

Upgrade Guide

Shavlik NetChk[®] Protect 7.8



Copyright

Copyright © 2009 – 2011 Shavlik Technologies, LLC. All rights reserved.

No part of this document may be reproduced or retransmitted in any form or by any means electronic, mechanical, or otherwise, including photocopying and recording for any purpose other than the purchaser's personal use without written permission of Shavlik Technologies.

Trademarks

Shavlik NetChk Protect, Shavlik NetPt Agent, Shavlik NetChk Limited, and Shavlik NetChk Deployment Tracker are registered trademarks of Shavlik Technologies. The Shavlik Technologies logo is a trademark of Shavlik Technologies. Microsoft, Windows, and Microsoft Baseline Security Analyzer are registered trademarks of Microsoft Corporation.

All other trademarks, tradenames, or images mentioned herein belong to their respective owners.

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. Remove “fully licensed” statement.

WELCOME

Purpose of this Guide

Welcome to Shavlik NetChk Protect 7.8. This document describes how to upgrade from NetChk Protect 6.x, 7.0, 7.1, 7.2, 7.5, or 7.6 to NetChk Protect 7.8. If you are currently using a version that is older than NetChk Protect 6.5.3, you must first upgrade to 6.5.3 before upgrading to 7.8.

In addition to describing the upgrade procedure, this document lists a number of functional differences you should be aware of when upgrading to Protect 7.8. It also highlights the areas in the user interface that have changed significantly.

System Requirements and Prerequisites

Please note the following new console requirements and prerequisites for NetChk Protect 7.8.

- As of NetChk Protect 7.0, Windows 2000 is no longer supported for use as a console.
- As of NetChk Protect 7.0, Windows Vista, SP1, Business, Enterprise, or Ultimate Edition, is supported for use as a console.
- As of NetChk Protect 7.1, Visual C++ 2008 SP1 Redistributable Package Run Time components are provided in the installation package.
- As of NetChk Protect 7.1, SQL Server 2000 is no longer supported as a back-end database.
- As of NetChk Protect 7.2, Windows 7, Professional, Enterprise, or Ultimate Edition, is supported for use as a console.
- As of NetChk Protect 7.5, VMware Virtual Disk Development Kit is no longer a requirement.
- Windows Installer 4.5 or later is required if you are using SQL Server 2008.
- As of NetChk Protect 7.8, SQL Server 2008 R2 Express Edition is installed if you do not have SQL Server (it supports larger databases than the earlier edition).
- As of NetChk Protect 7.8, Microsoft .NET Framework 4.0 is now required. If you are using Windows XP this means you must be at SP3 or later.

All missing software prerequisites will be automatically installed during the upgrade process.

UPGRADE PROCEDURE

This section describes how to upgrade from Shavlik NetChk Protect version 6.x, 7.0, 7.1, 7.2, 7.5, or 7.6 to Shavlik NetChk Protect 7.8. If you are taking this opportunity to move the console to a new machine, you should perform the upgrade before moving to the new machine.

Before performing the upgrade, be sure to read the *Functional Differences* section so you are aware of how the upgrade will affect your system.

Note: If you are currently using a version that is older than 6.5.3 you must upgrade to version 6.5.3 before upgrading to version 7.8. Use the following link to download version 6.5.3:

<http://www.shavlik.com/downloads.aspx>

If you are upgrading from version 7.0, 7.1, 7.2, 7.5, or 7.6, please skip to Step 6.

1. (Optional) If you are using agents, make sure the distribution servers they are using have the most up-to-date information by doing the following:
 - A) On the Shavlik NetChk Protect 6.x console, download the latest versions of the XML files by selecting **Tools > Refresh Files**.
 - B) Select **Tools > Distribution Servers** and then select the **Synchronize** tab.
 - C) Select all the distribution servers in the available list and then click **Synchronize Engines and XML**.
2. On the Shavlik NetChk Protect 6.x console, select **Tools > Manage Items** and delete any older data that are no longer needed.
3. (Optional) If you are a NetChk Spyware user, for auditing purposes you should consider generating reports to capture the latest spyware status.
4. Close the Shavlik NetChk Protect 6.x console program by selecting **File > Exit**.

If you have multiple consoles connected to the same SQL database, close all consoles and stop all NetChk Patch Services connected to the database.
5. Compress the database used to store scan results, patch deployment results, and signature remediation results:

You can do this in SQL Server Management Studio by right-clicking the ShavlikScans database and selecting **Tasks > Shrink > Database**. For additional database maintenance information, see:
<http://supportteamblog.shavlik.com/2010/01/13/sql-database-maintenance/>
6. Create a backup of your current database using SQL Enterprise Manager.
7. Close all programs running on the console machine.
8. Download the Shavlik NetChk Protect 7.8 executable file to your console machine using the following link:

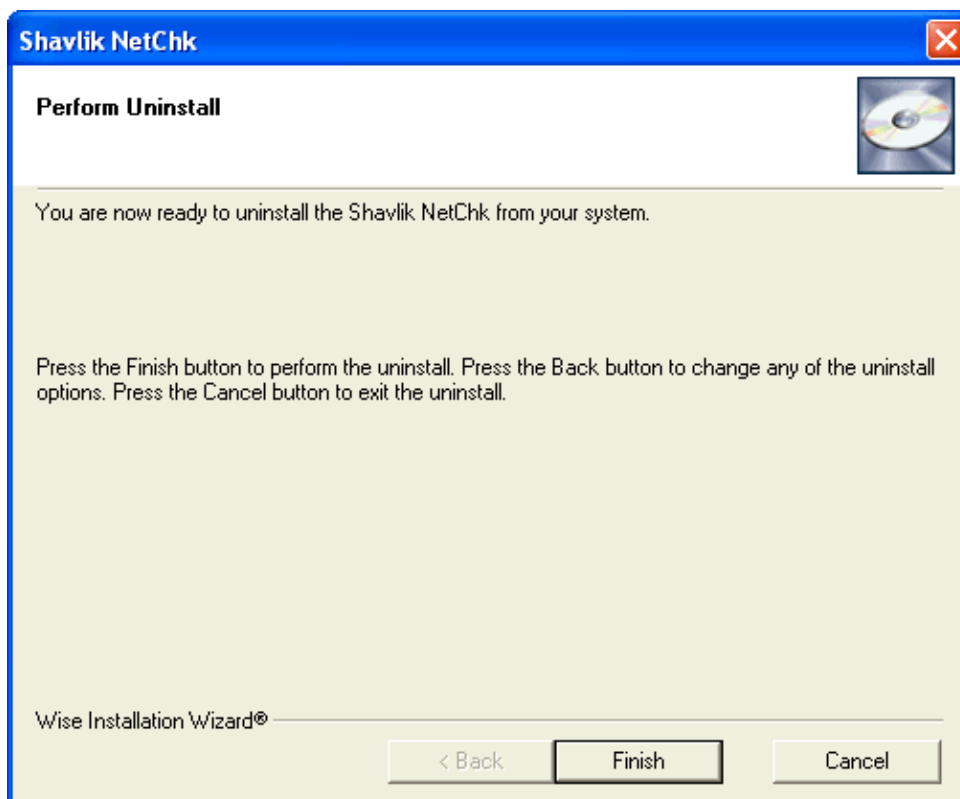
<http://www.shavlik.com/downloads.aspx>

9. Begin the installation process using one of the following methods:
- Double-click the file named **NetChk_Protect_Setup_7.8.0.#.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 `DBCMMANDTIMEOUT` option is used to specify the SQL command timeout value during installation. The default value is 1800 seconds (30 minutes). The recommended value is 15 minutes per GB, so if you have a 4 GB database you should increase the timeout value to 3600 seconds (60 minutes). For example:

```
NetChk_Protect_Setup_7.8.300.1 /wi:"DBCMMANDTIMEOUT=3600"
```

10. On the **Shavlik NetChk x.x has been detected on your system. Would you like to upgrade?** dialog, click **Yes**.

The **Perform Uninstall** dialog is displayed.



11. On the **Perform Uninstall** dialog, click **Finish**.

Your current version of NetChk Protect will be uninstalled. When the uninstall is complete a dialog similar to the following is displayed.



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

The Setup Wizard may need to perform a reboot during this portion of the installation process if the Microsoft .NET Framework 4.0 requirement is missing. If a reboot is required, when the machine is restarted the NetChk Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

The **Welcome** dialog is displayed.

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

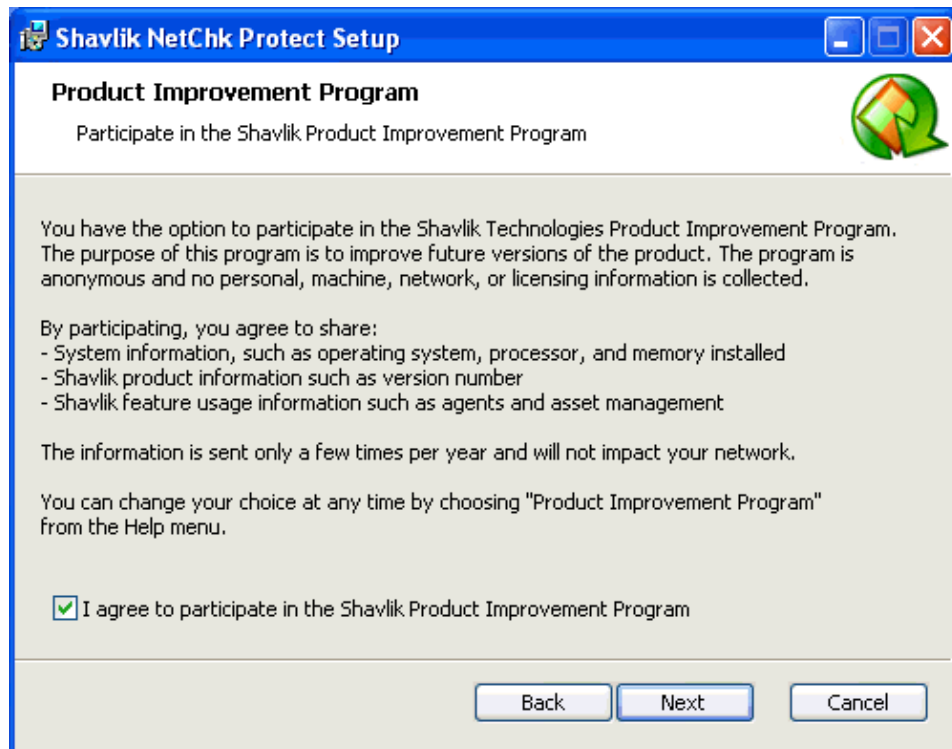
The license agreement is displayed. You must agree to the terms of the license agreement in order to install the program.

