Shavlik Protect

Upgrade Guide

Copyright

Trademarks

Document Information and Print History

Document number: N/A

Date	Version	Description
June 2009	NetChk Protect 7.0	Initial release of the **Shavlik NetChk Protect 7.x Upgrade Guide**.
August 2009	NetChk Protect 7.1 Document Rev A	Add SQL Server 2000 and C++ prereq info for 7.1 users, and info about the asset management feature. Add data rollup functional difference.
November 2009	NetChk Protect 7.2 Document Rev B	Add Windows 7 info to system requirements section.
April 2010	NetChk Protect 7.5	Add info about Scan View, the new power management feature, improvements to software asset scan and virtual machine capabilities.
May 2010	NetChk Protect 7.5, Document Rev A	Clarify licensing information, some additional feature descriptions.
September 2010	NetChk Protect 7.6	Update product branding, add information about new 7.6 features and improvements.
March 2011	NetChk Protect 7.8	Add information about new 7.8 features and improvements.
October 2011	VMware vCenter Protect 8.0	Update product branding, add info about 8.0 upgrade tasks. Remove all info about versions prior to 7.5.
December 2011	Vmware vCenter Protect 8.0, Document Rev A	Add step explaining how to compress the database before beginning the upgrade process.
September 2012	Vmware vCenter Protect 8.0.1	Update product name and version, update cover graphics.
May 2013	Shavlik Protect 9.0	Update the system requirements. Add information about the new v9.0 features and improvements.
April 2014	Shavlik Protect 9.1	Update the system requirements. Add information about the new v9.1 features and improvements.
September 2015	Shavlik Protect 9.2	Update the system requirements. Add information about the new v9.2 features and improvements.

WELCOME

Purpose of this Guide

Welcome to Shavlik Protect 9.2. This document describes how to upgrade from Shavlik Protect 9.0 or Shavlik Protect 9.1 to Shavlik Protect 9.2.

In addition to describing the upgrade procedure, this document lists a number of functional differences you should be aware of when upgrading to Shavlik Protect 9.2. It also highlights the areas in the user interface that have changed significantly.

New System Requirements and Prerequisites

Please note the following new requirements and prerequisites for Shavlik Protect 9.2.

- Windows 2000 is no longer a supported operating system on client machines.
- Windows 10 (Pro or Enterprise Editions) is now supported on client machines.

All missing software prerequisites will be automatically installed during the upgrade process. See the *Shavlik Protect Installation Guide* for the complete list of system requirements.

User Account Requirements for Performing an Upgrade

In order to perform an upgrade your user account must meet the following requirements:

- The user performing the database upgrade must be a member of the db_owner role.
- If you have multiple consoles that share a database and are linking an additional console to a database that is already upgraded, the user account you use must be a member of the following database roles: db_datareader, db_datawriter, STExec, and STCatalogupdate. In addition, the service account used for background operations must be a member the db_owner role. If your account is a member of the db_securityadmin and db_accessAdmin roles, the database upgrade tool will automatically attempt to map and configure the required roles for you.

UPGRADE PROCEDURE

Overview

This section describes how to upgrade from Shavlik Protect 9.0 or Shavlik Protect 9.1 to Shavlik Protect 9.2. If you are taking this opportunity to move the console to a new machine and you want to perform the migration using the Migration Tool, see the *Shavlik Protect Migration Tool User's Guide* before performing the upgrade.

Before performing the upgrade, be sure to read the *Significant Changes and Enhancements* section on page 18 so you are aware of how the upgrade will affect your system. You also may want to make a note of all your current custom user settings as some are not preserved during the upgrade (see page 17).

Performing the Upgrade

1. Compress the database used to store scan results, patch deployment results, and threat remediation results.

   You can do this in SQL Server Management Studio by right-clicking the ShavlikScans database and selecting **Tasks > Shrink > Database**.

2. Create a backup of your current database using SQL Server Management Studio.
3. Close all programs running on the console machine, including Shavlik Protect.
4. Download the Shavlik Protect 9.2 executable file to your console machine using the following link:

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

5. Begin the installation process using one of the following methods:

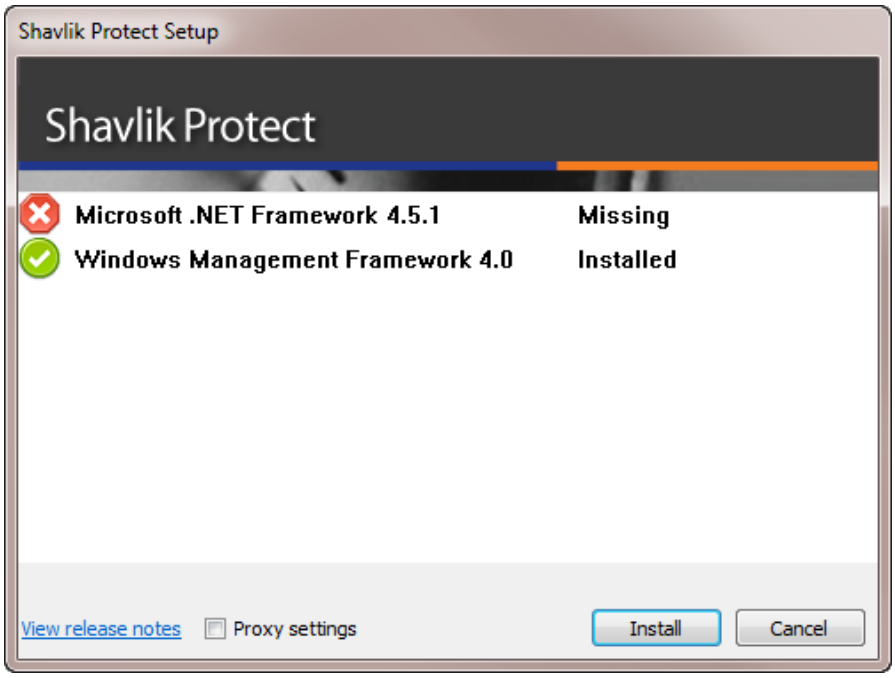
   - Double-click the file named **ShavlikProtect.exe**.
   - Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The DBCOMMANDTIMEOUT option is used to specify the SQL command timeout value during installation. The default value is 15 minutes per GB. The minimum timeout value is the greater of 15 minutes per GB or 1800 seconds (30 minutes). If you have a 4 GB database you should increase the timeout value to 3600 seconds (60 minutes). For example:

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

Note: If you receive a prompt indicating that a restart is required, click **OK** and the installation process will automatically resume after the restart.

6. Respond to the dialog that asks if you want to continue with the upgrade.

   If you click **Yes** and your console machine is missing one or more prerequisites, a dialog similar to the following is displayed. If you are not missing any prerequisites, skip the following step and proceed with the **Welcome** dialog.



7. Click **Install** to install any missing prerequisites.

   The Setup Wizard may need to perform a reboot during this portion of the installation process. If a reboot is required, when the machine is restarted the Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

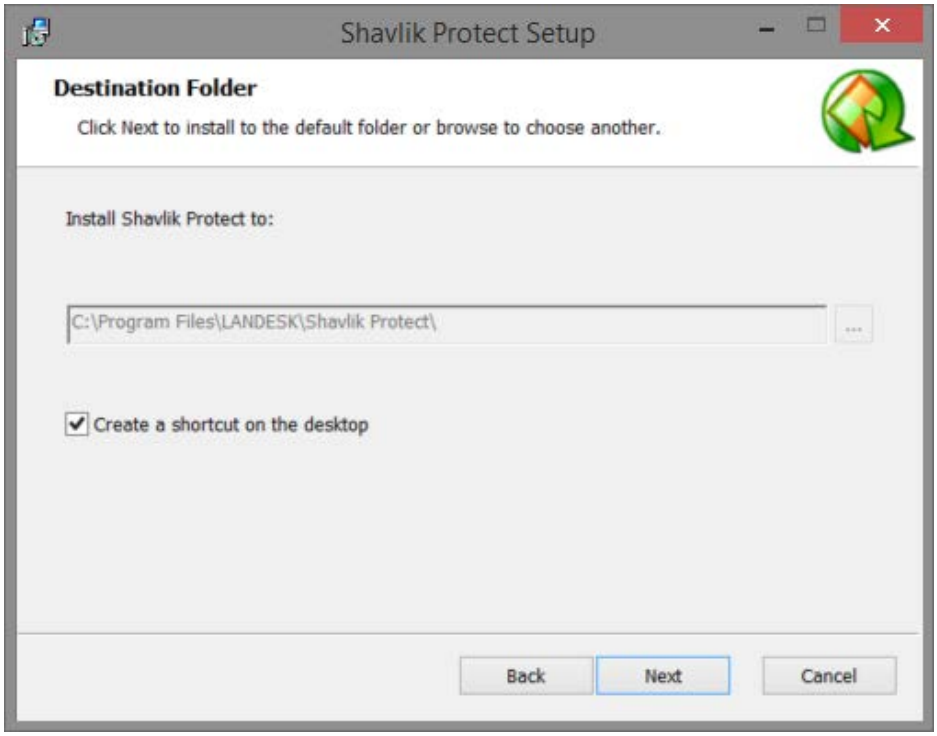
   The **Welcome** dialog is displayed.

8. Read the information on the **Welcome** dialog and then click **Next**.

   The license agreement is displayed. You must accept the terms of the license agreement in order to install the program.

9. Enable the **I accept the terms in the License Agreement** check box and then click **Next**.

   The **Destination Folder** dialog is displayed.



10. If you want to change the default location of the program, click the browse button and choose a new location. You also have the option here to install a shortcut icon on your desktop. When you are done, click **Next**.

