

Shavlik Patch for Microsoft System Center

Benutzerhandbuch

Zur Verwendung mit Microsoft System Center
Configuration Manager 2012



shavlik

Copyright

Copyright © 2014 Shavlik. Alle Rechte vorbehalten. Dieses Produkt ist durch das Urheberrecht und andere Gesetze zum Schutz geistigen Eigentums in den Vereinigten Staaten und anderen Ländern sowie durch internationale Verträge geschützt.

Kein Teil dieses Dokuments darf ohne ausdrückliche schriftliche Erlaubnis von Shavlik in irgendeiner Form (elektronisch, mechanisch, durch Fotokopie, Aufzeichnung oder mit anderen Mitteln) für andere Zwecke als der persönlichen Nutzung durch den Käufer reproduziert oder neu übertragen werden.

Marken

Shavlik ist eine Marke von Shavlik in den Vereinigten Staaten und anderen Ländern. Microsoft, Windows und System Center Configuration Manager sind entweder Marken oder eingetragene Marken der Microsoft Corporation.

Alle anderen hierin erwähnten Marken, Markennamen oder Bilder sind Eigentum der jeweiligen Inhaber.

Informationen zum Dokument und zur Historie

Dokumentnummer: nicht zutreffend

Datum	Version	Beschreibung
Februar 2014	Erstversion	Erstveröffentlichung des Shavlik Patch for Microsoft System Center – Benutzerhandbuchs .
November 2014	Shavlik Patch 2.1	Aufnahme von Informationen zur Synchronisierung von Updates von Drittanbietern. Aktualisierung der Systemanforderungen. Neue Informationen zu Configuration Checker, zusammengesetzten Filtern, Detailbereich, Proxykonfiguration, Ablösung, Metadaten, Sprachen und Ende der Lebensdauer.

Inhalt

VORBEREITUNGEN FÜR DIE VERWENDUNG VON SHAVLIK PATCH.....	5
Willkommen	5
Systemanforderungen	5
Installieren des Shavlik Patch Configuration Manager-Add-ins	7
Konfigurieren der Einstellungen für Shavlik Patch	8
Registerkarte WSUS-Server	9
Informationen zum WSUS-Server	9
Informationen zum Codesignaturzertifikat	10
Registerkarte „Proxy“	10
Registerkarte Konto	12
Registerkarte „Sprachen“	13
Registerkarte „Einrichtung überprüfen“	15
Registerkarte „Info“	16
Registerkarte „Planen“	16
Elemente, die durch das Shavlik Patch Add-in zu Configuration Manager hinzugefügt werden	17
Die Informationen im Raster	19
XML anzeigen	20
Verwendung der Filter	21
Vordefinierte Filter	21
Benutzerdefinierte Filter	22
Zusammengesetzte Filter	23
VORGEHENSWEISE BEIM VERÖFFENTLICHEN VON UPDATES	24
Manuelles Veröffentlichen von Updates von Drittanbietern	24
Automatisches Veröffentlichen von Updates mit einem wiederholten geplanten Task.....	27
Anzeigen und Verwalten von geplanten Veröffentlichungen.....	29
VORGEHENSWEISE BEIM SYNCHRONISIEREN VON UPDATES FÜR PRODUKTE VON DRITTANBIETERN.....	30
ABLAUFENLASSEN VON DRITTANBIETERUPDATES.....	31

- INFORMATIONEN ZUM SUPPORT 32
 - Unterstützte Produkte 32
 - Technische Unterstützung 32
 - Meldung zum Ende der Lebensdauer 32

- ANHANG A: ERSTELLEN UND VERTEILEN VON ZERTIFIKATEN 33
 - Übersicht 33
 - Referenz 33
 - Zertifikatanforderungen 33
 - Erstellen eines Codesignaturzertifikats 34
 - Erstellen eines Codesignaturzertifikats mit einer Zertifizierungsstelle 34
 - Erstellen eines Codesignaturzertifikats unter Verwendung von Shavlik Patch und WSUS 34
 - Importieren eines Zertifikats 35
 - Zertifikat exportieren 37
 - Verteilen des Zertifikats 37
 - Verwendung von Gruppenrichtlinien zur Verteilung des Zertifikats 38
 - Verwendung von MMC zur Verteilung des Zertifikats 38

VORBEREITUNGEN FÜR DIE VERWENDUNG VON SHAVLIK PATCH

Willkommen

Willkommen bei Shavlik Patch for Microsoft System Center, einem Add-in, das die Funktionen und Merkmale von Microsoft System Center Configuration Manager dahingehend erweitert, dass es die Veröffentlichung von Drittanbieterupdates und Legacyprodukten ermöglicht, die nicht mehr von Configuration Manager unterstützt werden. Mit Shavlik Patch können Sie einen einzigen Configuration Manager-Workflow zur Veröffentlichung von Updates für Microsoft und Nicht-Microsoft-Produkte nutzen.

Shavlik Patch umfasst zwei Komponenten:

- **Updatekatalog:** Enthält die Erkennungs- und Bereitstellungslogik, die zum Patchen von Nicht-Microsoft-Produkten und Microsoft Legacyprodukten verwendet wird. Der Katalog umfasst eine Vielzahl von Updatedateien unterschiedlicher Softwareanbieter wie Adobe, Apple, Firefox, Sun und andere.
- **Add-in für die Configuration Manager-Konsole:** Wird zur Auswahl von Updates aus dem Katalog, deren Veröffentlichung auf den WSUS-Servern, zur Synchronisierung mit Configuration Manager und zum Ablaufenlassen veröffentlichter Updates verwendet. Hierdurch können Sie Ihre Microsoft-Legacyprodukte und Ihre Nicht-Microsoft-Produkte mit demselben Configuration Manager-Workflow patchen, der auch fürs Patching von Microsoft-Produkten verwendet wird.

Systemanforderungen

Für die Installation und Verwendung von Shavlik Patch müssen folgende Voraussetzungen gegeben sein:

- Shavlik Patch wird als Add-on zu einer vorhandenen Configuration Manager 2012-Konsole (SP1 oder neuer) installiert. Die Configuration Manager-Konsole muss auf einem der folgenden Windows-Betriebssysteme installiert sein:
 - Windows Server 2012 oder höher
 - Windows Server 2008 R2 SP1 oder höher
 - Windows 8 oder höher
 - Windows 7 SP1 oder höher
- .NET Framework 4.5.1 oder höher
Falls die vorausgesetzte .NET Framework-Softwareversion nicht vorhanden ist, wird NET Framework 4.5.1 im Rahmen der Shavlik Patch-Installation installiert.
- Anforderungen für den Windows Server Update Services (WSUS)-Client
 - Wenn Shavlik Patch auf dem primären WSUS-Server installiert ist und Sie Windows Server 2012 oder Windows 8 verwenden, müssen die Features WSUS API und PowerShell-Cmdlets aktiviert werden.
 - Wenn sich WSUS auf einem remoten Windows 8- oder Windows 8.1-Computer befindet, muss das Feature „Remoteverwaltungstools“ auf dem betreffenden Computer installiert sein. Die Version der Remoteverwaltungstools und die WSUS-Version müssen übereinstimmen, sonst können Sie keine Updates bereitstellen.

- Wenn auf dem primären WSUS-Server WSUS 3.0 SP2 ausgeführt wird, dann muss die WSUS 3.0 SP2-Verwaltungskonsole auf demselben Computer installiert sein wie Shavlik Patch. Auf dem Computer mit dem WSUS-Server und auf dem Computer mit der Configuration Manager-Konsole müssen die beiden Patches KB2720211 und KB2734608 installiert sein.
- Der Microsoft Aufgabenplanungsdienst muss aktiviert sein und der Benutzer muss über die erforderlichen Rechte zur Erstellung geplanter Tasks verfügen.
- Shavlik Protect Cloud-Konto
- Der Benutzer, der Shavlik Patch ausführt, muss Rechte zum **Anmelden als Stapelverarbeitungsauftrag** haben und muss ein Mitglied der Gruppe „WSUS-Administratoren“ auf dem WSUS-Server sein. Wenn der WSUS-Server remote ist, muss der Benutzer außerdem ein Mitglied der lokalen Administratorengruppe auf dem WSUS-Server sein.
- Anforderungen an die Clientcomputer:

Jeder Ihrer Clientcomputer muss die folgenden Voraussetzungen erfüllen, damit die von einem WSUS-Server verteilten Nicht-Windows-Updates bereitgestellt werden können:

- Es muss eine Kopie des Codesignaturzertifikats im entsprechenden Zertifikatspeicher vorliegen.
- Die Richtlinieneinstellung **Signierte Updates aus einem Intranetspeicherort für Microsoft-Updatedienste zulassen** muss aktiviert sein.

Installieren des Shavlik Patch Configuration Manager-Add-ins

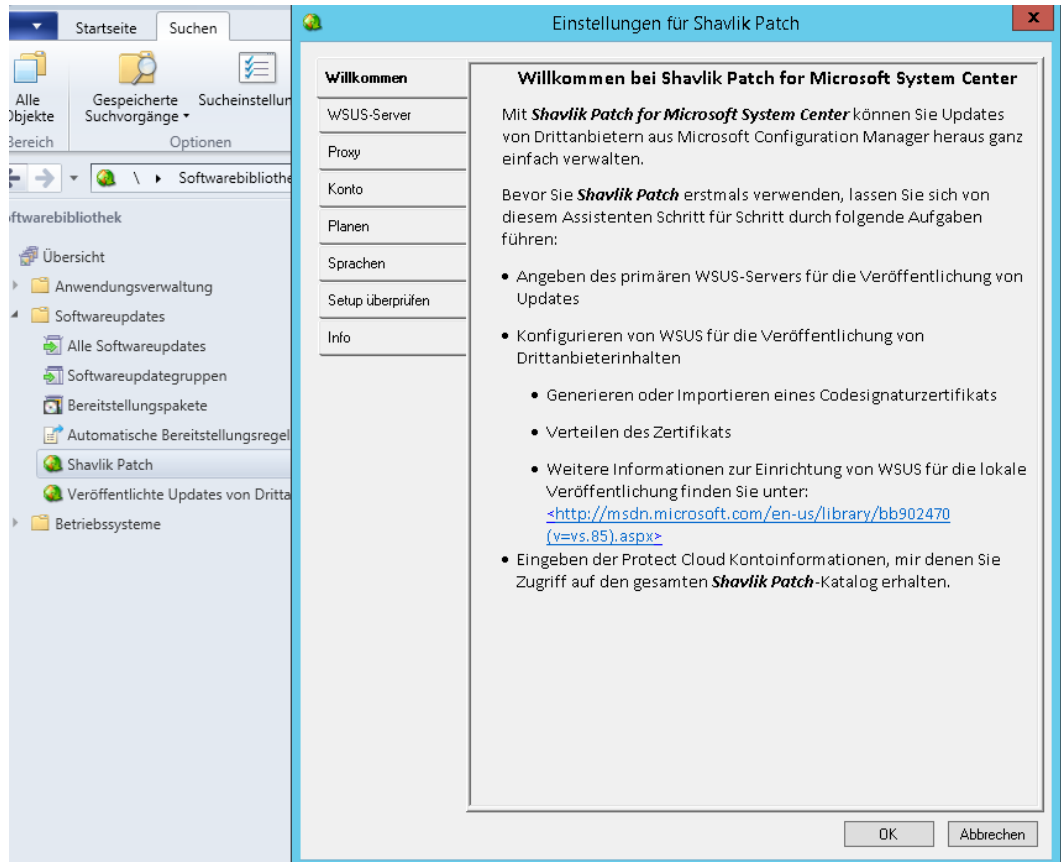
Hinweis: Die Installation des Add-ins muss als Administrator ausgeführt werden.

