Shavlik Patch for Microsoft System Center

Benutzerhandbuch

Zur Verwendung mit Microsoft System Center Configuration Manager 2012

Copyright

Marken

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.
02. Januar 2015	Shavlik Patch 2.1, Rev. A des Handbuchs	Aktualisierung der WSUS-Server-Screenshots zur Darstellung der Verwendung einer SSL-Verbindung.
März 2016	Shavlik Patch 2.2	Aufnahme neuer Funktionen für 2.2, einschließlich der Möglichkeit, Updates zu bearbeiten, nur als Metadaten zu veröffentlichen, Produkte zu verwalten, Updates vorab herunterzuladen usw.

Inhalt

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-in zu einer vorhandenen Configuration Manager 2012 SP1 oder höher Konsole oder einer Configuration Manager 2012 R2 SP1 oder höher Konsole 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 4.6.1 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 veröffentlichen.

  - 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. Außerdem muss der Benutzer dem Sicherheitsbereich **Alle Instanzen der Objekte, die in Beziehung zu den zugewiesenen Sicherheitsrollen stehen** zugewiesen sein. Wenn der WSUS-Server remote ist, muss der Benutzer 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 4.6.1 zu installieren, bevor Sie mit der Installation fortfahren können. 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.

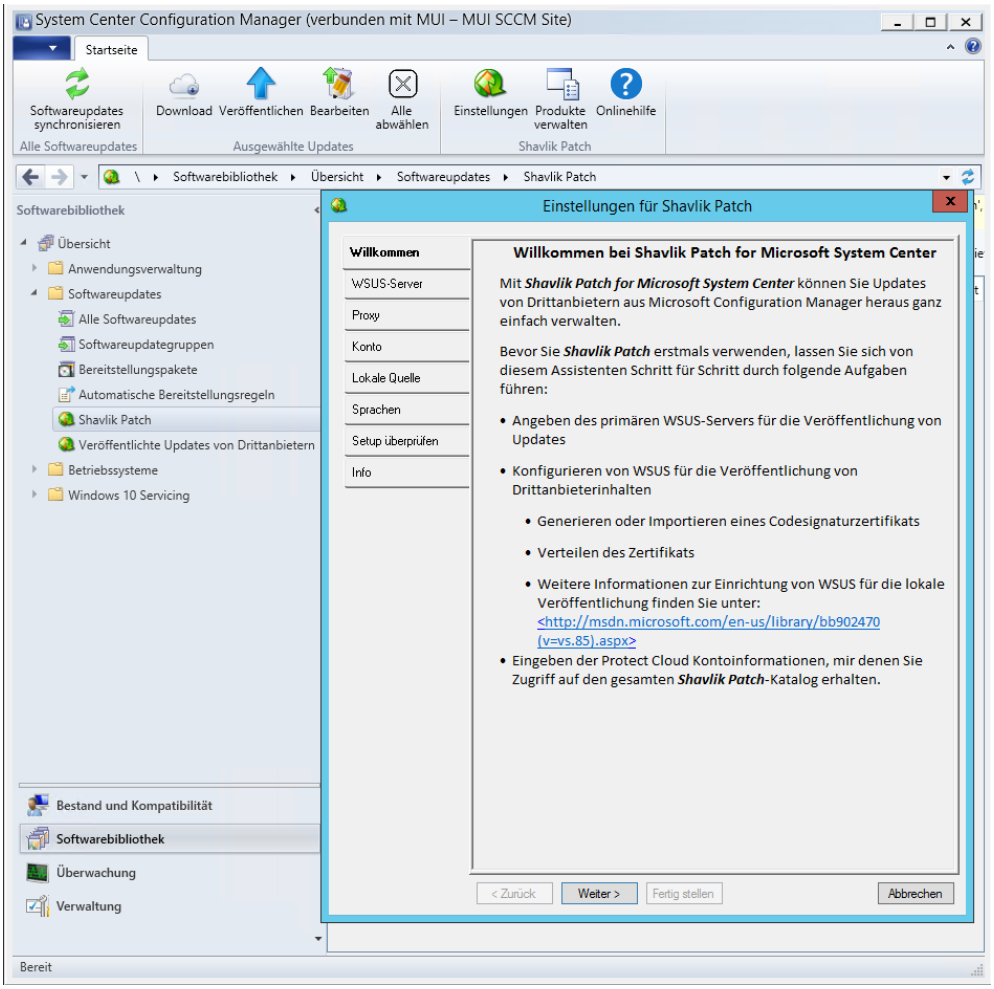
6. Aktivieren Sie das Kontrollkästchen, um die Lizenzvereinbarung zu akzeptieren, und klicken Sie dann auf **Installieren**.

   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.



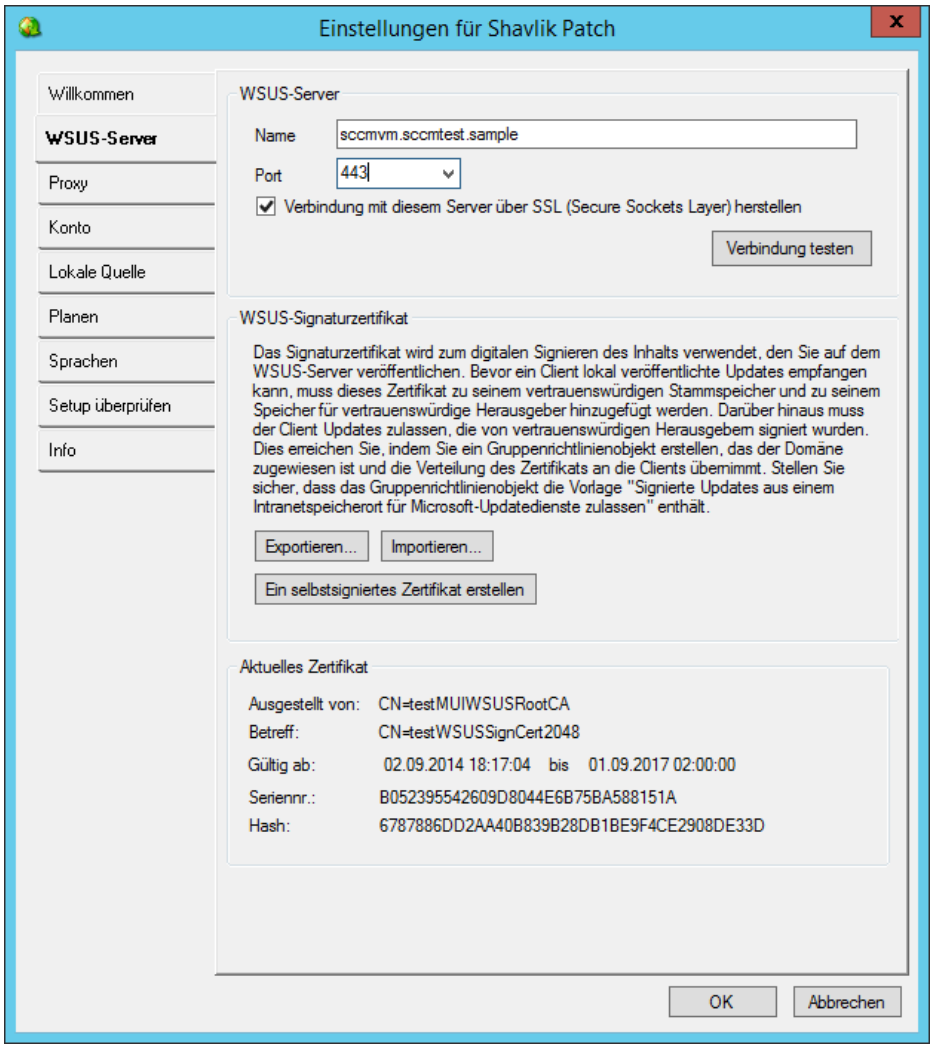
Der Assistent leitet Sie schrittweise durch die Registerkarten für den Einrichtungsvorgang. Shavlik Patch ist sofort nach Abschluss der Einrichtung und dem Speichern der Einstellungen einsatzbereit. Sie können jederzeit zu diesen Einstellungen zurückkehren, indem Sie auf der Registerkarte **Startseite** (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.
- **Secure Sockets Layer (SSL) für die Verbindung mit diesem Server verwenden:** 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:

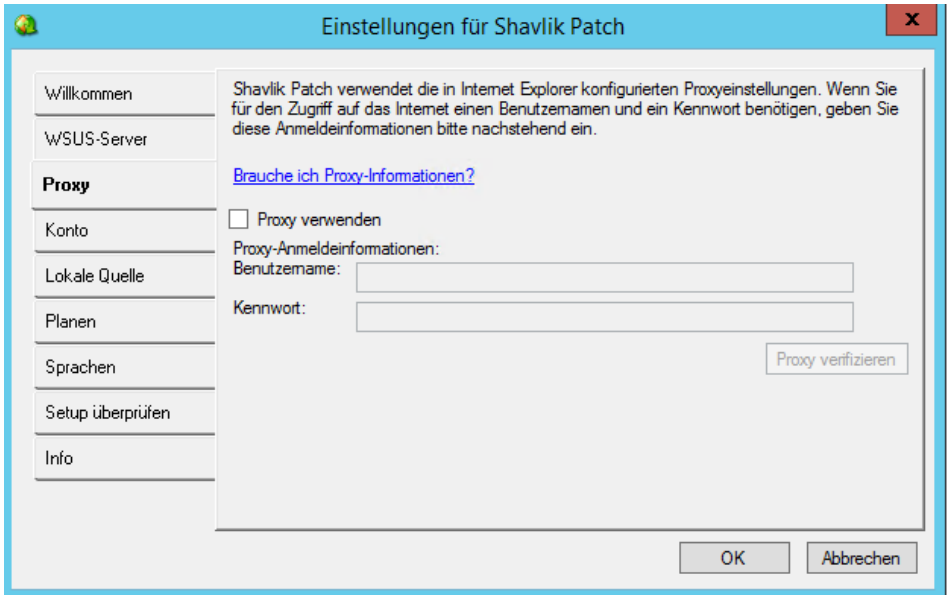
- **Exportieren:** Exportiert das aktuelle Zertifikat aus Shavlik Patch. Aus Sicherheitsgründen wird das Zertifikat ohne den privaten Schlüssel exportiert. Nach dem Exportieren des Zertifikats verteilen Sie es an Ihre Clients und Infrastrukturcomputer (z. B. andere Computer, auf denen das Shavlik Patch 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, Erstellen und Erneuern 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.

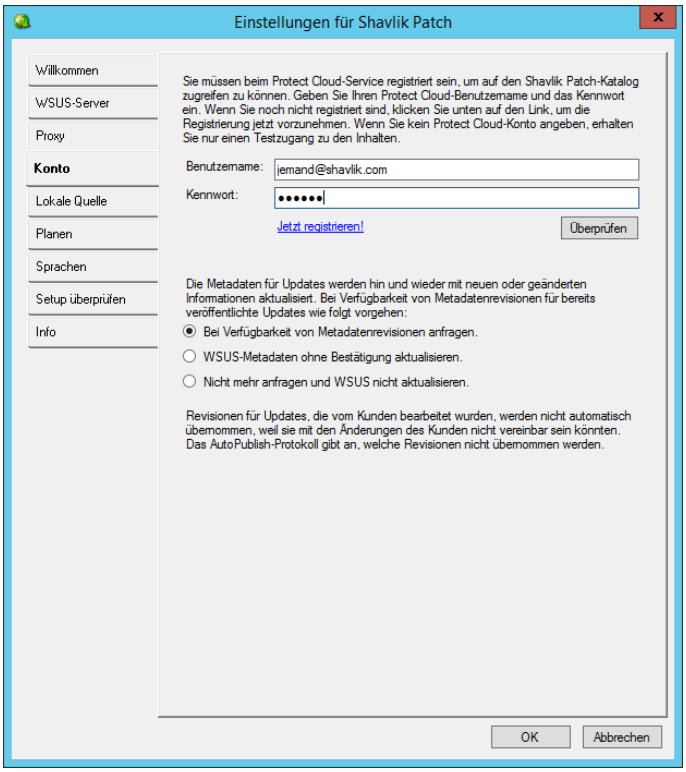


- **Benötige ich Proxyinformationen?**: Um herauszufinden, ob Shavlik Patch Ihre aktuellen Internet Explorer-Proxyeinstellungen für den Zugriff auf das Internet und für andere Vorgänge verwenden kann, klicken Sie auf diese Schaltfläche. Verläuft der Test erfolgreich, sind keine weiteren Schritte erforderlich. 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.
- **Proxy überprüfen**: Klicken Sie auf diese Schaltfläche, um die Anmeldeinformationen für den Proxy 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.**

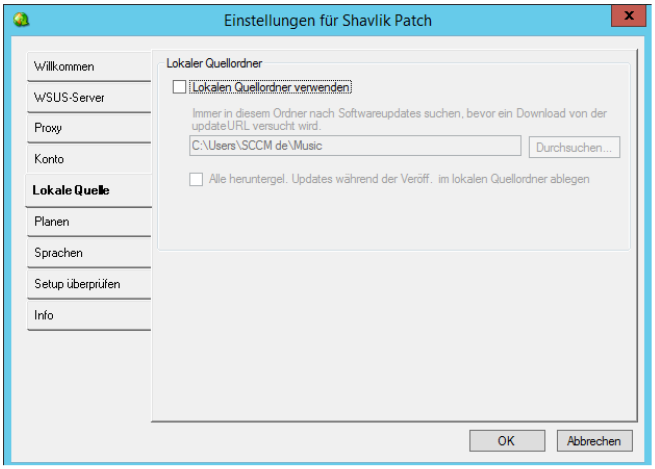
- **WSUS-Metadaten ohne Bestätigung aktualisieren:** Aktualisiert die veröffentlichten Updates automatisch mit den geänderten Metadaten, ohne Sie zu benachrichtigen.

