Shavlik Protect

Best Practices Guide

shavlik

Copyright

Trademarks

Document Information and Print History

Date	Version	Description
January 2009	Shavlik NetChk Protect 6.5	Initial release of this document.
February 2010	NetChk Protect 7.2	Updated for version 7.2
April 2010	NetChk Protect 7.5	Update screen shots and text to reflect 7.5 GUI.
September 2010	Shavlik NetChk Protect 7.6	Update product branding. Also some agent threat task interface changes.
March 2011	Shavlik NetChk Protect 7.8	Combine with Implementation & Planning Gd. Add info on 7.8 features.
November 2011	VMware vCenter Protect Essentials Plus 8.0	Rebrand the product. Update system requirements and other areas. Add disconnected console section.
December 2011	vCenter Protect Essentials Plus, Document Rev A	Update the Firewall Configuration section with new port forwarding information.
January 2012	vCenter Protect Essentials Plus, Document Rev B	Update the manual agent installation process to use STPlatformUpdater.exe, add Console Alias troubleshooting info, correct a few grammar errors.
April 2012	Rev C of document	Add DMZ network configuration information.
September 2012	VMware vCenter Protect 8.0.1	Update product name, version and cover graphics.
September 2012	VMware vCenter Protect 8.0.1, Document Rev A	Remove list of required Web addresses and replace with a link to a VMware Knowledge Base article.
May 2013	Shavlik Protect 9.0	Rebrand to Shavlik Protect, update UI references, add Protect Cloud info, remove DMZ sections.
April 2014	Shavlik Protect 9.1	Update Web links and legacy files and images.
September 2015	Shavlik Protect 9.2	Several updates to address user interface changes.

Table of Contents

ABOUT THIS GUIDE

This guide provides recommendations on configuring Shavlik 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.

For detailed installation instructions see the *Shavlik Protect Installation Guide*.

CONSOLE SOFTWARE AND HARDWARE RECOMMENDATIONS

Recommended OS

- Windows Server 2012 Family R2, excluding Server Core
- Windows Server 2012 Family, excluding Server Core
- Windows Server 2008 Family R2 SP1 or later, excluding Server Core

Prerequisites

- Use of Microsoft SQL Server 2005 (Full or Express Edition) or later
- Microsoft .NET Framework 4.5.1 or later
- Windows Management Framework 4.0 (contains Windows PowerShell 4.0, which is required in order to use the ITScripts feature).

  This prerequisite does not apply to Windows 8.1 and Windows Server 2012 R2 as PowerShell 4.0 is already included with these operating systems.

Average Console Install: 30-60 mins depending on prerequisites and Internet speed.

Physical Machine vs. Virtual Machine Considerations

The requirements for installing Shavlik Protect on a virtual machine are the same as for a physical machine. You should have a minimum of 4GB hard disk space for the patch repository and an additional 2GB for each operating system you support. For each additional language you support, add 4GB. If you use the Predictive Patch feature, which downloads patches in advance of their anticipated deployment, you should have at least 10GB of available space.

Recommended Console Machine Resources

1 – 250 seats

- **Processor:** 2 processor cores 2 GHZ or faster
- **Memory:** Minimum 2 GB RAM (recommended 3+ GB RAM if SQL is local)
- **Database:** Microsoft SQL Server 2005 (full or express edition) or later

251-1000 seats

- **Processor:** 4 processor cores 2 GHZ or faster
- **Memory:** 4 GB RAM
- **Database:** Microsoft SQL Server 2005 (full or express edition) or later

1001+ seats

- **Processor:** 8 processor cores 2 GHZ or Faster
- **Memory:** 8 GB RAM
- **Database:** Microsoft SQL Server 2005 (full or express edition) or later

To increase performance on any of the previous configurations, increase the number of processors and increase the amount of installed memory.

PORT REQUIREMENTS AND FIREWALL CONFIGURATION

These port requirements can also be found in the help files. With the following tables an administrator can configure firewalls in the environment and on the local machines to allow proper traffic in and out of machines for Shavlik Protect to manage the environment.

	Inbound Ports (Basic NAT Firewall)									
	TCP 80	**TCP 135**	**TCP 137-139 or TCP 445 (Windows file sharing/directory services)**		**TCP 443**	**TCP 3121**	**TCP 3122**	**TCP 4155**	**TCP 5120**	**TCP 5985**
Client System		X (For asset scans)	X	X				X (For listening agents)	X	X (For WinRM protocol)
Console System						X	X			
Distribution Server	X		X	X	X					

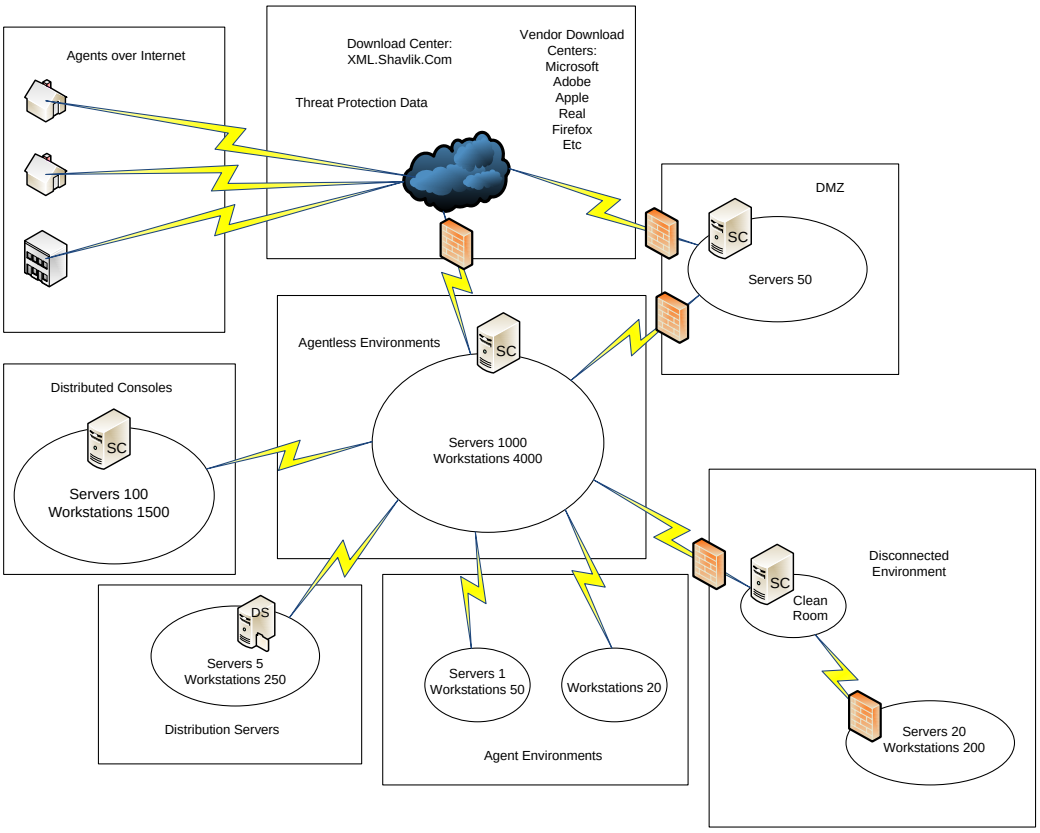
	Outbound Ports (Highly Restricted Network Environment)					
	TCP 80	**TCP 137-139 or TCP 445 (Windows file sharing/directory services)**		**TCP 443**	**TCP 3121**	**TCP 5120**	**UDP 9**
Client System	X (For agents)	X	X	X (For cloud agents)	X (For agents and Deployment Tracker)		
Console System	X	X	X	X (For cloud sync)		X	X (For WoL & error reporting)

Firewall Configuration

A number of different Web addresses must be accessible in order for Shavlik Protect to download the necessary patches, service packs, engines and XML files. This means you may need to add the Web addresses to your firewall rules and proxy exceptions list. For the complete list of Web addresses that must be accessible, go to the Shavlik community site at http://community.shavlik.com and see article DOC-2155.

