Ivanti Patch for Windows® Servers

Upgrade Guide

Copyright and Trademarks

Document Information and Print History

Document number: N/A

Date	Version	Description
September 2010	NetChk Protect 7.6	Update product branding, add information about new 7.6 features and improvements.
March 2011	NetChk Protect 7.8	Add information about new 7.8 features and improvements.
October 2011	VMware vCenter Protect 8.0	Update product branding, add info about 8.0 upgrade tasks. Remove all info about versions prior to 7.5.
December 2011	Vmware vCenter Protect 8.0, Document Rev A	Add step explaining how to compress the database before beginning the upgrade process.
September 2012	Vmware vCenter Protect 8.0.1	Update product name and version, update cover graphics.
May 2013	Shavlik Protect 9.0	Update the system requirements. Add information about the new v9.0 features and improvements.
April 2014	Shavlik Protect 9.1	Update the system requirements. Add information about the new v9.1 features and improvements.
September 2015	Shavlik Protect 9.2	Update the system requirements. Add information about the new v9.2 features and improvements.
April 2017	Ivanti Patch for Windows® Servers 9.3	Rebrand to Ivanti, remove references to AV, update system requirements, add information about the new v9.3 features and improvements.

WELCOME

Purpose of this Guide

Welcome to Ivanti Patch for Windows® Servers 9.3. This document describes how to upgrade from Shavlik Protect 9.1 or Shavlik Protect 9.2 to Ivanti Patch for Windows® Servers 9.3.

In addition to describing the upgrade procedure, this document lists a number of functional differences you should be aware of when upgrading to Ivanti Patch for Windows® Servers 9.3. It also highlights the areas in the user interface that have changed significantly.

New System Requirements and Prerequisites

Please note the following new requirements and prerequisites for Ivanti Patch for Windows® Servers 9.3.

- Windows Server 2016 and Windows 10 are now supported as a console machine
- Microsoft .NET Framework 4.6.2 or later
- Microsoft Visual C++ Redistributable for Visual Studio 2015
- Removed support for SQL Server 2005. The new minimum is SQL Server 2008.
- Windows XP and Windows Server 2003 are no longer supported on agent machines
- Antivirus is no longer supported in this release

All missing software prerequisites will be automatically installed during the upgrade process. See the *Ivanti Patch for Windows® Servers Installation Guide* for the complete list of system requirements.

Note: The URL used to download new patch content has changed. The new location is http://content.ivanti.com. Be sure that your console can reach this URL.

User Account Requirements for Performing an Upgrade

In order to perform an upgrade your user account must meet the following requirements:

- The user performing the database upgrade must be a member of the db_owner role.
- If you have multiple consoles that share a database and are linking an additional console to a database that is already upgraded, the user account you use must be a member of the following database roles: db_datareader, db_datawriter, STExec, and STCatalogupdate. In addition, the service account used for background operations must be a member the db_owner role. If your account is a member of the db_securityadmin and db_accessAdmin roles, the database upgrade tool will automatically attempt to map and configure the required roles for you.

UPGRADE PROCEDURE

Overview

This section describes how to upgrade from Shavlik Protect 9.1 or Shavlik Protect 9.2 to Ivanti Patch for Windows® Servers 9.3. If you are taking this opportunity to move the console to a new machine and you want to perform the migration using the Migration Tool, see the *Migration Tool User's Guide* before performing the upgrade.

Before performing the upgrade, be sure to read the *Significant Changes and Enhancements* section on page 20 so you are aware of how the upgrade will affect your system. You also may want to make a note of all your current custom user settings as some are not preserved during the upgrade (see page 17).

Note: Be aware that after the upgrade of the console is complete, any agents that are installed on your target machines will be automatically upgraded the next time they check in with the console.

Performing the Upgrade

1. Free up unused space in the database that is used to store scan results and patch deployment results.

   You can do this in SQL Server Management Studio by right-clicking the ShavlikScans database and selecting **Tasks > Shrink > Database**.

2. Create a backup of your current database using SQL Server Management Studio.

   The database contains results from program operations and it also contains configuration information. Backing up your database is an important step.

3. Close all programs running on the console machine, including Shavlik Protect.
4. Download the Ivanti Patch for Windows® Servers 9.3 executable file to your console machine using the following link:

   https://www.ivanti.com/en-US/resources/downloads

5. Begin the installation process using one of the following methods:

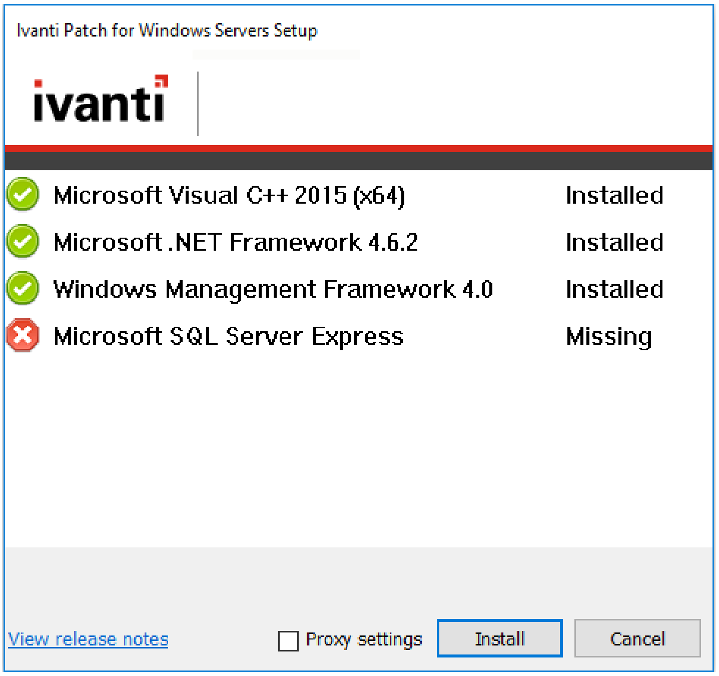
   - Double-click the file named **IvantiPatchForServers.exe**.
   - Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The DBCOMMANDTIMEOUT option is used to specify the SQL command timeout value during installation. The default value is 15 minutes per GB. The minimum timeout value is the greater of 15 minutes per GB or 1800 seconds (30 minutes). You should override the default value only if you expect the upgrade to take an exceptionally long time due to constrained resources. For example, if you have a 4 GB database, to double the default timeout value from 3600 seconds (60 minutes) to 7200 seconds (120 minutes) you would type the following command:

     ```
     IvantiPatchForServers /wi:"DBCOMMANDTIMEOUT =7200"
     ```

   Note: If you receive a prompt indicating that a restart is required, click **OK** and the installation process will automatically resume after the restart.

6. Respond to the dialog that asks if you want to continue with the upgrade.

   If you click **Yes** and your console machine is missing one or more prerequisites, a dialog similar to the following is displayed. If you are not missing any prerequisites, skip the following step and proceed with the **Welcome** dialog.



