

# Réinitialisation en libre-service des mots de passe 1.1

Dec 08, 2016

[À propos de la réinitialisation en libre-service des mots de passe](#)

[Problèmes connus](#)

[Configuration système requise](#)

[Installer et configurer](#)

[Sécuriser la configuration](#)

[Migrer les données depuis le magasin central Single Sign-On](#)

[Configurer StoreFront pour autoriser les utilisateurs à enregistrer des réponses à des questions de sécurité](#)

# À propos de la réinitialisation en libre-service des mots de passe

Dec 08, 2016

La réinitialisation en libre-service des mots de passe confère aux utilisateurs un plus grand contrôle sur leurs comptes d'utilisateur. Une fois la réinitialisation en libre-service des mots de passe configurée, si les utilisateurs rencontrent des problèmes lors de l'ouverture de session sur leurs systèmes, ils peuvent déverrouiller leurs comptes ou réinitialiser leurs mots de passe en répondant correctement à plusieurs questions de sécurité.

La réinitialisation des mots de passe des utilisateurs est un processus intrinsèquement sensible en matière de sécurité. Nous vous recommandons de vous reporter à l'article [Sécuriser la configuration](#) pour vous assurer que votre déploiement est correctement configuré.

Cette version comprend les améliorations principales suivantes :

- Configuration de liste noire - les administrateurs informatiques peuvent ajouter des utilisateurs et des groupes à une liste noire. Les utilisateurs et groupes sur la liste noire ne peuvent utiliser aucune des fonctionnalités de la réinitialisation en libre-service des mots de passe.
- Prise en charge du chinois simplifié : en plus de l'anglais, du français, du japonais et de l'espagnol, il est maintenant possible de définir des questions de sécurité en chinois simplifié.

La réinitialisation en libre-service des mots de passe contient trois composants :

- Console Configuration de la réinitialisation en libre-service des mots de passe
- Service de réinitialisation en libre-service des mots de passe
- Enregistrement de questions de sécurité dans StoreFront

## Console Configuration de la réinitialisation en libre-service des mots de passe

- **Configuration du service.** Configure le service de réinitialisation en libre-service des mots de passe, y compris l'adresse du magasin central, le compte du proxy de données et le compte de réinitialisation en libre-service des mots de passe.
  - Adresse du magasin central : emplacement du partage réseau pour le stockage des données de la réinitialisation en libre-service des mots de passe.
  - Compte du proxy de données : communique avec le magasin central. Ce compte requiert des droits d'accès en lecture et en écriture au magasin central.
  - Compte de réinitialisation en libre-service des mots de passe : permet de déverrouiller le compte et de réinitialiser le mot de passe.
- **Configuration utilisateur.** Configure les utilisateurs/groupes/unités d'organisation autorisés à utiliser la fonctionnalité de réinitialisation en libre-service des mots de passe, et spécifie l'adresse du serveur de licences et l'adresse du service par défaut.
  - Nommer la configuration utilisateur : définit le groupe d'utilisateurs cible du service de réinitialisation en libre-service des mots de passe, qui peut inclure des utilisateurs/groupes/unités d'organisation d'Active Directory.
  - Adresse du serveur de licences : vous pouvez utiliser la réinitialisation en libre-service des mots de passe uniquement avec XenApp ou XenDesktop édition Platinum. La version minimum du serveur de licences doit être 11.13.1 ou version ultérieure.

- Sélectionnez ou désélectionnez les fonctionnalités **Déverrouiller** et **Réinitialiser**.
- Adresse du service par défaut : spécifie l'URL du service de réinitialisation en libre-service des mots de passe.
- **Vérification d'identité**. Configure le questionnaire utilisé pour l'enregistrement et pour déverrouiller ou réinitialiser le mot de passe.
  - Ajoutez une question ou un groupe de questions au magasin de questions à partir duquel les questionnaires sont générés.
  - Sélectionnez une liste de questions dans le magasin de questions à utiliser pour l'enregistrement.
  - Exporter/importer les groupes ou questions de sécurité.

### Service de réinitialisation en libre-service des mots de passe

Le service de réinitialisation en libre-service des mots de passe est exécuté sur un serveur Web et permet aux utilisateurs de réinitialiser leurs mots de passe Windows et de déverrouiller leurs comptes Windows. Les demandes des utilisateurs sont envoyées au service via StoreFront.

### Enregistrement de questions de sécurité dans StoreFront

Utilisez StoreFront pour permettre aux utilisateurs d'enregistrer leurs réponses aux questions de sécurité. Une fois qu'elles sont enregistrées, ils peuvent réinitialiser des mots de passe de domaine et déverrouiller des comptes de domaine. Pour de plus amples informations, consultez la rubrique [Réinitialisation en libre-service des mots de passe](#) dans la documentation de StoreFront.

# Problèmes connus

Dec 08, 2016

Les problèmes connus suivants existent dans cette version.

- Les tentatives d'ajout d'un groupe d'utilisateurs dans l'assistant de configuration utilisateur peuvent échouer et s'accompagner d'un message indiquant que le groupe d'utilisateurs figure dans une liste noire. Ce message est incorrect. La tentative a échoué car vous avez déjà ajouté ce groupe.

[#665520]

- Vous ne pouvez pas ajouter d'utilisateurs et de groupes d'utilisateurs que vous venez de supprimer depuis l'assistant de configuration tant que vous n'avez pas terminé le processus de suppression et fermé l'assistant. Sinon un message d'erreur incorrect s'affiche indiquant que les utilisateurs ou groupes figurent dans une liste noire. Pour contourner le problème, terminez le processus de suppression, fermez l'assistant et rouvrez l'assistant pour ajouter de nouveau les utilisateurs ou groupes.

[#665352]

- Si vous mettez à niveau la Réinitialisation en libre-service des mots de passe vers la version 1.1 alors que la version 1.0 de la console est ouverte, cette dernière ne peut pas être utilisée.

[#664390]

- Les tentatives de mise à niveau sur Windows Server 2012 avec seulement .Net Framework 4.5 et sur Windows Server 2016 avec seulement .Net Framework 4.6 peuvent échouer. Les tentatives échouent car les mises à niveau sur place sur Windows Server 2012 et Windows Server 2016 dépendent de .Net Framework 3.5. Pour contourner le problème, installez .Net Framework 3.5 avant les mises à niveau.

[DNA-22761]

Les problèmes connus suivants existent dans cette version.

- Après ouverture de la console de réinitialisation en libre-service des mots de passe, il est possible que vous ne puissiez pas l'épingler à la barre des tâches.

[#646300]

Solution : épinglez la console à la barre des tâches depuis le raccourci de menu **Démarrer**.

- En raison d'un problème connu dans Windows 2016, vous ne pouvez pas rechercher la console de réinitialisation en libre-service des mots de passe dans Windows 2016.

[#648939]

Solution : utilisez le menu **Démarrer** pour localiser la console de réinitialisation en libre-service des mots de passe.

- Si l'âge minimum du mot de passe dans la stratégie de mot de passe de la stratégie de domaine par défaut est la valeur

par défaut (un jour), et que vos utilisateurs essayent de réinitialiser leur mot de passe mais que la réinitialisation échoue (par exemple parce qu'ils ne respectent pas les exigences de complexité), et qu'ils ferment l'assistant de réinitialisation des mots de passe, ils ne peuvent pas réinitialiser leur mot de passe pendant 24 heures.

[#653221]

- Lors de l'utilisation de Citrix Receiver pour Mac, le bouton de tâche d'inscription s'affiche la première fois que l'utilisateur se connecte à StoreFront. Après la déconnexion et la reconnexion à StoreFront, le bouton de tâche ne s'affiche pas.

[#657263]

Solution :

1. Cliquez sur le nom d'utilisateur dans le coin supérieur droit du magasin StoreFront.
  2. Cliquez sur le bouton **Actualiser applications** dans le menu déroulant.
  3. Fermez Citrix Receiver pour Mac, rouvrez-le et le bouton de tâche apparaît.
- Lors de la migration de questions de sécurité en provenance du module de vérification d'identité de Single Sign-On vers la réinitialisation en libre-service des mots de passe, il est possible que les questions ne s'affichent pas dans la console de réinitialisation en libre-service des mots de passe, même après avoir cliqué sur **Actualiser**.

[#657277]

Solution : fermez la console et rouvrez-la.

- Les questions de sécurité du questionnaire qui contiennent le caractère spécial **&** ne s'affichent pas lors de l'inscription dans StoreFront.

[#654913]

Solution : n'utilisez pas **&** dans les questions de sécurité.

# Configuration système requise

Dec 08, 2016

## Important

Citrix ne prend en charge l'installation d'aucun des composants du module de réinitialisation en libre-service des mots de passe sur un contrôleur de domaine. Déployez les composants de réinitialisation en libre-service des mots de passe sur des serveurs dédiés.

Cet article décrit les configurations logicielle et matérielle requises pour l'environnement de réinitialisation en libre-service des mots de passe. Il présuppose que chaque ordinateur répond à la configuration matérielle minimale requise pour le système d'exploitation installé.

### Logiciel

Les ordinateurs de l'environnement de réinitialisation en libre-service des mots de passe peuvent nécessiter l'utilisation des logiciels système suivants.

- **Windows 2016, Windows 2012 R2, Windows 2008 R2** (Nous recommandons d'utiliser Windows 2008 R2 uniquement avec un partage de fichiers local et des mesures de verrouillage appropriées. Pour de plus amples informations, consultez [Créer un magasin central](#).) : requis par le serveur de réinitialisation en libre-service des mots de passe.
- **Microsoft Windows Installer 2.0 ou version ultérieure** : requis par tous les composants.
- **Microsoft .NET Framework** : requis par le serveur de réinitialisation en libre-service des mots de passe.
  - 4.6.x (Windows 2016)
  - 4.5.2 (Windows 2012 R2)
  - 3.5.1 (Windows 2008 R2)
- **Internet Information Services (IIS)** : requis par le serveur de réinitialisation en libre-service des mots de passe.
  - IIS 10.0 (Windows 2016)
  - IIS 8.5 (Windows 2012 R2)
  - IIS 7.5 (Windows 2008 R2)

### Serveur de réinitialisation en libre-service des mots de passe

- Composant de réinitialisation en libre-service des mots de passe : magasin central
- Environnement pris en charge : partage de fichiers SMB
- Configuration matérielle requise : 30 Ko d'espace disque par utilisateur

### Configuration requise pour ASP.NET 3.5/4.x

Le composant ASP.NET pour votre version de .NET Framework sur votre ordinateur Windows Server.

### Exigences en matière de sécurité et de compte

Avant d'installer le service de réinitialisation en libre-service des mots de passe, assurez-vous que les comptes et composants nécessaires à sa prise en charge sont disponibles. Par ailleurs, étant donné que le service utilise le mode HTTP sécurisé (HTTPS), il requiert un certificat d'authentification serveur pour ses communications TLS avec StoreFront.

### *Exigences d'authentification serveur :*

Avant d'installer le service, vous devez obtenir d'une autorité de certification (CA) un certificat d'authentification serveur pour les communications à l'aide du protocole SSL ou votre infrastructure de clé publique (PKI), si disponible.

### *Comptes requis pour les modules du service :*

**Remarque :** assurez-vous que les comptes n'expirent pas.

Le service de réinitialisation en libre-service des mots de passe requiert ces types de compte pour la lecture et l'écriture de données lors de son exécution dans votre environnement :

- Compte du proxy de données
- Compte en libre-service

Lorsque différents modules nécessitent le même type de compte, vous pouvez utiliser le même compte pour plusieurs modules ou spécifier des comptes personnalisés différents pour chaque module.

