Shavlik Protect

Virtual Machine Quick Start Guide

shavlik

Copyright

Trademarks

Document Information and Print History

Document number: N/A

Date	Version	Description
August 2008	Shavlik NetChk Protect 6.5	Initial release of the **Offline Virtual Image Quick Start Guide**.
June 2009	Shavlik NetChk Protect 7.0	Updated for interface changes in version 7.0.
August 2009	Shavlik NetChk Protect 7.1	Removed "Offline" from document name. Updated for interface changes in version 7.1.
April 2010	Shavlik NetChk Protect 7.5	Improved scan capabilities for offline virtual machines, new VM notes, interface changes.
August 2010	Shavlik NetChk Protect 7.6	Update product branding.
March 2011	Shavlik NetChk Protect 7.8	Add new credential, snapshot, deployment, and virtual machine template info.
October 2011	VMware vCenter Protect 8.0	Update product branding and UI references for version 8.0.
September 2012	VMware vCenter Protect 8.0.1	Update product name and version, update cover graphics.
May 2013	Shavlik Protect 9.0	Rebrand to Shavlik Protect. Account for navigation pane and menu changes.
April 2014	Shavlik Protect 9.1	Update Web links and references to legacy files and screenshots.
September 2015	Shavlik Protect 9.2	Update to reflect user interface changes.

Table of Contents

VIRTUAL MACHINE OVERVIEW

Tip: To view a video tutorial on this topic, click the video icon.

A virtual machine is not actually a physical machine but rather a software environment (usually an operating system) designed to emulate a physical machine. A virtual machine can run programs just like a physical machine. The physical machine used to host the virtual machine can often support multiple virtual machines.

Shavlik Protect can scan for and deploy patches to the virtual machines on your network regardless of whether they are online or offline. It can also perform a software asset scan of your online and offline virtual machines.

Online Virtual Machines

A virtual machine that is online and running is treated by Shavlik Protect the same as a physical machine. Patch scans and asset scans will be performed in the same manner as on a physical machine. Any patches that may be missing can also be deployed in the same manner to both your physical machines and your online virtual machines. This means your online virtual machines are protected by the latest software patches just like your physical machines.

Offline Virtual Machines

Shavlik Protect also enables you to scan and patch offline virtual machines. Offline virtual machines are those that aren't powered on when a patch scan or an asset scan is performed. These virtual machines may be powered on for only a few hours or days a month and then powered off until they are needed again the next month. It's important to ensure that these systems are patched so that when they are brought online they don't place your network at risk.

Shavlik Protect makes it easy to scan these offline virtual machines. When you initiate a scan of a machine group that contains offline virtual machines, Shavlik Protect will perform a full assessment of the offline virtual machines and display the scan results alongside the results for running systems. Offline virtual machines will be differentiated in the patch scan results by a unique icon ( ). The scan results may even identify offline virtual machines that you don't even know about. When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was offline at the time of the scan.

Patching offline virtual machines is similarly simple. You simply highlight the machines and patches you'd like to install and then select **Deploy** from the Shavlik Protect menu. For offline virtual machines that are hosted on a server, the machines will be powered on, the patches installed, and the machines powered back down. For offline virtual machines that reside on workstations, the patches will be copied to the offline virtual machines and will be installed the moment that the virtual machine is started (or according to the scheduled patch deployment time).

Virtual Machine Templates

Virtual servers and virtual workstations are often created using a template. Templates enable you to quickly create new virtual machines that conform to your particular configuration requirements. A template that is offline poses no danger to your organization. A template that is brought online, however, is no different than an online virtual machine. It can perform tasks just like any other virtual machine, and it can also contain the same viruses, spyware, and other types of malware that target improperly patched machines. For this reason it is critical that your virtual machine templates receive the same patch management care as your physical and virtual machines.

Shavlik Protect enables you to patch your virtual machine templates. You simply add your templates to a machine group and Shavlik Protect will take of the rest. For complete details on the virtual machine template scan and deployment process, see *Notes About Virtual Machine Templates*.

System Requirements

Shavlik Protect supports offline virtual machines created by any of the following:

- VMware ESXi 5.0 or later (VMware Tools is required on the virtual machines)
- VMware vCenter (formally VMware VirtualCenter) 5.0 or later (VMware Tools is required on the virtual machines)
- VMware Workstation 9.0 or later
- VMware Player

Requirements for Successful Scans and Deployments to Virtual Machines

An offline virtual machine (workstation-based or hosted on a server) is a file or set of files. To scan or deploy to an offline virtual machine requires permissions to the file system where the files reside. An online virtual machine is almost indistinguishable from a physical machine. To deploy patches to an online virtual machine requires credentials for an administrator account on the virtual machine operating system.

Because of the differences between online and offline virtual machines, you may need to provide two sets of credentials – one for when the virtual machine is in the online state and one for when it is in the offline state.

For workstation virtual machines, if you wish to scan and/or deploy to the virtual machine in either its online or offline state, you should add the virtual machine to the machine group twice:

- For its online state, enter the machine identifier and online credentials in the machine group as you would any physical machine – on the **Machine Name**, **Domain Name**, **IP Address/Range**, or **Organizational Unit** tab.
- For its offline state, enter the information and credentials for the virtual machine file locations on the **Workstation Virtual Machines** tab.

For hosted virtual machines, you only need to specify the machine once, on the **Hosted Virtual Machines** tab. Separate credentials, however, are still required to access the machine in either the online or offline state. The browse credentials you enter when connecting to the VMware server are used when the machine is in the offline state. You should enter online credentials for each hosted virtual machine using the **Set Admin Credentials** option in the bottom pane of the machine group editor.

The following table summarizes the credentials used for various machine types.

Machine Type	Machine State	Machine Group Tab	Credentials Required
Physical Machine	Online	**Machine Name**, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Machine or machine group credentials
Workstation VM	Online	**Machine Name**, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Machine or machine group credentials
Workstation VM	Offline	**Workstation Virtual Machines**	Machine or machine group credentials
Hosted VM	Online	**Hosted Virtual Machines**	Machine or machine group credentials
Hosted VM	Offline	**Hosted Virtual Machines**	Browse credentials (the creds used to log on to the VM server)

Note: Integrated credentials will not work for deployments to offline virtual machines.

If you specify both online and offline credentials for virtual machines, you will be able to scan and deploy to those virtual machines whether they are online or offline.

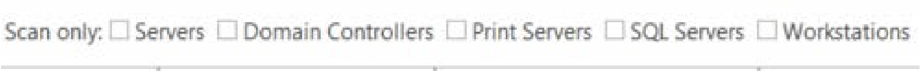
Notes About Virtual Machines

Requirements

- Dual boot systems (for example, a virtual machine with two partitions, each containing a different operating system) are not supported.
- When scanning virtual machines that are supported by VMware, please keep in mind the following:
  - You cannot mount encrypted virtual disks
  - You cannot mount a virtual machine if any of its .vmdk files are compressed or have read-only permissions
  - You cannot mount a virtual machine that is currently being used by a running or suspended virtual machine
  - Linked clones and compressed images are not supported

General Notes

- Only the current state of the virtual machine will be scanned and patched. Snapshots of virtual machines are not scanned or patched.
- A virtual machine is counted only once against the total number of license seats available, even if it is scanned both in online (powered on) mode and offline (powered off) mode.
- In machine groups and in scan results, special icons will distinguish an offline virtual machine (🖥) from a physical machine or an online virtual machine (🖥) and from a virtual machine template (🗎).
- Avoid using network drive letters when defining offline virtual machines in a machine group. The recommended practice is to instead specify the Uniform Naming Convention (UNC) path. This comes into play when performing a scheduled scan on an offline virtual machine. Network drive mappings are session-specific, so it is very possible that a specified mapping will no longer exist when the scheduled scan process is run.
- Within a machine group, the **Scan only** filters do not apply to offline virtual machines or to virtual machine templates.



