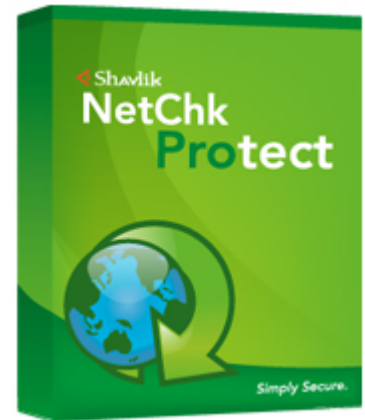




Quick Start Guide

Shavlik NetChk[®] Agent 7.5



Copyright

Copyright © 2006 - 2010 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 NetChk Agent, and the Shavlik Technologies logo are either registered trademarks or 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
October 2006	Shavlik NetChk Agent 5.8	Initial release of the Shavlik NetChk Agent Quick Start Guide .
April 2007	Shavlik NetChk Agent 5.9	Updated info on setting up a distribution server.
January 2008	Shavlik NetChk Agent 6.0	Added agent policy information.
June 2009	Shavlik NetChk Agent 7.0	Updated for version 7.0.
April 2010	Shavlik NetChk Agent 7.5	Updates for agent interface changes, add asset and power management, other miscellaneous changes.

PREPARING TO USE SHAVLIK NETCHK® AGENT

Welcome

This document provides a roadmap of tasks you must perform when preparing to use Shavlik NetChk Agent. For more detailed information see the Help system or the *Shavlik NetChk Protect Administration Guide*.

All agents are configured on the Shavlik NetChk® Protect console and then installed on the desired machines either by executing a menu command from the console or by manually installing them. You can configure several unique agent policies and install different agent policies on different machines.

(Optional) Set Up a Distribution Server

You have the option of setting up a distribution server that the agents can periodically access to download various files. There are several reasons for using a distribution server, including:

- If you will be configuring an agent policy that contains a threat task. The threat definition file is rather large and using a server will improve download performance.
- If some of your agents do not have Internet access and therefore will not be able to download the latest scan engines, XML data files, and patch files from the default Web sites. In this case you will need to store these files on a distribution server that the agents can access.
- If you have defined custom patches that are not available from the default Web sites. You must make the custom patches available by manually copying the patches to one or more distribution servers.

If your agent machines are able to access the NetChk Protect console to download all necessary files then you can skip this section. You may, however, elect to use one or more distribution servers anyway in order to speed the download process or to simply take some pressure off your console machine.

To set up a distribution server:

1. On the NetChk Protect console select **Manage > Distribution Servers**.
2. Click **New** and configure the distribution server.

In the top half of the **Distribution Servers** dialog be sure to specify a location and authentication method that all the agents can use when accessing the server. The lower half of the dialog is used to specify how the console will connect to this same location on the distribution server. Although the physical location you specify must be the same in both halves of the dialog, in the top half you can specify the method used by the agents when accessing the data (**UNC** vs. **Anonymous HTTP** vs. **Authenticated HTTP**).

3. Define which agent machines will use the distribution server by assigning the IP addresses of the agent machines to the distribution server.

To do this, select the **IP Ranges** tab, click **New** and type the name you want to give this collection of agent machines. Choose a primary and backup distribution server to use. Finally, click **Add** and define the IP address ranges of the machines that will use the designated distribution servers. For additional information, press **F1** to access the associated Help topic.

4. Update the distribution server with the latest patches, scan engines, and XML data files by manually synchronizing the server with the files contained on the console.

- **To update the server with patches:** On the **Synchronize** tab, select the distribution server(s) and then click **Synchronize Download Center**. All patches from the console's download center are copied to the distribution server(s).
- **To update the server with scan engines and XML data files:** Make sure you have the latest files on the console by selecting **Help > Refresh Files**. Then, on the **Synchronize** tab, select the distribution server(s) and click **Synchronize Engines and Definitions**. This will copy the scan engines and XML data files from the console to the distribution server(s).

You can configure NetChk Protect to automatically synchronize your distribution servers in the future. To do this, select **Tools > Options > Definitions** and then enable the **Automatically synchronize distribution servers after download** check box. For additional information, from the **Definitions** tab press **F1** to view the associated Help topic.