DISTRIBUTED ENVIRONMENT MANAGEMENT

Shavlik Protect provides a number of features to allow for management of an environment. In the following diagram you will see a variety of scenarios that we will discuss in this section.



Agentless Environments

Shavlik Protect can be rapidly configured to support large numbers of machines agentlessly. By creating a machine group from hostnames, domains, IP addresses/ranges or OUs, you can identify machines you want to scan and specify administrative credentials for the machines.

Distributed Consoles

Multiple Shavlik Protect consoles can be configured to distribute workload across large numbers of machines and across WANs to distribute management of the enterprise. Data can then be rolled up to a central console for reporting purposes.

Distribution Servers

To reduce WAN traffic a distribution server can be setup at a remote site to distribute data, engines, patches, and service packs to a remote site, reducing data transfer.

Disconnected Environments

Shavlik Protect can be configured to pull data, engines, patches, and service packs from an internal source.

- For partially disconnected environments you can use these features to download from an Internet-connected machine. You then move the files to a clean room and from there into the disconnected environment.
- In a fully disconnected environment the connected console would download everything. You then use a manual or “sneaker net” process to move the files from one console to another.

Agents

Shavlik Protect also includes agents. With the agent, administrators are able to work around many obstacles and reach machines where agentless scans may not gain total coverage. Low bandwidth WAN links, laptops that typically leave the environment, and secure environments such as DMZs are cases where an agent may be ideal.

DMZs

Shavlik Protect can be configured in a number of ways to support de-militarized zones (DMZs). The option to use agentless scans by IP address or IP ranges allows administrators to work around name resolution if it is not available in the DMZ. A distributed console can be configured in the DMZ if IP rules on the firewall are not acceptable to support agentless scanning from the network into the DMZ.

CONFIGURING AGENTLESS PATCH MANAGEMENT

The fastest way to get Shavlik Protect configured and patching machines is to do so agentlessly. Once the console is installed it can take as little as a few minutes to setup machine groups to scan an environment. The time to configure will be based on the complexity of the environment and the range of maintenance windows.

Example

An office that contains three floors, with approximately 500 end users per floor as well as a data center with 200 servers, could be broken out many ways. You might create a separate machine group for each floor based on the IP range of the workstations. Servers might be broken down into three more groups: Test, Development, and Production. You might consider breaking the Production department into separate groups such as domain controllers and Exchange / SQL Servers to allow flexibility in scheduling jobs.

Time to Implement

It will take approximately five minutes to create three groups covering the three floors of workstations. Plan on 10-30 minutes to create the server groups; they can be created by OU, by browsing and selecting machines, or by importing identities from a file. Plan on another 15 minutes to schedule the jobs that will scan and optionally auto deploy patches.

The overall time to configure the machine groups and to schedule the scans in this example environment is approximately 45 minutes. Once this is done we are configured and ready to go.

Port Requirements

For agentless scans you will need to be able to resolve the machine by the method you used to create the machine group. You must also be able to access TCP ports 137 - 139 or port 445 on the target machine. File and print sharing and remote registry must be enabled in order to perform the scan. For added security, firewall rules can be applied between vLANs or on the local machine firewall that restrict port access to all but the console's IP. Depending on the environment, complexity, rules, and change control requirements, the amount of time this will add to the initial configuration may vary.

BEST APPROACH FOR APPLYING PATCHES AND SERVICE PACKS IN AN AGENTLESS ENVIRONMENT

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 Shavlik 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 service packs. Though not as common, these product service packs 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 and then schedule .Net 3.0 SP1 (again w/ no reboot)
   - Give an adequate delay and then schedule MSXML 6.0 SP1, this time with a reboot.
   - Scan the target machines again.

4. After all service packs have been deployed and the target machines have been rebooted, deploy any missing Microsoft operating system patches and perform a reboot.
5. Deploy any other missing Microsoft patches such as Office, Internet Explorer, etc. and reboot as needed.
6. Deploy any third party patches and reboot as needed.
7. 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 that 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.

AUTOMATING PATCH MANAGEMENT IN AN AGENTLESS 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 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

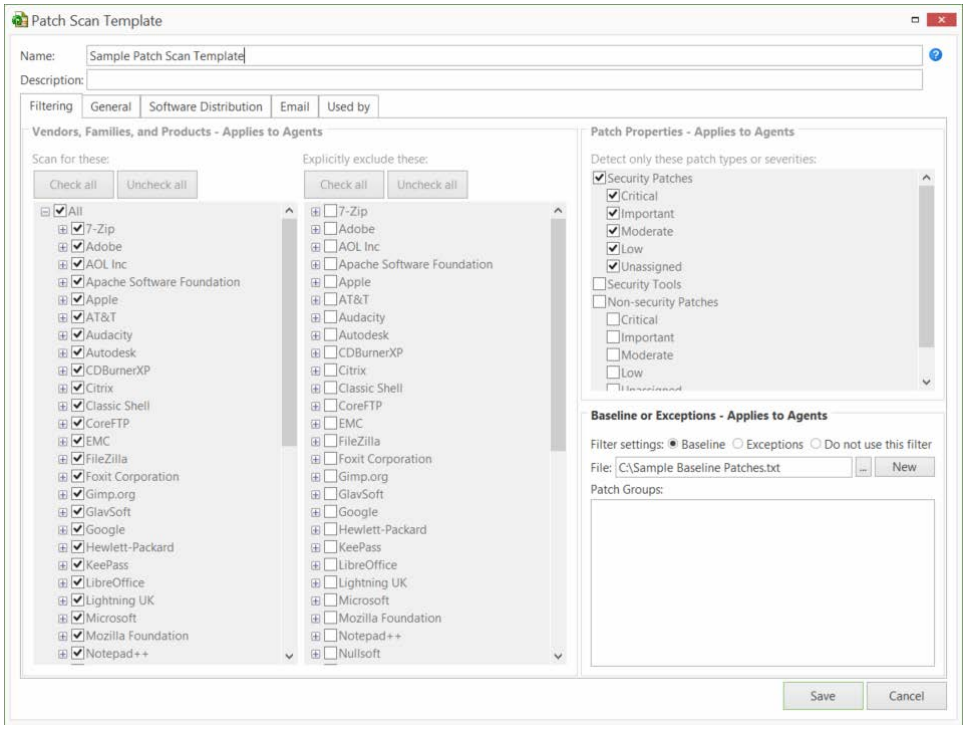
The first goal in automating the patch process is to create your machine groups as dynamically as possible. The easiest way to achieve this is to use Active Directory. If you group the machines in your environment the same way you will be managing the patching of machines, you can use the OU area of 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 the 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 your approved patch list with the new patches. A scheduled scan will take these changes into account by scanning and deploying the missing patches from the patch list.