Scan only: □ Servers □ Domain Controllers □ Print Servers □ SQL Servers □ Workstations

- It is possible for two offline virtual machines to have the same domain and computer name. This will be the case if you clone a virtual machine and do not change the computer name or domain name on one or both machines. In this situation, of the two duplicate virtual machines, only the last one scanned will be visible in Machine View. The machines displayed in Machine View are keyed on domain and computer name and duplicates are not allowed.
- Virtual machines that are offline (powered off) will be mounted before they are scanned. Virtual machines that are online (powered on) do not need to be mounted as they are treated no differently than a regular machine.
- When performing a patch or an asset scan, a virtual machine that was added to a machine group as an offline virtual machine but that is online at the time of a scan will be scanned if it is hosted on an ESX server and if the proper credentials are available in order to access that machine. (See *Supplying Credentials for Virtual Machines* for details.) Online virtual machines that are hosted on workstations will fail to mount and will not be scanned.
- When scanning multiple virtual machines that are hosted on one workstation, it is possible to reach the connection limit for that workstation. If the connection limit is reached an error will occur and the scans will fail. The maximum number of simultaneous connections supported varies for each Windows OS. For example, Windows XP only allows a maximum of 10 simultaneous connections while servers allow many more. See http://support.microsoft.com/kb/314882 for more information.

Patch Deployments

- When deploying patches to an offline virtual machine that is hosted on a server, the virtual machine will be powered on, the patches installed, and the virtual machine powered down. See *Deploying Patches to Virtual Machines* for more details.
- When deploying patches to an offline virtual machine that is hosted on a server, VMware tools must be installed on the virtual machine.
- When deploying patches to an offline virtual machine that is hosted on a server, the following VMware server permissions are required in order to manage snapshots and to change the power state of the machine during the deployment process:
  - VirtualMachine.State.CreateSnapshot
  - VirtualMachine.State.RemoveSnapshot
  - VirtualMachine.Interact.PowerOn
  - VirtualMachine.Interact.PowerOff
  - VirtualMachine.Interact.DeviceConnection (to disable/enable the network card)
- When deploying patches to an offline virtual machine that resides on a workstation, the new deployment job will overwrite any older deployment jobs that have not yet been performed. For this reason you should deploy all desired patches in a single deployment.

  Example: You deploy Patch A to a workstation-based offline virtual machine. The virtual machine is still offline a month later when you deploy Patches B and C. Because the first deployment job was never executed it gets overwritten and only Patches B and C are now scheduled for deployment. To avoid this you simply include Patch A along with Patches B and C in the second deployment job.

  One way to manage this is to use a patch group to define the patches you want deployed to your workstation-based virtual machines. When new patches are identified you simply add them to the list of patches in the patch group. This is particularly useful when specifying a patch group within a patch scan template and then enabling the **Auto-deploy patches after scan** check box on the **Run Operation** dialog. See *Performing Patch Scans* in the Help file for more details about these options.

Agents

- Shavlik Protect Agent operations are not supported on offline virtual machines.
- If you install Shavlik Protect Agent on an online virtual machine and then later scan the virtual machine while it is in an offline state, Shavlik Protect may report the wrong agent status for that image. For example, it may show that the agent is not installed, or it may let you attempt to uninstall the agent. This occurs because agent operations are not supported on offline virtual machines. The correct status will be reported once the virtual machine is brought back online and rescanned by Shavlik Protect.

Notes About Virtual Machine Templates

General Notes

- For information on using virtual machine templates in patch scans, asset scans, and patch deployments, see *Roadmap of Tasks*.
- The type of virtual machine template (server template, workstation template, etc.) does not matter, they are all supported by Shavlik Protect.
- Only virtual machine templates that are hosted on a VMware server are supported by Shavlik Protect. The templates are added to a machine group using the **Hosted Virtual Machines** tab. Virtual machine templates that reside on individual workstations are not supported.
- A unique icon (📄) is used to identify virtual machine templates. You will see this icon when adding a template to a machine group and when viewing scan results in Scan View and in Machine View.
- As with anything that involves components on a network, errors can occur if connections go bad, if servers are shut down, if a template is modified while being accessed by Shavlik Protect, etc. In general, the templates should not be touched at any time during the scanning or patch deployment process.
- When you initiate a patch or an asset scan of a virtual machine template, Shavlik Protect will scan the template in its current state and will report the results in the same way it does for virtual machines and physical machines.
- During a scan, a template will be accessed using the VMware server credentials. Any individual credentials supplied for the template are ignored.
- You should supply online credentials for any virtual machine template that will be included in a patch deployment process. During the patch deployment process the template is converted to a virtual machine and powered on—Shavlik Protect will need the supplied credentials in order to access the online version of the machine.

Patch Deployments

- When deploying patches to a virtual machine template, the following VMware server permissions are required in order to manage snapshots and to perform the deployment:
    - VirtualMachine.State.CreateSnapshot
    - VirtualMachine.State.RemoveSnapshot
    - VirtualMachine.Provisioning.MarkAsTemplate
    - VirtualMachine.Provisioning.MarkAsVM
- The patch deployment template you use must not specify the use of a distribution server. The virtual machine will be disconnected from the network and unable to download the patches from the distribution server.
- The patch deployment template you use must not specify the use of an Office media path. The offline virtual machine will be disconnected from the network and unable to access the location of the original Office installation media.
- The patch deployment template you use should not specify a pre-deploy reboot (the program will be unable to initiate the reboot because the machine will be

offline) but it should always perform a post-deploy reboot (this is a "best practice" when deploying patches). For deployments to virtual machine templates it is recommended you use the **Virtual Machine Standard** deployment template.

- During a patch deployment, a virtual machine template that may normally be available only to an administrator will become visible to other users. This is because during the patch deployment process the template is temporarily converted to a virtual machine and powered on.

Roadmap of Tasks

Patch Tasks

Shavlik Protect can scan for and deploy patches to online virtual machines, to offline virtual machines, and to virtual machine templates. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines and virtual machine templates you want to scan and patch.

   See *Adding Virtual Machines to a Machine Group* on page 13 for details.

2. Supply credentials for the virtual machines.

   When performing scans, the recommended best practice is to always supply credentials for the virtual machines and virtual machine templates. When performing patch deployments, credentials must be set at the machine, group, or default level. See *Supplying Credentials* on page 17 for details.

3. Use the machine group in a scan.

   See *How to Scan Virtual Machines* on page 19 for details.

