Shavlik Protect

Guida di aggiornamento

Copyright

Marchi commerciali

Informazioni sul documento e cronologia di stampa

Numero documento: N/D

Data	Versione	Descrizione
Settembre 2010	NetChk Protect 7.6	Aggiornato il product branding e aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 7.6.
Marzo 2011	NetChk Protect 7.8	Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 7.8.
Ottobre 2011	VMware vCenter Protect 8.0	Aggiornato il product branding e aggiunte informazioni sulle attività di aggiornamento per la versione 8.0. Rimosse tutte le informazioni relative alle versioni precedenti alla 7.5.
Dicembre 2011	Vmware vCenter Protect 8.0, Documento Rev A	Aggiunti passaggi esplicativi sulla compressione del database prima di iniziare il processo di aggiornamento.
Settembre 2012	Vmware vCenter Protect 8.0.1	Aggiornato il nome prodotto e la versione, aggiornate le grafiche della copertina.
Maggio 2013	Shavlik Protect 9.0	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.0.
Aprile 2014	Shavlik Protect 9.1	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.1.
Settembre 2015	Shavlik Protect 9.2	Aggiornati i requisiti di sistema. Aggiunte informazioni sulle nuove funzioni e sui miglioramenti della versione 9.2.

BENVENUTI

Scopo di questa guida

Benvenuti in Shavlik Protect 9.2. Questo documento descrive come effettuare l'aggiornamento da Shavlik Protect 9.0 o Shavlik Protect 9.1 a Shavlik Protect 9.2.

Oltre a descrivere la procedura di aggiornamento, questo documento elenca una serie di differenze funzionali di cui tenere conto in fase di aggiornamento a Shavlik Protect 9.2. Evidenzia inoltre le aree nell'interfaccia utente che hanno subito sostanziali cambiamenti.

Nuovi requisiti e prerequisiti di sistema

Considerare i seguenti nuovi requisiti e prerequisiti per Shavlik Protect 9.2.

- Il sistema operativo Windows 2000 non è più supportato sui computer client.
- Il sistema operativo Windows 10 (Pro o Enterprise Edition) è ora supportato sui computer client.

Tutti i prerequisiti software mancanti verranno installati automaticamente durante il processo di aggiornamento. Consultare la *Guida di installazione di Shavlik Protect* per l'elenco completo dei requisiti di sistema.

Requisiti dell'account utente per l'esecuzione di un upgrade

Al fine di eseguire un aggiornamento, l'account utente deve rispettare i seguenti requisiti:

- L'utente che esegue l'aggiornamento del database deve essere membro del ruolo db_owner.
- Se si dispone di più console che condividono un database e se si effettua il collegamento di una console aggiuntiva a un database già aggiornato, l'account utente utilizzato deve essere membro dei seguenti ruoli di database: db_datareader, db_datawriter, STExec e STCatalogupdate. Inoltre, l'account di servizio utilizzato per le operazioni in background deve essere membro del ruolo db_owner. Se il proprio account è membro dei ruoli db_securityadmin e db_accessAdmin, lo strumento di aggiornamento del database cercherà automaticamente di mappare e configurare i ruoli richiesti per l'utente.

PROCEDURA DI AGGIORNAMENTO

Panoramica

Questa sezione descrive come effettuare l'aggiornamento da Shavlik Protect 9.0 o Shavlik Protect 9.1 a Shavlik Protect 9.2. Se si sta cogliendo l'opportunità per spostare la console su una nuova macchina e si desidera eseguire la migrazione utilizzando lo Strumento di migrazione, consultare la *Guida per l'utente allo strumento di migrazione di Shavlik Protect* prima di eseguire l'aggiornamento.

Prima di eseguire l'aggiornamento, assicurarsi di leggere la sezione *Modifiche e ottimizzazioni significative* a pagina 18, in modo da essere consapevoli del modo in cui l'aggiornamento influirà sul sistema. Provvedere inoltre ad annotare tutte le impostazioni utente personalizzate correnti, dato che parte di esse non verrà mantenuta durante l'upgrade (vedere pagina 17).

Esecuzione dell'upgrade

1. Comprimere il database utilizzato per archiviare i risultati delle analisi, i risultati di distribuzione delle patch e i risultati dei rimedi contro le minacce.

   A tal fine, aprire SQL Server Management Studio facendo clic con il pulsante destro del mouse nel database ShavlikScans e selezionare **Attività > Riduci > Database**.

2. Creare un backup del database corrente utilizzando SQL Server Management Studio.

3. Chiudere tutti i programmi in funzione sul computer della console, incluso Shavlik Protect.

4. Scaricare il file eseguibile di Shavlik Protect 9.2 nel proprio computer della console utilizzando il seguente collegamento:

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

5. Avviare il processo di installazione utilizzando uno dei metodi seguenti:

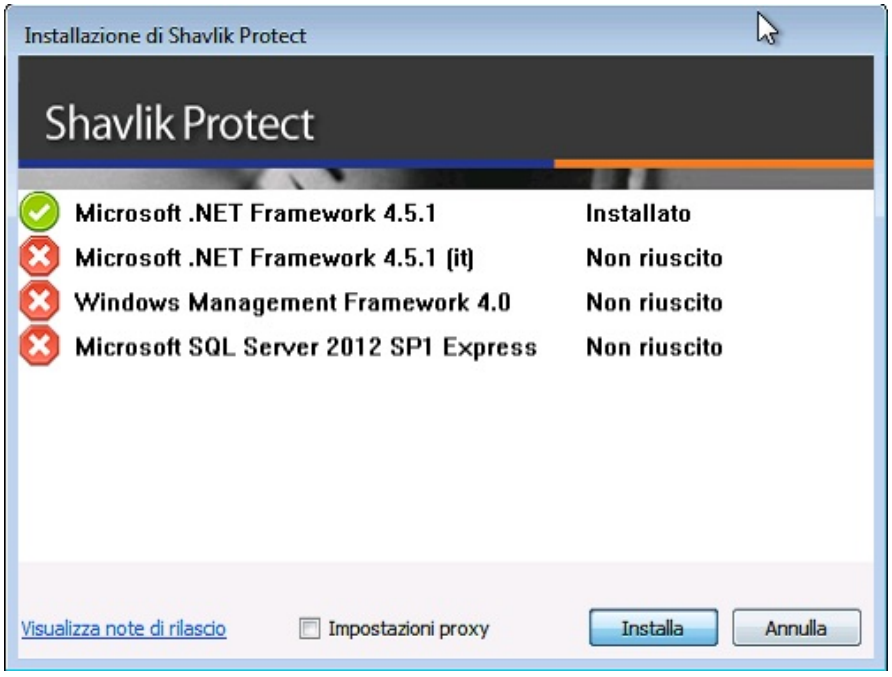
   - Fare doppio clic sul file denominato **ShavlikProtect.exe.**
   - Digitare il nome del file in un prompt dei comandi. In questo modo sarà possibile utilizzare una o più opzioni delle righe di comando. Considerare questo metodo se si sta aggiornando un database di grandi dimensioni. L'opzione DBCOMMANDTIMEOUT viene utilizzata per specificare il valore di timeout del comando SQL durante l'installazione. Il valore predefinito è 15 minuti per GB. Il valore di timeout minimo rappresenta il valore maggiore tra 15 minuti per GB e 1800 secondi (30 minuti). Se si dispone di un database da 4 GB incrementare il valore di timeout a 3600 secondi (60 minuti). Ad esempio:

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

Nota: se viene visualizzato un messaggio in cui si richiede un riavvio, fare clic su **OK**, la procedura di installazione riprenderà automaticamente dopo il riavvio.

6. Rispondere affermativamente alla finestra di dialogo che richiede se si desidera proseguire l'aggiornamento.

   Se si fa clic su Sì e il proprio computer della console risulta privo di uno o più prerequisiti, verrà visualizzata una finestra di dialogo simile alla seguente. Se non manca alcun prerequisito, ignorare il punto seguente e procedere con la finestra di dialogo **Benvenuti.**



7. Fare clic su **Installa** per installare qualsiasi prerequisito mancante.

   La procedura guidata di configurazione potrebbe richiedere un riavvio durante questa fase del processo di installazione. Se è richiesto un riavvio, una volta riavviato il computer verrà visualizzata la finestra di configurazione. Fare nuovamente clic su Installa per proseguire l'upgrade.

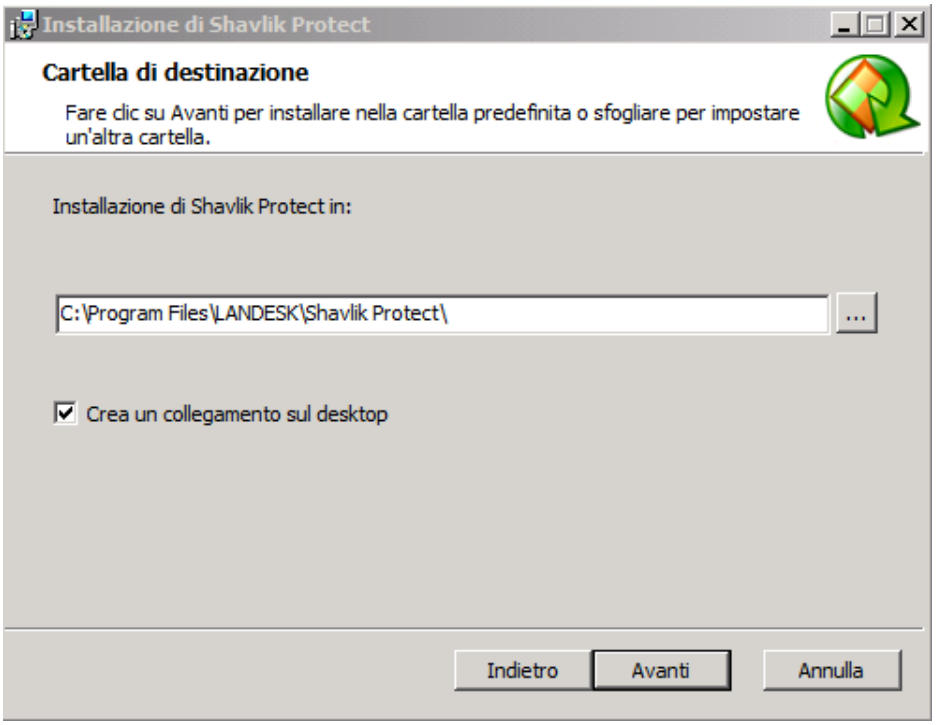
   Verrà visualizzata la finestra di dialogo **Benvenuti.**

8. Leggere le informazioni contenute nella finestra di dialogo **Benvenuti**, quindi fare clic su **Avanti**.

   Verrà visualizzato il contratto di licenza. Per poter installare il programma sarà necessario accettare i termini del contratto di licenza.

9. Spuntare la casella di controllo **Accetto i termini del Contratto di licenza**, quindi fare clic su **Avanti**.

   Verrà visualizzata la finestra di dialogo **Cartella di destinazione**.



10. Se si desidera modificare la posizione predefinita del programma, fare clic sul pulsante sfoglia e scegliere una nuova posizione. Qui è inoltre presente l'opzione che consente di installare un'icona del collegamento sul desktop. Al termine, fare clic su **Avanti**.

