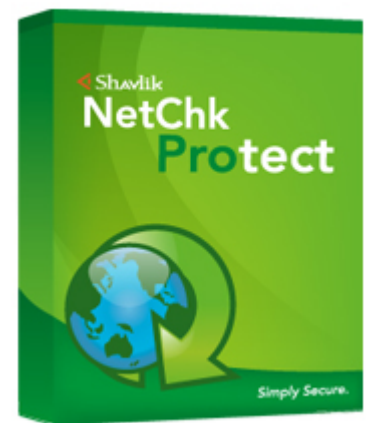


Best Practices Guide

Shavlik NetChk[®] Protect 7.5



Copyright

Copyright © 2009 - 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 Limited, Shavlik NetChk Deployment Tracker, and the Shavlik Technologies logo are trademarks or registered trademarks of Shavlik Technologies. VMware is a registered trademark of VMware, Inc. 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
January 2009	Shavlik NetChk Protect 6.5	Initial release of the Shavlik NetChk Protect Best Practices Guide .
February 2010	Shavlik NetChk Protect 7.2	Updated for version 7.2
April 2010	Shavlik NetChk Protect 7.5	Update screen shots and text to reflect 7.5 GUI.

Table Of Contents

ABOUT THIS GUIDE	1
BEST APPROACH FOR APPLYING PATCHES AND SERVICE PACKS	2
Overview	2
Detailed Course of Action	2
GUIDE TO SURVIVING PATCH TUESDAY	4
Overview	4
AUTOMATING PATCH MANAGEMENT FOR YOUR ENVIRONMENT	6
Overview	6
Automating Machine Discovery	6
Scan Template	6
Patch Groups	7
Patch View	7
Deployment Template	8
Automated Email Reporting	9
Scheduling Automated Jobs	9
Favorites	10
INSTALLING AGENTS ON INTERNET-BASED MACHINES	11
Configuration of the Agent Policy	11
Firewall Configuration	13
Agent Install	13
Additional References	14

This page intentionally left blank.

The document is designed for duplex printing.

ABOUT THIS GUIDE

This guide provides recommendations on configuring Shavlik NetChk Protect for optimum performance. It also describes the best approach to use for a number of common patch management situations. Many of the following *best practices* are based on actual customer examples. This information has been compiled by support and sales engineering personnel at Shavlik Technologies.

BEST APPROACH FOR APPLYING PATCHES AND SERVICE PACKS

Overview

Patch management can be tedious work. This section is intended to help reduce the amount of deployments to machines to make your work more effective.

The best order of approach to maintaining patch levels on a machine is to start with service packs. Service packs are very involved. Vendors recommend installing service packs one at a time and most should be followed by a reboot before any other patches or service packs are applied. Shavlik enforces this recommendation programmatically in NetChk Protect by only allowing service packs to be installed one at a time. The following example shows a machine with many service packs missing.

 Missing Service Pack	.NET Framework 2.0 Gold	.NET Framework 2.0 SP1
 Missing Service Pack	.NET Framework 3.0 Gold	.NET Framework 3.0 SP1
 Missing Service Pack	Microsoft Office Enterprise 2007 Gold	Microsoft Office Enterprise 2007 SP1
 Missing Service Pack	MSXML 6.0 Gold	MSXML 6.0 SP1
 Missing Service Pack	SQL Server 2000 SP3	SQL Server 2000 SP4
 Missing Service Pack	Visio 2003 Professional SP2	Visio 2003 Professional SP3
 Missing Service Pack	Windows Server 2003, Enterprise Edition SP1	Windows Server 2003, Enterprise Edit

Detailed Course of Action

Using the example above, the best course of action is as follows:

1. Start with any operating system service packs.

Be sure to adequately test the service pack before deploying it to your entire organization. After deploying the service pack you should reboot the target machines and then perform a fresh scan. Rescanning will give you the new state of the machine so you can continue applying service packs.

Note: Operating system service packs change the state of a machine and may inhibit you from rolling back patches that were applied prior to the release of the OS SP.

2. Apply major product service packs such as Office, Visio, and SQL.

Order does not matter here, but we do recommend rebooting in between each of these major SPs. Though not as common, these product SPs can also change the state of a machine considerably.