- **Compte du proxy de données**

Droits d'accès en lecture et en écriture au magasin central. Pour de plus amples informations, consultez la section [Créer un magasin central](#).

- **Compte en libre-service**

Requiert des droits suffisants pour déverrouiller et réinitialiser le mot de passe des utilisateurs appropriés dans la configuration utilisateur. Pour de plus amples informations, consultez la section [Sécuriser la configuration](#).

### **StoreFront**

- StoreFront 3.7
- StoreFront 3.8

### **Citrix Receiver**

Pris en charge :

- Citrix Receiver pour Web
- Citrix Receiver pour Windows
- Citrix Receiver pour Linux
- Citrix Receiver pour Mac (requiert StoreFront 3.8)

Périphériques non pris en charge :

- Citrix Receiver pour Chrome
- Appareils mobiles (même pas avec Receiver pour Web)

### **Utilisation externe avec NetScaler Gateway**

Non pris en charge

# Installer et configurer

Dec 08, 2016

Cet article contient ces sections :

[Checklist d'installation et de configuration](#)

[Ordre d'installation et de configuration](#)

[Créer un magasin central](#)

[Installer et configurer le module de réinitialisation en libre-service des mots de passe](#)

[Gérer les configurations utilisateur](#)

[Gérer les questions de vérification d'identité](#)

[Gérer la vérification d'identité](#)

Avant de commencer l'installation, effectuez les tâches de cette liste :

	Étape
	Choisir les ordinateurs de votre environnement sur lesquels vous allez installer le logiciel et les préparer pour l'installation. Consultez la section <a href="#">Configuration requise</a> .
	Installer le certificat TLS et les comptes requis pour le service. Consultez la rubrique <i>Exigences en matière de sécurité et de compte</i> dans la section <a href="#">Configuration système requise</a> .
	Installer le serveur de licences. Consultez la <a href="#">Documentation sur le serveur de licences</a> .
	Créer un magasin central. Consultez la section <a href="#">Créer un magasin central</a> .
	Installer le module de réinitialisation en libre-service des mots de passe. Consultez la section <a href="#">Installer et configurer le module de réinitialisation en libre-service des mots de passe</a> .
	Configurer le module de réinitialisation en libre-service des mots de passe à l'aide de la console. Consultez la section <a href="#">Installer et configurer le module de réinitialisation en libre-service des mots de passe</a> .
	Configurer le module de réinitialisation en libre-service des mots de passe sur StoreFront. Consultez la section <a href="#">Configurer StoreFront</a> .
	Assurez-vous que la configuration de la réinitialisation en libre-service des mots de passe est configurée de manière sécurisée. Consultez la section <a href="#">Sécuriser la configuration</a> .

Installer le certificat SSL et les comptes requis pour le service. Consultez la section *Exigences en matière de sécurité et de compte*.

Installer le certificat SSL et les comptes requis pour le service. Consultez la section *Exigences en matière de sécurité et de compte*.

Configurer le module de réinitialisation en libre-service des mots de passe sur StoreFront. Consultez la section [Configurer StoreFront](#).

Pour installer le service et exécuter l'assistant de configuration du service, le compte avec lequel vous vous connectez doit être un utilisateur du domaine et appartenir au groupe Administrateur local sur le serveur.

Nous vous suggérons d'installer le module de réinitialisation en libre-service des mots de passe dans l'ordre suivant :

1. Installez ou mettez à niveau le serveur de licences vers une version minimale de 11.13.1.2. Téléchargez le serveur de licences à partir de <https://www.citrix.com/downloads/licensing.html>.
2. Créez votre magasin central.
3. Installez le module de réinitialisation en libre-service des mots de passe.
4. Configurez le module de réinitialisation en libre-service des mots de passe dans la console.
5. Configurez StoreFront avec l'adresse du serveur de réinitialisation en libre-service des mots de passe.

Pour des raisons de sécurité, nous vous recommandons de créer le magasin central directement sur la machine exécutant le service de réinitialisation en libre-service des mots de passe. Pour les déploiements dans lesquels plus d'un serveur de réinitialisation en libre-service des mots de passe est requis, vous pouvez héberger le magasin central sur un partage réseau distant si le serveur de réinitialisation en libre-service des mots de passe et le serveur hébergeant le partage prennent tous deux en charge le cryptage SMB.

Cette fonctionnalité est uniquement disponible sur Windows Server 2012 R2 ou Windows Server 2016 ; par conséquent, nous ne prenons pas en charge Windows Server 2008 R2 lors de l'utilisation d'un partage de fichiers distant pour le magasin central.

## Créer un compte de proxy de données

Créez un utilisateur de domaine normal à utiliser comme compte de proxy de données. Ne configurez pas d'utilisateur depuis le groupe Administrateur de domaine/Administrateur local en tant que compte de proxy de données.

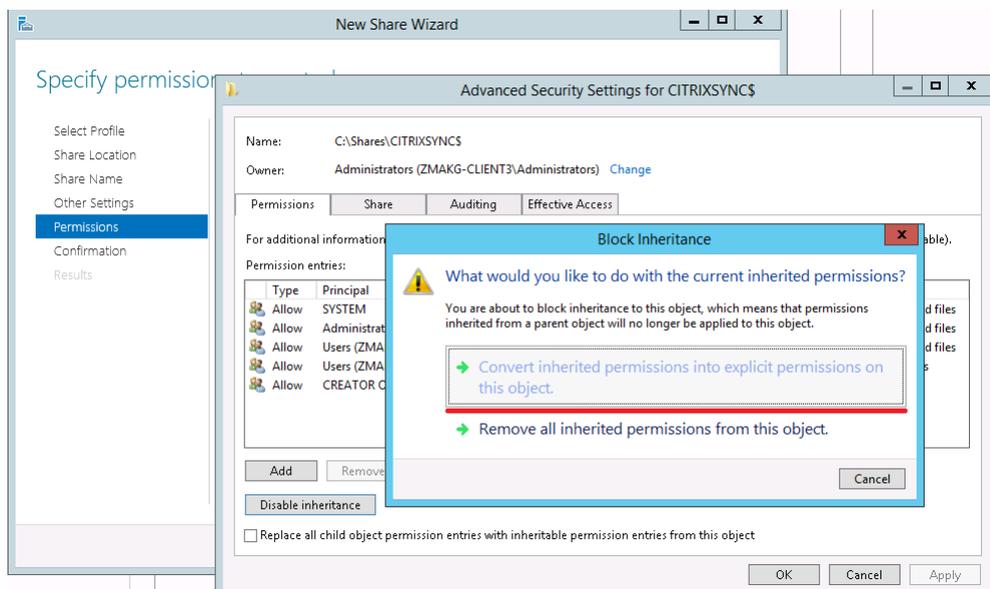
## Créer un magasin central pour Windows Server 2012 R2 ou Windows Server 2016

Lors de l'utilisation de Windows Server 2012 R2 ou Windows Server 2016 pour le serveur de réinitialisation en libre-service des mots de passe et le magasin central, vous pouvez utiliser un partage réseau distant s'il est configuré comme décrit dans cette section. Assurez-vous que **Chiffrer l'accès aux données** est sélectionné et suivez les indications de la section [Sécuriser la configuration](#).

1. Pour démarrer l'assistant **Nouveau partage**, ouvrez Gestionnaire de serveur. Depuis la page de détails **Services de fichiers et de stockage**, sélectionnez **Partages** dans le panneau de gauche

et cliquez sur **Tâches > Nouveau partage**.

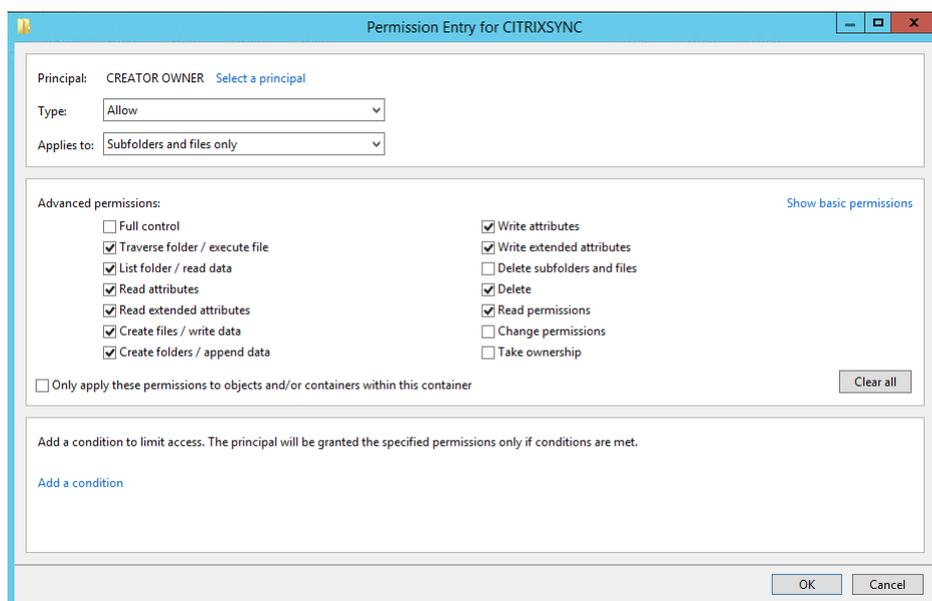
2. Choisissez **Sélectionner le profil** dans le panneau de gauche, sélectionnez **Partage SMB - rapide** et cliquez sur **Suivant**.
3. Choisissez **Emplacement du partage** dans le panneau de gauche. Dans la liste, sélectionnez le serveur sur lequel créer le nouveau partage et le volume sur lequel créer le nouveau dossier partagé, puis cliquez sur **Suivant**.
4. Choisissez **Nom de partage** dans le panneau de gauche, tapez le nom de votre nouveau partage, par exemple **CITRIXSYNCS** et cliquez sur **Suivant**.
5. Choisissez **Autres paramètres** dans le panneau de gauche, sélectionnez **Chiffrer les données**, désélectionnez **Autoriser la mise en cache du partage**, et cliquez sur **Suivant**.
6. Pour personnaliser les autorisations du **Partage**, choisissez **Autorisations** dans le panneau de gauche et sélectionnez **Personnaliser les autorisations > Partage**.
  - o Supprimez **Tout le monde**
  - o Ajoutez **Compte du proxy de données** avec Contrôle total
  - o Ajoutez **Administrateurs locaux** avec Contrôle total
  - o Ajoutez **Administrateurs de domaine** avec Contrôle total
7. Pour personnaliser les autorisations NTFS, choisissez **Autorisations** dans le panneau de gauche, sélectionnez **Personnaliser les autorisations**, cliquez sur **Désactiver l'héritage** et sélectionnez **Convertir les autorisations héritées en autorisations explicites sur cet objet**.



8. Pour supprimer tous les utilisateurs à l'exception de **Créateur propriétaire/Administrateurs locaux/Système**, sur **Personnaliser les autorisations > Autorisations**, cliquez sur **Supprimer**.

9. Pour modifier **Créateur propriétaire > Autorisations avancées**, cliquez sur **Modifier** et décochez les cases suivantes :

- o Contrôle total
- o Suppression de sous-dossier et fichier
- o Modifier les autorisations
- o Appropriation



10. Ajoutez un **compte de proxy de données** avec contrôle total.

11. Choisissez **Confirmation** dans le panneau de gauche de l'assistant Nouveau partage, vérifiez les paramètres sélectionnés pour le partage et cliquez sur **Créer** pour lancer le processus de création du nouveau dossier, puis sur **Fermer**.