4. Review the scan results. See *Reviewing Scan Results* on page 20 for details.

   In the scan results, unique icons will distinguish an offline virtual machine ( ) from a physical machine or an online virtual machine ( ) and from a virtual machine template ( ). When viewing machines in Machine View the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

5. (Optional) If you want to take snapshots of your hosted virtual machines and templates immediately before and/or immediately after the deployment process, make sure you specify this on the **Hosted VMs/Templates** tab of the deployment template you plan to use.

6. Deploy the desired patches to the desired virtual machines and virtual machine templates. See *Deploying Patches to Virtual Machines* on page 23 for details.

   You may not know if a particular virtual machine is online or offline at the time you perform a deployment, and it typically doesn't matter. The following guidelines apply for patch deployments to virtual machines:

   - If a virtual machine is hosted on a server, the deployment can be successful regardless of whether the virtual machine is online or offline at the time of the deployment.
   - If a virtual machine is defined in a machine group using the **Workstation Virtual Machines** tab, the deployment can be successful as long as the virtual machine is offline.

- If a virtual machine is defined in a machine group using the **Machine Name**, **Domain Name**, or **IP Address/Range** tab, the deployment can be successful as long as the virtual machine is online.

  If a virtual machine is online the patch deployment is performed in the same manner as for a physical machine. Patch deployments to offline virtual machines and to virtual machine templates are performed by Shavlik Protect in a slightly different manner. See *Deploying Patches to Virtual Machines* on page 23 for details.

7. Monitor the deployment activities.

   See *Monitoring Patch Deployments to Virtual Machines* on page 28 for details.

Asset Management Tasks

Shavlik Protect can perform asset management scans of online virtual machines, of offline virtual machines, and of virtual machine templates. You do this by performing the following tasks:

1. Create one or more machine groups that contain the virtual machines and virtual machine templates you want to scan.

   See *Adding Virtual Machines to a Machine Group* on page 13.

2. Supply credentials for the virtual machines and virtual machine templates.

   See *Supplying Credentials* on page 17 for details.

3. Use the machine group in an asset scan.

   See *How to Scan Virtual Machines* on page 19.

4. Review the asset scan results.

   See *Viewing Virtual Asset Summaries* in the Help system for details.

   When viewing machines in Machine View the Offline Scan column in the top pane will indicate if a virtual machine was online or offline at the time of the scan.

Power Management Tasks

You can use Shavlik Protect to power on and off the virtual machines that reside on your ESXi hosts. For more information, access the Help system and see the section titled **Managing Your vCenter Servers and ESXi Hypervisors**.

ADDING VIRTUAL MACHINES TO A MACHINE GROUP

Virtual machines can be added to a machine group. The recommended best practice is to create a machine group consisting of nothing but virtual machines. You can, however, add both physical machines and virtual machines to the same machine group if you wish.

There are four different ways to add virtual machines to a machine group:

- If virtual machines are hosted by a server you can add the server to the machine group. This effectively adds all virtual machines hosted by the server to the machine group. The virtual machines can be in either online or offline mode. See *Adding Servers and Virtual Machines Hosted by a Server* for details.
- If virtual machines are hosted by a server you can add individual virtual machines and virtual machine templates to the machine group. The virtual machines can be in either online or offline mode. See *Adding Servers and Virtual Machines Hosted by a Server* for details.

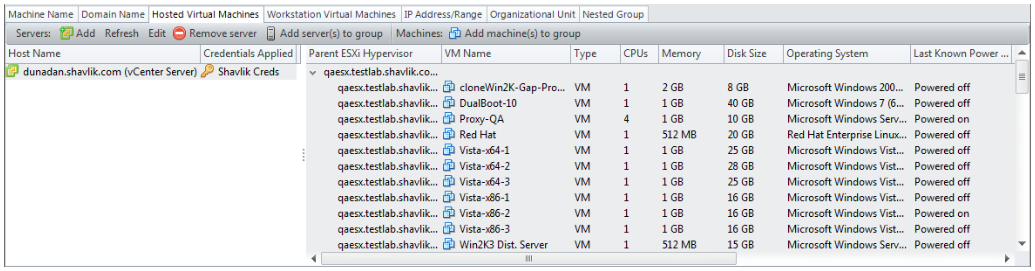
  You can also add virtual machine templates that may be hosted on a server. See *Notes About Virtual Machine Templates* for details.
- If virtual machines reside on individual workstations you may consider adding the machines to the group twice to ensure that each virtual machine is successfully scanned regardless of its current power state (online or offline).
  - You can add the full path names or directory names of the offline virtual machines to the machine group using the **Workstation Virtual Machines** tab. The virtual machines defined using this tab are scanned only if they are in offline mode. See *Adding Offline Virtual Machines That Reside on Workstations* on page 15 for details.
  - You can add the virtual machines to the machine group using the **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab. The virtual machines defined using this tab are scanned only if they are in online mode.

Adding Servers and Virtual Machines Hosted by a Server

Many organizations will host their virtual machines on one or more VMware servers. Doing so provides the means to manage the virtual machines in an organized fashion. There are two main types of VMware servers:

- **VMware ESX/ESXi Servers**: A server dedicated to hosting and managing multiple virtual machines. VMware ESX/ESXi servers (also referred to as ESXi hypervisors) are typically used in small- and medium-sized organizations that want to control multiple virtual machines from one location. The server often runs on a dedicated blade computer that is using a VMware operating system.
- **VMware vCenter Servers**: This type of server is typically used by large organizations that need to manage multiple VMware ESX/ESXi servers, each of which may be running multiple VMware images. For example, you can quickly move a highly-utilized virtual machine from a busy ESXi server to another less busy ESXi server.

You can use the **Hosted Virtual Machines** tab to log on to these servers and select the virtual machines and the virtual machine templates you want to include in your machine group. The virtual machines and templates can be in either offline or online mode.



Host Name	Credentials Applied
dunadan.shavlik.com (vCenter Server)	Shavlik Creds

Parent ESXi Hypervisor	VM Name	Type	CPUs	Memory	Disk Size	Operating System	Last Known Power ...
qaesx.testlab.shavlik.co...							
qaesx.testlab.shavlik...	cloneWin2K-Gap-Pro...	VM	1	2 GB	8 GB	Microsoft Windows 200...	Powered off
qaesx.testlab.shavlik...	DualBoot-10	VM	1	1 GB	40 GB	Microsoft Windows 7 (6...	Powered off
qaesx.testlab.shavlik...	Proxy-QA	VM	4	1 GB	10 GB	Microsoft Windows Serv...	Powered on
qaesx.testlab.shavlik...	Red Hat	VM	1	512 MB	20 GB	Red Hat Enterprise Linux...	Powered off
qaesx.testlab.shavlik...	Vista-x64-1	VM	1	1 GB	25 GB	Microsoft Windows Vist...	Powered off
qaesx.testlab.shavlik...	Vista-x64-2	VM	1	1 GB	28 GB	Microsoft Windows Vist...	Powered off
qaesx.testlab.shavlik...	Vista-x64-3	VM	1	1 GB	25 GB	Microsoft Windows Vist...	Powered off
qaesx.testlab.shavlik...	Vista-x86-1	VM	1	1 GB	16 GB	Microsoft Windows Vist...	Powered off
qaesx.testlab.shavlik...	Vista-x86-2	VM	1	1 GB	16 GB	Microsoft Windows Vist...	Powered on
qaesx.testlab.shavlik...	Vista-x86-3	VM	1	1 GB	16 GB	Microsoft Windows Vist...	Powered off
qaesx.testlab.shavlik...	Win2K3 Dist. Server	VM	1	512 MB	15 GB	Microsoft Windows Serv...	Powered off

1. Log on to the desired server by clicking **Add** and then specifying the server name and the proper credentials.

   The credentials you use to log on to the server are called *browse credentials*. They will be used to connect to the server and to enumerate the machines hosted by the server.