1. Navigieren Sie mit einem Webbrowser zur folgenden Adresse:
www.shavlik.com/downloads/
2. Klicken Sie auf den Link **Shavlik Patch Free Trial** für eine kostenlose Testversion.
3. Laden Sie die Setupdatei **Shavlik Patch for Configuration Manager 2012** herunter.
4. Schließen Sie System Center Configuration Manager.
5. Starten Sie die Installation, indem Sie auf die Datei mit dem Namen **SCCMPatchSetup.exe** doppelklicken.
 - Wenn auf dem Configuration Manager-Computer kein .NET Framework 4.5.1 oder höher installiert ist, werden Sie aufgefordert, .NET Framework 4.5.1 zu installieren, bevor Sie mit der Installation fortfahren. Zur Installation dieser Voraussetzung folgend Sie den Anweisungen auf dem Bildschirm.
 - Wenn alle Anforderungen installiert sind, wird die Lizenzvereinbarung angezeigt. Sie müssen die Bedingungen dieser Lizenzvereinbarung akzeptieren, damit Sie das Programm installieren können.
6. Aktivieren Sie das Kontrollkästchen, um die Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Installieren**.

Im Anschluss an die Installation der Dateien wird das Dialogfeld **Abgeschlossen** angezeigt.
7. Klicken Sie auf **Fertig stellen**.

Konfigurieren der Einstellungen für Shavlik Patch

Bei der Installation des Shavlik Patch Add-ins werden zwei neue Listenelemente zum Ordner **Softwarebibliothek > Softwareupdates** hinzugefügt. Die neuen Listenelemente heißen **Shavlik Patch** und **Veröffentlichte Updates von Drittanbietern**. Wenn Sie zum ersten Mal auf eines dieser beiden neuen Listenelemente zugreifen, wird der Setup-Assistent gestartet.



Der Assistent leitet Sie schrittweise durch die Registerkarten für den Einrichtungsvorgang. Shavlik Patch ist sofort nach Abschluss der Einrichtung und dem Speichern der Einstellungen einsatzbereit. Sie können jederzeit zu diesen Einstellungen zurückkehren, indem Sie auf der Registerkarte **Startseite** (Home) auf die Schaltfläche **Einstellungen** klicken.

Klicken Sie nach der Überprüfung der Angaben auf der Registerkarte **Willkommen** auf **Weiter**.

Die erste Registerkarte der Einrichtung ist die Registerkarte **WSUS-Server**.

Registerkarte **WSUS-Server**

Die Registerkarte **WSUS Server** wird zur Konfiguration der Kommunikation zwischen dem Add-in und dem WSUS-Server verwendet. Sie wird außerdem zur Definition des Zertifikats verwendet, das zum digitalen Signieren des Inhalts zum Einsatz kommt, der auf dem WSUS-Server veröffentlicht wird.

Informationen zum WSUS-Server

- **Name:** Geben Sie den Namen oder die IP-Adresse Ihres WSUS-Servers ein. Diese Informationen werden in der Regel ermittelt und automatisch aufgefüllt.
- **Port:** Bestätigen Sie die Portnummer, die zum Herstellen einer Verbindung zum WSUS-Server verwendet werden soll. Der Standardwert für nicht geschützte Verbindungen lautet entweder 80 oder 8530. Für sichere Verbindungen wird typischerweise 443 oder 8531 verwendet.
- **Sichere Verbindung:** Wenn Ihr WSUS-Server für die Verwendung einer sicheren Verbindung konfiguriert wurde, aktivieren Sie dieses Kontrollkästchen. Eine sichere Verbindung ist erforderlich, wenn Sie ein

Signaturzertifikat importieren müssen. Nähere Informationen siehe Anhang A, *Importieren eines Zertifikats*.

- **Verbindung testen:** Um zu testen, ob Sie auf den WSUS-Server zugreifen können, klicken Sie auf **Verbindung testen**.

Informationen zum Codesignaturzertifikat

Die Veröffentlichung von Updates auf dem WSUS-Server erfordert ein Codesignaturzertifikat. Wenn bereits ein Signaturzertifikat vorliegt, wird es im Bereich **Aktuelles Zertifikat** angezeigt.

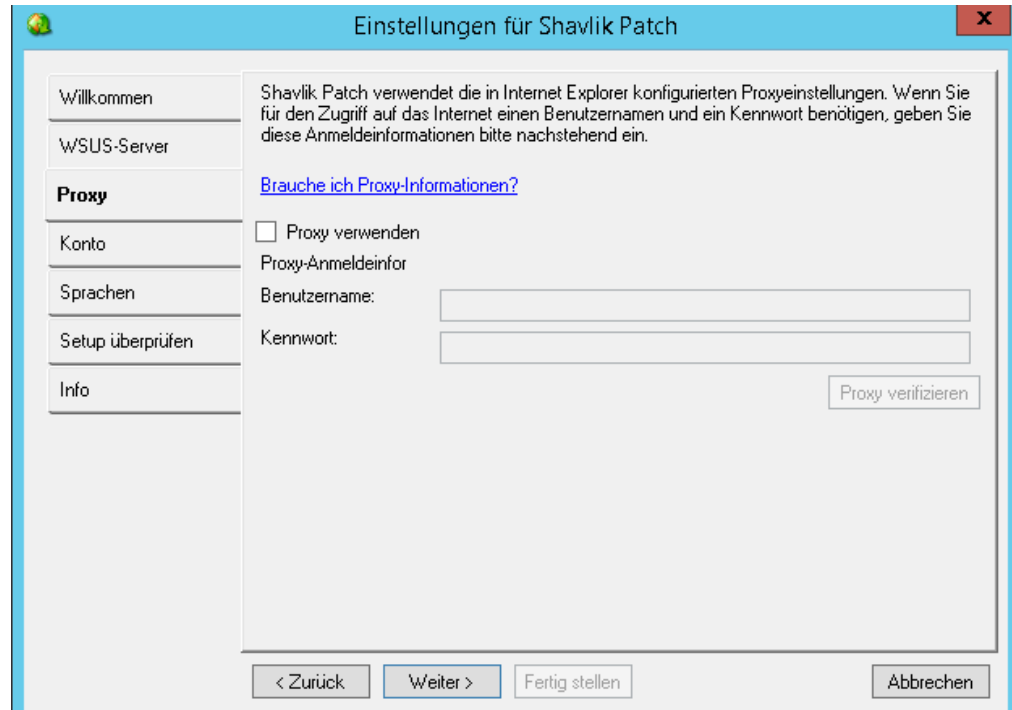
Sie können folgende Tasks für Zertifikate durchführen:

- **Exportieren:** Exportiert das aktuelle Zertifikat aus Shavlik Patch. Aus Sicherheitsgründen wird das Zertifikat ohne den privaten Schlüssel exportiert. Nach dem Exportieren des Zertifikats verteilen Sie es an Ihre Clients und Infrastrukturcomputer (z. B. andere Computer, auf denen das Shavlik Patch Add-in ausgeführt wird, nachgeordnete WSUS-Server und Windows Update-Clients). Dies ist notwendig, damit die Computer lokal veröffentlichte Updates erhalten.
- **Importieren:** Importiert ein Codesignaturzertifikat, das von einer Zertifizierungsstelle erstellt wurde. Zum Importieren eines Zertifikats wird eine sichere Verbindung benötigt.
- **Ein selbstsigniertes Zertifikat erstellen:** Erstellt ein Codesignaturzertifikat für Ihr Unternehmen. Dieser Prozess nutzt die Dienste von WSUS zur Erstellung des Zertifikats.

Ausführliche Informationen zum Exportieren, Importieren und Erstellen von Zertifikaten finden Sie im *Anhang A: Erstellen und Verwenden von Zertifikaten*.

Registerkarte „Proxy“

Auf der Registerkarte **Proxy** können Sie die Proxyeinstellungen ändern, die von Shavlik Protect beim Internetzugriff unter Verwendung Ihres Browsers verwendet werden sollen. Shavlik Patch kontrolliert generell die Proxyeinstellungen in Internet Explorer und führt einen Internet-Konnektivitätstest durch, um zu bestimmen, ob Proxyservereinstellungen erforderlich sind oder nicht. Wenn Shavlik Patch mit diesen Einstellungen nicht auf das Internet zugreifen kann oder wenn Sie jedes Mal einen Benutzernamen und ein Kennwort eingeben müssen, wenn Sie Ihren Browser starten und im Internet navigieren, dann müssen Sie die Proxyoptionen konfigurieren.



- **Benötige ich Proxyinformationen?:** Um herauszufinden, ob Shavlik Patch Ihre aktuellen Internet Explorer-Proxyeinstellungen für den Zugriff auf das Internet und für andere Vorgänge verwenden kann, klicken Sie auf diese Schaltfläche. Verläuft der Test erfolgreich, sind keine weiteren Schritte erforderlich. Schlägt der Test fehl, bedeutet dies in der Regel, dass Ihre Organisation eine andere Authentifizierung verwendet und Sie Ihre Proxyeinstellungen dahingehend ändern müssen, dass Sie die Anmeldeinformationen (Benutzername/Kennwort) angeben.
- **Proxy verwenden:** Wenn diese Option aktiviert ist, bedeutet das, dass Sie Proxyanmeldeinformationen angeben. Wenn Sie das Kontrollkästchen nach der Angabe von Anmeldeinformationen löschen, werden die Anmeldeinformationen zwar gespeichert, aber nicht verwendet.
- **Benutzername:** Geben Sie den Anmeldebenutzernamen ein. Es kann sein, dass Sie dabei als Teil Ihres Benutzernamens auch eine Domäne angeben müssen (beispielsweise: eigeneDomäne\eigener.Name).
- **Kennwort:** Geben Sie das Anmeldekennwort ein.
- **Testen:** Klicken Sie auf diese Schaltfläche, um die Anmeldeinformationen zu testen.