Ivanti Patch for Windows Servers Setup

✓	Microsoft Visual C++ 2015 (x64)	Installed
✓	Microsoft .NET Framework 4.6.2	Installed
✓	Windows Management Framework 4.0	Installed
✗	Microsoft SQL Server Express	Missing

7. Click **Install** to install any missing prerequisites.

   The Setup Wizard may need to perform a reboot during this portion of the installation process. If a reboot is required, when the machine is restarted the Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

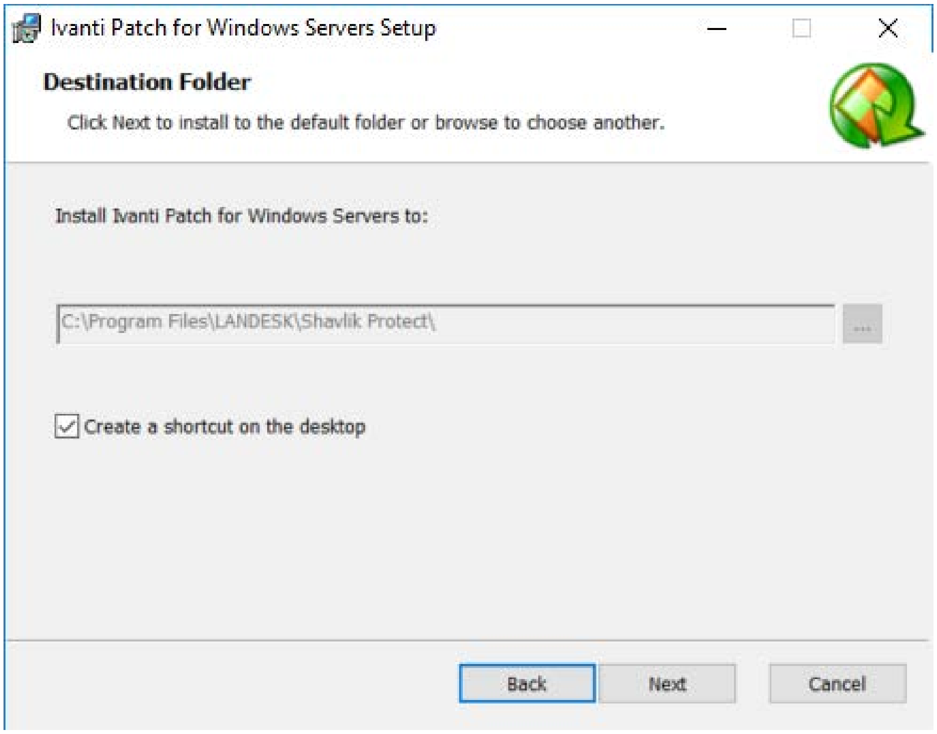
   The **Welcome** dialog is displayed.

8. Read the information on the **Welcome** dialog and then click **Next**.

   The license agreement is displayed. You must accept the terms of the license agreement in order to install the program.

9. Enable the **I accept the terms in the License Agreement** check box and then click **Next**.

   The **Destination Folder** dialog is displayed.



Ivanti Patch for Windows Servers Setup

Destination Folder

Click Next to install to the default folder or browse to choose another.

Install Ivanti Patch for Windows Servers to:

C:\Program Files\LANDESK\Shavlik Protect\

☑ Create a shortcut on the desktop

10. If you want to change the default location of the program, click the browse button and choose a new location. You also have the option here to install a shortcut icon on your desktop. When you are done, click **Next**.

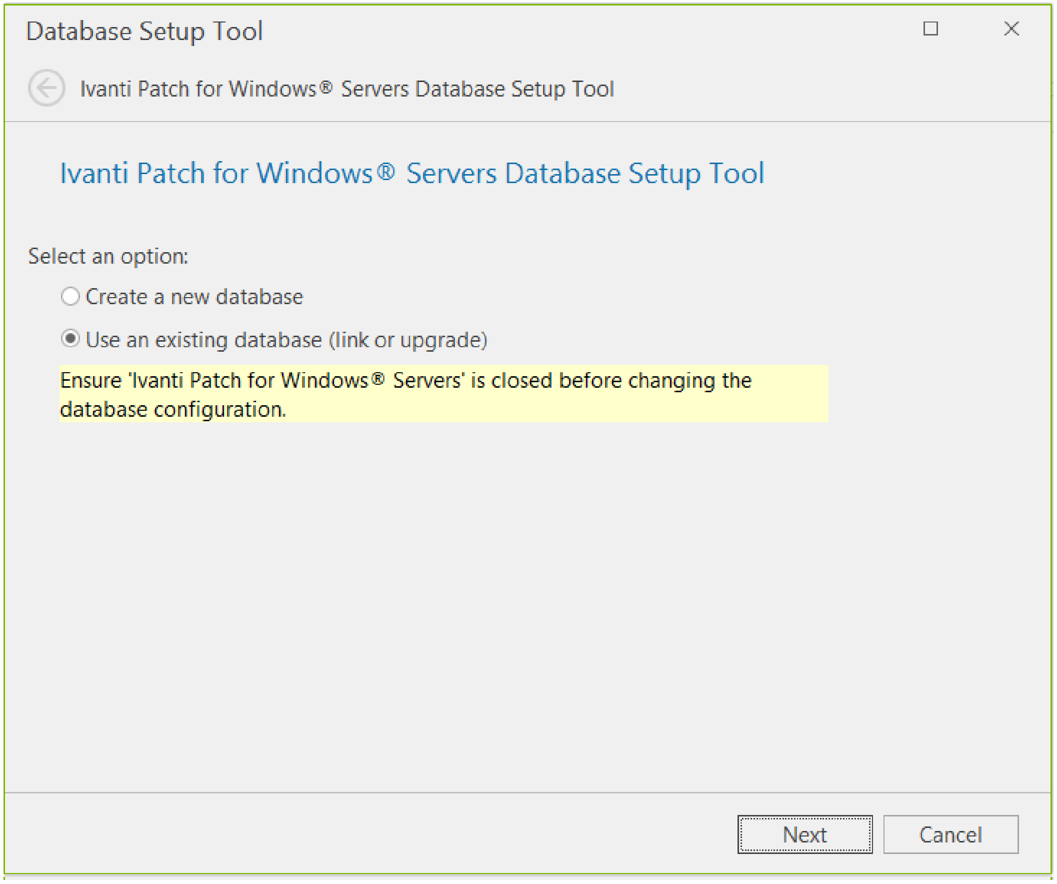
    The **Product Improvement Program** dialog is displayed. Read the description and decide if you agree to participate in the program. The program enables Ivanti to collect product usage information that will help improve future versions of the product.

11. Click **Next**.

    The **Ready to Install** dialog is displayed.

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

    Near the end of the installation process the **Database Setup Tool** dialog is displayed.


Database Setup Tool
Ivanti Patch for Windows® Servers Database Setup Tool
Ivanti Patch for Windows® Servers Database Setup Tool
Next
Cancel

Select an option:

○ Create a new database

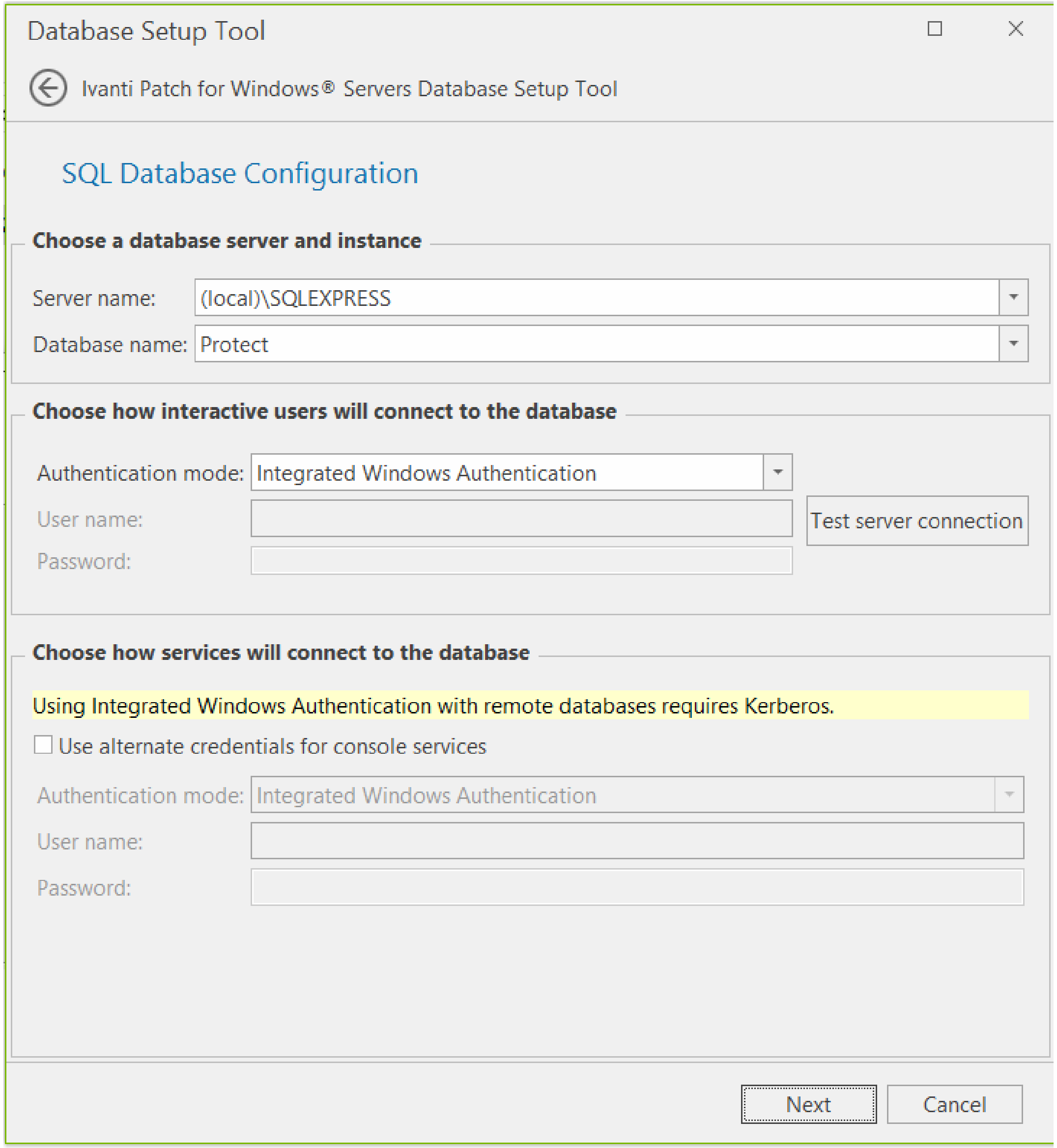
● Use an existing database (link or upgrade)

Ensure 'Ivanti Patch for Windows® Servers' is closed before changing the database configuration.

Important! In the next step DO NOT select **Create a new database**. If you do a new database will be created and your existing data will not be used.

13. Make sure **Use an existing database** is selected and then click **Next**.

    A dialog similar to the following is displayed:



Database Setup Tool

Ivanti Patch for Windows® Servers Database Setup Tool

SQL Database Configuration

Choose a database server and instance

Server name: (local)\SQLEXPRESS

Database name: Protect

Choose how interactive users will connect to the database

Authentication mode: Integrated Windows Authentication

User name:

Password:

Choose how services will connect to the database

Using Integrated Windows Authentication with remote databases requires Kerberos.

□ Use alternate credentials for console services

Authentication mode: Integrated Windows Authentication

User name:

Password:

14. Use the boxes provided to define how users and services will access the SQL Server database.

Choose a database server and instance

- **Server name:** You can specify a machine or you can specify a machine and the SQL Server instance running on that machine.
- **Database name:** Specify the database name you want to use. The default database name is **Protect**.

Choose how interactive users will connect to the database

Specify the credentials you want the program to use when a user performs an action that requires access to the database.

- **Integrated Windows Authentication:** This is the recommended and default option. Ivanti Patch for Windows® Servers will use the credentials of the currently logged on user to connect to the SQL Server database. The **User name** and **Password** boxes will be unavailable.
- **Specific Windows User:** Select this option only if the SQL Server database is on a remote machine. This option will have no effect if the database is on the local (console) machine. (See *Supplying Credentials* in the *Ivanti Patch for Windows® Servers Administration Guide* for more information about local machine credentials.) All Ivanti Patch for Windows® Servers users will use the supplied credentials when performing actions that require interaction with the remote SQL Server database.
- **SQL Authentication:** Select this option to enter a specific user name and password combination when logging on to the specified SQL Server.

  Caution! If you supply SQL authentication credentials and have not implemented SSL encryption for SQL connections, the credentials will be passed over the network in clear text.

- **Test database connection:** To verify that the program can use the supplied interactive user credentials to connect to the database, click this button.

Choose how services will connect to the database

Specify the credentials you want the background services to use when making the connection to the database. These are the credentials that the results importer, various agent operations, and other services will use to log on to SQL Server and provide status.

- **Use alternate credentials for console services:**
  - If the SQL Server database is installed on the local machine you will typically ignore this option by not enabling this check box. In this case the same credentials and mode of authentication that you specified above for interactive users will be used.
  - You will typically only enable this check box if the SQL Server database is on a remote machine. When the database is on a remote machine you need an account that can authenticate to the database on the remote database server.
- **Authentication method:** Available only if **Use alternate credentials for console services** is enabled.
  - **Integrated Windows Authentication:** Selecting this option means that the machine account will be used to connect to the remote SQL Server. The Kerberos network authentication protocol must be available in order to securely transmit the credentials. The User name and Password boxes will be unavailable.

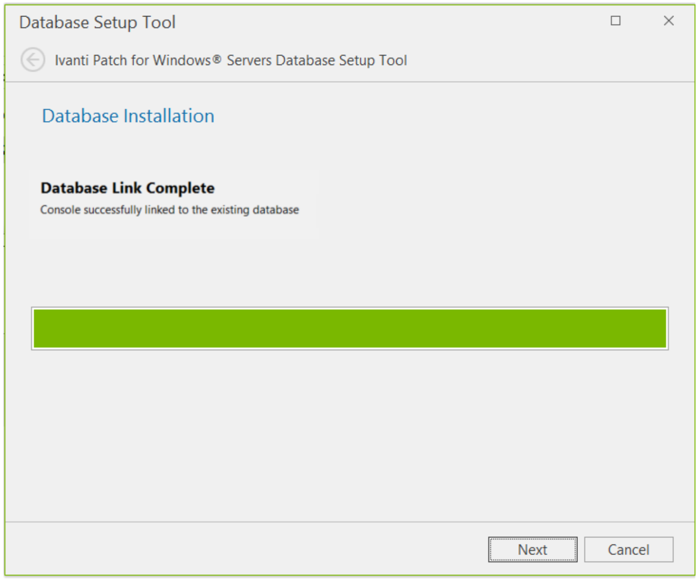
Note: If you choose **Integrated Windows Authentication** the installation program will attempt to create a SQL Server login for the machine account. If the account creation process fails, see *SQL Server Post-Installation Notes* in the *Ivanti Patch for Windows® Servers Installation Guide* for instructions on manually configuring a remote SQL Server to accept machine account credentials. Do this after you complete the Ivanti Patch for Windows® Servers upgrade process but before you start the program.

   - **Specific Windows User:** Select this option to enter a specific user name and password combination. Ivanti Patch for Windows® Servers' background services will use these credentials to connect to the SQL Server database. This is a good fallback option if for some reason you have difficulties implementing integrated Windows authentication.
   - **SQL Authentication:** Select this option to provide a specific user name and password combination for the services to use when logging on to SQL Server.

15. After providing all the required information, click **Next**.

    Note: If the installation program detects a problem with any of the specified credentials, an error message will be displayed. This typically indicates that a user account you specified does not exist. Make a correction and try again.