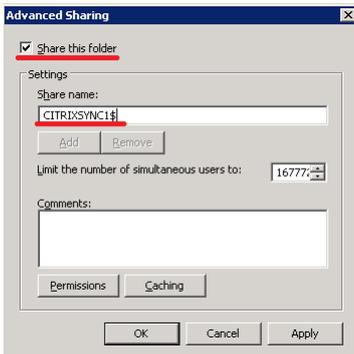
12. Créez deux sous-dossiers situés sous le dossier de partage **CITRIXSYNC5** : le dossier **CentralStoreRoot** et le dossier **People**.

**Important** : assurez-vous que le compte de proxy de données dispose d'un **Contrôle total** sur ces deux sous-dossiers.

### Créer un magasin central pour Windows Server 2008 R2

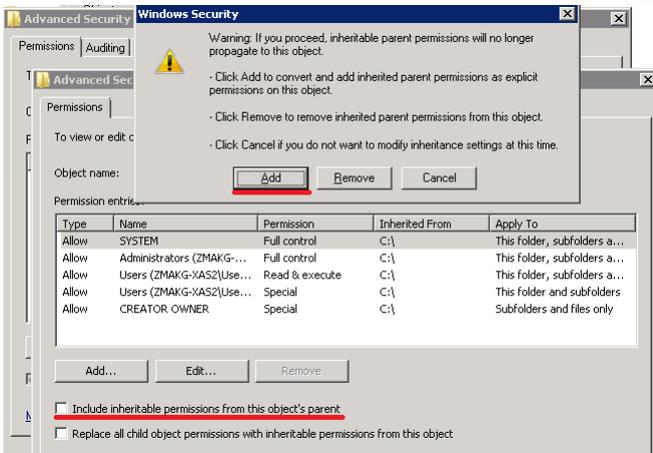
Assurez-vous de créer le magasin central sur le même serveur que celui du service de réinitialisation en libre-service des mots de passe, et configurez le pare-feu Windows de manière à interdire l'accès distant.

1. Créez un dossier local (**CITRIXSYNC1**) en tant que racine du partage de fichiers et créez deux sous-dossiers : **CentralStoreRoot** et **People**.
2. Définissez un partage de fichiers et accordez les autorisations de partage :
  - a. Cliquez avec le bouton droit sur le dossier **CITRIXSYNC1** et sélectionnez **Propriétés > Partage > Partage avancé**.
  - b. Cochez la case **Partager ce dossier**, et définissez le **Nom du partage** sur **CITRIXSYNC1\$**.
  - c. Pour accorder les autorisations de partage, cliquez sur **Autorisations**, supprimez tous les utilisateurs par défaut, et ajoutez le **Compte de proxy de données** avec l'autorisation **Contrôle total**, le **groupe Administrateurs locaux** avec l'autorisation **Contrôle total** et le **groupe Administrateur de domaine** avec l'autorisation **Contrôle total**.
  - d. Cliquez sur **Mise en cache** et cochez l'option **Aucun fichier ou programme du dossier partagé n'est disponible hors connexion**.



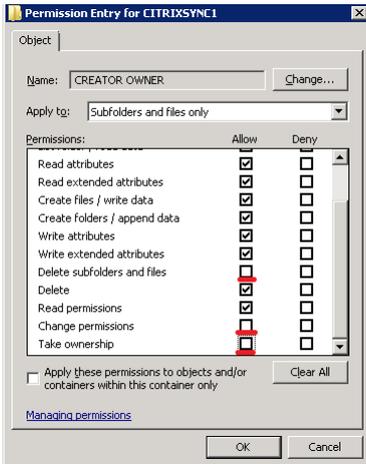
3. Pour accorder les autorisations de sécurité, cliquez avec le bouton droit sur le dossier **CITRIXSYNC1** et sélectionnez **Propriétés > Sécurité**.

4. Pour désactiver les autorisations pouvant être héritées, cliquez sur **Avancé > Modifier les autorisations**, décochez la case **Inclure les autorisations pouvant être héritées du parent de cet objet** et cliquez sur **Ajouter** dans la fenêtre d'avertissement.

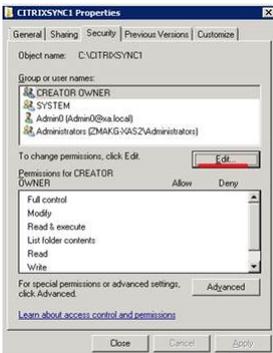


5. Cliquez sur **Modifier** pour modifier les autorisations **Créateur propriétaire** et décochez les cases suivantes :

- o Contrôle total
- o Suppression de sous-dossier et fichier
- o Modifier les autorisations
- o Appropriation



6. Pour supprimer le groupe d'utilisateurs non requis et ajouter le **Compte de proxy de données**, cliquez sur **Modifier** sur l'écran **Propriétés** et supprimez tous les utilisateurs à l'exception de **Créateur propriétaire/Système/Administrateurs locaux**, et ajoutez le **Compte de proxy de données** avec l'autorisation **Contrôle total**.



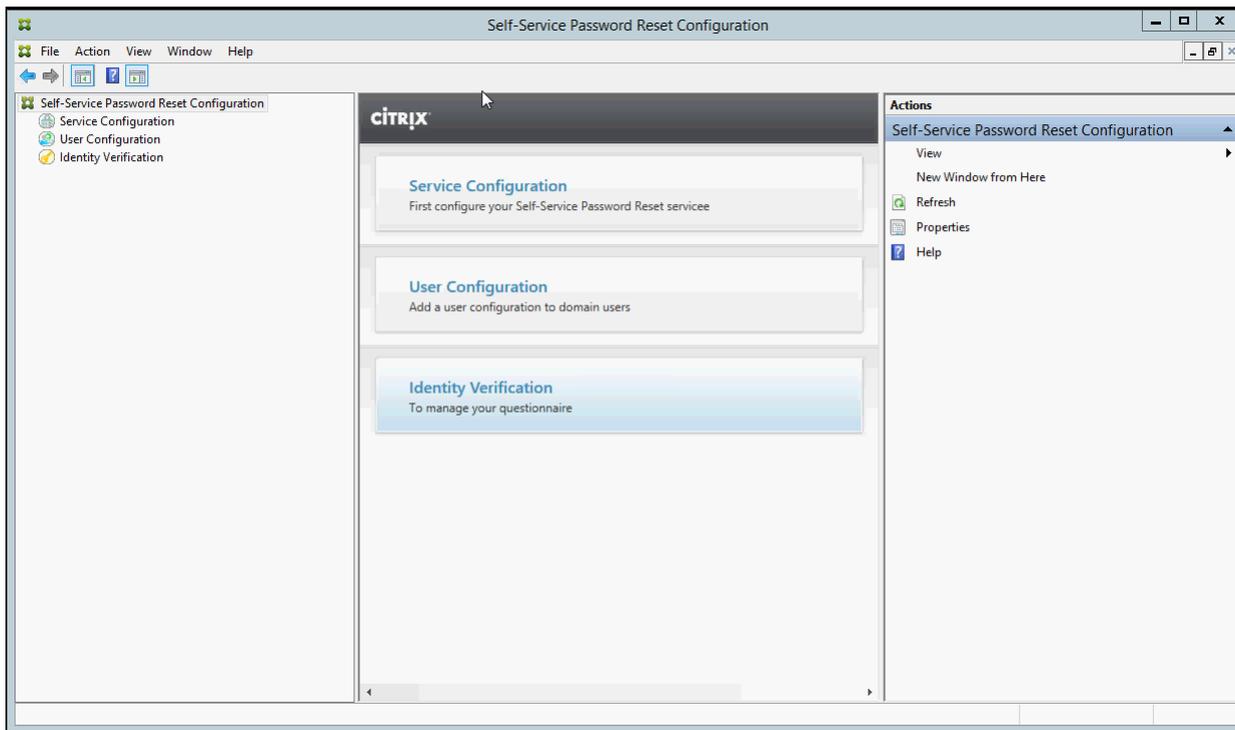
7. Pour activer la fonctionnalité de signature SMB, cliquez sur **Démarrer > Outils d'administration > Stratégie de sécurité locale**. Dans le panneau de gauche, choisissez **Paramètres de sécurité > Stratégies locales > Options de sécurité**.

8. Activez **Client réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)** et **Serveur réseau Microsoft : communications signées numériquement (lorsque le serveur l'accepte)**.

9. Pour interdire l'accès distant au magasin central local, terminez la configuration du pare-feu Windows. Pour de plus amples informations, consultez la section [Configurer les paramètres de pare-feu](#).

Le pack d'installation figure sur le support d'installation de XenApp et XenDesktop.

1. Démarrez l'assistant d'installation du module de réinitialisation en libre-service des mots de passe et suivez les étapes.
2. Cliquez sur **Démarrer > Tous les programmes > Citrix > Configuration du module de réinitialisation en libre-service des mots de passe de Citrix** pour configurer le service de réinitialisation en libre-service des mots de passe de Citrix.
3. Lorsque la console s'ouvre, suivez ces trois procédures de base pour configurer le service.



## Configuration du service

Avant de configurer le service, assurez-vous d'avoir créé le magasin central, le compte de proxy de données et le compte en libre-service.

1. Sélectionnez **Configuration du service** dans le panneau du milieu, puis cliquez sur **Nouvelle configuration du service** dans le panneau de droite.
2. Sur l'écran **Emplacement du magasin central**, spécifiez l'emplacement du magasin central et cliquez sur **Suivant**.
3. Dans l'écran **Configurations de domaines**, sélectionnez un domaine et cliquez sur **Propriétés**.
4. Spécifiez le nom d'utilisateur et le mot de passe du **compte du proxy de données** ainsi que le nom d'utilisateur et le mot de passe du **compte en libre-service**, puis cliquez sur **OK**, **Suivant** et **Terminer**.

## Configuration utilisateur

1. Dans le panneau de gauche, sélectionnez **Configuration utilisateur**, puis cliquez sur **Nouvelle configuration utilisateur** dans le panneau de droite.
2. Sur l'écran **Nommer la configuration utilisateur**, définissez les groupes d'utilisateurs cible du service de réinitialisation en libre-service des mots de passe, ajoutez des utilisateurs/groupes/unités d'organisation depuis Active Directory et cliquez sur **Suivant**.
3. Dans l'écran **Configurer les licences**, spécifiez le serveur de licences, puis cliquez sur **Suivant**.
4. Sur l'écran **Configurer la réinitialisation des mots de passe**, utilisez les cases à cocher pour indiquer si les utilisateurs peuvent réinitialiser leurs mots de passe Windows et déverrouiller leurs comptes de domaine sans l'intervention de l'administrateur, indiquez l'adresse et le port du service et cliquez sur **Créer**.

Pour de plus amples informations sur la gestion des configurations utilisateur, consultez la section [Gérer les configurations utilisateur](#).

## Vérification d'identité

1. Dans le panneau de gauche, sélectionnez le nœud **Vérification d'identité**, puis cliquez sur **Gérer les questions** dans le panneau de droite.
2. Sur l'écran **Authentification avec questions**, sélectionnez la langue par défaut, utilisez la case à cocher pour afficher ou masquer les réponses aux questions de sécurité, puis cliquez sur **Suivant**.
3. Sur l'écran **Questions de sécurité**, cliquez sur **Ajouter une question**, tapez une question dans la zone de texte, cliquez sur **OK**, puis cliquez sur **Suivant**.
4. Sur l'écran **Questionnaire**, cliquez sur **Ajouter** et sélectionnez une question. Vous pouvez réorganiser vos questions et groupes avec les boutons **Monter** et **Descendre**. Lorsque vous en avez terminé avec cette page, cliquez sur **Créer** et **OK**.

Pour de plus amples informations sur la gestion des questions de vérification d'identité, consultez la section [Gérer les questions de vérification d'identité](#).