Registerkarte **Konto**

Sie müssen beim Shavlik Protect Cloud-Service angemeldet sein, damit das Add-in automatisch auf den vollständigen Shavlik Patch-Katalog zugreifen und ihn herunterladen kann. Das Add-in verwendet Ihr Protect Cloud-Konto, um regelmäßig zu prüfen, ob ein neuer Katalog verfügbar ist. Wenn Sie kein Protect Cloud-Konto besitzen, erhalten Sie nur auf den Inhalt der Testversion Zugriff, der lediglich einige wenige Beispielupdates umfasst.

Hinweis: Nähere Informationen zur Shavlik Protect-Cloud finden Sie im Internet unter <https://protectcloud.shavlik.com>.

- **Benutzername:** Geben Sie den Benutzernamen ein, den Sie zur Authentifizierung bei Ihrem Protect Cloud-Konto verwenden.
- **Kennwort:** Geben Sie das Kennwort ein, das Sie zur Authentifizierung bei Ihrem Protect Cloud-Konto verwenden.
- **Jetzt registrieren:** Wenn Sie kein Protect Cloud-Konto besitzen, klicken Sie auf diese Schaltfläche und folgen Sie den Anweisungen auf dem Bildschirm, um sich als Benutzer registrieren zu lassen. Sie müssen ein registrierter Benutzer sein, um Zugriff auf den vollständigen Shavlik Patch-Katalog zu erhalten.
- **Überprüfen:** Wenn Sie testen wollen, ob Sie mit den angegebenen Anmeldeinformationen eine Verbindung zu Ihrem Protect Cloud-Konto herstellen können, klicken Sie auf **Überprüfen**. Wenn Sie keine Verbindung zu Ihrem Konto herstellen können, haben Sie keinen Zugriff auf den vollständigen Shavlik Patch-Katalog.

- **Informieren, wenn Metadaten-Revisionen verfügbar sind:** Sobald neue Metadaten für zuvor von Ihnen veröffentlichte Updates verfügbar sind, wird ein Dialogfeld angezeigt, in dem Sie die Updates entweder sofort in WSUS überarbeiten oder die neuen Metadaten ignorieren können.

Shavlik Patch sucht nach Metadaten-Revisionen, sobald eine neue Kopie des Katalogs heruntergeladen wird. In den meisten Fällen ist die empfohlene Vorgehensweise das Veröffentlichen der Revisionen.

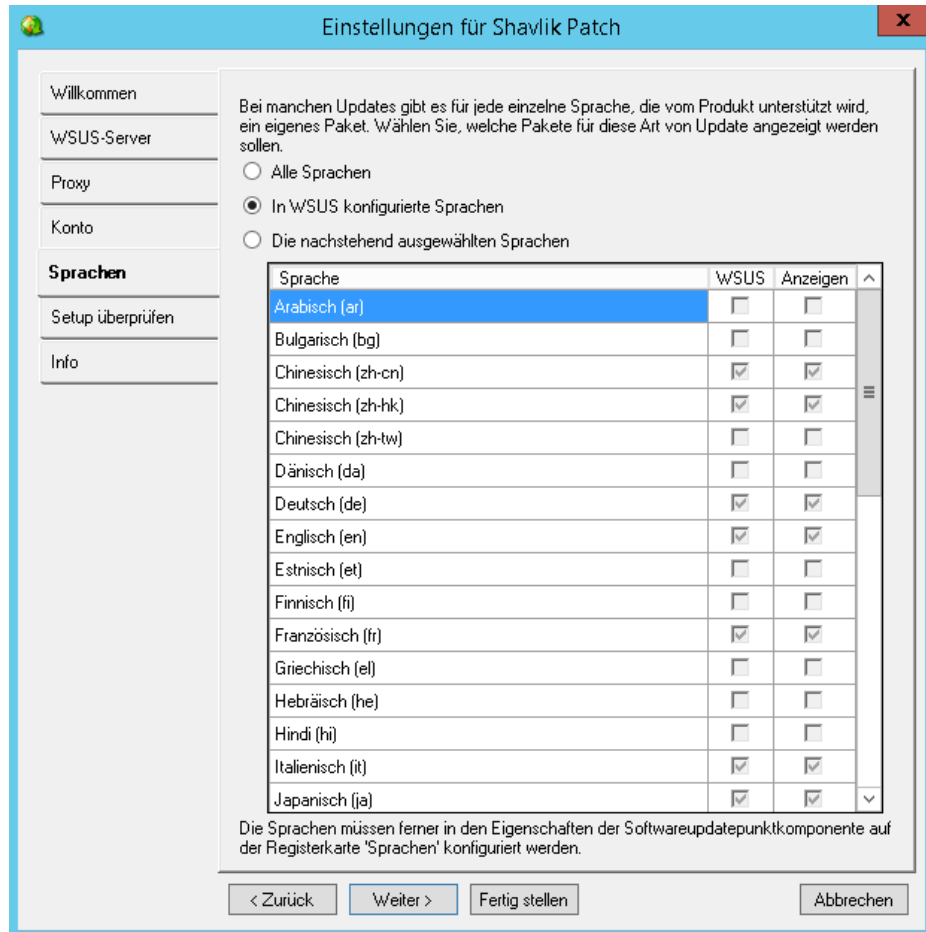
Wenn Sie das Kontrollkästchen **Meine Wahl merken und mich nicht noch einmal auffordern** aktivieren und dann auf **Ja** klicken, ändert sich die Option „Metadaten“ auf der Registerkarte **Konto** in **WSUS-Metadaten ohne Bestätigung aktualisieren**.

Wenn Sie das Kontrollkästchen **Meine Wahl merken und mich nicht noch einmal auffordern** aktivieren und dann auf **Nein** klicken, ändert sich die Option „Metadaten“ auf der Registerkarte **Konto** in **Nicht mehr fragen und WSUS nicht aktualisieren**.

- **WSUS-Metadaten ohne Bestätigung aktualisieren:** Aktualisiert die veröffentlichten Updates automatisch mit den geänderten Metadaten, ohne Sie zu benachrichtigen.
- **Nicht mehr fragen und WSUS nicht aktualisieren:** Es erfolgt keine Aktion, wenn geänderte Metadaten verfügbar sind. Mithilfe des Filters ***Geänderte Metadaten** können Sie ermitteln, wann Metadaten-Revisionen verfügbar sind.

Registerkarte „Sprachen“

Oft kann eine einzelne Aktualisierung für eine beliebige Sprachversion eines Produkts übernommen werden. Bei einigen Updates sind jedoch unterschiedliche Updatepakete für die einzelnen Produktsprachen vorhanden. Auf der Registerkarte **Sprachen** können Sie auswählen, welche Sprachen Sie bei diesen sprachspezifischen Updates berücksichtigen möchten. Durch die Auswahl der Sprachen wird festgelegt, welche Sprachversionen im Shavlik Patch-Raster angezeigt werden.



- **Alle Sprachen:** Shavlik Patch zeigt alle verfügbaren Sprachpakete für jedes Update an.
- **In WSUS konfigurierte Sprachen:** Shavlik Patch zeigt nur Pakete für diejenigen Sprachen an, die derzeit zum Download auf dem WSUS-Server konfiguriert sind. Dies ist die Standardeinstellung. (Um die WSUS-Spracheinstellungen zu überprüfen oder zu ändern, starten Sie Update Services auf dem WSUS-Server, klicken auf **Optionen**, dann auf **Updatedateien und -sprachen** und öffnen dann die Registerkarte **Updatesprachen**.)
- **Unten ausgewählte Sprachen:** Shavlik Patch zeigt nur Pakete für die in der Tabelle ausgewählten Sprachen an. Sie müssen mindestens eine Sprache auswählen.
 - **Spalte „WSUS“:** Gibt an, ob die Sprache derzeit auf Ihrem WSUS-Server konfiguriert ist. Die Kontrollkästchen in dieser Spalte können nicht geändert werden.
 - **Spalte „Anzeige“:** Aktivieren Sie das Kontrollkästchen für jede Sprache, die im **Shavlik Patch**-Raster angezeigt werden soll. Sie können eine Sprache auch dann auswählen, wenn sie derzeit nicht im WSUS konfiguriert ist.

Registerkarte „Einrichtung überprüfen“

Diese Registerkarte dient dazu, Configuration Checker zu starten. Dieses Dienstprogramm wird in der Regel unmittelbar nach der ersten Installation von Shavlik Patch einmal ausgeführt.

Mit Configuration Checker wird festgestellt, ob Sie alle Voraussetzungen für die Verwendung von Shavlik Patch erfüllen. Um Configuration Checker auszuführen, klicken Sie auf der Registerkarte **Setup überprüfen** auf die Schaltfläche **Configuration Checker starten**. Sie können Configuration Checker auch von der Befehlszeile aus ausführen: C:\Programme (x86)\Microsoft Configuration Manager\AdminConsole\bin\ST.SCCM.ConfigurationChecker.exe. Sie müssen Configuration Checker mit vollen Administratorrechten ausführen. Jedoch können Sie auch Konten auswerten, die nicht über volle Administratorrechte verfügen.

Die meisten Informationen in diesem Dialogfeld sind vorab ausgefüllt, können aber bei Bedarf geändert werden.

- **FQDN des WSUS-Servers:** Geben Sie den vollqualifizierten Domännennamen des WSUS-Servers ein.
- **Port:** Wählen Sie den Port für den Zugriff auf den WSUS-Server aus.
- **Cloud-Konto:** Geben Sie Ihren Protect Cloud-Benutzernamen ein.
- **Cloud-Kennwort:** Geben Sie Ihr Protect Cloud-Kennwort ein.
- **Benutzerkonto (Domäne/Benutzer):** Geben Sie die Domäne und den Benutzernamen des Kontos ein, das Sie auswerten möchten.
- **Kontokennwort:** Geben Sie das Kennwort für das Benutzerkonto ein. Dieses Feld kann leer bleiben, wenn Sie das Konto auswerten, mit dem Sie dieses Tool ausführen.
- **Proxy verwenden:** Wenn diese Option aktiviert ist, müssen Proxyserver-Anmeldeinformationen angegeben werden, um den Configuration Checker-Test auszuführen. Wenn Sie das Kontrollkästchen nach der Angabe von

Anmeldeinformationen löschen, werden die Anmeldeinformationen zwar gespeichert, aber nicht verwendet. Dieses Feld zeigt zunächst, was auf der Registerkarte **Proxy** konfiguriert ist. Die Angaben können hier jedoch vorübergehend überschrieben werden.