3. Deploy any remaining service packs to products such as MSXML, .Net, and MDAC.

These need to be pushed in separate deployments, but in this case you can do the deployments with no reboot and stagger them apart enough then reboot after they

have all been applied. Using the example above you would do the following:

- Start with scheduling deployment of .Net 2.0 SP1 with no reboot
 - Give an adequate delay then schedule .Net 3.0 SP1 (again w/ no reboot)
 - Give an adequate delay then schedule MSXML 6.0 SP1, this time with a reboot.
 - Scan the target machines again.
4. If all service packs now show as being applied, deploy all missing patches with reboot.
 5. Rescan and confirm all has been applied.

Note: The steps above may span several maintenance windows. In the case that you cannot do all of the above in a single maintenance window, each step should be followed up by a patch deployment to ensure you are not open to security vulnerabilities between maintenance windows.

Tip: The steps above should be built into your machine build policy. This will ensure machines go into the field as up to date as possible. Maintaining the machines is much easier than catching up on many month's worth of service packs and patches.

GUIDE TO SURVIVING PATCH TUESDAY

Overview

Patch day affects us all. This section is intended to give a workflow to surviving the patch day experience.

The first tip to a successful patch day is to stay on top of what is being released. Shavlik provides out of the box support for a wide variety of vendors which makes keeping up with what each product in your environment is doing a daunting task. Below are several sources that can be helpful in keeping up with what patches are releasing and what that means for you.

The single best source for any Shavlik customer is the Shavlik XML Announcements. This mailing list notifies you when new XML is available. This covers all vendors Shavlik supports and is the easiest way to keep up to date on what new patches\products are being supported by Shavlik. You can subscribe to these automatic announcements by going to the Shavlik XML Announcements Web page at:

<http://www.shavlik.com/support/xmlsubscribe.aspx>

Previous XML announcements can be viewed at:

<http://forum.shavlik.com/viewforum.php?f=29&sid=df66192f9fb848f75dc2ea640efa879d>

Just knowing the patches are available is great, but where can you go to get more in depth information on what the real impact of the newly release patches is for your environment? The Thursday before Patch Tuesday, Microsoft updates the following site to give an idea of what is expected to release. Since October of 2008 this also includes additional information regarding each patch called the Exploitability Index. Below are links to the Microsoft Advance Notification page and to an article about the Exploitability Index.

Microsoft Advance Notification:

<http://www.microsoft.com/technet/security/bulletin/advance.msp>

Click on the link [Read the most recent advance notification or the most recent security bulletin summary](#).

Note: This is what is expected to release. There are instances where not all items will release the following Tuesday.

Microsoft Exploitability Index Site:

<http://technet.microsoft.com/en-us/security/cc998259.aspx>

Other Vendors are realizing the importance of diligent patch management as well. Acrobat is following suit with a regular release schedule and ongoing security testing. The blog post below discusses Acrobat announcing a Quarterly release schedule on the third month second Tuesday of each quarter.

[http://voices.washingtonpost.com/securityfix/2009/05/adobe_adopts_microsofts_patch.htm
l](http://voices.washingtonpost.com/securityfix/2009/05/adobe_adopts_microsofts_patch.html)

Shavlik also provides a series of Webinars on Minimizing the Impact on Patch Tuesday. This webinar series is typically hosted by a member of the Shavlik Data Team as well as Shavlik Engineers who work with the products and customers on a regular basis. The Webinars provide insight into each month's patch releases and discusses their real world impact. You can sign up for the next session below at the Shavlik Webinars page.

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

Some other great resources on the Shavlik website include the Security Center Blog and the Support Team Blog. The Security Center Blog covers all shavlik supported releases and the Support Team Blog covers support related topics.

<http://securitycenterblog.shavlik.com/>

<http://supportteamblog.shavlik.com/>

Now that you are up to your elbows in what Shavlik and Microsoft sources are telling you let's look to a vendor agnostic source. PatchManagement.org is a site created by Security exports to provide a community for discussing all things patch related. This site provides the latest discussions on Patches (Windows and Linux\Unix) by a wide variety of security experts. It also has great information regarding many Patch Vendors in the market. The goal of this site is Patch Management Awareness and it meant to remain as vendor agnostic as possible.

