Shavlik Protect

Leitfaden zum Upgrade

Copyright

Marken

Informationen zum Dokument und zur Historie

Dokumentnummer: nicht zutreffend

Datum	Version	Beschreibung
September 2010	NetChk Protect 7.6	Aktualisierung des Produktbrandings; Hinzufügung von Informationen zu neuen Features und Verbesserungen in 7.6.
März 2011	NetChk Protect 7.8	Hinzufügung von Informationen zu neuen Features und Verbesserungen in 7.8.
Oktober 2011	VMware vCenter Protect 8.0	Aktualisierung des Produktbrandings; Hinzufügung von Informationen zu Tasks für das Upgrade auf 8.0. Entfernen aller Informationen zu Vorversionen von 7.5.
Dezember 2011	VMware vCenter Protect 8.0, Dokumentenversion A	Hinzufügung eines Schritts, in dem die Komprimierung der Datenbank vor dem Beginn des Upgradeprozesses erklärt wird.
September 2012	VMware vCenter Protect 8.0.1	Aktualisierung des Produktnamens und der Version; Aktualisierung der Titelblattgrafik.
Mai 2013	Shavlik Protect 9.0	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen zu neuen Features und Verbesserungen in v9.0.
April 2014	Shavlik Protect 9.1	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen zu neuen Features und Verbesserungen in v9.1.
September 2015	Shavlik Protect 9.2	Aktualisierung der Systemanforderungen. Hinzufügung von Informationen über den neue Funktionen und Verbesserungen in Version 9.2.

WILLKOMMEN

Zweck dieses Dokuments

Willkommen bei Shavlik Protect 9.2. In diesem Dokument erfahren Sie, wie ein Upgrade von Shavlik Protect 9.0 oder Shavlik Protect 9.1 auf Shavlik Protect 9.2 durchgeführt wird.

Zusätzlich zu der Beschreibung des Upgradevorgangs werden in diesem Dokument eine Reihe funktionaler Unterschiede aufgeführt, deren Sie sich beim Upgrade auf Shavlik Protect 9.2 bewusst sein sollten. Darüber hinaus werden die Bereiche der Benutzeroberfläche aufgezeigt, bei denen es erhebliche Änderungen gegeben hat.

Neue Systemanforderungen und Voraussetzungen

Beachten Sie bitte die folgenden neuen Anforderungen und Voraussetzungen für Shavlik Protect 9.2.

- Windows 2000 wird nicht mehr als Betriebssystem auf Clientcomputern unterstützt.
- Windows-10 (Pro oder Enterprise Edition) wird nun auf Clientcomputern unterstützt.

Alle fehlenden Softwarevoraussetzungen werden während des Upgradeprozesses automatisch installiert. Eine vollständige Liste der Systemanforderungen finden Sie im *Shavlik Protect Installationshandbuch*.

Für das Upgrade geltende Anforderungen an das Benutzerkonto

Damit Sie ein Upgrade für Ihr Benutzerkonto durchführen können, müssen die folgenden Anforderungen erfüllt sein:

- Der Benutzer, der das Datenbank-Upgrade vornimmt, muss Mitglied der Rolle db_owner sein.
- Falls mehrere Konsolen eine Datenbank gemeinsam verwenden und eine zusätzliche Konsole mit einer Datenbank verknüpft wird, für die das Upgrade bereits durchgeführt wurde, muss das verwendete Benutzerkonto ein Mitglied der folgenden Datenbankrollen sein: db_datareader, db_datawriter, STExec und STCatalogupdate. Darüber hinaus muss das für die Hintergrundvorgänge verwendete Dienstkonto ein Mitglied der Rolle db_owner sein. Wenn Ihr Konto Mitglied der Rollen db_securityadmin und db_accessAdmin ist, versucht das Tool für das Datenbank-Upgrade automatisch, die erforderlichen Rollen für Sie zuzuordnen und zu konfigurieren.

VERFAHRENSWEISE BEIM UPGRADE

Übersicht

In diesem Abschnitt erfahren Sie, wie ein Upgrade von Shavlik Protect 9.0 oder Shavlik Protect 9.1 auf Shavlik Protect 9.2 durchgeführt wird. Wenn Sie bei dieser Gelegenheit die Konsole auf einen neuen Computer verlegen und die Migration mithilfe des Migrationstools durchführen möchten, ziehen Sie vor dem Upgrade das *Shavlik Protect Migration Tool – Benutzerhandbuch* zu Rate.

Bevor Sie das Upgrade durchführen, sollten Sie unbedingt den Abschnitt *Wichtige Änderungen und Verbesserungen* auf der Seite 18 lesen, damit Sie wissen, welche Auswirkungen das Upgrade auf Ihr System hat. Sie sollten sich alle aktuellen benutzerdefinierten Benutzereinstellungen notieren, weil einige davon während des Upgradevorgangs nicht übernommen werden (siehe Seite 17).

Durchführen des Upgrades

1. Komprimieren Sie die Datenbank, die Sie zum Speichern der Ergebnisse von Scans, Patchbereitstellungen und Reparaturen verwendet haben.

   In SQL Server Management Studio klicken Sie hierzu mit der rechten Maustaste auf die ShavlikScans-Datenbank und wählen dann **Tasks > Verkleinern > Datenbank**.