Create and Configure a NetChk Agent Policy

There are many different features and capabilities you can enable within a NetChk Agent policy. This example will illustrate how to configure an agent policy that contains all available features. In order to keep things relatively simple the default settings will be used wherever possible. Please see the Help system for complete information on customizing a NetChk Agent policy.

Create a New NetChk Agent Policy

1. In the button tray at the bottom of the navigation bar, click **Agent Policies**.
2. In the **Agent Policies** pane, click **New Agent Policy**.
3. Type a unique name for the policy.
4. Click **OK**.

On the General Settings Tab

1. (Optional) If you elected to use a distribution server, in the **Engine and Data Download Location** area, choose **Distribution Server** and then specify the distribution server you configured earlier.
2. If the agent machines must authenticate themselves to a proxy server when accessing the Internet, click the **Internet proxy credentials** button and specify the necessary credentials.

On the Patch Tab

This example shows how to configure a regularly scheduled patch task to run following Microsoft's Patch Tuesday (the second Tuesday of each month).

1. Click **Add a Patch Task**.
2. Type a name for the patch task (for example, *Monthly Patch Scan*) and then click **Save**.
3. In the **Schedule** area, choose **Once per month** and in the associated boxes specify the *Second Wednesday*.

On the Assets Tab

This example shows how to configure a software, hardware, and virtual asset scan that is performed every Sunday at 12:00 pm.

1. Click **Add an Asset Task**.
2. Type a name for the asset task (for example, *Weekly Asset Scan*) and then click **Save**.
3. In the **Schedule** area, choose **Days**, enable the **Sunday** check box, and clear all other daily check boxes.

On the Threat Tab

This example shows how to configure a daily threat scan and enable Active Protection.

1. Click **Add a Full Scan Threat Task**.
2. Type a name for the threat task (for example, *Full Threat Scan*) and then click **Save**.
3. On the **Threat Tasks** tab, in the **Threat Task Options** box, select **Schedule**, choose **Hourly**, and in the **Run every hh hours** box specify **24**.

4. In the **Threat Task Options** box, select **Scan Options** and **Reboot Options** and review the available options.

For this example we will use the default values.

5. On the **Active Protection** tab, enable the **Enable Active Protection** check box.

On the Power Tab

This example shows the power management options that are available. It will not have you save a power task in the agent policy. You should not implement a power task unless you are certain you want to restart your machines, shut down your machines, or put them into a sleep or hibernate state.

1. Click **Add a Power State Task**.
2. Type a name for the power task (for example, *Temporary Power Task*) and then click **Save**.
3. In the **Power State Template** area click **New**.
4. On the **Power State Template** dialog, click the **Reboot and power options** box and review the power state options that are available.

You can use the power template to:

- Put machines directly into a sleep state (for overnight energy savings)
- Put machines directly into a hibernate state (for overnight energy savings)
- Shut down machines (for weekend and holiday energy savings)
- Restart machines (for maintenance purposes)
- Restart machines and then put them into a sleep state (for maintenance and for overnight energy savings)
- Restart machines and then put them into a hibernate state (for maintenance and for overnight energy savings)
- Restart machines and then shut them down (for maintenance and for weekend and holiday energy savings)

5. Click **Cancel**.

You do not want to save this new template, just review the available options.

6. In the upper-right corner of the power task click **Delete**.

You do not want to save this power task in this example.

Save the Agent Policy

Click **Save and Update Agents**. You can review the agent policy by selecting it from within the Agent Policies pane in the navigation bar.

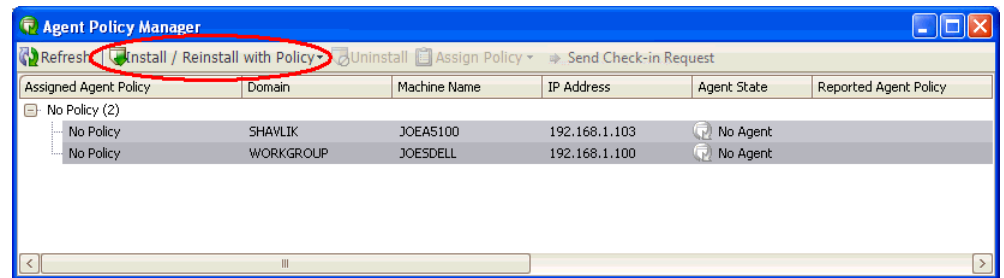
Use the Console to Install Agents on the Target Machines

You can use the console to "push install" the NetChk Agent service to connected target machines. In order to perform the push install, each target machine must be online and have an active network connection to the console during the NetChk Agent installation. This connection is required in order to exchange security information that will be used to establish an encrypted link for all future communication between the console and its agents.