<http://www.patchmanagement.org>

AUTOMATING PATCH MANAGEMENT FOR YOUR ENVIRONMENT

Overview

The goal of any IT group is to centralize and automate processes to reduce the amount of work needed to maintain your environment. The goal of Shavlik Technologies is to provide tools and solutions to help you achieve this level of automation. This section will discuss ways to help automate the patch management process.

Automating Machine Discovery

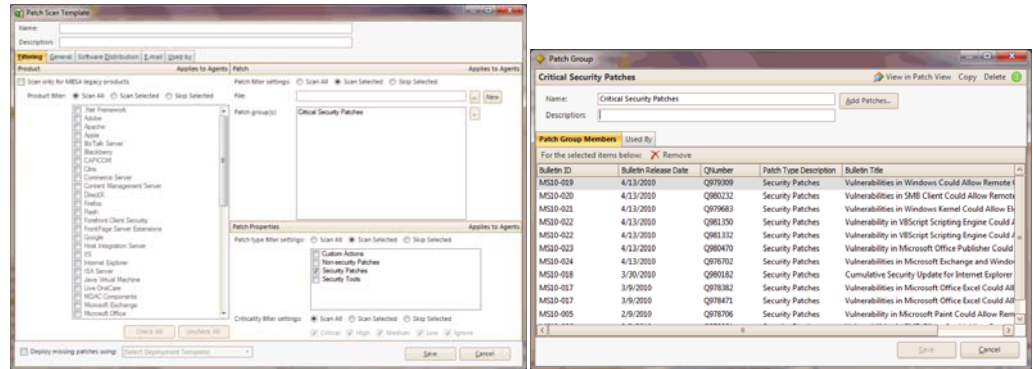
The first goal in automating the patch process is to create your machine groups as dynamically as possible. The easiest way to achieve this is to use Active Directory. If you group the machines in your environment the same way you will be managing the patching of machines, you can use the OU area of the machine group. Each time the machine group is used it will “talk” to Active Directory and pull the current list of machines from the OUs. The same can be said of using the Domain area, but that may encompass more than you want in an automated process. Another way to easily create dynamic groups is by IP range. Any new machines in those ranges will be captured whenever you perform a new scan.

Scan Template

When we start talking about automation we need to consider what we will be pushing. Most companies have very loosely defined approval processes for patches. Depending on your needs you will need to decide what works best for your situation. If you are concerned with all security patches, regardless of product, you can use the predefined *Security Patch Scan* template that is built into the product. Any new releases of XML data files will automatically include the security patches in this scan template next time it is used.

This may be adequate for your end-user environment, but for automating server patching you may want to consider using a patch group. The patch group or approved patch list allows you to define a list of specific patches to scan for. This can be tied to the scan template and then scheduled to scan with automatic deployment to automate the patch process start to finish. When new patches are released you can evaluate and determine what patches are approved for deployment in your environment and update your patch group or approve patch list with the new patches.

Next, scheduled scan will take the changes into account and scan and deploy the missing patches from the patch list. In the following screen shots you can see the scan template **Filtering** tab and a patch group. On the **Filtering** tab, in the **Patches** area, change the **Patch Filter** to **Scan Selected** and select either an approved patch list in the **File** box or select a patch group in the **Patch Group** box.



Patch Groups

To create a new patch group, in the **Patch Groups** list box click **New Patch Group**. You will be able to browse and select patches from a list as illustrated in the screen shot shown above. Once you have selected the patches you wish to support, click OK and then save the patch group. In your scan template, in the **Patch Groups** area, click the browse button and select the patch group(s) you wish to use. Now the scan template is configured to scan for a specific list of patches. If you enable the **Deploy missing patches using** check box you now have an automated patch process where you know exactly what will be pushed to machines.

