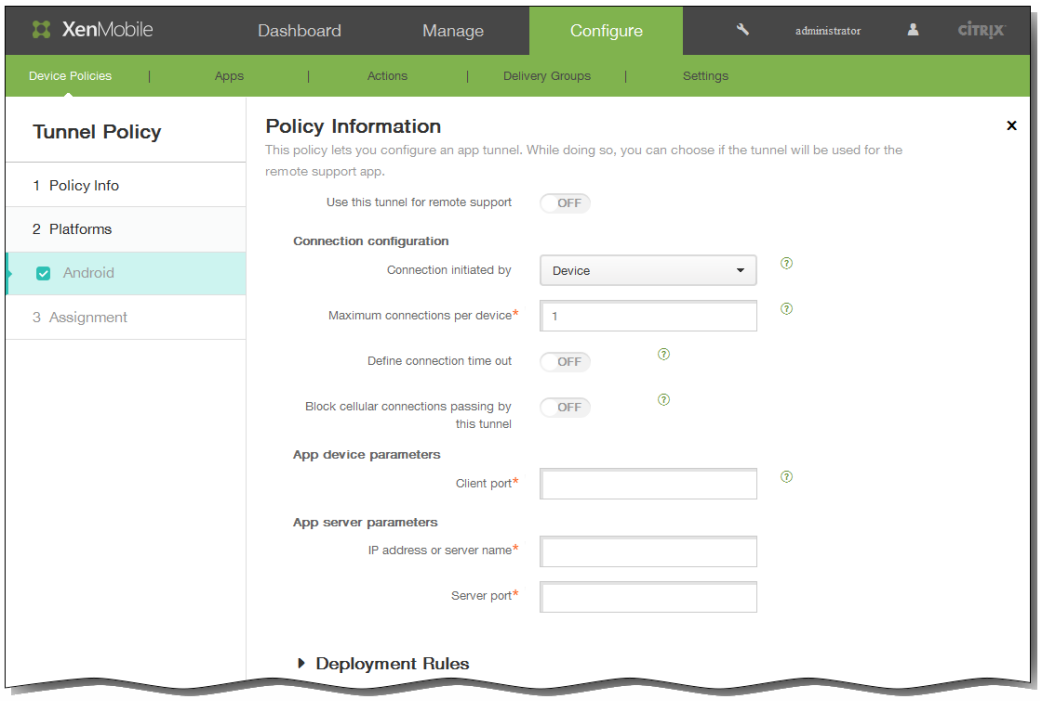
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



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.



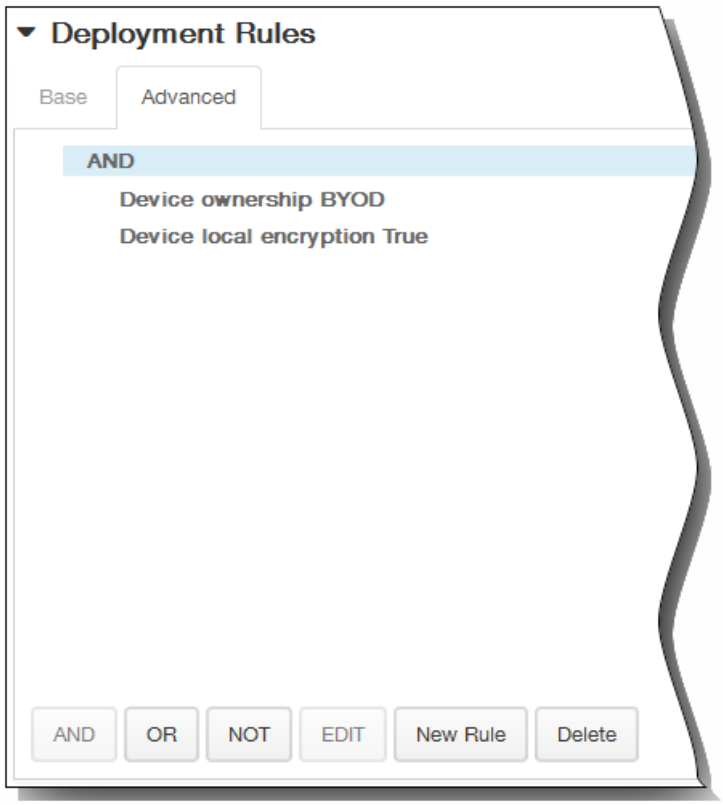
6. Dans Utiliser ce tunnel pour l'assistance à distance, spécifiez si le tunnel est utilisé pour l'assistance à distance.
   Remarque : les étapes de configuration diffèrent selon que l'assistance à distance est sélectionnée ou non.
   Si vous ne sélectionnez **pas** l'assistance à distance, procédez 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.

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.

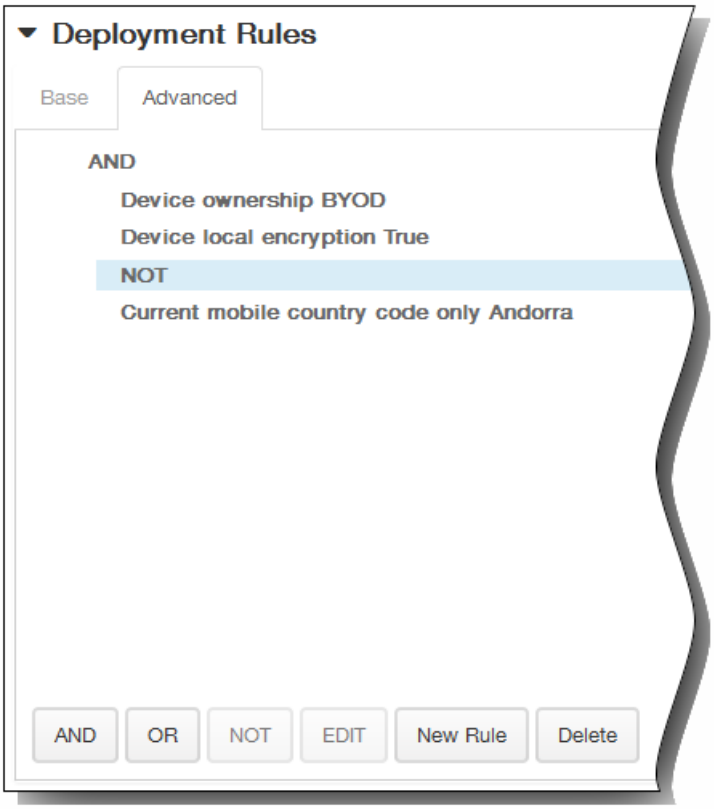


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

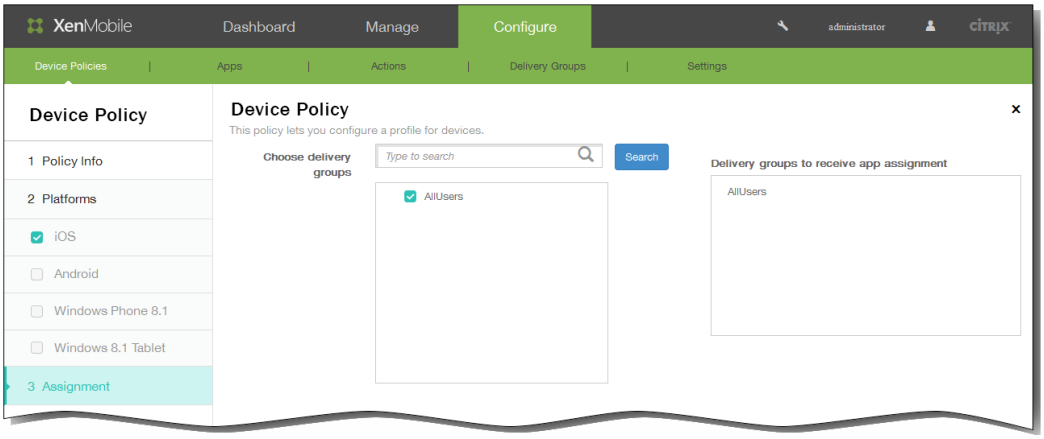
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.

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.
   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.

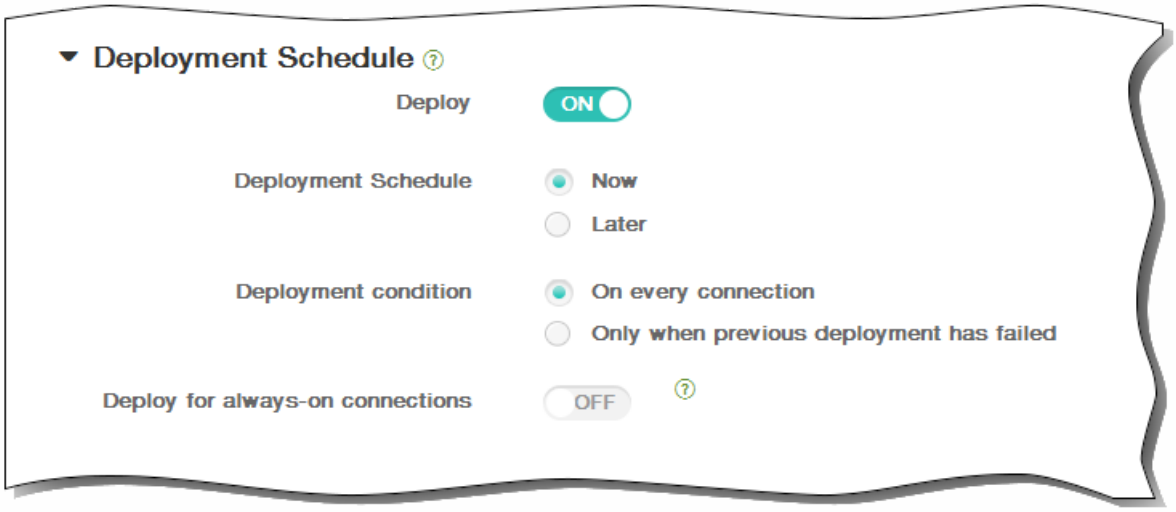


8. Cliquez sur Suivant. La page d'attribution de la Stratégie de tunnel s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



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.

Stratégies XML personnalisées

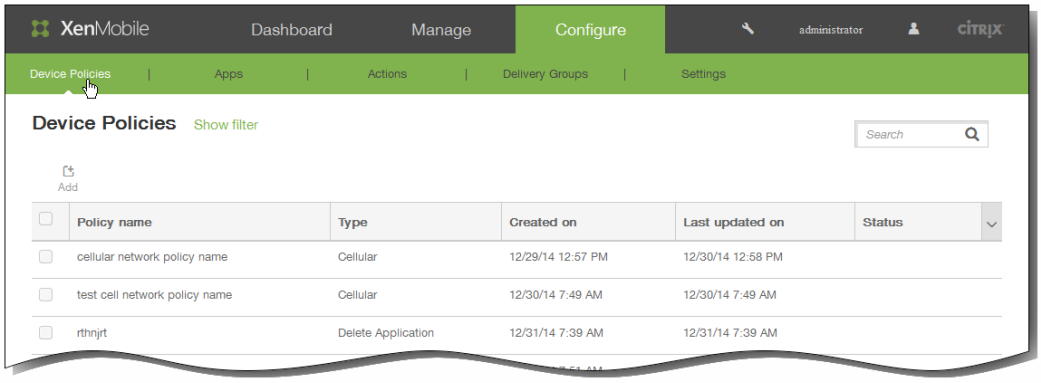
May 06, 2016

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 :

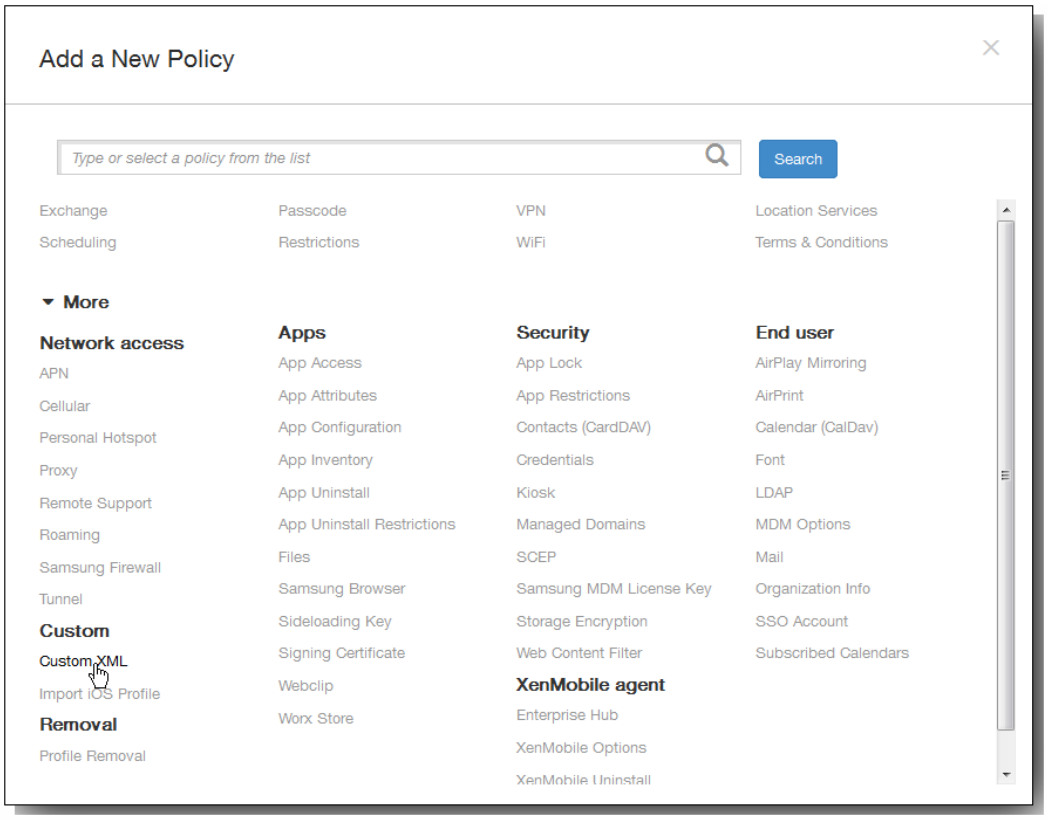
- Provisioning, qui comprend la configuration de l'appareil, et l'activation ou la désactivation de fonctionnalités.
- Configuration de l'appareil, ce qui permet aux utilisateurs de modifier les paramètres sur l'appareil.
- Mises à niveau logicielles, ce qui comprend la mise à disposition de nouveaux 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.

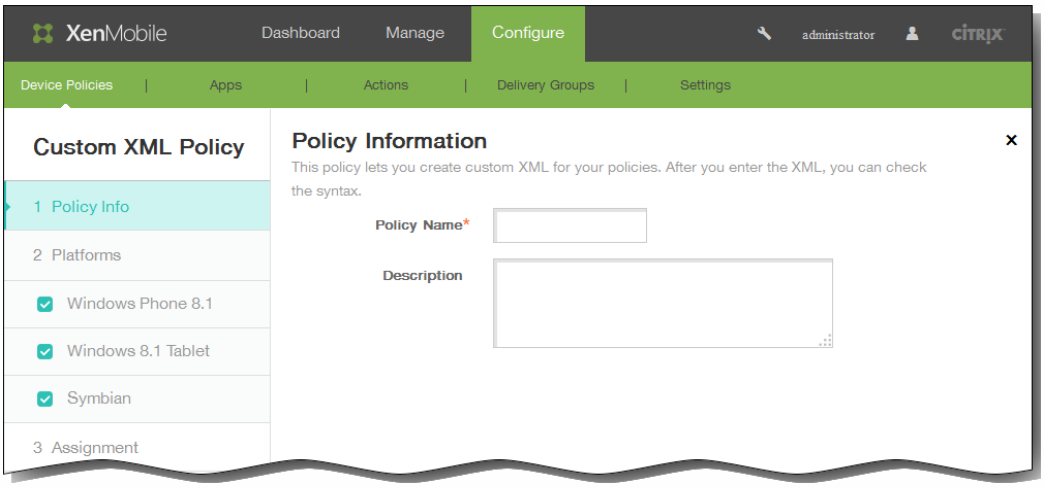
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



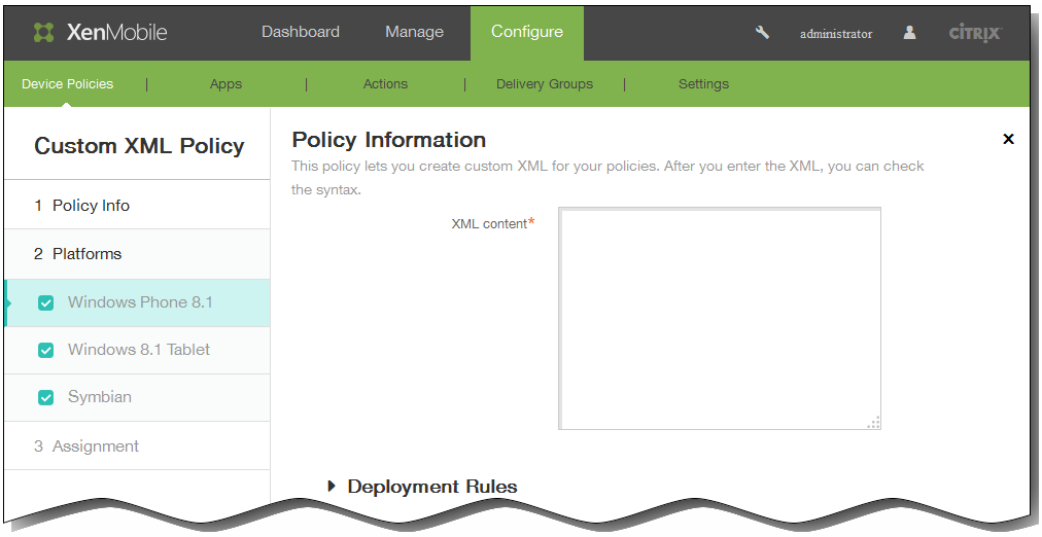
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus puis, sous Sécurité, cliquez sur XML personnalisé. La page d'informations Stratégie XML personnalisée s'affiche.

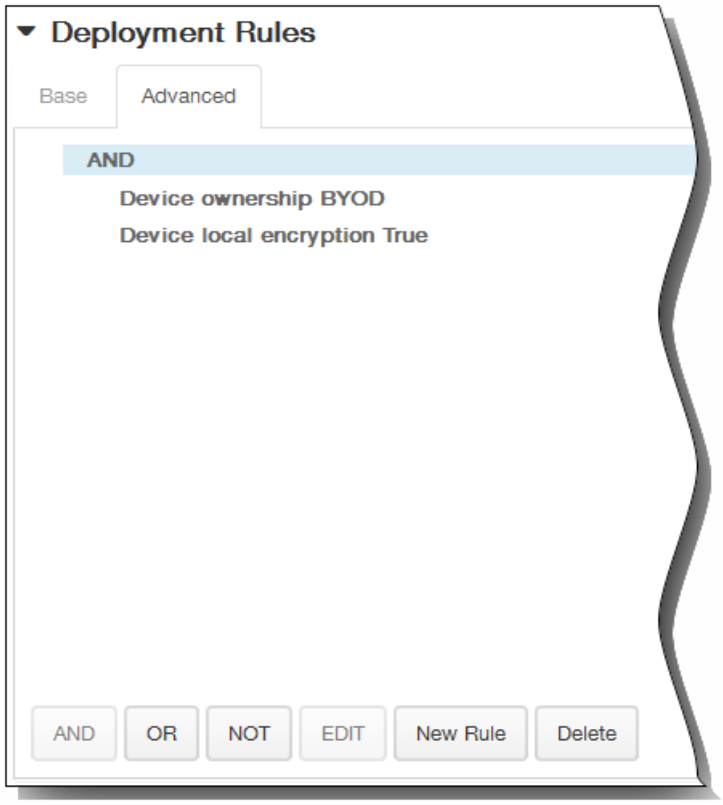


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Stratégie par plate-forme s'affiche.
   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.



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.

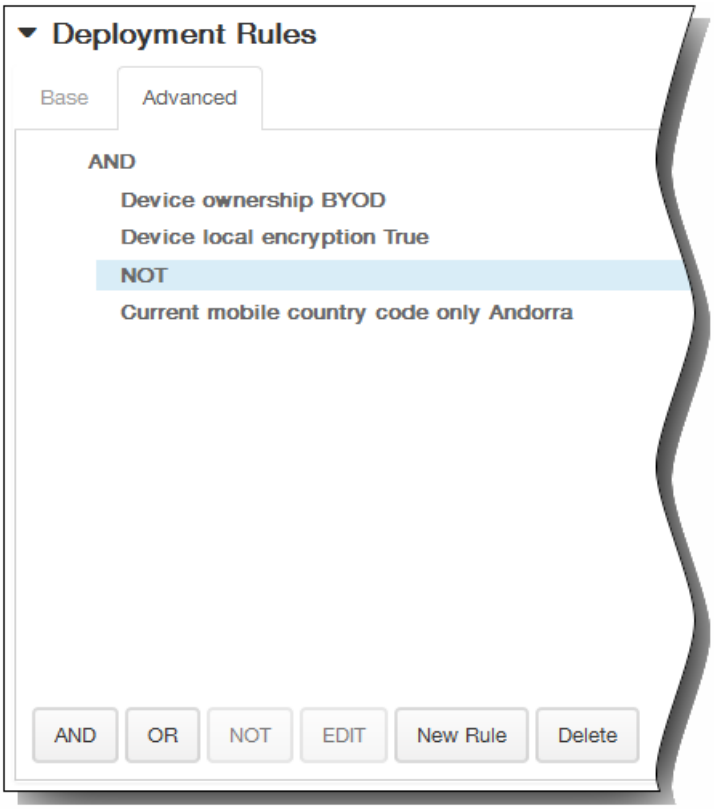
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



Les conditions que vous avez choisies sur l'onglet Base s'affichent.

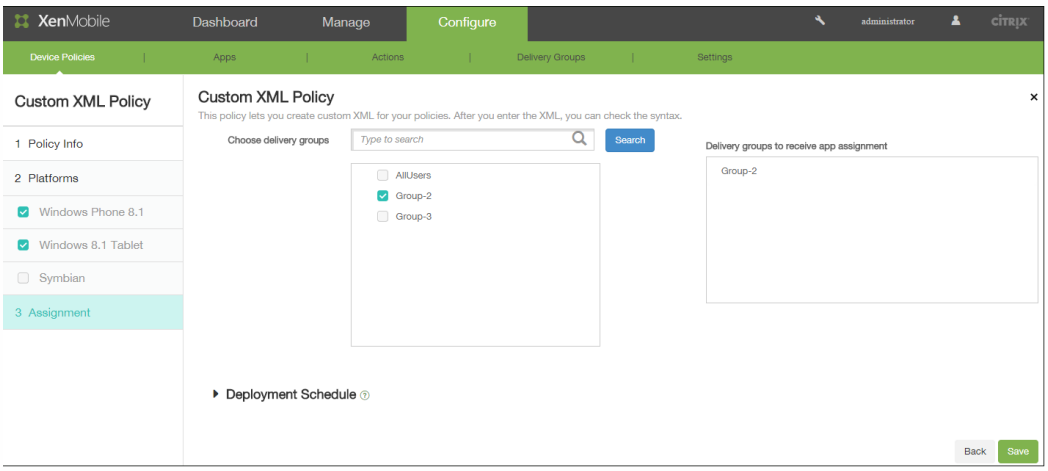
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter 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.



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.

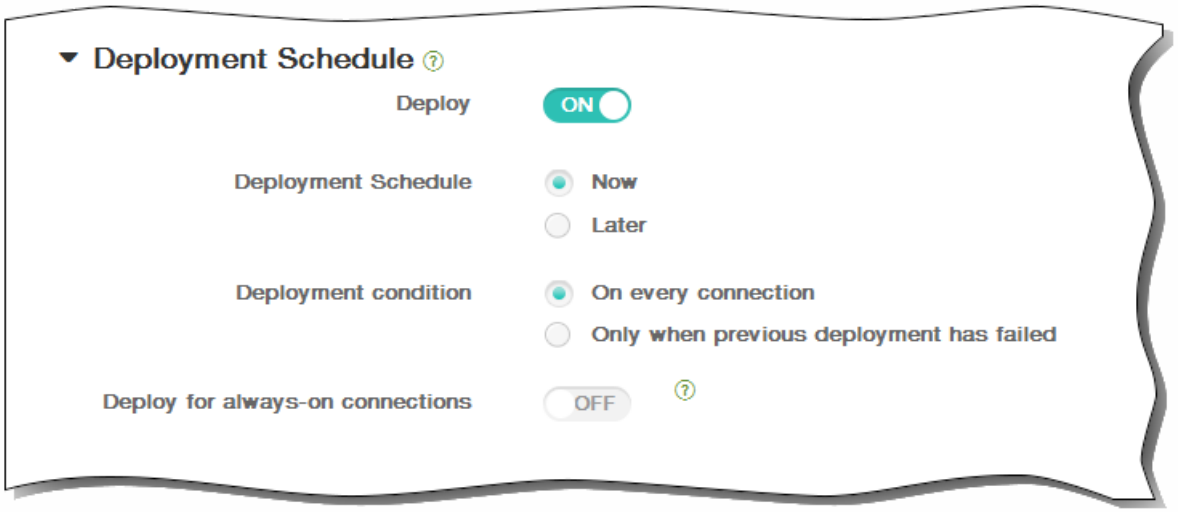
10. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition 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.

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.



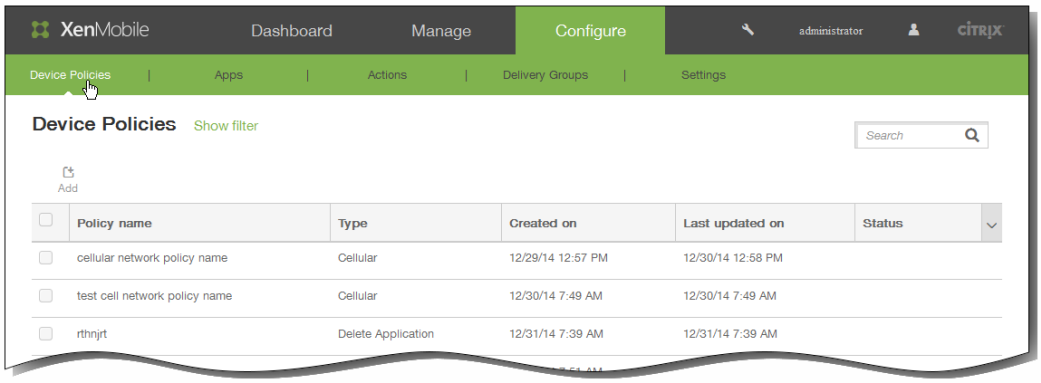
12. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de désinstallation d'application

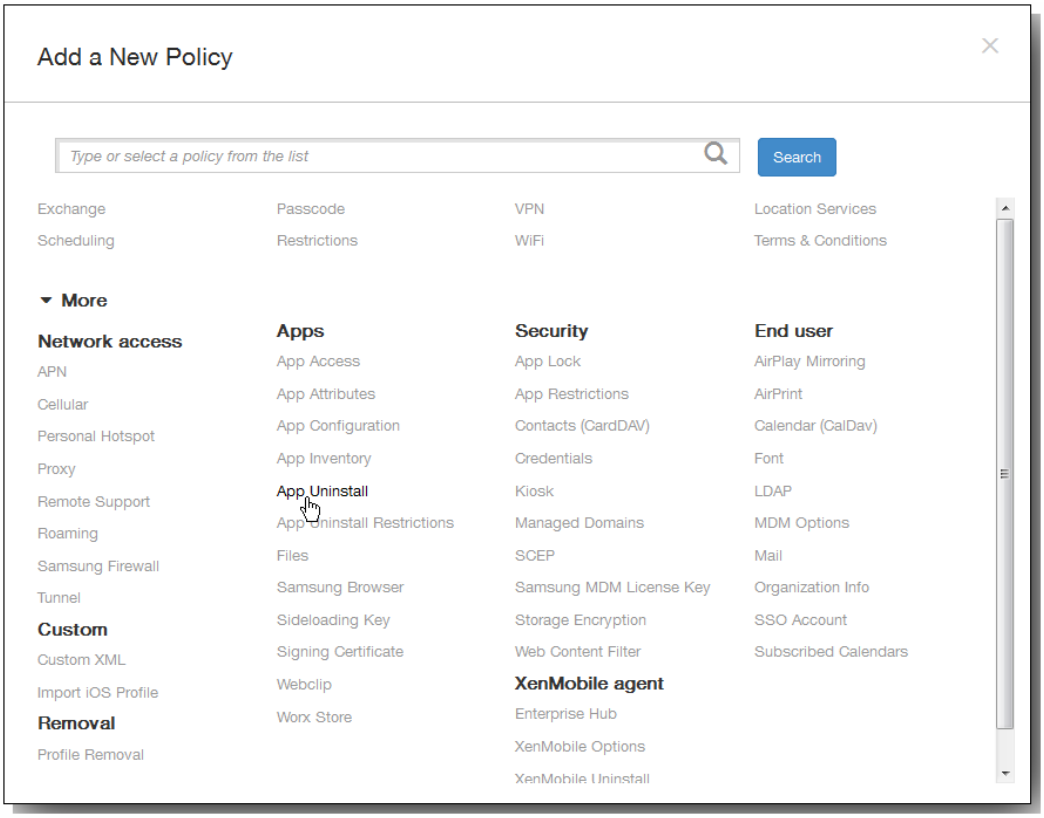
May 06, 2016

Vous pouvez créer une stratégie de désinstallation d'application pour les plates-formes iOS, Android, Samsung KNOX 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.

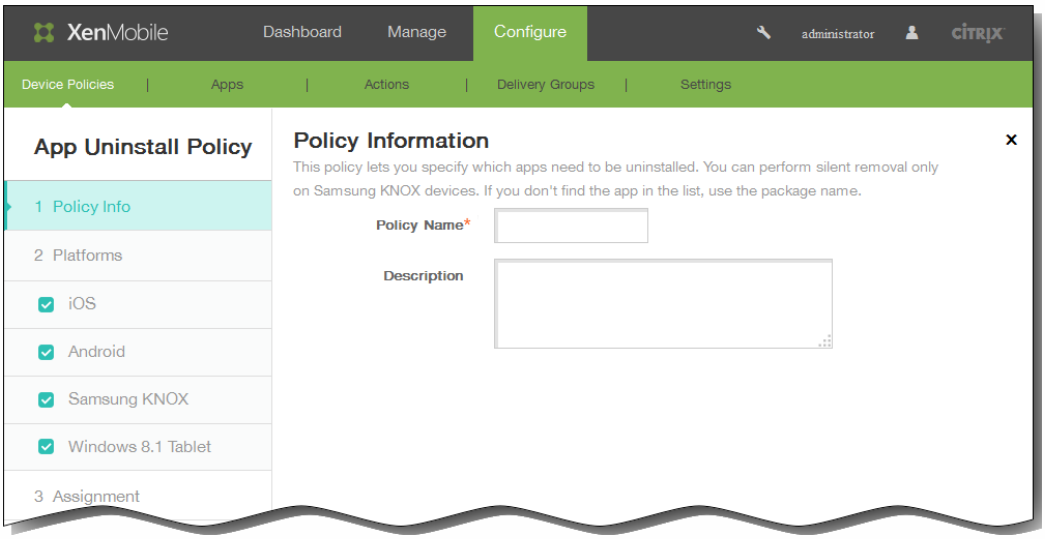
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche. Sur la page Stratégies d'appareil, cliquez sur Ajouter.



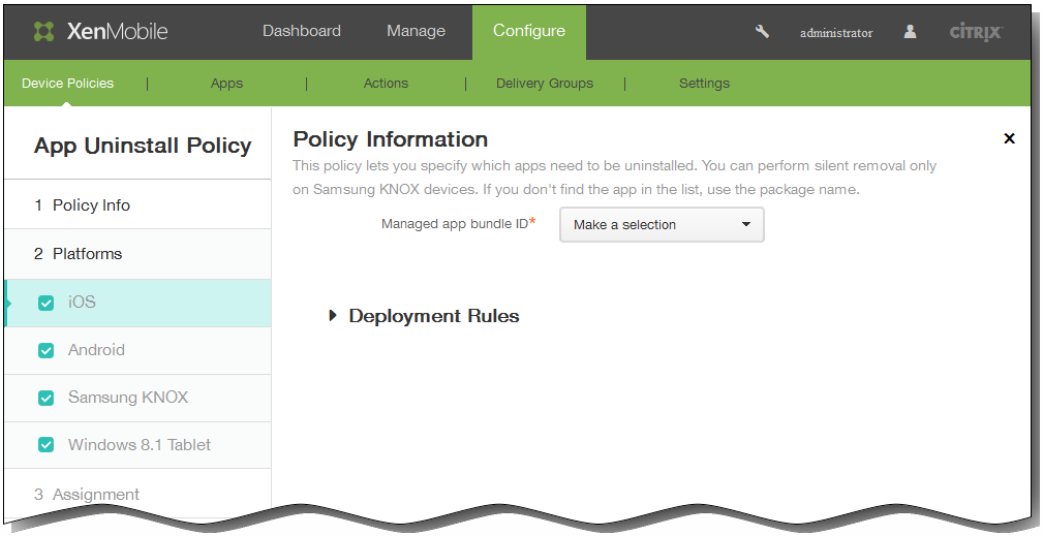
2. Dans la boîte de dialogue Ajouter une nouvelle stratégie, cliquez sur Plus puis dans Applications, cliquez sur Désinstallation des applications.



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.

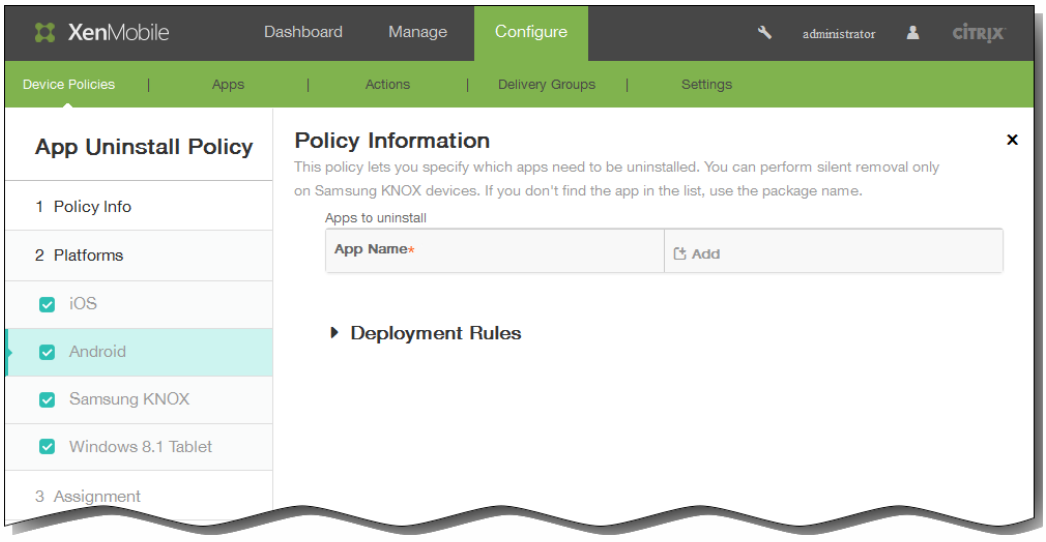


4. lorsque la page Stratégie par plate-forme s'affiche, toutes les plates-formes sont sélectionnées et le panneau de configuration de la plate-forme iOS s'affiche en premier. Dans Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter et désélectionnez celles que vous ne souhaitez pas ajouter.



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 ou Windows 8.1 Tablet :



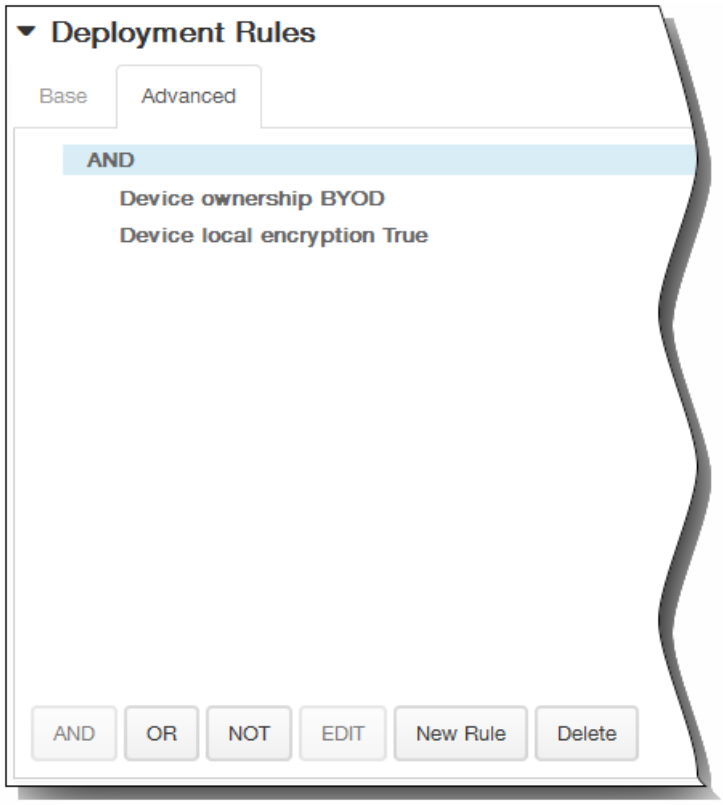
      Dans Applications à désinstaller, cliquez sur Ajouter, puis procédez comme suit :

      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.
      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.

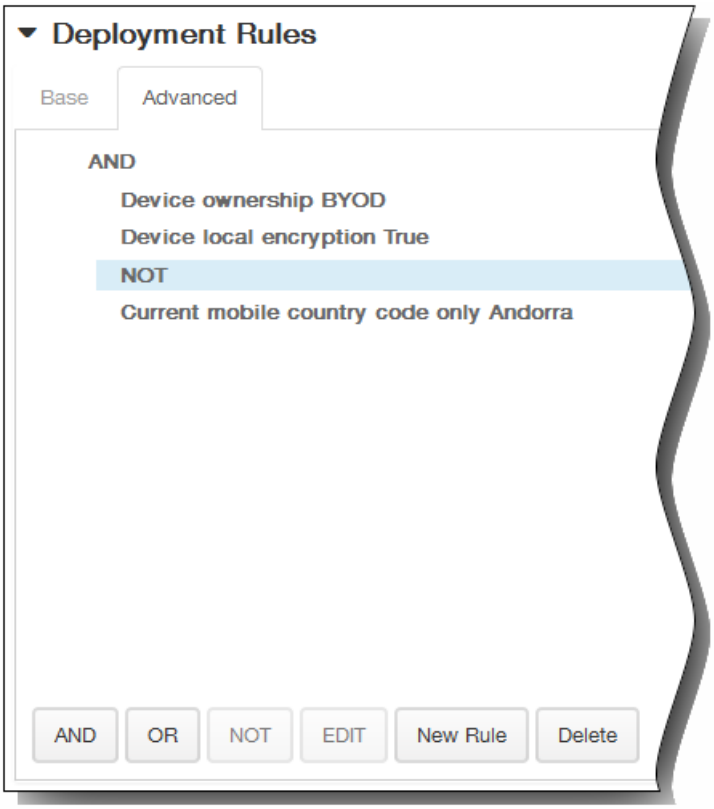
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



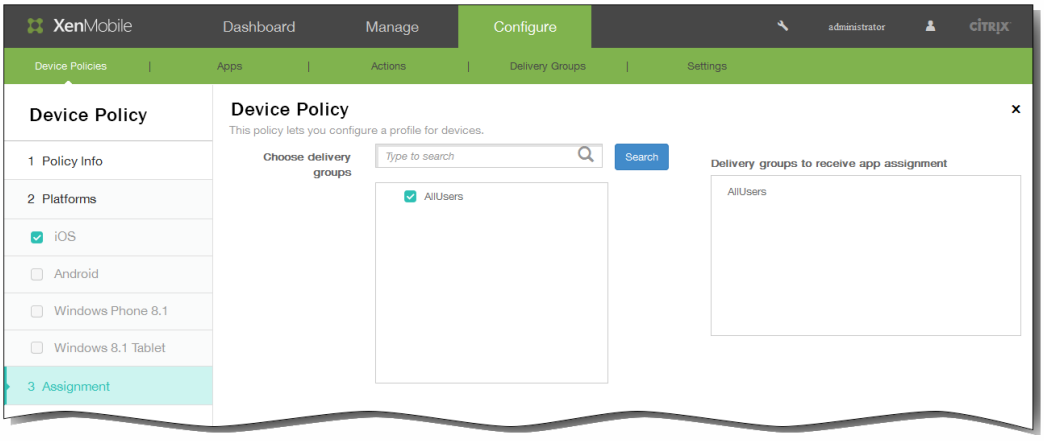
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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 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.

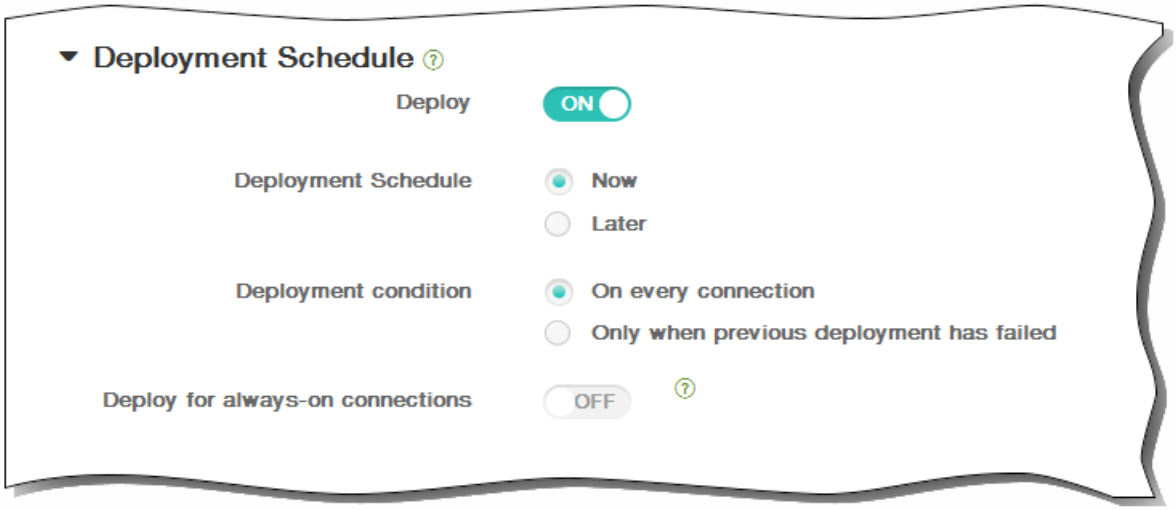


9. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

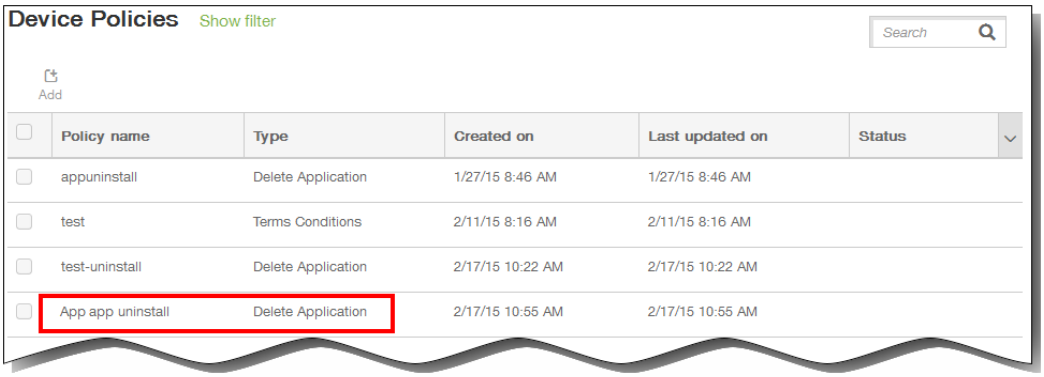
précédent a échoué. L'option par défaut est À chaque connexion.

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. Sur la page Stratégies d'appareil, la colonne Type liste les stratégies que vous avez ajoutées sous le type Supprimer une application.

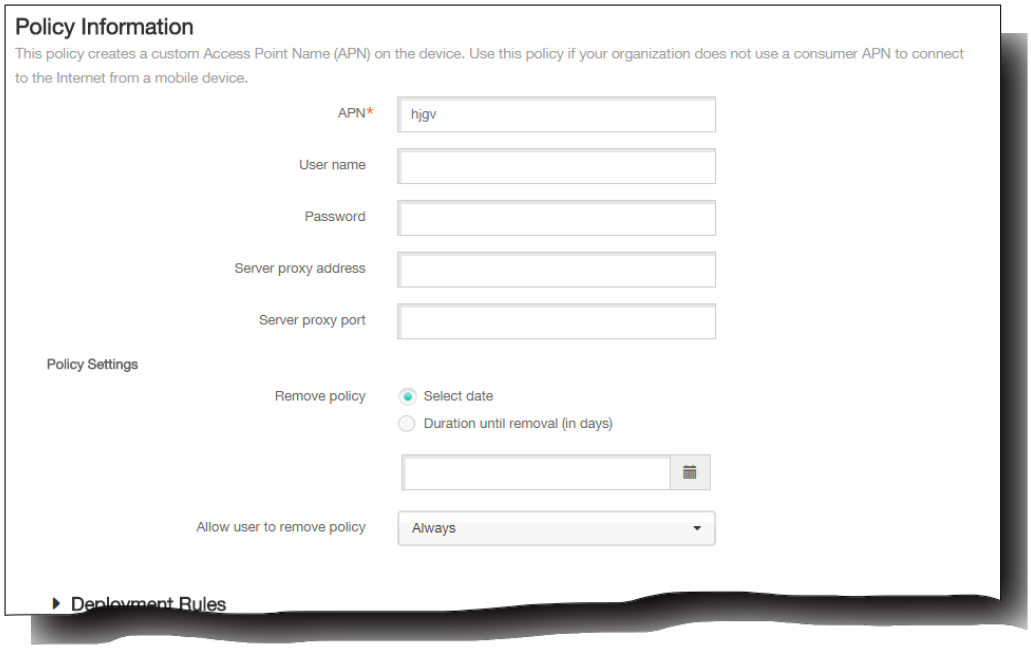


Pour ajouter une stratégie APN

May 06, 2016

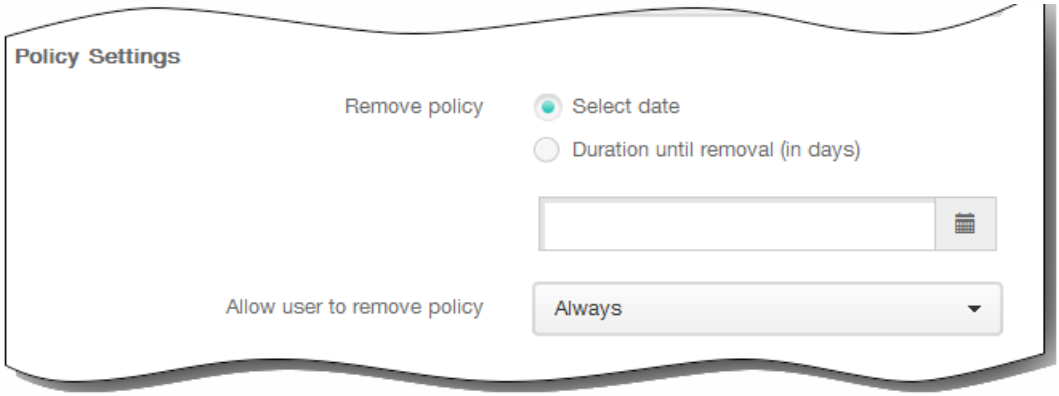
Cette stratégie vous permet de configurer un nom de point d'accès (APN) personnalisé sur iOS, Android ou Samsung KNOX. Une stratégie APN détermine les paramètres utilisés pour connecter vos appareils au service GPRS d'un opérateur de téléphonie spécifique. Ce paramètre est déjà défini dans la plupart des téléphones les plus récents.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil > Ajouter.
2. Sur la page Ajouter une nouvelle stratégie, cliquez sur Plus puis sous Accès réseau, cliquez sur APN.
3. Sélectionnez les plates-formes que vous souhaitez inclure dans la stratégie. Les pages de configuration pour la plate-forme sélectionnée s'affichent dans l'étape 5.
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 première page d'informations sur la plate-forme s'affiche.
6. Si vous avez sélectionné la plate-forme iOS, sur la page d'informations sur la plate-forme iOS, procédez comme suit :



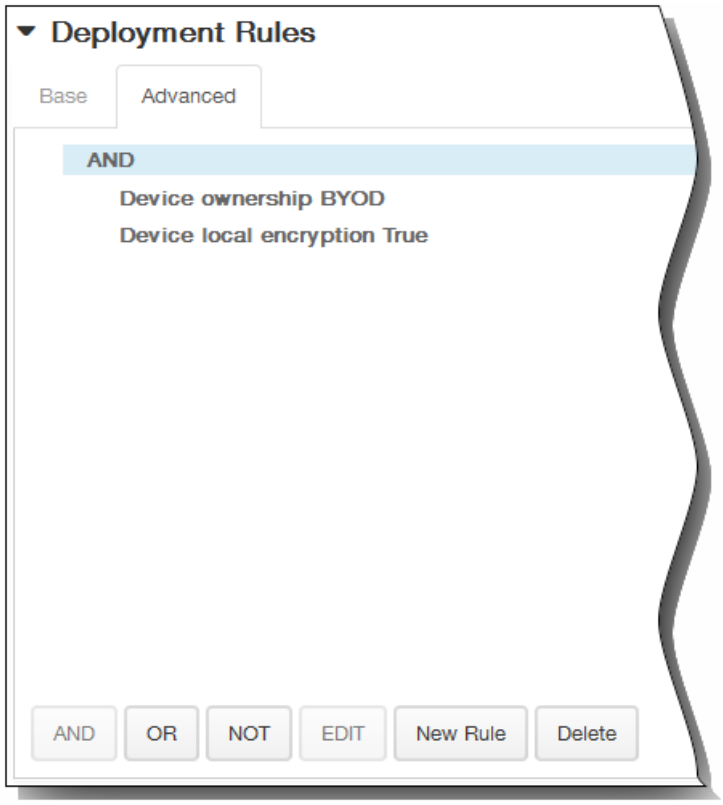
   1. APN. Entrez le nom du point d'accès.
   2. Nom d'utilisateur. Cette chaîne spécifie le nom d'utilisateur pour ce point d'accès. S'il est manquant, l'appareil invite à saisir la chaîne lors de l'installation du profil.
   3. Password. Mot de passe utilisateur pour ce point d'accès. Afin de masquer 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.
   4. Adresse du serveur proxy. Adresse IP ou adresse URL du proxy APN.
   5. Port du serveur proxy. Numéro de port du proxy APN.
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.

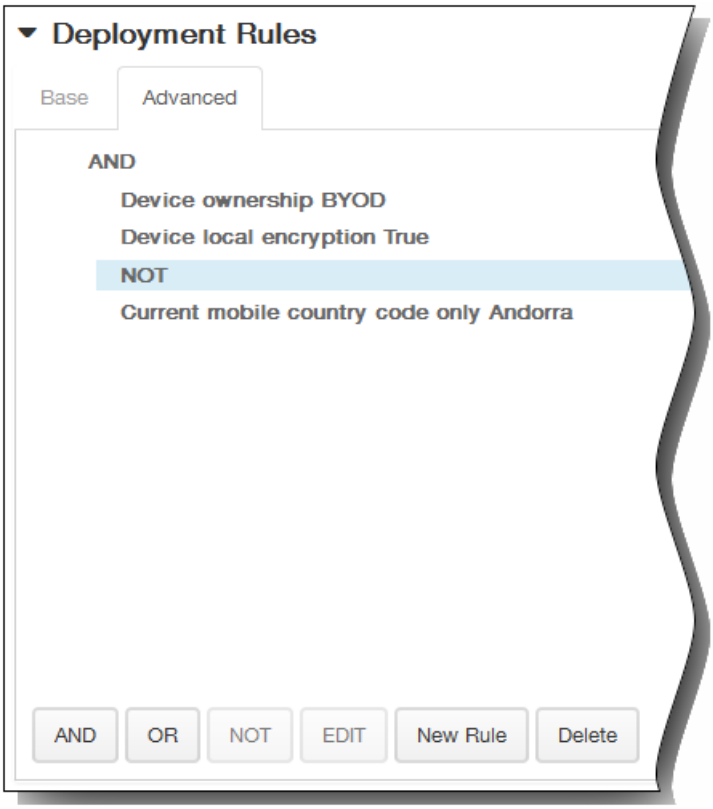
    1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
        1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
        2. Cliquez sur Nouvelle règle 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.



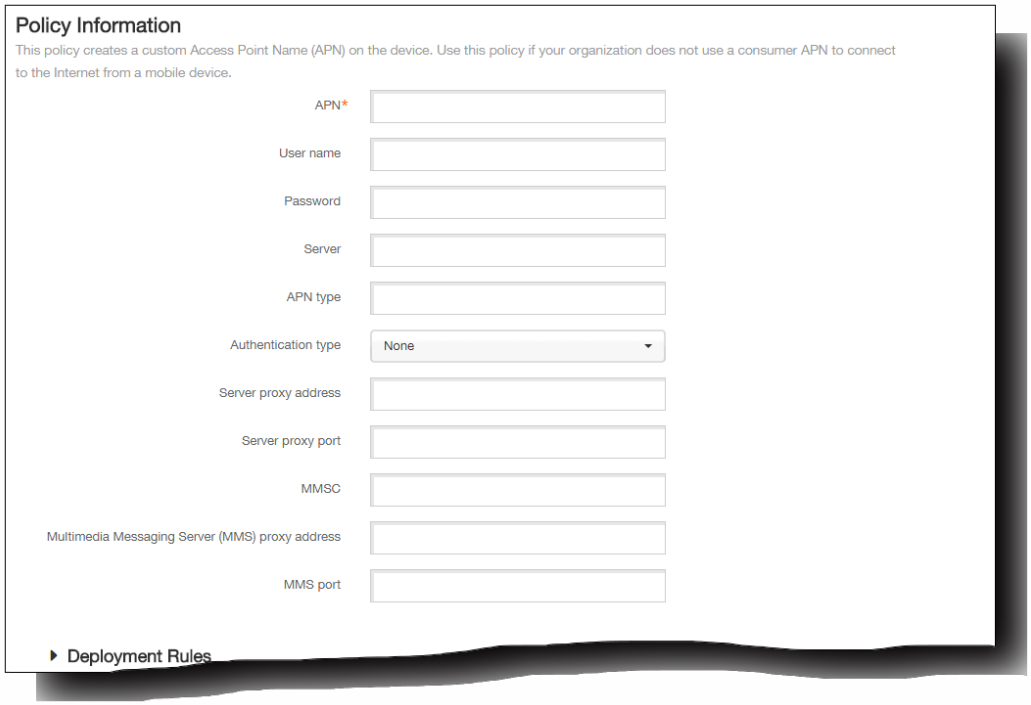
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



12. Si vous avez sélectionné les plates-formes Android ou Samsung KNOX, sur la page d'informations sur la plate-forme, procédez comme suit :

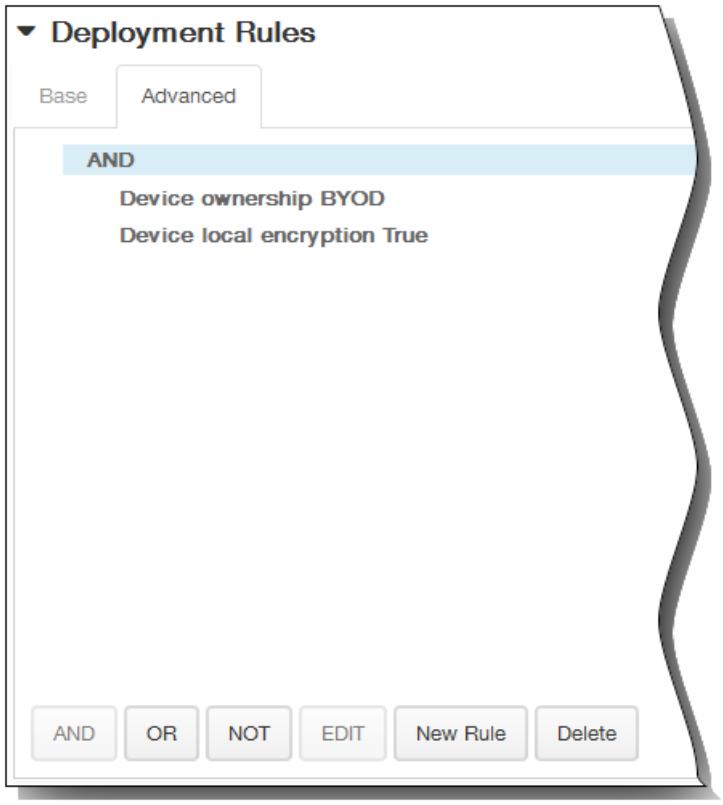


1. APN. Entrez le nom du point d'accès.

2. 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.
3. Password. 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.
4. 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.
5. Type d'APN. Ce paramètre doit s'aligner avec l'utilisation prévue du point d'accès par l'opérateur. Il s'agit d'une chaîne délimitée par des virgules des spécificateurs de service APN et doit correspondre aux définitions publiées de l'opérateur sans fil. Exemples :
   - *. Tout le trafic transite via ce point d'accès.
   - mms. Le trafic multimédia transite via ce point d'accès.
   - default. Tout le trafic, y compris le multimédia, transite via ce point d'accès.
   - supl. Le protocole SUPL est associé au GPS assisté.
   - dun. L'accès réseau à distance est obsolète et rarement utilisé.
   - hipri. Réseau haute priorité.
   - fota. FOTA (Firmware over the air) est utilisé pour recevoir les mises à jour du firmware.
6. Type d'authentification. Doit contenir PAP, CHAP ou PAP ou CHAP. Valeur par défaut Aucun.
7. Adresse du serveur proxy. Adresse IP ou adresse URL du proxy APN.
8. Port du serveur proxy. Numéro de port du proxy APN.
9. MMSC. Il s'agit du serveur du service de messagerie multimédia 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).
10. Adresse du proxy MMS. Il s'agit d'un serveur proxy HTTP pour le trafic MMS.
11. Port MMS. Port utilisé par le proxy MMS.

13. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

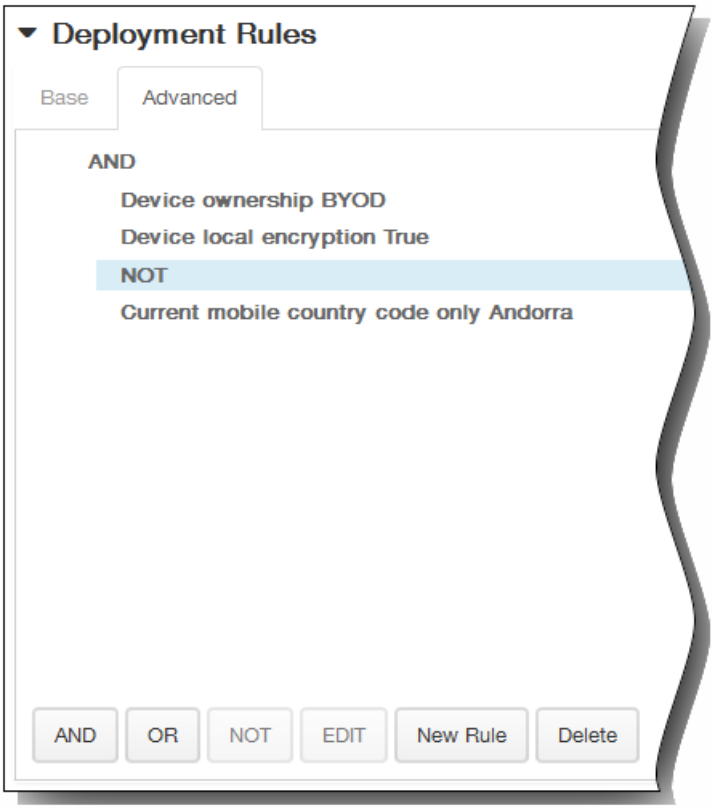
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



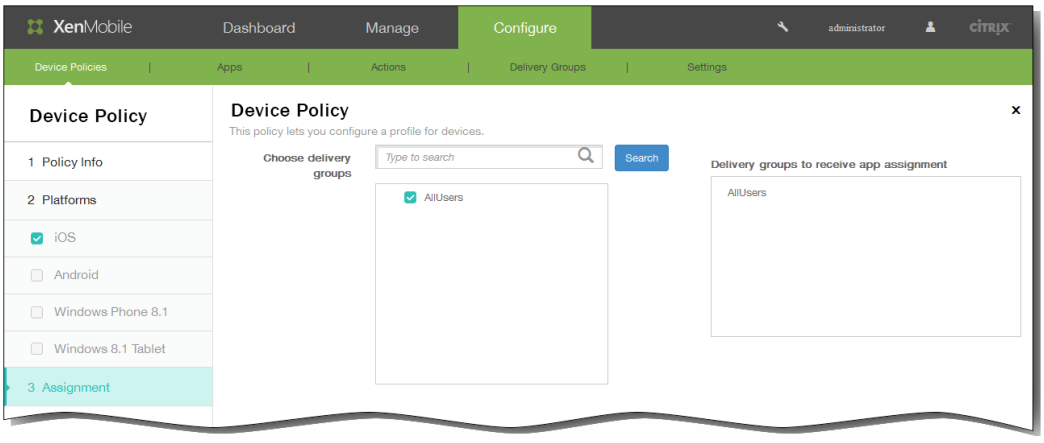
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
      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.



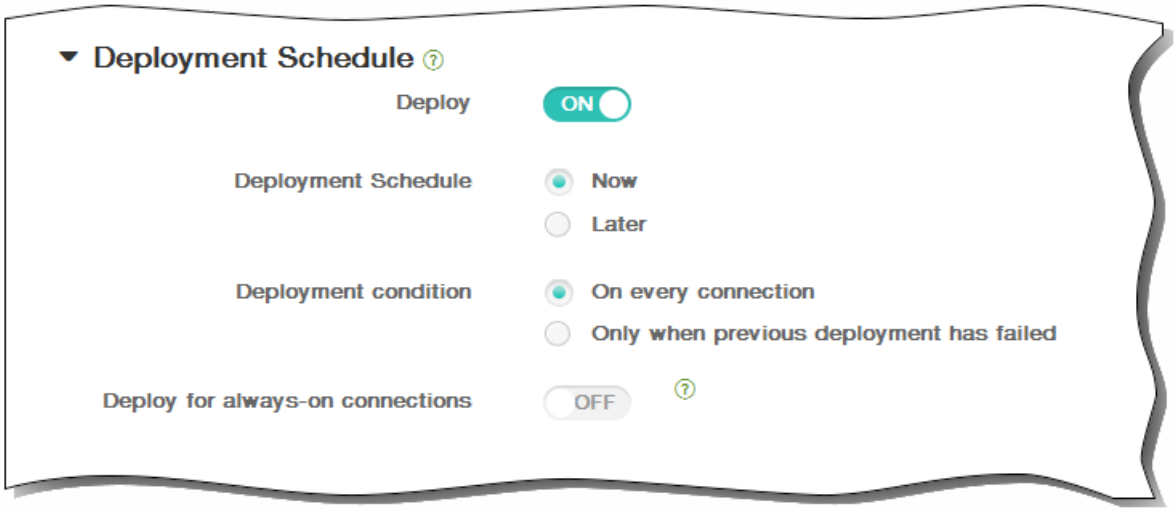
14. Si vous avez sélectionné les plates-formes Android ou Samsung KNOX, répétez l'étape 8 pour compléter la page des informations sur la plate-forme Samsung KNOX, puis cliquez sur Suivant. La page d'attribution de la Stratégie APN s'affiche.
15. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer 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. 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.



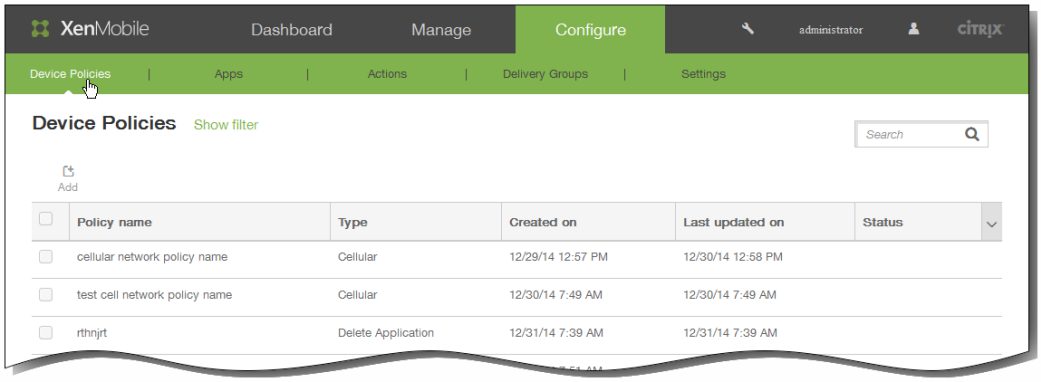
17. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie cellulaire pour iOS

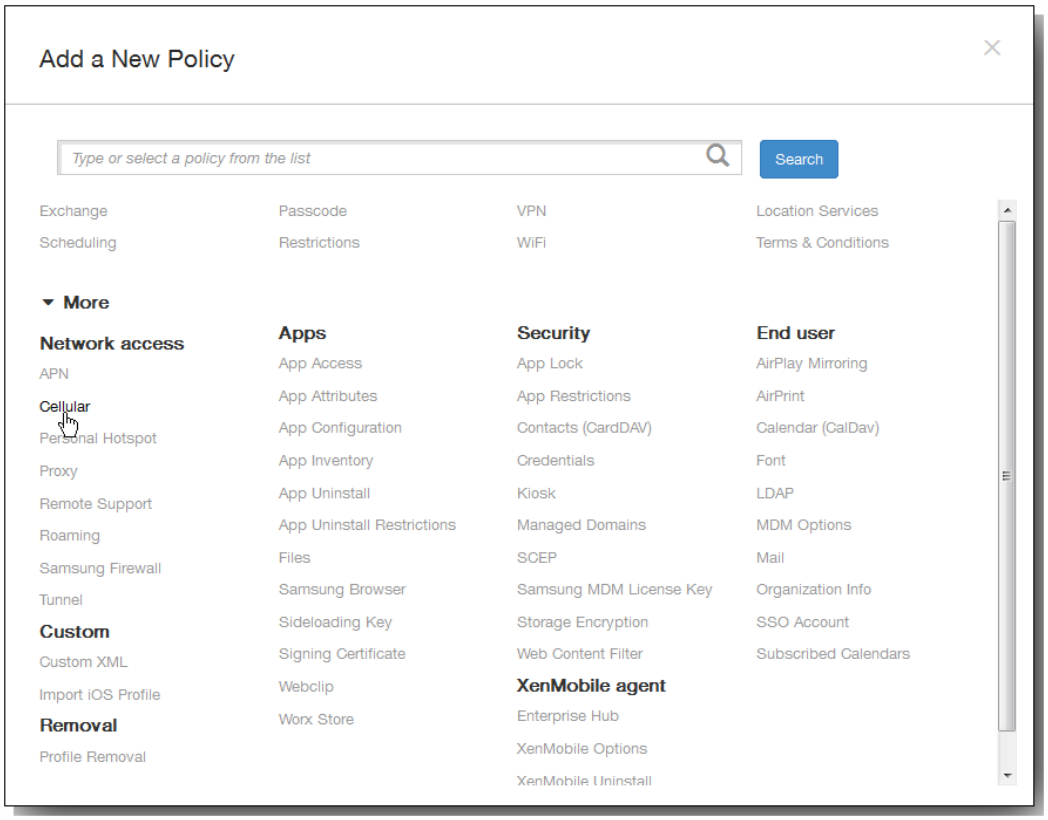
May 06, 2016

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.

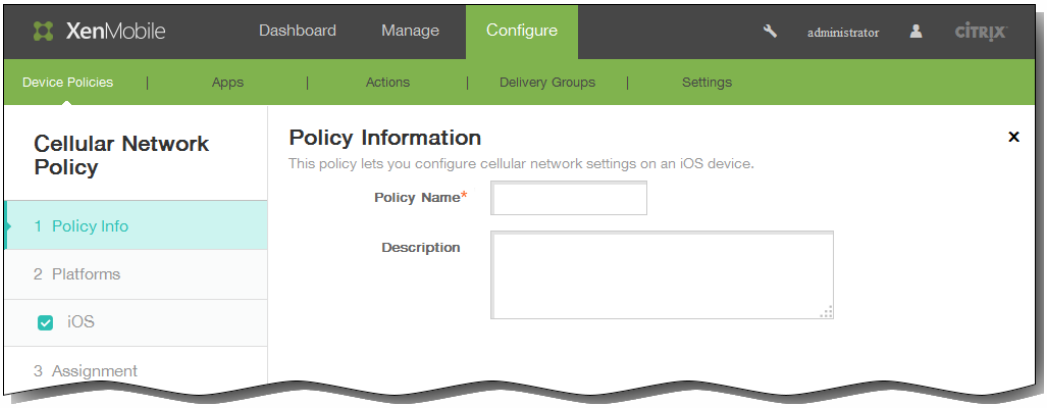


2. Cliquez sur Ajouter.
   La page Ajouter une nouvelle stratégie apparaît.

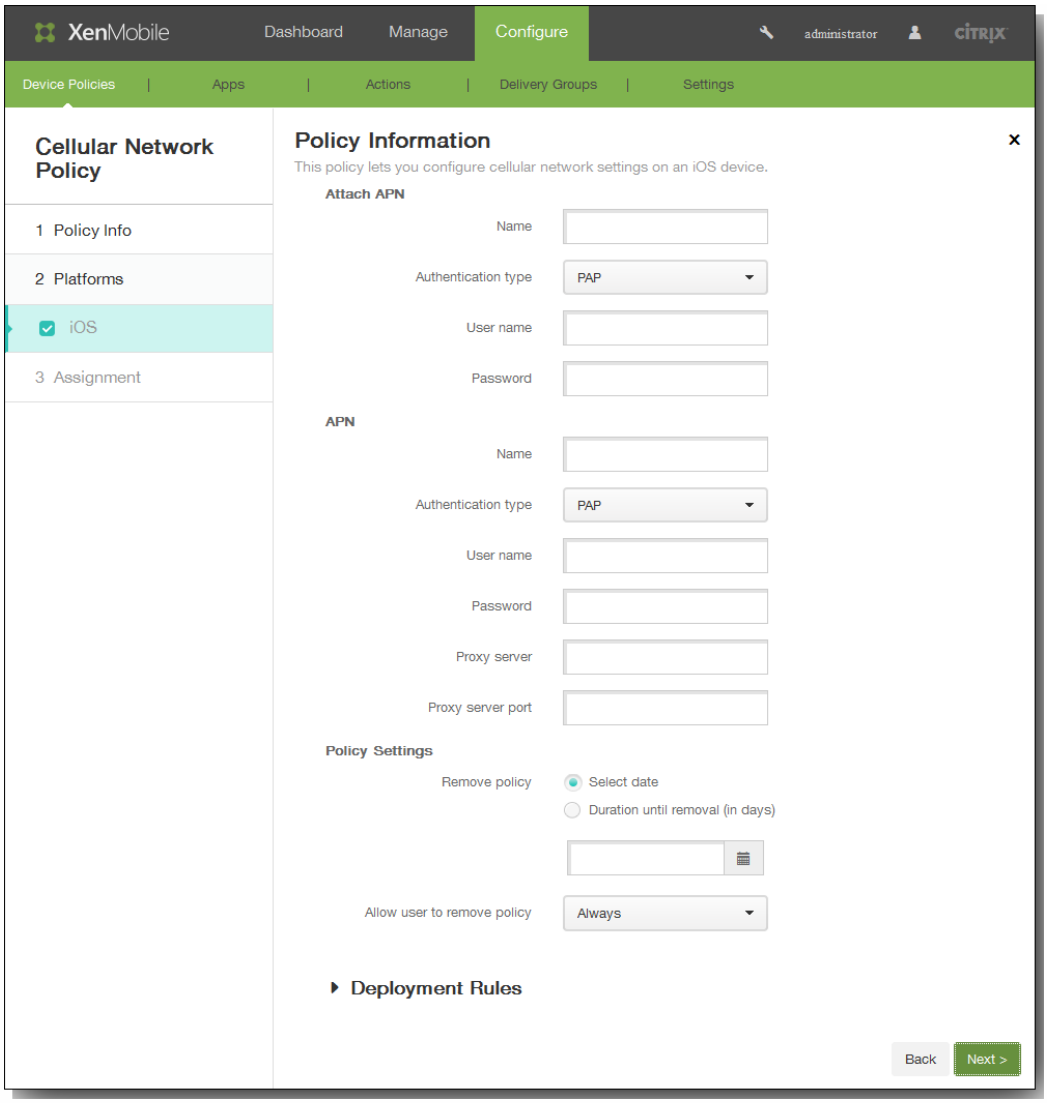


3. Sur la page Ajouter une nouvelle stratégie, cliquez sur Plus puis sous Accès réseau, cliquez sur Cellulaire.

La page d'informations sur la Stratégie de réseau cellulaire s'affiche.



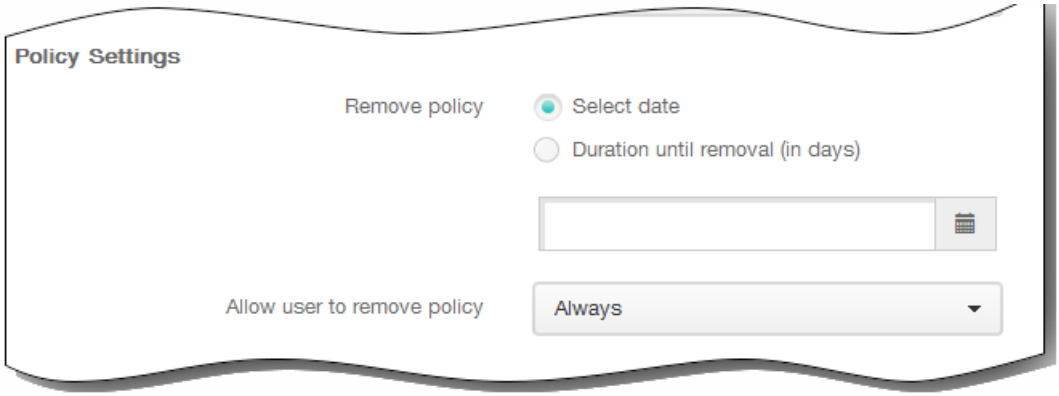
4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.



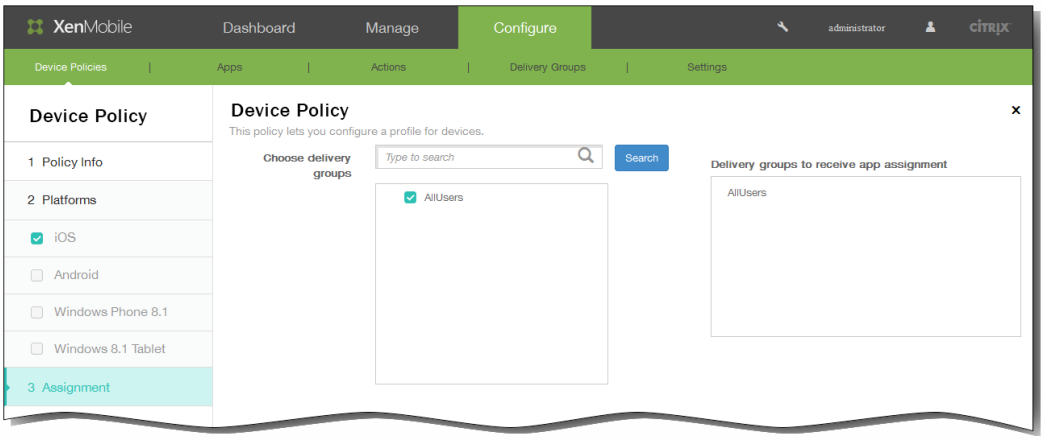
6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes : Sous **Attacher APN** :
   1. Nom : entrez un nom pour cette configuration.
   2. Type d'authentification : dans la liste, cliquez sur CHAP (Challenge Handshake Authentication Protocol) ou PAP (Password Authentication 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.

10. Si vous cliquez sur Mot de passe requis, à côté de Code secret de suppression, entrez le mot de passe requis.

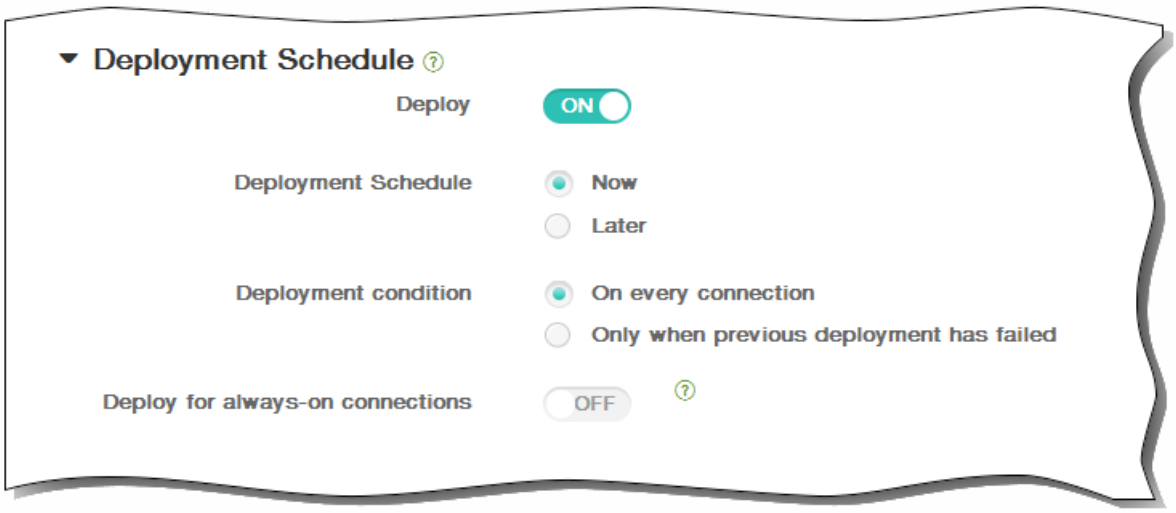


11. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition 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.



13. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour créer une stratégie d'hub d'entreprise pour Windows Phone 8.1

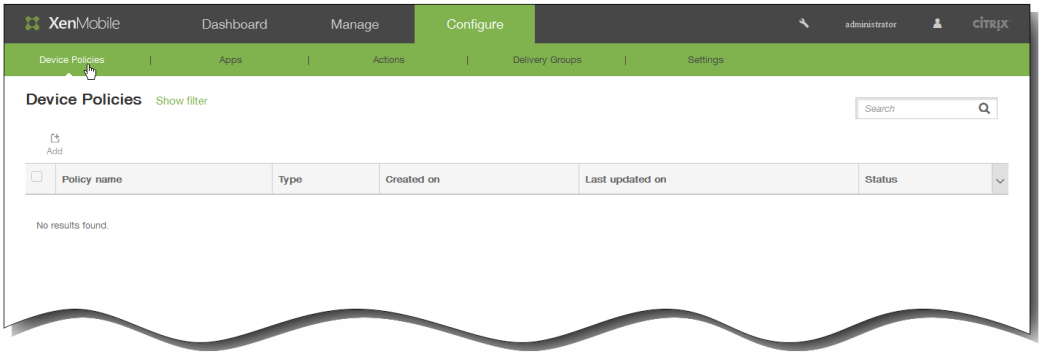
May 06, 2016

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.

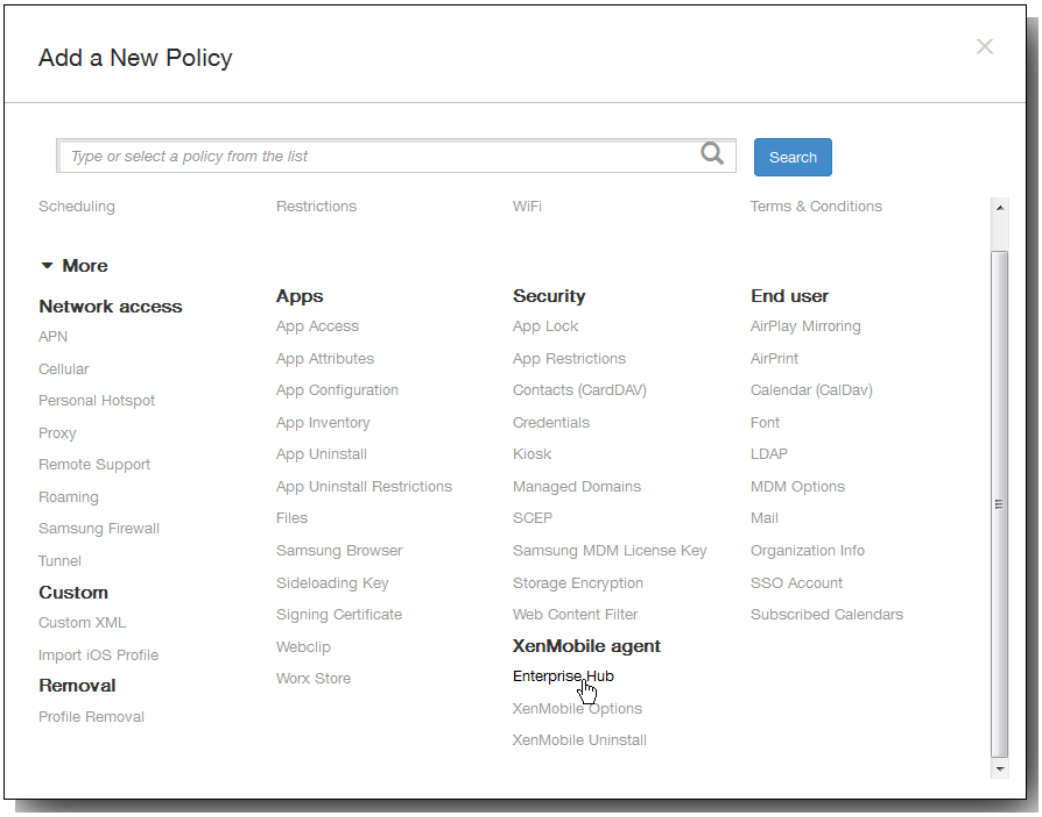
Avant de pouvoir créer la stratégie, vous avez besoin des éléments suivants :

- 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)

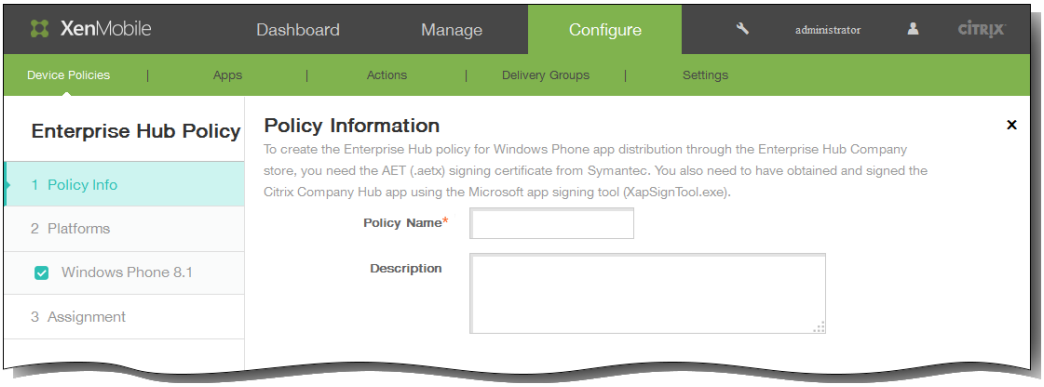
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



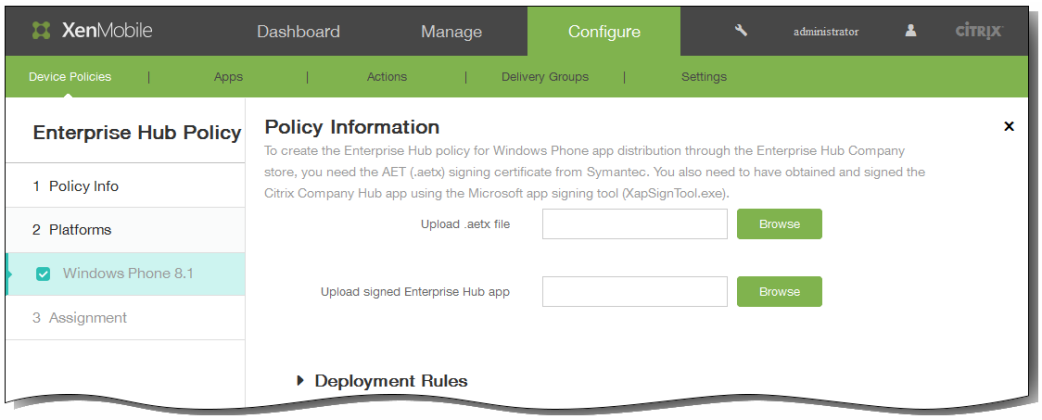
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Agent XenMobile, cliquez sur Hub d'entreprise. La page Stratégie d'hub d'entreprise s'affiche.

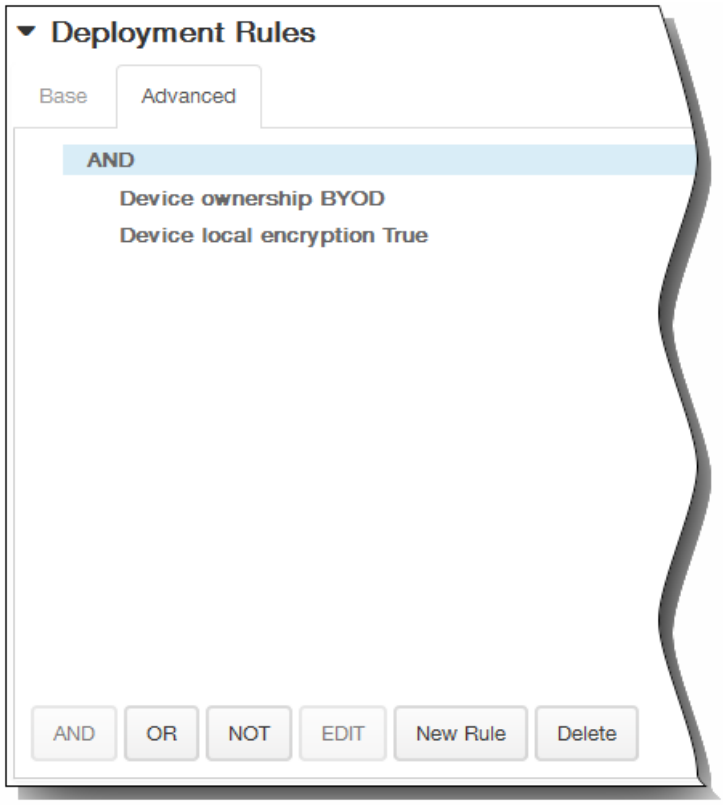


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page de plate-forme Windows Phone 8.1 s'affiche.



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.

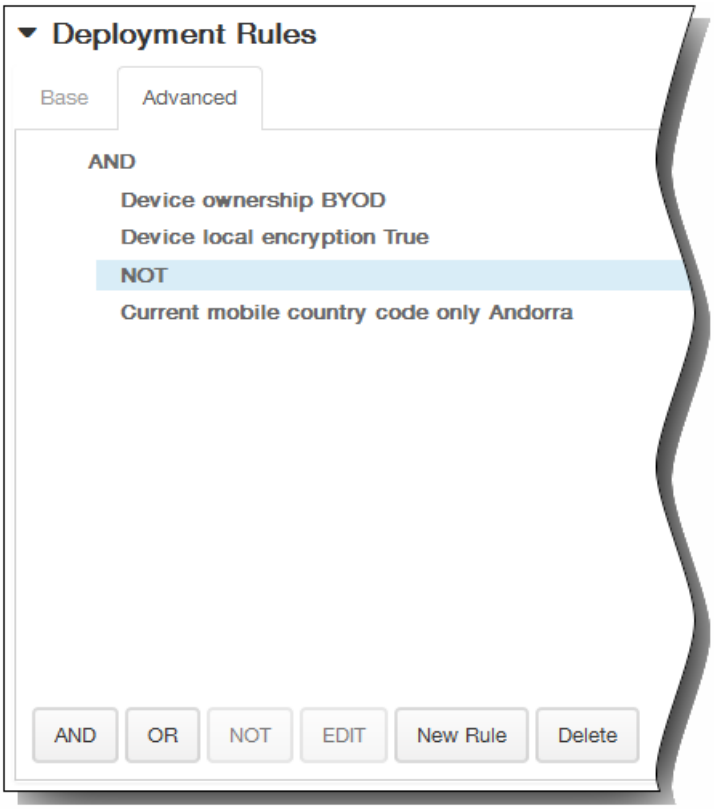
   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour 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.



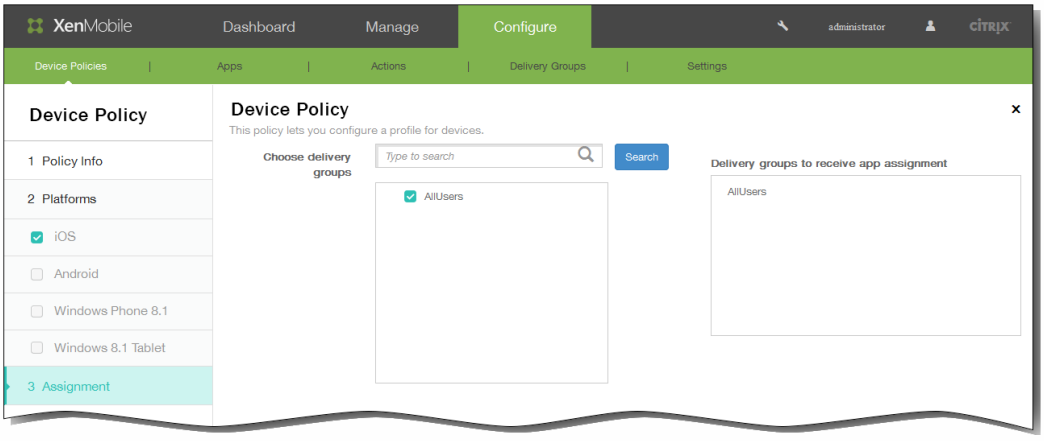
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

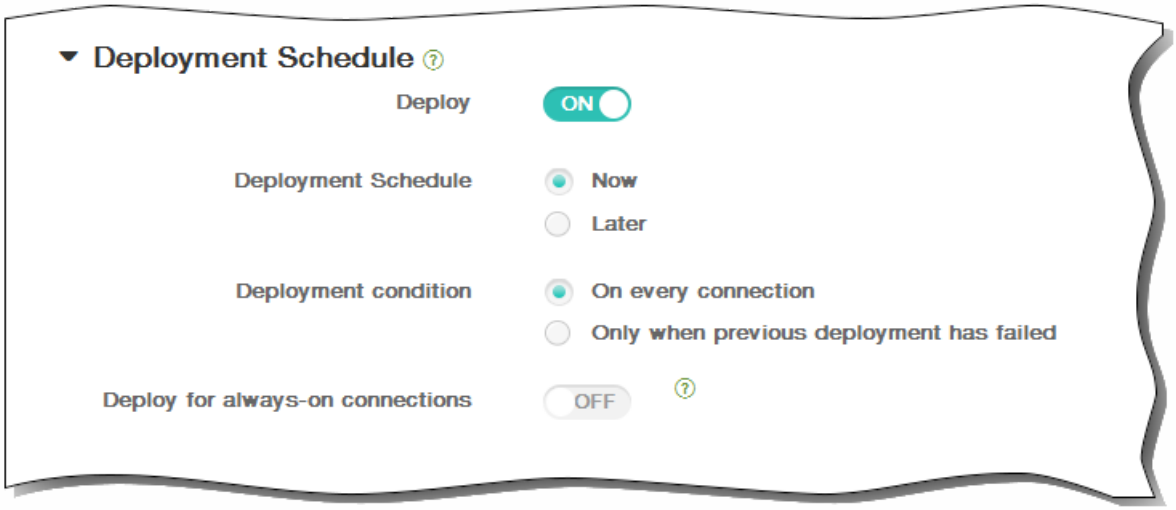


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

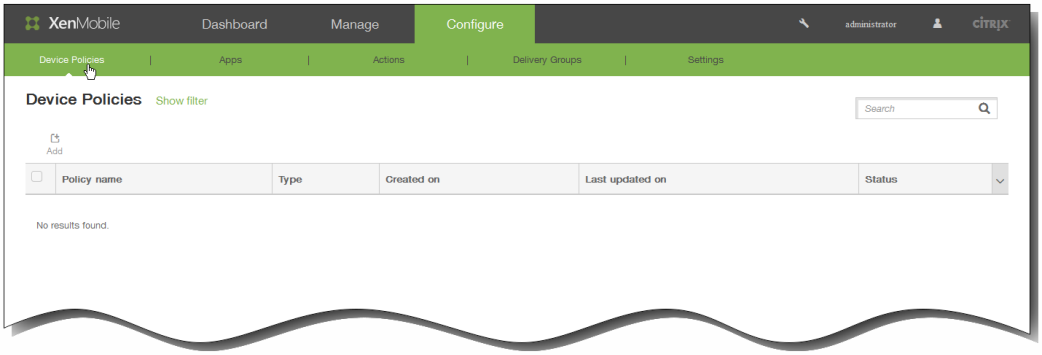
Stratégies Microsoft Exchange ActiveSync

May 06, 2016

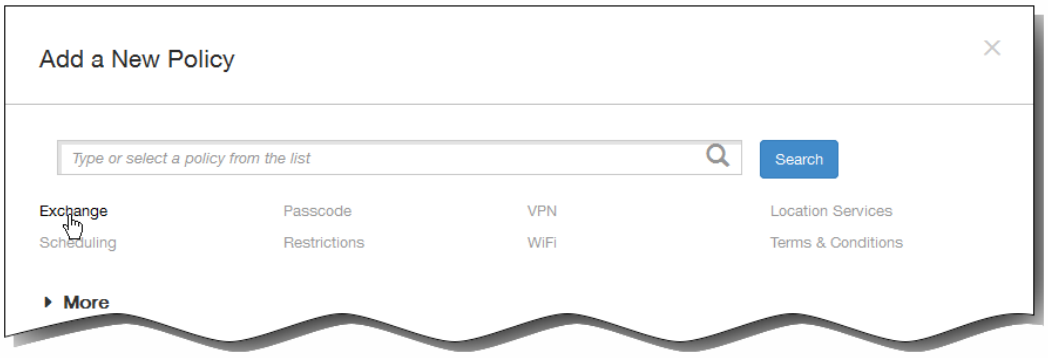
Vous pouvez utiliser la stratégie Exchange ActiveSync pour configurer un client de messagerie sur les appareils des utilisateurs pour leur permettre d'accéder à leur messagerie d'entreprise hébergée sur Exchange. Vous pouvez créer des stratégies pour iOS, Android HTC, Android TouchDown, Samsung SAFE, 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.

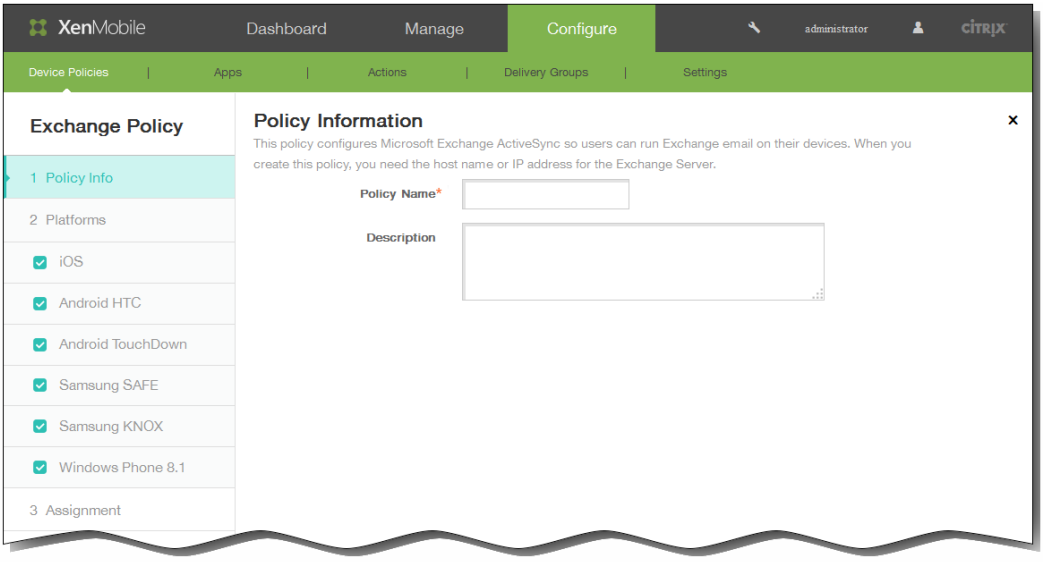
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



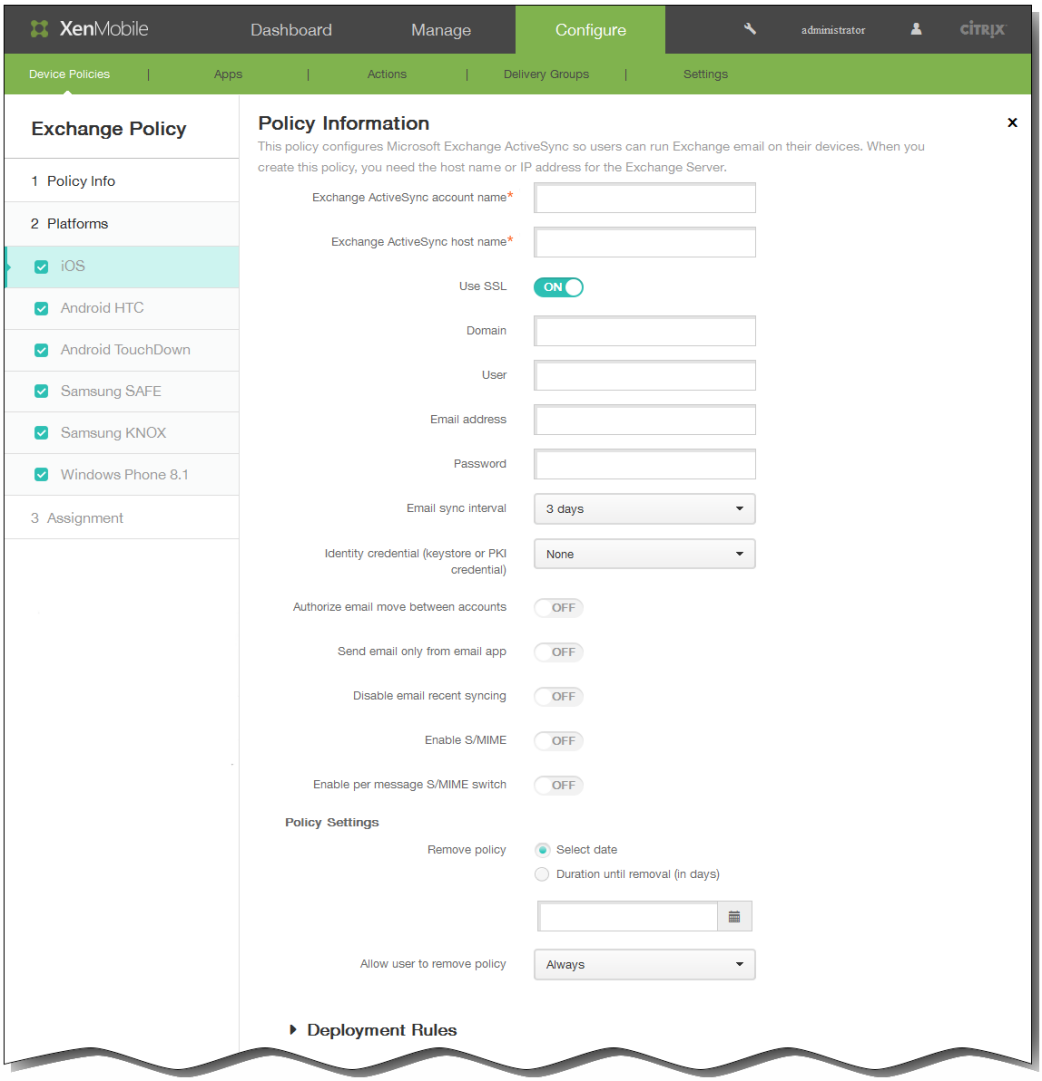
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie s'affiche.



3. Cliquez sur Exchange. La page d'informations Stratégie Exchange s'affiche.



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 :

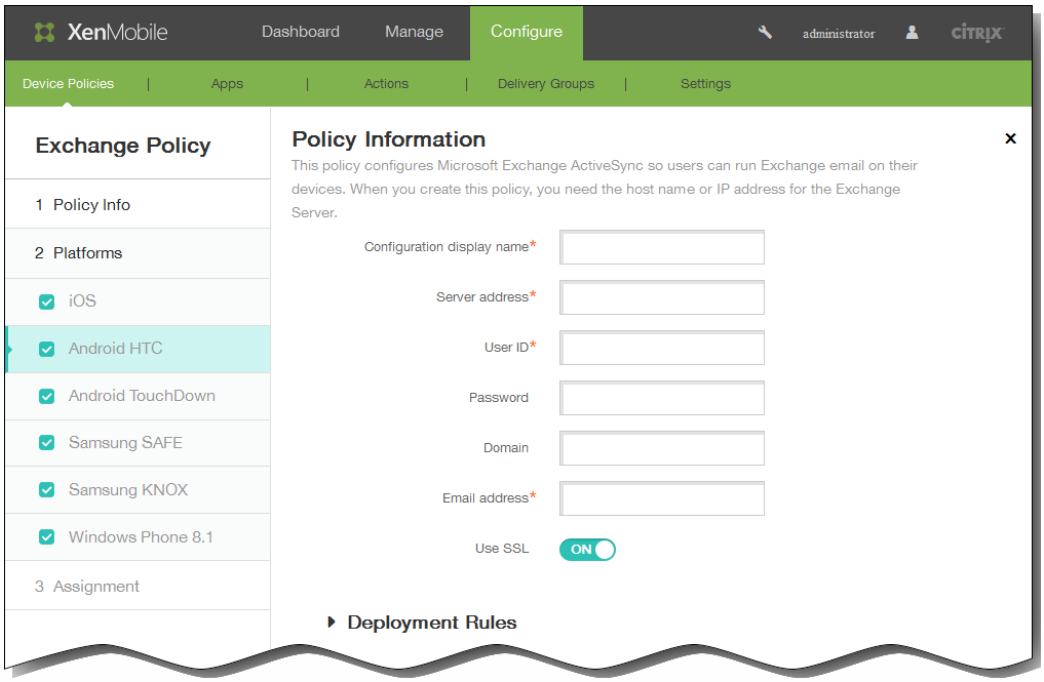
     Nom d'affichage de la configuration : entrez le nom de cette stratégie qui s'affiche sur les appareils des utilisateurs.

     Adresse du serveur : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.

     ID utilisateur : spécifiez le nom d'utilisateur du compte utilisateur Exchange.
     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 HTC, configurez les paramètres suivants :



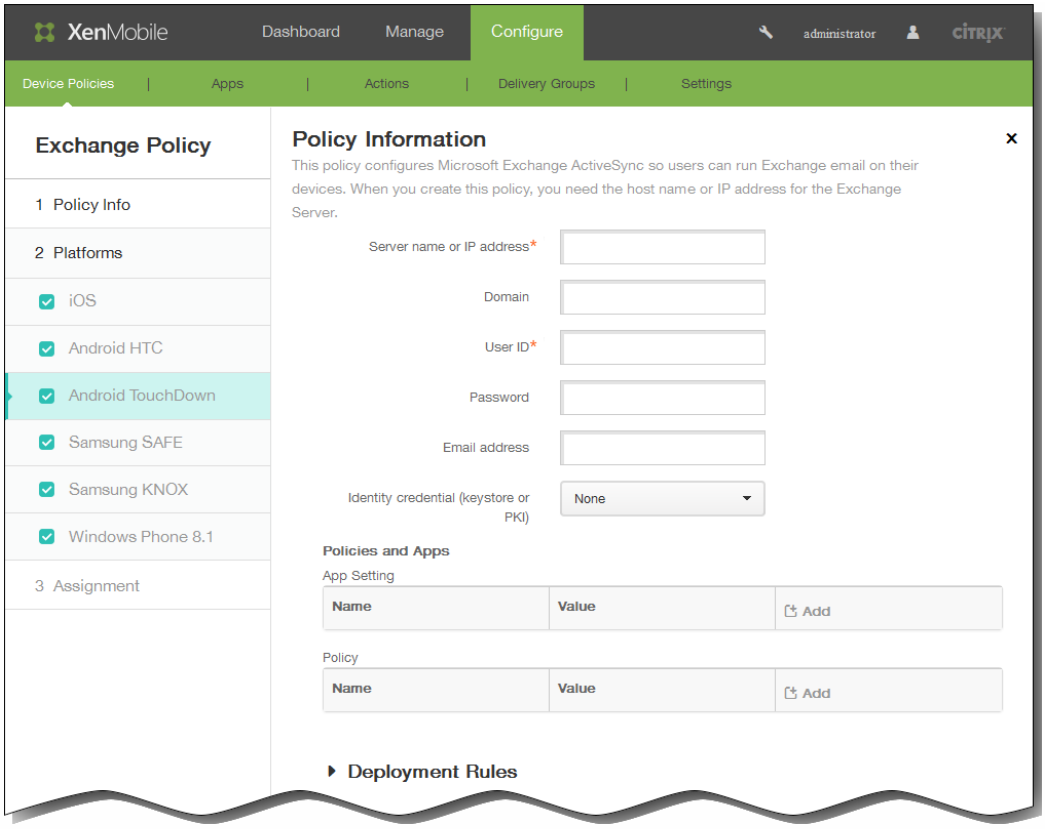
Nom d'affichage de la configuration : entrez le nom de cette stratégie qui s'affiche sur les appareils des utilisateurs.

Adresse du serveur : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.

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 : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.

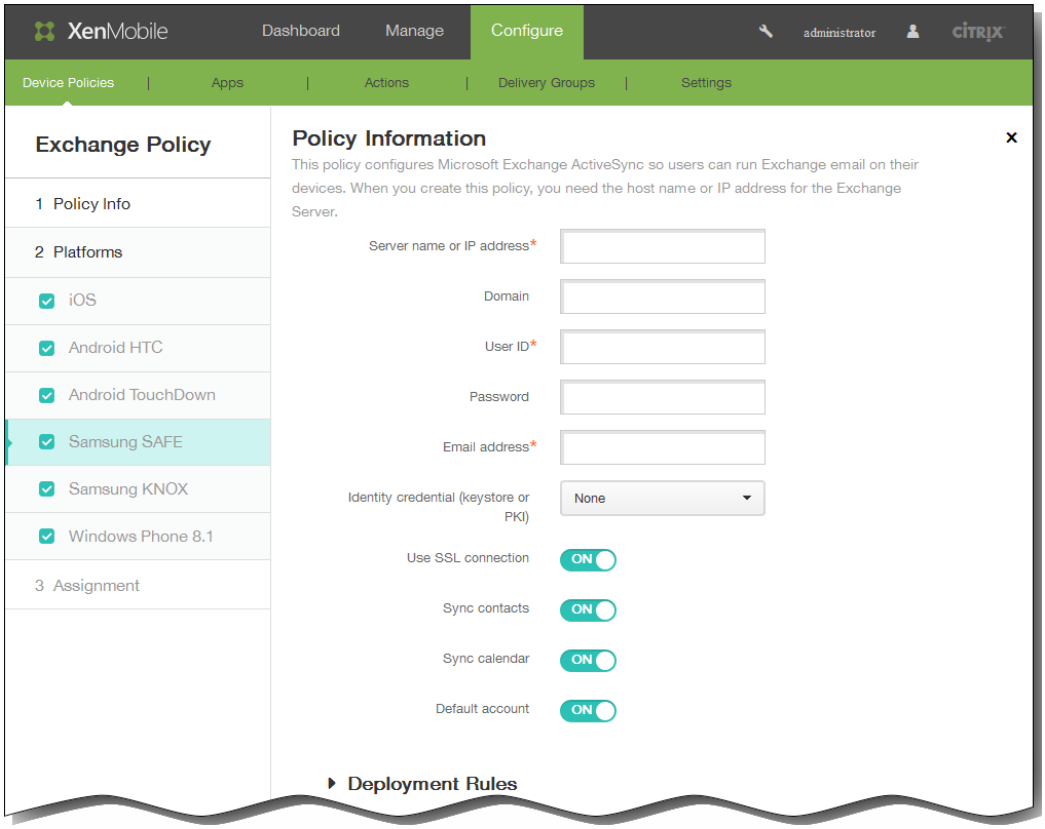
Domaine : entrez le domaine dans lequel réside le serveur Exchange.
Remarque : vous pouvez utiliser la macro système ${user.domainname} dans ce champ pour rechercher automatiquement les noms de domaines des utilisateurs.
ID utilisateur : spécifiez le nom d'utilisateur du compte utilisateur Exchange.
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.
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.

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 sélectionnez Samsung SAFE ou Samsung KNOX, configurez les paramètres suivants :



Nom du serveur ou adresse IP : entrez le nom d'hôte ou l'adresse IP du serveur Exchange.

Domaine : entrez le domaine dans lequel réside le serveur Exchange.
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.
Infos d'identification de l'identité (PKI ou keystore) : dans la liste, cliquez sur des informations d'identification de l'identité si vous avez configuré un fournisseur d'identités pour XenMobile. Ce champ est requis uniquement lorsque Exchange requiert l'authentification du certificat client.

Utiliser une connexion SSL : sélectionnez cette option pour sécuriser les connexions entre les appareils des utilisateurs et le serveur Exchange. La valeur par défaut est On.

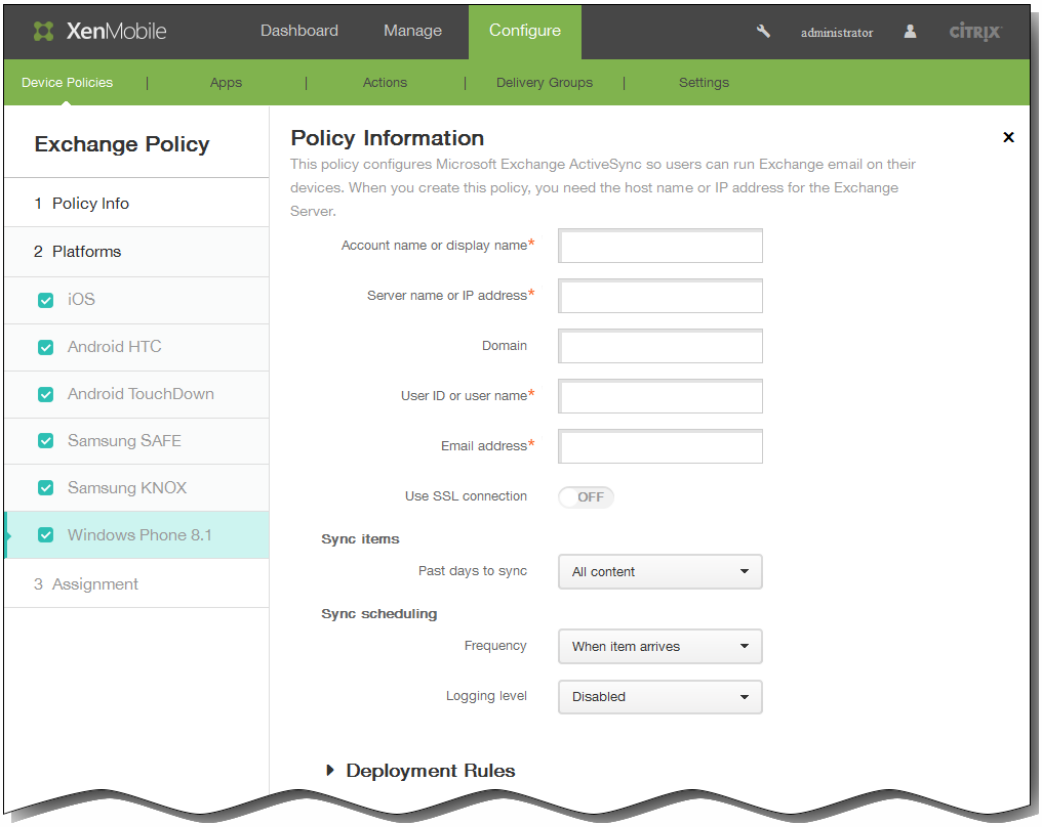
Synchroniser les contacts : sélectionnez cette option pour activer la synchronisation des contacts des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est On.

Synchroniser le calendrier : sélectionnez cette option pour activer la synchronisation des calendriers des utilisateurs entre leurs appareils et le serveur Exchange. La valeur par défaut est On.

Compte par défaut : sélectionnez cette option pour faire du compte Exchange des utilisateurs le compte par défaut pour l'envoi de courrier électronique à partir de leurs appareils. La valeur par défaut est On.

- 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 : entrez le nom d'hôte ou l'adresse IP du serveur 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.
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

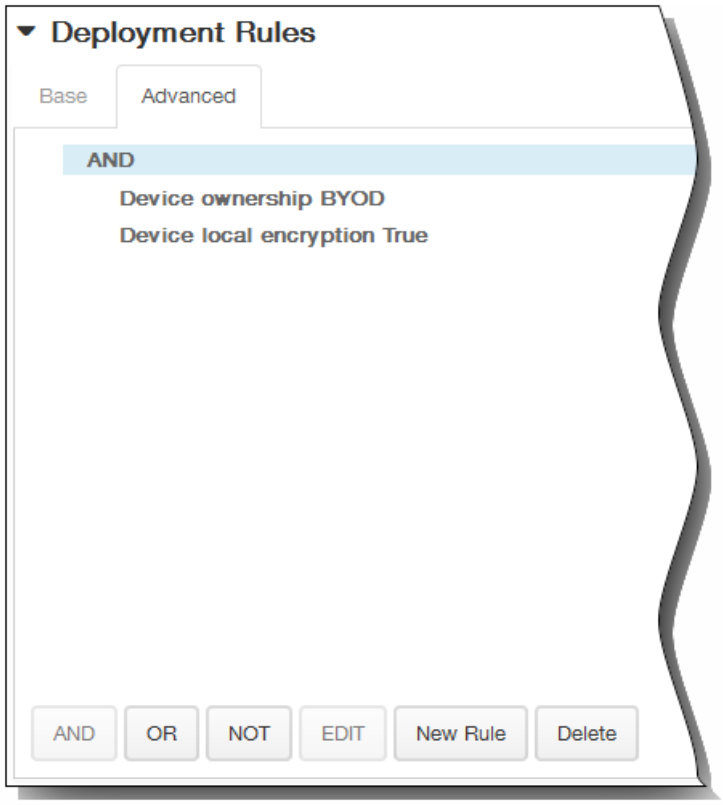
contenu de l'appareil avec le serveur Exchange.

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.

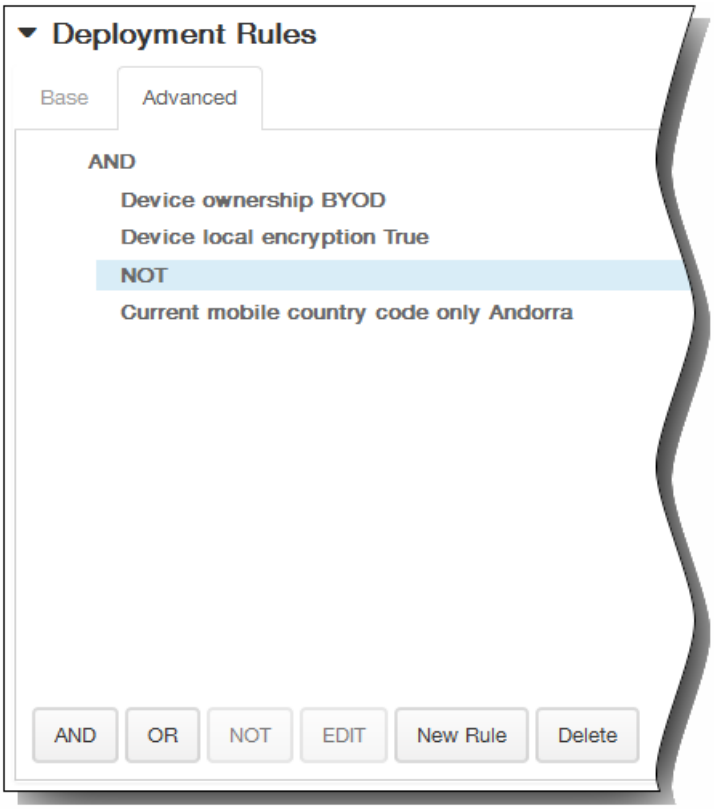
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



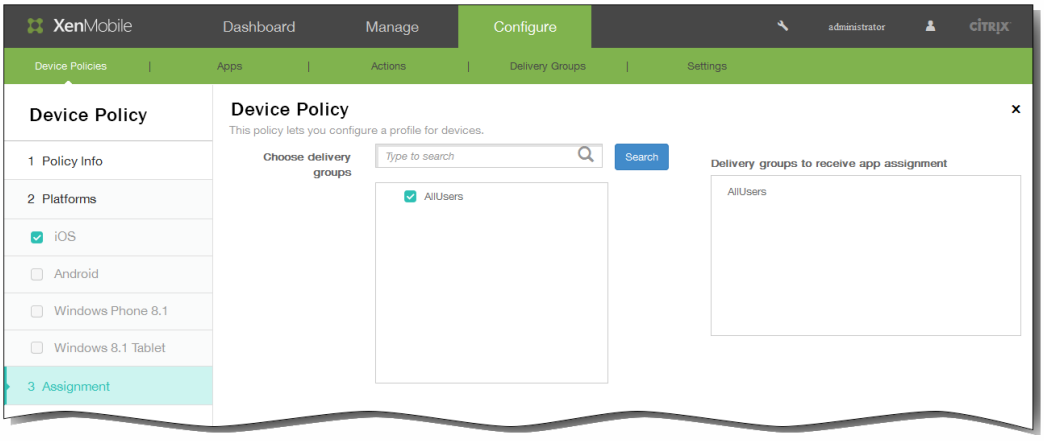
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

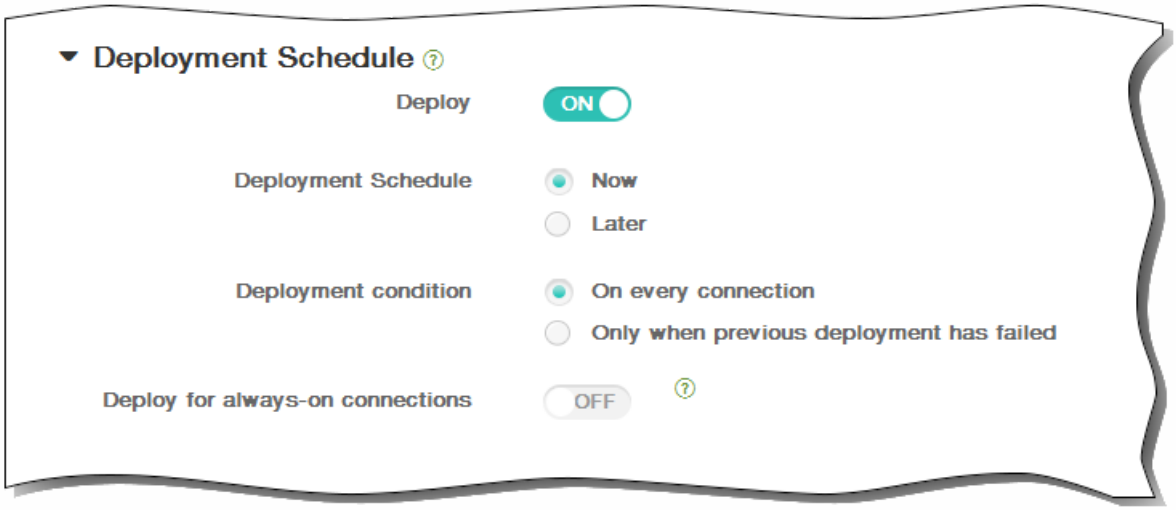


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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 Save.

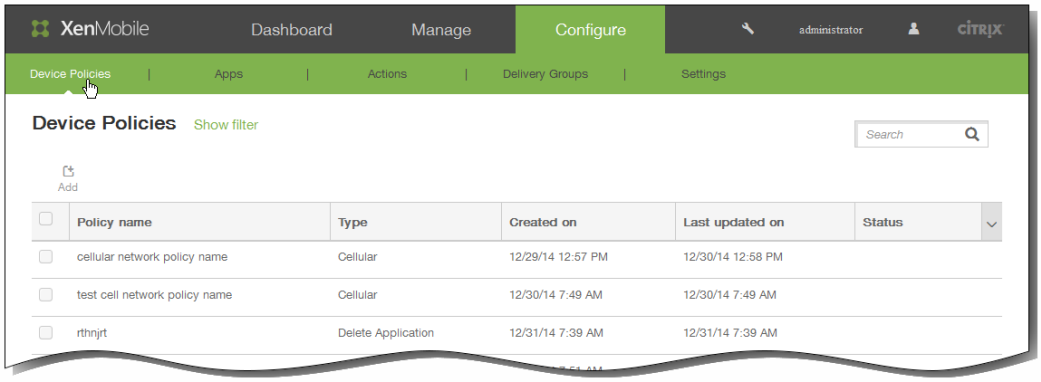
Stratégies d'emplacement

May 06, 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.

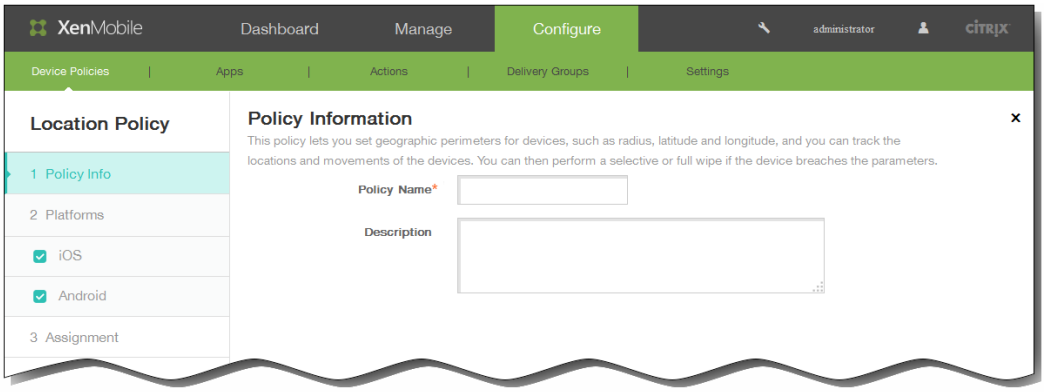
Vous pouvez créer des stratégies d'emplacement pour iOS et Android. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

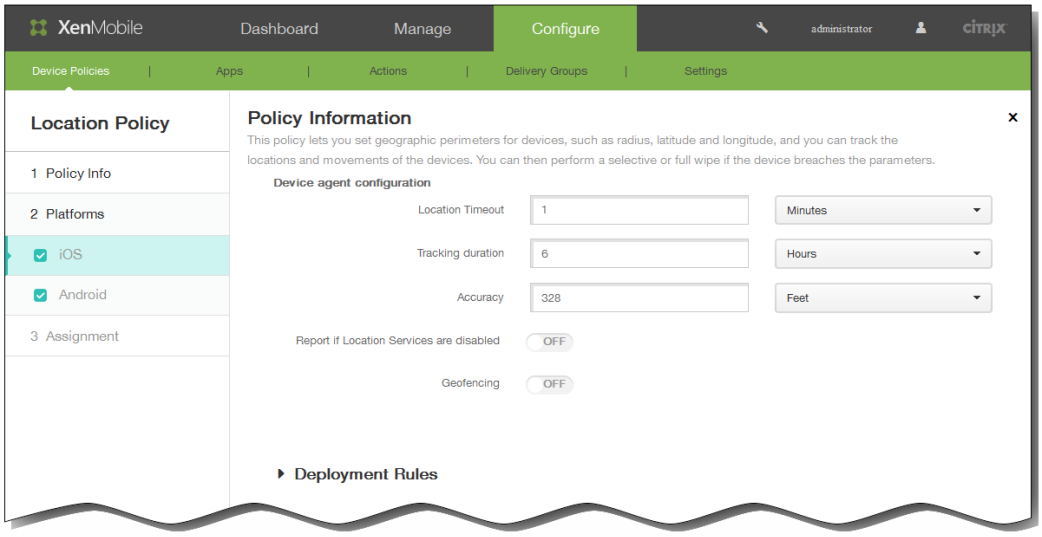


2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

3. Cliquez sur Services de localisation. La page d'informations Stratégie d'emplacement s'affiche.



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.



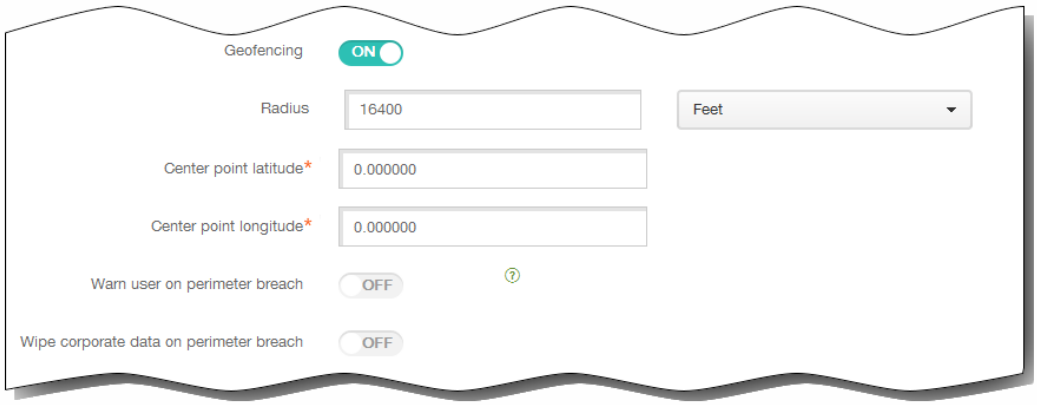
6. Sous Plates-formes, sélectionnez les plates-formes que vous souhaitez ajouter.
   - Si vous sélectionnez iOS, configurez les paramètres suivants :
     Délai max. de localisation : entrez un chiffre, puis, dans la liste, cliquez sur Secondes ou Minutes pour définir la fréquence à laquelle XenMobile 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.

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 :



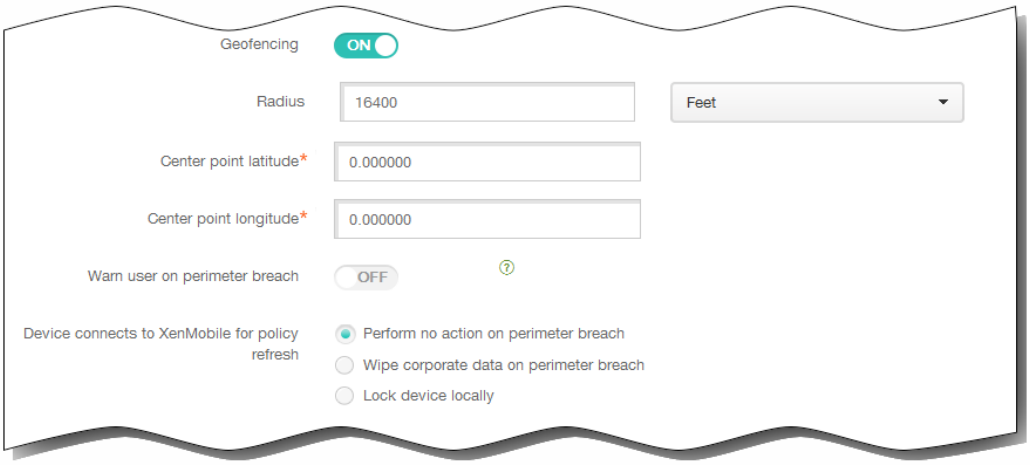
- Rayon : entrez un chiffre, puis, dans la liste, cliquez sur les unités à utiliser pour mesurer le rayon. La valeur par défaut est 16 400 feet.
  Les valeurs valides pour le rayon sont :
  - 164–164000 feet
  - 1–50 kilomètres
  - 50–50000 mètres
  - 54–54680 yards
  - 1–31 miles
- Latitude du point 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

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

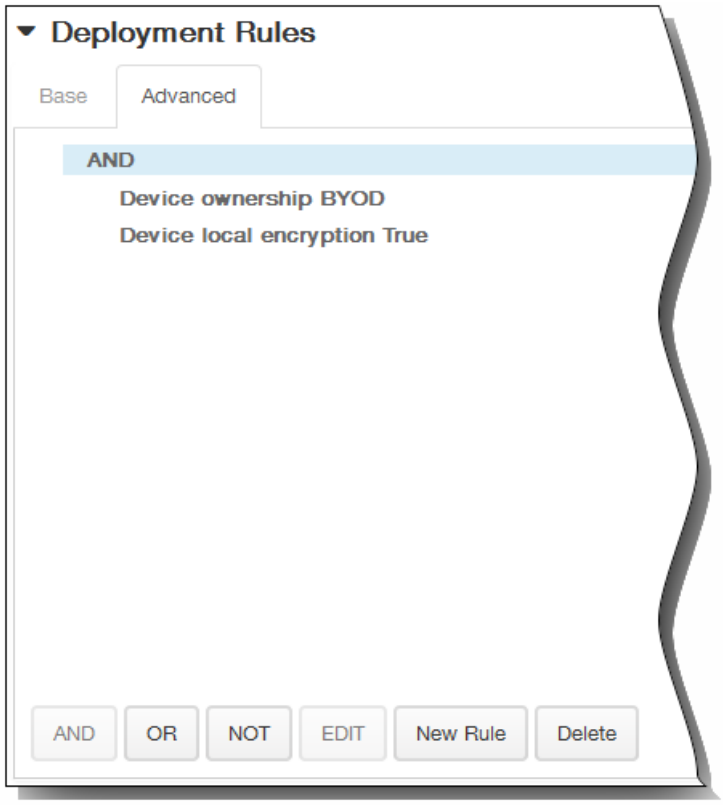
0 secondes.

- 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.

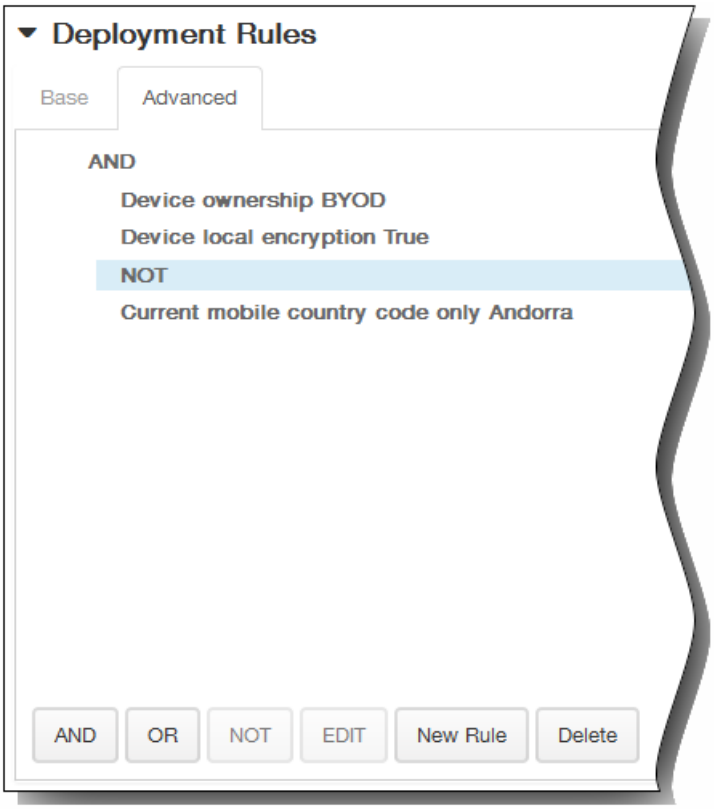
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



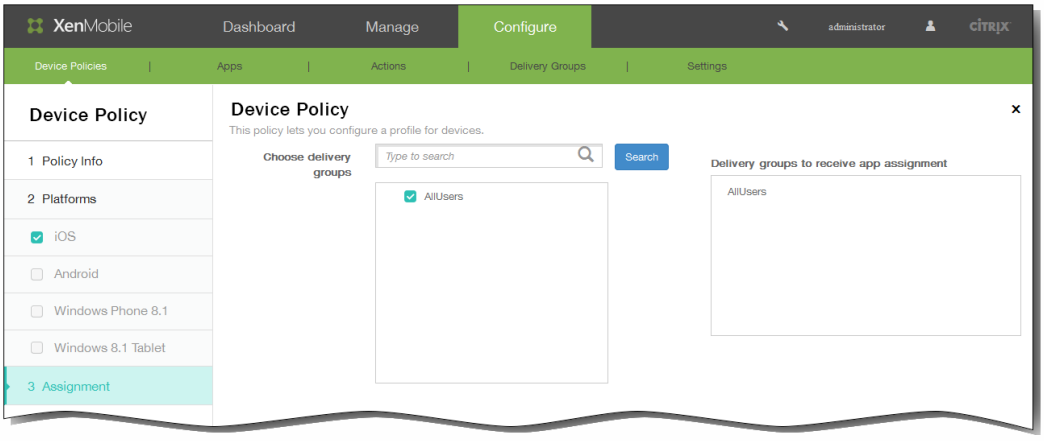
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

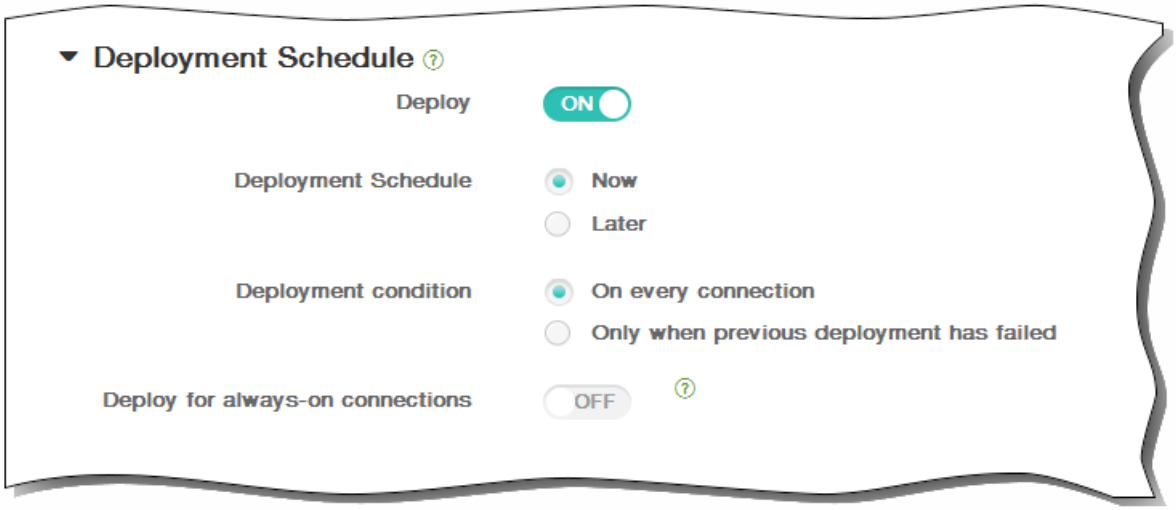


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.