   After a connection is made the server is displayed in the left-hand pane. The virtual machines hosted by the server are displayed in the right-hand pane. At this point you can either add the server itself to the group or you can add individual virtual machines and virtual machine templates.

   Note: You must have server permission set on the datacenter, the folder, or the individual virtual machines in order for the machine to be displayed. If you don't have permission for a specific virtual machine it will not be displayed in the right-hand pane.

   Tip: You can log on to multiple servers at the same time. All virtual machines found on the servers are displayed in the right-hand table.

2. To add all machines hosted by a server, select the server in the left-hand pane and click **Add server(s) to group**.

3. To add individual hosted machines, in the right-hand pane select the virtual machines you want to add to the machine group and then click **Add machine(s) to group**.

   The virtual machines are added to the bottom pane of the machine group.

4. Supply any credentials that may be needed for the individual virtual machines and virtual machine templates.

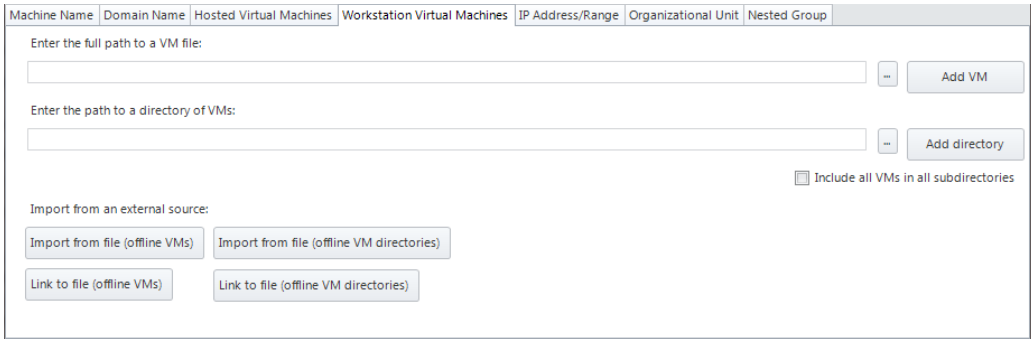
   See *Supplying Credentials for Virtual Machines* for details.

Adding Offline Virtual Machines That Reside on Workstations

Some virtual machines may reside on individual workstations. Any machine using VMware Workstation software is capable of supporting a virtual machine. The virtual machines may reside almost anywhere, including hard drives, network drives, jump drives, etc. You use the Workstation Virtual Machines tab to add these stand-alone offline virtual machines to a machine group.

Note: This tab is used to specify the offline identity of each virtual machine. If a virtual machine added here is online when a scan is performed, a mounting error will occur and the scan of that machine will fail.

Tip: If you want to be absolutely sure that all your virtual machines are successfully scanned, simply add the same machines to the group a second time using one of the other tabs (**Machine Name**, **Domain Name**, or **IP Address/Range**). This duplication assures that each virtual machine will be successfully scanned regardless of its power state (online or offline).


Machine Name
Domain Name
Hosted Virtual Machines
Workstation Virtual Machines
IP Address/Range
Organizational Unit
Nested Group
Enter the full path to a VM file:
...
Add VM
Enter the path to a directory of VMs:
...
Add directory
□ Include all VMs in all subdirectories
Import from an external source:
Import from file (offline VMs)
Import from file (offline VM directories)
Link to file (offline VMs)
Link to file (offline VM directories)

The virtual machines specified here are the actual images and you must therefore specify the full path name. Once the virtual machine is added to a machine group you should also specify the credentials used to connect to that virtual machine (see *Supplying Credentials* on page 17). This is different from virtual machines hosted by a server. On a server you can simply reference a file that points to the actual virtual machine, letting the server manage the path and credential information.

Adding a Virtual Machine Residing on a Workstation

There are two ways to add an offline virtual machine that is hosted on a workstation:

- In the **Enter the full path to a VM file** box, type the full path name of the virtual machine. You must specify the full path name and not just the name of the virtual machine. The name must contain a valid image extension (such as .vmx) and must not contain any illegal characters (such as @, ", etc.). When possible, avoid using network drive letters; the recommended practice is to instead specify the Uniform Naming Convention (UNC) path. For example: \\machinename\sharename\directory\machine.vmx.
- Click the Browse button (...) and locate the virtual machine by browsing your local machine and your network for the desired file.

Once the virtual machine is defined, click **Add VM** to add it to the machine group list.

Add a Directory of Virtual Machines

There are two ways to add a directory of offline virtual machines:

- In the **Enter the path to a directory of VMs** box, type the full path name of the directory. When possible, avoid using network drive letters. The recommended practice is to specify the Uniform Naming Convention (UNC) path. For example: *\\virtual\directory*.

  - OR -

- Click the Browse button (...) and locate the directory by browsing your local machine and your network for the desired directory.

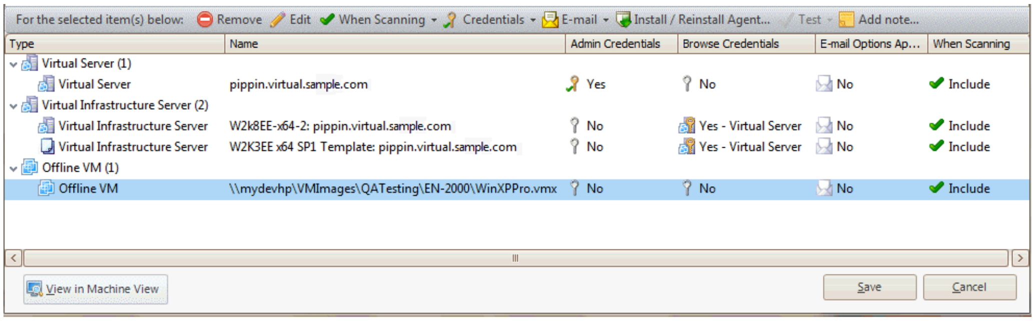
If you want the program to recursively search all subdirectories for virtual machines when performing a scan, enable the **Include all VMs in all subdirectories** check box.

Once the directory is defined, click **Add directory** to add it to the machine group list.

Note: Adding a large number of virtual machines that are all hosted on the same workstation could cause a connection limit error to occur when scanning the virtual machines. See *Notes About Virtual Machines* on page 7 for more information.