2. Erstellen Sie mit SQL Server Management Studio eine Sicherung Ihrer aktuellen Datenbank.

3. Schließen Sie alle Programme, die auf dem Konsolencomputer ausgeführt werden – auch Shavlik Protect.

4. Laden Sie die ausführbare Datei für Shavlik Protect 9.2 über den folgenden Link auf Ihren Konsolencomputer herunter:

   http://www.shavlik.com/downloads/

5. Beginnen Sie den Installationsvorgang auf eine der folgenden Weisen:

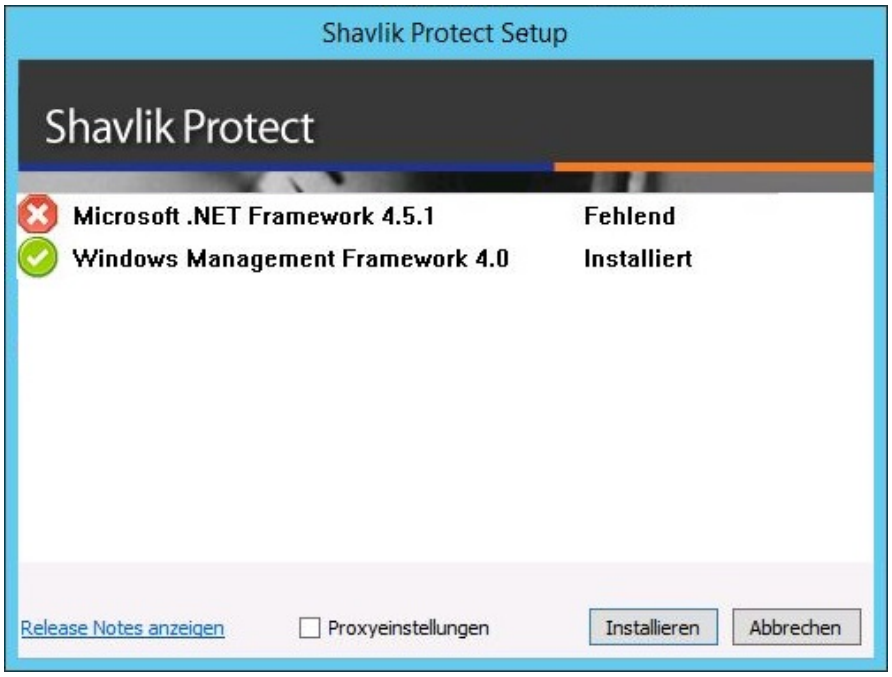
   - Doppelklicken Sie auf den Dateinamen **ShavlikProtect.exe.**
   - Geben Sie den Namen der Datei in einer Eingabeaufforderung ein. Damit können Sie mehrere Befehlszeilenoptionen verwenden. Dieses Methode ist beim Upgrade einer sehr großen Datenbank zu bevorzugen. Die Option DBCOMMANDTIMEOUT wird verwendet, um den Timeout-Wert des SQL-Befehls während der Installation anzugeben. Der Standardwert ist 15 Minuten pro GB. Die Minimum-Timeout-Wert ist der höhere Wert – entweder 15 Minuten pro GB oder 1800 Sekunden (30 Minuten). Bei einer 4 GB-Datenbank sollten Sie den Timeout-Wert auf 3600 Sekunden (60 Minuten) erhöhen. Beispiel:

     ```
     ShavlikProtect /wi:"DBCOMMANDTIMEOUT =3600"
     ```

Hinweis: Falls eine Meldung darauf hinweist, dass ein Neustart erforderlich ist, klicken Sie auf **OK**. Der Installationsvorgang wird dann automatisch nach dem Neustart fortgesetzt.

6. Beantworten Sie im anschließend angezeigten Dialogfeld die Frage, ob Sie mit dem Upgrade fortfahren wollen.

   Wenn Sie auf Ja klicken und auf dem Konsolencomputer nicht alle Voraussetzungen erfüllt sind, wird ein Dialogfeld ähnlich dem Folgenden angezeigt. Wenn alle Voraussetzungen erfüllt sind, überspringen Sie den folgenden Schritt und fahren mit dem Begrüßungsbildschirm fort.



7. Klicken Sie auf die Schaltfläche **Installieren**, um alle fehlenden Voraussetzungen zu installieren.

   Möglicherweise muss der Einrichtungsassistent während dieses Teils des Installationsprozesses einen Neustart durchführen. Falls ein Neustart erforderlich ist, wird nach dem Neustart des Computers das Dialogfeld „Einrichten" angezeigt. Klicken Sie einfach erneut auf Installieren, um mit dem Upgrade fortzufahren.

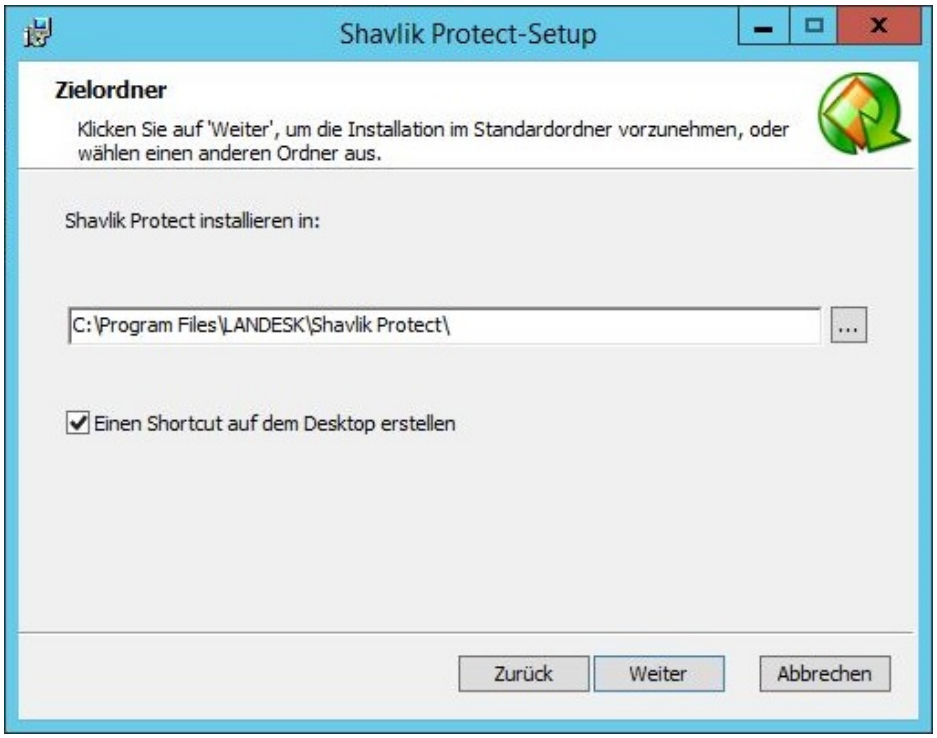
   Das Dialogfeld Willkommen wird angezeigt.

8. Lesen Sie die Informationen im Dialogfeld **Willkommen**, und klicken Sie dann auf **Weiter**.

   Die Lizenzvereinbarung wird angezeigt. Sie müssen die Bedingungen dieser Lizenzvereinbarung akzeptieren, damit Sie das Programm installieren können.

9. Aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**, und klicken Sie dann auf **Weiter**.

   Das Dialogfeld **Zielordner** wird angezeigt.



10. Wenn Sie den Standardspeicherort des Programms ändern möchten, klicken Sie auf die Schaltfläche zum Durchsuchen (...) und wählen Sie einen neuen Speicherort. Sie haben an dieser Stelle ferner die Option, einen Shortcut auf dem Desktop zu erstellen. Wenn Sie fertig sind, klicken Sie auf **Weiter**.