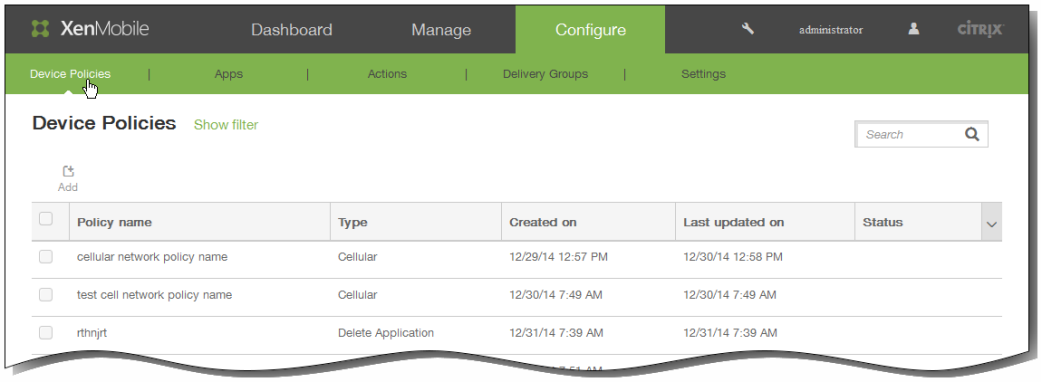
11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de planification de connexion

May 06, 2016

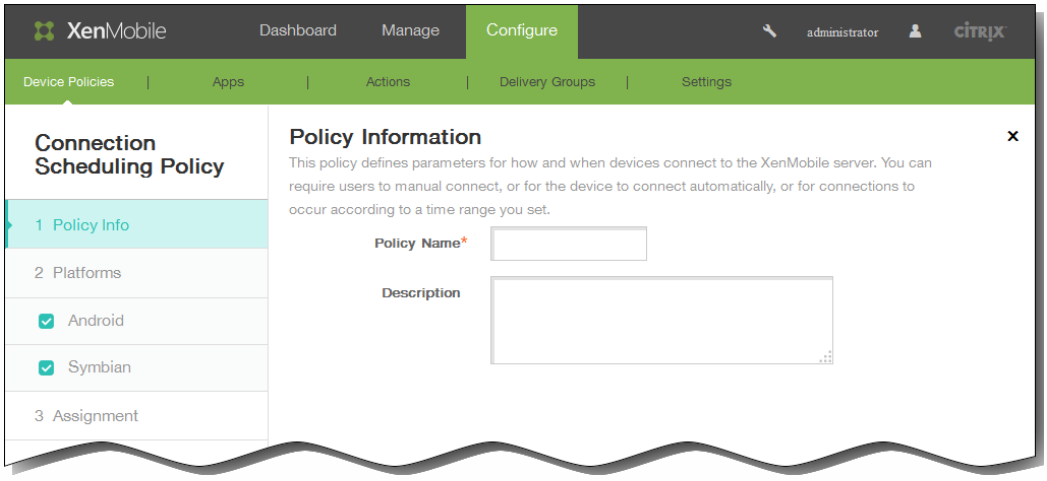
Vous pouvez créer des stratégies de planification de connexion afin de contrôler comment et quand les appareils Android et Symbian se connectent à XenMobile. Vous pouvez spécifier que les utilisateurs connectent leurs appareils manuellement, que les appareils restent connectés de manière permanente, 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.
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.

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.

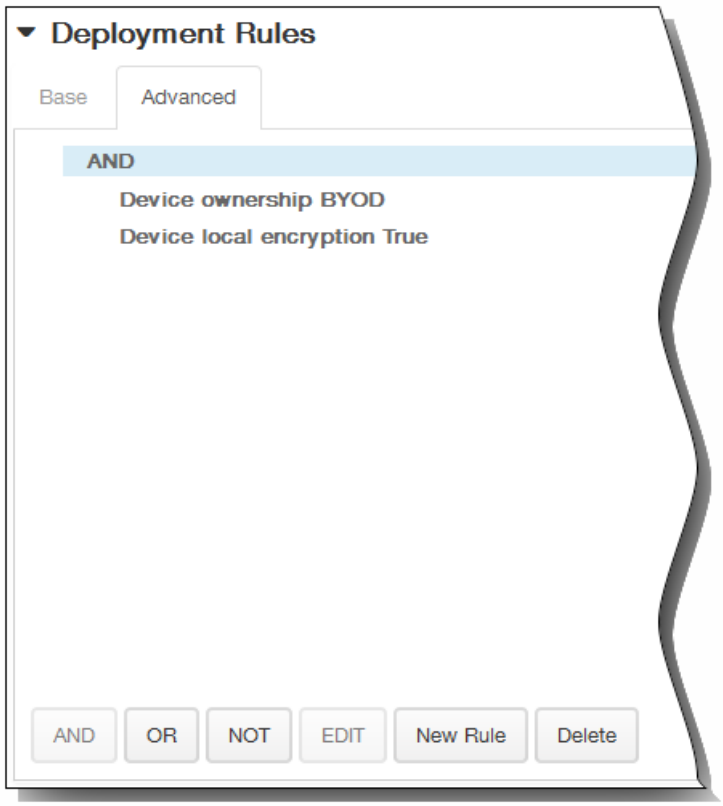
Utiliser l'heure locale de l'appareil comme référence et non l'heure UTC : synchronise les intervalles définis avec l'appareil local plutôt que le temps universel coordonné (UTC).

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.

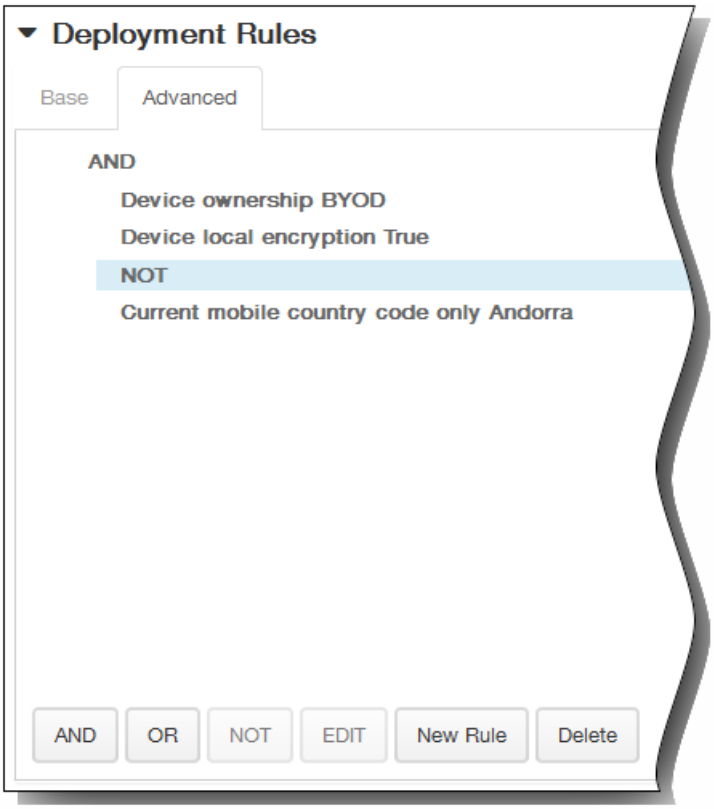
1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme 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.

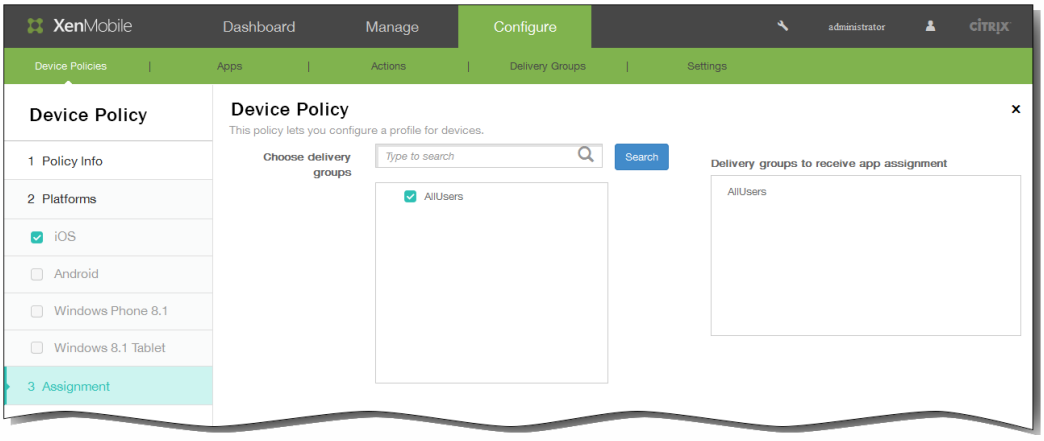


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

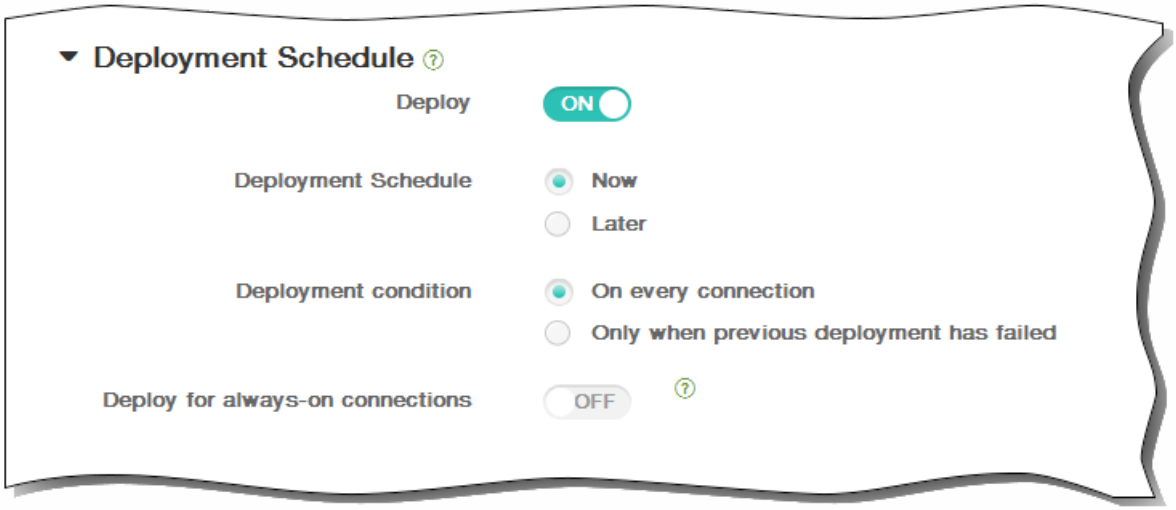


11. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.



12. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de mise en miroir AirPlay pour iOS

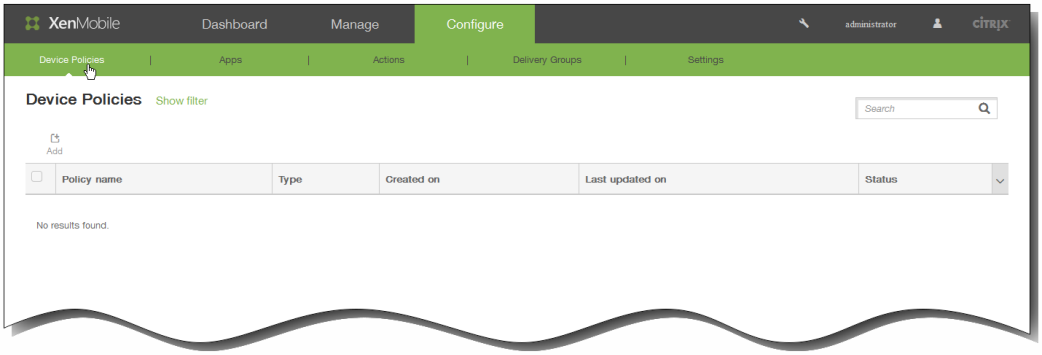
May 06, 2016

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.

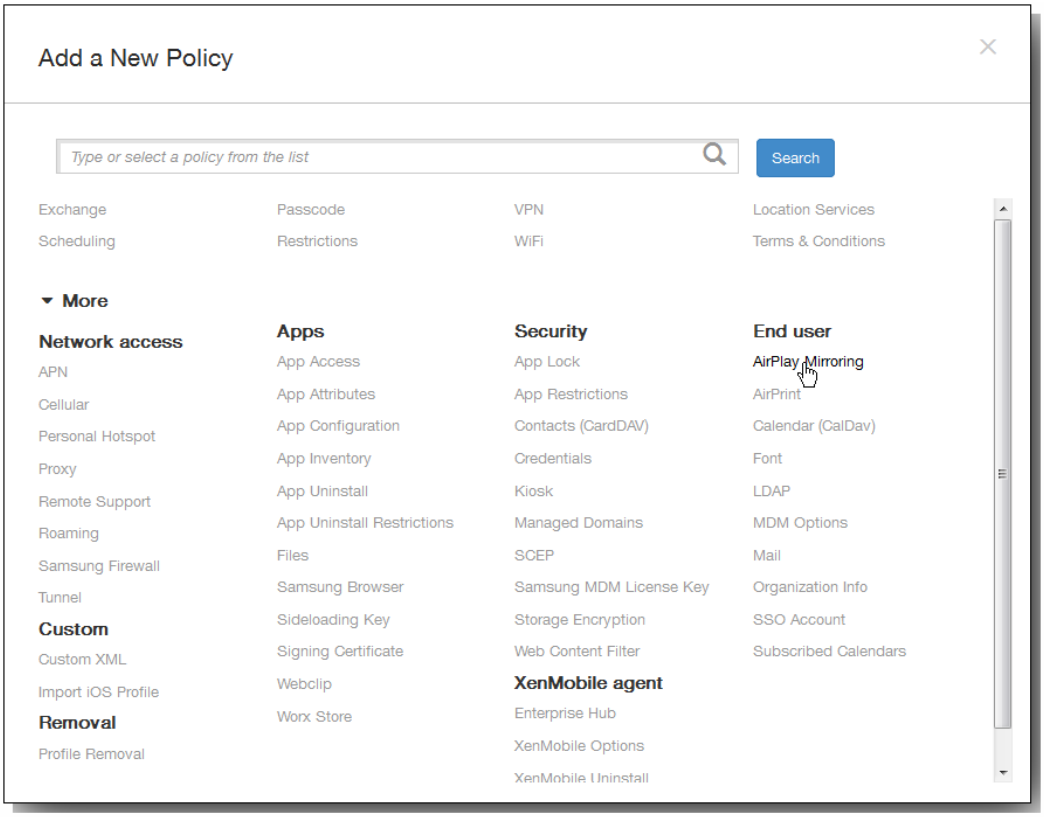
Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter des appareils AirPlay spécifiques (tels que Apple TV ou un autre ordinateur Mac) aux appareils iOS des utilisateurs. Vous avez aussi la possibilité d'ajouter des appareils à une liste blanche d'appareils supervisés, ce qui limite 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.

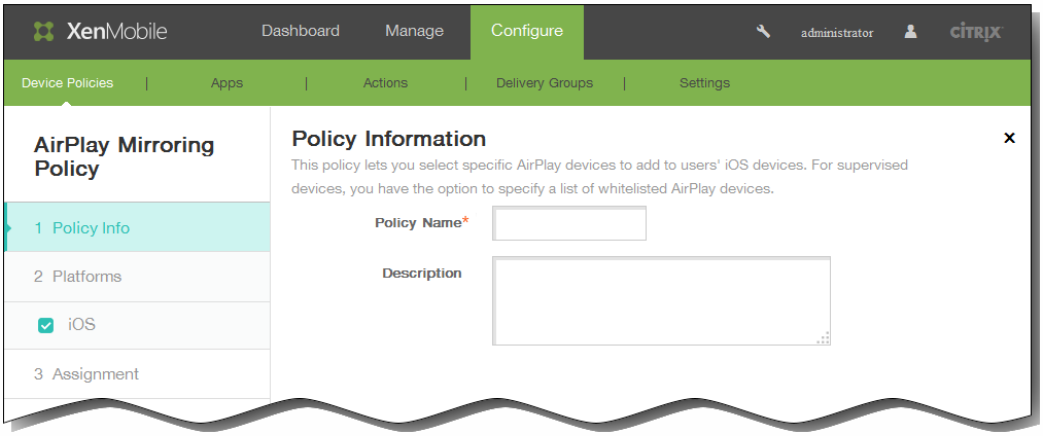
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



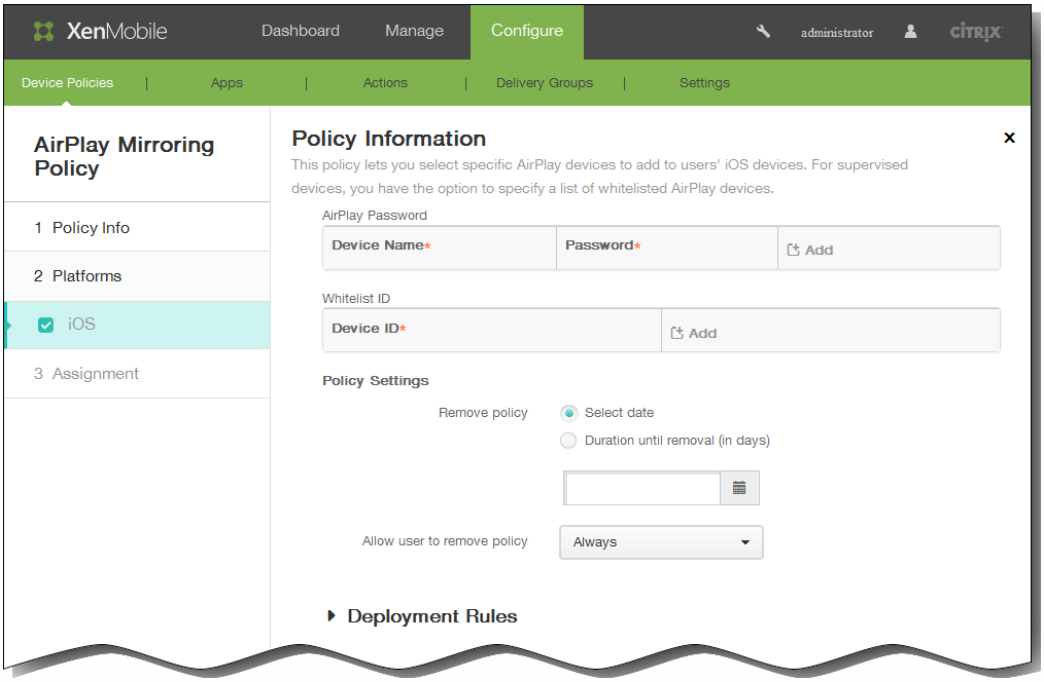
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



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.

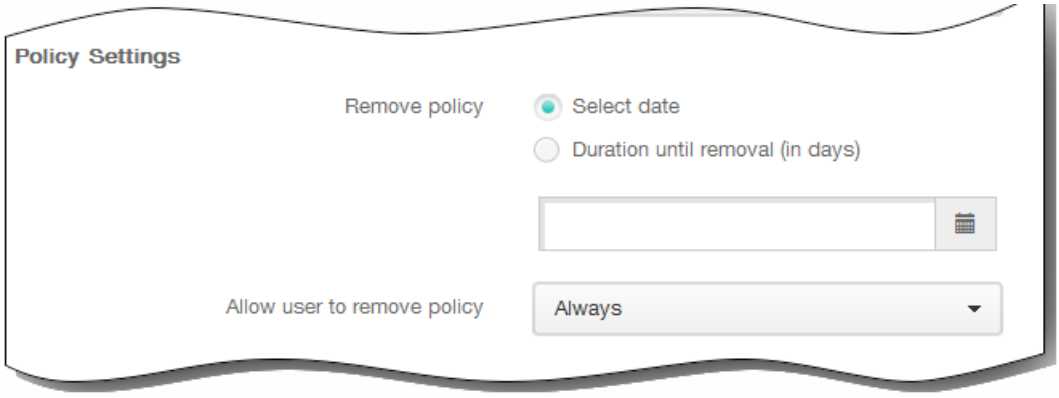


6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Mot de passe AirPlay : cliquez sur Ajouter et procédez comme suit :
      1. ID de l'appareil : entrez l'ID de l'appareil au format xx:xx:xx:xx:xx:xx. Ce champ n'est pas sensible à la casse.
      2. Mot de 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.

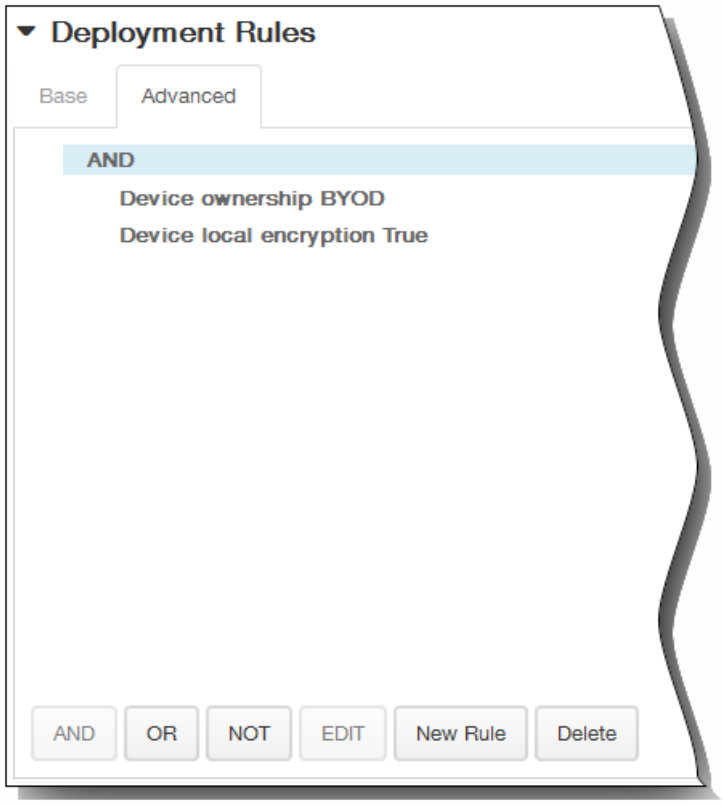
      Pour modifier un appareil existant, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de crayon sur le côté droit. Effectuez toutes les modifications nécessaires à la liste, puis cliquez sur Enregistrer pour enregistrer la nouvelle liste ou sur Annuler pour laisser la liste inchangée.

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.



11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

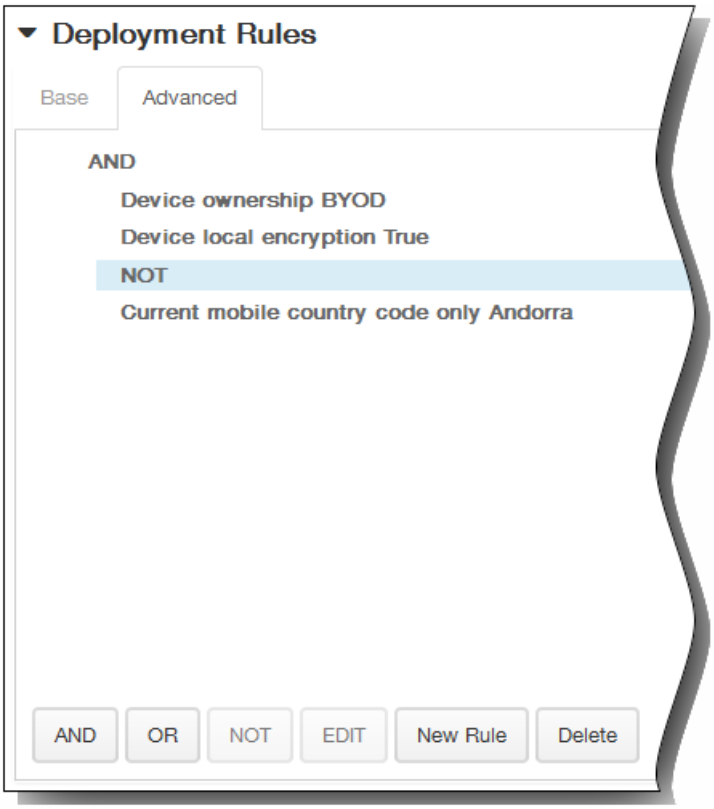
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



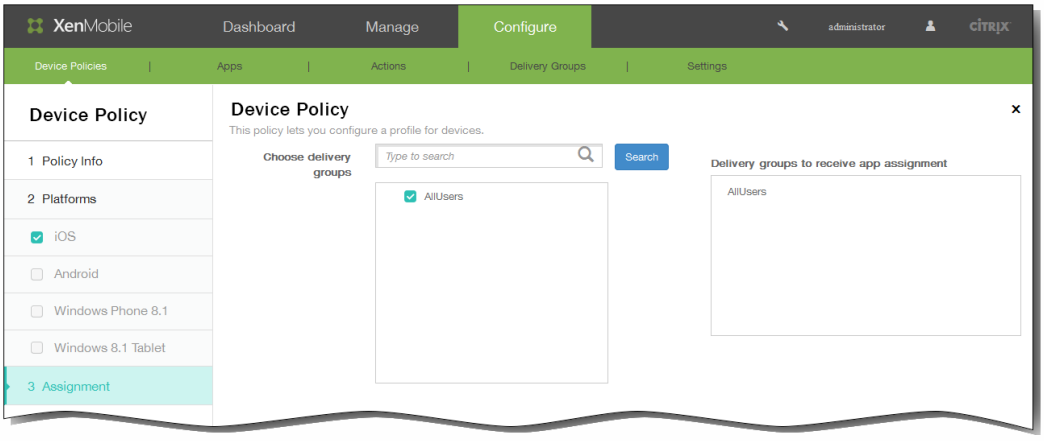
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

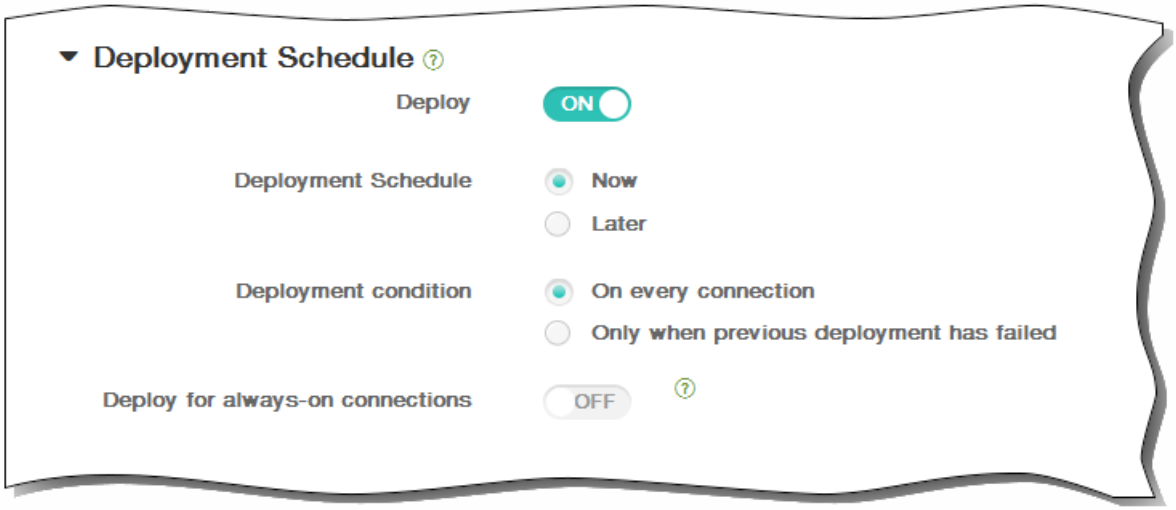


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

Pour ajouter une stratégie AirPrint pour iOS

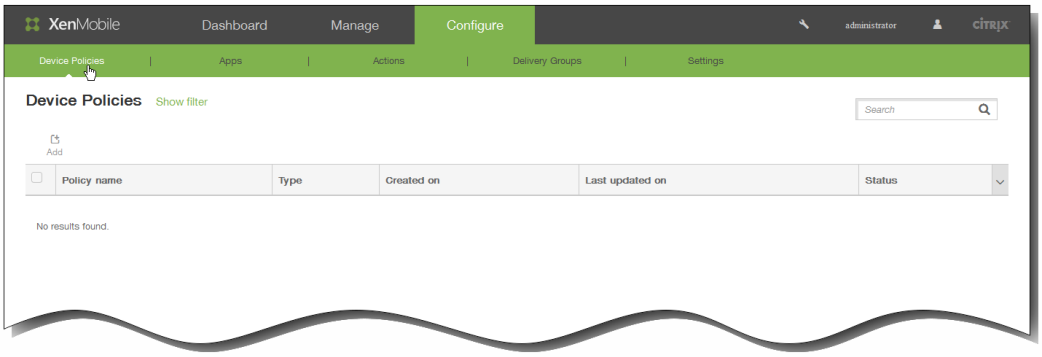
May 06, 2016

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.

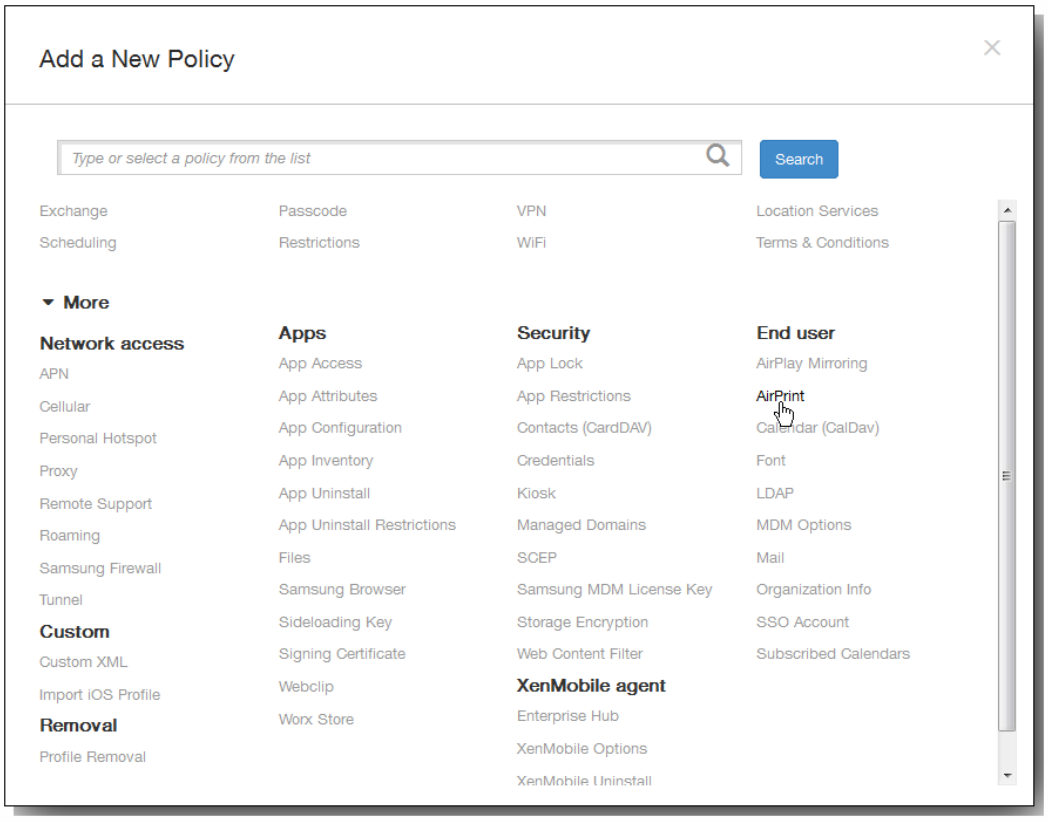
Remarque :

- 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.

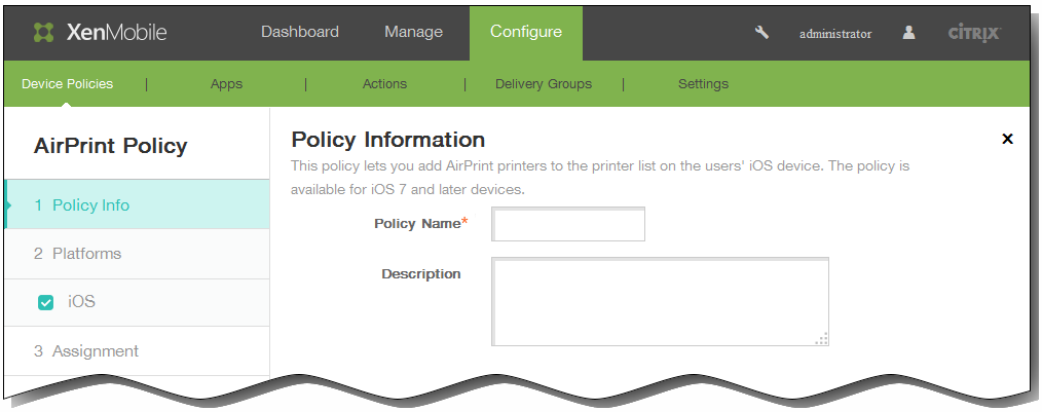
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



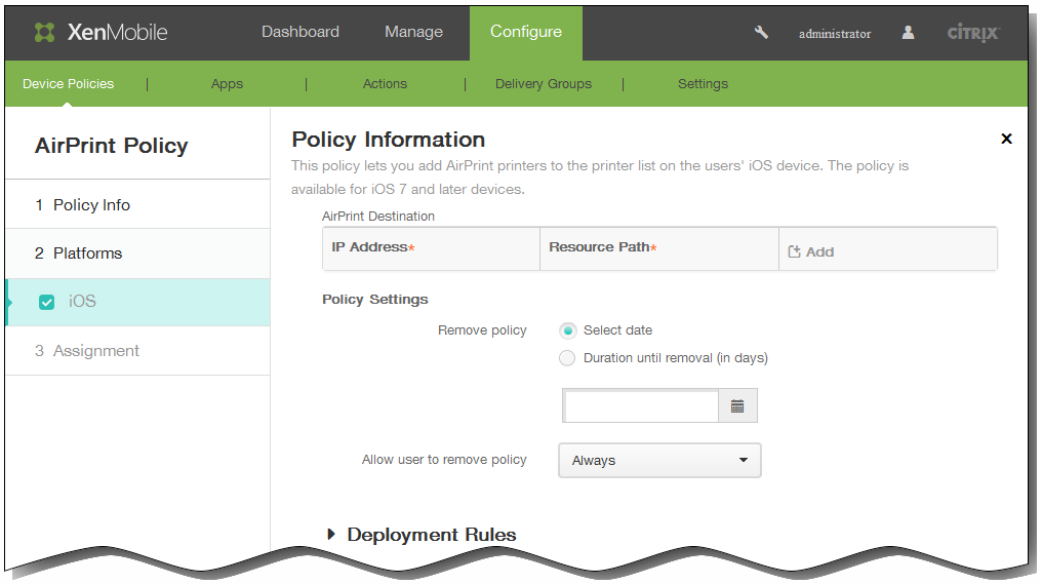
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur AirPrint. La page Stratégie AirPrint s'affiche.



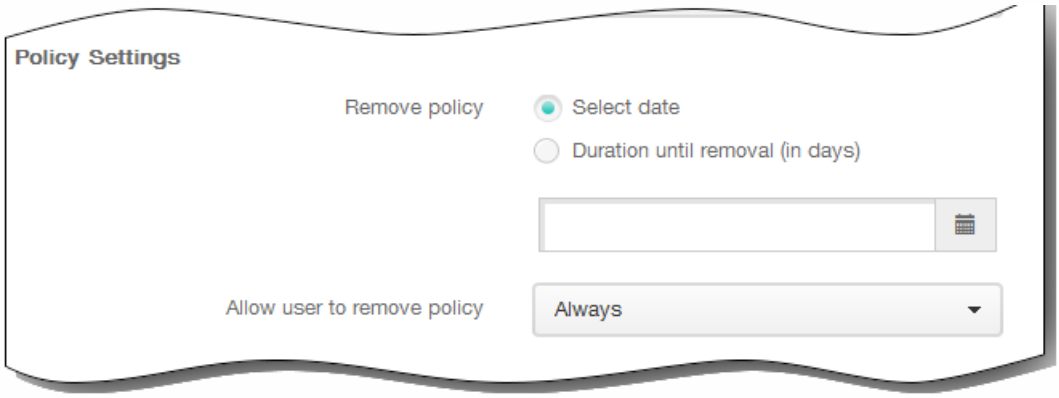
4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS 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.

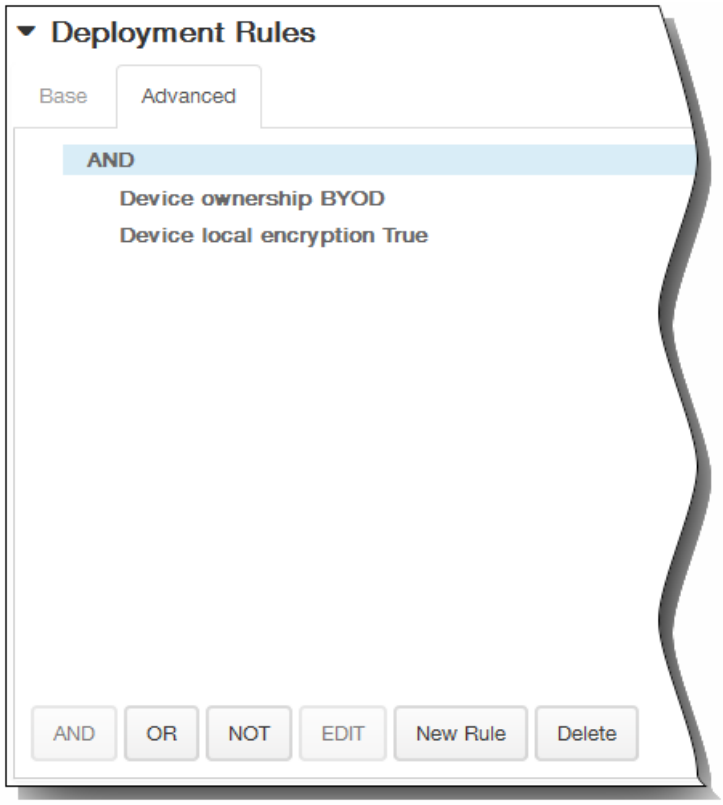
Remarque : pour supprimer une imprimante existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.
Pour modifier 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.

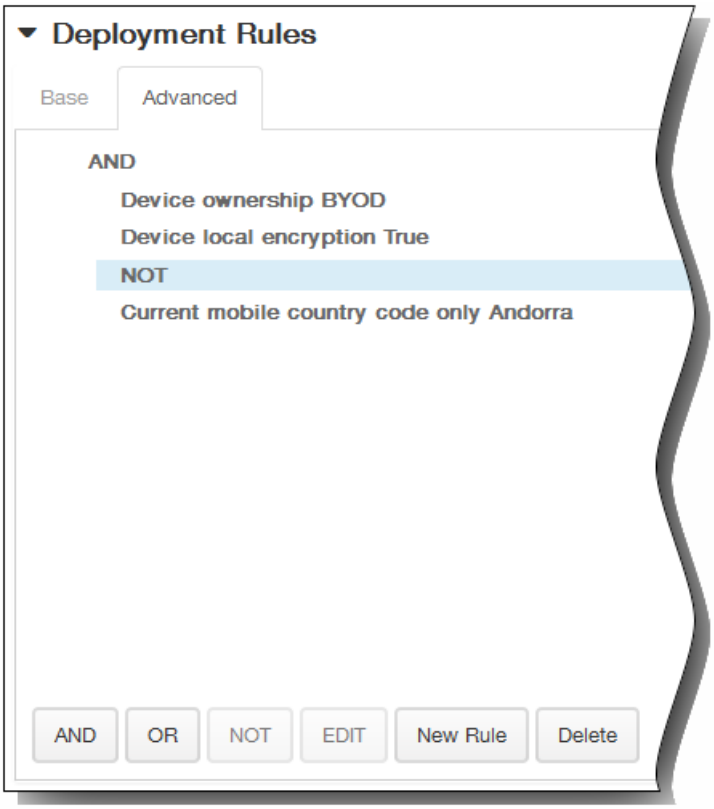
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



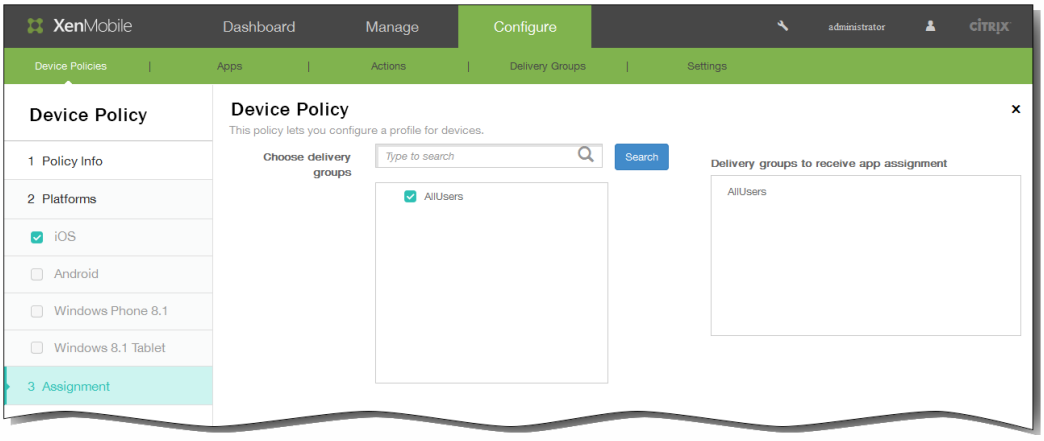
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

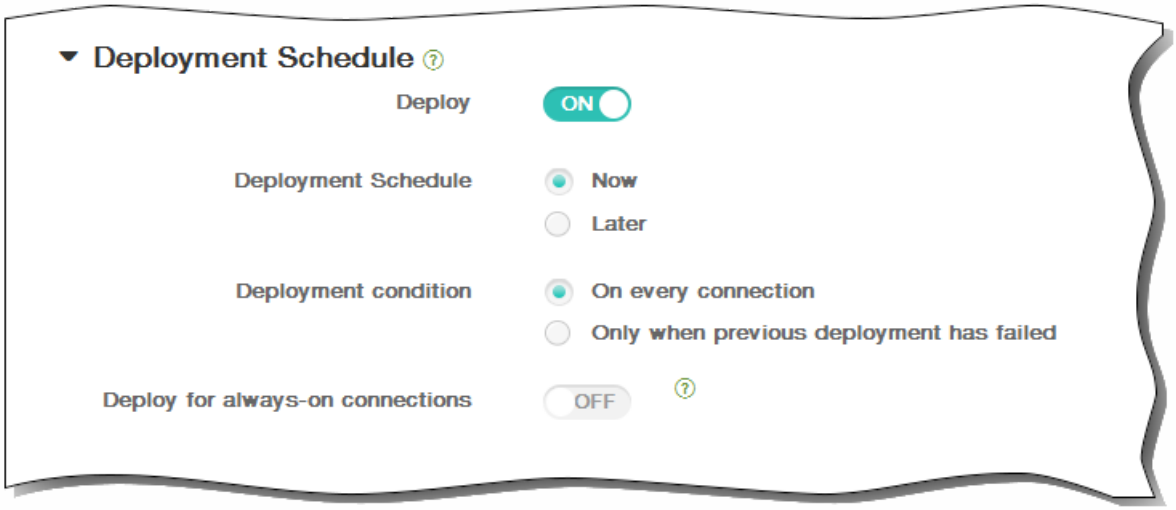


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.



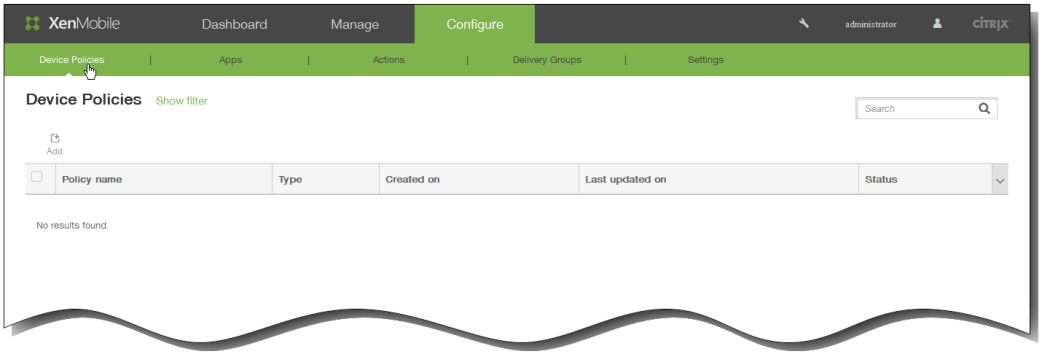
15. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de calendrier (CalDAV) pour iOS

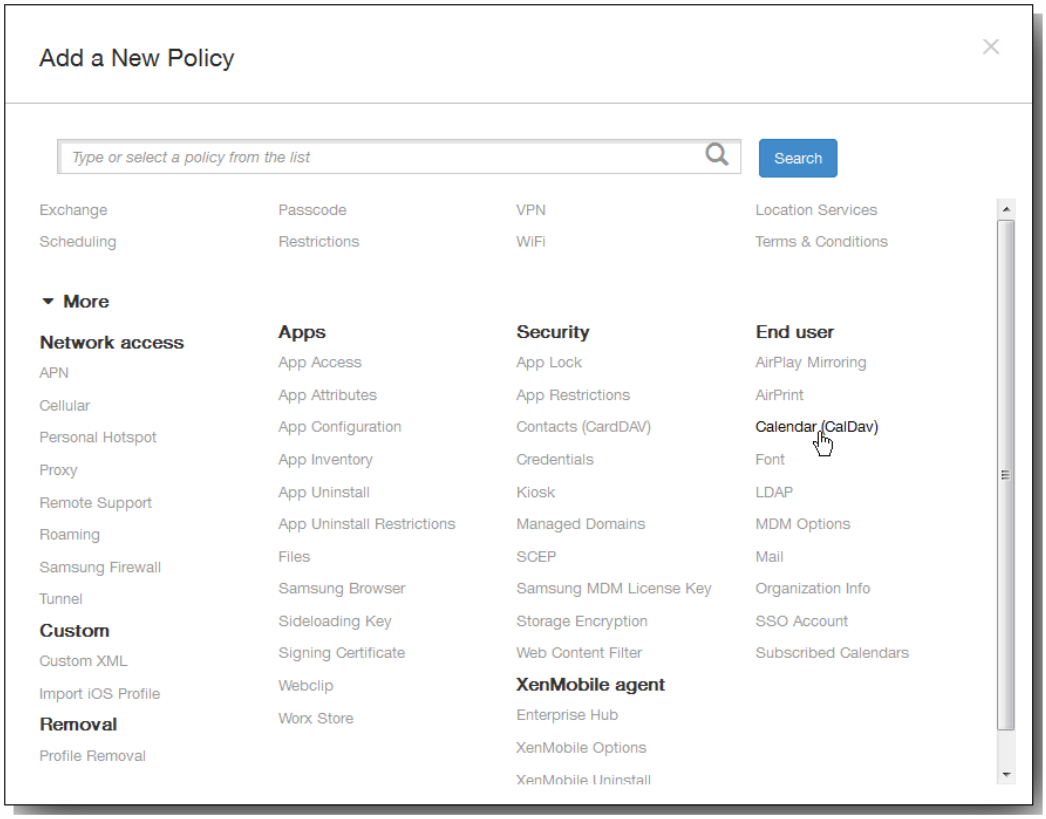
May 06, 2016

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.

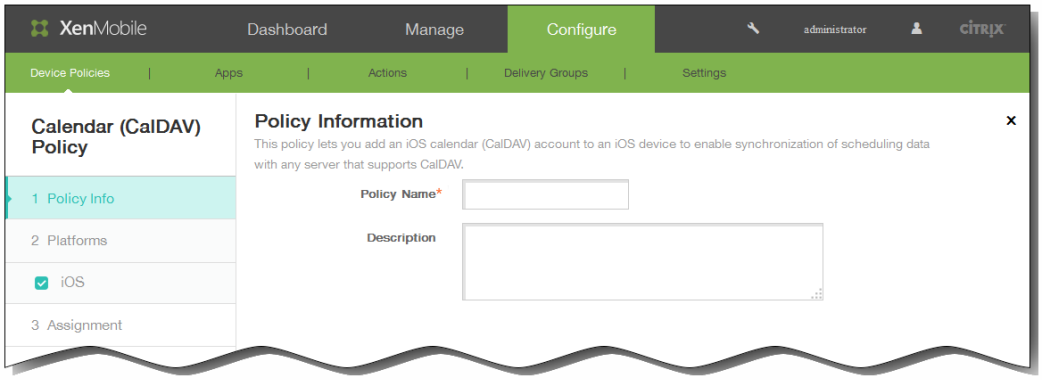
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



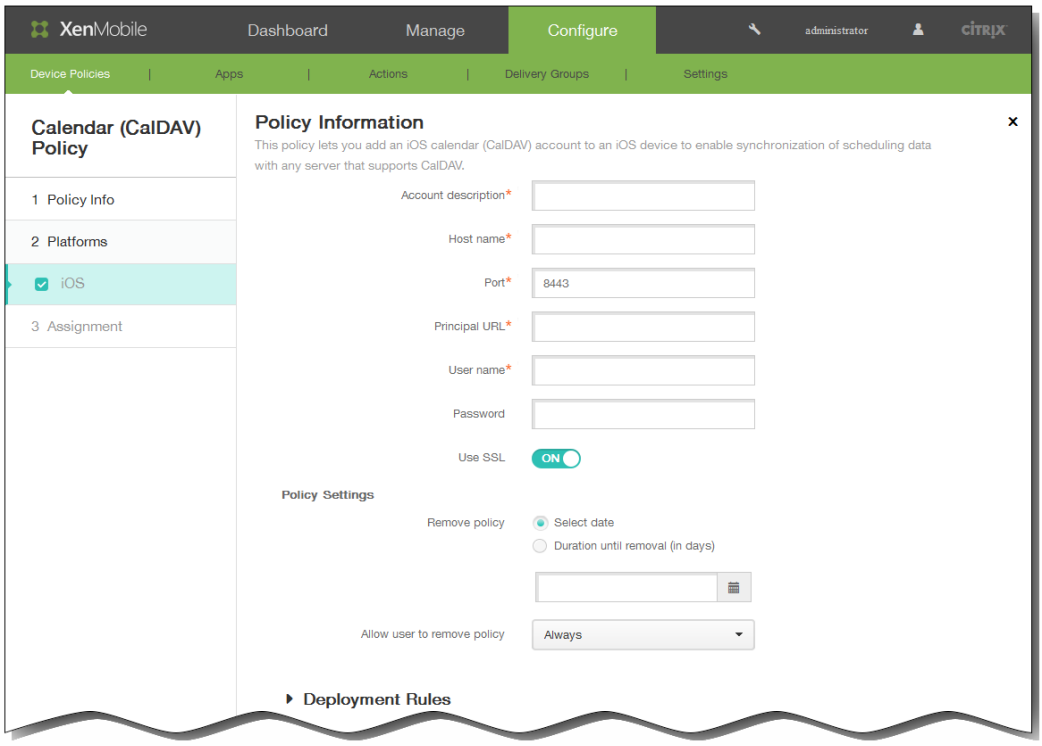
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Calendrier (CalDav). La page Stratégie de calendrier (CalDAV) s'affiche.



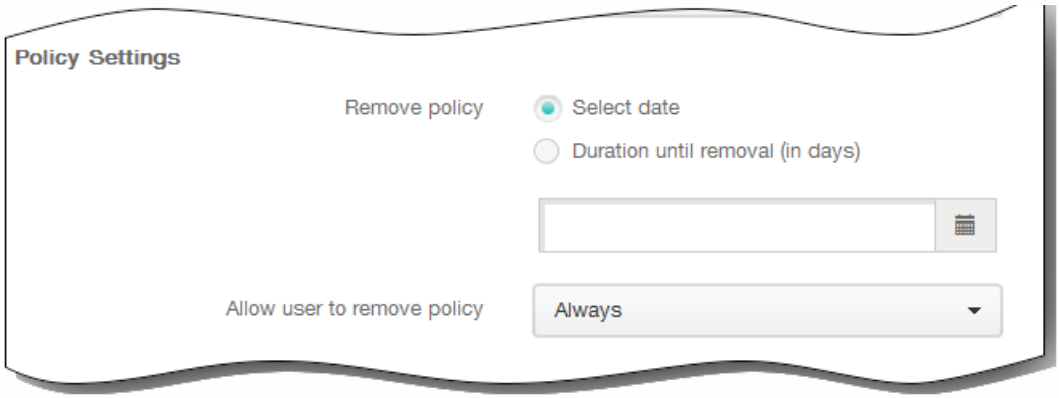
4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS 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.

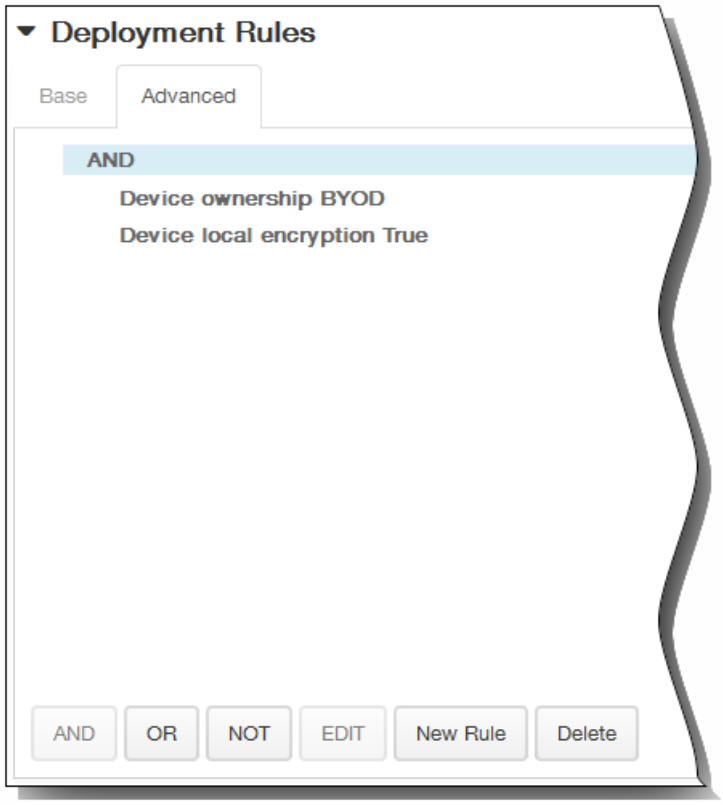
5. Nom d'utilisateur : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
6. Mot de passe : entrez un mot de passe utilisateur (facultatif).
7. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur CalDAV. La valeur par défaut est On.

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.

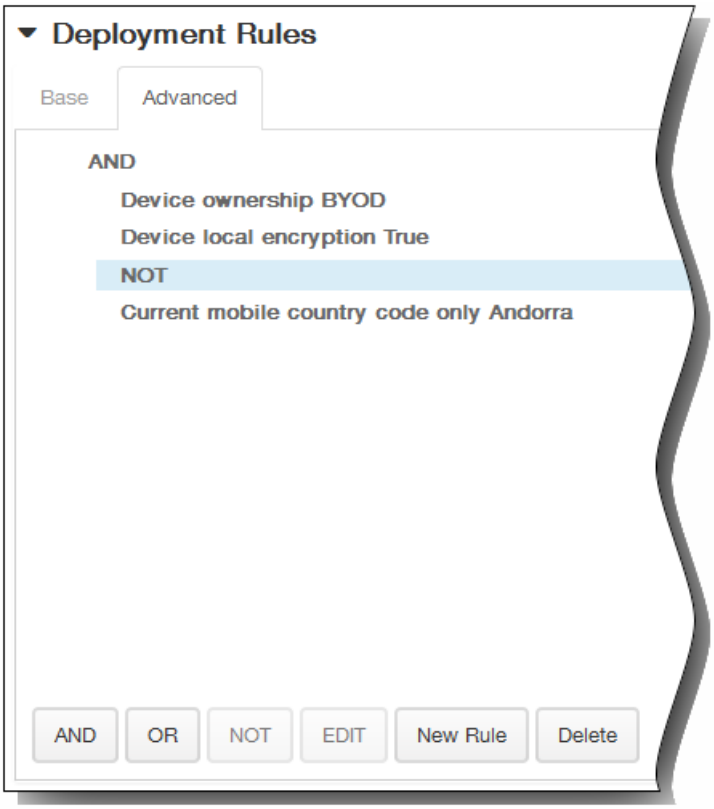
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



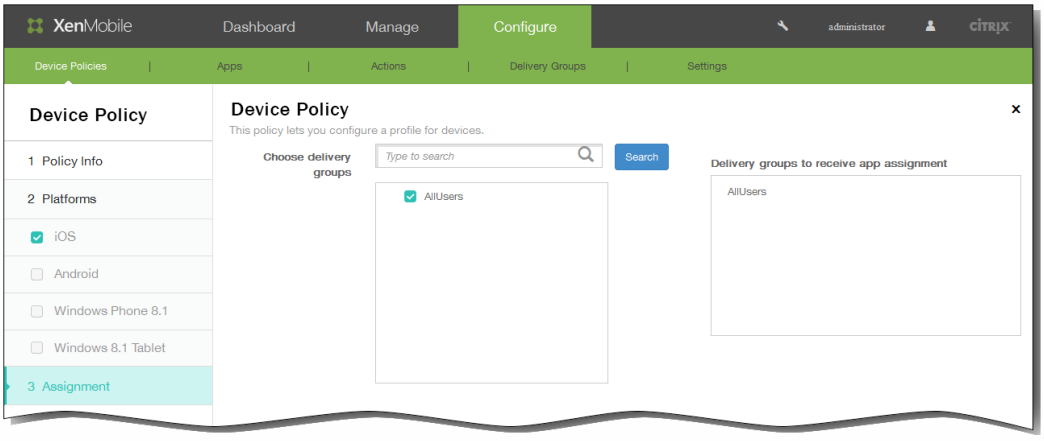
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

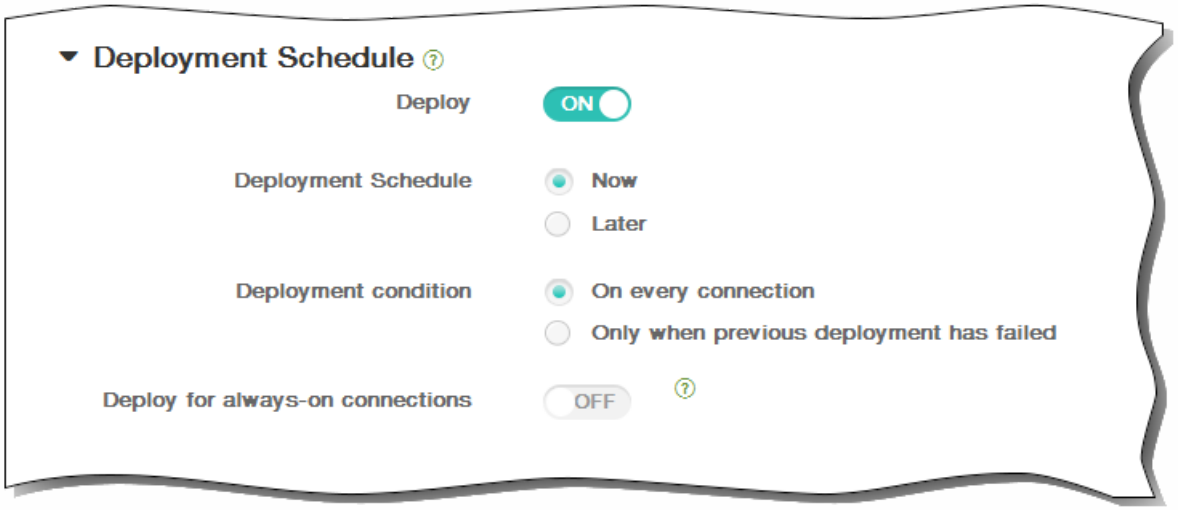


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.



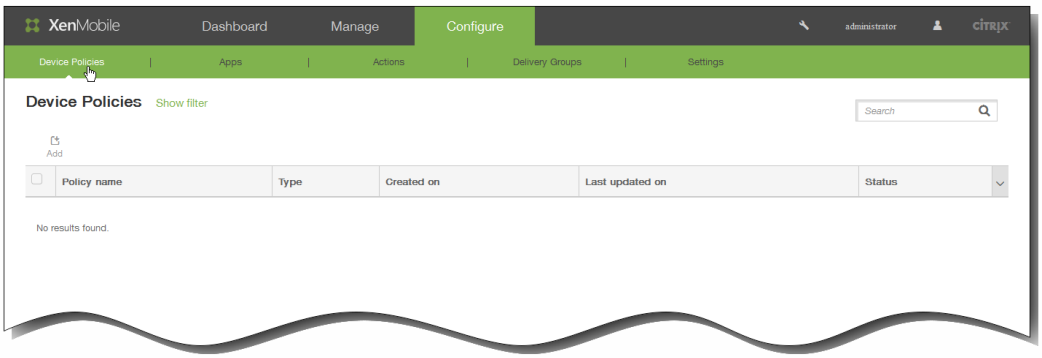
15. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de contacts (CardDAV) pour iOS

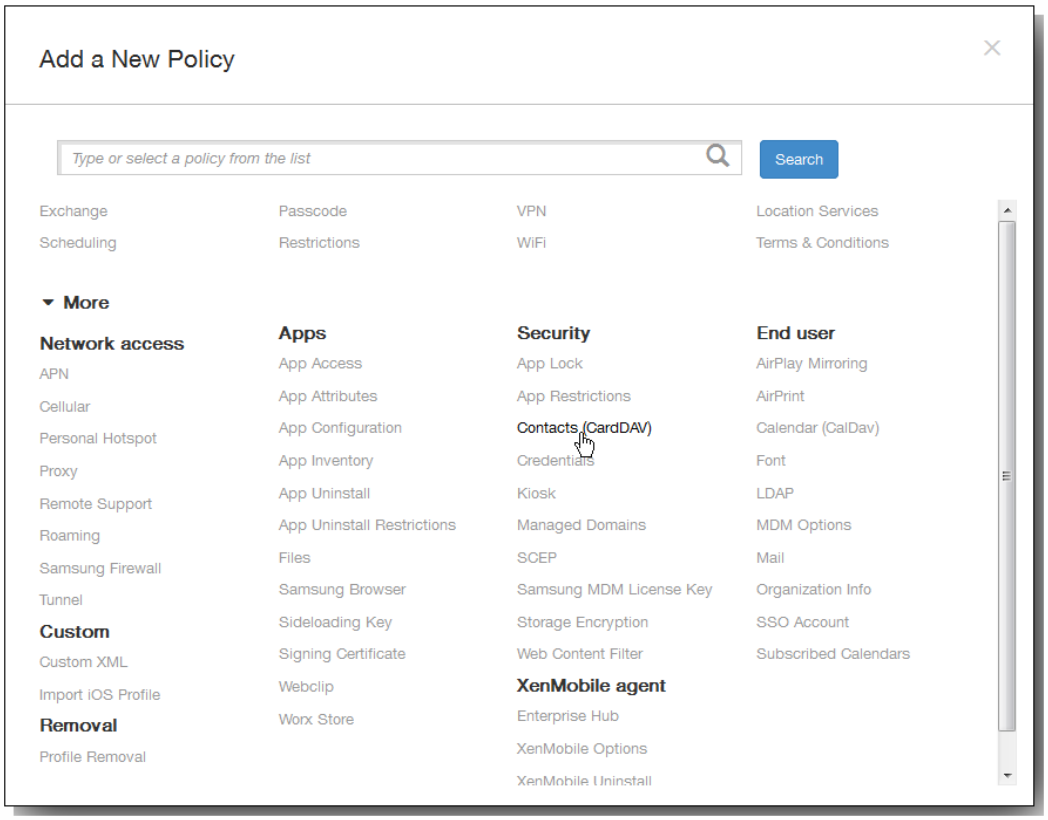
May 06, 2016

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.

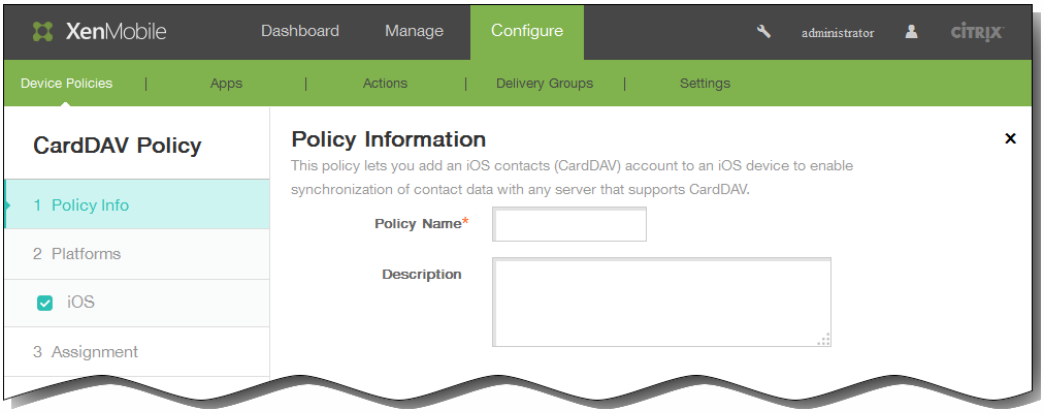
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



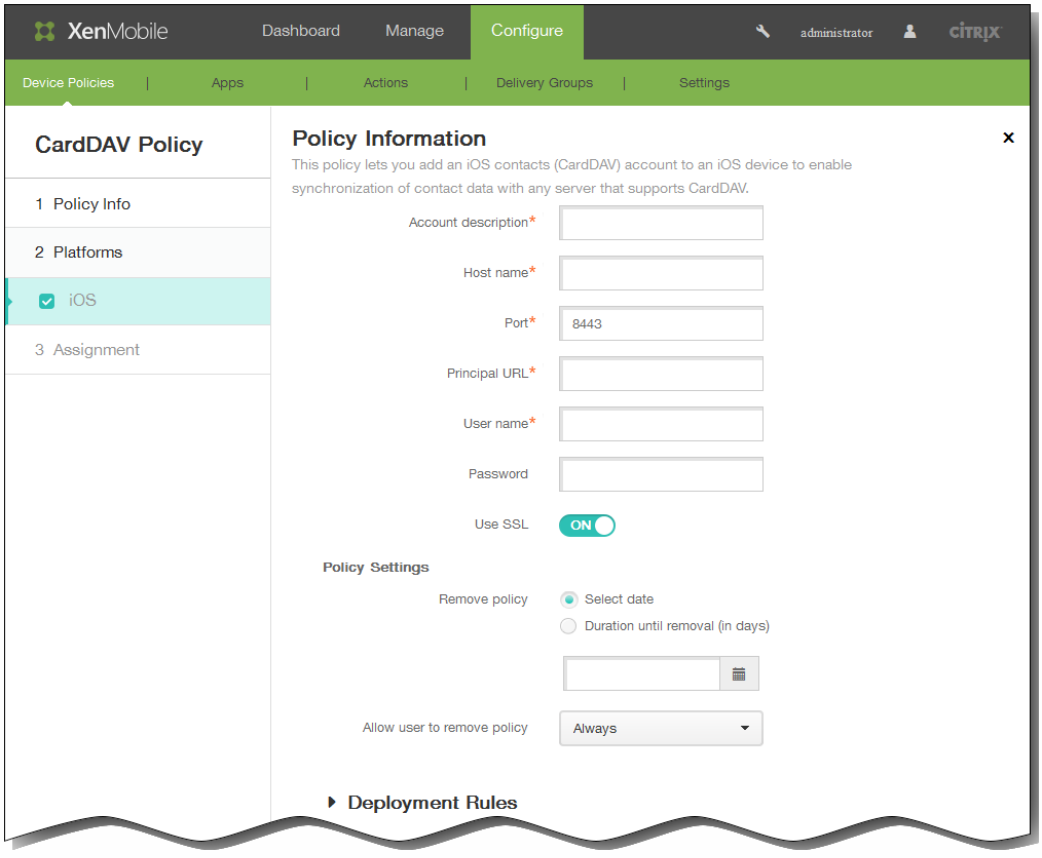
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



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.

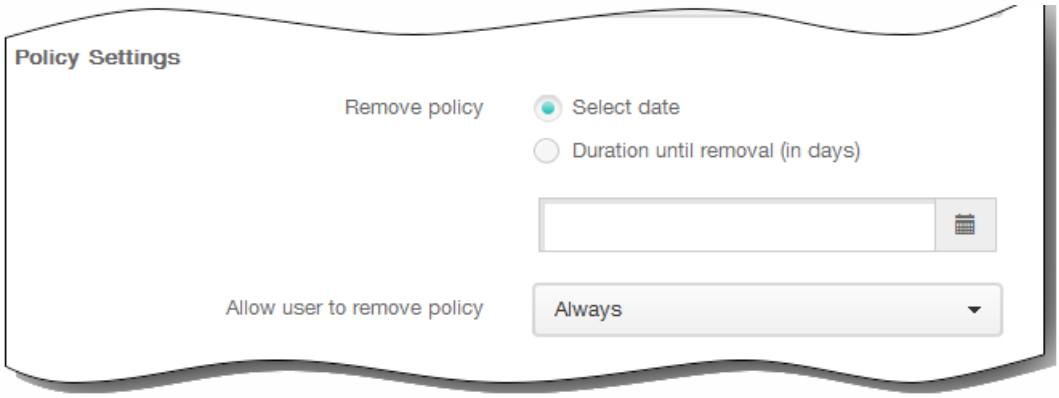


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Description du compte : entrez une description pour le compte. Ce champ est obligatoire.
   2. Nom d'hôte : entrez l'adresse du serveur CardDAV. Ce champ est obligatoire.
   3. Port : entrez le port sur lequel se connecter au serveur CardDAV. Ce champ est obligatoire. La valeur par défaut est

8443.

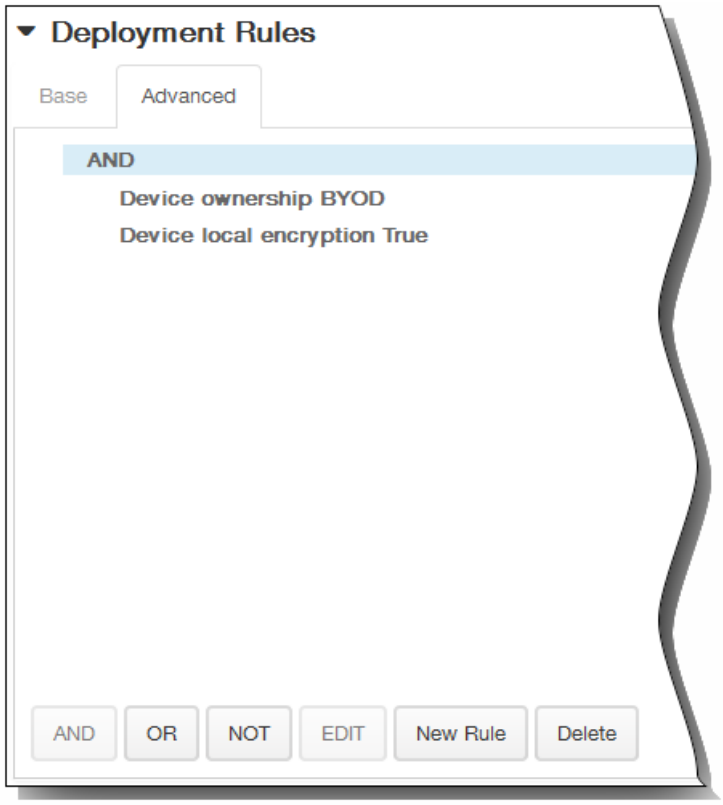
4. URL principale : entrez l'adresse URL du calendrier de l'utilisateur.
5. Nom d'utilisateur : entrez le nom de connexion de l'utilisateur. Ce champ est obligatoire.
6. Mot de passe : entrez un mot de passe utilisateur (facultatif).
7. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser 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.

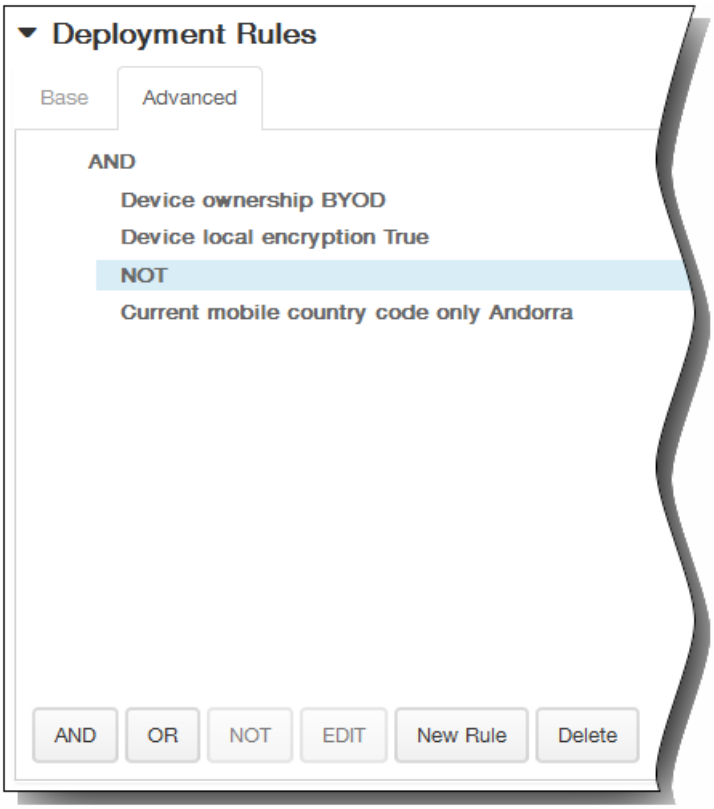
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



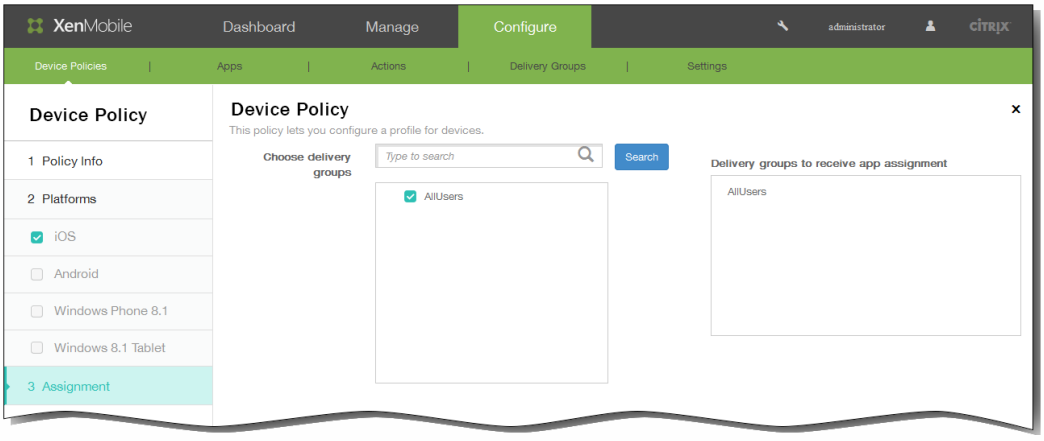
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

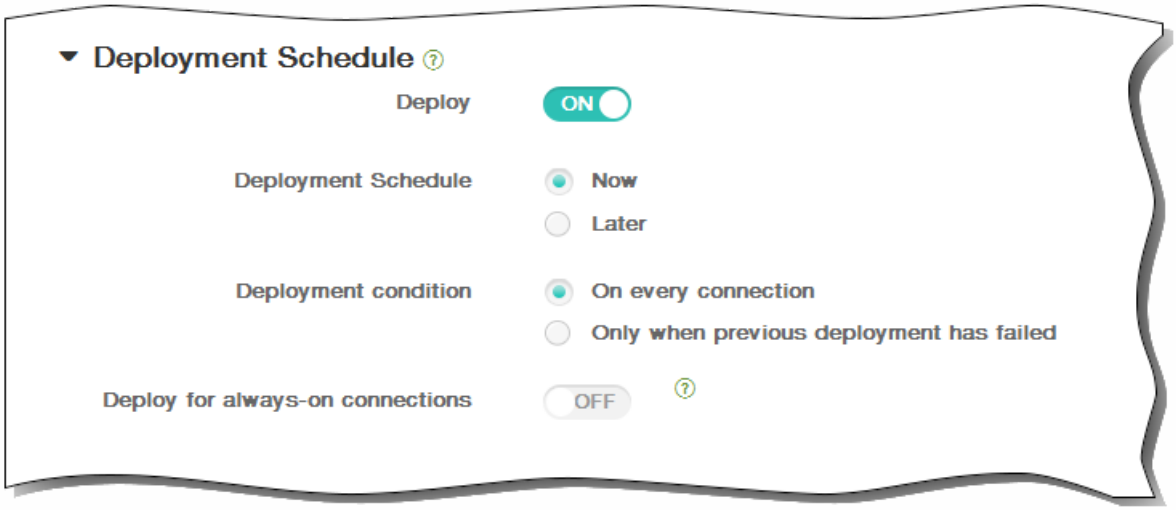


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

Stratégies d'informations d’identification

May 06, 2016

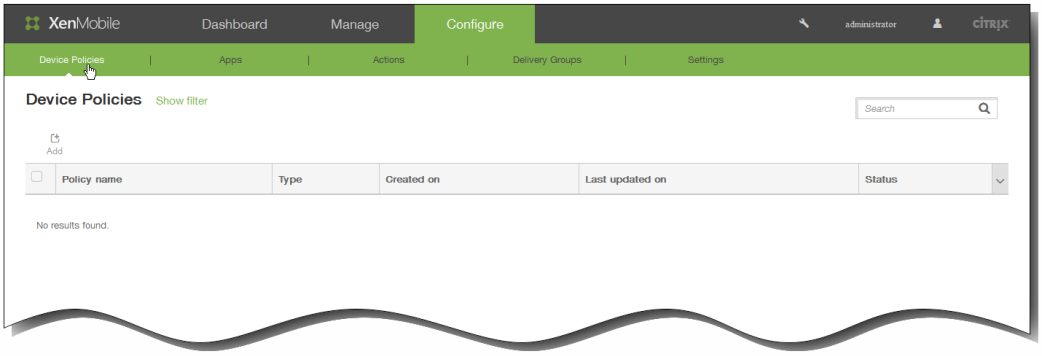
Vous pouvez créer des stratégies d'informations d'identification dans XenMobile afin d'intégrer l'authentification à votre configuration PKI dans XenMobile, comme une entité PKI, un keystore, un fournisseur d'informations d'identification ou un certificat de serveur. Pour plus d'informations sur les informations d’identification, veuillez consulter la section Certificats dans XenMobile.

Vous pouvez créer des stratégies d'informations d'identification pour iOS, Android, et Windows 8.1 Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

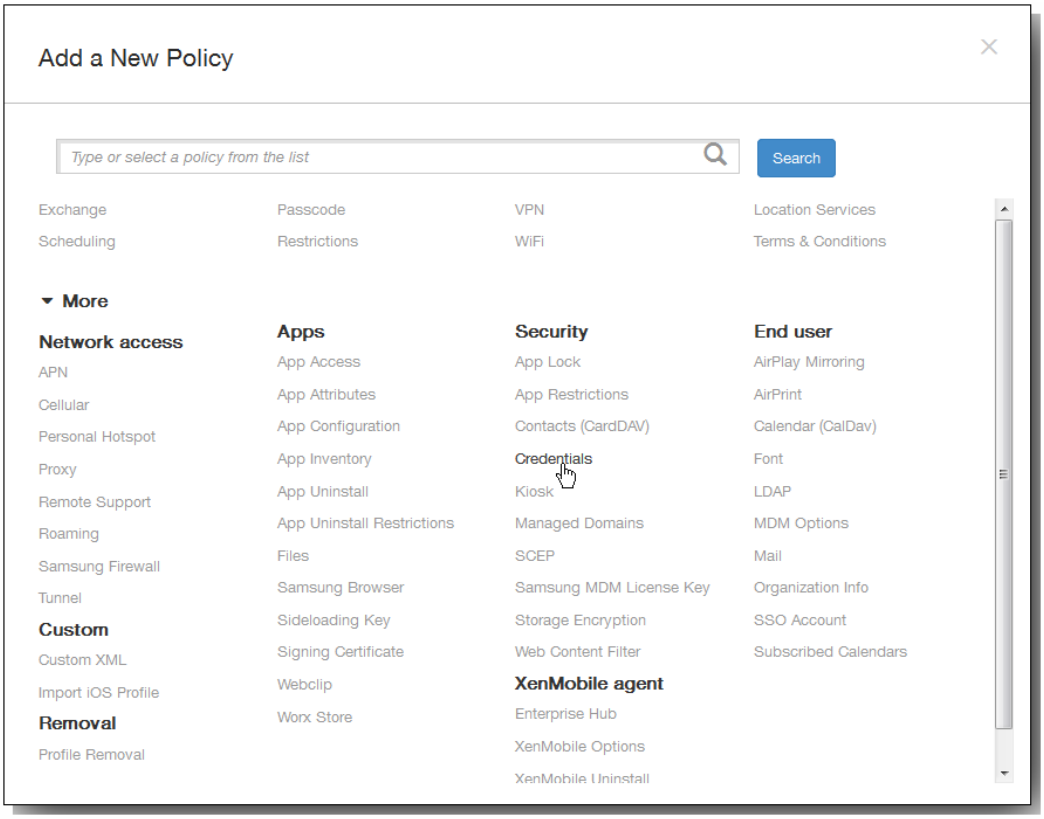
Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie :

- Informations d'identification que vous prévoyez d'utiliser pour chaque plate-forme, ainsi que les certificats et les mots de passe.

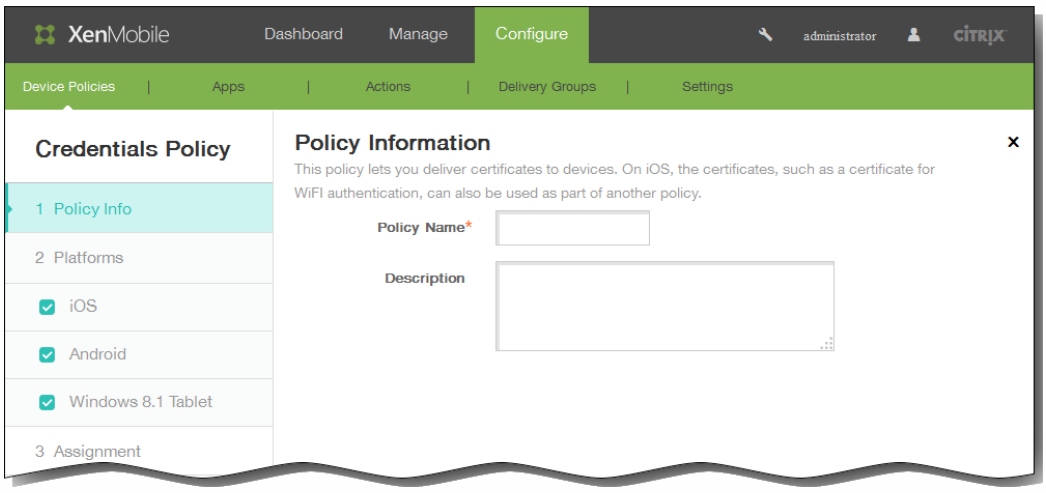
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



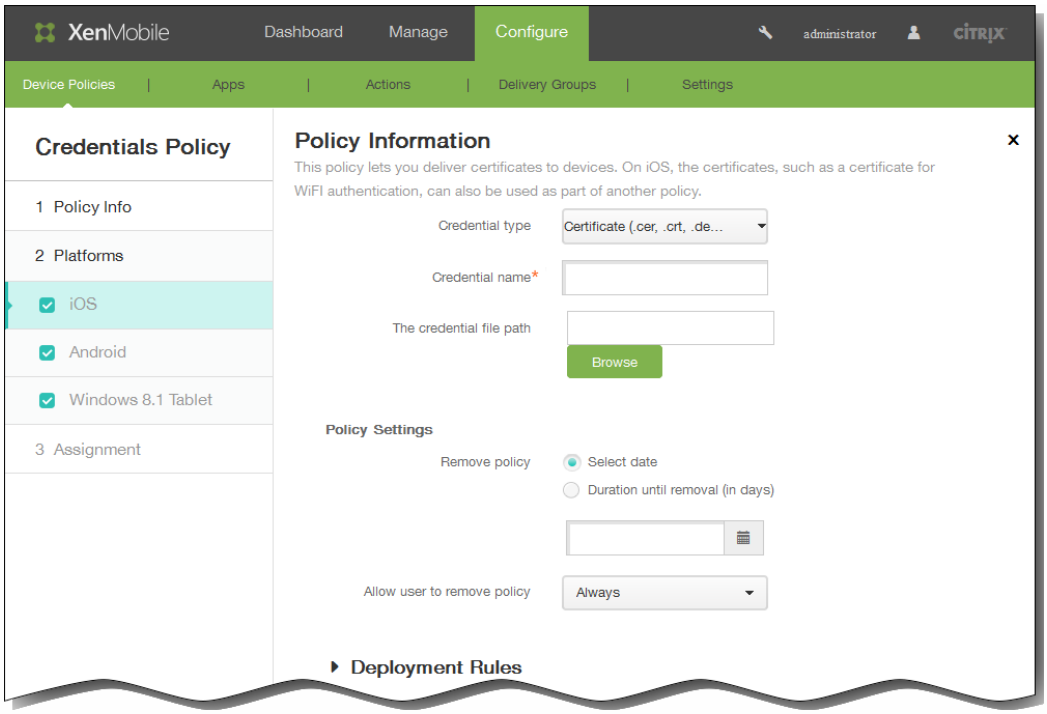
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



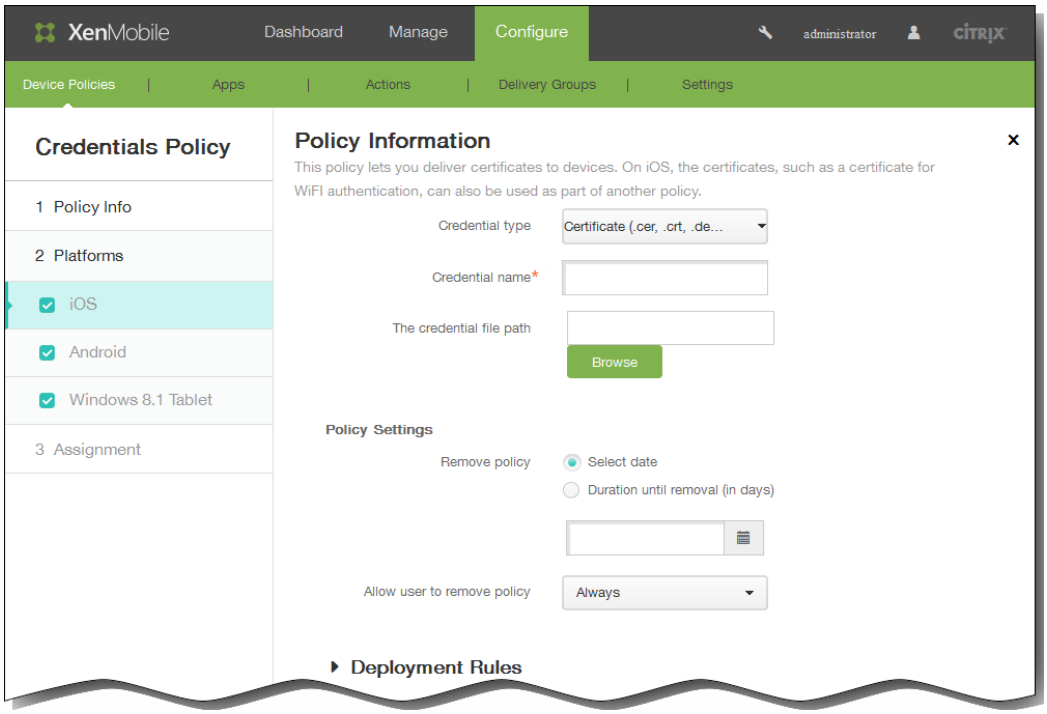
3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Informations d'identification. La page Stratégie d'informations d'identification s'affiche.



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.

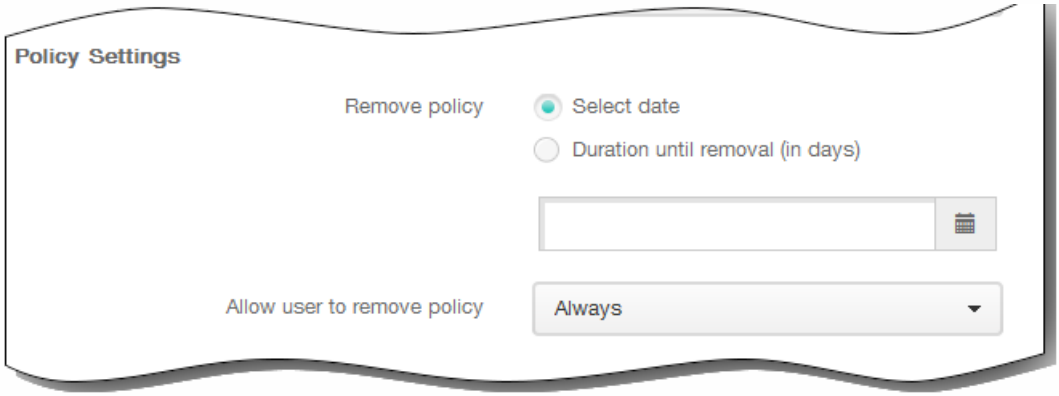
Entrez les informations suivantes pour les informations d'identification que vous sélectionnez :

- 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.

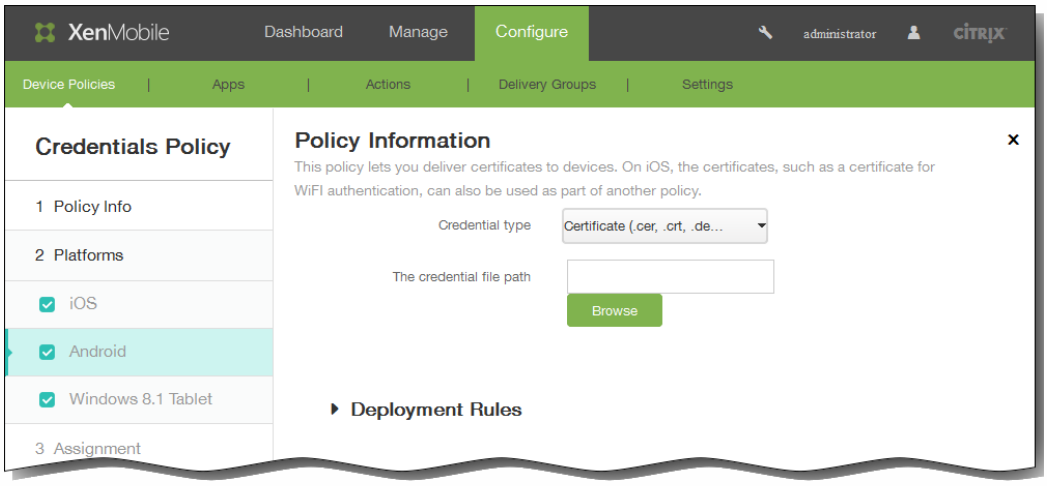
- **Keystore**
  - Nom du certificat : entrez un nom unique pour le certificat.
  - Emplacement du certificat : sélectionnez le fichier de certificat, en cliquant sur Parcourir et accédez à l'emplacement du fichier.
  - Mot de passe : entrez le mot de passe du magasin de clés pour le certificat.
- **Certificat 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.

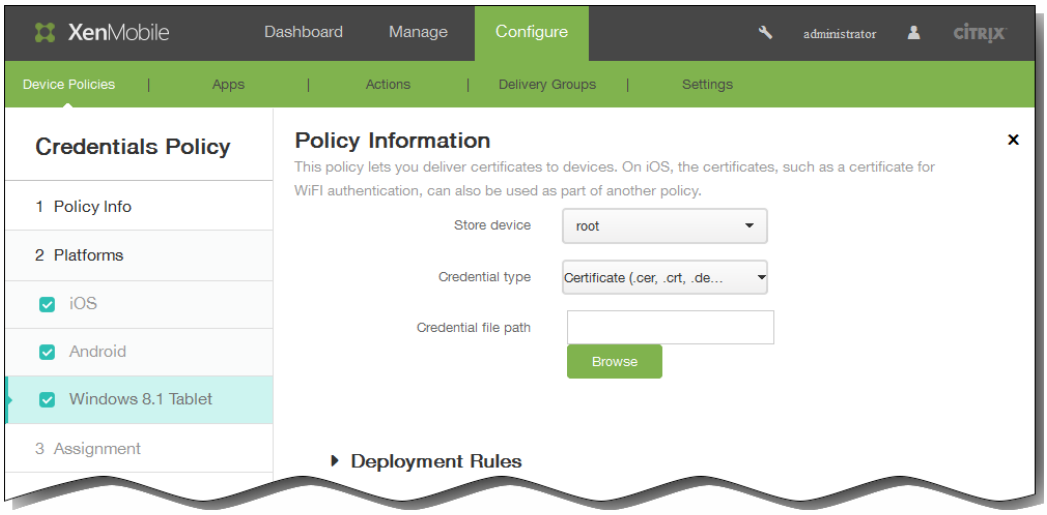
- Si vous avez sélectionné Android, configurez les paramètres suivants :



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**
  - 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 :



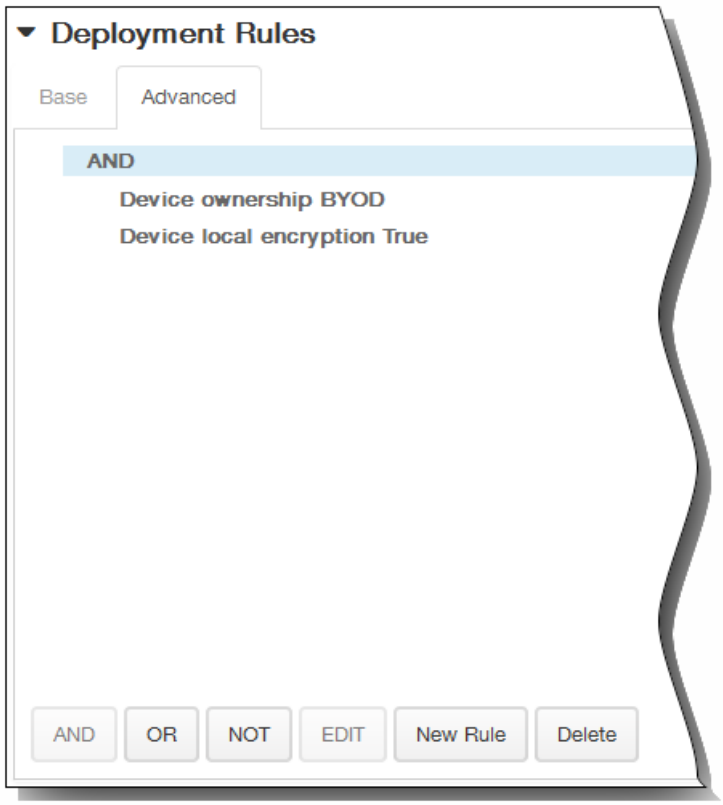
Périphérique de stockage : dans la liste, cliquez sur racine Mon magasin, ou Autorité de certification pour l'emplacement du magasin de certificats pour les informations d'identification. Mon magasin stocke les certificats dans les magasins de certificats des utilisateurs.

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.

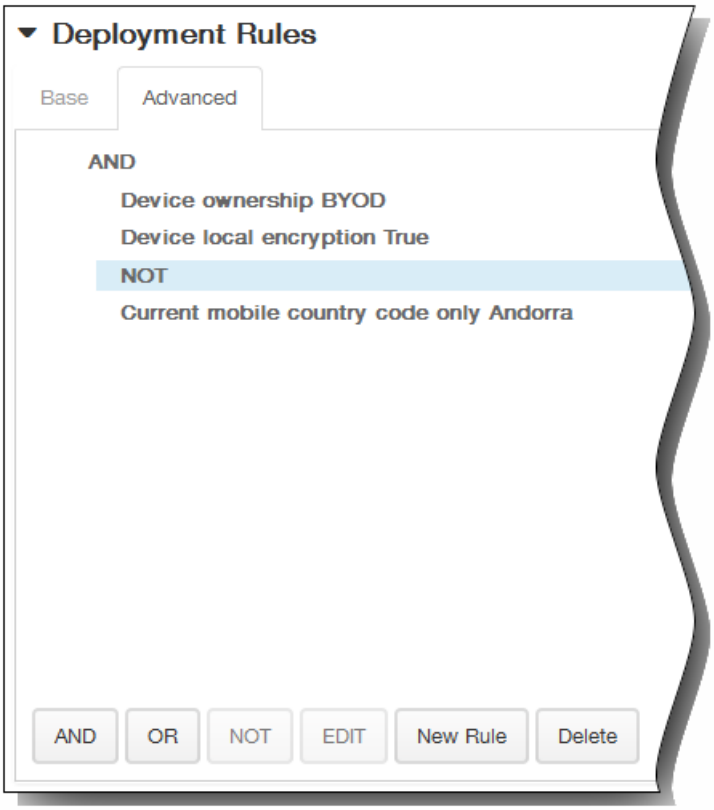
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



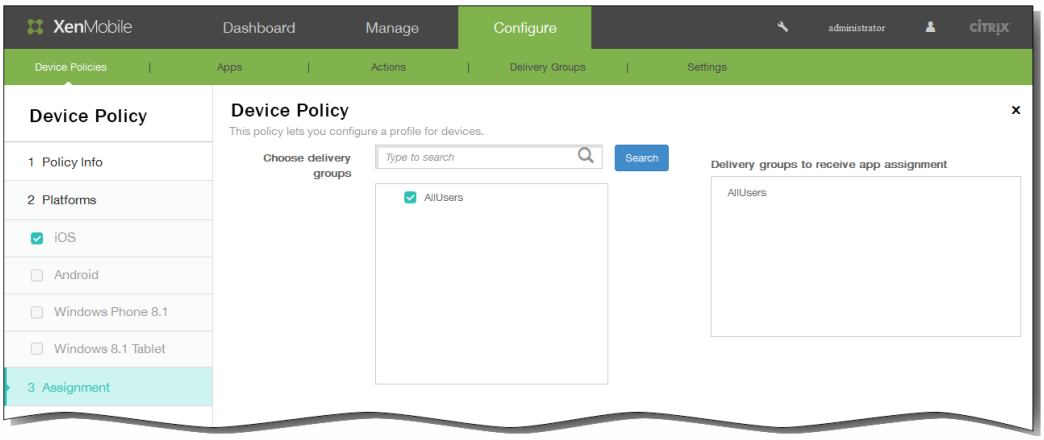
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



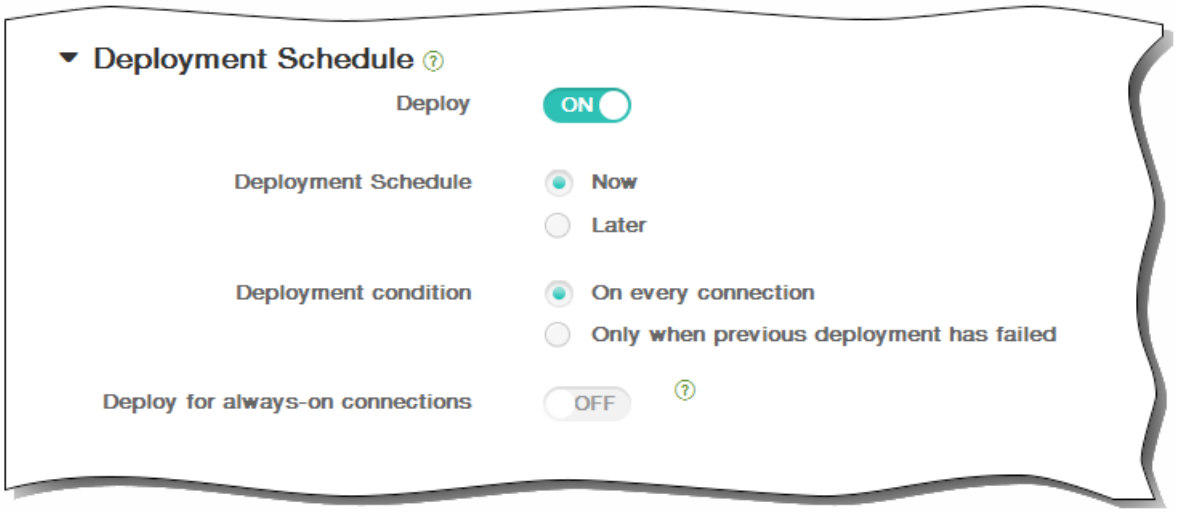
8. Cliquez sur Suivant. La page d'attribution de la Stratégie d'informations d'identification s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie kiosque pour Samsung SAFE

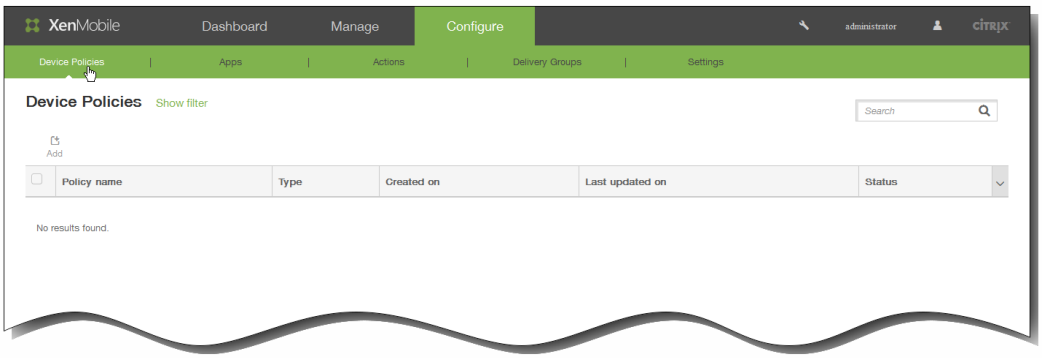
May 06, 2016

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.

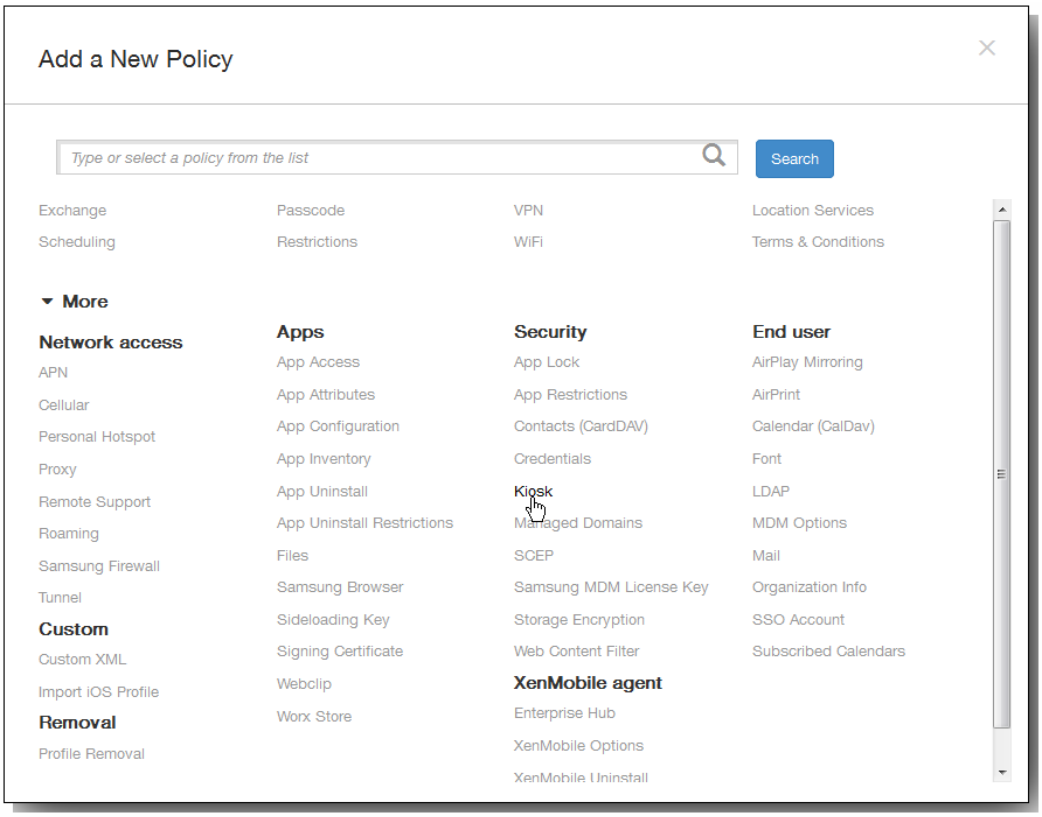
Remarque :

- 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.

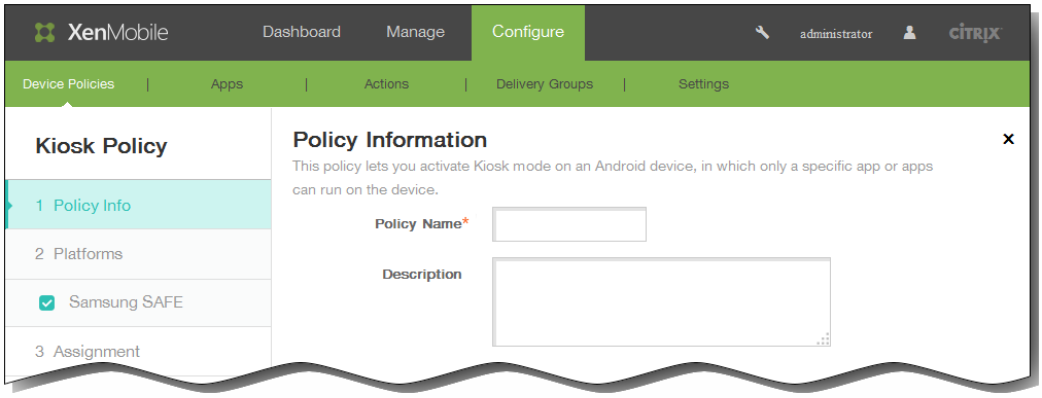
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



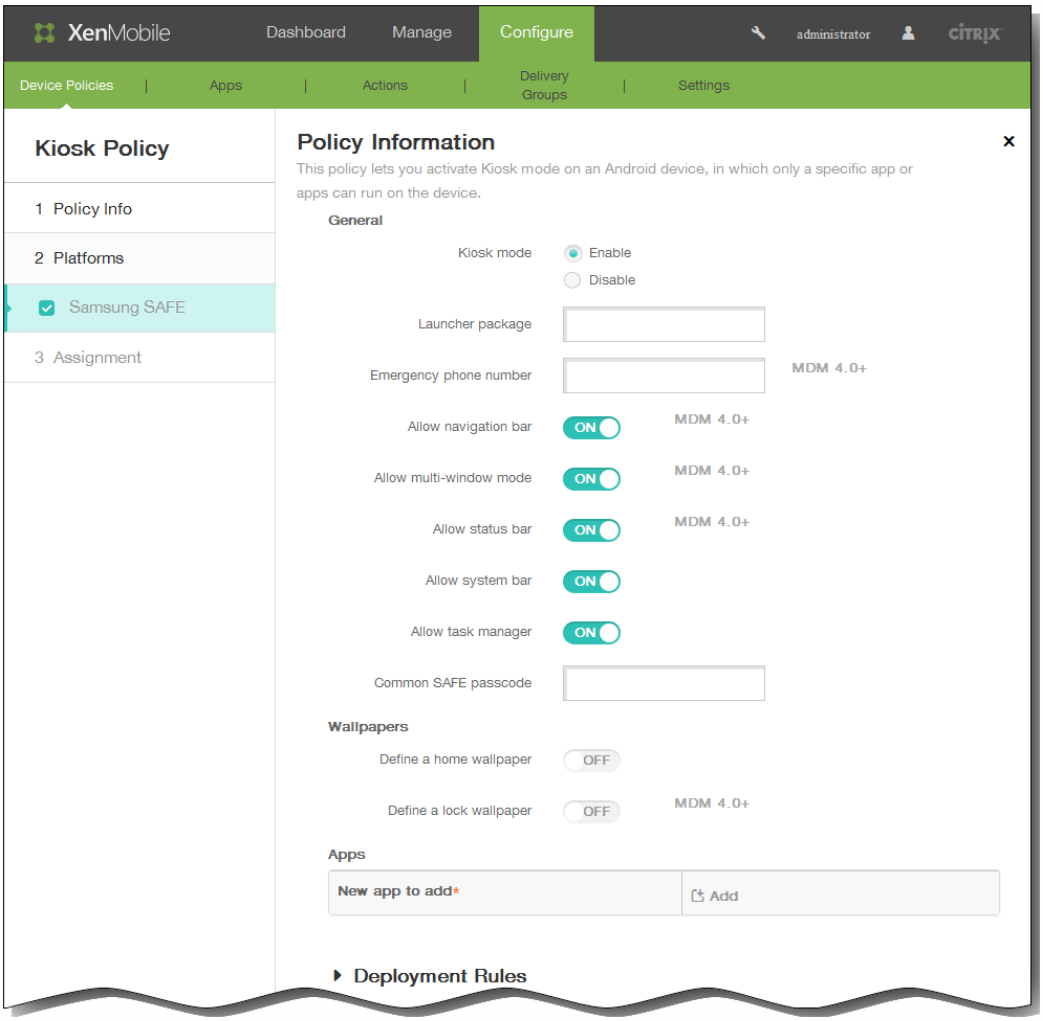
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Kiosque. La page Stratégie kiosque s'affiche.

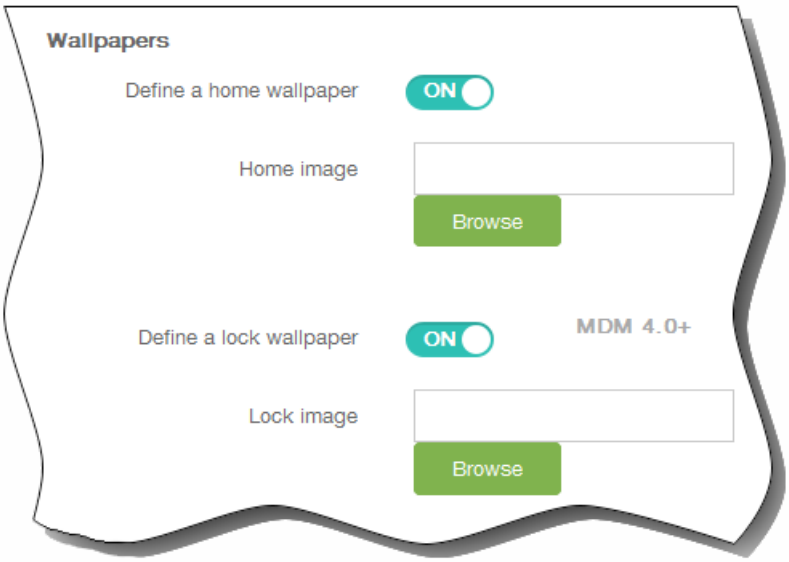


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations sur la plate-forme Samsung SAFE s'affiche.



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.

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.



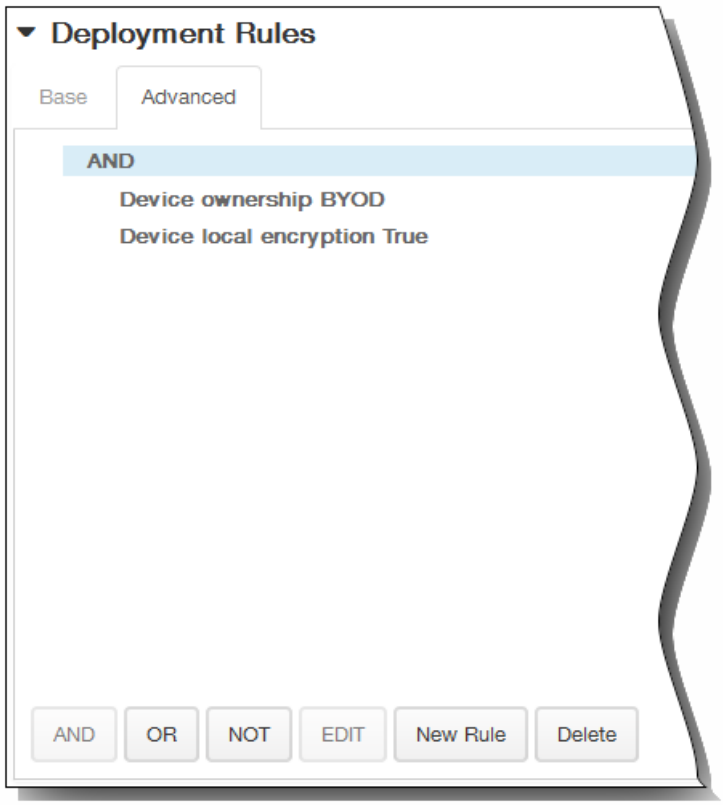
12. Applications : cliquez sur Ajouter, puis procédez comme suit :
    1. Nouvelle application à ajouter : entrez le nom complet de l'application à ajouter. Par exemple, com.android.calendar permet aux utilisateurs d'utiliser l'application calendrier d'Android.
    2. Cliquez sur Ajouter pour ajouter 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.

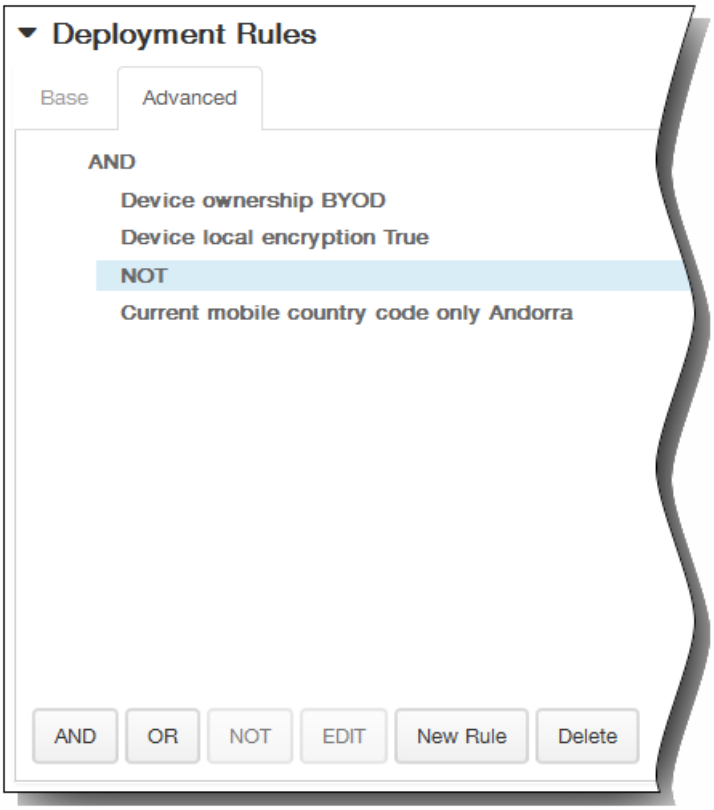
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



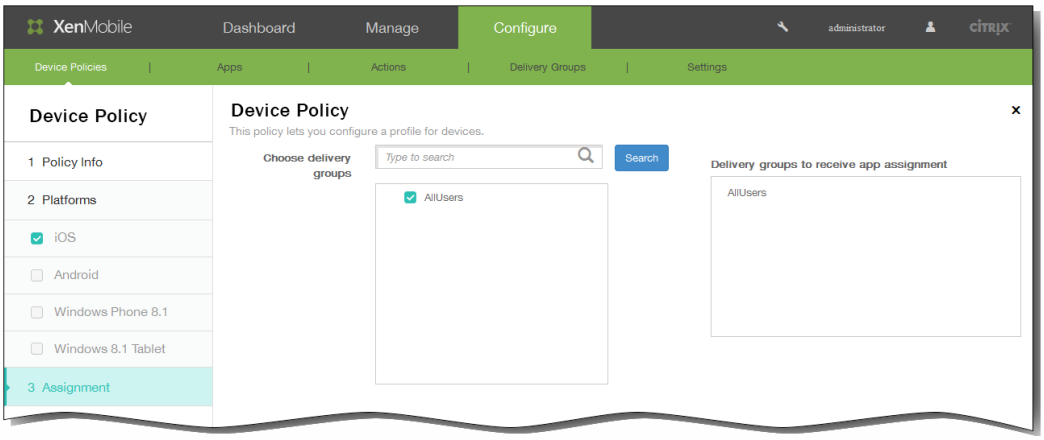
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



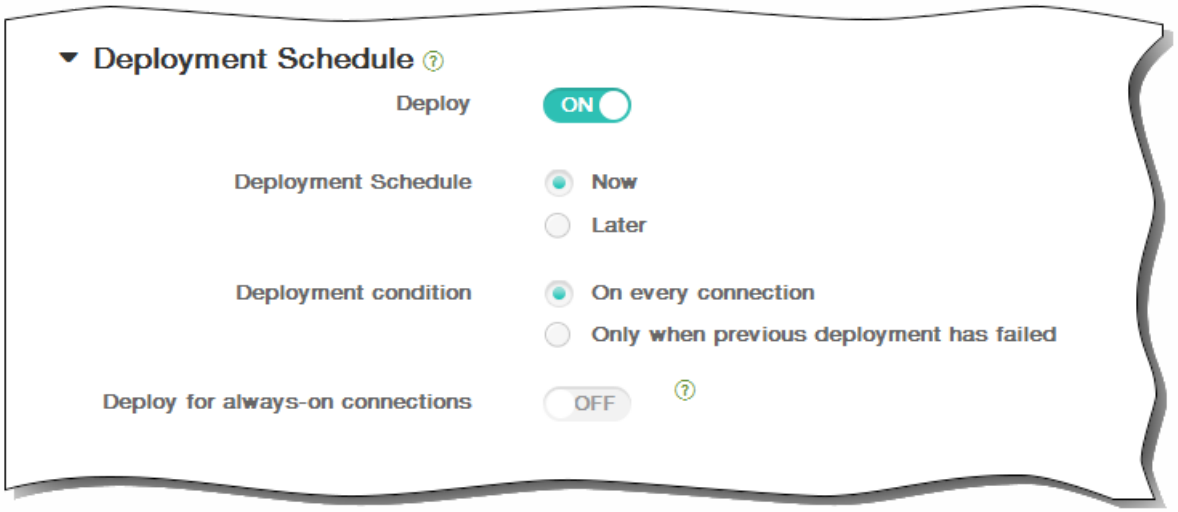
8. Cliquez sur Suivant. La page d'attribution de la Stratégie kiosque s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes 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 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.

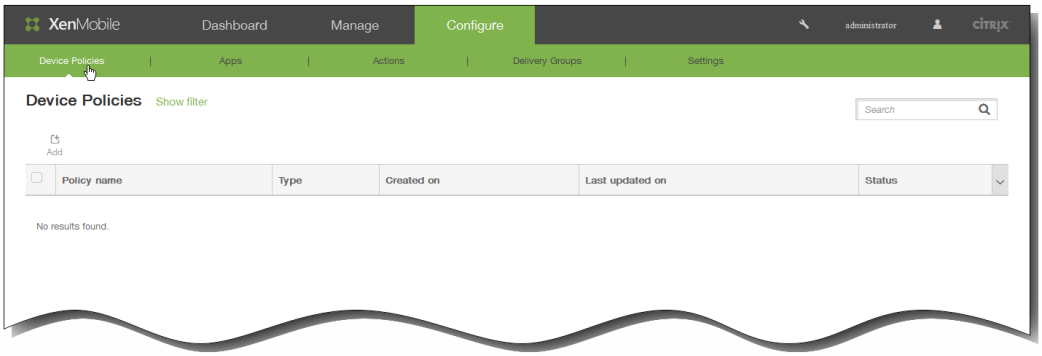
Pour ajouter une stratégie de police pour iOS

May 06, 2016

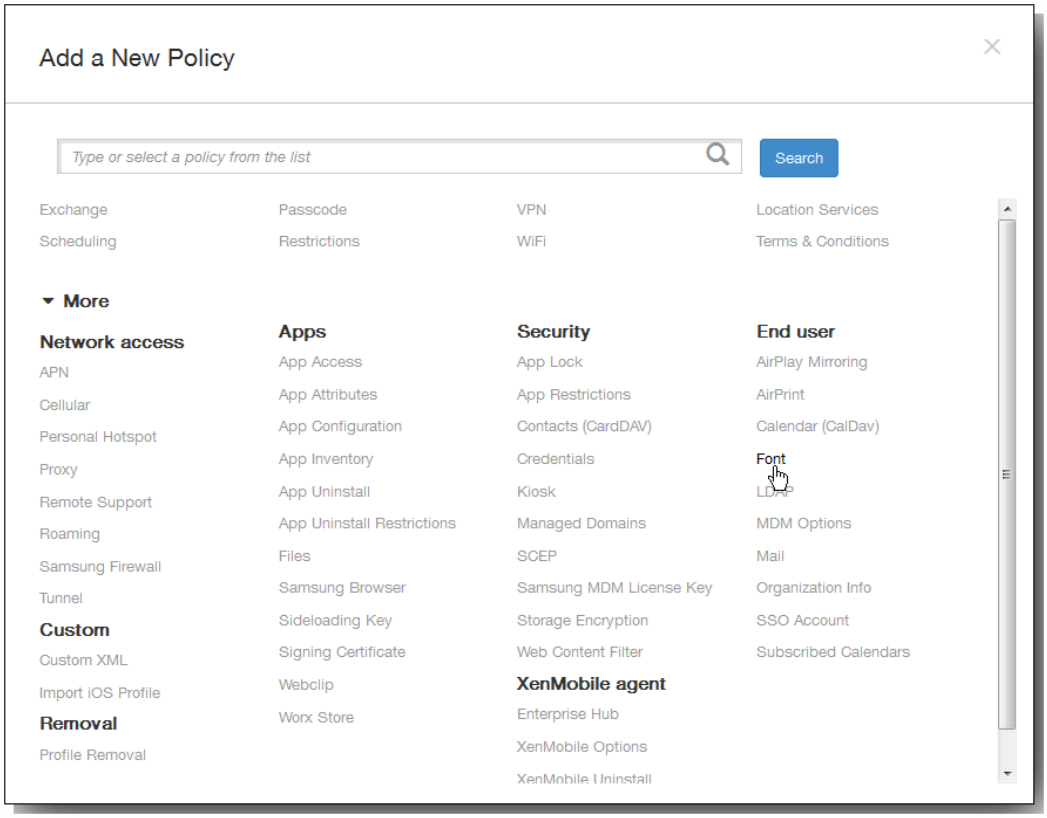
Vous pouvez ajouter une stratégie de police dans XenMobile pour ajouter des polices supplémentaires sur les appareils des utilisateurs. Les polices doivent être de type TrueType (.ttf) ou OpenType (.oft). Les collections de polices (.ttc ou.otc) ne sont pas prises en charge.

Remarque : cette stratégie s'applique uniquement à iOS 7.0 et versions supérieures.

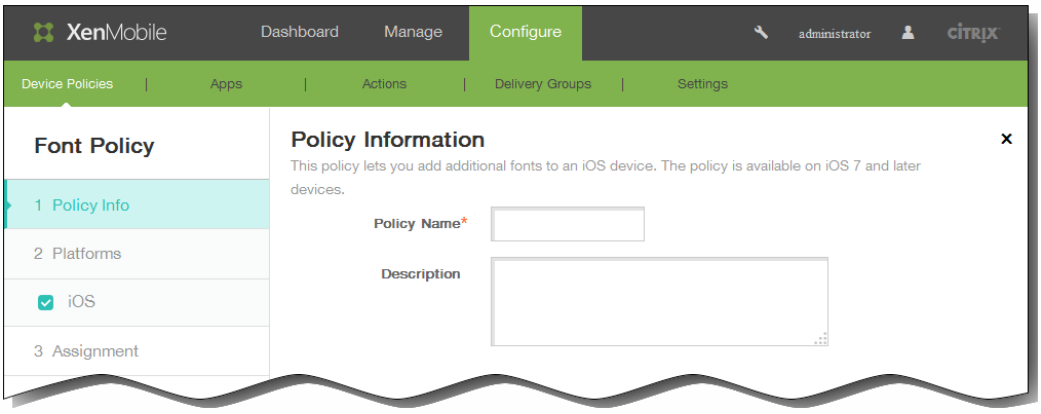
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



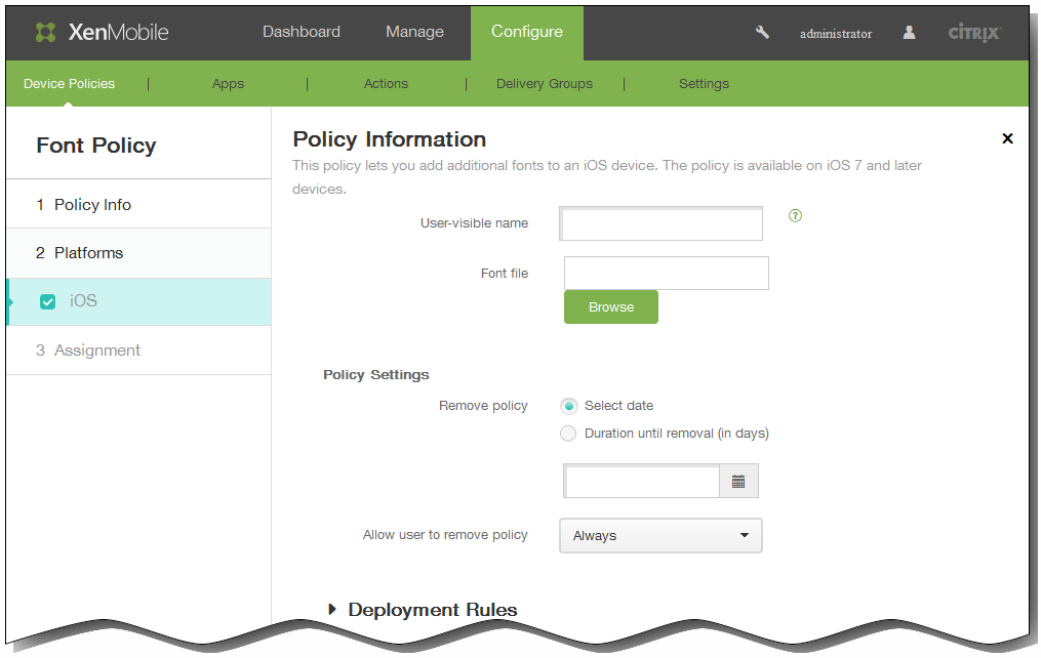
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



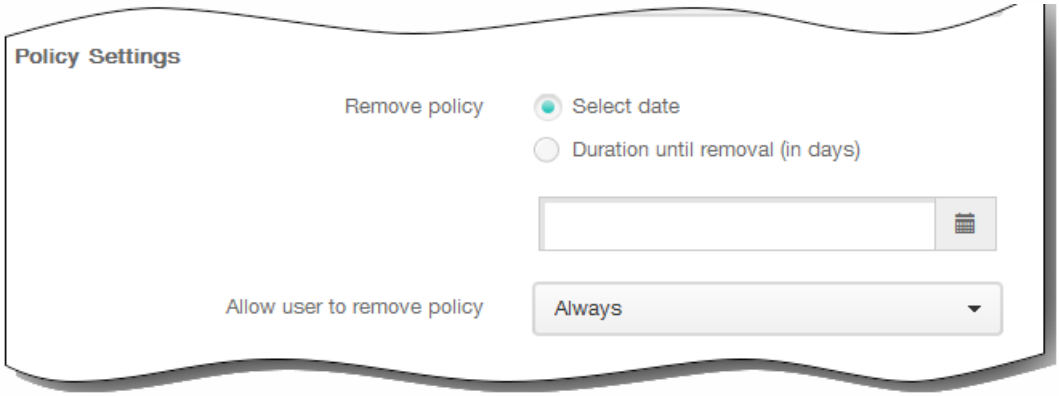
3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Police. La page Stratégie de police s'affiche.



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.

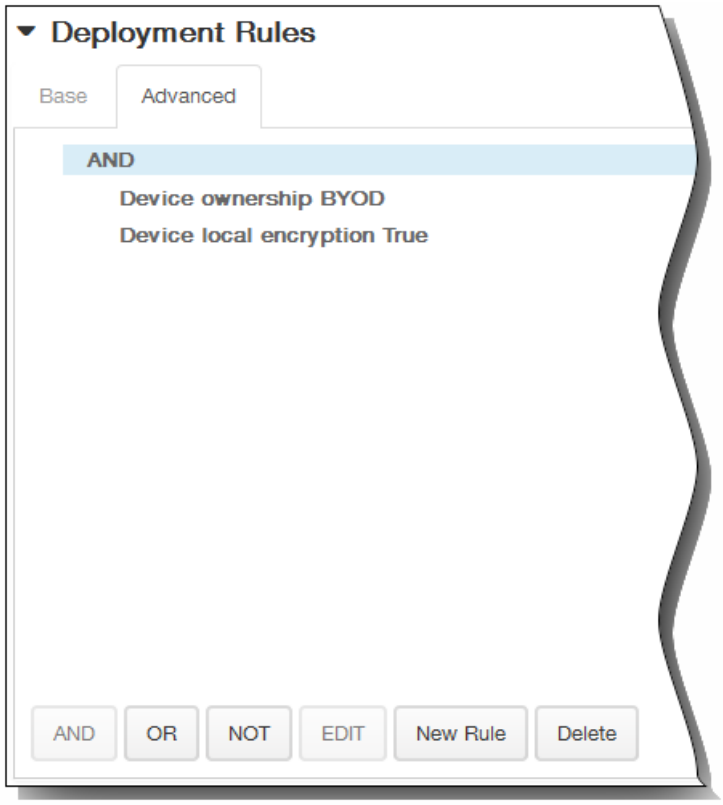


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Nom visible par l'utilisateur : entrez le nom que les utilisateurs voient dans leurs listes de polices.
   2. Fichier de police : sélectionnez le fichier de police à ajouter aux périphériques utilisateur 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.



11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

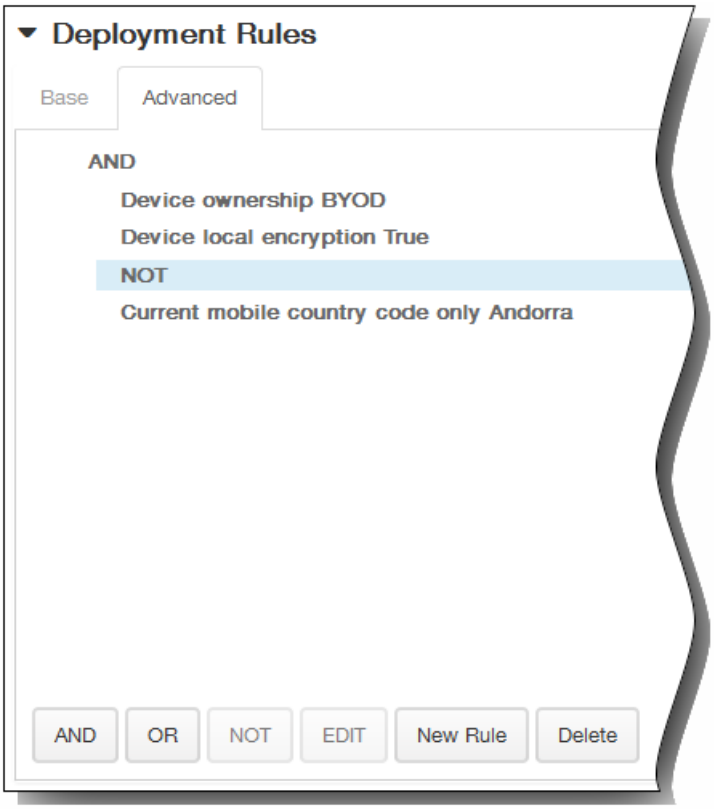
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



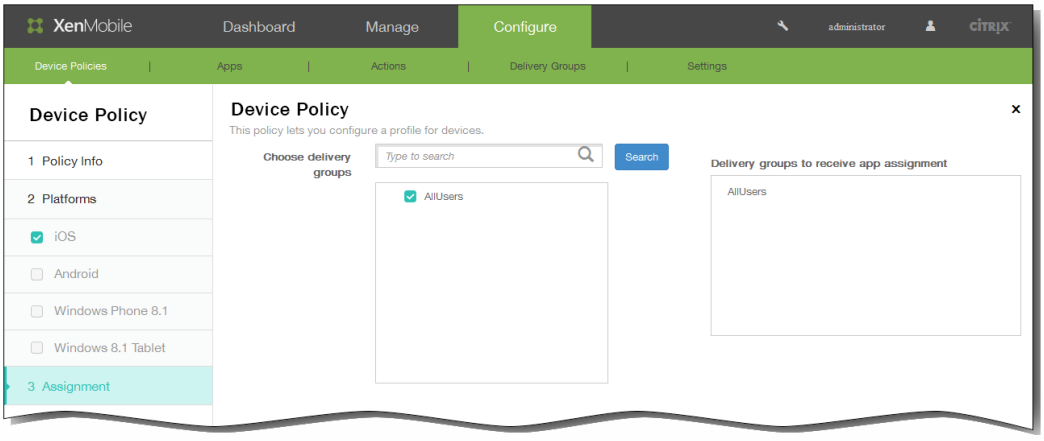
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

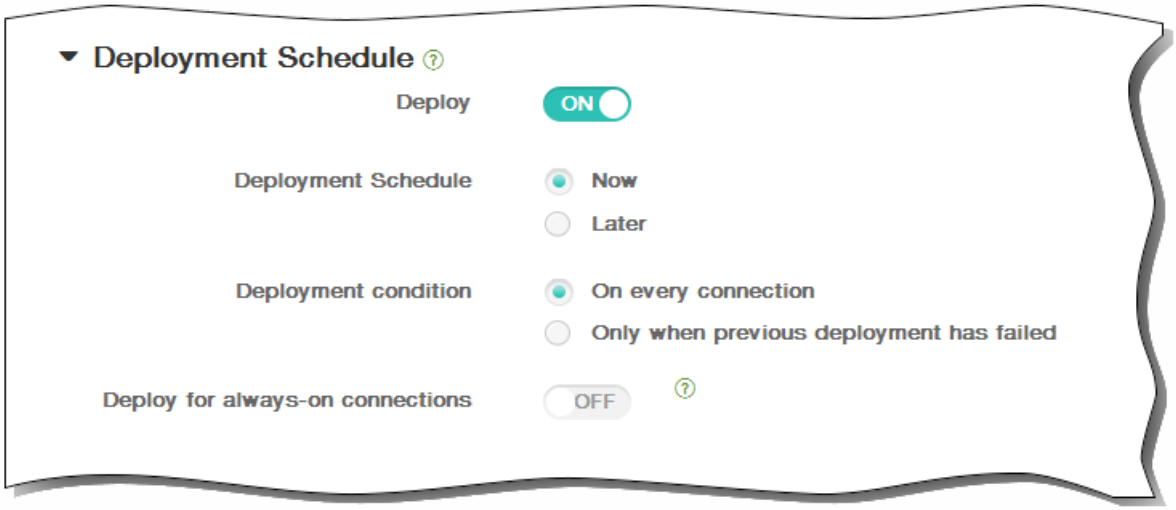


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.



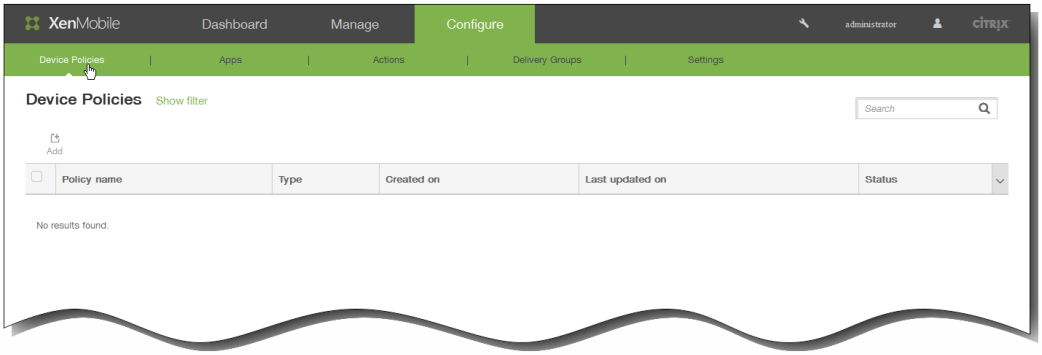
15. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie d'informations sur l'organisation pour iOS

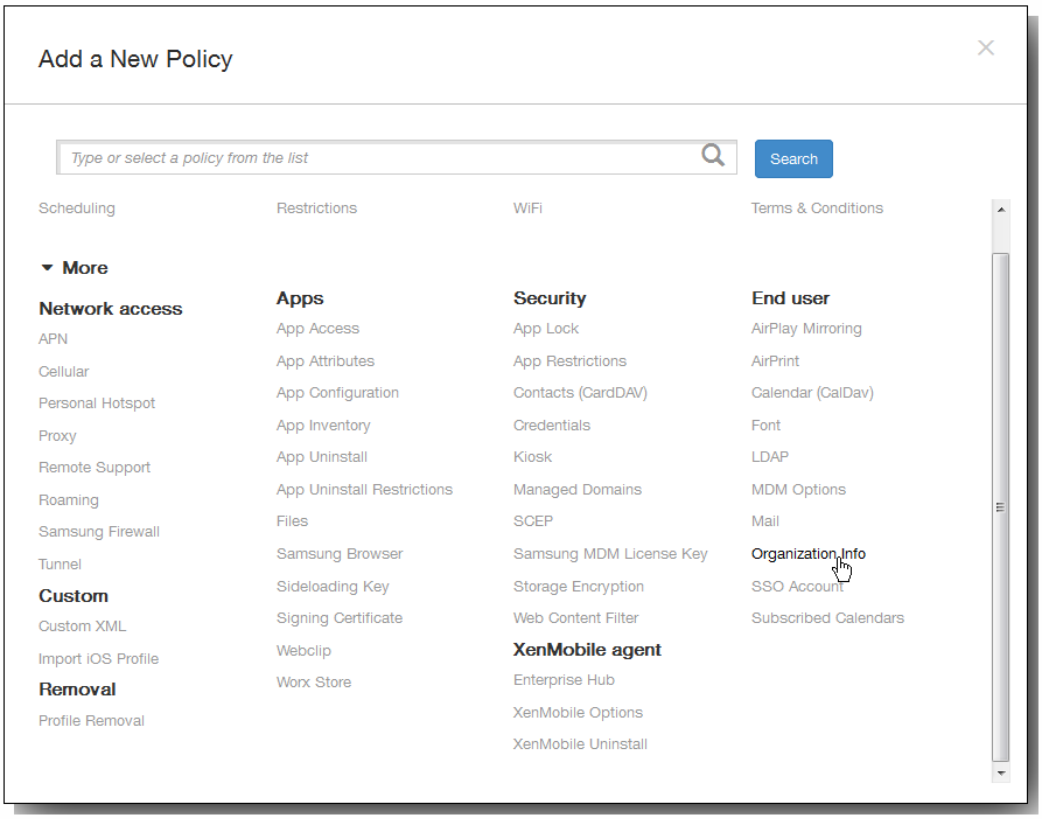
May 06, 2016

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.