For Machines That Have Been Previously Scanned

1. Select **Manage > Agent Policies**.
2. Select the desired machines, click **Install / Reinstall with Policy** and then select the desired agent policy.

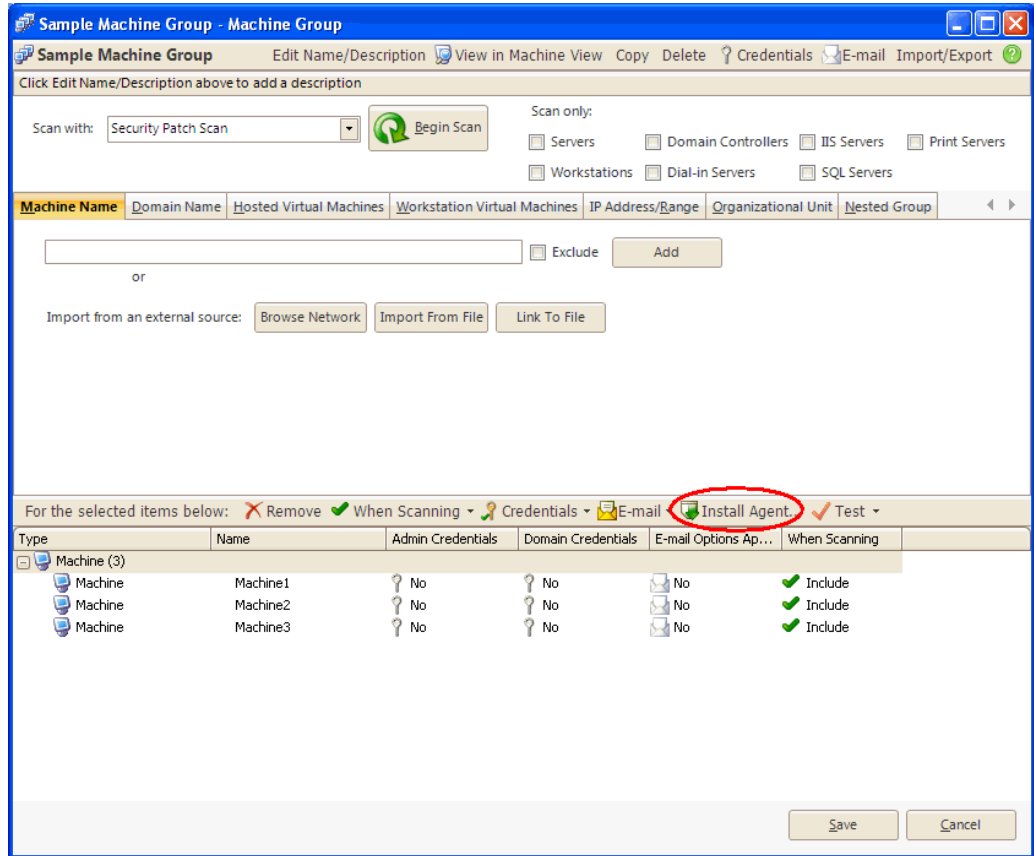
For example:



For Machines That Have Not Been Previously Scanned

You can install agents on machines that have not been previously scanned and are therefore not contained in the machine database. You simply create a machine group that contains all the machines that will run a particular agent policy, specify credentials for the machines, and then use the **Install Agent** button to install an agent policy on those machines. The caveat is that the machines must be online and connected to the network. If the console cannot make a connection to a machine the install will fail for that machine.

For example:



What Happens During the Installation Process

The following occurs when you push install the NetChk Agent service to a machine:

- The Operations Monitor is displayed and shows the status of the installation request.
- Once the agent is successfully installed on a target machine, the agent is automatically started on the machine.
- After an agent is installed on a machine, that machine becomes a managed machine and the status can be checked using Machine View. You'll have to wait until the next time the agent checks in with the console, but once that occurs the **Agent State** column will indicate that the machine contains an agent.