Viewing Servers and Virtual Machines in a Machine Group

When servers, virtual machines, and virtual machine templates are added to a machine group, the new entries are displayed within the bottom section of the machine group pane. For example:



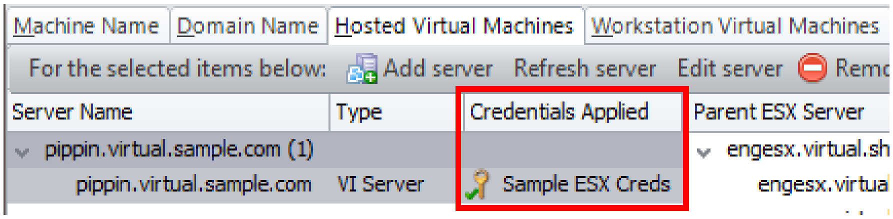
Type	Name	Admin Credentials	Browse Credentials	E-mail Options Ap...	When Scanning
Virtual Server (1)					
Virtual Server	pippin.virtual.sample.com	Yes	No	No	✓ Include
Virtual Infrastructure Server (2)					
Virtual Infrastructure Server	W2k8EE-x64-2: pippin.virtual.sample.com	No	Yes - Virtual Server	No	✓ Include
Virtual Infrastructure Server	W2K3EE x64 SP1 Template: pippin.virtual.sample.com	No	Yes - Virtual Server	No	✓ Include
Offline VM (1)					
Offline VM	\\mydevhp\VMImages\QATesting\EN-2000\WinXPPro.vmx	No	No	No	✓ Include

The recommended best practice is to always supply credentials for the VMware servers, the virtual machine templates, and the workstation virtual machines. See *Supplying Credentials for Virtual Machines* for details. Be careful if you have multiple console administrators, as different administrators are likely to provide different server credentials.

Supplying Credentials for Virtual Machines

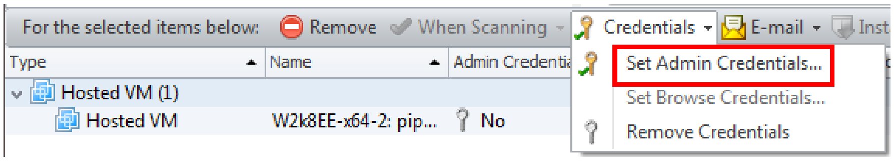
There are several different tabs that can be used to add virtual machines to a machine group. The credentials that will be used to scan and/or deploy patches to these machines depends on how the machines are defined to the group and on the current power state of each machine.

- **Hosted Virtual Machines** tab: Used to add virtual machines that are hosted by a server. The credentials used to scan each machine depends on the current power state of the machine.
  - A hosted virtual machine that is ***offline*** at the time of a scan will be accessed using the server's browse credentials. Any individual credentials supplied for the machine are ignored.



Server Name	Type	Credentials Applied	Parent ESX Server
pippin.virtual.sample.com (1)			engesx.virtual.sh
pippin.virtual.sample.com	VI Server	Sample ESX Creds	engesx.virtua

  - A hosted virtual machine that is ***online*** at the time of a scan will be accessed using authorized credentials for that machine. See *Credential Priorities* (below) for details.



Type	Name	Admin Credentia
Hosted VM (1)		
Hosted VM	W2k8EE-x64-2: pip...	No

- **Workstation Virtual Machines** tab: Used to add **offline** virtual machines that reside on individual workstations. You should assign individual machine credentials for each virtual machine defined using this tab. If appropriate, credentials can also be assigned at the machine group level. The credentials are used during the mounting process and provide permission for Shavlik Protect to access the virtual machine files on the workstation.
- **Machine Name** tab, the **Domain Name** tab, or the **IP Address/Range** tab: Used to add virtual machines that reside on individual workstations and that are **online** at the time of a scan. See *Credential Priorities* for details.

  You typically use these three tabs if you want to be absolutely sure that all your workstation-based virtual machines are successfully scanned. Adding the same machines here and on the **Workstation Virtual Machines** tab assures that each virtual machine will be successfully scanned regardless of its power state (online or offline).

Credential Precedence

Initiating Actions from the Home Page, a Machine Group, or a Favorite

The home page, machine groups, and favorites can be used to initiate patch scans and assets scans (on online/offline virtual machines) and power management actions (on online virtual machines). When performing these actions, Shavlik Protect will attempt to authenticate to each virtual machine using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:

   a. Machine-level credentials (described above in *Supplying Credentials for Virtual Machines*)

   b. Group-level credentials (via the **Credentials** button in the top pane of the machine group)

   c. Default credentials

   Example: If machine-level credentials are not available but group-level and default credentials are available, the program will use the group-level credentials.

2. If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

If none of these credentials work the scans and the power management tasks will fail.

One suggestion is to make your default credentials the same as the account credentials you typically use to log on to the program. This will eliminate problems that may occur if you forget to assign credentials.

Initiating Actions From Machine View or Scan View

When initiating a scan, a patch deployment, or a power management action from Machine View or Scan View, the program will attempt to authenticate to the target machines using a variety of credentials and will do so using the following strategy:

1. If one or more of the following are available, try to authenticate using the credential with the highest precedence, where the precedence order is as follows:

   a. Any manually or automatically assigned managed machine credentials

   b. Default credentials (used if the scan credentials are invalid or missing)

2. If the credential used above does not work, then Integrated Windows Authentication (the credentials of the person currently logged on to the program) will be used.

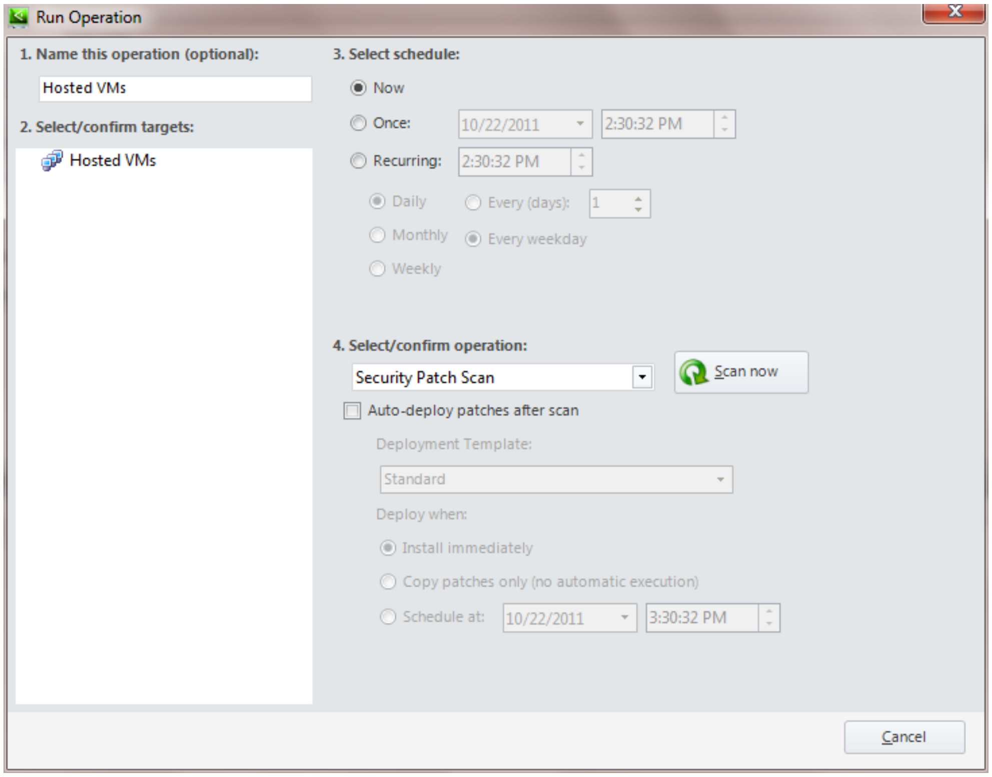
   Note: Integrated credentials will not work for deployments to offline virtual machines or for rescans.