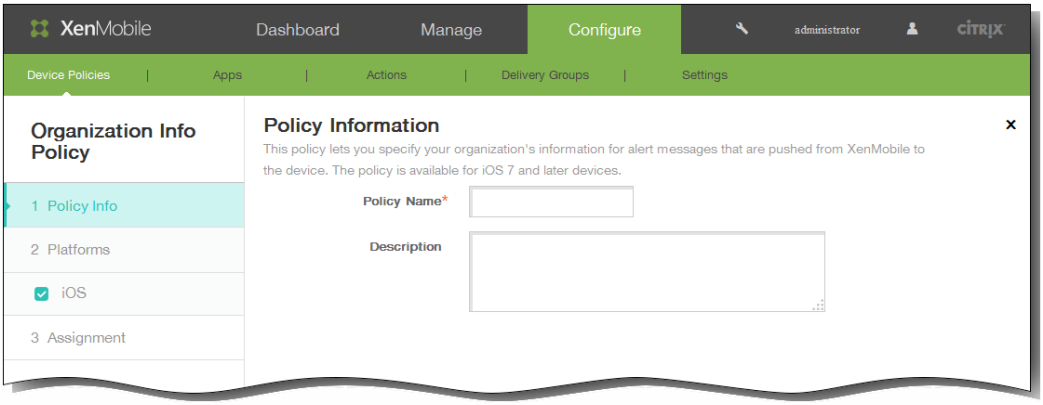
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



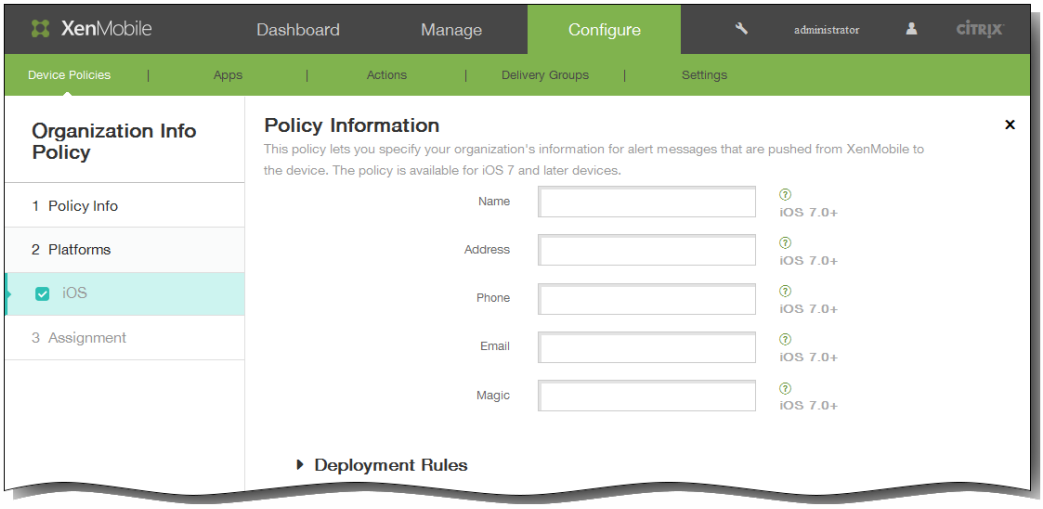
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Info organisation. La page Stratégie d'informations sur l'organisation s'affiche.

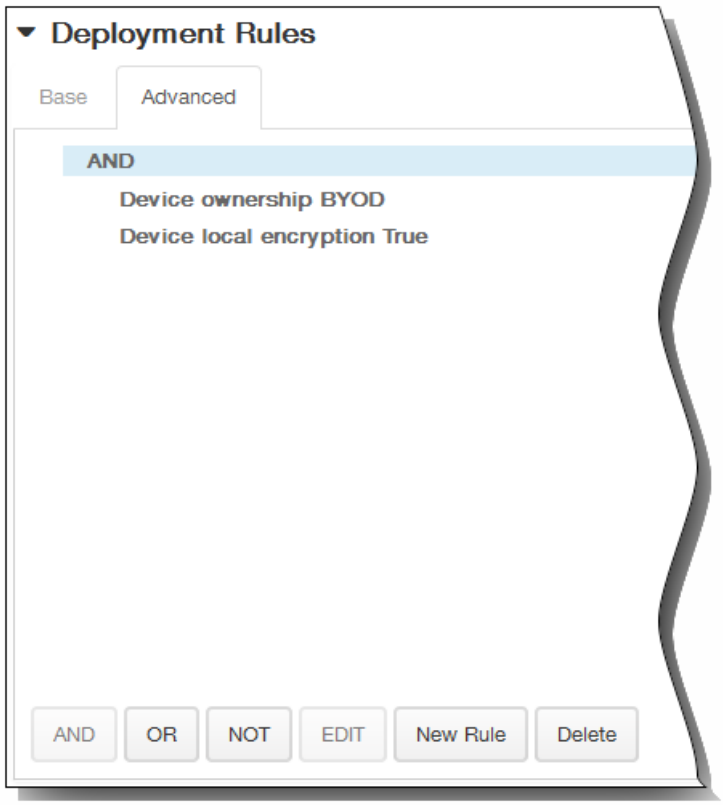


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS 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.

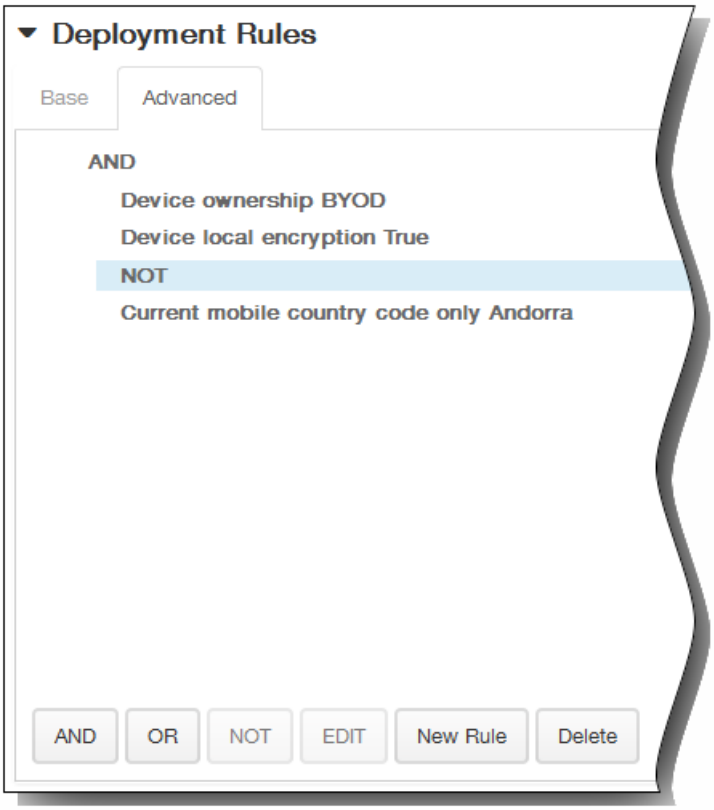
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



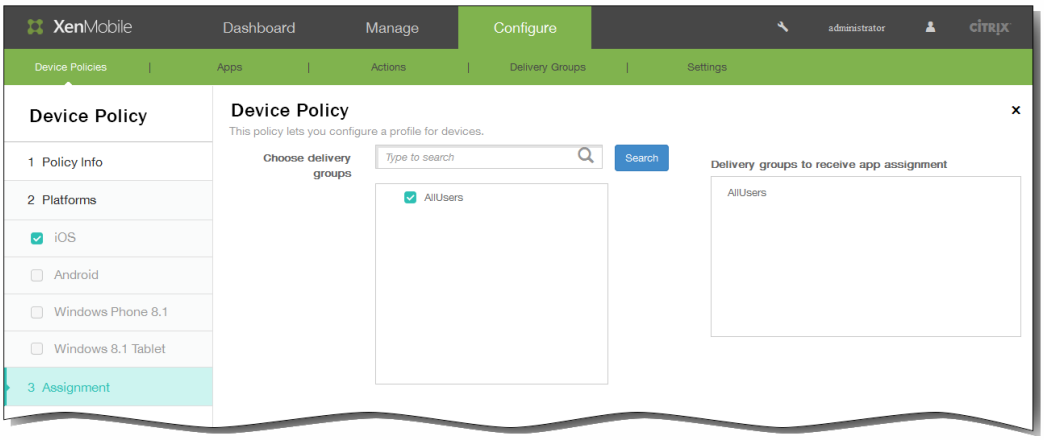
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



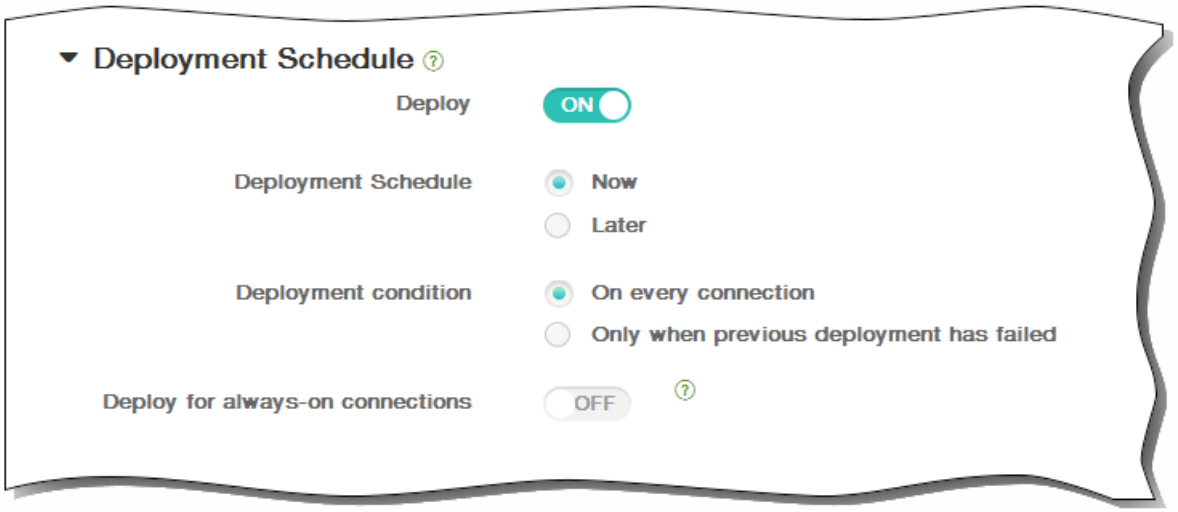
8. Cliquez sur Suivant. La page d'attribution de la Stratégie d'informations sur l'organisation s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer 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.
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.

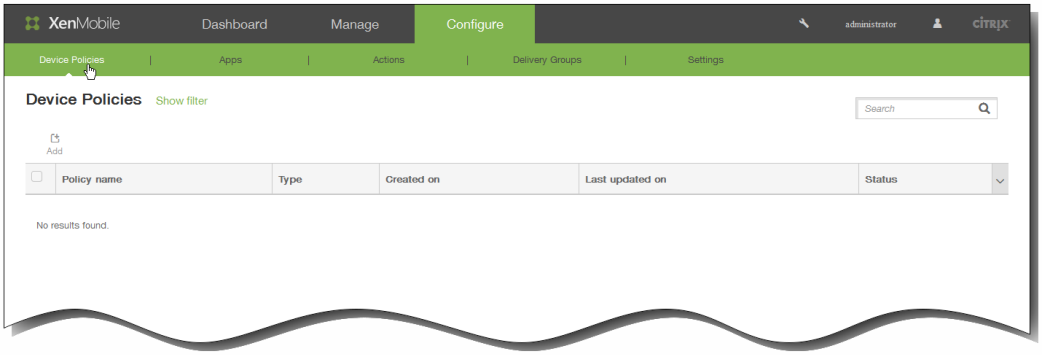
Pour ajouter une stratégie LDAP pour iOS

May 06, 2016

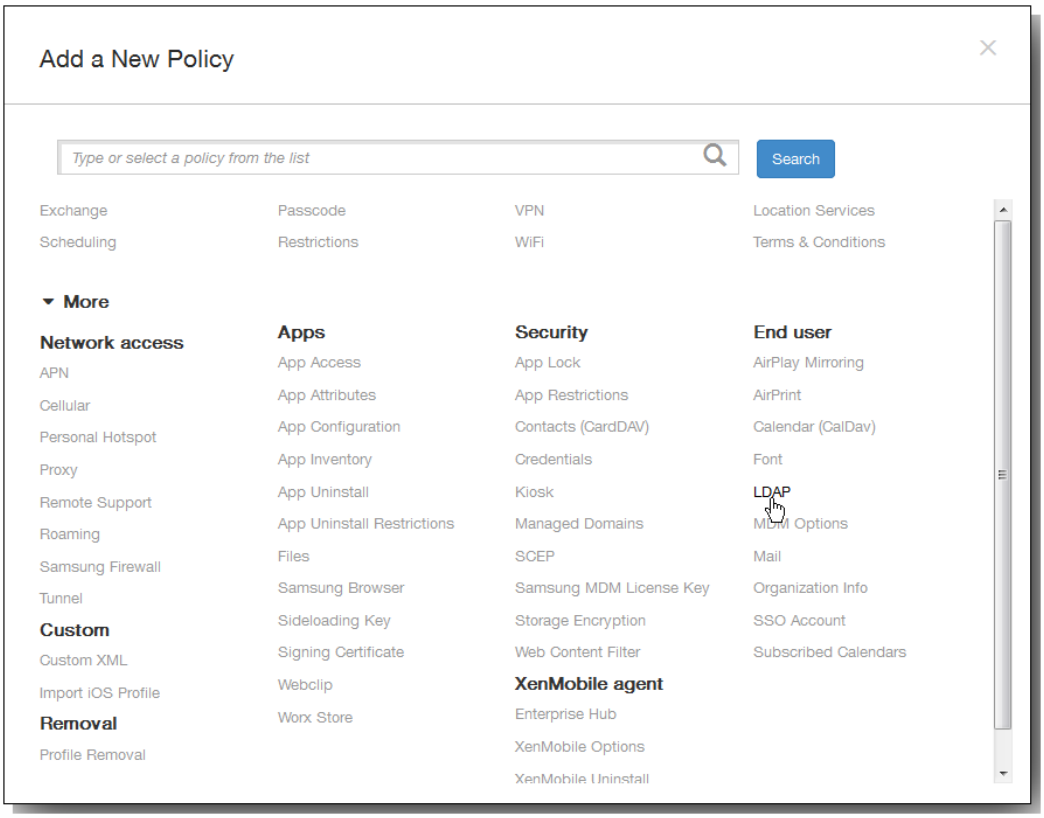
Vous créez une stratégie LDAP pour appareils iOS dans XenMobile pour fournir des informations sur un serveur LDAP à utiliser, y compris toute information sur le compte nécessaires. La stratégie fournit également un ensemble de stratégies de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP.

Vous devez utiliser le nom d'hôte LDAP avant de configurer cette stratégie.

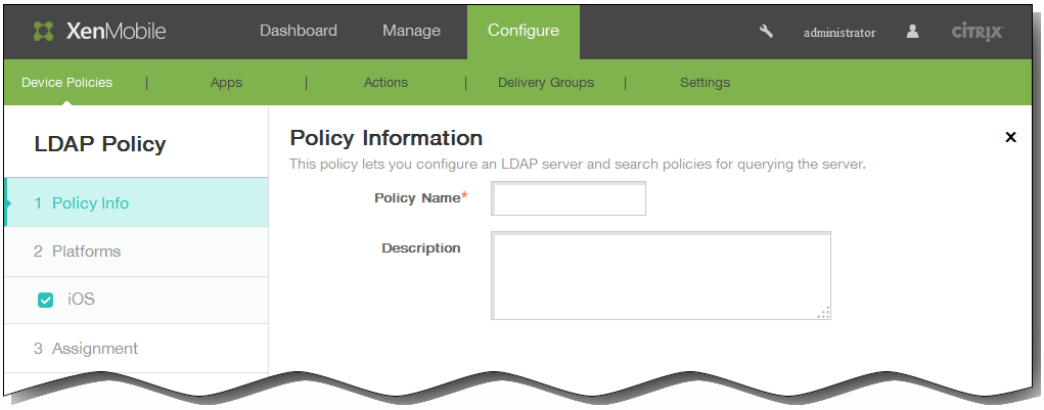
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



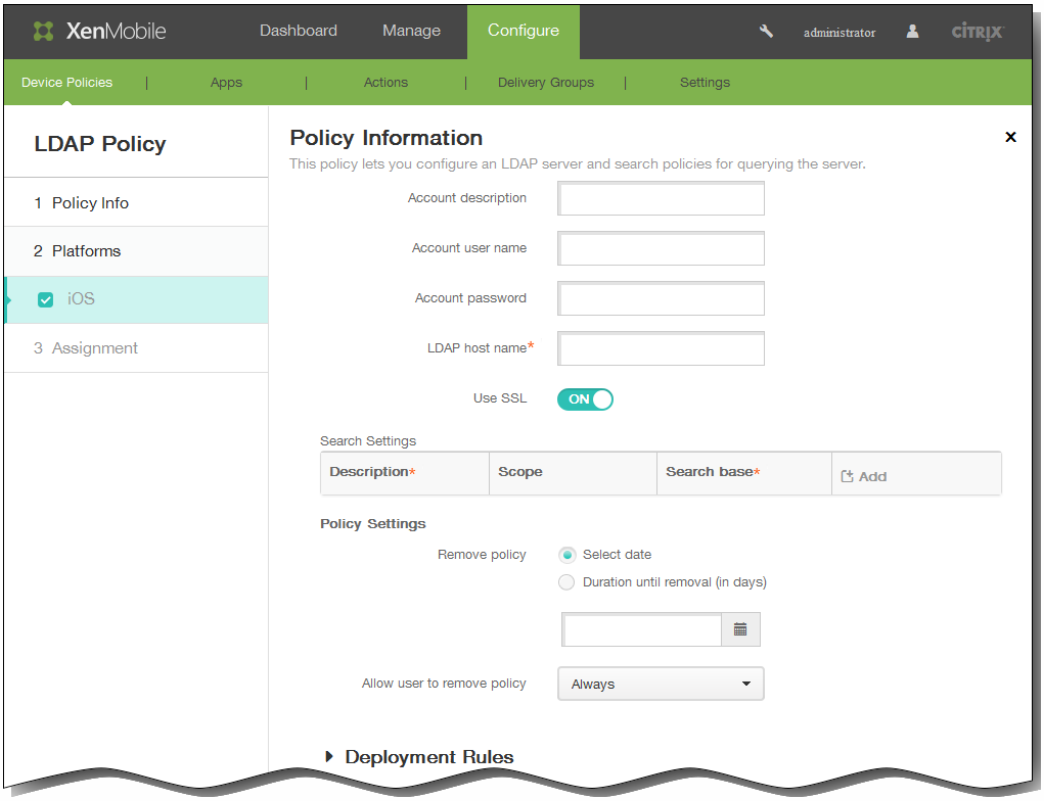
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur LDAP. La page Stratégie LDAP s'affiche.



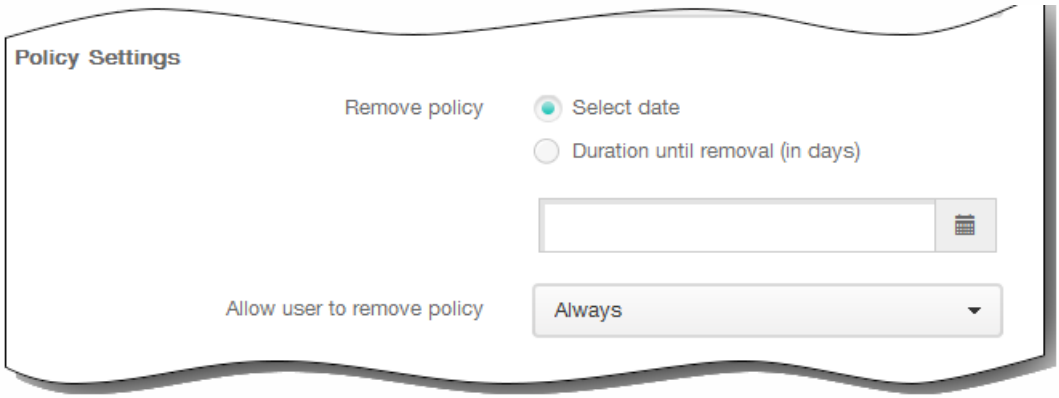
4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Plate-forme iOS s'affiche.



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.

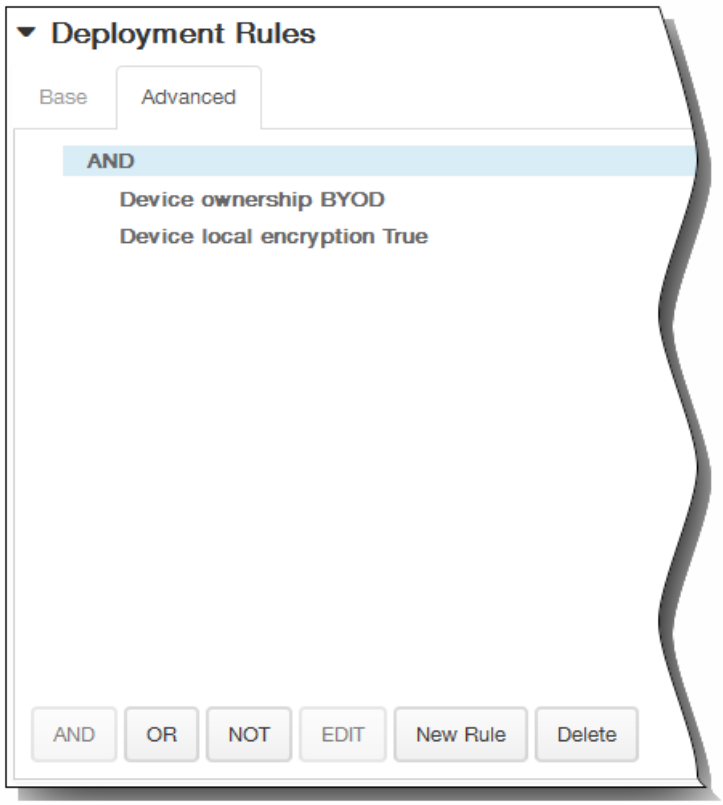
5. Utiliser SSL : sélectionnez cette option si vous souhaitez utiliser une connexion SSL au serveur LDAP. La valeur par défaut est ON.
6. Paramètres de recherche : cliquez sur Ajouter et procédez comme suit :
   Remarque : vous pouvez entrer autant de paramètres de recherche que vous voulez, mais vous 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.

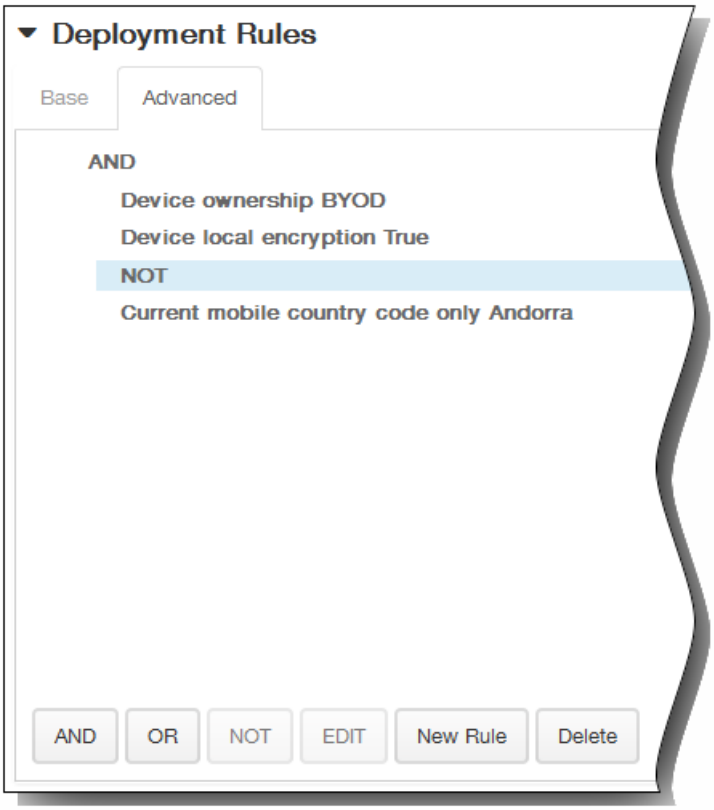
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



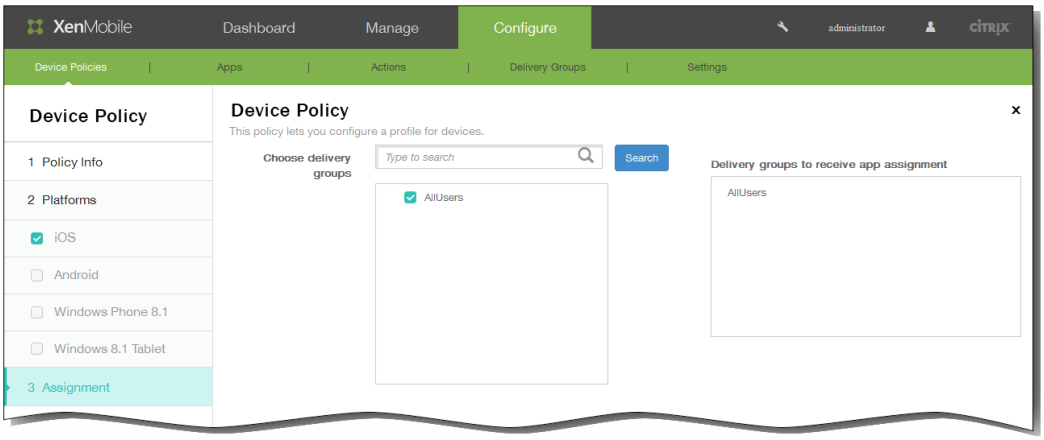
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



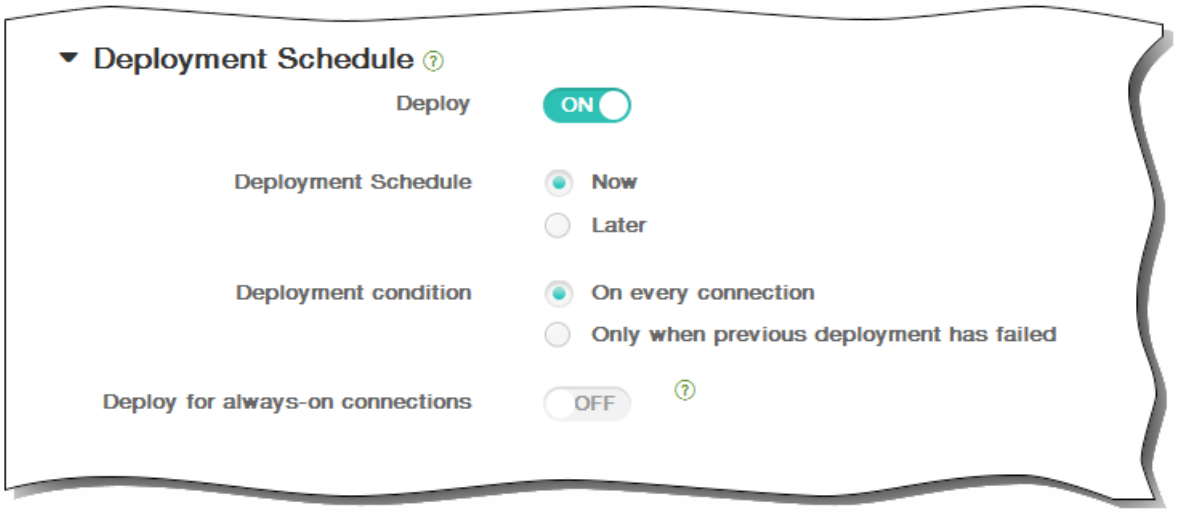
12. Cliquez sur Suivant. La page d'attribution de la Stratégie LDAP s'affiche.
13. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes 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.
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.

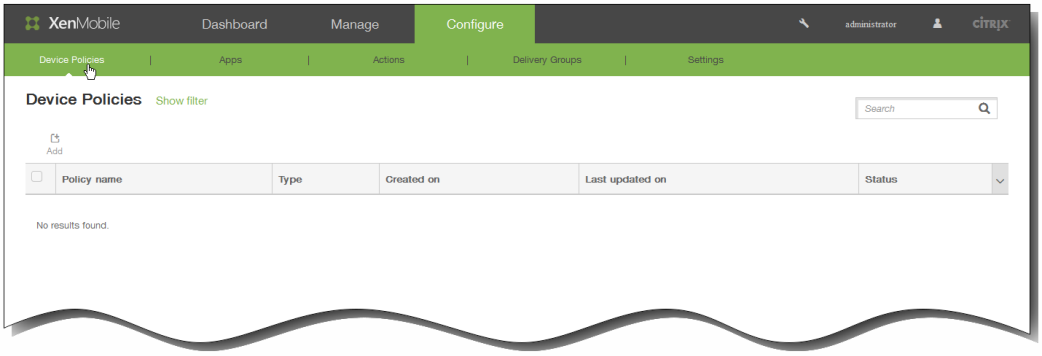
Pour ajouter une stratégie de compte SSO pour iOS

May 06, 2016

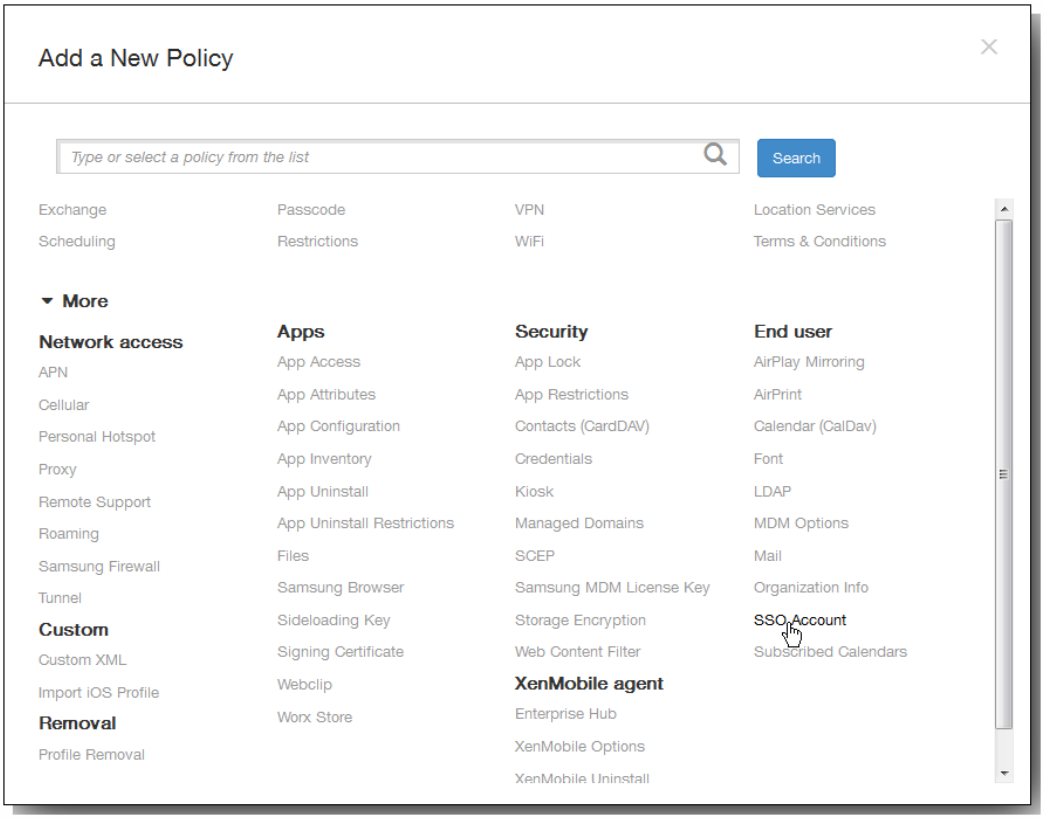
Vous créez des comptes SSO dans XenMobile pour permettre aux utilisateurs de s'authentifier une seule fois pour accéder à XenMobile et à vos ressources d'entreprise internes à partir de différentes applications. Les utilisateurs n'ont pas à stocker d'informations d'identification sur l'appareil. Les 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.

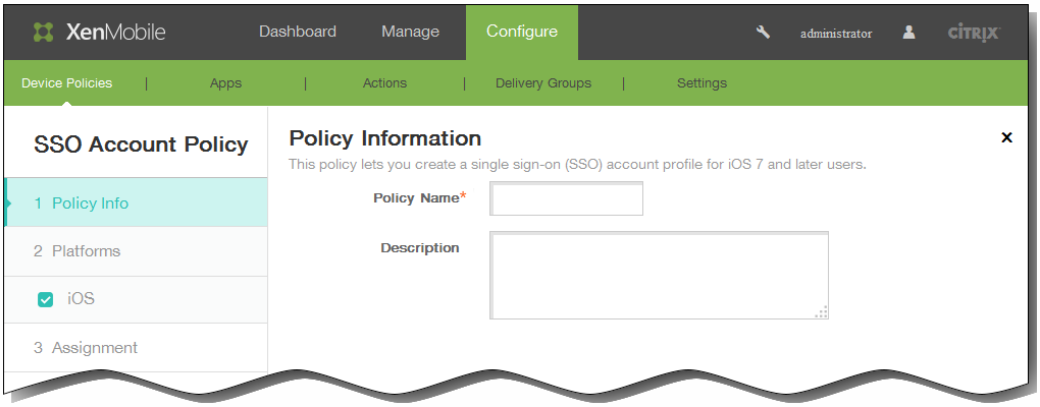
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



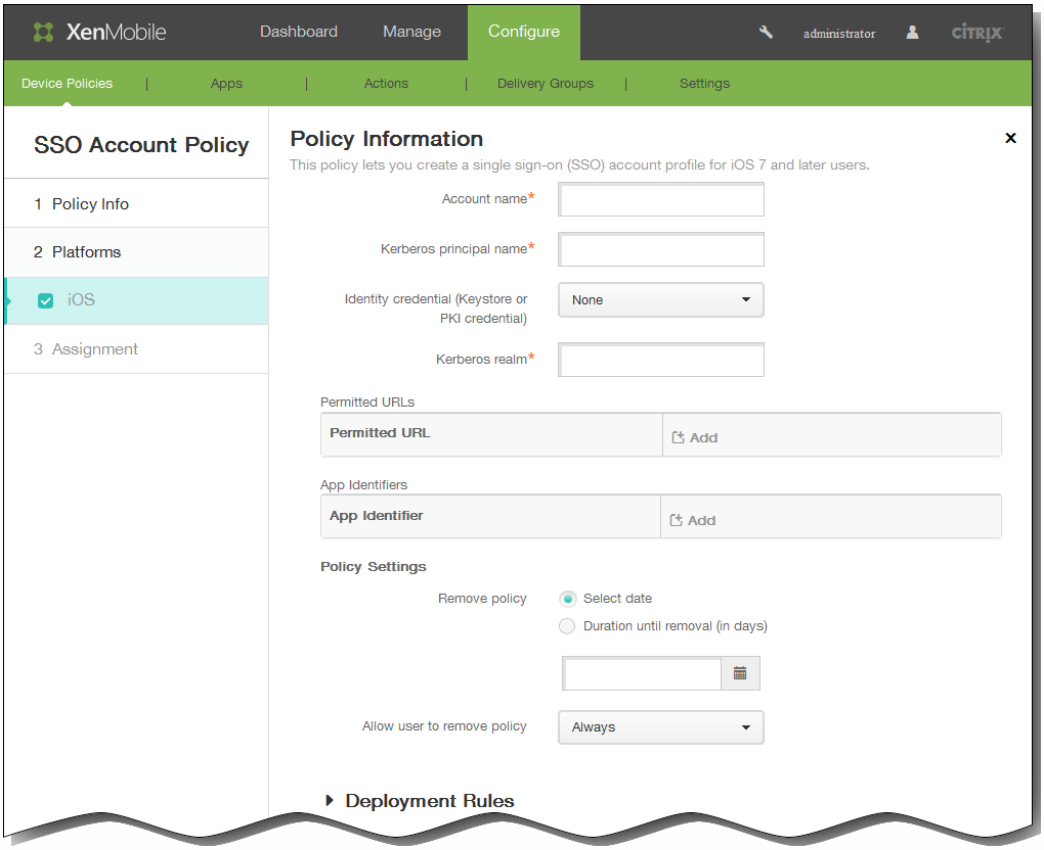
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



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.



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.

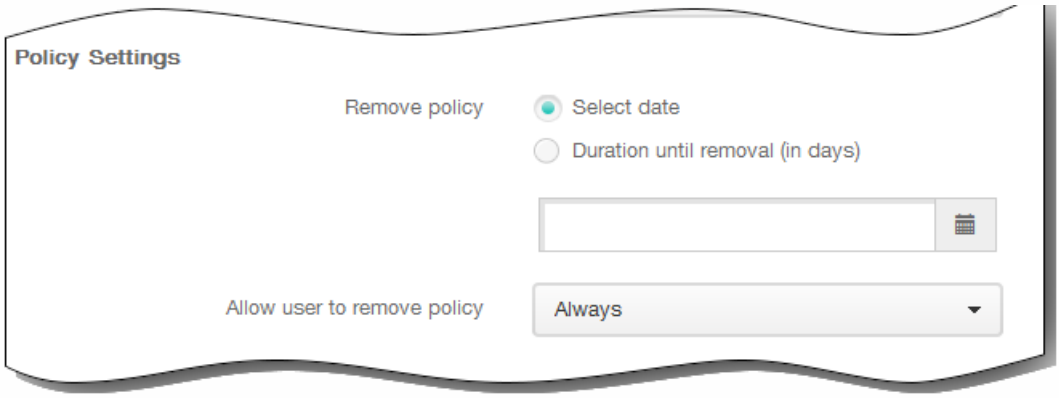
        2. Cliquez sur Ajouter pour ajouter l'URL, ou cliquez sur Annuler pour annuler l'ajout de l'URL.
        3. Répétez les étapes i et ii pour chaque adresse URL que vous souhaitez ajouter.
    6. Identifiants application : cliquez sur Ajouter, puis effectuez les opérations suivantes :

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.

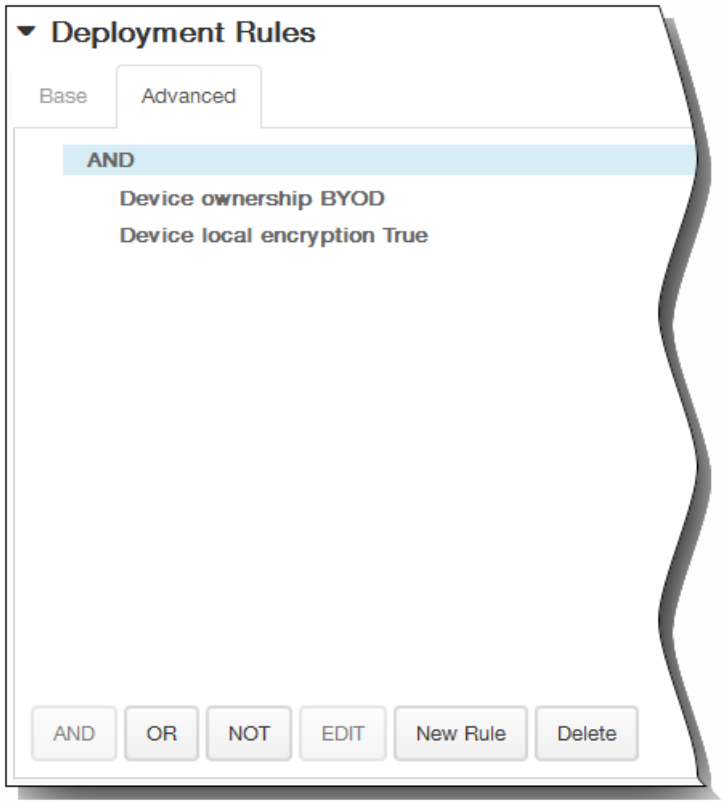


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

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.

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.

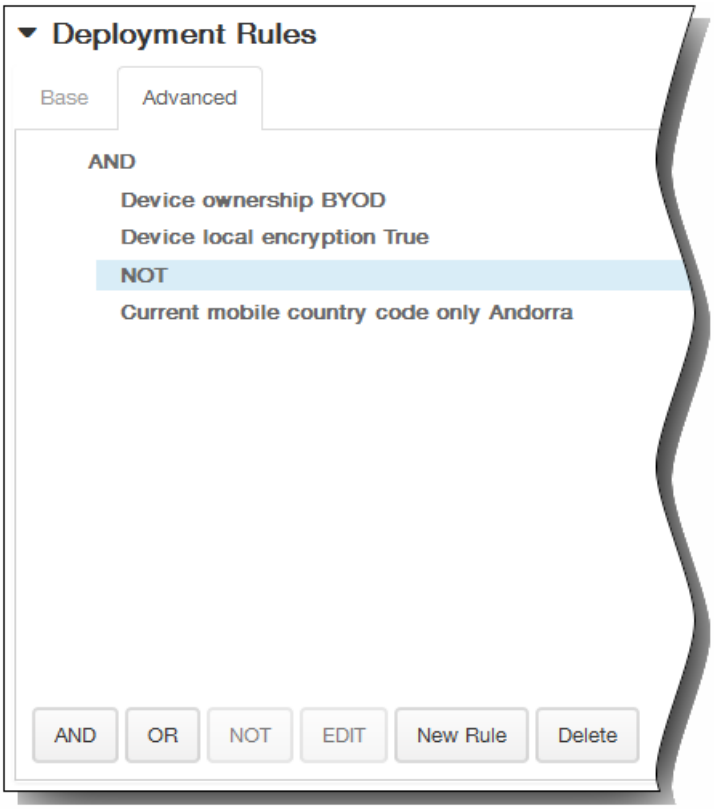
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



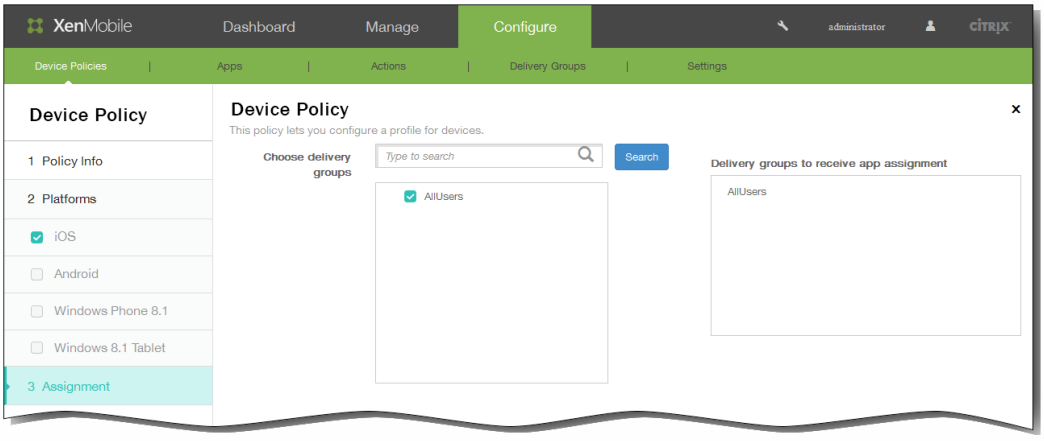
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

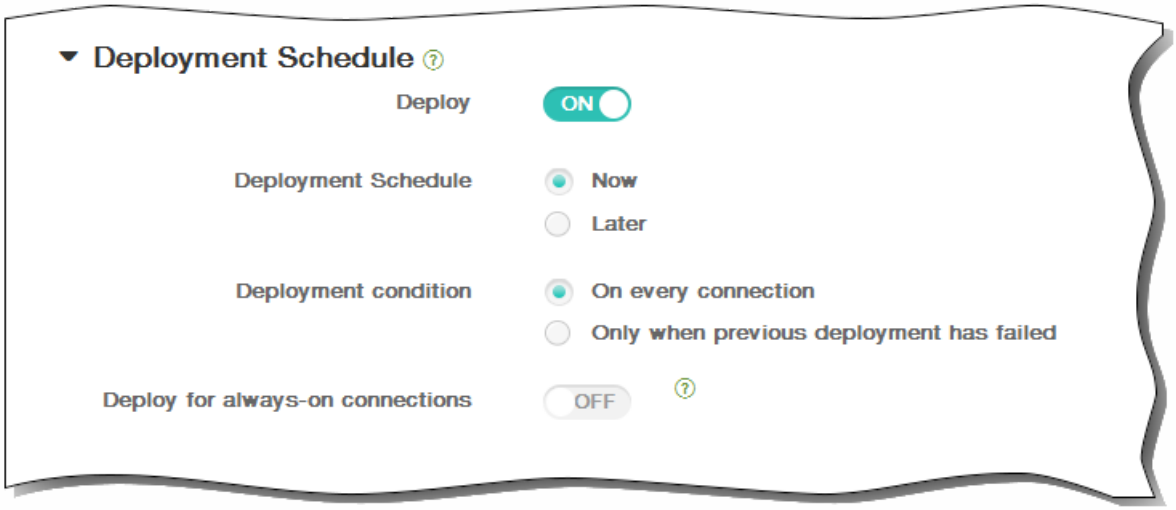


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

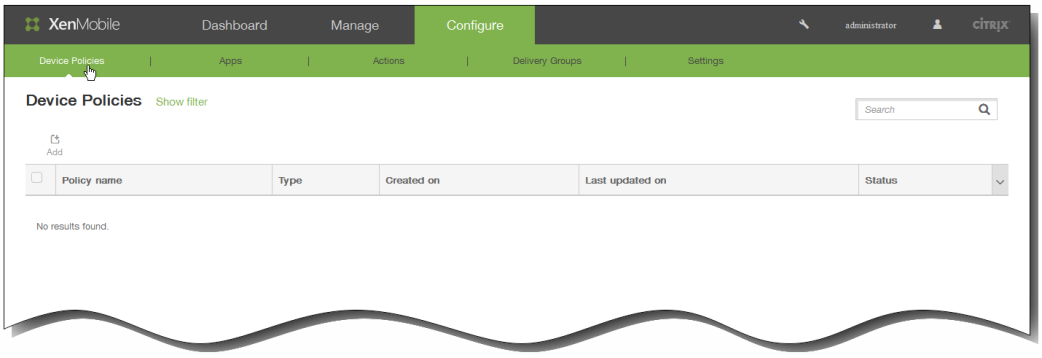
Pour ajouter une stratégie d'abonnements calendriers pour iOS

May 06, 2016

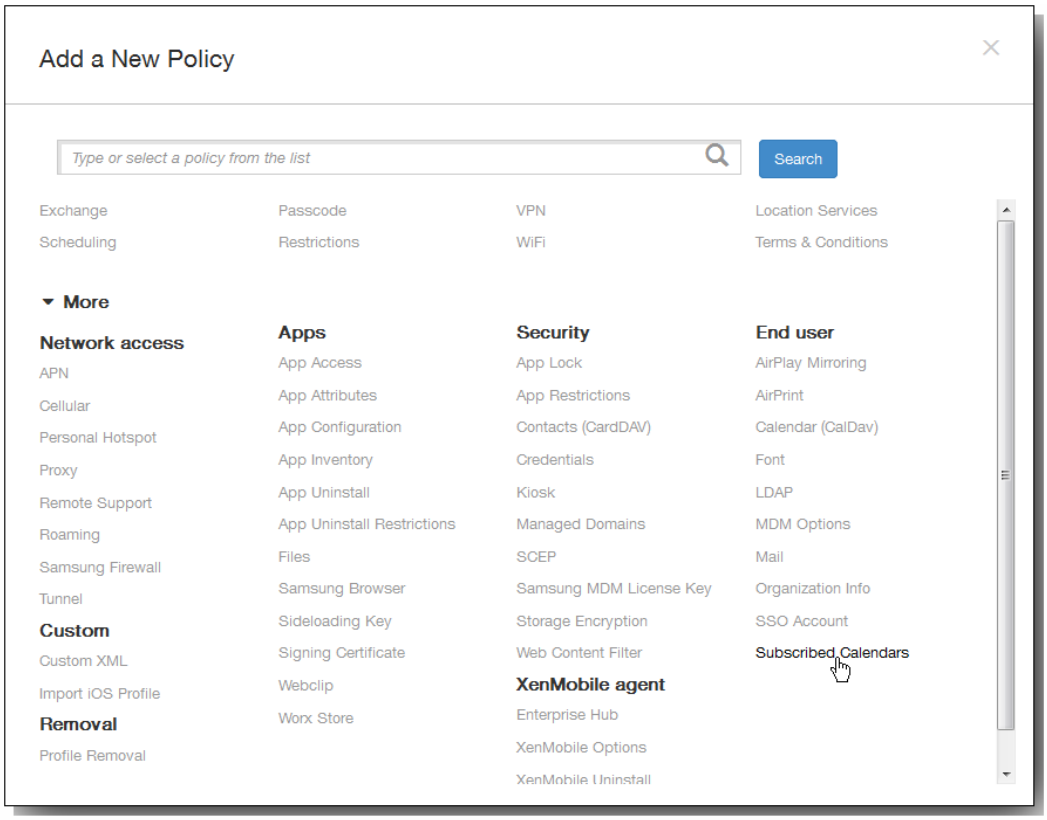
Vous pouvez ajouter une stratégie d'appareil dans XenMobile afin d'ajouter un abonnement calendrier à la liste des calendriers sur les appareils iOS des utilisateurs. La liste des calendriers publics auxquels vous pouvez vous abonner est disponible sur www.apple.com/downloads/macosx/calendars.

Remarque : vous devez être abonné à un calendrier avant de pouvoir l'ajouter à la liste des abonnements calendriers sur les appareils des utilisateurs.

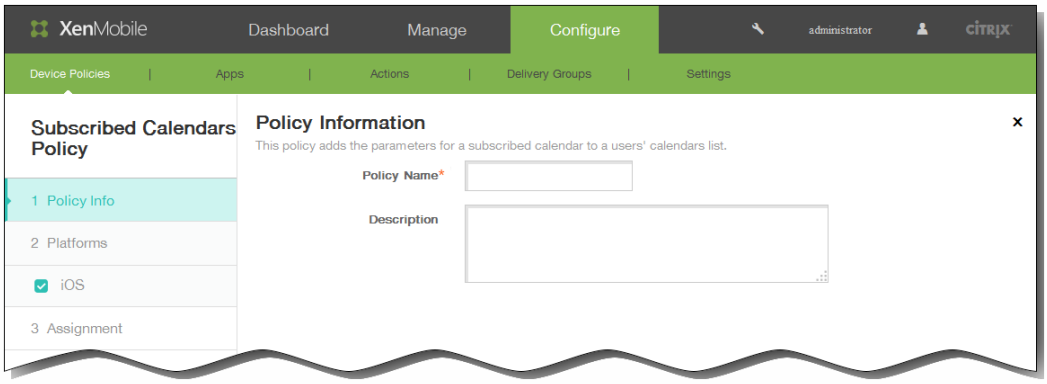
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



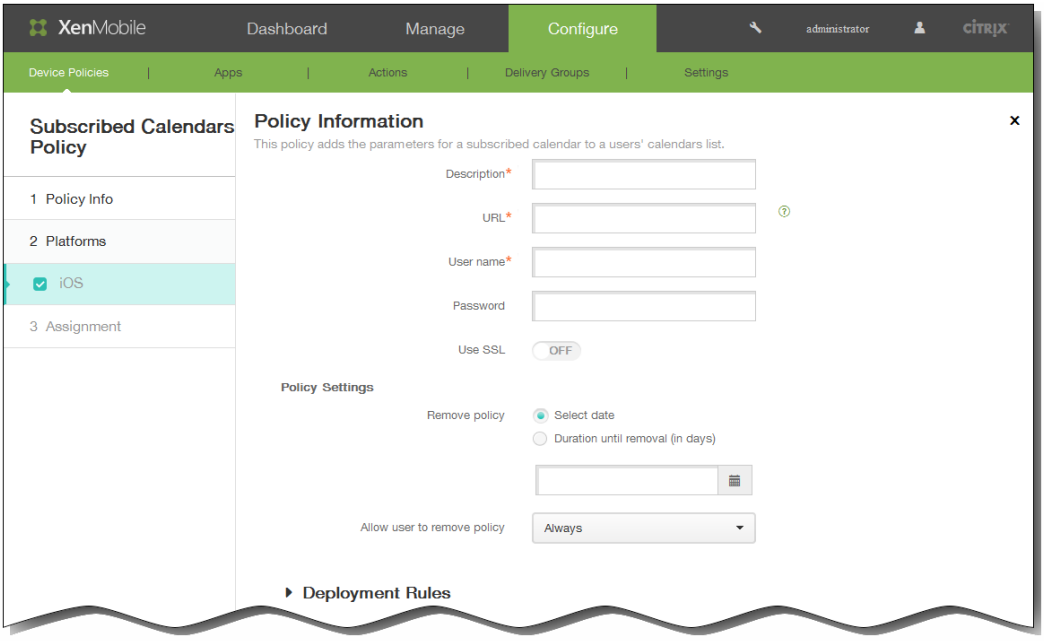
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



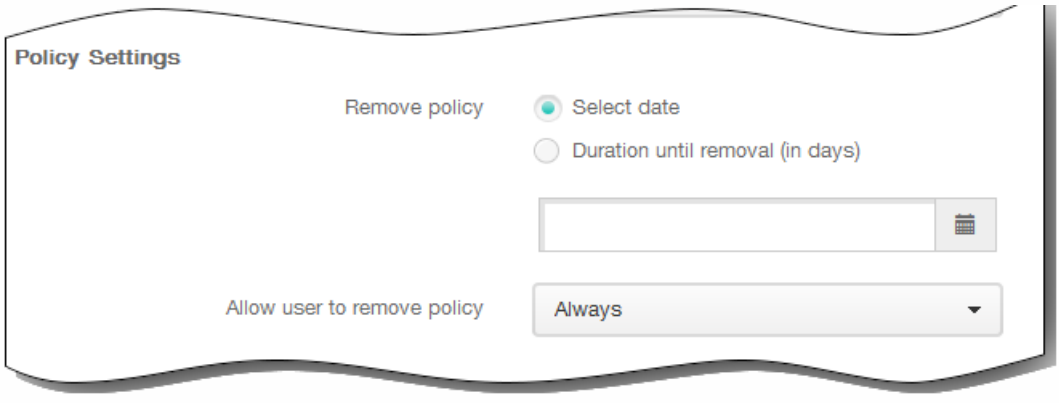
3. Cliquez sur Plus, puis, sous Utilisateur final, cliquez sur Abonnements calendriers. La page Stratégie d'abonnements calendriers s'affiche.



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.

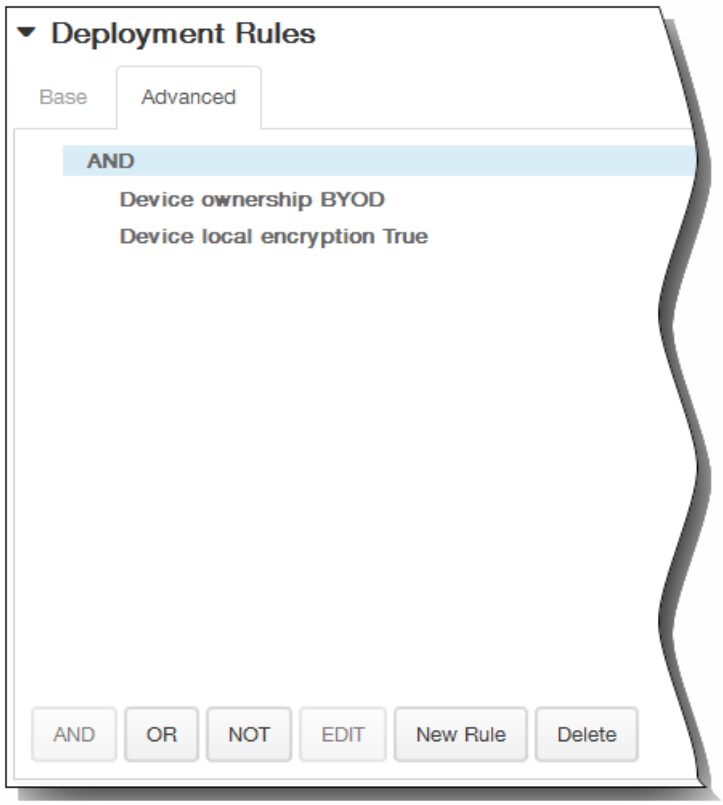


6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Description : entrez une description pour le calendrier. Ce champ est obligatoire.
   2. URL : entrez l'URL du calendrier. Vous pouvez entrer une URL webcal:// ou un lien http:// vers un fichier iCalendar (.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.

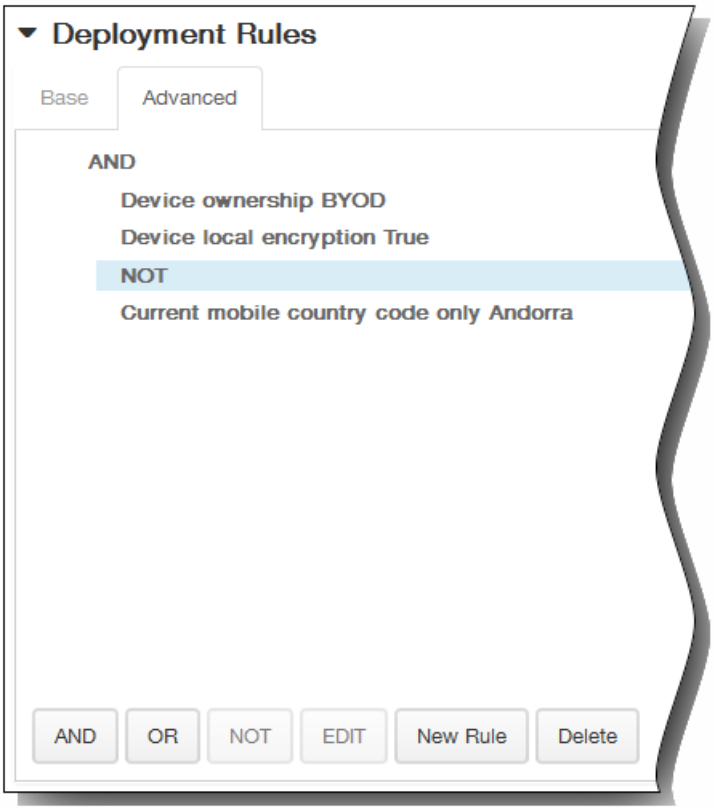
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



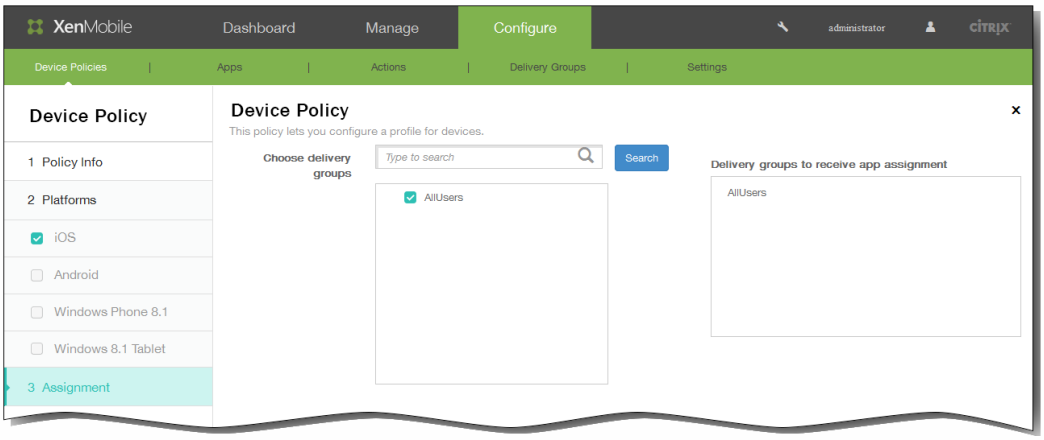
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



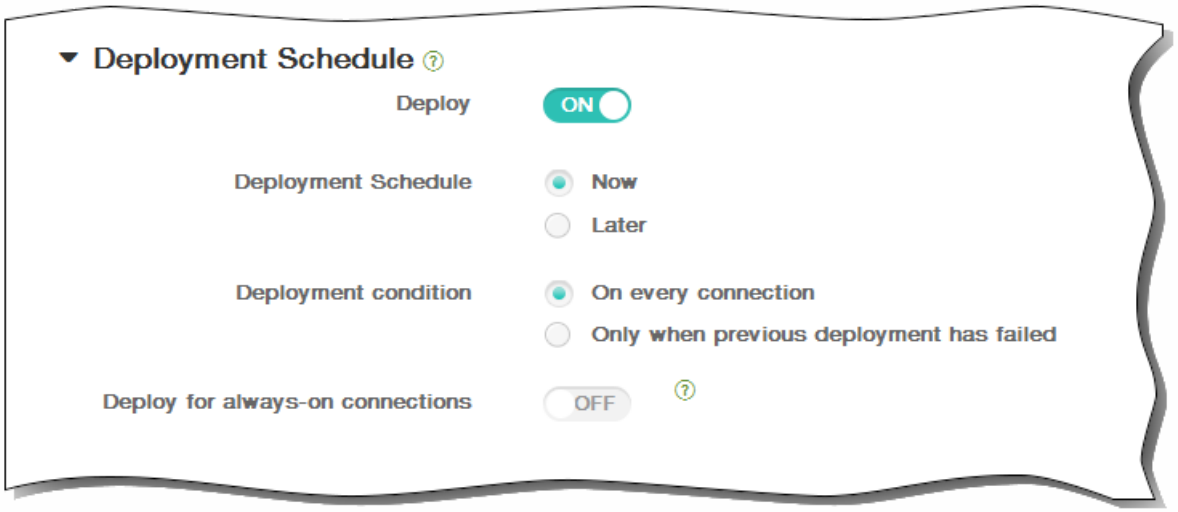
12. Cliquez sur Suivant. La page d'attribution de la Stratégie d'abonnements calendriers s'affiche.
13. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la 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. 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.



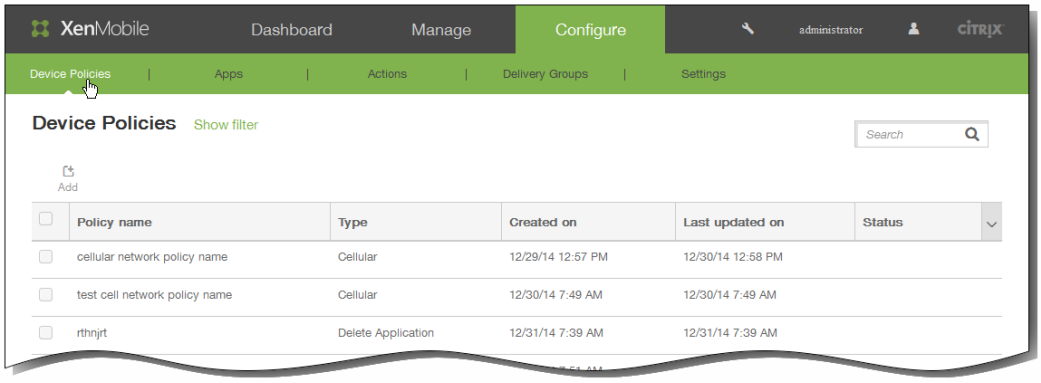
15. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de code secret

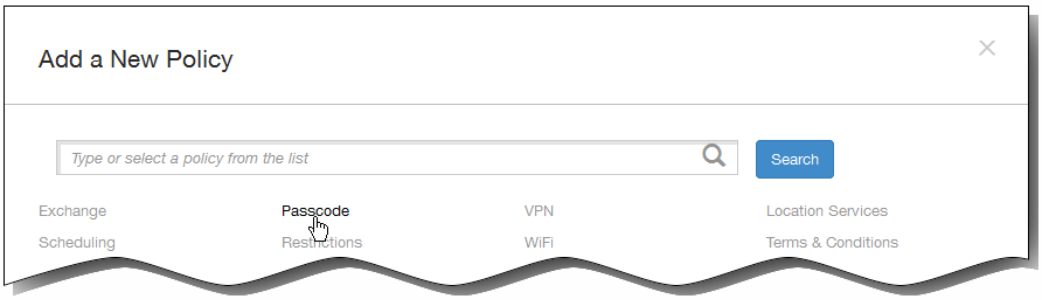
May 06, 2016

Vous créez une stratégie de code secret dans XenMobile en fonction des normes de votre organisation. Vous pouvez exiger la saisie de codes secrets sur les appareils des utilisateurs et définir diverses règles de code secret et de formatage. Vous pouvez créer des stratégies pour iOS, Android, Samsung KNOX, Windows Phone 8.1 et Windows 8.1 Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

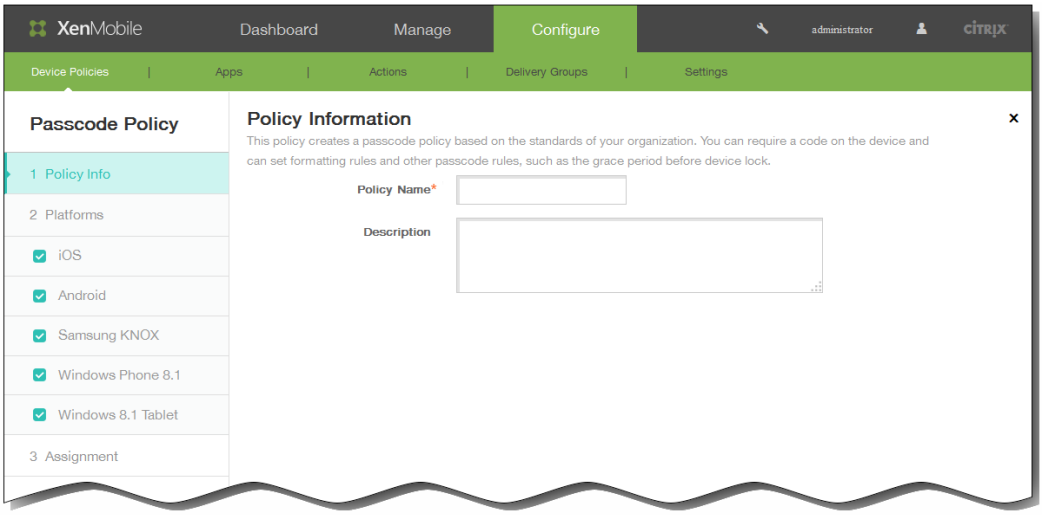
1. Dans la console XenMobile, cliquez sur ConfigurerStratégies d'appareil. La page Stratégies d'appareil s'affiche. Cliquez sur Ajouter pour ajouter une nouvelle stratégie.



2. Sur la page Ajouter une nouvelle stratégie, cliquez sur Code secret.

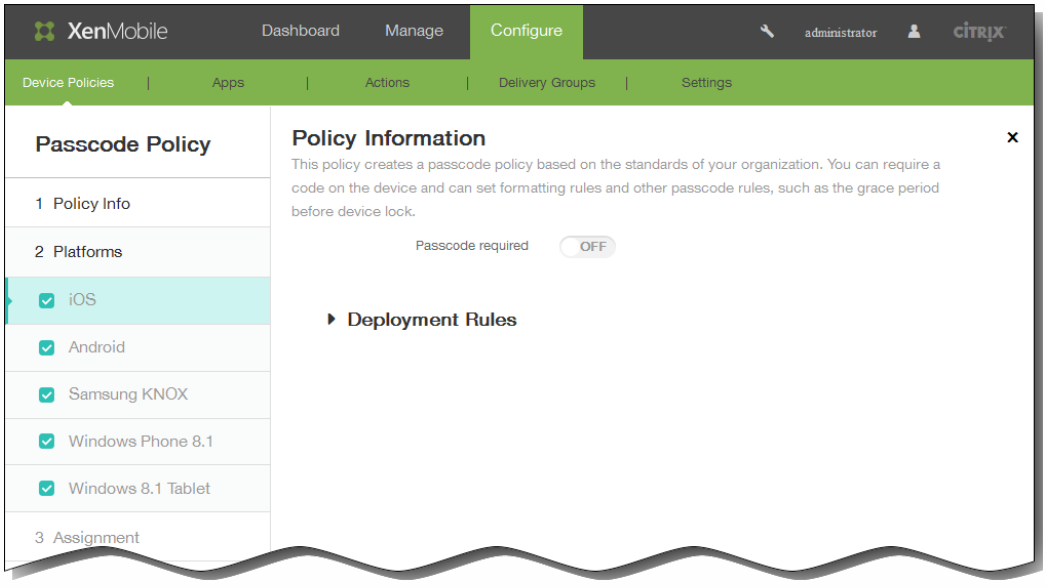


3. Dans la section Informations sur la stratégie, entrez les informations suivantes :

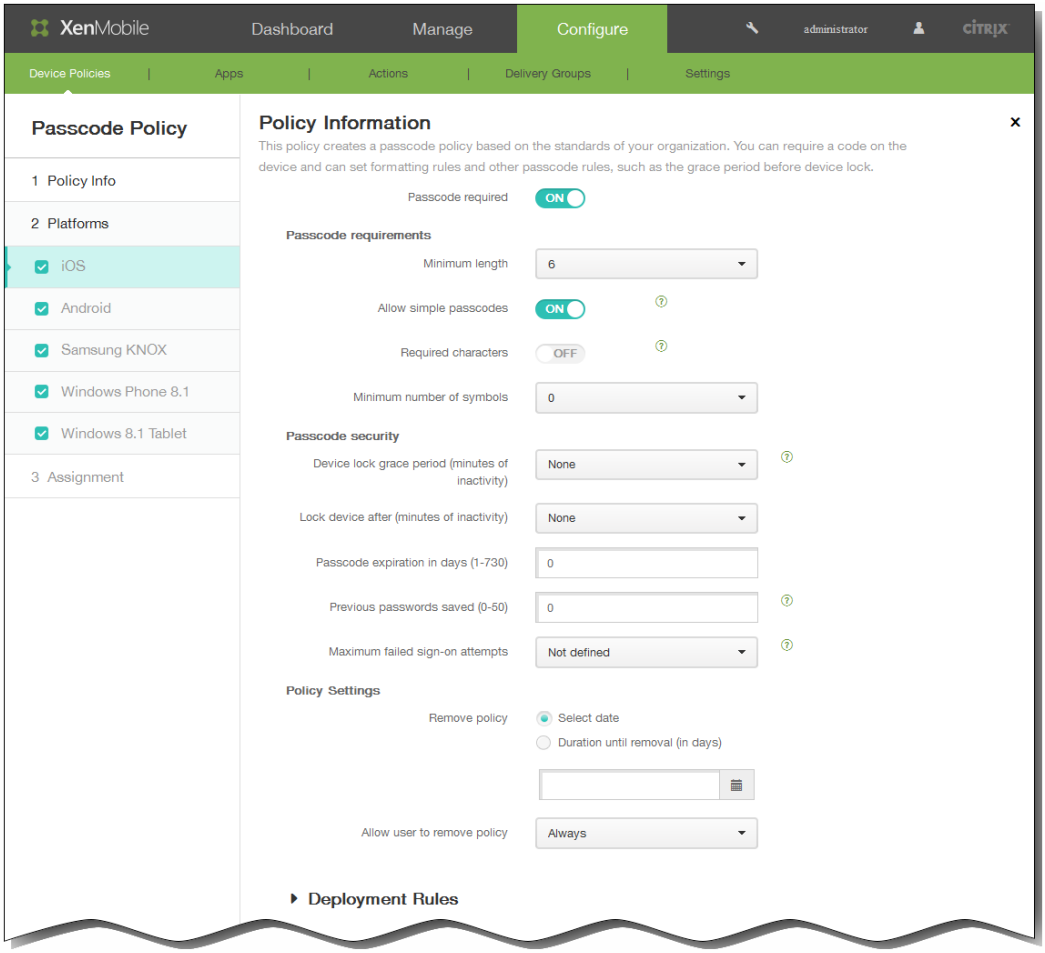


1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
2. Description : entrez une description pour la stratégie (facultatif).
3. Cliquez sur Suivant.

4. Sous Plates-formes, sélectionnez les plates-formes pour lesquelles vous voulez configurer cette stratégie.
   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.



- Si vous avez sélectionné iOS, configurez les paramètres suivants :



Code secret requis : sélectionnez cette option pour exiger la saisie d'un mot de passe et afficher les options de configuration d'une stratégie de code secret pour iOS. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité et paramètres de stratégie.

Conditions requises pour les codes secrets

Longueur minimale : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de 6.

Autoriser les codes secrets simples : sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est ON.

Caractères requis : sélectionnez cette option pour exiger que les codes secrets contiennent au moins une lettre. La valeur par défaut est OFF.

Nombre minimum de symboles : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir.

Sécurité des codes secrets

Période de grâce avant verrouillage de l'appareil (minutes d'inactivité) : dans la liste, cliquez sur la durée après laquelle les utilisateurs doivent entrer un code secret pour déverrouiller un appareil verrouillé. La valeur par défaut est Aucune.

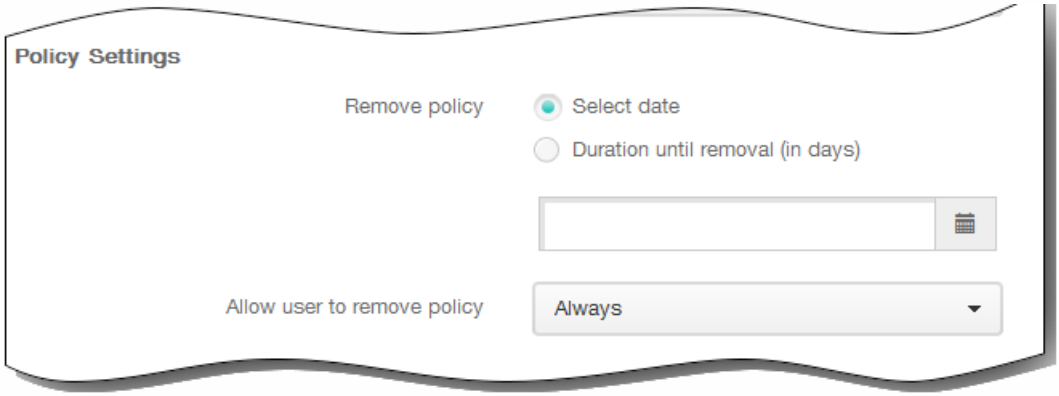
Verrouiller l'appareil après (minutes d'inactivité) : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est Aucune.

Expiration du code secret en jours (1 - 730) : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est 0, ce qui signifie que le code secret n'expire jamais.

Mots de passe précédents enregistrés (0-50) : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.

Nombre maximum de tentatives de connexion infructueuses : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil subit un effacement complet. La valeur par défaut est Aucun nombre défini.

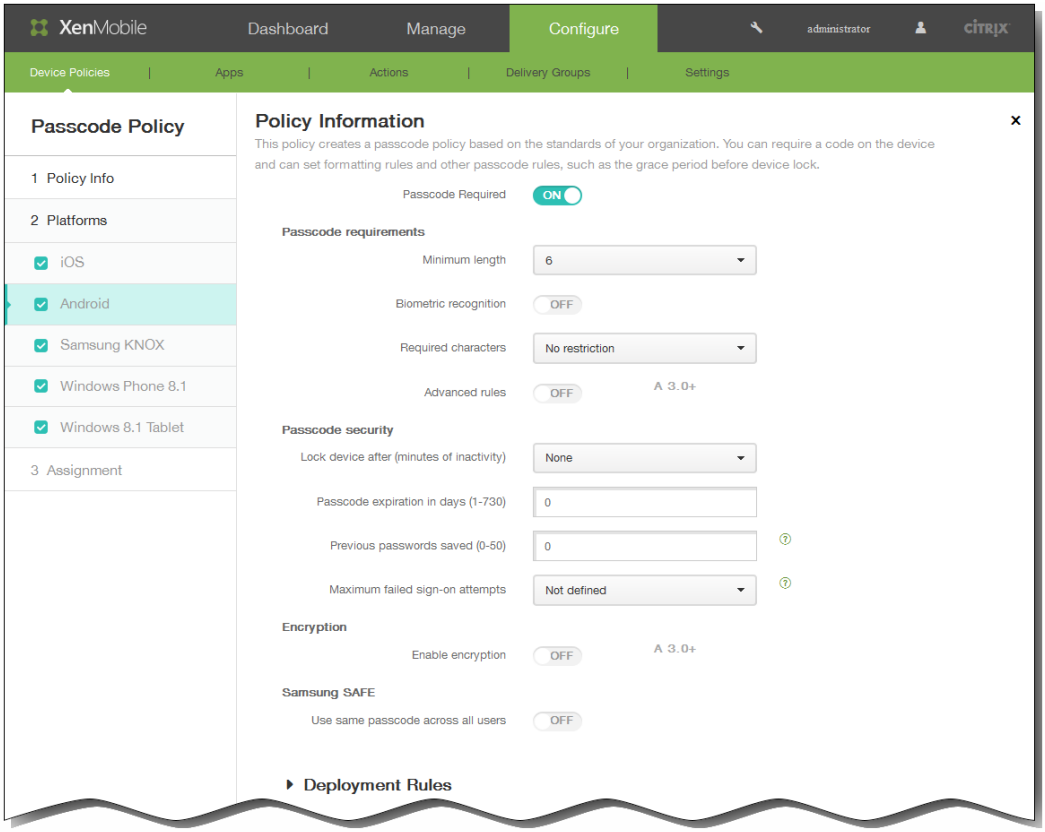
Paramètres de stratégie



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 :

  Remarque : le paramètre par défaut pour Android est OFF. La page se développe pour vous permettre de configurer les paramètres relatifs aux exigences en matière de code secret, sécurité du code secret, chiffrement et Samsung SAFE.



Conditions requises pour les codes secrets

Longueur minimale : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de 6.

Reconnaissance biométrique : sélectionnez cette option pour activer la reconnaissance biométrique. Si vous activez cette option, le champ Caractères requis est masqué. La valeur par défaut est OFF.

Caractères requis : dans la liste, cliquez sur Aucune restriction, Chiffres et lettres, Chiffres uniquement ou Lettres uniquement pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est Aucune restriction.

Règles avancées : sélectionnez cette option si vous souhaitez appliquer des règles de code secret avancées. Cette option est disponible pour Android 3.0 et versions ultérieures. La valeur par défaut est OFF.

Lorsque le paramètre Règles avancées est défini sur ON, à partir de chacune des listes suivantes et pour chaque type de caractère, cliquez sur le nombre minimal de caractère qu'un code secret doit contenir :

- Symboles : nombre minimal de symboles.
- Lettres : nombre minimal de lettres.
- Minuscules : nombre minimum de minuscules.
- Majuscules : nombre minimum de majuscules.
- Chiffres ou symboles : nombre minimal de chiffres ou de symboles.
- Chiffres : nombre minimal de chiffres.

Sécurité des codes secrets

Verrouiller l'appareil après (minutes d'inactivité) : dans la liste, cliquez sur la durée pendant laquelle un appareil peut

rester inactif avant d'être verrouillé. La valeur par défaut est Aucune.

Expiration du code secret en jours (1 - 730) : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est 0, ce qui signifie que le code secret n'expire jamais.

Mots de passe précédents enregistrés (0-50) : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.

Nombre maximum de tentatives de connexion infructueuses : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil subit un effacement complet. La valeur par défaut est Aucun nombre défini.

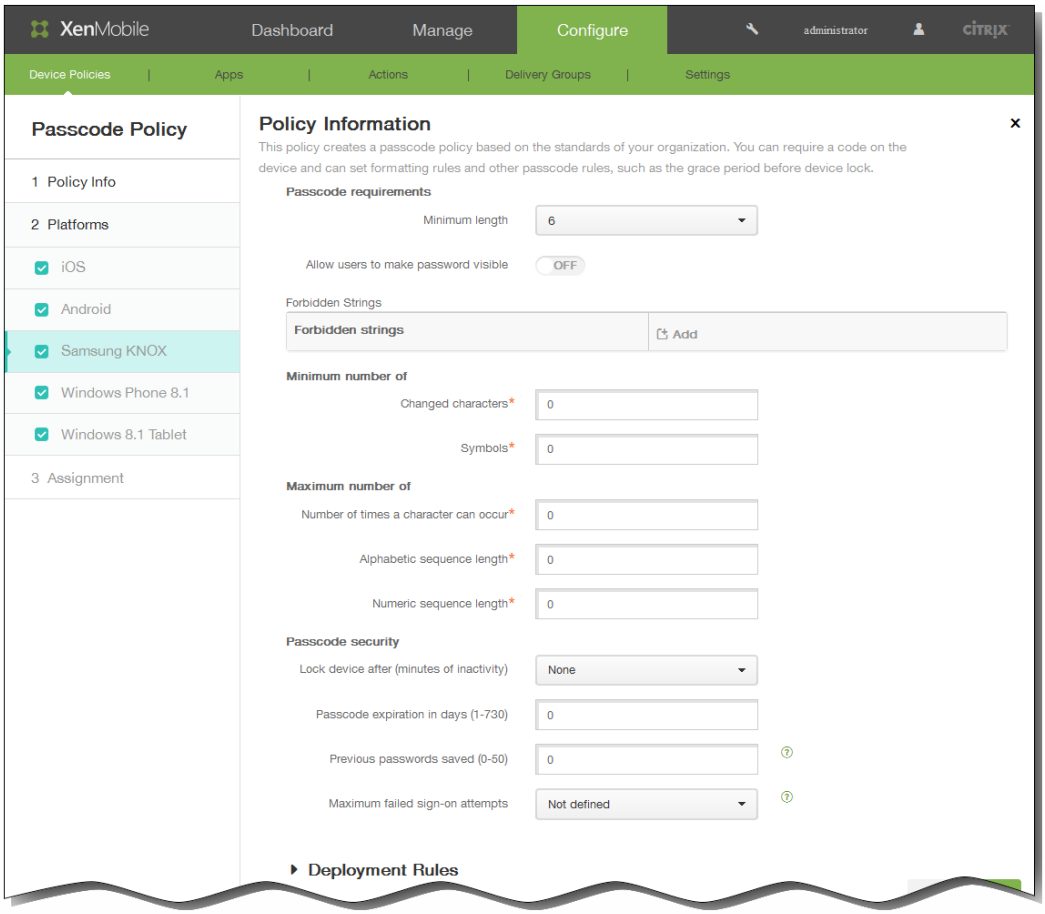
Chiffrement

Activer le chiffrement : sélectionnez cette option si vous souhaitez activer le cryptage. Cette option est disponible pour Android 3.0 et versions ultérieures. L'option est disponible, que le paramètre Code secret requis soit sélectionné ou non.

Utiliser le même code secret pour tous les utilisateurs : sélectionnez cette option si vous souhaitez utiliser le même code secret pour tous les utilisateurs. Cette option s'applique uniquement aux appareils Samsung SAFE et est disponible, que le paramètre Code secret requis soit sélectionné ou non. La valeur par défaut est OFF.

Entrez le code secret requis dans le champ qui apparaît lorsque vous activez cette option.

- Si vous sélectionnez Samsung KNOX, configurez les paramètres suivants :



Conditions requises pour les codes secrets

Longueur minimale : dans la liste, cliquez sur la longueur minimale du code secret.

Autoriser les utilisateurs à afficher les mots de passe : sélectionnez cette option pour autoriser les utilisateurs à afficher le mot de passe.

- Chaînes interdites : créez des chaînes interdites pour empêcher les utilisateurs d'utiliser des chaînes non sécurisées faciles à deviner, telles que « mot de passe », « mdp », « bienvenue », « 123456 », « 111111 », etc. Procédez comme suit :
  - **Pour ajouter une chaîne interdite**
    1. Cliquez sur Ajouter.
    2. Entrez la chaîne interdite.
    3. Cliquez sur Enregistrer pour enregistrer la chaîne ou sur Annuler pour annuler l'ajout de la chaîne.
    4. Répétez les étapes i à iii pour chaque chaîne interdite que vous souhaitez ajouter.
  - **Pour modifier une chaîne interdite**
    1. Mots de passe précédents enregistrés (0-50) : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.
    1. Placez le pointeur de la souris sur la chaîne que vous souhaitez modifier.
    2. Cliquez sur l'icône de crayon à droite de la liste.
    3. Apportez des modifications à la chaîne.

4. Cliquez sur Enregistrer pour enregistrer la chaîne ou sur Annuler pour annuler la modification de la chaîne.

Nombre minimum de

Caractères modifiés : entrez le nombre de caractères que les utilisateurs doivent changer par rapport à leur code secret précédent. La valeur par défaut est de 0.

Symboles : entrez le nombre minimum de symboles requis dans un code secret. La valeur par défaut est de 0.

Nombre maximum de

Nombre d'occurrences d'un caractère : entrez le nombre maximal d'occurrences d'un caractère dans un code secret. La valeur par défaut est de 0.

Longueur des séquences alphabétiques : entrez la longueur maximale d'une séquence alphabétique dans un code secret. La valeur par défaut est de 0.

Longueur des séquences numériques : entrez la longueur maximale d'une séquence numérique dans un code secret. La valeur par défaut est de 0.

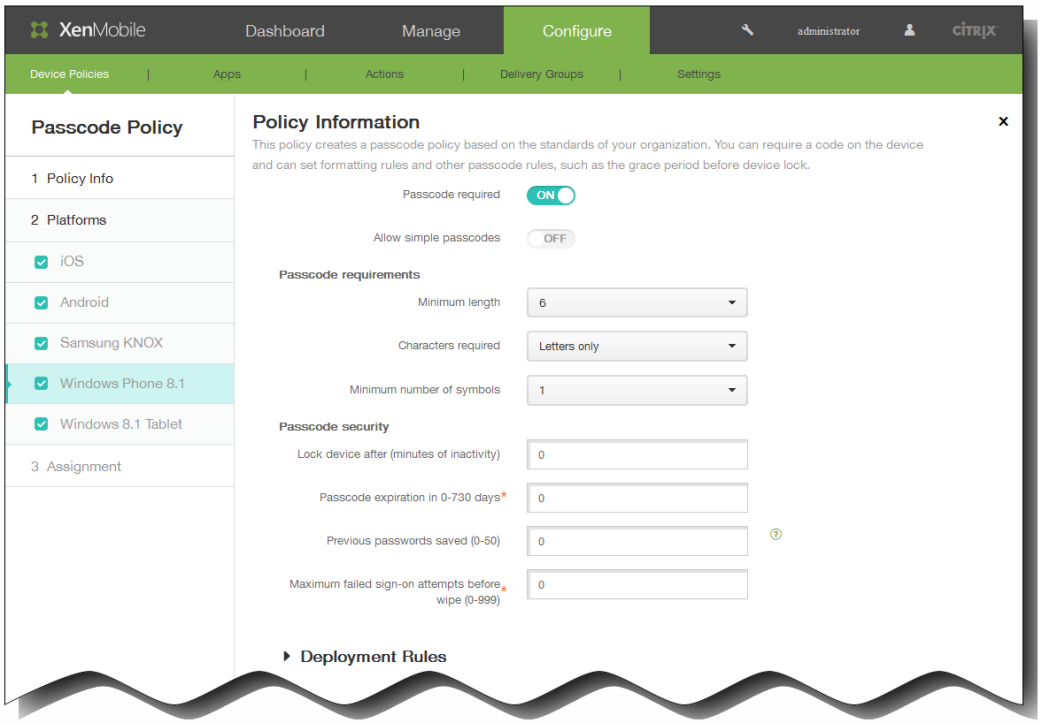
Sécurité des codes secrets

Verrouiller l'appareil après (minutes d'inactivité) : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est Aucune.
Remarque : bien que l'intitulé de ce champ indique « minutes d'inactivité », XenMobile applique le verrouillage après le nombre spécifié de *secondes*.
Expiration du code secret en jours (1 - 730) : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est 0, ce qui signifie que le code secret n'expire jamais.

Mots de passe précédents enregistrés (0-50) : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.

Nombre maximum de tentatives de connexion infructueuses : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est verrouillé. La valeur par défaut est Aucun nombre défini.

- Si vous avez sélectionné Windows Phone 8.1, configurez les paramètres suivants :



Code secret requis : sélectionnez cette option pour ne pas exiger de code secret sur les appareils Windows Phone 8.1. Le paramètre par défaut est ON, ce qui nécessite un mot de passe. La page se réduit et les options suivantes disparaissent. Si vous ne désactivez pas les exigences en matière de code secret, continuez à configurer les paramètres suivants.

Autoriser les codes secrets simples : sélectionnez cette option pour autoriser les codes secrets simples. Les codes secrets simples se caractérisent par des caractères répétés ou séquentiels. La valeur par défaut est OFF.

Conditions requises pour les codes secrets

Longueur minimale : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de 6.

Caractères requis : dans la liste, cliquez sur Numérique ou alphanumérique, Lettres uniquement ou Chiffres uniquement pour configurer la manière dont les codes secrets sont composés. La valeur par défaut est Lettres uniquement.

Nombre minimum de symboles : dans la liste, cliquez sur le nombre de symboles que le code secret doit contenir. La valeur par défaut est de 1.

Sécurité des codes secrets

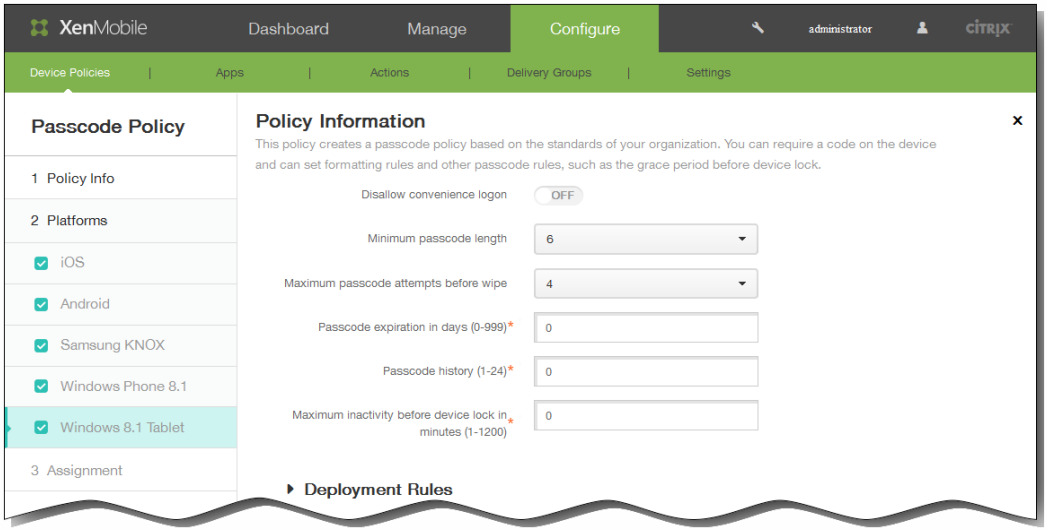
Verrouiller l'appareil après (minutes d'inactivité) : dans la liste, cliquez sur la durée pendant laquelle un appareil peut rester inactif avant d'être verrouillé. La valeur par défaut est de 0.

Expiration du mot de passe dans 0 - 730 jours : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-730. La valeur par défaut est 0, ce qui signifie que le code secret n'expire jamais.

Mots de passe précédents enregistrés (0-50) : entrez le nombre de mots de passe utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des mots de passe figurant dans cette liste. Les valeurs valides sont 0-50. La valeur par défaut est 0, ce qui signifie que les utilisateurs peuvent réutiliser des mots de passe.

Nombre maximum de tentatives de connexion infructueuses avant effacement (0 - 999) : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses qu'un utilisateur peut effectuer avant que les données d'entreprise ne soient effacées de l'appareil. La valeur par défaut est de 0.

- Si vous sélectionnez Windows 8.1 Tablet, configurez les paramètres suivants :



Interdire les dispositifs de connexion pratiques : sélectionnez cette option pour autoriser les utilisateurs à accéder à leurs appareils à l'aide de mots de passe image ou d'ouvertures de session biométriques. La valeur par défaut est OFF.

Longueur minimum du code secret : dans la liste, cliquez sur la longueur minimale du code secret. La valeur par défaut est de 6.

Nombre maximum de tentatives de saisie du code secret avant effacement : dans la liste, cliquez sur le nombre de tentatives de connexion infructueuses après lesquelles l'appareil est effacé. La valeur par défaut est de 4.

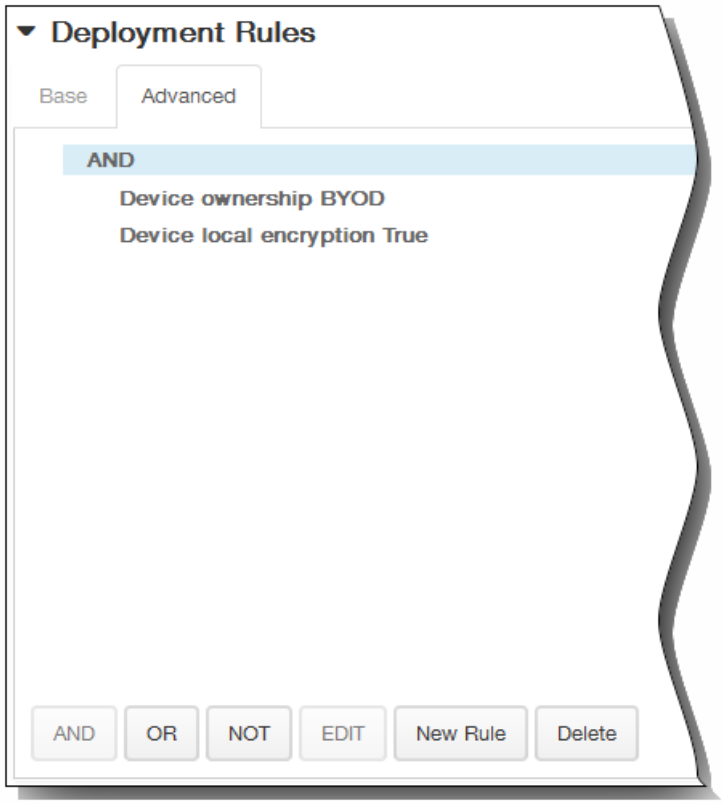
Expiration du code secret en jours (0 - 999) : entrez le nombre de jours après lequel le code secret expire. Les valeurs valides sont 1-999. La valeur par défaut est 0, ce qui signifie que le code secret n'expire jamais.

Historique du code secret (1 - 24) : entrez le nombre de codes secrets utilisés à enregistrer. Les utilisateurs ne peuvent utiliser aucun des codes secrets figurant dans cette liste. Les valeurs valides sont 1-24. Vous devez entrer un nombre compris entre 1 et 24.

Période d'inactivité maximale avant verrouillage de l'appareil en minutes (0 - 1200) : entrez la durée en minutes pendant laquelle un appareil peut rester inactif avant d'être verrouillé. Les valeurs valides sont 1-1200. Vous devez entrer un nombre compris entre 1 et 1200.

5. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

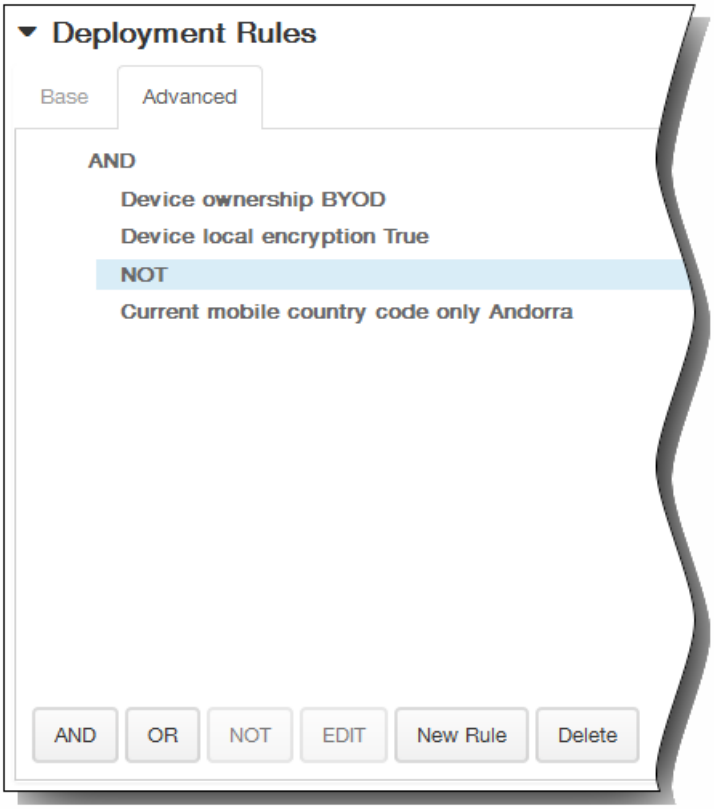
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



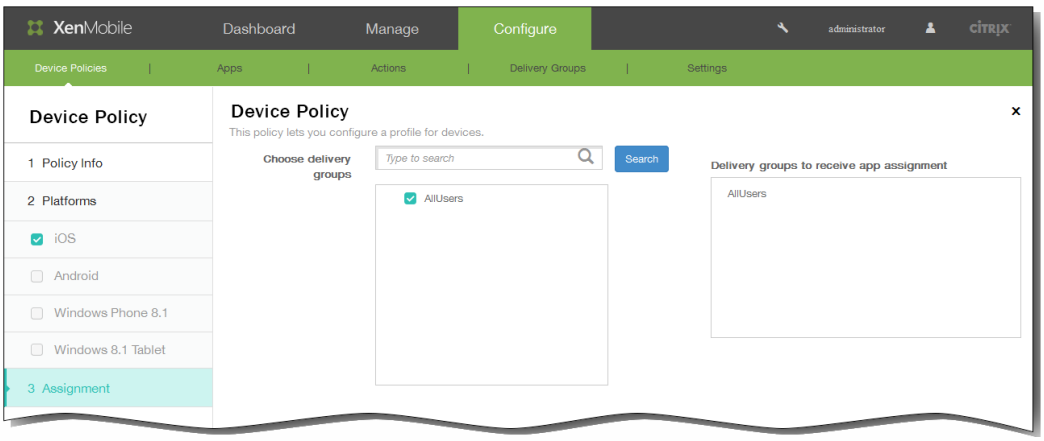
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus

(+) sur le côté droit pour ajouter la condition à la règle.
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.

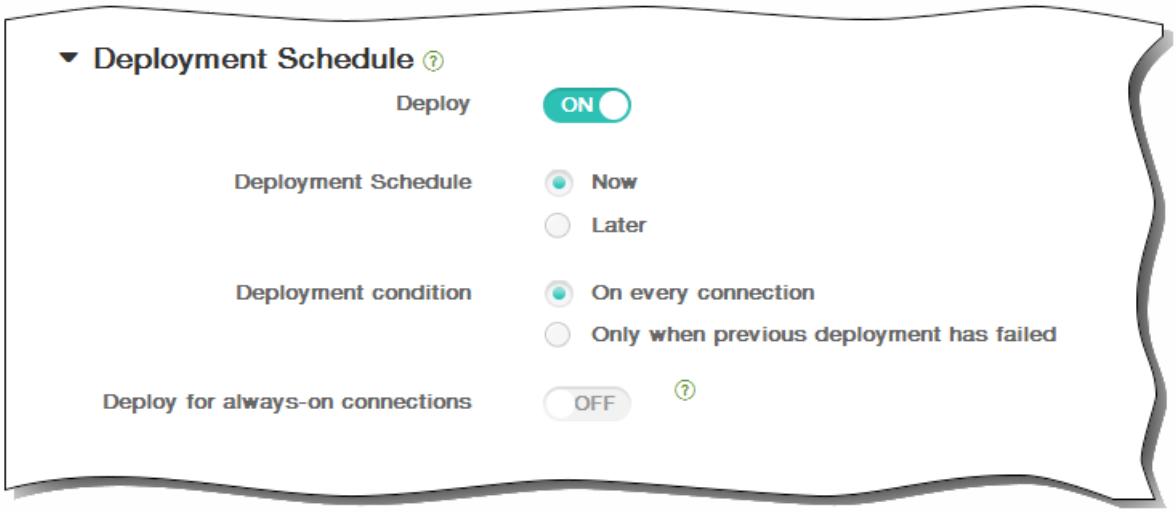


6. Cliquez sur Suivant. La page d'attribution de la Stratégie de code secret s'affiche.
7. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



8. 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.



9. Cliquez sur Enregistrer.

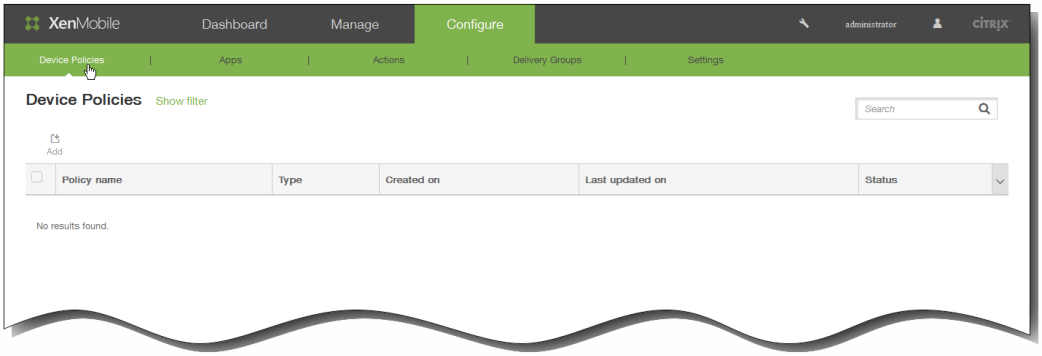
Pour ajouter une stratégie de proxy pour iOS

May 06, 2016

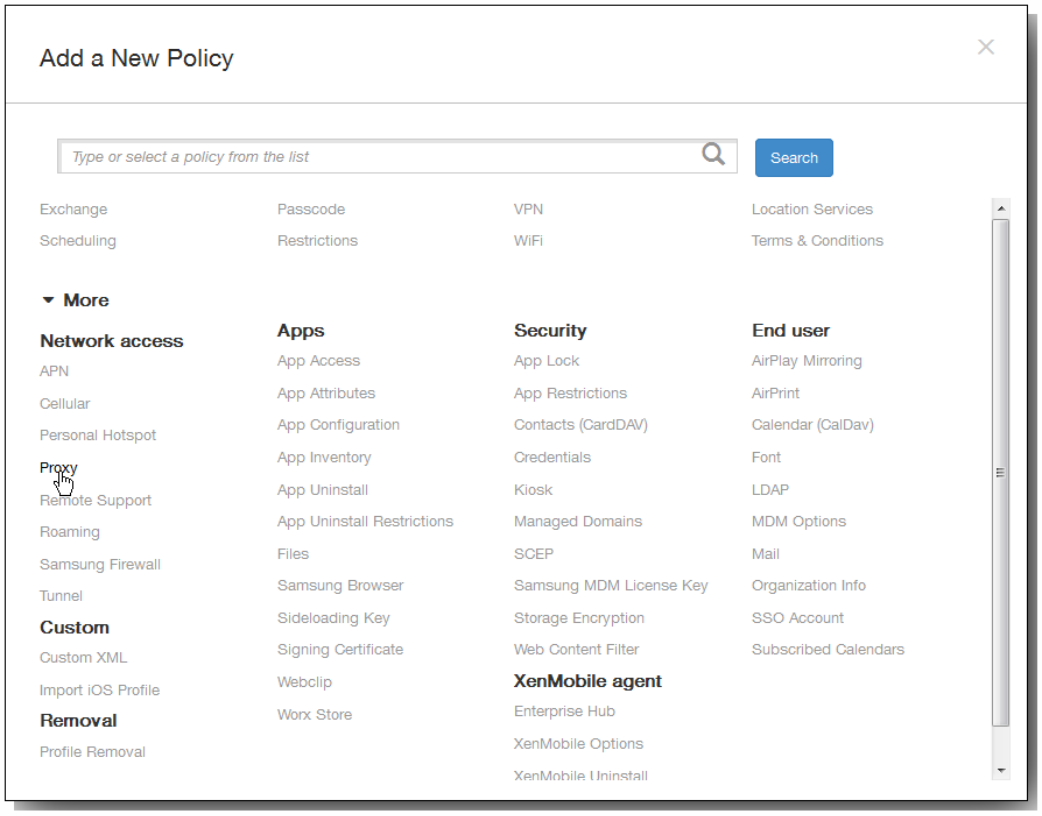
Vous pouvez ajouter une stratégie dans XenMobile pour spécifier les paramètres de proxy HTTP globaux pour les appareils exécutant iOS 6.0 ou version ultérieure. Vous ne pouvez déployer qu'une stratégie de proxy HTTP globale par appareil.

Remarque : avant de déployer cette stratégie, assurez-vous de définir tous les appareils iOS pour lesquels vous souhaitez définir un proxy HTTP global en mode supervisé. Pour de plus amples informations, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

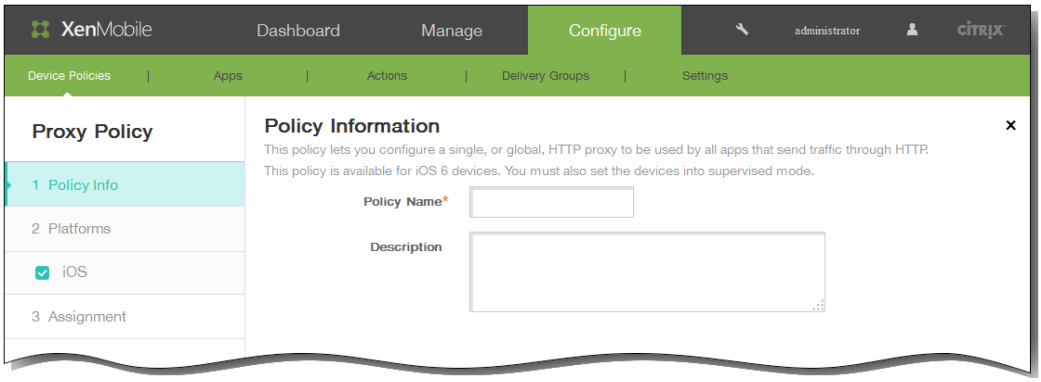
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



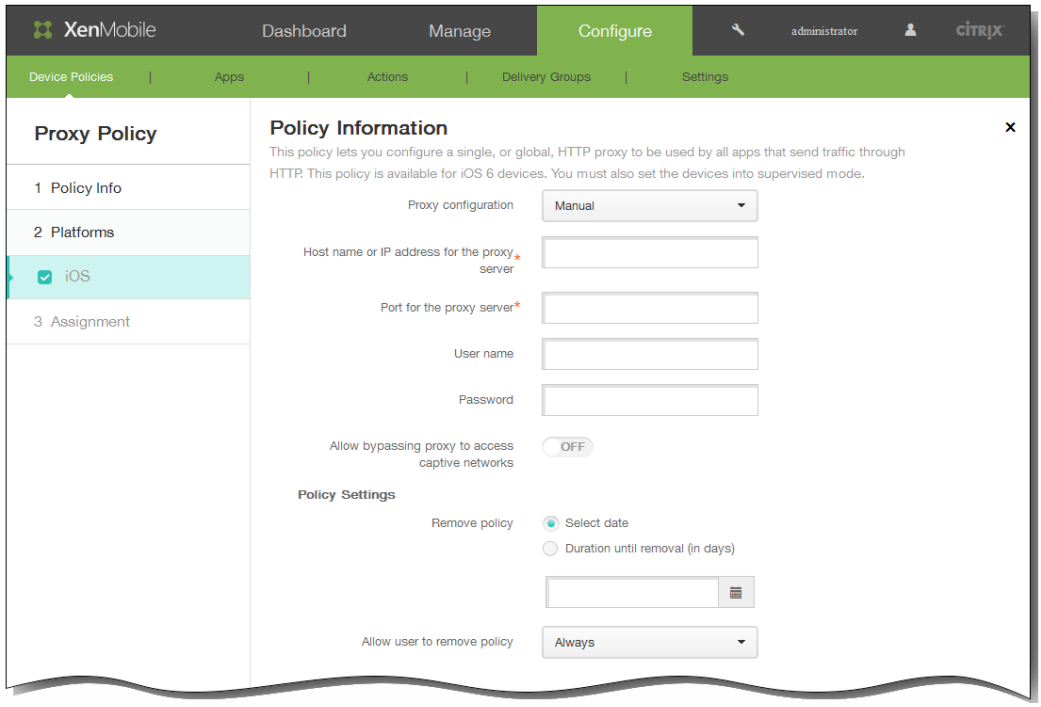
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Accès réseau, cliquez sur Proxy. La page Stratégie de proxy s'affiche.



4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   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.



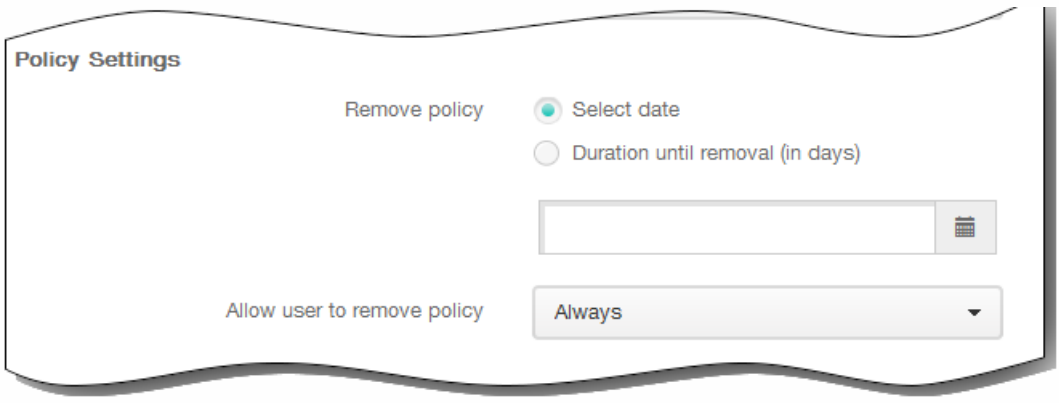
6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Configuration du proxy : cliquez sur Manuel ou Automatique pour choisir la méthode à utiliser pour configurer le proxy sur les appareils des utilisateurs. Le tableau suivant dresse la liste des options disponibles pour chaque configuration de proxy. Chaque cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Manuel	Automatique
Nom d'hôte ou adresse IP du serveur proxy	Requis	–

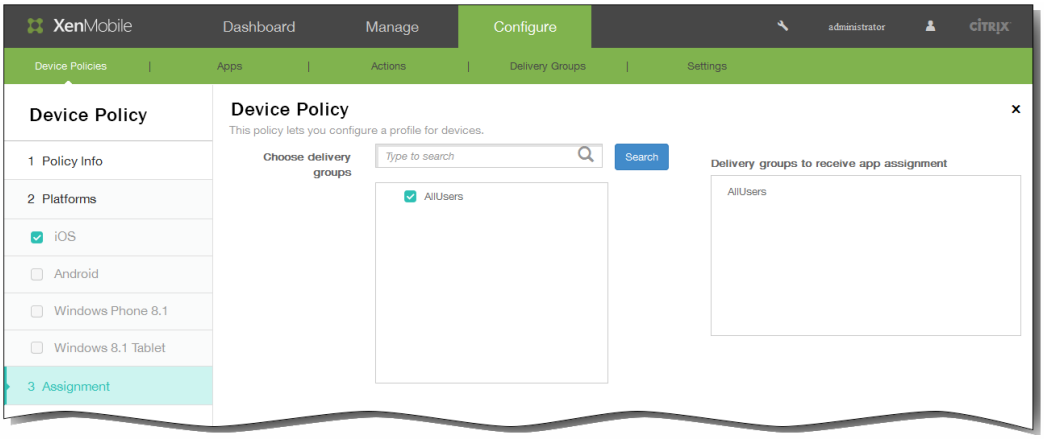
Port du serveur proxy	Manuel Requis	Automatique –
Nom d'utilisateur	Facultatif	–
Mot de passe	Facultatif	–
URL du fichier PAC proxy	–	Facultatif
Autoriser les connexions directes si le fichier PAC est inaccessible	–	OFF

2. Autoriser le contournement du proxy pour accéder aux réseaux captifs : sélectionnez cette option pour autoriser le contournement du proxy afin d'accéder aux réseaux captifs.

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.

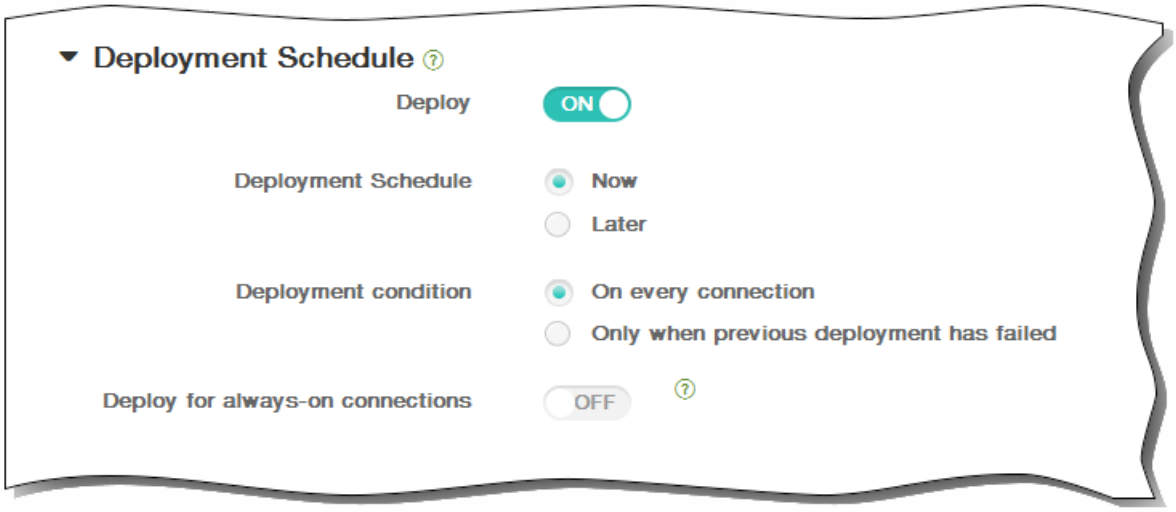


11. Cliquez sur Suivant. La page d'attribution de la Stratégie de proxy s'affiche.
12. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



13. 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.



14. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie d'assistance à distance pour Samsung KNOX

May 06, 2016

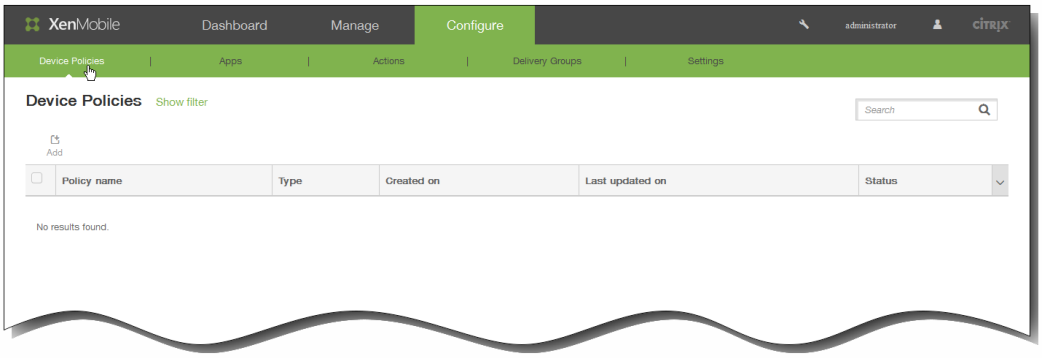
Vous créez une stratégie d'assistance à distance dans XenMobile pour vous permettre d'accéder à distance aux appareils Samsung KNOX des utilisateurs. Vous pouvez configurer deux types d'assistance :

- **Assistance à distance de base** : cette option vous permet d'afficher des informations de diagnostic sur l'appareil, telles que les informations système, les processus en cours d'exécution, le gestionnaire des tâches (utilisation de mémoire et de l'UC), le contenu du dossier des logiciels installés, etc.
- **Assistance à distance premium** : cette option vous permet de contrôler à distance l'écran de l'appareil, y compris le contrôle des couleurs (dans la fenêtre principale ou dans une fenêtre distincte flottante), d'établir une session Voix-sur-IP (VoIP) entre le bureau d'assistance et l'utilisateur, de configurer des paramètres et d'établir une session de chat entre le bureau d'assistance et l'utilisateur.

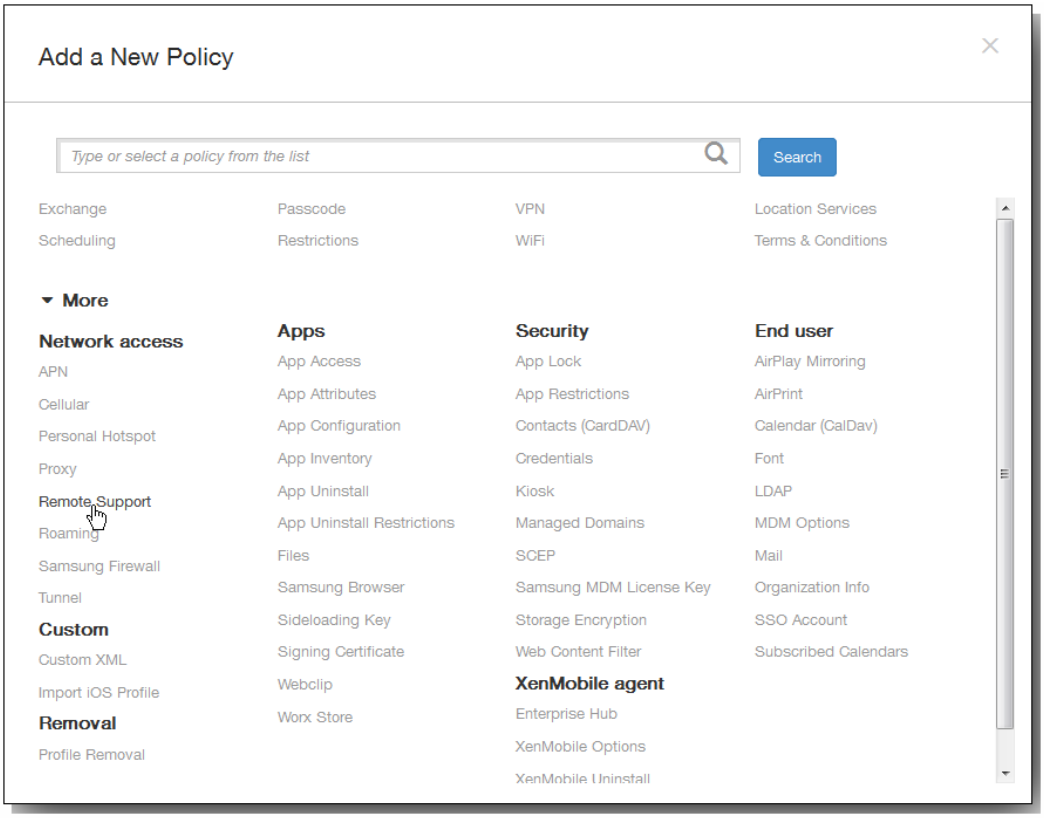
Remarque : pour implémenter cette stratégie, vous devez effectuer les tâches suivantes :

- Installez l'application d'assistance à distance XenMobile dans votre environnement.
- Configurez un tunnel applicatif d'assistance à distance. Pour de plus amples informations, consultez la section Pour ajouter une stratégie de tunnel applicatif pour Android.
- Configurez une stratégie d'assistance à distance Samsung KNOX comme décrit dans cette rubrique.
- Déployez la stratégie de tunnel applicatif à utiliser pour l'assistance à distance et la stratégie d'assistance à distance Samsung KNOX sur les appareils des utilisateurs.

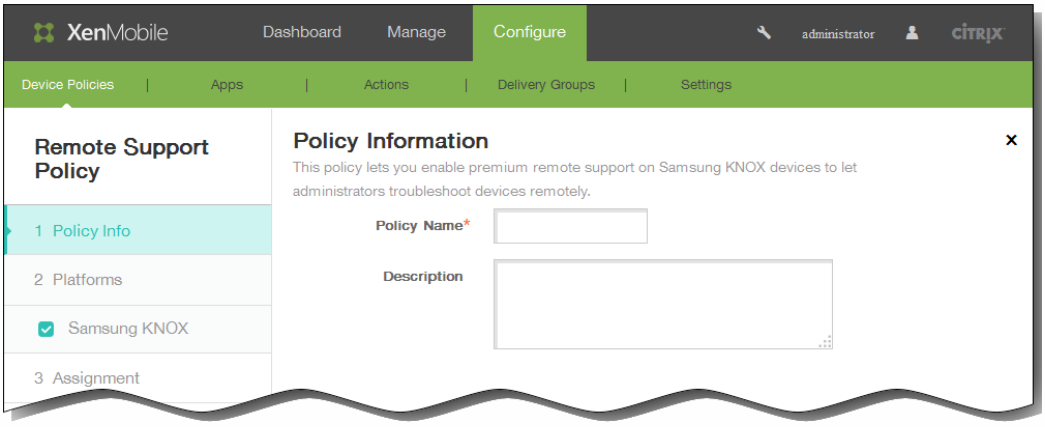
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



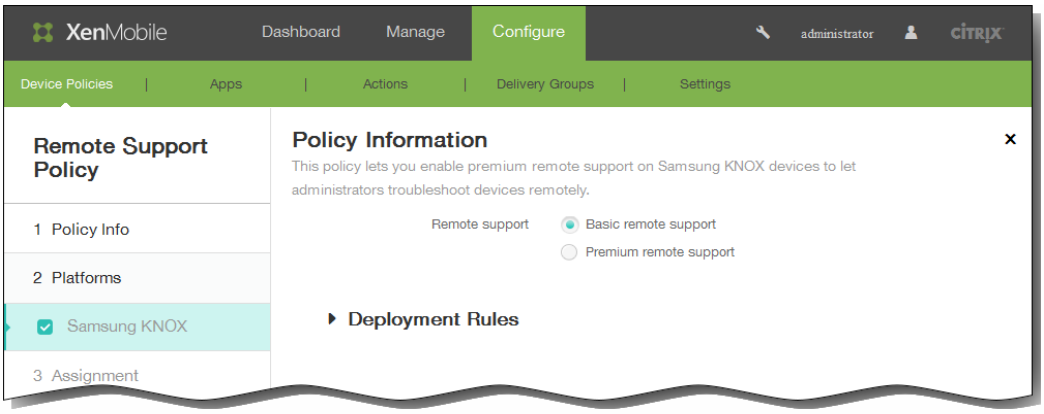
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Accès réseau, cliquez sur Assistance à distance. La page Stratégie d'assistance à distance s'affiche.

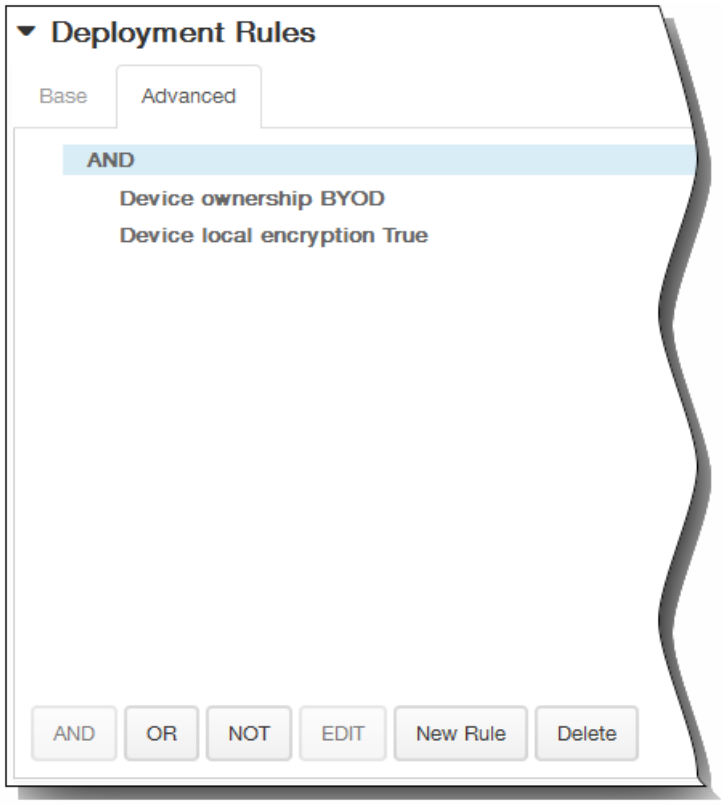


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations sur la plate-forme Samsung KNOX s'affiche.



6. Dans la page d'informations sur la plate-forme Samsung KNOX, entrez les informations suivantes :
   1. Assistance à distance : sélectionnez Assistance à distance de base ou Assistance à distance premium. La valeur par défaut est Assistance à distance de base.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

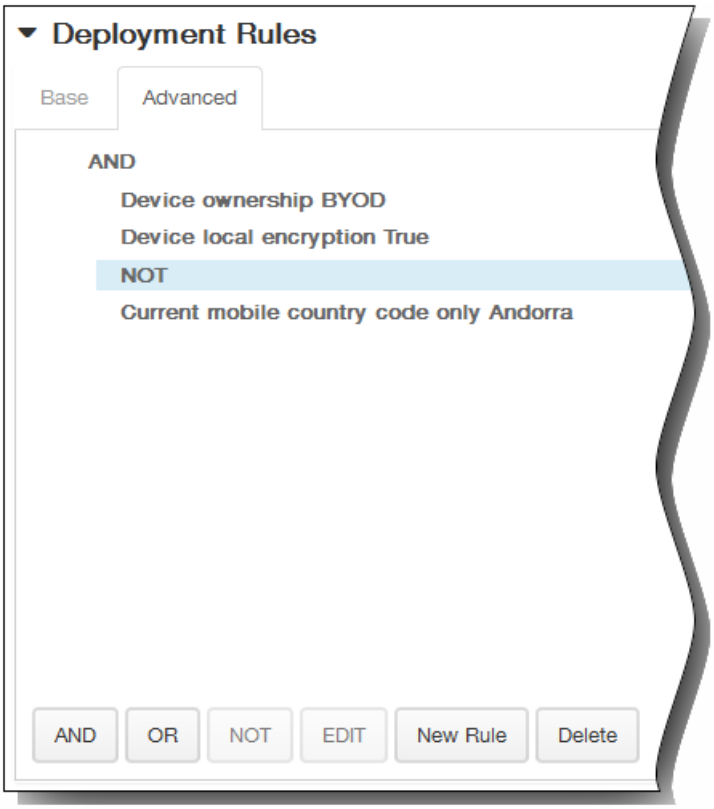
   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour 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.



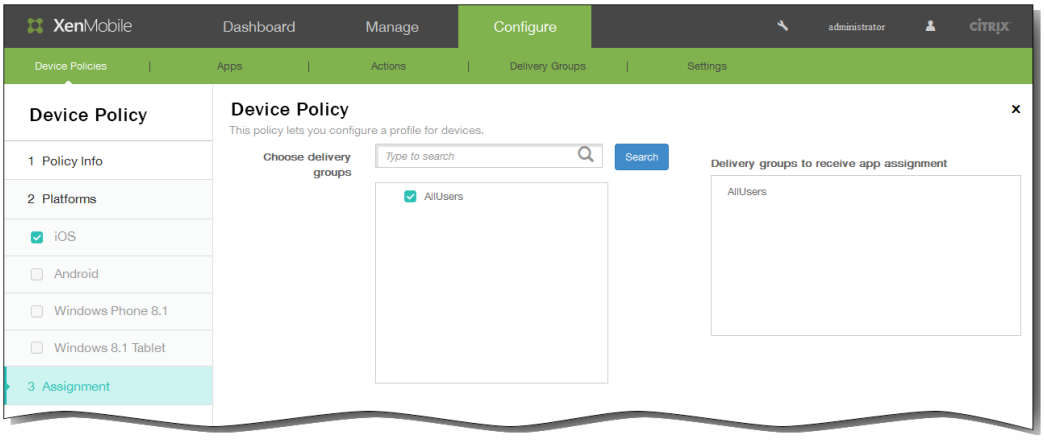
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
      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 d'assistance à distance s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

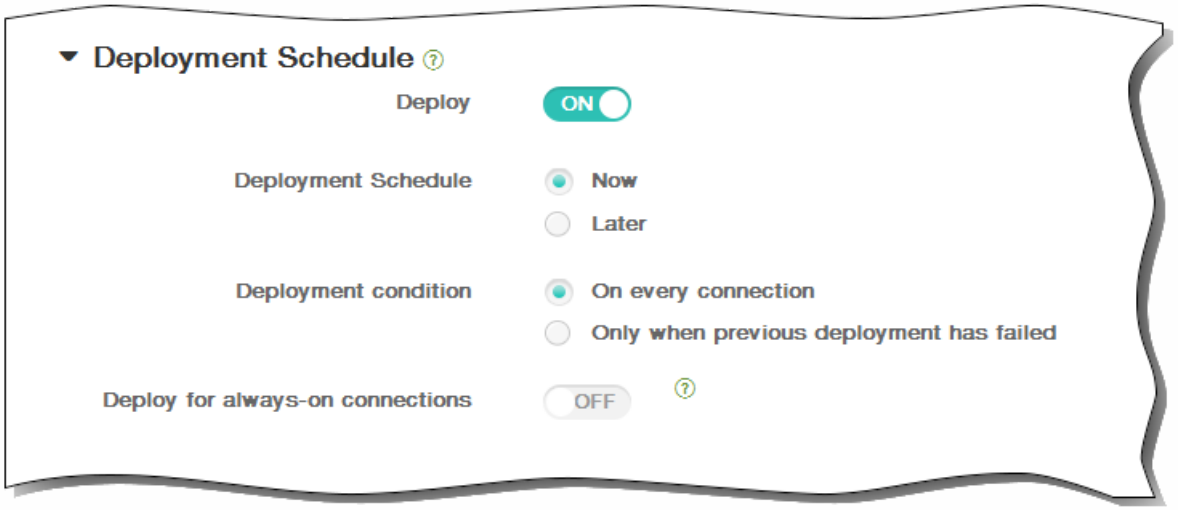


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de restrictions

May 06, 2016

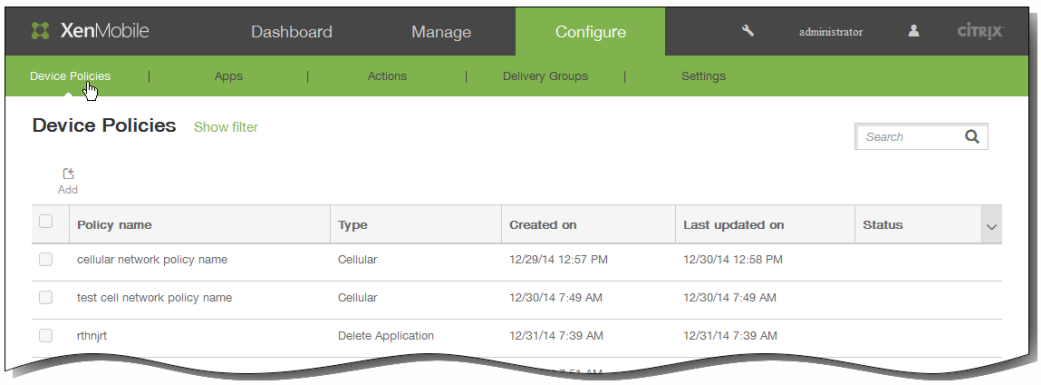
Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour limiter l'accès des utilisateurs à certaines fonctionnalités sur leurs appareils, téléphones, tablettes, etc. Vous pouvez configurer la stratégie de restriction pour les plates-formes suivantes : iOS, Samsung SAFE, Windows 8.1 Tablet, Windows Phone 8.1 et Amazon. Chaque plate-forme requiert des valeurs différentes, qui sont décrites dans cet article.

Cette stratégie permet ou empêche les utilisateurs d'utiliser certaines fonctionnalités sur leurs appareils, telles que l'appareil photo. Vous pouvez également définir des restrictions de sécurité, des restrictions d'accès au contenu multimédia ainsi que des restrictions sur les types d'applications que les utilisateurs peuvent ou ne peuvent pas installer. La plupart des paramètres de restriction sont réglés par défaut sur ON ou
— autorise
. L'exception principale concerne la fonctionnalité Sécuriser - Forcer qui est réglée par défaut sur OFF ou
— empêche
.
Conseil : toute option définie sur ON signifie que l'utilisateur
— peut
effectuer l'opération ou utiliser la fonctionnalité. Par exemple :

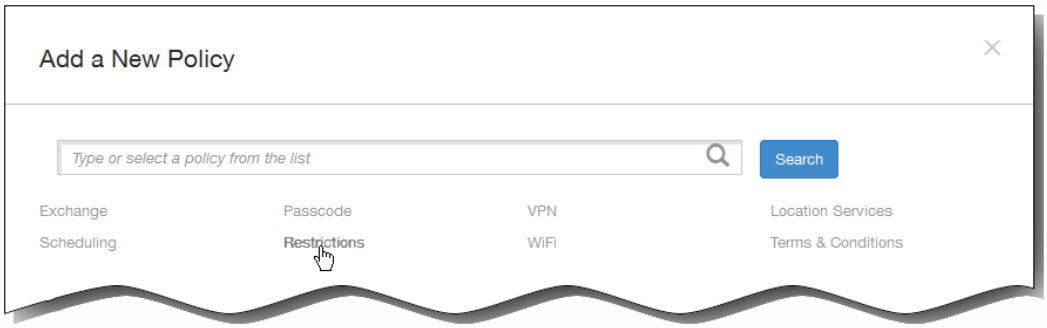
- Appareil photo. Si l'option est réglée sur ON, l'utilisateur peut utiliser l'appareil photo sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas utiliser l'appareil photo sur son appareil.
- **Captures d'écrans**. Si l'option est réglée sur ON, l'utilisateur peut prendre des captures d'écrans sur son appareil. Si l'option est réglée sur OFF, l'utilisateur ne peut pas prendre de captures d'écrans sur son appareil.

Remarque : certaines des options de restrictions iOS ne s'appliquent qu'à des versions spécifiques de iOS (et, le cas échéant, ces versions sont indiquées sur la page de la console XenMobile). Par ailleurs, certaines options s'appliquent uniquement si l'appareil est placé en mode supervisé. Par exemple, la possibilité d'autoriser ou de bloquer AirDrop est uniquement prise en charge sur les appareils exécutant iOS 7 et versions ultérieures, tandis que la possibilité d'autoriser ou de bloquer des flux de photos est prise en charge sur les appareils exécutant iOS 5 et version ultérieure. 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.

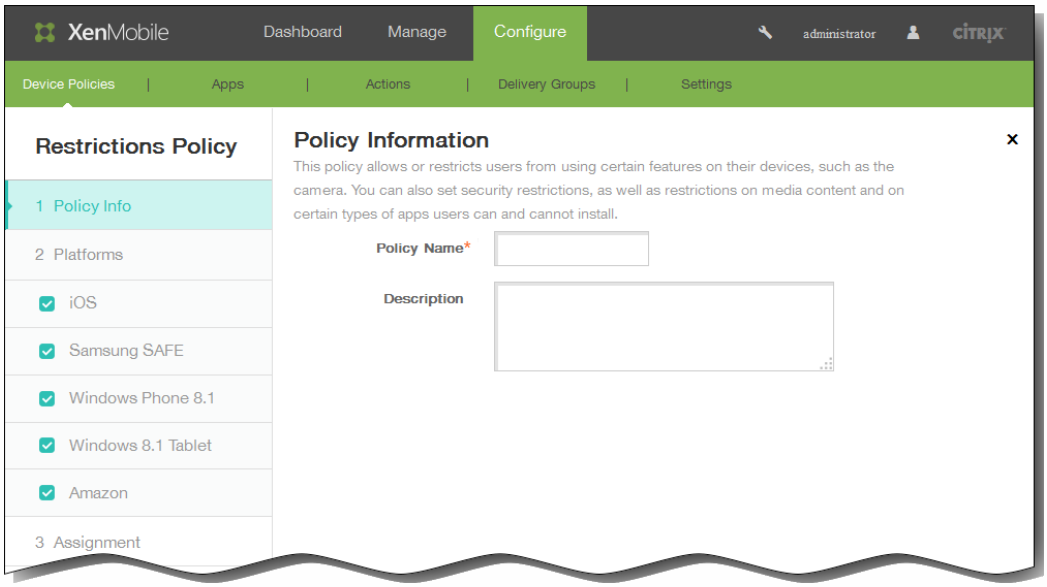
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



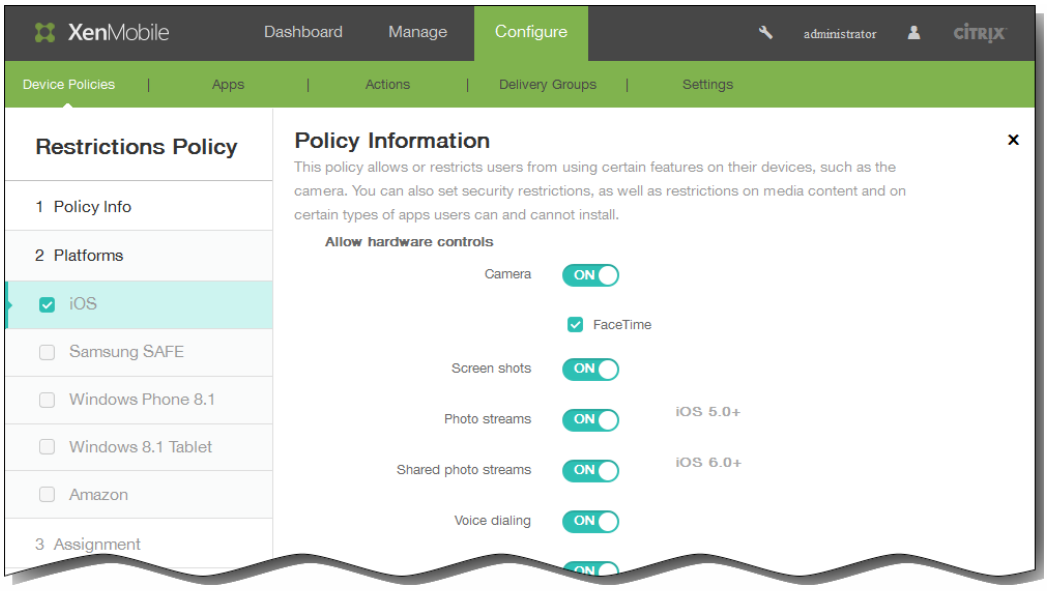
2. Cliquez sur Ajouter. La page Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Restrictions.
   La page d'informations Stratégie de restrictions s'affiche.



