

Shavlik Patch pour Microsoft System Center

Guide de l'utilisateur

Pour utilisation avec Microsoft System Center Configuration
Manager 2012



shavlik

Copyright

Copyright © 2014 Shavlik. Tous droits réservés. Ce produit est protégé par copyright et par les lois sur la propriété intellectuelle des États-Unis et d'autres pays, ainsi que par des clauses de traités internationaux.

Il est interdit de reproduire ou de retransmettre un élément quelconque de ce document, sous quelque forme et par quelque moyen que ce soit, électronique, mécanique ou autre, y compris par photocopie ou enregistrement, dans un but autre que l'utilisation personnelle du produit par la personne qui l'a acheté, sans l'autorisation écrite de Shavlik.

Marques

Shavlik est une marque de Shavlik aux États-Unis et/ou dans d'autres pays. Microsoft, Windows et System Center Configuration Manager sont des marques ou des marques déposées de Microsoft Corporation.

Tous les autres noms commerciaux, marques ou images utilisés dans ce document appartiennent à leur propriétaire respectif.

Informations sur le document et historique d'impression

Numéro de document : N/A

Date	Version	Description
Février 2014	Version initiale	Version initiale du Guide de l'utilisateur de Shavlik Patch pour Microsoft System Center .
Novembre 2014	Shavlik Patch 2.1	Ajout : infos de synchronisation pour les mises à jour tierces. Mise à jour de la configuration système requise. Ajout d'infos sur la vérification des configurations, les filtres composites, le volet des détails, la configuration proxy, l'historique de remplacement, les métadonnées, les langues et la fin de vie.

Table des matières

PREPARATION DE L'UTILISATION DE SHAVLIK PATCH	5
Bienvenue	5
Configuration système requise	5
Installation de l'extension Shavlik Patch pour Configuration Manager.....	6
Configuration des paramètres Shavlik Patch	7
Onglet Serveur WSUS.....	8
Informations sur le serveur WSUS	8
Informations sur le certificat de signature de code	9
Onglet Proxy	9
Onglet Compte.....	11
Onglet Langues.....	12
Onglet Vérifier la configuration	14
Onglet À propos	15
Onglet Planification	15
Ce que l'extension Shavlik Patch ajoute à Configuration Manager.....	16
Compréhension des informations de la grille	18
Afficher le XML	19
Utilisation de filtres.....	20
Filtres prédéfinis.....	20
Filtres personnalisés	21
Filtres composites.....	22
COMMENT PUBLIER DES MISES A JOUR	23
Publication manuelle de mises à jour tierces	23
Publication automatique de mises à jour à l'aide d'une tâche planifiée récurrente.....	25
Affichage et gestion des publications planifiées	28
COMMENT SYNCHRONISER LES MISES A JOUR POUR LES PRODUITS TIERS	29
EXPIRATION DES MISES A JOUR TIERCES.....	30

INFORMATIONS SUR LA PRISE EN CHARGE 31

- Produits pris en charge..... 31
- Support technique..... 31
- Notification de fin de vie 31

ANNEXE A : CREATION ET DISTRIBUTION DE CERTIFICATS 32

- Introduction 32
- Référence 32
- Configuration requise pour les certificats 33
- Création d'un certificat de signature de code 33
 - Création d'un certificat de signature de code avec une CA 33
 - Utilisation de Shavlik Patch et de WSUS pour créer un certificat de signature de code 33
- Importation d'un certificat..... 34
- Exportation d'un certificat 36
- Distribution du certificat 36
 - Utilisation d'une stratégie de groupe pour distribuer le certificat..... 37
 - Utilisation de MMC pour distribuer manuellement le certificat 37

PREPARATION DE L'UTILISATION DE SHAVLIK PATCH

Bienvenue

Bienvenue dans Shavlik Patch pour Microsoft System Center, extension qui enrichit les fonctions de Microsoft System Center Configuration Manager, en vous permettant de publier des mises à jour de produits tiers ou de produits traditionnels qui ne sont plus pris en charge par Configuration Manager. Shavlik Patch vous permet d'exploiter un seul workflow Configuration Manager pour publier les mises à jour des produits Microsoft et des produits non Microsoft.

Shavlik Patch comprend deux composants :

- **Catalogue de mises à jour** : Contient la logique de détection et de déploiement qui sert à appliquer des correctifs aux produits non Microsoft et aux anciennes versions des produits Microsoft. Ce catalogue regroupe un grand nombre de fichiers de mise à jour pour différents éditeurs de logiciels, comme Adobe, Apple, Firefox, Sun, etc.
- **Extension de la console Configuration Manager** : Permet de sélectionner des mises à jour dans le catalogue, de les publier sur vos serveurs WSUS, de synchroniser des mises à jour avec Configuration Manager et de faire expirer les mises à jour publiées. Vous pouvez ainsi appliquer des correctifs aux anciennes versions de vos produits Microsoft, ainsi qu'à vos produits non Microsoft, à l'aide du même workflow Configuration Manager que celui qui applique les correctifs aux produits Microsoft.

Configuration système requise

Voici la configuration requise pour l'installation et l'utilisation de Shavlik Patch :

- Shavlik Patch s'installe en tant qu'extension d'une console Configuration Manager 2012 existante (SP1 ou supérieur). La console Configuration Manager doit être installée sous l'un des systèmes d'exploitation Windows suivants :
 - Windows Server 2012 ou supérieur
 - Windows Server 2008 R2 SP1 ou supérieur
 - Windows 8 ou supérieur
 - Windows 7 SP1 ou supérieur
- .NET Framework 4.5.1 ou supérieur

Si ce logiciel requis est manquant, .NET Framework 4.5.1 est installé automatiquement lors de l'installation de Shavlik Patch.

- Configuration requise pour les clients Windows Server Update Services (WSUS) :
 - Si vous installez Shavlik Patch sur le serveur WSUS principal, et que vous utilisez Windows Server 2012 ou Windows 8, vous devez activer l'API WSUS et les cmdlets PowerShell.
 - Si WSUS est installé sur une machine Windows 8 ou Windows 8.1 distante, la fonction Outils d'administration à distance doit être installée sur cette machine. La version des outils d'administration à distance et celle de WSUS doivent correspondre. Sinon, vous ne pourrez pas déployer les mises à jour.

- Si le serveur WSUS principal exécute WSUS 3.0 SP2, vous devez installer la console d'administration WSUS 3.0 SP2 sur la même machine que Shavlik Patch. Les correctifs KB2720211 et KB2734608 doivent être appliqués au serveur WSUS et aux machines de console Configuration Manager.
- Le service Planificateur de tâches Microsoft doit être activé et l'utilisateur doit disposer des droits nécessaires pour créer des tâches planifiées.
- Compte Shavlik Protect Cloud
- L'utilisateur qui exécute Shavlik Patch doit disposer de droits **Ouvrir une session en tant que tâche** et être membre du groupe Administrateurs WSUS sur le serveur WSUS. De plus, en présence d'un serveur WSUS distant, l'utilisateur doit être membre du groupe local Administrateurs sur le serveur WSUS.
- Configuration requise pour la machine client :
Chacune des machines client doit respecter la configuration requise suivante pour qu'il soit possible de déployer des mises à jour de produits non Microsoft distribuées par un serveur WSUS :
 - La machine doit contenir une copie du certificat de signature de code dans les magasins de certificats appropriés.
 - Vous devez activer le paramètre de stratégie **Autoriser les mises à jour signées provenant d'un emplacement intranet du service de Mise à jour Microsoft**.

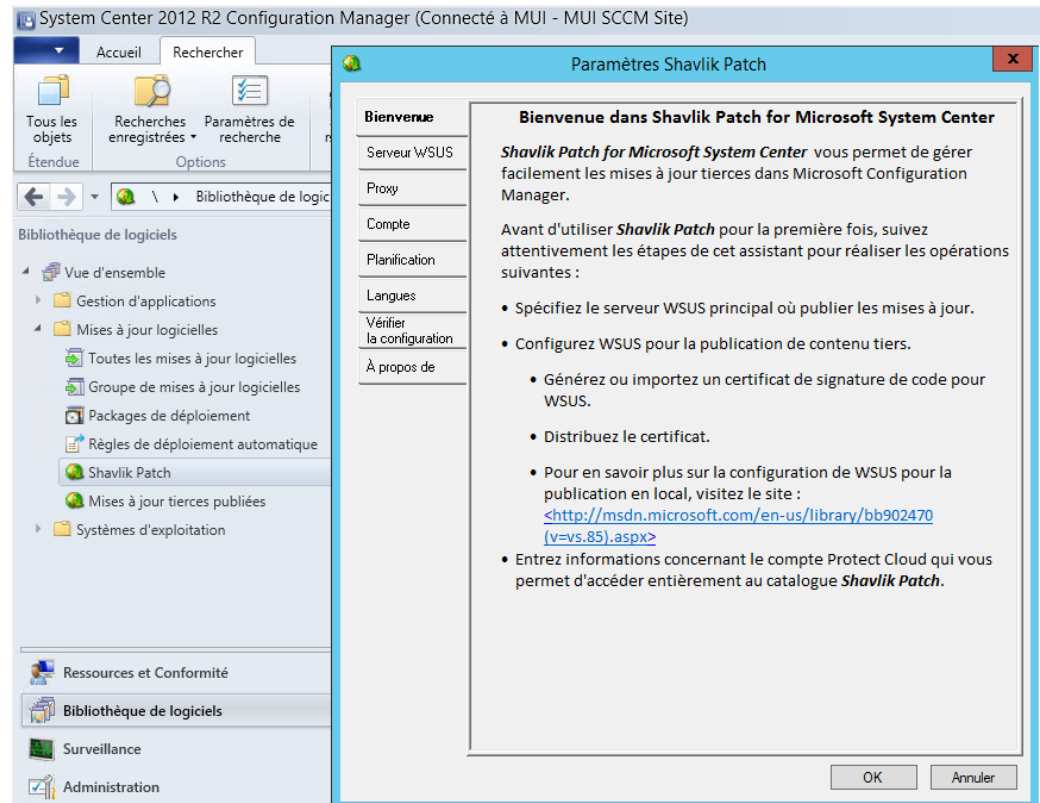
Installation de l'extension Shavlik Patch pour Configuration Manager

Remarque : Vous devez exécuter le programme en tant qu'administrateur pour installer l'extension.