14. To continue with the installation click **Next**.

The **Destination Folder** dialog is displayed.

15. 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.



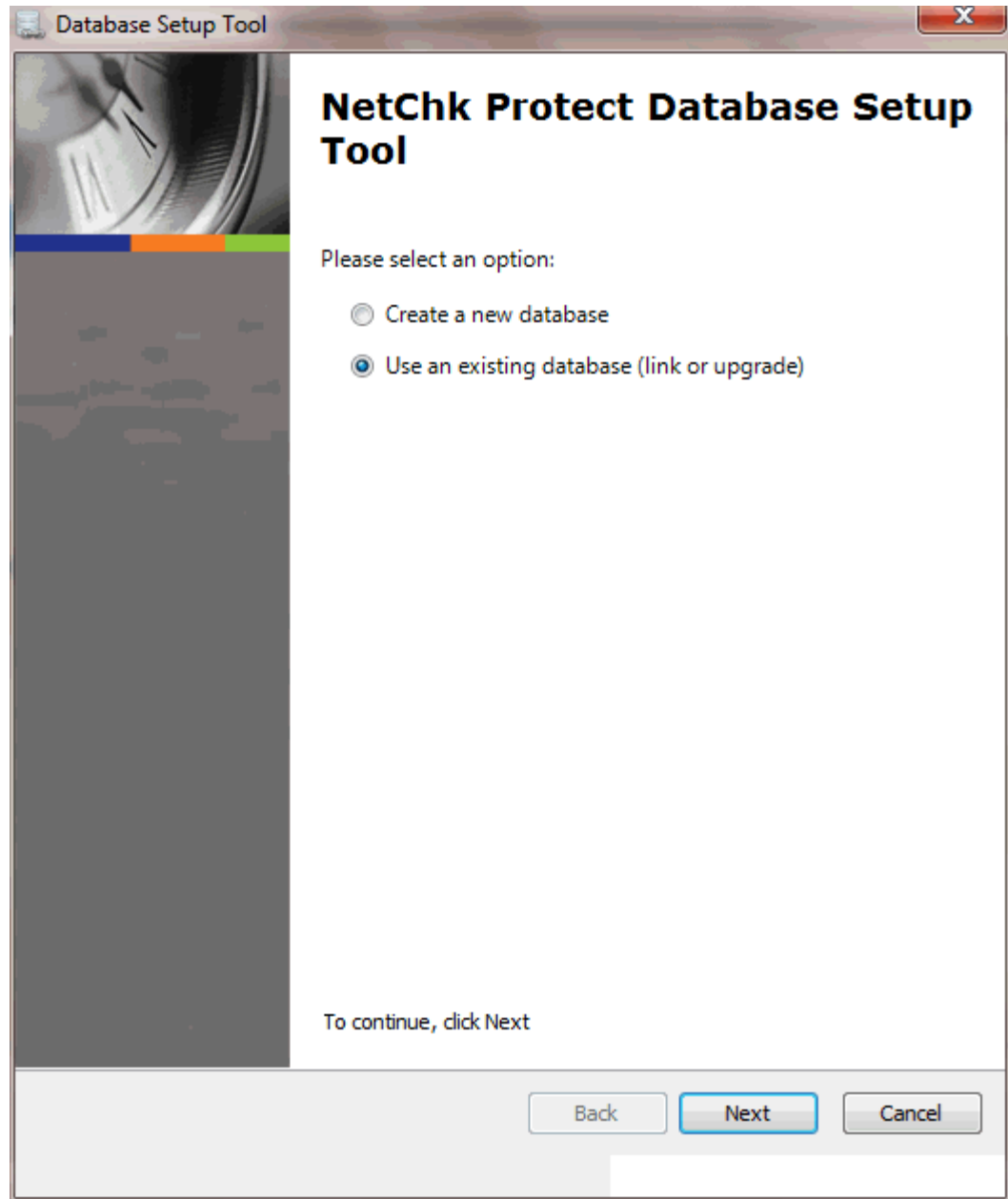
Read the description and decide if you agree to participate in the program. The program enables Shavlik Technologies to collect product usage information that will help improve future versions of the product.