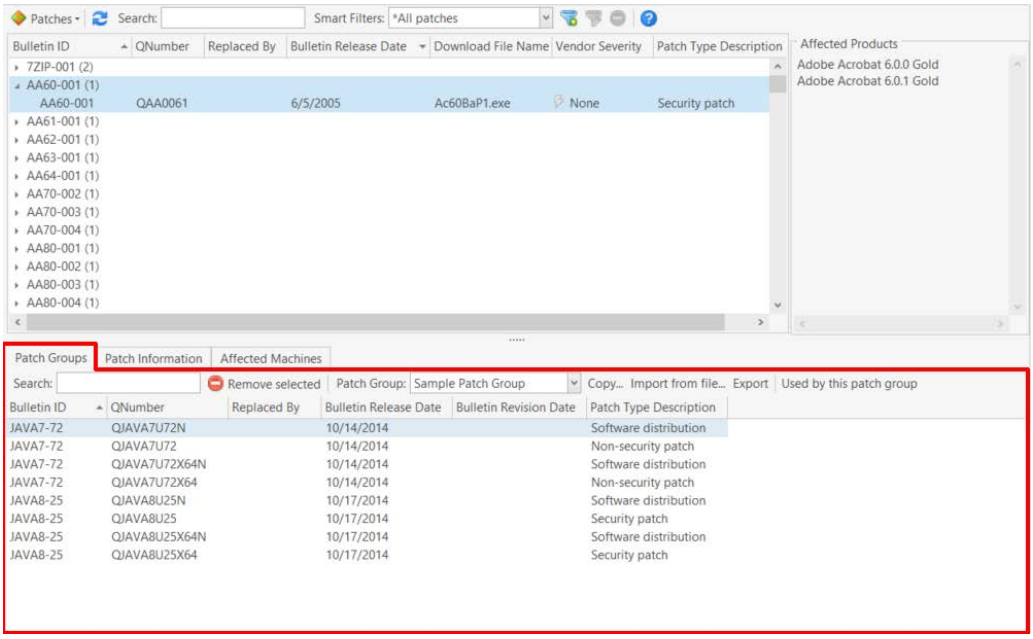
In the following screen shot you can see the scan template **Filtering** tab. You can use the **Baseline or Exceptions** filter to specify either an approved patch list or one or more patch groups that collectively represent a baseline set of patches. The section that follows explains how to create a patch group or patch list.



Patch Groups

Note: When Shavlik Protect uses a patch group to scan for selected patches, it always scans for and reports on the status of all service packs. It will also disable patch replacement, meaning it will show as missing earlier patches that have been replaced by later patches.

To create a new patch group, on the main menu select **New > Patch Group**. This presents the Patch View dialog. Any existing patch groups are displayed in the bottom pane. Use the Patch View filters to narrow the list of patches displayed in the top pane. You then right-click on the desired patch or patches, select **Add to patch group** and choose a patch group name. The patch group is automatically saved.



You might create a Smart Filter that identifies all of the current vendor critical security patches. From this point on, for each patch release you simply use your Smart Filter and from the filtered view select all and add to the existing patch group, creating an easily repeatable process that takes only minutes to maintain.

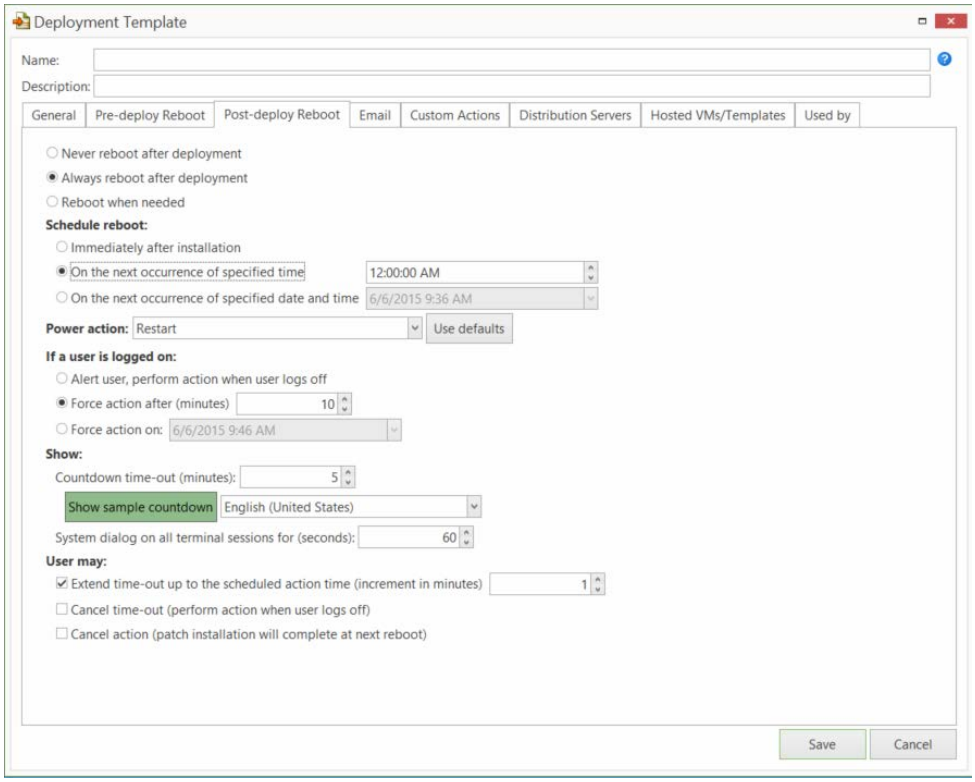
In your patch scan template, in the **Baseline or Exceptions** area, click the browse button and select the patch group(s) you wish to use. Now the scan template is configured to scan for a specific list of patches.

If you 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 **Baseline or Exceptions** 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

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 **Extend time-out** check box.



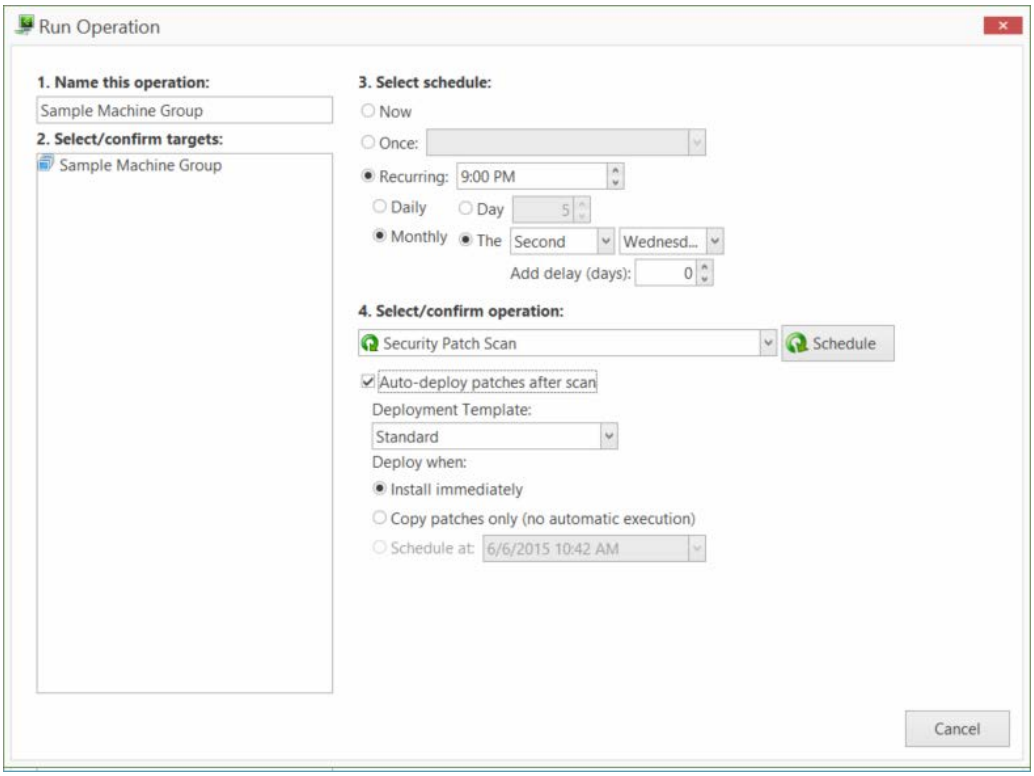
For server environments, the recommended reboot option is not as obvious.