Une configuration utilisateur vous permet de contrôler le comportement et l'apparence de l'interface lorsque les utilisateurs se connectent à StoreFront. La création d'une nouvelle configuration constitue la dernière étape à suivre avant de distribuer le module de réinitialisation en libre-service des mots de passe aux utilisateurs de votre environnement. Notez que vous pouvez modifier à tout moment les configurations utilisateur existantes.

Une configuration utilisateur constitue une collection unique de paramètres que vous appliquez à des utilisateurs associés à une hiérarchie Active Directory (une unité organisationnelle ou un utilisateur) ou à un groupe Active Directory.

Une configuration utilisateur comporte les éléments suivants :

- Les utilisateurs associés à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory.

**Important** : les groupes de distribution et les groupes locaux de domaine en mode Active Directory mixte ne sont pas pris en charge.

- Serveur de licences
- Fonctionnalités en libre-service (déverrouillage de compte et réinitialisation de mot de passe)

Avant de créer vos configurations utilisateur, assurez-vous que vous avez déjà créé ou défini les éléments suivants :

- Magasin central
- Configuration du service

#### Pour créer une configuration utilisateur

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Citrix** > **Configuration du module de réinitialisation en libre-service des mots de passe de Citrix**.
2. Dans le panneau gauche, sélectionnez le nœud **Configurations utilisateur**.
3. À partir du menu **Actions**, cliquez sur **Ajouter une nouvelle configuration utilisateur**.

#### Pour ajouter des utilisateurs, une unité d'organisation ou un groupe

La page **Nommer la configuration utilisateur** de l'assistant **Configuration utilisateur** vous permet d'associer la configuration utilisateur aux utilisateurs.

Association de la configuration utilisateur :

Vous disposez de deux options d'association des utilisateurs : à une hiérarchie de domaine Active Directory (unité organisationnelle ou utilisateur) ou à un groupe Active Directory. Si nécessaire, vous pouvez associer la configuration utilisateur à une autre hiérarchie ou un autre groupe plus tard, en cliquant sur **Modifier la configuration utilisateur** dans le menu **Actions**.

L'association de configurations utilisateur à des groupes n'est prise en charge que dans des domaines Active Directory utilisant l'authentification Active Directory.

Sélectionnez l'unité d'organisation, les utilisateurs ou le groupe sur la page **Nommer la configuration utilisateur** (à partir de l'assistant Nouvelle configuration utilisateur ou Modifier la configuration utilisateur).

**Remarque** : nous ne vous recommandons pas d'inclure de comptes avec privilèges (par exemple, Administrateurs locaux ou Administrateurs de domaine) dans le groupe d'utilisateurs pour lequel le compte de réinitialisation en libre-service des mots de passe peut réinitialiser des mots de passe. Utilisez un nouveau groupe dédié.

#### Pour configurer les licences

La page **Configurer les licences** de l'assistant **Configuration utilisateur** vous permet de configurer le serveur de licences utilisé par le service de réinitialisation en libre-service des mots de passe.

**Remarque**: vous pouvez utiliser les fonctionnalités Déverrouiller et réinitialiser uniquement si vous disposez de l'édition Platinum de XenApp ou XenDesktop.

Entrez le nom du serveur de licences et le numéro de port sur la page **Configurer les licences** (à partir de l'assistant Nouvelle configuration utilisateur ou Modifier la configuration utilisateur).

#### Pour activer les fonctionnalités de déverrouillage ou de réinitialisation

La réinitialisation en libre-service des mots de passe permet aux utilisateurs de réinitialiser leur mot de passe et déverrouiller leurs comptes de domaine Windows sans intervention de l'administrateur. Dans la page **Activer réinitialisation en libre-service des mots de passe**, vous pouvez sélectionner les fonctionnalités à activer.

Sélectionnez le composant que vous souhaitez que les utilisateurs utilisent : **Déverrouiller** ou **Réinitialiser** sur la page **Activer réinitialisation en libre-service des mots de passe** (à partir de l'assistant Nouvelle configuration utilisateur ou Modifier la configuration utilisateur).

#### Pour configurer une liste noire

Les administrateurs informatiques peuvent ajouter des utilisateurs et des groupes à la liste noire. Les utilisateurs et groupes présents dans une liste noire ne peuvent utiliser aucune des fonctionnalités de la Réinitialisation en libre-service des mots de passe - y compris l'inscription, le déverrouillage de compte et la réinitialisation des mots de passe. De même, un utilisateur répertorié sur la liste noire ne voit pas le bouton **TÂCHE** sur Citrix Receiver après s'être connecté.

Pour configurer la liste noire

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Citrix** > **Configuration du module de réinitialisation en libre-service des mots de passe de Citrix**.
2. Dans le panneau de gauche, sélectionnez **Configuration utilisateur**, puis cliquez sur **Configuration de la liste noire** dans le panneau de droite.
3. Utilisez les boutons **Ajouter** et **Supprimer** pour ajouter et supprimer des utilisateurs ou groupes de la liste noire.

La vérification d'identité de la console Configuration du module de réinitialisation en libre-service des mots de passe de Citrix fournit un emplacement central permettant de gérer toutes les questions de sécurité associées à la vérification d'identité, à la réinitialisation en libre-service des mots de passe et au déverrouillage de compte. Vous pouvez ajouter vos propres questions de sécurité à la liste de questions par défaut et créer des groupes de questions.

- Si vous modifiez les questions fournies par défaut après l'enregistrement des réponses des utilisateurs, tenez compte de la signification des questions modifiées. La modification d'une question ne force pas une réinscription. Toutefois, si la signification d'une question est changée, les utilisateurs qui ont répondu auparavant à cette question peuvent se retrouver incapables d'y apporter une réponse.
- L'ajout, la suppression et le remplacement de questions de sécurité après inscription des utilisateurs avec les anciennes questions entraînent l'impossibilité pour ces utilisateurs de s'authentifier et de réinitialiser leur mot de passe tant qu'ils ne sont pas réinscrits. Les utilisateurs doivent répondre à des nouvelles questions lorsqu'ils ouvrent les tâches dans Receiver.
- Chaque question de sécurité peut appartenir à plusieurs groupes de questions de sécurité. Lorsque vous créez des groupes de questions de sécurité, toutes vos questions peuvent être utilisées dans n'importe quel groupe.

Utilisez ces étapes pour accéder aux paramètres référencés dans les procédures suivantes :

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Citrix** > **Configuration du module de réinitialisation en libre-service des mots de passe de Citrix**.
2. Dans le panneau gauche, sélectionnez le nœud **Vérification d'identité**.
3. À partir du menu **Actions**, cliquez sur **Gérer les questions**.

#### Pour définir la langue par défaut

Dans la plupart des cas, les utilisateurs voient les questions de sécurité s'afficher dans la langue associée à leur profil utilisateur actuel. Si la langue n'est pas disponible, la réinitialisation en libre-service des mots de passe affiche les questions dans la langue par défaut spécifiée.

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Citrix** > **Configuration du module de réinitialisation en libre-service des mots de passe de Citrix**.
2. Dans le panneau gauche, sélectionnez le nœud **Vérification d'identité**.
3. À partir du menu **Actions**, cliquez sur **Gérer les questions**.
4. Dans la liste déroulante **Langue par défaut** de la page **Authentification avec questions**, sélectionnez la langue par défaut.

Pour activer le masquage des réponses de sécurité

Le masquage des réponses de sécurité apporte un niveau de sécurité supplémentaire à vos utilisateurs lorsqu'ils enregistrent leur réponses aux questions de sécurité ou qu'ils enregistrent leurs questions de sécurité ou qu'ils fournissent leurs réponses lors de la vérification d'identité. Lorsque cette fonctionnalité est activée, les réponses des utilisateurs sont masquées. Lors de l'enregistrement des réponses, ces utilisateurs sont invités à taper leurs réponses deux fois afin d'éviter les fautes de frappe ou d'orthographe. Les utilisateurs ne doivent taper leurs réponses qu'une seule fois lors de la validation d'identité, puisqu'ils sont invités à réessayer en cas d'erreur.

Sélectionnez **Masquer les réponses aux questions de sécurité** sur la page **Authentification avec questions**.

#### Pour créer de nouvelles questions de sécurité

Vous pouvez créer différentes questions et choisir une langue pour chacune d'entre elles. Vous pouvez aussi saisir plusieurs traductions d'une même question. L'inscription dans Receiver présente à l'utilisateur le questionnaire dans la langue définie dans les paramètres de langue de son profil. Si la langue n'est pas disponible, la réinitialisation en libre-service des mots de passe affiche les questions dans la langue par défaut.

Remarque : lorsque vous sélectionnez une langue pour une question de sécurité, la question est présentée aux utilisateurs dont les paramètres de système d'exploitation sont définis pour cette langue. Si les paramètres de système d'exploitation sélectionnés ne correspondent pas à ceux de certaines questions disponibles, la langue par défaut est utilisée.

1. Depuis la liste déroulante **Langue** de la page **Questions de sécurité**, sélectionnez une langue et cliquez sur **Ajouter une question**. La boîte de dialogue Question de sécurité s'affiche.
2. Créez la nouvelle question dans la boîte de dialogue **Question de sécurité**.

**Important** : vous devez utiliser le bouton **Modifier** pour ajouter le texte traduit des questions existantes. Si vous sélectionnez **Ajouter une question**, vous créez une nouvelle question qui n'est pas associée à l'original.

#### Pour ajouter ou modifier le texte de questions existantes

L'ajout, la suppression et le remplacement de questions de sécurité après inscription des utilisateurs avec les anciennes questions entraînent l'impossibilité pour ces utilisateurs de s'authentifier et de réinitialiser leur mot de passe tant qu'ils ne sont pas réinscrits. Les utilisateurs doivent répondre à des nouvelles questions lorsqu'ils ouvrent les tâches dans Receiver. La modification d'une question n'oblige pas un utilisateur à se réinscrire.

**Important** : si vous modifiez une question existante, préservez-en le sens. Dans le cas contraire, il est possible que les réponses des utilisateurs ne correspondent pas lors des authentifications ultérieures. En d'autres termes, l'utilisateur risque de fournir une réponse ne correspondant pas à la réponse enregistrée.

1. Sélectionnez une langue dans la liste déroulante **Langue** sur la page **Questions de sécurité**.
2. Sélectionnez la question et cliquez sur **Modifier**.
3. Modifiez la question dans la boîte de dialogue **Question de sécurité**.

#### Pour créer un groupe de questions de sécurité

Vous pouvez créer des questions de sécurité auxquelles répondent vos utilisateurs pour confirmer leur identité. Chaque question ajoutée au questionnaire doit recevoir une réponse des utilisateurs. Cependant, vous pouvez également rassembler ces questions dans un groupe de questions de sécurité.

Les groupes de questions permettent d'ajouter, par exemple, six questions à un questionnaire et de permettre aux utilisateurs de choisir de ne répondre qu'à trois d'entre elles. Ils bénéficient ainsi d'une plus grande souplesse dans la sélection des questions et la saisie des réponses de vérification d'identité.

1. Cliquez sur **Ajouter un groupe** sur la page **Questions de sécurité**.
2. Dans la boîte de dialogue **Groupe de questions de sécurité**, donnez un nom au groupe, sélectionnez les questions et spécifiez le nombre de questions auquel l'utilisateur doit répondre.

#### Pour modifier un groupe de questions de sécurité

Sélectionnez le groupe de questions de sécurité à modifier et cliquez sur **Modifier** sur la page **Questions de sécurité**. La boîte de dialogue Groupe de questions de sécurité présente une liste de questions de sécurité pouvant faire partie du groupe. Les questions du groupe sont signalées par une coche. Vous pouvez modifier le nom du groupe, ajouter des questions au groupe et sélectionner le nombre de questions nécessitant une réponse de l'utilisateur.