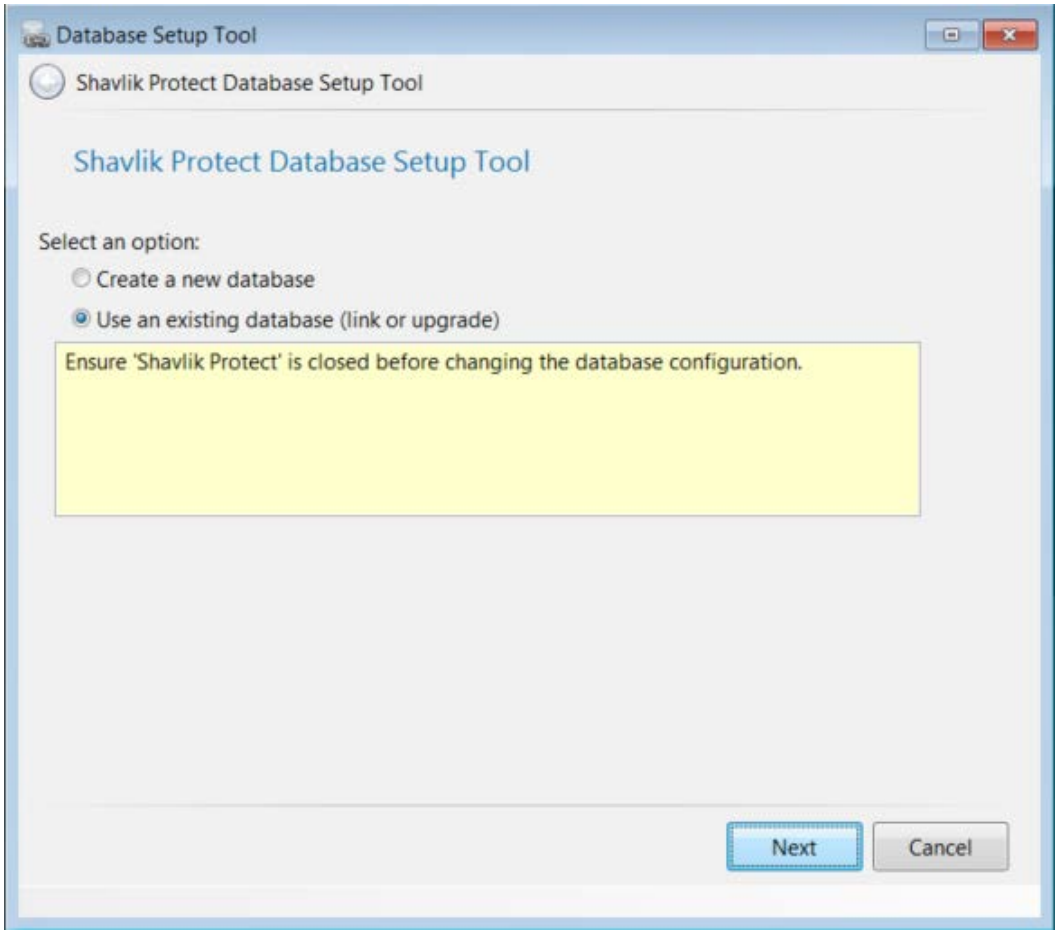
    The **Product Improvement Program** dialog is displayed. Read the description and decide if you agree to participate in the program. The program enables Shavlik to collect product usage information that will help improve future versions of the product.

11. Click **Next**.

    The **Ready to Install** dialog is displayed.

12. To begin the installation, click **Install**.

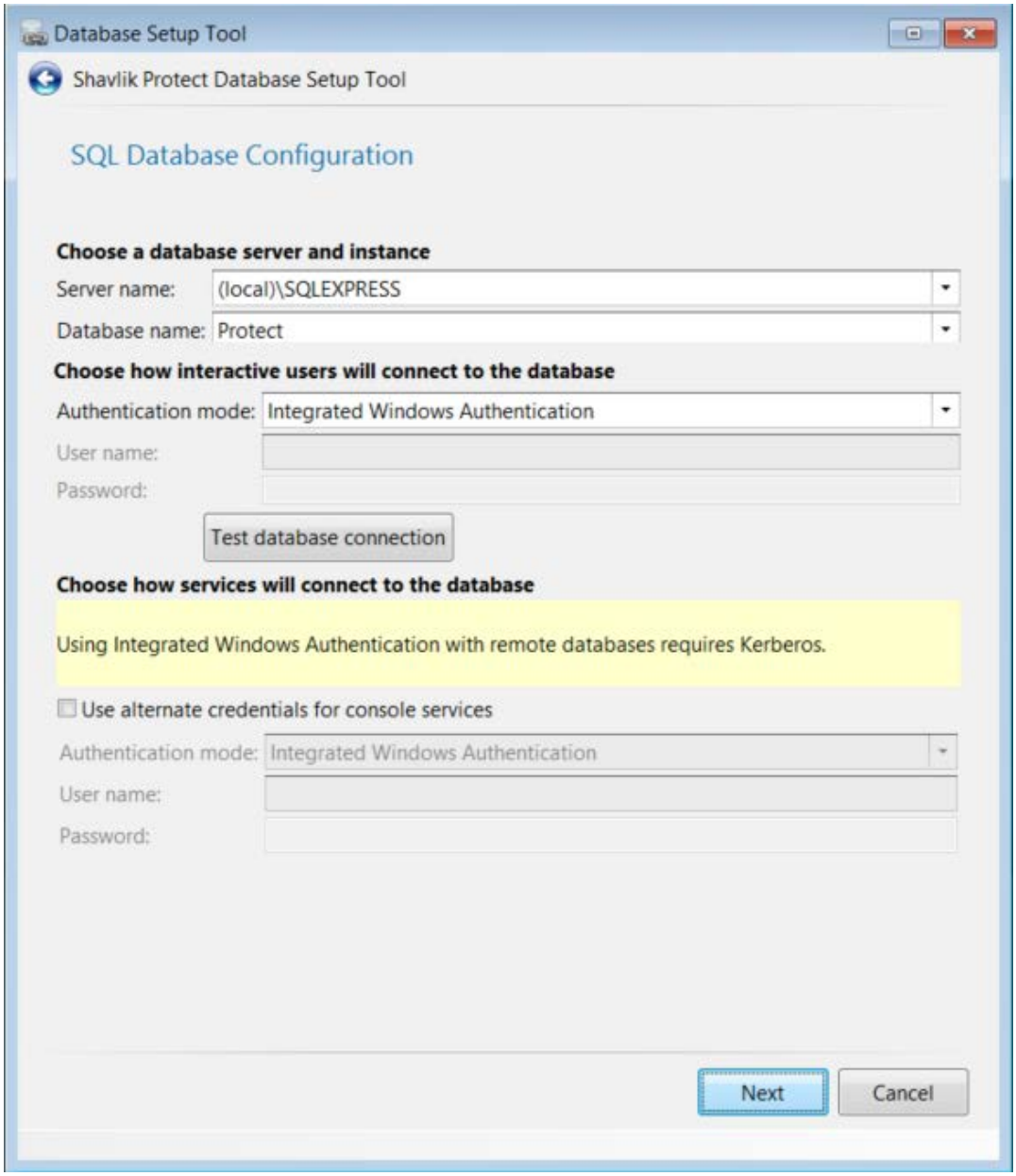
    Near the end of the installation process the **Database Setup Tool** dialog is displayed.