If neither of these credentials work then the action will fail.

How to Scan Virtual Machines

After defining your virtual machines in a machine group, you initiate a scan in the exact same manner as any other machine group.

1. In the **Machine Groups** list within the navigation pane, select the machine group that contains your virtual machines.
2. Verify the desired virtual machines are contained within the group.
3. Within the machine group dialog, click **Run operation**.
4. On the **Run Operation** dialog specify when you want the scan to run and which scan template you want to use.



1. Name this operation (optional): Hosted VMs

2. Select/confirm targets: Hosted VMs

3. Select schedule:
- ● Now
- ○ Once: 10/22/2011 2:30:32 PM
- ○ Recurring: 2:30:32 PM
  - ● Daily ○ Every (days): 1
  - ○ Monthly ● Every weekday
  - ○ Weekly

4. Select/confirm operation: Security Patch Scan
- □ Auto-deploy patches after scan
- Deployment Template: Standard
- Deploy when:
  - ● Install immediately
  - ○ Copy patches only (no automatic execution)
  - ○ Schedule at: 10/22/2011 3:30:32 PM

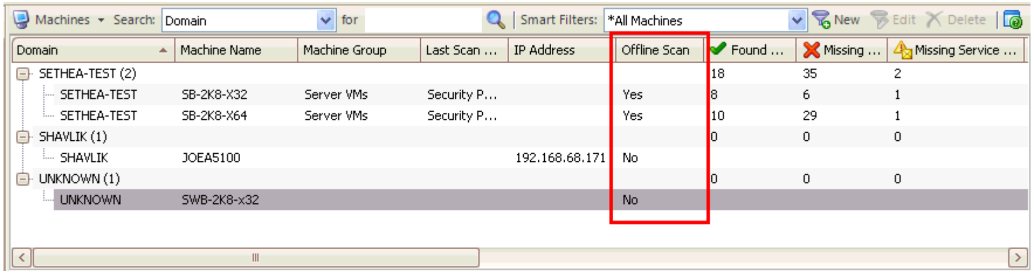
5. Click either **Scan now** or **Schedule**.

Shavlik Protect will perform a full assessment of each virtual machine. In the scan results, special icons will distinguish offline virtual machines ( ) and virtual machine templates ( ) from physical machines and online virtual machines ( ).

REVIEWING SCAN RESULTS

Reviewing Patch Scan Results

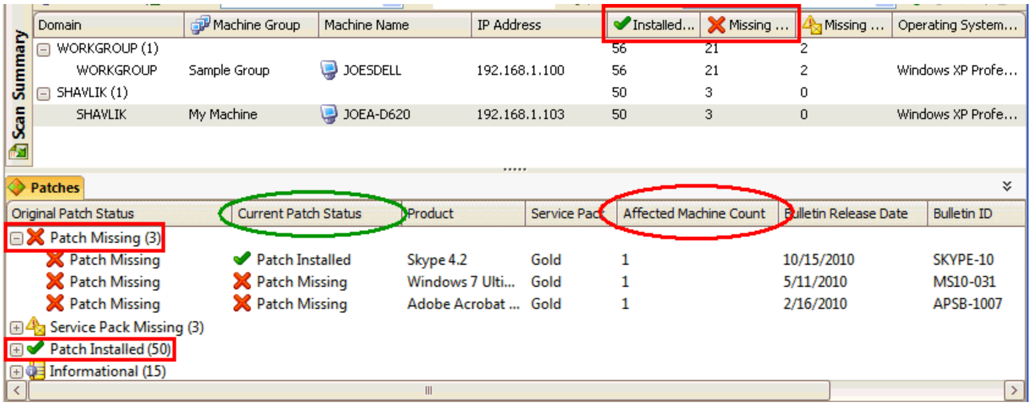
You can review patch scan results using either Scan View or Machine View. When reviewing your patch scan results, special icons will distinguish an offline virtual machine ( ) and a virtual machine template ( ) from a physical machine or an online virtual machine ( ). In addition, the **Offline Scan** column in the top pane will indicate if a virtual machine was online or offline at the time of the scan. For example:



Domain	Machine Name	Machine Group	Last Scan ...	IP Address	Offline Scan	Found ...	Missing ...	Missing Service ...
SETHEA-TEST (2)						18	35	2
SETHEA-TEST	SB-2K8-X32	Server VMs	Security P...		Yes	8	6	1
SETHEA-TEST	SB-2K8-X64	Server VMs	Security P...		Yes	10	29	1
SHAVLIK (1)						0	0	0
SHAVLIK	JOEA5100			192.168.68.171	No			
UNKNOWN (1)						0	0	0
UNKNOWN	SWB-2K8-x32				No			

Shavlik Protect will otherwise treat an offline virtual machine or virtual machine template no differently than a physical machine. If an offline machine is brought online and is rescanned, the offline virtual machine icon will be replaced by a regular machine icon.

The **Patches** tab in the middle pane displays general information about the machines selected in the top pane.

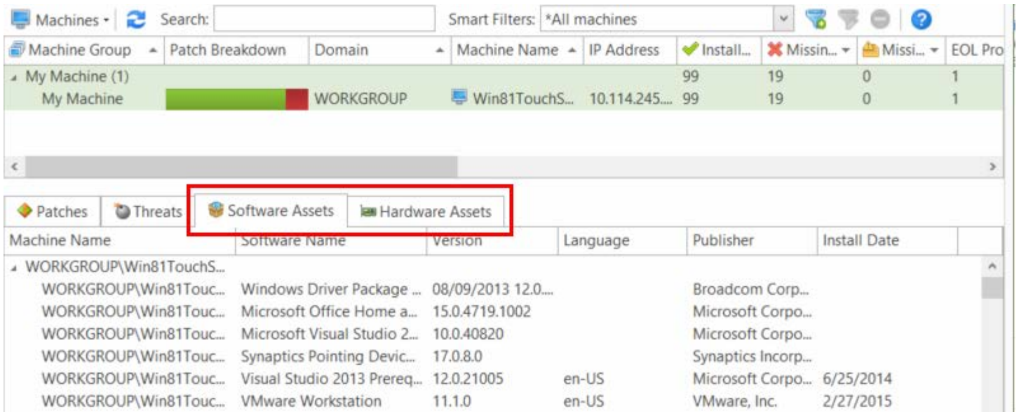


Domain	Machine Group	Machine Name	IP Address	Installed...	Missing ...	Missing ...	Operating System...
WORKGROUP (1)				56	21	2	
WORKGROUP	Sample Group	JOESDELL	192.168.1.100	56	21	2	Windows XP Profe...
SHAVLIK (1)				50	3	0	
SHAVLIK	My Machine	JOEA-D620	192.168.1.103	50	3	0	Windows XP Profe...