- **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 „Lokale Quelle“

Die Registerkarte **Lokale Quelle** bietet die Möglichkeit, einen lokalen Quellordner zu definieren, in dem die Updates gespeichert werden. Es gibt mehrere Gründe, weshalb Sie diesen Ordner definieren und verwenden würden:

- Sie können Updates vor der Veröffentlichung manuell in diesen Ordner herunterladen. Während der Veröffentlichung werden die Updates aus dem lokalen Ordner abgerufen, anstatt von den Websites-der Hersteller, um den Prozess zu beschleunigen.
- Wenn Sie über ein sicheres, isoliertes Netzwerk verfügen, können Sie Ihre Updates aus einem verbundenen Netzwerk in diesen Ordner herunterladen und die Updates dann in Ihr isoliertes Netzwerk verschieben.
- Sie können ein Archiv mit allen veröffentlichten Updates erstellen.



- **Lokalen Quellordner verwenden:** Bei Aktivierung dieser Option sucht das Programm die Quelldatei bei jedem Versuch einer Updateveröffentlichung zunächst im lokalen Ordner. Wenn sich die Binärdatei im lokalen Quellordner befindet und der Digest verifiziert ist, wird die Binärdatei der veröffentlichten CAB-Datei hinzugefügt. Befindet sich die Binärdatei nicht im lokalen Quellordner, oder ist der Digest nicht verifiziert, dann wird die Updatedatei aus dem Internet heruntergeladen.

- **Immer in diesem Ordner nach Softwareupdates suchen, bevor ein Download von der Update-URL versucht wird:** Geben Sie den vollständigen Pfadnamen zum lokalen Ordner bzw. der Netzwerkfreigabe an, wo die Updatedateien gespeichert werden.

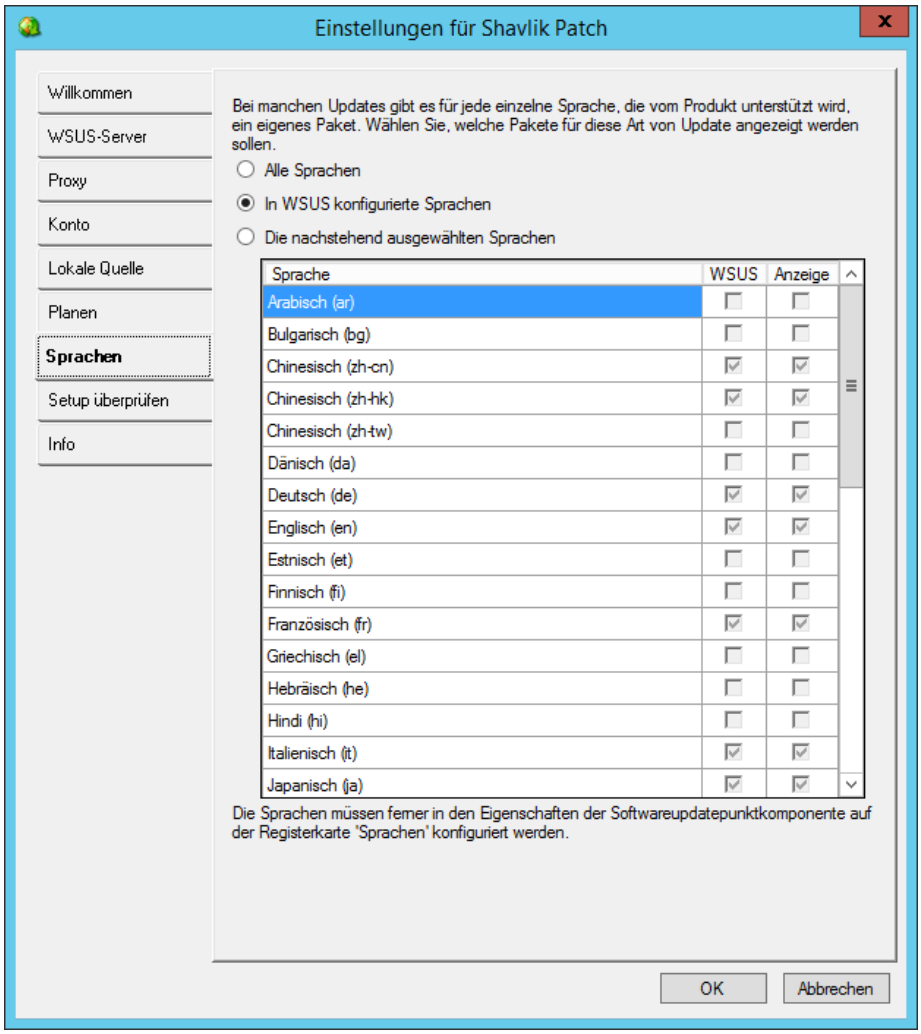
  Für das manuelle Herunterladen eines Updates in den lokalen Quellordner stehen mehrere Möglichkeiten zur Verfügung. Sie können das Update auswählen und anschließend in der Symbolleiste auf die Schaltfläche **Herunterladen** klicken, oder Sie klicken mit der rechten Maustaste auf das Update und wählen **In lokalen Quellordner herunterladen**. Sie können auch auf die Schaltfläche **Download überprüfen** auf der

Registerkarte **Binärdatei** des Update-Editors klicken. Einzelheiten hierzu finden Sie unter *How to Edit Updates* .

- **Alle bei der Veröffentlichung heruntergeladenen Updates im lokalen Quellordner ablegen:** Wenn diese Option aktiviert ist, bedeutet das, dass während der Veröffentlichung jedes Update in diesen Ordner kopiert wird, das sich noch nicht im lokalen Quellordner befindet. Damit können Sie ein komplettes Archiv aller Ihrer veröffentlichten Updates erstellen.

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.

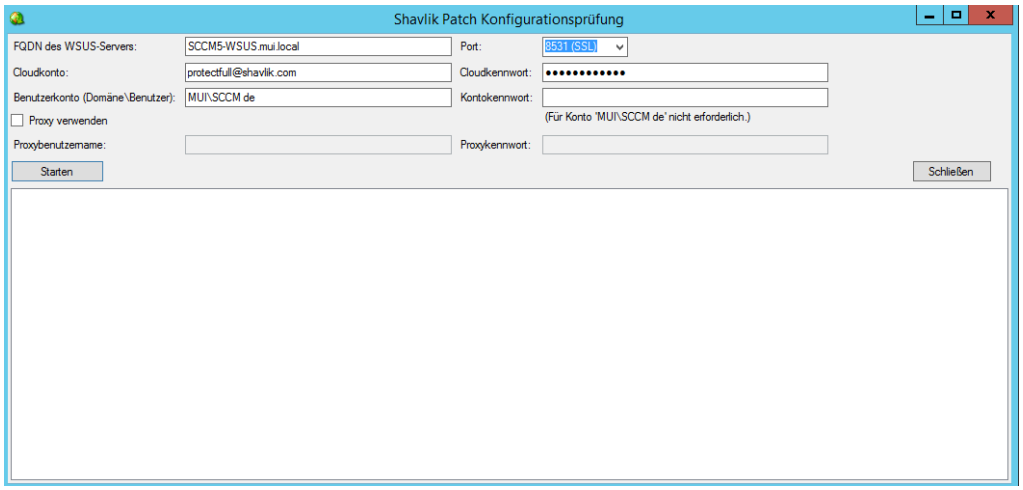


- **Alle Sprachen:** Shavlik Patch zeigt alle verfügbaren Sprachpakete für jedes Update an.
- **In WSUS konfigurierte Sprachen:** Shavlik Patch zeigt nur Pakete für diejenigen Sprachen an, die derzeit zum Download auf dem WSUS-Server konfiguriert sind. Dies ist die Standardeinstellung. (Um die WSUS-Spracheinstellungen 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:\Programmme (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 Domänennamen 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 Domänennamen 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**.

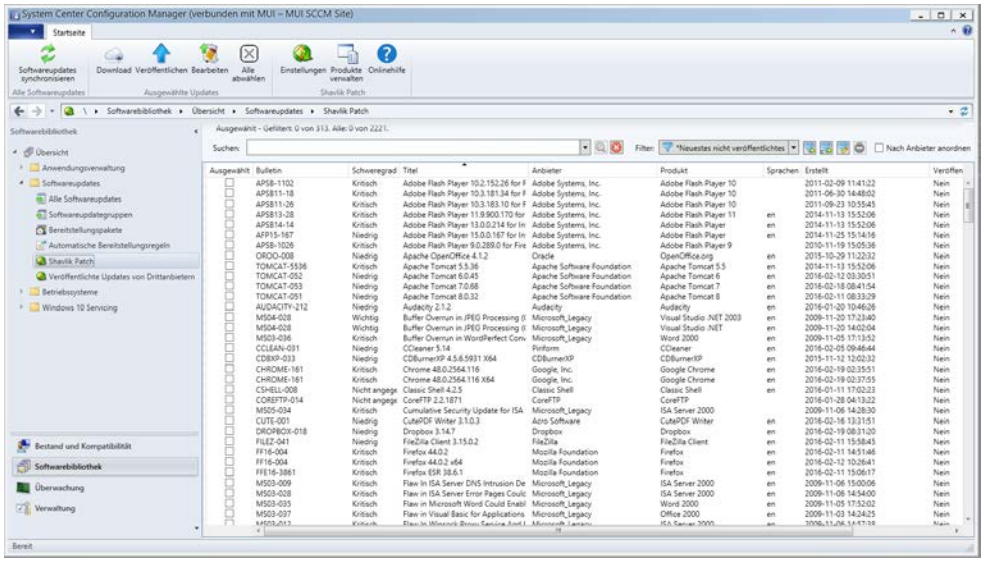
Registerkarte „Planen“

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 *Automatisches Veröffentlichen von Updates mit einem wiederholten geplanten Task*.

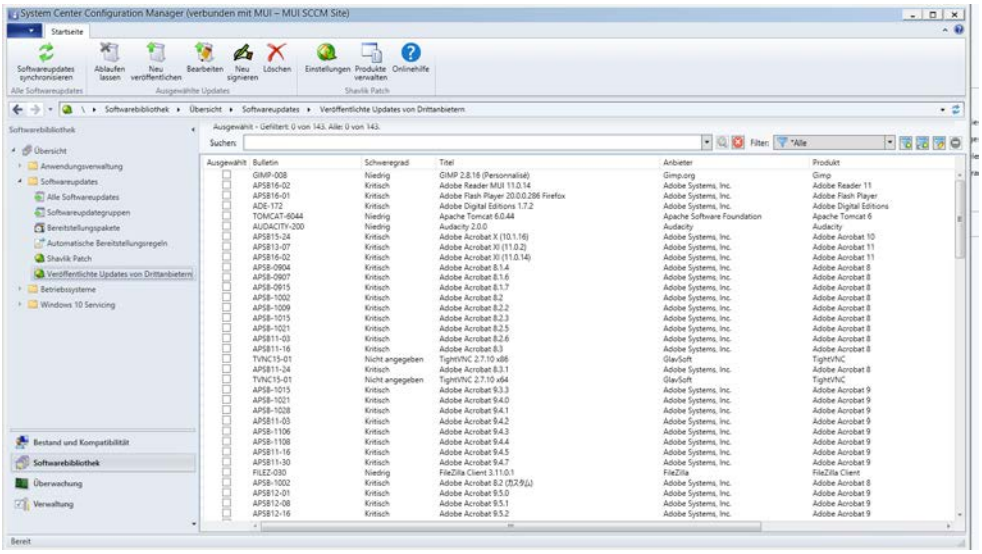
Elemente, die durch das Shavlik Patch Add-in zu Configuration Manager hinzugefügt werden

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 Reihe von Symbolleistenschaltflächen 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 *Verwendung der Filter*.

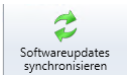


- **Veröffentlichte Updates von Drittanbietern:** Enthält alle Updates von Drittanbietern, die in WSUS veröffentlicht wurden. Diese Updates können entweder mit Shavlik Patch oder mit einem anderen Mechanismus veröffentlicht worden sein. Diese Liste verwenden Sie zur Überprüfung und Verwaltung von Updates.



- **Schaltflächen der Symbolleiste:** Mehrere Symbolleistenschaltflächen stehen auf der Registerkarte **Startseite** zur Verfügung, wenn **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** ausgewählt wurde.