- **Benutzername für Proxy:** Geben Sie den Benutzernamen für ein Konto auf dem Proxyserver ein. Dieses Feld wird automatisch mit dem Benutzernamen gefüllt, der auf der Registerkarte **Proxy** angegeben wurde. Es kann jedoch überschrieben werden. Es kann sein, dass Sie dabei als Teil Ihres Benutzernamens auch eine Domäne angeben müssen (beispielsweise: eigeneDomäne\eigener.Name).
- **Kennwort für Proxy:** Geben Sie das Kennwort für das Proxyserver-Konto ein.

Das Dienstprogramm überprüft Folgendes:

- Die Möglichkeit, mit einem vollqualifizierten Domännennamen und einer Portnummer eine Verbindung mit dem WSUS-Server herzustellen.
- Die Möglichkeit, mit einem Benutzernamen und einem Kennwort eine Verbindung zu Protect Cloud herzustellen.
- Die Möglichkeit, den Shavlik Patch-Katalog abzurufen.
- Das Benutzerkonto verfügt über die Rechte **Anmelden als Stapelverarbeitungsauftrag**.
- Das Benutzerkonto ist ein Mitglied der Gruppe **Administratoren** und der Gruppe **WSUS-Administratoren** auf dem WSUS-Server.
- Das WSUS-Signaturzertifikat ist im Speicher für vertrauenswürdigen Stamm und vertrauenswürdigen Herausgeber enthalten und es ist aktuell (nicht abgelaufen).

Sollte einer der Tests fehlschlagen, müssen Sie zunächst das Problem beheben, bevor Sie Shavlik Patch einsetzen.

Registerkarte „Info“

Auf der Registerkarte **Info** werden Informationen zu Produkt- und Katalogversion angezeigt. Außerdem wird angegeben, ob sich die eingesetzte Version dem Ende ihrer Lebensdauer nähert. Diese Registerkarte wird als letzte Registerkarte im Setup-Assistenten angezeigt. Um die Einstellungen zu speichern und den Assistenten zu beenden, klicken Sie auf **Fertig stellen**.

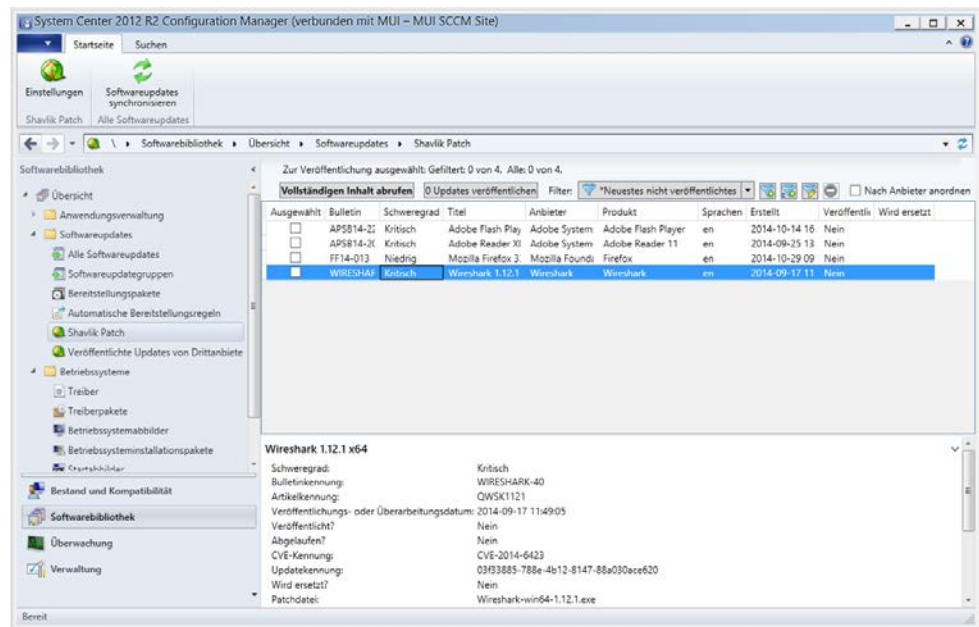
Registerkarte „Planen“

Die Registerkarte **Planen** wird erst angezeigt, nachdem Sie den Setup-Assistenten abgeschlossen und die Einstellungen gespeichert haben. Die Registerkarte wird zur Veröffentlichung von Updates mit einem wiederholten geplanten Task verwendet. Nähere Informationen zu dieser Registerkarte finden Sie im Abschnitt *Automatically Publishing Updates Using a Recurring Scheduled Task*.

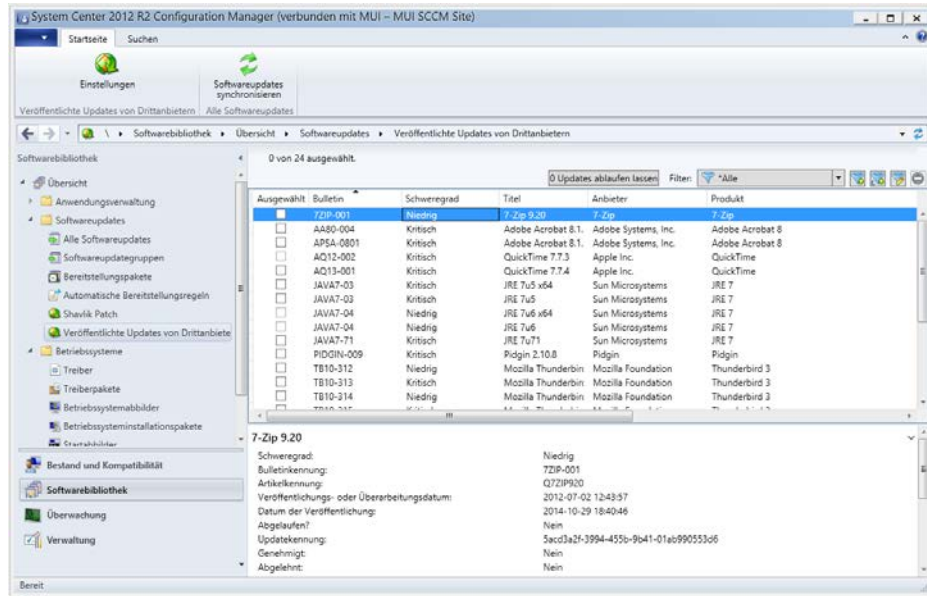
Elemente, die durch das Shavlik Patch Add-in zu Configuration Manager hinzugefügt werden

Bei der Installation des Shavlik Patch Add-ins werden zwei neue Listenelemente zum Ordner **Softwarebibliothek > Softwareupdates** hinzugefügt. Ferner wird bei der Auswahl eines dieser beiden Listenelemente eine Symbolleistenschaltfläche **Einstellungen** zur Registerkarte **Startseite** (Home) in Configuration Manager hinzugefügt.

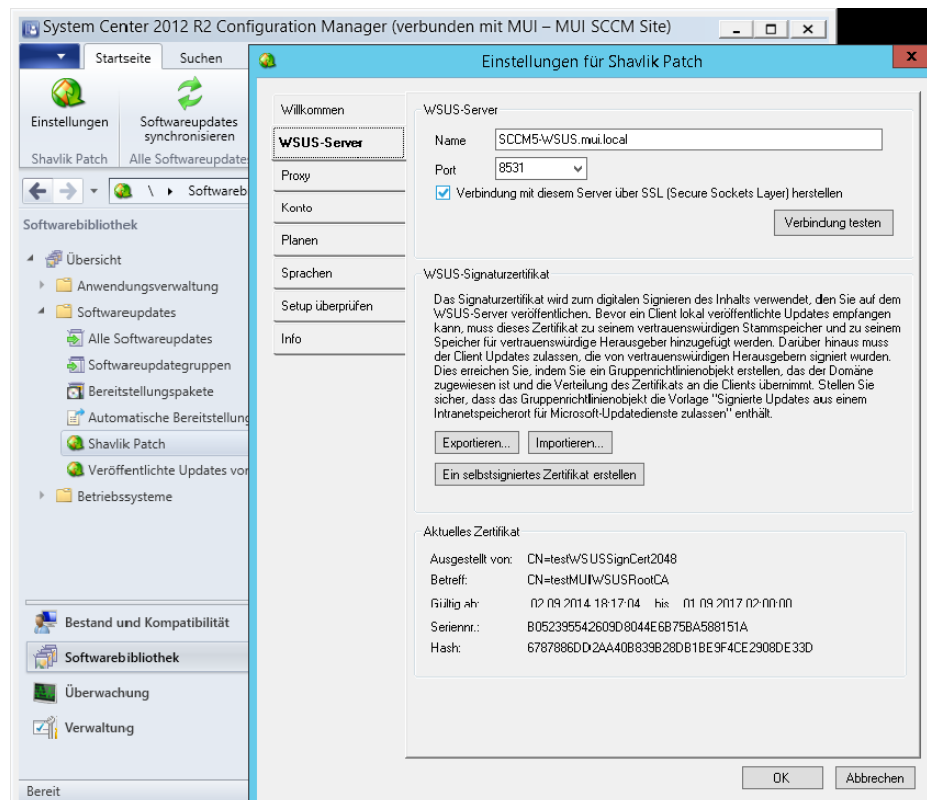
- **Shavlik Patch:** Enthält alle im Shavlik Patch-Katalog verfügbaren Updates. Diese Liste verwenden Sie zum Auffinden und Veröffentlichen von Updates. Mithilfe von Filtern können Sie einschränken, welche Updates angezeigt werden. Weitere Informationen finden Sie unter *Using the Filters*.



- **Veröffentlichte Updates von Drittanbietern:** Enthält alle Updates von Drittanbietern, die in WSUS veröffentlicht wurden. Diese Updates können entweder mit Shavlik Patch oder mit einem anderen Mechanismus veröffentlicht worden sein. Diese Liste verwenden Sie zur Überprüfung und Verwaltung von Updates. Sie werden diese Liste vornehmlich zum Ablaufenlassen von Updates verwenden.



- Einstellungen:** Diese Symbolleistenschaltfläche steht auf der Registerkarte **Startseite** zur Verfügung, wenn **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** ausgewählt wurde. Wenn Sie die Shavlik Patch-Einstellungen ändern müssen oder einen wiederholten Task für die Veröffentlichung planen, klicken Sie auf diese Schaltfläche.



Tip: Sie können dieses Dialogfeld auch öffnen, indem Sie mit der rechten Maustaste auf das Listenelement **Shavlik Patch** klicken.

Die Informationen im Raster

Die Raster **Shavlik Patch** und **Veröffentlichte Updates von Drittanbietern** sind in jeweils zwei Bereiche aufgeteilt. Jeder der Bereiche zeigt spezifische Informationen an und bietet eine ganz spezifische Funktionalität.