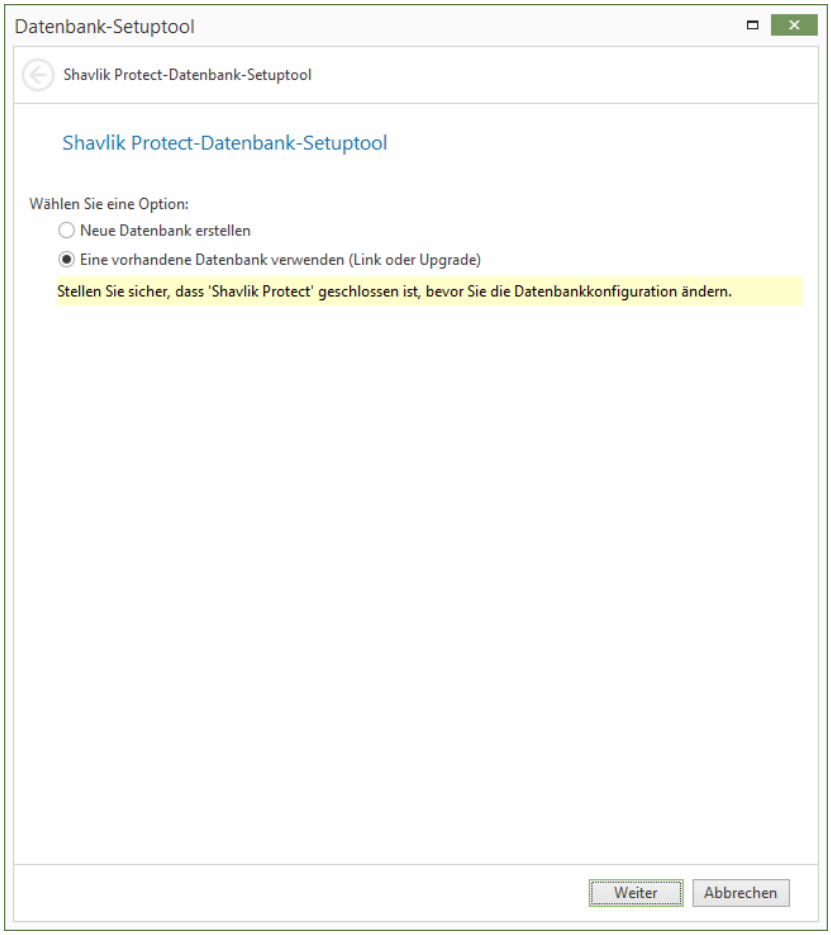
    Das Dialogfeld **Produktverbesserungsprogramm** wird angezeigt. Lesen Sie die Beschreibung und entscheiden Sie, ob Sie an dem Programm teilnehmen möchten. Das Programm versetzt Shavlik in die Lage, Nutzungsdaten zu sammeln, die zur Verbesserung zukünftiger Versionen des Produkts beitragen werden.

11. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Bereit zur Installation** wird angezeigt.

12. Um die Installation zu starten, klicken Sie auf **Installieren**.

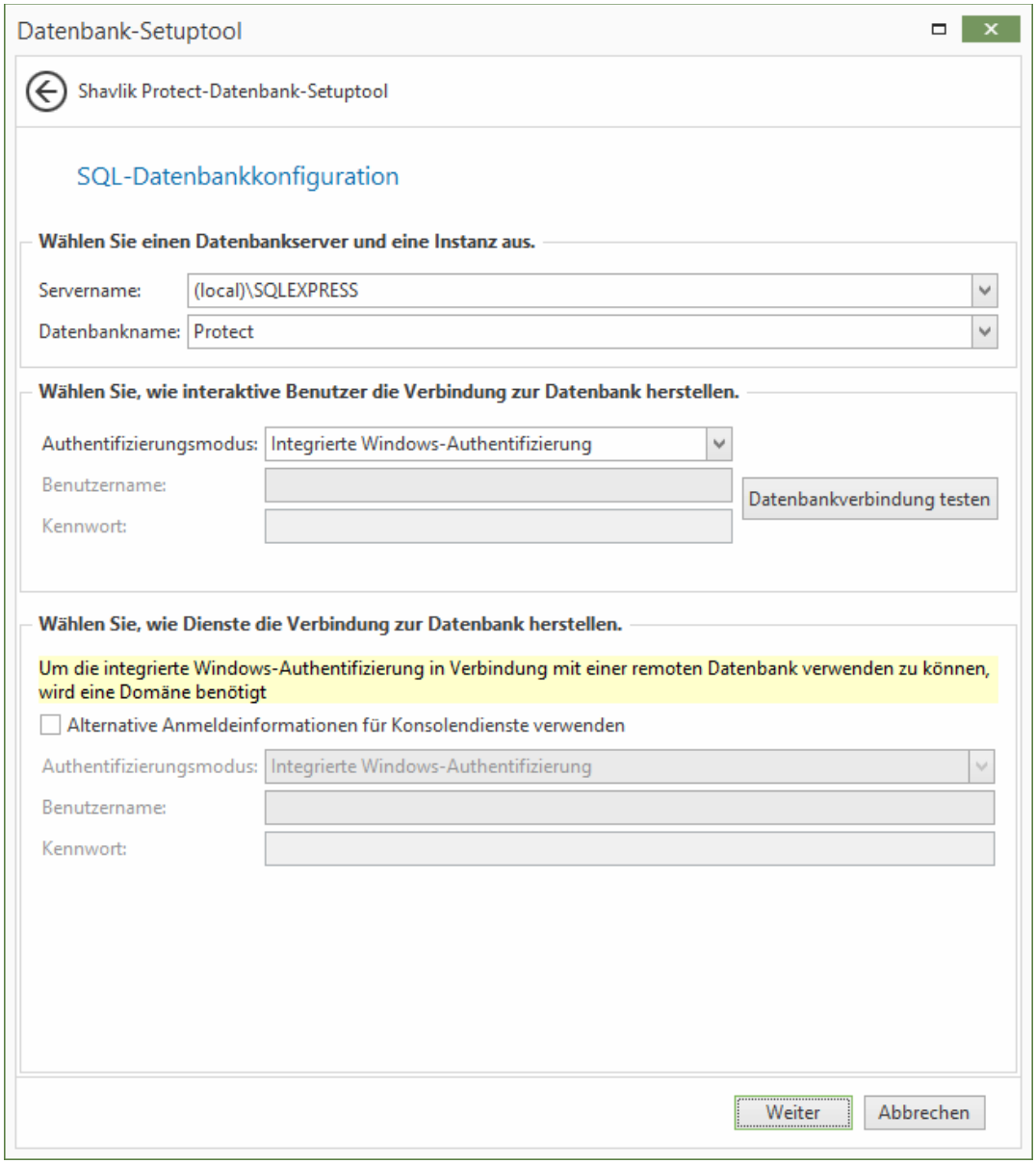
    Gegen Ende des Installationsvorgangs wird das Dialogfeld **Datenbank-Setuptool** angezeigt.



Wichtig! Wählen Sie im nächsten Schritt KEINESFALLS **Neue Datenbank erstellen** aus, denn sonst wird eine neue Datenbank erstellt und Ihre vorhandenen Daten werden nicht verwendet.

13. Vergewissern Sie sich, dass **Eine vorhandene Datenbank verwenden** ausgewählt ist und klicken Sie dann auf **Weiter**.

    Ein Dialogfeld ähnlich dem folgenden wird angezeigt:



14. Geben Sie mithilfe der verfügbaren Felder an, wie Benutzer und Dienste auf die SQL Server-Datenbank zugreifen werden.

    Wählen Sie einen Datenbankserver und eine Instanz aus.

    - **Servername:** Sie können einen Computer angeben oder Sie können einen Computer und die auf diesem Computer ausgeführte SQL Server-Instanz angeben.
    - **Datenbankname:** Geben Sie den Datenbanknamen an, den Sie verwenden möchten. Der Standard-Datenbankname lautet **Protect**.

Wählen Sie, wie interaktive Benutzer die Verbindung zur Datenbank herstellen.