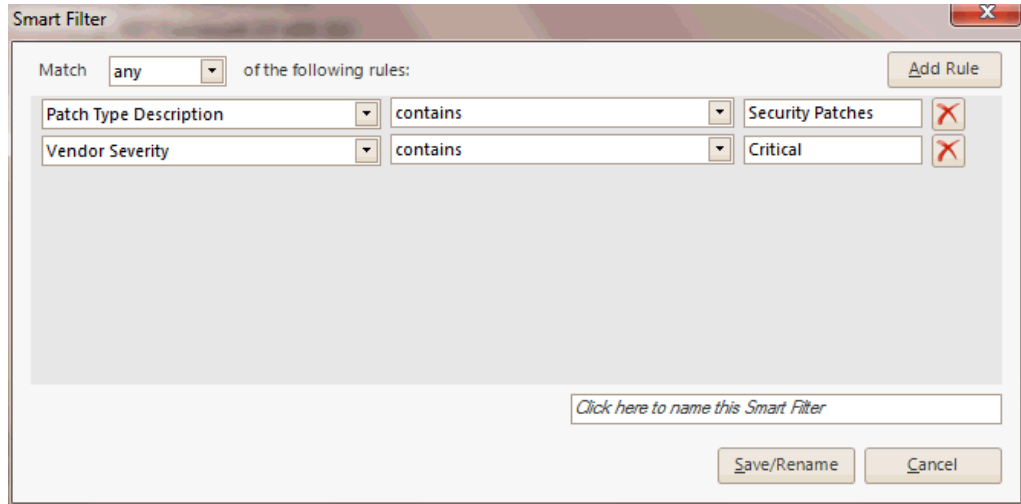
If you choose to use an approved patch list, all you need to do is create a text file and enter patches by Qnumber, one patch per line. In the **Patch filter settings** area of your scan template, click the **File** box's browse button and navigate to your text file. This file is easily distributed to multiple consoles for ease of use and simplification of patch approval across multiple consoles.

Example approved patch list:

```
Q123456
Q234567
Q345678
```

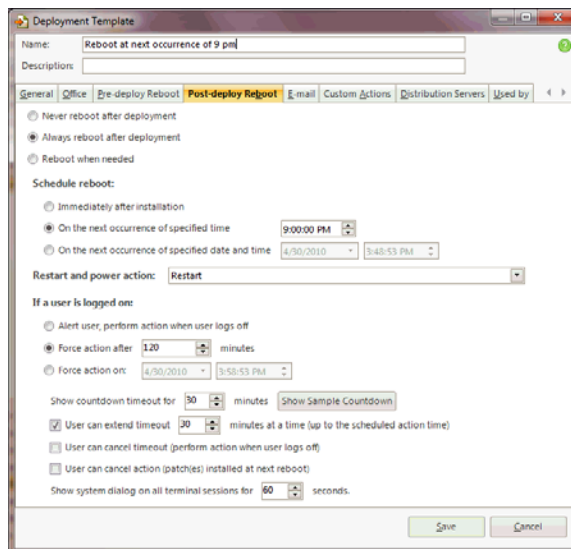
Patch View

The **Patch View** can be utilized to create or add to existing **Patch Groups** as well. Click on **Patch View** on the tool bar and you will go into the **Patch View**. From here you can use the Search feature or the Smart Filters to create filtered lists of patches and from the filtered view you can select all and right click and create a new patch group or add to an existing patch group. A good example is a patch group for all vendor critical security patches. Create a new smart filter and modify it to reflect the following screen shot. Save the filter and you will get the desired view. Select all and right-click and create a new machine group and from this point on you can come in each patch release and select your smart filter and select all and add to the existing patch group creating an easy repeatable process that takes only minutes to maintain.



Deployment Template

In your deployment template you will want to configure reboot options to meet the needs of the group you are intending to automate. If you are working with an end user environment you may want to set reboot options to be more flexible to work around people potentially working late. For example, on the **Post-deploy Reboot** tab, in the **Schedule reboot** area specify **On the next occurrence of specified time**. You might also enable the **Allow the user to extend the timeout** check box.



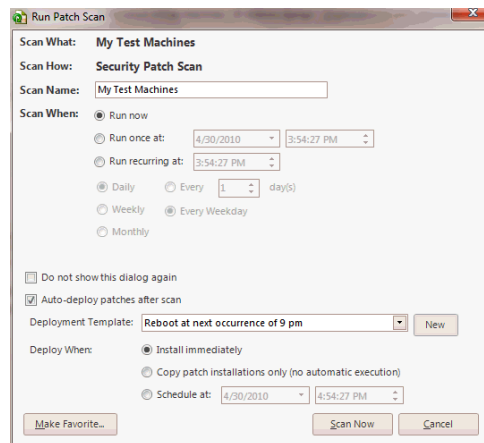
For a server environment you will want to set reboots to be immediately after installation. Why? Because you will normally run the scan and deployment in a maintenance window and will want the reboot to follow immediately. You can also shorten the timeouts on reboot to speed up the process as anyone who would be on these machines should be aware of the maintenance windows in advance.