- You may want to configure reboots to be performed 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.

- On the other hand, you may elect to **Never reboot after deployment** even though a reboot is typically required. This makes sense in situations where server availability is extremely critical to your business. You might want to manually reboot your servers so that you are always onhand in case something should go wrong during the reboot process.

Scheduling Automated Jobs

This final step is where it all comes together. Once you have your groups and templates configured you will want to schedule your jobs to execute on a regular basis. To schedule a job to run automatically you start at either the home page or the machine group. When starting from within a machine group, click **Run operation**. You will see a dialog similar to the following:

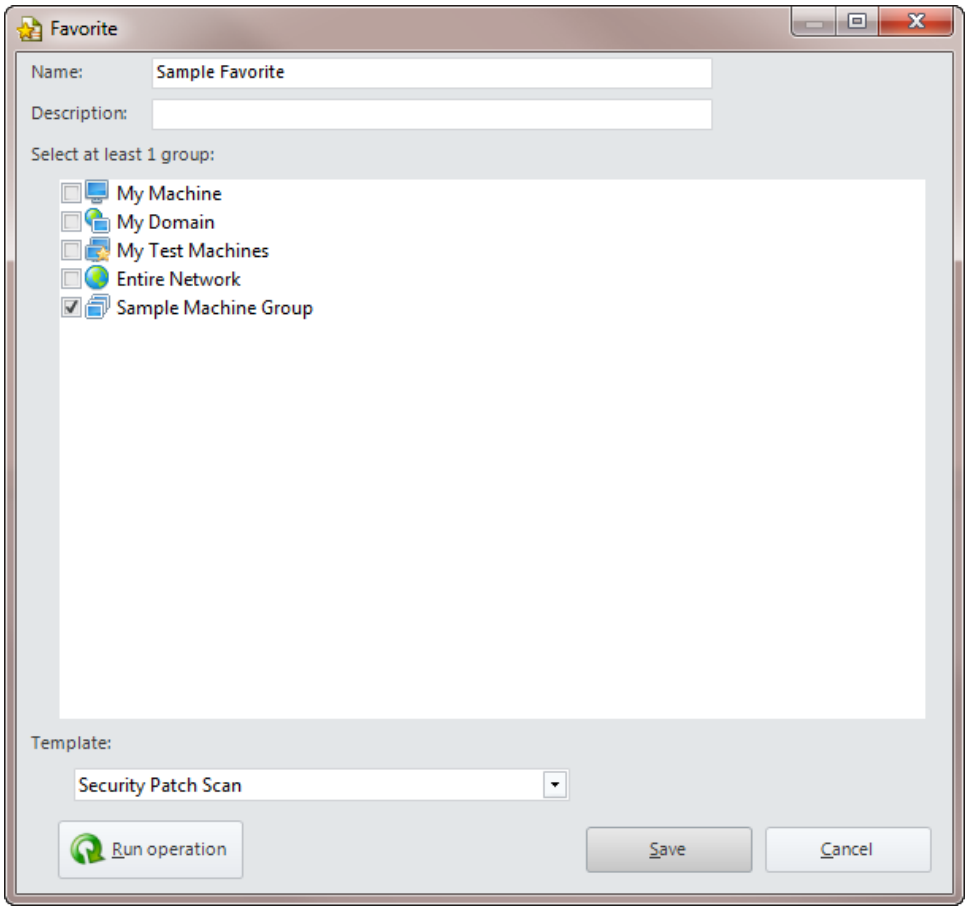


From this dialog you can execute jobs now, schedule to run once at a specific time and date, or schedule recurring jobs to run. You can also elect to auto-deploy patches after the scan. This is the most important option we will discuss in this section. The machine groups and scan and deployment templates we have created previously 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 above you will see we've defined a recurring scan with auto deploy that is 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.

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 based on the settings in the deployment template and on the target machine's 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 **Run Operation** and schedule out additional one time or recurring jobs as needed without having to recreate additional favorites.



Automated Email Reporting

From your machine group, scan template, and deployment template you can configure reports to be automatically generated and emailed 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.

To use the automated email feature you need to setup your email credentials. To do this you select **Tools > Operations > Email** and then provide your email server address and authentication information.

AGENT-BASED PATCH MANAGEMENT

Rolling out agents takes a little more preparation work to configure the environment to get the first scans coming in from machines. An agent is a great way to automate the management of some hard to reach machines, so it can be worth the effort to rollout agents to machines.

To configure and install an agent, you must create agent policies to manage different groups of machines. The policies may be based on geographic location, role, or a combination. Each policy can be configured to execute multiple tasks on an hourly, daily, weekly, or monthly basis. Once agent policies are set up the agent can be installed on a machine. Once the agent is installed it will start to manage the machine as it was configured to do.

So, if agents require a longer rollout time, why would they be ideal in some cases? There are three general cases where agents are the preferred solution.

Laptops Users

Laptops come and go in environments today. With the agent loaded on a machine it will not matter if the laptop is not online during a maintenance window. The agent policy can be configured to fill in the gaps and supplement agentless coverage, providing a solid support model for these hard to reach road warriors.

Secure Environments

Demilitarized zones (DMZs) are a good example of an environment that may not allow file and print sharing regardless of the firewall rules and security measures that are in place. With the agent the target can be locked down and only require an outbound port to the console to update its policy. This port is 3121 (inbound port on the console). Internet connectivity may be required if you specify **Vender over Internet** as a source for data and patches. If internal distribution servers are to be utilized the servers will require ports 137 - 139, 445, or (if using http) whatever port IIS is configured on for the virtual directory.

Be sure to check the **System Requirements** topic in the Help system for the latest port information.

Low Bandwidth Connections

The agent offsets the scans to the local machine. One of the advantages of agentless is that the bulk of the processing is done on the console. This involves network traffic and high CPU usage on the console, but the target is virtually unaware of any of this. If the agent runs the scan locally we reduce the WAN traffic from 2 - 4MB on average to 20 - 100KB on average to accurately scan and report the results to the database. An agent that also utilizes distribution servers for deployment purposes would do all of its major traffic on the local LAN and only a fraction of the WAN traffic would be required, reducing the impact on lower bandwidth connections.

Time to Implement

It typically will take 10 – 20 minutes to configure an agent policy. The rollout of the agents to the target machines may take several hours or several days depending on the number of machines and on the rollout option you choose. Rollout options are described in the next section.

AGENT ROLLOUT OPTIONS

Deploying the agent to an environment is no small task no matter what the product. Installing a piece of software on a machine that has to meet local prerequisites as well as communicate with a remote machine to pull down policy data involves a great many variables that can complicate matters. And then there is the delivery mechanism. Some environments may require multiple ways of installing an agent to do a successful rollout. Shavlik has simplified the agent installation process down to a single universal **STPlatformUpdater.exe** file. It is the same installer for all customers. This gives you a payload that can be delivered using a number of different methods.

Push Install from Console

Using Shavlik's agentless technology, you can push an agent install out by simply selecting a machine from the machine group or from Machine View and installing an agent with the policy desired. This is the quickest and easiest way to rollout the agent, but is bound by the same requirements as agentless scans.