4. Dans le panneau Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter. Vous pouvez ensuite modifier les informations de stratégie pour chaque plate-forme que vous avez sélectionnée. Cliquez pour limiter les fonctionnalités dans les sections suivantes, ce qui désactive le paramètre (OFF). Sauf spécification contraire, la fonctionnalité est activée par défaut.
   - Si vous avez sélectionné iOS, configurez les paramètres suivants :



- Autoriser le contrôle du matériel :

  Appareil photo ; FaceTime

  Captures d'écrans

  Flux de photos (disponible dans iOS 5.0 et version ultérieure)

  Flux de photos partagés (disponible dans iOS 6.0 et version ultérieure)

  Composition vocale

  Siri :
  - Autoriser lorsque l'appareil est verrouillé : laissez l'option sélectionnée par défaut ou décochez la case.
  - Filtre d'obscénité de Siri : laissez l'option désactivée par défaut ou cochez la case. Cette fonctionnalité est désactivée par défaut.

  Installation d'applications

- Autoriser les applications :

  YouTube

  iTunes Store

  Achats dans les applications : requiert le mot de passe iTunes pour les achats : laissez l'option désactivée par défaut ou cochez la case (disponible pour iOS 5.0 et version ultérieure). Cette fonctionnalité est désactivée par défaut.

  Safari :
  - Remplissage automatique : laissez l'option sélectionnée par défaut ou décochez la case.
  - Forcer l'avertissement de fraude : laissez l'option désactivée par défaut ou cochez la case. Cette fonctionnalité est désactivée par défaut.
  - Activer JavaScript : laissez l'option sélectionnée par défaut ou décochez la case.
  - Bloquer les fenêtres contextuelles : laissez l'option désactivée par défaut ou cochez la case. Cette fonctionnalité est désactivée par défaut.

Dans Accepter les cookies, cliquez sur l'une des options suivantes :

- Toujours
- Jamais
- Des sites visités uniquement

L'option par défaut est Toujours.

- Réseau - Autoriser les actions iCloud :

  Synchronisation des documents et des données (disponible dans iOS 5.0 et version ultérieure.)

  Sauvegarde de l'appareil (disponible dans iOS 5.0 et version ultérieure)

  Synchronisation automatique lors d'utilisation en itinérance

  Trousseau iCloud (disponible dans iOS 7.0 et version ultérieure)

- Sécurité - Forcer :

  Copies de sauvegarde chiffrées La valeur par défaut est OFF.

  Suivi limité des publicités (disponible dans iOS 7.0 ou version ultérieure) la valeur par défaut est OFF.

  Demander code secret lors du premier couplage AirPlay (disponible dans iOS 7.0 ou version ultérieure) La valeur par défaut est OFF.

- Sécurité - Autoriser :

  Accepter des certificats SSL non approuvés (disponible dans iOS 5.0 et version ultérieure)

  Mise à jour automatique des paramètres d'approbation de certificat (disponible dans iOS 7.0 et versions ultérieures)

  Documents provenant d'applications gérées dans les applications non gérées

  Documents provenant d'applications non gérées dans les applications gérées

  Envoi d'informations de diagnostic à Apple

  Touch ID pour déverrouiller un appareil (disponible dans iOS 7.0 et versions ultérieures)

  Notifications Passbook lorsque l'appareil est verrouillé (disponible dans iOS 6.0 et versions ultérieures)

  Handoff (disponible dans iOS 8.0 et versions ultérieures)

  Synchronisation iCloud pour applications gérées (disponible dans iOS 8.0 et versions ultérieures)

  Sauvegarde de livres d'entreprise (disponible dans iOS 8.0 et versions ultérieures)

  Synchronisation des notes et des extraits pour les livres d'entreprise (disponible dans iOS 8.0 et versions ultérieures)

- Paramètres supervisés uniquement - Autoriser :

  Résultats Internet dans Spotlight (disponible dans iOS 8.0 et versions ultérieures)

  Effacer tout le contenu et les paramètres (disponible dans iOS 8.0 et versions ultérieures)

Configuration des restrictions (disponible dans iOS 8.0 et versions ultérieures)

Installation des profils de configuration (disponible dans iOS 6.0 et versions ultérieures)

AirDrop (disponible dans iOS 7.0 et versions ultérieures)

iMessage (disponible dans iOS 6.0 et versions ultérieures)

Contenu généré par l'utilisateur dans Siri (disponible dans iOS 7.0 et versions ultérieures)

iBooks (disponible dans iOS 6.0 et versions ultérieures)

Suppression d'applications (disponible dans iOS 7.0 et versions ultérieures)

Game Center (disponible dans iOS 6.0 et versions ultérieures)
- Ajouter des amis : laissez l'option sélectionnée par défaut ou décochez la case.
- Jeux multijoueurs : laissez l'option sélectionnée par défaut ou décochez la case.

Modification des paramètres de compte (disponible dans iOS 7.0 et versions ultérieures)

Modification des paramètres des données cellulaires d'application (disponible dans iOS 7.0 et versions ultérieures)

Modification des paramètres Localiser mes amis (disponible dans iOS 7.0 et versions ultérieures)

Couplage avec des hôtes non Configurator (disponible dans iOS 7.0 et versions ultérieures)

Bundle ID d'application unique : dans Nom app, entrez une ou plusieurs applications.

- Sécurité - Afficher dans l'écran de verrouillage :

  Centre de contrôle (disponible dans iOS 7.0 et versions ultérieures)

  Notification (disponible dans iOS 7.0 et versions ultérieures)

  Vue Aujourd'hui

- Contenu multimédia - Autoriser :

  Musique, podcasts et cours iTunes U explicites

  Contenu sexuel explicite dans iBooks (disponible dans iOS 6.0 et versions ultérieures)

  Classements par région : cliquez sur un pays dans la liste. La valeur par défaut est États-Unis.

  Films : cliquez sur l'une de ces options : Autoriser tous les films, Bloquer les films, G, PG, PG-13, R, NC-17 ; la valeur par défaut est Autoriser tous les films.

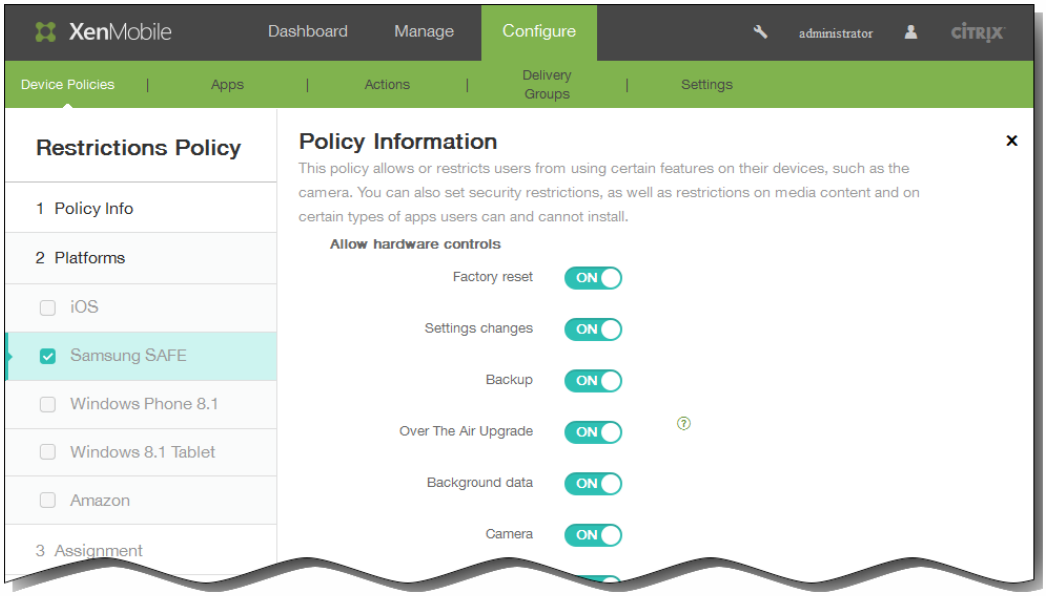
  Séries TV : cliquez sur l'une de ces options : Autoriser toutes les séries TV, Bloquer les séries TV, TV-Y, TV-Y7, TV-G, TV-PG TV-PG14, TV-MA ; la valeur par défaut est Autoriser toutes les séries TV.

  Applications : cliquez sur l'une de ces options : Autoriser toutes les apps, Bloquer les applications, 4+, 9+, 12+ ou 17+ ; la valeur par défaut est Autoriser toutes les apps.

- Si vous sélectionnez Samsung SAFE, configurez les paramètres suivants :

  Remarque : certaines options sont uniquement disponibles dans l'API Samsung Mobile Device Management 4.0 et

versions ultérieures ; elles sont marquées avec (MDM 4.0 et versions ultérieures).



- Dans Autoriser le contrôle du matériel :

  Réinitialisation d'usine

  Modification des paramètres

  Sauvegarde

  Mise à jour par réseau cellulaire (MDM 4.0 et versions ultérieures)

  Fonctionnement en arrière-plan

  Appareil photo

  Presse-papiers

  Partage du presse-papiers (MDM 4.0 et versions ultérieures)

  Touche début

  Microphone

  Localisation

  NFC (communication en champ proche) (MDM 4.0 et versions ultérieures)

  Arrêter (MDM 4.0 et versions ultérieures)

  Capture d'écran

  Carte SD

  Composeur vocal (MDM 4.0 et versions ultérieures)

SBeam (MDM 4.0 et versions ultérieures)

SVoice (MDM 4.0 et versions ultérieures)

- Dans Autoriser les applications :

  Navigateur

  YouTube

  GooglePlay/Marketplace

  Autoriser les applications non Google Play

  Arrêt des applications système (MDM 4.0 et versions ultérieures)

- Dans Réseau :

  Bluetooth ; Partage de connexion

  Wi-Fi ; partage de connexion, direct (MDM 4.0 et versions ultérieures)

  Partage de connexion

  Données cellulaires

  Autoriser l'itinérance. La valeur par défaut est OFF.

  Connexions sécurisées uniquement

  Android beam (MDM Android 4.0 et versions ultérieures)

  Enregistrement audio (MDM 4.0 et versions ultérieures)

  Enregistrement vidéo (MDM 4.0 et versions ultérieures)

  Services de localisation

  Limite par jour (Mo) : entrez l'allocation quotidienne en Mo. La valeur par défaut est 0, ce qui désactive cette fonctionnalité. (MDM 4.0 et versions ultérieures)

  Limite par semaine (Mo) : entrez l'allocation hebdomadaire en Mo. La valeur par défaut est 0, ce qui désactive cette fonctionnalité. (MDM 4.0 et versions ultérieures)

  Limite par mois (Mo) : entrez l'allocation mensuelle en Mo. La valeur par défaut est 0, ce qui désactive cette fonctionnalité. (MDM 4.0 et versions ultérieures)

- Dans Autoriser les actions USB :

  Débogage

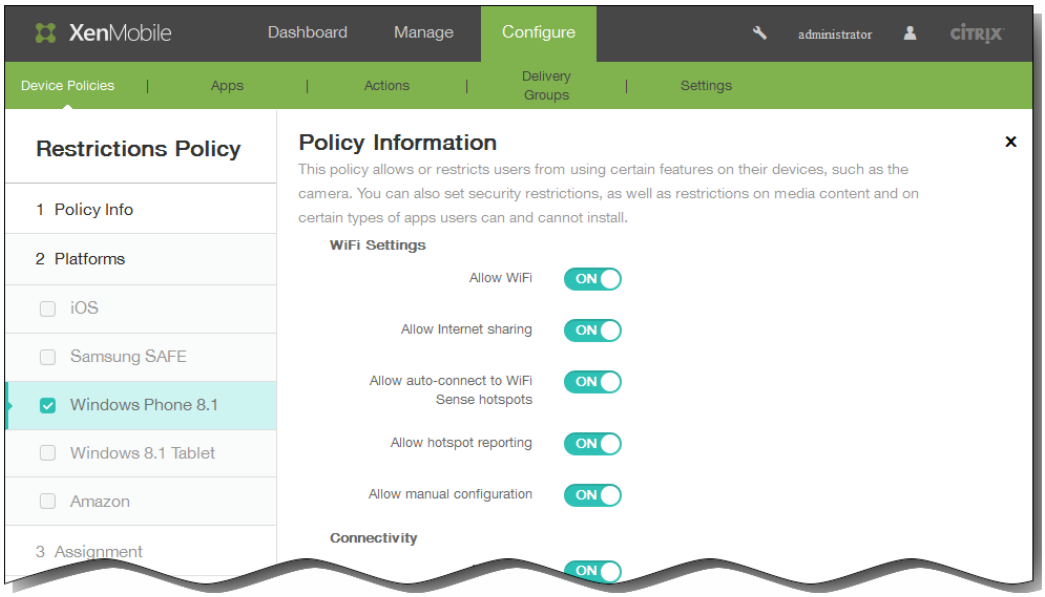
  Stockage hôte

  Stockage de masse

  Lecteur multimédia Kies

Partage de connexion

- Si vous avez sélectionné Windows Phone 8.1, configurez les paramètres suivants :



- Paramètres Wi-Fi :

  Autoriser le Wi-Fi

  Autoriser le partage Internet

  Autoriser la connexion automatique aux points d'accès Wi-Fi Sense

  Autoriser la recherche de points d'accès

  Autoriser la configuration manuelle

- Connectivité :

  Autoriser NFC

  Autoriser le bluetooth

  Autoriser les connexions VPN via réseau cellulaire

  Autoriser les connexions VPN via réseau cellulaire en itinérance

  Autoriser les connexions USB

  Autoriser les données cellulaires itinérantes

- Comptes :

  Autoriser la connexion au compte Microsoft

Autoriser les adresses e-mail non-Microsoft

- Rechercher :

  Autoriser utilisation des données de localisation

  Filtrer le contenu pour adultes (la valeur par défaut est OFF).

  Autoriser Bing Vision à stocker les images

- Système :

  Autoriser les cartes de stockage

  Autoriser les services de localisation

  Autoriser l'utilisation de l'appareil photo

  Télémétrie : cliquez sur l'un de ces paramètres : Autorisée, Non autorisée, Autorisée, excepté pour les demandes de données secondaires. La valeur par défaut est Autorisée.

- Sécurité :

  Autoriser installation manuelle certificat racine

  Activer le chiffrement de l'appareil la valeur par défaut est OFF.

  Autoriser le copier-coller

  Autoriser la capture d'écran

  Autoriser l'enregistrement vocal

  Autoriser l'enregistrement de fichiers Office

  Autoriser notifications du centre de maintenance

  Autoriser Cortana

  Autoriser synchronisation des paramètres de l'appareil

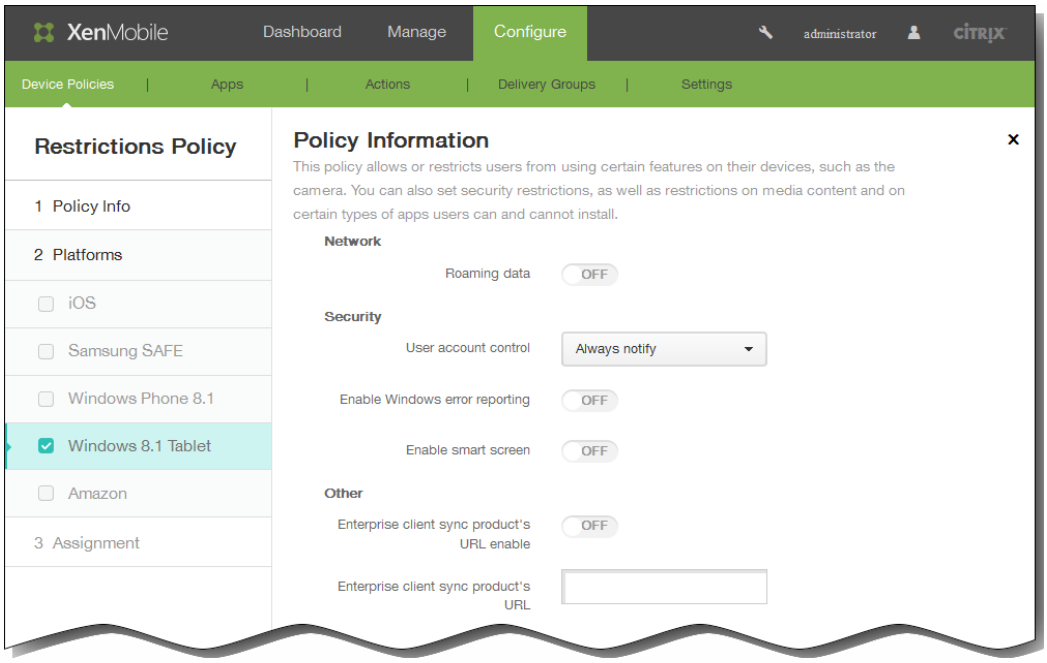
- Applications :

  Autoriser l'accès au magasin

  Autoriser le déblocage

  Autoriser l'accès au navigateur Web

- Si vous avez sélectionné Windows 8.1 tablet, configurez les paramètres suivants :



- Réseau :

  Données en itinérance

- Sécurité :

  Contrôle de compte d'utilisateur : dans la liste, cliquez sur l'un de ces paramètres : Toujours m'avertir, M'avertir des modifications, M'avertir des modif. (ne pas assombrir), Ne jamais m'avertir. La valeur par défaut est Toujours m'avertir.

  Activer le rapport d'erreurs Windows

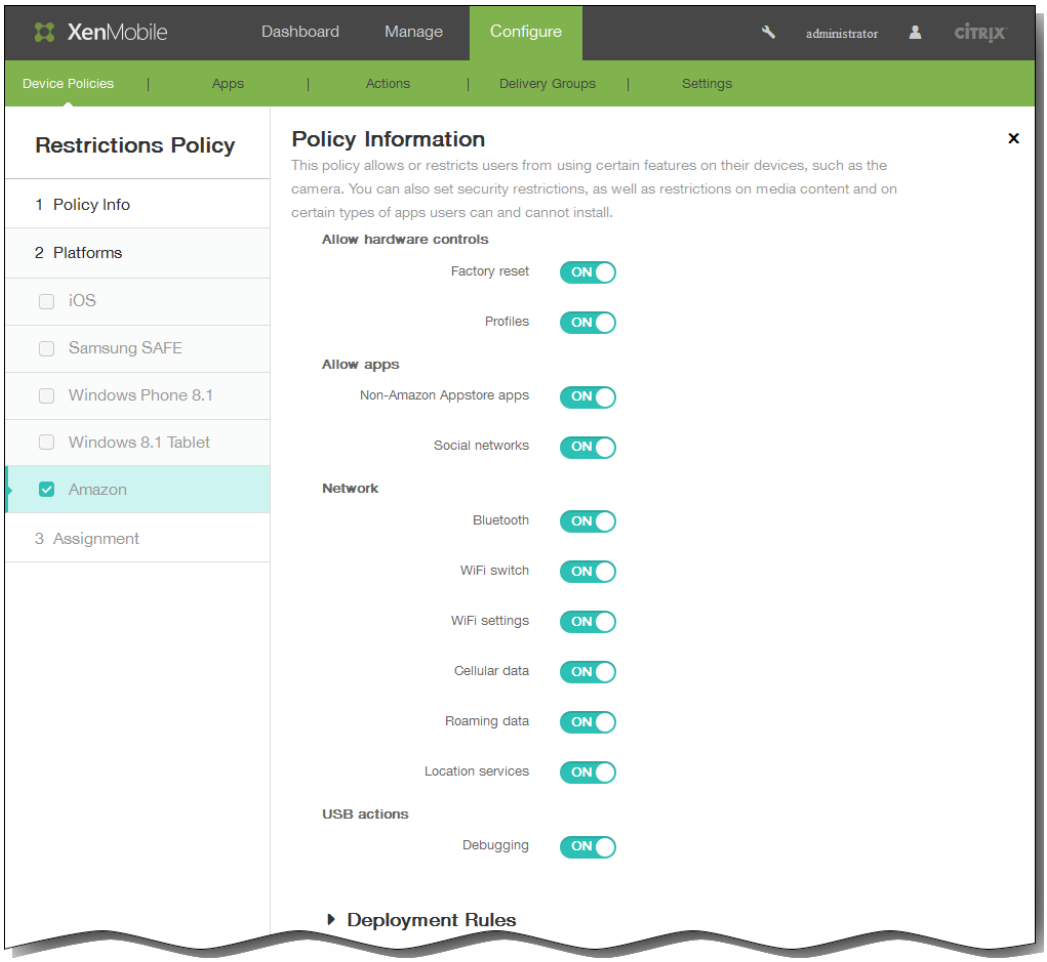
  Activer Smart Screen

- Autre :

  Activer l'URL du produit Enterprise Client Sync

  URL du produit Enterprise Client Sync : entrez une adresse URL valide.

- Si vous avez sélectionné Amazon, configurez les paramètres suivants :



- Autoriser le contrôle du matériel :

  Réinitialisation d'usine

  Profils

- Autoriser les applications :

  Applications non Amazon Appstore

  Réseaux sociaux

- Réseau :

  Bluetooth

  Commutateur Wi-Fi

  Paramètres Wi-Fi

  Données cellulaires

  Données en itinérance

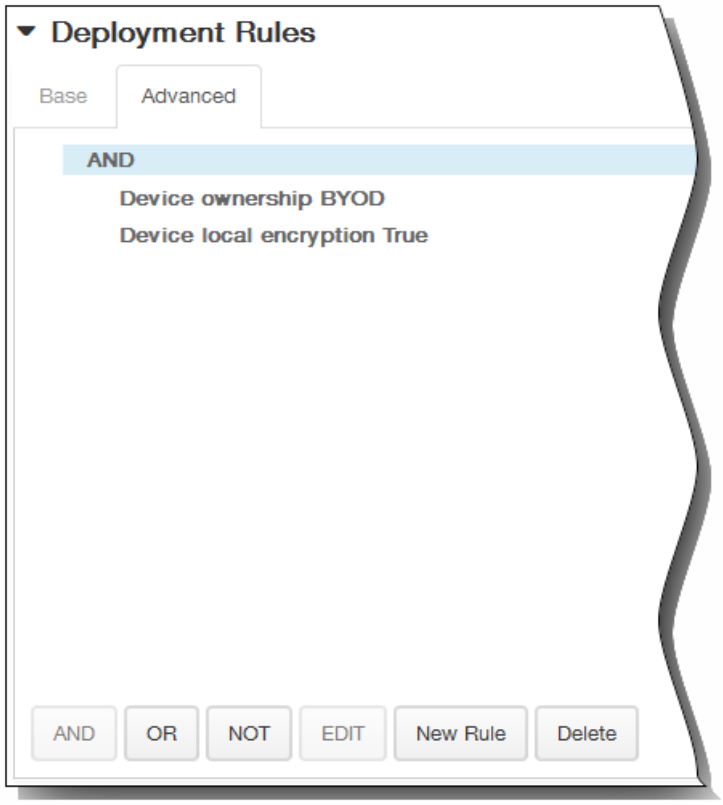
  Services de localisation

- Actions USB :

  Débogage

6. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

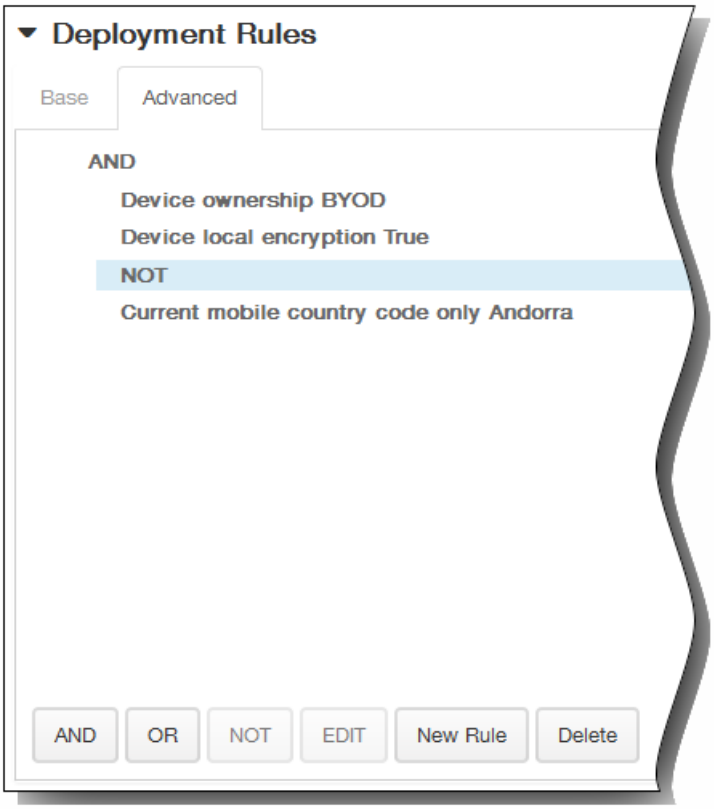
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



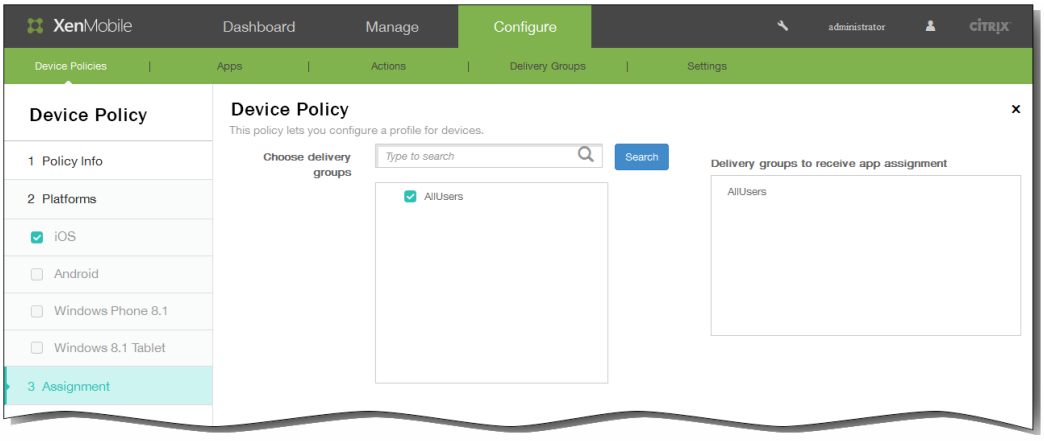
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.

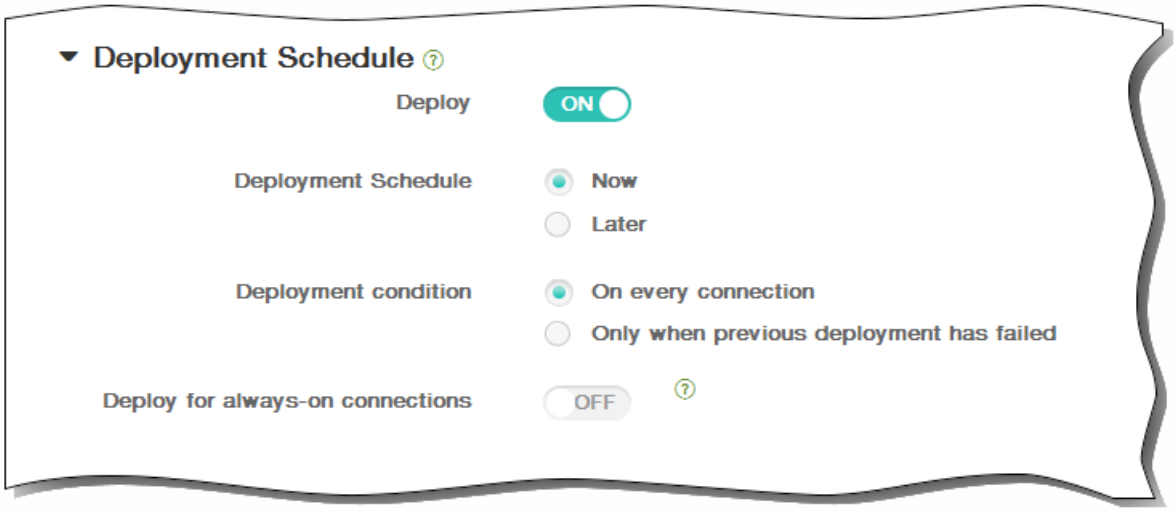


7. Une fois que vous avez terminé de configurer les paramètres pour une ou plusieurs plates-formes, cliquez sur Suivant et la page Attribution s'affiche.
8. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes 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.
   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.



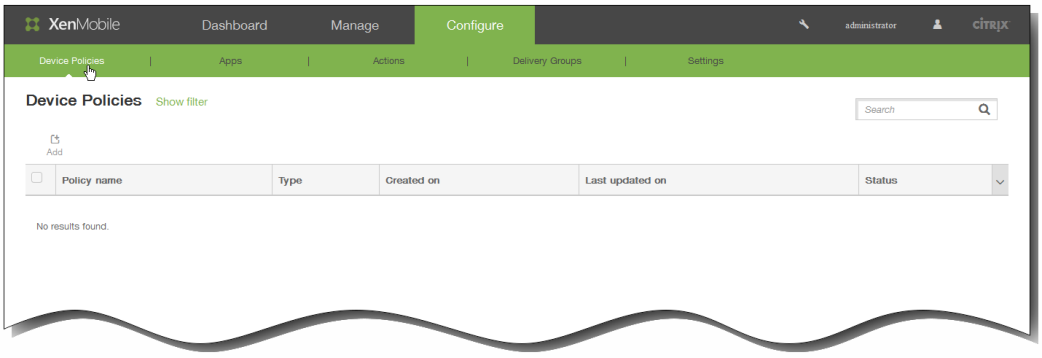
10. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie d'itinérance pour iOS

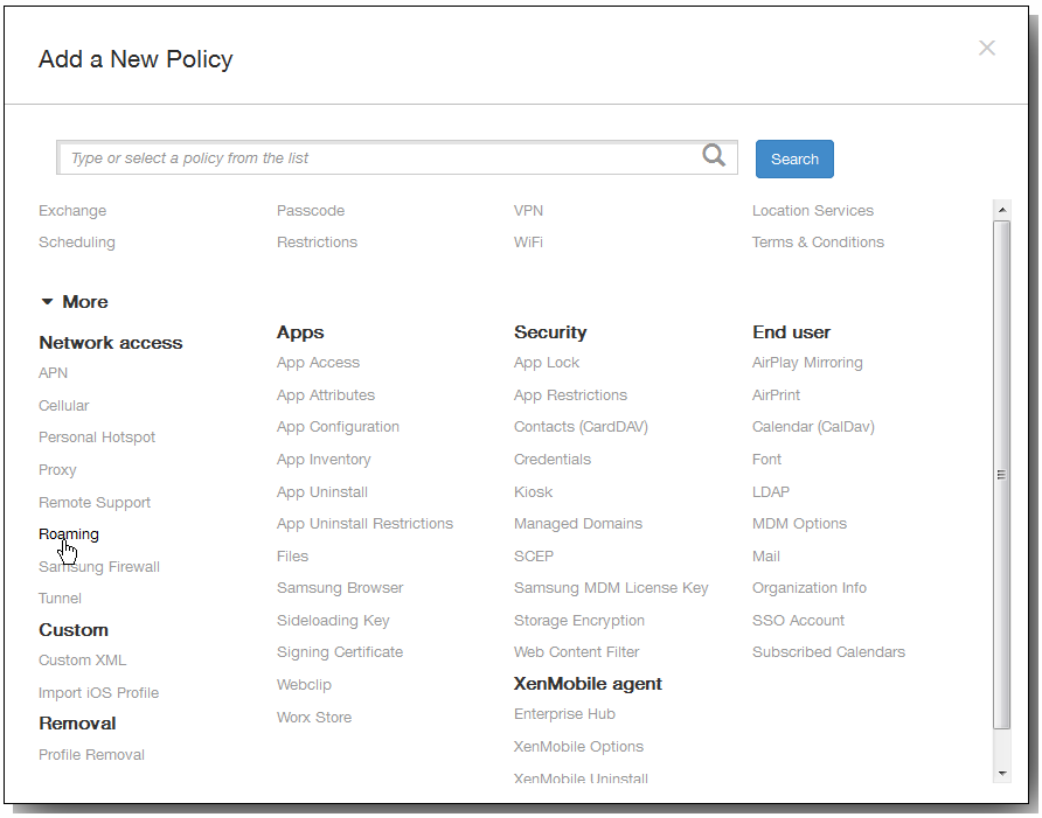
May 06, 2016

Vous pouvez ajouter une stratégie d'itinérance dans XenMobile afin d'activer les services de voix et de données en itinérance sur des appareils iOS. Lorsque l'itinérance de la voix est désactivée, l'itinérance des données est automatiquement désactivée. Cette stratégie est uniquement disponible sur les appareils iOS 5.0 et versions ultérieures.

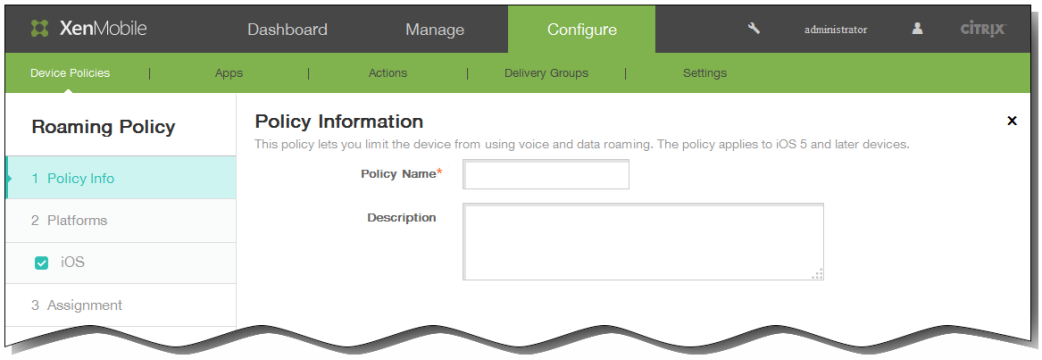
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



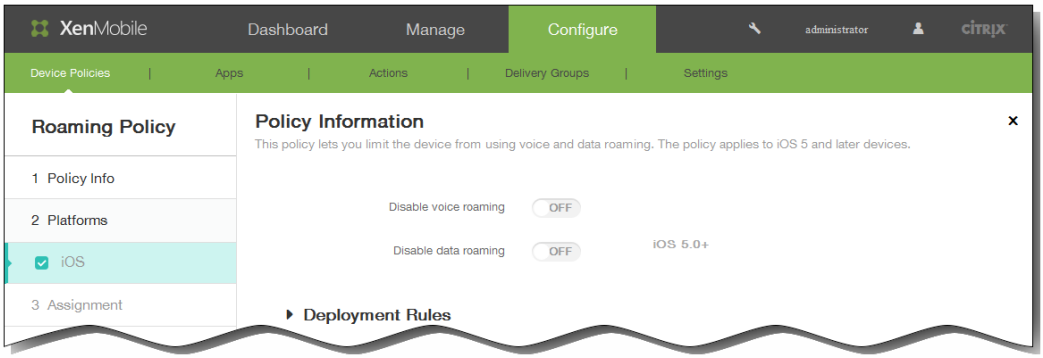
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Accès réseau, cliquez sur Itinérance. La page d'informations sur la Stratégie d'itinérance s'affiche.

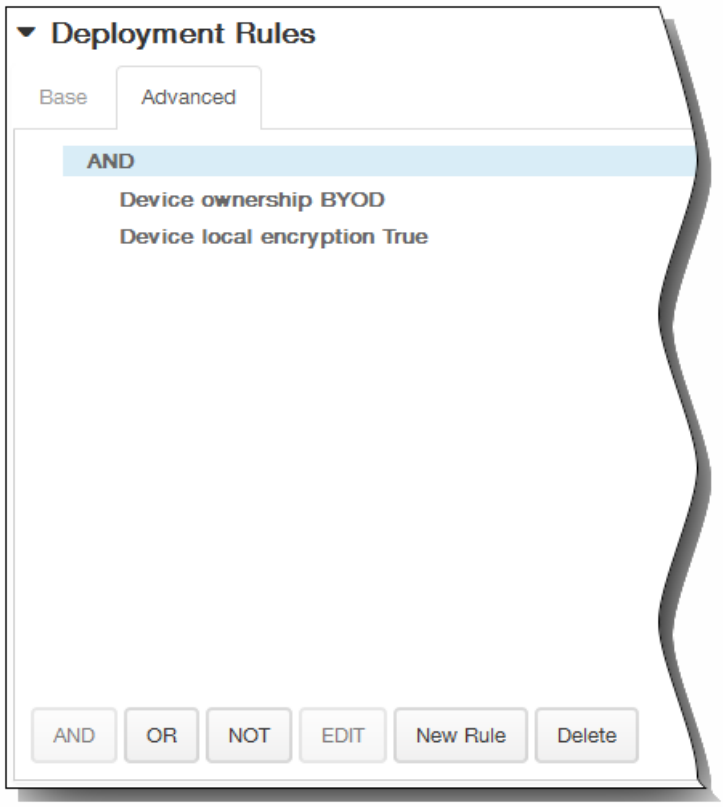


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme iOS s'affiche.



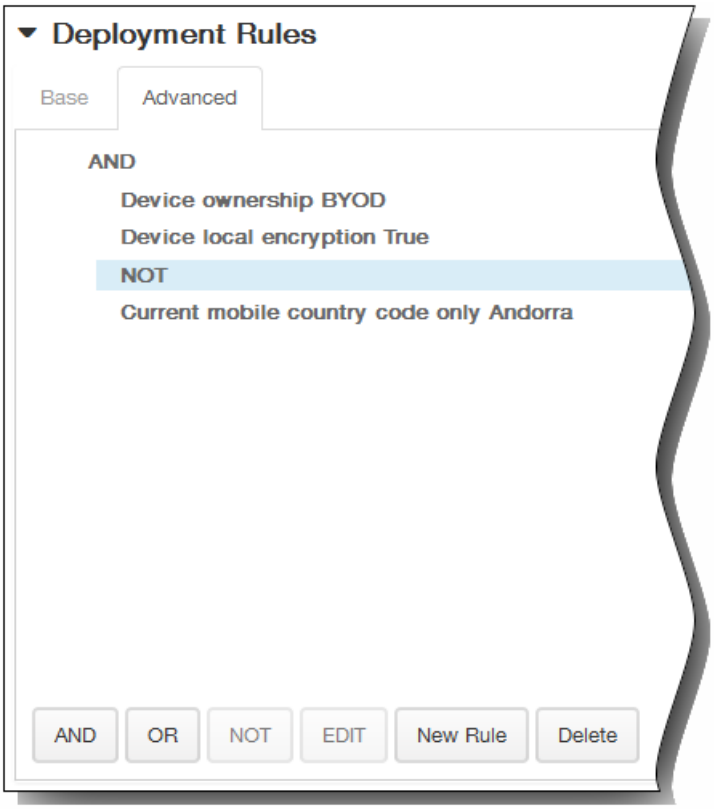
6. Dans la section Informations sur la plate-forme iOS, entrez les informations suivantes :
   1. Désactiver l'itinérance de la voix : sélectionnez cette option pour désactiver l'itinérance vocale. Lorsque cette option est activée, l'itinérance des données est automatiquement désactivée. La valeur par défaut est OFF, ce qui active l'itinérance de la voix.
   2. Désactiver l'itinérance des données : sélectionnez cette option pour désactiver l'itinérance des données. Cette option est disponible uniquement lorsque l'itinérance de la voix est activée. La valeur par défaut est OFF, ce qui active l'itinérance des données.
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.

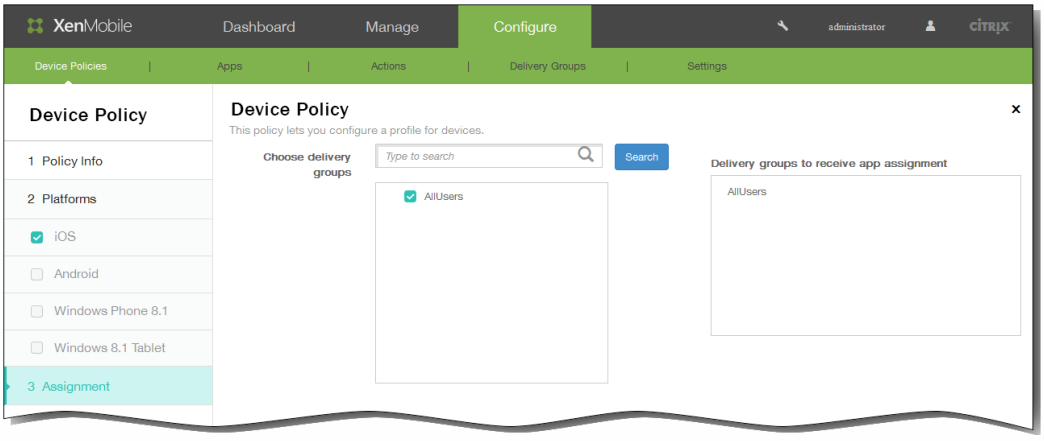


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
       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 d'itinérance 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.

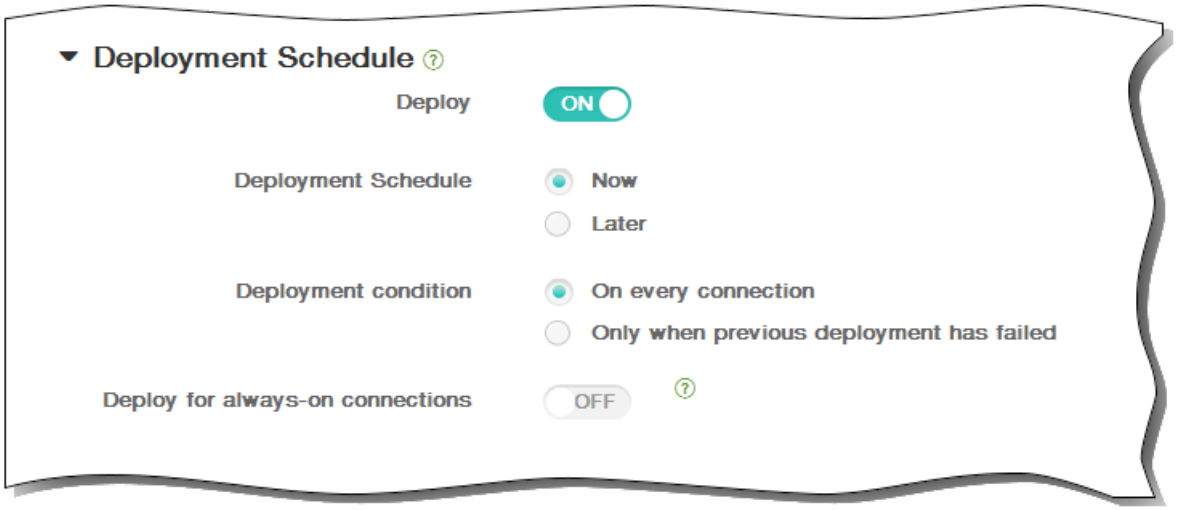


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.



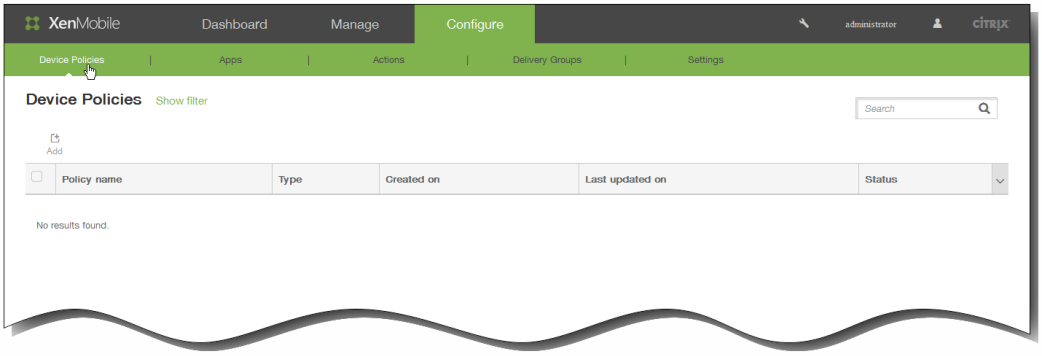
11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie SCEP pour iOS

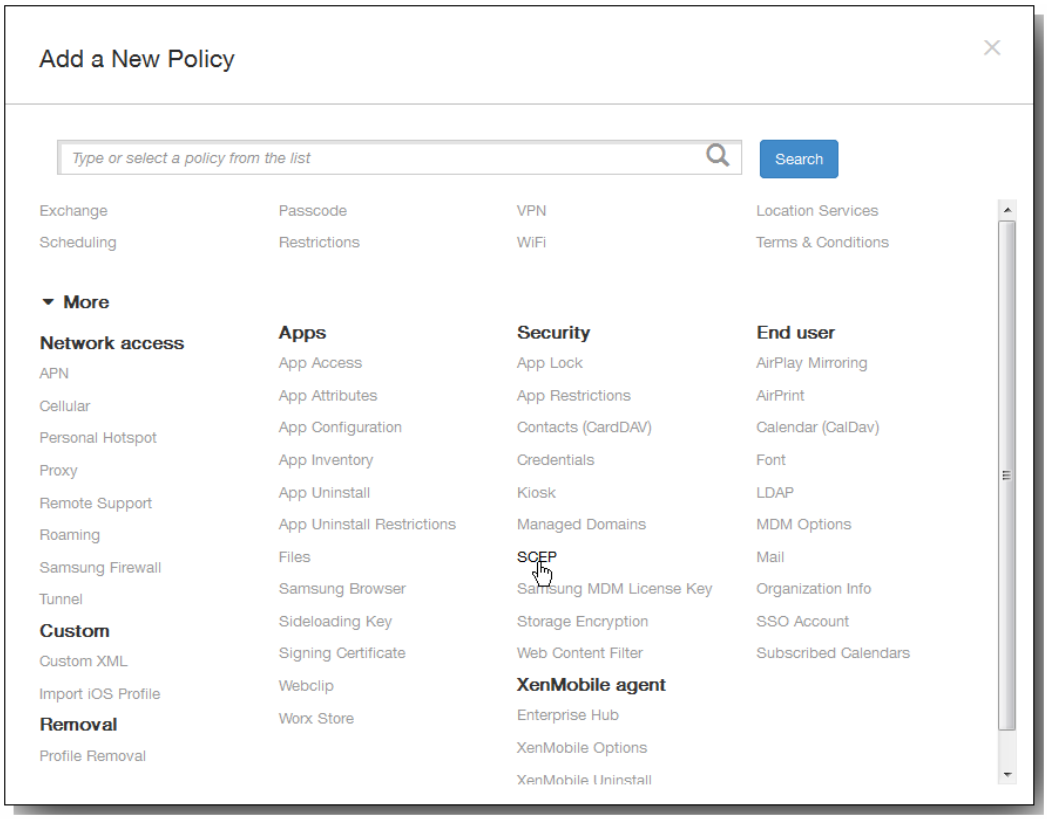
May 06, 2016

Cette stratégie vous permet de configurer des appareils iOS afin de récupérer un certificat à l'aide du protocole d'inscription du certificat simple (SCEP) à partir d'un serveur SCEP externe. Si vous souhaitez délivrer un certificat sur l'appareil à l'aide du protocole SCEP à partir d'une PKI connectée à XenMobile, vous devez créer une entité PKI et un fournisseur PKI en mode distribué. Pour plus d'informations, veuillez consulter la section Entités PKI.

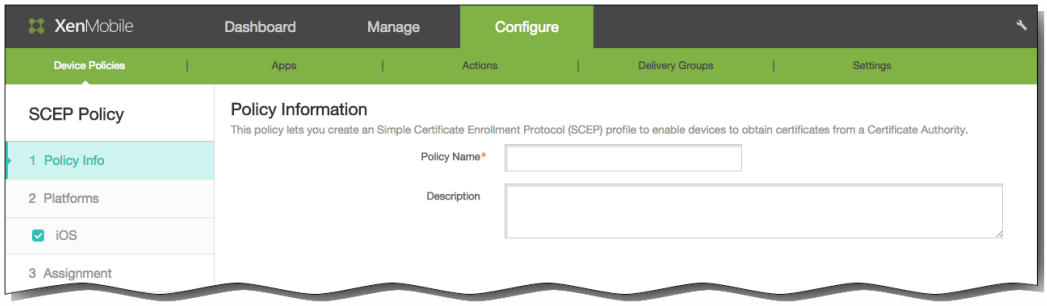
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil.
   La page Stratégies d'appareil s'affiche.



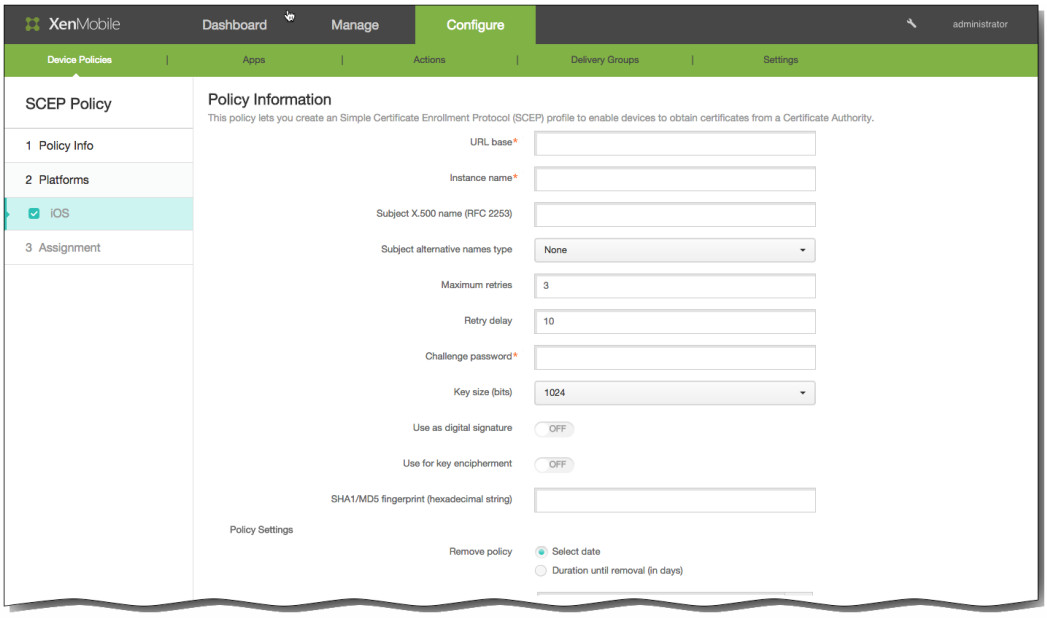
2. Cliquez sur Ajouter.
   La page Ajouter une nouvelle stratégie apparaît.



3. Sur la page Ajouter une nouvelle stratégie, cliquez sur Plus puis sous Sécurité, cliquez sur SCEP.
   La page d'informations Stratégie SCEP 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.

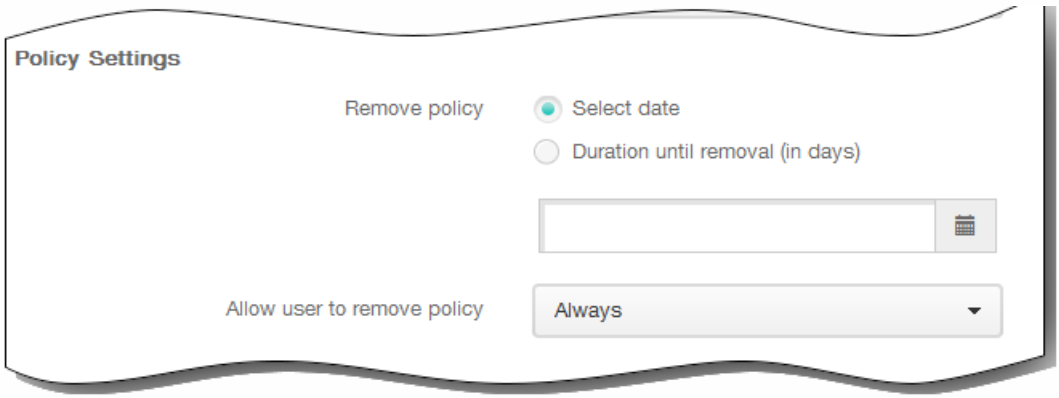


6. Sur la page Informations sur la plate-forme iOS, entrez les informations suivantes :
    1. URL de base : entrez l'adresse du serveur SCEP afin de définir où les demandes SCEP sont envoyées, par HTTP ou HTTPS. La clé privée n'est pas envoyée avec la demande de signature de certificat (CSR), il est donc possible d'envoyer la demande non chiffrée sans danger. Si, toutefois le mot de passe à usage unique est autorisé à être réutilisé, vous devez utiliser le protocole HTTPS pour protéger le mot de passe. Cette étape est requise.
    2. Nom d'instance : entrez une chaîne reconnue par le serveur SCEP. Par exemple, il peut s'agir d'un nom de domaine comme exemple.org. Si une autorité de certification dispose de plusieurs certificats d'autorité de certification, vous pouvez utiliser ce champ pour différencier le domaine requis. Cette étape est requise.
    3. Nom X.500 du sujet (RFC 2253) : entrez la représentation d'un nom X.500 représentée sous forme de tableau d'identificateurs d'objets (OID) et de valeurs. Par exemple, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, qui correspond à : [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]. Les OID peuvent être représentés en tant que nombres en pointillé, avec des raccourcis pour le pays (C), la ville (L), l'état (ST), l'organisation (O), l'unité d'organisation (OU) et le nom commun (CN).
    4. Type de noms de sujet alternatifs : sélectionnez un type de nom alternatif dans la liste. La stratégie SCEP permet de spécifier un type de nom alternatif facultatif qui fournit les valeurs requises par l'autorité de certification pour l'émission d'un certificat. Vous pouvez spécifier Aucun, Nom RFC 822, Nom DNS ou URI.
    5. Nombre maximal de tentatives : entrez le nombre de tentatives autorisées en cas de saisie incorrecte d'un mot de passe. La valeur par défaut est 3.
    6. Délai de nouvelle tentative : Entrez un intervalle de temps suite auquel les utilisateurs dépassent le nombre maximal de tentatives et le verrou est forcé. La valeur par défaut est 10.
    7. Vérifier le mot de passe : entrez un secret pré-partagé. Cette étape est requise.
    8. Taille de la clé (bits) : dans la liste, cliquez sur la taille de la clé en bits, 1024 ou 2048. La valeur par défaut est 1024.
    9. Utiliser une signature numérique : spécifiez si vous souhaitez que le certificat soit utilisé en tant que signature numérique. Si le certificat est utilisé pour vérifier une signature numérique, comme vérifier si un certificat a été émis par une autorité de certification, le serveur SCEP vérifie que le certificat peut être utilisé de cette façon avant d'utiliser la clé publique pour déchiffrer le hachage.
    10. Utiliser pour le chiffrement des clés : spécifiez si vous souhaitez que le certificat soit utilisé pour le chiffrement des clés. Si un serveur utilise la clé publique dans un certificat fourni par un client pour vérifier qu'une partie des données a été chiffrée à l'aide de la clé privée, le serveur vérifie d'abord si le certificat peut être utilisé pour le chiffrement de la

clé. Sinon, l'opération échoue.

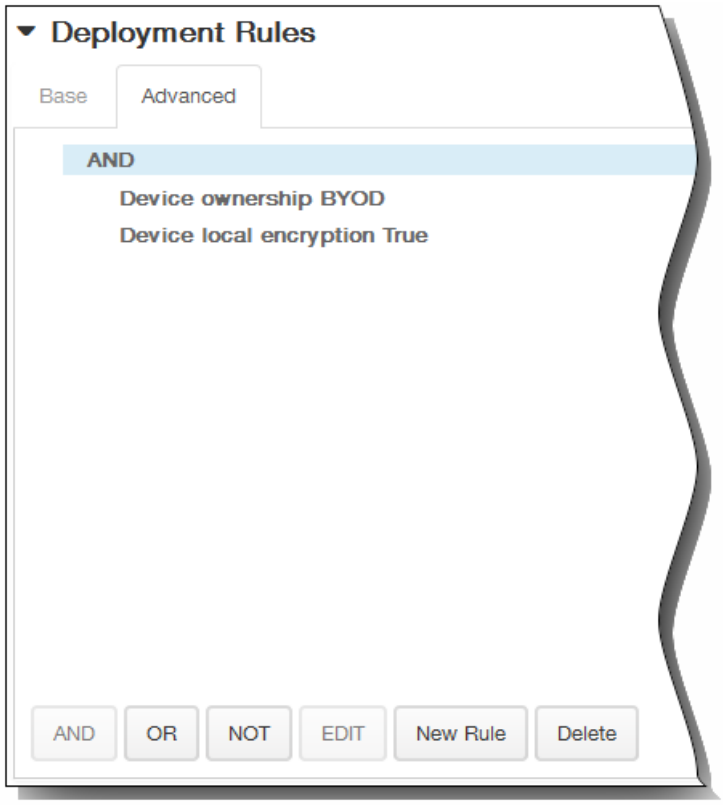
11. Empreinte digitale SHA1/MD5 (chaîne hexadécimale) : si votre Autorité de certification utilise le protocole HTTP, utilisez ce champ pour fournir l'empreinte digitale du certificat de la CA, que l'appareil utilise pour vérifier l'authenticité de la réponse de l'autorité de certification au cours de l'inscription. Vous pouvez entrer une empreinte digitale MD5 ou SHA1, ou vous pouvez sélectionner un certificat pour importer sa signature.

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.

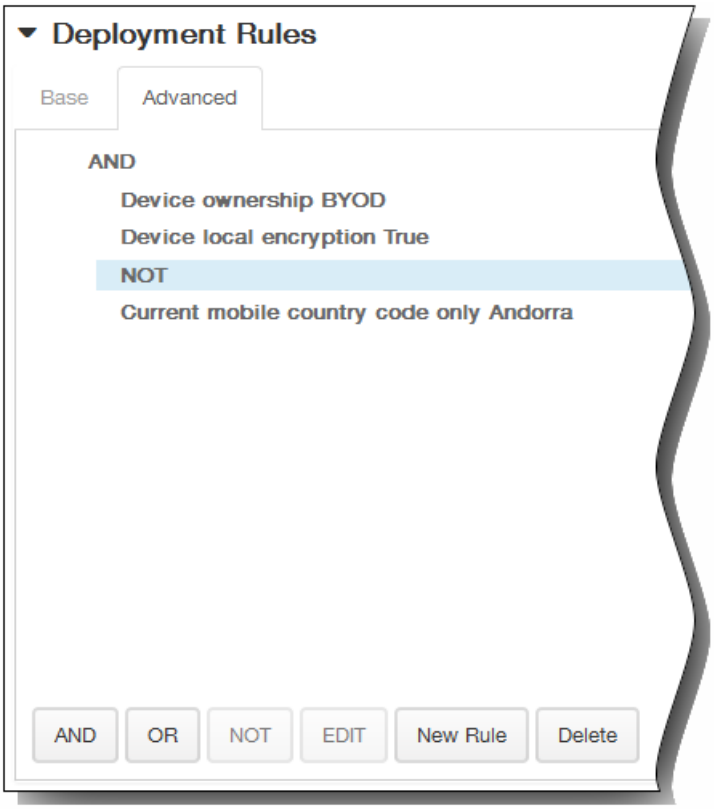
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



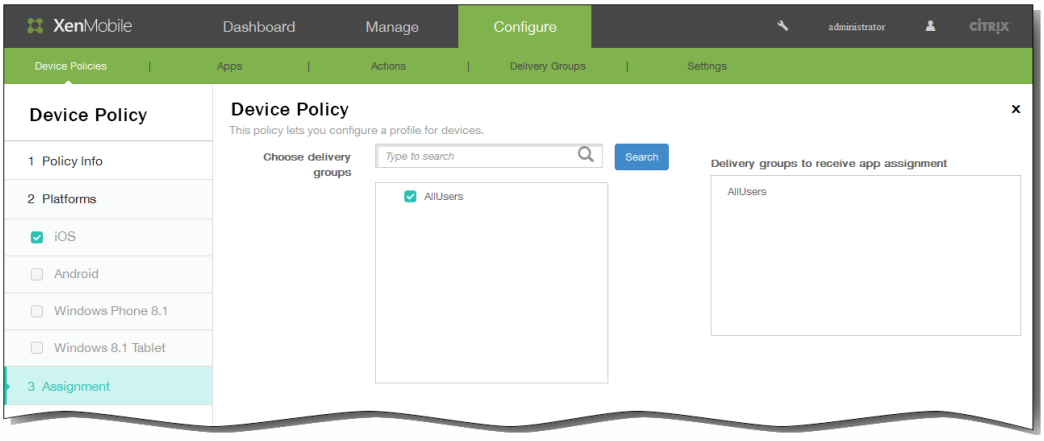
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie SCEP 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.

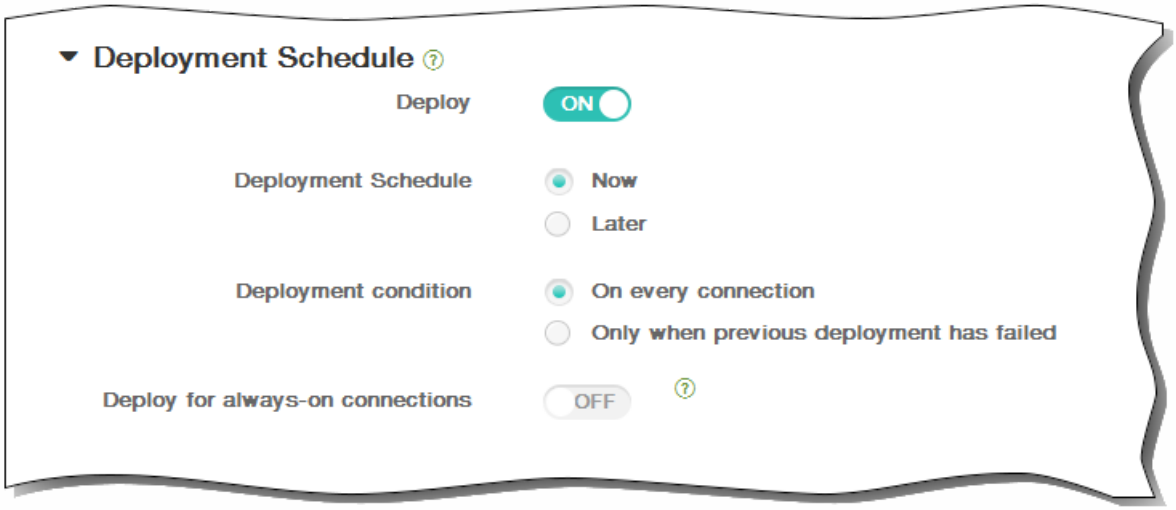


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.

Stratégies de clé de licence MDM Samsung

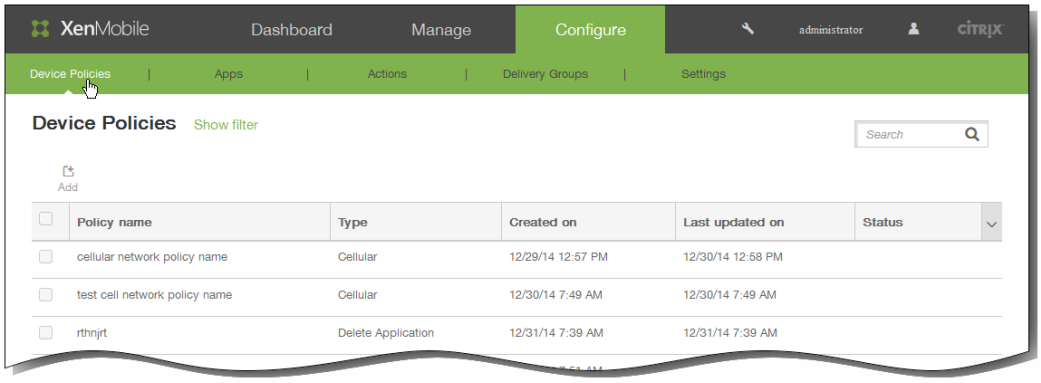
May 06, 2016

XenMobile prend en charge et étend les stratégies Samsung for Enterprise (SAFE) et Samsung KNOX. SAFE fait partie d'une famille de solutions qui fournit des améliorations de sécurité pour les entreprises via l'intégration à des solutions MDM. Samsung KNOX est une solution du programme SAFE destinée à une utilisation professionnelle conçue pour renforcer la sécurité sur la plate-forme Android.

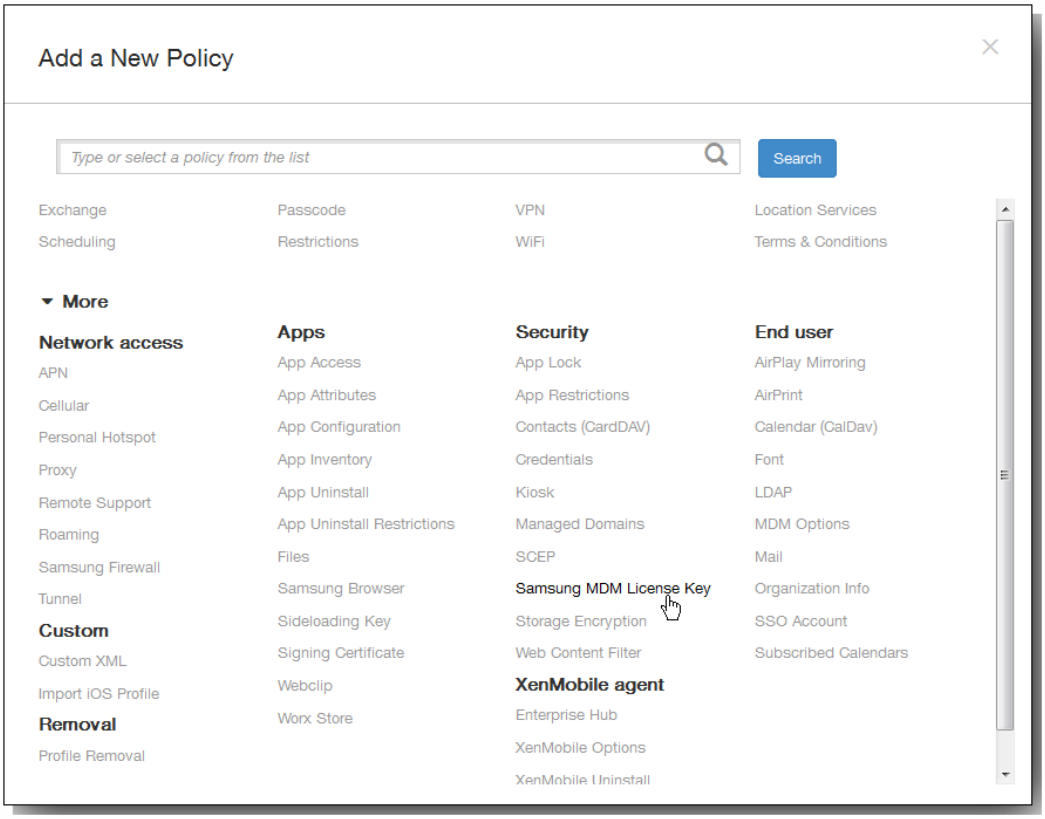
Vous devez activer les API SAFE en déployant la clé Samsung ELM (Enterprise License Management) intégrée sur un appareil avant de pouvoir déployer des stratégies et restrictions SAFE. Pour activer les API Samsung KNOX, vous devez acheter une licence Samsung KNOX à l'aide du Samsung KNOX License Management System (KLMS) en plus de déployer la clé Samsung ELM. Le KMLS Samsung provisionne des licences valides sur des solutions MDM afin d'activer les API Samsung KNOX sur les appareils mobiles. Vous devez vous procurer ces licences auprès de Samsung car elles ne sont pas fournies par Citrix.

Vous devez déployer Worx Home en conjonction avec la clé Samsung ELM pour activer les API SAFE et Samsung KNOX. Vous pouvez vérifier que les API SAFE sont activés en consultant les propriétés de l'appareil. Lorsque la clé Samsung ELM est déployée, le paramètre API Samsung MDM disponible est défini sur True.

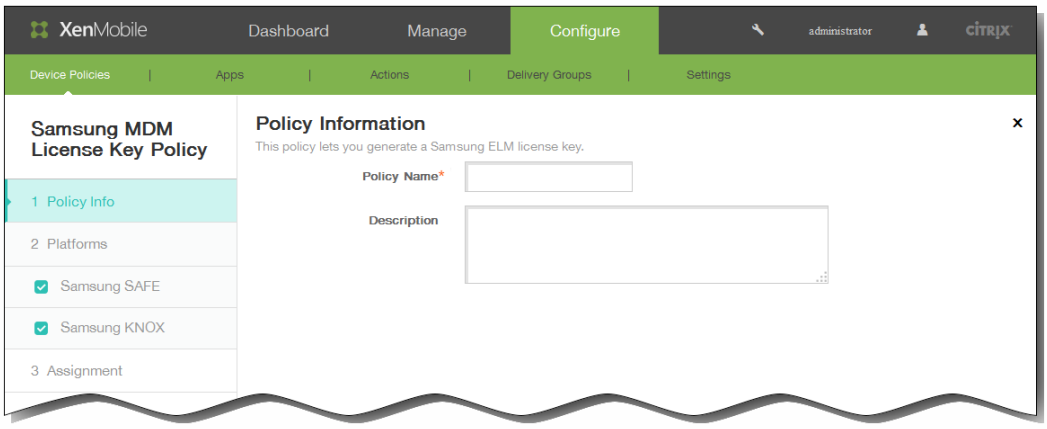
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



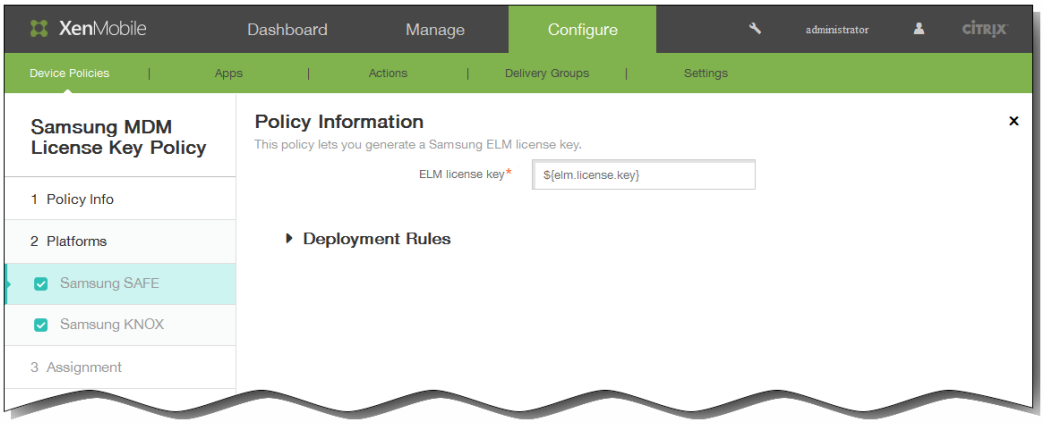
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie s'affiche.



3. Cliquez sur Plus, puis sous Sécurité, cliquez sur Clé de licence MDM Samsung. La page d'informations Stratégie de clé de licence MDM Samsung s'affiche.

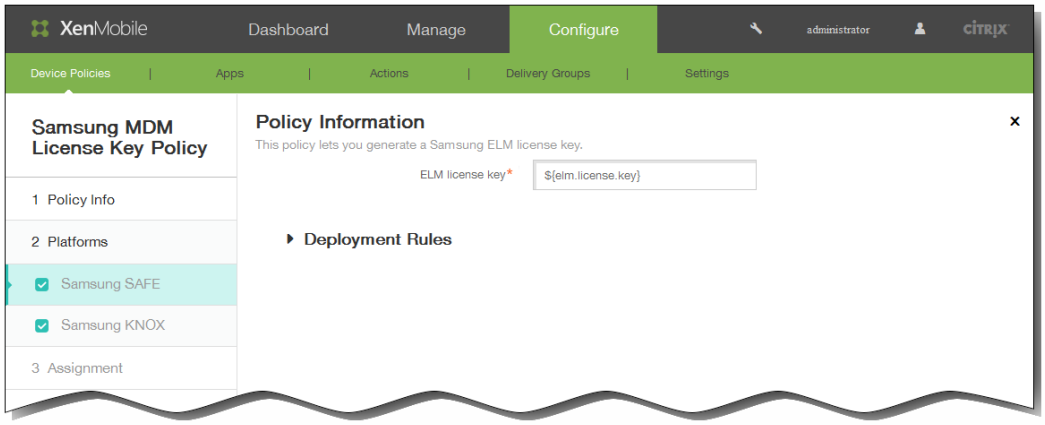


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Stratégie par plate-forme s'affiche.
   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 Samsung SAFE s'affiche.

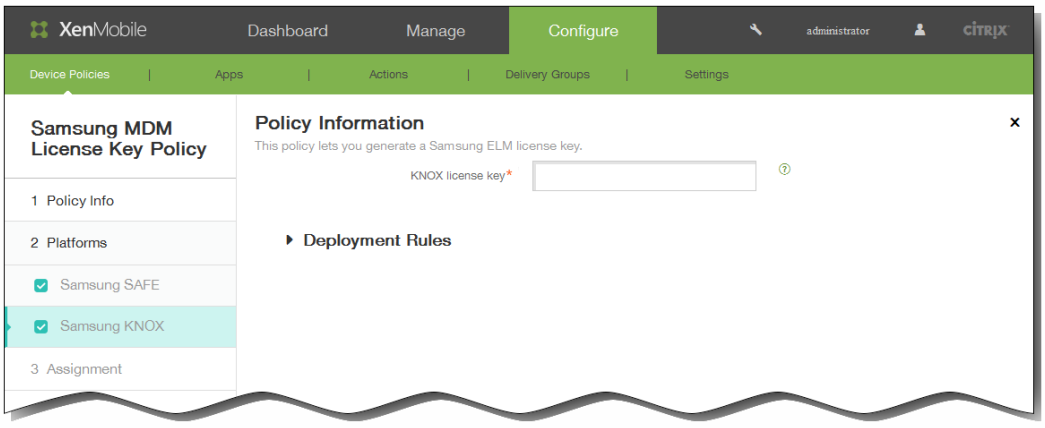


6. Sous Plates-formes, choisissez les plates-formes Samsung pour lesquelles vous voulez créer cette stratégie. Effacez toute autre plate-forme pouvant être sélectionnée que vous ne souhaitez pas inclure dans cette stratégie.

   - Si vous choisissez Samsung SAFE, pour la clé de licence ELM, entrez la macro ${elm.license.key} pour générer la clé de licence ELM. Le champ doit déjà contenir la macro :

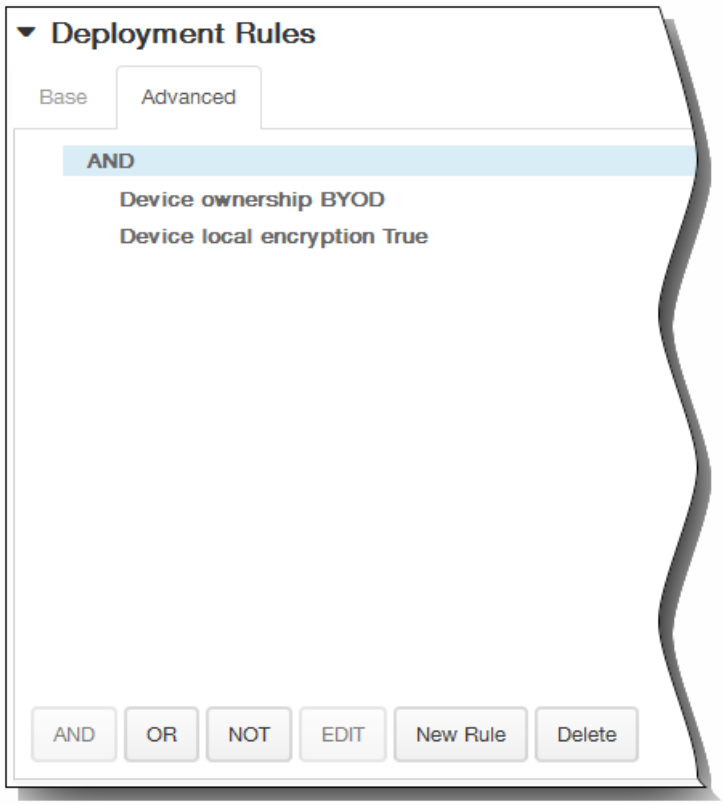


   - Si vous choisissez Samsung KNOX, pour la clé de licence KNOX, entrez la clé de licence KNOX à 25 caractères :



7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

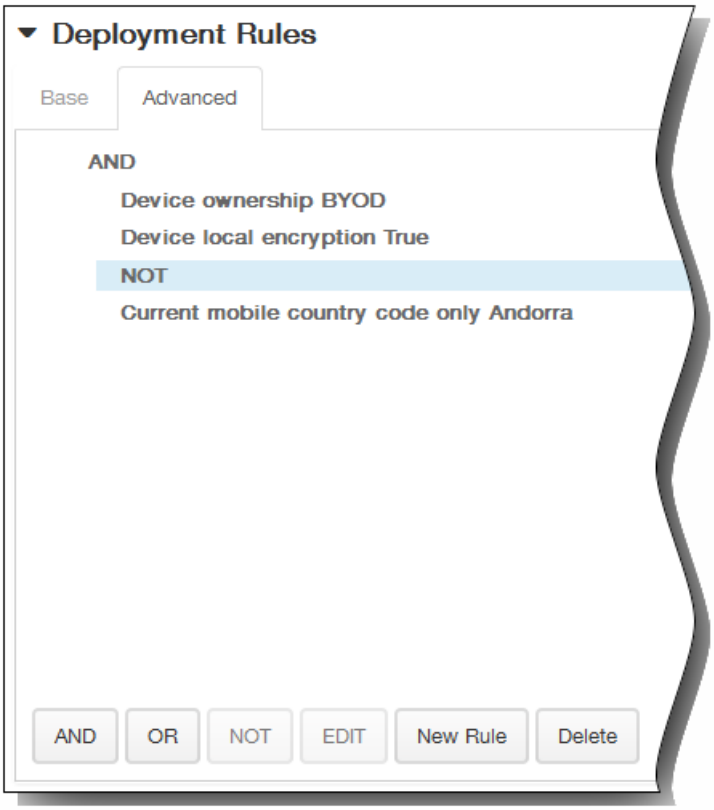
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



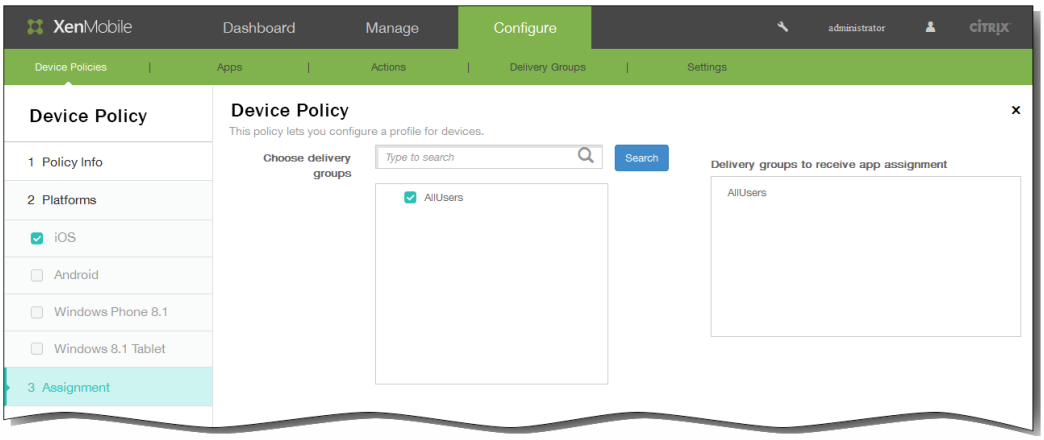
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      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.



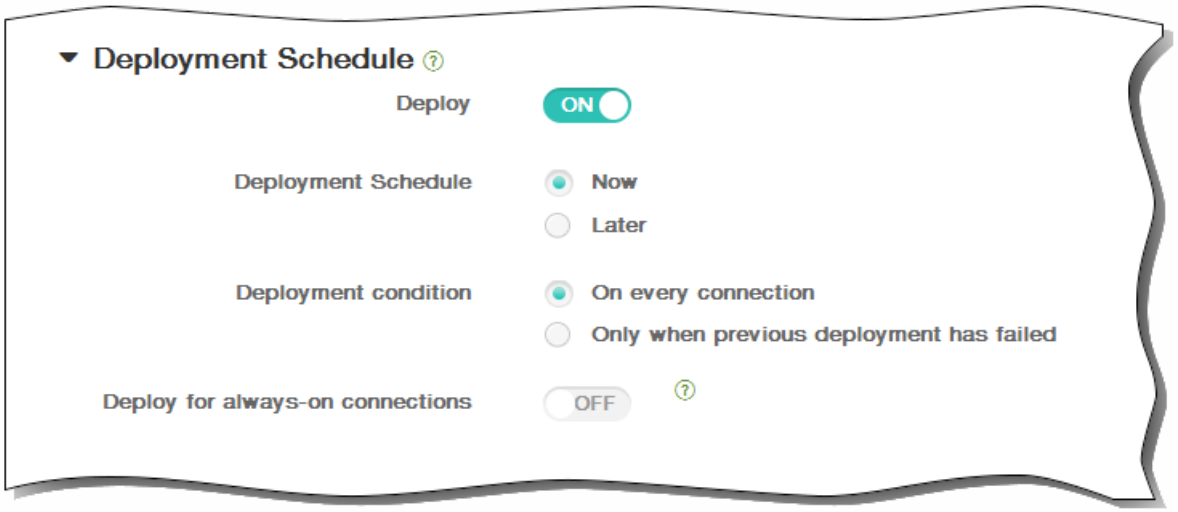
8. Cliquez sur Suivant. La page Stratégie de clé de licence MDM Samsung s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de chiffrement du stockage

May 06, 2016

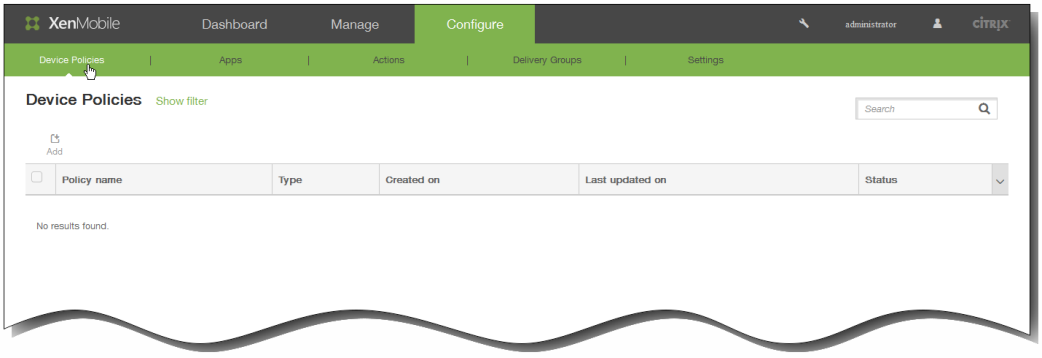
Vous pouvez créer des stratégies de chiffrement du stockage dans XenMobile pour chiffrer le stockage interne et externe, et, en fonction de l'appareil, pour empêcher les utilisateurs d'utiliser une carte de stockage sur leurs appareils.

Vous pouvez créer des stratégies pour Samsung SAFE, Windows 8.1 Tablet et Android Sony. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans les étapes suivantes.

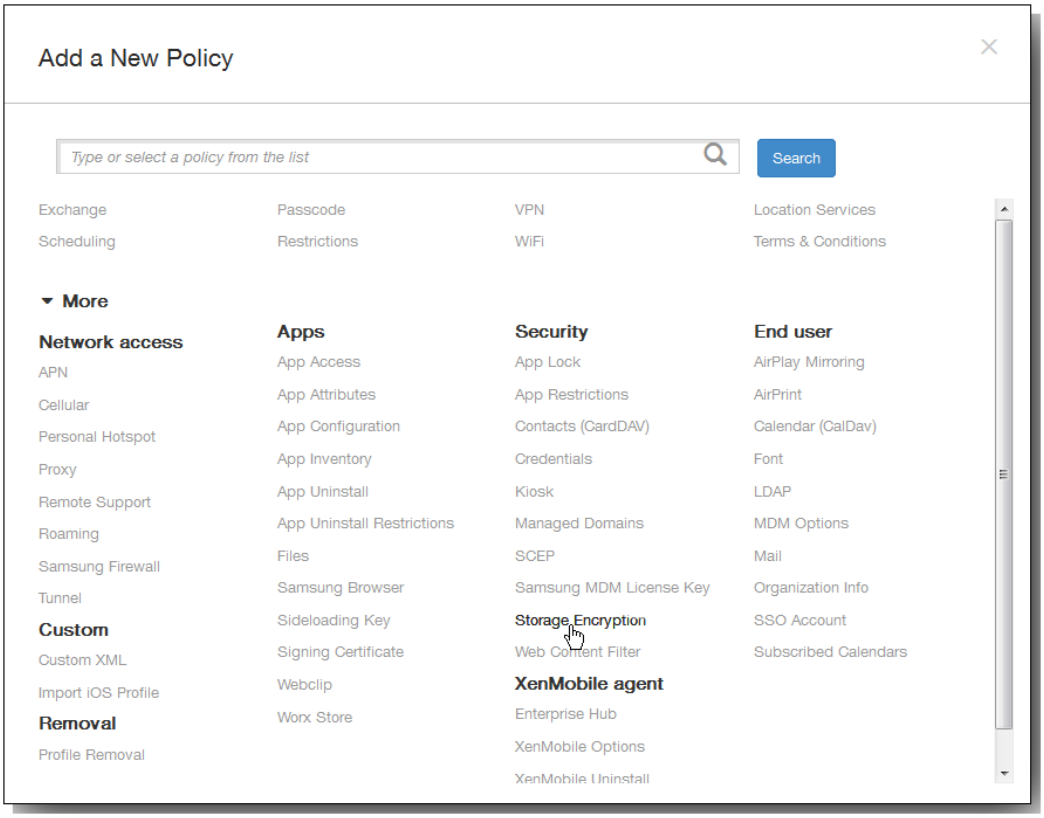
Remarque : pour les appareils Samsung SAFE, vérifiez que les conditions suivantes soient remplies avant de configurer cette stratégie :

- Vous devez définir l'option de verrouillage d'écran sur les appareils des utilisateurs.
- Les appareils doivent être branchés et chargés à 80 %.
- L'appareil doit exiger un mot de passe contenant des chiffres et des lettres ou des symboles.

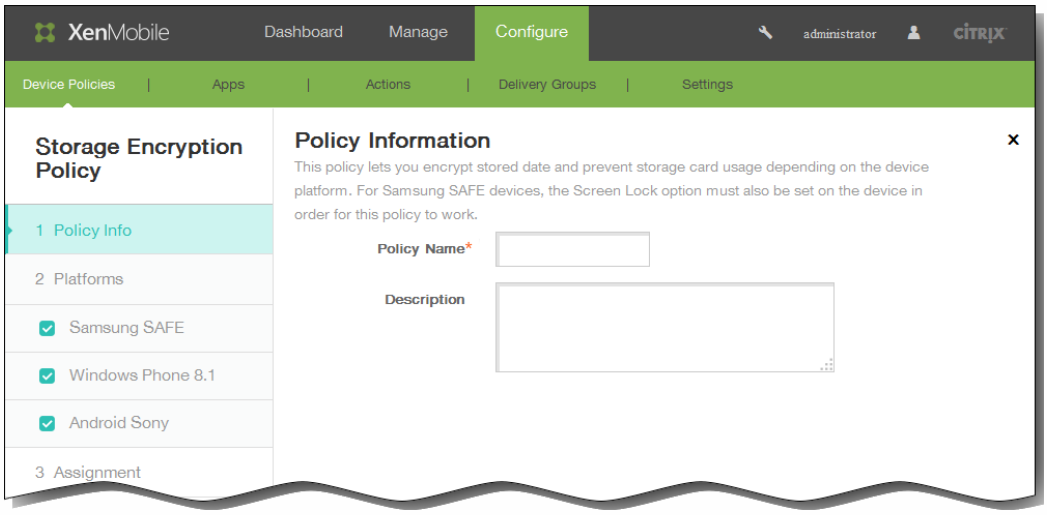
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

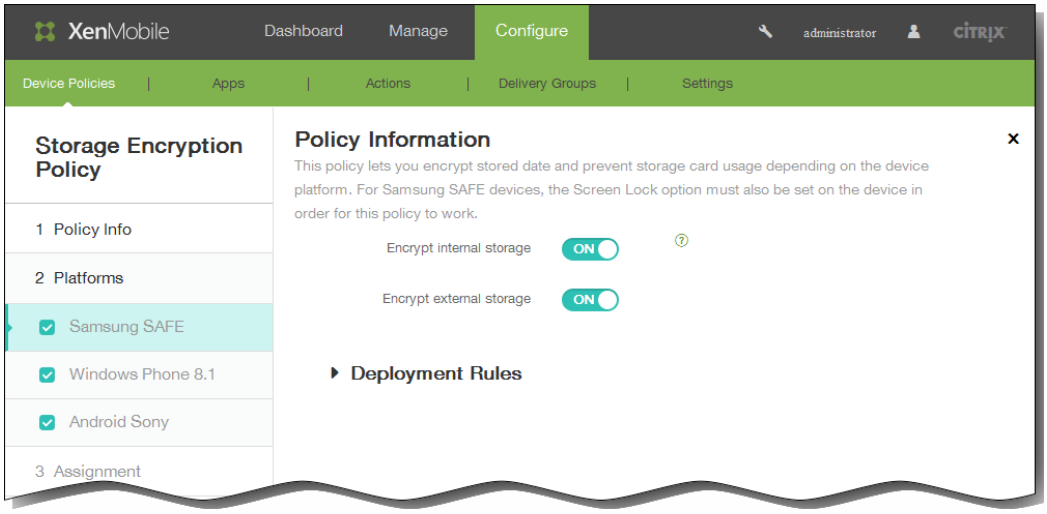


3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Chiffrement du stockage. La page d'informations sur la Stratégie de chiffrement du stockage s'affiche.

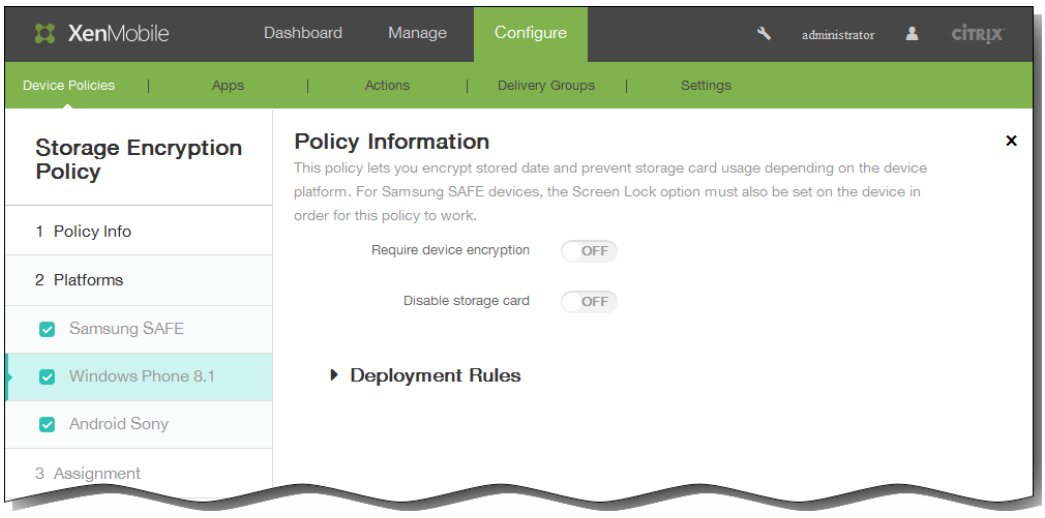


4. Dans le panneau Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Stratégie par plate-forme s'affiche.
   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 Samsung SAFE s'affiche.

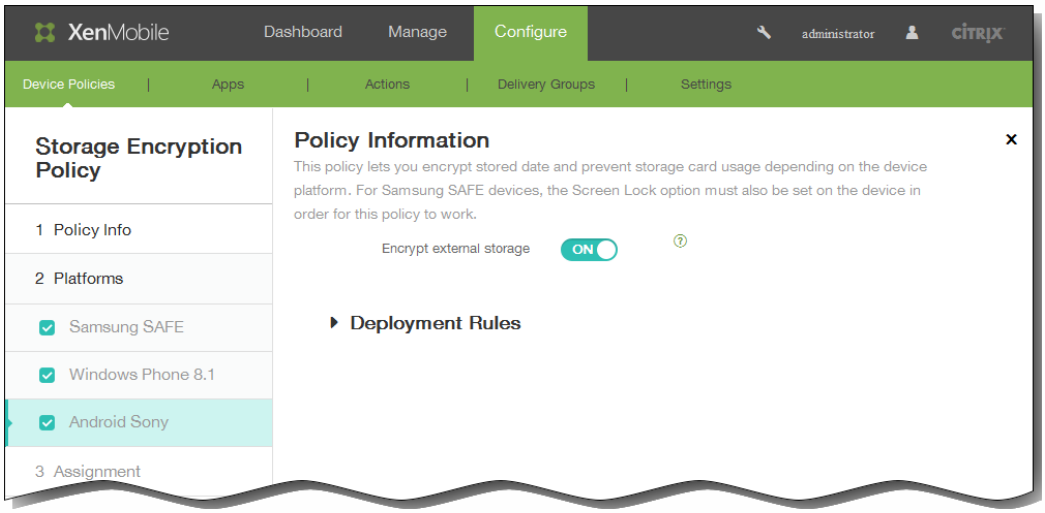
6. Sous Plates-formes, sélectionnez les plates-formes pour lesquelles vous voulez configurer cette stratégie. S'il s'agit de la seule plate-forme que vous configurez, désélectionnez toutes les autres plates-formes.
   - Si vous sélectionnez Samsung SAFE :
     - Chiffrer le stockage interne : sélectionnez cette option pour chiffrer le stockage interne sur les appareils des utilisateurs. Le stockage interne inclut la mémoire de l'appareil et le stockage interne. La valeur par défaut est ON.
     - Chiffrer le stockage externe : sélectionnez cette option pour chiffrer le stockage externe sur les appareils des utilisateurs. La valeur par défaut est ON.



   - Si vous sélectionnez Windows Phone 8.1 :
     - Activer le chiffrement de l'appareil : sélectionnez cette option pour chiffrer les appareils des utilisateurs. La valeur par défaut est OFF.
     - Désactiver la carte de stockage : sélectionnez cette option pour empêcher les utilisateurs d'utiliser une carte de stockage sur leurs appareils. La valeur par défaut est OFF.

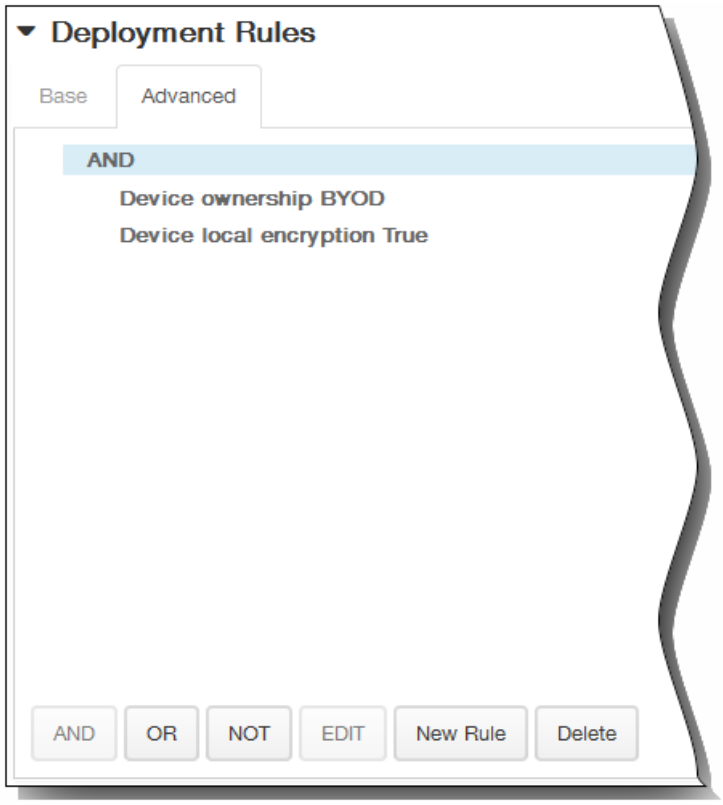


   - Si vous sélectionnez Android Sony, pour Chiffrer le stockage externe, choisissez si vous souhaitez chiffrer le stockage externe sur les appareils des utilisateurs. L'appareil doit exiger un mot de passe contenant des chiffres et des lettres ou des symboles. La valeur par défaut est ON.



7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

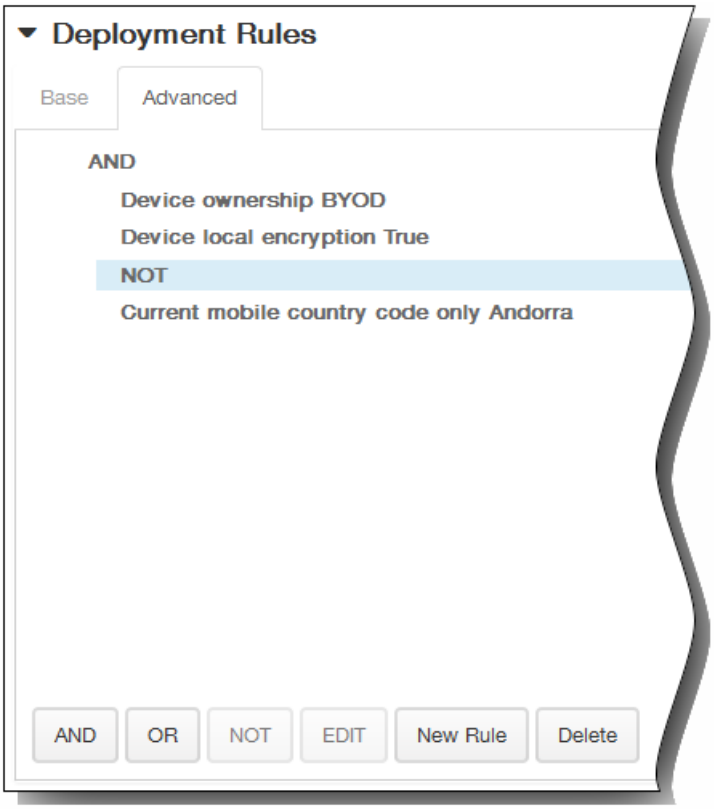
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



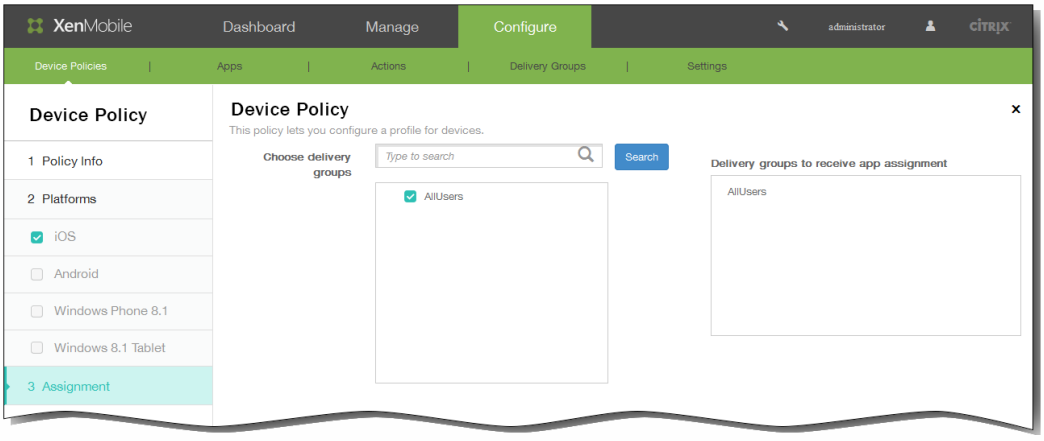
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



8. Cliquez sur Suivant. La page d'attribution de la Stratégie de chiffrement du stockage 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.

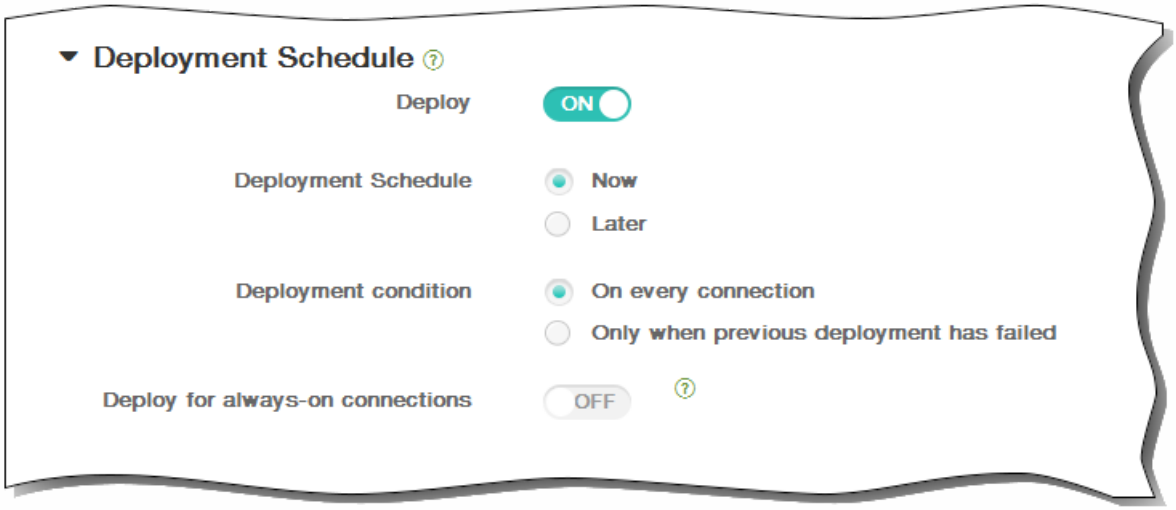


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.



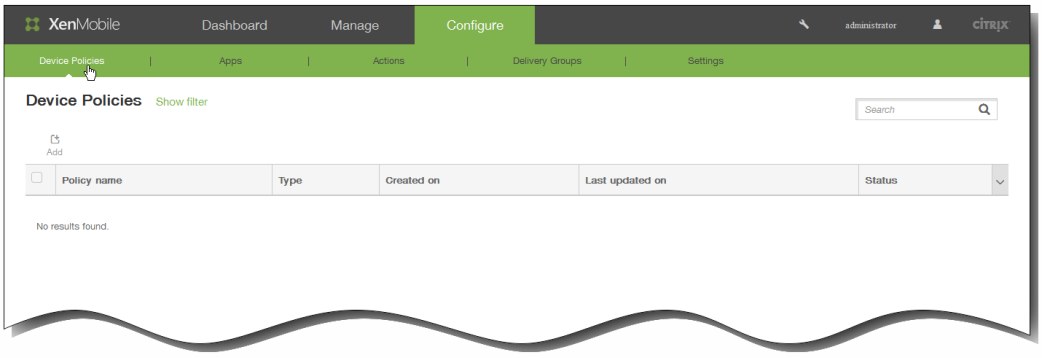
11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de filtre de contenu Web pour iOS

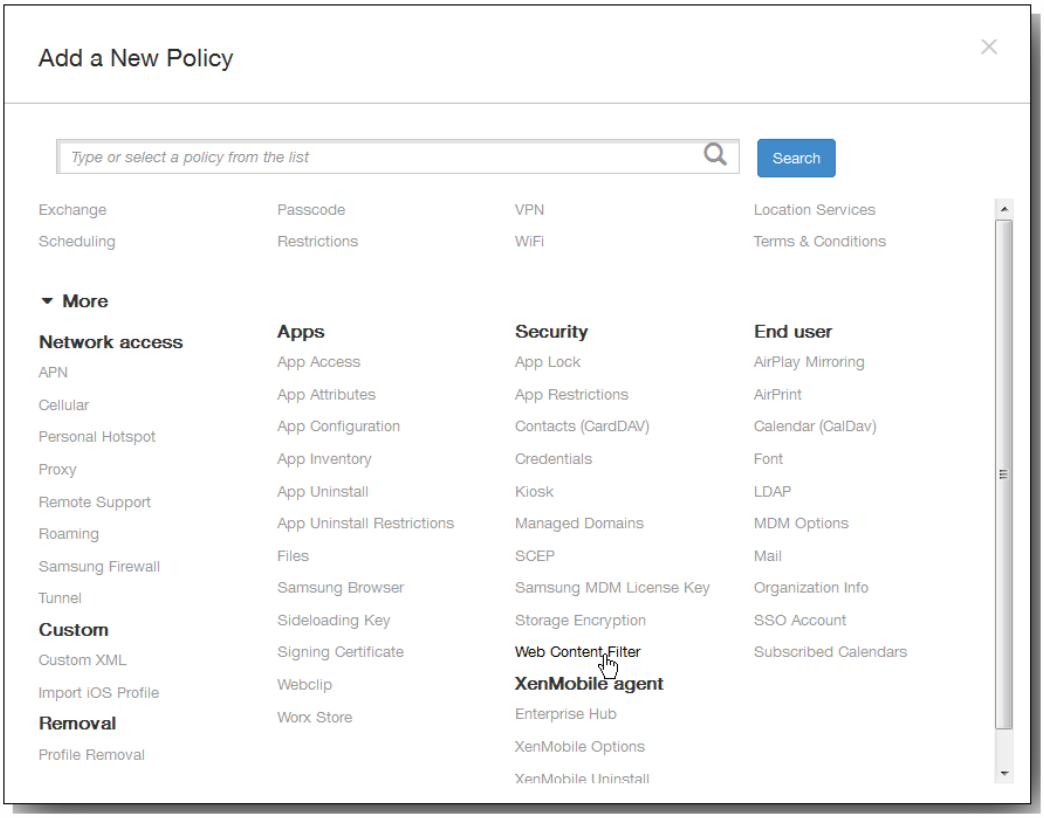
May 06, 2016

Vous pouvez ajouter une stratégie dans XenMobile destinée à filtrer le contenu Web sur les appareils iOS à l'aide de la fonction de filtrage automatique d'Apple en conjonction avec les sites spécifiques que vous ajoutez aux listes blanches et listes noires. Cette stratégie est uniquement disponible sur les appareils iOS 7.0 et versions ultérieures en mode Supervisé. Pour de plus amples informations sur le placement d'un appareil iOS en mode supervisé, consultez la section Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator.

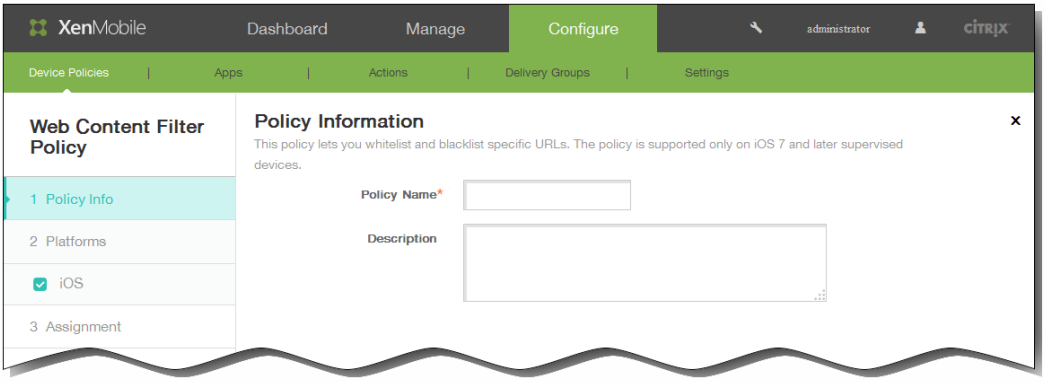
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



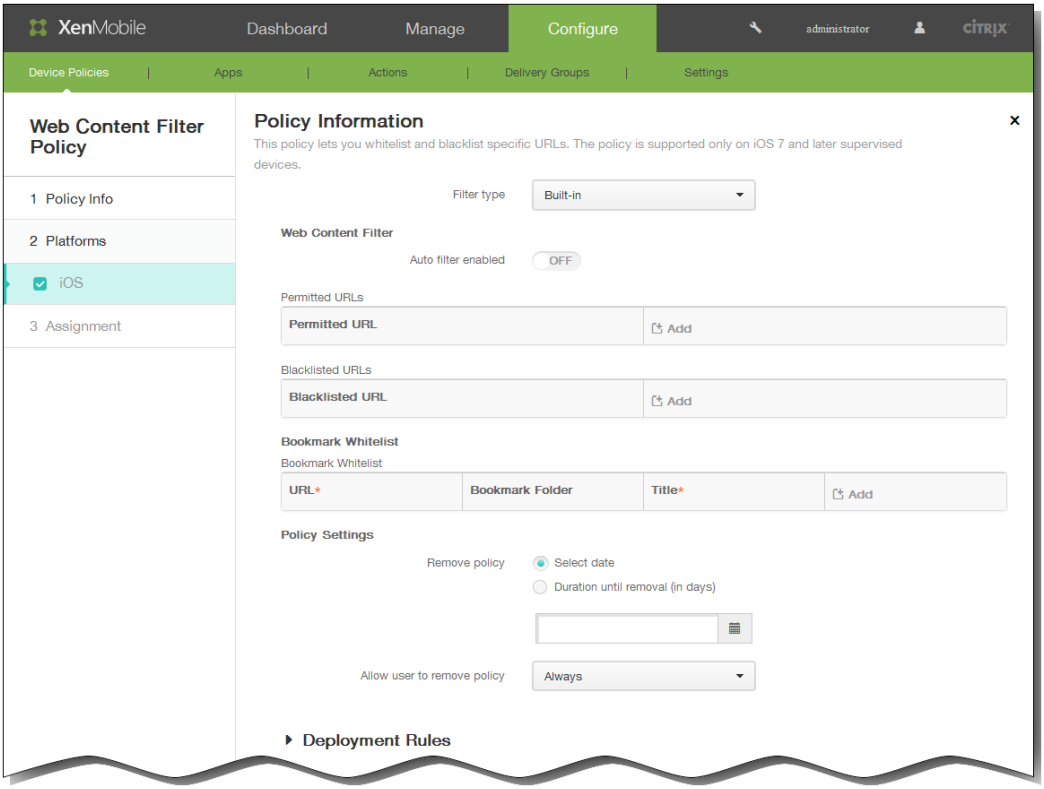
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus puis, sous Sécurité, cliquez sur Filtre de contenu Web. La page Stratégie de filtre de contenu Web 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. Dans la page Informations sur la plate-forme iOS, dans la liste Type de filtre, effectuez l'une des opérations suivantes et suivez les procédures détaillées dans cette rubrique pour décider de l'option à choisir :
   - Conservez la valeur de type de filtre par défaut Intégré.
   - Cliquez sur Plug-in pour configurer le type de filtre Plug-in.

   Pour configurer le type de filtre Intégré

   1. Filtrage automatique activé : sélectionnez cette option pour spécifier si vous souhaitez utiliser la fonction de filtrage automatique d'Apple afin de détecter tout contenu inapproprié sur les sites Web. La valeur par défaut est OFF.
   2. URL autorisées : cette liste est ignorée lorsque l'option Filtrage automatique activé est définie sur OFF. Lorsque l'option Filtrage automatique activé est définie sur ON, les éléments figurant dans cette liste sont toujours accessibles que le filtrage automatique en permette l'accès ou non.
      Cliquez sur Ajouter, puis effectuez les opérations suivantes pour ajouter des sites Web à la liste blanche :

      1. Entrez l'adresse URL du site Web autorisé. Vous devez ajouter http:// ou https:// avant l'adresse Web.
      2. Cliquez sur Enregistrer pour enregistrer le site Web dans la liste blanche ou cliquez sur Annuler pour ne pas l'enregistrer.
      3. Répétez les étapes i et ii pour chaque site Web que vous voulez ajouter à la liste blanche.
   3. URL sur liste noire : les éléments dans cette liste sont toujours bloqués.
      Cliquez sur Ajouter, puis procédez comme suit pour ajouter des sites Web à la liste noire :

      1. Entrez l'adresse URL du site Web à bloquer. Vous devez ajouter http:// ou https:// avant l'adresse Web.
      2. Cliquez sur Enregistrer pour enregistrer le site Web dans la liste noire ou cliquez sur Annuler pour ne pas l'enregistrer.
      3. Répétez les étapes i et ii pour chaque site Web que vous voulez ajouter à la liste noire.
   4. Liste blanche signets : les éléments dans cette liste sont les seuls sites auxquels les utilisateurs peuvent accéder.
      Cliquez sur Ajouter, puis procédez comme suit pour ajouter des sites Web à vos favoris :

      1. URL : entrez l'adresse URL du site Web à ajouter aux favoris. Vous devez ajouter http:// ou https:// avant l'adresse

Web. Ce champ est obligatoire.

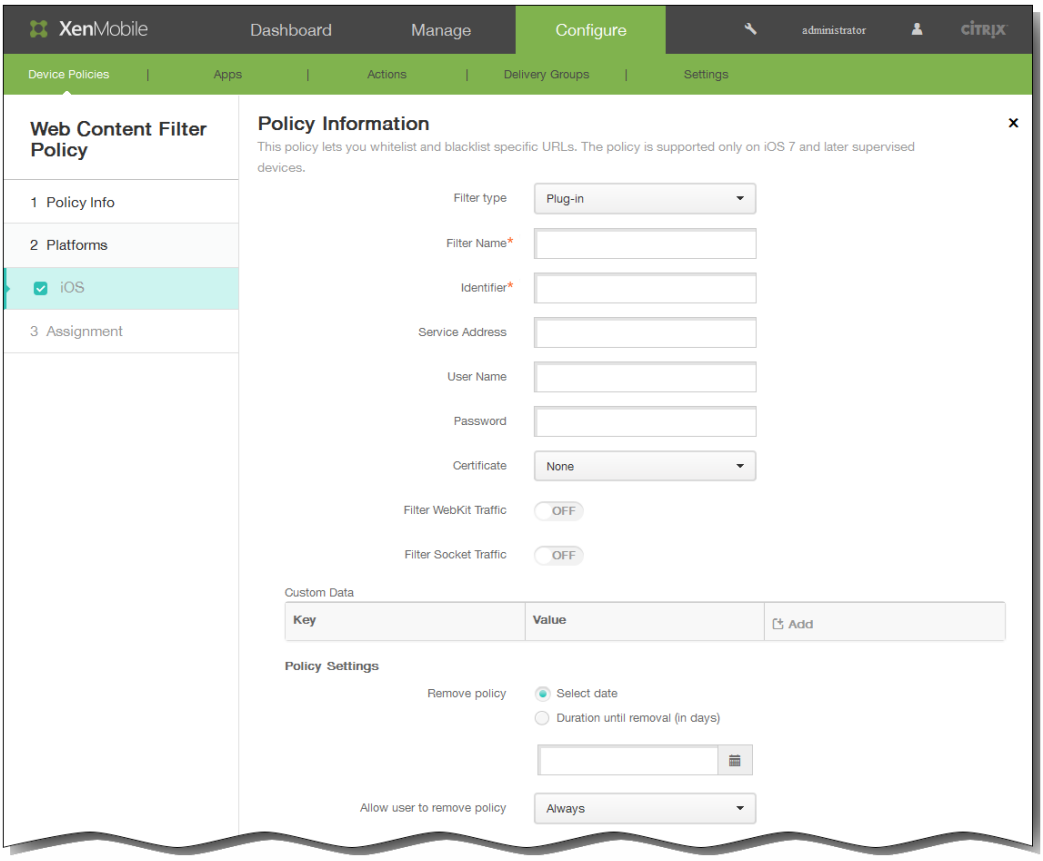
2. Dossier de signets : entrez un nom de dossier des signets (facultatif). Si ce champ est vide, le signet est ajouté au répertoire de signets par défaut.
3. Titre : entrez un titre descriptif pour le site Web. Par exemple, tapez « Google » pour l'adresse URL http://google.fr.
4. Cliquez sur Enregistrer pour enregistrer le site Web dans la liste noire ou cliquez sur Annuler pour ne pas l'enregistrer.
5. Répétez les étapes i à iv pour chaque site Web à marquer d'un signet.

Remarque : pour supprimer un site Web 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 site Web, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille 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.

5. Consultez l'étape 7 pour terminer la configuration du filtre Intégré.

Pour configurer le type de filtre Plug-in



1. Nom du filtre : entrez un nom unique pour le filtre.
2. Identifiant : entrez le Bundle ID du plug-in qui fournit le service de filtrage.
3. Adresse du service : entrez une adresse de serveur (facultatif). Les formats valides sont une adresse IP, un nom d'hôte ou une adresse URL.
4. Nom d'utilisateur : entrez un nom d'utilisateur pour le service (facultatif).
5. Mot de passe : entrez un mot de passe pour le service (facultatif).
6. Certificat : dans la liste, cliquez sur un certificat d'identité (facultatif) à utiliser pour authentifier l'utilisateur auprès du

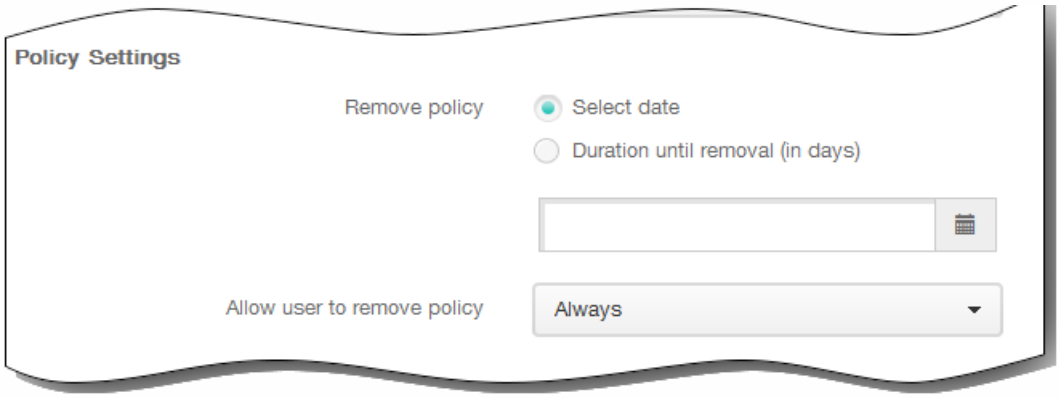
service. La valeur par défaut est Aucun.

7. Filtrer le trafic WebKit : sélectionnez cette option si vous voulez filtrer le trafic WebKit.
8. Filtrer le trafic de socket : sélectionnez cette option si vous voulez filtrer le trafic de socket.
9. Données personnalisées : cliquez sur Ajouter et procédez comme suit pour ajouter des données personnalisées au filtre de contenu Web :
   1. Clé : entrez la clé personnalisée.
   2. Valeur : entrez une valeur pour la clé personnalisée.
   3. Cliquez sur Enregistrer pour enregistrer la clé personnalisée ou cliquez sur Annuler pour ne pas l'enregistrer.
   4. Répétez les étapes i à iii pour chaque clé personnalisée que vous souhaitez ajouter.

   Remarque : pour supprimer une clé existante, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille sur le côté droit. Une boîte de dialogue de confirmation s'affiche. Cliquez sur Supprimer pour supprimer la liste ou sur Annuler pour conserver la liste.

   Pour modifier une clé, placez le curseur sur la ligne contenant la liste et cliquez sur l'icône de corbeille 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.

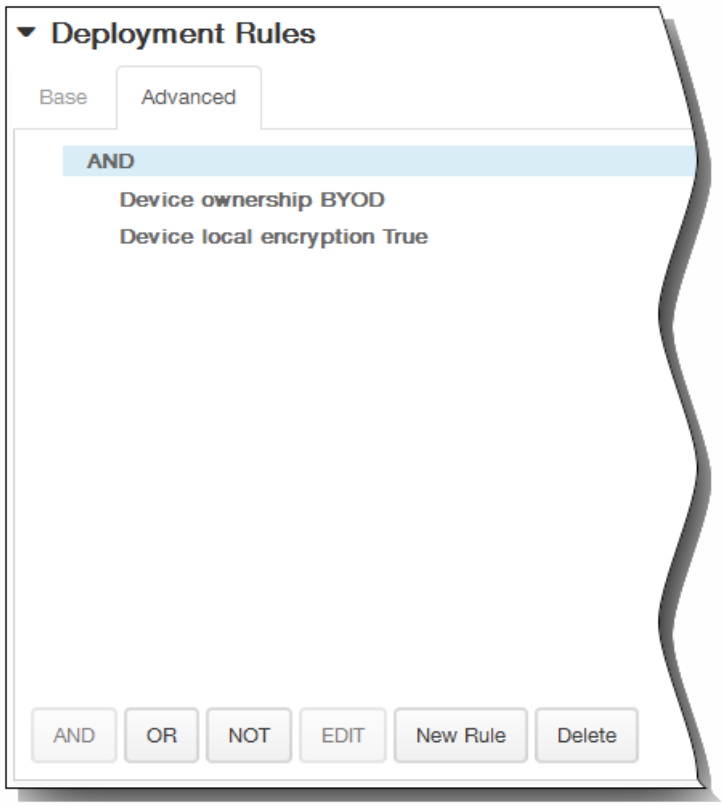


11. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.

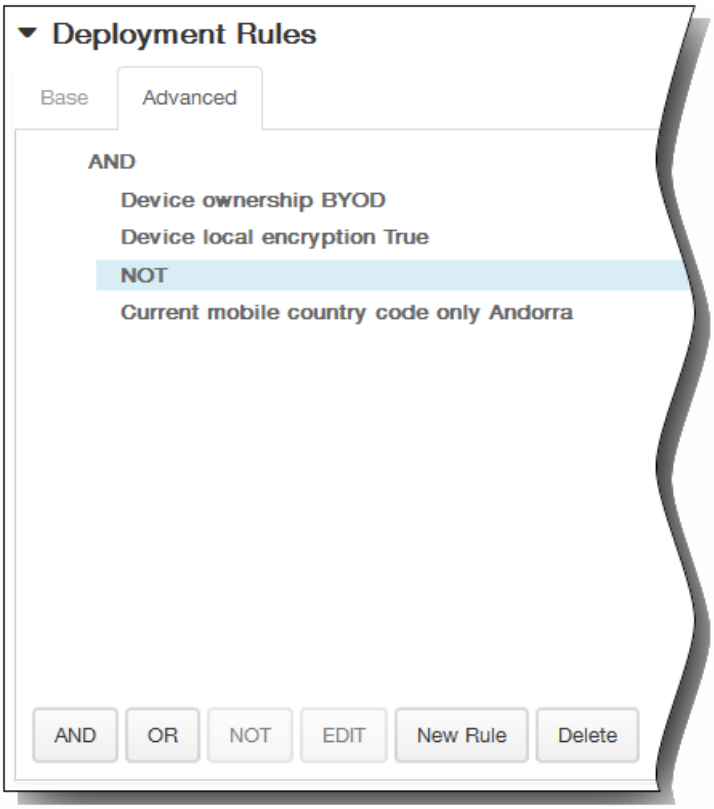
1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
2. Cliquez sur Nouvelle règle pour définir les conditions.
3. Dans la liste, cliquez sur les conditions, telles que Propriétaire et BYOD, comme 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.

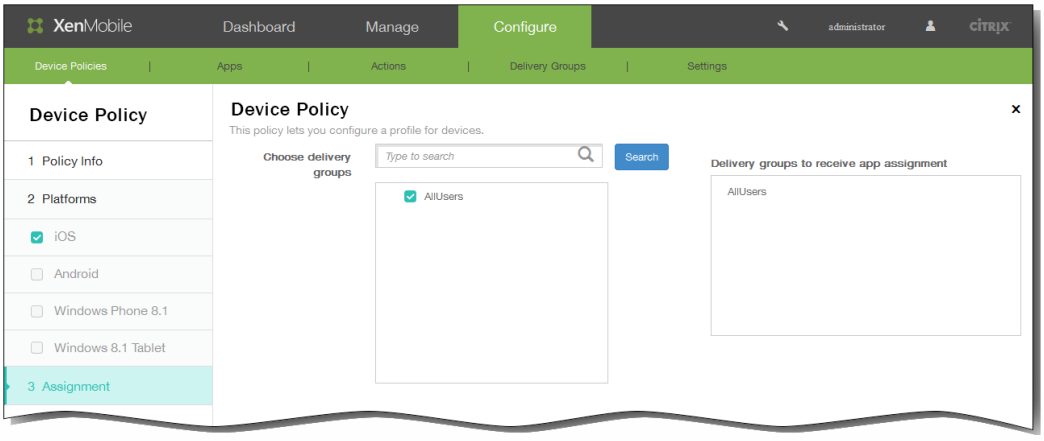


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



12. Cliquez sur Suivant. La page d'attribution de la Stratégie de filtre de contenu Web 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.

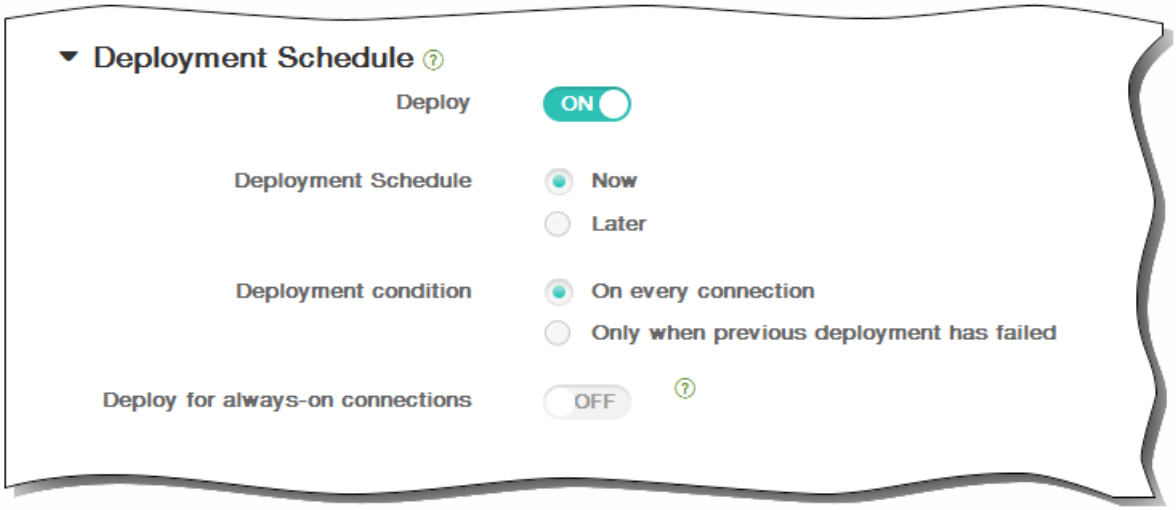


14. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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

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.



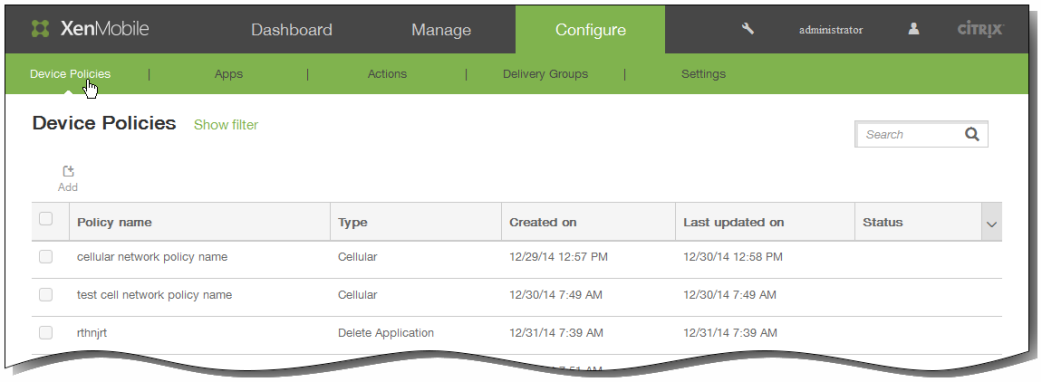
15. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies de navigateur Samsung

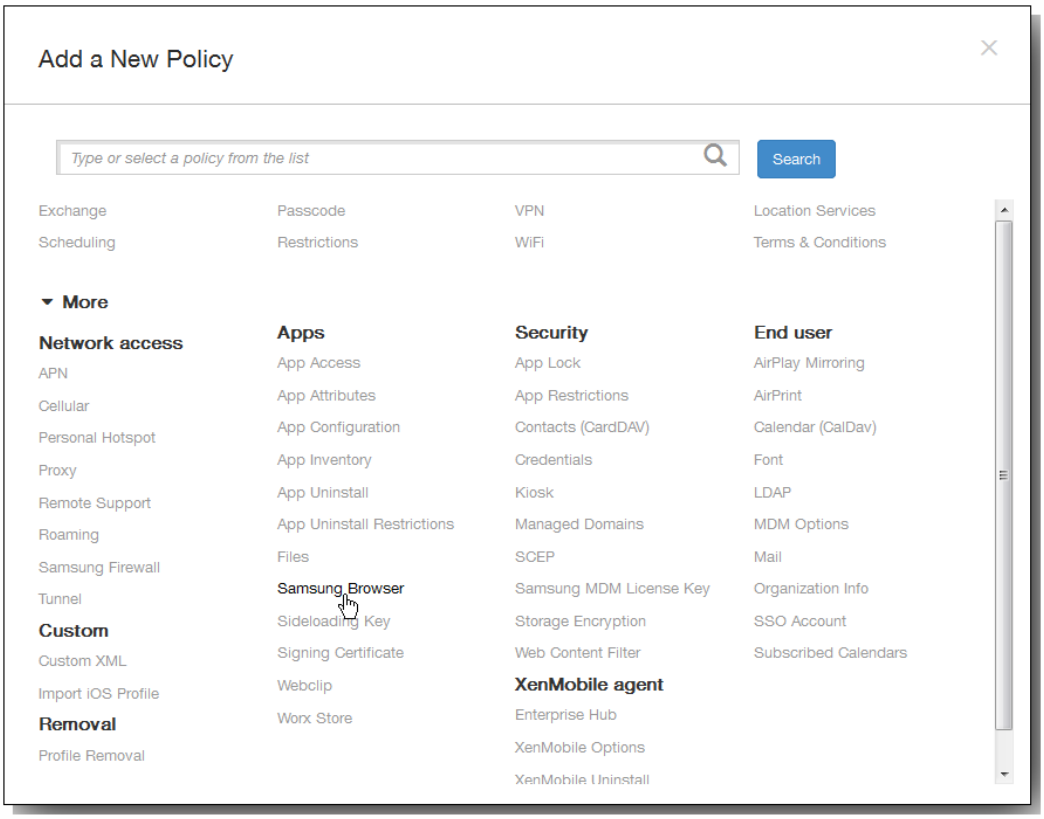
May 06, 2016

Vous pouvez créer des stratégies de navigateur Samsung pour Samsung SAFE et Samsung KNOX afin de définir si les appareils peuvent utiliser le navigateur ou pour limiter les fonctions du navigateur auxquelles les appareils ont accès. Vous pouvez désactiver complètement le navigateur, ou vous pouvez activer ou désactiver les fenêtres publicitaires intempestives Javascript, les cookies, le remplissage automatique, et l'affichage d'avertissements en cas de visite d'un site frauduleux.

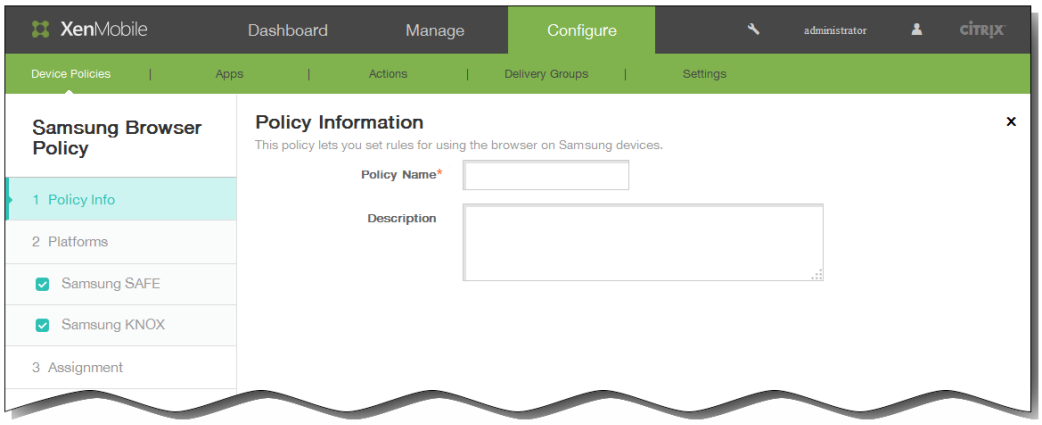
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



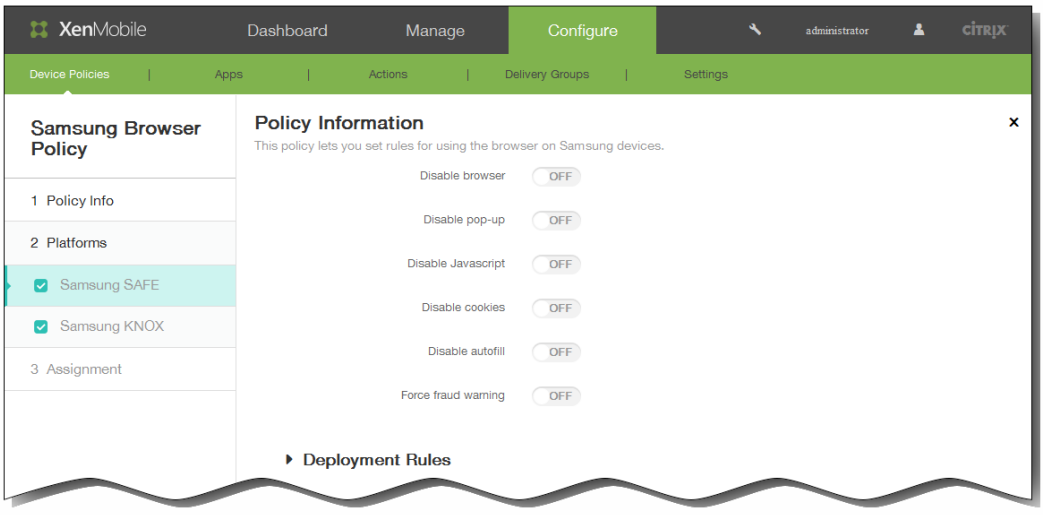
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus puis, sous Applications, cliquez sur Navigateur Samsung. La page d'informations sur la Stratégie de navigateur Samsungs'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 Samsung SAFE s'affiche.