Automated Email Reporting

From your machine group, scan template, and deployment template you can configure reports to be automatically generated and e-mailed to designated recipients. When automating the patching of an environment, this is an easy and efficient tool for keeping all necessary personnel up to date on the state of the environment. There are a variety of different reports to choose from that will present different data for different audiences and needs. You may need to try a few to find the best fit for your reporting needs.

Scheduling Automated Jobs

Once you have your groups and templates configured you will want to schedule your jobs to execute. To schedule a job to run automatically you start at the machine group. Select the desired scan template from the dropdown and click **Begin Scan**. You will see the following dialog:

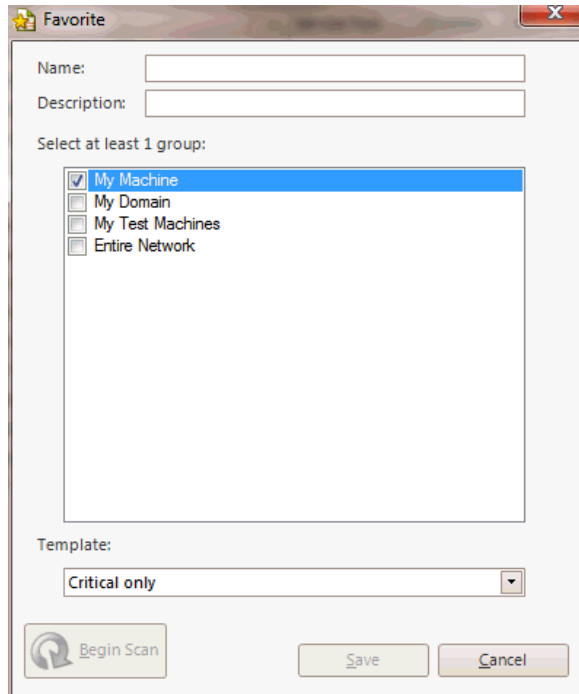


From this dialog you can execute jobs now, schedule to run once at a specific time and date, or schedule recurring jobs to run. You can also select to auto-deploy patches after scan. This is the most important option we will discuss in this section. The machine groups and scan and deployment templates we have created have fine tuned what we want to scan and deploy for our environment. With the knowledge of what will be pushed we can now schedule the job to execute from start to finish without the need to handle the job from one stage to the next. In the screen shot you will see the option used is a recurring scan with auto deploy set to execute on the second Wednesday of every month. This is the day after patch Tuesday, which will almost always have new patches to push. When you schedule this job it will ask you to make a favorite. The favorite is a combination of a machine group and a scan template that can be reused later.

Note: When scheduling jobs keep in mind where the scheduled task resides. A scheduled scan with auto deploy resides on the console until the scan completes. Once the scan completes it will push patches out to machines and execute immediately. The reboot will be scheduled on the targets local time.

Favorites

A favorite is a combination of machine group and scan template for the console to reference when it executes a job. You can reuse favorites to schedule multiple jobs to run at different times. From the favorite you can click on **Begin Scan** and schedule out additional one time or recurring jobs as needed without having to recreate additional favorites.



INSTALLING AGENTS ON INTERNET-BASED MACHINES

This walkthrough gives a base recommendation for Agent configuration to support machines outside the network environment. This configuration is ideal for laptop users who are frequently disconnected from the network, but regularly connected to the Internet and for standalone sites that do not have direct network connectivity, but do have internet access. Protect 7 agents communicate via SSL and use a console generated certificate to secure communication between Agent and Console. The Agent can be configured to pull all xml and engines from Shavlik and patches straight from the vendor leaving only one port requirement for communication with the Shavlik Console, which by default is over port 3121, but is configurable.