1. Ouvrez votre navigateur Web et accédez à : www.shavlik.com/downloads/
2. Cliquez sur le lien **Shavlik Patch - Évaluation gratuite**.
3. Téléchargez le fichier de programme d'installation **Shavlik Patch pour Configuration Manager 2012**.
4. Fermez System Center Configuration Manager.
5. Lancez l'installation de Shavlik Patch en double-cliquant sur le fichier nommé **SCCMPatchSetup.exe**.
 - Si .NET Framework 4.5.1 ou supérieur n'est pas installé sur la machine Configuration Manager, le programme vous invite à installer .NET Framework 4.5.1 avant de poursuivre l'installation. Suivez les instructions à l'écran pour installer ce logiciel prérequis.
 - Si tous les éléments prérequis sont installés, le contrat de licence s'affiche. Vous devez accepter les termes du contrat de licence pour installer le programme.
6. Cochez la case appropriée pour accepter le contrat de licence, puis cliquez sur **Installer**.
Une fois les fichiers installés, la boîte de dialogue **Terminé** s'affiche.
7. Cliquez sur **Terminer**.

Configuration des paramètres Shavlik Patch

L'installation de l'extension Shavlik Patch ajoute deux nouvelles entrées de liste au dossier **Bibliothèque de logiciels > Mises à jour logicielles** ; ces nouvelles entrées de liste s'appellent **Shavlik Patch** et **Mises à jour tierces publiées**. La première fois que vous tentez d'accéder à l'un de ces deux nouveaux éléments de liste, l'assistant de configuration démarre.



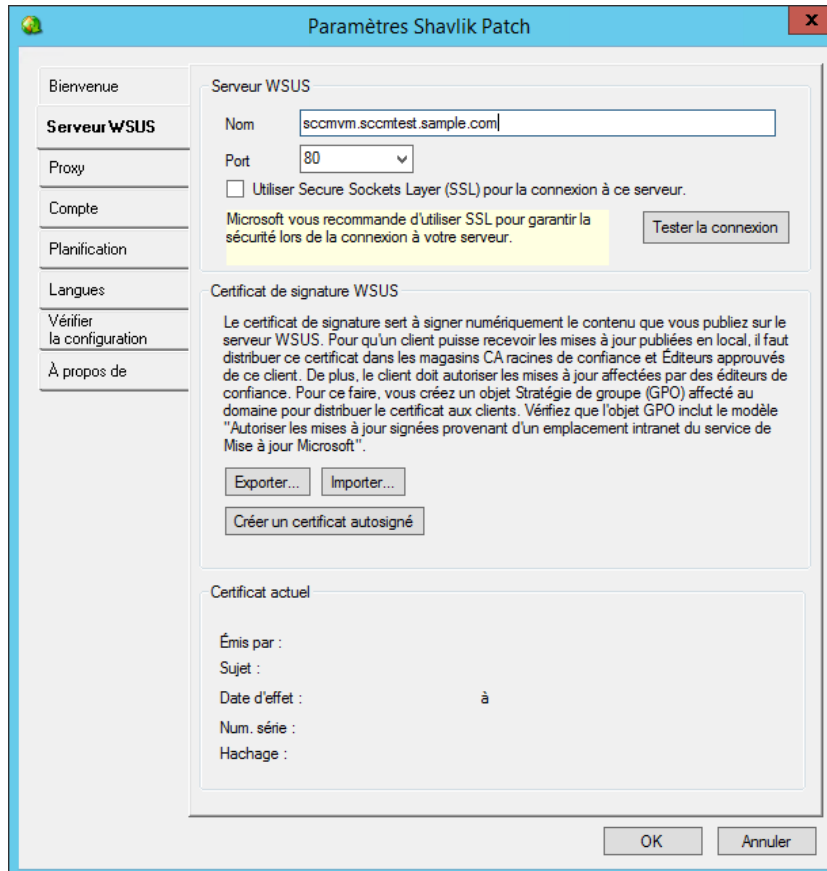
L'assistant vous guide pas à pas dans les différents onglets à remplir lors du processus de configuration. Shavlik Patch est prêt à l'emploi dès que vous avez terminé la configuration et enregistré vos paramètres. Vous pouvez revenir à tout moment à ces paramètres à l'aide du bouton **Paramètres** de l'onglet **Accueil**.

Après avoir pris connaissance des informations de l'onglet **Bienvenue**, cliquez sur **Suivant**.

Le premier onglet de configuration est intitulé **Serveur WSUS**.

Onglet Serveur WSUS

L'onglet **Serveur WSUS** sert à configurer la façon dont l'extension va communiquer avec votre serveur WSUS. Il permet aussi de définir le certificat à utiliser pour signer numériquement le contenu publié sur le serveur WSUS.



Informations sur le serveur WSUS

- **Nom** : Vérifiez le nom ou l'adresse IP de votre serveur WSUS. Normalement, ces informations sont automatiquement détectées et affichées.
- **Port** : Vérifiez le numéro de port utilisé pour établir la connexion avec le serveur WSUS. La valeur par défaut pour les connexions non sécurisées est 80 ou 8530. Les connexions sécurisées utilisent généralement le port 443 ou 8531.
- **Connexion sécurisée** : Si votre serveur WSUS a été configuré pour utiliser une connexion sécurisée, cochez cette case. La connexion sécurisée est obligatoire si vous devez importer un certificat de signature. Pour en savoir plus, reportez-vous à « *Importation d'un certificat* » dans l'annexe A.
- **Tester la connexion** : Pour vous assurer que vous parvenez à accéder au serveur WSUS, cliquez sur **Tester la connexion**.

Informations sur le certificat de signature de code

Le certificat de signature de code est obligatoire pour la publication de mises à jour sur le serveur WSUS. Si vous disposez déjà d'un certificat de signature, il apparaît dans la zone **Certificat actuel**.

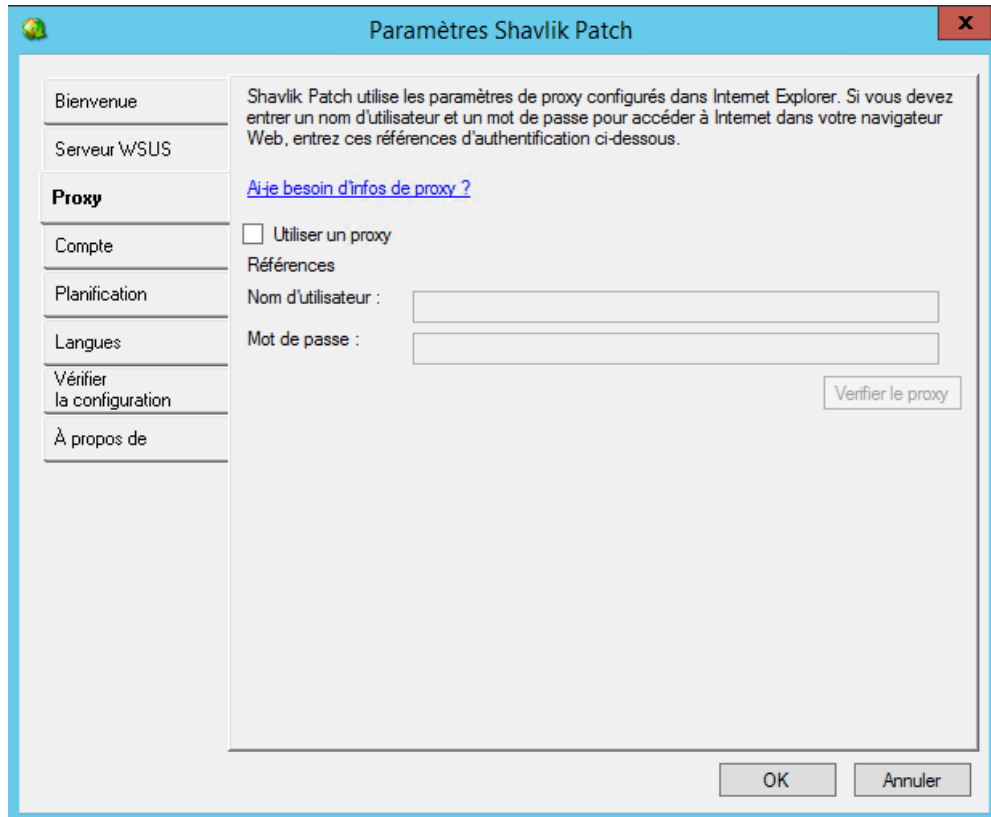
Vous pouvez réaliser les opérations suivantes sur le certificat :

- **Exporter** : Exporte le certificat actuel depuis Shavlik Patch. Pour des raisons de sécurité, le certificat est exporté sans la clé privée. Une fois le certificat exporté, vous le distribuez à vos postes client et à vos machines d'infrastructure (comme les autres machines exécutant l'extension Shavlik Patch, les serveurs WSUS en aval sur le réseau et les clients Windows Update). Cette opération est indispensable pour que les machines reçoivent les mises à jour publiées en local.
- **Importer** : Permet d'importer un certificat de signature de code créé par une autorité de certification (CA). Une connexion sécurisée est requise pour l'importation d'un certificat.
- **Créer un certificat autosigné** : Crée un certificat de signature de code pour votre entreprise. Ce processus utilise les services de WSUS pour créer le certificat.

Pour en savoir plus sur l'exportation, l'importation ou la création de certificats, reportez-vous à « *Annexe A : Création et utilisation de certificats* ».

Onglet Proxy

L'onglet **Proxy** vous permet de modifier les paramètres de proxy que Shavlik Patch utilise lorsqu'il accède à Internet à l'aide de votre navigateur Web. En général, Shavlik Patch vérifie les paramètres de proxy dans Internet Explorer, et effectue un test de connexion à Internet pour déterminer s'il faut ou non utiliser des paramètres de serveur proxy. Si Shavlik Patch ne peut pas accéder à Internet avec ces paramètres, ou si vous devez entrer un nom d'utilisateur et un mot de passe chaque fois que vous lancez votre navigateur pour accéder à Internet, vous devez configurer les options de proxy.



- **Ai-je besoin d'infos de proxy ?** : Pour savoir si Shavlik Patch peut utiliser vos paramètres de proxy Internet Explorer actuels pour accéder à Internet et réaliser des opérations, cliquez sur ce bouton. Si le test indique un succès, aucune autre opération n'est nécessaire. Si le test indique un échec, cela signifie généralement que votre entreprise utilise l'authentification et que vous avez besoin de modifier vos paramètres de proxy en définissant des références d'authentification (nom d'utilisateur et mot de passe).
- **Utiliser un proxy** : Si vous activez cette option, cela indique que vous allez fournir des références d'authentification de proxy. Si vous désélectionnez cette case à cocher après avoir spécifié des références d'authentification, ces références sont enregistrées mais pas utilisées.
- **Nom d'utilisateur** : Entrez le nom d'utilisateur qui fait partie des références d'authentification. Vous devez peut-être spécifier un domaine dans votre nom d'utilisateur (par exemple : mon-domaine\mon.nom).
- **Mot de passe** : Entrez le mot de passe qui fait partie des références d'authentification.
- **Test** : Cliquez sur ce bouton pour tester les références d'authentification.