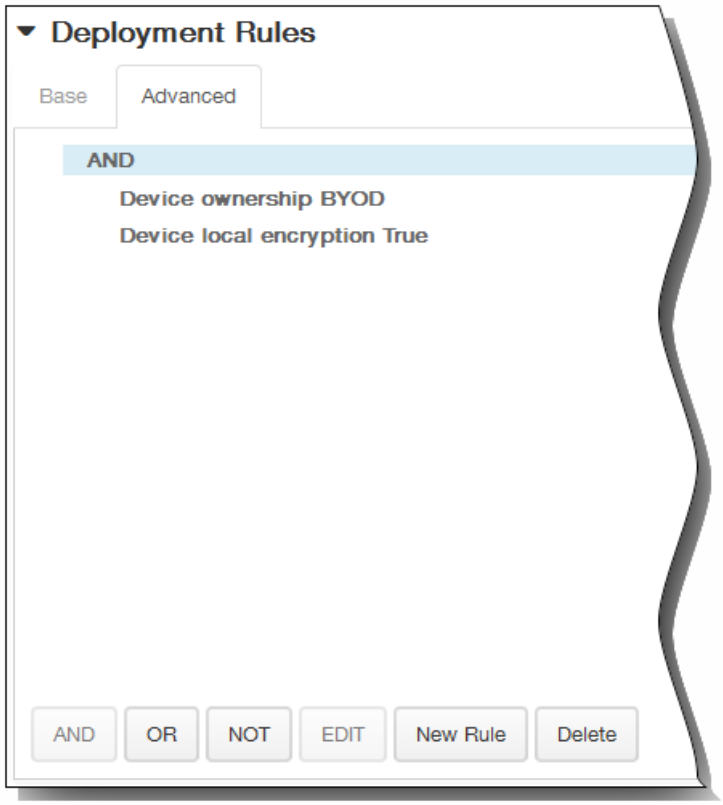
6.
7. Sous Plates-formes, sélectionnez les plates-formes Samsung que vous souhaitez ajouter. Si vous ne configurez qu'une plate-forme, désactivez l'autre, puis configurez les paramètres suivants :
   1. Désactiver le navigateur : sélectionnez cette option pour désactiver complètement le navigateur Samsung sur les appareils des utilisateurs. La valeur par défaut est OFF, ce qui permet aux utilisateurs d'utiliser le navigateur. Lorsque vous désactivez le navigateur, les options suivantes disparaissent.
   2. Désactiver les fenêtres pop-up : sélectionnez cette option pour autoriser les messages dans le navigateur.
   3. Désactiver le Javascript : sélectionnez cette option pour autoriser l'exécution de JavaScript sur le navigateur.
   4. Désactiver les cookies : sélectionnez cette option pour autoriser les cookies.
   5. Désactiver le remplissage automatique : sélectionnez cette option pour autoriser les utilisateurs à activer la fonction

de remplissage automatique du navigateur.

6. Forcer l'avertissement de fraude : sélectionnez cette option pour afficher un avertissement lorsqu'un utilisateur visite un site Web frauduleux.

8. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

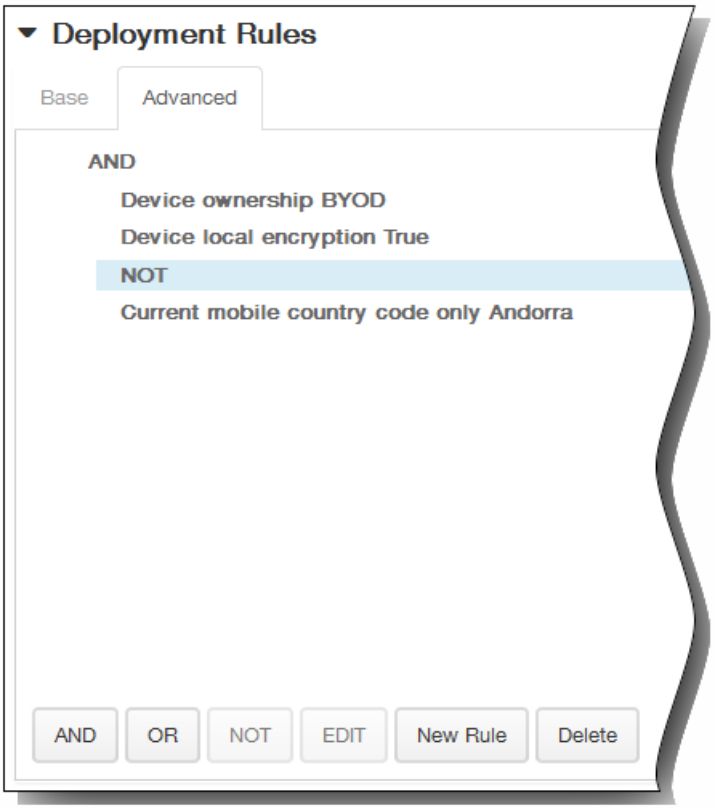
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
    1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



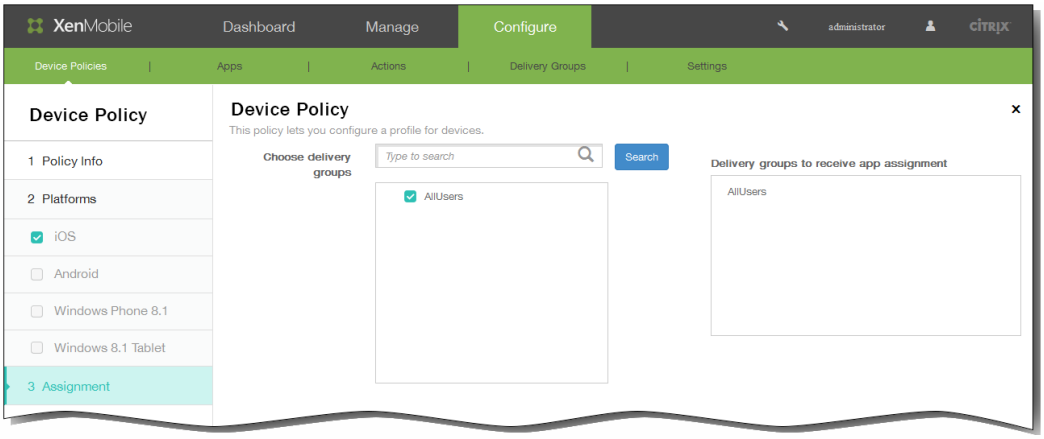
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.

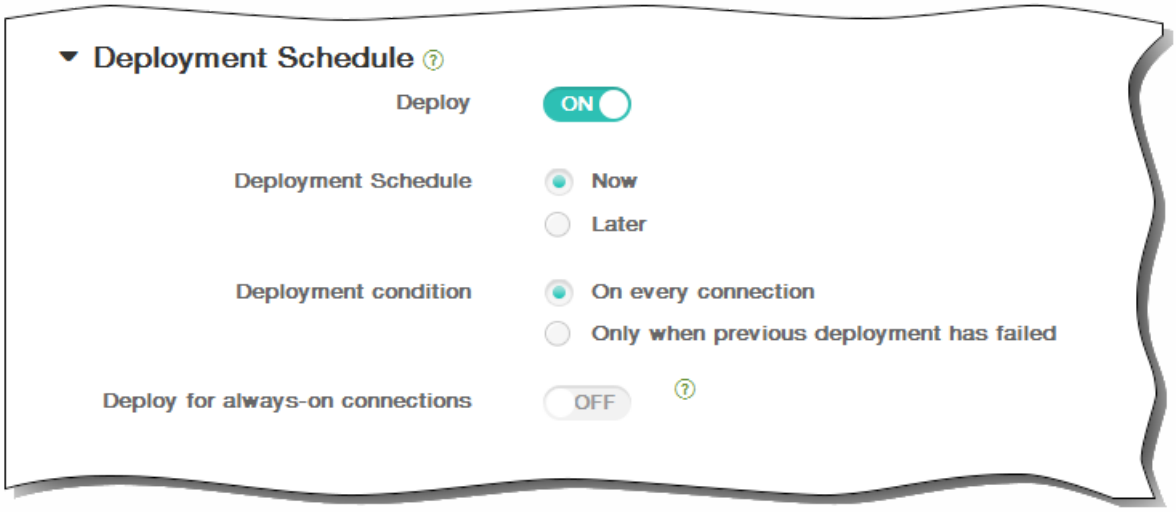


9. Cliquez sur Suivant. La page Stratégie de navigateur Samsung s'affiche.
10. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste 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.



12. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de clé de sideloading pour Windows 8.1 Tablet

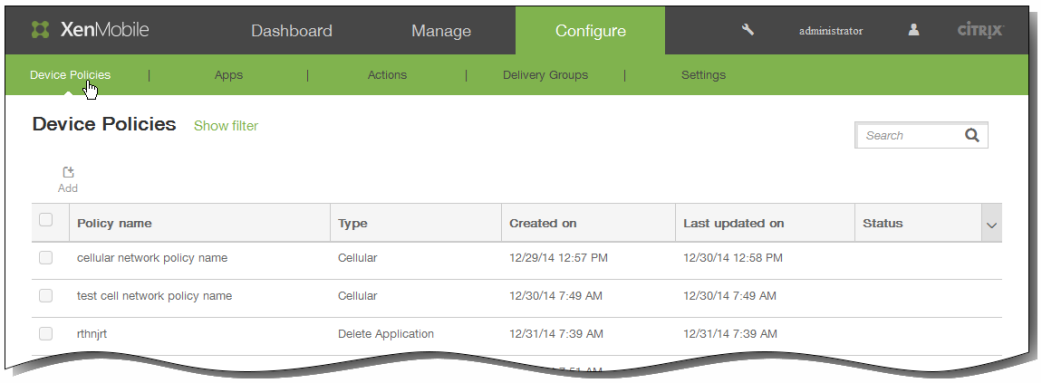
May 06, 2016

Le sideloading dans XenMobile vous permet de déployer des applications sur des appareils Windows 8.1 qui n'ont pas été achetées à partir du Windows Store. Dans la plupart des cas, vous sideloadez les applications que vous développez pour une utilisation en entreprise que vous ne souhaitez pas rendre publiques dans le Windows Store. Pour sideloader des applications, vous devez configurer la clé de sideloading et l'activation de clés et déployer les applications sur les appareils des utilisateurs.

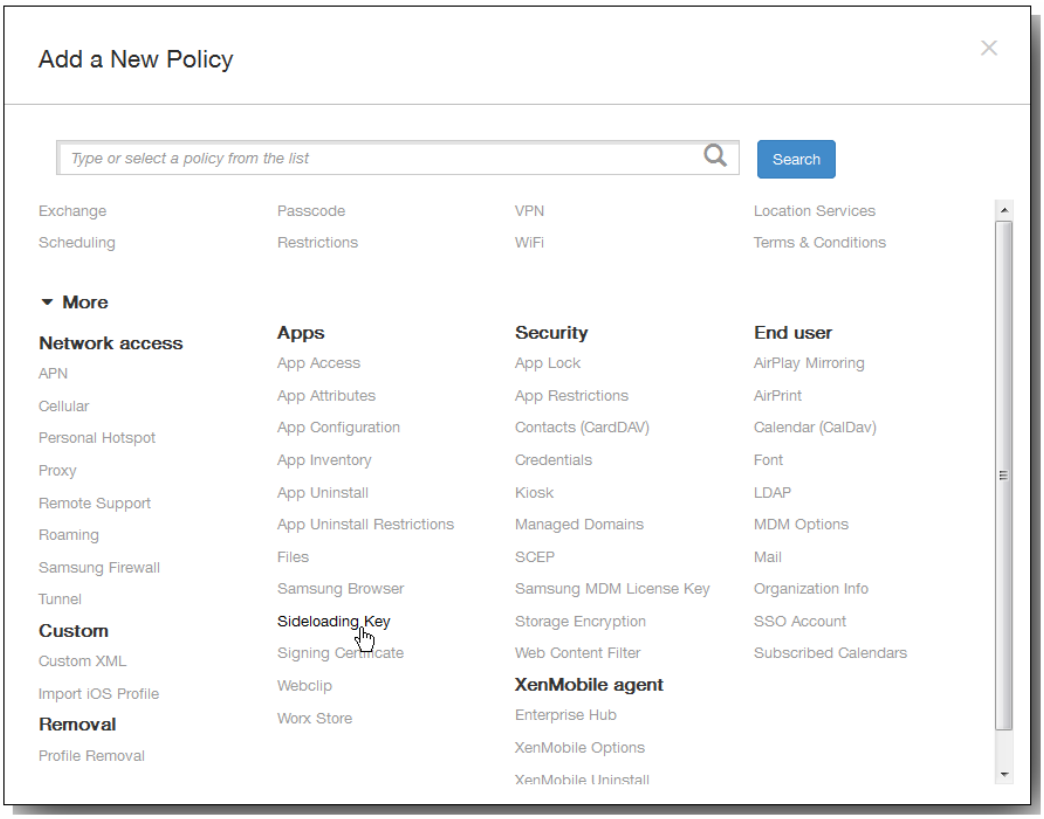
Vous devez disposer des informations suivantes avant de pouvoir créer cette stratégie :

- La clé de sideloading du produit, que vous pouvez obtenir en vous connectant au Centre de gestion des licences en volume Microsoft.
- L'activation de clé, que vous créez via la ligne de commande après avoir obtenu la clé de sideloading du produit.

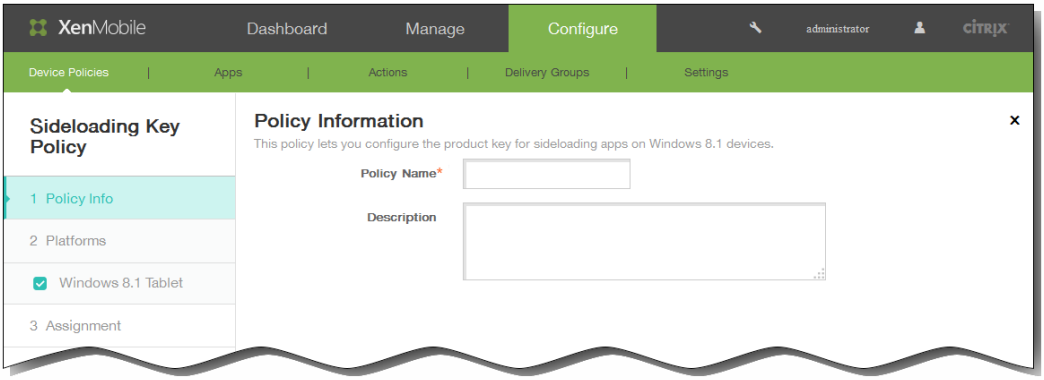
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



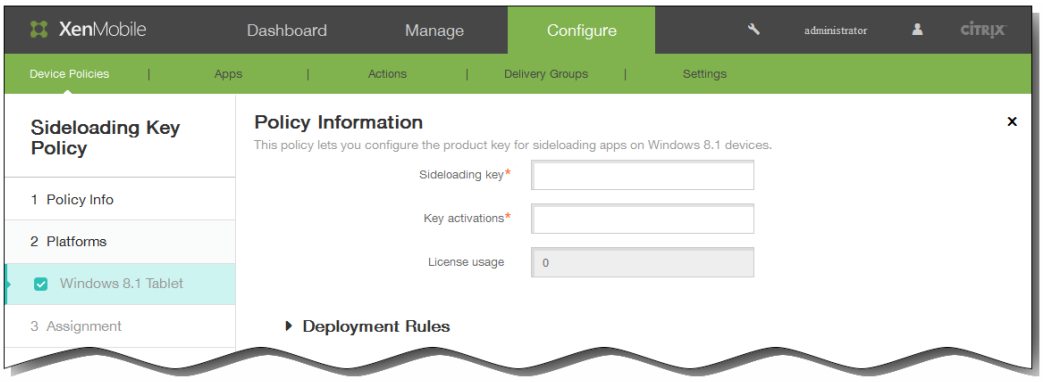
2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus puis, sous Applications, cliquez sur Clé de sideloading. La page Stratégie de clé de sideloading s'affiche.

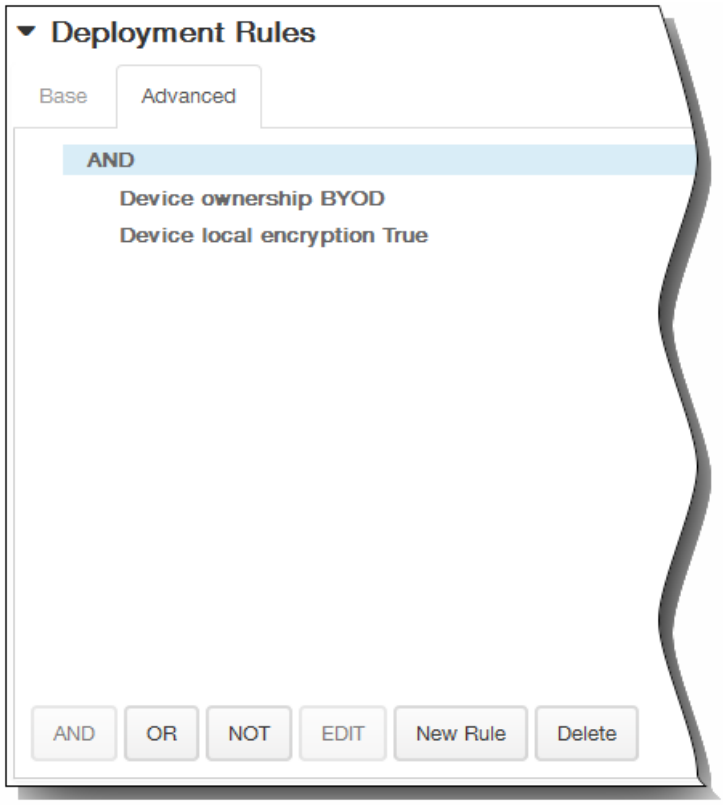


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant.
   La page d'informations Windows 8.1 Tablet s'affiche.



6. Configurez les paramètres suivants :
   1. Clé de sideloading : entrez la clé de sideloading que vous avez obtenue à partir du Centre de gestion des licences en volume Microsoft.
   2. Activation de clés : entrez l'activation de clé que vous avez créée pour la clé de sideloading.
   3. Utilisation des licences : XenMobile calcule cette valeur en fonction du nombre de tablettes inscrites. Vous ne pouvez pas modifier ce champ.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

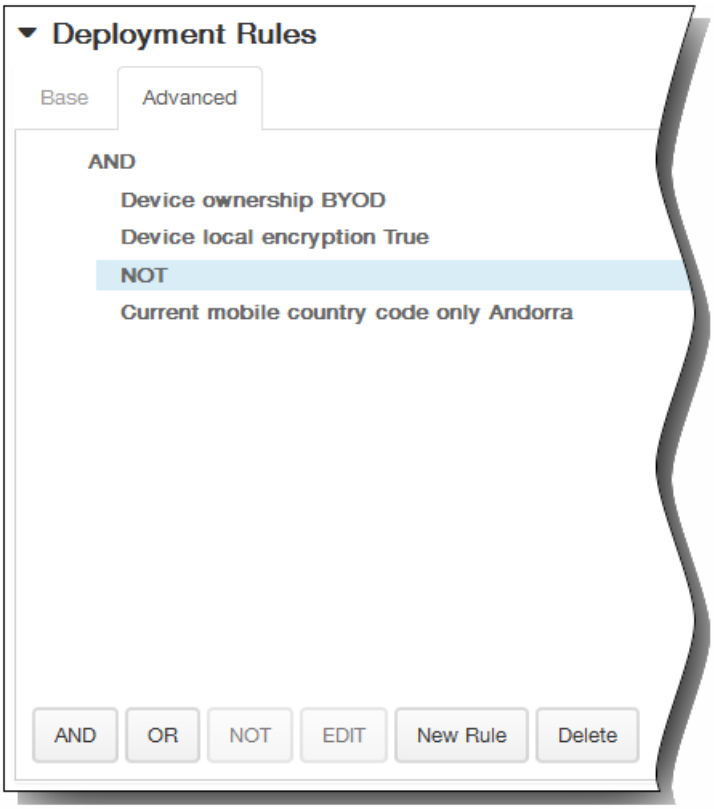
   1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
      1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
      2. Cliquez sur Nouvelle règle pour 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.



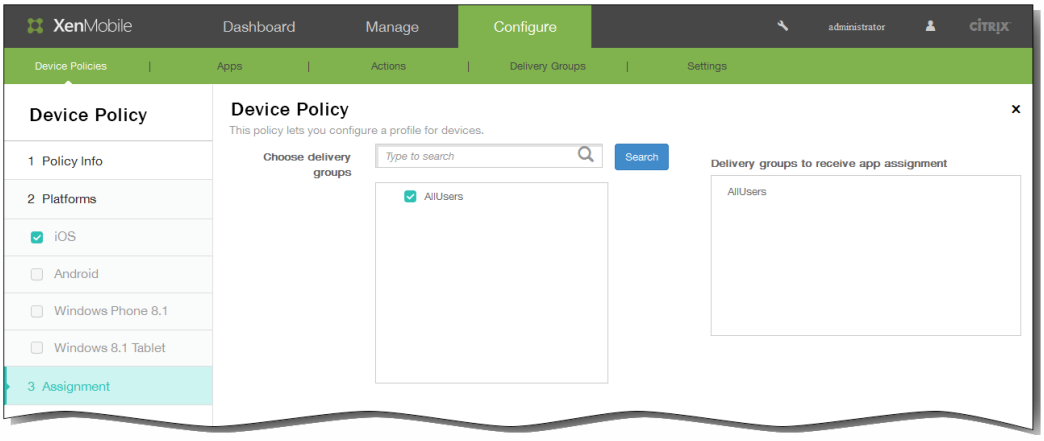
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
      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'assignation de la Stratégie de clé de sideloading 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.

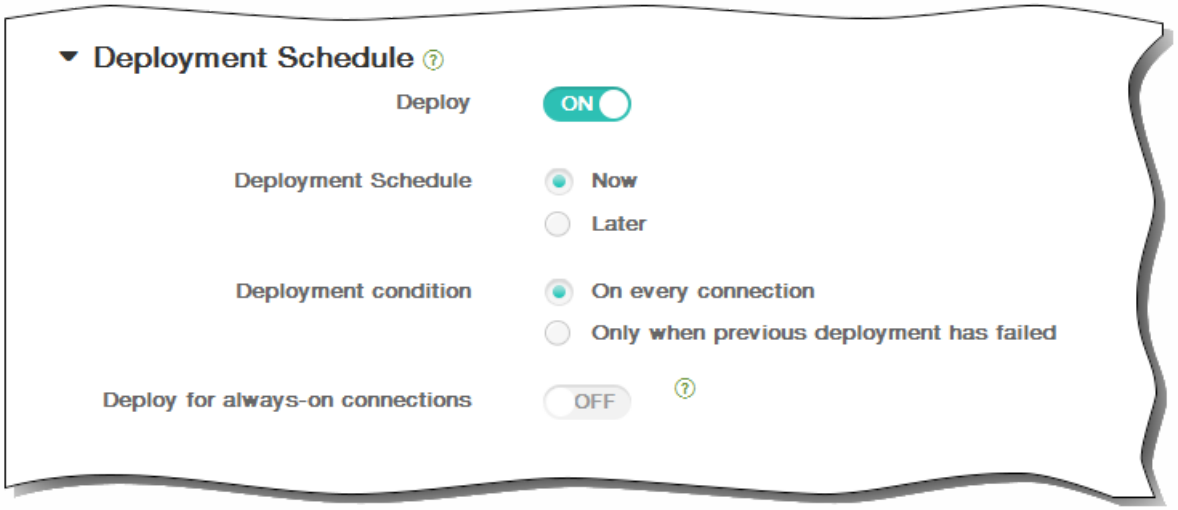


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.

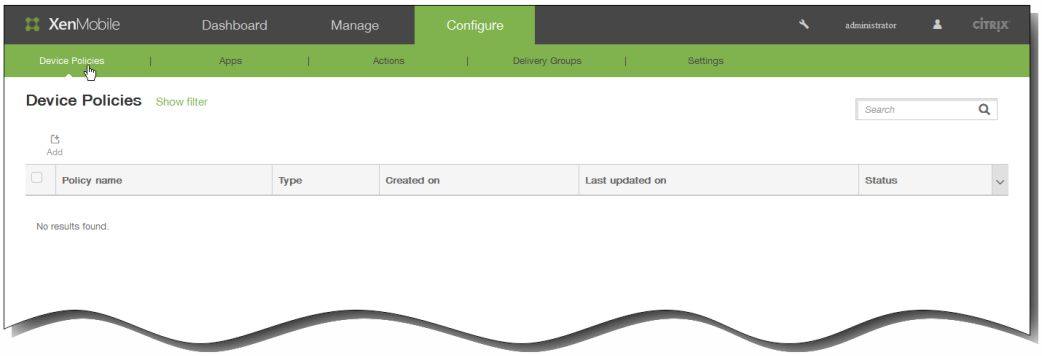


Pour ajouter une stratégie de certificat de signature pour Windows 8.1 Tablet

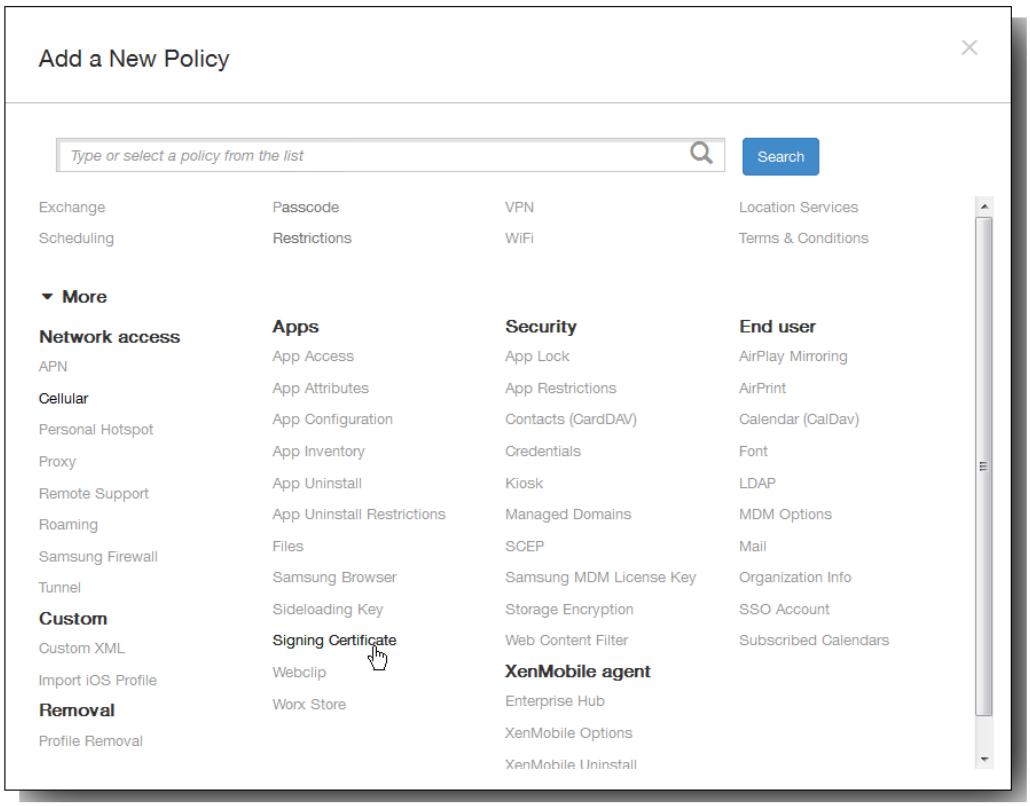
May 06, 2016

Vous pouvez ajouter une stratégie d'appareil dans XenMobile pour configurer les certificats de signature à utiliser pour signer les fichiers APPX. Vous avez besoin des certificats de signature si vous voulez distribuer des fichiers APPX aux utilisateurs pour les autoriser à installer des applications sur leurs tablettes Windows 8.1.

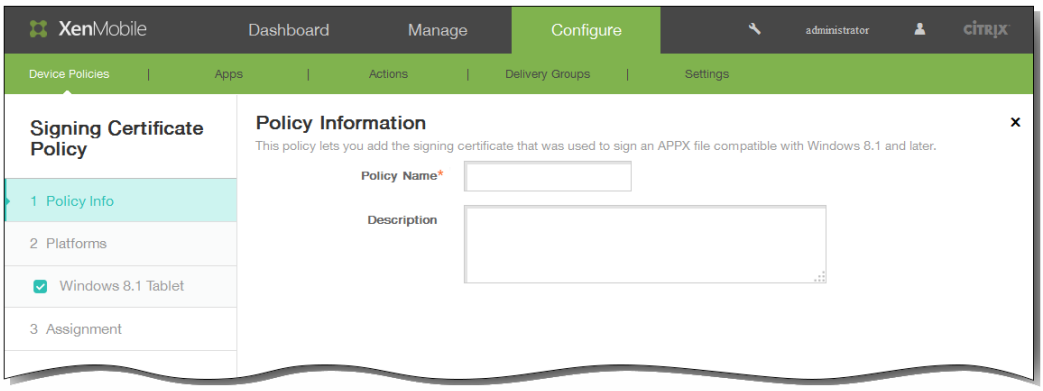
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



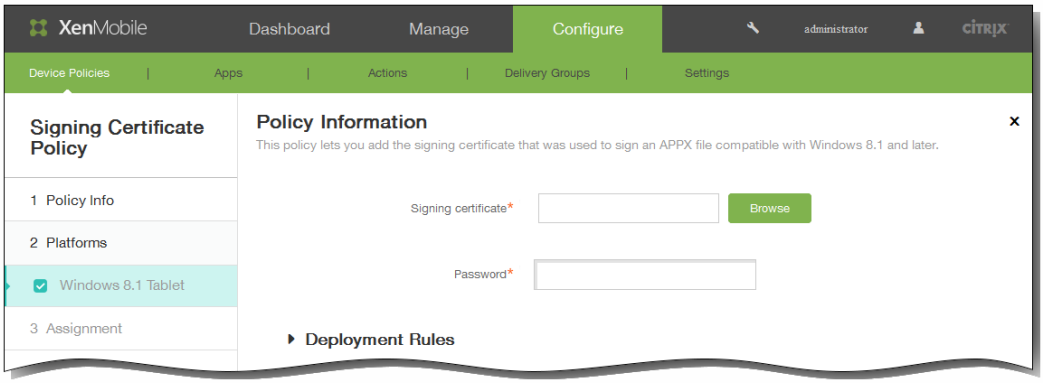
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. Lorsque vous cliquez sur Ajouter, la boîte de dialogue Ajouter une nouvelle stratégie s'affiche.



3. Cliquez sur Plus puis, sous Applications, cliquez sur Certificat de signature. La page Stratégie de certificat de signature s'affiche.

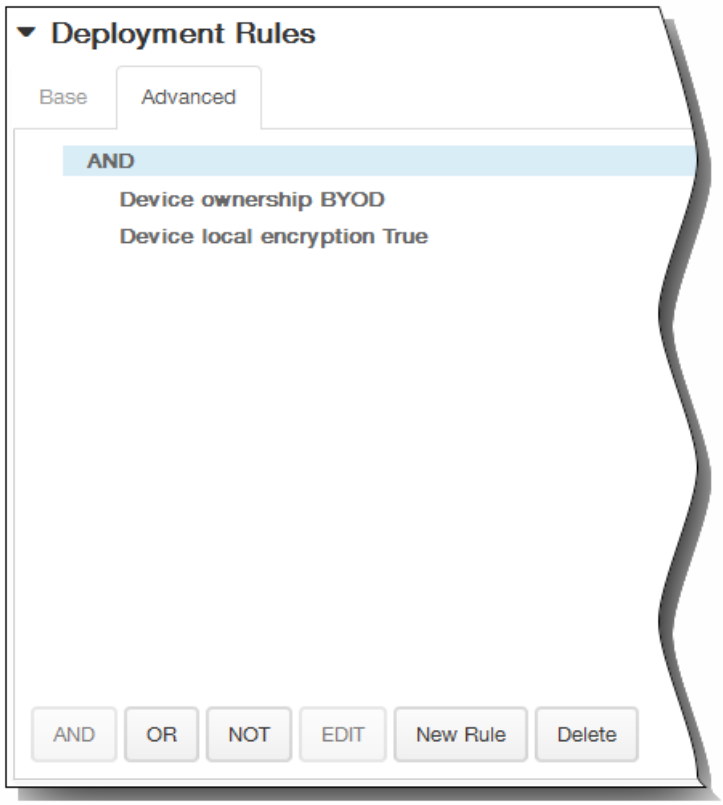


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page Informations sur la plate-forme s'affiche.



6. Configurez les paramètres suivants :
   1. Certificat de signature : naviguez jusqu'à l'emplacement du certificat utilisé pour signer le fichier APPX puis sélectionnez le certificat.
   2. Mot de passe : entrez le mot de passe requis pour accéder au certificat de signature.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

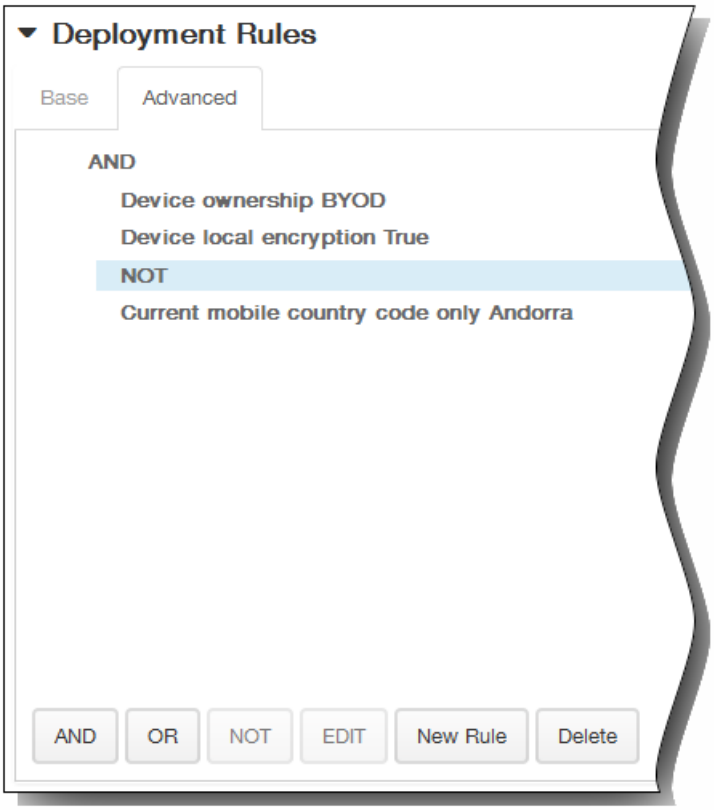
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



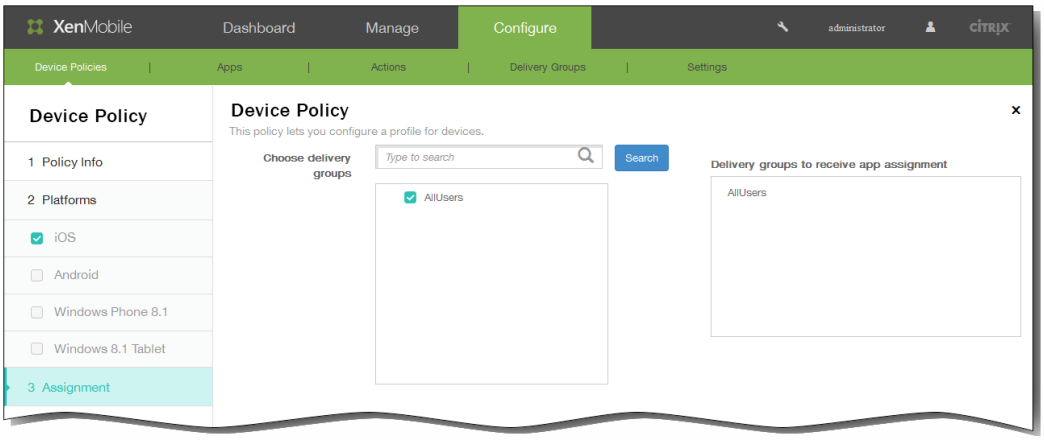
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      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.



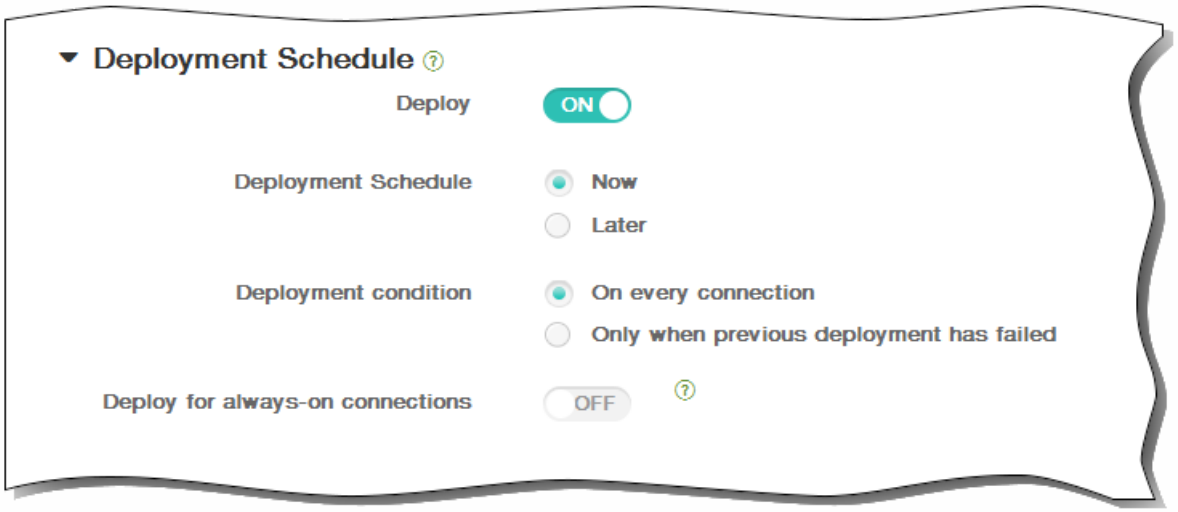
8. Cliquez sur Suivant. La page Attribution s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez 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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

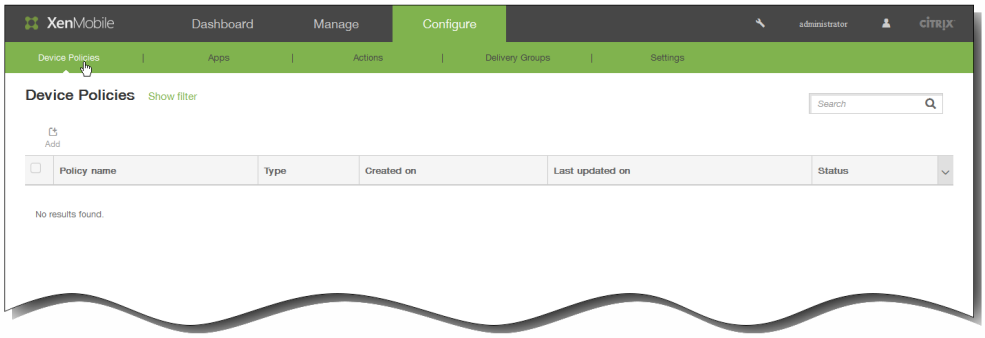
Stratégies VPN

May 06, 2016

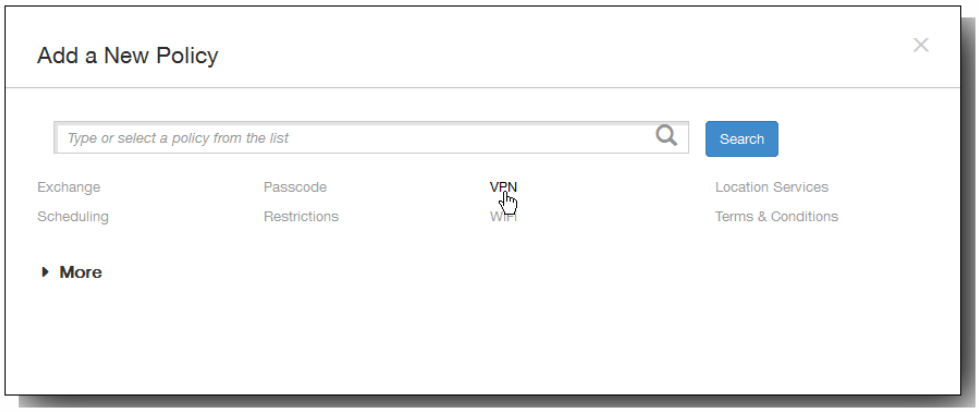
Vous pouvez ajouter une stratégie dans XenMobile pour configurer des paramètres de réseau privé virtuel (VPN) permettant aux appareils de se connecter de manière sécurisée aux ressources d'entreprise. Vous pouvez configurer la stratégie VPN pour les plates-formes suivantes : iOS, Android, Samsung SAFE, Samsung KNOX, Windows 8.1 Tablet et Amazon. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Pour ajouter une stratégie VPN

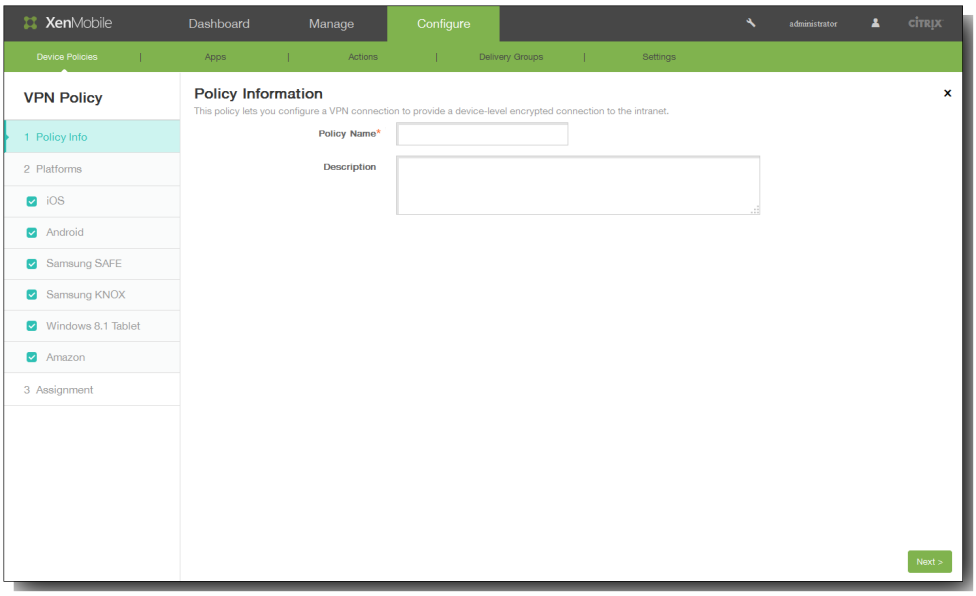
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



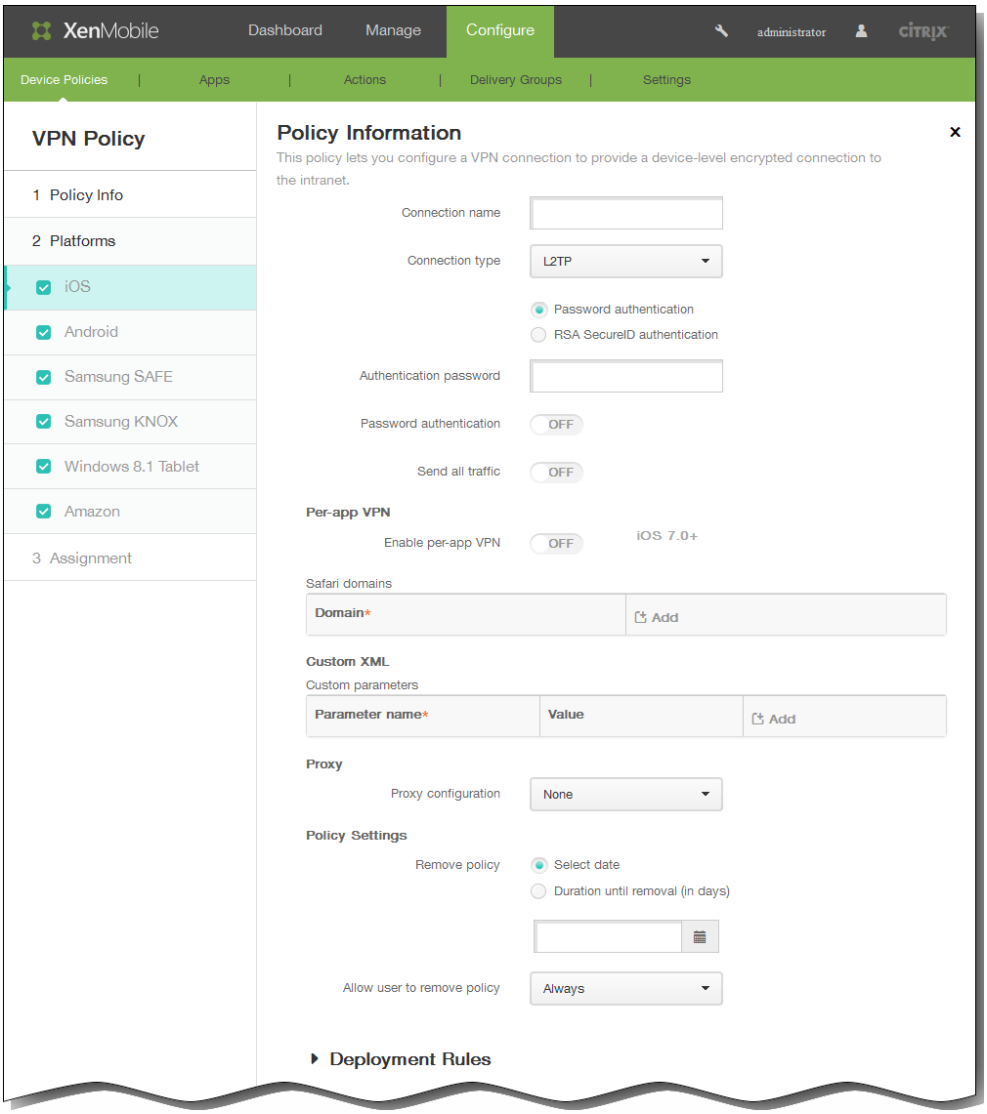
2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur VPN. La page Stratégie VPN 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).
   3. Cliquez sur Suivant.
5. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter.
   Si vous avez sélectionné iOS, configurez les paramètres suivants :



1. Nom de la connexion : entrez un nom pour la connexion.
2. Type de connexion : dans la liste, cliquez sur le protocole à utiliser pour cette connexion.
   - L2TP : Layer 2 Tunneling Protocol avec authentification par clé pré-partagée. C'est le réglage par défaut.
   - PPTP : protocole PPTP.
   - IPSec : votre connexion VPN d'entreprise.
   - Cisco AnyConnect : client Cisco AnyConnect VPN.
   - Juniper SSL : client Juniper Networks SSL VPN.
   - F5 SSL : client F5 Networks SSL VPN.
   - SonicWALL Mobile Connect : client VPN Dell unifié pour iOS.
   - Aruba VIA : client Aruba Networks Virtual Internet Access.
   - IKEv2 (iOS uniquement) : Internet Key Exchange version 2 pour iOS uniquement.
   - SSL personnalisé : Secure Sockets Layer personnalisé.

   Les sections suivantes répertorient les options de configuration pour chacun des types de connexion précédents.

Configurer les options suivantes pour le protocole L2TP

1. Sélectionnez Authentification par mot de passe ou Authentification RSA SecureID.
2. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
3. Authentification par mot de passe : sélectionnez cette option pour spécifier si l'authentification par mot de passe est

activée ou désactivée.

4. Envoyer tout le trafic : sélectionnez cette option pour envoyer tout le trafic via le VPN.

Configurer les options suivantes pour le protocole PPTP

1. Sélectionnez Authentification par mot de passe ou Authentification RSA SecureID.
2. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
3. Authentification par mot de passe : sélectionnez cette option pour spécifier si l'authentification par mot de passe est activée ou désactivée.
4. Niveau de chiffrement : sélectionnez le niveau de chiffrement souhaité.
5. Envoyer tout le trafic : sélectionnez cette option pour envoyer tout le trafic via le VPN.

Configurer les options suivantes pour le protocole IPSec

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	Certificat	Secret partagé
Nom de groupe	–	–	Facultatif
Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole Cisco AnyConnect

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Groupe : entrez un nom pour le groupe (facultatif).
3. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	Certificat	Secret partagé

Nom de groupe	Mot de passe	Certificat	Secret partagé
Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole SSL Juniper

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Domaine : entrez un nom de domaine (facultatif).
3. Rôle : entrez un nom de rôle (facultatif).
4. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	Certificat	Secret partagé
Nom de groupe	–	–	Facultatif
Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF

Demander le mot de passe	**Mot de passe**	**Certificat**	**Secret partagé**
	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole F5 SSL

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	**Certificat**	**Secret partagé**
Nom de groupe	–	–	Facultatif
Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole SonicWALL Mobile Connect

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Groupe ou domaine de connexion : entrez un groupe ou domaine de connexion (facultatif).
3. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	**Certificat**	**Secret partagé**
Nom de groupe	–	–	Facultatif

Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole Aruba VIA

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	Certificat	Secret partagé
Nom de groupe	–	–	Facultatif
Authentification par mot de passe	OFF	OFF	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	–

Configurer les options suivantes pour le protocole IKEv2 (iOS uniquement)

1. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
2. Authentification par mot de passe : sélectionnez cette option pour spécifier si l'authentification par mot de passe est activée ou désactivée.
3. VPN toujours connecté : sélectionnez cette option pour spécifier si la connexion VPN est toujours activée.
   Les options suivantes s'appliquent uniquement lorsque VPN toujours connecté = ON.

4. Nom du serveur ou adresse IP : entrez le nom ou l'adresse IP du serveur VPN.
5. Compte d'utilisateur : entrez un compte d'utilisateur (facultatif).
6. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Mot de passe	**Certificat**	**Secret partagé**
Nom de groupe	–	–	Facultatif
Secret partagé	–	–	Facultatif
Utiliser une authentification hybride	–	–	OFF
Demander le mot de passe	–	–	OFF
Autoriser l'utilisateur à désactiver la connexion automatique	OFF	OFF	OFF
Identifiant local	Requis	Requis	Requis
Identifiant distant	Requis	Requis	Requis
Authentification étendue activée	OFF	OFF	OFF
Intervalle DPD	Aucun(e)	Aucun(e)	Aucun(e)
Algorithme de chiffrement	2DES	2DES	2DES
Algorithme d'intégrité	SHA1-96	SHA1-96	SHA1-96
Groupe Diffie Hellman	2	2	2
Durée de vie en minutes	1440	1440	1440
Messagerie vocale	Autoriser le trafic via le	Autoriser le trafic via le	Autoriser le trafic via le

	Mot de passe	Certificat	Secret partagé
	tunnel	tunnel	tunnel
Autoriser le trafic en provenance de websheets captifs en dehors du tunnel VPN	OFF	OFF	OFF
Autoriser le trafic en provenance de toutes les applications de réseaux captifs en dehors du tunnel VPN	OFF	OFF	OFF
AirPrint	Autoriser le trafic via le tunnel	Autoriser le trafic via le tunnel	Autoriser le trafic via le tunnel
Bundle ID d'applications de réseaux captifs	Facultatif	Facultatif	Facultatif

Configurer les options suivantes pour le protocole SSL personnalisé

1. Identifiant SSL personnalisé (format DNS inverse) : entrez l'identifiant SSL au format DNS inverse.
2. Mot de passe d'authentification : entrez un mot de passe d'authentification (facultatif).
3. Authentification par mot de passe : sélectionnez cette option pour spécifier si l'authentification par mot de passe est activée ou désactivée.
4. Type d'authentification pour la connexion : sélectionnez le type d'authentification à utiliser pour cette connexion.

Le tableau suivant dresse la liste des options disponibles pour chaque type de connexion. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

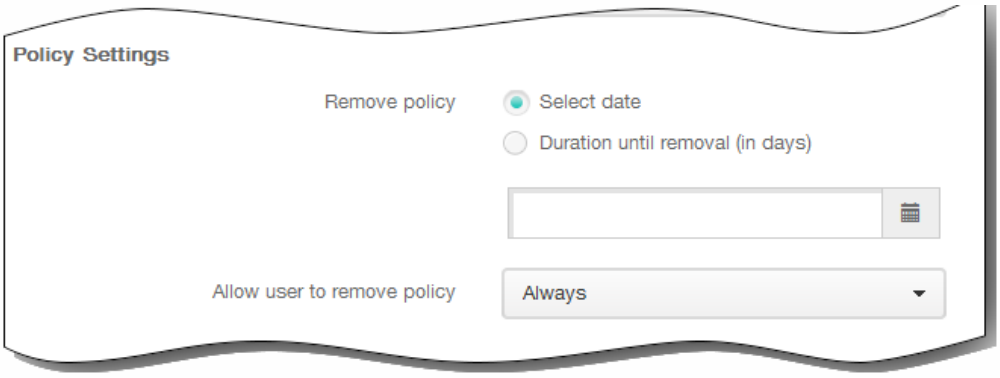
	Mot de passe	Certificat	Secret partagé
Nom de groupe	–	–	Facultatif
Demander le mot de passe	–	–	OFF
Mot de passe d'authentification	Facultatif	–	OFF
Certificats d'identité	–	Aucun(e)	–
Exiger PIN à la connexion	–	OFF	–
Activer VPN sur demande	–	OFF	–
Domaine sur demande	–	Requis si Activer VPN sur demande = ON	–
Utiliser une authentification hybride	–	–	OFF

3. Activer Per App VPN : activez ou désactivez le per-app VPN (disponible pour iOS 7 et versions ultérieures). Si cette option est activée, activez ou désactivez Correspondance d'application à la demande activée.
4. Domaines Safari : cliquez sur Ajouter pour ajouter un domaine Safari qui permet à l'application de créer une connexion sécurisée per-app VPN via Safari.

5. XML personnalisé : cliquez sur Ajouter pour entrer les paires Nom du paramètre et Valeur pour personnaliser la configuration.
6. Configuration du proxy : dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires.
   Le tableau suivant dresse la liste des options disponibles pour Manuel et Automatique ; la valeur Aucun ne nécessite aucune configuration supplémentaire. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

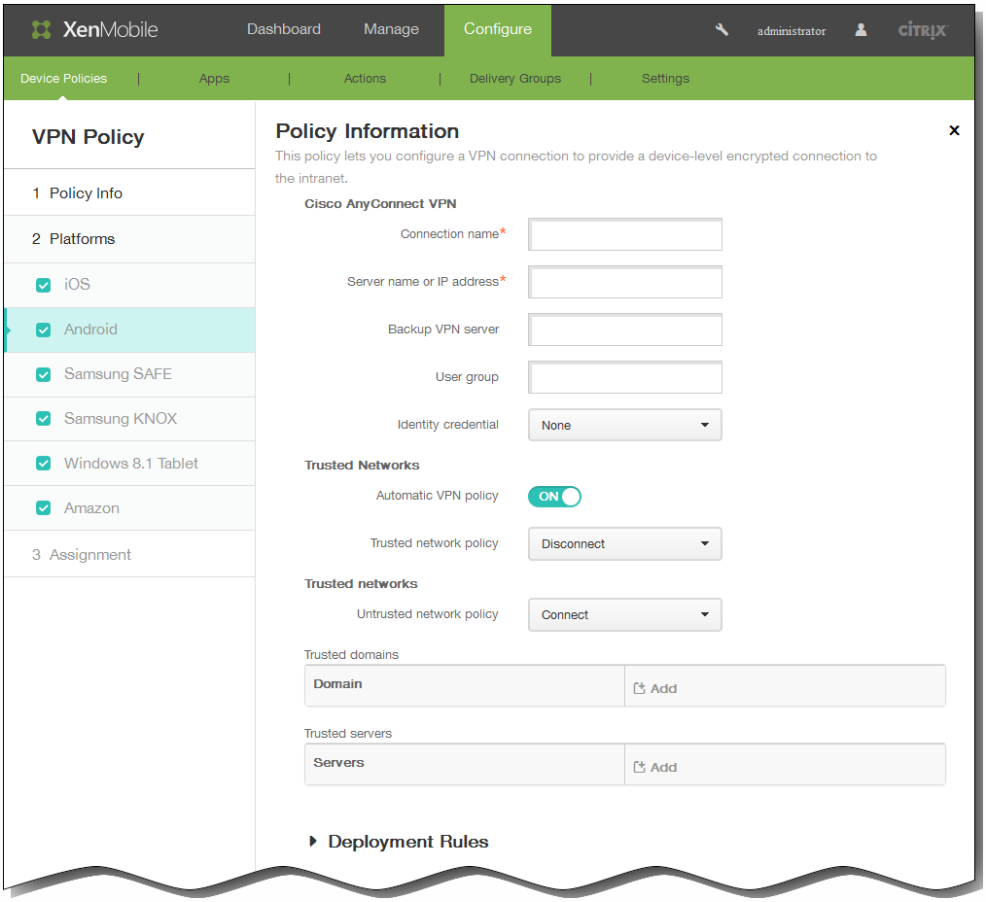
	Manuel	**Automatique**
Nom d'hôte/adresse IP du serveur proxy	Requis	–
Port du serveur proxy	Requis	–
Nom d'utilisateur	Facultatif	–
Mot de passe	Facultatif	–
URL du serveur proxy	–	Requis

Paramètres de stratégie



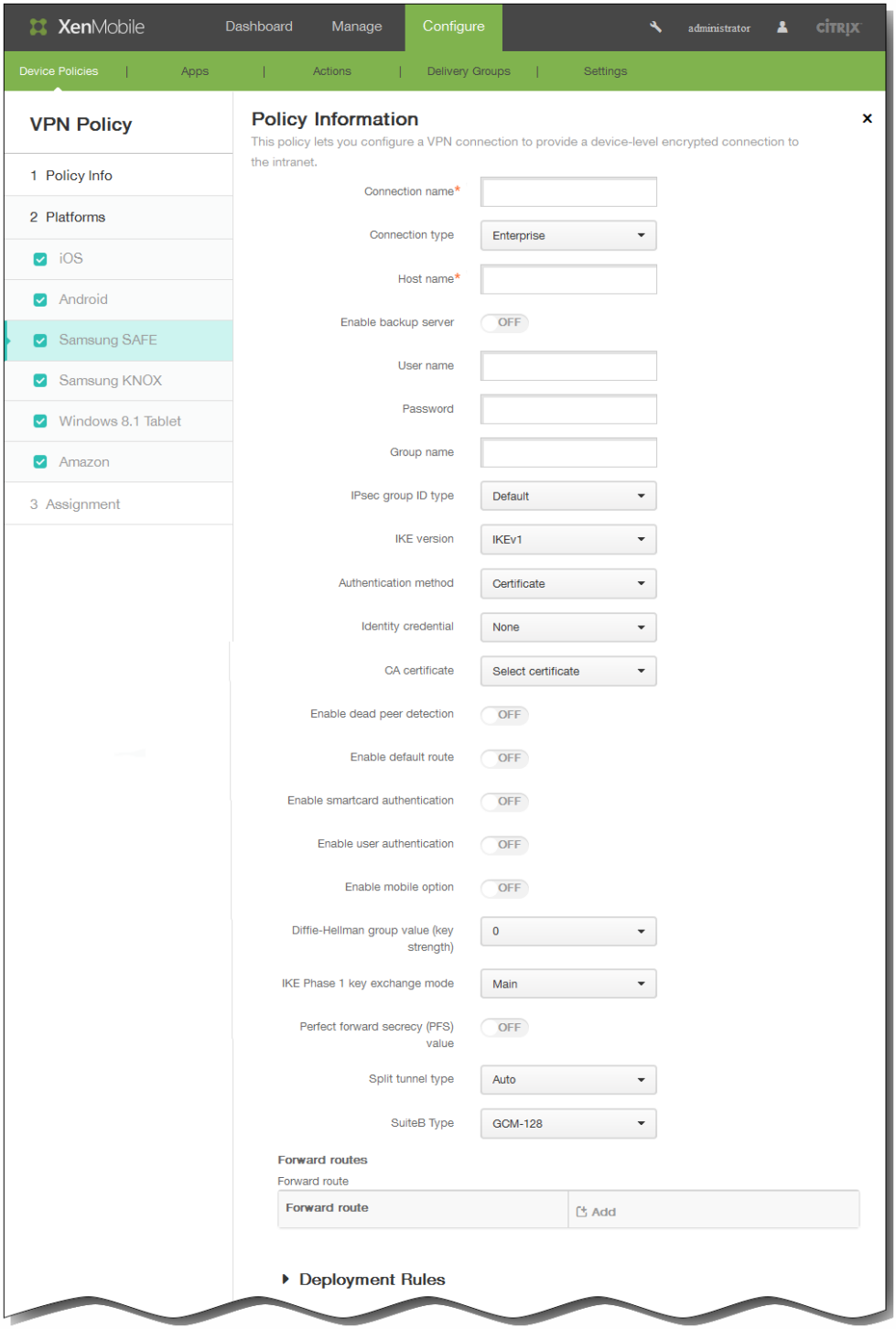
1. Sous Paramètres de stratégie, à côté de Supprimer la stratégie, cliquez sur Sélectionner une date ou Délai avant suppression (en jours).
2. Si vous cliquez sur Sélectionner une date, cliquez sur le calendrier pour sélectionner la date spécifique de la suppression.
3. Dans la liste Autoriser l'utilisateur 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 :



1. Nom de la connexion : entrez un nom pour la connexion au VPN Cisco AnyConnect.
2. Nom du serveur ou adresse IP : entrez le nom ou l'adresse IP du serveur VPN.
3. Serveur VPN de sauvegarde : entrez les informations du serveur VPN de sauvegarde.
4. Groupe d'utilisateurs : entrez les informations relatives au groupe d'utilisateurs.
5. Infos d'identification de l'identité : dans la liste, sélectionnez des Informations d'identification de l'identité.
6. Stratégie de VPN automatique : activez ou désactivez cette option pour définir la façon dont le VPN réagit aux réseaux approuvés et non approuvés. Si cette option est activée, entrez les informations suivantes :
   - Stratégie pour réseau fiable : dans la liste, cliquez sur la stratégie souhaitée.
   - Stratégie pour réseau non fiable : dans la liste, cliquez sur la stratégie souhaitée.

Si vous sélectionnez Samsung SAFE, configurez les paramètres suivants :



1. Nom de la connexion : entrez un nom pour la connexion.
2. Type de connexion : dans la liste, cliquez sur le protocole à utiliser pour cette connexion :
   - L2TP avec clé prépartagée : Layer 2 Tunneling Protocol (L2TP) avec authentification par clé pré-partagée. C'est le réglage par défaut.
   - L2TP avec certificat : Layer 2 Tunneling Protocol avec certificat.
   - PPTP : protocole PPTP.
   - Entreprise : votre connexion VPN d'entreprise.

   Le tableau suivant répertorie les options de configuration pour chacun des types de connexion précédents. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise,

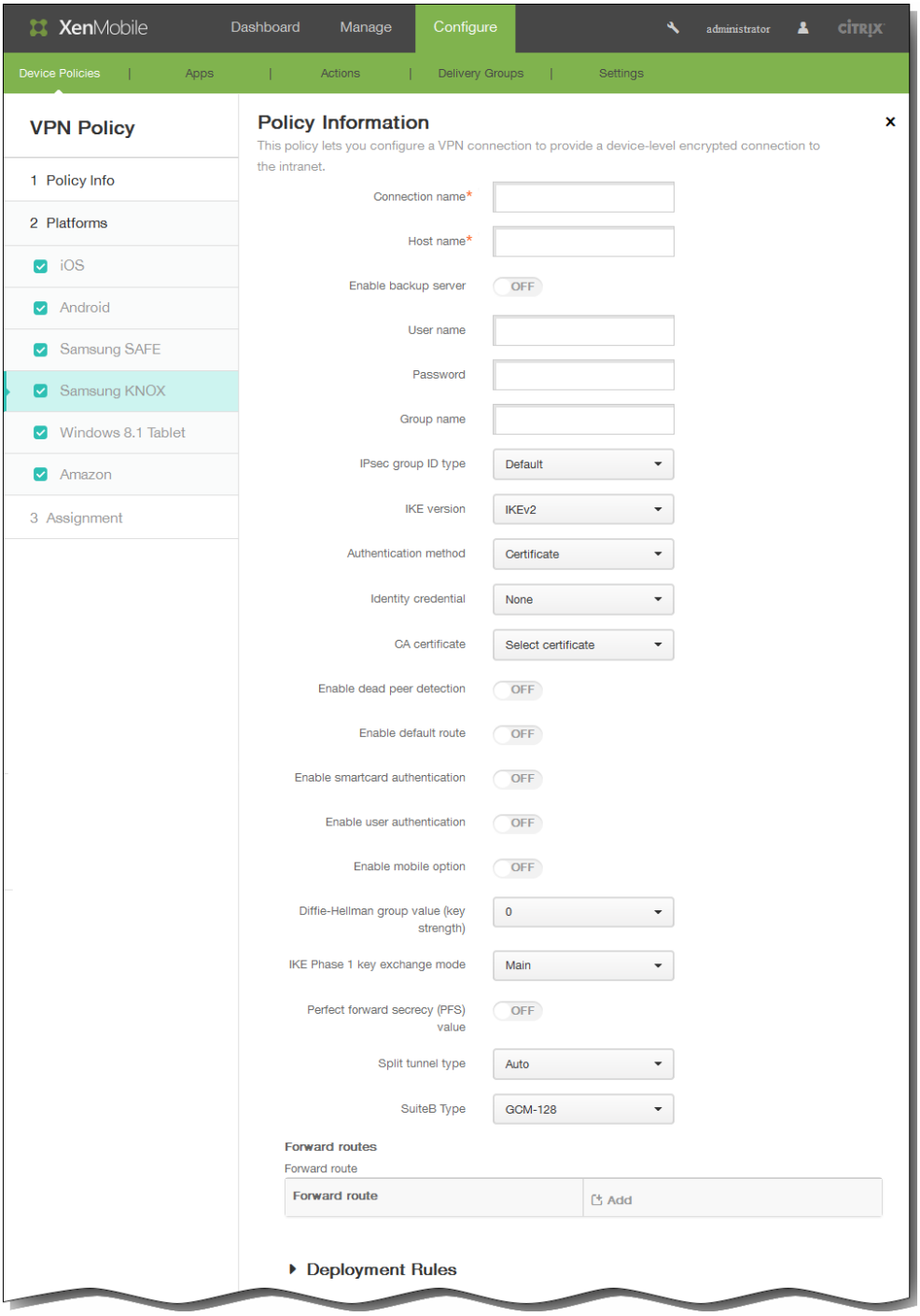
facultative ou si elle ne s'applique pas (-).

	L2TP avec clé prépartagée	**L2TP avec certificat**	**PPTP**	**Enterprise**				
Nom d'hôte	Requis	Requis	Requis	Requis				
Activer le serveur de sauvegarde	–	–	–	Off				
Serveur VPN de sauvegarde	–	–	–	Requis si Activer le serveur de sauvegarde = On				
Nom d'utilisateur	Facultatif	Facultatif	Facultatif	Facultatif				
Mot de passe	Facultatif	Facultatif	Facultatif	Facultatif				
Nom de groupe	–	–	–	Facultatif				
Type d'ID de groupe IPsec	–	–	–	Par défaut				
Version IKE	–	–	–	IKEv1				
Méthode d'authentification	–	–	–	Certificat (par défaut)	Clé prépartagée	RSA Hybride	EAP MD5	EAP MSCHAPv2
Certificats d'identité	–	Requis	–	Aucun(e)	Aucun(e)	–	–	–
Certificat CA	–	–	–	Sélectionner un certificat				
Activer la détection de perte des connexions	–	–	–	Off				
Activer l'itinéraire par défaut	–	–	–	Off				
Activer l'authentification par carte à puce	–	–		Off				
Activer l'authentification utilisateur	–	–	–	Off				

Activer l'option mobile	**L2TP avec clé prépartagée** –	**L2TP avec certificat** –	– **PPTP**	**Enterprise** Off				
Valeur du groupe Diffie-Hellman (puissance de clé)	–	–	–	0				
Mode d'échange de clés IKE Phase 1	–	–	–	Principal				
Perfect forward secrecy (PFS)	–	–	–	Off				
Type de tunnel de séparation	–			Auto				
Type SuiteB	–	–	–	GCM-128				
Clé prépartagée	Requis	–	–	–	Facultatif	–	–	–
Activer le cryptage	–	–	Off	–	–	–	–	–

3. Routes de transfert : ajoutez des routes de transfert supplémentaires si votre serveur VPN d'entreprise prend en charge plusieurs tables de routage.

Si vous sélectionnez Samsung KNOX, configurez les paramètres suivants :



1. Nom de la connexion : entrez un nom pour la connexion
2. Nom d'hôte : entrez le nom de l'ordinateur hôte.
3. Activer le serveur de sauvegarde : sélectionnez cette option pour activer un serveur VPN de sauvegarde. Un autre champ s'affiche lorsque vous sélectionnez cette option. Entrez les informations relatives au serveur de sauvegarde.
4. Nom d'utilisateur : entrez un nom d'utilisateur (facultatif).
5. Mot de passe : entrez un mot de passe (facultatif).
6. Nom du groupe : entrez un nom de groupe (facultatif).
7. Type d'ID de groupe IPsec : dans la liste, cliquez sur le type d'ID de groupe IPsec.
8. Version IKE : dans la liste, cliquez sur la version IKE.
9. Méthode d'authentification : dans la liste, cliquez sur la méthode d'authentification.

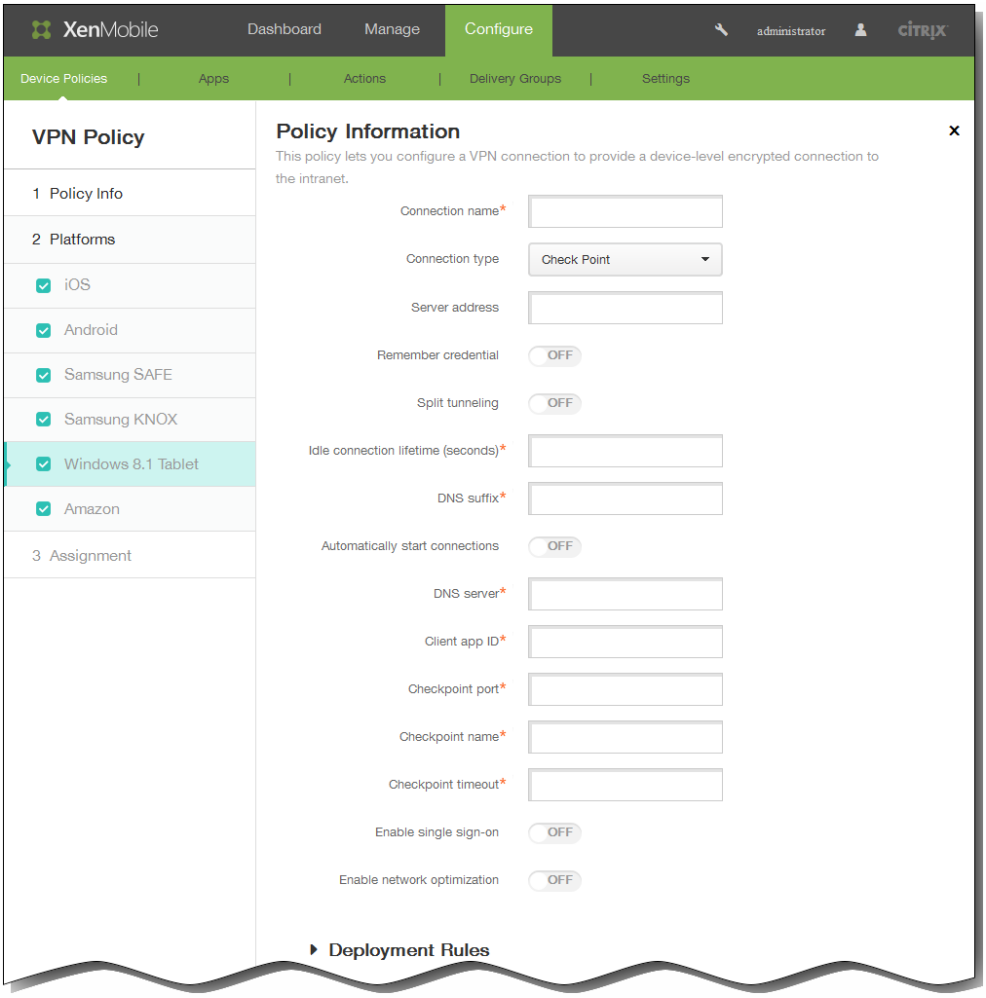
- Certificat : authentification basée sur le certificat
- Clé pré-partagée : authentification utilisant une clé pré-partagée
- RSA Hybride : authentification hybride utilisant des certificats RSA
- EAP MD5 : protocole EAP utilisant la fonction de hachage MD5
- EAP MSCHAPv2 : protocole EAP avec protocole CHAP Microsoft version 2

Le tableau suivant répertorie les options de configuration pour chacun des types de connexion précédents. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Certificat	**Clé prépartagée**	**RSA Hybride**	**EAP MD5**	**EAP MSCHAPv2**
Clé prépartagée	–	Requis	–	–	–
Certificats d'identité	Aucun(e)	Aucun(e)	–	–	–
Certificat CA	Requis	Requis	Requis	Requis	Requis
Activer la détection de perte des connexions	OFF	OFF	OFF	OFF	OFF
Activer l'itinéraire par défaut	OFF	OFF	OFF	OFF	OFF
Activer l'authentification par carte à puce	OFF	OFF	OFF	OFF	OFF
Activer l'authentification utilisateur	OFF	OFF	OFF	OFF	OFF
Activer l'option mobile	OFF	OFF	OFF	OFF	OFF
Valeur du groupe DIfffie-Hellman (puissance de clé)	0	0	0	0	0
Mode d'échange de clés IKE Phase 1	Principal	Principal	Principal	Principal	Principal
Perfect forward secrecy (PFS)	OFF	OFF	OFF	OFF	OFF
Type de tunnel de séparation	Auto	Auto	Auto	Auto	Auto
Type SuiteB	GCM-128	GCM-128	GCM-128	GCM-128	GCM-128

10. Routes de transfert : ajoutez des routes de transfert supplémentaires si votre serveur VPN d'entreprise prend en charge plusieurs tables de routage.

Si vous avez sélectionné Windows 8.1 tablet, configurez les paramètres suivants :



1. Nom de la connexion : entrez un nom pour la connexion
2. Type de connexion : dans la liste, cliquez sur le type de connexion
   - SonicWALL : client VPN Dell unifié pour Windows
   - Check Point : client Check Point Software Technologies SSL VPN
   - Juniper : client Juniper Networks SSL VPN
   - Microsoft : client Microsoft VPN
   - F5 : client F5 Networks SSL VPN

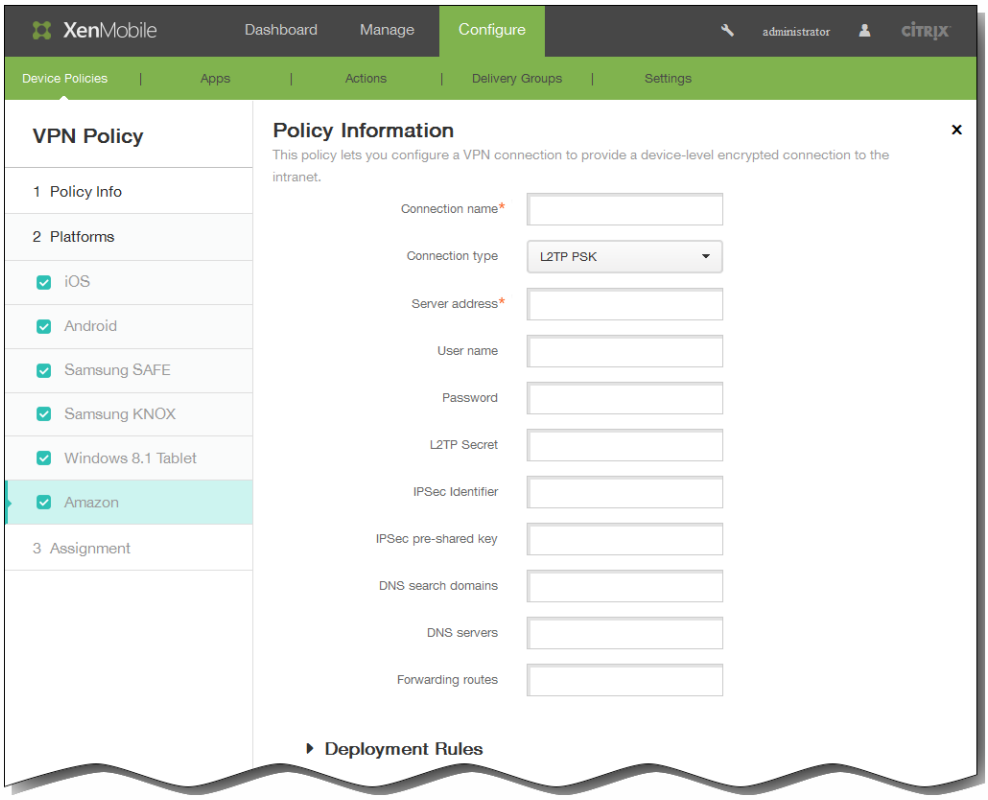
   Le tableau suivant répertorie les options de configuration pour chacun des types de connexion précédents. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	SonicWALL	Check Point	Juniper	Microsoft	F5
Adresse du serveur	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Mémoriser les informations d'identification	OFF	OFF	OFF	OFF	OFF
Split tunneling	OFF	OFF	OFF	OFF	OFF
Délai d'attente des connexions inactives (secondes)	Requis	Requis	Requis	Requis	Requis

Suffixe DNS	**SonicWALL** Requis	**Check Point** Requis	**Juniper** Requis	**Microsoft** Requis	**F5** Requis
Démarrer les connexions automatiquement	OFF	OFF	OFF	–	OFF
Serveur DNS	Requis	Requis	Requis	–	Requis
ID de l'application cliente	Requis	Requis	Requis	–	Requis
Port Check Point	–	Requis	–	–	–
Nom Check Point	–	Requis	–	–	–
Délai d'expiration Check Point	–	Requis	–	–	–
Activer le single sign-on	–	OFF	–	–	–
Activer l'optimisation du réseau	–	OFF	–	–	–
Activer la compression	OFF	–	–	–	–
Exiger un certificat de carte à puce	OFF	–	–	–	–
Sélectionner automatiquement le certificat client	OFF	–	–	–	–
Activer la journalisation des clients	OFF	–	–	–	–
Activer la capture de paquets	OFF	–	–	–	–
Utiliser les informations d'identification pour le single sign-on	–	–	OFF	–	–
Mettre les connexions à la disposition de tous les utilisateurs	–	–	–	OFF	–
Protocole de tunneling	–	–	–	Requis	–
Méthode d'authentification	–	–	–	Requis	–
Nom du serveur VPN	–	–	–	Requis	–
Nom VPN convivial	–	–	–	Requis	–

Détecter les paramètres automatiquement	SonicWALL –	Check Point –	Juniper –	Microsoft OFF	F5 –
Ne pas utiliser de serveur proxy pour les adresses locales	–	–	–	OFF	–
Utiliser automatiquement les informations d'identification Windows	–	–	–	OFF	–
Émetteur du certificat client	–	–	–	–	Requis

Si vous avez sélectionné Amazon, configurez les paramètres suivants :



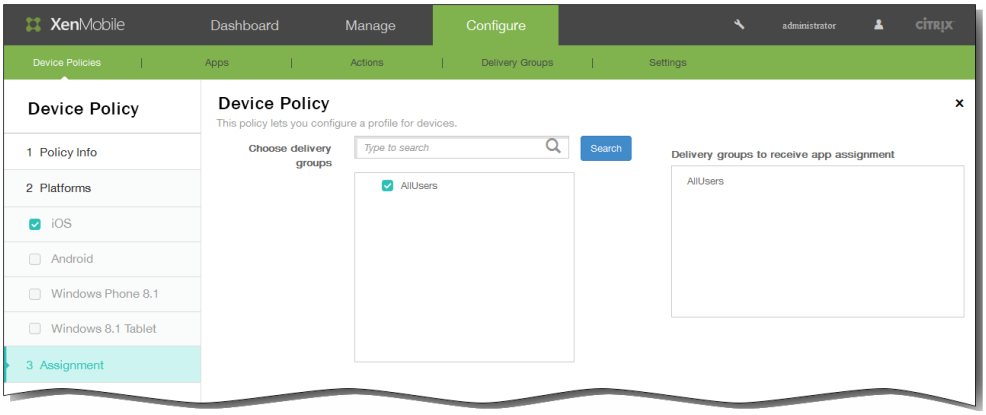
1. Nom de la connexion : entrez un nom pour la connexion
2. Type de connexion : cliquez sur le type de connexion.
   - L2TP PSK : Layer 2 Tunneling Protocol (L2TP) avec authentification par clé pré-partagée.
   - L2TP RSA : Layer 2 Tunneling Protocol avec authentification RSA.
   - IPSEC XAUTH PSK : Internet Protocol Security (IPSec) avec clé pré-partagée et authentification étendue
   - IPSEC XAUTH RSA : Internet Protocol Security (IPSec) avec RSA et authentification étendue
   - IPSEC HYBRID RSA : Internet Protocol Security (IPSec) avec authentification RSA hybride
   - PPTP : protocole PPTP

   Le tableau suivant répertorie les options de configuration pour chacun des types de connexion précédents. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	L2TP PSK	L2TP RSA	IPSEC XAUTH PSK	IPSEC XAUTH RSA	IPSEC HYBRID RSA	PPTP
Adresse du serveur	Requis	Requis	Requis	Requis	Requis	Requis
Nom d'utilisateur	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Mot de passe	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Secret L2TP	Facultatif	Facultatif	–	–	–	–
Identificateur IPSec	Facultatif	–	Facultatif	–	–	–
Clé pré-partagée IPSec	Facultatif	–	Facultatif	–	–	–
Domaines de recherche DNS	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Serveurs DNS	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Routes de transfert	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif	Facultatif
Certificat de serveur	–	Sélectionner	–	Sélectionner	Sélectionner	–
Certificat CA	–	Sélectionner	–	Sélectionner	Sélectionner	–
Certificats d'identité	–	Requis	–	Requis	–	–
Cryptage PPP (MMPE)	–	–	–	–	–	OFF

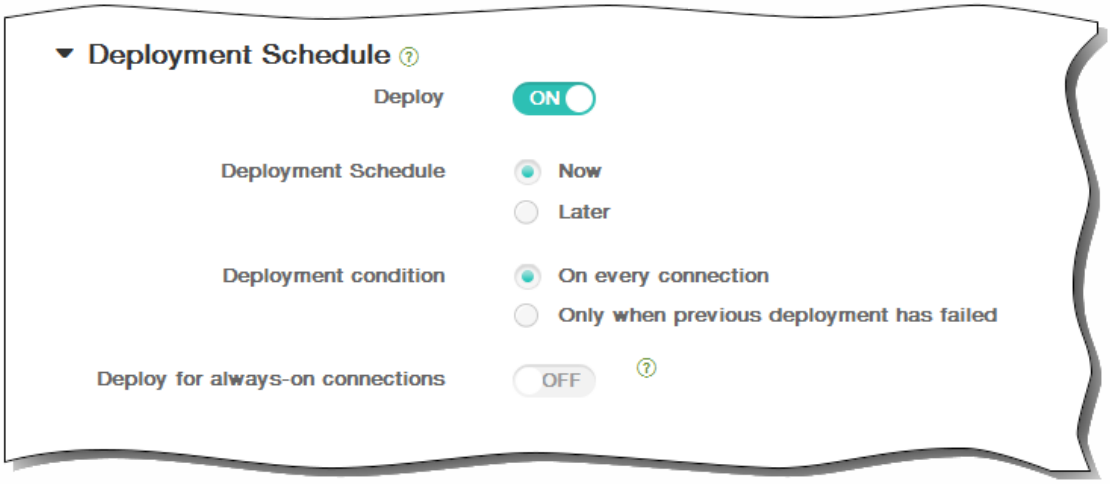
3. Routes de transfert : ajoutez des routes de transfert supplémentaires si votre serveur VPN d'entreprise prend en charge plusieurs tables de routage.

6. Une fois que vous avez terminé de configurer les paramètres pour une ou plusieurs plates-formes, cliquez sur Suivant et la page Stratégie VPN s'affiche.
7. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer 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.



8. 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.



9. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies WiFi

May 06, 2016

Vous pouvez créer ou modifier des stratégies Wi-Fi dans XenMobile sur la page Stratégies d'appareil de la console XenMobile. Les stratégies Wi-Fi vous permettent de gérer la manière dont les utilisateurs connectent leurs appareils à des réseaux sans fil en définissant ce qui suit : noms et types de réseau, stratégies d'authentification et de sécurité, serveurs proxy et d'autres détails liés à l'utilisation du Wi-Fi pour tous les utilisateurs sur les plates-formes que vous avez choisies.

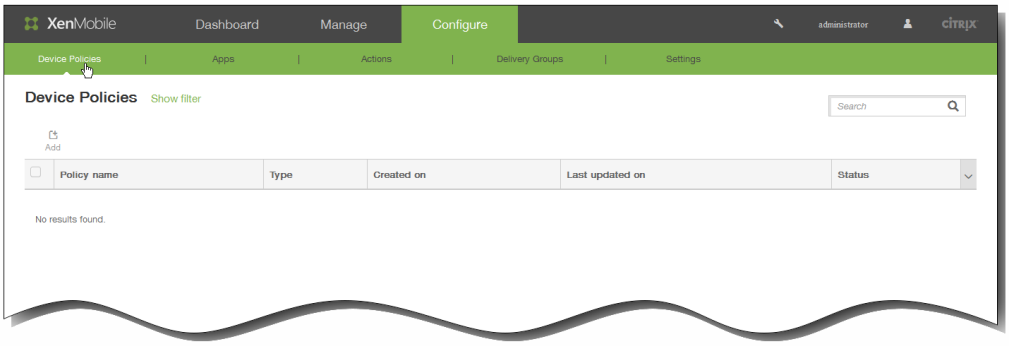
Vous pouvez configurer des paramètres Wi-Fi pour les utilisateurs pour les plates-formes suivantes : iOS, Android, Windows Phone 8.1 et Windows 8.1 Tablet. Chaque plate-forme requiert des valeurs différentes, qui sont décrites en détail dans cet article.

Important : avant de créer une nouvelle stratégie, vous devez effectuer les étapes suivantes :

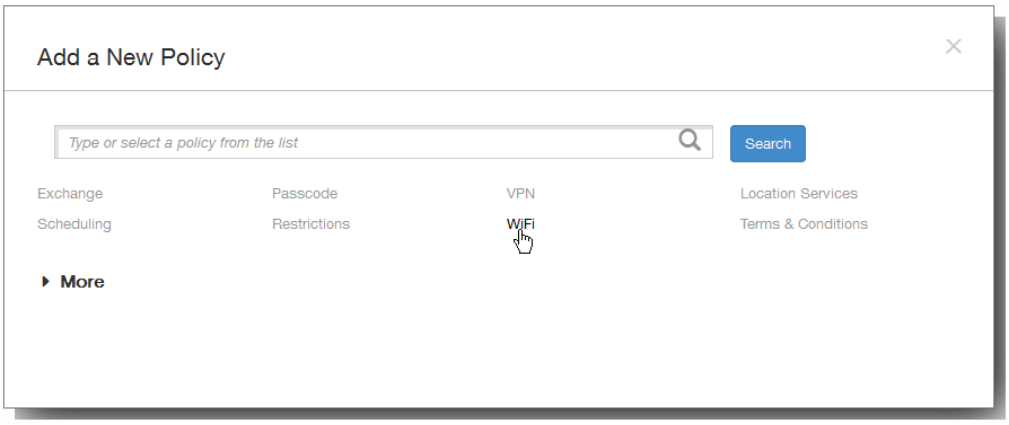
- Créez les groupes de déploiement que vous voulez utiliser.
- Notez le nom et type de réseau.
- Déterminez les types d'authentification ou de sécurité que vous voulez utiliser.
- Déterminez les informations de serveur proxy dont vous avez besoin.
- Installer les certificats d'autorité de certification nécessaires.
- Vérifiez que vous disposez des clés partagées nécessaires.

Pour créer une nouvelle stratégie Wi-Fi

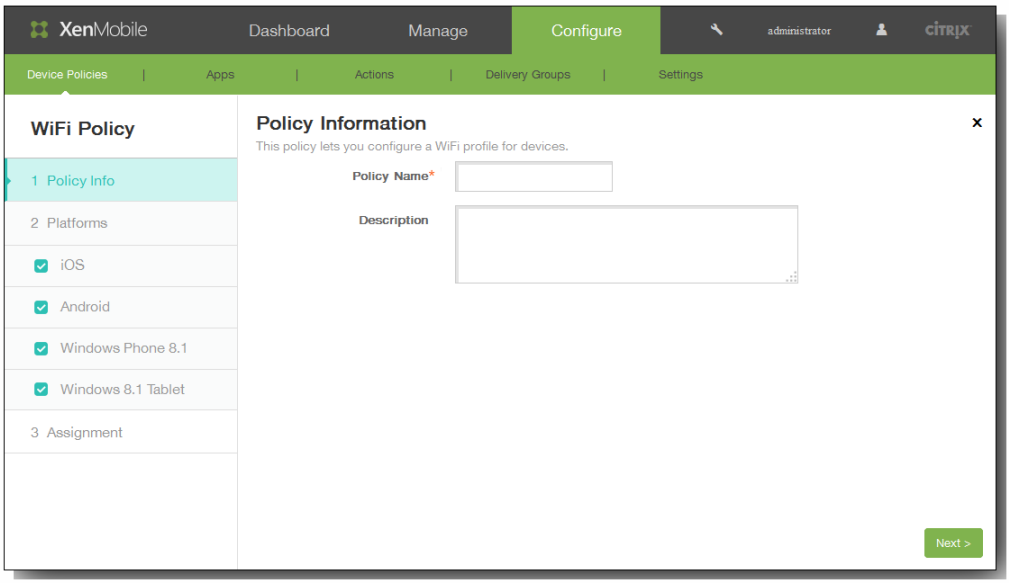
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



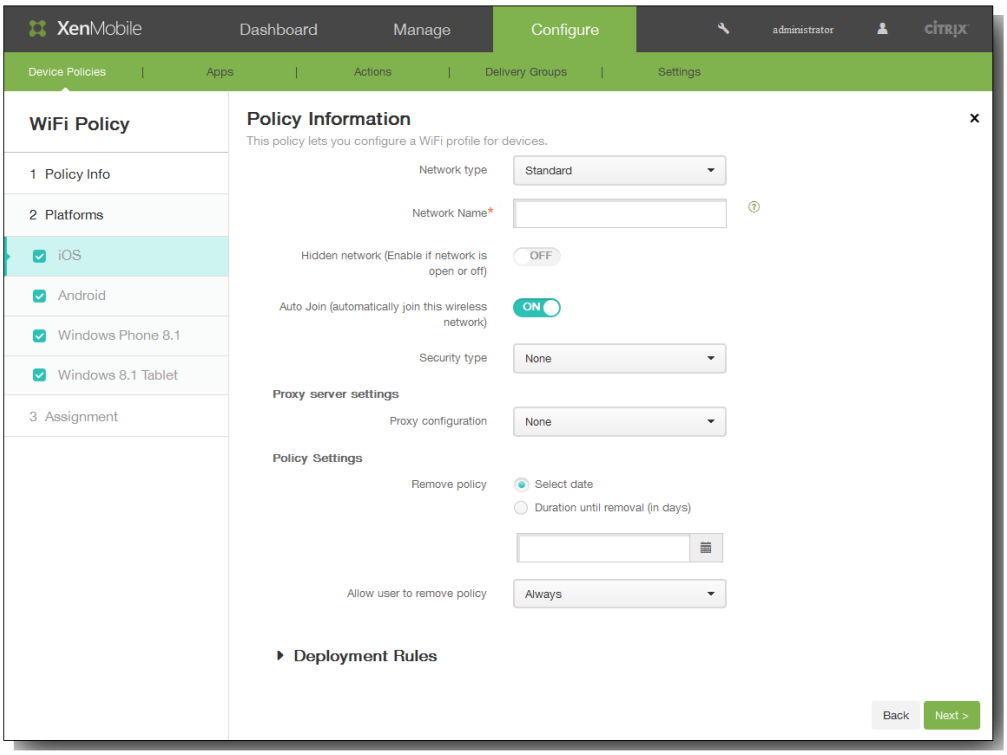
2. Cliquez sur Ajouter pour ajouter une nouvelle stratégie. La boîte de dialogue Ajouter une nouvelle stratégie apparaît. Cliquez sur WiFi.



La page Stratégie WiFi s'affiche.



3. 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).
   3. Cliquez sur Suivant.
4. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter ou modifier. Décochez les plates-formes que vous ne souhaitez pas configurer.
   Si vous avez sélectionné iOS, configurez les paramètres suivants :



1. Dans la liste Type de réseau, cliquez sur le type de réseau que vous voulez utiliser.
2. Si vous avez cliqué sur Standard ou Point d'accès d'ancienne génération, entrez les informations suivantes :
    1. Nom du réseau : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil.
    2. Réseau masqué (activer si le réseau est ouvert ou désactivé) : sélectionnez cette option pour spécifier si le réseau est masqué.
    3. Rejoindre automatiquement : sélectionnez cette option pour spécifier si le réseau est rejoint automatiquement.
3. Si vous avez cliqué sur Hotspot 2.0, entrez les informations suivantes, qui sont répertoriées après les informations de type de sécurité :

    Remarque : ces options s'appliquent uniquement à iOS 7.0 ou versions ultérieures.
    1. Nom d'opérateur affiché : entrez le nom d'opérateur à afficher.
    2. Nom de domaine : entrez le nom du domaine.
    3. Autoriser la connexion aux réseaux partenaires itinérants : sélectionnez cette option si vous voulez autoriser les appareils à se connecter à des réseaux partenaires itinérants.
    4. Identificateurs d'organisations (OI) du consortium d'itinérance : ajoutez des identificateurs d'organisations du consortium d'itinérance (facultatif).
    5. Noms de royaumes d'identificateur d'accès réseau (NAI) : ajoutez des noms de domaines d'identificateur d'accès réseau (facultatif).
    6. Codes de pays mobiles (MCCs) et configurations de réseaux mobiles (MNCs) : ajoutez des codes de pays mobiles et des configurations de réseaux mobiles (facultatif).
4. Type de sécurité : dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
    - Aucun(e)
    - WEP
    - WPA/WPA2 Personnel
    - Tous (Personnel)
    - WEP Enterprise
    - WPA/WPA2 Enterprise
    - Tous (Entreprise)

Le tableau suivant dresse la liste des options à configurer pour chaque type de connexion suivante. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Aucun(e)	**WEP**	**WPA/WPA2 Personnel**	**Tous (Personnel)**	**WEP Enterprise**	**WPA/WPA2 Enterprise**	**Tous (Entreprise)**
Mot de passe	–	Facultatif	Facultatif	Facultatif	–	–	–
TLS	–	–	–	–	OFF	OFF	OFF
TTLS	–	–	–	–	OFF	OFF	OFF
LEAP	–	–	–	–	OFF	OFF	OFF
PEAP	–	–	–	–	OFF	OFF	OFF
EAP-FAST	–	–	–	–	OFF	OFF	OFF
EAP-SIM	–	–	–	–	OFF	OFF	OFF
Authentification interne (TTLS)	–	–	–	–	MSCHAPv2 (lorsque TTLS = ON)	**MSCHAPv2 (lorsque TTLS = ON)**	MSCHAPv2 (lorsque TTLS = ON)
Identité externe	–	–	–	–	Facultatif (lorsque PEAP, TTLS ou EAP-FAST = On)	Facultatif (lorsque PEAP, TTLS ou EAP-FAST = On)	Facultatif (lorsque PEAP, TTLS ou EAP-FAST = On)
Utiliser PAC	–	–	–	–	OFF	OFF	OFF
Provisioning du PAC	–	–	–	–	OFF (lorsque Utiliser PAC = On)	OFF (lorsque Utiliser PAC = On)	OFF (lorsque Utiliser PAC = On)
Provisioning du PAC de manière anonyme	–	–	–	–	OFF (lorsque Provisioning du PAC = On)	OFF (lorsque Provisioning du PAC = On)	Désactivé (lorsque le provisioning du PAC = Activé)
Nom	–	–	–	–	Facultatif	Facultatif	Facultatif

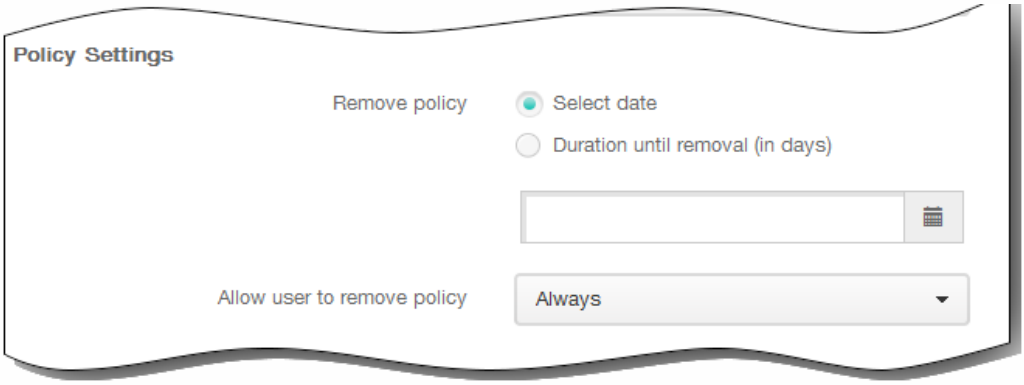
d'utilisateur Mot de passe par connexion	**Aucun(e)** –	**WEP** –	**WPA/WPA2 Personnel** –	**Tous (Personnel)** –	**WEP Enterprise** OFF	**WPA/WPA2 Enterprise** OFF	**Tous (Entreprise)** OFF
Mot de passe	–	–	–	–	Facultatif	Facultatif	Facultatif
Infos d'identification de l'identité (Keystore ou informations d'identification PKI)	–	–	–	–	Aucun(e)	Aucun(e)	Aucun(e)
Requiert un certificat TLS	–	–	–	–	OFF	OFF	OFF
Certificats approuvés	–	–	–	–	Facultatif	Facultatif	Facultatif
Noms de certificats de serveur approuvés	–	–	–	–	Facultatif	Facultatif	Facultatif
Autoriser les exceptions de fiabilité	–	–	–	–	ON	ON	ON

5. Configuration du proxy : dans la liste, sélectionnez la façon dont la connexion VPN transite via un serveur proxy et configurez des options supplémentaires.
   Le tableau suivant dresse la liste des options disponibles pour Manuel et Automatique ; la valeur Aucun ne nécessite aucune configuration supplémentaire. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Manuel	**Automatique**
Nom d'hôte/adresse IP du serveur proxy	Requis	–
Port du serveur proxy	Requis	–
Nom d'utilisateur	Facultatif	–
Mot de passe	Facultatif	–
URL du serveur proxy	–	Requis

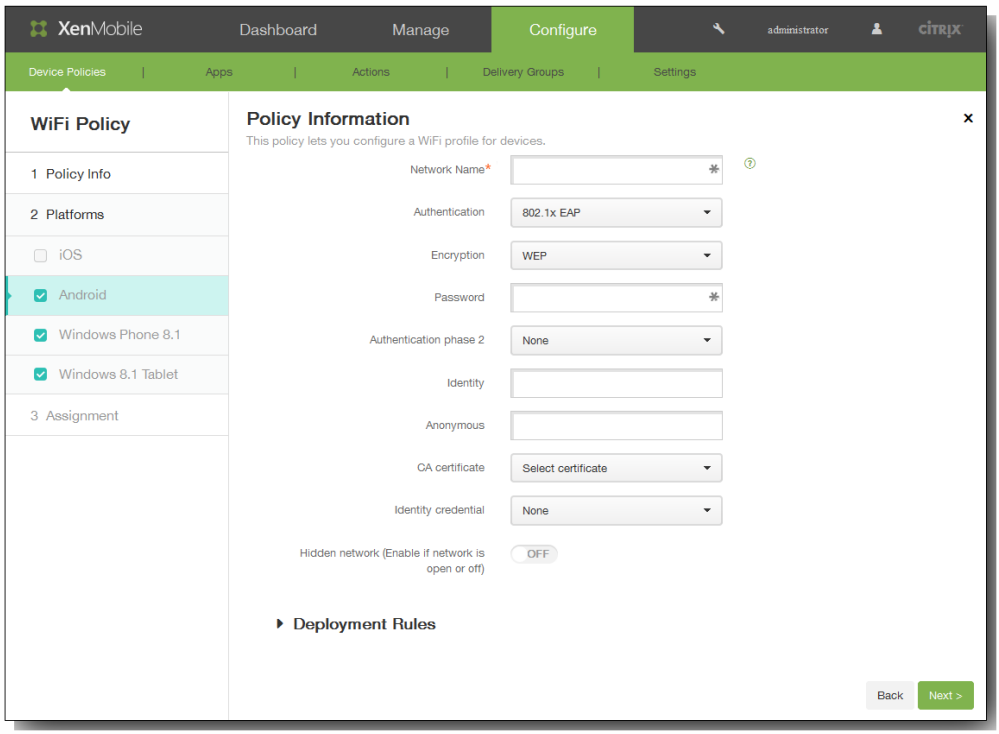
Autoriser les connexions directes si le fichier PAC est inaccessible	**Manuel**	**Automatique** (pour iOS 7.0 et versions ultérieures)

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 :



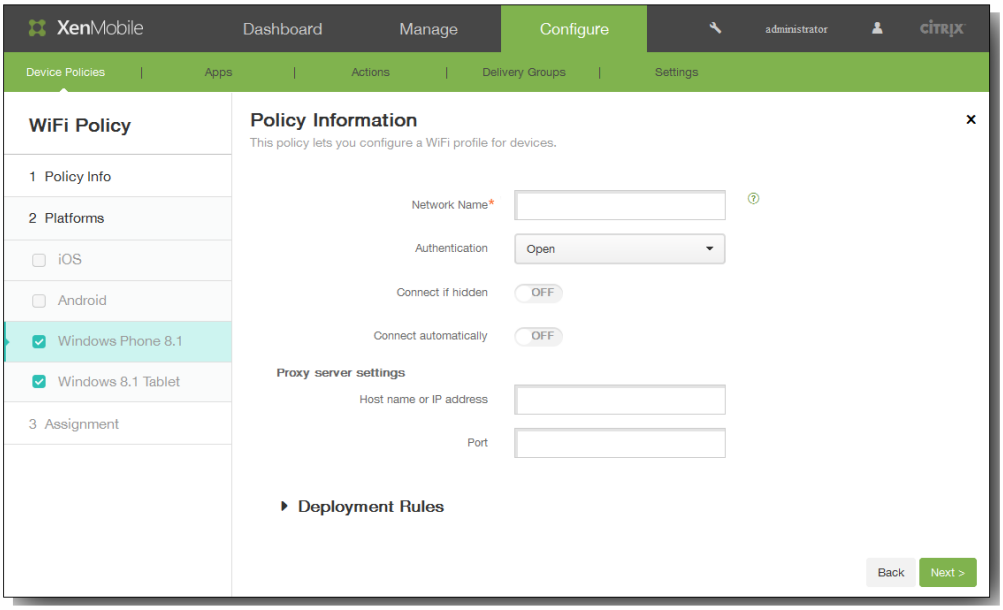
1. Nom du réseau : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
2. Authentification : dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
   - Ouverte
   - Partagé
   - WPA
   - WPA-PSK
   - WPA2
   - WPA2-PSK
   - 802.1x EAP

   Le tableau suivant dresse la liste des options à configurer pour chaque type de connexion suivante. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option est requise, facultative ou si elle ne s'applique pas (-).

	Ouverte	**Partagé**	**WPA**	**WPA-PSK**	**WPA2**	**WPA2-PSK**	**802.1 EAP**
Chiffrement	WEP	WEP	TKIP	TKIP	TKIP	TKIP	–
Mot de passe	Facultatif	Facultatif	–	–	–	–	Facultatif
Type EAP	–	–	–	–	–	–	PEAP
Authentification phase 2	–	–	–	–	–	–	Aucun(e)
Identité	–	–	–	–	–	–	Facultatif
Anonyme	–	–	–	–	–	–	Facultatif
Certificat CA	–	–	–	–	–	–	Sélectionner
Certificats d'identité	–	–	–	–	–	–	Aucun(e)

3. Réseau masqué (activer si le réseau est ouvert ou désactivé) : sélectionnez cette option pour spécifier si le réseau est masqué.

Si vous avez sélectionné Windows Phone 8.1, configurez les paramètres suivants :



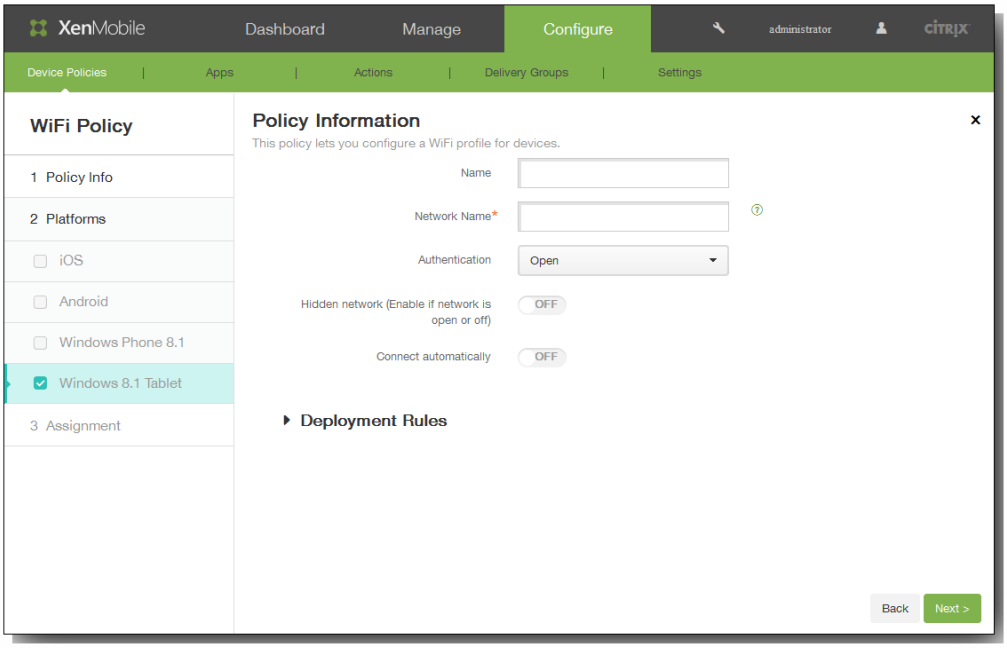
1. Nom du réseau : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
2. Authentification : dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
   - Ouverte
   - WPA Personnel
   - WPA-2 Personnel
   - WPA-2 Enterprise

   Le tableau suivant dresse la liste des options à configurer pour chaque type de connexion suivante. Chaque cellule répertorie la valeur par défaut d'une option lorsqu'une valeur par défaut existe ; sinon, la cellule indique si l'option n'est pas applicable (-), requise ou facultative.

	Ouverte	WPA Personnel	WPA-2 Personnel	WPA-2 Enterprise
Chiffrement	–	AES	AES	AES
Clé partagée	–	Facultatif	Facultatif	–

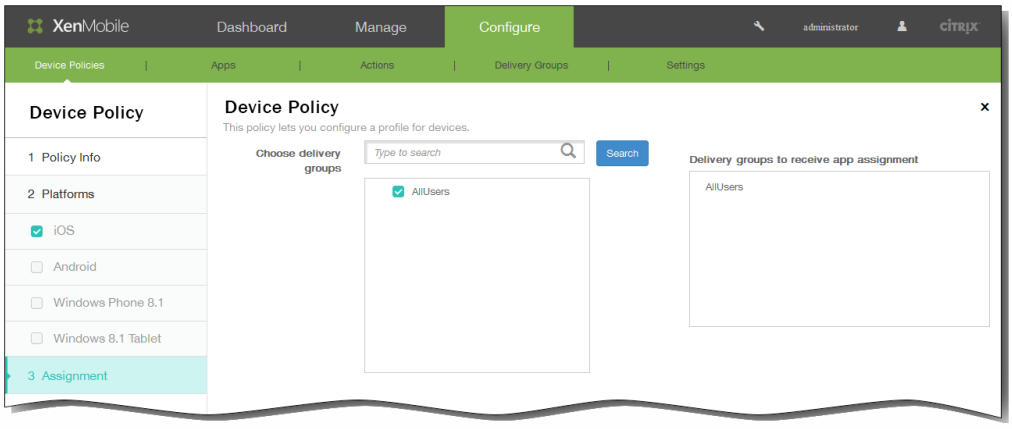
3. Se connecter si le réseau Wi-Fi est masqué : sélectionnez cette option pour spécifier si vous souhaitez vous connecter lorsque le réseau est masqué.
4. Se connecter automatiquement : sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.
5. Nom d'hôte ou adresse IP : entrez le nom ou l'adresse IP d'un serveur VPN.
6. Port : entrez le numéro de port du serveur proxy.

Si vous avez sélectionné Windows 8.1 tablet, configurez les paramètres suivants :



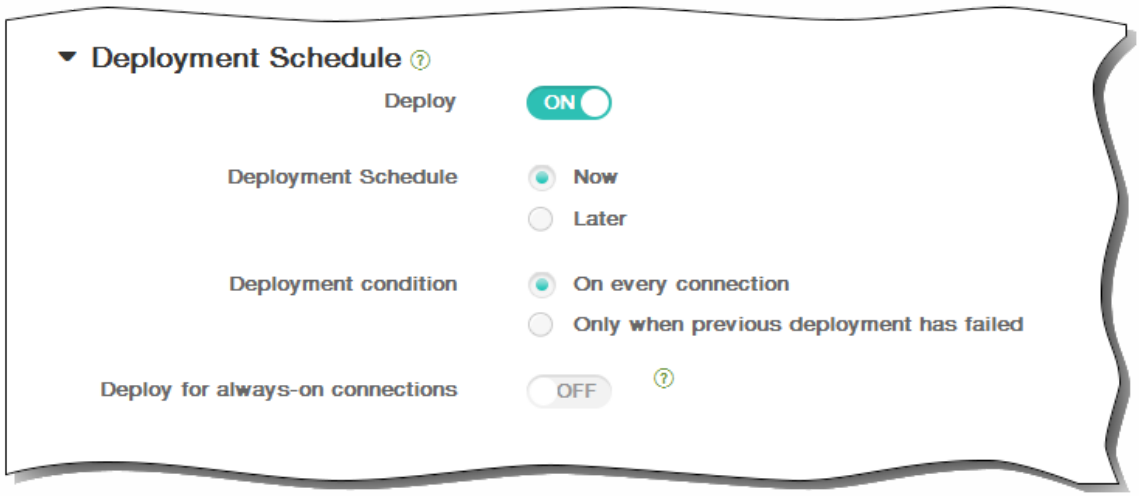
1. Nom : entrez un nom pour le réseau.
2. Nom du réseau : entrez le SSID qui est affiché dans la liste des réseaux disponibles sur l'appareil de l'utilisateur.
3. Authentification : dans la liste, cliquez sur le type de sécurité à utiliser avec la connexion Wi-Fi.
   - Ouverte
   - WPA Personnel
   - WPA-2 Personnel
   - WPA Enterprise
   - WPA-2 Enterprise
4. Réseau masqué (activer si le réseau est ouvert ou désactivé) : sélectionnez cette option pour spécifier si le réseau est masqué.
5. Se connecter automatiquement : sélectionnez cette option si vous souhaitez vous connecter au réseau automatiquement.

5. Une fois que vous avez terminé de configurer les paramètres pour un ou plusieurs plates-formes, cliquez sur Suivant et la page Attribution s'affiche.
6. 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.



7. 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.



8. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de termes et conditions pour toutes les plates-formes

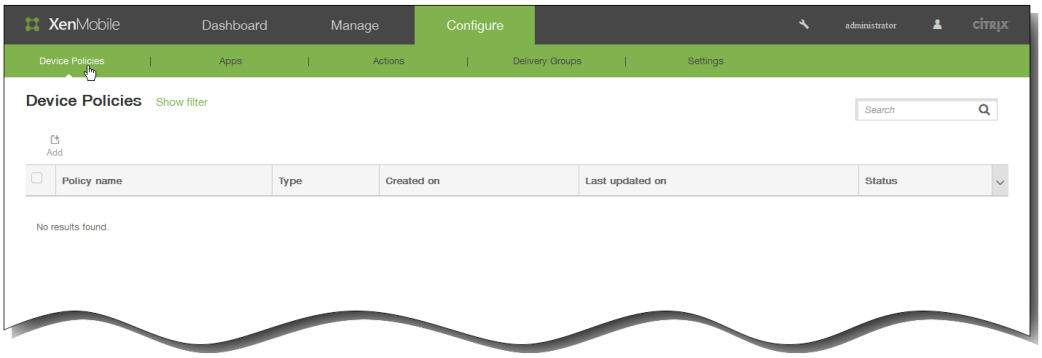
May 06, 2016

Vous créez des stratégies de termes et conditions dans XenMobile lorsque vous souhaitez que les utilisateurs acceptent les stratégies spécifiques à votre entreprise qui régissent les connexions au réseau d'entreprise. Lorsque les utilisateurs inscrivent leurs appareils auprès de XenMobile, ils voient s'afficher les termes et conditions et doivent les accepter pour inscrire leurs appareils. Le refus des termes et conditions annule le processus d'inscription.

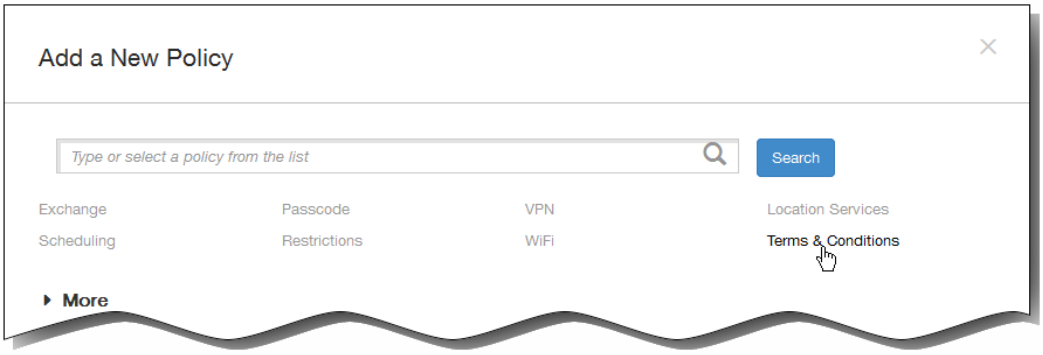
Vous pouvez créer différentes stratégies pour les termes et conditions dans différentes langues si votre société dispose d'utilisateurs internationaux pour leur permettre d'accepter les termes et conditions dans leur langue maternelle.

Remarque : les fichiers de termes et conditions doivent être au format PDF.

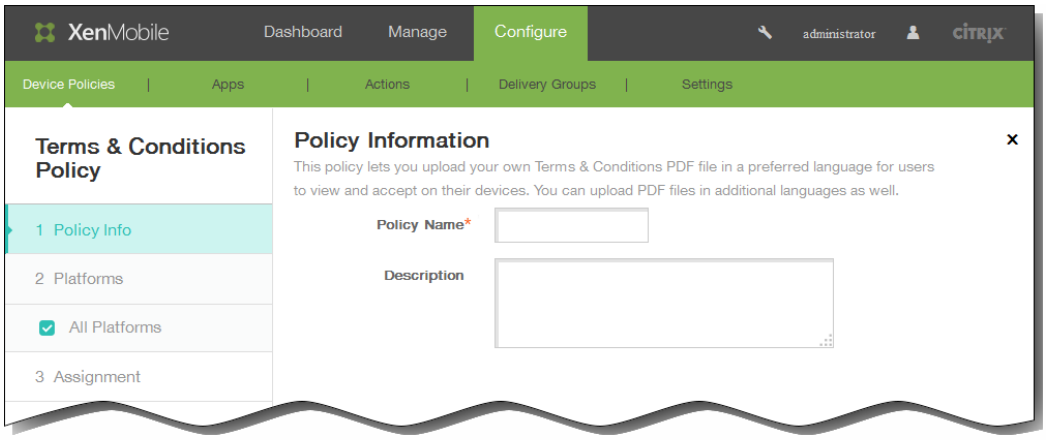
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



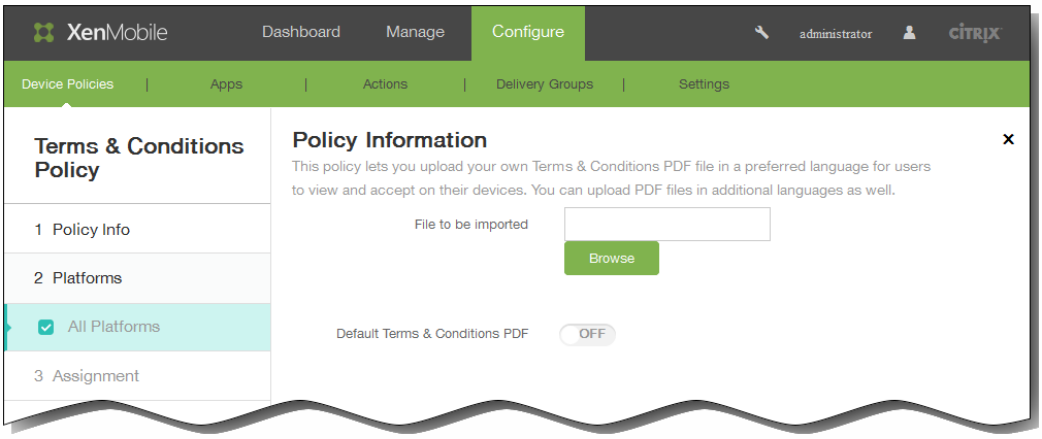
2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Termes et conditions. La page Stratégie termes et conditions s'affiche.

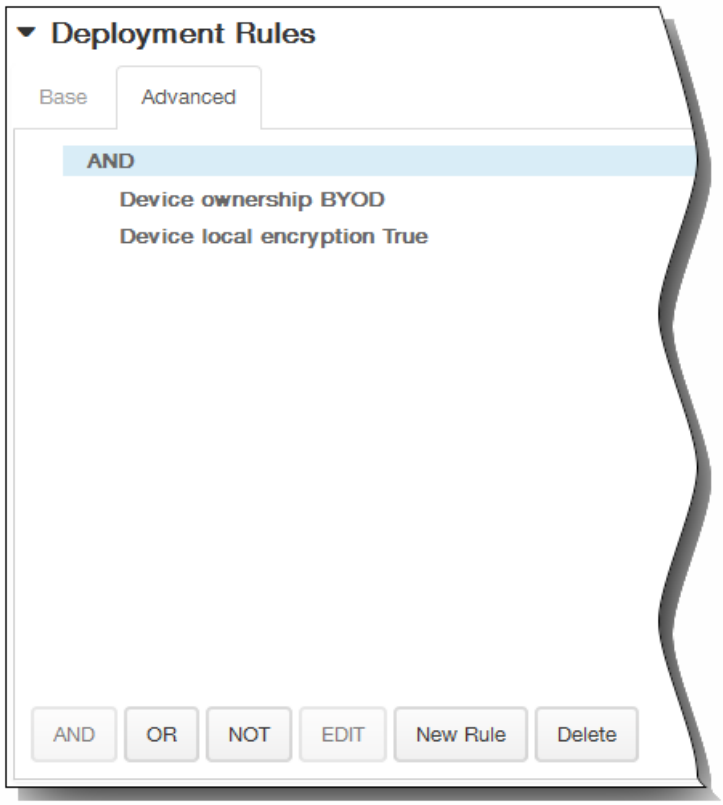


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Toutes les plates-formes s'affiche.



6. Dans la page d'informations Toutes les plates-formes, entrez les informations suivantes :
   1. Fichier à importer : sélectionnez le fichier de termes et conditions à importer en cliquant sur Parcourir, puis accédez à l'emplacement du fichier.
   2. PDF Termes et conditions par défaut : sélectionnez cette option pour désigner ce fichier comme le document par défaut pour les utilisateurs qui sont membres de plusieurs groupes avec différents termes et conditions. La valeur par défaut est OFF.
7. Développez Règles de déploiement, puis configurez les paramètres suivants : L'onglet Base s'affiche par défaut.

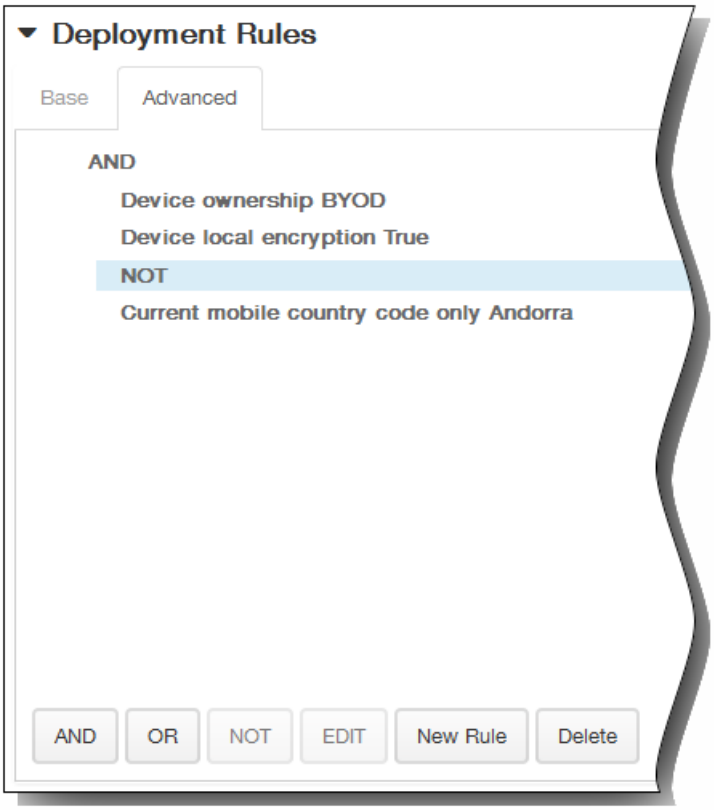
1. Dans la liste, cliquez sur les options pour déterminer quand la stratégie doit être déployée.
   1. Vous pouvez déployer la stratégie lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



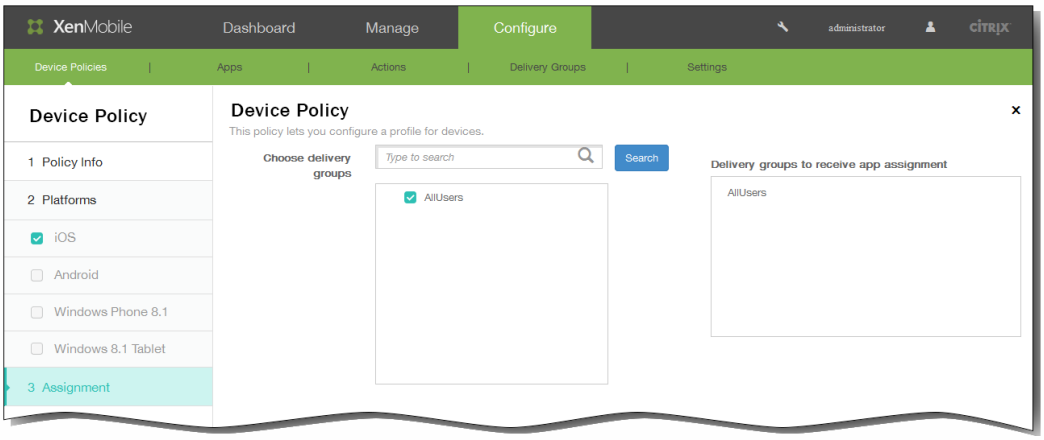
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la règle, puis cliquez sur le signe plus (+) sur le côté droit pour ajouter la condition à la règle.
      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.



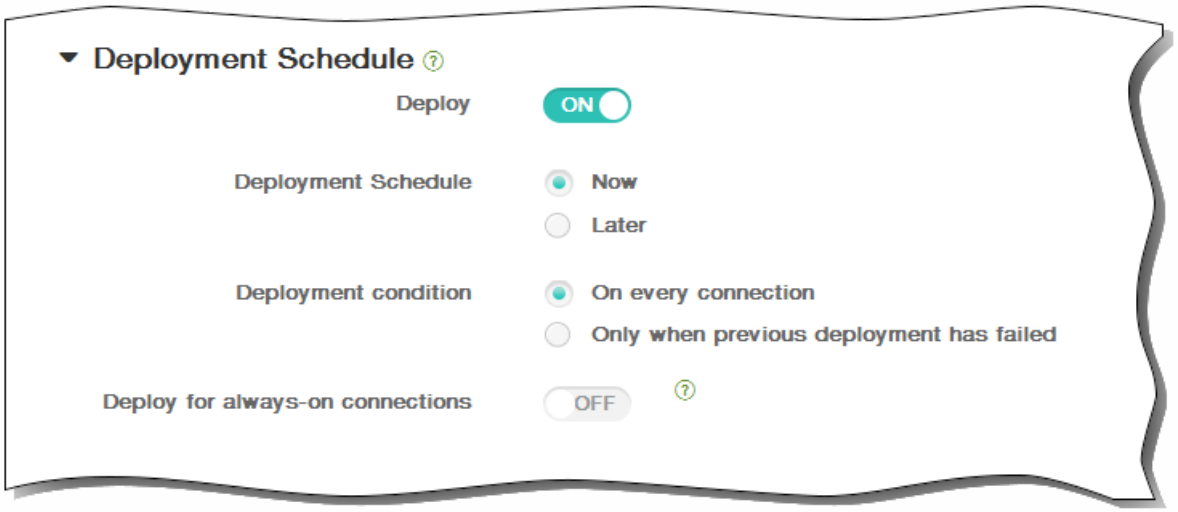
8. Cliquez sur Suivant. La page d'attribution de la Stratégie termes et conditions s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. 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.



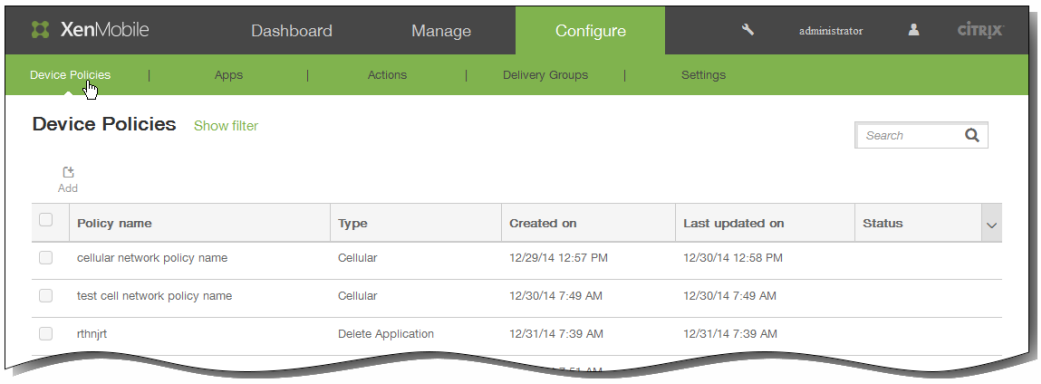
11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie Worx Store

May 06, 2016

Cette stratégie permet de spécifier si un clip Web Worx Store s'affiche sur les appareils. La stratégie peut s'appliquer aux plates-formes suivantes : iOS, Android ou Windows 8.1 Tablet.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

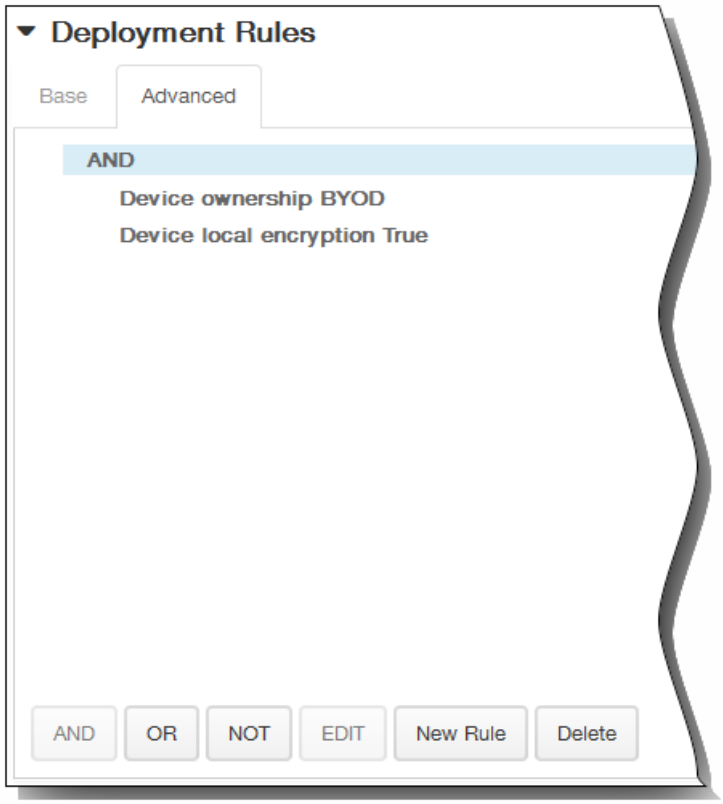


2. Sur la page Ajouter une nouvelle stratégie, cliquez sur PlusWorx Store.
3. Sur la page Stratégie Worx Store, dans le panneau Informations sur la stratégie, entrez les informations suivantes et cliquez sur Suivant.
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
4. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter.
5. Pour chaque plate-forme que vous sélectionnez, laissez la valeur par défaut ON ou cliquez sur OFF si vous ne souhaitez pas qu'un clip Web Worx Store s'affiche sur les appareils.
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.

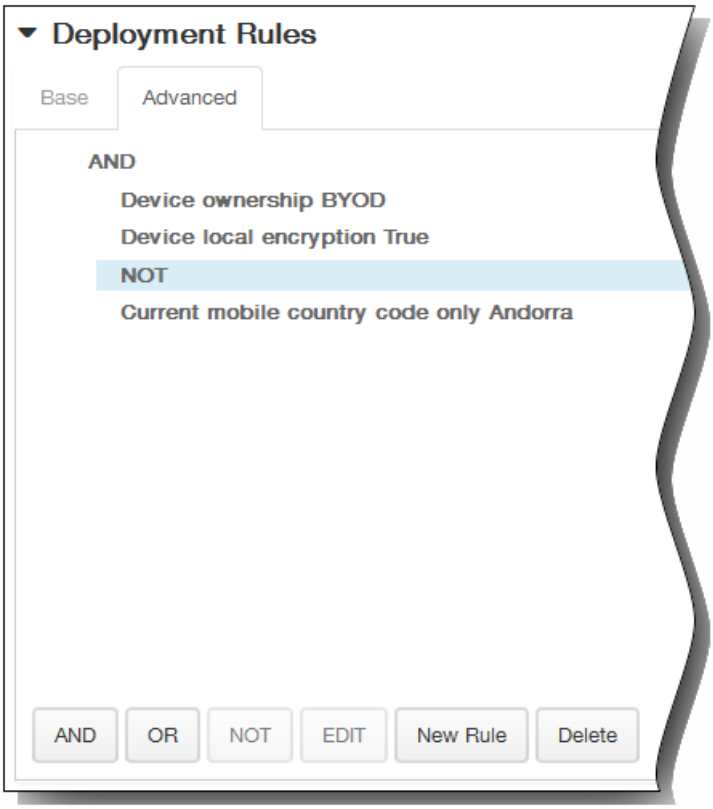
2. Cliquez sur l'onglet Avancé pour combiner les règles avec des options booléennes.



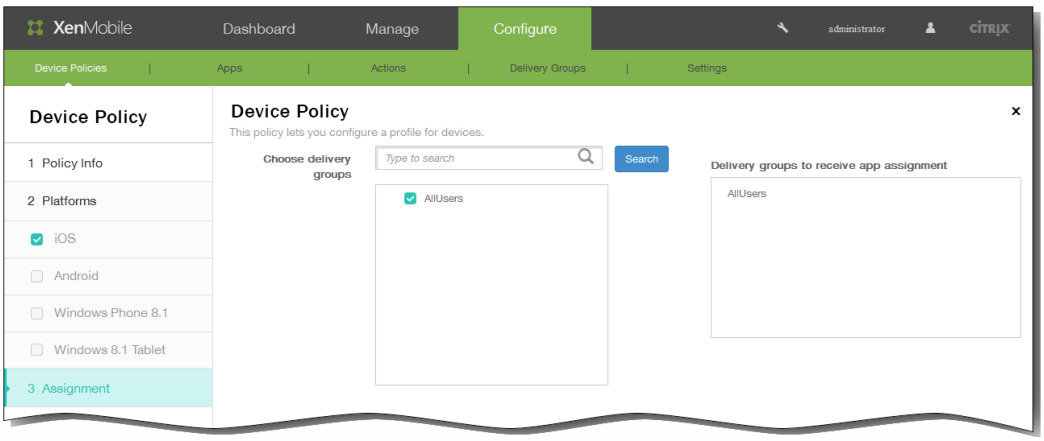
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



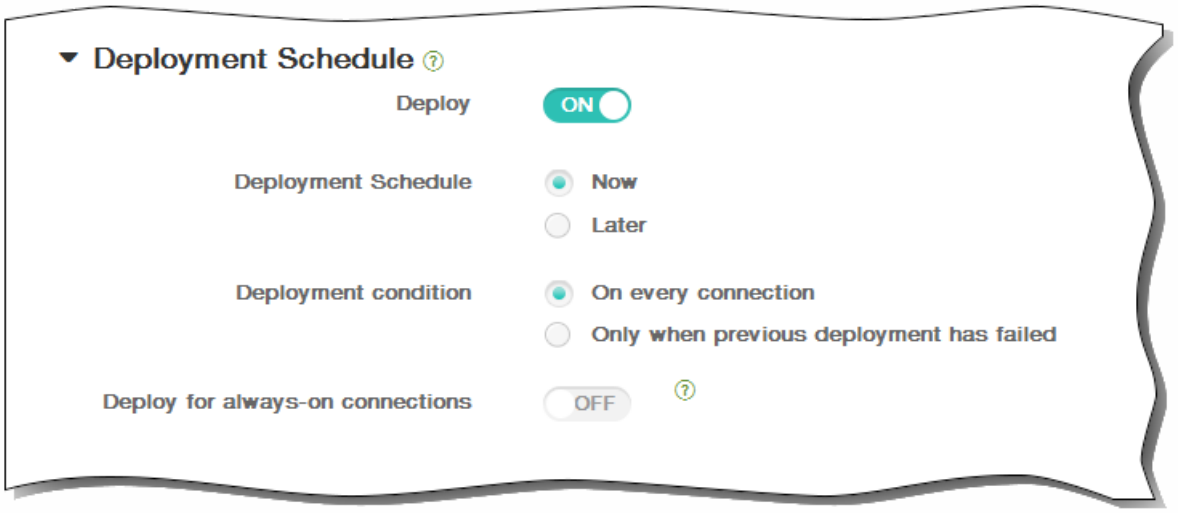
7. Une fois que vous avez terminé la configuration des paramètres pour les plates-formes sélectionnées, cliquez sur Suivant et la page Attribution s'affiche.
8. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes 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.
   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.



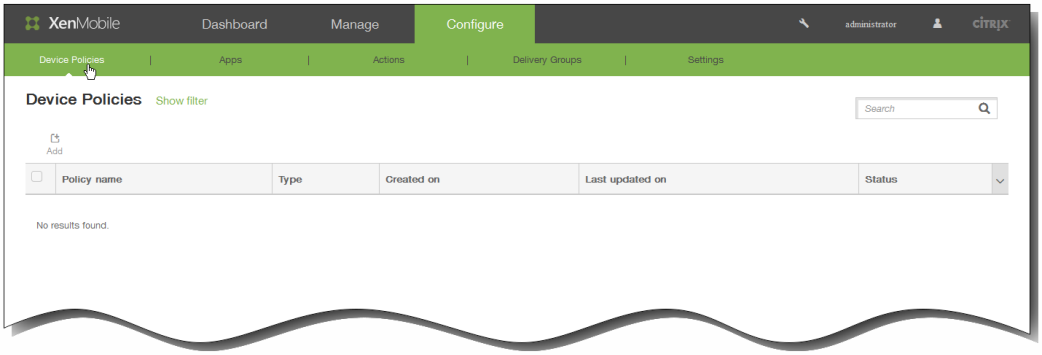
10. Cliquez sur Enregistrer pour enregistrer la stratégie.