Configuration of the Agent Policy

1. In the console go to **Tools > Options > Agents** and set a passphrase.

By default this option is disabled and is blank. Passphrase is ideal for mass rollout of the agents if you need to do scripted or manual installs and can be locked down after the mass rollout. With the passphrase option disabled you can still install the agent manually using administrator credentials. See the Reference section at the end of this document for scripted install options.

2. In the Navigation bar click on **Agent Policies > New Agent Policy**.
3. Name the policy.
4. Configure options on the **General Settings** tab.

You can configure the **User Interaction** settings as you see fit. The recommendation is to uncheck **Allow the user to abort a scan** as most users (if they are aware) will stop a scan whenever they know it is running, preventing the agent from performing its task.

In the **Check-in Intervals** section the recommendation is to keep the check-in to a frequent timeframe. This will keep the agent responsive to policy changes in your environment.

In the **Engine and Data Download Location** section, **Vendor over the Internet** is recommended in this case as we are expecting these agents to be primarily outside the network. If you are configuring a significant number of agents you may choose to enable **Distribution Server** and **Use vendor as backup source**. Agents will check for the latest engines and XML data file on the distribution server first, and they will use the vendor Web sites if the distribution server is not available. **Agent listens for updates** can be checked. If you do, it is recommended to modify firewall rules to block the port when outside the network and open the port while inside the network for best security practice.

5. Click the **Patch** tab and configure a patch task.

This policy is intended to focus on securing the machine so for this recommendation we suggest using the **Security Patch Scan**. You can choose to use a custom template if you wish, but we will stick to the basic Security Best

Practice for this example.

Enable the **Enable Patch Deployment** check box and choose a deployment template that uses a reboot option that delays reboot until next occurrence of a specified time and that time is after hours to not interrupt the end users work day.

In the **Patches Approved for Deployment** area, you can do **All patches detected as missing** which would be most secure, or you can deploy based on a **Patch Group** and enable the **Plus all vendor critical patches** check box. This option ensures that even if you have not applied the latest security patches to the patch group, or the agent has not pulled down an updated list, it will still deploy critical security patches released in the latest XML files.

In the **Schedule** area, choose **Daily** and specify a time that the machine will commonly be on but when network traffic might be lower (like the lunch hour). Usually check just the work week. If you choose to do a time of day that is outside normal business hours it is recommended to check the **Run on boot if schedule missed** option to ensure that the assessment occurs even if the last scheduled task was missed.

6. Click the **Threat** tab and configure your threat tasks.

Here we will create two tasks: **Quick Scan** which will do a scan of Common Locations, and **Full Scan** which will scan all system drives and archived files. The Quick Scan task is recommended to be done on a daily basis. It is a more focused scan and will be shorter so it will have less impact on the user. A lower traffic time of day like the lunch hour is ideal.

On the **Threat Task Options: Reboot Options** page consider using the **On the next occurrence of specified time** option to reduce impact on users work day.

The Full Scan is recommended to be done once per week and off hours as depending on the size of drives and amount of data and archived files this scan may take a long time. For this scan, on the **Threat Task Options: Schedule** page it is best to consider the **Run on boot if schedule missed** option to ensure this task executes each week to keep the system clean. Under the Reboot options consider keeping the reboot set to **Immediately after removing threats**. This task will likely be running while no user is on the machine so there should be less chance of impact on the users.

7. Configure options on the **Threat Actions** tab.

In threat actions you will notice the malicious categories are set to **Quarantine** by default and all other categories are set to **Report Only**. The Report Only items are set this way as there are some signatures that may be necessary for your environment. Modify at your discretions but it may be less of a support impact to monitor for a period of time and add flagged items to the **Allow** list before enforcing **Quarantine** and **Delete** options.

8. Configure options on the **Allowed Threats** tab.

As threats are detected you can flag detected threats as allowed if they are known items that are necessary for your day-to-day operations.

9. Configure options on the **Always Allow / Never Allow** tab.

Here you can add programs to be always or never allowed to run. With Active

Protection enabled and configured strictly you may want to add in items you always want to have allowed so the user does not get flagged with items they commonly use.