Manual Installation

In cases where there are a small number of machines that are not reachable agentlessly, you can consider performing a manual agent installation. The manual process requires you to enter a few variables (console hostname, port, passphrase or credentials, and policy) during the installation of the agent. This can be done quickly and easily for small numbers of machines, but becomes less viable the larger the target base becomes.

The **STPlatformUpdater.exe** file used for manual installation can be found here:

C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFiles

Installing Agents from the Cloud

If you are using Protect Cloud synchronization, you have the ability to install a Shavlik Protect Agent from the cloud. This is particularly helpful if you have target machines that are away from the corporate network and unable to contact the console. For more information see *Installing and Supporting Agents on Internet-based Machines* on page 26.

The requirements for installing an agent with this method are:

- You must have a Protect Cloud account
- The target machine must have Internet access
- The Shavlik Protect console must be registered with Protect Cloud (**Tools > Operations > Protect Cloud Sync**)
- There must be at least one policy that is configured to allow synchronization with Protect Cloud (see the **Sync with Protect Cloud** check box on the agent policy **General Settings** tab)
- You cannot install a cloud-based agent on a Shavlik Protect console machine
- Each user that installs an agent must have administrator access on their target machine

Scripted Installation

The **STPlatformUpdater.exe** allows command-line execution so install can be scripted and delivered in a number of different ways. The command-line options are all detailed in the Help file (see “Manual agent installation script” in the Help index). Delivery of the **STPlatformUpdater.exe** and execution using a command-line can be performed in a number of different ways quickly and easily. The problem here typically is how many agent policies need to be rolled out. Each policy means a different script and then sorting out which machines get what can be more difficult.

Custom Patch

The ability to push the agent from the Shavlik Protect console is nice to have, but if you are pushing the agent to 1000 machines in a machine group that is setup by an IP range, and if you hit 90% of the targets the first time through, what do you do with the remaining 10%? Using Shavlik Protect’s custom patch feature we can scan the same group and detect if the agent is installed and only install on machines it is not installed on. This can be helpful in many ways. Every few weeks or months an additional scan can be run to pick up machines that may have slipped through the build process and not received an agent.

Other

Using the options above, you can get creative with scripting options and deliver the agent in a number of different ways. The **STPlatformUpdater.exe** file can be wrapped in a self-extracting zip to extract and execute a command-line installation that is delivered via email (the .exe file is roughly 7MB). This can be used to reach some users who are rarely in the office. The same could be delivered through a hosted weblink. The user would simply click on the download and run the file to execute. In this case the user doing the executing would need local administrator rights, but in many cases where the user is at a standalone site or is a heavy remote user this is often the case. For customers who image using ghost or sysprep or some other means, you cannot install the agent and make it part of your image due to the nature of how the agent registers itself with the console for security purposes. You can embed the scripted install into the image so that the first time it reboots it can run the agent installation and be up and running as part of the build process.

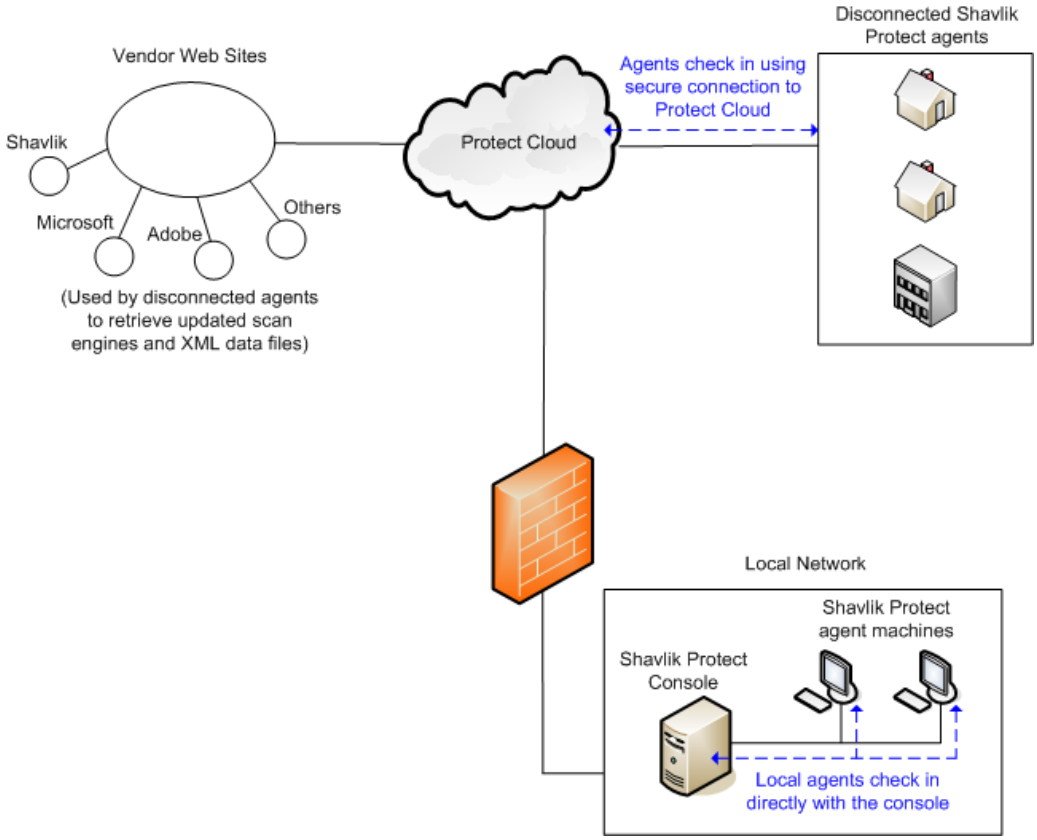
INSTALLING AND SUPPORTING AGENTS ON INTERNET-BASED MACHINES

This section provides a base recommendation for configuring an agent policy that supports machines outside the network environment. This configuration is ideal for laptop users who are frequently disconnected from the network but who are regularly connected to the Internet. It is also useful for standalone sites that do not have direct network connectivity but that do have Internet access.

In this solution your agents check in and receive policy updates from the cloud. This is accomplished using a Shavlik Protect feature called Protect Cloud synchronization. It allows you to manage agents on machines that are not able to communicate directly with the console. This feature also provides you with the ability to install a Shavlik Protect Agent using the Protect Cloud service.

Agents that are configured to use Protect Cloud will have two check-in options: they can continue to check in with the Shavlik Protect console, but they will also be capable of checking in and receiving policy updates via the cloud. This is particularly useful for disconnected agent machines that are away from the corporate network and unable to contact the console for updates. As long as an agent machine has Internet access, it will be able to send results and get updates using the cloud.

The following diagram illustrates the two agent check-in options:



When using Protect Cloud synchronization, the agent check-in process is as follows: At the scheduled check-in time, the agent will attempt to check in with the console. If the agent can access the console it will check in directly with the console. If the agent does not have access to the console but it does have Internet access, it will perform the check-in using the cloud.

When a disconnected agent checks in with the cloud it reports the same information (scan results, threat information, etc.) that it would to the Shavlik Protect console. Protect Cloud provides a generous amount of storage to cache results until the consoles retrieves the data. The console will automatically retrieve data from the cloud several times every hour.

Register the Console with Protect Cloud

1. (Recommended) Select **Tools** > **Edit database description** and make sure that the name the program uses when referring to the console database is a friendly name that has some meaning or significance to other users.

   This is the name that will be displayed within Protect Cloud after you register the Shavlik Protect console.