16. Click **Next**.

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

17. 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.

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

A dialog similar to the following is displayed:

Database Setup Tool

SQL Database Configuration
Please define how Shavlik NetChk will connect to your existing product database. This database will be upgraded to version 7.6.

Choose a database server and instance

Server name: VM-LS-2K3E\SQLEXPRESS

Database name: ShavlikScans 6.5(489)

Choose how interactive users will connect to the database

Authentication method: Integrated Windows Authentication

User name:

Password:

Test database connection

Choose how services will connect to the database

Using Integrated Windows Authentication with remote databases requires Kerberos.

Use alternate credentials for console services

Authentication method: Integrated Windows Authentication

User name:

Password:

Back Next Cancel

19. 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 **ShavlikScans**.

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. NetChk 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 **NetChk Protect Administration Guide** for more information about local machine credentials.) All NetChk 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 Server 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.

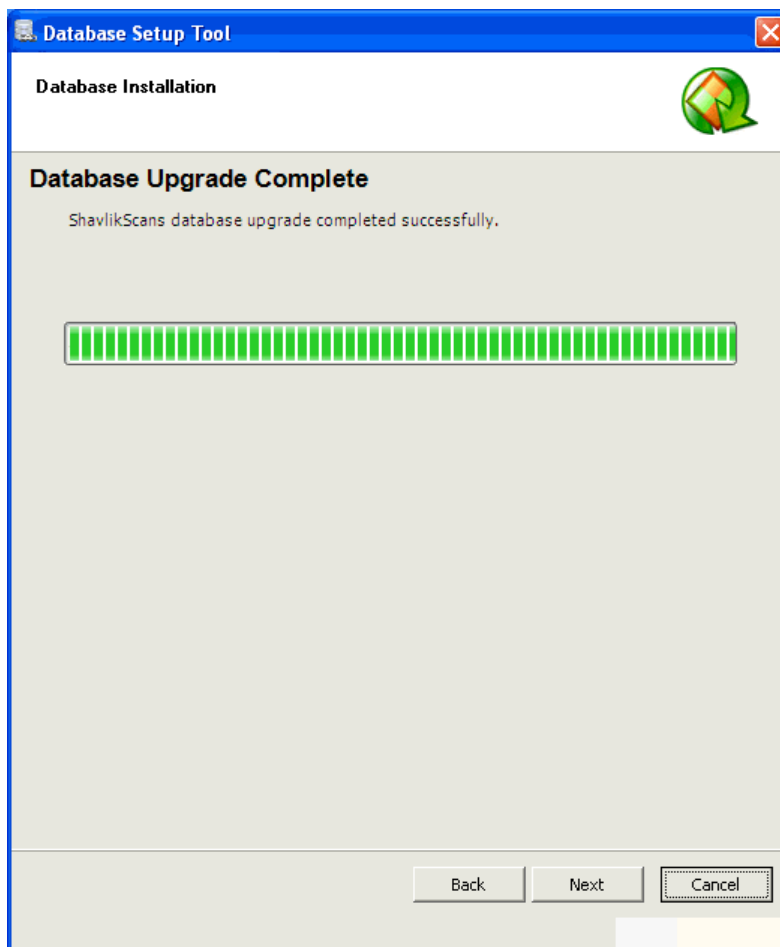
- **Use alternate credentials for console services:**
 - If the SQL Server database is installed on the local machine you will typically ignore this option by **not** enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will 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 *NetChk Protect 7.8 Installation Guide* for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the NetChk Protect upgrade process but before you start the program.

- **Specific Windows User:** Select this option to enter a specific user name and password combination. NetChk 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.
20. After providing all the required information, click **Next**.