Manually Installing Agents

You must manually install NetChk Agent on machines that are guarded by a firewall. You do this by copying the agent installation files to the desired machines and then running the NetChk Agent installation wizard on each machine.

Requirements

- The target machines must be on your network and able to communicate with the console.
 - You must configure at least one NetChk Agent policy before manually installing an agent.
 - You must specify how the agent will authenticate itself to the console during the registration process. See **Common Tasks > Configuring Program Options > Agent Options** in the Help system for details.
-

Installation Procedure

1. On the NetChk Protect console, locate the **AgentInstaller.msi** file.
 - On Windows Vista and other newer operating systems the file is located in the **C:\ProgramData\Shavlik Technologies\NetChk\DataFiles** directory.
 - On earlier Windows operating systems like Windows XP the file is located in the **C:\Documents and Settings\All Users\Application Data\Shavlik Technologies\NetChk\DataFiles** directory.

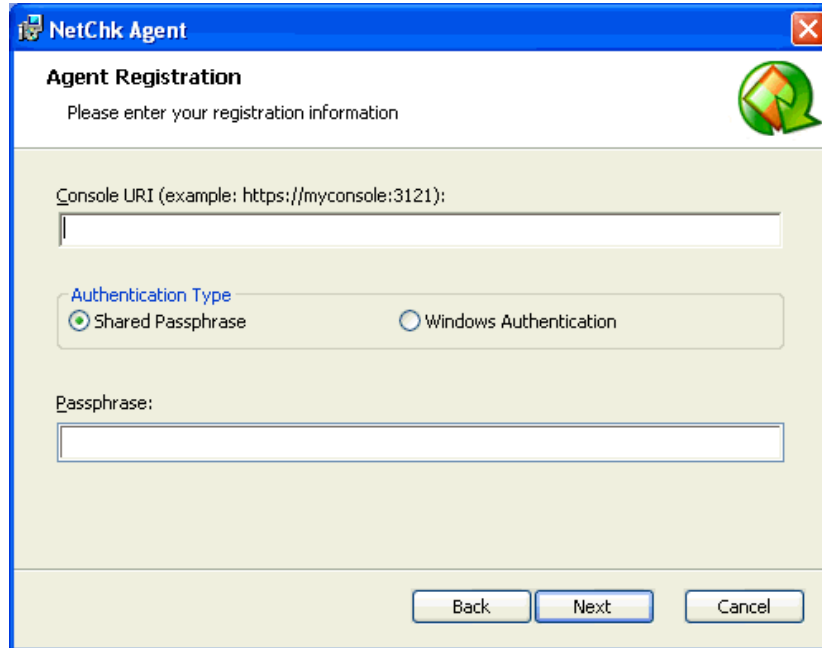
2. Copy the .msi file to the desired target machines.

You can distribute this file using Active Directory, or you can simply copy it to a physical media such as a CD or flash drive and manually distribute it to the desired machines.

Note: When distributing this file you may choose to create an installation script that automatically passes all necessary information to the installation wizard. See **Using Agents > Agent Overview > Creating and Using a Manual Installation Script** in the Help system for details.

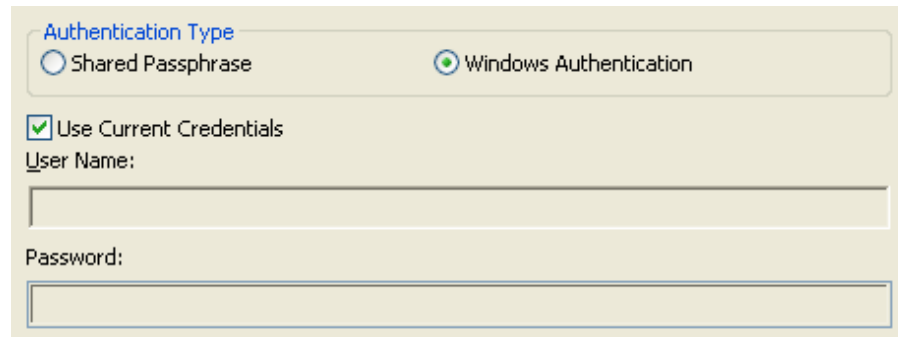
3. Log on to the target machine using an administrator account.
4. Double-click the file named **AgentInstaller.msi**.
The **NetChk Agent Setup Wizard** is displayed.
5. On the **Welcome** dialog, click **Next**.