Important! In the next step DO NOT select **Create a new database**. If you do a new database will be created and your existing data will not be used.

13. Make sure **Use an existing database** is selected and then click **Next**.

    A dialog similar to the following is displayed:



14. Use the boxes provided to define how users and services will access the SQL Server database.

    Choose a database server and instance

    - **Server name:** You can specify a machine or you can specify a machine and the SQL Server instance running on that machine.
    - **Database name:** Specify the database name you want to use. The default database name is **Protect**.

Choose how interactive users will connect to the database

Specify the credentials you want the program to use when a user performs an action that requires access to the database.

- **Integrated Windows Authentication:** This is the recommended and default option. Shavlik Protect will use the credentials of the currently logged on user to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **Specific Windows User:** Select this option only if the SQL Server database is on a remote machine. This option will have no effect if the database is on the local (console) machine. (See *Supplying Credentials* in the **Shavlik Protect Administration Guide** for more information about local machine credentials.) All Shavlik Protect users will use the supplied credentials when performing actions that require interaction with the remote SQL Server database.
- **SQL Authentication:** Select this option to enter a specific user name and password combination when logging on to the specified SQL Server.

  Caution! If you supply SQL authentication credentials and have not implemented SSL encryption for SQL connections, the credentials will be passed over the network in clear text.
- **Test database connection:** To verify that the program can use the supplied interactive user credentials to connect to the database, click this button.

Choose how services will connect to the database

Specify the credentials you want the background services to use when making the connection to the database. These are the credentials that the results importer, various agent operations, and other services will use to log on to SQL Server and provide status.

- **Use alternate credentials for console services:**
  - If the SQL Server database is installed on the local machine you will typically ignore this option by not enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will be used.
  - You will typically only enable this check box if the SQL Server database is on a remote machine. When the database is on a remote machine you need an account that can authenticate to the database on the remote database server.
- **Authentication method:** Available only if **Use alternate credentials for console services** is enabled.
  - **Integrated Windows Authentication:** Selecting this option means that the machine account will be used to connect to the remote SQL Server. The Kerberos network authentication protocol must be available in order to securely transmit the credentials. The User name and Password boxes will be unavailable.

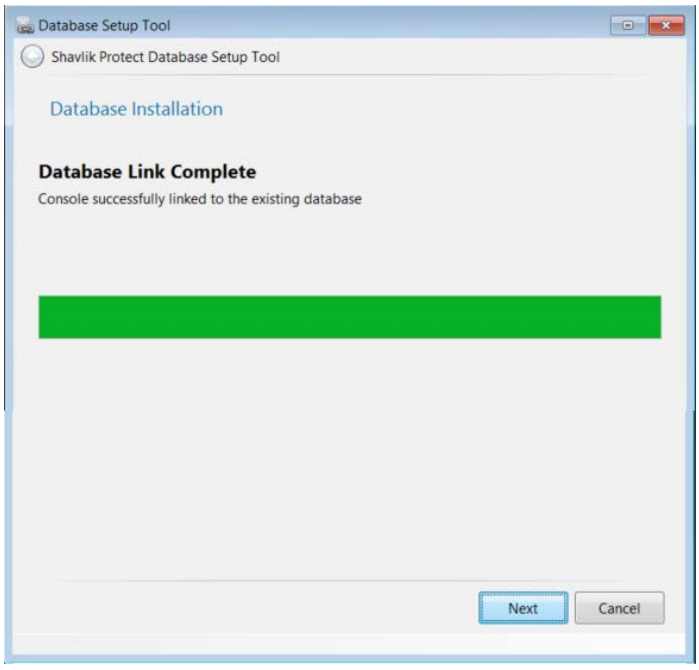
Note: If you choose **Integrated Windows Authentication** the installation program will attempt to create a SQL Server login for the machine account. If the account creation process fails, see *SQL Server Post-Installation Notes* in the *Shavlik Protect 9.2 Installation Guide* for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the Shavlik Protect upgrade process but before you start the program.

- **Specific Windows User:** Select this option to enter a specific user name and password combination. Shavlik Protect's background services will use these credentials to connect to the SQL Server database. This is a good fallback option if for some reason you have difficulties implementing integrated Windows authentication.
- **SQL Authentication:** Select this option to provide a specific user name and password combination for the services to use when logging on to SQL Server.