- Im oberen Bereich werden alle Updates für das ausgewählte Listenelement angezeigt. Dieser Bereich enthält eine große Anzahl von Spalten, die Übersichtsinformationen zu jedem Update geben. Sie können auch die Updates auswählen, bei denen Sie eine Aktion ausführen möchten.
- Im unteren Bereich werden detaillierte Informationen zu dem im oberen Bereich ausgewählten Update angezeigt. Dieser Bereich ist nicht verfügbar, wenn mehr als ein Update im oberen Bereich ausgewählt wurde.

Die Darstellung der in einem Raster angezeigten Informationen kann auf verschiedene Weise angepasst werden. Sie können:

- Filter zur Suche nach bestimmten Updates anwenden.
- Die Reihenfolge der Spalten ändern, indem Sie auf die Spaltenüberschriften klicken und sie an eine andere Position ziehen.
- Innerhalb einer Spaltenüberschrift klicken, um die Spalten in aufsteigender oder absteigenden Reihenfolge zu sortieren.
- Mit der rechten Maustaste in eine Spaltenüberschrift klicken, um die Größe der Spalten zu ändern und auszuwählen, welche Rasterlinien angezeigt werden sollen. Sie können auch auswählen, welche Spalten im Raster angezeigt werden sollen.

Das **Shavlik Patch**-Raster enthält eine Reihe spezifischer Spalten, anhand derer Sie den Status des jeweiligen Updates ablesen können.

- **Veröffentlicht:** Gibt an, ob das Update für WSUS veröffentlicht wurde.
- **Veröffentlichte Revision:** Dieser Zahlenwert wird jedes Mal um eins erhöht, wenn eine Revision für das Update veröffentlicht wird. Alle veröffentlichten Update weisen einen Zahlenwert größer als Null auf.
- **Überarbeitet:** Gibt an, ob es sich bei dem Update um eine Revision eines zuvor veröffentlichten Updates handelt. Ist dies der Fall, ist das Kontrollkästchen in der Spalte **Ausgewählt** aktiviert. Bei der Veröffentlichung eines solchen Updates wird eine neue Revisionsnummer erstellt und der Zahlenwert für die **Veröffentlichte Revision** erhöht.

Bei einem Revisionsupdate werden lediglich die Metadaten aktualisiert, aber nicht das Updatepaket. Eine Revision wird immer dann für den Shavlik Patch-Katalog bereitgestellt, wenn eine Aktualisierung für Folgendes erforderlich ist:

- die Erkennungslogik, mit der bestimmt wird, ob ein Patch für ein System anwendbar ist und ob er bereits installiert wurde
- einen beliebigen Text im Zusammenhang mit dem Update
- **Sprachen:** Zeigt die verschiedenen Sprachversionen, die für jedes Update verfügbar sind. Sie können im Dialogfeld **Einstellungen für Shavlik Patch** mithilfe der Registerkarte **Sprachen** einschränken, welche Sprachen angezeigt werden. Wenn der Eintrag in der Spalte **Sprachen** leer ist, gilt das Update für alle vom Produkt unterstützten Sprachen.

- **Abgelöst:** Gibt an, ob das Update durch ein anderes Update abgelöst wurde. Ein abgelöstes Update ist nicht das aktuellste verfügbare Update. Zur Anzeige der Ablösungsreihe für ein Update wählen Sie das Update aus. Die abgelösten Informationen werden dann im unteren Fensterbereich angezeigt. Der Standardfilter (***Neueste, nicht veröffentlicht**) zeigt keine abgelösten Updates an, die nicht bereits veröffentlicht wurden. Zur Ansicht aller Updates, einschließlich abgelöster Updates, wählen Sie den Filter ***Alle**.

XML anzeigen

Sie können mit der rechten Maustaste auf ein beliebiges Update im Raster klicken und die XML-Daten anzeigen, die das Update definieren. Sie können die XML-Daten so anzeigen, wie sie im Shavlik Patch-Katalog erscheinen, oder wie sie in veröffentlichter Form auf WSUS erscheinen (nur bei bereits veröffentlichten Updates). Dies ist als Tool zum Debuggen gedacht. Sie werden es normalerweise nicht nutzen müssen.

Verwendung der Filter

Die in den Listen **Shavlik Patch** und **Veröffentlichte Updates von Drittanbietern** angezeigten Informationen können zum Auffinden von spezifischen Updates gefiltert werden. Sie können auch bei der Planung eines wiederholten Tasks einen Filter verwenden.

Vordefinierte Filter

Die vordefinierten Filter sind durch ein vorangestelltes Sternchen gekennzeichnet. Vordefinierte Filter können weder geändert noch gelöscht werden. Zu den vordefinierten Filtern gehören:

Liste der Shavlik Patches

- ***Alle** Alle Updates werden angezeigt.
- ***Neueste, nicht veröffentlicht:** Es werden nur Updates angezeigt, die nicht abgelöst wurden und die nicht in WSUS veröffentlicht wurden. Dies ist der Standardfilter.
- ***Nicht veröffentlicht:** Es werden nur Updates angezeigt, die nicht in WSUS veröffentlicht wurden.
- ***Veröffentlicht:** Es werden nur Updates angezeigt, die in WSUS veröffentlicht wurden.
- ***Geänderte Metadaten:** Es werden nur die Updates angezeigt, die in WSUS veröffentlicht wurden und bei denen Metadaten-Revisionen im aktuellen Katalog vorliegen. Durch das erneute Veröffentlichen dieser Metadaten werden die Metadaten in WSUS aktualisiert.
- ***Ausgewählt:** Es werden nur die Updates angezeigt, die Sie im Raster auswählen. Sie können diesen Filter zur Überprüfung Ihrer Auswahl verwenden, bevor Sie Updates auf WSUS veröffentlichen.

Hinweis: Für Updates mit verschiedenen Paketen für jede Sprache ist ein spezieller Sprachfilter im Shavlik Patch-Raster vorhanden. Dabei werden nur die Updates angezeigt, die für alle Sprachen gelten (bei denen die Spalte **Sprachen** leer ist) und bei denen unter **Sprachen** mindestens eine der im Dialogfeld **Einstellungen** ausgewählten Sprachen eingetragen ist.

Liste der veröffentlichten Updates von Drittanbietern

- ***Alle** Alle Updates werden angezeigt.
- ***Ausgewählt:** Es werden nur die Updates angezeigt, die Sie im Raster auswählen.

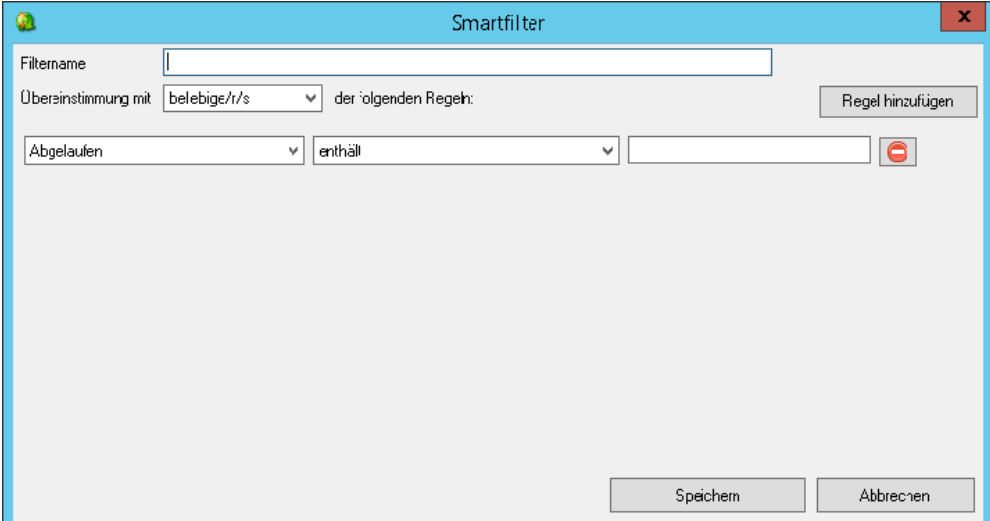
Benutzerdefinierte Filter

Sie können Ihre eigenen benutzerdefinierten Filter erstellen. Mit dem Tool SmartFilter können Sie genau angeben, welche Updates angezeigt werden. Jeder benutzerdefinierte Filter umfasst eine oder mehrere Regeln. Sie können in einem Filter so viele Regeln definieren, wie Sie benötigen.

So erstellen Sie einen neuen Filter:

1. Klicken Sie auf das Symbol „Neuer Filter“ ()

Das Dialogfeld **Smartfilter** wird angezeigt.



2. Geben Sie einen Namen für den Filter ein.
3. Geben Sie an, für welche Regeln im Filter eine Übereinstimmung gegeben sein muss.
 - **Alle:** Nur diejenigen Updates werden angezeigt, die allen Regeln im Filter entsprechen.
 - **Beliebige:** Alle Updates, die mindestens einer der Regeln im Filter entsprechen, werden angezeigt.
4. Definieren Sie eine oder mehrere Regeln.

Um eine Regel zu definieren, wählen Sie in jedem der ersten beiden Logikfelder eine Option aus und geben dann im dritten Feld das Kriterium ein. Um eine weitere Regel hinzuzufügen, klicken Sie einfach auf **Regel hinzufügen**.

Hinweis: Wenn Sie eine Regel definieren, die keinen Sinn macht (zum Beispiel: „Bulletin ist kleiner als 3“), dann wird die Regel ignoriert.

5. Klicken Sie auf **Speichern**.

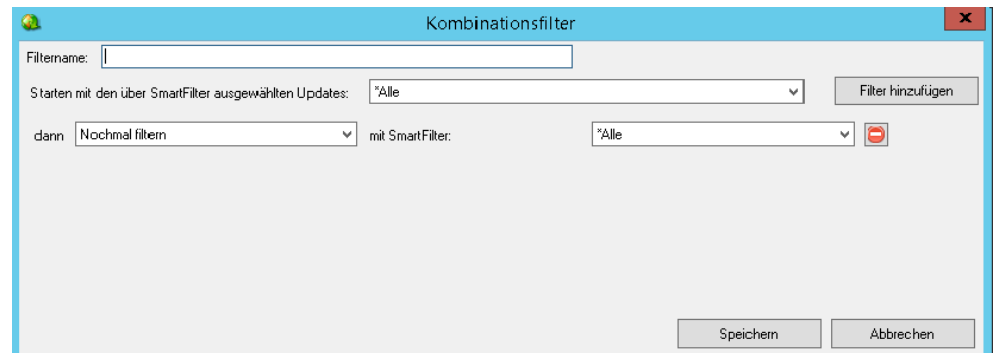
Zusammengesetzte Filter

Shavlik Patch bietet die Möglichkeit, zusammengesetzte Filter zu definieren. Ein zusammengesetzter Filter besteht aus mindestens zwei Filtern, die verknüpft sind und nacheinander ausgeführt werden. Mit dieser erweiterten Filterfunktion können Sie die Suche nach Updates innerhalb eines Rasters mehrfach einschränken oder erweitern, indem Sie zwei oder mehrere Filter automatisch hintereinander ausführen. Sie können Suchvorgänge mit **ODER**- und **UND**-Logik durchführen.