    The console is linked to your existing database. When the link process is complete the following dialog is displayed:



Database Link Complete

Console successfully linked to the existing database

16. Click **Next**.
17. On the **Installation Complete** dialog click **Finish**.
18. On the **Completed the Ivanti Patch for Windows® Servers Setup Wizard** dialog, enable the **Launch Ivanti Patch for Windows® Servers** check box and then click **Finish**.

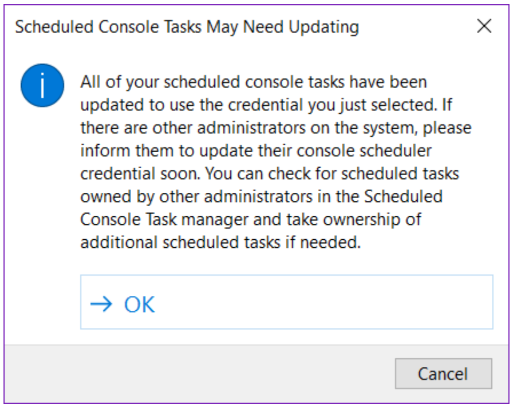
UPGRADE TASKS PERFORMED ON THE CONSOLE

In order to complete the upgrade, the following tasks must be performed on the Ivanti Patch for Windows® Servers console.

Assign Scheduler Credentials

Note: This applies only if you are upgrading from v9.1 to v9.3.

A scheduler credential that matches your current user account is now required to run scheduled console tasks. If there are scheduled tasks on the console and the scheduler credential has not been set, you will receive a prompt at startup time to set the credential. This check occurs every time Ivanti Patch for Windows® Servers is started to ensure that scheduled tasks continue to run.



Scheduled Console Tasks May Need Updating

All of your scheduled console tasks have been updated to use the credential you just selected. If there are other administrators on the system, please inform them to update their console scheduler credential soon. You can check for scheduled tasks owned by other administrators in the Scheduled Console Task manager and take ownership of additional scheduled tasks if needed.

Review Your Scheduled Tasks

Scheduled tasks are monitored and managed from two separate areas. You should review both scheduled tasks managers to verify that your existing tasks were properly ported.

- The **Scheduled Console Tasks Manager** provides one location to view tasks currently scheduled on the console such as patch scans, asset scans, patch deployments to the console machine, script execution and scheduled reports.
- The **Scheduled Remote Tasks Manager** provides one location from which to view power tasks and patch deployments tasks currently scheduled on your remote target machines.

Refresh Your License (Offline Consoles Only)

If your console is offline (if it does not have an Internet connection), in order to view and use the new features in Ivanti Patch for Windows® Servers 9.3 you must manually refresh your license. For information on activating a disconnected console, in the online Help system see **Quick Start > Setup > Your First Look at the Program > Activating the Program**.

If the console is online the license will be automatically refreshed during the upgrade process.

Review Your Patch Scan Templates and Patch Groups

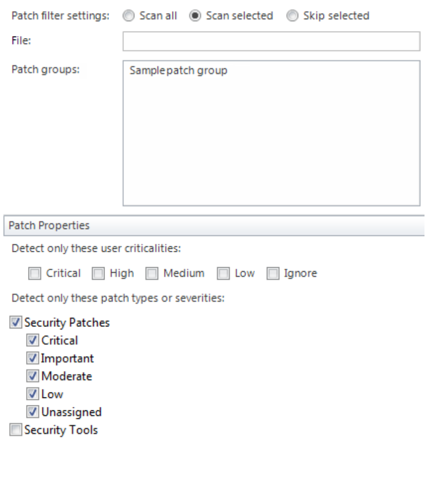
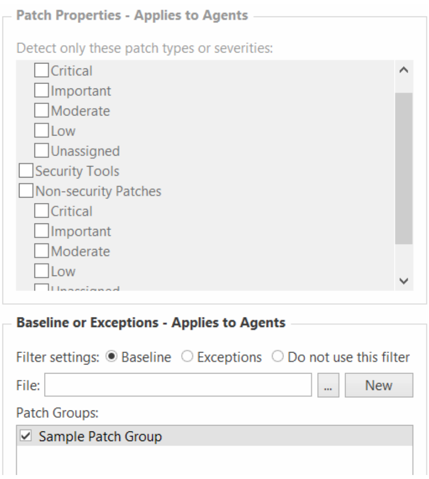
There are three issues to consider in these areas, particularly for those customers who are upgrading from v9.1 to v9.3.

- **Patch Scan Templates:** The **Filtering** tab on the **Patch Scan Template** dialog has been updated to allow for more precision when scanning. While the upgrade process will automatically convert your existing patch scan templates to the new style, you should double-check your templates to verify the changes.
- **Patch Groups:** Patch groups are no longer defined using a separate dialog; rather, they are now created and managed from within Patch View. While the upgrade process will automatically convert your existing patch groups to the new convention, you should double-check your groups to verify the changes. Your patch groups may be smaller after the upgrade as Ivanti has deprecated support for many old patches.
- **Modified and Auto-Generated Patch Groups:** In order to preserve the behavior of your patch scan templates, one or more of your existing patch groups may be modified during the upgrade process and one or more new patch groups may be automatically generated.
  - **Modified Patch Groups:** If you reference a patch group within the **Patch filter settings** section of your 9.1 patch scan template and **Scan selected** is enabled, any patches that do not meet the criteria defined by the scan template filters will be removed from the group. Here's why: In Protect 9.1, the scan template filters can mask the fact that your patch group may contain patch types that you never intended to actually scan for or deploy. In Ivanti Patch for Windows® Servers 9.3, when the patch group is used as a baseline, the scan template filters will not be applied and inaccuracies in your patch groups may be revealed. If the upgrade process detects this situation, it will automatically modify the patch group in order to preserve the intended interaction between the scan template and the patch group.

    Example:

    Assume your 9.1 patch group contains a mix of Security, Non-security and Software Distribution patches. In the scan template that references this patch group, the **Patch filter settings** section is set to **Scan selected** and the **Patch Properties** section is set to detect only Security patches. In this configuration, the **Patch Properties** filter will be honored and only Security patches will be detected (despite the fact that the patch group contains Non-security and Software Distribution patches).

    After upgrading to 9.3, the scan template will define the patch group as a Baseline filter and all other scan template filters will be ignored. If the patch group is not modified, Non-security and Software Distribution patches will now be detected (and deployed, if you enable the **Auto-deploy patches after scan** check box when performing a scan). The upgrade process will recognize this discrepancy and will remove the Non-security and Software Distribution patches from the patch group.

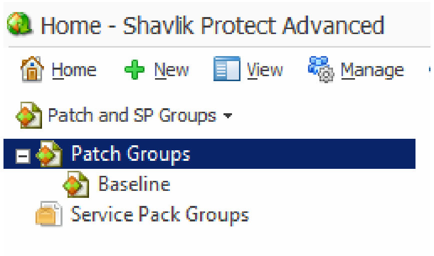
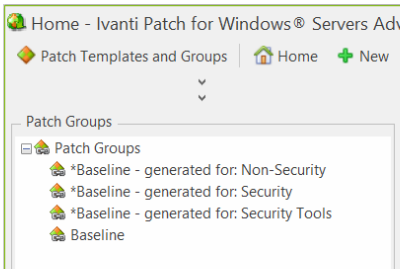
Protect 9.1 Scan Template	**PWS 9.3 Scan Template**
 Patch filter settings: ○ Scan all ● Scan selected ○ Skip selected File: Patch groups: Samplepatch group Patch Properties Detect only these user criticalities: □ Critical □ High □ Medium □ Low □ Ignore Detect only these patch types or severities: ☑ Security Patches ☑ Critical ☑ Important ☑ Moderate ☑ Low ☑ Unassigned □ Security Tools	 Patch Properties - Applies to Agents Detect only these patch types or severities: □ Critical □ Important □ Moderate □ Low □ Unassigned □ Security Tools □ Non-security Patches □ Critical □ Important □ Moderate □ Low Baseline or Exceptions - Applies to Agents Filter settings: ● Baseline ○ Exceptions ○ Do not use this filter File: ... New Patch Groups: ☑ Sample Patch Group