Original Patch Status	Current Patch Status	Product	Service Pack	Affected Machine Count	Bulletin Release Date	Bulletin ID
Patch Missing (3)						
Patch Missing	Patch Installed	Skype 4.2	Gold	1	10/15/2010	SKYPE-10
Patch Missing	Patch Missing	Windows 7 Ulti...	Gold	1	5/11/2010	MS10-031
Patch Missing	Patch Missing	Adobe Acrobat ...	Gold	1	2/16/2010	APSB-1007
Service Pack Missing (3)						
Patch Installed (50)						
Informational (15)						

Reviewing Asset Scan Results

Asset scan results are viewed within Machine View. The middle pane contains two tabs that are associated with an asset scan.



Machine Group	Patch Breakdown	Domain	Machine Name	IP Address	Install...	Missin...	Missi...	EOL Pro
My Machine (1)					99	19	0	1
My Machine		WORKGROUP	Win81TouchS...	10.114.245....	99	19	0	1

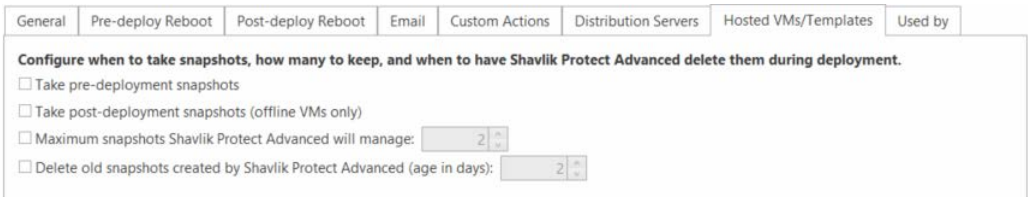
Machine Name	Software Name	Version	Language	Publisher	Install Date
WORKGROUP\Win81TouchS...					
WORKGROUP\Win81Touc...	Windows Driver Package ...	08/09/2013 12.0....		Broadcom Corp...	
WORKGROUP\Win81Touc...	Microsoft Office Home a...	15.0.4719.1002		Microsoft Corpo...	
WORKGROUP\Win81Touc...	Microsoft Visual Studio 2...	10.0.40820		Microsoft Corpo...	
WORKGROUP\Win81Touc...	Synaptics Pointing Devic...	17.0.8.0		Synaptics Incorp...	
WORKGROUP\Win81Touc...	Visual Studio 2013 Prereq...	12.0.21005	en-US	Microsoft Corpo...	6/25/2014
WORKGROUP\Win81Touc...	VMware Workstation	11.1.0	en-US	VMware, Inc.	2/27/2015

- **Software Assets**: Displays information about the software contained on physical machines, online virtual machines, offline virtual machines, and virtual machine templates.
- **Hardware Assets**: Displays information about the hardware components contained on physical machines and online virtual machines. Offline virtual machines and virtual machine templates are ignored by this scan.

CONFIGURING YOUR DEPLOYMENT TEMPLATE TO TAKE SNAPSHOTS

What is a virtual machine snapshot? A snapshot captures the state, configuration, and disk data of a virtual machine at a given time. Snapshots are useful for storing states that an administrator or user might want to return to at some point in the future.

If you want to take snapshots of your hosted virtual machines and virtual machine templates immediately before and/or immediately after the patch deployment process, make sure you specify this on the **Hosted VMs/Templates** tab of the deployment template you plan to use. This tab does not apply to virtual machines that reside on workstations.



Configure when to take snapshots, how many to keep, and when to have Shavlik Protect Advanced delete them during deployment.

□ Take pre-deployment snapshots

□ Take post-deployment snapshots (offline VMs only)

□ Maximum snapshots Shavlik Protect Advanced will manage: 2

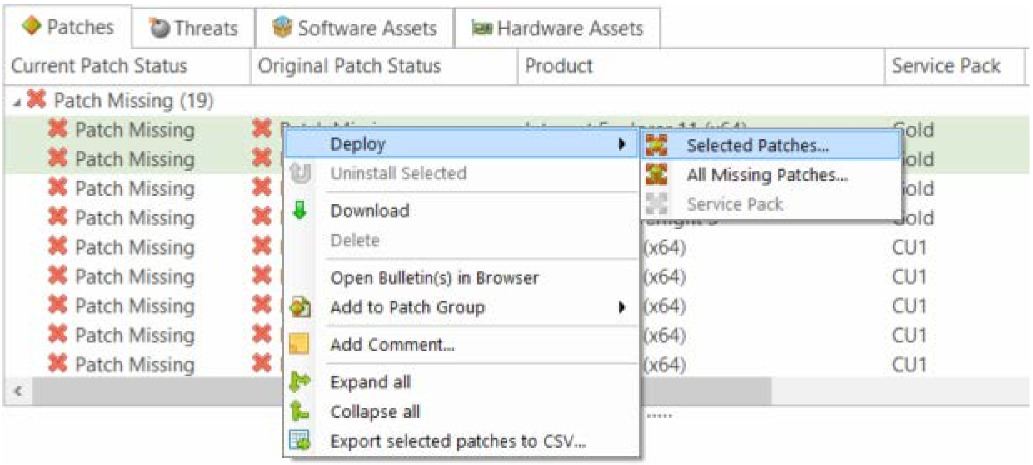
□ Delete old snapshots created by Shavlik Protect Advanced (age in days): 2

Complete snapshots are taken of offline virtual machines and of virtual machine templates. If a virtual machine is online at the time of the patch deployment the memory state will not be included in the snapshot—this will quicken the process and reduce the amount of time that the online virtual machine is affected.

There are reasons why you may choose to NOT take a snapshot. You may have a limited amount of disk space, or you may have performance concerns. Taking a snapshot reduces the performance of the virtual machine while the snapshot is created.

DEPLOYING PATCHES TO VIRTUAL MACHINES

The method for initiating a patch deployment is the same regardless of whether you are deploying to a physical machine, to an online virtual machine, to an offline virtual machine, or to a virtual machine template. You simply right-click the desired machines or patches and select **Deploy**.



It's what happens after you initiate the deployment, however, that is slightly different for virtual machines and virtual machine templates.

Note: For deployments to virtual machines that are hosted on a server it is recommended you use the **Virtual Machine Standard** deployment template. Also, in all cases, during deployment the virtual network will need to remain connected.

Immediate Patch Deployments

When you perform an immediate deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled to occur immediately using the scheduler on the target machine. The online/offline status of these machine types is determined at the time you initiate the deployment. The actual patch installation is performed on the target machines and the console is not actively involved in the patch installation.