Onglet Compte

Vous devez être connecté au service Shavlik Protect Cloud pour que l'extension accède automatiquement à l'ensemble du catalogue Shavlik Patch et télécharge des éléments. L'extension utilise votre compte Protect Cloud pour rechercher périodiquement un nouveau catalogue. Si vous n'avez pas de compte Protect Cloud, vous recevez uniquement les versions d'évaluation, à savoir quelques mises à jour échantillon.

Remarque : Pour en savoir plus sur Shavlik Protect Cloud, visitez le site : <https://protectcloud.shavlik.com>.

- **Nom d'utilisateur :** Entrez le nom d'utilisateur servant à l'authentification de votre compte Protect Cloud.
- **Mot de passe :** Entrez le mot de passe servant à l'authentification de votre compte Protect Cloud.
- **S'inscrire maintenant :** Si vous n'avez pas de compte Protect Cloud, cliquez sur ce bouton et suivez les instructions à l'écran pour vous inscrire comme utilisateur. Vous devez être un utilisateur inscrit pour accéder à l'ensemble du catalogue Shavlik Patch.
- **Vérifier :** Pour vous assurer que vous parvenez à vous connecter à votre compte Protect Cloud à l'aide des références d'authentification entrées, cliquez sur **Vérifier**. Si vous ne pouvez pas vous connecter à votre compte, vous ne pourrez pas accéder au catalogue Shavlik Patch en entier.

- **Me demander quand des révisions des métadonnées sont disponibles** : Si de nouvelles métadonnées deviennent disponibles pour les mises à jour que vous avez déjà publiées, une boîte de dialogue vous permet de choisir de réviser immédiatement les mises à jour dans WSUS ou d'ignorer les nouvelles métadonnées.

Shavlik Patch recherche les révisions des métadonnées à chaque téléchargement d'une nouvelle copie du catalogue. Dans la plupart des cas, il est recommandé de publier les révisions.

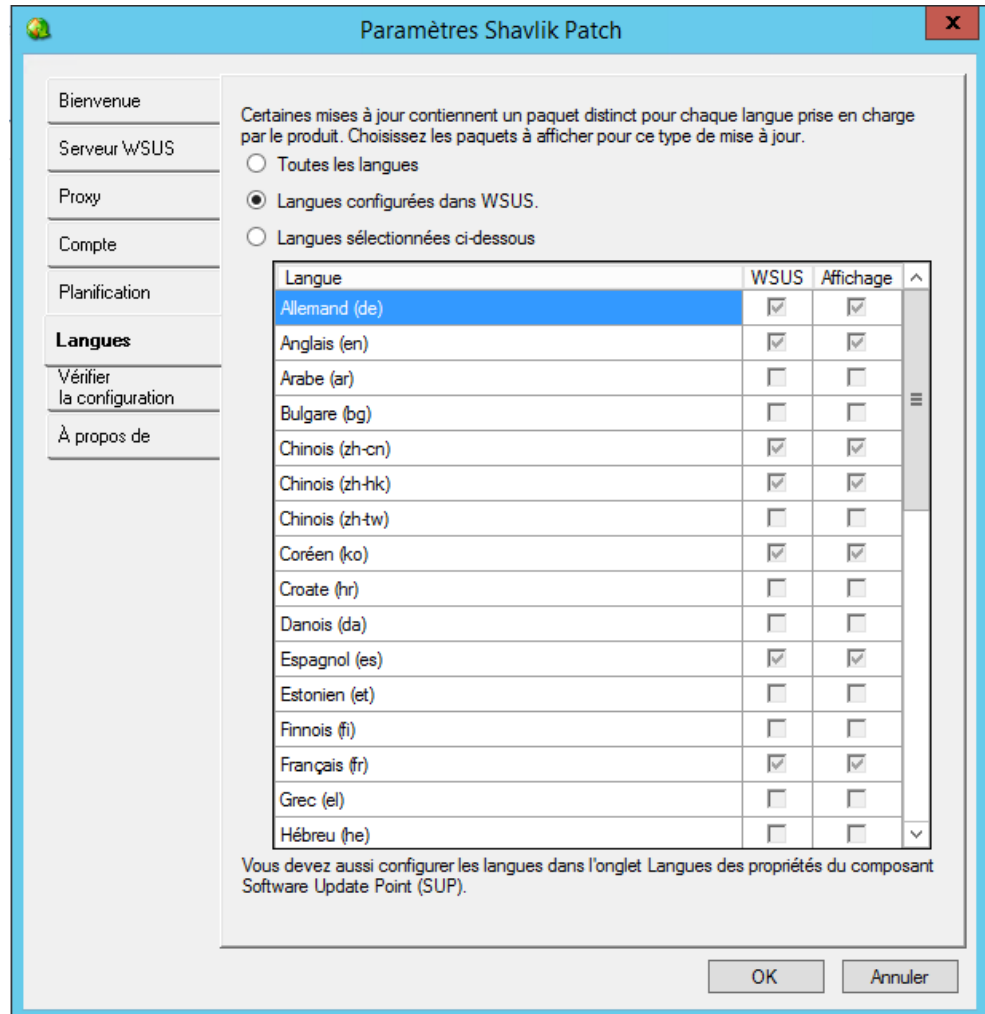
Si vous cochez la case **Mémoriser mon choix et ne plus me demander**, puis que vous cliquez sur **Oui**, l'option de métadonnées dans l'onglet **Compte** devient **Mettre à jour les métadonnées WSUS sans me demander**.

Si vous cochez la case **Mémoriser mon choix et ne plus me demander**, puis que vous cliquez sur **Non**, l'option de métadonnées dans l'onglet **Compte** devient **Ne pas me demander et ne pas mettre à jour WSUS**.

- **Mettre à jour les métadonnées WSUS sans me demander** : Met automatiquement à jour les mises à jour que vous avez déjà publiées avec les métadonnées révisées, sans vous avertir.
- **Ne pas me demander et ne pas mettre à jour WSUS** : Aucune opération n'est effectuée lorsque des métadonnées révisées sont disponibles. Vous pouvez utiliser le filtre ***Métadonnées révisées** pour déterminer si des révisions des métadonnées sont disponibles.

Onglet Langues

Souvent, une même mise à jour s'applique à toutes les langues d'un produit. Cependant, certaines mises à jour sont fournies sous forme d'un paquet différent pour chaque langue prise en charge par le produit. L'onglet **Langues** vous permet de choisir les langues qui vous intéressent pour ces mises à jour propres à la langue. Les langues que vous choisissez déterminent les langues affichées dans la grille Shavlik Patch.

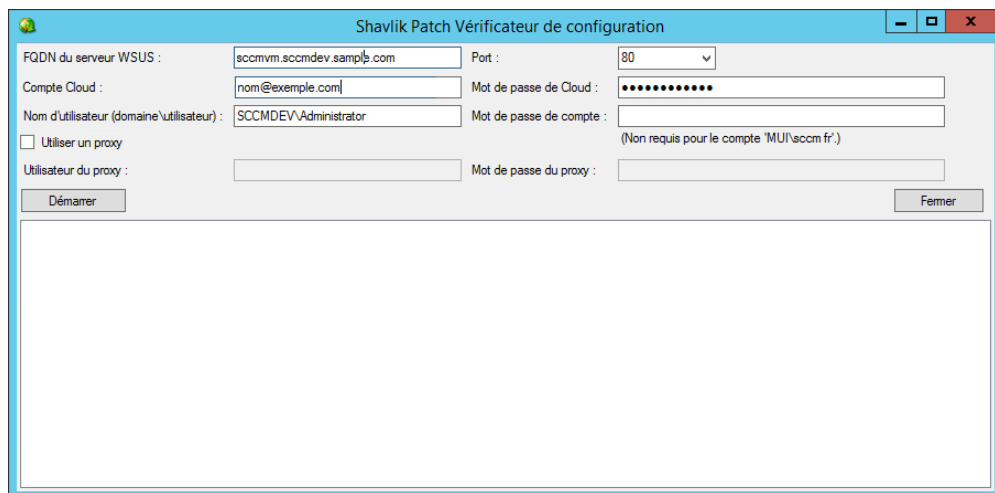


- **Toutes les langues** : Shavlik Patch affiche les paquets disponibles pour toutes les langues, pour chaque mise à jour.
- **Langues configurées dans WSUS** : Shavlik Patch affiche uniquement les paquets correspondant aux langues configurées pour téléchargement sur le serveur WSUS. Cette option est activée par défaut. (Pour vérifier ou changer les paramètres de langue WSUS, démarrez Update Services sur le serveur WSUS, cliquez sur **Options**, puis accédez à **Fichiers et langues des mises à jour**, et cliquez sur l'onglet **Langues des mises à jour**.)
- **Langues sélectionnées ci-dessous** : Shavlik Patch affiche uniquement les paquets correspondant aux langues sélectionnées dans la table. Vous devez sélectionner au moins une langue.
 - **Colonne WSUS** : Indique si la langue est actuellement configurée sur votre serveur WSUS. Vous ne pouvez modifier aucune des cases à cocher de cette colonne.
 - **Colonne Affichage** : Cochez la case de chaque langue à afficher dans la grille **Shavlik Patch**. Vous pouvez sélectionner une langue même si elle n'est pas configurée dans WSUS.

Onglet Vérifier la configuration

Cet onglet permet de démarrer l'outil Vérificateur de configuration. Cet utilitaire est généralement exécuté une seule fois après l'installation initiale de Shavlik Patch.

Vérificateur de configuration permet de déterminer si votre système répond à la configuration requise pour l'utilisation de Shavlik Patch. Vous exécutez Vérificateur de configuration en cliquant sur le bouton **Lancer le vérificateur de configuration** dans l'onglet **Vérifier la configuration**. Vous pouvez aussi l'exécuter via la ligne de commande : C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ST.SCCM.ConfigurationChecker.exe. Vous devez exécuter Vérificateur de configuration avec des privilèges Administrateur complet, mais il peut servir à évaluer des comptes qui ne disposent pas de ces privilèges d'administrateur.