2. Select **Tools** > **Operations** > **Protect Cloud Sync** and register the Shavlik Protect console with the cloud service.

   The registration process establishes a secure communication channel between the console and the specified Protect Cloud account.

Configuration of the Agent Policy

1. On the main menu select **New > Agent Policy**.
2. Name the policy.
3. Configure options on the **General Settings** tab.

   You can configure the **Allow the user to** settings as you see fit. The recommendation is to disable **Cancel operations** 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 interval** area the recommendation is to configure frequent check-ins. This will keep the agent responsive to policy changes in your environment.

   In the **Engine, data, and patch download location** area, **Vendor over Internet** is recommended in this case as the agents are expected 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.

   In the **Network** area, enable the **Sync with the Protect Cloud** check box. This specifies that the agent will have the option to use Protect Cloud to retrieve the latest agent policy information, enabling it to perform synchronization via the cloud. This check box is only available if your console is registered with Protect

Cloud. When you click **Save and update Agents**, a copy of the agent policy and all necessary components will be written to the Protect Cloud service.

Agent listens for updates on port can be enabled. If you do, the recommended best security practice is to modify the firewall rules to block the port when outside the network and open the port while inside the network.

4. On the **Patch** tab, click **Add a Patch Task**, name the task, and configure the task.

   This policy is intended to focus on securing the target machine, so for this policy we recommend using **Security Patch Scan** as the patch scan template. You can choose to use a custom template if you wish, but we will stick to the basic security best practice for this example.

   Verify that the **Deploy patches** check box is enabled and choose a deployment template that specifies the following on the **Post-deploy Reboot** tab:

   - Reboot when needed
   - Schedule reboot **on the next occurrence of specified time**
   - Specify a time that is after hours so as not to interrupt the end users work day.

   You can specify **All patches detected as missing**, which would be the 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 data files.

   Enable the **Deploy service packs** check box. You can choose to deploy all service packs that are identified as missing by a scan, or you can limit the deployment to only those service packs you define in a service pack group. See *Details on the Agent-based Service Pack and Patch Deployment Process* on page 34 for more information.

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

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

   Here we will create two threat tasks: A **Quick Scan** which will do a scan of those locations commonly affected by threats, and a **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. It should be scheduled for a time of day when network traffic is lower, like the lunch hour. On the **Reboot Options** tab consider using the **On the next occurrence of specified time** option to reduce impact on each users' work day.

   The Full Scan is recommended to be done once per week and during 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 **Schedule** tab 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. On the **Reboot Options** tab 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.

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

   On the **Threat Actions** tab 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.

   Another approach is to initially quarantine everything. After monitoring the results for a week or two you should get a good feel for what settings make the best sense for your organization. If you see that something is routinely getting quarantined that you determine is actually safe (for example, cookies for frequently-visited websites), feel free to use a less restrictive setting for that category. This approach provides the most protection but may initially create a little extra work for your Technical Support department.

7. 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.

8. Configure options on the **Exceptions** 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.

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

   Shavlik recommends enabling Active Protection. You can configure Active Protection to **Allow**, **Allow Notify User**, or **Prompt User For Action** for specific activity on the target machine.

10. Click **Save and update Agents**.

Agent Install

There are two primary options for installing agents on machines that are located outside the network environment.

- You can perform a manual installation of the agent on each target machine
- You can install agents via the cloud using Protect Cloud

A manual installation is fine if you only have a small number of machines. If you have a large target base, however, the recommendation is to perform the agent installations via the cloud.

Make sure you meet the following requirements before attempting an agent installation from Protect Cloud:

- You must have a Protect Cloud account
- The target machine must have Internet access
- The Shavlik Protect console must be registered with Protect Cloud
- There must be at least one agent policy that is configured to allow synchronization with Protect Cloud
- You cannot install a cloud-based agent on a Shavlik Protect console machine
- Each user that installs an agent must have administrator access on their target machine

There are two basics steps to a cloud-based installation:

1. You (the adminstrator) must log on to Protect Cloud, create an agent key, and then email the key to the users of each target machine.
2. The user on each target machine will follow the email instructions to install and register the agent.

For detailed information on this process, in the Help system see **Installing Agents from the Cloud**.

When the process is complete, each of your agents should be able to pull policy updates and roll up results both internally and externally. You can test this by connecting a machine to the Internet outside your network, kicking off a scan manually and then watching for the results; repeat this from within your network.

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 **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**.

IMPLEMENTING A DISCONNECTED CONSOLE CONFIGURATION

Overview

A disconnected console is a remote console that does not have Internet access. There are a number of reasons you may choose to implement a disconnected console, but it is typically used at sites with strict security policies.

This section describes the tasks you must perform when implementing a disconnected console. It assumes you have access to a previously installed Shavlik Protect console that is connected to the Internet and that can be used to download the necessary files. A distribution server is not required, but if you prefer to use a distribution server to support the disconnected console, please see the *Disconnected Console Configuration* section in the Help system.

Installing and Activating Shavlik Protect from a Disconnected Console

Important! Contact your sales representative to verify that your current license key supports multiple console installations.

1. On the disconnected console, install Shavlik Protect by following the instructions in the *Shavlik Protect Installation Guide*.

   This guide is available at: http://www.shavlik.com/support/protect/documentation

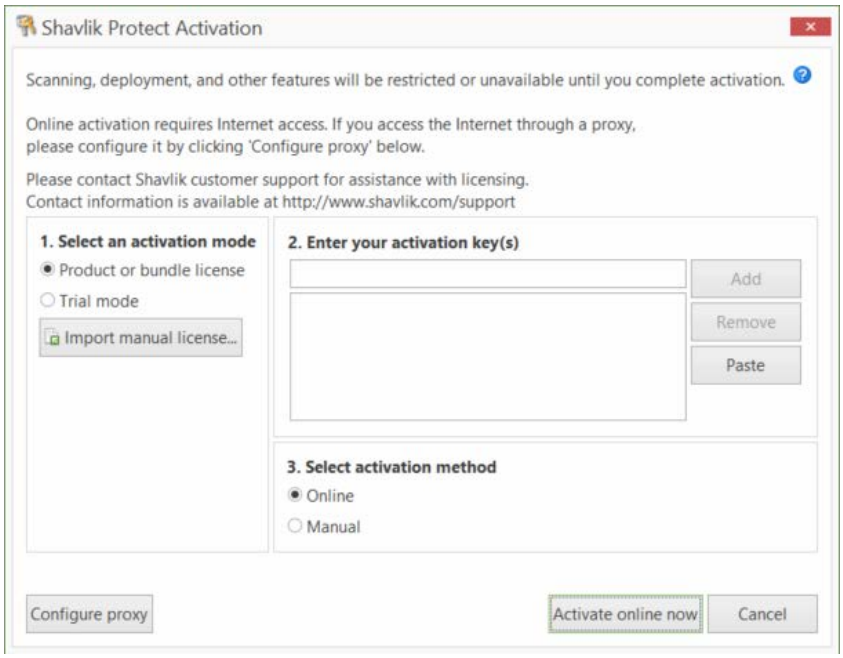
   Tip: Make sure your console machine meets all the system requirements listed in the *Shavlik Protect Installation Guide*. If you are missing any of the required software you must download it from a connected machine and then manually install it on the disconnected console.

2. If you have an electronic copy of your license key(s) copy it to the console's clipboard.

   Your license key(s) is typically sent to you in an e-mail from Shavlik when you purchase the product.

3. From the Shavlik Protect menu select **Help > Enter/refresh license key**.

   The **Activation** dialog is displayed.