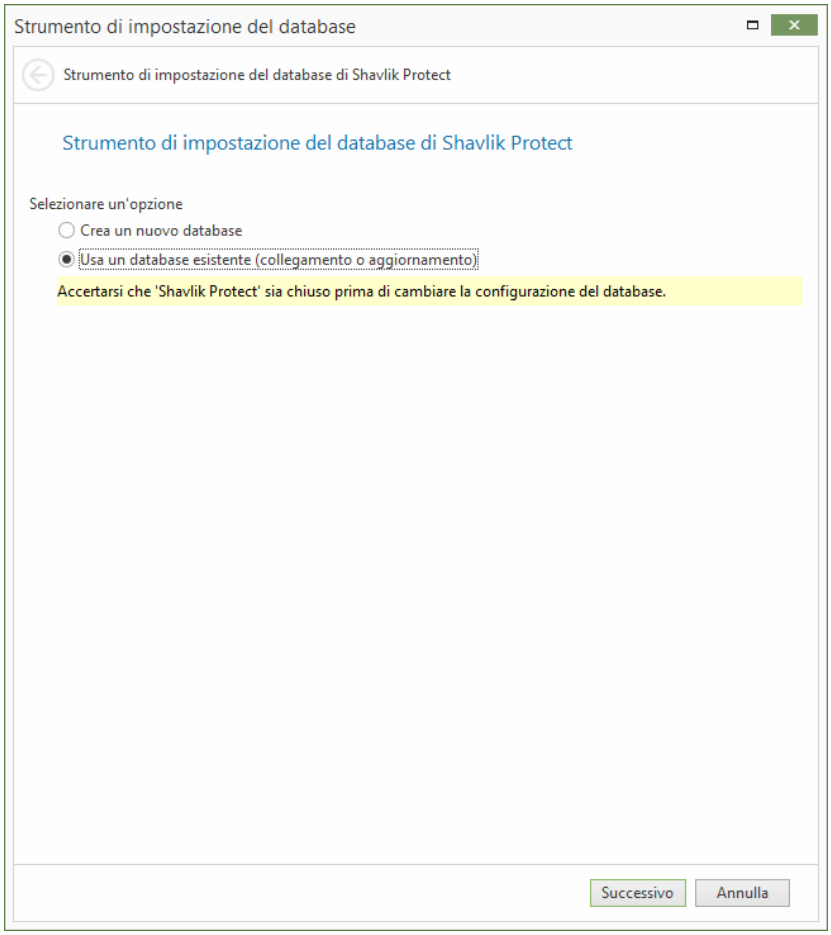
    Verrà visualizzata la finestra di dialogo **Programma di miglioramento del prodotto**. Leggere la descrizione e decidere se partecipare o meno al programma. Il programma consente a Shavlik di raccogliere informazioni sull'utilizzo del prodotto che verranno utilizzate per migliorare le versioni future.

11. Fare clic su **Avanti**.

    Verrà visualizzata la finestra di dialogo **Pronto per l'installazione**.

12. Per iniziare l'installazione fare clic su **Installa**.

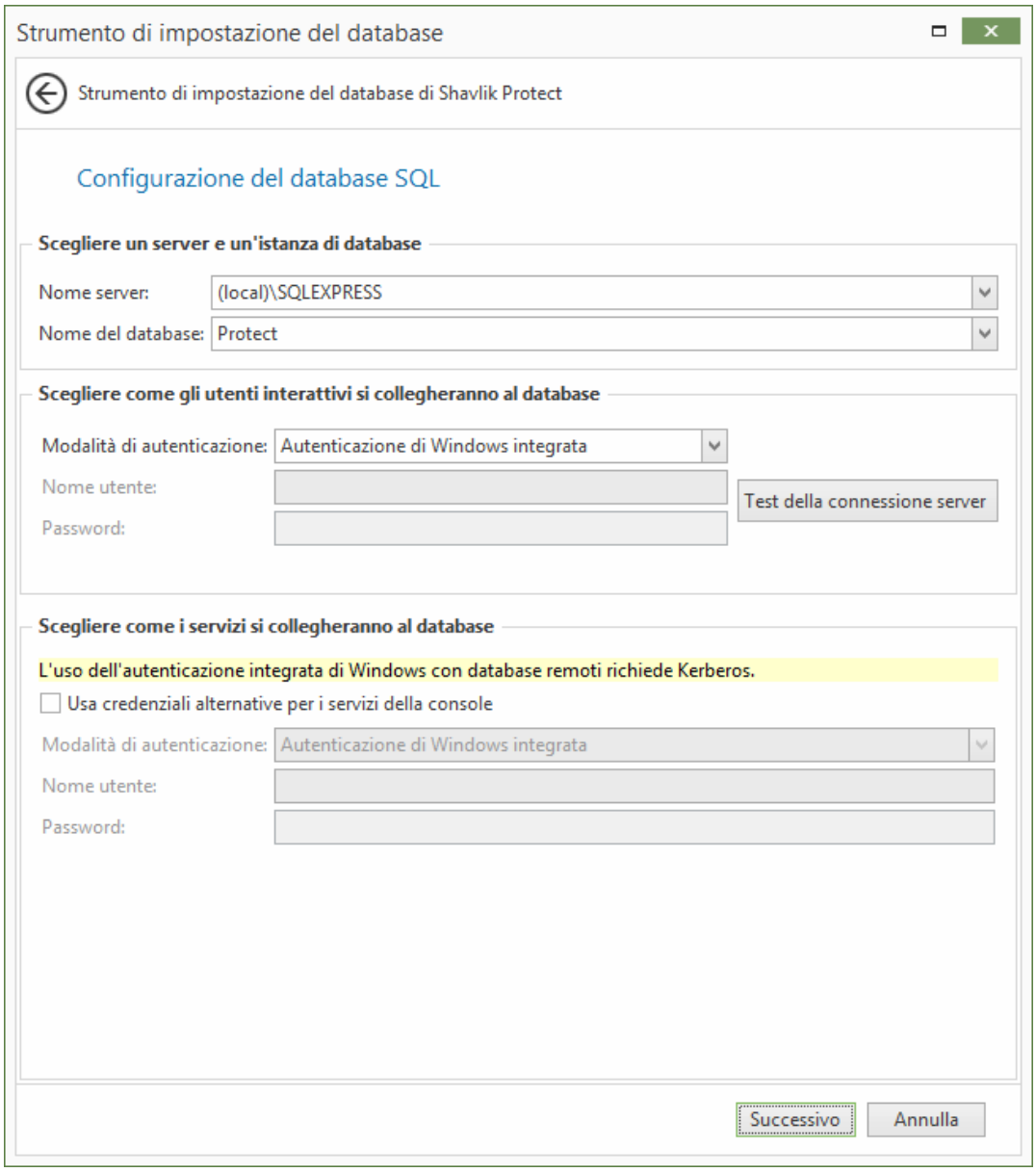
    In prossimità del termine del processo di installazione, verrà visualizzata la finestra di dialogo **Strumento di impostazione del database**.