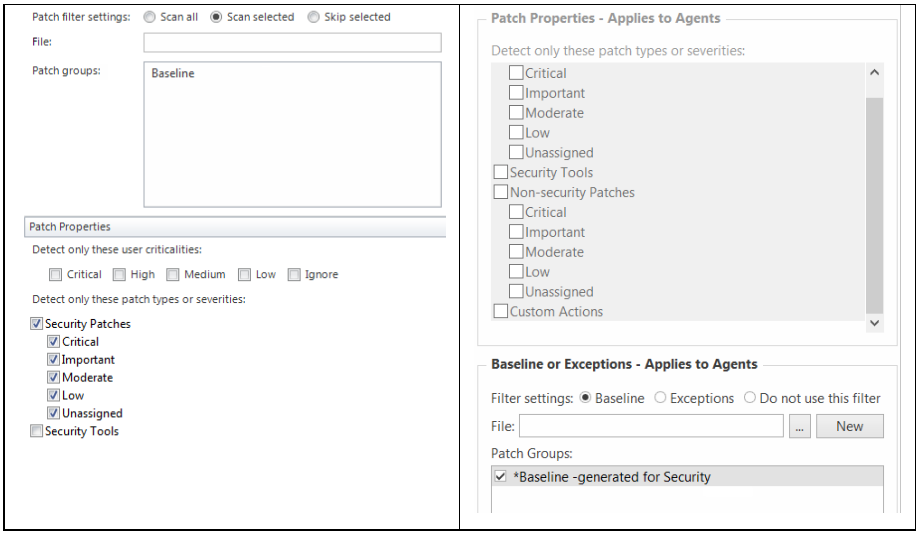
Note: Going forward, be careful to properly manage your patch groups by not adding unnecessary or unwanted patches or patch types.

- **Auto-Generated Patch Groups:** A copy of an existing patch group will be automatically generated by the upgrade process if all of the following conditions are met:
  - If the patch group is referenced within the **Patch filter settings** section of a patch scan template and **Scan selected** is enabled, and
  - If the patch group is referenced by an agent policy or by a second scan template that contains different filter definitions, and
  - If the patch group must be modified by the upgrade process to maintain compatibility (see above)

In this situation, a copy of the patch group will be generated and then modified as described above. The name of the new patch group will be ***<patch group name> -generated for <scan template name>**. The scan template(s) that reference the patch group will be updated to use the new patch group name. The original patch group is preserved so that references to it from your agent policies or other scan templates are maintained.

You should review the changes and, if desired, rename the auto-generated patch group to a more friendly or meaningful name.

Protect 9.1 Patch Group	**PWS 9.3 Patch Groups**
 Home - Shavlik Protect Advanced Home New View Manage Patch and SP Groups Patch Groups Baseline Service Pack Groups	 Home - Ivanti Patch for Windows® Servers Adv Patch Templates and Groups Home New Patch Groups Patch Groups *Baseline - generated for: Non-Security *Baseline - generated for: Security *Baseline - generated for: Security Tools Baseline
Protect 9.1 Scan Template	**PWS 9.3 Scan Template**



Patch filter settings: ○ Scan all ● Scan selected ○ Skip selected

File:

Patch groups: Baseline

Patch Properties

Detect only these user criticalities:

□ Critical □ High □ Medium □ Low □ Ignore

Detect only these patch types or severities:

- ☑ Security Patches
  - ☑ Critical
  - ☑ Important
  - ☑ Moderate
  - ☑ Low
  - ☑ Unassigned
- □ Security Tools

Patch Properties - Applies to Agents

Detect only these patch types or severities:

- □ Critical
- □ Important
- □ Moderate
- □ Low
- □ Unassigned
- □ Security Tools
- □ Non-security Patches
  - □ Critical
  - □ Important
  - □ Moderate
  - □ Low
  - □ Unassigned
- □ Custom Actions

Baseline or Exceptions - Applies to Agents

Filter settings: ● Baseline ○ Exceptions ○ Do not use this filter

File:

Patch Groups:

☑ *Baseline -generated for Security

Assign Aliases to the Console

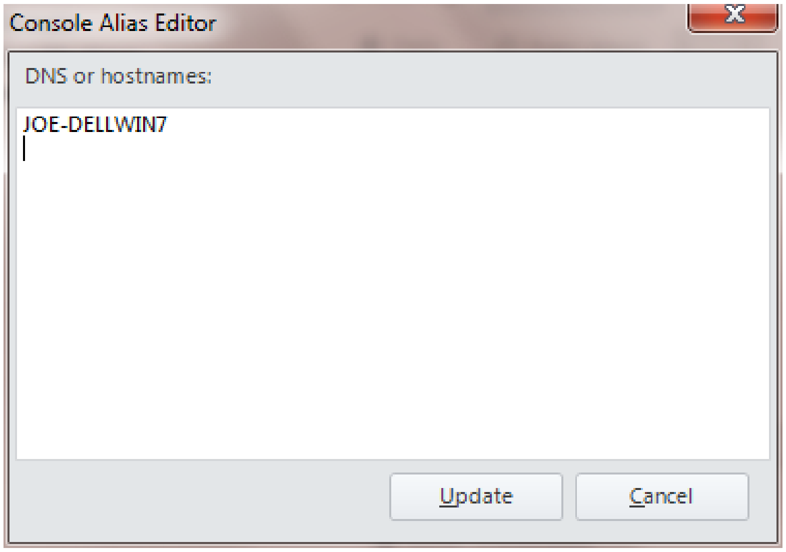
This task is necessary if one or more of the following conditions apply:

- You have assigned the console machine to a new domain
- You have given the console a new common name or IP address
- You manually installed agents and they use an IP address to communicate with the console

Under these conditions you must use the **Console Alias Editor** tool to identify the old console names or addresses as trusted aliases. If you don't, when an agent checks in with the Ivanti Patch for Windows® Servers console or when an agentless machine attempts to send patch deployment status messages to the console, they will not be able to verify that the machine they contacted is a trusted machine.

1. Select **Tools > Console alias editor**.

   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine. For example:



DNS or hostnames:

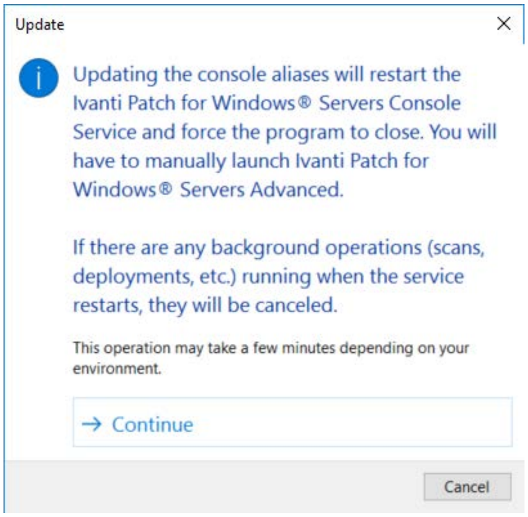
JOE-DELLWIN7

2. Type the names and/or IP addresses that you want to use as an alias for the console machine.

   You can specify IP addresses using either an IPv4 or IPv6 format.

3. Click **Update**.

   The following dialog is displayed:



Updating the console aliases will restart the Ivanti Patch for Windows® Servers Console Service and force the program to close. You will have to manually launch Ivanti Patch for Windows® Servers Advanced.