The program should automatically detect the activation key and paste it in the appropriate boxes. If it doesn't, click **Paste**.

4. Select **Product or bundle license**.
5. Select **Manual**.
6. Click **Create request**.

   Two files are generated and saved to the desktop of your console computer: an XML file named **LicenseInfo.xml** and a text file named **DisconnectedLicenseInfo.txt**. The XML file is used in this procedure.

   Note: The text file is used if you are activating from a secure disconnected network that does not allow files to be transferred out of the secure environment. See *Activating the Program* in the Help system for more details.

7. Move the XML activation request file to a computer that has an Internet connection.
8. On the Internet-connected computer, open a browser and go to https://license.shavlik.com/OfflineActivation.
9. Upload the **LicenseInfo.xml** activation request file.

   The web portal will process the license information and generate a license file.

10. Download the processed license file and move it to the console computer.
11. Within Shavlik Protect, select **Help > Enter/refresh license key**.
12. On the Shavlik Protect **Activation** dialog, click **Import manual license**.
13. Go to the location of the processed license file and then click **Open**.

    Shavlik Protect will process the file and the program will be activated.

14. Select **Tools > Auto-update Definitions** and make sure the command is not enabled.

Updating the Program Files

1. On a Shavlik Protect console that is connected to the Internet, update the current data files on it by selecting **Help** > **Refresh files**.

   This will download the latest scan engines and XML data files to the following folder:

   C:\ProgramData\LANDESK\Shavlik Protect\Console\DataFiles

2. Copy all the files in this folder to a media that can be transported to the disconnected console.
3. Copy all the files to the same folder on the disconnected console.

Downloading Missing Patches

Once the data files are updated on the disconnected console you can begin performing patch scans of your inside (non-networked) machines. Before you can deploy missing patches you must locate and transfer the missing patches to the disconnected console.

1. Use Machine View to view the list of missing patches.
2. Export the list of missing patches to a .csv file by right-clicking **Patch Missing** and selecting **Export selected patches to CSV**.

   You can use the .csv file as a reference when downloading the patches from the Internet-facing console. Another option is to generate a report that lists the missing patches.
3. On the Internet-facing console, use the Patch View smart filters to locate the patches that are missing on the disconnected console.
4. Right-click the patches and download them to the Internet-facing console.

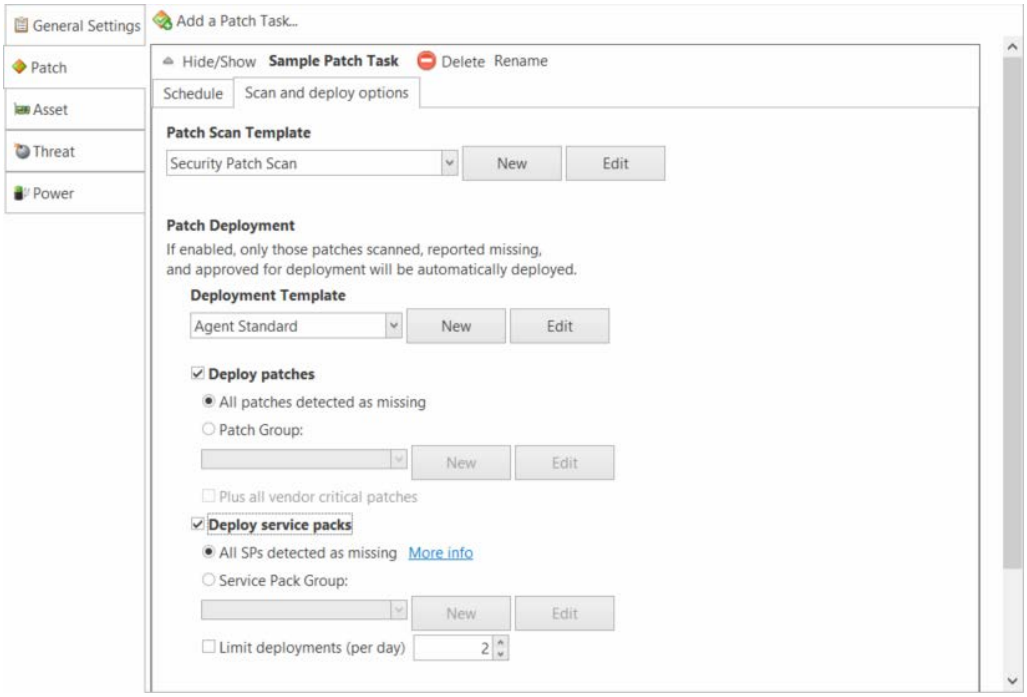
   The downloaded patches are stored in the following directory:

   C:\ProgramData\ LANDESK\Shavlik Protect\Console\Patches
5. Copy all the files in this folder to a media that can be transported to the disconnected console.
6. Copy all the files to the same folder on the disconnected console.

The disconnected console can now deploy patches to the inside machines.

DETAILS ON THE AGENT-BASED SERVICE PACK AND PATCH DEPLOYMENT PROCESS

You have the ability to use agents to deploy both service packs and patches. On an agent machine that is missing both service packs and patches, service packs are deployed first.



Service Pack Deployment Process

If an agent machine is missing multiple service packs, only one service pack will be installed at a time. The agent patch task will begin by initiating the download of the first service pack. Operating system service packs are downloaded at a higher priority than product service packs. After the service pack is successfully installed, the machine is restarted, rescanned, and the process is repeated until all service packs are deployed or until the daily limit is reached [see the **Limit deployments (per day)** option].

Limiting the Number of Service Packs That Can be Deployed in One Day

You can use the **Limit deployments (per day)** option to specify the maximum number of service packs that can be deployed to a machine in one day. Service packs can take a long time to deploy and almost always require a reboot of the machine, so you typically want to keep this number rather small. If you do not limit the number of service pack deployments in a day you run the risk of overwhelming a machine if it is missing a large number of service packs. If a machine is missing more service packs than the specified limit, the additional service packs will be deployed the next time the patch task is run.

Note that a "day" in this case is considered to be a calendar date and not a 24 hour period. This means the day is reset at midnight. If you were to schedule the patch task to run on an hourly basis (not recommended), it would allow you to maximize an overnight maintenance window by deploying the maximum number of service packs before midnight and then again immediately after midnight.

Patch Deployment Process

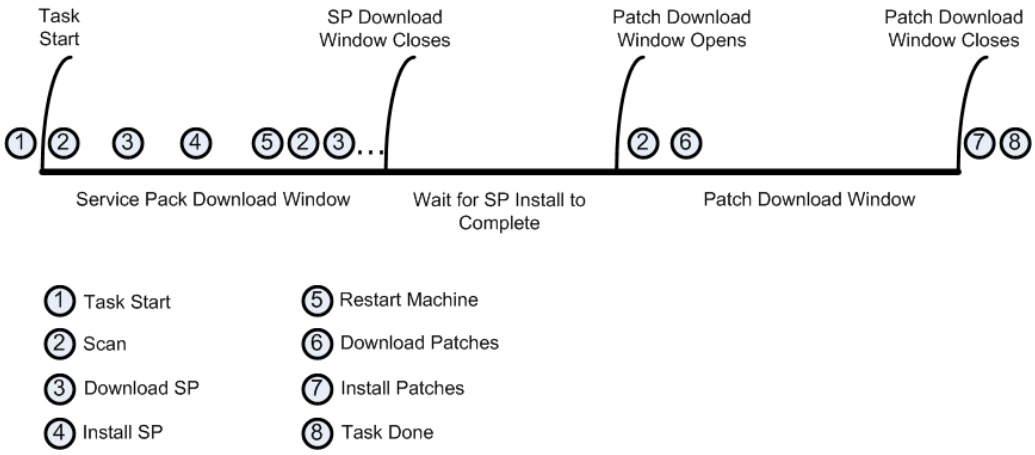
Once the list of approved patches is determined, the patches are downloaded and installed according to their priority. Security patches are downloaded first, followed by all other patch types.