Importante! Nella fase seguente NON selezionare **Crea un nuovo database**. Selezionando questa opzione si creerà un nuovo database e i dati esistenti non verranno utilizzati.

13. Verificare che risulti selezionato **Utilizzare un database esistente**, quindi fare clic su **Avanti**.

    Verrà visualizzata una finestra di dialogo simile alla seguente:



14. Utilizzare le caselle fornite per definire in che modo gli utenti e i servizi avranno accesso al database SQL Server.

    Scegliere un server e un'istanza di database

    - **Nome server:** è possibile specificare un computer oppure un computer e l'istanza di SQL Server in esecuzione su tale computer.
    - **Nome del database:** specificare il nome del database che si desidera utilizzare. Il nome del database predefinito è **Protect**.

Scegliere come gli utenti interattivi si collegheranno al database

Specificare le credenziali che si desidera vengano utilizzate dal programma quando un utente esegue un'azione che richiede l'accesso al database.

- **Autenticazione di Windows integrata:** si tratta dell'opzione raccomandata e predefinita. Shavlik Protect utilizzerà le credenziali dell'utente attualmente registrato per connettersi al database SQL Server. Le caselle **Nome utente** e **Password** non saranno disponibili.
- **Utente Windows specifico:** selezionare questa opzione solo se il database SQL Server si trova su un computer remoto. Questa opzione non avrà alcun effetto se il database si trova sul computer locale (console). (Consultare la sezione *Fornitura di credenziali* nella **Guida amministrativa di Shavlik Protect** per ulteriori informazioni sulle credenziali del computer locale). Tutti gli utenti di Shavlik Protect utilizzeranno le credenziali fornite al momento di eseguire azioni che richiedono un'interazione con il database SQL Server remoto.
- **Autenticazione SQL:** selezionare questa opzione per immettere una combinazione specifica di nome utente e password che verrà utilizzata per accedere all'SQL Server specificato.

  Attenzione! Se si forniscono credenziali di autenticazione SQL e non si è implementata la crittografia SSL per le connessioni SQL, le credenziali verranno trasmesse in rete come testo non crittografato.
- **Test connessione database:** per verificare che il programma possa utilizzare le credenziali utente interattive fornite per connettersi al database, fare clic su questo pulsante.

Scegliere come i servizi si collegheranno al database

Specificare le credenziali che si desidera vengano utilizzate dai servizi in background quando si effettua la connessione al database. Si tratta delle credenziali che l'unità di importazione risultati, le operazioni agente e altri servizi utilizzeranno per accedere all'SQL Server e fornire informazioni di stato.

- **Usa credenziali alternative per i servizi della console:**
  - Se il database SQL Server è installato sul computer locale, in genere si ignorerà questa opzione non attivando questa casella di controllo. In questo caso verranno utilizzate le stesse credenziali e la modalità di autenticazione specificate sopra per gli utenti interattivi.
  - In genere si spunterà questa casella di controllo solo se il database SQL Server si trova su un computer remoto. Quando il database si trova su un computer remoto, sarà richiesto un account in grado di autenticarsi al database sul server del database remoto.
- **Metodo di autenticazione:** disponibile solo se è stata attivata l'opzione **Usa credenziali alternative per i servizi della console**.
  - **Autenticazione di Windows integrata:** selezionando questa opzione l'account del computer verrà utilizzato per connettersi all'SQL Server remoto. Il protocollo di autenticazione di rete Kerberos deve essere disponibile al fine di trasmettere le credenziali in tutta sicurezza. Le caselle Nome utente e Password non saranno disponibili.

Nota: se si sceglie l'**Autenticazione di Windows integrata** il programma di installazione cercherà di creare un login di SQL Server per l'account del computer. Se la procedura di

creazione account non riesce, consultare la sezione *Note di post-installazione di SQL Server* nella *Guida di installazione di Shavlik Protect 9.2*, si otterranno istruzioni sulla configurazione manuale di un SQL Server remoto, al fine di accettare le credenziali dell'account del computer. Tale operazione è necessaria dopo il completamento del processo di aggiornamento di Shavlik Protect, ma prima di avviare il programma.

- **Utente Windows specifico:** selezionare questa opzione per immettere una combinazione specifica di nome utente e password. I servizi in background di Shavlik Protect utilizzeranno tali credenziali per connettersi al database di SQL Server. Si tratta di una valida opzione di fallback se per qualche motivo si ha difficoltà a implementare l'autenticazione di Windows integrata.
- **Autenticazione SQL:** selezionare questa opzione per fornire una combinazione specifica di nome utente e password per i servizi da utilizzare in fase di accesso a SQL Server.

15. Dopo aver fornito tutte le informazioni richieste, fare clic su **Avanti**.

Nota: se il programma di installazione rileva un problema con una qualsiasi delle credenziali specificate, verrà visualizzato un messaggio di errore. Ciò indica in genere che un account utente specificato non esiste. Effettuare le necessarie correzioni e riprovare.

La console è collegata al proprio database esistente. Al termine del processo di collegamento verrà visualizzata la seguente finestra di dialogo:

16. Fare clic su **Avanti**.
17. Sulla finestra di dialogo **Installazione completata**, fare clic su **Fine**.
18. Sulla finestra di dialogo **Procedura guidata di configurazione di Shavlik Protect completata**, attivare la casella di controllo **Avvia Shavlik Protect**, quindi fare clic su **Fine**.

ATTIVITÀ DI AGGIORNAMENTO ESEGUITE SULLA CONSOLE

Al fine di completare l'aggiornamento, eseguire le attività seguenti sulla console Shavlik Protect.