15. After providing all the required information, click **Next**.

Note: If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

The console is linked to your existing database. When the link process is complete the following dialog is displayed:



16. Click **Next**.
17. On the **Installation Complete** dialog click **Finish**.
18. On the **Completed the Shavlik Protect Setup Wizard** dialog, enable the **Launch Shavlik Protect** check box and then click **Finish**.

UPGRADE TASKS PERFORMED ON THE CONSOLE

In order to complete the upgrade, the following tasks must be performed on the Shavlik Protect console.

Assign Scheduler Credentials

A scheduler credential that matches your current user account is now required to run scheduled console tasks. If there are scheduled tasks on the console and the scheduler credential has not been set, you will receive a prompt at startup time to set the credential. This check occurs every time Shavlik Protect is started to ensure that scheduled tasks continue to run.

Review Your Scheduled Tasks

Scheduled tasks are now monitored and managed from two separate areas. You should review both scheduled tasks managers to verify that your existing tasks were properly ported.

- The **Scheduled Console Tasks Manager** provides one location to view tasks currently scheduled on the console such as patch scans, asset scans, patch deployments to the console machine, script execution and scheduled reports.
- The **Scheduled Remote Tasks Manager** provides one location from which to view power tasks and patch deployments tasks currently scheduled on your remote target machines.

Refresh Your License (Offline Consoles Only)

If your console is offline (it does not have an Internet connection), in order to view and use the new features in Shavlik Protect 9.2 you must manually refresh your license. For information on activating a disconnected console, in the Help system see **Installation and Setup > Getting Started > Activating the Program**.

If the console is online the license will be automatically refreshed during the upgrade process.

Review Your Patch Scan Templates and Patch Groups

There are three issues to consider in these areas.

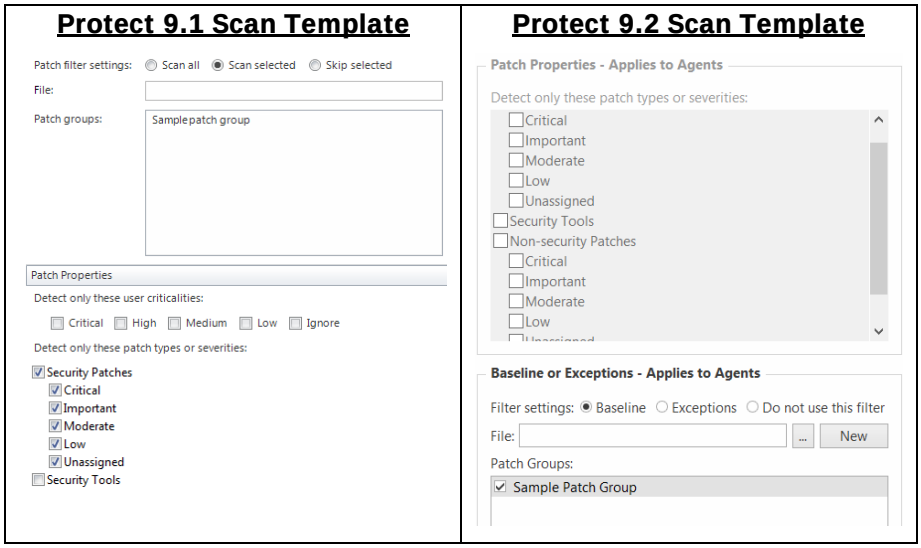
- **Patch Scan Templates:** The **Filtering** tab on the **Patch Scan Template** dialog has been updated to allow for more precision when scanning. While the upgrade process will automatically convert your existing patch scan templates to the new style, you should double-check your templates to verify the changes.
- **Patch Groups:** Patch groups are no longer defined using a separate dialog; rather, they are now created and managed from within Patch View. While the upgrade process will automatically convert your existing patch groups to the new convention, you should double-check your groups to verify the changes. Your patch groups may be smaller after the upgrade as Shavlik has deprecated support for many old patches.

- **Modified and Auto-Generated Patch Groups:** In order to preserve the behavior of your patch scan templates, one or more of your existing patch groups may be modified during the upgrade process and one or more new patch groups may be automatically generated.
    - **Modified Patch Groups:** If you reference a patch group within the **Patch filter settings** section of your 9.0 or 9.1 patch scan template and **Scan selected** is enabled, any patches that do not meet the criteria defined by the scan template filters will be removed from the group. Here's why: In Protect 9.0 and 9.1, the scan template filters can mask the fact that your patch group may contain patch types that you never intended to actually scan for or deploy. In Protect 9.2, when the patch group is used as a baseline, the scan template filters will not be applied and inaccuracies in your patch groups may be revealed. If the upgrade process detects this situation, it will automatically modify the patch group in order to preserve the intended interaction between the scan template and the patch group.

      Example:

      Assume your 9.1 patch group contains a mix of Security, Non-security and Software Distribution patches. In the scan template that references this patch group, the **Patch filter settings** section is set to **Scan selected** and the **Patch Properties** section is set to detect only Security patches. In this configuration, the **Patch Properties** filter will be honored and only Security patches will be detected (despite the fact that the patch group contains Non-security and Software Distribution patches).

      After upgrading to 9.2, the scan template will define the patch group as a Baseline filter and all other scan template filters will be ignored. If the patch group is not modified, Non-security and Software Distribution patches will now be detected (and deployed, if you enable the **Auto-deploy patches after scan** check box when performing a scan). The upgrade process will recognize this discrepancy and will remove the Non-security and Software Distribution patches from the patch group.