Stratégies d'options XenMobile

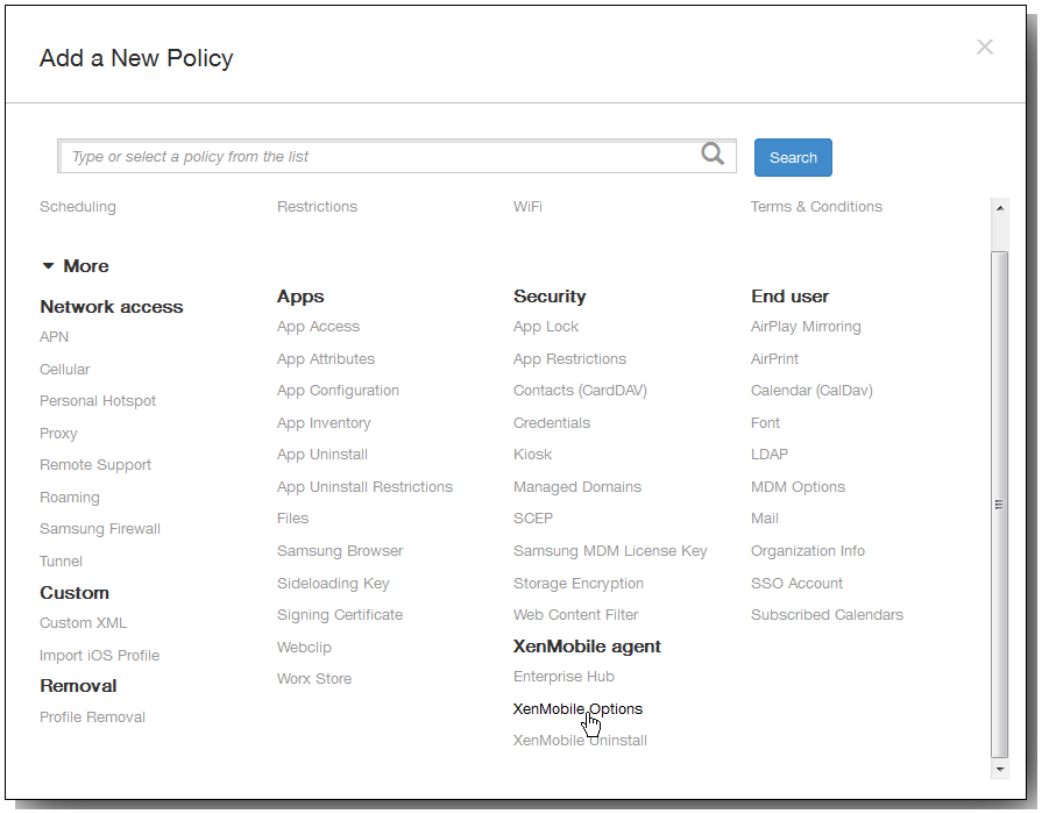
May 06, 2016

Vous ajoutez une stratégie d'options XenMobile pour configurer le comportement de Worx Home lors de la connexion à XenMobile à partir d'appareils Android et Symbian.

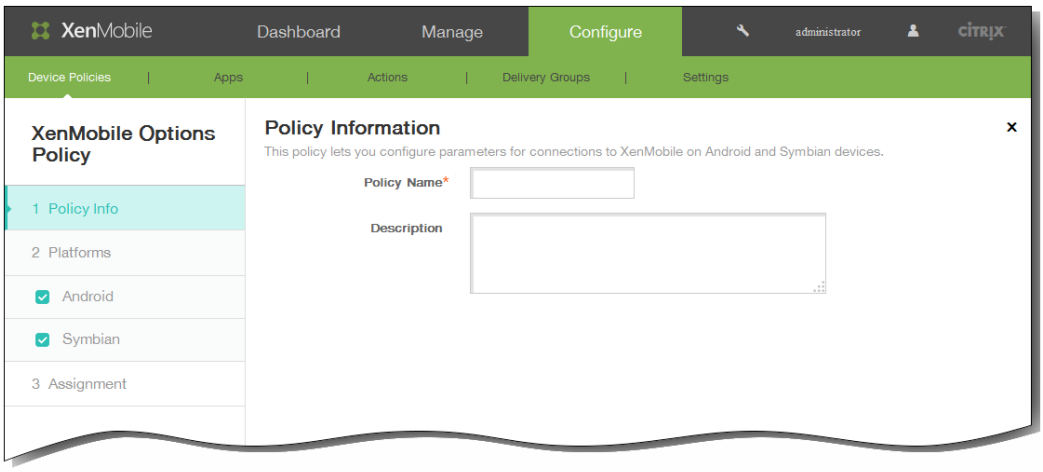
1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.



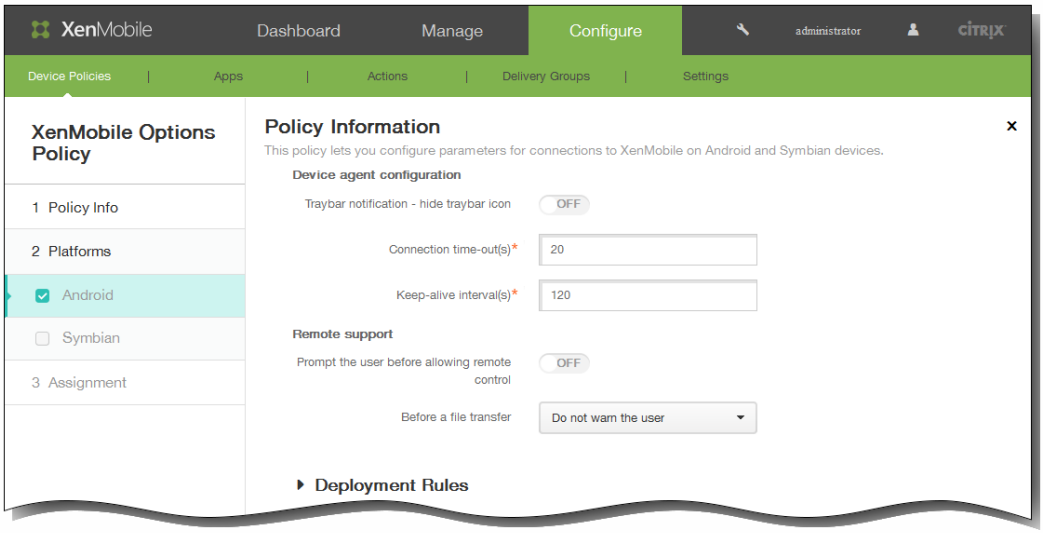
2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.



3. Cliquez sur Plus, puis, sous Agent XenMobile, cliquez sur Options XenMobile. La page Stratégie d'options XenMobile s'affiche.



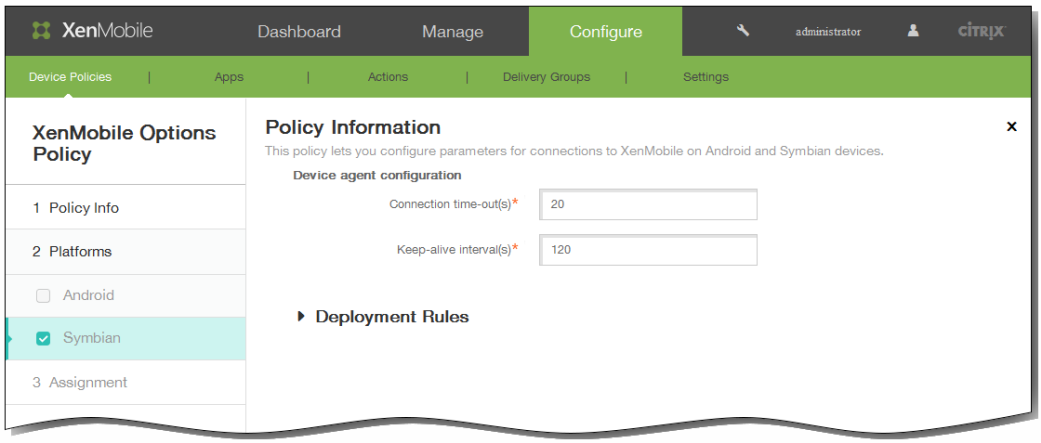
4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
   3. Cliquez sur Suivant.
5. Sous Plates-formes, sélectionnez la plate-forme ou les plates-formes que vous souhaitez ajouter.
   Si vous avez sélectionné Android, configurez les paramètres suivants :



1. Zone de notification - icône masquer la zone de notification : sélectionnez cette option pour spécifier si l'icône de la zone de notification est masquée ou visible.
2. Délai d'expiration des connexions : entrez la durée en secondes pendant laquelle une connexion peut rester inactive avant expiration de la connexion. La durée par défaut est de 20 secondes.
3. Intervalles de persistance des connexions : entrez la durée en secondes pendant laquelle maintenir une connexion ouverte. La durée par défaut est de 120 secondes.
4. Demander à l'utilisateur avant d'autoriser le contrôle à distance : indiquez si une invite s'affiche avant d'autoriser le contrôle à distance.

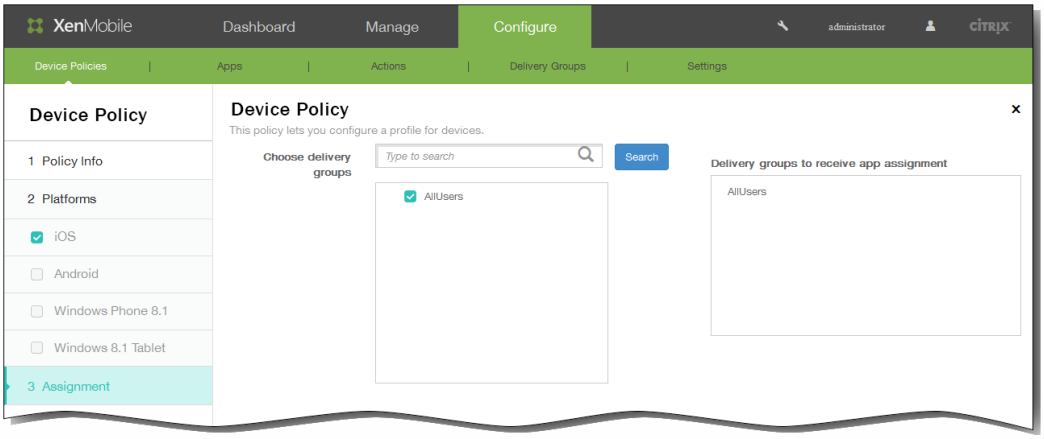
5. Avant un transfert de fichiers : dans la liste, cliquez pour informer l'utilisateur d'un transfert de fichiers ou pour lui demander l'autorisation.

Si vous avez sélectionné Symbian, configurez les paramètres suivants :



1. Délai d'expiration des connexions : entrez la durée en secondes pendant laquelle une connexion peut rester inactive avant expiration. La durée par défaut est de 20 secondes.
2. Intervalles de persistance des connexions : entrez la durée en secondes pendant laquelle maintenir une connexion ouverte. La durée par défaut est de 120 secondes.

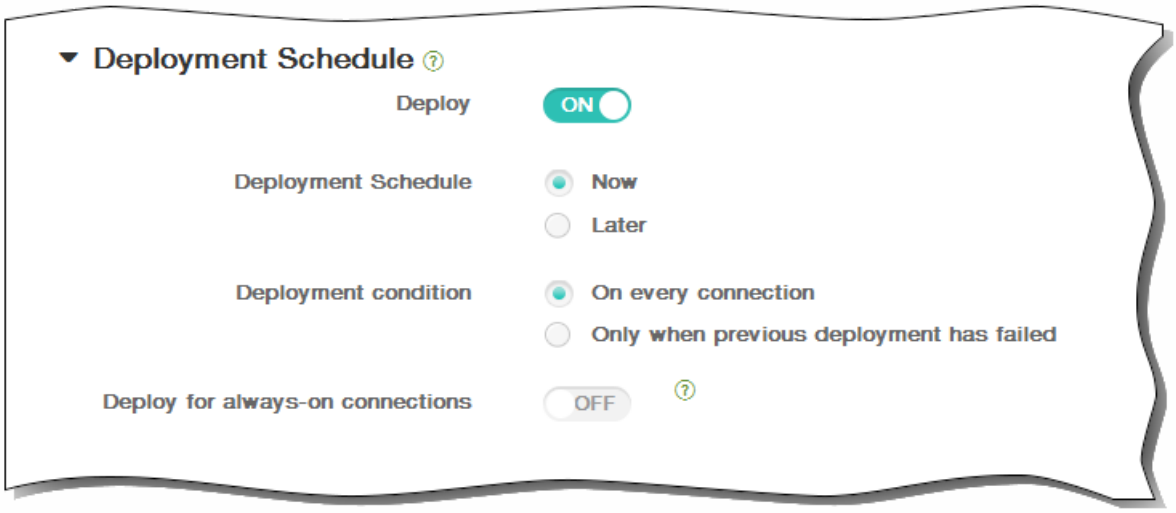
6. Une fois que vous avez terminé de configurer les paramètres pour un ou plusieurs plates-formes, cliquez sur Suivant et la page Attribution s'affiche.
7. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer 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.



8. 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.



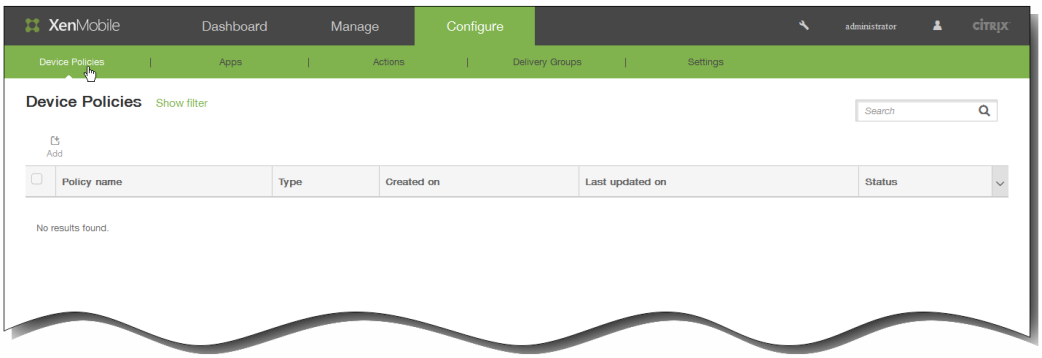
9. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour ajouter une stratégie de désinstallation de XenMobile pour Android

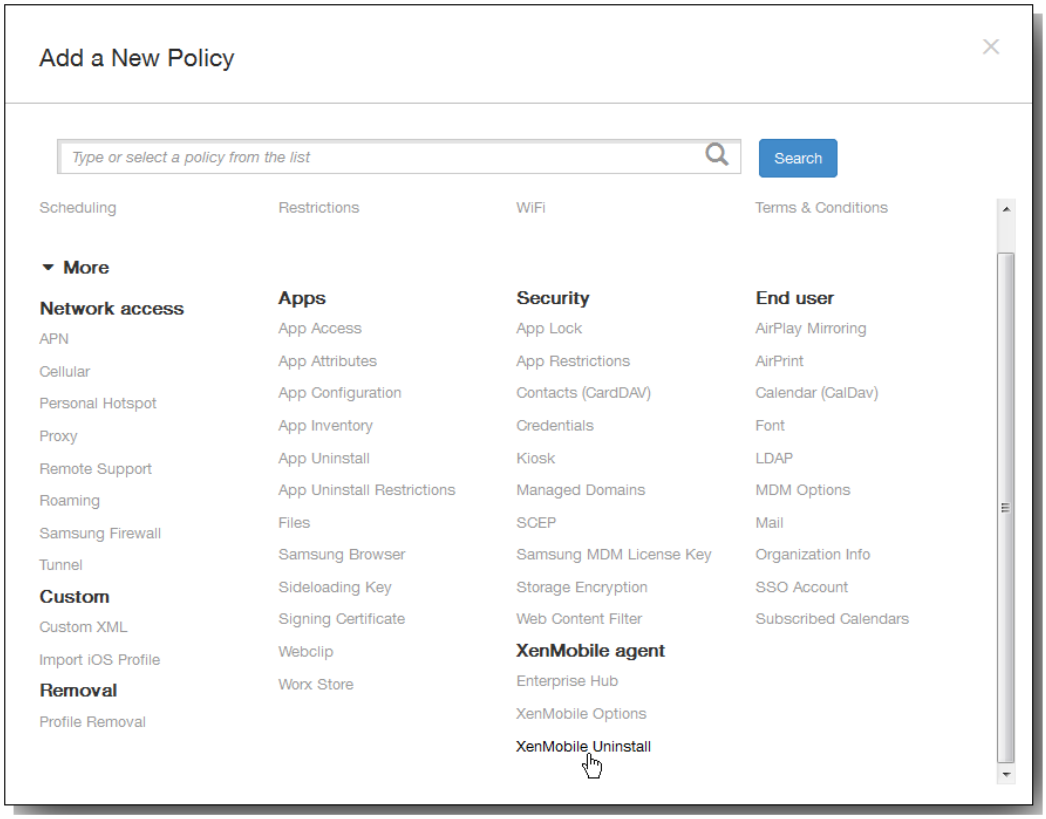
May 06, 2016

Vous pouvez ajouter une stratégie dans XenMobile afin de désinstaller XenMobile des appareils Android. Lorsqu'elle est déployée, cette stratégie supprime XenMobile sur tous les appareils Android dans le déploiement.

1. Dans la console XenMobile, cliquez sur Configurer > Stratégies d'appareil. La page Stratégies d'appareil s'affiche.

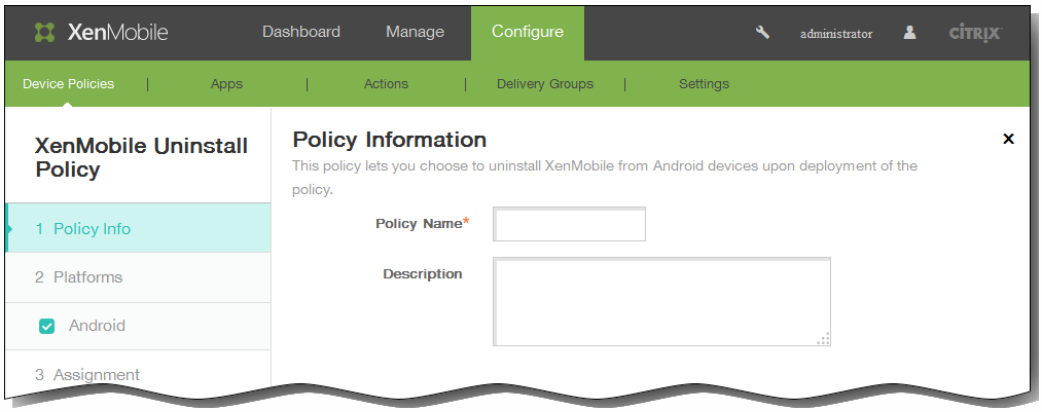


2. Cliquez sur Ajouter. La boîte de dialogue Ajouter une nouvelle stratégie apparaît.

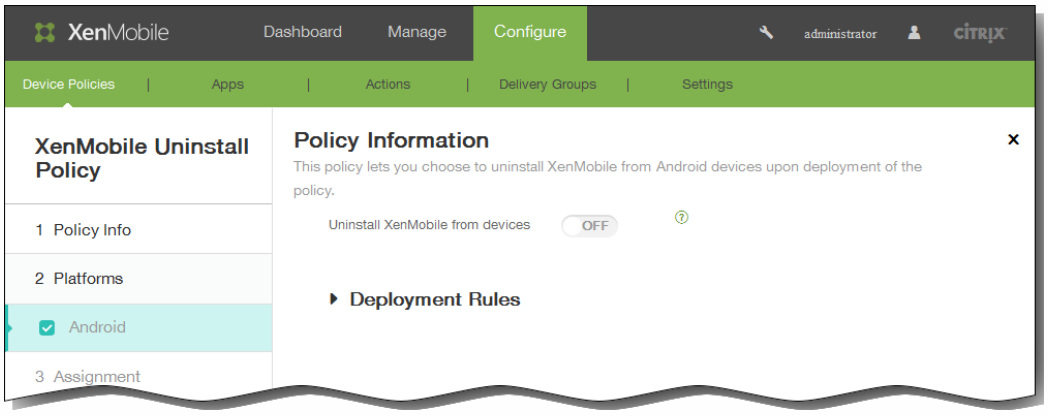


3. Cliquez sur Plus, puis, sous Agent XenMobile, cliquez sur Désinstallation de XenMobile. La page Stratégie de

désinstallation de XenMobile s'affiche.

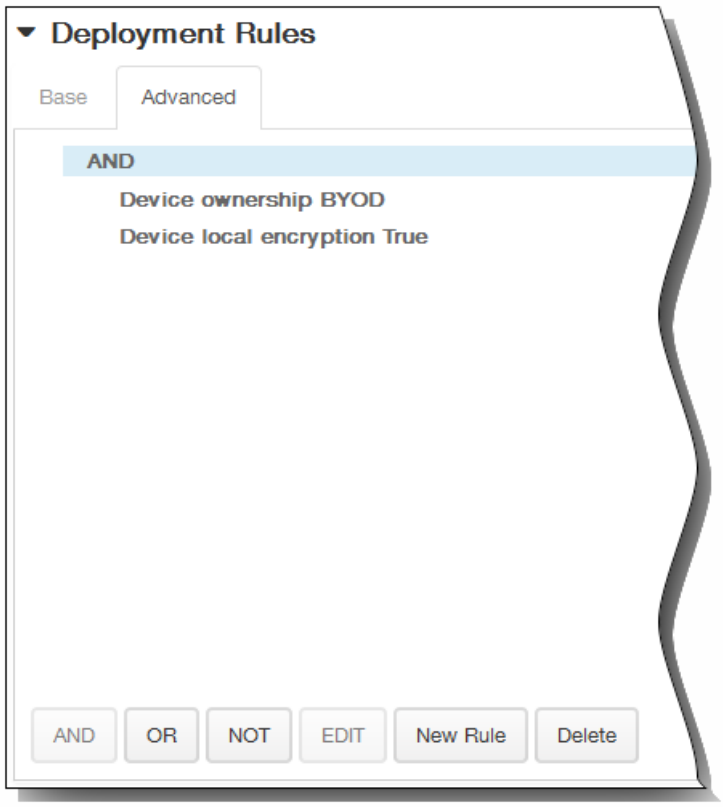


4. Dans la section Informations sur la stratégie, entrez les informations suivantes :
   1. Nom de la stratégie : entrez un nom descriptif pour la stratégie.
   2. Description : entrez une description pour la stratégie (facultatif).
5. Cliquez sur Suivant. La page d'informations Plate-forme Android s'affiche.



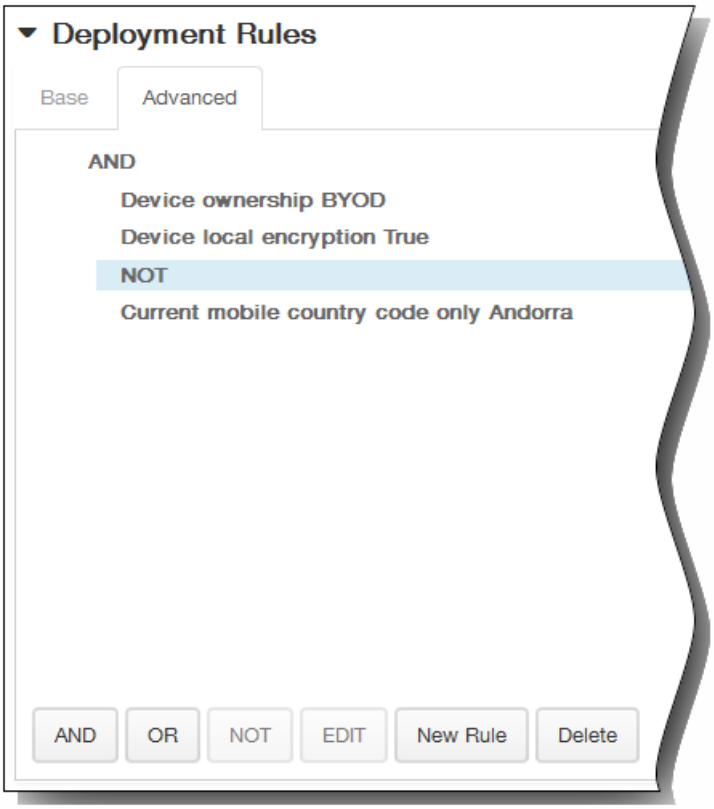
6. Dans la page d'informations Plate-forme Android, entrez les informations suivantes :
   1. Désinstaller XenMobile des appareils : sélectionnez cette option pour désinstaller XenMobile des appareils Android. La valeur par défaut est OFF.
7. Développez Règles de déploiement, puis configurez les paramètres 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.

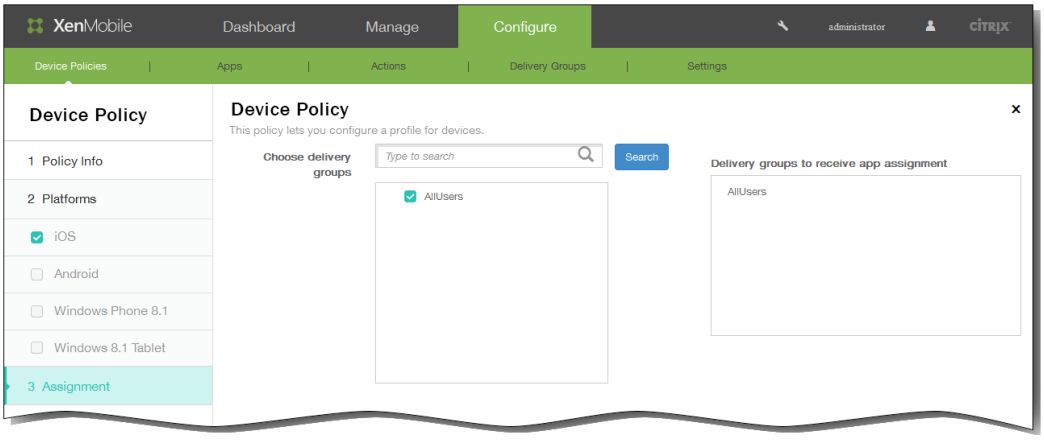


Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.
       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 désinstallation de XenMobile s'affiche.
9. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.

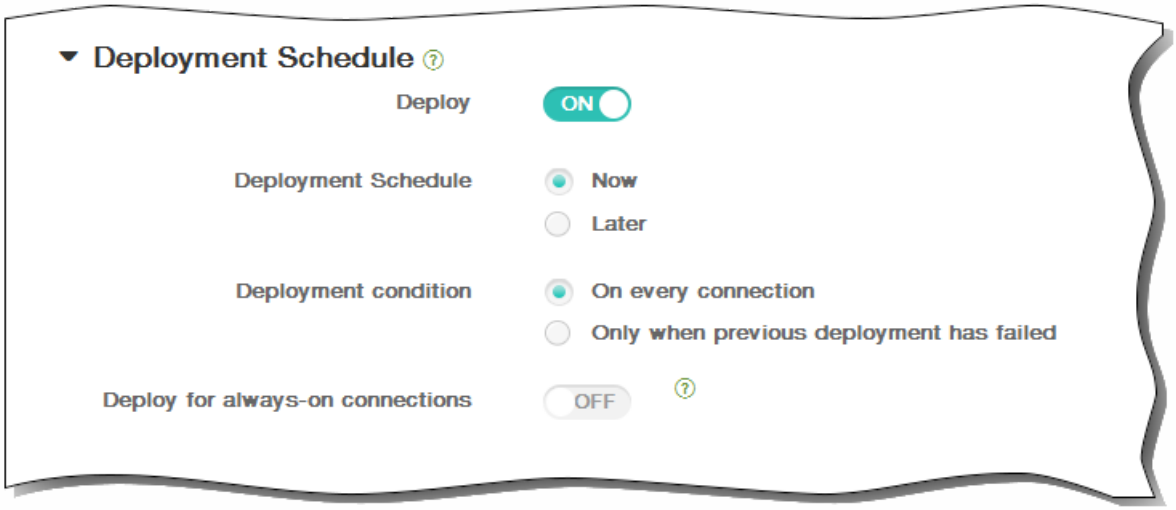


10. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.



11. Cliquez sur Enregistrer pour enregistrer la stratégie.

Pour placer un appareil iOS en mode supervisé à l'aide de Apple Configurator

May 06, 2016

Afin d'utiliser Apple Configurator, vous avez besoin d'un ordinateur Apple exécutant OS X 10.7.2 ou version ultérieure.

> **Important**
>
> le fait de placer un appareil en mode supervisé installera la version sélectionnée d'iOS sur l'appareil, ce qui efface complètement toutes les données et applications précédemment stockées par l'utilisateur.

1. Installez Apple Configurator depuis iTunes.
2. Connectez l'appareil iOS à votre ordinateur Apple.
3. Démarrez le configurateur d'Apple. Le Configurateur indique que vous possédez un appareil à préparer pour la supervision.
4. Pour préparer l'appareil à des fins de supervision :
   1. Basculer le contrôle de supervision sur Activé. Citrix vous recommande de sélectionner ce paramètre si vous prévoyez de gérer le contrôle de l'appareil en appliquant à nouveau une configuration régulièrement.
   2. Si vous le souhaitez, entrez un nom pour l'appareil.
   3. Dans iOS, cliquez sur l'option appropriée afin d'obtenir la version la plus récente d'iOS que vous souhaitez installer.
5. Lorsque vous êtes prêt à préparer l'appareil pour la supervision, cliquez sur Préparer.

Ajout d'applications

May 06, 2016

Vous pouvez ajouter des applications à XenMobile pour en assurer la gestion. Vous ajoutez les applications à la console XenMobile, où vous pouvez organiser les applications par catégorie et les déployer auprès des utilisateurs. Suivez la procédure détaillée plus loin dans cette rubrique pour ajouter des catégories d'applications.

Vous pouvez ajouter les types suivants d'applications à XenMobile :

- **MDX**. Applications wrappées avec le MDX Toolkit (et les stratégies associées). Vous déployez des applications MDX provenant de magasins internes et publics. Par exemple : WorxMail.
- **Magasin d'applications public**. Ces applications peuvent être gratuites ou payantes et sont disponibles dans un magasin public, tel que iTunes ou Google Play. Par exemple : GoToMeeting.
- **Web et SaaS**. Ces applications comprennent les applications accessibles à partir d'un réseau interne (applications web) ou sur un réseau public (SaaS). Vous pouvez créer vos propres applications, ou faire votre choix parmi un ensemble de connecteurs d'applications pour l'authentification unique aux applications Web existantes. Par exemple : GoogleApps_SAML.
- **Entreprise**. Ces applications représentent des applications natives qui ne sont pas wrappées avec le MDX Toolkit et qui ne contiennent aucune des stratégies associées aux applications MDX.
- **Lien Web**. Adresse Web (URL) à un site public ou privé, ou à une application Web qui ne requiert pas d'authentification unique (SSO).

Fonctionnement des applications mobiles et MDX

XenMobile prend en charge les applications iOS, Android et Windows Phone 8.x, y compris les applications Worx, telles que Worx Home, WorxMail et WorxWeb, ainsi que l'utilisation de stratégies MDX. Grâce à la console Web XenMobile, vous pouvez charger des applications mobiles et les mettre à disposition sur les appareils des utilisateurs. En plus des applications Worx, vous pouvez ajouter les types suivants d'applications mobiles :

- Applications que vous développez pour vos utilisateurs.
- Applications dans lesquelles vous souhaitez autoriser ou interdire des fonctionnalités d'appareils à l'aide de stratégies MDX.

Citrix fournit le MDX Toolkit qui wrappe les applications mobiles pour iOS, Android et Windows Phone 8.x avec une logique et des stratégies Citrix. L'outil peut wrapper une application qui a été créée au sein de votre organisation ou une application mobile développée par des tiers de manière sécurisée.

Fonctionnement des applications Web et SaaS

XenMobile est fourni avec un ensemble de connecteurs d'applications constituant des modèles qu'il est possible de configurer en vue de l'authentification unique (SSO) pour des applications Web et Software as a Service (SaaS) et, dans certains cas, pour la création et la gestion de comptes d'utilisateur. XenMobile inclut des connecteurs SAML (Security Assertion Markup Language). Les connecteurs SAML sont prévus pour les applications Web qui prennent en charge le protocole SAML en vue de l'authentification unique et de la gestion des comptes d'utilisateur. XenMobile prend en charge les protocoles SAML 1.1 et SAML 2.0.

Vous pouvez également construire vos propres connecteurs SAML d'entreprise.

Fonctionnement des applications d'entreprise

Vous pouvez créer votre propre connecteur d'application dans XenMobile. Ce type d'application réside généralement dans votre réseau interne. Les utilisateurs peuvent se connecter aux applications à l'aide de Worx Home. Lorsque vous ajoutez une application d'entreprise, vous créez le connecteur d'application en même temps.

Fonctionnement du magasin d'applications public

Vous pouvez configurer des paramètres afin de récupérer les noms et descriptions des applications mobiles depuis l'App Store d'Apple, Google Play et Windows Store. Lorsque vous récupérez les informations d'application dans le magasin, XenMobile remplace le nom et la description existants.

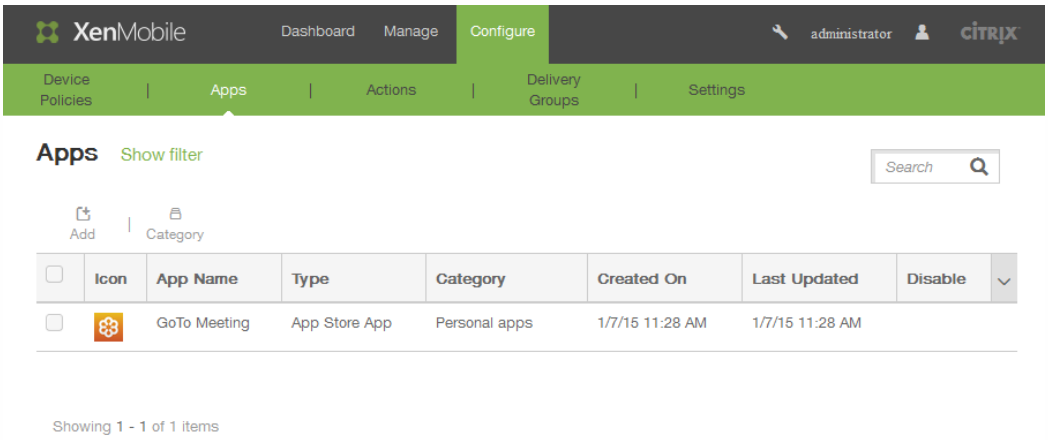
Fonctionnement des liens Web

Un lien Web est une adresse Web permettant d'accéder à un site Internet ou intranet. Un lien Web permet également d'accéder à une application Web qui ne requiert pas d'authentification unique (SSO). Une fois que vous avez terminé de configurer un lien Web, celui-ci s'affiche sous forme d'icône dans le Worx Store. Lorsque les utilisateurs ouvrent une session avec Worx Home, le lien s'affiche avec la liste des applications et bureaux disponibles.

L'ajout d'une application à l'aide de la console comprend les quatre étapes suivantes :

- Ajout d'informations sur l'application.
- Sélection et configuration de l'application pour chaque plate-forme prise en charge, telle que iOS ou Android.
- Définition d'une méthode d'approbation facultative.
- Définition d'attributions facultatives de groupes de mise à disposition.

1. Dans la console XenMobile, cliquez sur **Configurer > Applications**.
   La page Applications s'ouvre.



   Remarque : lorsque vous vous connectez à la console XenMobile pour la première fois, le tableau des applications est vide ; les seules options disponibles sont **Ajouter** et **Catégorie**.
2. Cliquez sur Ajouter, puis suivez les étapes dans les rubriques eDocs suivantes qui correspondent au type que vous voulez ajouter :

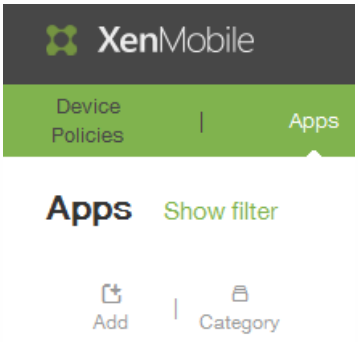
- Pour ajouter une application MDX à XenMobile
- Pour ajouter un magasin d'applications public à XenMobile
- Pour ajouter une application Web et SaaS à XenMobile
- Pour ajouter une application d'entreprise à XenMobile
- Pour ajouter un lien Web applicatif à XenMobile

Remarque : lorsque vous ajoutez une application, les applications s'affichent dans le tableau sur la page Applications, dans laquelle vous pouvez modifier ou catégoriser l'application à tout moment.

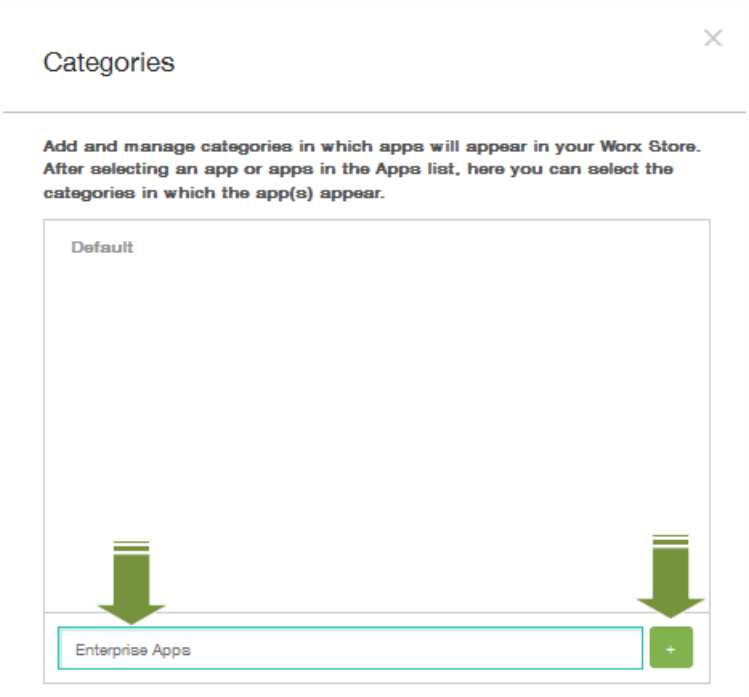
Pour ajouter des catégories d'applications

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.

1. Dans la console XenMobile, cliquez sur Configurer > Applications. La page Applications s'affiche.
2. Sur la page Applications, cliquez sur Catégorie.

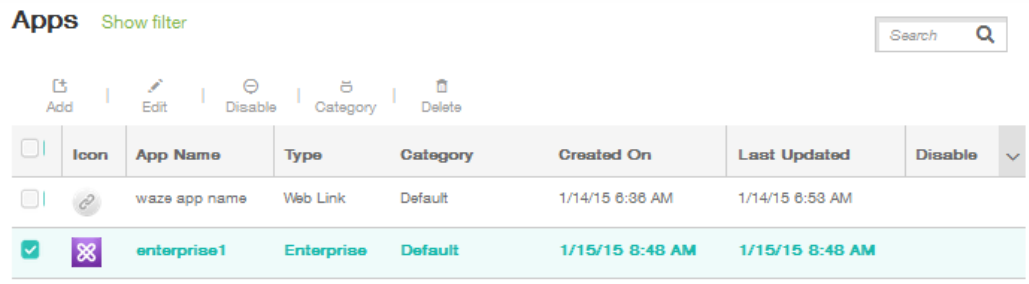


3. Dans la boîte de dialogue Catégories, entrez le nom de la catégorie que vous souhaitez ajouter, puis cliquez sur le signe plus (+). Par exemple, entrez *Applications d'entreprise*, puis cliquez sur le signe plus (+).

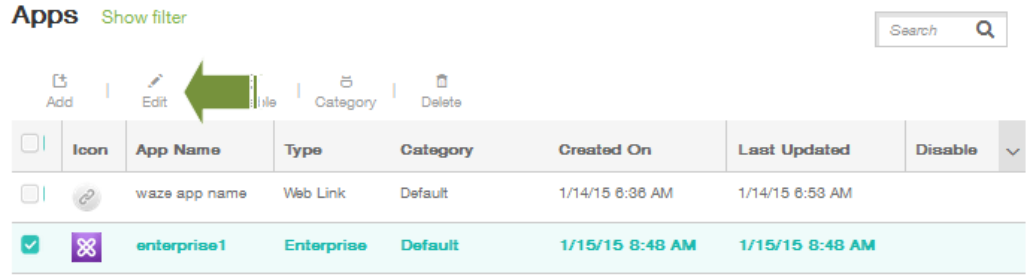


La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue Catégories. Si aucune catégorie n'est configurée, seule la catégorie **par défaut** s'affiche.

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.

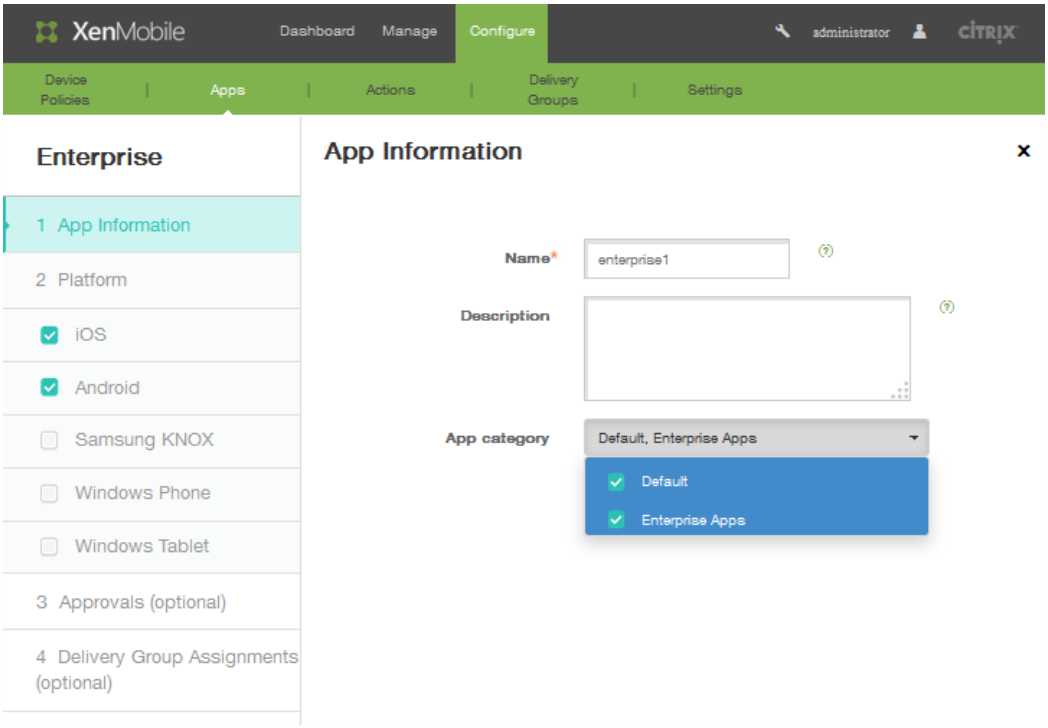


6. Cliquez sur Modifier pour classer l'application.

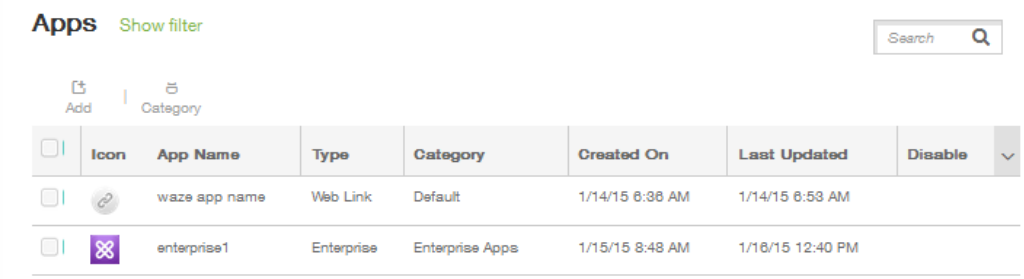


La page Informations sur l'application s'affiche.

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.

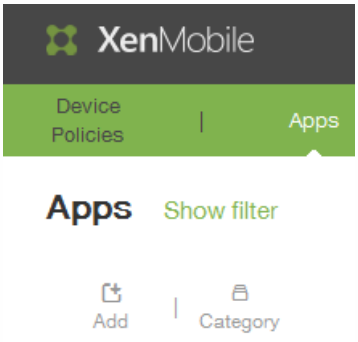


Pour ajouter une application MDX à XenMobile

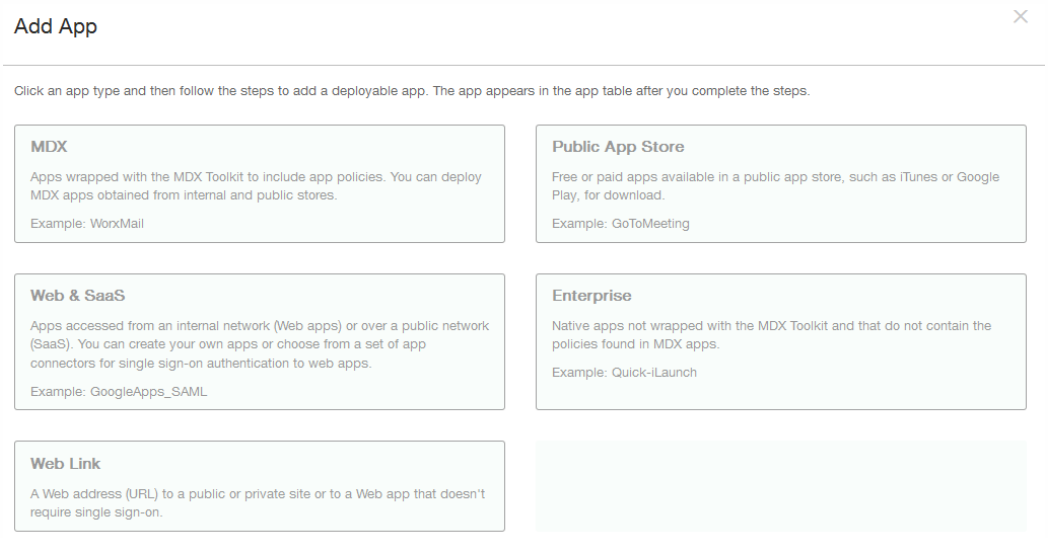
May 06, 2016

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.

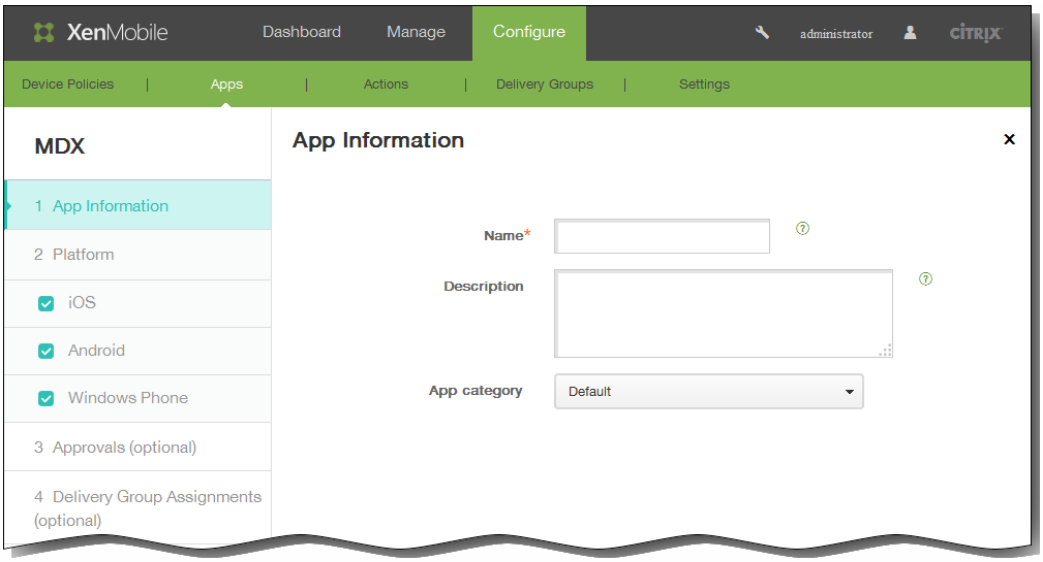
1. Dans la console XenMobile, cliquez sur Configurer > Applications. La page Applications s'affiche.
2. Cliquez sur Ajouter.



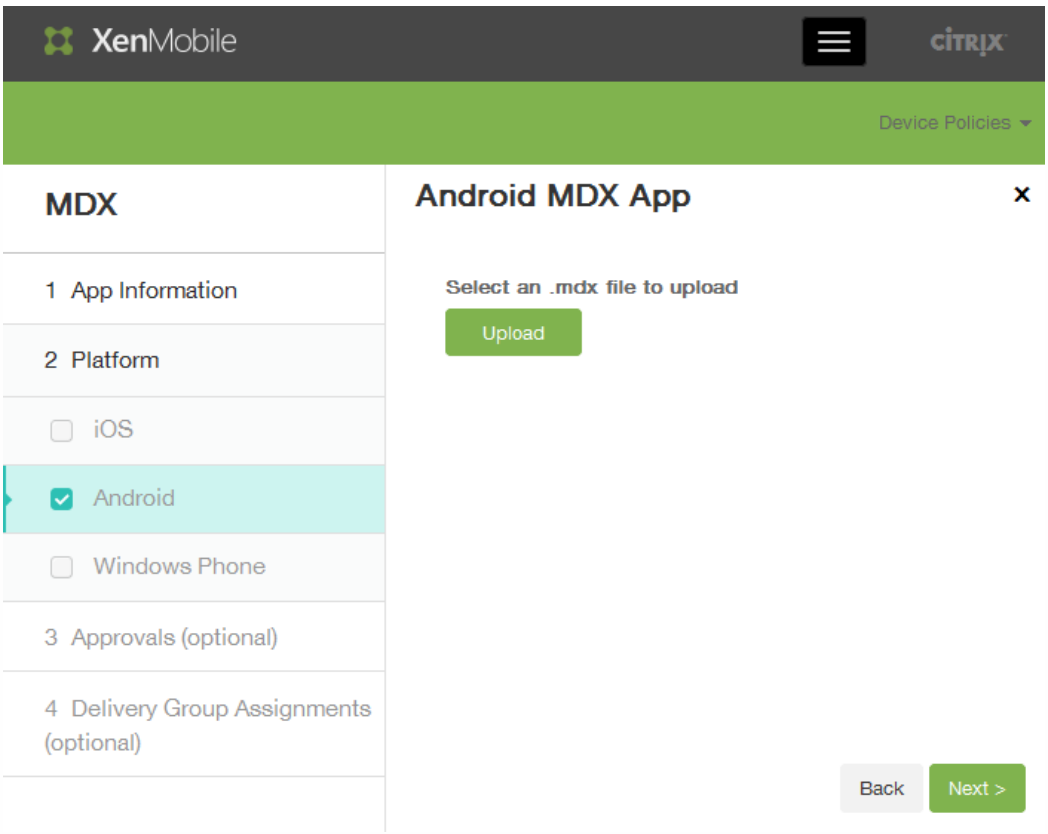
3. Dans l'écran Ajouter une application, cliquez sur MDX.



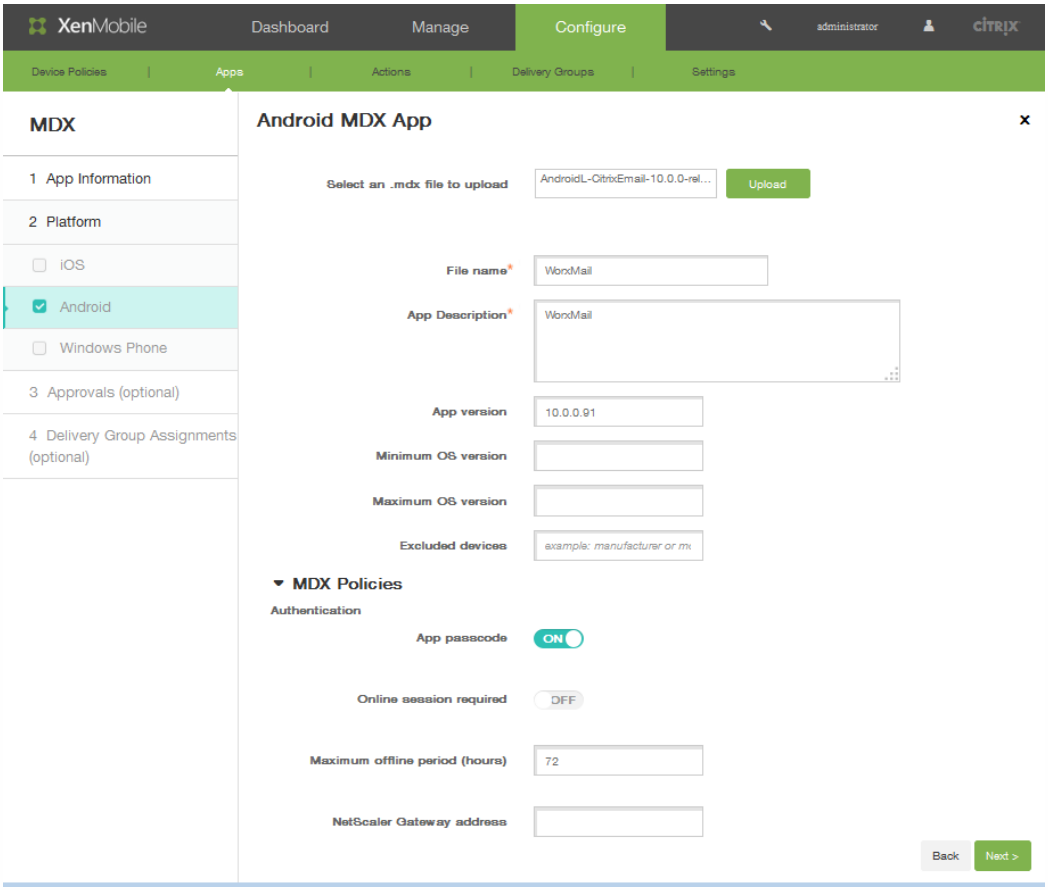
4. Sur la page Informations sur l'application, entrez un nom et une description facultative pour l'application. Ces champs sont utilisés à des fins internes. Si vous ajoutez des applications à de multiples appareils, utilisez les cases à cocher dans la partie gauche de l'écran pour les sélectionner.



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.

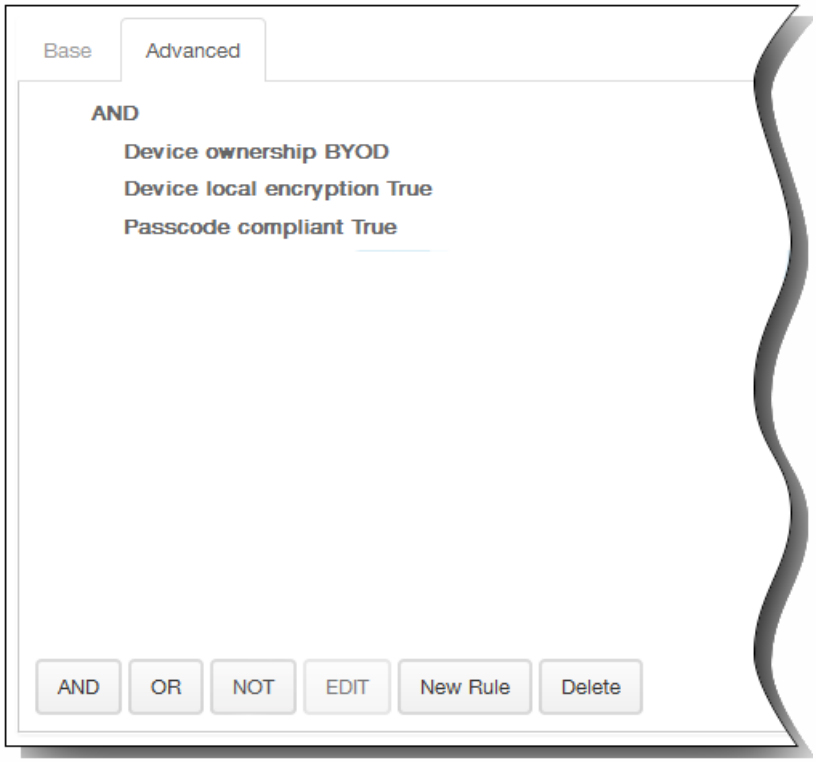


Les champs de détails sur l'application et de stratégies MDX apparaissent.



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.

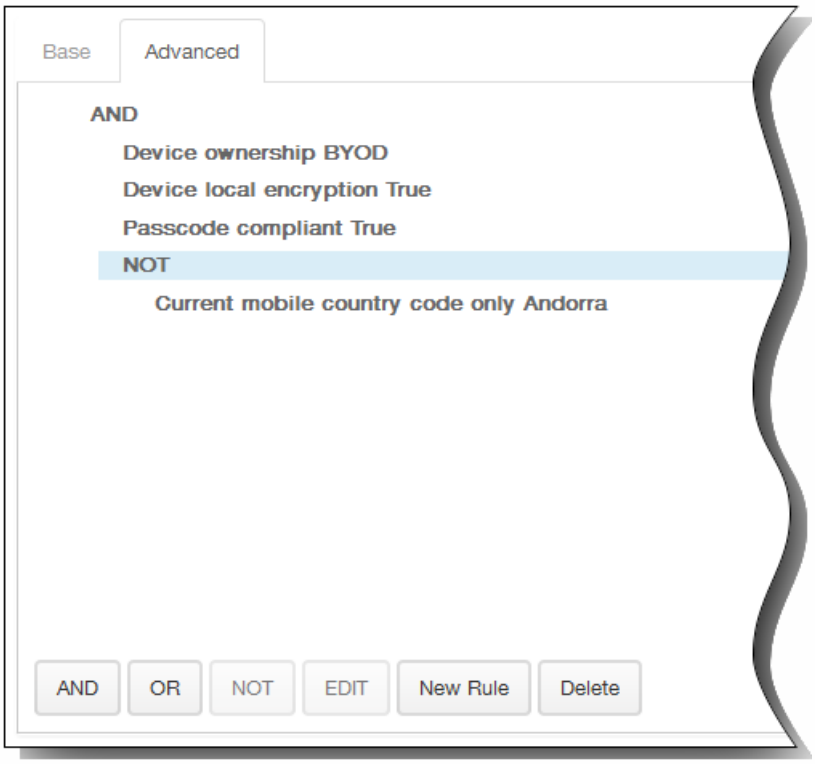
1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
   1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
   2. Cliquez sur Nouvelle règle pour définir 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.



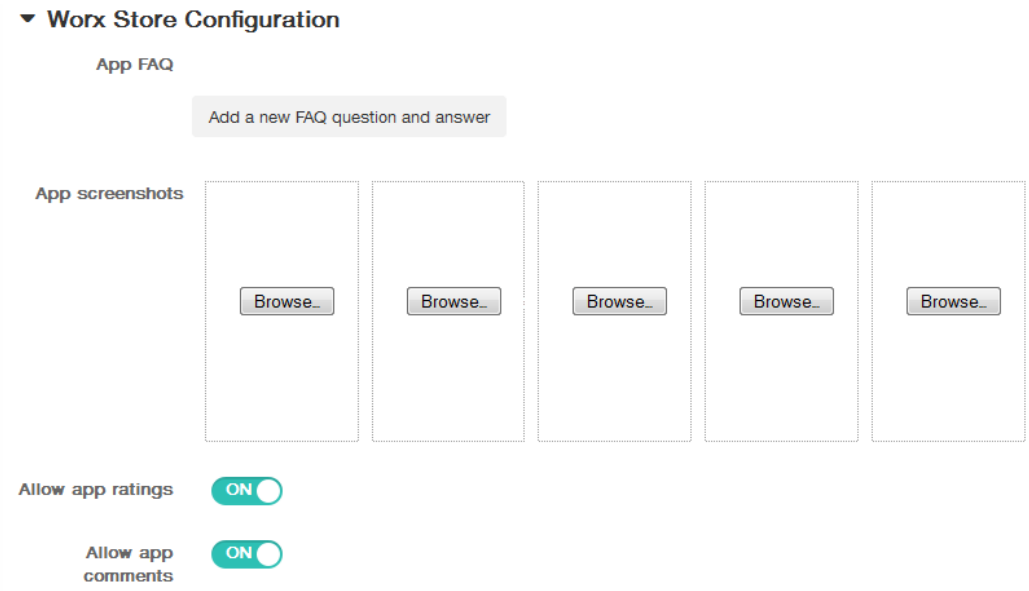
   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.

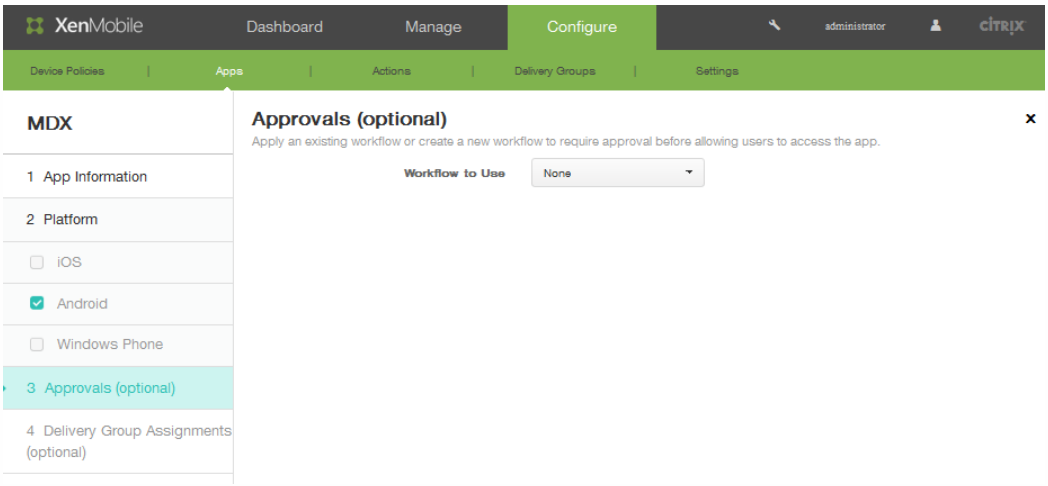


11. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.

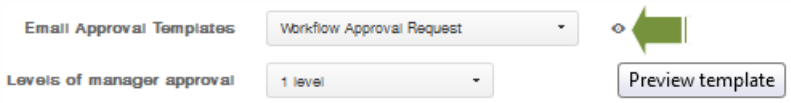


Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

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.



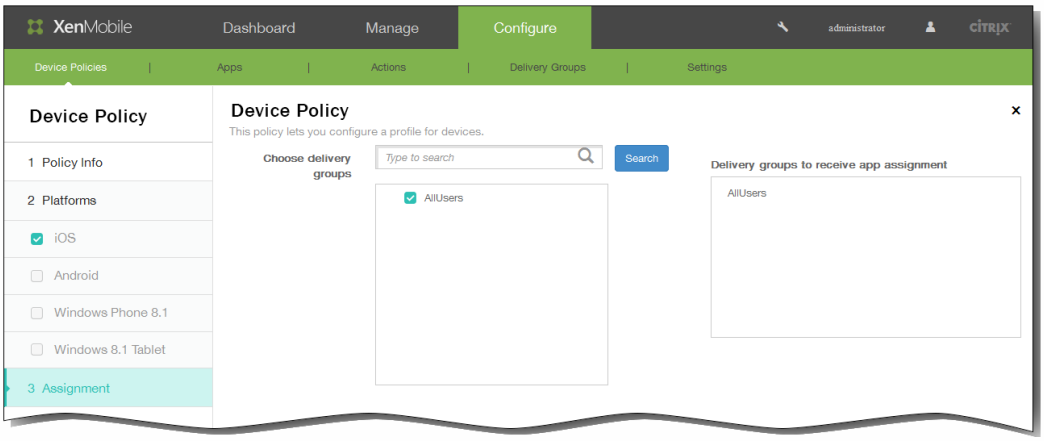
14. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur.
    1. Spécifiez 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. .

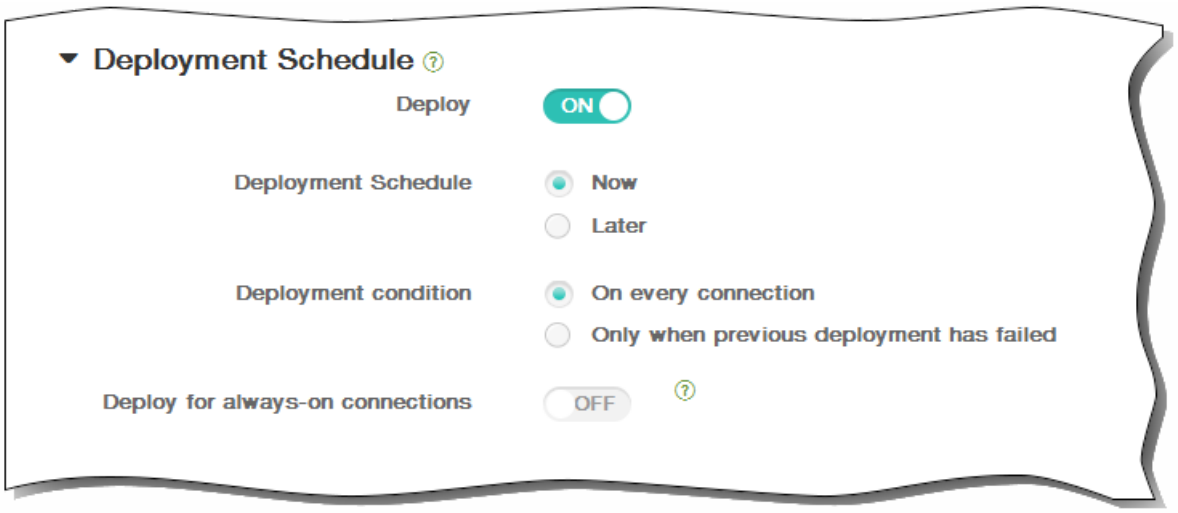
5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

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.



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.

Création de catégories d'applications dans XenMobile

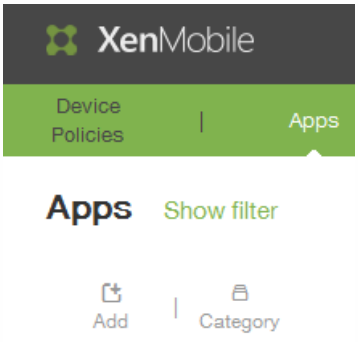
May 06, 2016

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.

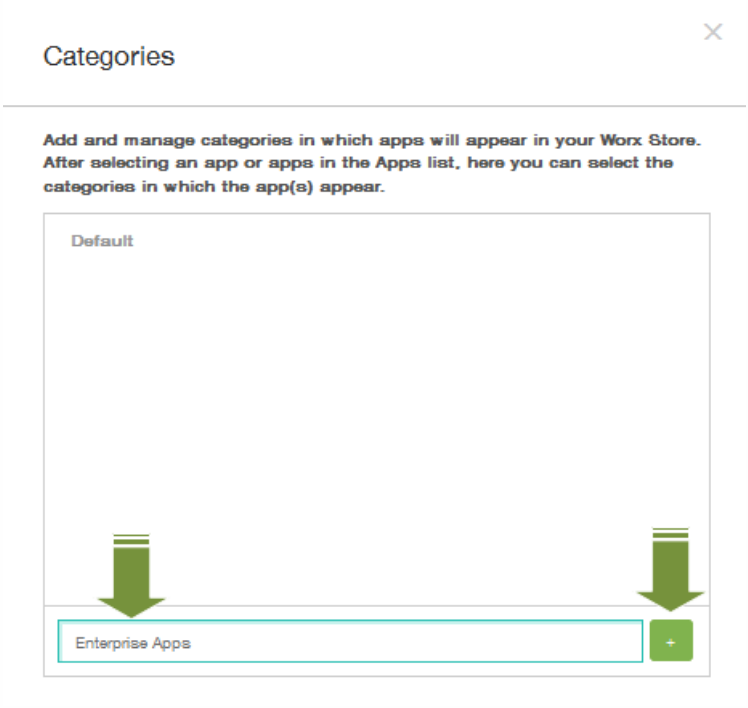
Vous configurez les catégories sur la page Applications dans la console XenMobile. Ensuite, lorsque vous configurez ou modifiez une application, un lien Web ou un magasin, vous pouvez ajouter l'application à l'une des catégories que vous avez configurées.

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.

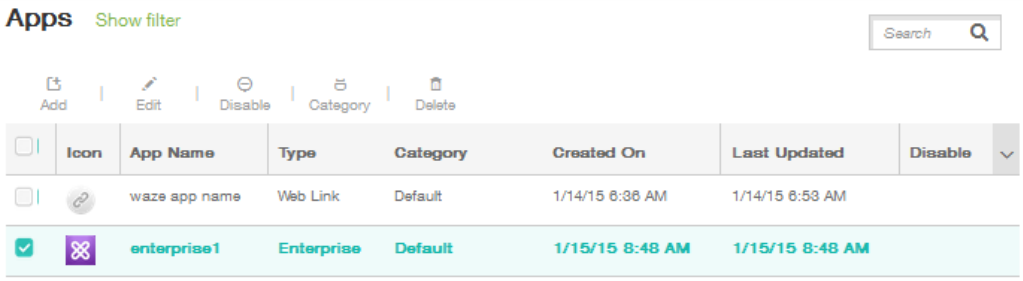


3. Dans la boîte de dialogue Catégories, entrez le nom de la catégorie que vous souhaitez ajouter, puis cliquez sur le signe plus (+). Par exemple, entrez *Applications d'entreprise*, puis cliquez sur le signe plus (+).

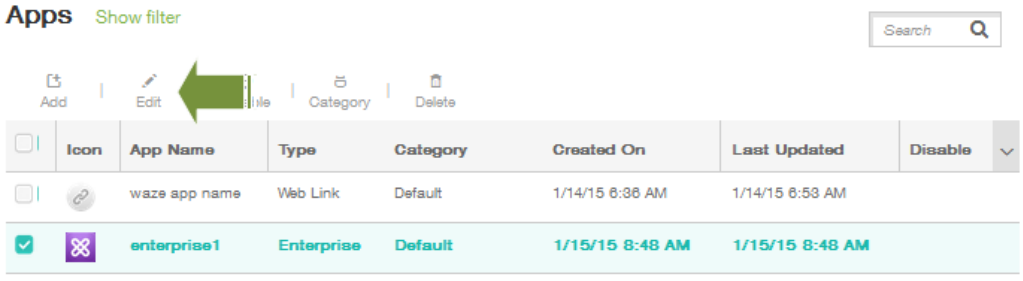


La nouvelle catégorie est ajoutée et s'affiche dans la boîte de dialogue Catégories. Si aucune catégorie n'est configurée, seule la catégorie **par défaut** s'affiche.

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.

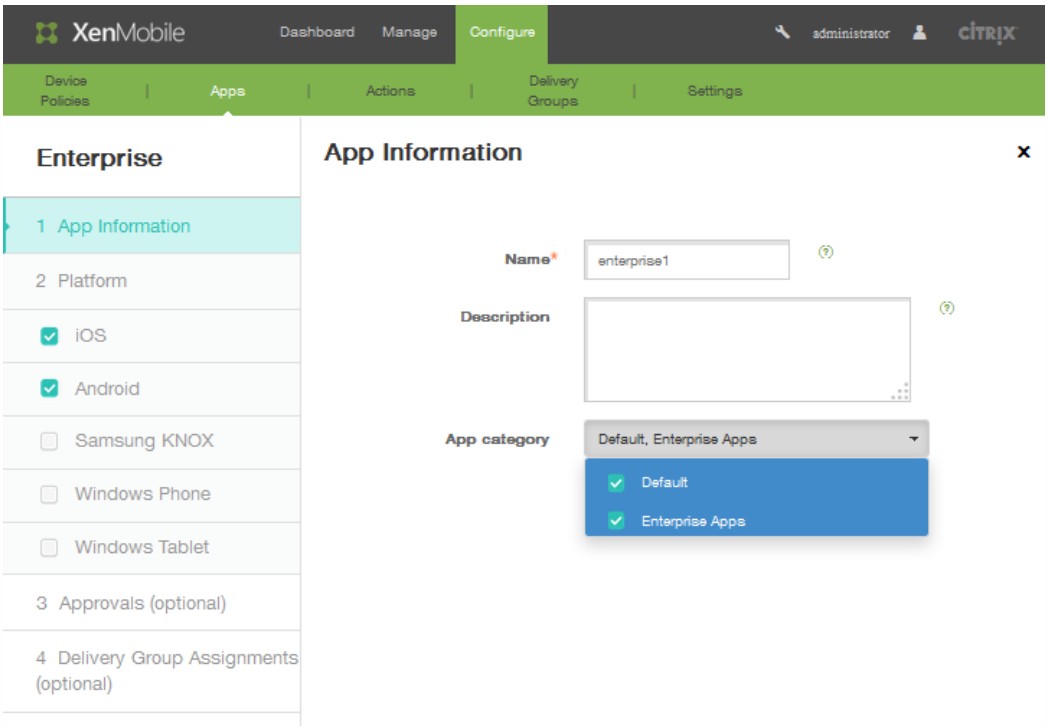


6. Cliquez sur Modifier pour classer l'application.

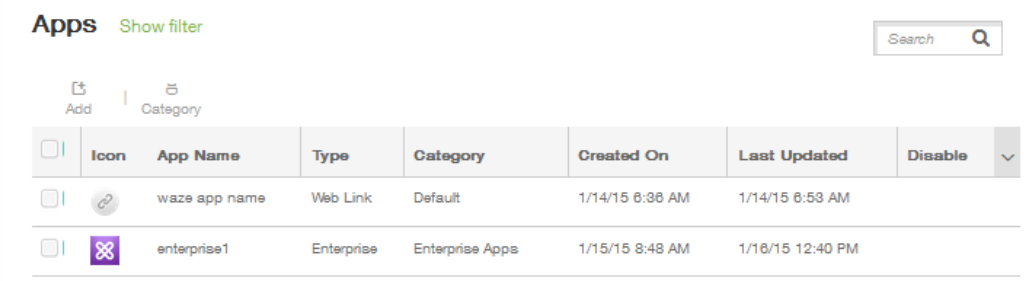


La page Informations sur l'application s'affiche.

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.

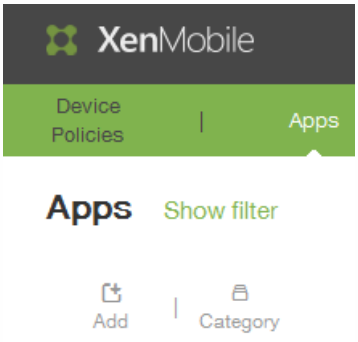


Pour ajouter un magasin d'applications public à XenMobile

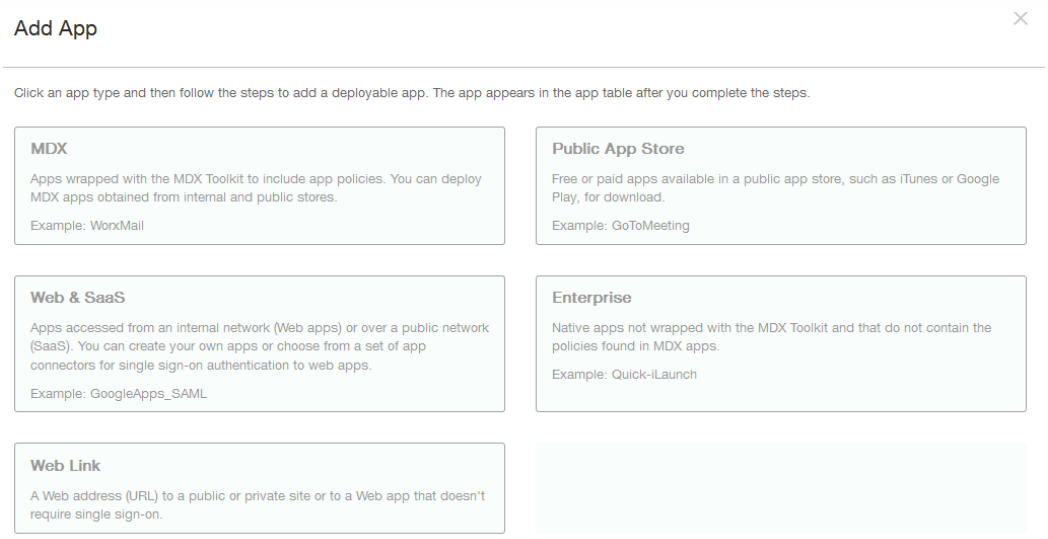
May 06, 2016

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.

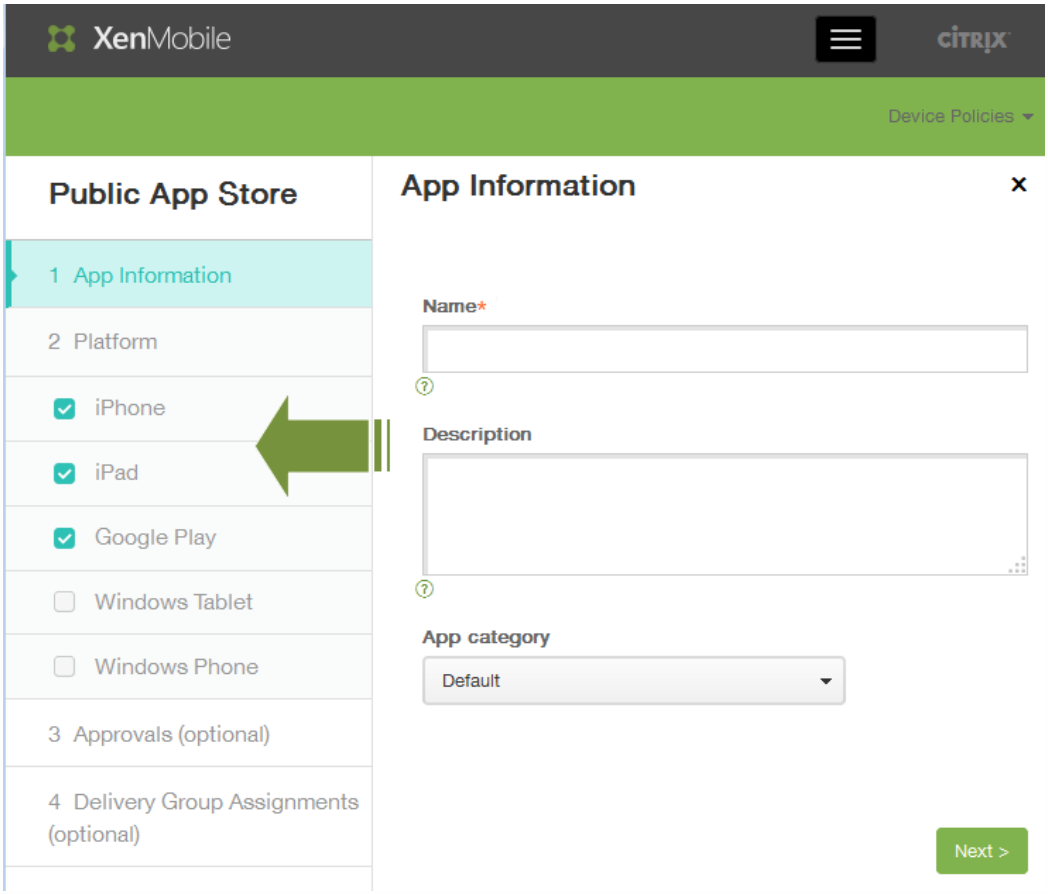
1. Dans la console XenMobile, cliquez sur Configurer > Applications. L'écran Applications s'affiche.



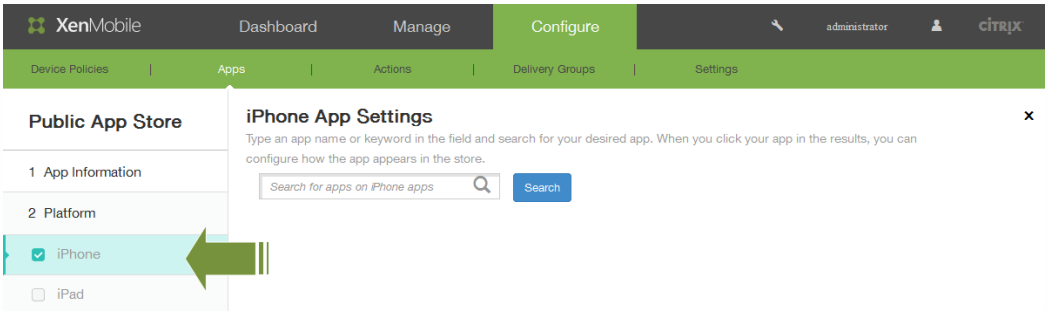
2. Cliquez sur Ajouter.
3. Dans l'écran Ajouter une application, cliquez sur Magasin d'applications public.



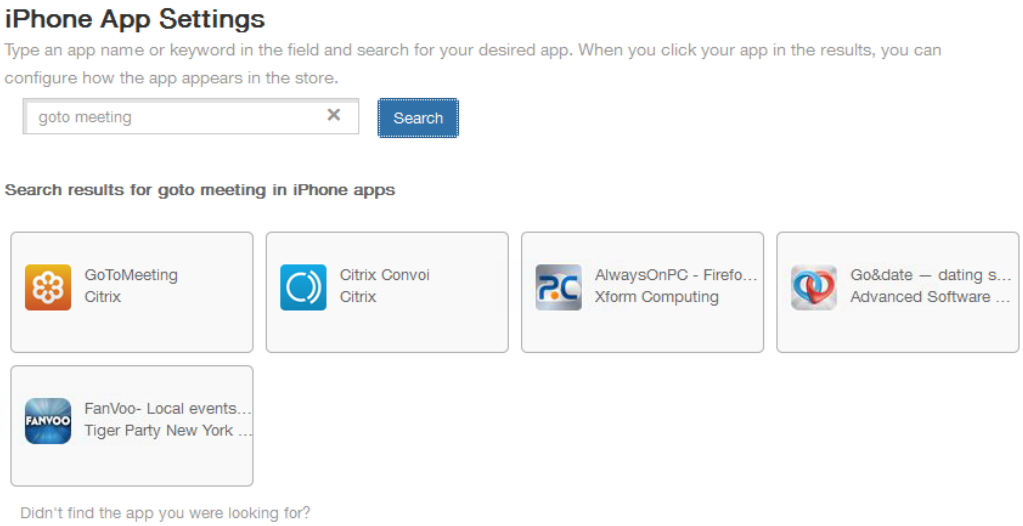
4. Sur la page Informations sur l'application, entrez un nom et une description pour l'application. Ces champs sont utilisés à des fins internes. Si vous ajoutez des applications pour de multiples appareils (par exemple, iPhone, iPad et GooglePlay), utilisez les cases à cocher dans la partie gauche de l'écran pour les sélectionner.



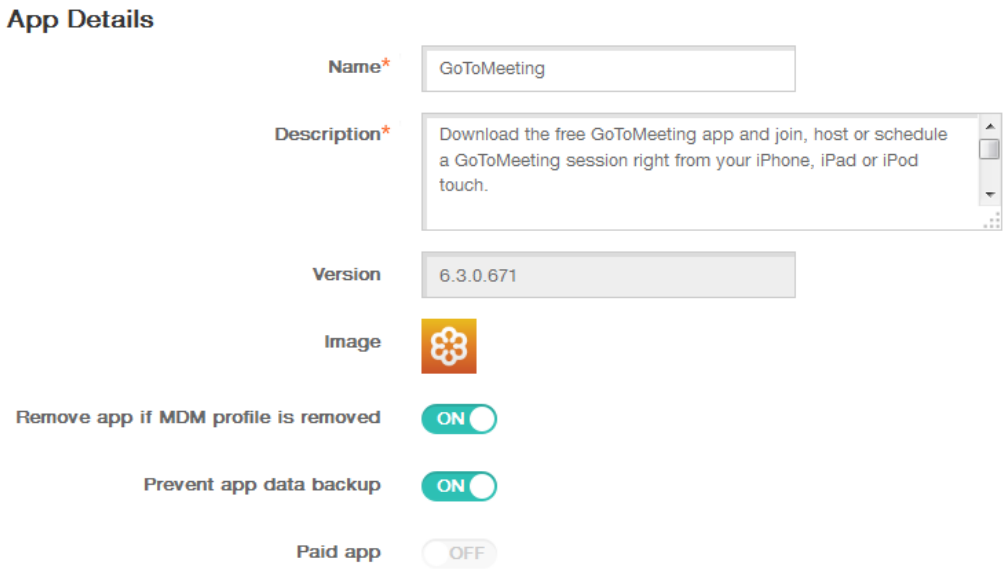
5. Dans la liste Catégorie d'application, cliquez sur Catégorie d'application.
6. Cliquez sur Suivant.
7. Sur l'écran Plate-forme de sélection du type de plate-forme, dans le champ de recherche, tapez le nom d'une application ou un mot clé pour localiser l'application que vous souhaitez ajouter. Par 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).

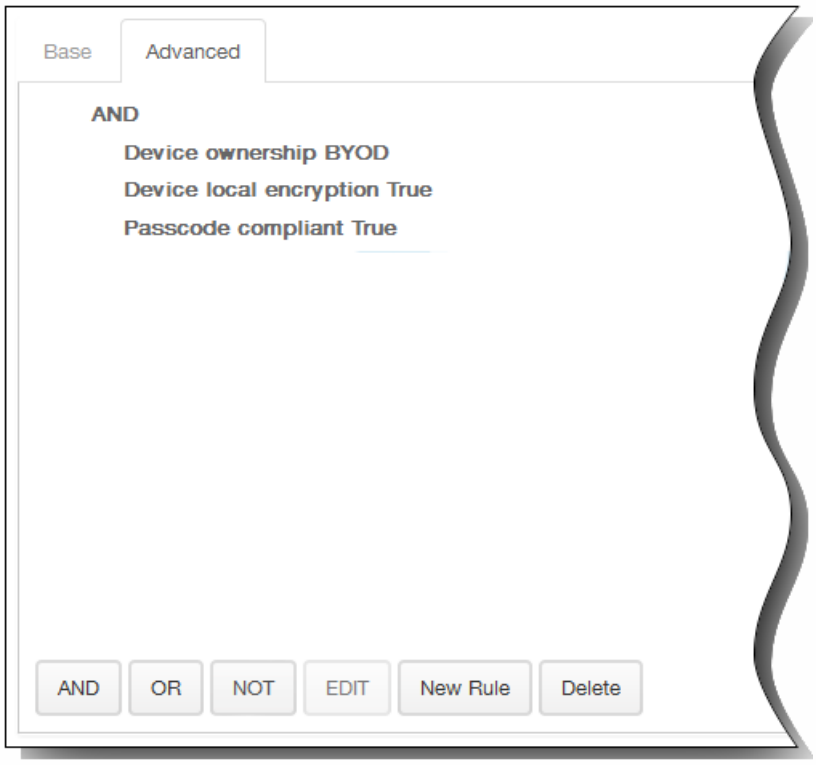


8. Cliquez sur une application dans les résultats pour configurer la manière dont elle s'affiche dans le magasin. Sur l'écran Détails sur l'application, les champs sont préremplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image). Si nécessaire, modifiez le nom et la description de l'application.



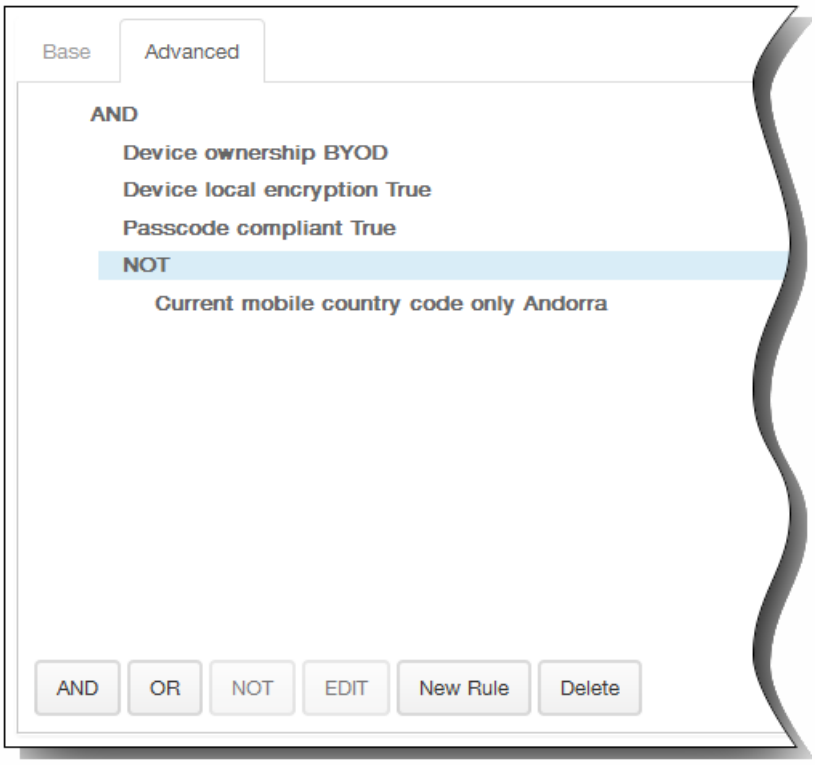
   1. Dans Supprimer l'application si le profil MDM est supprimé, cliquez sur ON pour supprimer l'application lorsque le profil MDM est supprimé. Par défaut, cette option est réglée sur ON.
   2. Dans Empêcher la sauvegarde des données d'application, cliquez sur ON pour empêcher l'application de sauvegarder 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.

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.

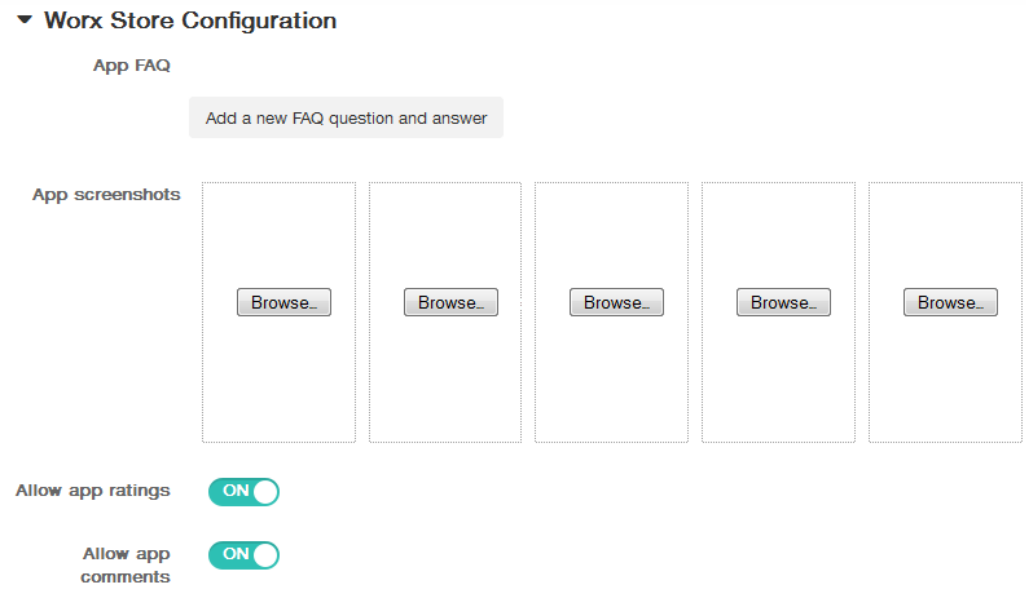


   Les conditions que vous avez choisies sur l'onglet Base s'affichent.
3. Vous pouvez utiliser une logique booléenne plus avancée pour combiner, modifier ou ajouter des règles.
   1. Cliquez sur ET, OU ou SAUF.
   2. Dans la liste qui s'affiche, sélectionnez les conditions que vous voulez ajouter à la 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.



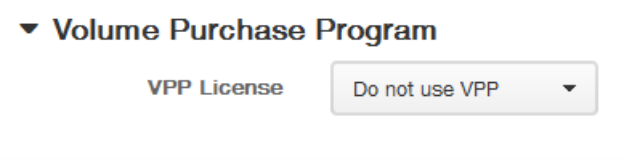
10. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



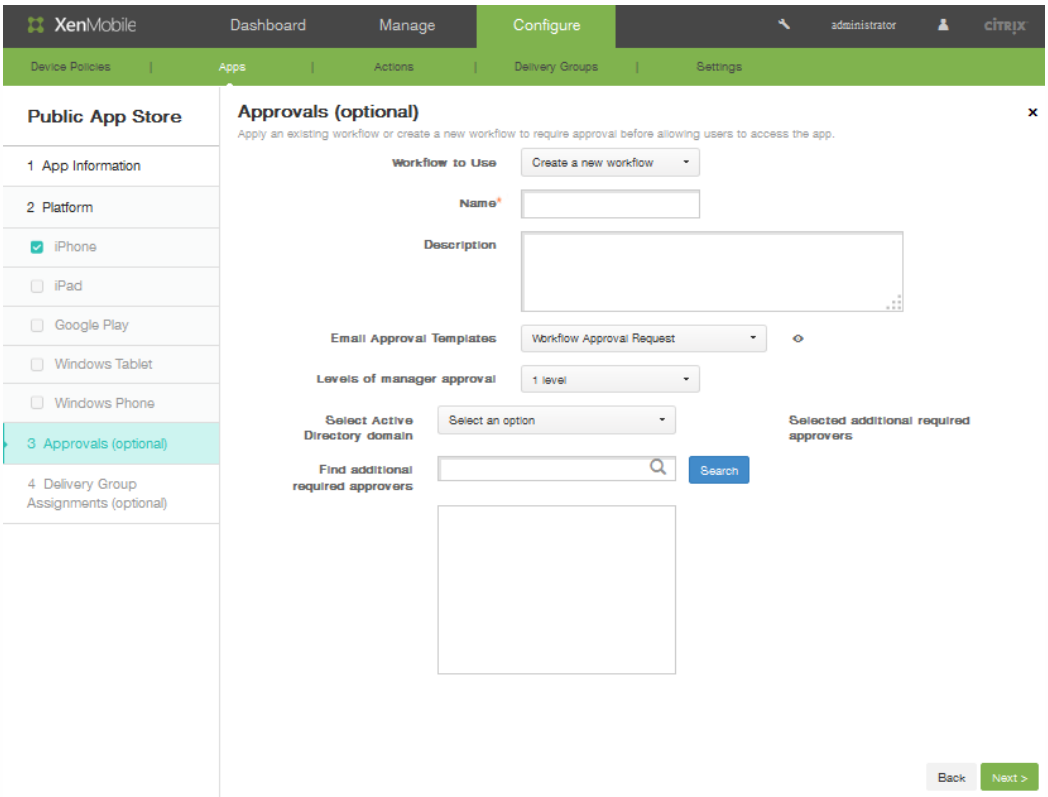
   Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.
11. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des

commentaires sur l'application sélectionnée.

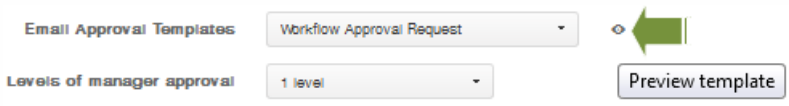
12. Développez Programme d'achat en volume, puis dans la liste Licences VPP, cliquez sur Charger un fichier de licences VPP si vous voulez autoriser XenMobile à appliquer une licence VPP pour l'application.



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.

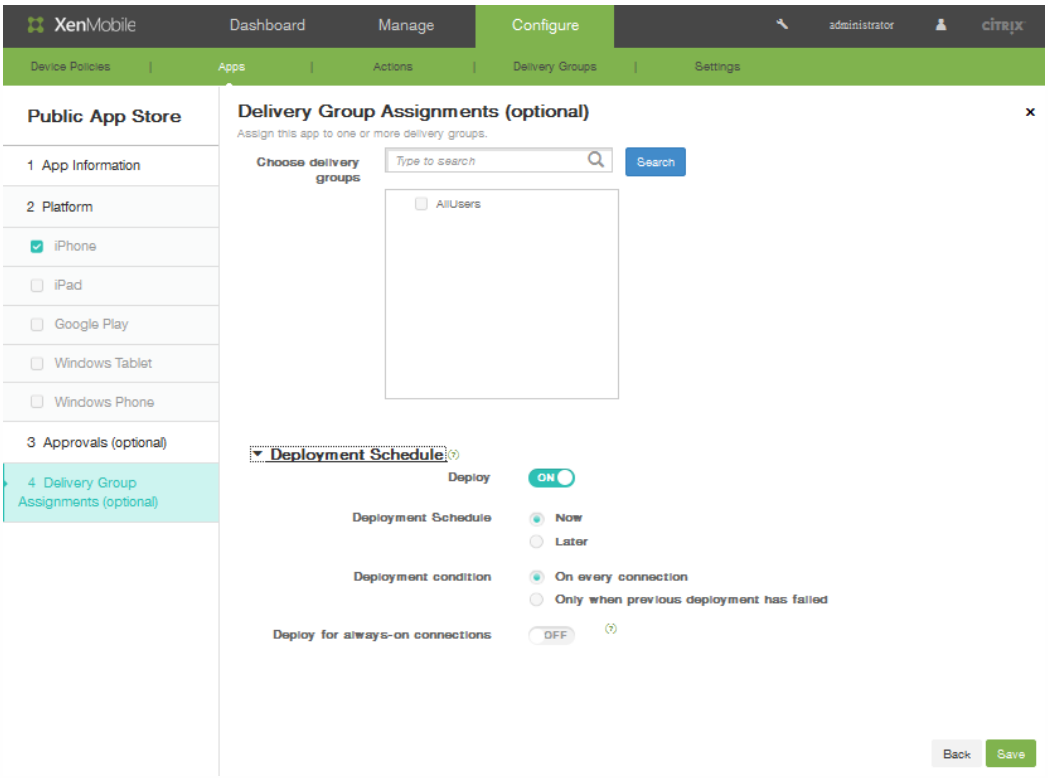


15. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur. Le fichier VPP chargé s'applique uniquement à l'ancien Programme d'achat en volume d'Apple. Pour le nouveau programme, la gestion des licences est basée sur les licences achetées par la société. Cette information est configurée dans **Paramètres > VPP iOS**.
    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.

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 Save. La console XenMobile applique les informations d'application.

Pour ajouter une application Web et SaaS à XenMobile

May 06, 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.

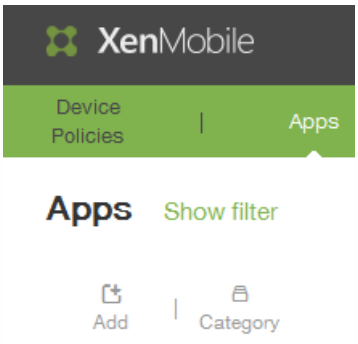
Pour configurer un connecteur, spécifiez les paramètres suivants :

- 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.

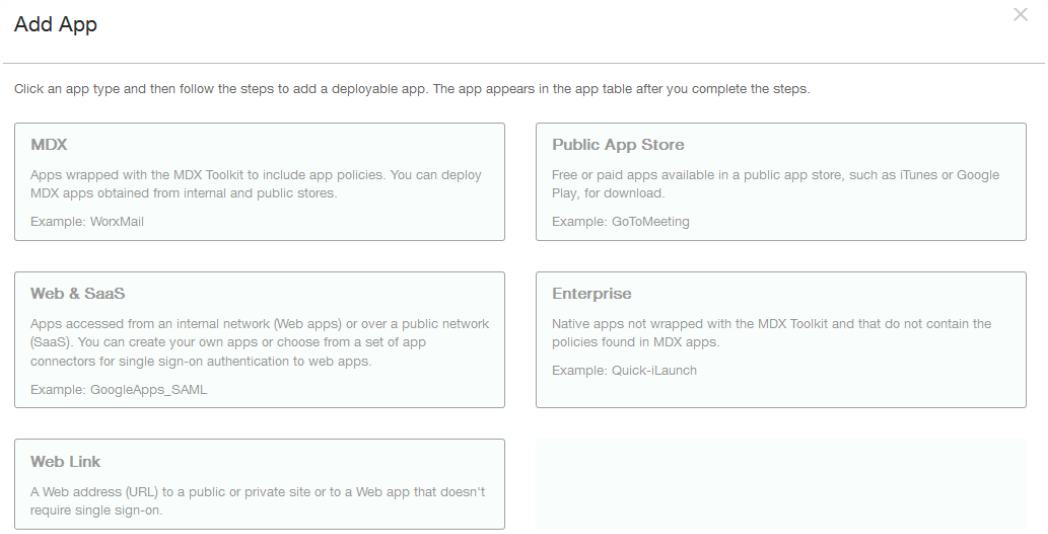
Si une application est uniquement disponible en authentification unique, enregistrez les paramètres lorsque vous terminez la configuration des paramètres précédents ; l'application s'affiche alors dans l'onglet Applications de la console XenMobile.

Pour ajouter un connecteur d'applications dans XenMobile

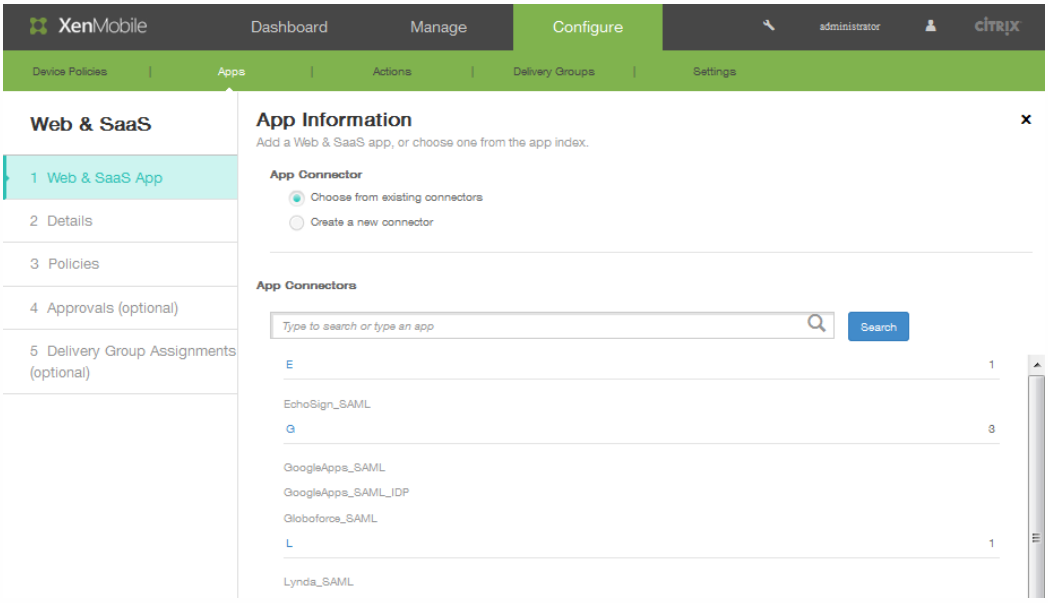
1. Dans la console Web XenMobile, cliquez sur Configurer > Applications. La page Applications s'ouvre.
2. Sur la page Applications, cliquez sur **Ajouter**.



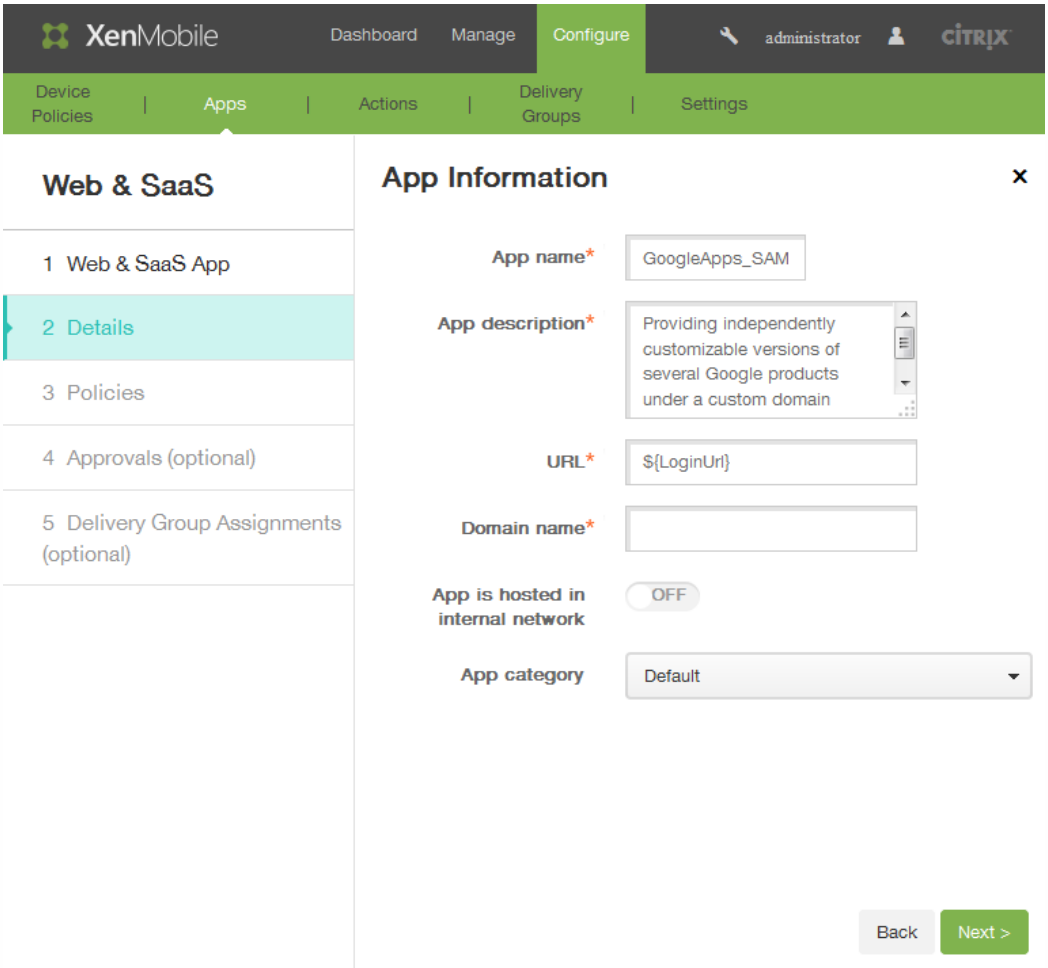
3. Sur la page **Ajouter une application**, cliquez sur **Web et SaaS**.



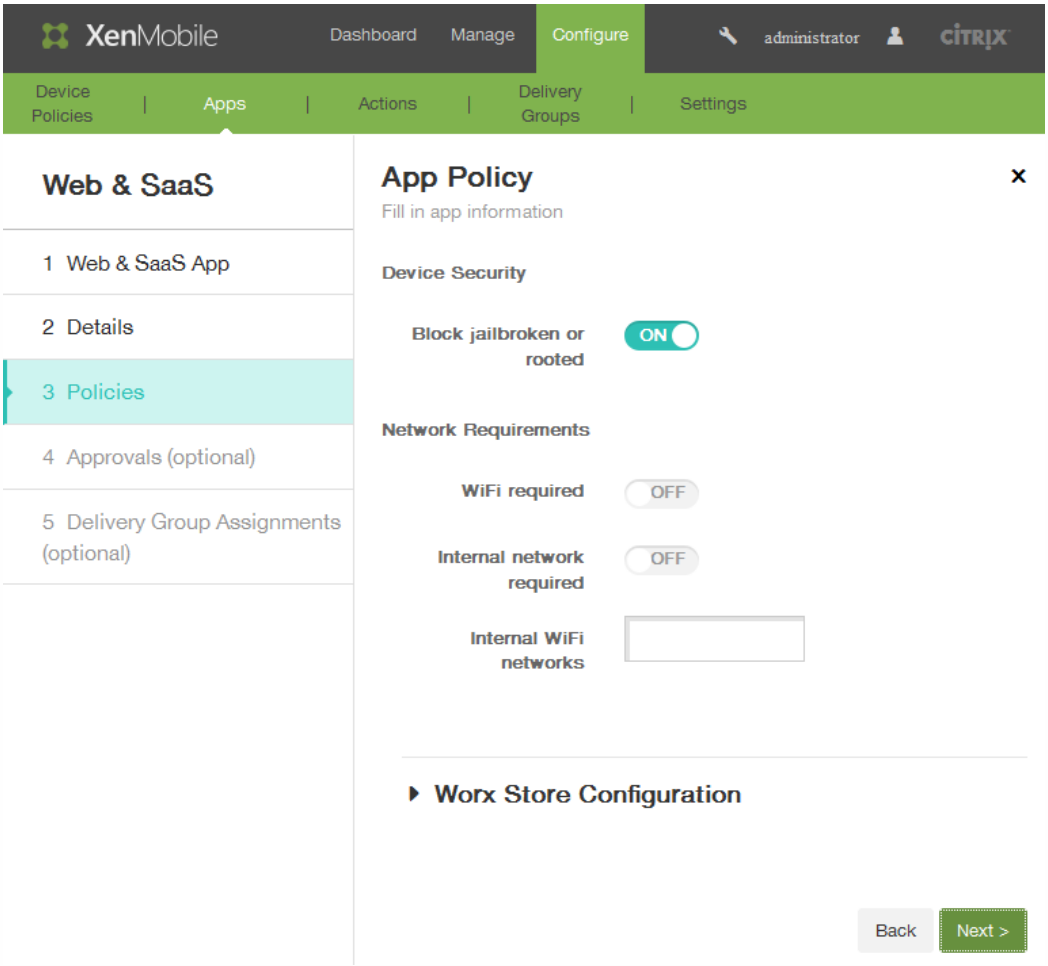
4. Sur la page Informations sur l'application, cliquez sur Choisir parmi les connecteurs existants ou Créer un nouveau connecteur.



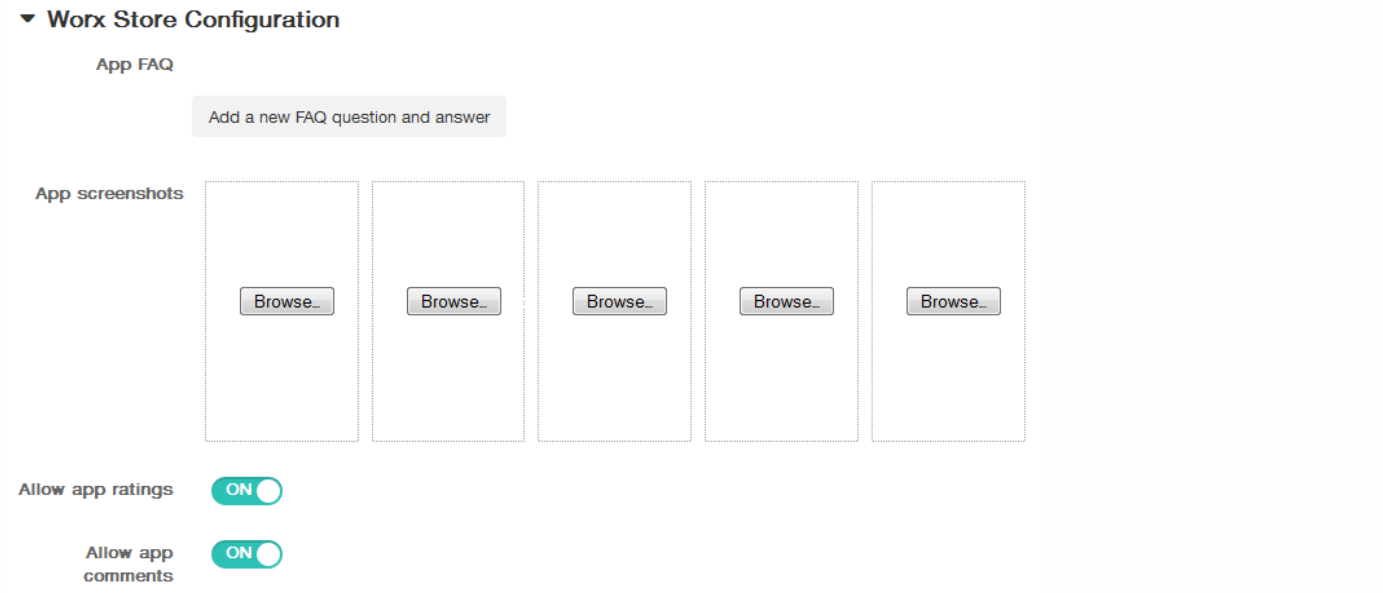
5. Si vous cliquez sur une application dans la liste, la page Détails s'ouvre. Les champs Nom app, Description et URL sont pré-remplis.



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 Next. La page Stratégies s'affiche.

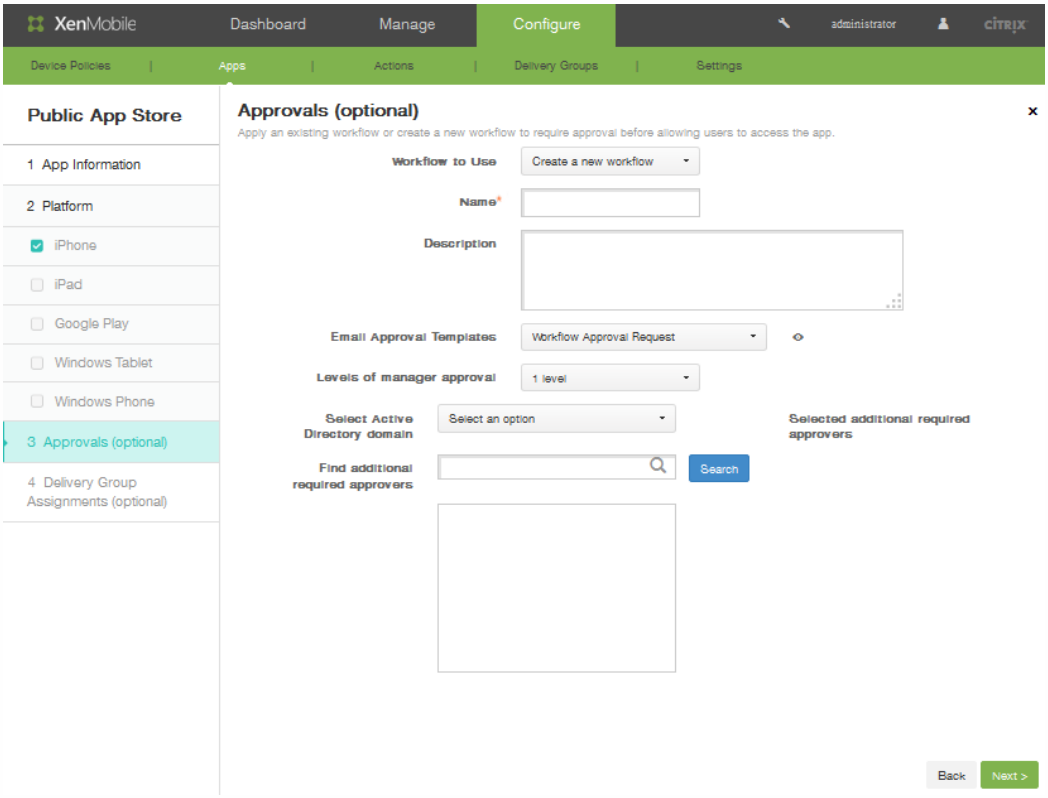


7. Dans Sécurité de l'appareil, dans Bloquer les appareils jailbreakés ou rootés, cliquez sur ON.
8. Dans Exigences du réseau, configurez les paramètres suivants :
   1. Dans Wi-Fi requis, cliquez sur Activé, puis spécifiez des réseaux Wi-Fi internes.
   2. Dans Réseau interne requis, cliquez sur ON 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.



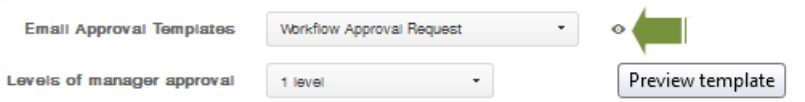
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

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 Next.
12. Sur la page Approbations, dans la liste Workflow à utiliser, cliquez sur un workflow ou sur Créer un nouveau workflow.



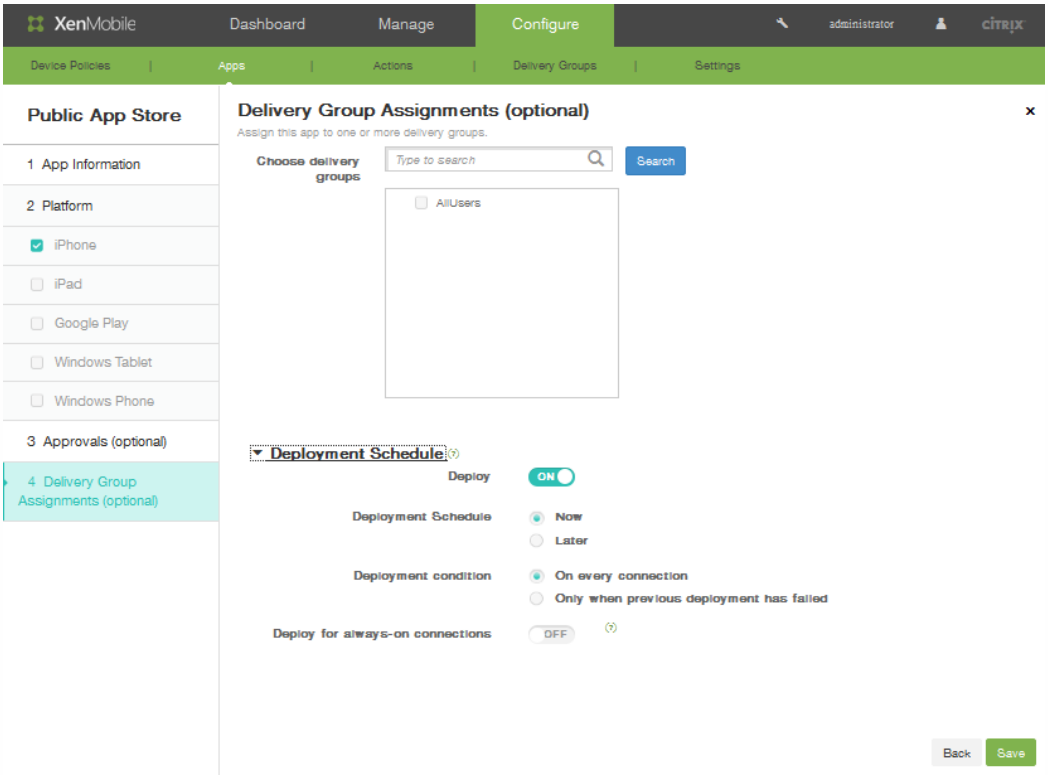
13. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur.
    1. Spécifiez 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.

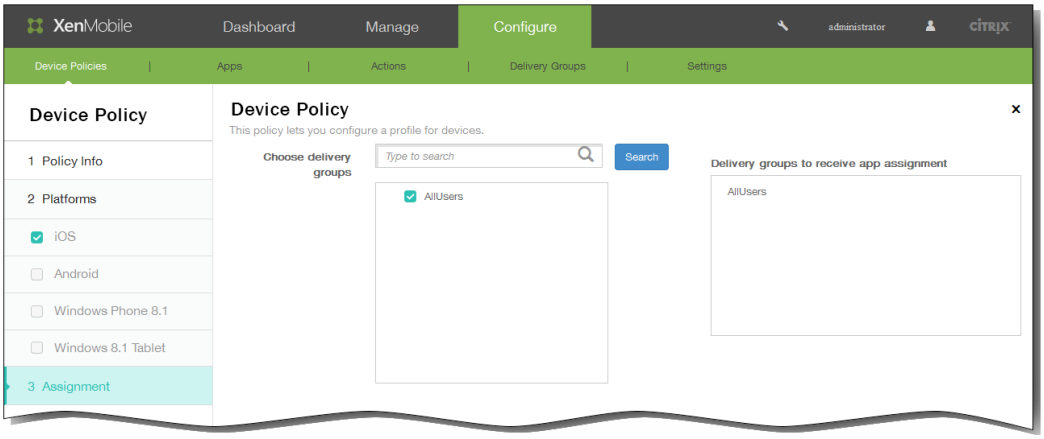


4. Dans **Niveaux d'approbation par un responsable**, cliquez sur le niveau approprié ; les valeurs disponibles vont de Aucun à 3.
5. Dans **Sélectionner un domaine Active Directory**, cliquez sur le domaine.
6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

14. Cliquez sur Next.
15. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez l'application à un ou plusieurs groupes de mise à disposition.

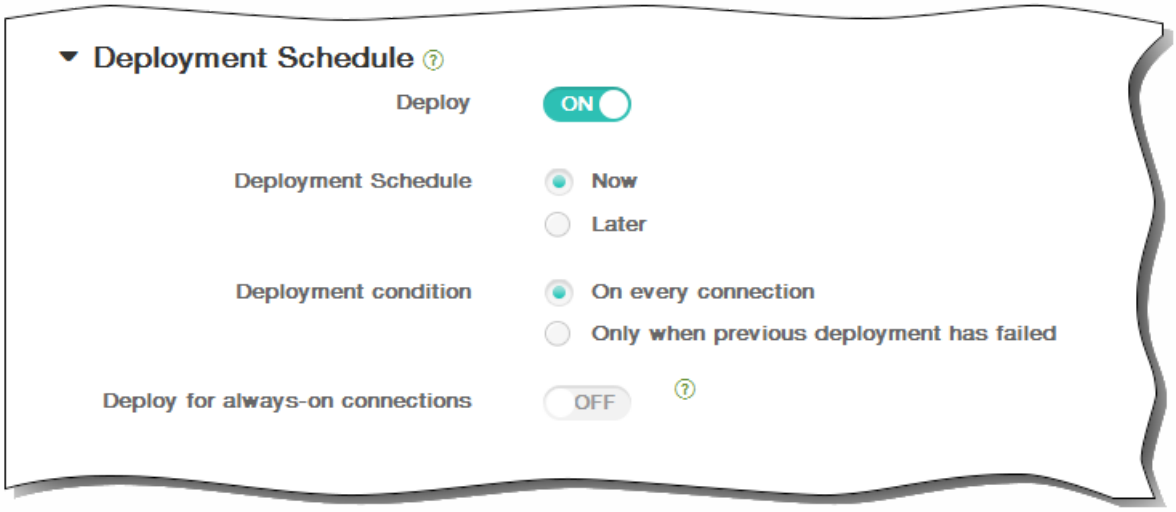


16. En regard de Choisir des groupes de mise à disposition, tapez pour trouver un groupe de mise à disposition ou sélectionnez un ou plusieurs groupes dans la liste auxquels vous souhaitez attribuer la stratégie. Les groupes que vous sélectionnez s'affichent dans liste de droite Groupes de mise à disposition qui vont recevoir l'attribution d'applications.



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**.

Liste des types de connecteur d'applications

May 06, 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

Pour ajouter une application d'entreprise à XenMobile

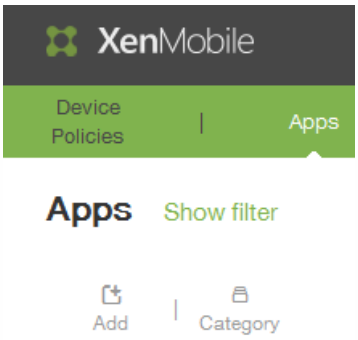
May 06, 2016

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) :

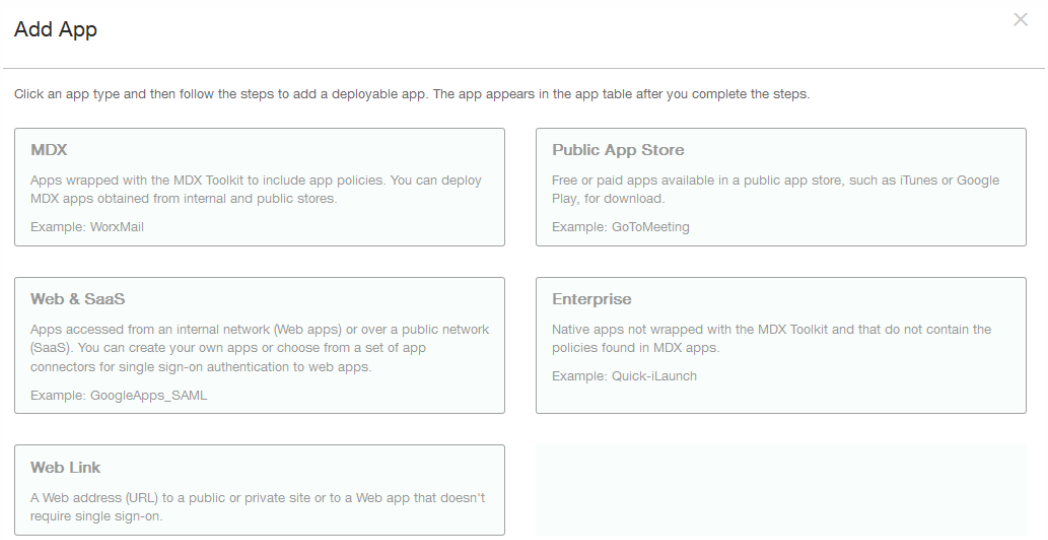
- iOS (fichier .ipa)
- Android (fichier .apk)
- Samsung KNOX (fichier .apk)
- Windows Phone (fichier .xap ou .appx)
- Windows Tablet (fichier .appx)

Pour créer une application d'entreprise

1. Dans la console XenMobile, cliquez sur Configurer > Applications.
2. Sur la page Applications, cliquez sur **Ajouter**.

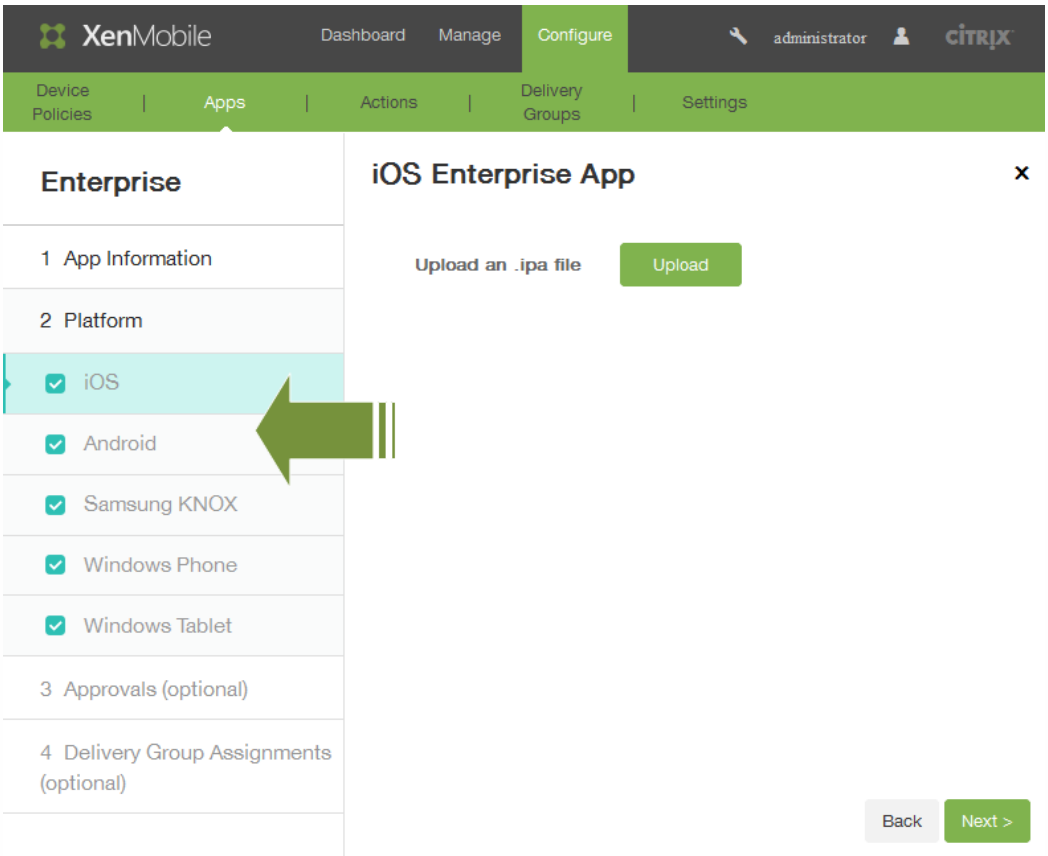


3. Sur la page Ajouter une application, cliquez sur **Entreprise**.

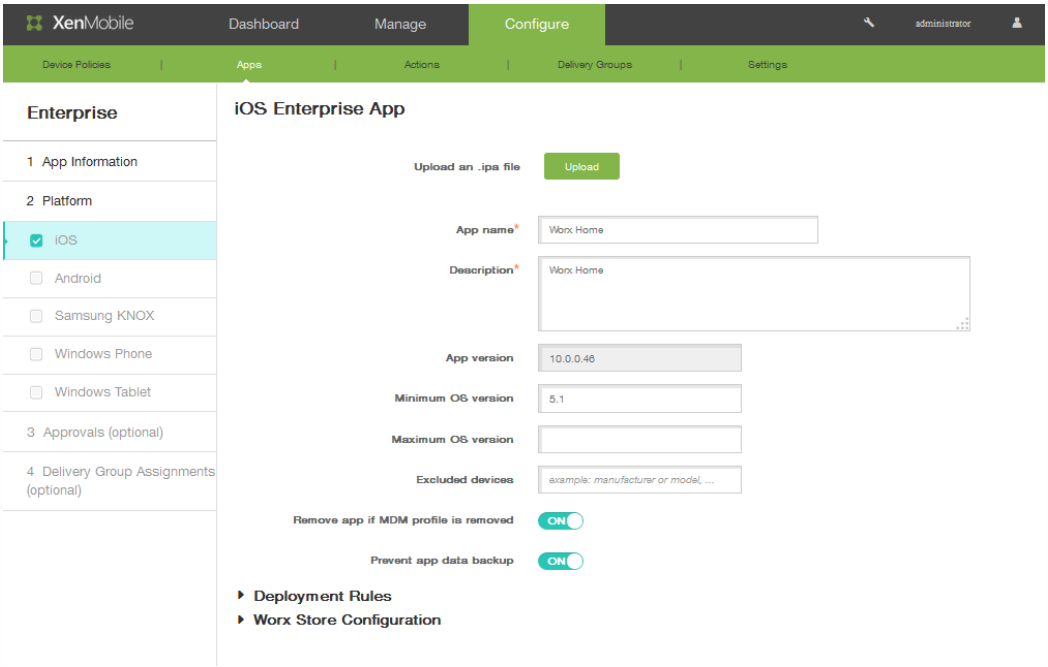


4. Dans le catalogue, cliquez sur Nouvelle application d'entreprise.

5. 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.
      Remarque : si vous souhaitez configurer une deuxième application avec la même adresse Web, vous devez donner un autre nom à l'application.
   3. Dans **Catégorie d'application**, cliquez sur une catégorie, puis sur Suivant.
6. 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).

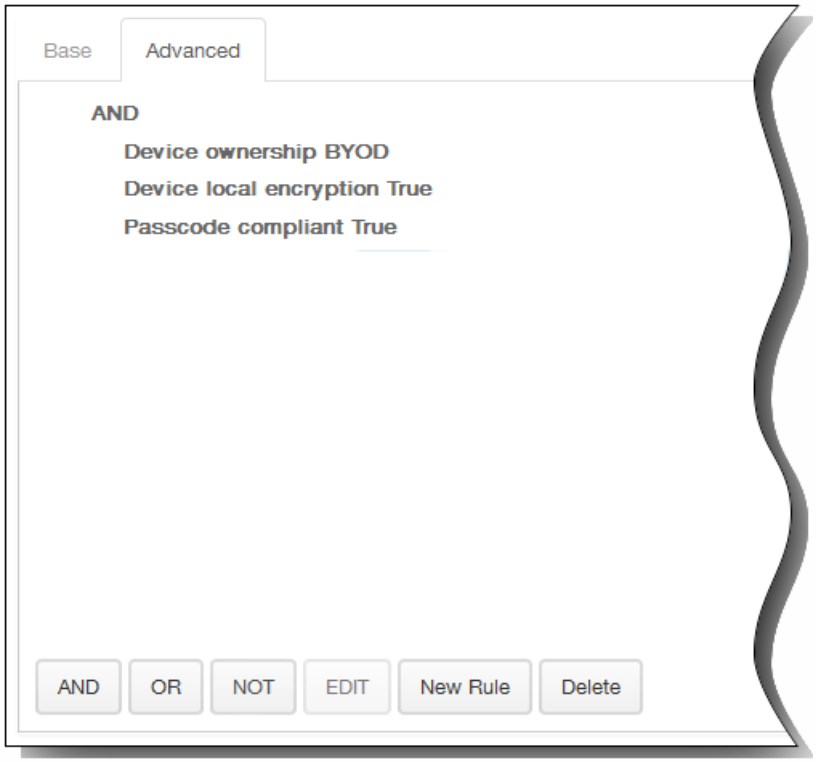


7. Cliquez sur Charger pour accéder à l'emplacement du fichier, puis cliquez sur Suivant. La page d'informations sur l'application s'affiche pour le type de plate-forme. Les champs sont pré-remplis avec les informations relatives à l'application choisie (y compris le nom, la description, le numéro de version et l'image). Si nécessaire, modifiez le nom et la description de l'application.



8. 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.
9. 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.
10. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.

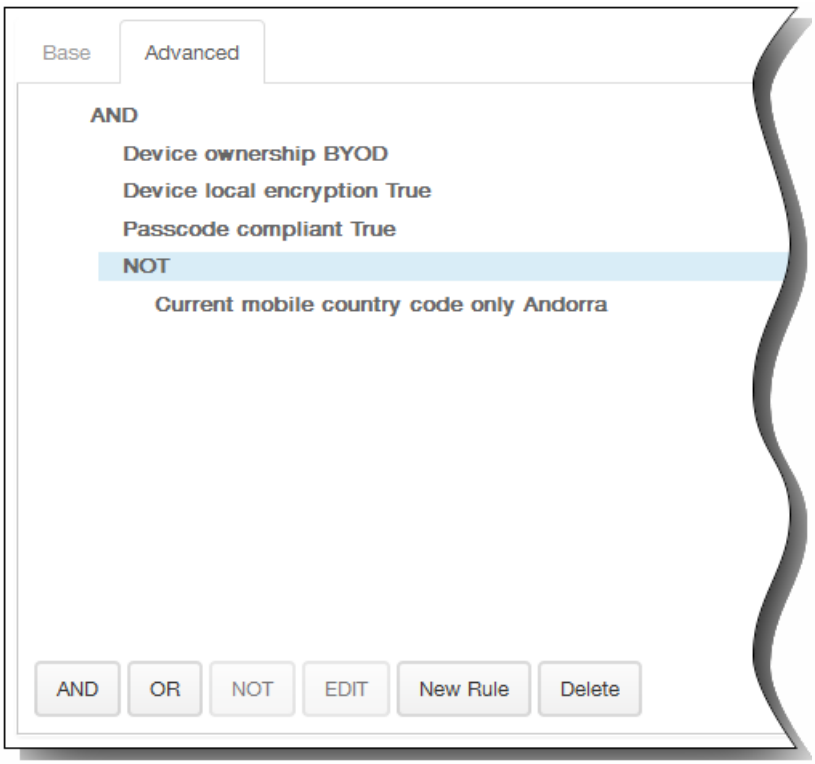
1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



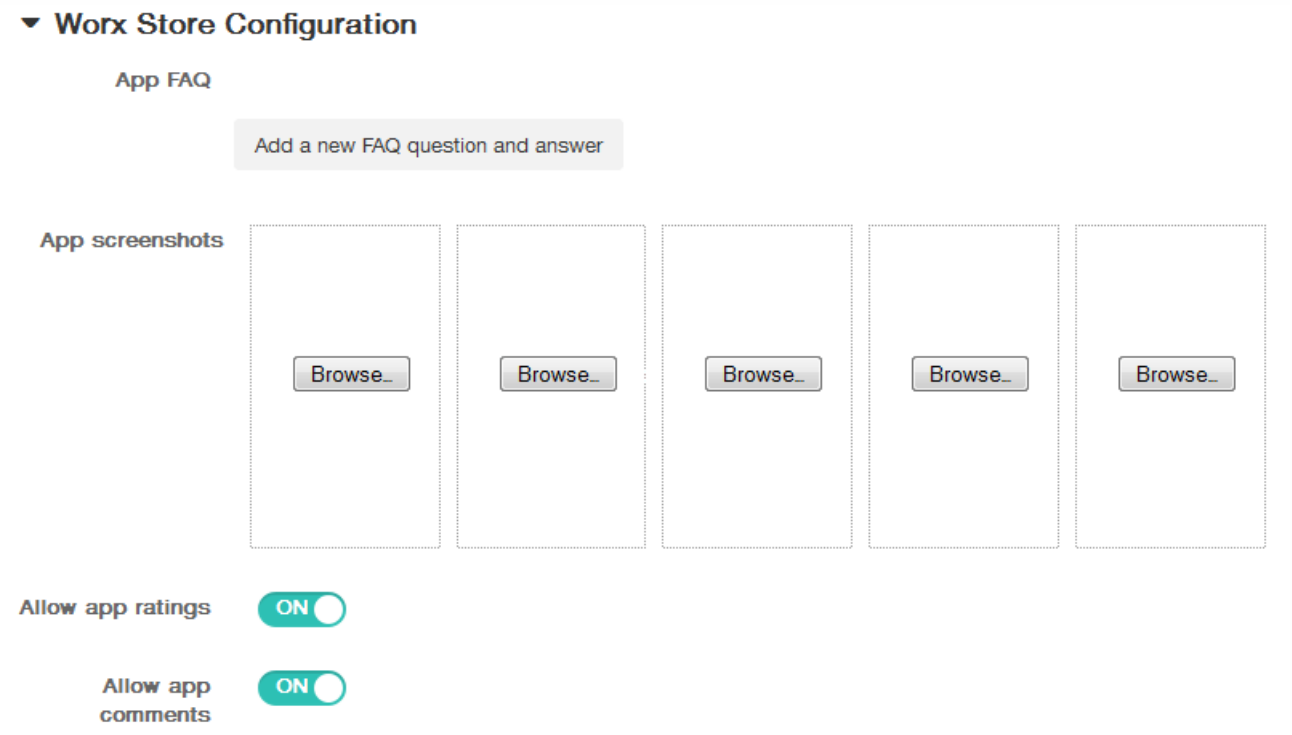
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



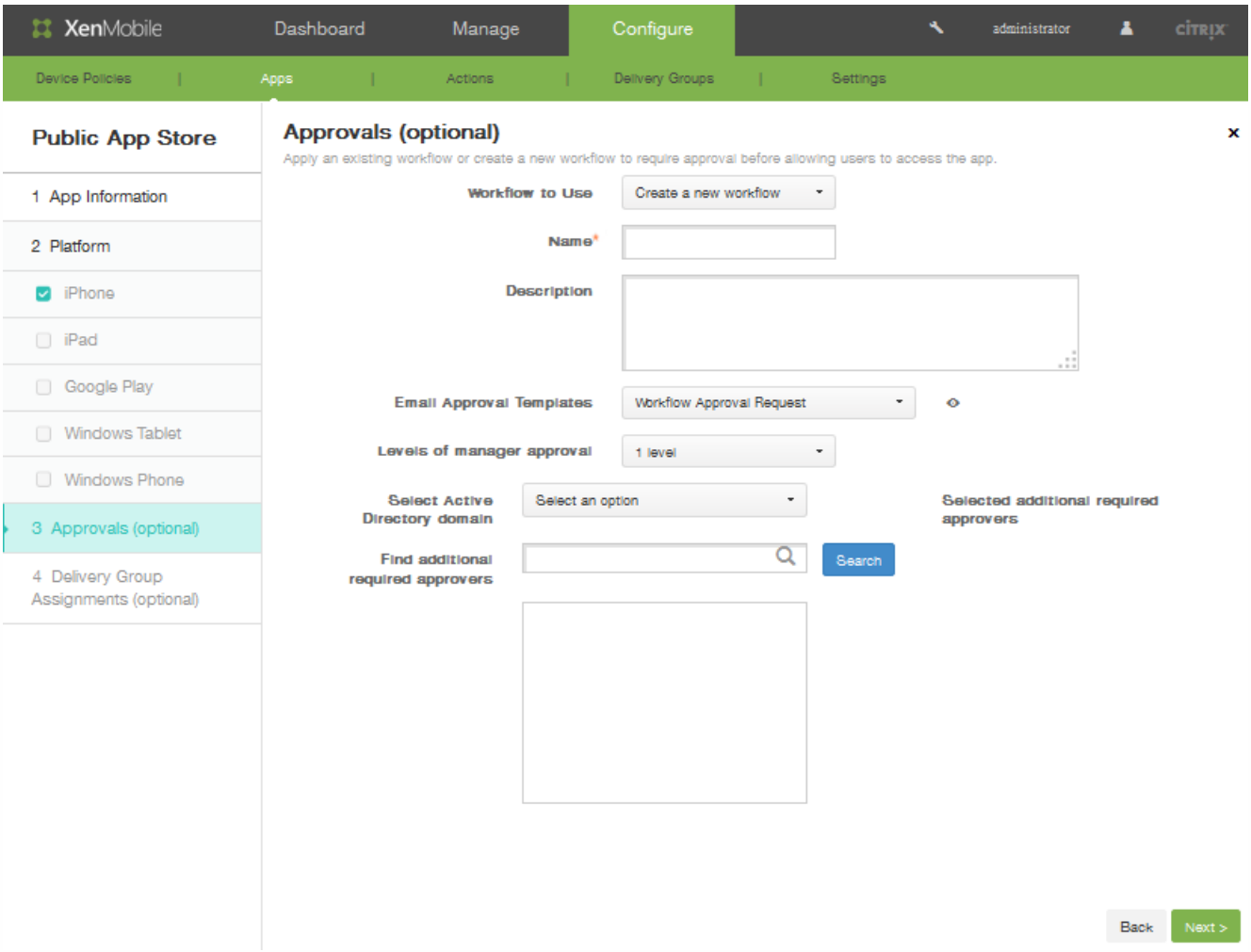
11. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.