When you perform an immediate deployment to a virtual machine that is hosted on a server, the entire deployment process occurs on the Shavlik Protect console machine. The console determines the online/offline status of the hosted virtual machines and the console service is actively involved during the patch installation. This allows the console service to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you perform an immediate deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab	Target Machine is Online	Target Machine is Offline
Machine Name, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Push files and initiate deployment immediately.	Fail
Workstation Virtual Machines	Fail	Push files and schedule on target; deployment will occur the next time the virtual machine is brought online.
Hosted Virtual Machines	Push files and initiate deployment immediately. The process is the same as a physical machines except that snapshots will be taken as directed by the deployment template.	*See steps below. VMware tools must be installed on the virtual machine in order for the deployment to be successful.

*During deployment to an offline hosted virtual machine or an offline virtual machine template, the following steps occur:

1. ***[Conditional: Templates Only]*** Convert the virtual machine template to an offline virtual machine.
2. ***(Optional)*** Take a snapshot if the deployment template is configured to take a pre-deployment snapshot.

3. *(Optional)* Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
4. Copy the patches to the offline virtual machine.
5. Reconfigure the following on the offline virtual machine:
    - Disable the network adaptor's **Connect at power on** option. This is done so that the machine is isolated from the network when the patch process is run.
    - Disable Sysprep so it will not automatically configure the machine's operating system when the machine is first powered on.
6. Power on the virtual machine.
7. Install the patches.
8. Power down the virtual machine.
9. Reset the machine configuration to its original network connection and Sysprep settings.
10. *(Optional)* Take a snapshot if the deployment template is configured to take a post-deployment snapshot.
11. *(Optional)* Delete old snapshots if one of the snapshot thresholds defined on the patch deployment template is exceeded.
12. *[Conditional: Templates Only]* Convert the offline virtual machine back to a virtual machine template.

Scheduled Patch Deployments

When you schedule a deployment to a physical machine, an online workstation virtual machine, or an offline workstation virtual machine, the files required for the deployment are copied to the target machine immediately and the deployment is scheduled using the scheduler on the target machine. The patch installation is performed on the target machines and the console is not actively involved. At the time of the actual deployment, if the machine is in a different power state from when it was last scanned, the deployment will fail.

When you schedule a deployment to a virtual machine that is hosted on a server, the entire deployment process is scheduled to occur on the Shavlik Protect console machine using the scheduler on the console. The online/offline status of the hosted virtual machines is determined at the scheduled time, and the console is actively involved at the time the patches are installed. This allows the console to modify the state of the hosted virtual machines during the deployment.

The following table summarizes what happens at the time you schedule a deployment based on where the virtual machines are defined within the machine group.

Machine Group Tab	Target Machine is Online When Scheduled	Target Machine is Offline When Scheduled
Machine Name, **Domain Name**, **IP Address/Range**, **Organizational Unit**	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both of the following are true: • The machine is online • The scheduled time has passed	Fail
Workstation Virtual Machines	Fail	Push files to the target and schedule the deployment on the target. The deployment will occur the next time both of the following are true: • The machine is online • The scheduled time has passed
Hosted Virtual Machines	Schedule the deployment on the console. At the scheduled time, treat as an immediate deployment (see *Hosted Virtual Machines* in the previous table).	

If the scheduled deployment contains a mix of hosted virtual machines and other types of machines, the machines are separated into two groups. The deployment of the hosted virtual machines is scheduled to occur on the console at the scheduled time. For all machines other than hosted virtual machines, the files are copied to the target machines immediately and the deployment is scheduled to occur using the scheduler on the target machine.

Power State and Credential Requirements for a Successful Deployment

Note: Keep in mind that, from Shavlik Protect's point of view, the definition of a successful deployment depends on where the virtual machine is located. A successful deployment to a hosted virtual machine means the machine is fully patched, while a successful deployment to a workstation-based virtual machine means the patches have been pushed to the offline virtual machine.

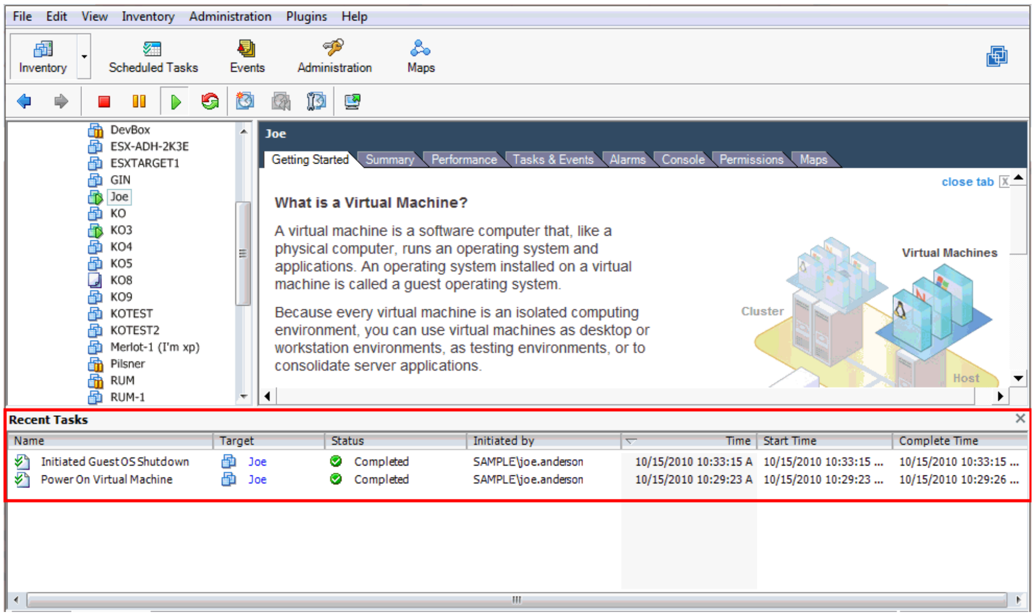
When performing the deployment, the program will attempt to authenticate to the target machine using the credentials defined in the **Manage Machines Properties** dialog. If the credential is invalid the deployment will fail. For workstation-based virtual machines, if the power state of the machine has changed since the scan, the deployment will fail.

MONITORING PATCH DEPLOYMENTS TO VIRTUAL MACHINES

Shavlik Protect provides a number of ways to monitor patch deployments:

- Scheduled patch deployments can be managed using the **Scheduled Task Manager**.
- Active patch deployments can be monitored using the **Deployment Tracker**. If you notice that a server task has failed for a virtual machine (for example, taking a snapshot or re-enabling the network), you can complete the task using your client software.
- When the deployment has completed, you can review the status of the deployment by selecting the deployment in the **Results** list of the navigation pane.

In addition to using the tracking tools provided by Shavlik Protect, for virtual machines that are hosted on a server you can also use your client software to monitor the patch deployment progress. For example:



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

Recent Tasks

Name	Target	Status	Initiated by	Time	Start Time	Complete Time
Initiated Guest OS Shutdown	Joe	Completed	SAMPLE\joe.anderson	10/15/2010 10:33:15 A	10/15/2010 10:33:15 ...	10/15/2010 10:33:15 ...
Power On Virtual Machine	Joe	Completed	SAMPLE\joe.anderson	10/15/2010 10:29:23 A	10/15/2010 10:29:23 ...	10/15/2010 10:29:26 ...