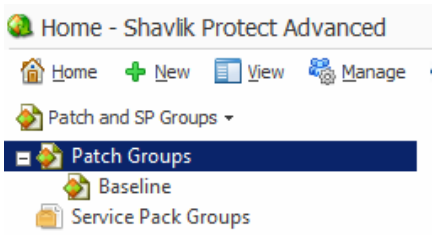
Note: Going forward, be careful to properly manage your patch groups by not adding unnecessary or unwanted patches or patch types.

- **Auto-Generated Patch Groups:** A copy of an existing patch group will be automatically generated by the upgrade process if all of the following conditions are met:
  - If the patch group is referenced within the **Patch filter settings** section of a patch scan template and **Scan selected** is enabled, and
  - If the patch group is referenced by an agent policy or by a second scan template that contains different filter definitions, and
  - If the patch group must be modified by the upgrade process to maintain compatibility (see above)

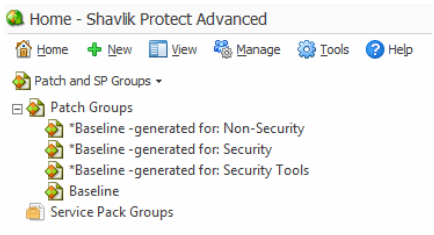
  In this situation, a copy of the patch group will be generated and then modified as described above. The name of the new patch group will be ***<patch group name> -generated for <scan template name>**. The scan template(s) that reference the patch group will be updated to use the new patch group name. The original patch group is preserved so that references to it from your agent policies or other scan templates are maintained.

  You should review the changes and, if desired, rename the auto-generated patch group to a more friendly or meaningful name.

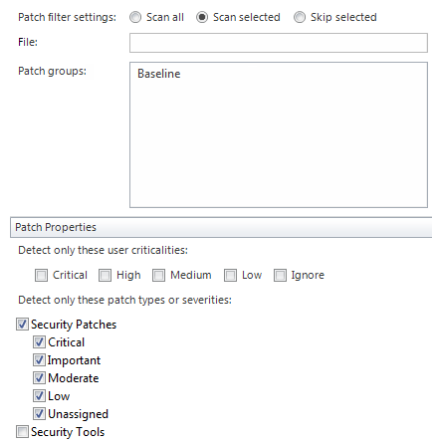
Protect 9.1 Patch Group



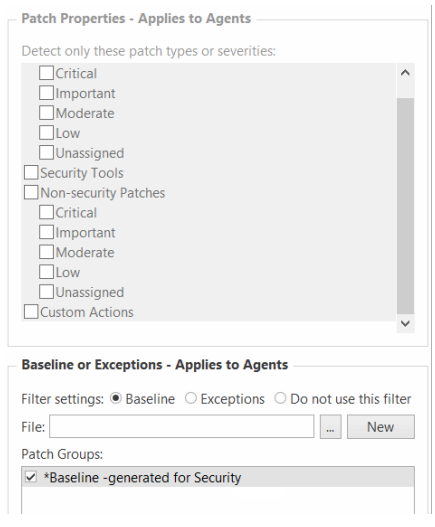
Protect 9.2 Patch Groups



Protect 9.1 Scan Template



Protect 9.2 Scan Template



Assign Aliases to the Console

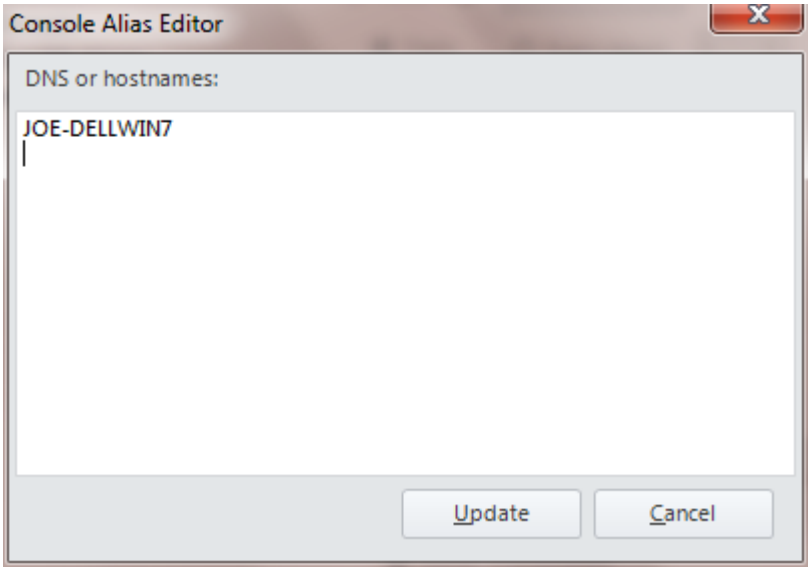
This task is necessary if one or more of the following conditions apply:

- You have assigned the console machine to a new domain
- You have given the console a new common name or IP address
- You manually installed agents and they use an IP address to communicate with the console

Under these conditions you must use the **Console Alias Editor** tool to identify the old console names or addresses as trusted aliases. If you don't, when an agent checks in with the Shavlik Protect console or when an agentless machine attempts to send patch deployment status messages to the console, they will not be able to verify that the machine they contacted is a trusted machine.