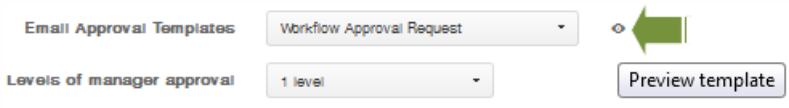
Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

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 Next.
14. Sur la page Approbations, dans la liste Workflow à utiliser, cliquez sur un workflow ou sur Créer un nouveau workflow.



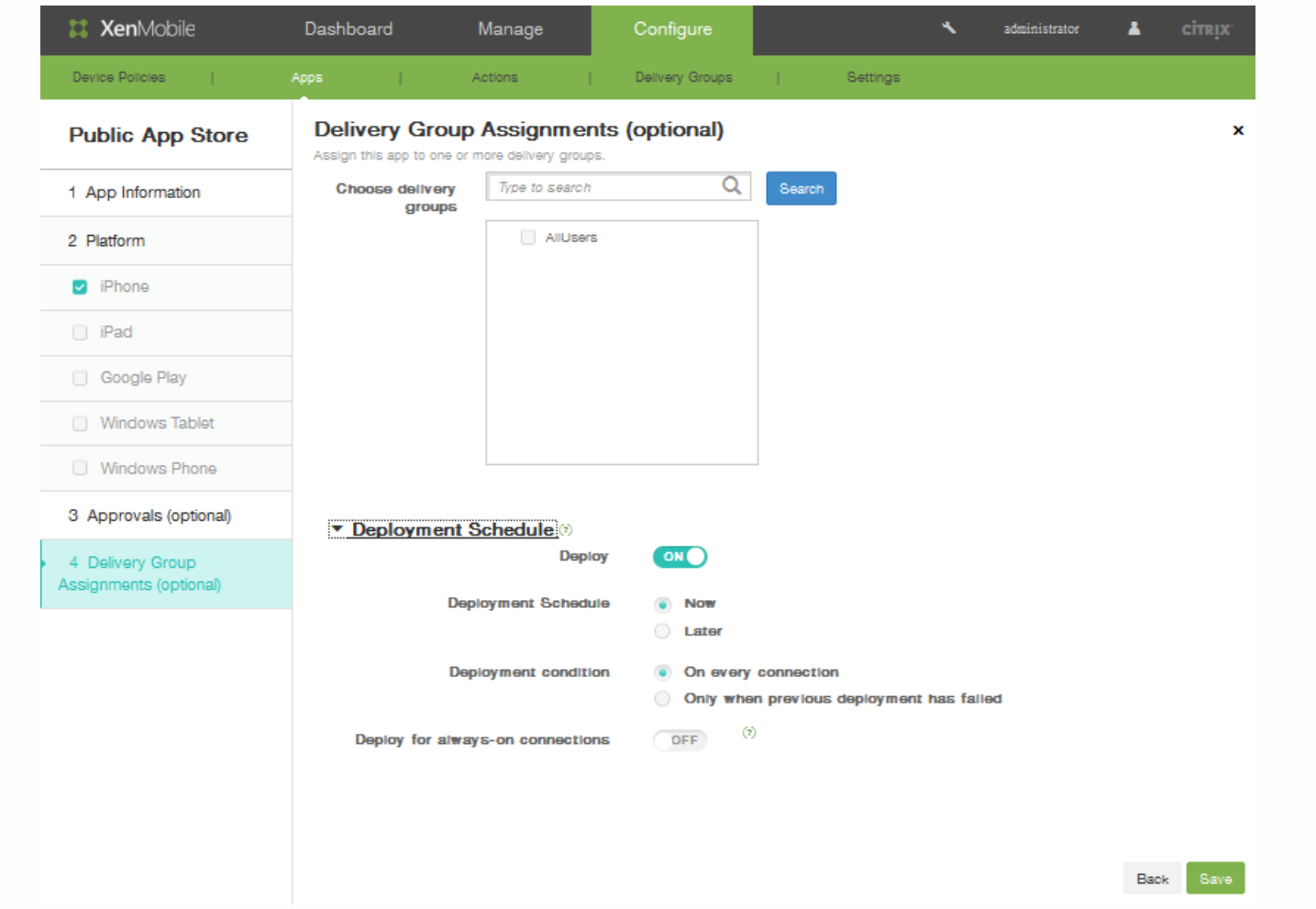
15. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer un compte d'utilisateur.
    1. Spécifiez 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) :

6. (Facultatif) Dans Rechercher des approbateurs supplémentaires requis, entrez les approbateurs supplémentaires requis, puis cliquez sur Rechercher.

16. (Facultatif) Sur la page **Attribution de groupes de mise à disposition**, attribuez l'application à un ou plusieurs groupes de mise à disposition.



17. 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.
18. 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.

19. Cliquez sur Enregistrer.

Pour ajouter un lien Web applicatif à XenMobile

May 06, 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).

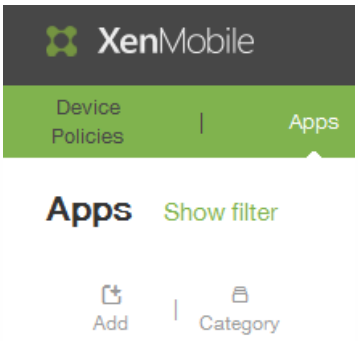
Vous pouvez configurer des liens Web dans l'onglet Applications de la console XenMobile. Une fois que vous avez terminé de configurer le lien Web, celui-ci s'affiche sous forme d'icône dans le tableau répertoriant les applications. Lorsque les utilisateurs ouvrent une session avec Worx Home, le lien s'affiche avec la liste des applications et bureaux disponibles.

Pour ajouter le lien, vous devez fournir les informations suivantes :

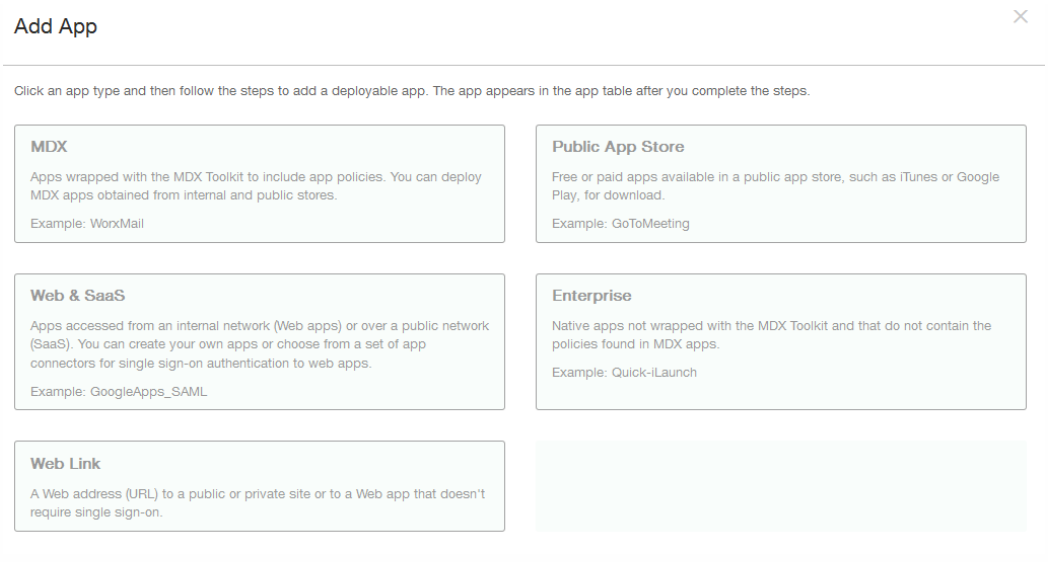
- Nom du lien
- Description du lien
- Adresse Web (URL)
- Catégorie
- Rôle
- Image au format .png (facultatif)

Pour ajouter un lien Web dans XenMobile

1. Configurer > Applications. La page Applications s'ouvre.
2. Sur la page Applications, cliquez sur Ajouter.

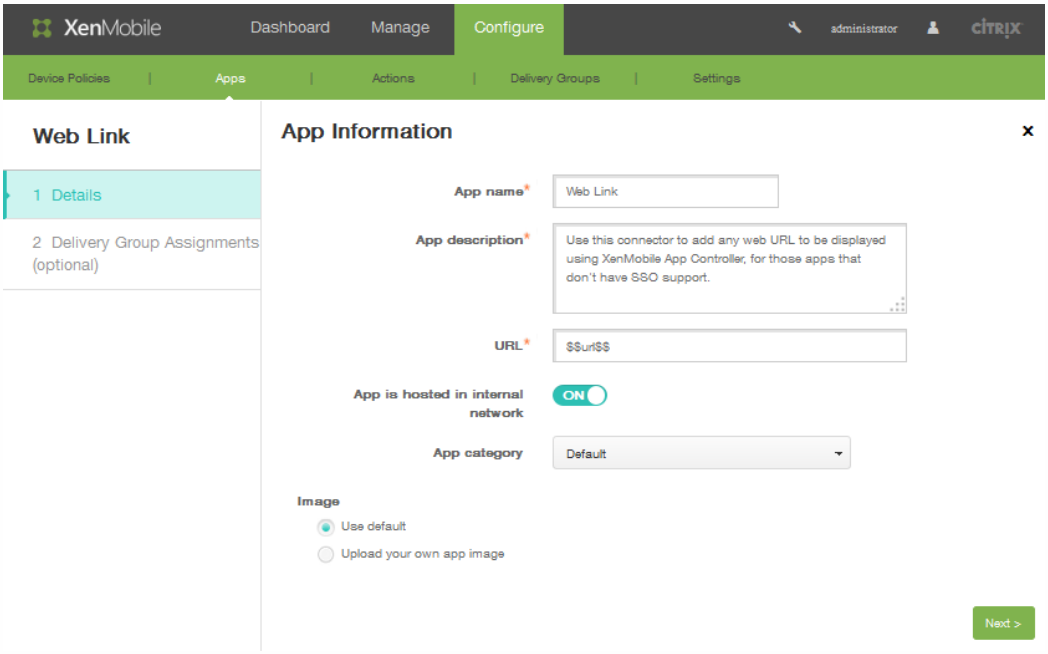


3. Sur la page Ajouter une application, cliquez sur Lien Web.

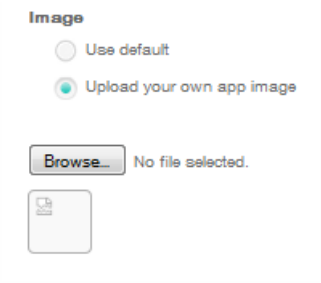


La page Informations sur l'application s'affiche.

4. Les champs Nom app, Description et URL sont pré-remplis.

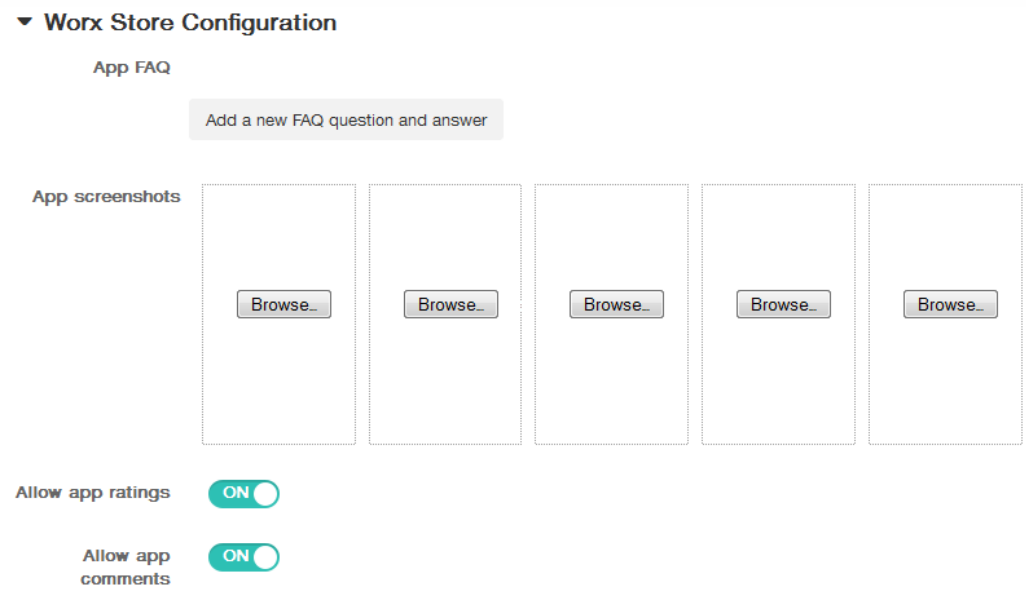


1. Le cas échéant, dans le champ URL, entrez l'adresse Web de l'application ou conservez l'adresse par défaut.
2. Sélectionnez L'application est hébergée dans le réseau interne et cliquez sur ON si l'application est exécutée sur un serveur de votre réseau interne. Si les utilisateurs se connectent à 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 :



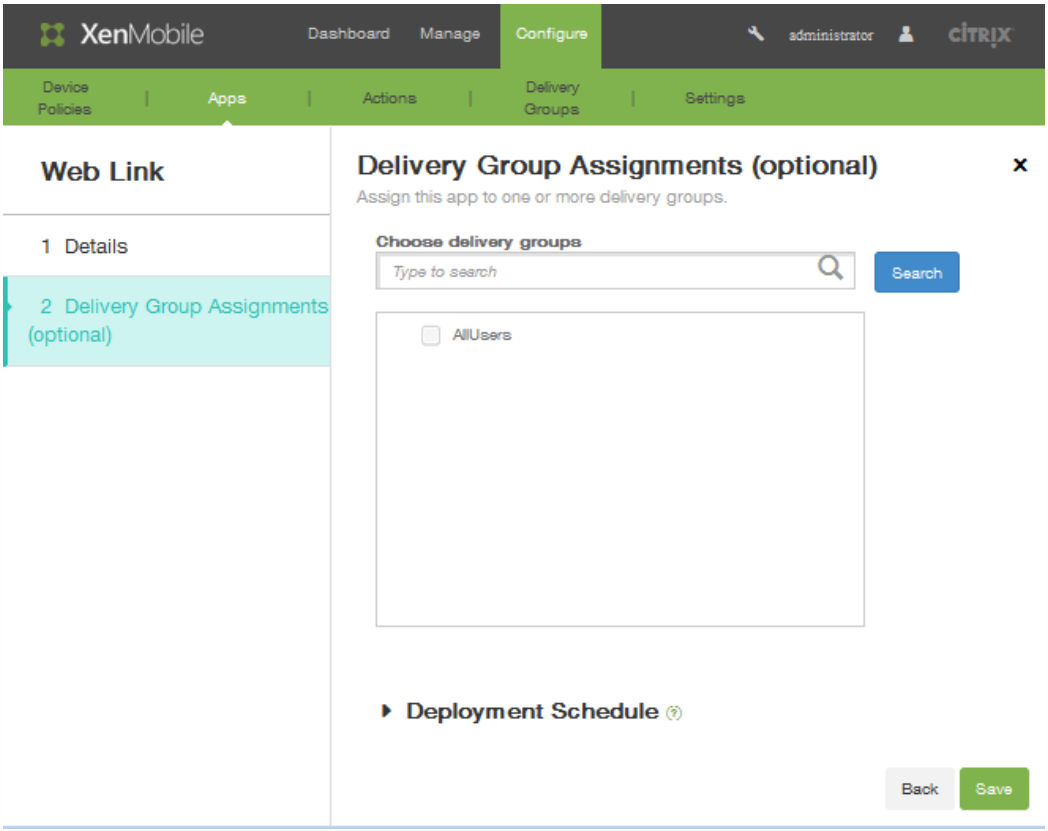
Les images doit être de type PNG.

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.

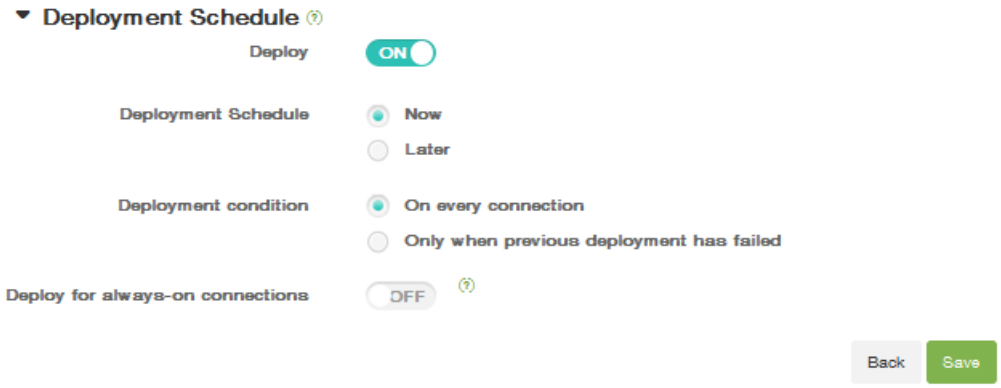


Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

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.



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 Save.

Création et gestion de workflows

May 06, 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.

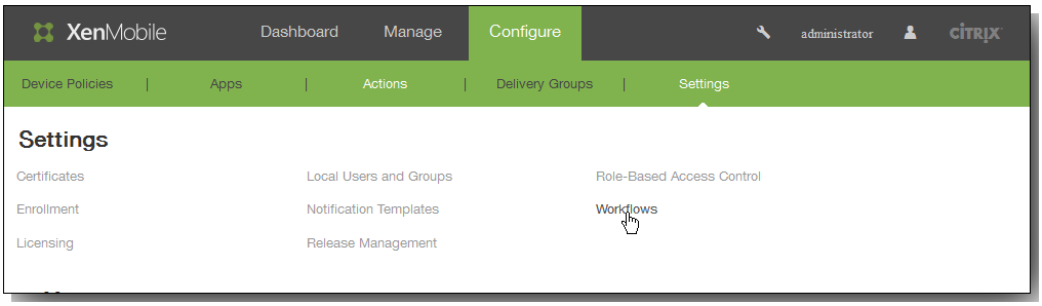
Lorsque vous configurez XenMobile pour la première fois, vous configurez les paramètres de messagerie de workflow. Il est indispensable de configurer les paramètres de messagerie de workflow pour utiliser les workflows. Vous pouvez modifier les paramètres de messagerie de workflow à tout moment. Ces 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.

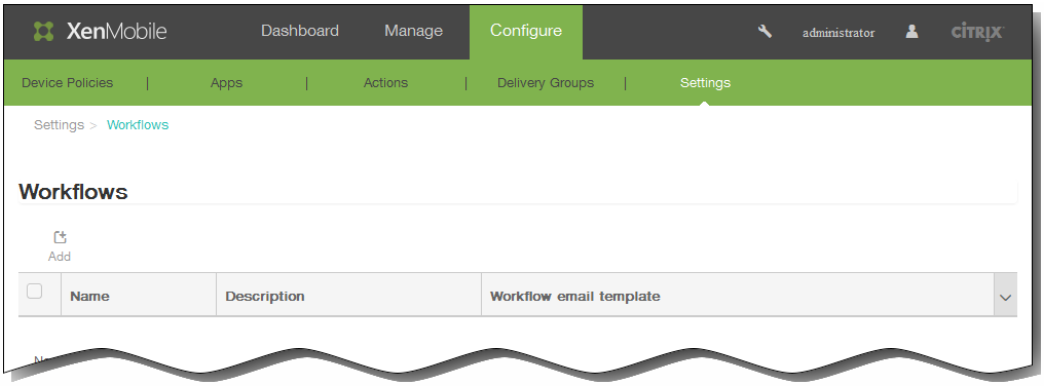
Vous pouvez configurer des workflows à deux emplacements dans XenMobile :

- 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.

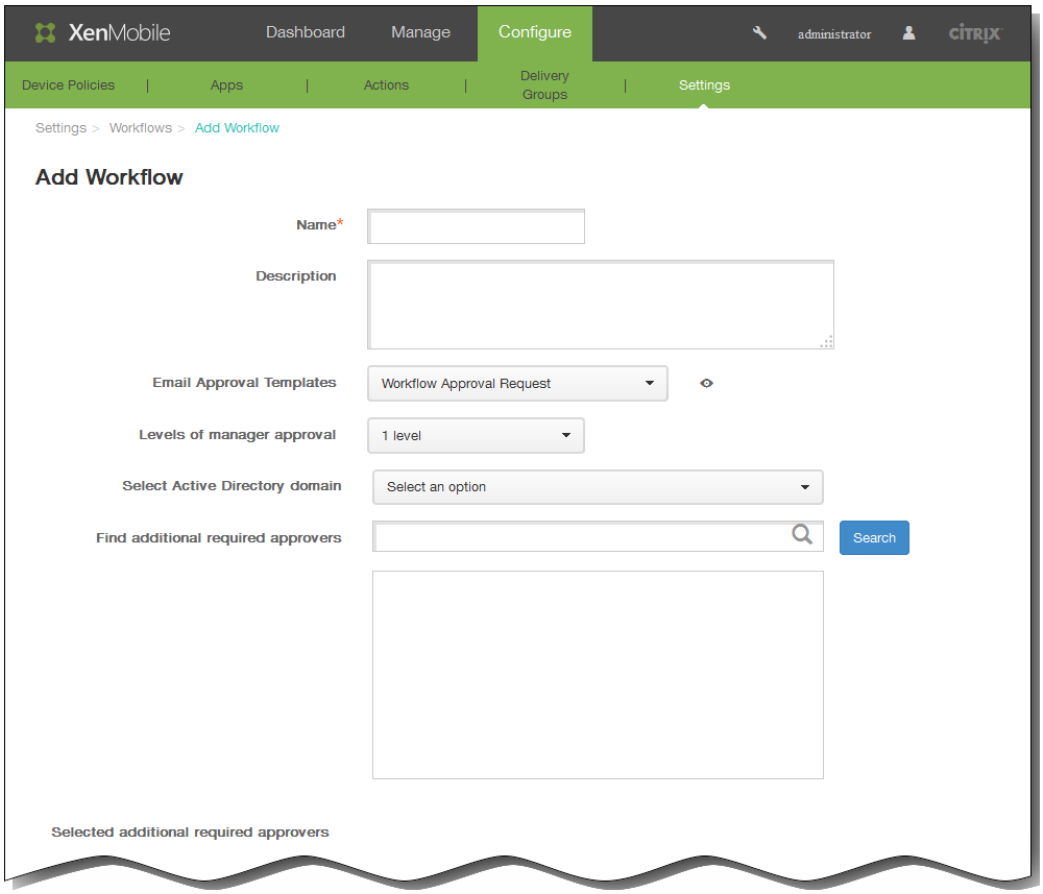
1. Dans la console XenMobile, cliquez sur Configurer > Paramètres > Workflows.





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.

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 Save.
    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

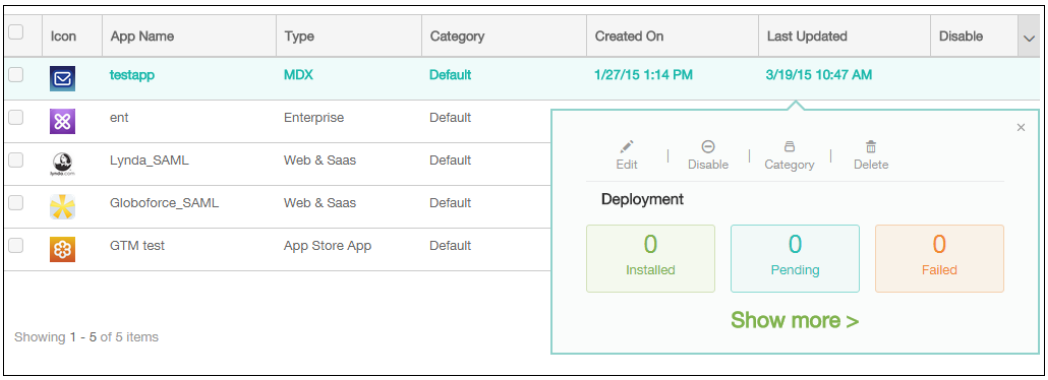
1. Sur la page Workflows, dans la liste des workflows, sélectionnez un workflow en cliquant sur la ligne dans le tableau ou en cochant la case à cocher en regard du workflow.
2. Pour supprimer un workflow, cliquez sur Supprimer. Une boîte de dialogue de confirmation s'affiche. Cliquez à nouveau sur Supprimer.
   Important : vous ne pouvez pas annuler cette opération.

Mise à niveau d'une application dans XenMobile

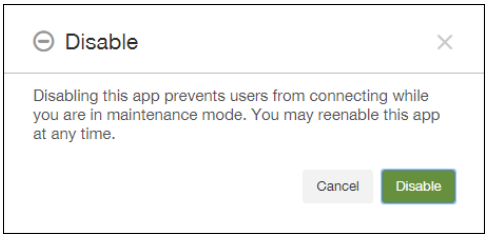
May 06, 2016

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.

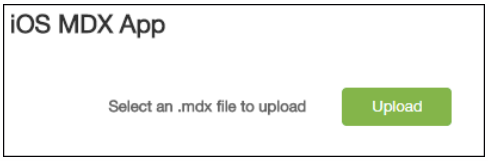


   2. Dans la boîte de dialogue de confirmation, cliquez sur Désactiver.



   Dans le tableau des applications, l'application est marquée Désactivée.

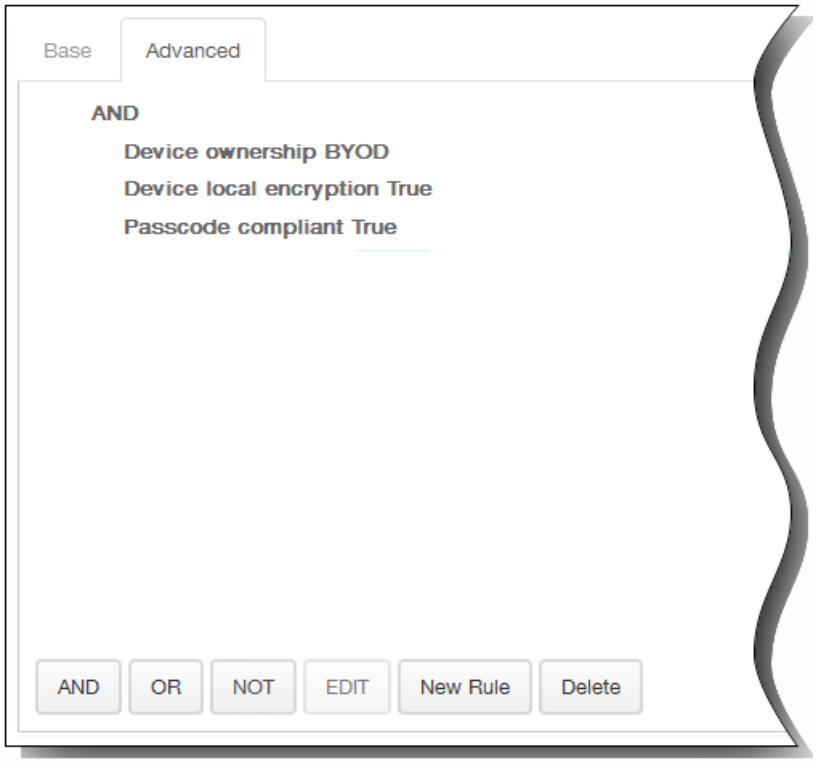
   Remarque : l'application désactivée passe en mode de maintenance. Quand l'application est désactivée, les utilisateurs ne pourront plus s'y connecter une fois la session fermée. La désactivation d'applications est un paramètre facultatif, mais Citrix recommande de désactiver l'application pour éviter 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.



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.

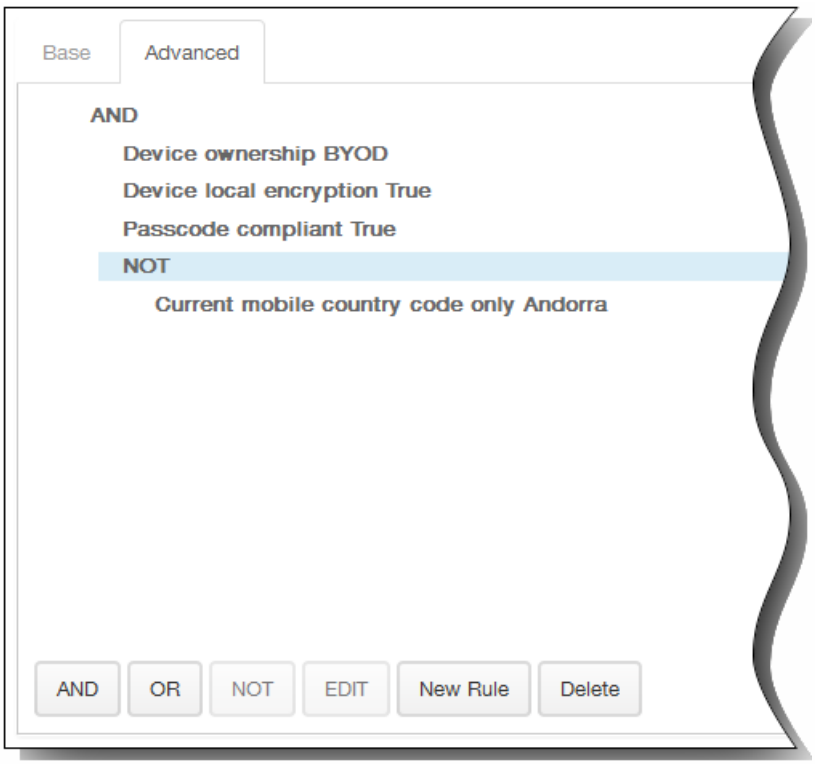
1. Dans la liste, cliquez sur les options pour déterminer quand l'application doit être déployée.
    1. Vous pouvez déployer l'application lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir 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.



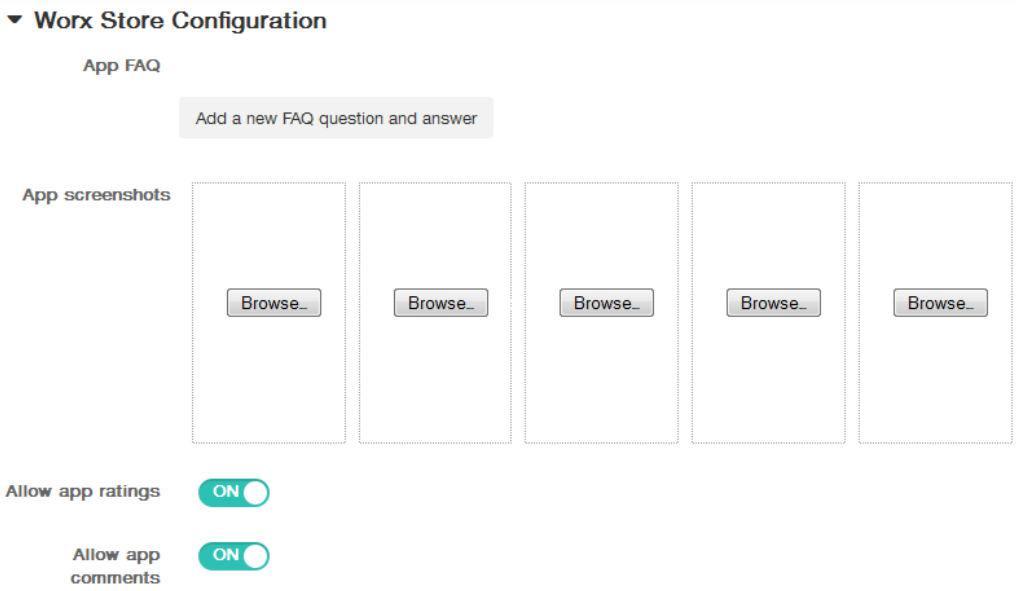
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.

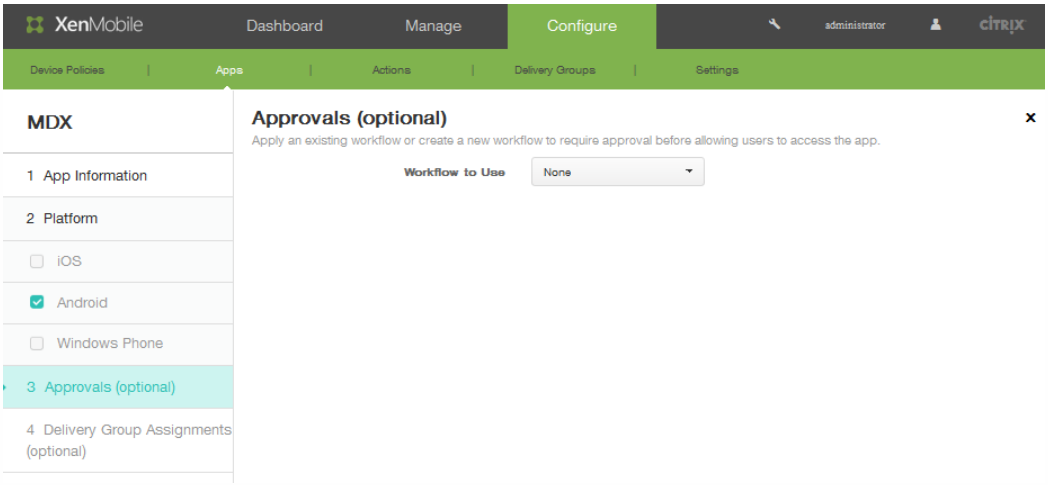


8. Développez Configuration de Worx Store pour ajouter un forum aux questions (FAQ) sur l'application, ou ajoutez des captures d'écran pour faciliter le classement de l'application dans le Worx Store. l'image que vous chargez doit être au format PNG. Vous ne pouvez pas charger une image GIF ou JPEG.

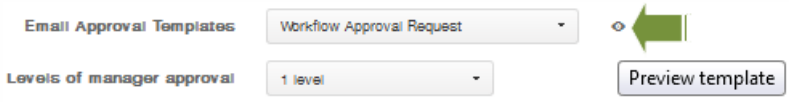


Dans Autoriser notation des applications, cliquez sur ON pour permettre à un utilisateur d'évaluer l'application.

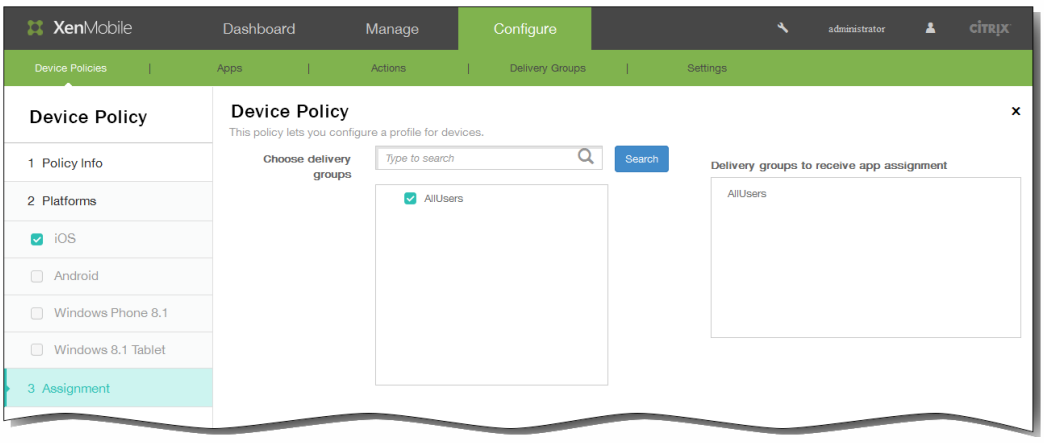
9. Dans Autoriser commentaires sur les applications, cliquez sur ON pour permettre aux utilisateurs de laisser des commentaires sur l'application sélectionnée.
10. Cliquez sur Suivant. L'écran Approbations s'affiche.



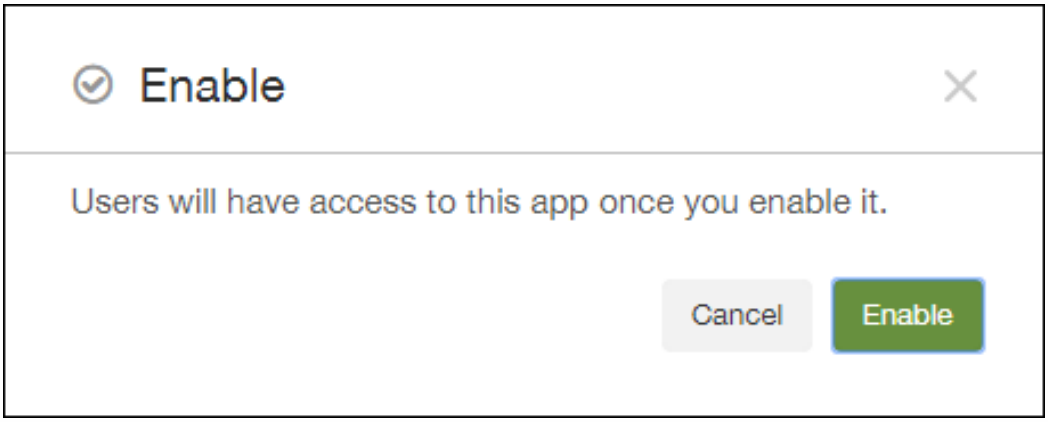
11. Lorsque vous créez un nouveau workflow, la console XenMobile affiche les options de configuration pour le processus d'approbation. Chacun de ces champs est décrit dans les étapes suivantes. Configurez ces champs si vous avez besoin d'une approbation pour créer des comptes d'utilisateurs.
    1. Spécifiez 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.



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.

Synopsis des stratégies applicatives MDX

May 06, 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 Administration de Worx Home.

Actions automatisées

May 06, 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.

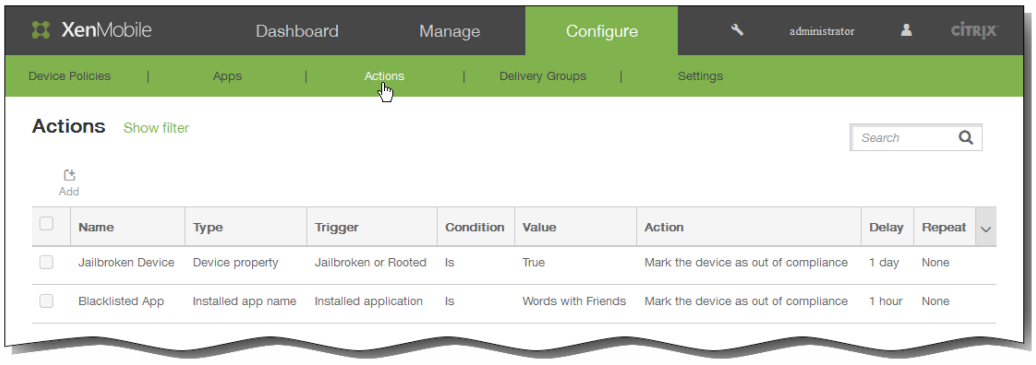
Les effets automatiques que vous pouvez paramétrer sont :

- 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.

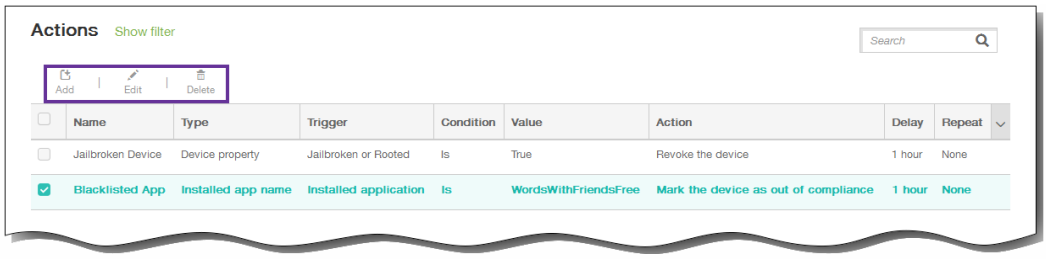
Remarque : pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans Paramètres pour SMTP et SMS afin que XenMobile puisse envoyer des messages, consultez la section Notifications dans XenMobile. Vous devez également configurer les modèles de notification que vous prévoyez 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.

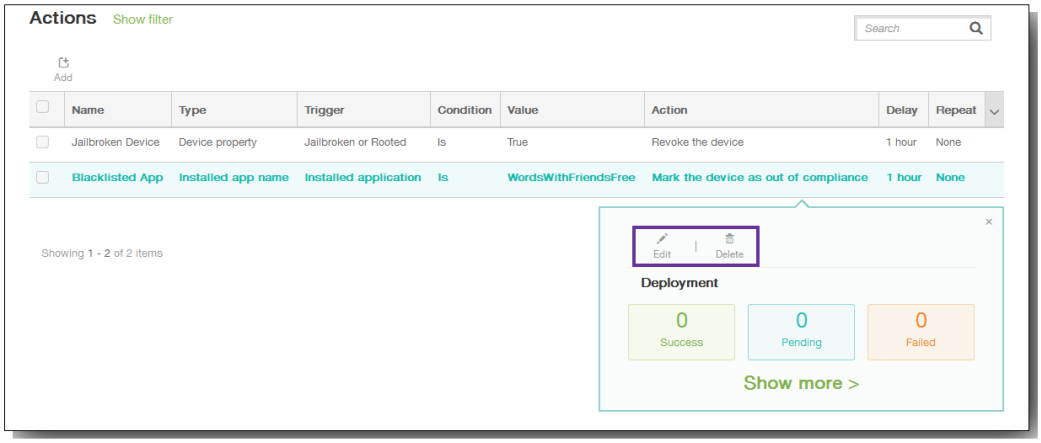
Cette rubrique explique comment ajouter, modifier et filtrer des actions automatisées dans XenMobile.

1. Dans la console XenMobile, cliquez sur Configurer > Actions. La page Actions s'affiche.

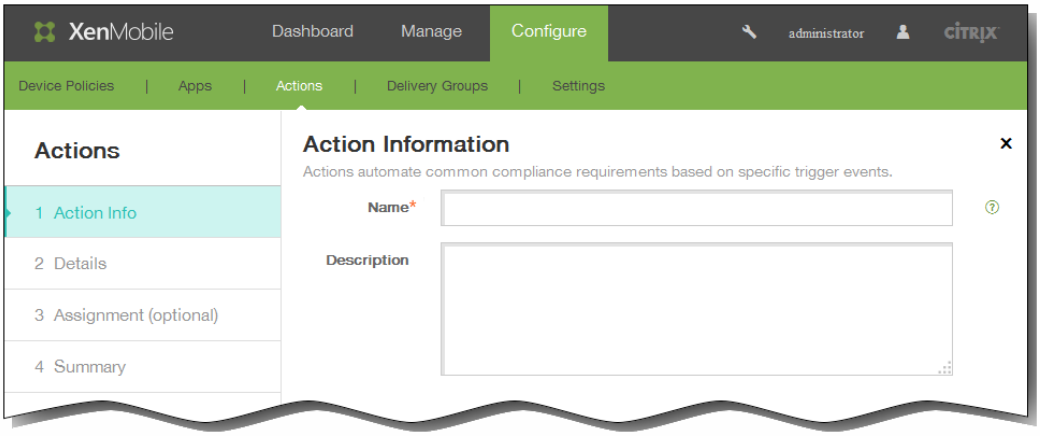


2. Sur la page Actions, effectuez l'une des actions suivantes :
   - Cliquez sur Ajouter pour ajouter une nouvelle action.
   - Sélectionnez une action existante à modifier ou à supprimer. Cliquez sur l'option que vous voulez utiliser.
     Remarque : lorsque vous activez la case à cocher en regard d'une 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.

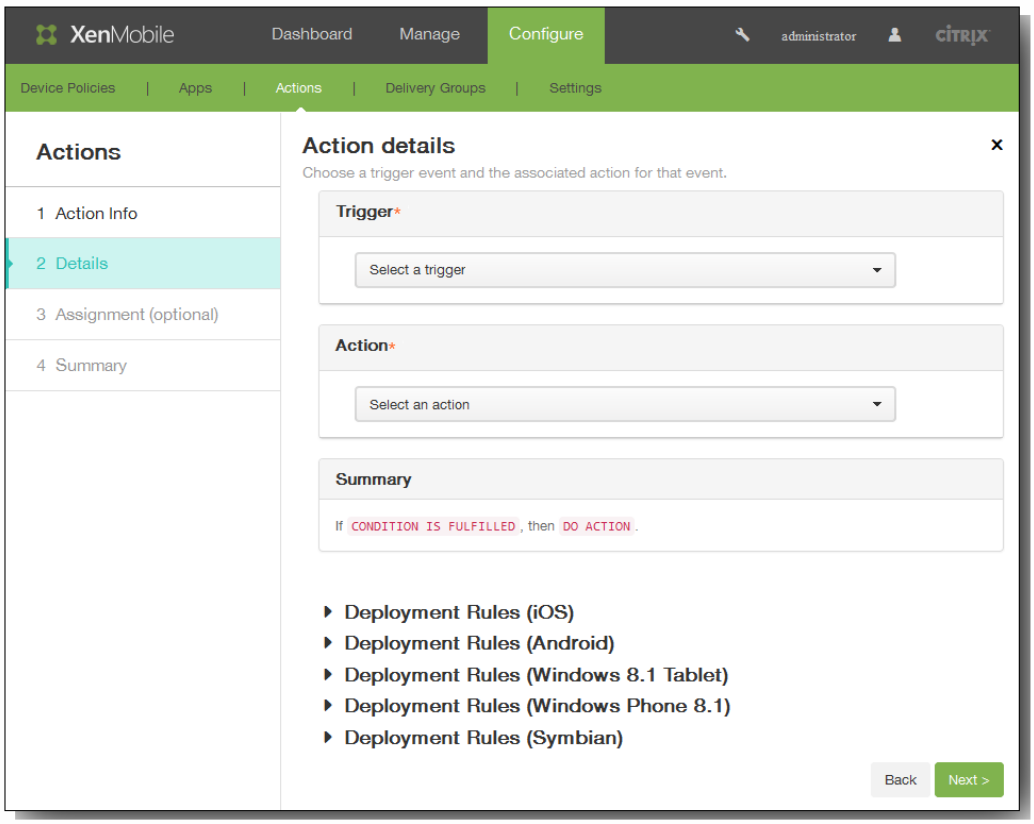




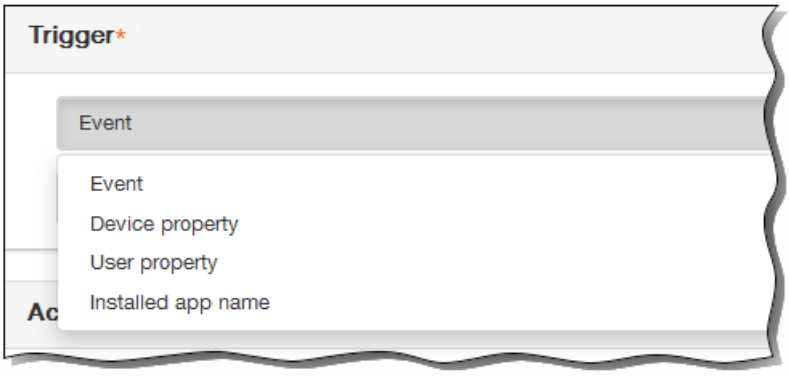
La page Informations sur l'action s'affiche.



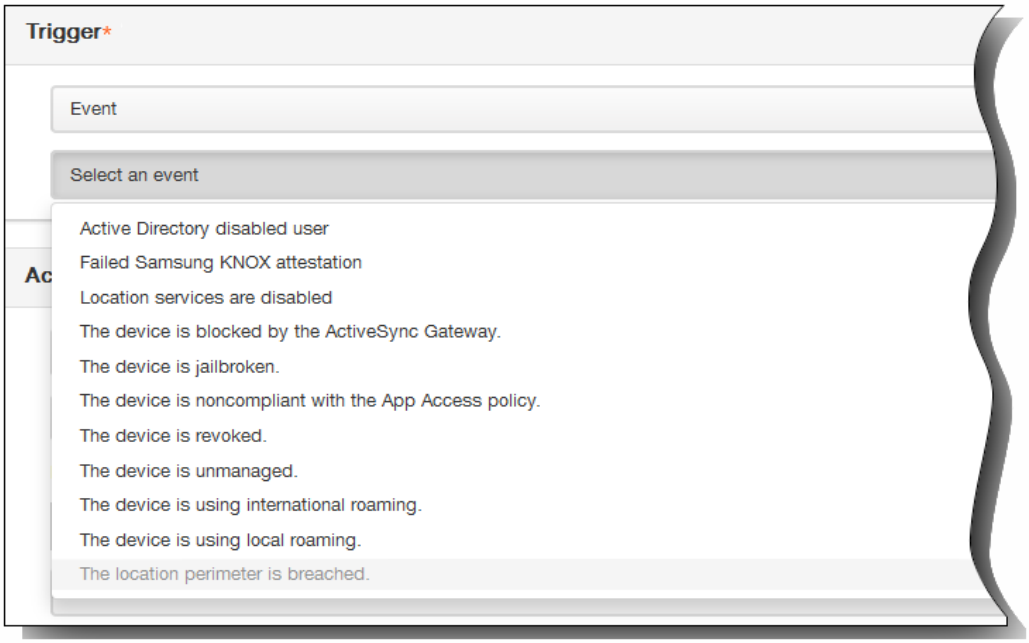
3. Sur la page Informations sur l'action, entrez ou modifiez les informations suivantes :
   1. Nom : entrez un nom permettant d'identifier de façon unique l'action. Ce champ est obligatoire.
   2. Description : décrivez ce que l'action doit faire.
4. Cliquez sur Suivant. La page sur les Détails de l'action 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.



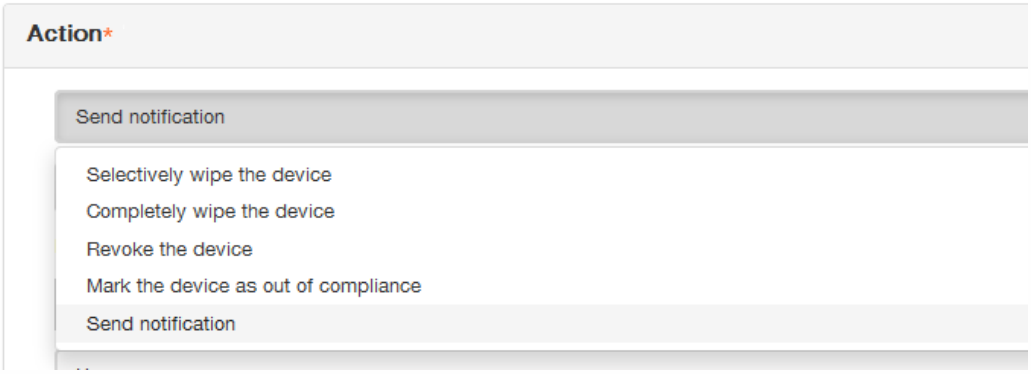
5. Sur la page Détails de l'action, entrez ou modifiez les informations suivantes :
    1. Dans la liste des Déclencheurs, cliquez sur le type de déclencheur d'événements pour cette action. Signification des déclencheurs :
        - Événement : réagit à un événement prédéfini.
        - Propriété de 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.

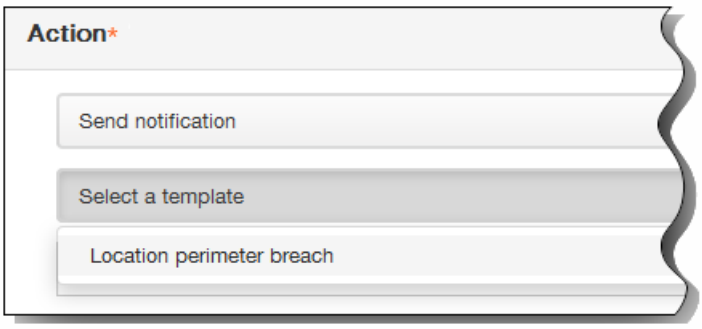


3. Dans la liste Action, cliquez sur l'action à effectuer lorsque le critère du déclencheur est rencontré. À l'exception de Envoyer une notification, vous choisissez un délai au cours duquel les utilisateurs devront avoir résolu le problème qui a activé le déclencheur. Si le problème n'est pas résolu dans ce délai, l'action sélectionnée est entreprise.



Le reste de cette procédure décrit comment envoyer une action de notification.

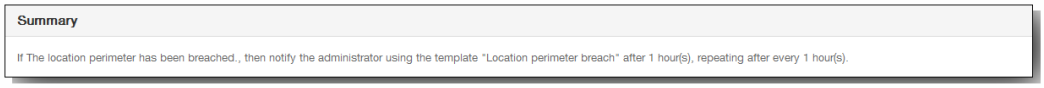
4. Dans la liste suivante, sélectionnez le modèle à utiliser pour la notification. Les modèles de notification correspondant à l'événement sélectionné apparaissent.
Remarque : pour avertir les utilisateurs, vous devez avoir configuré les serveurs de notification dans Paramètres pour SMTP et SMS afin 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.



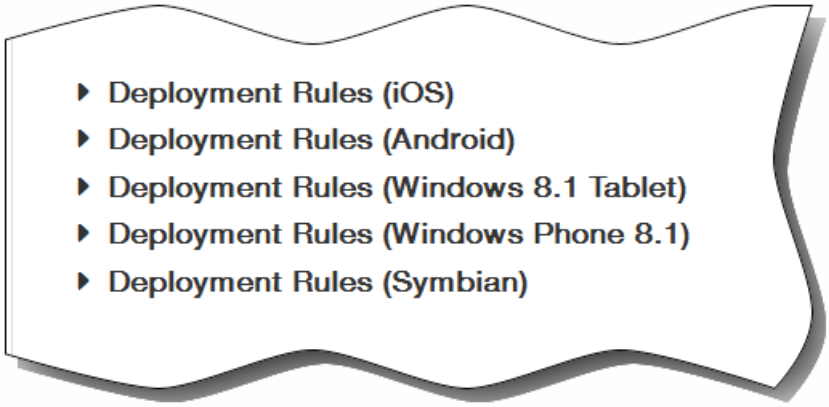
Remarque : après avoir sélectionné le modèle, vous pouvez afficher un aperçu de la notification en cliquant sur Aperçu du message de notification.

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.

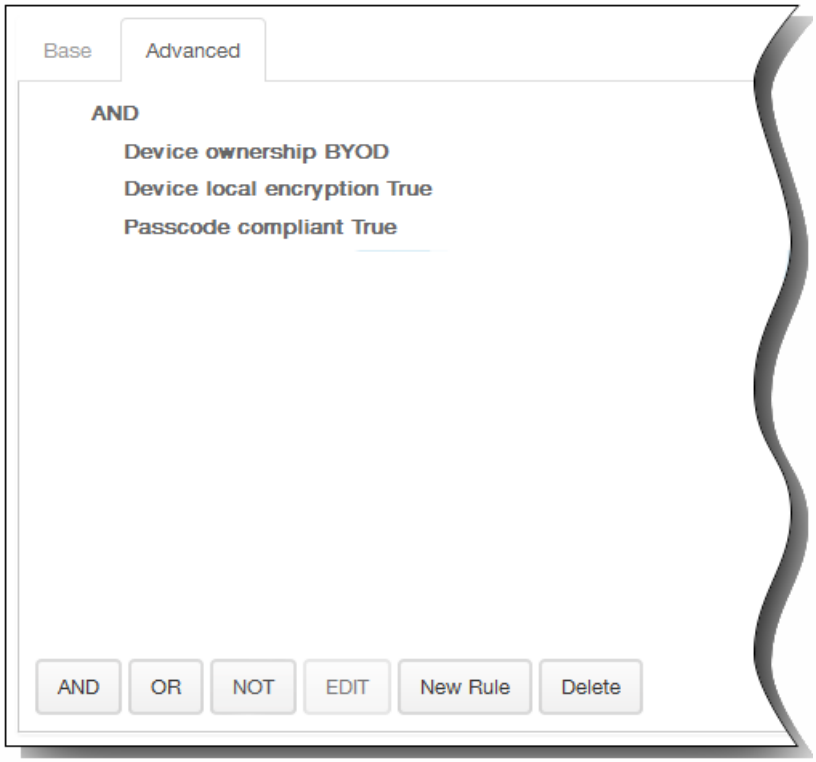


Après avoir configuré les détails de l'action, vous pouvez configurer des règles de déploiement pour chacune des plates-formes, iOS, Android, Windows 8.1 Tablet, Windows Phone 8.1 et Symbian. Pour ce faire, suivez les étapes 6 à 9 pour chacune des plates-formes que vous choisissez.



6. Développez Règles de déploiement. L'onglet Base s'affiche par défaut.

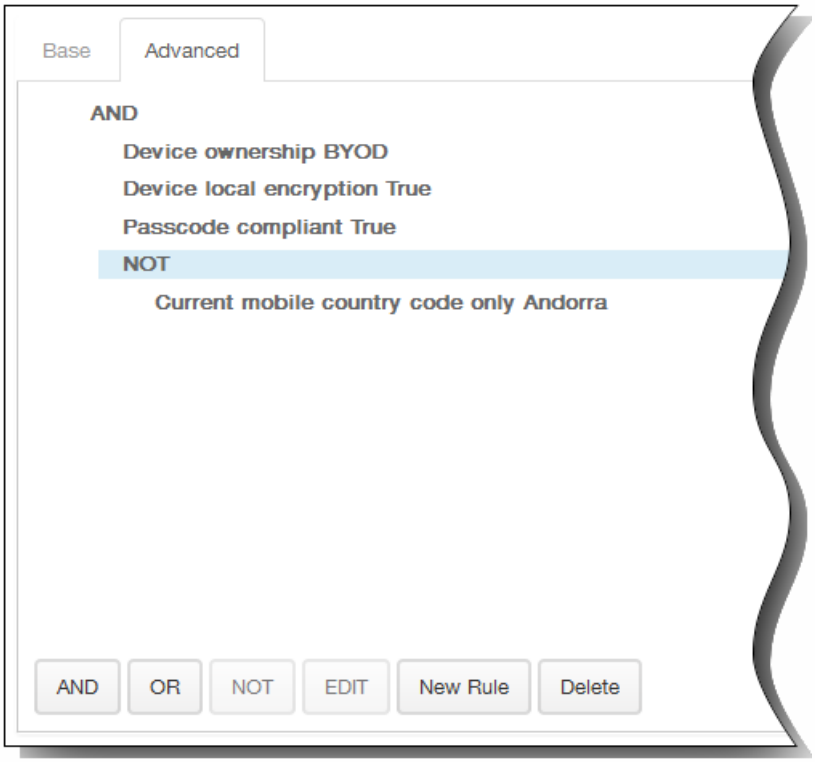
1. Dans la liste, cliquez sur les options pour déterminer quand l'action doit être déployée.
    1. Vous pouvez déployer l'action lorsque toutes les conditions sont remplies ou lorsque l'une des conditions est remplie. L'option par défaut est Toutes.
    2. Cliquez sur Nouvelle règle pour définir les 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.



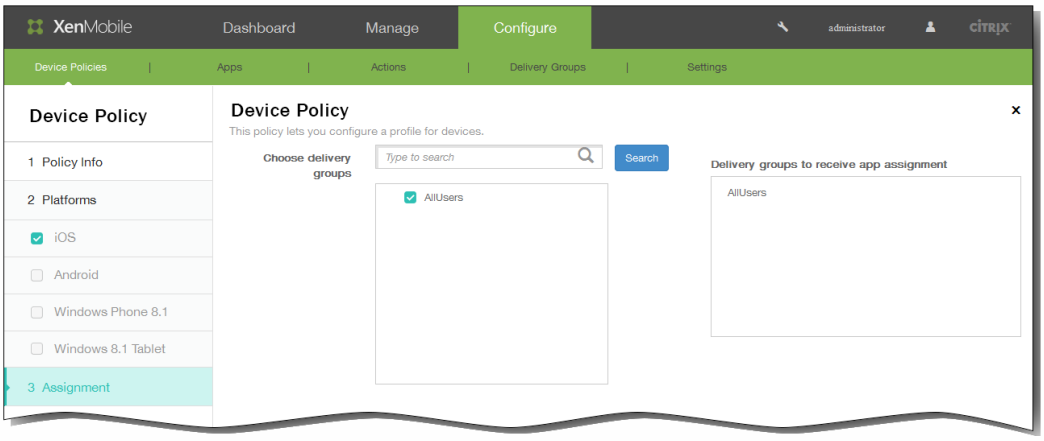
Les conditions que vous avez choisies sur l'onglet Base s'affichent.

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.



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.

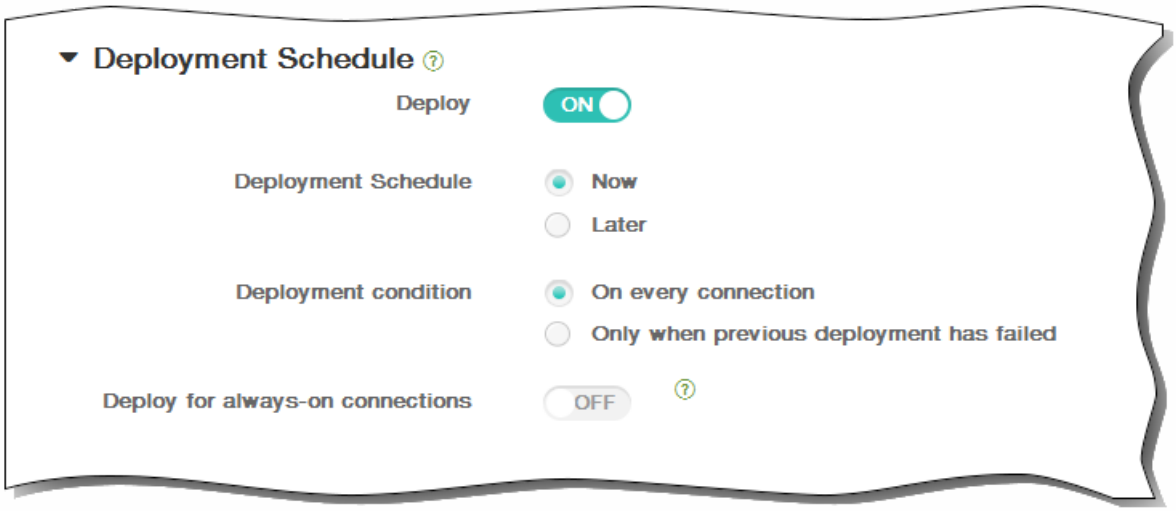


9. Développez Calendrier de déploiement et configurez les paramètres suivants :
    1. En regard de Déployer, cliquez sur ON pour planifier le déploiement ou cliquez sur OFF pour empêcher le déploiement. L'option par défaut est ON. Si vous choisissez OFF, aucune autre option ne doit être configurée.
    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.
    4. En regard de Conditions de déploiement, cliquez sur À chaque connexion ou Uniquement lorsque le déploiement

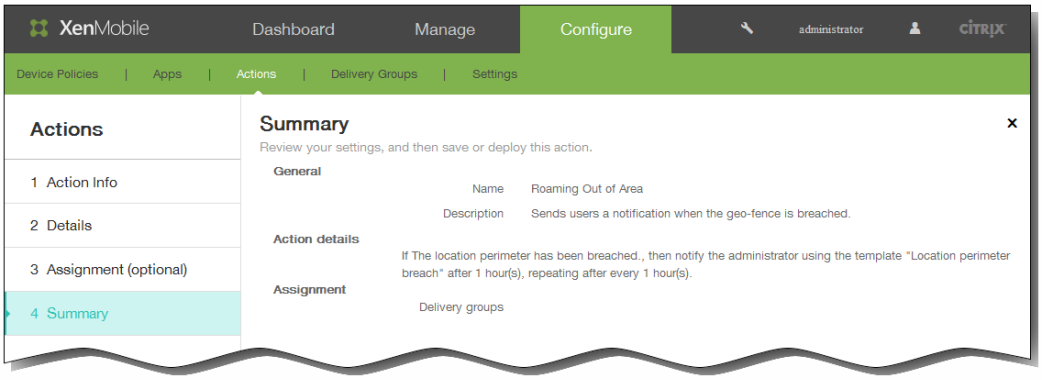
précédent a échoué. L'option par défaut est À chaque connexion.

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.

Paramètres du client XenMobile

May 06, 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.

Personnalisation du Worx Store pour appareils iOS

Oct 11, 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.

Création d'options d'assistance Worx Home et GoToAssist

May 06, 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.

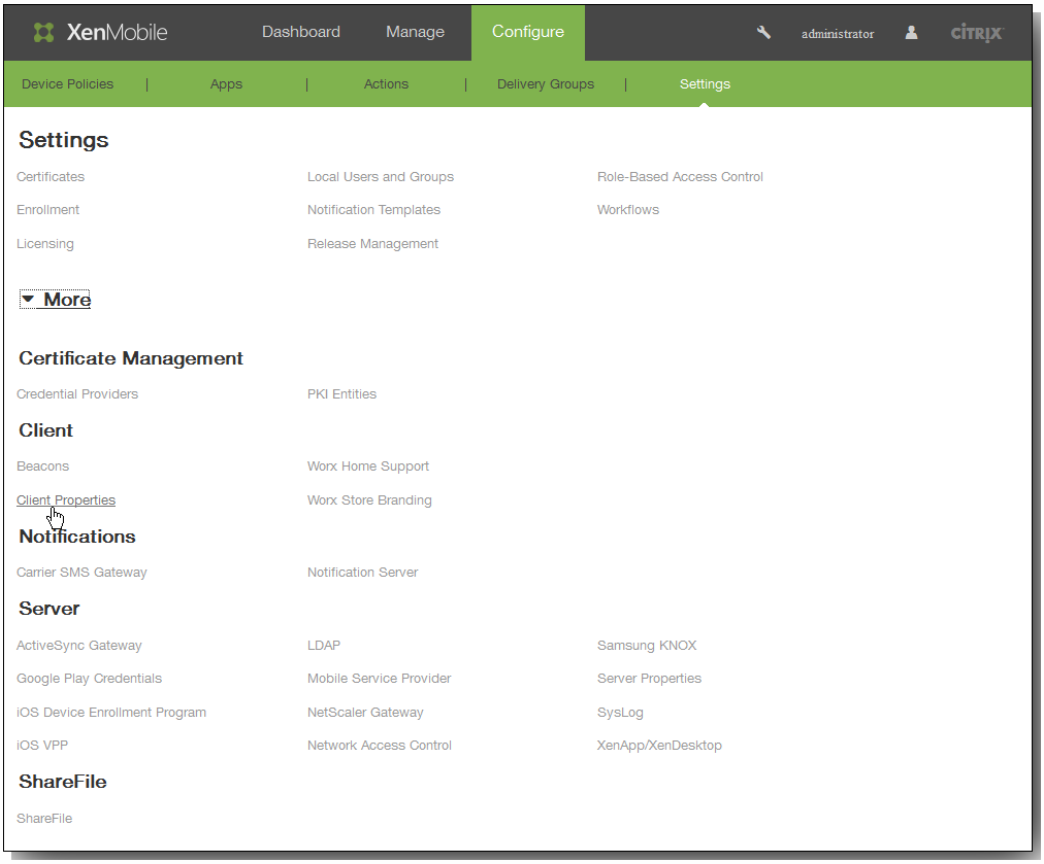
Pour ajouter, modifier ou supprimer des propriétés de client

May 06, 2016

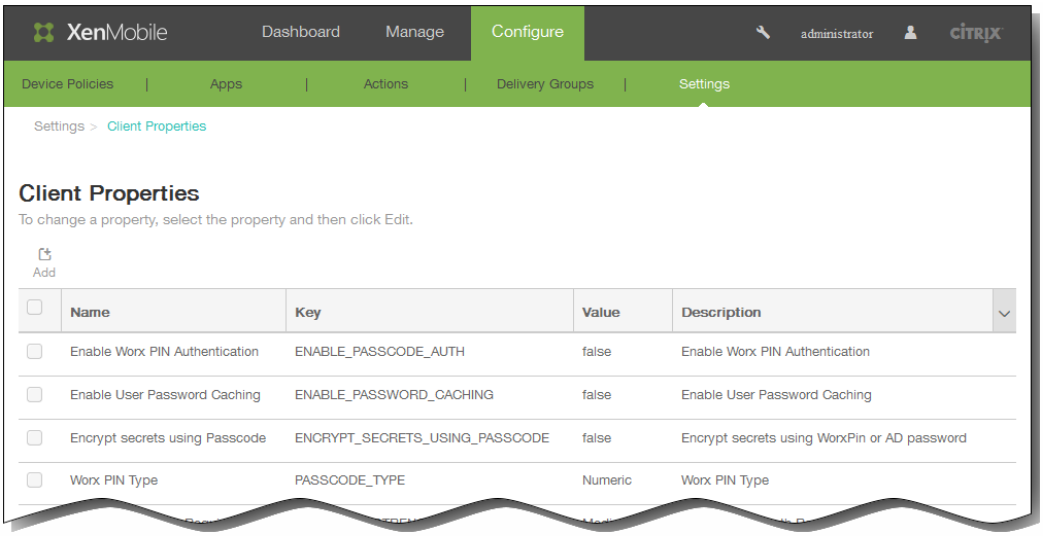
Les propriétés du client contiennent des informations qui sont fournies directement à Worx Home sur les appareils des utilisateurs. Les propriétés du client sont utilisées pour configurer des paramètres avancés tels que le code PIN Worx. Vous obtenez les propriétés du client à partir du support de Citrix.

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.

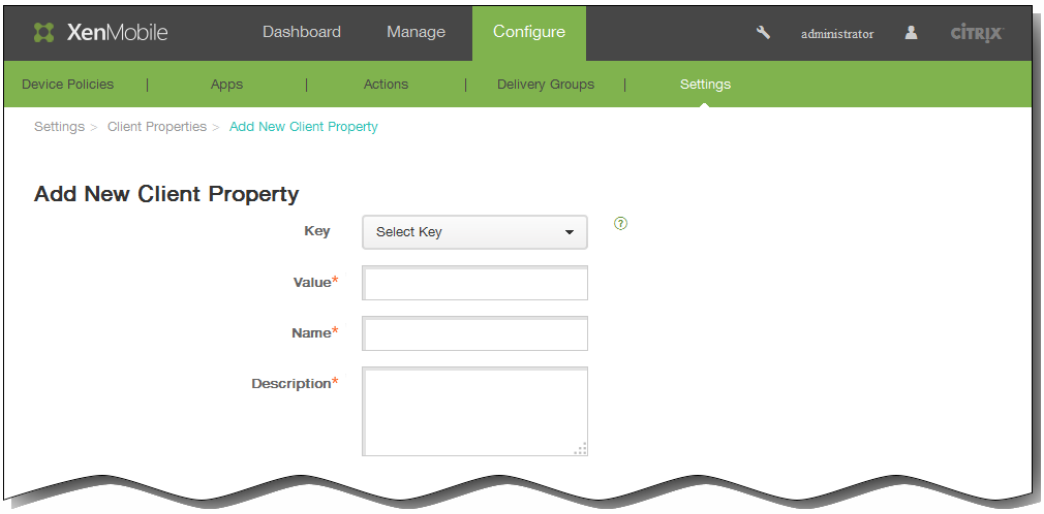


La boîte de dialogue Propriétés du client s'affiche. Vous pouvez ajouter, modifier et supprimer des propriétés de client à partir de cette page.



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.

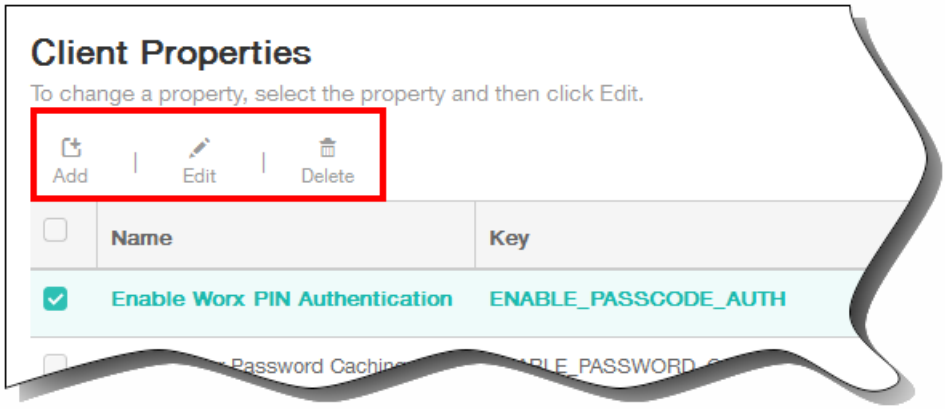


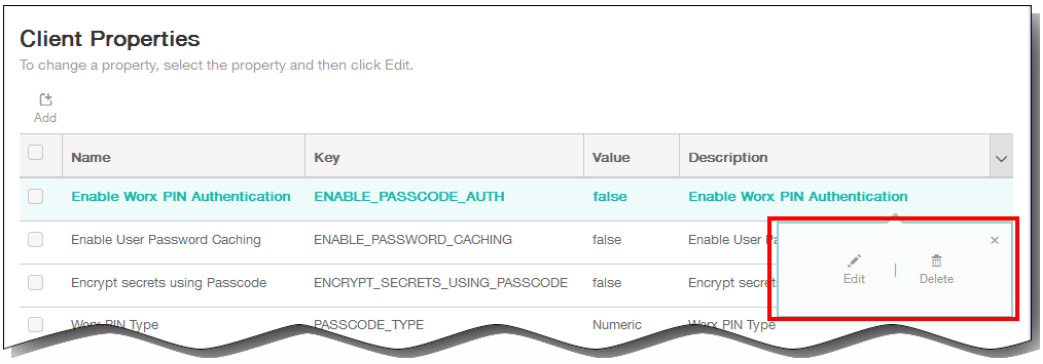
2. Dans la boîte de dialogue Ajouter une nouvelle propriété de client, entrez les informations suivantes :
   Remarque : tous les champs sont obligatoires.
   1. Clé : dans la liste, cliquez sur la clé de propriété que vous souhaitez ajouter.
      Important : contactez le support Citrix avant d'apporter 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

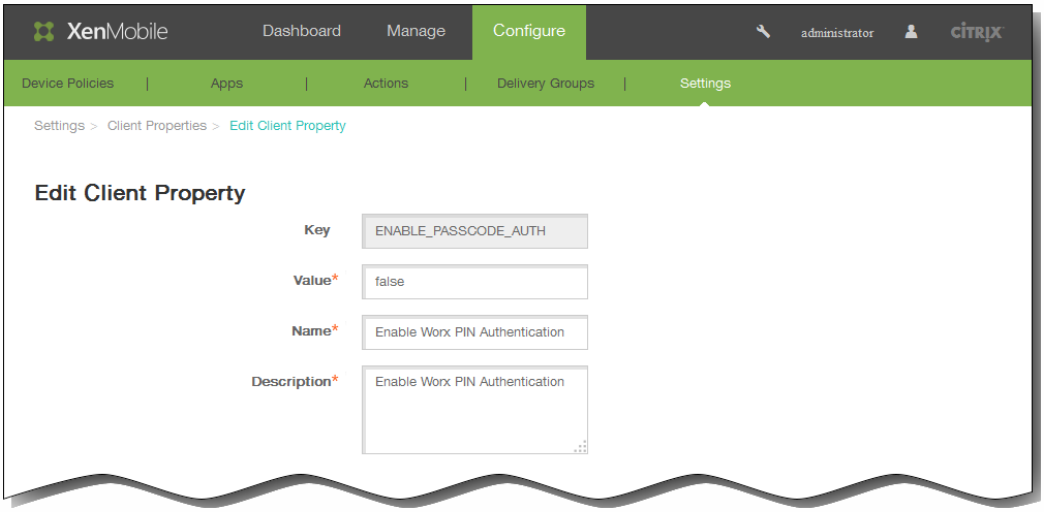
1. Dans le tableau Propriétés du client, sélectionnez la propriété de client que vous voulez modifier.
   Remarque : lorsque vous sélectionnez la case à cocher en regard d'une propriété de client, le menu d'options s'affiche au-dessus de la liste des propriétés de client ; lorsque vous cliquez ailleurs dans la liste, le menu d'options s'affiche sur le côté

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.

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.

Référence des propriétés du client

Oct 11, 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

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

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. **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)

Paramètres du serveur XenMobile

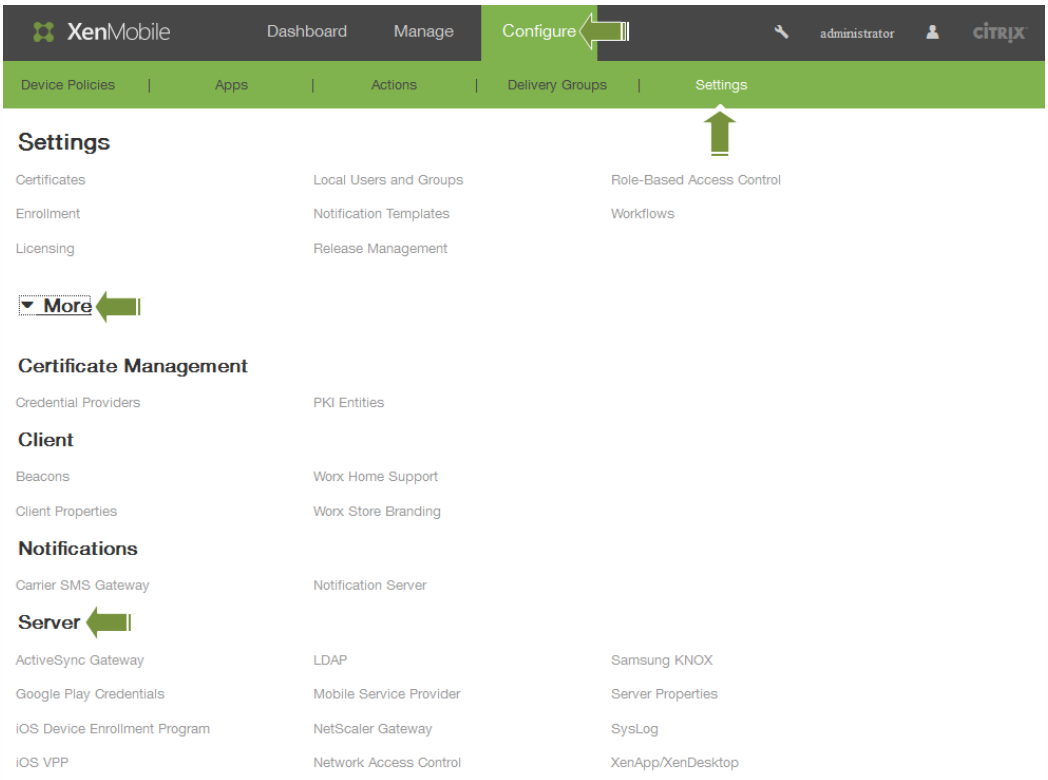
May 06, 2016

Vous pouvez configurer les paramètres du serveur XenMobile dans la console Web XenMobile.

Les options de configuration du serveur comprennent :

ActiveSync Gateway	VPP iOS	NetScaler Gateway	Propriétés du serveur
Informations d'identification Google Play	LDAP	Contrôle d'accès réseau	SysLog
iOS Device Enrollment Program	Fournisseur de services mobiles	Samsung KNOX	XenApp/XenDesktop

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.

ActiveSync Gateway dans XenMobile

May 06, 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.

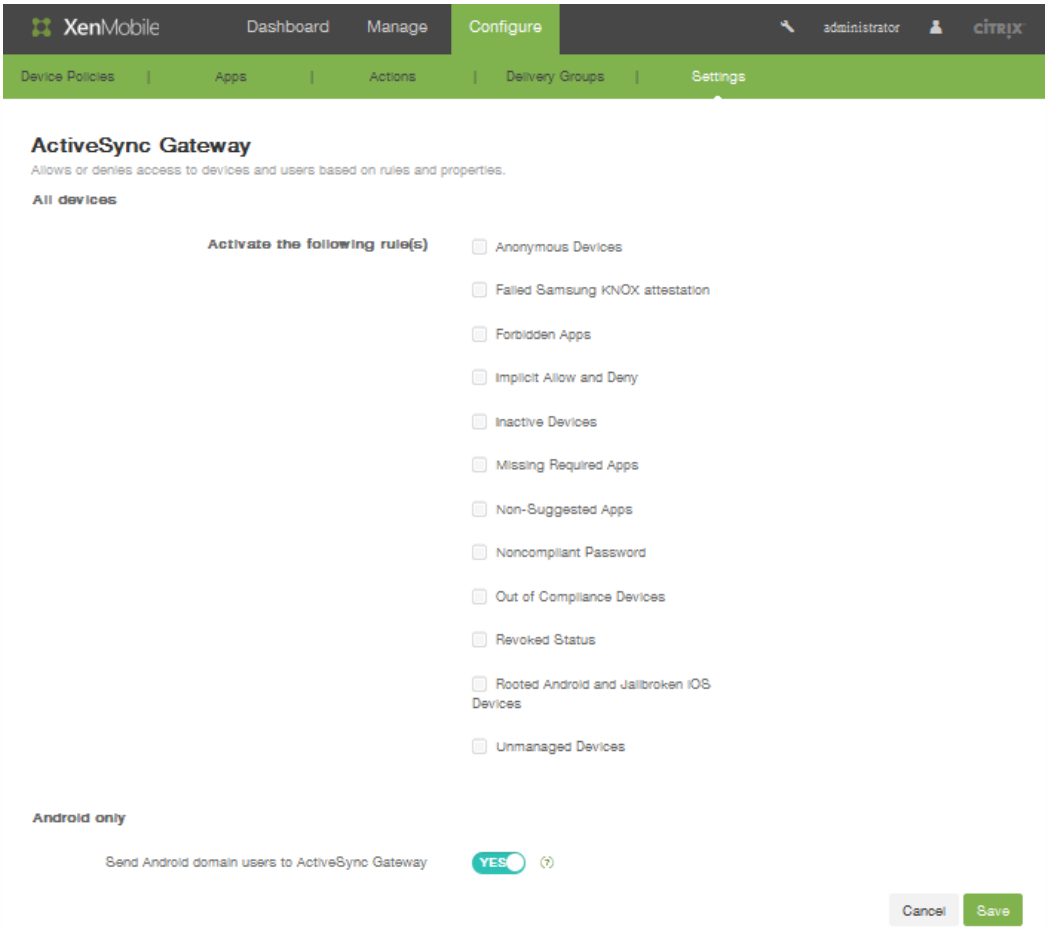
Appareils Android rootés et iOS jailbreakés : vérifie si un appareil Android ou iOS est rooté ou jailbreaké.

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.

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**.

Informations d'identification Google Play

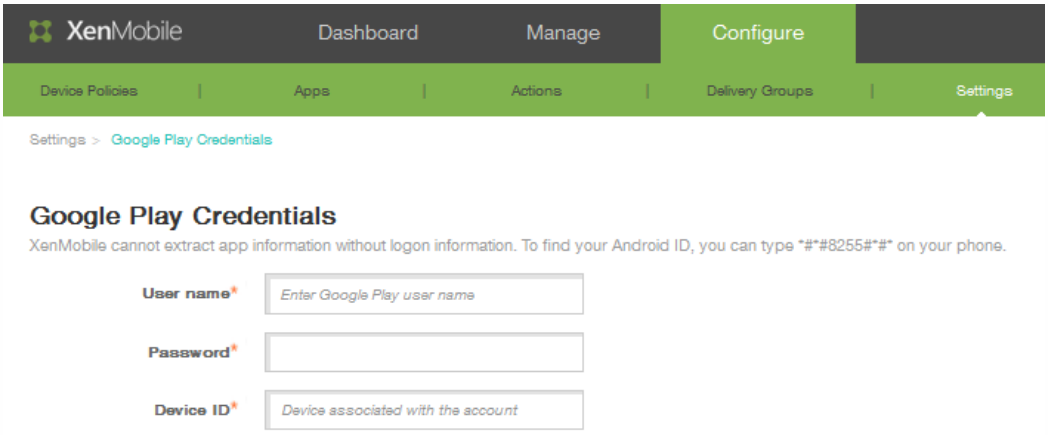
May 06, 2016

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 Save.

iOS Device Enrollment Program

May 06, 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

Avant de continuer, vous devez avoir créé un compte Apple DEP sur deploy.apple.com. Après avoir créé un compte DEP, configurez un serveur MDM virtuel pour autoriser les communications entre XenMobile et Apple. Pour ce faire, vous devez charger une clé publique XenMobile sur le site d'Apple. Lorsque Apple reçoit la clé publique, il renvoie un jeton de serveur que vous importez dans XenMobile. Suivez ces étapes pour établir la connexion entre XenMobile et Apple.

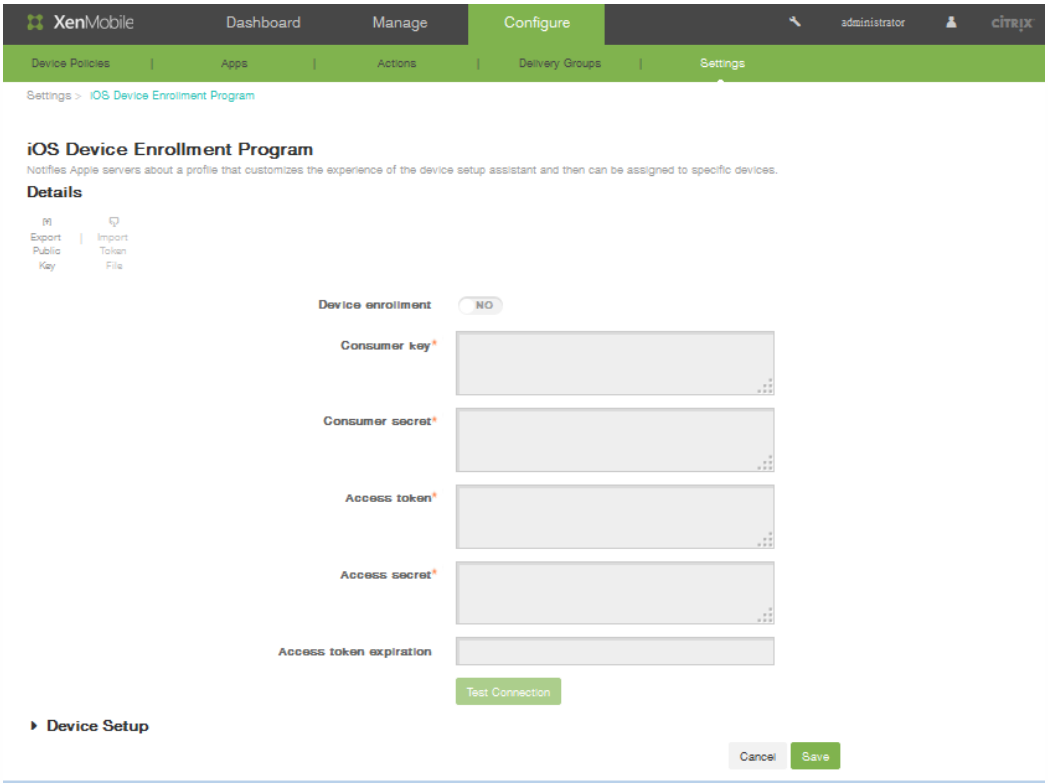
1. Pour obtenir la clé publique à charger sur Apple, sur la page **iOS Device Enrollment Program** sous **Paramètres > Plus**, cliquez sur **Exporter la clé publique** et enregistrez le fichier sur votre ordinateur.

2. Accédez à deploy.apple.com, connectez-vous à votre compte DEP et suivez les instructions pour configurer un serveur MDM. Dans le cadre de ce processus, Apple fournit un jeton de serveur.

3. Sur la page **iOS Device Enrollment Program**, définissez **Inscription d'appareils** sur **Oui** et cliquez sur **Importer un fichier jeton** pour ajouter le jeton du serveur Apple à XenMobile.

4. Le champ **Jetons de serveur** est renseigné automatiquement dès que le fichier de jeton est chargé sur XenMobile.

5. Cliquez sur **Tester la connectivité** pour confirmer que XenMobile et Apple peuvent communiquer. Si le test de la connexion échoue, vérifiez que vous avez bien ouvert tous les ports requis car ce type de problème est à l'origine de la plupart des échecs. Pour de plus amples informations sur les ports qui doivent être ouverts dans XenMobile, consultez la section Configuration requise pour les ports.



Dans **Détails**, configurez les paramètres suivants pour terminer la configuration DEP :

- Inscription d'appareils : cliquez sur OUI.
- Clé du client: 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.
- Cliquez sur Tester la connexion pour vérifier la connexion.

- 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).
  - Unique service ID : spécifiez un ID de service unique (facultatif)

- 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.

- Dans Étapes de configuration de l'appareil, configurez les paramètres suivants :
  - Services de localisation: 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 afin d'autoriser un appareil à restaurer les données à partir d'une copie de sauvegarde.
  - Apple 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 autoriser un appareil à utiliser Siri.
  - Touch ID : cliquez sur Configuration pour utiliser la fonction Touch ID sur l'appareil.
  - Apple Pay : cliquez sur Configuration afin d'autoriser Apple Pay sur l'appareil.
  - Zoom : cliquez sur Configuration pour activer le zoom.
  - Diagnostics : cliquez sur Configuration pour autoriser l'appareil à partager les diagnostics.

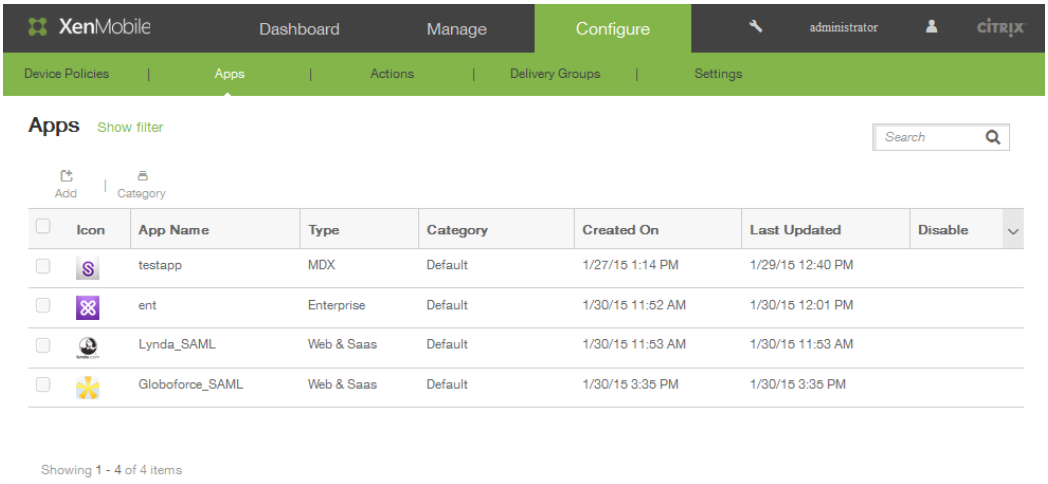
- Cliquez sur Enregistrer.

VPP iOS

May 06, 2016

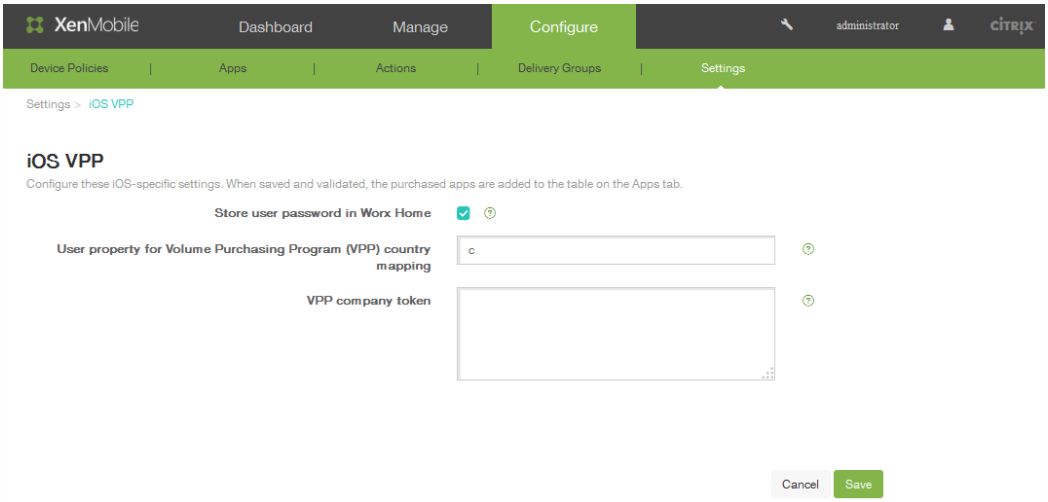
Vous pouvez configurer des paramètres spécifiques au Programme d'achat en volume iOS (VPP) dans XenMobile. Le programme VPP iOS simplifie la recherche, l'achat et la distribution d'applications en bloc pour une organisation. Le programme VPP fournit une solution simple et évolutive destinée à gérer les 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

1. Dans la console Web XenMobile, cliquez sur Configurer > Paramètres > Plus > VPP iOS. L'écran de configuration VPP iOS s'affiche.

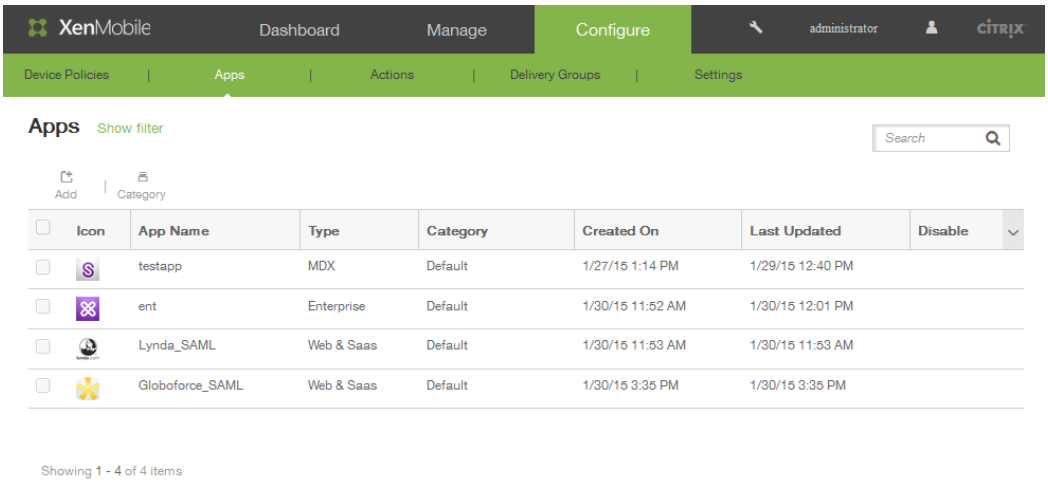


2. Dans Stocker le mot de passe utilisateur dans Worx Home, sélectionnez la case à cocher pour stocker de façon

sécurisée un nom d'utilisateur et un mot de passe dans Worx Home en vue de l'authentification sur XenMobile.

3. 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.

4. Dans Jeton d'entreprise VPP, 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.
5. Cliquez sur Save. Les informations sont alors affichées dans le tableau Applications :



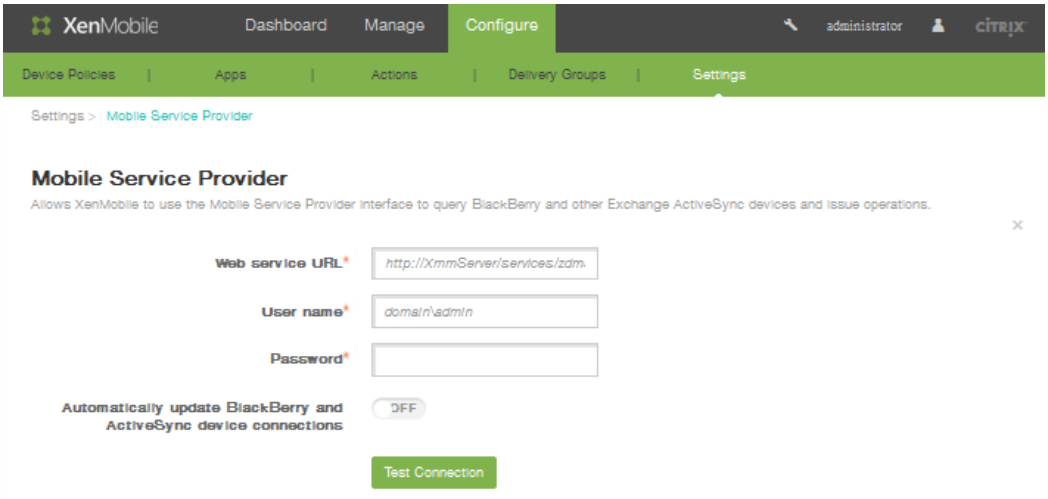
Fournisseur de services mobiles

May 06, 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 Save.

Contrôle d'accès réseau

May 06, 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

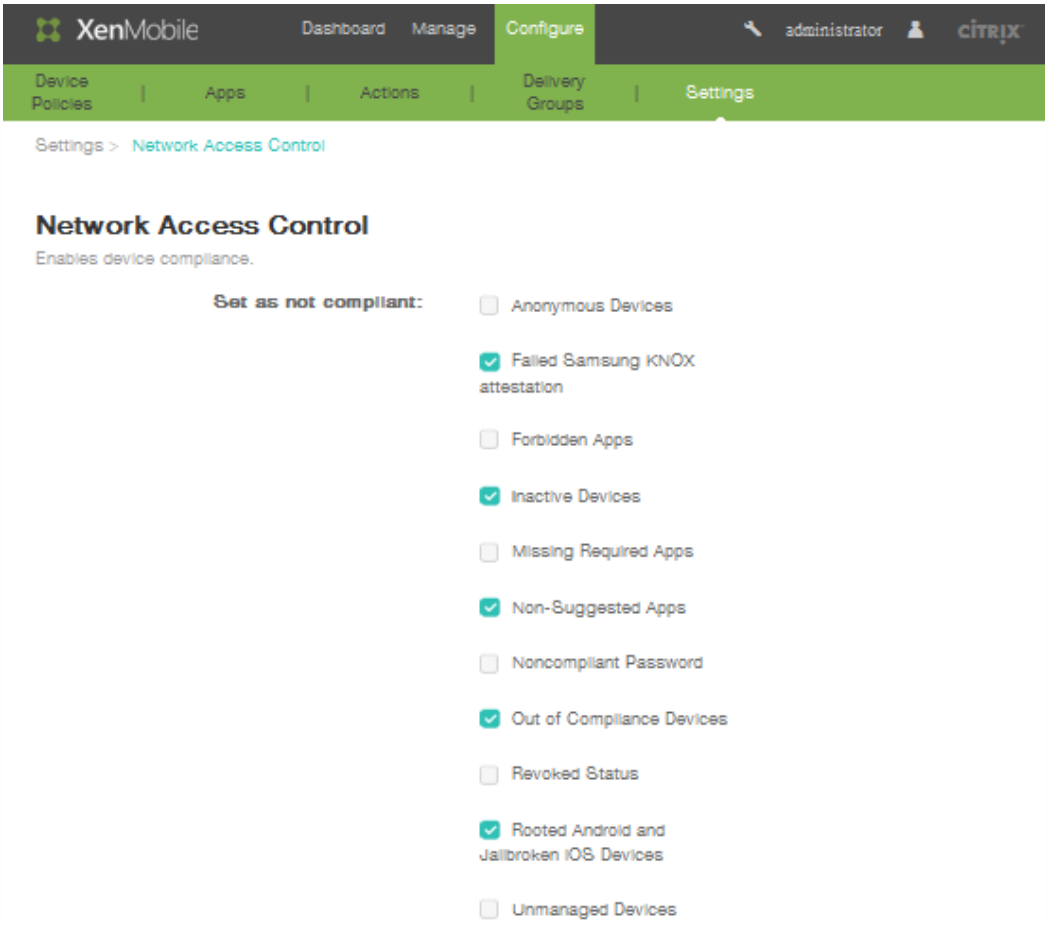
appareil exécuté en mode MAM ou un appareil désinscrit n'est pas géré.

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**.

Samsung KNOX

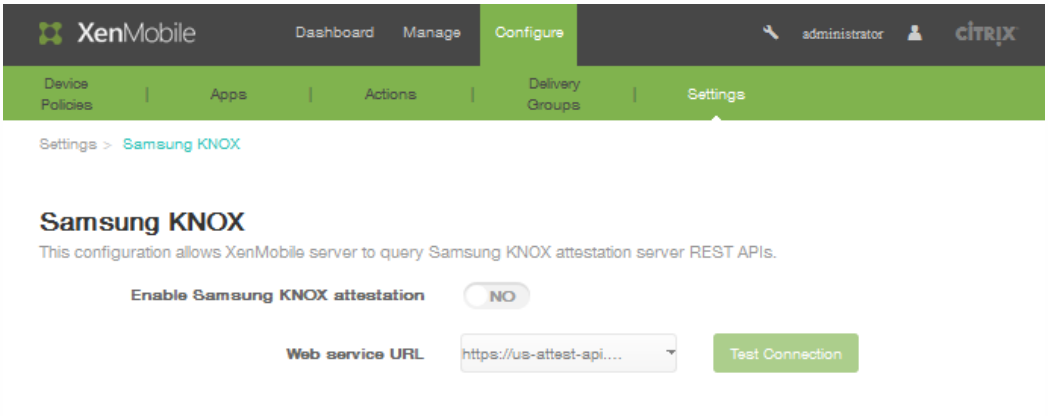
May 06, 2016

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 **Save**.

Propriétés du serveur

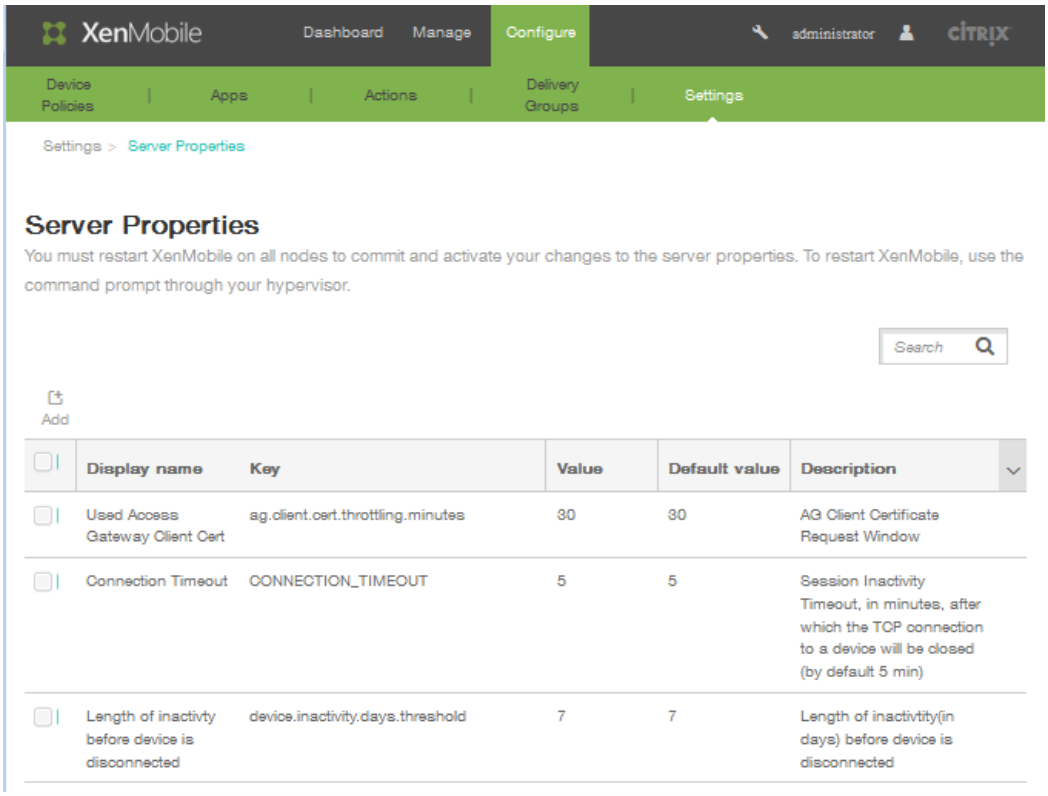
May 06, 2016

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.



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.

SysLog

May 06, 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.

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 :

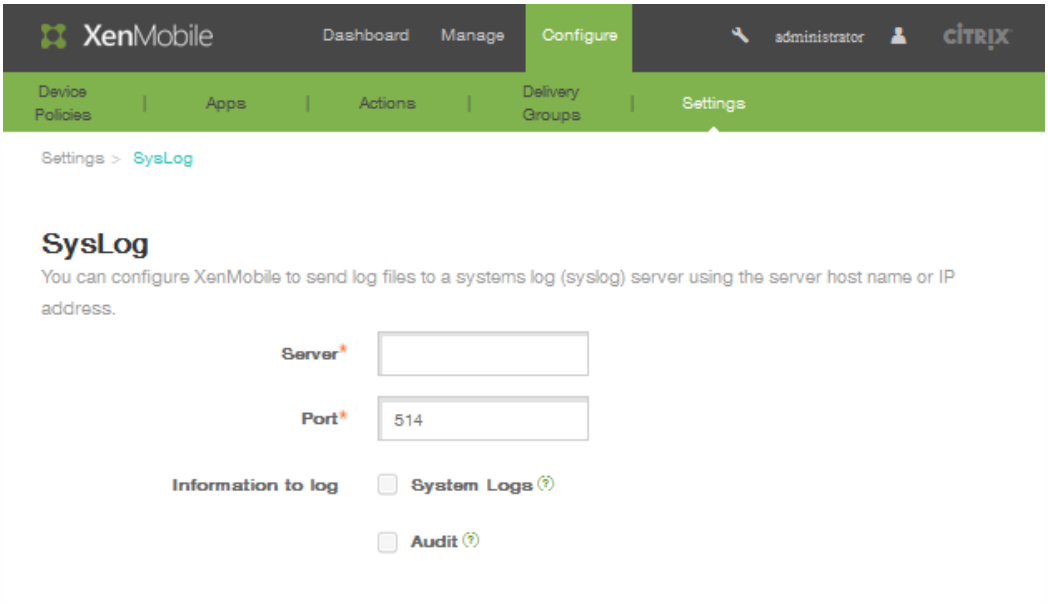
- L'adresse IP du boîtier qui a généré le message de journal
- Un horodatage
- Le type de message
- Le niveau de journalisation associé à un événement (critique, erreur, remarque, avertissement, informatif, débogage, alerte ou urgence)
- Les informations de message

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.



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 **Save**.

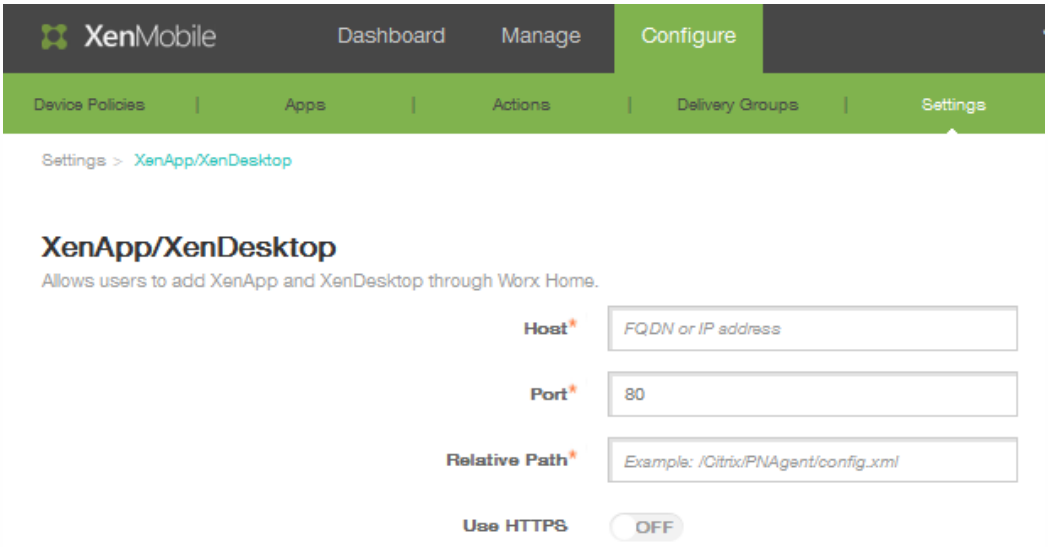
Pour configurer XenApp et XenDesktop

May 06, 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 de StoreFront ou du 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 de StoreFront ou du site Interface Web.
3. Dans Port, saisissez le numéro de port de StoreFront ou du 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**.

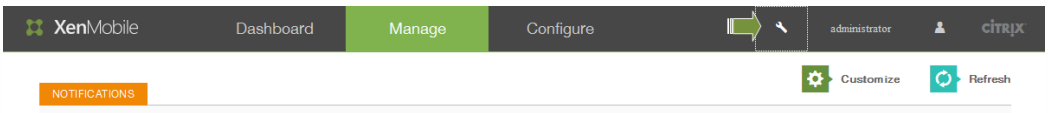
Support et maintenance de XenMobile

Oct 11, 2016

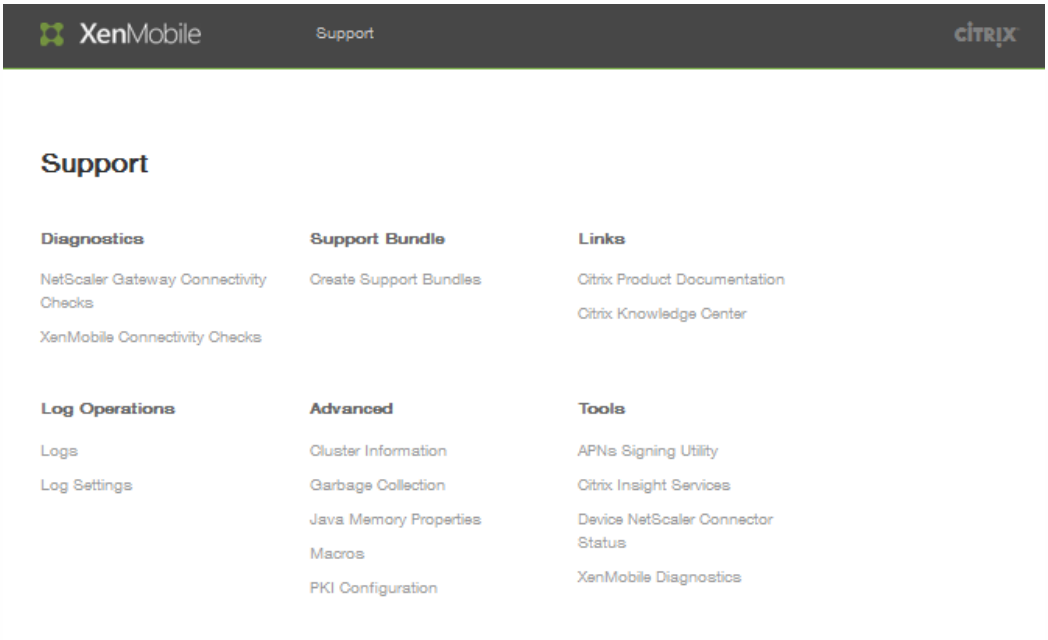
Utilisez la page Support de XenMobile pour accéder à des informations et outils de support. Vous pouvez également effectuer des actions à partir de l'interface de ligne de commande. Pour de plus amples informations, consultez la section Options d'interface de ligne de commande XenMobile.

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 :

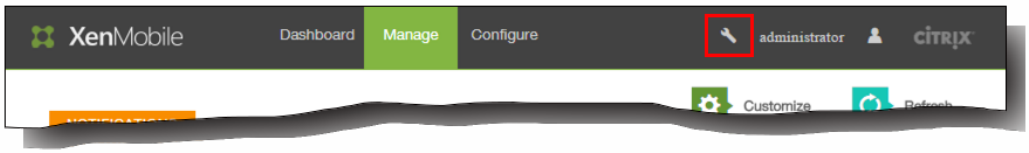
- Accéder aux diagnostics.
- Créer des packs d'assistance.
- Accéder aux liens de la documentation produit et du centre de connaissances Citrix.
- Accéder au journal des opérations.
- Sélectionner un ensemble d'options de configuration et d'informations avancées.
- Accéder à un ensemble d'outils et d'utilitaires.

Réalisation de contrôles de connectivité

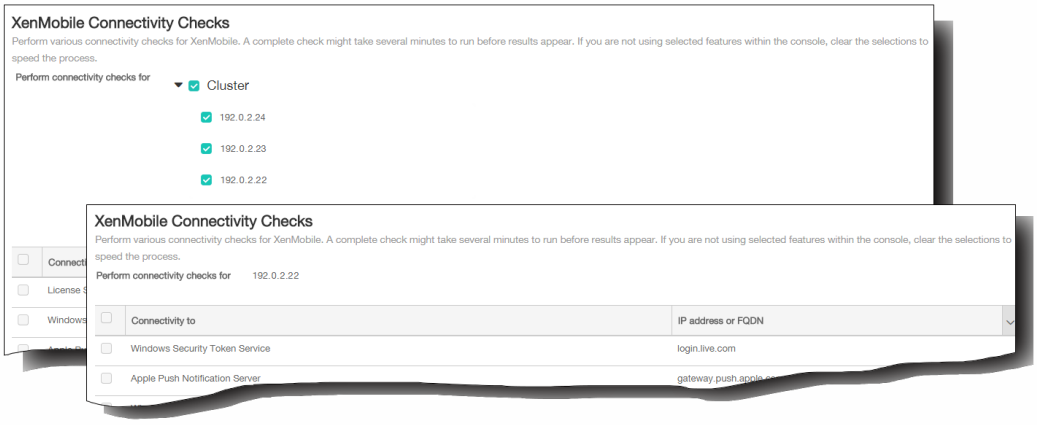
May 06, 2016

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 serez peut-être invité à entrer votre nom d'utilisateur et mot de passe.



   Un nouvel onglet de navigateur, Support XenMobile, s'ouvre. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



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. Sélectionnez un serveur dans la table Résultats du test pour afficher les résultats détaillés pour ce serveur.

Réalisation de contrôles de connectivité pour NetScaler Gateway

1. Sur la page Support, 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.

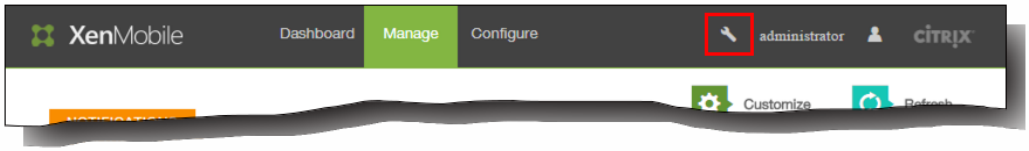
4. Tapez vos informations d'identification d'administrateur pour ce NetScaler Gateway.
   Remarque : si vous effectuez un contrôle de connectivité pour un serveur NetScaler Gateway qui est déjà ajouté, le nom d'utilisateur est renseigné.
5. Cliquez sur Ajouter. La passerelle NetScaler Gateway est ajoutée 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.

Création de packs d'assistance dans XenMobile

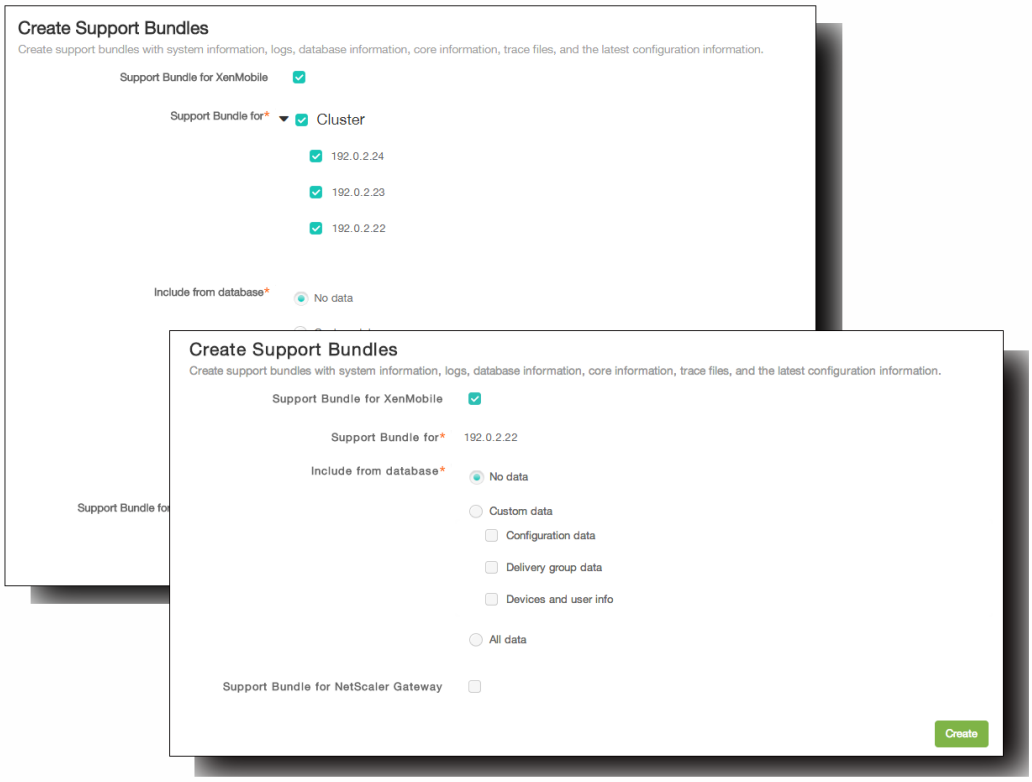
May 06, 2016

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.



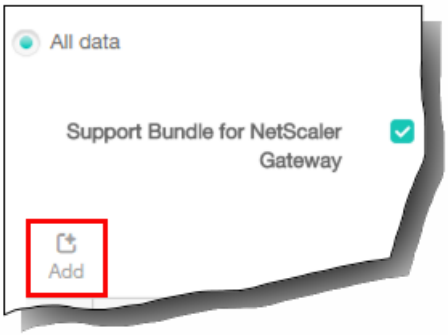
   L'assistance XenMobile s'ouvre dans un nouvel onglet de navigateur.
2. Sur la page Support, cliquez sur Créer des packs d'assistance. La page Créer des packs d'assistance s'affiche. Si votre environnement XenMobile contient des nœuds en cluster, tous les nœuds sont affichés.



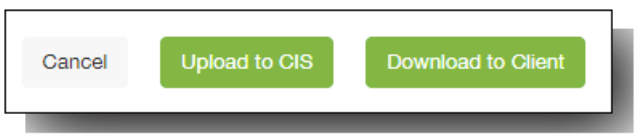
3. Assurez-vous que la case à cocher Pack d'assistance pour XenMobile est sélectionnée.
4. Si votre environnement XenMobile contient des nœuds en cluster, dans Pack d'assistance pour, vous pouvez sélectionner tous les nœuds ou une combinaison de nœuds à partir desquels extraire des données.
5. Dans Inclure depuis la base de données, effectuez l'une des opérations suivantes :

- Cliquez sur Aucune donnée.
- 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.

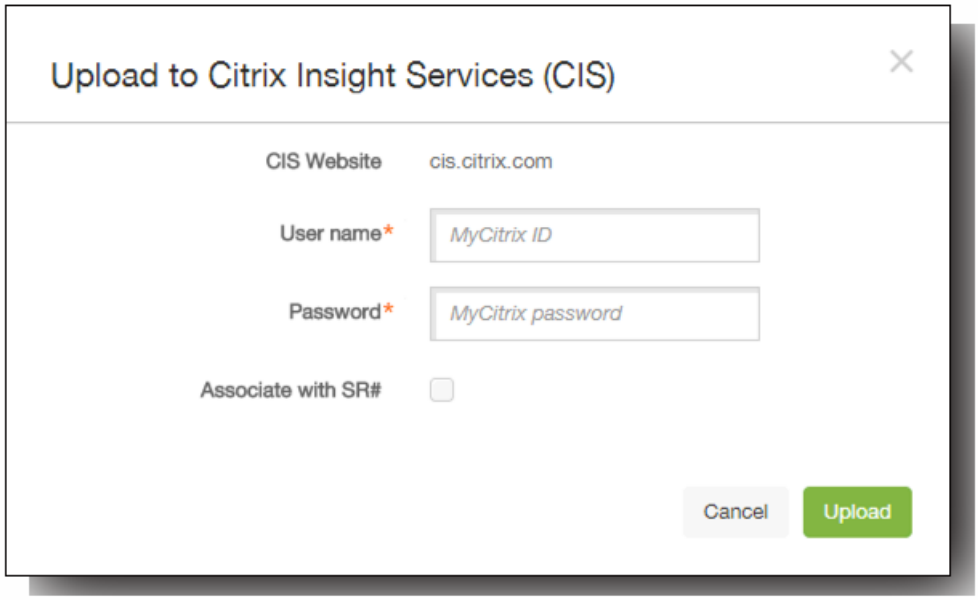


Poursuivez les procédures de **Chargement de packs d'assistance sur Citrix Insight Services** ou de **Téléchargement de packs d'assistance sur un client**.

Chargement de packs d'assistance sur Citrix Insight Services

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

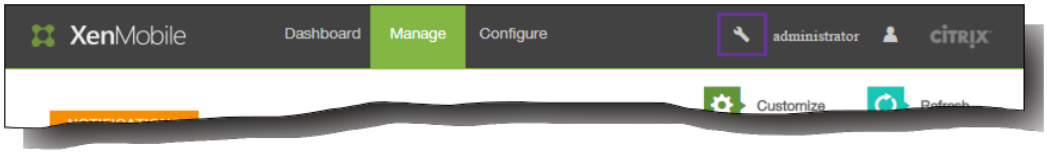
Après la création d'un pack d'assistance, vous pouvez le charger sur CIS ou le télécharger sur votre ordinateur. Si vous voulez résoudre le problème par vous-même, téléchargez le pack d'assistance sur votre ordinateur.
Sur la page Créer des packs d'assistance, cliquez sur Télécharger sur le client. Le pack est téléchargé sur votre ordinateur.

Pour afficher le fichier journal de débogage

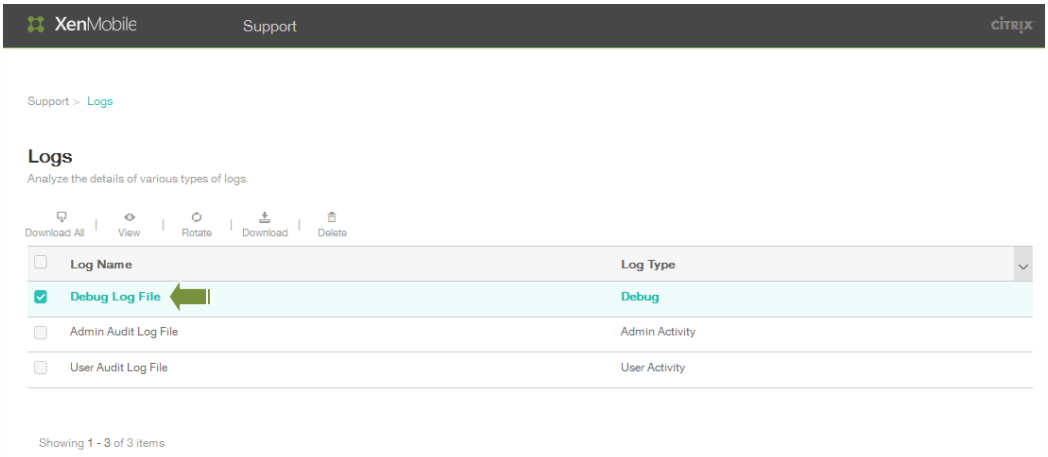
May 06, 2016

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).

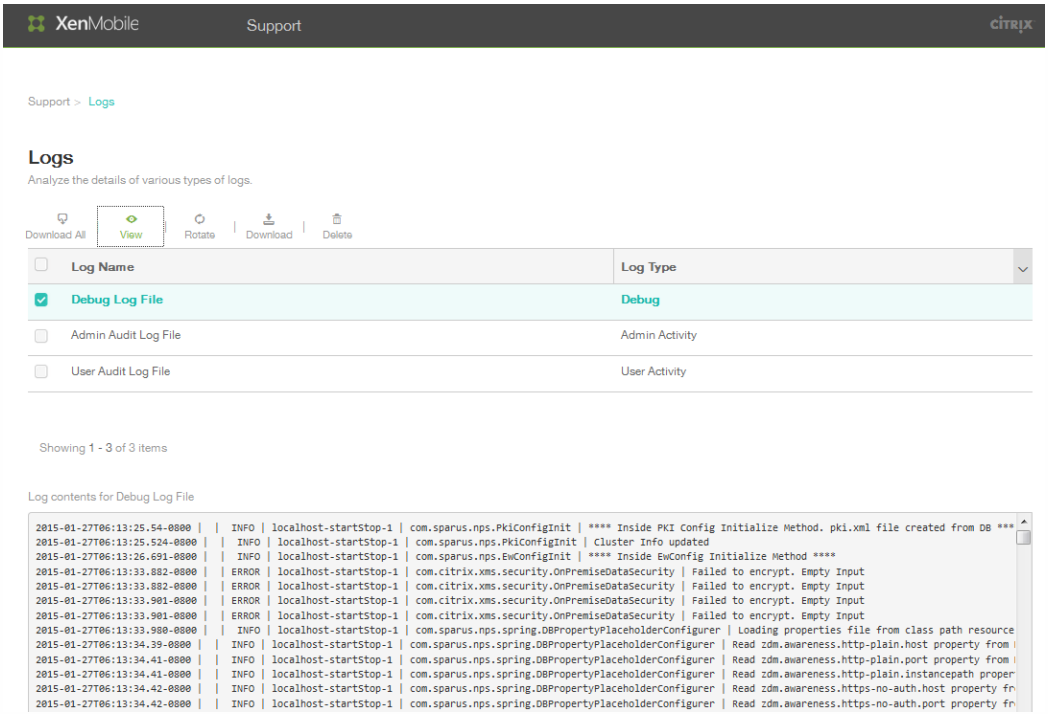
1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. L'icône de clé est disponible dans toutes les pages de la console XenMobile.



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.



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.

Pour configurer les paramètres du journal

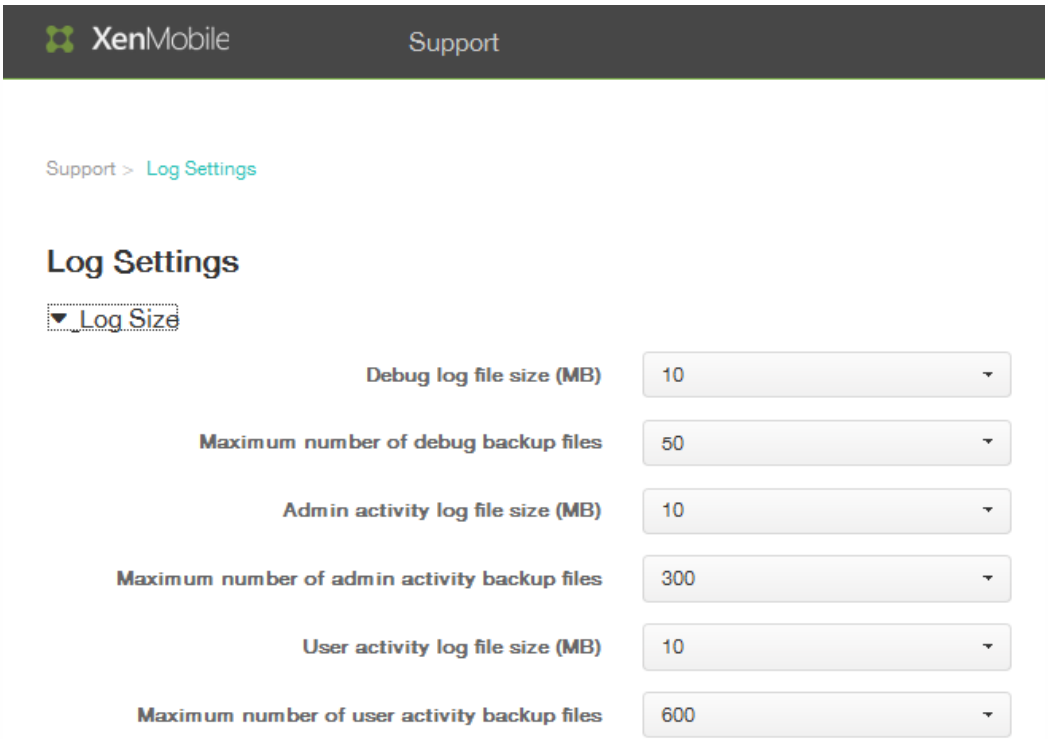
May 06, 2016

Vous pouvez configurer les paramètres du journal pour personnaliser les journaux générés par XenMobile. Dans la console XenMobile, cliquez sur Support > Paramètres du journal pour accéder aux options suivantes :

- 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 le journal des activités de l'utilisateur).
- Niveau du journal. Utilisez cette option pour modifier le nom de la classe, le nom de la sous-classe, 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. Cliquez sur Support > Paramètres du journal et développez Taille du journal.



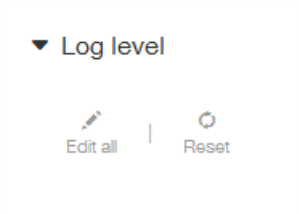
2. Dans la liste de Taille du fichier journal de débogage (Mo), sélectionnez une taille comprise entre 5 et 20 Mo pour modifier la taille maximale du fichier de débogage. Par défaut, la taille du fichier est de 10 Mo.
3. Dans la liste Nombre maximum de fichiers de sauvegarde de débogage, sélectionnez de 5 à 300 fichiers de débogage pour changer le nombre maximal de fichiers de débogage conservés sur le serveur. Par défaut, XenMobile conserve 50 fichiers de sauvegarde sur le serveur.
4. Dans la liste Taille du fichier journal des activités des administrateurs, sélectionnez une taille comprise entre 5 et 20 Mo. Par défaut, la taille du fichier est de 10 Mo.
5. Dans la liste Nombre maximum de fichiers de sauvegarde des activités des administrateurs, sélectionnez de 5 à 300 fichiers de débogage comme nombre maximal de fichiers de sauvegarde des activités des administrateurs conservés sur le

serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.

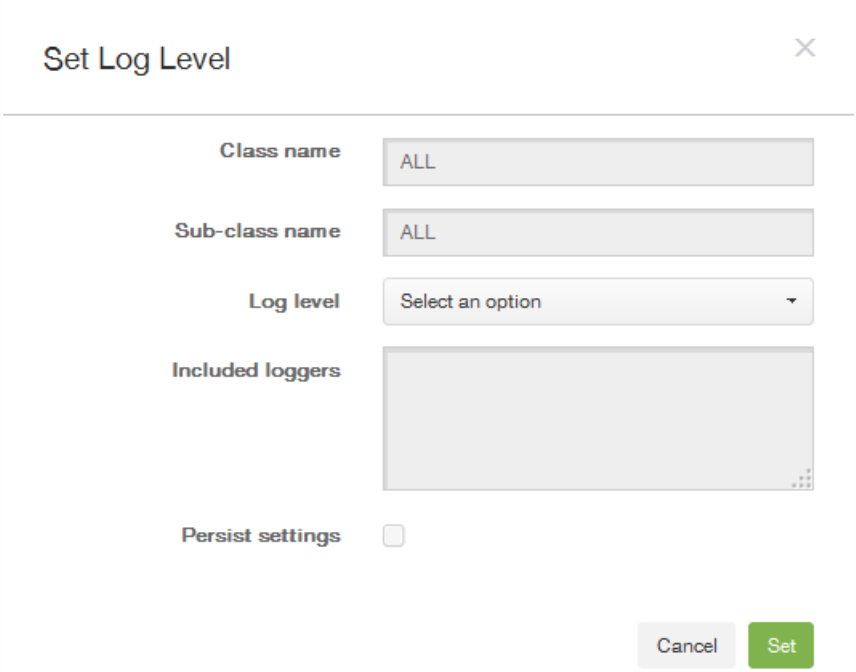
6. Dans la liste Taille du fichier journal des activités des utilisateurs, sélectionnez une taille comprise entre 5 et 20 Mo. Par défaut, la taille du fichier est de 10 Mo.
7. Dans la liste Nombre maximum de fichiers de sauvegarde des activités des administrateurs, sélectionnez de 5 à 300 fichiers de débogage comme nombre maximal de fichiers de sauvegarde des activités des administrateurs conservés sur le serveur. Par défaut, XenMobile conserve 300 fichiers de sauvegarde sur le serveur.

Pour configurer les options de niveau de journalisation

1. Cliquez sur Support > Paramètres du journal et développez Niveau de journalisation pour afficher les options de configuration. Cliquez sur Tout modifier pour configurer les éléments du niveau de journalisation.



L'écran des Définir le niveau du journal s'affiche.

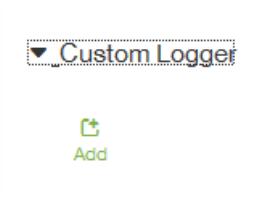


2. Entrez le Nom de la classe. Par défaut, ce champ est défini sur Toutes
3. Entrez le Nom de la sous-classe. Par défaut, ce champ est défini sur Toutes
4. Dans la liste Niveau de journalisation, sélectionnez un niveau de journalisation. Les niveaux de journalisation pris en charge incluent Fatal Erreur, Avertissement, Info, Débogage, Trace, ou Désactivé. Le champ Enregistreur d'événements inclus affiche les niveaux de journalisation configurés pour chaque classe configurée.
5. Si vous souhaitez conserver les paramètres de niveau de journalisation, sélectionnez la case à cocher Conserver les paramètres.