Service Pack and Patch Download Process

Each agent patch task is allocated a two hour total maintenance window that is allocated for downloading missing service packs and patches.

- Service packs are allotted a 60 minute window to complete the *download > install > restart > rescan* process.
- Patches are allotted a separate 60 minute window to download the missing patches.

Only those service packs and patches that are successfully downloaded during their respective 60 minute window will be installed by the active patch task. If the patch task cannot finish downloading all missing service packs during the first 60 minute window, the remaining service packs will be identified, downloaded, and installed the next time the patch task is run. Likewise, if the patch task cannot finish downloading all missing patches during its 60 minute window, the remaining patches will be identified, downloaded, and installed the next time the patch task is run.



Background Downloads and Checkpoint/Restart

The downloads occur in the background using idle bandwidth not being used by other applications. Foreground tasks such as Web browsing are not affected by the service pack and patch download process.

If an agent machine becomes disconnected from the network during a file download, the process will be suspended and will automatically resume where it left off when the network is available again. This technique is called *checkpoint/restart* and is extremely useful for machines that are frequently disconnected.

GUIDE TO SURVIVING PATCH TUESDAY

Overview

Patch Tuesday affects us all. This section is intended to give a workflow for 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, and keeping up with what each product in your environment is doing can be a daunting task. Below are several sources that can be helpful in keeping up with what patches are being released and what that means for you.

The single best source for information 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 using any of the following methods:

- Email: http://www.shavlik.com/support/xmlsubscribe/
- RSS: http://protect7.shavlik.com/feed/
- Twitter: @shavlikXML

Previous XML announcements can be viewed by scrolling through the news feed located at the bottom of the Shavlik Protect home page.

Another excellent source is the Shavlik blog (http://blog.shavlik.com). We typically provide a preview of new patches that are coming out as well as a round-up discussion of issues uncovered during the implementation of the patches.

Just knowing what 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 includes an *Exploitability Index* that contains additional information about each patch. 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.mspx

  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 a diligent patch management process. 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 second Tuesday of every third month.

http://voices.washingtonpost.com/securityfix/2009/05/adobe_adopts_microsofts_patch.html

Shavlik also provides a series of webinars on *Minimizing the Impact of 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 at the Shavlik Webinars page.

http://www.shavlik.com/webinars/

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 website created by security experts to provide a community for discussing all thing**s** 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 is meant to remain as vendor agnostic as possible.

http://www.patchmanagement.org

MICROSOFT SQL SERVER DATABASE MAINTENANCE

If you are at a company that is running Shavlik products in a full SQL Server environment and have a database administrator on staff with SQL Server maintenance and backup policies already running against our databases, great! If you are running SQL Server Express or a full edition of SQL Server but don't have a maintenance and backup plan in place, please keep reading.

Database instability and corruption is the single biggest cause of an upgrade issue that is encountered and the root cause of many GUI performance issues that can be mitigated and, in many cases, resolved by proactive maintenance on the database. Below are our recommendations for good regular maintenance on your database so you keep it running slim and clean for good performance and to reduce issues.

Keep in mind this is a starting point. If you have regulatory needs that require more data kept live you should adjust to keep more data live. If that is the case you may want to analyze how frequently you are scanning. 1000 agents scanning 8 times a day will grow your database at a much more rapid rate than once per day or once per week. And in most cases, you don't really need all of that data.

The following are our recommendations for regular database maintenance.

Data Retention

Determine the amount of data that needs be kept on hand for operational purposes. Typically 60-90 days is acceptable for operational purposes. Use the Shavlik Protect Database Maintenance tool to cleanup anything older than that number of days and schedule the task to run on a regular basis.

Reporting

Determine what report data is required for audit\regulatory requirements. Run monthly reports to fulfill these needs and keep the reports on file as far back as your policy requires. Typically, 13 months is an acceptable amount of time to save report data.

DB Backups

Shavlik recommends running weekly incremental and monthly full backups. The backup should be run just before your scheduled purge. Keep backups as far back as the reporting data.

DB Maintenance Schedule

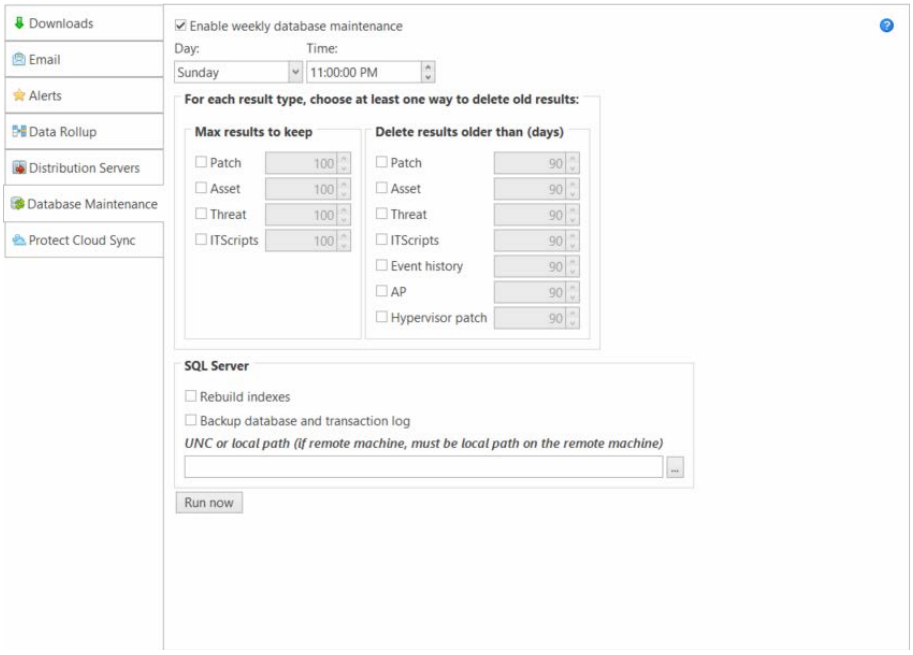
- **Backups:** Full monthly, just after patch maintenance for that month. Incremental weekly, end of each week (after weekend patch windows preferably).
- **Purge Data:** After the full monthly backup is run
- **Reindex:** After purge data is run
- **Integrity:** After reindex is run

SQL Server Express Users Can Use the Database Maintenance Tool

SQL Server Express users who do not have access to the SQL Server Maintenance Plan Wizard can use the Shavlik Protect Database Maintenance tool. The Database Maintenance tool enables you to:

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

You do this by selecting **Tools > Operations > Database maintenance** and then specifying exactly when and how your database maintenance tasks should be performed. See the Shavlik Protect Help file for information on the database maintenance options.



Full SQL Server Users Should Use the SQL Maintenance Plan Wizard

If you are using a full edition of SQL Server you should use the SQL Server Maintenance Plan Wizard to setup your maintenance plans. You could use the Shavlik Protect Database Maintenance tool, but the SQL Server Maintenance Plan Wizard is more robust and provides additional functionality.

Use the following link for information on using the wizard to implement your maintenance plan:

http://www.networkworld.com/subnets/microsoft/110107-ch8-sql-server.html?page=2