Geben Sie die Anmeldeinformationen an, die das Programm verwenden soll, wenn ein Benutzer eine Aktion ausführt, die Zugriff auf die Datenbank erfordert.

- **Integrierte Windows-Authentifizierung:** Dies ist die Standardoption, die auch empfohlen wird. Shavlik Protect verwendet die Anmeldeinformationen des derzeit angemeldeten Benutzers, um die Verbindung zur SQL Server-Datenbank herzustellen. Die Felder **Benutzername** und **Kennwort** sind dann nicht verfügbar.
- **Bestimmter Windows-Benutzer:** Wählen Sie diese Option nur, wenn sich die SQL Server-Datenbank auf einem Remotecomputer befindet. Diese Option hat keinerlei Auswirkungen, wenn sich die Datenbank auf dem lokalen (Konsolen-)Computer befindet. (Nähere Informationen über Anmeldeinformationen für lokale Computer finden Sie unter *Angeben von Anmeldeinformationen* im **Shavlik Protect Administrationshandbuch**.) Alle Shavlik Protect-Benutzer werden die angegebenen Anmeldeinformationen verwenden, wenn sie Aktionen durchführen, die eine Interaktion mit der remoten SQL Server-Datenbank erfordern.
- **SQL-Authentifizierung:** Wählen Sie diese Option, wenn Sie eine spezifische Kombination von Benutzername und Kennwort für die Anmeldung bei dem angegebenen SQL Server verwenden möchten.

  Vorsicht! Wenn Sie Anmeldeinformationen für die SQL-Authentifizierung angeben und für SQL-Verbindungen keine SSL-Verschlüsselung implementiert ist, werden die Anmeldeinformationen im Klartext über das Netzwerk weitergegeben.
- **Datenbankverbindung testen:** Um sicherzustellen, dass das Programm mit den angegebenen Informationen für die interaktive Benutzeranmeldung den Kontakt zur Datenbank herstellen kann, klicken Sie auf diese Schaltfläche.

Wählen Sie, wie Dienste die Verbindung zur Datenbank herstellen.

Geben Sie die Anmeldeinformationen an, die von den Hintergrunddiensten zum Herstellen einer Verbindung zur Datenbank verwendet werden sollen. Dies sind die Anmeldeinformationen, die vom Ergebnisimportprogramm, von Vorgängen mit Agents und anderen Diensten zur Anmeldung beim SQL Server und zur Weitergabe des Status verwendet werden.

- **Alternative Anmeldeinformationen für Konsolendienste verwenden:**
  - Wenn die SQL Server-Datenbank auf dem lokalen Computer installiert ist, werden Sie diese Option in der Regel ignorieren, indem Sie dieses Kontrollkästchen nicht aktivieren. In diesem Fall werden dieselben Anmeldeinformationen und derselbe Authentifizierungsmodus verwendet, den Sie oben für interaktive Benutzer angegeben haben.
  - Dieses Kontrollkästchen sollte normalerweise nur dann aktiviert werden, wenn sich die SQL Server-Datenbank auf einem Remotecomputer befindet. Wenn sich die Datenbank auf einem Remotecomputer befindet, benötigen Sie ein Konto, mit dem die Authentifizierung gegenüber der Datenbank auf dem remoten Datenbankserver möglich ist.
- **Authentifizierungsmethode:** Nur verfügbar, wenn **Alternative Anmeldeinformationen für Konsolendienste verwenden** aktiviert wurde.
  - **Integrierte Windows-Authentifizierung:** Die Auswahl dieser Option bedeutet, dass das Computerkonto zum Herstellen der Verbindung zum remoten SQL Server verwendet wird. Damit die Anmeldeinformationen sicher übertragen

werden können, muss das Netzwerk-Authentifizierungsprotokoll Kerberos verfügbar sein. The User name and Password boxes will be unavailable.

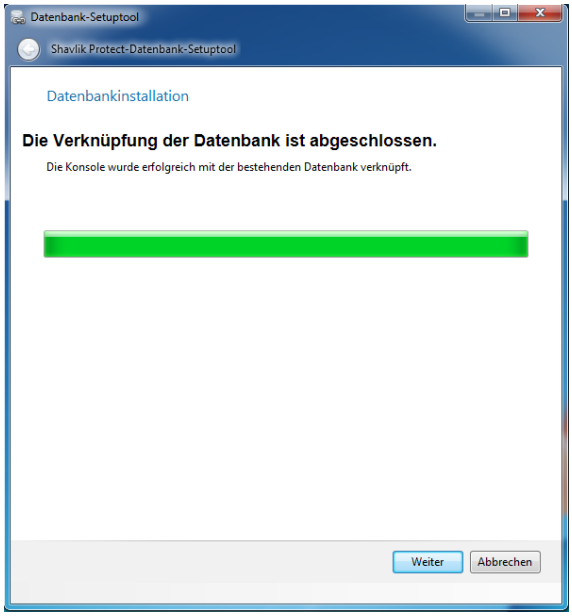
Hinweis: Wenn Sie die **Integrierte Windows-Authentifizierung** wählen, versucht das Installationsprogramm, eine SQL Server-Anmeldung für das Computerkonto zu erstellen. Sollte der Prozess zur Kontoerstellung fehlschlagen, lesen Sie unter *Nach der Installation von SQL Server – Hinweise* im *Shavlik Protect 9.2 Installationshandbuch* nach, wie ein remoter SQL Server manuell so konfiguriert wird, dass er die Anmeldeinformationen eines Computerkontos akzeptiert. Dieser Konfigurationsschritt sollte nach Abschluss des Shavlik Protect-Upgradeprozesses, aber *vor* dem ersten Programmstart durchgeführt werden.

- **Bestimmter Windows-Benutzer:** Diese Option wählen Sie, um eine spezifische Kombination von Benutzernamen und Kennwort anzugeben. Die Hintergrunddienste von Shavlik Protect verwenden diese Anmeldeinformationen zum Herstellen einer Verbindung zur SQL Server-Datenbank. Dies ist eine gute Ausweichoption, wenn aus irgendeinem Grund Schwierigkeiten bei der Implementierung der integrierten Windows-Authentifizierung auftreten sollten.
- **SQL-Authentifizierung:** Wählen Sie diese Option aus, wenn Sie eine spezifische Kombination von Benutzername und Kennwort vorgeben wollen, die von Diensten zur Anmeldung bei SQL Server verwendet werden soll.

15. Klicken Sie nach der Eingabe aller erforderlichen Informationen auf **Weiter**.

Hinweis: Wenn das Installationsprogramm bei beliebigen Anmeldeinformationen, die Sie angegeben, ein Problem erkennt, wird eine Fehlermeldung angezeigt. Zumeist ist dies ein Hinweis darauf, dass das von Ihnen angegebene Benutzerkonto nicht existiert. Nehmen Sie entsprechende Korrekturen vor und versuchen Sie es erneut.