1. Select **Tools > Console alias editor**.

   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine. For example:

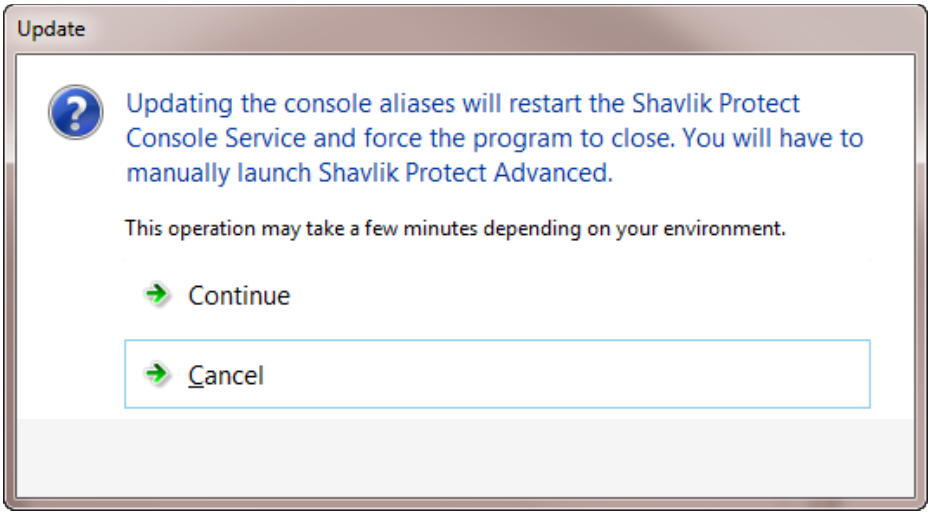


2. Type the names and/or IP addresses that you want to use as an alias for the console machine.

   You can specify IP addresses using either an IPv4 or IPv6 format.

3. Click **Update**.

   The following dialog is displayed:



In order to update the console aliases the console service must be restarted and Shavlik Protect must be closed and then manually restarted.

IMPORTANT! The agents will not recognize a new alias until after they check-in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check-in; a check-in command issued from the console to an agent will not update the console certificate.

Synchronize Your Distribution Servers

You must update your distribution servers with the latest patches and/or scan engines and XML definition files contained on the console. This is particularly important if your agents use distribution servers to download these files. The distribution servers must be synchronized with the updated console files **prior** to the agents performing their check-in.

To synchronize your distribution servers:

1. Select **Help > Refresh files** to make sure the console contains all the latest files.
2. Select **Tools > Operations > Distribution Servers**.
3. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.
4. In the top pane, select which distribution server you want to synchronize with the console.
5. Click **Add scheduled sync**.
6. Specify when you want the synchronization to occur and then click **Save**.
7. In the **Schedule automatic synchronization** pane, select the scheduled synchronization entry.
8. Click **Run now**.

Don't worry if the agents happen to check in before you have finished synchronizing the distribution servers. The agents will be updated the next time a scheduled task is run or the agent updates its binaries.

Consider Enabling the Predictive Patch Feature

This new feature enables Shavlik Protect to automatically download patches that are likely to be deployed in the near future. If you use distribution servers, you can synchronize Predictive Patch with your distribution servers so that they receive copies of the downloaded patches. The Predictive Patch option is enabled on the **Tools > Operations > Downloads** tab and it is synchronized with your distribution servers by enabling the **Synchronize with Predictive Patch** option on the **Distribution Server** dialog. See the Help system for complete details.

Re-establish Security Between Your Data Rollup Consoles

If you use multiple consoles and have a data rollup configuration in place, you must re-establish the security association between the central console and each remote console.

IMPORTANT! Once you begin the upgrade process, no data rollup activity will take place until both the central console and the remote console have been upgraded and the security association between the two consoles has been re-established. For this reason it is strongly recommended that you upgrade your consoles in tandem and at a time when you expect very little data rollup activity.

On the Central Console

1. Upgrade the central console.
2. Select **Tools Operations > Data Rollup** and verify that the **Accept and import results from a rollup sender** check box is enabled.

On Each Remote Console

1. Upgrade each remote console.
2. Select **Tools Operations > Data Rollup**.
3. Verify the IP Address/Hostname and port values of the rollup console.
4. Click **Register**.

For more information on data rollup, in the Help system see **Managing Multiple Consoles > Data Rollup Configuration**.

Scan Your Virtual Machines

If you have virtual machines defined in a machine group on either the **Hosted Virtual Machines** tab or the **Workstation Virtual Machines** tab, after performing the upgrade you must initiate a scan of these machines from either the home page or from within the machine group. You need to do this in order to re-establish the machine identities with Protect. If you do not perform the scan, the **Virtual Server** and **Path** fields may not be displayed in Machine View and deployments to these machines may fail.

Check Your Custom User Settings

The following custom user settings are not preserved during the upgrade.

- Tools > Options > Display tab:
  - Recent item (days)
  - Archive items
  - Show only items created by me
  - Show main newsfeed
  - Show informational items in patch scan results
  - Show service packs in View -> Patches
- Tools > Options > Notifications and Warnings tab:
  - Warn before scheduling deployments
  - Close Refresh Files when finished
  - Warn if Protect Cloud sync is not enabled on this console
  - Warn before opening 7 or more bulletins
- Tools > Options > Logging tab:
  - Diagnostic patch scanning
- Deployment Tracker:
  - Update speed
  - Days to show
  - Show failures
  - Show in progress
  - Show successfully completed
- Reports dialog
  - Sort by IAVA ID
- ESXi Hypervisor Bulletins tab:
  - Only show latest
- Event History
  - Limit results to previous (days)
- ITScripts Results View
  - Results since

Know That Protect 9.2 Uses a SHA-2 Root Certificate

Shavlik is introducing the use of SHA-2 root and console certificates in Protect 9.2. There are two primary reasons for this: the 2048-bit SHA-2 certificates are more secure than their 1024-bit SHA-1 predecessors, and SHA-1 root certificates are being deprecated and will stop being accepted by Windows beginning on January 1, 2017.