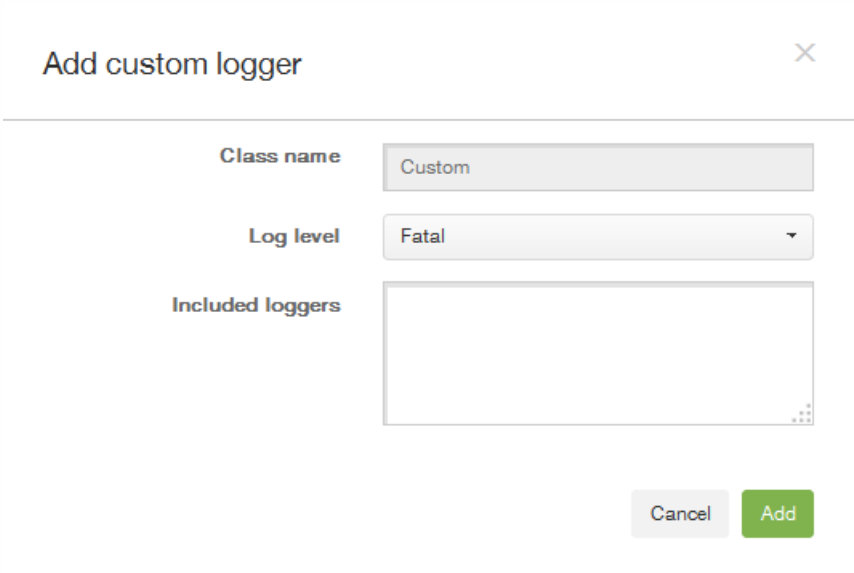
6. Cliquez sur Définir pour valider vos modifications.

Pour ajouter un enregistreur d'événements personnalisé

1. Pour ajouter un Enregistreur d'événements personnalisé, cliquez sur Ajouter.



L'écran Ajouter un enregistreur d'événements personnalisé s'affiche.

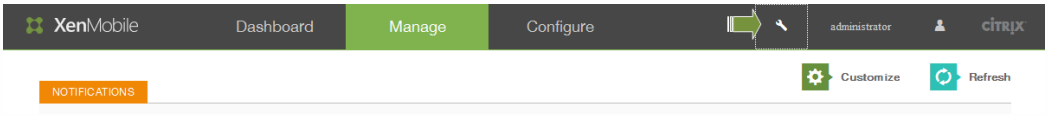


2. Spécifiez un Nom de classe.
3. Dans la liste Niveau de journalisation, sélectionnez un niveau de journalisation. Les niveaux de journalisation pris en charge incluent Fatal Erreur, Avertissement, Info, Débogage, Trace, ou Désactivé. Le champ Enregistreur d'événements inclus affiche les niveaux de journalisation configurés pour chaque classe configurée.
4. Cliquez sur Ajouter.

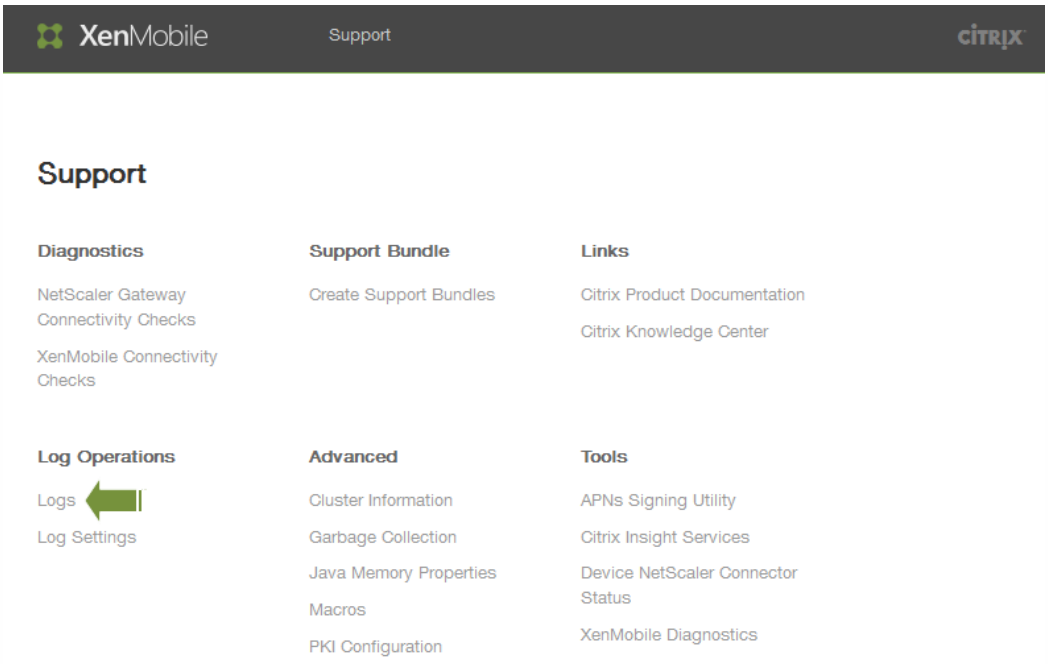
Visualisation et analyse des fichiers journaux dans XenMobile

May 06, 2016

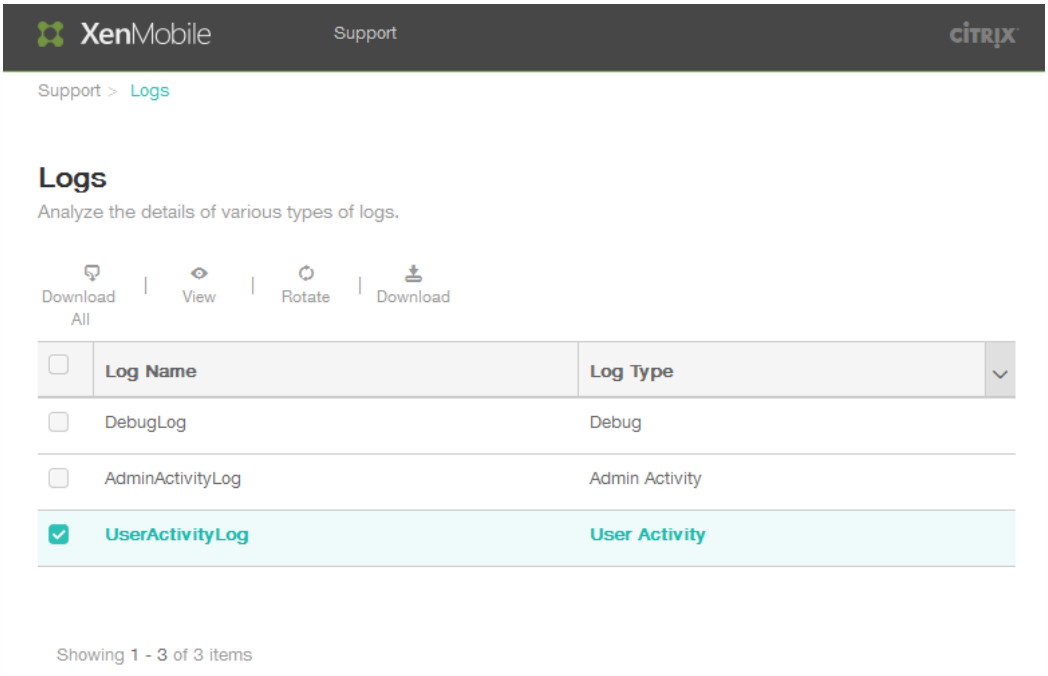
1. Dans la console XenMobile, cliquez sur l'icône de la clé dans le coin supérieur droit. La page Support s'ouvre dans une nouvelle fenêtre du navigateur.



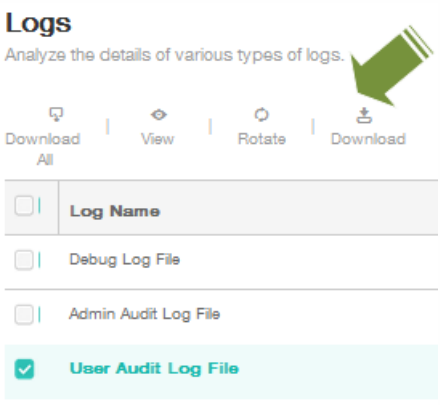
2. Sous Opérations du journal, cliquez sur **Journaux**. L'écran **Journaux** s'affiche. Des journaux individuels apparaissent dans un tableau.



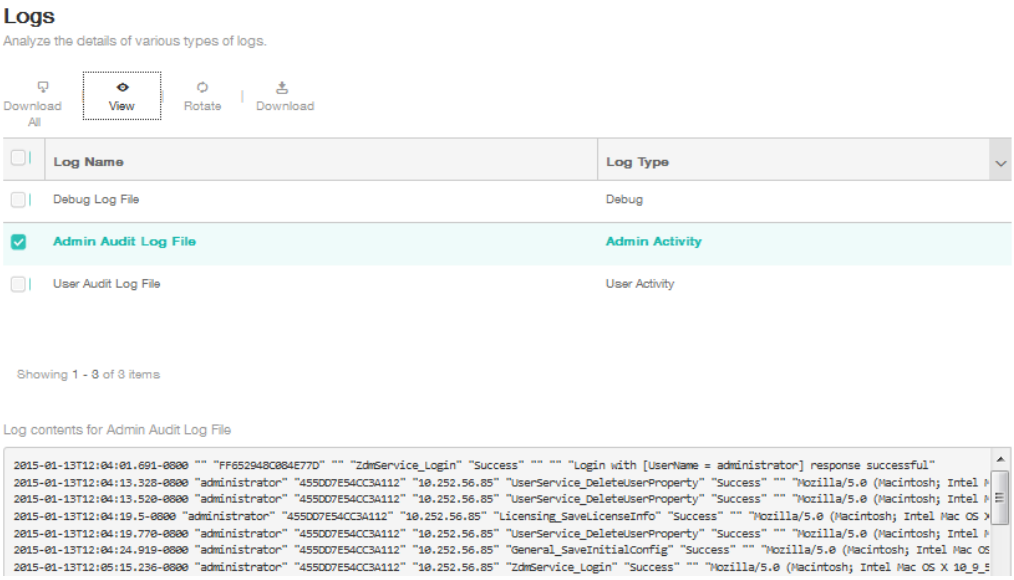
3. Sélectionnez le journal que vous souhaitez visualiser. Un journal de débogage contient des informations utiles pour le support Citrix ; il contient des informations telles que des messages d'erreur et des actions liées au serveur. Les journaux d'activités des utilisateurs affichent des informations relatives à chaque utilisateur configuré. L'écran **Journaux** s'affiche. Des journaux individuels apparaissent dans un tableau.



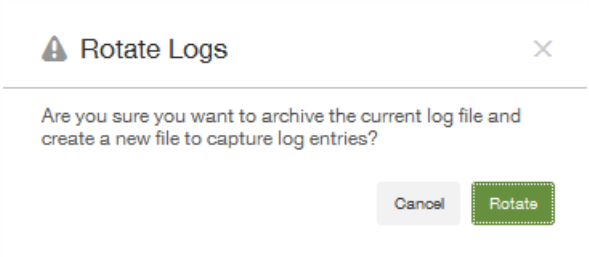
4. Utilisez les actions en haut du tableau pour effectuer les opérations suivantes :
   - Tout télécharger : la console télécharge tous les journaux présents sur le système (y compris les journaux de débogage, d'activité des utilisateurs/administrateurs, de serveur, etc.). Le bouton Télécharger permet d'enregistrer uniquement les journaux sélectionnés ; il permet également de télécharger les journaux archivés).



   - Afficher : affiche le contenu du journal en dessous du tableau.



- Supprimer : supprime de manière définitive un fichier journal sélectionné.
- 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.



Options d'interface de ligne de commande XenMobile

May 06, 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.

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

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 :

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 :

---

[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]

API XenMobile 10

May 06, 2016

Vous pouvez utiliser les API des services Web suivants dans XenMobile 10 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

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

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

XenMobile Mail Manager 10

May 06, 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.

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.

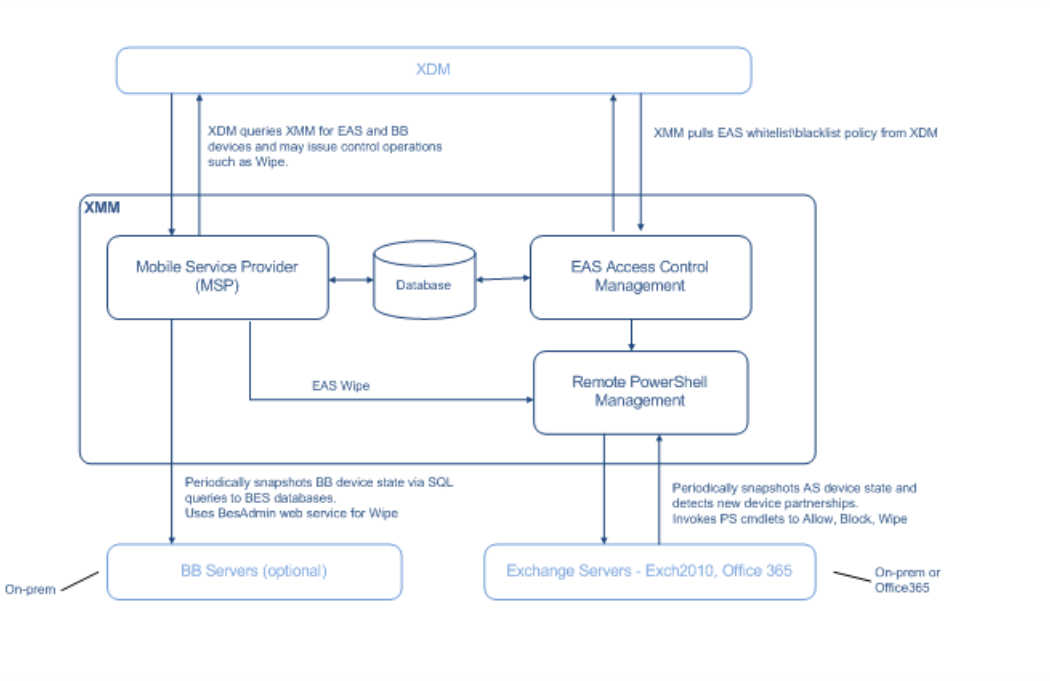
Journalisation

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.

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.

Configuration système requise et conditions préalables

May 06, 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.

- 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

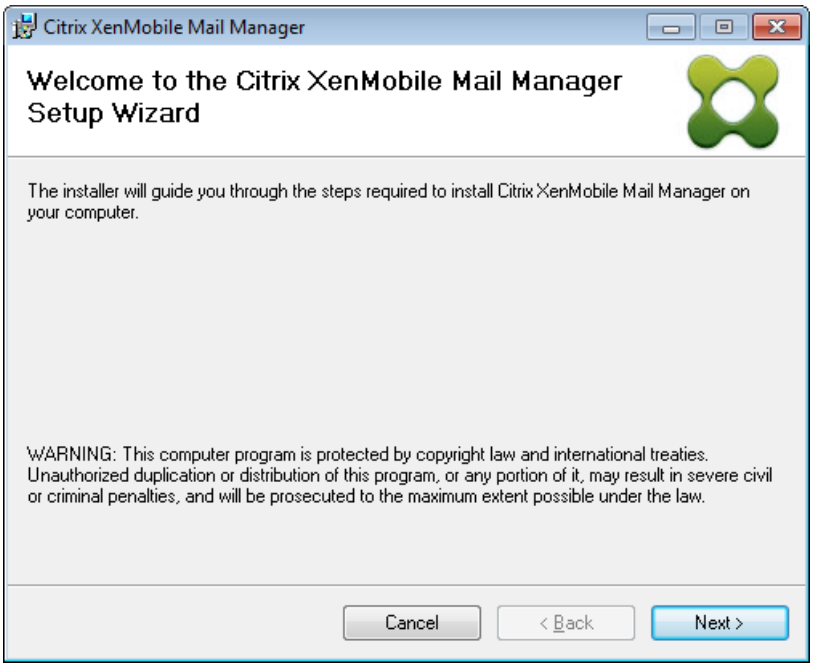
- **Autorisations**. Le contrôle d'accès basé sur rôle (RBAC) Exchange n'est pas couvert dans cette documentation. Cela dit, les informations d'identification spécifiées dans l'interface utilisateur de la console Exchange Configuration doivent, au minimum, être en mesure de se connecter à Office 365 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.

Installation et configuration

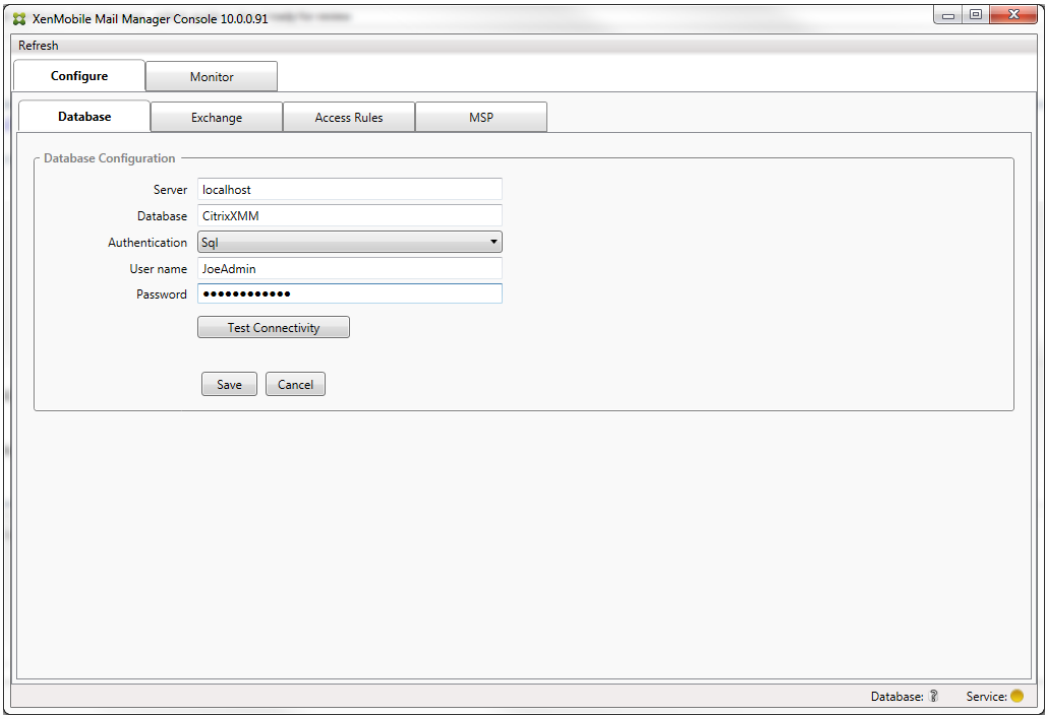
May 06, 2016

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.

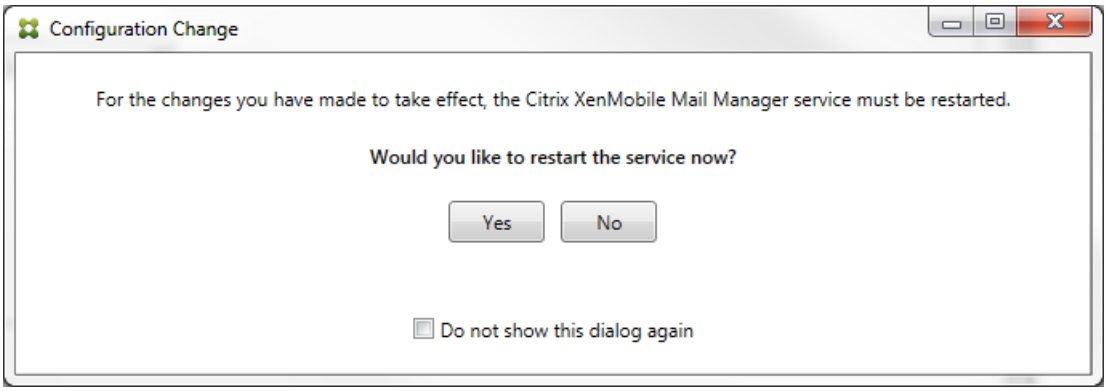


2. Dans le menu Démarrer, ouvrez XenMobile Mail Manager.
3. Configurez les propriétés de base de données suivantes :
   1. Sélectionnez l'onglet Configure > Database.
   2. Entrez le nom du serveur SQL (localhost par défaut).
   3. Conservez la base de données par défaut CitrixXmm.
   4. Sélectionnez 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.

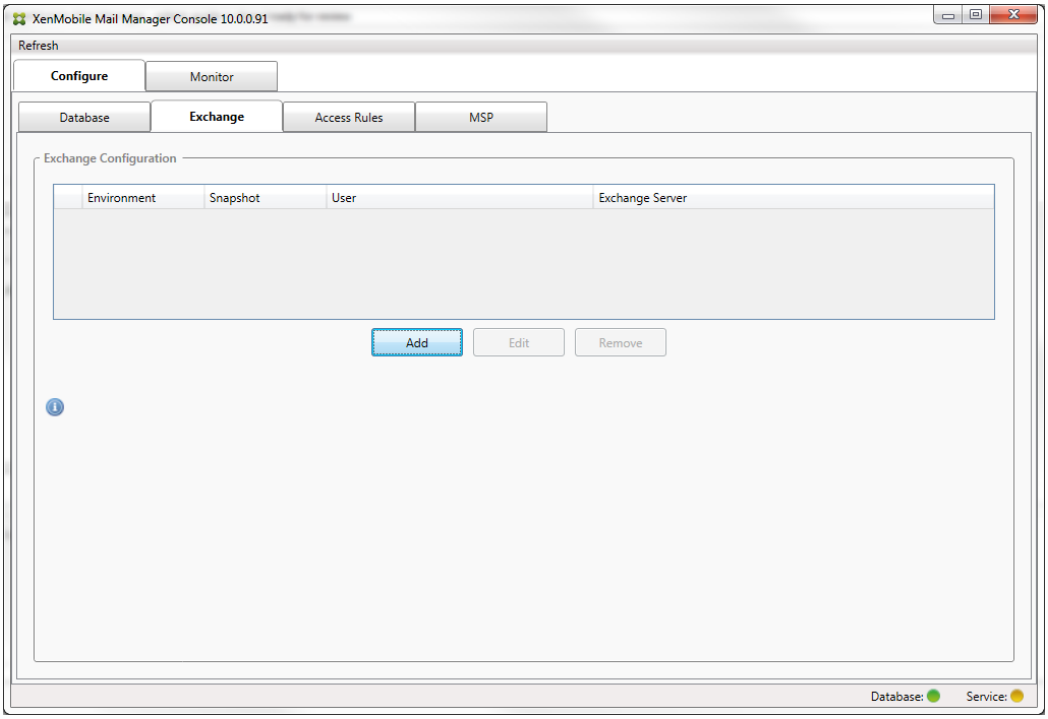


5. Cliquez sur Test Connectivity pour vérifier qu'une connexion peut être établie avec le serveur SQL, puis cliquez sur Save.

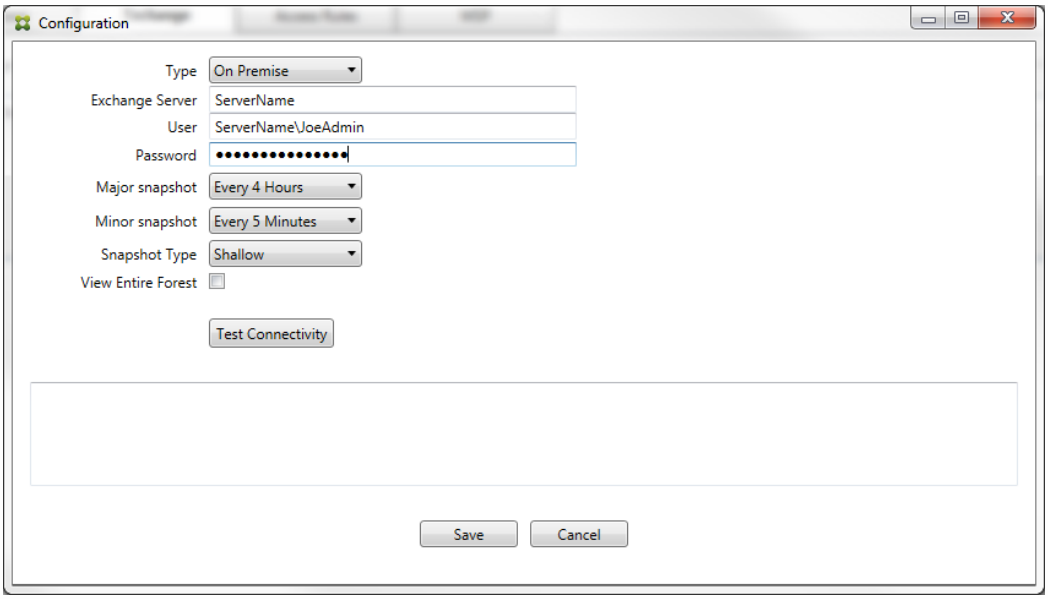
4. Un message vous invite à redémarrer le service. Cliquez sur Oui.



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.



3. Cliquez sur Add.
4. Sélectionnez le type d'environnement de serveur Exchange, soit On Premise soit Office 365.

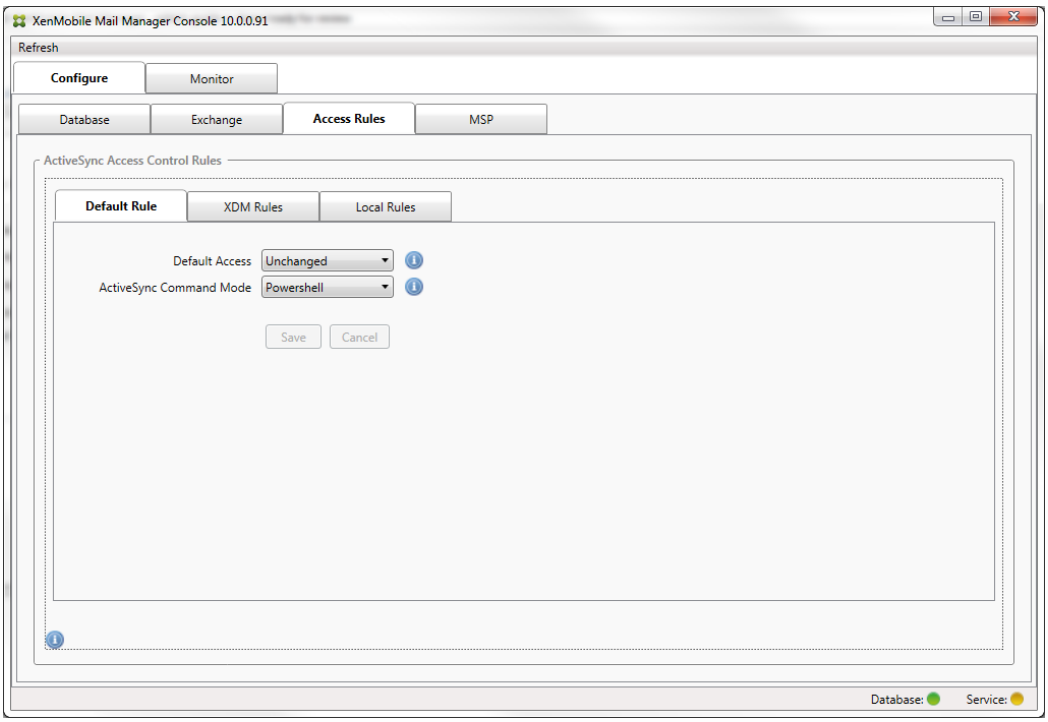


5. Si vous sélectionnez On Premise, entrez le nom du serveur Exchange qui sera utilisé pour les commandes PowerShell à distance.
6. Entrez le nom d'utilisateur d'une identité Windows disposant des droits appropriés sur le serveur Exchange comme indiqué dans la section Configuration requise.
7. Entrez 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

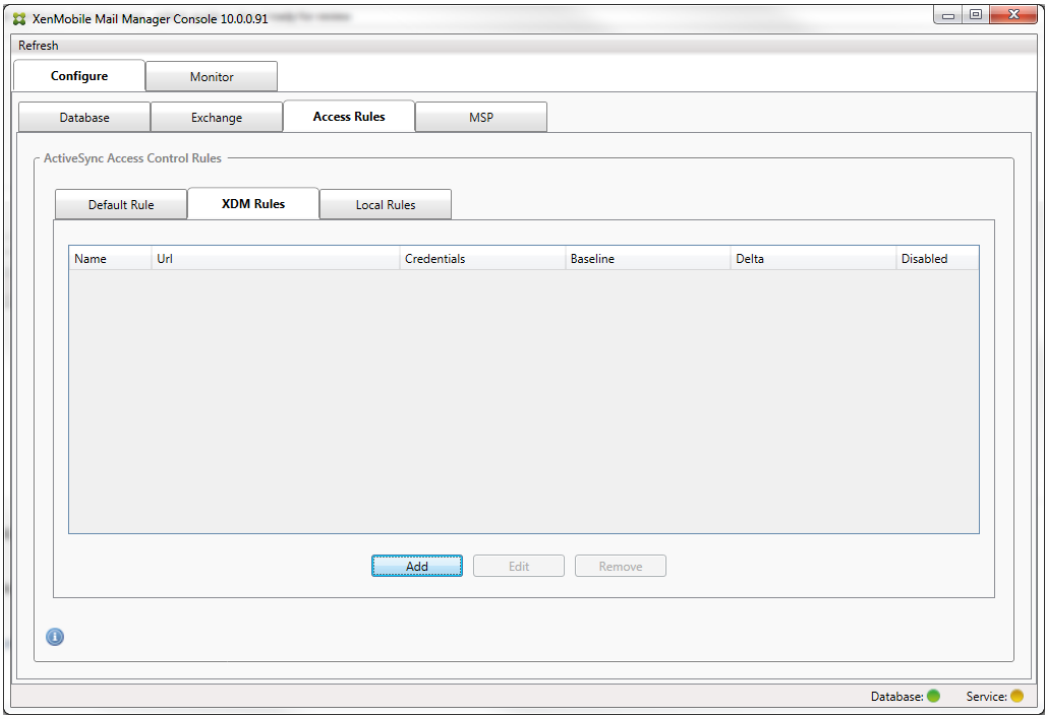
exécuter toutes les fonctions de contrôle d'accès Exchange ActiveSync de XenMobile Mail Manager. Les instantanés Deep peuvent prendre beaucoup plus de temps et sont uniquement nécessaires si Mobile Service Provider est activé pour ActiveSync (ce qui permet à Device Manager d'interroger les appareils 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.

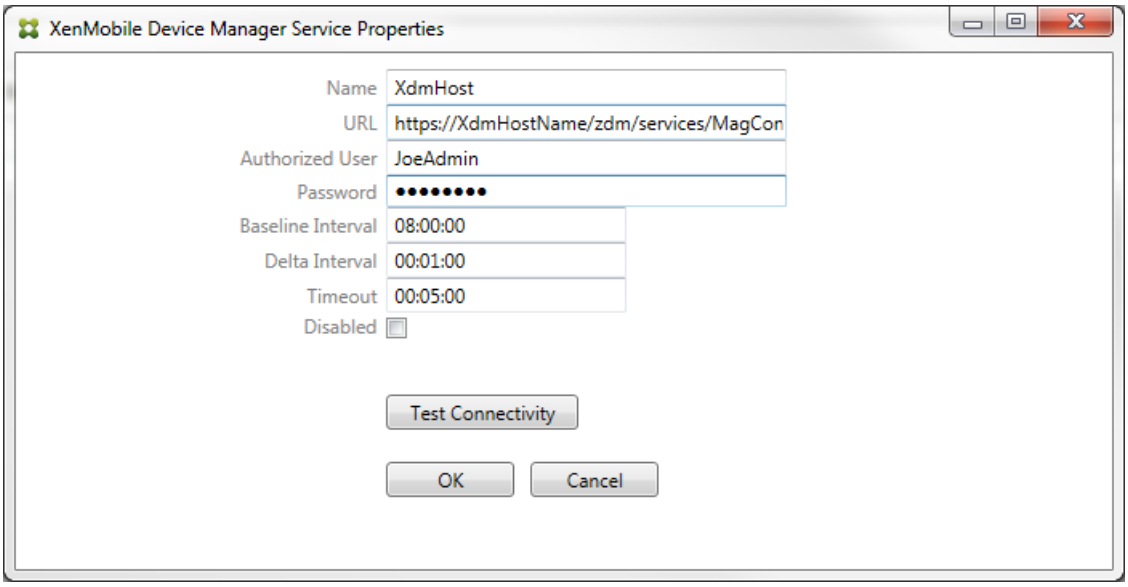
6. Configurez les règles d'accès :
    1. Sélectionnez l'onglet ConfigureAccess Rules.



    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.



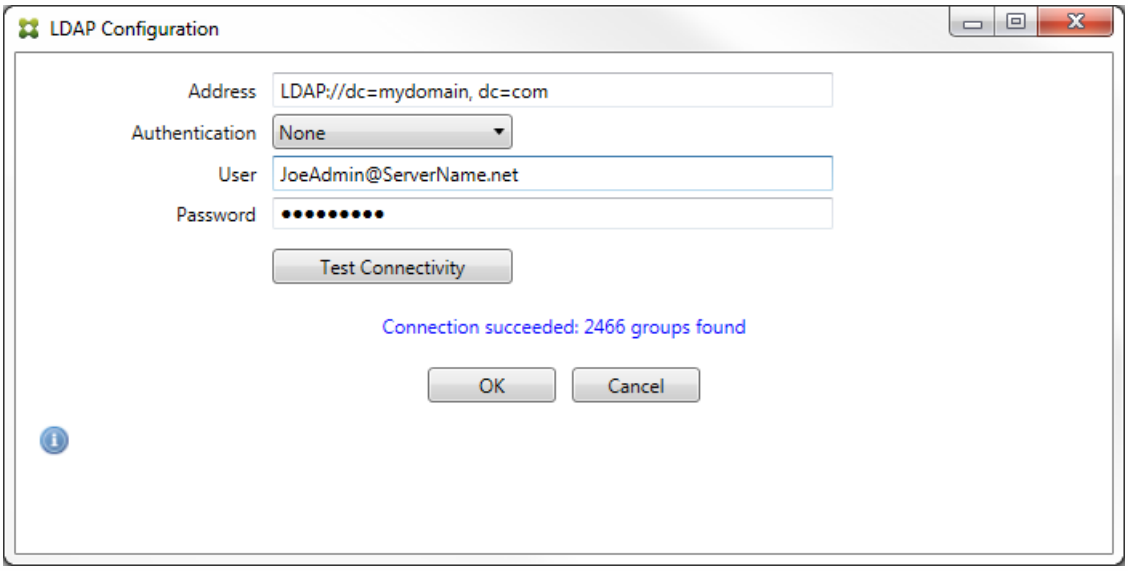
1. Cliquez sur Ajouter.
2. Entrez un nom pour les règles XDM, comme XdmHost.



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.

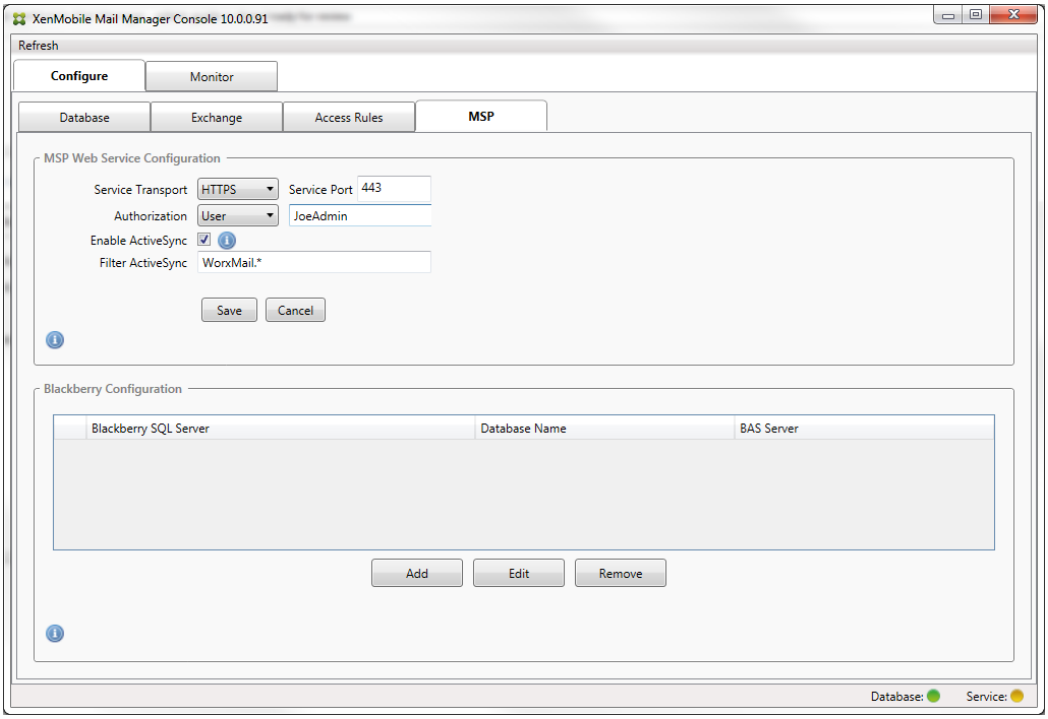
8. Cliquez sur l'onglet Local Rules.

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.



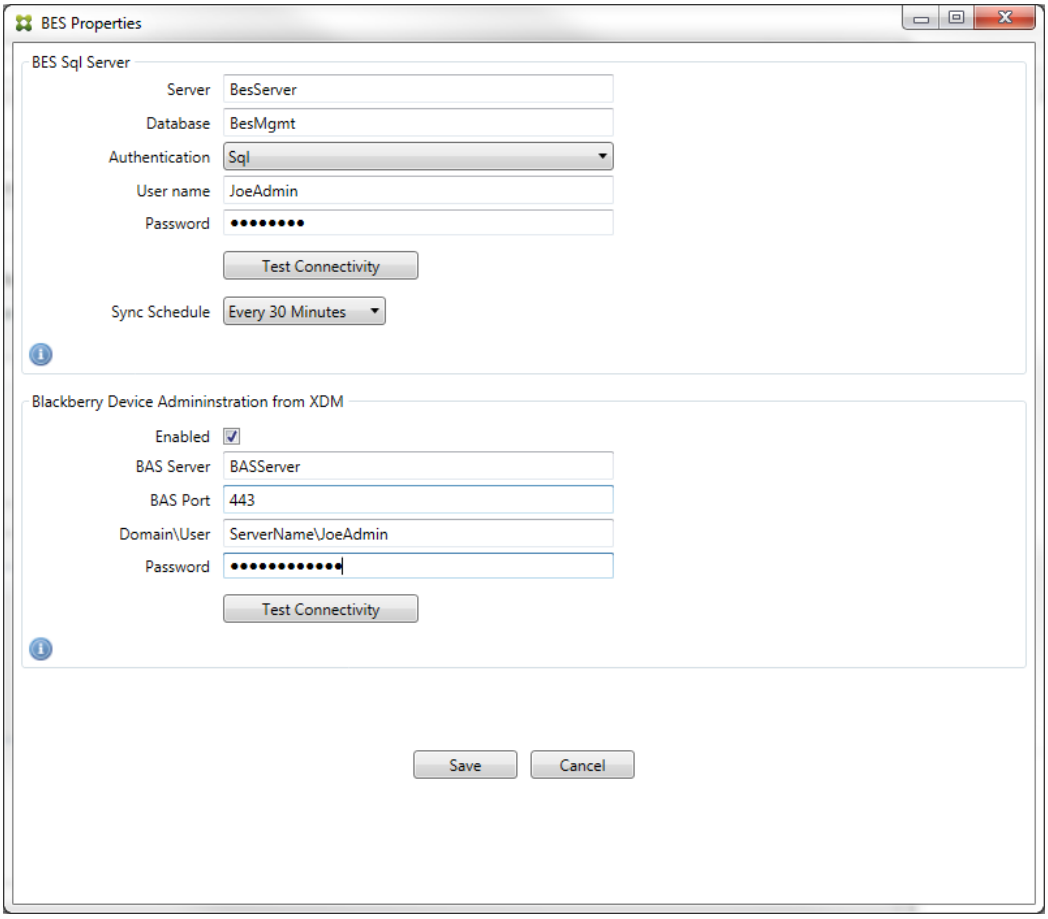
2. Vous pouvez ajouter des règles locales basées sur ActiveSync Device ID, Device Type, AD Group, User ou User Agent. Sélectionnez le type approprié dans la liste. Pour de plus amples informations, consultez la section Règles de contrôle d'accès à XenMobile Mail Manager.
3. Tapez le texte ou les fragments 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.



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 Add.
    2. Entrez le nom du serveur BES SQL.



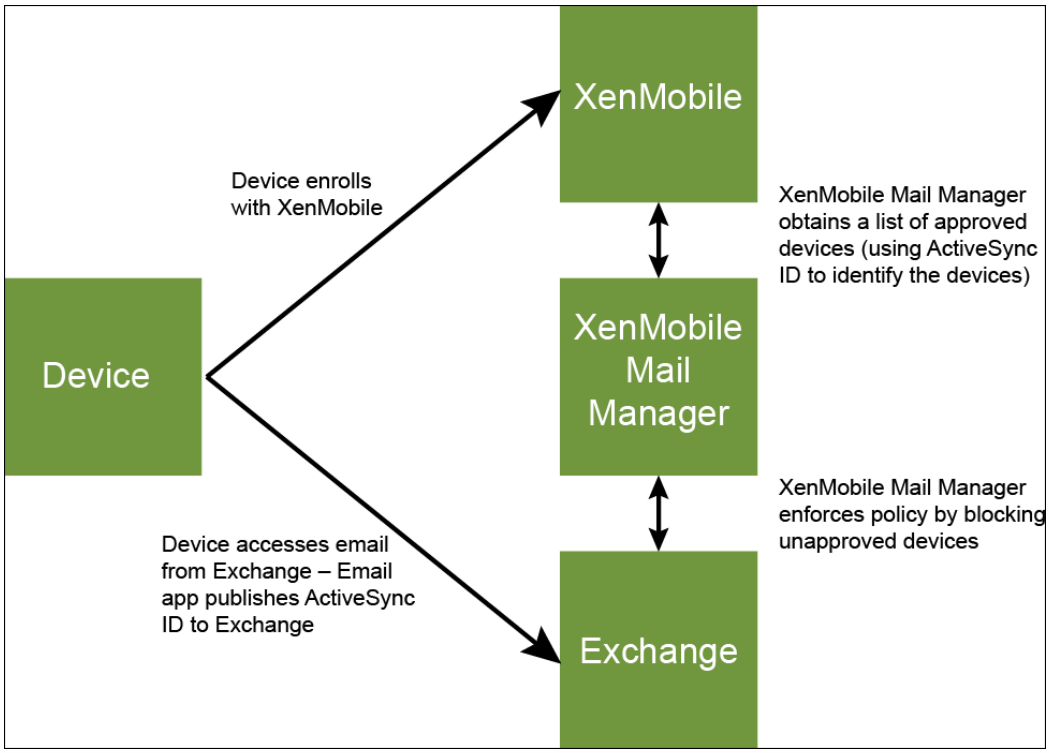
3. Tapez le nom de la base de données de gestion BES.
4. Sélectionnez le mode Authentication. Si vous sélectionnez l'authentification intégrée Windows, le compte d'utilisateur du service XenMobile Mail Manager est le compte utilisé pour se connecter au serveur BES SQL.
   Remarque : si vous choisissez 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 Save.

Application des stratégies de messagerie avec des ID ActiveSync

May 06, 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

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.

Règles de contrôle d'accès

May 06, 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,

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 :

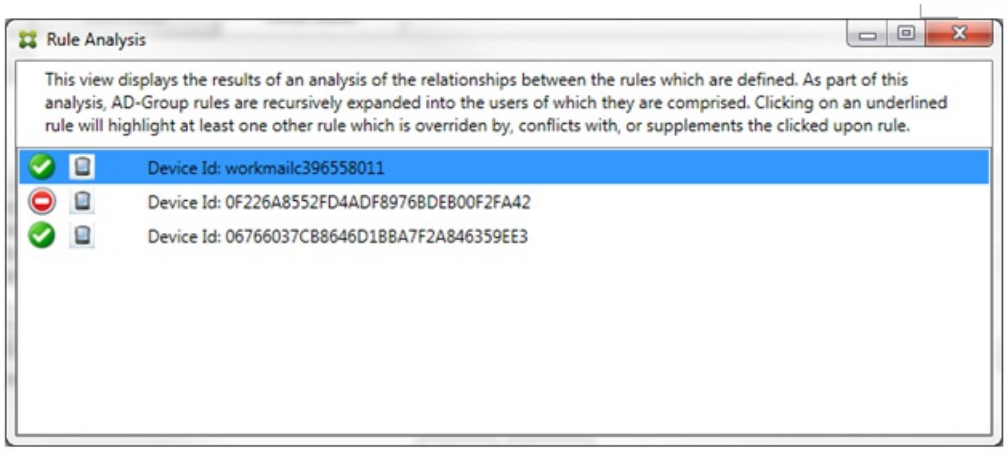
- **Règle absolue**. Une substitution se produit lorsque plusieurs règles s'appliquent à un même appareil. Étant donné que les règles sont évaluées par priorité dans la liste, la ou les dernières instances de règle devant s'appliquer peuvent ne jamais être évaluées.
- **Règle conflictuelle**. Un conflit 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

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.

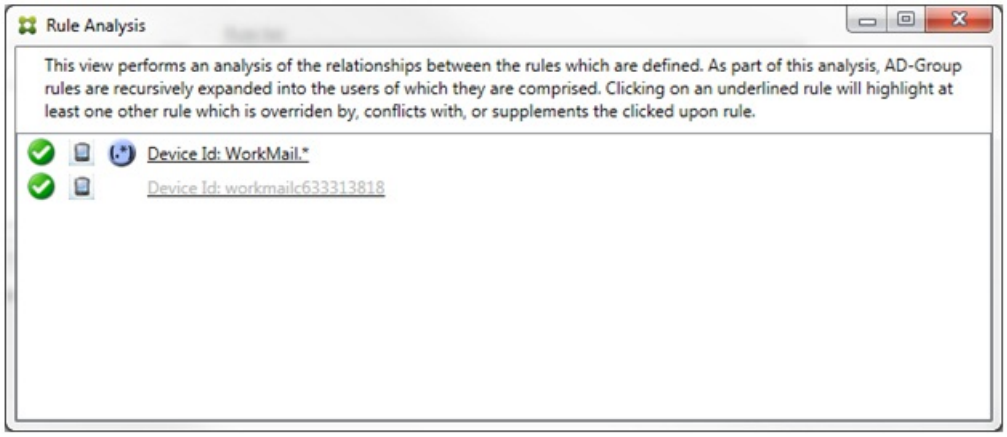
- **Règle secondaire**. Une règle secondaire est liée d'une certaine manière à la règle principale que ce soit via une relation de remplacement, de conflit ou supplémentaire. Les règles sont indiquées visuellement par une bordure en pointillés. Pour chaque règle principale, il peut y avoir une ou plusieurs 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

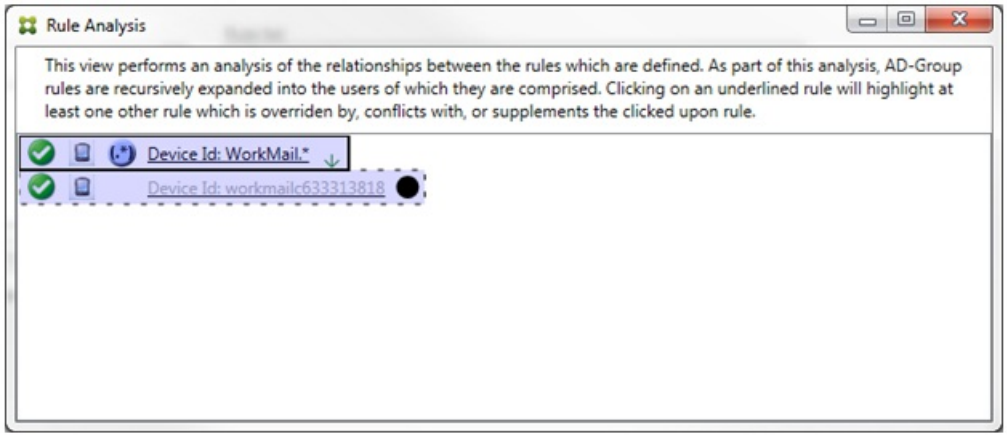
Lorsqu'il n'y a aucun conflit, remplacement, ou complément, il n'y a pas d'entrées soulignées dans la boite de dialogue Rule Analysis. Par exemple, cliquer sur des éléments n'a pas d'impact, les éléments normaux sélectionnés seront mis en évidence.



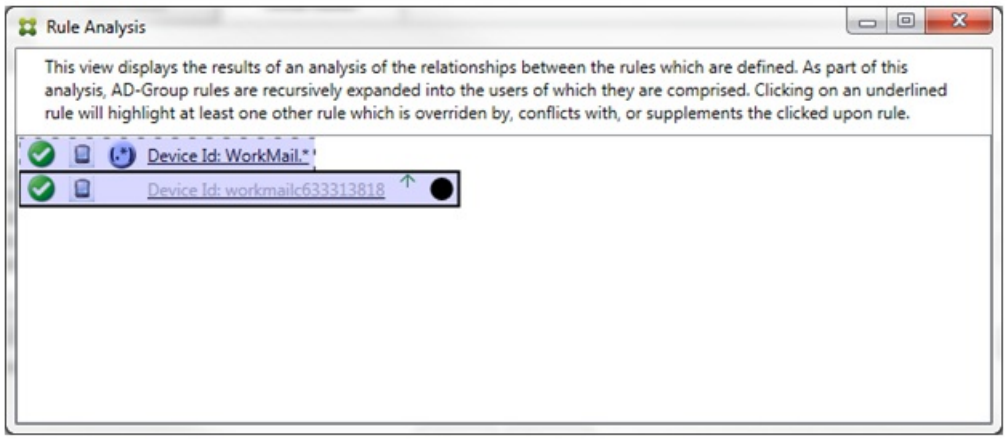
Lorsqu'une substitution se produit, au moins deux règles sont soulignées : la règle principale et la ou les règles secondaires. Au moins une règle secondaire s'affichera dans une police plus claire pour indiquer que la règle a été remplacée par une règle de priorité plus élevée. Vous pouvez cliquer sur 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 :



Lorsque vous cliquez sur la règle prioritaire, la boîte de dialogue se présente comme suit :

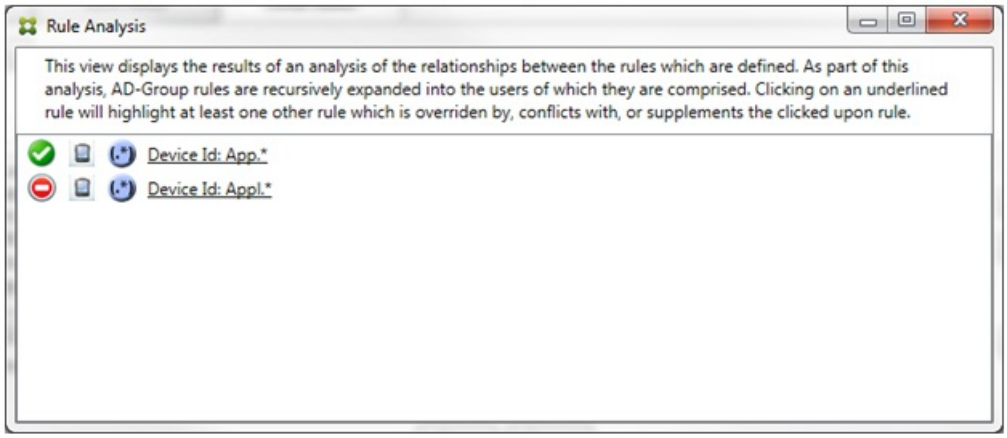


Dans cet exemple, la règle d'expression régulière WorkMail.* est la règle principale (indiquée par une bordure pleine) et la règle normale workmailc633313818 est une règle secondaire (indiquée par une bordure en pointillés). Le point noir à côté de la règle secondaire est une indication visuelle qui 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 :

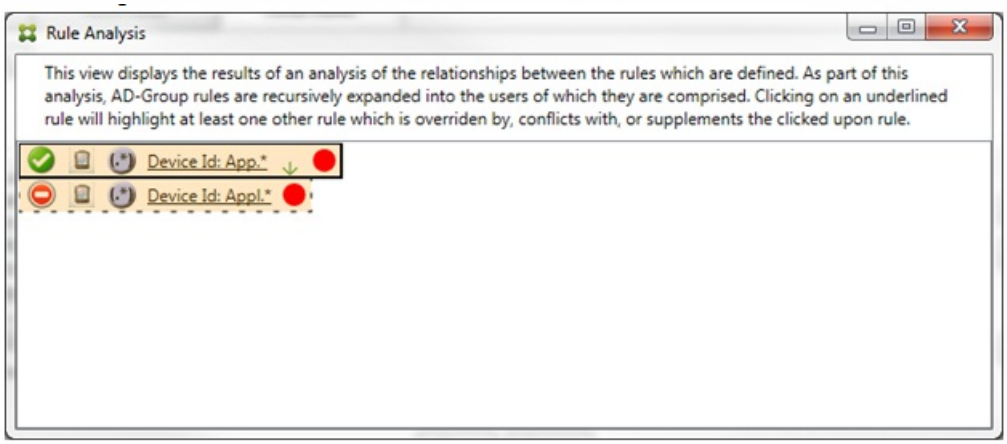


Dans l'exemple précédent, la règle d'expression régulière WorkMail.* est la règle secondaire (indiquée par une bordure en pointillés) et la règle normale workmailc633313818 est une règle principale (indiquée par une bordure pleine). Pour cet exemple simple, il n'y a pas grande différence. Pour un exemple 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 :

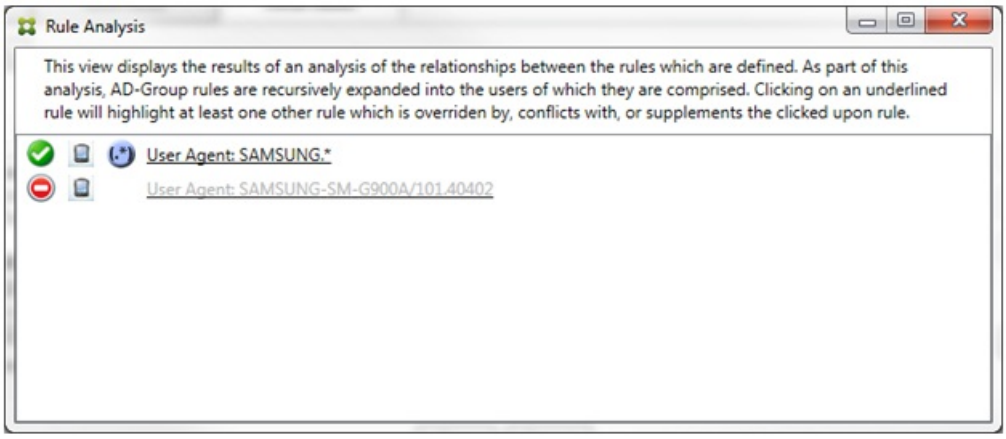


En inspectant les deux règles d'expressions régulières, il est évident que la première règle autorise tous les appareils avec un ID d'appareil contenant « App » et que la deuxième règle refuse tous les appareils avec un ID d'appareil contenant « Appl ». En outre, même si la deuxième règle refuse tous 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 :



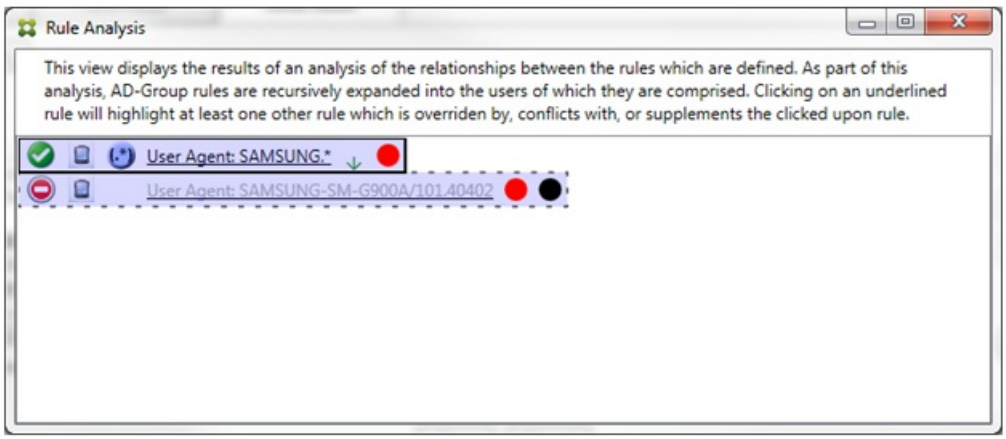
Dans le cas précédent, la règle principale (règle d'expression régulière App.*) et la règle secondaire (règle d'expression régulière Appl.*) sont toutes deux affichées en jaune. Il s'agit simplement d'une indication visuelle vous alertant du fait que vous avez appliqué plus d'une règle d'expression régulière 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.

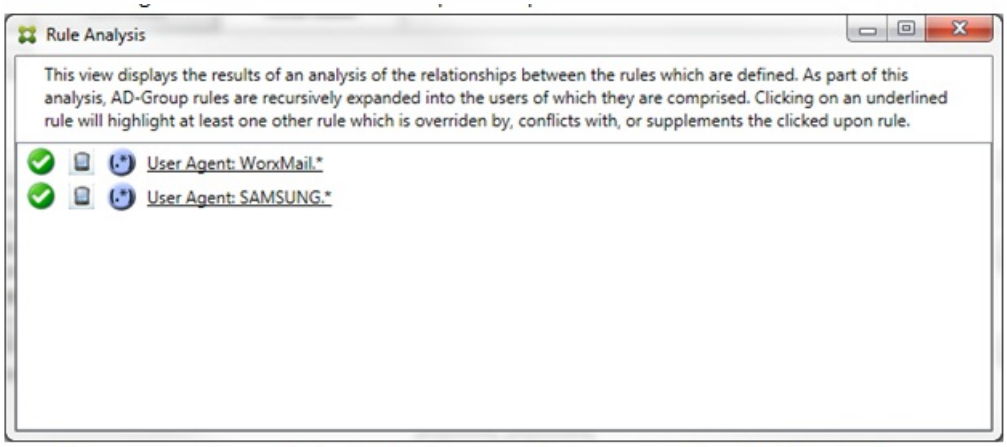
Après avoir cliqué sur la règle d'expression régulière, la boîte de dialogue se présente comme suit :



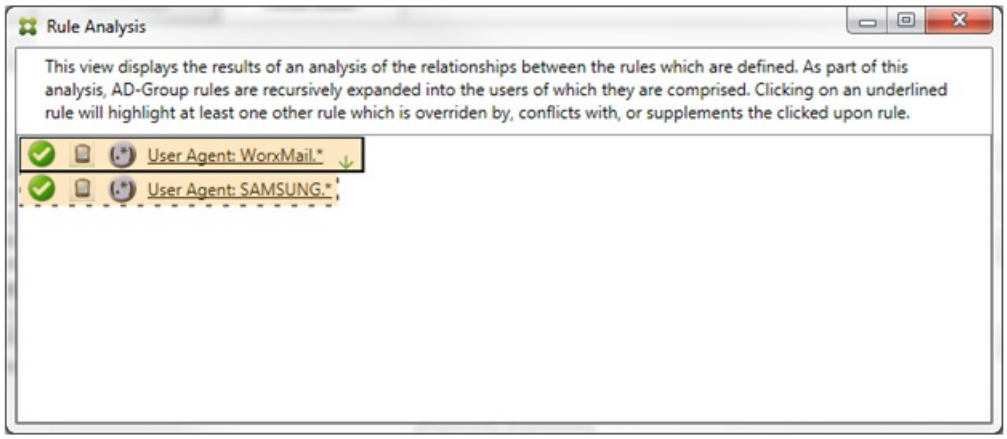
La règle principale (règle d'expression régulière SAMSUNG.*) est suivie d'un point rouge indiquant qu'elle entre en conflit avec

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 :



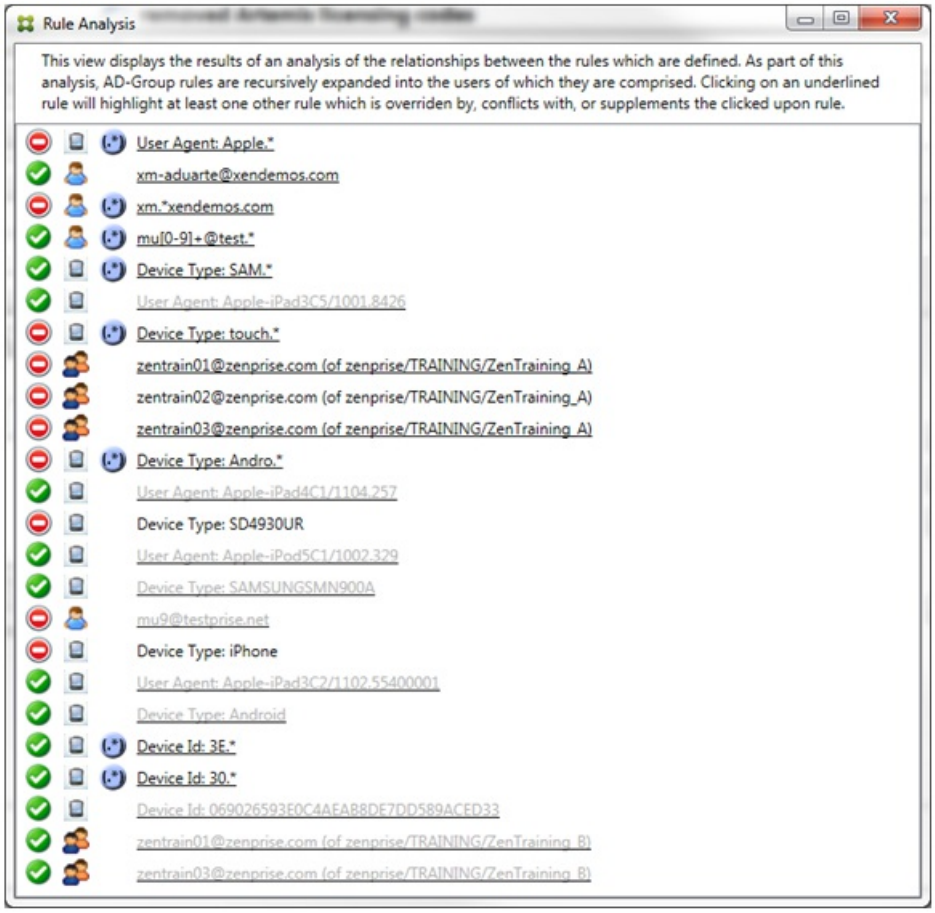
L'inspection visuelle révèle facilement que les deux règles sont des règles d'expressions régulières qui s'appliquent toutes les deux au champ ActiveSync device ID dans XenMobile Mail Manager. Après avoir cliqué sur la première règle, la boîte de dialogue se présente comme suit :



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.

Exemple d'expression complexe

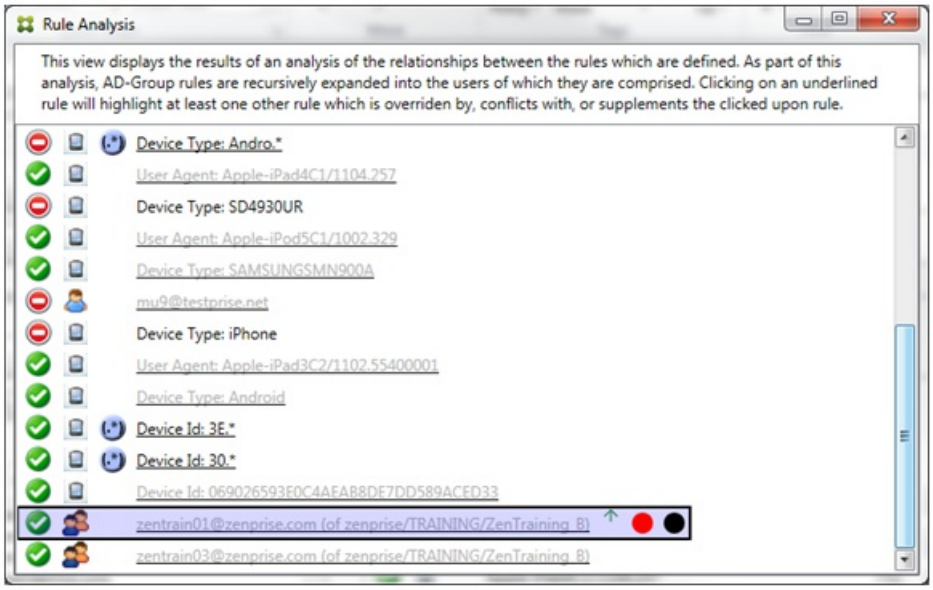
De nombreux remplacements, conflits ou compléments sont susceptibles de se produire, c'est pourquoi il est impossible de fournir des exemples couvrant tous les scénarios envisageables. L'exemple suivant explique ce qu'il ne faut pas faire, et sert aussi à illustrer toute la portée de la présentation 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.

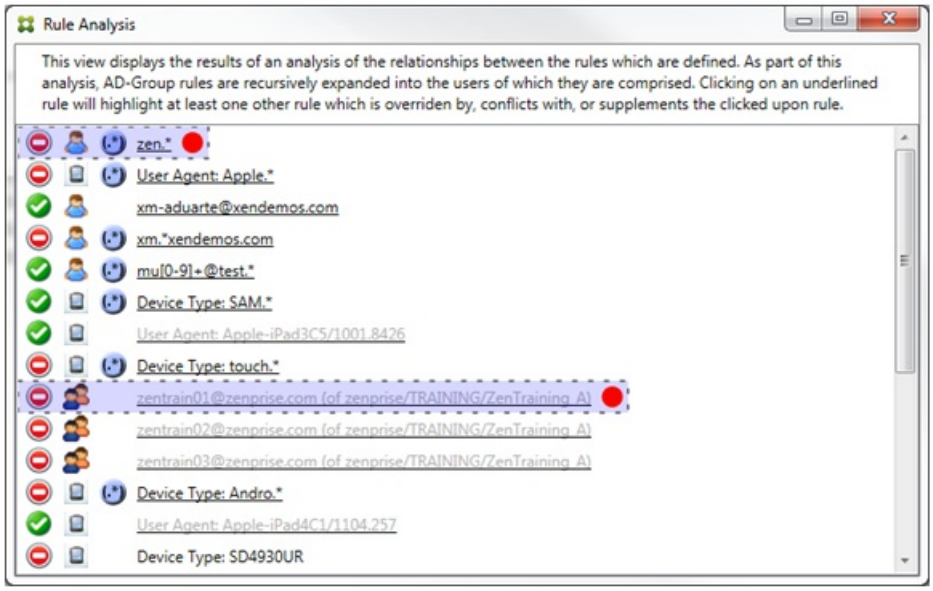
Exemple 1 : cet exemple explique pourquoi zentrain01@zenprise.com a été remplacée.



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.

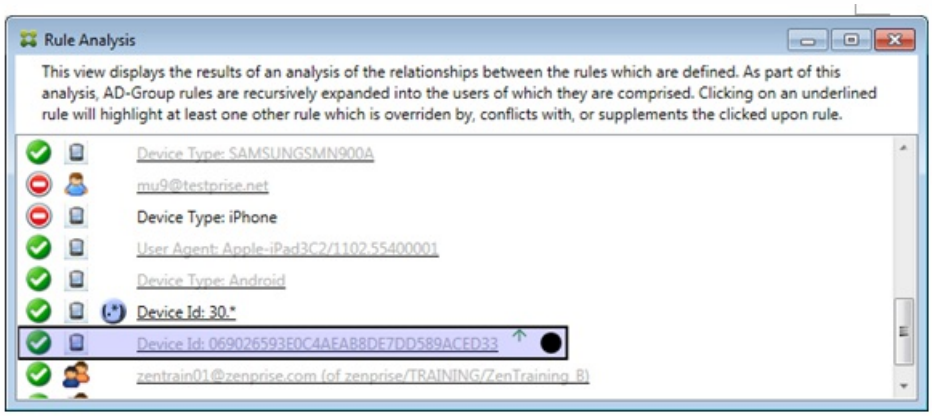
Si vous faites défiler vers le haut, vous pouvez voir ce qui suit :



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,

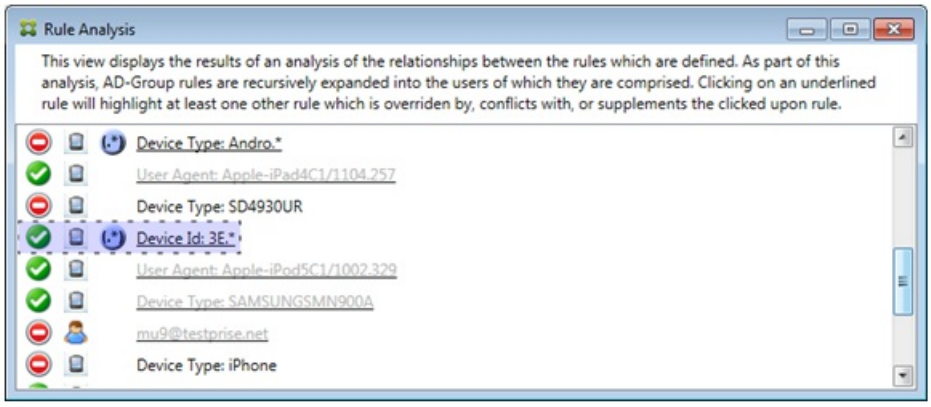
la règle de groupe Active Directory ZenTraining A contient l'utilisateur zentrain01@zenprise.com et la règle de groupe Active Directory ZenTraining B contient aussi l'utilisateur zentrain01@zenprise.com. Toutefois, étant donné que la règle secondaire a une priorité plus élevée que la règle principale, 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.

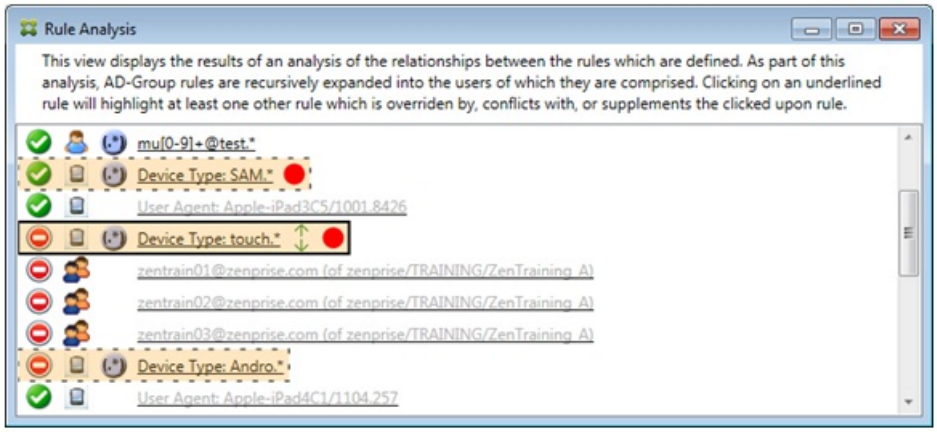


Dans ce cas, une seule règle secondaire remplace la règle principale : la règle d'expression régulière d'ID d'appareil ActiveSync 3E.* Comme l'expression régulière 3E.* correspond à 069026593E0C4AEAB8DE7DD589ACED33, la règle ne sera jamais évaluée.

Comment analyser un supplément et un conflit

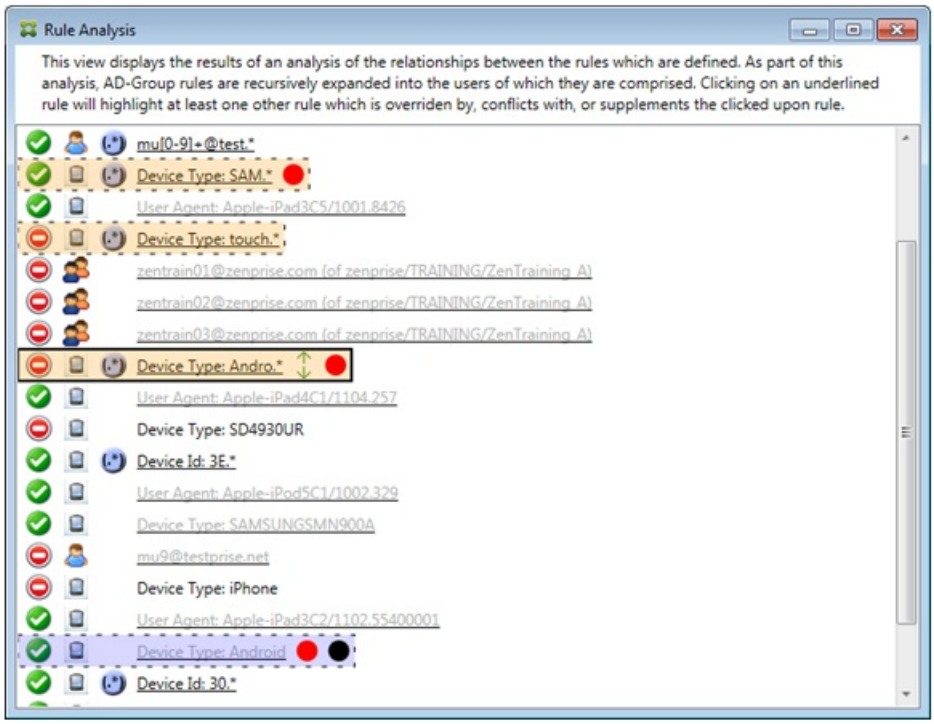
Dans ce cas, la règle principale est la règle d'expression régulière ActiveSync Device Type touch.* Les caractéristiques sont les suivantes :

- 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

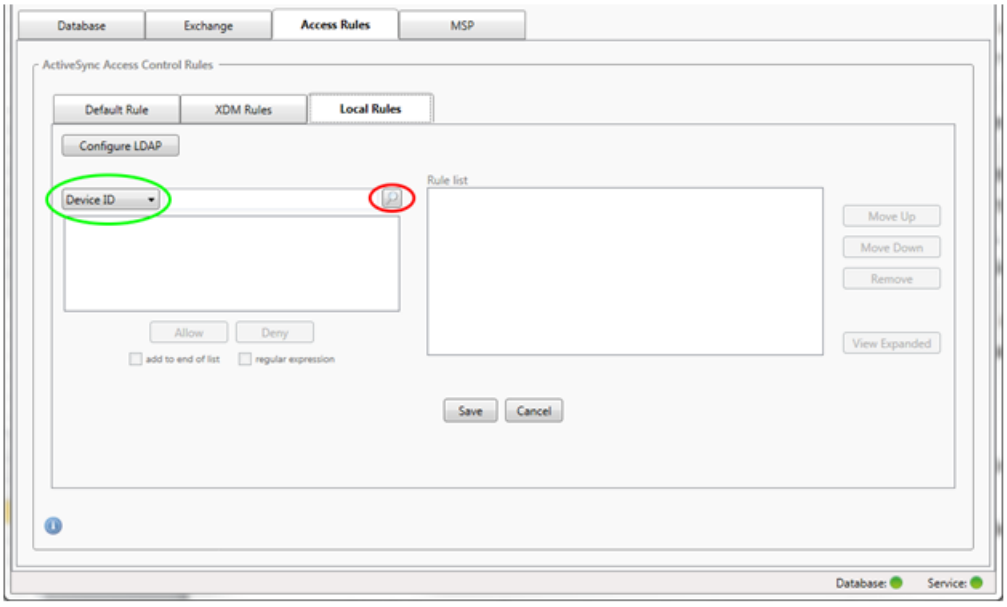
Cet exemple explique pourquoi les relations entre les règles sont toujours abordées du point de vue de la règle principale. L'exemple précédent a montré comment un clic sur la règle d'expression régulière s'appliquait au champ de règle Device Type avec la valeur touch.* En cliquant sur la règle secondaire Andro.* vous mettrez en avant un autre ensemble de règles secondaires.



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.

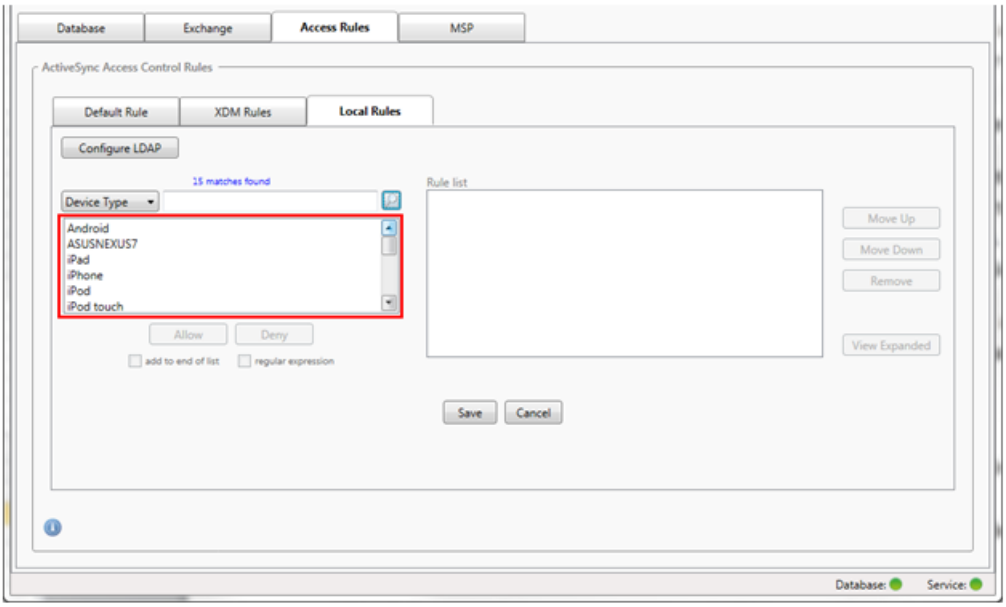
Pour configurer une règle locale d'expression normale

1. Cliquez sur l'onglet Access Rules.



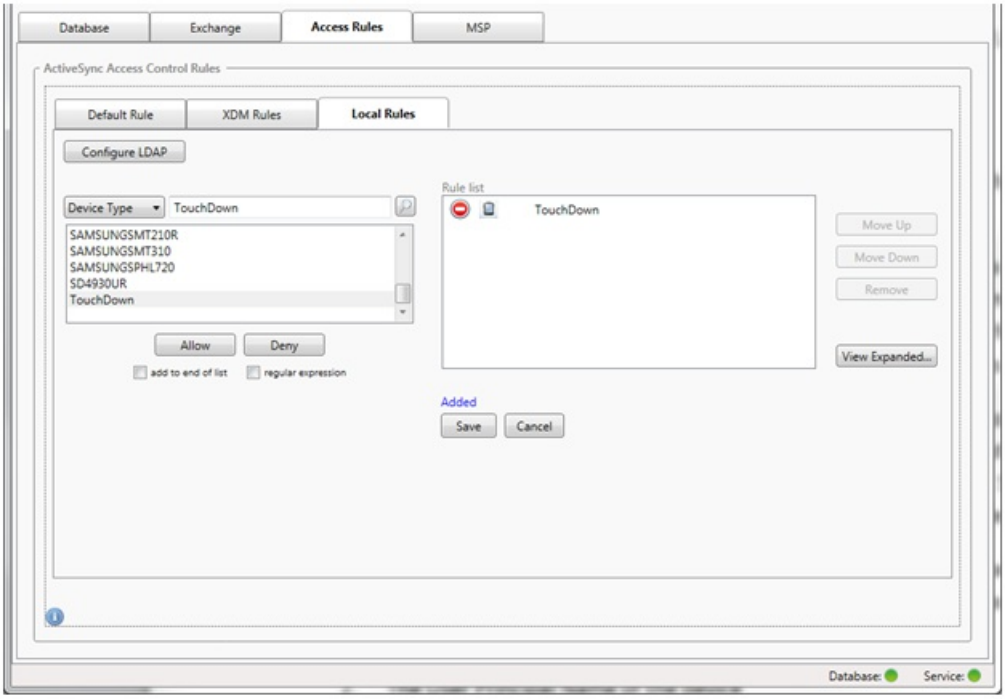
2. Dans la listeDevice ID, sélectionnez le champ pour lequel vous souhaitez créer une règle locale.

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.

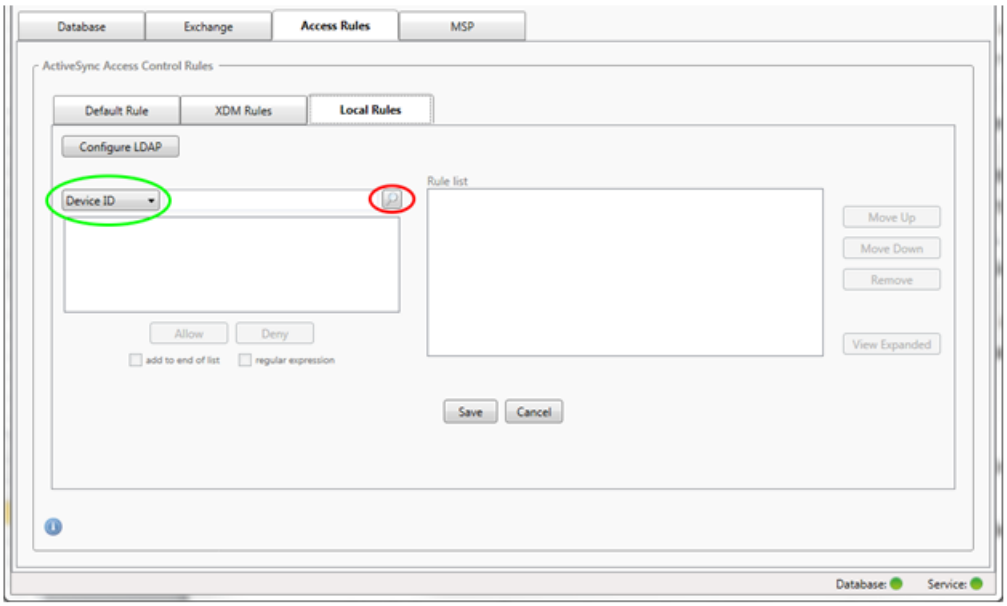


Pour ajouter une expression régulière

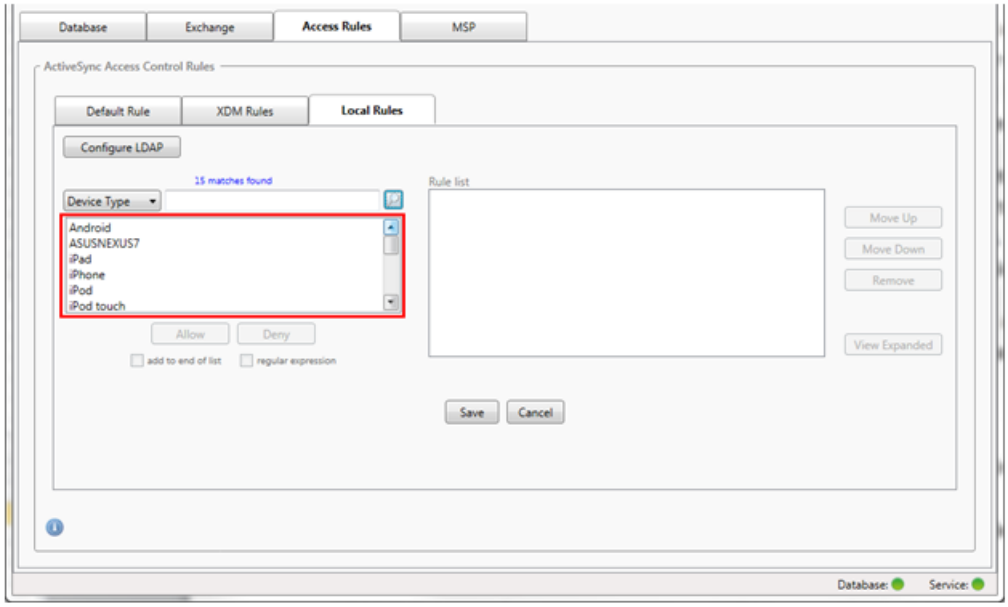
Les règles locales d'expressions régulières peuvent être différenciées par l'icône qui s'affiche à leur côté -  . Pour ajouter une règle d'expression régulière, vous pouvez créer une règle d'expression régulière à partir d'une valeur existante dans la liste des résultats pour un champ donné (si un instantané 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

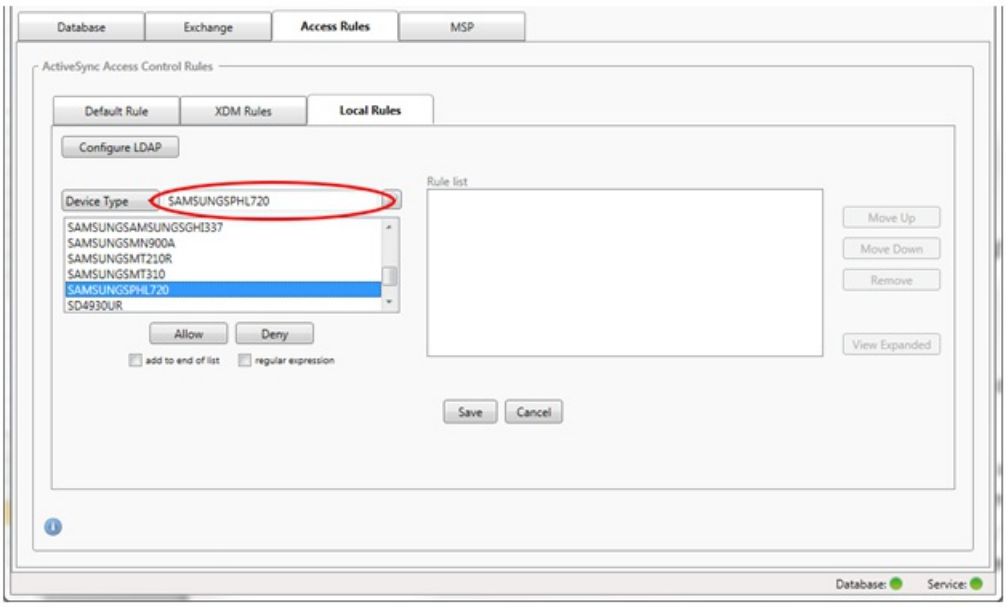
1. Cliquez sur l'onglet Access Rules.



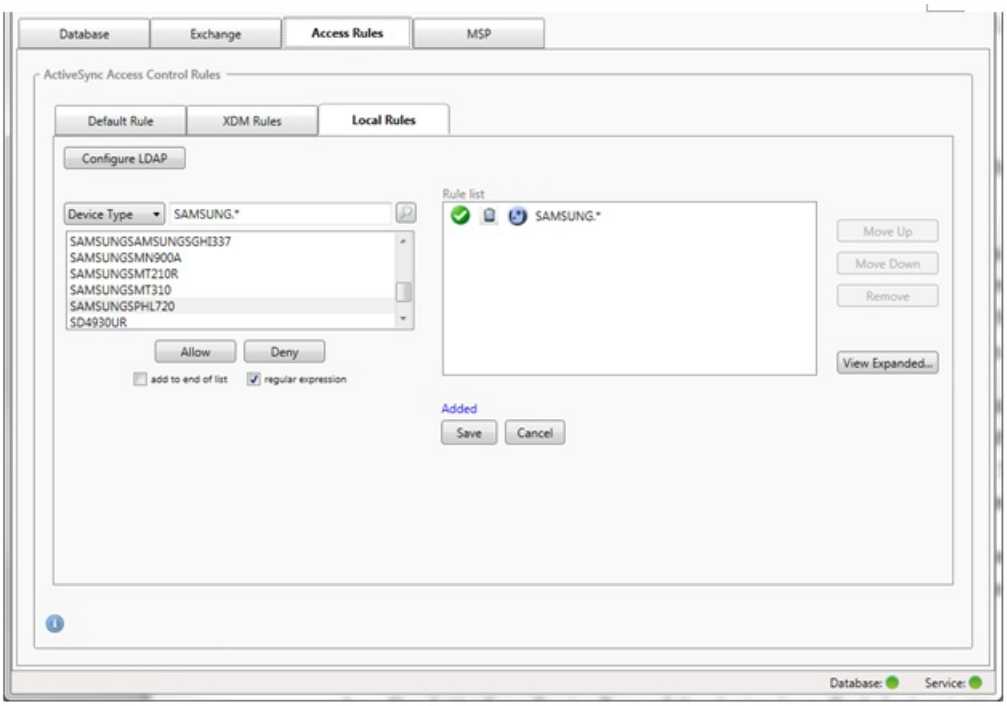
2. Dans la listeDevice ID, sélectionnez le champ pour lequel vous souhaitez créer une règle d'expression régulière locale.
3. Cliquez sur l'icône de la loupe pour afficher tous les résultats uniques pour le champ sélectionné. Dans cet exemple, le champ Device Type a été choisi et les choix sont affichés 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.

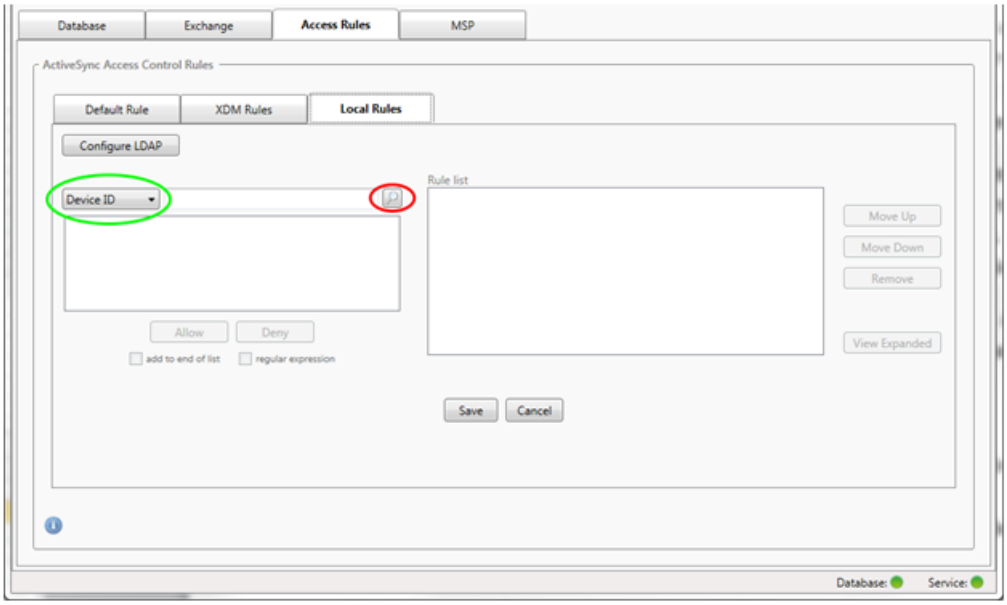


5. Pour autoriser tous les types d'appareils qui ont « Samsung » dans leur valeur Device Type, ajoutez une règle d'expression régulière en suivant les étapes suivantes :
   1. Cliquez dans la zone de texte de l'élément sélectionné.
   2. Modifiez le texte SAMSUNGSPHL720 par SAMSUNG.*
   3. Vérifiez que la case regular expression est cochée.
   4. Cliquez sur Allow.

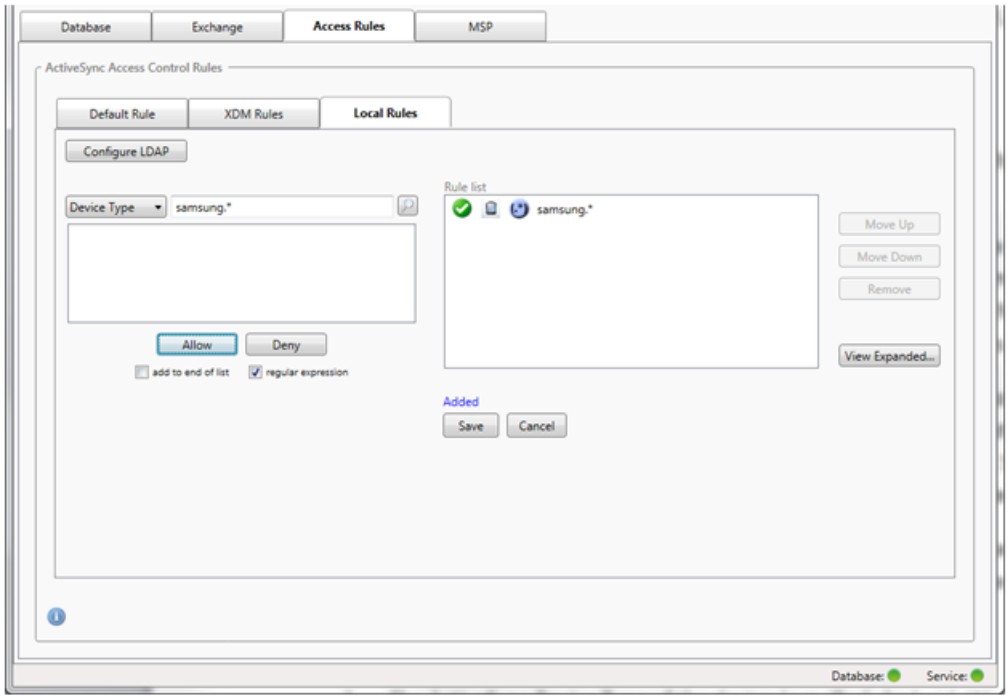


Pour créer une règle d'accès

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.



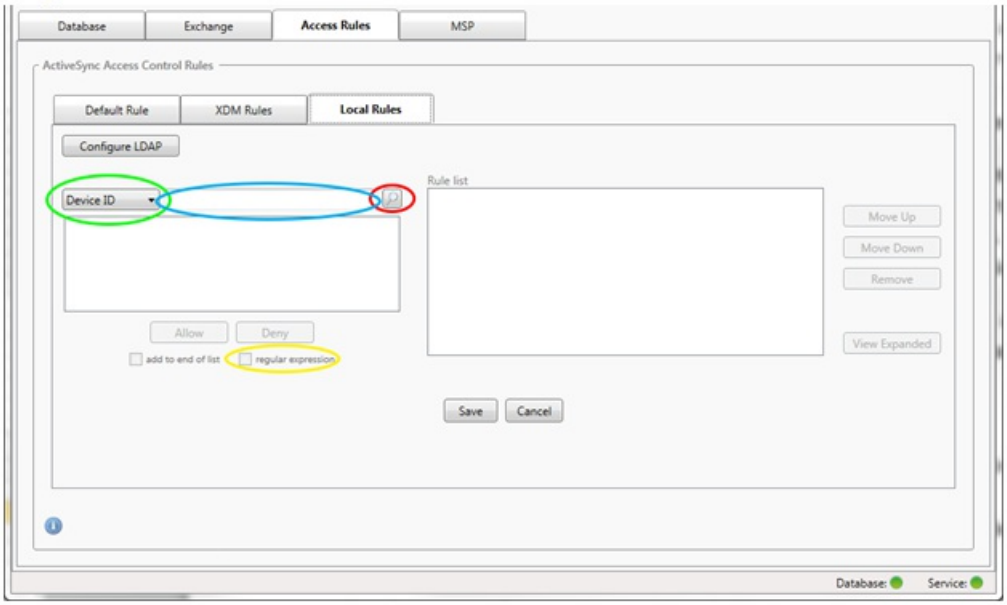
3. Sélectionnez le champ que vous voulez mettre en correspondance. Cet exemple utilise Device Type.
4. Entrez l'expression régulière. Cet exemple utilisesamsung.*
5. Assurez-vous que la case regular expression est cochée et cliquez sur Allow ou Deny. Dans cet exemple, le choix est Allow si bien que le résultat final est le suivant :



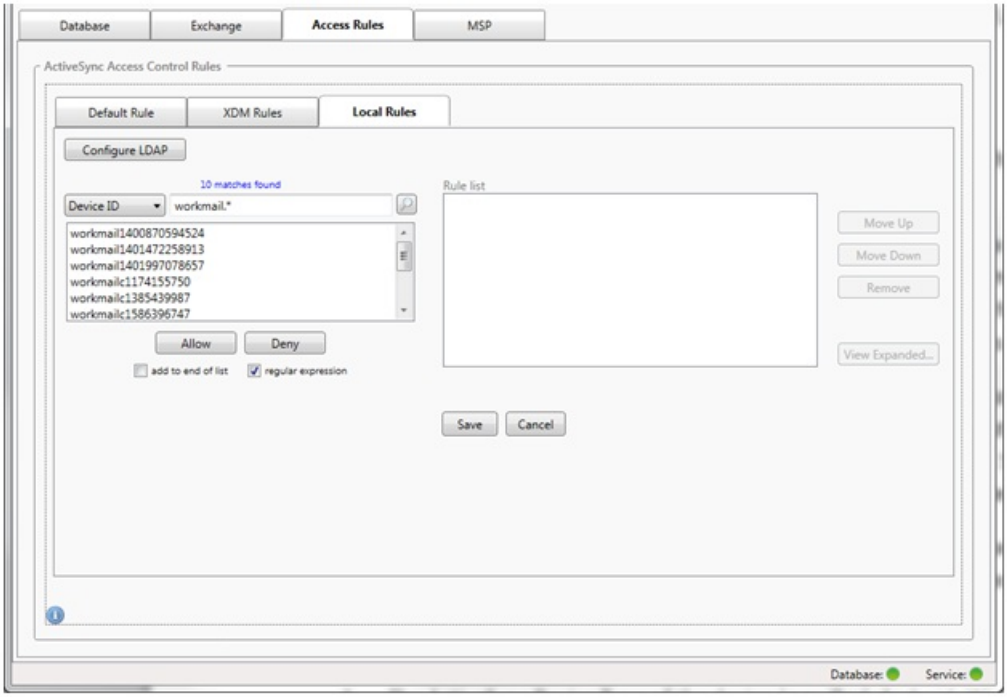
Pour rechercher des appareils

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.

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.

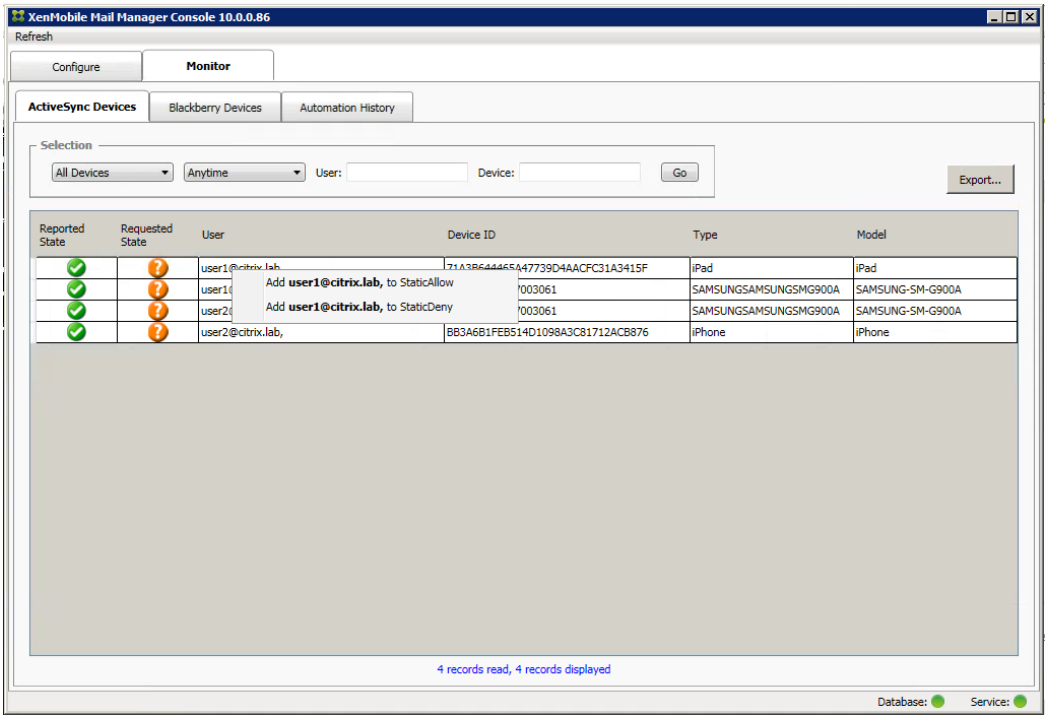


Pour ajouter un seul utilisateur, appareil ou type d'appareil à une règle statique

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.

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.



Surveillance des appareils

May 06, 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.

Dépannage et diagnostics

May 06, 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.

XenMobile NetScaler Connector

Oct 11, 2016

XenMobile NetScaler Connector est une solution qui contrôle l'accès aux e-mails, calendriers et contacts d'entreprise à partir d'appareils mobiles. XenMobile NetScaler Connector permet aux clients d'envoyer une liste des appareils compatibles depuis XenMobile vers NetScaler, qui à son tour contrôle les appareils mobiles qui sont autorisés à être synchronisés avec le serveur Exchange d'entreprise.

XenMobile offre une protection complète pour les applications mobiles, le réseau et les données, et assure une sécurité et une conformité de bout en bout. NetScaler optimise, sécurise et contrôle la mise à disposition de tous les services de cloud et d'entreprise. Ensemble, ces deux produits Citrix offrent une solution capable de monter en charge, garantissent une haute disponibilité pour les applications et assurent la sécurité tout en réduisant les coûts de gestion et de déploiement de la mobilité.

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.

XenMobile fournit des stratégies en listes blanches (approuvées) et en listes noires (interdites) des appareils en fonction de leur conformité aux stratégies de haut niveau, telles que la détection des appareils jailbreakés ou la détection d'applications spécifiques. Les règles locales XenMobile NetScaler Connector sont généralement utilisées pour renforcer les règles XenMobile dans les cas dans lesquels des substitutions spécifiques sont requises ; par exemple pour bloquer tous les appareils qui utilisent une version spécifique d'un système d'exploitation.

Les fonctionnalités principales de XenMobile NetScaler Connector sont les suivantes :

- **Contrôle d'accès des demandes HTTP ActiveSync**. XenMobile NetScaler Connector peut contrôler les demandes HTTP ActiveSync effectuées par les appareils mobiles sur les serveurs Exchange. Vous pouvez créer des filtres dans XenMobile NetScaler Connector qui vous permettent d'autoriser ou de bloquer les appareils utilisateur, en vous basant sur des règles et des critères que vous spécifiez. Lorsque vous définissez les règles dans XenMobile NetScaler Connector, vous pouvez activer et désactiver les règles dans XenMobile, qui gère ensuite la possibilité pour les appareils d'accéder aux e-mails au sein de l'organisation.
- **Configuration à distance**. XenMobile permet de contrôler les intervalles de ligne de base et delta utilisés par XenMobile NetScaler Connector.
- **Journalisation**. Sur l'onglet **Log** de l'utilitaire de configuration XenMobile NetScaler Connector, vous pouvez visualiser le moment où le cryptage est activé pour un appareil utilisateur donné au niveau requis, en plus des appareils qui sont autorisés ou bloqués.

XenMobile NetScaler Connector offre les possibilités suivantes :

- **Règles basées sur filtre pour autoriser ou bloquer l'accès**. XenMobile NetScaler Connector compare une requête client particulière acheminée via NetScaler aux règles de l'organisation. Le résultat final est un état binaire *autorisé*, dans lequel le client est autorisé à contacter le serveur d'accès au client (CAS) Microsoft Exchange 2010, ou *bloqué*, dans lequel la demande du client est abandonnée et l'accès à Exchange CAS n'est pas autorisé. Couplé avec des paramètres dans la console XenMobile, vous pouvez empêcher l'accès à la messagerie Exchange ActiveSync aux utilisateurs d'appareils en fonction de critères de conformité, par exemple lorsqu'une application se trouvant en liste noire est installée sur l'appareil, si l'appareil est jailbreaké, etc.
- **Un modèle de filtre à deux niveaux**. Le premier niveau analyse les demandes HTTP entrantes en fonction

d'informations de chemin spécifiques. Le second niveau effectue le filtrage en se basant sur des informations spécifiques à l'appareil ou l'utilisateur. Vous pouvez configurer les deux niveaux.

- **Règles de filtre stockées dans des fichiers de configuration**. Les règles de filtre spécifiques se rapportant à des comptes et appareils utilisateurs dans votre organisation sont stockées dans les fichiers de configuration XML de la passerelle.

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.

Déploiement de XenMobile NetScaler Connector

May 06, 2016

XenMobile NetScaler Connector vous permet d'utiliser NetScaler pour servir de proxy et équilibrer la charge des communications du serveur XenMobile avec les appareils gérés XenMobile. XenMobile NetScaler Connector communique périodiquement avec XenMobile pour synchroniser les stratégies. XenMobile NetScaler Connector et XenMobile peuvent être en cluster, ensemble ou indépendamment, et leur charge peut être équilibrée par NetScaler.

Composants de XenMobile NetScaler Connector

XenMobile NetScaler Connector se compose de quatre composants :

- Service XenMobile NetScaler Connector. Ce service offre une interface de service Web REST pouvant être invoquée par NetScaler pour déterminer si une demande ActiveSync provenant d'un appareil est autorisée.
- Service de configuration XenMobile. Ce service communique avec Device Manager pour synchroniser les modifications apportées aux stratégies Device Manager avec XenMobile NetScaler Connector.
- Service de notification XenMobile. Ce service envoie des notifications d'accès à des appareils non autorisés à Device Manager pour que Device Manager puisse prendre des mesures appropriées, telles que notifier l'utilisateur que l'appareil a été bloqué.
- Utilitaire de configuration XenMobile NetScaler. Cette application permet à l'administrateur de configurer et de surveiller XenMobile NetScaler Connector.

Pour configurer des adresses d'écoute pour XenMobile NetScaler Connector

Afin que XenMobile NetScaler Connector soit capable de recevoir des demandes depuis NetScaler pour autoriser le trafic ActiveSync, vous devez spécifier le port sur lequel XenMobile NetScaler Connector écoute les appels du service Web NetScaler.

1. À partir du menu Démarrer, sélectionnez l'utilitaire de configuration XenMobile NetScaler.
2. Cliquez sur l'onglet Web Service, puis entrez les adresses d'écoute pour le service Web XenMobile NetScaler Connector. Vous pouvez sélectionner le protocole HTTP et/ou HTTPS. Si XenMobile NetScaler Connector est co-résident avec XenMobile (installé sur le même serveur), sélectionnez les valeurs de port qui ne sont pas en conflit avec XenMobile.
3. Une fois les valeurs configurées, cliquez sur Save, puis sur Start Service pour démarrer le service Web.

Pour configurer des stratégies de contrôle d'accès à l'appareil dans XenMobile NetScaler Connector

Pour configurer la stratégie de contrôle d'accès que vous souhaitez appliquer à vos appareils gérés, effectuez les opérations suivantes :

1. Dans l'utilitaire de configuration XenMobile NetScaler, cliquez sur l'onglet Path Filters.
2. Sélectionner la première ligne, Microsoft-Server-ActiveSync is for ActiveSync, puis cliquez sur Edit.
3. À partir de la liste Policy, sélectionnez la stratégie désirée. Pour une stratégie qui comprend des stratégies XenMobile, sélectionnez Static + ZDM: Permit Mode ou Static + ZDM: Block Mode. Ces stratégies combinent des règles locales (ou statiques) avec les règles de XenMobile. Permit Mode signifie que tous les appareils non identifiés de manière explicite par les règles sont autorisés à accéder à ActiveSync. Block Mode signifie que de tels appareils seront bloqués.
4. Après avoir défini les stratégies, cliquez sur Save.

Pour configurer les communications avec XenMobile

Dans cette tâche, vous devrez spécifier le nom et les propriétés du serveur XenMobile (également appelé fournisseur de

configuration) que vous souhaitez utiliser avec XenMobile NetScaler Connector et NetScaler.

Remarque: cette tâche suppose que XenMobile soit déjà installé et configuré.

1. Dans l'utilitaire de configuration XenMobile NetScaler Connector, cliquez sur l'onglet Config Providers, puis cliquez sur Add.
2. Entrez le nom et l'URL du serveur XenMobile que vous utilisez pour ce déploiement. Si vous disposez de plusieurs serveurs XenMobile déployés dans un déploiement multi-locataire, ce nom doit être unique pour chaque instance de serveur. Par exemple, pour le champ Nom, vous pouvez entrerXMS.
3. Dans Url, entrez l'adresse Web du fournisseur GlobalConfig (GCP) XenMobile, généralement au format https://DeviceManagerHost/zdm/services/MagConfigService. Le nom MagConfigService est sensible à la casse.
4. Dans Password, saisissez le mot de passe qui sera utilisé pour l'autorisation HTTP de base avec le serveur Web XenMobile.
5. Dans Managing Host, entrez le nom du serveur sur lequel vous avez installé XenMobile NetScaler Connector.
6. Dans Baseline Interval, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis XenMobile.
7. Dans Request Timeout, spécifiez l'intervalle d'expiration du délai de demande du serveur.
8. Dans Config Provider, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
9. Dans Events Enabled, activez cette option si vous souhaitez que Secure Mobile Gateway informe XenMobile lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles Secure Mobile Gateway dans l'une des actions automatisées de votre Device Manager.
10. Une fois que le serveur est configuré, cliquez sur Test Connectivity pour tester la connexion au serveur XenMobile.
11. Lorsque la connexion est établie, cliquez sur Save.

Déploiement de XenMobile NetScaler Connector pour la redondance et la capacité à monter en charge

Si vous voulez étendre votre déploiement XenMobile NetScaler Connector et XenMobile, vous pouvez installer des instances de XenMobile NetScaler Connector sur de multiples serveurs Windows, et les faire pointer vers la même instance de XenMobile, puis vous pouvez utiliser NetScaler pour équilibrer la charge des serveurs.

Il existe deux modes de configuration de XenMobile NetScaler Connector :

- En mode non partagé, chaque instance de XenMobile NetScaler Connector communique avec un serveur XenMobile et conserve sa propre copie privée de la stratégie résultante. Par exemple, si vous possédez un cluster de serveurs XenMobile, vous pouvez exécuter une instance de XenMobile NetScaler Connector sur chaque serveur XenMobile et XenMobile NetScaler Connector obtiendra des stratégies depuis l'instance locale de XenMobile.
- En mode partagé, un nœud XenMobile NetScaler Connector est désigné comme nœud principal et il communique avec XenMobile. La configuration résultante est partagée entre les autres nœuds soit par un partage réseau Windows soit par une réplication Windows (ou tierce).

La totalité de la configuration XenMobile NetScaler Connector se trouve dans un dossier unique (composé de plusieurs fichiers XML). Le processus XenMobile NetScaler Connector détecte les modifications apportées à tout fichier dans ce dossier et recharge automatiquement la configuration. Il n'y a pas de basculement du nœud principal en mode partagé. Toutefois, le système peut tolérer le fait que le serveur principal soit arrêté pendant quelques minutes (par exemple, pour redémarrer), car la dernière configuration correcte connue est mise en cache dans le processus XenMobile NetScaler Connector.

Configuration système requise de XenMobile NetScaler Connector

Oct 11, 2016

XenMobile NetScaler Connector communique avec NetScaler sur un pont SSL configuré sur le boîtier NetScaler qui permet au boîtier d'acheminer tout le trafic sécurisé directement vers XenMobile. Vous pouvez installer XenMobile NetScaler Connector sur son propre serveur ou sur le même serveur que XenMobile. XenMobile NetScaler Connector requiert la configuration système minimale suivante :

Composant	Configuration requise
Ordinateur et processeur	733 MHz Pentium III 733 MHz ou processeur supérieur. 2.0 GHz Pentium III ou processeur supérieur (recommandé)
NetScaler	Boîtier NetScaler avec version du logiciel 10
Mémoire	1 gigaoctet (Go)
Disque dur	Partition locale au format NTFS avec 150 Mo d'espace disque dur disponible
Système d'exploitation	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2 (recommandé)
Autres périphériques	Carte réseau compatible avec le système d'exploitation hôte pour les communications avec le réseau interne.
Affichage	Moniteur VGA ou de plus haute résolution

L'ordinateur hôte pour XenMobile NetScaler Connector requiert l'espace disque disponible suivant :

- Application. 10 - 15 Mo (100 Mo recommandés)
- Journalisation. 1 Go (20 Go recommandés)

Pour de plus amples informations sur les plates-formes prises en charge pour XenMobile NetScaler Connector, consultez Plates-formes prises en charge dans XenMobile.

Installation de XenMobile NetScaler Connector

May 06, 2016

Vous pouvez installer XenMobile NetScaler Connector sur son propre serveur ou sur le même serveur où vous avez installé XenMobile.

Vous pouvez envisager d'installer XenMobile NetScaler Connector sur son propre serveur (distinct de XenMobile) pour les raisons suivantes :

- Votre serveur XenMobile est hébergé à distance dans le cloud (emplacement physique).
- Vous ne souhaitez pas que XenMobile NetScaler Connector soit affecté par les redémarrages du serveur XenMobile (disponibilité).
- Vous souhaitez que les ressources système d'un serveur soient entièrement dévouées à XenMobile NetScaler Connector (performances).

La charge de l'UC que XenMobile NetScaler Connector place sur un serveur dépend du nombre d'appareils gérés, mais un principe de base est de provisionner pour un noyau d'UC supplémentaire si XenMobile NetScaler Connector est déployé sur le même serveur que XenMobile. Pour un grand nombre d'appareils (plus de 50 000), il se peut que vous deviez provisionner des noyaux supplémentaires si vous ne disposez pas d'un environnement en cluster. L'encombrement mémoire de XenMobile NetScaler Connector n'est pas assez important pour justifier plus de mémoire.

Pour installer, mettre à niveau ou désinstaller XenMobile NetScaler Connector

May 06, 2016

1. Exécutez XncInstaller.exe avec un compte d'administrateur pour installer XenMobile NetScaler Connector (XNC) ou autoriser la mise à niveau ou la suppression d'un XenMobile NetScaler Connector.
2. Suivez les instructions à l'écran pour procéder à l'installation, la mise à niveau ou la désinstallation.

Après avoir installé XenMobile NetScaler Connector, vous devez redémarrer manuellement le service de configuration et le service de notification de XenMobile.

Pour désinstaller XNC

May 06, 2016

1. Exécutez XncInstaller.exe avec un compte d'administrateur.
2. Suivez les instructions à l'écran pour procéder à la désinstallation.

Gestion de XenMobile NetScaler Connector

May 06, 2016

Vous pouvez utiliser XenMobile NetScaler Connector pour générer des règles de contrôle d'accès pour autoriser ou bloquer l'accès aux demandes de connexion ActiveSync à partir d'appareils gérés, en fonction de l'état des appareils, des applications figurant sous liste noire ou blanche et d'autres critères de conformité.

À l'aide de l'utilitaire de configuration XenMobile NetScaler Connector, vous pouvez créer des règles dynamiques et statiques qui appliquent des stratégies de messagerie d'entreprise, ce qui vous permet de bloquer les utilisateurs qui ne respectent pas ces règles. Vous pouvez également configurer le cryptage des pièces jointes aux e-mails, de sorte que toutes les pièces jointes qui sont transmises par le biais de votre serveur Exchange vers les appareils gérés sont cryptées et uniquement disponibles sur les appareils gérés par des utilisateurs autorisés.

Choix d'un modèle de sécurité pour XenMobile NetScaler Connector

May 06, 2016

Modèle permissif (Permit Mode)

L'établissement d'un modèle de sécurité est nécessaire au succès d'un déploiement d'appareils mobiles pour les organisations de toutes tailles. Bien qu'il ne soit pas rare d'utiliser un contrôle de réseau protégé ou en quarantaine pour autoriser l'accès à un utilisateur, un ordinateur ou un appareil par défaut, ce n'est pas toujours une bonne pratique. Chaque organisation qui gère la sécurité informatique peut avoir une approche légèrement différente ou adaptée à la sécurité pour les appareils mobiles.

La même logique s'applique à la sécurité des appareils mobiles. Le grand nombre de types et d'appareils mobiles ainsi que les quantités d'appareils mobiles par utilisateur, et l'éventail de plates-formes de systèmes d'exploitation et d'applications disponibles font du modèle permissif un choix inadapté. Dans la plupart des organisations, le modèle restrictif sera le choix le plus logique.

Les scénarios de configuration que Citrix autorise pour l'intégration de Citrix XenMobile NetScaler Connector avec XenMobile sont les suivants :

Le modèle de sécurité permissif fonctionne sur le principe que l'accès est autorisé par défaut. Un blocage et une restriction seront appliqués uniquement dans le cas de règles et de filtrage. Le modèle de sécurité permissif est adapté aux organisations dans lesquelles la sécurité n'est pas une préoccupation principale pour les appareils mobiles et qui appliquent uniquement des contrôles restrictifs pour refuser l'accès lorsque cela est approprié (lorsqu'une règle de stratégie a échoué).

Modèle restrictif (Block Mode)

Le modèle de sécurité restrictif est basé sur le principe que l'accès n'est pas autorisé par défaut. Tout le contenu transitant par le point de vérification est filtré et inspecté, et l'accès est refusé, sauf si les règles autorisant l'accès sont satisfaites. Le modèle de sécurité restrictif est adapté aux organisations qui possèdent des mesures de sécurité relativement strictes pour les appareils mobiles. Le mode accorde seulement l'accès (à des fins d'utilisation et aux fonctionnalités) aux services réseau lorsque toutes les règles autorisant l'accès sont observées.

Configuration de XenMobile NetScaler Connector

May 06, 2016

Vous pouvez configurer XenMobile NetScaler Connector pour bloquer ou autoriser les demandes ActiveSync de manière sélective en vous basant sur les propriétés suivantes : Active Sync Service ID, Device type, User Agent (système d'exploitation de l'appareil), Authorized user et ActiveSync Command.

La configuration par défaut prend en charge une combinaison de groupes statiques et dynamiques. Vous pouvez gérer les groupes statiques à l'aide de l'utilitaire de configuration SMG Controller. Les groupes statiques peuvent être composés de catégories d'appareils connues, telles que les appareils utilisant un agent utilisateur donné.

Les groupes dynamiques sont gérés par une source externe appelée Gateway Configuration Provider et régulièrement collectés par XenMobile NetScaler Connector. XenMobile peut exporter des groupes d'appareils et d'utilisateurs autorisés et bloqués vers XenMobile NetScaler Connector.

Une stratégie est une liste ordonnée de groupes dans laquelle chaque groupe est associé à une action (autoriser ou bloquer) et une liste des membres du groupe. Une stratégie peut contenir n'importe quel nombre de groupes. L'ordre du groupe dans une stratégie est important car lorsqu'une correspondance est localisée, l'action du groupe est prise, et les autres groupes ne sont pas évalués.

Un membre définit une façon de faire correspondre les propriétés d'une demande. Il peut correspondre à une seule propriété, telle que l'ID d'appareil ou plusieurs propriétés, telles que le type d'appareil et l'agent utilisateur.

Configuration des modes de stratégie XenMobile NetScaler Connector

May 06, 2016

XenMobile NetScaler Connector peut s'exécuter dans les six modes suivants :

- Allow All. Ce mode de stratégie accorde l'accès à tout le trafic passant via XenMobile NetScaler Connector. Aucune autre règle de filtrage n'est utilisée.
- Deny All. Ce mode de stratégie bloque l'accès à tout le trafic passant via XenMobile NetScaler Connector. Aucune autre règle de filtrage n'est utilisée.
- Static Rules: Block Mode. Ce mode de stratégie exécute des règles statiques avec une instruction implicite de blocage ou de refus à la fin. Les appareils qui ne sont pas autorisés par d'autres règles de filtre sont bloqués par XenMobile NetScaler Connector.
- Static Rules: Permit Mode. Ce mode de stratégie exécute des règles statiques avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils qui ne sont pas bloqués ou refusés par d'autres règles de filtre sont autorisés via XenMobile NetScaler Connector.
- Static + ZDM Rules: Block Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis XenMobile avec une instruction implicite de blocage ou de refus à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles Device Manager. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont bloqués.
- Static + ZDM Rules: Permit Mode. Ce mode de stratégie exécute tout d'abord des règles statiques, suivies par des règles dynamiques depuis XenMobile avec une instruction implicite d'acceptation ou d'autorisation à la fin. Les appareils sont autorisés ou refusés en se basant sur des filtres définis et des règles XenMobile. Tous les appareils qui ne correspondent pas à des filtres et des règles définis sont autorisés.

Le processus XenMobile NetScaler Connector autorise ou bloque les règles dynamiques en se basant sur des ID ActiveSync uniques pour appareils mobiles iOS et Windows reçus de XenMobile. Les appareils Android changent de comportement en fonction du fabricant et certains n'exposent pas directement d'ID unique ActiveSync. Pour compenser, XenMobile envoie les informations d'ID de l'utilisateur pour les appareils Android pour effectuer une décision d'autorisation ou de blocage. Par conséquent, si un utilisateur possède un seul appareil Android, la fonctionnalité d'autorisation et de blocage fonctionne normalement. Si l'utilisateur possède plusieurs appareils Android, tous les appareils sont autorisés, car les appareils Android ne peuvent pas être différenciés avec certitude. La passerelle peut toujours être configurée pour bloquer de façon statique ces appareils par ActiveSyncID, s'ils sont connus, et peut également être configurée pour effectuer un blocage en fonction du type d'appareil ou de l'agent utilisateur.

Pour spécifier le mode de stratégie, dans l'outil SMG Controller Configuration, procédez comme suit :

1. Cliquez sur l'onglet Path Filters, puis cliquez sur Add.
2. Dans la boîte de dialogue Path Properties, sélectionnez un mode de stratégie à partir de la liste déroulante Policy, puis cliquez sur Save.

Vous pouvez vérifier les règles sur l'onglet Policies de l'utilitaire de configuration. Les règles sont traitées sur XenMobile NetScaler Connector de haut en bas. Les stratégies autorisées sont affichées avec une coche verte. Les stratégies refusées s'affichent un cercle rouge traversé d'une ligne. Pour actualiser l'écran et afficher les règles mises à jour le plus récemment, cliquez sur Refresh. Vous pouvez également modifier l'ordre des règles dans le fichier config.xml.

Pour tester les règles, cliquez sur l'onglet Simulator. Spécifiez des valeurs dans les champs. Elles peuvent également être

obtenues à partir des journaux. Un message de résultat apparaît spécifiant Allow ou Block.

Pour configurer des règles statiques

May 06, 2016

Vous devez entrer des règles statiques avec les valeurs qui sont lues par le filtrage ISAPI de la demande HTTP de connexion ActiveSync. Les règles statiques permettent à XenMobile NetScaler Connector d'autoriser ou de bloquer le trafic en fonction des critères suivants :

- Utilisateur. XenMobile NetScaler Connector utilise la valeur de l'utilisateur autorisé et la structure de nom qui a été capturée lors de l'inscription de l'appareil. Ceci est couramment détecté en tant que domaine\nomutilisateur comme référencé par le serveur qui exécute XenMobile connecté à Active Directory via LDAP. L'onglet Log dans l'utilitaire de configuration XenMobile NetScaler Connector affiche les valeurs qui sont transmises via XenMobile NetScaler Connector si la structure de valeur doit être déterminée ou est différente.
- Deviceid (ActiveSyncID). Également appelée ActiveSyncID de l'appareil connecté. Cette valeur est généralement présente dans la page de propriétés spécifiques de l'appareil dans la console XenMobile. Cette valeur peut être également vue depuis l'onglet Log de l'utilitaire de configuration XenMobile NetScaler Connector.
- DeviceType. XenMobile NetScaler Connector peut déterminer si un appareil est un iPhone, iPad ou tout autre type d'appareil et peut l'autoriser ou le bloquer en fonction de critères donnés. Comme avec d'autres valeurs, l'utilitaire de configuration XenMobile NetScaler Connector peut révéler tous les types d'appareils connectés en cours de traitement pour la connexion ActiveSync.
- UserAgent. Contient des informations sur le client ActiveSync utilisé. Dans la plupart des cas, la valeur spécifiée correspond à une version spécifique d'un système d'exploitation et à la version de plate-forme de l'appareil mobile.

L'utilitaire de configuration XenMobile NetScaler Connector en cours d'exécution sur le serveur gère toujours les règles statiques.

1. Dans l'utilitaire SMG Controller Configuration, cliquez sur l'onglet Static Rules, puis cliquez sur Add.
2. Dans la boîte de dialogue Static Rule Properties, spécifiez les valeurs que vous voulez utiliser en tant que critères. Par exemple, vous pouvez entrer un utilisateur pour autoriser l'accès en entrant le nom d'utilisateur (par exemple,AllowedUser) et désactiver la case à cocher Disabled.
3. Cliquez sur Save. La règle statique est maintenant effective. Par ailleurs, vous pouvez utiliser des expressions régulières pour définir des valeurs, mais vous devez activer le mode de traitement de la règle dans le fichier config.xml.

Pour configurer les règles dynamiques

May 06, 2016

Les règles dynamiques sont définies par les stratégies et les propriétés d'appareils dans Device Manager et peuvent déclencher un filtre XenMobile NetScaler Connector dynamique basé sur la présence d'une violation de stratégie ou d'un paramètre de propriété. Les filtres XenMobile NetScaler Connector fonctionnent en analysant un appareil à la recherche d'une violation de stratégie ou de paramètre de propriété donné. Si l'appareil est conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui satisfait au critère défini. Les options de configuration suivantes vous permettent de définir si vous souhaitez autoriser ou refuser les appareils dans la liste d'appareils en utilisant XenMobile NetScaler Connector.

Remarque : ces règles dynamiques doivent être configurées dans la console XenMobile.

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

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

3. Dans **Activer la ou les règles suivantes**, sélectionnez une ou plusieurs règles à activer.

4. Dans Android uniquement, 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. Lorsque cette option est activée, elle s'assure que XenMobile envoie les informations de l'appareil Android à XenMobile NetScaler Connector au cas où XenMobile ne dispose pas de l'identificateur ActiveSync de l'utilisateur de l'appareil Android.

Pour configurer des stratégies personnalisées en éditant le fichier XML de XenMobile NetScaler Connector

May 06, 2016

Vous pouvez afficher les stratégies de base dans la configuration par défaut sur l'onglet Policies de l'utilitaire de configuration XenMobile NetScaler Connector. Si vous souhaitez créer des stratégies, vous pouvez modifier le fichier de configuration XML XenMobile NetScaler Connector (config\config.xml).

1. Recherchez la section PolicyList dans le fichier, puis ajoutez un nouvel élément Policy.
2. Si un nouveau groupe est également requis, tel qu'un groupe statique ou un groupe pour prendre en charge un GCP supplémentaire, ajoutez le nouvel élément Group à la section GroupList.
3. Si vous le souhaitez, vous pouvez modifier l'ordre des groupes dans une stratégie existante en réorganisant les éléments GroupRef.

Configuration du fichier XML de XenMobile NetScaler Connector

May 06, 2016

XenMobile NetScaler Connector utilise un fichier de configuration XML pour dicter les actions de XenMobile NetScaler Connector. Entre autres entrées, le fichier spécifie les fichiers du groupe et les actions associées que le filtre effectuera lors de l'évaluation des requêtes HTTP. Par défaut, le fichier est appelé config.xml et est situé à l'emplacement suivant : ..\Program Files\Citrix\XenMobile NetScaler Connector\config\.

Nœuds GroupRef

Les nœuds GroupRef définissent les noms de groupes logiques : par défaut, AllowGroup et DenyGroup.
Remarque : l'ordre des nœuds GroupRef tels qu'ils apparaissent dans le nœud GroupRefList est significatif.
La valeur de l'ID d'un nœud GroupRef identifie un conteneur logique ou une collection de membres qui sont utilisés pour la mise en correspondance des comptes d'utilisateurs ou d'appareils spécifiques. Les attributs d'action spécifient la façon dont le filtre traitera un membre qui correspond à une règle dans la collection. Par exemple, un compte d'utilisateur ou d'appareil qui correspond à une règle dans l'ensemble AllowGroup sera accepté (autorisé à accéder à Exchange CAS), alors qu'un compte d'utilisateur ou d'appareil qui correspond à une règle dans l'ensemble DenyGroup sera rejeté (non autorisé à accéder à Exchange CAS).

Lorsqu'un compte utilisateur/appareil particulier ou une combinaison des deux répond aux règles dans les deux groupes, une convention de priorité est utilisée pour diriger le résultat de la requête. La priorité est incorporée dans l'ordre des nœuds GroupRef dans le fichier config.xml de haut en bas. Les nœuds GroupRef sont classés par ordre de priorité. Les règles pour une condition donnée dans le groupe Allow seront toujours prioritaires sur les règles de la même condition du groupe Deny.

Nœuds de groupe

De plus, le fichier config.xml définit les nœuds Groupe. Ces nœuds fournissent une liaison entre les conteneurs logiques AllowGroup et DenyGroup vers les fichiers XML externes. Les entrées stockées dans les fichiers externes forment la base des règles de filtre.
Remarque : dans cette version, seuls les fichiers XML externes sont pris en charge.
L'installation par défaut implémente deux fichiers XML de configuration : allow.xml et deny.xml.

Pour importer une stratégie depuis XenMobile

May 06, 2016

1. Dans l'utilitaire de configuration XenMobile NetScaler Configuration, cliquez sur l'onglet Config Providers, puis cliquez sur Add.
2. Dans la boîte de dialogue Config Providers, dans Name, entrez un nom d'utilisateur qui sera utilisé pour l'autorisation HTTP de base avec le serveur XenMobile et disposant de privilèges d'administrateur.
3. Dans URL, entrez l'adresse Web de XenMobile Gateway Configuration Service (GCS), généralement au format https://xdmHost/xdm/services/MagConfigService. Le nom MagConfigService est sensible à la casse.
4. Dans Password, saisissez le mot de passe qui sera utilisé pour l'autorisation HTTP de base avec le serveur XenMobile.
5. Cliquez sur Test Connectivity pour tester la connectivité du fournisseur de configuration vers la passerelle. Si la connexion échoue, vérifiez que vos paramètres locaux de pare-feu autorisent la connexion ou contactez votre administrateur.
6. Lorsqu'une connexion est établie, désactivez la case à cocher Disabled, puis cliquez sur Save.
7. Dans Managing Host, laissez la valeur par défaut du nom DNS de l'ordinateur hôte. Ce paramètre est utilisé pour coordonner les communications avec XenMobile lorsque plusieurs serveurs Forefront Threat Management Gateway (TMG) sont configurés dans un tableau.

Lorsque vous enregistrez les paramètres, ouvrez le GCS.

Pour configurer une connexion à XenMobile NetScaler Connector

May 06, 2016

XenMobile NetScaler Connector communique avec XenMobile et d'autres fournisseurs de configuration à distance via les services Web sécurisés.

1. Dans l'utilitaire de configuration XenMobile NetScaler Connector, cliquez sur l'onglet Config Providers, puis cliquez sur Add.
2. Dans la boîte de dialogue Config Providers, dans Name, entrez un nom d'utilisateur disposant des privilèges d'administration et qui sera utilisé pour l'autorisation HTTP de base avec le serveur XenMobile.
3. Dans URL, entrez l'adresse Web du service XenMobile GCS (Gateway Configuration Service), généralement au format https://ZdmHost/zdm/services/MagConfigService. Le nom MagConfigService est sensible à la casse.
4. Dans Password, saisissez le mot de passe qui sera utilisé pour l'autorisation HTTP de base avec le serveur XenMobile.
5. Dans Managing Host, entrez le nom du serveur XenMobile NetScaler Connector.
6. Dans Baseline Interval, spécifiez une période de temps après laquelle un nouveau ruleset dynamique actualisé est extrait depuis Device Manager.
7. Dans Delta interval, spécifiez une période de temps après laquelle une mise à jour de règles dynamiques est extraite.
8. Dans Request Timeout, spécifiez l'intervalle d'expiration du délai de demande du serveur.
9. Dans Config Provider, sélectionnez si l'instance de serveur du fournisseur de configuration fournit la configuration de la stratégie.
10. Dans Events Enabled, activez cette option si vous souhaitez que XenMobile NetScaler Connector informe XenMobile lorsqu'un appareil est bloqué. Cette option est requise si vous utilisez les règles XenMobile NetScaler Connector dans l'une de vos actions automatisées XenMobile.
11. Cliquez sur Save, puis cliquez sur Test Connectivity pour tester la connectivité du fournisseur de configuration vers la passerelle. Si la connexion échoue, vérifiez que les paramètres du pare-feu local acceptent la connexion ou contactez votre administrateur.
12. Si la connexion réussit, désactivez la case à cocher Disabled, puis cliquez sur Save.

Lorsque vous ajoutez un nouveau fournisseur de configuration, XenMobile NetScaler Connector crée automatiquement une ou plusieurs stratégies associées au fournisseur. Ces stratégies sont définies par une définition de modèle contenue dans config\policyTemplates.xml de la section NewPolicyTemplate. Pour chaque élément Policy est défini dans cette section, une nouvelle stratégie est créée. L'opérateur peut ajouter, supprimer ou modifier les éléments de stratégie à condition que l'élément de stratégie soit conforme à la définition du schéma et que les chaînes de substitution standard (entre accolades) ne soient pas modifiées. Ajoutez ensuite de nouveaux groupes pour le fournisseur et mettez à jour la stratégie pour inclure les nouveaux groupes.

Choix de filtres pour XenMobile NetScaler Connector

May 06, 2016

Les filtres XenMobile NetScaler Connector fonctionnent en analysant un appareil à la recherche d'une violation de stratégie ou de paramètre de propriété donné. Si l'appareil est conforme aux critères, l'appareil est placé dans une liste d'appareils. Cette liste d'appareils n'est ni une liste d'autorisation ni une liste de blocage. Il s'agit d'une liste d'appareils qui répondent aux critères définis. Les filtres suivants sont disponibles pour XenMobile NetScaler Connector dans XenMobile.

- Applications sur liste noire. Autorise ou refuse les appareils en fonction de la liste des appareils définie par les stratégies de liste noire et la présence d'applications en liste noire.
- Applications hors liste suggérée. Autorise ou refuse les appareils en fonction de la liste des appareils définie par les stratégies de liste blanche et la présence d'applications ne se trouvant pas en liste blanche.
- Appareils non gérés. Crée une liste d'appareils de tous les appareils dans la base de données XenMobile. Mobile Application Gateway doit être déployé dans un mode Block.
- Android rootés/iOS jailbreakés. Crée une liste d'appareils de tous les appareils marqués comme rootés et les autorise ou les refuse en se basant sur leur état racine.
- Appareils non conformes. Vous permet d'interdire ou d'autoriser des appareils qui répondent à vos critères de conformité informatiques internes. La conformité est un paramètre arbitraire défini par la propriété d'appareil nommée Non conforme, qui est un indicateur booléen qui peut être soit True soit False. (Vous pouvez créer cette propriété manuellement et définir sa valeur, ou vous pouvez utiliser les actions automatisées pour créer cette propriété sur un appareil si l'appareil correspond ou pas aux critères spécifiques.)
  - Out of Compliance = True. Si un appareil ne répond pas aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil n'est pas conforme.
  - Out of Compliance = False. Si un appareil répond aux normes de conformité et aux définitions de stratégie définies par votre service informatique, l'appareil est conforme.
- Mot de passe non conforme. Crée une liste d'appareils de tous les appareils qui ne disposent pas d'un code secret sur l'appareil.
- État révoqué. Crée une liste d'appareils de tous les appareils révoqués et les autorise ou les refuse en fonction de l'état de révocation.
- Appareils inactifs. Crée une liste d'appareils des appareils qui n'ont pas communiqué avec XenMobile dans une période de temps spécifiée et sont donc considérés comme étant inactifs et autorise ou refuse les appareils en conséquence.
- Appareils anonymes. Autorise ou refuse les appareils qui sont inscrits dans XenMobile, mais l'identité de l'utilisateur est inconnue. Par exemple, ceci peut être un utilisateur qui a été inscrit, mais le mot de passe Active Directory de l'utilisateur a expiré ou un utilisateur s'est inscrit avec des informations d'identification inconnues.
- Autorisation/refus implicite. Crée une liste d'appareils de tous les appareils qui ne répondent pas à tous les critères de règle de filtre et les autorise ou les refuse en se basant sur cette liste. L'option Autorisation/refus implicite garantit que l'état de XenMobile NetScaler Connector dans l'onglet Appareils est activé et affiche l'état de XenMobile NetScaler Connector pour vos appareils. L'option Autorisation/refus implicite contrôle également tous les autres filtres XenMobile NetScaler Connector qui n'ont pas été sélectionnés. Par exemple, les Applications sur liste noire seront refusées (bloquées) par XenMobile NetScaler Connector, tandis que tous les autres filtres seront autorisés, car l'option Autorisation/refus implicite est sélectionnée sur Autoriser.

Pour simuler le trafic ActiveSync avec XenMobile NetScaler Connector

May 06, 2016

Vous pouvez utiliser XenMobile NetScaler Connector pour simuler le trafic ActiveSync en conjonction avec vos stratégies. Dans l'utilitaire de configuration XenMobile NetScaler Connector, sélectionnez l'onglet Simulations. Les résultats vous montrent comment vos stratégies s'appliquent aux règles que vous avez configurées.

Contrôle de XenMobile NetScaler Connector

May 06, 2016

L'utilitaire de configuration XenMobile NetScaler Connector offre une journalisation détaillée que vous pouvez utiliser pour afficher tout le trafic transitant par le biais de votre serveur Exchange Server qui est autorisé ou bloqué par Secure Mobile Gateway.

Utilisez l'onglet Log pour afficher l'historique des demandes ActiveSync transmises à XenMobile NetScaler Connector par NetScaler pour autorisation.

De plus, pour vous assurer que le service Web XenMobile NetScaler Connector est en cours d'exécution, vous pouvez charger l'adresse URL suivante dans un navigateur sur le serveur XenMobile NetScaler Connector http:///services/ActiveSync/version. Si l'adresse URL retourne la version du produit en tant que chaîne, le service Web est réactif.