Die Konsole wird mit Ihrer vorhandenen Datenbank verknüpft. Wenn der Verknüpfungsvorgang abgeschlossen ist, wird das folgende Dialogfeld angezeigt:



16. Klicken Sie auf **Weiter**.
17. Klicken Sie im Dialogfeld **Installation abgeschlossen** auf **Fertig stellen**.
18. Aktivieren Sie im Dialogfeld **Shavlik Protect Setup-Assistent abgeschlossen** das Kontrollkästchen **Shavlik Protect starten** und klicken Sie dann auf **Fertig stellen**.

AUF DER KONSOLE DURCHGEFÜHRTE UPGRADETASKS

Für den Abschluss des Upgrades müssen die folgenden Tasks auf der Shavlik Protect-Konsole ausgeführt werden.

Zuweisen von Scheduler-Anmeldeinformationen

Jetzt werden zur Ausführung von Konsolentasks Scheduler-Anmeldeinformationen benötigt, die Ihrem aktuellen Benutzerkonto entsprechen. Falls auf der Konsole geplante Tasks vorliegen und die Scheduler-Anmeldeinformationen nicht festgelegt wurden, wird zur Startzeit der Tasks eine Meldung angezeigt, die zur Einrichtung der Anmeldeinformationen auffordert. Diese Prüfung erfolgt bei jedem Start von Shavlik Protect, um sicherzustellen, dass geplante Tasks weiterhin ausgeführt werden.

Überprüfen der geplanten Tasks

Geplante Tasks werden jetzt aus zwei getrennten Bereichen heraus überwacht und verwaltet. Sie müssen beide Bereiche der geplanten Tasks überprüfen, und sicherstellen, dass die vorhandenen Tasks ordnungsgemäß übertragen wurden.

- **Verwaltung für geplante Konsolentasks** ist die zentrale Stelle zur Anzeige der derzeit auf der Konsole geplanten Tasks, wie z. B. Patchscans, Assetscans, Patchbereitstellungen für den Konsolencomputer, Skriptausführung und geplante Berichte.
- **Verwaltung für geplante Remotetasks** ist die zentrale Stelle zur Anzeige von Energietasks und Patchbereitstellungstasks, die derzeit auf remoten Zielcomputern geplant sind.

Aktualisieren der Lizenz (nur bei Offline-Konsolen)

Ist Ihre Konsole offline (keine Internet-Verbindung vorhanden), müssen Sie zur Anzeige und Nutzung der neuen Funktionen in Shavlik Protect 9.2 Ihre Lizenz manuell aktualisieren. Informationen zur Aktivierung einer getrennten Konsole finden Sie im Hilfesystem unter **Installation und Setup > Erste Schritte > Aktivieren des Programms**.

Wenn die Konsole online ist, wird die Lizenz während des Upgradeprozesses automatisch aktualisiert.

Überprüfen Ihrer Patchscanvorlagen und Patchgruppen

In diesen Bereichen sind drei Dinge zu berücksichtigen.

- **Patchscanvorlagen:** Die Registerkarte **Filterung** des Dialogfelds **Patchscanvorlage** wurde aktualisiert und ermöglicht jetzt präziseres Scannen. Auch wenn beim Upgradevorgang automatisch vorhandene Patchscanvorlagen in den neuen Stil konvertiert werden, sollten Sie Ihre Vorlagen doch überprüfen, um die Änderungen zu bestätigen.
- **Patchgruppen:** Patchgruppen werden nicht mehr mit einem separaten Dialogfeld definiert, sondern werden jetzt aus der Patchansicht heraus erstellt und verwaltet. Auch wenn beim Upgradevorgang automatisch vorhandene Patchgruppen in den neuen Stil konvertiert werden, sollten Sie Ihre Gruppen doch überprüfen, um die Änderungen zu bestätigen. Möglicherweise sind Ihre Patchgruppen nachdem

Upgrade kleiner, weil Shavlik die Unterstützung für viele veraltete Patches aufgegeben hat.

- **Geänderte und automatisch generierte Patchgruppen:** Um das Verhalten der Patchscanvorlagen beizubehalten, werden während des Upgradeprozesses möglicherweise einige der vorhandenen Patchgruppen geändert bzw. automatisch einige neue Patchgruppen generiert.
    - **Geänderte Patchgruppen:** Wenn Sie im Abschnitt der **Patchfiltereinstellungen** Ihrer 9.0- oder 9.1-Patchscanvorlage auf eine Patchgruppe verweisen und **Ausgewählte scannen** aktiviert ist, werden alle Patches aus der Gruppe entfernt, welche die durch die Scanvorlagenfilter definierten Kriterien nicht erfüllen. Die Gründe sind: In Protect 9.0 und 9.1 können die Patchscanvorlagen die Tatsache verdecken, dass Ihre Patchgruppe möglicherweise Patchtypen enthält, die Sie nie tatsächlich scannen oder bereitstellen wollten. Wenn die Patchgruppe in Protect 9.2 als Baseline verwendet wird, werden die Scanvorlagenfilter nicht angewendet, wodurch Ungenauigkeiten in den Patchgruppen offenbar werden. Wird vom Upgradeprozess eine solche Situation erkannt, ändert er die Patchgruppe automatisch, um die beabsichtigte Interaktion zwischen Scanvorlage und Patchgruppe beizubehalten.

      Beispiel:

      Angenommen, Ihre 9.1-Patchgruppe enthält eine Kombination aus Sicherheitspatches, Softwareverteilungspatches und nicht sicherheitsrelevanten Patches. In der Scanvorlage, die auf diese Patchgruppe verweist, ist der Abschnitt **Patchfiltereinstellungen** auf **Ausgewählte scannen** eingestellt, und der Abschnitt **Patcheigenschaften** ist so eingestellt, dass nur Sicherheitspatches erkannt werden. Bei dieser Konfiguration wird der Filter **Patcheigenschaften** berücksichtigt, und es werden nur Sicherheitspatches erkannt (trotz der Tatsache, dass die Patchgruppe nicht sicherheitsrelevante und Softwareverteilungspatches enthält).

      Nach dem Upgrade auf 9.2 definiert die Scanvorlage die Patchgruppe als Baseline-Filter. Alle anderen Scanvorlagenfilter werden dann ignoriert. Wenn die Patchgruppe nicht geändert wird, werden nicht sicherheitsrelevante und Softwareverteilungspatches jetzt erkannt (und bereitgestellt, wenn Sie das Kontrollkästchen **Automatische Bereitstellung von Patches nach dem Scan** bei der Ausführung von Scans aktivieren). Der Upgradeprozess erkennt das und entfernt die nicht sicherheitsrelevanten und Softwareverteilungspatches aus der Patchgruppe.

      Hinweis: Achten Sie in Zukunft darauf, Ihre Patchgruppen ordnungsgemäß zu verwalten, d. h. Sie sollten keine unnötigen oder unerwünschten Patches oder Patchtypen hinzufügen.