#### Pour ajouter ou supprimer le questionnaire existant

Ajoutez ou supprimez des questions et des groupes de questions de sécurité du questionnaire. Déplacez les questions vers le haut ou vers le bas pour organiser leur ordre de présentation. Si le questionnaire a été modifié, l'utilisateur doit être averti qu'il doit réenregistrer des questions après l'ouverture de session StoreFront.

1. Cliquez sur **Ajouter** sur la page **Questionnaire** pour ajouter une question ou un groupe au questionnaire.
2. Cliquez sur **Supprimer** pour supprimer une question du questionnaire.
3. Cliquez sur **Monter** ou **Descendre** pour gérer les questions présentées à l'utilisateur.

La réinitialisation en libre-service des mots de passe vous permet d'effectuer ce qui suit :

- Importer ou exporter les questions de sécurité.
- Révoquer les questions de sécurité d'un utilisateur.

#### Pour importer ou exporter les questions de sécurité

Vous pouvez importer ou exporter les données de groupes et questions de sécurité.

1. Cliquez sur **Démarrer** > **Tous les programmes** > **Citrix** > **Configuration du module de réinitialisation en libre-service des mots de passe de Citrix**.
2. Dans le panneau gauche, sélectionnez le nœud **Vérification d'identité**.
3. Dans le menu **Actions**, cliquez sur l'une des options suivantes :

##### Importer les questions de sécurité

Spécifiez l'emplacement du fichier sur lequel importer les données des groupes et questions de sécurité.

##### Exporter les questions de sécurité

Spécifiez l'emplacement du fichier sur lequel exporter les données des groupes et questions de sécurité.

# Sécuriser la configuration

Dec 08, 2016

Cet article contient les procédures à suivre pour vous assurer que les composants de la réinitialisation en libre-service des mots de passe sont déployés et configurés de manière sécurisée.

- Créer un compte d'utilisateur de domaine pour réinitialiser le mot de passe de l'utilisateur et déverrouiller le compte utilisateur
- Configurer les paramètres du pare-feu

Si vous utilisez les fonctionnalités Réinitialisation du mot de passe ou Déverrouillage de compte de la réinitialisation en libre-service des mots de passe, spécifiez un compte en libre-service lors de la configuration du service. Ce compte est utilisé par le module en libre-service pour exécuter les fonctionnalités Réinitialisation du mot de passe et Déverrouillage de compte. Assurez-vous que le compte dispose de privilèges suffisants, mais nous ne recommandons pas d'utiliser un compte appartenant au groupe Administrateurs de domaine pour les déploiements de production. Les privilèges de compte recommandés sont les suivants :

- Membre du domaine
- Autorisations de réinitialisation du mot de passe et de déverrouillage de compte accordées aux utilisateurs du domaine appropriés

Dans **Utilisateurs et ordinateurs Active Directory**, créez le groupe ou compte d'utilisateur afin qu'il soit autorisé à réinitialiser le mot de passe de l'utilisateur et à déverrouiller des comptes d'utilisateur.

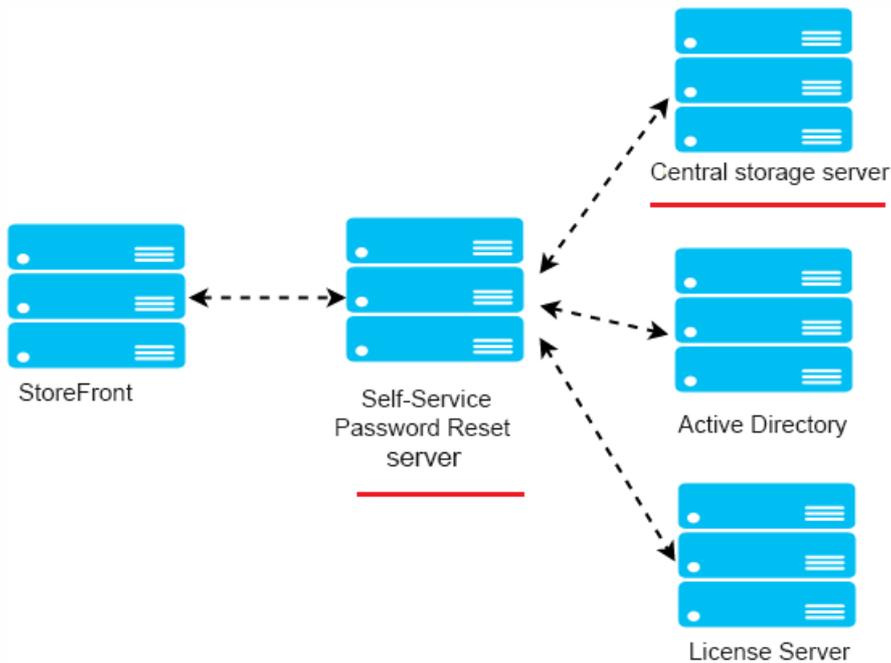
1. Dans **Utilisateurs et ordinateurs Active Directory**, cliquez avec le bouton droit sur le domaine, puis sur **Délégation de contrôle** dans le menu.
2. L'assistant **Délégation de contrôle** s'affiche. Dans la boîte de dialogue **Bienvenue**, cliquez sur **Suivant**.
3. Dans la boîte de dialogue **Utilisateurs et groupes**, cliquez sur **Ajouter**. Sélectionnez le groupe dans la liste auquel vous souhaitez accorder le droit de déverrouiller des comptes, puis cliquez sur **OK**. Dans la boîte de dialogue **Utilisateurs et groupes**, cliquez sur **Suivant**.
4. Sur la boîte de dialogue **Tâches à déléguer**, cliquez sur **Créer une tâche personnalisée à déléguer**, puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Type d'objet Active Directory**, cliquez sur **Seulement des objets suivants dans le dossier > Objets USER**, puis cliquez sur **Suivant**.
6. Dans la boîte de dialogue **Autorisations**, sélectionnez les cases à cocher **Général** et **Spécifiques aux propriétés**. Dans la liste **Autorisations**, sélectionnez les cases à cocher **Read lockoutTime**, **Write lockoutTime**, **Reset Password**, **Change Password**, **Read userAccountControl**, **Write userAccountControl**, **Read pwdLastSet** et **Write pwdLastSet**, puis cliquez sur **Suivant**.
7. Sur la boîte de dialogue **Fin de l'Assistant Délégation de contrôle**, cliquez sur **Terminer**.

Étant donné que les composants du serveur de réinitialisation en libre-service des mots de passe et du serveur de stockage central gèrent les mots de passe des utilisateurs, nous vous recommandons fortement de déployer ces composants sur un réseau fiable. Vous devez également vous assurer que ces serveurs ne peuvent être contactés que par des composants

approuvés spécifiques. Cette section décrit les étapes à suivre pour vous assurer de configurer correctement le pare-feu Windows pour ces serveurs. Nous vous recommandons également de configurer l'infrastructure réseau existante pour vous assurer que ces serveurs sont isolés du trafic réseau non fiable.

Après avoir terminé ces configurations dans le déploiement, les serveurs du magasin central de réinitialisation en libre-service des mots de passe peuvent être accessibles uniquement à partir de serveurs de réinitialisation en libre-service des mots de passe utilisant SMB (Server Message Block), et les serveurs de réinitialisation en libre-service des mots de passe sont accessibles uniquement à partir des serveurs StoreFront utilisant des connexions HTTPS.

## Déploiement d'un partage de fichiers à distance pour Windows 2012 R2



### Environnement

- Déployez les composants de réinitialisation en libre-service des mots de passe sur des serveurs dédiés. Ne les déployez pas sur les mêmes serveurs que ceux des composants StoreFront ou Delivery Controller existants, sinon la configuration du pare-feu affichée ci-dessous pourrait bloquer le trafic de StoreFront ou du Controller.
- Il n'existe aucun proxy HTTP/HTTPS non-transparent entre StoreFront et le serveur de réinitialisation en libre-service des mots de passe.

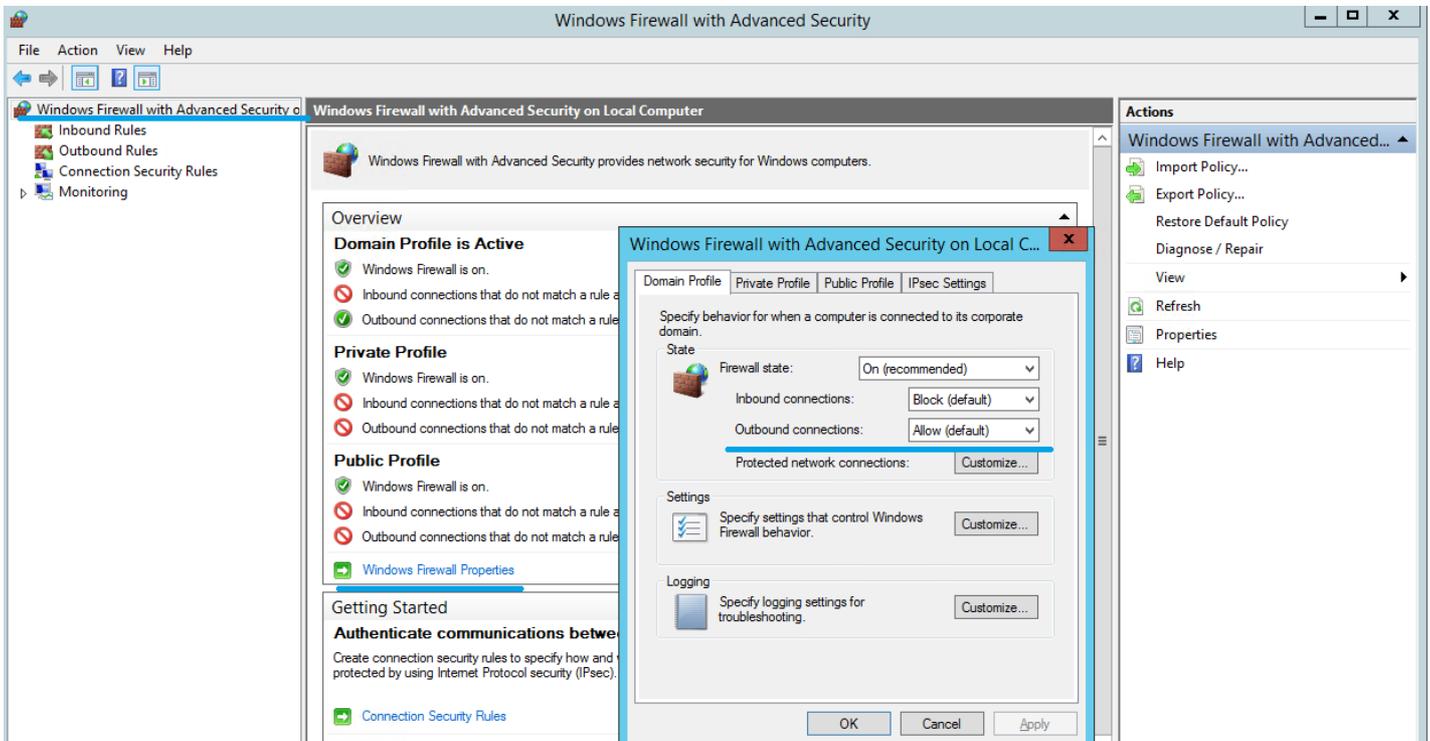
Si aucun proxy non-transparent n'existe entre StoreFront et le serveur de réinitialisation en libre-service des mots de passe, configurez le serveur de réinitialisation en libre-service des mots de passe de façon à ce qu'il soit uniquement accessible à partir du serveur proxy dans les règles de pare-feu.

- Les configurations dans ces procédures sont basées sur les règles de pare-feu Windows par défaut.