La plupart des informations de cette boîte de dialogue sont saisies automatiquement, mais vous pouvez les modifier si nécessaire.

- **FQDN du serveur WSUS** : Entrez le nom de domaine entièrement qualifié (FQDN) de votre serveur WSUS.
- **Port** : Sélectionnez le port servant à accéder au serveur WSUS.
- **Compte Cloud** : Entrez votre nom d'utilisateur Protect Cloud.
- **Mot de passe de Cloud** : Entrez votre mot de passe Protect Cloud.
- **Compte d'utilisateur (domaine/utilisateur)** : Entrez le nom de domaine et le nom d'utilisateur du compte à évaluer.
- **Mot de passe de compte** : Entrez le mot de passe associé au compte d'utilisateur. Vous pouvez laisser ce champ vide si vous évaluez le compte que vous avez utilisé pour exécuter cet outil.
- **Utiliser un proxy** : Si vous activez cette option, des références d'authentification de serveur proxy sont nécessaires pour exécuter le test Vérificateur de configuration. Si vous désélectionnez cette case à cocher après avoir spécifié des références d'authentification, ces références sont

enregistrées mais pas utilisées. Initialement, cette zone reflète les éléments configurés dans l'onglet **Proxy**, mais vous pouvez remplacer temporairement ces valeurs dans cet écran.

- **Nom d'utilisateur du proxy** : Entrez le nom d'utilisateur d'un compte sur le serveur proxy. Ce champ est automatiquement rempli avec le nom d'utilisateur indiqué dans l'onglet **Proxy**, mais vous pouvez remplacer cette valeur. Vous devez peut-être spécifier un domaine dans votre nom d'utilisateur (par exemple : mon-domaine\mon.nom).
- **Mot de passe du proxy** : Entrez le mot de passe associé au compte de serveur proxy.

L'utilitaire vérifie les éléments suivants :

- Capacité à se connecter au serveur WSUS à l'aide d'un nom de domaine entièrement qualifié (FQDN) et d'un numéro de port
- Capacité à se connecter à Protect Cloud à l'aide d'un nom d'utilisateur et d'un mot de passe
- Capacité à récupérer le catalogue Shavlik Patch
- Attribution de privilèges **Ouvrir une session en tant que tâche** à l'utilisateur
- Appartenance du compte d'utilisateur au groupe **Administrateurs** et au groupe **Administrateurs WSUS** sur le serveur WSUS
- Présence du certificat de signature WSUS dans les magasins CA racines de confiance et Éditeurs approuvés, et validité de ce certificat (non expiré)

Si l'un de ces tests échoue, vous devrez corriger le problème avant d'utiliser Shavlik Patch.

Onglet À propos

L'onglet **À propos** affiche des informations sur le produit et la version du catalogue, et fournit une notification si la version utilisée approche de sa fin de vie. C'est le dernier onglet affiché par l'assistant de configuration. Pour enregistrer les paramètres et quitter l'assistant, cliquez sur **Terminer**.

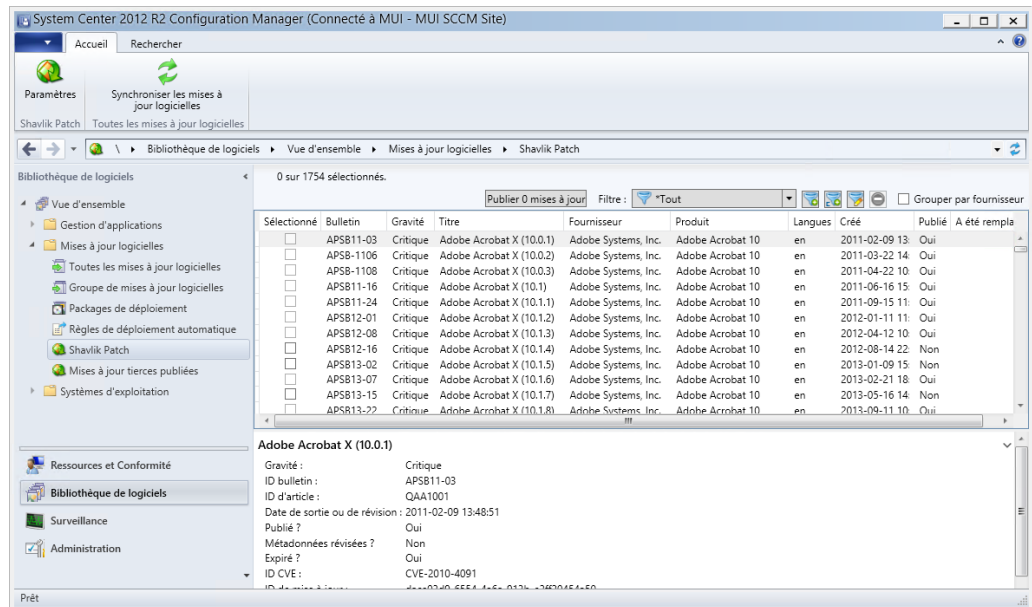
Onglet Planification

L'onglet **Planification** est disponible uniquement si vous avez suivi toutes les étapes de l'assistant de configuration et enregistré vos paramètres. Cet onglet sert à publier les mises à jour à l'aide d'une tâche planifiée récurrente. Pour en savoir plus sur cet onglet, reportez-vous à la section « *Automatically Publishing Updates Using a Recurring Scheduled Task* ».

Ce que l'extension Shavlik Patch ajoute à Configuration Manager

L'installation de l'extension Shavlik Patch ajoute deux nouvelles listes au dossier **Bibliothèque de logiciels > Mises à jour logicielles**. Elle ajoute également le bouton de barre d'outils **Paramètres** à l'onglet **Accueil** de Configuration Manager si l'une de ces deux nouvelles listes est sélectionnée.

- **Shavlik Patch** : Contient toutes les mises à jour disponibles dans le catalogue Shavlik Patch. Vous utilisez cette liste pour repérer et publier les mises à jour. Vous pouvez utiliser des filtres pour limiter les mises à jour affichées ; reportez-vous à « *Using the Filters* » pour en savoir plus.



- **Mises à jour tierces publiées** : Contient toutes les mises à jour de produits tiers publiées dans WSUS. Ces mises à jour peuvent avoir été publiées avec Shavlik Patch ou avec un autre mécanisme. Vous utilisez cette liste pour passer en revue et gérer les mises à jour. L'utilisation la plus courante consiste à faire expirer les mises à jour.

System Center 2012 R2 Configuration Manager (Connecté à MUI - MUI SCCM Site)

Accueil Rechercher

Paramètres Synchroniser les mises à jour logicielles

Mises à jour tierces publiées Toutes les mises à jour logicielles

Bibliothèque de logiciels \> Mises à jour logicielles \> Mises à jour tierces publiées

Bibliothèque de logiciels 1 sur 52 sélectionnés

Faire expirer les mises à jour sélectionnées Filtre : *Tout

Sélectionné	Bulletin	Gravité	Titre	Fournisseur	Produit	Langues	Article KB	Expiré
<input type="checkbox"/>	7ZIP-001	Faible	7-Zip 9.20	7-Zip	7-Zip	en	Q7Z1P920	Oui
<input type="checkbox"/>	7ZIP-001	Faible	7-Zip 9.20 x64	7-Zip	7-Zip	en	Q7Z1P920	Oui
<input type="checkbox"/>	AA80-004	Critique	Adobe Acrobat 8.1.3	Adobe Systems	Adobe Acrobat 8		QAA0813	Oui
<input checked="" type="checkbox"/>	APSB-0906	Critique	Adobe Acrobat 8.1.5	Adobe Systems	Adobe Acrobat 8		QAA0815	Non
<input type="checkbox"/>	APSB11-03	Critique	Adobe Acrobat 8.2.6	Adobe Systems	Adobe Acrobat 8		QAA0826	Non
<input type="checkbox"/>	APSB11-03	Critique	Adobe Acrobat X (10.0.1)	Adobe Systems	Adobe Acrobat 10	en	QAA1001	Oui
<input type="checkbox"/>	APSB-1106	Critique	Adobe Acrobat X (10.0.2)	Adobe Systems	Adobe Acrobat 10		QAA1002	Oui
<input type="checkbox"/>	APSB-1108	Critique	Adobe Acrobat X (10.0.3)	Adobe Systems	Adobe Acrobat 10		QAA1003	Oui
<input type="checkbox"/>	APSB11-16	Critique	Adobe Acrobat X (10.1)	Adobe Systems	Adobe Acrobat 10		QAA1010	Oui
<input type="checkbox"/>	APSB11-24	Critique	Adobe Acrobat X (10.1.1)	Adobe Systems	Adobe Acrobat 10		QAA1011	Oui
<input type="checkbox"/>	APSB14-15	Critique	Adobe Acrobat X (10.1.10)	Adobe Systems	Adobe Acrobat 10		QAA10110	Non
<input type="checkbox"/>	APSB14-19	Critique	Adobe Acrobat X (10.1.11)	Adobe Systems	Adobe Acrobat 10		QAA10111	Non
<input type="checkbox"/>	APSB14-20	Critique	Adobe Acrobat X (10.1.12)	Adobe Systems	Adobe Acrobat 10		QAA10112	Non
<input type="checkbox"/>	APSB12-01	Critique	Adobe Acrobat X (10.1.2)	Adobe Systems	Adobe Acrobat 10		QAA1012	Non

Adobe Acrobat 8.1.5

Gravité : Critique
 ID bulletin : APSB-0906
 ID d'article : QAA0815
 Date de sortie ou de révision : 2010-10-08 16:00:00
 Date de publication : 2014-10-11 03:04:02
 Expiré ? Non
 ID de mise à jour : d408a70a-a139-4743-870a-333089adfd07

Prêt

- **Paramètres** : Ce bouton de barre d'outils est disponible dans l'onglet **Accueil** lorsque l'utilisateur sélectionne **Shavlik Patch** ou **Mises à jour tierces publiées**. Cliquez sur ce bouton pour modifier les paramètres Shavlik Patch ou planifier une tâche de publication récurrente.