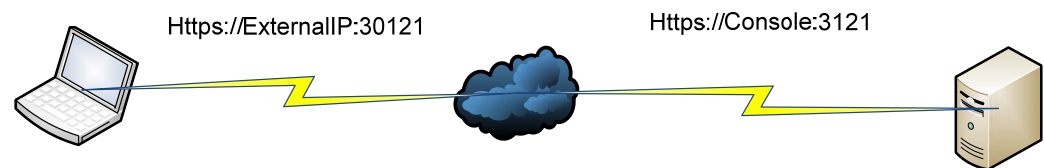
10. Configure options on the **Active Protection** tab.

Here you can enable Active Protection to **Allow**, **Allow Notify User**, or **Prompt User For Action** for specific activity on the target machine.

11. Click **Save and Update Agents**.

Firewall Configuration

Once your agent policy is configured you will need to configure a port redirect at the firewall to allow external machines to reach the console via TLS. The diagram below shows a default example of how to configure the firewall rule.



Once configured you can do a manual agent install using the **AgentInstaller.msi** file. The file is located on the NetChk Protect console in the following directory:

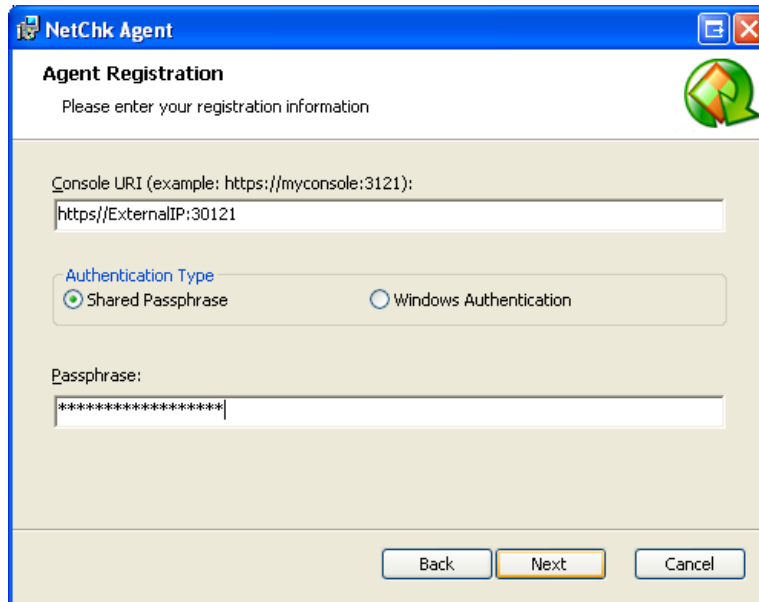
- On Windows Vista and other newer operating systems:
C:\ProgramData\Shavlik Technologies\NetChk\DataFiles
- On earlier Windows operating systems like Windows XP:
C:\Documents and Settings\All Users\Application Data\Shavlik Technologies\NetChk\DataFiles

Place the file in an accessible location and execute on the target machine. By default NetChk Protect 7 allows use of a passphrase to install the agent or Windows Authentication. The screenshot below shows the Agent Installer interface. For an agent you wish to support outside the network as well as inside it is recommended to install the agent while connected through the Internet. This sets the agent up to always look to the external address first then the internal console as a secondary. If you install the agent internally you would need to manually modify a config file to allow the agent to check the external address.

Agent Install

Run the **AgentInstaller.msi** while connected to the Internet outside your network. Console URI will be <https://ExternalIP:30121> as shown in the example above. **Shared Passphrase** is the default option and will be blank by default. Again, you will want to go into the console under **Tools > Options > Agents** and configure a passphrase here. Once initial rollout of agents is complete it is recommended to disable the passphrase option and rely on admin credentials going forward for one-off installs. Passphrase

can be reenabled as needed for additional mass rollouts.



Your agent should be able to pull policy updates and rollup results both internally and externally. You can test this by connecting the machine to the Internet outside your network and kick off a scan manually and watch for the results, then in your network do the same.

Additional References

Additional information on configuring and installing agents is available in the Help system. The Help system is accessible by selecting **Help > Contents**.

- For complete agent information, see the section titled **Using Agents**.
- For information on manually installing agents, see the Help topic titled **Manually installing agents**.
- For information creating a script to perform your agent installations, see the Help topic titled **Creating and Using a Manual Installation Script**.

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