- **Automatisch generierte Patchgruppen:** Vom Upgradeprozess wird automatisch eine Kopie einer vorhandenen Patchgruppe erzeugt, wenn alle der folgenden Bedingungen erfüllt sind:
  - Wenn im Abschnitt **Patchfiltereinstellungen** einer Patchvorlage auf die Patchgruppe verwiesen wird und **Ausgewählte scannen** aktiviert ist, und
  - Wenn von einer Agentrichtlinie oder einer weiteren Scanvorlage mit anderen Filterdefinitionen auf die Patchgruppe verwiesen wird, und
  - Wenn die Patchgruppe vom Upgradeprozess aus Kompatibilitätsgründen geändert werden muss (siehe oben)

  In diesem Fall wird eine Kopie der Patchgruppe erstellt, die dann wie oben beschrieben geändert wird. Der Name der neuen Patchgruppe lautet *__<Patchgruppenname> -generated for <Scanvorlagenname>__. Die Scanvorlagen, die auf die Patchgruppe verweisen, werden dahingehend aktualisiert, dass sie den neuen Patchgruppennamen verwenden. Die ursprüngliche Patchgruppe wird beibehalten, damit Verweise darauf durch Ihre Agentrichtlinien oder andere Scanvorlagen weiter unterstützt werden.

  Sie sollten die Änderungen überprüfen und, falls gewünscht, den Namen der automatisch generierte Patchgruppe in einen aussagekräftigeren Namen umbenennen.

Zuweisen von Aliasen zur Konsole

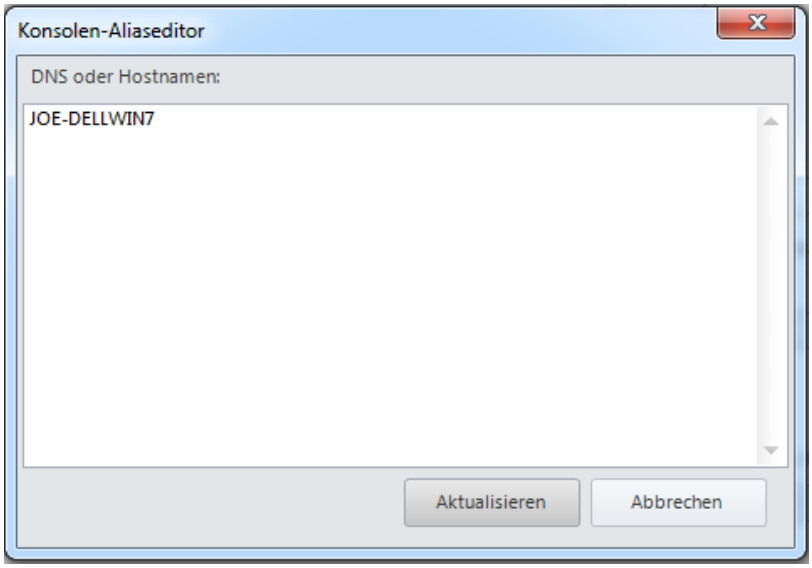
Dieser Task muss ausgeführt werden, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Sie haben den Konsolencomputer einer neuen Domäne zugewiesen.
- Sie haben der Konsole einen neuen allgemeinen Namen oder eine neue IP-Adresse zugewiesen.
- Sie haben Agents manuell installiert, und die Agents verwenden zur Kommunikation mit der Konsole eine IP-Adresse.

Unter diesen Bedingungen müssen Sie das Tool **Konsolen-Aliaseditor** zur Identifizierung der alten Konsolennamen oder Adressen einsetzen, die beide als vertrauenswürdige Aliase dienen. Wenn Sie dies unterlassen und ein Agent bei der Shavlik Protect-Konsole eincheckt oder ein agentenloser Computer versucht, eine Statusmeldung für die Patchbereitstellung an die Konsole zu senden, können die Agents nicht überprüfen, ob der von Ihnen kontaktierte Computer vertrauenswürdig ist.

1. Wählen Sie **Tools > Konsolen-Aliaseditor** aus.

   Das Dialogfeld **Konsolen-Aliaseditor** wird angezeigt. Es enthält die Namen und IP-Adressen, die derzeit zur Identifizierung des Konsolencomputers verwendet werden. Beispiel:

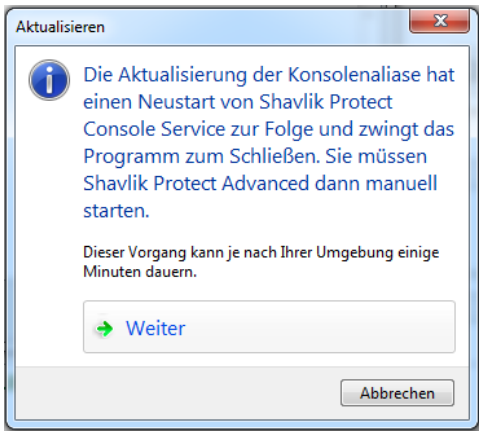


2. Geben Sie die Namen und/oder die IP-Adressen ein, die Sie als Alias für den Konsolencomputer verwenden möchten.

   IP-Adressen können entweder im IPv4-Format oder im IPv6-Format angegeben werden.

3. Klicken Sie auf **Aktualisieren**.

   Das folgende Dialogfeld wird angezeigt:



Zur Aktualisierung der Konsolenaliase ist ein Neustart des Konsolendiensts erforderlich. Außerdem muss Shavlik Protect geschlossen und manuell neu gestartet werden.

WICHTIG! Die Agents erkennen einen neuen Alias erst, nachdem sie bei der neu gestarteten Konsole einchecken. Das Einchecken muss von einem Agent entweder manuell mit dem Agentclientprogramm initiiert werden oder über ein geplantes Einchecken; ein von der Konsole ausgegebener Eincheckbefehl für einen Agent wird das Konsolenzertifikat nicht aktualisieren.

Synchronisieren von Verteilungsservern

Sie müssen Ihre Verteilungsserver mit den neuesten Patches und/oder Scanmodulen und XML-Definitionsdateien aktualisieren, die auf der Konsole vorliegen. Dies ist insbesondere dann wichtig, wenn Ihre Agents für den Download dieser Dateien auf Verteilungsserver zurückgreifen. Die Verteilungsserver müssen mit den aktualisierten Konsolendateien synchronisiert werden, **bevor** die Agents einchecken.

So synchronisieren Sie Ihre Verteilungsserver:

1. Wählen Sie **Hilfe > Dateien aktualisieren** aus, um sicherzustellen, dass die Konsole die neuesten Dateien aufweist.
2. Wählen Sie **Tools > Vorgänge > Verteilungsserver**.
3. Wählen Sie im oberen Bereich im Feld **Geplante Synchronisierung hinzufügen** die Komponente aus, die synchronisiert werden soll.
4. Wählen Sie im oberen Bereich den Verteilungsserver aus, den Sie mit der Konsole synchronisieren möchten.
5. Klicken Sie auf **Geplante Synchronisierung hinzufügen**.
6. Geben Sie an, wann die Synchronisierung erfolgen soll und klicken Sie dann auf **Speichern**.
7. Wählen Sie im Bereich **Geplante automatische Synchronisierung** den Eintrag für die geplante Synchronisierung aus.
8. Klicken Sie auf **Jetzt ausführen**.