Assegnazione credenziali utilità di pianificazione

Una credenziale utilità di pianificazione corrispondente al proprio account utente corrente è ora richiesta per eseguire le attività pianificate della console. In presenza di attività pianificate sulla console con la credenziale utilità di pianificazione non impostata, si riceverà un messaggio all'avvio in cui verrà richiesto di impostare la credenziale. Tale verifica avviene a ogni avvio di Shavlik Protect, al fine di assicurare il costante funzionamento delle attività pianificate.

Revisione delle attività pianificate

Le attività pianificate vengono ora monitorate e gestite da due aree separate. Esaminare entrambe le gestioni attività pianificate per verificare che le proprie attività esistenti siano state importate correttamente.

- La **Gestione attività console pianificate** fornisce una posizione in cui visualizzare le attività attualmente pianificate sulla console, come le analisi patch, le analisi asset, le distribuzioni di patch sul computer della console, l'esecuzione di script e i report pianificati.
- La **Gestione attività remote pianificate** fornisce una posizione in cui visualizzare le attività di alimentazione e le attività di distribuzione patch attualmente pianificate sui propri computer di destinazione remoti.

Aggiornamento della licenza (solo console offline)

Se la propria console è offline (non dispone di una connessione a Internet), al fine di poter visualizzare e utilizzare le nuove funzioni in Shavlik Protect 9.2 sarà necessario aggiornare manualmente la propria licenza. Per informazioni sull'attivazione di una console disconnessa, consultare all'interno della Guida la sezione **Installazione e configurazione > Per iniziare > Attivazione del programma**.

Se la console è online, la licenza verrà aggiornata automaticamente durante il processo di aggiornamento.

Revisione dei modelli di analisi delle patch e dei gruppi di patch

Vi sono tre problematiche da considerare in queste aree.

- **Modelli di analisi delle patch:** la scheda **Filtro** sulla finestra di dialogo **Modello di analisi delle patch** è stata aggiornata per consentire una maggiore precisione durante l'analisi. Mentre la procedura di upgrade convertirà automaticamente i propri modelli di analisi delle patch esistenti al nuovo stile, sarà necessario esaminare i modelli per verificare le modifiche.
- **Gruppi di patch:** i gruppi di patch non vengono più definiti utilizzando una finestra di dialogo separata, ma vengono creati e gestiti all'interno di Visualizzazione patch. Mentre la procedura di upgrade convertirà automaticamente i propri gruppi di patch esistenti alla nuova convenzione, sarà necessario esaminare i gruppi per verificare le modifiche. I propri gruppi di patch potrebbero risultare più piccoli dopo l'upgrade, dato che Shavlik ha interrotto il supporto per molte patch datate.

- **Gruppi di patch modificati e generati in automatico:** al fine di preservare il comportamento dei modelli di analisi delle patch, uno o più dei propri gruppi di patch esistenti può essere modificato durante il processo di upgrade e uno o più dei nuovi gruppi di patch può essere generato automaticamente.
    - **Gruppi di patch modificati:** se si fa riferimento a un gruppo di patch all'interno della sezione **Impostazioni filtro patch** del proprio modello di analisi delle patch 9.0 o 9.1 e **Analizza selezionati** risulta abilitato, qualsiasi patch che non rispetta i criteri definiti dai filtri del modello di analisi verrà rimossa dal gruppo. Ecco perché: in Protect 9.0 e 9.1, i filtri dei modelli di analisi possono mascherare il fatto che il proprio gruppo di patch può contenere tipi di patch che non si è mai scelto intenzionalmente di analizzare o distribuire. In Protect 9.2, quando il gruppo di patch viene utilizzato come baseline, i filtri dei modelli di analisi non verranno applicati, rivelando potenziali imprecisioni nei gruppi di patch. Se il processo di upgrade rileva tale situazione, modificherà automaticamente il gruppo di patch, al fine di preservare l'interazione prevista tra il modello di analisi e il gruppo di patch.

      Esempio:

      Ipotizziamo che il proprio gruppo di patch 9.1 contenga un mix di patch di Protezione, Non di protezione e di Distribuzione software. Nel modello di analisi che fa riferimento a questo gruppo di patch, la sezione **Impostazioni filtro patch** viene impostata su **Analizza selezionati**, mentre la sezione **Proprietà patch** viene impostata in modo da rilevare solo le patch di Protezione. In questa configurazione, il filtro **Proprietà patch** verrà rispettato e verranno rilevate solo le patch di Protezione (nonostante il gruppo di patch contenga patch Non di protezione e di Distribuzione software).

      Dopo l'upgrade alla versione 9.2, il modello di analisi definirà il gruppo di patch come filtro di baseline e tutti gli altri filtri dei modelli di analisi verranno ignorati. Se il gruppo di patch non viene modificato, le patch Non di protezione e di Distribuzione software verranno ora rilevate (e distribuite, se si spunta la casella di controllo **Distribuisci automaticamente le patch dopo l'analisi** al momento di eseguire un'analisi). Il processo di upgrade riconoscerà la discrepanza e rimuoverà le patch Non di protezione e di Distribuzione software dal gruppo di patch.

      Nota: proseguendo, prestare attenzione al fine di gestire correttamente i gruppi di patch, in modo da non aggiungere patch o tipi di patch non necessari o indesiderati.

- **Gruppi di patch generati in automatico:** una copia di un gruppo di patch esistenti verrà generata automaticamente dal processo di upgrade nel caso in cui vengano rispettate tutte le condizioni seguenti:
  - Se si fa riferimento al gruppo di patch all'interno della sezione **Impostazioni filtro patch** di un modello di analisi delle patch e **Analizza selezionati** risulta abilitato, e
  - Se un criterio agente o un secondo modello di analisi contenente definizioni dei filtri diverse fa riferimento al gruppo di patch, e
  - Se il gruppo di patch deve essere modificato dal processo di upgrade per mantenere la compatibilità (vedere sopra)

  In questa situazione, una copia del gruppo di patch verrà generata e quindi modificata come descritto sopra. Il nome del nuovo gruppo di patch sarà ***<nome gruppo di patch> -generated for <nome modello di analisi>**. I modelli di analisi che fanno riferimento al gruppo di patch verranno aggiornati in modo da utilizzare il nuovo nome del gruppo di patch. Il gruppo di patch originale verrà mantenuto, in modo da preservare i riferimenti a esso da parte dei propri criteri agente o di altri modelli di analisi.