After you have completed the upgrade process, Shavlik Protect 9.2 will begin its own process behind the scenes for issuing a new SHA-2 root certificate and a new SHA-2 console certificate. If you are not using agents then this process will be invisible to you and can be ignored. If you are using agents, part of the process involves waiting for your agents to check in so they will receive the new pending root certificate. This process may take a few days or weeks, depending on a number of factors, but it will all play out in the background. Your only involvement may be to monitor the Event History log to see if any problems occur that require your attention.

SIGNIFICANT CHANGES AND ENHANCEMENTS IN SHAVLIK PROTECT 9.2

Complete details about each of the following topics can be found in the Help system:

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

Patch Deployments	The engine for packaging and deploying patches to machines has been completely rewritten. Performance and reliability have been improved.
Patch Content	The patch assessment and deployment data that Shavlik Protect consumes has been repackaged and improved in many ways.
Patch Scan Template Filtering	More metadata has been added to the patch content. In addition, the **Filtering** tab on the **Patch Scan Template** dialog has been updated to allow for more precision when scanning.
Patch View / Patch Group	Patch View has been completely redesigned and updated. It leverages the new content format, enabling you to view patch information in a more concise way. In addition, patch groups are now created and managed from within Patch View. This allows you to research patches and create patch groups in a more unified manner.
Scheduled Tasks	Scheduled tasks on the console now use the Microsoft Task Scheduler. A new dialog, available via the **Manage > Scheduled Console Tasks** menu, enables you to view and manage these tasks.
Reports	A new **End-of-Life by Product** report is now available. In addition, a new **Schedule Report** dialog, available via the **Tools > Schedule Report** menu, enables you to automatically generate a report at some time in the future. The report can be automatically generated once or on a recurring basis.
Predictive Patch	This new option enables Shavlik Protect to automatically download patches that are likely to be deployed in the near future. Downloading patches in advance of their anticipated deployment will help speed the deployment process.
Patch Tuesday + X (days) Scheduling	When scheduling console scans, you now have the ability to delay a recurring scan by a number of days to coincide with a regular event. For example, you might schedule a monthly patch scan to occur the day after Patch Tuesday by using the new **Add delay (days)** option.

End of Life Notification

Going forward, if the version of Shavlik Protect that you are using is nearing its end of life (EOL) date, a notification will be displayed when you start Shavlik Protect.

Protect Cloud Integration

Patch scan and deployment results can be periodically sent to Protect Cloud. If you are a Shavlik Empower user, the patch data will be periodically retrieved by Empower from Protect Cloud and the data can then be viewed using the browser-based Shavlik Empower user interface.

User Interface Changes

The following user interface items have been changed:

- Patch View has been completely redesigned.
- Patch groups are now created and managed from within Patch View.
- In Machine View:
    - The top pane contains three new columns: Virtual Server, VM Name, and Path
    - The **Virtual Assets** tab has been removed from the middle pane
    - In the bottom pane, the **Machines Missing** and **Machines Installed** tabs have been combined into one new tab named **Affected Machines**.
- On the patch deployment template:
    - Office Install Points and Original Media support has been removed
    - The **Backup files for uninstall** and **Quiet Mode** options have been removed; they are now always enabled
    - The **Distribution Servers** tab has been redesigned to help identify the order in which download sources will be used
- On the patch scan template:
    - The Filtering tab has been completely redesigned
    - User criticality has been removed
    - The Software Distribution tab only shows products that have not been superseded
- In an agent policy, all tasks are now able to be created without a recurring schedule. This allows you to define tasks that will run only via the agent user interface or by remote task initiation from the console.
- In a machine group, the **Test Existence** and the **Test Credentials** options have been combined and are implemented by performing a power status scan.
- Virtual asset summaries are no longer available from within Machine View. All virtual asset information is now available using the Virtual Inventory feature.
- Removed the Virtual Machine Hardware Detail, Virtual Machine Memory Usage, and Virtual Machine Disk Usage reports.
- In Scan View, the Scan Summary sub-pane is no longer collapsible
- Scheduled tasks are now separated into two separate dialogs: **Manage > Scheduled Remote Tasks** and **Manage > Scheduled Console Tasks**

- In **Tools > Options**:
  - **Display:** Contains a new check box named **Show service packs in View > Patches**
  - **Notifications & Warnings:** Contains a new check box named **Warn before opening 7 or more bulletins** and removed the **Warn before scheduling operations when the Default Credentials do not match the current user** check box
  - **Patch Languages:** This tab has been removed. The program now automatically detects the operating system languages used on your managed machines and downloads only those language versions of the patch file that are needed.
  - **Scans:** Contains a new check box named **Always enforce machine group exclusions**
  - **Deployment:** Removed the **Deployment Tracker address** option. The address is now defined using the **Console Alias Editor**.
  - **Logging:** Contains a new check box named **Diagnostic patch scanning**