  Sowohl in **Shavlik Patch** als auch in **Veröffentlichte Updates von Drittanbietern:** verfügbar:

	Dient zur Initiierung einer standortweiten Synchronisierung der Softwareupdates. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf das Listenelement **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** klicken.
	Wird verwendet, um die Metadaten eines einzelnen Updates zu ändern und benutzerdefinierte Installationsskripte zu erstellen und dem Update beizufügen. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf ein Update in der Liste **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** klicken.
	Wird verwendet, um Shavlik Patch-Einstellungen zu ändern oder einen wiederholten Task für die Veröffentlichung zu planen. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf das Listenelement **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** klicken.
	Wird verwendet, um anzuzeigen und zu ändern, welche Drittanbieter und Produktkategorien mit dem WSUS-Server synchronisiert werden. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf das Listenelement **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** klicken.
	Wird verwendet, um auf Benutzerdokumentation und Schulungsvideos zuzugreifen, die auf der Shavlik-Website zur Verfügung stehen. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf das Listenelement **Shavlik Patch** oder **Veröffentlichte Updates von Drittanbietern** klicken.

  Ferner verfügbar, wenn **Shavlik Patch** ausgewählt ist:

	Dient zum Herunterladen der ausgewählten Updates in den auf der Registerkarte **Lokale Quelle“** des Dialogfelds **Einstellungen** angegebenen Ordner. Wenn kein lokaler Quellordner angegeben wurde, ist diese Schaltfläche nicht verfügbar. Sie können einen Download auch durchführen, indem Sie in der Liste **Shavlik Patches** mit der rechten Maustaste auf ein Update klicken.
	Wird verwendet, um ein oder mehrere Updates von Drittanbietern zu veröffentlichen.
	Dient zum Deselektieren aller Updates, die derzeit im Raster „Shavlik Patch“ ausgewählt sind. Diese Option ist auch verfügbar, wenn Sie mit der rechten Maustaste auf ein Update in der Liste **Shavlik Patch** klicken.

Ferner verfügbar, wenn **Veröffentlichte Updates von Drittanbietern** ausgewählt ist:

	Wird verwendet, um Updates von Drittanbietern ablaufen zu lassen.
	Wird verwendet, um Updates zu veröffentlichen, die zuvor veröffentlicht wurden. Sie könnten beispielsweise die Vollversion eines Updates veröffentlichen, das zuvor nur als Metadaten veröffentlicht wurde. Dadurch wird immer die unveränderte Version des Updates veröffentlicht, das sich im aktuellen Katalog befindet. Das ist auch dann hilfreich, wenn Sie ein Update ablaufen lassen und es wieder zurückholen möchten.
	Wird verwendet, um Updates neu zu signieren, wenn Ihr Signaturzertifikat sich geändert hat oder erneuert wurde. Einzelheiten hierzu finden Sie unter *How to Re-sign and Deploy Updates After Renewing a Certificate*.
	Wird verwendet, um ein Update von allen Bereitstellungen, Bereitstellungspaketen, Softwareupdategruppen und WSUS zu löschen. Das Update läuft im Rahmen des Löschvorgangs ab.

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 im oberen Teil des Bereichs 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. Lediglich die Spalte **Ausgewählt** kann nicht verschoben werden.
- 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 Updates 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.
- **Nur Metadaten:** Gibt an, ob die Erkennungslogik für das Update veröffentlicht wurde, jedoch nicht die eigentlichen Binärdateien der Software zur Installation des Updates.
- **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**.

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.

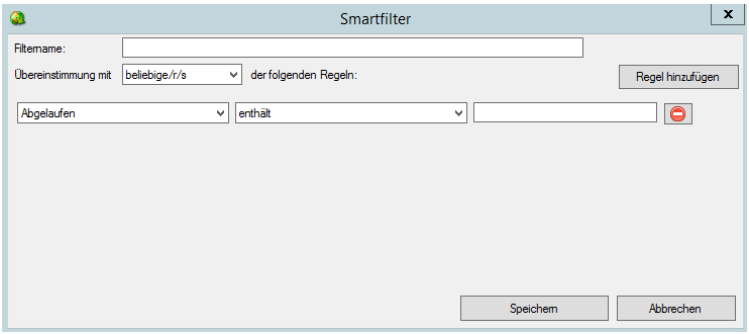
Benutzerdefinierte Filter

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 Smartfilter“ ().

   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**.

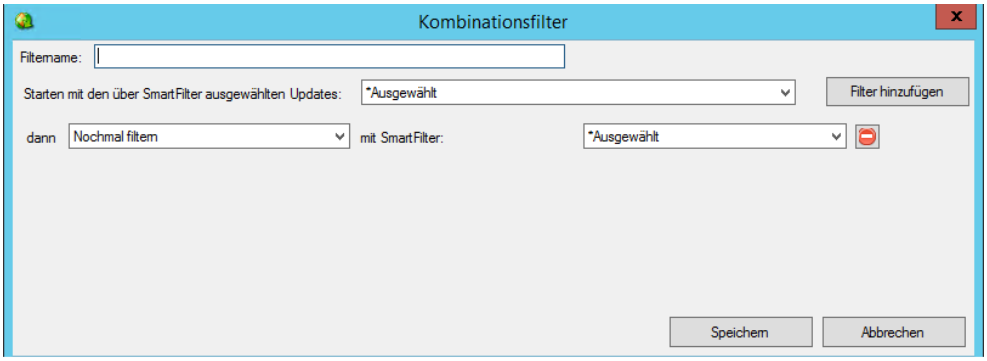
Zusammengesetzte Filter

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**.

Ausführen von Aktionen für den Bereich

Verwenden des Suchtools

Sie können im oberen Bereich einfach und bequem nach Updates suchen. Alle Suchvorgänge werden mit dem Suchtool durchgeführt. Um eine Suche zu starten, geben Sie den zu suchenden Text ein und drücken dann die Eingabetaste oder klicken auf das Suchsymbol (). Es werden nur diejenigen Updates angezeigt, die den Suchkriterien entsprechen; alle anderen Updates sind nicht sichtbar.

Tipps für die Verwendung des Suchtools

- Das Suchtool kann nur auf die Informationen angewendet werden, die derzeit im oberen Bereich sichtbar sind. Sie können mit der rechten Maustaste auf die Spaltenüberschriften klicken, um zu durchsuchende Spalten hinzuzufügen oder zu entfernen.
- Wenn ein Filter zur Anwendung kommt, werden nur die Updates angezeigt, die sowohl den Suchkriterien als auch den Filterkriterien entsprechen
- Alle teilweisen Übereinstimmungen werden angezeigt
- Bei der Suche werden Groß- und Kleinschreibung nicht unterschieden
- Folgende Operatoren stehen zur Verfügung:
    - & (und)
    - | (oder)
    - ^ (nicht)
- Platzhalter dürfen nicht verwendet werden.

XML anzeigen

Sie können mit der rechten Maustaste auf ein beliebiges Update im oberen Bereich 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.

Inhalt kopieren

Sie können den Inhalt im oberen bzw. unteren Bereich in die Zwischenablage Ihres Computers kopieren. Auf diese Weise können Sie beispielsweise Inhalt in eine E-Mail-Nachricht oder ein Tabellenkalkulationsprogramm einfügen.

Inhalte im oberen Bereich kopieren

- **Sichtbare Spalten kopieren:** Für die ausgewählten Updates werden damit die Spaltendaten kopiert, die aktuell im Bereich angezeigt werden.

- **Alle Spalten kopieren:** Für die ausgewählten Updates werden damit alle Spaltendaten kopiert, einschließlich der aktuell nicht im Bereich angezeigten Spalten.

Inhalte im unteren Bereich kopieren

Sie haben eine Vielzahl von Möglichkeiten.

- Alle Spalten kopieren: Klicken Sie mit der rechten Maustaste auf die Bereichsüberschriften und wählen Sie dann **Kopieren** aus.
- Ablösungsinformationen kopieren: Klicken Sie mit der rechten Maustaste auf die Tabelle **Ablösung** und wählen Sie dann **Kopieren** aus.
- Ausgewählte Zeilen kopieren: Wählen Sie die gewünschten Zeilen mithilfe der STRG- bzw. ALT-Taste aus, klicken Sie dann mit der rechten Maustaste und wählen Sie **Kopieren**.
- Eine URL kopieren: Klicken Sie mit der rechten Maustaste auf die URL und wählen Sie dann **Kopieren** aus. Anschließend können Sie die URL direkt in einen Browser einfügen.

Herunterladen eines oder mehrerer Updates in den lokalen Quellordner

Sie können ausgewählte Updates in einen lokalen Quellordner herunterladen. Wenn Sie Updates im Voraus herunterladen, kann dadurch der Veröffentlichungsvorgang beschleunigt werden. Diese Funktion ist auch dann nützlich, wenn Sie eine Möglichkeit suchen, Updates manuell herunterzuladen und dann in ein sicheres, isoliertes Netzwerk zu verschieben. Diese Option ist nur verfügbar, wenn die Option **Lokalen Quellordner verwenden** im Dialogfeld **Einstellungen für Shavlik Patch** aktiviert ist. Einzelheiten zum lokalen Quellordner finden Sie unter *Registerkarte „Lokale Quelle“* auf Seite 13.

Updates bearbeiten

Viele Einzelheiten zu einem Update können Sie entweder vor oder nach der Veröffentlichung bearbeiten. Nähere Informationen finden Sie unter *Vorgehensweise beim Bearbeiten von Updates* auf Seite 38.

Alle Aktualisierungen abwählen

Nutzen Sie diese Option zum Deselektieren aller Updates, die derzeit im Raster „Shavlik Patch“ ausgewählt sind.

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.

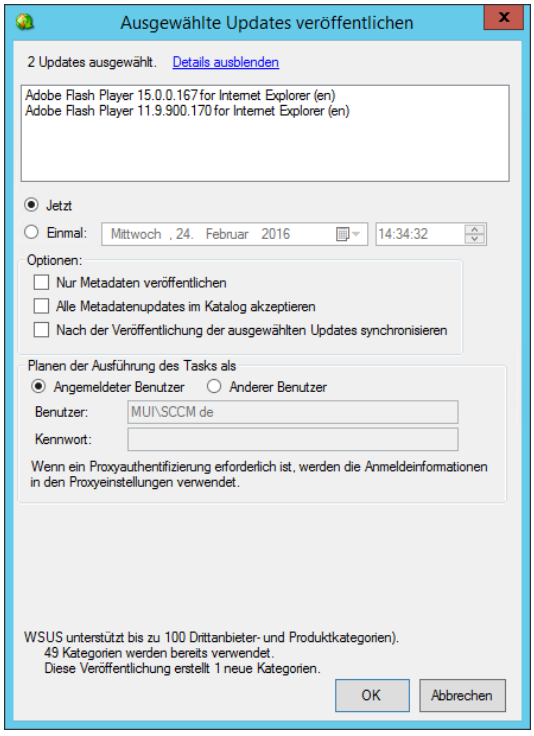
   Das Kontrollkästchen **Ausgewählt** wird deaktiviert, wenn die neueste Revision des Updates bereits veröffentlicht oder kürzlich zur Veröffentlichung geplant wurde.

   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 **Veröffentlichen**.

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



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.
    - **Nur Metadaten veröffentlichen:** Sofern diese Option aktiviert ist, wird die Erkennungslogik für das Update veröffentlicht, jedoch nicht die eigentlichen Binärdateien des Softwareupdates. Diese Option können Sie nutzen, wenn Sie erkennen möchten, ob ein Update von Ihren Clients benötigt wird, dabei aber sicherstellen möchten, dass das Update nicht installiert werden kann. Dies wird nur in sehr spezifischen Situationen und speziellen Serverkonfigurationen genutzt.

      Wenn Sie ein Update bearbeiten, das nur als Metadaten veröffentlicht wurde, wird das ursprüngliche Update gelöscht. Das entsprechende Update wird erneut als reine Metadaten veröffentlicht. Das bedeutet, dass die Revisionsnummer für diese Updates immer 1 ist. Ein Update, das nur als Metadaten veröffentlicht wurde, kann nicht neu signiert werden, weil kein zu signierender Inhalt vorhanden ist. Beim Versuch der Neusignierung wird eine Warnmeldung in die Protokolldatei eingetragen.
    - **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**.

   Eine Statusmeldung gibt an, ob der Veröffentlichungstask erfolgreich geplant wurde.

6. Während des Prozesses der Veröffentlichung zeigt die Spalte **Veröffentlicht** den Status **Geplant** an.

   Möglicherweise müssen Sie auf die Schaltfläche „Aktualisieren“ () klicken, um die Daten im Raster zu aktualisieren.

7. (Optional) Verwenden Sie das Configuration Manager Tool „Ablaufverfolgung“, um die Datei AutoPublish.log zu öffnen und den Veröffentlichungsprozess zu überwachen.

   Das Protokoll in der Datei AutoPublish.log wird bei allen einmaligen oder wiederholten geplanten Jobs fortgeschrieben, die auf WSUS veröffentlicht werden.

8. 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.