System Center 2012 R2 Configuration Manager (Connecté à MUI - MUI SCCM Site)

Accueil Rechercher

Paramètres Synchroniser les mises à jour logicielles

Shavlik Patch Toutes les mises à jour logicielles

Bibliothèque de logiciels \> Mises à jour logicielles \> Mises à jour tierces publiées

Bibliothèque de logiciels

Vue d'ensemble

Gestion d'applications

Mises à jour logicielles

Toutes les mises à jour logicielles

Groupe de mises à jour logicielles

Package de déploiement

Règles de déploiement automatique

Shavlik Patch

Mises à jour tierces publiées

Systèmes d'exploitation

Ressources et Conformité

Bibliothèque de logiciels

Surveillance

Administration

Paramètres Shavlik Patch

Bienvenue

Serveur WSUS

Nom : sccmvm.sccmtest.sample.com

Port : 80

Utiliser Secure Sockets Layer (SSL) pour la connexion à ce serveur.

Microsoft vous recommande d'utiliser SSL pour garantir la sécurité lors de la connexion à votre serveur.

Certificat de signature WSUS

Le certificat de signature sert à signer numériquement le contenu que vous publiez sur le serveur WSUS. Pour qu'un client puisse recevoir les mises à jour publiées en local, il faut distribuer ce certificat dans les magasins CA racines de confiance et Éditeurs approuvés de ce client. De plus, le client doit autoriser les mises à jour affectées par des éditeurs de confiance. Pour ce faire, vous créez un objet Stratégie de groupe (GPO) affecté au domaine pour distribuer le certificat aux clients. Vérifiez que l'objet GPO inclut le modèle "Autoriser les mises à jour signées provenant d'un emplacement intranet du service de Mise à jour Microsoft".

Certificat actuel

Émis par : CN=testWSUSSignCert2048
 Sujet : CN=testMUIWSUSRootCA
 Date d'effet : 02/09/2014 18:17:04 à 01/09/2017 02:00:00
 Num. série : 8052395542609D8044E6B75BA588151A
 Hachage : 6787886DD2AA40B839B28DB1BE9F4CE2908DE33D

Astuce : Vous accédez également à cette boîte de dialogue en cliquant avec le bouton droit sur l'entrée de liste **Shavlik Patch**.

Compréhension des informations de la grille

Les grilles **Shavlik Patch** et **Mises à jour tierces publiées** contiennent chacune deux volets. Chaque volet contient des informations différentes et a une fonctionnalité spécifique.

- Le volet supérieur affiche toutes les mises à jour correspondant à l'entrée de liste sélectionnée. Ce volet contient un grand nombre de colonnes, qui fournissent des informations très détaillées sur chaque mise à jour. Vous pouvez également sélectionner les mises à jour auxquelles appliquer une action donnée.
- Le volet inférieur affiche des informations détaillées sur la mise à jour sélectionnée dans le volet supérieur. Ce volet n'est pas disponible si vous sélectionnez plusieurs mises à jour dans le volet supérieur.

Vous disposez de plusieurs méthodes pour personnaliser le mode d'affichage des informations dans une grille. Vous pouvez réaliser les opérations suivantes :

- Application de filtres pour rechercher des mises à jour spécifiques.
- Réorganisation des colonnes en cliquant sur l'en-tête de la colonne voulue et en le faisant glisser vers une nouvelle position.
- Clic sur un en-tête de colonne pour trier la colonne dans l'ordre croissant ou décroissant.
- Clic avec le bouton droit sur un en-tête de colonne pour redimensionner les colonnes et choisir les lignes à afficher dans la grille. Choix des colonnes à afficher dans la grille.

La grille **Shavlik Patch** contient un certain nombre de colonnes uniques qui vous aident à identifier l'état de chaque mise à jour.

- **Publié** : Indique si la mise à jour a été publiée dans WSUS.
- **Révision publiée** : Ce numéro s'incrémente chaque fois que vous publiez une révision d'une mise à jour donnée. Toutes les mises à jour publiées portent un numéro supérieur à zéro.
- **Révisé** : Indique si la mise à jour est une révision d'une mise à jour publiée précédemment. Si tel est le cas, la case de la colonne **Sélectionné** est cochée. La publication de ce type de mise à jour crée une nouvelle révision et incrémente le numéro dans la colonne **Révision publiée**.

Les mises à jour de type Révision altèrent uniquement les métadonnées, pas le paquet de mise à jour. Une révision est insérée dans le catalogue Shavlik Patch chaque fois qu'il est nécessaire de mettre à jour l'un des éléments suivants :

- Logique de détection qui détermine si un correctif s'applique à un système donné et s'il est déjà installé
- Texte relatif à la mise à jour
- **Langues** : Identifie les différentes versions traduites disponibles pour chaque mise à jour. Vous pouvez limiter les langues affichées, à l'aide de l'onglet **Langues** de la boîte de dialogue **Paramètres Shavlik Patch**. Si la colonne **Langues** contient une entrée vide, cela signifie que la mise à jour s'applique à toutes les langues prises en charge par le produit.

- **A été remplacé** : Indique si la mise à jour a été remplacée par une autre. Si la mise à jour a été remplacée, elle n'est pas la plus récente disponible. Pour consulter la chaîne de remplacement d'une mise à jour, sélectionnez cette mise à jour ; les informations s'affichent dans le volet inférieur. Le filtre par défaut, ***Non publié le plus récent**, masque toutes les mises à jour remplacées qui n'ont pas été publiées. Pour afficher toutes les mises à jour, y compris celles qui ont été remplacées, sélectionnez le filtre ***Tout**.

Afficher le XML

Vous pouvez cliquer avec le bouton droit sur une mise à jour dans la grille pour afficher le fichier XML qui la définit. Vous pouvez afficher le fichier XML tel qu'il apparaît dans le catalogue Shavlik Patch ou tel qu'il apparaît après publication dans WSUS (pour les mises à jour publiées). Cet outil est prévu pour le débogage ; vous n'aurez pas besoin de l'utiliser au quotidien.

Utilisation de filtres

Vous pouvez filtrer le contenu des listes **Shavlik Patch** et **Mises à jour tierces publiées** afin de rechercher des mises à jour particulières. Vous pouvez aussi utiliser un filtre pour planifier une tâche récurrente.

Filtres prédéfinis

Les filtres prédéfinis sont identifiés par un astérisque au début de leur nom. Vous ne pouvez ni modifier, ni supprimer les filtres prédéfinis. Les filtres prédéfinis sont les suivants :

Liste Shavlik Patch

- ***Tout** : Toutes les mises à jour sont affichées.
- ***Non publié le plus récent** : Affiche uniquement les mises à jour non remplacées qui n'ont pas été publiées dans WSUS. Il s'agit du filtre par défaut.
- ***Non publié** : Affiche uniquement les mises à jour qui n'ont pas été publiées dans WSUS.
- ***Publié** : Affiche uniquement les mises à jour qui ont été publiées dans WSUS.
- ***Métadonnées révisées** : Affiche uniquement les mises à jour qui ont été publiées dans WSUS et pour lesquelles le catalogue actuel contient des métadonnées révisées. Republiez ces mises à jour pour mettre à jour les métadonnées dans WSUS.
- ***Sélectionné** : Affiche uniquement les mises à jour sélectionnées dans la grille. Vous pouvez utiliser ce filtre pour vérifier vos sélections avant de publier les mises à jour dans WSUS.

Remarque : Pour les mises à jour qui comportent un paquet différent pour chaque langue, il existe un filtre par langue implicite dans la grille Shavlik Patch. Les seules mises à jour affichées sont celles qui s'appliquent à toutes les langues (où la colonne **Langues** est vide) et dont les options **Langues** incluent au moins une des langues sélectionnées dans la boîte de dialogue **Paramètres**.

Liste Mises à jour tierces publiées

- ***Tout** : Toutes les mises à jour sont affichées.
- ***Sélectionné** : Affiche uniquement les mises à jour sélectionnées dans la grille.

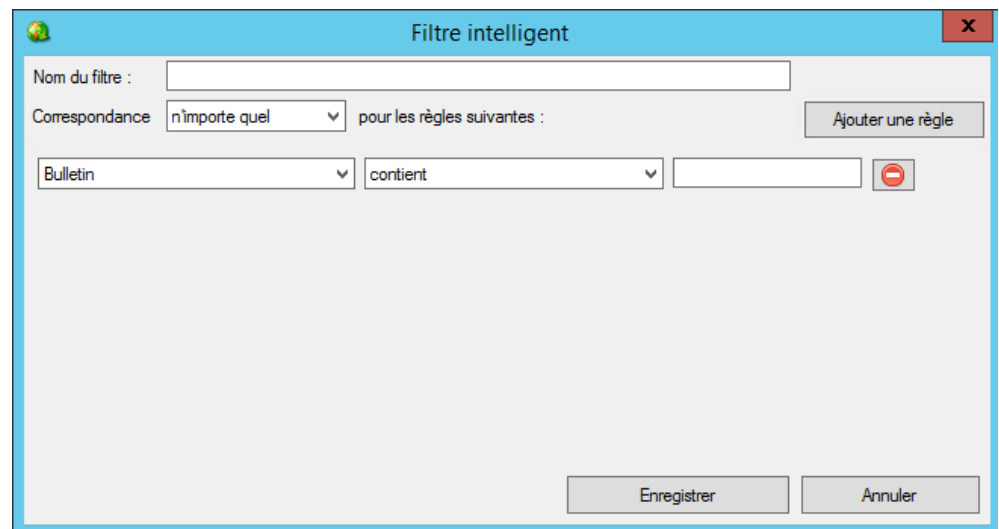
Filtres personnalisés

Vous pouvez créer vos propres filtres personnalisés. L'outil SmartFilter (Filtre intelligent) vous permet de spécifier très précisément les mises à jour à afficher. Chaque filtre personnalisé comprend une ou plusieurs règles. Vous pouvez ajouter à un filtre autant de règles que vous le souhaitez.

Pour créer un nouveau filtre :

1. Cliquez sur l'icône Nouveau filtre ()

La boîte de dialogue **Filtre intelligent** s'affiche.



La boîte de dialogue "Filtre intelligent" est affichée. Elle contient les éléments suivants :

- Titre de la fenêtre : Filtre intelligent
- Champ "Nom du filtre" : vide
- Menu déroulant "Correspondance" : n'importe quel
- Texte "pour les règles suivantes :"
- Bouton "Ajouter une règle"
- Menu déroulant "Bulletin" (dans une zone logique)
- Menu déroulant "contient" (dans une zone logique)
- Champ de texte vide (pour les critères)
- Bouton "Enregistrer"
- Bouton "Annuler"

2. Entrez un nom pour le filtre.
3. Spécifiez les règles du filtre qui doivent trouver une correspondance.
 - **Tout** : Seules les mises à jour qui correspondent à toutes les règles du filtre sont affichées.
 - **N'importe quel** : Les mises à jour qui correspondent à au moins une règle du filtre s'affichent.
4. Définissez une ou plusieurs règles.