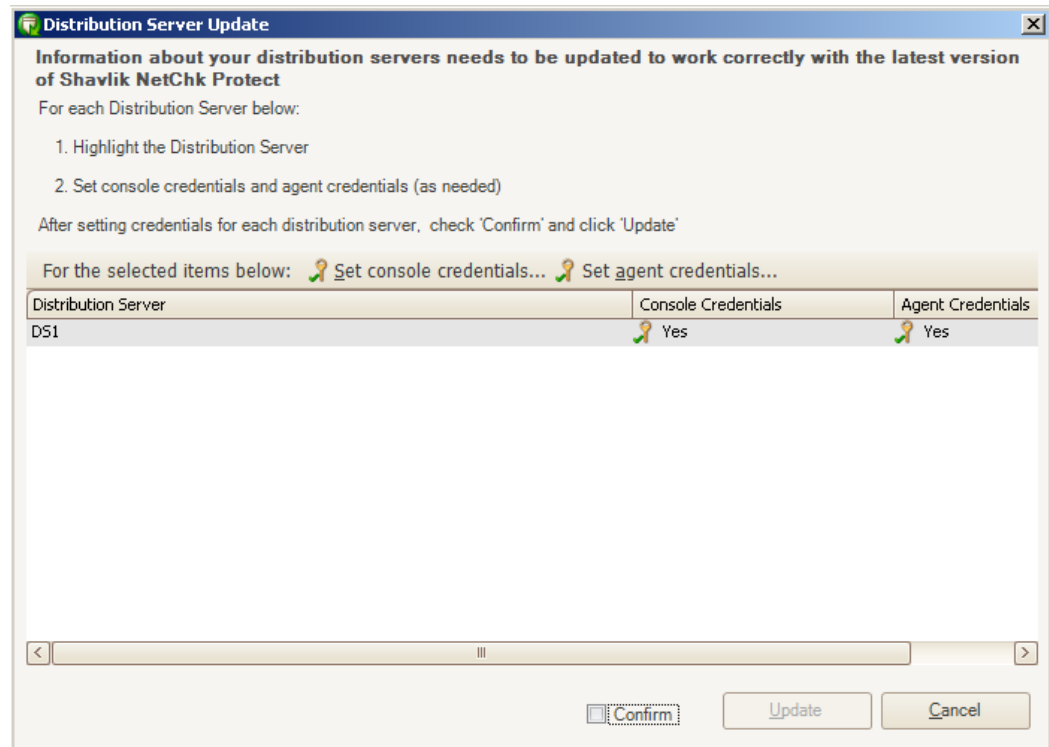
Note: If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

Your database is upgraded to the 7.8 format. When the database upgrade is complete the following dialog is displayed:



21. Click **Next**.
22. On the **Installation Complete** dialog click **Finish** and follow the setup wizard prompts to complete the installation.

23. Start Shavlik NetChk Protect.
24. (Optional) If you are using agents, the **Distribution Server Upgrade** dialog is displayed. For example:

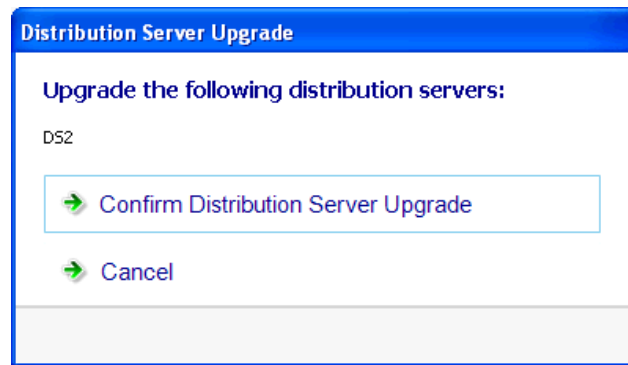


This dialog is used to reapply the credentials used by the console and by the agents when connecting to your distribution servers. It will also put the mechanisms in place to inform the agents that they need to upgrade themselves.

Important! Don't be fooled if the key icon indicates that credentials are already applied. You must reapply the credentials by performing the following steps or the upgrade will fail.

- A) Select the distribution server you want to update. If the same credentials are used by multiple servers you can select multiple servers.
- B) Click **Set console credentials** and specify the credentials used by the console to connect to the selected distribution servers.
- C) Click **Set agent credentials** and specify the credentials used by the agent machines to connect to the selected distribution servers.
- D) Repeat Steps A – C until you have specified credentials for all of your servers.
- E) Enable the **Confirm** check box and then click **Update**.

A dialog similar to the following is displayed:



F) Click **Confirm Distribution Server Upgrade**.

The distribution servers are updated for 7.8. When the upgrade is complete the NetChk Protect home page is displayed.

25. Verify that all the console data looks correct.

26. Synchronize all your distribution servers.

This is the trigger that will begin the process of upgrading your full agents. When the agents check in they will be upgraded to the new policy format.

A) Select **Manage > Distribution Servers** and then select the **Synchronize** tab.

B) Select all the distribution servers in the available list and then click **Synchronize engines and definitions**.

27. Run a test scan to verify that everything is working correctly.

28. Upgrade other consoles as needed.

FUNCTIONAL DIFFERENCES BETWEEN 6.X AND 7.X

Background Services

If in 6.x you defined a user account that was used by NetChk Protect background services to connect to a remote SQL Server, that account can no longer be used. This is because all services in 7.x must run as LocalSystem. You must instead create a new machine account on the remote SQL Server that will accept Windows authentication credentials from the NetChk Protect console. For detailed instructions on creating this account, open the NetChk Protect Help system and read the topic **Installation and Setup > Installation > SQL Server Post-Installation Notes**. This information is also available in the *Shavlik NetChk Protect Installation and Setup Guide*.

After creating this account you should restart the background services to ensure that they are connecting properly to your remote SQL Server. You can do this using the Windows **Control Panel > Administrative Tools > Services** dialog.

Approved Patch Lists

Any approved patch lists you may have created for use with a patch agent in version 6.x will be converted to patch groups during the upgrade process. This is because it is no longer necessary to create approved patch list files in version 7.x. You can now use a patch group to define your approved patches. The names of the patch groups will be similar to the names you used for the patch lists in 6.x. The patch groups will be referenced in your new agent policy on the **Patch Tasks** tab.

