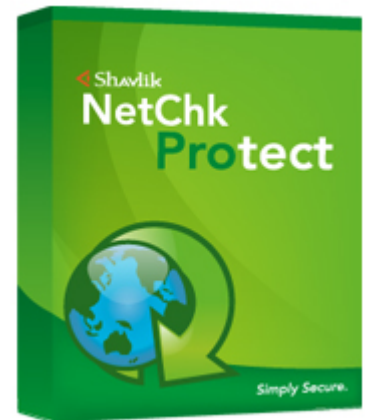


Upgrade Guide

Shavlik NetChk Protect 7.x



Copyright

© 2009 Shavlik Technologies. 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 HFNetChkPro Plus, Shavlik NetChk Limited, Shavlik NetChk Configure, and PatchPush Tracker are registered trademarks of Shavlik Technologies. Shavlik Security Intelligence and the Shavlik Technologies logo are trademarks 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 .

WELCOME

Purpose of this Guide

Welcome to Shavlik NetChk Protect 7.x. This document describes how to upgrade from NetChk Protect 6.0, 6.1, or 6.5 to NetChk Protect 7.x. If you are using NetChk Protect 5.9 you must first upgrade to 6.5 before upgrading to 7.x.

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.x. 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.x0.

- You must be using a fully licensed edition of NetChk Protect. If you are using a Limited, Audit, or Trial edition the upgrade will not be successful.
- Windows Vista, SP1, Business, Enterprise, or Ultimate Edition, is now supported for use as a console. Windows 2000 is no longer supported for use as a console.
- SQL Server 2008 and SQL Server 2008 Express Edition are now supported.
- Windows Installer 4.5 or later is required if you are using SQL Server 2008.
- Microsoft .NET Framework 3.5 is now required. If you are using Windows XP this means you must be at SP3 or later.
- Visual C++ 2008 SP1 Redistributable Package Run Time components are now required.

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 to Shavlik NetChk Protect 7.x. 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 using version 5.9 you must upgrade to version 6.5 before upgrading to version 7.x. Use the following link to download version 6.5:
<http://www.shavlik.com/downloads.aspx>

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**.
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.x executable file to your console machine using the following link:

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

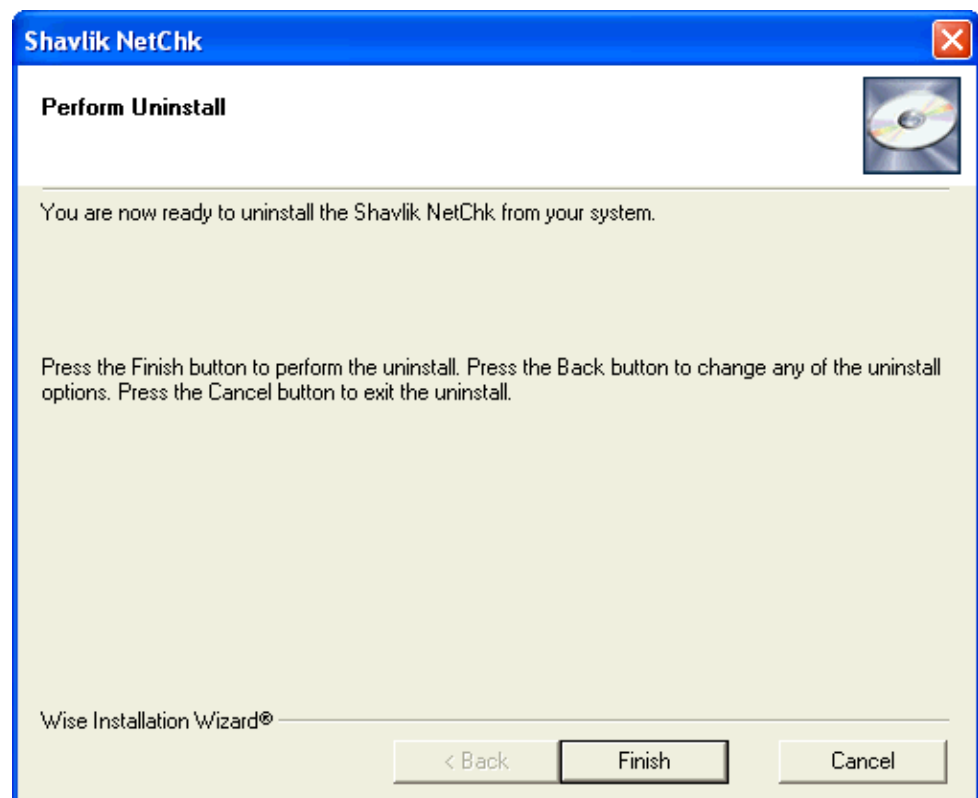
9. Begin the installation process by double-clicking the file you just downloaded to your console machine.