  È necessario esaminare le modifiche e, se desiderato, rinominare il gruppo di patch con generazione automatica utilizzando un nome più semplice o comprensibile.

Assegnazione di alias alla console

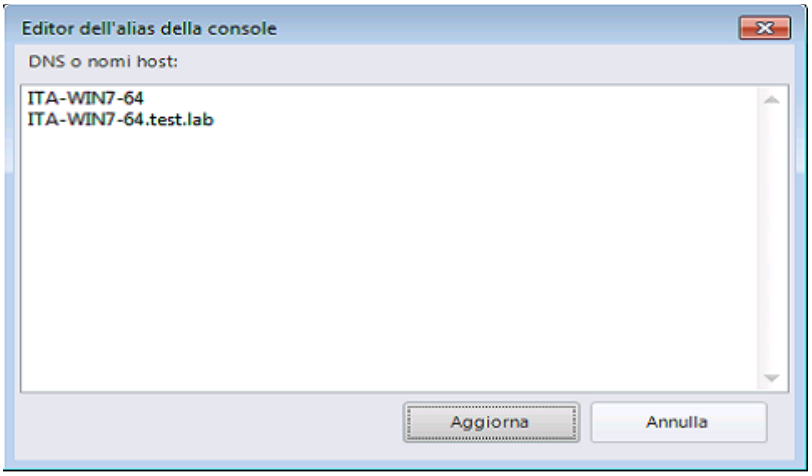
Questa attività è necessaria in caso di applicazione di una o più delle seguenti condizioni:

- Il computer della console è stato assegnato a un nuovo dominio
- Alla console è stato assegnato un nuovo nome comune o indirizzo IP
- Gli agenti sono stati installati manualmente e utilizzano un indirizzo IP per comunicare con la console

In presenza di tali condizioni è necessario utilizzare lo strumento **Editor dell'alias della console** per identificare i nomi o gli indirizzi della console precedente come alias attendibili. In caso contrario, quando un agente effettua il check-in con la console Shavlik Protect o quando un computer senza agente tenta di inviare messaggi di stato di distribuzione patch alla console, non sarà in grado di verificare l'attendibilità del computer contattato.

1. Selezionare **Strumenti > Editor dell'alias della console**.

   Verrà visualizzata la finestra di dialogo **Editor dell'alias della console**. Contiene i nomi e gli indirizzi IP attualmente utilizzati per identificare il computer della console. Ad esempio:

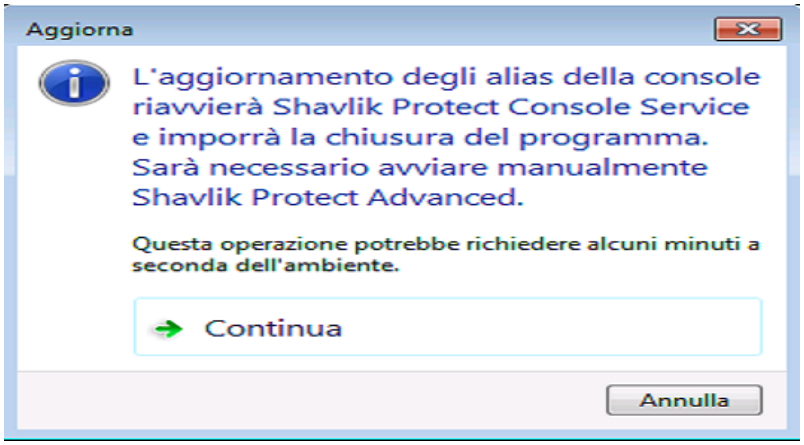


2. Digitare i nomi e/o gli indirizzi IP che si desidera utilizzare come alias per il computer della console.

   È possibile specificare gli indirizzi IP utilizzando un formato IPv4 o IPv6.

3. Fare clic su **Aggiorna**.

   Verrà visualizzata la seguente finestra di dialogo:



Al fine di aggiornare gli alias della console, riavviare il servizio della console, quindi chiudere e riavviare manualmente Shavlik Protect.

IMPORTANTE! Gli agenti non riconosceranno un nuovo alias fino a quando non avranno effettuato il check-in con la console riavviata. Il check-in deve essere inizializzato da un agente manualmente utilizzando il programma client agente o mediante un check-in pianificato; un comando di check-in emesso dalla console per un agente non aggiornerà il certificato della console.

Sincronizzazione dei server di distribuzione

È necessario aggiornare i server di distribuzione con le patch e/o i motori di analisi e i file XML delle definizioni più recenti contenuti sulla console. Ciò risulta particolarmente importante se i propri agenti utilizzano server di distribuzione per scaricare tali file. I server di distribuzione devono essere sincronizzati con i file aggiornati della console **prima** che gli agenti eseguano il relativo check-in.

Per sincronizzare i propri server di distribuzione:

1. Selezionare **Guida > Aggiorna file** per assicurarsi che la console contenga tutti i file più recenti.
2. Selezionare **Strumenti > Operazioni > Server di distribuzione**.
3. Nella casella **Aggiungi sincronizzazione pianificata** contenuta nel riquadro superiore, selezionare il componente che si desidera sincronizzare.
4. Nel riquadro superiore, selezionare quale server di distribuzione si desidera sincronizzare con la console.
5. Fare clic su **Aggiungi sincronizzazione pianificata**.
6. Specificare quando si desidera che avvenga la sincronizzazione, quindi fare clic su **Salva**.
7. Nel riquadro **Sincronizzazione automatica pianificata**, selezionare la voce di sincronizzazione pianificata.
8. Fare clic su **Esegui adesso**.