Signature Groups

Signature groups no longer apply in NetChk Protect 7.x and will not be migrated to the new interface.

Spyware Templates & Remediation Templates

Spyware templates and remediation templates no longer apply in NetChk Protect 7.x and will not be migrated to the new interface.

6.x Spyware Data is Not Migrated

Any spyware data contained in your 6.x database will not be migrated to 7.x. The method used for detecting spyware is completely different in 7.x and the 6.x data is not compatible. The threat management capabilities in 7.x are new, improved, and much more complete. One of your first tasks after upgrading to 7.x should be to create an agent policy with threat management capabilities, install the agents on your target machines and perform a threat scan.

Distribution Servers per IP Address map option

The **Distribution Servers based on IP range** option has been removed from the following three areas:

- **Tools > Options > File Download > Standard**
- **Tools > Options > File Download > User-Defined**
- **Tools > Options > File Download > Patches and Service Packs**

The reasoning here is a console will never need to download from more than one distribution server, and the option is therefore unnecessary.

If you selected the **Distribution Servers based on IP range** option in NetChk Protect 6.x, after the upgrade process is complete the download location will be set to the first distribution server listed as an option.

Note: It continues to make sense for target machines and agents to download from distribution servers by IP range, and this ability is still available when configuring your distribution server.

6.x Agent Policies are Upgraded to 7.x Agent Policies

Your 6.x agent policies are upgraded to 7.x agents as follows:

- Patch-enabled agents will be converted to an equivalent agent patch task in 7.x. The policy name will be appended with the term (upgraded) to identify it as an upgraded policy.
- Spyware-enabled agents will be converted to an equivalent agent threat task in 7.x. The **WUScan** template will be used and all scheduling options will be preserved. The default action for all detected threats will be **Report Only**. If **Real-Time Protection** was enabled in 6.x then **Active Protection** will be enabled in 7.x.

Agent Status May Initially Show Out of Date

In 7.x, agent status is displayed in Machine View. If the upgraded agents have not checked in since the upgrade was performed, the agent information in Machine View will be out of date. The default check-in period is 120 minutes (two hours) so the status of most agents should be updated relatively quickly. Agents that reside on machines that are offline, however, will remain out of date until the machines come online and a check-in can occur.

NetChk Limited Agents are Removed

Agents are not supported in NetChk Limited 7.x and are removed during the upgrade process.

Limiting Agent-based Patch Scanning to Certain Patch Types

Prior to 7.x, agent patch scanning could be limited to certain patch types by creating an optional local registry value named **AgentPatchTypeSuppress**. This value was located in the registry path **HKEY_LOCAL_MACHINE\SOFTWARE\Shavlik\HFNetChkPro4**. This registry value is now obsolete.

Patch type scanning is now controlled much more easily using a patch scan template. On the **Filtering** tab set the **Patch type filter settings** option to **Scan Selected** and then specify the desired patch types. You then simply reference this custom patch scan template on the **Patch Tasks** tab in the Agent Policy Editor.

Shavlik Scheduler May Require Updating

If you experience problems using the Scheduled Tasks Manager to communicate with your machines, it could be you need to install the latest version of the Shavlik Scheduler on your machines. The installation will happen automatically whenever a deployment is performed, or you can do it manually by performing the following steps:

1. From within the Scheduled Tasks Manager, right-click the desired machine and select **Scheduler Service > Install**.
2. Type the user name and password of an account on the machine that contains administrative privileges.
3. Click **Install**.

See **Common Tasks > Using the Scheduled Tasks Manager > Installing the Shavlik Scheduler** in the Help system for more details.

Data Rollup Configuration Will Need to be Reset

If you were using the data rollup feature you will need to reset your data rollup configuration settings on the central console and on each remote console. This is a very simple process and is described in the Help system at **Managing Multiple Consoles > Data Rollup Configuration > Implementing a Data Rollup Configuration**.

SIGNIFICANT ENHANCEMENTS IN NETCHK PROTECT 7.X

Navigation Bar Enhancements

(Version 7.0 or later)

The navigation bar now consists of an active function pane at the top and a button tray at the bottom. The button tray contains buttons representing each of the major functions within the program. To work with a function, simply click the desired button in the button tray. The function is displayed within the active function pane at the top of the navigation bar.

Home Page Enhancements

(Version 7.0 or later)

The home page has an entirely new look and feel. The biggest change is the addition of charts that show the security status of the machines in your network. Also new is a **How Do I ...?** List that contains links to Help topics that explain how to quickly get started performing a number of common tasks. The announcement area has been moved to the top-right corner of the home page. **Previous** and **Next** buttons enable you to scroll through all the available messages.