The file will be named **NetChk_7.x.0#.exe**.

Important! Once you begin, do not cancel out of the installation wizard at any time. If you do, you must contact our Technical Support group for instructions on restarting the upgrade.

10. On the **NetChk Protect 6.x is already installed. Would you like to upgrade?** dialog, click **Yes**.

The **Perform Uninstall** dialog is displayed.



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

NetChk Protect 6.x 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 3.5 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**.

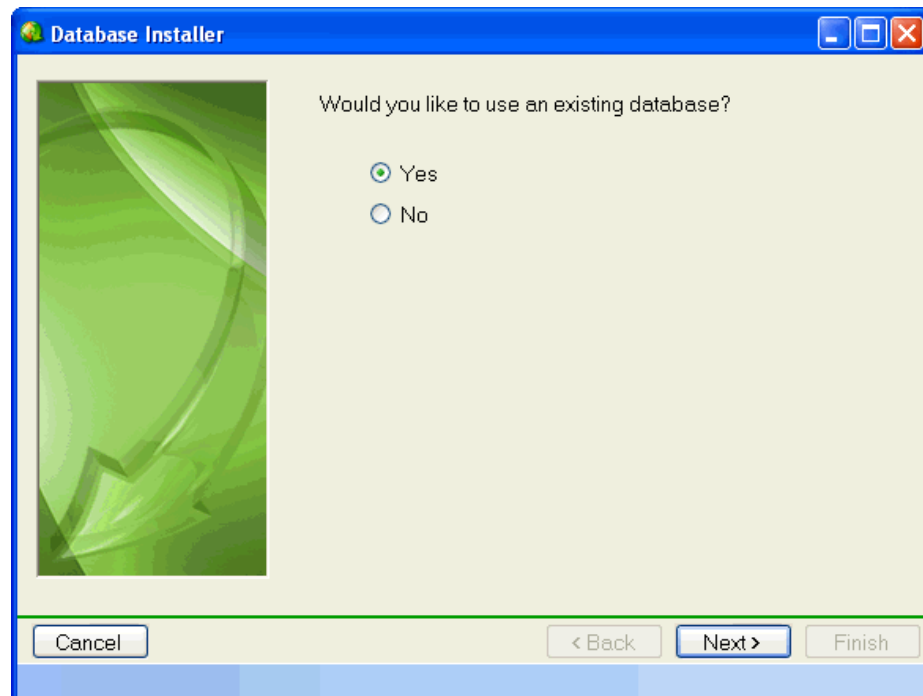
The **Destination Folder** dialog is displayed.

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 **Ready to Install** dialog is displayed.