Pour définir une règle, sélectionnez une option dans chacune des deux zones logiques, puis entrez des critères dans la troisième zone. Pour ajouter une autre règle, cliquez simplement sur **Ajouter une règle**.

Remarque : Si vous définissez une règle qui n'a pas de sens (par exemple, « Bulletin Inférieur à 3 »), cette règle est ignorée.

5. Cliquez sur **Enregistrer**.

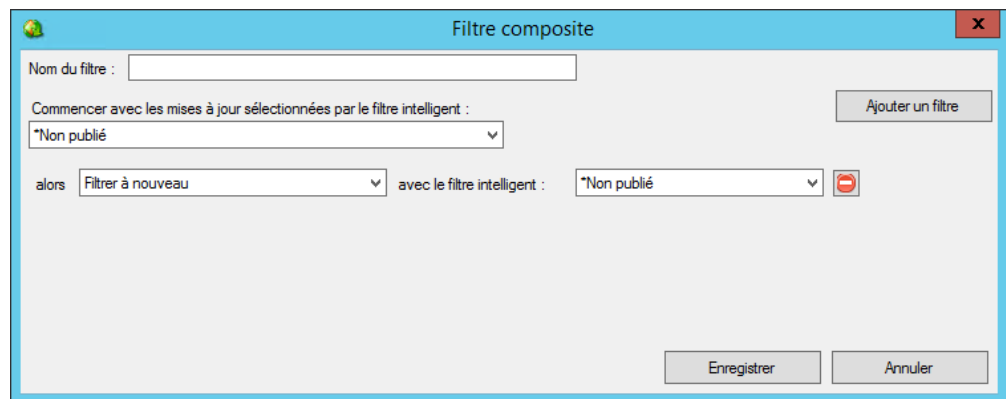
Filtres composites

Shavlik Patch permet de définir des filtres composites. Un filtre composite est constitué de plusieurs filtres liés, qui sont exécutés en série. Cette fonction de filtrage avancé vous permet de cibler ou d'étendre votre recherche dans une règle, de façon répétitive, en exécutant automatiquement plusieurs filtres l'un après l'autre. Vous pouvez ainsi effectuer des recherches qui impliquent à la fois la logique **ou** et la logique **et**.

Pour créer un nouveau filtre composite :

1. Cliquez sur l'icône Nouveau filtre composite (.

La boîte de dialogue **Filtre composite** s'affiche.



2. Entrez un nom pour le filtre composite.
3. Choisissez un filtre de départ.
4. Ajoutez un ou plusieurs niveaux de filtrage.

Pour définir un niveau, choisissez une action (**Ajouter**, **Supprimer** ou **Filtrer à nouveau**), puis cliquez sur le filtre supplémentaire à appliquer. Pour ajouter un autre niveau, cliquez sur **Ajouter un filtre**.

5. Cliquez sur **Enregistrer**.

COMMENT PUBLIER DES MISES A JOUR

Publication manuelle de mises à jour tierces

Vous pouvez publier manuellement une ou plusieurs mises à jour tierces. Les mises à jour sont soit publiées immédiatement, soit planifiées pour publication à une date ultérieure. Vous utilisez le Planificateur de tâches Microsoft pour planifier la publication. La publication est toujours exécutée sous la forme d'une tâche séparée, mais vous pouvez la surveiller pendant son exécution.

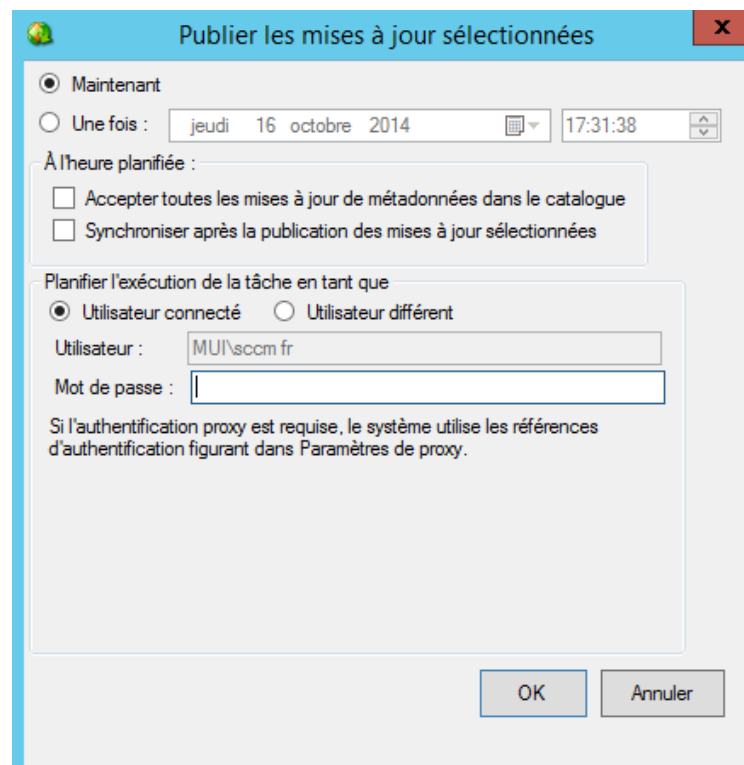
1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Shavlik Patch**.
2. Cochez la case **Sélectionné** de chaque mise à jour à publier.

La case à cocher **Sélectionné** est désactivée si la dernière révision de la mise à jour a déjà été publiée ou si elle a été planifiée pour publication.

Pour trouver les mises à jour voulues, vous pouvez :

- Utiliser un filtre
 - Utiliser la case à cocher **Grouper par fournisseur**
 - Trier les données en cliquant sur les en-têtes de colonne
3. Cliquez sur **Publier X mises à jour** (où X = nombre de mises à jour sélectionnées).

La boîte de dialogue **Publier les mises à jour sélectionnées** s'affiche.



4. Spécifiez la date et le mode de publication des mises à jour.

- **Maintenant** : Le processus de publication démarre dès que vous cliquez sur **OK**.
- **Une fois** : Planifiez le processus de publication afin qu'il s'exécute à une date ultérieure.
- **Accepter toutes les mises à jour de métadonnées dans le catalogue** : Pour mettre à jour WSUS automatiquement avec toutes les révisions de métadonnées disponibles pour les mises à jour déjà publiées, cochez cette case.
- **Synchroniser après la publication des mises à jour sélectionnées** : Pour que Configuration Manager se synchronise automatiquement avec votre base de données WSUS au cours de cette tâche, cochez cette case. Cela provoque une synchronisation incrémentielle. Si vous ne cochez pas cette case, la ou les mises à jour publiées ne seront disponibles pour déploiement qu'après l'exécution de votre processus de synchronisation planifiée standard. Vous pouvez aussi démarrer la synchronisation en cliquant sur l'onglet **Accueil**, puis en sélectionnant **Synchroniser les mises à jour logicielles**.
- **Utilisateur connecté** : Si vous activez cette option, le programme utilise les références d'authentification de l'utilisateur actuellement connecté pour ajouter la tâche de publication au Planificateur Microsoft. Le champ **Utilisateur** est rempli automatiquement, si bien qu'il vous suffit d'entrer le mot de passe du compte.
- **Utilisateur différent** : Si vous activez cette option, cela indique que vous souhaitez utiliser un autre compte d'utilisateur pour ajouter la tâche de publication au Planificateur Microsoft. Par exemple, vous pouvez spécifier un compte de service dont le mot de passe n'expire jamais.

Le compte doit :

- disposer de droits **Ouvrir une session en tant que tâche** ;
- être membre du groupe Administrateurs WSUS sur le serveur WSUS ;
- être membre du groupe local Administrateurs sur le serveur WSUS s'il s'agit d'un serveur distant.

Lorsque vous spécifiez un utilisateur différent, vous devez préciser si les références d'authentification correspondantes doivent s'authentifier auprès d'un serveur proxy.

- **Authentification proxy requise - Utiliser ces références d'authentification** : Si vous activez cette option, cela indique que des références d'authentification de serveur proxy sont nécessaires pour utiliser le compte d'utilisateur indiqué. Si vous choisissez ensuite **Identique à ci-dessus**, les références d'authentification du compte d'utilisateur sont utilisées comme références d'authentification de proxy. Si vous choisissez **Références d'authentification ci-dessous**, vous pouvez indiquer des références d'authentification de proxy entièrement différentes.

- **Nom d'utilisateur** : Entrez le nom d'utilisateur d'un compte sur le serveur proxy. Vous devez peut-être spécifier un domaine dans votre nom d'utilisateur (par exemple : mon-domaine\mon.nom).
 - **Mot de passe** : Entrez le mot de passe associé au compte de serveur proxy.
 - **Confirmer le mot de passe** : Entrez de nouveau le même mot de passe.
5. Cliquez sur **OK**.

La boîte de dialogue **Attention** s'affiche.

6. Au cours du processus de publication, l'état indiqué dans la colonne passe de **Publié** à **Planifié**.
7. Une fois la mise à jour publiée avec succès, l'état indiqué dans la colonne passe de **Publié** à **Oui** lorsque vous actualisez la grille.

Notez que la case à cocher de la colonne **Sélectionné** est désactivée si vous avez publié la dernière révision d'une mise à jour.