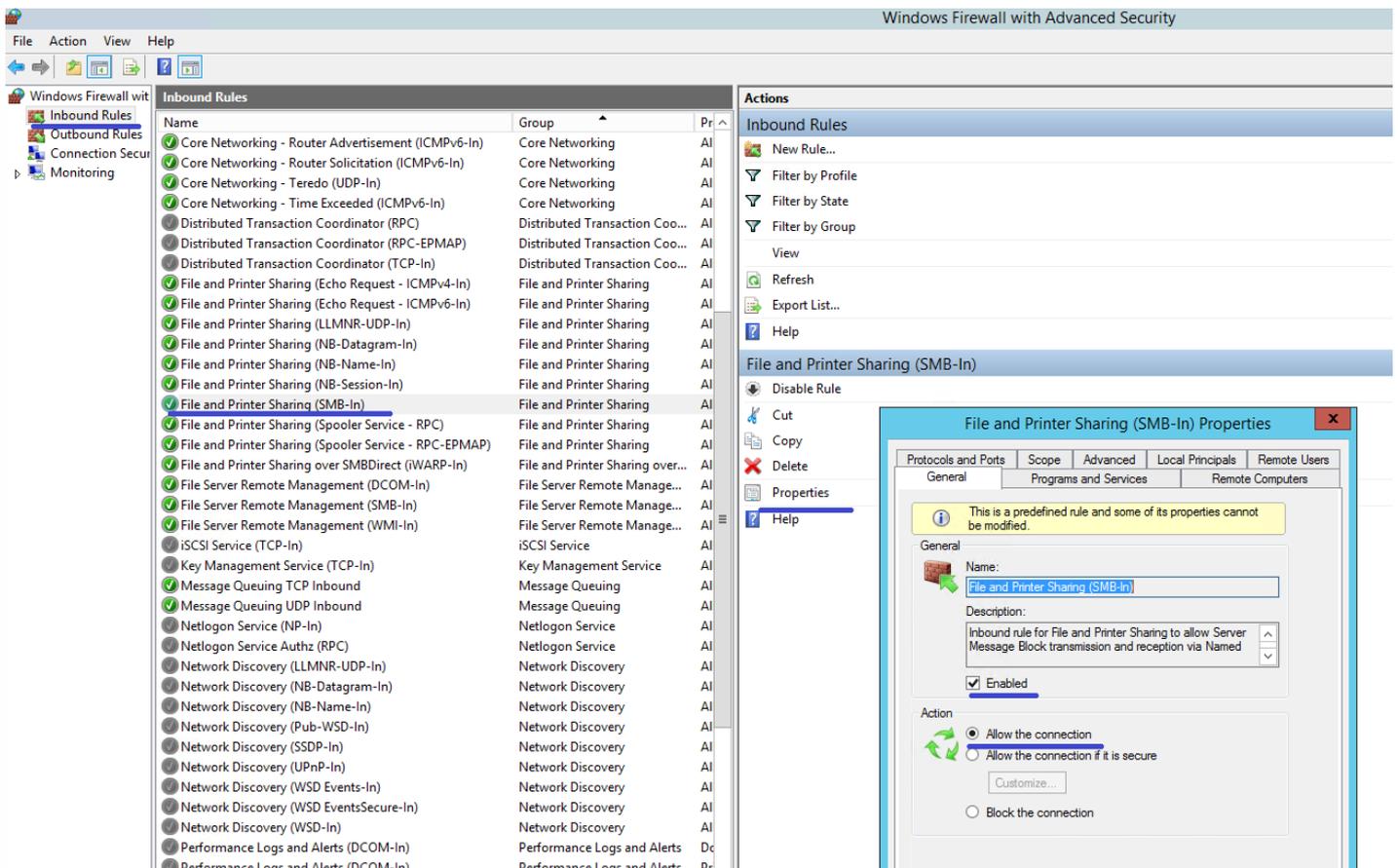
### Configurer le pare-feu pour le magasin central de réinitialisation en libre-service des mots de passe

Une fois la configuration terminée, le service SMB fourni par le magasin central de réinitialisation en libre-service des mots de passe est accessible uniquement à partir des serveurs de réinitialisation en libre-service des mots de passe pour le trafic entrant, et le serveur du magasin central de réinitialisation en libre-service des mots de passe peut accéder au service se trouvant sur le réseau d'entreprise uniquement pour le trafic sortant.

1. Ouvrez le Gestionnaire de serveur, et à partir du menu **Outils** sur la barre de navigation supérieure, sélectionnez **Pare-feu Windows avec sécurité avancée**.
2. Dans la boîte de dialogue **Pare-feu Windows avec sécurité avancée**, sélectionnez **Propriétés du Pare-feu Windows** dans le panneau central. Il existe trois profils de pare-feu : domaine, privé et public. Sélectionnez l'onglet **Profil de domaine**. Vérifiez que **État du pare-feu** est défini sur **Activé**, que **Connexions entrantes** est défini sur **Bloquer** et que **Connexions sortantes** est défini sur **Autoriser**.



3. Sélectionnez les onglets **Profil privé** et **Profil public** et vérifiez que **État du pare-feu** est défini sur **Activé**, et que **Connexions entrantes** et **Connexions sortantes** sont définis sur **Bloquer**. Appliquez et enregistrez les modifications.
4. À partir de **Règles de trafic entrant**, choisissez **Partage de fichiers et d'imprimantes (SMB-Entrée)** et assurez-vous que cette règle est **Activée**, et que **Action** est défini sur **Autoriser la connexion**.



5. Sur **Propriétés du partage de fichiers et d'imprimantes (SMB-Entrée)**, sur l'onglet **Étendue**, choisissez **Ces adresses IP**, et ajoutez toutes les adresses IP du serveur de réinitialisation en libre-service des mots de passe à la liste. Par exemple, le serveur de réinitialisation en libre-service des mots de passe A (192.168.1.10) et le serveur de réinitialisation en libre-service des mots de passer B (192.168.1.11).

6. Sur **Propriétés du partage de fichiers et d'imprimantes (SMB-Entrée)**, sur l'onglet **Avancé**, sélectionnez les profils **Domaine**, **Privé** et **Public**, et enregistrez les modifications apportées à cette règle.

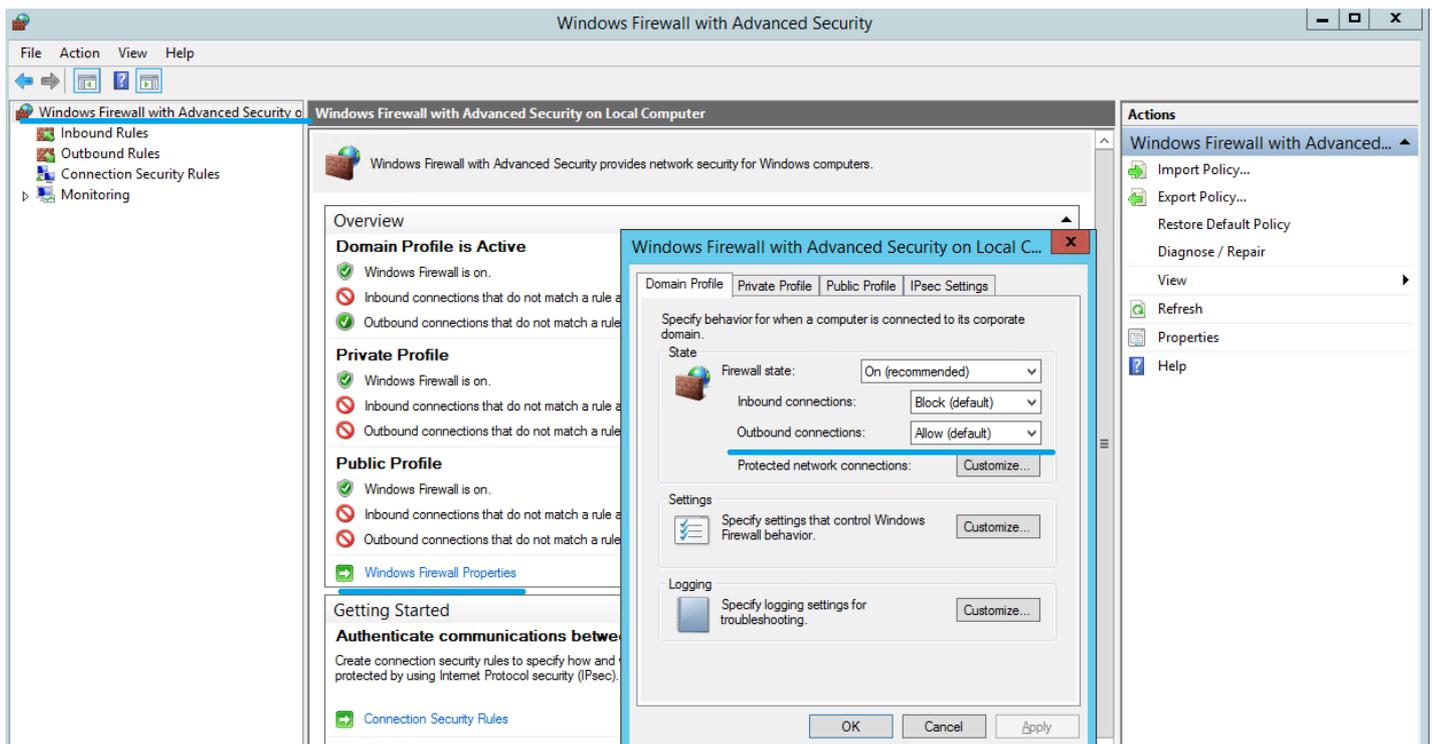
7. Répétez cette procédure pour les règles de **trafic entrant pour Administration à distance du serveur de fichiers (SMB-In)** et **Partage de fichiers et d'imprimantes (NB-Session-Entrée)**.

## Configurer le pare-feu pour le serveur de réinitialisation en libre-service des mots de passe

Une fois la configuration terminée, le service Web fourni par les serveurs de réinitialisation en libre-service des mots de passe est accessible uniquement à partir des serveurs StoreFront utilisant HTTPS, et les serveurs de réinitialisation en libre-service des mots de passe peuvent accéder au service se trouvant sur le réseau d'entreprise.

1. Ouvrez le **Gestionnaire de serveur**, et à partir du menu **Outils** sur la barre de navigation supérieure, sélectionnez **Pare-feu Windows avec sécurité avancée**.

2. Dans la boîte de dialogue **Pare-feu Windows avec sécurité avancée**, sélectionnez **Propriétés du Pare-feu Windows** dans le panneau central. Il existe trois profils de pare-feu : domaine, privé et public. Sélectionnez l'onglet **Profil de domaine**. Vérifiez que **État du pare-feu** est défini sur **Activé**, que **Connexions entrantes** est défini sur **Bloquer** et que **Connexions sortantes** est défini sur **Autoriser**.