Menu Changes

(Version 7.0 or later)

The menu command has been totally reworked. Some of the command names have changed to better represent their function. Other commands have been moved to more logical locations. Commands that no longer apply have been removed. For example, all spyware-related commands have been removed as the antispyware functionality is now available as part of the improved agent-based threat management capability.

You should take a few minutes to click on each menu and review the available commands.

Toolbar Changes

(Version 7.0 or later)

There are fewer toolbar buttons in 7.x. There are two reasons for this:

- Several of the 6.x spyware buttons no longer apply in 7.x.
- Some seldom-used buttons have been removed. The buttons that remain represent the most commonly used features and functions.

Machine Group Enhancements

(Version 7.0 or later)

Machine groups are presented in a whole new manner. The new method enables easier grouping and sorting of members. It also provides a scalable view of all machines in the group. Finally, you can right-click on a machine from within Machine View or Scan View and add the machine to an existing machine group.

Machine-Centric View is Now Machine View

(Version 7.0 or later)

Machine-Centric View is now named Machine View. It has been reworked and now contains three unique panes rather than two, enabling it to provide more information about the selected items. It also contains improved search, sort, and filtering capabilities.

New Patch View

(Version 7.0 or later)

A new and important addition to 7.x is Patch View. Patch View replaces the Patch Information list that was available in 6.x.

Patch View is an extremely powerful and flexible tool. It enables you to display detailed information about every product patch contained in the XML patch data file. It organizes the information so it is displayed in one comprehensive view, regardless of when the patches were released.

The benefits of Patch View include:

- You can quickly and easily display the list of products supported and the associated patches with each product
- You can display detailed information about any patch
- You can filter the information and drill down into the table for a more detailed analysis
- You can search for specific patches or patch components
- You can perform actions on each patch
- You can quickly determine which machines have a selected patch installed or are missing a selected patch

Agent Enhancements

(Version 7.0 or later)

Shavlik NetPt[®] Agent has a much different look and feel than it did in version 6.x. Agent policies are now configured using the Agent Policy Editor. There are now many more features that can be configured within an agent policy. The biggest change involves the threat management capabilities, which now includes much more than just antispyware. You are now able to detect and remediate malware of all types, including viruses, spyware, worms, rootkits, and more.

The agent-based Active Protection feature has also been enhanced. It now can monitor all files and areas on the agent machine and instantly warn the user if it detects a threat.

Other changes to note include:

- Agents no longer require the use of a distribution server; a server is optional.
- You no longer need to create a separate approved patch list file for patch management tasks. You are now able to use a patch group to define your approved patches.
- Agent results are no longer reported and logged in the Today's Items list. Agent results are instead monitored using the Operations Monitor and Machine View.
- As of version 7.x, agents can be used to perform all major program functions (patch, threat, asset, and power management).

Agent Client GUI

(Version 7.0 or later)

The agent client program used by users on the agent machines has been completely rewritten. It is now much more complete, robust, and user-friendly. It allows the user to monitor the agent as it protects the machine. The user can now initiate their own patch, asset, and threat scans, and they can manage the contents of the quarantine directory.

Patch Group Enhancements

(Version 7.0 or later)

The patch group dialog now has an updated look and feel. It also contains more information about each patch in the group, including:

- Bulletin ID
- Bulletin Date
- Qnumber
- Patch Type
- Bulletin Title

Patch Scan Templates

(Version 7.0 or later)

The **Filtering** tab on the patch scan template has a new look to it but all the original functionality is still there. One of the many improvements is that the filters are reordered to better indicate their order of precedence. This is important when using multiple filters. Be sure to read the **Creating a New Patch Scan Template** Help topic for complete information on filter precedence.

Background Tasking

(Version 7.0 or later)

Version 7.x now enables multiple tasks to run at the same time. You can simultaneously perform scans, deploy patches, download files, install agents, and keep on working.

Auto Sync of Distribution Servers

(Version 7.0 or later)

You can configure NetChk Protect so that all your distribution servers are automatically synchronized with the console. If auto sync is enabled, the default synchronization period is three times a day (every 8 hours), although this value is configurable.

Scheduled Data File Downloads

(Version 7.0 or later)

Enabling this feature will cause the program to automatically check for and download updated engines, XML files, and data definition files to the console on a regular basis. This can speed your scan processes by making the necessary files available in advance of a scan.

NetChk Operations Monitor

(Version 7.0 or later)

The NetChk Operations Monitor is new in 7.x. It is designed to give you a single console from which to monitor background tasks. The background tasks currently monitored include patch and asset scans, power management tasks, agent installations, and test patch deployments. The Operations Monitor is automatically displayed whenever an agent installation or test patch deployment is performed. To manually access the Operations Monitor, select **View > Operations Monitor**.

File Locations

(Version 7.0 or later)

In 6.x all files were located in the **C:\Program Files\Shavlik Technologies** directory. In 7.x many files now reside in one of the following:

- On Windows Vista and other newer operating systems: *C:\Program Data\Shavlik Technologies*.
- On earlier Windows operating systems like Windows XP: *C:\Documents and Settings\All Users\Application Data\Shavlik Technologies*.