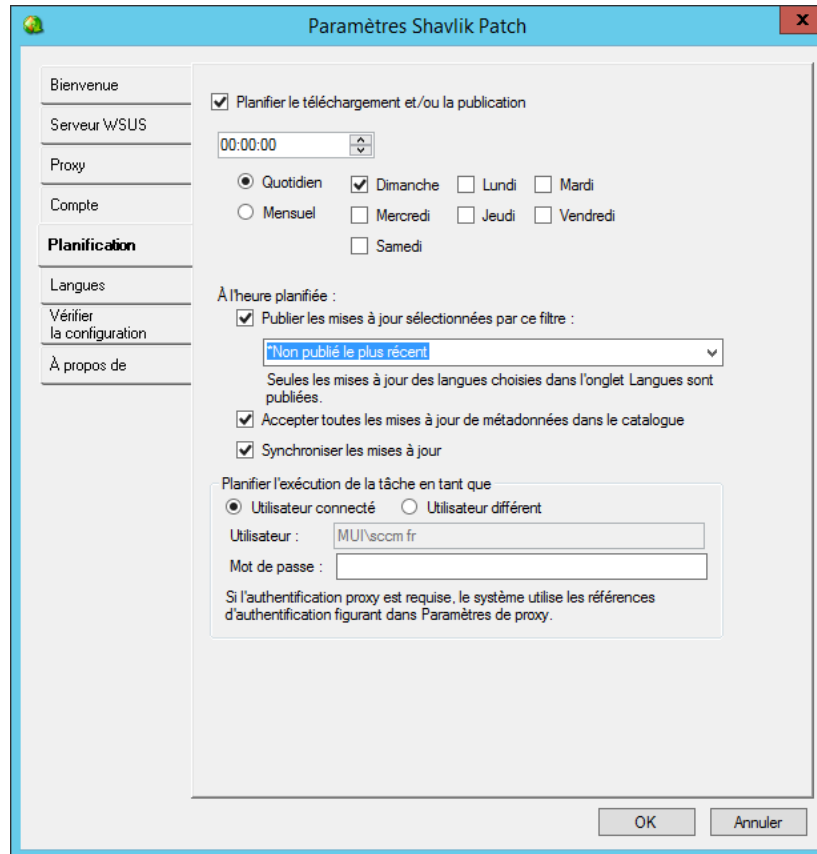
Vous pouvez trier la colonne **Publié** pour afficher la liste des mises à jour publiées, ou utiliser le filtre ***Publié**.

Publication automatique de mises à jour à l'aide d'une tâche planifiée récurrente

Vous pouvez publier automatiquement des mises à jour à intervalle régulier, en créant une tâche planifiée. Vous ne pouvez définir qu'une seule tâche récurrente planifiée à la fois.

1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Shavlik Patch**.
2. Dans l'onglet **Accueil**, cliquez sur **Paramètres** (ou cliquez avec le bouton droit sur Shavlik Patch et sélectionnez **Paramètres**).

La boîte de dialogue **Paramètres Shavlik Patch** s'affiche.



3. Dans l'onglet **Planification**, spécifiez la date d'exécution de la tâche planifiée, ainsi que la ou les actions à réaliser.

- **Planifier le téléchargement et/ou la publication** : Spécifiez le moment où la tâche récurrente doit s'exécuter.
- **Publier les paquets sélectionnés par ce filtre** : Permet de spécifier les mises à jour à planifier de façon récurrente. Vous pouvez choisir le filtre prédéfini nommé ***Non publié le plus récent** ou préférer l'un de vos filtres personnalisés.

Exemple 1 : Pour publier toutes les mises à jour non publiées précédemment et non remplacées, sélectionnez le filtre ***Non publié le plus récent**. C'est un moyen facile de publier automatiquement les nouvelles mises à jour de façon récurrente.

Exemple 2 : Supposons que vous ayez précédemment créé un filtre personnalisé qui identifie toutes les mises à jour critiques non publiées pour les produits utilisés dans votre entreprise. Il vous suffit de sélectionner ce filtre pour publier uniquement ces mises à jour spécifiques, à intervalle régulier.

Remarque : Si une mise à jour contient des paquets différents pour les différentes langues, seules les versions traduites spécifiées dans l'onglet **Langues** sont publiées.

- **Accepter toutes les mises à jour de métadonnées dans le catalogue** : Pour mettre à jour WSUS automatiquement avec toutes les révisions de métadonnées disponibles pour les mises à jour déjà publiées, cochez cette case.
- **Synchroniser les mises à jour** : Pour que Configuration Manager se synchronise automatiquement avec votre base de données WSUS au cours de cette tâche, cochez cette case. Cela provoque une synchronisation incrémentielle. Si vous ne cochez pas cette case, les mises à jour publiées ne seront disponibles pour déploiement qu'après l'exécution de votre processus de synchronisation planifiée standard. Vous pouvez aussi démarrer la synchronisation en cliquant sur l'onglet **Accueil**, puis en sélectionnant **Synchroniser les mises à jour logicielles**.
- **Utilisateur connecté** : Si vous activez cette option, le programme utilise les références d'authentification de l'utilisateur actuellement connecté pour ajouter la tâche de publication au Planificateur Microsoft. Le champ **Utilisateur** est rempli automatiquement, si bien qu'il vous suffit d'entrer le mot de passe du compte.
- **Utilisateur différent** : Si vous activez cette option, cela indique que vous souhaitez utiliser un autre compte d'utilisateur pour ajouter la tâche de publication au Planificateur Microsoft. Par exemple, vous pouvez spécifier un compte de service dont le mot de passe n'expire jamais.

Le compte doit :

- disposer de droits **Ouvrir une session en tant que tâche** ;
- être membre du groupe Administrateurs WSUS sur le serveur WSUS ;
- être membre du groupe local Administrateurs sur le serveur WSUS s'il s'agit d'un serveur distant.

Lorsque vous spécifiez un utilisateur différent, vous devez préciser si les références d'authentification correspondantes doivent s'authentifier auprès d'un serveur proxy.

- **Authentification proxy requise - Utiliser ces références d'authentification** : Si vous activez cette option, cela indique que des références d'authentification de serveur proxy sont nécessaires pour utiliser le compte d'utilisateur indiqué. Si vous choisissez ensuite **Identique à ci-dessus**, les références d'authentification du compte d'utilisateur sont utilisées comme références d'authentification de proxy. Si vous choisissez **Références d'authentification ci-dessous**, vous pouvez indiquer des références d'authentification de proxy entièrement différentes.
- **Nom d'utilisateur** : Entrez le nom d'utilisateur d'un compte sur le serveur proxy. Vous devez peut-être spécifier un domaine dans votre nom d'utilisateur (par exemple : mon-domaine\mon.nom).
- **Mot de passe** : Entrez le mot de passe associé au compte de serveur proxy.
- **Confirmer le mot de passe** : Entrez de nouveau le même mot de passe.

Vous pouvez combiner la fonction Publication auto de Shavlik Patch et les règles de déploiement automatique de Configuration Manager afin de tenir les clients à jour avec les mises à jour tierces les plus récentes.

Affichage et gestion des publications planifiées

Vous pouvez utiliser le Planificateur de tâches Microsoft pour afficher et gérer vos publications planifiées. Pour accéder aux tâches planifiées Shavlik Patch, sélectionnez **Démarrer > Outils d'administration > Tâches planifiées > Bibliothèque du Planificateur de tâches > Shavlik Patch**.

- Les tâches à exécution unique peuvent être exécutées, supprimées, désactivées ou replanifiées dans le Planificateur de tâches Microsoft.
- Si vous modifiez une planification de publication automatique récurrente dans la boîte de dialogue **Paramètres** de Shavlik Patch, la tâche est automatiquement replanifiée.
- Si vous désélectionnez la case à cocher **Planifier le téléchargement et/ou la publication** dans la boîte de dialogue **Paramètres**, puis que vous cliquez sur **OK**, la tâche récurrente est supprimée du Planificateur de tâches Microsoft.
- Une fois la tâche de publication achevée, elle reste visible dans le Planificateur de tâches Microsoft pendant un ou deux jours.

COMMENT SYNCHRONISER LES MISES A JOUR POUR LES PRODUITS TIERS

Vous devez configurer correctement System Center Configuration Manager pour synchroniser les mises à jour de produits tiers.

1. Dans l'espace de travail **Administration** de Configuration Manager, développez le dossier **Configuration du site** et cliquez sur **Sites**.
2. Cliquez avec le bouton droit sur le nom du site et sélectionnez **Configurer les composants de site > Point de mise à jour logicielle**.
3. Dans la boîte de dialogue **Propriétés du point de mise à jour logicielle**, sélectionnez l'onglet **Produits**.
4. Cochez les cases de tous les produits tiers, puis cliquez sur **OK**.

Cela spécifie les produits pour lesquels le programme doit synchroniser les mises à jour logicielles.

Vous devez répéter le processus à chaque publication d'une mise à jour pour un produit tiers.


EXPIRATION DES MISES A JOUR TIERCES

Vous pouvez faire expirer les mises à jour tierces invalidées par le fournisseur du produit ou remplacées par d'autres mises à jour. Les mises à jour logicielles expirées ne peuvent pas être déployées. Les mises à jour que vous marquez comme ayant expiré peuvent ensuite être supprimées à l'aide de l'outil de nettoyage WSUS.

Pour faire expirer une mise à jour :

1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Mises à jour tierces publiées**.
2. Sélectionnez les mises à jour à faire expirer.
3. Cliquez sur **Faire expirer X mises à jour** (où X = nombre de mises à jour sélectionnées).

Pour afficher les mises à jour expirées :

- Dans la liste **Mises à jour tierces publiées**, triez les données d'après la colonne **Expiré**. Notez que les cases à cocher de la colonne **Sélectionné** sont désactivées.
- Dans la liste **Mises à jour tierces publiées**, après une synchronisation, les mises à jour ayant expiré sont représentées par l'icône suivante : .

INFORMATIONS SUR LA PRISE EN CHARGE

Produits pris en charge

Pour consulter la liste complète des produits pris en charge par Shavlik Patch, reportez-vous au document suivant :

<http://community.shavlik.com/docs/DOC-2285>

Support technique

Pour obtenir un support technique concernant Shavlik Patch, utilisez l'une des options de support suivantes :

- Parcourez la section Shavlik Patch du site de la communauté Shavlik, à l'adresse : <http://community.shavlik.com>. Vous devez devenir membre de la communauté pour accéder à toutes les ressources disponibles.
- Ouvrez une requête de support dans la page <http://support.shavlik.com/CaseLogging.aspx>.
- Téléphonnez au support technique, au 1-866-407-5279.
- Visionnez nos didacticiels vidéo en ligne, à l'adresse <http://www.shavlik.com/support/training-videos/patch>.

Notification de fin de vie

Si la version de Shavlik Patch que vous utilisez approche de sa date de fin de vie, le message **Mise à jour disponible** s'affiche lorsque vous démarrez Shavlik Patch. Ce message indique la date d'expiration de la version et fournit un lien permettant d'obtenir la dernière version. Vous ne devez jamais laisser votre version du produit atteindre sa date de fin de vie, parce que le catalogue des mises à jour, qui contient la logique de détection et de déploiement, ne serait plus actualisé.

ANNEXE A : CREATION ET DISTRIBUTION DE CERTIFICATS

Introduction

Un certificat de signature de code est obligatoire si vous utilisez Shavlik Patch avec Configuration Manager et WSUS pour publier des mises à jour tierces. En général, la procédure est la suivante :

1. Créez un certificat de signature de code.

Vous utilisez pour ce faire une autorité de certification (CA) interne ou votre serveur WSUS.