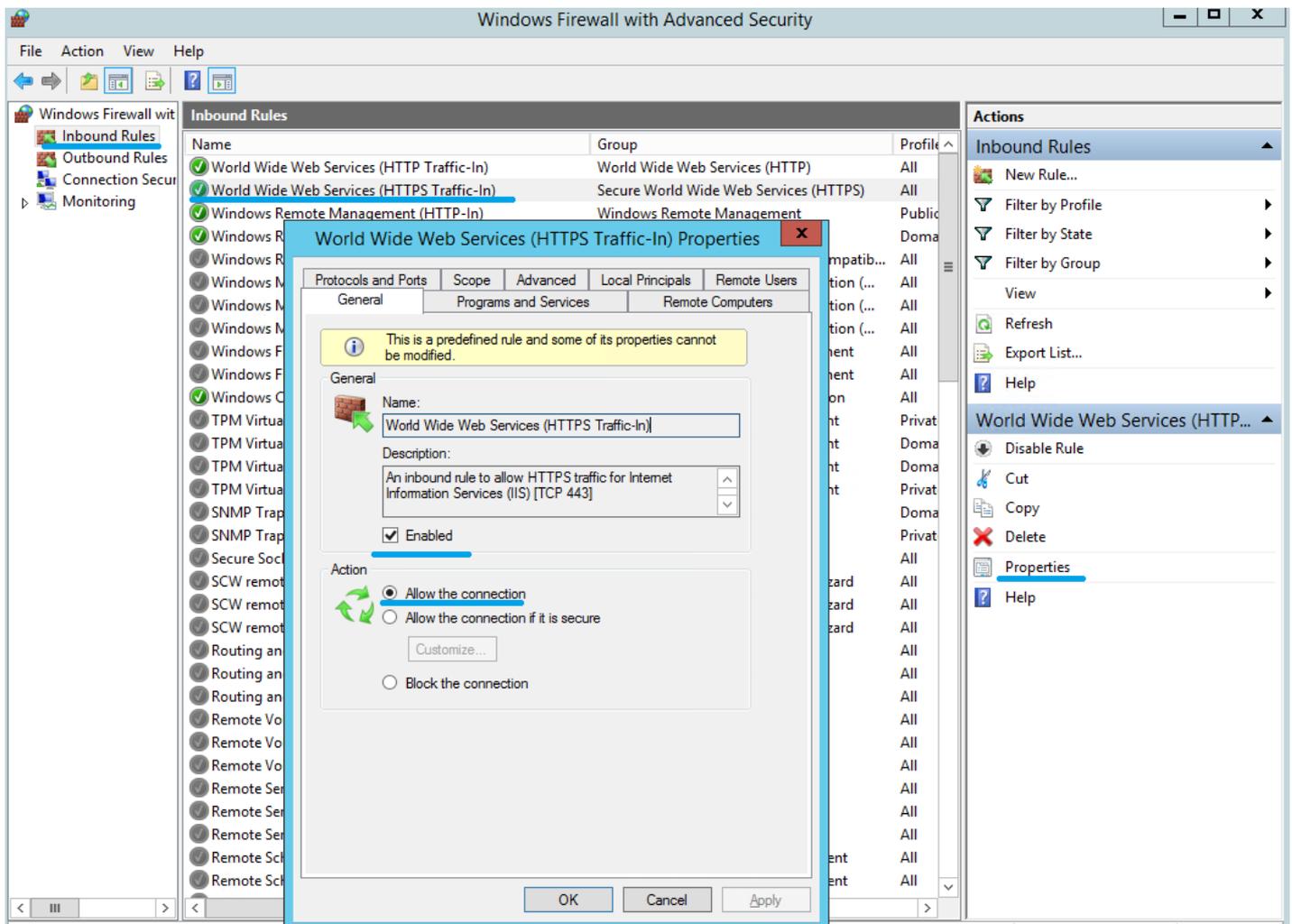


3. Sélectionnez les onglets **Profil privé** et **Profil public** et vérifiez que **État du pare-feu** est défini sur **Activé**, et que **Connexions entrantes** et **Connexions sortantes** sont définis sur **Bloquer**. Appliquez et enregistrez les modifications.

4. À partir de **Règles de trafic entrant**, choisissez **Services World Wide Web (trafic HTTP)** et assurez-vous que cette règle est **Activée**, et que **Action** est défini sur **Bloquer la connexion**.

5. Sur **Propriétés des services World Wide Web (trafic HTTP)**, sur l'onglet **Avancé**, sélectionnez les profils **Domaine**, **Privé** et **Public**, et enregistrez les modifications apportées à cette règle.

6. À partir de **Règles de trafic entrant**, choisissez **Services World Wide Web (trafic HTTPS)** et assurez-vous que cette règle est **Activée**, et que **Action** est défini sur **Autoriser la connexion**.



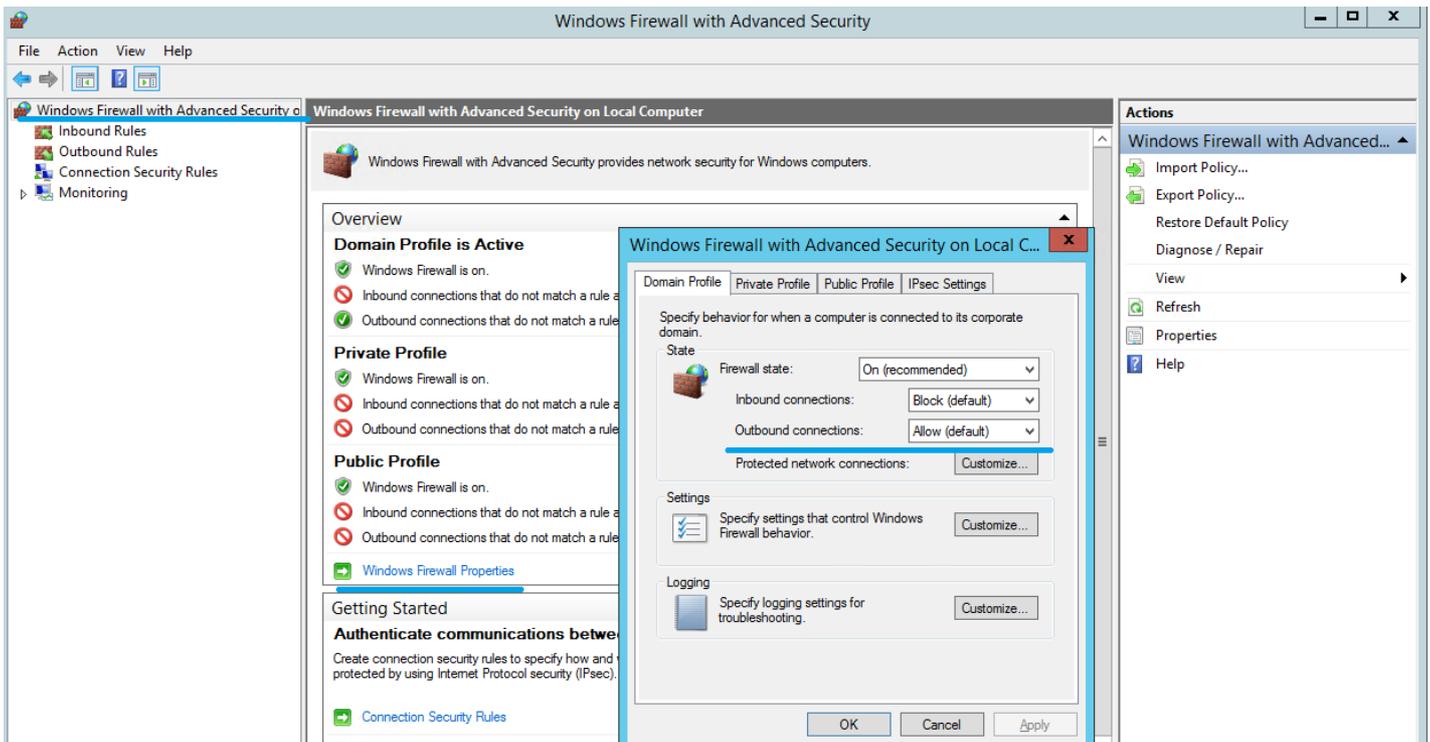
7. Sur **Propriétés des services World Wide Web (trafic HTTPS)**, sur l'onglet **Étendue**, choisissez **Ces adresses IP**, et ajoutez toutes les adresses IP du serveur StoreFront à la liste. Par exemple, StoreFront A (192.168.1.50) et StoreFront B (192.158.1.51).

8. Sur **Propriétés des services World Wide Web (trafic HTTPS)**, sur l'onglet **Avancé**, sélectionnez les profils **Domaine**, **Privé** et **Public**, et enregistrez les modifications apportées à cette règle.

## Déploiement d'un partage de fichiers local pour Windows 2008 R2

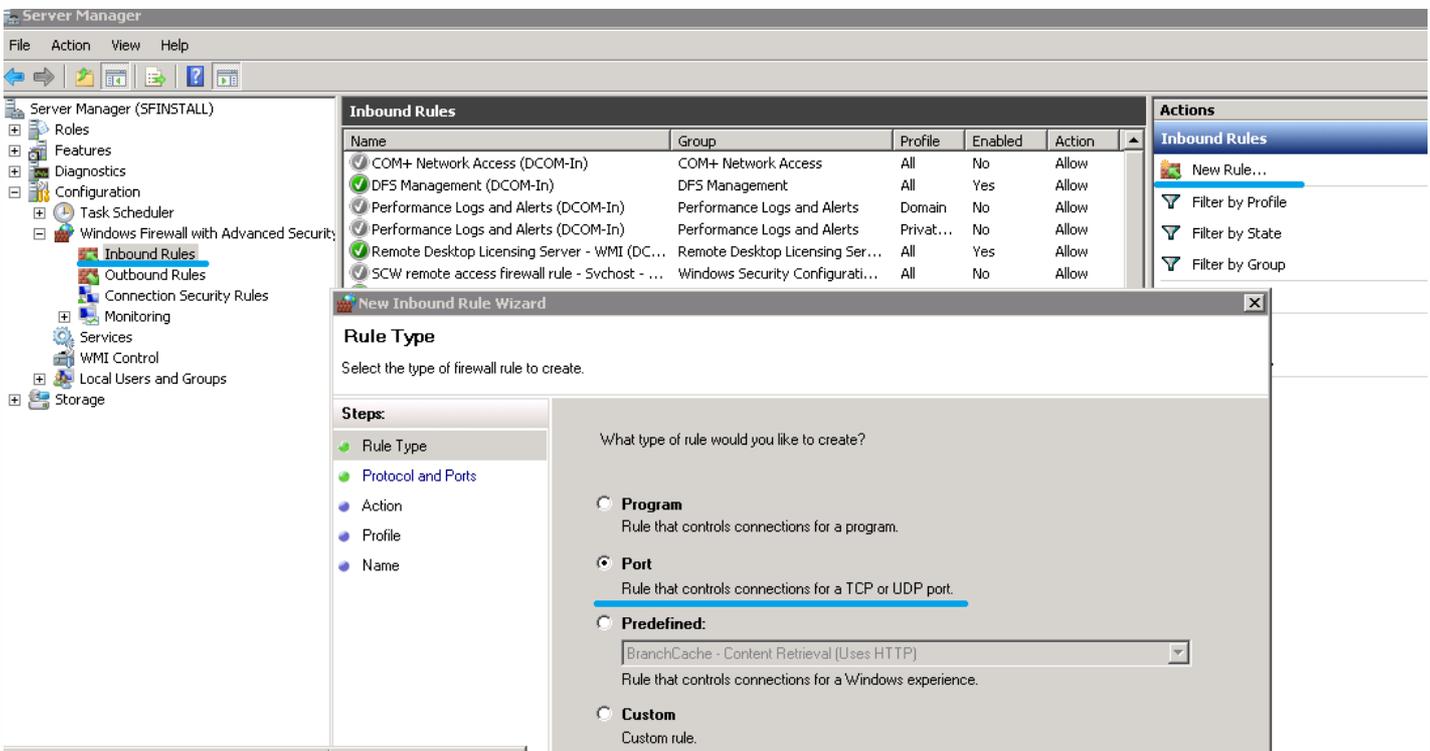
Une fois la configuration terminée, tout accès SMB à partir d'un client distant est bloqué. Le partage de fichiers SMB est uniquement accessible en local, et le service de réinitialisation en libre-service des mots de passe est uniquement accessible depuis les serveurs StoreFront qui utilisent une connexion HTTPS.