Sollten die Agents einchecken, bevor Sie die Synchronisierung der Verteilungsserver abgeschlossen haben, ist das kein Problem. Die Agents werden aktualisiert, sobald das nächste Mal ein geplanter Task ausgeführt wird oder der Agent seine Binärdateien aktualisiert.

Erwägen der Aktivierung der Funktion „Prädiktiver Patch“

Mit dieser neuen Funktion kann Shavlik Protect automatisch Patches herunterladen, die in naher Zukunft wahrscheinlich installiert werden sollen. Wenn Sie Verteilungsserver verwenden, können Sie „Prädiktiver Patch“ mit Ihrem Verteilungsserver synchronisieren, sodass die Server Kopien der heruntergeladenen Patches erhalten. Die Option „Prädiktiver Patch“ wird auf der Registerkarte **Tools > Vorgänge > Downloads** aktiviert. Die Synchronisierung mit dem Verteilungsserver erfolgt durch Aktivieren der Option **Mit prädiktivem Patch synchronisieren** im Dialogfeld **Verteilungsserver**. Umfassende Informationen finden Sie im Hilfesystem.

Wiederherstellung der Sicherheit zwischen den Datenrollup-Konsolen

Wenn Sie mehrere Konsolen verwenden und eine Datenrollup-Konfiguration eingerichtet ist, müssen Sie die Sicherheitszuordnung zwischen der zentralen Konsole und jeder einzelnen Remotekonsole wiederherstellen.

WICHTIG! Sobald Sie den Upgradevorgang beginnen, finden solange keine Rollup-Aktivitäten mehr statt, bis das Upgrade sowohl für die zentrale Konsole als auch für die Remotekonsole durchgeführt und die Sicherheitszuordnungen zwischen beiden Konsolen wieder hergestellt wurden. Daher wird dringend empfohlen, die Konsolen hintereinander und zu einem Zeitpunkt zu aktualisieren, zu dem eine sehr geringe Datenrollup-Aktivität zu erwarten ist.

Auf der zentralen Konsole

1. Führen Sie das Upgrade für die zentrale Konsole durch.
2. Wählen Sie **Tools > Vorgänge > Datenrollup** und vergewissern Sie sich, dass das Kontrollkästchen **Ergebnisse von einem Rollup-Absender akzeptieren und importieren** aktiviert ist.

Auf allen Remotekonsolen

1. Führen Sie das Upgrade auf allen Remotekonsolen durch.
2. Wählen Sie **Tools > Vorgänge > Datenrollup** aus.
3. Überprüfen Sie die Werte für IP-Adresse/Hostnamen und Port der Rollup-Konsole.
4. Klicken Sie auf **Registrieren**.

Weitere Informationen zum Datenrollup finden Sie im Hilfesystem unter **Verwalten von mehreren Konsolen > Datenrollup-Konfiguration**.

Scannen von virtuellen Maschinen

Sind in Ihrer Computergruppe virtuelle Maschinen definiert – entweder auf der Registerkarte **Gehostete virtuelle Maschinen** oder auf der Registerkarte **Workstation virtuelle Maschinen** – müssen Sie nach dem Upgrade entweder von der Startseite aus oder aus der Computergruppe heraus einen Scan dieser Maschinen initiieren. Das ist notwendig, um die Maschinen wieder bei Protect zu identifizieren. Falls Sie den Scan nicht durchführen, werden die Felder **Virtueller Server** und **Pfad** in der Computeransicht möglicherweise nicht angezeigt, und Bereitstellungen für diese Maschinen können fehlschlagen.

Überprüfen der benutzerdefinierten Benutzereinstellungen

Folgende individuelle Benutzereinstellungen werden während des Upgradevorgangs nicht beibehalten.

- Tools > Optionen > Registerkarte „Anzeige“:
  - Aktuelles Element (Tage)
  - Archivierte Elemente
  - Nur von mir erstellte Elemente anzeigen
  - Primären Newsfeed anzeigen
  - 'Zur Information' in Patchscanergebnissen anzeigen
  - Service Packs in Ansicht > Patches anzeigen
- Tools > Einstellungen > Registerkarte „Benachrichtigungen und Warnungen“:
  - Vor dem Planen von Bereitstellungen warnen
  - 'Dateien aktualisieren' nach Abschluss schließen
  - Warnung bei nicht aktivierter Protect Cloud-Synchronisierung auf dieser Konsole
  - Vor dem Öffnen von 7 oder mehr Bulletins eine Warnung anzeigen
- Tools > Optionen > Registerkarte „Protokollierung“:
  - Diagnosepatch-Scan
- Bereitstellungsverfolgung:
  - Aktualisierungsgeschwindigkeit
  - Anzuzeigende Tage
  - Fehler anzeigen:
  - In Bearbeitung anzeigen:
  - Erfolgreich abgeschlossene anzeigen:
- Das Dialogfeld „Berichte“
  - Nach IAVA-Kennung sortieren
- Registerkarte „ESXi Hypervisor-Bulletins“:
  - Nur neueste anzeigen
- Ereignisverlauf
  - Ergebnisse auf vorherige (Tage) begrenzen
- ITScripts-Ergebnisansicht
  - Ergebnisse seit

Protect 9.2 verwendet ein SHA-2-Stammzertifikat

Shavlik führt in Protect 9.2 die Nutzung von SHA-2-Stamm- und Konsolenzertifikaten ein. Die beiden Hauptgründe dafür sind: 2048-Bit SHA-2-Zertifikate sind sicherer als ihre 1024 Bit SHA-1 Vorgänger, und SHA-1-Stammzertifikate sind bald veraltet und werden ab 1. Januar 2017 nicht mehr von Windows akzeptiert.

Nach Abschluss des Upgradevorgangs startet Shavlik Protect 9.2 hinter den Kulissen seinen eigenen Prozess, um ein neues SHA-2-Stammzertifikat und ein neues SHA-2-Konsolenzertifikat auszustellen. Falls Sie keine Agents einsetzen, ist dieser Vorgang für Sie nicht sichtbar und kann ignoriert werden. Wenn Sie Agents einsetzen, gehört zu diesem Vorgang, dass auf das Einchecken der Agents gewartet wird, damit sie das neue ausstehende Stammzertifikat erhalten können. Dieser Vorgang kann einige Tage oder Wochen dauern. Die Dauer hängt von einer Reihe von Faktoren ab, doch wird der gesamte Prozess im Hintergrund abgewickelt. Einzig die Überwachung des Ereignisverlaufsprotokolls liegt bei Ihnen, um zu prüfen, ob Probleme auftreten, um die Sie sich kümmern müssen.