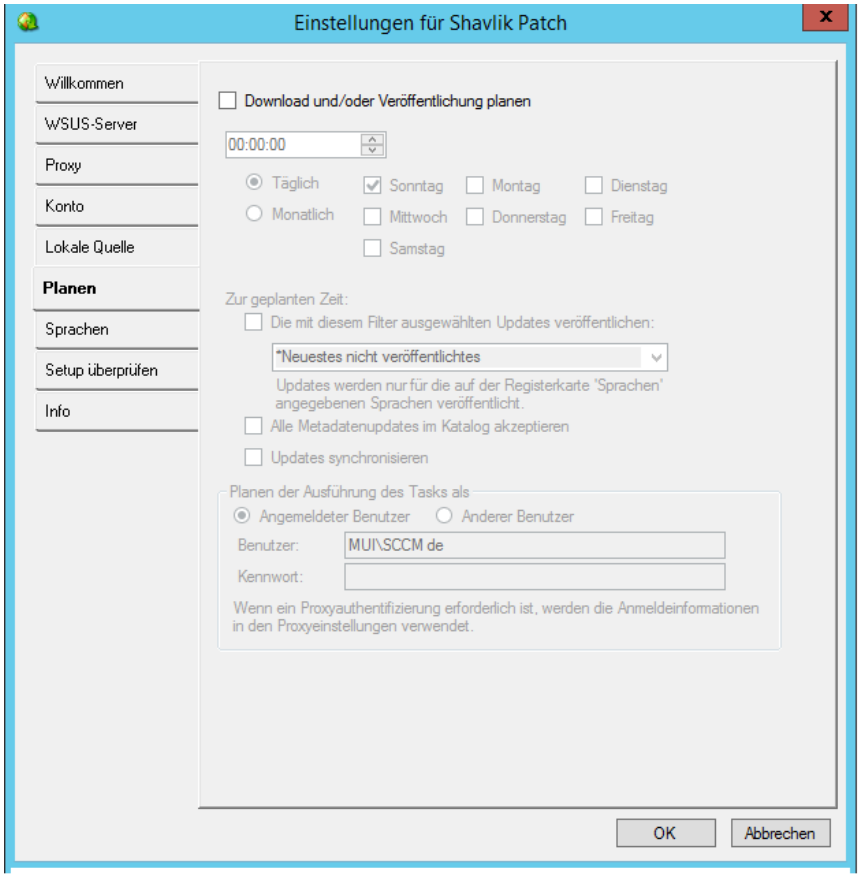
Automatisches Veröffentlichen von Updates mit einem wiederholten geplanten Task

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.

4. (Optional) Verwenden Sie das Configuration Manager Tool „Ablaufverfolgung“, um die Datei AutoPublish.log zu öffnen und den Veröffentlichungsprozess zu überwachen.

   Das Protokoll in der Datei AutoPublish.log wird bei allen einmaligen oder wiederholten geplanten Jobs fortgeschrieben, die auf WSUS veröffentlicht werden.

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.
- Nach Abschuss eines einmaligen Veröffentlichungstasks wird der Task für weitere ein bis zwei Tage angezeigt.
- 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.

VERWALTEN VON PRODUKTEN

Das Dialogfeld **Produkte verwalten** dient mehreren Zwecken. Sie haben folgende Möglichkeiten: Sie können:

- Anzeigen und bearbeiten, welche Drittanbieter und Produktkategorien mit dem WSUS-Server synchronisiert und bereitgestellt werden können
- Wählen Sie die Kategorien aus, die Sie mit Configuration Manager synchronisieren möchten.
- Starten einer Synchronisierung mit WSUS
- Löschen von Produkt- und Anbieterkategorien

Um zu beginnen, klicken Sie auf das Symbol **Produkte verwalten**.

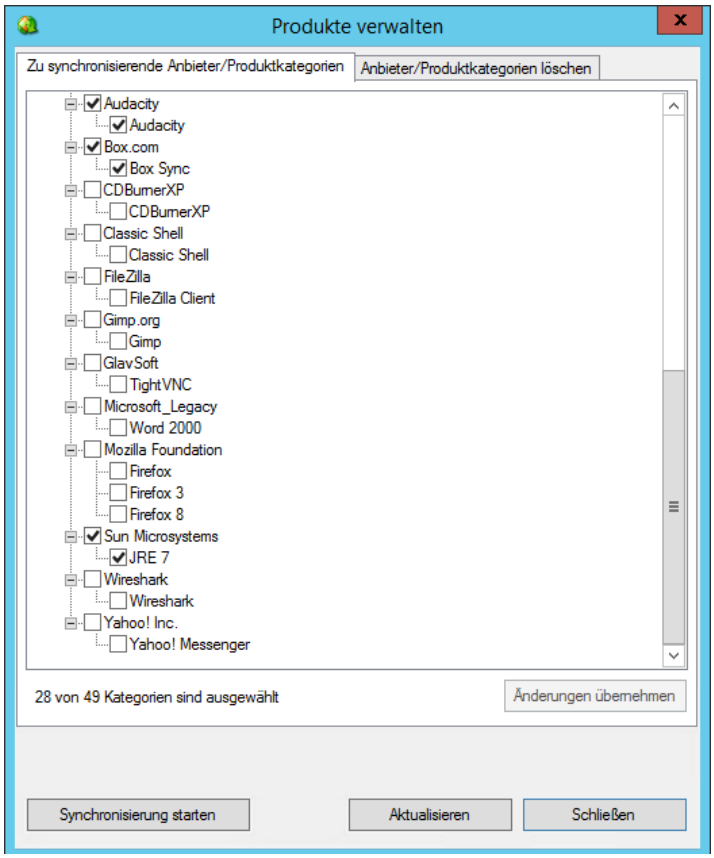
Hinweis: Das Dialogfeld **Produkte verwalten** ähnelt der Registerkarte **Produkte** des Dialogfelds **Softwareupdatepunkt-Komponenteneigenschaften** in Configuration Manager, bietet aber noch zusätzliche Funktionen.

Zu synchronisierende Anbieter/Produktkategorien

Um anzuzeigen, welche Drittanbieter und Produkte veröffentlicht wurden und welche derzeit mit WSUS synchronisiert werden, öffnen Sie die Registerkarte **Zu synchronisierende Anbieter/Produktkategorien**. Diese Registerkarte ist wichtig für die Überwachung und Verwaltung. Bei jeder Veröffentlichung eines Updates für ein neues Drittanbieterprodukt wird eine neue Kategorie angelegt. Sie müssen jede neue Anbieter- bzw. Produktkategorie genehmigen, wenn Updates in dieser Kategorie synchronisiert werden sollen.

Außerdem unterstützt WSUS nur bis zu 100 Drittanbieterkategorien. Sie sollten möglicherweise die Anzahl der unterstützten Kategorien überwachen und sicherstellen, dass dieser Grenzwert nicht überschritten wird. Jeder Anbieter belegt eine Kategorie, und jedes Anbieterprodukt belegt eine weitere Kategorie. Wenn Sie das Limit von 100 Kategorien erreichen, schlagen Updateveröffentlichungen für weitere Drittanbieterprodukte fehl.

Tipp: Die Anzahl der derzeit genutzten Drittanbieterkategorien wird unten im Dialogfeld **Produkte verwalten** und im Dialogfeld **Ausgewählte Updates veröffentlichen** angezeigt.



Sie können jede der Kategorien in der Liste abonnieren bzw. das Abonnement aufheben.

- Wenn eine Kategorie in der Liste vorhanden ist, bedeutet das, dass ein Update für ein Produkt in dieser Kategorie veröffentlicht wurde und eine Synchronisierung mit WSUS stattgefunden hat. Es bedeutet auch, dass die Kategorie als eine der 100 von WSUS unterstützten Drittanbieter- und Produktkategorien gezählt wird.

- Ist das Kontrollkästchen einer Kategorie aktiviert, wird sie mit WSUS synchronisiert. Eine Produktkategorie kann erst dann bereitgestellt werden, wenn Sie die Kategorie genehmigt und die Synchronisierung mit dem Configuration Manager durchgeführt haben.

- Ist das Kontrollkästchen einer Kategorie deaktiviert, wird sie nicht mit WSUS synchronisiert, und die Produktkategorie kann nicht bereitgestellt werden.

- Wenn eine Kategorie rot dargestellt wird, bedeutet das, dass nach der letzten Synchronisierung mit WSUS ein Update für ein Produkt in dieser Kategorie veröffentlicht wurde. Rot dargestellte Kategorien stehen nicht zur Auswahl, bis entweder ein Configuration Manager-Hintergrundtask die Änderung erkennt (normalerweise einmal pro Stunde) oder eine Synchronisierung mit WSUS durchgeführt wird.

Um zu ändern, welche Kategorien in der Liste mit WSUS synchronisiert werden, aktivieren bzw. deaktivieren Sie die Kontrollkästchen und klicken dann auf

Änderungen übernehmen. In einem Bestätigungsdialogfeld werden Sie darüber informiert, dass die Änderungen durchgeführt wurden. Sie erhalten dabei auch die Möglichkeit, eine Synchronisierung mit WSUS durchzuführen. Sie können veröffentlichte Updates für neu ausgewählte Kategorien erst dann bereitstellen, wenn eine Synchronisierung stattfindet.

Hinweis: Wenn Sie ein Kontrollkästchen deaktivieren und dann eine Synchronisierung durchführen, wird kein Element aus der WSUS-Liste der 100 Drittanbieterkategorien entfernt. Zum Entfernen müssen Sie die Kategorien durch Löschen aller Updates in dieser Kategorie löschen.

Anbieter/ Produktkategorien löschen

Um eine oder mehrere Kategorien aus der Liste zu löschen, öffnen Sie die Registerkarte **Anbieter/Produktkategorien** Tab. Es ist ratsam, eine Kategorie zu löschen, wenn Sie ein Produkt in Ihrer Umgebung nicht mehr weiter unterstützen, oder wenn die Updates in einer Kategorie nicht mehr für die von Ihnen unterstützten Produktversionen gelten. Standardmäßig ist keines der Kontrollkästchen auf dieser Registerkarte aktiviert.

Hinweis: Zum Löschen von Kategorien muss der Benutzer, der Shavlik Patch ausführt, über vollständige Administratorrechte verfügen, und ihm muss der Sicherheitsbereich **Alle Instanzen der Objekte, die in Beziehung zu den zu den zugewiesenen Sicherheitsrollen stehen** zugewiesen sein.

So löschen Sie eine Produkt- oder Anbieterkategorie:

1. Aktivieren Sie die entsprechenden Kontrollkästchen.
2. Klicken Sie auf **Kategorien löschen**.

   Es wird ein Bestätigungsdialogfeld angezeigt.
3. Durch Klicken auf **Ja** bestätigen Sie den Löschvorgang. Um den Vorgang abzubrechen, klicken Sie auf **Nein**.

Beim Löschen einer Produktkategorie geschieht Folgendes:

- Alle veröffentlichten Updates für dieses Produkt werden als abgelaufen eingestuft
- Die Updates werden aus allen Bereitstellungen und Bereitstellungspaketen in Configuration Manager entfernt
- Die Updates werden aus allen Softwareupdategruppen in Configuration Manager entfernt
- Die Updates werden aus WSUS gelöscht

Wenn Sie alle Produkte für einen Anbieter löschen, wird die Anbieterkategorie ebenfalls gelöscht.

Der Löschvorgang wird durch einen separaten Hintergrundprozess durchgeführt, der sofort beginnt. Der Vorgang wird auch dann fortgesetzt, wenn Sie Shavlik Patch beenden. Sobald die Updates gelöscht werden, werden sie aus der Liste **Veröffentlichte Updates von Drittanbietern** entfernt. Im Configuration Manager-

Tool „Ablaufverfolgung“ können Sie die Datei AutoPublish.log öffnen, um den Fortschritt des Vorgangs zu überwachen.

Der neue Status der Updates wird erst in SCM in der Liste **Alle Softwareupdates** angezeigt, nachdem die nächste Synchronisierung durchgeführt wurde. Nach einer Synchronisierung werden die Updates als abgelaufen angezeigt und können nicht mehr bereitgestellt werden. Die Updates bleiben einige Tage lang in der Liste **Alle Softwareupdates** stehen, bis sie von einem SCCM-Hintergrundtask entfernt werden.

Hinweis: Damit eine gelöschte Produktkategorie wieder im Dialogfeld **Produkte verwalten** angezeigt wird, müssen Sie mindestens ein Update für dieses Produkt veröffentlichen. Siehe *Vorgehensweise beim Veröffentlichen von Updates*.

Ausführen von Aktionen im Dialogfeld „Produkte verwalten“

Mit den Schaltflächen am unteren Rand des Dialogfelds können Sie die folgenden Aktionen ausführen.

- **Synchronisierung starten:** Startet eine Synchronisierung mit WSUS. Wenn keine Änderungen an den zu synchronisierenden Kategorien vorgenommen wurden, wird eine inkrementelle Synchronisierung durchgeführt. Falls Sie Änderungen an der Kategorieauswahl vorgenommen haben, macht Configuration Manager daraus automatisch eine vollständige Synchronisierung. Sie sollten dies nicht während der Stoßzeiten durchführen, weil es ein aufwändiger Vorgang ist, wenn viele veröffentlichte Updates vorliegen.