The **Agent Registration** dialog is displayed.



6. Type the required information and then click **Next**.

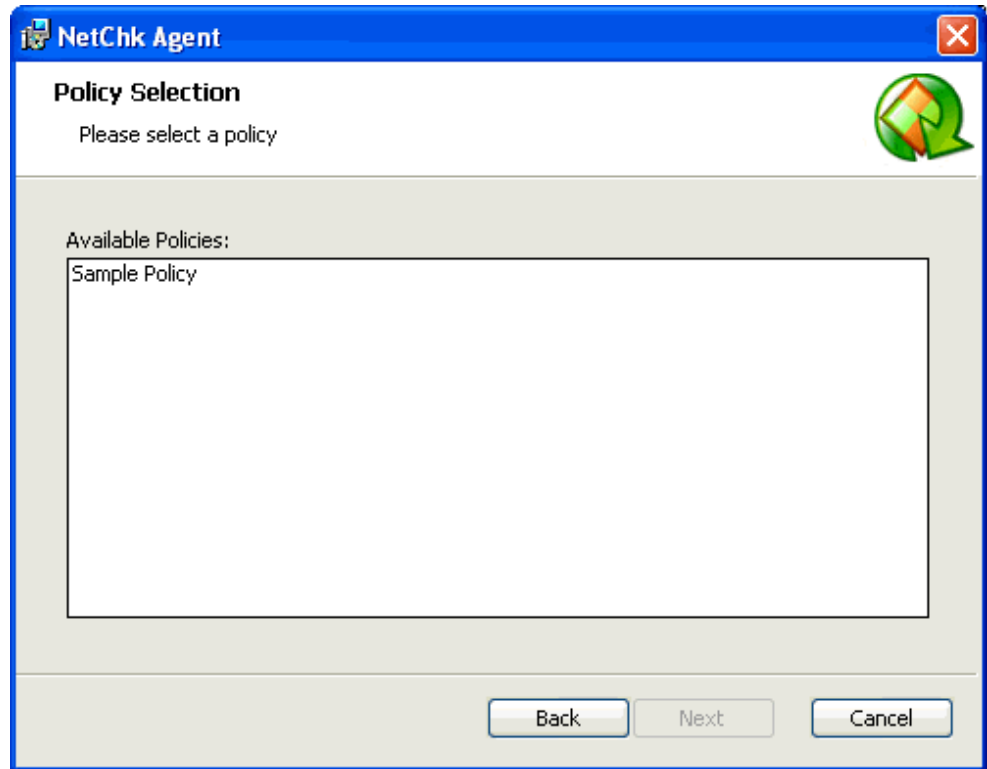
- **Console URI:** The URI consists of the NetChk Protect console's machine name or IP address and the port number used for forwarding information to the console. 3121 is the default port number.
- **Authentication Type:** You must choose the authentication method dictated by the NetChk Protect **Tools > Options > Agents** dialog.
 - If the **Enable passphrase in Agent installations** check box is enabled on that dialog, then choose **Shared Passphrase** and type the matching passphrase.
 - Otherwise, choose **Windows Authentication**. The lower portion of the **Agent Registration** dialog will change, providing you the opportunity to specify credentials.



If the credentials you used to log on to the target machine can also be used to log on to the NetChk Protect console, then simply enable the **Use Current Credentials** check box. Otherwise, do not enable this check box

but instead provide the necessary administrator credentials for the NetChk Protect console. The credentials must be in *domain\user.name* format and they must have administrator rights on the NetChk Protect console.

You will know you have specified the right information if the **Policy Selection** dialog is displayed after you click **Next**. For example:



7. From the list of available policies, select the policy you want assigned to this agent and then click **Next**.
8. On the **Ready to Install NetChk Agent** dialog, click **Install**.
9. On the **Installation Complete** dialog, click **Finish**.

When the installation process is complete the agent will be started automatically.

USING AN AGENT ON A MACHINE

The users of each agent machine can, if you permit, control many of the agent features on their machine. They do this using the NetChk Agent client program. To access this program they either:

- Select **Start > Programs > Shavlik Technologies > NetChk Agent**
- Double-click the NetChk Protect icon that resides in their machine's system tray.



A window similar to the following is displayed:



If users want information on how to use the client program they can simply click **Help > Contents** from the main menu.

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