So erstellen Sie einen neuen zusammengesetzten Filter:

1. Klicken Sie auf das Symbol „Neuer zusammengesetzter Filter“ ()

Das Dialogfeld **Zusammengesetzter Filter** wird angezeigt.



2. Geben Sie einen Namen für den zusammengesetzten Filter ein.
3. Wählen Sie einen Startfilter.
4. Fügen Sie eine oder mehrere Filterebenen hinzu.

Zur Definition einer Ebene wählen Sie eine Aktion (**Hinzufügen**, **Entfernen** oder **Erneut filtern**) und dann den zusätzlichen Filter, den Sie anwenden möchten. Um eine weitere Ebene hinzuzufügen, klicken Sie einfach auf **Filter hinzufügen**.

5. Klicken Sie auf **Speichern**.

VORGEHENSWEISE BEIM VERÖFFENTLICHEN VON UPDATES

Manuelles Veröffentlichen von Updates von Drittanbietern

Sie können ein oder mehrere Updates von Drittanbietern veröffentlichen. Die Veröffentlichung von Updates kann entweder sofort oder zu einem bestimmten Zeitpunkt in der Zukunft erfolgen. Zur Planung der Veröffentlichung kommt die Microsoft Aufgabenplanung (Task Scheduler) zum Einsatz. Die Veröffentlichung wird stets als separater Task ausgeführt, doch die Ausführung kann überwacht werden.

1. Erweitern Sie im Arbeitsbereich **Softwarebibliothek** von Configuration Manager den Ordner **Softwareupdates** und klicken Sie auf **Shavlik Patch**.
2. Aktivieren Sie das Kontrollkästchen **Ausgewählt** für jedes Update, das Sie veröffentlichen möchten.

Das Kontrollkästchen **Ausgewählt** wird deaktiviert, wenn die neueste Revision des Updates bereits veröffentlicht oder kürzlich zur Veröffentlichung geplant wurde.

Die gewünschten Updates können Sie wie folgt finden:

- Verwenden Sie einen Filter.
 - Verwenden Sie das Kontrollkästchen **Nach Anbieter anordnen**.
 - Sortieren Sie die Spalten, indem Sie auf die Spaltenköpfe klicken.
3. Klicken Sie auf **n Updates veröffentlichen** (wobei n die Anzahl der ausgewählten Updates angibt).

Das Dialogfeld **Ausgewählte Updates veröffentlichen** wird angezeigt.

Ausgewählte Updates veröffentlichen

Jetzt

Einmal: Montag, 3. November 2014 16:06:08

Zur geplanten Zeit:

Alle Metadatenupdates im Katalog akzeptieren

Nach der Veröffentlichung der ausgewählten Updates synchronisieren

Planen der Ausführung des Tasks als:

Angemeldeter Benutzer Anderer Benutzer

Benutzer: MUJ\scdm.de

Kennwort:

Wenn eine Proxyauthentifizierung erforderlich ist, werden die Anmeldeinformationen in den Proxyeinstellungen verwendet.

[Bei einigen der ausgewählten Updates kann unter Umständen keine Synchronisierung durchgeführt werden. Klicken Sie hier, um Einzelheiten anzuzeigen.](#)

OK Abbrechen

4. Geben Sie an, wann und wie das bzw. die Updates veröffentlicht werden sollen.
- **Jetzt:** Der Veröffentlichungsprozess beginnt, sobald Sie auf **OK** klicken.
 - **Einmal:** Planen Sie den Veröffentlichungsprozess für einen bestimmten Zeitpunkt in der Zukunft.
 - **Akzeptieren Sie alle Metadaten-Updates im Katalog:** Aktivieren Sie dieses Kontrollkästchen für eine automatische WSUS-Aktualisierung mit allen Metadaten-Revisionen, die für zuvor veröffentlichte Updates vorhanden sind.
 - **Nach der Veröffentlichung der ausgewählten Updates synchronisieren:** Wenn Configuration Manager im Rahmen dieses Tasks automatisch eine Synchronisierung mit der WSUS-Datenbank vornehmen soll, aktivieren Sie dieses Kontrollkästchen. Hierdurch wird eine inkrementelle Synchronisierung veranlasst. Wenn Sie dieses Kontrollkästchen nicht aktivieren, steht bzw. stehen das bzw. die veröffentlichte(n) Update(s) erst zur Bereitstellung zur Verfügung, wenn der regelmäßige, geplante Synchronisierungsprozess stattfindet. Die Synchronisierung kann auch gestartet werden, indem Sie auf der Registerkarte **Startseite** (Home) auf **Softwareupdates synchronisieren** klicken.
 - **Angemeldeter Benutzer:** Wenn diese Option aktiviert ist, verwenden Sie die Anmeldeinformationen des aktuell angemeldeten Benutzers, um den Veröffentlichungstask zu Microsoft Planer hinzuzufügen. Das Feld **Benutzer** wird automatisch gefüllt. Sie brauchen also nur das Kontokennwort einzugeben.
 - **Anderer Benutzer:** Wenn diese Option aktiviert ist, verwenden Sie ein anderes Benutzerkonto, um den Veröffentlichungstask zu Microsoft Planer

hinzuzufügen. Sie könnten beispielsweise ein Dienstkonto angeben, dessen Kennwort nie abläuft.

Das Konto muss:

- Über die Rechte **Anmelden als Stapelverarbeitungsauftrag** verfügen
- Ein Mitglied der Gruppe „WSUS-Administratoren“ auf dem WSUS-Server sein
- Ein Mitglied der lokalen Administratorengruppe auf dem WSUS-Server sein, wenn der WSUS-Server remote ist

Bei der Angabe eines anderen Benutzers müssen Sie festlegen, ob die Anmeldeinformationen für die Authentifizierung bei einem Proxyserver erforderlich sind.

- **Proxyauthentifizierung ist erforderlich - Verwenden Sie diese Anmeldeinformationen:** Wenn diese Option aktiviert ist, sind bei Verwendung des Benutzerkontos Proxyserver-Anmeldeinformationen erforderlich. Bei der Auswahl von **Wie oben** werden die Anmeldeinformationen des Benutzerkontos als Proxy-Anmeldeinformationen verwendet. Bei der Auswahl **Folgende Anmeldeinformationen** können Sie separate Proxy-Anmeldeinformationen angeben.
- **Benutzername:** Geben Sie den Benutzernamen für ein Konto auf dem Proxyserver ein. Es kann sein, dass Sie dabei als Teil Ihres Benutzernamens auch eine Domäne angeben müssen (beispielsweise: eigeneDomäne\eigener.Name).
- **Kennwort:** Geben Sie das Kennwort für das Proxyserver-Konto ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein.

5. Klicken Sie auf **OK**.

Das Dialogfeld **Hinweis** wird angezeigt.

6. Während des Prozesses der Veröffentlichung zeigt die Spalte **Veröffentlicht** den Status **Geplant** an.
7. Wenn das Update erfolgreich veröffentlicht wurde, ändert sich der Status der Spalte **Veröffentlicht** bei der nächsten Aktualisierung in **Ja**.

Beachten Sie, dass das Kontrollkästchen in der Spalte **Ausgewählt** deaktiviert wird, wenn die neueste Revision eines Update veröffentlicht wurde.

Um die Liste der veröffentlichten Updates anzuzeigen, können Sie entweder die Spalte **Veröffentlicht** sortieren oder den Filter ***Veröffentlicht** verwenden.

Automatisches Veröffentlichen von Updates mit einem wiederholten geplanten Task

Sie können Updates in regelmäßigen Abständen automatisch veröffentlichen, indem Sie einen geplanten Task erstellen. Es darf nur jeweils ein geplanter, wiederkehrender Task gleichzeitig vorhanden sein.

1. Erweitern Sie im Arbeitsbereich **Softwarebibliothek** von Configuration Manager den Ordner **Softwareupdates** und klicken Sie auf **Shavlik Patch**.
2. Klicken Sie auf der Registerkarte **Startseite** (Home) auf **Einstellungen** (oder klicken Sie mit der rechten Maustaste auf **Shavlik Patch** und klicken Sie dann auf **Einstellungen**).

Das Dialogfeld **Einstellungen für Shavlik Patch** wird angezeigt.

3. Geben Sie auf der Registerkarte **Planen** an, wann der geplante Task ausgeführt und welche Aktion bzw. welche Aktionen durchgeführt werden sollen.
 - **Download und/oder Veröffentlichung planen:** Geben Sie an, wann der wiederholte Task ausgeführt werden soll.
 - **Die mit diesem Filter ausgewählten Pakete veröffentlichen:** Gibt Ihnen die Möglichkeit, die Updates anzugeben, die periodisch wiederkehrend veröffentlicht werden sollen. Sie können entweder den vordefinierten Filter ***Neueste, nicht veröffentlicht** oder Ihre benutzerdefinierten Filter auswählen.

Beispiel 1: Um alle Updates zu veröffentlichen, die bisher noch nicht veröffentlicht und nicht abgelöst wurden, wählen Sie den Filter ***Neueste, nicht veröffentlicht** aus. Dies ist der einfachste Weg, neue Updates wiederholt zu veröffentlichen.

Beispiel 2: Angenommen, Sie haben zuvor einen benutzerdefinierten Filter erstellt, der alle nicht veröffentlichten kritischen Updates für die in Ihrem Unternehmen verwendeten Produkte identifiziert. Wählen Sie an dieser Stelle einfach diesen Filter aus, um nur diese Updates wiederholt zu veröffentlichen.

Hinweis: Wenn ein Update verschiedene Pakete für verschiedene Sprachen enthält, werden nur die auf der Registerkarte **Sprachen** angegebenen Sprachversionen veröffentlicht.