  Diese Schaltfläche hat dieselbe Funktion wie die Symbolleistenschaltfläche **Softwareupdates synchronisieren**. Wenn Sie die Synchronisierung mit dieser Schaltfläche starten, hat das den Vorteil, dass der Status der Synchronisierung solange angezeigt wird, wie das Dialogfeld geöffnet ist. Sie können das Dialogfeld geöffnet lassen und den Configuration Manager weiter nutzen. Um das Dialogfeld in den Vordergrund zu bringen, klicken Sie in der Taskleiste auf das Shavlik-Symbol oder in der Symbolleiste auf die Schaltfläche **Produkte verwalten**.

  Das Initiieren einer Synchronisierung ist auch eine Möglichkeit, neue Produktkategorien auswählbar zu machen. Neue Kategorien werden in der Kategorieliste rot dargestellt und stehen erst dann zur Auswahl, wenn eine Synchronisierung stattfindet oder ein Configuration Manager-Hintergrundtask die Änderung erkennt.

- **Aktualisieren:** Aktualisiert die Informationen des Dialogfelds.

- **Schließen:** Schließt das Dialogfeld.

ABLAUFENLASSEN VON DRITTANBIETERUPDATES

Sie können Drittanbieterupdates ablaufen lassen, die vom Produktanbieter unwirksam gemacht oder durch andere 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 Updates aus, die Sie ablaufen lassen wollen.
3. Klicken Sie auf **ablaufen lassen**.

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 Kontrollkästen in der Spalte **Ausgewählt** deaktiviert wird.
- Innerhalb der Liste **Alle Softwareupdates** werden abgelaufene Updates nach einer Synchronisierung mit dem Symbol „abgelaufen“ () dargestellt.

VORGEHENSWEISE BEIM BEARBEITEN VON UPDATES

Shavlik Patch bietet die Möglichkeit, ein einzelnes Update zu bearbeiten. Erfahrene Benutzer können die Metadaten eines Updates ändern und Befehle für vor bzw. nach der Installation eingeben. Sie können ein Update entweder vor oder nach der Veröffentlichung bearbeiten.

Warnung! Ein Update zu bearbeiten kann riskant sein, und das Bearbeitungstool ist nicht für jeden Benutzer vorgesehen. Nur qualifizierte Administratoren sollten versuchen, ein Update zu ändern.

Die möglichen Änderungen an Updates lassen sich in zwei Haupttypen einteilen:

- **Änderungen an den reinen Metadaten des Updates:** Änderungen, die auf einer der Registerkarten des Editors außer der Registerkarte **Benutzerdefiniertes Installationsskript** vorgenommen wurden, verändern nur die Metadaten eines Updates. Durch das Ändern der Metadaten wird keine neue Installationsdatei oder Update-ID erstellt. Nachdem Sie die Änderungen vorgenommen haben, wird - falls das Update zuvor veröffentlicht wurde - eine Revision an den WSUS-Server gesendet. Falls Sie das Update zuvor bereitgestellt haben, ist nach dem Bearbeiten der Metadaten keine Änderung der Bereitstellungen erforderlich. Die Clientcomputer, auf denen das Update nicht installiert ist, erhalten die aktualisierten Metadaten.

- **Änderungen an der Installationsdatei:** Alle auf der Registerkarte **Benutzerdefiniertes Installationsskript** vorgenommenen Änderungen führen dazu, dass ein neues Update generiert wird, welches das bearbeitete Update ersetzt. Nachdem das neue Update veröffentlicht wurde, müssen Sie es bereitstellen, damit die Clients die Änderungen erhalten.

Updates können entweder über das Listenelement **Shavlik Patch** oder über das Listenelement **Veröffentlichte Updates von Drittanbietern** bearbeitet werden.

- Updates in der Liste **Shavlik Patch** können sowohl bereits veröffentlicht als auch nicht veröffentlicht worden sein. Wird von dieser Stelle aus auf ein Update zugegriffen, ist der Startpunkt für das Update immer das aktuelle Katalogupdate. Wurde ein Update nur mit Metadatenänderungen bearbeitet und veröffentlicht, werden Sie benachrichtigt. Diese Änderungen werden nicht im Editor angezeigt.

- Wenn Sie den Editor zum Öffnen eines Updates in der Liste **Veröffentlichte Updates von Drittanbietern** verwenden, sind alle zuvor vorgenommenen Änderungen verfügbar.

- Falls Sie versuchen, ein Update zu bearbeiten, das durch ein anderes veröffentlichtes Update abgelöst wurde (z. B. ein Update, das durch Veröffentlichung des Updates mit benutzerdefinierten Skripts erzeugt wurde), können Sie lediglich die Metadaten des Updates bearbeiten. Die Steuerelemente auf der Registerkarte **Benutzerdefiniertes Installationsskript** sind deaktiviert.

So öffnen Sie den Update-Editor: Markieren Sie das spezifische Update, das Sie ändern möchten, und klicken Sie dann auf die Schaltfläche **Bearbeiten** in der Symbolleiste, oder klicken Sie mit der rechten Maustaste auf das Update und wählen Sie **Bearbeiten**.

Tipps zur Bearbeitung

Mit dem Update-Editor haben Sie folgende Möglichkeiten:

- Informationen eines Updates bearbeiten. Sie können beispielsweise den Titel, die Beschreibung, den Schweregrad usw. eines Updates ändern.
- Befehlszeilenoptionen hinzufügen (sofern zutreffend).
- Die Regeln **Ist installiert** und **Kann installiert werden** bearbeiten.
- Ändern, welche CPU-Architekturen und Betriebssystemsprachen gepatcht werden
- Die Liste abgelöster Updates bearbeiten
- Befehle für vor und nach der Installation hinzufügen. Mit diesen Befehlen können andere Skripte, Eingabedateien oder ausführbare Dateien aufgerufen werden, die Sie zur Verfügung stellen und die ein Bestandteil des Updates werden.

Folgendes ermöglicht Ihnen der Editor nicht:

- Völlig neue Updates erstellen
- Das ursprüngliche binäre Update ersetzen
- Anbieter, Produkte, Bulletin, KB-Artikel, CVE-IDs oder JAVA-IDs ändern
- Beliebige Änderungen an der XLM-Datei des Softwareverteilungspakets vornehmen

Erkennen bearbeiteter Updates

Beim Veröffentlichen eines bearbeiteten Updates werden Titel und Beschreibung des Updates automatisch geändert, um darauf hinzuweisen, dass Änderungen vorgenommen wurden. Falls nur die Metadaten verändert wurden, wird an den Titel der Begriff *(Bearbeitet)* angehängt. Falls ein benutzerdefiniertes Installationsskript hinzugefügt wurde, wird der Begriff *(Benutzerdefiniert)* an den Titel angehängt. In jedem Fall werden die folgenden Elemente an die Beschreibung angehängt: *(Bearbeitet) <Zeitstempel> <Benutzername des Bearbeiters>*.

Speichern der Arbeit

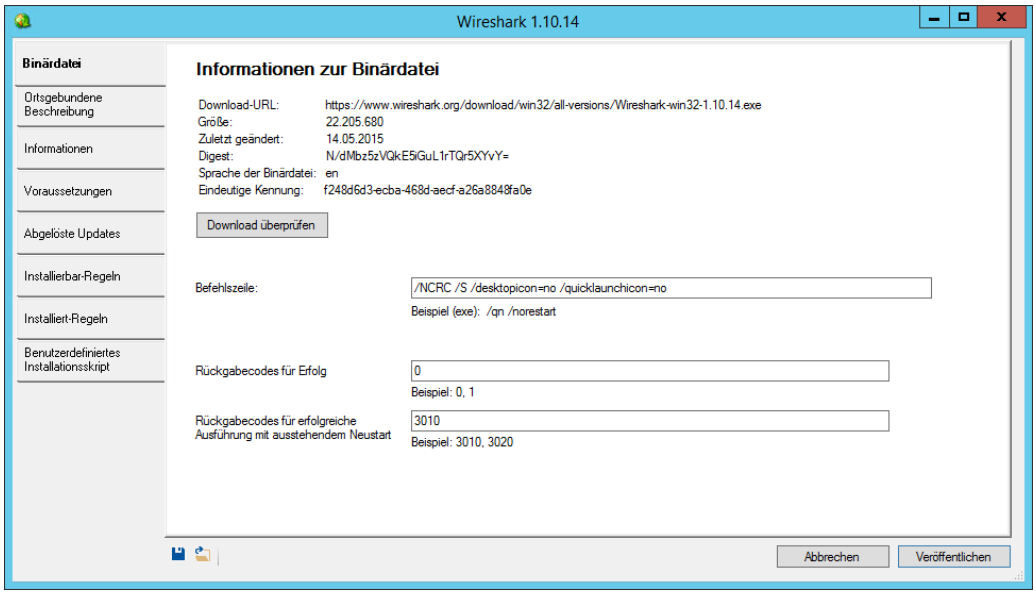
Sie können Ihre Arbeit während des Bearbeitungsvorgangs jederzeit speichern. Es ist ratsam, die Änderungen regelmäßig zu speichern. Auf jeden Fall sollten Sie Ihre Arbeit speichern, wenn Sie den Update-Editor schließen, bevor Sie die Bearbeitung abgeschlossen haben, oder wenn Sie vor der Veröffentlichung der Änderungen noch eine Prüfung vornehmen möchten.

Um Ihre Änderungen zu speichern, klicken Sie auf das Symbol „Speichern“ ( ) und geben dann einen Dateinamen und einen Speicherort für die bearbeitete Datei an. Ihre Änderungen werden vom Programm überprüft und auf Fehler geprüft. Falls Fehler gefunden wurden, können Sie die Datei nicht speichern.

Wenn Sie den Editor beendet haben und Ihre Änderungen abrufen möchten, markieren Sie das richtige Update, starten den Editor und klicken dann auf das Symbol „Öffnen“ (). Suchen Sie die richtige gespeicherte Datei und klicken Sie auf **Öffnen**. Die bearbeitete Version des Updates wird in den Editor geladen. Wenn Sie versehentlich eine bearbeitete Version eines anderen Updates zu laden versuchen, tritt ein Fehler auf.

Bearbeiten der Binärdateidaten

Auf der Registerkarte **Binärdatei** können Sie Informationen zu der Binärdatei des Updates ansehen. Außerdem können Sie prüfen, ob Sie das Update herunterladen können, und Befehlszeilenoptionen sowie Rückgabecodes definieren.



- **Statische Informationen zur Binärdateidatei:** Zeigt Informationen über die Binärdatei. Diese Informationen können nicht geändert werden.
- **Download überprüfen:** Lädt das Update von der angegebenen URL an einem temporären Speicherort herunter und überprüft, ob der Digest auf den Updatecomputern dem Digest in den Metadaten entspricht. Wenn der Digest genehmigt ist und im Dialogfeld **Einstellungen** auf der Registerkarte **Lokale Quelle** ein lokaler Quellordner angegeben wurde, wird das Update auch dorthin kopiert und braucht nicht erneut heruntergeladen zu werden, wenn es veröffentlicht wird. Nach Abschluss des Vorgangs wird die Datei von ihrem temporären Speicherort gelöscht.
- **Befehlszeile:** Gibt Befehlszeilenoptionen an, die bei der Installation des Updates zu verwenden sind. Zum Beispiel könnten Sie Schalter angeben, die ein automatisches Update deaktivieren, oder die dem Update mitteilen, keine Desktop-Verknüpfung zu installieren usw.

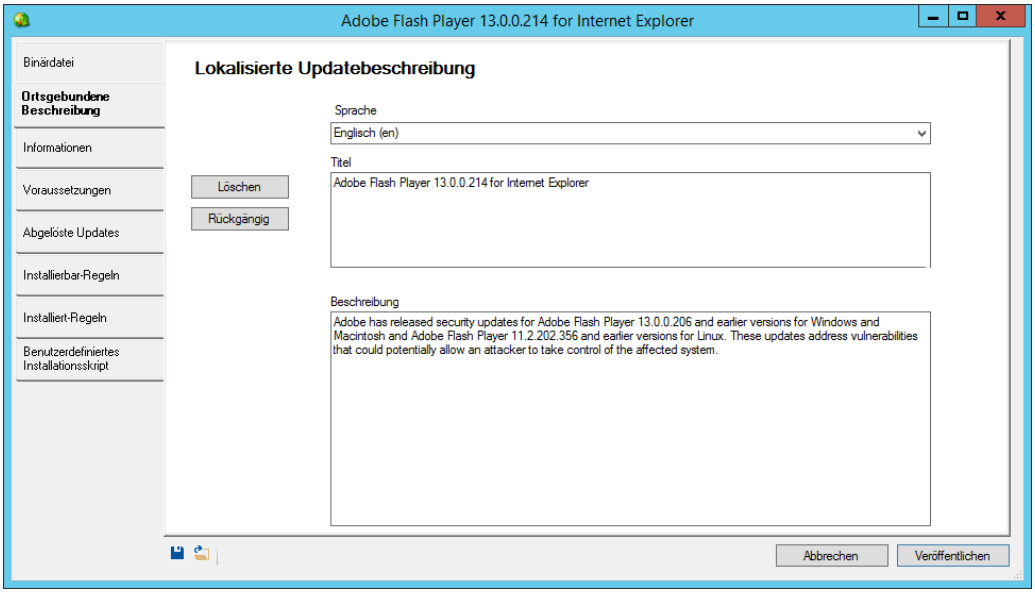
Hinweis: Bei bestimmten Updates wird setup.bat als Befehlszeile angezeigt. In diesem Fall kann keines der Felder auf dieser Registerkarte bearbeitet werden. Dies geschieht dann, wenn bei einem Update im Shavlik Patch-Katalog spezielle, nicht standardmäßige Installationsverfahren erforderlich sind oder ein Update bereits so bearbeitet wurde, dass es ein benutzerdefiniertes

Installationsskript enthält. Bei diesen Updates ist es nicht möglich, die Befehlszeilenoptionen zu ändern.