Non vi saranno problemi in caso di esecuzione del check-in degli agenti prima del termine della sincronizzazione dei server di distribuzione. Gli agenti verranno aggiornati alla prossima esecuzione di un'attività pianificata o al prossimo aggiornamento dei relativi file binari da parte degli agenti.

Valutazione dell'attivazione della funzione Patch predittiva

Questa nuova funzione consente a Shavlik Protect di scaricare automaticamente le patch che con tutta probabilità verranno distribuite nel prossimo futuro. Se si utilizzano i server di distribuzione, è possibile sincronizzare Patch predittiva con i propri server di distribuzione in modo che possano ricevere copie delle patch scaricate L'opzione Patch predittiva si attiva nella scheda **Strumenti > Operazioni > Download** e viene sincronizzata con i propri server di distribuzione spuntando l'opzione **Sincronizza con patch predittiva** sulla finestra di dialogo **Server di distribuzione**. Consultare la sezione Guida per i dettagli completi.

Ristabilimento della sicurezza tra le console di rollup dei dati

Se si utilizzano più console ed è stata stabilita una configurazione di rollup dei dati, è necessario ristabilire l'associazione di sicurezza tra la console centrale e ciascuna console remota.

IMPORTANTE! All'inizio del processo di aggiornamento, non avrà luogo alcuna attività di rollup dei dati fino a che non viene aggiornata la console centrale e la console remota e non viene ristabilita l'associazione di sicurezza tra le due console. Pertanto, si consiglia caldamente di aggiornare entrambe le console insieme e nello stesso momento quando si prevede una scarsa attività di rollup dei dati.

Sulla console centrale

1. Aggiornare la console centrale.
2. Selezionare **Strumenti > Operazioni > Rollup dei dati** e verificare che la casella di controllo **Accetta e importa risultati da un mittente di rollup** sia spuntata.

Su ciascuna console remota

1. Aggiornare ciascuna console remota.
2. Selezionare **Strumenti > Operazioni > Rollup dei dati**.
3. Verificare i valori Indirizzo IP/Nome host e porta utilizzati dalla console di rollup.
4. Fare clic su **Registra**.

Per ulteriori informazioni sul rollup dei dati, consultare nella Guida **Gestione di più console > Configurazione di rollup dei dati.**

Scansione delle proprie macchine virtuali

Se si dispone di macchine virtuali definite in un gruppo di computer o nella scheda **Macchine virtuali ospitate** o **Macchine virtuali workstation**, dopo aver eseguito l'upgrade è necessario inizializzare un'analisi di tali computer dalla pagina home o dall'interno del gruppo di computer. Ciò risulta necessario al fine di ristabilire le identità dei computer con Protect. Se non si esegue l'analisi, i campi **Server virtuale** e **Percorso** potrebbero non essere visualizzati in Visualizzazione computer e le distribuzioni a tali computer potrebbero non riuscire.

Verifica delle impostazioni utente personalizzate

Le seguenti impostazioni utente personalizzate non vengono preservate durante l'upgrade.

- Scheda Strumenti > Opzioni > Visualizzazione:
  - Elemento recente (giorni)
  - Elementi antecedenti
  - Mostra solo gli elementi creati da me
  - Mostra newsfeed principale
  - Mostra elementi informativi nei risultati di analisi delle patch
  - Mostra service pack in Visualizza -> Patch
- Scheda Strumenti > Opzioni > Notifiche e avvisi:
  - Avvisa prima di pianificare distribuzioni
  - Chiudi Aggiorna file quando terminato
  - Avvisa se la sincronizzazione di Cloud Protect non è abilitata su questa console
  - Avvisa prima di aprire 7 o più bollettini
- Scheda Strumenti > Opzioni > Registrazione:
  - Analisi diagnostica delle patch
- Monitoraggio distribuzione:
  - Velocità di aggiornamento
  - Giorni da mostrare
  - Mostra operazioni non riuscite
  - Mostra in corso
  - Mostra operazioni completate correttamente
- Finestra di dialogo Report
  - Ordina per ID IAVA
- Scheda Bollettini dell'hypervisor ESXi
  - Mostra solo i più recenti
- Cronologia eventi
  - Limita risultati ai precedenti (giorni)
- Visualizzazione risultati di ITScripts
  - Risultati dal

Da sapere: Protect 9.2 utilizza un certificato root SHA-2

Shavlik sta introducendo l'utilizzo dei certificati root e console SHA-2 in Protect 9.2. Sono due i motivi principali alla base di questa scelta: i certificati SHA-2 a 2048 bit sono più sicuri dei rispettivi predecessori SHA-1 a 1024 bit e i certificati root SHA-1 sono ora obsoleti e non verranno più accettati da Windows a partire dal 1° gennaio 2017.

Una volta completata la procedura di upgrade, Shavlik Protect 9.2 inizierà una procedura in background relativa all'emissione di un nuovo certificato root SHA-2 e di un nuovo certificato console SHA-2. Se non si stanno utilizzando agenti, tale procedura risulterà invisibile e potrà essere ignorata. Se invece si utilizzano agenti, parte della procedura coinvolge l'attesa del check-in degli agenti, pertanto essi riceveranno il nuovo certificato root in sospeso. Tale procedura potrà richiedere alcuni giorni o alcune settimane, in base a una serie di fattori, ma avverrà sempre in background. L'unica attività riservata all'utente potrà prevedere il monitoraggio del registro Cronologia eventi per rilevare l'eventuale presenza di problemi che ne richiedono l'intervento.