- **Akzeptieren Sie alle Metadaten-Updates im Katalog:** Aktivieren Sie dieses Kontrollkästchen für eine automatische WSUS-Aktualisierung mit allen Metadaten-Revisionen, die für zuvor veröffentlichte Updates vorhanden sind.
- **Updates synchronisieren:** Wenn Configuration Manager im Rahmen dieses Tasks automatisch eine Synchronisierung mit der WSUS-Datenbank vornehmen soll, aktivieren Sie dieses Kontrollkästchen. Hierdurch wird eine inkrementelle Synchronisierung veranlasst. Wenn Sie dieses Kontrollkästchen nicht aktivieren, stehen die veröffentlichten Updates erst zur Bereitstellung zur Verfügung, wenn der regelmäßige, geplante Synchronisierungsprozess stattfindet. Die Synchronisierung kann auch gestartet werden, indem Sie auf der Registerkarte **Startseite** (Home) auf **Softwareupdates synchronisieren** klicken.
- **Angemeldeter Benutzer:** Wenn diese Option aktiviert ist, verwenden Sie die Anmeldeinformationen des aktuell angemeldeten Benutzers, um den Veröffentlichungstask zu Microsoft Planer hinzuzufügen. Das Feld **Benutzer** wird automatisch gefüllt. Sie brauchen also nur das Kontokennwort einzugeben.
- **Anderer Benutzer:** Wenn diese Option aktiviert ist, verwenden Sie ein anderes Benutzerkonto, um den Veröffentlichungstask zu Microsoft Planer hinzuzufügen. Sie könnten beispielsweise ein Dienstkonto angeben, dessen Kennwort nie abläuft.

Das Konto muss:

- Über die Rechte **Anmelden als Stapelverarbeitungsauftrag** verfügen
- Ein Mitglied der Gruppe „WSUS-Administratoren“ auf dem WSUS-Server sein
- Ein Mitglied der lokalen Administratorengruppe auf dem WSUS-Server sein, wenn der WSUS-Server remote ist

Bei der Angabe eines anderen Benutzers müssen Sie festlegen, ob die Anmeldeinformationen für die Authentifizierung bei einem Proxyserver erforderlich sind.

- **Proxyauthentifizierung ist erforderlich - Verwenden Sie diese**

Anmeldeinformationen: Wenn diese Option aktiviert ist, sind bei Verwendung des Benutzerkontos Proxyserver-Anmeldeinformationen erforderlich. Bei der Auswahl von **Wie oben** werden die Anmeldeinformationen des Benutzerkontos als Proxy-Anmeldeinformationen verwendet. Bei der Auswahl **Folgende Anmeldeinformationen** können Sie separate Proxy-Anmeldeinformationen angeben.

- **Benutzername:** Geben Sie den Benutzernamen für ein Konto auf dem Proxyserver ein. Es kann sein, dass Sie dabei als Teil Ihres Benutzernamens auch eine Domäne angeben müssen (beispielsweise: eigeneDomäne\eigener.Name).
- **Kennwort:** Geben Sie das Kennwort für das Proxyserver-Konto ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein.

Sie können das Shavlik Patch Feature zur automatischen Veröffentlichung in Verbindung mit automatischen Bereitstellungsregeln in Configuration Manager verwenden, um Clients stets mit aktuellen Updates von Drittanbietern auf dem neuesten Stand zu halten.

Anzeigen und Verwalten von geplanten Veröffentlichungen

Mit der Microsoft Aufgabenplanung können Sie die von Ihnen geplanten Veröffentlichungen anzeigen und verwalten. Für den Zugriff auf mit Shavlik Patch geplante Tasks wählen Sie **Start > Administratortools > Aufgabenplanung > Aufgabenplanungsbibliothek > Shavlik Patch**.

- Einmalige Tasks können mit der Microsoft Aufgabenplanung (Task Scheduler) ausgeführt, gelöscht, deaktiviert oder neu geplant werden.
- Wenn Sie einen Zeitplan für wiederholte automatische Veröffentlichung über das Shavlik Patch-Dialogfeld **Einstellungen** ändern, wird der Task automatisch neu geplant.
- Wenn Sie im Dialogfeld **Einstellungen** das Kontrollkästchen **Download und/oder Veröffentlichung planen** deaktivieren und auf **OK** klicken, wird der wiederkehrende Task aus der Microsoft Aufgabenplanung gelöscht.
- Nach Abschluss eines Veröffentlichungstasks wird der Task für weitere ein bis zwei Tage angezeigt.

VORGEHENSWEISE BEIM SYNCHRONISIEREN VON UPDATES FÜR PRODUKTE VON DRITTANBIETERN

System Center Configuration Manager muss ordnungsgemäß konfiguriert werden, um Updates für Produkte von Drittanbietern zu synchronisieren.

1. Erweitern Sie im Arbeitsbereich **Verwaltung** von Configuration Manager den Ordner **Standortkonfiguration** und klicken Sie auf **Standorte**.
2. Klicken Sie mit der rechten Maustaste auf den Standortnamen und wählen Sie dann **Standortkomponenten konfigurieren > Softwareupdatepunkt**.
3. Öffnen Sie im Dialogfeld **Eigenschaften der Softwareupdatepunkt-Komponente** die Registerkarte **Produkte**.
4. Aktivieren Sie die Kontrollkästchen für alle Produkte von Drittanbietern und klicken Sie dann auf **OK**.

Dadurch werden die Produkte angegeben, für die Softwareupdates synchronisiert werden.

Diesen Vorgang müssen Sie jedes Mal wiederholen, wenn Sie ein Update für ein neues Produkt von Drittanbietern veröffentlichen.


ABLAUFENLASSEN VON DRITTANBIETERUPDATES

Sie können Drittanbieterupdates ablaufen lassen, die vom Produktanbieter unwirksam gemacht oder durch anderen Updates abgelöst wurden. Abgelaufene Softwareupdates können nicht bereitgestellt werden. Updates, die Sie als abgelaufen definiert haben, können dann mit dem WSUS-Bereinigungstool gelöscht werden.

So lassen Sie ein Update ablaufen:

1. Erweitern Sie im Configuration Manager-Arbeitsbereich **Softwarebibliothek** den Ordner **Softwareupdates** und klicken Sie auf **Veröffentlichte Updates von Drittanbietern**.
2. Wählen Sie die Update aus, die Sie ablaufen lassen wollen.
3. Klicken Sie auf **n Updates ablaufen lassen** (wobei n die Anzahl der ausgewählten Updates angibt).

So zeigen Sie abgelaufene Updates an:

- Nehmen Sie in der Liste **Veröffentlichte Updates von Drittanbietern** eine Sortierung anhand der Spalte **Abgelaufen** vor. Beachten Sie, dass das Kontrollkästchen in der Spalte **Ausgewählt** deaktiviert wird.
- Innerhalb der Liste **Alle Softwareupdates** werden abgelaufene Updates nach einer Synchronisierung mit dem Symbol „abgelaufen“ () dargestellt.

INFORMATIONEN ZUM SUPPORT

Unterstützte Produkte

Ein vollständige Liste der von Shavlik Patch unterstützten Produkte finden Sie hier:

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

Technische Unterstützung

Sollten Sie im Zusammenhang mit Shavlik Patch technische Unterstützung benötigen, können Sie auf eine der folgenden Supportoptionen zurückgreifen:

- Durchsuchen Sie den Bereich zu Shavlik Patch auf der Shavlik Community-Webseite: <http://community.shavlik.com>. Damit Sie vollen Zugriff auf alle verfügbaren Ressourcen erhalten, müssen Sie ein Mitglied der Community werden.
 - Reichen Sie eine Support-Anforderung unter <http://support.shavlik.com/CaseLogging.aspx> ein.
 - Rufen Sie den Technischen Support unter der Rufnummer +1 866-407-5279 an.
 - Sehen Sie sich die Online-Video-Tutorials unter folgender Adresse an: www.shavlik.com/support/training-videos/patch
-

Meldung zum Ende der Lebensdauer

Wenn sich das Lebensdauerablaufdatum der von Ihnen genutzten Version von Shavlik Patch nähert, wird beim Start von Shavlik Patch eine Meldung **Update verfügbar** angezeigt. Die Meldung enthält Informationen zum Ablaufzeitpunkt der Version und einen Link zum Abrufen der aktuellsten Version. Achten Sie darauf, dass Ihre Version des Produkts nie das Lebensdauerablaufdatum erreicht, weil der Updatekatalog, der die Erkennungs- und Bereitstellungslogik enthält, danach nicht mehr aktualisiert wird.

ANHANG A: ERSTELLEN UND VERTEILEN VON ZERTIFIKATEN

Übersicht

Wenn Sie Shavlik Patch in Verbindung mit Configuration Manager und WSUS zur Veröffentlichung von Drittanbieterupdates verwenden wollen, benötigen Sie ein Codesignaturzertifikat. Folgende Schritte müssen Sie hierzu auszuführen:

1. Erstellen Sie ein Codesignaturzertifikat.
 Sie können dies entweder unter Verwendung einer internen Zertifizierungsstelle oder über Ihren WSUS-Server erledigen.
2. (Bedingt) Wenn Sie eine interne Zertifizierungsstelle zur Erstellung des Codesignaturzertifikats verwenden, müssen Sie das Zertifikat in WSUS importieren. Diesen Schritt können Sie mit Shavlik Patch durchführen.
 Wenn Sie WSUS zur Erstellung des Codesignaturzertifikats verwenden, wird das Zertifikat automatisch in WSUS importiert.
3. Exportieren Sie das Zertifikat.
4. Verteilen Sie das Codesignaturzertifikat an die entsprechenden Zertifikatspeicher auf allen Ihren WSUS-Servern, dezentralen SCCM-Konsolen und an alle Clientcomputer.
 - Zertifikatspeicher für vertrauenswürdige Herausgeber
 - Zertifikatspeicher für vertrauenswürdige Stammzertifizierungsstellen

Dieser Anhang enthält Einzelheiten dazu, wie jede dieser Aufgaben durchgeführt wird.

Referenz

Detaillierte Zertifikatinformationen, die über den Inhalt dieses Anhangs hinausgehen, finden Sie in den folgenden Artikeln.

- Informationen, wie Sie eine Vertrauensstellung zur Unterstützung des Patchings von Drittanbieteranwendungen einrichten, finden Sie hier:
[http://msdn.microsoft.com/en-us/library/bb902479\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/bb902479(v=vs.85).aspx)
- Informationen dazu, warum WSUS in Windows Server 2012 R2 die Generierung von Codesignaturzertifikaten standardmäßig nicht mehr unterstützt und wie Sie dieses Problem umgehen können, finden Sie unter:
<http://blogs.technet.com/b/wsus/archive/2013/08/15/wsus-no-longer-issues-self-signed-certificates.aspx>

Hinweis: Shavlik Patch wird automatisch auf diese Problemlösung zurückgreifen, wenn Sie sich im Dialogfeld **Einstellungen** für die Erstellung eines selbstsignierten Zertifikats entscheiden.

Zertifikatanforderungen

Mindestanforderungen für das Signaturzertifikat:

- Der private Schlüssel muss exportierbar sein.
- Der Schlüssel muss eine Größe von mindestens 2048 aufweisen.
- Das Zertifikat muss ein Codesignaturzertifikat sein.