If there are any background operations (scans, deployments, etc.) running when the service restarts, they will be canceled.

This operation may take a few minutes depending on your environment.

4. Click either **Continue** or **Cancel**.

   If you click **Continue**, both the console service and the Ivanti Patch for Windows® Servers program will be automatically restarted; this is necessary in order to update the console aliases list. If you click **Cancel**, the console aliases list will not be updated.

IMPORTANT! The agents will not recognize a new alias until after they check-in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check-in; a check-in command issued from the console to an agent will not update the console certificate.

Synchronize Your Distribution Servers

You must update your distribution servers with the latest patches and/or scan engines and XML definition files contained on the console. This is particularly important if your agents use distribution servers to download these files. The distribution servers must be synchronized with the updated console files **prior** to the agents performing their check-in.

To synchronize your distribution servers:

1. Select **Help > Refresh files** to make sure the console contains all the latest files.
2. Select **Tools > Options > Distribution Servers**.
3. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.
4. In the top pane, select which distribution server you want to synchronize with the console.
5. Click **Add scheduled sync**.
6. Specify when you want the synchronization to occur and then click **Save**.
7. In the **Schedule automatic synchronization** pane, select the scheduled synchronization entry.
8. Click **Run now**.

Don’t worry if the agents happen to check in before you have finished synchronizing the distribution servers. The agents will be updated the next time a scheduled task is run or the agent updates its binaries.

Consider Enabling the Predictive Patch Feature

This feature became available in v9.2 so it is new if you are upgrading from v9.1. It enables Ivanti Patch for Windows® Servers to automatically download patches that are likely to be deployed in the near future. If you use distribution servers, you can synchronize Predictive Patch with your distribution servers so that they receive copies of the downloaded patches. The Predictive Patch option is enabled on the **Tools > Options > Downloads** tab and it is synchronized with your distribution servers by enabling the **Synchronize with Predictive Patch** option on the **Distribution Server** dialog. See the help system for complete details.

Re-establish Security Between Your Data Rollup Consoles

Note: This applies only if you are upgrading from v9.1 to v9.3. The security association established in v9.2 will continue to work in v9.3.

If you use multiple consoles and have a data rollup configuration in place, you must re-establish the security association between the central console and each remote console.

IMPORTANT! Once you begin the upgrade process, no data rollup activity will take place until both the central console and the remote console have been upgraded and the security association between the two consoles has been re-established. For this reason, it is strongly recommended that you upgrade your consoles in tandem and at a time when you expect very little data rollup activity.

On the Central Console

1. Upgrade the central console.
2. Select **Tools Options > Data Rollup** and verify that the **Accept and import results from a rollup sender** check box is enabled.

On Each Remote Console

1. Upgrade each remote console.
2. Select **Tools Options > Data Rollup**.
3. Verify the IP Address/Hostname and port values of the rollup console.
4. Click **Register**.

For more information on data rollup, in the online help system see **Administration > Managing Multiple Consoles > Data Rollup Configuration**.

Scan Your Virtual Machines

Note: This applies only if you are upgrading from v9.1 to v9.3.

If you have virtual machines defined in a machine group on either the **Hosted Virtual Machines** tab or the **Workstation Virtual Machines** tab, after performing the upgrade you must initiate a scan of these machines from either the home page or from within the machine group. You need to do this in order to re-establish the machine identities with Ivanti Patch for Windows® Servers. If you do not perform the scan, the **Virtual Server** and **Path** fields may not be displayed in Machine View and deployments to these machines may fail.

Check Your Custom User Settings

The following custom user settings are not preserved during the upgrade.

- Tools > Options > Display tab:
  - Recent item (days)
  - Archive items
  - Show only items created by me
  - Show main newsfeed
  - Show informational items in patch scan results
  - Show service packs in View -> Patches
- Tools > Options > Notifications and Warnings tab:
  - Warn before scheduling deployments
  - Close Refresh Files when finished
  - Warn if Protect Cloud sync is not enabled on this console
  - Warn before opening 7 or more bulletins
- Tools > Options > Patch tab:
  - Global thread pool

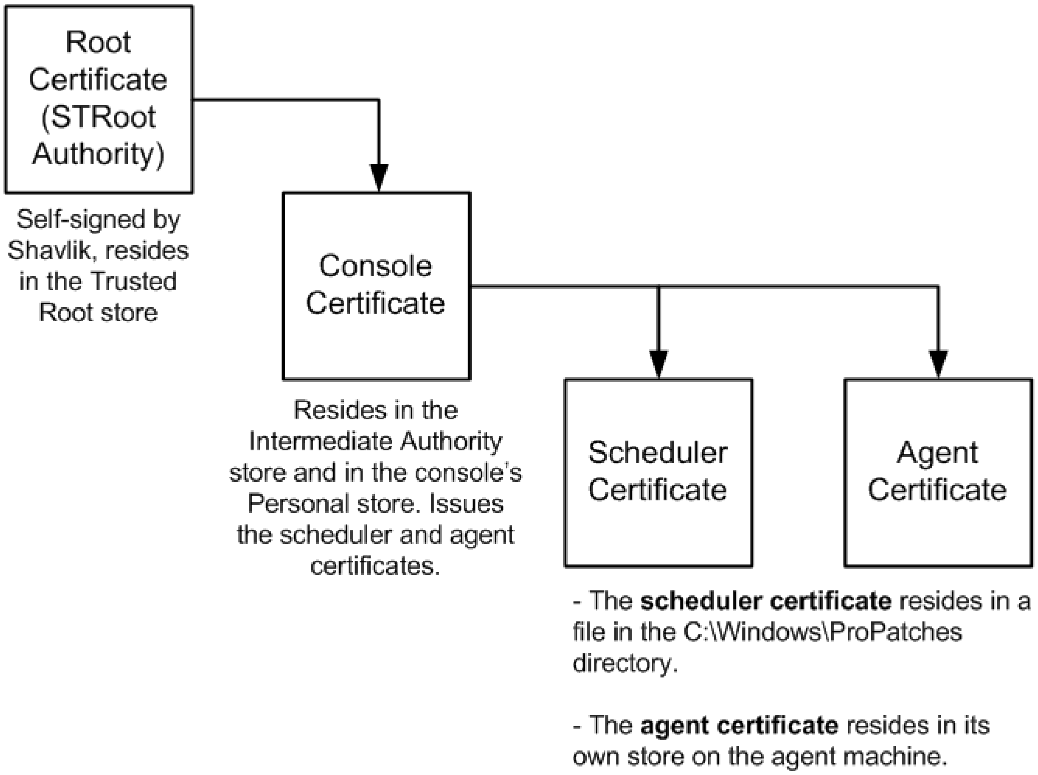
    This is new in v9.3 and it applies to all features in the product. In v9.2 the thread pool was defined on the Asset Scan template, but this is removed during the upgrade. The new default value may be different than what you had specified on the old thread pool option.
- Tools > Options > Logging tab:
  - Diagnostic patch scanning

- Deployment Tracker:
  - Update speed
  - Days to show
  - Show failures
  - Show in progress
  - Show successfully completed
- Reports dialog
  - Sort by IAVA ID
- ESXi Hypervisor Bulletins tab:
  - Only show latest
- Event History
  - Limit results to previous (days)
- ITScripts Results View
  - Results since