- **Rückgabecodes für Erfolg:** Gibt die Ganzzahlcodes an, die vom Update zurückgegeben werden, wenn es erfolgreich installiert wurde und kein Neustart erforderlich ist. Diese Box wird bei MSI- bzw. MSP-Updates nicht angezeigt.
- **Rückgabecodes für erfolgreiche Ausführung mit ausstehendem Neustart** Gibt die Ganzzahlcodes an, die vom Update zurückgegeben werden, wenn es erfolgreich installiert wurde, jedoch noch ein Neustart erforderlich ist. Diese Box wird bei MSI- bzw. MSP-Updates nicht angezeigt.

Bearbeiten der lokalisierten Beschreibung

Auf der Registerkarte **Lokalisierte Beschreibung** können Sie den Titel und den Beschreibungstext anzeigen und ändern, der für jedes Update zur Verfügung gestellt wird. Sie können eindeutigen Text für jede der unterstützten Sprachen angeben.

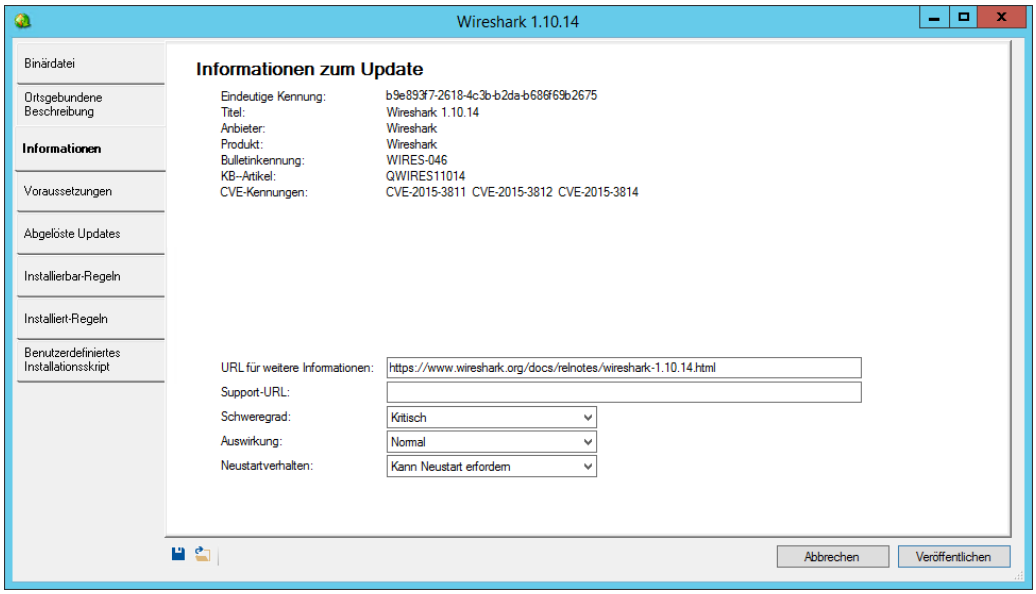


- **Sprache:** Hier können Sie auswählen, welche Sprache Sie anzeigen und ändern möchten. Die Updates im Shavlik Patch-Katalog liefern in der Regel nur englische Titel und Beschreibungen. Wenn Ihre Benutzer nicht mit einer englischen Versionen des Betriebssystems arbeiten, möchten Sie möglicherweise Text in anderen Sprachen bereitzustellen.
- **Löschen:** Entfernt den gesamten Text aus den Feldern **Titel** und **Beschreibung** für die ausgewählte Sprache.
- **Rückgängig:** Stellt den Originaltext für die ausgewählte Sprache wieder her. Wenn Sie zu einer anderen Sprache wechseln, können Sie die an anderen Sprachen von Ihnen vorgenommenen Änderungen nicht mehr rückgängig machen.
- **Titel:** Zeigt den Text, der derzeit als Titel für das Update verwendet wird. Beim Veröffentlichen des Updates wird der Zusatz *(Bearbeitet)* oder *(Benutzerdefiniert)* an den Titel angehängt.

- **Beschreibung:** Zeigt den Text, der derzeit als Beschreibung für das Update verwendet wird. Beim Veröffentlichen des Updates werden die folgenden Elemente an die Beschreibung angehängt: *(Bearbeitet) <Zeitstempel> <Benutzername des Bearbeiters>*.

Information bearbeiten

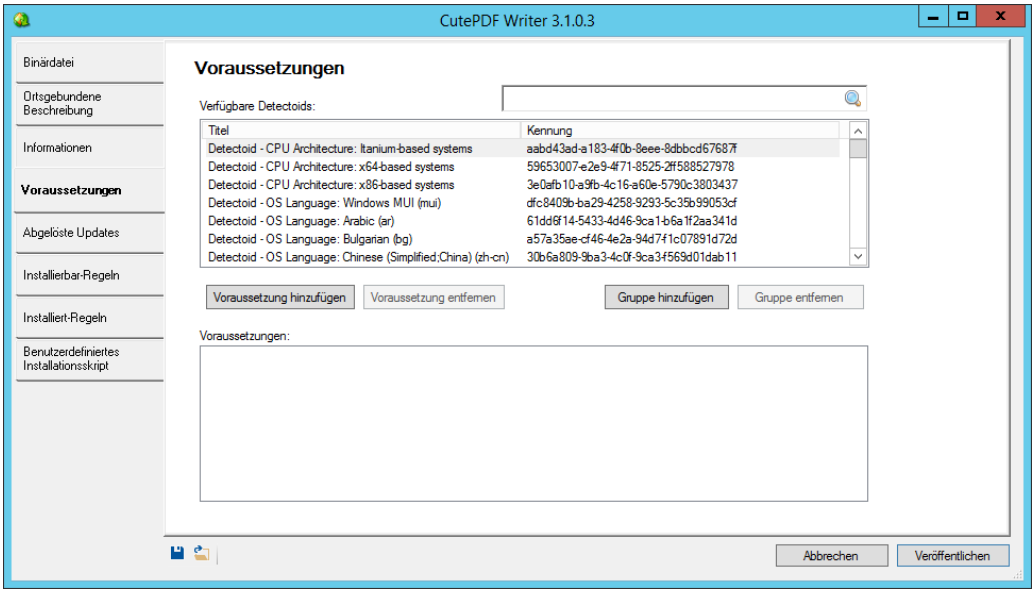
Auf der Registerkarte **Informationen** können Sie die allgemeinen Informationen zum Update anzeigen und ändern.



- **Statische Informationen:** Zeigt allgemeine Informationen über das Update. Diese Informationen können nicht geändert werden.
- **URL für weitere Informationen:** Gibt eine URL an, die Sie besuchen können, und die weitere Informationen über das Update enthält. Dies ist ein Pflichtfeld, und es muss eine gültige URL enthalten.
- **Support-URL:** Gibt die URL-Adresse an, die dann zu verwenden ist, wenn Sie Unterstützung für dieses Update benötigen. Dies ist kein Pflichtfeld. Wenn jedoch eine URL angegeben wird, muss sie eine gültige URL-Syntax aufweisen.
- **Schweregrad:** Ermöglicht es Ihnen, das Update in Abhängigkeit der von Ihnen wahrgenommen Bedrohung einen der fünf folgenden Schweregrade zuzuweisen:
- **Auswirkung:** Dieses Feld hat keine Auswirkung darauf, wie das Update erkannt oder installiert wird; es dient lediglich zur Information.
- **Neustartverhalten:** Dieses Feld hat keine Auswirkung darauf, wie das Update erkannt oder installiert wird; es dient lediglich zur Information.

Bearbeiten der Voraussetzungen

Auf der Registerkarte **Voraussetzungen** können Sie die Voraussetzungen angeben, die erfüllt sein müssen, damit ein Update installiert werden kann.



- **Verfügbare Detectoids:** Ein Detectoid ist eine Regel bzw. Voraussetzung, die bestimmt, ob ein Update installiert werden kann. Für ein einzelnes Update können mehrere Detectoids definiert werden. Diese Liste zeigt die zur Auswahl stehenden Detectoids an. Es gibt zwei Arten von Detectoids: **CPU-Architektur**-Detectoids geben die Computerarchitektur an, die erforderlich ist, und **BS-Sprache**-Detectoids geben Sie die Sprache des Betriebssystems an, die auf dem Zielcomputer erforderlich ist.

  Mithilfe des Suchfelds können Sie ein bestimmtes Detectoid schnell in der Liste finden.

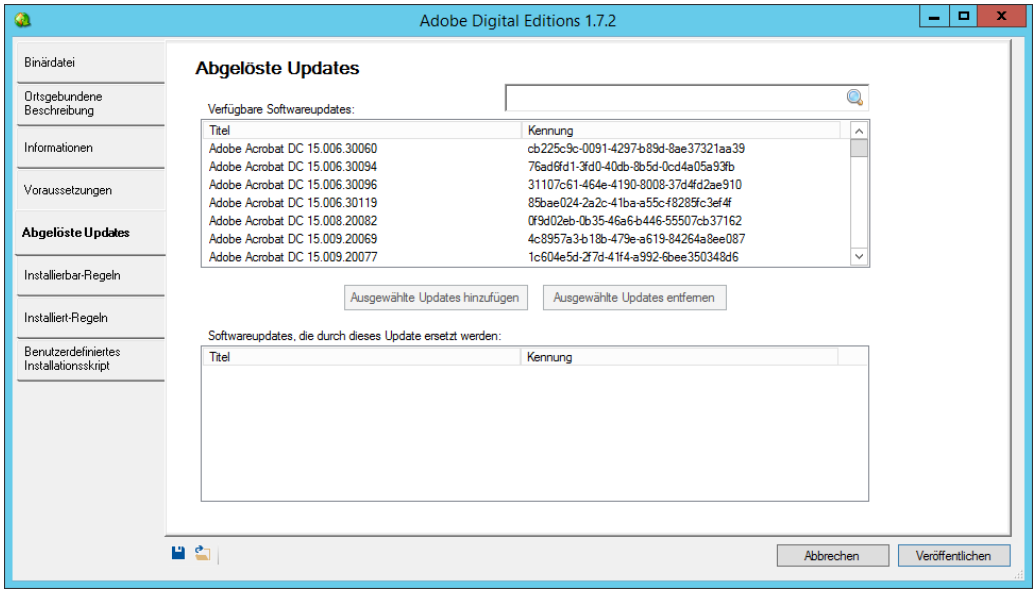
Tipp: Verwenden Sie beim Definieren der Voraussetzungen zuerst die Schaltfläche **Gruppe hinzufügen**, um Ihre Voraussetzungsgruppen zu erstellen, und fügen Sie diesen Gruppen dann mit der Schaltfläche **Voraussetzung hinzufügen** weitere Voraussetzungen hinzu.

- **Voraussetzung hinzufügen**: Fügt die ausgewählten Detectoids zur Liste **Voraussetzungen** hinzu. Die Detectoids werden in die Gruppe aufgenommen, die derzeit in der Liste **Voraussetzungen** ausgewählt ist. Sind keine Gruppen vorhanden, werden die Detectoids als neue Gruppe hinzugefügt.
- **Voraussetzung entfernen:** Entfernt das in der Liste **Voraussetzungen** ausgewählte Detectoid.
- **Gruppe hinzufügen:** Fügt die ausgewählten Detectoids als eine neue Gruppe zur Liste **Voraussetzungen** hinzu. Mithilfe der Schaltfläche **Voraussetzung hinzufügen** können Sie weitere Detectoids in die Gruppe aufnehmen. Damit die Voraussetzungen erfüllt sind, muss mindestens eines der Detectoids in jeder Gruppe erfüllt sein.
- **Gruppe entfernen:** Entfernt die in der Liste **Voraussetzungen** ausgewählte Gruppe.

Bearbeiten abgelöster Updates

Auf der Registerkarte **Abgelöste Updates** können Sie festlegen, welche Updates durch dieses Update abgelöst werden sollen. Ein abgelöstes Update ist nicht das aktuellste verfügbare Update.