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

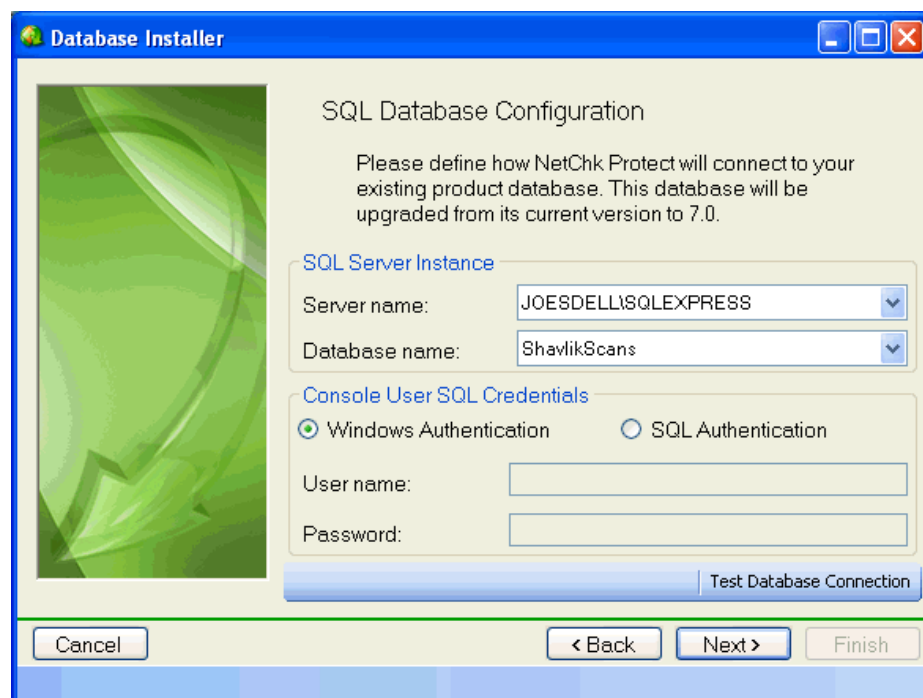
17. Near the end of the installation the **Would you like to use an existing database?** dialog is displayed.



18. Select **Yes** and then click **Next**.

Important! Be sure to select **Yes**. If you select **No** a new database will be created and your existing data will not be used.

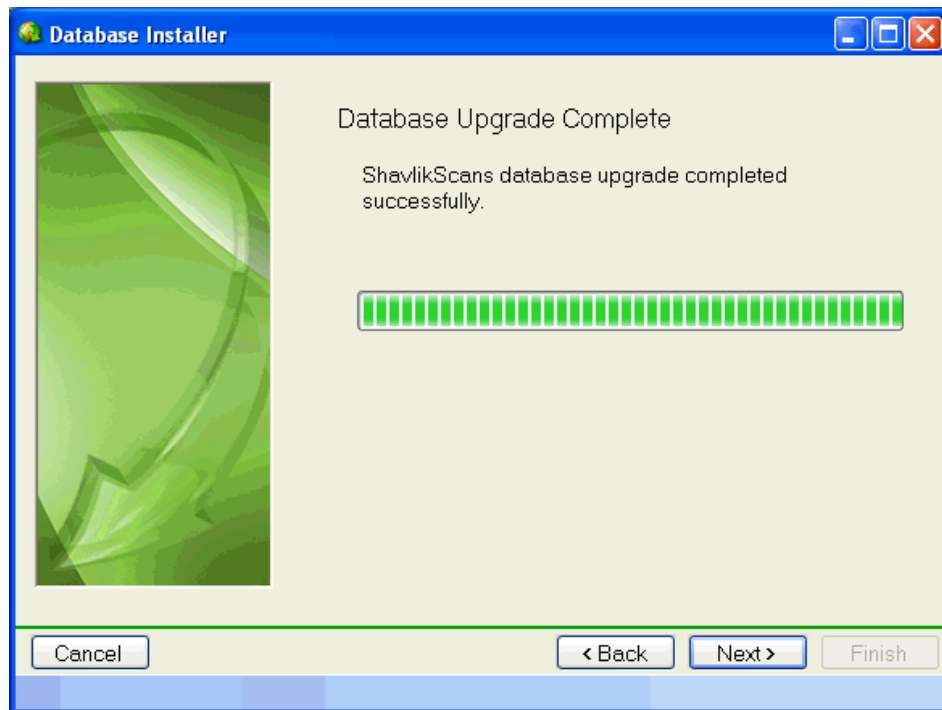
19. On the subsequent dialog, specify the existing server and database names. For example:



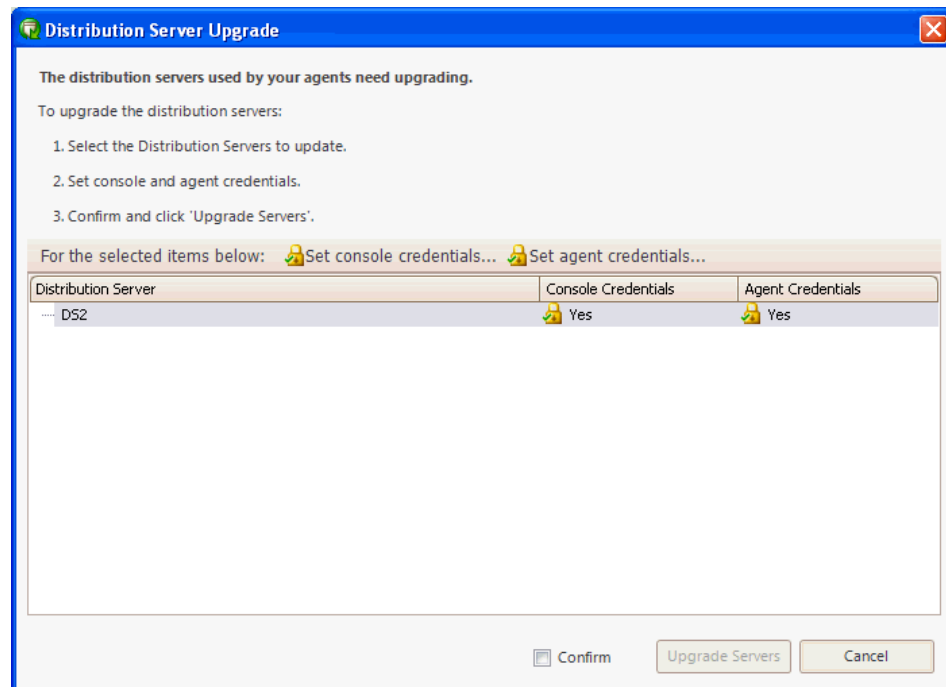
- **Windows Authentication:** This is the recommended and default option. NetChk Protect will use the currently logged on user credentials to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **SQL Authentication:** Select this option to enter a specific 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 credentials to connect to the SQL Server, click this button.

20. Click **Next**.

Your 6.x database is upgraded to the 7.x format. When the database upgrade is complete the following dialog is displayed:



21. Click **Next** and follow the setup wizard prompts to complete the installation.
22. Start Shavlik NetChk Protect.
23. (Optional) If you are using agents, the **Distribution Server Upgrade** dialog is displayed. For example:

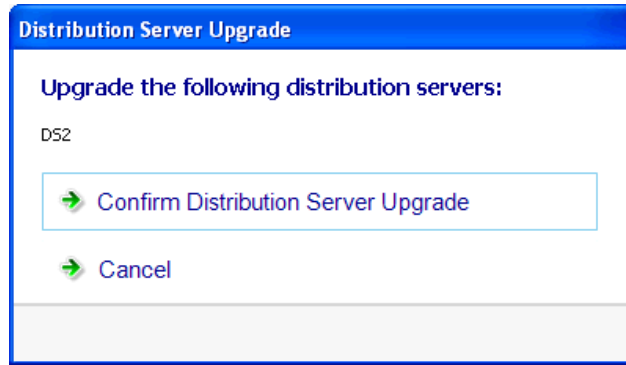


This dialog is used to reapply the credentials used by the console and by the agents when connecting to your distribution servers. It will also put the mechanisms in place to inform the agents that they need to upgrade themselves.

Important! Don't be fooled if the padlock 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 **Upgrade Servers**.

A dialog similar to the following is displayed:



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

The distribution servers are updated for 7.x. When the upgrade is complete the NetChk Protect home page is displayed.

24. Verify that all the console data looks correct.

25. 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 XML**.

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

27. Upgrade other consoles as needed.

FUNCTIONAL DIFFERENCES

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 7.0 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.
- 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

Limited agents are not supported in Protect 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 **General Tasks > Using the Scheduled Tasks Manager > Installing the Shavlik Scheduler** in the online Help system for more details.

SIGNIFICANT ENHANCEMENTS IN NETCHK PROTECT 7.X

Navigation Bar Enhancements

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

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

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

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

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

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

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

Shavlik NetChk Agent has a much different look and feel. 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.

Agent Client GUI

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 and threat scans, and they can manage the contents of the quarantine directory.

Patch Group Enhancements

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

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.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

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

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

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 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

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

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**.

Shavlik Technologies
Web : www.shavlik.com
E-mail: info@shavlik.com