AutoUpdate Feature Change

(Version 7.0 or later)

The AutoUpdate feature has been changed in 7.x. It is no longer configurable via the **Tools > Options** menu. It has been simplified to instead always check for updates when the program is started. You can also do this manually by selecting **Help > Check for Program Updates**.

Asset Management

(Version 7.1 or later)

A new asset management feature is provided in NetChk Protect 7.1. It enables you to track your software, hardware, and virtual assets. The feature works with both physical and virtual machines. You can perform scans to detect and categorize the software and hardware contained on your physical and online virtual machines. You can also scan for the properties of your online and offline virtual machines. Detailed information about your software, hardware, and virtual assets is available immediately following a scan. You also have the ability to create reports that can be used to track your asset inventory over time.

Power Management

(Version 7.5 or later)

The power management function enables you to control the power state of the machines in your organization. The primary reasons for using power management are to:

- Prepare your machines for maintenance tasks
- Reduce power consumption and noise
- Reduce operating costs
- Prolong battery life

You can shut down, restart, or wake up machines either immediately or on a scheduled basis. You also have the ability to put machines into a sleep or hibernate state.

Note: Power management (which includes Wake-on-LAN) is a separately licensable function. Contact your sales representative or sales@shavlik.com to add this function to your Shavlik NetChk Protect license.

Improved Patch Scan Results (Scan View)

(Version 7.5 or later)

The patch scan results are now displayed in a manner that is very similar to Machine View. The results are presented in a grid that contains three separate panes. Each pane displays unique information and provides unique functionality. The panes are interrelated in that the information presented in a lower pane is dependant on what is selected in the pane directly above it. This "top down" approach means you use the top pane to view high-level information and the two lower panes to drill down to more detailed information.

Virtual Machine Improvements

(Version 7.5 or later)

Virtual machine capabilities have been extended as follows:

- You can perform a software asset scan on an offline virtual machine.
- You can perform a patch scan and patch deployment on an online virtual machine even if the machine was defined in a machine group as an offline virtual machine hosted on an ESX server.

Threat Events View

(Version 7.6 or later)

Threat Events View provides a way to view all the threat tasks and Active Protection events that have occurred on your agent machines. It displays all threat events that have ever been reported to the console by your agents, providing a complete historical record for your organization. Compare this to the **Threats** tab available within Machine View, which displays only the most current threat task event information and does not display Active Protection information.

Antivirus & Patch Improvements

(Version 7.6 or later)

Antivirus and patch capabilities have been extended as follows:

- You can remotely manage the contents of an agent's quarantine directory from the console.
- You can configure a NetPt Agent policy to never allow specific files, to always allow specific files, and to always allow specific folders.
- You can use the new **Alerts Options** dialog to automatically send an e-mail message whenever one or more Active Protection thresholds are reached.
- The user of an agent machine can initiate an antivirus scan on a specific file, folder, or drive on the machine.
- A new Threat Protection Status Report has been added.
- You can send a number of different ad-hoc commands from the console to your agents. For example, you can command your agents to check-in, to update all binaries and XML data, and to clear their patch counters if an install fails after multiple attempts.
- Patch scan performance has been increased by caching the dynamic product detection (DPD) data.

Virtual Machine Improvements

(Version 7.8 or later)

Virtual machine capabilities have been extended as follows:

- You can scan and patch VMware templates
- You can take pre- and post-deployment snapshots of hosted virtual machines
- You can deploy to a virtual machine in a different state than was scanned
- You can schedule deployments to offline virtual machines
- NetChk Protect will disable networking while deploying to offline virtual machines

Service Pack Support in Agents

(Version 7.8 or later)

Service Pack Groups are introduced in NetChk Protect 7.8 so that administrators can approve service packs to be deployed to agents. The Agent Policy Editor / Patch Task page now includes a section for allowing service packs to be installed on agents. The agent UI now refers to service packs as well as patches.

GUI and Performance Enhancements

(Version 7.8 or later)

A number of improvements have been made in the following areas:

- The navigator pane has been reorganized. The nine choices at the bottom of the pane in NetChk Protect 7.6 have been reduced to six in NetChk Protect 7.8.
- In previous versions you could only edit machine properties for one machine at a time. This has been extended to allow you to edit certain properties for all selected machines.
- You now have the option to reduce Active Protection overhead by choosing to scan only high-risk file types (as defined by SunBelt) during file access. This choice can be made in the Agent Policy Editor on the **Active Protection** tab.
- Initial database data import is much faster. On start-up, you are no longer prompted to import data into a new database. The import will take place in the background without prompting the user.
- Asset scan results import is faster and consumes much less space in the database.

Database Maintenance

(Version 7.8 or later)

You can now clean up the database with a few clicks and/or schedule a cleanup to occur automatically on a weekly basis. The maintenance tasks include:

- Delete old results
- Rebuild your SQL Server indexes
- Create backup copies of your database and your transaction log