WESENTLICHE ÄNDERUNGEN UND VERBESSERUNGEN IN SHAVLIK PROTECT 9.2

Umfassende Einzelheiten zu jedem der folgenden Themen finden Sie im Hilfesystem:

http://help.shavlik.com/Protect/onlinehelp/92/ENU/PRT.htm

Patchbereitstellungen	Die Engine für das Zusammenstellen und Bereitstellen von Patches für virtuelle Maschinen wurde vollständig neu geschrieben. Leistung und Zuverlässigkeit wurden verbessert.
Patchinhalt	Die Patchbewertung und die Bereitstellungsdaten, die Shavlik Protect nutzt, wurden neu zusammengestellt und in vielerlei Hinsicht verbessert.
Patchscanvorlage – Filterung	In den Patchinhalt wurden mehr Metadaten aufgenommen. Außerdem wurde die Registerkarte **Filterung** des Dialogfels **Patchscanvorlage** aktualisiert und ermöglicht präziseres Scannen.
Patchansicht/Patchgruppe	Die Patchansicht wurde vollständig neu gestaltet und aktualisiert. Sie nutzt das neue Inhaltsfomat, wodurch Sie Patchinformationen präziser anzeigen können. Darüber hinaus werden Patchgruppen jetzt aus der Patchansicht heraus erstellt und verwaltet. Dadurch wird Ihnen eine einheitlichere Methode für das Suchen von Patches und das Erstellen von Patchgruppen geboten.
Geplante Tasks	Geplante Tasks auf der Konsole nutzen jetzt den Microsoft Taskplaner. In einem neuen Dialogfeld, das über das Menü **Verwalten > Geplante Konsolentasks** geöffnet werden kann, können Sie Tasks anzeigen und diese dann verwalten.
Berichte	Jetzt steht ein neuer Bericht **End-of-Life nach Produkt** zur Verfügung. Außerdem können Sie in einem neuen Dialogfeld **Bericht planen**, das über das Menü **Tools > Bericht planen** geöffnet wird, einen Bericht automatisch an einem zukünftigen Zeitpunkt generieren lassen. Der Bericht kann automatisch einmalig oder wiederholt generiert werden.
Prädiktiver Patch	Mit dieser neuen Option kann Shavlik Protect automatisch Patches herunterladen, die in naher Zukunft wahrscheinlich installiert werden sollen. Durch das Herunterladen von Patches im Vorfeld ihrer voraussichtlichen Bereitstellung lässt sich der Bereitstellungsvorgang beschleunigen.

Patch-Dienstag + X (Tage) – Planung

Bei der Planung von Konsolenscans können Sie jetzt einen wiederkehrenden Scanvorgang durch die Verzögerung (als Anzahl von Tagen), bezogen auf ein regelmäßiges Ereignis, angeben. So könnten Sie zum Beispiel mit der neuen Option **Verzögerung hinzufügen (Tage)** planen, dass ein monatlicher Patchscan am Tag nach dem Patch-Dienstag ausgeführt wird.

Meldung zum Ende der Lebensdauer

Wenn die von Ihnen eingesetzte Version von Shavlik Protect sich ihrem EOL-Datum (End-of-Life) nähert, wird beim Starten von Shavlik Protect eine Benachrichtigung angezeigt.

Protect Cloud-Integration

Wenn dies aktiviert ist, können Patchscan- und Bereitstellungsergebnisse regelmäßig an die Protect Cloud gesendet werden. Sofern Sie ein Shavlik Empower-Benutzer sind, ruft Empower die Patchdaten regelmäßig von der Protect Cloud ab, und die Daten können dann in der browserbasierten Benutzeroberfläche von Shavlik Empower angezeigt werden

Änderungen an der Benutzeroberfläche

Folgende Elemente der Benutzeroberfläche wurden geändert:

- Die Patchansicht wurde vollständig neu gestaltet.
- Patchgruppen werden jetzt aus der Patchansicht heraus erstellt und verwaltet.
- In der Computeransicht:
    - Der obere Fensterbereich enthält drei neue Spalten Virtueller Server, VM-Name und Pfad
    - Die Registerkarte **Virtuelle Assets** wurde aus dem mittleren Fensterbereich entfernt.
    - Im unteren Bereich wurden die Registerkarten **Computer ohne Installation** und **Computer mit Installation** in einer neuen Registerkarte namens **Betroffene Computer** zusammengeführt.
- In der Patchbereitstellungsvorlage:
    - Unterstützung für Office-Installationspunkte und Originalmedien wurde entfernt.
    - Die Optionen **Dateien für Deinstallation sichern** und **Quiet-Modus** wurden entfernt; sie sind jetzt immer aktiviert.
    - Die Registerkarte **Verteilungsserver** wurde neu entworfen, sodass die Reihenfolge der verwendeten Downloadquellen besser erkannt werden kann.
- In der Patchscanvorlage:
    - Registerkarte Filter wurde komplett neu entworfen
    - Kritikalität laut Benutzer wurde entfernt.
    - Die Registerkarte Softwareverteilung zeigt nur Produkte an, die nicht ersetzt wurden.

- In der Agentrichtlinie können jetzt alle Tasks ohne Wiederholungsplanung erstellt werden. Dadurch können Sie Tasks definieren, die nur über die Benutzeroberfläche des Agent oder durch Initiierung eines Remotetask von der Konsole aus ausgeführt werden.
- In der Computergruppe wurden die Optionen **Existenz testen** und **Anmeldeinformationen testen** zusammengefasst; sie werden durch das Ausführen eines Energiestatusscans implementiert.
- Zusammenfassungen für virtuelle Assets sind in der Computeransicht nicht mehr verfügbar. Alle Informationen zu virtuellen Assets stehen jetzt über die Funktion „Virtuelles Inventar“ zur Verfügung.
- Die Berichte über Hardwaredetails, Speicherverwendung und Festplattennutzung bei virtuellen Maschinen wurden entfernt.
- In der Scanansicht kann der Unterbereich Scanübersicht nicht mehr ausgeblendet werden.
- Geplante Tasks werden jetzt in zwei separate Dialogfelder aufgeteilt: **Verwalten > Geplante Remotetasks** und **Verwalten > Geplante Konsolentasks**.
- In **Tools > Optionen**:
    - **Anzeige:** Enthält ein neues Kontrollkästchen namens **Service Packs in Ansicht > Patches anzeigen**.
    - **Benachrichtigungen und Warnungen:** Enthält ein neues Kontrollkästchen namens **Vor dem Öffnen von 7 oder mehr Bulletins eine Warnung anzeigen**; das Kontrollkästchen **Warnung vor der Planung von Vorgängen, bei denen die Standardanmeldeinformationen nicht mit dem aktuellen Benutzer übereinstimmen** wurde entfernt.
    - **Patchsprachen:** Diese Registerkarte wurde entfernt. Das Programm erkennt automatisch die auf den verwalteten Computern verwendeten Betriebssystemsprachen und lädt dann nur die benötigten Sprachversionen der Patchdatei herunter.
    - **Scans:** Enthält ein neues Kontrollkästchen namens **Ausschlüsse von Computergruppen immer erzwingen**.
    - **Bereitstellung:** Die Option für die **Adresse der Bereitstellungsverfolgung** wurde entfernt. Die Adresse wird jetzt über den **Konsolen-Aliaseditor** definiert.
    - **Protokollierung:** Enthält ein neues Kontrollkästchen namens **Diagnosepatch-Scan**.