Tipp: Zur Anzeige der vollständigen Ablösungsreihe für ein Update wählen Sie das Update im Bereich **Shavlik Patch** aus. Die abgelösten Informationen werden dann im unteren Fensterbereich angezeigt.



- **Verfügbare Softwareupdates:** In dieser Liste werden alle Updates im Shavlik Patch-Katalog angezeigt, die vom Anbieter des bearbeiteten Updates bereitgestellt wurden. Außerdem enthält die Liste benutzerdefinierte Updates für diesen Anbieter, die zuvor mithilfe des Update-Editors erstellt wurden.

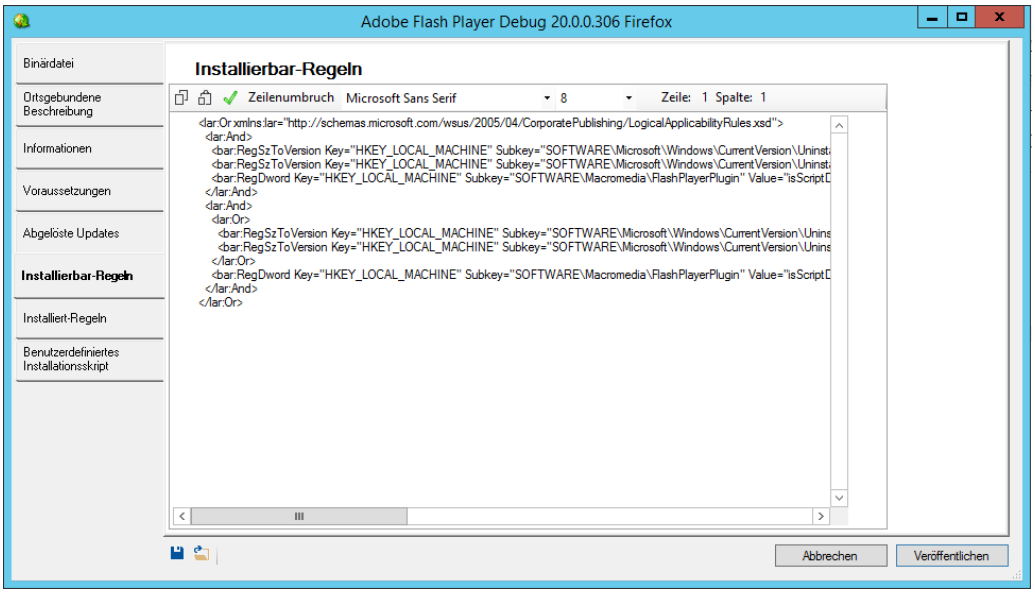
  Mithilfe des Suchfelds können Sie ein bestimmtes Update schnell in der Liste finden.

- **Ausgewählte Updates hinzufügen:** Um ein abgelöstes Update hinzuzufügen, wählen Sie das gewünschte Update in der Liste **Verfügbare Softwareupdates** aus und klicken auf **Ausgewählte Updates hinzufügen**.

- **Ausgewählte Updates entfernen:** Um Updates zu entfernen, wählen Sie sie in der Liste der abgelösten Updates aus und klicken auf diese Schaltfläche.

Bearbeiten von Installierbar-Regeln und Installiert-Regeln

Auf den Registerkarten **Instalierbar-Regeln** und **Installiert-Regeln** können Sie die Regeln bearbeiten, die dazu dienen zu bestimmen, ob ein Update für einen Zielcomputer gilt und ob derzeit ein Update auf einem Zielcomputer installiert ist. Die Regeln können für MSI- und EXE-Updates bearbeitet werden, jedoch nicht für MSP-Updates. Beide Registerkarten enthalten die gleichen Bearbeitungswerkzeuge.



- **Alle in Zwischenablage kopieren ( ):** Kopiert die vorhandenen Regeln in die Zwischenablage Ihres Computers. Dadurch können Sie, wenn gewünscht, einen leistungsfähigeren externen XML-Editor verwenden.
- **Alle aus Zwischenablage ersetzen ( ):** Ersetzt die vorhandenen Regeln durch die, die in der Zwischenablage Ihres Computers enthalten sind.
- **XML auf ordnungsgemäßes Format prüfen ( ):** Hiermit können Sie während der Entwicklung der Regeln in regelmäßigen Abständen die ordnungsgemäße XML-Formatierung überprüfen. Sie können diese Register nicht verlassen, wenn Regeln schlecht formatiertes XML enthalten. Wenn Sie versuchen, die Registerkarte zu verlassen, wird immer eine Prüfung durchgeführt.
- **Zeilenumbruch:** Schaltet den Zeilenumbruch ein bzw. aus.
- **Schriftart und Schriftgröße:** Ermöglicht es Ihnen, die Schriftart und die Schriftgröße für die Anzeige der Regeln zu ändern.
- **Zeilen und Spalten:** Zeigt die aktuelle Position des Cursors an. Das ist nützlich, wenn Sie eine Zeilen- und Spaltenposition finden müssen, die in einer Fehlermeldung angegeben ist.

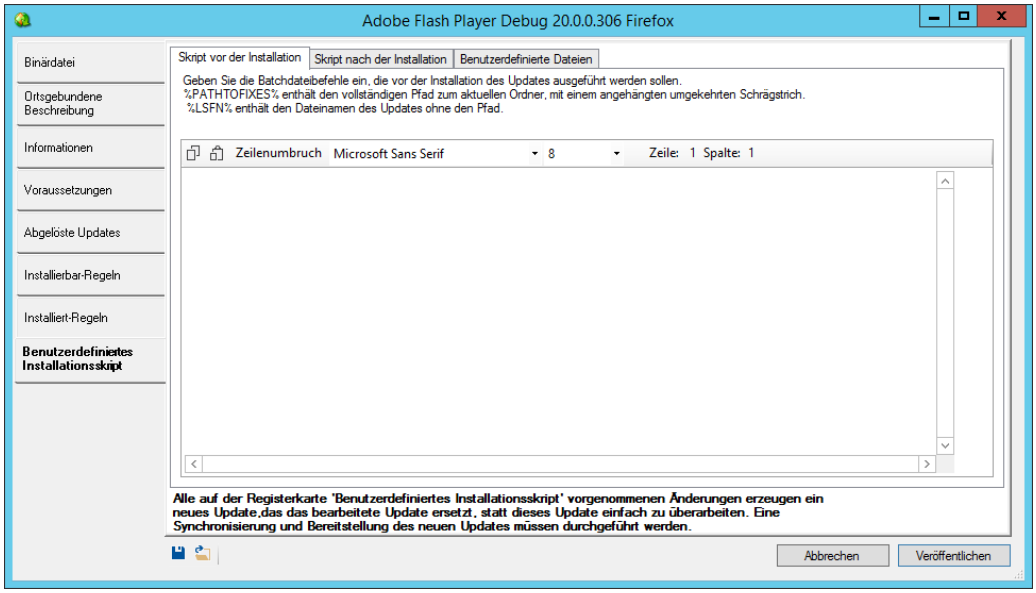
Benutzerdefinierte Installationsskripte

Auf der Registerkarte **Benutzerdefiniertes Installationsskript** können Sie Windows Batchdatei-Befehle direkt in das Installationsskript einfügen. Die Befehle können vor oder nach der Installation des Updates ausgeführt werden. Falls für die Ausführung der benutzerdefinierten Befehle andere Dateien benötigt werden, können diese in das Updatepaket aufgenommen werden.

Beispielsweise können Sie diese Funktion dann nutzen, wenn Sie Dienste stoppen und neu starten, in Konflikt stehende Software entfernen oder eine benutzerdefinierte Protokollierung durchführen möchten.

Registerkarten „Skript vor der Installation“ und „Skript nach der Installation“

Sie können benutzerdefinierte Batchbefehle definieren, die vor oder nach der Installation des Updates ausgeführt werden. Das Verfahren ist auf beiden Registerkarten gleich.

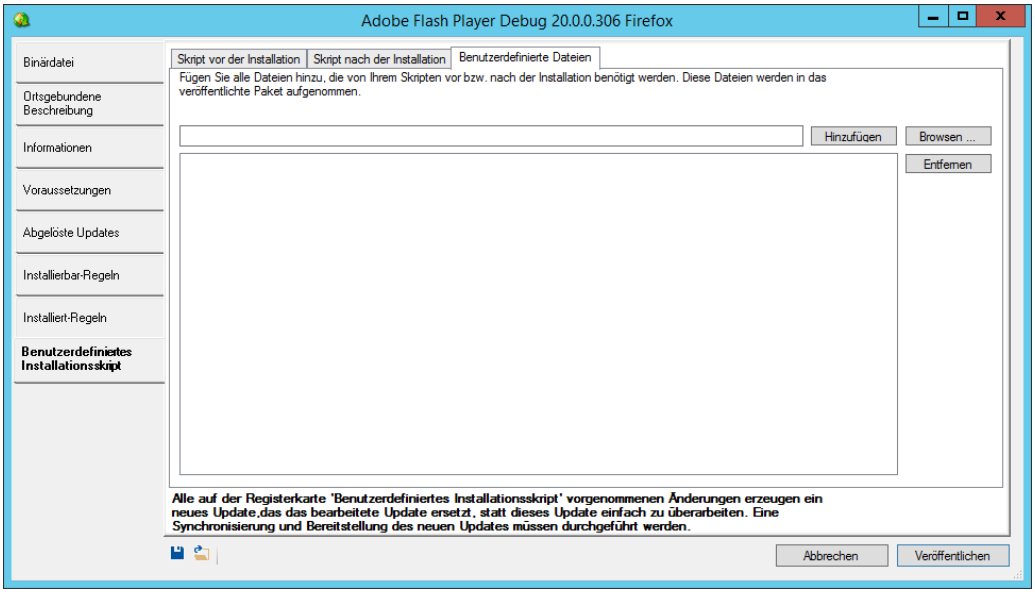


Um die Batchdatei-Befehle zu definieren, geben Sie sie in den dafür vorgesehenen Bereich ein. Sie können auch die Symbole und verwenden, um Befehle in die Zwischenablage des Computers zu kopieren bzw. daraus einzufügen. Bei den Befehlen stehen die folgenden Umgebungsvariablen zur Verfügung:

- **%PATHTOFIXES%:** Enthält den vollständigen Pfad zum aktuellen Ordner, mit einem angehängten umgekehrten Schrägstrich.
- **%LSFN%:** Die Variable für den sprachspezifischen Dateinamen liefert einen Verweis auf den Namen und die Erweiterung der Updatedatei. Der vollständige Pfad der Datei ist hierin nicht enthalten.

Registerkarte „Benutzerdefinierte Dateien“

Auf der Registerkarte **Benutzerdefinierte Dateien** geben Sie den Speicherort der Dateien an, die von Ihren benutzerdefinierten Skripten benötigt werden. Die hier angegebenen Dateien werden dem veröffentlichten Paket hinzugefügt und bei der Installation des Patches in das Arbeitsverzeichnis des Zielcomputers geschrieben.



Um eine erforderliche Datei hinzufügen, geben Sie den vollständigen Pfad zur Datei an und klicken dann auf **Hinzufügen**. Sie können auch auf **Durchsuchen** klicken, um die Datei zu suchen.

Jede von Ihnen angegebene Datei muss sich in einem Ordner oder einer Freigabe befinden, auf den bzw. die das Konto zugreifen kann, das zur Veröffentlichung des Updates genutzt wird.

Tipps zum Debuggen von benutzerdefinierten Skripts

Mit Ablaufverfolgung

Wenn Sie beim Testen eines benutzerdefinierten Installationsskripts auf Probleme stoßen, können Sie Tracing-Schritte zur Ablaufverfolgung an verschiedenen Stellen des Skripts einfügen. Eine Möglichkeit ist, Echo-Befehle zu verwenden, um Ablaufverfolgungsmeldungen in eine Textdatei zu schreiben. Zum Beispiel:

```
@echo Skript vor der Installation wird gestartet >>.\trace.txt
.
. <Ihre Skriptbefehle>
.
@echo Skript vor der Installation wird beendet >>.\trace.txt

@echo Skript nach der Installation wird gestartet >>.\trace.txt
.
. <Ihre Skriptbefehle>
.
@echo Skript nach der Installation wird beendet >>.\trace.txt
```

Bei diesem Beispiel werden die Ablaufverfolgungsmeldungen während der Installation des benutzerdefinierten Updates in die Datei trace.txt geschrieben. Anhand der Textdatei können Sie überprüfen, wo genau in Ihrem benutzerdefinierten Skript ein Fehler aufgetreten ist. Die Datei befindet sich im Sandbox-Ordner der Installation auf dem Zielcomputer. Im folgenden Abschnitt finden Sie Informationen zum Sandbox-Ordner.

Überprüfen der Dateien im Sandbox-Verzeichnis

Bei jeder Installation eines benutzerdefinierten Updates wird ein eindeutiger Sandbox-Ordner erstellt. Der Sandbox-Ordner befindet sich auf dem Zielcomputer unter:

%ProgramData%\Shavlik\Installation\InstallationSandbox#Datums-/Zeitstempel

Im Sandbox-Ordner stehen mehrere Dateien, die für Sie bei der Fehlersuche nützlich sein können. Dazu gehören alle Dateien, die in der CAB-Datei veröffentlicht wurden, sowie alle Dateien, die Sie auf der Registerkarte **Benutzerdefinierte Dateien** angegeben haben.