MODIFICHE E OTTIMIZZAZIONI SIGNIFICATIVE IN SHAVLIK PROTECT 9.2

Nella Guida sono riportati i dettagli completi relativi a ciascuno dei seguenti argomenti:

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

Distribuzioni di patch	Il motore per la creazione di pacchetti e la distribuzione di patch ai computer è stato completamente riscritto. In questo modo è stato possibile migliorare le prestazioni e l'affidabilità.
Contenuto delle patch	I dati di valutazione e distribuzione delle patch utilizzati da Shavlik Protect sono stati inseriti in un nuovo pacchetto e migliorati in svariati modi.
Filtro del modello di analisi delle patch	Sono stati aggiunti ulteriori metadati al contenuto delle patch. Inoltre, la scheda **Filtro** sulla finestra di dialogo **Modello di analisi delle patch** è stata aggiornata per consentire una maggiore precisione durante l'analisi.
Visualizzazione patch / Gruppo di patch	Visualizzazione patch è stato completamento ridisegnato e aggiornato. Sfrutta ora il nuovo formato dei contenuti, consentendo all'utente di visualizzare le informazioni sulle patch in modo più conciso. Inoltre, i gruppi di patch vengono ora creati e gestiti all'interno di Visualizzazione patch. Ciò consente di ricercare patch e di creare gruppi di patch in un modo più unificato.
Attività pianificate	Le attività pianificate sulla console utilizzano ora l'Utilità di pianificazione Microsoft. Una nuova finestra di dialogo, disponibile nel menu **Gestisci > Attività console pianificate** consente di visualizzare e gestire tali attività.
Report	È ora disponibile un nuovo report **Fine ciclo vita per prodotto**. Inoltre, una nuova finestra di dialogo **Pianifica report**, disponibile mediante il menu **Strumenti > Pianifica report**, consente di generare automaticamente un report in un dato momento futuro. Il report può essere pianificato una volta o su base ricorrente.
Patch predittiva	Questa nuova opzione consente a Shavlik Protect di scaricare automaticamente le patch che con tutta probabilità verranno distribuite nel prossimo futuro. Il download delle patch in anticipo rispetto alla loro distribuzione prevista contribuirà a migliorare la velocità del processo di distribuzione.
Pianificazione Patch Tuesday + X (giorni)	Quando si pianificano le analisi della console, è possibile ritardare un'analisi ricorrente di un dato numero di giorni, in modo da farla coincidere con un evento regolare. Ad esempio, si potrebbe pianificare un'analisi delle patch mensile per effettuarla il giorno dopo il Patch Tuesday, mediante la nuova opzione **Aggiungi ritardo (giorni)**.

Notifica fine vita

Proseguendo, se la versione di Shavlik Protect che si sta utilizzando è vicina alla data di fine vita (EOL), verrà visualizzata una notifica all'avvio di Shavlik Protect.

Integrazione di Cloud Protect

I risultati dell'analisi delle patch e di distribuzione possono essere inviati periodicamente a Cloud Protect. Se si è utenti di Shavlik Empower, Empower provvederà a recuperare periodicamente i dati delle patch da Cloud Protect, dopodiché sarà possibile visualizzare i dati all'interno dell'interfaccia utente di Shavlik Empower basata sul browser.

Modifiche all'interfaccia utente

I seguenti elementi dell'interfaccia utente sono stati modificati:

- Visualizzazione patch è stato completamento ridisegnato.
- I gruppi di patch vengono ora creati e gestiti all'interno di Visualizzazione patch.
- In visualizzazione computer:
    - Il riquadro superiore contiene tre nuove colonne: Server virtuale, Nome macchina virtuale e Percorso
    - La scheda **Asset virtuali** è stata rimossa dal riquadro centrale
    - Nel riquadro inferiore, le schede **Computer mancanti** e **Computer installati** sono state combinate in un'unica nuova scheda denominata **Computer interessati**.
- Sul modello di distribuzione patch:
    - Il supporto di Office Install Points e Original Media è stato rimosso
    - Le opzioni **Backup dei file per la disinstallazione** e **Modalità non interattiva** sono state rimosse e risultano ora sempre attive
    - La scheda **Server di distribuzione** è stata ridisegnata per aiutare a identificare l'ordine in cui verranno utilizzate le sorgenti di download
- Sul modello di analisi delle patch:
    - La scheda Filtro è stata completamente ridisegnata
    - La criticità utente è stata rimossa
    - La scheda Distribuzione software mostra solo i prodotti che non sono stati sostituiti
- Nel criterio agente, tutte le attività possono ora essere create senza una pianificazione ricorrente. Ciò consente di definire le attività che verranno eseguite solo mediante l'interfaccia utente dell'agente o l'inizializzazione di un'attività remota dalla console.
- In un gruppo di computer, le opzioni **Test esistenza** e **Test credenziali** sono state combinate e vengono ora implementate mediante l'esecuzione di un'analisi dello stato di alimentazione.
- I riepiloghi degli asset virtuali non sono più disponibili all'interno di Visualizzazione computer. Tutte le informazioni sugli asset virtuali sono ora disponibili mediante la funzione Inventario virtuale.

- I seguenti report sono stati rimossi: Report sull'hardware delle macchine virtuali, Report sull'utilizzo della memoria delle macchine virtuali e Report sull'utilizzo del disco delle macchine virtuali.
- In Visualizzazione analisi, il riquadro secondario Riepilogo analisi non è più comprimibile
- Le attività pianificate sono ora separate in due finestre di dialogo distinte: **Gestisci > Attività remote pianificate** e **Gestisci > Attività console pianificate**
- In **Strumenti > Opzioni**:
    - **Visualizzazione:** contiene una nuova casella di controllo denominata **Mostra service pack in Visualizza > Patch**
    - **Notifiche e Avvisi:** contiene una nuova casella di controllo denominata **Avvisa prima di aprire 7 o più bollettini**, mentre la casella di controllo **Avvisa prima di pianificare operazioni quando le credenziali predefinite non corrispondono all'utente corrente** è stata eliminata
    - **Lingue patch:** questa scheda è stata rimossa. Il programma rileva ora automaticamente le lingue del sistema operativo utilizzate sui propri computer gestiti e scarica solo le versioni del file di patch corrispondenti alle lingue necessarie.
    - **Analisi:** contiene una nuova casella di controllo denominata **Imporre sempre le esclusioni dei gruppi di computer**
    - **Distribuzione:** è stata rimossa l'opzione **Indirizzo Monitoraggio distribuzione**. L'indirizzo viene ora definito utilizzando l'**Editor dell'alias della console**.
    - **Registrazione:** contiene una nuova casella di controllo denominata **Analisi diagnostica delle patch**.