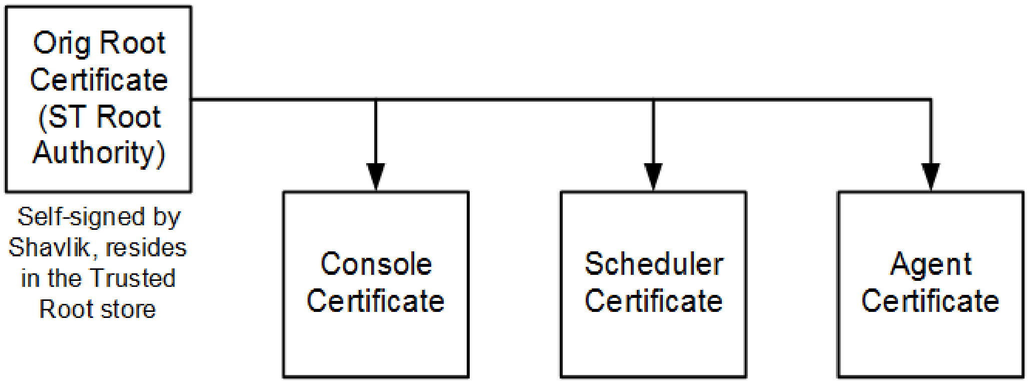
Know That v9.3 Uses a Different Certificate Structure

The certificate locations and relationships will change when you upgrade from Shavlik Protect 9.1 or 9.2 to Ivanti Patch for Windows® Servers 9.3. In v9.1 and v9.2, the scheduler and agent certificates were issued by the console certificate. In v9.3, the console certificate, the scheduler certificate and the agent certificate are all issued by the self-signed root certificate. The following diagrams illustrate the difference.

Before upgrading from Shavlik Protect 9.1 or 9.2


Root Certificate (STRoot Authority)
Self-signed by Shavlik, resides in the Trusted Root store
Console Certificate
Resides in the Intermediate Authority store and in the console's Personal store. Issues the scheduler and agent certificates.
Scheduler Certificate
Agent Certificate
- The **scheduler certificate** resides in a file in the C:\Windows\ProPatches directory.
- The **agent certificate** resides in its own store on the agent machine.

After upgrading to Ivanti Patch for Windows® Servers 9.3


Orig Root Certificate (ST Root Authority)
Self-signed by Shavlik, resides in the Trusted Root store
Console Certificate
Scheduler Certificate
Agent Certificate

- The console certificate resides on the Patch for Windows® Servers console in the computer account Personal store.
- The scheduler certificates reside in the /ProPatches/ Scheduler directory.
- On agent machines, the console certificate and the agent certificate reside in the Shavlik Protect Agent store.

After you have completed the upgrade process, Ivanti Patch for Windows® Servers 9.3 will begin its own process behind the scenes for managing the certificates.

- The existing console certificate will be removed from the Intermediate Authority store. This occurs within the first day or two of operation, depending on your maintenance activities.
- A new scheduler certificate will be issued from the root certificate whenever the Ivanti Scheduler is installed or an agentless deployment using the Ivanti Scheduler is performed. The old scheduler certificate (the one originally issued by the 9.2 console certificate) will be deleted.
- A new agent certificate will be issued from the root certificate whenever a new agent is installed or an existing agent's certificate needs to be reissued. The agent will store the agent certificate in its local store, and it will move the console certificate from the Trusted Root store on the agent machine to the Personal store. The old agent certificate (the one originally issued by the 9.2 console) will be deleted.

  Part of the agent upgrade process involves waiting for your agents to check in so they will receive a new agent certificate. This process may take a few days or weeks, depending on a number of factors, but it will all play out in the background. Your only involvement may be to monitor the Event History log to see if any problems occur that require your attention.

If You Use an Agent on the Console

If you have an agent installed on the Ivanti Patch for Windows® Server console, you should manually reinstall that agent. This should be done in order to ensure that the console agent is properly upgraded with the new agent certificate. No actions are required for agents that are installed on target machines.

SIGNIFICANT CHANGES AND ENHANCEMENTS IN IVANTI PATCH FOR WINDOWS® SERVERS 9.3

Complete details about each of the following topics can be found in the online help system:

https://help.ivanti.com/sh/help/en_US/PWS/93/PWS.htm

API Feature

The API feature is meant for advanced users who have a working knowledge of PowerShell and who want to perform tasks beyond those available through the Ivanti Patch for Windows® Servers user interface. You can use the API feature to:

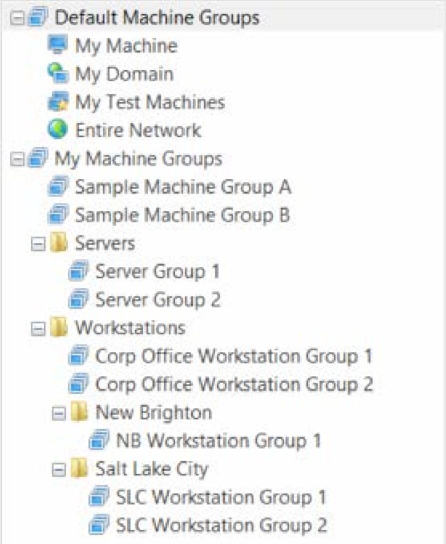
- Interact with different systems in your environment
- Script a sequence of complex events that contain dependencies
- Perform bulk operations or process list inputs from other systems
- Programmatically stage patch deployments or initiate patch downloads

For details on how to use the API feature, see the *API Quick Start Guide*.

Folder Paths in Navigation Pane

Another new feature is the ability to create a hierarchical structure for your machine groups, patch scan templates and patch deployment templates. If you create many groups or templates, you should consider organizing them into logical folders. Doing so will enable you to quickly locate and manage your groups and templates. Y

You can create as many folders and sub-folders as needed in the navigation pane. For example, you might choose to organize your groups based on the types of machines they contain, by location, etc.



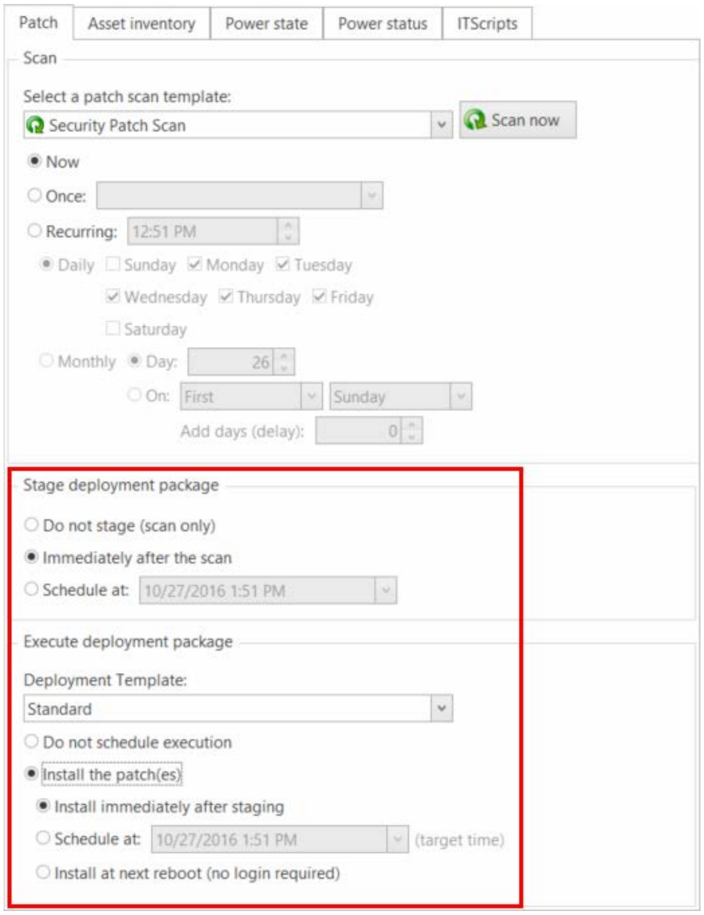
```
⊟ Default Machine Groups
    My Machine
    My Domain
    My Test Machines
    Entire Network
⊟ My Machine Groups
    Sample Machine Group A
    Sample Machine Group B
  ⊟ Servers
      Server Group 1
      Server Group 2
  ⊟ Workstations
      Corp Office Workstation Group 1
      Corp Office Workstation Group 2
    ⊟ New Brighton
        NB Workstation Group 1
    ⊟ Salt Lake City
        SLC Workstation Group 1
        SLC Workstation Group 2
```

Once created, you can drag and drop items from one folder to another. You can also right-click on any level of the hierarchy and perform an operation on all items at or below that level.