2. (Facultatif) Si vous utilisez une CA interne pour créer le certificat de signature de code, vous devez importer le certificat dans WSUS, ce que vous faites avec Shavlik Patch.

Si vous utilisez WSUS interne pour créer le certificat de signature de code, ce dernier est automatiquement importé dans WSUS.

3. Exportez le certificat.
4. Distribuez le certificat de signature de code aux magasins de certificats appropriés sur tous vos serveurs WSUS, toutes vos consoles SCCM et toutes vos machines client.
 - Magasin de certificats Éditeurs approuvés
 - Magasin de certificats Autorités de certification racines de confiance

Cette annexe fournit des détails sur la façon de réaliser chacune de ces tâches.

Référence

Pour consulter des informations détaillées sur les certificats, au-delà du champ de la présente annexe, consultez les articles suivants.

- Pour en savoir plus sur l'établissement d'une relation de confiance en vue de prendre en charge la gestion des correctifs tiers :
[http://msdn.microsoft.com/en-us/library/bb902479\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/bb902479(v=vs.85).aspx)
- Pour en savoir plus sur la raison pour laquelle WSUS sous Windows Server 2012 R2 ne prend plus en charge par défaut la génération de certificats de signature de code, et pour connaître la solution à appliquer :
<http://blogs.technet.com/b/wsus/archive/2013/08/15/wsus-no-longer-issues-self-signed-certificates.aspx>

Remarque : Shavlik Patch applique automatiquement cette solution de rechange si vous choisissez de créer un certificat autosigné dans la boîte de dialogue **Paramètres**.

Configuration requise pour les certificats

La configuration minimale requise pour le certificat de signature est la suivante :

- La clé privée doit être exportable.
- La taille de la clé doit être de 2 048 octets ou plus.
- Il doit s'agir d'un certificat de signature de code.

Création d'un certificat de signature de code

Remarque : Vous pouvez sauter cette section si vous possédez déjà un certificat de signature de code.

Vous disposez de deux options pour créer un certificat de signature de code :

- Utiliser un certificat de signature de code créé par une autorité de certification (CA) interne
- Utiliser l'interface utilisateur Shavlik Patch pour demander à WSUS de créer un certificat de signature de code autosigné

Création d'un certificat de signature de code avec une CA

La création d'un certificat à l'aide d'une autorité de certification (CA) de confiance offre plusieurs avantages :

- Distribution : Plus besoin de distribuer le certificat aux autres machines du même domaine.
- Gestion : Simplifie la gestion, car le certificat peut être géré comme les autres certificats de votre environnement.

Suivez votre processus habituel pour créer un certificat à partir de votre CA interne. Une fois le certificat créé, vous devez l'écrire sur le serveur WSUS. Pour ce faire, utilisez la fonction **Importer un certificat** de Shavlik Patch. Pour en savoir plus, reportez-vous à la section « *Importation d'un certificat* ».

Utilisation de Shavlik Patch et de WSUS pour créer un certificat de signature de code

Remarque : Le compte d'utilisateur employé doit être membre du groupe Administrateurs WSUS pour pouvoir créer un certificat de signature de code dans l'interface Shavlik Patch.

Vous pouvez utiliser l'interface Shavlik Patch pour demander à WSUS de créer un certificat de signature de code autosigné pour votre entreprise. La création d'un certificat de signature de code est activée par défaut dans les versions de WSUS antérieures à Windows Server 2012 R2.

Important ! Si vous utilisez WSUS sous Windows Server 2012 R2, la fonction de génération de certificats de signature de code autosignés n'est plus utilisée et est désactivée par défaut. Vous pouvez toutefois restaurer cette fonction à l'aide de la

solution de rechange présentée dans l'article suivant :

<http://blogs.technet.com/b/wsus/archive/2013/08/15/wsus-no-longer-issues-self-signed-certificates.aspx>

Si vous choisissez de créer un certificat de signature de code dans Shavlik Patch à l'aide d'un point de mise à jour logicielle (serveur WSUS) sous Windows Server 2012 R2 ou supérieur, cette solution de rechange est appliquée automatiquement.

Pour créer un certificat de signature de code autosigné avec WSUS :

1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Shavlik Patch**.
2. Dans l'onglet **Accueil** de Configuration Manager, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue **Paramètres Shavlik Patch**, sélectionnez l'onglet **Serveur WSUS**.
4. Cliquez sur **Créer un certificat autosigné**.

S'il existe déjà un certificat, la boîte de dialogue **Avertissement** s'affiche. Ne continuez que si vous êtes certain d'avoir besoin d'un nouveau certificat. Le message d'avertissement explique comment procéder si vous devez remplacer ou supprimer un certificat existant.

Si vous cliquez sur **OK**, une deuxième boîte de dialogue **Avertissement** s'affiche. Cette boîte de dialogue affiche la configuration requise pour le certificat que vous êtes sur le point de créer. Lisez attentivement ces informations, puis cliquez sur **OK**.

Le nouveau certificat est créé sur le serveur WSUS et inscrit auprès de WSUS. Les détails de ce certificat s'affichent dans la zone **Certificat actuel**.

Le certificat est également installé dans les magasins de certificats suivants sur la console Configuration Manager locale :

- Autorités de certification racines de confiance
- Éditeurs approuvés

Importation d'un certificat

Cette section s'applique uniquement si vous avez créé votre certificat de signature de code à l'aide d'une CA interne. L'importation du certificat permet d'écrire ce certificat sur le serveur WSUS et dans les magasins de certificats appropriés sur votre machine. Vous n'avez pas besoin d'exécuter le processus d'importation si vous avez utilisé WSUS pour créer le certificat de signature de code, car ce certificat est automatiquement écrit aux emplacements voulus.

Remarque : Pour importer un certificat, vous devez disposer d'une connexion sécurisée (SSL) avec le serveur WSUS. Pour ce faire, vous devez d'abord cocher la case **Connexion sécurisée** dans la zone **Serveur WSUS** de l'onglet **Serveur WSUS**. Vous devez également configurer IIS afin d'utiliser SSL.

Pour importer un certificat :

1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Shavlik Patch**.
2. Dans l'onglet **Accueil** de Configuration Manager, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue **Paramètres Shavlik Patch**, sélectionnez l'onglet **Serveur WSUS**.
4. Cliquez sur **Importer**.
5. Naviguez jusqu'au fichier de certificat et cliquez sur **OK**.

Le fichier de certificat contient une copie de la clé privée et est identifié par l'extension .PFX.

Exportation d'un certificat

Le processus d'exportation permet d'exporter le certificat qui sert à signer les mises à jour publiées afin de le stocker dans un emplacement accessible sur le réseau.

Remarque : Le processus d'exportation exporte uniquement le certificat public ; la clé privée n'est PAS exportée.

1. Dans l'espace de travail **Bibliothèque de logiciels** de Configuration Manager, développez le dossier **Mises à jour logicielles** et cliquez sur **Shavlik Patch**.
2. Dans l'onglet **Accueil** de Configuration Manager, cliquez sur **Paramètres**.
3. Dans la boîte de dialogue **Paramètres Shavlik Patch**, sélectionnez l'onglet **Serveur WSUS**.
4. Cliquez sur **Exporter**.
5. Spécifiez l'emplacement et le nom de fichier voulus, puis cliquez sur **Enregistrer**.

Il s'agit généralement d'un fichier .CER.

Après avoir exporté le certificat, vous devez le distribuer à tous les autres serveurs WSUS et à toutes vos machines client. Cette opération est indispensable pour que les machines reçoivent les mises à jour publiées en local.

Le processus de distribution est décrit à la section suivante.

Distribution du certificat

Vous devez distribuer le certificat de signature de code à tous les autres serveurs hébergeant vos consoles Configuration Manager et WSUS, ainsi qu'à toutes les machines client. Le ou les magasins de certificats où le certificat est copié dépendent du mode de création de ce certificat de signature de code.

- Si votre certificat de signature de code a été créé par WSUS (et qu'il s'agit donc d'un certificat autosigné), vous devez le copier vers les emplacements suivants sur tous vos serveurs WSUS, toutes vos consoles SCCM et toutes vos machines client :
 - Magasin de certificats Éditeurs approuvés
 - Magasin de certificats Autorités de certification racines de confiance
- Si le certificat de signature de code a été créé par une autorité de certification (CA) dont la racine est déjà reconnue comme élément de confiance par vos clients, il vous suffit de copier ce certificat vers le magasin de certificats Éditeurs approuvés sur vos serveurs WSUS et machines client.

Utilisation d'une stratégie de groupe pour distribuer le certificat

L'une des méthodes courantes pour distribuer le certificat de signature de code à vos serveurs et/ou machines client consiste à utiliser une stratégie de groupe. Pour consulter des instructions d'ordre général concernant cette tâche, reportez-vous à l'étape 3 de l'article suivant :

<http://blogs.technet.com/b/jasonlewis/archive/2011/07/12/system-center-updates-publisher-signing-certificate-requirements-amp-step-by-step-guide.aspx>

Utilisation de MMC pour distribuer manuellement le certificat

L'autre méthode de distribution du certificat de signature de code consiste à utiliser MMC. C'est un moyen facile pour distribuer le certificat à une poignée de machines locales, mais cette méthode est peu pratique si vous voulez distribuer le certificat à un grand nombre de machines réparties dans toute votre entreprise.

1. Sur la machine cible, démarrez Microsoft Management Console (MMC).
2. Dans le magasin de certificats, cliquez avec le bouton droit sur **Éditeurs approuvés**, puis sélectionnez **Toutes les tâches > Importer**.
3. Dans la boîte de dialogue **Bienvenue dans l'Assistant Importation du certificat**, cliquez sur **Suivant**.
4. Dans la boîte de dialogue **Fichier à importer**, naviguez jusqu'à votre fichier de clé publique, puis cliquez sur **Suivant**.
5. Dans la boîte de dialogue **Magasin de certificats**, cliquez sur **Placer tous les certificats dans le magasin suivant**, puis sur **Suivant**.
6. Dans la boîte de dialogue **Fin de l'Assistant Importation de certificat**, cliquez sur **Terminer**.
7. Dans la boîte de dialogue de confirmation, cliquez sur **OK**.
8. (Facultatif) Si vous avez créé votre certificat avec WSUS, répétez les opérations 2 à 7, mais en sélectionnant **Autorités de certification racines de confiance** à l'étape 2.