1. Ouvrez le Gestionnaire de serveur, et à partir du menu **Outils** sur la barre de navigation supérieure, sélectionnez **Pare-feu Windows avec sécurité avancée**.
2. Dans la boîte de dialogue **Pare-feu Windows avec sécurité avancée**, sélectionnez **Propriétés du Pare-feu Windows** dans le panneau central. Il existe trois profils de pare-feu : domaine, privé et public. Sélectionnez l'onglet **Profil de domaine**. Vérifiez que **État du pare-feu** est défini sur **Activé**, que **Connexions entrantes** est défini sur **Bloquer** et que **Connexions sortantes** est défini sur **Autoriser**.



3. Sélectionnez les onglets **Profil privé** et **Profil public** et vérifiez que **État du pare-feu** est défini sur **Activé**, et que **Connexions entrantes** et **Connexions sortantes** sont définis sur **Bloquer**. Appliquez et enregistrez les modifications.

4. À partir de **Règles de trafic entrant**, choisissez **Nouvelles règles** pour créer une nouvelle règle de trafic entrant. Dans l'**Assistant Nouvelle règle de trafic entrant**, sélectionnez **Type de règle**, choisissez **Port** en tant que type de la nouvelle règle et cliquez sur **Suivant**.



5. Dans l'**Assistant Nouvelle règle de trafic entrant**, sélectionnez **Protocole et ports**, et choisissez **TCP, Ports**

locaux spécifiques, tapez 445 dans la zone de texte et cliquez sur **Suivant**.

- Dans l'Assistant **Nouvelle règle de trafic entrant**, sélectionnez **Action**, choisissez **Bloquer la connexion** et cliquez sur **Suivant**.
- Dans l'Assistant **Nouvelle règle de trafic entrant**, sélectionnez **Profil**, choisissez **Domaine**, **Privé** et **Public** et cliquez sur **Suivant**.
- Dans l'Assistant **Nouvelle règle de trafic entrant**, sélectionnez **Nom**, entrez un nom et une description et cliquez sur **Suivant**.
- À partir de **Règles de trafic entrant**, choisissez **Services World Wide Web (trafic HTTP)** et assurez-vous que cette règle est **Activée**, et que **Action** est défini sur **Bloquer la connexion**.

The screenshot shows the Windows Firewall with Advanced Security console. The left pane shows the tree view with 'Inbound Rules' selected. The right pane displays a list of inbound rules. The rule 'World Wide Web Services (HTTP Traffic-In)' is highlighted. A properties dialog box is open for this rule, showing the 'General' tab. The 'Name' is 'World Wide Web Services (HTTP Traffic-In)' and the 'Description' is 'An inbound rule to allow HTTP traffic for Internet Information Services (IIS) [TCP 80]'. The 'Action' section shows 'Block the connection' selected.

Rule Name	Protocol	Ports	Scope	Action	Profile	Status
Secure Socket Tunneling Protocol (SSTP-In)	Secure Socket Tunneling Proto...	All	No	Allow	No	System
World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Servi...	All	No	Allow	No	System
DFS Management (SMB-In)	DFS Management	All	Yes	Allow	No	System
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No	Allow	No	System
Netlogon Service (NP-In)	Netlogon Service	All	No	Allow	No	System
Remote Administration (NP-In)	Remote Administration	All	No	Allow	No	System
Remote Desktop Licensing Server (NP-In)	Remote Desktop Licensing Ser...	All	Yes	Allow	No	System
Remote Event Log Management (NP-In)	Remote Event Log Management	All	No	Allow	No	System
Remote Service Management (NP-In)	Remote Service Management	All	No	Allow	No	System
Terminal Services (NP-In)	Terminal Services	All	Yes	Allow	No	System
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow	No	%System...
Network Discovery (LLMNR-UDP-In)	Network Discovery	All	No	Allow	No	%System...
Network Discovery (WSD Events-In)	Network Discovery	All	No	Allow	No	System
Network Discovery (WSD EventsSecure-In)	Network Discovery	All	No	Allow	No	System
Core Networking - Dynamic Host Configurati...	Core I					
Windows Remote Management (HTTP-In)	Windc					
Core Networking - Dynamic Host Configurati...	Core I					
BranchCache Content Retrieval (HTTP-In)	Branc					
Windows Remote Management - Compatibilit...	Windc					
World Wide Web Services (HTTP Traffic-In)	World					
Windows Communication Foundation Net.TC...	Windc					
Web Management Service (HTTP Traffic-In)	Web f					
Core Networking - Destination Unreachable (...)	Core I					
Core Networking - Destination Unreachable (...)	Core I					
Core Networking - Internet Group Managem...	Core I					
Core Networking - IPv6 (IPv6-In)	Core I					
Core Networking - Multicast Listener Done (I...	Core I					
Core Networking - Multicast Listener Query (...)	Core I					
Core Networking - Multicast Listener Report ...	Core I					
Core Networking - Multicast Listener Report ...	Core I					
Core Networking - Neighbor Discovery Adve...	Core I					
Core Networking - Neighbor Discovery Solicit...	Core I					
Core Networking - Packet Too Big (ICMPv6-In)	Core I					
Core Networking - Parameter Problem (ICMP...	Core I					
Core Networking - Router Advertisement (IC...	Core I					
Core Networking - Router Solicitation (ICMP...	Core I					
Core Networking - Time Exceeded (ICMPv6-In)	Core I					
Distributed Transaction Coordinator (TCP-In)	Distrib					
File and Printer Sharing (Echo Request - ICM...	File ar					
File and Printer Sharing (Echo Request - ICM...	File ar					
ISCSI Service (TCP-In)	iscsi					

- Sur **Propriétés des services World Wide Web (trafic HTTP)**, sur l'onglet **Avancé**, sélectionnez les profils **Domaine**, **Privé** et **Public**, et enregistrez les modifications apportées à cette règle.
- À partir de **Règles de trafic entrant**, choisissez **Services World Wide Web (trafic HTTPS)** et assurez-vous que cette règle est **Activée**, et que **Action** est défini sur **Autoriser la connexion**.
- Sur **Propriétés des services World Wide Web (trafic HTTPS)**, passez à l'onglet **Étendue**. Dans la section **Adresse IP distante**, choisissez **Ces adresses IP**, et ajoutez toutes les adresses IP du serveur StoreFront à la liste. Par exemple, StoreFront A (192.168.1.13) et StoreFront B (192.158.1.14).

13. Sur **Propriétés des services World Wide Web (trafic HTTP)**, sur l'onglet **Avancé**, sélectionnez les profils **Domaine**, **Privé** et **Public**, et enregistrez les modifications apportées à cette règle.

# Migrer les données depuis le magasin central Single Sign-On

Dec 08, 2016

Le magasin central Single Sign-On est un stockage centralisé permettant à Single Sign-On de stocker et de gérer les données utilisateur et d'administration. Les données utilisateur comprennent notamment les informations d'identification, les réponses aux questions de sécurité et d'autres données relatives à l'utilisateur. Les données d'administration incluent les stratégies de mot de passe, les définitions d'application, les questions de sécurité et d'autres données de portée plus large.

Vous ne pouvez pas migrer toutes les données du magasin central Single Sign-On sur le magasin central de réinitialisation en libre-service des mots de passe. Ce tableau décrit les données qui peuvent et ne peuvent pas être migrées.

Migration impossible	Migration possible
Stratégies de mot de passe : non prises en charge	Dossiers People contenant les données d'enregistrement
Modèles d'application : non pris en charge	Questionnaires utilisés par les clients
Définitions d'application : non pris en charge	
Configurations utilisateur : créées sur la console de réinitialisation en libre-service des mots de passe	
Groupes d'applications : non pris en charge	
Données du service Single Sign-On : créées sur la console de réinitialisation en libre-service des mots de passe	

## Important

- La réinitialisation en libre-service des mots de passe ne prend pas en charge Active Directory en tant que magasin central, uniquement les partages réseau.
- La réinitialisation en libre-service des mots de passe prend uniquement en charge les données provenant de Single Sign-On 4.8 ou 5.0.

## Pour migrer les données depuis le magasin central Single Sign-On

Avant de procéder à la migration de vos données, familiarisez-vous avec l'installation et la configuration de la réinitialisation en libre-service des mots de passe. Pour de plus amples informations, consultez la section Installer et configurer.

1. Créez un nouveau magasin central.
2. Installez le service et la console de réinitialisation en libre-service des mots de passe.
3. Dans la console, spécifiez l'emplacement du nouveau magasin central.
4. Créez une nouvelle configuration utilisateur et incluez des utilisateurs disposant de la réinitialisation en libre-service des

mots de passe sur Single Sign-On.

5. Copiez les données d'enregistrement Single Sign-On et les questions de sécurité dans le nouveau magasin central.

**Remarque** : assurez-vous que le compte de proxy de données dispose de l'autorisation Contrôle total sur tous les fichiers copiés.

Vous n'avez besoin que de deux dossiers/fichiers.

### Exemples

Copiez toutes les données d'enregistrement de l'utilisateur :

```
\\SSO-SERVER\citrixsync$\People
```

à

```
\\SSPR-SVC\citrixsync$\People
```

Utilisez cette commande :

```
Robocopy \\SSO-SERVER\citrixsync$\People \\SSPR-SVC\citrixsync$\People /e /xd QBA  
/Log+:copylog.txt /tee
```

Copiez les questions de sécurité qui sont utilisées par les clients :

```
\\SSOSERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\  
QuestionBasedAuthentication2
```

à

```
\\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\  
QuestionBasedAuthentication2
```

Utilisez cette commande :

```
Robocopy \\SSO-SERVER\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2\  
\\SSPR-SVC\citrixsync$\CentralStoreRoot\AdminConsole\QuestionBasedAuthentication2 /e  
/Log+:copylog.txt /tee
```

Désormais, tous les utilisateurs peuvent déverrouiller et réinitialiser leurs questions et réponses d'enregistrement Single Sign-On.

# Configurer StoreFront pour autoriser les utilisateurs à enregistrer des réponses à des questions de sécurité

Dec 08, 2016

Configurez StoreFront pour permettre aux utilisateurs d'enregistrer leurs réponses aux questions de sécurité. Une fois qu'elles sont enregistrées, ils peuvent réinitialiser des mots de passe de domaine et déverrouiller des comptes de domaine. Pour plus d'informations, veuillez consulter la [documentation de StoreFront](#).

1. Configurez les services Internet (IIS) StoreFront sur HTTPS.
2. Créez un nouveau déploiement dans StoreFront.
3. Dans le panneau droit de la console de gestion StoreFront, sélectionnez **Gérer les méthodes d'authentification > Nom d'utilisateur et mot de passe**. Sélectionnez **Gérer les options de mot de passe** dans le menu déroulant.
4. Choisissez si vous voulez autoriser les utilisateurs à modifier les mots de passe et cliquez sur **OK**.
5. À partir du menu déroulant **Nom d'utilisateur et mot de passe**, choisissez **Configurer libre-service de compte**, sélectionnez **Citrix SSPR**, puis cliquez sur **Configurer**.
6. Spécifiez si les utilisateurs sont autorisés à réinitialiser leurs mots de passe et à déverrouiller leurs comptes avec la réinitialisation en libre-service des mots de passe, ajoutez l'URL du service de compte du service de mot de passe et cliquez sur **OK**.

**Remarque:** vous devez configurer le site de manière à utiliser l'expérience unifiée.

La prochaine fois que l'utilisateur ouvre une session sur Citrix Receiver ou Citrix Receiver pour Web, l'enregistrement de questions de sécurité est disponible. Après avoir cliqué sur **Démarrer**, les questions sont affichées et l'utilisateur doit fournir des réponses.