Staged Deployments

There are now four discrete schedulable points in the patch scanning and deployment process. This gives you much greater control over the entire process. You might:

- Perform a scan only
- Perform a scan and then stage the missing patches on the target machine at a specific time without installing the patches
- Perform a scan, stage the missing patches and then install the patches at a time of your choosing



Scan

Select a patch scan template: Security Patch Scan

● Now

○ Once:

○ Recurring: 12:51 PM

● Daily □ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday

○ Monthly ● Day: 26

○ On: First Sunday

Add days (delay): 0

Stage deployment package

○ Do not stage (scan only)

● Immediately after the scan

○ Schedule at: 10/27/2016 1:51 PM

Execute deployment package

Deployment Template: Standard

○ Do not schedule execution

● Install the patch(es)

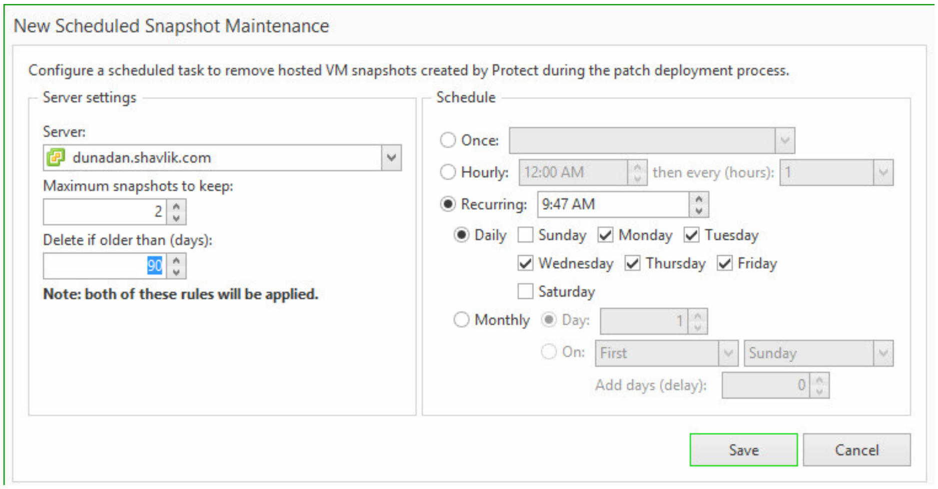
● Install immediately after staging

○ Schedule at: 10/27/2016 1:51 PM (target time)

○ Install at next reboot (no login required)

Scheduled Snapshot Maintenance

This new feature enables you to schedule a one-time or recurring task that will remove old virtual machine snapshots from the server. Previously, the only way you could remove old snapshots was in real time during a deployment task. To access this feature, select **Tools > Options > Snapshot Maintenance** and add a task.



New Scheduled Snapshot Maintenance

Configure a scheduled task to remove hosted VM snapshots created by Protect during the patch deployment process.

Server settings

Server: dunadan.shavlik.com

Maximum snapshots to keep: 2

Delete if older than (days): 90

Note: both of these rules will be applied.

Schedule

○ Once:

○ Hourly: 12:00 AM then every (hours): 1

● Recurring: 9:47 AM

● Daily ☐ Sunday ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☐ Saturday

○ Monthly ● Day: 1

○ On: First Sunday

Add days (delay): 0

Ability to Use a Third-Party CA

You have the option to use a trusted certificate authority (CA) from your own PKI infrastructure to issue a replacement root certificate for Ivanti Patch for Windows® Servers. This is not a necessity, but if you use a security tool that sees the default self-signed root certificate as a medium-level security risk, a process in now available for generating a replacement certificate. For more information, in the online help system see **Administration > Utilities > Generating a Certificate from a 3rd Party CA**.

Scheduled Remote Tasks Manager

There are several changes to the Scheduled Remote Tasks Manager.

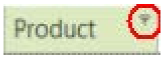
- It is now accessed by right-clicking on a machine in either Machine View or Scan View and then selecting **View scheduled tasks**.
- Information about power tasks and patch deployment tasks is now presented in a format that is similar to the Scheduled Console Tasks Manager.
- It will now display tasks that are scheduled on the remote machine using either the Ivanti Scheduler or the Microsoft Task Scheduler.

New Skins

A new option is now available on the **Display Options** dialog that enables you to specify the color theme you want to use for the Ivanti Patch for Windows® Servers interface. In addition to choosing a color that suits your eye, you might also consider a skin that provides lots of contrast, particularly in low-bandwidth RDP environments.

New Column Filter Capabilities

You can now apply filters to one or more column headers in the grid. You do this by hovering over a column header and then clicking the filter icon located in the upper-right corner. For example:



Use the filter menu to select which of the values currently contained in the column should be displayed.

Manual Download Method

A new **Download method** column indicates whether a patch can be downloaded automatically or if it must be downloaded manually. If the value in this column is **Automatic**, it means that Ivanti Patch for Windows® Servers can download the patch automatically. If the value is **Acquire from vendor** or some other value, it means that you must manually download the patch on your own and then move it into the patch download directory. Once the patch is there it can be deployed using the normal deployment process. If auto-deploy is used and a patch requires a manual download, the automatic deployment process will not work.

There may be a number of different reasons why a patch cannot be automatically downloadable. For example, you may have a patch that was created for a proprietary software program, or you may receive patches for a program that is no longer officially supported by the vendor.

Deployment Configuration Information

The **Deployment Configuration** dialog now shows information about the disk space requirements when deploying patches.

Consolidated Program Options

All program options are now consolidated in a single location. To view the options, select **Tools > Options**. The **Tools > Operations** menu has been removed.

Patch Group Filter

Patch View contains a new patch group filter. The **Show patches (above) currently included in the selected Patch Group** checkbox enables you to choose whether patches contained in the selected patch group will be displayed in the Patch View list.

Deployment Tracker UI Changes

Deployment Tracker has been redesigned to provide more detail about the patch deployment tasks that are currently in progress. You can also now use Deployment Tracker to cancel a deployment; the deployment preparation process must be complete but the actual deployment cannot have started.

Export Download Package

You can now export the download links for selected patches to a Comma Separated Values (CSV) file. This is especially useful for a console that is in a disconnected environment. The CSV file can be used by a connected machine to download the patches and the patches can then be copied into the disconnected console's patch directory.

Note: A File Downloader PowerShell script is available to assist with the file download process.

New IAVA Reports

Two new IAVA reports are now available: Machine Compliance (IAVA) and Machine Non-Compliance (IAVA). These two reports contain additional information that is required by the U.S. Government when submitting report data.

Global Thread Pool

Thread Management has moved from the template level to a system-wide pool and is now defined on the **Tools > Options > Patch** dialog. By default the program will use 8 threads per CPU core, but you can adjust the value as you see fit. This single value specifies the total number of threads that can be used during a patch scan or deployment, an asset scan or a power status scan.

Expanded Search Capabilities

The product’s search capabilities have been extended into more areas. You can now perform searches:

- On the **Hosted Virtual Machines** tab of a machine group.
- By right-clicking any machine group in the navigation pane and selecting **Search Machine Groups**. This enables you to locate specific machines and groups across all of your machine groups.
- Using the new Search box in the middle pane in Scan View and Machine View.