Erstellen eines Codesignaturzertifikats

Hinweis: Sie können diesen Abschnitt überspringen, wenn bereits ein Codesignaturzertifikat vorliegt.

Ihnen stehen zwei Optionen für die Erstellung eines Codesignaturzertifikats zur Verfügung:

- Verwenden Sie ein Codesignaturzertifikat, das unter Verwendung einer internen Zertifizierungsstelle erstellt wurde.
- Verwenden Sie die Shavlik Patch-Benutzeroberfläche, um die Erstellung eines selbstsignierten Codesignaturzertifikats über WSUS zu veranlassen.

Erstellen eines Codesignaturzertifikats mit einer Zertifizierungsstelle

Die Erstellung eines Zertifikats über eine vertrauenswürdige Zertifizierungsstelle bietet eine Reihe von Vorteilen:

- Verteilung: Wegfall der Notwendigkeit, das Zertifikat an andere Computer in derselben Domäne zu verteilen.
- Verwaltung: Vereinfachung der Verwaltung, da das Zertifikat auf dieselbe Weise verwaltet werden kann, wie andere Zertifikate in Ihrer Umgebung.

Befolgen Sie Ihren normalen Prozess zur Erstellung eines Zertifikats von Ihrer internen Zertifizierungsstelle. Nachdem Sie das Zertifikat erstellt haben, müssen Sie es auf den WSUS-Server schreiben. Sie können hierfür die Funktion **Zertifikat importieren** in Shavlik Patch verwenden. Nähere Informationen finden Sie im Abschnitt *Importieren eines Zertifikats*.

Erstellen eines Codesignaturzertifikats unter Verwendung von Shavlik Patch und WSUS

Hinweis: Ihr Benutzerkonto muss ein Mitglied der Gruppe „WSUS-Administratoren“ sein, um ein Codesignaturzertifikat über die Shavlik Patch-Oberfläche erstellen zu können.

Über die Benutzeroberfläche von Shavlik Patch können Sie WSUS anweisen, ein selbstsigniertes Codesignaturzertifikat für Ihr Unternehmen zu erstellen. Die Erstellung eines Codesignaturzertifikats ist in den Vorgängerversionen von Windows Server 2012 R2 standardmäßig für WSUS aktiviert.

Wichtig! Wenn Sie WSUS auf Windows Server 2012 R2 verwenden, müssen Sie beachten, dass die Funktion zum Erstellen eines selbstsignierten Codesignaturzertifikats verworfen wurde und daher standardmäßig deaktiviert ist. Sie können dies Funktion jedoch wiederherstellen, indem Sie wie im folgenden Artikel beschrieben vorgehen.

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

Wenn Sie ein Codesignaturzertifikat in Shavlik Patch unter Verwendung eines Softwareupdatepunkts (WSUS-Server) unter Windows Server 2012 R2 oder einer neueren Version erstellen, kommt diese Problemumgehung automatisch zur Anwendung.

So erstellen Sie ein selbstsigniertes Codesignaturzertifikat mit WSUS:

1. Erweitern Sie im Arbeitsbereich **Softwarebibliothek** von Configuration Manager den Ordner **Softwareupdates** und klicken Sie auf **Shavlik Patch**.
2. Klicken Sie in Configuration Manager auf der Registerkarte **Startseite** (Home) auf **Einstellungen**.
3. Wählen Sie im Dialogfeld **Einstellungen für Shavlik Patch** die Registerkarte **WSUS-Server**.
4. Klicken Sie auf **Ein selbstsigniertes Zertifikat erstellen**.

Wenn bereits ein Zertifikat vorhanden ist, wird ein Dialogfeld **Warnung** angezeigt. Fahren Sie keinesfalls fort, es sei denn, Sie sind sicher, dass Sie anderes Zertifikat benötigen. Die Warnmeldung erläutert, wie Sie vorgehen müssen, um ein vorhandenes Zertifikat zu ersetzen oder zu löschen.

Wenn Sie auf **OK** klicken, wird ein zweites Dialogfeld **Warnung** angezeigt. Im Dialogfeld sind die Anforderungen für das Zertifikat aufgeführt, das Sie gerade erstellen. Lesen Sie die Information durch und klicken Sie dann auf **OK**.

Das neue Zertifikat wird auf dem WSUS-Server erstellt und bei WSUS registriert. Details zum Zertifikat werden im Bereich **Aktuelles Zertifikat** angezeigt.

Das Zertifikat wird ebenfalls in folgenden Zertifikatspeichern auf der lokalen Configuration Manager-Konsole gespeichert:

- Vertrauenswürdige Stammzertifizierungsstellen
- Vertrauenswürdige Herausgeber

Importieren eines Zertifikats

Dieser Abschnitt ist nur anwendbar, wenn Sie Ihr Codesignaturzertifikat unter Verwendung einer internen Zertifizierungsstelle erstellt haben. Bei Importieren des Zertifikats wird das Zertifikat auf den WSUS-Server und in die entsprechenden Zertifikatspeicher auf Ihren Computern geschrieben. Sie müssen diesen Importvorgang nicht durchführen, wenn Sie WSUS zur Erstellung eines Codesignaturzertifikats verwendet haben, da das Zertifikat in diesem Fall automatisch an die richtigen Speicherorte geschrieben wurde.

Hinweis: Zum Importieren eines Zertifikats muss eine sichere (SSL-)Verbindung zum WSUS-Server vorhanden sein. Dies wird zum Teil durch Aktivieren des Kontrollkästchens **Sichere Verbindung** im Bereich **WSUS-Server** der Registerkarte **WSUS-Server** erreicht. Sie müssen aber auch Ihr IIS für die Verwendung von SSL konfigurieren.

So importieren Sie ein Zertifikat:

1. Erweitern Sie im Arbeitsbereich **Softwarebibliothek** von Configuration Manager den Ordner **Softwareupdates** und klicken Sie auf **Shavlik Patch**.
2. Klicken Sie in Configuration Manager auf der Registerkarte **Startseite** (Home) auf **Einstellungen**.
3. Wählen Sie im Dialogfeld **Einstellungen für Shavlik Patch** die Registerkarte **WSUS-Server**.
4. Klicken Sie auf **Importieren**.
5. Navigieren Sie zur Zertifikatsdatei und klicken Sie auf **OK**.

Die Zertifikatsdatei enthält eine Kopie des privaten Schlüssels und ist an der Dateierweiterung PFX zu erkennen.

Zertifikat exportieren

Der Exportprozess wird zum Exportieren des Zertifikats verwendet, mit dem die an einem zugänglichen Speicherort in Ihrem Netzwerk veröffentlichten Updates signiert werden.

Hinweis: Der Exportprozess exportiert nur das öffentliche Zertifikat; der private Schlüssel wird NICHT exportiert.

1. Erweitern Sie im Arbeitsbereich **Softwarebibliothek** von Configuration Manager den Ordner **Softwareupdates** und klicken Sie auf **Shavlik Patch**.
2. Klicken Sie in Configuration Manager auf der Registerkarte **Startseite** (Home) auf **Einstellungen**.
3. Wählen Sie im Dialogfeld **Einstellungen für Shavlik Patch** die Registerkarte **WSUS-Server**.
4. Klicken Sie auf **Exportieren**.
5. Geben Sie den Speicherort und den Dateinamen an und klicken Sie auf **Speichern**.

Die Datei ist in der Regel eine CER-Datei.

Nachdem Sie das Zertifikat exportiert haben, müssen Sie es an alle WSUS-Server und an Ihre Clientcomputer verteilen. Dies ist notwendig, damit die Computer lokal veröffentlichte Updates erhalten.

Der Verteilungsprozess wird im folgenden Abschnitt beschrieben.

Verteilen des Zertifikats

Sie müssen das Codesignaturzertifikat an aller Server verteilen, auf denen sich die Configuration Manager-Konsole und Ihre WSUS-Konsolen befinden sowie an alle Ihre Clientcomputer. In welche(n) Zertifikatspeicher das Zertifikat kopiert wird, hängt davon ab, wie das Codesignaturzertifikat erstellt wurde.

- Wurde Ihr Codesignaturzertifikat von WSUS erstellt (und ist daher ein selbstsigniertes Codesignaturzertifikat), müssen Sie das Zertifikat auf allen Ihren WSUS-Servern, Ihren dezentralen SCCM-Konsolen und Clientcomputern an folgende Speicherorte kopieren:
 - Zertifikatspeicher für vertrauenswürdige Herausgeber
 - Zertifikatspeicher für vertrauenswürdige Stammzertifizierungsstellen
- Wurde das Codesignaturzertifikat von einer Zertifizierungsstelle ausgegeben, deren Stamm bereits vertrauenswürdig für Ihre Clients ist, müssen Sie das Zertifikat lediglich in den Zertifikatspeicher für vertrauenswürdige Herausgeber kopieren.

Verwendung von Gruppenrichtlinien zur Verteilung des Zertifikats

Eine gängige Methode für die Verteilung des Codesignaturzertifikats an Ihre Server und/oder Clientcomputer besteht in der Verwendung einer Gruppenrichtlinie. Allgemeine Anweisungen, wie Sie diesen Task durchführen, finden Sie unter Schritt 3 im folgenden Artikel:

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

Verwendung von MMC zur Verteilung des Zertifikats

Eine weitere Methode zur Verteilung des Codesignaturzertifikats besteht in der Verwendung von MMC. Dies ist eine einfache Methode zur Verteilung des Zertifikat an eine Handvoll von lokalen Computern. Zur Verteilung des Zertifikats an eine ganze Reihe von Computern, die über das gesamte Unternehmen verteilt sind, könnte sie sich als untauglich erweisen.

1. Starten Sie auf dem Zielcomputer die Microsoft Management Console (MMC).
2. Klicken Sie im Zertifikatspeicher mit der rechten Maustaste auf **Vertrauenswürdige Herausgeber** und wählen Sie dann **Alle Tasks > Importieren**.
3. Klicken Sie im Dialogfeld **Willkommen** auf **Weiter**.
4. Suchen Sie im Dialogfeld **Zu importierende Datei** nach Ihrer Datei für den öffentlichen Schlüssel und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie im Dialogfeld **Zertifikatspeicher** die Option **Alle Zertifikate in folgendem Speicher speichern** und klicken Sie dann auf **Weiter**.
6. Klicken Sie im Dialogfeld **Fertigstellen des Assistenten** auf **Weiter**.
7. Klicken Sie im Dialogfeld zur Bestätigung auf **OK**.
8. (Bedingt) Wenn Sie Ihr Zertifikat mit WSUS erstellt haben, wiederholen Sie die Schritte 2 bis 7, wählen aber dieses Mal in Schritt 2 **Vertrauenswürdige Stammzertifizierungsstellen** aus