Sandbox-Ordner sind temporäre Ordner und werden automatisch nach einer bestimmten Anzahl von Tagen entfernt. Deshalb sollten Sie, wenn Sie einen Sandbox-Ordner behalten möchten, den Ordner an einen anderen Speicherort kopieren.

Schließlich sind benutzerdefinierte Updates nicht die einzigen Updates, die Sandbox-Ordner verwenden. Sandbox-Ordner werden auch für Updates erstellt, die eine besondere Bearbeitung erfordern. Achten Sie also darauf, beim Debuggen den richtigen Sandbox-Ordner auszuwählen.

Testen der Änderungen

Jede Änderung eines Updatepakets birgt das Risiko, dass sich Fehler einschleichen. Aus diesem Grund sollten Sie Ihre Änderungen immer testen, indem Sie ein modifiziertes Update auf dem WSUS-Server veröffentlichen und dann auf einer Reihe von Testcomputern bereitstellen. Sie sollten ein modifiziertes Update niemals auf Ihren Produktionscomputern bereitstellen, bevor es vollständig getestet wurde.

Wenn Ihre Testbereitstellung fehlschlägt und Sie weitere Änderungen vornehmen müssen, wählen Sie das Update aus der Liste **Veröffentlichte Updates von Drittanbietern** aus und klicken dann auf **Bearbeiten**. Nehmen Sie die neuen Änderungen vor, und klicken Sie dann auf **Veröffentlichen**. Wenn durch die weiteren Änderungen nur die Metadaten verändert werden, wird eine Revision veröffentlicht, doch die Kennung des Updates bleibt unverändert. Bei neuen oder zusätzlichen Änderungen auf der Registerkarte **Benutzerdefiniertes Installationsskript** wird ein neues Update veröffentlicht, welches das bearbeitete Update ersetzt.

Wenn Sie während der Entwicklungs- und Testphase mehrere Iterationen eines benutzerdefinierten Skripts veröffentlichen, kann das zu einer Reihe von abgelösten Updates führen, die nie verwendet werden. Sie sollten also die Zwischenupdates nach der Veröffentlichung der endgültigen Version löschen. Dazu wählen Sie in der Liste **Veröffentlichte Updates von Drittanbietern** alle Versionen außer der endgültigen Version der benutzerdefinierten Updates aus, die Sie erstellt haben, und klicken dann auf **Löschen**. Dadurch werden alle angepassten Zwischenversionen und alle damit verbundenen Bereitstellungen gelöscht, die Sie während des Testvorgangs durchgeführt haben.

Falls Sie alle Bearbeitungen löschen und die ursprüngliche Katalogversion des Updates veröffentlichen möchten, gehen Sie wie folgt vor:

1. Wenn Sie benutzerdefinierte Updates der Verwendung der Option **Benutzerdefiniertes Installationsskript** erstellt haben, wählen Sie die Updates in der Liste **Veröffentlichte Updates von Drittanbietern** aus und klicken dann auf **Löschen**.

2. Wenn Sie das nicht bearbeitete Update veröffentlicht haben, wählen Sie es in der Liste **Veröffentlichte Updates von Drittanbietern** aus und klicken dann auf **Neu veröffentlichen**. Wenn Sie das ursprüngliche Update noch nie veröffentlicht haben, es jetzt aber veröffentlichen möchten, wählen Sie es in der Liste **Shavlik Patches** aus und veröffentlichen es von dort aus.

Veröffentlichen der Änderungen

Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf **Veröffentlichen**, um mit der Veröffentlichung des Updates zu beginnen. Wenn Sie Ihre Änderungen speichern möchten ohne sie zu veröffentlichen, klicken Sie auf das Symbol „Speichern“ (), speichern die Änderungen in einer Datei, und klicken dann auf **Abbrechen**. Alle erkennbaren Fehler müssen vor dem Speichern der Änderungen korrigiert werden. Um die Bearbeitung fortzusetzen, wählen Sie dasselbe Update aus, starten den Editor erneut, klicken auf das Symbol „Öffnen“ () und wählen dann Ihre gespeicherte Datei aus.

Je nach Situation können Sie die bearbeiteten Updates entweder wahlweise als reine Metadaten oder als vollständigen Inhalt veröffentlichen, oder Sie müssen sie als vollständigen Inhalt veröffentlichen. Wenn Sie ein Update nur als Metadaten

veröffentlichen, wird für das Update eine Revision erstellt, und die Erkennungslogik für das Update wird bereitgestellt, jedoch sind die eigentlichen Binärdateien des Softwareupdates nicht darin enthalten. Wenn Sie ein Update als vollständigen Inhalt veröffentlichen, wird für das Update eine neue Kennung angewendet.

In folgenden Fällen können Sie ein bearbeitetes Update wahlweise entweder nur als Metadaten oder vollständigen Inhalt veröffentlichen:

- Sie nehmen nur Metadatenänderungen an einem Update vor, das bisher noch nicht veröffentlicht wurde

  Alle Registerkarten im Update-Editor - bis auf die letzte Registerkarte (**Benutzerdefiniertes Installationsskript**) - betreffen nur die Metadaten.

- Metadatenänderungen können Sie nur an einem Update vornehmen, das nur als Metadaten veröffentlicht wird

In folgenden Fällen müssen Sie ein bearbeitetes Update als vollständigen Inhalt veröffentlichen:

- Sie fügen ein benutzerdefiniertes Installationsskript hinzu bzw. bearbeiten es

  Wenn Sie auf der Registerkarte **Benutzerdefiniertes Installationsskript** Änderungen vorgenommen haben, wurde das Updatepaket modifiziert, und es muss als vollständiger Inhalt veröffentlicht werden.

- Sie bearbeiten ein Update, das als vollständiger Inhalt veröffentlicht wurde

  Für den sehr seltenen Fall, dass Sie ein Update nur als Metadaten veröffentlichen wollen und das Update bereits mit vollem Inhalt veröffentlicht wurde, müssen Sie das ursprüngliche Katalogupdate bearbeiten und dieses dann nur als Metadaten veröffentlichen. Beachten Sie, dass Configuration Manager in diesem Fall Schwierigkeiten haben kann, das Update ordnungsgemäß zu synchronisieren.

Beim Veröffentlichen eines Updates aus dem Update-Editor heraus werden Ihre Änderungen auf Fehler überprüft. Falls Fehler gefunden wurden, können Sie das Update nicht veröffentlichen. Tritt ein Fehler auf, werden Sie benachrichtigt, und Sie erhalten die Möglichkeit zur Korrektur des Fehlers. Wurden keine Fehler gefunden, wird das Dialogfeld **Ausgewählte Updates veröffentlichen** angezeigt, und Sie fahren mit dem normalen Veröffentlichungsvorgang fort.

Wenn Sie den Update-Editor dazu verwenden, ein Update zu veröffentlichen, das nicht geändert wurde, werden keine Änderungen vorgenommen und der normale Veröffentlichungsvorgang wird durchgeführt.

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

- 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 Problemumgehung 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 Zertifikat 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 diese 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**.

   Hinweis: Stellen Sie sicher, dass das Kontrollkästchen **Secure Sockets Layer (SSL) für die Verbindung mit diesem Server verwenden** aktiviert ist. Normalerweise ist eine sichere Verbindung zum WSUS-Server bei der Erstellung eines selbstsignierten Zertifikats erforderlich.
4. Klicken Sie auf **Ein selbstsigniertes Zertifikat erstellen**.

   Wenn bereits ein Zertifikat vorhanden ist, wird das folgende 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 zur ersetzen oder zu löschen.

   Wenn Sie auf **OK** klicken, wird ein zweites Dialogfeld **Warnung** angezeigt.
5. Lesen Sie die Information durch und klicken Sie dann auf **OK**.

   Im Dialogfeld werden die Anforderungen angezeigt, die erfüllt sein müssen, bevor das Zertifikat genutzt werden kann.

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

Wenn Sie den Configuration Manager mit den Berechtigungen **Als Administrator ausführen** ausführen, wird das Zertifikat auch automatisch in den folgenden Zertifikatspeichern auf der lokalen Configuration Manager-Konsole installiert:

- Vertrauenswürdige Stammzertifizierungsstellen
- Vertrauenswürdige Herausgeber

Wenn die automatische Installation fehlschlägt, müssen Sie das Zertifikat manuell an die Speicher verteilen.

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 Zertifikatdatei 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 Signaturzertifikats an einem zugänglichen Speicherort in Ihrem Netzwerk verwendet.

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 Zertifikats 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

Verlängern eines ablaufenden Signaturzertifikats

Wenn die Gültigkeit Ihres Signaturzertifikats innerhalb der nächsten 90 Tage abläuft, wird eine Warnmeldung angezeigt.

Auch wenn Sie diese Warnung mehrere Tage verzögern können, sollten Sie diese Aufgabe nicht auf die lange Bank schieben. Sobald das Gültigkeitsdatum Ihres Signaturzertifikats überschritten ist, können Sie keine Updates von Drittanbietern mehr veröffentlichen.

Vorgehensweise beim Neusignieren und Bereitstellen von Updates nach dem Erneuern eines Zertifikats

Nach dem Erneuern des Signaturzertifikats müssen Sie Ihre Updates erneut signieren und dann bereitstellen bzw. erneut bereitstellen. Das spezifische Vorgehen hängt vom aktuellen Status Ihrer Updates ab.

Szenario 1: Es liegen Updates vor, die mit einem alten Zertifikat veröffentlicht wurden, aber noch bereitgestellt wurden.

1. Signieren Sie die Updates erneut.
2. Führen Sie eine Synchronisierung mit WSUS durch.

Ihre Updates sind jetzt für die Bereitstellung bereit.

Szenario 2: Es liegen Updates vor, die mit einem alten Zertifikat veröffentlicht und bereitgestellt wurden.

In diesem Szenario müssen Sie jedes Bereitstellungspaket ändern, das ein neu signiertes Update enthält. Sie müssen jedes Update löschen, das mit dem alten Zertifikat signiert wurde, und durch die neu signierten Updates ersetzen

1. Signieren Sie die Updates erneut.
2. Führen Sie eine Synchronisierung mit WSUS durch.
3. Löschen Sie die Updates aus den Bereitstellungspaketen.
    a. Erweitern Sie im Configuration Manager-Arbeitsbereich **Softwarebibliothek** den Ordner **Softwareupdates** und klicken Sie auf **Bereitstellungspakete**.
    b. Doppelklicken Sie auf ein Bereitstellungspaket, das ein neu signiertes Update enthält.

       Dadurch wird das Bereitstellungspaket geöffnet.
    c. Klicken Sie im Bereitstellungspaket mit der rechten Maustaste auf die Updates, die Sie erneut signiert haben, und wählen Sie dann **Löschen**.
    d. Deaktivieren Sie in der Bestätigungsaufforderung das Kontrollkästchen **Verteilungspunkte aktualisieren**, und klicken Sie dann auf **OK**.

       Wenn Sie eine Warnmeldung erhalten, dass die Bereitstellung fehlschlagen wird, klicken Sie auf **OK**.
    e. Wiederholen Sie die Schritte b – d für jedes Bereitstellungspaket, das ein neu signiertes Update enthält.

4. Laden Sie die neu signierten Updates herunter und fügen Sie sie wieder in die Bereitstellungspakete ein.

    a. Öffnen Sie den Ordner **Alle Softwareupdates**.

    b. Klicken Sie mit der rechten Maustaste auf das gerade von Ihnen gelöschte Update und wählen Sie dann **Herunterladen**.

    Der Assistent **Softwareupdates herunterladen** wird angezeigt.

    c. Wählen Sie **Bereitstellungspaket auswählen**, und geben Sie dann das Bereitstellungspaket an, aus dem Sie das Update in Schritt 3 gelöscht haben.

    d. Führen Sie den Download durch, indem Sie auf **Übersicht** und dann auf **Weiter** klicken.

    e. Wiederholen Sie die Schritte b – d für jedes Update, das Sie gelöscht haben.

    Tipp: Falls die Updates zu einer Softwareupdate-Gruppe gehören, können Sie statt der einzelnen Updates die Gruppe herunterladen.

Clients zum Download neu signierter Updates befähigen

Möglicherweise haben einige Clients bereits Updates heruntergeladen, die mit dem alten Zertifikat signiert wurden. In diesem Fall müssen Sie die alten Updates aus dem Cache der Clients löschen, damit die neu signierten Updates vom Client heruntergeladen werden können.

1. Suchen und öffnen Sie auf jedem Client mithilfe der Systemsteuerung das Dialogfeld **Configuration Manager - Eigenschaften**.
2. Klicken Sie auf der Registerkarte **Cache** auf **Einstellungen konfigurieren**.
3. Klicken Sie auf **Dateien löschen**.
4. Aktivieren Sie das Kontrollkästchen **Dauerhafte Cache-Inhalte löschen**.
5. Klicken Sie auf **Ja** und dann auf **OK**.